servicenow

취리히 보안 관리

마지막 업데이트 날짜: 2025년12월17일

기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

servicenow

해당 자료는 사용자 편의를 위해 번역 소프트웨어를 사용하여 번역되었습니다. 정확한 번역을 제공하기 위해 합당한 노력을 기울였지만, 사람이 직접 번역하는 것을 대체할 수 있는 기계 번역은 없습니다. 번역은 "기계 번역 결과 그대로" 제공됩니다. 다른 언어로 번역한 내용의 정확성, 신뢰성 또는 무결성에 대해서 명시적이든 묵시적이든 어떠한 보증도 하지 않습니다. 일부 콘텐츠는 번역 소프트웨어의 한계로 인해 정확하게 번역되지 않을 수 있습니다. 해당 자료의 공식 언어는 영어입니다. 번역에서 발생한 불일치 또는 차이점은 구속력이 없으며 규정 준수나 시행을 위한 법적 효력이 없습니다.

여기에 표시된 일부 예와 그래픽은 설명을 위해서만 제공됩니다.
ServiceNow 제품 또는 서비스와의 실제 연관 또는 연결을 의도하지 않았으며 그렇게 유추해서는 안 됩니다.

ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다. 기타 회사 및 제품 이름은 관련된 해당 회사의 상표일 수 있습니다.

다음 사이트에서 ServiceNow 웹 사이트 이용 약관을 읽어보십시오.
www.servicenow.com/terms-of-use.html

기계번역

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

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

목차

보안 운영 5
보안 운영 탐색 7
보안 인시던트 응답용 Now Assist 12
탐색 14
구성 17
보안 인시던트 종결에 사용 Now Assist 24
에이전트 워크플로우 사용 35
취약성 응답용 Now Assist 49
탐색 50
구성 53
생성 AI 기술 사용 55
에이전트 워크플로우 사용 62
참조 67
공격 표면 관리 애플리케이션 70
취약성 대응 71
애플리케이션 취약성 대응 784
컨테이너 취약성 대응 969
구성 준수 1040
취약성 대응 작업 공간 1281
소프트웨어 자재 명세서 1453
엔터프라이즈 보안 케이스 관리 애플리케이션 1488
보안 인시던트 응답 1490
위협 인텔리전스 2845
보안 태세 통제 3061
탐색 3063
작업 공간 사용 3077
완화 통제 사용 3095
참조 3116
사이버 보안 임원 대시보드 3127
벤치마크 점수에 대한 옵트인 3143
대상 설정 3144
Security Operations를 위한 보안 시뮬레이션 및 교육 통합 3144
용 위험 및 준수 대시보드 GRC: 메트릭 3147
위협 인텔리전스 보안 센터 3155
탐색 3156
구성 3161
통합 3164
관리자 3244
참조 3285

기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용 3292
Data Loss Prevention Incident Response 3499
탐색 3500
구성 3503
관리자 3504
인시던트 관리 3555
인바운드 통합 3575
통합 3578
보안 운영 공통 기능 3643
Security Operations에서 필터 그룹 생성 및 정의 3645
공유 데이터 변환 3647
보안 운영 이메일 처리 3650
보안 운영 필드 매핑 3659
보안 운영 필드 값 변환 3663
보안 운영 보강 데이터 매핑 3664
보안 운영 사용자 정의 에스컬레이션 3666
도메인 분리 속성 재정의 생성 3667
운영 체제 그룹 작성 3668
보안 태그 그룹 및 태그 설정 3670
보안 주석 3674
Security Support Common 앱과 함께 설치되는 구성요소 3676
보안 운영 애플리케이션에 대한 역할별 모듈 액세스 3677
〔store-future: BEGIN review〕
〔End〕
보안 운영 검색 4344
Security Operations Integrations 참조 4344
보안 운영 워크플로우 트리거 4438
Security Operations 오케스트레이션 4440
보안 운영 시나리오 및 예시 4440
〔store-future: BEGIN review〕
자동화를 사용하여 위협 분석 시간 단축 4440
〔store-future: BEGIN review〕
〔End〕
세간의 이목을 끄는 취약성 우선순위 지정 4446
〔store-future: BEGIN review〕
〔End〕
〔End〕
보안 운영 그리고 ServiceNow Store 4448
에서 처음으로 애플리케이션 ServiceNow Store 다운로드 4449
보안 운영 통합 설치 4454
에서 이전에 다운로드한 애플리케이션 업데이트 ServiceNow Store 4458
인스턴스를 다음 제품군 릴리스로 업그레이드 4459

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 운영

ServiceNow# 보안 운영 애플리케이션은 보안 도구의 인시던트 데이터를 지능형 워크플로우, 자동화, 데이터 시각화 및 IT와의 긴밀한 연결을 사용하는 구조화된 응답 엔진으로 임포트하여 위협이 조직에 미치는 영향에 따라 우선순위를 지정하고 위협을 해결합니다.

다음 타일 중 하나를 선택하여 시작합니다.

보안 운영 애플리케이션 및 해당 작업 공간

애플리케이션이 보안 태세를 보안 운영 개선하는 데 어떻게 도움이 되는지 알아보십시오.

보안 인시던트 응답용 **Now Assist**

보안 인시던트 응답용 Now Assist가 보안 인시던트 응답 작업 공간 및 코어 UI(UI16)에서 생성형 AI(GenAI) 기술을 지원하는 ServiceNow# 방법에 대해 알아봅니다.

취약성 응답용 **Now Assist**

가 취약성 대응 작업 공간 및 코어 UI(UI16)에서 생성형 AI(GenAI) 기술을 지원하는 ServiceNow# 방법에 대해 취약성 응답용 Now Assist 알아봅니다.

기계 면역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

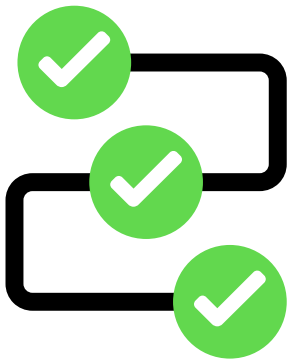
공격 표면 관리 애플리케이션

사이버 공격 표면 전반에서 취약성을 식별하고 수정하는 데 도움이 되는 Vulnerability Response의 애플리케이션에 대해 알아봅니다.

엔터프라이즈 보안 케이스 관리 애플리케이션

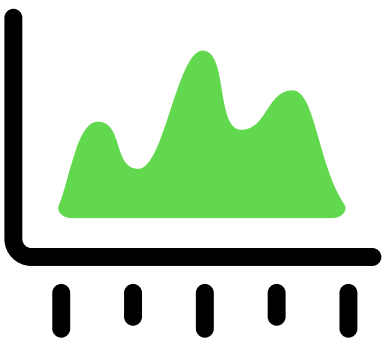
진화하는 중요한 보안 인시던트를 분석, 격리 및 수정하는 데 도움이 되는 Security Incident Response의 애플리케이션에 대해 알아봅니다.

보안 태세 통제 애플리케이션



전반적인 보안 태세에 대한 인사이트를 얻는 데 도움이 되는 애플리케이션에 대해 알아봅니다.

사이버 보안 임원 대시보드

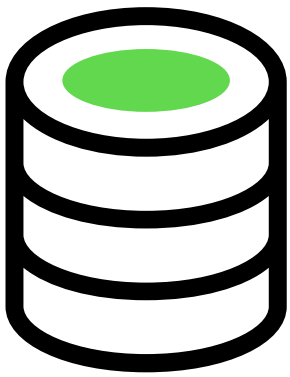


사이버 보안 임원 대시보드가 다양한 SecOps 제품의 데이터를 통합 대시보드로 통합하는 방법을 알아보십시오.

위협 인텔리전스 보안 센터

(TISC) 플랫폼이 위협 인텔리전스 보안 센터 위협 인텔리전스의 집계 및 관리를 위한 기술 솔루션을 제공하는 방법을 알아보십시오.

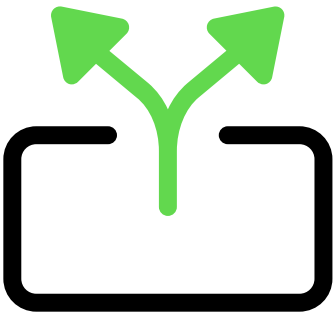
데이터 손실 방지 인시던트 응답



고객의 중요한 정보를 관리하고 데이터 손실 채널을 식별 및 보호하는 방법을 알아봅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 운영 공유 애플리케이션



에서 공통 기능을 보안 운영제공하는 기능 및 모듈에 대해 알아봅니다.

보안 운영 시나리오 및 예시

에서 애플리케이션을 ServiceNow# Store 가져오는 보안 운영 방법과 제품을 사용하는 동안 사용할 수 있는 애플리케이션의 시나리오에 대해 자세히 알아보십시오.

문제 해결 및 도움 받기

- Security Operations 리소스 라이브러리
- Security Operations 커뮤니티
- 알려진 오류 포털에서 알려진 오류 문서 검색
- 연락처 고객 서비스 및 지원

보안 운영 탐색

ServiceNow 보안 운영 애플리케이션과 ServiceNow AI Platform#. 보안 팀과 IT 팀을 연결하여 위협이 조직에 미치는 영향에 따라 우선순위를 정하고 위협을 해결할 수 있도록 지원합니다.

보안 운영 개요

애플리케이션 제품군을 사용하면 보안 운영 전반적인 보안 태세를 개선하여 자산을 보호할 수 있습니다. 예를 들어, , 와 같은 보안 인시던트 응답취약성 대응애플리케이션을 기존 보안 태세 통제 보안 도구와 통합함으로써 SOC(Security Operation Center) 분석가, 관리자 및 IT 팀은 다음을 수행할 수 있습니다.

- 빠르게 진화하는 사이버 및 보안 위협에 대응
- 취약성 식별, 우선순위 지정 및 정정
- 전체 자산 인벤토리 보기
- 전반적인 보안 도구 범위 결정
- 지능형 워크플로우와 ServiceNow GenAI(생성형 AI 기술)로 보안 인시던트를 더 빠르게 해결합니다. 자세한 내용은 보안 인시던트 응답용 Now Assist 문서를 참조하십시오.

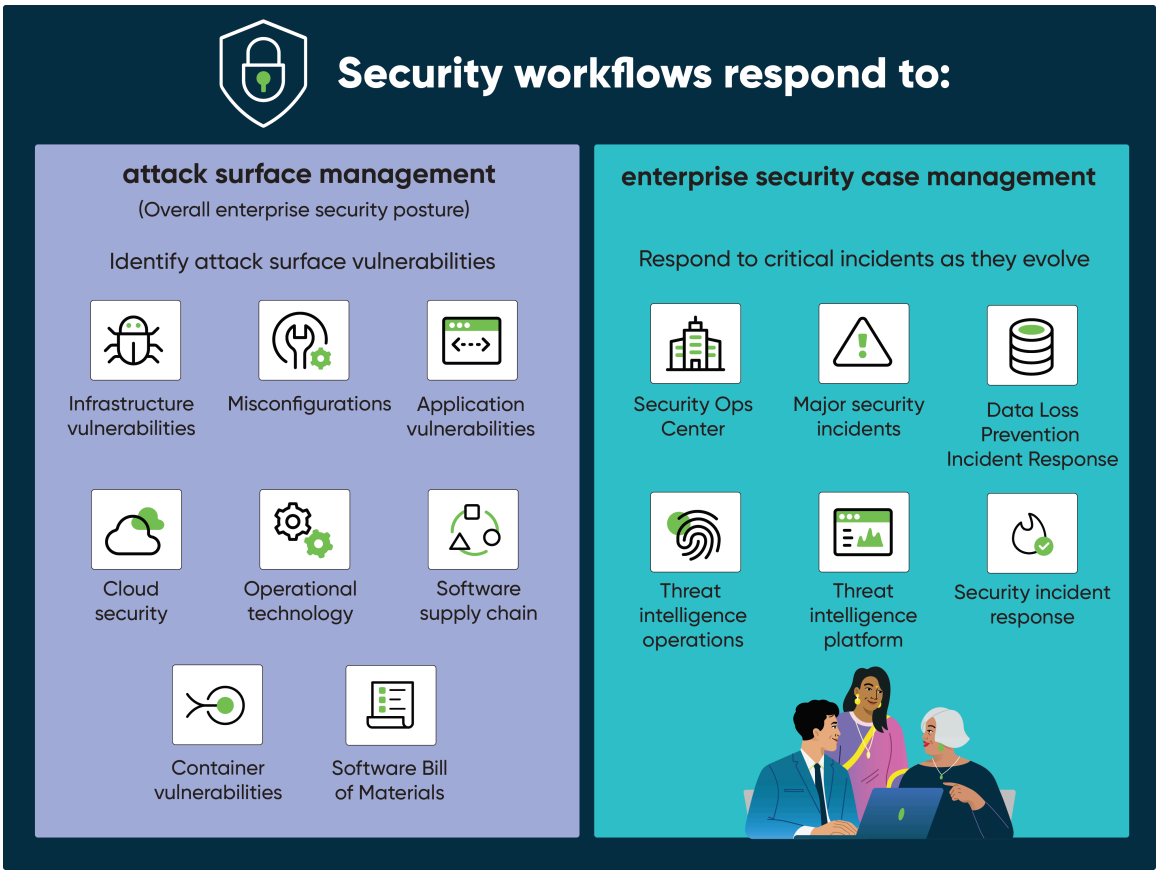
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 운영 워크플로우용 애플리케이션

보안 운영 애플리케이션은 워크플로우와 관련하여 크게 두 가지 범주로 보안 운영 분류됩니다.

- 공격 표면 관리 - 취약성을 예측, 이해 및 종결하는 데 도움이 되는 애플리케이션 및 도구입니다.
- 엔터프라이즈 보안 케이스 관리 - 중요한 인시던트에 신속하게 대응하는 데 도움이 되는 애플리케이션 및 도구입니다.

보안 워크플로우



보안 운영 애플리케이션의 두 가지 범주와 이를 통해 엔터프라이즈 환경에서 해결할 수 있는 사용 사례가 있습니다.

보안 운영 애플리케이션의 이점

차세대 사용자 인터페이스(작업 공간)를 사용하여 애플리케이션과 데이터를 봅니다 보안 운영 . 작업 공간을 사용하면 조직의 보안 분석가, SOC(보안 운영 센터) 관리자 및 정정 전문가가 한 위치에서 다음 유형의 워크플로를 모니터링하고 관리할 수 있습니다.

- 초기 분석부터 방지, 근절, 복구에 이르는 보안 인시던트의 수명주기입니다.
- 가장 중요하게 생각하는 취약성이므로 수정을 위해 IT 팀에 보낼 취약성을 전략적으로 결정할 수 있습니다.
- 자산에 대해 임포트된 정보를 보고하고 모니터링하는 보안 도구 범위 및 자산 청결성에 대한 주요 통찰력과 주요 사용 케이스입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

공격 표면 관리 애플리케이션

위협을 예측하고 취약성을 식별하는 데 도움이 되는 애플리케이션

애플리케이션	설명	사용자
보안 태세 통제	자산 인벤토리 및 임포트한 데이터를 기반으로 보안 도구가 얼마나 잘 배포되고 자산을 포괄하는지에 대한 인사이트를 얻습니다. 데이터 임포트에는 서비스 그래프 커넥터와 하드웨어 자산 관리(HAM) 및 ITOM 디스커버리와 같은 ServiceNow 제품이 지원됩니다. 정책을 기반으로 하는 감사는 인터넷 노출 및 알려진 취약성과 같은 고위험 조합의 정정 우선 순위를 지정하는 데 도움이 됩니다. 사용자 지정 정책 및 인사이트를 생성하여 자산이 내부 보안 도구 구성 표준을 준수하는지 모니터링합니다.	• CISO • 정보 보안 분석가 • 보안 운영 관리자 • IT 운영 엔지니어 • 서비스 소유자(정정 소유자 가상 사용자)
취약성 대응	타사 취약성 스캐너 및 평가 도구는 취약성이 다음과 같은 유형의 자산에 제기하는 위험을 식별하는 데 도움이 됩니다. • 인프라(호스트) • 컨테이너 • 애플리케이션 • 소프트웨어 자재 명세서 이러한 도구에서 식별된 취약성은 조직의 자산 유지 관리 및 보안을 담당하는 보안 및 IT 팀에 위험으로 해석됩니다.	• CISO • 정보 보안 분석가 • 보안 운영 관리자 • IT 운영 엔지니어 • 서비스 소유자(정정 소유자 가상 사용자)
구성 준수	보안 또는 회사 정책을 준수하는지 확인합니다. 타사 SCA(Secure Configuration Assessment) 통합에서 얻은 테스트 결과를 통해 미준수 구성 항목을 식별하고, 우선순위를 지정하고, 정정합니다.	• CISO • 정보 보안 분석가 • 보안 운영 관리자 • IT 운영 엔지니어 • 서비스 소유자(정정 소유자 가상 사용자)

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

엔터프라이즈 보안 케이스 관리 애플리케이션

중요한 보안 위반 및 인시던트에 대응하는 데 도움이 되는 애플리케이션

애플리케이션	설명	사용자
보안 인시던트 응답	정정 속도를 높이는 강력한 워크플로우 및 자동화 도구를 적용하여 중요한 인시던트를 식별하는 프로세스를 단순화합니다. 기존 SIEM(보안 정보 및 이벤트 관리자) 도구를 보안 인시던트 응답 보안 운영 애플리케이션과 통합하여 다양한 소스에서 위협 데이터를 임포트하고 우선순위가 지정된 보안 인시던트를 자동으로 생성합니다.	• CISO • 정보 보안 분석가 • 보안 운영 관리자 • 위협 인텔리전스 분석가
중요 보안 인시던트 관리	주요 보안 인시던트 관리 기능은 기존 보안 인시던트 응답 제품 기능과 함께 작동합니다. 여기에는 보안 분석가가 표준 보안 인시던트를 중요 보안 인시던트로 에스컬레이션하여 새로운 제품 기능을 사용하여 정정 프로세스를 지원할 수 있는 기능이 포함됩니다. 검색부터 분석까지 MSI(주요 보안 인시던트)의 진행 상황을 추적합니다. 솔루션을 제안하고, 보안 인시던트와 종결을 승격 및 연결합니다.	• CISO • 정보 보안 분석가 • 보안 운영 관리자 • IT 운영 엔지니어 • 서비스 소유자(정정 소유자 가상 사용자) • 총회
데이터 손실 방지 인시던트 응답	DLP IR(Data Loss Prevention Incident Response)을 사용하면 엔드포인트, 네트워크, 이메일 및 클라우드와 같은 여러 소스에서 DLP 인시던트의 정정 워크플로우를 검토하고 관리할 수 있습니다. DLP 애플리케이션을 사용하여 데이터 손실 채널을 식별, 응답 및 보호할 수 있습니다.	• CISO • 정보 보안 분석가 • 보안 운영 관리자
위협 인텔리전스	인시던트 대응 팀이 위협 조회, 검색, 상관 관계를 자동화할 수 있습니다. MITRE	• CISO • 정보 보안 분석가

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

중요한 보안 위반 및 인시던트에 대응하는 데 도움이 되는 애플리케이션

애플리케이션	설명	사용자
	ATT&CK와의 통합을 통해 탐지 및 완화 범위를 측정하고 이해할 수 있으며 위협 헌팅을 지원할 수 있습니다.	• 보안 운영 관리자 • 위협 인텔리전스 분석가
위협 인텔리전스 보안 센터(TISC)	여러 소스의 위협 인텔리전스를 집계, 선별 및 관리하고 위협 인텔리전스 케이스 관리를 수행합니다. 캠페인을 추적하고, 위협 인텔리전스를 운영하고, 실행 가능한 인텔리전스에 대응합니다.	• CISO • 정보 보안 분석가 • 보안 운영 관리자 • 위협 인텔리전스 분석가

다음으로 살펴볼 내용

작업 공간을 시작하려면 보안 운영 타일을 선택합니다.

보안 인시던트 응답 작업 공간	취약성 관리자 작업 공간	보안 태세 통제 작업 공간
Security Incident Response 작업 공간에 대해 알아보기	취약성 관리자 작업 공간에 대해 알아보기	보안 태세 통제 작업 공간에 대해 알아보기

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약성 평가 작업 공간

취약성 평가 작업 공간에 대해 알아보기

IT 정정 작업 공간

IT 정정 작업 공간에 대해 알아보기

소프트웨어 자재 명세서 작업 공간

소프트웨어 자재 명세서 작업 공간에 대해 알아보기

위협 인텔리전스 보안 센터**(TISC)** 작업 공간

TISC 작업 공간에 대해 알아보기

데이터 손실 방지**(DLP)** 인시던트 응답 작업 공간

DLP 작업 공간에 대해 알아보기

Major Security Incident Management(MSIM) 작업 공간

MSIM 작업 공간에 대해 알아보기

기계번역

문제 해결 및 도움 받기

- Security Operations 리소스 라이브러리
- Security Operations 커뮤니티
- 알려진 오류 포털에서 알려진 오류 문서 검색
- 연락처 고객 서비스 및 지원

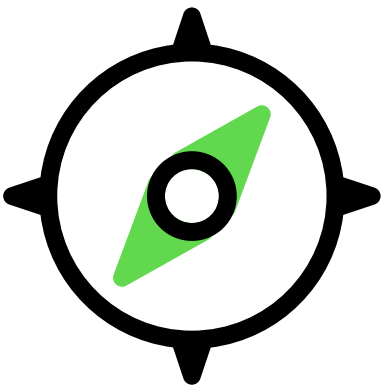
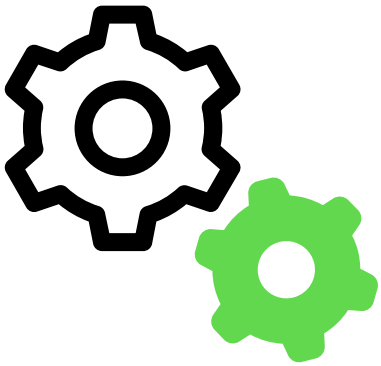
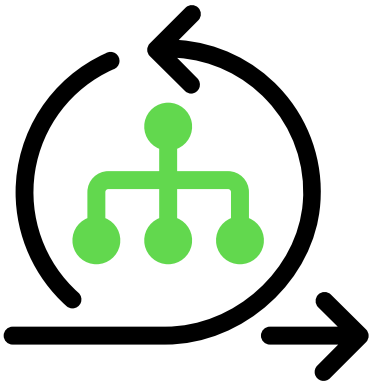
보안 인시던트 응답용 **Now Assist**

보안 분석가는 지능형 워크플로우와 ServiceNow 생성형 AI 기술을 사용하여 보안 인시던트를 해결할 수 있습니다. 보안 관리자는 보안 인시던트의 컨텍스트 및 종결 메모를 간결하고 읽기 쉬운

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

형식으로 신속하게 검토하고, 사후 인시던트 분석 데이터를 보고, 애플리케이션에 대한 권장 정정 단계를 확인할 수 있습니다 보안 인시던트 응답용 Now Assist .

시작하기

탐색	구성	사용
		
보안 인시던트 응답용 Now Assist에 대해 알아보기	에 대한 기술을 구성하고 활성화하는 방법 알아보기 보안 인시던트 응답용 Now Assist	생성형 AI를 사용하여 보안 인시던트에 대한 상세 정보를 요약하고 종결 메모를 생성하는 방법에 대해 알아봅니다. 보안 인시던트 응답용 Now Assist

중요사항:

- 국내 SKU를 보유한 고객은 일부 모델 제공자를 이용할 수 없으며, 일부 Now Assist 제품/기능은 현재 국내 고객에게 제공되지 않습니다. 자세한 내용은 Now Support 지식베이스의 KB1584492 문서를 참조하십시오. 향후 릴리스에서 모델 제공자 가용성 업데이트를 확인하십시오.
- 일부 Now Assist 제품/기능은 현재 FedRAMP, NSC DOD IL5 또는 호주 IRAP 보호 데이터 센터, 자체 호스팅 고객 또는 기타 제한된 환경에서는 사용할 수 없습니다. 자세한 내용은 Now Support 지식베이스의 KB0743854 문서를 참조하십시오. 향후 릴리스에서 가용성 업데이트를 확인하십시오.
- 일부 Now Assist 제품/기능은 현재 일부 지역의 고객에게만 제공됩니다. 향후 릴리스에서 가용성 업데이트를 확인하십시오.

문제 해결 및 도움 받기

- Security Operations 리소스 라이브러리
- Security Operations 커뮤니티
- 알려진 오류 포털에서 알려진 오류 문서 검색
- 연락처 고객 서비스 및 지원

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

AI 제한 사항

이 애플리케이션은 데이터의 패턴을 기반으로 예측을 생성하는 빠르게 진화하는 연구 분야인 인공 지능(AI) 및 머신 러닝을 사용합니다. 따라서 이 애플리케이션이 항상 정확하고 완전하거나 적절한 정보를 생성하지 못할 수도 있습니다. 또한 이 애플리케이션이 사용 사례에 대해 완전히 학습되거나 테스트되었다는 보장은 없습니다. 이러한 문제를 완화하기 위해 사용 사례에 대한 정확성, 피해 및 적절성에 대해 이 애플리케이션의 사용을 테스트 및 평가하고, 출력에 대한 사람의 감독을 적용하고, 의사 결정 목적으로 AI 생성 출력에만 의존하지 않는 것은 사용자의 책임입니다. 이는 의료, 재무, 법률, 고용 보안 또는 인프라와 같이 결과적인 영향을 미치는 영역에 이 애플리케이션을 배포하려는 경우 특히 중요합니다. ServiceNow에서 업데이트할 수 있는 ServiceNow의 AI 이용 목적 제한 정책을 준수하는 데 동의합니다.

데이터 처리

이 애플리케이션을 사용하려면 ServiceNow 고객의 개별 인스턴스에서 사용자의 인스턴스가 있는 지역과 다른 데이터 센터 지역에 있을 수 있는 중앙 집중식 ServiceNow 환경으로 데이터를 전송해야 하며, Microsoft Azure와 같은 외부 공급업체 클라우드 제공자에게 데이터를 전송해야 합니다. 이 데이터는 당사의 CORE Compliance 포털을 통해 제공되는 당사의 정책을 포함하여 ServiceNow의 내부 정책 및 절차에 따라 처리됩니다.

데이터 수집

ServiceNow는 이 애플리케이션의 입력, 출력 및 출력 편집 내용을 수집하고 사용하여 ServiceNow 모델 및 AI 제품을 포함한 ServiceNow 기술을 개발하고 개선합니다. 또한 이 애플리케이션은 보안 인시던트, 인시던트, 변경 요청, 문제 및 취약한 항목의 데이터입니다. 고객은 Now Assist옵트아웃 페이지에 설명된 대로 언제든지 향후 데이터 수집을 옵트아웃할 수 있습니다.

자세한 내용은 Now Assist 설명서를 참조하십시오.

보안 인시던트 응답용 **Now Assist** 탐색

보안 분석가는 지능형 워크플로우와 ServiceNow 생성형 AI 기술을 사용하여 애플리케이션과의 작업 흐름 내에서 보안 인시던트를 분류, 조사 및 종결할 수 있습니다 보안 인시던트 응답용 Now Assist .

보안 인시던트 응답용 **Now Assist** 개요

생성형 AI 기술과 에이전트 워크플로를 통해 보안 분석가는 다음을 수행할 수 있습니다.

- 보안 인시던트 상세 정보를 요약하고 간결하고 읽기 쉬운 형식으로 컨텍스트를 신속하게 검토합니다.
- 보안 인시던트에 대한 권장 다음 단계를 생성합니다.
- 사후 인시던트 분석 데이터를 생성합니다.
- 종결 메모를 생성합니다.
- 상관 관계 인사이트 생성

보안 분석가는 결과, 인시던트 상세 정보 및 종결 메모를 다른 분석가, 관리자 및 주요 이해 관계자와 공유할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 인시던트 응답용 **Now Assist** 사용자

사용자

사용자	설명
보안 분석가 및 관리자	보안 인시던트 상세 정보를 미리 보고, 잠재적인 영향을 확인하고, 생성형 AI를 사용하는 보안 인시던트 요약을 통해 이미 수행된 주요 정정 작업을 봅니다. 요약 및 권장되는 다음 단계(작업)를 통해 분석가와 관리자는 조사를 미리 시작하고 보안 인시던트를 종결하는 데 도움을 받을 수 있습니다. 생성형 AI를 사용하여 종결 메모의 초안을 자동으로 생성합니다. 보안 인시던트에 대한 종결 메모는 정정 및 방지 활동과 종결과 관련된 기타 관련 상세 정보를 기반으로 신속하게 생성됩니다.

보안 인시던트 응답용 **Now Assist** 이점

보안 인시던트 응답용 **Now Assist** 기능

혜택	기능	사용자
작업 메모와 상황별 정보를 간결하고 읽기 쉬운 형식으로 신속하게 검토하여 활동 스트림이 긴 보안 인시던트를 신속하게 분류합니다.	다음 정보를 포함하는 보안 인시던트에 대한 요약을 생성합니다. • 문제 • 상세 정보 • 관찰 결과 • 수행한 주요 작업 • 종결 상세 정보	• 보안 분석가 • 보안 관리자
보안 인시던트가 종결될 준비가 되면 자동으로 종결 메모 초안을 생성합니다. 분석가는 보안 인시던트를 종결하기 전에 AI 기술로 생성된 콘텐츠를 편집, 제거 또는 자체 메모를 추가하여 수정할 수 있습니다.	보안 인시던트 종결 메모 생성	• 보안 분석가 • 보안 관리자
요청 시 보안 인시던트를 종결하는 데 도움이 되도록 워크플로우 내에서 권장되는 다음 단계를 생성합니다.	보안 인시던트 권장 작업 생성	• 보안 분석가 • 보안 관리자
근본 원인 분석, 영향 평가 및 보안 인시던트 종결 워크플로우 내에서 학습한 교훈을 포함하는 사후 인시던트 분석을 생성합니다.	사후 인시던트 분석 생성	• 보안 분석가 • 보안 관리자
동일한 영향을 받는 사용자, 구성 항목(CI) 또는 옵저버블과 관련된 과거 이벤트에 현재 인시던트를 연결합니다.	상관 관계 인사이트 생성	• 보안 분석가 • 보안 관리자

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 인시던트 응답용 **Now Assist** 기능

혜택	기능	사용자
패널에서 요약 및 종결 메모 Now Assist 에 액세스하여 보안 인시던트의 상세 정보를 빠르게 알아봅니다.	패널에서 생성 AI 요약 및 종결 메모에 Now Assist 액세스합니다. 패널의 보안 인시던트에 대한 자세한 기본 정보에 대한 요청을 입력합니다.	• 보안 분석가 • 보안 관리자
필요에 맞게 요약 및 종결 메모에 대한 생성형 AI 기술을 사용자 지정합니다.	기술을 복사하고 관련 테이블 필드를 선택하고, 기술의 가용성을 정의하고, 기술이 표시되는 위치를 선택합니다.	관리자

다음으로 살펴볼 내용

보안 인시던트 응답용 Now Assist 구성 및 사용에 대한 자세한 내용은 다음을 참조하십시오.

- 보안 인시던트 응답용 Now Assist 구성
- 를 사용하여 보안 인시던트 요약 보안 인시던트 응답용 Now Assist
- 를 사용하여 보안 인시던트에 대한 종결 메모 생성 보안 인시던트 응답용 Now Assist
- 를 사용하여 패널에서 상관 관계 인사이트 Now Assist 생성 보안 인시던트 응답용 Now Assist
- 를 사용하여 보안 인시던트에 대한 권장 작업 생성 보안 인시던트 응답용 Now Assist
- 를 사용하여 보안 인시던트에 대한 사후 인시던트 분석 생성 보안 인시던트 응답용 Now Assist
- 보안 인시던트 응답용 Now Assist에 대한 입력 및 트리거

보안 인시던트 응답용 **Now Assist**에 대한 지원 정보

보안 인시던트 응답용 Now Assist 애플리케이션과 관련된 중요한 정보의 간략한 개요를 확인합니다.

지원되는 버전

버전 2.0.1 보안 인시던트 응답용 Now Assist 은 다음을 지원합니다.

- Legacy UI(UI16): 보안 인시던트 응답 핵심 애플리케이션, v13.6.4
- 보안 인시던트 응답 작업 공간 (),SIR Workspace v1.7.0
- v6.0.1용 ServiceNow AI Platform# Now Assist

지원되는 사용자 인터페이스

여기에는 보안 인시던트 응답용 Now Assist 다음 테이블에 나열된 생성형 AI 기술이 포함됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 인시던트 응답용 **Now Assist** 지원되는 인터페이스 및 기술

인터페이스	기능
보안 인시던트 응답	• 보안 인시던트 요약입니다. • 보안 인시던트에 권장되는 다음 단계 생성입니다. • 근본 원인 분석, 영향 평가 및 학습한 교훈을 포함하는 사후 인시던트 분석 생성. • Now Assist 패널. • 종결 메모 생성. • 패널의 상관 관계 인사이트. Now Assist
Legacy UI16	• 보안 인시던트 요약 • 보안 인시던트에 권장되는 다음 단계 생성입니다. • 근본 원인 분석, 영향 평가 및 학습한 교훈을 포함하는 사후 인시던트 분석 생성. • Now Assist 패널. • 종결 메모 생성. • 패널의 상관 관계 인사이트. Now Assist

보안 인시던트 응답용 **Now Assist** 구성

보안 인시던트 응답용 Now Assist 이 애플리케이션은 및 코어 UI(UI16)에서 보안 인시던트 응답 작업 공간Legacy 지원됩니다. 콘솔의 Now Assist 관리자 안내 설정을 사용하여 를 구성할 보안 인시던트 응답용 Now Assist수 있습니다.

구성 개요

AI 개발 프로그램과 데이터를 ServiceNow# 공유하면 예측 정확도, 사용자 경험을 개선하고 비즈니스 요구 사항에 맞게 제품을 조정하며 활성화된 Now Assist 기술에 대한 환각을 줄이는 데 도움이 되는 관련 데이터를 제공할 수 있습니다.

참여를 원하지 않는 경우 콘솔의 Now Assist 관리자 데이터 공유에서 인스턴스를 옵트아웃 ServiceNow 하도록 선택할 수 있습니다. Opt out of data sharing for Now Assist 문서를 참조하십시오. 해당 기능을 사용하는 Now Assist 모든 인스턴스에 대해 옵트아웃 프로세스를 반복합니다.

Now Assist 관리자 콘솔을 사용하여 보안 인시던트 응답용 Now Assist를 구성합니다. 이 콘솔에는 애플리케이션을 설치하고 생성 AI 기술을 구성하는 데 필요한 모든 것이 포함되어 있습니다. 자세한 내용은 Configuring Now Assist Admin features 문서를 참조하십시오.

다음 표에는 Now Assist 관리자 콘솔에서 액세스할 수 있는 기능과 기술이 나열되어 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Now Assist 관리자 콘솔의 보안 인시던트 응답용 **Now Assist** 기능 및 기술

Now Assist 기술 제품	보안 인시던트 기술
보안 인시던트 응답용 Now Assist	보안 인시던트 요약 주: 인시던트 요약은 초안 이외의 모든 상태의 보안 인시던트를 지원합니다.
	해결 메모 생성.
	보안 인시던트 권장 작업 보안 인시던트 권장 작업 기술은 종결 및 취소됨 이외의 모든 상태의 보안 인시던트를 지원합니다. 주: 권장 작업 기술이 보안 인시던트에 적용되도록 AI 검색 애플리케이션을 활성화해야 합니다. 인스턴스에서 AI 검색이 활성화되어 있는지 확인하려면 다음으로 이동합니다. 모두 〉 **AI** 검색 〉 **AI** 검색 상태. 페이지에 AI 검색이 활성화되어 있지 않다고 표시되면 지원 센터에 문의하십시오. 상관 관계 인사이트는 모든 상태의 보안 인시던트를 지원합니다.
	사후 인시던트 분석 생성

1. Install Now Assist plugins .

   보안 인시던트 응답용 Now Assist 애플리케이션(sn_sec_gen_ai) 및 보안 인시던트 응답 Core [sn_si] 애플리케이션을 설치합니다.

2. 에 대한 기술 구성 및 활성화 보안 인시던트 응답용 Now Assist

   기술에 대한 세부 정보를 구성하고 검토합니다. 에서 안내 설정기술을 활성화합니다.

안내 설정을 사용하여 보안 인시던트 응답용 **Now Assist** 구현

안내 설정은 ServiceNow 인스턴스에서 보안 인시던트 응답용 Now Assist를 구성하는 데 도움이 되는 일련의 작업을 제공합니다. 를 보안 인시던트 응답용 Now Assist열려면 안내 설정 다음으로 이동합니다. 모두 〉 **Now Assist** 관리자 〉 기능.

자세한 내용은 에 대한 기술 구성 및 활성화 보안 인시던트 응답용 Now Assist 문서를 참조하십시오.

에 대한 기술 구성 및 활성화 보안 인시던트 응답용 **Now Assist**

에서 안내 설정기술에 대한 세부 정보를 구성하고 검토합니다. 에서 기술을 활성화할 수 있습니다 안내 설정.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 〉 **Now Assist** 관리자 〉 기능.
2. 탐색 패널에서 기술을 선택한 상태의 목록에서 보안 작업을 선택합니다.
   이러한 보안 인시던트 기술은 보안 인시던트 카드에 표시됩니다.
   - 보안 인시던트 권장 작업

     권장 작업 기술이 보안 인시던트에 적용되도록 AI 검색 애플리케이션을 활성화해야 합니다. 인스턴스에서 AI 검색이 활성화되어 있는지 확인하려면 다음으로 이동합니다. 모두 〉 **AI** 검색 〉 **AI** 검색 상태. 페이지에 AI 검색이 활성화되어 있지 않다고 표시되면 지원 센터에 문의하십시오.
   - 사후 인시던트 분석
   - 상관 관계 인사이트 생성
   - 보안 인시던트 요약
   - 해결 메모 생성
3. 상세 정보 보기를 선택합니다.
   애플리케이션에 포함된 기술은 편집할 수 없습니다. 기본 설정을 편집하려면 복사본을 만들어야 합니다. 기술 사용자 지정에 대한 자세한 내용은 다음 문서를 참조하십시오 보안 인시던트 응답용 Now Assist 기술 사용자 지정.
4. 원하는 기술에 대해 기술 활성화 를 선택합니다.
5. 단계에 따라 를 안내 설정사용하여 기술을 구성하고 활성화합니다.

   주:
   일부 기술의 경우 아래 나열된 구성 단계가 모두 필요하지는 않습니다. 왼쪽 패널에 표시되는 작업만 선택하고 프롬프트를 따릅니다. 작업을 완료한 후 기술을 활성화합니다.

   a. 탐색 패널에서 입력 선택을 선택하여 선택한 기술에 대한 입력 또는 트리거를 구성합니다.

   기술에 대한 다음 입력 템플릿 중 일부 또는 전부가 나열됩니다. 진행 중, 검토 및 종결됨 진행 중 템플릿이 선택됩니다.

   기술이 보안 운영용 Now Assist 작동하는 방식에 익숙해질 때까지 이러한 입력 템플릿을 기본 설정으로 두는 것을 선호할 수 있습니다.

   그러나 일부 기술의 경우 특정 관련 테이블 필드를 수정하고, 보안 인시던트에 대한 프롬프트를 테스트하고, 기술의 가용성을 정의하고, 기술이 표시되는 위치를 선택할 수 있습니다.

   필드를 수정하려면 입력 데이터의 일부로 제공되는 목록에서 지원되는 옵션만 선택합니다.

   기술에 대한 입력 또는 트리거를 수정하는 경우 기술이 사용되는 방법과 시기를 결정합니다. 기술의 입력 데이터 소스는 수정할 수 없습니다. 데이터 소스에는 기술이 사용하는 테이블과 필드가 포함되어 있습니다. 그러나 기술을 복사하고 사용자 지정할 수 있습니다. 자세한 내용은 보안 인시던트 응답용 Now Assist 기술 사용자 지정 문서를 참조하십시오.

6. 저장 및 계속을 선택하여 의 안내 설정다음 단계로 이동합니다.
7. 옵션: 보안 인시던트 기록에서 프롬프트를 테스트합니다.
8. 저장 및 계속을 선택하여 의 안내 설정다음 단계로 이동합니다.
9. 옵션: 다음 옵션 중 하나를 선택하여 가용성을 정의합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

10. 저장 및 계속을 선택하여 의 안내 설정다음 단계로 이동합니다.
11. 표시 선택을 선택하여 기술을 표시할 위치를 결정합니다.
12. 저장 후 계속을 선택하여 다음 단계로 이동합니다.
13. 옵션: 역할을 추가하거나 제거합니다.

    (Optional) 기본적으로 sn_si.analyst 및 sn_si.manager 역할이 추가되며 자동화된 기술 생성의 결과를 볼 수 있습니다. 다음 경우에만 역할을 추가하거나 제거할 수 있습니다 보안 인시던트 응답용 Now Assist 기술 사용자 지정.
14. 선택 항목을 검토하고 활성화를 선택하여 기술 구성을 완료합니다.
15. 보안 인시던트로 돌아가기를 선택합니다.
    기술이 활성 기술 섹션에 표시됩니다.

보안 인시던트 응답용 **Now Assist** 기술 사용자 지정

환경의 요구 사항에 맞게 생성 AI 기술의 일부 입력 필드를 사용자 지정합니다.

시작하기 전에

필요한 역할: admin

프로시저

1. 다음으로 이동합니다. 모두 〉 **Now Assist** 관리자 〉 기능 탭의 탭입니다 Now Assist 관리자 .
2. 탐색 패널에서 기술을 선택한 상태의 목록에서 보안 작업을 선택합니다.
   이러한 보안 인시던트 기술은 다음과 같이 표시됩니다.
   - 보안 인시던트 권장 작업
   - 사후 인시던트 분석
   - 상관 관계 인사이트 생성
   - 보안 인시던트 요약
   - 해결 메모 생성
3. 기술 사본을 생성하고 입력 필드를 사용자 지정합니다.

   a. 보안 인시던트 기능 카드에서 상세 정보 보기를 선택합니다.

   b. 활성 기술 섹션에서 복사할 기술을 찾고 추가 작업 아이콘(.)을 선택합니다.

   c. 사본 만들기를 선택합니다.

   d. 모달에서 선택 사항을 확인합니다.
   안내 설정이 표시됩니다.

   e. 일반 세부 정보에서 기술의 고유한 이름과 설명을 입력합니다.

   f. 저장 및 계속을 선택하여 다음 단계로 진행합니다.

   g. 입력 선택을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

입력 선택을 선택하면 기술에 대한 입력 템플릿이 나열됩니다. 진행 중, 검토 및 종결됨 진행 중 템플릿이 선택됩니다.

템플릿에 대한 일부 기본 입력 테이블 필드, 조건 및 관련 목록을 구성할 수 있습니다. 입력 데이터에 대해 목록에서 지원되는 관련 테이블 중에서만 선택합니다.

기본 입력 테이블 〔sn_si_incident〕을(를) 수정하거나 보안 인시던트 요약 기술 사본에 대한 새 데이터 소스를 추가할 수 없습니다.

h. 조건 작성기와 필터링 조건을 사용하여 진행 중 템플릿의 편집 가능한 필드를 계속 수정합니다.

i. 저장 및 계속을 선택하여 진행 중인 작업 템플릿의 안내 설정 다음 단계로 진행합니다.

- 프롬프트 사용자 지정: 미리 정의된 섹션의 순서를 변경하거나 제거하여 프롬프트를 편집합니다. 각 입력 템플릿 구성에 대한 보안 인시던트 기록에서 프롬프트를 검토하고 테스트할 수 있습니다.
- 가용성 정의:

옵션	설명
기술은 항상 사용 가능	이 기술은 사용자가 항상 사용할 수 있습니다.
기술 가용성 사용자 지정	조건은 충족되는 경우에만 사용할 수 있습니다(기본값). 조건 작성기를 사용하여 조건을 설정합니다.

- 표시 선택:

옵션	설명
제품 내	모든 보안 제품에 보안 인시던트 요약을 표시합니다. Now Assist 기술은 양식과 작업 공간에 표시됩니다.
사용자 역할	확장 아이콘(⌄.)을 선택합니다.
Now Assist 패널	Now Assist 패널에서 기술을 사용할 수 있습니다 Now Assist . **주:** 이 옵션이 표시되지 않으면 Now Assist 패널을 활성화해야 합니다. 자세한 내용은 Turn on the Now Assist panel 문서를 참조하십시오.

j. 템플릿 저장을 선택하여 진행 중인 템플릿에 대한 변경 내용을 저장합니다.

k. 검토 템플릿을 선택합니다.

l. 이전 단계에서 설명한 대로 필터링 조건을 사용하여 검토 및 종결됨 템플릿에서 편집 가능한 필드를 계속 수정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

m. 저장 및 계속을 선택하여 의 안내 설정다음 단계로 진행합니다.

n. 템플릿 저장을 선택하여 템플릿에 대한 변경 내용을 저장합니다.

o. 검토 및 활성화를 선택하여 기술을 검토하고 추가 수정을 수행합니다.

4. 활성화를 선택합니다.
   기술이 보안 인시던트 페이지의 사용 가능한 모든 보안 인시던트 기술 섹션에 표시됩니다.
5. 기술 활성화를 선택합니다.

에 대한 입력 및 트리거 보안 인시던트 응답용 **Now Assist**

생성형 AI 기술에 대한 일부 입력 또는 트리거를 구성할 수 있습니다. 입력 또는 트리거를 사용하면 기술이 사용되는 방법과 시기를 결정할 수 있습니다.

입력 및 트리거

입력은 기술에 사용되는 데이터를 식별합니다. 입력에는 보안 인시던트 요약을 생성하는 데 사용되는 테이블과 필드가 포함됩니다. 트리거는 작업을 시작합니다. 예를 들어 트리거는 시스템이 요약을 생성하는 시기를 결정합니다.

입력과 트리거를 수정할 수 있지만 기술의 데이터 소스는 수정할 수 없습니다. 데이터 소스에는 기술이 사용하는 테이블과 필드가 포함되어 있습니다.

보안 인시던트 요약 기술

보안 인시던트 요약 기술에 대한 입력은 보안 인시던트 요약이 생성될 때 사용되는 테이블과 필드를 식별합니다. 다음 표에는 콘솔의 입력 선택 페이지에 있는 보안 인시던트 요약 기술에 대한 입력이 나열되어 있습니다 Now Assist 관리자 .

입력	설명
데이터 소스	보안 인시던트 〔sn_si_incident〕 테이블.
입력 필드	• 간단한 설명 • 설명 • 상태 • 우선순위 • 작업 메모 • 추가 의견
관련 입력 테이블	• 영향을 받는 CI - 구성 항목 • 영향을 받는 사용자 - 사용자 • 보안 인시던트 응답 작업 - 간단한 설명

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

입력	설명
	• 상태 - 취소됨 이외의 모든 상태입니다. • 연결된 옵저버블 - 옵저버블 찾기가 악성이거나 의심스럽습니다.

해결 메모 생성 기술

해결 메모 생성 기술에 대한 입력은 보안 인시던트에 대한 해결 메모가 생성될 때 사용되는 테이블과 필드를 식별합니다. 다음 표에는 콘솔의 [Choose Input] 페이지에 있는 해결 메모 생성 기술에 대한 입력이 Now Assist 관리자 나열되어 있습니다.

입력	설명
데이터 소스	보안 인시던트 〔sn_si_incident〕 테이블.
입력 필드	• 간단한 설명 • 설명 • 작업 메모 • 추가 의견

보안 인시던트 권장 작업 생성 기술

입력	설명
데이터 소스	보안 인시던트 〔sn_si_incident〕 테이블.

사후 인시던트 분석 생성 기술

입력	설명
데이터 소스	보안 인시던트 〔sn_si_incident〕 테이블.

상관 관계 인사이트 생성 기술

보안 인시던트에 대한 상관 관계 인사이트에는 다음 테이블의 기록이 포함될 수 있지만 이러한 테이블과 기록에 액세스할 수 있는 권한이 있어야 합니다.

입력	설명
데이터 소스	보안 인시던트 [sn_si_incident] 테이블. 구성 항목 [cmdb_ci] 테이블입니다. 인시던트 [incident] 테이블 변경 요청 [change_request] 테이블 문제 [problem] 테이블

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

입력	설명
	취약한 항목 [sn_vul_vulnerable_item] 테이블입니다. 옵저버블 [sn_ti_observable] 테이블을 연결합니다.

보안 인시던트를 종결하는 데 사용 보안 인시던트 응답용 **Now Assist**

보안 분석가는 에서 보안 인시던트 응답용 Now Assist지원하는 생성형 AI 기술을 사용하여 작업 흐름 내에서 보안 인시던트를 신속하게 종결할 수 있습니다.

다음의 개요 보안 인시던트 응답용 **Now Assist**

를 통한 보안 인시던트 응답용 Now Assist생성형 AI 기술을 통해 보안 분석가는 다음을 수행할 수 있습니다.

- 보안 인시던트 상세 정보를 요약하고 간결하고 읽기 쉬운 형식으로 컨텍스트를 신속하게 검토합니다.
- 종결(해결) 메모를 생성합니다.
- 보안 인시던트에 대한 권장 작업 생성
- 사후 인시던트 분석 데이터 생성
- 상관 관계 인사이트를 생성하여 인시던트 조사 속도를 높입니다.

보안 관리자와 분석가는 다음 위치에서 보안 인시던트 요약 및 종결 메모를 요청할 수 있습니다.

- 보안 인시던트 기록
- 보안 인시던트 응답 작업
- Now Assist 패널.

> **주:**
> 보안 인시던트 권장 작업 및 사후 인시던트 분석 기술은 패널에서 사용할 수 Now Assist 없습니다.

보안 관리자와 분석가는 다음 위치에서 권장되는 다음 단계와 사후 인시던트 분석 데이터를 생성할 수 있습니다.

- 보안 인시던트 기록
- 보안 인시던트 응답 작업

보안 관리자와 분석가는 작업 공간의 보안 인시던트에서만 생성된 권장 작업에서 정정 작업을 생성할 수 있습니다 보안 인시던트 응답 .

1. 를 사용하여 보안 인시던트 요약 보안 인시던트 응답용 Now Assist

   근본적인 문제, 인시던트 상세 정보, 관련 목록 데이터(옵저버블) 및 이미 수행된 주요 작업을 포함하는 보안 인시던트에 대한 요약을 생성합니다.

2. 를 사용하여 보안 인시던트에 대한 권장 작업 생성 보안 인시던트 응답용 Now Assist
3. 를 사용하여 보안 인시던트에 대한 사후 인시던트 분석 생성 보안 인시던트 응답용 Now Assist
4. 를 사용하여 패널에서 상관 관계 인사이트 Now Assist 생성 보안 인시던트 응답용 Now Assist

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. 를 사용하여 보안 인시던트에 대한 종결 메모 생성 보안 인시던트 응답용 Now Assist

   보안 인시던트에 대한 종결 메모를 자동으로 생성합니다.

6. 용 패널에서 생성 AI 기술 Now Assist 요청 보안 인시던트 응답용 Now Assist

   패널에서 요약 및 종결 메모를 Now Assist 생성합니다.

   > 주:
   > 보안 인시던트 권장 작업 및 사후 인시던트 분석 기술은 패널에서 사용할 수 Now Assist 없습니다.

7. 보안 인시던트 응답용 Now Assist 기술 사용자 지정

   환경의 요구 사항에 맞게 기술의 입력 필드를 사용자 지정합니다.

를 사용하여 보안 인시던트 요약 보안 인시던트 응답용 **Now Assist**

보안 인시던트 요약 생성 AI 기술로 보안 인시던트의 컨텍스트를 이해합니다.

시작하기 전에
코어 UI(UI16) 및 보안 인시던트 응답 작업 공간에서 보안 인시던트를 Legacy 요약할 수 있습니다. 생성형 AI를 사용하여 인시던트를 요약하려면 입력 데이터에 사용되는 필드에 최소 50개의 단어가 있어야 합니다. 입력 필드에 대한 자세한 내용은 다음 문서를 참조하십시오 에 대한 입력 및 트리거 보안 인시던트 응답용 Now Assist.

필요한 역할: sn_si.analyst, sn_si.manager 또는 sn_si.basic

프로시저

1. Legacy 코어 UI에서 모두 〉 보안 인시던트 〉 인시던트 을 클릭하고 나에게 할당된 보안 인시던트를 엽니다.
2. 또는 다음으로 이동합니다. 모두 〉 보안 인시던트 〉 보안 인시던트 응답 작업 공간 을 클릭하고 나에게 할당된 보안 인시던트를 엽니다.
3. 개요 탭에서 요약을 선택합니다.
   - 생성된 요약은 코어 UI16의 보안 인시던트 기록 Legacy 맨 위에 있는 배너에 표시됩니다.
   - 생성된 요약은 의보안 인시던트 응답 작업 공간개요 탭에 표시됩니다.
4. 옵션: 요약이 생성된 후 다음 옵션 중에서 선택합니다.

   (Optional) AI가 생성한 요약에는 주요 세부 정보가 누락될 수 있습니다. 계속하기 전에 요약의 정확성과 완전성을 검토하는 것이 좋습니다.

를 사용하여 보안 인시던트에 대한 종결 메모 생성 보안 인시던트 응답용 **Now Assist**

보안 인시던트를 종결하면 종결 메모 초안이 자동으로 생성됩니다. 보안 인시던트를 종결하기 전에 초안을 편집하고 검토합니다. 필요에 따라 사용하거나 수정할 수 있습니다. 종결 메모는 다른 분석가, 관리자 및 주요 이해 관계자에게 보안 인시던트 해결에 대한 정보를 제공합니다.

시작하기 전에
필요한 역할: sn_si.analyst, sn_si.manager 또는 sn_si.basic

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

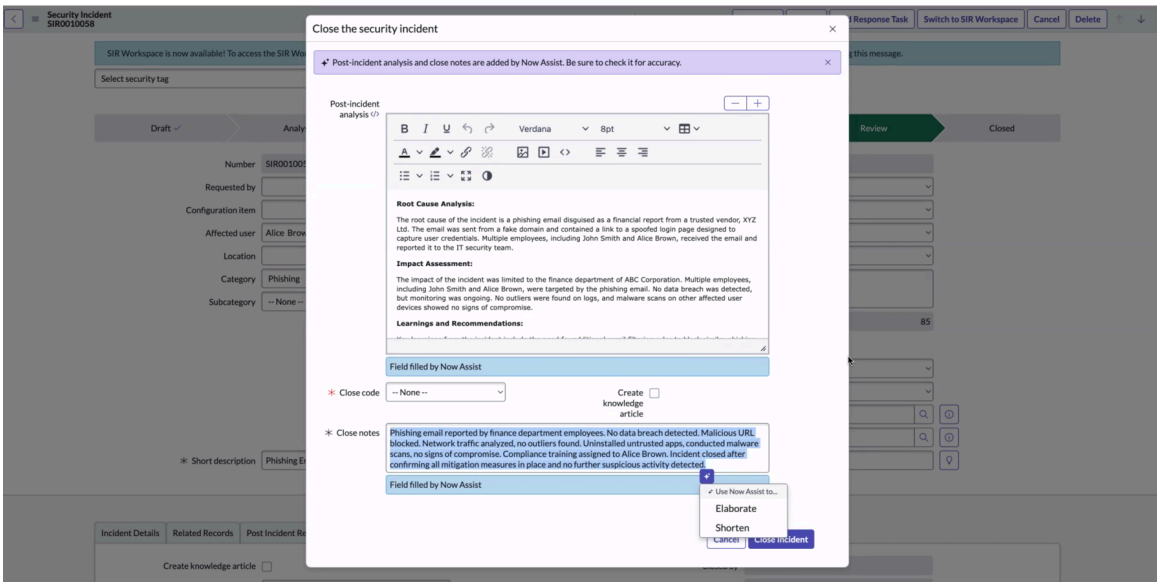
주:

보안 인시던트에 대해 종결 코드 또는 종결 메모 필드가 이미 업데이트된 경우 Now Assist는 인시던트의 현재 상태와 관계없이 이러한 필드를 수정하지 않습니다. Now Assist가 이러한 필드를 업데이트할 수 있도록 하려면 종결 코드 필드와 종결 메모 필드를 모두 비워 두십시오.

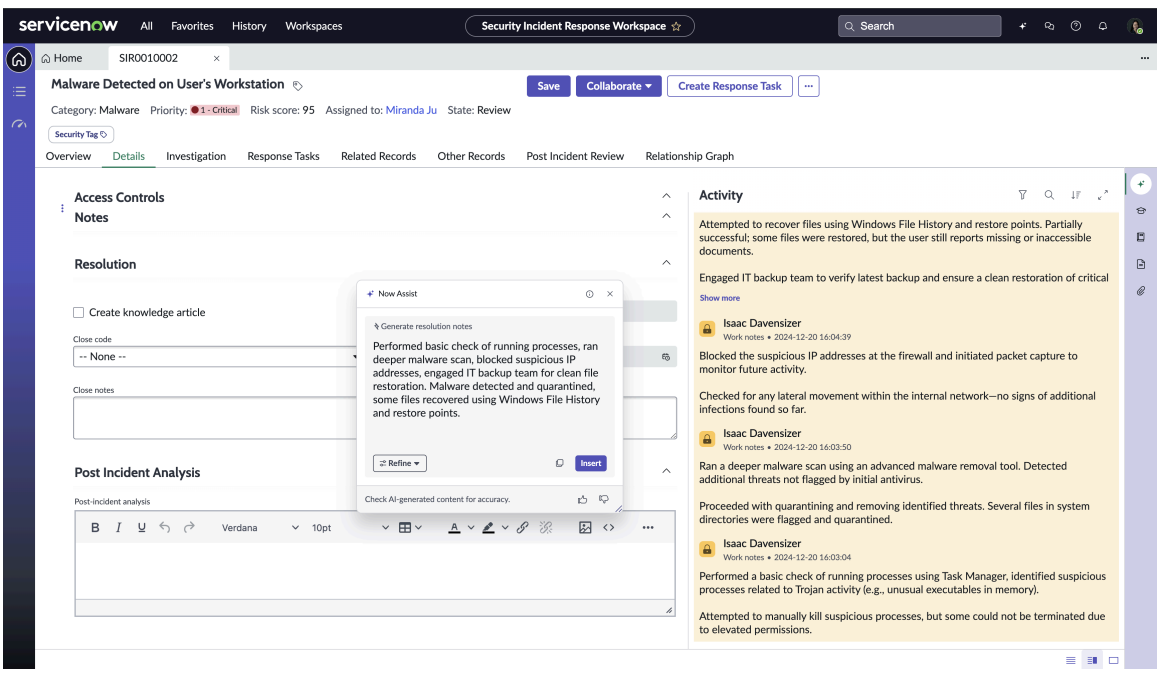
프로시저

1. Legacy 코어 UI에서 모두 〉 보안 인시던트 〉 인시던트 을 클릭하고 나에게 할당된 보안 인시던트를 엽니다.
2. 또는 다음으로 이동합니다. 모두 〉 보안 인시던트 〉 보안 인시던트 응답 작업 공간 을 클릭하고 나에게 할당된 보안 인시던트를 엽니다.
3. 보안 인시던트를 종결합니다.

다음 스크린샷은 코어 UI16에서 보안 인시던트를 종결하기 위해 생성된 해결 메모를 보여줍니다.

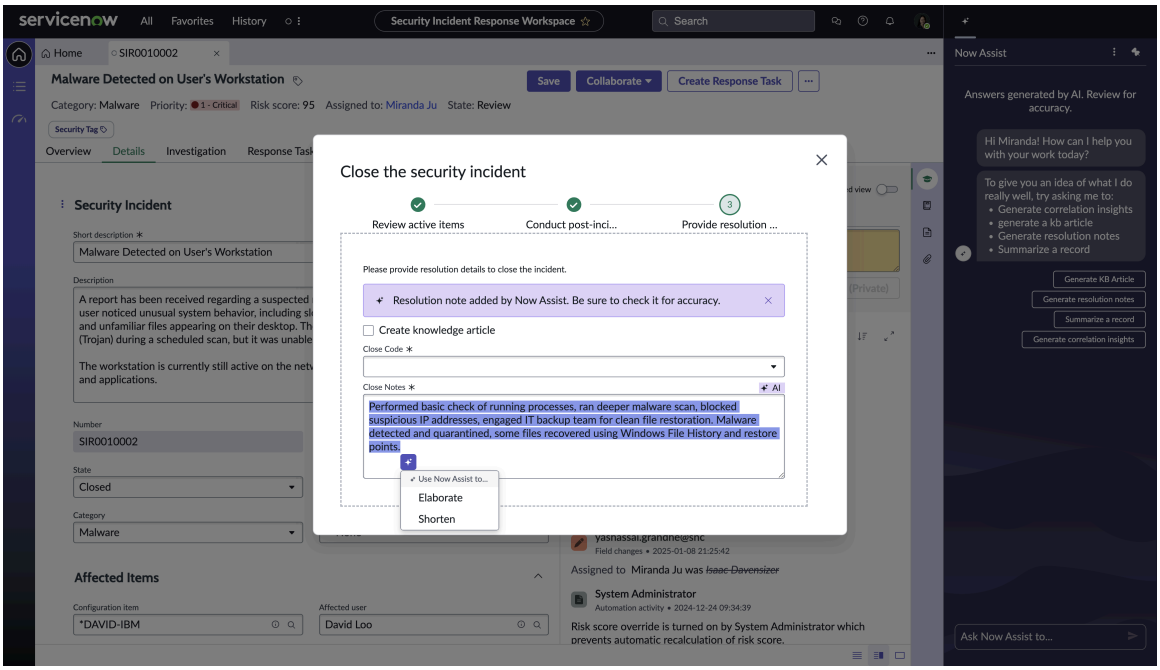


보안 인시던트 응답 작업 공간에서 자동 생성된 해결 메모



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 인시던트 응답 작업 공간에서 Now Assist 상황에 맞는 메뉴를 사용하여 생성된 해결 메모를 편집합니다.



를 사용하여 보안 인시던트에 대한 권장 작업 생성 보안 인시던트 응답용 **Now Assist**

분석가가 보안 인시던트 응답 작업 공간에서 보안 인시던트를 종결하는 데 도움이 될 수 있는 다음 단계를 자동으로 생성합니다. 권장되는 단계는 기존 보안 인시던트 및 지식 문서를 기반으로 합니다.

시작하기 전에

권장되는 다음 단계는 종결 또는 취소됨을 제외한 모든 상태의 활성 보안 인시던트에 적용됩니다.

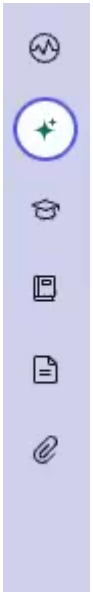
권장 작업 기술이 보안 인시던트에 적용되도록 AI 검색 애플리케이션을 활성화해야 합니다. 인스턴스에서 AI 검색이 활성화되어 있는지 확인하려면 다음으로 이동합니다. 모두 〉 **AI** 검색 〉 **AI** 검색 상태. 페이지에 AI 검색이 활성화되어 있지 않다고 표시되면 지원 센터에 문의하십시오.

필요한 역할: sn_si.analyst, sn_si.manager 또는 sn_si.basic

프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 보안 인시던트 응답 작업 공간 을 클릭하고 나에게 할당된 보안 인시던트를 엽니다.
2. 상황별 사이드바에서 권장 작업 아이콘(✦)을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



3. 권장 사항 가져오기를 선택합니다.
4. AI 생성 컨텐츠 확인 모달에서 확인을 선택합니다.
   생성된 권장 작업은 카드에 표시됩니다. 작업에 대한 최대 4개의 참조가 맨 위에 표시됩니다. 이러한 참조는 지식 문서(KB) 또는 보안 인시던트(SIR#)의 조합일 수 있습니다.
5. 카드에서 하나를 선택합니다.
6. 옵션: 권장 작업 패널에서 새로 고침 아이콘을 선택하여 권장 작업을 다시 생성합니다.

   권장 작업은 1시간 동안 캐시된 상태로 유지됩니다. 다음과 같은 경우 권장 단계를 새로 고치도록 선택할 수 있습니다.

   - 마지막으로 작업을 생성한 이후로 보안 인시던트와 관련된 정보가 변경되었다고 생각합니다.
   - 페이지에서 나갔다가 로그아웃했다가 다시 로그인한 다음 1시간 이내에 보안 인시던트로 돌아갑니다.

   1시간 후에 보려면 3단계부터 작업을 재생성해야 합니다.
7. 카드에서 응답 작업 생성을 선택합니다.
   작업 공간에 새 탭이 열립니다. 간단한 설명과 설명 필드는 선택한 권장 작업 카드의 상세 정보를 사용하여 자동으로 채워집니다.
8. 필요에 따라 양식을 편집하고 저장을 선택하여 응답 작업을 생성합니다.
   시스템 속성의 값을 변경할 때까지 생성한 권장 작업의 두 가지 옵션은 상세 정보 보기 및 응답 작업 생성으로 유지됩니다.
9. 옵션: 권장 작업에서 응답 작업을 생성합니다.
   기본적으로 워크플로우는 카드의 작업 메모에 권장 작업을 저장하는 옵션을 제공합니다. 응답 작업을 작업 메모에 저장하는 대신 작업 카드에서 응답 작업을 생성하는 옵션을 사용하려면 **SecOps** 권장 작업 〔sn_sec_ra.card_action_config〕 시스템 속성의 값 필드를 변경해야 합니다.

   a. 보안 인시던트 관리자 역할 〔sn_si.manager〕을 가진 사용자가 sys_properties로 이동합니다. 목록.

   b. SecOps 권장 작업 〔sn_sec_ra.card_action_config〕 시스템 속성을 찾아 기록을 엽니다.

   c. 값을 share_to_work_notes 에서 create_task로 변경합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

d. 레코드를 저장합니다.

e. 보안 인시던트 기록으로 돌아가서 페이지를 새로 고칩니다.
작업 카드는 상세 정보를 보고응답 작업을 생성하는 옵션을 제공합니다.

를 사용하여 보안 인시던트에 대한 사후 인시던트 분석 생성 보안 인시던트 응답용 Now Assist

근본 원인 분석, 영향 평가, 학습 및 권장 사항 정보를 포함하는 보안 인시던트에 대한 사후 인시던트 분석을 자동으로 생성합니다.

시작하기 전에

에서 자동으로 보안 인시던트 응답용 Now Assist인시던트 사후 분석을 생성하려면 사후 인시던트 분석 기술을 활성화해야 합니다.

보안 인시던트를 종결하기 전에 종결 메모가 이미 수동으로 채워져 있는 경우 분석가가 상태 필드를 종결로 설정할 때 보안 인시던트 응답용 Now Assist 이 내용을 덮어쓰지 않습니다.

필요한 역할: sn_si.analyst, sn_si.manager 또는 sn_si.basic

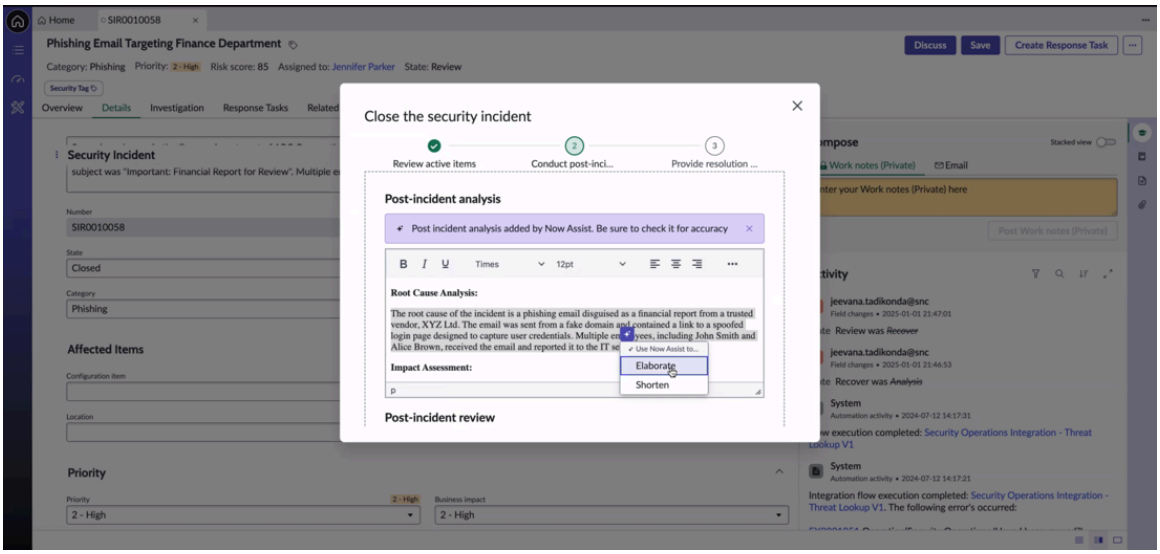
프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 보안 인시던트 응답 작업 공간 을 클릭하고 나에게 할당된 보안 인시던트를 엽니다.
2. 상세 정보 탭의 상태 필드에서 종결됨을 선택하여 보안 인시던트를 종결합니다.
보안 인시던트 종결 모달이 열립니다.
3. 옵션: 이 인시던트와 연결된 활성 정정 작업을 검토하려면 활성 작업 검토 를 선택합니다.
검토할 기록과 함께 새 탭이 열립니다. 이 옵션을 사용하면 연결된 워크플로우 및 활동이 취소되고 연결된 모든 정정 작업에서 인시던트가 종결되므로 보안 인시던트를 종결할 준비가 되었는지 확인할 수 있습니다.
4. 사후 인시던트 분석을 생성하려면 다음을 선택합니다.
사후 인시던트 분석이 세 개의 섹션이 있는 모달에 표시됩니다. 참고로 Now Assist 아이콘( )은 컨텐츠가 에 의해 보안 인시던트 응답용 Now Assist생성되었음을 나타냅니다.
   - 근본 원인 분석
   - 영향 평가
   - 학습 및 권장 사항

   주:
   사후 인시던트 분석 옵션에서 Now Assist 상황에 맞는 메뉴를 사용하여 근본 원인 분석/영향 평가/학습 및 권장 사항을 자세히 설명하거나 축약하고 텍스트를 대체할 수 있습니다. 자세히 보기 는 기존 텍스트에 더 많은 정보를 추가하는 데 도움이 됩니다. 단축 은 선택한 텍스트를 더 간결하게 만듭니다.

   다음 스크린샷은 Now Assist 상황에 맞는 메뉴를 사용하여 원하는 사후 인시던트 분석 텍스트를 자세히 설명하거나 축약하고 대체하는 방법을 보여줍니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



5. 보고서를 검토하여 정확성을 확인하고 필요한 경우 편집합니다.
6. 옵션: 평가 받기 및 보고서 구성/미리 보기를 선택하여 사후 인시던트 검토를 수행합니다.
   평가를 수행하거나 다른 작업을 수행하기 위해 이 페이지에서 나가면 사후 인시던트 검토에 대한 편집 내용이 1시간 동안 보존됩니다. 1시간 후에 인시던트에서 상태를 다시 종결 로 설정하여 사후 인시던트 분석 및 종결 메모를 다시 생성해야 합니다.
7. 다음을 선택하여 해결 메모를 생성합니다.
   해결 메모는 종결 메모 필드에 표시됩니다.
8. 종결 코드에 대한 목록에서 하나를 선택합니다.
9. 인시던트 종결을 선택합니다.
   사후 인시던트 분석은 상세 정보 탭의 사후 인시던트 분석 필드와 보안 인시던트 응답 작업 공간의 보안 인시던트에 대한 개요 탭에 저장됩니다.

를 통한 상관 관계 인사이트 탐색 보안 인시던트 응답용 **Now Assist**

영향을 받는 사용자, 구성 항목 및 옵저버블에 대한 조사 중복을 방지하고 작업 중인 보안 인시던트를 보다 신속하게 해결하는 데 도움이 되는 상관 관계 인사이트를 생성할 수 있습니다. 상관 관계 인사이트의 기반이 될 보안 인시던트에서 기준을 선택합니다.

보안 인시던트 응답 작업 공간에서 상관 관계 인사이트 생성

의 v3.0.0보안 인시던트 응답용 Now Assist부터 상관 관계 인사이트를 보안 인시던트 응답 작업 공간생성 및 보고 .

- 이전에는 인사이트를 기반으로 CI(구성 항목) 또는 영향을 받는 사용자를 선택한 경우 조회에서 보안 인시던트와 연결된 영향을 받는 기본 사용자 또는 기본 CI가 반환되었습니다. v3.0.0부터 에이전트는 관련 목록에서 보안 인시던트를 어떤 CI 또는 영향을 받는 사용자와 상관관계를 지정하겠는지 묻습니다.
- 의 모든 상태의 보안 인시던트에 대한 조사 탭에서 상관 관계 인사이트를 생성할 수 있습니다보안 인시던트 응답 작업 공간.
- 관련된 옵저버블, 구성 항목 및 영향을 받는 사용자에 대해 여러 항목에 대한 인사이트를 동시에 생성할 수 있습니다.
- 결과는 크기 조정 및 이동이 가능한 모덜리스 대화 상자에 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 상관 관계 조회를 위한 시간 범위는 30일입니다.

  주:
  보안 인시던트와 관련된 옵저버블을 생성한 후에는 다른 시간 범위로 다시 생성할 때까지 해당 옵저버블에 대한 인사이트가 저장됩니다. 새 시간 범위에 대한 인사이트가 표시됩니다.

에서 상관 관계 인사이트 생성 옵션을 보안 인시던트 응답 작업 공간보려면 먼저 상관 관계 인사이트 생성 기술을 활성화해야 합니다. 자세한 내용은 에 대한 기술 구성 및 활성화 보안 인시던트 응답용 Now Assist 문서를 참조하십시오.

및 UI의 패널에서 보안 인시던트 응답 작업 공간 상관 관계 인사이트 **Now Assist** 생성 **(UI16)**

패널에 상관 관계 인사이트 생성 옵션을 표시하려면 먼저 상관 관계 인사이트 생성 기술을 활성화해야 합니다 Now Assist .

패널이 Now Assist 표시되지 않으면 활성화해야 합니다. 자세한 내용은 Turn on the Now Assist panel 문서를 참조하십시오.

- 또는 UI(UI16)의 모든 상태에 보안 인시던트 응답 작업 공간 있는 보안 인시던트 기록에서 상관 관계 인사이트를 생성할 수 있습니다 Legacy .
- 기본적으로 상관 관계 인사이트는 지난 30일 간의 일치하는 기록을 검색합니다.
- 의 보안 인시던트 응답 작업 공간상세 정보 탭 또는 UI(UI16)의 구성 항목, 영향을 받는 사용자 및 옵저버블 관련 목록에서 상관 관계 인사이트 필터에 대한 구성 항목, 영향을 받는 사용자 및 옵저버블 값을 찾아 검토할 수 있습니다Legacy.
- 대화를 재설정할 때까지 검색 기준과 결과는 패널에 계속 표시됩니다 Now Assist . 대화를 재설정하려면 패널에서 추가 옵션 아이콘( )을 Now Assist 선택하고 대화 재설정을 선택합니다.
- 생성된 상관 관계 인사이트에서 이러한 기록을 보려면 다음 테이블에 대한 액세스 권한이 있어야 합니다.
  - 구성 항목 [cmdb_ci] 테이블입니다.
  - 인시던트 [incident] 테이블
  - 변경 요청 [change_request] 테이블
  - 문제 [problem] 테이블
  - 취약한 항목 [sn_vul_vulnerable_item] 테이블입니다.
  - 옵저버블 [sn_ti_observable] 테이블을 연결합니다.
- 상관 관계 인사이트에 대한 결과는 액세스할 수 있는 테이블을 기반으로 합니다. 예를 들어 상관 관계 인사이트 결과에서 취약한 항목(VIT)을 보려면 애플리케이션과 읽기 액세스 역할(sn_vul.read_all)이 설치되어 있어야 합니다 취약성 대응 .

상관 관계 인사이트를 생성하는 단계는 다음 문서를 를 사용하여 패널에서 상관 관계 인사이트 Now Assist 생성 보안 인시던트 응답용 Now Assist참조하십시오.

다음을 통해 보안 인시던트 응답 작업 공간 상관 관계 인사이트 생성 보안 인시던트 응답용 **Now Assist**

에서 상관관계 인사이트를 보안 인시던트 응답 작업 공간 생성하고 확인하여 과거 이벤트를 작업 중인 보안 인시던트에 연결할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.analyst, sn_si.manager 또는 sn_si.basic

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 보안 인시던트 응답 작업 공간 을 클릭하고 나에게 할당된 보안 인시던트를 엽니다.
2. 보안 인시던트 기록에서 조사 탭을 선택합니다.
3. 상관 관계 인사이트의 기반이 될 필터를 하나 이상 선택합니다.

   두 개 이상의 옵저버블을 선택할 수 있습니다.

   - 연결된 옵저버블: 지속 가능한 공격 또는 악의적인 인프라의 반복적인 사용을 시사하는 공유 옵저버블로 연결된 기록입니다. IP 주소, URL 또는 파일 해시를 예로 들 수 있습니다.
   - CI(구성 항목): 특정 시스템에서 잠재적인 취약성을 식별하는 데 도움이 되는 동일한 CI가 포함된 레코드입니다. 예를 들어 사용자의 노트북을 들 수 있습니다.
   - 영향을 받는 사용자: 빈번한 피싱 시도 또는 여러 번의 무단 액세스 시도와 같은 패턴을 확인하는 데 도움이 되는 동일한 사용자의 과거 인시던트입니다. 특정 사용자의 이름을 예로 들 수 있습니다.

   일치하는 항목 목록이 표시됩니다.
4. 목록에서 인사이트를 생성할 항목을 선택합니다.
5. 인사이트 생성을 선택합니다.
   대화 상자가 열립니다. 잠시 후 상관 관계 인사이트가 표시됩니다. 이 대화 상자에는 다음과 같은 옵션이 있습니다.

   - 인사이트 새로 고침(- 초기 인사이트가 생성된 후 목록의 항목을 변경하고 결과를 업데이트할 수 있습니다.
   - 확장(- 대화 상자의 크기를 조정하고 페이지에서 끌어옵니다.

   대화 상자의 각 상관관계 인사이트 항목에 대해 다음과 같은 옵션이 있습니다.

   - 시간 범위 변경 - 일치하는 인사이트로 대화 상자를 다시 로드할 시간 범위를 선택합니다. 새 시간 범위를 선택하면 이 항목에 대한 결과가 자동으로 다시 생성됩니다. 각 항목의 시간 범위는 인사이트 옆에 표시됩니다(예: 35.35.35.35). (100#)입니다.
   - 마지막으로 생성된 날짜 - 인사이트가 마지막으로 생성된 날짜입니다.
   - 컨텐츠 평가 - ( ) 및 ( ).
   - 복사 - ( ) 인사이트를 클립보드에 복사합니다.
   - 작업 메모에 공유 - 컨텐츠를 편집하고 보안 인시던트에 대한 작업 메모에 게시합니다.

   상관 관계 인사이트는 기본 조회 기간(30일)을 기준으로 옵저버블을 처음 생성할 때 옵저버블에 저장됩니다. 이러한 통찰력은 다른 조회 기간으로 옵저버블에 대한 통찰력을 다시 생성할 때까지 저장됩니다. 다음 단계에 따라 쿼리에 대한 30일 제한을 수정합니다.

   a. 보안 인시던트 관리자 역할 〔sn_si.manager〕을 가진 사용자가 sys_properties로 이동합니다. 목록.

   b. 상관 관계 조사 기간 [sn_sec_gen_ai.correlation_lookback_period] 시스템 속성을 찾아 기록을 엽니다.

   c. 값 필드에 최대 360의 숫자를 입력합니다.

   d. 레코드를 저장합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

e. 보안 인시던트 기록으로 돌아가서 페이지를 새로 고칩니다.

f. 상관 관계 인사이트를 생성합니다. 결과는 새 조회 기간을 기준으로 합니다.

를 사용하여 패널에서 상관 관계 인사이트 **Now Assist** 생성 보안 인시던트 응답용 **Now Assist**

패널에서 상관 관계 인사이트를 Now Assist 생성하면 과거 이벤트를 작업 중인 보안 인시던트에 연결하는 데 도움이 됩니다.

시작하기 전에
필요한 역할: sn_si.analyst, sn_si.manager 또는 sn_si.basic

프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 보안 인시던트 응답 작업 공간 을 클릭하고 나에게 할당된 보안 인시던트를 엽니다.
2. 또는 UI(UI16)의 Legacy 보안 인시던트 〔sn_si_incident〕 테이블에서 보안 인시던트를 찾아 엽니다.
3. 상단 헤더에서 아이콘( )을 Now Assist 선택하여 패널을 엽니다Now Assist.
4. 상관 관계 인사이트 생성을 선택합니다.

   다음 값 중 하나 이상을 일치시킬 수 있으면 상관 관계 인사이트가 생성됩니다. 인사이트의 기반이 되는 다음 필터가 패널에 표시됩니다 Now Assist . 다른 보안 인시던트와 일치하는 필터만 표시됩니다.

   주:
   보안 인시던트 기록이 열려 있지 않은 경우 상관 관계 인사이트 생성을 선택한 후 보안 인시던트 기록의 번호를 입력하라는 메시지가 표시됩니다.

   - CI(구성 항목): 특정 시스템에서 잠재적인 취약성을 식별하는 데 도움이 되는 동일한 CI가 포함된 레코드입니다. 예를 들어 사용자의 노트북을 들 수 있습니다.
   - 영향을 받는 사용자: 사용자가 동일한 과거 인시던트를 통해 빈번한 피싱 시도 또는 여러 무단 액세스 시도와 같은 패턴을 확인할 수 있습니다. 특정 사용자의 이름을 예로 들 수 있습니다.
   - 옵저버블: 지속 가능한 공격 또는 악의적인 인프라의 반복적인 사용을 시사하는 공유 옵저버블로 연결된 레코드입니다. IP 주소, URL 또는 파일 해시를 예로 들 수 있습니다. 옵저버블에 대한 정확한 값(예: 전체 파일 해시)을 입력해야 합니다.

   이러한 필터에 대해 일치하는 데이터가 없으면 아무 것도 표시되지 않습니다. 작업 중인 보안 인시던트에 이러한 값 중 하나를 추가하고 저장한 다음 패널에서 대화를 재설정하고 다시 시도하라는 메시지가 표시됩니다.

5. 패널에서 추가 옵션 메뉴 아이콘( )을 Now Assist 선택하여 대화를 재설정하고 대화 재설정을 선택합니다.
6. 필터를 선택합니다.

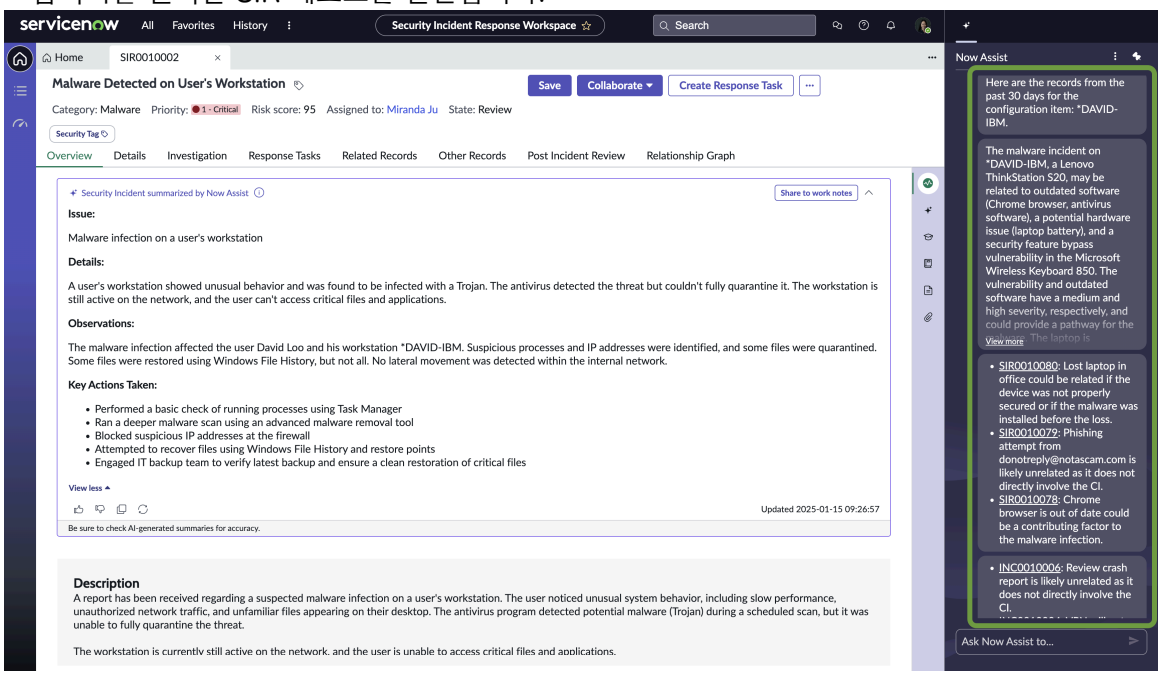
   일치하는 결과가 패널에 표시됩니다 Now Assist .

   다음 예시에서는 구성 항목이 요청되었습니다. 이 검색은 높은 수준의 요약과 일치하는 구성 항목이 있는 기록에 대한 링크를 반환했습니다.

   결과는 보안 인시던트 기록(SIR), 인시던트(INC), 변경 요청(CHG), 문제(PRB) 및 취약한 항목(VIT)과 같은 기록 유형별로 그룹화됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 영향을 받는 사용자 필터는 SIR, INC 및 CHG 레코드를 반환합니다.
- 구성 필터 항목은 SIR, INC, CHG, PRB 및 VIT 레코드를 반환합니다.
- 옵저버블 필터는 SIR 레코드를 반환합니다.



7. 옵션: 다음 단계에 따라 쿼리에 대한 30일 제한을 수정합니다.

a. 보안 인시던트 관리자 역할 〔sn_si.manager〕을 가진 사용자가 sys_properties로 이동합니다. 목록.

b. 상관 관계 조사 기간 〔sn_sec_gen_ai.correlation_lookback_period〕 시스템 속성을 찾아 기록을 엽니다.

c. 값 필드에 최대 360의 숫자를 입력합니다.

d. 레코드를 저장합니다.

e. 보안 인시던트 기록으로 돌아가서 페이지를 새로 고칩니다.

용 패널에서 생성 **AI** 기술 **Now Assist** 요청 보안 인시던트 응답용 **Now Assist**

패널에서 보안 인시던트 요약 또는 종결 메모를 Now Assist 요청합니다.

시작하기 전에

패널을 활성화하는 Now Assist 방법은 을 참조하십시오Now Assist panel .

필요한 역할: si_analyst, si_manager 또는 sn_si.basic

프로시저

1. 보안 인시던트 응답용 Now Assist 애플리케이션이 설치된 인스턴스에 로그인합니다.

2. Legacy 코어 UI에서 모두 〉 보안 인시던트 〉 인시던트 을 클릭하고 나에게 할당된 보안 인시던트를 엽니다.

3. 또는 다음으로 이동합니다. 모두 〉 보안 인시던트 〉 보안 인시던트 응답 작업 공간 을 클릭하고 나에게 할당된 보안 인시던트를 엽니다.

4. 상단 배너에서 Now Assist 아이콘( )을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

에서 AI 에이전트 워크플로우 Now Assist 사용 보안 인시던트 응답

보안 인시던트 응답 AI 에이전트를 사용하여 작업을 자율적으로 완료합니다.

용 AI 에이전트에 사용 가능한 에이전트 워크플로우 보안 인시던트 응답

에이전트 워크플로우 이름	설명	사용 가능한 AI 에이전트
보안 인시던트 종결	이 에이전트 워크플로우는 보안 분석가가 패널에서 자연어를 사용하여 보안 인시던트를 종료하는 데 도움이 됩니다 Now Assist .	보안 인시던트 마무리 생성기
보안 운영 메트릭 분석	이 에이전트 워크플로는 SOC(보안 운영 센터) 관리자가 보안 분석가의 성과를 분석하는 데 도움이 됩니다. 케이스 볼륨, 평균 할당 시간 (MTTA) 및 평균 해결 시간 (MTTR)에 대한 보안 인시던트 응답()SIR 기록에 대한 메트릭이 생성됩니다.	• 보안 인시던트 검색 AI 에이전트 • 보안 메트릭 분석 AI 에이전트
보안 인시던트 해결	이 에이전트 워크플로우는 보안 분석가가 보안 인시던트 해결 경로를 식별하는 데 도움이 됩니다. 또한 이 워크플로우는 보안 분석가가 패널에서 자연어를 사용하여 보안 인시던트를 종료하는 데 도움이 됩니다 Now Assist .	• 보안 인시던트 해결 AI 에이전트 • Exchange Online 통합 처리 AI 에이전트 • 보안 인시던트 마무리 생성기 AI 에이전트 • 옵저버블 분석 AI 에이전트 • 보안 인시던트 활동 처리 AI 에이전트
SIR 교대조 핸드오버 보고서 생성	이 에이전트 워크플로우는 교대조 핸드오버 보고서에 보안 인시던트의 상세 정보를 추가합니다. 에이전트는 보안 인시던트에서 관련 상세 정보를 식별하여 교대조 핸드오버의 여러 섹션을 적절한 컨텐츠로 채웁니다.	보안 인시던트 교대 인수인계 AI 에이전트

중요사항:
기본적으로 모든 에이전트 워크플로우와 AI 에이전트 기록은 읽기 전용입니다.

에이전트 워크플로우를 수정하려면 먼저 Duplicate an agentic workflow 를 수행한 후 다음 단계를 진행해야 합니다.

- 워크플로우를 활성화합니다.
- 워크플로우 내에서 모든 AI 에이전트를 활성화합니다.
- 필요한 경우 워크플로우를 자동으로 호출하는 트리거를 추가할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

AI 에이전트를 찾고 계십니까?

- 애플리케이션과 함께 Now Assist 설치된 AI 에이전트 중에 에이전틱 워크플로우에서 사용되지 않을 수 있습니다. 인스턴스에서 사용할 수 있는 모든 에이전트를 보는 방법에 대한 자세한 내용은 AI 에이전트 찾기를 참조하십시오.
- 인스턴스에 설치되어 있지 않을 수 있는 에이전트를 찾으려면 에서 ServiceNow StoreAI 에이전트 마켓플레이스를 방문하십시오.

보안 인시던트 응답 AI 에이전트 컬렉션 보안 인시던트 종결 에이전트 워크플로우

보안 분석가는 보안 인시던트 종결 에이전트 워크플로우를 사용하여 보안 인시던트를 종결할 수 있습니다.

보안 인시던트 종결 에이전트 워크플로우 개요

보안 인시던트 종결 에이전트 워크플로우를 사용하여 관련 응답 작업을 취소하고, 보안 인시던트 종결 시 해결 메모, 종결 메모, 종결 코드 및 사후 인시던트 분석(PIA)을 생성하고, 패널에서 자연어로 피드백을 제공하고 콘텐츠를 조정할 수 있습니다 Now Assist .

이 에이전트 워크플로우를 수정하려는 경우 이를 복제 하고, 특정 요구에 맞게 설정을 조정하고, 그 대신 에이전트 워크플로우의 복제된 버전을 활성화할 수 있습니다.

보안 인시던트 종결 에이전트 워크플로우에 사용되는 에이전트

보안 인시던트 마무리 생성기 전문가는 보안 인시던트 종결 에이전트 워크플로우에 사용됩니다.

〔store-future: BEGIN review〕

보안 인시던트 종결 에이전트 워크플로우에 매핑된 도구

다음 도구는 보안 인시던트 종결 에이전트 워크플로우에 사용되는 AI 에이전트에 매핑됩니다.

보안 인시던트를 종결하기 위해 매핑된 도구

도구 유형	실행 모드	이름	설명
스크립트	자율적	보안 인시던트 상세 정보 가져오기	보안 인시던트 번호에서 보안 인시던트 상세 정보를 가져오는 도구입니다.
스크립트	자율적	종결 코드 값을 가져옵니다.	보안 인시던트에 사용 가능한 종결 코드 값을 가져오는 도구입니다.
스크립트	자율적	보안 인시던트를 긍정 오류로 종결합니다.	인시던트가 긍정 오류로 종결될 때 사용되는 도구입니다.
스크립트	자율적	보안 인시던트 업데이트	보안 인시던트의 필드를 업데이트하는 도구입니다.
하위 플로우	자율적	종결 메모 작성	보안 인시던트에 대한 종결 메모를 생성하는 도구입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 인시던트를 종결하기 위해 매핑된 도구

도구 유형	실행 모드	이름	설명
하위 플로우	자율적	사후 인시던트 분석을 생성합니다.	보안 인시던트에 대한 사후 인시던트 분석을 생성하는 도구입니다.

〔End〕

〔store-future: BEGIN review〕

보안 인시던트 종결 에이전트 워크플로우에 대한 트리거

이 에이전트 워크플로우에 대한 트리거가 없습니다. 필요한 경우 에이전트 워크플로우를 자동으로 호출하는 트리거를 추가할 수 있습니다.

〔End〕

보안 인시던트 종결

패널에서 AI 에이전트 Now Assist 와 채팅하면 보안 인시던트를 종결하는 데 도움이 됩니다.

시작하기 전에
필요한 역할: sn_si.analyst 또는 sn_si.manager

프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 보안 인시던트 응답 작업 공간.
2. AI 에이전트를 사용하여 종결하려는 보안 인시던트를 엽니다.
3. Now Assist( ) 아이콘을 선택합니다.
   패널이 Now Assist 표시됩니다.
4. 다음 옵션 중 하나를 사용하여 보안 인시던트를 종결합니다.

보안 인시던트 응답 AI 에이전트 수집 보안 인시던트 해결 에이전트 워크플로우

패널에서 AI 에이전트 Now Assist 와 채팅하면 보안 인시던트에 대한 해결 계획을 생성하고 해결하는 데 도움이 됩니다.

보안 인시던트 해결 에이전트 워크플로우 개요

보안 인시던트 해결 에이전트 워크플로우를 사용하여 인시던트 상세 정보를 가져오고, 지식 문서 및 유사한 종결된 보안 인시던트를 가져오고, 해결 계획을 가져오고, 보안 인시던트를 해결합니다.

이 에이전트 워크플로우를 수정하려는 경우 이를 복제 하고, 특정 요구에 맞게 설정을 조정하고, 그 대신 에이전트 워크플로우의 복제된 버전을 활성화할 수 있습니다.

보안 인시던트 해결 에이전트 워크플로우에 사용되는 에이전트

보안 인시던트 해결 에이전트 워크플로우에는 다음과 같은 에이전트가 포함됩니다.

- 보안 인시던트 해결 AI 에이전트
- Exchange Online 통합 처리 AI 에이전트
- 보안 인시던트 마무리 생성기 AI 에이전트

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 옵저버블 분석 AI 에이전트
- 보안 인시던트 활동 처리 AI 에이전트

〔store-future: BEGIN review〕

보안 인시던트 해결 계획 생성기 **AI** 에이전트에 매핑된 도구

모든 도구는 스크립트 유형입니다.

보안 인시던트 해결 계획 생성기 **AI** 에이전트에 매핑된 도구

이름	실행 모드	설명
보안 인시던트 상세 정보 가져오기	자율적	보안 인시던트 번호에서 보안 인시던트 상세 정보를 가져옵니다.
지식 및 유사한 인시던트 가져오기	자율적	검색 쿼리를 통해 관련 지식 문서 및 유사한 종결된 보안 인시던트를 가져옵니다.

〔End〕

〔store-future: BEGIN review〕

보안 인시던트 마무리 생성기 **AI** 에이전트에 매핑된 도구

보안 인시던트 마무리 생성기에 매핑된 도구

도구 유형	실행 모드	이름	설명
스크립트	자율적	보안 인시던트 상세 정보 가져오기	보안 인시던트 번호에서 보안 인시던트 상세 정보를 가져옵니다.
스크립트	자율적	종결 코드 값을 가져옵니다.	보안 인시던트에 사용 가능한 종결 코드 값을 가져오는 도구입니다.
스크립트	자율적	보안 인시던트를 긍정 오류로 종결합니다.	인시던트가 가양성으로 종결될 때 사용되는 도구입니다.
스크립트	자율적	보안 인시던트 업데이트	보안 인시던트의 필드를 업데이트합니다.
하위 플로우	자율적	종결 메모 작성	보안 인시던트에 대한 종결 메모를 생성합니다.
하위 플로우	자율적	사후 인시던트 분석 생성	보안 인시던트에 대한 사후 인시던트 분석을 생성합니다.

〔End〕

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

〔store-future: BEGIN review〕

보안 인시던트 옵저버블 분석기 **AI** 에이전트에 매핑된 도구

모든 도구는 스크립트 유형입니다.

보안 인시던트에 매핑된 도구 옵저버블 분석기 **AI** 에이전트

이름	실행 모드	설명
역량 실행 결과 검색	자율적	위협 조회를 검색하고 옵저버블 보강 결과를 제공합니다.
위협 조회 실행	자율적	옵저버블에 대한 위협 조회를 수행합니다.
옵저버블 보강 실행	자율적	옵저버블과 관련된 추가 컨텍스트를 가져옵니다.
보안 인시던트와 관련된 옵저버블 가져오기	자율적	보안 인시던트와 관련된 옵저버블을 검색합니다.

〔End〕

〔store-future: BEGIN review〕

보안 인시던트 핵심 활동 핸들러에 매핑된 도구 **AI** 에이전트

모든 도구는 스크립트 유형입니다.

보안 인시던트 핵심 활동 핸들러에 매핑된 도구 **AI** 에이전트

이름	실행 모드	설명
인시던트 상태 업데이트	자율적	보안 인시던트의 상태 필드를 업데이트합니다.
이메일 보내기	자율적	이메일을 보냅니다.
관련 기록 생성	자율적	인시던트, 문제, 변경 요청 또는 응답 작업을 만듭니다. 이 도구를 호출하려면 short_description, 설명 security_incident_sys_id 입력 매개변수가 필수입니다.

〔End〕

〔store-future: BEGIN review〕

보안 인시던트 해결 에이전트 워크플로우에 대한 트리거

이 사용 케이스에 대한 트리거가 없습니다. 필요한 경우 사용 사례를 자동으로 호출하는 트리거를 추가할 수 있습니다.

〔End〕

보안 인시던트 해결

패널에서 AI 에이전트 Now Assist 와 채팅하여 인시던트를 해결합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_si.analyst

프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 보안 인시던트 응답 작업 공간.
2. AI 에이전트를 사용하여 해결하려는 보안 인시던트를 엽니다.
3. Now Assist ( ) 아이콘을 선택합니다.
   보안 인시던트 해결 에이전트 워크플로우는 주문형입니다. 이 에이전트 워크플로우를 사용하여 보안 인시던트를 해결하기 위해 자연어로 쿼리를 입력할 수 있습니다.
4. Now Assist 패널에서 에이전트에게 `# #### ##`, `# ## #### ##` 또는 `## #### ##`: SIR0012345를 입력하여 보안 인시던트를 해결하도록 요청합니다.
   이 패널은 Now Assist 보안 인시던트에서 수행할 수 있는 모든 작업을 제공합니다.
5. 보안 인시던트 해결을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Resolution Plan for Security Incident

1. Set the incident to Analysis state.
2. Run Threat Look up and observable enrichment on observables.
3. If the observables are not malicious, close the security incident as a false positive, else proceed with next step.
4. If the observables are malicious, send an email to the management informing them about the phishing attack/campaign has occurred.
5. Check with the affected user if they have interacted with the phishing email.
6. Set the incident to Contain state.
7. If the user has interacted with the phishing email, create an incident to immediately reset the password credentials.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

AI 에이전트는 보안 인시던트를 분석하고 인시던트 및 현재 상태에 대한 요약을 제공합니다. 또한 AI 에이전트는 인시던트 상세 정보, 지식 문서 및 이와 유사한 종결된 보안 인시던트를 사용하여 해결 계획을 제공합니다.

6. 해결 계획에 동의하는 경우 `## ###` 또는 `##` 과 같은 긍정적인 응답을 입력합니다.
긍정적인 응답을 위해 AI 에이전트는 해결 계획의 각 단계를 조사하고 분석가(sn_si.analyst 역할이 있는 사용자)가 이를 해결하도록 지원합니다. 각 단계에서 AI 에이전트는 분석가의 피드백과 개입 요청을 제공합니다. 예를 들어 AI 에이전트가 피싱 이메일에 대해 생성된 인시던트를 식별하면 다음과 같은 에이전트 워크플로우가 발생합니다.

피싱 이메일 인시던트를 해결하기 위한 에이전트 워크플로우

보안 인시던트 해결을 위한 작업	설명
보안 인시던트의 상태 업데이트	AI 에이전트가 보안 인시던트의 상태를 업데이트합니다. 예를 들어 보안 인시던트의 상태가 초안인 경우 AI 에이전트는 이를 분석으로 업데이트합니다.
옵저버블에서 위협 조회 및 옵저버블 보강 실행	AI 에이전트는 위협 조회 및 옵저버블 보강 프로세스를 시작합니다. 분석가가 긍정적인 입력으로 확인하면 AI 에이전트가 옵저버블 분석 및 보강 요약을 제공합니다.
악의적인 옵저버블의 경우 경영진에게 이메일을 전송합니다.	분석가는 AI 에이전트에게 경영진에게 메일을 보내도록 요청할 수 있습니다. AI 에이전트는 이메일 초안을 제공하고 이메일 수신자를 묻습니다. 주: 분석가는 기타 기록 탭에서 보낸 이메일을 확인할 수 있습니다.
영향을 받는 사용자가 피싱 이메일과 상호작용했는지 확인합니다.	분석가는 영향을 받는 사용자가 피싱 이메일과 상호작용했는지 수동으로 확인합니다.
사용자가 피싱 이메일과 상호작용한 경우 암호 자격 증명을 재설정하십시오.	영향을 받는 사용자가 피싱 이메일과 상호작용한 경우 분석가는 AI 에이전트에게 사용자 암호를 재설정하는 인시던트를 생성하도록 요청할 수 있습니다. AI 에이전트는 인시던트에 대한 요약을 제공하고 분석가가 요약을 승인하면 인시던트를 생성합니다.
이메일 게이트웨이에서 보낸 사람/이메일/URL 차단	AI 에이전트는 분석가에게 이메일 게이트웨이의 보낸 사람/이메일/URL 차단을 요청합니다. 분석가는 AI 에이전트에게 이메일 게이트웨이에서 보낸 사람/이메일/URL을 차단하기 위한 응답 작업을 생성하도록 요청할 수 있습니다. AI 에이전트는 응답 작업에 대한 정보를 제공하고 분석가가 승인하면 응답 작업을 생성합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 인시던트 해결을 위한 작업	설명
	주: 분석가는 응답 작업을 완료하고 응답 작업 탭에서 응답 작업을 완료로 표시할 수 있습니다. 분석가는 AI 에이전트에게 응답 작업이 완료되었음을 확인합니다.
모든 사용자 받은 편지함에서 피싱 이메일 검색 및 삭제	AI 에이전트는 분석가에게 모든 사용자 받은 편지함에서 피싱 이메일을 삭제하도록 알립니다. 분석가는 피싱 이메일을 삭제하고 AI 에이전트에게 확인합니다.
영향을 받는 사용자를 필수 피싱 교육에 등록	영향을 받는 사용자가 피싱 이메일과 상호작용한 경우 AI 에이전트는 분석가에게 영향을 받는 사용자를 필수 피싱 교육에 등록하도록 알립니다.
보안 인시던트에 대한 감사 수행	AI 에이전트는 보안 인시던트에 대한 감사를 수행하고 요약을 제공합니다.
보안 인시던트 종결	AI 에이전트가 인시던트를 종결합니다. 자세한 내용은 보안 인시던트 종결 문서를 참조하십시오.

보안 인시던트 응답 보안 운영 메트릭 분석 에이전트 워크플로우를 위한 **AI** 에이전트 컬렉션

보안 운영 메트릭 분석 에이전트 워크플로우는 보안 운영 센터 관리자가 보안 팀의 성과를 분석하는 데 도움이 됩니다.

보안 운영 메트릭 분석 에이전트 워크플로우 개요

보안 운영 센터(SOC) 관리자는 보안 분석가의 성과에 대한 인사이트를 제공하기 위해 보안 인시던트 응답(SIR) 기록의 전체 케이스 볼륨, 평균 할당 시간(MTTA) 및 평균 해결 시간(MTTR)에 대한 메트릭을 분석할 수 있습니다. 또한 메트릭을 개선하는 방법에 대한 권장 사항을 요청할 수도 있습니다.

보안 운영 메트릭 분석 에이전트 워크플로우에 사용되는 에이전트

- 보안 인시던트 검색 AI 에이전트
- 보안 메트릭 분석 AI 에이전트

보안 운영 메트릭 분석 에이전트 워크플로우에 매핑된 도구

다음 도구는 보안 운영 메트릭 분석 에이전트 워크플로우에 사용되는 AI 에이전트에 매핑됩니다.

도구 유형	실행 모드	이름	설명
스크립트	자율적	보안 인시던트 조회	이 도구는 사용자 쿼리에서

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

도구 유형	실행 모드	이름	설명
			올바른 입력으로 스크립트를 호출하여 데이터베이스에서 보안 인시던트를 검색합니다.
스크립트	자율적	분석	SOC 성과에 대해 지정된 메트릭 유형, ###, ##, startDate, endDate에 대한 추가 분석을 제공합니다.
스크립트	자율적	계산	평균 해결 시간(MTTR) 및 평균 할당 시간(MTTA)과 같은 SOC 관리자의 성과 메트릭을 계산합니다.
스크립트	자율적	권장	메트릭 분석을 기반으로 수행할 수 있는 관리 작업을 권장합니다.

보안 운영 메트릭 분석 에이전트 워크플로우에 대한 트리거

이 사용 케이스에 대한 트리거가 없습니다. 필요한 경우 사용 사례를 자동으로 호출하는 트리거를 추가할 수 있습니다.

보안 운영 메트릭 분석 에이전트 워크플로우

패널에서 AI 에이전트 Now Assist 와 채팅하면 보안 분석가가 보안 인시던트 해결을 얼마나 효율적으로 수행하고 있는지에 대한 인사이트를 얻을 수 있습니다.

시작하기 전에

보안 운영 메트릭 분석 에이전트 워크플로우에서 AI 에이전트를 사용하려면 먼저 보안 운영 메트릭 분석 기술을 활성화해야 Now Assist 합니다. 자세한 내용은 에 대한 기술 구성 및 활성화 보안 인시던트 응답용 Now Assist 문서를 참조하십시오.

필요한 역할: sn_si.manager

프로시저

1. 인스턴스의 아무 곳에서나 아이콘( )을 Now Assist 선택합니다.
   패널이 Now Assist 표시됩니다.
2. 패널에서 보안 운영 메트릭Now Assist 분석을 선택합니다.
3. 프롬프트에서 보안 인시던트 메트릭 분석을 선택합니다.

   보안 운영 메트릭 분석 에이전트 워크플로우 케이스는 주문형입니다. 자연어로 쿼리를 입력할 수 있지만 다음 표와 단계에 설명된 프롬프트를 사용하여 사용 가능한 메트릭 데이터와 이 데이터로 수행할 수 있는 작업에 익숙해지는 것을 고려할 수 있습니다.

사용자의 요청 또는 응답	설명
보안 분석가 그룹 및 요청 메트릭 중 하나의 이름을 입력합니다. 예:	이름으로 팀을 지정하고 기간을 지정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용자의 요청 또는 응답	설명
○ **L1** 분석가 팀에 대한 보안 운영 메트릭을 분석합니다. ○ 지난 6개월 동안 **L1** 분석가 팀의 보안 메트릭입니다. ○ 지난달 **L1** 분석가 팀의 성과는 어땠습니까?	
세션을 종료하거나 중지합니다.	대화를 종료합니다.

보안 인시던트 응답 프롬프트에 대한 할당 그룹, 날짜 및 기타 정보를 참조할 수 있도록 작업 공간을 다른 탭에서 여는 것이 좋습니다.

새 채팅을 시작할 때까지 대화가 저장됩니다. 새 채팅을 시작하려면 새 채팅 아이콘(.)을 선택합니다.

요청이 반복되고 자세한 정보와 함께 강조 표시된 텍스트로 표시됩니다.

잠시 후 특정 분석가 또는 분석가 그룹에 대한 추가 정보를 제공하라는 메시지가 표시됩니다.

4. 할당 그룹 이름(예: **L1** 분석가 팀)을 입력합니다.
5. 프롬프트에 시간 범위(예: 지난 6개월)를 입력합니다.
   MTTR(평균 해결 시간), MTTA(평균 할당 시간) 및 팀에서 처리한 총 보안 인시던트 수에 대한 결과가 표시됩니다. 추가 정보를 보려면 링크를 선택하십시오. UI16에서 목록과 함께 새 탭이 열립니다.
6. 소스 목록을 확장하고 보안 인시던트 목록 링크를 선택합니다.
   L1 분석가 그룹에 할당된 보안 인시던트 목록이 UI 16의 새 탭에 표시됩니다. 목록 맨 위에 요청한 날짜 범위(6개월)가 ### > = 2024-09-23 > ### < = 2025-03-23 형식으로 표시됩니다. MTTR, MTTA 또는 케이스 볼륨에 대한 자세한 분석을 보려면 묻는 메시지가 표시됩니다.

   이 목록에서 검토할 개별 보안 인시던트를 여는 링크를 선택할 수 있습니다. 채팅 목록에서 기록 번호를 입력하면 AI 에이전트가 요약할 수 있습니다.
7. 채팅으로 돌아가서 자연어로 성과 메트릭에 대한 요청을 입력합니다(예: #, MTTR# ## ### ####).
   보안 인시던트 필드에 대한 섹션으로 구성된 요약 및 데이터를 포함하는 추가 정보가 요청에 따라 제공됩니다.
   - 범주 분석 - 범주별 세부 항목입니다. 예를 들어 ## ###, #### ## ###, ## ## 등이 포함될 수 있습니다.
   - 우선순위 분석 - 심각도별 세부 항목: 중요, 높음, 보통.
   - 팀 분석 - 팀 개별 구성원별 MTTR 세부 항목입니다.
   - 이상값 분석 - 비정상적으로 높거나 낮거나 기타 고유한 값이 있는 보안 인시던트의 세부 항목입니다.
8. 프롬프트에서 개선 제안 요청에 대한 긍정 응답을 입력합니다.
   제안 사항이 표시됩니다. 평가 결과에 따라 특정 유형의 보안 인시던트에 대한 자세한 정보를 조회할 수 있습니다.
9. 예를 들어 프롬프트에서 분석 상태에 있는 피싱 범주의 모든 보안 인시던트에 대해 자연어로 요청합니다.
10. 결과 보기 링크를 선택합니다.
    요청과 일치하는 보안 인시던트 목록이 UI16의 새 탭에 제공됩니다.

    이 목록에서 개별 인시던트를 열고 AI 에이전트에게 요약을 요청할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

11. 옵션: 메트릭 분석에 사용되는 소스 필드와 이상값 요소의 값에 대한 시스템 속성을 수정합니다.
    - sn_sec_gen_ai.aia_metric_analysis_dimensions - AI 에이전트는 MTTR 및 MTTA 메트릭을 분석할 때 범주, 우선순위, **close_code**, **assigned_toalert_sensor** 필드를 기반으로 분석을 세분화합니다. sn_si.manager 및 sn_si.admin 역할을 가진 사용자는 이 목록을 수정할 수 있습니다.
    - sn_sec_gen_ai.aia_metric_analysis_outlier_factor - 이 속성은 MTTR 및 MTTA에 대한 이상값 요인을 결정합니다. 기본 이상값 2입니다. 기본적으로 MTTR이 할당 그룹이 요청한 시간 범위에 대한 보안 인시던트를 해결하는 데 걸리는 평균 시간의 2배를 초과하는 경우 기록은 이상치입니다. sn_si.manager 및 sn_si.admin 역할을 가진 사용자는 이 값을 수정할 수 있습니다.

SIR 교대조 핸드오버 보고서 생성

패널에서 AI 에이전트 Now Assist 와 채팅하여 SIR 교대조 핸드오버 보고서 생성 에이전트 워크플로우를 사용하면 교대조 핸드오버 보고서에 보안 인시던트의 상세 정보를 추가하는 데 도움이 됩니다.

SIR 교대조 핸드오버 보고서 개요 생성

SIR 교대조 핸드오버 보고서 생성 에이전트 워크플로우를 사용하여 교대조 핸드오버 보고서에 보안 인시던트 상세 정보를 추가합니다. 에이전트는 보안 인시던트에서 관련 상세 정보를 식별하여 교대조 핸드오버의 여러 섹션을 적절한 컨텐츠로 채웁니다.

AI 에이전트는 분석가가 교대조 핸드오버 기록에 액세스할 수 있는지 식별하고 교대조 핸드오버 보고서의 각 섹션에 대한 보안 인시던트 상세 정보에서 컨텐츠를 생성합니다. 분석가는 컨텐츠에 대한 피드백을 제공할 수 있으며, AI 에이전트는 업데이트된 컨텐츠를 생성하고 분석가가 승인할 때 컨텐츠를 교대조 핸드오버 보고서에 저장합니다.

이 에이전트 워크플로우를 수정하려는 경우 이를 복제 하고, 특정 요구에 맞게 설정을 조정하고, 그 대신 에이전트 워크플로우의 복제된 버전을 활성화할 수 있습니다.

SIR 교대조 핸드오버 보고서 생성에 사용되는 에이전트 개요

SIR 교대조 핸드오버 보고서 생성 에이전트 워크플로우에는 다음 에이전트가 포함됩니다. 보안 인시던트 교대조 핸드오버 AI 에이전트.

교대조 핸드오버 보고서에 보안 인시던트 추가

패널에서 AI 에이전트 Now Assist 와 채팅하여 교대조 핸드오버 보고서에 보안 인시던트 상세 정보를 추가합니다.

시작하기 전에
필요한 역할: sn_si.analyst

프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 보안 인시던트 응답 작업 공간.
2. AI 에이전트를 사용하여 교대조 핸드오버 보고서에 추가할 보안 인시던트를 엽니다.
3. Now Assist ( ) 아이콘을 선택합니다.
   SIR 교대조 핸드오버 보고서 생성 에이전트 워크플로우는 주문형입니다. 자연어로 쿼리를 입력하여 교대조 핸드오버 보고서에 보안 인시던트를 추가할 수 있습니다.
4. Now Assist 패널에서 에이전트에게 교대조 핸드오버 보고서에 보안 인시던트를 추가하도록 요청합니다. 교## ##### # ## ##### ######## ##### # ##### #####. SIR0012345하고 Enter 키를 누릅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

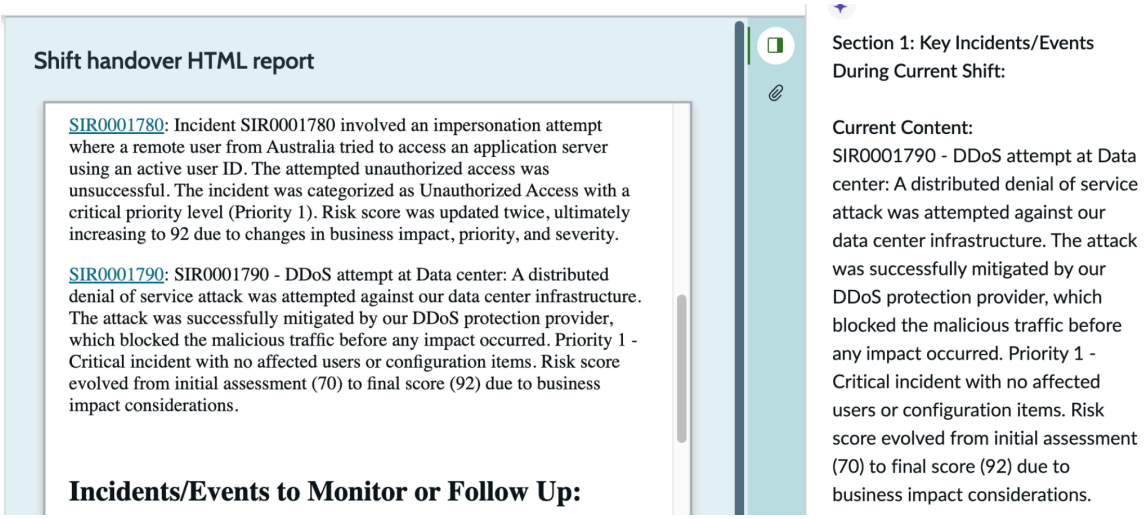
패널은 Now Assist "교대조 인계를 위한 보안 인시던트 추가" 워크플로우를 트리거합니다. 이 워크플로우는 보안 인시던트의 상세 정보를 가져옵니다.

AI 에이전트는 분석가가 액세스할 수 있는 진행 중인 교대조 핸드오버 기록을 찾고 여기에 보안 인시던트 상세 정보를 추가합니다. 분석가가 액세스할 수 있는 진행 중인 교대조 핸드오버 기록이 여러 개 있는 경우 AI 에이전트는 분석가가 선택할 상위 5개 교대조 핸드오버 기록을 나열합니다.

"진행 중" 상태이며 사용자 그룹에 할당된 교대조 핸드오버 기록이 없거나 교대조 핸드오버 기록이 없는 경우, 사용자에 대한 활성 교대조 핸드오버 기록이 없다는 알림 메시지가 표시됩니다.

5. 교대조 핸드오버 기록 번호를 입력하고 Enter 키를 누릅니다.
AI 에이전트는 교대조 핸드오버 기록의 유효성을 검사하여 기록이 유효하고 진행 중인지 식별하며, 로그인한 분석가가 교대조 핸드오버 기록에 액세스할 수 있습니다. 확인에 성공하면 AI 에이전트가 교대조 핸드오버 기록에 대한 콘텐츠를 생성하고 승인을 위해 제공합니다.
6. 콘텐츠에 동의하는 경우 `## ##`, `##`됨 또는 `##` 과 같은 긍정적인 응답을 입력합니다.
AI 에이전트는 승인된 컨텐츠를 교대조 핸드오버 보고서의 관련 섹션에 저장합니다.

교대조 핸드오버 보고서의 각 섹션에 대해 AI 에이전트는 컨텐츠를 제공하고 분석가에게 피드백을 요청합니다. 필요한 경우 모든 섹션을 업데이트하기 위해 건너뛸 수 있습니다.



결과
AI 에이전트는 업데이트되고 건너뛴 모든 섹션의 요약을 표시합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Shift Handover Report Update Complete

Security incident SIR0051335 has been successfully added to shift handover report SHR0001013.

Summary of Processing:

Sections Saved (7 total):

1. ✅ Key Incidents/Events During Current Shift
2. ✅ Incidents/Events to Monitor or Follow Up
3. ✅ System/Infrastructure Updates
4. ✅ Outstanding Action Items
5. ✅ Shift Notes/Comments
6. ✅ Next Steps for Incoming Shift
7. ✅ References

Sections Skipped: None

All sections have been successfully

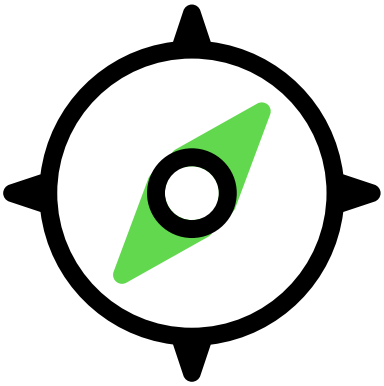
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약성 응답용 **Now Assist**

취약성 응답용 Now Assist 이 애플리케이션을 사용하면 취약성 관리자와 분석가가 중요 취약성에 대한 잠재적 노출을 평가하고 취약한 항목에 대한 서비스 수준 계약(SLA) 준수에 대한 인사이트를 얻을 수 있습니다.

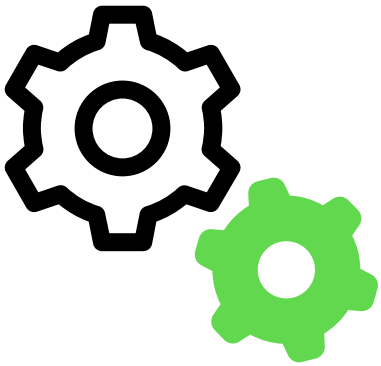
시작하기

탐색



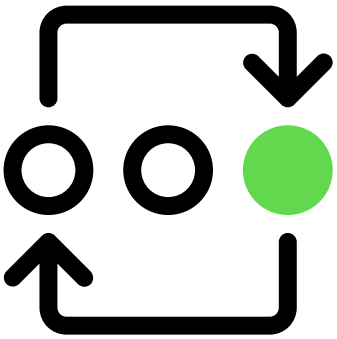
취약성 응답용 Now Assist에 대해 알아보기

구성



에 대한 생성형 AI 기술 및 에이전트 워크플로우를 구성하고 활성화하는 방법 알아보기 취약성 응답용 Now Assist

사용



사용 방법 알아보기 취약성 응답용 Now Assist

AI 에이전트

수집

용 AI 에이전트 및 에이전트 워크플로우에 대한 정보 가져오기 취약성 응답용 Now Assist

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

중요사항:

- 국내 SKU를 보유한 고객은 일부 모델 제공자를 이용할 수 없으며, 일부 Now Assist 제품/기능은 현재 국내 고객에게 제공되지 않습니다. 자세한 내용은 Now Support 지식베이스의 KB1584492 문서를 참조하십시오. 향후 릴리스에서 모델 제공자 가용성 업데이트를 확인하십시오.
- 일부 Now Assist 제품/기능은 현재 FedRAMP, NSC DOD IL5 또는 호주 IRAP 보호 데이터 센터, 자체 호스팅 고객 또는 기타 제한된 환경에서는 사용할 수 없습니다. 자세한 내용은 Now Support 지식베이스의 KB0743854 문서를 참조하십시오. 향후 릴리스에서 가용성 업데이트를 확인하십시오.
- 일부 Now Assist 제품/기능은 현재 일부 지역의 고객에게만 제공됩니다. 향후 릴리스에서 가용성 업데이트를 확인하십시오.

유용한 리소스

유용한 정보를 제공할 수 있는 몇 가지 ServiceNow 리소스는 다음과 같습니다.

- Security Operations 리소스 라이브러리
- Security Operations 커뮤니티
- 알려진 오류 포털에서 알려진 오류 문서 검색
- 연락처 고객 서비스 및 지원

데이터 처리

이 애플리케이션을 사용하려면 ServiceNow 고객의 개별 인스턴스에서 사용자의 인스턴스가 있는 지역과 다른 데이터 센터 지역에 있을 수 있는 중앙 집중식 ServiceNow 환경으로 데이터를 전송해야 하며, Microsoft Azure와 같은 외부 공급업체 클라우드 제공자에게 데이터를 전송해야 합니다. 이 데이터는 당사의 CORE Compliance 포털을 통해 제공되는 당사의 정책을 포함하여 ServiceNow의 내부 정책 및 절차에 따라 처리됩니다.

데이터 수집

ServiceNow는 이 애플리케이션의 입력, 출력 및 출력 편집 내용을 수집하고 사용하여 ServiceNow 모델 및 AI 제품을 포함한 ServiceNow 기술을 개발하고 개선합니다. 또한 이 애플리케이션은 임포트하는 취약성 데이터와 CMDB의 구성 항목에 대한 정보입니다. 고객은 Now Assist옵트아웃 페이지에 설명된 대로 언제든지 향후 데이터 수집을 옵트아웃할 수 있습니다.

자세한 내용은 다음을 참조하십시오. Now Assist 설명서.

취약성 응답용 **Now Assist** 탐색

취약성 관리자와 분석가가 Now Assist 와 함께 취약성 응답용 Now Assist기술 및 AI 에이전트를 사용할 수 있는 방법에 대한 정보를 얻습니다.

취약성 응답용 **Now Assist** 개요

애플리케이션과 함께 취약성 응답용 Now Assist 제공되는 기술을 통해 Now Assist 취약성 관리자와 분석가는 취약성 스캐너에서 임포트된 중복 취약한 항목을 식별, 검토 및 종결할 수 있습니다.

또한 관리자와 분석가는 외부 공급업체 Now Assist 기술에서 임포트한 선호하는 잠재적 솔루션을 제공하는 것을 포함하여 취약한 항목을 해결하는 방법에 대한 명확한 지침을 얻을 수 있습니다.

애플리케이션과 함께 제공되는 AI 에이전트 및 에이전트 워크플로우를 취약성 응답용 Now Assist 사용하면 취약성 관리자와 분석가는 최근에 알려진 취약성에 대한 환경의 잠재적 노출을 확인하고 정정 대상이 서비스 수준 계약(SLA)을 얼마나 잘 준수하는지 확인할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약성 응답용 **Now Assist** 사용자

사용자

사용자	설명
취약성 관리자 및 분석가	환경의 취약성에 대한 노출과 구성 항목(CI) 및 비즈니스 서비스에 대한 잠재적 영향을 확인합니다.
취약성 관리자 및 분석가	SLA(서비스 수준 계약)에 따라 취약성에 대한 정정 목표를 얼마나 잘 달성하고 있는지에 대한 인사이트를 얻습니다.
취약성 관리자 및 분석가	분석가가 감시 주제 및 정정 노력을 통해 할당된 취약한 항목(VIT)을 정정할 수 있는 단계를 제공합니다.
취약성 관리자 및 분석가	잠재적인 기본 솔루션이 포함된 정정 작업을 해결하는 방법에 대한 명확한 정정 지원을 받습니다(사용 가능한 경우).
취약성 관리자 및 분석가	취약성 스캐너에서 임포트한 중복 취약한 항목을 식별하고 검토합니다. 구성 항목과 연결된 기본 취약한 항목을 식별합니다.

취약성 응답용 **Now Assist** 이점

취약성 응답용 **Now Assist** 기능

혜택	기능	사용자
구성 항목에 대한 기본(처음 발견된) 취약한 항목을 식별하고 중복 호스트 취약한 항목(VIT)을 제거합니다.	취약한 항목 중복 제거 기술	취약성 관리자 및 분석가
외부 공급업체 벤더가 제공하는 사용 가능한 잠재적 기본 솔루션을 포함하는 정정 작업을 해결하는 방법에 대한 지침을 얻습니다.	VIT 기술에 대한 기본 솔루션 권장	취약성 관리자 및 분석가
• CVE(Common Vulnerabilities and Exposures)가 있는 자산을 식별합니다. • CVE에 해당하는 활성 취약성 항목(VIT)의 수를 결정합니다. • 알려진 취약성이 있는 비즈니스 서비스를 식별합니다. • 제공된 정보를 기반으로 취약한 항목(VIT) 정정에 대한 감시 주제를 생성합니다. AI 에이전트는 감시 주제와 연결된 활성 VIT에 대한 정정 작업을 생성할 수 있습니다.	취약성 노출 평가 에이전트 워크플로우	취약성 관리자 및 분석가
지난 30일 동안의 서비스 수준 계약(SLA) 준수 요약 진행 상황에 대한 인사이트를 얻습니다. SLA가 누락된 그룹 및 자산 유형을 확인하여 대상을 추적하고 조정하는 데 도움이 됩니다.	취약성 정정 상태 분석 에이전트 워크플로우	취약성 관리자 및 분석가
할당된 취약한 항목에 대한 관련 컨텍스트 및 상세 정보를 검색합니다. 정정 단계를 분석, 계획 및 생성합니다.	문제 해결 단계	취약성 분석가

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음으로 살펴볼 내용

취약성 응답용 Now Assist 구성 및 사용에 대한 자세한 내용은 다음을 참조하십시오.

- 취약성 응답용 Now Assist 구성
- 에서 에이전트 워크플로우 Now Assist 사용 취약성 대응

취약성 응답용 **Now Assist**에 대한 지원 정보

취약성 응답용 Now Assist 애플리케이션과 관련된 중요한 정보의 간략한 개요를 확인합니다.

지원되는 버전 및 필수 애플리케이션

다음 애플리케이션이 필요합니다.

애플리케이션	버전
취약성 응답용 Now Assist	1.0.4
Now Assist 플랫폼용 〔sn_genai_platform〕	9.1.0
취약성 대응 CISA와의 통합 〔sn_vul_cisa〕	1.5.1
취약성 대응 〔sn_vul〕	26.2.1
취약성 대응 라이선싱 및 사용 〔sn_vul_licensing〕 (〔sn_vul〕과 함께 설치됨)	2.7.1
취약성 대응 공통 작업 공간 〔sn_vul_cmn_ws〕 (〔sn_vul〕과 함께 설치됨)	1.7.0
취약성 대응 통합 프레임워크 〔sn_vul_int_fw〕	1.1.2
취약성 솔루션 관리 〔sn_vul_solution〕	10.4.3

지원되는 사용자 인터페이스

취약성 응답용 Now Assist 에는 다음 테이블에 나열된 생성형 AI 기술이 포함됩니다.

취약성 대응용 **Now Assist** 지원 인터페이스

인터페이스	기능
취약성 관리자 작업 공간	Now Assist 기술: • 호스트 취약한 항목(VIT)의 중복 제거. • 외부 공급업체 벤더의 잠재적인 기본 솔루션 제공을 포함하는 정정 지원입니다. AI 에이전트: 취약성 관리자와 분석가는 구성 항목(CI)과 비즈니스 서비스가 취약성에 노출되었는지 평가할 수 있습니다. 악용 가능한 것으로 알려진 새로운 CISA(사이버 보안 및 인프라 보안국)를 확인하고 환경에 대한 잠재적 영향을 평가합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약성 대응용 **Now Assist** 지원 인터페이스

인터페이스	기능
	취약성 관리자와 분석가는 규정 준수 메트릭에 대한 인사이트를 확보하여 조직이 서비스 수준 계약(SLA)을 기반으로 취약성에 대한 정정 목표를 얼마나 효과적으로 충족하고 있는지 파악할 수 있습니다.
UI6	패널의 응답Now Assist 에 있는 링크는 브라우저에서 새 탭을 엽니다.

취약성 응답용 **Now Assist** 구성

취약성 응답용 Now Assist 애플리케이션은 패널에서 지원 Now Assist 되며 요청 시 사용할 수 있습니다.

구성 개요

AI 개발 프로그램과 데이터를 ServiceNow# 공유하면 예측 정확도, 사용자 경험을 개선하고 비즈니스 요구 사항에 맞게 제품을 조정하며 활성화된 Now Assist 기술에 대한 환각을 줄이는 데 도움이 되는 관련 데이터를 제공할 수 있습니다.

참여를 원하지 않는 경우 콘솔의 Now Assist 관리자 데이터 공유에서 인스턴스를 옵트아웃 ServiceNow 하도록 선택할 수 있습니다. 자세한 내용은 Opt out of data sharing for Now Assist 문서를 참조하십시오. 해당 기능을 사용하는 Now Assist 모든 인스턴스에 대해 옵트아웃 프로세스를 반복합니다.

v1.0.4 이전에는 를 AI 에이전트 스튜디오 사용하여 .취약성 응답용 Now Assist

v1.0.4부터 콘솔을 사용하여 Now Assist 관리자 .취약성 응답용 Now Assist 이 콘솔에는 애플리케이션을 설치하고 생성 AI 기술을 구성하는 데 필요한 모든 것이 포함되어 있습니다. 자세한 내용은 Configuring Now Assist Admin features 문서를 참조하십시오.

Now Assist 패널을 활성화해야 합니다. 자세한 내용은 Turn on the Now Assist panel 문서를 참조하십시오.

- Install Now Assist plugins .

  취약성 응답용 Now Assist 애플리케이션을 설치합니다(sn_vul_ai).

- 에 대한 기술 구성 및 활성화 취약성 응답용 Now Assist

  에서 안내 설정기술에 대한 세부 정보를 구성하고 검토합니다. 에서 기술을 활성화할 수 있습니다 안내 설정.

- 에 대한 에이전트 워크플로우 활성화 취약성 응답용 Now Assist

  취약성 응답용 Now Assist 애플리케이션에 포함된 AI 에이전트는 기본적으로 활성화됩니다. 에서 취약성 응답용 Now Assist에이전트 워크플로우 AI 에이전트 스튜디오 를 활성화해야 합니다. 자세한 내용은 에 대한 에이전트 워크플로우 활성화 취약성 응답용 Now Assist 문서를 참조하십시오.

  에서 안내 설정에이전트 워크플로우를 구성하고 활성화합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

에 대한 기술 구성 및 활성화 취약성 응답용 **Now Assist**

에서 안내 설정기술에 대한 세부 정보를 구성하고 검토합니다. 에서 기술을 활성화할 수 있습니다 안내 설정.

시작하기 전에

필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 〉 **Now Assist** 관리자 〉 기술.
2. 탐색 패널에서 기술을 선택한 상태의 목록에서 보안 작업을 선택합니다.
   Now Assist 보안 운영용 기술 페이지가 표시됩니다. 이러한 취약성 응답용 Now Assist 기술은 다음에 대해 취약성 응답용 Now Assist지원됩니다.
   - VIT에 대한 기본 솔루션 권장
   - 취약한 항목 중복 제거
3. 원하는 기술에 대해 기술 활성화 를 선택합니다.
4. 단계에 따라 를 안내 설정사용하여 기술을 구성하고 활성화합니다.

   주:
   일부 기술의 경우 아래 나열된 구성 단계가 모두 필요하지는 않습니다. 왼쪽 패널에 표시되는 작업만 선택하고 프롬프트를 따릅니다. 작업을 완료한 후 기술을 활성화합니다.

5. 일반 상세 페이지에서 저장 및 계속을 선택합니다.
   이 페이지는 읽기 전용입니다.
6. 옵션: 다음 옵션 중 하나를 선택하여 가용성을 정의합니다.

7. 저장 및 계속을 선택합니다.
8. 액세스 권한을 정의합니다.

   주:
   - 취약한 항목 중복 제거 기술의 경우 sn_vul_ai.run_vi_dedup_job 역할이 표시됩니다. 이 역할은 작업 공간에서 중복 제거 작업을 실행하는 데 필요합니다.
   - VIT 기술에 대한 기본 솔루션 권장의 경우 sn_vul_ai.run_suggest_solution 역할이 표시됩니다. 이 역할은 취약한 항목에 대해 권장되는 솔루션 기능을 실행하는 데 필요합니다.
   - 정정 작업에 대해 예약된 작업을 실행하고, 솔루션 작업 권장 [sn_vul_ai_suggest_solution_job] 테이블을 보고, 실행 상태를 보려면 sn_vul_ai.read_suggest_solution_job 역할이 필요합니다.

   이러한 역할을 편집할 수 있지만 이 단계의 기본 설정으로 두는 것을 선호할 수 있습니다.

9. 저장 및 계속을 선택합니다.
10. 기술을 표시할 위치와 작업 공간에서 기술을 볼 수 있는 사용자를 결정합니다.

11. 저장 및 계속을 선택합니다.
12. 선택 항목을 검토하고 활성화를 선택하여 기술 구성을 완료합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

13. 보안 운영으로 돌아가기를 선택하여 보안 운영용 Now Assist 기술 페이지로 돌아갑니다.
이제 을 검토할 취약한 항목 정정에 사용 취약성 응답용 Now Assist준비가 되었습니다.

에 대한 에이전트 워크플로우 활성화 취약성 응답용 **Now Assist**

AI 에이전트 스튜디오에서 에이전트 워크플로우를 활성화해야 합니다. 취약성 응답용 Now Assist 애플리케이션에 포함되어 에이전트 워크플로우에 사용되는 AI 에이전트는 기본적으로 활성화됩니다.

시작하기 전에
Now Assist 패널을 활성화해야 합니다. 자세한 내용은 Turn on the Now Assist panel 문서를 참조하십시오.

필요한 역할: aia-admin

프로시저

1. 다음으로 이동 모두 〉 **AI** 에이전트 스튜디오 〉 개요.
2. 구성하고 활성화할 에이전트 워크플로우에 대한 카드를 선택합니다.
   - 사용 사례 취약성 노출 평가
   - 사용 사례 취약성 정정 상태 분석

   이 에이전트 워크플로우를 수정하려면 이를 복제 하고, 특정 요구에 맞게 설정을 조정하고, 중복을 활성화할 수 있습니다.
   안내 설정이 표시됩니다. 설명 및 연결 페이지는 읽기 전용입니다.
3. 계속을 선택합니다.
4. 트리거 정의에서 계속을 선택합니다.

   트리거 정의 페이지는 읽기 전용입니다.
5. AI 에이전트와의 대화가 패널에 표시 Now Assist 되도록 표시 선택 페이지의 표시 토글을 선택합니다.
6. 화살표 아이콘을 선택하여 섹션을 확장합니다.
   sn_vul.vulnerability_admin 및 sn_vul.vulnerability_analyst 역할이 표시됩니다. 이러한 역할은 애플리케이션의 에이전트 워크플로우에 취약성 응답용 Now Assist 대해 지원됩니다.
7. 에이전트 워크플로우를 활성화하려면 저장 및 테스트를 선택합니다.
   이제 요청 시 에이전트 워크플로우를 호출할 수 있습니다.
8. 옵션: 사용 사례(에이전트 워크플로우)를 선택하고 테스트할 정보를 입력한 다음 테스트 시작을 선택합니다.

취약한 항목 정정에 사용 취약성 응답용 **Now Assist**

취약성 관리자와 분석가는 에서 지원하는 취약성 응답용 Now Assist생성형 AI 기술을 사용하여 작업 플로우 내에서 정정 작업을 해결할 수 있습니다.

취약성 응답용 **Now Assist** 기술 개요

를 통한 취약성 응답용 Now Assist생성형 AI 기술을 사용하면 취약성 관리자와 분석가가 다음을 수행할 수 있습니다.

중복된 취약한 항목을 식별하고 종결합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
중복 제거는 활성 호스트 취약한 항목(VIT)에 대해서만 지원됩니다.

취약한 항목에 대한 권장 선호 취약성 솔루션을 봅니다.

주:

- 기본 설정 및 사용 가능한 취약성 솔루션을 임포트하고 보려면 〔sn_vul_solution〕를 설치하고 활성화해야 취약성 솔루션 관리 합니다. 이 애플리케이션은 예약된 임포트와 함께 현재 솔루션을 제공합니다. 취약성 솔루션 관리 에서 사용할 수 있습니다 ServiceNow# Store.
- 이 생성형 AI 기술은 활성 호스트 취약 항목(VIT)만 지원합니다. VIT는 오픈, 조사 중, 구현 대기 중 또는 검토 중 상태여야 합니다.
- 취약성을 가장 효과적으로 해결하는 현재 솔루션, 대체 가능성이 가장 높은 솔루션이라고도 하는 현재 솔루션은 외부 공급업체 벤더에서 임포트할 수 있어야 합니다. 통합에 대한 취약성 솔루션 관리 자세한 내용과 지원되는 통합에 대한 자세한 내용은 을 참조하십시오취약성 솔루션 관리.
- VIT의 구성 항목 필드는 구성 항목 [cmdb_ci] 테이블의 값으로 채워져야 합니다.
- VIT의 취약성 필드를 채워야 합니다.

- 을 사용하여 중복 취약한 항목 식별 취약성 응답용 Now Assist

  여러 스캐너에서 생성된 중복 취약한 항목(VIT)을 식별하고 그룹화합니다. 기본 취약한 항목을 식별하고 중복을 제거(종결)합니다.

- 를 사용하여 선호하는 취약성 솔루션 제안 취약성 응답용 Now Assist

  지정된 취약한 항목(VIT)에 가장 적합한 기본 솔루션을 식별합니다.

을 사용하여 중복 취약한 항목 식별 취약성 응답용 **Now Assist**

취약성 스캐너에서 임포트한 중복 취약한 항목과 더불어 구성 항목에 대한 기본(처음 발견된) 취약한 항목을 식별하는 작업을 만들거나 실행합니다.

시작하기 전에

이 Now Assist 기술의 요구 사항에 대한 자세한 내용은 을 참조하십시오취약한 항목 정정에 사용 취약성 응답용 Now Assist. 활성화하는 방법에 대한 자세한 내용은 을 참조하십시오 에 대한 기술 구성 및 활성화 취약성 응답용 Now Assist .

필요한 역할:

주:
애플리케이션을 설치할 때 sn_vul.vulnerability_admin 및 sn_vul.vulnerability_analyst는 다음 역할을 상속합니다 취약성 응답용 Now Assist .

- 작업 공간에서 취약한 항목 중복 제거 모듈 보기 - sn_vul_ai.now_assist_user
- 중복 제거 작업 구성 생성 - sn_vul_ai.configure_vi_dedup
- 중복 제거 작업 실행 - sn_vul_ai.run_vi_dedup_job
- 중복 작업 기록 검토 - sn_vul_ai.review_duplicate_vi

프로시저

1. 다음으로 이동 모두 〉 작업 공간 〉 취약성 관리자 작업 공간.
2. 탐색 패널에서 Now Assist ✨ 아이콘을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모든 작업 구성, 모든 작업 및 모든 중복 검토 탭이 Now Assist 페이지에 표시됩니다.
VIT(취약한 항목) 중복 제거를 위한 첫 번째 단계로 중복 제거 작업을 생성해야 합니다.

주:
작업을 생성하려면 sn_vul_ai.configure_vi_dedup 역할이 있어야 합니다.

3. 작업을 생성하려면 새로 만들기를 선택하고 필드를 입력합니다.

필드	설명
직위	다른 작업에서 이 작업을 식별하는 데 도움이 되는 고유한 이름입니다.
이메일 알림	이 작업이 완료될 때 이메일 알림을 받으려면 확인란을 선택합니다. 선택하면 이메일에서 다음 정보를 볼 수 있습니다. ○ 중복 취약한 항목이 발견되었습니다. ○ 처리된 취약 항목 합계 ○ 영향을 받는 구성 항목 ○ 작업 공간에서 중복 목록을 보려면 중복 검토 링크를 선택합니다. 또는 상단 배너에서 알림 표시(종) 아이콘을 선택하여 완료된 작업에 대해 발견된 중복 취약한 항목이 있는 메시지를 볼 수 있습니다.
조건 설정	**a.** 조건 설정 링크를 선택하여 중복을 검토하려는 취약한 항목을 필터링합니다. 예: **[Configuration item] [contains] [server-based-VIs]**. 조건 설정 링크가 새로 고쳐지고 일치하는 결과와 함께 개수가 표시됩니다. 반환된 결과에 따라 작업 이름을 바꾸는 것이 좋습니다. 일치하는 결과 보기 링크를 선택하여 조건을 충족하는 취약한 항목과 조건 모달의 요약, 구성 항목 및 위험 등급과 같은 자세한 내용을 볼 수 있습니다. **b.** 결과가 만족스러우면 저장을 선택합니다.

4. 작업을 저장하면 작업 실행 버튼이 표시되고 기록에 활성화됩니다.

작업을 실행할 준비가 되었습니다.

주:
작업 실행 버튼을 보고 작업을 시작하려면 sn_vul_ai.run_vi_dedup_job 역할이 있어야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 작업을 실행하려면 다음으로 이동합니다. 모두 〉 작업 공간 〉 취약성 관리자 작업 공간 〉 **Now Assist** 〉 모든 작업 구성.

b. 원하는 작업을 찾고 번호 열에서 기록을 선택하여 연 다음 작업 실행을 선택합니다.
작업이 백그라운드에서 실행 중이라는 메시지가 표시됩니다. 작업 상태에 대한 자세한 내용을 보려면 진행 상황 보기 링크를 선택합니다.

작업 실행을 선택하면 취약 항목 중복 제거 작업 완료 확인 작업이 시작되고 백그라운드에서 실행됩니다.

활성 작업이 완료되었는지 확인하기 위해 30분마다 실행되는 다른 작업이 있습니다.

작업이 성공적으로 완료된 후에는 작업에서 찾은 중복 VIT를 검토, 평가 및 종결할 수 있습니다.

주:
중복 VIT를 검토하려면 sn_vul_ai.review_duplicate_vi 역할이 있어야 합니다.

5. 중복 VIT를 검토합니다.

a. 완료된 작업과 중복된 취약한 항목 목록을 검토하려면 다음으로 이동하십시오. 모두 〉 작업 공간 〉 취약성 관리자 작업 공간 〉 **Now Assist** 〉 모든 작업.

b. 기록(**JOB#**)을 열고 중복 취약한 항목 검토 관련 목록을 선택합니다.

c. 옵션: 기록의 VIT가 중복되는지 확인하기 전에 링크를 선택하여 취약한 항목(**VIT#**) 기록을 검토용으로 엽니다.

d. 중복 VIT 기록을 나란히 비교하려면 (**DUP#**) 기록을 선택하여 엽니다.

- 작업 번호와 상태(검토 필요)가 표시됩니다.
- 신뢰도 및 이유 필드는 더 많은 정보를 제공합니다. 이유 열에는 이러한 VIT가 중복으로 간주되는 이유에 대한 생성형 AI 및 Now LLM 서비스 추론이 표시됩니다.
- 취약한 항목 상세 정보 섹션에는 기본 VIT와 중복 VIT에 대한 정보가 나란히 있습니다.
- 기본 및 중복 VIT의 첫 번째 발견 날짜입니다. 기본 VIT는 일반적으로 가장 빠른 첫 발견 날짜를 가집니다.
- 이 페이지에서 VIT 기록을 열려면 기본 취약한 항목 상세 정보에서 ⓘ 아이콘과 중복 필드를 선택합니다.

e. 하나를 선택합니다.

옵션	설명
중복 안 됨 표시	이 두 항목은 두 개 이상의 고유한 취약성을 나타내는 두 가지 고유한 취약한 항목입니다. 이 두 가지 취약한 항목은 앞으로 생성하는 작업에서 중복으로 간주되지 않습니다. **DUP#** 기록에 대해 상태가 검토 필요에서중복 없음으로 전환됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵션	설명
중복 확인	검토 결과 이 두 VIT가 중복된 것으로 나타났습니다. 종결로의 ## 전환이라고 레이블이 지정된 중복 기록에 표시되는 VIT 기록입니다. 종결 메모가 있는 작업 메모가 종결된 VIT 기록에 추가됩니다. 종결된 VIT의 모든 관련 탐지는 기본 VIT 기록으로 이동됩니다. 작업 메모가 기본 VIT에 추가되어 중복이 종결되었고 해당 탐지가 연결되었음을 나타냅니다. **주:** sn_vul_ai.duplicate_vi_confidence_threshold 시스템 속성은 취약한 항목 중복 제거 워크플로우를 자동화합니다. 이 시스템 속성은 기본적으로 활성화되지만 신뢰 점수에 대한 임계치 값은 없습니다. 임계치 값이 없으면 자동화된 워크플로우는 중복을 종결하지 않습니다. **주:** VIT에 대한 신뢰 점수 100은 기술로 계산 Now Assist 되지 않습니다. 이 점수는 결정적 논리와 일치시켜 계산됩니다. 임계치 값을 입력하면 신뢰 점수가 지정한 값보다 큰 중복 항목이 자동으로 종결되고 탐지가 기본 취약한 항목으로 롤업됩니다. 워크플로우에 익숙해지고 정확한 값을 설정할 시간이 있을 때까지 이 시스템 속성을 임계치 값 없이 기본 설정으로 두는 것이 좋습니다. 기본 설정에서는 중복 VIT가 검토, 표시 및 처리되는 조건을 제어할 수 있습니다. 이 시스템 속성을 수정하려면 sn_vul_ai.configure_vi_dedup 또는 sn_vul_ai.review_duplicate_vi 역할이 있어야 합니다.

f. 옵션: 또는 **DUP#** 기록의 모든 중복 검토 목록 탭에서 중복 항목을 검토할 수 있습니다. 이 목록을 사용하면 중복 기록 및 연결된 VIT 기록에 대해 대량 편집을 수행할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

를 사용하여 선호하는 취약성 솔루션 제안 취약성 응답용 **Now Assist**

VR과 함께 취약성 응답용 Now AssistNow Assist 생성형 AI 추론을 사용하여 분석가가 자산의 취약성에 대해 외부 공급업체 공급업체의 잠재적인 기본 솔루션을 찾을 수 있도록 지원합니다.

시작하기 전에

이 Now Assist 기술의 요구 사항에 대한 자세한 내용은 을 참조하십시오취약한 항목 정정에 사용 취약성 응답용 Now Assist. 활성화하는 방법에 대한 자세한 내용은 을 참조하십시오 에 대한 기술 구성 및 활성화 취약성 응답용 Now Assist .

필요한 역할:

> **주:**
> 애플리케이션을 설치할 취약성 응답용 Now Assist 때 sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst, sn_vul.remediation_owner는 다음 역할을 상속합니다.

- sn_vul_ai.run_suggest_solution - 취약한 항목에서 권장 솔루션 기능을 실행하는 데 필요합니다.
- sn_vul_ai.read_suggest_solution_job - 정정 작업에 대해 예약된 작업을 실행하고 솔루션 작업 권장 [sn_vul_ai_suggest_solution_job] 테이블 및 실행 상태를 보는 데 필요합니다.

프로시저

1. 다음으로 이동 모두 〉 작업 공간 〉 취약성 관리자 작업 공간.
2. 호스트 취약한 항목(VIT) 기록을 열고 상세 정보 탭을 선택합니다.
3. VR 추론과 함께 사용하여 Now Assist 취약성에 가장 잘 맞는 솔루션을 찾으려면 솔루션 권장을 선택합니다.
4. 또는 사용자에게 할당된 정정 작업(RT)을 열고 권장 솔루션을 선택합니다.

   다음 테이블에서는 VIT 및 정정 작업 기록에서 솔루션 권장 을 선택한 후 표시되는 메시지와 알림, 데이터가 채워지는 위치에 대해 설명합니다.

   > **주:**
   > Now Assist VR은 취약점 솔루션을 생성하지 않습니다. 솔루션은 외부 공급업체 통합에서 임포트됩니다. VIT 및 정정 작업 기록에 솔루션 권장 버튼이 표시되려면 해당 VIT와 관련된 취약성에 대해 대체 가능성이 가장 높은 솔루션이 하나 이상 있어야 합니다.

취약한 항목**(VIT)** 기록

메시지 또는 알림	설명
Now Assist for VR### # #### #### # ### ## #### #### #####. ### ### ## ## ### ## ### ## #### ######.	기본 솔루션에 대한 정보는 정정 섹션의 기본 솔루션 및 요약 필드에 있는 VIT의 상세 정보 탭에 채워집니다. 작업 메모는 활동 스트림에 입력됩니다. 솔루션의 정확성을 확인하십시오. **주:** VIT에 VR용으로 제공된 Now Assist 솔루션이 있는 경우 더 많은 솔루션을 가져오고 작업을 다시 실행하면 솔루션이 변경될 수 있습니다(솔루션 권장 선택).

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

메시지 또는 알림	설명
## ### ## VR# Now Assist# #### # #### ## #### #####.	VR이 기본 솔루션으로 결정 Now Assist 된 이유에 대한 VIT의 활동 스트림 상세 정보입니다. 추론은 VIT에만 표시됩니다. 기술에서 찾은 기본 솔루션은 정정 작업의 솔루션 탭으로 롤업됩니다. 솔루션의 정확성을 확인하십시오.
#### ## # ####. ### ### ## ## ### ## ### ## #### ######.	솔루션을 찾을 수 없는 이유에 대한 VIT의 상세 정보 탭에 있는 활동 스트림에 요약되어 있습니다. 추론은 VIT에만 표시됩니다.

정정 작업**(RT)** 기록

메시지 또는 알림	설명
VR# Now Assist# #### # ## ### ### ### ## ##### #### #### ## # ### ###. ## ### ## ## VIT# ## ## ### ### # # ####.	○ RT에는 하나 이상의 VIT가 있어야 합니다. RT의 최대 VIT 수의 기본값은 1,000입니다. 이 값을 기본 설정으로 유지하는 것이 좋습니다. 주: sn_vul_ai.max_vits_allowed_for_suggest_solution 시스템 속성을 사용하여 최대값을 수정할 수 있습니다. ○ 정정 작업의 모든 VIT를 검토하지만, 솔루션은 활성 상태이고 대체 가능성이 가장 높으며 아직 솔루션이 없는 정정 작업의 VIT에만 권장됩니다. 주: 정정 작업에 대한 작업을 다시 실행하면 (솔루션 권장 선택) 기본적으로 작업은 솔루션 없이 VIT만 평가합니다(true). 솔루션을 사용하여 VIT를 평가하려면 sn_vul_ai.exclude_vits_with_solution 시스템 속성을 false로 변경해야 합니다. ○ 정정 작업의 상세 정보 탭에 있는 활동 스트림에서 기본 솔루션에 대한 요약을 제공합니다. ○ 기술에서 찾은 기본 솔루션은 정정 작업의 솔루션 탭으로 롤업됩니다. ○ 정정 작업에서 VIT를 일치시키기 위한 솔루션 정보를 롤다운합니다. 솔루션 정보는 기본 설정 솔루션 및 요약 필드와 상세 정보 탭의 활동 스트림에 채워집니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

메시지 또는 알림	설명
	○ 백그라운드 작업이 진행 중이고 해당 기록에 대한 솔루션을 평가하는 경우 정정 작업에 솔루션 권장 버튼이 표시되지 않습니다. 작업이 완료된 후 버튼을 볼 수 있습니다. 솔루션의 정확성을 확인하십시오.
## VIT# ## #### #### ####. #### ##### # ### #####.	작업 상태 및 다음 정보가 포함된 요약을 참조하십시오. ○ 정정 작업의 총 VIT 수: n ○ 처리된 VIT 수: n ○ 솔루션이 있는 VIT: n VIT 솔루션을 자신 있게 제안할 수 있는 정보가 충분하지 않으면 VIT에 대한 솔루션이 제공되지 않습니다. 요약은 작업이 완료된 후 활동 스트림에도 제공됩니다.
## ## #### ### # ## ### #### ### VIT# ## #### #### ####.	특정 VIT에 대한 솔루션을 찾을 수 없습니다. 이는 솔루션을 결정하는 데 충분한 정보가 없거나 대체 가능성이 가장 높은 솔루션이 제공되지 Now Assist 않았기 때문입니다. ○ VIT에서 기본 솔루션 및 요약 필드는 비어 있습니다. ○ 작업 메모는 VIT 및 정정 작업의 활동 스트림에 입력됩니다. ○ 추론은 VIT에만 표시됩니다.

에서 에이전트 워크플로우 **Now Assist** 사용 취약성 대응

취약성 대응 AI 에이전트를 사용하여 작업을 자율적으로 완료합니다.

용 **AI** 에이전트에 사용 가능한 에이전트 워크플로우 취약성 대응

에이전트 워크플로우 이름	설명	사용 가능한 **AI** 에이전트
취약성 노출 평가	• 구성 항목(CI) 및 비즈니스 서비스가 알려진 취약성에 노출되었는지 확인합니다. • 특정 취약성이 사용자 환경 전체에 미칠 수 있는 잠재적 영향을 확인합니다. • 새로운 CISA(사이버 보안 및 인프라 보안국)에서 악용	• CISA 취약성 분석 AI 에이전트 • 취약성 노출 분석 AI 에이전트 • 감시 주제 생성 AI 에이전트

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

용 **AI** 에이전트에 사용 가능한 에이전트 워크플로우 취약성 대응

에이전트 워크플로우 이름	설명	사용 가능한 **AI** 에이전트
	가능한(제로 데이) 취약성이 있는지 CI를 확인합니다. • 취약성 관리자 작업 공간에서 감시 주제를 생성하여 취약한 항목을 정정합니다.	
취약성 개선 상태 분석	• 규정 준수 메트릭 및 통계에 대한 인사이트를 확보하여 취약한 항목(VIT) 기록의 정정 목표 날짜를 얼마나 잘 충족하고 있는지 확인합니다. • 월별 VIT 기록 정정 합계를 보고 누락된 대상을 식별합니다. • 월간 서비스 수준 계약(SLA) 준수 검토를 위해 **VIT**에 대한 정정 데이터를 심각도, 할당 그룹, 구성 항목 및 취약성 별로 분류합니다.	정정 준수 분석 AI 에이전트

중요사항:
기본적으로 모든 에이전트 워크플로우와 AI 에이전트 기록은 읽기 전용입니다.

에이전트 워크플로우를 수정하려면 먼저 Duplicate an agentic workflow 를 수행한 후 다음 단계를 진행해야 합니다.

- 에이전트 워크플로우를 활성화합니다. 취약성 응답용 Now Assist 애플리케이션에 포함된 AI 에이전트는 기본적으로 활성화됩니다.
- 필요한 경우 에이전트 워크플로우를 자동으로 호출하는 트리거를 추가할 수 있습니다.

AI 에이전트를 찾고 계십니까?

- 애플리케이션과 함께 Now Assist 설치된 AI 에이전트 중에 에이전틱 워크플로우에서 사용되지 않을 수 있습니다. 인스턴스에서 사용할 수 있는 모든 에이전트를 보는 방법에 대한 자세한 내용은 AI 에이전트 찾기를 참조하십시오.
- 인스턴스에 설치되어 있지 않을 수 있는 에이전트를 찾으려면 에서 ServiceNow StoreAI 에이전트 마켓플레이스를 방문하십시오.

- 취약성 노출 평가 에이전트 워크플로우.

  패널에서 AI 에이전트 Now Assist 와 채팅하면 구성 항목과 비즈니스 서비스가 취약성에 노출되었는지 평가하는 데 도움이 됩니다.

- 취약성 정정 상태 분석 에이전트 워크플로우.

  패널에서 AI 에이전트 Now Assist 와 채팅하면 취약한 항목을 해결하기 위한 규정 준수 메트릭에 대한 인사이트를 얻는 데 도움이 됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약성 노출 평가 에이전트 워크플로우

패널에서 AI 에이전트 Now Assist 와 채팅하면 구성 항목과 비즈니스 서비스가 취약성에 노출될 가능성을 평가하는 데 도움이 됩니다.

시작하기 전에
Now Assist 패널을 활성화해야 합니다. 자세한 내용은 Turn on the Now Assist panel 문서를 참조하십시오.

필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.vulnerability_analyst

프로시저

1. 인스턴스의 아무 곳에서나 아이콘( )을 Now Assist 선택합니다.
   패널이 Now Assist 표시됩니다.

   취약성 노출 평가 에이전트 워크플로우는 주문형입니다. 자연어로 쿼리를 입력할 수 있지만 다음 표와 시작 단계에 설명된 프롬프트를 사용하여 사용 가능한 취약성 데이터와 이 데이터로 수행할 수 있는 작업에 익숙해지는 것을 고려할 수 있습니다. 다음 단계에서는 현재 취약성 데이터를 요청하고, 반환된 결과에 따라 주시 주제를 만들고, 취약성이 사용자 환경에 미칠 수 있는 전반적인 영향을 확인하는 방법을 보여줍니다.

사용자의 요청 또는 응답	설명
최근 **CISA** 취약점은 무엇입니까?	최근 질문은 지난 7일 동안 드러난 새로운 취약점을 나타냅니다. 에이전트 워크플로우의 기본 기간은 7일(1주일)입니다. 7일이 아닌 특정 기간에 대한 새로운 취약성을 검색하려면 지난 30일 동안의 최근 취약성은 무엇입니까?
예, 취약성 CVE-2018-9065에 대한 주시 주제를 생성합니다.	주시 주제를 만들고 싶은지 물으면 구체적으로 응답하는 것이 더 나을 수 있습니다. 예를 들어 요청을 확인하고 **CVE-2018-9065** 형식의 특정 취약성을 입력합니다.
CVE-2018-9065 취약성에 대한 자세한 영향 분석을 제공해 주시겠습니까?	취약성의 잠재적 영향 분석은 영향을 받는 비즈니스 서비스 및 구성 항목 클래스에 대해서만 지원됩니다.
이전 질문의 출력을 표시합니다.	답변을 제공하지 않으면 에이전트에게 이전 질문을 검토하도록 요청하십시오.
세션을 종료하거나 중지합니다.	대화를 종료합니다.

   새 채팅을 시작할 때까지 대화가 저장됩니다. 대화가 예기치 않게 종료되면 새 채팅을 시작합니다. 새 채팅을 시작하려면 새 채팅 아이콘(.)을 선택합니다.

2. 최근 취약성에 노출되었는지 확인하기 위해 자연어로 요청을 입력합니다(예: 최근 **CISA** 취약성은 무엇입니까?

   항목에 범위가 지정되어 있지 않기 때문에 에이전트는 기본적으로 자산에 대한 CISA(사이버 보안 및 인프라 보안국)의 악용 가능한 취약성 데이터를 수집하고 지난 7일 동안의 정보를 반환합니다.

   자산에 영향을 미치고 사용자 환경에서 취약한 항목이 연결된 CVE(Common Vulnerabilities and Exposures) 취약성이 나열됩니다.

   에이전트가 CVE와 일치하는 별칭도 반환하는 것을 확인할 수 있습니다. 외부 공급업체 스캐너를 사용하여 취약성 데이터를 임포트하는 경우 별칭이 보고됩니다. 예를 들어 #### ###

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

CVE-2018-8627(##: TEN-119686, TEN-119596)## 4## ### ##(VIT)# ####. 이 응답은 취약성이 Tenable(TEN) 스캐너 제품에서 검색되어 임포트되었음을 나타냅니다.

3. 옵션: 반환된 모든 CVE에 대한 자세한 내용을 보려면 CISA 알려진 악용 가능한 취약성 링크를 선택합니다.
   UI16의 새 탭에서 목록이 열립니다.
4. 채팅으로 돌아가서 프롬프트에서 에이전트에게 CVE에 대한 감시 주제를 생성하도록 요청을 입력합니다(예: 예, 취약성 CVE-2018-9065에 대한 감시 주제를 생성합니다).
   에이전트가 주시 주제의 이름을 제안하고 확인을 요청합니다. 이름을 변경할 수 있습니다.
5. 확인을 입력합니다.
6. 링크를 선택하여 취약성 관리자 작업 공간에서 감시 주제를 보고 자세한 내용과 CVE와 관련된 취약한 항목을 봅니다.
   UI16의 새 탭에서 목록이 열립니다. 데이터를 검토한 후 CVE가 다른 자산에 미치는 영향에 대해 더 많은 정보가 필요하기로 결정할 수 있습니다.
7. 패널로 Now Assist 돌아가서 자세한 영향 분석을 입력하고 에이전트에게 요청합니다(예: **CVE-2018-9065** 취약성에 대한 자세한 영향 분석을 제공해 주시겠습니까?).
   이 요청은 이 CVE의 영향을 받는 구성 항목 및 비즈니스 서비스에 대한 정보를 반환합니다. 중요도 세부 항목, 영향을 받는 비즈니스 서비스 목록, 영향을 받는 구성 항목의 클래스 목록이 제공됩니다. 자세한 내용을 볼 수 있는 링크도 있습니다.
8. 옵션: 특정 비즈니스 서비스에 대한 전반적인 취약성 노출 평가를 요청합니다.
   비즈니스 서비스에 대한 정보에는 연관된 취약한 항목이 포함되며, 심각도(위험) 및 클래스별 구성 항목이 나열됩니다.

취약성 정정 상태 분석 에이전트 워크플로우

패널에서 AI 에이전트 Now Assist 와 채팅하면 취약한 항목에 대한 월별 정정 준수 메트릭에 대한 인사이트를 얻는 데 도움이 됩니다.

시작하기 전에

Now Assist 패널을 활성화해야 합니다. 자세한 내용은 Turn on the Now Assist panel 문서를 참조하십시오.

필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.vulnerability_analyst admin

프로시저

1. 아이콘( )을 Now Assist 선택합니다.
   패널이 Now Assist 표시됩니다.

   취약성 정정 상태 분석 에이전트 워크플로우는 주문형입니다. 자연어로 쿼리를 입력할 수 있지만 다음 표와 단계에 설명된 프롬프트를 사용하여 사용 가능한 데이터와 데이터로 수행할 수 있는 작업을 숙지하는 것이 좋습니다.

   이러한 단계는 팀이 서비스 수준 계약(SLA)에 보고된 취약한 항목 기록에 대한 월별 정정 목표 날짜를 얼마나 잘 충족하는지에 대한 규정 준수 메트릭에 대한 인사이트를 제공합니다.

사용자의 요청 또는 응답	설명
2024년 10월 한 달 동안 정정에 대한 나의 준수 사항은 무엇입니까?	기본적으로 조회는 할당 그룹을 기반으로 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용자의 요청 또는 응답	설명
	월을 지정하지 않으면 AI 에이전트는 현재 월을 찾은 다음 한 번에 한 달씩 시간을 거슬러 올라가기 시작합니다. 또는 에이전트에게 구성 항목 클래스 또는 취약성별 세부 항목을 요청할 수 있습니다. 예를 들어 **Windows** 서버에 대한 2024년 10월의 내 규정 준수는 무엇인가요?를 입력합니다.
누락된 SLA가 가장 많이 발생한 자산 유형은 무엇입니까?	결과는 자산 유형별로 원래 요청한 월의 데이터를 기반으로 구성됩니다.
누락된 중요 SLA가 가장 적은 할당 그룹은 무엇입니까?	취약한 항목(VIT) 심각도인 ##, ##, ## 및 ##에 따라 누락된 SLA가 가장 많거나 가장 적은 할당 그룹을 가져옵니다. 또한 AI 에이전트에게 VIT 범주별로 누락된 SLA를 조회하도록 요청할 수 있습니다.
이전 질문의 출력을 표시합니다.	답변을 제공하지 않으면 에이전트에게 이전 질문을 검토하도록 요청하십시오.
세션을 종료하거나 중지합니다.	대화를 종료합니다.

새 채팅을 시작할 때까지 대화가 저장됩니다. 대화가 예기치 않게 종료되면 새 채팅을 시작합니다.

새 채팅을 시작하려면 새 채팅 아이콘(+)을 선택합니다.

2. 지정된 월 및 연도에 대한 정정 메트릭을 보려면 자연어로 요청을 입력합니다(예: 2024# 10# # # ## ### ## # ## ### #####?).

   결과는 섹션으로 구성됩니다.

   - 요약 - 요청한 월 및 연도의 SLA 정정 목표가 포함된 총 기록과 목표 날짜를 놓치거나 충족한 백분율 합계입니다.
   - 심각도별 세부 항목 - 정정 대상을 놓친 취약한 항목은 중요, 높음, 중간 및 낮음 심각도로 세분화됩니다.
   - 할당 그룹별 세부 항목 - 할당 그룹별로 세분화된 대상이 누락된 총 기록의 백분율입니다.
   - 추가 정보: 2024년 10월 정정 준수 링크 - 데이터에 대한 자세한 정보를 봅니다. UI16에 새 탭이 열립니다.

3. 누락된 SLA에 대한 보다 구체적인 정보를 요청할 수 있습니다(예: ## ## ### ## ## ### SLA# ######?).
   결과는 자산 유형(예: Windows Server, 데이터베이스, Linux Server 등)별로 원래 요청한 월의 데이터에 대해 구성됩니다.

4. 해당 월 동안 팀의 생산성에 대한 보다 구체적인 정보를 요청할 수 있습니다(예: ### ## SLA# ## ## ## ### #####?
   SLA를 놓친 ## VIT 수가 가장 적은 할당 그룹이 반환됩니다.

5. 이러한 결과를 다른 달과 비교할 수 있습니다(예: # #### 2024# 11## ### #####?).
   결과는 섹션으로 구성됩니다.

   - 비교 요약 - 최근 요청(2024년 11월)과 비교하여 처음 요청한 기간(2024년 10월) 동안 SLA 정정 대상이 있었던 총 기록입니다.
   - 심각도별 세부 항목 - 정정 대상을 놓친 취약한 항목은 ##, ##, ## 및 ##의 심각도별로 분류됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 관찰 - 데이터를 분석하고 비교를 기반으로 데이터 추세를 파악합니다.
- 추가 정보: 2024년 11월 정정 준수 링크 - 비교에 사용되는 데이터에 대한 자세한 정보를 봅니다. UI16에 새 탭이 열립니다.

취약성 응답용 **Now Assist** 참조 정보

에 대한 취약성 응답용 Now Assist도구, 에이전트 및 AI 에이전트 수집 정보입니다.

참조

다음 에이전트 워크플로우에 대한 개요를 봅니다.

- 취약성 대응 취약성 노출 평가 에이전트 워크플로우를 위한 AI 에이전트 컬렉션
- 취약성 대응 취약성 정정 상태 분석 에이전트 워크플로우를 위한 AI 에이전트 컬렉션

취약성 대응 취약성 노출 평가 에이전트 워크플로우를 위한 **AI** 에이전트 컬렉션

취약성 노출 평가 에이전트 워크플로우를 위한 도구 및 AI 에이전트입니다.

에이전트 워크플로우 개요

취약성 대응용 Now Assist 애플리케이션에는 다음 에이전트 워크플로우가 포함되어 있습니다.

- 취약성 노출 평가 에이전트 워크플로우
- 취약성 정정 상태 워크플로우 분석

이 에이전트 워크플로우를 수정하려는 경우 이를 복제 하고, 특정 요구에 맞게 설정을 조정하고, 에이전트 워크플로우의 복제된 버전을 활성화할 수 있습니다.

취약성 노출 평가 에이전트 워크플로우 에이전트 워크플로우 개요

패널의 취약성 노출 평가 에이전트 워크플로우 Now Assist 를 사용하면 다음을 수행할 수 있습니다.

- 구성 항목(CI) 및 비즈니스 서비스가 알려진 취약성에 노출되었는지 확인합니다.
- 특정 취약성이 환경 전체에 미칠 수 있는 잠재적 영향을 확인합니다.
- 새로운 CISA(사이버 보안 및 인프라 보안국)에서 악용 가능한(제로 데이) 취약성이 있는지 CI를 확인합니다.
- 취약성 관리자 작업 공간에서 감시 주제를 생성하여 취약한 항목을 정정합니다.
- 자연어로 콘텐츠를 조정합니다.

취약성 노출 평가 에이전트 워크플로우에 사용되는 에이전트

- 취약성 대응 작업 실행자
- CISA 알려진 악용 취약성 분석기
- 취약성 노출 평가 자문가

〔store-future: BEGIN review〕

취약성 대응: 영향 및 노출 평가 에이전트 워크플로우에 매핑된 도구

다음 도구는 취약성 대응: 영향 및 노출 평가 에이전트 워크플로우에 사용되는 AI 에이전트에 매핑됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약성 대응: 영향 및 노출 평가 에이전트 워크플로우에 매핑된 도구

도구 유형	실행 모드	이름	설명
스크립트	자율적	취약성에 대한 자세한 정보 가져오기	CISA용 도구 악용된 것으로 알려진 취약성 분석기 에이전트는 ID 취약성 ID를 사용하여 취약성에 대한 추가 정보를 가져옵니다.
스크립트	자율적	최근 CISA KEV 확인	CISA 알려진 악용된 취약성 분석기 도구인 에이전트는 입력한 일수에 따라 최근 CISA 취약성 및 KEV(알려진 악용된 취약성) 카탈로그를 검사합니다.
스크립트	자율적	비즈니스 서비스 취약성 요약	취약성 노출 평가 자문가용 도구 에이전트는 영향을 받는 CI(구성 항목)와 해당 취약성을 식별합니다. 또한 활성 취약한 항목(VIT) 및 VIT 분류를 식별합니다.
스크립트	자율적	CI 취약성 분석	취약성 노출 평가 도구용 Advisor 에이전트는 구성 항목에 영향을 주는 취약성을 식별합니다.
스크립트	자율적	CVE 영향 분석	취약성 노출 평가 도구 자문가 에이전트는 영향을 받는 VIT 및 비즈니스 서비스의 수와 각각의 중요도를 고려하여 CVE(일반적인 취약성 노출 ID)의 영향을 분석합니다.
스크립트	자율적	주시 주제 생성	취약성 대응 도구: 수집된 취약성 및 구성 항목 정보를 기반으로 감시 주제를 생성하는 작업 실행자 에이전트입니다.

〔End〕

〔store-future: BEGIN review〕

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약성 대응에 대한 트리거: 영향 및 노출 평가 에이전트 워크플로우

이 에이전트 워크플로우에 대한 트리거가 없습니다. 필요한 경우 에이전트 워크플로우를 자동으로 호출하는 트리거를 추가할 수 있습니다.

〔End〕

취약성 대응 취약성 정정 상태 분석 에이전트 워크플로우를 위한 **AI** 에이전트 컬렉션

취약성 정정 상태 분석 에이전트 워크플로우를 위한 도구 및 AI 에이전트입니다.

취약성 정정 상태 분석 에이전트 워크플로우 개요

패널에서 취약성 정정 상태 분석 에이전트 워크플로우를 Now Assist 사용하여 다음을 수행할 수 있습니다.

- 규정 준수 메트릭 및 통계에 대한 인사이트를 확보하여 취약한 항목(VIT) 기록의 정정 목표 날짜를 얼마나 잘 충족하고 있는지 확인합니다.
- 월별 VIT 기록 정정 합계를 보고 누락된 대상을 식별합니다.
- 월간 서비스 수준 계약(SLA) 준수 검토를 위해 **VIT**에 대한 정정 데이터를 심각도, 할당 그룹, 구성 항목 및 취약성 별로 분류합니다.

이 에이전트 워크플로우를 수정하려는 경우 이를 복제 하고, 특정 요구에 맞게 설정을 조정하고, 에이전트 워크플로우의 복제된 버전을 활성화할 수 있습니다.

취약성 정정 상태 분석 에이전트 워크플로우에 사용되는 에이전트

정정 준수 인사이트 제공자는 취약성 정정 상태 분석 에이전트 워크플로우에서 사용됩니다.

〔store-future: BEGIN review〕

취약성 대응: 정정 대상 사용 케이스에 매핑된 도구

다음 도구는 취약성 대응에 사용되는 AI 에이전트에 매핑됩니다. 정정은 에이전트 워크플로우를 대상으로 합니다.

취약성 대응: 정정 대상 에이전트 워크플로우에 매핑된 도구

도구 유형	실행 모드	이름	설명
스크립트	자율적	정정 준수 통계 가져오기	정정 준수 인사이트 제공자를 위한 도구 에이전트는 월별, 심각도, 할당 그룹, 취약성 및 구성 항목별로 정정 준수 통계를 수집합니다.

〔End〕

〔store-future: BEGIN review〕

Vulnerability Response 트리거: 정정 대상 에이전트 워크플로우

이 에이전트 워크플로우에 대한 트리거가 없습니다. 필요한 경우 에이전트 워크플로우를 자동으로 호출하는 트리거를 추가할 수 있습니다.

〔End〕

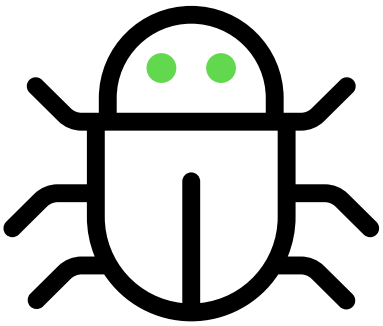
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

공격 표면 관리 애플리케이션

취약성 대응 및 공격 표면 관리를 구성하는 기타 애플리케이션은 취약한 자산의 우선 순위를 지정하고 비즈니스 크리티컬 시스템이 위협받는 시기를 확인하는 데 도움이 되는 컨텍스트를 추가합니다. 또한 보안 팀은 CMDB를 사용하여 시스템 간 종속성을 쉽게 식별하고 변경 또는 다운타임이 비즈니스에 미치는 영향을 신속하게 평가할 수 있습니다.

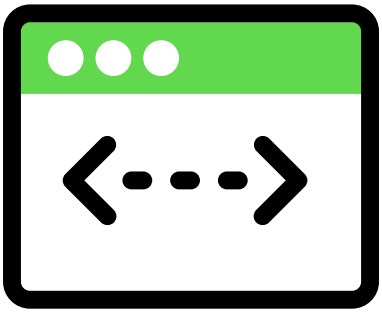
취약성 대응 애플리케이션

취약성 대응



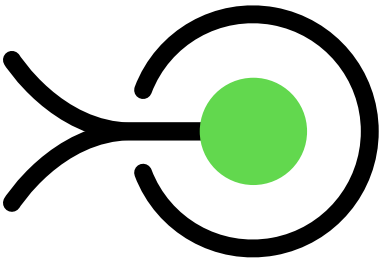
Vulnerability Response 애플리케이션에 대해 알아보기

애플리케이션 취약성 대응



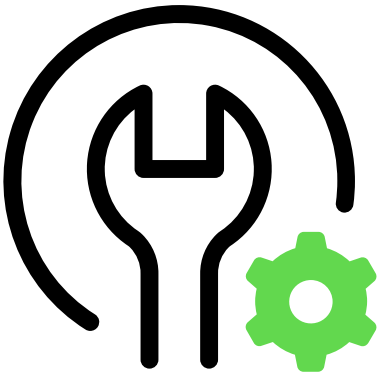
Application Vulnerability Response 애플리케이션에 대해 알아보기

컨테이너 취약성 대응



컨테이너 취약성 대응 애플리케이션에 대해 알아보기

구성 준수



Configuration Compliance 애플리케이션에 대해 알아보기

소프트웨어 자재 명세서

소프트웨어 자재 명세서 애플리케이션에 대해 알아보기

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약성 대응 작업 공간

취약성 관리자 작업 공간	IT 정정 작업 공간	취약성 평가 작업 공간
취약성 관리자 작업 공간에 대해 알아보기	IT 정정 작업 공간에 대해 알아보기	취약성 평가 작업 공간에 대해 알아보기

문제 해결 및 도움 받기

- Security Operations 리소스 라이브러리
- Security Operations 커뮤니티
- 알려진 오류 포털에서 알려진 오류 문서 검색
- 연락처 고객 서비스 및 지원

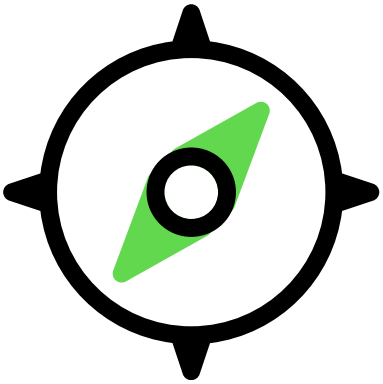
취약성 대응

NVD(국가 취약성 데이터베이스) 및 기타 소스는 알려진 취약성에 대한 정보를 수집합니다. 이러한 취약성에는 소프트웨어, 맬웨어가 악용할 수 있는 운영 체제 및 기타 공격의 약점이 포함될 수 있습니다. 이 ServiceNow# 취약성 대응 애플리케이션은 이러한 취약성을 추적, 우선순위 지정 및 해결하는 데 도움이 됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

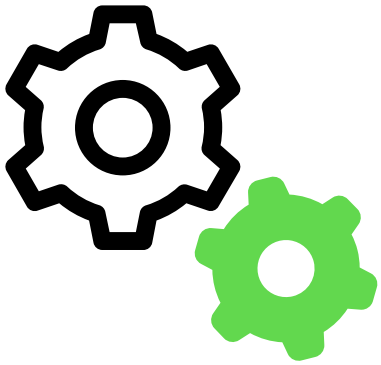
취약성 대응

탐색



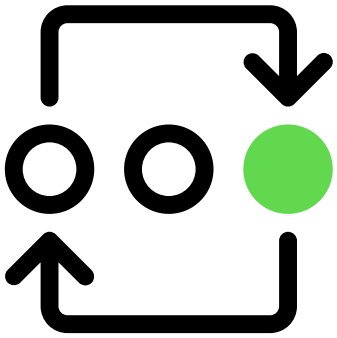
Vulnerability Response 기능에 대해 알아보기

설정 및 구성



Vulnerability Response 애플리케이션 설치 및 설정

통합

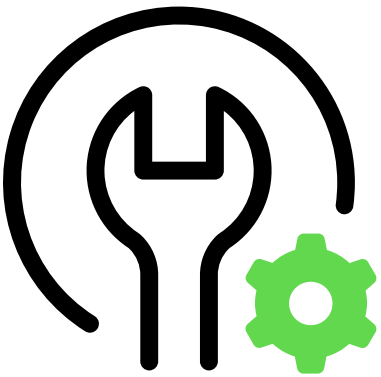


다른 애플리케이션과 통합하여 Vulnerability Response 확장

Vulnerability Response 작업 공간 사용

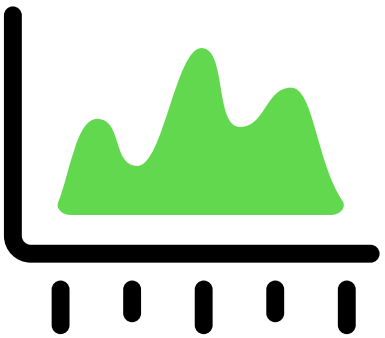
취약성 관리자, IT 정정 및 취약성 평가 작업 공간에서 VIT를 모니터링, 관리 및 정정하는 방법을 알아봅니다.

정정



Vulnerability Response의 기능을 사용하여 취약성을 정정하고 자산을 보호합니다.

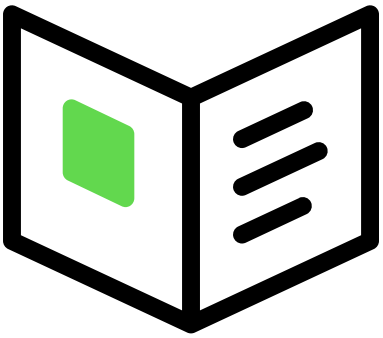
분석 및 보고



정정 진행률 모니터링

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

참조



Vulnerability Response 릴리스 정보, 구성요소에 대한 자세한 정보와 필드, 테이블 및 속성에 대한 참조 정보를 얻습니다.

문제 해결 및 도움 받기

- Security Operations 리소스 라이브러리
- Security Operations 커뮤니티
- 알려진 오류 포털에서 알려진 오류 문서 검색
- 연락처 고객 서비스 및 지원

애플리케이션 탐색 취약성 대응

이 ServiceNow# 취약성 대응 애플리케이션은 취약성을 신속하게 정정할 수 있는 규칙에 따라 취약한 항목을 임포트하고 자동으로 그룹화합니다. 취약성 데이터는 NVD(국가 취약성 데이터베이스) 및 타사 통합과 같은 외부 소스에서 가져와 에서 개발한 ServiceNow#애플리케이션으로 처리됩니다.

취약한 항목, 정정 작업 및 수명주기를 정의하는 취약성 대응에 대한 개요를 시청하십시오.

엔터프라이즈 내의 일반적인 취약성 대응과 ServiceNow의 취약성 대응을 비교하여 개요로 취약한 항목, 취약성 그룹 및 이들의 수명주기를 정의합니다.

취약성 대응 및 기업 환경

일반적으로 엔터프라이즈 환경 내에서 조직은 취약성 스캐너와 평가 도구를 사용하여 취약성이 자산에 미치는 위험을 식별하고 관리합니다. 이러한 도구에서 식별된 취약성은 조직의 자산 유지 관리 및 보안을 담당하는 보안 및 IT 팀에 위험으로 해석됩니다. 일부 위험에는 다음과 같은 유형의 식별된 취약성이 포함될 수 있지만 이에 국한되지는 않습니다.

- 오래된 소프트웨어 또는 잘못 구성된 시스템에 대한 의존
- 보안되지 않은 네트워크 프로토콜
- 결함이 있는 외부 공급업체 소프트웨어 라이브러리에 대한 종속성

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 열악하거나 일관되지 않은 시스템 관리 위생
- 강화되지 않은 기준선 시스템 이미지

이러한 잠재적 위험이 노출됨에 따라 보안 및 IT 팀은 일반적으로 검사 및 평가 도구에서 생성된 많은 양의 취약성 정보를 처리하고 처리하는 데 어려움을 겪습니다. 특히 이러한 팀은 대량의 식별된 취약성을 관리하고 조직이 직면한 잠재적 위험을 완화하기 위해 실행 가능한 대응 노력을 만들 때 압도당합니다.

다음 질문을 통해 자신의 보안 태세에 대한 이러한 도전 과제를 식별할 수 있습니다.

- 식별된 어떤 취약성을 먼저 검토해야 합니까?
- 이렇게 식별된 취약성은 조직에 어떤 의미가 있습니까?
- 식별된 위험에 대해 책임을 지고 소유해야 하는 사람은 누구입니까?
- 이러한 위험을 해결/완화하기 위해 직접 관여해야 하는 사람은 누구입니까?
- 보유한 리소스로 식별된 취약성을 효과적으로 완화하려면 어떻게 해야 합니까?
- 식별된 취약성을 줄임으로써 의도하지 않은 잠재적 결과는 무엇입니까?
- 취약성을 정정하고, 수행한 단계를 추적하고, 조치가 제대로 되었는지 확인하기 위해 후속 조치를 취하려면 어떤 프로세스를 따라야 합니까?
- 전반적인 위험 태세를 줄이는 데 진전이 있는지 어떻게 알 수 있습니까?

취약성 대응및 보안 운영**ServiceNow AI Platform®**

이 취약성 대응 애플리케이션은 보안 운영 제품군의 일부입니다. 이러한 애플리케이션을 함께 사용하면 전반적인 보안 태세를 개선하여 자산을 보호할 수 있습니다.

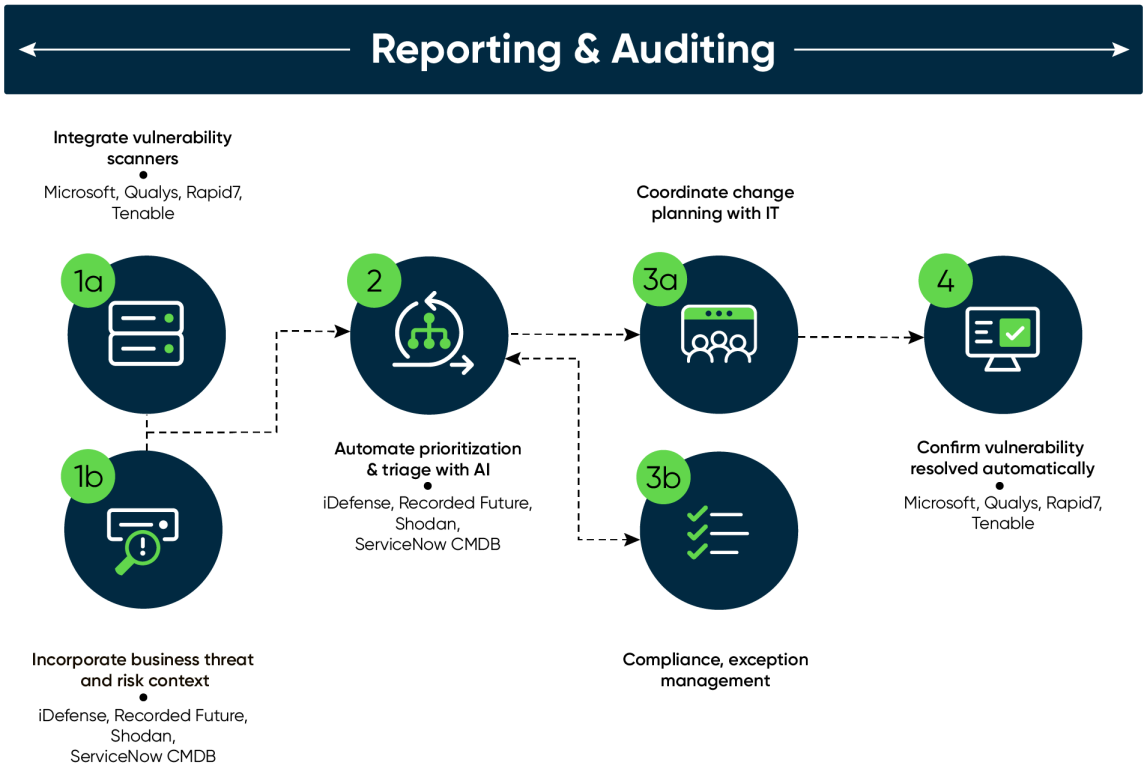
애플리케이션에는 ServiceNow 취약성 대응 두 가지 기본 목표가 있습니다.

- 방대한 양의 취약성 데이터를 처리해야 하는 보안 팀을 지원합니다.
- 취약성 해결을 담당하는 운영 팀을 지원합니다.

이러한 방식으로 애플리케이션을 사용하여 취약성 대응 통합에서 조사, 그리고 해결에 이르는 정보 플로우를 자동화할 수 있습니다.

의 ServiceNow AI Platform# 취약성 관리 프로세스에는 프로세스, 데이터, 보고 및 자동화가 CMDB포함될 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



- 외부 공급업체 스캐너 및 ServiceNow# 애플리케이션을 취약성 대응 애플리케이션과 통합하여 알려진 취약성 데이터를 수집합니다.
- 수집된 취약성 데이터를 악용, 위협 인텔리전스, 위험 및 비즈니스 컨텍스트로 개선합니다. 이 데이터를 사용하면 패치 적용 및 정정 전략에 도움이 됩니다.
- NVD에서 임포트한 취약성과 외부 공급업체 제품의 탐지 데이터가 CMDB의 자산과 조정됩니다. 환자 분류에는 여러 취약한 항목, 즉 취약성이 있는 것으로 확인된 자산으로 구성된 정정 작업을 생성하고, 이러한 작업을 범주별로 그룹화하고, 우선순위를 지정하고, 팀에 할당하는 작업이 포함될 수 있습니다.
- 조정된 변경 및 예외 관리를 사용하면 추가적인 수동 개입, 해결에 더 많은 시간 또는 광범위한 조사가 필요할 수 있는 취약성을 해결하는 데 도움이 됩니다.
- 스캐너 제품의 탐지를 통해 취약성이 자동으로 해결되고 업데이트되는지 확인합니다.

조직에서 사용할 취약성 대응 수 있는 사용자

취약성 대응 사용자는 일반적으로 두 가지 가상 사용자로 나뉩니다.

취약성 분석가

취약성 분석가 가상 사용자는 일반적으로 보안, 위험 및 준수 또는 관리에 있습니다. 이러한 사용자는 취약성을 모니터링하고 정정 프로세스를 시작할 시기를 결정합니다.

> **중요사항:**
> 취약성 분석가는 주로 를 취약성 관리자 작업 공간 사용하여 정정 작업을 모니터링하고 생성합니다.

정정 소유자

정정 소유자 가상 사용자는 일반적으로 IT 운영, DevOps/엔지니어링 또는 서비스 소유자의 일부입니다. 이러한 사용자는 취약성을 수정하는 데 필요한 정정 작업을

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

완료합니다. 자산 유지관리 또는 제거를 위해 제어된 프로세스가 필요한 경우 예외 또는 변경 요청을 제출할 수 있습니다.

중요사항:
정정 소유자는 주로 IT 정정 작업 공간.

애플리케이션 취약성 대응

애플리케이션 취약성 대응 애플리케이션의 (AVR) 기능은 ServiceNow# 취약성 대응 애플리케이션 취약한 항목(AVIT)을 임포트하고 규칙에 따라 애플리케이션 취약성을 정정할 수 있습니다. 별도의 구독으로 사용할 수 있습니다. 설명서는 문서를 참조하십시오 애플리케이션 취약성 대응애플리케이션 취약성 대응 탐색.

사용 가능한 버전

에 있는 양식 및 기록 취약성 대응의 필드 데이터 외에 링크, 문제 해결, 지식 문서를 포함하는 용어집 및 추가 참조 항목은 를 참조하십시오 취약성 대응 참조 정보.

릴리스 버전	릴리스 정보
취약성 대응 v23.0	호환성 정보는 KB0856498 Vulnerability Response 호환성 매트릭스 및 릴리스 스키마 변경을 참조하십시오.

취약성 대응 애플리케이션 및 **CSDM** 테이블

, 취약성 대응애플리케이션 취약성 대응, 타사 취약성 통합 및 소프트웨어 자재 명세서 애플리케이션은 테이블을 관리(데이터 기여) CSDM 합니다. 이러한 애플리케이션은 다른 애플리케이션이 생성하는 테이블의 데이터 CSDM 도 사용합니다. 따라서 여러 ServiceNow 제품이 이러한 보안 운영 애플리케이션의 이점을 누리고 가치를 더합니다. 자세한 내용은 취약성 대응 애플리케이션 및 CSDM 테이블 문서를 참조하십시오.

취약성 대응 설치 및 지원되는 애플리케이션

취약성 대응 응용 프로그램은 에서 사용할 수 있습니다ServiceNow Store. 이 애플리케이션은 에서 ServiceNow Store다운로드하는 다른 ServiceNow 애플리케이션 및 타사 통합을 지원합니다. 기본 설정을 확장하기 위해 더 많은 옵션을 사용할 수도 있습니다.

기본 설정을 위한 작업

취약성 대응 첫 번째 단계로 애플리케이션이 필요합니다. 설치에 대한 자세한 정보는 취약성 대응 애플리케이션 설치의 내용을 참조하십시오애플리케이션의 구현 검사 목록 취약성 대응.

- 설치가 완료되면 설정 도우미를 사용하여 취약성 대응을 구성할 수 있습니다.

  설정 도우미를 사용하여 애플리케이션에 액세스할 사용자 및 그룹을 할당하고, 담당 규칙, 정정 작업 규칙 및 목표 날짜를 생성 또는 편집하고, 위험 계산기를 설정합니다.

- 설정 도우미에서 지원되는 타사 통합을 하나 이상 선택, 설치 및 구성할 수도 있습니다. 이러한 통합은 외부 시스템 및 벤더에서 취약성 데이터를 검색합니다. 통합의 작동 방식과 에서 취약성 대응지원하는 통합에 대한 자세한 내용은 을 참조하십시오 취약성 대응 통합.
- 외부 공급업체 통합을 구현하기 전에 의 초기 설정 취약성 대응의 일부로 NVD 통합 및 CWE 예약된 작업을 실행합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

NVD 및 CWE 라이브러리 설치, 구성 및 보기에 대한 자세한 내용은 을 CWE 기록을 업데이트하기 위해 예약된 작업을 구성하고 실행합니다. 참조하십시오NVD 및 CWE 통합을 통해 데이터를 임포트하고 외부 공급업체 라이브러리를 관리합니다.

- 해당하는 경우 분석 애플리케이션을 선택합니다. Performance Analytics Content Pack for Vulnerability Response 애플리케이션에는 취약성 관리 수명주기의 모든 단계를 다루는 보고서가 포함되어 있습니다.

  〔선택사항〕〔PA〕애플리케이션 설치 및 구성 취약성 대응용 퍼포먼스 분석 신청.

- 해당하는 경우 솔루션 애플리케이션을 선택합니다. 솔루션 관리는 사용자 환경의 취약성과 이를 정정할 수 있는 솔루션의 상관 관계를 파악하는 데 도움이 됩니다. 〔선택 사항〕취약성 대응용 솔루션 관리 애플리케이션 설치.

  주:

  - 취약성 솔루션 관리 애플리케이션이 활성화되면 설정 도우미에서 및 Microsoft Security Response Center 솔루션 통합 을(를Red Hat Solution Integration) 편집할 수 있습니다.
  - 취약성 솔루션 관리 별도의 구독이 필요합니다. 자세한 내용은 취약성 솔루션 관리 문서를 참조하십시오.

- 〔선택사항〕에 대한 취약성 대응용 모바일 환경ServiceNow Agent 앱 및 취약성 대응 Mobile 앱을 설치합니다.

수행할 수 있는 기타 설정 작업

이러한 추가 설정 작업은 기본 구성에 추가되며 보고, 이메일 알림, 네이티브 통합 구성 및 취약한 항목 작업에 대한 옵션을 통해 정정을 지원합니다. 이러한 작업의 대부분은 설정 도우미 외부에서 수행됩니다. 추가 취약성 대응 설정 및 구성 작업 문서를 참조하십시오.

기본 설정 외의 고급 작업

이러한 선택적 구성 작업은 설정 도우미 외부에서 수행되며 코딩 또는 고급 ServiceNow 전문 지식이 필요하며 기본 구성의 일부로 간주되지 않습니다. 고급 취약성 대응 구성 작업 문서를 참조하십시오.

취약성 대응 가상 사용자 및 세분화된 역할

애플리케이션의 취약성 취약성 대응 을 성공적으로 정정하려면 먼저 설정 도우미에서 사용자 및 그룹에 가상 사용자와 역할을 할당해야 합니다.

애플리케이션에 필요한 취약성 대응 첫 번째 구성 단계 중 하나는 사용자 및 그룹에 역할을 할당하는 것입니다. 역할은 사용자와 그룹이 에서 보고 수행할 취약성 대응수 있는 것을 정의하고, 취약성 대응용 퍼포먼스 분석와 모든 외부 공급업체 통합을 취약성 대응정의합니다.

설정 도우미에서 기존 사용자 및 그룹에 가상 사용자 역할을 할당합니다. 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당 문서를 참조하십시오.

주:

업그레이드 고객인 경우 애플리케이션에 대한 기존 역할을 계속 사용할 수 있습니다 취약성 대응 . v10.3 이전의 sn_vul.vulnerability_read 및 sn_vul.vulnerability_write 권한으로 할당된 사용자 및 그룹과 정정 소유자에 대한 액세스 권한은 변경되지 않았습니다.

그러나 작업 수준의 애플리케이션에서 사용자 및 그룹이 수행하고 볼 취약성 대응 수 있는 것을 보다 세부적으로 제어하려면 세분화된 역할을 사용하는 것이 좋습니다. 자세한 내용은 의 가상 사용자 및 세분화된 역할 관리 취약성 대응 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설정 도우미를 사용하여 역할을 이미 할당한 경우 사용자 관리 모듈에서 모든 사용자 및 그룹에 대한 세분화된 역할 할당을 관리하려면 자세한 내용을 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응 .

가상 사용자 역할 및 세분화된 역할 시작

주요 용어입니다.

역할

역할은 애플리케이션에서 보고 수행할 취약성 대응 수 있는 사용자와 그룹을 정의합니다.

그룹

특정 역할과 공통의 목적을 공유하는 사용자의 집합입니다.

가상 사용자 역할

애플리케이션에서 미리 구성된 역할로, 세분화된 여러 역할로 구성됩니다. 설정 도우미, 취약성 관리자, 취약성 분석가, 정정 소유자, 구성 항목 관리자 및 예외 관리자의 가상 사용자 역할은 IT 조직 또는 취약성 개선 그룹의 관리자, 분석가 및 서비스 소유자의 일반적인 직책에 해당하도록 설계되었습니다.

상속된 역할

사용자가 다른 역할을 할당받을 때 자동으로 획득하는 역할을 설명하는 용어입니다. 예를 들어 sn_vul.remediation_owner 가상 사용자 역할이 할당된 모든 사용자 또는 그룹은 sn_vul.read_assigned,sn_vul.write_assigned 세분화된 역할도 상속합니다.

접근 제어 목록(ACL)

접근 제어 목록은 사용자가 데이터와 상호작용하기 전에 일련의 요구 사항을 통과하도록 요구하여 데이터에 대한 액세스를 제한합니다.

v16.5부터 취약성 대응 보고서가 노출되지 않도록 보호하려면 모든 **report_view** ACL을 로 *active=true*설정합니다. 이 ACL을 사용하면 보호된 데이터를 권한 있는 사용자만 사용할 수 있습니다.

설정 지원에서 가상 사용자 역할에 그룹과 사용자를 할당합니다.

주:
설정 도우미에서 시스템 관리자 역할(admin)은 첫 번째 섹션의 작업, 역할 할당 및 통합 설치에 필요합니다. 설정 도우미에서 가상 사용자 역할을 할당하고 통합을 설치한 후 sn_vul.vulnerability_admin 역할을 가진 사용자 또는 그룹을 할당하여 설정 도우미에서 나머지 작업을 완료하고 애플리케이션을 관리할 취약성 대응 수 있습니다.

다음 표에는 애플리케이션과 함께 설치되는 가상 사용자 역할이 나열되어 취약성 대응 있습니다.

의 가상 사용자 역할 취약성 대응	설명
사용자 또는 그룹에 sn_vul.vulnerability_admin - 취약성 관리자를 할당합니다.	이 역할을 가진 사용자는 취약성 대응(VR) 애플리케이션 및 해당 기록에 대한 전체 액세스 권한을 갖습니다. 이 역할을 가진 사용자는 모든 VR 애플리케이션 및 규칙을 구성하고 외부 공급업체 통합을 설치합니다.
사용자 및 그룹에 sn_vul.vulnerability_analyst - 취약성 분석가를 할당합니다.	이 역할을 가진 사용자 및 그룹은 VI 정정에 대한 모든 기록을 보고 업데이트합니다.
사용자 및 그룹에 sn_vul.remediation_owner - 정정 소유자를 할당합니다.	이 역할을 가진 사용자와 그룹은 자신 또는 자신이 속한 그룹에 할당된 취약성을 정정합니다. 이 역할을 가진 그룹 또는 사용자는

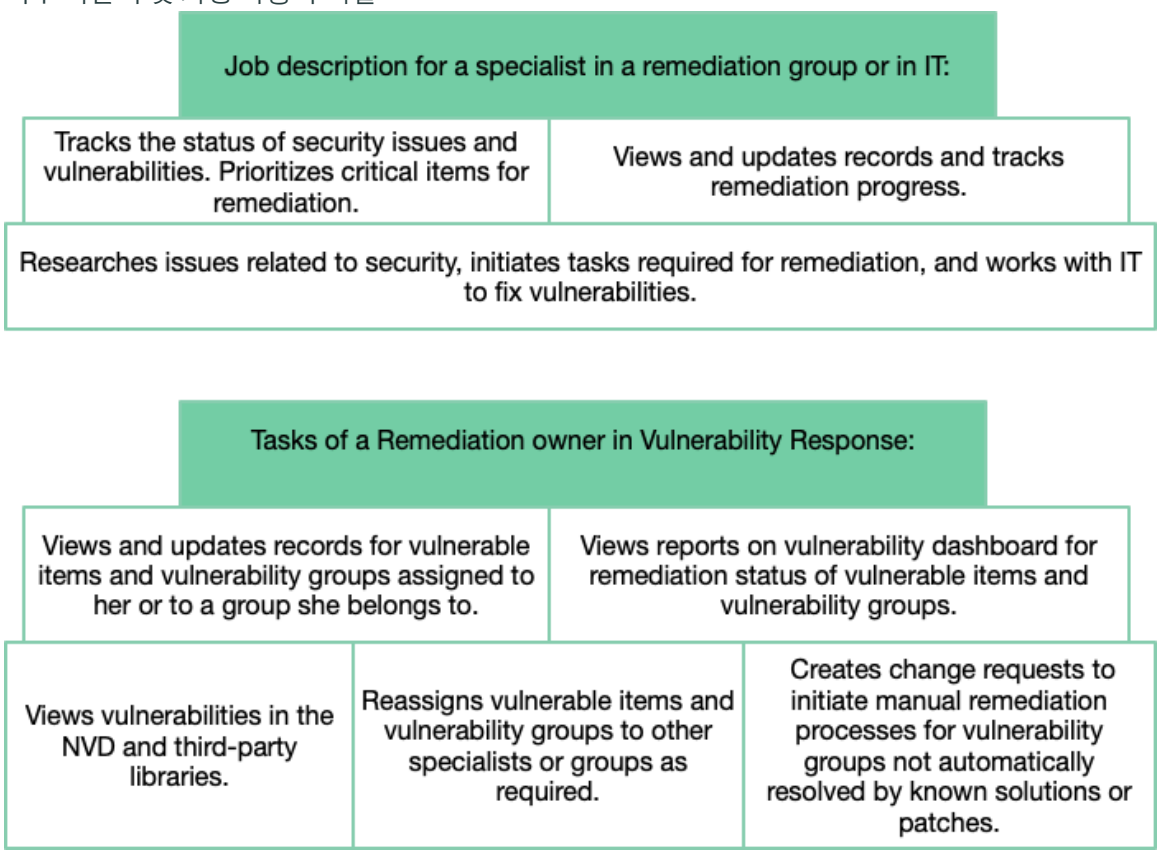
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

의 가상 사용자 역할 취약성 대응	설명
	자신 또는 자신이 속한 그룹에 할당된 기록을 확인하고 업데이트합니다.
사용자 및 그룹에 sn_vul.ci_manager를 할당합니다.	이 역할을 가진 사용자와 그룹은 구성 관리 데이터베이스(CMDB)에서 찾을 수 없는 일치하지 않는 구성 항목(CI)의 재분류를 관리합니다.
작업별로 애플리케이션의 특정 영역에 대한 읽기 권한을 할당합니다.	예를 들어 사용자가 모든 VR 기록을 볼 수 있도록 sn_vul.read_all을 할당합니다. 정정 작업 규칙을 보기 위한 읽기 권한의 경우 sn_vul.read_group_rules를 할당합니다. 이 역할을 가진 사용자와 그룹은 기록을 업데이트하지 않습니다.

세분화된 역할 및 가상 사용자 역할

가상 사용자 역할에 대해 생각하는 한 가지 방법은 해당 설명이 조직의 다양한 IT 또는 취약성 수정 직책에 대한 직무 설명과 어떻게 관련될 수 있는지 고려하는 것입니다. 다음 그림은 IT 정정 전문가가 수행할 수 있는 직무 설명과 이 작업과 관련된 작업이 애플리케이션의 정정 소유자 가상 사용자 역할 취약성 대응 의 작업과 어떤 관련이 있는지 보여줍니다.

직무 기술서 및 가상 사용자 역할



직무 기술서와 정정 소유자 가상 사용자 역할은 모두 일련의 정정 작업으로 정의할 수 있습니다. 앞의 이미지에서 녹색 블록의 직무 설명과 가상 사용자 역할은 직무를 설명하는 작업 위에 있습니다. 이 예에서 정정 그룹의 전문가에 대한 일반적인 작업 요구사항 중 일부는 다음의 취약성 대응정정 소유자 가상 사용자를 구성하는 작업에 직접 해당합니다. 기록을 검토 및 업데이트하고, 취약성의 정정 상태를 추적하고, 정정할 항목의 우선순위를 지정하고, IT와 함께 수정 사항 및 패치를 적용합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

하지만 조직의 작업이 애플리케이션의 5가지 가상 사용자 역할 중 하나를 구성하는 작업과 직접적으로 일치하지 않을 수도 있습니다 취약성 대응 . 중요한 데이터 보호 또는 규정 준수와 같은 다양한 이유로 일부 가상 사용자 역할이 사용자 및 그룹에 제공하는 광범위한 액세스를 제한해야 합니다. 또는 반대로 작업을 수행할 수 있도록 사용자와 그룹에 더 많은 액세스 권한을 제공해야 합니다. 세분화된 역할을 사용하면 역할을 쉽게 사용자 지정하고 사용자 및 그룹이 , , 외부 공급업체 통합에 대해 취약성 대응취약성 대응용 퍼포먼스 분석갖는 접근 권한을 제어할 수 있습니다.

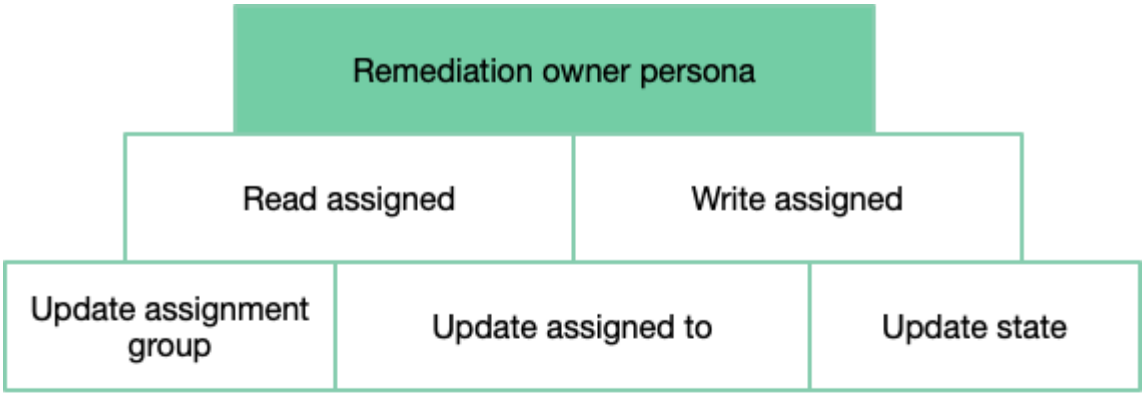
세분화된 역할은 작업을 정의합니다

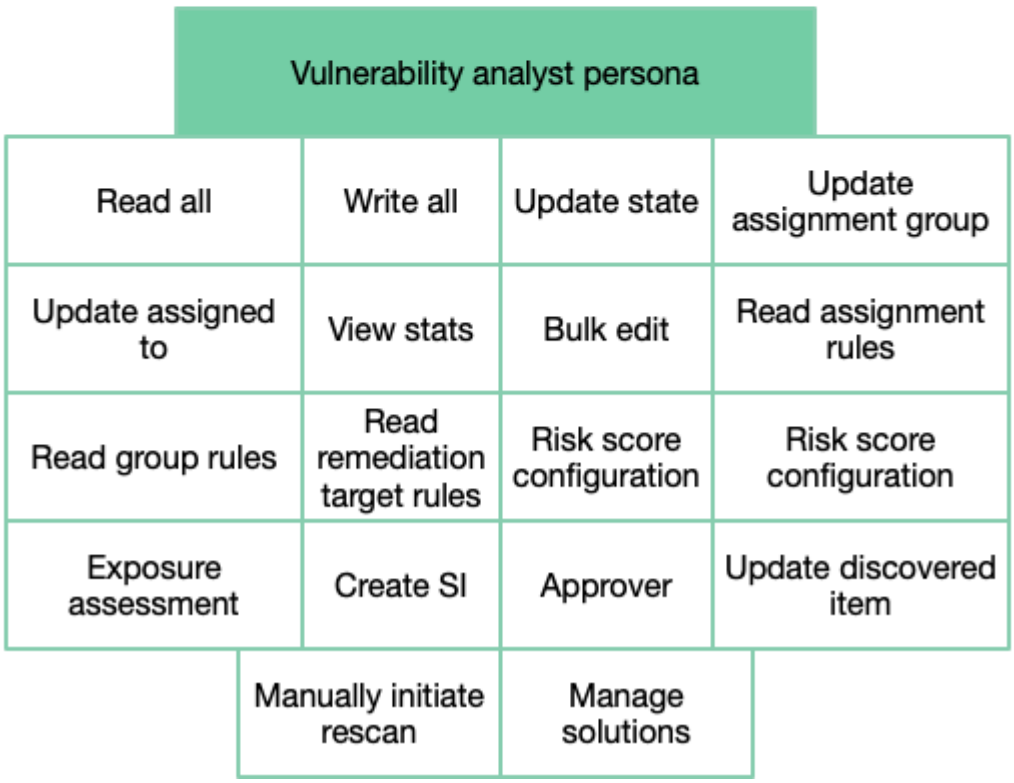
의 취약성 대응 세분화된 역할 이름은 일반적으로 애플리케이션에서 사용자가 수행하고 볼 취약성 대응 수 있는 것을 설명합니다. 예를 들어 이전 이미지에서 정정 소유자 가상 사용자가 할당된 사용자 및 그룹에는 sn_vul.read_assigned 및 sn_vul.write_assigned 세분화된 역할이 있습니다. 이러한 세분화된 역할을 통해 사용자나 그룹은 자신에게 할당된 취약한 항목 및 정정 작업 기록을 보고 업데이트할 수 있습니다. 세분화된 특정 역할에 대한 설명을 보려면 시스템 관리자 역할을 가진 사용자는 다음으로 이동합니다. 사용자 관리 〉 역할 원하는 역할을 찾습니다. 역할이 할당될 때 자동으로 상속되는 역할이 나열됩니다. 또한 역할이 다른 역할 할당에 종속되는 경우 필요한 역할도 나열됩니다.

다음 이미지에는 정정 소유자 가상 사용자 역할과 취약성 분석가 가상 사용자의 세분화된 역할이 설명되어 있습니다. 정정 소유자 가상 사용자에는 취약성 분석가 가상 사용자의 read_all 및 write_all 권한이 포함되지 않습니다. 사용자와 그룹이 모든 취약한 항목 및 정정 작업 기록을 읽고 편집하려면 세분화된 역할(read_all 및 write_all)이 필요합니다. 이러한 역할을 사용자 지정하려면 세분화된 역할을 추가하거나 제거하여 액세스를 확장하거나 제한하기만 하면 됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

세분화된 역할과 정정 소유자 및 취약성 분석가 가상 사용자





사용자와 그룹이 가상 사용자 역할이 허용하는 것보다 더 많은 액세스 권한을 갖도록 하려면 사용자 및 그룹에 더 세부적인 역할을 추가할 수 있습니다. 반대로 작업 수준에서 특정 사용자 및 그룹에 대한 액세스를 제한하려면 세분화된 역할을 제거할 수 있습니다.

주:
사용자 관리 모듈에서 세분화된 역할을 할당하고 편집하려면 시스템 관리자 역할이 필요합니다.

스크립팅 액세스 권한이 있는 세분화된 역할

다음 역할은 나열된 테이블에 대한 스크립팅 액세스 권한을 제공합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

역할	테이블	애플리케이션
sn_vul.manage_auto_close_stale_vi	sn_vul_cmn_auto_close_rule	취약성 대응
sn_vul.app_manage_auto_close_rule		취약성 대응
sn_vul_container.manage_auto_close_stale_vi		컨테이너 취약성 대응
sn_vul_container.manage_assignment_rules	sn_vul_assignment_rule	컨테이너 취약성 대응
sn_vul.app_manage_assignment_rules		애플리케이션 취약성 대응
sn_vul.manage_assignment_rules		취약성 대응
sn_vul_agile.쓰기	sn_vul_agile_tool	취약성 대응
sn_vul_int_fw.configure_integrations	sn_vul_int_fw_integration	취약성 대응

사용자 관리 모듈의 세분화된 역할

사용자 또는 그룹의 세분화된 역할을 관리하는 방법의 예는 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

가상 사용자 역할을 할당하려면 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당.

취약성 대응 할당 규칙 개요

정정을 위해 취약한 항목(VIT)이 할당 그룹에 자동으로 할당되는 기준을 정의합니다.

기본 할당 규칙인 **CI** 지원 그룹에 할당은 **CI** 지원 그룹에 취약한 항목을 할당하는 기본 시스템에 포함됩니다. CI에 할당 지원 그룹 규칙은 VIT와 연결된 CI(구성 항목)에 대해 설정된 지원 그룹에 VIT를 할당합니다.

주:
담당 규칙은 수동으로 생성된 할당을 다시 평가하지 않습니다.

VIT 양식 및 목록 뷰에서 수동 또는 규칙을 사용할 수 있는지 여부를 나타내는 할당 유형입니다. 원래 규칙에 의해 할당되었지만 이후에 수동으로 재할당된 VIT에는 원래 규칙에 대한 참조가 포함되어 있습니다.

할당 규칙 및 할당 유형 정보를 사용하여 담당 규칙이 의도한 수신자에 대한 올바른 일치 항목을 찾지 못한 케이스를 식별합니다. 또한 이 정보를 사용하여 가장 많은 재할당이 이루어진 규칙을 식별할 수 있습니다.

할당 규칙에 의해 설정된 할당 그룹은 정정 작업 규칙 에서 소유자를 VUL(정정 작업)에 할당하는 데 사용됩니다.

주:
담당 규칙의 조건 필터에서 자산 태그를 사용할 수 있게 하려면 Rapid7 InsightVM 다른 Rapid7 InsightVM 통합보다 먼저 자산 목록 통합을 실행해야 Rapid7 InsightVM 합니다.

조건 작성기에 입력한 검색 텍스트의 대소문자 구분은 이 기록이나 양식에서 지원되지 않습니다.

취약한 항목을 자동으로 할당

할당을 사용하여 취약한 항목을 할당하는 방법에는 세 가지가 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 사용자 그룹: 이 옵션을 사용하면 기존 ServiceNow AI Platform# 사용자 그룹을 선택할 수 있습니다.
- 사용자 그룹 필드: 이 옵션을 사용하면 cmdb_ci 테이블을 사용하여 사용 가능한 할당 그룹 필드를 선택할 수 있습니다. 기본적으로 다음과 같은 세 개의 그룹 필드가 표시됩니다.
  - 없음: 이 필수 필드의 기본값이 없음을 나타냅니다.
  - 구성 항목: 승인 그룹
  - 구성 항목: 담당 그룹
  - 구성 항목: 지원 그룹
- 스크립트: 이 옵션을 사용하면 스크립트를 사용하여 조건을 정의할 수 있습니다. 이 옵션을 사용하려면 코딩 또는 고급 ServiceNow 전문 지식이 필요합니다. 스크립트 편집기를 사용하여 복잡한 조건을 정의하는 방법에 대한 자세한 내용은 KB0965240 KB 문서를 참조하십시오.

우선 순위가 높은 규칙(특별한 처리가 필요하거나 위험이 중요하거나 규정 준수에서 VIT를 처리해야 하는 항목)을 먼저 실행합니다. 다음으로, 특별한 처리가 필요하지 않은 일반 규칙을 실행하고 누가 이를 담당해야 하는지 알 수 있습니다. 마지막으로, VIT가 속해야 하는 할당 그룹을 파악하는 그룹에 VIT를 할당하는 기본 규칙을 생성합니다. 이 그룹은 그들의 결정을 다루기 위해 또 다른 규칙을 추가할 수 있습니다. 이 기본 규칙은 마지막에 실행됩니다.

할당 규칙 평가 프로세스

담당 규칙은 새 VIT가 열릴 때, 즉 임포트, 수동 생성 또는 다시 열 때 VIT를 평가하고 할당하는 데 사용됩니다. VIT 또는 상태가 변경된 후 할당 규칙을 수동으로 다시 적용하지 않는 한 VI는 한 번 평가됩니다.

다음 프로세스는 새로 또는 업데이트되거나 다시 열린 각 VIT에 사용됩니다.

- 각 취약성 할당 규칙에 대해 VIT는 할당 필터와 비교됩니다. 가장 낮은 순서의 규칙이 먼저 적용됩니다.
- 조건이 일치하는 경우 VIT에 할당 그룹이 할당됩니다. 조회가 중지됩니다.
- 조건이 다른 모든 규칙 간에 일치하는 항목을 찾지 못하면 기본 규칙이 있으면 VIT가 기본 할당 그룹에 할당됩니다.

  취약한 항목이 할당되면 적절한 정정 작업 규칙은 취약한 항목을 정정 작업에 배치하기 위한 기준 중 하나로 할당을 사용합니다. 자세한 내용은 AND 내부 필터링 취약성 대응 문서를 참조하십시오취약성 대응 정정 작업 및 정정 작업 규칙 개요.

  주:
  기본 규칙은 실행 순서 값이 가장 높은 규칙입니다. 좋은 포괄적 인 최종 규칙은 active=true 입니다. 기본 규칙이 없으면 정정 작업 규칙이 할당할 때 VIT가 할당되지 않은 상태로 유지됩니다.

담당 규칙 다시 적용

할당 규칙을 변경할 때 할당 규칙 목록 페이지의 변경 사항 적용 버튼을 사용하여 수동으로 할당된 규칙을 제외한 모든 활성 VI에서 변경된 모든 규칙을 다시 실행합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

*Reapply all vulnerability assignment rules*변경 적용을 처음 사용하기 전에 예약된 작업이 실행되지 않은 경우 수동으로 할당된 VI를 제외한 모든 오픈 VIT에 대해 모든 할당 규칙이 실행됩니다. 이후에는 변경 내용 적용을 이후에 사용할 때마다 변경된 규칙과 종속 규칙만 다시 실행됩니다. 한 규칙을 변경하면 VIT가 수정되지 않은 다른 규칙과 일치할 수 있습니다. 담당 규칙을 다시 적용해도 취약한 항목은 다시 그룹화되지 않습니다.

예약된 작업 [*Reapply all vulnerability assignment rules*]은 기본적으로 비활성 상태입니다. 활성화되면 수동으로 할당된 VIT를 제외한 모든 오픈 VIT에 모든 규칙이 적용됩니다. 매일, 매주, 매월, 주기적으로, 한 번 또는 요청 시에 실행할 수 있습니다. 환경에 얼마나 많은 활성 VI가 있는지에 따라 성능에 영향을 미치지 않도록 초기 실행 후 실행 필드를 적절하게 설정해야 합니다.

업그레이드 고객은 이 기능이 기존 VIT에 미치는 영향에 대한 자세한 내용은 릴리스 정보를 참조 취약성 대응 해야 합니다.

중요사항:
취약성 관리자와 분석가는 에서 취약성 관리자 작업 공간선택한 취약한 항목에 대한 최신 할당을 얻을 수 있습니다. 이 방법은 시간이 오래 걸리는 프로세스인, 클래식 UI에서 모든 취약한 항목에 대해 할당 규칙을 실행하는 것보다 더 효율적입니다. 자세한 내용은 에 있는 기록의 정정 속성 재평가 취약성 관리자 작업 공간 문서를 참조하십시오.

할당 규칙의 할당 그룹이 변경되면 시스템 속성 sn_vul.rerun_task_rules 및 비즈니스 규칙 정정 작업에 연결을 활성화하여 취약한 항목을 자동으로 재평가하고 다시 그룹화할 수 있습니다.

시스템 속성을 활성화하려면 다음을 수행합니다.

1. 다음으로 이동 모두 〉 시스템 속성 〉 모든 속성.
2. sn_vul.rerun_task_rules 시스템 속성을 엽니다.
3. 값 필드에서 값을 true로 설정합니다.

시스템 속성이 true로 설정되고 담당 규칙이 다시 적용되면 조건이 더 이상 일치하지 않는 취약한 항목이 정정 작업에서 연결 해제됩니다.

주:
기본적으로 시스템 속성 sn_vul.rerun_task_rules은 false로 설정됩니다.

취약한 항목의 재그룹화를 자동화하려면 비즈니스 규칙 정정 작업 연결 을 활성화해야 합니다.

비즈니스 규칙을 활성화하려면 다음을 수행합니다.

1. 다음으로 이동 모두 〉 시스템 정의 〉 비즈니스 규칙.
2. 정정 작업에 대한 링크 열기 비즈니스 규칙.
3. 비즈니스 규칙을 활성화하려면 활성 확인란을 선택합니다.

활성화된 비즈니스 규칙은 취약한 항목을 관련 그룹으로 이동하거나, 기존 그룹 아래에 그룹화할 수 없는 경우 그룹을 생성하여 취약한 항목을 다시 그룹화합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

- 취약한 항목은 그룹을 삭제하지 않고 그룹에서 제거됩니다.
- 정정 작업 규칙 또는 정정 작업을 사용하여 생성된 항목만 제거됩니다.
- 재그룹화는 할당 그룹이 할당 규칙의 일부로 변경될 때만 자동으로 수행되며 수동으로 변경될 때는 변경되지 않습니다.
- 지연 상태의 VIT에는 할당 규칙이 적용되지 않습니다. VIT가 지연된 경우 필요한 경우 수동으로 할당해야 합니다.

작업 공간에서의 재그룹화는 정정 작업에서 생성된 정정 작업에 대해 수행됩니다.

취약성 대응 정정 작업 및 정정 작업 규칙 개요

분석가와 정정 전문가가 VI(취약한 항목)를 구성하고 대량으로 분석할 수 있도록 정정 작업(VUL)을 구성합니다. 취약한 항목을 정정 작업에 수동으로 할당할 필요가 없도록 정정 작업이 구성되는 기준이 구성됩니다. 정정 작업을 사용하여 진행 상황을 모니터링하고 정정 프로세스를 보다 효율적으로 추진할 수 있습니다.

취약한 항목 및 정정 작업에 대한 지연 수 추적

취약한 항목, 애플리케이션 취약한 항목, 컨테이너 취약한 항목 또는 정정 작업이 지연된 횟수를 추적합니다. 지연 수 설정이라는 예약된 작업은 매일 실행되어 지연 수 열에 두 번 이상 지연된 기록에 대한 개수를 게시합니다. 기록은 VR, AVR 및 CVR에 대한 여러 지연 모듈에 표시됩니다.

취약한 항목을 자동으로 새로 고침

주:
취약한 항목 새로 고침 자동화는 조건 필터 또는 필터 그룹을 사용하여 만든 정정 작업에만 적용됩니다. 자동화는 수동으로 추가되거나 정정 작업 규칙을 사용하여 그룹화된 VI에는 적용되지 않습니다.

관련 취약한 항목 자동 업데이트 확인란을 선택하면 정정 작업 필터 기준과 일치하는 새 VI가 작업에 자동으로 추가됩니다. 정정 작업에서 더 이상 필터 기준과 일치하지 않는 취약한 항목이 작업에서 자동으로 제거됩니다.

기본적으로 정정 작업이 열림 상태로 유지되면 확인란의 선택이 취소 됩니다. 상태에 관계없이 취약한 항목이 정정 작업에 계속 추가되도록 하려면 비즈니스 규칙을 비활성화합니다 ***Set auto refresh vulnerable items*** .

조사 중 상태에서 확인란을 수동으로 다시 선택할 수 있습니다. 정정 작업이 구현 대기 중 상태로 전환되면 관련된 취약한 항목 자동 업데이트가 비활성화되지 않습니다. 구현 대기 중 상태가 되면 기존 작업에 새로운 취약한 항목을 추가할 수 없으며 기존의 취약한 항목을 제거할 수도 없습니다.

주:
정정 작업이 수동으로 생성되고 조건 필터 또는 필터 그룹을 사용하여 VI가 추가되면 확인란이 선택 취소됩니다. 상자를 선택할지 여부를 선택할 수 있습니다.

취약한 항목을 수동으로 새로 고침

필터 그룹 또는 조건 필터를 사용하여 수동으로 생성된 정정 작업의 경우, 정정 작업 페이지에서 연결된 취약한 항목 새로 고침 관련 링크를 클릭하면 필터 기준과 일치하는 모든 취약한 항목이 추가됩니다. 더 이상 기준과 일치하지 않는 항목은 제거됩니다. 이 작업을 수행하면 취약한 항목 목록을 즉시 업데이트할 수 있으며 관련 취약한 항목 자동 업데이트 확인란의 선택 여부와 관계없이 사용됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

조건 또는 필터 그룹 필터 유형을 사용하여 수동으로 생성된 정정 작업은 한 시간에 한 번 새로 고침됩니다.

정정 작업 규칙 이해

정정 작업 규칙을 사용하면 취약한 항목을 자동으로 그룹화하고 할당하는 방법을 정의할 수 있습니다. 기본 규칙인 취약성은 취약성을 기반으로 취약한 항목을 수집하는 기본 시스템에 포함됩니다. 그러나 VI에서 액세스할 수 있는 열의 다른 값 집합으로 그룹화할 수 있습니다. 이러한 값에는 CI(구성 항목), 지원 그룹, 취약성 심각도 등이 포함될 수 있습니다.

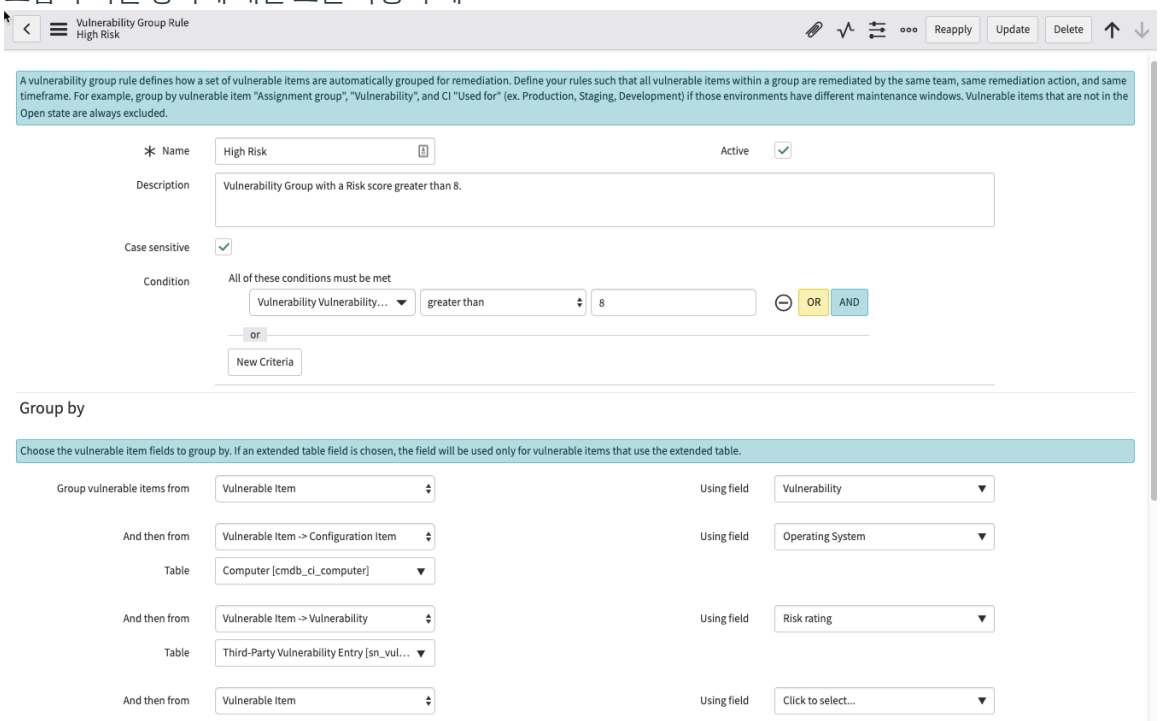
원하는 수만큼 조건을 생성할 수 있습니다. 선택 기준으로 그룹을 설정하면 다른 행이 나타납니다. 최대 6개의 그룹화 기준 선택 항목을 가질 수 있습니다. 그룹 할당을 자동화할 수도 있습니다. 자세한 내용은 AND 내부 필터링 취약성 대응 문서를 참조하십시오정정 작업 규칙 생성 또는 편집 취약성 대응.

주:
정정 작업 규칙의 조건 필터에 자산 태그를 사용할 수 있도록 하려면 Rapid7 InsightVM 다른 Rapid7 InsightVM 통합보다 먼저 자산 목록 통합을 실행해야 Rapid7 InsightVM 합니다.

예를 들어 취약한 CI의 비용 센터 또는 취약성의 공격 벡터별로 취약한 항목을 그룹화할 수 있습니다. 심각도가 낮은 취약성 또는 위험도가 낮은 CI에 대해 하나의 작업 규칙을 가질 수 있습니다. 중요한 서버에 대한 또 다른 작업 규칙과 익스플로잇이 있는 취약점(회사를 더 많은 위험에 노출시키는 취약한 항목)이 있을 수 있습니다.

회사를 더 큰 위험에 노출시키는 취약한 항목에는 다른 규칙 집합을 사용할 수 있습니다. 정정 작업 이름이 정정 작업 규칙 그룹화 기준 값에 추가되어 새 기록에 대한 짧은 설명을 작성합니다. 사용 가능한 필드에 대한 자세한 내용은 을 참조하십시오 에서 수동으로 정정 작업 생성 취약성 대응 .

그룹화 기준 항목에 대한 조건 작성기 예



새로운 취약한 항목이 생성되거나, 임포트되거나, 종결된 후 다시 열리면 취약성 규칙이 평가됩니다. VI는 닫힌 후 다시 열리거나 규칙이 수동으로 다시 적용되지 않는 한 자동으로 한 번만 평가됩니다.

새 VI 또는 다시 열린 각 VI에 대해 다음 프로세스가 사용됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 각 정정 작업 규칙에 대해 VI는 정정 작업 규칙 필터와 비교됩니다.

- 정정 작업 규칙 조건이 일치하는 각 규칙에 대해 규칙은 VI의 그룹화 기준 선택 항목에서 데이터를 가져옵니다. 그룹 이름과 필드를 빌드합니다. 이 경우 고위험: **QID-32342:** *QID-3242 ##* (이름: 취약성 ID: 취약성 요약)입니다.

  주:
  간단한 설명 필드는 160자로 제한됩니다. 긴 취약성 요약은 잘립니다.

  이 규칙은 VI와 동일한 할당 그룹에 할당된 일치하는 미해결 정정 작업이 있는지 확인합니다.

  - 태스크가 발견되면 VI가 열림 상태의 기존 태스크에 추가됩니다.
  - 열림 상태의 작업을 찾을 수 없는 경우, 이 규칙은 높은 위험: **QID-32342** 작업을 생성하고 VI와 동일한 할당 그룹에 할당하며 VI를 정정 작업에 배치합니다.

다양한 종류의 취약성을 그룹화하기 위해 둘 이상의 정정 작업 규칙을 정의할 수 있습니다. 각 취약성은 정정 작업에 넣기 전에 정정 작업 규칙 조건과 비교되므로 규칙이 너무 많으면 성능에 영향을 줄 수 있습니다.

기본적으로 정정 작업 규칙은 항목을 그룹화할 때 취약한 항목에 대한 할당 규칙에 따라 설정된 할당 그룹을 사용하고 취약한 항목과 일치하도록 정정 작업을 할당합니다.

기본 작업 규칙의 일부로 이러한 정정 작업의 할당은 할당 규칙 모듈의 규칙에 의해 제어됩니다. 담당 규칙에 대한 자세한 내용은 다음 문서를 참조하십시오 취약성 대응 할당 규칙 개요.

작업 규칙이 삭제되면 양식 또는 목록 뷰에서 해당 규칙에 따라 생성된 모든 오픈 작업을 삭제할 수 있습니다. 오픈 상태가 아닌 작업은 제외됩니다.

정정 작업 규칙 다시 적용

정정 작업 규칙을 변경하려면 정정 작업 규칙 페이지의 다시 적용 버튼을 사용하여 해당 규칙에 의해 생성된 모든 활성 미결 정정 작업에서 변경된 규칙을 다시 실행합니다. 변경된 규칙에 따라 정정 작업을 자동으로 삭제하고 다시 생성합니다.

중요사항:
취약성 관리자와 분석가는 에서 선택한 취약한 항목에 대한 정정 작업 규칙을 평가할 수 있습니다 취약성 관리자 작업 공간. 이 방법은 시간이 오래 걸리는 프로세스인 클래식 UI에서 정정 작업 규칙을 다시 적용하는 것보다 더 효율적입니다. 자세한 내용은 에 있는 기록의 정정 속성 재평가 취약성 관리자 작업 공간 문서를 참조하십시오.

취약성 대응 정정 대상 규칙

SLA가 취약성 자체를 정정하기 위한 시간 범위를 제공하는 것과 마찬가지로 정정 대상 규칙은 VI(취약한 항목)를 정정하기 위한 예상 기간을 정의합니다. 예를 들어 자산에 PCI 데이터(신용 카드 데이터)가 포함된 경우 PCI DSS에 따라 해당 항목의 취약성을 30일 이내에 수정해야 합니다.

취약성 관리자는 다음을 정의하여 정정 대상 규칙을 생성할 수 있습니다.

- 정정 대상
- 미리 알림 대상
- 미리 알림 및 알림 수신자 — 취약한 항목(VI)이 미리 알림 또는 정정 목표 날짜가 지났고 정정되지 않은 경우 알림을 받을 사람입니다.

취약성 분석가와 관리자는 취약한 항목이 지연됨, 해결됨 또는 종결 됨 상태가 아닌 한 취약성 항목 양식 및 목록 뷰에서 정정 목표 날짜를 볼 수 있습니다. 정정 대상 규칙은 임포트 시 실행되고 VI가 다시 열리면 다시 실행됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

정정 목표 날짜는 다음과 같이 VI 목록 뷰에서 색상으로 구분됩니다.

- 알림 날짜가 되지 않은 취약한 항목은 녹색으로 표시됩니다.
- 정정 목표 날짜에 근접한 취약한 항목은 주황색으로 표시됩니다.
- 정정 목표 날짜가 지난 취약한 항목은 빨간색으로 표시됩니다.

하나 이상의 VI가 정정 목표 날짜에 가까워지거나 정정 목표 날짜가 지난 경우 정정 대상 규칙에 따라 요약 이메일이 전송됩니다.

정정 대상 규칙은 비활성화하거나 삭제할 수 있습니다.

규칙이 비활성화되면 규칙이 적용된 VI의 현재 정정 목표 날짜가 지워집니다. VI가 활성 규칙을 만족하면 해당 규칙이 적용되고, 그렇지 않으면 VI에 규칙 또는 대상 날짜가 없으며 해당 상태는 대상 없음입니다.

규칙이 삭제되면 종결, 연기 또는 해결된 VI의 정정 목표 날짜와 관련 필드가 유지됩니다. 종결되지 않은 VI의 정정 목표 날짜와 관련 필드가 지워지고 모든 종속 규칙이 다시 적용됩니다.

정정 대상 규칙 시나리오

동일한 취약한 항목에 여러 정정 대상 규칙이 적용되면 가장 제한적인 규칙이 적용됩니다.

주:
정정 목표는 마지막으로 개시 된 날짜와 일 수(24시간 단위로 측정)의 합계로 계산됩니다.

V17.1부터 정정 대상은 대상(날짜)부터 계산됩니다. 기본값은 마지막으로 열린 날짜로 유지됩니다.

예를 들어, 취약한 항목이 두 가지 정정 대상 규칙의 조건을 충족하는 경우:

시나리오: 취약한 항목이 2018년 3월 1일 10:00:00에 마지막으로 오픈되었습니다.

- 정정 대상 규칙 1: 2018년 3월 7일에 마지막으로 열림. 정정 목표는 마지막으로 오픈된 이후 15일입니다. 계산된 정정 목표 날짜는 03/16/2018 10:00:00입니다.
- 정정 대상 규칙 2: 2018년 3월 10일에 마지막으로 열림. 정정 목표는 마지막으로 오픈된 이후 10일입니다. 계산된 정정 목표 날짜는 03/11/2018 10:00:00입니다.

이 시나리오에서는 날짜가 더 제한적인 취약한 항목에 정정 대상 규칙 2가 적용됩니다. 취약한 항목이 처음 식별된 지 10일 대 15일

주:
정정 대상 규칙이 정의되면 예약된 작업에 따라 *Evaluate remediation targets* 정정 대상 날짜가 계산됩니다.

정정 대상 평가 예약된 작업 정보

Evaluate remediation targets 매일 4:00:00에 한 번 실행됩니다.

정정 목표 날짜가 가장 빠른 규칙부터 시작하여 모든 활성 취약성 규칙을 반복합니다. 다음과 같은 모든 취약한 항목을 살펴봅니다.

- 이 종결, 연기됨 또는 해결됨 상태가 아닙니다.
- 정정 대상 날짜가 없습니다.
- 정정 대상 날짜가 정정 대상 규칙의 날짜보다 나중이어야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Evaluate remediation targets 정정 목표 날짜가 없거나 규칙의 결과가 기록의 날짜보다 이른 경우 추가합니다. 기존 대상 날짜를 업데이트합니다. 마지막으로 취약한 항목 양식에서 정정 대상 및 정정 상태 필드를 업데이트합니다.

실행되면 *Evaluate remediation targets* 사용 가능한 알림이 전송됩니다.

Evaluate remediation targets VI의 정정 필드를 지우고 알림 전송을 중지합니다.

이 *sn_sec_cmn.evaluate_targetmissed_records* 속성을 활성화하면 예약된 작업이 누락된 VI를 *Remediation Target Rules* 평가할 수 없습니다. 이 속성은 기본적으로 사용하도록 설정됩니다.

정정 대상 규칙 다시 적용

정정 대상 규칙을 변경할 때 정정 대상 규칙 목록 페이지의 **Apply** Changes 버튼을 사용하여 **Closed**, **Deferred** 또는 **Resolved** 상태를 제외한 모든 활성 VI에서 변경된 모든 규칙을 다시 실행합니다. 보유한 VI 수에 따라 시간이 걸릴 수 있습니다.

주:

예약된 작업이 실행 중인 *Evaluate remediation targets* 경우 다시 적용 프로세스를 시작할 수 없습니다. 그러나 재적용 프로세스가 이미 실행 중이고 이 프로세스가 트리거한 예약된 작업은 병렬로 실행됩니다.

의 재적용 프로세스는 취약성 대응 독립적 애플리케이션 취약성 대응 이며 병렬로 실행할 수 있습니다.

중요사항:
취약성 관리자와 분석가는 다음에서 선택한 취약한 항목에 대한 최신 정정 목표 날짜를 얻을 수 있습니다 취약성 관리자 작업 공간. 이 방법은 시간이 오래 걸리는 프로세스인, UI의 클래식 모든 취약한 항목에 대해 정정 대상 규칙을 실행하는 것보다 더 효율적입니다. 자세한 내용은 에 있는 기록의 정정 속성 재평가 취약성 관리자 작업 공간 문서를 참조하십시오.

관련 정보

정정 대상 규칙 생성 또는 편집 취약성 대응

취약한 항목의 정정 대상 상태 취약성 대응 보기

정정 대상 알림 만들기 또는 편집

취약성 분류 그룹 및 규칙

분류 그룹은 그룹에 정의된 분류 규칙에 따라 테이블 값의 분류를 자동화합니다. 각 규칙의 조건은 순서대로 평가되며 첫 번째로 일치하는 규칙이 사용됩니다.

Vulnerability Response 기본 시스템에는 검색된 항목과 취약성을 각각 분류하는 다음과 같은 두 개의 분류 그룹이 포함됩니다.

- 검색된 항목 분류
- 취약성 항목 분류

취약성 및 검색된 항목을 임포트할 때마다 해당 그룹의 취약성 분류 규칙이 실행됩니다. 규칙에 설정된 조건에 따라 기록은 관련 분류 그룹으로 분류됩니다. 이러한 규칙을 생성, 편집 또는 삭제하거나 기존 취약성에 다시 적용할 수 있습니다.

주:

- 선택한 테이블의 경우 활성 분류 그룹이 하나만 있을 수 있습니다.
- 그룹을 생성한 후에는 삭제할 수 없습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

자세한 내용은 분류 규칙 생성 및 편집, 기존 취약성에 규칙 적용, 분류 규칙 비활성화 또는 삭제 문서를 참조하십시오.

용 머신 러닝 솔루션 취약성 대응

취약점 할당 권장 는 및 머신 러닝을 사용하여 ServiceNow# 예측 인텔리전스 취약한 항목(VI) 및 정정 작업(VUL 또는 RT)에 대한 할당 그룹을 권장합니다. 할당되지 않았거나 잘못 할당된 취약성 결과의 소유자를 식별하는 데 소요되는 시간을 줄일 수 있습니다. 또한 권장 할당 그룹이 취약성을 해결하는 데 적합한지 평가하는 시스템 생성 신뢰도 점수를 볼 수 있습니다.

이러한 예측 인텔리전스 역량은 기존 데이터를 기반으로 할당 그룹을 예측할 수 있는 솔루션 정의 모델을 만들고 교육하여 더 나은 작업 경험을 제공하는 데 사용됩니다 취약성 대응 .

자세한 내용은 예측 인텔리전스 를 참조하십시오.

취약점 할당 권장

시스템에서는 애플리케이션(com.snc.vulnerability.recom)취약성 대응ServiceNow 예측 인텔리전스을 취약점 할당 권장 사용하여 . 이 플러그인에는 다음이 필요합니다.

- 취약성 대응 (com.snc.vulnerability)
- 예측 인텔리전스 (com.glide.platform_ml)

자세한 내용은 예측 인텔리전스 를 참조하십시오.

신뢰 점수

취약점 할당 권장 애플리케이션을 사용하여 선택한 RT 또는 VI에 대해 권장되는 할당 그룹의 신뢰 수준을 보고하는 신뢰 점수를 생성합니다. 신뢰 점수는 권장 할당 그룹이 취약성을 해결하는 데 적합하다고 시스템에서 확신하는지 여부를 평가합니다. 최대 10개의 권장 사항이 나타납니다. 이러한 권장 사항은 할당 성공률이 가장 높은 것을 기반으로 합니다. 목록의 첫 번째 권장 사항은 시스템이 올바른 할당 그룹이라는 확신도가 가장 높다는 것을 의미합니다.

예를 들어, 0-100의 척도에서 각 할당 그룹에 대한 신뢰 점수는 해당 특정 그룹에 속하는 VI 또는 RT의 확률을 나타냅니다.

관련 정보

예측 인텔리전스

분류 솔루션 생성 및 교육

유사성 솔루션 생성 및 교육

클러스터링 솔루션 만들기 및 교육

ML 솔루션에 대한 고급 설정 구성

외부 공급업체 취약성 통합에서 취약성 대응 구성 항목을 식별하기 위한 **CI** 조회 규칙

외부 공급업체 통합에서 데이터를 임포트하면 에서 취약성 대응 일치하는 항목을 구성 관리 데이터베이스(CMDB)찾기 위해 자동으로 호스트 데이터를 사용합니다. 이는 **CI** 조회 규칙을 사용합니다. 이러한 규칙은 CI(구성 항목)를 식별하고 정정에 도움이 되도록 취약한 항목 기록에 추가하는 데 사용됩니다.

버전 19.0부터 보안 운영 〉 **CMDB** 〉 조회 규칙 을 클릭하여 인스턴스에서 목록을 찾습니다.

자산을 임포트할 때 검색된 항목 목록에서 먼저 외부 공급업체 ID를 사용하여 조회가 수행되어 이전 임포트의 구성 항목(CI)과 일치하는 항목을 찾습니다. 호스트 ID 일치가 발견되면 취약한 항목 기록의 구성 항목 필드로 사용됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

검색된 항목 목록을 사용하여 임포트한 자산이 CI에 매핑되는 방식을 볼 수 있습니다. 일치하는 항목이 없거나 호스트 ID 필드가 비어 있는 경우 규칙은 다른 호스트 정보를 사용하여 CI를 올바르게 식별하려고 시도합니다. 그래도 일치하는 항목이 없으면 자리 표시자 CI가 만들어지고 일치하지 않는 **CI**로 지정됩니다. 이러한 CI가 처리되는 방식에 대한 자세한 내용은 을 참조하십시오 일치하지 않는 CI .

CI 조회 규칙은 도메인으로 분리될 수 있으며 소스에 따라 다릅니다. 각 소스에는 여러 배포가 있을 수 있습니다.

주:
CI 조회 규칙은 취약성 소스 통합의 모든 배포에서 공유됩니다. 규칙이 삭제되거나 수정되면 삭제 또는 변경이 취약성 통합의 모든 배포에 영향을 줍니다.

일치를 시도할 때 첫 번째 단계는 벤더 ID를 조회하여 소스, source_instance 및 벤더 ID 간에 정확히 일치하는 항목을 찾습니다. 그런 다음, 조회 규칙이 가장 낮은 규칙에서 가장 높은 순서로 실행되고 규칙이 일치하는 CI를 하나만 반환하면 중지됩니다. 둘 이상의 CI를 반환하는 방식으로 규칙이 생성되면 첫 번째 일치 항목만 사용됩니다.

주:
낮은 수준의 네트워킹 요소에서 일치하지 않도록 하기 위해 일치하는 CI가 dscy_switchport, cmdb_ci_network_adapter, cmdb_ci_nic 또는 cmdb_ci_ip_address 중 하나이면 상위 CI가 반환됩니다.

CI 클래스를 제외하는 시스템 속성을 사용할 수 있습니다. 이 속성은 업그레이드에 사용할 수 없습니다. 속성 설정에 대한 업그레이드 정보 및 지침을 참조하십시오 CI 클래스 무시 .

일치하는 문제를 쉽게 찾을 수 있도록 일치하는 항목을 찾으면 이를 찾는 데 사용되는 CI 조회 규칙이 **CI** 일치 규칙 필드의 검색된 항목 기록에 추가됩니다. 조회 규칙은 가장 낮은 순서 값으로 먼저 평가됩니다.

CI 조회 규칙은 해당 통합 플러그인과 함께 제공됩니다.

CI 조회 규칙의 일부는 다음과 같습니다.Qualys

- QUALYS 호스트 ID
- FQDN
- NetBIOS
- DNS
- IP

CI 조회 규칙의 일부는 다음과 같습니다.Rapid7

- MacAddress
- FQDN
- 호스트 이름
- IP

Tenable.io CI 조회 규칙의 일부는 다음과 같습니다.

- FQDN
- NETBIOS
- 호스트 이름

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- MacAddress
- DNS

주:
Tenable.io CI 조회 규칙은 검색된 항목의 일반 FDQN, IPV4 및 MacAddress 값보다 비어 있지 않은 네트워크 인터페이스 값(FDQN, IPV4 및 MacAddress)의 우선순위를 정하고 채웁니다. 이러한 네트워크 인터페이스 값이 비어 있으면 검색된 항목에 대해 일반 FDQN, IPV4 및 MacAddress 값이 채워집니다.

Tenable.sc CI 조회 규칙의 일부는 다음과 같습니다.

- MacAddress
- FQDN
- NETBIOS

주:
제거된 규칙은 복구할 수 없습니다. 기존 규칙을 제거하는 대신 새 규칙을 만들 때 비활성화하십시오.

취약성 데이터를 임포트하면 인스턴스에 부담이 가중될 수 있으며 규칙을 신중하게 구성하지 않으면 자원에 성능 문제가 발생할 수 있습니다. 반복을 수행하고 일치를 수행하는 데 사용되는 논리로 CMDB 인해 처리 시간이 길어질 수 있습니다. 자원의 잠재적 저하나 성능 저하를 방지하려면 사용자 지정 작성된 CI 조회 규칙을 테스트하거나 사전 정의된 **CI** 조회 규칙을 수정하십시오. 고아 기록 중복 방지, 데이터 삭제 및 데이터 정리에 대한 자세한 내용은 을 참조하십시오 CI 조회 규칙을 실행 취약성 대응 한 후 중복 또는 고아 기록을 방지하는 데 도움이 되는 단계 .

주:
CI 일치에 대한 자세한 내용은 KB0998706 문서를 참조하십시오.

업데이트된 **CI** 조회 규칙 다시 적용

CI 조회 규칙을 변경할 때 CI 조회 규칙 목록 페이지에서 변경 내용 적용을 클릭하여 검색된 항목에 대해 다음과 같은 모든 규칙을 다시 실행합니다.

- 업데이트된 규칙과 일치함
- 어떤 규칙과도 일치하지 않습니다.

조회 규칙을 다시 적용한 후 CI(구성 항목)가 변경되면 검색된 항목이 새 CI로 업데이트됩니다. 영향을 받는 탐지 및 취약한 항목도 업데이트됩니다. 자세한 내용은 선택한 검색 항목에 CI 조회 규칙 다시 적용을 참조하십시오.

분류되지 않은 하드웨어

자산이 CI 조회 규칙별 일치 항목에서 구성 관리 데이터베이스(CMDB) 일치하는 항목을 찾지 못하는 경우 해당 자산을 분류되지 않은 하드웨어라고 합니다.

구축된 통합에서 ServiceNow 데이터를 임포트하면 에서 취약성 대응 자동으로 호스트 데이터를 CMDB사용하여 . CI 조회 규칙은 구성 항목(CI)을 식별하고 정정에 도움이 되도록 취약한 항목 기록에 추가하는 데 사용됩니다. 에서 CMDB자산을 찾을 수 없는 경우 IRE(식별 및 조정 엔진)는 하드웨어 클래스와 모든 하위 항목에 정의된 자체 식별 규칙을 실행하고 분류되지 않은 하드웨어 클래스 아래에 CI를 만듭니다. 디스커버리 이 자산을 찾으면 분류되지 않은 기존 하드웨어를 재분류하는 대신 CI를 생성합니다. 이는 식별 규칙이 하드웨어 CI의 이름을 사용하기 때문입니다.

IRE(식별 및 조정 엔진)가 활성화되면 검색된 항목의 재분류 옵션은 지원되지 않습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음 추출은 각각 및 를 디스커버리 통해 취약성 대응 분류되지 않은 하드웨어에서 CI를 생성하기 위한 IRE 페이로드를 보여줍니다.

```
"className": "cmdb_ci_unclassed_hardware",

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

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

```
"className": "cmdb_ci_cmdb_ci_win_server"

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

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

이 경우 분류되지 않은 기존 하드웨어 CI는 Windows 서버로 재분류되지 않고 대신 Windows 서버 아래에 새 CI가 생성됩니다. 그 이유는 식별 규칙이 하드웨어 CI의 이름에 따라 달라지기 때문입니다. 페이로드를 발견하면 페이로드 취약성 대응 의 이름은 FQDN/NETBIOS와 동일하지만 의 페이로드 디스커버리에 대한 호스트 이름일 뿐입니다.

관련 정보

분류되지 않은 하드웨어 재분류

일치하지 않는 CI

구성 항목(CI)은 임포트될 때 CI 구성 관리 데이터베이스(CMDB) 와 자동으로 일치합니다. 기본적으로 보안 운영 〉 **CMDB** 〉 검색된 항목 모듈에는 일치 항목이 없는 구성 항목이 나열됩니다.

일치하지 않는 CI가 CMDB의 기존 클래스에 속한다고 생각되면 CI 조회 규칙을 검토하십시오. 그렇지 않으면 구성 항목을 재분류하는 것이 좋습니다.

주:
이 목록의 기본 필터는 일치하지 않음으로 설정됩니다. 필터를 제거하여 임포트에서 검색된 모든 항목을 볼 수 있습니다.

IRE(식별 및 조정 엔진)가 활성화되면 검색된 항목의 재분류 옵션은 지원되지 않습니다.

관련 정보

일치하지 않는 구성 항목 보기 및 재분류

불일치하는 검색 항목을 일치시키기

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

CI 조회 규칙을 실행 취약성 대응 한 후 중복 또는 고아 기록을 방지하는 데 도움이 되는 단계

기존 구성 항목 중복 제거

식별 및 조정 엔진을 사용하기 위한 취약성 대응 **CI** 생성

IRE(식별 및 조정 엔진) API를 사용하여 CI 구성 관리 데이터베이스(CMDB) (구성 항목)를 생성할 수 있습니다. IRE API를 사용하여 CI를 생성하면 중복 CI가 생성되는 것을 방지할 수 있으며 신뢰할 수 있는 데이터 소스만 에 쓸 CMDB수 있도록 하여 CI 속성을 조정할 수 있습니다.

CI 클래스(테이블)는 인스턴스 데이터베이스의 원래 테이블 이름입니다. CMDB 에는 CI에 대한 데이터를 저장하는 기본 시스템 클래스가 포함되어 있습니다.

CI 생성에 **IRE** 사용

취약성 대응 v12.2 이전에는 검색된 항목 목록 또는 CMDB에서 일치하는 CI를 찾을 수 없는 경우 일치하지 않는 CI 클래스(sn_sec_cmn_unmatched_ci)에 CI가 생성됩니다. 자세한 내용은 일치하지 않는 CI를 참조하십시오.

의 취약성 대응v24.0.6부터 IRE에서 CI 생성을 방해하는 예외가 발생하면 이러한 예외의 세부 사항이 추가 정보 필드에 기록됩니다. 이 필드의 상세 정보를 검토하여 근본 원인을 확인하고 필요한 수정을 수행하여 CI가 성공적으로 생성되도록 할 수 있습니다.

취약성 대응 v12.2에서 v18.0까지, CI 조회 규칙이 적용될 때 일치하는 항목이 없으면 자산 정보가 IRE로 전송되고 `#### ## ####` 및 `#### IP ## ##` 클래스 중 하나에 CI가 생성됩니다. v18.0부터 취약성 대응 새로운 클래스인 `Cloud Resource` 도 포함됩니다. 일치하지 않는 클라우드 자원의 분류를 기본 CI 클래스로 구성하는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 일치하지 않는 클라우드 자산에 대한 CI 클래스 업데이트 중.

CMDB CI 클래스

주:
새 클래스를 사용하려면 CI Class Models 플러그인을 활성화하십시오 CMDB . 그렇지 않으면 CI가 Unmatched CI 클래스에 생성됩니다.

외부 공급업체 스캐너에서 임포트한 호스트를 검색된 항목 목록에서 CMDB찾을 수 없거나 다음과 같은 새 CMDB CI 클래스 중 하나로 생성됩니다.

CMDB CI 클래스

CMDB **CI** 클래스	설명
불완전한 IP 식별 장치 (`cmdb_ci_incomplete_ip`)	스캐너에서 받은 호스트 정보에서 IP 주소만 사용할 수 있는 경우 이 테이블에 CI가 생성됩니다.
분류되지 않은 하드웨어 (`cmdb_ci_unclassed_hardware`)	스캐너에서 받은 호스트 정보에서 다음 정보를 사용할 수 있는 경우 이 테이블에 CI가 생성됩니다. • 호스트 이름 • IP 주소 • DNS • NETBIOS • MAC 주소

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

CMDB CI 클래스

CMDB **CI** 클래스	설명
	주: MAC 주소를 사용할 수 있으면 네트워크 어댑터 항목이 생성되고 분류되지 않은 하드웨어 CI와 연관됩니다. IP 주소와 MAC 주소를 모두 사용할 수 있는 경우 IP 주소 CI도 생성되고 분류되지 않은 하드웨어 CI와 연결됩니다.
클라우드 자원(*cmdb_ci_cmp_resource*)	스캐너에서 받은 호스트 정보에서 사용할 수 있는 경우 *Cloud Resource ID* 이 테이블에 CI가 생성됩니다. 주: 스캐너 통합의 자산 유형이 ####드이고 *sn_sec_cmn.unmatched_cloud_resource_enabled* 시스템 속성이 false인 경우 CI는 #### ## 클래스가 아닌 #### ## #### 클래스에서 생성됩니다.

IRE(식별 및 조정 엔진)가 활성화되면 검색된 항목의 재분류 옵션은 지원되지 않습니다.

다음 중 하나가 발생할 경우 시스템에서 자동으로 일치하지 않는 CI 클래스를 사용합니다.

- CI 클래스 플러그인이 CMDB 활성화되지 않았습니다.
- IRE는 CI를 생성하는 동안 예외를 발생시킵니다.

자세한 내용은 일치하지 않는 CI를 참조하십시오.

관련 정보

CMDB CI Class Models 스토어 앱

IRE(식별 및 조정 엔진)

일치하지 않는 클라우드 자산에 대한 **CI** 클래스 업데이트 중

v20.0부터 취약성 대응 는 시스템 속성을 사용하여 *sn_sec_cmn.unmatched_cloud_resource_enabled* , Rapid7 및 Tenable 스캐너의 Qualys일치하지 않는 #### ### #### ## ####로 분류할 수 있습니다.

False가 기본값인 이 시스템 속성은 기본 시스템과 함께 제공됩니다. 이는 인프라 및 클라우드 자산을 모두 가져오는 통합에 대해 일치하지 않는 #### ### #### ## #### ()*cmdb_ci_unclassed_hardware* 또는 #### ## ()*cmdb_ci_cmp_resource* 클래스로 분류합니다.

취약성 대응 v20.0부터 인프라 및 클라우드 자산을 모두 지원하는 통합을 식별하기 위해 자산 유형 열이 sn_sec_int_integration(외부 공급업체 통합) 테이블에 추가됩니다. 자산 유형 열에는 인프라 및 클라우드 자산을 모두 가져오는 스캐너에 대한 하이 ### 값이 있습니다. 예를 들어, Qualys, Rapid7 및 Tenable 통합은 자산 유형 열에서 하이 #### 값을 가집니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- v20.0 이상을 새로 설치하는 취약성 대응 경우 일치하지 않는 모든 클라우드 자산은 다음과 같이 분류됩니다.
  - 기본적으로 `#### ## ####` 클래스입니다.
  - `Cloud Resources` 클래스(시스템 속성을 true로 변경하는 `sn_sec_cmn.unmatched_cloud_resource_enabled` 경우)
- v20.0으로 취약성 대응 업그레이드하는 경우:
  - `#### ##` 클래스에 자산이 있는 경우 일치하지 않는 클라우드 자산이 `#### ##` ()`cmdb_ci_cmp_resource` 클래스에 계속 추가되도록 `sn_sec_cmn.unmatched_cloud_resource_enabled` 시스템 속성이 true로 설정됩니다.
  - 그렇지 않으면 일치하지 않는 클라우드 자산이 `#### ## ####` 클래스로 분류되도록 `sn_sec_cmn.unmatched_cloud_resource_enabled` 시스템 속성이 false로 설정됩니다.

주:
시스템 속성의 값을 `sn_sec_cmn.unmatched_cloud_resource_enabled` 수정하는 경우 이전에 대상으로 지정된 CI 클래스에서 일치하지 않는 구성 항목을 삭제하고 조회 규칙을 다시 적용해야 합니다. 새 CI가 올바른 클래스에 생성되도록 기존 CI를 삭제하고 CI 조회 규칙을 다시 적용하는 방법에 대한 자세한 내용은 KB1533376 문서를 참조하십시오.

검색된 항목

자산은 **CI** 조회 규칙을 사용하여 임포트될 때 CI구성 관리 데이터베이스(CMDB)(구성 항목)와 자동으로 일치합니다. 검색된 항목을 통해 자산 식별이 의 CI에 매핑되는 방식을 볼 수 있습니다 CMDB.

검색된 항목은 일치,일치하지 않음 또는 재분류된 것으로 간주됩니다. 식별된 CI가 일치함 상태입니다.

잠재적인 일치 문제를 쉽게 찾을 수 있도록 CI와 일치하는 CI 조회 규칙이 **CI** 일치 규칙 필드에 나타납니다.

기본적으로 보안 운영 〉 **CMDB** 〉 검색된 항목 모듈에는 일치하지 않는 구성 항목이 나열됩니다. 필터를 제거하여 임포트에서 검색된 모든 항목을 볼 수 있습니다.

검색된 항목의 필드에 대한 설명은 다음 문서를 참조하십시오 검색된 항목 양식 필드. 일치하지 않는 검색된 항목을 조정하고 선택한 검색된 항목에 CI 조회 규칙을 다시 적용하는 방법에 대한 자세한 내용은 각각 문서를 선택한 검색 항목에 CI 조회 규칙 재적용 참조하십시오불일치하는 검색 항목을 일치시키기.

검색된 항목에 대한 **CI** 변경 내용

검색된 항목(DI)의 CI(구성 항목)가 변경되면 영향을 받는 탐지 및 VI(취약한 항목)가 업데이트됩니다. 위험 점수, 담당 규칙, 그룹 규칙 및 정정 대상 규칙이 다시 평가됩니다.

v24.0.6 부터 취약성 대응검색된 항목 테이블에서 CI에 대한 업데이트를 볼 수 있습니다. 이전 CI, 업데이트된 CI 및 변경한 사용자를 포함한 정보는 감사 이력 관련 목록에 문서화됩니다.

취약성 및 CI가 동일한 VI가 있는 경우 탐지는 기존 VI로 업데이트되고 현재 VI는 ## ### invalidCI인 상태로 종결됩니다. 다음과 같은 이유로 작업 메모가 추가됩니다.

- 탐지가 한 VI에서 다른 VI로 이동할 때
- 중복 VI가 닫힌 경우.

기존 VI에 대한 CI를 업데이트하지 않으려면 ## sn_sec_cmn.update_on_ci_change 를 false로 설정하십시오. 그런 다음 CI가 변경되면 새 VI가 생성되고 기존 VI# ### CI로 닫힙니다.

sn_sec_cmn.update_on_ci_change의 기본값은 true입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

검색된 항목 재평가

검색된 항목에 대한 새 데이터가 수신될 때 검색된 항목은 즉시 다시 평가되지 않습니다. 새 데이터를 `reevaluate_ci` 받으면 이 옵션은 기본적으로 설정됩니다 `true` .

예약된 작업은 `Re-apply CI Lookup Rules on the Changed Discovered items` 스캐너에 의해 소스 데이터가 변경되고 있는 검색된 모든 항목을 평가합니다. 검색된 항목을 다시 처리하고 소스 데이터가 변경된 검색된 항목과 관련된 취약한 항목을 업데이트합니다. 이 예약된 작업의 값은 기본값입니다 `On Demand` .

주:
이 예약된 작업을 매일 실행하도록 선택할 수도 있습니다. 이 작업을 시작하는 방법, 작업 빈도 및 처리하는 기록 수를 보는 방법에 대한 자세한 내용은 KB1695110 취약성 대응: 변경된 검색 항목에 CI 조회 규칙 다시 적용 문서를 참조하십시오.

취약성 대응 정정 작업 및 취약한 항목 상태

취약성 대응 애플리케이션에서 상태 모델을 사용하여 언제든지 정정 작업의 상태를 볼 수 있습니다. 각 상태가 서로 어떻게 관련되고 영향을 미치는지 알면 취약한 항목(VI)을 정정하는 시기와 방법을 결정하는 데 도움이 됩니다.

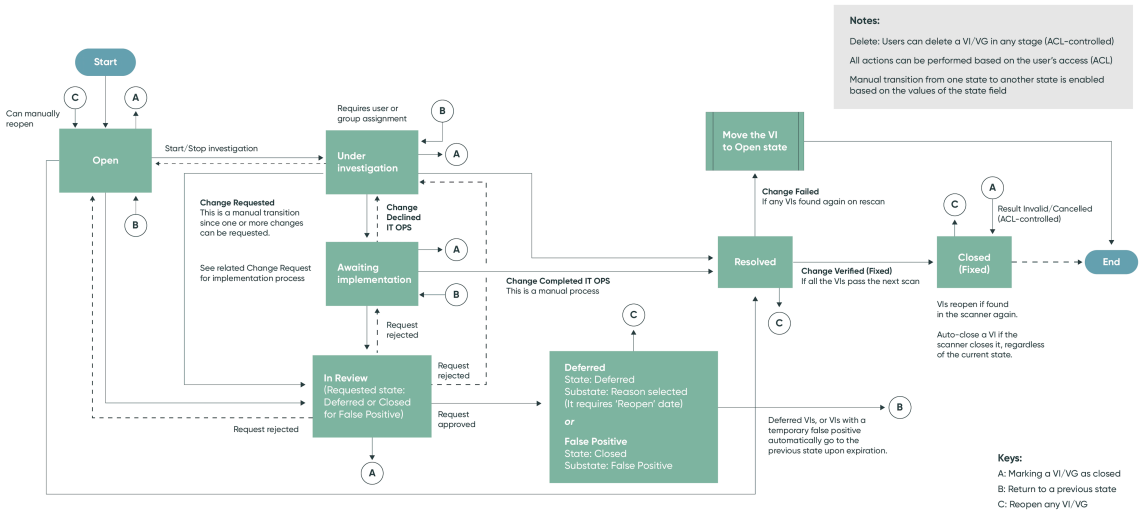
정정 작업 상태

복잡한 사용 사례로 인해 취약한 항목이 정정 작업과 다른 상태가 되는 경우가 있습니다. 상태의 작동 방식을 이해하면 이 동작을 설명하는 데 도움이 되며, 정정 작업 생성 및 정정 작업 규칙 생성 또는 편집에 도움이 됩니다.

주:
의 취약성 대응v23.0부터 취약한 항목 상태 승인 워크플로우는 더 이상 사용되지 않으며 플로우 디자이너의 플로우 취약성 상태 승인 변경으로 대체됩니다.

정정 작업에는 다음 다이어그램과 같이 여러 가지 가능한 상태가 있습니다.

취약성 대응 상태 플로우



주:
각 작업 양식에는 작업의 표준 ServiceNow 인 팔로우 및 업데이트 버튼이 있습니다.

정정 작업 상태 및 각 상태에서 수행할 수 있는 작업에 대한 자세한 내용은 다음 문서를 참조하십시오 취약성 대응 정정 작업 상태.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

탐지, 정정 작업 및 취약한 항목 상태에 대한 자세한 내용은 다음 문서를 참조하십시오 탐지, 정정 작업 및 취약한 항목 상태.

정정 작업 및 VI 상태에 대한 자세한 내용은 문서를 정정 작업 및 취약한 항목 상태참조하십시오.

여러 그룹의 VI에 대한 정정 작업 상태에 대한 자세한 내용은 문서를 참조하십시오 여러 그룹의 취약한 항목(VIT)에 대한 정정 작업 상태.

취약한 항목 기간 계산 및 표시

VI(취약한 항목)의 기간이 애플리케이션에 더 자세히 표시됩니다 취약성 대응 .

VI(취약한 항목) 기간은 취약한 항목 목록 뷰의 기간 열과 VI(VIT) 기록의 기간 및 기간 종결 필드에 일/시간/분 형식으로 표시됩니다. 나이를 더 큰 유효 숫자로 표시하면 다음 활동을 보다 정확하게 수행하는 데 도움이 될 수 있습니다.

- 자동 삭제 규칙 모듈에서 일/시간/분 단위로 특정 VI 기록을 대상으로 지정하고 삭제하도록 규칙을 구성합니다. 더 정확하게 기록을 제거하면 특히 인스턴스에 많은 수의 VI 기록이 있는 경우 성능이 향상될 수 있습니다.
- 애플리케이션에 대한 취약성 대응 퍼포먼스 분석에서 보다 구체적인 상세 정보가 포함된 보고서를 봅니다.
- 원하는 VI만 식별하는 필터를 생성합니다.
- 목록 뷰를 정리하여 원하는 VI만 표시합니다.
- 더 쉽게 닷워킹을 할 수 있습니다.

예약된 작업으로 기간을 계산하고 모든 활성 VI를 업데이트했습니다. VI 기록이 많은 인스턴스에서는 이 프로세스가 느려지고 성능에 부정적인 영향을 미칠 수 있습니다. VI 연령은 요청 시 더 효율적으로 계산되고 향상된 연령 열을 통해 더 많은 유효 숫자로 표시됩니다. 애플리케이션을 설치하거나 업그레이드할 취약성 대응 때 향상된 연령 열이 자동으로 추가됩니다.

> **주:**
> 업그레이드를 수행할 때 VI 기간이 취약한 항목 목록 뷰와 활성 VI(VIT) 기록의 기간 및 종결 기간 필드에 일/시간/분(9일, 18시간, 29분) 형식으로 표시되지 않으면 인스턴스의 기간 열이 현재 상태가 아닙니다. 업그레이드 후 이 문제를 해결하는 방법에 대한 자세한 내용은 KB0749231 참조하십시오.

연령 열과 필드는 편집할 수 없습니다. sn_vul.vulnerability_read 권한이 있는 취약성 관리자 또는 취약성 관리자 가상 사용자는 이 값을 볼 수 있으며 sn_vul.remediation_owner 역할을 가진 IT 정정 소유자는 자신에게 할당된 기록에서 이 값을 볼 수 있습니다.

가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

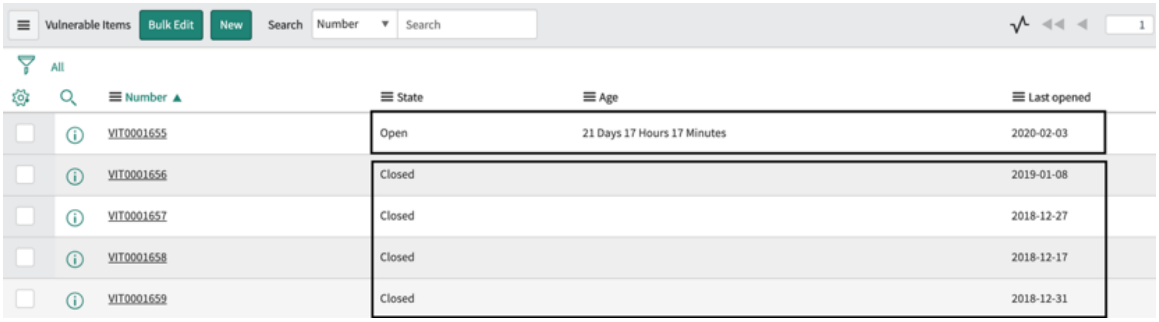
VI 연령은 다음 이미지와 같이 표시됩니다.

취약한 항목 목록

다음 그림과 같이 취약한 항목 목록 뷰에서 활성 VI에 대해서만 기간이 일/시간/분(21일 17시간 17분) 단위로 기간 열에 표시됩니다. 활성 VI는 '종결' 이외의 모든 상태에 있는 VI입니다. 이 기간 값은 VI가 활성화된 일 수를 나타냅니다.

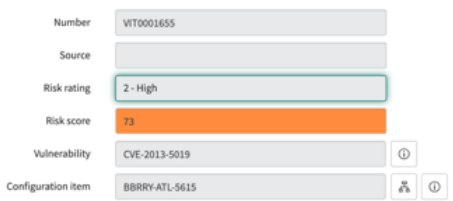
'종결' 상태의 VI에 대해서는 연령이 표시되지 않습니다. 이전에 'Closed' 상태였다가 다시 열린 VI의 경우, 이 값은 VI가 마지막으로 열린 날짜 이후 활성화된 일 수를 나타냅니다.

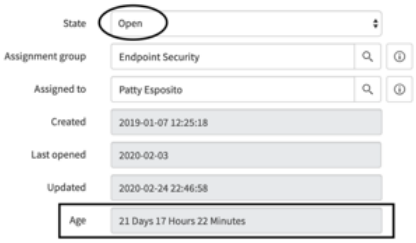
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



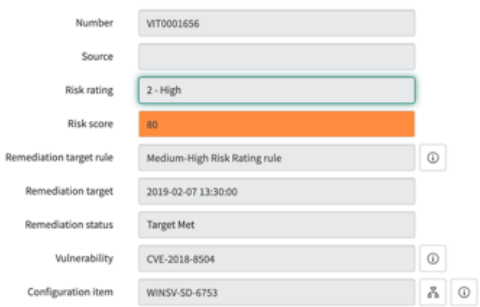
VI 기록의 기간

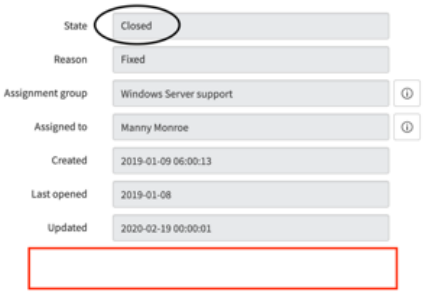
VI 기록에서 목록 뷰의 연령 열 값은 연령 필드의 활성 VI에 대해 표시됩니다.





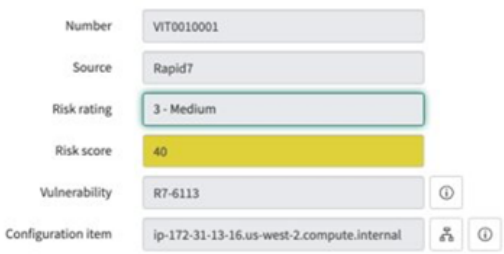
"종결" 상태의 VI 기록에 대해서는 연령 열의 값이 표시되지 않습니다.

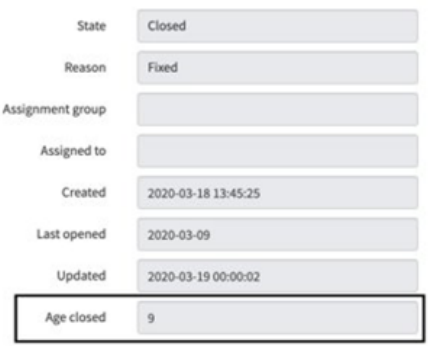




VI가 업데이트될 때 취약한 항목 목록 및 VI 기록의 기간

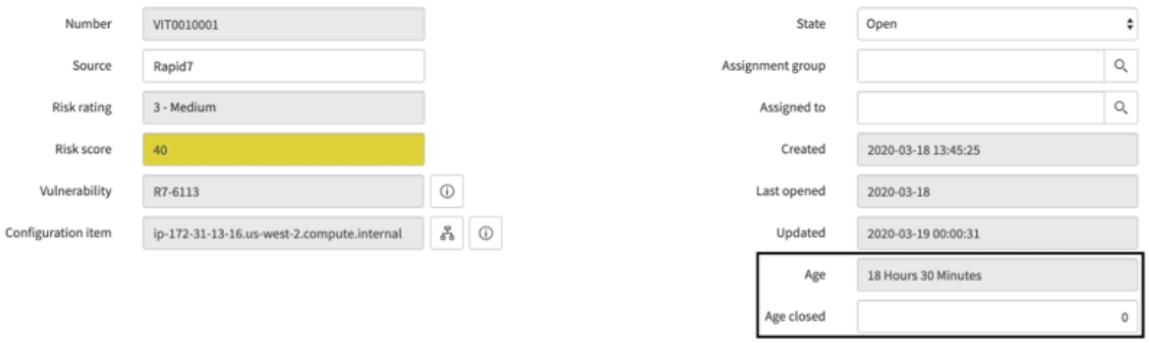
VI가 '종결' 상태인 경우 Age 필드가 표시되지 않습니다. VI가 'Closed'로 전환되면 다음 그림과 같이 Age 열의 날짜 수 값이 Aged closed 필드(9)에 표시됩니다. 이 값은 VI가 "종결"로 전환되기 전에 활성 상태였던 일 수를 나타냅니다. 예를 들어, 다음 이미지에서 이 VI는 9일 18시간 29분 동안 활성 상태였지만 종결된 기록에는 일수(9)만 표시됩니다.





© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 VI가 다시 열리면 VI 상태가 다시 '오픈'으로 전환될 때 종결 연령 필드가 0으로 재설정됩니다. VI가 다시 활성화되기 때문에 기간(일/시간/분)이 기간 열의 목록 뷰와 VIT의 기간 필드에 표시됩니다.



Age 및 Age closed 계산을 사용자 지정하는 방법에 대한 자세한 내용은 KB1703270 문서를 참조하십시오.

취약한 항목 및 정정 작업에서 할당 제거

사용자 또는 그룹에 잘못 할당되었을 수 있다고 판단되는 취약한 항목 및 정정 작업 기록에서 취약한 항목의 할당 대상 및 할당 그룹 필드를 직접 지울 수 있습니다.

워크플로우 개요

정정 소유자와 취약성 분석가는 할당 대상 및 할당 그룹 필드를 지우고 할당 해제 UI 작업으로 재할당을 위해 기록을 업데이트할 수 있습니다.

사용 케이스

기록이 정정 범위 내에 있지 않다고 판단되거나 기록이 사용자 또는 그룹에 잘못 할당되었다고 생각되는 경우 취약한 항목 및 정정 작업 기록의 할당 대상 및 할당 그룹 필드에서 자신 또는 그룹을 제거할 수 있습니다.

할당 해제 UI 작업 및 기타 옵션 메뉴

UI 작업을 사용하거나 추가 옵션 메뉴( )에서 종결 또는 해결됨 이외의 상태에서 다음 기록의 할당을 해제할 수 있습니다.

- 클래식 환경과 작업 공간 모두에서 정정 작업(VUL, AVUL, CVUL)을 수행합니다.

  이 기능으로 정정 작업이 업데이트되면 동일한 할당 그룹이 있는 연결된 모든 VIT의 할당 대상 및 할당 그룹 필드도 지워집니다.

  주:
  정정 작업의 VIT, AVIT 또는 CVIT에 정정 작업과 다른 할당 그룹이 있는 경우 할당되지 않은 것은 아닙니다. 대부분의 경우 이러한 취약한 항목은 수동으로 할당되었습니다.

- 클래식 환경 및 작업 공간의 취약한 항목(VIT, AVIT 및 CVIT).

UI 작업을 사용하여 할당을 업데이트하거나 수동으로 할당한 기록은 해당 제품 모듈 아래의 할당되지 않음 모듈에 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

UI 작업을 사용하여 기록에서 할당 대상 및 할당 그룹 필드를 지우는 *Unassigned* 단계는 자세한 내용을 참조하십시오 취약한 항목 및 정정 작업에서 할당 제거 .

시스템 속성 및 알림

기록에서 할당 해제 를 선택하면 기본적으로 *sn_vul.unassign_vr.approval_required* AND 시스템 속성이 승인 플로우를 트리거하고 검토 상태에서 상태 변경 승인 기록을 생성하며, 승인자에 대한 승인 요청이 발생하여 내 승인 목록에 표시됩니다.

주:
취약성 관리자(sn_vul.vulnerability_admin)는 *sn_vul.unassign_vr.approval_required* 시스템 속성을 **false** 로 설정하여 승인 프로세스를 비활성화할 수 있습니다.

- 요청이 승인 *sn_vul.default_assignment_group* 되면 할당 대상 및 할당 그룹 필드를 지우고 할당 유형 필드를 미할당으로 채웁니다. 취약성 관리자는 할당 필드를 지우고 특정 그룹을 할당하도록 시스템 속성의 값을 *sn_vul.default_assignment_group* 변경할 수 있습니다. 예를 들어 사용자가 기록에서 할당 해제 를 클릭하고 검토를 위해 특정 그룹으로 리디렉션하려는 경우 시스템 속성의 값 필드에서 선택한 그룹의 시스템 ID를 추가할 수 있습니다.

  주:
  이 값을 변경하면 할당되지 않은 모든 VIT, AVIT 및 CVIT 에 대한 알림이 지정한 그룹으로 전송됩니다.

- 요청이 거부되면 메모 탭에 이유가 표시됩니다.

또는 특정 그룹에 대해 구성되지 않은 경우 *sn_vul.default_assignment_group* 기본적으로 할당되지 않은 알림 사용자 그룹에 추가한 사용자는 기록이 할당되지 않을 때 경보를 받습니다. *sn_vul.default_assignment_group* 시스템 속성은 이 그룹에 대한 알림을 결정합니다.

할당 유형(수동, 규칙 또는 미할당)은 VIT 기록 및 목록 뷰에서 사용할 수 있습니다. 할당되지 않은 할당 유형은 시스템 속성으로 할당 대상 및 할당 그룹 필드를 지운 후 기록에 표시됩니다.

요청 승인에 대한 자세한 내용은 을 참조하십시오 에서 할당 해제 요청 승인 또는 거부 취약성 대응 .

이 기능에 대해 예약된 작업으로 담당 규칙 모니터링

일일 예약 작업은 할당되지 않은 할당 유형으로 전환될 때의 기록을 계산합니다. 이 개수로 취약성 분석가는 할당되지 않은 VI 수가 더 많은 할당 규칙을 기반으로 수행되지 않을 수 있는 할당 규칙을 모니터링하고 조정할 수 있습니다.

Reassignment count for assignment rules 예약된 작업은 매일 실행되며 특정 할당 규칙에 대해 이 기능에 의해 할당되지 않은 총 VI 수를 게시합니다.

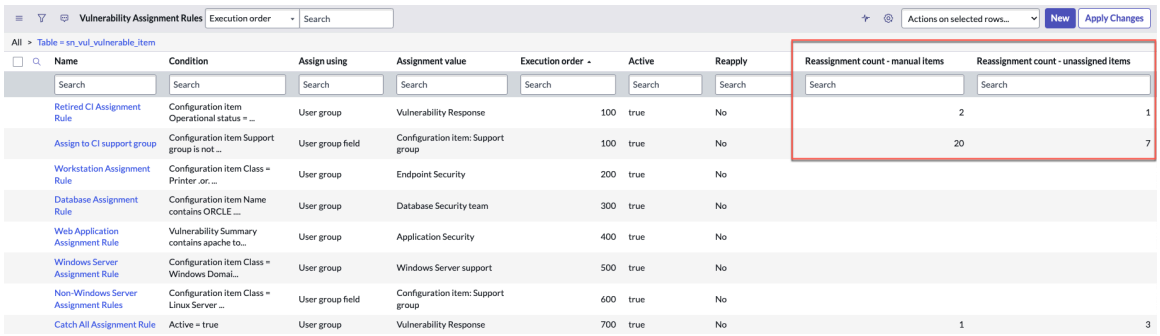
이 작업으로 수집된 개수는 취약 항목 및 및 애플리케이션 취약성 대응에 대한 취약성 대응 고유 할당 규칙에 적용됩니다. 개수는 각 모듈의 각 담당 규칙 목록에 할당 규칙에 따라 표시됩니다.

이 작업은 수동으로 할당되지 않은 모든 기록도 계산합니다. 수동 개수와 이 기능으로 수집된 개수는 모두 취약성 할당 규칙 목록의 두 개 열 *Reassignment count - manual items* (및 *Reassignment count - unassigned items*.

1. 취약성 관리자가 이러한 개수를 보려면 다음으로 이동합니다. 취약성 대응 〉 관리 〉 담당 규칙.
2. 목록의 오른쪽 상단에 있는 기어 아이콘을 클릭하고 , 및 *Reassignment count - unassigned items* 표시를 선택합니다*Reassignment count - manual items*.
3. 원래 규칙에 의해 할당되었지만 이후에 자동 또는 수동으로 재할당된 모든 VI에는 목록 뷰의 원래 규칙에 대한 참조가 포함됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음 예는 두 가지 할당 규칙의 재할당 횟수를 보여줍니다.



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

All > Table = sn_vul_vulnerable_item

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

취약성 대응 계산기 및 취약성 계산기 규칙

취약성 계산기는 취약한 항목 필드의 초기 값 계산을 자동화합니다. 각 계산기의 조건은 순서대로 평가되며 첫 번째로 일치하는 계산기가 사용됩니다.

취약성 계산기

기본 시스템에는 취약성 대응 취약한 항목의 기본 위험 점수를 설정하는 두 가지 취약성 계산기가 포함되어 있습니다.

- 기본 위험 계산기
- 취약성 심각도

조건 필터를 사용하여 어떤 기준에 따라 취약한 항목의 영향도 우선순위를 지정하고 등급을 지정하도록 취약성 계산기를 빌드할 수 있습니다. 취약성의 비즈니스 영향, CI(구성 항목)의 클래스 또는 취약한 항목의 기간 등에 관계없이 추가 취약성 계산기를 만들어 취약한 항목에 대한 다른 필드를 설정할 수 있습니다. 또는 기존 취약성 계산기를 사용자 지정할 수 있습니다. 계산기는 우선순위 집합을 반영하도록 작성할 수 있습니다. 자세한 내용은 AND 내부 필터링 취약성 대응 문서를 참조하십시오계산기 생성 취약성 대응.

또한 구성 관리 데이터베이스(CMDB)의 configuration_item [cmdb_ci]에 있는 속성을 사용하면 취약성 대응 위험 계산기의 논리를 만드는 데 도움을 받을 수 있습니다. 예를 들어 조직에서 외부 연결 CI가 더 취약하고 즉각적인 수정이 필요할 수 있다고 판단되는 경우 이러한 CI와 같은 *Internet Facing* 속성을 할당할 수 있습니다. 이 특성 및 기타 특성은 Common Service Data Model 릴리스 정보 에 나열되어 있습니다 . 에 CMDB대한 최신 정보 및 지침은 다음 주제를 참조하십시오.

- Common Service Data Model 개념적 모델
- CMDB 스키마 모델
- 취약성 대응: 위험 점수 계산(KB1169927)

각 계산기에는 규칙 적용 시기를 결정하는 조건과 함께 계산기 규칙 목록이 포함되어 있습니다. 계산기를 실행하면 각 계산기 규칙의 조건이 순서대로 평가되고 첫 번째로 일치하는 계산기 규칙이 사용됩니다.

취약성 심각도 계산기는 정규화된 취약성 심각도를 사용하여 취약한 항목에 대한 위험 점수를 계산합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

- 대상 필드(위험 점수)당 한 번에 하나의 계산기만 활성화할 수 있습니다. 취약성 심각도 는 기본적으로 비활성화되어 있습니다.
- VIT에서 위험 점수가 업데이트될 때마다 메모 섹션이 다음 상세 정보로 업데이트됩니다.
  - 계산기 그룹 이름
  - 계산기 이름: 계산기 규칙이 템플릿 또는 스크립트를 기반으로 하는지 여부에 따라 괄호 안에 이름이 세부 정보와 함께 추가됩니다. 계산기 규칙의 기초를 수정하거나 보려면 규칙을 클릭하고 고급 뷰 확인란을 선택합니다. 값 유형 드롭다운 상자에서 필요한 옵션을 선택합니다. 템플릿을 선택하면 규칙에 지정된 조건에 따라 위험 점수가 업데이트됩니다. 스크립트를 선택한 경우 기존 스크립트를 추가하거나 업데이트할 수 있습니다.

    시스템 속성은 *sn_sec_cmn.risk_score_changes_add_worknotes* 작업 메모 섹션을 채우는 데 도움이 됩니다. 의 취약성 대응v25.0.3부터 시스템 속성은 기본적으로 비활성입니다. 이를 활성화한 경우에만 위험 점수와 관련된 모든 변경 내용을 볼 수 있습니다.

활성화된 모든 취약성 계산기는 취약한 항목이 생성될 때마다, 연결된 CI 또는 취약성이 변경될 때마다, 또는 취약한 항목의 위험 점수 계산 관련 링크를 사용할 때마다 선택한 필드를 설정합니다. 예를 들어, 임포트된 취약성에서 심각도 값이 업데이트되면 취약한 항목 기록에서 위험 점수가 자동으로 업데이트됩니다. 취약성 임포트에서 취약성 점수를 업데이트한 후에는 해당 취약성에 대해 다시 계산 플래그가 활성화됩니다. 해당 취약성에 다시 계산 플래그가 사용(true)된 취약한 항목에 대한 위험 점수가 다시 계산됩니다.

기존 취약한 항목에서 위험 점수 계산 관련 링크를 클릭하고 계산기 중 하나를 사용하도록 설정하면 취약한 항목의 위험 점수 필드가 업데이트됩니다.

주:

- 위험 점수 계산 관련 링크는 하나 이상의 취약성 계산기가 활성화된 경우에만 표시됩니다.
- 에서 IT 정정 작업 공간 그리고 해당 기록 뷰에서 위험 점수 계산 버튼을 선택하여 취약한 항목에 취약성 관리자 작업 공간 대한 위험 점수를 업데이트할 수 있습니다.
- VIT의 위험 점수가 변경될 때마다 다음 상세 정보가 VIT의 메모 섹션에 문서화됩니다.
  - 계산기 그룹 이름
  - 계산기 이름
  - 가중치 및 위험 점수 기여도가 있는 필드 값
  - 최종 위험 점수

취약성 계산기 규칙

기본 시스템 계산기인 기본 위험 계산기에는 위험 규칙이라고 하는 특수 취약성 계산기 규칙인기본 위험 규칙 규칙이 포함되어 있습니다. 여러 값을 기준으로 위험 점수를 계산합니다.

- 취약성 심각도
- 악용 정보
- 중요도
- 취약성이 있는 CI의 외부 노출
- EPSS 점수

기본 위험 규칙에 사용할 값과 이러한 각 값에 지정할 가중치를 조정할 수 있습니다. 가중치는 기본 위험 점수를 설정할 때 각 요소의 수를 조정하는 데 사용됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

기본 위험 규칙의 기준을 사용자 지정할 수 있습니다. 자세한 내용은 Vulnerability Response 위험 계산기의 위험 규칙에 대한 필드와 가중치 정의 문서를 참조하십시오.

위험 규칙 계산기의 위험 점수가 결정되는 방식의 예는 다음 문서를 에 대한 위험 점수 계산 예 취약성 대응참조하십시오.

가중치 백분율 할당

필드 값 수준에서 가중치 백분율(0-100)을 할당할 수도 있습니다. 예를 들어, 각 심각도 수준에 가중치 백분율을 할당할 수 있습니다(없음에서 중요).

위험 규칙에 대해 심각도 가중치가 50이고 심각도 수준에 대해 다음 가중치 값이 할당된 경우:

취약성 심각도	위험 점수
중요	100
높음	50
중간	20
안 함	0

심각도가 중요인 경우 해당 가중치는 50입니다. 심각도가 높으면 등가 가중치는 25이고, 심각도가 중간이면 등가 가중치는 10입니다. 심각도가 없음이면 해당 가중치는 0입니다. 자세한 내용은 를 에 대한 위험 점수 계산 예 취약성 대응참조하십시오.

취약성 계산기 규칙 설정

각 규칙에는 순서 설정이 있습니다. 그러나 조건과 일치하는 첫 번째 조건이 취약한 항목의 위험 점수 필드를 업데이트합니다. 취약성 계산기 규칙 설정에 대한 자세한 내용은 다음 문서를 참조하십시오 계산기 생성 취약성 대응. 일반적으로 스크립트되지 않은 계산기 규칙은 스크립트된 계산기 규칙보다 성능에 미치는 영향이 적습니다.

기본 시스템 취약성 심각도 계산기에는 심각도에 따라 위험 점수 의 각 심각도 수준(없음에서 위험)을 할당하는 계산기 규칙이 포함되어 있습니다. 알 수 없는 심각도 에는 위험 점수 100이 자동으로 할당됩니다. 이러한 값은 조정할 수 있으며 기본 위험 계산기와 마찬가지로 새 계산기 규칙이나 새 위험 규칙을 만들 수 있습니다.

취약성 위험 점수 가중치

모든 취약성에는 심각도, 중요도, 악용 정보 등의 요인에 따라 위험 점수와 등급이 할당됩니다. 취약한 항목 테이블의 비즈니스 규칙은 *`Update Risk Rating from Risk Score`* 위험 등급 계산을 담당합니다. 위험 점수가 변경될 때마다 취약한 항목에 대한 위험 등급이 계산되어 채워집니다.

값(위험 등급)	가중치(위험 점수)
1	90–100
2	70–89
3	40–69
4	1–39
5	0

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 위험 등급 유형은 기본 테이블에 vr_risk_rating으로 제공됩니다. 이러한 유형은 위험 등급이 계산되는 각 테이블에서 비즈니스 규칙의 일부로 전달됩니다.
- 위험 등급 계산을 위해 위험 점수 가중치 테이블 값의 항목을 쿼리할 수 있도록 스크립트가 수정됩니다.
- 기존 형식에 대한 항목을 추가하거나 새 형식을 만듭니다. 새 유형을 만들 때는 새 위험 등급에 대한 레이블을 추가하고 관련 스크립트 및 비즈니스 규칙도 수정해야 합니다. 또한 새 위험 점수에 대한 새 스타일을 추가해야 합니다.
- 스크립트를 수정하여 기본 테이블의 기록을 쿼리합니다.

필터 탐색기에 sn_sec_cmn_risk_score_weight 입력하여 위험 점수 가중치 테이블에 액세스할 수 있습니다.

또한 연관된 CVE(Common Vulnerabilities and Exposures) 또는 VI(취약성 항목)의 타사 항목(TPE)이 CVE Known Exploit Vulnerability(KEV)에 연결되면 위험 점수가 자동으로 다시 계산됩니다.

Tenable 취약성 통합 및 **Tenable** 위험 규칙

Tenable 위험 규칙은 와 함께 사용할 수 있습니다 Tenable Vulnerability Integration. VPR(취약성 우선순위 등급)은 에서 임포트되어 새 기본 위험 계산기 취약성 대응와 함께 사용되는 Tenable 제품의 속성입니다. Tenable 위험 규칙은 의 취약성 계산기취약성 대응에 기본 위험 계산기의 일부로 애플리케이션과 함께 Vulnerability Response Integration with Tenable 설치됩니다.

이 위험 규칙은 기본적으로 사용되지 않습니다. 설정 도우미를 사용하여 Tenable 취약성 통합 구성 문서를 참조하십시오.

취약성 대응 외부 공급업체 통합에서 취약한 항목 탐지

인스턴스에서 외부 공급업체 검사 ServiceNow AI Platform# 로 수집된 모든 정보를 봅니다. 스캐너에서 반환된 탐지 및 VI(취약한 항목) 기록에 대한 검사 결과를 봅니다.

개요

이 취약성 대응 애플리케이션은 엔터프라이즈 환경에서 취약한 항목 데이터를 검색하는 타사 통합을 지원합니다. 탐지에 대한 자세한 데이터, 즉 외부 공급업체 통합의 스캐너에서 보고되는 고유한 단일 취약성 발생이 임포트되어 인스턴스의 탐지 및 취약한 항목 기록 ServiceNow AI Platform 모두에 표시됩니다.

외부 공급업체 통합은 취약한 항목 탐지 데이터를 검색합니다. 탐지는 스캐너에서 보고되는 취약성의 명백한 발생입니다. 탐지 데이터는 취약한 항목과 쌍을 이루고 탐지 상태에 따라 VI 상태가 업데이트됩니다. VI를 찾을 수 없는 경우 새 VI가 생성됩니다. 탐지는 스캐너에서 직접 찾은 데이터에 의해서만 열리거나 닫힙니다.

이전 버전의 취약성 대응에서 취약한 항목 탐지는 환경의 CI(자산)와 외부 공급업체 스캐너에서 가져온 취약성 간의 관계로 인해 인스턴스에 고유한 취약한 항목이 ServiceNow AI Platform 생성되었습니다.

스캐너에서 제공하는 원본 데이터의 세분성은 보존됩니다. 탐지를 사용하면 탐지 데이터가 취약한 항목과 쌍을 이룹니다. 수집 중에 취약한 항목을 찾을 수 없으면 새 VI가 생성됩니다.

의 버전 21.1.2 취약성 대응부터 기본 시스템에 시스템 속성이 *sn_vul.show_last_open_detection* 제공됩니다. 기본적으로 이 프로퍼티의 값은 false로 설정되며 초기 감지에서 VI로 값을 집계하는 현재 동작은 변경되지 않습니다. 그러나 true로 설정된 경우 VI는 수집 후 마지막으로 열린 탐지로 자동 업데이트됩니다. VI 탐지를 위해 IP 주소, SSL, 포트, 프로토콜, NetBIOS 및 증거와 같은 필드가 업데이트됩니다. 필요한 경우 DetectionBase 스크립트를 수정하여 업데이트해야 하는 탐지 필드를 사용자 지정할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

마지막으로 열린 탐지 값을 보려면 VI 양식 뷰에서 마지막으로 열린 탐지 탭으로 이동합니다. 작년에 열린 모든 VI를 마지막으로 열린 탐지 값으로 업데이트하려면 요청 시 예약된 작업을 *Update Last Open Detection Value To VITs* 실행할 수 있습니다. 이 예약된 작업은 기본 시스템에서도 제공됩니다.

주:
검색된 항목에서 CI(구성 항목)가 변경되면 해당 업데이트도 탐지에 반영됩니다. 결과적으로 탐지가 한 VI에서 다른 VI로 이동될 수 있습니다. 이 변경과 프로퍼티 값에 *sn_vul.show_last_open_detection* 따라 탐지 값이 소스 및 타겟 VI로 롤업됩니다.

지원되는 버전 취약성 대응

애플리케이션 설치 또는 업데이트에 취약성 대응 대한 자세한 내용은 문서를 참조하십시오 취약성 대응 설치.

지원되는 외부 공급업체 통합

취약한 항목 탐지에는 애플리케이션과 함께 취약성 대응 지원되는 외부 공급업체 통합이 필요합니다. 다음 외부 공급업체 통합은 취약한 항목 탐지를 위해 애플리케이션에서 지원됩니다 취약성 대응 .

- Qualys 호스트 탐지 통합
- Rapid7 데이터 웨어하우스:
  - 취약한 항목 통합
  - 취약한 항목 해결 통합
- Rapid7 취약한 항목 해결 통합(InsightVM)
  - 인사이트 VM 통합
  - 취약한 항목 통합 - API
- Tenable Vulnerability Integration
- Microsoft Defender 취약성 관리

이러한 타사 통합은 별도의 구독을 통해 사용할 수 있습니다 ServiceNow Store. 이러한 통합에 대한 자세한 내용은 을 참조하십시오 및 권리 획득에 대한 자세한 내용은 을 보안 운영 그리고 ServiceNow Store 참조하십시오취약성 대응 통합.

타사 스캐너가 임포트하도록 구성되었는지 확인하려면 보안 운영용 Rapid7 통합 애플리케이션Qualys Vulnerability Integration 설치설치 및 구성을 참조하십시오.

취약한 항목 탐지에 대한 주요 용어

취약성

내부 및 외부 소스에서 임포트한 소프트웨어, 운영 체제 및 자산의 약점에 대한 데이터입니다. 이 데이터를 임포트하여 CMDB에 나열된 기존 자산(구성 항목, CI)과 비교합니다.

취약한 항목

임포트한 취약성이 CMDB의 CI와 일치하면 취약한 항목이 생성되거나 업데이트됩니다.

탐지

환경 내에서 취약한 항목 탐지라고 하는 스캐너에 의해 보고되는 분명한 한 건의 취약성 발생입니다 ServiceNow AI Platform . 탐지에는 취약성 및 해당 취약한 항목에 대한 보강된 데이터가 포함됩니다. 이 데이터는 탐지 기록(VID#) 및 다음 상세 정보를 포함하는 취약한 항목 목록 뷰에 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 첫 발견(데이터)
- 마지막 발견(날짜)
- DNS 이름
- 순 BIOS이름
- IP 주소
- 포트
- 프로토콜
- 증명
- SSL
- 발견 시간

주:
탐지 테이블에 비즈니스 규칙을 추가하면 수집 성능에 영향을 줍니다.

탐지 키

탐지를 식별하고 취약한 항목에 연결하는 방법을 제공한 해시된 필드 조합입니다. 탐지 키는 통합에 따라 다릅니다.

탐지 키 구성

스캐너	취약성	포트	프로토콜	자산 **ID**	증명	**NIC**
Qualys	예	예	예	예	아니요	해당 사항 없음
Tenable	예	예	예	예	아니요	해당 사항 없음
Rapid7	예	예	예	예	예 (대소문자 구분 없음)	예

주:

- 탐지 키가 지정되지 않은 경우 또는 14.0 이전 취약성 대응 버전의 경우 탐지 키는 취약성 항목, 포트, 프로토콜, 자산 ID 및 증명의 조합입니다.
- 의 취약성 대응v19.0부터 기본적으로 활성화되는 새 탐지 키 NIC가 추가됩니다 Rapid7 InsightVM. NIC가 없는 기존 탐지는 의 Rapid7페이로드에서 첫 번째 수신 NIC로 업데이트됩니다. 탐지 키가 다시 계산되고 NIC를 포함한 탐지 시 다시 채워집니다. NIC 값이 다른 유사한 탐지가 확인되면 새 탐지가 생성됩니다. 이 데이터는 취약한 항목 테이블로 롤업되지 않습니다. NIC 값은 sn_vul_detection_key_config 및 sn_vul_detection 테이블의 새 열에 저장됩니다.

De dup

데이터가 하드 코딩된 특정 기준을 충족하는 경우 개별 탐지를 단일 VI로 축소하는 애플리케이션에서 사용하는 취약성 대응 프로세스입니다.

VI 외부 ID

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

VI 테이블의 외부 ID 필드에 저장된 값입니다. 이 값은 VI 내의 키 조합으로 구성된 해시로, 어플리케이션 내에서 고유한 요소를 나타냅니다. CI와 취약한 항목으로 구성됩니다.

해결된 취약 항목 다시 열기

인스턴스에서 해결됨ServiceNow AI Platform 으로 설정되었지만 후속 통합 실행에 의해 종결/수정됨으로 전환되지 않은 취약한 항목은 재스캔 중에 탐지되면 다시 열립니다.

하위 상태가 고정 또는 부실 인 종결된 VI는 새로운 탐지가 생성되고 VI를 새로운 취약성과 일치시킬 수 있는 경우 다시 열립니다.

스크립트 포함, *`DetectionBase`*메서드*`_shouldReOpenVI()`*에 따라 VIT가 이전에 하위 상태가 고정, 부실 또는 **CI** 해제된 상태로 종결된 경우 VIT가 다시 열리고 탐지가 기존 VIT에 매핑됩니다.

예를 들어 VIT의 종결 날짜가 탐지 last_found 날짜보다 나중이라고 가정해 보겠습니다. 이러한 VIT 기록은 종결된 상태로 유지될 것으로 예상할 수 있습니다. 그러나 이전에 닫힌 VIT가 다시 열린 경우 VIT가 이전 탐지에 의해 닫혔고 이후 검사에서 취약성이 다시 발견되었음을 의미합니다. VIT의 구성 항목에서 동일한 취약성이 있는 종결된 VIT와 일치하는 새 탐지가 발견되면 VIT가 다시 열립니다.

탐지의 경우 Rapid7 , 이제 인스턴스의 Rapid7 구성 페이지에서 해결된 VI를 기간별로 다시 여는 옵션을 사용할 수 있습니다. 활성화된 경우 VI가 해결됨 으로 설정되었지만 후속 스캔에 의해 종결/수정 으로 전환되지 않고 입력한 날짜 수가 지나면 다시 열림 으로 전환됩니다.

탐지의 경우 Qualys 스캐너가 해결됨 으로 설정되었지만 후속 스캔에서 종결/수정 으로 전환되지 않은 VI를 계속 찾으면 마지막으로 발견된 날짜가 해결됨 날짜보다 나중일 때 이러한 VI가 다시 열림 으로 이동합니다.

탐지 데이터 보기

VI 기록의 취약한 항목 탐지에서 임포트한 데이터를 볼 수 있습니다. 자세한 내용은 취약한 항목 탐지 데이터 보기 취약성 대응 및 통합 실행(VINTRUN) 기록에서 취약한 항목 탐지 데이터 확인 취약성 대응 문서를 참조하십시오.

취약성 솔루션 관리

환경의 취약성과 이를 정정할 수 있는 솔루션의 상관관계를 자동으로 지정합니다. 취약성에 적용되는 정정 작업을 식별하고 취약성 위험을 최대한 줄여 우선순위를 지정합니다.

취약성 솔루션 관리

보안 및 IT 팀은 환경에 가장 효과적인 치료법을 찾기 위해 취약성 발견 사항을 조사하는 데 상당한 시간을 할애하는 경우가 많습니다. 대규모 조직의 취약성 양과 복잡성을 고려할 때 취약성 결과를 정정 작업으로 변환하는 것은 지루하고 오류가 발생하기 쉬운 수동 프로세스입니다.

를 사용하면 취약성 솔루션 관리취약성 결과를 정정 솔루션과 자동으로 연관시킬 수 있습니다. 수동 오버헤드 없이 조직에 가장 큰 영향을 미치는 소프트웨어 패치, 구성 업데이트 및 기타 제어를 식별합니다.

취약성 솔루션 관리 요구 사항

취약성 솔루션 관리 애플리케이션 내에서 취약성 대응 사용할 수 있는 기능입니다. 취약성 솔루션 관리별도의 구독이 필요합니다.

에서 ServiceNow Store애플리케이션에 대한 권리를 얻는 방법에 대한 자세한 내용은 을 참조하십시오 제품 또는 애플리케이션에 대한 보안 운영 권리 가져오기. 애플리케이션을 인스턴스에 다운로드한 후 설치하는 방법에 대한 자세한 내용은 을 참조하십시오 취약성 대응용 솔루션 관리 애플리케이션 설치 .

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설치가 취약성 솔루션 관리 완료되면 내부에서 취약성 대응및 솔루션 데이터에 액세스할 Microsoft Security Response Center 수 Red Hat 있습니다.

주:

설정 도우미 내에서 두 솔루션 애플리케이션을 모두 구성할 수 있습니다. 설치 도우미를 사용하기 위해 취약성 솔루션 관리 설치된 솔루션 통합 구성 문서를 참조하십시오.

Microsoft Security Response Center 솔루션 통합 임포트한 솔루션에 대한 자세한 내용은 을 Red Hat Solution Integration참조하십시오.

사용 가능한 버전

최신 버전의 취약성 솔루션 관리경우 최신 버전이 취약성 대응 설치되어 있는지 확인합니다.

의 릴리스 버전 취약성 솔루션 관리	호환되는 버전 취약성 대응	릴리스 정보
취약성 솔루션 관리 v10.3	취약성 대응 v18.0	호환성 정보는 KB0856498 Vulnerability Response 호환성 매트릭스 및 릴리스 스키마 변경을 참조하십시오.

솔루션 및 대체 정보

대체된 업데이트는 이전 릴리스를 완전히 대체하는 것입니다. 예를 들어 핫픽스 업데이트는 서비스 팩으로 대체될 수 있습니다. 솔루션은 취약성과 관련이 있습니다. 솔루션은 대체 체인의 다른 솔루션과도 관련될 수 있습니다. 솔루션은 이전 솔루션의 취약성과 누적된 취약성을 해결합니다. 취약성 솔루션 관리 는 이전 솔루션의 취약성을 대체 솔루션과 자동으로 연결합니다. 더 오래된 취약성이 발견되면 더 높은 대체 솔루션으로 해결할 수 있지만 가장 누적적이므로 가장 높은 대체 솔루션이 선호됩니다.

잠재적 솔루션 대 선호 솔루션

잠재적 솔루션은 취약성을 해결할 수 있는 솔루션입니다. 취약성에는 종종 많은 잠재적인 솔루션이 있습니다. 기본 솔루션은 취약성 또는 VI(취약한 항목)를 정정하기 위한 단일 솔루션입니다. 의도를 전달하고 더 자세한 배포 메트릭을 활성화합니다.

기본 설정 솔루션

취약성 솔루션 관리 대체 가능성이 가장 높은 솔루션이 하나만 있는 경우 대체 가능성이 가장 높은 솔루션을 기준으로 탐지된 취약성에 대해 가장 효과적인 솔루션(기본 솔루션)을 자동으로 설정합니다. 취약성에 대해 대체 가능성이 가장 높은 항목이 두 개 이상 있는 경우 값이 설정되지 않습니다. 에서 취약성 대응기본 솔루션은Microsoft Security Response Center 취약성과 연관된 솔루션에서 파생된 대체 가능성이 가장 높은 또는 Red Hat 솔루션입니다.

취약한 항목 또는 취약성에 기본 솔루션 값을 설정할 수 있습니다. 취약성에 직접 설정하면 취약성과 관련된 모든 취약한 항목이 해당 솔루션을 상속합니다. 대량 편집 기능을 사용하여 여러 취약한 항목에 대한 기본 솔루션 값을 변경합니다. 취약성 엔트리 수준에서 기본 솔루션을 설정하면 이후의 모든 새로운 VI에 대한 기본 솔루션이 설정되므로 대량 편집 시, 취약한 항목에 대한 기본 솔루션만 업데이트됩니다. 대량 편집은 현재 취약한 항목에만 적용됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

> **주:**
> 취약성에 대해 대체 가능성이 가장 높은 솔루션이 여러 개 있는 경우 해당 솔루션은 영향을 받는 자산에 따라 달라지므로 취약성 수준의 기본 솔루션 값이 지워집니다. 취약성에 대해 대체 가능성이 가장 높은 솔루션이 여러 개 있는 경우 취약한 항목에 기본 솔루션을 설정합니다. 취약한 항목 양식의 조회 목록을 사용하여 다른 솔루션을 설정할 수 있습니다.

정정 작업의 취약한 항목에 대해 기본 설정된 모든 솔루션은 정정 작업 기록의 관련 목록에 있습니다.

모든 솔루션 임포트로 인해 전체 데이터가 새로 고침되는 것은 아닙니다. 다음과 같은 경우 대체 프로세스가 업데이트됩니다.

- 취약한 항목이 생성됩니다.
- 활성 VI에서 데이터가 변경되었습니다.

> **주:**
> v22.0 부터 취약성 대응위의 두 경우에는 솔루션이 큐에 대기하지 않습니다.

- CVE를 사용하는 외부 공급업체 항목에 대해 새 매핑이 생성됩니다.
- 마지막 임포트 이후 새 솔루션 데이터가 릴리스되었으며 기존 솔루션이 업데이트됩니다.

v24.0.6 부터 취약성 대응벤더 솔루션 외에도 스캐너에서 솔루션을 수집할 수 있습니다. Tenable, Qualys및 Microsoft TVM과 같은 스캐너의 정정 데이터를 활용하여 솔루션을 만듭니다. 이러한 스캐너 솔루션은 다음 통합을 사용하여 임포트됩니다.

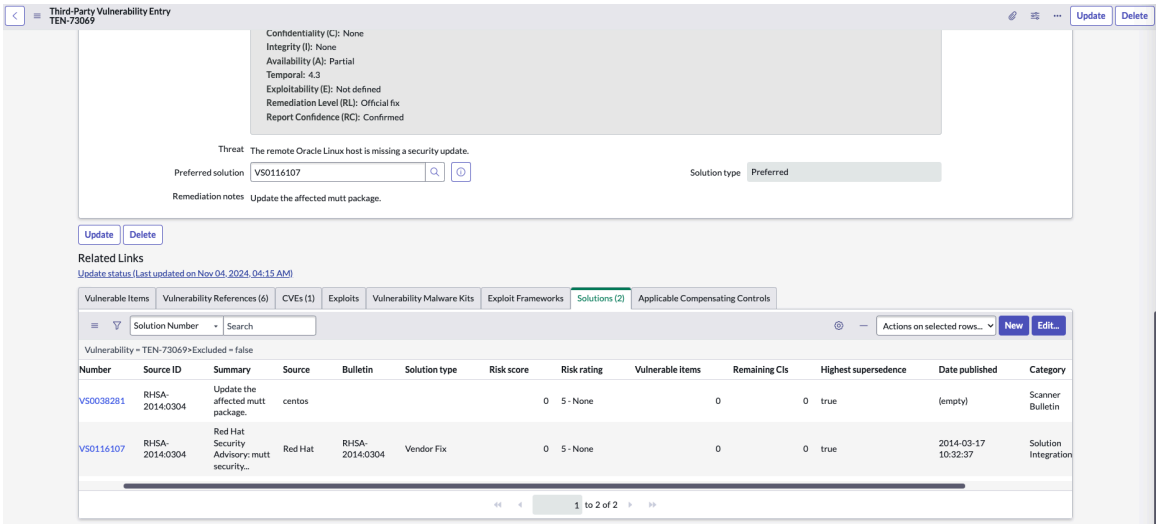
- Tenable.sc 플러그인 통합
- Tenable.io 플러그인 통합
- Qualys 지식베이스(백필)
- Microsoft TVM 머신 취약성 통합(전체 임포트)
- Microsoft TVM 머신 취약성 통합(델타 임포트)

취약성 통합이 실행되면 외부 공급업체 항목을 처리하기 전에 정정 정보의 페이로드가 생성됩니다. Tenable 및 Qualys의 경우 정정 데이터는 취약성 또는 타사 엔트리 레벨에서 수신됩니다. 반대로 Microsoft TVM의 경우 솔루션이 검색 수준에서 생성되므로 추가 처리 없이 취약한 항목에 대한 기본 설정 솔루션을 직접 채울 수 있습니다. 이러한 솔루션은 이 정정 정보를 기반으로 생성되고 필요에 따라 처리됩니다. 처리 시 기본 솔루션이 취약성에 채워지고 취약한 항목으로 롤다운됩니다. 기본 솔루션은 다음 순서로 채워집니다.

- 수동 선택: 솔루션을 수동으로 선택하면 재정의되지 않습니다.
- 벤더 솔루션(Microsoft, RedHat, CVRF 및 CSAF 임포트): 솔루션을 수동으로 선택하지 않으면 벤더 솔루션이 자동으로 선택됩니다.
- 최신 솔루션(활성화된 경우): 취약성에 사용할 수 있는 더 높은 대체 솔루션이 여러 개 있는 경우 기본 솔루션 필드는 비어 있습니다. 이러한 경우 속성을 *sn_vul.latest_solutions*활성화하면 더 높은 최신 대체 벤더 솔루션이 기본 솔루션으로 채워집니다.
- 스캐너 공지 솔루션(활성화된 경우): 솔루션을 수동으로 선택하지 않거나 벤더 솔루션을 사용할 수 없는 경우, 기본 솔루션 필드는 단일 스캐너 솔루션이 있는 경우 스캐너 솔루션으로 채워집니다. 스캐너 솔루션을 채우려면 속성을 *sn_vul.populate_scanner_solutions* 활성화해야 합니다.

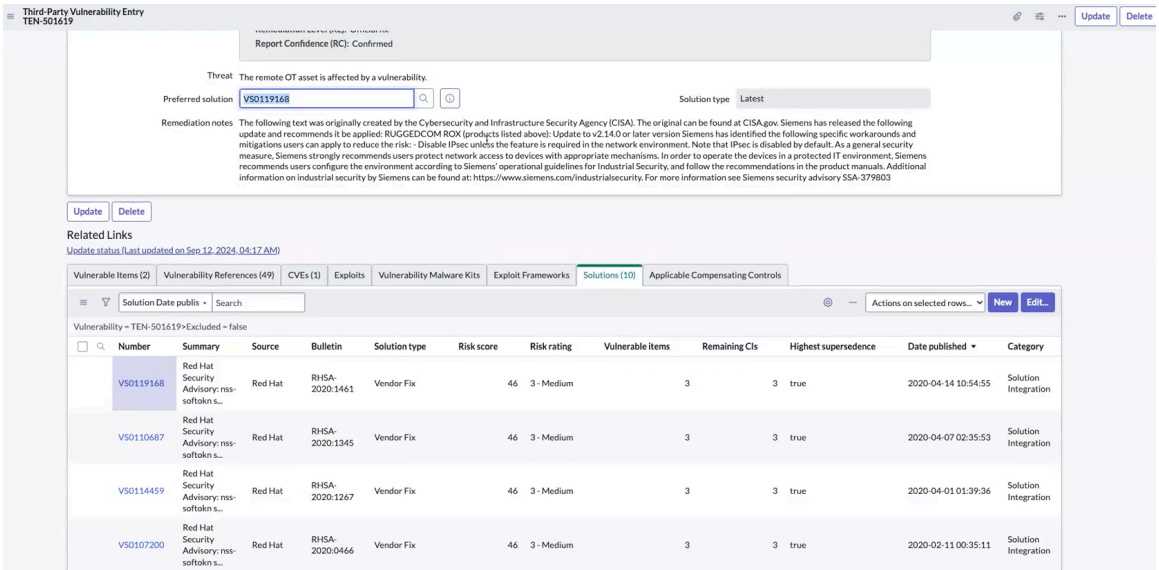
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

여러 소스의 솔루션



이 예에서는 서로 다른 소스에서 여러 솔루션을 사용할 수 있는 경우 솔루션을 선택하는 방법을 보여줍니다. 이 경우 취약성에 대한 두 가지 솔루션이 있는데, 하나는 벤더의 솔루션이고 다른 하나는 스캐너의 솔루션이다. 기본 설정이 더 높은 벤더(예: Redhat)로부터 솔루션 VS0116107 받으면 기본 솔루션으로 선택됩니다.

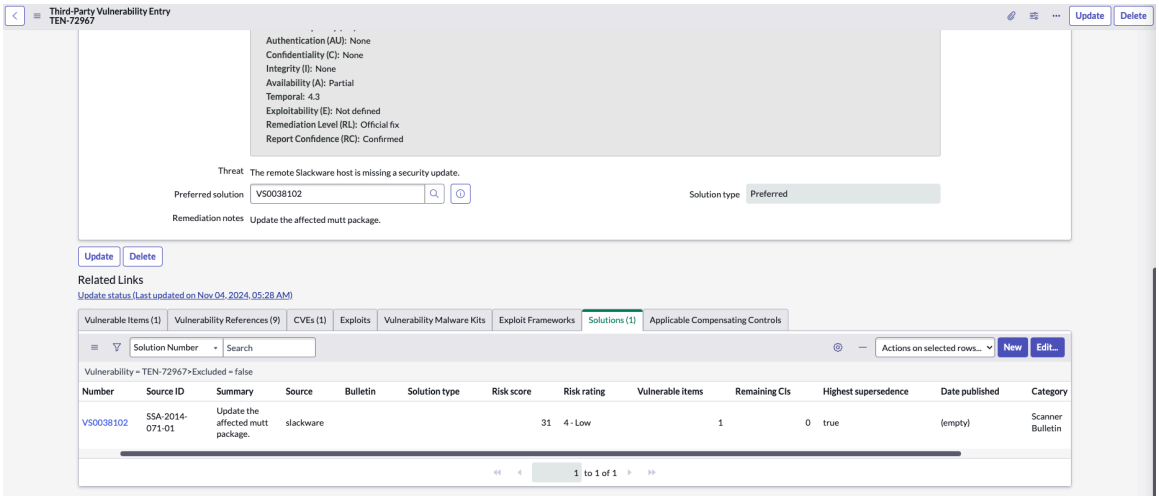
동일한 벤더의 솔루션



이 예에서는 동일한 벤더(이 경우 Redhat)에서 여러 솔루션을 사용할 수 있는 경우 솔루션을 선택하는 방법을 보여줍니다. *sn_vul.latest_solutions* 속성이 활성화되고 특정 취약성에 사용할 수 있는 다른 벤더 솔루션이 없는 경우 이러한 솔루션이 처리되어 취약성에 대한 기본 솔루션이 채워지고 이후에 취약한 항목에 채워집니다. 이 속성을 *sn_vul.latest_solutions* 활성화하면 최신 솔루션이 기본 솔루션으로 선택됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

동일한 스캐너의 솔루션



이 예에서는 스캐너에서 하나의 스캐너 솔루션만 사용할 수 있는 경우 솔루션을 선택하는 방법을 보여줍니다. *sn_vul.populate_scanner_solutions* 이 속성을 사용하도록 설정하면 솔루션이 처리되어 취약성에 대한 기본 솔루션이 채워지고 이후에 취약한 항목에 채워집니다. 스캐너 솔루션이 여러 개 있는 경우, 모호성으로 인해 기본 솔루션 필드가 비어 있습니다.

솔루션 관리 및 성능 최적화 강화

솔루션은 Microsoft 및 Redhat을 비롯한 다양한 통합에서 수신됩니다. 전자는 매월 업데이트를 제공하고 취약성에 대해 선호하는 솔루션을 추적하기 위해 종속성 체인을 설정합니다. 그러나 다른 통합은 이 업데이트 형식을 따르지 않으며 종속성 체인을 설정할 필요가 없습니다. 이전에는 우선 순위를 유지하고 가장 높은 대체 솔루션을 식별하기 위해 그래프를 만드는 것과 관련된 처리 논리가 사용되었습니다. 이러한 솔루션은 취약성에 대해 기본 솔루션으로 제안되었습니다. 그러나 그래프를 구성하는 데 시간이 많이 걸리기 때문에 다른 통합은 이 프로세스에서 제외됩니다. 성능을 향상시키기 위해 v22.0 부터 취약성 대응유틸리티 메소드 *utility.processNonGraphSolutions()* 가 *Process Vulnerability Solutions Metrics Queue* 예약된 작업에서 호출됩니다. 이 메서드는 Microsoft 이외의 통합에서 솔루션을 처리합니다.

둘째, 솔루션은 예약된 작업을 *Process Vulnerability Solutions Metrics Queue*사용하여 다양한 소스에서 대기합니다. 이 예약된 작업에는 NVD 항목에서 외부 공급업체 항목으로 솔루션을 롤업하고, 취약성에 대한 기본 솔루션을 채우고, 솔루션의 정정 상태 메트릭을 업데이트하는 작업이 포함됩니다. 다음 시나리오에서는 정정 상태 메트릭만 업데이트해야 합니다.

- 취약성에 대해 기본 솔루션이 변경되는 경우
- VIT가 생성되거나 삭제될 때
- VIT 임포트가 완료된 경우

솔루션은 정정 상태 메트릭만 업데이트하기 위해 큐에 대기하지만 NVD 항목에서 외부 공급업체 항목으로 솔루션을 롤업하고 기본 솔루션을 채우려고 시도합니다. 이 프로세스를 최적화하기 위해 취약성 솔루션 테이블에 업데이트 상태 열이 도입되었습니다. 기본 솔루션의 롤업 또는 채우기 없이 솔루션의 정정 상태 메트릭을 업데이트해야 하는 경우 솔루션이 더 이상 큐에 대기하지 않습니다. 대신 업데이트 상태 열이 true로 직접 업데이트됩니다. 이 접근 방식을 사용하면 정정 상태 메트릭만 업데이트해야 하는 케이스를 처리할 수 있으므로 시간과 리소스가 절약됩니다. 예약된 작업에서 큐에 대기 중인 솔루션의 처리가 완료되면 업데이트 상태가 true로 표시된 솔루션이 식별됩니다. 그런 다음, 이러한 솔루션을 반복하여 개수를 계산하고 그에 따라 정정 상태 메트릭을 업데이트합니다. 이 단계는 큐에 대기해야 하는 솔루션 수가 줄어들기 때문에 예약된 작업의 성능을 개선하는 데 중요한 역할을 합니다. 정정 상태 메트릭을 보려면 취약성 솔루션 [sn_vul_solution] 테이블로 이동하여 취약성 솔루션을 선택하십시오. 그런 다음 정정 상태 탭을 선택합니다. 이 탭에는 다음 필드가 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

정정 상태 메트릭

필드	설명
기본 솔루션 대상 - 이 솔루션이 기본 솔루션인 VI의 정정 상태	
취약한 항목	정정에 이 솔루션이 기본인 활성(종결되지 않음) 취약한 항목 수. 이 개수에서 지연된 취약한 항목은 제외됩니다.
남아 있는 CI	정정에 이 솔루션이 기본인 하나 이상의 활성 취약한 항목과 연결된 CI 수. 이 개수에서 지연된 취약한 항목은 제외됩니다.
총 VI	정정에 이 솔루션이 기본인 활성 및 종결된 취약한 항목 수. 이 개수에서 지연된 취약한 항목은 제외됩니다.
총 CI	정정에 이 솔루션이 기본인 하나 이상의 활성 및 종결된 취약한 항목과 연결된 CI 수. 이 개수에서 지연된 취약한 항목은 제외됩니다.
정정된 VI 비율(%)	VI(취약한 항목) 정정에 대한 완료율입니다. 이 솔루션이 기본인 VI에 적용됩니다. 이 개수에서 지연된 취약한 항목은 제외됩니다.
정정된 CI 비율(%)	CI 정정에 대한 완료율입니다. 이 솔루션이 기본인 VI에 적용됩니다. 이 개수에서 지연된 취약한 항목은 제외됩니다.
기본 솔루션 대상(지연 포함) - VI에 대한 정정 상태(지연 포함)로, 이것이 기본 솔루션임	
취약한 항목	정정에 이 솔루션이 기본인 활성(종결되지 않음) 취약한 항목 수.
남아 있는 CI	정정에 이 솔루션이 기본인 하나 이상의 활성 취약한 항목과 연결된 CI 수. 이 개수에서 지연된 취약한 항목은 제외됩니다.
총 VI	정정에 이 솔루션이 기본인 활성 및 종결된 취약한 항목 수.
총 CI	정정에 이 솔루션이 기본인 하나 이상의 활성 및 종결된 취약한 항목과 연결된 CI 수.
정정된 VI 비율(%)	VI(취약한 항목) 정정에 대한 완료율입니다. 이 솔루션이 기본인 VI에 적용됩니다.
정정된 CI 비율(%)	CI 정정에 대한 완료율입니다. 이 솔루션이 기본인 VI에 적용됩니다.
잠재적 솔루션 대상 - 이 솔루션과 관련된 취약성이 있는 모든 VI에 대한 정정 상태	
취약한 항목	이 솔루션이 정정을 위한 잠재적 솔루션인 활성(종결되지 않음) 취약한 항목 수입니다. 이 개수에서 지연된 취약한 항목은 제외됩니다.
남아 있는 CI	이 솔루션이 정정을 위한 잠재적 솔루션인 하나 이상의 활성 취약한 항목과 연결된 CI 수. 이 개수에서 지연된 취약한 항목은 제외됩니다.
잠재적 솔루션 대상(지연 포함) - 지연을 포함한 모든 VI에 대한 정정 상태이며 이 솔루션과 관련된 취약성이 있음	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

정정 상태 메트릭

필드	설명
취약한 항목	이 솔루션이 정정을 위한 잠재적 솔루션인 활성(종결되지 않음) 취약한 항목 수.
남아 있는 CI	이 솔루션이 정정을 위한 잠재적 솔루션인 하나 이상의 활성 취약한 항목과 연결된 CI 수.

셋째, 취약성을 정정하기 위해 취약성 및 VIT에 대해 선호하는 솔루션의 가용성을 보장해야 합니다. 그러나 취약성에 대해 더 높은 대체 솔루션이 여러 개 있는 상황에서는 모호성으로 인해 기본 솔루션이 채워지지 않습니다. 이 시나리오를 해결하기 위해 처리 논리를 실행하고 사용 가능한 경우 기본 솔루션을 채우는 방법을 구현합니다. 더 높은 대체 솔루션이 하나만 있는 경우 기본 솔루션으로 채워집니다. 더 높은 대체 솔루션이 여러 개 있는 경우 기본 설정 솔루션 필드는 비어 있습니다. 그러나 목표는 가장 최신으로 게시된 가장 높은 대체 솔루션을 기본 솔루션으로 채우는 것입니다. 이를 위해 시스템 속성이 *sn_vul.latest_solutions* 도입되었습니다. 기본적으로 이 속성은 False로 설정됩니다. 사용할 수 있는 기본 솔루션이 없을 때 최신 솔루션을 기본 솔루션으로 채우는 기능을 활성화하려면 이 속성을 활성화할 수 있습니다. 활성화되면 취약성 테이블에서 솔루션 유형 열이 다음 옵션으로 업데이트됩니다.

- 기본 설정: 기본 솔루션이 채워진 경우
- 최신: 기본 솔루션을 사용할 수 없는 경우 게시된 날짜 값을 기준으로 가장 높은 대체 솔루션 집합에서 최신 솔루션이 선택됩니다. 최신 솔루션으로 선택할 필드는 시스템 속성을 사용하여 사용자 지정할 수 있습니다 *sn_vul.latest_solutions* . 기본적으로 이 값은 "게시된 날짜"로 설정되어 있지만 "마지막으로 수정한 날짜"로 변경하여 솔루션에서 마지막으로 수정한 열을 기준으로 솔루션을 선택할 수 있습니다.
- 수동: 기본 솔루션 유형이 수동으로 업데이트되는 경우. 이 유형의 솔루션에 대한 우선 순위가 가장 높습니다.

특정 시나리오에서는 취약한 항목(VIT)에 대한 기본 솔루션이 해당 취약성에 대한 기본 솔루션과 다를 수 있습니다. 이는 기본 솔루션이 취약성이 아닌 VIT에서 수동으로 업데이트될 때 발생합니다. 이러한 경우 솔루션 유형 필드는 VIT에서 숨겨집니다.

수행하는 작업 취약성 솔루션 관리

- Microsoft Security Response Center 솔루션 통합 및 Red Hat Solution Integration 임포트 중에 새로운 취약한 항목(VIT) 및 정정 작업을 솔루션과 자동으로 연결합니다.

  MSRC 솔루션은 해당 솔루션이 표시되는 최신 게시판과 연결됩니다.

- 취약성 기록이 솔루션과 수동으로 연결되면 취약한 항목 및 정정 작업을 솔루션과 자동으로 연결합니다.

  주:
  다른 솔루션에 수동으로 재할당된 취약한 항목은 취약성 수준의 솔루션 변경 내용으로 자동으로 업데이트되지 않습니다.

- MSRC: 임포트 중에 솔루션의 관련 목록에서 볼 수 있는 대체 체인을 생성합니다.
- 솔루션이 가장 높은 대체 솔루션인지 여부를 나타냅니다.
- 각 솔루션과 연결된 솔루션 위험 점수를 나열하여 가장 큰 위험 감소 기회를 제공합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 정정 진행률을 추적할 수 있도록 외부 공급업체 취약성 항목, 정정 작업 및 취약성 솔루션 기록의 솔루션에 대한 정정 상태를 유지합니다.

  여기에는 다음이 포함됩니다.

  - 지연 상태의 취약한 항목 수(기본 솔루션이 있는 VI의 경우, 지연됨 상태의 취약한 항목 포함/미포함).
  - CI(구성 항목)는 기본 솔루션이 있는 VI에 대해 지연됨 상태의 해당 VI가 있거나 없는 경우 정정된 백분율을 기준으로 계산됩니다.
  - 지연됨 상태의 취약한 항목 수(잠재적 솔루션이 있는 VI의 경우, 지연됨 상태의 VI 유무에 관계없이)에 대한 정정된 비율로 나타낸 취약한 항목 수입니다.
  - 기본 솔루션이 있는 VI에 대해 지연됨 상태의 해당 VI가 있거나 없는 구성 항목 수입니다 (정정된 비율).

로 수행할 수 있는 작업 취약성 솔루션 관리

- 외부 공급업체 솔루션 콘텐츠에서 다루지 않는 취약성 솔루션을 추적할 수 있도록 취약성과 연관된 솔루션을 생성, 업데이트, 조회 또는 삭제합니다. 솔루션 Rapid7 데이터 웨어하우스와의 통합은 지원되지 않습니다.
- 타사 취약성 및 NVD 항목을 솔루션 기록과 연결합니다.
- 취약한 항목을 제거하고 솔루션과 다시 연결합니다.
- 취약성 및 취약한 항목 양식에서 지정된 취약성에 적용할 수 있는 기본 솔루션을 봅니다.
- 정정 작업 양식에서 해당 그룹 내에서 하나 이상의 활성 VI가 선호하는 모든 솔루션을 나열하는 기본 솔루션 관련 목록을 봅니다.
- 취약성, 취약한 항목, 정정 작업 및 솔루션 양식에 기본 솔루션 배포와 관련된 위험 감소를 보여주는 솔루션의 정정 상태 상세 정보를 봅니다.
- 솔루션 양식에서 지정된 솔루션에 적용할 수 있는 취약성을 봅니다.
- MSRC: 취약성에서 지정된 솔루션에 대한 대체 솔루션을 보고 배포할 최신 업데이트 또는 보다 집중적이고 효율적인 이전 업데이트를 찾습니다.
- 다양한 특성에 따라 정렬된 솔루션 목록을 봅니다.
  - 모두: 게시 날짜 및 번호로 정렬된 솔루션입니다.
  - MSRC: 가장 높은 대체: 활성 상태의 지연되지 않은 취약한 항목이 있는 솔루션입니다. 가장 높은 대체, 게시 날짜 및 번호로 정렬됩니다.
  - 취약한 항목 포함: 활성 상태이며 지연되지 않은 취약한 항목이 있는 솔루션입니다. 가장 높은 대체 또는 기본 설정, 위험 점수 및 숫자로 정렬됩니다. 배포되면 목록의 상위 항목이 환경의 자산에 대해 가장 큰 위험 감소를 제공합니다.

솔루션 기록 위험 점수 및 위험 등급

주:
솔루션 기록 위험 점수 및 위험 등급 은 취약성, 취약한 항목 및 정정 작업에 사용되는 필드와 다릅니다.

솔루션 기록 위험 점수 는 취약한 항목, 위험 점수 , 그리고 이 솔루션을 잠재적 솔루션으로 사용하는 활성 취약한 항목의 수를 기준으로 한 가중치 계산입니다. 솔루션 위험 점수 는 솔루션이 달성할 것으로 예상되는 위험 감소의 추정치를 제공합니다.

솔루션 레코드 위험 점수 는 다음과 같이 계산됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 먼저 해당 잠재적 솔루션을 사용하여 활성 취약한 항목의 최고 또는 최대 위험 점수 의 85%를 취합니다.
- 그런 다음 솔루션 레코드인 위험 점수 는 해당 잠재적 솔루션이 포함된 취약한 항목의 총 수를 표로 만듭니다. 취약한 항목 수의 각 범위에 대해 몇 가지 포인트를 추가하고 합계에 도달합니다.
  - 0–09개의 취약한 항목은 점수를 추가하지 않습니다.
  - 취약 아이템 10–99개 5점 추가
  - 100–999개의 취약한 항목이 10점 추가
  - 1,000 이상의 취약한 아이템은 15포인트 추가

  예를 들어 취약한 항목 위험 점수 가 80인 경우 솔루션 레코드 위험 점수 는 68에서 시작합니다. 해당 잠재적 솔루션을 가진 활성 총 취약한 항목이 200개 있는 경우 최종 솔루션 위험 점수 는 78이 됩니다.

솔루션 기록 위험 등급 은 솔루션 기록 위험 점수를 중요에서 없음까지의 범위로 구분합니다. 솔루션 위험 등급 은 이 솔루션이 정정하는 취약한 항목에 대한 위험 감소의 등급을 지정합니다.

VR v16.1까지 위험 등급은 결과 솔루션 위험 점수를 다음 범위로 구분했습니다.

- 1 — 중요(90+ 솔루션 위험 점수)
- 2 — 높음(70-89 솔루션 레코드 위험 점수)
- 3 — 중간(30-69 솔루션 레코드 위험 점수)
- 4 — 낮음(1-29 솔루션 레코드 위험 점수)
- 5 — 없음(0 솔루션 기록 위험 점수)

VR v16.1부터 위험 등급은 결과 솔루션 위험 점수를 솔루션 관리에 대해 다음 범위로 구분합니다.

- 1 — 중요(90+ 솔루션 위험 점수)
- 2 — 높음(70-89 솔루션 레코드 위험 점수)
- 3 — 중간(40-69 솔루션 레코드 위험 점수)
- 4 — 낮음(1-39 솔루션 레코드 위험 점수)
- 5 — 없음(0 솔루션 기록 위험 점수)

사용 케이스

날짜별로 정렬된 최고 대체 모듈을 사용하여 현재 패치 주기의 상태 배포 진행률을 봅니다.

취약한 항목 포함 모듈을 사용하여 위험 점수별로 정렬된 가장 가치가 높은 솔루션을 봅니다.

솔루션 목록은 주요 솔루션 상세 정보, 위험 점수 및 배포 메트릭을 전달합니다. 우선순위 지정에 위험 점수 와 활성 VI 수를 사용합니다. 현재 패치 주기에서 진행되지 않는 솔루션을 확인할 수 있으며, 이는 필수 구성 요소가 누락된 배포의 표시일 수 있습니다.

> **주:**
> 취약성 솔루션 양식의 정정 진행률을 위해 개인화 목록 열 메뉴에서 정정된 **%VI(percent_nd_pref_vis_remediated)**를 추가합니다.

Microsoft Security Response Center 솔루션 통합

에서 Microsoft Security Response Center 솔루션 통합제공하는 제안된 정정 솔루션을 검토하고 구현합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Microsoft Security Response Center 솔루션 통합의 기능에 취약성 대응포함되어 취약성 솔루션 관리 있으며 별도의 구독으로 사용할 수 있습니다. 솔루션을 통합하는 방법에 취약성 대응 대한 자세한 내용은 을 참조하십시오취약성 솔루션 관리.

Microsoft Security Response Center 는 Microsoft 제품 및 서비스에 영향을 미치는 보안 취약성에 대한 보고서를 조사하고 보안 위험을 관리하는 데 도움이 되는 솔루션 정보를 제공합니다. 솔루션은 제품에서 Microsoft Security Response Center 사용자 Microsoft Security Response Center 솔루션 통합 안으로 임포트한 알려진 정정 사항입니다.

Microsoft Security Response Center 솔루션 통합 예약된 작업으로 호출되는 제품에 대한 Microsoft Security Response Center 엔트리포인트를 포함합니다. 예약된 작업은 인스턴스를 다른 취약성 관리 시스템과 동기화된 상태로 유지하여 취약성 정정 수명주기를 단순화합니다. 예약된 작업은 지정된 순서대로 자동으로 실행됩니다. 예약된 개별 작업을 수동으로 실행할 수도 있습니다.

각 통합 기록에 대해 구성된 실행 사용자가 있습니다. 이 사용자의 기본값은 VR입니다. 시스템. 이 값은 변경하지 마십시오.

사용 가능한 버전

최신 버전 취약성 솔루션 관리 및 Microsoft Security Response Center 솔루션의 경우 최신 버전이 취약성 대응 설치되어 있는지 확인하십시오.

설치 및 구성 취약성 솔루션 관리 과 솔루션 통합에 대한 자세한 내용은 해당 문서를 설치 도우미를 사용하기 위해 취약성 솔루션 관리 설치된 솔루션 통합 구성참조하십시오취약성 대응용 솔루션 관리 애플리케이션 설치.

의 릴리스 버전 취약성 대응	의 버전 취약성 솔루션 관리	릴리스 정보
취약성 대응 v15.0	v10.3	호환성 정보는 KB0856498 Vulnerability Response 호환성 매트릭스 및 릴리스 스키마 변경을 참조하십시오.

역할

Microsoft Security Response Center 솔루션 통합 작업에는 다음과 같은 역할이 포함됩니다.

- sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음): 기록을 읽고, 쓰고, 삭제할 수 있습니다.
- sn_vul.vulnerability_write: 기록을 읽고 쓸 수 있습니다.
- sn_vul.vulnerability.read: 기록을 읽을 수 있습니다.
- sn_vul.remediation_owner: 정정 전문가 그룹 또는 개인에게 할당된 기록의 내부 메모를 읽고 쓸 수 있습니다. (itil 역할에 포함되어 있습니다.)

가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Microsoft Security Response Center 솔루션 통합

을(를 Microsoft Security Response Center 솔루션 통합) 보려면 다음으로 이동하십시오. 모두 〉 취약성 대응 〉 관리 〉 통합.

기본 시스템에는 다음과 같은 통합이 포함되어 있습니다.

Microsoft Security Response Center 솔루션 통합

통합	설명
Microsoft 보안 응답 센터 솔루션 통합	솔루션 및 NVD(국가 취약성 데이터베이스) 매핑을 검색하여 솔루션을 취약성, 취약한 항목 및 정정 작업과 연결합니다. 주: 2016 Microsoft Security Response Center 솔루션 통합 년 이전에는 솔루션을 제공하지 않습니다.

솔루션

임포트한 솔루션을 목록에서 보려면 문서를 솔루션 보기참조하십시오.

Red Hat Solution Integration

애플리케이션에서 제공하는 Red Hat Solution Integration 제안된 정정 솔루션을 검토하고 구현할 수 있습니다 취약성 대응 .

Red Hat Solution Integration의 기능에 취약성 대응포함되어 취약성 솔루션 관리 있으며 별도의 구독으로 사용할 수 있습니다. 솔루션을 통합하는 방법에 취약성 대응 대한 자세한 내용은 을 참조하십시오취약성 솔루션 관리.

Red Hat Solution Integration 제품 및 서비스에 영향을 미치는 Red Hat 보안 취약성 보고서를 조사하고 보안 위험을 관리하는 데 도움이 되는 솔루션 정보를 제공합니다. 정정 Red Hat Solution Integration 으로 알려진 솔루션은 에서 Red Hat.

의 버전 21.0 취약성 대응부터 는 Red Hat CVRF(공통 취약성 보고 프레임워크) 형식이 아닌 CSAF(일반 보안 자문 프레임워크) 형식으로 페이로드를 전송합니다. XML 기반 표준인 CSAF는 CVRF와 구조와 형식이 모두 다릅니다. 이러한 변경 사항을 수용하기 위해 새로운 CSAF 파서가 개발되었습니다. 이 파서는 CSAF 형식을 해석하여 그에 따라 테이블을 채우는 데 필요한 필드를 추출합니다.

주:
기본적으로 CSAF 형식으로 페이로드를 받게 됩니다.

다음 발췌에서는 수신된 Red Hat 페이로드를 각각 CSAF 및 CVRF 형식으로 구문 분석하기 위한 통합 스크립트를 보여 줍니다.

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

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

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

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

// Pass true if CSAF payload is expected. Pass false if CVRF payload is expected
```


© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
return new sn_vul.RedHatSolutionIntegration(true);
})(integrationProcessGr);
```

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

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

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

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

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

Red Hat Solution Integration 에는 예약된 작업으로 호출되는 Red Hat 제품의 엔트리포인트가 포함되어 있습니다. 예약된 작업은 인스턴스를 다른 취약성 관리 시스템과 동기화된 상태로 유지하여 취약성 정정 수명주기를 단순화합니다. 자동으로 실행됩니다. 예약된 작업을 수동으로 실행할 수도 있습니다.

각 통합 기록에 대해 구성된 실행 사용자가 있습니다. 이 사용자의 기본값은 VR입니다. 시스템. 이 값은 변경하지 마십시오.

사용 가능한 버전

최신 버전 취약성 솔루션 관리 및 Red Hat 솔루션의 경우 최신 버전이 취약성 대응 설치되어 있는지 확인하십시오.

설치 및 구성 취약성 솔루션 관리 과 솔루션 통합에 대한 자세한 내용은 해당 문서를 설치 도우미를 사용하기 위해 취약성 솔루션 관리 설치된 솔루션 통합 구성참조하십시오취약성 대응용 솔루션 관리 애플리케이션 설치.

의 릴리스 버전 취약성 대응	의 버전 취약성 솔루션 관리	릴리스 정보
취약성 대응 v15.0	v10.3	호환성 정보는 KB0856498 Vulnerability Response 호환성 매트릭스 및 릴리스 스키마 변경을 참조하십시오.

역할

Red Hat Solution Integration작업에는 sn_vul.configure_rhsa_integration 역할이 포함됩니다.

가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

Red Hat Solution Integration

을(를 Red Hat Solution Integration) 보려면 다음으로 이동하십시오. 취약성 대응 〉 관리 〉 통합.

기본 시스템에는 다음과 같은 통합이 포함되어 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Red Hat 통합

통합	설명
Red Hat Solution Integration	솔루션 및 NVD(국가 취약성 데이터베이스) 매핑을 검색하여 솔루션을 취약성, 취약한 항목 및 정정 작업과 연결합니다.

솔루션

임포트한 솔루션을 목록에서 보려면 문서를 솔루션 보기참조하십시오.

Rapid7 솔루션 관리

솔루션은 데이터 웨어하우스 또는 Rapid7 InsightVM. Rapid7 데이터 웨어하우스에서 가져온 Rapid7 취약성 통합Rapid7 알려진 정정입니다. 데이터 웨어하우스는 솔루션과 대체 솔루션을 모두 가져옵니다. Rapid7 InsightVM를 사용하면 Rapid7 취약한 항목 통합 API(Functional Item Integration)의 일부로 솔루션을 얻을 수 있습니다.

의 버전 21.0 취약성 대응부터 솔루션에 의해 Rapid7 InsightVM솔루션이 생성되는 방식이 변경되었습니다. 이제 Rapid7 InsightVM**solution_summary**, **solution_fix** 또는 **solution_type** 필드에 의존하는 대신 스캐너에서 제공하는 solution_id 사용하여 솔루션을 생성합니다. 즉, 이러한 필드가 비어 있더라도 솔루션 ID를 사용할 수 있는 한 솔루션이 생성됩니다.

임포트한 솔루션을 목록으로 보려면 다음으로 이동하십시오. **Rapid7** 〉 솔루션.

플러그인이 취약성 솔루션 관리 활성화되면 최신 버전은 Rapid7 취약성 통합 솔루션과 관련된 다음과 같은 주요 기능을 제공합니다.

- 솔루션 Rapid7 관리가 취약성 솔루션 관리로 이동됩니다.
- 데이터 웨어하우스를 위한 새로운 통합 Rapid7 필수 솔루션 관리가 도입되었습니다. 통합은 데이터 웨어하우스에서 Rapid7 필수 구성요소 솔루션을 가져옵니다.
- 타사 항목(TPE)의 Rapid7(솔루션) 관련 목록이 숨겨져 있습니다.
- 이전에 임포트한 데이터를 새 데이터 모델에서 볼 수 있습니다. Rapid7 솔루션, 솔루션 대체 및 취약성 솔루션 맵이 다시 임포트되고 다음 이후 임포트 필드가 비어 있게 설정됩니다. 이 필드는 솔루션 관리에서 채워집니다.
- 탐지가 업데이트되어 솔루션 필드가 채워집니다. 탐지는 취약성 솔루션 관리의 일부인 솔루션을 보여줍니다.
- Rapid7 데이터 웨어하우스의 Rapid7 TPE에 대한 기본 솔루션을 설정하는 동안 다른 솔루션보다 높은 기본 설정을 얻습니다.
- 솔루션은 에 대한 Rapid7 InsightVM탐지에서 VI(취약한 항목)로 롤업됩니다.

> **주:**
> 플러그인을 활성화 취약성 솔루션 관리 하지 않은 경우 애플리케이션이 그대로 작동합니다.

취약성 솔루션 관리

플러그인을 Rapid7 활성화하면 취약성 솔루션 관리 데이터 웨어하우스와 Rapid7 InsightVM 취약성 Rapid7 솔루션 [sn_vul_solution] 테이블에 대한 솔루션이 모두 채워집니다. 그러나 플러그인을 활성화하지 않은 경우 Rapid7 취약성 통합 해당 플러그인은 취약성 솔루션 관리 그대로 작동하며 사용자 지정 [sn_vul_r7_solution] 테이블에서 솔루션을 임포트합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약성 솔루션 테이블을 보려면 다음으로 이동하십시오. 모두 〉 취약성 대응 〉 취약성 솔루션 여기에서 여러 벤더의 솔루션을 보고 비교할 수 있습니다. 사용자 지정 테이블에서 임포트한 솔루션을 보려면 다음으로 이동합니다. 모두 〉 **Rapid7** 취약성 통합 〉 솔루션.

주:
벤더를 기준으로 솔루션을 보려면 소스별로 그룹화합니다.

Rapid7 필수 솔루션 관리 통합

플러그인을 활성화하면 취약성 솔루션 관리 수정 스크립트가 실행되고 통합 순서가 변경됩니다. 데이터 웨어하우스를 위한 Rapid7 새로운 Rapid7 필수 솔루션 통합은 솔루션을 필수 솔루션과 매핑합니다. 통합은 다음 순서로 실행됩니다.

1. Rapid7 솔루션 통합
2. Rapid7 필수 솔루션
3. Rapid7 대체 솔루션 통합
4. Rapid7 취약성 솔루션 맵 통합
5. Rapid7 VI 솔루션 통합(v19.0 취약성 대응부터)

주:
통합을 수동으로 실행하는 경우 솔루션 통합으로 Rapid7 시작합니다 . 통합에서 다음 통합 체인을 Rapid7 변경하지 마십시오. 시퀀스는 다음 통합 열에 정의됩니다.

TPE의 Rapid7 (솔루션) 관련 목록

플러그인을 활성화 취약성 솔루션 관리 한 경우 다음을 수행할 수 있습니다.

- 다음으로 이동하여 TPE를 볼 수 있습니다. 모두 〉 취약성 대응 〉 외부 공급업체.
- 이전 릴리스에서 사용할 수 있었던 솔루션(Rapid7) 관련 목록을 볼 수 없습니다.
- 솔루션 관련 목록에서 RedHat, Microsoft(MSRC) 등 다른 소스의 솔루션과 함께 Rapid7 관련 솔루션을 볼 수 있습니다.

플러그인을 활성화 취약성 솔루션 관리 하지 않은 경우 다음과 같은 상황이 발생합니다.

- 관련 목록 기능은 동일하게 유지됩니다.
- 솔루션(Rapid7) 관련 목록을 볼 수 있습니다.
- 솔루션 관련 목록이 숨겨져 있습니다.

TPE 및 VI에 대한 기본 솔루션

Rapid7 타사 항목(TPE) 수준 및 Rapid7 InsightVM 탐지 수준에서 데이터 웨어하우스에서 솔루션을 가져옵니다.

데이터 웨어하우스의 Rapid7 경우 솔루션은 다음과 같은 방식으로 관리됩니다.

- 기본 솔루션은 취약성 및 솔루션 매핑에 따라 TPE에 설정됩니다.
- 의 Rapid7 취약성에 대체 가능성이 가장 높은 단일 솔루션이 Rapid7있는 경우 해당 취약성에 연결된 벤더의 다른 솔루션과 관계없이 기본 솔루션으로 설정됩니다.
- 그 외 모든 경우에는 기본 솔루션의 플로우가 동일하게 유지됩니다. 기본 솔루션의 기본 동작에 대한 자세한 내용은 다음 문서를 참조하십시오 취약성 솔루션 관리.

의 경우 Rapid7 InsightVM솔루션은 다음과 같은 방식으로 관리됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 기본 솔루션은 탐지에서 VI로 롤업됩니다.
- 에서 Rapid7단일 탐지 및 솔루션이 있는 경우 해당 솔루션은 VI로 롤업됩니다.
- 여러 탐지가 있고 모두 의 동일한 솔루션을 Rapid7포함하는 경우 솔루션이 VI로 롤업됩니다.
- 여러 탐지에 의 여러 솔루션이 Rapid7있는 경우 최신 솔루션이 VI로 롤업됩니다.

의 취약성 대응v19.0부터 Rapid7 Data Warehouse에서 생성된 기본 솔루션은 에 대한 취약성 솔루션 관리필요성을 우회하여 Rapid7 취약한 항목에 직접 채워집니다. 이러한 변경을 통해 이러한 취약한 항목에 대한 잠재적 솔루션에 대한 불확실성이 제거됩니다.

를 통해 Rapid7이러한 직접 채우기를 달성하기 위해 다음 단계가 수행됩니다.

- 새로운 통합인 Rapid7 VI 솔루션 통합이 설정되고 기존 Rapid7 취약성 통합 워크플로우에 통합됩니다.
- 새 테이블 〔sn_vul_r7_rapid7_vi_solution_import〕이(가) 생성됩니다.
- 새 변환 맵 Rapid7 VI 솔루션 변환이 생성됩니다.
- 스크립트 포함 Rapid7AssetsImportProcessor는 내에서 취약성 솔루션 관리Rapid7에 의해 생성된 솔루션의 처리를 제외하도록 수정됩니다.

Rapid7 VI 솔루션 통합이 실행되면 에서 Rapid7 얻은 처리되지 않은 데이터가 새로 생성된 테이블에 저장됩니다. 이어서 Rapid7 VI 솔루션 변환이 트리거되어 이 데이터를 처리하고 기본 솔루션을 취약한 항목 테이블에 직접 채웁니다.

주:
Rapid7 VI 솔루션 통합은 플러그인이 설치된 경우에만 취약성 솔루션 관리 기본 설정 솔루션을 채웁니다.

v22.0 of 취약성 대응부터 의 솔루션은 Rapid7 예약된 작업을 *Process Vulnerability Solutions Metrics Queue*실행할 때 더 이상 큐에 대기하지 않습니다. 이 예약된 작업에는 NVD 항목에서 외부 공급업체 항목으로 솔루션을 롤업하고, 취약성에 대한 기본 솔루션을 채우고, 솔루션의 정정 상태 메트릭을 업데이트하는 작업이 포함됩니다. 다음 시나리오에서는 정정 상태 메트릭만 업데이트해야 합니다.

- 취약성에 대해 기본 솔루션이 변경되는 경우
- VIT가 생성되거나 삭제될 때
- VIT 임포트가 완료된 경우

솔루션은 정정 상태 메트릭만 업데이트하기 위해 큐에 대기하지만 NVD 항목에서 외부 공급업체 항목으로 솔루션을 롤업하고 기본 솔루션을 채우려고 시도합니다. 이 프로세스를 최적화하기 위해 취약성 솔루션 테이블에 업데이트 상태 열이 도입되었습니다. NVD 항목에서 외부 공급업체 항목으로 솔루션을 롤업하거나 기본 솔루션을 채울 필요 없이 솔루션의 정정 상태 메트릭을 업데이트해야 하는 경우 해당 항목이 더 이상 큐에 대기하지 않습니다. 대신 업데이트 상태 열이 true로 직접 업데이트됩니다. 이 접근 방식을 사용하면 정정 상태 메트릭만 업데이트해야 하는 케이스를 처리할 수 있으므로 시간과 리소스가 절약됩니다. 예약된 작업에서 큐에 대기 중인 솔루션의 처리가 완료되면 업데이트 상태가 true로 표시된 솔루션이 식별됩니다. 그런 다음, 이러한 솔루션을 반복하여 개수를 계산하고 그에 따라 정정 상태 메트릭을 업데이트합니다. 이 단계는 큐에 대기해야 하는 솔루션 수가 줄어들기 때문에 예약된 작업의 성능을 개선하는 데 중요한 역할을 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약성에 대해 **Rapid7** 데이터 웨어하우스에서 임포트한 솔루션 대체 체인

취약성 솔루션을 선택하고 대체 솔루션 관련 목록을 선택하여 솔루션에 대한 대체 솔루션을 볼 수 있습니다. 이전 솔루션 관련 목록을 선택하여 이전 솔루션을 볼 수 있습니다. TPE에 솔루션을 부착하면 해당 솔루션의 대체 솔루션이 해당 TPE에 부착됩니다.

시스템 속성별로 그래프에서 솔루션 대체 체인의 최대 깊이 변경

데이터 모델에서 받은 솔루션 대체 체인이 Rapid7 너무 길어서 기본 솔루션을 채우는 동안 그래프를 생성할 수 없습니다. 따라서 체인의 깊이를 제한하기 위해 값 500으로 명명된 *sn_vul.max_recursion_depth* 시스템 속성이 생성됩니다. 체인 깊이가 500보다 크면 체인의 나머지 부분은 무시됩니다. 체인의 최대 깊이를 변경하려면 [sys_properties] 테이블로 이동하여 속성 값을 변경합니다.

애플리케이션 업그레이드 **Rapid7**

플러그인을 업그레이드 Rapid7 취약성 통합 하고 아직 플러그인을 활성화 취약성 솔루션 관리 하지 않은 경우 애플리케이션이 그대로 작동합니다.

애플리케이션을 업그레이드 Rapid7 하기 전이나 후에 플러그인을 활성화 취약성 솔루션 관리 하든, 다음 통합에 대해 다음 이후 임포트 필드는 빈 상태로 유지됩니다.

- Rapid7 대체 솔루션 통합
- Rapid7 취약성 솔루션 맵 통합
- Rapid7 솔루션 통합

> **주:**
> 다음 통합 실행에서 데이터가 취약성 솔루션 테이블에 채워집니다.

의 경우 Rapid7 InsightVM데이터는 탐지 수준에서 수신됩니다. 통합이 Rapid7 InsightVM 실행되면 취약성 솔루션 테이블에 솔루션이 임포트됩니다.

모든 솔루션 벤더에서 데이터를 수집하는 일반 프레임워크

솔루션 인텔리전스 통합을 위한 일반 프레임워크를 사용하여 솔루션 벤더에서 제공하는 다양한 파일 형식의 데이터 수집을 지원할 수 있습니다. 이러한 형식은 정보 교환 및 처리 속도를 높이고 표준화된 보고 형식으로 중요한 보안 관련 정보를 쉽게 공유할 수 있도록 합니다.

지원되는 파일 형식은 다음과 같습니다.

공통 취약성 보고 프레임워크(CVRF)

CVRF(Common Vulnerability Reporting Framework)는 XML 기반 언어입니다. , Red Hat, Cisco및 와 Microsoft 같은 Oracle주요 벤더는 CVRF 형식을 지원합니다.

CSAF(일반 보안 자문 프레임워크)

CSAF(Common Security Advisory Framework)는 JSON 기반의 구조화되고 머신이 읽을 수 있는 보안 권고를 제공하는 오픈 소스 표준입니다. Siemens, Red Hat, Hitachi 및 Schneider와 같은 주요 공급업체는 CSAF 형식을 지원합니다.

CVRF 또는 CSAF 지원 솔루션 관리에는 다음과 같은 주요 기능이 포함됩니다.

- 설정 도우미를 통한 구성
- 파일 임포트를 통한 CVRF 또는 CSAF 데이터 임포트 지원
- CVRF 또는 CSAF URL을 통한 CVRF 또는 CSAF 데이터 임포트 지원
- 권고를 통한 CVRF 또는 CSAF 데이터 임포트 지원
- 관련 취약성이 있는 솔루션 매핑

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약성 대응 플러그인은 생성된 솔루션의 메트릭 상태 업데이트를 처리합니다.

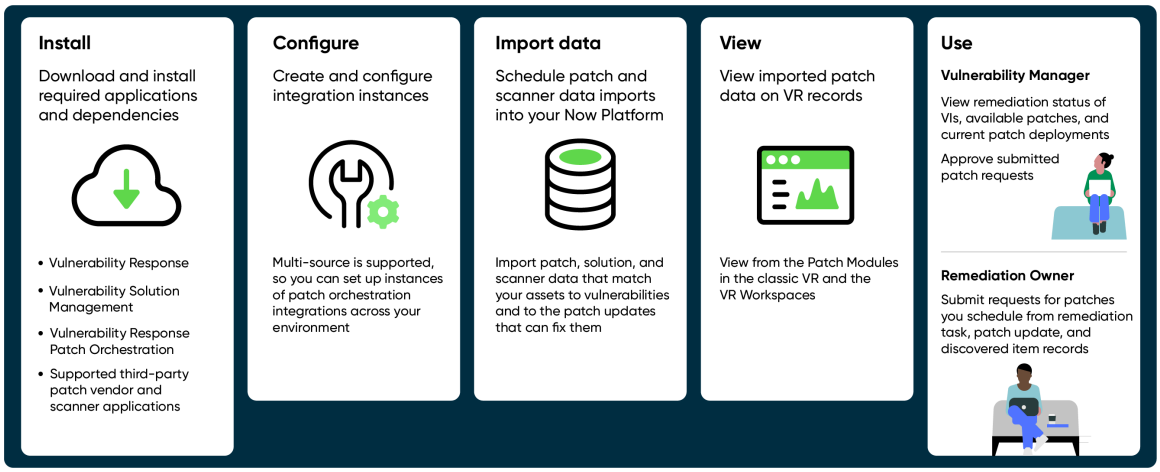
솔루션 제공자를 구성하는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 취약성 솔루션 제공자 구성.

다음으로 오케스트레이션 패치 취약성 대응

를 사용한 취약성 대응Patch 오케스트레이션을 사용하여 대규모 자산 그룹의 중요한 취약성에 대한 패치 및 패치 배포를 관리할 수 있습니다. 취약성 대응 패치 오케스트레이션 및 패치 오케스트레이션 통합은 에서 사용할 수 있습니다 ServiceNow# Store.

를 사용한 패치 오케스트레이션 이해 취약성 대응

를 포함한 취약성 대응 패치 오케스트레이션은 타사 솔루션 통합, 패치 벤더 및 취약성 스캐너에서 예약된 임포트의 데이터를 사용합니다. 이 데이터는 애플리케이션에서 상관 관계가 지정됩니다 취약성 대응 . 이 데이터 구성을 통해 취약성 정정 주기의 단계를 완료할 수 있습니다. 취약성 식별부터 시작하여 패치와 업데이트를 적용하고 마지막으로 인스턴스 내에서 ServiceNow AI Platform# 타사 스캐너 데이터를 사용하여 취약한 항목을 종결합니다.



를 사용한 취약성 대응 패치 오케스트레이션은 클래식 환경과 취약성 대응 작업 공간 모두에서 지원됩니다.

작업 공간의 패치 오케스트레이션에 대한 자세한 내용은 다음 문서를 참조하십시오 작업 공간으로 취약성 대응 오케스트레이션 패치.

의 취약성 대응패치 오케스트레이션을 사용하면 취약성 관리자와 분석가 및 IT 정정 전문가가 다음과 같은 정정 작업을 수행할 수 있습니다.

- 솔루션(패치)을 구성하는 패치 유형 및 벤더에 대한 자세한 컨텍스트와 정보를 참조하십시오.
- 작업 공간 또는 클래식 환경의 기록에서 취약성 및 솔루션 데이터뿐만 아니라 취약성 정정 진행 상황도 취약성 대응 보고 모니터링합니다.
- 외부 공급업체 솔루션 벤더가 지원하는 , CentOS, macOS, Oracle및 기타 자산에 대해 Windows정기적이고 예약된 간격으로 패치를 배포합니다. 근무 시간 외 시간에 패치를 예약하여 작업 중인 패치와의 충돌을 피할 수 있습니다.
- 외부 공급업체 스캐너에서 제공하는 임포트한 탐지 데이터를 사용하여 취약성이 있지만 패치되지 않았거나 예약된 패치로 업데이트되지 않은 자산을 식별합니다.
- 애플리케이션에서 패치 업데이트, 정정 작업 및 검색된 항목 기록의 업데이트가 필요한 자산에 대해 사용 가능한 패치를 시작하고 예약합니다 취약성 대응 .
- 정정 전문가가 제출한 패치 요청에 대한 선택적 승인 프로세스를 통해 패치 배포를 모니터링합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주요 용어

CI(구성 항목)

CI는 CMDB(구성 관리 데이터베이스)에 나열된 기존 자산입니다.

VI(취약한 항목)

CMDB의 기존 자산과 일치하는 임포트한 취약성입니다. 취약한 항목(VIT)은 VI에 대한 정정 작업을 지정하는 특정 기준에 따라 정정 작업 또는 목록으로 그룹화됩니다.

인스턴스

솔루션 벤더 애플리케이션의 고유한 계정을 참조합니다. 예를 들어, 각 사용자 계정은 HCLD BigFix 애플리케이션의 인스턴스가 될 수 있습니다. 이 용어는 인스턴스에 대한 고유하고 안전한 웹 주소를 의미하기도 합니다 ServiceNow AI Platform# .

솔루션

이러한 통합의 맥락에서 솔루션에는 두 가지 유형, 즉 잠재적 솔루션과 기본 솔루션이 있습니다. 잠재적 솔루션은 취약성을 해결할 수 있는 솔루션입니다. 취약성에는 종종 많은 잠재적인 솔루션이 있습니다. #기본 솔루션은 탐지된 특정 취약성에 대해 가장 효과적인 솔루션과 일치합니다.

패치

취약성을 수정하는 소프트웨어 업데이트. 패치 벤더는 패치에 대해 고유한 이름을 사용합니다(예: HCL BigFix 애플리케이션에서 패치는 Fixlet이라고 합니다).

기본 패치

기본 패치는 특정 취약점을 수정하기 위한 소프트웨어 업데이트입니다. 패치가 배포되면 특정 취약성과 관련된 취약한 항목에 매핑되어 수정합니다.

배포

이 통합을 위한 배포는 컴퓨터에 패치를 적용, 시작 또는 예약하는 경우를 의미합니다.

의 ServiceNow AI Platform 배포는 다중 소스를 지원하는 통합을 참조할 수도 있습니다. 단일 통합 존재를 통합의 배포라고 합니다. 배포는 환경 전반의 통합 및 제품을 의미합니다. 예를 들어, 사용자 환경에 타사 스캐너 또는 솔루션 벤더 통합이 여러 개 배포되어 있을 수 있습니다.

패치 오케스트레이션 통합에 필요한 애플리케이션 및 의존성의 사용 가능한 버전

- 취약성 대응 애플리케이션 및 의존성 플러그인, 보안 지원 공통 및 보안 지원 오케스트레이션.
- 취약성 솔루션 관리.
- 취약성 대응 패치 오케스트레이션 애플리케이션은 다음에서 사용할 수 있습니다 ServiceNow# Store.
- HCL BigFix와의 취약성 대응 패치 오케스트레이션 통합 또는 Microsoft SCCM과의 취약성 대응 패치 오케스트레이션 통합과 같이 지원되는 외부 공급업체 패치 벤더 애플리케이션
- Vulnerability Response와의 외부 공급업체 스캐너 통합을 지원합니다.

필요한 역할

사용자에게는 애플리케이션에서 데이터를 보고 패치를 취약성 대응 예약하는 데 사용 중인 패치 오케스트레이션 통합과 관련된 역할이 필요합니다. 자세한 내용은 아래 나열된 지원되는 통합에 대한 구성 정보를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 와 HCL BigFix 패치 오케스트레이션의 통합 이해 취약성 대응및 Microsoft SCCM과의 취약성 대응 패치 오케스트레이션 통합.
- 취약성 대응 작업 공간 및 클래식 환경에서 사용자가 데이터를 볼 수 있지만 편집할 수 없는 sn_vul_patch_orch.read_patch 역할은 sn_vul.remediation_owner 및 sn_vuln.vulnerability_analyst 역할로 상속됩니다.

  패치 벤더에 대한 연결을 구성하고 패치를 예약하는 데 필요한 할당해야 하는 역할은 통합에 따라 다릅니다. 자세한 내용은 MS SCCM으로 취약성 대응 패치 오케스트레이션을 참조하십시오HCL BigFix와의 취약성 대응 패치 오케스트레이션 통합 구성.

애플리케이션에 포함된 패치 요청에 대한 제출 및 승인 프로세스가 있습니다. 기본적으로 시스템 속성은 인스턴스의 취약성 대응 패치 오케스트레이션 애플리케이션에서 ServiceNow AI Platform [**sn_vul_patch_orch.patch_approval_required**] 활성화됩니다.

이 시스템 속성은 패치 배포가 예약될 때 수준 1 - 패치 업데이트 승인 그룹에 할당된 사용자에게 검토 및 승인을 위해 제출되도록 활성화됩니다. sn_vul_patch_orch.configure_patch 역할의 사용자가 승인 없이 패치를 예약하도록 하려면 [**sn_vul_patch_orch.patch_approval_required**] 속성을 비활성화할 수 있습니다. 예약된 패치가 정상 작업 시간과 상충되지 않도록 승인을 활성화된 상태로 두는 것을 선호할 수 있습니다. 승인 시스템 속성을 비활성화하면 sn_vul_patch_orch.configure_patch 역할을 가진 모든 사용자가 검토 및 승인 없이 패치를 예약하고 배포할 수 있습니다.

자세한 내용 및 이 시스템 속성을 비활성화하는 방법은 지원되는 통합의 구성 항목을 참조하십시오.

- HCL BigFix와의 취약성 대응 패치 오케스트레이션 통합 구성.
- SCCM 통합을 사용하여 Microsoft 취약성 대응 패치 오케스트레이션 구성.

기록에서 취약성 대응 패치 예약

정정 전문가는 패치 업데이트를 예약하여 취약한 항목을 해결하고 애플리케이션의 모든 기록 취약성 대응 에서 정정 진행 상황을 모니터링할 수 있습니다.

다음 기록에서 패치를 예약할 수 있습니다.

- 패치 업데이트
- 정정 작업
- 검색된 항목

에서 활성 **VI** 카운트를 롤업하는 기록 취약성 대응

모든 패치를 모든 취약성에 롤업할 때 잠재적인 성능 문제를 방지하기 위해 변경 사항을 선택하는 예약된 작업은 활성 VI 카운트만 수정합니다. 이러한 카운트 변경 및 관련 데이터는 애플리케이션의 다음 기록으로 롤업됩니다.취약성 대응

- VIT(취약한 항목)
- RT(정정 작업)
- 취약성 솔루션
- 패치 업데이트

패치 데이터 및 패치 데이터 롤업을 보고 솔루션 없이 패치를 보는 방법에 대한 자세한 내용은 다음 주제를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 의 패치 오케스트레이션에 대한 패치 데이터 및 상태 롤업 취약성 대응.
- 에서 패치 데이터 보기 및 패치 스케줄링 취약성 대응.
- 에서 솔루션이 없는 패치 보기 취약성 대응.

패치로 취약한 항목 대량 편집

클래식 환경의 패치가 있는 클래식 환경에서 취약한 항목을 대량 편집할 수 있습니다. 대량 편집의 작동 방식에 대한 자세한 내용은 다음 문서를 참조하십시오 에서 취약한 항목을 대량으로 편집 취약성 대응. 대량 편집을 위해 선택한 모든 VI에 대한 기본 설정 패치입니다. 편집에 대한 이 옵션은 선택한 모든 VI에 매핑된 기본 패치가 있는 경우에만 작동합니다.

Patch Management Data Model 개선 사항

패치 관리 데이터 모델 플러그인 — VR 패치 오케스트레이션 애플리케이션에서 현재 사용되는 데이터 모델을 캡슐화하는 독립 실행형 무료 플러그인입니다. 여기에는 수집, 패치 업데이트, 패치 배포 등의 주요 테이블이 포함됩니다.

이 플러그인은 패치 관리 도구에서 ITSM, 취약성 대응 등의 애플리케이션에서 기존 워크플로우에 사용할 패치 관리 데이터를 수집하는 데 사용할 수 있습니다.

주요 개선 사항:

- 수집 장치, 패치 업데이트, 패치 배포 등의 기존 패치 오케스트레이션 플러그인의 테이블이 새 데이터 모델 플러그인으로 이동됩니다.
- 이전 테이블의 데이터가 기존 VR 패치 오케스트레이션 기능의 새 테이블로 마이그레이션됩니다.

예외 관리 개요

조직이 게시된 취약성 관리 또는 보안 정책, 표준 또는 가이드라인을 준수할 수 없는 경우 예외를 요청할 수 있습니다. 예외 관리에는 정책에 따라 정정할 수 없는 VI(취약한 항목) 또는 RT(정정 작업)에 대한 예외를 요청, 검토, 승인 또는 거부하는 작업이 포함됩니다.

일부 취약성에는 기존 패치, 수정 프로그램 또는 솔루션이 없을 수 있습니다. 예외가 승인되면 취약성을 수정하지 않은 결과를 인정하고 이에 동의하기 때문에 위험을 수락한다는 의미이기도 합니다.

예외의 수명주기

예외의 정의

예외는 지정된 기간 동안 VI 또는 RT의 정정을 연기하는 요청입니다. 예를 들어 정정 소유자는 머신에 패치를 사용할 수 없는 경우 예외를 요청할 수 있습니다.

예외 요청

정정 소유자는 예외 관리 프로세스를 사용하여 VI 또는 RT에 대한 면제를 요청할 수 있습니다. 예외 승인자가 이 요청을 승인하면 VI 또는 RT가 지연 상태로 전환됩니다.

예외 요청 승인

즉시 정정할 수 없는 VI 또는 RT는 취약성 분석가가 검토하고, 위험에 대해 평가하고, 정정할 수 있을 때까지 연기 승인을 받습니다. 예외 요청 승인은 2단계 워크플로가 될 수 있습니다. 첫 번째 수준 승인자만 있는 경우 예외를 요청하고 승인할 수 있습니다. 그러나 첫 번째 수준 승인자가 없으면 예외를 요청할 수 없습니다. 자세한 내용은 예외 승인자 추가 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

- v15.0부터 취약성 대응 VR 애플리케이션을 처음 배포하는 경우 예외 관리용 플로우 디자이너가 기본적으로 활성화됩니다. 워크플로우를 이미 사용 중인 경우 플로우 디자이너로 업데이트할 수 있습니다. 두 경우 모두 다시 워크플로우로 변경할 수 없습니다. 예외 관리 및 가양성에 대한 승인 규칙을 구성하려면 문서를 참조하십시오 예외 관리에 대한 승인 규칙 구성.

  VI 또는 RT에 대한 예외 요청이 승인되면 다음 작업을 수행할 수 있습니다.

  - 재개설
  - 삭제
  - 할당 대상 또는 할당 그룹 필드 업데이트

- v23.0 부터 취약성 대응예외 규칙 상태 승인 워크플로우는 더 이상 사용되지 않으며 Flow Designer의 플로우 예외 규칙 승인으로 대체됩니다.

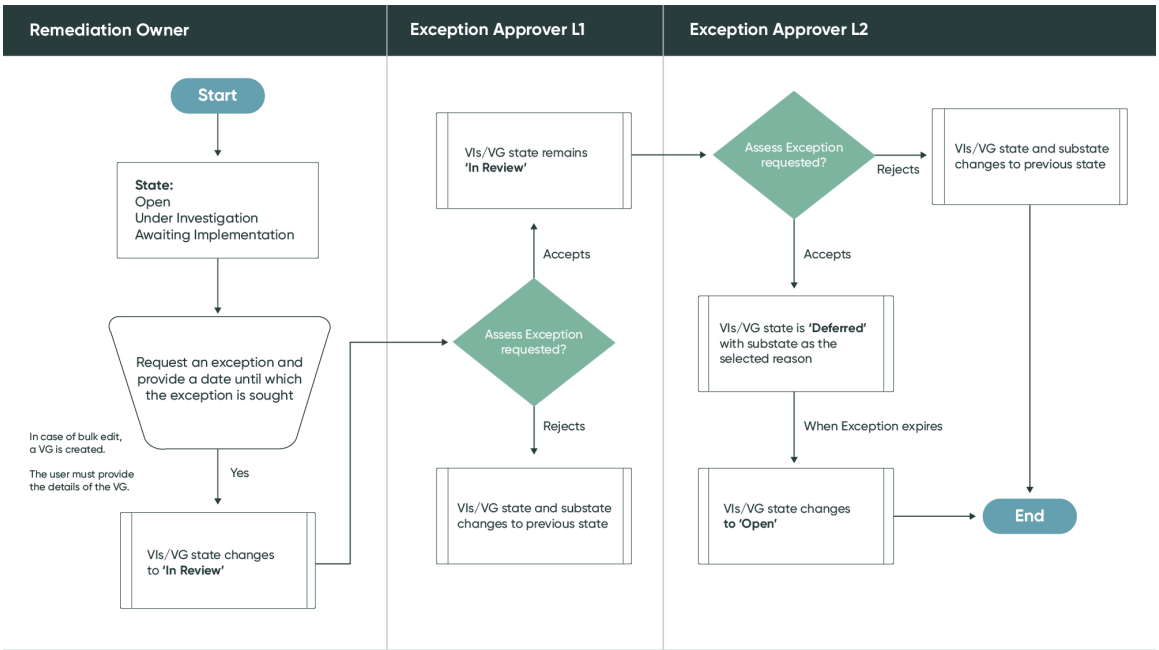
예외 요청 추적

예외를 발생시킨 후 VI 또는 RT의 상태 변경 승인 탭을 사용하여 상태를 추적할 수 있습니다. RT에서 동작이 수행되면 해당 RT에서 개별 VI의 상태를 추적할 수 없습니다.

예외 요청의 만료

특정 VI 또는 RT에 대한 예외 요청이 만료되면 영향을 받는 VI 또는 RT는 오픈 상태로 되돌아갑니다.

VR v15.0 이전의 예외 관리 승인 프로세스



단일 VI 또는 RT의 모든 VI가 다음 스캔을 통과하면 VI 및 RT 상태 필드 (해당되는 경우)가 하위 상태가 고정된상태로 종결됨으로 변경됩니다.

여러 지연

기록 또는 정정 작업이 지연된 횟수를 추적합니다. 예약된 작업인 *set deferral counts*는 매일 실행되어 VR용 여러 지연 모듈의 지연 횟수 열에 두 번 이상 지연된 기록에 대한 개수를 게시합니다. 정정 작업이 두 번 이상 지연된 경우 정정 작업과 연결된 기록에 대한 모든 카운트가 수집되고 게시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관련 정보

에서 정정 작업 및 기록에 대한 예외 요청 취약성 관리자 작업 공간

에서 예외 요청 IT 정정 작업 공간

에서 사용하는 예외 GRC: 정책 및 준수 관리 요청 IT 정정 작업 공간

예외 규칙 개요

에 대한 취약성 대응 예외 규칙을 사용하면 VI(취약한 항목)에 대한 지연 프로세스를 자동화할 수 있습니다. 영향을 받는 취약성, CI(구성 항목) 또는 VI를 식별하여 즉시 수정하거나 연기할 수 없는 VI(취약한 항목)에 대한 예외를 요청합니다. 시스템에서 VI 지연 프로세스를 자동화하여 일치하는 VI를 식별할 때 규칙에 따라 일치하는 VI를 지연시킵니다.

조직에서 예외 규칙 사용

승인된 규칙 조건과 일치하는 경우 예외 규칙을 사용하여 특정 기간 동안 신규 및 기존 VI를 자동으로 연기할 수 있습니다. 자동화는 서비스 수준 계약 누락 위험을 최소화하고 수동 개입을 제거하므로 여러 항목을 더 쉽게 관리할 수 있습니다.

지연 규칙은 순서를 지원합니다. 즉, 우선순위가 가장 높은 규칙이 먼저 실행됩니다. 우선순위가 높은 규칙이 VI에 적용되면 조건이 VI와 일치하더라도 후속 규칙이 다시 적용되지 않습니다.

주:

- 예외 관리 구성에서 선택하는 취약성 대응 경우에만 규칙을 만들 수 있습니다. 자세한 내용은 에 대한 예외 관리 구성 취약성 대응 문서를 참조하십시오.
- VI가 예외 규칙에 의해 지연되면 생성된 지연 정정 작업(RT)으로 복사됩니다. VI는 이전에 속했던 RT의 일부입니다.

예외 규칙의 수명주기는 다음과 같습니다.

- 예외 규칙 생성
- 예외 규칙 요청 승인
- 예외 규칙 활성화
- 예외 규칙 연기
- 예외 규칙의 만료

예외 규칙 생성

지정된 기간 동안 정의된 조건과 일치하는 VI를 자동으로 지연시키는 예외 규칙을 생성할 수 있습니다. 예외 규칙을 생성한 후 승인을 위해 제출합니다.

예외 규칙 요청 승인

예외 규칙 요청 승인은 2단계 프로세스입니다. 첫 번째 수준 승인자만 있는 경우 단일 승인으로 예외 규칙을 평가하고 승인할 수 있습니다. 그러나 첫 번째 수준 승인자가 없으면 예외 규칙 승인을 승인할 수 없습니다. 규칙이 승인되면 정정 작업(RT)이 생성됩니다. 자세한 내용은 예외 규칙 요청 승인 문서를 참조하십시오.

주:

v15.0부터 취약성 대응 VR 애플리케이션을 처음 배포하는 경우 예외 관리용 플로우 디자이너가 기본적으로 활성화됩니다. 워크플로우를 이미 사용 중인 경우 플로우 디자이너로 업데이트할 수 있습니다. 두 경우 모두 다시 워크플로우로 변경할 수 없습니다. 예외 관리 및 가양성에 대한 승인 규칙을 구성하려면 문서를 참조하십시오 예외 관리에 대한 승인 규칙 구성.

예외 규칙 요청이 승인된 후 다음 작업을 수행할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 취소
- 삭제

예외 규칙 활성화

예외 규칙이 승인되면 정정 작업은 기본적으로 연기됨 상태로 생성됩니다. "유효 기간(시작)" 날짜부터 예외 규칙은 생성된 모든 VI와 종결 상태에서 오픈 상태로 전환된 VI에서 실행됩니다.

주:
기존 데이터에서 실행 옵션을 사용하도록 설정하면 예약된 작업이 "유효 기간(시작)" 날짜에 기존 데이터에서 한 번 실행됩니다.

예외 규칙 연기

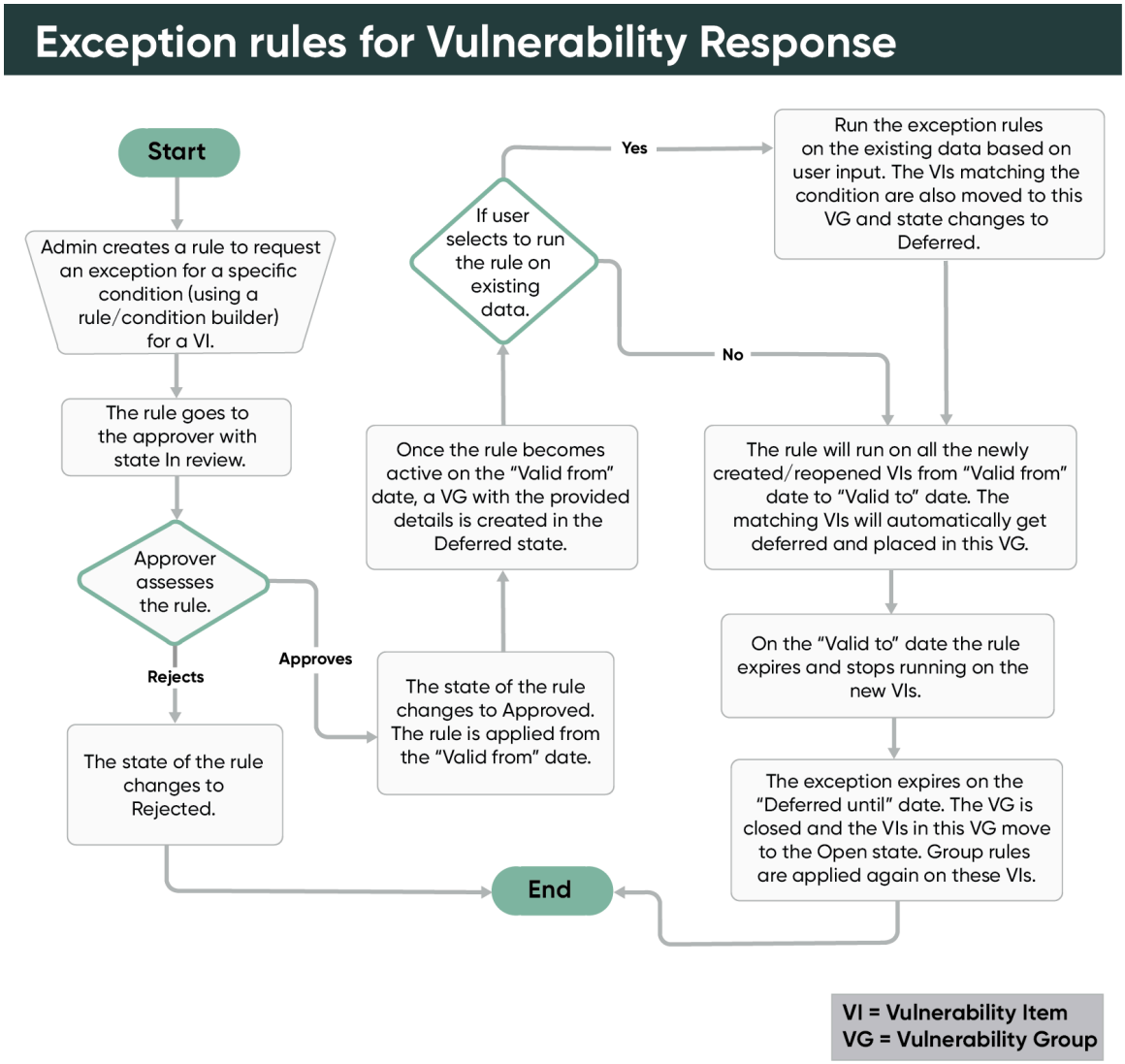
이 예외 규칙에 정의된 조건과 일치하는 VI를 규칙에 정의된 "연기 기한" 날짜까지 연기할 수 있습니다. 이 날짜에 예외 규칙에 대해 생성한 정정 작업이 종결되고 이 그룹의 모든 VI가 열림 상태로 돌아갑니다. 필요한 RT에 할당하기 위해 그룹 규칙이 다시 적용됩니다.

예외 규칙의 만료

예외 규칙이 만료되면 새 VI 또는 다시 열린 VI에서 더 이상 실행되지 않습니다. 연결된 RT는 "Deferred until" 날짜까지 Deferred 상태로 유지됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

v15.0 이전의 예외 규칙 작업 흐름



제외 규칙 개요

제외 규칙은 에서 수집 프로세스 취약성 대응중에 탐지가 취약한 항목(VIT)으로 변환되지 않도록 필터링하거나 제외하는 방법을 제공합니다.

이러한 규칙은 다음과 같은 다양한 시나리오를 처리하도록 설정할 수 있습니다.

- 심각도가 낮거나 즉각적인 정정이 필요하지 않은 위험은 제외됩니다.
- 작업에 가장 중요한 VIT의 우선순위를 지정하여 정정 프로세스를 개선합니다.
- VIT 변환에서 탐지 백분율을 제외하여 데이터를 임포트하는 동안 처리 시간을 단축합니다.

데이터를 수집하는 과정에서 신규 및 기존 탐지를 처리하기 위한 고유한 접근 방식이 있습니다.

- 새 탐지의 경우:
  - 새 탐지가 제외 규칙의 조건을 충족하지 않으면 VIT를 사용하여 탐지가 생성됩니다.
  - 새 탐지가 제외 규칙의 조건을 충족하면 규칙이 탐지와 연결되지만 VIT는 생성되지 않습니다. 탐지 기록에서 일치하는 제외 규칙 참조를 채웁니다. 제외 규칙 열은 그에 따라 탐지 기록에 대한 제외 규칙 참조로 채워집니다.
- 기존 탐지의 경우:

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 탐지가 제외 규칙의 조건을 충족하지 않으면 일반 워크플로우를 진행합니다.
- 기존 탐지가 제외 규칙의 조건과 일치하는 경우 해당 탐지와 연결된 VIT는 현재 상태로 유지되지만 규칙은 탐지와 연결됩니다. VIT의 상태는 속성에 정의된 *sn_vul.close_vit_with_excluded_detections* 값에 의해 제어됩니다. 기본적으로 이 속성의 값은 False로 설정됩니다. 값이 아니오로 설정되면 VIT의 탐지가 제외되고 VIT의 상태가 현재 상태로 유지됩니다. 그러나 값을 True로 설정하면 다음과 같은 시나리오가 발생할 수 있습니다.
  - VIT의 모든 탐지가 제외되면 VIT의 상태가 종결된 제외됨으로 업데이트됩니다.

    주:
    v22.1.2 취약성 대응 부터 Excluded라는 새로운 하위 상태가 추가되었습니다.

  - 하나의 탐지가 종결됨으로 표시되고 나머지는 제외되면 VIT는 고정 종결로 지정됩니다.
  - VIT에 오픈 탐지가 있는 경우 VIT는 오픈 상태로 유지됩니다.

관련 정보

제외 규칙 생성

긍정 오류 개요

가양성은 스캐너에서 시스템에 취약성이 존재한다고 보고하지만 실제로는 취약성이 없는 조건입니다. 스캐너의 잘못된 분류, 부적절한 논리 또는 알고리즘과 같은 여러 가지 이유가 있을 수 있습니다. 정정 소유자는 VI(취약한 항목) 또는 RT(정정 작업)를 가양성으로 표시할 수 있습니다.

중요사항:
에서 호스트 취약한 항목을 대량으로 오탐지로 표시할 수 있습니다 취약성 관리자 작업 공간. 호스트 취약한 항목을 대량으로 가양성으로 표시하는 방법에 대한 자세한 내용은 문서를 참조하십시오 취약성 관리자 작업 공간에서 가양성에 대한 대량 편집.

긍정 오류의 수명주기

긍정 오류의 의미

스캐너는 때때로 경고를 표시하지만 실제로는 취약점이 없습니다. 예를 들어 구성 항목이 해제되었지만 스캐너에서 여전히 이와 관련된 문제를 제기하는 경우 이를 가양성으로 표시합니다.

긍정 오류로 표시

VI 또는 RT를 긍정 오류로 표시하는 방법에 대한 자세한 내용은 다음을 참조하십시오 긍정 오류로 표시.

거짓 긍정 작업

VI 또는 RT가 긍정 오류로 표시되면 상태가 종결됨으로 업데이트되고 하위 상태가 긍정 오류로 변경됩니다. 다음 작업을 수행할 수 있습니다.

- 재개설
- 삭제
- 종료 필드에 날짜를 업데이트합니다. 그런 다음 이 날짜는 가양성의 만료 날짜로 사용됩니다.

주:
승인되지 않으면 VI 또는 RT가 이전 상태로 되돌아갑니다.

긍정 오류 승인

승인자는 승인 워크플로우에서 긍정 오류를 승인할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

Vulnerability Response v15.0부터 VR 애플리케이션을 처음 배포하는 경우 예외 관리용 플로우 디자이너가 기본적으로 활성화됩니다. 워크플로우를 이미 사용 중인 경우 플로우 디자이너로 업데이트할 수 있습니다. 두 경우 모두 다시 워크플로우로 변경할 수 없습니다. 예외 관리 및 가양성에 대한 승인 규칙을 구성하려면 문서를 참조하십시오 예외 관리에 대한 승인 규칙 구성.

긍정 오류 다시 열기

긍정 오류 하위 상태의 VI 또는 RT는 언제든지 다시 열 수 있습니다.

긍정 오류 추적

상태 변경 승인 섹션을 사용하여 가양성의 상태를 추적합니다. 승인되면 VI 또는 RT의 상태가 종결로 업데이트되고 그 이유는 긍정 오류로 업데이트됩니다.

긍정 오류 만료

긍정 오류 승인자만 VI 또는 RT가 만료되도록 긍정 오류에 대해 종료 날짜를 설정할 수 있습니다. 또한 승인자가 종료 날짜를 제공한 긍정 오류만 만료될 수 있습니다. 이 날짜는 긍정 오류가 승인된 후에 제공될 수 있습니다.

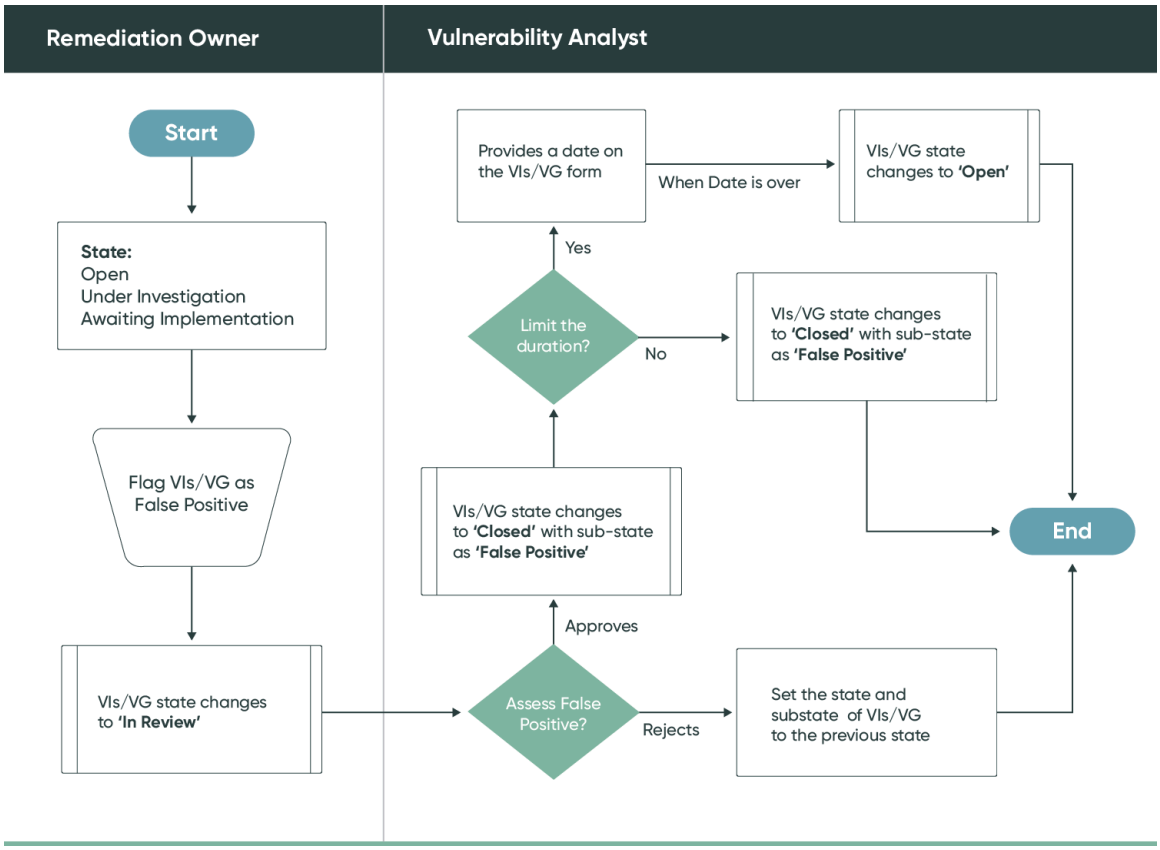
종료 날짜가 없는 가양성은 영구적인 가양성입니다. 거짓 긍정이 만료되면 VI 또는 VR의 상태가 다시 열림으로 이동합니다.

주:

v21.0 부터 취약성 대응설정된 일 수 후에 승인자와 요청자 모두에 대한 이메일 알림과 함께 긍정 오류 및 예외를 승인하기 위한 시간 범위를 구성할 수 있습니다. 요청이 발생하면 취약한 항목이 검토 중 상태로 변경되고 상태 변경 기록이 생성됩니다. 승인자가 구성된 시간 범위 내에 응답하지 않으면 취약한 항목 또는 정정 작업이 열림 상태로 되돌아갑니다. 이전 상태는 **backup_state** 필드에 저장됩니다. 자세한 내용은 예외 관리에 대한 승인 규칙 구성 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

v15.0 이전의 긍정 오류 승인 프로세스



모든 VI가 다음 스캔을 통과하면 승인 프로세스가 자동으로 진행됩니다. VI는 현재 상태에 관계없이 자동으로 닫힙니다. VI 또는 RT 상태 필드 (해당되는 경우)는 하위 상태가 고정된 상태로 종결 됨으로 변경됩니다 .

자세한 내용은 긍정 오류 표시 및 승인 문서를 참조하십시오.

관련 정보

취약한 항목 또는 정정 작업에 대한 가양성 요청

스마트 평가를 통한 예외 관리의 질문서 지원

스마트 평가를 사용하여 예외 관리 프로세스의 일부로 고급 질문서를 구성합니다. 이를 통해 정정 소유자는 예외 요청에 대해 보다 자세한 컨텍스트를 제공할 수 있으며 승인자는 조건부 질문을 구성하여 정보에 입각한 의사 결정을 위한 정보를 수집할 수 있습니다.

필요한 역할

스마트 평가 템플릿 판독기: **sn_vul_cmn.smart_assessment_template_manager** (취약성 관리자 및 템플릿 판독기)를 사용하면 관리자가 템플릿을 만들고 편집할 수 있습니다.

스마트 평가 액터: **sn_vul_cmn.smart_assessment_actor** 사용자(정정 소유자 및 관리자)가 질문서/평가를 작성할 수 있습니다.

스마트 평가 판독기: **sn_vul_cmn.smart_assessment_reader** 를 사용하면 승인자(승인자)가 제출된 질문서 응답을 읽을 수 있습니다.

필수 구성요소: 스마트 평가는 취약성 대응에 종속되므로 스마트 평가 플러그인을 설치해야 합니다.

이제 스마트 평가를 사용하여 예외 관리 프로세스의 일부로 질문서를 구성할 수 있습니다. 취약성 관리자/관리자는 조건부 질문을 구성하여 정보에 입각한 의사 결정에 필요한 올바른 정보를 수집할

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

수 있으며, 정정 소유자는 예외 요청에 대해 보다 자세한 컨텍스트를 제공할 수 있습니다. 이렇게 하면 승인 프로세스를 간소화하고 예외 근거의 명확성과 완전성을 보장하여 취약성 관리 팀과 정정 팀 간의 공동 작업이 향상됩니다.

일부 워크플로우에는 여전히 이전 스타일의 질문서가 필요한 반면, 새로운 평가는 사용자 친화적이며 작업 공간에서만 지원되기 때문에 작업 공간뿐만 아니라 클래식 사용자 인터페이스에서도 질문서 및 스마트 평가에 액세스할 수 있습니다.

이제 예외 관리 구성 화면에서 보상 통제, 요청 예외 및 긍정 오류 기록에 대한 평가를 선택할 수 있습니다.

주:
"예외를 요청하기 위한 평가" 필드를 완료하기로 선택한 경우 시스템에서 스마트 평가 템플릿을 고려할 수 있거나 클래식 질문서가 고려됩니다.

아래에 제공된 두 가지 옵션을 사용할 수 있습니다.

- 스마트 평가: 취약성 작업 공간에서 질문서를 관리합니다.
- 기존 질문서: 작업 공간 환경과 클래식 환경 모두에서 기존 질문서에 액세스할 수 있습니다.

위의 템플릿은 스마트 평가 템플릿 판독기(**sn_vul_cmn.smart_assessment_template_manager**)에서 액세스/편집할 수 있습니다.

평가 템플릿 구성

평가 템플릿에는 요청 프로세스 중(예: 예외 요청 시) 표시될 질문이 포함되어 있습니다. 위에서 언급한 미리 구성된 템플릿은 스마트 평가와 함께 제공됩니다. 필요에 따라 템플릿을 직접 생성할 수도 있습니다.

시작하기 전에
필요한 역할:

템플릿 판독기 역할: **sn_vul_cmn.smart_assessment_reader** 를 사용하면 승인자(승인자)가 제출된 질문서 응답을 읽을 수 있습니다.

템플릿 액터 역할: **sn_vul_cmn.smart_assessment_actor** 사용자(정정 소유자 및 관리자)가 질문서/평가를 작성할 수 있습니다.

이 태스크 정보
취약성 대응 작업 공간에서 예외 요청(예: 취약성 대응에 대한 예외, 취약성 대응에 대한 가양성)에 사용할 평가 대상이 VCA인 템플릿을 선택할 수 있습니다. 기본 템플릿을 선택하면 질문이 자동으로 채워집니다. 템플릿을 직접 생성하기로 선택한 경우 수정할 수 있습니다.

프로시저

1. 평가 작업 공간으로 이동합니다.
2. 기존 평가 템플릿 선택 또는새 템플릿 선택
3. 다음 세부 정보를 입력합니다.
   - 템플릿 이름: 템플릿의 고유 이름입니다
   - 평가 이름: 평가를 볼 때 시스템에 표시되는 이름입니다.
   - 템플릿 범주: 보다 쉽게 관리할 수 있도록 템플릿이 분류됩니다. 취약성 대응 질문서 템플릿과 같은 일부 템플릿 범주가 바로 사용 가능한 기본으로 제공되며, 원하는 템플릿을 생성할 수 있습니다.
   - 평가 대상: 템플릿과 관련된 테이블을 지정합니다. VR의 경우 VCA 테이블(취약성 변경 승인 테이블)입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

스마트 평가 워크플로우

정정 소유자는 승인을 위해 제출하기 전에 질문서를 작성해야 합니다. 승인자는 질문서를 검토하고 제공된 정보를 바탕으로 승인/거부 결정을 내립니다.

시작하기 전에

필요한 역할: **sn_vul_cmn.smart_assessment_reader**

이 태스크 정보

다음은 스마트 평가 적용의 워크플로우입니다.

- 예외/긍정 오류 요청 예외를 요청하거나 긍정 오류로 표시하면 시스템에서 질문서가 필요한지 확인합니다.
- 질문서 옵션을 사용하는 경우, 승인 프로세스를 진행하기 전에 사용자에게 질문서를 작성하라는 필수 메시지가 표시됩니다.
- 초안 상태: 취약성 상태 변경 승인 (VCA) 기록은 질문서가 제출될 때까지 초안 상태로 유지되고 취약성 항목(VIT)은 오픈 상태입니다.
- 승인자 뷰: 정정 소유자가 질문서를 작성하고 제출하면 취약성 상태 변경 승인(VCA) 및 취약성 항목(VIT) 기록이 검토 중 상태로 전환됩니다. 승인자는 "내 승인> 전체"에서 질문서를 검토할 수 있습니다. VIT는 기록이 승인되면 지연 상태로 전환됩니다. 기록 양식의 헤더에서 정정 소유자가 제출한 링크를 통해 질문서를 볼 수 있습니다.

프로시저

1. 이동 모두 〉 내 승인클릭하여 질문서를 봅니다.
2. 기록이 승인되면 VIT는 지연 상태로 이동됩니다.
3. 기록 양식의 헤더에서 정정 소유자가 제출한 링크를 통해 질문서를 볼 수 있습니다.

긍정 오류 또는 예외 요청에 대한 질문서

긍정 오류 또는 예외 요청에 대한 질문서가 제기되었지만 완전히 채워지지 않은 경우

긍정 오류 또는 예외 요청에 대한 질문서가 제기되었지만 완전히 채워지지 않은 경우 VCA 레코드는 "초안" 상태가 됩니다. 동일한 범주에서 예외를 제기하려면 동일한 범주에 대한 팝업 메모에 따라 이전 질문서로 이동합니다. 기존 요청 예외 대신 가양성 기록을 제기하려는 경우 시스템은 취약성 상태 변경 승인(VCA)을 무효화하고 새 가양성 취약성 상태 변경 승인(VCA) 기록을 생성합니다.

질문서가 절반 채워져 있고 동일한 취약성 항목(VIT)/또는 다른 항목이 클래식 뷰에서 열려 있는 경우, 동일한 유형의 요청이 다시 발생하면 나머지 데이터를 채우기 위해 작업 공간 질문서로 이동합니다. 클래식 뷰의 질문서가 선택적으로 채워지고 작업 공간에서 동일한 항목이 열리면 클래식 뷰 질문서가 작업 공간에서 열립니다.

다음에 대한 워치독 취약성 대응

워치독은 지정한 조건에 따라 테이블을 추적하는 데 사용됩니다. 예를 들어 통합 실행 실패의 상세 정보를 에 기록하는 데 사용할 수 있습니다 취약성 대응.

이러한 오류에 대한 알림을 받도록 선택할 수 있습니다. 이 알림에 따라 정정을 계획할 수 있습니다. 기본 워치독은 다음과 같습니다.

- 통합 실행 실패: 통합 실행 상태가 완료로 설정되고 하위 상태가 실패로 설정된 경우, 조건이 0보다 큰 카운트를 반환하면 즉 통합 실행이 실패한다는 알림을 사용자 및 사용자 그룹에 알립니다.
- 장기 실행 통합: 통합 실행이 설정된 시간을 초과하는지 확인하는 스크립트입니다. 이 감시 장치는 통합 실행 완료가 지연될 때마다 사용자에게 사전 경고를 보냅니다.
- 중복된 주기적 실행: 예정된 발생 중에도 계속 실행되는 반복 통합 실행을 확인하는 스크립트입니다. 이러한 통합 실행 목록이 포함된 링크가 생성됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

감시 로그

워치독에는 조건이 충족된 횟수를 계산하는 워치 로그가 함께 제공됩니다.

개요 대시보드

개요 대시보드를 사용하여 지난 30일 동안의 워치독을 모니터링합니다. 모니터링 중인 다른 감시 주제를 추적하기 위해 여러 위젯을 만들 수 있습니다.

의 취약성 대응버전 19.0부터 이 대시보드는 New Experience UI에서 사용할 수 있습니다.

주:
Tokyo에 있는 경우 Next Experience UI에서 대시보드를 볼 수 있지만 일부 기능 손실이 있습니다.

보고서

이름	설명
지난 30일 동안 WatchDog 실패	지난 30일 동안 모든 조건이 충족되었습니다.

자세한 내용은 워치독 구성 및 탐지를 위한 오류 처리 문서를 참조하십시오.

를 위한 변경 관리 취약성 대응

IT 정정 소유자는 애플리케이션의 정정 작업(RT)에서 직접 변경 요청(CHG)을 생성하고 관리할 수 있습니다 취약성 대응 . 변경 요청은 정정 작업 및 해당 취약한 항목을 정정할 수 있도록 자산에 대한 변경 활동을 시작하고 추적하는 데 도움이 됩니다.

변경 요청 및 취약성 워크플로우

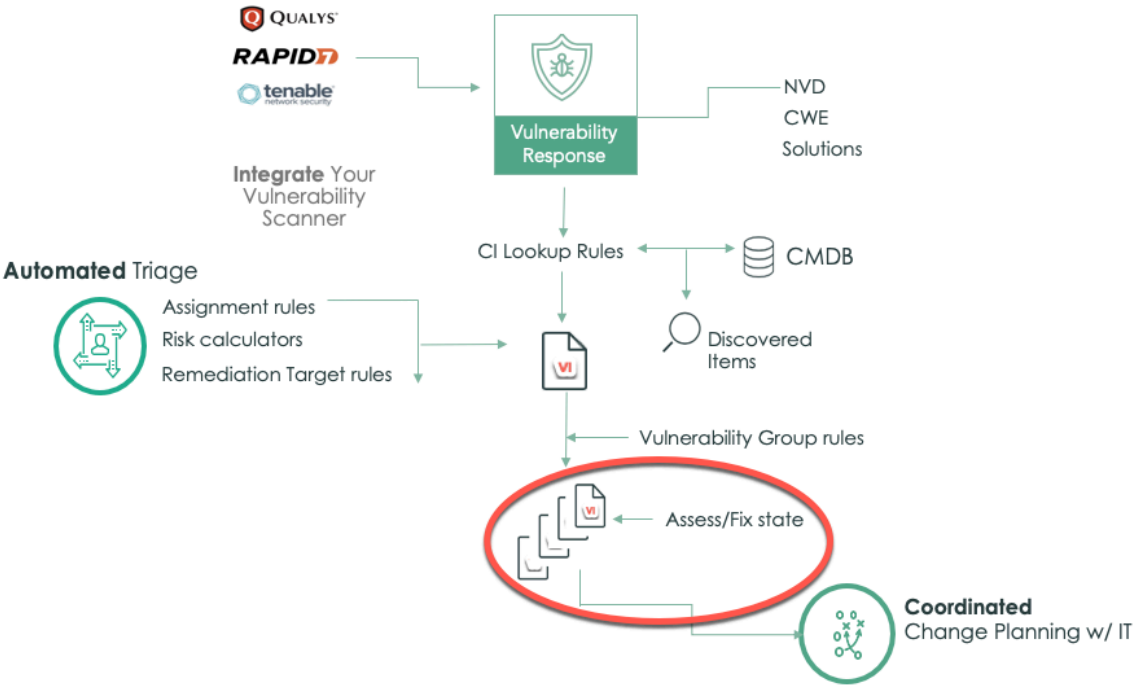
Vulnerability Response 애플리케이션에 익숙하지 않은 경우 자세한 내용은 을 참조하십시오 애플리케이션 탐색 취약성 대응.

다음 이미지는 자동 분류를 통해 설정된 통합(스캐너)에서 조사로의 정보 취약성 대응플로우를 보여줍니다.

변경 요청 및 변경 관리는 다음 그림에 표시된 워크플로우에서 정정 프로세스(평가/수정 상태)의 취약성 대응 일부입니다. 이 단계에서 변경 요청을 사용하여 취약성 정정을 시작하고 추적할 수 있습니다. 정정 작업에서 직접 변경 요청을 생성 및 관리하고, CMDB의 CI(구성 항목)에 대해 영향을 받는 자산에 대한 솔루션을 포함하는 조사 및 정정 작업을 나열할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Vulnerability Response의 변경 요청



Vulnerability Response에서 변경 요청을 사용하는 경우

IT 정정 소유자는 CMDB에서 지원되는 구성 항목(CI)을 수정 또는 제거하기 위해 어떤 종류의 제어된 수동 프로세스가 필요한 경우 정정 작업에서 변경 요청을 생성할 수 있습니다. 정정 작업 기록에서 직접 변경 요청을 생성하고 관리하면 취약성을 신속하게 조사하고 해결하는 데 도움이 됩니다. 해결된 정정 작업의 VI는 다음 예약 스캔 중에 스캔 및 검증되어 워크플로우의 취약성 대응 자동화된 분류로 반환될 수 있습니다ServiceNow AI Platform. 변경 요청이 필요할 수 있는 수동 개입에는 다음과 같은 예가 포함됩니다.

- RT 해결 전에 취약한 항목에 필요한 IT의 소프트웨어 패치, 수정 또는 기타 작업입니다.
- 정정 작업에 있는 취약한 항목의 하위 집합을 확인하면 추가 조사 또는 다른 부서로의 재할당이 필요합니다.
- RT에서 많은 취약한 항목 집합이 있는 취약한 항목의 하위 집합을 새로운 정정 작업으로 이동할 수 있다고 결정합니다.
- 정정 작업의 중복을 피하기 위해 정정 작업을 기존 변경 요청에 연결할 수 있습니다.

RT에 대한 변경 요청 유형

애플리케이션은 취약성 대응 인스턴스의 제품 ServiceNow AI Platform# 에서 ITSM 변경 관리 지원하는 세 가지 유형의 서비스 변경(표준, 긴급 및 일반)을 활용합니다. 선택한 변경 유형에 따라 호출되는 상태 모델과 따라야 하는 변경 프로세스가 결정됩니다. 변경 요청은 변경 사유, 우선순위, 위험, 변경 유형 및 변경 범주와 같은 변경에 대한 자세한 정보를 기록합니다. 변경 유형을 참조하십시오.

취약성 대응 IT 정정 소유자는 정정 작업에서 직접 일반, 표준 및 긴급 변경 요청을 생성할 수 있는 다음과 같은 옵션을 사용할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 정정 작업에서 미리 채워진 정보가 포함된 변경 요청을 생성하여 프로세스를 간소화하고 시간을 절약할 수 있습니다.
- 정정 작업을 기존 변경 요청에 연결하여 유사한 정보 및 취약한 항목을 공유하는 중복 변경 요청이 생성되는 것을 방지할 수 있습니다.
- 조건 집합을 사용하여 취약한 항목의 하위 집합을 필터링하고 정정 작업을 분할할 수 있습니다. 선택한 항목은 자동으로 새 RT로 이동됩니다.

정정 작업의 필드 값을 사용하여 취약한 항목을 필터링하고 필터 기준과 일치하는 항목에만 변경 요청을 적용할 수 있습니다.

관련 정보

정정 작업에서 변경 요청 만들기

정정 작업을 기존 변경 요청에 연결

정정 작업 분할

변경 요청과 정정 작업 간의 상태 동기화

Software Asset Management를 사용한 소프트웨어 노출 평가**()SAM Foundation**

ServiceNow# 취약성 노출 평가 애플리케이션을 사용하여 자산의 특정 소프트웨어 패키지에 대해 설치된 총 소프트웨어 수를 확인합니다. Software Asset Management(SAM) Foundation 애플리케이션과 함께 ServiceNow# 사용할 경우 노출을 평가하고, 취약한 항목을 만들고, 발견한 취약한 소프트웨어에 대한 정정 조치를 관리합니다.

> **중요사항:**
> CVE(Common Vulnerabilities and Exposures) 및 소프트웨어별로 노출 평가를 수행하여 취약성 평가 작업 공간의 추가 기능을 활용할 수 있습니다. 자세한 내용은 취약성 평가 작업 공간 탐색 문서를 참조하십시오.

CVE(Common Vulnerabilities and Exposures) 데이터베이스를 사용하지 않고 취약한 소프트웨어 정보(게시자, 제품, 에디션 및 버전)를 제공하여 취약한 소프트웨어에 대한 노출을 확인합니다. 다음 케이스에 대해 소프트웨어에 대한 제로 데이(현재 날짜) 취약성 케이스를 평가합니다.

- 제품에 아직 CVE 데이터가 없는 경우.
- 취약성이 공개적으로 알려지는 시간과 취약성이 포함된 CVE 데이터가 NVD에서 업데이트되는 시간 사이에 지연이 있는 경우.
- 취약성 스캐너의 예약된 검사 사이에 취약성에 대해 알게 되는 경우

취약성 노출 평가 애플리케이션에서 취약한 소프트웨어의 게시자와 제품을 알고 있는 경우 애플리케이션에서 만든 SAM Foundation 네트워크에 설치된 소프트웨어를 나열하는 레코드를 사용하여 요청 시 잠재적으로 악의적인 소프트웨어 패키지에 대한 노출을 평가할 수 있습니다.

이러한 유형의 취약성에 대한 노출 규모를 알면 빨간색 경고를 구현하고 소프트웨어를 제거하거나 SOC(보안 운영 센터)에 특정 패치를 찾도록 알리는 등 사전에 대응할 수 있습니다. 추가 조사 정정을 위해 취약한 항목을 생성하고 정정 전문가에게 작업을 할당할 수 있습니다. 정정 작업(VUL) 목록을 보고 원하는 취약한 항목이 생성되어 VUL에 올바르게 연결되었는지 확인합니다.

관련 정보

취약성 노출 평가 구성

취약한 소프트웨어에 대한 노출 평가

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약성 위기 관리

취약성 위기 관리(VCM) 워크플로우를 통해 중요한 취약성 이벤트를 생성하고 추적합니다. 취약성 평가 기록을 생성하고 취약성의 주요 속성을 기록하여 위험을 계산하고 평가를 수행하여 노출 수준을 식별하고, 이해 관계자를 참여시켜 취약성에 대한 조정되고 신속한 대응을 수행합니다.

취약성 위기 이벤트 관리

취약성 위기 관리는 다음 기능을 사용하여 취약성 위기 이벤트를 처리하는 완전한 워크플로우입니다.

- 중요한 취약성을 소프트웨어 설치 인벤토리 소프트웨어 자산 관리 및 소프트웨어 자재 명세서(SBOM) 인벤토리, 스캐너에서 보고된 취약성 및 구성 관리 데이터베이스(CMDB)와 상관 관계를 지정하여 취약한 구성 항목을 효율적으로 식별합니다.
- 평가 결과를 정정을 위한 취약한 항목으로 변환합니다.
- 위협에 신속하고 조직적으로 대응할 수 있도록 중요 보안 인시던트를 개시합니다.
- 조직 전체의 팀과 협력하고 협업하여 취약성에 대한 통합 대응을 촉진합니다.
- 부서 간 이해 관계자 및 관련 팀에 정기적인 상태 보고서를 제공하여 위기 상황 전반에서 투명성과 소통을 유지합니다.

취약성 평가 작업 공간을 사용한 취약성 위기 관리

주:
Vulnerability Crisis Management v1.0.1부터 스토어에서 별도의 구독으로 애플리케이션을 사용할 수 있습니다. 세분화된 권리가 있거나 스토어에서 애플리케이션을 설치한 경우에만 취약성 평가 작업 공간에서 취약성 위기 관리에 액세스할 수 있습니다. 이전에는 Vulnerability Crisis Management가 Vulnerability Emergency Response 플러그인에 포함되었습니다. v3.2.2부터 Vulnerability Emergency Response 플러그인의 이름이 Vulnerability Exposure Assessment로 변경되었습니다.

관심 있는 취약성을 식별하면 취약성 이벤트 관리자는 위협 인텔리전스 소스, 취약성 특성 및 영향을 받는 제품에 대한 정보가 포함된 취약성 평가 기록을 생성합니다. 이 정보는 추가 영향 및 노출 분석에 사용됩니다.

관심 있는 취약성에 대한 기록이 생성되면 위험 평가가 수행됩니다. 이 평가는 구조화된 위험 점수 산정, 기록 검토, 작업을 수행하는 분석가의 관찰로 구성됩니다. 관심 취약성에 대한 초기 위험 점수는 이벤트 생성 시 사용할 수 있는 속성을 사용하여 계산됩니다. 평가에 대한 위험 점수는 추가 인텔리전스를 사용할 수 있게 되면 변경될 수 있습니다. 위험 점수를 사용하여 악용의 잠재적 영향을 확인하고 대응 우선순위를 설정합니다.

관심 취약성에 대한 평가가 생성되고 조직의 인프라에 위험을 나타내는 것으로 확인되면 , (SBOM) 인벤토리, 스캐너에서 보고된 취약성 및 구성 관리 데이터베이스(CMDB)의 소프트웨어 설치 인벤토리 소프트웨어 자산 관리소프트웨어 자재 명세서 를 사용하여 심층 노출 평가로 위험 평가를 업데이트하여 위협을 추가로 분석할 수 있습니다. 영향을 받는 구성 항목 및 애플리케이션은 평가를 통해 자동으로 식별됩니다. 영향을 받는 추가 항목은 수동으로 추가할 수 있습니다.

평가가 완료되면 아직 연결된 취약한 항목이 없는 노출 결과에 대해 취약한 항목 또는 애플리케이션 취약한 항목을 만들 수 있습니다. 취약한 항목의 위험 점수 계산기를 활용/구성하여 취약성 평가 기록에 연결된 취약한 항목에 대한 위험 점수를 조정할 수 있습니다. 취약성 평가 기록에 노출 수준 및 이벤트 우선순위를 할당할 수 있습니다. 이벤트 우선순위에 따라 취약성 이벤트 관리자는 취약성 평가를 제안, 승격 또는 주요 보안 인시던트에 연결하도록 선택할 수 있습니다.

에서 중요 보안 인시던트 관리사용 가능한 공동 작업 통합을 사용하여 정정 활동을 추적 및 관리하고, 진행 중인 보안 인시던트를 연결하고, 임시 작업을 생성하고, 영향을 받는 팀을 참여시키고, 상태 보고서를 전송하고, 공동 작업하는 데 사용할 중요 보안 인시던트 관리 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

ServiceNow® 소프트웨어 자산 관리 및 소프트웨어 자재 명세서 (SBOM) 평가 처리 논리

소프트웨어 자산 관리 데이터를 사용하여 CVE에 대한 NVD에서 제공되는 CPE와 문자열 일치 논리를 사용하여 검색 모델을 가져옵니다. 검색 모델을 가져오면 관련 설치에 대한 스캔이 실행되고 관련 구성 항목을 가져오며 영향을 받는 구성 항목 테이블이 채워집니다. 게시자, 제품, 버전 및 에디션과 같은 추가 상세 정보를 제공할 수 있습니다. 이를 기반으로 일치하는 모든 검색 모델과 기록에 대한 소프트웨어 설치를 가져옵니다. 이어서 관련 구성 항목을 가져오고 영향을 받는 구성 항목 테이블이 다시 채워집니다.

의 경우 SBOM관련(m2m) 테이블(CVE와 소프트웨어 사이)에서 CVE에 연결된 소프트웨어를 가져옵니다. 소프트웨어 세부 정보를 가져온 후 SBOM 구성 요소의 제품 및 버전을 식별된 소프트웨어의 제품 및 버전과 일치시켜 관련 SBOM 구성요소를 식별합니다.

연결된 구성요소가 발견되면 구성요소와 관련된 엔터티를 가져옵니다. 엔터티 및 관련 CI(있는 경우)의 제품 모델을 가져오고 구성 항목이 영향을 받는 구성 항목 테이블에 저장됩니다. 구성 항목에 취약한 항목이 없는 경우 이를 사용하여 취약한 항목을 생성할 수 있습니다. 구성 항목을 찾을 수 없으면 제품 모델이 영향을 받는 소프트웨어 모델 테이블에 저장되고 애플리케이션 취약한 항목을 만드는 데 사용할 수 있습니다.

취약성 위기 관리 워크플로우 사용에 대한 자세한 내용은 취약성 평가 작업 공간 사용을 참조하십시오.

관련 정보

- 취약성 평가 탐색
- 취약성 평가 작업 공간 탐색
- 평가 탭

도메인 분리 및 취약성 대응

취약성 대응에서는 도메인 분리가 지원됩니다. 도메인 분리를 사용하여 데이터, 프로세스 및 관리 작업을 도메인이라는 논리적 그룹으로 분할할 수 있습니다. 어떤 사용자가 데이터를 보고 액세스할 수 있는지를 포함하여 이러한 분리의 여러 측면을 제어할 수 있습니다.

지원 수준: 표준

- 기본 수준 지원의 모든 측면을 포함합니다.
- 애플리케이션 속성이 필요에 따라 도메인을 인식합니다.
- 비즈니스 논리: 서비스 제공자(SP)가 고객별로 프로세스를 만들거나 수정합니다. 사용 사례는 여러 SP 고객이 단일 인스턴스에서 애플리케이션을 올바르게 사용하는 것을 반영합니다.
- 인스턴스 소유자는 특정 애플리케이션에 필요한 대로 테넌트별 최소 실행 가능한 제품(MVP) 비즈니스 논리 및 데이터 매개변수를 구성해야 합니다.

샘플 사용 사례: 관리자가 한 테넌트에 대해서는 기록이 닫히지만 다른 테넌트에 대해서는 기록이 닫히지 않는 경우 설명이 필요하도록 설정할 수 있어야 합니다.

지원 수준에 대한 자세한 내용은 도메인 분리를 위한 애플리케이션 지원 을 참조하십시오.

취약성 대응에서 도메인 분리가 작동하는 방식

도메인 분리를 사용하면 서비스를 제공하는 고객 기반 전체에서 VR()취약성 대응 절차를 표준화하여 운영 비용을 절감하고 서비스 품질을 높일 수 있습니다.

워크플로우, 대시보드, 보고서 등을 위한 별도의 고객 작업 공간을 사용하면 고객 데이터가 분리되어 다른 클라이언트에게 노출되지 않습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

버전 릴리스별 **Vulnerability** Response의 도메인 분리 지원

릴리스	지원 수준	메모
Orlando	표준	
파리	표준	
Quebec	표준	
Rome	표준	
San Diego	표준	
Tokyo	표준	
유타	표준	
밴쿠버	표준	
워싱턴 DC	표준	

애플리케이션의 도메인 분리는 취약성 대응 다음 제품 기능을 포함합니다.

- 올바른 도메인의 외부 공급업체 스캐너(예: Qualys, Rapid 7 또는 Tenable)에서 취약한 항목을 수집합니다. 통합 사용자의 데이터와 동일한 도메인에서 데이터 수집으로, 해당 자격 증명이 통합에 사용됩니다.
- 요청된 도메인에서 특정 자산을 취약성 대응 다시 스캔합니다.
- CMDB CI 조회 프로세스를 사용하여 스캐너의 CI 정보가 통합 사용자 도메인의 CMDB에 있는 CI와 일치하는지 확인합니다.
- 통합 사용자와 동일한 도메인에 정의된 위험 점수 계산기에 따라 취약한 항목 수준에서 위험 점수를 계산합니다.
- 정정 대상 규칙은 통합 사용자와 동일한 도메인에 정의된 정정 대상 규칙에 따라 취약한 항목에 실행됩니다.
- 정정 작업 규칙은 통합 사용자의 도메인과 동일한 도메인을 정의하고 유지할 수 있습니다.
- 정정 작업 규칙을 사용하여 생성된 정정 작업은 그룹 규칙이 생성된 도메인과 동일한 도메인에 유지됩니다.
- 연기 워크플로우는 연기가 요청되는 동일한 도메인에서 승인 프로세스를 진행합니다.
- 보고서와 대시보드에는 취약한 항목의 기간, CI별 미해결된 취약한 항목, 영향별 취약성 및 자신이 속한 도메인의 정정 목표 날짜 상태와 같은 취약한 항목 상태가 표시됩니다.
- 타사 스캐너 또는 NVD(국가 취약성 데이터베이스)의 지식은 전역 도메인에서 수집될 수 있으며 여러 클라이언트에서 데이터를 공유할 수 있습니다.

주:
위의 모든 경우에 NOW Platform에서 분리된 도메인 분리의 가시성에 대한 중요한 원칙이 적용됩니다.

도메인 분리 임포트를 만들고 지원하는 방법에 대한 자세한 내용은 해당 백그라운드 작업 프레임워크에서 여러 도메인 생성 및 지원문서를 참조하십시오통합을 위해 도메인 분리 임포트 작성.

사용 사례

애플리케이션은 취약성 대응 취약성 항목의 수명주기를 엔드투엔드로 관리합니다. 다음 사용 사례는 도메인 분리를 인식합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 외부 공급업체 통합에서 취약한 항목(자산의 취약성)을 수집합니다.
  - 여러 인스턴스에서 데이터 수집
  - 취약한 항목의 중복을 제거합니다.
  - CMDB CI와 매칭
- 위험 점수 및 정정 목표 날짜로 취약한 항목 보강
  - 자산 보강(CMDB)
  - 위험 점수 및 정정 대상 날짜 보강
- 취약한 항목을 그룹화하고 정정 작업을 할당합니다.
  - 취약한 항목을 자동으로 그룹화
  - 정정 작업 자동으로 할당
- 정정
  - 정정 작업
  - 포괄적인 정정 수명주기
  - 연기 워크플로우
- 조직의 보안 태세 및 취약성 관리 프로그램 측정
  - 취약성 추세, 가장 취약한 자산, 기간별 취약성
  - 정정 목표 날짜까지의 정정 상태

설정

의 취약성 대응 도메인 분리를 설정하는 데는 추가 단계가 필요하지 않습니다. 모든 취약성 대응 테이블은 인스턴스가 도메인으로 분리된 후 도메인 열을 획득합니다. 취약성 통합 임포트 데이터를 특정 도메인으로 보낼 수 있습니다. 자세한 내용은 통합을 위해 도메인 분리 임포트 작성 문서를 참조하십시오.

도메인 분리 데이터

데이터는 도메인으로 분리될 수 있으며 이는 다음을 의미합니다.

- 외부 공급업체 스캐너에서 수집된 취약한 항목은 통합 사용자의 도메인과 동일한 도메인에 유지되며 다른 도메인에서는 액세스할 수 없습니다.
- 한 도메인의 취약성, 취약한 항목(인스턴스) 또는 자산은 다른 도메인에서 볼 수 없습니다.
- 위험 점수 산정 알고리즘, 정정 작업 규칙 및 정정 대상 규칙은 도메인 외부의 사용자가 볼 수 없습니다.
- NVD의 취약성 정보는 전역 도메인에 존재할 수 있으며 모든 고객과 공유될 수 있습니다.
- 한 도메인의 정정 작업은 다른 도메인에서 볼 수 없습니다.
- 한 도메인에서 생성된 지연 워크플로우는 다른 도메인에 표시되지 않습니다.
- 모든 이메일 알림은 자신이 속한 도메인에 포함됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

인스턴스에서 사용할 수 있는 예약된 임포트 템플릿은 기본적으로 "도메인: 전역"으로 설정됩니다. 따라서 인스턴스에 여러 도메인이 있을 때 충돌을 방지하려면 다음 방법을 적용하십시오.

- 인스턴스에서 사용할 수 있는 임포트 템플릿을 통합과 관련된 여러 도메인 수에 분산합니다.
- 임포트 템플릿 기록의 도메인을 대상 도메인의 sys_id 업데이트합니다.
- 필요한 경우 각 도메인에 대한 임포트 템플릿을 생성합니다.
- 각 도메인에 2개의 임포트 템플릿이 있는지 확인합니다.
- sn_vul_sched_import_pool: 인스턴스에 도메인 분리가 있는 경우 이 테이블 기록은 도메인으로 분리되어야 합니다.

취약성 분석가가 자신의 애플리케이션 데이터를 관리하는 방법

- 분석가는 자체 애플리케이션 설치, 다중 소스 애플리케이션 관리 및 CI 조회 규칙을 생성합니다.
- 분석가는 도메인 내에서만 사용할 특정 통합을 구성할 수 있습니다.
- 분석가는 고유한 지연 및 변경 관리 워크플로우를 생성할 수 있습니다.
- 분석가는 자체 정정 작업 규칙, 위험 점수 산정 논리를 생성하여 취약성의 우선순위를 정확하게 지정하고 정정 작업을 자동으로 할당하고 올바른 할당 그룹에 할당할 수 있습니다.
- 도메인 사용자는 수동 취약성 항목을 생성한 다음 해당 항목을 종결합니다.

인스턴스 소유자가 도메인 분리할 수 있는 비즈니스 로직 및 프로세스

- 취약성 대응 사용자 및 그룹
- 취약성 대응 통합
- 전체 설정 구성(사용자 및 그룹 관리, 애플리케이션 설치, 다중 소스 애플리케이션 관리, CI 조회 규칙, 정정 작업 규칙, 위험 계산기, 정정 대상 규칙 등)
- 지연을 포함한 전체 정정 수명주기
- 작업 예약

관련 정보

서비스 제공자용 도메인 분리

의 서비스 매핑 취약성 대응

서비스 매핑은 조직이 IT 인프라와 다양한 구성요소 간의 관계를 포괄적으로 이해하는 데 도움이 됩니다. 서비스, 애플리케이션 및 인프라 구성요소를 자동으로 검색하고 매핑하여 의존성과 관계를 시각적으로 나타낼 수 있습니다.

에서 취약성 대응예약된 작업은 `Set related CI services` 영향을 받는 비즈니스 서비스와 취약한 항목(VIT)과 연결된 구성 항목(CI) 간의 연결을 설정합니다. 통합 임포트가 완료되고 지정된 시간에 연결 프로세스가 수행됩니다. 이 예약된 작업의 성능을 향상시키기 위해 의 취약성 대응v21.1.2부터 몇 가지 변경 사항이 구현되었습니다. 다음과 같습니다.

- 위험 점수 계산: 위험 점수를 계산하는 프로세스에는 예약된 작업의 활용이 `Set related CI services` 포함됩니다. CI가 처리되면 이 작업은 필요한 데이터를 관련 서비스 [sn_vul_m2m_ci_services] 테이블에 저장합니다. 이전에는 구성 준수에서 위험 계산에 API(애플리케이션 프로그래밍 인터페이스) `CIUtils#`구성 관리 데이터베이스(CMDB) 직접 액세스하여 가져오는 동안 각 테스트 결과에 대한 서비스를 검색해야 했습니다. 그러나 현재

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로세스는 관련 서비스 [sn_vul_m2m_ci_services] 테이블의 예약된 작업 출력을 사용하여 의 구성 준수위험 점수를 계산합니다. 또한 관련 서비스 [sn_vul_m2m_ci_services] 테이블을 활용하도록 기본 시스템 계산기가 수정되었습니다.

- 서비스 크기: 예약된 작업과 관련된 *Set related CI services* 시스템 속성의 *sn_sec_cmn.services_affected_by_CI_max_size*서비스 값이 1,000에서 500으로 감소합니다.
- 서비스 깊이: 예약된 작업과 관련된 시스템 속성의 *sn_sec_cmn.services_affected_by_CI_max_depth*깊이가 *Set related CI services* 10에서 5로 줄어듭니다. 서비스 값도 1,000에서 500으로 감소합니다.
- 클래스 제외CMDB: 서비스 계산을 건너뛰어야 하는 클래스를 구성할 CMDB 수 있도록 시스템 속성이 *sn_sec_cmn.ignoreCIClassForService* 도입되었습니다. 기본 시스템에서 이 속성은 *cmdb_ci_unclassed_hardware*, *cmdb_ci_incomplete_ipsn_sec_cmn_unmatched_ci* 클래스에 의해 취약성 대응 생성되고 서비스 매핑이 없을 수 있으므로 이러한 클래스에 대해 설정됩니다. 이전에는 서비스 계산이 VIT를 기반으로 했습니다. 그러나 검색된 항목을 대신 사용하도록 논리가 수정되었습니다. 검색된 항목은 서비스를 계산하는 데 사용되며, 이 서비스는 동일한 테이블의 CI와 연결됩니다.
- 전체 서비스 새로 고침을 위한 예약된 작업: 서비스 전체를 새로 고침하기 위해 요청 시 예약된 작업이 *Full refresh-related CI services for VI*도입되었습니다. 의 취약성 대응*Set related CI services* v21.0으로 업그레이드하면 기본 테이블이 취약한 항목 대신 검색된 항목을 사용하기 때문에 처음에는 작업이 더 오래 실행됩니다. 따라서 이 작업은 지난 90일 이내에 스캔되었으며 검색된 모든 항목을 처리해야 합니다. 또한 서비스를 더 자주 새로 고쳐야 하는 경우에는 매주 주기적인 새로 고침을 예약하거나 전체 새로 고침을 수행하여 수용할 수 있습니다. 활동을 수행하여 CI와 연결된 서비스가 변경되고 이러한 변경 내용을 반영하려는 취약성 대응 경우 요청 시 예약된 작업을 *Full refresh related CI services for VI*실행할 수 있습니다. 이 작업은 지난 90일 동안 기록된 검색된 모든 항목을 가져와 그에 따라 연결된 서비스를 새로 고칩니다.

관련 정보

Service Mapping

CIUtils - Global

취약성 대응 구현

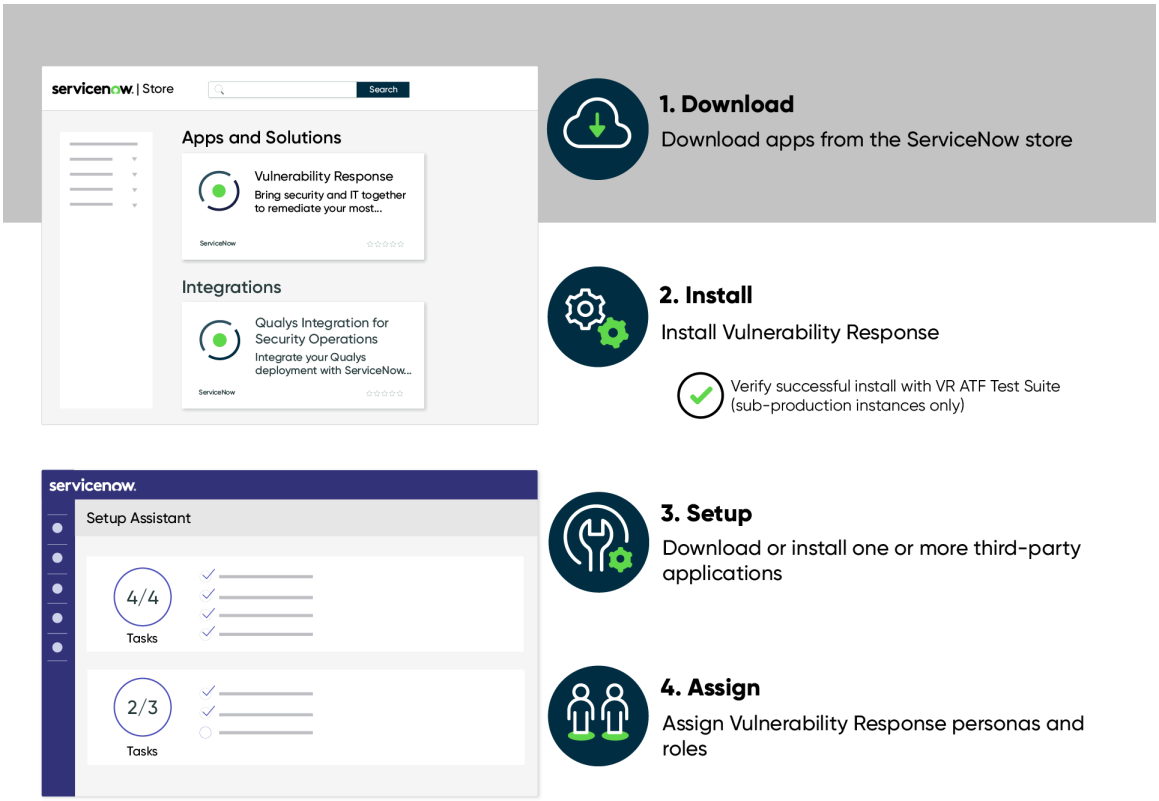
다음 이미지에 설명된 단계를 사용하여 에서 ServiceNow Store애플리케이션을 다운로드 취약성 대응 하고, 인스턴스에 설치 ServiceNow AI Platform# 하고, 설정 도우미를 사용하여 구성합니다.

기본 시스템, 취약성 대응 애플리케이션 및 타사 스캐너 애플리케이션인 Qualys 애플리케이션을 설치하기 위한 설치 및 구성 예가 다음 이미지에 설명되어 있습니다. 필수 역할과 필수 작업, 선택적 단계도 나열됩니다.

- 다음 이미지에 설명된 각 단계와 지원 설명서에 대한 링크가 있는 검사 목록에 대한 자세한 내용은 다음 문서를 참조하십시오 애플리케이션의 구현 검사 목록 취약성 대응.
- 이 예제에 제시된 개념과 단계 순서를 에 대해 취약성 대응지원되는 다른 애플리케이션의 설치 및 구성으로 확장할 수 있습니다. 지원 애플리케이션 목록은 문서를 참조하십시오 취약성 대응 설치 및 지원되는 애플리케이션.
- 이 예시에 사용된 애플리케이션 및 Qualys 취약성 애플리케이션을 다운로드하고 설치하려면 취약성 대응 관리자 역할이 필요합니다.
- 또한 관리자 역할은 취약성 관리자 [sn_vul.vulnerability_admin] 가상 사용자 및 기타 취약성 대응 가상 사용자 역할을 사용자 및 그룹에 할당합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관리자 작업

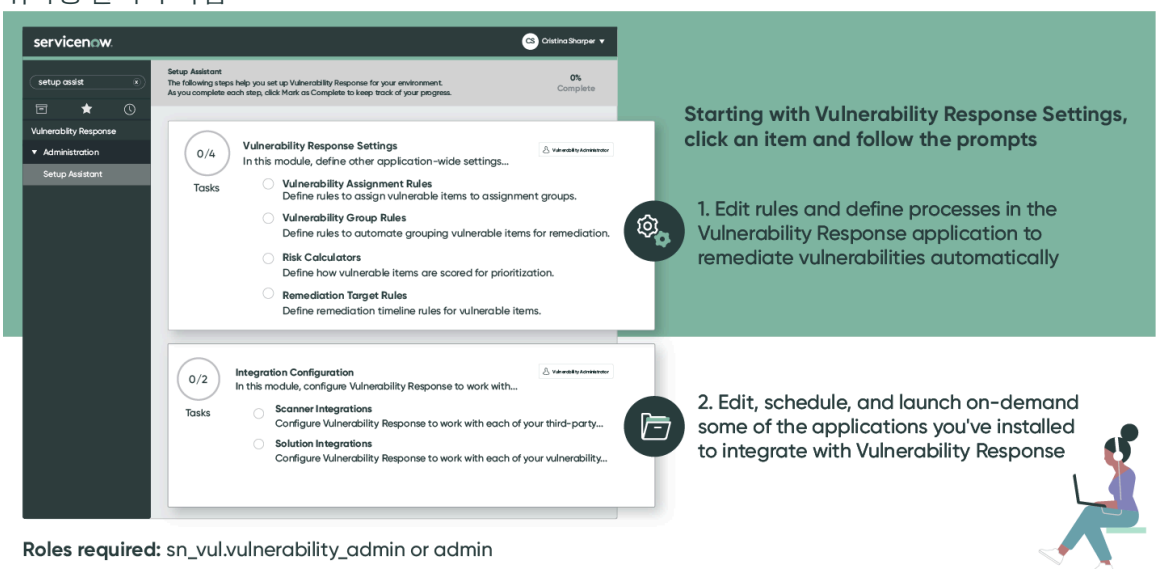


sn_vul.vulnerability_admin 역할은 설정 도우미에서 및 Qualys 애플리케이션을 구성하고 취약성 대응 예상 결과를 확인합니다.

취약성 대응 설정 섹션부터 설정 도우미의 단계와 프롬프트에 따라 설치 및 구성을 계속합니다. 이러한 설정을 검토하면 환경을 계속 설정할 때 프로세스를 취약성 대응 이해하고 확인하는 데 도움이 됩니다.

필요한 역할: sn_vul.vulnerability_admin 또는 admin.

취약성 관리자 작업



Roles required: sn_vul.vulnerability_admin or admin

다음 섹션에서 애플리케이션과 함께 설치한 설명, 기본 설정 및 데모 데이터를 검토합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 취약성 담당 규칙 - 취약한 항목(VI)을 적절한 담당 그룹에 자동으로 할당합니다.
- 정정 작업 규칙 - 특정 조건에 따라 취약한 항목(VI)이 임포트될 때 자동으로 그룹화합니다.
- 위험 계산기 - 기본 위험 계산기가 활성화되어 있습니다.
- 정정 대상 규칙 - VI 및 정정 작업(RT)에 대한 정정 타임라인을 정의합니다.
- 설치한 타사 애플리케이션 및 설치된 솔루션에 대한 설정을 검토 및 편집하고 데이터 임포트에 대한 조건을 정의합니다. 외부 공급업체 계정 정보를 입력하고 임포트 설정, 일정, CI(구성 항목) 조회 규칙 및 기타 설정을 구성합니다.

자세한 내용은 애플리케이션의 구현 검사 목록 취약성 대응 문서를 참조하십시오.

애플리케이션을 사용자 지정하거나 구현하는 취약성 대응 동안 자세한 내용은 KB1000704 문서를 참조하십시오.

취약성 대응 설치

인스턴스에서 애플리케이션을 ServiceNow AI Platform 실행하기 취약성 대응 전에 권리를 얻고, 에서 ServiceNow Store애플리케이션을 다운로드하고, 인스턴스에 설치 ServiceNow AI Platform 하고, 설정 도우미에서 몇 가지 설치 단계를 완료해야 합니다.

시작하기 전에

주:
이 프로세스는 프로덕션 인스턴스에 다운로드된 애플리케이션에만 적용됩니다. 애플리케이션을 비프로덕션 또는 개발 인스턴스에 다운로드하는 경우에는 권리를 얻을 필요가 없습니다. 로 애플리케이션 활성화 ServiceNow Store계속 진행합니다.

- 인스턴스에 필요한 ServiceNow 역할이 할당되어 있는지 확인합니다.
- 역할을 설치하고 할당하려면 관리자 역할이 필요합니다.

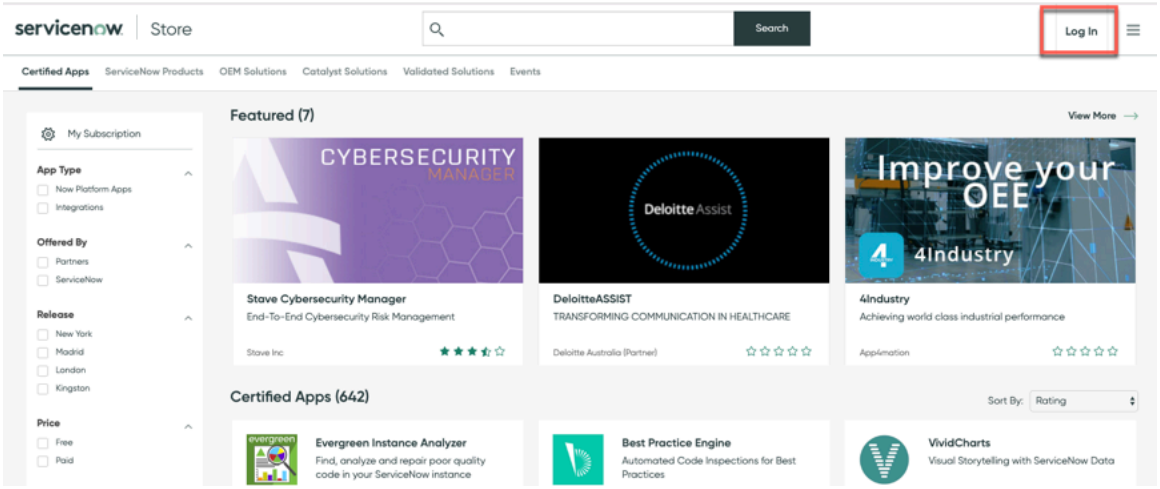
필요한 역할: 관리자

가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

프로시저

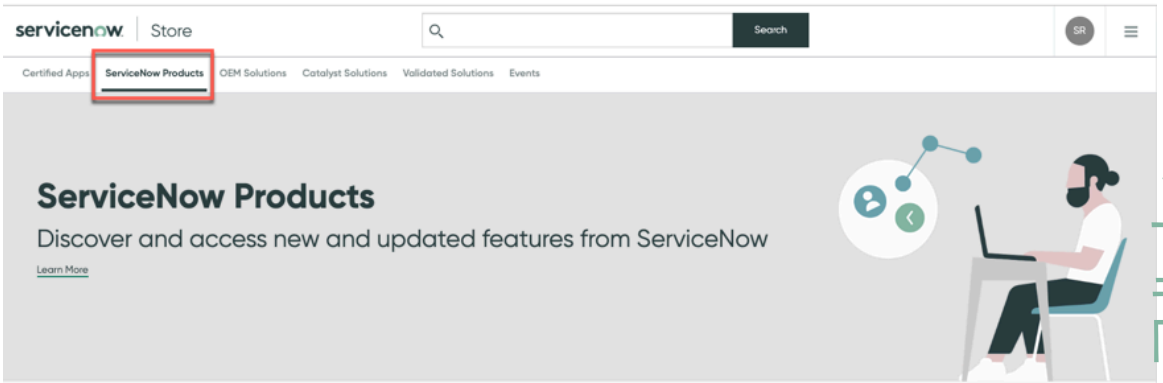
1. 권리를 얻고 핵심 애플리케이션을 다운로드하려면 취약성 대응 로 ServiceNow Store이동합니다.
2. 페이지 오른쪽 상단에서 로그인을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



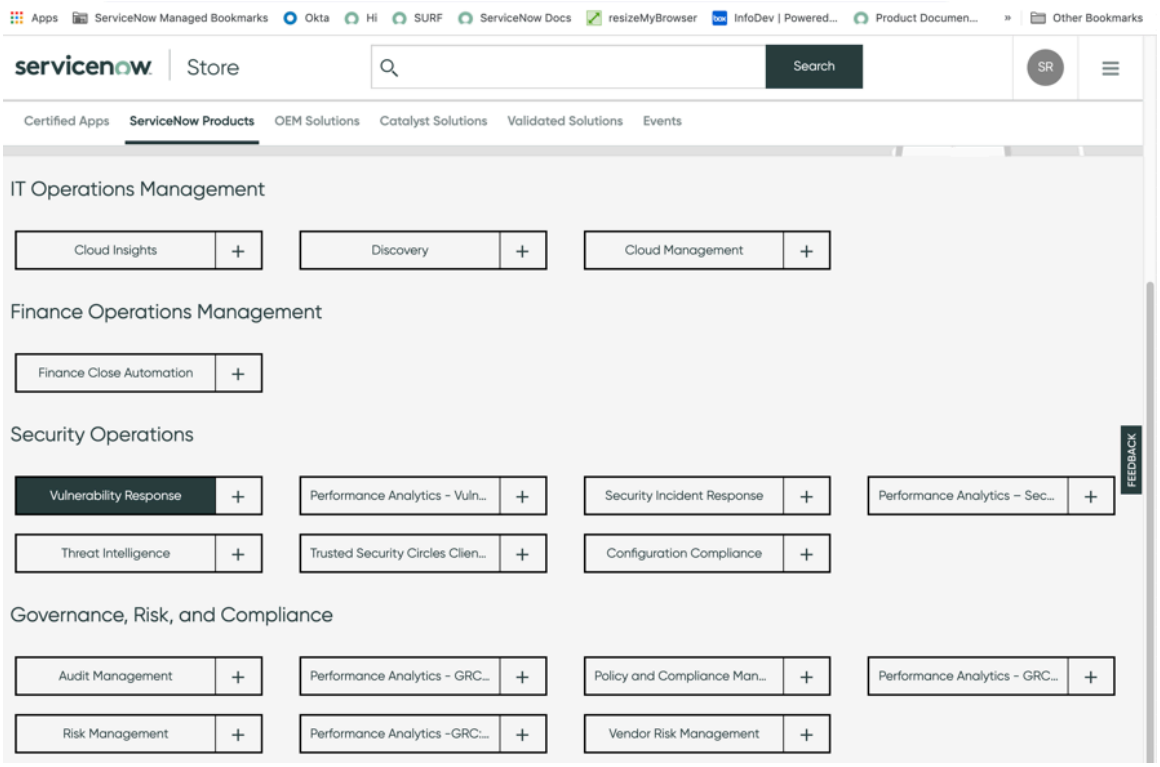
3. 표시되는 대화 상자에서 HI 자격 증명을 입력하고 로그인을 클릭합니다.

4. 표시된 페이지에서 선택하지 않은 경우 **ServiceNow** 제품 탭을 클릭합니다.

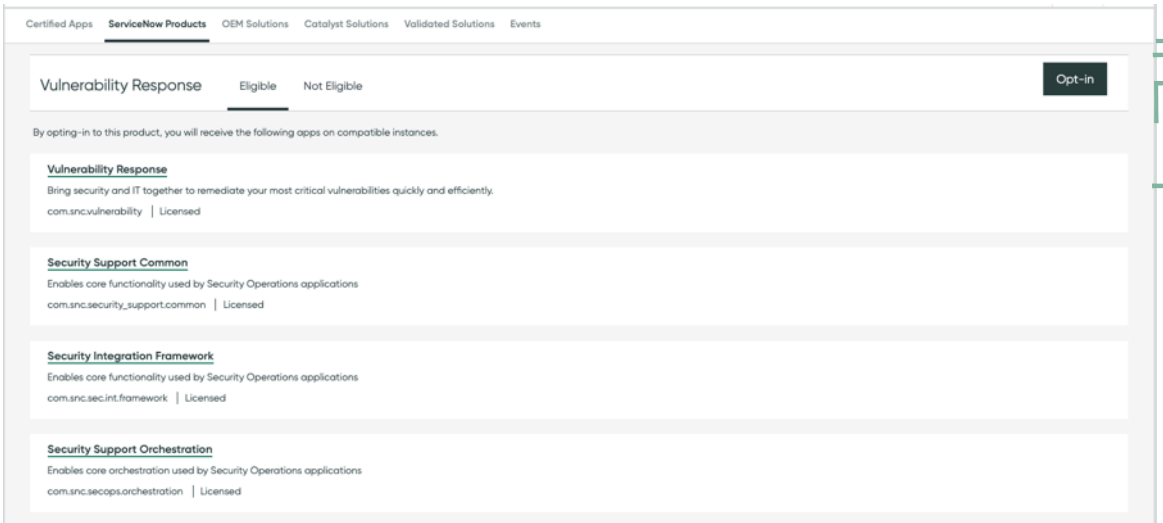


5. 애플리케이션과 함께 사용할 취약성 대응 수 있는 연결된 애플리케이션을 보려면 제품 목록 페이지에서 취약성 대응 제품을 클릭합니다.

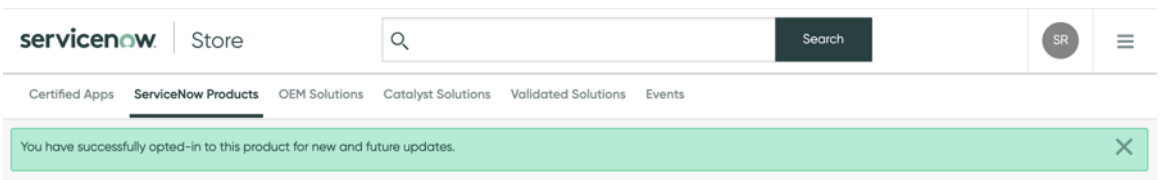
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



적격 탭에는 옵트인할 경우 사용할 수 있는 모든 애플리케이션이 나열됩니다. 애플리케이션에 대한 자세한 내용을 보려면 링크를 클릭하십시오.



6. 핵심 애플리케이션을 가져오려면 취약성 대응옵트인을 클릭합니다.
7. 사용 약관에 동의하려면 프롬프트에서 확인란을 선택하고 수락을 클릭합니다.
애플리케이션에 대해 성공적으로 옵트인했음을 나타내는 메시지가 표시됩니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

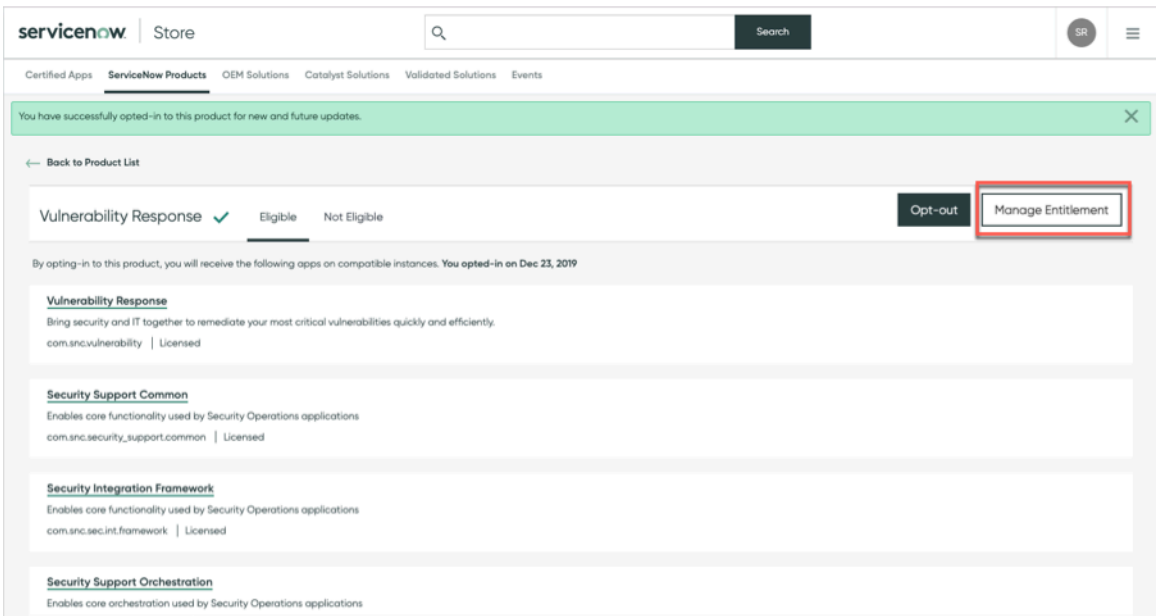
ServiceNow 제품 탭이 선택되고 표시되면 다음 그림과 같이 응용 프로그램 오른쪽 취약성 대응 의 더하기 기호가 녹색 확인 표시로 바뀝니다.

ServiceNow 제품 탭의 제품 목록 페이지에서 더하기 기호(+)를 클릭하여 권리를 얻고 클릭 한 번으로 이 페이지의 다른 애플리케이션에 대한 옵트인(opt-in)하여 사용 약관을 가져옵니다.

8. 인스턴스에 애플리케이션을 ServiceNow AI Platform 설치하려면 10단계로 건너뜁니다.
9. 옵션: 또는 다른 ServiceNow AI Platform 인스턴스에서 애플리케이션에 대한 취약성 대응 권리를 관리하려면 다음 단계를 수행합니다.

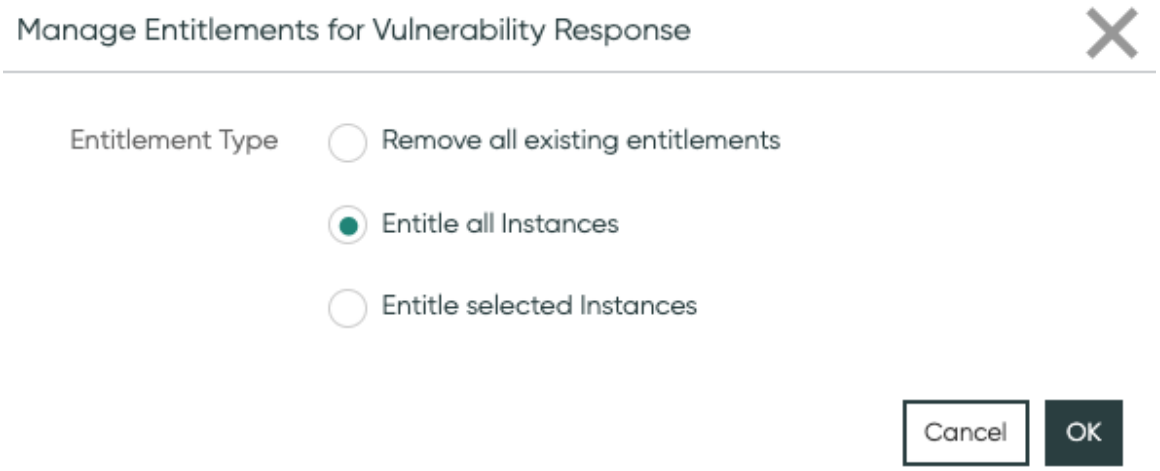
   a. 권리 관리 버튼이 표시되지 않으면 제품 목록에서 응용 프로그램을 클릭하여 취약성 대응 표시합니다.

   b. 적격 탭을 선택하고 권리 관리를 클릭합니다.



   c. 표시되는 Vulnerability Response에 대한 권리 관리 대화 상자에서 다음 중 하나를 선택합니다.

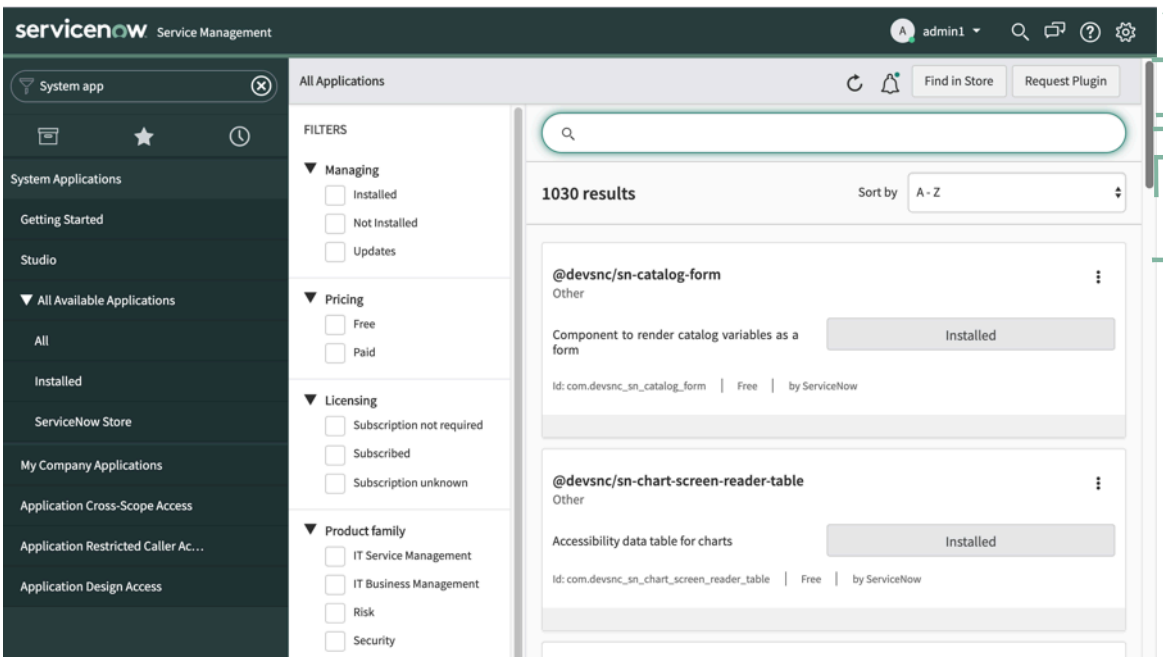
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



d. 계속하려면 확인 또는 취소를 클릭하십시오.
플러그인을 활성화하고 인스턴스에 애플리케이션을 ServiceNow AI Platform 설치할 준비가 되었습니다.

10. ServiceNow AI Platform 애플리케이션을 설치할 취약성 대응 인스턴스에 로그인합니다.

11. 다음으로 이동 모두 〉 시스템 애플리케이션 〉 모든 사용 가능 애플리케이션 〉 모두.

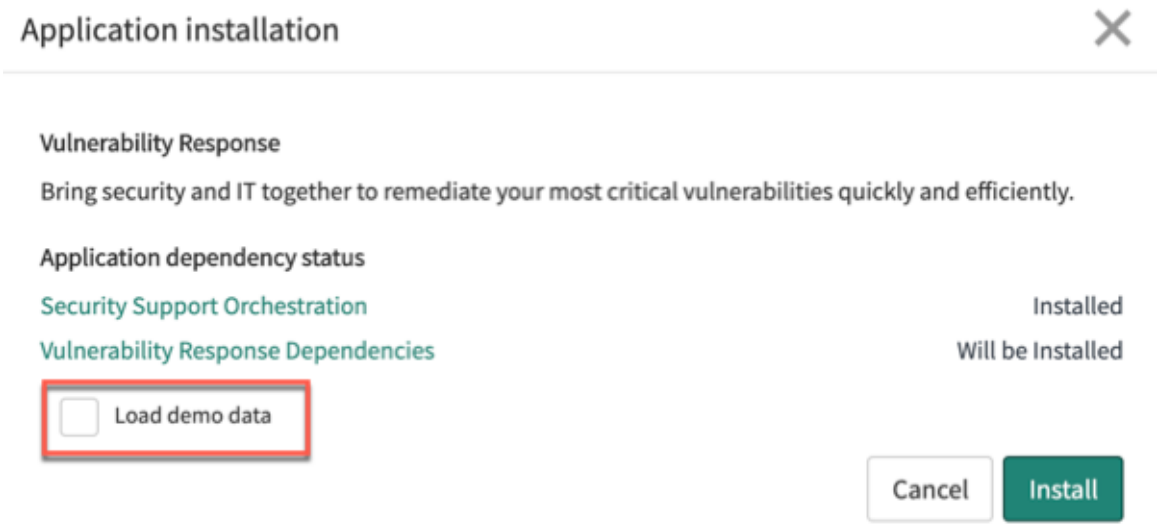


12. 나열된 애플리케이션에서 Vulnerability Response 애플리케이션(sn_vul)을 찾아 선택 목록에서 버전을 선택하고 설치를 클릭하십시오.
애플리케이션 설치 대화 상자가 표시됩니다. 설치될 모든 종속성이 표시됩니다.

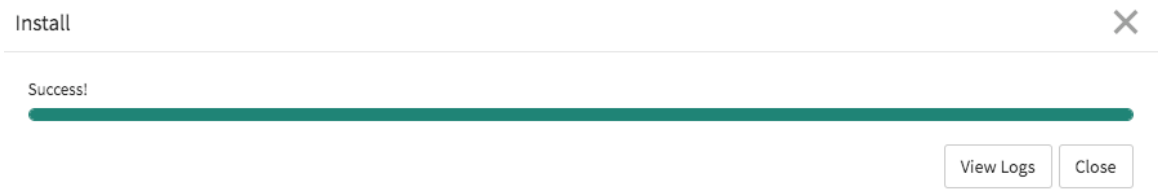
13. 옵션: 데모 데이터를 원하는 경우 데모 데이터 로드 확인란을 선택하고 설치를 클릭합니다.

주:
데모 데이터 로드 확인란을 선택하지 않으면 나중에 애플리케이션 관리자에서 데모 데이터를 설치할 수 없습니다. 초기 설치 후 데모 데이터를 설치하거나 다시 설치하는 방법에 대한 자세한 내용은 지식베이스에서 애플리케이션이 이미 설치된 경우 데모 데이터를 설치하기 위한 임시 해결책 (KB0722909) 문서를 Now Support 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



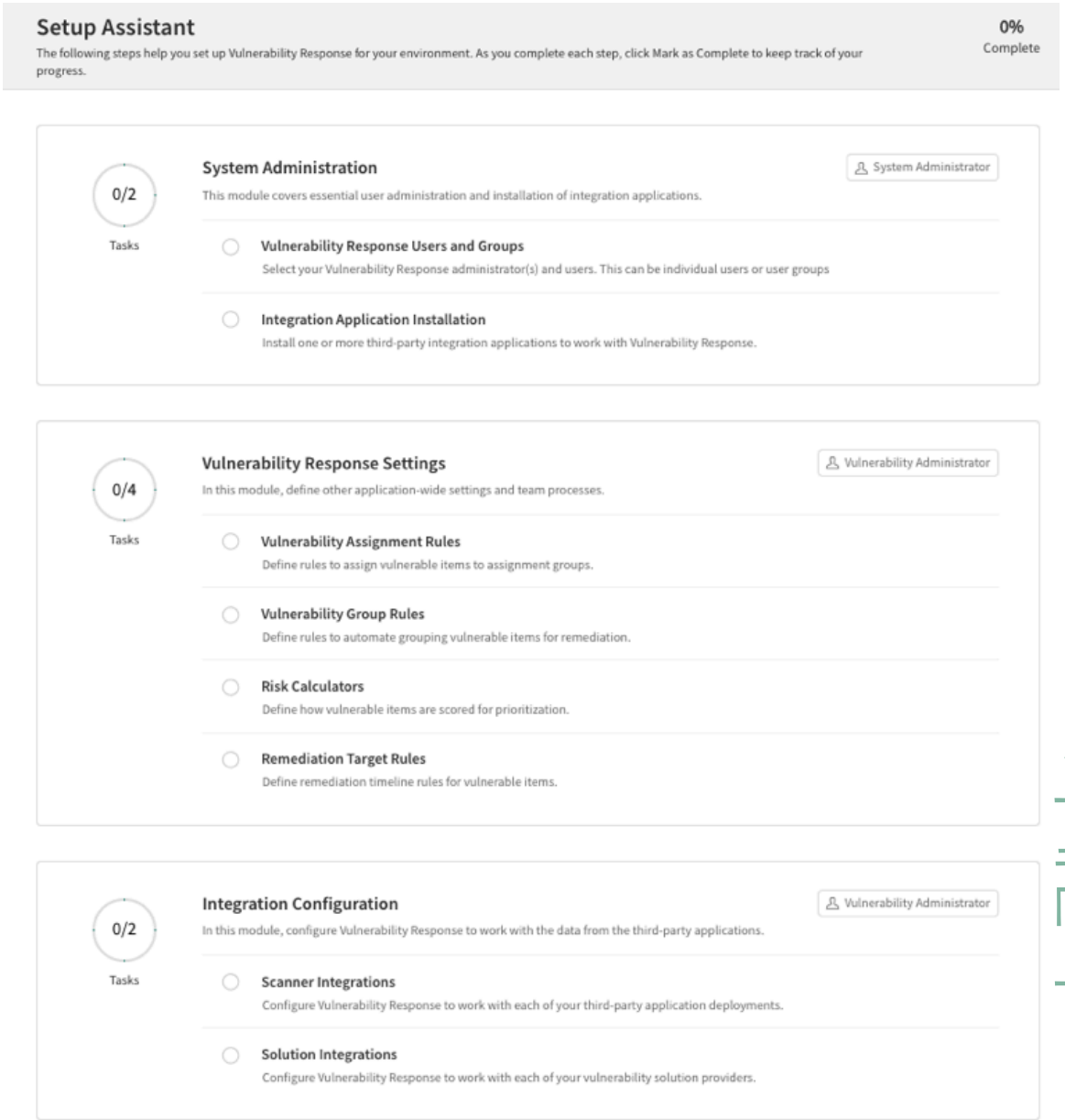
이 설치에는 다소 시간이 걸릴 수 있습니다. 애플리케이션이 성공적으로 설치된 후 설치 대화 상자에 메시지가 표시됩니다.



14. 닫기를 클릭합니다.

15. 설치가 성공적으로 완료되면 모두 〉 취약성 대응 〉 관리 〉 설정 도우미.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



16. 각 섹션의 양식에 있는 지침을 따릅니다.

다음에 수행할 작업
설정, 애플리케이션 설치, 구성, 통합, 그룹 규칙, 위험 계산기 및 정정 대상 규칙에 대한 취약성 대응 자세한 내용은 문서를 참조하십시오 설정 지원을 사용하여 구성 취약성 대응 하기.

취약성 대응 앱과 함께 설치되는 구성요소

취약성 대응 애플리케이션을 활성화하면 테이블, 사용자 역할, 예약된 작업을 포함하여 여러 유형의 구성요소가 설치됩니다.

애플리케이션과 함께 설치된 구성요소에 대해 필터링된 목록 보기

의 취약성 대응v24.0.6부터 가장 자주 사용되는 시스템 속성에 애플리케이션 내에서 액세스할 수 있습니다 취약성 대응 . 이러한 시스템 속성을 보려면 다음으로 이동합니다. 모두취약성 대응속성.

애플리케이션과 함께 설치되는 역할, 예약된 작업 및 테이블만 표시되도록 애플리케이션 파일 테이블을 필터링합니다. 해당 파일이 인스턴스와 메타데이터 테이블에 로드되도록 이러한

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

구성요소를 보려는 애플리케이션을 설치해야 합니다. 다음 단계에 따라 애플리케이션 파일 테이블에서 필터링된 목록을 봅니다.

1. 필터 탐색기에서 **sys_metadata.list** 를 입력하여 메타데이터 테이블로 이동합니다.
2. 조건 작성기(필터 아이콘)를 선택하고 애플리케이션 〉 다음과 같음 다음에 애플리케이션 이름이 표시됩니다. 예: 애플리케이션 〉 다음과 같음 〉 취약성 대응.
3. 조건 작성기에서 두 번째 필터를 추가하려면 **AND**를 선택한 뒤 클래스 〉 다음 중 하나 을 클릭하고 목록에서 역할, 예약된 작업 또는 테이블 클래스 중 하나를 선택합니다.
4. 실행을 선택합니다.

선택한 클래스의 결과가 필터링된 목록에 표시됩니다.

설치되는 역할

주:
역할, 예약된 작업 및 테이블은 애플리케이션 취약성 대응 에서 찾을 수 있습니다.애플리케이션 취약성 대응와 함께 설치되는 구성요소

역할 이름 **[name]**	설명	포함하는 역할
sn_vul_prisma.configure_prisma_integration	sn_vul_prisma_hosts_import 테이블에서 CRUD + report_view 운영을 보호하고 테이블에서 report_view 운영을 보호합니다 sn_vul_prisma_host_attrb.	
sn_vul.view_manager_workspace	보기 취약성 관리자 작업 공간.	
sn_vul.삭제	소스 기록 과 취약한 항목을 삭제합니다. v23.0 이전에는 관리자 역할이 소스 기록을 삭제할 수 있는 권한이 있었습니다.	• sn_vul_cmn.삭제 • sn_vul.delete_vulnerable_ite
sn_vul_cmn.삭제	소스 기록을 삭제합니다.	
sn_vulc.bulk_edit	테스트 결과에 대해 대량 편집 작업을 수행합니다.	
sn_vul.app_bulk_edit	애플리케이션 취약한 항목(AVIT)에 대해 대량 편집 작업을 수행합니다.	sn_vul.app_write_all
sn_vul_container.container_bulk_edit	컨테이너 취약한 항목(CVIT)에 대한 대량 편집 작업을 수행합니다.	sn_vul_container.write_all
sn_vul_cisa.configure_intelligence_integration	인텔리전스 통합을 구성합니다.	
취약성 관리자 및 선임 분석가 [sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)〕	속성 및 취약성 통합을 업데이트합니다. 취약성 통합, 정정 작업 규칙, 계산기, 정정 대상 규칙 및 작업, 보고서, 외부 공급업체 통합 구성을 포함한 관리를 위해서는 취약성 대응 sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음) 역할이 필요합니다.	• sn_vul.vulnerability_write • sn_vul.ciso_write • sn_sec_cmn.admin • sn_vul_qualys.admin(Qualys 통합이 설치된 경우) • sn_vul_r7.admin(Rapid7 취약 설치된 경우)

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

역할 이름 **[name]**	설명	포함하는 역할
		• sn_vul_shodan.admin(Shoda 익스플로잇 통합이 설치된 경우 • sn_vul.configure_nvd_integr 통합이 설치된 경우) • treemap_admin(Performanc 애플리케이션이 설치된 경우)
패치 오케스트레이션	지원되는 외부 공급업체 패치 벤더 통합을 구성합니다. 패치 데이터와 패치 기록을 보고 적용합니다.	• sn_vul_patch_orch.configure 패치를 구성하고 적용합니다. • sn_vul_patch_orch.read_pat 패치 기록과 데이터를 볼 수 있 • sn_vul_bigfix.configure_integ BigFix Patch 오케스트레이션 애플리케이션을 구성합니다. 이 사용자가 BigFix 콘솔에 연결할 허용하는 sn_vul_bigfix.read_i 및 connection_admin 세분화 포함되어 있습니다. • sn_vul_sccm.configure_integ 이 역할에는 사용자가 SCCM 콘솔에 연결하는 데 사용할 수 sn_vul_sccm.read_integratio connection_admin 세분화된 포함됩니다. • sn_vul_bigfix.read_integratio 이 역할을 가진 사용자는 취약성 BigFix 패치 오케스트레이션 통 애플리케이션 및 패치 오케스트 데이터의 기록을 보거나 읽기 권 사용할 수 있습니다. • sn_vul_sccm.read_integratio 이 역할을 가진 사용자는 취약성 Microsoft SCCM 패치 오케스 통합 애플리케이션 및 패치 오케 데이터의 기록을 보거나 읽기 권 사용할 수 있습니다.
취약성 분석가 〔sn_vul.취약성_쓰기〕	정정 작업 및 취약한 항목을 관리하고 정정 진행 상황을 모니터링하려면 sn_vul.vulnerability_write 역할이 필요합니다.	• sn_vul.모두 읽기 • sn_sc_cmn.쓰기

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

역할 이름 **[name]**	설명	포함하는 역할
		• sn_vul_qualys.user(Qualys V Integration이 설치된 경우) • sn_vul_shodan.write(Shodar 통합이 설치된 경우)
V19.0: 취약성 이벤트 관리자 〔sn_vul_analyst.vul_이벤트_관리자〕	sn_vul_analyst.vul_event_manager 역할은 새로운 취약성 또는 소프트웨어의 영향을 평가하거나 제로 데이 취약성을 추가하여 영향을 받는 자산을 식별하고 취약한 항목(VI)을 생성하는 데 사용됩니다.	• sn_sec_cmn.읽기 • canvas_user • sn_vul_analyst.emergency_r • sn_vul.노출관리_평가
기타 〔sn_vul.읽기_모두〕 sn_vul.vulnerability_read 역할은 더 이상 사용되지 않습니다.	취약성 관리에 대한 가시성이 필요한 모든 사람에게 sn_vul.read_all 역할이 필요합니다. 예를 들어 IT 및 보안 임원 또는 상위 수준 대시보드에서 대시보드 시각적 개체를 구성하는 항목으로 드릴다운하려는 사람이 있습니다. **중요사항:** 의 v24.0.6 취약성 대응부터 sn_vul.read_all 역할은 취약성 관리자 작업 공간.	• sn_sec_cmn.읽기 • sn_vul_qualys.read(Qualys 취 설치된 경우) • sn_vul_shodan.read(Shodan 통합이 설치된 경우) • pa_viewer(Performance Ana 애플리케이션이 설치된 경우) • sn_vul_tenable.read_integra 취약성 통합이 설치된 경우) • sn_vul.view_manager_works
sn_vul.read_assigned	사용자 또는 사용자의 할당 그룹에 할당된 취약한 항목을 클래식 UI와 IT 정정 작업 공간. **중요사항:** v24.0.6 부터 취약성 대응sn_vul.read_assigned 역할은 에 액세스할 수 있는 IT 정정 작업 공간권한이 있습니다.	sn_vul.view_rem_workspace
VR 시스템 임포트 관리자 [sn_vul.vr_import_admin]	시스템 실행 사용자입니다. 예약된 작업을 실행합니다. **주:** 이 사용자는 각 통합 기록에 대한 기본 실행 사용자입니다. 변경하지 마십시오.	• import_admin • sn_vul.vulnerability_write
정정 소유자 [sn_vul.remediation_owner]	본인 또는 그룹에 할당된 취약한 항목, 정정 작업에 대한 권한을 확인하고 업데이트합니다. 모든 취약성과 솔루션을 볼 수 있습니다.	itil 역할에 포함되어 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

역할 이름 **[name]**	설명	포함하는 역할
	솔루션 기록의내부 메모 필드에 대한 쓰기 권한이 있습니다.	
CISO 및 취약성 담당 임원 〔sn_vul.취약성_ciso〕	취약성 대응용 Performance Analytics에서 CISO 대시보드를 봅니다.	• sn_vul.ciso_read • sn_vul.모두 읽기
거짓 긍정 승인자 [sn_vul.false_positive_approver]	긍정 오류 요청을 승인/거부합니다.	sn_vul.view_manager_workspac
예외 승인자 [sn_vul.exception_approver]	예외 요청을 승인/거부합니다.	sn_vul.view_manager_workspac

설치되는 예약된 작업

예약된 작업	설명
호스트 및 앱 모듈에 대한 OOTB 저장된 필터 채우기	호스트 및 앱 모듈과 관련된 모듈을 마이그레이션합니다.
참조 모듈에 대한 OOTB 저장된 필터 채우기	참조 모듈과 관련된 모듈을 마이그레이션합니다.
컨테이너 모듈에 대한 OOTB 저장된 필터 채우기	컨테이너 모듈과 관련된 모듈을 마이그레이션합니다.
호스트 관련 저장된 필터 새로 고침	호스트 모듈의 저장된 필터와 관련된 모든 집계 데이터를 새로 고칩니다.
참조 관련 새로 고침 저장된 필터	CC 모듈의 저장된 필터와 관련된 모든 집계 데이터를 새로 고칩니다.
컨테이너 관련 저장된 필터 새로 고침	컨테이너 모듈의 저장된 필터와 관련된 모든 집계 데이터를 새로 고칩니다.
앱 관련 저장된 필터 새로 고침	앱 모듈의 저장된 필터와 관련된 모든 집계 데이터를 새로 고칩니다.
저장된 필터에 대해 집계 생성 및 실행 트리거	저장된 필터와 관련된 집계를 생성, 업데이트, 실행 및 새로 고침합니다.
Vulnerability Response 버전 19.0 및 Veracode	Veracode CWE 통합은 위협 정보 및 정정 권장 사항에 대한 특정 CWE(일반적인 약점 열거) 데이터를 검색합니다 Veracode .

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예약된 작업	설명
Vulnerability Integration v4.0	Veracode SBOM 통합은 소프트웨어 프로젝트의 구성요소와 Veracode 관련하여 발생하는 릴리스, 버전 및 취약성 정보를 수집합니다. 통합은 CycloneDx JSON 형식으로 SBOM을 생성하고 인스턴스에 업로드합니다 Veracode 범주 통합은 Veracode에서 향상된 범주 데이터를 검색합니다. Veracode DevOps 통합을 사용하면 DevOps 사용자가 SecOps 라이센스 없이 타사 취약성 스캔에 대한 요약 상세 정보를 볼 수 있습니다. 다음 Veracode 통합을 위한 JSON 기반 API: 애플리케이션 취약한 항목, 검사 요약, 애플리케이션 목록. 이러한 통합의 XML 기반 API 버전은 더 이상 사용되지 않습니다.
기존 VI를 자동 예외 규칙과 연결	자동 예외 규칙을 기존 VI와 자동으로 연결합니다.
취약한 탐지 자동 종결	테이블 'sn_vul_auto_close_config'에 정의된 구성에 따라 부실하고 취약한 탐지를 자동으로 종결합니다.
버전 16.1: HCL BigFix 수집, Fixlet 및 조치 통합.	HCL BigFix 제품의 패치를 사용하여 취약성에 대한 패치 배포 및 패치를 관리합니다.
모든 솔루션의 관련 개수를 계산합니다.	기본적으로 비활성 상태입니다. 솔루션 데이터를 지속적으로 처리하는 대신 야간에 한 번 처리합니다. v22.0부터 요청 시에만 이 작업을 실행할 수 있습니다. 이 예약된 작업은 모든 솔루션을 처리하므로 성능에 영향을 줄 수 있습니다. 따라서 솔루션 데이터가 손상된 경우 이 작업을 한 번만 실행하는 것이 좋습니다.
취약성 및 정정 작업에 대한 관련 VI 수 계산	해당 날짜의 수동 및 VI 임포트 변경 내용을 캡처합니다. 취약성 및 솔루션 관계를 조정하고 합계를 다시 계산합니다. 솔루션 데이터는 취약성 솔루션 메트릭 큐 프로세스 예약 작업에 의해 별도로 큐에 추가되고 처리됩니다.
MID 서버 시간 제한 확인	MID 서버를 ping하고 30초 후에 오류를 출력합니다.
V19.0: 잠재적인 취약성 노출 확인	델타 CVE, 소프트웨어 및 설치를 처리하여 노출을 가져옵니다.
실행 상태 WaitComplete 확인	통합 실행이 완전히 완료된 것으로 확인되면 완료로 표시합니다.
취약한 항목 및 그룹 확인 연기 만료	취약한 항목 또는 취약성이 만료된 경우(그리고 1주일 후에 만료되는 경우) 알림을 보냅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예약된 작업	설명
	지연된 VI에 예외 규칙을 적용할 수 있는지 확인하고 예외 규칙에 따라 이유 및 **Until** 필드를 업데이트합니다. VI의 상태는 최근 만료 날짜까지 지연됨 상태로 유지됩니다.
CI가 연결되지 않은 취소 VIT 닫기	연결된 CI(구성 항목)가 없고 3일 동안 업데이트되지 않은 취약한 항목을 자동으로 종결합니다. 상태가 종결/취소됨으로 설정됩니다.
exp 기록 삭제 시 VI 닫기	VI가 삭제되면 닫습니다.
준수 결과 통합	구성 준수 애플리케이션에서 처리할 신뢰할 수 있는 소스가 있는 정책, 구성 테스트(통제) 및 인용과 함께 테스트 결과를 임포트합니다.
준수 결과 백필 통합	자산 통합과 Tenable.io 함께 실행되는 체인 통합의 일부로, 검색된 무시된 자산에 대한 구성 평가 데이터를 임포트합니다(자산 통합을 통해 임포트됨).
CR 상태 동기화	스크립트는 기존의 모든 정정 작업을 CHG 관계로 개조하여 동기화합니다. 앞으로 동기화를 활성화합니다.
버전 15.0 스캔 자격 증명 통합	요청 시 다시 스캔을 위해 스캐너에 액세스하는 데 사용되는 자격 증명을 임포트하여 안전하게 Tenable.io 저장합니다.
CWE Comprehensive 2000 통합	MITRE Corporation에서 큐레이팅한 CWE(Common Weakness Enumeration) 데이터 세트에서 취약성 정보를 가져오는 취약성 통합입니다.
V18.0: 부실 분할 작업 기록 삭제	분할 작업 중간 테이블에서 부실 기록을 정리하는 일일 작업입니다.
솔루션 애플리케이션이 활성화되지 않은 경우 VR 솔루션 사용 안 함	애플리케이션이 설치되지 않은 경우 취약성 대응용 솔루션 관리 기능을 비활성화하고 숨깁니다취약성 솔루션 관리.
정정 대상 평가	모든 취약한 항목에 대한 정정 목표 날짜를 설정하거나 업데이트합니다. 규칙에 대한 정정 목표 날짜의 상태를 결정합니다.
• Rapid7의 업데이트된 키에 대한 탐지 수정 • Qualys의 업데이트된 키에 대한 탐지 수정 • Tenable의 업데이트된 키에 대한 탐지 수정	로의 업그레이드 취약성 대응후 트리거되는 통합별 예약된 작업에 의해 탐지 데이터를 자동으로 정리합니다.
버전 16.1: 정정 다이제스트 생성	이 작업은 정정 소유자 사용자 그룹의 모든 사용자에 대한 이메일 다이제스트를 자동으로 생성합니다. 이 작업은 기본적으로 활성화됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예약된 작업	설명
V19.0: CISA 악용 CVE를 노출 구성에 삽입	CISA CVE를 노출 구성 테이블에 삽입하여 노출을 계산합니다.
V18.0: 통합 정정 작업에 클래식 정정 작업 삽입	클래식 UI에서 만든 모든 정정 작업을 sn_vul_remediation_task(통합 정정 작업)에 삽입하는 일회성 예약 작업입니다.
Microsoft 보안 응답 센터 솔루션 통합	취약성 솔루션 관리 에서 솔루션을 검색하는 통합입니다 Microsoft Security Response Center.
버전 16.1: Microsoft SCCM 수집, 패치 업데이트 및 배포 통합	SCCM 패치를 사용하여 Microsoft 취약성에 대한 패치 및 패치 배포를 관리합니다.
제한된 통합 프로세스 선택	에 Shodan Exploit 통합대한 통합 프로세스를 생성합니다.
영향을 받는 제품 텍스트 채우기	업그레이드 후에는 기존 솔루션을 처리하여 영향을 받는 제품 텍스트를 채웁니다. 이 작업은 한 번만 실행됩니다.
새 CR 카운트 열 채우기	정정 작업 〔sn_vul_vulnerability〕 테이블에 기존 데이터가 있는 고객의 새 CR 카운트 열을 자동으로 채웁니다.
취약성 솔루션 메트릭 큐 처리	다음을 통해 큐에 대기 중인 솔루션 데이터를 처리합니다. • NVD 항목에서 외부 공급업체 항목으로 솔루션 롤업 • 취약성에 대한 기본 솔루션 채우기 및 • 솔루션에서 정정 상태 메트릭 업데이트 또한 업데이트 상태로 표시된 솔루션도 처리합니다. 주: 만 사용하는 Rapid7경우 이 예약 작업을 비활성화하여 성능을 개선할 수 있습니다.
취약성 벤더 매핑 테이블의 기록 채우기 Rapid7 취약성에 대한 취약성 벤더 매핑 테이블의 기록 채우기	기존 취약성에 대한 취약성 벤더 매핑 테이블에 기록을 삽입합니다.
지연된 취약성 그룹 다시 열기	연기 날짜가 지나면 지연된 정정 작업을 다시 엽니다.
모든 취약성 담당 규칙 다시 적용	모든 오픈 VI에 대해 담당 규칙을 재평가합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예약된 작업	설명
버전 16.5: 담당 규칙의 재할당 횟수	매일 실행되며 특정 할당 규칙에 대해 이 기능에 의해 할당되지 않은 총 VI 및 정정 작업 수를 게시합니다.
Red Hat Solution Integration	취약성 솔루션 관리 에서 솔루션을 검색하는 통합입니다 Red Hat Security Advisory.
V17.1: 정정 작업에서 중복 VIT 새로 고침 및 해결	"중복 VI 자동 새로 고침"이 활성 상태인 정정 작업의 항목에 대해 중복된 취약한 항목을 찾습니다.
비정정 작업에 대해 연관된 취약한 항목 새로 고침 규칙 기반 정정 작업	필터 그룹 및 조건 그룹 기준과 일치하는 취약한 항목으로 정정 작업을 업데이트합니다.
마지막으로 열고 닫은 잘못된 취약한 항목 복구	이전에 수정한 결함으로 인해 손상된 기존 UI 데이터를 복구합니다.
계산기 다시 실행	변경의 영향을 받는 취약한 항목에 계산기를 다시 적용합니다. 이렇게 하면 정정 작업의누적 위험 점수가 다시 계산됩니다. **주:** 환경에 따라 계산기를 다시 실행하는 데 시간이 오래 걸릴 수 있습니다.
취소된 통합 임포트 세트 재시도	재시도 취소된 통합 임포트 세트입니다. 5회 재시도한 후 오류를 반환합니다.
통합 프로세스 재시도	통합 프로세스를 재시도합니다. 5회 재시도한 후 오류를 반환합니다.
취약한 항목 값을 취약성 및 그룹에 롤업	롤업 계산기를 사용하여 정정 작업에 대한 위험 점수, 취약한 항목 수 및 정정 목표 상태를 계산합니다. **주:** 의 취약성 대응v23.0부터 예약된 작업이 개선되어 멀티스레딩 기능이 있는 백그라운드 작업을 생성할 수 있습니다. 이 업그레이드에는 작업을 여러 개의 더 작은 하위 작업으로 분할하는 작업이 포함되며, 이러한 작업은 병렬로 또는 동시에 실행됩니다. 이렇게 수정하면 여러 기록을 동시에 처리할 수 있으므로 전체 작업 속도가 크게 향상됩니다.
취약성 항목 승격 후 심각도 계산기 실행	이전에 누락된 취약성이 해당 점수 및 외부 공급업체 제공자의 기타 데이터(예 Qualys Cloud Platform: , Rapid7 Nexpose)로 업데이트된 후 심각도 계산기를 실행합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예약된 작업	설명
	주: 의 취약성 대응v25.0.3부터 예약된 작업이 개선되어 멀티스레딩 기능을 사용하여 백그라운드 작업을 생성합니다. 이 업그레이드에는 작업을 여러 개의 더 작은 하위 작업으로 분할하는 작업이 포함되며, 이러한 작업은 병렬로 또는 동시에 실행됩니다. 이렇게 수정하면 여러 기록을 동시에 처리할 수 있으므로 전체 작업 속도가 크게 향상됩니다.
V19.0: 구성된 CVE에 대한 노출 평가 실행	노출 구성 테이블의 모든 CVE 기록에 대한 노출을 계산합니다.
V19.0: 소프트웨어 노출 실행	노출 구성 테이블의 모든 소프트웨어 기록에 대한 노출을 계산합니다.
예약된 취약성 데이터 소스 프로세서	임포트 큐에서 처리할 항목을 확인하고 사용 가능한 자원에 따라 예약된 임포트 작업을 할당합니다.
예약된 취약성 통합 프로세스 첨부 파일 정리	통합 XML 첨부 파일이 14일이 지나면 제거합니다. 이 보존 시간은 구성할 수 없습니다.
예약된 취약성 통합 시간 제한 검사기	완료하는 데 60분 이상 걸리는 통합 실행을 취소합니다.
VI에 대한 관련 CI 서비스 설정	통합 임포트가 완료되면 지정된 시간에 취약한 항목에 연결된 CI에 영향을 받는 비즈니스 서비스가 연결됩니다. 자세한 내용은 의 서비스 매핑 취약성 대응 문서를 참조하십시오.
지연 수 설정	취약한 항목, 애플리케이션 취약한 항목, 컨테이너 취약한 항목 또는 정정 작업이 지연된 횟수를 수집합니다.
다음 통합 트리거	연결된 통합 실행에서 다음 통합을 트리거합니다.
템플릿 통합	재스캔 중에 단일 템플릿 기록이 Tenable.io 전송됩니다.
그룹화되지 않은 취약한 항목 업데이트	취약한 항목이 정정 작업에 있는지 확인하고 그룹화되지 않은 취약한 항목 목록에서 추가하거나 제거합니다. 주: 이 작업은 업그레이드 후에 실행되며 데이터 세트에 따라 완료하는 데 시간이 오래 걸릴 수 있습니다.
VG의 취약성 업데이트	업그레이드 후 sn_vul_vulnerabilty(정정 작업) 테이블의 취약성 필드를 업데이트합니다. 이 작업은 한 번 트리거되고 이후에는 비활성화됩니다.
취약성 임포트 템플릿	임포트 큐를 처리하는 엔진입니다. 10개 중 하나입니다.
취약성 대응 종결 기간 업데이트	VI 테이블에서 종결 연령 열을 업데이트합니다.
취약성 대응 CI 수	지난 30일 동안 외부 공급업체 스캐너로 검사한 CI 수를 계산합니다.
Vulnerability Response 위험	업그레이드할 때 데이터에 대한 위험 등급을 업데이트합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예약된 작업	설명
및 정정 상태 업그레이드	
v20.0: 위험 완화 만료 확인	취약한 항목 및 정정 작업에 대한 보상 통제가 만료되었는지 확인합니다. 만료되면 위험 점수를 원래 위험 점수로 되돌리고 보상 통제가 만료되었음을 나타내는 이메일 알림을 보냅니다. 보상 통제가 7일 이내에 만료되도록 설정된 경우에도 이메일 알림을 보냅니다.

설치되는 테이블

테이블	설명
v24.0.6 Prisma 호스트 임포트 [sn_vul_prisma_hosts_import]	호스트의 임포트 세트 테이블입니다.
v24.0.6 Prisma 호스트 속성 [sn_vul_prisma_host_attrb]	호스트 통합을 위한 자산 속성 테이블입니다.
v22.0 sn_vul_cmn_auto_close_rule	필터 조건에 따라 부실 탐지를 자동으로 종결합니다.
sn_vul_cmn_ws_saved_filter	저장된 필터의 데이터를 저장합니다.
sn_vul_licensing_usage	중복 자산, 불완전한 IP 자산, 총 스캐너 자산 수 및 최종 사용량을 포함합니다.
sn_vul_m2m_entry_compensating_control	취약성 항목과 보상 통제 간의 연결을 나타냅니다.
v21.0 Rapid7 스캔 엔진 [sn_vul_r7_scan_engine)	스캔하는 동안 자산을 검색하고 취약성을 검사하는 임포트한 스캔 엔진 데이터를 저장합니다.
v21.0 Rapid7 스캔 엔진 임포트 [sn_vul_r7_scan_engine_import]	Rapid7 스캔 엔진 통합에서 처리 전에 임포트 데이터를 준비하는 데 사용됩니다.
버전 19.0: [sn_vul_veracode_cwe_import]	CWE 정정 권장 사항에 대한 Veracode 범주 테이블을 확장합니다.
버전 19.0: [sn_vul_veracode_category_import]	임포트한 범주 데이터를 저장합니다.
버전 19.0: [sn_vul_veracode_sbom_import]	Veracode에서 가져온 임포트 SBOM 데이터를 저장합니다.
V17.1: VI 키에 증명 추가 [sn_vul_proof_key_vulnerability]	VI 키에 증거를 포함해야 하는 Rapid7 취약성입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테이블	설명
	의 취약성 대응v24.0.6부터 'Tenable VIT를 분할하는 정규 표현식' 열이 추가됩니다. 페이로드에서 증명을 구문 분석하는 데 사용되는 사용자가 입력한 정규 표현식을 저장합니다.
평가된 취약한 항목 [sn_vul_m2m_exp_sw_vi]	정정 작업을 생성하는 동안 할당 그룹에 정정 작업을 할당합니다.
할당 규칙 [sn_vul_vgr_assignment_rule]	정정 작업을 생성하는 동안 할당 그룹에 정정 작업을 할당합니다. v15.0 이전: 정정 작업을 생성하는 동안 할당 그룹에 정정 작업을 할당합니다.
변경 요청 연결 [sn_vul_action_associate_cr]	새 정정 작업-CHG 연결을 처리하는 데 사용되는 스테이징 테이블입니다. v15.0 이전: 새 VG-CHG 연결을 처리하는 데 사용되는 스테이징 테이블입니다.
비동기 취약한 항목 작업 [sn_vul_async_vi_job]	취약한 항목을 처리하는 백그라운드 작업을 포함합니다. 하나의 작업 유형만 지원됩니다. 취약성을 대량으로 편집하는 데 사용됩니다.
비동기 취약한 항목 작업 유형 [sn_vul_async_vi_job_type]	백그라운드 작업의 유형을 포함하고 관련 스크립트를 참조합니다. **VulnerabilityBulkEditProcessor** 프로세서가 하나만 있습니다.
부실 항목 탐지 자동 종결 [sn_vul_auto_close_config]	부실 탐지를 자동으로 종결하는 방법에 대한 구성을 저장합니다.
취약한 항목 세분성 구성 [sn_vul_action_vi_granularity_config]	구성 페이지에서 포트 포함을 활성화하거나 비활성화하는 데 사용되는 UI 양식을 VI 세분성 구성 모듈에 저장합니다.
변경 요청 작성 [sn_vul_action_create_cr]	정정 작업에서 변경 요청을 생성하는 데 사용됩니다.
취약한 항목 생성 [sn_vul_action_create_vi]	정보의 자리 표시자로 사용되는 준비 테이블입니다. 이 테이블에는 기록이 저장되지 않습니다.
컬렉션 [sn_vul_patch_orch_collection]	개별 인스턴스의 컬렉션 데이터를 저장합니다.
CWE [sn_vul_cwe]	CWE(일반적인 약점 및 열거) 소프트웨어 취약성 카탈로그입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테이블	설명
CWE 적용 가능 플랫폼 [sn_vul_cwe_m2m_cwe_platform]	임포트한 CWE 적용 플랫폼 데이터를 포함합니다.
CWE 범주 [sn_vul_cwe_category]	임포트한 CWE 범주 데이터를 포함합니다.
CWE 일반적인 결과 [sn_vul_cwe_consquence]	임포트한 CWE 공통 결과 데이터를 포함합니다.
CWE 외부 참조 [sn_vul_cwe_reference]	임포트한 CWE 외부 참조 데이터를 포함합니다.
CWE 관찰 예 [sn_vul_m2m_cwe_cve]	임포트한 CWE CVE 데이터를 포함합니다.
CWE 플랫폼 [sn_vul_cwe_platform]	임포트한 CWE 플랫폼 데이터를 포함합니다.
CWE 외부 참조 [sn_vul_cwe_reference]	임포트한 CWE 관련 외부 참조 데이터를 포함합니다.
CWE 관계 [sn_vul_m2m_cwe_relation]	임포트한 CWE 관계 데이터를 포함합니다.
CWE 뷰 [sn_vul_cwe_view]	임포트한 CWE 뷰 데이터를 포함합니다.
CWE 약점 [sn_vul_cwe_weakness]	임포트한 CWE 약점 데이터를 포함합니다.
버전 16.1: 장치 컬렉션 [sn_vul_patch_orch_m2m_src_ci_collection]	검색된 항목에 대한 컬렉션 데이터를 저장합니다.
버전 16.1: 장치 업데이트 [sn_vul_patch_orch_m2m_src_ci_update]	배포 상태와 함께 검색된 항목 기록에 표시되는 배포된 패치에 대한 데이터를 저장합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테이블	설명
디스커버리 모델 취약한 소프트웨어 일치 [sn_vul_discovery_model_software_match]	취약한 소프트웨어와 검색 모델의 일치를 보완합니다.
예외 관리 구성 [sn_vul_exception_config]	예외 관리 기능에 대한 구성 설정을 저장합니다.
예외 규칙 [sn_vul_auto_exception_rule]	예외 관리에 대해 평가된 규칙 집합을 포함합니다.
익스플로잇 [sn_vul_exploit]	익스플로잇의 정의를 포함합니다. 취약성을 이용하는 공개적으로 사용 가능한 코드입니다.
익스플로잇 프레임워크 sn_vul_exploit_framework	익스플로잇 프레임워크의 이름을 포함합니다: 많은 익스플로잇을 실행할 수 있는 전체 소프트웨어 패키지입니다.
노출된 디스커버리 모델 [sn_vul_m2m_exp_sw_model]	검색 모델과 취약성 노출 평가 간의 매핑을 저장합니다.
노출 평가 [sn_vul_exp_by_sw]	노출 평가를 위한 기록을 저장합니다.
V19.0: 노출 매니페스트 sn_vul_analyst_exposure_manifest	델타 처리를 위한 매니페스트 테이블입니다.
노출 취약성 항목 [sn_vul_m2m_entry_exp]	취약성(sn_vul_entry)과 노출 평가 간의 매핑을 저장합니다.
맬웨어 키트 [sn_vul_malware_kit]	맬웨어 키트의 세부 정보 포함: 추가 코딩 또는 구성 작업 없이 익스플로잇 또는 관련 익스플로잇 집합을 쉽게 실행할 수 있도록 미리 작성된 도구
자산 테이블 〔sn_vul_tenable_missing_asset〕 누락	일치하지 않는 자산이 있는 무시된 구성 준수 평가 데이터에 대한 임시 자산 ID를 포함합니다.
Microsoft 응답 센터 솔루션 업데이트 [sn_vul_msrc_update]	Microsoft에서 솔루션 데이터를 마지막으로 업데이트한 시간을 포함합니다. 다운로드할 델타 데이터를 결정하기 위해 야간 임포트와 비교하는 데 사용됩니다.
Microsoft Security Response Center 솔루션 임포트 [sn_vul_msrc_solution_import]	Microsoft 보안 응답 센터 솔루션 통합에서 임포트 데이터를 처리하기 전에 스테이징하는 데 사용됩니다.
Microsoft Security Response Center 솔루션 통합	에 Microsoft Security Response Center 솔루션 통합대한 취약성 통합 〔sn_vul_integration〕 테이블을 확장합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테이블	설명
[sn_vul_msrc_integration]	
국가 취약성 데이터베이스 항목 [sn_vul_nvd_entry]	NIST 국가 취약성 데이터베이스에서 문서화된 취약성입니다.
NVD CVSS 임포트 [sn_vul_nvd_cvss_import]	NVD 임포트 중에 스키마로 취약성 대응 아직 변환되지 않은 준비 데이터를 포함합니다.
버전 16.1 〔sn_vul_patch_orch.패치_승인_필수〕	패치 통합에서 패치 배포가 예약되면 수준 1 - 패치 업데이트 승인 그룹에 할당된 사용자에게 검토 및 승인을 위해 요청이 제출됩니다. 이 속성은 기본적으로 활성화됩니다.
버전 16.1: 패치 배포 [sn_vul_patch_orch_deployment]	컬렉션 및 CI에 대해 배포된 패치에 대한 정보를 저장합니다.
버전 16.1: 패치 업데이트 [sn_vul_patch_orch_update]	개별 인스턴스에서 사용할 수 있는 패치에 대한 정보를 저장합니다.
버전 16.1: 잠재적 패치 [sn_vul_patch_orch_m2m_vuln_patch]	취약성을 해결하는 데 사용될 수 있는 패치를 식별하는 패치 및 취약성에 대한 데이터를 저장합니다.
V19.0: 잠재적 취약성 노출 sn_vul_analyst_m2m_pot_exp_sw_model	CVE에 대한 노출 평가 테이블입니다.
제품 범주 [sn_vul_product_category]	임포트한 제품 범주 데이터를 포함합니다.
Red Hat Security Advisory [sn_vul_rhsa_update]	솔루션을 야간 작업과 비교하여 Red Hat 임포트할 델타 데이터를 결정합니다.
Red Hat 솔루션 임포트 [sn_vul_rh_solution_import]	처리 전에 임포트 데이터를 스테이징하는 데 Red Hat Solution Integration 사용됩니다.
Red Hat Solution Integration [sn_vul_rh_integration]	에 Red Hat Solution Integration대한 취약성 통합 〔sn_vul_integration〕 테이블을 확장합니다.
관련 비즈니스 서비스 [sn_vul_m2m_ci_services]	영향을 받는 서비스 조회를 위해 CI를 비즈니스 서비스에 연결합니다. 서비스 매핑에서 추가되었는지 여부를 나타내는 플래그를 포함합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테이블	설명
V18.0: 정정 작업 수 [sn_vul_daily_count_re]	정정 작업의 일일 카운트입니다. 이 테이블은 매일 업데이트됩니다.
V18.0: 정정 작업 기록 [sn_vul_remediation_effort_record]	RE(정정 작업)에 대한 정정 진행률을 추적합니다. RE에 대한 참조를 포함합니다.
정정 대상 규칙 [sn_vul_ttr_rule]	취약한 항목을 정정하기 위한 예상 시간 범위를 정의합니다. 애플리케이션 파일을 확장합니다.
V18.0: 정정 작업 [sn_vul_remediation_task]	VR, AVR, CVR 및 테스트 결과 그룹에 대한 모든 정정 작업을 저장합니다. [sn_vul_vulnerability] 테이블 기록과 관련된 정보로 구성됩니다. [sn_vul_vulnerability] 테이블 목록 뷰에서 기록을 볼 수 없는 사용자는 [sn_vul_remediation_task] 테이블 목록 뷰에서 해당 기록 정보를 볼 수 있습니다. 이 테이블은 취약성 관리자 작업 공간 또는 IT 정정 작업 공간의 사용자가 액세스할 수 있습니다
REST 통합 [sn_vul_rest_integration]	REST 기반 통합을 위해 취약성 통합 〔sn_vul_integration〕 테이블을 확장합니다.
SAM NVD 취약성 탐지 [sn_vul_sam_config]	SAM NVD로 모니터링되는 CI 및 취약성과 SAM NVD 취약성 탐지 사용 여부를 포함합니다.
예약된 임포트 풀 [sn_vul_sched_import_pool]	동시 데이터 소스 임포트를 용이하게 하는 데 사용되는 예약된 임포트 세트 기록의 컬렉션입니다.
취약한 항목 선택 [sn_vul_action_select_vi]	분할 VG를 처리하고, CHG를 만들고, CHG를 연결하는 데 사용되는 기본 준비 테이블
설정 상태 [sn_vul_setup_status]	내부 전용: 설정 도우미에서 사용됩니다. 설정 도우미가 열릴 때마다 완료된 단계의 상태가 표시되고 오른쪽 상단 모서리의 백분율은 이 표에서 가져옵니다.
심각도 맵 [sn_vul_severity_map]	소스 심각도에서 정규화된 심각도로의 매핑을 포함합니다.
솔루션 스캐너 매핑 [sn_vul_solution_scanner_mapping]	제외 또는 포함을 위해 벤더, 스캐너 및 키워드를 매핑합니다.
분리 정정 작업	정정 작업을 분할하는 데 사용되는 스테이징 테이블입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테이블	설명
[sn_vul_action_split_vg]	
외부 공급업체 취약성 항목 [sn_vul_third_party_entry]	외부 공급업체 소스에서 제공한 문서화된 취약성입니다.
[sn_vul_tenable_io_template	템플릿 기록은 소스로 있는 Tenable.io 항목으로 전송된 Tenable.io 다음 다시 스캔하는 동안 임포트됩니다.
매니페스트 업데이트 [sn_vul_update_manifest]	업데이트되어 롤업 계산기로 다시 계산해야 하는 정정 작업의 목록입니다.
V17.1: CI 클래스별 사용량 [sn_vul_licensing_usage_by_ci_classes]	CI 클래스별로 집계된 사용 횟수를 포함합니다.
VR 구성 항목 수 [sn_vul_vr_configuration_item_count]	외부 공급업체 통합에서 임포트한 구성 항목의 90일 연속 누적 평균을 포함합니다.
취약성 담당 규칙 [sn_vul_assignment_rule]	VI에 할당 그룹을 설정하기 위해 평가된 규칙 세트를 포함합니다.
취약성 계산기 [sn_vul_calculator_group]	취약성 계산기 규칙을 포함합니다. 계산기 순서에 따라 먼저 평가되는 계산기가 결정되며, 각 계산기에서 최대 하나의 계산기 규칙이 사용됩니다.
취약성 계산기 규칙 [sn_vul_calculator]	모든 계산기에 대한 규칙을 포함합니다. 각 계산기에 대해 계산기 규칙을 순서대로 검토합니다. 조건과 일치하는 첫 번째 계산기는 해당 규칙 내의 값을 사용합니다.
취약성 CVE [sn_vul_m2m_entry_cve]	NVD CVE(Common Vulnerability Exposures) 데이터를 취약한 항목에 연결합니다.
취약성 데이터 소스 임포트 큐 항목 [sn_vul_ds_import_q_entry]	데이터 소스에서 처리되기 전에 첨부 파일을 큐에 넣습니다. 취약성 통합에 활용됩니다.
취약성 항목 [sn_vul_entry]	문서화된 취약성입니다.
취약성 항목 검사 [sn_vul_entry_scan]	검사와 취약성 항목 간의 관계를 저장합니다.
취약성 익스플로잇 프레임워크 [sn_vul_m2m_framework_vul]	익스플로잇 프레임워크와 취약성 간의 관계를 포함합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테이블	설명
V19.0: 취약성 노출 평가 sn_vul_analyst_sam_config	CVE에 대한 노출 평가 구성 테이블입니다.
취약성 세분성 구성 [sn_vul_granularity_config]	VI 세분성 구성 모듈에 대한 포함 또는 제외 포트 상태를 저장하고 유지 관리합니다.
정정 작업 [sn_vul_vulnerability]	정정을 위해 조직된 취약한 항목의 컬렉션입니다.
정정 작업 변경 요청 [sn_vul_m2m_vg_change_request]	정정 작업 및 CHG 요청의 연결을 저장합니다.
정정 작업 항목 [sn_vul_m2m_vul_group_item]	정정 작업 및 취약한 항목의 연결입니다.
정정 작업 규칙 [sn_vul_grouping_rule]	취약한 항목 집합에 대해 그룹이 자동으로 생성되는 기준을 정의하는 규칙을 포함합니다.
취약성 통합 [sn_vul_integration]	외부 소스에서 취약성 데이터를 임포트하기 위한 예약 가능한 기록입니다. 예약된 스크립트 실행을 연장합니다.
취약성 통합 데이터 소스 [sn_vul_int_data_src]	취약성 통합에 사용할 데이터 소스입니다.
취약성 통합 로그 [sn_vul_integration_log]	취약성 통합 실행에 의해 출력된 로그 정보를 기록합니다.
취약성 통합 프로세스 [sn_vul_integration_process]	취약성 통합에 대한 단일 프로세스 발생입니다.
취약성 통합 큐 [sn_vul_integration_queue]	모든 데이터 소스가 사용 중일 때 통합 실행을 위한 임포트 요청을 큐에 넣습니다.
취약성 통합 실행 [sn_vul_integration_run]	취약성 통합 발동. 주: 통합 실행이 진행 중인 경우 하나의 통합만 백로그에서 준비 상태일 수 있습니다.
취약성 통합 실행 통계 [sn_vul_integration_stats]	통합 실행을 위한 각 단계의 세부 항목(예: REST API 시간, VI 생성 시간 등)을 저장합니다.
취약성 항목 작업	문제, 변경 및 보안 인시던트와 관련된 취약한 항목입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테이블	설명
[sn_vul_m2m_item_task]	
취약성 맬웨어 키트 [sn_vul_m2m_malware_kit_vul]	취약성과 맬웨어 키트 간의 관계를 포함합니다.
취약성 필수 솔루션 [sn_vul_m2m_solution_prerequisite]	사용 가능한 경우 솔루션을 적용하기 위한 소스별 필수 구성 요소를 포함합니다.
취약성 속도 제한 [sn_vul_rate_limit]	스캐너에서 사용할 요율 제한을 정의합니다.
취약성 참조 [sn_vul_reference]	알려진 취약성에 대한 외부 참조입니다.
취약성 개선 상태 [sn_vul_m2m_ttr_status]	가장 근접하게 적용된 정정 대상 규칙에 대한 취약한 항목의 상태입니다.
취약성 위험 규칙 [sn_vul_calc_risk]	위험 점수 계산기에 사용되는 특수 계산기 규칙입니다. 위험 점수를 계산하는 데 사용할 VI와 관련된 값을 나타내는 가중치를 취합니다.
취약성 롤업 계산기 [sn_vul_rollup]	취약성 롤업 계산기 목록입니다.
취약성 검사 [sn_vul_scan]	취약성 스캔. 검사할 대상, 스캐너 및 검사 결과 요약을 포함합니다.
취약성 스캔 구성 항목 [sn_vul_m2m_scan_configuration_item]	스캔하기 위해 큐에 있는 CMDB CI를 연결합니다.
취약성 스캔 큐 항목 [sn_vul_scan_q_entry]	스캔 또는 처리를 위해 대기 중인 스캔 기록입니다. 명시된 요율 한도 내에서 요청을 용이하게 합니다.
취약성 스캔 소스 [sn_vul_m2m_scan_source]	소스를 스캔 기록에 연결하고 스캔 대기 중인 모든 기록을 나타냅니다.
취약성 스캔 작업 [sn_vul_m2m_scan_vulnerability]	스캔 기록의 소스에 대한 취약성 작업을 연결합니다.
취약성 스캐너 [sn_vul_scanner]	검사에 사용할 외부 공급업체 스캐너를 정의합니다.
취약성 스캐너 속도 제한 [sn_cmn_scanner_rate_limit]	스캐너를 속도 제한과 연결합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

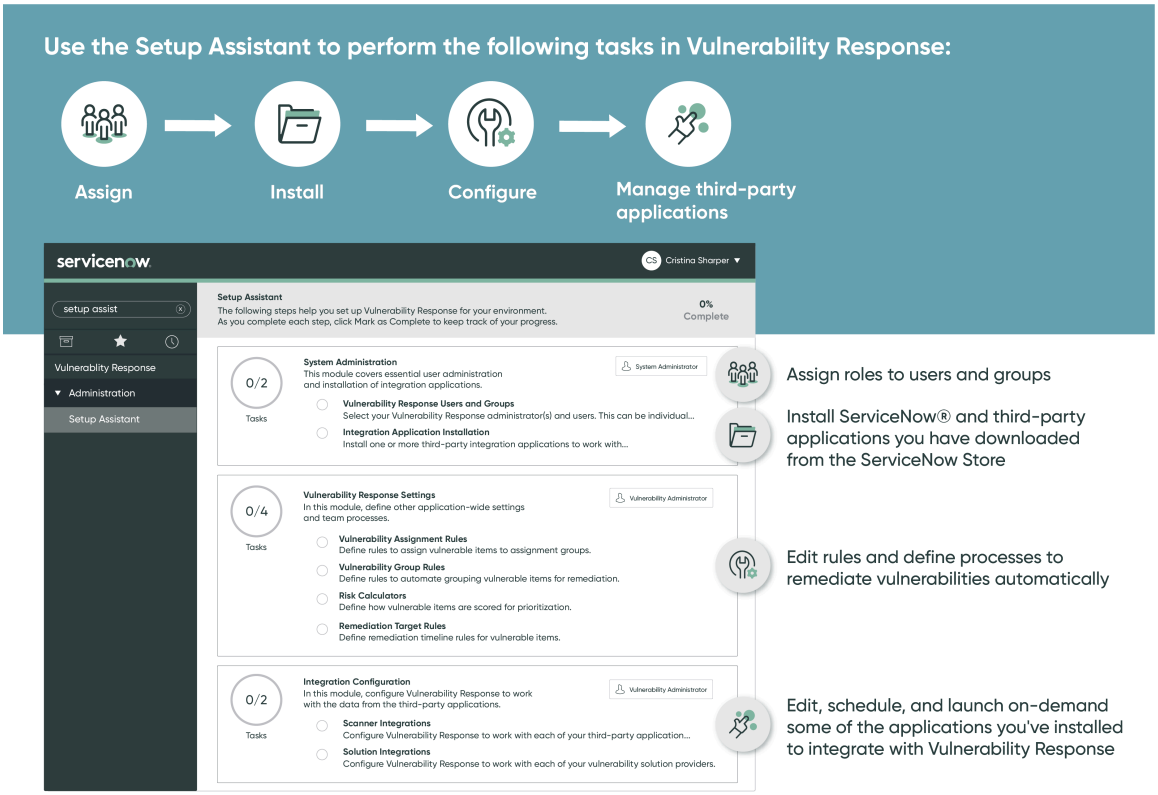
테이블	설명
취약성 소프트웨어 [sn_vul_m2m_entry_software]	취약성과 취약한 소프트웨어 간의 연결을 포함합니다.
취약성 솔루션 [sn_vul_solution]	취약성과 이에 대한 가능한 솔루션 간의 관계 데이터를 포함합니다. v24.0.6 부터 취약성 대응스캐너 게시판이라는 새 열이 이 테이블에 추가됩니다.
취약성 솔루션 [sn_vul_m2m_vulnerability_solution]	취약성 항목(sn_vul_entry) 테이블을 취약성 솔루션(sn_vul_solution) 테이블에 연결합니다.
취약성 상태 변경 승인 [sn_vul_change_approval]	취약성에 대한 승인 프로세스를 추적합니다.
취약성 대체 솔루션 [sn_vul_m2m_solution_supersedence]	솔루션 간의 소스별 관계를 포함합니다.
취약성 업데이트 매니페스트 [sn_vul_vuln_update]	취약한 항목이 업데이트 또는 종결되거나 위험 점수가 변경된 후 롤업 데이터를 업데이트해야 하는 취약성 목록을 포함합니다.
취약성 벤더 매핑 [sun_vul_vulnerability_vendor_mapping]	취약성과 해당 벤더의 목록을 포함합니다.
취약한 항목 [sn_vul_vulnerable_item]	구성 항목에 대한 취약성 발생을 포함합니다.
취약한 항목 탐지 [sn_vul_detection]	외부 공급업체 통합에서 탐지된 취약한 항목을 포함합니다.
취약한 소프트웨어 [sn_vul_software]	특정 취약성이 있는 것으로 알려진 소프트웨어.

설정 지원을 사용하여 구성 취약성 대응 하기

설정 도우미가 사용자 환경에 대한 설정 취약성 대응 및 특정 타사 통합을 안내합니다. 설정 도우미는 를 사용할 취약성 대응수 있도록 환경을 설치하고 설정하는 데 필요한 거의 모든 것을 제공합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설정 도우미 기능



Now Platform® roles: admin and vulnerability admin

설정 도우미를 사용하려면 관리자와 취약성 관리자라는 두 가지 ServiceNow AI Platform[#] 역할이 필요합니다.

다음 섹션을 참조하여 설정 도우미에서 제공되는 지침과 프롬프트를 보완합니다.

시스템 관리 - 사용자 및 그룹 할당 및 통합 애플리케이션 설치

필요한 역할: admin

이러한 작업을 시작하기 전에 취약성 관리자로부터 사용자 및 통합 목록을 가져와야 합니다.

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 설정 도우미.
2. 첫 번째 섹션인 시스템 관리에서 관리자는 사용자와 그룹에 역할을 할당하고 지원되는 통합을 설치합니다.

   설정 도우미에서 사용자 및 그룹에 가상 사용자와 역할을 할당합니다 취약성 대응 .

   가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.
3. 설정 도우미에서 역할을 할당합니다.
   - 사용자 또는 그룹에 sn_vul.admin의 역할을 할당합니다.
   - 취약성 통합, 정정 작업 규칙, 계산기 및 정정 시간 규칙을 포함한 취약성 대응 관리 및 구성에 대한 sn_vul.admin 역할을 할당합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 정정 작업 및 취약한 항목을 생성하고 업데이트하기 위한 sn_vul_vulnerability_write 역할을 할당합니다.

  주:
  다른 모든 사용자는 자신에게 할당된 정정 작업에 대한 쓰기 권한만 자동으로 부여받습니다.

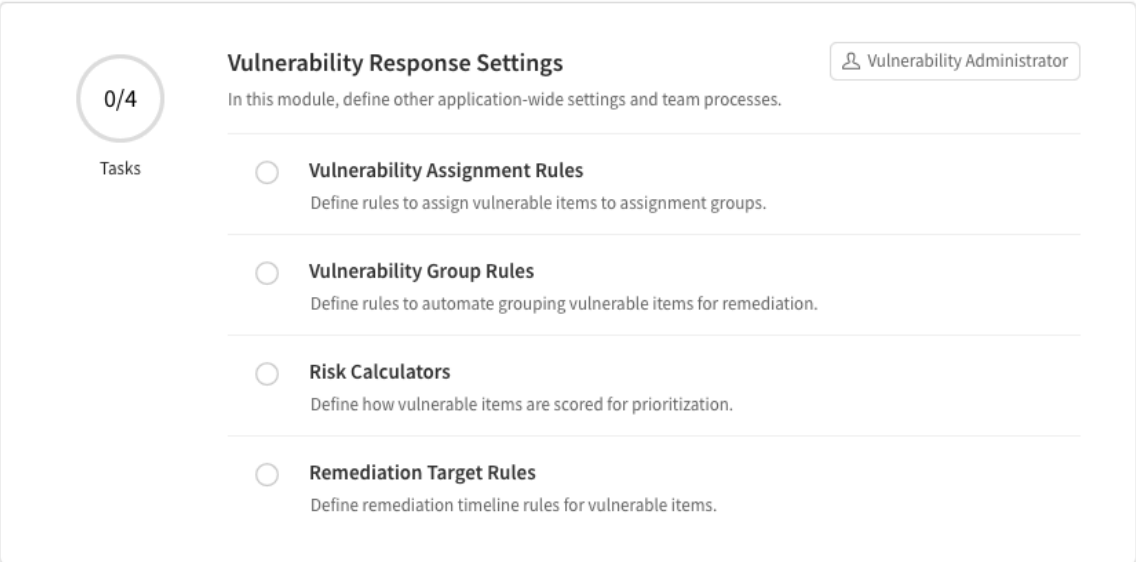
- sn_vul_vulnerability_read 역할을 할당하여 정정 작업, 취약한 항목 및 기타 취약성 정보를 봅니다.

  주:
  itil 역할을 가진 사용자에게는 sn_vul.remediation_owner 역할이 자동으로 부여되어 해당 인스턴스의 애플리케이션 및 취약성 대응 애플리케이션에서 할당된 정정 작업 및 취약한 항목, 취약성 항목 및 솔루션을 볼 수 있습니다 모바일 에이전트 . 추가 할당이 필요하지 않습니다.

4. 외부 공급업체 통합 애플리케이션을 설치합니다.
   - 에서 취약성 대응지원하는 애플리케이션에 대한 자세한 내용은 을 취약성 대응 통합 참조하십시오취약성 대응 설치 및 지원되는 애플리케이션.
   - 설정 도우미를 사용하여 지원되는 앱을 설치하는 방법에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 사용하여 타사 응용 프로그램 설치 취약성 대응.

취약성 대응 설정

필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음) 또는 admin



취약성 관리자는 Vulnerability Response 설정에서 애플리케이션 전체 설정을 정의하고 에 대한 취약성 대응규칙을 정의합니다. 또는 관리자가 다음 작업을 수행할 수 있습니다.

1. 취약성 담당 규칙을 생성합니다.

   해결을 위한 정정 작업의 자동 할당을 정의하는 규칙을 생성합니다. 하나 이상의 규칙이 기본 시스템과 함께 제공됩니다. 자세한 내용은 취약성 대응 할당 규칙 개요 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

다시 적용 기능을 사용하려면 규칙의 베이스라인 적용이 필요합니다. 규칙이 생성되면 편한 시간에 실행할 예약된 작업을 활성화합니다 ***Reapply all vulnerability assignment rules*** . 그렇지 않으면 규칙을 변경하기 전에 모든 Open VI에 모든 규칙을 다시 적용해야 합니다.

작업이 완료되면 환경에 맞게 예약된 작업의 실행 필드를 설정합니다. 보유하고 있는 활성 VI의 개수에 따라 매일 평가하고 업데이트하면 성능에 큰 영향을 미칠 수 있습니다. 대규모 환경의 경우 일주일에 한 번 또는 한 달에 한 번 업데이트하는 것이 좋습니다.

담당 규칙을 다시 적용해도 취약한 항목은 다시 그룹화되지 않습니다.

2. 정정 작업 규칙을 생성합니다.

   해결을 위한 정정 작업의 자동 생성을 정의하는 규칙을 생성합니다. 하나 이상의 규칙인 취약성 이 기본 시스템과 함께 제공됩니다. 양식 또는 목록 뷰에서 규칙을 다시 적용할 수 있습니다.

   - 그룹 규칙이 삭제되면 양식 또는 목록 보기에서 해당 규칙에 따라 생성된 모든 오픈 그룹을 삭제할 수 있습니다. 오픈 상태가 아닌 그룹은 제외됩니다.
   - 사용자 환경에 대한 규칙 생성에 대한 자세한 내용은 을 참조하십시오 외부 공급업체 취약성 통합에서 취약성 대응 구성 항목을 식별하기 위한 CI 조회 규칙 .
   - 를 사용하여 취약성 대응 취약성을 정정하는 방법에 대한 자세한 내용은 을 참조하십시오애플리케이션 탐색 취약성 대응.

3. 위험 계산기를 만들고 활성화합니다.

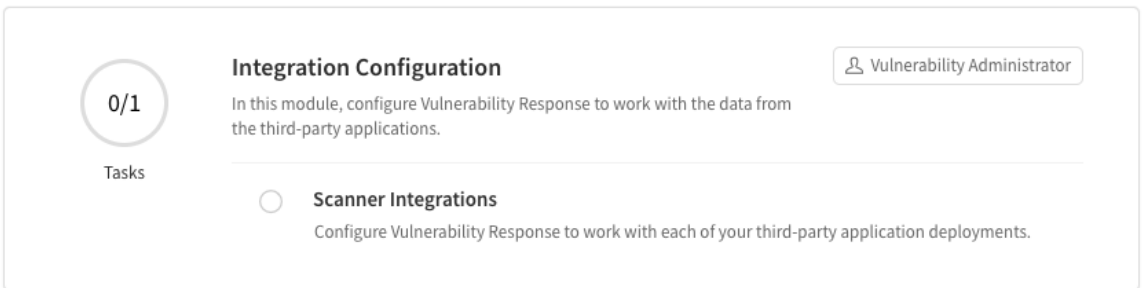
   취약한 항목의 우선순위 점수 산정 방법을 정의하는 위험 계산기를 사용합니다. 여러 가지 위험 계산기가 기본 시스템과 함께 제공됩니다. 사용자 환경에 대한 위험 계산기 생성 또는 편집에 대한 정보를 참조하십시오 취약성 대응 계산기 및 취약성 계산기 규칙 .

4. 정정 대상 규칙을 만듭니다.

   정정 범주에 대한 정정 대상 규칙을 생성합니다. 하나 이상의 규칙이 기본 시스템과 함께 제공됩니다. 사용자 환경에 대한 규칙 생성에 대한 자세한 내용은 을 참조하십시오 취약성 대응 정정 대상 규칙 .

통합 구성

필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음) 또는 admin.



통합 구성 섹션에서 다음과 같은 타사 취약성 스캐너 통합을 구성하고 예약, 편집하여 요청 시 실행하고, 애플리케이션이 설치된 경우 취약성 대응용 솔루션 관리 솔루션 제공자도 지원합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 구성에 Qualys Vulnerability Integration대한 자세한 내용은 을 참조하십시오Qualys Vulnerability Integration 설정 도우미 사용 구성.
- Vulnerability Response Integration with Tenable 애플리케이션 구성이 지원됩니다. 설정 도우미를 사용하여 Tenable 취약성 통합 구성 문서를 참조하십시오.
- 애플리케이션을 설치하면 취약성 솔루션 관리스캐너 통합 아래에 솔루션 통합 옵션이 표시됩니다. 솔루션 통합을 클릭하여 설정 도우미의 이 섹션에서 설치된 취약성 솔루션 제공자를 구성합니다. 및 Red Hat Solution IntegrationMicrosoft Security Response Center 솔루션 통합 지원됩니다.

  설치된 솔루션에 대한 자세한 내용은 을 참조하십시오 취약성 솔루션 관리 . 설치에 대한 자세한 내용은 을 참조하십시오 취약성 대응용 솔루션 관리 애플리케이션 설치 .

  설치된 솔루션 구성에 대한 자세한 내용은 을 참조하십시오 설치 도우미를 사용하기 위해 취약성 솔루션 관리 설치된 솔루션 통합 구성 .

- 통합이 다중 소스인 경우 동일한 외부 공급업체 통합을 여러 개 배포할 수 있습니다.
- 원래 외부 공급업체 통합의 설정은 각각의 새 통합 설정에 대한 템플릿으로 사용됩니다.

  주:
  원래 취약성 통합을 삭제할 경우, 템플릿으로 사용할 다른 통합을 선택해야 합니다. 통합을 삭제하는 대신 사용하지 않도록 설정하는 것이 좋습니다. 비활성화된 템플릿에서 만든 통합은 기본적으로 비활성화됩니다.

  각 외부 공급업체 통합의 데이터는 고유하게 식별되며 의 취약성 대응단일 인스턴스에서 사용할 수 있습니다.

주:
에 대한 Rapid7 InsightVM 여러 취약성 통합은 설정 도우미 내에서 사용할 수 없습니다. 다중 Rapid7 InsightVM 통합 구성 및 생성에 대한 자세한 내용은 을 참조하십시오통합을 위해 도메인 분리 임포트 작성.

추가 작업

설정 도우미에 포함되지 않은 설정 작업에 대한 자세한 내용은 을 참조하십시오 추가 취약성 대응 설정 및 구성 작업 .

설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당

설정 도우미를 취약성 대응 사용하여 그룹 또는 사용자에게 가상 사용자 역할을 할당합니다.

시작하기 전에
설정 도우미를 취약성 대응 사용하여 가상 사용자 역할을 이미 할당한 경우 사용자 관리 모듈에서 세분화된 역할 및 역할 할당을 편집하고 관리하는 방법에 대한 자세한 내용을 보려면 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

업그레이드 고객인 경우 취약성 대응 애플리케이션에 대한 기존 역할을 계속 사용할 수 있습니다. 이전 버전에서 취약성 대응 사용할 수 있는 sn_vul.vulnerability_read 및 sn_vul.vulnerability_write 권한으로 할당된 사용자 및 그룹과 정정 소유자 역할에 대한 액세스 권한은 변경되지 않았습니다.

그러나 작업 수준에서 애플리케이션과 사용자가 취약성 대응 수행하고 볼 수 있는 것을 보다 세부적으로 제어하려면 가상 사용자 및 세분화된 역할을 사용하는 것이 좋습니다.

설정 도우미를 사용하여 sn_vul.vulnerability_admin 가상 사용자 역할을 아직 할당하지 않은 경우 아래 단계에 따라 할당하십시오. 일단 할당되면 이 가상 사용자 역할을 가진 취약성 관리자는 첫 번째 섹션 이후의 설정 도우미 작업을 완료하고 애플리케이션에서 규칙과 타사 통합을 관리할 수 있는 권한을 갖게 됩니다 취약성 대응 .

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

가상 사용자 역할 및 세분화된 역할에 대한 개요는 다음 문서를 참조하십시오 취약성 대응 가상 사용자 및 세분화된 역할.

업그레이드 고객인 경우 다음 표를 참조로 사용하십시오.

이전 할당	권장 할당 〔사용자 가상 사용자〕	설명
sn_vul.admin	sn_vul.vulnerability_admin 〔취약성 관리자〕	취약성 대응(VR) 애플리케이션에 대한 전체 액세스 권한을 제공합니다. 이 역할을 가진 사용자는 VR 애플리케이션 및 규칙을 구성하고 외부 공급업체 통합을 설치합니다.
sn_vulnerability_write	sn_vul.vulnerability_analyst 〔취약성 분석가〕	VIT 정정을 위한 모든 기록을 보고 업데이트할 수 있습니다.
sn_vul.remediation_owner	sn_vul.remediation_owner 〔정정 소유자〕	사용자 및 그룹이 자신 또는 그룹에 할당된 취약성을 정정하고 관련 기록을 업데이트할 수 있습니다.
sn_vul.admin	sn_vul.ci 〔CI 관리자〕	검색된 항목 업데이트를 포함하여 CMDB에서 찾을 수 없는 일치하지 않는 구성 항목을 관리할 수 있습니다.
sn_vul.admin	sn_vul.exception_approver 〔예외 승인자〕	정정 작업 및 취약한 항목의 예외, 연기 및 종결을 승인할 수 있습니다.
sn_vul.vulnerability_read	sn_vul.read_all 또는 sn_vul.read_group_rules	애플리케이션의 특정 영역에 대한 읽기 전용 권한을 부여합니다. 모든 VR 기록을 보려면 sn_vul.read_all을 사용하거나 정정 작업 규칙을 보려면 sn_vul.read_group_rules를 사용합니다. 이러한 역할을 가진 사용자는 기록을 업데이트할 수 없습니다. **주:** 보다 세분화된 액세스를 위해 범위에서 여러 가지 다른 읽기 역할을 사용할 수 취약성 대응 있습니다.

가상 사용자 역할이 있는 사용자 또는 그룹이 기본적으로 상속하는 세분화된 역할을 보려면 다음으로 이동합니다. 모두 〉 사용자 관리 〉 역할. 원하는 역할을 찾은 후 클릭하여 기록을 엽니다. 역할 포함 탭에는 가상 사용자 역할의 모든 세분화된 역할과 상속된 역할이 나열됩니다.

설정 도우미에서 역할을 할당하기 전에 필요한 모든 사용자와 그룹이 생성되었는지 확인하는 것이 좋습니다. 또는 설정 도우미 내에서 새 사용자 및 그룹을 추가하려면 다음 그림에 표시된 양식에서 사용자 관리 모듈 링크를 클릭합니다.

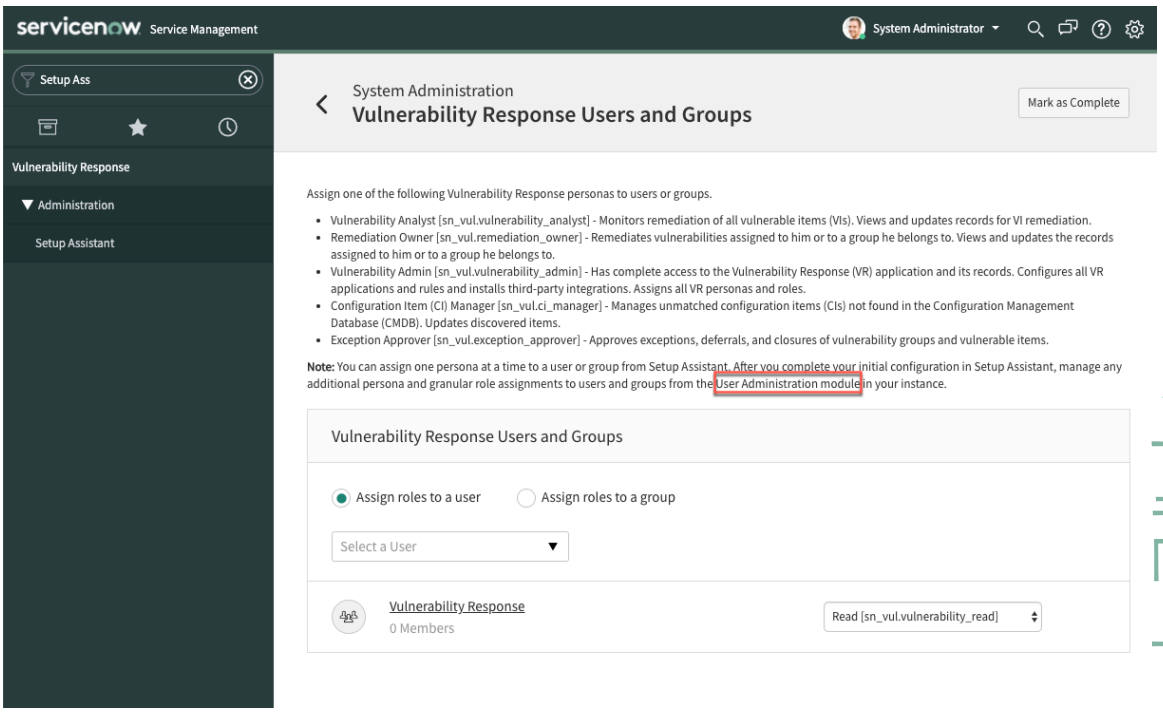
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음 예에서는 애플리케이션에 대한 취약성 대응 액세스를 제한하기 위해 취약성 관리자 가상 사용자를 사용자에게 할당하는 방법을 보여줍니다. 일반적으로 sn_vul.vulnerability_admin 이외의 가상 사용자 역할을 그룹에 할당하는 것을 선호할 수 있습니다.

필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 설정 도우미.
   설정 도우미 페이지가 표시됩니다.
2. Vulnerability Response 사용자 및 그룹을 클릭합니다.
   시스템 관리 취약성 대응 사용자 및 그룹 페이지가 표시됩니다.



3. 사용자에게 역할 할당을 선택한 상태에서 목록에서 기존 사용자를 선택합니다.

   하나의 페르소나 역할이 있는 사용자 또는 그룹만 할당할 수 있습니다.

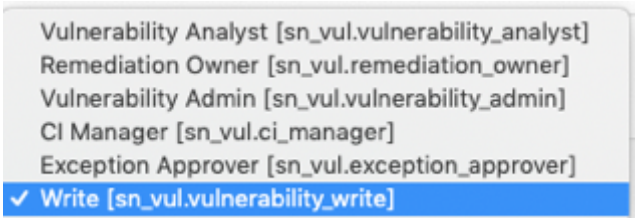
   양식 오른쪽에서 사용자나 그룹을 선택하면 기본 가상 사용자인 정정 소유자 (sn_vul.remediation_owner)가 기본적으로 할당되고 변경할 때까지 목록에 표시됩니다.

   주:
   새 버전으로 취약성 대응 업그레이드하는 경우 이전에 업그레이드 전에 사용자나 그룹에 sn_vul.vulnerability_read 또는 sn_vul.vulnerability_write 역할을 할당하면 다음 그림과 같이 새 가상 사용자 역할과 함께 표시됩니다.

   업그레이드 고객인 경우 취약성 대응 애플리케이션에 대한 기존 역할을 계속 사용할 수 있습니다. v10.3 이전의 sn_vul.vulnerability_read 및 sn_vul.vulnerability_write 권한으로 할당된 사용자 및 그룹과 정정 소유자에 대한 액세스 권한은 변경되지 않았습니다.

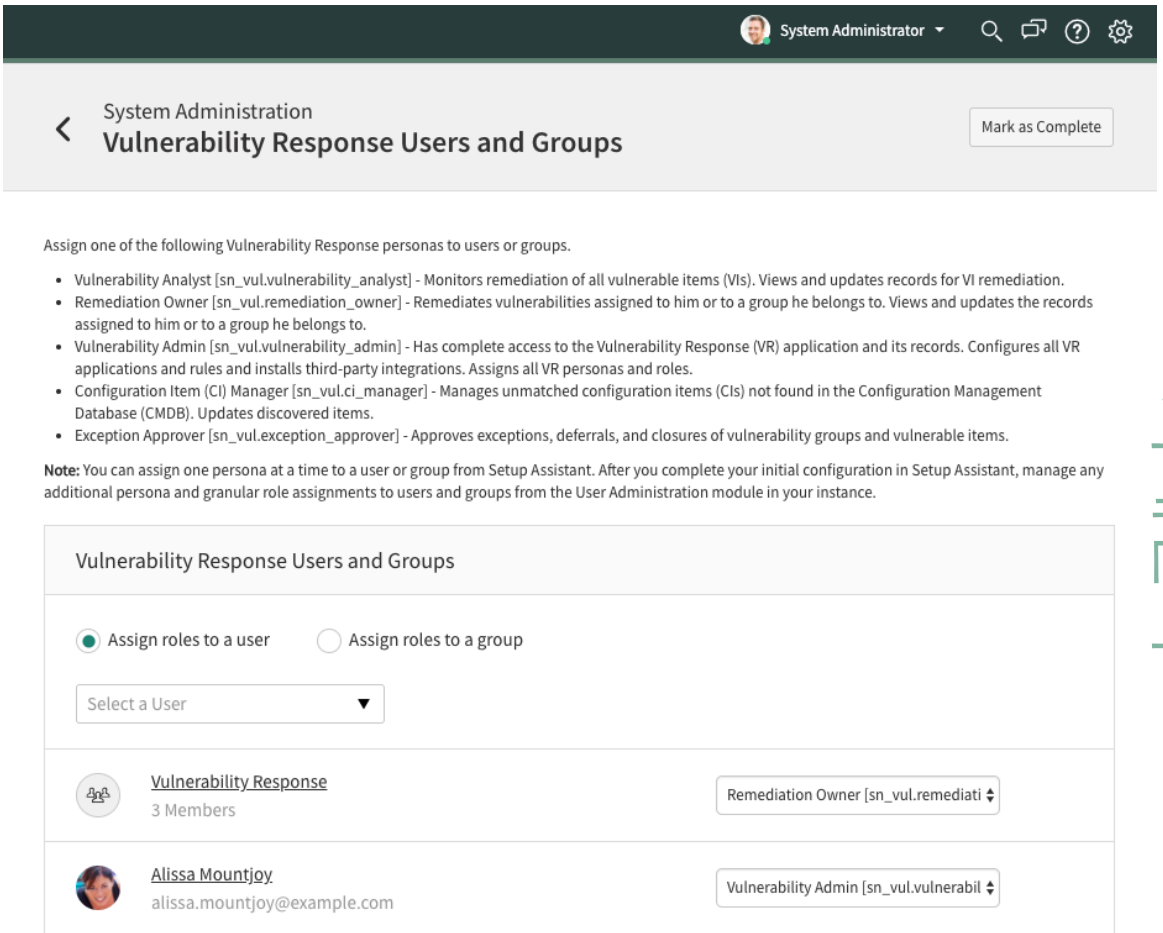
   기존 사용자 또는 현재 sn_vul.vulnerability_read 또는 sn_vul.vulnerability_write 역할이 할당된 그룹의 경우 이러한 역할이 가상 사용자 역할과 함께 목록에 표시됩니다. 가상 사용자 역할을 할당하면 이전 역할은 앞으로 더 이상 사용할 수 없습니다. 예를 들어, 다음 그림과 같이 쓰기 [sn_vul.vulnerability_write] 역할은 가상 사용자 역할 중 하나가 할당된 후 이 사용자나 그룹에 대한 옵션으로 더 이상 표시되지 않습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 양식 오른쪽에 있는 목록에서 취약성 관리자 **[sn_vul.vulnerability_admin]**을 선택합니다.
사용자 또는 그룹이 가상 사용자와 성공적으로 할당되었음을 나타내는 메시지가 표시됩니다.

그룹에 할당된 정정 소유자 가상 사용자 및 사용자에게 할당된 취약성 관리자 가상 사용자



5. 위에 나열된 가상 사용자 역할에 대한 설명을 사용하여 나머지 가상 사용자 역할(정정 소유자, 취약성 분석가, CI 관리자 및 예외 승인자)에 사용자와 그룹을 계속 할당합니다.
설정 도우미를 사용하여 사용자와 그룹에 가상 사용자 역할을 할당하는 작업을 성공적으로 완료했습니다.

6. 옵션: 설정 도우미에서 그룹의 사용자를 편집하려면 다음 단계를 수행합니다.

a. 양식에 그룹이 표시되면 편집할 그룹의 이름을 클릭합니다.
그룹 기록이 표시됩니다.

b. 그룹 구성원(Group Members) 탭을 선택한 상태에서 편집**(Edit)**을 클릭합니다.
구성원 편집 양식이 표시됩니다

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

c. 슬러쉬버킷을 사용하여 사용자를 선택하거나 제거합니다.

d. 저장을 클릭하여 변경 내용을 저장하고 그룹 기록으로 돌아갑니다.

e. 업데이트를 클릭하여 설정 도우미로 돌아갑니다.

f. 설정 도우미 페이지에서 취약성 대응 사용자 및 그룹을 클릭하여 설정 도우미에서 구성을 계속합니다.

다음에 수행할 작업

시스템 관리자 자격으로 설정 도우미의 취약성 대응 구성을 계속합니다. 첫 번째 섹션이 완료되면 취약성 관리자 가상 사용자 역할로 할당된 사용자가 설정 도우미에서 작업을 완료하도록 할 수 있습니다. 세분화된 역할 및 예제를 관리하는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

의 가상 사용자 및 세분화된 역할 관리 취약성 대응

설정 도우미를 사용하여 가상 사용자 역할의 초기 할당을 완료한 후 인스턴스의 사용자 관리 모듈에서 사용자 또는 그룹에 대한 추가적인 세분화된 역할 할당을 관리합니다.

시작하기 전에

설정 도우미 사용을 위한 취약성 대응 초기 설정 및 구성을 완료하지 않았거나 사용자 및 그룹에 가상 사용자 역할을 할당하지 않은 경우 취약성 대응 〉 관리 〉 설정 도우미. 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당 문서를 참조하십시오.

주요 용어와 가상 사용자 역할에 대한 개요는 다음 문서를 취약성 대응 가상 사용자 및 세분화된 역할참조하십시오.

가상 사용자 역할은 애플리케이션에서 미리 구성된 역할로, 세분화된 여러 역할로 구성됩니다. 설정 도우미, 취약성 관리자, 취약성 분석가, 정정 소유자, 구성 항목 관리자 및 예외 관리자의 가상 사용자 역할은 IT 조직 또는 취약성 개선 그룹의 관리자, 분석가 및 서비스 소유자의 일반적인 직책에 해당하도록 설계되었습니다.

사용자 및 그룹이 역할 중 하나에서 허용하는 것보다 더 많은 액세스 권한을 가지도록 하려면 사용자 및 그룹에 더 세부적인 역할을 추가할 수 있습니다. 반대로 작업 수준에서 특정 사용자 및 그룹에 대한 액세스를 제한하려면 세분화된 역할을 제거할 수 있습니다. 또한 필요에 맞게 사용자 지정 역할을 빌드할 수 있습니다.

필요한 역할: 관리자

프로시저

1. 사용자 및 그룹에 대해 세분화된 역할을 관리하려면 계속할 역할을 선택합니다.

에서 취약성 대응 세분화된 역할의 이름은 일반적으로 사용자가 수행하고 볼 수 있는 것을 설명합니다. 세분화된 특정 역할에 대한 설명을 보려면 다음으로 이동하십시오. 모두 〉 사용자 관리 〉 역할 원하는 역할을 찾습니다. 역할 설명, 역할이 할당될 때 자동으로 상속되는 역할 및 다른 역할에 종속된 역할도 나열됩니다.

2. 사용자 또는 그룹에 세분화된 역할을 할당하거나 제거하려면 다음 단계를 수행합니다.
예를 들어, IT 관리자가 기록을 볼 수 있지만 업데이트하거나 편집할 수 없는 역할을 할당하려고 한다고 가정해 보겠습니다. 에서 취약성 대응용 퍼포먼스 분석기록을 취약성 대응보고 모든 외부 공급업체 통합에 대해 이 사용자에게 sn_vul.read_all 세분화된 역할을 할당합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 다음으로 이동 모두 〉 사용자 관리 〉 사용자.

b. 사용자를 찾고 이름 열에서 기록을 클릭하여 엽니다.
사용자의 기록이 표시됩니다.

c. 선택하지 않은 경우 역할 탭을 선택합니다.
현재 사용자에게 할당된 역할이 표시됩니다.

d. 편집을 클릭합니다.
구성원 편집 양식이 표시됩니다.

e. Slushbucket의 컬렉션 필드에 역할 이름(알고 있는 경우)을 입력하거나, `*sn_vul` 를 입력하여 Vulnerability Response에 사용할 수 있는 세분화된 역할만 봅니다.

f. sn_vul.read_all을 찾아 역할 목록으로 이동합니다.

> 주:
> 역할을 역할 목록에서 컬렉션 목록으로 이동하여 슬러시버킷의 사용자로부터 세분화된 특정 역할을 제거하려면 동일한 프로세스를 사용합니다.

g. 저장을 클릭합니다.
사용자 기록이 새 세분화된 역할과 함께 표시됩니다.

h. 업데이트를 클릭하여 변경 내용을 저장하고 사용자 목록으로 돌아갑니다.
, 및 외부 공급업체 통합에 취약성 대응취약성 대응용 퍼포먼스 분석대한 기록을 읽을 수는 있지만 업데이트할 수 없는 권한을 사용자에게 제공했습니다.

3. 특정 구성원만 더 세분화된 역할로 확장된 액세스 권한을 가질 수 있도록 그룹을 편집하려면 다음 단계를 따르십시오.
예를 들어, 정정 소유자(sn_vul.remediation_owner) 그룹의 특정 사용자가 취약한 항목을 수동으로 생성할 수 있도록 허용하되 해당 권한을 그룹의 모든 사용자로 확장하지는 않으려고 합니다. 취약한 항목을 수동으로 생성할 수 있는 권한은 sn_vul.create_vulnerable_items 세분화된 역할에 의해 부여됩니다. 이 그룹의 사용자에게만 이 권한을 부여하려면 다음 단계를 수행합니다.

a. 다음으로 이동 모두 〉 사용자 관리 〉 그룹.

b. 정정 소유자 그룹을 찾고 이름 열에서 그룹을 클릭하여 기록을 엽니다.
그룹 기록이 표시됩니다.

c. 선택하지 않은 경우 그룹 구성원 탭을 선택합니다.
그룹의 현재 구성원이 표시됩니다.

d. 목록에서 세분화된 역할을 할당할 이름을 클릭하고 기록을 엽니다.

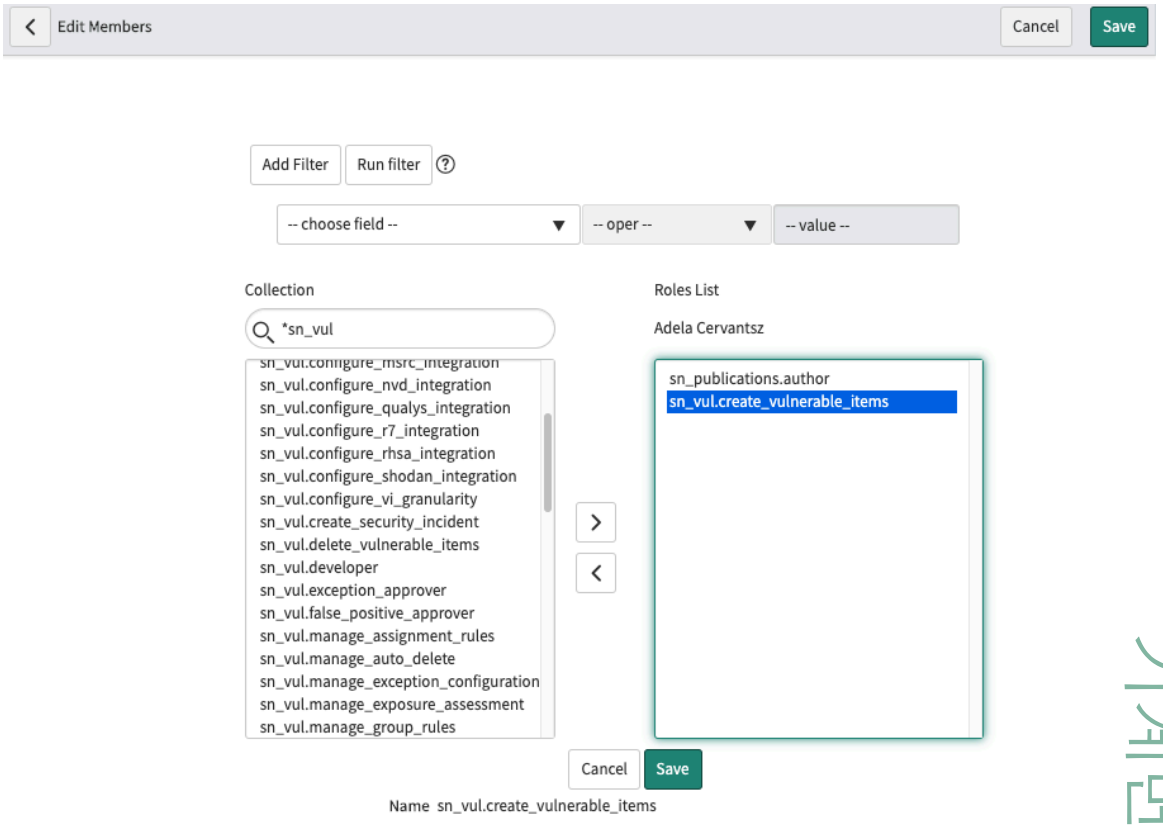
e. 기록에서 역할 탭까지 스크롤한 후 선택합니다.
사용자에게 할당된 역할이 표시됩니다.

f. 편집을 클릭합니다.
구성원 편집 양식이 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

g. 컬렉션 필드에 역할의 이름(알고 있는 경우)을 입력하거나 *sn_vul 를 입력하여 취약성 대응에 사용할 수 있는 세분화된 역할을 모두 봅니다.

h. sn_vul.create_vulnerable_items를 찾아 역할 목록으로 이동합니다.



i. 저장을 클릭합니다.
사용자 기록이 새 세분화된 역할과 함께 표시됩니다.

j. 뒤로 화살표를 클릭하여 정정 소유자 그룹의 기록에서 사용자를 봅니다

k. 이 세분화된 역할을 할당할 목록에서 이름을 클릭하고 해당 기록을 연 후 슬러시버킷을 사용하여 역할을 할당합니다.

l. 편집을 완료한 후 업데이트를 클릭하여 변경 내용을 저장하고 그룹 목록으로 돌아갑니다.
취약한 항목을 수동으로 생성할 수 있는 정정 소유자(sn_vul.remediation_owner) 그룹 권한을 일부 사용자에게 제공했습니다.

4. 선택한 세분화된 역할만 사용하여 새 역할을 만들려면 다음 단계를 수행합니다.
이 예에서는 규정 준수 감사자에 대한 역할을 생성한다고 가정합니다. 이 역할은 거버넌스, 리스크 및 컴플라이언스(GRC)와 긴밀하게 협력하며, 이 작업을 수행하려면 다음 권한 취약성 대응및 작업이 필요합니다.

- 취약한 항목 및 취약성 그룹에 대한 정정 기한 관리
- 기한 연장 또는 정정 연기에 대한 예외 요청 승인
- 자동 삭제로 오래된 취약한 항목의 정리 관리

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 위험 점수 정의
- 모든 취약성 대응 기록을 읽지만 편집할 수는 없습니다.

a. 다음으로 이동 모두 〉 사용자 관리 〉 역할.

b. 역할 목록에서 새로 만들기를 클릭합니다.

c. 역할 기록의 필드에 내용을 입력합니다.

이름을 만들고 이 기록이 포함된 애플리케이션을 선택한 후 새 역할에 대한 간단한 설명을 입력합니다. 양식의 다른 필드에 대한 자세한 내용은 역할 생성 섹션을 참조하십시오

> **주:**
> 새 역할의 이름을 만들 때 역할 목록에서 쉽게 인식되고 역할의 기능을 설명하는 이름을 사용하는 것이 좋습니다. 이 예에서는 준수 감사자 - GRC-VR과 같은 제목을 선호할 수 있습니다.

d. 제출을 클릭합니다.
역할 목록이 표시됩니다.

e. 새 역할을 찾아서 클릭하여 기록을 엽니다.

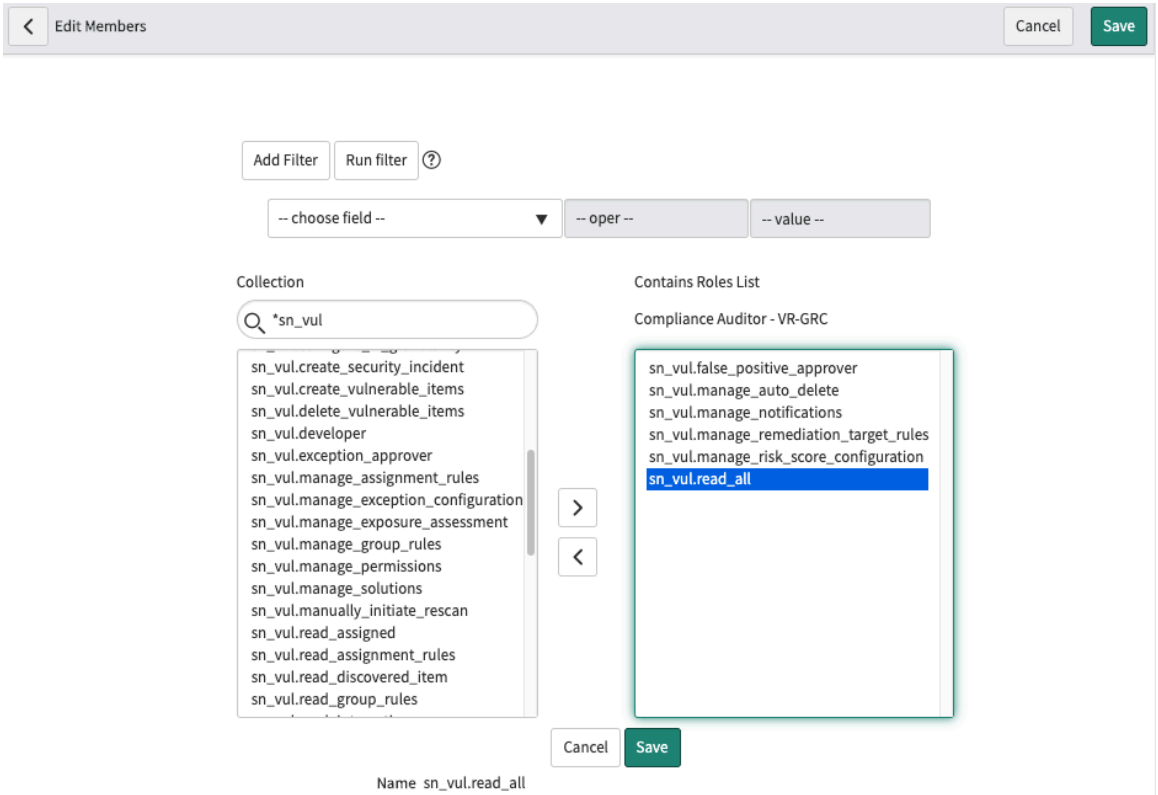
f. 편집을 클릭합니다.
구성원 편집 양식이 표시됩니다.

g. 슬러시버킷을 사용하여 새 역할에 세부적인 역할을 추가합니다.

이 예에서는 이 새 역할에 필요한 역할이 다음 그림의 오른쪽 열에 표시되어 있습니다.

취약성 대응에 대한 세분화된 역할만 표시하려면 컬렉션 필드에 `*sn_vul`를 입력합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



h. 저장을 클릭합니다.
새 역할에 대한 기록이 표시됩니다. 역할 포함 탭을 시작으로 필요에 따라 역할을 계속 편집합니다.

i. 변경 사항을 저장하려면 업데이트를 클릭합니다.
새 역할이 역할 목록에 표시됩니다.

설정 도우미를 사용하여 타사 응용 프로그램 설치 취약성 대응

설정 도우미를 사용할 수 있는 권리가 취약성 대응 있는 타사 통합 애플리케이션을 설치합니다.

시작하기 전에

설정 도우미는 를 사용하여 취약성 대응대부분의 타사 통합 애플리케이션 설치를 지원하지만, 인스턴스의 구성 모듈에서 설치하는 일부 애플리케이션에 대한 구성을 계속 진행합니다. 에서 취약성 대응지원하는 애플리케이션 목록은 을 참조하십시오취약성 대응 통합.

주:
이 프로세스는 프로덕션 인스턴스에 다운로드된 애플리케이션에만 적용됩니다. 애플리케이션을 비프로덕션 또는 개발 인스턴스에 다운로드하는 경우에는 권리를 얻을 필요가 없습니다. 로 애플리케이션 활성화 ServiceNow Store계속 진행합니다.

- 설치 취약성 솔루션 관리 후 이 취약성 대응 기능을 사용하면 및 Red Hat Solution Integration 설정 도우미에 액세스할 Microsoft Security Response Center 솔루션 통합 수 있습니다.
- 취약성 솔루션 관리 는 별도의 구독으로 사용할 수 있습니다. 솔루션을 통합하는 방법에 취약성 대응 대한 자세한 내용은 을 참조하십시오취약성 솔루션 관리.

설치 도우미에서 타사 응용 프로그램을 설치하고 활성화하려면 먼저 원활한 설치를 위해 다음 작업을 수행해야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업 설정	설명
설치하려는 통합 애플리케이션에 대한 유효한 ServiceNow 권리가 있는지 확인합니다.	다음으로 이동 구독 관리 〉 구독 권한을 확인합니다. 목록에 조직이 구매한 구독이 표시됩니다. 에서 애플리케이션에 대한 보안 운영 권리를 얻는 방법에 대한 자세한 내용은 을 참조하십시오제품 또는 애플리케이션에 대한 보안 운영 권리 가져오기.ServiceNow Store
(선택 사항) 아직 설치 및 활성화되지 않은 경우 타사 애플리케이션을 설치하기 전에 애플리케이션을 설치하는 취약성 대응 것이 좋습니다.	애플리케이션 설치 및 활성화에 취약성 대응 대한 자세한 내용은 취약성 대응 설치 및 구성을 참조하십시오.
아직 설치 및 활성화되지 않은 경우 타사 스캐너 애플리케이션을 실행하여 데이터를 임포트하기 전에 NVD 통합 및 CWE 예약된 작업을 사용하여 취약성 데이터를 활성화하고 임포트해야 합니다.	외부 공급업체 스캐너 제품을 사용하여 취약성 데이터를 인스턴스로 임포트하기 전에 초기 설정 취약성 대응 의 일부로 NVD 및 CWE 통합을 실행합니다. 자세한 내용은 NVD 통합 이해 문서를 참조하십시오.
에 대한 취약성 대응외부 공급업체 통합에 필요한 설정 작업을 완료했는지 확인합니다.	에서 취약성 대응 통합설치하려는 각 통합에 필요한 설정 작업을 검토합니다.

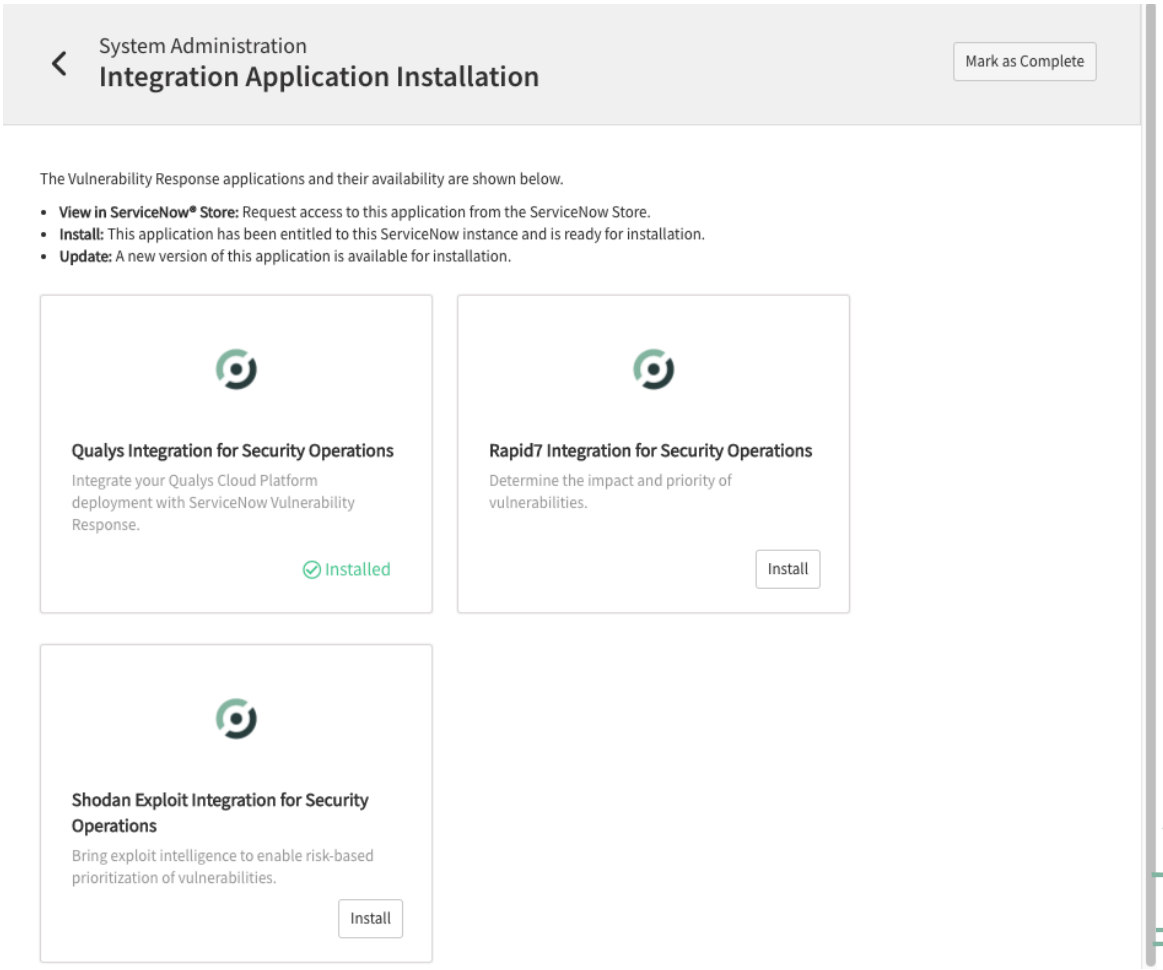
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 설정 도우미 〉 시스템 관리 〉 통합 애플리케이션 설치.

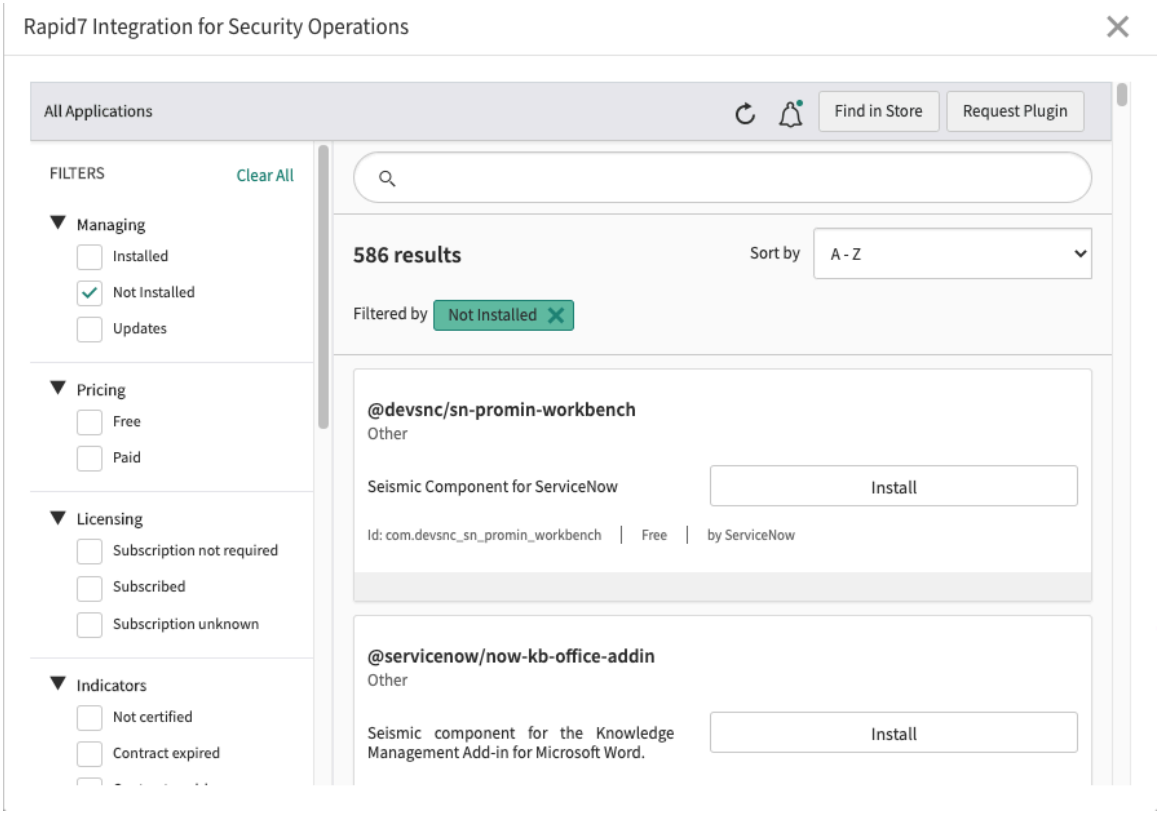
잠시 후 권리가 있고 인스턴스에 설치할 수 있는 애플리케이션이 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



2. 설치할 애플리케이션을 찾아 애플리케이션 타일에서 설치를 클릭합니다.
   다음 그림과 같이 모든 응용 프로그램 대화 상자가 클릭한 응용 프로그램 타일(예: Rapid7 Integration for Security Operations)과 함께 표시됩니다.

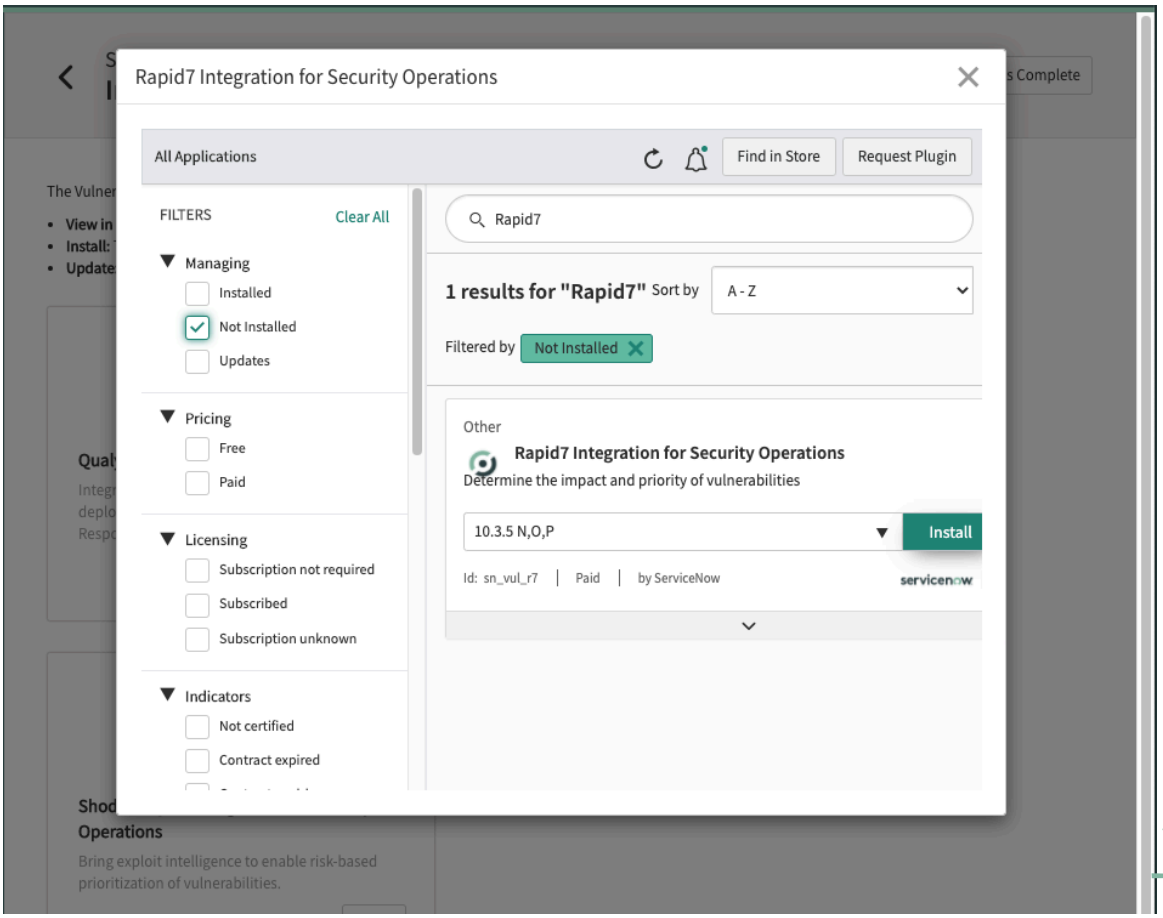
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



3. 응용 프로그램을 찾아 선택 목록에서 버전을 선택하고 설치를 클릭합니다.

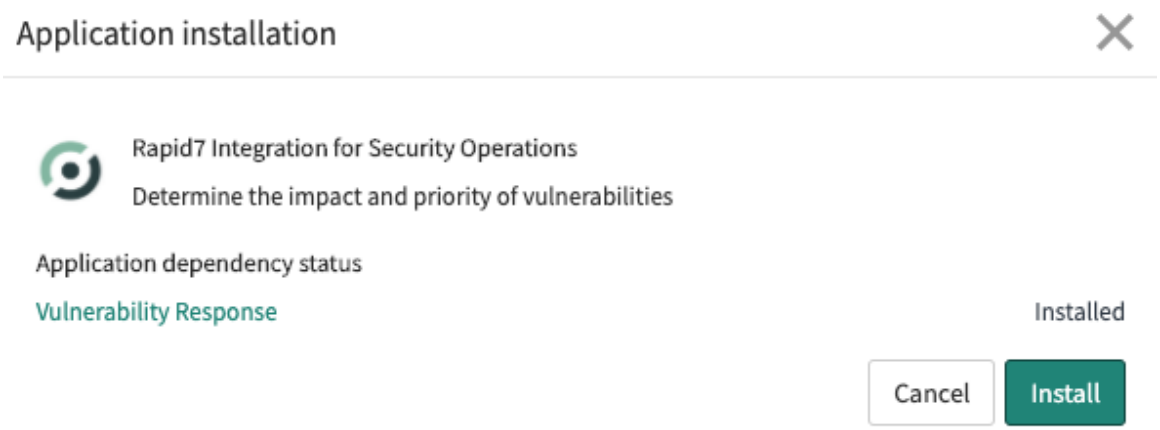
애플리케이션에 사용할 수 있는 업데이트가 있으면 업데이트 버튼이 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



애플리케이션 설치 대화 상자에 애플리케이션 종속성 상태가 표시됩니다. 아직 설치되지 않은 필수 종속성은 애플리케이션과 함께 자동으로 설치됩니다.

4. Application installation(애플리케이션 설치) 대화 상자에서 Install(설치)을 클릭합니다.



설치 대화 상자에 설치가 성공적으로 완료된 시기가 표시됩니다.

5. 대화 상자를 닫습니다.
애플리케이션이 성공적으로 설치되었음을 보여주는 모든 애플리케이션 페이지가 표시됩니다.

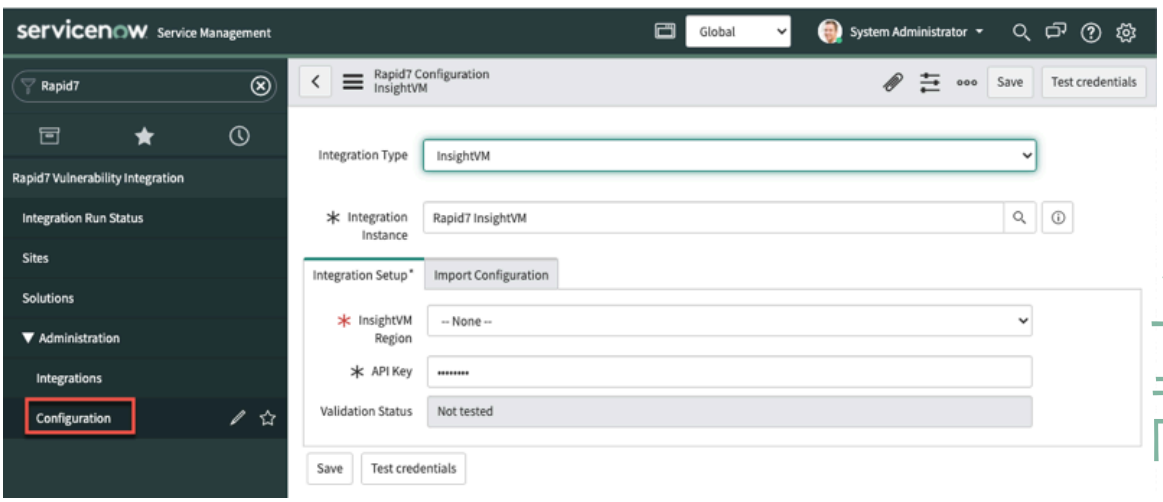
설치 및 활성화 후에는 설정 도우미의 통합 구성 섹션에서 다음 애플리케이션과 설치된 솔루션을 직접 구성, 예약 및 실행할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 이 Qualys Vulnerability Integration
- 이 Vulnerability Response Integration with Tenable.
- 이 Microsoft Security Response Center 솔루션 통합
- 이 Red Hat Solution Integration
- Microsoft Security Response Center 솔루션 통합
- Microsoft Defender 취약성 관리 통합

위에 나열되지 않은 다른 애플리케이션의 경우 애플리케이션의 구성 모듈로 직접 이동하여 구성을 계속 진행하고 필요한 외부 공급업체 자격 증명을 입력합니다. 예를 들어, 다음 이미지는 애플리케이션에 대한 Rapid7 구성 및 모듈의 위치를 보여줍니다.

특정 애플리케이션을 구성하는 방법에 대한 자세한 정보는 각 애플리케이션에 대해 제공된 제품 이름별 설치 및 구성 제품 설명서를 참조하십시오.



다음에 수행할 작업
애플리케이션이 지원되는 경우 설정 도우미에서 애플리케이션 구성을 계속합니다.

애플리케이션이 설정 도우미의 구성에 지원되지 않는 경우 애플리케이션의 구성 모듈로 직접 이동하여 구성을 계속합니다. 설정 도우미에서 지원되는 응용 프로그램을 보려면 문서를 참조하십시오 취약성 대응 설치 및 지원되는 애플리케이션.

NVD 및 **CWE** 통합을 통해 데이터를 임포트하고 외부 공급업체 라이브러리를 관리합니다

아직 설치하지 않은 경우 NVD 통합을 다운로드하여 실행하고 외부 공급업체 스캐너 제품을 사용하여 취약성 데이터를 인스턴스로 임포트하기 전에 취약성 대응 초기 설정의 일부로 CWE 예약된 작업을 실행합니다. NVD와의 취약성 대응 통합은 다음에서 사용할 수 있습니다 ServiceNow Store.

CWE 및 **NVD** 데이터 수집

NVD 및 CWE 통합에서 임포트한 데이터는 인스턴스의 취약성 데이터를 보강하고 취약성, 취약한 항목 또는 정정 작업에 대한 정정을 에스컬레이션할지 여부를 결정하는 데 사용됩니다. 초기 임포트 후에는 요청 시 라이브러리 레코드를 업데이트하거나 레코드를 정기적으로 업데이트하도록 예약된 작업을 구성할 수 있습니다. 취약성 대응라이브러리 아래에 저장합니다.

NVD 및 타사 항목에 포함된 CVSS(공통 취약성 평가 시스템)는 취약성의 주요 특징을 캡처합니다. 취약성 대응 는 CVSS 데이터를 사용하여 취약성 심각도를 반영하는 정규화된 값을 생성합니다. 심각도를 계산할 때 취약성은 이 취약성이 조직에 미치는 위험을 더 잘 이해할 수 있도록 합니다. 심각도는 취약성 정정을 평가하고 우선순위를 지정하는 데 도움이 됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

를 처음 설치하거나 취약성 대응외부 공급업체 스캐너 제품을 사용하여 처음으로 데이터를 수집하기 전인 경우:

1. CWE Comprehensive 2000 Integration을 사용하여 CWE 데이터의 초기 임포트를 수행합니다.

   자세한 내용은 CWE 기록을 업데이트하기 위해 예약된 작업을 구성하고 실행합니다. 문서를 참조하십시오. CWE 업데이트는 기본적으로 통합 기록에서 요청 시 수행하며, 예약된 작업으로 실행하려면 이를 구성해야 합니다.

   주:
   NVD 데이터베이스 업데이트 전에 실행되도록 CWE 업데이트를 예약합니다. NVD 업데이트의 기본 요일은 매주 월요일입니다.

2. 취약성 대응 NVD와 통합 애플리케이션이 설치되었고 NIST 국가 취약성 데이터베이스 통합 API(CVE만) 또는 NIST 국가 취약성 데이터베이스 통합 API(CVE 및 CPE)의 데이터를 성공적으로 임포트했는지 확인하십시오.

   프로덕션 인스턴스에서 이 플러그인을 활성화하려면 별도의 라이센스가 필요할 수 있습니다. NIST 국가 취약성 데이터베이스 통합 API(CVE만 해당) 통합이 설치되면 기본적으로 활성화됩니다. 매일 실행됩니다. 자세한 내용은 AND 취약성 대응 NIST 국가 취약성 데이터베이스와의 통합 설치 문서를 참조하십시오 NVD 통합 이해 .

3. 타사 라이브러리는 예약된 작업으로 업데이트됩니다. 외부 공급업체 통합에 대한 자세한 내용은 통합 설명서를 참조하십시오 취약성 대응 통합 .

임포트한 취약성 데이터 및 취약한 항목 보기

다음 라이브러리를 사용할 수 있습니다.

라이브러리	설명
NVD	NVD에서 발견한 취약성 목록으로, 보안 검사 목록, 보안 관련 소프트웨어 결함, 잘못된 구성, 제품 이름 및 익스플로잇을 포함한 영향 메트릭이 포함됩니다.
CWE	커뮤니티에서 개발한 소프트웨어 약점 유형 목록입니다. 각 CWE 기록에는 약점을 설명하는 관련 지식 문서도 포함되어 있습니다. 일반 약점 열거 화면에서 취약성을 에스컬레이션할 수 없으며 참조용으로만 사용해야 합니다.
외부 공급업체	인스턴스에 임포트한 외부 공급업체 취약성의 목록입니다. 관련 참조, 취약한 항목, 익스플로잇 및 CVE 목록을 포함합니다.

관련 정보

취약성 라이브러리 보기 취약성 대응

취약성 대응용 솔루션 관리 애플리케이션 설치

인스턴스에서 기능을 취약성 대응 사용하려면 취약성 대응용 솔루션 관리 먼저 애플리케이션 설치를 취약성 솔루션 관리 완료해야 합니다. 이 애플리케이션은 에서 별도의 구독으로 사용할 수 있습니다 ServiceNow Store.

시작하기 전에
설치하기 전에 다음 설정 검사 목록을 완료합니다. 원활한 설치를 위해 이러한 설정 작업을 수행합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
이 프로세스는 프로덕션 인스턴스에 다운로드된 애플리케이션에만 적용됩니다. 애플리케이션을 비프로덕션 또는 개발 인스턴스에 다운로드하는 경우에는 권리를 얻을 필요가 없습니다. 로 애플리케이션 활성화 ServiceNow Store계속 진행합니다.

및 Microsoft Security Response Center 솔루션 통합Red Hat Solution Integration 는 설치 취약성 솔루션 관리후 사용할 수 취약성 대응용 솔루션 관리 있는 솔루션 애플리케이션입니다.

작업 설정	설명
애플리케이션이 설치되고 활성화되었는지 취약성 대응 확인합니다.	취약성 대응용 솔루션 관리 애플리케이션이 취약성 대응 필요합니다. 최신 버전의 취약성 솔루션 관리경우 최신 버전이 취약성 대응 설치되어 있는지 확인합니다. KB0856498 취약성 대응 호환성 매트릭스 및 릴리스 스키마 변경 사항을 참조하십시오. 애플리케이션이 설치 및 활성화되지 않은 경우을 참조하십시오 취약성 대응 설치.
애플리케이션에 대한 권리가 있는지 확인합니다.	애플리케이션에 대한 취약성 솔루션 관리 권리가 있는지 확인하려면 다음으로 이동하십시오. 구독 관리 〉 구독 인스턴스에 있습니다. 목록에 조직이 구매한 구독이 표시됩니다. 에서 애플리케이션에 대한 취약성 솔루션 관리 권리를 얻고 인스턴스에 다운로드하려면 ServiceNow AI Platform 문서를 제품 또는 애플리케이션에 대한 보안 운영 권리 가져오기참조하십시오.ServiceNow Store
지난 10년 동안의 NVD 기록이 최신 상태인지 확인합니다.	NVD 및 CWE 통합을 통해 데이터를 임포트하고 외부 공급업체 라이브러리를 관리합니다 문서를 참조하십시오.
외부 공급업체 취약성이 최신 상태인지 확인합니다.	타사 취약성 통합에 대한 자세한 내용은 을 참조하십시오 취약성 대응 통합 .
인스턴스에 필요한 ServiceNow AI Platform 역할이 할당되어 있는지 확인합니다.	설치 및 예상 결과 검증에 필요한 역할은 다음과 같습니다. 가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응. • 시스템 관리자 〔admin〕가 애플리케이션을 설치합니다. 아직 할당되지 않은 경우 관리자는 취약성 관리자 [sn_vul.vulnerability_admin 또는

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업 설정	설명
	sn_vul.admin(사용하지 않음)) 역할을 할당합니다. • 취약성 관리자는 구성을 감독하고 예상 결과를 검증합니다.

필요한 역할: 애플리케이션을 설치하기 취약성 솔루션 관리 위한 관리자와 이를 구성하려면 취약성 관리자.

프로시저

1. ServiceNow Store로 이동합니다.
2. 로그인을 클릭하고 HI 자격 증명을 입력합니다.
3. **ServiceNow** 제품 탭을 클릭하여 사용 가능한 ServiceNow 제품을 확인합니다.
4. 취약성 솔루션 관리 옆에 있는 더하기**(+)** 기호를 클릭하여 자격이 있는 모든 관련 애플리케이션을 봅니다.
5. 옵트인을 클릭하여 애플리케이션에 대한 취약성 솔루션 관리 권리가 있는지 확인합니다.
6. 이미 권리가 있는 경우 10단계로 건너뛰고 인스턴스에 애플리케이션을 ServiceNow AI Platform 설치합니다.
7. 확인란을 선택하고 수락 을 클릭하여 프롬프트의 사용 약관에 동의합니다.
   애플리케이션에 대해 성공적으로 옵트인했음을 나타내는 메시지가 표시됩니다.
8. 옵션: 다른 ServiceNow AI Platform 인스턴스에 대한 취약성 솔루션 관리 권리를 관리하려면 권리 관리를 클릭합니다.

   주:
   권리 관리 버튼이 표시되지 않으면 제품 목록에서 취약성 솔루션 관리 애플리케이션을 클릭하여 표시하십시오.

   a. 옵션 선택

   b. 계속하려면 확인 또는 취소를 클릭하십시오.
      플러그인을 활성화하고 인스턴스에 애플리케이션을 설치할 준비가 되었습니다.

9. ServiceNow AI Platform 애플리케이션을 설치할 취약성 솔루션 관리 인스턴스에 로그인합니다.
10. 다음으로 이동 모두 〉 시스템 애플리케이션 〉 모든 사용 가능 애플리케이션 〉 모두.
11. 애플리케이션(sn_vul_solution)을 취약성 솔루션 관리 찾아 설치를 클릭합니다.
    애플리케이션 설치 대화 상자에 애플리케이션 의존성 플러그인 상태가 표시됩니다. 아직 설치되지 않은 필수 종속성은 애플리케이션과 함께 자동으로 설치됩니다.
12. 설치를 클릭합니다.
    이 설치에는 다소 시간이 걸릴 수 있습니다. 애플리케이션과 해당 의존성이 성공적으로 설치된 후 설치 대화 상자에 메시지가 표시됩니다.

    취약성 관리자는 이제 설정 도우미 내에서 애플리케이션을 구성할 수 있습니다.
13. 닫기를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

및 Microsoft Security Response Center 솔루션 통합Red Hat Solution Integration 는 설치 취약성 솔루션 관리후 사용할 수 취약성 대응용 솔루션 관리 있는 솔루션 애플리케이션입니다.

다음으로 이동하여 취약성 솔루션 보기 모두 〉 취약성 대응 〉 관리 〉 설정 도우미 〉 통합 구성 〉 솔루션 통합. 자세한 내용은 설치 도우미를 사용하기 위해 취약성 솔루션 관리 설치된 솔루션 통합 구성 문서를 참조하십시오.

다음에 수행할 작업

애플리케이션 및 사용 가능한 솔루션을 구성한 후 취약성 솔루션 [sn_vul_m2m_vulnerability_solution] 테이블을 사용하여 CVE와 솔루션이 일치하는지 확인합니다.

[PA] 애플리케이션 설치 및 구성 취약성 대응용 퍼포먼스 분석

애플리케이션을 사용하려면 취약성 대응용 퍼포먼스 분석 먼저 권리를 얻고, 에서 ServiceNow Store애플리케이션을 다운로드하고, 인스턴스에 설치 ServiceNow AI Platform# 하고, 몇 가지 설치 및 구성 단계를 완료해야 합니다. PA 애플리케이션이 애플리케이션의 일부로 취약성 대응 설치되지 않았습니다. 별도의 구독으로 사용할 수 있습니다.

시작하기 전에

인스턴스에 이미 애플리케이션이 있고 최신 버전의 애플리케이션으로 업데이트하려는 경우 다음 단계의 8단계로 진행하여 업데이트 및 구성을 계속합니다.

새로 설치하는 경우 설치하기 전에 다음 설정 검사 목록을 완료하십시오. 이러한 설정 작업은 원활한 설치 및 구성을 위해 필요합니다.

플러그인과 애플리케이션이 설치되고 활성화되었는지 확인하려면 다음으로 이동합니다. 모두 〉 구독 관리 〉 구독 인스턴스에 있습니다. 목록에 조직이 구매한 구독이 표시됩니다.

주:
이 프로세스는 프로덕션 인스턴스에 다운로드된 애플리케이션에만 적용됩니다. 애플리케이션을 비프로덕션 또는 개발 인스턴스에 다운로드하는 경우에는 권리를 얻을 필요가 없습니다. 로 애플리케이션 활성화 ServiceNow Store계속 진행합니다.

작업 설정	설명
Vulnerability Response 종속성 플러그인(com.snc.vul_dep)이 설치되고 활성화되었는지 확인합니다.	취약성 대응 의존성 이 플러그인에는 애플리케이션을 지원하는 데 필요한 모든 종속성 플러그인이 포함되어 있습니다. 플러그인이 설치되고 활성화되었는지 확인하려면 애플리케이션을 사용하려는 인스턴스에서 시스템 애플리케이션 〉 모든 사용 가능 애플리케이션 〉 모두. 다른 종속성 플러그인을 업데이트하라는 메시지가 표시되면 대화 상자의 링크를 클릭하고 프롬프트에 따라 계속합니다.
애플리케이션(sn_vul)이 ServiceNow 취약성 대응 설치되고 활성화되었는지 확인합니다.	취약성 대응 플러그인이 설치되고 활성화되었는지 확인하려면 애플리케이션을 사용하려는

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

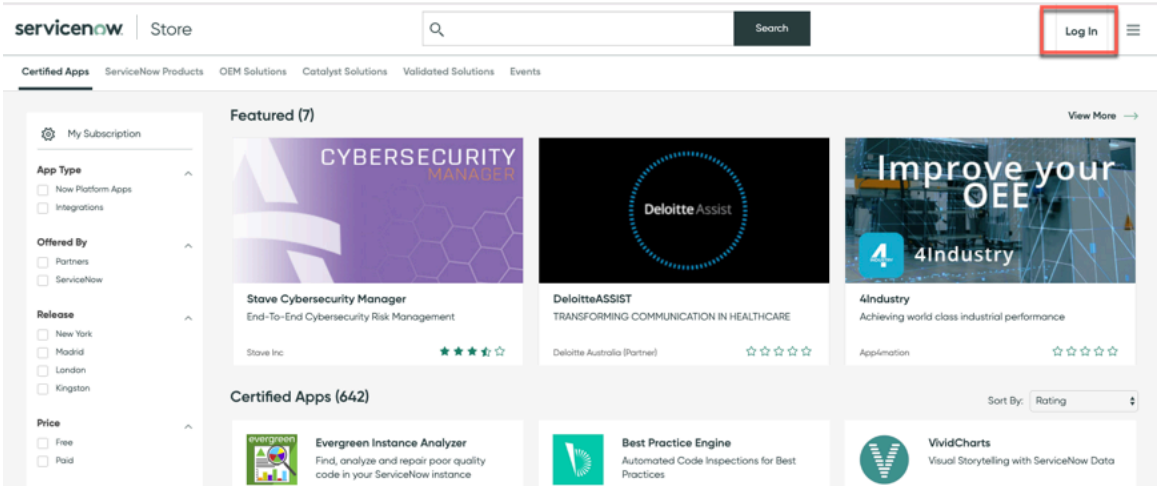
작업 설정	설명
	인스턴스에서 시스템 애플리케이션 〉 모든 사용 가능 애플리케이션 〉 모두. 다른 종속성 플러그인을 업데이트하라는 메시지가 표시되면 대화 상자의 링크를 클릭하고 프롬프트에 따라 계속합니다. 프로덕션 인스턴스에서 이 플러그인을 활성화하려면 별도의 라이센스가 필요할 수 있습니다. 자세한 내용은 ServiceNow에 문의하십시오.
인스턴스에 필요한 ServiceNow 역할이 있는지 확인합니다. 가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.	예상 결과의 설치, 구성 및 검증에 필요한 역할은 다음과 같습니다. • 퍼포먼스 분석 관리자 [pa_admin] 또는 시스템 〔admin〕이 애플리케이션을 설치하고 예상 결과를 검증합니다. • 취약성 관리자 [sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)〕는 구성을 감독하고 PA 대시보드를 사용하여 예상 결과를 검증합니다. • 정정 소유자 〔sn_vul.remediation_owner〕는 변경 관리 작업을 감독하고 할당된 기록을 읽고 업데이트합니다. 사용자에게 itil 역할이 할당되면 sn_vul.remediation_owner 역할도 자동으로 할당됩니다.
Performance Analytics 및 취약성 대응 애플리케이션이 호환되는지 확인합니다.	호환성 정보는 KB0856498 Vulnerability Response 호환성 매트릭스 및 릴리스 스키마 변경을 참조하십시오.

필요한 역할: admin 또는 pa_admin

프로시저

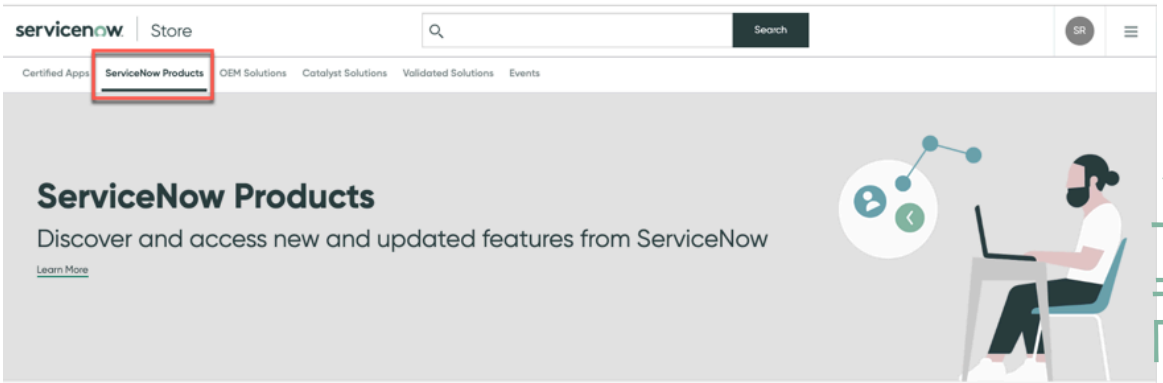
1. 권리를 얻고 인스턴스에서 애플리케이션을 ServiceNow AI Platform 다운로드하려면 로 ServiceNow Store이동합니다.
2. 페이지 오른쪽 상단에서 로그인을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



3. 표시되는 대화 상자에서 HI 자격 증명을 입력하고 로그인을 클릭합니다.

4. 표시된 페이지에서 선택하지 않은 경우 **ServiceNow** 제품 탭을 클릭합니다.

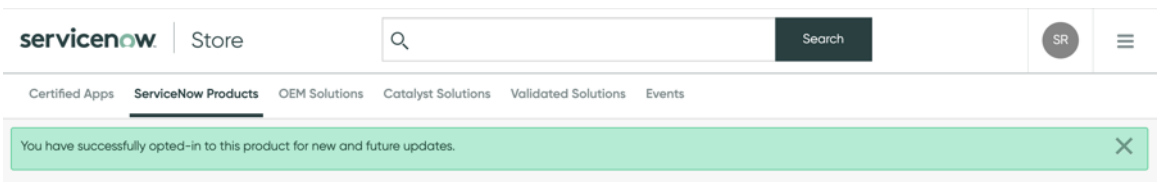


5. 제품 목록 페이지에서 퍼포먼스 분석 **-** 취약성 대응을 클릭합니다.

6. 인스턴스 이름 및 인스턴스 이유를 입력하고 인스턴스 확인을 클릭합니다.
옵트인 버튼이 있는 페이지가 표시됩니다.

7. 애플리케이션을 다운로드하려면 취약성 대응용 퍼포먼스 분석옵트인을 클릭합니다.

8. 사용 약관에 동의하려면 프롬프트에서 확인란을 선택하고 수락을 클릭합니다.



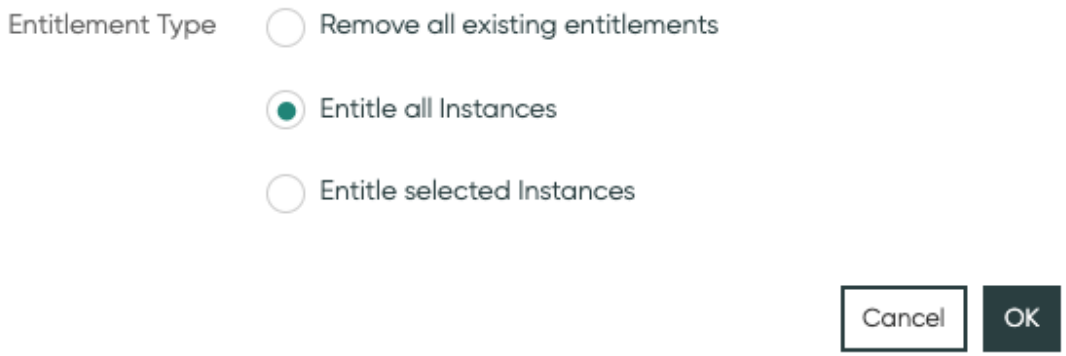
9. 옵션: 또는 다른 ServiceNow AI Platform 인스턴스에서 애플리케이션에 대한 권리를 관리하려면 다음 단계를 수행합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 권리 관리 버튼이 표시되지 않으면 제품 목록에서 응용 프로그램을 클릭하여 취약성 대응용 퍼포먼스 분석 표시합니다.

b. 적격 탭을 선택하고 권리 관리를 클릭합니다.

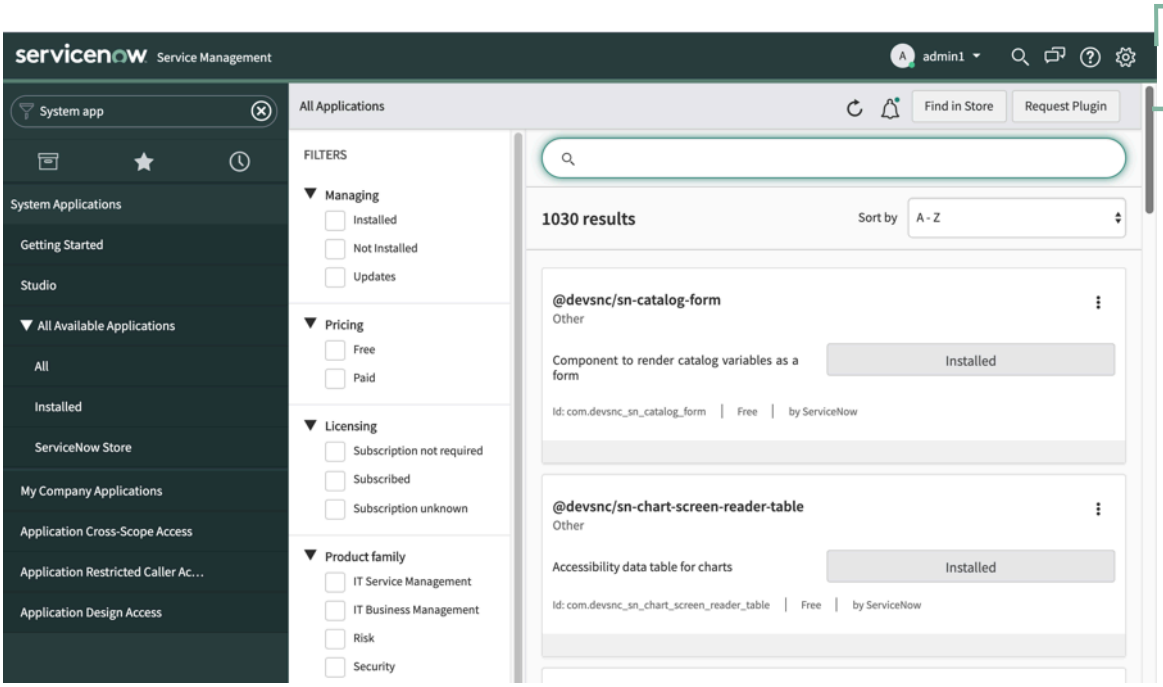
c. 표시되는 Vulnerability Response에 대한 권리 관리 대화 상자에서 다음 중 하나를 선택합니다.



d. 계속하려면 확인 또는 취소를 클릭하십시오.
플러그인을 활성화하고 인스턴스에 애플리케이션을 ServiceNow AI Platform 설치할 준비가 되었습니다.

10. ServiceNow AI Platform 애플리케이션을 설치할 취약성 대응 인스턴스에 로그인합니다.

11. 다음으로 이동 모두 〉 시스템 애플리케이션 〉 모든 사용 가능 애플리케이션 〉 모두.



12. 나열된 애플리케이션에서 Performance Analytics - Content Pack - Vulnerability Response(sn_vul_analytics) 애플리케이션을 찾아 설치를 클릭합니다.

주:
새 버전으로 업데이트하는 경우 선택 목록에서 원하는 버전을 선택합니다.

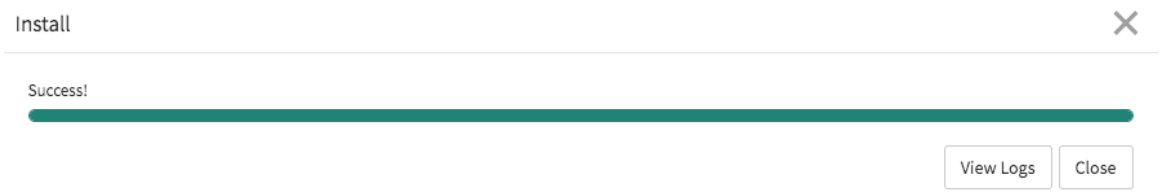
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

을 클릭하고 업데이트를 클릭합니다.
애플리케이션 설치 대화 상자가 표시됩니다. 애플리케이션과 함께 자동으로 설치될 모든 종속성도 표시됩니다.

13. 옵션: 데모 데이터를 원하는 경우 데모 데이터 로드 확인란을 선택하고 설치를 클릭합니다.

> 주:
> 데모 데이터 로드 확인란을 선택하지 않으면 나중에 애플리케이션 관리자에서 데모 데이터를 설치할 수 없습니다. 초기 설치 후 데모 데이터를 설치하거나 다시 설치하는 방법에 대한 자세한 내용은 지식베이스에서 애플리케이션이 이미 설치된 경우 데모 데이터를 설치하기 위한 임시 해결책 (KB0722909) 문서를 Now Support 참조하십시오.

이 설치에는 다소 시간이 걸릴 수 있습니다. 애플리케이션이
성공적으로 설치된 후 설치 대화 상자에 메시지가 표시됩니다.



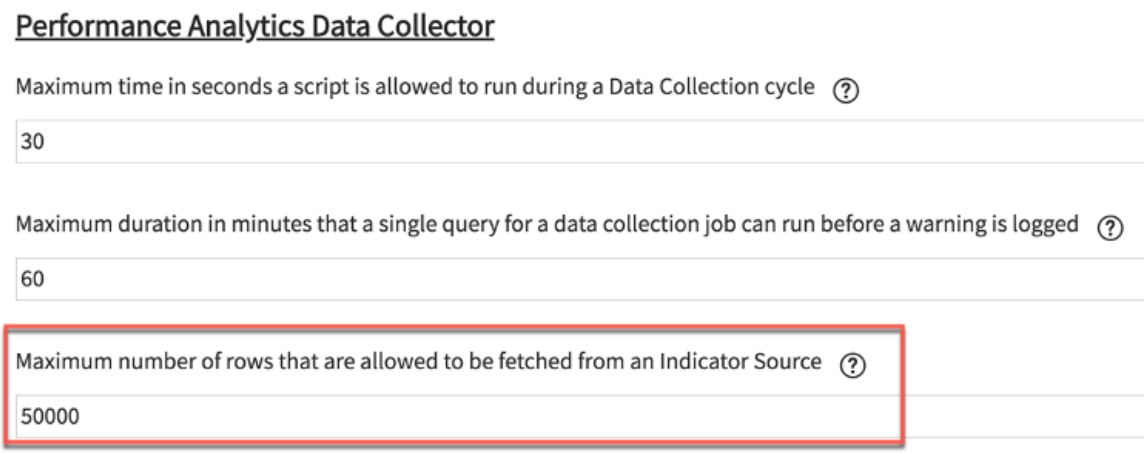
14. 닫기를 클릭합니다.

15. 옵션: 사용자 환경에서 활성 취약한 항목이 많을 것으로 예상되는 경우 수집된 기록의 최대 수에 대한 기본 설정을 변경하고, 예약된 작업을 사용하도록 설정하고, 근무 외 시간 동안 수집 시간을 설정할 수 있습니다.
애플리케이션을 설치한 후 애플리케이션에 대한 이러한 설정 및 기타 설정을 변경하려면 다음 단계를 수행합니다.

   a. 다음으로 이동 모두 〉 퍼포먼스 분석 〉 관리자 콘솔.

   b. 고급 구성 타일에서 **Performance Analytics** 속성 링크를 클릭합니다.

   c. 관리 콘솔 〔퍼포먼스 분석〕 페이지에서 퍼포먼스 분석 데이터 수집기 섹션으로 스크롤합니다.
   기본 설정(50,000개 기록)은 표시기 소스에서 가져올 수 있는 최대 행 수에 대해 표시됩니다.



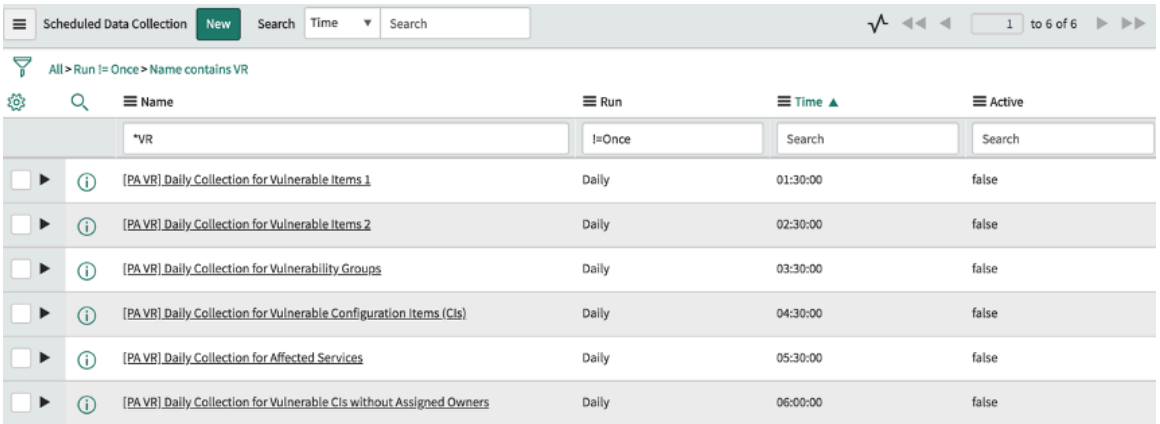
   d. 이 수치를 환경에서 예상되는 총 활성 취약한 항목(VI) 수보다 약 20% 더 큰 값으로 늘리는 것을 선호할 수 있습니다.

   e. 저장을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

f. 예약된 작업을 활성화하려면 다음으로 이동합니다. 퍼포먼스 분석 〉 데이터 수집기 〉 작업.
예약된 데이터 수집 목록이 표시됩니다. 활성 열에서 퍼포먼스 분석 - 콘텐츠 팩 - 취약성 대응에 대한 애플리케이션 열에 나열된 예약된 작업은 기본적으로 사용되지 않습니다(false).

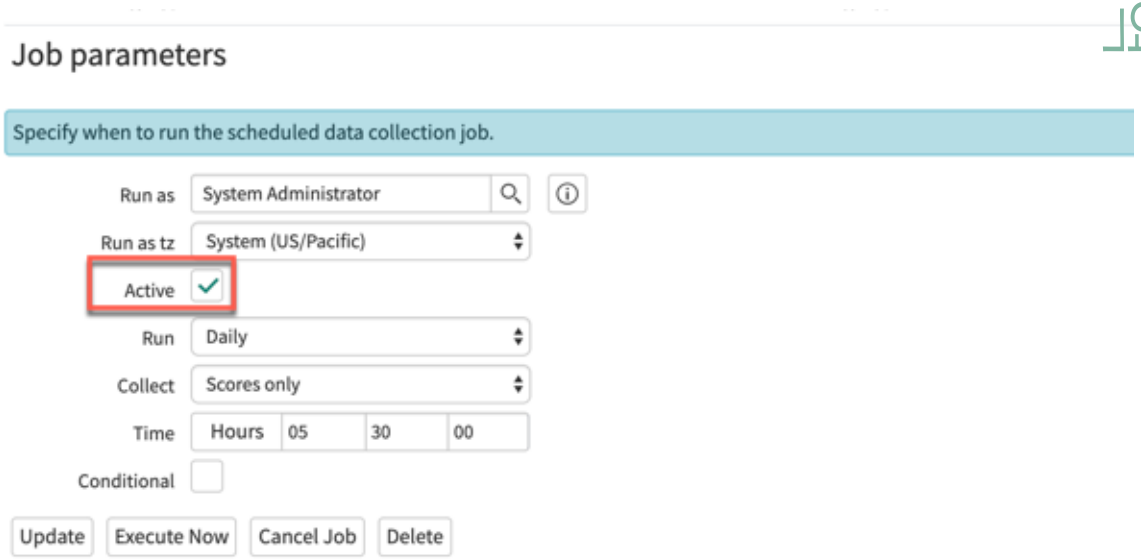
> **주:**
> 기록 데이터 수집을 위한 예약된 작업이 작업 목록에 표시되지 않습니다. 대규모 데이터 집합의 경우 애플리케이션에 대해 취약성 대응 퍼포먼스 분석을 설정할 때 일상적인 작업을 활성화하여 시간 경과에 따른 데이터 및 추세 수집을 시작하는 것이 좋습니다.



g. 이름 열에서 링크를 클릭하여 PA_VR 작업 기록을 엽니다.

h. 필드를 편집할 수 없는 경우 여기 링크를 클릭하여 편집합니다.

i. 작업 매개변수 섹션에서 활성 확인란을 클릭하여 작업을 예약합니다.
시간 필드가 표시됩니다.



j. 작업 시작 시간을 입력합니다.
양이 많을 것으로 예상되는 경우 근무 외 시간에 수거 시간을 설정하는 것이 좋습니다. 사용자 환경에서 1,000만 개 이상의 활성 VI가 예상되면 구현 파트너에게 데이터 수집 환경 설정에 대한 자세한 내용을 문의하십시오 ServiceNow[#] .

데이터 수집에 사용되는 표시기에 대한 자세한 내용은 다음 문서를 참조하십시오 [PA]에 퍼포먼스 분석 대한 취약성 대응 표시기 보기.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

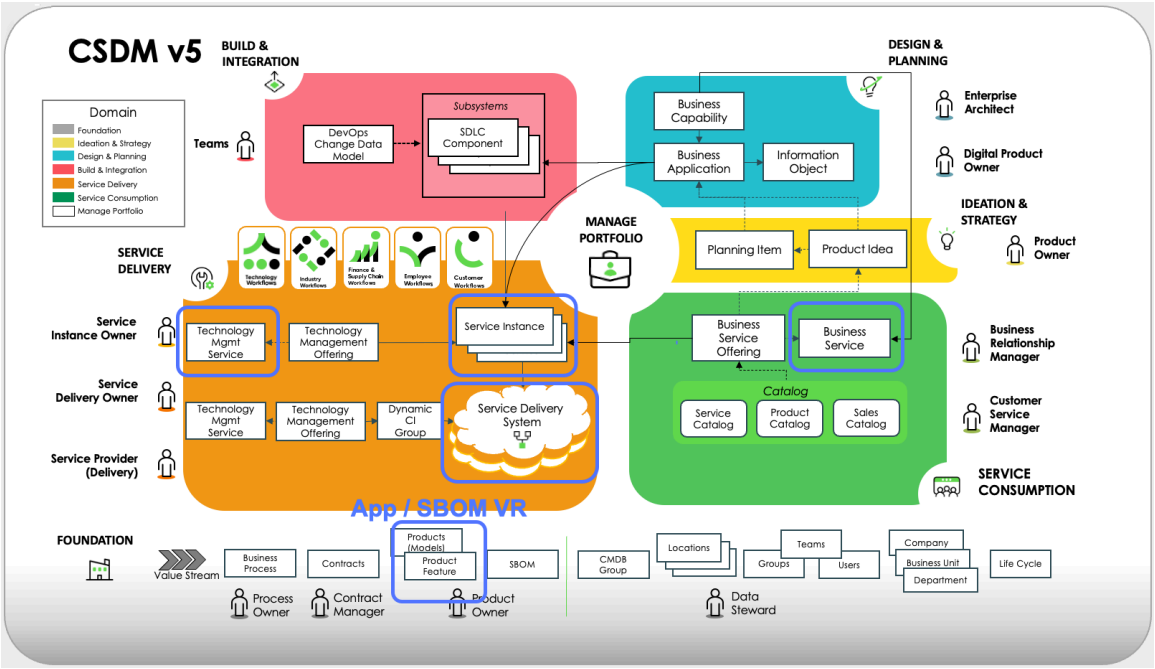
k. 원하는 모든 작업을 활성화한 후 업데이트를 클릭합니다.
예약된 데이터 수집 목록이 표시됩니다. 자세한 내용은 퍼포먼스 분석 속성을 참조하십시오.

다음에 수행할 작업
다음으로 이동 취약성 대응 〉 개요 을 클릭하여 대시보드를 봅니다.

취약성 대응 애플리케이션 및 **CSDM** 테이블

, 취약성 대응애플리케이션 취약성 대응, 타사 취약성 통합 및 소프트웨어 자재 명세서 애플리케이션은 테이블을 관리(데이터 기여) CSDM 합니다. 이러한 애플리케이션은 다른 애플리케이션이 생성하는 테이블의 데이터 CSDM 도 사용합니다. 따라서 여러 ServiceNow 제품이 이러한 보안 운영 애플리케이션의 이점을 누리고 가치를 더합니다.

데이터 **CSDM** 프레임워크 및 취약성 대응 애플리케이션



CSDM 에서 참조하는 취약성 대응테이블 , 애플리케이션 취약성 대응, 타사 취약성 통합 및 소프트웨어 자재 명세서 애플리케이션

자산은 외부 공급업체 취약성 스캐너(통합)에서 임포트될 때 특정 테이블로 취약성 대응 가져와서 표시됩니다.

- 검색된 항목을 호스팅 취약성 대응 합니다.
- 클라우드 및 컨테이너 취약성 대응 검색된 이미지
- 애플리케이션 취약성 대응 검색된 애플리케이션(제품 모델)

CMDB 구성 항목(CI) 조회의 일부 보안 운영 로서 임포트한 데이터의 (CI) 기록을 CMDB의 기존 기록과 일치시키기 위해 검색이 수행됩니다.

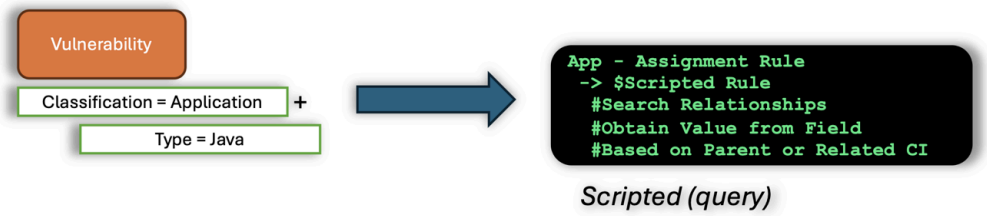
각 특정 CI 기록에는 취약한 항목 할당 규칙에 대한 입력으로 사용할 수 있는 CI에 채워진 검색 불가능한 속성(예: 지원 그룹 또는 분류)이 포함될 수 있습니다. 이러한 속성은 업스트림 기술 서비스 오퍼링을 기반으로 하는 Common Service Data Model(CSDM) 동기화에서 채워질 수 있습니다.

, , 외부 공급업체 취약성 통합 및 소프트웨어 자재 명세서 애플리케이션에 관련 CSDM 객체를 애플리케이션 취약성 대응취약성 대응활용하려면 스크립팅된 규칙을 사용해야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예를 들어 취약한 항목 담당 규칙을 사용하여 정정할 취약한 항목을 자동으로 할당하려면 임포트한 취약성 항목에서 업데이트되는 구성 항목 분류 값을 활용하는 규칙을 만들 수 있습니다. 이 경우 관련 CSDM 객체에서 원하는 대상 값을 쿼리하는 스크립팅된 규칙이 필요합니다.

다음은 CI에 Java가 있고 취약성 항목에 연결되어 있는지 확인하는 데 사용할 수 있는 스크립팅된 쿼리의 예입니다.



Scripted (query)

취약성 대응, 애플리케이션 취약성 대응, 타사 취약성 통합 및 소프트웨어 자재 명세서 애플리케이션은 다음 테이블을 참조합니다. 자세한 내용은 CSDM 데이터 프레임워크 및 취약성 대응 애플리케이션 이미지를 참조하십시오.

- 제품 모델 [cmdb_model] 테이블(및 소프트웨어 자재 명세서에서 참조애플리케이션 취약성 대응).
- 애플리케이션 모델 [cmdb_application_product_model] 테이블(및 소프트웨어 자재 명세서에서 참조애플리케이션 취약성 대응).
- 구성 항목 [cmdb_ci] 테이블입니다.
- 비즈니스 서비스 [cmdb_ci_service_business] 테이블입니다.
- 서비스 [cmdb_ci_service] 테이블입니다.
- CMDB 그룹 [cmdb_group] 테이블입니다.
- 동적 CI 그룹 [cmdb_ci_query_based_service] 테이블.

CSDM, 애플리케이션 취약성 대응**,** 외부 공급업체 취약성 통합 및 소프트웨어 자재 명세서 애플리케이션에서 사용하는 취약성 대응테이블

1. 제품 모델 [cmdb_model] 테이블(및 소프트웨어 자재 명세서에서 사용됨애플리케이션 취약성 대응).
2. 애플리케이션 모델 [cmdb_application_product_model] 테이블(및 소프트웨어 자재 명세서에서 사용됨애플리케이션 취약성 대응).
3. 구성 항목 [cmdb_ci] 테이블입니다.
4. 비즈니스 애플리케이션 [cmdb_ci_business_app](및 소프트웨어 자재 명세서에서 사용애플리케이션 취약성 대응).
5. 비즈니스 서비스 [cmdb_ci_service_business]
6. 기술 관리 서비스[cmdb_ci_service_technical] 테이블(이전의 기술 서비스)

주:

파일을 업로드할 소프트웨어 자재 명세서 때 SBOM 애플리케이션은 업로드하는 모든 제품 모델 및 비즈니스 애플리케이션을 CMDB에 이미 있는 제품 모델 및 비즈니스 애플리케이션과 일치시키려고 합니다. 서비스 인스턴스(이전의 애플리케이션 서비스) 또는 비즈니스 애플리케이션을 제품 모델에 연결할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

,, 애플리케이션 취약성 대응외부 공급업체 취약성 통합 및 소프트웨어 자재 명세서 애플리케이션에 가치를 취약성 대응더하는 제품

취약성 대응 다음 ServiceNow 제품과 함께 애플리케이션을 사용하면 조직에 도움이 될 수 있습니다.

외부 공급업체 취약성 스캐너 및 통합

NVD(국가 취약성 데이터베이스)에서 임포트한 취약성과 외부 공급업체 스캐너의 탐지 데이터가 CMDB의 자산과 조정됩니다. 임포트한 취약성이 기존 자산과 일치하면 취약한 항목이 생성됩니다. 취약한 항목은 정정 작업으로 자동 그룹화되고, 비즈니스 컨텍스트에 따라 위험 점수가 매겨지며, 정정을 위해 우선순위가 지정되고 적절한 팀에 할당됩니다. 자세한 내용 및 통합 목록은 다음 문서를 참조하십시오 취약성 대응 통합.

CWE Comprehensive 2000 및 NVD 통합

NIST NVD(국가 취약성 데이터베이스) 및 CWE(일반적인 약점 열거) 통합에서 임포트한 데이터는 인스턴스의 취약성 데이터를 보강하고 취약성, 취약한 항목 또는 정정 작업에 대한 정정을 에스컬레이션할지 여부를 결정하는 데 사용됩니다. 자세한 내용은 AND CWE 기록을 업데이트하기 위해 예약된 작업을 구성하고 실행합니다. 문서를 참조하십시오NVD 통합 이해.

와의 통합이 도움이 되는 제품 소프트웨어 자재 명세서

보안 태세 통제

보안 태세 통제 를 사용하면 사이버 보안 팀이 전체 엔터프라이즈 자산 인벤토리에 대한 가시성을 확보하고 전반적인 보안 태세를 결정할 수 있습니다. 의 SPC 정책은 애플리케이션과 함께 취약성 대응 임포트한 취약성이 있는 자산을 탐지하여 보안 도구 범위 격차를 찾는 데 도움이 될 수 있습니다.

거버넌스, 리스크 및 컴플라이언스

지속적인 모니터링, 우선순위 지정 및 자동화를 제공하는 통합 위험 프로그램과 보안과 IT를 연결합니다.

DevOps

GitHub 환경에서 시작하는 GitHub Actions를 사용하여 소프트웨어 개발 주기 동안 잠재적으로 유해한 구성 요소로부터 환경을 보호합니다. GitHub 리포지토리에서 SBOM 파일을 ServiceNow AI Platform 업로드합니다.

담당 규칙 생성 또는 편집 취약성 대응

설정 도우미를 사용하여 담당 규칙에 대한 초기 평가를 완료한 후에는 필터 조건에 따라 취약한 항목을 자동으로 할당하는 규칙을 만들 수 있습니다. 이러한 규칙은 취약한 항목을 임포트하거나 수동으로 생성할 때 할당합니다.

시작하기 전에

필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)
가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

이 태스크 정보

기본 시스템에는 CI 지원 그룹과 동일한 할당 그룹에 취약한 항목을 할당하는 하나의 취약성 할당 규칙인 **CI** 지원 그룹에 할당이 함께 제공됩니다. 필터 조건을 사용하여 이 규칙을 수정하거나 새 규칙을 만들 수 있습니다. 담당 규칙을 사용하여 할당 조건과 실행 순서를 정의합니다. VI가 규칙 조건과 일치하면 할당 조회가 중지됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 담당 규칙.
2. CI에 할당 지원 그룹 규칙을 열거나 새로 만들기를 클릭합니다.
3. 새로 만들기인 경우 양식의 필드에 적절한 정보를 입력합니다.

취약성 담당 규칙

필드	설명
이름	그룹 규칙의 이름입니다.
활성	할당 규칙이 활성 상태인지 여부를 나타냅니다.
실행 순서	규칙이 평가되는 순서입니다. 우선 순위가 높은 규칙, 특별한 처리가 필요한 항목, 위험이 중요한 경우 또는 규정 준수에서 VI를 처리해야 하는 항목을 먼저 실행해야 합니다. 다음으로, 특별한 처리가 필요하지 않은 일반 규칙을 실행하고 누가 책임을 져야 하는지 알 수 있습니다. 마지막으로, VI가 속해야 하는 할당 그룹을 파악하기 위해 VI를 그룹에 할당하는 기본 규칙을 생성합니다. 이 그룹은 그들의 결정을 다루기 위해 또 다른 규칙을 추가할 수 있습니다. 이 기본 규칙은 마지막에 실행됩니다.
설명	할당 규칙에 대한 설명입니다.
조건	
미리 보기	이 쿼리가 반환하는 결과 수를 표시합니다.
조건 필드	충족되어야 하는 조건입니다. 주: 담당 규칙의 조건 필터에서 자산 태그를 사용할 수 있게 하려면 Rapid7 InsightVM 다른 Rapid7 InsightVM 통합보다 먼저 자산 목록 통합을 실행해야 Rapid7 InsightVM 합니다. 조건 작성기에 입력한 검색 텍스트의 대소문자 구분은 이 기록이나 양식에서 지원되지 않습니다.
새 기준	선택할 조건 필터 필드를 더 추가합니다.
할당 사용	이 규칙에 따라 생성된 그룹의 할당을 자동화하려면 사용 가능한 옵션 중 하나를 선택합니다. ○ 사용자 그룹: 조회 테이블에서 사용자 그룹을 선택합니다. ○ 사용자 그룹 필드: 드롭다운 메뉴에서 사용자 그룹 필드를 선택합니다. ○ 스크립트: 스크립트를 만들거나 편집합니다. 주: 스크립트를 만들거나 편집하려면 전문 지식이 필요합니다 ServiceNow .

4. 제출을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

새 규칙이나 업데이트된 규칙은 다음 임포트 시 평가됩니다.

주:

다시 적용 기능을 사용하려면 규칙의 베이스라인 적용이 필요합니다. 규칙이 생성되면 아직 수행하지 않은 경우 편한 시간에 실행할 예약된 작업을 활성화합니다 *Reapply all vulnerability assignment rules* . 수동으로 할당된 규칙을 제외한 모든 Open VI에 모든 규칙이 적용됩니다. 환경에 얼마나 많은 활성 VI가 있는지에 따라 성능에 영향을 미치지 않도록 초기 실행 후 실행 필드를 적절하게 설정해야 합니다.

이 예약된 작업을 실행하지 않은 경우 할당 규칙 양식에서 변경 적용 단추를 사용하려고 할 때 실행해야 합니다. 담당 규칙을 다시 적용해도 취약한 항목은 다시 그룹화되지 않습니다.

ML을 취약성 대응 사용하여 할당 규칙 생성

다음 스크립트를 사용하여 예측 인텔리전스의 ML 권장 사항을 사용하여 정정을 위해 취약한 항목을 자동으로 할당하는 예비 연락망 할당 규칙을 생성합니다.

시작하기 전에

애플리케이션에 대한 취약성 대응 취약성 할당 권장 사항을 설치하고 활성화해야 합니다. 이 애플리케이션은 에서 사용할 수 있습니다 ServiceNow Store.

분류 솔루션을 정의하고, 활성화하고, 교육해야 합니다. 이 모델을 사용하면 담당 규칙에서 의도한 수신자에 대한 올바른 일치 항목을 찾지 못한 경우 VI(취약한 항목)에 대한 적절한 할당 그룹을 예측하는 데 도움이 됩니다.

이 규칙은 다른 할당 규칙이 이미 완료된 후 할당되지 않은 VI 수를 줄이는 데 도움이 될 수 있습니다.

자세한 내용은 AND 에 대한 솔루션 정의 생성 및 교육 취약성 대응 문서를 참조하십시오취약성 대응용 취약점 할당 권장 설치.

필요한 역할: sn_vul.vulnerability_admin

이 태스크 정보

고급 코딩 경험이 있거나 예측 인텔리전스 기능 및 담당 규칙의 작동 방식에 대한 ServiceNow AI Platform심층적인 지식이 있는 경우에만 이 작업을 수행하는 것을 선호할 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 담당 규칙.
2. 새로 만들기를 선택합니다.
3. 양식의 필드에 적절히 입력합니다.
   이러한 필드에 대한 자세한 내용은 을 참조하십시오 담당 규칙 생성 또는 편집 취약성 대응 .
4. 선택 사용 할당 목록에서 스크립트를 선택합니다.
5. 편집기에서 다음 스크립트를 복사하여 붙여넣습니다.

```
  /*
  * Catch-all assignment rule using ML recommendation
  * NOTE: Requires Vulnerability Assignment Recommendations for Vulnerability Response
  * Classification Solution must be active and trained
  */
var vitID = current.sys_id;
getMLAssignmentRecommendation(vitID);

function getMLAssignmentRecommendation(vulnerableItemSysId) {
  var ARU = new sn_vul.AssignmentRecommendationUtils();
  ARU.initialize();
```


© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
    var viPredictionObj = ARU.getPredictionsForVI(vulnerableItemSysId);
    /*
    *returns object containing array of predictions
    *payload structure:
    *
    {
       "predictions": [
          {
             "sys_id": "b6ed54f3db7b23005daef4eabf9619f3",
             "name": "Windows Server support ",
             "confidence_score": "57.54"
          },
          ...
       ],
       "exception": ""
    }
    */
    var viPredictionArray = viPredictionObj['predictions'];
    var topPredictionObj = viPredictionArray.shift();

    return topPredictionObj['sys_id'];
}
```

6. 제출을 선택합니다.

다음에 수행할 작업
담당 규칙 및 예약된 작업에 대한 보다 일반적인 정보는 검토하십시오 취약성 대응 할당 규칙 개요*Reapply all vulnerability assignment rules* .

취약성 대응 서비스 지원을 위한 할당 규칙 생성

다음 스크립트를 사용하여 영향을 받는 비즈니스 서비스에 따라 정정할 취약한 항목을 할당하는 규칙을 생성합니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin

이 태스크 정보
고급 코딩 경험이 있거나 담당 규칙의 작동 방식에 대한 ServiceNow AI Platform 심층적인 지식이 있는 경우에만 이 작업을 수행하는 것이 좋습니다.

이 규칙을 사용하면 CMDB에 나열된 비즈니스 서비스와 얼마나 밀접하게 일치하는지에 따라 VI가 할당됩니다. 관련 서비스, 부서 또는 지원 그룹이 일치하지 않으면 VI가 취약성 분석가 그룹에 할당됩니다.

이 규칙은 다른 할당 규칙이 이미 완료된 후 잘못 할당되거나 할당되지 않은 VI 수를 줄이는 데 도움이 될 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 담당 규칙.

2. 새로 만들기를 선택합니다.

3. 양식의 필드에 적절히 입력합니다.
이러한 필드에 대한 자세한 내용은 을 참조하십시오 담당 규칙 생성 또는 편집 취약성 대응 .

4. 선택 사용 할당 목록에서 스크립트를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. 편집기에서 다음 스크립트를 복사하여 붙여넣습니다.

```
/*
Assigns Vulnerable Item based on related Business Service
Assigns to default Vulnerability Analyst group if no related Business Service
*/
assignToServiceSupport(current);

function assignToServiceSupport(vitGR) {
   var ci = vitGR.getValue('cmdb_ci');
   var defaultAssignmentGroup = 'Vulnerability Analyst';
   var defaultGR = new GlideRecord('sys_user_group');
   defaultGR.get('name', defaultAssignmentGroup);
   var defaultAssignmentGroupID = defaultGR.sys_id;

   var maxSizeValue =
global.SecProperty.getProperty("sn_sec_cmn.services_affected_by_CI_max_size", 1000);
   var maxDepthValue =
global.SecProperty.getProperty("sn_sec_cmn.services_affected_by_CI_max_depth", 10);
   var customValues = {
      "maxDepth": maxDepthValue,
      "maxSize": maxSizeValue
   };
   var ciu = new global.CIUtils();
   var services = ciu.servicesAffectedByCI(ci, customValues);
   var svc = new GlideRecord("cmdb_ci_service");
   var hasSvc = false;
   if (services && services.length > 0) {
      svc.addQuery("sys_id", "IN", services.join(",")); // returns the service with highest
business criticality. Implement alternate logic here.
      svc.addNotNullQuery("busines_criticality"); // typo intended
      svc.orderBy("busines_criticality");
      svc.setLimit(1);
      svc.query();
      hasSvc = svc.next();
   }
   if (!hasSvc) {
      // If there are no services it should be assigned to a default assignent group
      return defaultAssignmentGroupID;
   } else {
      var serviceAssignmentGroup = hasSvc.getValue('support_group'); //Also consider
managed_by_group, assignment_group, change_control
      return !gs.nil(serviceAssignmentGroup) ? serviceAssignmentGroup :
defaultAssignmentGroupID; //Return the Service assignment group if it is not empty, return
the default assignment group otherwise.
   }
}
```

6. 제출을 선택합니다.

다음에 수행할 작업
담당 규칙 및 예약된 작업에 대한 보다 일반적인 정보는 검토하십시오 취약성 대응 할당 규칙 개요*Reapply all vulnerability assignment rules*.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

정정 작업 규칙 생성 또는 편집 취약성 대응

설정 도우미를 사용하여 정정 작업 규칙에 대한 초기 평가를 완료한 후에는 필터 조건에 따라 취약한 항목을 자동으로 그룹화하는 규칙을 만들 수 있습니다. 이러한 규칙은 취약한 항목을 가져오거나 수동으로 생성할 때 자동으로 그룹화합니다. 이 규칙에 따라 그룹화된 취약한 항목을 제한하려면 필터를 사용합니다(예: 익스플로잇이 있는 모든 취약한 항목 선택).

시작하기 전에

필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)

이 태스크 정보

기본 시스템에는 취약성 및 할당 그룹(할당 규칙)별로 취약한 항목을 그룹화하는 하나의 정정 작업 규칙인 취약성이 함께 제공됩니다. 양식 또는 목록 뷰에서 규칙을 다시 적용할 수 있습니다. 일부 샘플 항목의 취약성 대응 정정 작업 규칙의 예경우 .

이 규칙은 다음과 같이 수정할 수 있습니다.

필터 조건 사용 및 선택 사항별 그룹화

기본적으로 정정 작업은 사용 가능한 경우 담당 규칙을 필터 기준의 일부로 사용합니다.

> **주:**
> 담당 규칙이 없는 경우 사용자 그룹 필드를 사용하여 그룹을 선택할 수 있습니다.

의 취약성 대응버전 18.0부터 취약성 정정 작업 규칙이 새로운 구현에 대해 비활성화 취약성 대응 됩니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 정정 작업 규칙.
2. 규칙을 열거나 새로 만들기를 클릭합니다.
3. 새로 만들기인 경우 양식의 필드에 적절한 정보를 입력합니다.

정정 작업 규칙

필드	설명
이름	작업 규칙의 이름입니다.
활성	작업이 활성 상태인지 여부를 나타냅니다.
설명	규칙에 대한 설명입니다.
대소문자 구분	조건이 대/소문자를 구분하는지 여부를 결정합니다. **주:** 기본값은 대/소문자를 구분하지 않습니다.
조건	규칙에 대한 선택적 필터 조건입니다. **주:** 정정 작업 규칙의 조건 필터에 자산 태그를 사용할 수 있도록 하려면 Rapid7 InsightVM 다른 Rapid7 InsightVM 통합보다 먼저 자산 목록 통합을 실행해야 Rapid7 InsightVM 합니다. 기본적으로 (대/소문자 구분 확인란 비활성화) 작업 규칙 기록 및 양식의 조건 작성기에서 입력하는 검색 텍스트는 대소문자를 구분하지 않습니다. 작업 기록 및 양식에서 대/소문자 구분 검색을 사용하도록 설정할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
그룹화 기준(최대 6개의 조건 세트 사용 가능)	
다음 중 취약한 항목 그룹화	규칙이 VI를 그룹화하는 데 사용하는 테이블입니다. 최대 6개의 필터를 사용할 수 있습니다. 선택 항목은 다음과 같습니다. ○ 취약한 항목 [sn_vul_vulnerable_item] ○ 취약한 항목 → 구성 항목 [cmdb_ci] ○ 취약한 항목 → 취약성 [sn_vul_third_party_entry] 주: 확장된 테이블을 선택하면 해당 확장 테이블을 사용하는 취약한 항목에만 사용 필드가 적용됩니다.
필드 사용	규칙이 VI를 그룹화하는 데 사용하는 테이블의 필드입니다.
할당	
정정 작업 할당자	정정 작업을 자동으로 할당하면 취약한 항목을 그룹화하기 위해 그룹화 기준 선택 사항과 함께 할당 선택 항목이 사용됩니다. 각 취약한 항목이 일치하는 할당 그룹 집합이 있는 작업에 배치되도록 필요에 따라 새 작업이 생성됩니다. 이 규칙을 기반으로 생성된 작업의 할당을 자동화하려면 사용 가능한 옵션 중 하나를 선택합니다. ○ 필드별로 그룹화: 그룹화 기준섹션의 필드 값 사용 섹션에서 사용자 그룹 필드를 선택한 경우 드롭다운 메뉴에 표시됩니다. ○ 사용자 그룹: 조회 목록을 사용하여 정적 사용자 그룹을 선택합니다.

주:
그룹화 기준 설정에 대한 생각이 변경되면 필드별로 그룹화 지우기 관련 링크는 양식의 그룹화 기준 필드를 재설정합니다.

그룹 규칙이 삭제되면 양식 또는 목록 보기에서 해당 규칙에 따라 생성된 모든 오픈 그룹을 삭제할 수 있습니다. 오픈 상태가 아닌 그룹은 제외됩니다.

일부 샘플 항목은 다음 문서를 참조하십시오 취약성 대응 정정 작업 규칙의 예.

Vulnerability Response 위험 계산기의 위험 규칙에 대한 필드와 가중치 정의

조직에 고유한 취약성 및 자산 데이터를 사용하는 위험 점수를 생성할 수 있도록 위험 규칙의 매개변수와 가중치를 사용자 지정합니다. 위험 규칙에 포함된 필드를 선택하여 효과적인 위험 점수 매기기 프레임워크를 정의할 수 있습니다.

시작하기 전에
또한 구성 관리 데이터베이스(CMDB)의 configuration_item [cmdb_ci]에 있는 속성을 사용하면 취약성 대응 위험 계산기의 논리를 만드는 데 도움을 받을 수 있습니다. 예를 들어 조직에서 외부 연결 CI가 더 취약하고 즉각적인 수정이 필요할 수 있다고 판단되는 경우 이러한 CI와 같은 *Internet Facing* 속성을 할당할 수 있습니다. 이 속성 및 기타 속성은 Orlando 제품군 릴리스에 대한 Common Service Data Model 릴리스 정보에 나열되어 있습니다. 에 CMDB대한 최신 정보 및 지침은 다음 주제를 참조하십시오.

- Common Service Data Model 개념적 모델
- CMDB 스키마 모델

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필요한 역할: sn_vul.manage_risk_score_configuration

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 취약성 계산기.
2. 취약성 계산기 페이지에서 기본 위험 계산기를 선택합니다.
3. 다음으로 이동 취약성 계산기 페이지 〉 취약성 계산기 규칙 탭 〉 기본 위험 규칙.
4. 옵션: 취약성 위험 규칙 페이지의 위험 계산기 기준 섹션에서 전체 위험 점수 계산에서 중요도에 따라 각 기준의 가중치를 설정합니다.
5. 규칙을 비활성화하려면 활성 확인란의 선택을 취소해야 합니다.
6. 위험 계산 기준에 위험 규칙 필드를 추가하려면 기준 추가를 선택합니다.
7. 양식에서 필드를 채웁니다.

위험 규칙 필드 양식

필드	설명
참조 테이블 선택	위험 점수 가중치를 정의하는 데 사용하는 테이블입니다. 다음 옵션 중 하나를 선택할 수 있습니다. ○ 취약한 항목: 취약한 항목(VI)에서 직접 닷워킹 가능한 필드를 추가합니다. ○ 취약한 항목 - 구성 항목: 하드웨어 테이블과 같은 기본 테이블 확장의 일부인 dot-walkable 필드를 추가합니다. 이러한 필드는 기본 테이블(cmdb_ci)의 일부가 아닙니다. ○ 취약한 항목 - 취약성: 기본 테이블을 확장하는 테이블의 일부인 dot-walkable 필드를 추가합니다(예: 외부 공급업체 항목). 이러한 필드는 취약성 항목 기본 테이블의 일부가 아닙니다. ○ 취약한 항목 참조 테이블: 관련 테이블(m2m) 또는 취약한 항목에 대한 참조가 있는 테이블에 속하는 필드를 추가합니다. 이러한 필드는 VI에서 직접 닷워킹할 수 없습니다. ○ 구성 항목 참조 테이블: cmdb_ci에 대한 참조가 있는 cmdb_ci 또는 테이블의 관련 테이블(m2m)에 속하는 필드를 추가합니다. 이러한 필드는 VI에서 직접 닷워킹할 수 없습니다. ○ 취약성 참조 테이블: sn_vul_entry에 대한 참조가 있는 sn_vul_entry 또는 테이블의 관련 테이블(m2m)에 속하는 필드를 추가합니다. 이러한 필드는 VI에서 직접 닷워킹할 수 없습니다. ○ 사용자 지정 조건: 조건을 평가하여 규칙에 가중치를 할당하려면 이 옵션을 사용합니다. 예를 들어 인터넷 연결 필터는 CI(구성 항목)가 외부인지 내부인지를 결정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
테이블	참조 테이블 선택에서 다음 옵션 중 하나를 선택한 경우에만 나타나는 필드입니다. ○ 취약한 항목 -> 구성 항목 ○ 취약한 항목 -> 취약성 ○ 취약한 항목 참조 테이블 ○ 구성 항목 참조 테이블 ○ 취약성 참조 테이블
필드	이 규칙에 대한 위험 점수 계산에 사용할 필드입니다.
집계	참조 테이블 선택에서 참조 테이블을 선택한 경우에만 나타나는 필드입니다. 관련 테이블(m2m)에서 필드를 선택할 때 계산에 고려할 최소값 또는 최대값을 선택합니다.
가중치	위험 규칙 내에서 이 필드의 가중치입니다. 값은 0에서 100 사이의 정수여야 합니다.
값 가중치 정의	각 필드 값에 가중치를 할당하는 구성요소입니다. 숫자 필드의 경우 필드 값을 범위(예: 1-5)로 정의할 수 있습니다. 가중치는 0에서 100 사이의 정수여야 합니다. 주: 참조 테이블 선택에서 사용자 지정 조건 옵션을 선택한 경우에는 이 필드가 표시되지 않습니다.
조건 테이블	참조 테이블 선택에서 사용자 지정 조건을 선택한 경우에만 나타나는 필드입니다. 목록에서 조건을 선택합니다.
필드 이름	참조 테이블 선택에서 사용자 지정 조건을 선택한 경우에만 나타나는 필드입니다. 위험 기준의 이름을 입력합니다.
조건	참조 테이블 선택에서 사용자 지정 조건을 선택한 경우에만 나타나는 필드입니다. 정의된 조건과 일치하는 이 테이블의 항목을 미리 봅니다.

8. 제출을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

9. 규칙 페이지에서 규칙을 활성화하고 다시 적용하여 활성 취약한 항목의 위험 점수를 다시 평가합니다.

   주:
   의 버전 23.0 취약성 대응부터 다음의 경우:

   - 기본 위험 계산기 규칙: 취약한 항목(VIT)의 위험 점수가 변경될 때마다 다음 상세 정보가 VIT의 메모 섹션에 문서화됩니다.
     - 계산기 그룹 이름
     - 계산기 이름
     - 가중치가 1보다 크고 위험 점수가 기여하는 필드 값입니다.
     - 최종 위험 점수
   - 취약성 심각도 위험 규칙: VIT에서 위험 점수가 업데이트될 때마다 메모 섹션이 다음 상세 정보로 업데이트됩니다.
     - 계산기 그룹 이름
     - 계산기 이름: 계산기 규칙이 템플릿 또는 스크립트를 기반으로 하는지 여부에 따라 괄호 안에 이름이 세부 정보와 함께 추가됩니다. 계산기 규칙의 기초를 수정하거나 보려면 규칙을 선택하고 고급 보기 확인란을 선택합니다. 값 유형 드롭다운 상자에서 필요한 옵션을 선택합니다. 템플릿을 선택하면 규칙에 지정된 조건에 따라 위험 점수가 업데이트됩니다. 스크립트를 선택한 경우 기존 스크립트를 추가하거나 업데이트할 수 있습니다.

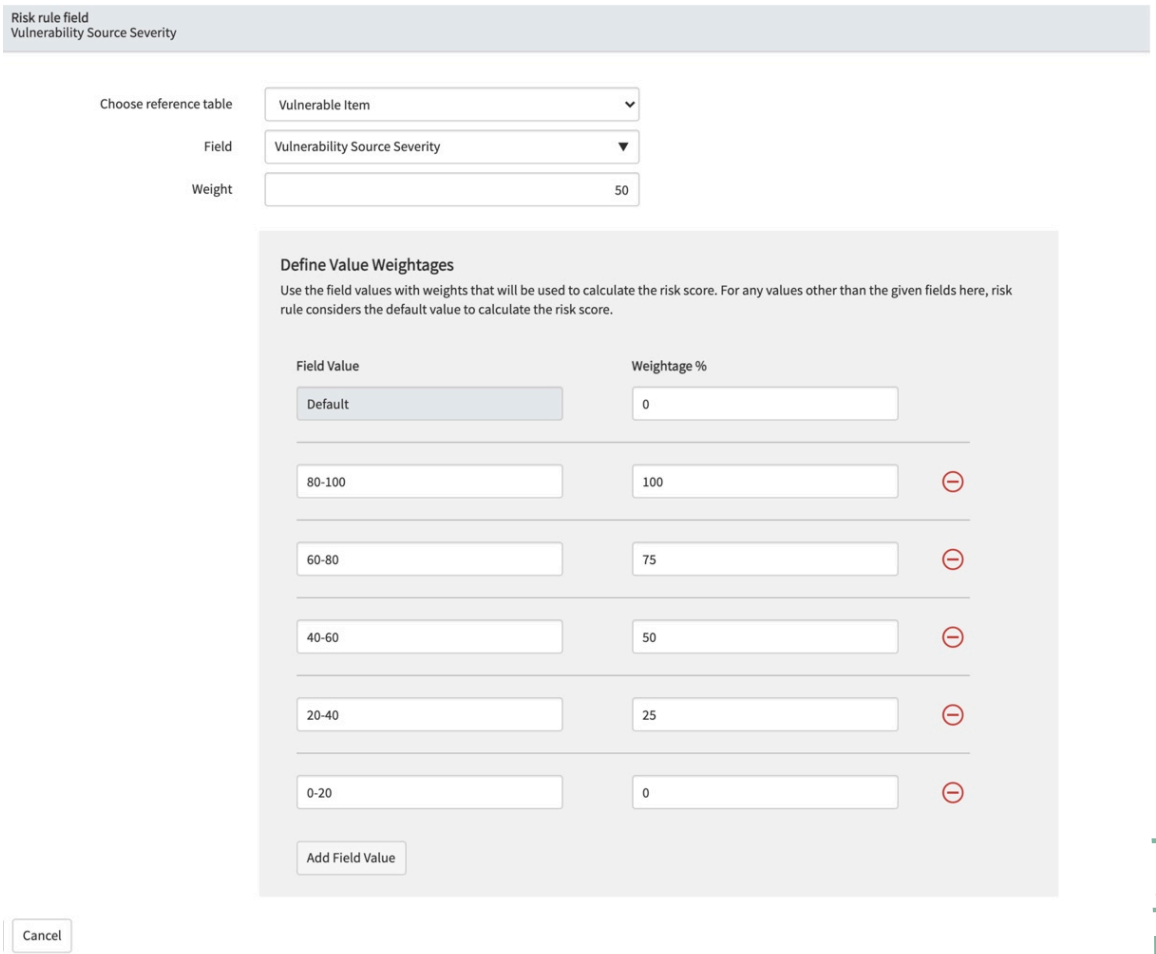
Example:
예시 1: 소스 심각도를 위험 규칙의 기준으로 추가합니다.

사용 사례: Qualys 및 Tenable과 같은 외부 공급업체 벤더는 자체 점수를 제공합니다. 이러한 점수는 sn_vul_entry 테이블의 소스 심각도 필드에 채워집니다. 이 필드는 위험 점수 계산에 사용합니다. 이 점수를 사용하여 위험 점수를 계산하려면 다음을 수행합니다.

1. 위험 규칙 페이지로 이동합니다.
2. 규칙을 비활성화하려면 활성 확인란의 선택을 취소합니다.
3. 위험 계산 기준에 위험 규칙 필드를 추가하려면 기준 추가를 선택합니다.
4. 참조 테이블 선택 목록에서 취약한 항목을 선택합니다.
5. 필드 목록에서 취약성.소스 심각도를 선택합니다.
6. 가중치 필드에 위험 규칙 내에서 이 필드의 상대적 중요도를 입력합니다. 값은 0에서 100 사이의 정수여야 합니다.
7. 값 가중치 정의 섹션에서 필드 값을 추가하고 가중치를 할당합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약한 항목 테이블



8. 제출을 선택합니다.

예 2: 비즈니스 중요도를 위험 규칙의 기준으로 추가합니다.

사용 사례: 조직에 많은 비즈니스 서비스가 있다고 가정해 보겠습니다. 구성 항목(CI) LINUX-SF-6381은 다음 서비스에서 사용되고 있습니다.

비즈니스 서비스의 중요도

비즈니스 서비스	중요도
클라우드 관리	1 - 가장 중요함
전자 상거래	2 - 다소 중요함
클라이언트 서비스	3 - 덜 중요함
출장 및 경비	4 - 중요하지 않음

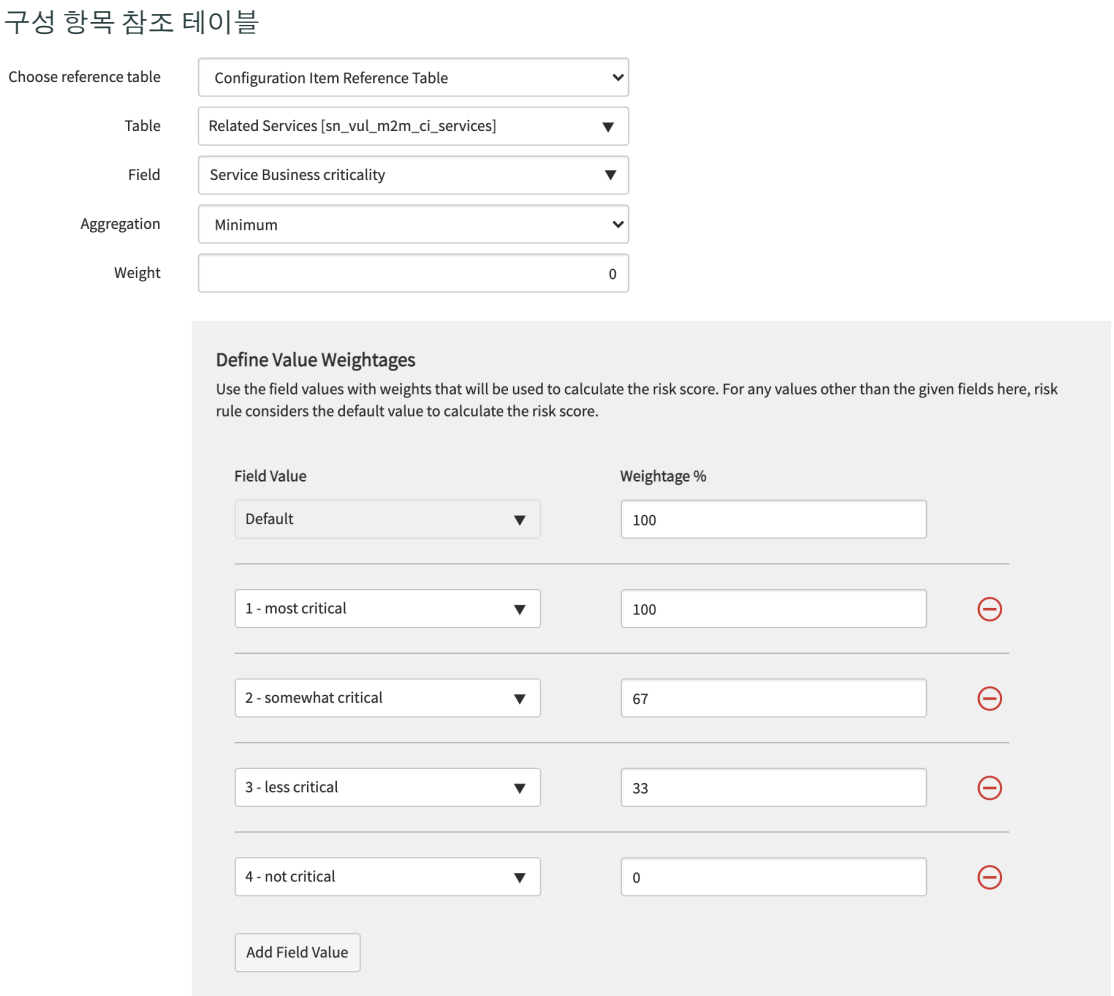
CI와 서비스 간의 매핑은 관련 서비스 [sn_vul_m2m_ci_services] 테이블에 저장됩니다. 자산 LINUX-SF-6381에서 취약성이 발견되면 VI(취약한 항목)가 생성됩니다. 영향을 받는 서비스의 비즈니스 중요도 값을 사용하여 이 VI에 대한 위험 점수를 계산할 수 있습니다. 이러한 서비스의 중요도 값을 사용하여 위험 점수를 계산하려면 다음을 수행합니다.

1. 위험 규칙 페이지로 이동합니다.

2. 규칙을 비활성화하려면 활성 확인란의 선택을 취소합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 위험 계산 기준에 위험 규칙 필드를 추가하려면 기준 추가를 선택합니다.
4. 참조 테이블 선택 목록에서 구성 항목 참조 테이블을 선택합니다.
5. 테이블 목록에서 관련 서비스 (sn_vul_m2m_ci_services)를 선택합니다.
6. 필드 목록에서 **Service.Business** 중요도를 선택합니다.
7. 집계 필드에서 최소를 선택하여 이 사용 사례에 대해 가장 중요한 서비스(**1 -** 가장 중요한 값)를 검색하거나 최대를 선택하여 이 사용 사례에서 이 사용 사례에 대해 가장 중요하지 않은 서비스(**4 -** 중요하지 않은 값)를 검색합니다.
8. 가중치 필드에 위험 규칙 내에서 이 필드의 상대적 중요도를 입력합니다. 값은 0에서 100 사이의 정수여야 합니다.
9. 값 가중치 정의 섹션에서 필드 값을 추가하고 가중치를 할당합니다.



10. 제출을 선택합니다.

예 3: 위험 계산기에 조건부 기준을 추가합니다.

조직에 여러 개의 구성 항목(CI)이 있고 그 중 일부만 외부 사용자가 액세스할 수 있다고 가정해 봅니다. 사용자는 이러한 외부 방향 CI에 대해 위험 점수 가중치를 추가할 수 있습니다.

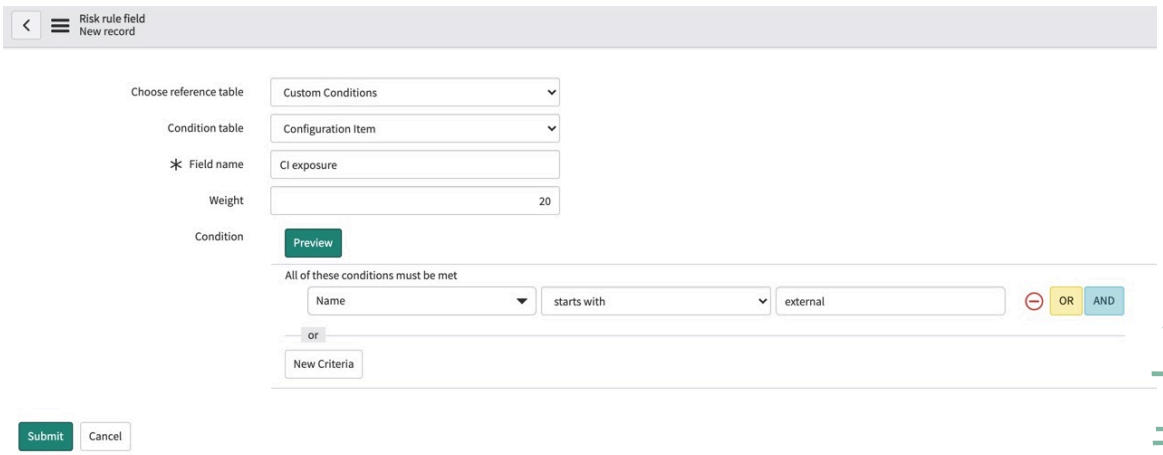
주:
이러한 CI는 이름으로 식별할 수 있습니다. 이름은 'external'로 시작합니다.

위험 규칙에 조건부 기준을 추가하려면 다음을 수행합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

1. 위험 규칙 페이지로 이동합니다.
2. 규칙을 비활성화하려면 활성 확인란의 선택을 취소합니다.
3. 위험 계산 기준에 위험 규칙 필드를 추가하려면 기준 추가를 선택합니다.
4. 참조 테이블 선택 목록에서 사용자 지정 조건을 선택합니다.
5. 조건 테이블 목록에서 구성 항목을 선택합니다.
6. 필드 이름 필드에 **CI** 노출 이름을 입력합니다.
7. 가중치 필드에 위험 규칙 내에서 이 필드의 상대적 중요도를 입력합니다. 값은 0에서 100 사이의 정수여야 합니다.
8. 조건 필드에서 이름 〉 시작 을 클릭하고 외부 값을 입력합니다.

새 위험 규칙에 대한 사용자 지정 조건



9. 제출을 선택합니다.

> **주:**
> 위험 규칙에 조건부 기준을 추가하면 성능이 저하될 수 있습니다.

관련 정보

Vulnerability Response 계산기 및 취약성 계산기 규칙

Vulnerability Response 계산기 생성

Vulnerability Response 내에서 필터링

취약성 대응 롤업 계산기

설정 도우미에서 위험 계산기를 처음 평가한 후에는 취약성 롤업 계산기를 사용하여 정정 작업 및 임포트한 취약성에 대해 누적 위험 점수를 계산하는 방법을 구성합니다.

취약성 롤업 계산기를 사용하여 정정 작업 및 임포트한 취약성에 대해 누적 위험 점수를 계산하는 방법을 구성합니다. 기본 시스템과 함께 제공되는 롤업 계산기는 다음과 같습니다.

- *Remediation Task Rollup*: 전체 취약한 항목 그룹의 전체 위험 점수를 제공하기 위해 정정 작업에 있는 모든 취약한 항목에 대한 위험 점수를 롤업합니다.
- *Patch Update Rollup*: 패치 업데이트에 대한 전체 위험 점수를 제공하기 위해 패치 업데이트가 같은 모든 취약한 항목에 대한 위험 점수를 롤업합니다.
- *Organization Risk Score Rollup*: 조직의 모든 호스트 취약한 항목, 애플리케이션 취약한 항목, 컨테이너 취약한 항목 및 구성 문제에 대한 위험 점수를 롤업하여 통합 대시보드에서 전체 조직에 대한 전체 위험 점수를 제공합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
의 취약성 대응v22.0부터 조직 점수에 대한 롤업 가중치를 구성할 수 있습니다. 또한 개별 롤업 계산기가 제거되었습니다.

- *Vulnerable Item Rollup*: 조직의 모든 호스트 취약한 항목에 대한 위험 점수를 롤업하여 통합 대시보드에서 전체 조직의 전체 위험 점수에 기여합니다.
- *Vulnerability Entry Rollup*: 취약성 항목에 대한 전체 위험 점수를 제공하기 위해 취약성 항목이 같은 모든 취약한 항목에 대한 위험 점수를 롤업합니다.
- *Rollup EPSS Scores from NVD to TPEs*: NVD 테이블에 나열된 모든 취약 항목/CVE에 대한 EPSS 점수를 기존 TPE에 롤업하여 취약성이 악용될 전체 확률을 제공합니다.
- *Remediation Effort Rollup*: 정정 작업에 대한 전체 위험 점수를 제공하기 위해 정정 작업에 있는 모든 기록에 대한 위험 점수를 롤업합니다.

다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 취약성 롤업 계산기.

롤업 계산기를 구성하여 누적 위험 점수를 설정할 때 계산된 각 값에 지정할 가중치를 지정합니다. 가중치가 높을수록 취약성 또는 정정 작업에서 롤업된 위험 점수를 결정하는 데 해당 값이 더 많이 사용됩니다.

주:
지연 포함을 선택하면 지연된 모든 취약한 항목이 정정 작업의 롤업 계산에 포함됩니다. 이 옵션을 선택하기 전에 총 계산에 미치는 영향을 이해해야 합니다.

롤업 계산기는 15분마다 예약된 작업을 *Rollup vulnerable item values to vulnerability and groups*실행하여 변경 사항을 선택하고 상세 정보 및 위험 점수를 정정 작업 및 취약성에 롤업합니다. 이러한 예약된 작업은 VI 수, 최대 위험 점수, 정정 목표 날짜 및 정정 작업 상태에 대한 누적 값도 계산합니다.

주:
취약성 항목에 대해 계산된 값에는 정정 대상 데이터가 포함되지 않습니다.

위험 점수는 다음과 같은 경우에 계산됩니다.

- 취약한 항목에 대한 위험 점수, 정정 대상, 정정 상태 또는 취약성 변경 내용입니다.
- 취약한 항목 상태가 오픈, 연기됨, 종결로 변경되거나 종결 또는 연기됨에서 변경됩니다.
- 취약한 항목이 삭제됩니다.
- 취약한 항목이 정정 작업에서 추가되거나 제거됩니다.

취약성 롤업 계산기 예: 다음과 같은 취약한 항목이 있는 정정 작업 VUL324567 생각해 보십시오.

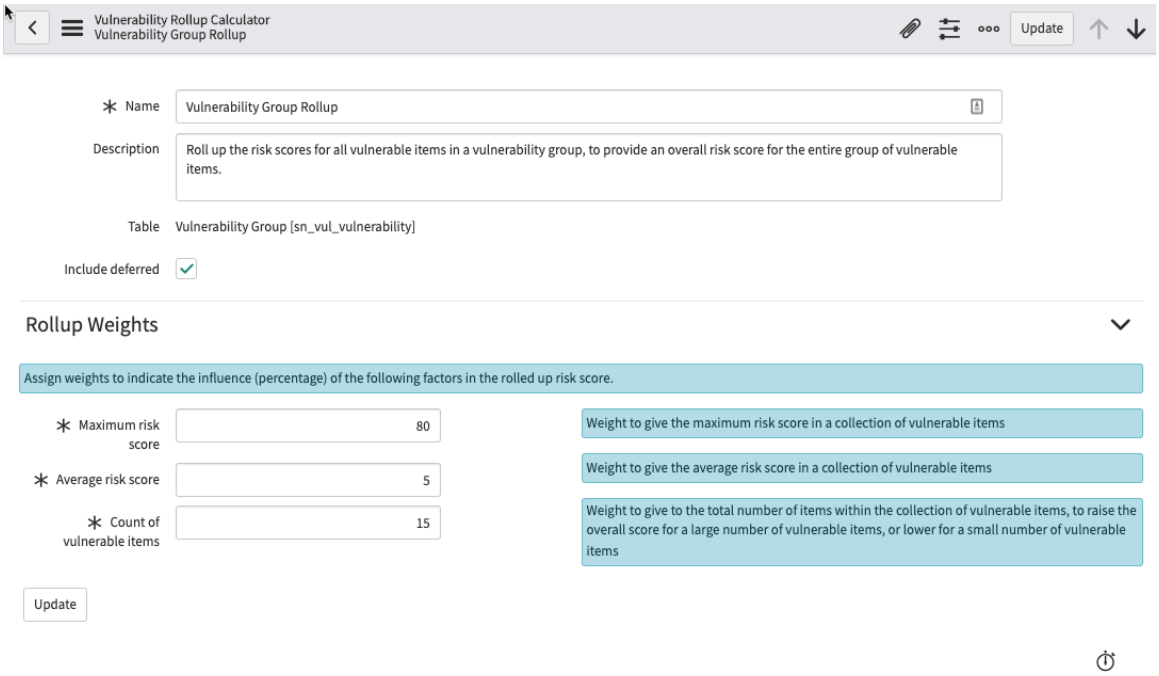
- 위험 점수가 30인 VIT1001
- 위험 점수가 40인 VIT1002
- 위험 점수가 50인 VIT1003

또한 취약성 롤업 계산기에서 다음 가중치를 고려하십시오.

- 최대 위험 점수: 80
- 평균 위험 점수: 5
- 취약한 항목 수: 15

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약성 롤업 계산기 예



취약성 롤업 계산기 예에서 정정 작업 위험 점수를 결정하는 수식은 다음과 같습니다.

(최대 위험 점수/100) * 80 + (평균 위험 점수 /100) * 5 + (계수 * 15)

요인은 다음과 같이 결정됩니다.

VI 수	요인
〈10	0.2
10-100	0.4
101-1000	0.6
1001-10000	0.8
〉10000	1

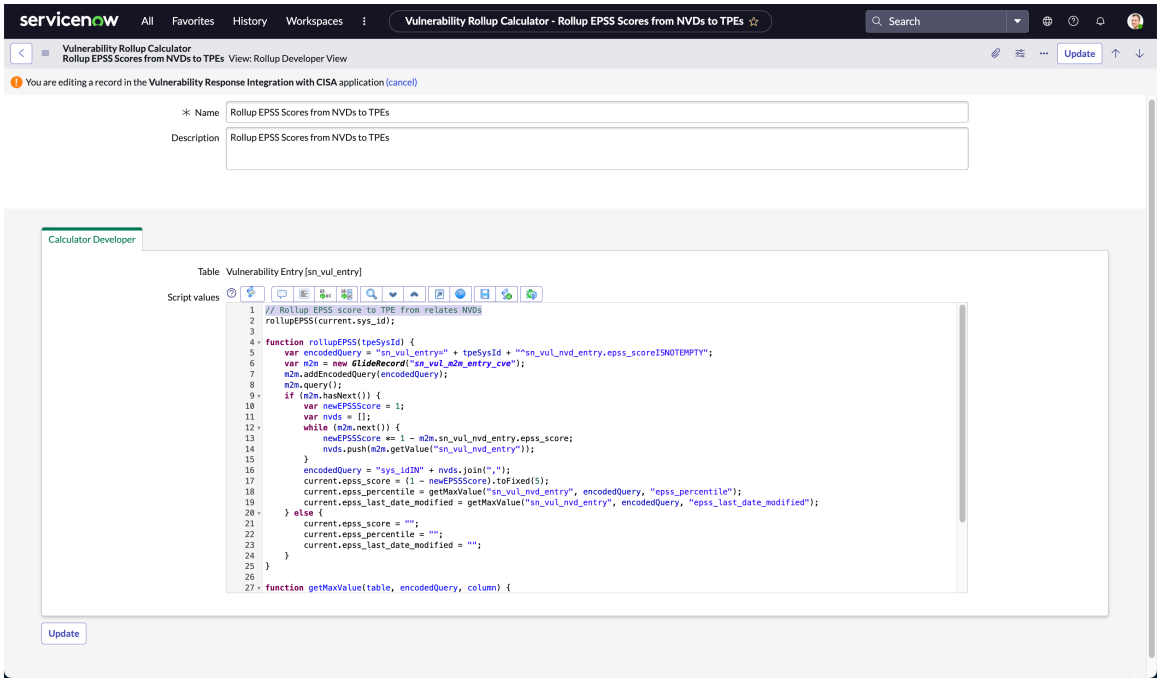
따라서 정정 작업의 경우 다음을 VUL324567.

- 평균 위험 점수는 40입니다.
- 최대 위험 점수는 50입니다.
- 50(최대 위험 점수)
- 계수는 0.2입니다.

위험 점수는 45 [(50/100) * 80 + (40/100) * 5 + 0.2 * 15 = 40 + 2 + 3 = 45〕입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

NVD에서 TPE로 **EPSS** 점수 롤업



EPSS 롤업 계산기 - 예제

예를 들어 각각 악용될 확률이 5%인 100개의 취약성이 있는 조직을 고려합니다. 네트워크 방어자가 가장 관심을 갖는 질문은 이러한 취약점 중 하나 이상이 악용될 확률은 얼마인지, 따라서 전반적인 위협은 무엇인지일 수 있습니다. 적어도 하나의 사건이 발생할 확률은 단순히 사건이 발생하지 않는 것의 보수(반대)입니다.

```
P(at least one exploited vulnerability) = 1 - P(no vulnerabilities are exploited)
```

여기서 취약성이 없을 확률은 악용되지 않는 각 취약성의 선형 곱입니다. 이 예에서 각 취약성은 악용될 확률이 5%이므로 각각 악용되지 않을 확률은 95%입니다. 그리고 100개가 있으므로 다음과 같이 작성할 수 있습니다.

```
P(at least one vuln exploited) = 1 - P(no vulns are exploited) = 1 - P(one vuln not
 exploited)^100 = 1 - 0.95^100 = 0.994
```

즉, 취약점 중 하나 이상이 악용될 확률은 99.4%입니다.

중요사항:
를 *`Rollup EPSS Scores from NVD to TPEs`*수정하려면 양식 컨텍스트 메뉴 뷰를 기본 뷰에서 롤업 개발자 뷰로 전환해야 합니다.

〔store-future: BEGIN review〕

조직 위험 점수 롤업 계산

조직 위험 점수 롤업 기능은 통합 대시보드에서 조직의 전체 위험 점수를 계산합니다. 호스트 취약한 항목, 애플리케이션 취약한 항목, 컨테이너 취약한 항목 및 구성 문제에 대한 위험 점수를 롤업합니다. 이전에는 최대 위험 점수가 VIT, AVIT, 테스트 결과 및 CVIT에 대한 점수의 평균으로 결정되었습니다. 그러나 의 버전 22 취약성 대응부터는 이제 4가지 중 가장 높은 점수를 선택하여 최대 위험 점수를 결정합니다.

최대 위험 점수를 계산하기 위해 VIT, AVIT, 테스트 결과 및 CVIT 중에서 가장 높은 점수가 선택됩니다. 예를 들어 VIT의 점수가 가장 높은 경우 해당 점수는 최대 위험 점수로 간주됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

VIT, AVIT, CVIT 및 테스트 결과의 카운트를 얻으면 카운트 방법을 사용하여 합산하고 정규화합니다. 그런 다음 결과 위험 점수에 구성에 지정된 카운트 가중치를 곱합니다.

평균 위험 점수를 계산하는 데 동일한 프로세스가 따릅니다. AVIT의 위험 점수, 구성 문제, 테스트 결과 및 기타 점수를 합산한 다음 총 개수로 나누어 평균 위험 점수를 구합니다. 마지막으로 모든 위험 점수를 합산하여 조직 위험 점수를 도출합니다.

〔End〕

정정 대상 규칙 생성 또는 편집 취약성 대응

설정 도우미에서 정정 대상 규칙을 초기에 평가한 후 취약성 관리자는 취약한 항목 수준에서 정정 대상 규칙을 설정하여 고위험 취약성을 적시에 정정할 수 있습니다. 취약한 항목에 대한 정정 날짜가 가까워지면 규칙에 지정된 사용자 또는 그룹에 알림이 전송됩니다.

시작하기 전에

필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)

가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 정정 대상 규칙.
2. 새로 만들기를 클릭합니다.
3. 양식의 필드에 적절히 입력합니다.

필드	설명
이름	규칙의 이름입니다.
목표(일수)	취약한 항목을 마지막으로 연 이후 정정해야 하는 일 수를 지정합니다.
V17.1: 대상 시작일(날짜)	목표 SLA가 계산된 시작 날짜입니다. 날짜 또는 날짜 및 시간 유형 필드만 지정할 수 있습니다. 기본값은 마지막으로 열린 날짜입니다. 이 필드의 값을 사용자 지정하려면 KB1642413 문서를 참조하십시오.
활성	기본적으로 활성 확인란이 선택되어 있으며, 이는 정정 대상 규칙이 활성 상태임을 의미합니다. 이 확인란의 선택을 취소하면 시스템에서 생성된 새로운 취약한 항목에 이 규칙이 적용되지 않습니다.
알림(기한 이전 남은 일수)	알림을 보낼 대상이 된 정정 시간 이전의 일 수입니다. 이 값을 사용하여 계산된 알림 날짜는 정정 상태 및 색상 코딩을 표시하는 데 사용됩니다. 날짜가 알림 날짜 이전인 경우 정정 상태는 "전송 중"입니다. 알림 날짜를 지나 정정 목표 날짜 이전이면 상태가 목표에 임박한 것으로 표시됩니다. 주: 이 필드를 0으로 설정하면 대상 누락 알림만 전송됩니다.
설명	정정 대상 규칙을 설명하는 텍스트입니다.
조건	조건 필터를 사용하여 취약한 항목에 규칙을 적용하기 위한 기준을 선택합니다. 성능 영향을 방지하려면 전체 생산 규모에서 조건을 테스트하십시오. 테스트를 통해 의 조건과 규모에 따라 정정 대상 평가 작업을 실행하는 데 걸리는 시간을 확인할 수 있습니다 구성 관리 데이터베이스(CMDB).

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	조건 작성기에 입력한 검색 텍스트의 대소문자 구분은 이 기록이나 양식에서 지원되지 않습니다.
알림 주: 알림 이메일에 표시된 개수에는 지연됨, 해결됨 또는 종결 됨 상태의 취약한 항목이 포함되지 않습니다.	
사용자	선택한 취약한 항목이 대상 정정 목표 시간에 근접하거나 이를 통과할 때 알릴 사람입니다.
그룹	선택한 취약한 항목이 대상 정정 목표 시간에 근접하거나 이를 통과할 때 알릴 그룹입니다.
업데이트 이력	
	규칙을 처음 생성하는 데 사용되지 않습니다. 이어서 시스템 작업 메모가 여기에 로깅됩니다.

4. 제출을 클릭합니다.
   이 규칙은 예약된 작업을 다음에 실행하는 동안 또는 ***Evaluate remediation targets*** 정정 대상 규칙 목록 뷰에서 변경 내용 적용 버튼을 사용할 때 적용됩니다. 기존 규칙이 업데이트될 때도 마찬가지입니다. 예약된 작업 및 변경 적용에 대한 자세한 내용은 다음 문서를 참조하십시오 취약성 대응 정정 대상 규칙.

설정 도우미를 사용하여 설치된 외부 공급업체 통합 구성

설치된 각 외부 공급업체 애플리케이션 배치에 작동하도록 취약성 대응을 구성합니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 설정 도우미 〉 통합 구성.
2. 스캐너 통합을 선택하여 설치된 외부 공급업체 애플리케이션 배포를 구성합니다.
3. 가 설치된 경우 취약성 대응용 솔루션 관리솔루션 통합을 선택하여 취약성 솔루션 제공자를 구성할 수 있습니다.

설치 도우미를 사용하기 위해 취약성 솔루션 관리 설치된 솔루션 통합 구성

취약성 솔루션 관리 애플리케이션을 설치한 후 설정 도우미를 사용하여 취약성 솔루션 제공자를 구성할 수 있습니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음) 또는 admin
다음 섹션을 사용하여 에 대해 취약성 대응용 솔루션 관리설치된 솔루션 통합에 대해 Setup Assistant에 제공된 지침과 프롬프트를 보완합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 시작하기 전에 솔루션 통합이 이미 설치되어 취약성 솔루션 관리 있고 원하는 솔루션 통합이 있는지 확인하십시오. 자세한 내용은 설정 도우미를 사용하여 타사 응용 프로그램 설치 취약성 대응 문서를 참조하십시오.
- 사용할 수 있는 외부 공급업체 계정 자격 증명이 있는지 확인합니다. 일부 솔루션 통합을 편집하는 데 필요합니다.
- 설치된 솔루션을 구성하기 전에 자세한 내용은 을 참조하십시오 취약성 대응용 솔루션 관리 애플리케이션 설치 .

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 설정 도우미 〉 통합 구성 〉 솔루션 통합.

   Microsoft Security Response Center 솔루션 통합 이를 구성하려면 API 키와 URL Microsoft Security Response Center 이 필요합니다.

   > 주:
   > 의 경우 MSRCAPI 키를 입력하는 것은 선택 사항입니다. 키를 얻으려면 MSRC live.com, outlook.com 또는 Microsoft.com 전자 메일 계정의 Microsoft ID, Microsoft에 등록된 전화 번호 또는 Skype 로그인이 있어야 합니다.

2. URL을 입력합니다.
   MSRC용 설정 도우미의 URL은 https://api.msrc.microsoft.com 입니다.
3. 마침을 클릭합니다.
4. 옵션: 자격 증명을 입력한 후 구성 페이지에서 지금 실행을 클릭하여 요청 시 임포트를 실행할 수 있습니다.
5. 도 Red Hat Solution Integration 사용할 수 있습니다.
   API 키는 필요하지 않습니다.
6. 설정 지원에서 오른쪽에 있는 Red Hat Solution Integration편집을 클릭합니다.
7. 에 대한 RHSI 설정 도우미의 URL이 https://access.redhat.com/hydra/rest 되어 있는지 확인
8. 옵션: 구성 페이지에서 지금 실행**(Execute Now**)을 클릭하여 요청 시 임포트를 실행할 수 있습니다.
9. Finish(마침)를 클릭한 다음 **Mark as** Complete(완료로 표시)를 클릭하여 구성을 완료합니다.
   구성을 완료하면 솔루션 통합을 위한 설정 도우미에 확인 표시가 표시됩니다.

설정 도우미를 사용하여 **MS TVM** 취약성 통합 구성

설치 도우미를 취약성 대응 사용하여 설치한 후 MS TVM(Microsoft Threat and Vulnerability Management) 애플리케이션과의 통합을 구성합니다.

시작하기 전에
Microsoft Threat and Vulnerability Management 통합과의 통합을 위해 취약성 대응 설치 도우미에 제공되는 지침 및 프롬프트 외에도 다음 작업을 수행합니다.

- 시작하기 전에 애플리케이션을 이미 설치했는지 확인하십시오. 자세한 내용은 설정 도우미를 사용하여 타사 응용 프로그램 설치 취약성 대응 문서를 참조하십시오.
- 에 대한 취약성 대응Microsoft Threat and Vulnerability Management 통합을 구성하기 전에 자세한 내용은 을 참조하십시오Microsoft Threat and Vulnerability Management 취약성 통합 준비.
- 사용 가능한 MS TVM 계정 자격 증명이 있는지 확인합니다. 이러한 자격 증명을 얻으려면 다음 문서를 참조하십시오 Microsoft MS TVM 통합을 위한 Azure 설정.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필요한 역할: 설치를 위한 시스템 관리자(admin), 취약성 관리자(sn_vul.vulnerability_admin) 또는 sn_vul.admin(사용하지 않음), 구성을 위한 통합 구성(sn_vul_msft_tvm.configure_integration)

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 설정 도우미 〉 통합 구성 〉 스캐너 통합.

   Microsoft Threat & Vulnerability Management 타일이 표시됩니다.

   MS TVM은 다중 소스 통합으로, 동일한 외부 공급업체 통합을 여러 개 배포할 수 있습니다. 원래 외부 공급업체 통합의 설정은 각각의 새 통합 설정에 대한 템플릿으로 사용됩니다.

   주:
   원래 취약성 통합을 삭제할 경우, 템플릿으로 사용할 다른 통합을 선택해야 합니다. 통합을 삭제하는 대신 사용하지 않도록 설정하는 것이 좋습니다. 비활성화된 템플릿에서 만든 통합은 기본적으로 비활성화됩니다.

   각 외부 공급업체 통합의 데이터는 고유하게 식별되며 의 취약성 대응단일 인스턴스에서 사용할 수 있습니다.

2. Microsoft Threat and Vulnerability Management 통합을 구성하려면 편집을 클릭하십시오.
3. 양식에서 필드를 채웁니다.

   계정 자격 증명 양식

필드	설명
이름	인스턴스의 이름입니다.
TVM 지역	서버 위치와 가까운 지역. API의 성능을 최적화하려면 현재 위치에서 가장 가까운 서버를 사용하십시오.
인증 유형	ID를 확인하는 방법입니다. 사용자 인증은 특정 사용자에게 특정 자산의 가시성을 제어합니다. MS TVM은 이 사용자에 대해 권리가 있는 장치 그룹을 내보냅니다. 기본값은 애플리케이션입니다.
테넌트 ID	조직의 테넌트 ID입니다.
클라이언트 ID	Microsoft Azure에서 MS TVM을 등록한 후 생성되는 클라이언트 ID입니다.
사용자 이름	전체 장치 그룹에 액세스할 수 있는 사용자입니다. 이 필드는 인증 유형에서 사용자를 선택한 경우에만 나타납니다.
암호	전체 장치 그룹에 액세스할 수 있는 사용자 이름의 암호입니다. 이 필드는 인증 유형에서 사용자를 선택한 경우에만 나타납니다.
클라이언트 비밀	MS TVM 애플리케이션을 등록한 후 생성되는 클라이언트 비밀입니다. 이 필드는 인증 유형에서 애플리케이션을 선택한 경우에만 나타납니다.

4. 변경 내용을 저장하고 첫 번째 통합 양식으로 이동하려면 다음을 클릭합니다.
   취약성 임포트 구성 양식이 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. 취약성 임포트를 활성화하거나 비활성화하고, 임포트할 취약성의 초기 시작 날짜를 결정하고, MS TVM 취약성 임포트를 실행할 시기를 예약합니다.
   모든 취약성을 임포트하려면 초기 시작 날짜를 비워 둡니다.
   a. 요청 시 데이터를 가져오려면 지금 취약성 임포트를 클릭합니다.
   b. 통합 기록을 보려면 고급 설정을 클릭합니다.
6. 변경 내용을 저장하고 첫 번째 통합 양식으로 이동하려면 다음을 클릭합니다.
   권장 사항 임포트 구성 양식이 표시됩니다.
7. 권장 사항 임포트를 활성화하거나 비활성화하고 MS TVM 취약성 임포트를 실행할 일정을 결정합니다.
   a. 요청 시 데이터를 임포트하려면 지금 권장 사항 임포트를 클릭합니다.
   b. 통합 기록을 보려면 고급 설정을 클릭합니다.
8. 변경 내용을 저장하고 첫 번째 통합 양식으로 이동하려면 다음을 클릭합니다.
   머신 임포트 구성 양식이 표시됩니다.
9. 시스템 임포트를 활성화하거나 비활성화하고, 임포트할 시스템의 초기 시작 날짜를 결정하고, MS TVM 머신 임포트를 실행할 시기를 예약합니다.
   모든 컴퓨터를 임포트하려면 초기 시작 날짜를 비워 둡니다.

   주:
   머신 태그는 기본적으로 임포트되며 MS TVM 환경에 나열된 머신을 구성하고 추적하는 데 사용됩니다.

   a. 기본 CI(구성 항목) 조회 규칙을 표시하려면 **CI** 조회 규칙을 클릭합니다. CI 조회 규칙은 에서 CI(구성 항목) ServiceNow AI Platform CMDB를 식별하기 위해 타사 소스의 머신 데이터(machine data)를 사용하는 방법을 정의합니다. 이 페이지에서 조회 규칙을 추가하거나 기본 CI 조회 규칙을 수정할 수 있습니다. 자세한 내용은 외부 공급업체 취약성 통합에서 취약성 대응 구성 항목을 식별하기 위한 CI 조회 규칙 문서를 참조하십시오.
   b. 요청 시 데이터를 임포트하려면 지금 머신 임포트를 클릭합니다.

      주:
      MS TVM에 온보딩됨 상태인 머신은 ServiceNow 애플리케이션에서 검색됩니다.

   c. 통합 기록을 보려면 고급 설정을 클릭합니다.
10. 변경 내용을 저장하고 첫 번째 통합 양식으로 이동하려면 다음을 클릭합니다.
    머신 취약성 임포트 구성 양식이 표시됩니다.
11. 다음 통합을 사용하도록 설정하고 임포트하려는 취약성의 초기 시작 날짜를 결정합니다.

머신 취약성 임포트 구성 양식

통합	설명
Microsoft TVM 머신 취약성 델타 임포트	신규, 고정, 업데이트된 취약성을 포함하여 전체 취약성 임포트 중에 업데이트된 취약성을 검색합니다. 지난 14일 동안의 델타 데이터만 임포트할 수 있습니다.
Microsoft TVM 머신 취약성 전체 임포트	열려 있는 모든 취약성을 검색합니다. 데이터 임포트 양이 많기 때문에 매주 실행되도록 예약할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

머신 취약성 통합 전에 머신 임포트를 실행합니다. 그렇지 않으면 누락된 머신에 대한 VI가 생성되지 않습니다.

12. 변경 사항을 저장하고 설정 지원에서 구성을 완료하려면 마침을 클릭합니다.

다음에 수행할 작업
클래식 환경에서 취약한 항목 그룹화를 활성화하려면 다음으로 이동합니다. 〉 취약성 대응 〉 관리 〉 정정 작업 규칙 〉 **Microsoft TVM** 권장 사항.

표시되는 양식에서 활성 옵션을 선택하여 활성화합니다. 또는 새로 만들기를 선택하여 새 규칙을 만듭니다.

자세한 내용은 취약성 대응 정정 작업 및 정정 작업 규칙 개요 문서를 참조하십시오.

Qualys Vulnerability Integration 설정 도우미 사용 구성

애플리케이션을 설치한 Qualys 후 설정 도우미를 사용하여 구성합니다.

시작하기 전에
다음 섹션을 사용하여 설정 도우미 Qualys Vulnerability Integration에서 제공하는 지침과 프롬프트를 보완하여 .

- 시작하기 전에 애플리케이션을 이미 설치했는지 확인하십시오. 자세한 내용은 설정 도우미를 사용하여 타사 응용 프로그램 설치 취약성 대응 문서를 참조하십시오.
- 를 구성하기 전에 자세한 내용은 를 Qualys Vulnerability Integration참조하십시오준비 중 Qualys Vulnerability Integration.
- 사용할 수 있는 외부 공급업체 계정 자격 증명이 있는지 확인합니다. 일부 외부 공급업체 애플리케이션을 편집해야 합니다.

필요한 역할: 설치를 위한 시스템 관리자(admin), 구성을 위한 취약성 관리자 (sn_vul.vulnerability_admin) 또는 sn_vul.admin(사용하지 않음).

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 설정 도우미 〉 통합 구성 〉 스캐너 통합.
설치된 통합이 표시됩니다.

2. 구성하려는 항목의 Qualys Vulnerability Integration 오른쪽에 있는 편집을 클릭합니다.

3. 계정 자격 증명 양식에서 자격 Qualys Cloud Platform 증명을 입력합니다.
구성하려면 자격 증명이 필요합니다.

4. 구성을 계속할 때 다음 참고 사항을 가이드로 사용합니다.

- 고급 설정 링크는 통합 기록을 가리킵니다Qualys. 임포트한 취약성 데이터를 필터링하는 데 도움이 되도록 예약된 쿼리에 대해 제품에서 지원하는 Qualys 매개변수를 추가할 수 있습니다. 자세한 내용은 을 참조하십시오 임포트에 대한 Qualys 추가 필터 매개변수 설정 .
- 이미 구성한 버전을 Qualys Vulnerability Integration 사용하여 이전 버전에서 취약성 대응 업그레이드한 경우 구성 설정이 유지된 해당 버전을 계속 사용할 수 있습니다.

  에 대한 Qualys Vulnerability Integration호스트 탐지 구성의 설정 임포트 아래에는 고정된 Qualys 취약성 탐지 기록을 볼 수 있는 옵션이 있습니다. 이 옵션을 사용하면 고정 상태(상태=고정)의 탐지 기록에서 취약한 항목을 생성할 수 있습니다. 취약한 항목 탐지에 대한 자세한 내용은 다음 문서를 참조하십시오 취약성 대응 외부 공급업체 통합에서 취약한 항목 탐지.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

호스트 탐지 구성 페이지에서 네트워크 파티션별 조회 확인란을 활성화하여 IP 주소 조회에 네트워크 파티션 식별자를 포함할 수 있습니다. 자세한 내용은 의 네트워크 파티션 식별자로 구성 항목을 업데이트합니다. Qualys Vulnerability Integration 문서를 참조하십시오.

호스트 목록 통합의 Qualys 일부로 모든 호스트 태그가 임포트됩니다. 호스트 태그는 할당 및 정정 작업 규칙의 필터링에 취약성 대응 주로 사용됩니다. 검색된 항목 양식에 표시됩니다.

주:
호스트 목록 통합은 Qualys 할당 또는 정정 작업 규칙을 취약성 대응 생성하기 전에 실행되어야 모든 태그가 규칙에 포함될 수 있고 취약한 항목을 임포트 및 그룹화할 수 있습니다.

Qualys 자산 태그는 호스트 태그 모듈의 Qualys Vulnerability Integration.

- Qualys Vulnerability Integration 다중 소스를 지원합니다. 동일한 외부 공급업체 통합을 여러 개 배포할 수 있습니다. 다른 통합을 추가하려면 스캐너 통합 페이지에서 통합 추가를 클릭합니다.

  원래 외부 공급업체 통합의 설정은 각각의 새 통합 설정에 대한 템플릿으로 사용됩니다.

  주:
  원래 취약성 통합을 삭제할 경우, 템플릿으로 사용할 다른 통합을 선택해야 합니다. 통합을 삭제하는 대신 사용하지 않도록 설정하는 것이 좋습니다. 비활성화된 템플릿에서 만든 통합은 기본적으로 비활성화됩니다.

  각 외부 공급업체 통합의 데이터는 고유하게 식별되며 의 취약성 대응단일 인스턴스에서 사용할 수 있습니다.

- 구성 페이지에서 지금 실행**(Execute Now**)을 클릭하여 요청 시 임포트를 실행할 수 있습니다.

5. Finish(마침)를 클릭하여 설정 도우미에서 구성을 완료합니다.

설정 도우미를 사용하여 **Tenable** 취약성 통합 구성

애플리케이션을 설치한 Vulnerability Response Integration with Tenable 후 설정 도우미를 사용하여 구성합니다.

시작하기 전에

다음 섹션을 사용하여 통합을 위해 설정 도우미에 제공된 지침과 프롬프트를 보완합니다 Vulnerability Response Integration with Tenable .

- 시작하기 전에 애플리케이션을 이미 설치했는지 확인하십시오. 자세한 내용은 설정 도우미를 사용하여 타사 응용 프로그램 설치 취약성 대응 문서를 참조하십시오.
- 를 구성하기 전에 자세한 내용은 를 Tenable for Vulnerability Response참조하십시오Tenable 취약성 통합 준비.
- 사용할 수 있는 외부 공급업체 계정 자격 증명이 있는지 확인합니다. 일부 외부 공급업체 애플리케이션을 편집해야 합니다.

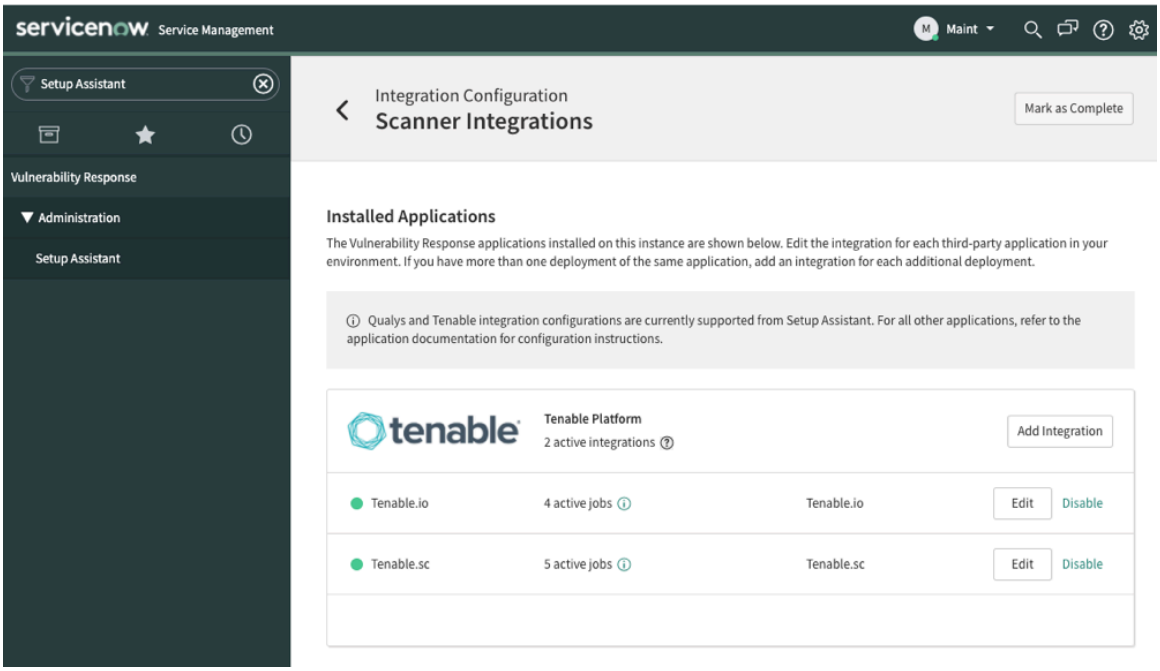
필요한 역할: 설치를 위한 시스템 관리자(admin), 취약성 관리자(sn_vul.vulnerability_admin) 또는 sn_vul.admin(사용하지 않음), 구성을 위한 통합 구성(sn_vul_tenable.configure_integrations).

프로시저

1. 표시되지 않으면 모두 〉 취약성 대응 〉 관리 〉 설정 도우미 〉 통합 구성 〉 스캐너 통합.

, Tenable.ioTenable.sc및 Tenable.cs 통합이 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



Tenable은 다중 소스 통합이며, 동일한 외부 공급업체 통합을 여러 개 배포할 수 있습니다. 원래 외부 공급업체 통합의 설정은 각각의 새 통합 설정에 대한 템플릿으로 사용됩니다.

> **주:**
> 원래 취약성 통합을 삭제할 경우, 템플릿으로 사용할 다른 통합을 선택해야 합니다. 통합을 삭제하는 대신 사용하지 않도록 설정하는 것이 좋습니다. 비활성화된 템플릿에서 만든 통합은 기본적으로 비활성화됩니다.

각 외부 공급업체 통합의 데이터는 고유하게 식별되며 의 취약성 대응단일 인스턴스에서 사용할 수 있습니다.

2. 구성하려는 Tenable 통합의 오른쪽에서 편집을 선택합니다.

3. 계정 자격 증명 양식의 필드에 내용을 입력합니다.

- Tenable.io 권한 속성이 64 이상인 관리자 액세스 권한이 필요합니다.

  > **주:**
  > 의 Vulnerability Response Integration with Tenablev3.8부터는 더 이상 관리자 Tenable.io 권한이 필요하지 않습니다. 권한 속성이 16인 기본 사용자도 제품에 액세스할 수 있습니다.

- Tenable.sc 보안 분석가 또는 관리자 액세스 권한이 필요합니다.
- Tenable.cs 에는 Tenable CS 플랫폼 토큰 생성에 접근할 수 있는 토큰이 필요합니다.

a. Tenable 제품을 선택합니다.

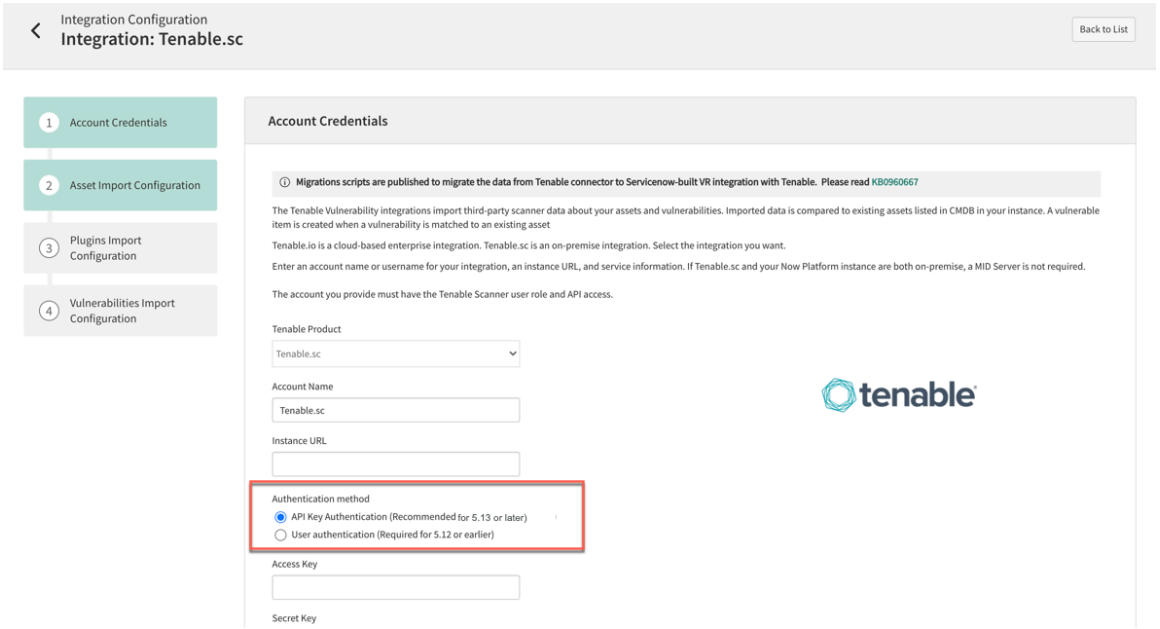
b. Tenable 계정 이름을 입력합니다.

c. 인스턴스 URL 필드에 Tenable 플랫폼의 URL을 입력합니다.

d. 인증 방법을 선택합니다(의 Tenable.cs경우 f 단계로 진행).

버전에 Tenable.sc따라 인증에 대한 두 가지 옵션이 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



i. 의 Tenable.scv5.13부터 **API** 키 인증을 선택합니다. Tenable 액세스 및 비밀 키를 입력합니다.

ii. v5.13 이전에는 인스턴스에서 사용자 인증이 지원 ServiceNow AI Platform# 되며 인증이 필요합니다. ServiceNow AI Platform 사용자 이름과 암호를 입력합니다.

에 대해서는 Tenable.scAPI 키 인증만 지원됩니다. Tenable 액세스 및 비밀 키를 입력합니다.

e. 옵션: MID 서버를 선택합니다.

(Optional) ServiceNow AI Platform 인스턴스와 Tenable.sc 애플리케이션이 같은 위치에 있지 않은 경우 목록에서 구성된 MID 서버를 선택합니다. 자세한 내용은 MID 서버를 참조하십시오.

- 의 v15.0 취약성 대응 및 v3.0Tenable Vulnerability Integration부터 에 설명된 Tenable 취약성 통합에 대한 데이터 검색 설정대로 매개변수를 활성화할 *Async_request* 수 있는 옵션이 있습니다. 동기 호출을 하려면 Tenable을 사용한 일부 구성이 필요합니다. Tenable 제품에 도움을 요청하십시오. 이 매개변수가 활성화되면 모든 Tenable.sc 통합에 적용할 수 있으며 30초의 시간 제한이 있습니다. 수정 스크립트를 보려면 다음으로 이동하십시오. 시스템 정의 〉 스크립트 수정.

- (Optional) 기존 고객의 경우 비동기 호출을 사용하는 경우 수정 스크립트를 사용할 수 있습니다.

ServiceNow AI Platform 인스턴스와 Tenable.sc 애플리케이션이 모두 사내인 경우 (필수는 아니지만) 목록에서 구성된 MID 서버를 선택할 수 있습니다.

주:
사용 MID 서버 여부에 관계없이 5분 후에 통합이 시간 초과되고 서버의 응답이 없으면 메시지가 표시됩니다.

시간 초과 오류가 발생하면 설정 도우미에서 올바른 자격 증명과 URL을 입력했는지 확인합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

f. API 토큰을 입력합니다.

> 주:
> 설정 도우미에서 잘못된 자격 증명에 대한 오류가 발생하면 올바른 자격 증명과 URL을 입력했는지 확인하십시오.

4. 다음을 선택하여 변경 내용을 저장하고 첫 번째 통합 양식으로 진행합니다.
및 Tenable.sc의 경우 Tenable.io 자산 임포트 구성 양식이 표시됩니다. 의 Tenable.cs경우 컨테이너 자산 임포트 구성 양식이 표시됩니다.

> 주:
> 컨테이너 자산 임포트 구성 양식은 설치된 경우에만 컨테이너 취약성 대응 표시됩니다.

5. 이 양식에서 자산 임포트 통합을 활성화 또는 비활성화하고, 임포트할 자산의 최초 시작 날짜를 결정하고, Tenable 자산 임포트를 실행할 시기를 예약합니다.

Tenable.io에 대해

- 자산 통합을 준수 결과 및 준수 결과 백필 통합과 함께 Tenable.io 사용하면 자산에 대한 보안 구성 평가 데이터를 애플리케이션으로 임포트할 수 있습니다 구성 준수 .
- 이 보안 구성 평가 데이터를 임포트하고 보려면 인스턴스에 애플리케이션의 버전 12.2 구성 준수 가 필요합니다.

  이러한 통합으로 임포트되는 데이터와 게시된 위치에 대한 자세한 내용은 을 참조하십시오 구성 준수 임포트된 데이터 .
- Tenable.io 규정 준수 결과 및 규정 준수 결과 백필 통합은 기본적으로 활성화되어 있지 않습니다. 이러한 일정을 활성화하는 경우 제공된 기본 일정 설정을 사용하는 것이 좋습니다. 에 Tenable Vulnerability Integration대한 통합을 찾고 활성화하는 방법은 아래 나열된 단계를 참조하십시오.
- 인스턴스에서 제품의 취약한 항목에 대한 요청 시 재스캔을 Tenable.io 시작할 수 있습니다. Tenable.io 재스캔을 시작하기 전에 템플릿 통합과 Tenable.io 스캔 자격 증명 통합을 활성화해야 합니다.

기본적으로 이러한 통합은 비활성화되어 있습니다. 에 대한 Tenable.io자격 증명을 입력하면 모든 Tenable.io 통합이 자동으로 활성화됩니다. 통합을 수동으로 활성화하거나 비활성화하려면 다음을 수행합니다.

a. 다음으로 이동 **Tenable** 취약성 통합 〉 관리 〉 통합.

b. 표시되는 목록에서 원하는 통합 기록을 찾습니다 Tenable.io .

c. 통합을 활성화하려면 각 기록을 열고 활성 확인란을 선택합니다.

d. 업데이트를 선택하여 변경 내용을 저장합니다.

e. 설정 도우미로 돌아가 에 취약성 대응대한 Tenable Vulnerability Integration 구성을 계속합니다.

- Tenable.io 통합의 경우 자산 태그 임포트를 활성화 및 비활성화하는 옵션도 있습니다. 자산 태그는 기본적으로 임포트되며, 환경에서 CMDB Tenable.io 에 나열된 자산을 구성하고 추적하는 데 사용됩니다.
- AND 제품 모두에 Tenable.io 대해 네트워크 파티션별 조회에서 네트워크 파티션별 조회 사용을 선택하면 동일한 IP 주소를 가진 자산에 대해 IRE(식별 및 조정 엔진)를 사용하여 개별 CI를 만들 수 있습니다.Tenable.sc 자세한 내용은 AND 식별 및 조정 엔진을 사용하기 위한 취약성 대응 CI 생성 문서를 참조하십시오의 네트워크 파티션 식별자로 구성 항목을 업데이트합니다. Tenable Vulnerability Integration.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 화면 상단의 자산 임포트 링크 옆에 있는 Tenable.io 및 Tenable.sc 위해 **CI** 조회 규칙 링크를 선택하여 기본 CI(구성 항목) 조회 규칙을 표시합니다. CI 조회 규칙은 타사 소스의 자산 데이터를 사용하여 CMDB의 CI(구성 항목)를 ServiceNow AI Platform 식별하는 방법을 정의합니다. 이 페이지에서 조회 규칙을 추가하거나 기본 CI 조회 규칙을 수정할 수 있습니다. 자세한 내용은 외부 공급업체 취약성 통합에서 취약성 대응 구성 항목을 식별하기 위한 CI 조회 규칙 문서를 참조하십시오.
- 지금 자산 임포트 를 선택하여 요청 시 데이터를 임포트합니다.
- 고급 설정 링크는 자산 통합 기록을 가리킵니다. v3.3부터 예약된 쿼리에 대해 제품에서 Tenable.io 지원하는 매개변수를 추가하여 자산과 수정된 취약성 통합과 미해결 취약성 통합을 사용하여 Tenable.io 임포트하는 취약성 데이터를 필터링할 수 있습니다. 자세한 내용은 을 참조하십시오 임포트에 대한 Tenable.io 추가 필터 매개변수 설정 .

6. 다음을 선택하여 변경 내용을 저장하고 다음 양식으로 진행합니다.

> **주:**
> 의 경우 Tenable.io 및 Tenable.sc. Tenable.cs 호스트 취약성 임포트 구성 양식이 표시되면 9단계부터 계속하여 추가 Tenable CS 구성을 수행합니다.

플러그인 임포트 구성 양식이 표시됩니다.

7. 플러그인 임포트 구성 양식에서 플러그인(타사 취약성 항목) 임포트를 활성화하거나 비활성화하고, 임포트할 플러그인의 최초 시작 날짜를 결정하고, Tenable 플러그인 임포트를 실행할 시기를 예약합니다.

모든 플러그인, 취약성 및 자산을 임포트하려면 초기 시작 날짜를 비워 둡니다.

- 지금 플러그인 임포트를 선택하여 요청 시 데이터를 임포트합니다.
- 고급 설정 링크는 플러그인 통합 기록을 가리킵니다.
- 취약성 임포트의 경우 수집하려는 취약성에 대한 Tenable.io 심각도 수준을 예약하고 설정할 수 있습니다. 특정 날짜로 시작하여 생성되거나 업데이트된 취약성만 임포트되도록 날짜를 결정합니다.
- 통합의 Tenable.sc 경우 특정 날짜로 시작하여 생성되거나 업데이트된 취약성만 임포트되도록 쿼리 필터와 날짜를 결정할 수 있습니다.

8. 다음을 선택하여 변경 내용을 저장하고 다음 양식으로 진행합니다.
취약성 임포트 구성 양식이 표시됩니다. 통합을 사용하거나 사용하지 않도록 설정하고 임포트하려는 취약성의 초기 시작 날짜를 결정합니다.

Tenable.io 제품의 경우:

- 심각도 필터를 사용하여 선택한 조건과 일치하는 취약성 및 관련 VI만 임포트합니다.
- 자산 통합 `Last Scan Time` 의 Tenable.io 경우 취약성이 있는 자산에 대해서만 임포트되고 업데이트됩니다.
- 수정된 취약성 옵션을 활성화하여 고정 탐지 기록에 대한 VI를 봅니다. 설정 도우미에서 이 플래그를 활성화하면 인스턴스에 존재하지 않는 고정 상태의 감지에 대해 새 VI가 생성됩니다. 이 기능을 사용하면 수집 성능에 부정적인 영향을 줄 수 있습니다.
- 필터 임포트 옆에 있는 고급 설정 링크는 취약성 통합 기록으로 연결됩니다.
- 상단의 일정 임포트 링크를 선택하여 취약성이 수집되는 빈도를 구성하고 통합을 활성화합니다.

Tenable.sc 제품의 경우:

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- Tenable 플랫폼에서 Tenable 쿼리로 설정된 조건 필터와 일치하는 취약성 및 관련 VI만 임포트합니다. Tenable 쿼리에 대한 자세한 내용은 Tenable 설명서를 참조하십시오.

  설정 도우미에서 선택하는 Tenable 쿼리 필터는 자산 통합에도 Tenable.sc 적용됩니다. 쿼리 필터의 조건과 일치하는 취약성이 있는 자산만 임포트됩니다.

- 수정된 취약성 옵션을 활성화하여 고정 탐지 기록에 대한 VI를 봅니다. 설정 도우미에서 이 플래그가 활성화되면 인스턴스에 존재하지 않는 고정 상태의 탐지에 대해 새 VI가 생성됩니다. 이 기능이 활성화되면 수집 성능에 부정적인 영향을 줄 수 있습니다.
- IP 주소 조회에 네트워크 파티션 식별자를 포함하려면 네트워크 파티션별 조회 사용 의 확인란 네트워크 파티션별 조회 절. 자세한 내용은 의 네트워크 파티션 식별자로 구성 항목을 업데이트합니다. Tenable Vulnerability Integration 문서를 참조하십시오.
- 상단에서 일정 임포트를 선택하여 취약성 수집 빈도를 구성하고 통합을 활성화합니다.
- 필터 임포트 옆에 있는 고급 설정 링크는 취약성 통합 기록으로 연결됩니다.
- ServiceNow# Tenable.sc 취약성 통합(Tenable.sc미해결 및 수정된 취약성 통합)을 구성할 때 인스턴스의 설정 도우미 내에서 검사 자격 증명 통합이 자동으로 활성화(##)됩니다Tenable.sc.

  이 통합은 인스턴스의 제품에서 Tenable.sc 스캐너 자격 증명을 임포트하고 업데이트합니다. 이 통합은 매주 실행되어 Tenable 자격 증명 데이터를 임포트하고 안전하게 저장합니다. 다음으로 이동 **Tenable** 취약성 통합 〉 통합 〉 **Tenable.sc** 스캔 자격 증명 통합 스캔 자격 증명 통합에 대한 자세한 내용을 보려면

9. 컨테이너 자산 임포트 구성 단계에서 다음을 선택합니다.
호스트 취약성 임포트 구성 양식이 표시됩니다. 통합을 사용하거나 사용하지 않도록 설정합니다.

- 심각도 필터를 사용하여 선택한 조건과 일치하는 취약성 및 관련 VI만 임포트합니다.
- 필터 임포트 옆에 있는 고급 설정 링크는 취약성 통합 기록으로 연결됩니다.
- 상단의 일정 임포트 링크를 선택하여 취약성이 수집되는 빈도를 구성하고 통합을 활성화합니다.
- 화면 상단에서 일정 임포트 링크 옆에 있는 CI 조회 규칙 링크를 선택하여 기본 CI(구성 항목) 조회 규칙을 표시합니다. CI 조회 규칙은 타사 소스의 자산 데이터를 사용하여 CMDB의 CI(구성 항목)를 ServiceNow AI Platform 식별하는 방법을 정의합니다. 이 페이지에서 조회 규칙을 추가하거나 기본 CI 조회 규칙을 수정할 수 있습니다. 자세한 내용은 취약성 대응 외부 공급업체 취약성 통합에서 구성 항목을 식별하기 위한 CI 조회 규칙을 참조하십시오.

10. 주:
이 단계는 제품에만 적용됩니다 Tenable.cs .

다음을 선택하여 변경 내용을 저장하고 다음 양식으로 진행합니다.

- 심각도 필터를 사용하여 선택한 조건과 일치하는 컨테이너 취약성 및 관련 CVI만 임포트합니다.
- 필터 임포트 옆에 있는 고급 설정 링크는 취약성 통합 기록으로 연결됩니다.
- 상단의 일정 임포트 링크를 선택하여 취약성이 수집되는 빈도를 구성하고 통합을 활성화합니다.
- 컨테이너 취약성 임포트 구성은 컨테이너 취약성 대응이 설치된 경우에만 표시됩니다.
컨테이너 취약점 임포트 구성 양식이 표시됩니다. 통합을 사용하거나 사용하지 않도록 설정합니다.

11. 마침을 선택하여 변경 사항을 저장하고 설정 도우미에서 구성을 완료합니다.

다음에 수행할 작업
(선택 사항) 다음으로 이동합니다. 모두 〉 취약성 대응 〉 관리 〉 취약성 계산기 〉 기본 위험 계산기 〉 **Tenable** 위험 규칙 Tenable 위험 규칙을 활성화합니다.

표시되는 취약성 계산기 규칙 양식에서 활성 확인란을 선택하여 사용하도록 설정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Tenable 위험 규칙은 의 취약성 계산기취약성 대응에 기본 위험 계산기의 일부로 애플리케이션과 함께 Vulnerability Response Integration with Tenable 설치됩니다. VPR(취약성 우선순위 등급)은 임포트되어 새 기본 위험 계산기와 함께 사용되는 Tenable 제품의 속성입니다. 이 위험 규칙은 기본적으로 비활성화되어 있습니다. Tenable 위험 계산기 규칙을 사용하면 임포트한 VPR 값이 취약한 항목의 위험 점수를 계산하는 데 사용됩니다. 이 위험 계산기의 기본 가중치 분포는 VPR = 70%, 자산=15%, 비즈니스 중요도=15%입니다. 이 Tenable 위험 계산기 규칙을 사용하도록 설정하면 데이터 수집 성능에 영향을 줄 수 있습니다.

취약성 대응 계산기 및 취약성 계산기 규칙 문서를 참조하십시오.

취약성 솔루션 제공자 설정

검사 목록에 따라 취약성 솔루션 제공자를 설정한 다음 설정 도우미에서 제공자를 구성합니다.

솔루션 통합 검사 목록 준비

설정 도우미를 사용하여 CVRF(공통 취약성 보고 프레임워크) 또는 CSAF(공통 보안 자문 프레임워크) 데이터 형식을 지원하는 모든 벤더에 대한 솔루션 인텔리전스 통합 구현을 준비합니다.

CVRF(Common Vulnerability Reporting Framework) 솔루션 통합 준비

설정 도우미를 사용하여 CVRF(공통 취약성 보고 프레임워크) 데이터 형식을 지원하는 모든 벤더에 대한 솔루션 인텔리전스 통합 구현을 준비합니다.

시작하기 전에

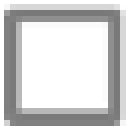
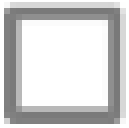
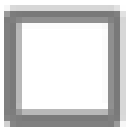
솔루션을 제공하는 벤더와 통합하려면 다음 검사 목록의 작업을 수행해야 합니다. 애플리케이션을 설치하기 전에 검사 목록을 인쇄하고 나열된 항목이 완료되었는지 확인할 수 있습니다.

통합 준비 검사 목록

작업	설명
종속 애플리케이션 ☐	에서 다음 애플리케이션이 설치되는지 확인합니다.ServiceNow Store • 취약성 솔루션 관리: 설치에 취약성 솔루션 관리대한 자세한 내용은 을 참조하십시오 설정 도우미를 사용하여 타사 응용 프로그램 설치 취약성 대응취약성 대응용 솔루션 관리 애플리케이션 설치. • 취약성 대응: 애플리케이션 설치 및 활성화에 취약성 대응 대한 자세한 내용은 을 참조하십시오 취약성 대응 설치. 이 통합에는 버전 16.1 취약성 대응 이상이 필요합니다.
외부 공급업체 계정 자격 증명 ☐	사용할 수 있는 외부 공급업체 계정 자격 증명이 있는지 확인합니다. 일부 솔루션 통합을 편집하는 데 필요합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

통합 준비 검사 목록

작업	설명
벤더 인증 	API를 사용하여 솔루션을 임포트할 수 있도록 벤더를 인증했는지 확인합니다. 벤더를 인증하는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 연결 및 자격 증명 별칭 구성. API 기반 벤더를 구성하지 않으려면 이 단계를 건너뛸 수 있습니다.
플로우 및 플로우 작업의 커스터마이제이션 	Cisco 이외의 API 기반 벤더를 구성하려면 자문의 응답에서 고유 키 및 CVRF URL을 추출하기 위한 플로우 및 플로우 작업을 사용자 정의해야 합니다. 주: CVRF URL을 게시하는 것은 벤더 간에 표준이 아닙니다. Cisco 이외의 벤더에 대한 플로우를 사용자 지정하려면 문서를 참조하십시오 Cisco 이외의 공통 취약성 보고 프레임워크 벤더 구성. Cisco 이외의 벤더를 구성하지 않으려면 이 단계를 건너뛸 수 있습니다. 기본적으로 Cisco의 플로우는 애플리케이션과 함께 제공되었습니다.
역할 	통합을 관리할 수 있는 관리자 그룹 또는 사용자가 있는지 확인합니다. 할당되지 않은 경우 관리자는 취약성 관리자(sn_vul.vulnerability_admin) 및 기타 역할을 할당합니다.

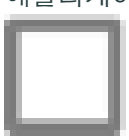
CSAF(Common Security Advisory Framework) 솔루션 통합 준비

설정 도우미를 사용하여 CSAF(공통 보안 자문 프레임워크) 데이터 형식을 지원하는 모든 벤더에 대한 솔루션 인텔리전스 통합 구현을 준비합니다.

시작하기 전에

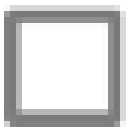
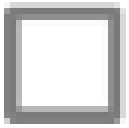
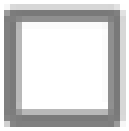
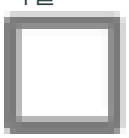
솔루션을 제공하는 벤더와 통합하려면 다음 검사 목록의 작업을 수행해야 합니다. 애플리케이션을 설치하기 전에 검사 목록을 인쇄하고 나열된 항목이 완료되었는지 확인할 수 있습니다.

통합 준비 검사 목록

작업	설명
종속 애플리케이션 	에서 다음 애플리케이션이 설치되는지 확인합니다.ServiceNow Store • 취약성 솔루션 관리: 설치에 취약성 솔루션 관리대한 자세한 내용은 을 참조하십시오 설정 도우미를 사용하여 타사 응용 프로그램 설치 취약성 대응취약성 대응용 솔루션 관리 애플리케이션 설치. • 취약성 대응: 애플리케이션 설치 및 활성화에 취약성 대응 대한 자세한 내용은 을 참조하십시오 취약성 대응 설치. 이 통합에는 버전 16.1 취약성 대응 이상이 필요합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

통합 준비 검사 목록

작업	설명
외부 공급업체 계정 자격 증명 	사용할 수 있는 외부 공급업체 계정 자격 증명이 있는지 확인합니다. 일부 솔루션 통합을 편집하는 데 필요합니다.
벤더 인증 	API를 사용하여 솔루션을 임포트할 수 있도록 벤더를 인증했는지 확인합니다. 벤더를 인증하는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 CSAF(일반 보안 자문 프레임워크)에 대한 연결 및 자격 증명 별칭 구성. API 기반 벤더를 구성하지 않으려면 이 단계를 건너뛸 수 있습니다.
플로우 및 플로우 작업의 커스터마이제이션 	이외의 API 기반 벤더 Red Hat를 구성하려면 권고의 응답에서 고유 키 및 CSAF URL을 추출하기 위한 플로우 및 플로우 작업을 사용자 지정해야 합니다. 주: CSAF URL 게시는 벤더 간에 표준이 아닙니다. 이외의 벤더 Red Hat에 대한 플로우를 사용자 지정하려면 문서를 참조하십시오 공통 보안 자문 프레임워크 구성 이외의 벤더 Red Hat. 이외의 벤더 Red Hat를 구성하지 않으려면 이 단계를 건너뛸 수 있습니다. 기본적으로 에 대한 Red Hat 플로우는 애플리케이션과 함께 제공되었습니다.
역할 	통합을 관리할 수 있는 관리자 그룹 또는 사용자가 있는지 확인합니다. 할당되지 않은 경우 관리자는 취약성 관리자(sn_vul.vulnerability_admin) 및 기타 역할을 할당합니다.

취약성 솔루션 제공자 구성

취약성 솔루션 관리 애플리케이션을 설치한 후 설정 도우미를 사용하여 취약성 솔루션 제공자를 구성합니다.

시작하기 전에

필요한 역할: sn_vul.vulnerability_admin, sn_vul.admin(사용하지 않음) 또는 admin.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 설정 도우미 〉 통합 구성.
2. 솔루션 통합을 클릭합니다.
3. 설치된 솔루션 섹션에서 URL, API 또는 임포트를 사용하여 데이터를 가져옵니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- URL 또는 API를 사용하여 데이터를 가져오려면 통합 추가를 클릭합니다.
- CVRF(Common Vulnerability Response Framework) 또는 CSAF(Common Security Advisory Framework) 파일을 업로드하여 데이터를 가져오려면 파일 임포트를 클릭하십시오.

다음에 수행할 작업
데이터를 임포트 하려는 형식에 따라 다음 작업 중 하나를 수행할 수 있습니다.

- CVRF의 경우:
  - CVRF 파일을 임포트하려면 문서를 참조하십시오 파일 임포트를 통해 Common Vulnerability Reporting Framework 데이터 임포트.
  - API를 사용하여 CVRF 데이터를 임포트하려면 문서를 CVRF URL을 통해 CVRF(Common Vulnerability Reporting Framework) 데이터 임포트참조하십시오.
  - 권고를 통해 CVRF 데이터를 임포트하려면 문서를 권고에서 일반 취약성 보고 프레임워크 데이터 임포트참조하십시오.
- CSAF의 경우:
  - CSAF 파일을 임포트하려면 문서를 참조하십시오 파일 임포트를 통해 일반 보안 자문 프레임워크 데이터 임포트.
  - API를 사용하여 CSAF 데이터를 임포트하려면 단원을 참조하십시오 CSAF URL을 통해 일반 보안 자문 프레임워크(CSAF) 데이터 임포트.
  - 권고를 통해 CSAF 데이터를 임포트하려면 문서를 참조하십시오 권고에서 일반 보안 자문 프레임워크 데이터 임포트.
-

공통 취약성 보고 프레임워크**(CVRF)**

CVRF(Common Vulnerability Reporting Framework)는 취약성 보고서 문서 작성을 위한 표준화된 프레임워크를 제공합니다. 여러 조직의 다양한 이해 관계자 간에 중요한 보안 관련 정보의 공유를 간소화하는 XML 기반 언어입니다. CVRF 형식을 활용하여 정보 교환 및 처리를 신속하게 처리할 수 있습니다.

파일 임포트를 통해 **Common Vulnerability Reporting Framework** 데이터 임포트

CVRF 파일을 임포트하여 CVRF 형식으로 데이터를 봅니다. 임포트는 일회성 활동입니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음) 또는 admin.

이 태스크 정보
임포트되면 큐 항목이 첨부 파일과 함께 작성되고 항목이 처리될 때 구문 분석됩니다. 그러면 해당 테이블에 데이터가 채워집니다. CVRF 데이터를 구문 분석하기 전에 구성에 따라 스캐너 매핑 레코드가 생성됩니다. 그런 다음 스캐너 매핑 데이터가 벤더 매핑 데이터로 변환됩니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 설정 도우미 〉 통합 구성 〉 솔루션 통합 〉 일반 취약성 대응 프레임워크.
2. 파일 임포트를 클릭합니다.

   주:
   한 번에 하나의 XML 파일만 업로드할 수 있으며 최대 파일 크기는 1GB입니다.

3. 이름 필드에 통합의 고유한 이름을 입력합니다.
   스케줄러는 이 이름으로 생성됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 벤더 필드에 벤더의 이름을 입력합니다.
   솔루션의 소스 필드가 벤더 이름으로 채워집니다.
5. 마침을 클릭합니다.

결과
임포트 큐가 생성됩니다. 관련 목록과 함께 벤더의 큐 항목을 보려면 정보 표시줄의 링크를 클릭하십시오. 작업 상태를 볼 수도 있습니다.

데이터를 CVRF 형식으로 임포트한 후 데이터는 다음과 같은 방식으로 처리됩니다.

1. 큐가 처리되면 전용 데이터 소스를 사용하여 파일이 구문 분석됩니다.
2. 처리가 완료되면 애플리케이션 로그가 업데이트됩니다.
3. CVRF XML 파일이 구문 분석되면 애플리케이션에 다음 테이블이 ServiceNow# 취약성 대응 채워집니다.
   - sn_vul_solution
   - sn_vul_m2m_vulnerability_solution
   - sn_vul_nvd_entry
   - sn_vul_software
   - sn_vul_product_category

애플리케이션 로그에서 오류 또는 예외와 관련된 자세한 정보를 볼 수 있습니다.

연결 및 자격 증명 별칭 구성

벤더를 인증하도록 연결 및 자격 증명 별칭을 구성합니다. 권고 구문 분석에서는 외부 공급업체 벤더가 인증됩니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin, sn_vul.admin(사용하지 않음) 또는 admin

프로시저

1. OAuth 인증을 생성합니다.
   클라이언트가 인스턴스에 액세스할 수 있도록 엔드포인트 만들기를 참조하세요.
2. 연결 및 자격 증명 별칭을 생성합니다.
   연결 및 자격 증명 별칭 생성의 내용을 참조하십시오.
3. 연결을 생성합니다.
   a. 새로 생성한 연결 및 자격 증명 별칭의 이름을 클릭합니다.
   b. 연결 탭에서 새로 만들기를 클릭합니다.
   c. 인증 유형이 OAuth인 경우 1단계에서 만든 애플리케이션 레지스트리 프로파일을 **OAuth** 엔터티 프로파일로 선택합니다.
   d. 기록의 관련 목록에서 연결의 기록을 생성합니다.
   e. 자격 증명 필드에서 3d 단계에서 만든 자격 증명 기록을 선택합니다.
   f. 연결 **URL** 필드에 벤더의 URL을 입력합니다.
   g. 제출을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Cisco 이외의 공통 취약성 보고 프레임워크 벤더 구성

API를 지원하는 Cisco 이외의 CVRF(Common Vulnerability Reporting Framework) 벤더를 구성합니다.

시작하기 전에

필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음) 또는 admin

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 연결 및 자격 증명 〉 연결 및 자격 증명 별칭.
2. 벤더에서 지원하는 인증 유형으로 기록을 생성합니다.
   벤더를 인증하는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 연결 및 자격 증명 별칭 구성.
3. 다음으로 이동 모두 〉 취약성 대응 〉 플로우 디자이너.
4. "자문 구문 분석"이라는 플로우를 복제합니다.

   주:
   - 변경해야 하는 작업이 있는 경우 해당 작업을 복사하여 새 플로우에서 사용합니다.
   - 벤더에 따라 페이지 매김 관련 논리를 업데이트합니다

5. 날짜 범위 매개변수 논리가 Cisco와 같지 않은 경우 페이지 매김 매개변수 업데이트 작업을 복사하고 벤더에 필요한 대로 변경합니다.
6. 다음으로 이동 모두 〉 취약성 대응 〉 보강 데이터 매핑.
7. 벤더에 따라 속성 키 값을 변경하여 Cisco에 따라 기록을 생성합니다.
   이 논리는 자문 페이로드에서 테이블로 필수 필드를 매핑하기 위한 ServiceNow 것입니다.
8. API 페이로드에서 다음 API 태그를 매핑합니다.
   이러한 태그는 보강 데이터 매핑 테이블에 채울 세부 정보와 매핑되어야 합니다. 기본적으로 Cisco 관련 매핑이 제공됩니다.

   주:
   권고를 게시하는 벤더를 여러 개 구성해야 하는 경우 기록을 생성해야 합니다.

자문 페이로드 태그	테이블 sn_vul_cvrf_solution_integration_up 열	설명
CVRF URL	cvrf_url	CVRF URL이 포함된 태그 이름입니다.
자문 ID(응답의 고유 키)	ID	고유 식별자가 포함된 태그 이름입니다.
마지막으로 수정한 날짜	last_modified_date	기록이 마지막으로 업데이트된 날짜가 포함된 태그 이름입니다.
securityAdvisoryIntegrationSysId	통합	취약성 솔루션 기록을 생성하는 통합의 예약된 작업 sysId를 참조합니다.

9. 응답 형식에 따라 자문 구문 분석 플로우에서 목록 검색 작업을 복사하여 구문 분석 논리를 변경합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

권고에서 일반 취약성 보고 프레임워크 데이터 임포트

임포트 유형을 API로 하는 벤더 URL을 구성하여 권고에서 CVRF 데이터를 임포트합니다.

시작하기 전에

필요한 역할: sn_vul.vulnerability_admin, sn_vul.admin(사용하지 않음) 또는 admin

이 태스크 정보

통합이 실행되면 권고를 가져옵니다. CVRF URL 및 권고 ID는 페이로드에서 추출됩니다. REST API 호출은 각 CVRF URL에 대해 수행되며 데이터는 구문 분석되어 sn_vul_solution 테이블에 저장됩니다.

프로시저

1. 다음으로 이동 취약성 대응 〉 관리 〉 설정 도우미 〉 통합 구성 〉 솔루션 통합 〉 일반 취약성 대응 프레임워크.
2. **Add** Integration(통합 추가)을 클릭합니다.
3. 양식에서 필드를 채웁니다.

솔루션 권고 임포트 양식

필드	설명
임포트 유형	임포트 유형을 선택하는 옵션입니다. **API**를 선택합니다.
이름	통합의 고유 이름입니다.
벤더	벤더의 이름입니다. 주: 솔루션의 소스 필드가 벤더 이름으로 채워집니다.
연결 별칭	인증된 자격 증명을 선택하는 옵션입니다. 주: sys_alias 테이블에는 자격 증명과 권고의 기본 URL이 저장됩니다.
일정	데이터를 업데이트해야 하는 빈도입니다.
일	데이터를 업데이트할 요일입니다.
시간	데이터를 업데이트할 요일입니다.
API 구성	
플로우	플로우를 선택하는 옵션입니다. 스케줄러가 실행될 때 플로우가 트리거됩니다. 플로우는 권고 구문 분석을 처리하고 CVRF URL을 추출하여 업데이트 테이블에 해당 세부 정보를 저장합니다. 기존 플로우를 복사하고 필요한 경우 편집할 수 있습니다. 예를 들어 페이지 매김과 관련된 변경 작업을 수행할 수 있습니다.
플로우 작업	플로우 작업을 선택하는 옵션입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	플로우 작업은 슬라이딩 윈도우 기능을 처리합니다. 끌어서 플로우 작업을 업데이트하고 쿼리 매개변수를 작업에 직접 추가할 수 있습니다.
매핑 테이블	매핑 테이블을 선택하는 옵션입니다. 보강 데이터 매핑 테이블의 기록은 권고 페이로드에서 CVRF URL 및 자문 ID를 추출하는 데 사용됩니다.
응답의 권고	권고 목록을 추출할 수 있는 권고 페이로드에서 태그 이름을 입력하는 옵션입니다.
필터 기준	
시간 범위 매개변수	요청의 시간 범위와 API 호출의 날짜 형식을 선택하는 옵션입니다. 시작 날짜/종료 날짜 요청 매개변수는 API 호출 중 시작 날짜 및 종료 날짜에 사용되는 매개변수 이름입니다. 예를 들어 StartDate, start_date, endDate end_date입니다.
날짜 형식	mm/dd/yyyy와 같은 날짜 형식을 입력하는 옵션입니다. 날짜 형식은 API에서 필터링하는 데 필요한 형식입니다. GlideDate에서 지원하지 않는 형식은 작동하지 않습니다.
초기 범위(일)	스케줄러가 처음 실행될 때 데이터를 가져와야 하는 요일입니다. 후속 실행에서는 슬라이딩 창 메커니즘을 따릅니다. **주:** 시간 범위를 선택하지 않으려면 매개변수 없음을 선택합니다.
스캐너 매핑	
스캐너 소스	타사 항목(TPE)의 소스를 선택하는 옵션입니다.
취약성 열	키워드를 선택하는 옵션입니다.
키워드	선택한 취약성 열을 검색하기 위한 키워드를 입력하는 옵션입니다.

4. 마침을 클릭합니다.

CVRF URL을 통해 **CVRF(Common Vulnerability Reporting Framework)** 데이터 임포트

설정 도우미에서 벤더 URL을 구성하여 CVRF 데이터를 임포트합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin, sn_vul.admin(사용하지 않음) 또는 admin

이 태스크 정보
통합이 실행되면 구문 분석되는 URL에서 데이터를 가져옵니다. 그런 다음, 데이터는 소스가 벤더 이름으로 포함된 sn_vul_solution 테이블에 저장됩니다.

주:
Oracle은 솔루션 제공을 위해 CVRF URL을 직접 게시합니다. 따라서 Oracle 데이터를 임포트하기 위한 통합을 구성하려면 Oracle에 대한 CVRF URL이 있는지 확인하고 다음 단계를 따르십시오.

프로시저

1. 다음으로 이동 취약성 대응 〉 관리 〉 설정 도우미 〉 통합 구성 〉 솔루션 통합 〉 일반 취약성 대응 프레임워크.
2. **Add** Integration(통합 추가)을 클릭합니다.
3. 양식에서 필드를 채웁니다.

CVRF 임포트 양식

필드	설명
임포트 유형	임포트 유형입니다. **URL**을 선택합니다.
이름	통합의 고유 이름입니다.
벤더	벤더의 이름입니다. 주: 솔루션의 소스 필드가 벤더 이름으로 채워집니다.
URL	솔루션 데이터를 CVRF 형식으로 가져올 URL입니다.
일정	데이터를 업데이트해야 하는 빈도입니다. 주: CVRF의 상태 태그가 "FINAL"로 표시되면 불필요한 실행을 방지하기 위해 필드가 요청 시 로 자동 설정됩니다.
일	데이터를 업데이트할 요일입니다.
시간	데이터를 업데이트할 요일입니다.

4. 마침을 클릭합니다.

Common Vulnerability Reporting Framework 데이터 임포트 문제 해결

문제 해결 작업은 취약성 대응 애플리케이션에서 CVRF 데이터를 임포트할 때 발생하는 일반적인 문제를 해결하는 데 도움이 될 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

문제	작업
통합 실행 기간이 깁니다.	통합이 예상보다 오래 실행되는 경우 다음을 수행합니다. **1.** sn_vul_ds_import_q_entry 테이블로 이동합니다. **2.** 상태 필드별로 그룹화합니다. 완료됨, 진행 중 또는 대기 중 상태의 항목을 볼 수 있습니다.
API 기반 임포트에서 통합 실패	API 기반 임포트에서 통합이 실패하면 다음을 수행합니다. **1.** **Flow Designer**로 이동합니다. **2.** 구성에서 선택한 플로우를 엽니다. 주: Cisco의 경우 자문 구문 분석 플로우를 엽니다. **3.** 실행을 클릭합니다. **4.** 마지막 실행 또는 디버그해야 하는 실행을 엽니다. **5.** 각 스테이지에서 플로우를 확인합니다.
API 기반 임포트에서 시간 초과 오류로 통합에 실패했습니다.	권고 구문 분석 플로우의 시간 초과로 인해 API 기반 임포트에서 통합이 실패하면 다음을 수행합니다. **1.** sys_properties 열어 시간 제한을 늘립니다 . ##. **2.** 이름 열에서 sn_vul #####. CVRFFlowTimeout (inMiliSeconds)입니다. 주: 시간은 밀리초 단위입니다. **3.** 기록을 열고 큰 숫자로 값을 업데이트합니다. **4.** 기록을 저장하고 통합을 다시 실행합니다.
"벤더 매핑 데이터 변환에 대한 스캐너 매핑이 진행 중입니다." 오류와 함께 통합에 실패했습니다.	URL 또는 API 기반 임포트 중에 다음 오류# ## ### ##### #####. ## ### ## ### ## ### ### ## ####. #### ### ### ### #####. ## # ### ######. 이 오류가 발생하면 잠시 기다렸다가 통합을 다시 실행하십시오.
파일 임포트 중에 임포트 큐가 생성되지 않음	파일을 임포트하는 동안 임포트 큐가 생성되지 않는 경우가 있습니다. 이 실패는 스캐너 매핑 데이터를 공급업체 매핑 데이터에 매핑하는

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

문제	작업
	변환이 진행 중임을 의미합니다. 프로세스가 완료되면 큐 항목이 생성됩니다.

CSAF(일반 보안 자문 프레임워크)

CSAF(Common Security Advisory Framework)와 함께 취약성 솔루션 관리사용하면 기계가 읽을 수 있는 JSON 형식을 통해 자동화 보안 알림을 사용할 수 있습니다.

CSAF를 사용하면 솔루션 관리 프레임워크를 사용하여 모든 솔루션 인텔리전스 벤더와 통합하여 인텔리전스 데이터를 임포트할 수 있습니다. CSAF 보안 알림은 다음 유형 중 하나일 수 있습니다.

- 보안 자문
- 취약성 악용 가능성 교환(VEX)
- 보안 인시던트 응답
- 정보 자문

CSAF는 벤더의 보안 권고에 대한 파일 가져오기, URL 가져오기 및 API 가져오기만 지원합니다.

파일 임포트를 통해 일반 보안 자문 프레임워크 데이터 임포트

CSAF 파일을 임포트하여 CSAF 형식으로 데이터를 봅니다. 임포트는 일회성 활동입니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음) 또는 admin

이 태스크 정보
임포트되면 큐 항목이 첨부 파일과 함께 작성되고 항목이 처리될 때 구문 분석됩니다. 그러면 해당 테이블에 데이터가 채워집니다. CSAF 데이터를 구문 분석하기 전에 구성에 따라 스캐너 매핑 기록이 생성됩니다. 그런 다음 스캐너 매핑 데이터가 벤더 매핑 데이터로 변환됩니다.

스캐너 매핑은 NVD 데이터베이스의 CVE(공통 취약성 항목)가 있는 취약성인 NVD(국가 취약성 데이터베이스) 기반 취약성에는 적용되지 않습니다.

대체 가능성이 가장 높은 솔루션이 하나만 있고 취약한 항목으로 롤다운되는 경우 기본 솔루션이 채워집니다. 하나의 NVD 항목에 여러 공급업체 솔루션이 포함된 경우 가장 높은 대체 솔루션이 두 개 이상 있으므로 기본 솔루션이 채워지지 않습니다. 이 경우 솔루션을 수동으로 선택해야 합니다. 타사 취약성의 경우 해당 스캐너 매핑을 추가하는 경우에만 기본 솔루션이 채워집니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 설정 도우미 〉 통합 구성 〉 솔루션 통합 〉 일반 보안 자문 프레임워크.
2. 파일 임포트를 선택합니다.

   주:
   한 번에 하나의 JSON 파일만 업로드할 수 있으며 최대 파일 크기는 15MB입니다.

3. 이름 필드에 통합의 고유한 이름을 입력합니다.
   스케줄러는 이 이름으로 생성됩니다.
4. 벤더 필드에 벤더의 이름을 입력합니다.
   솔루션의 소스 필드가 벤더 이름으로 채워집니다.
5. 마침을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

결과
임포트 큐가 생성됩니다. 관련 목록과 함께 벤더의 큐 항목을 보려면 정보 표시줄의 링크를 선택합니다. 작업 상태를 볼 수도 있습니다.

데이터를 CSAF 형식으로 임포트한 후에는 다음과 같은 방식으로 데이터가 처리됩니다.

1. 큐가 처리되면 전용 데이터 소스를 사용하여 파일이 구문 분석됩니다.
2. 처리가 완료되면 애플리케이션 로그가 업데이트됩니다.
3. CSAF JSON 파일이 구문 분석되면 애플리케이션의 다음 테이블이 ServiceNow# 취약성 대응 채워집니다.
   - sn_vul_solution
   - sn_vul_m2m_vulnerability_solution
   - sn_vul_nvd_entry
   - sn_vul_software
   - sn_vul_product_category

애플리케이션 로그에서 오류 또는 예외와 관련된 자세한 정보를 볼 수 있습니다.

CSAF(일반 보안 자문 프레임워크)에 대한 연결 및 자격 증명 별칭 구성

벤더를 인증하도록 연결 및 자격 증명 별칭을 구성합니다. 권고 구문 분석에서는 외부 공급업체 벤더가 인증됩니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin, sn_vul.admin(사용하지 않음) 또는 admin

프로시저

1. OAuth 인증을 생성합니다.
   클라이언트가 인스턴스에 액세스할 수 있도록 엔드포인트 만들기를 참조하세요.
2. 연결 및 자격 증명 별칭을 생성합니다.
   연결 및 자격 증명 별칭 생성의 내용을 참조하십시오.
3. 연결을 생성합니다.
   a. 새로 작성된 연결 및 자격 증명 별칭의 이름을 선택하십시오.
   b. 연결 탭에서 새로 만들기를 선택합니다.
   c. 인증 유형이 OAuth인 경우 1단계에서 만든 애플리케이션 레지스트리 프로파일을 **OAuth** 엔터티 프로파일로 선택합니다.
   d. 기록의 관련 목록에서 연결의 기록을 생성합니다.
   e. 자격 증명 필드에서 3d 단계에서 만든 자격 증명 기록을 선택합니다.
   f. 연결 **URL** 필드에 벤더의 URL을 입력합니다.
   g. 제출을 선택합니다.

공통 보안 자문 프레임워크 구성 이외의 벤더 **Red Hat**

API 지원 이외의 Red Hat CSAF(공통 보안 자문 프레임워크) 벤더를 구성합니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음) 또는 admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 연결 및 자격 증명 〉 연결 및 자격 증명 별칭.
2. 벤더에서 지원하는 인증 유형으로 기록을 생성합니다.
   벤더를 인증하는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 CSAF(일반 보안 자문 프레임워크)에 대한 연결 및 자격 증명 별칭 구성.
3. 다음으로 이동 모두 〉 취약성 대응 〉 플로우 디자이너.
4. "자문 구문 분석"이라는 플로우를 복제합니다.

   주:
   - 변경해야 하는 작업이 있는 경우 해당 작업을 복사하여 새 플로우에서 사용합니다.
   - 벤더 API에 따라 page_index_key 및 page_size_key 매개변수를 검토합니다.
   - 벤더에 따라 페이지 매김 관련 논리를 업데이트합니다

5. 날짜 범위 매개변수 논리가 다음과 Red Hat같지 않으면 페이지 매김 매개변수 업데이트 작업을 복사하고 벤더의 필요에 따라 변경합니다.
6. 다음으로 이동 모두 〉 취약성 대응 〉 보강 데이터 매핑.
7. 벤더에 따라 속성 키 값을 변경하여 기록에 따라 Red Hat 생성합니다.
   이 논리는 자문 페이로드에서 테이블로 필수 필드를 매핑하기 위한 ServiceNow 것입니다.
8. API 페이로드에서 다음 API 태그를 매핑합니다.
   이러한 태그는 보강 데이터 매핑 테이블에 채울 세부 정보와 매핑되어야 합니다. 기본적으로 특정 매핑이 Red Hat 제공됩니다.

   주:
   권고를 게시하는 벤더를 여러 개 구성해야 하는 경우 기록을 생성해야 합니다.

자문 페이로드 태그	테이블 sn_vul_cvrf_solution_integration_up 열	설명
CSAF URL(CSAF 페이로드를 가리키는 자원 URL)	cvrf_url	CSAF URL이 포함된 태그 이름입니다.
자문 ID(응답의 고유 키)	ID	고유 식별자가 포함된 태그 이름입니다.
마지막으로 수정한 날짜	last_modified_date	기록이 마지막으로 업데이트된 날짜가 포함된 태그 이름입니다.
csaf(정적 값)	advisory_format	CSAF 페이로드에 대한 자문 형식 값입니다. 이 값은 모든 CSAF 통합에 적용할 수 있는 정적 값입니다.
securityAdvisoryIntegrationSysId	통합	취약성 솔루션 기록을 생성하는 통합의 예약된 작업 sysId를 참조합니다.

9. 응답 형식에 따라 자문 구문 분석 플로우에서 목록 검색 작업을 복사하여 구문 분석 논리를 변경합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

권고에서 일반 보안 자문 프레임워크 데이터 임포트

임포트 유형을 API로 하는 벤더 URL을 구성하여 권고에서 CSAF 데이터를 임포트합니다.

시작하기 전에

필요한 역할: sn_vul.vulnerability_admin, sn_vul.admin(사용하지 않음) 또는 admin

이 태스크 정보

통합이 실행되면 권고를 가져옵니다. CSAF URL 및 권고 ID가 페이로드에서 추출됩니다. REST API 호출은 각 CSAF URL에 대해 수행되며 데이터는 구문 분석되어 sn_vul_solution 테이블에 저장됩니다.

스캐너 매핑은 NVD 데이터베이스의 CVE(공통 취약성 항목)가 있는 취약성인 NVD(국가 취약성 데이터베이스) 기반 취약성에는 적용되지 않습니다.

대체 가능성이 가장 높은 솔루션이 하나만 있고 취약한 항목으로 롤다운되는 경우 기본 솔루션이 채워집니다. 하나의 NVD 항목에 여러 공급업체 솔루션이 포함된 경우 가장 높은 대체 솔루션이 두 개 이상 있으므로 기본 솔루션이 채워지지 않습니다. 이 경우 솔루션을 수동으로 선택해야 합니다. 타사 취약성의 경우 해당 스캐너 매핑을 추가하는 경우에만 기본 솔루션이 채워집니다.

프로시저

1. 다음으로 이동 취약성 대응 〉 관리 〉 설정 도우미 〉 통합 구성 〉 솔루션 통합 〉 일반 보안 자문 프레임워크.
2. 통합 추가를 선택합니다.
3. 양식에서 필드를 채웁니다.

솔루션 권고 임포트 양식

필드	설명
임포트 유형	임포트 유형을 선택하는 옵션입니다. **API**를 선택합니다.
이름	통합의 고유 이름입니다.
벤더	벤더의 이름입니다. 주: 솔루션의 소스 필드가 벤더 이름으로 채워집니다.
연결 별칭	인증된 자격 증명을 선택하는 옵션입니다. 주: sys_alias 테이블에는 자격 증명과 권고의 기본 URL이 저장됩니다.
일정	데이터를 업데이트해야 하는 빈도입니다.
일	데이터를 업데이트할 요일입니다.
시간	데이터를 업데이트할 요일입니다.
API 구성	
플로우	플로우를 선택하는 옵션입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	스케줄러가 실행될 때 플로우가 트리거됩니다. 플로우는 권고 구문 분석을 처리하고 CSAF URL을 추출하여 업데이트 테이블에 해당 세부 정보를 저장합니다. 기존 플로우를 복사하고 필요한 경우 편집할 수 있습니다. 예를 들어 페이지 매김과 관련된 변경 작업을 수행할 수 있습니다.
플로우 작업	플로우 작업을 선택하는 옵션입니다. 플로우 작업은 슬라이딩 윈도우 기능을 처리합니다. 끌어서 플로우 작업을 업데이트하고 쿼리 매개변수를 작업에 직접 추가할 수 있습니다.
매핑 테이블	매핑 테이블을 선택하는 옵션입니다. 보강 데이터 매핑 테이블의 기록은 권고 페이로드에서 CSAF URL 및 자문 ID를 추출하는 데 사용됩니다.
응답의 권고	권고 목록을 추출할 수 있는 권고 페이로드에서 태그 이름을 입력하는 옵션입니다.
필터 기준	
시간 범위 매개변수	요청의 시간 범위와 API 호출의 날짜 형식을 선택하는 옵션입니다. 시작 날짜/종료 날짜 요청 매개변수는 API 호출 중 시작 날짜 및 종료 날짜에 사용되는 매개변수 이름입니다. 예를 들어 StartDate, start_date, endDate end_date입니다.
날짜 형식	mm/dd/yyyy와 같은 날짜 형식을 입력하는 옵션입니다. 날짜 형식은 API에서 필터링하는 데 필요한 형식입니다. GlideDate에서 지원하지 않는 형식은 작동하지 않습니다.
초기 범위(일)	스케줄러가 처음 실행될 때 데이터를 가져와야 하는 요일입니다. 후속 실행에서는 슬라이딩 창 메커니즘을 따릅니다. **주:** 시간 범위를 선택하지 않으려면 매개변수 없음을 선택합니다.
스캐너 매핑	
스캐너 소스	타사 항목(TPE)의 소스를 선택하는 옵션입니다.
취약성 열	키워드를 선택하는 옵션입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
키워드	선택한 취약성 열을 검색하기 위한 키워드를 입력하는 옵션입니다.

4. 마침을 선택합니다.

CSAF URL을 통해 일반 보안 자문 프레임워크(CSAF) 데이터 임포트

설정 도우미에서 벤더 URL을 구성하여 CSAF 데이터를 임포트합니다.

시작하기 전에

필요한 역할: sn_vul.vulnerability_admin, sn_vul.admin(사용하지 않음) 또는 admin

이 태스크 정보

통합이 실행되면 구문 분석되는 URL에서 데이터를 가져옵니다. 그런 다음, 데이터는 소스가 벤더 이름으로 포함된 sn_vul_solution 테이블에 저장됩니다.

> **주:**
> URL은 권고 상세 정보가 포함된 직접 CSAF 페이로드 또는 ROLIE(Resource-Oriented Lightweight Information Exchange) 피드 URL일 수 있습니다. 두 경우 모두 그에 따라 페이로드가 구문 분석되고 솔루션 기록이 생성됩니다. CSAF URL 임포트에 대해 다음 단계를 완료합니다.

ROLIE 피드를 지원하는 URL 임포트를 통해 CSAF 집계기 또는 신뢰할 수 있는 제공자로부터 취약성 솔루션을 임포트할 수도 있습니다. 이러한 취약성 솔루션은 CVE(Common Vulnerabilities and Exposures)에 따라 올바른 벤더 및 취약한 항목(VIT)에 자동으로 매핑됩니다.

스캐너 매핑은 NVD 데이터베이스의 CVE(공통 취약성 항목)가 있는 취약성인 NVD(국가 취약성 데이터베이스) 기반 취약성에는 적용되지 않습니다.

대체 가능성이 가장 높은 솔루션이 하나만 있고 취약한 항목으로 롤다운되는 경우 기본 솔루션이 채워집니다. 하나의 NVD 항목에 여러 공급업체 솔루션이 포함된 경우 가장 높은 대체 솔루션이 두 개 이상 있으므로 기본 솔루션이 채워지지 않습니다. 이 경우 솔루션을 수동으로 선택해야 합니다. 타사 취약성의 경우 해당 스캐너 매핑을 추가하는 경우에만 기본 솔루션이 채워집니다.

프로시저

1. 다음으로 이동 취약성 대응 〉 관리 〉 설정 도우미 〉 통합 구성 〉 솔루션 통합 〉 일반 보안 자문 프레임워크.
2. 통합 추가를 선택합니다.
3. 양식에서 필드를 채웁니다.

CSAF 임포트 양식

필드	설명
임포트 유형	임포트 유형입니다. **URL**을 선택합니다.
이름	통합의 고유 이름입니다.
단일 벤더	한 벤더에서 CSAF를 임포트하는 경우 이 옵션을 선택합니다.
벤더	벤더의 이름입니다. 이 필드는 단일 벤더를 선택하는 경우에만 사용할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	주: 솔루션의 소스 필드가 벤더 이름으로 채워집니다.
다중 벤더	여러 벤더에서 CSAF를 임포트하는 경우 이 옵션을 선택합니다.
집계	솔루션을 임포트할 수 있는 신뢰할 수 있는 제공자입니다.
URL	CSAF 형식의 솔루션 데이터를 가져올 URL입니다.
일정	데이터를 업데이트해야 하는 빈도입니다. 주: CSAF의 상태 태그가 "최종"으로 표시되면 불필요한 실행을 방지하기 위해 필드가 요청 시 로 자동 설정됩니다.
일	데이터를 업데이트할 요일입니다.
시간	데이터를 업데이트할 요일입니다.
스캐너 매핑 주: 스캐너 매핑 섹션은 CSAF에서 선택 사항입니다.	
스캐너 소스	타사 항목(TPE)의 소스를 선택하는 옵션입니다.
취약성 열	키워드를 선택하는 옵션입니다.
키워드	선택한 취약성 열을 검색하기 위한 키워드를 입력하는 옵션입니다.

4. 마침을 선택합니다.

일반 보안 자문 프레임워크 데이터 임포트 문제 해결

문제 해결 작업은 취약성 대응 애플리케이션에서 CSAF 데이터를 임포트할 때 발생하는 일반적인 문제를 해결하는 데 도움이 될 수 있습니다.

문제	작업
통합 실행 기간이 깁니다.	통합이 예상보다 오래 실행되는 경우 다음을 수행합니다. 1. sn_vul_ds_import_q_entry 테이블로 이동합니다. 2. 상태 필드별로 그룹화합니다. 완료됨, 진행 중 또는 대기 중 상태의 항목을 볼 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

문제	작업
API 기반 임포트에서 통합 실패	API 기반 임포트에서 통합이 실패하면 다음을 수행합니다. **1.** **Flow Designer**로 이동합니다. **2.** 구성에서 선택한 플로우를 엽니다. 주: 의 Red Hat경우 자문 구문 분석 플로우를 엽니다. **3.** 실행을 선택합니다. **4.** 마지막 실행 또는 디버그해야 하는 실행을 엽니다. **5.** 각 스테이지에서 플로우를 확인합니다.
API 기반 임포트에서 시간 초과 오류로 통합에 실패했습니다.	권고 구문 분석 플로우의 시간 초과로 인해 API 기반 임포트에서 통합이 실패하면 다음을 수행합니다. **1.** sys_properties 열어 시간 제한을 늘립니다 . ##. **2.** 이름 열에서 sn_vul #####. CVRFFlowTimeout (inMiliSeconds)입니다. 주: 시간은 밀리초 단위입니다. **3.** 기록을 열고 큰 숫자로 값을 업데이트합니다. **4.** 기록을 저장하고 통합을 다시 실행합니다.
"벤더 매핑 데이터 변환에 대한 스캐너 매핑이 진행 중입니다." 오류와 함께 통합에 실패했습니다.	URL 또는 API 기반 임포트 중에 다음 오류# ## ### ##### #####. ## ### ## ### ## ### ### ## ####. #### ### ### ### #####. ## # ### ######. 이 오류가 발생하면 잠시 기다렸다가 통합을 다시 실행하십시오.
파일 임포트 중에 임포트 큐가 생성되지 않음	파일을 임포트하는 동안 임포트 큐가 생성되지 않는 경우가 있습니다. 이 실패는 스캐너 매핑 데이터를 공급업체 매핑 데이터에 매핑하는 변환이 진행 중임을 의미합니다. 프로세스가 완료되면 큐 항목이 생성됩니다.

추가 취약성 대응 설정 및 구성 작업

정정에 도움이 되도록 기본 설정 이외의 구성의 일부로 이러한 추가 관리 설정 작업을 수행할 수 있습니다. 이러한 작업은 설정 도우미 외부에서 수행할 수 있습니다.

함께 취약성 대응 제공되는 기본 보고를 사용하여 보안 태세를 감독할 수 있습니다. 환경에 적합하지 않은 경우 해당 보고서를 편집하거나 템플릿으로 사용하여 직접 만들 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약성 대응용 퍼포먼스 분석 애플리케이션이 설치된 경우 보고서, 응답 대시보드 등을 만들 수 있습니다. 자세한 내용은 보고서 시작을 참조하십시오.

이메일 알림은 생산성과 원활한 워크플로우를 향상시킵니다.

소프트웨어 노출 평가를 통해 소프트웨어 자산 관리(SAM Foundation)에서 게시자, 제품 이름 및 버전 번호를 조회하여 취약한 소프트웨어에 대한 노출을 확인합니다.

취약성 라이브러리에 대한 가시성은 그룹화 및 정정 작업에 유연성을 제공할 수 있습니다.

조직이 게시된 취약성 관리 또는 보안 정책, 표준 또는 가이드라인을 준수할 수 없는 경우 예외를 요청할 수 있도록 예외 관리를 구성합니다.

추가 설정 작업에 대한 자세한 내용은 이 개요 다음에 나오는 항목을 참조하십시오.

취약성 대응에 대한 빠른 시작 테스트

업그레이드 적용 또는 애플리케이션 개발과 같이 구성 변경 후에도 취약성 대응 앱이 계속 작동하는지 확인합니다. 인스턴스별 데이터를 사용할 때 통과하도록 이러한 빠른 시작 테스트를 복사하여 사용자 지정합니다.

테스트 실행 속성은 프로덕션 시스템에서 테스트를 실행할 수 없도록 기본적으로 비활성화되어 있습니다. 개발, 테스트 및 기타 비프로덕션 인스턴스에 대해서만 테스트를 실행합니다. 데모 데이터 또는 데모 계정이 생성된 경우 비프로덕션 또는 프로덕션에서 인스턴스를 사용하기 전에 모든 데모 데이터를 제거해야 합니다. 에 대한 취약성 대응테스트 도구 모음 설정 및 실행에 대한 자세한 내용은 을 참조하십시오에 대해 Automated Test Framework(ATF) 테스트 도구 모음 실행 취약성 대응.

취약성 대응 빠른 시작 테스트를 하려면 취약성 대응 애플리케이션(sn_vul)을 활성화하고 데모 데이터를 로드해야 합니다.

취약성 대응 테스트

테스트	설명	릴리스 버전
VR: 재구성 대상 규칙 만들기	정정 대상 규칙을 만듭니다.	Madrid
VR: 취약성 그룹 규칙 만들기	취약성 그룹 규칙을 만듭니다.	Madrid
VR: 양식을 통해 취약한 항목 만들기	사용자가 취약한 항목 양식에서 취약한 항목을 성공적으로 만들 수 있는지를 결정합니다.	Madrid
VR: 취약성 그룹 수명주기	사용자가 취약성 그룹을 성공적으로 해결할 수 있는지를 결정합니다.	Madrid
VR: 취약한 항목 수명주기	사용자가 취약한 항목의 수명주기 동안 취약한 항목을 성공적으로 이동할 수 있는지 여부를 판별하고, 종결된 취약한 항목을 다시 열 수 있는지도 결정합니다.	Madrid
VR: 롤업 계산기	롤업 위험 계산기가 취약성 그룹의 모든 취약 항목에 대한 점수를 사용하여 취약 항목의 전체 그룹에 대한 전반적인 위험 점수를 제공할 수 있는지 여부를 확인합니다.	New York

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약성 대응 테스트

테스트	설명	릴리스 버전
VR: 취약성 대응 담당 규칙	담당 규칙의 예시 집합이 정정을 위해 할당 그룹에 취약 항목을 성공적으로 자동 할당할 수 있는지 여부를 확인합니다.	New York
VR: 취약성 계산기	취약성 계산기를 테스트합니다.	New York
VR: CI 조회 - Qualys	Qualys용 "Lookup By Network Adapter"(네트워크 어댑터로 조회)라는 "field_matching" 메서드로 새 조회 규칙을 만듭니다. 새로운 조회 규칙을 통해 구성 항목이 검색된 항목 테이블에서 네트워크 어댑터 및 IP 주소와 성공적으로 일치하는지 여부를 확인합니다.	Orlando
VR: 일반 및 긴급 변경 요청 만들기	사용자가 취약성 그룹에서 일반 및 긴급 변경 요청을 성공적으로 만들 수 있는지 여부를 확인합니다.	Orlando
VR: 취약성 그룹 분할	사용자가 취약성 그룹을 성공적으로 분할할 수 있는지 여부를 확인합니다.	Orlando
VR: CHG가 취소되면 VG 상태를 업데이트합니다.	취약성 그룹과 연결된 변경 요청이 취소될 때 취약성 그룹의 상태 필드가 성공적으로 전환되는지 여부를 확인합니다.	Orlando
VR: CHG가 검토로 전환될 때 VG 상태를 업데이트합니다.	취약성 그룹의 상태 필드가 이와 연결된 변경 요청이 검토 상태로 이동할 때 성공적으로 전환되는지 여부를 확인합니다.	Orlando
VR: CI 조회 - Rapid7	기존 Rapid7 취약성 통합 조회 규칙, **IP** 주소를 사용하여 CI 조회를 테스트합니다.	Orlando
VR: CI 조회 - Qualys	Qualys Vulnerability Integration에 대한 새 조회 규칙을 생성하여 CI 조회를 테스트합니다.	Orlando
VR: VI에 대한 예외 승인 워크플로우	예외 요청을 생성하고 승인 프로세스가 작동하는지 확인합니다.	Orlando
VR: VI에 대한 가양성 승인 워크플로우	가양성 예외 요청을 생성하고 승인 프로세스가 작동하는지 확인합니다.	Orlando
VR: AVR(애플리케이션 취약성 대응)	규칙과 계산기가 올바로 작동하는지 확인합니다. 업데이트가 작동하는지 확인합니다.	Orlando

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약성 대응 테스트

테스트	설명	릴리스 버전
정정 대상 규칙: VI 임포트 테스트	임포트 중 VR 정정 대상 규칙을 테스트합니다.	Paris
VR: 분류 규칙	취약성을 자동으로 분류하는 샘플 분류 규칙입니다.	Tokyo

관련 정보

빠른 시작 테스트

에 대해 **Automated Test Framework(ATF)** 테스트 도구 모음 실행 취약성 대응

애플리케이션을 설치하거나 업그레이드한 후 Automated Test Framework(ATF) 테스트 도구 모음을 취약성 대응 실행합니다.

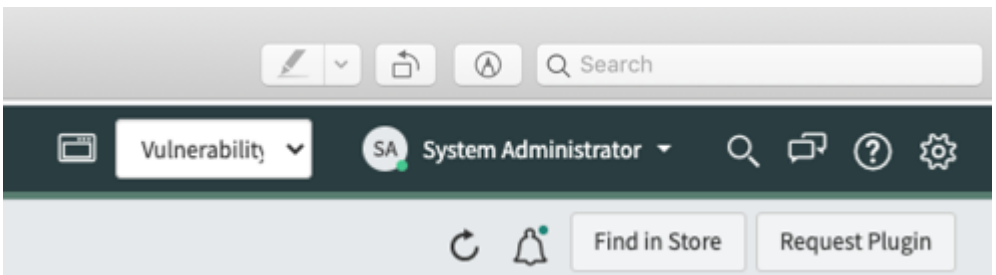
시작하기 전에
설치가 성공적으로 되었고 인스턴스가 설계된 대로 작동하는지 확인합니다.

테스트 실행 속성은 프로덕션 시스템에서 테스트를 실행할 수 없도록 기본적으로 비활성화되어 있습니다. 개발, 테스트 및 기타 비프로덕션 인스턴스에 대해서만 테스트를 실행합니다. 데모 데이터 또는 데모 계정이 생성된 경우 비프로덕션 또는 프로덕션에서 인스턴스를 사용하기 전에 모든 데모 데이터를 제거해야 합니다.

- 를 설치할 취약성 대응때 데모 데이터를 설치했는지 확인합니다. 테스트 도구 모음을 취약성 대응 실행하려면 데모 데이터가 필요합니다.
- 테스트를 활성화하려면 다음 단계를 수행합니다.

1. 다음으로 이동 모두 〉 **ATF(Automated Test Framework)** 〉 관리 〉 속성.
2. 선택하지 않은 경우 테스트/테스트 도구 모음 실행 사용 확인란을 선택합니다.
3. 저장을 클릭합니다.
4. 헤더에서 범위가 **Vulnerability Response** 로 설정되지 않았거나 범위가 헤더에 표시되지 않은 경우 브라우저 창의 페이지 상단에 있는 설정 아이콘을 클릭합니다. .
5. 시스템 설정 창에서 개발자를 클릭합니다.
6. 선택하지 않은 경우 헤더에 애플리케이션 선택기 표시를 클릭하고 창을 닫습니다.
7. ### ### 옆에 표시되는 목록에서 필드에 대해 취약성 대응을 클릭합니다.

   필드는 다음 이미지와 같이 표시됩니다.

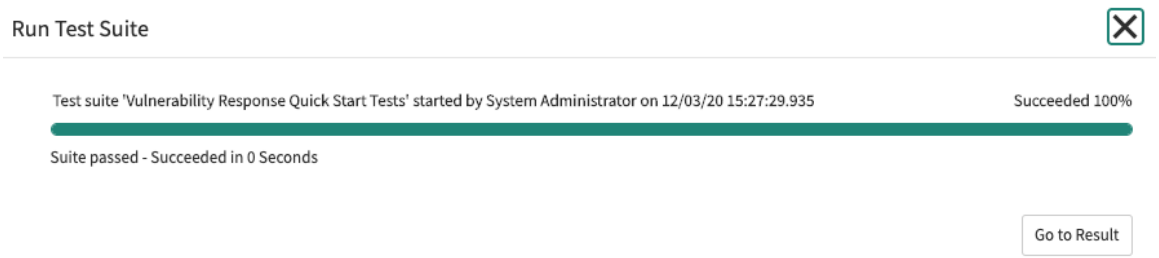


필요한 역할: admin 또는 atf_test_admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 **ATF(Automated Test Framework)** 〉 도구 모음.
2. 테스트 도구 모음 목록에서 **Vulnerability Response** 빠른 시작 테스트를 찾습니다.
3. 클릭하여 기록을 엽니다.
4. 열려 있는 기록에서 활성 확인란을 선택합니다.
5. 업데이트를 클릭합니다.
6. 테스트 도구 모음 실행 버튼이 표시되지 않으면 화면을 새로 고치고 레코드를 다시 연 다음 테스트 도구 모음 실행을 클릭하여 테스트를 시작합니다.
   잠시 후 테스트 도구 모음 실행 대화 상자에 테스트가 성공적으로 완료되었다고 표시됩니다. 자세한 내용은 결과로 이동을



클릭합니다.

다음에 수행할 작업
축하합니다! 의 취약성 대응구성을 계속할 수 있습니다.

자동화된 테스트 및 자동화된 테스트, 테스트 도구 모음 및 자동화된 테스트 만들기에 대한 취약성 대응 자세한 내용은 Automated Test Framework(ATF) 를 참조하십시오.

취약성 대응용 취약점 할당 권장 설치

할당되지 않았거나 잘못 할당된 취약성 결과의 소유자를 식별하는 데 소요되는 시간을 줄일 수 있도록 설치합니다 취약점 할당 권장 . 이 애플리케이션은 에서 별도의 구독으로 사용할 수 있습니다 ServiceNow Store.

시작하기 전에
인스턴스에서 기능을 취약성 대응ServiceNow AI Platform# 실행하려면 취약점 할당 권장 먼저 용 취약성 대응 애플리케이션을 다운로드하여 설치해야 취약점 할당 권장 합니다. 설치하기 전에 다음 설정 검사 목록을 완료합니다. 이러한 설정 작업은 원활한 설치 및 구성을 위해 필요합니다.

> **주:**
> 이 프로세스는 프로덕션 인스턴스에 다운로드된 애플리케이션에만 적용됩니다. 애플리케이션을 비프로덕션 또는 개발 인스턴스에 다운로드하는 경우에는 권리를 얻을 필요가 없습니다. 자세한 내용은 ServiceNow Store 애플리케이션 활성화를 참조하십시오.

필요한 역할: admin

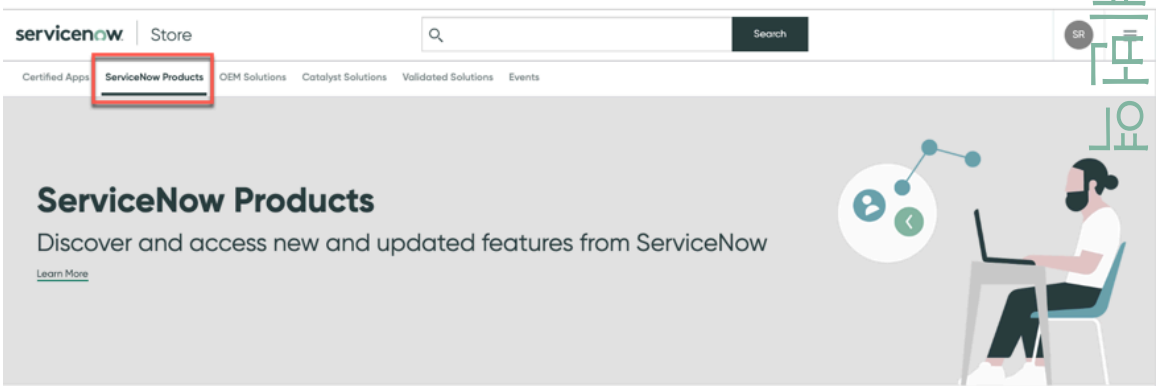
작업 설정	작업
애플리케이션이 설치되고 활성화되었는지 취약성 대응 확인합니다.	다음으로 이동 모두 〉 시스템 애플리케이션 〉 모든 애플리케이션 〉 인스턴스에 설치됨. 취약성 대응 설치된 경우 이 목록에 표시됩니다. 애플리케이션이 설치 및 활성화되지 않은 경우 을 참조하십시오 취약성 대응 설치.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업 설정	작업
애플리케이션이 설치되고 활성화되었는지 예측 인텔리전스 확인합니다.	다음으로 이동 시스템 애플리케이션 〉 모든 애플리케이션 〉 인스턴스에 설치됨. 예측 인텔리전스 설치된 경우 이 목록에 표시됩니다. 애플리케이션이 설치 및 활성화되지 않은 경우 을 참조하십시오 Install Predictive Intelligence .
인스턴스에 필요한 ServiceNow 역할이 있는지 확인합니다.	예상 결과의 설치 및 검증에 필요한 다음 역할이 있는지 확인합니다. • vulnerability_admin: 를 사용하도록 설정하고 구성하는 취약점 할당 권장데 필요합니다. 또한 이를 사용하여 취약한 항목 및 정정 작업에 대한 할당 권장 사항을 보고 선택할 수 있습니다. • ServiceNow admin: 애플리케이션을 설치하는 데 필요합니다.

프로시저

1. ServiceNow Store로 이동합니다.
2. 로그인을 클릭하고 HI 자격 증명을 입력합니다.
3. 사용 가능한 ServiceNow 제품을 보려면 ServiceNow 제품 탭을



클릭합니다.

4. 자격이 취약점 할당 권장있는 연결된 모든 애플리케이션을 보려면 제품을 취약성 대응 클릭합니다.

   이 페이지에는 옵트인할 경우 사용할 수 있는 모든 애플리케이션이 나열됩니다. 애플리케이션에 대한 자세한 내용을 보려면 애플리케이션에 대한 링크를 클릭하십시오.

5. 에 대한 취약점 할당 권장권리가 있는지 확인하려면 옵트인을 클릭합니다.
6. 사용 약관에 동의하려면 프롬프트에서 확인란을 선택하고 수락을 클릭합니다.
   애플리케이션에 대해 성공적으로 옵트인했음을 나타내는 메시지가 나타납니다.
7. 인스턴스에 애플리케이션을 ServiceNow AI Platform 설치하려면 10단계로 건너뜁니다.
8. 옵션: 다른 인스턴스에서 애플리케이션에 대한 취약점 할당 권장 권리를 관리하려면 권리 관리를 클릭하십시오.ServiceNow AI Platform

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

(Optional) 권리 관리 버튼이 표시되지 않으면 제품 목록에서 응용 프로그램을 클릭하여 취약점 할당 권장 표시합니다.

a. 옵션을 선택합니다.

b. 계속하려면 확인 또는 취소를 클릭하십시오.
플러그인을 활성화하고 인스턴스에 애플리케이션을 ServiceNow AI Platform 설치할 준비가 되었습니다.

9. ServiceNow AI Platform 애플리케이션을 설치할 취약점 할당 권장 인스턴스에 로그인합니다.

10. 다음으로 이동 모두 〉 시스템 애플리케이션 〉 모든 사용 가능 애플리케이션 〉 모두.

11. 나열된 응용 프로그램에서 응용 프로그램(sn_vul_recom)을 취약점 할당 권장 찾아 설치를 클릭합니다.
애플리케이션 설치 대화 상자가 표시되고 설치된 모든 종속성이 표시됩니다.

12. 옵션: 데모 데이터를 원하는 경우 데모 데이터 로드 확인란을 선택하고 설치를 클릭합니다.

주:
데모 데이터 로드 확인란을 선택하지 않으면 나중에 애플리케이션 관리자에서 데모 데이터를 설치할 수 없습니다. 초기 설치 후 데모 데이터를 설치하거나 다시 설치하는 방법에 대한 자세한 내용은 지식베이스에서 애플리케이션이 이미 설치된 경우 데모 데이터를 설치하기 위한 임시 해결책 (KB0722909) 문서를 Now Support 참조하십시오.

이 설치에는 다소 시간이 걸릴 수 있습니다. 애플리케이션과 해당 의존성이 성공적으로 설치된 후 설치 대화 상자에 메시지가 표시됩니다.

13. 닫기를 클릭합니다.

14. 구성하려면 취약점 할당 권장다음 문서를 참조하십시오 에 대한 취약성 할당 권장 사항 구성 취약성 대응.

에 대한 취약성 할당 권장 사항 구성 취약성 대응

사용하도록 설정하면 취약점 할당 권장 할당되지 않았거나 잘못 할당된 취약성 결과의 소유자를 식별하는 데 소요되는 시간을 줄일 수 있습니다.

시작하기 전에
필요한 역할: sn_vul.manage_assignment_recom_config

이 태스크 정보
이 애플리케이션은 기본적으로 활성화되어 있지 않습니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 할당 권장 사항.

2. 할당 권장 사항 사용을 선택합니다.
예측 인텔리전스 솔루션 정의 필드가 나타납니다. 기본값은 취약한 항목 할당입니다.

3. 저장을 클릭합니다.

에 대한 솔루션 정의 생성 및 교육 취약성 대응

를 사용하여 예측 인텔리전스에 대한 취약성 대응 솔루션 정의 모델을 만들고 교육합니다. 이 모델을 사용하여 기존 데이터를 기반으로 VI(취약한 항목) 또는 RT(정정 작업)에 대한 할당 그룹을 예측할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin

프로시저

1. 다음으로 이동 모두 〉 예측 인텔리전스 〉 분류 〉 솔루션 정의.
2. 분류 정의 양식에서 취약한 항목 할당을 클릭합니다.
   기본 솔루션 정의입니다.

   주:
   - 기본 교육 빈도는 30일입니다. 즉, 모델은 30일마다 구성된 필터 조건과 일치하는 VI 데이터 세트를 사용하여 자동으로 재교육합니다.
   - 취약한 항목 테이블의 필드를 교육에 사용할 수 있습니다. 기본 솔루션 정의는 두 개의 VI 필드인 **Vulnerability.Summary** 및 구성 항목에서 교육됩니다 **.** 이름. 조직의 취약성 소유권을 예측하는 데 유용한 필드에 따라 교육에 사용되는 필드를 사용자 지정할 수 있습니다.

3. 분류 솔루션을 만들고 교육하려면 Create and train a classification solution 항목을 참조하십시오.

   주:
   유사성 또는 클러스터링 솔루션을 생성하고 교육할 수도 있습니다. 자세한 내용은 다음을 참조하십시오.
   - 유사성 솔루션을 생성하고 교육합니다 .
   - 클러스터링 솔루션을 만들고 교육 합니다.

4. 업데이트 및 재교육을 클릭합니다.

   주:
   ML 솔루션에 대한 고급 설정을 구성하려면 ML 솔루션에 대한 고급 설정 구성을 참조하세요.

계산기 생성 취약성 대응

취약성 계산기는 특정 조건이 충족될 때 대상 필드를 계산하는 미리 정의된 수식입니다. 취약한 항목 위험 점수를 계산하는 계산기에는 위험 규칙이 포함될 수 있습니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)

가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

주:
스크립트가 포함된 취약성 계산기를 실행할 때 성능 저하가 발생할 수 있습니다.

가장 간단한 규칙을 먼저 실행하고 조건 및 템플릿 값 또는 위험 규칙으로 처리할 수 없는 항목에 대해서만 스크립트를 실행하도록 규칙의 순서를 지정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 〉 관리 〉 취약성 계산기.
2. 새로 만들기를 클릭합니다.
3. 양식의 필드에 적절히 입력합니다.

취약성 계산기 양식

필드	설명
이름	취약성 계산기의 이름입니다.
테이블	취약한 항목 테이블의 이름으로 자동으로 채워집니다.
애플리케이션	로 취약성 대응자동 채워집니다.
대상 필드	계산할 필드입니다.
설명	계산기에 대한 텍스트 설명입니다.
활성	계산기를 켜거나 끕니다.

4. 저장하려면 헤더를 마우스 오른쪽 버튼으로 클릭합니다.
   취약성 계산기 규칙 섹션이 나타납니다.
5. 새로 만들기를 클릭하여 계산기에 대한 규칙을 생성합니다.

   주:
   새 위험 규칙 양식(대상 필드가위험 점수인 경우에만 사용 가능)은 10단계를 참조하십시오.

6. 필드에 적절한 정보를 입력합니다.

취약성 계산기 규칙 양식

필드	설명
이름	계산기 규칙의 이름입니다.
순서	취약성 계산기를 실행하는 순서입니다. 주문 항목이 100인 계산기는 주문 항목이 200인 계산기 앞에 실행됩니다.
계산기	상위 계산기로 자동으로 채워집니다.
활성	기본적으로 활성 확인란이 선택되어 있으며, 이는 계산기 규칙이 활성 상태임을 의미합니다. 이 확인란의 선택을 취소하면 시스템에서 생성된 새로운 취약한 항목에 이 규칙이 적용되지 않습니다.
고급 뷰	이 옵션을 선택하면 조건 유형 및 값 유형에서 스크립팅된 조건 및 스크립팅된 값을 선택할 수 있습니다.

7. 이 조건이 충족되는 경우 탭의 필드에 적절한 정보를 입력합니다.

이 조건이 충족될 경우 탭

필드	설명
이름	계산기 규칙의 이름입니다.
순서	취약성 계산기를 실행하는 순서입니다. 주문 항목이 100인 계산기는 주문 항목이 200인 계산기 앞에 실행됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
계산기	상위 계산기로 자동으로 채워집니다.
활성	기본적으로 활성 확인란이 선택되어 있으며, 이는 계산기 규칙이 활성 상태임을 의미합니다. 이 확인란의 선택을 취소하면 시스템에서 생성된 취약한 항목에 이 규칙이 적용되지 않습니다.
고급 뷰	선택 시, 조건 유형 및 값 유형에서 스크립팅된 조건과 스크립팅된 값을 선택합니다.
조건 유형	고급 뷰를 선택한 경우에 사용할 수 있습니다. 선택 항목은 다음과 같습니다. ○ 필터: 필터 조건을 사용합니다. ○ 필터 그룹: 새 필터 그룹을 만들어 계산기 조건 정의 참조 ○ 스크립트: 이 계산기를 적용할 시기를 결정하는 데 사용되는 스크립트 조건입니다. 주: 계산기를 적용할 시기를 결정하기 위한 스크립트를 작성하기 전에 취약성 계산기 목록으로 돌아가십시오. 기본 시스템과 함께 제공된 취약성 계산기 기록을 살펴봅니다.
조건	계산기 사용 여부를 결정하는 기본 필터 조건을 정의합니다. 필터 그룹 또는 스크립트 조건 유형을 선택하면 이 필드가 숨겨집니다. 조건 작성기에 입력한 검색 텍스트의 대소문자 구분은 이 기록이나 양식에서 지원되지 않습니다.

8. 이 값 설정 탭을 클릭하고 양식의 필드에 적절한 정보를 입력합니다.

이 필드 탭 설정

필드	설명
값 유형	고급 뷰를 선택한 경우에 사용할 수 있습니다. 선택 항목은 다음과 같습니다. ○ 템플릿: 각 필드에 설정할 값을 정의합니다. ○ 스크립트: 각 필드의 값을 설정하는 데 사용됩니다.
스크립트 값	스크립트 값 유형을 선택한 경우 사용할 수 있습니다. 계산에 적용할 값을 정의합니다.
템플릿	계산기에 사용할 필드와 값을 선택합니다. 스크립트 값 유형 중 하나를 선택하면 이 필드가 숨겨집니다.

9. 모든 항목을 완료했으면 제출을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
기존 계산기를 편집하고 기존 점수를 모두 업데이트하려는 경우 계산기 다시 적용 버튼을 사용할 수 있습니다. 이는 모든 활성 취약한 항목(VI)에 실행되며, 계산기를 사용하여 값을 설정하는 경우 해당 VI의 값을 다시 계산합니다. 계산기를 다시 적용하는 데 시간이 오래 걸릴 수 있으므로 예약된 작업이 이를 처리합니다.

10. 새 위험 규칙 양식의 경우 필드에 적절한 정보를 입력합니다.

해당 값에서 가져와야 하는 결과의 백분율에 따라 각 가중치를 설정합니다. 스캐너가 제공하지 않는 데이터 또는 위험 점수의 일부가 아니어야 하는 데이터의 경우 가중치를 0으로 설정합니다.

필드를 추가, 삭제 또는 업데이트할 수 있습니다. 필드 값에 대한 가중치 백분율을 구성할 수도 있습니다. 자세한 내용은 Vulnerability Response 위험 계산기의 위험 규칙에 대한 필드와 가중치 정의 문서를 참조하십시오.

가중치를 업데이트하면 시나리오에 남은 가중치와 예상 위험 점수 결과가 표시됩니다.

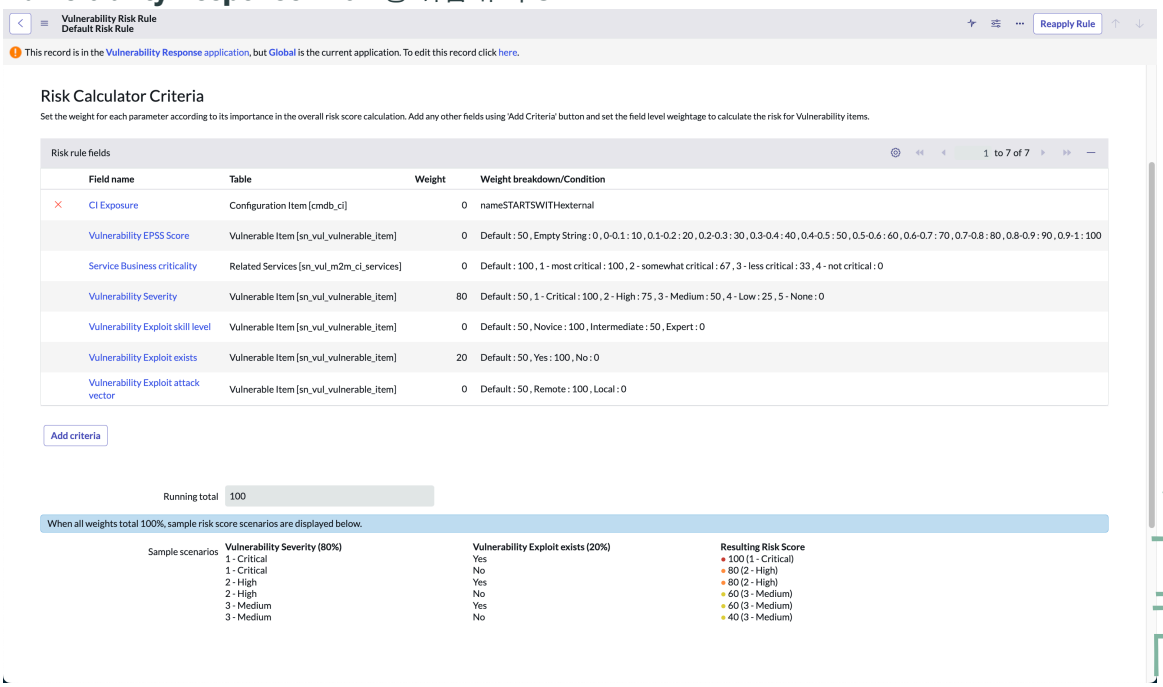
필드	설명
이름	계산기 규칙의 이름입니다.
순서	취약성 계산기를 실행하는 순서입니다. 주문 항목이 100인 계산기는 주문 항목이 200인 계산기 앞에 실행됩니다.
계산기	상위 계산기로 자동으로 채워집니다.
활성	기본적으로 활성 확인란이 선택되어 있으며, 이는 계산기 규칙이 활성 상태임을 의미합니다. 이 확인란의 선택을 취소하면 시스템에서 생성된 새로운 취약한 항목에 이 규칙이 적용되지 않습니다.
조건	계산기 사용 여부를 결정하는 기본 필터 조건을 정의합니다. 필터 그룹 또는 스크립트 조건 유형을 선택하면 이 필드가 숨겨집니다.
가중치	
취약성 심각도	심각도에서 비롯된 결과의 백분율입니다.
취약성 EPSS 점수	취약성이 악용될 확률입니다. 기본적으로 이 기준의 가중치는 0입니다. 위험 점수 계산에 이를 사용하려면 이 기준에 대해 적절한 가중치를 설정합니다.
익스플로잇 존재	익스플로잇 존재로 인한 결과의 백분율입니다. 이 정보가 취약성에 없으면 가중치를 0으로 설정합니다.
익스플로잇 기술 수준	익스플로잇에 필요한 기술 수준에서 비롯된 결과의 백분율입니다. 이 정보가 취약성에 없으면 가중치를 0으로 설정합니다.
익스플로잇 공격 벡터	공격의 대상에서 나온 결과의 백분율입니다. 이 정보가 취약성에 없으면 가중치를 0으로 설정합니다.
서비스 비즈니스 중요도	비즈니스 중요도에서 비롯된 결과의 백분율입니다. CI를 비즈니스 서비스에 연결하지 않은 경우 가중치를 0으로 설정합니다.
CI 노출	CI의 인터넷 접속 여부에서 비롯된 결과의 백분율입니다. 가중치가 0이 아닌 경우 인터넷에 연결된 CI를 정의하는 조건 필터가 나타납니다. 인터넷 연결 구성 항목을 선택하도록 필터를 설정합니다. 조건과 일치하는 기록을 미리 볼 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
누계	자동 계산된 백분율 합계. 이 값이 100에 도달하면 시나리오 미리 보기에 여러 시나리오의 샘플 위험 점수가 표시됩니다.
위험 점수 시나리오	모든 가중치의 합계가 100%이면 위험 점수 시나리오가 표시되어 일부 가능한 시나리오에서 위험 점수의 미리 보기를 제공합니다.

포함된 목록을 사용하여 기준을 추가 또는 제거하고 각 기준의 가중치를 조정할 수 있습니다.

Vulnerability Response v20.x용 위험 규칙 **CI**



11. 제출을 클릭합니다.

사용하지 않는 경우 기본 취약성 계산기 사용 안 함

취약성 계산기를 사용하지 않는 경우 정의한 다른 계산기 외에 기본 계산기를 비활성화합니다. 취약성 계산기는 취약한 항목 기록이 생성되거나 업데이트될 때마다 실행되며 초기 임포트 성능에 영향을 줄 수 있습니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 취약성 계산기.

2. 관련 계산기를 엽니다.

3. 계산기를 비활성화하려면 활성 확인란의 선택을 취소합니다.

4. 업데이트를 클릭합니다.

자동 삭제 규칙 생성, 활성화 또는 수정 취약성 대응

VI(취약성 항목) 삭제 및 RT(정정 작업) 삭제 규칙을 생성, 사용 또는 수정할 수 있습니다. 자동 삭제를 사용하여 VI 및 RT 테이블에서 이전 기록을 제거합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에

가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

필요한 역할:

- 관리자: 자동 삭제 규칙 수정
- sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음): 자동 삭제 모듈 보기

이 태스크 정보

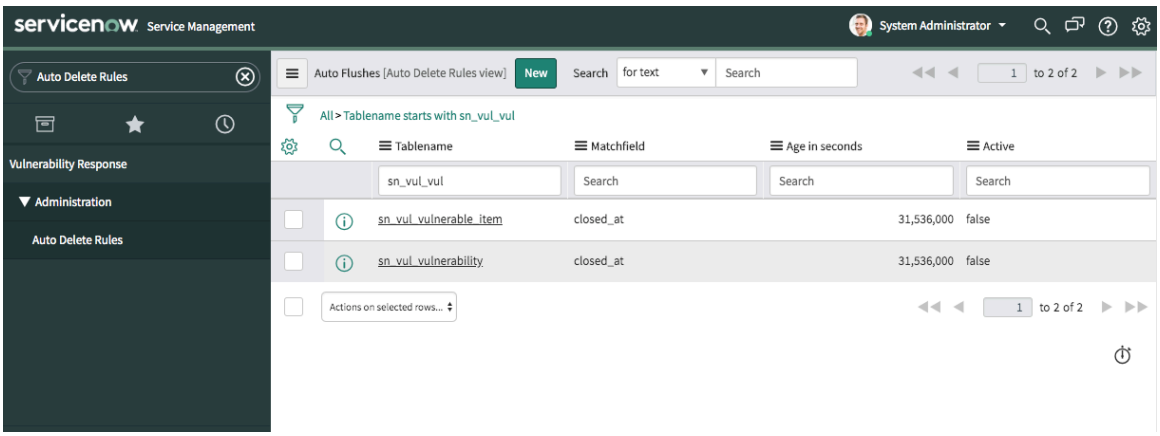
시간이 지남에 따라 많은 양의 종결된 기록이 인스턴스의 VI 및 VUL 테이블에 누적될 수 있습니다. 이러한 기록 중 상당수는 365일 이상 종결되었지만 제거되지 않았을 수 있습니다. 자동 삭제 규칙을 사용하여 오래되고 종결된 기록을 다수 제거합니다. 이러한 레코드를 제거하면 VI 및 VUL 테이블의 레코드 수가 크게 줄어들 뿐만 아니라 삭제해도 높은 성능을 유지하는 데 도움이 됩니다.

자동 삭제는 기본적으로 365일 동안 종결된 레코드를 대상으로 하지만 첫 번째 실행에서 단일 트랜잭션에서 너무 많은 레코드를 제거하려고 시도할 수 있습니다. 환경의 크기에 따라 삭제 프로세스를 엇갈리게 하여 쿼리 범위를 제한할 수 있습니다. 예를 들어, 450일이 지난 종결된 기록에 대해 첫 번째 실행을 시작할 수 있습니다. 실행이 완료된 후에는 365일이 지난 레코드 수를 줄일 때까지 더 작은 증분(425, 400, 375)으로 작업을 줄일 수 있습니다.

지정된 조건을 충족하는 종결된 기록을 이를 참조하는 기록과 함께 자동으로 삭제하는 두 가지 규칙이 제공됩니다 ServiceNow AI Platform# . 한 규칙은 취약한 항목을 삭제하고 다른 규칙은 정정 작업을 삭제합니다. 기본적으로 이러한 자동 삭제 규칙은 사용하지 않도록 설정되어 있으므로 기록을 삭제하기 전에 수동으로 활성화해야 합니다. 인스턴스와 함께 제공되는 미리 구성된 규칙 2개를 선택하거나 직접 만들 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 자동 삭제 규칙.
   목록 뷰가 표시됩니다.

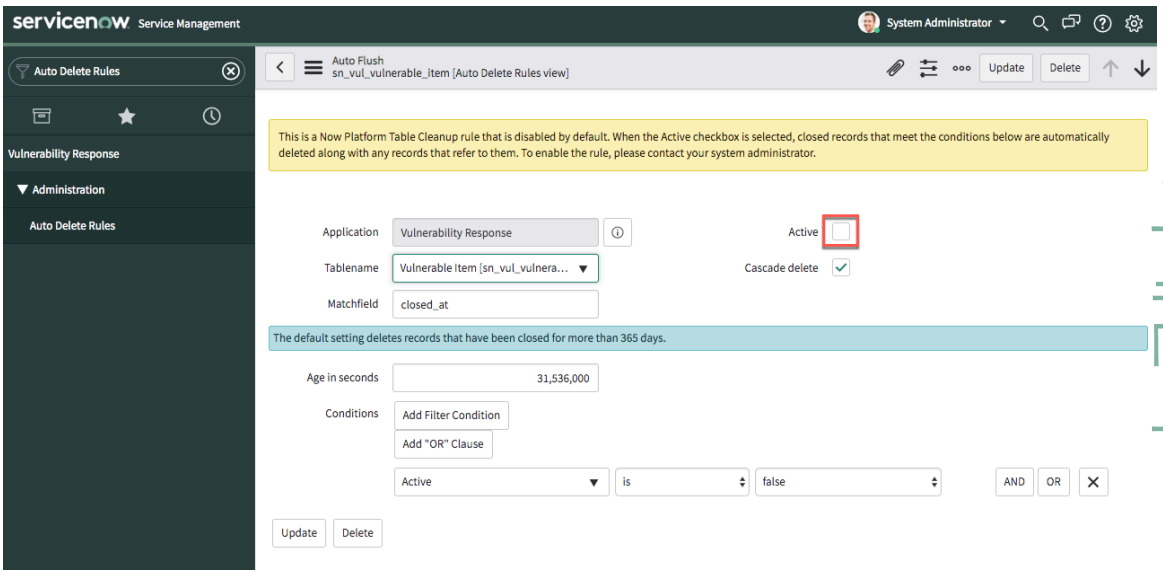


2. 편집하려면 취약한 항목에 대한 삭제 규칙(sn_vul_vulnerable_item) 또는 정정 작업에 대한 규칙(sn_vul_vulnerability)을 선택합니다.
3. 새 규칙을 만들려면 새로 만들기를 클릭합니다.
4. 양식의 필드를 적절하게 입력하거나 편집합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
애플리케이션	기록이 삭제되고 있는 애플리케이션의 이름입니다. 기본값은 취약성 대응입니다.
Tablename	규칙이 적용되는 테이블의 이름입니다.
필드 연결	시스템에서 기간을 모니터링하는 필드입니다.
활성	규칙을 활성화하기 위한 옵션입니다. 활성화되면 기록을 삭제할 수 있습니다.
단계적 삭제	일치하는 모든 기록과 이를 참조하는 모든 기록을 삭제하는 옵션입니다. 이 옵션을 선택하지 않으면 일치하는 기록만 삭제되고 이를 참조하는 기록은 삭제되지 않습니다.
기간(초)	삭제할 취약성 기록의 기간입니다. VI 규칙과 RT 규칙 모두 사용 기간은 365일입니다. 이 기간은 초 단위로 표시됩니다.
조건	규칙이 적용되는 VI 및 RT(VUL) 테이블의 기록을 정의하는 필터 조건입니다.

5. 활성 확인란을 선택하여 규칙을 활성화합니다.



규칙이 활성화되면 시간별 플랫폼 기능인 자동 플러시가 규칙이 활성화된 테이블에서 해당 기록을 삭제합니다.

환경에 삭제 기준과 일치하는 수백만 또는 수천만 개의 레코드가 있는 경우 자동 삭제 규칙을 사용하도록 설정하기 전에 고객 지원에 문의하여 ServiceNow 단계별 프로세스를 사용하여 기록을 삭제할 수 있습니다.

취약성 대응 홈페이지에 취약성 유의성 차트 추가

취약성 유의성 정의 차트와 기타 시각화를 개요에 추가할 수 있습니다.

시작하기 전에

- 가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

- 취약성 분석 플러그인을 활성화해야 합니다.

필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 개요.
   일부 보고서는 기본적으로 대시보드에 추가됩니다. 이러한 보고서에 대한 자세한 내용은 다음 문서를 참조하십시오 기본 취약성 대응 대시보드 사용.
2. 대시보드 헤더 근처에서 카드 뷰 아이콘 + 클릭합니다. 콘텐츠 추가 대화 상자를 열고 위젯을 더 추가합니다.
3. 위젯 추가 대화 상자의 목록에서 보고서를 선택하여 더 많은 취약성 대응 보고서를 표시합니다.
4. 화면에서 게이지를 추가할 위치를 클릭합니다.
5. 콘텐츠 추가 상자를 닫습니다.

이메일 알림 정의 취약성 대응

가양성 요청 승인 및 거부와 같은 중요한 업데이트 및 활동에 대한 유용한 정보를 공유하도록 이메일 알림을 설정합니다. 이메일 알림을 생성하려면 알림 전송 시기, 받는 사람 및 포함된 항목 지정이 포함됩니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 이메일 템플릿.
2. 새로 만들기를 선택합니다.

   이메일 알림 생성에 대한 자세한 지침은 다음 문서를 참조하십시오 Create an email notification .

결과
수신자가 이메일 알림의 링크를 클릭하면 역할에 따라 OR IT 정정 작업 공간 에서 취약성 관리자 작업 공간 링크가 열립니다.

- 역할이 있는 사용자(sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin)에 대해 링크가 열립니다 취약성 관리자 작업 공간 .
- 역할이 있는 사용자에 대해 sn_vul.remediation_owner 에서 링크가 열립니다 IT 정정 작업 공간 .

수신자에게 위의 역할이 없는 경우 이메일 알림의 링크가 클래식 UI에서 열립니다.

이메일 템플릿 정의 취약성 대응

이메일 알림을 생성하려면 알림 전송 시기, 받는 사람 및 포함된 항목 지정이 포함됩니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 〉 관리 〉 이메일 템플릿.
2. 새로 만들기를 선택합니다.

   이메일 템플릿 생성에 대한 자세한 지침은 다음 문서를 참조하십시오 Construct an email message with a template .

정정 대상 알림 만들기 또는 편집

취약성 관리자는 정정 대상 알림을 편집하거나 새로 추가하여 알림 전송 시기, 알림 수신자, 알림의 내용을 지정할 수 있습니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 알림.
2. 정정 대상 알림 기록을 선택하거나 새로 만들기를 선택합니다.
3. 양식의 필드에 적절한 정보를 입력합니다.
   양식 필드에 대한 자세한 내용은 Create an email notification 문서를 참조하십시오.
4. 메시지를 보려면 알림 미리 보기를 선택합니다.

결과
v21.0 of 취약성 대응부터 수신자가 이메일 알림의 링크를 클릭하면 역할에 따라 기록이 OR IT 정정 작업 공간 에서 취약성 관리자 작업 공간 열립니다.

- 역할이 있는 사용자(sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin)에 대해 링크가 열립니다 취약성 관리자 작업 공간 .
- 역할이 있는 사용자에 대해 sn_vul.remediation_owner에서 링크가 열립니다 IT 정정 작업 공간 .

수신자에게 위의 역할이 없는 경우 이메일 알림의 링크가 클래식 UI에서 열립니다.

취약성 노출 평가 구성

취약성 노출 평가 애플리케이션을 사용하여 취약한 소프트웨어에 대한 자산의 제로 데이(현재 날짜) 노출을 평가합니다.

> **중요사항:**
> CVE(Common Vulnerabilities and Exposures) 및 소프트웨어별로 노출 평가를 수행하여 취약성 평가 작업 공간의 추가 기능을 활용할 수 있습니다. 자세한 내용은 취약성 평가 작업 공간 탐색 문서를 참조하십시오.

필요한 역할: 관리자

호환성 및 시스템 요구 사항

취약성 대응 응용 프로그램은 에서 사용할 수 있습니다ServiceNow Store. (SAM) Foundation 애플리케이션 〔com.snc.asset_management〕이 소프트웨어 자산 관리 애플리케이션의 일부로 취약성 대응 설치됩니다. 애플리케이션이 인스턴스에 설치되었는지 확인하려면 SAM Foundation 시스템 애플리케이션 〉 모든 사용 가능 애플리케이션 〉 모두 # #### com.snc.asset_management 검색합니다. 애플리케이션이 설치되지 않은 경우 설치를 선택합니다. SAM Foundation에 대한 자세한 내용은 Software Asset Management Foundation plugin 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약성 노출 평가 애플리케이션을 사용하려면 인스턴스의 자산 데이터에 ServiceNow AI Platform# 액세스해야 하므로 자산 관리 애플리케이션에는 참조할 데이터가 있어야 합니다. 소프트웨어 검색 모델 테이블 [cmdb_sam_sw_discovery_model] 및 소프트웨어 설치 〔cmdb_sam_sw_install〕에는 데이터가 필요합니다.

Vulnerability Exposure Assessment 애플리케이션은SAM Pro 애플리케이션 또는 SAM Pro ServiceNow AI Platform# 애플리케이션에서도 SAM Foundation 작동합니다. SAM Pro 애플리케이션은 핵심 취약성 대응ServiceNow Store 제품에 속하지 않으며 별도의 구독이 필요합니다.

주:
SAM Pro 애플리케이션은 더 나은 결과를 얻을 수 있는 콘텐츠 라이브러리에만 필요합니다.

의 취약성 대응v23.0부터 Pro 또는 Enterprise 구독이 있는 경우 모두 메뉴에서 노출 평가 링크를 클릭하면 역할에 따라 작업 공간의 노출 평가 페이지로 리디렉션됩니다.

작업 공간에서 노출 평가 페이지 액세스

역할	작업 공간
취약성 매니저	취약성 관리자 작업 공간
이벤트 관리자 〔sn_vul_analyst.vul_event_manager〕 또는 긴급 대응 〔sn_vul_analyst.emergency_response〕	취약성 평가 작업 공간

작업 공간으로 리디렉션되지 않고 클래식 노출 평가 페이지에 남아 있으려면 모듈 - 노출 평가 페이지의 링크 유형 탭에서 링크 유형을기록 목록으로 설정합니다. 모두 메뉴의 노출 평가 링크 옆에 있는 모듈 편집 아이콘을 선택하여 모듈 - 노출 평가 페이지에 액세스할 수 있습니다.

취약성 쓰기 역할 〔sn_vulnerability_write〕을 사용하면 노출 평가 모듈을 보고 애플리케이션을 사용하여 취약성 대응 인스턴스의 취약한 소프트웨어에 대한 요청 시 노출 평가 기록을 만들고 편집할 수 있습니다.

관련 정보

취약한 소프트웨어에 대한 노출 평가

에 대한 예외 관리 구성 취약성 대응

조직이 게시된 취약성 관리 또는 보안 정책, 표준 또는 가이드라인을 준수할 수 없는 경우 예외를 요청할 수 있습니다. 예외 관리에는 정책에 따라 정정할 수 없는 VI(취약한 항목) 또는 RT(정정 작업)에 대한 예외를 요청, 검토, 승인 또는 거부하는 작업이 포함됩니다.

시작하기 전에
모듈을 사용하여 취약성 대응 요청된 예외의 기간을 제한하고 예외 또는 긍정 오류 요청에 질문서를 추가합니다. 기본적으로, 예외를 설정하면 모듈을 사용하여 요청됩니다 ServiceNow# 취약성 대응 . 통합을 사용하여 예외를 요청할 수도 있습니다 GRC: 정책 및 준수 관리 .

가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

필요한 역할: sn_vul.manage_exception_configuration

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보
가 활성화된 경우 취약성 대응 예외를 요청할 수 있는 기간을 제한할 수 있습니다. 마찬가지로 모듈이 설치되어 있으면 GRC: 정책 및 준수 관리 구성 화면에서 선택할 GRC: 정책 및 준수 관리 수 있습니다. 이 옵션을 사용하면 에서 정책 및 제어 목표를 GRC지정하는 예외를 요청할 수 있습니다.

질문서를 추가하면 예외 또는 긍정 오류 요청을 제기하는 사람에게 전송됩니다. 기본 질문서를 사용하거나 요구 사항에 따라 만들 수 있습니다.

예외 승인자가 예외를 요청하는 이유를 이해하는 것이 좋습니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 예외 관리.
2. 예외 관리 구성 양식의 다음을 사용하여 예외 관리 목록에서 옵션을 선택하여 예외를 관리할 방법을 선택합니다.
   또는 GRC: 정책 및 준수 관리를 선택할 취약성 대응 수 있습니다. 예외를 요청하는 데 사용할 GRC: 정책 및 준수 관리 플러그인을 활성화해야 GRC 합니다. 구성을 변경해도 기존 데이터에는 영향을 주지 않습니다.
3. 옵션을 선택한 취약성 대응 경우 다음 정보를 입력합니다.

VR 예외 관리 설정 양식

필드	설명
지속 시간	예외를 요청할 수 있는 기간입니다.
단위	지정된 기간의 시간 단위입니다.
예외를 요청하려면 질문서 사용	제기 중인 예외 요청에 질문서를 추가하는 옵션입니다.
예외를 요청하기 위한 질문서	예외를 요청하기 위해 선택한 질문서가 표시됩니다. 예외 질문서가 기본적으로 표시됩니다. 주: 이 필드는 예외를 요청하기 위해 질문서 사용 확인란을 선택한 경우에만 나타납니다.
보상 통제에 대한 질문서	정정 소유자가 위험 감소 요청에 대해 대답해야 하는 질문서를 표시합니다. 의 취약성 대응v20.0부터 리스크 경감 요청에 대한 설문지를 설정할 수 있습니다. 기본적으로 보상 통제 질문서가 선택됩니다. 주: 이 필드는 예외를 요청하기 위해 질문서 사용 확인란을 선택한 경우에만 나타납니다.
긍정 오류로 표시하려면 질문서 사용	제기 중인 긍정 오류 요청에 질문서를 추가하는 옵션입니다.
긍정 오류를 표시하기 위한 질문서	긍정 오류로 표시하기 위해 선택한 질문서를 표시합니다. 긍정 오류 요청에 대한 질문서가 기본적으로 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	주: 이 필드는 긍정 오류로 표시하려면 질문서 사용 확인란을 선택한 경우에만 나타납니다.

기존 질문서를 사용자 지정하고 v20.0으로 업그레이드한 경우, 기본 보상 통제 질문서 대신 위험 감소 요청에 대해 이 사용자 지정 질문서가 나타납니다.

4. 옵션을 선택한 GRC: 정책 및 준수 관리 경우 다음 정보를 입력합니다.

VR 예외 관리 설정 양식

필드	설명
긍정 오류로 표시하려면 질문서 사용	제기 중인 긍정 오류 요청에 질문서를 추가하는 옵션입니다.
긍정 오류를 표시하기 위한 질문서	긍정 오류로 표시하기 위해 선택한 질문서를 표시합니다. 긍정 오류 요청에 대한 질문서가 기본적으로 표시됩니다.

5. 예외 요청 및 긍정 오류 요청에 대한 조건에 따라 질문서를 구성하려면 다음을 수행합니다.

   a. VR 질문서 구성 섹션에서 새로 만들기를 선택합니다.

   b. 질문서 구성 - 새 기록 양식에서 필드에 내용을 입력하고 제출을 선택합니다.
   질문서 구성 양식 필드에 대한 자세한 내용은 다음 문서를 참조하십시오 질문서 구성 양식 필드.
   생성된 질문서는 VR 예외 관리 설정 양식의 VR 질문서 구성 섹션에 나타납니다.

   예를 들어 중요한 취약한 항목에 대한 가양성 요청에 대한 질문서를 구성하려면 취약한 항목 승인 규칙에 대한 가 양성 규칙을 선택하고 `## ### 1 - ####` 조건을 제공하고 질문서 구성 양식에서 원하는 질문서를 선택합니다.

6. 저장을 선택합니다.

예외 승인자 추가

예외를 요청할 수 있도록 승인자 그룹에 사용자를 추가합니다.

시작하기 전에
가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

필요한 역할: sn_vul.exception_approver

이 태스크 정보
v14.0까지는 취약성 대응 취약한 항목 또는 정정 작업에 대한 예외요청이 기본 2단계 승인 워크플로우를 사용하여 승인됩니다. 요청은 두 가지 수준의 승인자가 승인해야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
v14.0까지는 취약성 대응 첫 번째 수준 승인자가 없으면 예외를 요청할 수 없습니다. 그러나 v15.0부터 취약성 대응 VR 애플리케이션을 처음 배포하는 경우 예외 관리용 플로우 디자이너가 기본적으로 활성화됩니다. 워크플로우를 이미 사용 중인 경우 플로우 디자이너로 업데이트할 수 있습니다. 두 경우 모두 다시 워크플로우로 변경할 수 없습니다. 예외 관리 및 가양성에 대한 승인 규칙을 구성하려면 문서를 참조하십시오 예외 관리에 대한 승인 규칙 구성.

프로시저

1. 다음으로 이동 모두 〉 사용자 관리 〉 그룹.
2. 이름 열에서 예외를 검색하고 예외 승인자 - 수준 1을 클릭합니다.

주:
v12.8.1부터 취약성 대응 시스템 속성〔sys_properties〕 테이블의 워크플로우를 통해 예외 승인을 위해 기본 시스템에 제공된 시스템 속성을 사용할 수 있습니다. 따라서 워크플로우를 통해 예외 또는 가양성 요청이 발생하면 승인을 위해 시스템 속성에 정의된 그룹 ID로 전송됩니다. 다음으로 이동 모두 〉 시스템 속성 및 , *sn_vul.exception_approver_L2*, 또는 *sn_vul.false_positive_approver_group* 을 선택하여 *sn_vul.exception_approver_L1*속성 값을 변경합니다.

3. 그룹 예외 승인자 - 수준 1 양식에서 그룹 구성원 관련 목록을 클릭합니다.
4. 새로 만들기를 클릭하여 목록을 만듭니다.
5. 양식에서 필드를 채웁니다.

사용자 양식

필드	설명
사용자 ID	사용자의 고유 식별자입니다.
이름	사용자의 이름입니다.
성	사용자의 성입니다.
직위	사용자의 직함입니다. 직함 또는 직무 설명을 입력하거나 목록에서 선택합니다.
부서	사용자의 부서입니다.
암호	사용자에게 할당된 암호입니다. 이 암호는 영구적이거나 임시적일 수 있습니다.
암호 다시 설정 필요	사용자가 보안을 보장하기 위해 암호를 재설정할 수 있도록 하는 옵션입니다.
잠겨 있음	사용자를 인스턴스에서 잠그고 사용자의 모든 활성 세션을 종료하는 옵션입니다. 시스템은 관리자 역할을 가진 사용자가 자신을 잠그는 것을 방지합니다.
활성	이 사용자를 활성화하는 옵션입니다. 다음 영역에서는 비활성 사용자만 볼 수 있습니다. ○ 사용자 목록 ○ 참조 필드의 선택 목록(돋보기 아이콘) ○ 참조 필드에 입력할 때 나타나는 자동 완성 목록

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
웹 서비스 접근만 허용	이 사용자를 비대화형 사용자로 지정하는 옵션입니다.
내부 통합 사용자	이 사용자를 내부 통합 사용자로 지정하는 옵션입니다.
이메일	사용자의 이메일 주소입니다.
언어	사용자의 기본 설정 언어입니다.
달력 통합	작업 일정을 관리하는 데 사용되는 달력입니다. 예를 들어 Outlook입니다.
시간대	이 사용자의 위치에 대한 시간대입니다.
날짜 형식	사용자가 선호하는 날짜 형식입니다.
직장 전화번호	사용자의 직장 전화 번호입니다.
휴대폰	사용자의 휴대폰입니다.
사진	추가하려면 클릭...을 클릭하여 업로드할 수 있는 사진입니다.

6. 제출을 클릭합니다.
7. 1-5단계를 반복하여 예외 승인자 - 수준 2를 생성합니다.
   승인자는 취약성 대응 〉 내 승인 으로 이동하여 요청을 승인해야 합니다.

> **주:**
> 에 대한 GRC: 정책 및 준수 관리예외를 승인하려면 정책 및 준수 관리 선택적 설정을 참조하십시오.

예외 관리에 대한 승인 규칙 구성

v15.0부터 취약성 대응 플로우 디자이너를 사용하여 예외 관리, 예외 규칙 및 긍정 오류 관리에 대한 예외 요청을 승인합니다. 처음 배포 취약성 대응 (VR)하는 경우 Flow Designer가 기본적으로 활성화됩니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin

이 태스크 정보
기존 VR 사용자인 경우 기본 옵션은 워크플로우입니다.
v15.0 이상을 배포 취약성 대응 한 경우 시스템 속성의 *sn_vul.flow_designer_activation* 값이 true로 설정됩니다. 즉, Flow Designer가 기본적으로 활성화됩니다.

v15.0 이전 버전을 이미 사용 취약성 대응 중인 경우 이 시스템 속성의 값은 false로 설정됩니다. 값을 true로 변경하여 플로우 디자이너를 활성화할 수 있습니다.

> **주:**
> Flow Designer를 활성화한 후에는 워크플로우 사용으로 되돌릴 수 없습니다. 워크플로우와 Flow Designer를 자세히 비교하려면 다음 항목을 참조하십시오 예외 관리 워크플로우와 Flow Designer 비교.

플로우 디자이너를 사용하려면 승인 규칙 모듈을 사용하여 규칙을 생성합니다. 이 모듈을 사용하여 다음의 각 예외 관리 워크플로우에 대한 승인 규칙을 구성할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 정정 작업에 대한 예외 요청
- 취약한 항목에 대한 예외 요청
- 예외 규칙
- 정정 작업에 대한 긍정 오류
- 취약한 항목에 대한 가양성

주:
규칙 내에 여러 수준의 승인을 포함하는 조건을 정의할 수도 있습니다. Flow Designer는 이 모듈에서 생성된 규칙을 자동으로 상속하고 일치하는 승인 워크플로우를 처리합니다. 승인 수준 구성에 대한 자세한 내용은 다음 문서를 참조하십시오 예외 관리에 대한 승인 수준 생성.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 승인 규칙.
2. 승인 규칙 페이지에서 승인 규칙을 설정할 그룹을 선택합니다.
3. 양식에서 필드를 채웁니다.

승인 규칙 양식

필드	설명
이름	승인 구성 이름입니다.
테이블	규칙이 적용되는 테이블입니다.
애플리케이션	기본값은 취약성 대응입니다.
규칙 유형	규칙 유형을 지정합니다. 예를 들어 예외 관리, 가양성 또는 예외 규칙이 있습니다.
활성	기본적으로 활성화되며, 승인 규칙이 사용 중임을 나타냅니다.
설명	승인 규칙에 대한 간단한 설명입니다.
승인 만료Y (일) v21.0 of 취약성 대응	승인자가 요청을 승인할 수 있을 때까지의 날짜입니다.
승인자에게 알림(일) v21.0 of 취약성 대응	승인자에게 조치를 취하라는 알림이 전송된 날짜입니다.

4. 업데이트를 선택합니다.
승인 구성 탭에는 기본적으로 두 가지 수준의 승인자가 설정됩니다. 규칙을 선택하여 규칙 내의 다양한 사용 사례를 기반으로 조건을 정의할 수 있습니다. 자세한 내용은 승인 규칙에 대한 구성 생성 문서를 참조하십시오.

주:
각 구성 페이지에서 여러 승인 수준을 생성할 수 있습니다. 자세한 내용은 예외 관리에 대한 승인 수준 생성 문서를 참조하십시오.

Example:
다양한 사용 사례를 기반으로 서로 다른 구성 항목에서 발견된 동일한 취약성에 대해 서로 다른 승인 프로세스를 정의할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

승인 규칙에 대한 구성 생성

승인 수준에 대해 일치하는 취약한 항목, 정정 작업 또는 예외 규칙을 필터링하는 조건을 정의합니다.

시작하기 전에

필요한 역할: sn_vul.vulnerability_admin

이 태스크 정보

승인 구성 모듈에서 서로 다른 구성에 대해 여러 수준의 승인을 구성할 수 있습니다. 각 규칙에 여러 수준의 승인이 포함된 조건 기반 규칙을 정의합니다.

주:
승인 규칙 모듈을 사용하여 예외 관리 워크플로우에 대한 승인 규칙을 구성합니다. 승인 규칙 구성에 대한 자세한 내용은 문서를 참조하십시오 예외 관리에 대한 승인 규칙 구성.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 승인 규칙.
2. 승인 규칙을 선택하고 승인 구성 탭으로 이동합니다.
3. 구성을 선택합니다.
4. 양식에서 필드를 채웁니다.

승인 구성 양식

필드	설명
이름	승인 구성 이름입니다.
승인 규칙	승인 규칙에 대한 테이블 및 유형 상세 정보를 포함합니다.
순서	규칙 내에서 다양한 구성의 실행 순서입니다. 예를 들어 주문 항목이 100인 구성은 주문 항목이 200인 구성보다 먼저 실행됩니다.
활성	기본적으로 활성화되며, 승인 구성이 사용 중임을 나타냅니다.
설명	승인 구성 수준에 대한 짧은 설명입니다.

5. 다음 방법 중 하나로 취약한 항목 또는 정정 작업에 대한 조건을 설정합니다.

필드	설명
조건	일치하는 취약한 항목 또는 정정 작업을 식별합니다.
고급 조건	취약한 항목 또는 정정 작업에 대한 조건을 정의하는 스크립트입니다. **주:** 이 필드는 고급 확인란을 선택할 때 나타납니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

6. 업데이트를 선택합니다.
   규칙 내에서 여러 수준의 승인을 포함하는 조건을 정의할 수 있습니다. Flow Designer는 이 모듈에서 생성된 규칙을 자동으로 상속하고 일치하는 승인 워크플로우를 처리합니다. 승인 수준 구성에 대한 자세한 내용은 다음 문서를 참조하십시오 예외 관리에 대한 승인 수준 생성.

Example:
다음에 대해 서로 다른 승인 경로를 정의할 수 있습니다.

- 예 1: 다양한 유형의 취약성 또는 구성 항목(인터넷 연결 또는 내부).
- 예 2: 업데이트 적용 소유자가 호스트 취약한 항목(VIT) 또는 업데이트 적용 작업(VUL)에 대해 이러한 요청을 동시에 제기하는 경우 지연 및 위험 감소 요청.

  변경 승인 열에는 지연 상태 변경 승인 기록이 있습니다. 조건 작성기를 사용하여 변경 승인 열에서 조건을 설정하면 지연 승인 기록이 고려되지만 위험 감소 승인 기록은 고려되지 않습니다. 따라서 위험 감소 상태 변경 승인 기록에 조건을 설정하려면 고급 조건 필드를 사용합니다.

  취약한 항목에 대한 예외 요청 승인 규칙의 경우 중간에서 낮음까지의 위험 등급 요청 승인 구성이 기본 시스템과 함께 제공됩니다. 이 구성은 기본적으로 false로 설정됩니다. 이 구성을 사용하여 위험 감소 요청에 대한 승인 경로를 중간에서 낮음으로 설정할 수 있습니다. 위험 감소 요청의 다양한 위험 등급 변경에 적용할 수 있도록 이 구성의 스크립트를 업데이트할 수도 있습니다.

  중간에서 낮음까지의 위험 등급 요청 구성:

```
function evaluate() {
   var gr = new GlideRecord("sn_vul_change_approval");
   gr.addQuery("sys_id", approval);
   gr.addQuery("current_value", "3 - Medium");
   gr.addQuery("desired_value", "4 - Low");
   gr.query();
   if (gr.next()) {
      return true;
   }
   return false;
}
evaluate();
```

  가장 낮은 순서로 이전 구성을 true로 설정하고 **VI** 구성에 대한 기본 구성 **-** 예외 요청을 true로 설정합니다.

  결과: 정정 소유자가 IT 정정 작업 공간에서 동시에 지연 및 위험 감소 요청을 제기하면 지연 승인 요청이 VI에 대한 기본 구성 **-** 예외 요청에 정의된 승인자에게 리디렉션되고 위험 감소 승인 요청이 중간에서 낮음까지의 위험 등급 요청에 정의된 승인자에게 리디렉션됩니다.

예외 관리에 대한 승인 수준 생성

예외 요청을 승인할 사용자 및 사용자 그룹의 수준을 정의합니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 승인 규칙.
2. 승인 규칙을 선택하고 승인 구성 탭으로 이동합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 구성을 선택합니다.
4. 승인자 수준 섹션에서 승인자 수준을 선택합니다.
5. 양식에서 필드를 채웁니다.

승인자 수준 양식

필드	설명
이름	승인 수준 이름입니다.
필요한 승인	선택한 수준에 필요한 승인 수를 선택합니다. ○ 승인자 1명 필요 ○ 모든 사용자의 승인 필요
활성	기본적으로 활성화되며, 승인 수준이 사용 중임을 나타냅니다.
순서	규칙 내에서 다양한 구성의 실행 순서입니다. 예를 들어 주문 항목이 100인 구성은 주문 항목이 200인 구성보다 먼저 실행됩니다.
승인 규칙	승인 규칙에 대한 테이블 및 유형 상세 정보를 포함합니다.
승인 구성	승인 구성을 포함합니다.
할당 사용	다음 옵션 중에서 선택합니다. ○ 사용자 및 사용자 그룹 ○ 승인 테이블 필드 ○ 스크립트
그룹	여러 사용자로 구성된 승인자 수준 그룹입니다. 사용자에게 다음 역할 중 하나가 있어야 합니다. ○ sn_vul.exception_approver: 예외 관리 및 예외 규칙의 경우 ○ sn_vul.false_positive_approver: 긍정 오류에 대해
사용자	그룹에 나열된 사용자를 편집합니다.

6. 변경 내용을 저장하려면 업데이트를 선택합니다.

주:
v15.0 이전에는 예외 수준 1에만 사용자가 있는 경우 워크플로우 프로세스가 작동합니다. 단, v15.0부터는 각 레벨에 최소 한 명의 사용자가 있어야 합니다.

v15.0 이전에는 워크플로우에서 두 번째 수준에 사용자가 없으면 취약성 항목 또는 취약한 그룹이 지연되었습니다. 그러나 v15.0 이상에서는 두 번째 수준에 사용자가 없으면 승인 요청이 자동으로 거부됩니다.

Example:
Linux 및 Windows 서버의 취약성에 대한 승인 수준은 다를 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예외 관리 워크플로우와 **Flow Designer** 비교

취약성 대응 v15.0부터 처음 배포 취약성 대응 (VR)하는 경우 예외 관리에서 예외 요청을 승인하기 위한 플로우 디자이너가 기본적으로 활성화됩니다. 기존 VR 사용자인 경우 기본 옵션은 워크플로우입니다.

주:
v19.0부터 취약성 대응 는 신규 고객에게는 Flow Designer만 지원됩니다. 기존 사용자가 v19.0으로 취약성 대응 업그레이드하면 Flow Designer와 예외 관리 워크플로우가 모두 지원됩니다.

워크플로우와 **Flow Designer** 비교

고려 사항	워크플로우	**Flow Designer**
버전	의 v15.0 취약성 대응이전.	의 v15.0 취약성 대응부터 시작합니다.
기본 옵션	기존 VR 사용자인 경우 기본 옵션입니다.	v15.0부터 새 VR 사용자를 위한 기본 옵션입니다.
승인 프로세스 설정	예외 관리에는 예외 규칙과 함께 예외 요청 및 긍정 오류 요청이 포함됩니다.	다양한 수준을 정의하고 다양한 사용 사례에 대해 서로 다른 승인자를 추가하는 작업이 포함됩니다. 워크플로우보다 구현하기 쉽습니다. 예외 관리에는 예외 규칙과 함께 예외 요청 및 긍정 오류 요청이 포함됩니다.
Flow Designer로 업그레이드	워크플로우에서 Flow Designer로 업그레이드할 수 있습니다. 그러나 기존 요청은 워크플로우를 사용해야만 승인할 수 있습니다.	플로우 디자이너는 기본적으로 활성화되어 있습니다.
시스템 속성 *sn_vul.flow_designer_activated*	v15.0 이전의 예외 관리에 워크플로우를 사용한 경우 시스템 속성이 false로 설정됩니다. 플로우 디자이너를 활성화하려면 이 속성을 true로 설정합니다. **주:** Flow Designer를 활성화한 후에는 워크플로우 사용으로 되돌릴 수 없습니다.	v15.0 이상에서 VR을 처음 사용하는 경우 시스템 속성 값은 기본적으로 true로 설정됩니다.
승인 규칙 모듈	시스템 속성을 true로 설정하면 모듈 승인 규칙 사용 예약된 작업이 24시간 이내에 실행됩니다. 이 예약된 작업은 승인 규칙 모듈을 활성화합니다. 이 모듈을 즉시 활성화하려면 이 작업을 수동으로 실행하십시오.	VR v15.0에서 VR을 처음 배포한 경우 기본적으로 이 모듈을 사용할 수 있습니다.
승인 수준	승인자 수준을 두 개만 설정하는 옵션을 제공합니다.	원하는 수의 구성 및 승인자 수준 설정 및 각 규칙에 대한

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

워크플로우와 **Flow Designer** 비교

고려 사항	워크플로우	**Flow Designer**
		승인자를 동적으로 추가하는 등 다양한 옵션을 제공합니다.

긍정 오류 승인자 추가

거짓 긍정 승인자 그룹에 추가된 사용자만 취약한 항목(VI) 및 정정 작업(VUL)에 대한 가양성을 승인할 수 있습니다. 긍정 오류 부여는 단일 수준 승인 프로세스입니다.

시작하기 전에

가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

주:

Vulnerability Response v15.0부터 VR 애플리케이션을 처음 배포하는 경우 예외 관리용 플로우 디자이너가 기본적으로 활성화됩니다. 워크플로우를 이미 사용 중인 경우 플로우 디자이너로 업데이트할 수 있습니다. 두 경우 모두 다시 워크플로우로 변경할 수 없습니다. 예외 관리 및 가양성에 대한 승인 규칙을 구성하려면 문서를 참조하십시오 예외 관리에 대한 승인 규칙 구성.

필요한 역할: sn_vul.vulnerability_admin

프로시저

1. 다음으로 이동 모두 〉 〉 사용자 관리 〉 그룹.
2. 이름 열에서 **False Positive**를 검색하고 옵션을 클릭합니다.
3. 그룹 양식에서 새로 만들기(또는 편집)를 〉 그룹 구성원으로 이동합니다.
4. 사용자 양식에서 사용자 세부 정보를 입력하여 기록을 생성하고 제출을 클릭합니다.
   사용자에게 모든 역할이 부여됩니다. 선택한 사용자가 그룹 구성원 목록에 추가됩니다. 이러한 구성원은 VI 또는 정정 작업을 긍정 오류로 표시하는 요청을 승인할 수 있습니다. 승인되면 기록의 상태가 종결로 업데이트되고 지정된 날짜에만 다시 열립니다.

위험 감소를 위한 질문서 구성

v20.0부터 취약성 대응 필터링된 취약한 항목 또는 정정 작업 세트에 대한 위험 감소 요청의 질문서를 사용자 지정할 수 있습니다.

시작하기 전에

필요한 역할: 관리자

이 태스크 정보

취약한 항목에 대한 보상 통제에 대한 질문서 및 취약한 그룹에 대한 보상 통제에 대한 질문서 승인 규칙은 기본 시스템과 함께 제공됩니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 예외 관리.
2. VR 예외 관리 설정 양식에서 예외를 요청하려면 질문서 사용 확인란을 선택합니다.
3. 위험 감소 요청에 대한 조건에 따라 질문서를 구성하려면 다음을 수행합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. VR 질문서 구성 섹션에서 새로 만들기를 선택합니다.

b. 질문서 구성 - 새 기록 양식에서 취약 그룹에 대한 보상 통제에 대한 질 문서 또는 취약 항목에 대한 보상 통제에 대한 질 문서 승인 규칙을 선택하고 조건을 제공합니다.

c. 원하는 질문서를 선택하고 제출을 선택합니다.
질문서 구성 양식 필드에 대한 자세한 내용은 다음 문서를 참조하십시오 질문서 구성 양식 필드.
생성된 질문서는 VR 예외 관리 설정 양식의 VR 질문서 구성 섹션에 나타납니다.

4. VR 예외 관리 설정 양식에서 저장을 선택합니다.

정정 작업에 대한 취약성 대응 **SLA** 보기

취약한 항목이 올바르게 처리되도록 정정 작업에 대한 취약성 대응 서비스 수준 계약(SLA)을 정의할 수 있습니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)

가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

이 태스크 정보
이 목록의 SLA 정의는 에 특정한 취약성 대응플랫폼 SLA 목록의 하위 집합입니다.

자세한 지침은 Create an SLA definition 문서를 참조하십시오.

VI를 정정하는 데 걸리는 시간을 추적하는 경우 를 사용하는 취약성 대응 정정 대상 규칙것이 좋습니다. 정정 대상 규칙은 특히 취약성 대응의 컨텍스트 내에서 VI(취약한 항목)를 정정하기 위한 예상 시간 범위를 정의하는 반면, SLA는 취약성 자체를 정정하기 위한 시간 범위를 제공할 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 **SLA** 정의.
2. 정의를 클릭합니다.
작업 **SLA** 는 정정 작업의 관련 목록에 표시됩니다.

워치독 구성

감시 구성 페이지를 사용하여 새 감시 장치를 생성하거나 지정하려는 조건으로 기존 감시 장치를 업데이트합니다. 각 감시단에 대해 알림을 활성화하고 조건이 충족될 때 알림을 받을 수 있습니다.

시작하기 전에
필요한 역할: sn_sec_cmn.admin

프로시저

1. 다음으로 이동 모두 〉 보안 운영 〉 **WatchDog** 〉 구성.
2. 구현하려는 워치독을 선택합니다.
3. 양식에서 필드를 채웁니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

WatchDog 통합 양식

필드	설명
이름	워치독의 이름입니다.
활성	Watchdog을 사용하려면 확인란을 *true* 설정합니다.
조건 유형	필터 또는 스크립트 중에서 선택합니다.
고급 조건	이 필드는 조건 유형에서 스크립트를 선택한 경우에만 나타납니다.
테이블	감시 조건을 실행하려면 테이블을 선택합니다.
조건	워치독을 평가하는 조건입니다.
알림	감시 조건이 충족될 경우 그룹 또는 사용자에게 알리는 확인란입니다.
사용자	감시 조건이 충족될 경우 알림을 받을 사용자 목록입니다.
그룹	감시 조건이 충족될 경우 알림을 받을 그룹입니다.
감시 로그	
워치독	감시 테이블에 대한 참조입니다.
카운트	감시 기준을 충족하는 기록 수입니다.
메모	감시 로그에 대한 추가 참고 사항입니다.

4. 업데이트를 선택합니다.

관련 목록의 최대 행 수 구성

관련 목록에 표시되는 행 수를 제어하여 VR(취약성 대응), CC(구성 준수), CVR(클라우드 취약성 대응) 및 AVR(애플리케이션 취약성 대응)에서 로드 시간을 줄이고 가독성과 성능을 개선합니다. 관련 목록에는 영향을 받는 CI, 발견 사항 또는 정정 작업과 같은 관련 기록이 표시되므로 양식에서 나가지 않고도 관련 상세 정보에 빠르게 액세스할 수 있습니다.

시작하기 전에

필요한 역할: sn_vul_cmn.admin

프로시저

1. 다음으로 이동 모두 〉 **sys_properties.** 목록.
2. 속성: *sn_vul_cmn.related_list.set_max_row*
3. 값 필드에 다음 중 하나를 입력합니다.
   - 양의 정수: 각 관련 목록의 행 수를 표시합니다.
   - 음의 정수: 잘못된 입력 또는 값을 무시합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

○ 비어 있음(값 없음): 모든 행을 표시합니다.

주:
100개 이상의 행을 표시하면 성능에 영향을 줍니다.

4. 업데이트를 선택하여 변경 내용을 적용합니다.

결과
시스템 속성을 업데이트하면 다음 관련 목록에 구성된 행 제한이 반영됩니다.

클래식 UI에서

- 영향을 받는 CI
- 이미지 결과
- 잠재적 중복 항목
- 잠재적 솔루션
- 기본 설정 솔루션
- 정정 작업
- 취약 항목

작업 공간 UI에서

- 잠재적 솔루션
- 영향을 받는 CI
- 영향을 받는 애플리케이션
- 영향을 받는 Docker 이미지

고급 취약성 대응 구성 작업

다음 설정 작업에는 코딩 또는 고급 ServiceNow 전문 지식이 필요하며 기본 구성의 일부로 간주되지 않습니다.

고급 코딩 경험이 있거나 에 대한 ServiceNow AI Platform전문 지식이 있는 경우에만 이러한 작업을 수행하는 것이 좋습니다.

통합을 위해 도메인 분리 임포트 작성

임포트한 데이터를 특정 도메인에 있도록 하려면 통합을 실행하도록 할당된 사용자가 해당 도메인에 속해야 합니다.

시작하기 전에
필요한 역할:
특정 통합에 대한 import_admin 및 구성 통합 역할(예: sn_vul.configure_r7_integration 또는 sn_vul_tenable.configure_integration).

이 태스크 정보
이 작업에는 코딩 또는 고급 ServiceNow 전문 지식이 필요합니다.

임포트 큐에는 예약된 작업(통합)이 처리하는 데이터 첨부 파일이 포함되어 있습니다. 도메인 분리 환경에서는 예약된 작업을 올바른 임포트 큐와 일치시켜야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 도메인을 생성합니다.
2. 생성하는 모든 도메인에 대해 사용자를 생성하고 사용자를 해당 도메인에 할당합니다.

   이 사용자를 취약성 통합에서 도메인의 **run_as** 자리 표시자로 생각하십시오. VR과 동일합니다. 전역 도메인의 시스템 사용자입니다. 이 사용자는 데이터 소스, 변환 맵 및 취약성 데이터에 액세스해야 합니다.

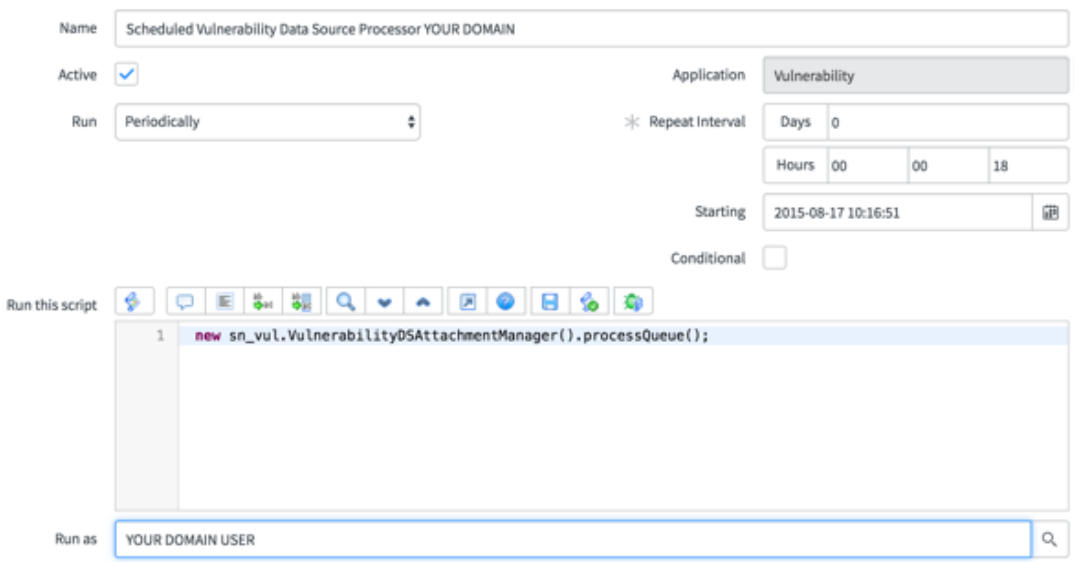
   주:
   이 사용자를 다른 용도로 사용하지 마십시오.

3. 각 도메인에서 예약된 작업을 생성합니다 .
   추가 주의 사항 및 설정에 대한 자세한 내용은 문서를 참조하십시오 도메인 분리에 대한 추가 설정.

   a. 다음으로 이동 모두 〉 시스템 정의 〉 예약된 작업.

   b. 예약된 취약성 데이터 소스 프로세서를 도메인에 복사합니다.

   c. 예약된 작업을 식별하려면 이름에 도메인을 추가합니다.



   d. 실행 필드에서 **run_as** 사용자를 2단계에서 생성한 사용자로 변경합니다.

   v20.1 of 취약성 대응부터 다음 스크립트 변경 사항이 기본 시스템과 함께 제공됩니다.

4. 주:
   통합이 **run_as** 사용자 도메인에서 실행되도록 다음 UI 작업을 편집합니다.

   Qualys 호스트 탐지 통합 통합 작업에서지금 실행 UI 작업을 편집하여 이 코드 블록을 파일의 맨 위에 추가합니다.

   Example

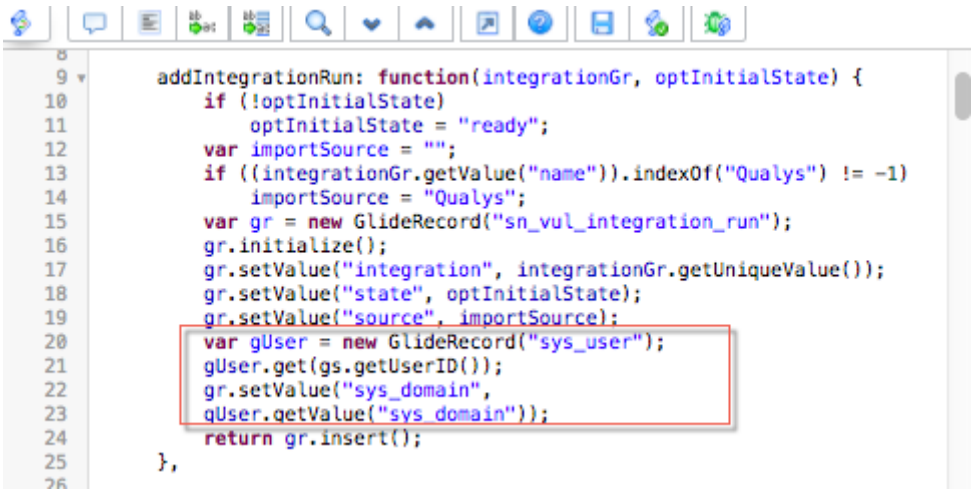
```
//sys id below is of host detection integration
if(current.sys_id == "5d9cf0daff540300c68c9f783894fa4d"){
current.run_as = gs.getUserID
();
```


© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
}
```

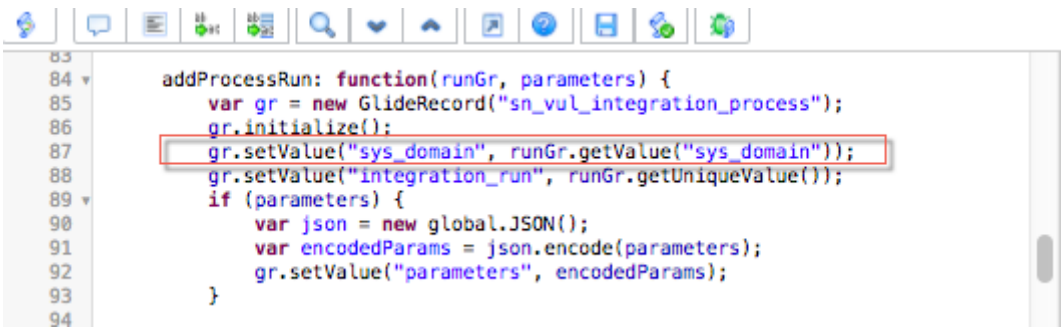
5. 주:
   run_as 사용자 도메인에서 통합이 실행되도록 다음 스크립트 포함을 편집합니다.

   VulnerabilityIntegrationUtils 스크립트 포함 메서드 **addIntegrationRun**을 편집하여 강조 표시된 코드를 추가합니다.



```
addIntegrationRun: function(integrationGr, optInitialState) {
    if (!optInitialState)
        optInitialState = "ready";
    var importSource = "";
    if ((integrationGr.getValue("name")).indexOf("Qualys") != -1)
        importSource = "Qualys";
    var gr = new GlideRecord("sn_vul_integration_run");
    gr.initialize();
    gr.setValue("integration", integrationGr.getUniqueValue());
    gr.setValue("state", optInitialState);
    gr.setValue("source", importSource);
    var gUser = new GlideRecord("sys_user");
    gUser.get(gs.getUserID());
    gr.setValue("sys_domain",
    gUser.getValue("sys_domain"));
    return gr.insert();
},
```

6. **VulnerabilityIntegrationUtils** 스크립트 포함 메서드 **addProcessRun**을 편집하여 강조 표시된 코드를 다음 이미지에 추가합니다.
   addProcessRun 코드



```
addProcessRun: function(runGr, parameters) {
    var gr = new GlideRecord("sn_vul_integration_process");
    gr.initialize();
    gr.setValue("sys_domain", runGr.getValue("sys_domain"));
    gr.setValue("integration_run", runGr.getUniqueValue());
    if (parameters) {
        var json = new global.JSON();
        var encodedParams = json.encode(parameters);
        gr.setValue("parameters", encodedParams);
    }
```

7. **VulnerabilityIntegrationUtils** 스크립트 포함 메서드인 **copyProcess**를 편집하여 강조 표시된 코드를 다음 이미지에 추가합니다.
   copyProcess 코드

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Script

```
325
326     _copyProcess: function(intProcGr, isProcessErrored) {
327         var copy = new GlideRecord('sn_vul_integration_process');
328         copy.initialize();
329         copy.setValue('integration_run', intProcGr.getValue('integration_run'));
330         copy.setValue('parameters', intProcGr.getValue('parameters'));
331         copy.setValue('state', 'new');
332         copy.setValue('notes', '');
333         copy.setValue('sys_domain', intProcGr.getValue('sys_domain'));
334         if (isProcessErrored) {
335             copy.setValue('errored_retries', parseInt(intProcGr.getValue('errored_retries')) + 1);
336             var nextRetryDueOn;
337             if (intProcGr.getValue('next_retry_due_on') != '')
338                 nextRetryDueOn = new GlideDateTime(intProcGr.getValue('next_retry_due_on'));
339             else
340                 nextRetryDueOn = new GlideDateTime();
341
342             var intgInstance = new sn_vul.VulnerabilityIntegrationHelper().getIntScriptInstance(intProcGr);
343             var nextRetryDelay = intgInstance.getNextRetry(intProcGr.errored_retries);
344             nextRetryDueOn.addSeconds(nextRetryDelay * 60);
345             if (parseInt(intProcGr.getValue('errored_retries')) + 1 < intgInstance.getMaxRetry())
346                 copy.setValue('next_retry_due_on', nextRetryDueOn.getValue());
347         } else
348             copy.setValue('retries', intProcGr.retries + 1);
349
350         copy.insert();
351         return copy;
352     },
```

8. **DataSourceVulnReportRefreshProcessor** 스크립트 포함 메서드 **_processFromDataSourceGroups** 편집하여 이 원래 코드를 변경합니다.
원본 _processFromDataSourcesGroups 코드

```
23
24     _processFromDataSourceGroups: function(payload, fileName) {
25         var gr = new GlideRecord("sn_vul_int_data_src");
26         gr.addQuery("sn_vul_integration", this.integrationGr.sys_id + "");
27         gr.orderBy("ds_group_number");
28         gr.orderBy("last_used");
29         gr.query();
30         var lastGroup;
31         if (gr.getRowCount() == 0) {
32             throw new Error("There are no data sources to provide data to.");
33         }
34         while (gr.next()) {
35             var thisGroup = gr.getValue("ds_group_number");
36             if (lastGroup == thisGroup && lastGroup !== undefined) {
37                 continue;
38             } else {
39                 var ds = new GlideRecord("sys_data_source");
40                 if (!ds.get(gr.sys_data_source + ""))
41                     continue;
42
43                 var mgr = new sn_vul.VulnerabilityDSAttachmentManager();
44                 mgr.queueItem(ds.getUniqueValue(), fileName, payload,
   this.integrationProcessGr.getUniqueValue());
45                 gr.setValue("last_used", new GlideDateTime().getValue());
46                 gr.update();
47                 lastGroup = thisGroup;
48             }
```

대상:

_processFromDataSourcesGroups 코드 편집됨

```
43                 var mgr = new sn_vul.VulnerabilityDSAttachmentManager();
44                 mgr.queueItem(ds.getUniqueValue(), fileName, payload,
   this.integrationProcessGr.getUniqueValue(),this.integrationProcessGr.getValue("sys_domain"));
45                 gr.setValue("last_used", new GlideDateTime().getValue());
46                 gr.update();
47                 lastGroup = thisGroup;
```

9. **VulnerabilityDSAttachmentManager** 스크립트 포함 메서드인 **queueItem**을 편집하여 강조 표시된 다음 코드 블록을 추가합니다
큐 항목

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
44      queueItem: function(dataSource, attachmentName, reportData, optIntegrationProcess,optDomain) {
45          var gr = new GlideRecord(this._QUEUE_TABLE);
46          gr.initialize();
47          gr.setValue("status", "NEW");
48          gr.setValue("data_source", dataSource);
49          if (optIntegrationProcess)
50              gr.setValue("integration_process", optIntegrationProcess);
51          if(optDomain){
52                  gr.setValue("sys_domain", optDomain);
53          }
54          var sysId = gr.insert();
```

_getNext

```
156     _getNext: function() {
157         // First go through the retries, if any
158         var gUser = new GlideRecord("sys_user");
159         gUser.get(gs.getUserID());
160         var sysDomainUser = gUser.getValue("sys_domain");
161         var gr = new GlideRecord(this._QUEUE_TABLE);
162         gr.addQuery("status", "RETRY");
163         gr.addQuery("sys_domain", sysDomainUser);
164         gr.orderBy("queued_on");
165         gr.query();
166         if (gr.next()) {
167             return gr;
168         }
169
170         // Then handle the regular queued items
171         gr = new GlideRecord(this._QUEUE_TABLE);
172         gr.addQuery("status", "QUEUED");
173         gr.orderBy("queued_on");
174         gr.addQuery("sys_domain", sysDomainUser);
175         gr.query();
176         if (gr.next()) {
177             return gr;
178         }
179
```

_processQueueEntry 기능

```
182     _processQueueEntry: function(entry) {
183         var schedGrId = this._getScheduledImportSet(entry.data_source);
184         if (gs.nil(schedGrId)) {
185             return;
186         }
187
188         var dataSourceGr = new GlideRecord("sys_data_source");
189         if (!dataSourceGr.get(entry.data_source)) {
190             gs.warn("Non existent data source - marking as complete");
191             entry.setValue("status", "COMPLETE");
192             entry.setValue("processing_notes", "Data source does not exist, could not process.");
193             entry.update();
194             return;
195         }
196
197         try {
198             this._deleteDataSourceAttachments(entry.data_source);
199             if (!this._verifyDataSourceAttachmentsDeleted(entry.data_source)) {
200                 gs.error("VulnerabilityDSAttachmentManager._processQueueEntry: Attachments not deleted for queue
entry " + entry.sys_id);
201                 throw "Attachments not deleted";
202             }
203             var attachmentApi = new GlideSysAttachment();
204             attachmentApi.copy(this._QUEUE_TABLE, entry.sys_id + "", this._DATA_SOURCE, dataSourceGr.sys_id + "");
205             var schedGr = new GlideRecord("scheduled_import_set");
206             schedGr.get(schedGrId);
207             schedGr.setValue("data_source", entry.data_source);
208             schedGr.setValue("run_as", gs.getUserID());
209             schedGr.update();
```

이제 도메인으로 구분된 임포트를 수행할 준비가 된 것입니다.

주:
OR 애플리케이션 취약성 대응 통합이 취약성 대응 여러 개 있는 경우 각 배포에 대해 이 프로세스를 반복합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

백그라운드 작업 프레임워크에서 여러 도메인 생성 및 지원

Vulnerability Response 제품의 백그라운드 작업은 오랜 시간 동안 실행되어 기록에 대한 여러 프로세스를 수행하도록 설계되었습니다. 백그라운드 작업 프로세서는 시스템 사용자를 통해 실행되고 전역 도메인에 기록을 생성하는 기본 시스템과 함께 제공됩니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 〉 도메인 관리 〉 도메인.
2. 도메인을 생성합니다.

   도메인을 생성하는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 Create a domain.

   생성된 모든 도메인에 대해 사용자를 생성하고 사용자를 도메인에 할당합니다. 이 사용자를 도메인의 run_as 자리 표시자로 가정합니다. VR과 같습니다. 전역 도메인의 시스템 사용자입니다. 이 사용자는 취약성 데이터에 액세스해야 합니다.

3. 예약된 작업의 *Scheduled Background Job Manager*run_as 변경 및 *Close the parent background job*.

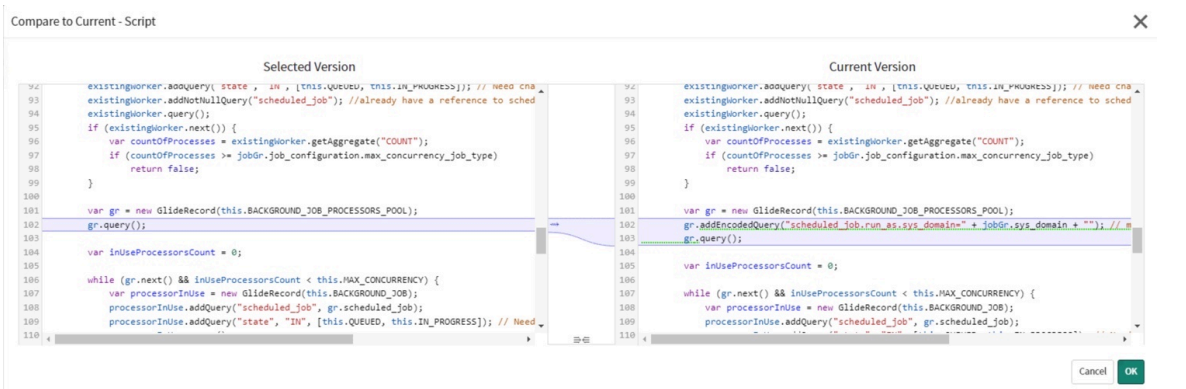
   여러 도메인이 생성된 경우 이 작업을 복제하고 그에 따라 사용자를 변경합니다run_as. 비활성 모드에서 전역 도메인의 run_as 사용자와 함께 이전 작업의 사본을 보관할 수도 있습니다.

   10개의 프로세서 작업(예: *Background job processor 10*)이 기본 시스템과 함께 제공됩니다. 이러한 작업의 실행을 도메인으로 구분된 사용자로 변경합니다. 여러 도메인이 있는 경우 도메인당 두 개의 작업으로 충분하지만 필요한 경우 이러한 작업을 복제할 수도 있습니다. 전역 도메인에서 run_as 사용자와 함께 두 개의 프로세서 작업을 유지합니다.

   의 취약성 대응v20.0부터 다음과 같은 스크립트 변경 사항이 기본 시스템과 함께 제공됩니다.

4. 스크립트 포함 *BackgroundJobManager*을 수정하고 다음 이미지와 같이 다음 줄을 추가합니다.

```
gr.addEncodedQuery("scheduled_job.run_as.sys_domain=" + jobGr.sys_domain + "");
```



> **주:**
> 올바른 도메인에서 규칙을 요청 시 다시 적용하도록 트리거합니다.

취약성 대응 CI 조회 규칙 생성

CI 조회 규칙 모듈에는 외부 공급업체 취약성 통합 임포트 중에 받은 호스트 정보에 대해 일치하는 기록을 찾는 데 사용되는 규칙이 포함되어 있습니다. 호스트 정보는 검색된 항목, 일치하지 않는 구성 항목 클래스 및 .구성 관리 데이터베이스(CMDB)

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에

가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

필요한 역할: sn_vul.vulnerability_admin

이 태스크 정보

CI 조회 규칙을 생성하려면 고급 ServiceNow 전문 취약성 대응 지식이 필요합니다. 기존 조회 규칙 중 하나를 수정하지 말고 복사하여 복사본을 수정하는 것이 좋습니다. 새 규칙이 원하는 작업을 수행한다고 생각되면 원래 규칙을 비활성화합니다.

주:
제거된 규칙은 복구할 수 없습니다. 기존 규칙을 제거하는 대신 새 규칙을 만들 때 비활성화하십시오.

프로시저

1. 다음으로 이동 모두 〉 보안 운영 〉 **CMDB** 〉 **CI** 조회 규칙.
2. 새로 만들기를 클릭합니다.
3. 양식에서 필드를 채웁니다.

CI 조회 규칙 양식

필드	설명
이름	규칙의 이름입니다.
조회 메서드	일치에 사용되는 메서드입니다. 선택 항목은 다음과 같습니다. ○ 스크립트: 사전 빌드(IP 주소, DNS 이름 등) 또는 사용자 지정 스크립트. ○ 필드 일치: CMDB의 테이블 또는 필드를 검색합니다.
유형	스크립트 조회 메서드에 사용되는 유형입니다.
순서	규칙의 우선순위 순서입니다. 순서가 가장 낮은 규칙이 먼저 평가됩니다.
활성	규칙의 활성 또는 사용 안 함 여부에 대한 확인란입니다.
소스	이 규칙에 대한 입력으로 사용되는 소스입니다.
소스 필드	이 규칙에 대한 입력으로 사용되는 소스 필드입니다. 필드를 선택하되 이는 문자열 값으로 처리됩니다 .
조건	CI 조회 규칙이 적용되는 조건입니다. 이 조건은 외부 공급업체 스캐너의 속성에 따라 다릅니다. **주:** 자산 속성은 페이로드의 일부입니다. 외부 공급업체 스캐너에서 수신합니다. 페이로드 예는 검색된 항목 테이블을 참조하십시오.
스크립트	유형에 따라 편집 가능한 샘플 스크립트가 표시됩니다. 기본 기능의 템플릿에 포함된 설명에 따라 사용자 지정 스크립트를 구현합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

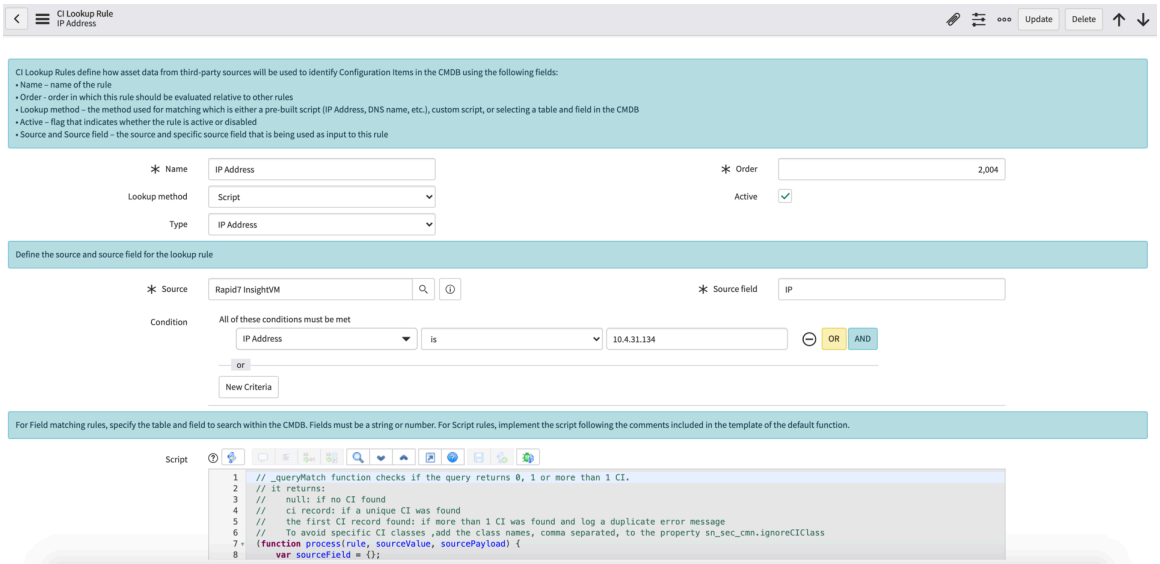
필드	설명
	주: process 함수에는 세 개의 매개 변수가 있습니다. *rulesourceValuesourcePayload*
테이블에서 검색	CMDB 내에서 검색할 테이블입니다. 필드 일치 조회 메서드와 함께 사용됩니다.
필드 검색	CI를 찾는 데 사용할 수 있는 정보가 담긴 필드입니다. 필드 일치 조회 메서드와 함께 사용됩니다. 이 필드는 CI 기록 또는 네트워크 어댑터와 같은 관련 기록에 있을 수 있습니다.

4. 제출을 클릭합니다.

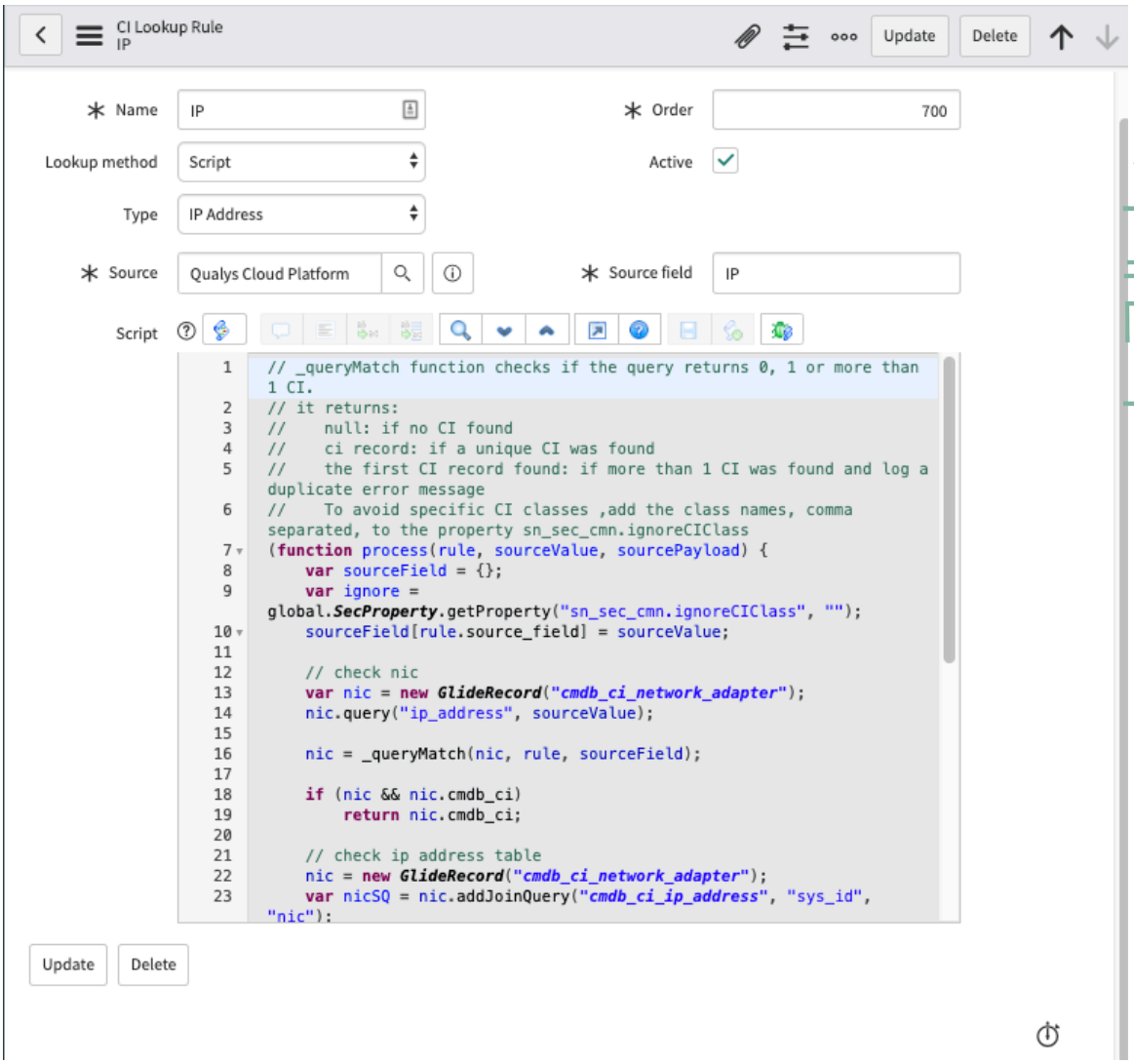
CI 조회 규칙에 대한 구현 정보에 대한 자세한 내용은 을 참조하십시오 CI 조회 규칙을 실행 취약성 대응 한 후 중복 또는 고아 기록을 방지하는 데 도움이 되는 단계.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

V12.0용 조건 작성기를 사용하는 CI 조회 규칙의 예



V12.0 이전 스크립트를 사용하는 CI 조회 규칙의 예



관련 정보

취약성 대응 취약한 항목 양식 필드

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

CI 클래스 무시

CI 조회 규칙을 실행할 때 부하 분산 장치 [cmdb_ci_lb]와 같은 일부 CI(구성 항목) 클래스를 무시하려면 **ignoreCIClass** [*sn_sec_cmn.ignoreCIClass*] 시스템 속성을 설정합니다.

시작하기 전에
필요한 역할: 관리자

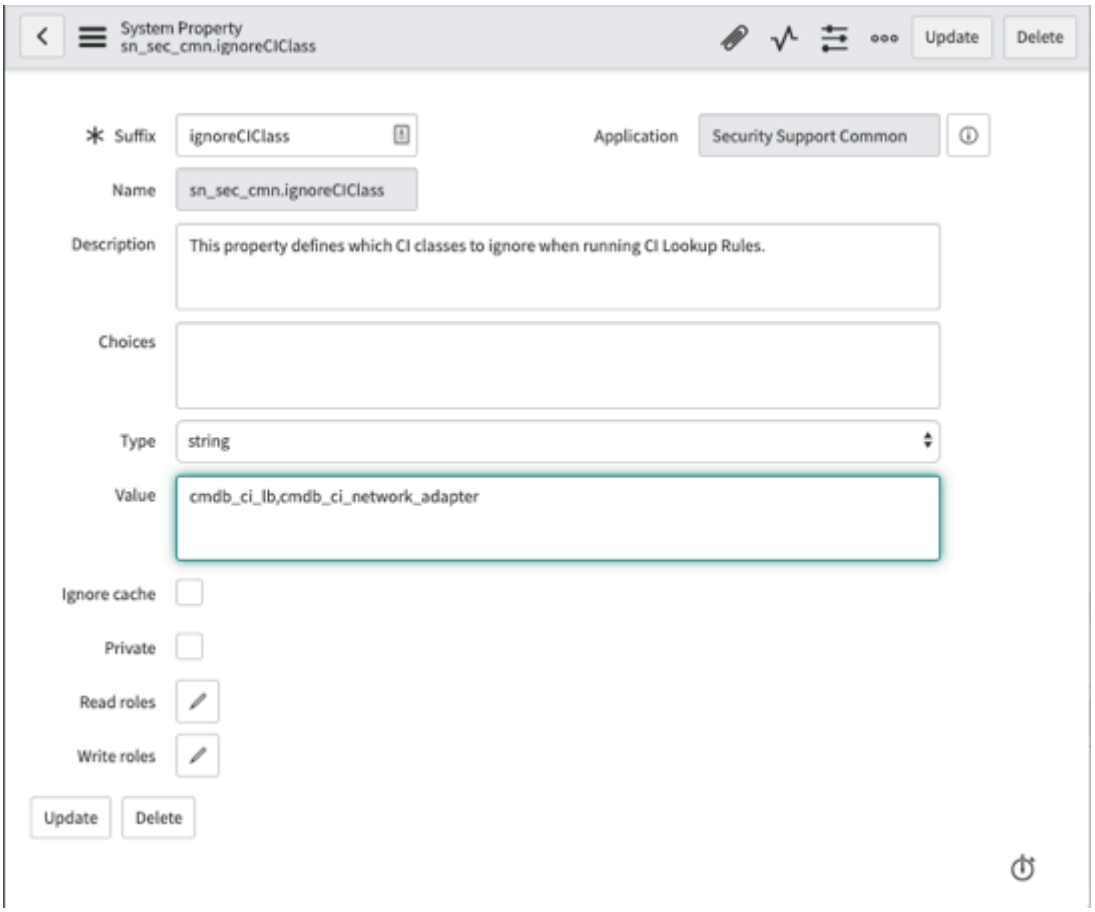
주:

ignoreCIClass 시스템 속성은 v9.0부터 취약성 대응 사용할 수 있지만 이전 버전에서 업그레이드할 때 속성 기능을 사용할 수 없습니다.

버전 9.0 이전의 애플리케이션에서 업그레이드 보안 운영 한 경우 이 기능을 활성화하는 방법에 대한 지침은 KB0788209 참조하십시오.

프로시저

1. 왼쪽 탐색 모음에 sys_properties.list 를 입력합니다.
2. 입력을 클릭합니다.
3. 검색 메뉴의 이름에서 sn_sec_cmn.ignoreCIClass# 입력합니다.
4. 값 텍스트 상자에 제외할 CI 클래스를 쉼표로 구분된 목록으로 입력합니다.



5. 업데이트를 클릭합니다.
   이 목록은 다음 임포트 중에 CI 조회 규칙에서 사용됩니다. 임포트 중에 생성된 취약한 항목은 sn_sec_cmn.ignoreCIClass 시스템 속성의 값 필드에 나열된 어떤 유형의 CI에도 연결되지 않습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

해제된 CI 필터링

CI 조회 규칙을 실행하는 동안 폐기된 CI(구성 항목)를 필터링합니다. 보안 운영 CMDB CI 조회 규칙을 실행할 때 해제된 CI를 필터링하려면 **filterOutDecommissionedCI** [**sn_sec_cmn.filterOutDecommissionedCI**] 시스템 속성을 true로 설정합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
시스템 속성의 기본값은 true입니다. 이 속성은 의 취약성 대응 CI 조회 규칙에만 적용되며 IRE 조회 논리에는 영향을 주지 않습니다.

프로시저

1. 왼쪽 탐색 모음에 sys_properties.list 를 입력합니다.
2. Enter를 선택합니다.
3. 검색 메뉴의 이름 아래에 sn_sec_cmn.filterOutDecommissionedCI를 입력하여 해제된 CI를 필터링합니다.
4. 값 텍스트 상자에 true 또는 false 값을 입력합니다.
   기본값은 true입니다.
5. 업데이트를 선택합니다.
   이 값은 다음 임포트 중에 CI 조회 규칙에서 사용됩니다. sn_sec_cmn.filterOutDecommissionedCI 시스템 속성은 조회 규칙을 실행하는 동안 아래 표시된 조건을 충족하는 CI를 필터링합니다.

```
_isCIDecommissioned: function(gr, filterDecommissionCi) {
      var install_status = false;
      var life_cycle_stage_status = false;
      // check for property
      if (filterDecommissionCi == "true") {
         if (gr.isValidField("install_status"))
            install_status = gr.install_status == 7;
         if (gr.isValidField("life_cycle_stage_status"))
            life_cycle_stage_status = gr.life_cycle_stage_status == "Retired";
      }
      return install_status || life_cycle_stage_status;
```

CI 자동 승격

autoPromoteFields [**sn_sec_cmn.autoPromoteFields**] 시스템 속성에서 JSON 문자열을 편집하여 CI(구성 항목) 조회 규칙이 모든 보안 운영 CMDB CI를 [cmdb_ci] 테이블의 일치하는 항목으로 자동 승격하도록 합니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin

이 태스크 정보
시스템 속성 유형은 '문자열'이며 JSON 문자열을 입력해야 합니다. 이 속성은 기본적으로 활성화되며 CI 조회 규칙을 실행하는 동안 일치하는 CI를 승격합니다.

사용자 지정 작성 조회 스크립트는 스크립트에서 하위 테이블 기록을 반환할 수 있습니다. 이 속성의 `_autoPromoteCI` 경우 의 `CIIdentify Script Include` 함수는 조회 스크립트에서 반환된 CI를 가져오고 자동으로 관계를 트래버스하여 항목에 도달 `cmdb_ci` 하여 반환합니다.

자동 승격 논리를 재정의하려면, 즉 새 CI 클래스를 추가하거나 업데이트하려면 [**sn_sec_cmn.autoPromoteFields**] 시스템 속성의 값 필드에 JSON 객체를 추가합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 왼쪽 탐색 모음에 sys_properties.list 를 입력합니다.
2. Enter를 선택합니다.
3. [**sn_sec_cmn.autoPromoteFields**] 시스템 속성을 찾은 다음 기록을 선택하여 엽니다.

   기본 문자열:

```
{
 "dscy_switchport":"cmdb_ci",
 "cmdb_ci_network_adapter":"cmdb_ci",
 "cmdb_ci_nic":"cmdb_ci",
 "cmdb_ci_ip_address":"nic"
}
```

4. 값 텍스트 상자에서 기본 페어링 형식을 사용하여 문자열을 편집합니다.
5. 업데이트를 선택합니다.
   이 값은 다음 임포트 중에 CI 조회 규칙에서 사용됩니다.

취약한 항목 키 구성

애플리케이션에서 VIT(취약한 항목) 키의 취약성 대응 세분성을 구성하여 조직에서 VIT(취약한 항목)를 만드는 요소를 정의합니다.

시작하기 전에
필요한 역할: 관리자
가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

주요 용어:

CI(구성 항목)
: CMDB에 나열된 기존 자산입니다.

취약성
: NIST(National Institute of Standards and Technology), NVD(National Vulnerability Database), CWE(Common Vulnerabilities and Exposures) 또는 와의 외부 공급업체 통합에서 임포트한 취약성 대응알려진 취약성의 기록입니다.

취약한 항목
: 취약한 항목은 임포트한 취약성이 CMDB의 구성 항목과 일치할 때 생성됩니다.

탐지
: 외부 공급업체 통합 스캐너에서 보고되는 분명한 한 건의 취약성 발생입니다. 탐지가 임포트되어 인스턴스의 탐지 및 취약한 항목 기록 모두에 표시됩니다. 취약한 항목 탐지라고도 합니다.

기본적으로 취약한 항목은 CI(구성 항목), 취약성 및 통합 인스턴스의 고유한 조합입니다. 더 세분화된 취약한 항목을 생성하려면 취약한 항목 탐지에서 고유한 포트 또는 권장 사항(Microsoft TVM 취약성에만 해당) 을 추가합니다. 이렇게 하면 조직에 가장 효과적이라고 생각되는 수준에서 취약성 수정을 관리할 수 있습니다.

취약한 항목을 더 세밀하게 생성하려면 취약한 항목 키에 포트 또는 권장 사항이 포함되도록 구성합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 포트 포함이 활성화되면 취약한 항목 탐지의 고유한 포트에 의해 취약한 항목이 생성됩니다.
- 권장 사항 포함을 활성화하면 취약성과 연결된 각 권장 사항에 대해 별도의 취약한 항목이 생성됩니다.

주:
권장 사항 포함 옵션은 사용자 환경에서 Microsoft TVM 통합이 활성화된 경우에만 UI에 나타납니다.

Vulnerability Response V17.1부터 VI 키로 증명을 추가하여 Rapid7 취약성을 식별하고 정정할 수 있습니다. 자세한 내용은 Rapid7 취약한 항목 키에 증명 추가 문서를 참조하십시오.

다음 표에서 옵션을 선택하여 포트 포함 옵션을 활성화합니다.

처음으로 **VI** 키로 포트 포함 옵션을 활성화하는 세 가지 시나리오

면...	설명
다음 조건 중 하나 이상이 참입니다. • 취약한 항목 탐지를 지원하지 않는 v10.0 이전 버전에서 취약성 대응 업그레이드하고 있습니다. • 신규 고객이며 인스턴스에 취약성 대응 데이터(취약한 항목 또는 취약한 항목 탐지) ServiceNow AI Platform# 가 없습니다. • 인스턴스에서 취약한 항목 기록과 관련 데이터를 모두 삭제 했으며 고유한 포트로 구분된 VI를 포함하도록 새로운 임포트를 시작으로 모든 취약성 대응 데이터를 빌드할 준비가 되었습니다.	포트 포함을 활성화합니다. 포트 포함이 활성화되면 임포트한 탐지는 다음 임포트로 시작하는 고유한 포트로 구분된 VI를 포함하는 취약한 항목을 생성합니다.
두 조건 모두 true입니다. • v10.0 이상이 취약성 대응 있고 보존하려는 인스턴스에 기존 취약성 대응 데이터(취약한 항목 또는 취약한 항목 탐지)가 있습니다. • 고유한 포트로 구분된 VI를 포함하도록 새로운 취약한 항목을 생성하려고 합니다.	포트 포함을 활성화합니다. 기존 탐지 및 관련된 취약한 항목은 보존됩니다. 포트 포함이 활성화되면 새 탐지는 다음 임포트로 시작하는 고유한 포트로 구분된 VI를 포함하는 새로운 취약한 항목을 생성합니다.
두 조건 모두 true입니다. • v10.0 이상이 취약성 대응있습니다. • 기존 Vulnerability Response 데이터(취약한 항목 또는 취약한 항목 탐지)가 있지만 새로운 임포트부터 취약성 데이터를 빌드하는 것을 선호하고 고유한 포트로 구분된 VI를 포함하려고 하기 때문에 기존 데이터를 보존하고 싶지 않습니다.	1. 인스턴스에서 취약한 항목 기록과 관련 데이터를 모두 삭제합니다. 2. 포트 포함을 활성화합니다. 포트 포함이 활성화되면 새 탐지는 다음 임포트로 시작하는 고유한 포트로 구분된 VI를 포함하는 새로운 취약한 항목을 생성합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

포트 포함 옵션을 사용하는 경우 구성 항목에 대해 둘 이상의 취약한 항목을 만들 수 있습니다. 예를 들어 구성 항목의 두 포트(포트 80 및 443)에 대해 취약성이 있는 경우 다음 임포트로 시작하는 각 포트에 대해 하나씩 두 개의 고유한 VI가 생성됩니다.

주:
이 기능을 활성화하기 전에 고유한 포트별로 VI를 포함하도록 VI를 생성해야 합니다. VI 키를 사용하여 포트를 포함하면 먼저 취약성 대응 데이터를 삭제한 후 포트 포함을 비활성화하고 기본 VI 키 세분성(즉, VI가 포트에 대해 생성되지만 고유한 포트로 구분되지 않음)을 사용하여 취약성 데이터 임포트로 돌아갈 수 있습니다. 취약성 데이터 삭제에 대한 자세한 내용은 을 참조하십시오 에서 취약한 항목 기록 및 관련 데이터를 모두 삭제합니다. 취약성 대응.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 취약한 항목 G란성 구성 .

   마지막 업데이트 필드에는 VI 키가 마지막으로 구성된 날짜가 표시됩니다.

2. **Include** Port(포트 포함) 확인란을 선택하여 사용하도록 설정합니다.

   주:
   Microsoft TVM 통합을 구성한 경우 권장 사항 포함 옵션도 사용할 수 있습니다. 이를 통해 Microsoft TVM 데이터의 고유한 권장 사항에 따라 취약한 항목을 분할할 수 있습니다.

3. 저장을 선택합니다.
   확인 대화 상자가 표시됩니다.

   인스턴스에 취약한 항목 탐지 기록이 없는 경우 취약한 항목 탐지와 취약한 항목은 모두 다음 임포트와 함께 시작되는 고유한 포트에 의해 생성됩니다.

   인스턴스에 기존 취약한 항목 탐지와 취약한 항목이 있는 경우 기존 탐지 및 관련된 취약한 항목이 보존됩니다. 새로운 탐지는 다음 임포트로 시작하는 고유한 포트로 구분되는 VI를 포함하는 새로운 취약성을 생성합니다.

다음에 수행할 작업
포트별로 취약한 항목이 취약한 항목 탐지 및 취약한 항목 기록에 표시되는지 확인합니다. 자세한 내용은 취약한 항목 탐지 데이터 보기 취약성 대응 문서를 참조하십시오.

Rapid7 취약한 항목 키에 증명 추가

VI에 대한 Rapid7 VI(취약한 항목) 키로 증명을 추가합니다. 특정 취약성에 대한 증명을 포함하면 스캐너 통합이 Rapid7 에서 Rapid7수신한 각 증명에 대한 VI를 생성할 수 있습니다.

VI 키는 취약성, CI(구성 항목) 및 통합 인스턴스의 조합입니다. 증명을 기반으로 탐지를 여러 VI로 분할하면 여러 VI가 생성됩니다. 적절한 정정 소유자에게 취약성을 할당할 수 있습니다.

예를 들어 취약성과 CI가 동일하지만 증명이 다른 두 개의 탐지가 있을 수 있으며, 이로 인해 하나의 VI가 생성될 수 있습니다. V17.1부터 취약성 대응 VI 키로 증명을 추가하여 취약성을 식별하고 정정할 수 있습니다.

다음과 같은 방법으로 증명을 VI 키로 추가할 수 있습니다.

다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 **VI** 세분성 구성 을 클릭하고 증명을 포함하는 옵션을 선택합니다.

사용 사례: 기존 VI에 대한 **VI** 키에 증명 포함 또는 탐지 증명에 따라 기존 **VI** 분할

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

증명을 기반으로 VI를 생성하려면 R7 log4j 취약성을 사용할 수 있습니다. 예를 들어 R7-apache-log4j-core-cve-2021-44228, R7-amazon_linux-cve-2021-44228 또는 R7-amazon-linux-ami-2-cve-2021-44228과 같은 여러 R7 log4j 취약성 중 하나를 사용할 수 있습니다.

VI의 모든 감지에 동일한 증명이 있는 경우 기존 VI는 'VI 키(external_id)의 증명'을 포함하도록 업데이트됩니다. 증명이 다른 여러 탐지가 있는 경우 기존 VI가 닫힙니다. 탐지는 'VI 키의 증거(external_id)'를 사용하여 새 VI 간에 분할됩니다.

주:

취약성 ID를 제공하면 기존 VI가 증명을 기반으로 분할됩니다. 이 취약성 ID의 새로운 취약성에는 VI 키 중 하나로 증명도 있습니다.

에서 취약한 항목 기록 및 관련 데이터를 모두 삭제합니다. 취약성 대응

인스턴스의 애플리케이션에서 ServiceNow AI Platform# 모든 취약성 대응 데이터(취약한 항목 또는 취약한 항목 탐지) 및 관련 데이터와 기록을 취약성 대응 영구적으로 제거합니다.

시작하기 전에
인스턴스에서 애플리케이션의 취약한 항목 탐지 기록, 취약한 항목, 취약성 그룹 및 관련 기록을 취약성 대응 삭제합니다. 이 프로세스를 사용하여 인스턴스를 정리하여 외부 공급업체 통합에서 새로 시작하여 데이터를 임포트하거나, 취약한 항목(VI) 키 구성을 기본 설정으로 되돌리기 위한 전제 조건으로 데이터를 임포트합니다. VI 키 구성에 대한 자세한 내용은 문서를 참조하십시오 취약한 항목 키 구성.

주:
이 작업은 인스턴스에서 모든 취약한 항목 기록과 모든 관련 데이터를 삭제합니다. 이 데이터는 한 번 삭제되면 검색할 수 없습니다. 또한 데이터 임포트를 일시 중단하고 와의 활성 외부 공급업체 통합을 취약성 대응비활성화해야 합니다.

VI 키 구성을 변경하기 전에 이 프로세스에서 취약한 항목 데이터를 삭제해야 합니다. 모든 데이터를 제거하면 모든 취약한 항목과 취약한 항목 탐지가 매핑되고 다음 임포트를 시작하는 최신 데이터로 업데이트됩니다.

데이터를 삭제하기 전에 다음 조건이 적용되는지 확인하십시오.

- v10.0 이상이 취약성 대응 설치되어 있습니다. 자세한 내용은 취약성 대응 외부 공급업체 통합에서 취약한 항목 탐지 문서를 참조하십시오.
- 포트 포함을 비활성화하고 VI 키 구성을 기본 설정으로 되돌리려고 합니다.
- 기존의 취약한 항목과 취약한 항목 탐지가 있지만 이를 업데이트하고 유지할 필요가 없거나 필요하지 않습니다.
- 인스턴스를 정리하기 위해 기존의 모든 취약성 대응 데이터와 관련 기록을 제거하기로 결정했습니다.

필요한 역할: sn_vul.vulnerability_admin

가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 취약성 통합.
2. 표시되는 모든 활성 통합을 기록합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약한 항목 및 관련 데이터를 모두 삭제하기 전에 예약된 작업과 함께 나열된 모든 활성 통합을 비활성화하여 데이터를 제거하는 동안 새 데이터가 임포트되지 않도록 합니다. 이 목록을 기록하면 삭제가 완료된 후 통합을 활성화하는 데 도움이 됩니다.

3. HI 지식베이스에서 다시 임포트하기 위해 기존 취약성 대응 데이터를 삭제하는 방법에 대한 문서를 검토하십시오.
4. 활성 열에 쓸 수 없도록 하는 경고 메시지가 표시되는 경우 활성 통합을 비활성화하려면 다음 단계를 수행합니다.

   a. 이름 열에서 항목을 클릭하여 기록을 엽니다.

   b. 활성 확인란을 편집할 수 없으면 여기 링크를 클릭하여 기록을 편집합니다.

   c. 통합을 사용하지 않도록 설정하고 예약된 다음 작업을 취소하려면 활성 확인란을 클릭합니다.

   d. 업데이트를 클릭하여 변경 내용을 저장하고 목록으로 돌아갑니다.

   e. 통합 목록에서 활성 통합을 비활성화했는지 확인합니다.
   통합을 사용하지 않도록 설정하면 활성 통합 목록에 더 이상 표시되지 않습니다. 비활성 통합 목록을 보고 모든 취약성 데이터를 삭제한 후 비활성화한 모든 통합을 찾으려면 상단의 활성 열에 =false를 입력합니다.

5. 기존 취약성 데이터를 삭제하기 위한 KB 문서의 단계를 계속 진행합니다.
6. 모든 데이터가 성공적으로 삭제되었는지 확인한 후 취약성 대응 〉 관리 〉 **VI** 세분성 구성.
7. 양식에서 다음을 수행합니다.
   - 새로 가져온 포트를 포함하도록 취약성 데이터를 빌드하기 위해 데이터를 삭제한 경우 포트 포함을 사용하도록 설정하고 저장을 클릭합니다.
   - VI 키를 기본 설정으로 되돌리기 위해 데이터를 삭제한 경우 포트 포함을 비활성화하고 저장을 클릭합니다.

   자세한 내용은 취약한 항목 키 구성 문서를 참조하십시오.

내부 필터링 취약성 대응

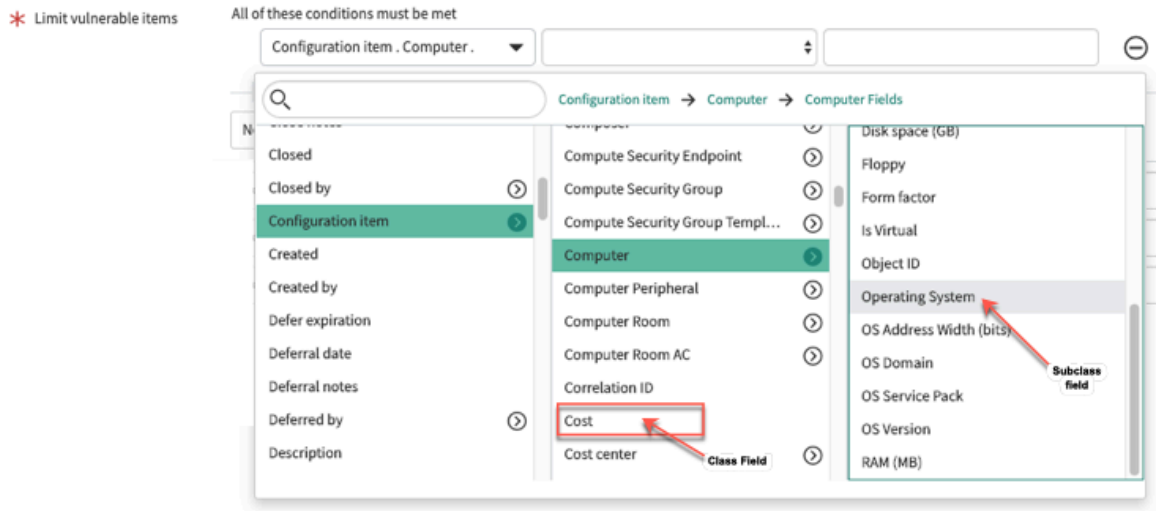
정정 작업 규칙, 계산기 및 할당 규칙은 조건 작성기를 사용하여 생성한 임포트 중 조건을 사용합니다. 이러한 필터를 사용하여 각 기록을 평가하므로 기준을 변경하면 성능에 영향을 줄 수 있습니다.

기본 시스템과 함께 제공되는 규칙과 계산기는 성능에 최적화되어 있습니다. 규칙 또는 계산기를 편집하거나 생성할 때는 주의가 필요하며 두 가지 모두 ServiceNow 와 취약성 대응 전문 지식이 필요할 수 있습니다.

하위 클래스 필드를 기준으로 필터링하지 마십시오.

일부 테이블은 확장을 지원합니다. CMDB CI [cmdb_ci] 테이블이 그 예입니다. cmdb_ci_hardware 및 cmdb_ci_computer와 같은 테이블은 이 테이블을 확장합니다. 상위 테이블에 없는 필드를 기준으로 필터링하는 경우 해당 필터를 구성하고 평가하는 데 비용이 많이 들 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



예를 들어 필터링: 구성 항목 〉 비용 **Cost**는 구성 항목의 하위 클래스 필드가 아니라 클래스 필드이므로 성능에 부정적인 영향을 주지 않습니다.

구성 항목 〉 컴퓨터그러나 다른 필드(이 경우 운영 체제)로 닷워킹이 필요한 하위 클래스입니다. 이 프로세스는 수백만 개의 취약한 항목을 임포트할 때 빠르게 추가되어 성능에 영향을 주는 데 수 밀리초가 걸릴 수 있습니다.

주:
〔contains〕 조건을 사용하는 것은 와일드카드 검색과 비슷하며 성능에 영향을 줄 수 있습니다. 가능하면 〔is〕를 사용하는 것이 더 효율적입니다.

Vulnerability Response에 대한 심각도 매핑

Vulnerability Response는 표준화된 ServiceNow 심각도 매핑을 위해 NVD(국가 취약성 데이터베이스)와 함께 제공됩니다. ServiceNow 외부 공급업체 통합은 설치 시 심각도 매핑을 제공합니다. 이러한 맵은 기존 맵의 필드를 변경하여 조정할 수 있습니다.

Rapid7 취약성 통합 심각도 매핑

Normalised_Severity

테이블에서 가져온 심각도를 사용하여 외부 공급업체 항목의 **normalised_severity** 계산합니다 **sn_vul_nvd_entry** 이는 **sn_vul_entry** 테이블에서 조회된 심각도 조회에 대한 비즈니스 규칙을 사용하여 설정됩니다.

Source_severity

Rapid7 취약성 통합 **API**가 실행되는 동안 **severity_score** 테이블의 데이터가 **source_severity** 테이블에 매핑됩니다.

우선순위

이 필드가 비어 있습니다.

Qualys 취약성 통합 심각도 매핑

Normalised_Severity

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테이블에서 가져온 심각도를 사용하여 외부 공급업체 항목의 **normalised_severity** 계산합니다 **sn_vul_nvd_entry** 이는 **sn_vul_entry** 테이블에서 조회된 심각도 조회에 대한 비즈니스 규칙을 사용하여 설정됩니다.

Source_severity

Qualys 지식베이스 통합이 실행되는 동안 **SEVERITY_LEVEL**의 데이터가 **source_severity** 테이블에 매핑됩니다.

우선순위

우선순위 필드에 대한 데이터는 심각도 테이블에서 가져와 우선순위 테이블에 매핑되며, **Qualys** 호스트 탐지 통합이 **Qualys** 데이터에 매핑된 비즈니스 규칙을 사용하여 실행되는 동안 우선순위 테이블에 매핑됩니다.

주:
비즈니스 규칙은 백그라운드에서 실행되고 Qualys의 우선순위를 확인하고 그에 따라 우선순위를 매핑합니다. 따라서 Qualys 데이터를 매핑하려면 BR이 책임이 있습니다.

취약성 통합 심각도 매핑 **Tenable.io**

Normalised_Severity

테이블에서 가져온 심각도를 사용하여 외부 공급업체 항목의 **normalised_severity** 계산합니다 **sn_vul_nvd_entry** 이는 **sn_vul_entry** 테이블에서 조회된 심각도 조회에 대한 비즈니스 규칙을 사용하여 설정됩니다.

Source_severity

Tenable.io 플러그인 통합risk_factor 실행되는 동안 테이블의 데이터가 **source_severity** 테이블에 매핑됩니다.

우선순위

Tenable.io 미해결 취약성 통합이 실행되는 동안 **severity_id**의 데이터가 **source_severity**에 매핑됩니다.

VPR

Tenable.io 플러그인 통합이 실행 중인 동안 점수의 데이터가 **Source_risk_score**에 매핑됩니다.

다음에서 계산됨 점수의 데이터는 **Tenable.io** 플러그인 통합이 실행 중인 동안 **Source_risk_rating**에 매핑됩니다.

취약성 통합 심각도 매핑 **Tenable.sc**

Normalised_Severity

테이블에서 가져온 심각도를 사용하여 외부 공급업체 항목의 **normalised_severity** 계산합니다 sn_vul_nvd_entry 이는 **sn_vul_entry** 테이블에서 조회된 심각도 조회에 대한 비즈니스 규칙을 사용하여 설정됩니다.

Source_severity

Tenable.io 플러그인 통합이 실행되는 동안 **riskFactor** 테이블의 데이터가 **source_severity**에 매핑됩니다.

우선순위

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

"severity": { "id": "0", "name": "Info", "description": "Informative" }로 수신된 심각도의 데이터는 **Tenable.io** 미해결 취약성 통합이 실행되는 동안 **source_severity**에 매핑됩니다.

VPR

플러그인 통합이 실행되는 동안 **vprScore**의 데이터가 **Source_risk_score**에 매핑 Tenable.io.

vprScore에서 계산됨의 데이터는 **Tenable.io** 플러그인 통합이 실행되는 동안 **Source_risk_rating**에 매핑됩니다.

TVM 심각도 매핑

Normalised_Severity

테이블에서 가져온 심각도를 사용하여 외부 부품 항목의 **normalised_severity** 계산합니다 **sn_vul_nvd_entry** 이는 **sn_vul_entry** 테이블에서 조회된 심각도 조회에 대한 비즈니스 규칙을 사용하여 설정됩니다.

Source_severity

CVE(Microsoft TVM 취약성) 통합이 실행되는 동안 심각도 테이블의 데이터가 **source_severity**에 매핑됩니다.

우선순위

이 필드가 비어 있습니다.

취약성 대응 심각도 맵 생성

취약성 대응 심각도 매핑은 외부 공급업체 소스 심각도 필드를 의 인식 가능한 필드 취약성 대응로 변환합니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)
가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

이 태스크 정보
취약성 대응 은 NVD(국가 취약성 데이터베이스)와 함께 제공되어 심각도 매핑을 정규화 ServiceNow 합니다. ServiceNow 설치 시 심각도 매핑을 Qualys Vulnerability Integration 제공하는 등의 외부 공급업체 통합입니다. 이러한 맵은 기존 맵의 필드를 변경하여 조정할 수 있습니다.

심각도 맵을 만들거나 편집하는 것은 사용자 환경에서 사용자 지정된 또는 비표준 외부 공급업체 매핑에만 사용됩니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 표준화된 심각성 매핑.
2. 새로 만들기를 클릭합니다.
3. 양식의 필드에 적절히 입력합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드 매핑

필드	설명
소스	심각도 매핑에 대한 소스의 이름입니다.
소스 값	소스 심각도 값입니다.
대상 값	대상 심각도 값입니다. 선택 항목은 다음과 같습니다. ○ 1 - 심각 ○ 2 - 높음 ○ 3 - 보통 ○ 4 - 낮음 ○ 5 - 없음

4. 각 소스 심각도 수준에 대해 3단계를 반복합니다.
5. 제출을 클릭합니다.

보고 및 관련 목록에 대한 취약성 대응 서비스 분류 정의

서비스 분류를 정의하여 보고 취약성 대응 및 관련 목록에 더 집중합니다. 또한 요청된 서비스 분류 수를 줄이면 데이터 수집 성능이 취약성 대응 향상될 수 있습니다.

시작하기 전에

필요한 역할: 관리자

주:

시스템 속성을 편집하려면 두 가지 모두 ServiceNow 와 취약성 대응 전문 지식이 필요합니다.

프로시저

1. 왼쪽 탐색 모음에 sys_properties_list.do 를 입력합니다.
2. 입력을 클릭합니다.
3. 검색 메뉴의 이름에서 sn_vul.service_classifications를 입력합니다.
4. *sn_vul.service_classifications* 시스템 속성을 엽니다.
5. 값 텍스트 상자에 원하는 서비스 분류의 쉼표로 구분된 목록을 입력합니다.

   주:
   이 설정이 비어 있으면 모든 서비스가 나열됩니다.

   예제:

   비즈니스 서비스, 기술 서비스 및 애플리케이션 서비스를 보고 서비스 오퍼링, 공유 서비스 및 미분류 서비스를 제외하려면 값을 비즈니스 서비스, 기술 서비스, 애플리케이션 서비스로 설정합니다.

   애플리케이션 서비스를 보려면 값을 애플리케이션 서비스로 설정합니다.

6. 업데이트를 클릭합니다.
   각 보고서 및 취약한 항목 관련 목록의 데이터는 다음에 야간 퍼포먼스 분석 작업을 실행하는 동안 서비스 분류에 따라 필터링됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약한 항목 테이블에서 선택한 필드 감사

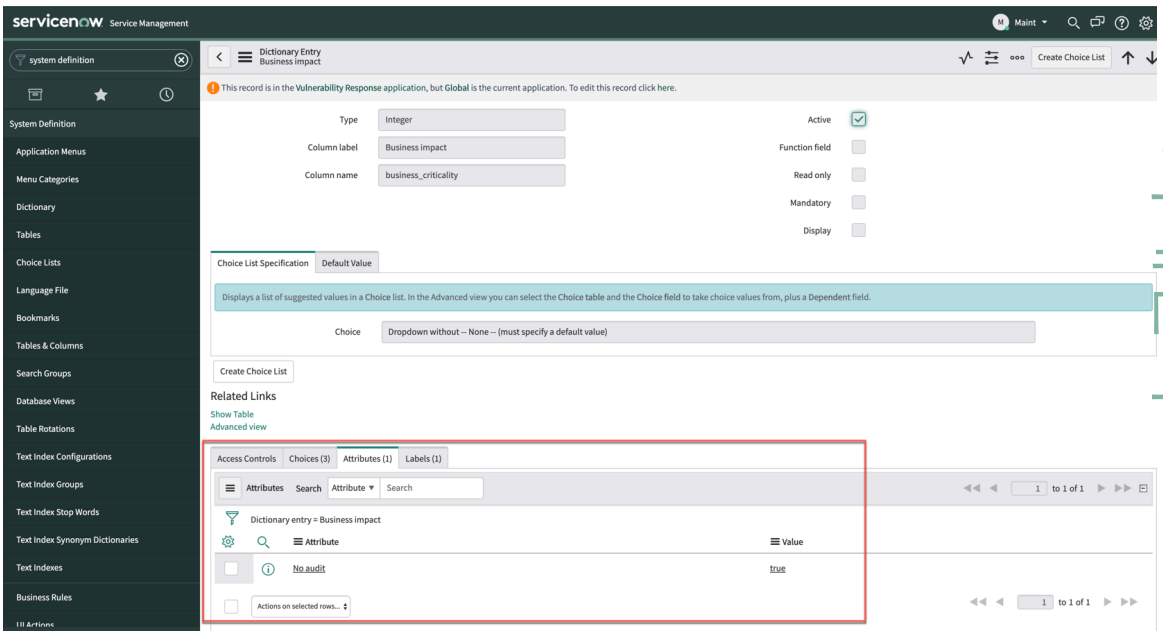
취약한 항목 [sn_vul_vulnerable_item] 테이블에 지정한 필드에 대해 감사를 활성화합니다. 이 감사 방법은 기본적으로 감사할 수 없는 필드를 감사하려는 경우에 유용합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
sn_vul_vulnerable_item 테이블은 기본적으로 감사 가능합니다. no_audit 속성이 true로 설정된 필드는 감사할 수 없습니다. 테이블 감사에 대한 자세한 내용은 테이블에 대한 감사 사용을 참조하세요.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 시스템 정의 〉 테이블 을 클릭하고 sn_vul_vulnerable_item 테이블을 검색합니다.
   테이블의 딕셔너리 항목 목록이 표시됩니다.
2. 필드에 대한 감사를 사용하려면 항목 이름을 클릭합니다.
   해당 항목에 대한 딕셔너리 항목 페이지가 표시됩니다.



3. 다음으로 이동 속성 〉 감사 없음.
   딕셔너리 속성 페이지가 표시됩니다.
4. no audit=true 속성을 제거하려면 삭제를 클릭합니다.
   이 필드에 대한 감사가 활성화됩니다.

취약성 대응 백그라운드 작업 프레임워크 구성

인스턴스에서 백그라운드 작업 프레임워크를 ServiceNow AI Platform# 정의합니다. 이러한 구성 변경은 백그라운드 작업을 실행하는 데 사용되는 시스템 자원의 양을 줄여 성능을 향상시키는 데 도움이 될 수 있습니다.

백그라운드 작업 프레임워크에서 편집할 수 있는 항목

백그라운드 작업 구성 모듈을 사용하면 프레임워크에 다음과 같은 설정 옵션이 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 프로세스에 대해 취약성 대응 동시에 실행되는 백그라운드 작업의 수를 정의할 수 있습니다.
- 백그라운드에서 실행되고 많은 양의 데이터를 처리하는 긴 작업의 경우 파티션을 생성하여 데이터를 더 작은 청크로 처리할 수 있습니다.
- 작업을 취소할 수 있습니다.

백그라운드 작업 프레임워크를 구성하는 이유

의 ServiceNow AI Platform# 백그라운드 작업은 의 기록 취약성 대응에 대해 여러 프로세스를 수행하기 위해 오랜 시간 동안 실행되도록 설계되었습니다. 이전에는 이러한 작업이 비동기식으로 실행되는 비즈니스 규칙을 기반으로 했습니다. 이러한 작업의 영향을 받는 많은 양의 기록을 처리할 수 있도록 인스턴스의 백그라운드에서 실행할 수 있는 이러한 작업의 수에는 제한이 없습니다. 완료하는 데 시간이 오래 걸리는 여러 작업이 백그라운드에서 동시에 실행되면 예약된 작업을 실행하는 데 사용되는 시스템 자원이 영향을 받아 성능에 부정적인 영향을 줄 수 있습니다.

백그라운드 작업 프레임워크를 구성하면 백그라운드 작업을 실행하는 데 사용되는 시스템 자원의 양을 줄여 성능을 향상시킬 수 있습니다.

주요 용어

직무 역량

특정 작업에 대해 설명합니다. 예를 들어 특정 작업에는 다음과 같은 기능이 포함될 수 있습니다.

- 작업은 같은 유형의 다른 작업과 동시에 실행할 수 있습니다.
- 작업을 분할할 수 있습니다.
- 실행 중에 작업을 취소할 수 있습니다.

동시 허용 사용자 수

병렬로 실행되는 작업 또는 작업의 일부를 나타냅니다.

파티션

파티션은 더 나은 성능을 달성하기 위해 병렬로 처리할 수 있도록 분할할 수 있는 작업 조각입니다. 일반적으로 실행 시간이 긴 작업을 나타냅니다.

작업 구성

특정 예약된 작업에 대한 설정을 참조합니다.

예약된 작업

예약된 작업은 특정 시간에 또는 반복 일정에서 수행할 수 있는 자동화된 작업 조각입니다.

시스템 자원

사용자 환경에서 지정된 수의 백그라운드 작업과 예약된 작업을 지원해야 하는 시스템 자원의 양을 나타냅니다.

시스템 속성

시스템 속성은 거의 또는 전혀 변경되지 않는 구성 정보를 저장합니다. 시스템 속성을 변경하거나 추가할 때마다 시스템은 캐시를 플러시하여 클러스터의 모든 노드를 동기화된 상태로 유지합니다. 이 캐시 플러시는 성능에 영향을 줍니다.

비즈니스 규칙

비즈니스 규칙은 기록이 표시, 삽입, 업데이트 또는 삭제되거나 테이블이 쿼리될 때 실행되는 서버 쪽 스크립트입니다. 비즈니스 규칙은 특정 조건이 충족될 때 양식 필드의 값을 자동으로 변경하거나 이메일 알림 및 스크립트 작업에 대한 이벤트를 만드는 등의 작업을 수행합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

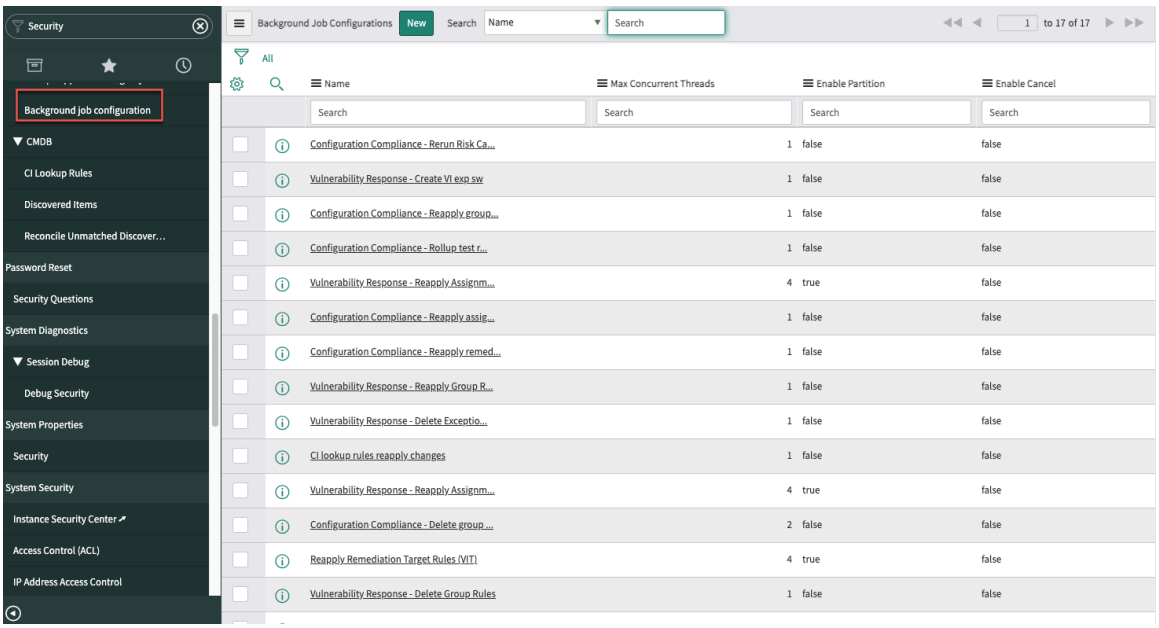
백그라운드 작업 프레임워크를 정의하기 위한 사용 사례

예를 들어, 취약한 항목 기록(VIT) 및 애플리케이션 취약성 대응 취약한 항목 기록(AVIT)에 대한 정정 대상 규칙을 적용하는 백그라운드 작업은 여러 작업이 포함된 대량의 기록을 동시에 처리합니다.

임포트의 크기와 환경에 있는 기록 수에 따라 이 작업은 사용 가능한 시스템 자원을 많이 사용할 수 있으며 성공적으로 완료하는 데 시간이 오래 걸릴 수 있습니다. 시스템 유지관리 작업이나 기타 예약된 작업은 실행 속도가 느려질 수 있습니다.

백그라운드 작업 구성 모듈, 작업은 이름 및 고유한 구성 ID별로 나열됩니다. 이러한 기록에서 지정된 백그라운드 작업에 대해 동시에 실행할 작업 수를 정의할 수 있습니다. 또한 데이터 파티션을 처리하도록 작업을 설정하여 작업을 더 빠르고 쉽게 완료하고 시스템 자원을 덜 사용하도록 할 수 있습니다. 작업이 너무 오래 실행된 것으로 판단되면 작업을 취소할 수도 있습니다.

백그라운드 작업 구성 모듈



백그라운드 작업 구성을 정의하는 데 필요한 단계에 대한 자세한 내용은 다음 문서를 참조하십시오 에서 백그라운드 작업 구성 정의 취약성 대응.

에서 백그라운드 작업 구성 정의 취약성 대응

지정된 백그라운드 작업에 대해 동시에 실행할 작업 수를 정의합니다. 또한 데이터 파티션을 가져오도록 작업을 설정하여 작업을 더 빠르고 쉽게 완료하고 시스템 자원을 덜 사용하도록 할 수 있습니다. 작업이 너무 오래 실행된 것으로 판단되면 작업을 취소할 수도 있습니다.

시작하기 전에

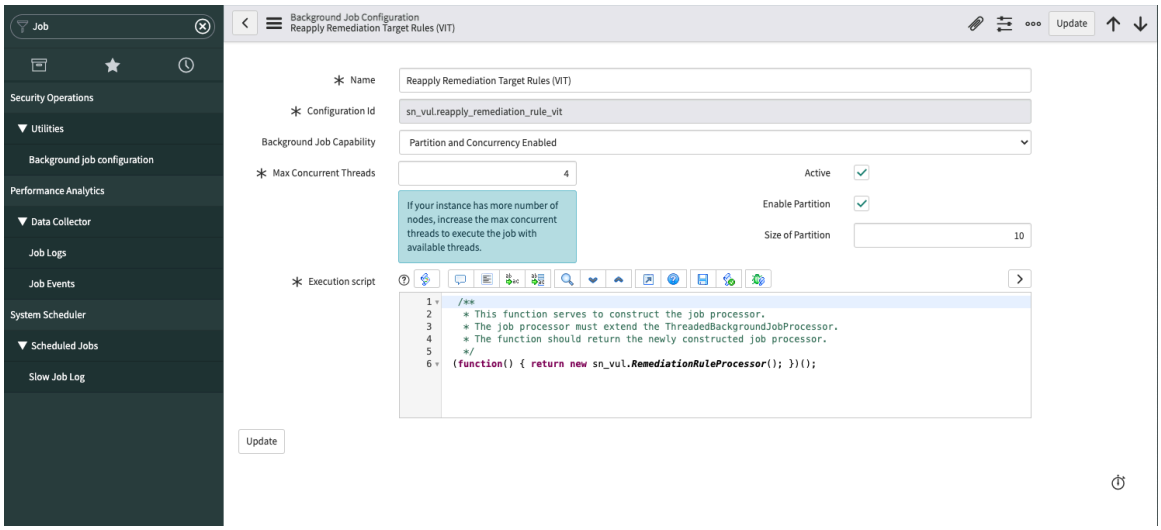
필요한 역할: sn_vul.vulnerability_admin 또는 sn_sec_cmn.manage_background_job 세분화된 역할을 가진 취약성 관리자

예를 보려면 아래 단계 섹션을 참조하십시오.

프로시저

1. 다음으로 이동 모두 〉 보안 운영 〉 백그라운드 작업 구성.
2. 이름 열에서 기록을 클릭하여 엽니다.
3. 필드를 편집합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



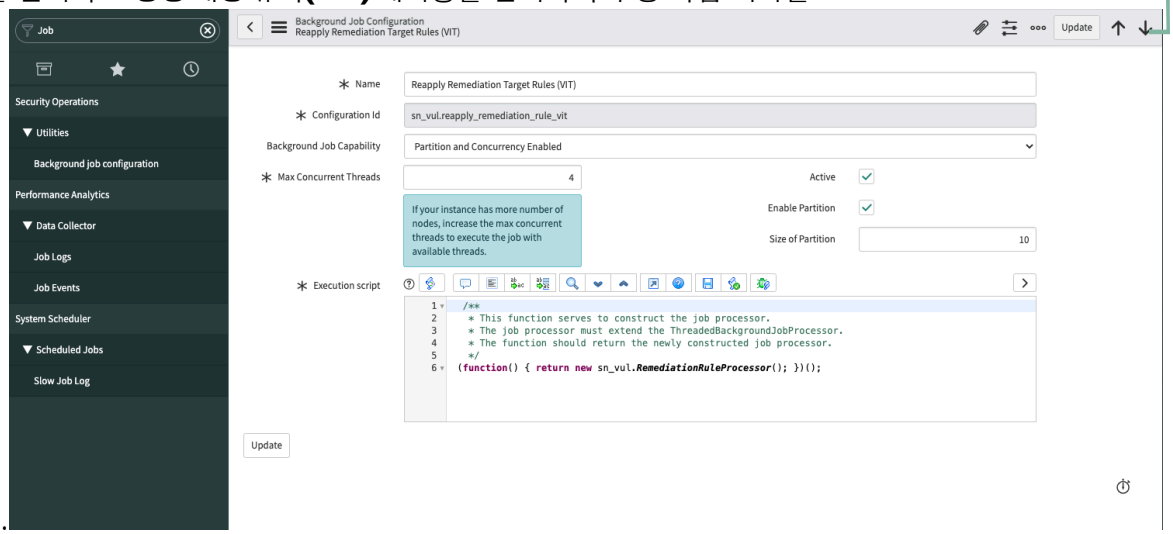
4. 변경 사항을 저장하려면 업데이트를 클릭합니다.
구성 변경에 대한 결과를 확인하는 방법은 다음 예시를 참조하십시오.

   애플리케이션에는 두 가지 정정 대상 규칙 작업 구성이 있는데, 하나는 취약한 항목에 대한 것이고 다른 하나는 애플리케이션 취약한 항목에 대한 것입니다.

   - 정정 대상 규칙(VIT) 재적용
   - 정정 대상 규칙(AVIT) 다시 적용

   정정 대상 규칙을 변경하고 사용 가능한 대부분의 시스템 처리 자원을 사용하지 않고 해당 규칙을 다시 적용하려 한다고 가정해 보겠습니다. 처리 리소스를 제한하기 위해 백그라운드 작업 구성 모듈에서 실행하는 백그라운드 작업 수와 작업당 처리하는 항목 수를 제어할 수 있습니다.

5. 이러한 설정을 정의하려면 다음으로 이동합니다. 보안 운영 〉 백그라운드 작업 구성 을 클릭하고 정정 대상 규칙**(VIT)** 재적용을 클릭하여 구성 작업 기록을 엽니다.

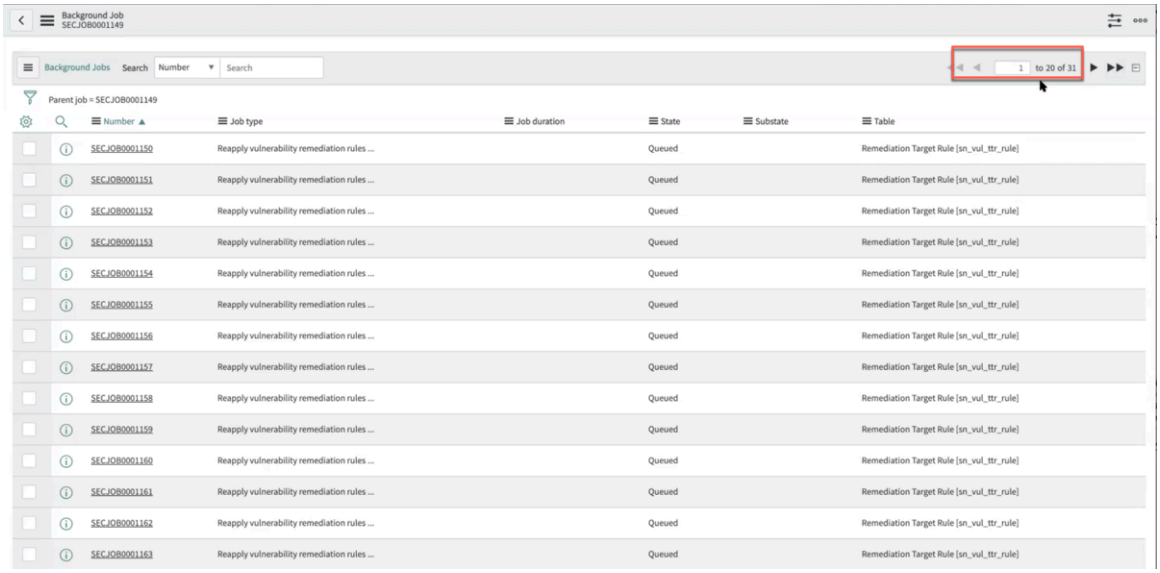


   예를 들어 VI가 300개가 조금 넘는다고 가정해 보겠습니다.

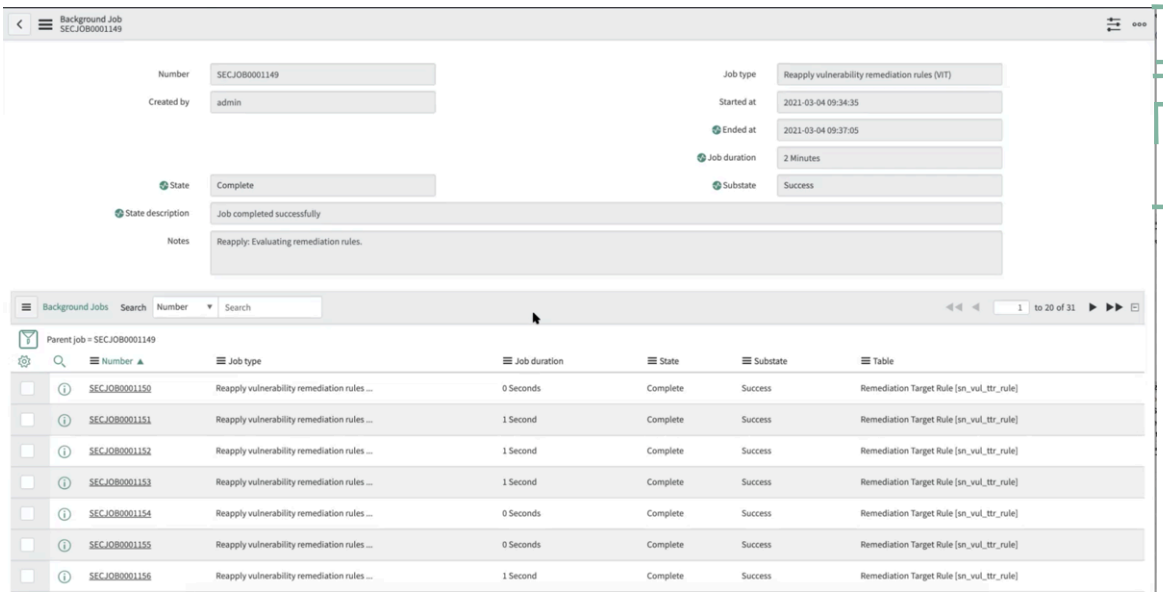
6. 열린 구성 작업 기록에서 파티션 크기 값을 **4** 에서 **10**으로 변경합니다.
7. 다음으로 이동 취약성 대응 〉 정정 대상 규칙, 변경한 취약성 정정 규칙 다시 적용을 찾아 목록에서 레코드를 선택하고 변경 내용 적용을 클릭하여 기존 VI에 대한 대상 규칙을 다시 평가합니다.
취약성 개선 규칙(VIT) 재적용 작업이 큐에 대기 중입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

8. 다음 이미지와 같이 상태 보기 링크를 클릭하여 백그라운드 작업 기록을 보고 작업이 큐에 대기하는지 확인합니다.
이 예에서는 307개의 VI(작업당 최대 10개 항목)에 대한 타겟 규칙을 처리하기 위해 31개의 작업이 생성됩니다. 이러한 작업은 기본 백그라운드 작업의 하위 작업입니다. 하위 작업은 기록을 순차적으로 처리합니다.



모든 작업이 성공적으로 완료되면 백그라운드 작업 기록의 필드가 업데이트됩니다.



9. 취약한 항목으로 이동하여 새 규칙 변경 내용이 반영되었는지 확인합니다.

에서 백그라운드 작업을 위한 고급 병렬 처리 취약성 대응

이 고급 설정을 사용하면 작업 유형에 관계없이 병렬로 처리되는 백그라운드 작업의 총 수를 제어할 수 있습니다.

시작하기 전에

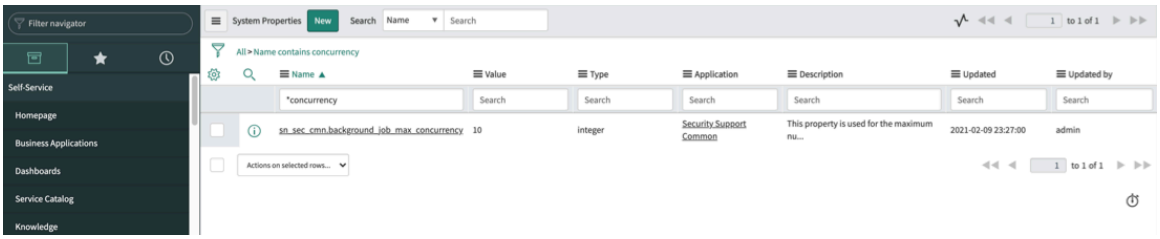
필요한 역할: sn_vul.vulnerability_admin 또는 sn_sec_cmn.manage_background_job 세분화된 역할을 가진 취약성 관리자

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
이 절차를 수행하려면 고급 프로그래밍 지식이 필요합니다.

프로시저

1. 필터 탐색기에서 **sys_properties.list** 를 *sn_sec_cmn.background_job_max_concurrency* 입력하고 시스템 속성을 찾습니다.



2. 클릭하여 기록을 엽니다.

   기본적으로 *sn_sec_cmn.background_job_max_concurrency* 시스템 속성은 최대 10개의 백그라운드 작업을 병렬로 실행합니다.

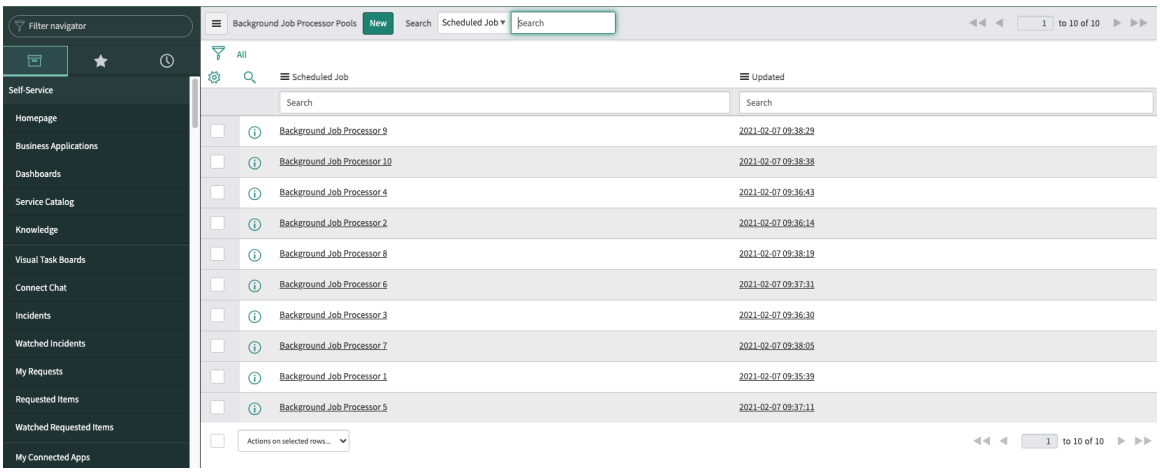
   인스턴스에 노드 수가 적은 경우 시스템 속성에서 이 값을 줄일 수 있습니다. 예를 들어, 그룹 규칙 목록에 7개의 담당 규칙이 있다고 가정해 보겠습니다. 할당 규칙 재적용 작업 구성 기록에서 최대 동시 스레드에 대해 세 개의 작업이 설정됩니다. 프레임워크의 동시성 값은 10이지만 시스템은 단일 노드 인스턴스이므로 할당 규칙 재적용 작업에서 분할된 두 작업을 동시에 처리할 수 있습니다. 최대 최대 동시 스레드를 하나의 담당 규칙 작업 기록으로 설정하면 모든 담당 규칙 재적용 작업 유형이 순차적으로 처리됩니다.

   반대로 인스턴스에 노드가 더 많으면 이 값을 늘릴 수 있지만 이렇게 변경하려면 예약된 작업도 더 추가해야 합니다.

   예약된 작업 수를 늘리려면 시스템 속성을 늘린 값과 일치해야 하는 만큼 예약된 작업을 복제합니다. 예를 들어 기본적으로 10개의 예약된 작업이 있습니다. 따라서 20개의 작업을 원하면 작업을 10번 복제해야 합니다.

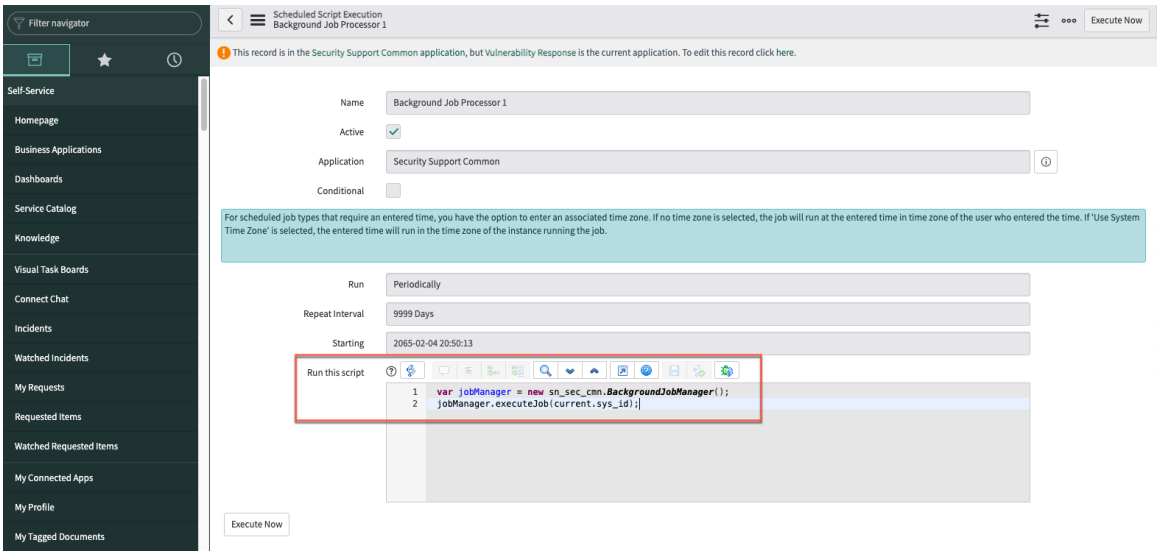
   처리를 위해 포함된 ServiceNow AI Platform# 10개의 예약된 작업이 sn_sec_cmn_background_job_processor_pool 테이블에 표시됩니다.

3. 필터 탐색기에서 **sn_sec_cmn_background_job_processor_pool.list**를 입력합니다.



4. 작업을 클릭하여 필요한 만큼 복사 및 복제하여 작업 수가 시스템 속성을 늘린 값과 일치하도록 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

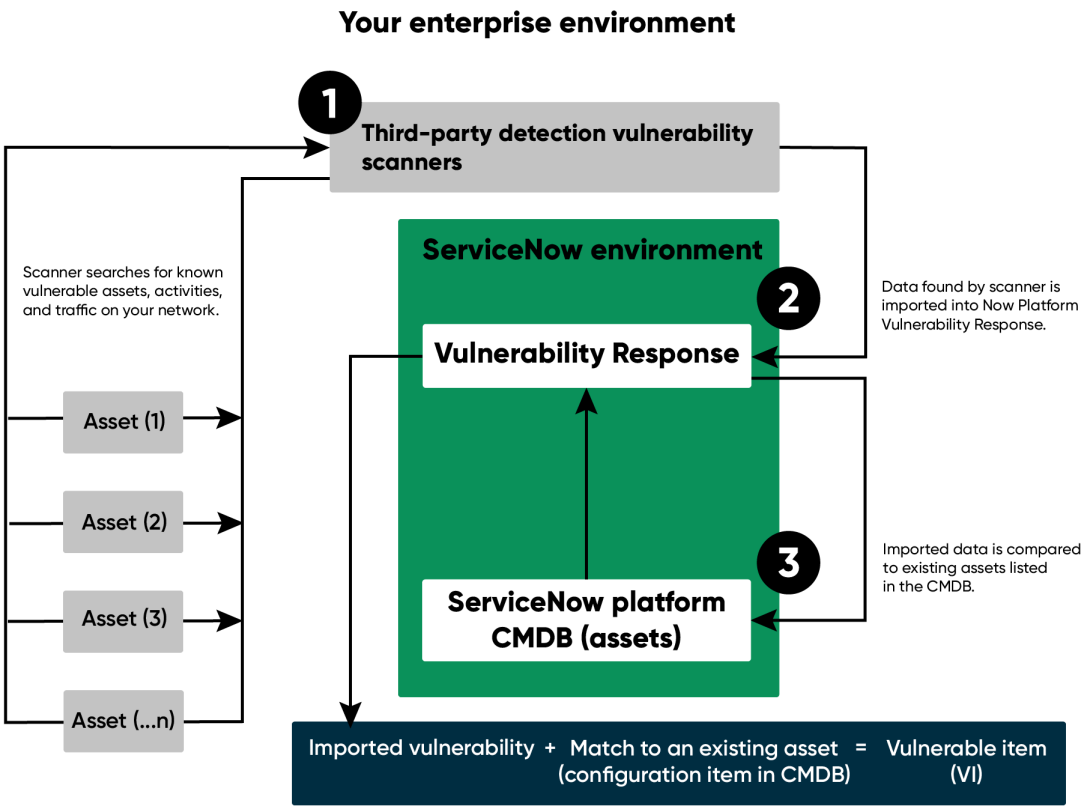


5. 예약된 작업이 정의되면 복사한 작업의 sn_sec_cmn_background_job_processor_pool 목록에서 새로 만들기를 클릭하여 참조를 추가합니다.

취약성 대응 통합

취약성 대응 에는 외부 공급업체 통합에 대한 지원이 포함됩니다. 이 섹션에는 자체 통합을 개발하기 위한 몇 가지 기본 지침이 포함되어 있습니다.

외부 공급업체 통합



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

NVD(국가 취약성 데이터베이스)에서 임포트한 취약성과 외부 공급업체 스캐너의 탐지 데이터가 CMDB의 자산과 조정됩니다. 임포트한 취약성이 기존 자산과 일치하면 취약한 항목이 생성됩니다. 취약한 항목은 정정 작업으로 자동 그룹화되고, 비즈니스 컨텍스트에 따라 위험 점수가 매겨지며, 정정을 위해 우선순위가 지정되고 적절한 팀에 할당됩니다.

주:

타사 통합은 별도로 처리됩니다. 사용자 환경에서 둘 이상의 외부 공급업체 통합 애플리케이션이 사용 중인 경우 통합 전반에 걸쳐 VI(취약한 항목) 중복 제거가 없습니다. 예를 들어 및 사이의 Qualys VI 중복 Rapid7 제거는 사용할 수 없습니다.

그러나 IP, 포트 등에서 중복을 제거하기 때문에 타사 스캐너(예 Qualys:)와 인스턴스의 ServiceNow VI 간의 탐지 수가 일치하지 않을 수 있습니다.

[store-future: BEGIN review〕다음 표에는 취약성을 임포트하고 취약한 항목을 생성하기 위해 만든 파트너 및 파트너가 만든 ServiceNow# 인프라 통합 목록이 취약성 대응 나와 있습니다.
〔store-future: BEGIN review〕

Vulnerability Response - 인프라 통합

벤더	벤더 제품	통합 요약	스토어 링크	주요 기능	작성자
Tenable	• Tenable.io • Tenable.sc	자산을 일치시키고 외부 공급업체 취약성을 임포트하여 취약한 항목을 생성합니다. **주:** Tenable.io 는 에이전트 기반 컴퓨터에서 다시 스캔 시작을 지원하지 않습니다.		• 취약성 다시 스캔 • 솔루션 데이터 • 외부 공급업체 정의 • 태그 지정	ServiceNow#
Rapid7	Rapid7 InsightVM	자산을 일치시키고 타사 취약성을 임포트하여 취약한 항목을 생성합니다.			ServiceNow#
Qualys	Qualys VMDR	자산을 일치시키고 타사 취약성을 임포트하여 취약한 항목을 생성합니다.		요청 시 다시 스캔합니다.	ServiceNow#
CrowdStrike	Crowdstrike Falcon 스포트라이트	자산을 일치시키고 NVD를 사용하여 취약한 항목을 생성합니다.		• NVD 정의입니다. • 임포트 시 태그 기반 필터링을 지원합니다.	파트너
Microsoft	Microsoft Defender 취약성 관리	자산을 일치시키고 엔드포인트 취약성을 임포트하여 취약한 항목을 생성합니다.		외부 공급업체 정의.	ServiceNow#

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Vulnerability Response - 인프라 통합

벤더	벤더 제품	통합 요약	스토어 링크	주요 기능	작성자
Microsoft	Microsoft Defender for IoT IoT용 Microsoft Azure Defender	취약성을 ServiceNow 운영 기술 취약성 대응 로 임포트하고 프로덕션 프로세스 컨텍스트로 위험 기반 조치를 취합니다.			ServiceNow#
Cisco (케나)	Kenna.VM	자산을 일치시키고 NVD를 사용하여 취약한 항목을 생성합니다. Kenna 위험 점수를 포함합니다.		• NVD 정의 • 솔루션 데이터	파트너
Tanium	준수	자산을 일치시키고 외부 공급업체 취약성을 임포트하여 취약한 항목을 생성합니다.			파트너
범고래	Orca 보안	자산을 일치시키고 외부 공급업체 취약성을 임포트하여 취약한 항목을 생성합니다.			파트너
오냅시스	Onapsis for SAP 취약성	자산을 일치시키고 외부 공급업체 취약성을 임포트하여 SAP 자산 및 애플리케이션에 대한 취약한 항목을 생성합니다.			파트너
시낙	Synack 레드팀	Synack에서 취약성을 임포트합니다.			파트너
Wiz	Wiz	클라우드 자산을 일치시키고 외부 공급업체 취약성을 임포트하여 취약한 항목을 생성합니다.			파트너
레이스 세공	레이스 세공	클라우드 자산 소스에서 인프라 취약성을 임포트합니다.		취약성 계산기와 심각도에 따른 필터링을 지원합니다.	파트너
Recorded Future	VR용 공격 표면 인텔리전스	ServiceNow Vulnerability Response로 임포트된 외부 공격 표면 자산 및 노출입니다. 외부 자산 탐지에서 취약한 항목을 생성합니다.			파트너

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Vulnerability Response - 인프라 통합

벤더	벤더 제품	통합 요약	스토어 링크	주요 기능	작성자
		기록된 미래 위협 및 취약성 보강을 포함합니다.			
맨디언트	Mandiant 공격 표면 관리	Mandiant 공격 표면 관리 플랫폼에서 취약성 및 취약한 항목에 대한 정보를 임포트합니다.			파트너
IBM	보안 가드움	IBM Guardium 데이터베이스 취약성 스캔 결과를 ServiceNow#.			파트너
CyCognito	CyCognito SaaS	Cycognito SaaS 플랫폼에서 문제 및 자산 임포트			파트너
VMware	카본 블랙 클라우드	VMwareCarbon Black Cloud에서 취약성 데이터와 컨텍스트를 수집합니다. Carbon Black Cloud 끝점 및 작업 부하에서 구성 항목을 생성합니다.			파트너
핵	취약성 관리	Nucleus Security에서 결과를 가져옵니다. 취약한 항목을 자동으로 업데이트합니다. 의견 필드를 통한 양방향 업데이트. 사용자 지정 필드를 매핑합니다.			파트너
InfoSec 글로벌 (ISG)	AgileSec 분석	암호화 자산에 대한 취약성 찾기를 임포트합니다. 암호화 키, 키 저장소 및 라이브러리.			파트너
센시스	외부 공격 표면 관리	인터넷 연결 자산의 취약성을 스캔, 검색 및 카탈로그화합니다.			파트너

〔End〕
[End]

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

에서 애플리케이션 취약성 대응 지원하는 외부 공급업체 통합에 대한 자세한 내용은 다음을 참조하십시오. 다른 애플리케이션과 애플리케이션 취약성 대응의 통합

- CISA Known Exploit Vulnerability(KEV) 통합
- Microsoft Threat and Vulnerability Management 취약성 통합 이해
- 와 HCL BigFix 패치 오케스트레이션의 통합 이해 취약성 대응
- SCCM 취약성 대응 과의 Microsoft 패치 오케스트레이션 통합 이해
- NVD 통합 이해
- Qualys Vulnerability Integration
- Rapid7 취약성 통합 이해
- Shodan Exploit Integration
- Tenable 취약성 통합 이해
- Microsoft Security Response Center 솔루션 통합

  는 Microsoft Security Response Center 솔루션 통합 와 함께 사용할 수 있습니다 취약성 솔루션 관리. 및 의 Red Hat Solution Integration설치 및 구성에 Microsoft Security Response Center 솔루션 통합 대한 자세한 내용은 을 참조하십시오취약성 대응용 솔루션 관리 애플리케이션 설치. 설정 도우미 내에서 요청 시 및 Microsoft Security Response Center 솔루션 통합 를 Red Hat Solution Integration 구성, 편집, 예약 및 시작할 수 있습니다.

통합에 대한 추가 참고 사항

통합에 대해 여러 배포가 지원되는 경우 문서를 참조하십시오 통합을 위해 도메인 분리 임포트 작성.

- 설치 도우미 내에서 요청 시 많은 통합 애플리케이션을 설치, 구성, 예약 및 시작할 수 있습니다.
- 설정 도우미에서 Rapid7 취약성 통합 애플리케이션을 설치할 수 있지만 설정 도우미 내에서 이 통합에 대한 구성은 지원되지 않습니다. 자세한 내용은 Rapid7 취약성 통합 설치 문서를 참조하십시오.
- Tenable에 의한 애플리케이션은 Tenable에 Tenable for Vulnerability Response 의해 생성되고 유지관리됩니다. 다음에서 문서를 참조하십시오. Tenable for Vulnerability Response.

통합 실행 중에 여러 프로세스가 생성되고 데이터가 페이지 형식으로 수신됩니다. 각 프로세스에는 페이지에 첨부된 데이터가 있는 하나 이상의 임포트 큐 항목이 포함될 수 있습니다. 이러한 항목은 1시간의 시간 제한 내에 데이터를 처리해야 합니다. 그러나 페이로드 크기가 크면 처리 시간이 1시간을 초과하거나 중단되어 통합 시간 제한 오류가 발생할 수 있습니다. 통합은 시간 초과 오류에도 불구하고 데이터를 계속 처리합니다. 이러한 잘못된 통신을 피하기 위해 버전 18.2.4 취약성 대응부터 큐가 활성 상태이고 데이터를 처리하는지 여부를 나타내기 위해 타임스탬프(하트비트)가 주기적으로 전송됩니다. 임포트 큐 항목 페이지의 처리된 마지막 기록 필드는 임포트 큐가 생성하거나 업데이트하는 기록 수에 따라 업데이트됩니다. 임포트 큐 항목이 1시간의 시간 제한을 초과하는 경우, 시스템은 마지막으로 처리된 기록 필드를 검사하여 1시간보다 오래되었는지도 확인합니다. 이 경우 이는 임포트 큐 항목이 고착되었음을 나타내며 처리 시 더 이상의 지연을 방지하기 위해 시간 초과됩니다.

주:
마지막으로 처리된 기록 필드는 다음 시스템 속성에 정의된 내용에 따라 업데이트됩니다.

- *sn_sec_cmn.record_threshold_heartbeat*: 하트비트(타임스탬프)가 임포트 큐 항목으로 전송된 후 처리된 기록 수를 정의합니다.
- *sn_sec_cmn.maximum_heartbeat_delay*: 임포트 큐 항목을 시간 초과해야 하는 시간을 정의합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

VR v17.1부터 다음 통합 프로세스 상태 이름이 업데이트되었습니다.

V17.1 이전의 상태 이름	상태 이름 **V17.1** 이상
처리 중	검색 중
WaitComplete	대기/처리 중

주:
다운로드되어 처리된 첨부 파일을 볼 수 있습니다. 통합 실행의 상태가 ## ##이면 완료된 통합의 백분율이 표시됩니다.

[store-future: BEGIN review]v22.1.2 부터 취약성 대응제외 규칙을 사용하여 취약성이 수집되지 않도록 제외할 수 있습니다. 또한 , Qualys, Tenable for Vulnerability Response, Microsoft Defender 취약성 관리 통합을 실행Rapid7하거나 취약성을 수동으로 수집하는 경우 제외된 탐지 수를 볼 수 있습니다. 이 정보는 통합 실행 화면의 탐지 탭에서 액세스할 수 있습니다. 자세한 내용은 제외 규칙 개요 및 제외 규칙 생성 문서를 참조하십시오.[End]

취약성 대응 애플리케이션 및 **CSDM** 테이블

, 취약성 대응애플리케이션 취약성 대응, 타사 취약성 통합 및 소프트웨어 자재 명세서 애플리케이션은 테이블을 관리(데이터 기여) CSDM 합니다. 이러한 애플리케이션은 다른 애플리케이션이 생성하는 테이블의 데이터 CSDM 도 사용합니다. 따라서 여러 ServiceNow 제품이 이러한 보안 운영 애플리케이션의 이점을 누리고 가치를 더합니다. 자세한 내용은 취약성 대응 애플리케이션 및 CSDM 테이블 문서를 참조하십시오.

수동으로 생성된 통합

필요에 따라 애플리케이션으로 ServiceNow Store 사용할 수 없는 다른 통합을 추가할 수 있습니다. 자세한 내용은 취약성 통합을 수동으로 생성 문서를 참조하십시오.

NVD 통합 이해

NVD 통합은 NIST(National Institute of Standards and Technology) NVD(국가 취약성 데이터베이스) 제품에서 임포트한 데이터를 사용하여 코드 결함의 영향과 우선순위를 파악하는 데 도움을 줍니다. 외부 공급업체 스캐너 제품을 사용하여 취약성 데이터를 인스턴스로 임포트하기 전에 초기 설정 취약성 대응 의 일부로 이 통합을 실행합니다.

스토어에서 앱 요청

ServiceNow Store 웹 사이트를 방문하면 사용 가능한 모든 앱을 확인하고 스토어에 요청을 제출하는 방법에 대한 정보를 참조할 수 있습니다. 출시된 모든 앱의 누적 릴리스 정보는 ServiceNow Store 버전 기록 릴리스 정보 를 참조하십시오.

NIST NVD는 CVE(Common Vulnerabilities and Exposures) 및 CPE(Common Platform Enumeration) 데이터를 모두 수집하고 해당 데이터를 ServiceNow AI Platform#. 와 취약성 대응 쉽게 통합되어 CVE 및 CPE 취약성을 매핑하여 인스턴스의 데이터를 보강합니다.

중요사항:
각 통합 기록에 대해 구성된 실행 사용자가 있습니다. 이 사용자의 기본값은 VR입니다. 시스템. 이 값은 변경하지 마십시오.

설치가 완료되면 NIST CVE(국가 취약성 데이터베이스 통합-API) 통합이 예약된 작업으로 자동으로 호출되고 매일 실행됩니다. 예약된 개별 작업을 수동으로 실행할 수도 있습니다. 예약된 작업은 인스턴스를 다른 취약성 관리 시스템과 동기화된 상태로 유지하여 취약성 정정 수명주기를 단순화합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

팁:
프로덕션 인스턴스에서 이 플러그인을 활성화하려면 별도의 라이센스가 필요할 수 있습니다.

사용 가능한 버전

릴리스 버전	릴리스 정보
취약성 대응 NVD v1.2와 통합	

NVD 및 CWE 통합을 사용하여 취약성 데이터의 초기 임포트

1. CWE Comprehensive 2000 Integration을 사용하여 CWE 데이터의 초기 임포트를 수행합니다.

   CWE 기록을 업데이트하기 위해 예약된 작업을 구성하고 실행합니다. 문서를 참조하십시오. 기본적으로 통합 기록에서 요청 시 CWE 업데이트를 수행하며, 이를 구성해야 합니다.

   주:
   NVD 데이터베이스 업데이트 전에 실행되도록 CWE 업데이트를 예약합니다. NVD 업데이트의 기본 요일은 매주 월요일입니다.

2. 취약성 대응 NVD와 통합 애플리케이션이 설치되었고 NIST 국가 취약성 데이터베이스 통합 API(CVE만) 또는 NIST 국가 취약성 데이터베이스 통합 API(CVE 및 CPE)에서 초기 데이터 임포트가 성공했는지 확인합니다.

   CPE의 경우 NIST 국가 취약성 데이터베이스 통합 API(CPE 한정)에서 초기 데이터 임포트가 성공했는지 확인합니다.

   프로덕션 인스턴스에서 이 플러그인을 활성화하려면 별도의 라이센스가 필요할 수 있습니다. 플러그인이 설치되면 NIST 국가 취약성 데이터베이스 통합 API(CVE만)가 기본적으로 활성화됩니다. 매일 실행됩니다. 자세한 내용은 취약성 대응 NIST 국가 취약성 데이터베이스와의 통합 설치 문서를 참조하십시오.

3. 타사 라이브러리는 예약된 작업으로 업데이트됩니다. 외부 공급업체 통합에 대한 자세한 내용은 통합 설명서를 참조하십시오 취약성 대응 통합 .

임포트한 취약성 데이터 및 취약한 항목 이해

해당 ServiceNow AI Platform 인스턴스에서 임포트된 각 취약성은 예를 들어 와 같은 Qualys외부 공급업체 스캐너 제품의 소스 라이브러리에 있는 취약성 항목으로 표시됩니다. 인스턴스에서 임포트되고 업데이트되는 취약한 항목(VI)은 라이브러리와 같은 외부 공급업체 라이브러리에 대한 참조입니다 Qualys . 타사 라이브러리는 NVD를 다시 참조할 수 있습니다.

예를 들어 와 같은 Qualys제품에서 타사 취약성 데이터를 수집하면 QID(Qualys 식별자)를 참조하는 VI를 수집하게 됩니다. 의 경우 QualysQID는 NVD 라이브러리의 CVE를 참조합니다. 애플리케이션의 정정 작업 또는 취약한 항목 기록에서 해당 QID를 취약성 대응 클릭하고 NVD 및 CWE 통합을 실행하여 데이터를 수집하면 VI와 CVE , CWE 및 CPE 간에 존재하는 관계를 볼 수 있는 현재의 보강된 취약성 데이터를 볼 수 있습니다.

자체 라이브러리가 있는 외부 공급업체 스캐너 제품을 Qualys 실행하기 전에 먼저 최소한 NIST 국가 취약성 데이터베이스 통합 API(CVE만 해당) 통합(CISA 관련 세부 정보도 포함), CWE 통합을 설치하고 실행하여 취약성 데이터를 수집해야 합니다. 이러한 NVD 및 CWE 데이터 임포트는 타사 제품으로 데이터를 임포트하기 전에 OR 애플리케이션 취약성 대응 데이터를 보강 취약성 대응 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

NVD, CWE 및 외부 공급업체 라이브러리의 관리 및 보기에 대한 자세한 내용은 및 취약성 라이브러리 보기 취약성 대응를 참조하십시오NVD 및 CWE 통합을 통해 데이터를 임포트하고 외부 공급업체 라이브러리를 관리합니다.

NVD 임포트가 성공했는지 확인한 후 취약성 데이터를 CWE 기록을 업데이트하기 위해 예약된 작업을 구성하고 실행합니다.더욱 보강하려면 .

외부 공급업체 제품과 함께 취약성 데이터를 임포트하기 전에 NVD 및 CWE 임포트를 수행합니다. 타사 라이브러리는 예약된 작업으로 업데이트됩니다. 외부 공급업체 통합에 대한 자세한 내용은 통합 설명서를 참조하십시오 취약성 대응 통합 .

NVD 통합 찾기

NVD 통합을 보려면 다음으로 이동합니다. **Vulnerability Response** 또는 **Application Vulnerability Response** 〉 관리 〉 통합.

기본 시스템에는 다음과 같은 통합이 포함됩니다.

주:
기본적으로 NIST 국가 취약성 데이터베이스 통합 API(CVE만) 통합만 활성화되어 있습니다.

NVD 통합

통합	설명
NIST 국가 취약성 데이터베이스 통합 - API(CVE만)	NIST NVD 취약성 데이터(CVE)만 검색합니다. 기본적으로 이 통합은 매일 실행하도록 자동 설정됩니다.
NIST 국가 취약성 데이터베이스 통합- API(CPE만 해당)	NIST NVD에서 CPE 데이터를 검색합니다. 이 통합은 기본적으로 비활성 상태입니다. 정식 이름 형식, 시스템에 대해 이름을 검사하는 방법, 텍스트 및 테스트를 이름에 바인딩하기 위한 설명 형식을 포함하는 CPE 데이터를 캡처하려면 이 통합을 활성화합니다. 이 정보는 취약한 소프트웨어에 저장됩니다. 이 통합은 매일 실행되도록 설정되고 기본적으로 비활성 상태입니다. 이 통합을 활성화하려면 문서를 NIST 국가 취약성 데이터베이스–API 활성화(CPE만 해당)참조하십시오.
NIST 국가 취약성 데이터베이스 통합- API(매핑되지 않은 CPE)	NIST NVD에서 가져온 CVE와 연결된 CPE 데이터를 검색합니다. 이 통합은 기본적으로 비활성 상태입니다. 정식 이름 형식, 시스템에 대해 이름을 검사하는 방법, 텍스트 및 테스트를 이름에 바인딩하기 위한 설명 형식을 포함하는 CPE 데이터를 캡처하려면 이 통합을 활성화합니다. 이 정보는 NVD 취약성 항목 레코드 관련 목록에 저장됩니다. 이 통합은 요청 시 실행되도록 설정되며 기본적으로 비활성 상태입니다. 이 통합을 활성화하려면 문서를 NIST 국가 취약성 데이터베이스–API(매핑되지 않은 CPE) 활성화참조하십시오.

중요사항:
"NIST 국가 취약성 데이터베이스 통합-API(CVE 및 CPE)" 통합은 더 이상 사용되지 않습니다.

통합 실행 상태는 문서를 참조하십시오 (국가 취약성 데이터베이스) NVD 통합 임포트 실행 상태 보기.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

NVD 통합 준비

성공적인 통합을 위해서는 통합 전 작업을 계획하고 신중하게 실행해야 합니다. 다음 작업을 수행하여 통합을 준비합니다. NVD 통합에서는 사용자가 NIST NVD(국가 취약성 데이터베이스)에 익숙하다고 가정합니다.

필요한 역할: 관리자

주:
NVD 통합을 실행하기 전에 요구 사항에 따라 필요한 구성을 변경합니다.

각 통합 기록에 대해 구성된 실행 사용자가 있습니다. 이 사용자의 기본값은 VR입니다. 시스템. 이 값은 변경하지 마십시오.

CWE 기록을 업데이트하기 위해 예약된 작업을 구성하고 실행합니다.

CWE에서 데이터를 임포트하면 인스턴스의 취약성 데이터가 더욱 보강됩니다. 취약성을 에스컬레이션해야 하는지 여부를 결정할 때 CWE 데이터베이스에서 다운로드한 CWE(일반적인 약점 열거) 기록을 참조용으로 사용합니다. 외부 공급업체 스캐너 제품을 사용하여 취약성 데이터를 인스턴스로 임포트하기 전에 초기 설정 취약성 대응 의 일부로 이 통합을 실행합니다.

시작하기 전에

필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)

주:
NVD 데이터베이스 업데이트 전에 실행되도록 CWE 업데이트를 예약합니다. NVD 업데이트의 기본 요일은 매주 월요일입니다.

정기적으로 Common Weakness Enumeration 데이터베이스에서 일반 약점 기록을 업데이트합니다. 기본 스크립트를 업데이트하거나 필요에 따라 스크립트를 직접 작성할 수도 있습니다.

각 CWE 기록에는 약점을 설명하는 관련 지식 문서도 포함되어 있습니다. 일반 약점 열거 페이지에서 취약성을 에스컬레이션할 수 없습니다.

- 관리자 역할이 있는 경우 예약된 작업에 리포지토리를 추가할 수 있습니다.
- sn_vul.vulnerability_read가 있으면 예약된 작업을 실행할 수 있습니다.
- sn_vul.vulnerability_write가 있는 경우 예약된 작업의 상세 정보를 편집할 수 있습니다.

이 태스크 정보

통합 실행 중에 여러 프로세스가 생성되고 데이터가 페이지 형식으로 수신됩니다. 각 프로세스에는 페이지에 첨부된 데이터가 있는 하나 이상의 임포트 큐 항목이 포함될 수 있습니다. 이러한 항목은 1시간의 시간 제한 내에 데이터를 처리해야 합니다. 그러나 페이로드 크기가 크면 처리 시간이 1시간을 초과하거나 중단되어 통합 시간 제한 오류가 발생할 수 있습니다. 통합은 시간 초과 오류에도 불구하고 데이터를 계속 처리합니다. 이러한 잘못된 통신을 피하기 위해 버전 18.2.4 취약성 대응부터 큐가 활성 상태이고 데이터를 처리하는지 여부를 나타내기 위해 타임스탬프(하트비트)가 주기적으로 전송됩니다. 임포트 큐 항목 페이지의 처리된 마지막 기록 필드는 임포트 큐가 생성하거나 업데이트하는 기록 수에 따라 업데이트됩니다. 임포트 큐 항목이 1시간의 시간 제한을 초과하는 경우, 시스템은 마지막으로 처리된 기록 필드를 검사하여 1시간보다 오래되었는지도 확인합니다. 이 경우 이는 임포트 큐 항목이 고착되었음을 나타내며 처리 시 더 이상의 지연을 방지하기 위해 시간 초과됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
마지막으로 처리된 기록 필드는 다음 시스템 속성에 정의된 내용에 따라 업데이트됩니다.

- *sn_sec_cmn.record_threshold_heartbeat*: 하트비트(타임스탬프)가 임포트 큐 항목으로 전송된 후 처리된 기록 수를 정의합니다.
- *sn_sec_cmn.maximum_heartbeat_delay*: 임포트 큐 항목을 시간 초과해야 하는 시간을 정의합니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 통합.
2. **CWE Comprehensive 2000 Integration** 예약 작업을 선택합니다.
3. 필요한 경우 필드를 수정합니다.

취약성 통합 양식

필드	설명
이름	예약된 작업의 이름입니다.
활성	예약된 작업이 활성 상태인지 여부입니다. 특정 기간 동안 작업을 실행하지 않으려면 사용할 매개변수를 설정하고 작업을 비활성화할 수 있습니다.
실행	작업을 실행할 빈도입니다. 후속 필드는 이 필드의 설정에 따라 표시되거나 숨겨집니다. 주: CWE 업데이트는 기본적으로 요청 시입니다. NVD 업데이트 이전의 예약된 기간으로 설정합니다. 선택 항목은 다음과 같습니다. ○ 매일: 시간 선택 ○ 주별: (가장 일반적인 선택) 날짜 및시간 선택 ○ 월별: 날짜 및 시간 선택 ○ 주기적으로: 반복 간격, 시작 날짜 및 시간을 선택합니다. ○ 한 번: 시작 날짜 및 시간 선택
일	예약된 작업을 실행하려는 요일입니다. 실행 필드에서 매주를 선택한 경우 이 필드에 요일이 표시됩니다. 실행 필드에서 매월을 선택한 경우 이 필드에 월의 일수가 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	주: NVD 데이터베이스 업데이트 전에 실행되도록 CWE 업데이트를 예약합니다. NVD 업데이트의 기본 요일은 매주 월요일입니다.
시간	예약된 작업을 시작할 시간입니다. 주: NVD 데이터베이스 업데이트 전에 실행되도록 CWE 업데이트를 예약합니다. NVD 업데이트의 기본 시간은 01:00:00입니다
통합 스크립트	데이터 소스 관련 목록에 지정된 데이터 소스에서 데이터를 끌어오기 위한 스크립트입니다.
소스 통합	〔읽기 전용〕
소스 인스턴스	〔읽기 전용〕
애플리케이션	〔읽기 전용〕 예약된 작업을 실행 중인 애플리케이션의 이름입니다.
반복 간격	예약된 작업이 다시 실행되기까지 걸리는 일 및 시간입니다. 이 필드는 실행 목록에서 주기적으로를 선택한 경우에 나타납니다.
시작 중	정기 업데이트를 시작하는 날짜 및 시간입니다. 이 필드는 실행 목록에서 주기적으로를 선택한 경우에 나타납니다.
조건부	조건부 매개변수를 추가하는 확인란입니다.
조건	예약 작업을 실행하기 위한 조건입니다. 이 필드는 조건부 확인란이 선택된 경우에 나타납니다.
프로세서 전략 보고	데이터를 끌어오고 예약된 작업을 처리하기 위한 전략입니다. ○ 통합 스크립트 필드의 스크립트를 사용하여 데이터 소스 관련 목록의 데이터 소스에서 데이터를 끌어오려면 데이터 소스 첨부 파일을 선택합니다. ○ 보고서 프로세서 스크립트 필드에서 사용자 지정 프로세서를 선택하려면 사용자 지정 보고서 프로세서를 선택합니다.
보고서 프로세서	예약된 작업이 실행될 때 실행할 스크립트입니다. 이 필드는 보고서 프로세서 전략 목록에서 사용자 지정 보고서 프로세서가 선택된 경우에 나타납니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
프로세서 공장 스크립트	보고서 프로세서를 빌드할 스크립트입니다. 이 필드는 보고서 프로세서 전략 목록에서 사용자 지정 보고서 프로세서가 선택된 경우에 나타납니다.

4. 헤더를 마우스 오른쪽 버튼으로 클릭하여 변경 내용을 저장합니다 .
5. 예약된 작업을 즉시 실행하려면 지금 실행을 클릭합니다.
   취약성 통합 뷰로 돌아갑니다.
6. 임포트 진행률을 보려면 **CWE Comprehensive 2000 Integration** 예약 작업을 다시 선택하고 취약성 통합 실행 탭을 선택하십시오.

   임포트한 항목을 보려면 을 참조하십시오 취약성 라이브러리 보기 취약성 대응 .

취약성 대응 **NIST** 국가 취약성 데이터베이스와의 통합 설치

인스턴스에서 통합을 실행하기 전에 설치 및 구성 단계를 완료해야 NIST NVD(국가 취약성 데이터베이스) 제품이 취약성 대응. 이 애플리케이션은 별도의 구독으로 사용할 수 있습니다.

시작하기 전에

설치하기 전에 다음 설정 검사 목록을 완료합니다. 이러한 설정 작업은 원활한 설치 및 구성을 위해 필요합니다.

주:
이 프로세스는 프로덕션 인스턴스에 다운로드된 애플리케이션에만 적용됩니다. 애플리케이션을 비프로덕션 또는 개발 인스턴스에 다운로드하는 경우에는 권리를 얻을 필요가 없습니다. 로 애플리케이션 활성화 ServiceNow Store계속 진행합니다.

작업 설정	설명
애플리케이션이 설치되고 활성화되었는지 취약성 대응 확인합니다.	이 애플리케이션이 활성화되었는지 확인하려면 다음으로 이동하십시오. 구독 관리 〉 구독 인스턴스에 있습니다. 목록에 조직이 구매한 구독이 표시됩니다. 애플리케이션이 설치 및 활성화되지 않은 경우를 참조하십시오 취약성 대응 설치.
인스턴스에 필요한 ServiceNow 역할이 있는지 확인합니다.	예상 결과의 설치, 구성 및 검증에 필요한 역할은 다음과 같습니다. • 아직 할당되지 않은 경우 시스템 관리자 〔admin〕가 애플리케이션을 설치하고 의 취약성 대응 취약성 관리자 또는 의 App-Sec 관리자 그룹에 애플리케이션 취약성 대응사용자를 할당합니다. 의 취약성 대응 그룹 역할에 대한 자세한 내용은 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응. 의 애플리케이션 취약성 대응 그룹 역할에 대한 자세한 내용은

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업 설정	설명
	문서를 참조하십시오 애플리케이션 취약성 대응 사용자 그룹 및 역할. • 취약성 관리자 또는 App-Sec 관리자는 구성을 감독하고 예상 결과를 검증합니다.

필요한 역할: admin

주:
NVD 통합을 실행하기 전에 요구 사항에 따라 필요한 구성을 변경합니다.

각 통합 기록에 대해 구성된 실행 사용자가 있습니다. 이 사용자의 기본값은 VR입니다. 시스템. 이 값을 변경하지 마십시오.

프로시저

1. NVD 통합을 설치할 인스턴스에 로그인합니다.
2. ServiceNow Store로 이동합니다.
3. 에서 ServiceNow StoreNVD와 취약성 대응 통합 애플리케이션을 검색합니다.
4. 애플리케이션 타일을 선택합니다.
   설치 중인 애플리케이션에 대한 자세한 정보가 표시됩니다.

   주:
   해당하는 경우 다른 요구 사항 및 종속성 섹션을 읽어보십시오.

5. 요청 앱을 선택하고 로그인 자격 증명을 입력합니다Now Support.
6. 가져오기를 선택합니다.
7. 인스턴스의 인스턴스 이름과이유를 입력하고 인스턴스 확인을 선택합니다.
8. 요청을 선택합니다.
   자세한 설치 지침이 포함된 이메일을 받게 됩니다.
9. 다음으로 이동 모두 〉 시스템 애플리케이션 〉 애플리케이션 〉 모두.
10. 응용 프로그램을 찾아서 선택하고 설치를 선택합니다.
    애플리케이션이 인스턴스에 자동으로 설치됩니다.

다음에 수행할 작업
초기 설치 후 수정 사항은 를 선택적 NVD 통합 수정 및 활동참조하십시오.

NIST 국가 취약성 데이터베이스–API(매핑되지 않은 **CPE)** 활성화

가져온 CVE(Common Vulnerabilities and Exposures) 데이터에 대해 CPE(Common Platform Enumeration) 데이터를 수집하려면 요청 시 예약된 작업을 사용하여 전체 데이터 임포트를 수행할 수 있습니다.

시작하기 전에
NIST(National Institute of Standards and Technology) NVD(National Vulnerability Database Integration)–API(Unmapped CPE) 통합은 정규 이름 형식, 시스템에 대해 이름을 검사하는 방법, 텍스트 및 테스트를 이름에 바인딩하기 위한 설명 형식을 포함하는 CPE(CPE) 데이터를 캡처합니다. 이 정보는 NVD 취약성 항목 레코드 관련 목록에 저장됩니다.

필요한 역할: sn_vul.vulnerability_admin 또는 App-Sec 관리자

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 **Vulnerability Response** 또는 **Application Vulnerability Response** 〉 **NVD** 〉 통합.
2. NIST 국가 취약성 데이터베이스 통합-API(매핑되지 않은 CPE) 통합을 선택합니다.
3. 활성 확인란을 선택합니다.

   주:
   통합은 요청 시 실행되도록 미리 구성되어 있습니다. 통합을 활성화하면 NIST NVD 통합-API(CVE만 해당) 통합 후 자동으로 실행됩니다. 다른 통합 매개변수를 변경하려면 AND 취약성 대응 및 전문 지식이 모두 ServiceNow 필요하며 불완전한 데이터가 생성될 수 있습니다.

   a. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 통합.
   b. NIST 국가 취약성 데이터베이스 통합–API(매핑되지 않은 CPE) 통합을 선택합니다.
   c. 통합 세부 정보 탭을 선택합니다.
   임포트 이후 필드의 값에 관계없이 검색된 모든 CVE에 대한 CPE가 검색됩니다.
4. 지금 실행을 선택하여 초기 전체 지원 통합 실행을 수행합니다.
   초기 임포트가 완료되면 델타 데이터의 예약된 임포트가 재개됩니다. 통합 실행 상태에 대해서는 다음 문서를 참조하십시오 (국가 취약성 데이터베이스) NVD 통합 임포트 실행 상태 보기.

NIST 국가 취약성 데이터베이스–**API** 활성화(CPE만 해당)

CPE(Common Platform Enumeration) 데이터를 수집하려면 일일 예약 작업으로 전체 데이터 임포트를 수행할 수 있습니다.

시작하기 전에
NIST(National Institute of Standards and Technology) NVD(National Vulnerability Database Integration)–API(CPE만 해당) 통합은 정규 이름 형식, 시스템에 대해 이름을 검사하는 방법, 텍스트 및 테스트를 이름에 바인딩하기 위한 설명 형식을 포함하는 CPE(CPE) 데이터를 캡처합니다. 이 정보는 취약한 소프트웨어 테이블에 저장됩니다.

필요한 역할: sn_vul.vulnerability_admin 또는 App-Sec 관리자

프로시저

1. 다음으로 이동 모두 〉 **Vulnerability Response** 또는 **Application Vulnerability Response** 〉 **NVD** 〉 통합.
2. NIST 국가 취약성 데이터베이스 통합-API(CPE 전용) 통합을 선택합니다.
3. 활성 확인란을 선택합니다.

   - 통합은 매일 실행되도록 미리 구성되어 있습니다. 다른 통합 매개변수를 변경하려면 전문 지식이 모두 ServiceNow 필요하며 불완전한 데이터가 발생할 수 있습니다.
   - 이 통합을 활성화하면 NIST 국가 취약성 데이터베이스 통합 API(CVE만) 및 NIST 국가 취약성 데이터베이스 통합 API(매핑되지 않은 CPE) 통합이 자동으로 활성화되고 실행 필드가 요청 시로 설정됩니다.
   - 또한 NIST 국가 취약성 데이터베이스 통합 API(CPE 전용)의 성공적인 통합 실행은 NIST 국가 취약성 데이터베이스 통합 API(CVE만)를 자동으로 트리거합니다. 그리고 NIST 국가 취약성 데이터베이스 통합 API(CVE만)가 성공적으로 완료되면 NIST 국가 취약성 데이터베이스 통합 API(매핑되지 않은 CPE)가 자동으로 트리거됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
NIST 국가 취약성 데이터베이스 통합 API(CPE 전용) 통합의 임포트 날짜 이후 필드는 기본적으로 비어 있습니다. 지난 357일 동안의 데이터를 가져오려면 이 항목을 비워 둡니다.

NVD 스캔에서 초기 임포트 중에 기록 데이터를 검색하려면 NIST 국가 취약성 데이터베이스 통합 API(CPE 전용) 통합 기록에서 시작 날짜를 설정합니다.

a. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 통합.

b. NIST 국가 취약성 데이터베이스 통합–API(CPE 전용) 통합을 선택합니다.

c. 통합 세부 정보 탭을 선택합니다.

d. 다음 이후 임포트 필드의 값을 검색하려는 가장 빠른 날짜로 설정합니다.
임포트에 성공할 때마다 이 날짜는 선택한 날짜와 시간으로 재설정됩니다.

4. 지금 실행을 선택하여 초기 전체 지원 통합 실행을 수행합니다.
초기 임포트가 완료되면 델타 데이터의 예약된 임포트가 재개됩니다. 통합 실행 상태에 대해서는 다음 문서를 참조하십시오 (국가 취약성 데이터베이스) NVD 통합 임포트 실행 상태 보기.

선택적 **NVD** 통합 수정 및 활동

NVD 통합을 위해 특별히 선택적 수정 사항을 구성합니다.

주:
여기에 나열된 설정 이외의 다른 NVD 통합 설정을 변경하려면 고급 ServiceNow 전문 취약성 대응 지식이 필요하며 이는 제품 설명서의 범위를 벗어납니다.

수동 **NVD** 통합 임포트 수행

초기 임포트에 실패했거나 예약된 초기 임포트를 기다리지 않으려는 경우 매일 또는 매주 예약된 작업과 관계없이 전체 데이터 임포트를 수행할 수 있습니다.

시작하기 전에

주:
NIST 국가 취약성 데이터베이스 통합 API(CPE 전용) 및 NIST 국가 취약성 데이터베이스 통합 API(매핑되지 않은 CPE) 통합은 기본적으로 비활성 상태입니다. 자세한 내용은 AND NIST 국가 취약성 데이터베이스–API(매핑되지 않은 CPE) 활성화 문서를 참조하십시오NIST 국가 취약성 데이터베이스–API 활성화(CPE만 해당).

필요한 역할: sn_vul.vulnerability_admin

프로시저

1. 다음으로 이동 모두 〉 **Vulnerability Response** 또는 **Application Vulnerability Response** 〉 관리 〉 통합.

2. 통합(예: NIST 국가 취약성 데이터베이스 통합 API(CVE만 해당) 통합)을 선택하고 통합합니다.

3. 지금 실행을 선택합니다.

주:
NIST 국가 취약성 데이터베이스 통합-API(매핑되지 않은 CPE) 통합이 활성화되면 관련 CPE 데이터가 NVD 취약성 항목의 취약한 소프트웨어 관련 목록에 저장됩니다. 취약성 대응 취약성 양식 필드 문서를 참조하십시오.

4. 통합 실행 상태는 문서를 참조하십시오 (국가 취약성 데이터베이스) NVD 통합 임포트 실행 상태 보기.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

(국가 취약성 데이터베이스) **NVD** 통합 임포트 실행 상태 보기

취약성 통합 실행 관련 목록을 사용하여 통합 실행의 성공을 확인하고, 문제를 찾고, 정정 결정을 알립니다.

시작하기 전에
NVD 통합 임포트 실행 상태를 보려면 다음을 수행합니다.

- 취약성 대응 및 NVD 통합 애플리케이션과 취약성 대응 통합을 설치하고 구성해야 합니다.
- NVD 통합 임포트가 실행 중이어야 합니다. NIST 국가 취약성 데이터베이스 통합-API(CVE만) 통합이 기본적으로 실행됩니다.

> **주:**
> NIST 국가 취약성 데이터베이스 통합-API(CPE 전용) 및 NIST 국가 취약성 데이터베이스 통합-API(매핑되지 않은 CPE) 통합은 기본적으로 비활성 상태입니다. 자세한 내용은 AND NIST 국가 취약성 데이터베이스-API(매핑되지 않은 CPE) 활성화 문서를 참조하십시오NIST 국가 취약성 데이터베이스-API 활성화(CPE만 해당).

필요한 역할: sn_vul.vulnerability_admin 또는 App-Sec 관리자

이 태스크 정보
통합 실행 중에 여러 프로세스가 생성되고 데이터가 페이지 형식으로 수신됩니다. 각 프로세스에는 페이지에 첨부된 데이터가 있는 하나 이상의 임포트 큐 항목이 포함될 수 있습니다. 이러한 항목은 1시간의 시간 제한 내에 데이터를 처리해야 합니다. 그러나 페이로드 크기가 크면 처리 시간이 1시간을 초과하거나 중단되어 통합 시간 제한 오류가 발생할 수 있습니다. 통합은 시간 초과 오류에도 불구하고 데이터를 계속 처리합니다.

이러한 잘못된 통신을 피하기 위해 버전 18.2.4 취약성 대응부터 큐가 활성 상태이고 데이터를 처리하는지 여부를 나타내기 위해 타임스탬프(하트비트)가 주기적으로 전송됩니다. 임포트 큐 항목 페이지의 처리된 마지막 기록 필드는 임포트 큐가 생성하거나 업데이트하는 기록 수에 따라 업데이트됩니다. 임포트 큐 항목이 1시간의 시간 제한을 초과하는 경우, 시스템은 처리된 마지막 기록 필드를 검사하여 1시간보다 오래되었는지도 확인합니다. 마지막으로 처리된 기록이 1시간보다 오래되었다는 것은 임포트 큐 항목이 고착되었음을 나타내며, 처리 시 더 이상의 지연을 방지하기 위해 시간이 초과되었습니다.

> **주:**
> 마지막으로 처리된 기록 필드는 다음 시스템 속성에 정의된 내용에 따라 업데이트됩니다.
>
> - *sn_sec_cmn.record_threshold_heartbeat*: 하트비트(타임스탬프)가 임포트 큐 항목으로 전송된 후 처리된 기록 수를 정의합니다.
> - *sn_sec_cmn.maximum_heartbeat_delay*: 임포트 큐 항목을 시간 초과해야 하는 시간을 정의합니다.

프로시저

1. NVD 통합 실행 상태 차트를 다음으로 이동합니다. 모두 〉 **Vulnerability Response** 또는 **Application Vulnerability Response** 〉 관리 〉 통합.
2. 통합에 대한 링크를 선택합니다.
3. 취약성 통합 실행 관련 목록을 선택합니다.
4. 모든 임포트가 성공했는지 확인합니다.

Trouble?

실행 실패의 가장 일반적인 원인은 다음과 같습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 네트워크 중단.
- 데이터 전송 문제로 인해 변환 중에 데이터가 손상되었습니다.

이러한 조건이 발생하면 지금 실행을 선택하고 통합을 다시 실행합니다.

관련 정보

취약성 대응 취약성 양식 필드

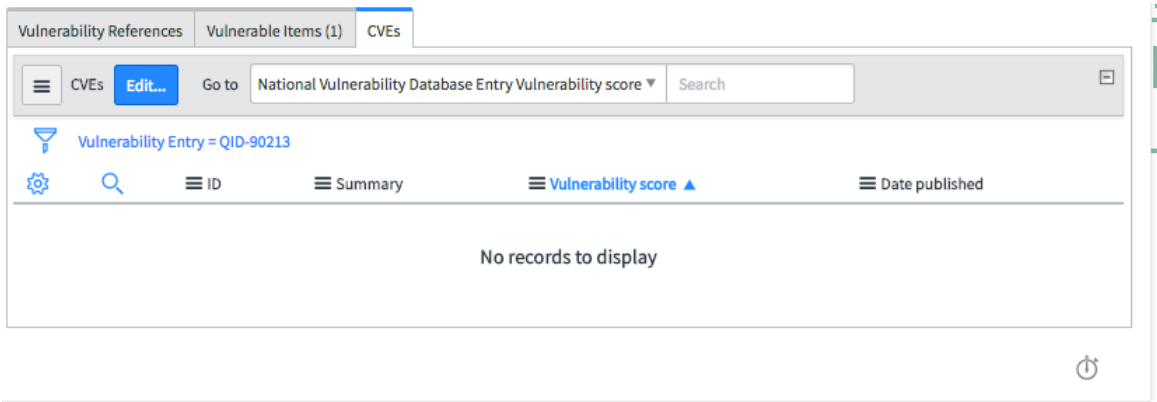
외부 공급업체 항목에 **CVE** 추가

CVE(일반적인 취약성 및 노출) 정보는 단일 타사 취약성과 관련될 수 있습니다. 일반적으로 외부 공급업체 통합 임포트 중에 추가되지만 수동으로 여러 CVE(취약성)를 추가할 수 있습니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)
가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 라이브러리 〉 외부 공급업체.
2. 기록을 엽니다.
3. **CVE** 관련 목록 탭을 클릭합니다.



4. 편집을 클릭합니다.
5. 추가할 CVE를 선택합니다.

> 주:
> 조건 필터를 사용하여 CVE 컬렉션을 세분화할 수 있습니다.

6. 저장을 클릭합니다.

관련 정보

취약성 대응 취약성 양식 필드

취약성 라이브러리 보기 취약성 대응

NVD(국가 취약성 데이터베이스), CWE(일반적인 약점 열거) 또는 타사에서 임포트한 취약성 데이터를 보고 정정 작업을 에스컬레이션할지 여부를 결정할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_vul.remediation_owner

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 라이브러리.

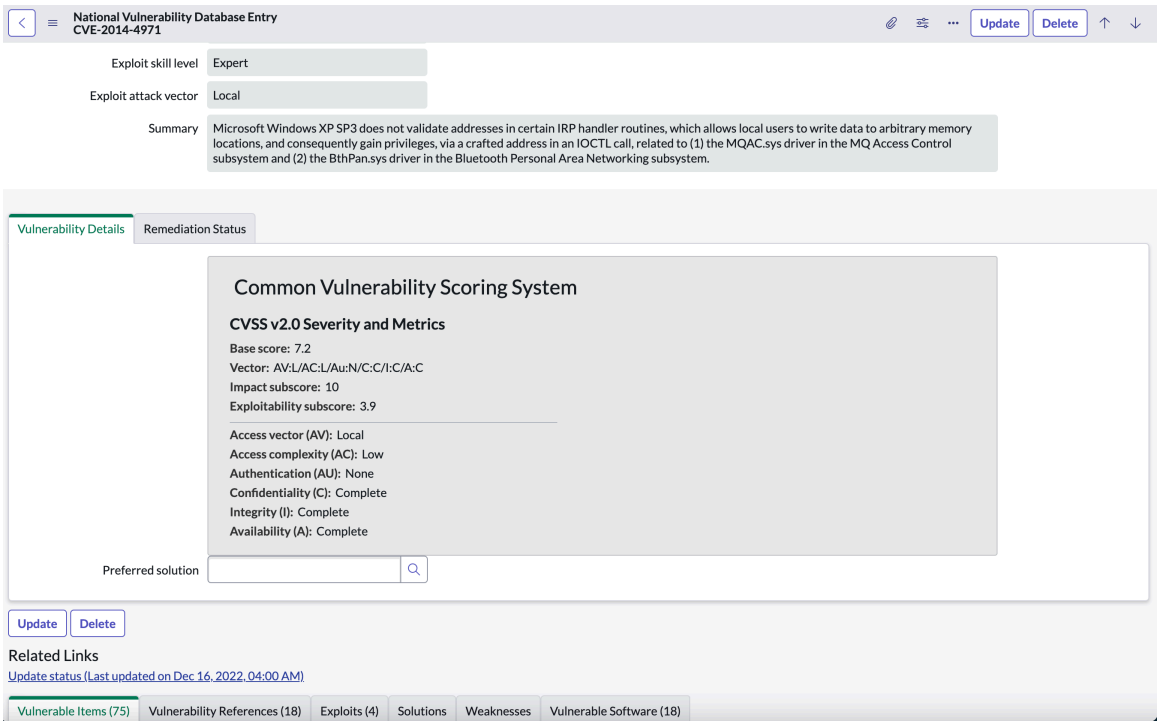
   특정 필드에 대한 자세한 내용은 다음 문서를 참조하십시오 취약성 대응 취약성 양식 필드.

   다음 라이브러리를 사용할 수 있습니다.

라이브러리	설명
NVD	NVD에서 발견한 취약성 목록으로, 보안 검사 목록, 보안 관련 소프트웨어 결함, 잘못된 구성, 제품 이름 및 익스플로잇을 포함한 영향 메트릭이 포함됩니다.
CWE	커뮤니티에서 개발한 소프트웨어 약점 유형 목록입니다. 각 CWE 기록에는 약점을 설명하는 관련 지식 문서도 포함되어 있습니다. 일반 약점 열거 화면에서 취약성을 에스컬레이션할 수 없으며 참조용으로만 사용해야 합니다.
외부 공급업체	인스턴스에 임포트한 외부 공급업체 취약성의 목록입니다. 관련 참조, 취약한 항목, 익스플로잇 및 CVE 목록을 포함합니다.

2. 취약성을 확인할 라이브러리를 선택합니다.
3. 목록의 링크를 클릭하여 기록을 엽니다.

   National Vulnerabilities Database Entries 라이브러리의 CVE 기록. 자세한 내용은 관련 링크에서 확인할 수 있습니다. 데이터를 임포트한 후에는 취약성을 선택하여 취약한 항목, 익스플로잇, 가능한 솔루션, 잠재적 패치 및 HI 지식베이스의 KB 문서 참조와의 관계를 탐색할 수 있습니다. 가 설치된 경우 취약성 솔루션 관리 NVD 기록에서 기본 솔루션을 볼 수 있습니다 (사용 가능한 경우).



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

CISA Known Exploit Vulnerability(KEV) 통합

취약성 대응 CISA KEV(Known Exploited Vulnerabilities) 카탈로그와의 통합은 데이터를 수집하여 이러한 취약성의 우선순위를 효과적으로 지정하고 정정하는 데 도움이 됩니다.

스토어에서 앱 요청

ServiceNow Store 웹 사이트를 방문하면 사용 가능한 모든 앱을 확인하고 스토어에 요청을 제출하는 방법에 대한 정보를 참조할 수 있습니다. 출시된 모든 앱의 누적 릴리스 정보는 ServiceNow Store 버전 기록 릴리스 정보를 참조하십시오.

CISA를 사용하면 정부 기관 및 기업이 적극적으로 악용되는 취약성을 긴급하고 우선적으로 해결할 수 있습니다.

CISA 소개

CISA(Cybersecurity & Infrastructure Security Agency)는 가장 많이 악용된 취약성에 대한 보고서를 게시하는 미국 사이버 보안 및 인프라 보안 기관입니다. 일반적인 취약성과 노출(CVE) 취약성을 매핑하기 취약성 대응 위해 쉽게 통합되어 인스턴스의 데이터를 보강합니다. 그런 다음 이 정보는 타사 취약성 항목 테이블로 롤업됩니다. 취약한 항목에 대한 롤업에는 가장 빠른 기한이 고려됩니다.

주:
CISA에서 검색한 CVE에 대한 **CISA** 존재 확인란입니다.

CISA 통합에서 검색되는 값:

- CVE ID
- 기한
- 추가된 날짜
- 벤더/프로젝트
- 제품
- 알려진 랜섬웨어(v21.0 of 취약성 대응부터 랜섬웨어 캠페인에 사용되는 것으로 알려진 새 필드가 CISA KEV(Known Exploited Vulnerabilities) 카탈로그에서 수집됩니다. 국가 취약성 항목 데이터베이스 테이블에서 알려진 랜섬웨어 필드에 플래그가 지정되어 표시됩니다. 플래그는 CVE(Common Vulnerabilities and Exposures) 수준에서 설정되고 TPE(외부 공급업체 항목)로 롤업됩니다.

각 통합 기록에 대해 구성된 실행 사용자가 있습니다. 이 사용자의 기본값은 VR입니다. 시스템. 이 값은 변경하지 마십시오.

예약된 작업

CISA 통합은 매일 예약된 작업으로 자동 호출됩니다. 예약된 개별 작업을 수동으로 실행할 수도 있습니다. 예약된 작업은 인스턴스를 다른 취약성 관리 시스템과 동기화된 상태로 유지하여 취약성 정정 수명주기를 단순화합니다.

사용 가능한 버전

릴리스 버전	릴리스 정보
취약성 대응 v16.5, v18.0	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

릴리스 버전	릴리스 정보
취약성 대응 CISA v1.0, v1.2와 통합	

CISA 통합 보기

CISA 통합을 보려면 다음으로 이동합니다. 취약성 대응 〉 관리 〉 통합 〉 **CISA** 알려진 익스플로잇 취약성 통합.

기본 시스템에는 다음과 같은 통합이 포함됩니다.

주:
기본적으로 CISA 통합만 활성화됩니다.

CISA 통합

통합	설명
사이버 보안 및 인프라 보안국(CISA) 통합	CISA 취약성 데이터(CVE)를 검색하고 기존 취약성 데이터를 보강합니다. 이 통합은 매일 실행하도록 자동으로 설정됩니다.

외부 공급업체 취약성의 데이터를 보려면 을 참조하십시오 취약성 라이브러리 보기 취약성 대응.

CISA 통합 준비

성공적인 통합을 위해서는 통합 전 작업을 계획하고 신중하게 실행해야 합니다. 다음 작업을 수행하여 통합을 준비합니다. CISA Known Exploited Vulnerability 통합에서는 사용자가 CISA(사이버 보안 및 인프라 보안국)에 대해 잘 알고 있다고 가정합니다.

필요한 역할: sn_vul.vulnerability_admin

각 통합 기록에 대해 구성된 실행 사용자가 있습니다. 이 사용자의 기본값은 VR입니다. 시스템. 이 값은 변경하지 마십시오.

주:
CISA 통합을 실행하기 전에 요구 사항에 따라 필요한 구성을 변경합니다.

통합 실행 중에 여러 프로세스가 생성되고 데이터가 페이지 형식으로 수신됩니다. 각 프로세스에는 페이지에 첨부된 데이터가 있는 하나 이상의 임포트 큐 항목이 포함될 수 있습니다. 이러한 항목은 1시간의 시간 제한 내에 데이터를 처리해야 합니다. 그러나 페이로드 크기가 크면 처리 시간이 1시간을 초과하거나 중단되어 통합 시간 제한 오류가 발생할 수 있습니다. 통합은 시간 초과 오류에도 불구하고 데이터를 계속 처리합니다. 이러한 잘못된 통신을 피하기 위해 버전 18.2.4 취약성 대응부터 큐가 활성 상태이고 데이터를 처리하는지 여부를 나타내기 위해 타임스탬프(하트비트)가 주기적으로 전송됩니다. 임포트 큐 항목 페이지의 처리된 마지막 기록 필드는 임포트 큐가 생성하거나 업데이트하는 기록 수에 따라 업데이트됩니다. 임포트 큐 항목이 1시간의 시간 제한을 초과하는 경우, 시스템은 마지막으로 처리된 기록 필드를 검사하여 1시간보다 오래되었는지도 확인합니다. 이 경우 이는 임포트 큐 항목이 고착되었음을 나타내며 처리 시 더 이상의 지연을 방지하기 위해 시간 초과됩니다.

주:
마지막으로 처리된 기록 필드는 다음 시스템 속성에 정의된 내용에 따라 업데이트됩니다.

- *sn_sec_cmn.record_threshold_heartbeat*: 하트비트(타임스탬프)가 임포트 큐 항목으로 전송된 후 처리된 기록 수를 정의합니다.
- *sn_sec_cmn.maximum_heartbeat_delay*: 임포트 큐 항목을 시간 초과해야 하는 시간을 정의합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

ServiceNow® CISA와 취약성 대응 통합 애플리케이션 설치

인스턴스에서 통합을 실행하기 전에 CISA(Cybersecurity & Infrastructure Security Agency) Known Exploited Vulnerability Advisor가 와 통합 취약성 대응되도록 설치 및 구성 단계를 완료해야 합니다. 이 애플리케이션은 별도의 구독으로 사용할 수 있습니다.

시작하기 전에

설치하기 전에 다음 설정 검사 목록을 완료합니다. 이러한 설정 작업은 원활한 설치 및 구성을 위해 필요합니다.

주:
이 프로세스는 프로덕션 인스턴스에 다운로드된 애플리케이션에만 적용됩니다. 애플리케이션을 비프로덕션 또는 개발 인스턴스에 다운로드하는 경우에는 권리를 얻을 필요가 없습니다. 로 애플리케이션 활성화 ServiceNow Store계속 진행합니다.

작업 설정	설명
애플리케이션이 설치되고 활성화되었는지 취약성 대응 확인합니다.	이 애플리케이션이 활성화되었는지 확인하려면 다음으로 이동하십시오. 구독 관리 〉 구독 인스턴스에 있습니다. 목록에 조직이 구매한 구독이 표시됩니다. 애플리케이션이 설치 및 활성화되지 않은 경우 을 참조하십시오 취약성 대응 설치.
취약성 대응 NVD와 통합 애플리케이션이 설치되고 활성화되었는지 확인합니다.	이 애플리케이션이 활성화되었는지 확인하려면 다음으로 이동하십시오. 구독 관리 〉 구독 인스턴스에 있습니다. 목록에 조직이 구매한 구독이 표시됩니다. 애플리케이션이 설치 및 활성화되지 않은 경우 을 참조하십시오 취약성 대응 NIST 국가 취약성 데이터베이스와의 통합 설치.
인스턴스에 필요한 ServiceNow 역할이 있는지 확인합니다.	예상 결과의 설치, 구성 및 검증에 필요한 역할은 다음과 같습니다. • 아직 할당되지 않은 경우 시스템 관리자〔admin〕가 애플리케이션을 설치하고 의 취약성 관리자에게 취약성 대응사용자를 할당합니다. 의 취약성 대응 그룹 역할에 대한 자세한 내용은 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응. • 취약성 관리자는 구성을 감독하고 예상 결과를 검증합니다.

필요한 역할: 관리자

프로시저

1. 설치 Vulnerability Response Integration with CISA 하려는 인스턴스에 로그인합니다.
2. ServiceNow Store로 이동합니다.
3. 에서 ServiceNow Store애플리케이션을 검색합니다 Vulnerability Response Integration with CISA .
4. 애플리케이션 타일을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설치 중인 애플리케이션에 대한 자세한 정보가 표시됩니다.

주:
해당하는 경우 다른 요구 사항 및 종속성 섹션을 읽어보십시오.

5. 요청 앱을 선택하고 로그인 자격 증명을 입력합니다Now Support.
6. 가져오기를 선택합니다.
7. 인스턴스의 인스턴스 이름과이유를 입력하고 인스턴스 확인을 선택합니다.
8. 요청을 선택합니다.
   자세한 설치 지침이 포함된 이메일을 받게 됩니다.
9. 다음으로 이동 시스템 애플리케이션 〉 애플리케이션.
10. 응용 프로그램을 찾아 선택한 다음 설치를 선택합니다.
    애플리케이션이 인스턴스에 자동으로 설치됩니다.

다음에 수행할 작업

주:
통합에 CISA 구성이 필요하지 않습니다.

익스플로잇 예측 점수 매기기 시스템**(EPSS)** 통합 이해

와 EPSS 통합 취약성 대응의 개요입니다.

스토어에서 앱 요청

ServiceNow Store 웹 사이트를 방문하면 사용 가능한 모든 앱을 확인하고 스토어에 요청을 제출하는 방법에 대한 정보를 참조할 수 있습니다. 출시된 모든 앱의 누적 릴리스 정보는 ServiceNow Store 버전 기록 릴리스 정보를 참조하십시오.

통합 개요

EPSS(익스플로잇 예측 점수 매기기 시스템) 통합은 First.org 에서 CVE(일반적인 취약성 및 노출)와 관련된 EPSS 데이터를 임포트하여 취약성의 우선순위를 지정하고 정정합니다. 자세한 내용은 https://www.first.org 문서를 참조하십시오. 익스플로잇 예측 점수 매기기 시스템(EPSS)은 소프트웨어 취약성이 외부에서 악용될 가능성(확률)을 추정하기 위한 데이터 기반 노력입니다. EPSS 모델은 0에서 1(0에서 100%) 사이의 확률 점수를 생성합니다. 점수가 높을수록 취약성이 악용될 가능성이 커집니다.

EPSS 통합에서 데이터를 임포트하면 인스턴스의 NVD 데이터가 더욱 보강됩니다. NVD 기록이 없으면 CVE 테이블에 자리 표시자를 생성하고 동일한 테이블에 EPSS 상세 정보를 추가합니다. 외부 공급업체 스캐너 제품을 사용하여 취약성 데이터를 인스턴스로 임포트하기 전에 초기 설정 취약성 대응 의 일부로 이 통합을 실행합니다.

중요사항:
각 통합 기록에 대해 구성된 실행 사용자가 있습니다. 이 사용자의 기본값은 VR입니다. 체계. 이 값은 변경하지 마십시오.

EPSS 통합을 통한 데이터의 초기 임포트

1. First.org EPSS 통합을 사용하여 EPSS 데이터의 초기 임포트를 수행합니다. 자세한 내용은 EPSS 데이터로 CVE 기록을 업데이트하도록 예약된 작업을 구성 및 실행합니다. 문서를 참조하십시오.

   중요사항:
   EPSS 업데이트는 기본적으로 통합 기록에서 매일 수행하며, 예약된 작업으로 실행하려면 EPSS 업데이트를 구성해야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

2. 타사 라이브러리는 예약된 작업으로 업데이트됩니다. 자세한 내용은 NVD 및 CWE 통합을 통해 데이터를 임포트하고 외부 공급업체 라이브러리를 관리합니다 문서를 참조하십시오.

> **중요사항:**
> EPSS 전에 NIST 국가 취약성 데이터베이스 통합 API(CVE만 해당) 통합을 수행하는 것이 좋습니다.

외부 공급업체 제품과 함께 취약성 데이터를 임포트하기 전에 EPSS 임포트를 수행합니다. 타사 라이브러리는 예약된 작업으로 업데이트됩니다. 외부 공급업체 통합에 대한 자세한 내용은 취약성 대응 통합에서 통합 설명서를 참조하십시오.

> **중요사항:**
> 기본 시스템에는 다음과 같은 통합이 포함되어 있습니다. 통합은 기본적으로 활성화되어 있습니다.

초기 실행 후 기본 시스템 예약된 작업은 통합을 순서대로 자동으로 실행합니다. 예약된 개별 작업을 수동으로 실행할 수도 있습니다. 예약된 작업은 인스턴스를 다른 취약성 관리 시스템과 동기화된 상태로 유지하여 취약성 정정 수명주기를 단순화합니다.

EPSS 통합이 활성화되면 EPSS 점수, EPSS 백분위수 및 EPSS 마지막으로 수정된 필드가 취약성 항목 테이블에 추가됩니다. 기존 CVE의 경우 이러한 필드는 초기 임포트 작업이 성공적으로 완료되면 자동으로 업데이트됩니다. EPSS 예약된 작업이 완료된 후 취약성 항목 테이블에 추가된 새 CVE가 있는 경우 새로 추가된 CVE는 소스를 EPSS로 표시합니다. 점수는 기본 시스템을 `Rollup EPSS score from NVD to TPEs calculator`사용하여 NVD 테이블의 CVE에서 기존 TPE로 롤업됩니다. 계산기를 수정할 수도 있습니다. 자세한 내용은 취약성 대응 롤업 계산기 문서를 참조하십시오.

관련 정보

계산기 생성 취약성 대응

EPSS 데이터로 **CVE** 기록을 업데이트하도록 예약된 작업을 구성 및 실행합니다.

기본 시스템 예약된 작업을 사용자 지정하여 CVE 기록을 EPSS 데이터로 업데이트합니다.

시작하기 전에

> **중요사항:**
> EPSS 통합을 사용하려면 (com.snc.vulnerability.cisa) 플러그인을 다운로드하고 활성화해야 Vulnerability Response Integration with CISA 합니다.

다음은 EPSS 데이터를 저장하기 위해 NVD 테이블에 추가된 새 필드 목록입니다.

- EPSS 점수
- EPSS 백분위수
- EPSS 마지막으로 수정됨

> **주:**
> 새로 추가된 필드를 보기 위한 요구 사항에 따라 목록 뷰 또는 양식 뷰를 구성합니다.

필요한 역할: 관리자

이 태스크 정보

EPSS 통합에서 데이터를 임포트하면 인스턴스의 NVD 데이터가 더욱 보강됩니다. NVD 기록이 없으면 CVE 테이블에 자리 표시자를 생성하고 동일한 테이블에 EPSS 상세 정보를 추가합니다. 취약성 대응 초기 설정의 일부로 이 통합을 실행하고 취약성 데이터를 인스턴스로 임포트하는 과정에 게시합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
기본적으로 First.org EPSS 통합은 활성 상태입니다. 기본 시스템의 예정된 작업은 기본적으로 매일 실행되도록 구성됩니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 통합.
2. First.org EPSS 통합을 찾아 선택합니다.
3. 필요한 경우 필드를 수정합니다.
4. 헤더를 마우스 오른쪽 버튼으로 클릭하여 변경 내용을 저장합니다 .
5. 지금 실행을 선택하여 예약된 작업을 즉시 실행합니다.
   취약성 통합 뷰로 돌아갑니다.
6. 선택 **First.org EPSS** 〉 취약성 통합 실행 탭 임포트 진행률을 보려면 다음을 수행합니다.
   예약된 작업이 성공적으로 완료되면 EPSS 점수, 백분위수 및 마지막으로 수정된 EPSS 점수 타임스탬프가 CVE에서 업데이트됩니다.

다음에 수행할 작업

- 위험 계산기에 EPSS 점수 조건 추가 비즈니스 규칙 문서를 참조하십시오.
- 임포트한 항목을 보려면 을 참조하십시오 취약성 라이브러리 보기 취약성 대응 .

위험 계산기에 **EPSS** 점수 조건 추가 비즈니스 규칙

비즈니스 규칙을 수정하여 EPSS 점수 조건을 위험 계산기에 추가합니다.

시작하기 전에

주:
취약성에 대한 EPSS 업데이트를 취약한 항목으로 롤다운하려면 다음 절차가 필요합니다.

필요한 역할: sn_vul.manage_risk_score_configuration

프로시저

1. 다음으로 이동 모두 〉 시스템 정의 〉 비즈니스 규칙.
2. 다시 계산 플래그 설정을 검색합니다.

   주:
   두 가지 *Set recalculate flag* 비즈니스 규칙이 있습니다. 둘 중 하나를 사용할 수 있습니다.

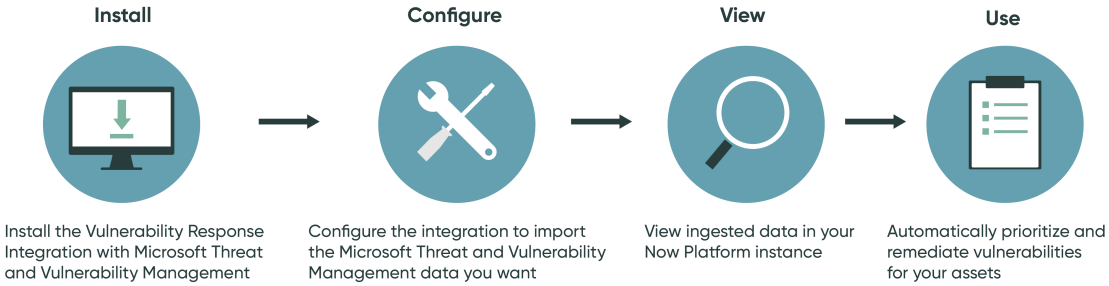
3. 실행 시기 탭으로 이동합니다.
4. **"OR"** 절 추가를 선택하고 필드 선택에서 EPSS ### 선택하고 연산자 필드 선택에서 #####.
5. 업데이트를 선택합니다.

Microsoft Threat and Vulnerability Management 취약성 통합 이해

Microsoft Threat and Vulnerability Management(MS TVM) 애플리케이션과의 통합은 취약성 대응 MS TVM에서 임포트한 데이터를 사용하여 자산의 취약성 우선순위를 지정하고 정정하는 데 도움을 줍니다. 이 애플리케이션은 .ServiceNow Store

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

MS TVM 취약성 통합을 사용하여 자산 및 취약성에 대한 외부 공급업체 스캐너 데이터를 임포트할 수 있습니다. 그런 다음 대시보드에서 취약성 및 취약한 항목에 대한 보고서를 볼 수 있습니다 취약성 대응 .



사용 가능한 버전

릴리스 버전	릴리스 정보
취약성 대응 MS TVM v2.2와 통합	취약성 대응 애플리케이션의 릴리스 버전, 호환성 및 스키마 변경 사항에 대한 자세한 내용은 HI 지식베이스에서 취약성 대응 호환성 매트릭스 및 릴리스 스키마 변경 〔KB0856498〕 문서를 참조하십시오.

도메인 분리 및 **MS TVM**

통합을 실행할 사용자를 해당 도메인에 할당하여 취약성 통합 데이터를 지정된 도메인에 임포트합니다. MS TVM 취약성 통합에 대해 도메인 분리 임포트를 생성하려면 문서를 참조하십시오 통합을 위해 도메인 분리 임포트 작성.

통합의 용어 및 주요 기능

취약한 항목 및 취약성

취약한 항목은 다음과 같은 경우에 인스턴스에 ServiceNow AI Platform 생성됩니다.

- 외부 공급업체 스캐너에서 임포트한 취약성이 의 CMDB기존 자산(구성 항목)과 일치합니다. MS TVM 제품에서는 이러한 일치 항목을 취약성이라고 합니다.
- 외부 공급업체 스캐너에서 임포트한 취약성이 의 CMDB기존 자산과 일치하지 않습니다. 이 경우 일치하지 않는 CI(구성 항목)도 취약한 항목과 함께 생성됩니다.

  기존 CI를 호스트와 일치시킬 수 없는 경우 IRE(식별 및 조정 엔진)를 사용하여 두 개의 새 클래스에서 CI를 생성합니다. 그렇지 않으면 일치하지 않는 CI 클래스에 일치하지 않는 CI가 생성됩니다. 자세한 내용은 식별 및 조정 엔진을 사용하기 위한 취약성 대응 CI 생성 문서를 참조하십시오.

타사 취약성 항목

타사 취약성 항목은 MS TVM과 같은 외부 공급업체 스캐너에서 임포트되며 인스턴스의 ServiceNow AI Platform 외부 공급업체 취약성 항목 테이블에 나열됩니다. 또한 CVE(국가 취약성 데이터베이스) 항목은 MS TVM에서 임포트됩니다. 이 두 가지 유형의 항목과 연관된 악용 정보는 MS TVM에서 제공됩니다. 이 악용 정보는 위험 계산에 사용할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

> **주:**
> 타사 취약성은 CVE가 할당되지 않은 취약성에 대해서만 검색됩니다. MS TVM은 취약성에 대한 임시 이름(예: TVM-XXXX-XXXX)을 추가할 수 있습니다. 이 이름은 CVE ID가 할당된 후 업데이트됩니다.

CI(구성 항목)

CI는 에 나열된 CMDB기존 자산입니다.

검색된 항목

검색된 항목은 의 기존 CI와 CMDB일치하는 MS TVM 머신 임포트에서 수집된 자산입니다.

일치하는 항목이 없으면 의 CMDB일치하지 않는 CI 클래스에 CI가 작성됩니다. CMDB CI Class Models 플러그인을 활성화하면 IRE(식별 및 조정 엔진)에서 새 클래스를 사용하여 CI를 만듭니다. 자세한 내용은 식별 및 조정 엔진을 사용하기 위한 취약성 대응 CI 생성 문서를 참조하십시오. 일치하지 않는 원래 CI가 재분류되면 검색된 항목 기록이 해당 상태를 반영하도록 업데이트됩니다. 검색된 항목을 통해 자산을 식별하고 의 CI에 매핑하는 방법을 볼 수 있습니다 CMDB.

CI 조회 규칙

MS TVM에서 데이터를 가져오면 는 취약성 대응 자동으로 시스템(자산) 데이터를 CMDB사용하여 . CI 조회 규칙은 CI를 식별하고 VI가 생성될 때 VI 기록에 추가하는 데 사용됩니다.

인스턴스

인스턴스는 MS TVM의 여러 계정을 참조합니다. 각 계정은 MS TVM 애플리케이션의 인스턴스가 될 수 있습니다.

통합

통합은 MS TVM 머신의 통합과 같은 외부 공급업체 소스에서 정보를 검색하는 예약된 작업입니다.

배포

통합이 다중 소스를 지원하는 경우, 단일 통합 존재를 통합의 배포라고 합니다. 배포는 환경 전반의 통합 및 제품을 의미합니다. 예를 들어, 사용자 환경에 MS TVM이 여러 개 배포되어 있을 수 있습니다.

MS TVM 통합에는 다음과 같은 주요 기능도 포함됩니다.

- 환경 전체에서 자산을 식별하고 기존 검색된 항목, 취약한 항목 및 탐지 레코드의 CI를 업데이트하여 취약성에 대한 자세한 정보를 제공할 수 있습니다.
- 모든 MS TVM 통합에 대해 작업을 실행할 시기를 예약할 수 있습니다. 요청 시 예약된 작업을 실행할 수도 있습니다.
- 취약한 항목을 그룹화할 수 있습니다.
- CI 조회 규칙을 구성하여 외부 공급업체 소스의 자산 데이터를 사용하여 사용자의 CI를 식별하는 방법을 정의할 수 있습니다 CMDB.

필요한 **ServiceNow AI Platform** 역할

통합 작업에는 인스턴스에서 다음 역할이 ServiceNow AI Platform 필요합니다.

가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관리자

시스템 관리자는 설정 도우미를 사용하여 MS TVM 애플리케이션을 설치합니다. 할당되지 않은 경우 관리자는 취약성 관리자(sn_vul.vulnerability_admin) 및 설정 도우미의 다른 역할을 할당합니다.

sn_vul.vulnerability_admin

할당된 취약성 관리자는 설정 도우미에서 MS TVM 통합 구성을 완료합니다. 이 역할은 애플리케이션 및 해당 기록에 취약성 대응 대한 전체 액세스 권한을 갖습니다. 취약성 관리자는 설치된 외부 공급업체 통합에 대한 모든 취약성 대응 애플리케이션과 규칙을 구성합니다.

sn_vul_msft_tvm.configure_integration

이 역할에는 sn_vul_msft_tvm.read_integration 세분화된 역할이 포함됩니다. 이 역할을 수행하는 사용자는 Microsoft Threat and Vulnerability Management 애플리케이션과의 취약성 대응 통합을 구성할 수 있습니다.

sn_vul_msft_tvm.read_integration

이 역할을 가진 사용자는 Microsoft Threat and Vulnerability Management 애플리케이션 레코드와의 취약성 대응 통합을 볼 수만 있습니다.

취약성 대응 그룹

기본적으로 취약성 대응 그룹은 설정 도우미에서 사용할 수 있습니다. 취약성 대응 그룹에 할당된 사용자는 sn_vul.read_all 및 sn_vul.remediation_owner 역할을 자동으로 상속합니다.

MS TVM 통합

모든 MS TVM 통합에 대해 다중 소스가 지원됩니다. 의 취약성 대응설정 도우미에서 환경 전체에 다음 통합의 여러 인스턴스를 추가하고 배포할 수 있습니다. 또한 설정 도우미에서 MS TVM 애플리케이션과의 통합을 설치하고 구성합니다 취약성 대응 .

MS TVM 통합을 보려면 다음으로 이동합니다. **Microsoft TVM** 취약성 통합 〉 관리 〉 통합. 취약성 대응 는 MS TVM 엔드포인트와의 통합을 제공하여 예약된 시간 간격에 따라 데이터를 임포트합니다. 기본 시스템에는 다음과 같은 통합이 포함됩니다.

MS TVM 통합

실행 시퀀스	일정	통합	설명
1	매일	Microsoft TVM 권장 사항 통합	취약성을 정정하기 위해 실행 가능한 모든 보안 권장 사항의 목록을 검색합니다.
2	매일	Microsoft TVM 취약성(CVE) 통합	국가 취약성 데이터베이스 항목 및 타사 취약성 항목의 목록과 해당 악용 정보를 검색합니다.
3	매일	Microsoft TVM 머신 통합	Microsoft TVM에서 머신 태그를

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

MS TVM 통합

실행 시퀀스	일정	통합	설명
			포함한 모든 자산(컴퓨터) 데이터를 검색하고 인스턴스에서 처리합니다.
4	주별 주: 설치 후 이 통합은 컴퓨터를 임포트한 후 자동으로 실행됩니다.	Microsoft TVM 머신 취약성 통합(전체 임포트)	모든 자산에서 미해결 취약성을 모두 검색합니다.
5	매일	Microsoft TVM 머신 취약성 통합(델타 임포트)	새로운 취약성, 수정된 취약성 및 업데이트된 취약성을 포함하여 조직의 전체 취약성 임포트에서 변경된 모든 정보를 검색합니다.

취약한 항목은 설정한 그룹 규칙에 따라 정정 작업으로 그룹화되고 할당 규칙에 따라 정정을 위해 할당됩니다. 자세한 내용은 취약성 대응 정정 작업 및 정정 작업 규칙 개요 및 취약성 대응 할당 규칙 개요 문서를 참조하십시오.

CI 조회 규칙

MS TVM에서 데이터를 가져오면 는 취약성 대응 자동으로 시스템(자산) 데이터를 구성 관리 데이터베이스(CMDB)사용하여 . CI 조회 규칙은 CI를 식별하고 VI가 생성될 때 VI 기록에 추가하는 데 사용됩니다. CI 조회 규칙의 작동 방식에 대한 자세한 내용은 다음 문서를 참조하십시오 외부 공급업체 취약성 통합에서 취약성 대응 구성 항목을 식별하기 위한 CI 조회 규칙.

주:
규칙을 제거하면 복구할 수 없습니다. 기존 규칙을 제거하는 대신 사용하지 않도록 설정해야 합니다.

다음 MS TVM 조회 규칙이 기본 시스템과 함께 제공됩니다.

- MAC_ADDRESS
- FQDN
- IP

주:
자산의 IP_ADDRESS 및 MAC_ADDRESS에 대해 여러 값을 사용할 수 있습니다. CI 조회 규칙은 일치하는 모든 값을 고려합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

검색된 항목

MS TVM 머신 통합에서 임포트하는 동안 탐지된 CI를 볼 수 있습니다.

> **주:**
> 이 목록의 기본 필터는 #### ##으로 설정됩니다. 필터를 제거하여 임포트에서 검색된 모든 항목을 볼 수 있습니다.

자세한 내용은 검색된 항목 문서를 참조하십시오.

머신 태그

호스트 태그라고도 하는 머신 태그는 조직의 자산을 구성하고 추적하는 데 사용됩니다. 머신에 태그를 할당합니다.

모든 머신 태그는 MS TVM 머신 통합의 일부로 임포트됩니다. 머신 태그는 일반적으로 할당 규칙 및 정정 작업 규칙의 취약성 대응 필터링에 사용됩니다. 검색된 항목 양식에 태그가 표시됩니다.

> **주:**
> 애플리케이션에서 할당 또는 정정 작업 규칙을 취약성 대응 생성하기 취약성 대응 전에 MS TVM 머신 통합을 실행하여 취약한 항목을 임포트 및 그룹화하기 전에 이러한 규칙에 모든 태그를 사용할 수 있도록 합니다. 태그에 대한 다음 사항도 참고하십시오.
>
> - 태그 스토리지는 대/소문자를 구분하지 않습니다. Paris 태그가 생성되면 PARIS 태그를 머신 태그 테이블에 저장할 수 없습니다. Paris 와 PARIS 는 시스템에서 동일한 머신 태그로 간주됩니다. 어떤 태그가 먼저 임포트되든 저장되고 인식되는 태그입니다.
> - 정정 작업 규칙에서 머신 태그를 그룹 키로 사용하면 예기치 않은 결과가 발생할 수 있습니다. 그룹 키는 정정 작업 테이블의 열인 반면 머신 태그는 조건 작성기에서만 사용할 수 있습니다.
> - 머신 태그는 전역 시스템 속성 sn_vul.import_host_tags에 의해 제어됩니다. 이 속성은 기본적으로 true 로 설정됩니다. 태그를 비활성화하면 모든 ServiceNow AI Platform# 인스턴스에서 비활성화됩니다.

다음에 할 일

에서 ServiceNow# StoreMicrosoft Threat and Vulnerability Management와의 통합을 다운로드한 취약성 대응 후 의 설치 도우미취약성 대응에서 설치 및 구성이 지원됩니다. 자세한 내용은 설정 도우미를 사용하여 MS TVM 애플리케이션과의 취약성 대응 통합 설치 및 구성 문서를 참조하십시오.

Microsoft Threat and Vulnerability Management 취약성 통합 준비

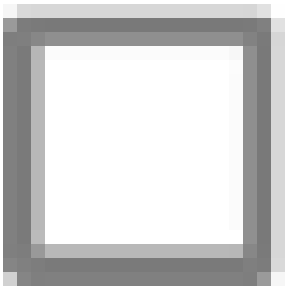
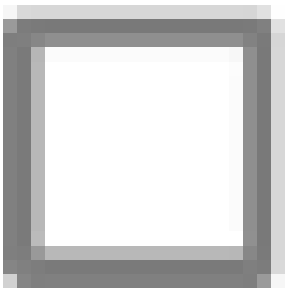
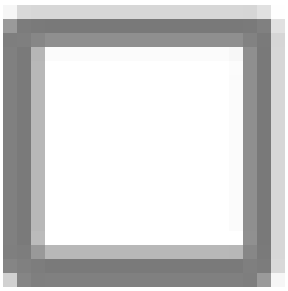
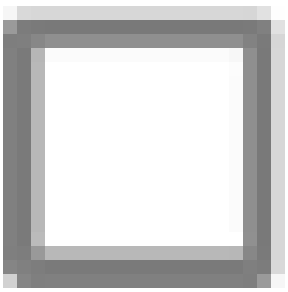
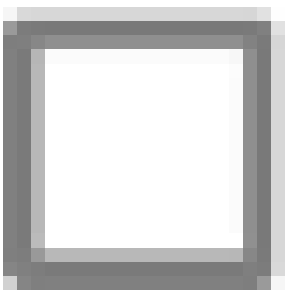
설정 작업을 수행하여 MS TVM(Microsoft Threat and Vulnerability Management) 취약성 통합을 준비할 ServiceNow# 수 있습니다.

검사 목록 사용을 시작하기 전에

MS TVM 애플리케이션과의 통합을 설치하고 구성 취약성 대응 하려면, 애플리케이션을 설치하고 취약성 데이터를 인스턴스로 임포트하기 전에 다음 검사 목록을 인쇄하고 나열된 항목이 완료되었는지 확인할 수 있습니다 ServiceNow AI Platform# .

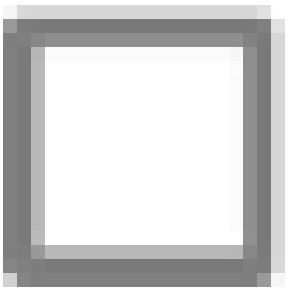
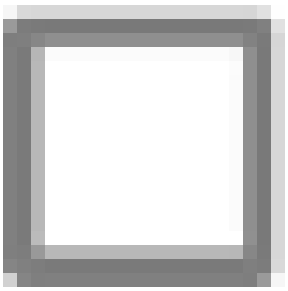
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

통합 준비 검사 목록

작업	설명
	다음 정보 집합 중 하나가 있는지 확인합니다. • MS TVM 계정의 ClientSecret, ClientId 및 TenantId • MS TVM 계정의 사용자 이름, 암호, ClientId 및 TenantId입니다. 이 정보를 얻으려면 다음 문서를 참조하십시오 Microsoft MS TVM 통합을 위한 Azure 설정.
	아직 설치 및 활성화되지 않은 경우 타사 애플리케이션을 설치하기 전에 애플리케이션을 설치합니다 취약성 대응 . 애플리케이션 설치 및 활성화에 취약성 대응 대한 자세한 내용은 다음 문서를 참조하십시오 취약성 대응 설치. 이 통합에는 버전 14.0 취약성 대응 이상이 필요합니다.
	인스턴스에 애플리케이션이 아직 없는 경우 권리를 얻고 MS TVM과의 통합 애플리케이션을 ServiceNow AI Platform# 인스턴스에 다운로드합니다취약성 대응. 문서를 참조하십시오.
	임포트할 것으로 예상되는 취약한 항목의 수를 예상합니다. 임포트하려는 취약한 항목 수를 인스턴스가 수락할 수 있는지 확인합니다. 인스턴스 크기가 작으면 로드 시간이 길어질 수 있습니다. 인스턴스 크기를 모르거나 도움이 필요한 경우 기술 지원에 문의하십시오 ServiceNow# .
	통합을 관리하고 취약한 항목을 정정할 다음 그룹 또는 사용자가 있는지 확인합니다. 관리자 설정 도우미를 사용하여 MS TVM 애플리케이션과의 취약성 대응 통합을 설치합니다. 할당되지 않은 경우 관리자는 취약성 관리자(sn_vul.vulnerability_admin) 및 설정 도우미의 다른 역할을 할당합니다. sn_vul.vulnerability_admin MS TVM 통합 구성을 완료합니다. 이 역할은 (VR) 애플리케이션 및 해당 기록에 대한 취약성 대응 전체 액세스 권한을 보유합니다. 이 관리자는 모든 VR 애플리케이션 및 규칙을 구성하고 외부 공급업체 통합을 구성합니다. sn_vul_msft_tvm.configure_integration

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

통합 준비 검사 목록

작업	설명
	MS TVM 취약성 통합을 구성합니다. 이 역할에는 sn_vul_msft_tvm.read_integration 세분화된 역할이 포함됩니다. sn_vul_msft_tvm.read_integration MS TVM 취약성 통합의 기록을 봅니다(읽기). 취약성 대응 그룹 기본적으로 취약성 대응 그룹은 설정 도우미에서 사용할 수 있습니다. 취약성 대응 그룹에 할당된 사용자는 sn_vul.read_all 및 sn_vul.remediation_owner 역할을 자동으로 상속합니다. 아직 생성하지 않은 경우 설정 도우미를 사용하기 전에 추가 그룹을 생성하고 인스턴스에서 사용자 관리 모듈을 사용하여 사용자를 추가하는 것이 좋습니다. 자세한 내용은 사용자 그룹 만들기를 참조하세요. 가상 사용자와 세분화된 역할을 사용하여 애플리케이션에서 사용자가 수행하고 볼 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할을 처음 할당하려면 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당.
	취약성 대응 NVD와의 통합을 설치하고 NIST 국가 취약성 데이터베이스 통합 API(CVE만 해당)를 실행합니다.
	첫 번째 임포트의 성능을 향상시키려면 인스턴스에서 특정 기능, 규칙 또는 작업을 비활성화하면 됩니다. • 취약성 계산기를 사용하지 않는 경우 비활성화합니다. 이러한 계산기와 사용자가 정의한 계산기는 취약한 항목 레코드가 생성되거나 업데이트될 때마다 실행됩니다. 자세한 내용은 사용하지 않는 경우 기본 취약성 계산기 사용 안 함을 참조하세요. • 기록을 처음 임포트하는 동안 특정 알림 관련 비즈니스 규칙으로 인해 많은 알림이 생성되어 수집 성능에 영향을 줄 수 있습니다.

준비가 되었습니다 설정 도우미를 사용하여 MS TVM 애플리케이션과의 취약성 대응 통합 설치 및 구성.

Microsoft MS TVM 통합을 위한 **Azure** 설정

Azure Portal에서 Microsoft 계정을 설정하여 MS TVM(Microsoft Threat and Vulnerability Management) API에 원격으로 액세스합니다. MS TVM 테넌트에 액세스하여 시스템, 취약성 및 보안 권장 사항에 대한 정보를 수집하려면 이 계정이 필요합니다.

시작하기 전에
필요한 역할: Microsoft Azure Portal 관리자.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보
이 통합을 위해 애플리케이션을 설치하기 ServiceNow# 전에 Azure Portal에서 Microsoft 다음 설정 작업을 완료합니다.

최신 콘텐츠에 액세스할 수 있는지 확인하려면 Microsoft 문서 웹 사이트를 참조하세요. Azure Portal에서 OAuth 2.0 인증을 위한 애플리케이션 ID를 Microsoft 만들지 않은 경우 이 절차의 단계를 따릅니다.

프로시저

1. Azure Portal 관리자 자격 증명을 사용하여 Azure Portal에 Microsoft 로그인합니다.
2. 홈 창의 왼쪽 탐색 패널에서 **Azure Active Directory**를 클릭합니다.
3. 개요 창에서 **App Registrations (Preview)**(앱 등록(미리 보기))을 클릭합니다.
4. App registrations (Preview)(앱 등록(미리 보기)) 창에서 **New** Registration(새 등록)을 클릭합니다.
   애플리케이션 등록 양식이 표시됩니다.
5. 양식에서 필드를 채웁니다.

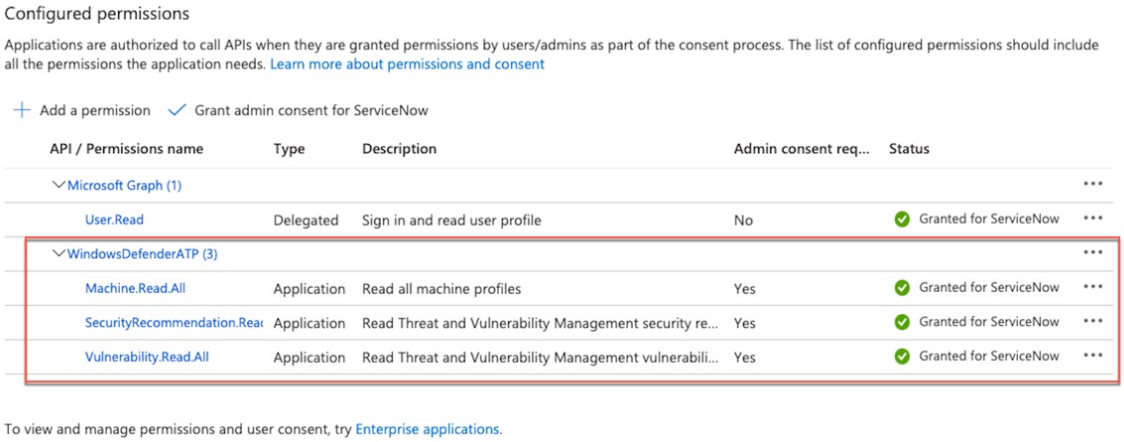
애플리케이션 등록 양식

필드	설명
이름	애플리케이션의 이름입니다. 이 예에서는 ServiceNow MS TVM ## 이 입력됩니다.
지원되는 계정 유형	이 계정의 경우 지원되는 계정 유형에서 이 조직 디렉터리의 계정만**(ServiceNow** 전용 **-** 단일 테넌트)을 클릭합니다.
리디렉션 URL(선택 사항)	이 필드에 대한 값을 입력하면 통합에서 사용되지 않습니다.

6. 등록을 클릭합니다.
   애플리케이션(클라이언트) ID 및 디렉터리(테넌트) ID가 생성됩니다. VR-TVM 통합 설정 도우미의 구성 단계 ServiceNow 중에 클라이언트 **ID** 및 테넌트 **ID** 필드의 구성 페이지에 다음 값을 입력합니다. 이 단계는 에 설명되어 있습니다 설정 도우미를 사용하여 MS TVM 애플리케이션과의 취약성 대응 통합 설치 및 구성.
7. MS TVM 통합 창에 애플리케이션(클라이언트) ID가 표시되면 ServiceNow**API** 권한 보기를 클릭합니다.
8. 다음으로 이동 **API** 권한 요청 〉 내 조직에서 사용하는 **API**을 클릭한 다음 **Windows Defender** ATP를 클릭합니다.
9. ServiceNow MS TVM 통합 - API 권한 창에서 권한 추가를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

10. 머신, 취약성 및 보안 권장 사항에 대한 읽기 권한을



제공합니다.

11. 〈조직 이름〉에 대한 관리자 동의 부여를 클릭합니다.

주:
인스턴스에서 애플리케이션 ServiceNow 으로 인증하려면 다음 작업을 수행합니다.

a. 다음으로 이동 **ServiceNow MS TVM** 통합 〉 인증서 및 비밀을 클릭한 다음 새 클라이언트 암호를 클릭합니다.

b. 양식에서 필드를 채웁니다.

클라이언트 비밀 양식

필드	설명
설명	애플리케이션의 이름입니다.
만료	만료 날짜입니다.

c. 추가를 클릭합니다.

값 필드는 새 클라이언트 암호인 새 클라이언트 암호로 채워집니다.

주:
인스턴스에서 통합을 ServiceNow AI Platform 구성할 때 이 암호가 필요합니다.
자세한 내용은 설정 도우미를 사용하여 MS TVM 애플리케이션과의 취약성 대응 통합 설치 및 구성 문서를 참조하십시오.

d. 이 암호를 안전한 위치에 저장합니다. 이 페이지에서 나가면 이 암호를 사용할 수 없습니다.

Azure Portal에서 인증을 위한 애플리케이션 ID를 Microsoft 성공적으로 만들었습니다.

다음에 수행할 작업
통합을 위한 인스턴스를 설정할 ServiceNow AI Platform# 준비가 되었습니다.

설정 도우미를 사용하여 **MS TVM** 애플리케이션과의 취약성 대응 통합 설치 및 구성

MS TVM에서 임포트한 데이터를 사용하여 자산의 취약성 우선순위를 지정하고 정정할 수 있도록 MS TVM(Microsoft 위협 및 취약성 관리) 애플리케이션과의 통합을 설치하고 구성합니다 취약성 대응 .

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에

Microsoft Threat and Vulnerability Management 취약성 통합을 실행하기 ServiceNow# 전에 애플리케이션에서 Microsoft Threat and Vulnerability Management 애플리케이션과 ServiceNow Store 취약성 대응 통합을 다운로드하고 애플리케이션에서 설정 도우미 취약성 대응 를 사용하여 설치하고 구성해야 합니다.

MS TVM 애플리케이션을 설치하기 전에 체크리스트의 Microsoft Threat and Vulnerability Management 취약성 통합 준비 모든 항목을 완료했는지 확인하십시오. Azure 계정 설정에 Microsoft 대한 자세한 내용은 다음 문서를 참조하십시오 Microsoft MS TVM 통합을 위한 Azure 설정.

필요한 역할:

- admin sn_vul.vulnerability_admin 역할의 초기 할당과 설정 도우미에서 Microsoft Threat and Vulnerability Management 애플리케이션 설치를 위한 관리자
- 취약성 관리자(sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음))는 애플리케이션을 설치한 후 설정 도우미에서 애플리케이션을 구성할 수 있습니다.

이 태스크 정보

MS TVM 통합을 설치 및 구성하기 전에 다음 절차를 수행합니다.

주:
이 프로세스는 프로덕션 인스턴스에 다운로드된 애플리케이션에만 적용됩니다. 애플리케이션을 비프로덕션 또는 개발 인스턴스에 다운로드하는 경우에는 권리를 얻을 필요가 없습니다. 로 애플리케이션 활성화 ServiceNow Store계속 진행합니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 설정 도우미 〉 통합 애플리케이션 설치.

   잠시 후 인스턴스에 설치할 수 있는 애플리케이션이 표시됩니다.

2. **Microsoft Threat and Vulnerability Management** 타일을 찾아 설치를 클릭합니다.

   취약성 대응 에서 ServiceNow Store 다운로드한 Integration with Microsoft Threat and Vulnerability Management 애플리케이션이 설치됩니다.

3. 설치 도우미의 지시에 따라 설치를 계속합니다.
   설치 도우미를 사용하여 응용 프로그램을 설치하는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 설정 도우미를 사용하여 타사 응용 프로그램 설치 취약성 대응.

다음에 수행할 작업

설치 도우미에서 설치를 완료한 후 통합 구성 〉 스캐너 통합 설정 도우미에서 구성을 계속합니다. 설정 도우미에서 제공되는 프롬프트를 보완하기 위한 자세한 내용은 문서를 참조하십시오 설정 도우미를 사용하여 MS TVM 취약성 통합 구성.

Microsoft Threat and Vulnerability Management 통합에 대한 데이터 검색 설정

데이터 검색 설정을 사용하여 MS TVM(Microsoft Threat and Vulnerability Management) 취약성 통합에서 ServiceNow# 인스턴스로 임포트할 데이터의 유형과 범위를 결정할 수 있습니다 ServiceNow AI Platform# .

데이터 검색 설정은 임포트하려는 데이터를 제어하는 데 도움이 됩니다. 통합 인스턴스에서 이러한 필터의 값을 설정할 수 있습니다. 통합 인스턴스를 보려면 다음으로 이동합니다. **Microsoft Threat and Vulnerability Management** 취약성 통합 〉 통합 인스턴스 을 클릭하고 MS TVM 통합을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

통합 인스턴스 페이지에서 통합 인스턴스 매개변수를 클릭하여 매개변수 목록을 표시하거나 일정, REST 상세 정보, 통합 상세 정보, 데이터 소스 및 통합 실행 정보를 보려면 취약성 통합 탭을 클릭합니다.

인스턴스의 **MS TVM** 통합 **ServiceNow AI Platform** 에 대한 데이터 검색 설정 및 필터

인스턴스의 MS TVM 통합에 다음 설정을 사용할 수 있습니다 ServiceNow AI Platform . 이러한 구성 설정 및 기타 구성 설정은 인스턴스의 ServiceNow AI Platform 통합 인스턴스 페이지에 표시됩니다. 처음 몇 번의 통합 실행에 대해서는 이러한 설정을 기본 설정으로 두는 것을 선호할 수 있습니다.

미스 TVM.

vi_size_limit

MS TVM 머신 취약성 통합의 결과 집합에 포함할 취약한 항목 기록 수를 정의합니다. 이 설정은 int32 형식이어야 합니다. 기본값은 2,000입니다.

vulnerabilities_size_limit

MS TVM 취약성(CVE) 통합의 결과 집합에 포함할 취약성 기록 수를 정의합니다. 이 설정은 int32 형식이어야 합니다. 기본값은 2,000입니다.

recommendations_size_limit

MS TVM 권장 사항 통합의 결과 세트에 포함할 취약성 기록 수를 정의합니다. 이 설정은 int32 형식이어야 합니다. 기본값은 2,000입니다.

asset_size_limit

MS TVM 머신 통합의 결과 세트에 포함할 취약성 기록 수를 정의합니다. 이 설정은 int32 형식이어야 합니다. 기본값은 2,000입니다.

machine_filter

MS TVM에서 오는 시스템을 필터링합니다. 이 필터는 MS TVM 머신 통합에 적용됩니다. 기본값은 onBoardingStatus가 onBoarded인 컴퓨터를 가져오는 것입니다.

Microsoft Threat and Vulnerability Management 취약성 통합에 대한 **REST** 메시지

MS TVM(Microsoft Threat and Vulnerability Management) 취약성 통합에 ServiceNow# 대한 REST 메시지를 사용하여 MS TVM API를 호출할 수 있습니다.

MS TVM 액세스 토큰

REST API 요청을 인증할 수 있도록 MS TVM 액세스 토큰에 대한 REST 메시지를 사용하여 MS TVM API에서 액세스 토큰을 검색할 수도 있습니다. REST 메시지의 기록 방법에 대한 변경은 MS TVM에 대한 인증 요청에 영향을 미칩니다.

MS TVM 통합

MS TVM 통합에 REST 메시지를 사용하여 MS TVM에서 정보를 검색할 수 있습니다. REST 메시지의 기록 방법을 변경하면 정보를 검색하기 위해 MS TVM에 대한 요청에 영향을 미칩니다. REST 메시지에는 다음과 같은 REST 메서드가 포함됩니다.

REST 메서드

REST 메서드	방법 설명
취약성 가져오기	MS TVM에서 취약성 및 악용 정보를 검색합니다.
머신별 소프트웨어 취약성 가져오기	열려 있는 모든 취약성을 검색합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

REST 메서드

REST 메서드	방법 설명
권장 사항 가져오기	조직에 영향을 주는 실행 가능한 모든 보안 권장 사항의 목록을 검색합니다.
GET 머신	자산의 컬렉션을 검색합니다.
머신별 소프트웨어 취약성 변경 내용 가져오기	새 취약성, 수정된 취약성 및 업데이트된 취약성을 포함하여 조직의 전체 취약성 임포트에서 변경된 모든 정보를 검색합니다.

Microsoft Threat and Vulnerability Management 취약성 통합에 대한 데이터 변환

임포트할 데이터를 식별한 후에는 MS TVM(Microsoft Threat and Vulnerability Management) 애플리케이션에서 데이터를 검색하고 ServiceNow# 데이터 소스 세트를 통해 처리한 다음 인스턴스에서 변환합니다.

설치하는 동안 정규화된 심각도 맵이 정규화된 심각도 매핑 모듈에 설치됩니다. 이러한 맵은 임포트한 Microsoft 외부 공급업체 취약성 심각도 수준을 인스턴스에서 처리할 표준 심각도 수준으로 변환합니다. 심각도 맵 생성에 대한 자세한 내용은 다음 문서를 참조하십시오 취약성 대응 심각도 맵 생성.

MS TVM 머신 임포트

임포트한 머신의 데이터는 먼저 MS TVM 머신 임포트 [sn_vul_msft_tvm_machines_import] 테이블에 로드됩니다.

MS TVM 머신 변환은 임포트한 머신 정보를 변환하는 데 사용됩니다.

주:
이 변환 맵을 변경하면 MS TVM 머신 임포트의 데이터가 처리되는 방식이 변경됩니다.

이 변환 맵에 액세스하려면 다음으로 이동하십시오. 시스템 임포트 세트 〉 변환 맵 을 클릭하고 **Microsoft TVM** 머신 변환을 검색합니다.

다음 표에는 통합별 변환 맵 필드가 나열되어 있습니다.

MS TVM 머신 변환 맵 필드

소스 필드	대상 필드	설명
u_id	source_id	자산의 고유 ID. 이 ID는 검색된 항목 기록의 source_id에 매핑됩니다.
u_ipaddresses.mac주소	mac_address	API에서 cmdb_ci 기록의 호스트 MAC 주소 필드로 매핑되는 MAC 주소입니다.
u_ipaddresses.ipAddress	ip_address	cmdb_ci 기록의 IP 주소 필드에 매핑되는 IP 주소 필드입니다.
u_lastseen	last_scan_date	검색된 항목 기록의 last_scan_date 필드에 매핑되는 필드입니다.
u_machinetags		sn_sec_cmn_host_tag에 저장된 태그입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

MS TVM 머신 변환 맵 필드

소스 필드	대상 필드	설명
		태그에서 자산으로의 매핑은 sn_sec_cmn_m2m_src_ci_tag에 저장됩니다.
u_osplatform	os	cmdb_ci 기록의 os 필드에 매핑되는 필드입니다.
u_computerdnsname	fqdn	API의 dnsname 필드를 cmdb_ci 기록의 fqdn 필드에 매핑하는 필드입니다.

변환 프로세스 중에 다음 변환 스크립트가 실행됩니다.

MS TVM 머신 변환 맵 스크립트 타이밍 및 목적

스크립트가 실행될 때	목적
onStart(임포트 세트가 변환을 시작한 경우)	통합 프로세스의 범위 변수(sn_vul_msft_tvm)의 값을 초기화하는 데 사용되는 스크립트입니다. 이 스크립트는 내부용이며 수정하거나 삭제하면 안 됩니다.
onBefore(임포트 세트가 변환을 완료하기 전)	호스트의 값을 업데이트하고 호스트가 존재하는지 여부를 확인하는 데 사용되는 스크립트입니다. 결과에 따라 이 스크립트는 범위 변수(sn_vul_msft_tvm)의 값을 수정합니다. 이 스크립트는 내부용이며 수정하거나 삭제하면 안 됩니다.
onComplete(임포트 세트가 변환을 완료한 경우)	생성, 업데이트 및 무시되는 CI 수를 설정하는 데 사용되는 스크립트입니다. 이 스크립트는 내부용이며 수정하거나 삭제하면 안 됩니다.

MicrosoftTVMMachinesProcessor 스크립트 포함은 onBefore 변환 스크립트에서 호출됩니다. Microsoft TVM 컴퓨터의 통합에서 출력을 가져와 CI로 변환합니다. 이 스크립트 포함을 변경하면 CI 및 검색된 항목 테이블에서 Microsoft TVM 컴퓨터의 데이터 변환이 변경될 수 있습니다.

MS TVM 취약성 통합

임포트된 취약성 데이터는 먼저 Microsoft TVM CVE(취약성) 임포트 [sn_vul_msft_tvm_vulnerabilities_import] 테이블에 로드됩니다.

주:
이 변환 맵을 변경하면 MS TVM 취약성 임포트의 데이터가 처리되는 방식이 변경됩니다.

이 변환 맵에 액세스하려면 다음으로 이동하십시오. 시스템 임포트 세트 〉 변환 맵 을 클릭하고 **Microsoft TVM** 취약성 변환을 검색합니다.

다음 표에는 통합별 변환 맵 필드가 나열되어 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Microsoft TVM 취약성 변환 맵 필드

소스 필드	대상 필드	설명
u_id	ID	sn_vul_entry 기록의 ID 열에 매핑합니다.
u_severity	source_severity	심각도 필드를 심각도에 매핑합니다. 기본값은 5입니다.
u_publishedon	date_published	u_publishedon 필드를 게시된 날짜에 매핑합니다.
u_publicexploit	public_exploit	스캐너에서 제공하는 u_publicexploit 취약성 항목 테이블의 공개 익스플로잇 열에 매핑합니다.
u_cvssv3	v3_base_score	cvssv3 점수를 취약성 항목 기록의 v3 기본 점수에 매핑합니다.
u_description	요약	취약성 항목 기록의 요약 필드에 설명을 매핑합니다.
u_exploitinkit	malware_kit	익스플로잇 테이블의 맬웨어 키트에 u_exploitinkit 필드를 매핑합니다.
u_exploittypes	유형	익스플로잇 유형을 익스플로잇 테이블의 유형에 매핑합니다.
u_exploitverified	is_exploit_verified	익스플로잇 테이블의 검증된 익스플로잇에 u_exploitverified 필드를 매핑합니다.
u_exploituris	exploit_links	익스플로잇 테이블의 익스플로잇 링크에 u_exploituris 필드를 매핑합니다.

변환 프로세스 중에 다음 변환 스크립트가 실행됩니다.

스크립트가 실행될 때	목적
onStart(임포트 세트가 변환을 시작한 경우)	통합 프로세스의 범위 변수(sn_vul_msft_tvm)의 값을 초기화하는 데 사용되는 스크립트입니다. 이 스크립트는 내부용이며 수정하거나 삭제하면 안 됩니다.
onBefore(임포트 세트가 변환을 완료하기 전)	NVD 또는 타사 항목 테이블에서 값을 만들거나 업데이트하는 데 사용되는 스크립트입니다. 이 스크립트는 내부용이며 수정하거나 삭제하면 안 됩니다.
onComplete(임포트 세트가 변환을 완료한 경우)	생성된 새 항목과 업데이트 후 무시된 항목의 값을 설정하는 데 사용되는 스크립트입니다. 이 스크립트는 내부용이며 수정하거나 삭제하면 안 됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

MS TVM 권장 사항 임포트

임포트한 권장 사항 데이터는 먼저 MS TVM 권장 사항 임포트 [sn_vul_msft_tvm_recom_import] 테이블에 로드됩니다.

주:
이 변환 맵을 변경하면 MS TVM 권장 사항 임포트의 데이터가 처리되는 방식이 변경됩니다.

이 변환 맵에 액세스하려면 다음으로 이동하십시오. 시스템 임포트 세트 〉 변환 맵 을 클릭하고 **MS TVM** 권장 사항 변환을 검색합니다.

다음 표에는 통합별 변환 맵 필드가 나열되어 있습니다.

MS TVM 권장 사항 변환 맵 필드

소스 필드	대상 필드	설명
u_recommendedvendor	recommended_vendor	u_recommendedvendor 필드를 벤더 열에 매핑합니다.
u_weaknesses	약점	u_weaknesses 필드를 약점 열에 매핑합니다.
u_exposedmachinescount	src_exposed_machines_cnt	u_exposedmachinescount 필드를 노출된 컴퓨터 수 열에 매핑합니다.
u_status	상태	상태를 권장 사항 기록의 상태 필드에 매핑합니다.
u_productname	product_name	u_productname 필드를 권장 사항 기록의 제품 이름에 매핑합니다.
u_nonproductiv_impactedassets	non_prod_impacted_assets	u_nonproductiv_impactedassets 필드를 권장 사항 기록의 영향을 받는 자산 열에 매핑합니다.
u_activealert	active_alert	u_activealert 필드를 권장 사항 기록의 활성 경보 열에 매핑합니다.
u_recommendedversion	recommended_version	u_recommendedversion 필드를 권장 사항 기록의 권장 버전 열에 매핑합니다.
u_totalmachinecount	total_machine_count	u_totalmachinecount 필드를 권장 사항 기록의 총 머신 수 열에 매핑합니다.
u_exposureimpact	exposure_impact	u_exposureimpact 필드를 권장 사항 기록의 노출 영향 열에 매핑합니다.
u_recommendationname	recommendation_name	u_recommendationname 필드를 권장 사항 기록의 권장 사항 이름 열에 매핑합니다.
u_subcategory	하위 범주	u_subcategory 필드를 권장 사항 기록의 하위 범주 열에 매핑합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

MS TVM 권장 사항 변환 맵 필드

소스 필드	대상 필드	설명
u_id	source_id	MS TVM의 권장 사항 ID를 소스 ID 열에 매핑합니다.
u_remediationtype	remediation_type	u_remediationtype 필드를 권장 사항 기록의 정정 유형 열에 매핑합니다.
u_relatedcomponent	related_component	u_relatedcomponent 필드를 권장 사항 기록의 관련 구성요소 열에 매핑합니다.
u_recommendedprogram	recommended_program	u_recommendedprogram 필드를 권장 사항 기록의 권장 프로그램 열에 매핑합니다.
u_recommendationcategory	recommendation_category	u_recommendationcategory 필드를 권장 사항 기록의 권장 사항 범주 열에 매핑합니다.
u_publicexploit	public_exploit	u_publicexploit 필드를 권장 사항 기록의 공개 익스플로잇 열에 매핑합니다.
u_vendor	벤더	u_vendor 필드를 권장 사항 기록의 벤더 열에 매핑합니다.
〔스크립트〕	integration_instance	권장 사항을 임포트하는 인스턴스의 이름입니다.
〔스크립트〕	sys_domain	이 기록을 임포트하는 도메인입니다.

변환 프로세스 중에 다음 변환 스크립트가 실행됩니다.

MS TVM 권장 사항 변환 맵 스크립트

스크립트가 실행될 때	목적
onStart(임포트 세트가 변환을 시작한 경우)	통합 프로세스의 범위 변수(sn_vul_msft_tvm)의 값을 초기화하는 데 사용되는 스크립트입니다. 이 스크립트는 내부용이며 수정하거나 삭제하면 안 됩니다.
onBefore(임포트 세트가 변환을 완료하기 전)	권장 사항의 값을 업데이트하고 권장 사항이 있는지 확인하는 데 사용되는 스크립트입니다. 이 스크립트는 내부용이며 수정하거나 삭제하면 안 됩니다.
onComplete(임포트 세트가 변환을 완료한 경우)	생성, 업데이트 및 무시된 항목의 값을 설정하는 데 사용되는 스크립트입니다. 이 스크립트는 내부용이며 수정하거나 삭제하면 안 됩니다.

MS TVM 머신 취약성 임포트

MS TVM 머신 취약성 변환 맵은 MS TVM에서 임포트한 미해결 및 고정 취약성 정보를 변환하는 데 사용됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
이 변환 맵을 변경하면 MS TVM 머신 취약성 임포트의 데이터가 처리되는 방식이 변경됩니다.

MS TVM 미해결 및 수정된 취약성 변환 맵에 접근하려면 다음으로 이동하십시오. 시스템 임포트 세트 〉 변환 맵 을 클릭하고 **MS TVM** 머신 취약성 변환을 검색합니다.

다음 표에는 통합별 변환 맵 필드가 나열되어 있습니다.

MS TVM 머신 취약성 변환 맵 필드

소스 필드	대상 필드	설명
u_id	detection_key	u_id 필드를 탐지 테이블의 탐지 키 열에 매핑합니다.
u_diskpaths	증명	u_diskpaths 필드를 탐지 테이블의 증명 열에 매핑합니다.
u_registrypaths	증명	u_registrypaths 필드를 탐지 테이블의 증명 열에 매핑합니다.
u_recommendedsecurityupdateid	preferred_solution	sn_vul_solution 테이블에 ID가 동일한 솔루션이 있는 경우 취약한 항목 테이블의 기본 솔루션 열에 u_recommendedsecurityupdateid 필드를 매핑합니다.
u_recommendationreference	권장 사항	u_recommendationreference 필드를 취약한 항목 테이블의 권장 사항 열에 매핑합니다.
u_cveid	취약성	u_cveid 필드를 취약한 항목 테이블의 취약성 열에 매핑합니다.
u_status	source_status	u_status 필드를 탐지 테이블의 소스 상태 열에 매핑합니다.
u_eventtimestamp	temporal_score	u_eventtimestamp 필드를 취약한 항목 테이블의 마지막으로 발견된 열에 매핑합니다.
u_lastseentimestamp	last_seen	u_lastseentimestamp 필드를 취약한 항목 테이블의 마지막으로 발견됨 열에 매핑합니다.
u_firstseentimestamp	first_seen	u_firstseentimestamp 필드를 취약한 항목 테이블의 처음 발견됨 열에 매핑합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

MS TVM 머신 취약성 변환 맵 필드

소스 필드	대상 필드	설명
u_recommendedsecurityupdate	solution_summary	u_recommendedsecurityupdate 필드를 취약한 항목 테이블의 솔루션 요약 열에 매핑합니다.
u_recommendedsecurityupdateurl	solution_summary	u_recommendedsecurityupdateurl 필드를 취약한 항목 테이블의 솔루션 요약 열에 매핑합니다.

변환 프로세스 중에 다음 변환 스크립트가 실행됩니다.

스크립트가 실행될 때	목적
onStart(임포트 세트가 변환을 시작한 경우)	통합 프로세스의 범위 변수(sn_vul_msft_tvm)의 값을 초기화하는 데 사용되는 스크립트입니다. 이 스크립트는 내부용이며 수정하거나 삭제하면 안 됩니다.
onBefore(임포트 세트가 변환을 완료하기 전)	취약성 항목 및 탐지가 있는지 확인하는 데 사용되는 스크립트입니다. 그렇지 않은 경우 이러한 기록은 해당 테이블에 생성됩니다. 이 스크립트는 내부용이며 수정하거나 삭제하면 안 됩니다.
onComplete(임포트 세트가 변환을 완료한 경우)	MS TVM에서 임포트한 VI 및 탐지 수를 업데이트하는 데 사용되는 스크립트입니다. 이 스크립트는 내부용이며 수정하거나 삭제하면 안 됩니다.

Microsoft Threat and Vulnerability Management 취약성 통합에 대한 통합 실행 상태 차트

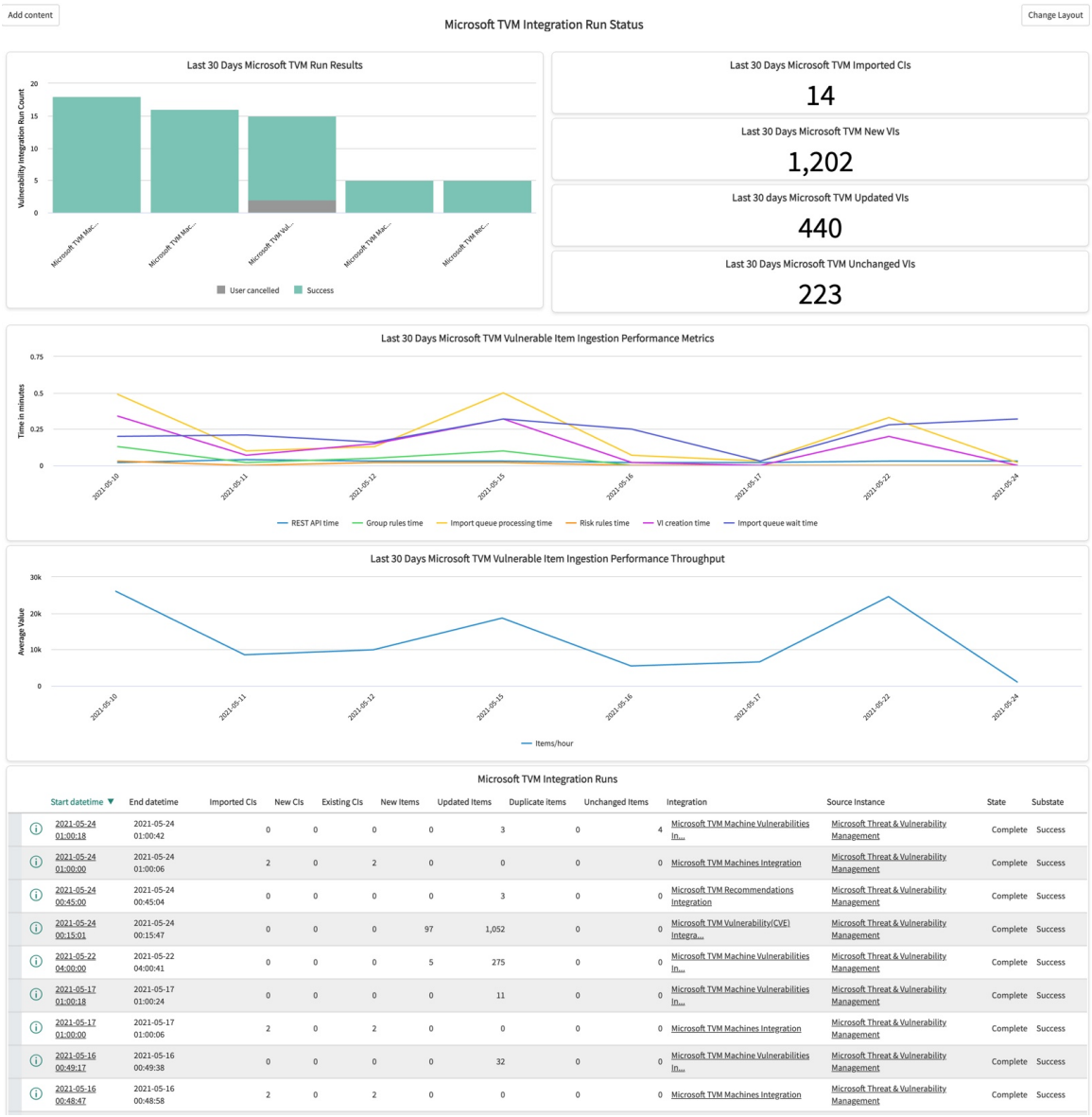
MS TVM(Microsoft Threat and Vulnerability Management) 통합 실행 상태 모듈을 사용하여 MS TVM 통합 실행 상태에 대한 그래픽 뷰를 제공할 수 있습니다.

의 취약성 대응버전 19.0부터 이 대시보드는 New Experience UI에서 사용할 수 있습니다.

주:
Tokyo에 있는 경우 Next Experience UI에서 대시보드를 볼 수 있지만 일부 기능 손실이 있습니다.

차트에서 그래프의 특정 부분을 가리켜 해당 부분과 관련된 데이터 요약을 표시할 수 있습니다. 막대 그래프에서 부품을 클릭하면 더 자세한 정보를 제공하는 목록이 열립니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



MS TVM 통합 실행 상태 차트 보고서

이름	설명
지난 30일 Microsoft TVM 결과	각 통합에 대해 완료된 통합 실행 수입니다. 이 보고서에는 성공한 실행과 실패한 실행이 모두 표시됩니다. 각 실행은 그래프에 막대로 표시됩니다.
지난 30일 Microsoft TVM 신규 VI	지난 30일 동안 임포트된 새로운 취약한 항목 수입니다.
지난 30일 Microsoft TVM 업데이트된 VI	지난 30일 동안 임포트된 업데이트된 취약한 항목 수입니다.
지난 30일 Microsoft TVM 변경 안 된 VI	지난 30일 동안 임포트된 중복 취약한 항목 수입니다.
MS TVM 통합 실행	통합 실행 기록이 목록에 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이름	설명
	주: **V16.1:** 이 통합에 대한 탐지를 확인하려면 탐지 또는 결과를 ServiceNow 테이블의 탐지 데이터와 *sn_vul_detection* 비교합니다. 통합이 진행되는 동안 탐지 또는 발견 개수가 변경될 수 있습니다. 이 보고서는 통합 실행이 완료된 후 인스턴스의 "종료 날짜 카운트" 열에 탐지 횟수를 표시합니다.
지난 30일 Microsoft TVM 취약한 항목 수집 성과 메트릭	지난 30일 동안과 비교하여 취약한 항목에 대한 일일 성과 메트릭입니다.
지난 30일 Microsoft TVM 취약한 항목 수집 성능 처리량	지난 30일 동안 Microsoft TVM 호스트 탐지 통합에 대해 측정된 일일 취약한 항목 수집 처리량입니다.
지난 30일 Microsoft TVM 임포트한 CI	지난 30일 동안 임포트한 새 구성 항목 수입니다.

Microsoft Threat and Vulnerability Management 통합 임포트 실행 상태 확인

Microsoft Threat and Vulnerability Management(MS TVM) 임포트 실행 상태를 사용하여 통합 실행의 성공을 확인하고 문제를 찾습니다.

시작하기 전에
이 절차에서는 다음과 같은 가정을 합니다.

- MS TVM 취약성 통합이 설치 및 구성되어 있습니다 취약성 대응 .
- MS TVM 취약성 통합 임포트가 예약되어 실행 중입니다.

필요한 역할: sn_vul.vulnerability_admin

이 태스크 정보
통합 실행 중에 여러 프로세스가 생성되고 데이터가 페이지 형식으로 수신됩니다. 각 프로세스에는 페이지에 첨부된 데이터가 있는 하나 이상의 임포트 큐 항목이 포함될 수 있습니다. 이러한 항목은 1시간의 시간 제한 내에 데이터를 처리해야 합니다. 그러나 페이로드 크기가 크면 처리 시간이 1시간을 초과하거나 중단되어 통합 시간 제한 오류가 발생할 수 있습니다. 통합은 시간 초과 오류에도 불구하고 데이터를 계속 처리합니다. 이러한 잘못된 통신을 피하기 위해 버전 18.2.4 취약성 대응부터 큐가 활성 상태이고 데이터를 처리하는지 여부를 나타내기 위해 타임스탬프(하트비트)가 주기적으로 전송됩니다. 임포트 큐 항목 페이지의 처리된 마지막 기록 필드는 임포트 큐가 생성하거나 업데이트하는 기록 수에 따라 업데이트됩니다. 임포트 큐 항목이 1시간의 시간 제한을 초과하는 경우, 시스템은 마지막으로 처리된 기록 필드를 검사하여 1시간보다 오래되었는지도 확인합니다. 이 경우 이는 임포트 큐 항목이 고착되었음을 나타내며 처리 시 더 이상의 지연을 방지하기 위해 시간 초과됩니다.

주:
마지막으로 처리된 기록 필드는 다음 시스템 속성에 정의된 내용에 따라 업데이트됩니다.

- *sn_sec_cmn.record_threshold_heartbeat*: 하트비트(타임스탬프)가 임포트 큐 항목으로 전송된 후 처리된 기록 수를 정의합니다.
- *sn_sec_cmn.maximum_heartbeat_delay*: 임포트 큐 항목을 시간 초과해야 하는 시간을 정의합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 **Microsoft** 위협 및 취약성 관리 〉 통합.
   a. 통합을 선택합니다.
   b. 취약성 통합 실행 관련 목록을 클릭합니다.
2. 임포트 상태가 완료이고 하위 상태가 성공인지 확인합니다.
   실행 실패의 가장 일반적인 원인은 다음과 같습니다.
   - 네트워크 중단.
   - 데이터 전송 시 비트 감쇠로 인해 변환 중에 데이터가 손상됩니다.
3. 옵션: 실행 실패를 초래한 이러한 조건 중 하나가 표시되면 지금 실행을 클릭하고 통합을 다시 실행합니다.

취약성 인스턴스를 기반으로 **Microsoft TVM** 탐지를 분할하여 취약 항목을 분할합니다.

ServiceNow# 취약성 대응을 사용하면 MS TVM(Microsoft Threat and Vulnerability Management) 스캐너에서 탐지 항목을 분할하여 탐지된 각 취약성 인스턴스에 대해 고유한 취약한 항목(VIT)을 생성할 수 있습니다. 이렇게 분할하면 다양한 정정 팀에 VIT를 할당하여 취약성 관리 및 추적을 강화할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
MS TVM(Microsoft Threat and Vulnerability Management) 스캐너의 페이로드에는 탐지 데이터가 포함되어 있으며, 증명 내의 각 경로는 탐지를 분할하는 데 사용됩니다. 페이로드의 diskpath 태그는 취약성의 위치를 식별하여 특정 경로에 따라 취약성을 정확하게 식별하고 관리할 수 있도록 합니다.

프로시저

1. 외부 공급업체 통합 테이블 〔sn_sec_int_integration〕에서 및 Tenable.sc에 대해 **VI** 키 열 값에 증명 Tenable.io 포함을 true로 설정합니다.
2. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 **VI** 세분성 구성.
3. 포트 포함 양식에서 포트 포함 확인란을 선택하고 여기 클릭 링크를 선택합니다.
4. VI 키에 증명 추가 목록에서 새로 만들기를 선택합니다.
5. VI 키에 증명 추가 - 새 레코드 양식의 취약성 필드에서 증명을 포함할 Microsoft Threat and Vulnerability Management(MS TVM) CVE를 추가하고 제출을 선택합니다.
   선택한 취약성이 VI 키에 증명 추가 목록에 나타납니다.

Example: MS TVM(Microsoft Threat and Vulnerability Management) 스캐너에서 탐지 분할

MS TVM(Microsoft Threat and Vulnerability Management) 스캐너의 다음 탐지는 diskpath 태그의 증거를 보여줍니다.

```
        "id": "329f3283
fae116€796ff1b59c8dd56fef4067elf_mozilla_firefox_126.0.1.0_CVE-2024-7528",
        "deviceId":"329f3283fae116e796ff1b59c8dd56fef4067e1f",
```


© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
          "rbacGroupId":
     "rbacGroupName": "Unassigned",
      "deviceName": "ip-0a1409fd.secops.com",
       "osPlatform": "WindowsServer2019",
         "oVersion": "10.0.17763.5936",
       "osArchitecture": "x64",
        "softwareVendor": "mozilla",
       "softwareName": "firefox",
       "softwareVersion": "126.0.1.0",

           "cveId"; "CVE-2024-7528",
          #vulnerabilitySeverityLevel": "High",
        #recommendedSecurityUpdate":; "mfsa2024-33",

        "recommendedSecurityUpdateId": null,

           "recommendedSecurityUpdateUrl": null,
            "diskPaths": ['c: llprogram files\lamazonllcfn-bootstraplilibcrypto-3.dll", "C: \lprogram
files\lamazon\lcfn-bootstrap\\libsst-3.dll,

         "registryPaths":
          1 "HKEY LOCAL, MACHINE\\SOFTWAREW\WOW6432Nodel
IMicrosoft|\Windows|1CurrentVersion\|Uninstalll\Mozilla Firefox 126.0.1 (x86 en-US)"


        #lastSeenTimestamp": "2024-08-28 19:36:07",

         "firstSeenTimestamp": "2024-08-06 20:32:34",

       "end0fSupportStatus": null,
          "end0fSupportDate": null,
      "exploitabilityLevel": "NoExploit",
          "recommendationReference": "va-_-mozilla-_-firefox",

         "cvssScore": 8.8,
       "securityUpdateAvailable": true,
         "cveMitigationStatus": null
```


와 **HCL BigFix** 패치 오케스트레이션의 통합 이해 취약성 대응

HCL BigFix 제품과의 패치 오케스트레이션 통합을 통해 취약성 대응 대규모 자산 그룹의 중요 취약성에 대한 패치 및 패치 배치를 관리할 수 있습니다.

다음으로 오케스트레이션 패치 취약성 대응

를 사용하여 취약성 대응 오케스트레이션을 패치하면 타사 솔루션 통합, 패치 벤더 및 취약성 스캐너에서 예약된 임포트를 사용합니다. 스캐너 탐지 데이터는 환경의 자산을 취약성 및 이를 수정할 수 있는 패치 업데이트와 일치시킵니다. 승인을 위해 패치 요청을 제출하고, 패치 업데이트를 예약하여 취약한 항목을 해결하고, 애플리케이션의 ServiceNow AI Platform#모든 기록 취약성 대응에서 정정 진행 상황을 모니터링합니다.

HCL BigFix를 사용한 취약성 대응 패치 오케스트레이션

Vulnerability Response Patch Orchestration with HCL BigFix 통합 애플리케이션을 Patch 오케스트레이션 및 취약성 대응 애플리케이션과 함께 ServiceNow# 취약성 솔루션 관리사용하는 경우 취약성 관리자와 분석가는 다음 태스크를 수행할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 패치 유형 및 벤더의 솔루션(패치)에 대한 자세한 컨텍스트와 정보를 참조하십시오.
- 작업 공간의 기록 취약성 대응 에서 취약성 및 솔루션 데이터뿐 아니라 취약성 정정 진행 상황을 보고 모니터링합니다.

IT 전문가와 정정 소유자는 다음 작업을 수행할 수 있습니다.

- 업무 상충을 피하기 위해 업무 외 시간에 정기적으로 예약된 간격으로 BigFix 제품 Windows에서 지원하는 패치, CentOS, MAC, Oracle 및 기타 자산을 배포합니다.
- 취약성이 있는 패치되지 않은 자산 또는 외부 공급업체 스캐너에서 임포트한 탐지 데이터의 예약된 패치를 통해 성공적으로 업데이트되었거나 업데이트되지 않은 자산을 식별합니다.
- 패치 업데이트, 정정 작업 및 검색된 항목 기록에서 취약하고 패치가 적용되지 않은 자산에 대해 IT 정정 작업 공간 또는 클래식 환경에서 사용 가능한 패치를 예약합니다.

및 **BigFix** 애플리케이션의 주요 용어 취약성 대응

CI(구성 항목)

CI는 에 나열된 구성 관리 데이터베이스(CMDB)기존 자산입니다. BigFix는 CI, 컴퓨터를 호출합니다.

컴퓨터 그룹

자산 그룹을 나타내는 BigFix 제품에서 사용되는 용어입니다.

취약한 항목

CMDB의 기존 자산과 일치하는 임포트한 취약성입니다.

인스턴스

BigFix 애플리케이션에 대한 고유한 계정입니다. 각 사용자 계정은 BigFix 애플리케이션의 인스턴스가 될 수 있습니다. 이 용어는 인스턴스에 대한 고유하고 안전한 웹 주소를 의미하기도 합니다 ServiceNow AI Platform .

통합

통합은 BigFix 머신과의 통합과 같은 외부 공급업체 소스에서 정보를 검색하는 예약된 작업 ServiceNow AI Platform 입니다.

솔루션

이러한 통합의 맥락에서 솔루션에는 두 가지 유형, 즉 잠재적 솔루션과 기본 솔루션이 있습니다. 잠재적 솔루션은 취약성을 해결할 수 있는 솔루션입니다. 취약성에는 종종 많은 잠재적인 솔루션이 있습니다. #기본 솔루션은 탐지된 특정 취약성에 대해 가장 효과적인 솔루션과 일치합니다.

패치

취약성을 수정하는 소프트웨어 업데이트. BigFix 애플리케이션에서 패치를 Fixlet이라고 합니다. 예를 들어, BigFix에는 , CentOS, MAC Oracle 및 기타 제품에 대한 WindowsFixlet이 있습니다.

기본 패치

기본 패치는 특정 취약점을 수정하기 위한 소프트웨어 업데이트입니다. 패치가 배포되면 특정 취약성과 관련된 취약한 항목에 매핑되어 수정합니다.

정정 작업

취약성을 수정하는 데 필요한 작업 애플리케이션의 취약한 항목 취약성 대응 목록입니다.

배포

이 통합을 위한 배포는 컴퓨터에 패치를 적용, 시작 또는 예약하는 경우를 의미합니다. BigFix는 이러한 배포를 작업이라고 합니다. BigFix에서 다운로드한 패치에 대한 배포

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

(작업 생성)를 수행할 수 있습니다 ServiceNow AI Platform. 의 취약성 대응개별 기록에서 검색된 항목, 패치 또는 정정 작업으로 이동합니다. 예약된 작업이 있는 패치를 개별 컴퓨터 또는 컴퓨터 그룹에 배포할 수 있습니다.

의 ServiceNow AI Platform 배포는 다중 소스를 지원하는 통합을 참조할 수도 있습니다. 단일 통합 존재를 통합의 배포라고 합니다. 배포는 환경 전반의 통합 및 제품을 의미합니다. 예를 들어 사용자 환경에 BigFix Vulnerability 통합이 여러 개 배치되어 있을 수 있습니다.

Vulnerability Solution Management 및 **Vulnerability Response Patch Orchestration with HCL BigFix** 통합

솔루션 관리는 애플리케이션에서 제공하며 취약성 솔루션 관리 , ServiceNow AI Platform 애플리케이션은 취약성 결과를 이를 정정하는 솔루션(패치)의 세부 항목과 연관시킵니다. 제품 및 서비스, 구성 업데이트 및 조직에 가장 큰 영향을 미치는 기타 통제에 대한 외부 공급업체의 소프트웨어 패치를 식별합니다. 외부 공급업체 스캐너 정보와 취약성 대응용 솔루션 관리함께 , 취약성 대응, 및 HCL을 사용한 취약성 대응 Patch Orchestration BigFix 애플리케이션이 함께 작동하여 솔루션에서 취약성 및 취약한 항목으로 기본 패치를 롤업하여 사용자 환경에 맞게 취약성을 수정하고 종결하는 데 도움을 줍니다.

취약성 대응용 솔루션 관리, 취약성 대응, 및 HCL BigFix 통합을 사용하는 취약성 대응 패치 오케스트레이션은 모두 ServiceNow# Store.

필요한 **ServiceNow AI Platform** 역할

통합 설치, 구성 및 정정 작업에는 인스턴스에서 다음 역할이 ServiceNow AI Platform 필요합니다.

관리자

이 역할을 가진 사용자는 에 있는 ServiceNow Store 애플리케이션에 대한 권리를 얻고 인스턴스에 다운로드합니다 ServiceNow AI Platform .

sn_vul.vulnerability_admin

이 역할이 있는 사용자는 인스턴스에서 애플리케이션을 ServiceNow AI Platform 활성화하고 애플리케이션 구성을 취약성 대응 완료합니다. 이 역할은 (VR) 애플리케이션 및 해당 기록에 대한 취약성 대응 전체 액세스 권한을 보유합니다. 이 관리자는 모든 VR 애플리케이션, 규칙 및 외부 공급업체 통합을 구성합니다.

sn_vul_bigfix.configure_integration

이 역할이 있는 사용자는 BigFix Patch 오케스트레이션 통합 애플리케이션을 구성합니다. 이 역할에는 sn_vul_bigfix.read_integration 세분화된 역할이 포함됩니다.

sn_vul_bigfix.read_integration

이 역할을 가진 사용자는 BigFix Patch 오케스트레이션 통합 애플리케이션 및 패치 오케스트레이션 데이터의 기록을 취약성 대응 보기(읽기 전용)할 수 있습니다.

sn_vul_patch_orch.configure_patch

이 역할을 가진 사용자는 패치를 구성하고 적용할 수 있습니다.

sn_vul_patch_orch.read_patch

이 역할을 가진 사용자는 패치 정보를 보거나 읽기 전용으로 사용할 수 있습니다.

승인자

배포 전에 제출된 패치 요청을 승인하려면 승인자 수준 1 및 승인자 수준 2 승인자 그룹에 용도를 할당합니다.

설정 도우미를 사용하여 이러한 역할을 할당하는 방법에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 의 역할에 대한 취약성 대응 자세한 내용은 를 참조하십시오취약성 대응 가상 사용자 및 세분화된 역할.ServiceNow AI Platform

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

CI 조회 규칙

BigFix 애플리케이션에서 취약성 대응 데이터를 임포트할 때 애플리케이션은 사용 중인 시스템(자산) 데이터에서 구성 관리 데이터베이스(CMDB) 일치하는 항목을 자동으로 검색합니다. CI 조회 규칙은 VI(자산)를 식별하고 VI가 생성될 때 VI(취약한 항목) 기록에 자동으로 추가하는 데 사용됩니다.

다음 CI 조회 규칙은 기본 시스템과 함께 제공되며 CI(자산)를 식별하고 애플리케이션에 추가하는 취약성 대응 데 사용됩니다.

- MAC_ADDRESS
- IP_ADDRESS
- DNS_NAME

자산 IP_ADDRESS에 여러 값을 사용할 수 있습니다. CI 조회 규칙은 일치하는 모든 값을 고려합니다. CI 조회 규칙의 방식과 작동 방식에 대한 자세한 내용은 다음 문서를 참조하십시오 외부 공급업체 취약성 통합에서 취약성 대응 구성 항목을 식별하기 위한 CI 조회 규칙.

MID 서버

HCL을 사용한 패치 오케스트레이션 BigFix 통합은 취약성 대응 온 프레미스 통합입니다. MID 서버 클러스터에 속하지 않는 독립 실행형 MID 서버가 필요합니다. MID 서버는 BigFix 서버에서 데이터를 임포트하기 위해 인스턴스의 원격 머신에서 스크립트를 실행하는 데 필요합니다. 이 통합에 대한 API는 인스턴스에서 설정한 ServiceNow AI Platform MID Server를 사용하여 호출됩니다. 자세한 내용은 취약성 대응 HCL BigFix와의 패치 오케스트레이션 통합 준비 문서를 참조하십시오.

HCL BigFix와 패치 오케스트레이션 통합의 취약성 대응 통합 및 의존성

HCL BigFix 통합을 사용하는 취약성 대응 패치 오케스트레이션에 필요한 제품 및 종속성 애플리케이션은 다음과 같습니다. 이러한 애플리케이션은 다음에서 사용할 수 있습니다 ServiceNow# Store.

패치 오케스트레이션 통합에 필요한 애플리케이션 및 의존성의 사용 가능한 버전

의 취약성 대응작업 공간에서 패치 오케스트레이션 데이터와 사용 가능한 업데이트(패치)를 보려면 다음 애플리케이션이 필요합니다. 나열된 모든 애플리케이션은 에서 사용할 수 있습니다 ServiceNow# Store. 일부 애플리케이션에는 별도의 구독이 필요합니다.

필수 애플리케이션 및 제품군 릴리스와의 버전 호환성에 대한 자세한 내용은 HI 지식베이스에서 KB0856498 Vulnerability Response 호환성 매트릭스 및 릴리스 스키마 변경 문서를 참조하십시오.

애플리케이션 및 릴리스 버전
취약성 대응
취약성 솔루션 관리
취약성 대응 Patch 오케스트레이션 애플리케이션
취약성 대응 HCL을 사용한 오케스트레이션 패치 BigFix 애플리케이션
Security Support Common
보안 지원 오케스트레이션
지원되는 외부 공급업체 취약성 스캐너 애플리케이션

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약성 대응 **Patch** 오케스트레이션 애플리케이션 테이블

패치 오케스트레이션 애플리케이션에는 취약성 대응 다음 테이블이 포함되어 있습니다.

테이블	설명
패치 업데이트 〔sn_vul_patch_orch_update〕	개별 인스턴스에서 사용할 수 있는 패치에 대한 정보를 저장합니다.
장치 업데이트 〔sn_vul_patch_orch_m2m_src_ci_update〕	배포 상태와 함께 검색된 항목 기록에 표시되는 배포된 패치에 대한 데이터를 저장합니다.
컬렉션 〔sn_vul_patch_orch_collection〕	개별 인스턴스의 컬렉션 데이터를 저장합니다.
장치 컬렉션 〔sn_vul_patch_orch_m2m_src_ci_collection〕	검색된 항목에 대한 컬렉션 데이터를 저장합니다.
패치 배포 〔sn_vul_patch_orch_deployment〕	컬렉션 및 CI에 대해 배포된 패치에 대한 정보를 저장합니다.
잠재적 패치 〔sn_vul_patch_orch_m2m_vuln_patch〕	취약성을 해결하는 데 사용될 수 있는 패치를 식별하는 패치 및 취약성에 대한 데이터를 저장합니다.

HCL BigFix와의 취약성 대응 패치 오케스트레이션 통합

엔지니어링에 의해 ServiceNow# 개발된 통합은 BigFix 제품과의 오케스트레이션된 솔루션 배치를 구성합니다. 다음 통합은 에서 다운로드하는 ServiceNow# StoreHCL BigFix 애플리케이션과의 패치 오케스트레이션 통합에 포함되어 취약성 대응 있습니다.

인스턴스에 통합 애플리케이션을 ServiceNow AI Platform 설치한 후 이러한 통합을 보려면 통합 〉 **BigFix** 패치 오케스트레이션 통합 〉 통합. 취약성 대응 애플리케이션은 BigFix 엔드포인트와의 통합으로 임포트된 예약된 시간 간격으로 데이터를 처리합니다.

통합	설명
BigFix 컬렉션 통합	• 이 통합은 매일 실행되도록 예약되어 있으며 연결된 통합 실행에서 먼저 실행됩니다. • BigFix 애플리케이션에서 컴퓨터 그룹(구성 항목)을 구성하는 컴퓨터와 컴퓨터 그룹을 검색합니다.
BigFix Fixlet 통합	• 예약되면 이 통합은 BigFix 컬렉션 통합이 완료될 때 트리거됩니다. 요청 시 실행할 수도 있습니다. • BigFix 서버에서 사용 가능한 모든 Fixlet(패치)에 대한 정보를 검색합니다.
BigFix 장치 Fixlet 통합	• 예약되면 BigFix Fixlet 통합이 완료되면 이 통합이 트리거됩니다. 요청 시 실행할 수도 있습니다. • BigFix 서버에서 현재 컴퓨터(자산)에 있는 Fixlet에 대한 정보를 검색합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

통합	설명
BigFix 작업 통합	• 스케줄된 경우, 이 통합은 BigFix 장치 Fixlet 통합이 완료되면 트리거됩니다. 요청 시 실행할 수도 있습니다. • BigFix 서버에서 IT 팀이 예약한 패치에 대한 정보를 검색합니다.

취약성 대응 **HCL** BigFix와의 패치 오케스트레이션 통합 준비

다음 설정 작업을 수행하여 통합을 준비합니다.

시작하기 전에

필요한 역할: 애플리케이션 설치 및 역할 할당을 위한 관리자 다른 역할은 다음 테이블에 나열되어 있습니다.

이 태스크 정보

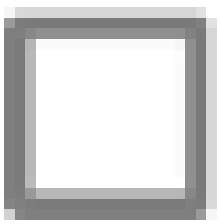
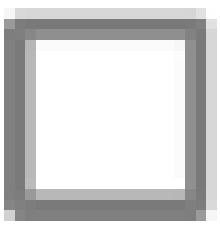
성공적인 통합을 위해서는 통합 전 작업을 계획하고 신중하게 실행해야 합니다.

준비가 되었습니다 취약성 대응 HCL을 사용하여 Patch 오케스트레이션 설치 BigFix 애플리케이션.

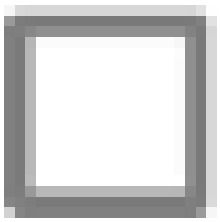
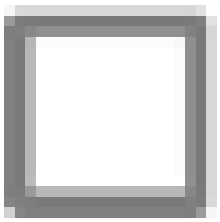
프로시저

1. Patch Orchestration with HCL BigFix 애플리케이션의 원활한 설치 및 구성을 취약성 대응 위해 제공된 검사 목록을 따르십시오.
2. 애플리케이션을 설치하기 전에 다음 검사 목록을 인쇄하고 나열된 항목이 완료되었는지 확인할 수 있습니다.

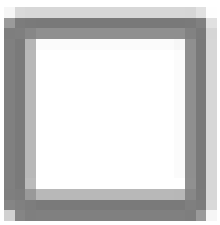
   설치 및 구성 후 취약성 및 패치 관련 정보를 인스턴스로 임포트합니다 ServiceNow AI Platform# .

작업	설명
	(선택 사항) 아직 설치 및 활성화되지 않은 경우 타사 애플리케이션을 설치하기 전에 애플리케이션을 설치하는 취약성 대응 것이 좋습니다. 애플리케이션 설치 및 활성화에 취약성 대응 대한 자세한 내용은 을 참조하십시오 취약성 대응 설치. 이 통합에는 버전 16.0 취약성 대응 이상이 필요합니다.
	아직 설치하지 않은 경우 권리를 확보하고 타사 스캐너 애플리케이션을 설치하여 취약성 데이터를 임포트합니다. 에서 취약성 대응지원하는 외부 공급업체 스캐너에 대한 자세한 내용은 을 참조하십시오취약성 대응 통합. 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업	설명
	아직 설치하지 않은 경우 권리를 확보하고 Vulnerability Response Patch Orchestration with HCL BigFix 애플리케이션을 ServiceNow AI Platform# 인스턴스에 다운로드합니다. 문서를 참조하십시오.
	BigFix 자격 증명을 얻습니다. BigFix 제품에 액세스할 수 있도록 BigFix 제품에 필요한 계정 이름, 비밀번호 및 기타 서비스 정보가 있는지 확인하십시오.
	통합을 관리하고 취약한 항목을 정정할 그룹 또는 사용자가 있는지 확인합니다. 관리자 시스템 관리자는 BigFix Patch 오케스트레이션 애플리케이션 및 통합에 필요한 기타 애플리케이션을 권리 확보, 다운로드 및 설치합니다. 할당되지 않은 경우 관리자는 사용자 관리 모듈 안 취약성 대응 팎에서 취약성 관리자 (sn_vul.vulnerability_admin) 및 설정 도우미의 다른 역할을 할당합니다. sn_vul.vulnerability_admin 할당된 취약성 관리자는 BigFix 통합 및 기타 외부 공급업체 애플리케이션의 구성을 완료합니다. 이 역할은 (VR) 애플리케이션 및 해당 기록에 대한 취약성 대응 전체 액세스 권한을 보유합니다. 이 역할은 모든 VR 애플리케이션, 규칙, 외부 공급업체 통합, 취약성 대응, 패치 오케스트레이션 및 취약성 솔루션 관리 애플리케이션을 구성합니다. sn_vul_bigfix.configure_integration 이 역할이 있는 사용자는 BigFix Patch 오케스트레이션 통합 애플리케이션을 구성합니다. 이 역할에는 사용자가 BigFix 콘솔에 연결하고 사용자의 통합 인스턴스를 구성할 수 있도록 허용하는 sn_vul_bigfix.read_integration 및 connection_admin 세분화된 역할이 포함되어 있습니다 ServiceNow AI Platform. sn_vul_bigfix.read_integration 이 역할을 가진 사용자는 BigFix Patch 오케스트레이션 통합 애플리케이션 및 패치 오케스트레이션 데이터의 기록을 취약성 대응 보기 (읽기 전용)할 수 있습니다. sn_vul_patch_orch.configure_patch 이 역할을 가진 사용자는 패치를 구성하고 적용할 수 있습니다. 변경 관리가 활성 상태이고 승인자가 할당된 경우 취약한 항목 및 패치 업데이트

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업	설명
	기록에서 이 사용자가 요청한 패치가 승인을 위해 전송됩니다. sn_vul_patch_orch.read_patch 이 역할을 가진 사용자는 기록에 대한 패치 정보를 보거나 읽기 전용으로 사용할 수 있습니다. 이 역할은 IT 정정 및 취약성 관리자 작업 공간에 필요한 sn_vul.remediation_owner 및 sn_vuln.vulnerability_analyst 역할로 상속됩니다. 승인자 승인자 수준 1 및 선택적으로 승인자 수준 2에 할당된 사용자, 승인자 그룹은 제출된 패치 요청을 승인합니다. 기본적으로 패치는 배포 전에 승인을 위해 승인자 수준 1 그룹에 제출됩니다. 승인 프로세스에 대한 자세한 내용은 다음 문서를 참조하십시오 다음으로 오케스트레이션 패치 취약성 대응. 승인자 및 그룹 설정에 대한 자세한 내용은 다음 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 시스템 관리자는 통합을 위해 사용자 및 그룹에 초기 역할 할당을 수행합니다. 기본적으로 취약성 대응 그룹을 사용할 수 있습니다. 아직 생성하지 않은 경우 정정 전문가 및 취약성 분석가 역할에 대한 추가 그룹을 생성하고 인스턴스에서 사용자 관리 모듈을 사용하여 사용자를 추가할 수 있습니다. 사용자 그룹 만들기를 참조하십시오.
	통합에 필요한 인스턴스의 기능, 규칙, 의존성 플러그인 또는 작업을 활성화했는지 확인합니다. ○ HCL을 사용한 취약성 대응 패치 오케스트레이션 BigFix는 독립 실행형 MID 서버를 사용해야 하는 온 프레미스 통합입니다. 인스턴스의 MID 서버에 대한 자세한 내용은 MID 서버 단원을 참조하십시오. ○ 다음으로 이동 시스템 애플리케이션 〉 모든 사용 가능 애플리케이션 〉 모두 플러그인을 찾습니다. 인스턴스에 설치되어 있지 않은 경우 설치하고 활성화합니다.

다음에 수행할 작업
이제 할 준비가 취약성 대응 HCL을 사용하여 Patch 오케스트레이션 설치 BigFix 애플리케이션되었습니다.

취약성 대응 HCL을 사용하여 **Patch** 오케스트레이션 설치 **BigFix** 애플리케이션

에서 ServiceNow# StoreVulnerability Response Patch Orchestration with HCL BigFix 애플리케이션을 .

시작하기 전에
필요한 역할: admin sn_vul.vulnerability_admin 역할의 초기 할당 및 애플리케이션 설치를 위한 admin. 취약성 관리자(sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음))를 사용하여 HCL, BigFix 및 기타 애플리케이션을 설치한 후 취약성 대응 패치 오케스트레이션을 구성합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보
애플리케이션을 설치하기 전에 의 취약성 대응 HCL BigFix와의 패치 오케스트레이션 통합 준비검사 목록에 있는 모든 항목을 완료했는지 확인합니다.

주:
이 프로세스는 프로덕션 인스턴스에 다운로드된 애플리케이션에만 적용됩니다. 애플리케이션을 비프로덕션 또는 개발 인스턴스에 다운로드하는 경우에는 권리를 얻을 필요가 없습니다. 로 애플리케이션 활성화 ServiceNow Store계속 진행합니다.

프로시저

1. 다음으로 이동 모두 〉 시스템 애플리케이션 〉 사용 가능한 모든 애플리케이션 〉 모두.
2. **Vulnerability Response Patch Orchestration with HCL BigFix** 애플리케이션을 찾아 설치를 클릭하십시오.

   이 작업은 에서 ServiceNow Store다운로드한 애플리케이션을 설치합니다.
3. 또는 설정 도우미에서 애플리케이션을 설치할 수 있습니다.
   설치 도우미를 사용하여 응용 프로그램을 설치하는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 설정 도우미를 사용하여 타사 응용 프로그램 설치 취약성 대응.

다음에 수행할 작업
설치를 완료한 후 모두 〉 **BigFix** 패치 오케스트레이션 통합 〉 구성 구성을 계속합니다.

HCL BigFix와의 취약성 대응 패치 오케스트레이션 통합 구성

애플리케이션을 설치한 후 BigFix 계정 정보로 구성하고 자격 증명의 유효성을 검증하십시오.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin 및 sn_vul_bigfix.configure_integration

프로시저

1. 다음으로 이동 **BigFix** 패치 오케스트레이션 통합 〉 구성.
2. BigFix 정보 및 자격 증명으로 필드를 채웁니다.

필드	설명
통합 인스턴스	사용할 BigFix 인스턴스 계정의 이름(예: BigFix ## ## ##)
호스트 이름	BigFix 호스트의 URL을 입력합니다.
사용자 이름	BigFix 계정 사용자 이름을 입력합니다.
암호	BigFix 계정 암호를 입력합니다.
MID 서버	사용할 목록에서 독립 실행형 MID 서버의 이름을 입력합니다. MID Server에 대한 자세한 내용은 을 참조 취약성 대응 HCL BigFix와의 패치 오케스트레이션 통합 준비 하고 작업을 ServiceNow AI Platform#설정하십시오.

3. 자격 증명 저장 및 테스트를 클릭합니다.
   BigFix와 ServiceNow AI Platform# 인스턴스 간의 연결 상태가 유효성 확인 상태 필드에 표시됩니다. 성공적인 테스트가 표시되지 않으면 프롬프트를 따릅니다.
4. 옵션: 이 통합에는 도메인 분리가 지원됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

인스턴스에 여러 구성을 추가할 수 있습니다. 구성을 추가하려면 다음을 수행합니다.

a. 다음으로 이동 **BigFix** 패치 오케스트레이션 통합 통합 인스턴스.

b. 애플리케이션 범위인 HCL BigFix# ### ### ## ## #######이 애플리케이션 범위 필드에 표시되는지 확인합니다.

c. 새로 만들기를 클릭합니다.

d. 양식을 작성합니다.

필드	설명
이름	통합 인스턴스의 이름입니다.
애플리케이션	HCL BigFix를 사용한 취약성 대응 패치 오케스트레이션
통합	〔읽기 전용〕 BigFix 패치 관리가 기본값입니다.
활성	기본값은 활성화(선택)입니다. 선택을 취소하면 인스턴스가 활성화되지 않습니다.

e. 제출을 클릭합니다.
새 통합 인스턴스가 통합 인스턴스 목록에 표시됩니다.

f. 1-3단계를 반복하여 통합 인스턴스를 구성하고 자격 증명을 테스트합니다.

5. 패치 요청에 대한 승인을 설정합니다.
기본적으로 패치 배포가 예약되면 검토 및 승인을 위해 수준 1 - 패치 업데이트 승인 그룹에 할당된 사용자에게 제출되도록 시스템 속성 〔**sn_vul_patch_orch.patch_approval_required**〕이 활성화됩니다.

sn_vul_patch_orch.configure_patch 역할의 사용자가 승인 없이 패치를 예약하도록 하려면 [**sn_vul_patch_orch.patch_approval_required**] 속성을 비활성화할 수 있습니다. 예약된 패치가 정상 작업 시간과 상충되지 않도록 승인을 활성화된 상태로 두는 것을 선호할 수 있습니다.

주:
승인 시스템 속성을 비활성화하면 sn_vul_patch_orch.configure_patch 역할을 가진 모든 사용자가 검토 및 승인 없이 패치를 예약하고 배포할 수 있습니다.

sn_vul.vulnerability_admin 역할을 가진 사용자가 시스템 속성을 비활성화하려면 다음을 수행합니다.

a. 다음으로 이동 **sys.properties.list**.

b. **sn_vul_patch_orch.patch_approval_required**를 찾은 후 클릭하여 기록을 엽니다.

c. 값 필드에 false를 입력합니다.

d. 업데이트를 클릭합니다.

6. 이 속성을 비활성화하지 않으면 패치 요청에 대한 승인자를 할당해야 합니다.
sn_vul.vulnerability_admin 역할을 가진 사용자는 다음 단계를 수행합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 다음으로 이동 취약성 대응 〉 관리 〉 승인 규칙.

b. 패치 업데이트 승인 배포 승인 규칙이 목록에 표시되지 않는 경우, 화면 왼쪽 상단의 녹색 필터 아이콘 오른쪽에 있는 전체를 클릭하여 전체 목록을 표시합니다.

c. 목록에서 **Deploy patch update** approval(패치 업데이트 승인 배포)을 클릭합니다.

d. 기록에서 승인 구성 탭을 선택한 상태에서 기본 구성 패치 업데이트 승인을 클릭합니다.

e. 기록에서 수준 **1 -** 패치 업데이트 승인을 클릭합니다.

f. 이 그룹에 사용자를 추가합니다.

이 그룹에 할당된 사용자는 sn_vul_patch_orch.configure_patch 역할을 가진 사용자가 제출한 패치 요청을 승인합니다. 내 승인으로 이동하여 요청을 보고 처리합니다.

7. 업데이트를 클릭하여 변경 내용을 저장합니다.

8. 옵션: 예약된 패치 요청을 배포하기 전에 둘 이상의 승인이 필요하도록 다단계 승인을 설정할 수 있습니다.

a. 기본 구성 패치 업데이트 승인 기록이 표시되면 새로 만들기를 클릭합니다.

b. 필드에 내용을 입력합니다.

필드	설명
이름	승인 수준 이름(예: 수준 **2 -** 패치 업데이트 승인)
활성	기본적으로 활성화되며, 승인 수준이 사용 중임을 나타냅니다.
필요한 승인	선택한 수준에 필요한 승인 수를 선택합니다. ▪ 승인자 1명 필요 ▪ 모든 사용자의 승인 필요
순서	규칙 내에서 다양한 구성의 실행 순서입니다. 예를 들어 주문 항목이 100인 구성은 주문 항목이 200인 구성보다 먼저 실행됩니다.
역할	목록에서 그룹의 역할을 선택합니다.
승인 규칙	승인 규칙에 대한 테이블 및 유형 상세 정보를 포함합니다.
승인 구성	승인 구성을 포함합니다.
할당 사용	옵션 선택: ▪ 사용자 및 사용자 그룹 ▪ 승인 테이블 필드 ▪ 스크립트

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
그룹	여러 사용자로 구성된 승인자 수준 그룹입니다. 사용자는 다음 역할 중 하나를 지정해야 합니다.
사용자	그룹에 나열된 사용자를 편집합니다.

c. 제출을 클릭하여 편집 내용을 저장합니다.

HCL BigFix와의 패치 오케스트레이션 통합에 취약성 대응 대한 패치 데이터 보기

패치 데이터와 패치 롤업 데이터뿐 아니라 취약성 정보와 취약성의 정정 상태도 인스턴스의 기록에 표시됩니다.

작업 공간에서 패치 데이터 취약성 대응 보기

필요한 역할:

- 패치를 구성하고 예약하는 sn_vul_patch_orch.configure_patch 역할
- sn_vul_patch_orch.read_patch - 기록에 대한 패치 정보를 (읽기 전용) 볼 수 있습니다. 이 역할은 IT Remediation 및 Vulnerability Manager Workspace에 필요한 sn_vul.remediation_owner 및 sn_vuln.vulnerability_analyst 역할과 함께 상속됩니다

IT 정정 작업 공간에서 패치를 볼 수 있습니다.

- 성과표를 클릭하여 VI의 기본 솔루션, 취약한 CI 및 VI의 기본 패치에 대한 기록을 볼 수 있는 홈 뷰.
- 패치 링크의 모든 패치 업데이트 기록(VPU)과 패치가 있는 사용자에게 할당된 취약한 항목(VIT)을 볼 수 있는 목록 뷰.

다음 기록에서 패치를 예약할 수 있습니다.

- 패치 업데이트(VPU)에서
- 정정 작업(RT)
- 검색된 항목(SDI) 기록

취약성 관리자 작업 공간에서 패치를 볼 수 있습니다.

- 감시 주제의 홈 뷰에서 선호하는 패치와 잠재적 패치, 패치 일정 날짜, 패치가 다운로드된 경우 취약한 항목 탭에 있는 모든 항목을 볼 수 있습니다.
- 정정 작업에 대한 목록 뷰의취약한 항목 탭에서 VI 기록에 대한 패치 데이터를 볼 수 있습니다.

클래식 환경 뷰에서 모두 〉 취약성 대응 〉 패치.

VR 작업 공간 및 클래식 환경 뷰에서 패치 업데이트 기록

패치 데이터와 패치 롤업 데이터 및 상태가 인스턴스의 기록에 표시됩니다. 패치 기록은 와 취약성 대응통합의 패치 오케스트레이션 기능의 일부로 포함됩니다. IT 정정 작업 공간의 목록 뷰에서 작업 공간의 패치(VPU) 기록을 취약성 대응 봅니다. 클래식 뷰와 취약성 대응 작업 공간 모두에서 패치 업데이트 기록에는 다음 데이터가 포함됩니다.

- 취약성 솔루션 관리 애플리케이션에서 임포트한 패치 벤더의 취약성 솔루션 데이터 및 정보입니다.
- 패치로 해결할 수 있는 특정 취약성이 있는 총 장치 수와 업데이트가 누락된 모든 장치를 포함하는 소스 정정 상태입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 정정된 VI의 비율(%)과 기본 패치로 패치가 있는 총 VI를 포함하는 정정 상태입니다.
- 클래스 뷰의 기록에 대한 관련 링크에 연결된 장치, 취약한 항목, 패치 배포 및 패치 요청. 이 데이터는 작업 공간에 있는 취약성 대응 기록의 탭에 표시됩니다.
- 정정 소유자가 승인을 위해 제출한 패치 요청입니다.

취약한 항목 기록에 대한 상태 롤업

기록에 대한 상태 롤업에 대한 자세한 내용은 다음 문서를 참조하십시오 의 패치 오케스트레이션에 대한 패치 데이터 및 상태 롤업 취약성 대응.

활성 **VI** 카운트를 롤업하는 기록

모든 패치를 모든 취약성에 롤업하지 않기 위해 예약된 작업은 활성 VI 수에 대한 변경 내용만 선택합니다. 이러한 카운트 변경 및 관련 데이터는 다음의 취약성 대응다음 기록으로 롤업됩니다.

- VIT
- RT
- 취약성 솔루션
- 패치 업데이트

솔루션 없이 패치에 대한 데이터 보기

솔루션 없이 패치를 보는 방법에 대한 자세한 내용은 문서를 참조하십시오 에서 솔루션이 없는 패치 보기 취약성 대응.

를 사용하여 데이터 패치 취약성 대응

취약성 관리(PA) 및 CISO 대시보드는 애플리케이션에 대한 퍼포먼스 분석취약성 대응 구독에 포함됩니다. 를 구독 퍼포먼스 분석하지만 패치 오케스트레이션 통합이 설치되어 있지 않은 경우 CISO 대시보드에 정정 탭이 표시되지만 데이터로 채워지지는 않습니다.

취약성 관리(PA) 대시보드의 경우 모두 〉 취약성 대응 〉 개요. 정정 탭을 클릭하고 페이지 하단으로 스크롤하여 패치 업데이트 데이터(예약된 패치와 예약되지 않은 패치, 대상 날짜가 누락된 패치, 주별 개수)를 확인합니다.

CISO 대시보드의 경우 다음으로 이동합니다. 모두 〉 취약성 대응 〉 **CISO** 대시보드. 개요 탭을 선택한 상태에서 페이지 아래쪽으로 스크롤하여 패치 범위 데이터(중요도, 예약된 패치와 예약되지 않은 패치, 대상 날짜가 누락된 패치)를 봅니다.

대시보드에 취약성 대응 대한 자세한 내용은 기본 취약성 대응 대시보드 사용, 작업 공간으로 취약성 대응 오케스트레이션 패치, 및 대시보드에서 취약성 대응 패치 오케스트레이션 데이터 보기를 참조하십시오.

패치 오케스트레이션 통합으로 취약성 대응 패치 예약 **HCL BigFix**

인스턴스의 애플리케이션에서 ServiceNow AI Platform 패치, 업데이트 및 정정 작업 기록에서 패치를 예약합니다취약성 대응.

시작하기 전에
버전 16.1부터 작업 공간 또는 클래식 환경에서 패치를 취약성 대응 예약할 수 있습니다.

필요한 역할:

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 패치를 구성하고 예약하는 sn_vul_patch_orch.configure_patch 역할
- sn_vul_patch_orch.read_patch - 기록에 대한 패치 정보를 (읽기 전용) 볼 수 있습니다. 이 역할은 IT Remediation 및 Vulnerability Manager Workspace에 필요한 sn_vul.remediation_owner 및 sn_vuln.vulnerability_analyst 역할과 함께 상속됩니다

프로시저

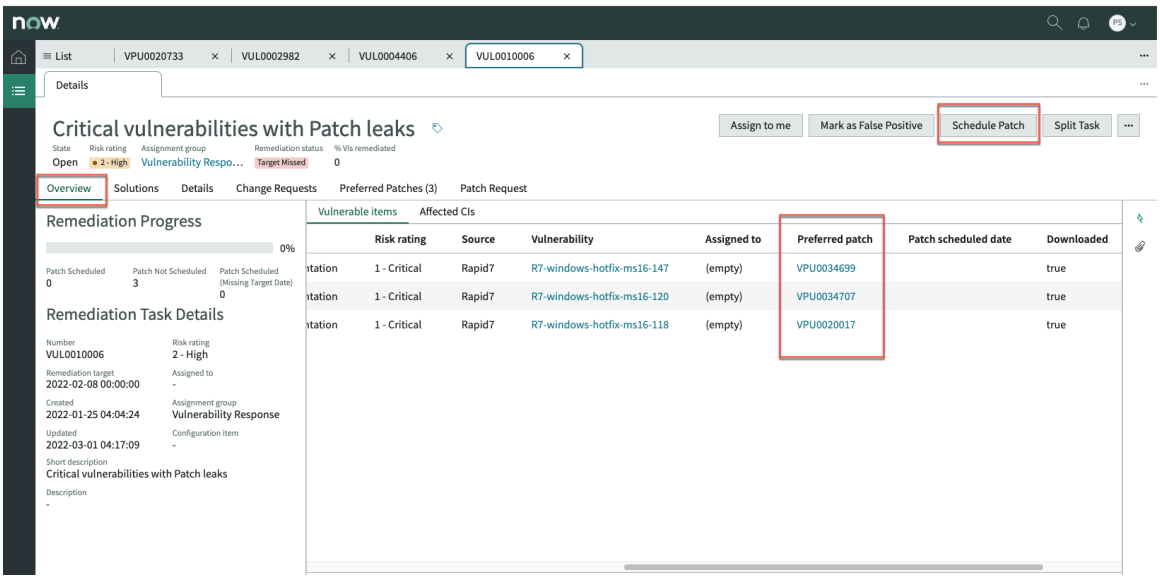
1. 취약성 취약성 대응 작업 공간에서 sn_vul.remediation_owner 역할을 가진 사용자는 모두 〉 취약성 대응 〉 **IT** 정정 작업 공간.
2. 홈 페이지에서 VI의 기본 패치를 클릭합니다.
   할당된 기본 패치가 있는 VI에 대한 패치 업데이트 기록 목록이 표시됩니다.
3. 열려는 기록을 찾아 클릭하여 엽니다.
4. 또는 작업 공간의 목록 뷰에서 패치 〉 모두 패치 업데이트 기록을 찾습니다.
   패치 업데이트 기록이 표시됩니다. 다른 패치가 이미 예약되어 있을 수 있으므로 패치를 예약하기 전에 데이터를 검토하는 것이 좋습니다.
5. 표시되는 데이터 및 수행할 수 있는 작업에 대한 다음 테이블을 참조하십시오.

6. **Schedule** Patch(패치 예약)를 클릭합니다.
7. 대화 상자에서 필드에 내용을 입력합니다.

8. 배포를 클릭합니다.
   패치 요청이 검토를 위해 전송됩니다. 에서 제출된 모든 요청의 상태를 볼 수 있습니다. 예외 요청 〉 내 요청 목록 뷰에서.
9. 또는 사용자 또는 그룹에 할당된 정정 작업(RT)에서 패치를 예약할 수 있습니다.

> **주:**
> 정정 작업 기록에서 패치를 예약하는 옵션은 작업의 VI에 매핑된(연결된 패치가 있는) 경우에만 사용할 수 있습니다. 이러한 패치는 개요 탭을 선택한 상태에서 정정 작업 기록의 오른쪽으로 스크롤하는 경우 기본 패치 열에 표시됩니다.

기본 패치가 있는 정정 작업



10. RT 기록에서 패치 예약을 클릭하고 위에 나열된 단계에 따라 대화 상자에서 예약합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

11. 클래식 환경에서 이전에 나열된 단계에 대한 패치를 예약할 수 있습니다. 이러한 기록을 찾으려면 다음 단계를 수행합니다.

a. 클래식 환경에서 다음으로 이동합니다. 취약성 대응 〉 패치 〉 모두.

b. 표시되는 목록에서 패치 업데이트 기록을 찾습니다.

c. 정정 작업의 경우 다음으로 이동하십시오. 취약성 대응 〉 정정 작업 을 클릭하고 기록을 찾습니다. 정정 상태 탭에서 정정 상태를 추적합니다. 기록 하단에 패치 데이터가 관련 링크에 표시됩니다.

d. 패치 예약을 클릭하고 필드를 채웁니다.

필드	설명
배포 이름	이 패치 배포의 이름을 입력합니다. 이 이름은 업데이트를 추적하는 데 도움이 됩니다.
패치 업데이트	목록에서 사용 가능한 패치 중 하나를 선택합니다.
자산	다음 중 하나를 선택합니다. ▪ 컴퓨터 그룹: 이 패치에 대한 컬렉션(자산 그룹)을 선택하려면 이 옵션을 선택합니다. 그룹은 BigFix 애플리케이션에서 임포트한 구성 항목으로 구성됩니다. ▪ 컴퓨터 목록: 이 패치에 대한 개별 컴퓨터(자산)를 선택하려면 이 옵션을 선택합니다. 제조업체, 위치, 클래스, 마지막 업데이트 시간 및 표시되는 대화 상자에서 유지관리 일정에 대한 데이터를 볼 수 있습니다.
시작 시간 및 종료 시간	시간 창의 시작 및 종료 시간을 입력합니다. 패치 배포를 시작할 시기와 패치를 설치할 수 있는 마지막 날을 입력합니다.

HCL BigFix와의 취약성 대응 패치 오케스트레이션 통합에 대한 **REST** 메시지

취약성 대응 HCL BigFix REST 메시지와의 패치 오케스트레이션 통합은 BigFix API를 호출하는 데 사용됩니다.

BigFix 로그인

REST API 요청을 인증할 수 있도록 BigFix 로그인에 대한 REST 메시지를 사용할 수도 있습니다. REST 메시지의 레코드 메소드에 대한 변경사항은 BigFix에 대한 인증 요청에 영향을 줍니다.

매개변수 이름	값	설명
sourceType	누적하는	소스 통합이 데이터를 가져오는 출처를 나타냅니다. 코드에서 사용됩니다. 변경하지 않는 것이 좋습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

매개변수 이름	값	설명
정렬 DIR	설명	통합에서 가져온 데이터의 정렬 방향을 나타냅니다. 변경하지 않는 것이 좋습니다.
sortField	severity	데이터 정렬의 기준 필드를 나타냅니다. 변경하지 않는 것이 좋습니다.
유형	취약성	자산 통합을 위한 통합에서 가져올 데이터 유형을 나타냅니다. 변경하지 않는 것이 좋습니다.

BigFix 통합

BigFix 통합에 REST 메시지를 사용하여 BigFix에서 정보를 검색할 수 있습니다. REST 메시지의 레코드 메소드에 대한 변경사항은 정보를 검색하기 위해 BigFix에 대한 요청에 영향을 줍니다. REST 메시지에는 다음과 같은 REST 메서드가 포함됩니다.

REST 메서드

REST 메서드	설명
데이터 가져오기 가져오기	제공된 쿼리를 기반으로 BigFix에서 다음 중 하나에 관한 정보를 검색합니다. • 컴퓨터/컴퓨터 그룹 • Fixlet • 컴퓨터의 관련 Fixlet • 작업

매개변수 이름	값	설명
URL	사용자에 기반한 동적 값	BigFix 콘솔의 엔드포인트를 나타냄

BigFix 배포 패치

BigFix 통합에 대한 REST 메시지를 사용하여 사용자의 ServiceNow AI Platform# BigFix에 대한 패치를 예약할 수 있습니다. REST 메시지의 레코드 메소드에 대한 변경사항은 정보를 검색하기 위해 BigFix에 대한 요청에 영향을 줍니다. REST 메시지에는 다음과 같은 REST 메서드가 포함됩니다.

REST 메서드	설명
POST 배포 패치	단일/여러 대의 컴퓨터에서 BigFix 콘솔에 패치를 예약합니다.

매개변수 이름	값	설명
URL	사용자에 기반한 동적 값	BigFix 콘솔의 엔드포인트를 나타냅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

매개변수 이름	값	설명
직위	사용자에 기반한 동적 값	배포의 제목입니다.
settings_tag	값이 있는 XML 태그 이름 지정 설정	다른 매개변수가 있고 패치를 스케줄하는 동안 BigFix로 전송되는 설정을 나타냅니다.
computer_tag	값이 있는 XML 태그 이름의 컴퓨터	패치가 예약될 컴퓨터 목록을 나타냅니다.
site_name	패치 업데이트 값	Fixlet이 있는 사이트의 이름입니다.
fixlet_id	패치 업데이트 값	Fixlet의 ID입니다.

HCL BigFix와의 패치 오케스트레이션 통합을 위한 데이터 변환

데이터는 HCL BigFix 통합을 통해 패치 오케스트레이션에서 검색 취약성 대응 되고 데이터 소스 세트를 통해 처리되어 인스턴스에서 변환됩니다 ServiceNow AI Platform# .

BigFix 컬렉션 임포트

임포트한 자산(컴퓨터 및 컴퓨터 그룹)의 데이터가 BigFix 컬렉션 임포트 [sn_vul_bigfix_collection_import] 테이블에 로드됩니다. BigFix 컴퓨터 및 컴퓨터 그룹 임포트 TM(변환 맵?)은 임포트한 정보를 변환하는 데 사용됩니다.

주:
이 변환 맵을 변경하면 BigFix Collection 임포트의 데이터가 처리되는 방식이 변경됩니다.

이 변환 맵에 액세스하려면 다음으로 이동하십시오. 시스템 임포트 세트 〉 변환 맵 을 클릭하고 BigFix 컴퓨터 및 컴퓨터 그룹 임포트 TM을 찾습니다. 다음 표에는 통합별 변환 맵 필드가 나열되어 있습니다.

BigFix 컴퓨터 및 컴퓨터 그룹 임포트 변환 맵 스크립트 타이밍

스크립트	설명
OnStart(임포트 세트에서 변환을 생성한 경우)	통합 프로세스에 대한 범위 변수 〔sn_vul_bigfix〕의 값을 초기화하는 데 사용되는 스크립트입니다. 이 스크립트는 내부용이며 수정하거나 삭제하면 안 됩니다.
onBefore(임포트 세트가 변환을 완료하기 전)	CI 조회 규칙 및 컬렉션뿐 아니라 이들 간의 관계를 기반으로 CI를 만들고 업데이트하는 데 사용되는 스크립트입니다. 결과에 따라 이 스크립트는 범위 변수 〔sn_vul_bigfix〕의 값을 수정합니다. 이 스크립트는 내부용이며 수정하거나 삭제하면 안 됩니다.
onComplete(임포트 세트가 변환을 완료한 경우)	생성, 업데이트 및 무시되는 CI 수를 설정하는 데 사용되는 스크립트입니다. 이 스크립트는 내부용이며 수정하거나 삭제하면 안 됩니다.

BigFix Fixlet 임포트

임포트된 Fixlet의 데이터가 BigFix Fixlet 임포트 [sn_vul_bigfix_patch_update_import] 테이블에 로드됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

BigFix Fixlet Import TM은 임포트한 정보를 변환하는 데 사용됩니다.

주:
이 변환 맵의 변경사항은 BigFix Fixlet 임포트의 데이터가 처리되는 방식을 변경합니다.

이 변환 맵에 액세스하려면 다음으로 이동하십시오. 시스템 임포트 세트 〉 변환 맵 을 클릭하고 BigFix Fixlet Import TM을 찾으십시오.

다음 표에는 통합별 변환 맵 필드가 나열되어 있습니다.

BigFix Fixlet 임포트 변환 맵 필드

소스 필드	대상 필드	설명
u_id	article_id	사이트에 있는 Fixlet의 고유 ID입니다.
u_id	source_id	사이트에 있는 Fixlet의 고유 ID입니다.
U_site_name	Sn_vul_bigfix_site_name	Fixlet이 사용되는 BigFix의 사이트 이름입니다.
U_display_name	직위	Fixlet의 제목입니다.
〔스크립트〕	Bulletin_id	솔루션의 소스 ID입니다.
〔스크립트〕	Sn_vul_solution	소스 ID를 기반으로 하는 솔루션입니다.
U_source	bulletin_source	솔루션의 소스 벤더입니다.
〔스크립트〕	Date_release	Fixlet의 릴리스 날짜입니다.
U_category	Update_category	Fixlet의 범주입니다.
〔스크립트〕	Is_highest_supersedence	Fixlet이 가장 높은 대체인지 여부에 대한 부울입니다.
〔스크립트〕	Is_downloaded	Fixlet이 다운로드되었는지 여부에 대한 부울입니다.
〔스크립트〕	Integration_instance	Fixlet을 가져오는 인스턴스의 이름입니다.
U_source_severity	Source_severity	Fixlet의 심각도입니다.
U_applicable_count	Num_total	Fixlet이 누락된 총 장치 수입니다.
〔스크립트〕	Last_modified	Fixlet의 마지막 수정 날짜입니다.

BigFix Fixlet 임포트 변환 맵 스크립트 타이밍

스크립트	설명
OnStart(임포트 세트에서 변환을 생성한 경우)	통합 프로세스에 대한 범위 변수 〔sn_vul_bigfix〕의 값을 초기화하는 데 사용되는 스크립트입니다. 이 스크립트는 내부용이며 수정하거나 삭제하면 안 됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

BigFix Fixlet 임포트 변환 맵 스크립트 타이밍

스크립트	설명
onBefore(임포트 세트가 변환을 완료하기 전)	범위 변수 〔sn_vul_bigfix〕의 값을 업데이트하는 데 사용되는 스크립트입니다. 이 스크립트는 내부용이며 수정하거나 삭제하면 안 됩니다.
onComplete(임포트 세트가 변환을 완료한 경우)	작성, 업데이트 및 무시되는 Fixlet의 수를 설정하는 데 사용되는 스크립트입니다. 이 스크립트는 내부용이며 수정하거나 삭제하면 안 됩니다.

BigFix 장치 Fixlet 임포트

컴퓨터에서 가져온 관련 fixlet의 데이터는 BigFix Device Fixlet Import [sn_vul_bigfix_device_patch_import] 테이블에 로드됩니다.

BigFix Device Fixlet TM은 임포트한 정보를 변환하는 데 사용됩니다.

주:
이 변환 맵의 변경사항은 BigFix Device Fixlet 임포트의 데이터가 처리되는 방식을 변경합니다.

이 변환 맵에 액세스하려면 다음으로 이동하십시오. 시스템 임포트 세트 〉 변환 맵 을 클릭하고 BigFix Device Fixlet TM을 찾으십시오.

다음 표에는 통합별 변환 맵 필드가 나열되어 있습니다.

BigFix 장치 Fixlet 변환 맵 스크립트 타이밍

스크립트	설명
OnStart(임포트 세트에서 변환을 생성한 경우)	통합 프로세스에 대한 범위 변수 〔sn_vul_bigfix〕의 값을 초기화하는 데 사용되는 스크립트입니다. 이 스크립트는 내부용이며 수정하거나 삭제하면 안 됩니다.
onBefore(임포트 세트가 변환을 완료하기 전)	CI 조회 규칙 및 컬렉션뿐 아니라 이들 간의 관계를 기반으로 CI를 만들고 업데이트하는 데 사용되는 스크립트입니다. 결과에 따라 이 스크립트는 범위 변수 〔sn_vul_bigfix〕의 값을 수정합니다. 이 스크립트는 내부용이며 수정하거나 삭제하면 안 됩니다.
onComplete(임포트 세트가 변환을 완료한 경우)	생성, 업데이트 및 무시되는 CI 수를 설정하는 데 사용되는 스크립트입니다. 이 스크립트는 내부용이며 수정하거나 삭제하면 안 됩니다.

BigFix 작업 임포트

임포트한 작업의 데이터가 BigFix 작업 임포트 [sn_vul_bigfix_deployment_import] 테이블에 로드됩니다.

BigFix 작업 임포트 TM은 임포트한 정보를 변환하는 데 사용됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
이 변환 맵을 변경하면 BigFix Actions 임포트의 데이터가 처리되는 방식이 변경됩니다.

이 변환 맵에 액세스하려면 다음으로 이동하십시오. 시스템 임포트 세트 〉 변환 맵 을 클릭하고 BigFix Fixlet Import TM을 찾으십시오.

다음 표에는 통합별 변환 맵 필드가 나열되어 있습니다.

BigFix 작업 변환 맵 필드 임포트

소스 필드	대상 필드	설명
u_id	source_id	작업의 고유 ID입니다.
U_name	이름	작업의 이름
〔스크립트〕	Sn_vul_bigfix_discovered_item	패치가 배포되어 검색된 항목의 참조
U_status	상태	작업 상태
〔스크립트〕	Sn_vul_patch_orch_update	패치의 참조
U_apply_count	Count_success	작업의 성공 카운트입니다.
U_retry_count	재시도	작업의 재시도 횟수입니다.
〔스크립트〕	Deployment_time	작업의 시작 시간입니다.
〔스크립트〕	마감	작업의 종료 시간입니다.
〔스크립트〕	Source_created	작업을 생성한 시간입니다.
〔스크립트〕	Integration_instance	작업을 임포트하는 인스턴스의 이름입니다.

BigFix 작업 임포트 변환 맵 스크립트 타이밍

스크립트	설명
OnStart(임포트 세트에서 변환을 생성한 경우)	통합 프로세스에 대한 범위 변수 〔sn_vul_bigfix〕의 값을 초기화하는 데 사용되는 스크립트입니다. 이 스크립트는 내부용이며 수정하거나 삭제하면 안 됩니다.
onBefore(임포트 세트가 변환을 완료하기 전)	범위 변수 〔sn_vul_bigfix〕의 값을 업데이트하는 데 사용되는 스크립트입니다. 이 스크립트는 내부용이며 수정하거나 삭제하면 안 됩니다.
onComplete(임포트 세트가 변환을 완료한 경우)	작성, 업데이트 및 무시되는 작업 수를 설정하는 데 사용되는 스크립트입니다. 이 스크립트는 내부용이며 수정하거나 삭제하면 안 됩니다.

HCL BigFix와의 취약성 대응 패치 오케스트레이션 통합에 대한 예시 워크플로우

HCL BigFix 제품에서 패치 오케스트레이션이 작동하는 방식의 예입니다.

시작하기 전에
예를 들어 전체 환경이 3주에 한 번씩 패치된다고 가정해 보겠습니다. 가장 최근의 패치 적용 기간이 일주일 전에 완료되었지만 최근에 알려진 중요한 취약점을 수정하기 위해 패치를 적용하려고 합니다. 이 취약성의 중요한 특성으로 인해 예정된 다음 패치를 위해 2주를 더 기다릴 수 없습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필요한 역할:

- 취약성 관리자 작업 공간의 sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin
- sn_vul.remediation_owner - IT 정정 소유자 작업 공간을 볼 수 있습니다.
- sn_vul_patch_orch.configure_patch 역할을 구성하여 패치를 구성하고 예약합니다.
- sn_vul_patch_orch.read_patch - 기록에 대한 패치 정보를 (읽기 전용) 볼 수 있습니다. 이 역할은 IT 정정 및 취약성 관리자 작업 공간에 필요한 sn_vul.remediation_owner 및 sn_vuln.vulnerability_analyst 역할로 상속됩니다.

이 태스크 정보

취약성 관리자 작업 공간에서 작업하는 취약성 관리자 또는 분석가는 중요 취약성이 있는 임포트된 VI를 캡처하는 데 도움이 되도록 감시 주제를 생성하거나 기존 감시 주제를 편집하는 것을 고려할 수 있습니다. 패치 오케스트레이션 통합을 사용하면 이러한 취약성을 수정하고 추적하는 데 사용할 패치를 확인할 수도 있습니다. 다음 표에는 패치 오케스트레이션에 대한 주시 주제에 대해 설정할 수 있는 조건이 포함된 몇 가지 샘플이 나와 있습니다. 이러한 예제를 사용하면 환경에 가장 적합한 설정을 결정하는 데 도움이 됩니다. 감시 항목 설정에 대한 자세한 정보는 을 참조하십시오 에서 주시 주제 생성 취약성 관리자 작업 공간 .

취약성 관리자 작업 공간의 패치 오케스트레이션에 대한 샘플 주시 주제

주시 주제 이름	설명
패치 유출이 있는 치명적인 취약성	## ### 1 - ## 그리고 ### ### #### ### #####.
패치 예약됨(SLA 누락)이 있는 위험한 취약성	## ## ## ###(## ## ##)
패치가 예약된 위험한 취약성	## ### 1 - ## 그리고 ## ## ### ## ## ####. 그리고 ### ## ### ##### #####.

- 취약성 관리자 또는 분석가는 감시 주제 및 정정 작업을 생성한 후 정정 작업을 생성합니다. VI 레코드 및 정정 작업에서 탐지 탭으로 드릴다운하고 BigFix 제품에서 임포트한 자산과 함께 추적 중인 취약성이 있는 검색된 항목 레코드를 찾을 수 있습니다.
- 취약성 분석가 또는 관리자는 취약성과 연관된 패치 데이터를 모니터링할 수 있습니다. 검색된 항목 기록에서 특정 자산(구성 항목)에 패치 하나 또는 여러 개의 패치를 배포할 수도 있습니다.

IT 정정 전문가는 패치 배포로 취약성을 해결하는 방법에 대한 옵션을 제공합니다.

- 패치 업데이트 기록(VPU#)에서 패치를 예약할 수 있습니다.
- 취약한 항목(VI)에 기본 솔루션이 매핑되어 있고 사용자 또는 그룹에 할당된 경우 이러한 취약한 항목이 있는 정정 작업에서 패치를 예약할 수 있습니다.

프로시저

1. IT 정정 전문가는 IT 정정 작업 공간에서 홈 뷰를 클릭합니다.
2. 홈 뷰에서 할당된 정정 작업 성과표를 클릭하여 기록을 봅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 예에서는 정정 작업(VUL#)의 간단한 설명 필드에서 중요 취약성과 관련된 텍스트를 확인할 수 있습니다. 예를 들어, 취약성 관리자가 이 중요한 취약성으로 VI(VIT#)를 포착하기 위해 패치 누출이 있는 위험한 취약성이라는 감시 주제를 생성했음을 알 수 있습니다.

기록이 열린 상태에서 VI, 기본 패치를 검토하고 자신 또는 그룹 구성원이 승인을 위한 패치 요청을 이미 제출했는지 확인할 수도 있습니다.

3. 충분한 정보가 있는 경우 이 정정 작업에서 지금 패치 요청을 제출하는 것이 좋습니다.

   주:
   기록과 연결된 VI에 매핑된 패치가 없는 경우 기록에서 패치 일정 예약 버튼을 사용할 수 없습니다.

4. 패치 예약을 클릭하고 대화 상자의 필드를 입력합니다.
   패치를 예약하는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 패치 오케스트레이션 통합으로 취약성 대응 패치 예약 HCL BigFix.
5. 또는 IT 정정 작업 공간의 목록 뷰에서 정정 작업, 취약한 항목, 솔루션 및 패치 링크를 클릭하여 이러한 기록을 볼 수 있습니다.

   이 예제의 경우 주시 주제 이름 대신 패치의 문서 ID 또는 공지 ID 및 제목을 알 수 있습니다. 그렇다면 이 취약성이 있는 VI가 사용자 또는 그룹에 할당되었는지 확인할 수 있습니다. 패치 업데이트 기록에서 패치 요청을 제출할 수 있습니다. VI 기록에서 잠재적인 패치를 확인하고 패치 요청을 제출하려는 경우 관련 정정 작업을 열 수 있습니다.

6. 작업 영역에 액세스할 수 없거나 클래식 환경에서 데이터를 보고 패치를 예약하려는 경우 다음 단계를 수행합니다.

   a. 다음으로 이동 모두 〉 취약성 대응 〉 패치 〉 모두.

   b. 원하는 패치 업데이트 기록을 찾습니다.
   ## 위험 점수로 기록을 필터링하는 것이 좋습니다.

   c. 정정 상태 탭에서 연결된 VI 및 정정된 VI 비율(%) 필드를 검토합니다.
   VI에 사용 가능한 패치가 있는 경우 기록의 오른쪽 상단에 패치 예약 버튼이 표시됩니다.

   d. 요청을 제출하려면 패치 예약을 클릭합니다.
   패치를 예약하는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 패치 오케스트레이션 통합으로 취약성 대응 패치 예약 HCL BigFix.

   e. 또는 패치 ID 정보가 없지만 그룹에 할당된 정정 작업의 간단한 설명 필드에 중요 취약성과 관련된 텍스트가 있는지 확인할 수 있습니다.

   f. 다음으로 이동 모두 〉 취약성 대응 〉 정정 작업 〉 사용자 그룹에 할당됨.

   g. 원하는 기록을 찾아 클릭하여 엽니다.
   오픈 기록에서 정정 상태 탭에서 VI 및 정정된 VI 비율(%)을 검토합니다. VI 기록, 기본 솔루션, 기본 패치 및 패치 요청에 대한 관련 링크를 클릭합니다.

      주:
      기록과 연결된 VI에 매핑된 패치가 없는 경우 기록에서 패치 일정 예약 버튼을 사용할 수 없습니다.

   h. 패치 요청을 제출하려면 기록에서 패치 예약을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

SCCM 취약성 대응 과의 **Microsoft** 패치 오케스트레이션 통합 이해

시스템 센터 구성 관리자(SCCM) 제품과 통합하여 Microsoft 자산의 취약성 대응 중요 취약성에 대한 패치 및 패치 배포를 관리합니다.

다음으로 오케스트레이션 패치 취약성 대응

를 사용하여 취약성 대응 오케스트레이션을 패치하면 타사 솔루션 통합, 패치 벤더 및 취약성 스캐너에서 예약된 임포트를 사용합니다. 스캐너 탐지 데이터는 환경의 자산을 취약성 및 이를 수정할 수 있는 패치 업데이트와 일치시킵니다. 승인을 위해 패치 요청을 제출하고, 취약한 항목을 해결하기 위해 패치 업데이트를 예약하고, 정정 진행 상황을 모니터링할 수 있습니다 ServiceNow AI Platform# .

취약성 대응 SCCM으로 **Microsoft** 오케스트레이션 패치

SCCM 애플리케이션의 Vulnerability Response Patch Orchestration Microsoft 을 패치 오케스트레이션 및 취약성 대응 애플리케이션과 함께 ServiceNow# 취약성 솔루션 관리사용하는 경우 취약성 관리자와 분석가는 다음 작업을 수행할 수 있습니다.

- 패치 유형 및 벤더의 솔루션(패치)에 대한 자세한 컨텍스트와 정보를 참조하십시오.
- 작업 공간의 기록 취약성 대응 에서 취약성 및 솔루션 데이터뿐 아니라 취약성 정정 진행 상황을 보고 모니터링합니다.

IT 전문가와 정정 소유자는 다음 작업을 수행할 수 있습니다.

- 작업과의 충돌을 피하기 위해 업무 외 시간에 정기적으로 예약된 간격으로 해당 Windows자산, CentOS OraclemacOS및 기타 자산에 대해 SCCM 제품에서 Microsoft 지원하는 패치를 배포합니다.
- 취약성이 있는 패치되지 않은 자산 또는 외부 공급업체 스캐너에서 임포트한 탐지 데이터의 예약된 패치를 통해 성공적으로 업데이트되었거나 업데이트되지 않은 자산을 식별합니다.
- 패치 업데이트, 정정 작업 및 검색된 항목 기록에서 취약하고 패치되지 않은 자산에 대해 IT 정정 작업 공간 또는 클래식 UI에서 사용 가능한 패치를 예약합니다.

및 **Microsoft SCCM** 애플리케이션의 주요 용어 취약성 대응

CI(구성 항목)

CI는 에 나열된 구성 관리 데이터베이스(CMDB)기존 자산입니다. Microsoft SCCM은 CI, 장치를 호출합니다.

컬렉션 및 장치 컬렉션

자산 그룹을 나타내는 SCCM 제품에 사용되는 Microsoft 용어입니다.

취약한 항목

CMDB의 기존 자산과 일치하는 임포트한 취약성입니다.

인스턴스

SCCM 애플리케이션에 대한 고유한 계정입니다 Microsoft . 각 사용자 계정은 Microsoft SCCM 애플리케이션의 인스턴스가 될 수 있습니다. 이 용어는 인스턴스에 대한 고유하고 안전한 웹 주소를 의미하기도 합니다 ServiceNow AI Platform .

통합

통합은 SCCM 시스템과의 통합과 같은 외부 공급업체 소스에서 정보를 검색하는 예약된 작업 ServiceNow AI Platform 입니다 Microsoft .

솔루션

이러한 통합의 맥락에서 솔루션에는 두 가지 유형, 즉 잠재적 솔루션과 기본 솔루션이 있습니다. 잠재적 솔루션은 취약성을 해결할 수 있는 솔루션입니다. 취약성에는 종종

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

많은 잠재적인 솔루션이 있습니다. #기본 솔루션은 탐지된 특정 취약성에 대해 가장 효과적인 솔루션과 일치합니다.

패치

취약성을 수정하는 소프트웨어 업데이트. Microsoft SCCM 응용 프로그램에서는 패치를 패치라고 합니다. 예를 들어, Microsoft SCCM에는 CentOS, Oracle MAC 및 기타 제품에 대한 Windows패치가 있습니다.

기본 패치

기본 패치는 특정 취약점을 수정하기 위한 소프트웨어 업데이트입니다. 패치가 배포되면 특정 취약성과 관련된 취약한 항목에 매핑되어 수정합니다.

정정 작업 또는 취약성 그룹(v15.0 취약성 대응이전)

취약성을 수정하는 데 필요한 작업 애플리케이션의 취약한 항목 취약성 대응 목록입니다.

배포

이 통합을 위한 배포는 컴퓨터에 패치를 적용, 시작 또는 예약하는 경우를 의미합니다. 의 취약성 대응개별 기록에서 검색된 항목, 패치 또는 정정 작업으로 이동하여 SCCM에서 Microsoft 다운로드한 패치를 배포할 수 있습니다ServiceNow AI Platform. 예약된 작업이 있는 패치를 개별 컴퓨터 또는 컴퓨터 그룹에 배포할 수 있습니다.

의 ServiceNow AI Platform 배포는 다중 소스를 지원하는 통합을 참조할 수도 있습니다. 단일 통합 존재를 통합의 배포라고 합니다. 배포는 환경 전반의 통합 및 제품을 의미합니다. 예를 들어 사용자 환경에 SCCM 취약성 통합이 Microsoft 여러 개 배포되어 있을 수 있습니다.

취약성 솔루션 관리 SCCM과의 취약성 대응**Microsoft** 패치 오케스트레이션 통합

이 취약성 솔루션 관리 애플리케이션은 취약성 결과를 정정하는 솔루션(패치)의 세부 항목과 연관시키는 애플리케이션입니다 ServiceNow AI Platform . 제품 및 서비스, 구성 업데이트 및 조직에 가장 큰 영향을 미치는 기타 통제에 대한 외부 공급업체의 소프트웨어 패치를 식별합니다. 외부 공급업체 스캐너 정보와 취약성 대응용 솔루션 관리함께 , 취약성 대응, 및 SCCM을 사용한 Microsoft 취약성 대응 Patch Orchestration 애플리케이션이 함께 작동하여 솔루션에서 취약성, 취약한 항목으로 기본 패치를 롤업하여 사용자 환경의 취약성을 수정하고 종결하는 데 도움을 줍니다. 취약성 대응용 솔루션 관리, 취약성 대응, 및 취약성 대응 패치 오케스트레이션 Microsoft SCCM 통합 애플리케이션은 모두 에서 사용할 수 있습니다ServiceNow# Store.

필요한 **ServiceNow AI Platform** 역할

통합 설치, 구성 및 정정 작업에는 인스턴스에서 다음 역할이 ServiceNow AI Platform 필요합니다.

관리자

이 역할을 가진 사용자는 에 있는 ServiceNow Store 애플리케이션에 대한 권리를 얻고 인스턴스에 다운로드합니다 ServiceNow AI Platform .

sn_vul.vulnerability_admin

이 역할이 있는 사용자는 인스턴스에서 애플리케이션을 ServiceNow AI Platform 활성화하고 애플리케이션 구성을 취약성 대응 완료합니다. 이 역할은 (VR) 애플리케이션 및 해당 기록에 대한 취약성 대응 전체 액세스 권한을 보유합니다. 이 관리자는 모든 VR 애플리케이션, 규칙 및 외부 공급업체 통합을 구성합니다.

sn_vul_sccm.configure_integration

이 역할이 있는 사용자는 SCCM 패치 오케스트레이션 통합 애플리케이션을 구성합니다 Microsoft . 이 역할에는 sn_vul_sccm.read_integration 세분화된 역할이 포함됩니다.

sn_vul_sccm.read_integration

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 역할을 가진 사용자는 SCCM 패치 오케스트레이션 통합 애플리케이션과 패치 오케스트레이션 데이터의 기록을 취약성 대응Microsoft 봅니다(읽기 전용).

sn_vul_patch_orch.configure_patch

이 역할을 가진 사용자는 패치를 구성하고 적용할 수 있습니다.

sn_vul_patch_orch.read_patch

이 역할을 가진 사용자는 패치 정보를 보거나 읽기 전용으로 사용할 수 있습니다.

승인자

배포 전에 제출된 패치 요청을 승인하려면 승인자 수준 1 및 승인자 수준 2 승인자 그룹에 용도를 할당합니다.

설정 도우미를 사용하여 이러한 역할을 할당하는 방법에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당.

CI 조회 규칙

SCCM 애플리케이션에서 취약성 대응 데이터를 임포트 Microsoft 하면 애플리케이션은 자원 ID 데이터를 사용하여 일치하는 항목을 구성 관리 데이터베이스(CMDB) 자동으로 검색합니다. CI 조회 규칙은 VI(자산)를 식별하고 VI가 생성될 때 VI(취약한 항목) 기록에 자동으로 추가하는 데 사용됩니다. 다음 CI 조회 규칙은 기본 시스템과 함께 제공되며 CI(자산)를 식별하고 검색된 항목에 추가하는 데 사용됩니다.

이 조회 규칙은 SCCM이 있는 서비스 그래프 커넥터에서 가져온 데이터를 사용합니다. SCCM 통합을 실행하기 전에 CMDB 통합을 설치하고 실행해야 합니다. SCCM 서버가 여러 개 설치되어 있는 경우 SCCM 패치 오케스트레이션 구성 페이지에서 서비스 그래프 커넥터 연결 별칭을 구성할 수 있습니다.

MID 서버

SCCM이 포함된 Microsoft 취약성 대응 패치 오케스트레이션은 온 프레미스 통합입니다. MID 서버 클러스터에 속하지 않는 독립 실행형 Windows MID 서버가 필요합니다. MID 서버는 SCCM 서버에서 데이터를 임포트하기 위해 인스턴스의 원격 컴퓨터에서 스크립트를 실행하는 데 필요합니다. 이 통합을 위한 API는 인스턴스에서 설정한 ServiceNow AI Platform MID Server를 사용하여 호출됩니다. SCCM과의 취약성 대응Microsoft 패치 오케스트레이션 통합 준비

SCCM 애플리케이션과 Vulnerability Response Patch Orchestration Microsoft 의 통합 및 종속성

시스템 센터 구성 관리자(SCCM)와의 Microsoft 취약성 대응 패치 오케스트레이션 통합에 필요한 제품 및 종속성 애플리케이션은 다음과 같습니다. 이러한 애플리케이션은 다음에서 사용할 수 있습니다. ServiceNow# Store

패치 오케스트레이션 통합에 필요한 애플리케이션 및 의존성의 사용 가능한 버전

작업 공간과 의 취약성 대응클래식 UI에서 패치 오케스트레이션 데이터 및 사용 가능한 업데이트(패치)를 보려면 다음 애플리케이션이 필요합니다. 나열된 모든 애플리케이션은 에서 사용할 수 있습니다 ServiceNow# Store. 일부 애플리케이션에는 별도의 구독이 필요합니다.

필수 애플리케이션 및 제품군 릴리스와의 버전 호환성에 대한 자세한 내용은 HI 지식베이스에서 KB0856498 Vulnerability Response 호환성 매트릭스 및 릴리스 스키마 변경 문서를 참조하십시오.

애플리케이션 및 릴리스 버전
취약성 대응
취약성 솔루션 관리

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

애플리케이션 및 릴리스 버전
취약성 대응 Patch 오케스트레이션 애플리케이션
Vulnerability Response Patch Orchestration with Microsoft SCCM 애플리케이션
Security Support Common
보안 지원 오케스트레이션
SCCM이 있는 서비스 그래프 커넥터

취약성 대응 **Patch** 오케스트레이션 애플리케이션 테이블

패치 오케스트레이션 애플리케이션에는 취약성 대응 다음 테이블이 포함되어 있습니다.

테이블	설명
패치 업데이트 〔sn_vul_patch_orch_update〕	개별 인스턴스에서 사용할 수 있는 패치에 대한 정보를 저장합니다.
장치 업데이트 〔sn_vul_patch_orch_m2m_src_ci_update〕	배포 상태와 함께 검색된 항목 기록에 표시되는 배포된 패치에 대한 데이터를 저장합니다.
컬렉션 〔sn_vul_patch_orch_collection〕	개별 인스턴스의 컬렉션 데이터를 저장합니다.
장치 컬렉션 〔sn_vul_patch_orch_m2m_src_ci_collection〕	검색된 항목에 대한 컬렉션 데이터를 저장합니다.
패치 배포 〔sn_vul_patch_orch_deployment〕	컬렉션 및 CI에 대해 배포된 패치에 대한 정보를 저장합니다.
잠재적 패치 〔sn_vul_patch_orch_m2m_vuln_patch〕	취약성을 해결하는 데 사용될 수 있는 패치를 식별하는 패치 및 취약성에 대한 데이터를 저장합니다.

SCCM 통합을 통한 **Microsoft** 취약성 대응 **Patch Orchestration**

엔지니어링에 의해 ServiceNow# 개발된 통합은 SCCM 제품과 함께 Microsoft 오케스트레이션된 솔루션 배포를 구성합니다. 다음 통합은 에서 다운로드한 Microsoft SCCM 패치 오케스트레이션 통합 애플리케이션에 포함되어 있습니다 ServiceNow# Store.

인스턴스에 통합 애플리케이션을 ServiceNow AI Platform 설치한 후 이러한 통합을 보려면 통합 〉 **SCCM** 패치 오케스트레이션 통합 〉 통합. 취약성 대응 애플리케이션은 SCCM 엔드포인트와의 Microsoft 통합으로 임포트된 예약된 시간 간격으로 데이터를 처리합니다.

통합	설명
Microsoft SCCM 컬렉션 통합	• 이 통합은 매일 실행되도록 예약되어 있으며 연결된 통합 실행에서 먼저 실행됩니다. • SCCM 컬렉션에서 장치 컬렉션을 검색합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

통합	설명
Microsoft SCCM 장치 컬렉션 통합	• 예약되면 이 통합은 SCCM 컬렉션 통합이 완료될 때 트리거됩니다. 요청 시 실행할 수도 있습니다. • 이 통합은 각 컬렉션 아래에 있는 장치를 가져옵니다. 이 통합은 검색된 항목 테이블과 장치 컬렉션 테이블에 기록을 생성합니다.
Microsoft SCCM 패치 업데이트 통합	• 예약되면 이 통합은 SCCM 장치 컬렉션 통합이 완료될 때 트리거됩니다. 요청 시 실행할 수도 있습니다. • SCCM 서버에서 장치(자산)에 설치되었거나 누락된 패치에 대한 정보를 검색합니다.
Microsoft SCCM 배포 통합	• 예약된 경우 이 통합은 패치 업데이트 통합이 완료될 때 트리거됩니다. 요청 시 실행할 수도 있습니다. • SCCM 서버에서 IT 팀이 예약한 패치에 대한 정보를 검색합니다.

SCCM과의 취약성 대응**Microsoft** 패치 오케스트레이션 통합 준비

다음 설정 작업을 수행하여 통합을 준비합니다.

시작하기 전에

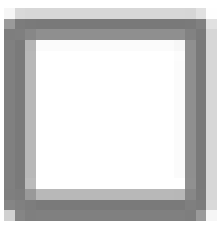
필요한 역할: 애플리케이션 설치 및 역할 할당을 위한 관리자 다른 역할은 다음 테이블에 나열되어 있습니다.

이 태스크 정보

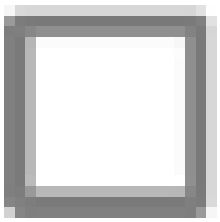
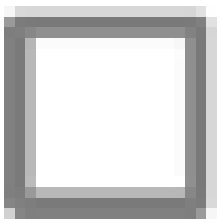
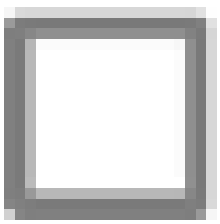
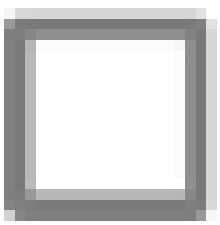
성공적인 통합을 위해서는 통합 전 작업을 계획하고 신중하게 실행해야 합니다.

프로시저

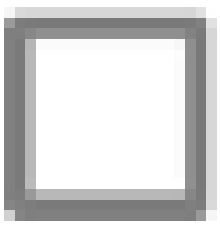
1. SCCM을 포함한 Microsoft 취약성 대응 패치 오케스트레이션 애플리케이션의 원활한 설치 및 구성을 위해 아래에 제공된 검사 목록을 따르십시오.
2. 애플리케이션을 설치하고 취약성 및 패치 관련 정보를 인스턴스로 ServiceNow AI Platform# 임포트하기 전에 다음 검사 목록을 인쇄하고 나열된 항목이 완료되었는지 확인하는 것이 좋습니다.

작업	설명
	(선택 사항) 아직 설치 및 활성화되지 않은 경우 타사 애플리케이션을 설치하기 전에 애플리케이션을 설치하는 취약성 대응 것이 좋습니다. 애플리케이션 설치 및 활성화에 취약성 대응 대한 자세한 내용은 을 참조하십시오 취약성 대응 설치. 이 통합에는 버전 16.1 취약성 대응 이상이 필요합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업	설명
	아직 설치하지 않은 경우 권리를 확보하고 타사 스캐너 애플리케이션을 설치하여 취약성 데이터를 임포트합니다. 에서 취약성 대응지원하는 외부 공급업체 스캐너에 대한 자세한 내용은 을 참조하십시오취약성 대응 통합. 문서를 참조하십시오.
	아직 설치하지 않은 경우 권리를 얻고 SCCM을 사용한 Microsoft 취약성 대응 Patch Orchestration 애플리케이션을 ServiceNow AI Platform# 인스턴스에 다운로드합니다. 문서를 참조하십시오.
	SCCM 자격 증명을 얻습니다 Microsoft . 제품에 액세스할 수 있도록 제품에 필요한 Microsoft 계정 이름, 암호 및 기타 서비스 정보가 있는지 확인합니다.
	통합을 관리하고 취약한 항목을 정정할 그룹 또는 사용자가 있는지 확인합니다. 관리자 시스템 관리자는 SCCM 패치 오케스트레이션 애플리케이션과 통합에 필요한 기타 애플리케이션을 권리를 얻고 다운로드하고 설치합니다 Microsoft . 할당되지 않은 경우 관리자는 사용자 관리 모듈 안 취약성 대응 팎에서 취약성 관리자(sn_vul.vulnerability_admin) 및 설정 도우미의 다른 역할을 할당합니다. sn_vul.vulnerability_admin 할당된 취약성 관리자는 SCCM 통합 및 기타 외부 공급업체 애플리케이션의 구성을 Microsoft 완료합니다. 이 역할은 (VR) 애플리케이션 및 해당 기록에 대한 취약성 대응 전체 액세스 권한을 보유합니다. 이 역할은 모든 VR 애플리케이션, 규칙, 외부 공급업체 통합, 취약성 대응 패치 오케스트레이션 및 취약성 솔루션 관리 애플리케이션을 구성합니다. sn_vul_sccm.configure_integration 이 역할이 있는 사용자는 SCCM 패치 오케스트레이션 통합 애플리케이션을 구성합니다 Microsoft . 이 역할에는 사용자가 SCCM 콘솔에 연결하고 사용자의 sn_vul_sccm.read_integration에서 통합

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업	설명
	인스턴스를 ServiceNow AI Platform구성할 수 있는 connection_admin 세분화된 역할이 포함됩니다. sn_vul_sccm.read_integration 이 역할을 가진 사용자는 SCCM 패치 오케스트레이션 통합 애플리케이션과 패치 오케스트레이션 데이터의 기록을 취약성 대응Microsoft 봅니다(읽기 전용). sn_vul_patch_orch.configure_patch 이 역할을 가진 사용자는 패치를 구성하고 적용할 수 있습니다. 변경 관리가 활성 상태이고 승인자가 할당된 경우 취약한 항목 및 패치 업데이트 기록에서 이 사용자가 요청한 패치가 승인을 위해 전송됩니다. sn_vul_patch_orch.read_patch 이 역할을 가진 사용자는 기록에 대한 패치 정보를 보거나 읽기 전용으로 사용할 수 있습니다. 이 역할은 IT 정정 및 취약성 관리자 작업 공간에 필요한 sn_vul.remediation_owner 및 sn_vuln.vulnerability_analyst 역할로 상속됩니다. 승인자 승인자 수준 1 및 선택적으로 승인자 수준 2에 할당된 사용자, 승인자 그룹은 제출된 패치 요청을 승인합니다. 기본적으로 패치는 배포 전에 승인을 위해 승인자 수준 1 그룹에 제출됩니다. 승인 프로세스에 대한 자세한 내용은 다음 문서를 참조하십시오 SCCM 통합을 사용하여 Microsoft 취약성 대응 패치 오케스트레이션 구성. 승인자 및 그룹 설정에 대한 자세한 내용은 다음 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 시스템 관리자는 통합을 위해 사용자 및 그룹에 초기 역할 할당을 수행합니다. 기본적으로 취약성 대응 그룹을 사용할 수 있습니다. 아직 생성하지 않은 경우 정정 전문가 및 취약성 분석가 역할에 대한 추가 그룹을 생성하고 인스턴스에서 사용자 관리 모듈을 사용하여 사용자를 추가할 수 있습니다. 사용자 그룹 만들기를 참조하십시오.
	통합에 필요한 인스턴스의 기능, 규칙, 의존성 플러그인 또는 작업을 활성화했는지 확인합니다. ○ SCCM이 포함된 Microsoft 취약성 대응 패치 오케스트레이션은 독립 실행형 Windows MID 서버를 사용해야 하는 사내 통합입니다. 인스턴스의 MID 서버에 대한 자세한 내용은 MID 서버 단원을 참조하십시오. ○ 다음으로 이동 시스템 애플리케이션 〉 모든 사용 가능 애플리케이션 〉 모두 플러그인을 찾습니다. 인스턴스에 설치되어 있지 않은 경우 설치하고 활성화합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약성 대응 **SCCM** 애플리케이션을 사용하여 **Microsoft** 패치 오케스트레이션 설치

에서 ServiceNow Store애플리케이션을 다운로드합니다.

시작하기 전에
애플리케이션을 설치하기 전에 의 SCCM과의 취약성 대응Microsoft 패치 오케스트레이션 통합 준비검사 목록에 있는 모든 항목을 완료했는지 확인합니다.

필요한 역할: admin sn_vul.vulnerability_admin 역할의 초기 할당 및 애플리케이션 설치를 위한 admin. 취약성 관리자(sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음))는 패치 오케스트레이션 Microsoft SCCM 및 기타 애플리케이션을 설치한 후 구성합니다취약성 대응.

주:
이 프로세스는 프로덕션 인스턴스에 다운로드된 애플리케이션에만 적용됩니다. 애플리케이션을 하위 프로덕션 또는 개발 인스턴스에 다운로드하는 경우에는 권리를 애플리케이션 활성화 ServiceNow Store얻을 필요가 없습니다.

프로시저

1. 다음으로 이동 모두 〉 시스템 애플리케이션 〉 사용 가능한 모든 애플리케이션 〉 모두.
2. **Vulnerability Response Patch Orchestration with Microsoft SCCM** 애플리케이션을 찾아 설치를 클릭합니다.

   이 작업은 에서 ServiceNow Store다운로드한 애플리케이션을 설치합니다.
3. 또는 설정 도우미에서 애플리케이션을 설치할 수 있습니다.
   설치 도우미를 사용하여 응용 프로그램을 설치하는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 설정 도우미를 사용하여 타사 응용 프로그램 설치 취약성 대응.

다음에 수행할 작업
설치를 완료한 후 모두 〉 **Microsoft SCCM** 패치 오케스트레이션 통합 〉 구성 구성을 계속합니다.

SCCM 통합을 사용하여 **Microsoft** 취약성 대응 패치 오케스트레이션 구성

애플리케이션을 설치한 후 계정 정보로 구성하고 자격 증명의 유효성을 검사합니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin 및 sn_vul_sccm.configure_integration

프로시저

1. 다음으로 이동 모두 〉 **Microsoft SCCM** 패치 오케스트레이션 통합 〉 구성.
2. Microsoft 필드에 SCCM 정보와 자격 증명을 입력합니다.

필드	설명
통합 인스턴스	사용할 SCCM 인스턴스 계정의 Microsoft 이름입니다(예: Microsoft SCCM ## ## ##).
호스트 이름	SCCM 호스트의 URL을 Microsoft 입력합니다.
사용자 이름	Microsoft SCCM 계정 사용자 이름을 입력합니다.
암호	Microsoft SCCM 계정 암호를 입력합니다.
MID 서버	사용할 목록에서 독립 실행형 MID 서버의 이름을 입력합니다. MID Server에 대한 자세한 내용은 을 참조 SCCM과의 취약성 대응

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	Microsoft 패치 오케스트레이션 통합 준비 하고 작업을 ServiceNow AI Platform#설정하십시오.

3. 자격 증명 저장 및 테스트를 클릭합니다.
   SCCM과 ServiceNow AI Platform# 인스턴스 간의 Microsoft 연결 상태가 확인 상태 필드에 표시됩니다. 성공적인 테스트가 표시되지 않으면 프롬프트를 따릅니다.
4. 옵션: 이 통합에는 도메인 분리가 지원됩니다.
   인스턴스에 여러 구성을 추가할 수 있습니다. 구성을 추가하려면 다음을 수행합니다.

   a. 다음으로 이동 모두 〉 **Microsoft SCCM** 패치 오케스트레이션 통합 통합 인스턴스.

   b. 애플리케이션 범위인 Vulnerability Response Patch Orchestration with Microsoft SCCM이 애플리케이션 범위 필드에 표시되는지 확인합니다.

   c. 새로 만들기를 클릭합니다.

   d. 양식을 작성합니다.

필드	설명
이름	통합 인스턴스의 이름입니다.
애플리케이션	SCCM을 사용한 Microsoft 취약성 대응 패치 오케스트레이션
통합	〔읽기 전용〕 Microsoft SCCM 패치 관리가 기본값입니다.
활성	기본값은 활성화되어 있습니다. 선택을 취소하면 인스턴스가 활성화되지 않습니다.

   e. 제출을 클릭합니다.
   새 통합 인스턴스가 통합 인스턴스 목록에 표시됩니다.

   f. 1-3단계를 반복하여 통합 인스턴스를 구성하고 자격 증명을 테스트합니다.

5. 패치 요청에 대한 승인을 설정합니다.
   기본적으로 패치 배포가 예약되면 검토 및 승인을 위해 수준 1 - 패치 업데이트 승인 그룹에 할당된 사용자에게 제출되도록 시스템 속성 〔**sn_vul_patch_orch.patch_approval_required**〕이 활성화됩니다.

   sn_vul_patch_orch.configure_patch 역할의 사용자가 승인 없이 패치를 예약하도록 하려면 [**sn_vul_patch_orch.patch_approval_required**] 속성을 비활성화할 수 있습니다. 예약된 패치가 정상 작업 시간과 상충되지 않도록 승인을 활성화된 상태로 두는 것을 선호할 수 있습니다.

   주:
   승인 시스템 속성을 비활성화하면 sn_vul_patch_orch.configure_patch 역할을 가진 모든 사용자가 검토 및 승인 없이 패치를 예약하고 배포할 수 있습니다.

   sn_vul.vulnerability_admin 역할을 가진 사용자가 시스템 속성을 비활성화하려면 다음을 수행합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 다음으로 이동 모두 〉 **sys.properties.list**.

b. **sn_vul_patch_orch.patch_approval_required**를 찾은 후 클릭하여 기록을 엽니다.

c. 값 필드에 false를 입력합니다.

d. 업데이트를 클릭합니다.

6. 이 속성을 비활성화하지 않으면 패치 요청에 대한 승인자를 할당해야 합니다. sn_vul.vulnerability_admin 역할을 가진 사용자는 다음 단계를 수행합니다.

a. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 승인 규칙.

b. 패치 업데이트 승인 배포 승인 규칙이 목록에 표시되지 않는 경우, 화면 왼쪽 상단의 녹색 필터 아이콘 오른쪽에 있는 전체를 클릭하여 전체 목록을 표시합니다.

c. 목록에서 **Deploy patch update** approval(패치 업데이트 승인 배포)을 클릭합니다.

d. 기록에서 승인 구성 탭을 선택한 상태에서 기본 구성 패치 업데이트 승인을 클릭합니다.

e. 기록에서 수준 **1 -** 패치 업데이트 승인을 클릭합니다.

f. 이 그룹에 사용자를 추가합니다.

이 그룹에 할당된 사용자는 sn_vul_patch_orch.configure_patch 역할을 가진 사용자가 제출한 패치 요청을 승인합니다. 내 승인으로 이동하여 요청을 보고 처리합니다.

7. 업데이트를 클릭하여 변경 내용을 저장합니다.

8. 옵션: 예약된 패치 요청을 배포하기 전에 둘 이상의 승인이 필요하도록 다단계 승인을 설정할 수 있습니다.

a. 기본 구성 패치 업데이트 승인 기록이 표시되면 새로 만들기를 클릭합니다.

b. 필드에 내용을 입력합니다.

필드	설명
이름	승인 수준 이름(예: 수준 **2 -** 패치 업데이트 승인)
활성	기본적으로 활성화되며, 승인 수준이 사용 중임을 나타냅니다.
필요한 승인	선택한 수준에 필요한 승인 수를 선택합니다. ▪ 승인자 1명 필요 ▪ 모든 사용자의 승인 필요
순서	규칙 내에서 다양한 구성의 실행 순서입니다. 예를 들어 주문 항목이 100인 구성은 주문 항목이 200인 구성보다 먼저 실행됩니다.
역할	목록에서 그룹의 역할을 선택합니다.
승인 규칙	승인 규칙에 대한 테이블 및 유형 상세 정보를 포함합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
승인 구성	승인 구성을 포함합니다.
할당 사용	옵션 선택: ▪ 사용자 및 사용자 그룹 ▪ 승인 테이블 필드 ▪ 스크립트
그룹	여러 사용자로 구성된 승인자 수준 그룹입니다. 사용자는 다음 역할 중 하나를 지정해야 합니다.
사용자	그룹에 나열된 사용자를 편집합니다.

c. 제출을 클릭하여 편집 내용을 저장합니다.

SCCM과 **Microsoft** 패치 오케스트레이션 통합에 취약성 대응 대한 패치 데이터 및 패치 데이터 롤업 보기

패치 데이터와 패치 롤업 데이터뿐 아니라 취약성 정보와 취약성의 정정 상태가 인스턴스의 기록에 표시됩니다.

작업 공간에서 패치 데이터 취약성 대응 보기

필요한 역할:

- 패치를 구성하고 예약하는 sn_vul_patch_orch.configure_patch 역할
- sn_vul_patch_orch.read_patch - 기록에 대한 패치 정보를 (읽기 전용) 볼 수 있습니다. 이 역할은 IT Remediation 및 Vulnerability Manager Workspace에 필요한 sn_vul.remediation_owner 및 sn_vuln.vulnerability_analyst 역할과 함께 상속됩니다

IT 정정 작업 공간에서 패치를 볼 수 있습니다.

- 성과표를 클릭하여 VI의 기본 솔루션, 취약한 CI 및 VI의 기본 패치에 대한 기록을 볼 수 있는 홈 뷰.
- 패치 링크의 모든 패치 업데이트 기록(VPU)과 패치가 있는 사용자에게 할당된 취약한 항목(VIT)을 볼 수 있는 목록 뷰.

다음 기록에서 패치를 예약할 수 있습니다.

- 패치 업데이트(VPU)에서
- 정정 작업(RT)
- 검색된 항목(SDI) 기록

취약성 관리자 작업 공간에서 패치를 볼 수 있습니다.

- 감시 주제의 홈 뷰에서 선호하는 패치와 잠재적 패치, 패치 일정 날짜, 패치가 다운로드된 경우 취약한 항목 탭에 있는 모든 항목을 볼 수 있습니다.
- 정정 작업에 대한 목록 뷰의취약한 항목 탭에서 VI 기록에 대한 패치 데이터를 볼 수 있습니다.

클래식 환경 뷰에서 모두 〉 취약성 대응 〉 패치.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

VR 작업 공간 및 클래식 환경 뷰에서 패치 업데이트 기록

패치 데이터와 패치 롤업 데이터 및 상태가 인스턴스의 기록에 표시됩니다. 패치 기록은 와 취약성 대응통합의 패치 오케스트레이션 기능의 일부로 포함됩니다. IT 정정 작업 공간의 목록 뷰에서 작업 공간의 패치(VPU) 기록을 취약성 대응 봅니다. 클래식 환경과 취약성 대응 작업 공간 모두의 패치 업데이트 기록에는 다음 데이터가 포함됩니다.

- 취약성 솔루션 관리 애플리케이션에서 임포트한 패치 벤더의 취약성 솔루션 데이터 및 정보입니다.
- 패치로 해결할 수 있는 특정 취약성이 있는 총 장치 수를 포함하는 소스 정정 상태입니다. 또한 업데이트가 누락된 모든 장치도 포함됩니다.
- 정정된 VI의 비율(%)과 기본 패치로 패치가 있는 총 VI를 포함하는 정정 상태입니다.
- 클래스 뷰의 기록에 대한 관련 링크에 연결된 장치, 취약한 항목, 패치 배포 및 패치 요청. 이 데이터는 작업 공간에 있는 취약성 대응 기록의 탭에 표시됩니다.
- 정정 소유자가 승인을 위해 제출한 패치 요청입니다.

취약한 항목 기록에 대한 상태 롤업

기록에 대한 상태 롤업에 대한 자세한 내용은 다음 문서를 참조하십시오 의 패치 오케스트레이션에 대한 패치 데이터 및 상태 롤업 취약성 대응.

활성 VI 카운트를 롤업하는 기록

모든 패치를 모든 취약성에 롤업하지 않기 위해 예약된 작업은 활성 VI 수에 대한 변경 내용만 선택합니다. 이러한 카운트 변경 및 관련 데이터는 다음의 취약성 대응다음 기록으로 롤업됩니다.

- VIT
- RT
- 취약성 솔루션
- 패치 업데이트

솔루션 없이 패치에 대한 데이터 보기

솔루션 없이 패치를 보는 방법에 대한 자세한 내용은 문서를 참조하십시오 에서 솔루션이 없는 패치 보기 취약성 대응.

를 사용하여 데이터 패치 취약성 대응

취약성 관리(PA) 및 CISO 대시보드는 애플리케이션에 대한 퍼포먼스 분석취약성 대응 구독에 포함됩니다. 를 구독 퍼포먼스 분석하지만 패치 오케스트레이션 통합이 설치되어 있지 않은 경우 CISO 대시보드에 정정 탭이 표시되지만 데이터로 채워지지는 않습니다.

취약성 관리(PA) 대시보드의 경우 모두 〉 취약성 대응 〉 개요. 정정 탭을 클릭하고 페이지 하단으로 스크롤하여 패치 업데이트 데이터(예약된 패치와 예약되지 않은 패치, 대상 날짜가 누락된 패치, 주별 개수)를 확인합니다.

CISO 대시보드의 경우 다음으로 이동합니다. 모두 〉 취약성 대응 〉 **CISO** 대시보드. 개요 탭을 선택한 상태에서 페이지 아래쪽으로 스크롤하여 패치 범위 데이터(중요도, 예약된 패치와 예약되지 않은 패치, 대상 날짜가 누락된 패치)를 봅니다.

대시보드에 취약성 대응 대한 자세한 내용은 기본 취약성 대응 대시보드 사용, 작업 공간으로 취약성 대응 오케스트레이션 패치, 및 대시보드에서 취약성 대응 패치 오케스트레이션 데이터 보기를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

와 SCCM의 **Microsoft** 통합으로 패치 예약 취약성 대응

인스턴스의 애플리케이션에서 ServiceNow AI Platform 패치, 업데이트 및 정정 작업 기록에서 패치를 예약합니다취약성 대응.

시작하기 전에

버전 16.1부터 작업 공간 또는 클래식 환경에서 패치를 취약성 대응 예약할 수 있습니다.

필요한 역할:

- 패치를 구성하고 예약하는 sn_vul_patch_orch.configure_patch 역할
- sn_vul_patch_orch.read_patch - 기록에 대한 패치 정보를 (읽기 전용) 볼 수 있습니다. 이 역할은 IT Remediation 및 Vulnerability Manager Workspace에 필요한 sn_vul.remediation_owner 및 sn_vuln.vulnerability_analyst 역할과 함께 상속됩니다

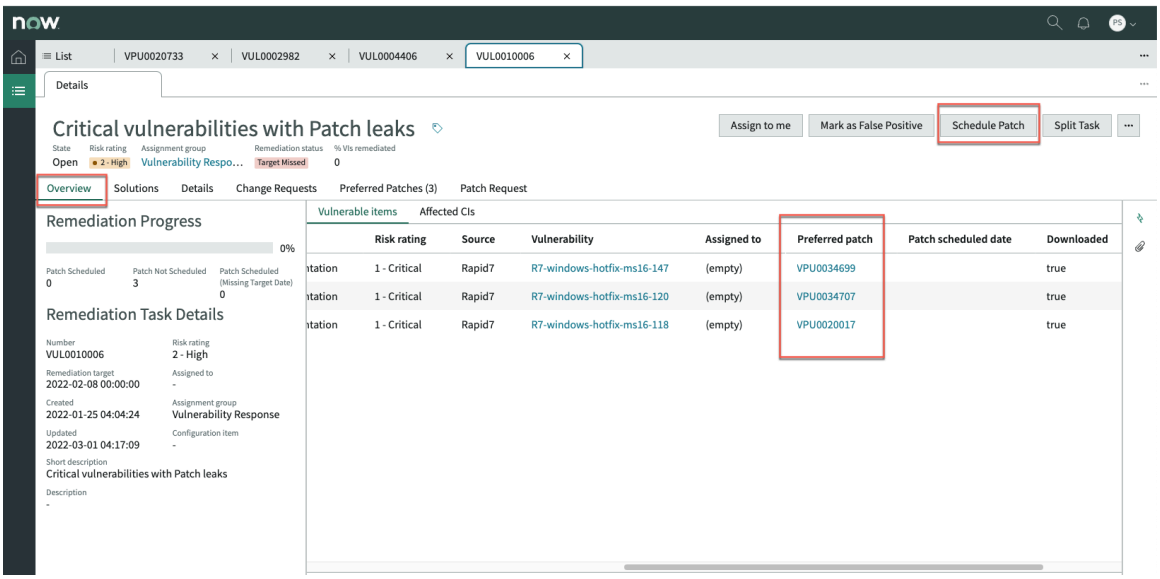
프로시저

1. 취약성 취약성 대응 작업 공간에서 sn_vul.remediation_owner 역할을 가진 사용자는 모두 〉 취약성 대응 〉 **IT** 정정 작업 공간.
2. 홈 페이지에서 VI의 기본 패치를 클릭합니다.
   할당된 기본 패치가 있는 VI에 대한 패치 업데이트 기록 목록이 표시됩니다.
3. 열려는 기록을 찾아 클릭하여 엽니다.
4. 또는 작업 공간의 목록 뷰에서 패치 〉 모두 패치 업데이트 기록을 찾습니다.
   패치 업데이트 기록이 표시됩니다. 다른 패치가 이미 예약되어 있을 수 있으므로 패치를 예약하기 전에 데이터를 검토하는 것이 좋습니다.
5. IT 정정 작업 공간에 표시되는 데이터와 수행 가능한 작업에 대한 다음 테이블을 참조하십시오.
6. **Schedule** Patch(패치 예약)를 클릭합니다.
7. 대화 상자에서 필드에 내용을 입력합니다.
8. 배포를 클릭합니다.
   패치 요청이 검토를 위해 전송됩니다. 에서 제출된 모든 요청의 상태를 볼 수 있습니다. 예외 요청 〉 내 요청 목록 뷰에서.
9. 또는 사용자 또는 그룹에 할당된 정정 작업(RT)에서 패치를 예약할 수 있습니다.

> **주:**
> 정정 작업 기록에서 패치를 예약하는 옵션은 작업의 VI에 매핑된(연결된 패치가 있는) 경우에만 사용할 수 있습니다. 이러한 패치는 개요 탭을 선택한 상태에서 정정 작업 기록의 오른쪽으로 스크롤하는 경우 기본 패치 열에 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

기본 패치가 있는 정정 작업



10. RT 기록에서 패치 예약을 클릭하고 위에 나열된 단계에 따라 대화 상자에서 예약합니다.

11. 옵션: 클래식 환경에서 이전에 진행했던 단계에 대한 패치를 예약할 수 있습니다. 이러한 기록을 찾으려면 다음 단계를 수행합니다.

a. 클래식 환경에서 다음으로 이동합니다. 모두 〉 취약성 대응 〉 패치 〉 모두.

b. 표시되는 목록에서 패치 업데이트 기록을 찾습니다.

c. 정정 작업의 경우 다음으로 이동하십시오. 취약성 대응 〉 정정 작업 을 클릭하고 기록을 찾습니다. 정정 상태 탭에서 정정 상태를 추적합니다. 기록 하단에 패치 데이터가 관련 링크에 표시됩니다.

d. 패치 예약을 클릭하고 필드를 채웁니다.

필드	설명
배포 이름	이 패치 배포의 이름을 입력합니다. 이 이름은 업데이트를 추적하는 데 도움이 됩니다.
설명	패치에 대한 텍스트를 더 추가합니다. 이 정보는 패치 업데이트 기록의 설명 필드에 표시됩니다.
배포 유형	목록에서 하나의 옵션을 선택합니다. ▪ 필수 - 이 패치는 필수 업데이트입니다. ▪ 사용 가능 - 이 패치는 필수는 아니지만 배포에 사용할 수 있습니다.
컬렉션	목록에서 컬렉션(자산 그룹)을 선택하여 계속합니다. 이러한 그룹은 SCCM에서 임포트한 자산 컬렉션입니다.
배포 시간 기준	목록에서 배포 시간 창의 기준이 될 시간대를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
사용 가능한 시간	패치를 처음 배포할 수 있게 되는 시간 값을 설정합니다.
기한	기한을 설정합니다. 이 값은 패치를 설치할 수 있는 마지막 날을 나타냅니다.

e. 배포를 클릭합니다.

SCCM 취약성 대응 이 있는 Microsoft 패치 오케스트레이션에 대한 REST 메시지

SCCM을 사용한 Microsoft 취약성 대응 패치 오케스트레이션은 SCCM WMI(Windows Management Instrumentation) 클래스를 사용하여 SCCM 서버 API를 호출합니다.

REST 메시지 개요

SMS 공급자 는 관리 서비스라고 하는 HTTPS를 통해 API에 상호 운용성 액세스를 제공합니다. 관리 서비스는 Open Data(OData) v4 프로토콜을 기반으로 하는 REST(Representational State Transfer) API입니다.

이 통합에서 사용되는 관리 서비스에 대한 자세한 내용은 Configuration Manager의 관리 서비스 항목을 참조하십시오.

필요한 인증은 Windows New Technology LAN Manager NTLM 프로토콜을 사용하므로 API에 대한 호출은 PowerShell 스크립트를 사용하여 MID Server를 통해 이루어집니다.

Microsoft SCCM 통합

SCCM 통합에 대한 Microsoft REST 메시지를 사용하여 SCCM에서 Microsoft 정보를 검색할 수 있습니다. REST 메시지의 기록 방법이 변경되면 정보를 검색하기 위해 SCCM에 Microsoft 대한 요청에 영향을 미칩니다. REST 메시지에는 다음과 같은 REST 메서드가 포함됩니다.

WMI 클래스 이름:

- SMS_Collection
- SMS_DeploymentSummary

매개변수 이름	값	설명
URL	사용자에 기반한 동적 값	SCCM 콘솔의 엔드포인트를 나타냅니다.

Microsoft SCCM 배포 패치

Microsoft SCCM 통합에 대한 REST 메시지를 사용하여 SCCM ServiceNow AI Platform# 으로의 패치 일정을 예약할 수 있습니다 Microsoft . REST 메시지의 기록 방법이 변경되면 정보를 검색하기 위해 SCCM에 대한 요청에 영향을 미칩니다. REST 메시지에는 다음과 같은 REST 메서드가 포함됩니다.

REST 메서드	설명
POST 배포 패치	단일/여러 컴퓨터의 SCCM 콘솔에 패치를 예약합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

매개변수 이름	값	설명
URL	사용자에 기반한 동적 값	SCCM 콘솔의 엔드포인트를 나타냅니다.
직위	사용자에 기반한 동적 값	배포의 제목입니다.
settings_tag	값이 있는 XML 태그 이름 지정 설정	매개변수가 다르고 패치를 예약하는 동안 SCCM으로 전송되는 설정을 나타냅니다.
computer_tag	값이 있는 XML 태그 이름의 컴퓨터	패치가 예약될 컴퓨터 목록을 나타냅니다.
site_name	패치 업데이트 값	패치가 있는 사이트의 이름입니다.
Patch_id	패치 업데이트 값	패치의 ID입니다.

SCCM 통합을 사용한 **Microsoft** 패치 오케스트레이션을 위한 데이터 변환

데이터는 SCCM 통합을 통해 Microsoft 패치 오케스트레이션에서 검색되고 일련의 데이터 소스를 통해 처리되고 인스턴스에서 변환됩니다 ServiceNow AI Platform# .

SCCM 컬렉션 임포트

임포트한 컬렉션의 데이터가 SCCM 컬렉션 임포트 [sn_vul_sccm_collection_import] 테이블로 로드됩니다. SCCM 컬렉션(변환 맵)은 임포트한 정보를 변환하는 데 사용됩니다.

주:
이 변환 맵을 변경하면 SCCM 컬렉션 임포트의 데이터 처리 방법이 변경됩니다.

이 변환 맵에 액세스하려면 다음으로 이동하십시오. 모두 〉 시스템 임포트 세트 〉 변환 맵 을 클릭하고 SCCM 컬렉션 변환을 찾습니다. 다음 표에는 통합별 변환 맵 필드가 나열되어 있습니다.

소스 필드	대상 필드	설명
u_collectionid	source_id	컬렉션의 고유 ID입니다.
u_name	이름	수집의 이름입니다.
u_membercount	device_count	이 컬렉션의 장치 수입니다.
〔스크립트〕	integration_instance	패치를 임포트하는 인스턴스의 이름입니다.

SCCM 컬렉션 임포트 변환 맵 스크립트 타이밍

스크립트	설명
OnStart(임포트 세트에서 변환을 생성한 경우)	통합 프로세스에 대한 범위 변수 〔sn_vul_sccm〕의 값을 초기화하는 데 사용되는 스크립트입니다. 이 스크립트는 내부용이며 수정하거나 삭제하면 안 됩니다.
onBefore(임포트 세트가 변환을 완료하기 전)	범위 변수 〔sn_vul_sccm〕의 값을 업데이트하는 데 사용되는 스크립트입니다. 이 스크립트는 내부용이며 수정하거나 삭제하면 안 됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

SCCM 컬렉션 임포트 변환 맵 스크립트 타이밍

스크립트	설명
onComplete(임포트 세트가 변환을 완료한 경우)	생성, 업데이트 및 무시되는 항목 수를 설정하는 데 사용되는 스크립트입니다. 이 스크립트는 내부용이며 수정하거나 삭제하면 안 됩니다.

SCCM 패치 업데이트 임포트

임포트한 패치의 데이터가 SCCM 패치 업데이트 임포트 [sn_vul_sccm_patch_update_import] 테이블에 로드됩니다.

SCCM 패치 업데이트 변환은 임포트한 정보를 변환하는 데 사용됩니다.

주:
이 변환 맵을 변경하면 SCCM 패치 업데이트 임포트의 데이터가 처리되는 방식이 변경됩니다.

이 변환 맵에 액세스하려면 다음으로 이동하십시오. 모두 〉 시스템 임포트 세트 〉 변환 맵 를 클릭하고 SCCM 패치 업데이트 변환을 찾습니다.

다음 표에는 통합별 변환 맵 필드가 나열되어 있습니다.

SCCM 패치 업데이트 임포트 변환 맵 필드

소스 필드	대상 필드	설명
〔스크립트〕	URL	패치의 URL입니다.
u_nummissing	num_missing	이 패치가 누락된 장치 수입니다.
〔스크립트〕	date_release	패치 릴리스 날짜입니다.
u_bulletinid	bulletin_id	패치의 공지 ID입니다.
u_numtotal	num_total	총 장치 수입니다.
u_localizeddescription	설명	패치에 대한 설명입니다.
〔스크립트〕	is_highest_supersedence	대체 가능성이 가장 높은 패치입니다.
u_numnotapplicable	num_not_applicable	이 패치에 적용되지 않는 장치 수입니다.
u_iscontentprovisioned	is_downloaded	패치가 SCCM 서버에 다운로드된 경우
u_numunknown	num_unknown	알 수 없는 장치의 총 수입니다.
u_articleid	article_id	패치의 문서 ID입니다.
u_localizeddisplayname	직위	패치의 제목입니다.
u_ci_id	source_id	SCCM의 패치에 대한 고유 ID입니다.
u_numpresent	num_present	패치가 설치된 장치 수입니다.
〔스크립트〕	integration_instance	패치를 임포트하는 인스턴스의 이름입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

SCCM 패치 업데이트 임포트 변환 맵 필드

소스 필드	대상 필드	설명
〔스크립트〕	sn_vul_solution	소스 ID를 기반으로 하는 솔루션입니다.
〔스크립트〕	last_modified	마지막으로 수정한 패치 날짜입니다.
u_severity	source_severity	패치의 심각도입니다.

SCCM 패치 업데이트 임포트 변환 맵 스크립트 타이밍

스크립트	설명
OnStart(임포트 세트에서 변환을 생성한 경우)	통합 프로세스의 범위 변수 〔sn_vul_sccm〕의 값을 초기화하는 데 사용되는 스크립트입니다. 이 스크립트는 내부용이며 수정하거나 삭제하면 안 됩니다.
onBefore(임포트 세트가 변환을 완료하기 전)	범위 변수 〔sn_vul_sccm〕의 값을 업데이트하는 데 사용되는 스크립트입니다. 이 스크립트는 내부용이며 수정하거나 삭제하면 안 됩니다.
onComplete(임포트 세트가 변환을 완료한 경우)	생성, 업데이트 및 무시되는 항목 수를 설정하는 데 사용되는 스크립트입니다. 이 스크립트는 내부용이며 수정하거나 삭제하면 안 됩니다.

SCCM 장치 패치 업데이트 임포트

장치에서 임포트한 관련 패치의 데이터는 SCCM 장치 패치 업데이트 임포트 [sn_vul_sccm_device_patch_import] 테이블로 로드됩니다.

SCCM 장치 패치 업데이트 변환은 임포트한 정보를 변환하는 데 사용됩니다.

주:
이 변환 맵을 변경하면 SCCM 장치 패치 업데이트 임포트의 데이터가 처리되는 방식이 변경됩니다.

이 변환 맵에 액세스하려면 다음으로 이동하십시오. 모두 〉 시스템 임포트 세트 〉 변환 맵 를 클릭하고 SCCM 장치 패치 업데이트 변환을 찾습니다.

다음 표에는 통합별 변환 맵 필드가 나열되어 있습니다.

SCCM 장치 패치 업데이트 변환 맵 스크립트 타이밍

스크립트	설명
OnStart(임포트 세트에서 변환을 생성한 경우)	통합 프로세스의 범위 변수 〔sn_vul_sccm〕의 값을 초기화하는 데 사용되는 스크립트입니다. 이 스크립트는 내부용이며 수정하거나 삭제하면 안 됩니다.
onBefore(임포트 세트가 변환을 완료하기 전)	CI 조회 규칙 및 패치뿐 아니라 이들 간의 관계를 기반으로 CI를 만들고 업데이트하는 데 사용되는 스크립트입니다. 결과에 따라 이 스크립트는

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

SCCM 장치 패치 업데이트 변환 맵 스크립트 타이밍

스크립트	설명
	범위 변수 〔sn_vul_sccm〕의 값을 수정합니다. 이 스크립트는 내부용이며 수정하거나 삭제하면 안 됩니다.
onComplete(임포트 세트가 변환을 완료한 경우)	생성, 업데이트 및 무시되는 항목 수를 설정하는 데 사용되는 스크립트입니다. 이 스크립트는 내부용이며 수정하거나 삭제하면 안 됩니다.

SCCM 장치 컬렉션 임포트

임포트한 장치 컬렉션의 데이터는 SCCM 장치 컬렉션 임포트 [sn_vul_sccm_device_collection_import] 테이블로 로드됩니다.

SCCM 장치 컬렉션 임포트 변환은 임포트한 정보를 변환하는 데 사용됩니다.

주:
이 변환 맵을 변경하면 SCCM 장치 컬렉션 임포트의 데이터가 처리되는 방식이 변경됩니다.

이 변환 맵에 액세스하려면 다음으로 이동하십시오. 모두 〉 시스템 임포트 세트 〉 변환 맵 를 클릭하고 SCCM 장치 컬렉션 변환을 찾습니다.

다음 표에는 통합별 변환 맵 필드가 나열되어 있습니다.

장치 컬렉션 임포트 변환 맵 스크립트 타이밍

스크립트	설명
OnStart(임포트 세트에서 변환을 생성한 경우)	통합 프로세스의 범위 변수 〔sn_vul_sccm〕의 값을 초기화하는 데 사용되는 스크립트입니다. 이 스크립트는 내부용이며 수정하거나 삭제하면 안 됩니다.
onBefore(임포트 세트가 변환을 완료하기 전)	CI 조회 규칙 및 컬렉션뿐 아니라 이들 간의 관계를 기반으로 CI를 만들고 업데이트하는 데 사용되는 스크립트입니다. 결과에 따라 이 스크립트는 범위 변수 〔sn_vul_sccm〕의 값을 수정합니다. 이 스크립트는 내부용이며 수정하거나 삭제하면 안 됩니다.
onComplete(임포트 세트가 변환을 완료한 경우)	생성, 업데이트 및 무시되는 항목 수를 설정하는 데 사용되는 스크립트입니다. 이 스크립트는 내부용이며 수정하거나 삭제하면 안 됩니다.

SCCM 장치 컬렉션 임포트 변환 맵 필드

소스 필드	대상 필드	설명
u_id	source_id	작업의 고유 ID입니다.
U_name	이름	작업의 이름
〔스크립트〕	Sn_vul_sccm_discovered_item	패치가 배포되어 검색된 항목의 참조

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

SCCM 장치 컬렉션 임포트 변환 맵 필드

소스 필드	대상 필드	설명
U_status	상태	작업 상태
〔스크립트〕	Sn_vul_patch_orch_update	패치의 참조
U_apply_count	Count_success	작업의 성공 카운트입니다.
U_retry_count	재시도	작업의 재시도 횟수입니다.
〔스크립트〕	Deployment_time	작업의 시작 시간입니다.
〔스크립트〕	마감	작업의 종료 시간입니다.
〔스크립트〕	Source_created	작업을 생성한 시간입니다.
〔스크립트〕	Integration_instance	작업을 임포트하는 인스턴스의 이름입니다.

SCCM 배포 임포트

임포트한 배치의 데이터가 SCCM 배포 임포트 [sn_vul_sccm_deployment_import] 테이블로 로드됩니다.

SCCM 배포 임포트 변환은 임포트한 정보를 변환하는 데 사용됩니다.

주:
이 변환 맵을 변경하면 SCCM 배포 임포트의 데이터가 처리되는 방법이 변경됩니다.

이 변환 맵에 액세스하려면 다음으로 이동하십시오. 모두 〉 시스템 임포트 세트 〉 변환 맵 를 클릭하고 SCCM 배포 변환을 찾습니다.

SCCM 배포 변환 맵 필드

소스 필드	대상 필드	설명
u_id	source_id	배치의 고유 ID입니다.
u_name	이름	배포의 이름입니다.
〔스크립트〕	마감	배포의 마감 시간입니다.
u_numberinprogress	count_progress	배포에 대해 진행 중인 장치 수입니다.
〔스크립트〕	deployment_time	배포 시작 시간입니다.
〔스크립트〕	integration_instance	배포를 임포트하는 인스턴스의 이름입니다.
〔스크립트〕	source_created	배포의 생성 시간입니다.
〔스크립트〕	sn_vul_patch_orch_update	패치 참조
〔스크립트〕	sn_vul_patch_orch_collection	패치가 배포되는 검색된 항목의 참조입니다.
u_softwarename	이름	배포의 이름입니다.
u_numberother	count_other	배치에 대한 다른 장치 수입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

SCCM 배포 변환 맵 필드

소스 필드	대상 필드	설명
u_numberunknown	count_unknown	알 수 없는 상태의 배포 장치 수입니다.
u_deploymentid	source_id	배포의 고유 식별자입니다.
u_numbersuccess	count_success	배포에 대한 장치의 성공 수입니다.
u_numbererrors	count_error	배치에 대한 장치 오류 수입니다.
u_numbertargeted	count_total	배포에 대한 총 장치 수입니다.

SCCM 배포 임포트 변환 맵 스크립트 타이밍

스크립트	설명
OnStart(임포트 세트에서 변환을 생성한 경우)	통합 프로세스의 범위 변수 〔sn_vul_sccm〕의 값을 초기화하는 데 사용되는 스크립트입니다. 이 스크립트는 내부용이며 수정하거나 삭제하면 안 됩니다.
onBefore(임포트 세트가 변환을 완료하기 전)	범위 변수 〔sn_vul_sccm〕의 값을 업데이트하는 데 사용되는 스크립트입니다. 이 스크립트는 내부용이며 수정하거나 삭제하면 안 됩니다.
onComplete(임포트 세트가 변환을 완료한 경우)	생성, 업데이트 및 무시되는 항목 수를 설정하는 데 사용되는 스크립트입니다. 이 스크립트는 내부용이며 수정하거나 삭제하면 안 됩니다.

SCCM 취약성 대응 과의 **Microsoft** 패치 오케스트레이션 통합을 위한 예시 워크플로우

SCCM에서 Microsoft 패치 오케스트레이션이 작동하는 방식의 예입니다.

시작하기 전에

예를 들어 전체 환경이 3주에 한 번씩 패치된다고 가정해 보겠습니다. 가장 최근의 패치 적용 기간이 일주일 전에 완료되었지만 최근에 알려진 중요한 취약점을 수정하기 위해 패치를 적용하려고 합니다. 이 취약성의 중요한 특성으로 인해 예정된 다음 패치를 위해 2주를 더 기다릴 수 없습니다.

필요한 역할:

- 취약성 관리자 작업 공간의 sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin
- sn_vul.remediation_owner - IT 정정 소유자 작업 공간을 볼 수 있습니다.
- sn_vul_patch_orch.configure_patch 역할을 구성하여 패치를 구성하고 예약합니다.
- sn_vul_patch_orch.read_patch - 기록에 대한 패치 정보를 (읽기 전용) 볼 수 있습니다. 이 역할은 IT 정정 및 취약성 관리자 작업 공간에 필요한 sn_vul.remediation_owner 및 sn_vuln.vulnerability_analyst 역할로 상속됩니다.

이 태스크 정보

취약성 관리자 작업 공간에서 작업하는 취약성 관리자 또는 분석가는 중요 취약성이 있는 임포트된 VI를 캡처하는 데 도움이 되도록 감시 주제를 생성하거나 기존 감시 주제를 편집하는 것을 고려할 수 있습니다. 패치 오케스트레이션 통합을 사용하면 이러한 취약성을 수정하고 추적하는 데 사용할 패치를 확인할 수도 있습니다. 다음 표에는 패치 오케스트레이션에 대한 주시 주제에 대해 설정할

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

수 있는 조건이 포함된 몇 가지 샘플이 나와 있습니다. 이러한 예제를 사용하면 환경에 가장 적합한 설정을 결정하는 데 도움이 됩니다. 감시 항목 설정에 대한 자세한 정보는 을 참조하십시오 에서 주시 주제 생성 취약성 관리자 작업 공간 .

취약성 관리자 작업 공간의 패치 오케스트레이션에 대한 샘플 주시 주제

주시 주제 이름	설명
패치 유출이 있는 치명적인 취약성	## ### 1 - ## 그리고 ### ### #### ### #####.
패치 예약됨(SLA 누락)이 있는 위험한 취약성	## ## ## ###(## ## ##)
패치가 예약된 위험한 취약성	## ### 1 - ## 그리고 ## ## ### ## ## ####. 그리고 ### ## ### ##### #####.

- 취약성 관리자 또는 분석가는 감시 주제 및 정정 작업을 생성한 후 정정 작업을 생성합니다. VI 기록 및 정정 작업에서 탐지 탭으로 드릴다운하고 SCCM 제품에서 임포트한 자산과 함께 추적 중인 취약성이 있는 검색된 항목 기록을 찾을 수 있습니다.
- 취약성 분석가 또는 관리자는 취약성과 연관된 패치 데이터를 모니터링할 수 있습니다. 검색된 항목 기록에서 특정 자산(구성 항목)에 패치 하나 또는 여러 개의 패치를 배포할 수도 있습니다.

IT 정정 전문가는 패치 배포로 취약성을 해결하는 방법에 대한 옵션을 제공합니다.

- 패치 업데이트 기록(VPU#)에서 패치를 예약할 수 있습니다.
- 취약한 항목(VI)에 기본 솔루션이 매핑되어 있고 사용자 또는 그룹에 할당된 경우 이러한 취약한 항목이 있는 정정 작업에서 패치를 예약할 수 있습니다.

프로시저

1. IT 정정 전문가는 IT 정정 작업 공간에서 홈 뷰를 클릭합니다.
2. 홈 뷰에서 할당된 정정 작업 성과표를 클릭하여 기록을 봅니다.

   이 예에서는 정정 작업(VUL#)의 간단한 설명 필드에서 중요 취약성과 관련된 텍스트를 확인할 수 있습니다. 예를 들어, 취약성 관리자가 이 중요한 취약성으로 VI(VIT#)를 포착하기 위해 패치 누출이 있는 위험한 취약성이라는 감시 주제를 생성했음을 알 수 있습니다.

   기록이 열린 상태에서 VI, 기본 패치를 검토하고 자신 또는 그룹 구성원이 승인을 위한 패치 요청을 이미 제출했는지 확인할 수도 있습니다.
3. 충분한 정보가 있는 경우 이 정정 작업에서 지금 패치 요청을 제출하는 것이 좋습니다.

   주:
   기록과 연결된 VI에 매핑된 패치가 없는 경우 기록에서 패치 일정 예약 버튼을 사용할 수 없습니다.
4. 패치 예약을 클릭하고 대화 상자의 필드를 입력합니다.
   패치를 예약하는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 와 SCCM의 Microsoft 통합으로 패치 예약 취약성 대응.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. 또는 IT 정정 작업 공간의 목록 뷰에서 정정 작업, 취약한 항목, 솔루션 및 패치 링크를 클릭하여 이러한 기록을 볼 수 있습니다.
이 예제의 경우 주시 주제 이름 대신 패치의 문서 ID 또는 공지 ID 및 제목을 알 수 있습니다. 그렇다면 이 취약성이 있는 VI가 사용자 또는 그룹에 할당되었는지 확인할 수 있습니다. 패치 업데이트 기록에서 패치 요청을 제출할 수 있습니다. VI 기록에서 잠재적인 패치를 확인하고 패치 요청을 제출하려는 경우 관련 정정 작업을 열 수 있습니다.
6. 작업 영역에 액세스할 수 없거나 클래식 환경에서 데이터를 보고 패치를 예약하려는 경우 다음 단계를 수행합니다.

   a. 다음으로 이동 취약성 대응 〉 패치 〉 모두.

   b. 원하는 패치 업데이트 기록을 찾습니다.
   ## 위험 점수로 기록을 필터링하는 것이 좋습니다.

   c. 정정 상태 탭에서 연결된 VI 및 정정된 VI 비율(%) 필드를 검토합니다.
   VI에 사용 가능한 패치가 있는 경우 기록의 오른쪽 상단에 패치 예약 버튼이 표시됩니다.

   d. 요청을 제출하려면 패치 예약을 클릭합니다.
   패치를 예약하는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 와 SCCM의 Microsoft 통합으로 패치 예약 취약성 대응.

   e. 또는 패치 ID 정보가 없지만 그룹에 할당된 정정 작업의 간단한 설명 필드에 중요 취약성과 관련된 텍스트가 있는지 확인할 수 있습니다.

   f. 다음으로 이동 취약성 대응 〉 정정 작업 〉 사용자 그룹에 할당됨.

   g. 원하는 기록을 찾아 클릭하여 엽니다.
   오픈 기록에서 정정 상태 탭에서 VI 및 정정된 VI 비율(%)을 검토합니다. VI 기록, 기본 솔루션, 기본 패치 및 패치 요청에 대한 관련 링크를 클릭합니다.

      주:
      기록과 연결된 VI에 매핑된 패치가 없는 경우 기록에서 패치 일정 예약 버튼을 사용할 수 없습니다.

   h. 패치 요청을 제출하려면 기록에서 패치 예약을 클릭합니다.

Qualys Vulnerability Integration 이해

Qualys 제품 센서는 데이터를 수집하여 자동으로 애플리케이션에 전송 Qualys 하여 정보를 지속적으로 분석하고 상관 관계를 지정합니다. 이는 취약성을 취약성 대응 CI 및 비즈니스 서비스에 매핑하여 잠재적으로 악의적인 위협의 영향과 우선순위를 결정하기 위해 AS 와 Qualys Vulnerability Integration 쉽게 통합됩니다.

Qualys Vulnerability Integration 다음을 사용하여 구성 취약성 〉 관리 〉 설정 도우미 데이터 검색을 보다 유연하고 확장 가능하게 만듭니다.

애플리케이션 배포가 Qualys Cloud Platform 여러 개 있는 경우 각 배포에 대한 통합을 추가할 수 있습니다. 여러 외부 공급업체 배포 및 해당 취약성으로 식별된 자산이 CMDB와 통합되고 조정됩니다. 이러한 통합은 여러 배포 간에 스캔 프로세스가 겹치는 경우에도 발생합니다. 각 배포에서 소싱된 데이터가 식별되고 의 단일 인스턴스에서 취약성 대응사용할 수 있습니다. Qualys Vulnerability Integration 지식베이스 기록은 배포 전반에 걸쳐 정규화되어 배포 전반에 걸쳐 동일한 취약성의 인스턴스가 동일한 취약성으로 처리되도록 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
원래 취약성 통합을 삭제할 수는 없지만 사용하지 않도록 설정할 수는 있습니다. 비활성화된 템플릿에서 만든 통합은 기본적으로 비활성화됩니다.

각 통합 기록에 대해 구성된 실행 사용자가 있습니다. 이 사용자의 기본값은 VR입니다. 시스템. 이 값은 변경하지 마십시오.

주:
어플라이언스 Qualys Vulnerability Integration 목록, 자산 그룹, 동적 검색 목록 및 정적 검색 목록에 대한 통합을 생성하지만 정상 작동에는 필요하지 않습니다.

사용 가능한 버전

의 릴리스 버전 Yokohama	릴리스 정보
Qualys Vulnerability Integration v12.7, v12.8	호환성 정보는 KB0856498 Vulnerability Response 호환성 매트릭스 및 릴리스 스키마 변경을 참조하십시오.

설치된 구성요소

통합과 함께 설치되는 역할, 통합 작업 및 테이블의 현재 목록과 인스턴스에 현재 설치된 항목을 보는 방법에 대한 지침 링크는 문서를 앱과 함께 설치되는 구성요소 Qualys Vulnerability Integration참조하십시오.

기본 및 지원 통합

Qualys 기본 및 지원 통합은 Qualys 취약성 통합에서 데이터를 검색하여 인스턴스의 취약성 데이터를 보강합니다. 일련의 예약된 작업이 통합을 자동으로 호출합니다. 수동으로 실행할 수도 있습니다. 예약된 작업은 인스턴스를 다른 취약성 관리 시스템과 동기화된 상태로 유지하여 취약성 정정 수명주기를 단순화합니다. 기본 및 지원 통합을 수정할 수 있습니다.

Qualys 통합은 예약된 작업으로 실행됩니다. 각 통합 기록에 대해 구성된 실행 사용자가 있습니다. 이 사용자의 기본값은 VR입니다. 시스템. 이 값은 변경하면 안 됩니다.

주:
유효한 실행 사용자를 설정하지 못하면 통합이 실행될 때마다 데이터 소스 기록에 여러 개의 데이터 검색 첨부 파일이 중복되는 경우가 많습니다. 데이터 소스에 첨부 파일이 여러 개 있으면 처리 시간이 늘어나 일관되지 않은 변환 결과가 발생합니다.

임포트하는 동안 아직 존재하지 않는 CVE 기록이 NVD 기록으로 생성되고 기본적으로 외부 공급업체 항목 Qualys 에서 참조됩니다.

가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

기본 통합

기본 통합은 일정에 따라 호출된 API와 Qualys 상호작용하기 Qualys Cloud Platform 위한 엔트리포인트입니다.

다음으로 이동하여 기본 통합을 봅니다. **Qualys** 취약성 통합 〉 관리 〉 기본 통합.

지원 통합

지원 통합은 일정에 따라 또는 기본 통합의 호출 없이 실행되지 않는 프로세스입니다.

다음으로 이동하여 지원 통합을 보려면 **Qualys** 취약성 통합 〉 관리 〉 지원 통합.

용 서비스 그래프 커넥터 **Qualys**

버전 2.2부터 에서 서비스 그래프 커넥터를 Qualys 사용할 수 있습니다 ServiceNow# Store. 자세한 내용은 Service Graph Connector for Qualys 문서를 참조하십시오.

Qualys 데이터 소스 필드의 데이터는 전역 자산 API와 자산 관리 및 태깅 API를 사용하여 임포트됩니다.

전역 자산 API:

- CSAM 라이센스가 필요합니다.
- 자산 정보에는 하드웨어 범주 및 OS 범주와 같은 상세 정보가 포함됩니다.

자산 관리 및 태깅 API:

- CSAM 라이센스는 필요하지 않습니다.
- 자산 정보에는 하드웨어 범주 및 OS 범주에 대한 상세 정보가 포함되지 않습니다.

자세한 내용은 Service Graph Connector for Qualys APIs 문서를 참조하십시오.

.

IRE(식별 및 조정 엔진)를 사용하여 **CI** 생성

기존 CI를 외부 공급업체 스캐너에서 임포트한 호스트와 일치시킬 수 없는 경우 식별 및 조정 엔진을 사용하여 새 CI를 만들 수 있습니다. CMDB CI Class Models 플러그인을 활성화하여 새 클래스를 사용하여 CI를 생성합니다. 그렇지 않으면 일치하지 않는 CI가 일치하지 않는 CI 클래스에 생성됩니다. 자세한 내용은 식별 및 조정 엔진을 사용하기 위한 취약성 대응 CI 생성 문서를 참조하십시오. 일치하지 않는 클라우드 자원의 분류를 기본 CI 클래스로 구성하는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 일치하지 않는 클라우드 자산에 대한 CI 클래스 업데이트 중.

검색 목록

검색 목록은 취약성의 사용자 지정 그룹을 만드는 데 사용됩니다 Qualys . 이를 저장하여 티켓 생성에 사용하고 취약성 검사 및 보고서를 사용자 지정할 수 있습니다. 검색 목록 모듈을 사용하면 일정에 따라 Qualys에서 인스턴스로 검색 목록 데이터를 다운로드할 수 있습니다.

동적 검색 목록 임포트 및/또는 정적 검색 목록 임포트 데이터 변환 맵을 사용하여 검색 목록을 가져옵니다Qualys. 이러한 각 변환에서 임포트 수행 일정을 정의할 수 있습니다.

옵션 프로파일

옵션 프로파일은 스캔 설정에서 사용할 수 Qualys 있습니다. 옵션 프로파일은 에서 ServiceNow AI Platform스캔을 시작할 때 필요합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵션 프로파일은 Qualys 옵션 프로파일 목록 통합을 통해 제품에서 임포트됩니다. 옵션 프로파일과 연결된 검색 목록을 확인할 수 있도록 검색 목록 통합, Qualys 동적 검색 목록 및 Qualys 정적 검색 목록 통합에서 임포트한 후 옵션 프로파일 목록 통합을 실행하는 것을 선호할 수 있습니다.

자산 그룹

자산 그룹은 플랫폼에서 설정됩니다 Qualys . 자산 그룹은 에서 스캔이 시작될 ServiceNow AI Platform때 일치하는 IP 주소를 스캔하는 데 사용되는 스캐너 장치를 식별합니다.

연결된 장치가 있는 자산 그룹은 자산 그룹 목록 통합을 통해 끌어옵니다 Qualys .

자산 그룹을 임포트한 후 장치 목록 통합을 시작하여 의 기본 애플리케이션 기록ServiceNow AI Platform에서 Qualys 장치 이름 및 장치 상태 필드를 채우십시오.

호스트 태그

호스트 목록 통합의 Qualys 일부로 모든 호스트 태그가 임포트됩니다. 호스트 태그는 할당 및 정정 작업 규칙의 필터링에 취약성 대응 주로 사용됩니다. 검색된 항목 양식에 표시됩니다.

> **주:**
> 호스트 목록 통합은 Qualys 할당 또는 정정 작업 규칙을 취약성 대응 생성하기 전에 실행되어야 모든 태그가 규칙에 포함될 수 있고 취약한 항목을 임포트 및 그룹화할 수 있습니다.

- 태그 스토리지는 대/소문자를 구분하지 않습니다. **San Diego** 태그가 생성되면 호스트 태그 테이블에 **SAN DIEGO** 태그를 저장할 수 없습니다. 'San Diego'와 'SAN DIEGO'는 동일한 호스트 태그로 간주됩니다. 먼저 가져온 태그가 우선합니다.
- 정정 작업 규칙에서 호스트 태그를 그룹 키로 사용하면 예기치 않은 결과가 발생할 수 있습니다. 호스트 태그는 조건 작성기에서만 사용할 수 있습니다.
- 호스트 태그는 전역 시스템 속성 sn_vul.import_host_tags에 의해 제어됩니다. 이 속성은 기본적으로 true로 설정됩니다. 태그를 끄면 모든 인스턴스에서 태그가 꺼집니다.

호스트 태그(자산 태그라고도 함)는 조직의 자산을 구성하고 추적하는 데 사용됩니다. 호스트 자산에 태그를 할당할 수 있습니다. 그런 다음 검사를 시작할 때 검사할 호스트와 연결된 태그를 선택할 수 있습니다. 호스트 태그 모듈을 사용하면 일정에 따라 호스트 태그 데이터를 Qualys 인스턴스에서 인스턴스로 다운로드할 수 있습니다.

스캔으로 종결되지 않은 해결된 취약한 항목 다시 열기

인스턴스에서 "해결됨" ServiceNow AI Platform 으로 설정되었지만 외부 공급업체 통합 실행에 의해 "종결/수정됨"으로 전환되지 않은 취약한 항목은 재스캔 중에 탐지되면 다시 열립니다.

탐지의 경우 Qualys , 스캐너가 '해결됨'으로 설정되었지만 후속 스캔에서 '종결/수정됨'으로 전환되지 않은 VI를 계속 찾으면 마지막으로 발견된 날짜가 해결 날짜보다 나중일 때 이러한 VI가 다시 '오픈'으로 이동합니다.

데이터 검색 제한 사항

기본적으로 에서 데이터를 검색하는 Qualys방법에는 제한이 없습니다. 많은 기록이 고객이 취약성 대응 프로세스를 사용하여 정정하지 않으려는 낮은 심각도 취약성과 관련될 수 있습니다. 해당 REST 메시지/메서드 매개변수를 업데이트하면 이 동작을 수정할 수 있습니다.

이 업데이트를 담당하는 REST 메시지/메서드는 **Qualys** 호스트 탐지 – 표준/게시입니다. 값을 업데이트하려면 다음 값을 사용하여 post 메서드에 새 HTTP 쿼리 매개변수를 추가합니다.

- 이름: severities
- 값: 3-5(또는 원하는 적절한 심각도)

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

스토어에서 앱 요청

ServiceNow Store 웹 사이트를 방문하면 사용 가능한 모든 앱을 확인하고 스토어에 요청을 제출하는 방법에 대한 정보를 참조할 수 있습니다. 출시된 모든 앱의 누적 릴리스 정보는 ServiceNow Store 버전 기록 릴리스 정보를 참조하십시오.

관련 정보

Qualys REST 메시지

준비 중 **Qualys Vulnerability Integration**

성공적인 통합을 위해서는 통합 전 작업을 계획하고 신중하게 실행해야 합니다. 이러한 절차를 수행하여 통합을 준비해야 합니다. 사용자는 Qualys Vulnerability Integration 사용자 환경에서 Qualys 클라우드 플랫폼 스캔을 숙지하고 실행한다고 가정합니다.

주:
통합을 실행하기 전에 요구 사항에 따라 필요한 구성을 변경합니다.

중요한 필수 구성 요소

임포트하려는 취약한 항목 수에 따라 인스턴스 크기를 조정하십시오. 인스턴스 크기가 작으면 로드 시간이 길어질 수 있습니다. 인스턴스 크기를 모르는 경우 에 문의하십시오 고객 서비스 및 지원.

필터링을 사용하여 초기 임포트에 대한 항목 수를 제한하고 후속 임포트에서 필터를 조정하여 배포를 단계적으로 수행합니다.

스캐너는 Qualys 애플리케이션에서 기본적으로 비활성화되어 있습니다 취약성 대응 . 이러한 애플리케이션을 소스로 사용하는 취약한 항목 또는 정정 작업에서 다시 검색을 수행하려고 하면 다시 검색 버튼을 사용할 수 없습니다.

수행할 작업

- 호스트 탐지 목록 임포트 통합의 초기 시작 날짜를 결정합니다.

  시작 시간 필드를 몇 시간 또는 며칠 전으로 설정하는 것이 좋습니다. 이상적으로는 마지막 Qualys 검사 날짜를 선택하는 것이 좋습니다. 시작 날짜에는 취약성 관리 솔루션을 사용하기 전에 검색된 취약성이 포함될 수 있습니다. 스캔 주기를 시작하는 데 사용되는 가장 빠른 시작 시간을 설정합니다. 따라서 모든 호스트를 스캔하는 데 일주일이 걸리는 경우 이 값을 그 시간 1주 전으로 설정합니다.

- admin, sn_vuln.admin 및 sn_vul_qualys.admin 역할에 사용자를 추가합니다. 자세한 내용은 사용자에게 역할 할당을 참조하십시오.

- 각 통합 기록에 대해 구성된 실행 사용자가 있습니다. 이 사용자의 기본값은 VR입니다. 시스템. 이 값은 변경하지 마십시오.

- 정의한 다른 모든 것 외에 취약성 계산기를 사용하지 않는 경우. 사용하지 않는 경우 기본 취약성 계산기 사용 안 함 취약성 계산기는 취약한 항목 기록이 생성되거나 업데이트될 때마다 실행되며 초기 임포트 성능에 영향을 줄 수 있습니다.
- 기록을 처음 임포트하는 동안 특정 알림 관련 비즈니스 규칙으로 인해 많은 알림이 생성되어 성능에 영향을 줄 수 있습니다. 초기 임포트에 앞서 비즈니스 규칙을 비활성화합니다.
- Qualys 기본값이 아닌 다른 스캐너를 사용하려면 스캐너 장치 설정을 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- Qualys 서버 URL 및 인증 자격 증명을 준비합니다. 자격 증명은 Qualys 구독에 대한 지식, 검사 및 탐지 정보를 검색할 수 있는 적절한 권한을 제공해야 합니다.
- 할당 또는 정정 작업 규칙에서 취약성 대응 호스트 태그를 사용할 계획이라면 규칙을 작성하기 전에 호스트 목록 통합을 실행했는지 확인하십시오 Qualys .

Qualys Vulnerability Integration 설치

인스턴스에서 실행하기 Qualys Vulnerability Integration 전에 먼저 애플리케이션을 설치하고 구성해야 Qualys Vulnerability Integration 합니다. 이 애플리케이션은 별도의 구독으로 사용할 수 있습니다.

시작하기 전에
설치하기 전에 다음 설정 검사 목록을 완료합니다. 이러한 설정 작업은 원활한 설치 및 구성을 위해 필요합니다.

주:
이 프로세스는 프로덕션 인스턴스에 다운로드된 애플리케이션에만 적용됩니다. 애플리케이션을 비프로덕션 또는 개발 인스턴스에 다운로드하는 경우에는 권리를 얻을 필요가 없습니다. 로 애플리케이션 활성화 ServiceNow Store계속 진행합니다.

필요한 역할: 애플리케이션을 다운로드하고 설치하려면 admin

작업 설정	설명
애플리케이션이 설치되고 활성화되었는지 취약성 대응 확인합니다.	활성화되었는지 확인하려면 다음으로 이동하십시오. 구독 관리 〉 구독 인스턴스에 있습니다. 목록에 조직이 구매한 구독이 표시됩니다. 애플리케이션이 설치 및 활성화되지 않은 경우 을 참조하십시오 취약성 대응 설치.
애플리케이션에 대한 Qualys Vulnerability Integration 권리를 가져와 인스턴스에 다운로드합니다 ServiceNow AI Platform# .	애플리케이션이 인스턴스에 아직 다운로드되지 않은 경우 문서를 참조하십시오.
통합을 준비합니다.	준비 중 Qualys Vulnerability Integration 문서를 참조하십시오.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 설정 도우미.

   잠시 후 인스턴스에 설치할 수 있는 애플리케이션이 표시됩니다.

2. 타일을 Qualys Vulnerability Integration 찾아 설치를 클릭합니다.
3. 설정 지원의 지시를 따릅니다.
   설치 도우미를 사용하여 응용 프로그램을 설치하는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 설정 도우미를 사용하여 타사 응용 프로그램 설치 취약성 대응.
4. 설정 도우미에서 통합 구성〉스캐너 통합 으로 이동하여 구성을 계속합니다.
   설정 도우미에서 제공하는 프롬프트를 보완하는 방법에 대한 자세한 내용은 문서를 참조하십시오 Qualys Vulnerability Integration 설정 도우미 사용 구성.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 수행할 작업
스캐너가 기본적으로 애플리케이션에서 비활성 상태이므로 스캐너를 취약성 대응 활성화합니다. 스캐너를 Qualys 활성화하는 방법에 대한 자세한 내용은 을 참조하십시오 스캐너 활성화 Qualys.

스캐너 활성화 **Qualys**

스캐너는 애플리케이션에서 기본적으로 취약성 대응 비활성화되어 있으므로 설치 Qualys Vulnerability Integration 후 스캐너를 활성화해야 합니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin

이 태스크 정보
이러한 애플리케이션을 소스로 포함하는 취약한 항목 또는 정정 작업에서 다시 검색을 수행하려고 하면 다시 검색 버튼을 사용할 수 없습니다.

프로시저
1. 다음으로 이동 모두 〉 취약성 대응 〉 취약성 스캐닝 〉 스캐너.
2. 활성화할 스캐너 제품을 찾고 레코드를 선택하여 엽니다.
3. 활성 확인란을 선택합니다.
4. 업데이트를 선택합니다.
5. 활성화한 제품은 다음 임포트 후 취약한 항목 및 정정 작업 기록의 소스 필드에 표시되며, 다시 스캔은 UI 작업으로 사용할 수 있습니다.

의 네트워크 파티션 식별자로 구성 항목을 업데이트합니다. **Qualys Vulnerability Integration**

IP 주소를 공유하는 환경의 자산에 대한 고유한 CI(구성 항목)를 생성합니다. 환경 전반에서 고유한 자산을 식별하고 기존 검색된 항목, 취약한 항목 및 탐지 레코드의 CI를 자동으로 업데이트하여 취약성에 대한 자세한 정보를 제공합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
기본적으로 취약성 대응 애플리케이션에서 자산을 식별하는 한 가지 방법은 IP 주소를 사용하는 것입니다. 경우에 따라 자산은 IP 주소를 공유할 수 있지만 CMDB에 하나의 CI로 저장됩니다.

예를 들어 다음 표와 같이 환경의 여러 자산(CI)은 IP 주소를 공유할 수 있지만 고유한 네트워크 및 리포지토리 ID를 가질 수 있습니다. 그러나 기본적으로 이러한 자산은 일반적으로 IP 주소 조회 중에 단일 CI (CI 1) 로 식별되고 저장됩니다.

기본 **IP** 조회 및 **CI** 생성

소스	IP 주소	NETWORK_ID	구성 항목
Qualys Vulnerability Integration: 자산과 고정 및 미해결 취약성 통합	123.12.12.141	03712	CI 1
	123.12.12.141	03713	CI 1

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

소스	IP 주소	REPOSITORY_ID	구성 항목
Qualys Vulnerability Integration: 자산과 고정 및 미해결 취약성 통합	123.12.12.141	12	CI 1
	123.12.12.141	13	CI 1

동일한 IP 주소를 가진 자산에 대해 개별 CI를 생성하여 고유한 자산으로 식별할 수 있습니다. 새로운 데이터 임포트를 시작으로 예약된 작업을 실행하여 네트워크 파티션 식별자(network_partition_identifier)를 포함하는 기존 CI *`Update existing discovered items with network partition identifier`*를 보다 세밀하게 업데이트할 수 있습니다.

이 예약된 작업은 기본적으로 비활성화되어 있습니다. 설정 도우미에서 자산 및 고정 및 미해결 취약성 통합 Qualys Vulnerability Integration 에 대해 이 기능을 활성화하여 기록에서 이 식별자를 봅니다.

이 예약된 작업은 활성화되면 임포트한 데이터의 기존 CI 기록에 네트워크 파티션 식별자(network_partition_identifier)를 추가합니다. IRE에서 만든 기존 CI도 업데이트됩니다. 또한 예약된 작업은 다음 임포트로 시작하는 네트워크 파티션 식별자를 포함하는 CI를 생성합니다. 또는 요청 시 작업을 시작하여 기존 데이터를 업데이트할 수 있습니다.

취약성 통합 v14.0 취약성 대응 및 v12.1 Qualys Vulnerability Integration 부터 CMDB CI Class Models(1.0.21.)가 지원됩니다. 클래스 모델에는 IRE(식별 및 조정) 식별 규칙에 네트워크 파티션 식별자(network_partition_identifier)가 있습니다.

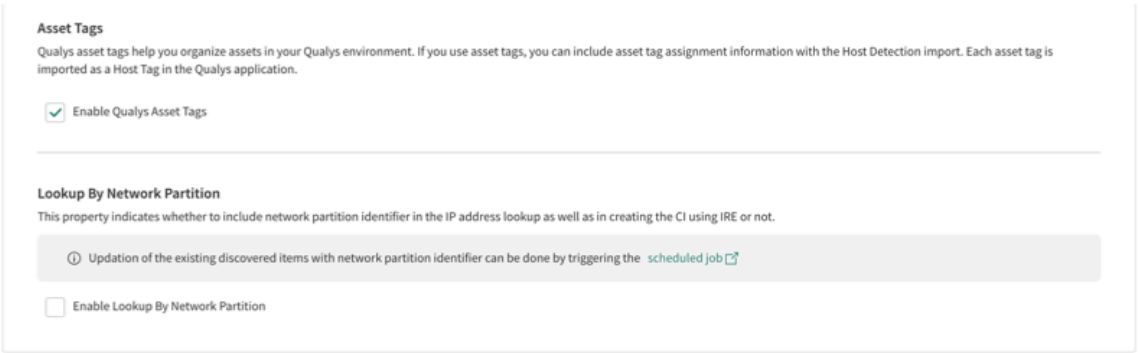
옵션	설명
요청 시 예약된 작업을 실행합니다.	기존 검색 항목을 업데이트합니다. 기존 Qualys Vulnerability Integration 데이터에 대한 CI는 네트워크 파티션 식별자 세분성을 포함하도록 생성되거나 업데이트됩니다. 검색된 항목, 취약한 항목 및 탐지 기록이 모두 새 CI로 업데이트됩니다.
다음 예약된 작업과의 통합에서 최신 데이터가 임포트될 때까지 기다립니다.	예약된 다음 작업으로 시작하는 네트워크 파티션 식별자를 사용하여 각각의 새 자산에 대한 CI를 생성합니다. CI, 취약한 항목 및 탐지 기록이 모두 새로운 세분성을 포함하도록 업데이트됩니다. 정확히 일치하는 항목이 없으면 새 CI가 만들어집니다.

프로시저

1. 다음으로 이동 취약성 대응 > 설정 도우미 > 통합 구성 > 스캐너 통합.
2. 을(를) 선택합니다 Qualys Vulnerability Integration.
3. 필요한 통합을 편집합니다.
4. 선택 호스트 탐지 구성.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. 선택 네트워크 파티션별 조회 사용 의 확인란 네트워크 파티션별 조회



절.

6. 마침을 클릭합니다.

네트워크 파티션 식별자 **NETWORK_ID** 및 리포지토리**_ID IP** 조회 및 **CI** 생성에 포함됩니다.

소스	**IP** 주소	**NETWORK_ID**	네트워크 파티션 식별자가 없는 자산에 대한 **CI**	**CI** 네트워크 파티션 식별자가 있는 자산
Qualys Vulnerability Integration: 자산과 고정 및 미해결 취약성 통합	123.12.12.141	03712	CI 1	CI 1
	123.12.12.141	03713	CI 1	CI 2

소스	**IP** 주소	**REPOSITORY_ID**	네트워크 파티션 식별자가 없는 자산에 대한 **CI**	**CI** 네트워크 파티션 식별자가 있는 자산
Qualys: 자산 및 고정 및 미해결 취약성 통합	123.12.12.141	12	CI 1	CI 1
	123.12.12.141	13	CI 1	CI 2

IP 주소 및 불완전한 IP 주소 CI 식별 조회 규칙에는 자산 및 의 고정 및 미해결 취약성 통합 Qualys Vulnerability Integration에서 데이터를 임포트하기 위한 네트워크 파티션 식별자 속성이 자동으로 포함됩니다.

예약된 작업을 활성화하고 기록을 저장한 후 요청 시 예약된 작업을 시작하여 네트워크 파티션 식별자가 포함된 CI로 기존 검색된 항목을 업데이트할 수도 있습니다. 기존 검색된 항목, 취약한 항목 및 탐지 기록의 CI가 자동으로 업데이트됩니다.

선택적 **Qualys** 수정 사항

선택적 수정을 구성하고 특히 Qualys 통합을 위해 일부 데이터를 간소화합니다.

설정 도우미 또는 기본 통합에서 시작 날짜를 재설정하거나 비즈니스 규칙을 수정하여 초기 임포트 중에 비활성화할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

초기 기록을 임포트하기 전에 알림 관련 비즈니스 규칙을 비활성화합니다.

기록을 처음 임포트하는 동안 특정 알림 관련 비즈니스 규칙에서 많은 알림이 생성되어 성능에 영향을 줄 수 있습니다. 이러한 비즈니스 규칙은 임포트 중에 비활성화하도록 수정해야 합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동모두 〉 시스템 정의 〉 비즈니스 규칙.
2. 영향을 받는 **CI** 알림을 검색합니다.
3. 비즈니스 규칙을 열고 current.sys_class_name != "sn_vul_vulnerable_item" 조건을 삽입합니다.
4. 업데이트를 클릭합니다.
5. 다음 비즈니스 규칙에 대해 이 절차를 반복합니다.
   - 영향을 받는 비용 센터 알림
   - 영향을 받는 그룹 알림
   - 영향을 받는 위치 알림

> **주:**
> 초기 기록 임포트가 완료된 후 이러한 비즈니스 규칙을 다시 사용하도록 설정할 수 있습니다. 그러나 비활성화된 상태로 두는 것이 좋습니다. 이로 인해 많은 수의 알림이 생성되고 인스턴스 성능에 영향을 줄 수 있습니다.

QVS 점수 통합 활성화 Qualys

Qualys QVS 점수 통합을 사용하면 CVE에 대한 QVS 점수를 자동으로 채워 sn_vul_nvd_entry에서 취약성 위험을 보다 정확하게 평가할 수 있습니다. 목록 테이블.

시작하기 전에
필요한 역할: sn_vul_cmn.admin

프로시저

1. 다음으로 이동 모두 〉 **Qualys** 통합 〉 **Qualys QVS** 점수 통합.
2. 통합을 사용하려면 활성 확인란을 선택합니다.

> **주:**
> 이 기능은 기본적으로 비활성 상태입니다.

결과
통합이 실행되면 지난 15일 동안 업데이트된 CVE의 최신 QVS 점수를 쿼리 Qualys 하고 [sn_vul_nvd_entry. LIST] 테이블에 있습니다.

> **주:**
> QVS 점수가 비어 있으면 지난 15일 동안 CVE가 업데이트되지 않은 것입니다.

초기 시작 날짜 수정

설치 도우미를 사용하여 설치하는 동안 Qualys 통합의 초기 시작 날짜를 설정합니다. 아래와 같이 설정 도우미 또는 기본 통합에서 시작 날짜를 재설정할 수 있습니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

이 태스크 정보

통합 실행 중에 여러 프로세스가 생성되고 데이터가 페이지 형식으로 수신됩니다. 각 프로세스에는 페이지에 첨부된 데이터가 있는 하나 이상의 임포트 큐 항목이 포함될 수 있습니다. 이러한 항목은 1시간의 시간 제한 내에 데이터를 처리해야 합니다. 그러나 페이로드 크기가 크면 처리 시간이 1시간을 초과하거나 중단되어 통합 시간 제한 오류가 발생할 수 있습니다. 통합은 시간 초과 오류에도 불구하고 데이터를 계속 처리합니다. 이러한 잘못된 통신을 피하기 위해 버전 18.2.4 취약성 대응부터 큐가 활성 상태이고 데이터를 처리하는지 여부를 나타내기 위해 타임스탬프(하트비트)가 주기적으로 전송됩니다. 임포트 큐 항목 페이지의 처리된 마지막 기록 필드는 임포트 큐가 생성하거나 업데이트하는 기록 수에 따라 업데이트됩니다. 임포트 큐 항목이 1시간의 시간 제한을 초과하는 경우, 시스템은 마지막으로 처리된 기록 필드를 검사하여 1시간보다 오래되었는지도 확인합니다. 이 경우 이는 임포트 큐 항목이 고착되었음을 나타내며 처리 시 더 이상의 지연을 방지하기 위해 시간 초과됩니다.

주:
마지막으로 처리된 기록 필드는 다음 시스템 속성에 정의된 내용에 따라 업데이트됩니다.

- *sn_sec_cmn.record_threshold_heartbeat*: 하트비트(타임스탬프)가 임포트 큐 항목으로 전송된 후 처리된 기록 수를 정의합니다.
- *sn_sec_cmn.maximum_heartbeat_delay*: 임포트 큐 항목을 시간 초과해야 하는 시간을 정의합니다.

프로시저

1. 다음으로 이동 모두 〉 **Qualys** 취약성 통합 〉 관리 〉 기본 통합.
2. **Qualys** 호스트 탐지 통합을 클릭합니다.
3. 통합 상세 정보를 클릭합니다.
4. 시작 시간 필드를 과거의 값으로 설정하면 해당 시간 이후에 스캔되고 탐지된 모든 취약성이 탐지됩니다.

   설정 도우미를 사용하여 구성한 Qualys 경우 시작 시간 필드는 처음에는 오늘 날짜의 3개월 전으로, 그 다음에는 오늘 날짜로 미리 채워집니다.

   주:
   값을 과거 최대 월로 설정하는 것이 좋습니다. 이렇게 하면 많은 양의 데이터가 Qualys API 속도 제한을 초과하지 않고 실행 시간 초과가 트리거되는 것을 방지할 수 있습니다.

5. 제출 또는 업데이트를 클릭합니다.
6. 옵션: 지금 실행을 클릭하여 즉시 실행합니다.

고급 **Qualys** 구성 및 수정

고급 선택적 수정을 구성하고 통합을 위해 일부 데이터를 간소화합니다 Qualys . 이러한 수정의 대부분은 코딩이나 고급 ServiceNow 또는 Qualys Cloud Platform 전문 지식이 필요합니다.

임포트에 대한 Qualys 추가 팁은 HI 지식베이스에서 Qualys 임포트 작업에 대한 성능 튜닝 팁 지식 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Qualys에서 **ServiceNow** 우선순위 및 상태 매핑 값으로 수정

요구 사항의 우선순위 및 상태에 대한 매핑 값을 수정합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
이는 고급 사용자 지정 옵션입니다.

프로시저

1. 다음으로 이동 모두 〉 시스템 정의 〉 비즈니스 규칙.
2. **Map Qualys Values**를 검색하여 엽니다.
3. 고급 탭을 클릭합니다.
4. 요구 사항에 따라 수정하십시오.
   가장 일반적인 수정에는 새 상태 값 추가 또는 중요도 또는 우선순위 수정이 포함됩니다.
5. 업데이트를 클릭합니다.

할당 그룹에 따라 기록에 대한 쓰기 기능 제한

할당된 그룹에 대한 구성원 자격을 기준으로 기록에 대한 쓰기/읽기 권한을 제한할 수 있습니다. 특정 요구사항에 따라 조건과 스크립트를 수정합니다.

시작하기 전에
필요한 역할: security_admin(관리자에서 상승된 역할)

주:
이 동작은 취약성 범위에서 수행됩니다.

프로시저

1. 다음으로 이동 모두 〉 시스템 보안 〉 접근 통제**(ACL)**.
2. sn_vul로 시작하는 ACL을 검색합니다.
3. 접근 제어 기록(예: sn_vul_vulnerable_item, 작업 쓰기)을 선택합니다.
4. 필요한 경우 기록에서 고급 상자를 선택하여 역할 항목을 표시합니다.
5. 요구 사항에 맞게 역할 스크립트를 수정합니다.
   그룹별 접근 권한의 스크립트 수정 예시입니다.

```
answer = (current.assigned_to == gs.getUserID() ||
 isMemberOfForScopedApp(current.assignment_group));
// Note: standard 'isMemberOf' does not work within Scoped App
// gs.getUser().isMemberOf(current.assignment_group);
function isMemberOfForScopedApp(groupID){
var result = false;
if (groupID != ''){
var userID = gs.getUserID();
var now_GR = new GlideRecord("sys_user_grmember");
gr.addQuery("group", groupID);
gr.addQuery("user", userID);
gr.query();
if (gr.next()){
result = true;
}
}
```


© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
return result;
}
```

6. 업데이트를 클릭합니다.

스캐너 장치 설정

Qualys에서 직접 검사를 시작하는 대신 사용자 앞에서 ServiceNow AI Platform# 검사를 시작하는 경우 IP 주소 범위에 대한 검사를 설정할 수 있습니다.

시작하기 전에

데이터는 자산 그룹 및 관련 기본 어플라이언스(스캐너)를 Qualys 기반으로 하는 통합에서 Qualys 가져옵니다.

대상 IP 주소 범위에 대해 장치가 구성되지 않은 경우 통합 인스턴스의 기본값으로 설정된 장치가 검사에 사용됩니다.

필요한 역할: sn_vul_qualys.admin

프로시저

1. 다음으로 이동 모두 〉 **Qualys** 취약성 통합 〉 스캐너 장치.

2. 양식의 필드에 적절히 입력합니다.

필드	설명
장치 이름	기록을 수동으로 생성할 때 이 필드를 채울 것을 요청합니다. 구성 항목 일치를 위한 스캔을 불러올 때 사용할 스캐너 장치의 이름을 Qualys 입력합니다. 외부 스캐너로 스캔을 시작하려는 경우 ## 값을 사용합니다.
장치 ID	구성 항목 일치를 위한 스캔을 불러올 때 사용할 스캐너 장치의 장치 식별자 Qualys 를 입력합니다. 기록을 수동으로 생성할 때 이 필드를 채울 것을 요청합니다. 외부 스캐너로 스캔을 시작하려면 0 값을 사용합니다.
장치 상태	통합에 의해 Qualys 반환된 데이터에 스캐너 장치의 마지막 상태를 표시합니다. 수동으로 만든 기록의 경우 유효한 장치 **ID** 가 지정된 경우에만 상태가 업데이트됩니다.
자산 그룹 ID	이 기록을 생성한 자산 그룹 식별자를 Qualys 표시합니다. 이 필드에는 통합으로 Qualys 생성된 기록에 대한 값만 표시됩니다.
자산 그룹 이름	Qualys 이 기록을 생성한 자산 그룹 이름을 표시합니다. 이 필드에는 통합으로 Qualys 생성된 기록에 대한 값만 표시됩니다.
순서	스캔 우선순위를 결정하는 데 사용할 값을 입력합니다. 상충하는 조건이 있는 장치의 경우 순서 값이 낮은 장치에 높은 우선 순위가 부여됩니다.
수동 작성됨	사용자가 이 기록을 수동으로 생성했는지 여부를 나타냅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
필터 그룹 이용	스캔할 일치하는 구성 항목을 찾기 위한 필터 그룹을 지정하려면 이 확인란을 선택합니다.
필터 그룹	스캔할 일치하는 구성 항목을 찾는 데 사용할 필터 그룹을 선택합니다. 이 필드는 필터 그룹 사용을 선택한 경우에만 나타납니다.
IP	스캔을 불러올 때 이 장치에서 사용할 쉼표로 구분된 IP 주소 목록 또는 IP 주소 범위.
통합 인스턴스	이 Qualys 장치와 연결된 통합 인스턴스입니다.
옵션 프로파일	구성 항목을 일치시키기 위한 검색에 사용할 옵션 프로필을 선택합니다.

3. 업데이트를 클릭합니다.

취약성 스캐너 및 검사 구성 및 관리 **Qualys**

Qualys 취약성 스캔을 수행하여 CI에 영향을 주는 소프트웨어 취약성을 찾을 수 있습니다. 취약한 항목 기록에서 스캔을 시작하거나 구성 항목(CI) 및 IP 주소에 대한 스캔 기록을 직접 생성하여 스캔을 시작할 수 있습니다.

취약한 항목 화면에서 직접 취약한 항목을 검사 Qualys 하는 경우 여러 취약한 항목을 동시에 검사할 수도 있습니다.

가 활성화된 경우 보안 인시던트 응답 보안 인시던트 카탈로그, 보안 인시던트 기록 또는 보안 검사 요청에서 검사를 시작할 수도 있습니다.

취약한 항목, 보안 인시던트 카탈로그보안 인시던트 또는 보안 검사 요청에서 Qualys 제출된 검사는 기본 Qualys 스캐너에서 수행됩니다.

구성 항목을 일치시키기 위한 검색에 사용할 옵션 프로파일을 선택할 수 있습니다.

- 옵션 프로파일에는 검사 설정이 포함되어 Qualys 있습니다.
- 옵션 프로파일은 에서 ServiceNow AI Platform#스캔을 Qualys 시작할 때 필요합니다.

ServiceNow에서 시작한 **Qualys IP** 스캔 구성

기본 시스템에 포함된 스캐너는 Qualys IP 주소를 기반으로 스캔을 시작하는 기준선 통합을 제공합니다.

시작하기 전에

구성 항목을 일치시키기 위한 검색에 사용할 옵션 프로파일을 선택할 수 있습니다.

- 옵션 프로파일에는 검사 설정이 포함되어 Qualys 있습니다.
- 에서 Qualys 스캔 ServiceNow AI Platform#을 시작할 때 옵션 프로파일이 필요합니다.

필요한 역할: sn_vul_qualys.admin

가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 취약성 스캐닝 〉 스캐너.
2. Qualys 기록을 엽니다.
3. 활성 및 기본 확인란을 선택합니다.

   스캐너를 사용하여 Qualys VI를 자동으로 스캔 Qualys 하려면 활성을 선택해야 합니다. 자동으로 실행되도록 기본값을 선택할 필요도 없습니다.

   v12.0 이전에는 스캐너를 사용하려면 **Active** 가 필요합니다. 기본값도 선택하면 스캔 중에 선택할 필요 없이 스캐너가 자동으로 사용됩니다.
4. 소스 통합 필드의 경우 검색 아이콘을 클릭하고 **Qualys**에 대한 옵션(예: **Qualys** 클라우드 플랫폼)을 선택합니다.
5. 업데이트를 클릭합니다.
6. 다음으로 이동 모두 〉 **Qualys** 취약성 통합 〉 관리 〉 기본 통합.
7. **Qualys** 자산 그룹 목록 통합을 엽니다.
   a. 활성 확인란을 선택합니다.
   b. 지금 실행을 클릭합니다.
8. 다음 단계를 수행하여 스캐너 장치를 채웁니다.

   주:
   검색 목록 통합, Qualys 동적 검색 목록 및 Qualys 정적 검색 목록 통합에서 임포트한 후 옵션 프로파일 목록 통합을 실행하여 옵션 프로파일과 연결된 검색 목록을 확인할 수 있습니다.

   a. **Qualys** 옵션 프로파일 목록 통합을 엽니다.
   b. 활성 확인란을 선택합니다.
   c. 지금 실행을 클릭합니다.
   d. 스캐너 장치를 구성하려면 나열된 스캐너 장치 설정 단계를 따르십시오.
   해당 단계를 완료한 후 여기로 돌아와 구성을 계속합니다.
   e. 다음으로 이동 모두 〉 **Qualys** 취약성 통합 〉 관리 〉 기본 통합.
   f. **Qualys** 장치 목록 통합을 엽니다.
   g. 활성 확인란을 선택합니다.
   h. 지금 실행을 클릭합니다.
   Qualys 이제 스캐너 장치가 올바르게 채워졌습니다.

관련 정보

Qualys Vulnerability Integration 이해

여러 **Qualys** 취약성 또는 취약한 항목 검사

양식에 채워진 IP 주소 또는 영향을 받는 CI(구성 항목)가 하나 이상 포함된 여러 Qualys 취약성 또는 취약한 항목을 동시에 검사할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_write

가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

프로시저

1. 다음 중 하나를 수행합니다.
   - 다음으로 이동 모두 〉 취약성 대응 〉 정정 작업.
   - 다음으로 이동 모두 〉 취약성 대응 〉 모든 취약한 항목.
2. 스캔하려는 기록의 확인란을 선택합니다.
3. 선택한 행 목록에서 작업을 클릭하고 취약한 항목 다시 검색을 클릭합니다.
   스캔에 대한 링크가 포함된 메시지가 나타나고 작업 메모가 업데이트됩니다.
4. 스캔 진행률 또는 결과를 보려면 링크를 클릭하십시오.

Qualys 해결된 정정 작업에 대한 자동 스캔 구성

자동으로 실행되는 검사를 예약하여 취약한 항목을 업데이트할 수 있습니다 Qualys .

시작하기 전에
정정 작업이 해결됨으로 전환되면 관련된 취약한 항목의 상태를 업데이트하기 위한 검사가 자동으로 시작됩니다.

- 이 검사는 기본적으로 비활성화되어 있습니다.
- 에 위치한 **Qualys** 기록의 **scan_on_resolved** 통합 인스턴스 매개변수를 사용해 스캔을 활성화합니다. 모두 〉 **Qualys** 취약성 통합 〉 통합 인스턴스 〉 **Qualys**. 자세한 내용은 다음 단계를 참조하십시오.
- 이 스캔은 인스턴스에 따라 다릅니다. 인스턴스가 여러 개 있고 이 스캔을 활성화하거나 비활성화하려면 변경하려는 각 인스턴스의 통합 인스턴스 매개변수에서 **scan_on_resolved** 매개변수를 비활성화해야 합니다.
- 검사가 활성화된 경우 요청 시 검사를 시작하거나 지정된 기간 내에만 검사가 실행되도록 예약할 수 있습니다. 이 기간의 시작 및 종료 시간을 설정하는 방법은 을 참조하십시오 예약된 간격 내에서만 실행되도록 다시 스캔 구성 Qualys .

필요한 역할: sn_vul_qualys.admin

프로시저

1. 다음으로 이동 모두 〉 **Qualys** 취약성 통합 〉 관리 〉 통합 인스턴스.
2. **Qualys**를 선택하여 기록을 엽니다.
   에 대한 Qualys 통합 인스턴스 매개변수가 탭에 표시됩니다.
3. 자동 스캔을 활성화하려면 매개변수를 찾습니다 *scan_on_resolved* .
4. 속성의 값 열에 true를 입력합니다.
5. 업데이트를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예약된 간격 내에서만 실행되도록 다시 스캔 구성 **Qualys**

취약성 통합의 Qualys 경우 원하는 시간 동안에만 재스캔이 실행되거나 사용할 수 있도록 스캔 시작 및 종료 시간 매개변수를 설정합니다.

시작하기 전에
이 구성은 예약된 재스캔과 인스턴스의 제품 ServiceNow AI Platform# 에서 Qualys 수동으로 시작하는 재스캔 모두에 적용됩니다.

통합 인스턴스에 대한 스캔 시작 및 종료 시간 매개변수를 설정하면 제품에서 재스캔을 Qualys 사용할 수 있는 기간을 지정할 수 있습니다. 예를 들어, 자정부터 오전 10시까지와 같이 업무 외 시간에만 재스캔이 가능하도록 지정할 수 있습니다.

이 설정은 인스턴스에 따라 다릅니다. 인스턴스가 여러 개인 경우 변경하려는 각 인스턴스의 통합 인스턴스 매개변수에서 scan_start_time 및 scan_end_time 값을 구성해야 합니다.

필요한 역할: sn_vul_qualys.admin

프로시저

1. 다음으로 이동 모두 〉 **Qualys** 취약성 통합 〉 통합 인스턴스 〉 **Qualys**.
2. **Qualys**를 클릭하여 기록을 엽니다.
   에 대한 Qualys 통합 인스턴스 매개변수가 표시됩니다.
3. scan_start_time 매개변수의 경우 값 열에 재스캔을 사용할 수 있는 창의 시작 시간에 대해 UTC 표준 시간대의 시간을 24시간 형식(00:00 - 24:00)으로 입력합니다.
4. scan_end_time의 경우 값 열에 사용 가능한 창의 종료 시간에 대해 동일한 형식(00:00 - 24:00)으로 시간을 입력합니다.
   예를 들어 scan_start_time 매개변수에 대해 00:00의 시작 시간을 입력하고 같은 날 오전 10:00로 scan_end_time 경우 자정에서 오전 10시 이외의 시간대 외에 예약되거나 수동으로 실행된 검사는 큐에 대기하고 다음 날 시간대의 시작 시간인 00:00에 실행됩니다.

   같은 예에서 정정 소유자가 오전 11:00에 수동으로 다시 검색을 시작하는 경우 다시 검색은 사용 가능한 구성된 검색 시간을 벗어나기 때문에 즉시 시작되지 않습니다. 스캔 요청은 다음 날 기간(이 예에서는 00:00)이 시작될 때까지 큐에 대기된 상태로 유지됩니다.
5. 업데이트를 클릭하여 설정을 저장합니다.

Qualys 취약성 검사 속도 제한

다양한 유형의 검사가 수행되는 속도를 정의하여 외부 스캐너로 전송되는 요청 수를 제한할 수 있습니다. 속도 제한을 정의한 후 스캐너에 적용할 수 있습니다 Qualys .

스캔 속도 제한 정의 **Qualys**

스캔 큐의 부하를 분산하기 위해 다양한 유형의 스캔이 수행되는 속도를 정의할 수 있습니다. 속도 제한에 정의된 조건에 따라 큐에 대기 중인 항목에 속도 제한이 적용되는지 여부가 결정됩니다.

시작하기 전에
필요한 역할: sn_vul.admin

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 취약성 스캐닝 〉 속도 제한 정의.
2. 새로 만들기를 클릭합니다.
3. 양식의 필드에 적절히 입력합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속도 제한 정의

필드	설명
이름	큐 항목이 충족해야 하는 조건을 식별하는 설명이 포함된 이름을 제공합니다. 예를 들어, 분당 검사 수가 있습니다.
큐 조건	대기 중인 스캔 항목에 이 요율 제한이 적용되는지 여부를 결정하는 데 사용되는 조건을 입력합니다. 조건은 특정 스캐너에 국한되어서는 안 됩니다.
평가 스크립트	큐에 대기 중인 항목을 평가하는 논리가 있는 스크립트를 작성합니다. 항목이 처리되는지 여부를 정의하려면 스크립트가 true/false를 반환해야 합니다. 또한 평가 스크립트는 평가 중인 큐에 대기 중인 항목을 기반으로 합니다.

4. 제출을 클릭합니다.

스캐너에 **Qualys** 스캔 속도 제한 적용

속도 제한 정의를 사용하여 스캔 속도 제한을 정의한 후 특정 Qualys 스캐너에 속도 제한을 적용할 수 있습니다.

시작하기 전에
필요한 역할: sn.vul_admin

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 취약성 스캐닝 〉 스캐너 속도 제한.
2. 새로 만들기를 클릭합니다.
3. 양식의 필드에 적절히 입력합니다.

스캐너 속도 제한

필드	설명
스캐너	속도 제한을 적용할 스캐너를 선택합니다.
속도 제한	이 스캐너에 적용할 속도 제한을 선택합니다.
임계치	선택한 요율 제한에 대해 선택한 스캐너를 적용할 임계치를 입력합니다. 예를 들어 스캐너가 분당 4개의 스캔을 허용하고 속도 제한이 분당 요청으로 정의되는 경우 임계값은 4입니다.

4. 제출을 클릭합니다.

Qualys 취약성 스캔 큐 보기

시스템 자원에 과부하가 걸리지 않도록 취약성 검사 통합에 제출된 Qualys 취약성 검사 요청이 큐에 대기됩니다. 필요에 따라 대기 중인 요청의 상태를 볼 수 있습니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)

가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

이 태스크 정보

대기 중인 스캔 목록에서 각 스캔에는 스캔된 CI를 식별하는 자동으로 생성된 스캔 이름이 포함됩니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 취약성 스캐닝 〉 스캔 큐.
   제출된 모든 Qualys 스캔 요청이 목록에 표시됩니다. 상태 열에는 대기 중인 각 항목의 현재 상태가 표시됩니다. 완료 상태는 스캔이 큐에서 벗어났음을 나타냅니다. 그렇다고 해서 반드시 스캔 처리가 완료되었음을 나타내는 것은 아닙니다. 스캔이 완료되거나 실패하면 처리 열에 적절한 작업 메모 텍스트가 표시됩니다.

   주:
   스캔을 위해 해시 값을 제출하고 스캐너가 결과를 찾지 못하면 상태가완료 로 표시되고 처리 열의 작업 메모는 알 수 없음으로 표시됩니다.

2. 스캔 처리가 완료되면 대기 중인 기록을 클릭하여 스캔 요청에 대한 상세 정보를 봅니다.

확인된 탐지 임포트에 기본 시스템 필터 사용

통합 매개변수를 사용하여 에서 확인된 탐지 Qualys Cloud Platform만 임포트하는 기본 필터를 활성화합니다.

시작하기 전에

필요한 역할: sn_vul_qualys.admin, sn_vul.vr_import_admin

이 태스크 정보

에서 필터링된 탐지 Qualys Cloud Platform목록을 임포트하는 데 기본 시스템 통합 인스턴스 매개변수 "include_only_confirmed"을 사용할 수 있습니다. 기본적으로 이 매개변수는 *FALSE*로 설정되며 잠재적, 확인됨 또는 정보용 탐지 등 모든 탐지가 임포트됩니다.

프로시저

1. 다음으로 이동 모두 〉 **Qualys** 취약성 통합 〉 관리 〉 통합 인스턴스.
2. 통합 인스턴스 목록에서 Qualys 클라우드 플랫폼 통합을 엽니다.
3. 통합 인스턴스 매개변수 목록에서 *'include_only_confirmed'* 매개변수를 엽니다.
4. 기본값을 *True*로 업데이트합니다.
5. 업데이트를 클릭합니다.
   통합에서 Qualys Cloud Platform 확인된 탐지를 임포트하는 필터를 활성화했습니다.

결과

기본적으로 다음 Qualys 취약성 임포트가 실행될 때 통합에서 Qualys Cloud Platform 확인된 탐지만 임포트됩니다. 정보 및 잠재성과 같은 다른 모든 탐지는 무시되고 임포트되지 않습니다. 자세한 내용은 취약성 대응 취약한 항목 탐지 데이터 보기를 참조하십시오.

다음에 대한 재스캔 시작 **Qualys Vulnerability Integration**

요청 시 제품 ServiceNow AI Platform 재 Qualys 스캔을 시작하여 예약된 검사 주기 사이에 취약한 항목이 정정되었는지 확인합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
취약성 대응 작업 공간에서 다시 스캔을 시작할 수 있습니다. 자세한 내용은 에서 기록 및 정정 작업을 다시 스캔 취약성 관리자 작업 공간 및 에서 취약한 항목 및 정정 작업 다시 스캔 IT 정정 작업 공간 문서를 참조하십시오.

클래식 환경에서 다시 검색하는 경우 다음 섹션에서 다시 검색을 시작하는 방법을 참조하십시오.

다음ServiceNow AI Platform에서 시작된 제품의 재스캔에 필요한 설정:Qualys

인스턴스에서 제품의 취약한 항목에 대한 요청 시 재스캔을 Qualys 시작할 수 있습니다 ServiceNow AI Platform# .

예약된 전체 검사와 관련된 오버헤드와 볼륨을 줄이기 위해 정정 소유자, IT 전문가, 취약성 분석가 또는 취약성 관리자는 해당 환경에서 자산(구성 항목)의 특정 취약성에 대한 요청 시 대상 재검사를 시작할 수 있습니다. VI(취약한 항목), RT(정정 작업), TPE(외부 공급업체 항목) 또는 인스턴스에서 검색된 항목 기록에서 제품 재스캔 Qualys 을 시작할 수 있습니다 ServiceNow AI Platform .

재검색을 통해 정정 활동, 패치 및 기타 작업이 구성 항목(CI)의 특정 취약성을 성공적으로 수정했는지 확인할 수 있습니다.

사용 사례:

예를 들어, 전체 환경이 3주에 한 번씩 검사된다고 가정해 보겠습니다. 가장 최근의 전체 검사는 일주일 전에 완료되었지만 중요한 취약성을 수정하기 위해 어제 패치를 적용했습니다. 이 취약성의 특성으로 인해 다음 예약된 검사에서 정정되었는지 확인할 때까지 2주를 기다릴 수 없습니다. 패치가 이전 검사 중에 발견된 중요 취약성을 성공적으로 수정했는지 확인하기 위해 취약한 항목에 대한 Qualys 대상 재스캔 ServiceNow AI Platform 을 시작할 수 있습니다.

종결 이외의 상태에서 소스로 있는 Qualys VI에 대한 재스캔을 시작할 수 있습니다. 에서 기록 및 정정 작업을 다시 스캔 취약성 관리자 작업 공간 및 에서 취약한 항목 및 정정 작업 다시 스캔 IT 정정 작업 공간 문서를 참조하십시오.

재스캔에 필요한 다음 설정을 완료했는지 확인합니다. 자세한 내용은 이전 섹션에 나열된 취약성 스캐너 및 검사 구성 및 관리 Qualys 로 시작하는 단계를 참조하십시오.

필요한 역할: sn_vul_manually_initiate_rescan

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 취약한 항목.
2. 다시 스캔을 트리거할 취약한 항목 기록을 찾아 엽니다.

   주:
   VI Qualys 에 대한 재스캔만 소스로 시작할 수 있습니다. 확인 Qualys 이 VI 목록 뷰의 소스 열 또는 개별 기록의 소스 필드에 표시됩니다. 조건 빌더를 사용하여 소스별로 VI를 그룹화할 수 있습니다. 또는 소스 열이 VI 목록 뷰에 표시되지 않은 경우 목록의 왼쪽 상단에서목록 개인화 아이콘(기어 아이콘)을 클릭하고 슬러 시버킷을 사용하여 소스를 사용 가능 에서 선택됨으로 이동합니다.

3. 또는 다음으로 이동합니다. 모두 〉 취약성 대응 〉 정정 작업, 취약성 대응 〉 라이브러리 〉 외부 공급업체또는 다시 스캔에 사용할 정정 작업, 타사 항목 또는 검색된 항목 기록에 대해 각각 검색된 항목 입니다.

   선택에 따라 다음 기록에서 다시 스캔 버튼을 사용할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 단일 VI 기록에서 VI는 제품에서 나온 Qualys 것이어야 하며 종결 이외의 상태여야 합니다. 여러 VI 레코드의 경우 모든 VI가 소스로 있어야 Qualys 하며 종결 이외의 상태여야 합니다.
- RT 레코드에서 정정 작업은 종결 이외의 모든 상태일 수 있으며 연결된 모든 VI가 소스로 있어야 Qualys 합니다.
- 외부 공급업체 항목(TPE) 기록에서 기록에는 소스로 Qualys종결 이외의 상태인 연결된 VI 기록이 하나 이상 있어야 합니다.
- 검색된 항목 기록에서 구성 항목에는 종결됨 이외의 상태에서 소스로 Qualys 연결된 VI가 하나 이상 있습니다.

4. 선택한 레코드의 오른쪽 상단에서 Rescan(다시 스캔)을 클릭합니다.
표시되는 대화 상자에서 하나를 선택하여 계속합니다.

옵션	설명
옵션 프로파일 지정 확인란을 선택합니다.	목록에서 다시 스캔에 사용할 스캐너의 Qualys 옵션 프로필을 선택합니다. 구성하고 나열한 장치(스캐너)입니다. **Qualys 취약성 통합 〉 스캐너 장치.**
옵션 프로파일 지정 확인란의 선택을 취소합니다 (선택하지 않음).	Qualys 스캐너 기기 목록에서 기본 스캐너로 설정한 스캐너의 옵션 프로파일이 스캔에 사용됩니다. 에서 ServiceNow AI Platform시작하는 기본 스캐너 설정에 대한 자세한 내용은 이전 섹션에 나열된 스캐너 장치를 설정하여 자세한 내용을 확인하십시오.

5. 스캔 요청을 클릭합니다.

스캔이 처리 중임을 나타내는 메시지가 표시됩니다. 모든 재스캔의 상태는 재스캔을 시작하는 데 사용한 VI, RT, TPE 및 검색된 항목 레코드의 스캔 관련 목록에서 언제든지 확인할 수 있습니다. 메시지에서 세부 정보 보기를 클릭하여 다시 스캔 상태를 확인하고 지정된 기록에서 시작된 다른 다시 스캔을 봅니다.

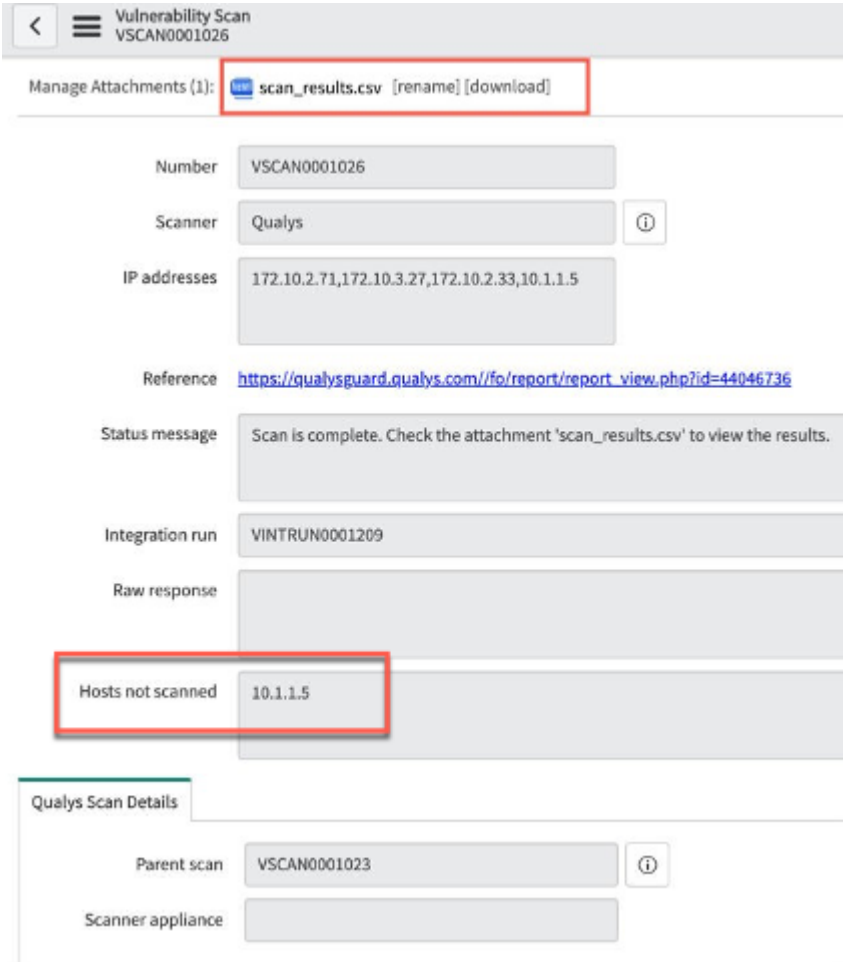
인스턴스는 재스캔 상태가 성공적으로 완료될 때까지, 또는 설정된 추적 기간의 시간 초과 중 먼저 발생하는 시점까지 재스캔 상태를 추적합니다. 시간 제한은 검사를 중지하지 않습니다. 시간 제한은 실제 다시 검색이 중지된 시간이 아니라 다시 스캔 상태 추적이 ServiceNow AI Platform 중지된 시기를 나타냅니다.

다시 스캔이 성공적으로 완료되면 호스트 탐지 통합이 Qualys 자동으로 시작되어 취약한 항목을 업데이트합니다. 보유한 VI 수에 따라 호스트 탐지 통합 스캔이 완료된 후 탐지, VI 및 RT가 Qualys 업데이트됩니다. 호스트 탐지 통합이 완료된 후 이러한 기록으로 이동하여 업데이트를 확인합니다.

이 스캔은 인스턴스에 따라 다르며 사용하지 않도록 설정할 수 있습니다. 통합 및 통합을 보는 방법에 대한 Qualys 자세한 내용은 다음 문서를 Qualys Vulnerability Integration 이해참조하십시오.

다음에 수행할 작업
스캔 기록에서 .csv 첨부 파일을 보고 다시 스캔에 대한 상세 정보를 볼 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



이전 이미지와 같이 다시 검색하는 동안 환경의 호스트(구성 항목)에 액세스할 수 없는 경우 다시 스캔이 완료될 때 이러한 자산과 연결된 탐지 및 VI가 업데이트되지 않습니다. 포함되지 않은 이유를 이해하는 데 도움이 되도록 재스캔이 완료된 후 이러한 CI의 자산 IP 주소가 스캔되지 않은 호스트 필드의 취약성 기록에 나열됩니다.

Qualys 취약성에 대한 메타데이터

호스트 탐지 통합이 Qualys 개선되어 의 더 많은 필드를 Qualys포함합니다. 이러한 필드는 악용할 수 없는 Linux 취약성을 필터링하는 데 도움이 됩니다. 이렇게 향상된 기능은 탐지 수준과 VI(취약한 항목) 수준에서 통합을 개선합니다.

다음에서 추가 메타데이터 임포트 **Qualys**

VI(취약성 항목)에 대한 추가 메타데이터를 임포트하여 커널 또는 서비스에 미치는 영향에 따라 취약성을 필터링합니다.

시작하기 전에

필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 설정 도우미.
2. 통합 구성 아래에서 스캐너 통합을 클릭합니다.
3. 설치된 애플리케이션에서 애플리케이션에 대해 Qualys 편집을 클릭합니다.
4. 호스트 탐지 구성을 클릭합니다.
5. 다음으로 이동 탐지를 위한 추가 메타데이터 임포트.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

6. 에서 Qualys추가 메타데이터를 임포트하려면 필요한 다음 확인란 중 하나를 수동으로 선택합니다.
   - 커널 메타데이터: 실행 중이거나 실행되고 있지 않은 Linux 커널에서 발견된 취약성을 식별합니다.

     반환된 메타데이터의 값이 아니요이면 실행 중이 아닌 커널로 인해 취약성을 악용할 수 없음을 의미합니다. 검색된 값에 대한 자세한 내용은 을 참조하십시오 Qualys 취약성에 대한 메타데이터 값.
   - 서비스 메타데이터: 실행 중이거나 실행되고 있지 않은 포트 또는 서비스에서 발견된 취약성을 식별합니다.
   - 악용 가능한 구성 메타데이터: 현재 호스트 구성으로 인해 악용될 수 있거나 악용되지 않을 수 있는 취약성을 식별합니다.

   주:
   기본적으로 이러한 확인란은 선택되어 있지 않습니다.

7. Qualys 소급 적용으로 호스트 탐지 통합을 실행합니다.
   시작 날짜를 설정하는 방법에 대한 자세한 내용은 문서를 참조하십시오 선택적 Qualys 수정 사항.

결과
메타데이터를 가져왔습니다.

다음에 수행할 작업
임포트한 메타데이터를 보려면 필터 탐색에 sn_vul_detection.list 를 입력합니다. 취약한 항목 탐지 목록이 표시됩니다. 새로 추가된 열에 표시되는 값에 대한 자세한 내용은 을 참조하십시오 Qualys 취약성에 대한 메타데이터 값.

Qualys 취약성에 대한 메타데이터 값

커널 메타데이터, 서비스 메타데이터 및 구성 메타데이터를 가져오면 일부 값도 검색됩니다. 값 **0**, **1** 및 사용할 수 없음은 백엔드에서 처리되고 각각 아니요, 예 및 비어 있음으로 변환됩니다.

이러한 값은 취약성 항목 탐지 및 취약성 항목 목록의 다음 열에 채워집니다.

- 실행 중인 서비스 열에 영향을 미칩니다.
- 악용 가능한 구성 열에 영향을 미칩니다.
- 실행 중인 커널 열에 영향을 미칩니다.

주:

- 이러한 열은 기본적으로 표시되지 않습니다. 양식 레이아웃을 구성하는 방법에 대한 자세한 내용은 양식 레이아웃 구성을 참조하십시오
- 이전 탐지의 경우 이러한 열의 값이 비어 있을 수 있습니다. 데이터를 업데이트하려면 이전 날짜의 Qualys 호스트 탐지 통합을 실행합니다. 시작 날짜를 설정하는 방법에 대한 자세한 내용은 문서를 참조하십시오 선택적 Qualys 수정 사항.

다음 표에서는 검색된 값과 해당 중요도를 보여 줍니다.

검색된 필드 값과 그 중요성

필드	값	심각도
AFFECT_RUNNING_KERNEL	0	실행 중이 아닌 커널에서 취약성이 발견되었습니다. 취약성은 악용될 수 없습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

검색된 필드 값과 그 중요성

필드	값	심각도
AFFECT_RUNNING_KERNEL	1	실행 중인 커널에서 취약성이 발견되었습니다. 취약성은 악용 가능합니다.
AFFECT_RUNNING_KERNEL	사용 불가	취약성은 커널 관련 취약성이 아닙니다.
AFFECT_RUNNING_SERVICE	1	실행 중이 아닌 포트 또는 서비스에서 취약성이 발견되었습니다. 취약성은 악용될 수 없습니다.
AFFECT_RUNNING_SERVICE	0	실행 중인 포트 또는 서비스에서 취약성이 발견되었습니다. 취약성은 악용 가능합니다.
AFFECT_RUNNING_SERVICE	사용 불가	취약성은 관련 취약성이 아닙니다.
AFFECT_EXPLOITABLE_CONFIG	1	취약성은 호스트 구성으로 인해 악용될 수 없습니다.
AFFECT_EXPLOITABLE_CONFIG	0	호스트 구성으로 인해 취약성이 악용될 수 있습니다.
AFFECT_EXPLOITABLE_CONFIG	사용 불가	취약성은 관련 취약성이 아닙니다.

임포트에 대한 **Qualys** 추가 필터 매개변수 설정

지원되는 Qualys Vulnerability IntegrationQualys 통합을 통해 임포트하는 취약성 데이터를 더욱 구체화할 수 있도록 예약된 쿼리에 대한 필터링 매개변수를 사용자 지정합니다.

시작하기 전에

사용 사례: 취약성 관리자 또는 분석가는 특정 취약성 상세 정보만 검토할 수 있도록 쿼리에서 데이터를 필터링할 수 있습니다. 예를 들어 특정 IP 또는 IP 범위별로 필터링되는 임포트된 취약성을 보려는 경우를 가정해 보겠습니다. 또는 사용자 범위 내에 있는 컴퓨터만 가져오려는 경우(예: 외부 장치가 아닌 회사 네트워크 내의 컴퓨터만 가져오려는 경우)

이 데이터를 수집하는 데 도움이 되도록 필요한 특정 취약성 상세 정보를 가져오는 데 도움이 되는 매개변수를 추가할 Qualys 수 있습니다.

이 기능을 사용하면 API 호출이나 코딩을 추가하지 않고도 HTTP 요청 정보를 QualysServiceNow AI Platform. 지원되는 Qualys 통합 Qualys Vulnerability Integration에 대한 REST 메서드 아래의 HTTP 메서드 기록에서 이러한 값을 수정하거나 추가합니다.

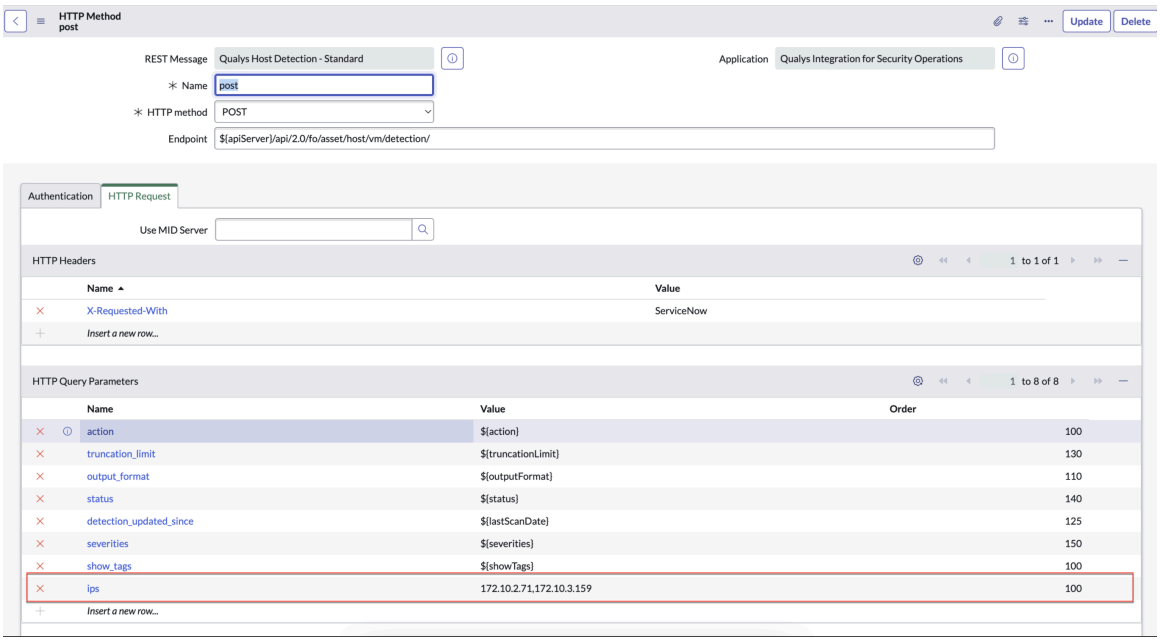
필요한 역할: sn_vul.vulnerability_admin

프로시저

1. 필터링에 사용할 개발자 사이트의 제품에서 Qualys 지원하는 매개변수를 찾습니다.
   제품에서 Qualys 입력하는 매개변수와 값은 의 통합 인스턴스 수준 ServiceNow AI Platform에서만 지원됩니다. 모든 Qualys 통합은 쿼리 매개변수를 사용한 필터링을 지원합니다.
2. 다음으로 이동 모두 〉 **Qualys** 취약성 통합 〉 관리 〉 기본 통합.
3. Qualys 통합 목록 페이지에서 기록을 열고자 하는 통합에 대한 기록을 클릭합니다.
4. Qualys REST 상세 정보 탭을 선택한 상태에서 REST 메서드에 대한 정보 아이콘(ⓘ)과 기록 열기를 차례로 찾아 클릭하여 HTTP 메서드 기록을 엽니다.
5. **HTTP** 요청 탭을 선택합니다.
6. 요청 본문에 대한 HTTP 쿼리 매개변수에서 개발자 사이트에서 가져온 Qualys 값을 추가합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예를 들어 다음 이미지에서는 특정 IP 주소/범위 *ips={value}* 만 수집하는 매개 변수가 추가되었습니다. 이 경우 값은 지정한 하나 이상의 IP/범위입니다. 여러 항목은 쉼표로 구분되고 (172.10.2.71, 172.10.3.159) 범위는 하이픈(10.10.10.1-10.10.10.100)으로 지정됩니다. Qualys 자세한 내용은 개발자 사이트를 참조하십시오.



둘 이상의 매개변수를 입력하려면 각 값을 구분하는 방법에 대한 자세한 내용은 설명서를 참조하십시오 Qualys .

> **주:**
> API 요구 사항을 알고 있어야 합니다. 이러한 API 속성을 쿼리 매개변수 또는 본문 콘텐츠에 추가해야 할 수 있습니다.

개발자 사이트에서 유용할 수 있는 몇 가지 다른 매개변수:Qualys

- *ag_ids* - 검색할 자산 그룹 목록 ID입니다. 이 매개변수를 사용하면 사용자 범위 아래에 있는 컴퓨터만 가져올 수 있습니다.
- *qids* - 이 매개변수는 특정 취약점(외부 공급업체 항목 테이블의 QID)으로만 결과를 제한합니다. 이 설정은 시스템에 정보 레코드가 넘쳐나는 것을 방지합니다.

7. 업데이트를 클릭합니다.

Qualys 취약성 통합 문제 해결

일반적으로 발생하는 몇 가지 문제와 임시 해결책에 대해 논의합니다.

임포트 후 첨부 파일이 표시되지 않음

외부 공급업체 통합을 임포트한 후 데이터 소스 또는 보안 인시던트에 첨부 파일이 예상대로 표시되지 않으면 IP 제한을 확인하십시오.

IP 액세스 제한으로 인해 안전한 IP에서 로그인하지 않으면 첨부 파일을 볼 수 없습니다. 가져올 때마다 새 첨부 파일이 추가되므로 제거해야 하는 중복이 발생할 수 있습니다.

예를 들어 타사 호스트 임포트 통합을 실행할 때 데이터 소스에 첨부 파일이 표시되지 않으면 IP 제한을 확인하고 임포트하기 전에 사용자를 허용 목록에 추가하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

변환 맵 수정

변환 맵은 기본 구성으로 제공되며 일반적으로 충분합니다. 조직의 필요에 따라 변환 매핑을 수정할 수 있습니다.

시작하기 전에
필요한 역할: sn_vul_qualys.admin + import_admin

프로시저

1. 다음으로 이동 모두 〉 시스템 임포트 세트 〉 관리 〉 변환 맵 을 클릭하여 REST 메시지를 봅니다.
2. 결과 목록을 애플리케이션별로 필터링하고 목록을 **Qualys** 취약성 통합 애플리케이션으로 제한합니다.
3. 고객 요구사항에 따라 변환 맵을 수정합니다.

   Qualys API에서 제공하는 데이터에 대한 자세한 내용은 Qualys API 문서를 참조하십시오.

XML 첨부 파일 속성 크기 확인

XML 첨부 파일 속성이 큰 파일에 충분한지 확인합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 〉 시스템 속성 〉 임포트 익스포트.
2. 까지 아래로 스크롤합니다. 임포트 속성 〉 **XML** 형식 페이지 하단에 있습니다.

3. 필요한 경우 값을 250으로 변경하고 저장을 클릭합니다.

관련 정보

사용 가능한 시스템 속성

데이터 검색 제한 사항

기본적으로 Qualys에서 데이터를 검색하는 방법에는 제한이 없습니다. 많은 기록이 고객이 취약성 대응 프로세스를 사용하여 정정하지 않으려는 낮은 심각도 취약성과 관련될 수 있습니다. 해당 REST 메시지/메서드 매개변수를 업데이트하면 이 동작을 수정할 수 있습니다.

이 업데이트를 담당하는 REST 메시지/메서드는 **Qualys** 호스트 탐지 – 표준/게시입니다. 값을 업데이트하려면 다음 값을 사용하여 post 메서드에 새 HTTP 쿼리 매개변수를 추가합니다.

- 이름: severities
- 값: 3-5(또는 원하는 적절한 심각도)

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Qualys 기술 자료 통합 실패 해결

에서 Qualys 수신되는 페이로드 첨부 파일 크기를 지정된 한도로 줄여 지식베이스 통합 실패를 해결합니다Qualys.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin

프로시저

1. 페이로드 첨부 파일 크기가 지정된 한도 내에 있는지 확인합니다.
   a. 다음으로 이동 모두 〉 **Qualys** 취약성 통합 〉 통합 인스턴스.
   b. 통합 인스턴스 매개변수 탭을 선택합니다.
   c. **max_delta_days** 선택하고 기본값을 3으로 수정합니다.
2. 통합이 계속 실패하면 다음 단계를 수행합니다.
   a. 다음으로 이동 모두 〉 **Qualys** 취약성 통합 〉 기본 통합.
   b. **Qualys** 기술 자료를 선택합니다.
   c. 통합 세부 정보 탭을 선택합니다.
   d. 시작 시간 필드에서 현재 날짜를 선택하여 해당 날짜의 실행 실행을 건너뜁니다.
   e. 다음으로 이동 모두 〉 **Qualys** 취약성 통합 〉 통합 인스턴스.
   f. 통합 인스턴스 매개변수 탭을 선택합니다.
   g. **kb_backfill_full_import** 선택하고 기본값을 true로 수정합니다.

결과
Qualys 지식베이스 백필 통합을 실행하면 시스템의 모든 타사 항목(TPE)이 업데이트됩니다. Qualys 호스트 탐지 통합이 자리 표시자 항목을 생성하는 동안 Qualys 지식베이스 백필 통합이 이를 업데이트합니다.

Qualys Vulnerability Integration 보고

개요는 취약성 활동에 대한 경영적 뷰입니다 Qualys Cloud Platform . 추세, 보고서 및 특정 데이터에 대한 드릴다운을 제공하여 관리자나 분석가는 관심 영역을 신속하게 찾아낼 수 있습니다. 차트는 취약한 항목 이후의 Qualys 데이터와 지식베이스 데이터를 검색한 후 데이터로 채워집니다.

작업 공간의 데이터 시각화 취약성 대응

작업 공간에는 취약성 대응 정정 진행 상황을 모니터링하는 데 도움이 될 수 있는 데이터 시각화가 포함되어 있습니다. 취약성 데이터가 변경될 때 업데이트되는 동적 데이터 시각화에서 조직에 중요한 활성 취약성의 수와 심각도를 확인하여 조직에 대한 위협 수준을 확인할 수 있습니다. 취약성 관리자 작업 공간IT 정정 작업 공간 살펴보기 를 참조취약성 대응 작업 공간하고 사용 가능한 동적 데이터 시각화에 대한 자세한 내용을 확인할 수 있습니다.

이전 버전 취약성 대응

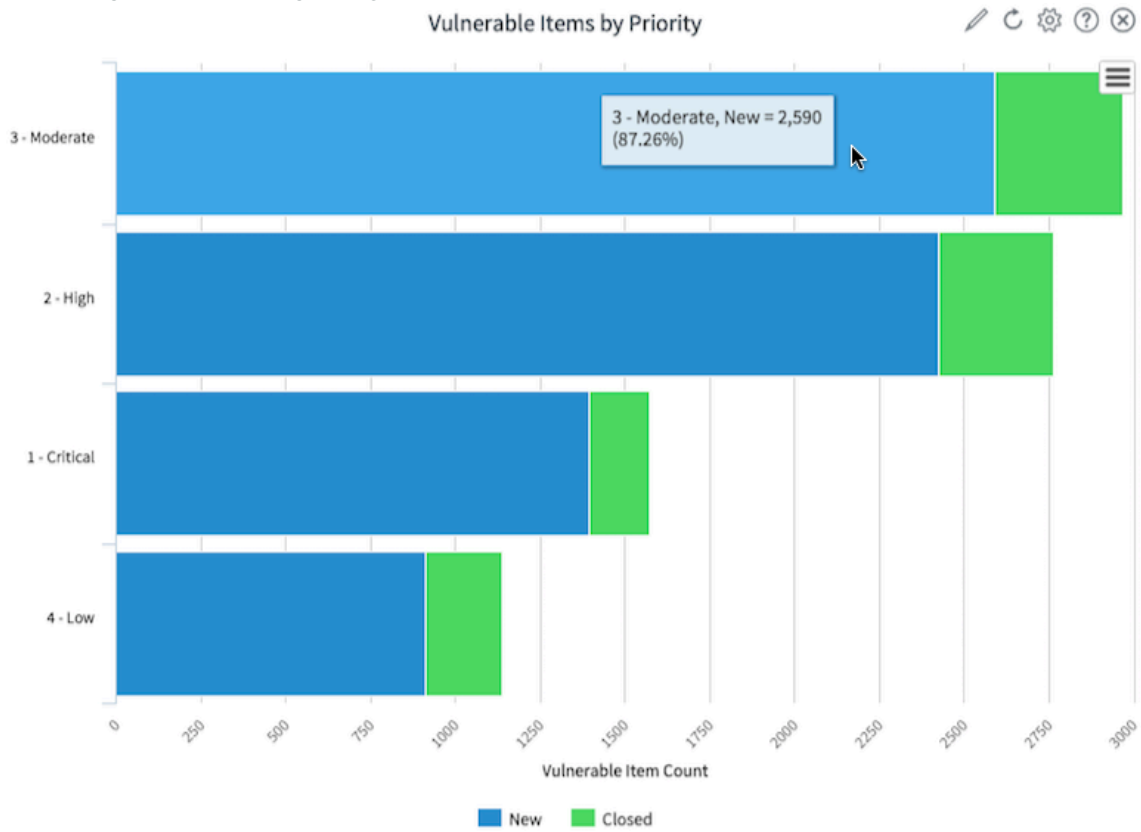
취약성 분석가는 클래식 환경의 기본 대시보드를 사용하여 취약성 데이터를 모니터링할 수도 있습니다. 자세한 내용은 기본 취약성 대응 대시보드 사용 문서를 참조하십시오.

주:
Qualys Cloud Platform 취약성 통합을 사용하는 경우 인스턴스에서 조정, 테스트 및 배포가 수행된 것으로 가정합니다. 이러한 기능은 제품 설명서에 포함되지 않는 영역입니다. 도움이 필요하면 에 문의하십시오 고객 서비스 및 지원.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

각 차트에서 차트의 특정 부분(막대형, 원형, 데이터 요소 등)을 가리키면 해당 부분과 관련된 일반 데이터를 볼 수 있습니다. 보고서의 일부를 클릭하면 자세한 정보를 제공하는 목록이 열립니다.

샘플 **Qualys Vulnerability Integration** 차트



홈페이지에서 다음 보고서를 사용할 수 있습니다 Qualys Cloud Platform .

Qualys Vulnerability Integration 개요 보고서

이름	**Visual**	설명
Qualys와 동기화된 CI	막대	각 CI에 대해 기록된 미해결된 취약한 항목 수를 가장 많은 항목에서 가장 작은 항목 순으로 표시합니다.
Qualys 취약한 항목 열기	막대	취약성과 관련된 미해결된 취약한 항목의 수(CVE 기록)를 가장 많은 항목에서 가장 작은 항목 순으로 표시합니다.
총 Qualys 취약한 항목	막대	7일 이내에 만료될 것으로 예약된 무시된 취약한 항목 수를 표시합니다.
우선순위별 취약한 항목	추세	매주 기록된 취약성 항목 수를 표시합니다.
QID 배포	막대	각 모델에 대해 기록된 취약한 항목 수를 가장 많은 항목에서 가장 작은 항목 순으로 표시합니다.
Qualys 취약한 항목 열기	목록	각 게시자에 대해 기록된 취약한 항목 수를 가장 많은 항목에서 가장 작은 항목 순으로 표시합니다.

Qualys 통합 실행 상태 차트

Qualys 통합 실행 상태 모듈은 통합 실행 상태에 Qualys 대한 그래픽 뷰입니다.

통합 실행의 상태를 보려면 다음으로 이동합니다. **Qualys** 취약성 통합 〉 통합 실행 상태.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

의 취약성 대응버전 19.0부터 이 대시보드는 New Experience UI에서 사용할 수 있습니다.

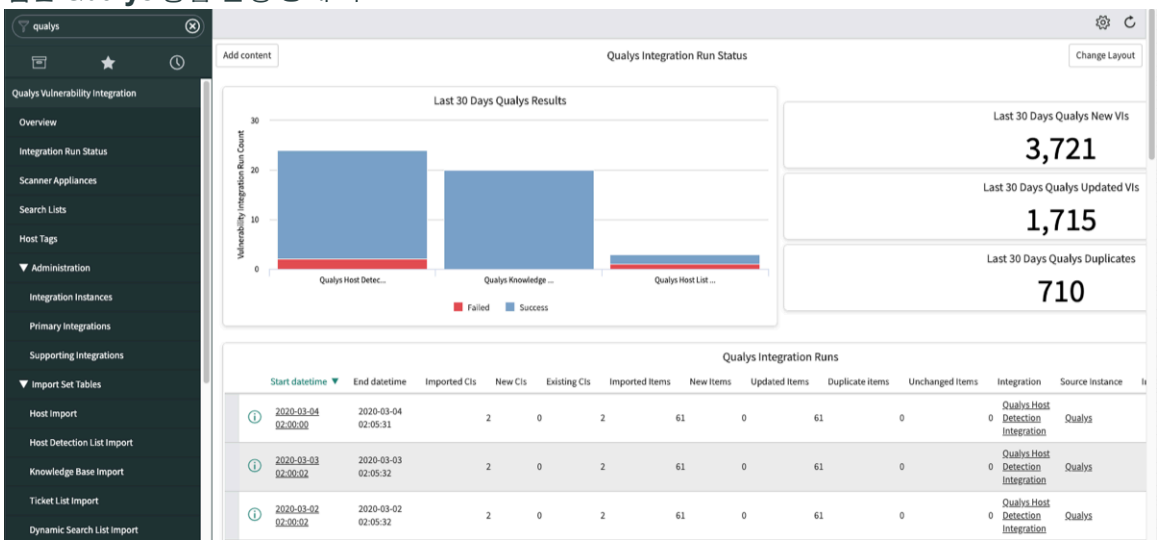
주:
Tokyo에 있는 경우 Next Experience UI에서 대시보드를 볼 수 있지만 일부 기능 손실이 있습니다.

차트에서 원하는 부품(막대형, 원형, 데이터 요소 등)을 가리키면 해당 부품과 관련된 일반 데이터를 볼 수 있습니다. 보고서의 일부를 클릭하면 자세한 정보를 제공하는 목록이 열립니다.

통합 실행 상태에는 Qualys 지난 30일 동안의 취약성 통합 실행 상태가 표시됩니다. Qualys[qualys] 업데이트된 VI 수는 동일한 자산 내 고유 탐지 수를 나타냅니다. 그런 다음 VI가 새로운 감지로 업데이트됩니다.

주:
취약성 통합 실행 횟수는 활성 상태로 설정된 통합에 대해서만 표시됩니다. 다음으로 이동 **Qualys** 취약성 통합 〉 관리 〉 기본 통합 을 클릭하고 상태를 활성으로 설정합니다.

샘플 **Qualys** 통합 실행 상태 차트



- 임포트한 항목 열의 값은 통합 실행에서 생성된 총 기록 수를 나타냅니다.
- 새 항목 열에는 통합 실행에서 생성된 기록 수가 표시됩니다.
- 중복 항목 열이 더 이상 채워지지 않습니다. 표시에서 이 열을 제거하는 것이 좋습니다.
- 업데이트된 항목 열에는 통합 실행 중에 기록 이 업데이트된 횟수가 표시됩니다. 이 값은 업데이트되는 고유 기록 수가 아닙니다. 예를 들어 통합 실행 중에 기록 이 두 번 업데이트되면 두 번 계산되어 2 개의 업데이트된 항목으로 표시됩니다.
- 변경되지 않은 항목 열에는 데이터베이스에 이미 있지만 관련 필드 값이 변경되지 않았기 때문에 업데이트되지 않은 통합 실행 중에 발견된 기록 이 표시됩니다.

주:
통합은 다음 네 가지 값 모두에 대해 0개의 결과로 실행됩니다. 새 **CI,**기존 **CI,**새 항목 및 업데이트된 항목은**Qualys** 통합 실행 목록에서 필터링됩니다.

Qualys 통합 실행 상태 차트 보고서

이름	설명
지난 30일 Qualys 결과	각 통합에 대해 완료된 통합 실행 수입니다. 성공한 실행과 실패한 실행을 모두 표시합니다. 시각적 개체 막대에서 실행합니다.

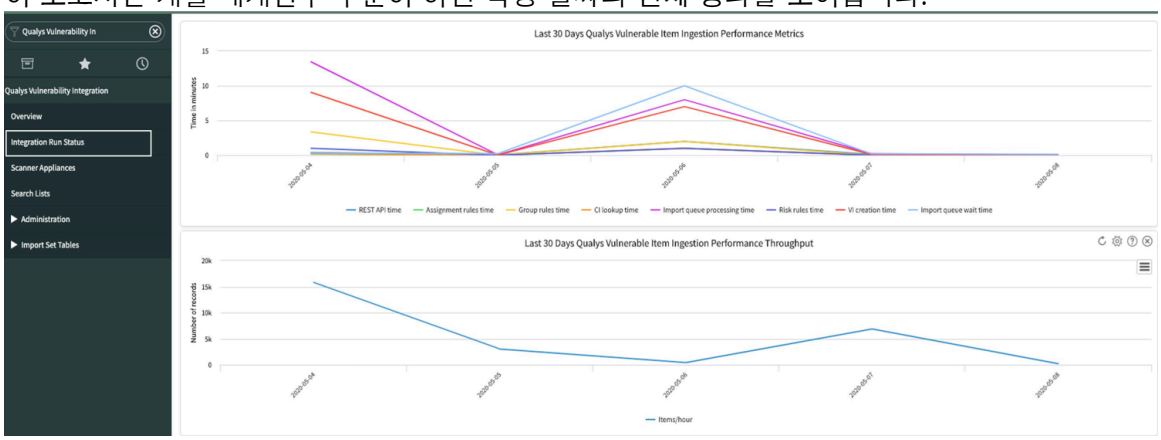
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Qualys 통합 실행 상태 차트 보고서

이름	설명
지난 30일 Qualys 신규 VI	지난 30일 동안 임포트한 새 기록 수입니다. 정수로 표시됩니다.
지난 30일 Qualys 업데이트된 VI	지난 30일 동안 임포트한 업데이트된 기록 수입니다. 정수로 표시됩니다.
지난 30일 Qualys 중복	지난 30일 동안 임포트된 중복 기록 수입니다. 정수로 표시됩니다.
Qualys 통합 실행	통합 실행 기록이 목록에 표시됩니다. 주: **V16.1:** 이 통합에 대한 탐지를 확인하려면 탐지 또는 결과를 ServiceNow 테이블의 탐지 데이터와 *sn_vul_detection* 비교합니다. 통합이 진행되는 동안 탐지 또는 발견 개수가 변경될 수 있습니다. 이 보고서는 통합 실행이 완료된 후 인스턴스의 "종료 날짜 카운트" 열에 탐지 횟수를 표시합니다.
지난 30일 Qualys 취약한 항목 수집 성과 메트릭	지난 30일 동안과 비교하여 취약한 항목에 대한 일일 성과 메트릭입니다.
지난 30일 Qualys 취약한 항목 수집 성능 처리량	지난 30일 동안 호스트 탐지 통합에 대해 측정된 일일 취약한 항목 수집 처리량입니다 Qualys .

이 데이터를 처리하는 데 걸린 데이터 양 및 시간과 같은 여러 요인이 통합 실행의 성능에 영향을 줄 수 있습니다. 두 그래프는 성과 메트릭을 비교합니다.

- Qualys 취약한 항목 수집 성과 메트릭: 지난 30일 동안 취약한 항목에 대한 담당 규칙, 그룹 규칙, 위험 규칙, 큐 대기 시간, 큐 처리 시간 및 기타 통계에 대한 일일 성과 메트릭을 비교하여 성능 편차의 원인을 식별합니다. 성과는 각 활동에 소요된 시간을 기준으로 계산됩니다. 이러한 매개변수는 통합 실행 수준에서 계산되고 연결됩니다. 각 매개변수는 쉽게 식별할 수 있도록 색상으로 구분되어 있습니다.
- Qualys 취약한 항목 수집 성능 처리량: 호스트 탐지 통합에 Qualys 대한 일일 취약한 항목 수집 처리량을 비교합니다. 처리량은 시간당 항목 단위로 측정됩니다. 이 보고서는 개별 매개변수 수준이 아닌 특정 날짜의 전체 성과를 보여줍니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Qualys 데이터 변환

Qualys에서 검색된 데이터는 일련의 데이터 소스 및 변환을 통해 처리됩니다.

에 대한 Qualys Vulnerability Integration 대부분의 변환은 변환 스크립트를 사용하여 수행됩니다. 이러한 스크립트는 내부용이므로 삭제하지 않는 것이 좋습니다. 수정하려면 코딩이나 고급 ServiceNow 또는 Qualys Vulnerability Integration 전문 지식이 필요합니다. 나머지 맵은 이 섹션에 나열되며 필드 맵을 사용합니다.

주:
설치하는 동안 임포트된 Qualys Cloud Platform 심각도 수준을 표준 ServiceNow 심각도 수준으로 변환하는 정규화된 심각도 맵이 정규화된 심각도 매핑 모듈에 설치됩니다 취약성 대응 . 자세한 내용은 취약성 대응 심각도 맵 생성 문서를 참조하십시오.

동적 검색 목록 임포트

Qualys 동적 검색 목록 변환 맵은 Qualys 동적 검색 목록을 변환하고 임포트하는 데 사용됩니다. 이 변환을 변경하면 동적 검색 목록이 처리되어 시스템에 삽입되는 방식이 변경됩니다.

이 변환 맵에 액세스하려면 다음으로 이동하십시오. **Qualys** 취약성 통합 〉 임포트 세트 테이블 〉 동적 검색 목록 임포트.

테이블에는 현재 변환 중인 필드가 표시됩니다.

Qualys 동적 검색 목록 변환 맵 필드

소스 필드	대상 필드	설명
u_id	ID	Qualys 동적 검색 목록의 식별자로 사용됩니다.
〔스크립트〕	list_type	검색 목록의 유형입니다. 동적은 동적 검색 목록 변환의 기본값입니다.
u_title	직위	이 검색 목록에 대한 Qualys의 이름입니다.

필드 매핑 외에도 변환 프로세스 중에 실행되는 변환 스크립트도 있습니다.

다음 표에서는 이 스크립트의 실행 시기와 용도를 보여줍니다.

Qualys 동적 검색 목록 변환 맵 스크립트 타이밍 및 목적

스크립트가 실행될 때	스크립트의 목적
onAfter(임포트 세트가 변환을 완료한 후)	검색 목록과 관련 취약성 간의 관계를 만듭니다. 내부용입니다. 수정하거나 삭제하지 않는 것이 좋습니다.

정적 검색 목록 임포트

Qualys 정적 검색 목록 변환 맵은 Qualys 정적 검색 목록을 변환하고 임포트하는 데 사용됩니다. 이 변환을 변경하면 정적 검색 목록이 처리되어 시스템에 삽입되는 방식이 변경됩니다.

이 변환 맵에 액세스하려면 다음으로 이동하십시오. **Qualys** 취약성 통합 〉 임포트 세트 테이블 〉 정적 검색 목록 임포트.

테이블에는 현재 변환 중인 필드가 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Qualys 정적 검색 목록 변환 맵 필드

소스 필드	대상 필드	설명
u_id	ID	Qualys 정적 검색 목록의 식별자로 사용됩니다.
u_title	직위	이 검색 목록에 대한 Qualys의 이름입니다.
〔스크립트〕	list_type	검색 목록의 유형입니다. 정적은 정적 검색 목록 변환의 기본값입니다.

필드 매핑 외에도 변환 프로세스 중에 실행되는 변환 스크립트도 있습니다.

다음 표에서는 이 스크립트의 실행 시기와 용도를 보여줍니다.

Qualys 정적 검색 목록 변환 맵 스크립트 타이밍 및 목적

스크립트가 실행될 때	스크립트의 목적
onAfter(임포트 세트가 변환을 완료한 후)	검색 목록과 관련 취약성 간의 관계를 만듭니다. 내부용입니다. 수정하거나 삭제하지 않는 것이 좋습니다.

자산 그룹 임포트

Qualys 자산 그룹 장치 변환 맵은 스캐너 장치 기록을 작성하기 위해 Qualys 자산 그룹 데이터를 변환하는 데 사용됩니다. 이 변환을 변경하면 스캐너 장치를 만들고 수정하는 방법이 변경됩니다.

이 변환 맵에 액세스하려면 다음으로 이동하십시오. **Qualys** 취약성 통합 〉 임포트 세트 테이블 〉 자산 그룹 임포트.

테이블에는 현재 변환 중인 필드가 표시됩니다.

Qualys 자산 그룹 변환 맵 필드

소스 필드	대상 필드	설명
u_id	ID	Qualys 자산 그룹의 식별자로 사용됩니다.
〔스크립트〕	수동	대상 기록이 생성된 방법을 결정하는 스크립팅된 값입니다. 변환을 통해 생성된 경우 이 필드는 항상 false입니다.
〔스크립트〕	ip	변환되는 자산 그룹과 연결된 IP 주소입니다.
u_default_appliance_id	appliance_id	이 자산 그룹의 기본 장치에 대한 Qualys 장치 식별자입니다.
u_title	asset_group_name	Qualys 자산 그룹의 이름입니다.

필드 매핑 외에도 변환 프로세스 중에 실행되는 변환 스크립트도 있습니다.

다음 표에서는 이 스크립트의 실행 시기와 용도를 보여줍니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Qualys 자산 그룹 변환 맵 스크립트 타이밍 및 목적

스크립트가 실행될 때	스크립트의 목적
onBefore(임포트 세트가 변환을 완료하기 전)	자산 그룹을 제한하는 스크립트는 기본 장치와 매핑된 IP 주소 집합이 있는 자산 그룹으로만 임포트합니다. 내부용입니다. 수정하거나 삭제하지 않는 것이 좋습니다.

장치 임포트

Qualys 어플라이언스 변환 맵은 Qualys 어플라이언스 데이터를 어플라이언스 기록으로 변환하는 데 사용됩니다. 이는 자산 그룹 임포트에서 처음에 생성될 어플라이언스 기록을 업데이트하는 데 사용됩니다. 이 변환을 변경하면 장치 레코드가 장치 세부 정보로 업데이트되는 방식이 변경됩니다.

이 변환 맵에 액세스하려면 다음으로 이동하십시오. **Qualys** 취약성 통합 〉 임포트 세트 테이블 〉 장치 임포트.

테이블에는 현재 변환 중인 필드가 표시됩니다.

Qualys 어플라이언스 변환 맵 필드

소스 필드	대상 필드	설명
u_name	appliance_name	Qualys 스캐너 장치의 이름입니다.
u_status	appliance_status	Qualys 스캐너 장치의 마지막으로 보고된 상태입니다.
u_id	appliance_id	Qualys 장치 식별자입니다.

필드 매핑 외에도 변환 프로세스 중에 실행되는 변환 스크립트도 있습니다.

다음 표에서는 이 스크립트의 실행 시기와 용도를 보여줍니다.

Qualys 어플라이언스 변환 맵 스크립트 타이밍 및 목적

스크립트가 실행될 때	스크립트의 목적
onBefore(임포트 세트가 변환을 완료하기 전)	지정된 ID의 기기 이름 및 상태를 업데이트하는 데 사용됩니다. 내부용입니다. 수정하거나 삭제하지 않는 것이 좋습니다.

Qualys REST 메시지

Qualys REST 메시지는 Qualys API를 호출하는 데 사용됩니다.

의 버전 12.9.2 Qualys부터 기본 인증 또는 OAuth 중에서 선택할 수 있는 옵션이 있습니다. 인스턴스 매개변수 Qualys Cloud 인증 방법은 기본 인증에 대해 미리 구성되어 있습니다. OAuth를 사용하려면 통합 인스턴스 매개변수를 수정한 후 OAuth에 대한 REST 메시지를 직접 설정해야 합니다.

Qualys 호스트 탐지 **REST** 메시지

Qualys 호스트 탐지 REST 메시지는 Qualys 호스트 탐지 통합을 위해 호스트 목록 탐지 API를 처음 호출합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Qualys 호스트 탐지 **REST** 메시지 매개변수

매개변수 이름	값	설명
작업	list	요청된 작업의 유형을 나타냅니다. 필수 매개변수입니다. 변경할 필요가 없습니다.
output_format	XML	Qualys에서 반환되는 보고서의 형식을 설정합니다. 다양한 스크립트 및 변환은 XML을 가정하므로 값을 변경하지 않는 것이 좋습니다.
detection_processed_after	${lastScanDate}	특정 날짜 및 시간 후에 탐지 상태가 변경된 탐지만 표시합니다. 변경되지 않은 탐지의 경우 이 날짜는 마지막 탐지 날짜에 적용됩니다.
truncation_limit	500	요청에 따라 데이터를 검색할 호스트 수입니다. 이 매개변수는 페이지 매김 목적으로 사용됩니다. 기본값은 500이지만 더 크거나 작은 값을 사용할 수 있습니다. 시스템 부하가 크게 증가하므로 100 미만으로 설정하지 마십시오. 값이 작을수록 Qualys API에 대한 호출이 더 많이 필요하며, 값이 클수록 처리할 결과 집합과 잠재적인 데이터 검색/처리 시간 초과가 발생합니다.
상태	새로 만들기, 고정, 활성, 다시 열림	Qualys에서 검색할 탐지 상태입니다. 기본값은 모든 상태를 검색하는 것입니다. 대규모 데이터 끌어오기(주로 초기 데이터 끌어오기)의 경우 이 목록에서 고정 상태를 제외하는 것이 좋습니다. 시스템에 이미 있는 취약성을 업데이트할 때 고정 상태를 포함하는 것이 중요합니다.

Qualys 호스트 탐지 페이지 매김 **REST** 메시지

호스트 탐지 페이지 매김 REST 메시지는 호스트 탐지 API에 대한 페이지 매김 요청을 처리합니다.

기본 호스트 검색이 실행될 때 Qualys API가 데이터의 다음 페이지를 가져오는 URL을 제공하는 경우 이 REST 메시지는 해당 추가 데이터를 검색합니다. 이 데이터는 호스트 탐지 페이지 매김 핸들러에서 사용됩니다.

호스트 탐지 페이지 매김 REST는 특수한 REST 메시지이며 수정할 수 없습니다.

Qualys 지식베이스(백필) **REST** 메시지

Qualys 지식베이스(백필) REST 메시지는 Qualys 지식베이스 통합에 대한 취약성 데이터의 마지막으로 수정된 타임스탬프를 기반으로 Qualys 지식베이스 데이터를 검색합니다.

REST 메시지 메서드 기록을 변경하면 지식베이스 정보를 검색하기 위해 Qualys에 대한 요청에 영향을 미칩니다.

다음 표에서는 전송되는 요청 매개변수를 보여 줍니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Qualys 기술 자료(백필) **REST** 메시지 매개변수

매개변수	값	설명
작업	list	요청 중인 작업의 유형을 나타냅니다. 필수 매개변수입니다. 변경은 권장되지 않습니다.
상세 정보	모두	검색된 취약성에 대해 표시되는 상세 정보 수준을 나타냅니다. 필요에 따라 수정해도 안전합니다.
id	${qids}	Qualys에서 검색할 QID를 지정합니다. 코드에서 참조됩니다. 수정은 권장되지 않습니다.

Qualys 기술 자료(날짜 기반) **REST** 메시지

Qualys 기술 자료(날짜 기반) REST 메시지는 취약성 데이터의 마지막으로 수정된 타임스탬프를 기반으로 Qualys 기술 자료 데이터를 검색하는 데 사용됩니다. 이 메시지는 Qualys 기술 자료 통합에서 사용됩니다.

REST 메시지 메서드 기록을 변경하면 지식베이스 정보를 검색하기 위해 Qualys에 대한 요청에 영향을 미칩니다.

다음 표에서는 전송되는 요청 매개변수를 보여 줍니다.

Qualys 기술 자료(날짜 기반) **REST** 메시지 매개변수

소스 필드	대상 필드	설명
작업	list	요청된 작업의 유형을 나타냅니다. 필수 매개변수입니다. 변경은 권장되지 않습니다.
상세 정보	모두	검색된 취약성에 대해 표시되는 상세 정보 수준을 나타냅니다. 필요에 따라 수정해도 안전합니다.
last_modified_after	${dateStart}	기록 데이터 검색을 시작할 시기를 나타냅니다. 코드에서 시작 시간을 결정하고 페이지 매김을 지원하는 데 사용됩니다. 수정 또는 제거는 권장되지 않습니다.
last_modifiedbefore	${dateEnd}	기록 데이터 검색을 종료할 시기를 나타냅니다. 코드에서 종료 시간을 결정하고 페이지 매김을 지원하는 데 사용됩니다. 수정 또는 제거는 권장되지 않습니다.

Qualys 티켓 **REST** 메시지

Qualys 티켓 REST 메시지는 Qualys 티켓 통합을 위한 Qualys 티켓 정보를 검색합니다. REST 메시지 메서드 기록의 변경은 티켓 정보를 검색하기 위해 Qualys에 대한 요청에 영향을 미칩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테이블에 전송되는 요청 매개변수가 표시됩니다.

Qualys 티켓 **REST** 메시지 매개변수

매개변수 이름	값	설명
modified_since_datetime	${lastRunDatetime}	통합의 마지막 실행 날짜와 데이터를 끌어올 날짜를 나타냅니다. 코드에서 사용됩니다. 변경은 권장되지 않습니다.
since_ticket_number	${lastTicketNumber}	Qualys에서 마지막으로 검색된 티켓을 나타냅니다. 페이지 매김에 사용됩니다. 변경은 권장되지 않습니다.
show_vuln_details	1	취약성 상세 정보를 검색할지 여부를 나타냅니다.

취약성 인스턴스를 기반으로 **Qualys** 탐지 분할

Vulnerability Response를 사용하면 Qualys 스캐너에서 탐지를 분할하여 탐지된 각 취약성 인스턴스에 대해 고유한 취약한 항목(VIT)을 생성할 수 있습니다. 이는 정정 팀에 보다 정확한 할당을 지원하고 취약성 관리 및 추적을 개선합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
Qualys 스캐너 페이로드에는 증명 상세 정보가 있는 탐지 데이터가 포함됩니다. 증명의 각 경로는 취약성 인스턴스를 식별하고 분할하는 데 사용됩니다. 페이로드의 출력 태그는 취약성의 위치를 나타내므로 탐지를 정확하게 분리하고 관리할 수 있습니다.

프로시저

1. 탐지 분할 사용
   a. 외부 공급업체 통합 테이블 [sn_sec_int_integration]로 이동합니다.
   b. `Qualys #### ####` 기록을 엽니다.
   c. `Include proof VI key`을 *true*로 설정합니다.
   d. 레코드를 저장합니다.
2. 옵션: 탐지 분할에서 특정 QID 제외
   a. 시스템 속성 [sn_vul_qualys.skip_split_detection_ids]를 엽니다.
   b. 값 필드에 분할에서 제외할 쉼표로 구분된 QID 목록을 입력합니다.

      주:
      기본적으로 QID-989920, QID-993308, QID-5001711, QID-5001632는 결과의 양으로 인해 분할에서 제외됩니다.

   c. 속성을 저장합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 분할을 위해 QID가 나열되는지 확인
   a. 증명 핵심 취약성 목록 테이블 [sn_vul_proof_key_vulnerability_list]로 이동합니다.
   b. 분할하려는 QID가 나열되는지 확인합니다.

결과
`Qualys ### ## ###` 실행한 후에는 탐지가 증명에 따라 분할되어 각 취약성 인스턴스에 대한 개별 취약한 항목(VIT)을 생성합니다. 각 탐지가 별도의 기록으로 표시되는 취약성 항목 탐지 테이블 [sn_vul_detection_list]에서 결과를 확인할 수 있습니다.

앱과 함께 설치되는 구성요소 **Qualys Vulnerability Integration**

다음 역할, 통합 작업 및 테이블이 와 Qualys Vulnerability Integration함께 설치됩니다.

> **주:**
> 애플리케이션 파일 테이블에는 이 애플리케이션과 함께 설치되는 구성요소가 나열됩니다. 이 테이블에 액세스하는 방법에 대한 지침은 애플리케이션과 함께 설치되는 구성요소 찾기 를 참조하십시오.

애플리케이션과 함께 설치된 구성요소에 대해 필터링된 목록 보기

애플리케이션과 함께 설치되는 역할, 예약된 작업 및 테이블만 표시되도록 애플리케이션 파일 테이블을 필터링합니다. 해당 파일이 인스턴스와 메타데이터 테이블에 로드되도록 이러한 구성요소를 보려는 애플리케이션을 설치해야 합니다. 다음 단계에 따라 애플리케이션 파일 테이블에서 필터링된 목록을 봅니다.

1. 필터 탐색기에서 **sys_metadata.list** 를 입력하여 메타데이터 테이블로 이동합니다.
2. 조건 작성기(필터 아이콘)를 선택하고 애플리케이션 〉 다음과 같음 다음에 애플리케이션 이름이 표시됩니다. 예: 애플리케이션 〉 다음과 같음 〉 취약성 대응.
3. 조건 작성기에서 두 번째 필터를 추가하려면 **AND**를 선택한 뒤 클래스 〉 다음 중 하나 을 클릭하고 목록에서 역할, 예약된 작업 또는 테이블 클래스 중 하나를 선택합니다.
4. 실행을 선택합니다.

선택한 클래스의 결과가 필터링된 목록에 표시됩니다.

설치되는 역할

역할 이름 **[name]**	설명	포함하는 역할
sn_vul_qualys.읽기	기록에 Qualys Vulnerability Integration 대한 읽기 권한이 있습니다.	
sn_vul_qualys.user	에 대한 사용자입니다 Qualys Vulnerability Integration. 기록을 읽고 쓸 수 있습니다.	sn_vul_qualys.읽기
sn_vul_qualys.admin	관리자.Qualys Vulnerability Integration 예를 들어 통합 시작 날짜를 수정하고 일부 고급 구성 설정을 수행할 수 있습니다.	• sn_vul_qualys.user • sn_vul.vulnerability_analyst
sn_vul.configure_qualys_integration	구성할 수 있는 항목 Qualys Vulnerability Integration	sn_vul_qualys.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설치되는 통합 작업

통합 작업	설명
Qualys 정적 검색 목록 통합	취약한 항목을 찾기 위해 검색 목록을 동기화 Qualys 합니다. 정적 목록 유형 기록만 조회합니다.
Qualys 포괄적인 호스트 탐지 통합	호스트에서 취약성 데이터를 Qualys 검색하고 인스턴스에서 처리합니다. 호스트 검색 API에 대한 REST 메시지 호출을 조정합니다. 이 통합의 출력은 취약 항목입니다. 이 통합은 취약성의 모든 상태(신규, 고정됨, 활성 및 다시 열림)를 임포트합니다. 기본적으로 이 통합은 비활성 상태이며 매주 실행됩니다. 주: 이 통합이 활성화되면 일별 종합 작업은 신규, 고정 및 다시 열림 상태만 임포트합니다.
Qualys 호스트 목록 통합	일주일에 한 번씩 Qualys 인증 및 인증되지 않은 호스트 스캔 데이터와 호스트 태그를 검색하여 인스턴스의 검색된 항목 모듈에 저장합니다. 최근에 스캔되지 않은 자산을 식별하는 데 도움이 됩니다.
Qualys 호스트 탐지 통합	호스트에서 취약성 데이터를 Qualys 검색하고 인스턴스에서 처리합니다. 호스트 목록 탐지 API에 대한 REST 메시지 호출을 조정합니다. 이 통합의 출력은 취약한 항목입니다. Qualys 이 통합에서 호스트 태그가 임포트됩니다.
Qualys 티켓 통합	티켓을 검색하여 Qualys 인스턴스에 추가합니다. 티켓 목록 API에 대한 REST 메시지 호출을 조정합니다. 설정이 티켓을 발생시키는 감지를 제한할 수 있기 때문에 Qualys 호스트 감지보다 티켓 수가 적은 경우가 많습니다.
Qualys 옵션 프로파일 목록 통합	제품에서 Qualys 옵션 프로파일을 검색합니다. 옵션 프로파일에는 인스턴스에서 스캔 ServiceNow AI Platform 을 시작할 때 필요한 스캔 설정이 포함됩니다.
Qualys 기기 목록 통합	에서 Qualys스캐너 장치 정보를 검색합니다.
Qualys 자산 그룹 통합	에서 Qualys자산 그룹 정보를 조회합니다. 자산 그룹은 일치하는 구성 항목을 스캔하는 데 사용할 스캐너 장치를 식별하는 데 사용됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

통합 작업	설명
Qualys 지식베이스(백필)	지식베이스 항목을 검색합니다 Qualys . 호스트 탐지 통합 후 실행되도록 예약되었습니다 Qualys . 호스트 탐지 통합에서 참조되었지만 시스템에 없는 QID로 인스턴스를 업데이트합니다.
Qualys 지식베이스	지식베이스 항목을 검색합니다 Qualys . 검색된 데이터는 취약성이 업데이트된 Qualys 날짜와 통합이 마지막으로 실행된 시간을 기준으로 합니다. 이 데이터는 이력 데이터를 인스턴스에 채우고 식별자(QID)가 Qualys 최신 상태인지 확인하는 데 유용합니다.
Qualys 동적 검색 목록 통합	취약한 Qualys 항목을 찾기 위해 검색 목록을 동기화하고 동적 목록 유형 기록을 검색합니다.
의 업데이트된 키에 대한 탐지 수정 Qualys	탐지를 식별하고 취약한 항목에 연결하는 방법을 제공한 해시된 필드 조합입니다 Qualys .
Qualys 네트워크 파티션 식별자로 기존 검색 항목 업데이트	기존 검색 항목을 업데이트합니다. 네트워크 파티션 식별자 세분성을 포함하도록 기존 Qualys 취약성 통합 데이터에 대한 CI가 생성되거나 업데이트됩니다.

설치되는 테이블

테이블	설명
검색 목록 취약성 sn_vul_qualys_m2m_search_list_vul	검색 목록과 취약성 간의 Qualys 매핑을 저장합니다.
Qualys 취약성 스캐너 sn_vul_qualys_scanner	다시 스캔 기능에 대한 스캐너 정보를 저장하기 위해 취약성 스캐너를 확장하는 테이블입니다 Qualys .
Qualys 검색 목록 sn_vul_qualys_search_list	검색 목록 통합으로 Qualys 검색된 검색 목록을 저장합니다.
Qualys 장치 임포트 sn_vul_qualys_appliance_imp	임포트 세트 행을 확장하는 테이블입니다. 필드 맵 변환을 건너뛰고 응답 첨부 파일이 onComplete 스크립트로 직접 처리됩니다.
Qualys CI sn_vul_qualys_ci	테이블은 더 이상 사용되지 않습니다.
호스트 탐지 페이지 매김 sn_vul_qualys_host_detection_pagination	테이블은 더 이상 사용되지 않습니다.
Qualys 통합 실행	테이블은 더 이상 사용되지 않습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테이블	설명
sn_vul_qualys_integration_run	
Qualys 통합 sn_vul_qualys_integration	취약성 통합을 확장하고 에 해당하는 모든 통합을 저장하는 테이블입니다 Qualys.
Qualys 정적 검색 목록 임포트 sn_vul_qualys_static_search_list_imp	임포트 세트 행을 확장하는 테이블입니다. 필드 맵은 데이터를 대상 테이블, Qualys 검색 목록으로 변환하는 데 사용됩니다.
Qualys 지식베이스 sn_vul_qualys_knowledge_base	임포트 세트 행을 확장하는 테이블입니다. 필드 맵 변환을 건너뛰고 응답 첨부 파일이 onComplete 스크립트로 직접 처리됩니다.
Qualys 티켓 목록 sn_vul_qualys_ticket_list_imp	임포트 세트 행을 확장하는 테이블입니다. 필드 맵 변환을 건너뛰고 응답 첨부 파일이 onComplete 스크립트로 직접 처리됩니다.
Qualys 옵션 프로파일 sn_vul_qualys_option_profile	에서 Qualys가져온 옵션 프로파일을 저장하는 테이블입니다. 이 테이블은 재스캔에 사용됩니다.
Qualys 동적 검색 목록 임포트 sn_vul_qualys_dynamic_search_list_imp	임포트 세트 행을 확장하는 테이블입니다. 필드 맵은 데이터를 대상 테이블, Qualys 검색 목록으로 변환하는 데 사용됩니다.
Qualys 임포트 세트 재실행 sn_vul_qualys_import_rerun	테이블은 더 이상 사용되지 않습니다.
Qualys 옵션 프로파일 임포트 sn_vul_qualys_option_profile_import	임포트 세트 행을 확장하는 테이블입니다. 필드 맵 변환을 건너뛰고 응답 첨부 파일이 onComplete 스크립트로 직접 처리됩니다.

Rapid7 취약성 통합 이해

데이터 ServiceNow# Rapid7 취약성 통합 웨어하우스 또는 Rapid7 InsightVM 제품에서 Rapid7 임포트한 데이터를 사용하여 잠재적으로 악의적인 위협의 영향과 우선순위를 파악하는 데 도움을 줍니다.

Rapid7 Nexpose센서는 데이터를 수집하여 데이터 웨어하우스(온프레미스) 또는 Rapid7 InsightVM (클라우드 기반) 제품에 자동으로 전송 Rapid7 하여 정보를 지속적으로 분석하고 상관 관계를 지정합니다. 와 ServiceNow# 취약성 대응 쉽게 통합되어 취약성을 CI 및 서비스에 매핑합니다. 인스턴스의 Rapid7 취약성 통합 취약성 데이터를 보강합니다.

Rapid7 통합은 데이터 웨어하우스 또는 Rapid7 InsightVM 제품과 상호작용 Rapid7 하는 엔트리포인트로, 예약된 작업으로 호출됩니다. 예약된 작업은 인스턴스를 다른 취약성 관리 시스템과 동기화된 상태로 유지하여 취약성 정정 수명주기를 단순화합니다. 예약된 작업은 지정된 순서대로 자동으로 실행됩니다. 예약된 개별 작업을 수동으로 실행할 수도 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

데이터 웨어하우스와 Rapid7 InsightVM 데이터 소스로 모두 Rapid7 사용하는 경우 중복 취약성 레코드의 위험이 있습니다.

주:
데이터 웨어하우스 통합 유형에서 **InsightVM** 유형으로 마이그레이션할 때 기존 데이터 웨어하우스 기록의 중복을 제거할 수 있습니다. 자세한 내용은 데이터 웨어하우스 기록 중복 Rapid7 취약성 통합 제거 문서를 참조하십시오.

취약성 통합 배포 Rapid7 InsightVM 가 여러 개 있는 경우 각 배포에 통합을 추가할 수 있습니다. 여러 외부 공급업체 배포 및 해당 취약성으로 식별된 자산이 CMDB와 통합되고 조정됩니다. 이러한 통합은 여러 배포 간에 스캔 프로세스가 겹치는 경우에도 발생합니다. 각 배포에서 소싱된 데이터가 식별되고 의 단일 인스턴스에서 취약성 대응사용할 수 있습니다.

주:
원래 취약성 통합을 삭제할 수는 없지만 사용하지 않도록 설정할 수는 있습니다. 비활성화된 템플릿에서 만든 통합은 기본적으로 비활성화됩니다.

각 통합 기록에 대해 구성된 실행 사용자가 있습니다. 이 사용자의 기본값은 VR입니다. 시스템. 이 값은 변경하지 마십시오.

사용 가능한 버전

의 릴리스 버전 Yokohama	릴리스 정보
Rapid7 취약성 통합 v13.6, 13.7	호환성 정보는 KB0856498 Vulnerability Response 호환성 매트릭스 및 릴리스 스키마 변경을 참조하십시오.

역할

Rapid7 취약성 통합 작업에는 다음 역할이 포함됩니다.

- sn_vul_r7.admin: 기록을 읽고, 쓰고, 삭제할 수 있습니다.
- sn_vul_r7.user: 기록을 읽고 쓸 수 있습니다.
- sn_vul_r7.read: 기록을 읽을 수 있습니다.

Rapid7 취약성 통합 통합

을(를 Rapid7 취약성 통합) 보려면 다음으로 이동하십시오. **Rapid7** 〉 관리 〉 통합.

기본 시스템에는 다음과 같은 통합이 포함됩니다.

Rapid7 데이터 웨어하우스 통합

통합	설명
Rapid7 취약성 통합	취약성 데이터를 Rapid7 Nexpose 검색하고 인스턴스에서 처리합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Rapid7 데이터 웨어하우스 통합

통합	설명
Rapid7 자산 목록 통합	데이터 웨어하우스에서 Rapid7 Nexpose 일주일에 한 번 스캔 데이터를 검색하여 인스턴스의 검색된 항목 모듈에 저장합니다. 마지막 스캔 날짜를 사용하여 최근에 스캔되지 않은 자산을 식별하는 데 도움이 됩니다. 의 취약성 대응검색된 항목 목록에서 마지막 스캔 시간을 확인합니다.
Rapid7 범주 통합	에서 Rapid7 Nexpose범주 정보를 검색합니다. 범주는 취약성에 대한 높은 수준의 분류를 제공합니다.
Rapid7 남용 통합	에서 익스플로잇 정보를 조회합니다 Rapid7 Nexpose.
Rapid7 맬웨어 키트 통합	에서 Rapid7 Nexpose맬웨어 키트 정보를 검색합니다.
Rapid7 참조 통합	CVE 또는 벤더별 취약성 참조와 같은 외부 권한 문서에 대한 참조를 검색합니다.
Rapid7 솔루션 통합	특정 취약성에 대한 권장 솔루션을 제공하는 에서 Rapid7 Nexpose솔루션 데이터를 검색합니다.
Rapid7 대체 솔루션 통합	다른 솔루션으로 대체되는 솔루션에 대한 정보를 검색합니다.
Rapid7 필수 솔루션 통합	다른 솔루션의 전제 조건인 솔루션에 대한 정보를 검색합니다. 이 통합이 실행되면 데이터 웨어하우스에서 Rapid7 솔루션 매핑과 필수 구성요소 솔루션을 가져옵니다. 주: 이 통합은 플러그인이 취약성 솔루션 관리 활성화된 경우에만 작동합니다.
Rapid7 취약성 솔루션 맵 통합	취약성과 솔루션을 연결하기 위해 매핑을 검색합니다.
Rapid7 취약한 항목 통합	인스턴스에서 취약한 항목 데이터를 Rapid7 Nexpose 검색하고 처리합니다. 이 통합의 출력은 취약한 항목입니다.
Rapid7 취약한 항목 해결 통합	종결 Rapid7 Nexpose 로 표시된 취약한 항목에 대한 정보를 검색하고 에서 해당 취약한 항목을 취약성 대응종결합니다.
Rapid7 사이트 통합	에서 Rapid7 Nexpose사이트 데이터를 조회합니다. 사이트는 스캔 대상인 자산의 모음입니다.
Rapid7 자산 목록 통합	데이터 웨어하우스에서 Rapid7 일주일에 한 번씩 호스트 태그와 스캔 데이터를 검색하여 인스턴스의 검색된 항목 모듈에 저장합니다. 마지막 스캔 날짜를 사용하여 최근에 스캔되지 않은 자산을 식별하는 데 도움이 됩니다. 의 검색된 항목 목록에서 마지막 스캔 시간 보기 취약성 대응

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Rapid7 데이터 웨어하우스 통합

통합	설명
Rapid7 포괄적인 취약한 항목 통합	마지막으로 성공한 통합 실행 이후 검사한 모든 구성 항목에 대한 모든 Rapid7 탐지를 임포트합니다. 가장 최근에 임포트한 데이터를 기반으로 부실 취약한 항목 자동 종결 모듈이 활성화되면 스캔 중에 최근에 발견되지 않은 취약한 항목이 자동으로 "종결"로 전환됩니다.

Rapid7 InsightVM 통합

통합	설명
Rapid7 취약한 항목 통합 — API	InsightVM에서 Rapid7 취약한 항목 데이터를 검색하고 인스턴스에서 처리합니다.
Rapid7 취약성 통합 — API	InsightVM에서 Rapid7 참조, 범주, 익스플로잇, 맬웨어 키트 및 취약성 데이터를 검색하고 인스턴스에서 처리합니다.
Rapid7 자산 목록 통합 - API	일주일에 한 번씩 Rapid7 InsightVM 호스트 태그와 스캔 데이터를 검색하여 인스턴스의 검색된 항목 모듈에 저장합니다. 마지막 스캔 날짜를 사용하여 최근에 스캔되지 않은 자산을 식별하는 데 도움이 됩니다. 의 취약성 대응검색된 항목 목록에서 마지막 스캔 시간을 확인합니다.
Rapid7 포괄적인 취약한 항목 통합 - API	마지막으로 성공한 통합 실행 이후 검사한 모든 구성 항목에 대한 모든 Rapid7 탐지를 임포트합니다. 가장 최근에 임포트한 데이터를 기반으로 부실 취약한 항목 자동 종결 모듈이 활성화되면 스캔 중에 최근에 발견되지 않은 취약한 항목이 자동으로 "종결"로 전환됩니다.
Rapid7 사이트 통합	제품에서 사이트 데이터를 조회합니다 Rapid7 InsightVM . 이 통합은 매주 00:00:00에 실행되도록 설정됩니다.

임포트하는 동안 아직 존재하지 않는 CVE 기록은 NVD 기록으로 생성되고 기본적으로 외부 공급업체 항목 Rapid7 에서 참조됩니다. 에 대한 Rapid7 템플릿 통합을 삭제할 수 없습니다. 대신 비활성화하십시오.

Rapid7용 서비스 그래프 커넥터

버전 2.0부터 Rapid7용 서비스 그래프 커넥터는 .ServiceNow# Store 자세한 내용은 Service Graph Connector for Rapid7 문서를 참조하십시오.

CI 조회 규칙

CI 조회 규칙은 취약한 항목 기록에서 구성 항목 필드를 채우는 방법을 결정합니다.

CI 조회 규칙의 작동 방식에 대한 자세한 내용은 다음 문서를 참조하십시오 외부 공급업체 취약성 통합에서 취약성 대응 구성 항목을 식별하기 위한 CI 조회 규칙.

조회 규칙을 만들거나 편집하려면 다음 문서를 참조하십시오 취약성 대응 CI 조회 규칙 생성.

주:
제거된 규칙은 복구할 수 없습니다. 기존 규칙을 제거하는 대신 새 규칙을 만들 때 비활성화하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

검색된 항목

이 모듈에는 취약한 항목 통합(데이터 웨어하우스 또는 InsightVM API) 및 자산 목록 통합 - API에서 Rapid7 임포트하는 동안 탐지된 Rapid7 구성 항목이 나열됩니다. 자산 목록 통합 - API는 Rapid7 마지막 통합 실행 이후 취약성이 있는지 검사한 모든 Rapid7 자산을 임포트합니다. 데이터 웨어하우스 자산 목록 통합이 Rapid7 포함됩니다.

> **주:**
> 이 목록의 기본 필터는 일치하지 않음으로 설정됩니다. 필터를 제거하여 임포트에서 검색된 모든 항목을 볼 수 있습니다.

검색된 항목 모듈에 대한 자세한 내용은 을 취약성 대응 참조하십시오검색된 항목.

호스트 태그

호스트 태그는 자산 목록 통합 - 에 대한 Rapid7 InsightVMAPI 통합의 Rapid7 일부로 임포트됩니다. 의 할당 및 정정 작업 규칙Rapid7 InsightVM에서 취약성 대응 필터링하는 데 주로 사용됩니다. 검색된 항목 양식에 표시됩니다.

호스트 태그

> **주:**
> Rapid7 모든 태그가 규칙에 존재할 수 있도록 그리고 취약한 항목을 임포트 및 그룹화하기 전에 할당 또는 정정 작업 규칙을 취약성 대응 생성하기 전에 자산 목록 통합 - API 통합을 실행해야 합니다.

- 태그 스토리지는 대/소문자를 구분하지 않습니다. **San Diego** 태그가 생성되면 호스트 태그 테이블에 **SAN DIEGO** 태그를 저장할 수 없습니다. 'San Diego'와 'SAN DIEGO'는 동일한 호스트 태그로 간주됩니다. 먼저 가져온 태그가 우선합니다.
- 정정 작업 규칙에서 호스트 태그를 그룹 키로 사용하면 예기치 않은 결과가 발생할 수 있습니다. 호스트 태그는 조건 작성기에서만 사용할 수 있습니다.
- 호스트 태그는 전역 시스템 속성 sn_vul.import_host_tags에 의해 제어됩니다. 이 속성은 기본적으로 true로 설정됩니다. 태그를 끄면 모든 인스턴스에서 태그가 꺼집니다.

사이트

사이트는 스캔 대상 자산의 모음입니다. 사이트는 대상 자산, 스캔 템플릿, 하나 이상의 스캔 엔진 및 기타 스캔 관련 설정(예: 일정 또는 경보)으로 구성됩니다. 사이트는 애플리케이션에 의해 Rapid7 관리됩니다.

Rapid7 취약성 통합 구성 중 사이트 필터링을 사용하면 임포트하는 동안 사이트별로 자산을 분류하고 요청할 수 있습니다. 임포트 필터링에 대한 자세한 내용은 을 참조하십시오 사이트를 기준으로 Rapid7 필터링 .

데이터 웨어하우스 및 Rapid7 InsightVM 사이트 통합은 Rapid7 사이트를 주간 예약 작업으로 임포트합니다.

목록에서 임포트한 사이트를 보려면 **Rapid7** 〉 사이트.

스캔으로 종결되지 않은 해결된 취약한 항목 다시 열기

인스턴스에서 "해결됨" ServiceNow AI Platform 으로 설정되었지만 후속 통합 실행에 의해 "종결/수정됨"으로 전환되지 않은 취약한 항목은 재스캔 중에 탐지되면 다시 열립니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

탐지의 경우 Rapid7 , 이제 인스턴스의 Rapid7 구성 페이지에서 해결된 VI를 기간별로 다시 여는 옵션을 사용할 수 있습니다. 활성화된 경우 VI가 '해결됨'으로 설정되었지만 후속 스캔에서 '종결/수정됨'으로 전환되지 않은 경우 입력한 일수 후에 다시 '오픈'으로 전환됩니다.

IRE(식별 및 조정 엔진)를 사용하여 **CI** 생성

기존 CI를 외부 공급업체 스캐너에서 임포트한 호스트와 일치시킬 수 없는 경우 식별 및 조정 엔진을 사용하여 새 CI를 만들 수 있습니다. CMDB CI Class Models 플러그인을 활성화하여 새 클래스를 사용하여 CI를 생성합니다. 그렇지 않으면 일치하지 않는 CI가 일치하지 않는 CI 클래스에 생성됩니다. 자세한 내용은 식별 및 조정 엔진을 사용하기 위한 취약성 대응 CI 생성 문서를 참조하십시오. 일치하지 않는 클라우드 자원의 분류를 기본 CI 클래스로 구성하는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 일치하지 않는 클라우드 자산에 대한 CI 클래스 업데이트 중.

취약한 항목 재스캔

플랫폼에서 재스캔 Rapid7 을 시작하여 예약된 스캔 주기 사이에 취약한 항목이 정정되었는지 확인합니다. 취약성 통합에 Rapid7 대한 재스캔 시작 문서를 참조하십시오.

스토어에서 앱 요청

ServiceNow Store 웹 사이트를 방문하면 사용 가능한 모든 앱을 확인하고 스토어에 요청을 제출하는 방법에 대한 정보를 참조할 수 있습니다. 출시된 모든 앱의 누적 릴리스 정보는 ServiceNow Store 버전 기록 릴리스 정보 를 참조하십시오.

Rapid7 솔루션 관리

플러그인을 Rapid7 활성화하면 취약성 솔루션 관리 데이터 웨어하우스와 Rapid7 InsightVM 취약성 Rapid7 솔루션 [sn_vul_solution] 테이블에 대한 솔루션이 모두 채워집니다. 그러나 플러그인을 활성화하지 않은 경우 Rapid7 취약성 통합 해당 플러그인은 취약성 솔루션 관리 그대로 작동하며 사용자 지정 [sn_vul_r7_solution] 테이블에서 솔루션을 임포트합니다. 자세한 내용은 Rapid7 솔루션 관리 문서를 참조하십시오.

준비 중 **Rapid7** 취약성 통합

성공적인 통합을 위해서는 통합 전 작업을 계획하고 신중하게 실행해야 합니다. 다음 작업을 수행하여 통합을 준비합니다. 여기서는 Rapid7 취약성 통합 사용자가 사용자 환경에서 데이터 웨어하우스 또는 Rapid7 InsightVM 제품 스캔을 잘 알고 실행 Rapid7 한다고 가정합니다.

필요한 역할: 관리자

스캐너는 Rapid7 애플리케이션에서 기본적으로 비활성화되어 있습니다 취약성 대응 . 이러한 애플리케이션을 소스로 사용하는 취약한 항목 또는 정정 작업에서 다시 검색을 수행하려고 하면 다시 검색 버튼을 사용할 수 없습니다.

에서 애플리케이션을 ServiceNow# Store 다운로드하여 Rapid7 취약성 통합 인스턴스에 설치하기 전에 통합 유형 및 설정 정보에 대한 다음 정보를 검토하십시오.

에서 Rapid7 취약성 통합 사용할 수 있는 통합에는 두 가지 유형이 포함됩니다.ServiceNow# Store

- Rapid7 InsightVM
- Rapid7 데이터 웨어하우스

데이터 Rapid7 웨어하우스 유형:

- 데이터 웨어하우스 서버 URL 및 인증 자격 증명이 Rapid7 필요합니다.
- MID 서버 필요

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- PostgresSQL 드라이버를 사용하여 데이터 웨어하우스에서 쿼리를 실행합니다.
- 여러 인스턴스를 지원하지 않습니다.

Rapid7 InsightVM 통합 유형:

- 클라우드 기반이며 REST API를 사용합니다. 이 통합에는 Insight 계정 내의 Rapid7 API 키가 필요합니다.
- 여러 인스턴스를 지원합니다.

이러한 통합 유형의 설정 요구 사항에 대한 자세한 내용은 (데이터 웨어하우스) 문서를 통합을 위한 Rapid7 InsightVM 설정 참조하십시오 데이터 웨어하우스 통합을 위한 Rapid7 설정 .

데이터 웨어하우스 통합을 위한 **Rapid7** 설정

데이터 웨어하우스 통합은 Rapid7 에 Rapid7 취약성 통합 Rapid7 취약성 통합포함된 통합 유형 중 하나입니다.

시작하기 전에

데이터 웨어하우스 통합을 실행하기 Rapid7 전에 다음 설정 작업을 완료합니다.

- Rapid7 데이터 웨어하우스 추가 기능을 가져옵니다. 이 추가 기능을 획득하고 설치하려면 Rapid7 웹 사이트 및 설명서를 참조하십시오.
- 최신 PostgresSQL 드라이버를 가져옵니다. 최신 드라이버로 https://jdbc.postgresql.org/ 이동하여 다운로드합니다.
- 데이터 웨어하우스에 대한 쿼리를 실행할 MID 서버. MID 서버 설정 방법에 대한 자세한 내용은 MID 서버를 참조하십시오.

  데이터 웨어하우스 이름을 기록해 둡니다. Rapid7 데이터 웨어하우스 통합 유형은 독립 실행형 MID Server만 지원합니다. 클러스터된 MID Server는 지원되지 않습니다.

- Rapid7 데이터 웨어하우스 서버 URL 및 인증 자격 증명을 가져오고 액세스할 수 있도록 합니다.

필요한 역할: 시스템 관리자 〔admin〕가 앱을 다운로드하여 설치합니다. sn_vul.vulnerability_admin 또는 sn_vul.admin은 구성을 감독하고 예상 결과를 검증합니다.

프로시저

1. 애플리케이션을 설치할 Rapid7 취약성 통합 인스턴스에 로그인합니다ServiceNow AI Platform.
2. 이전에 나열된 설정 작업에서 다운로드한 PostgreSQL JAR 파일을 설치합니다.

   a. 인스턴스에서 ServiceNow AI Platform 다음으로 이동합니다. 모두 〉 **MID** 서버 〉 **JAR** 파일.

   b. 새로 만들기를 클릭합니다.

   c. 이전에 다운로드한 PostgresSQL 드라이버의 이름을 입력합니다.

      필요한 경우 버전, 소스 및 설명 정보를 입력합니다. 활성 확인란을 선택한 상태로 둡니다.

   d. 헤더에 종이 클립 아이콘, 사용하여 다운로드한 JAR 파일을 첨부합니다.

   e. 제출을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

데이터 웨어하우스 통합 설정을 완료했습니다 Rapid7 . 통합에 대한 Rapid7 InsightVM 요구 사항을 검토하지 않은 경우 설치하기 Rapid7 취약성 통합전에 및 을 참조하십시오 통합을 위한 Rapid7 InsightVM 설정준비 중 Rapid7 취약성 통합.

권리를 얻고, 다운로드하고, 설치하는 Rapid7 취약성 통합단계는 문서를 참조하십시오 Rapid7 취약성 통합 설치.

통합을 위한 **Rapid7 InsightVM** 설정

통합 Rapid7 InsightVM 은 에 Rapid7 취약성 통합 Rapid7 취약성 통합포함된 통합 유형 중 하나입니다.

시작하기 전에

통합을 실행하기 Rapid7 InsightVM 전에 다음 설정 작업을 완료합니다.

필요한 역할: 시스템 관리자 〔admin〕가 앱을 다운로드하여 설치합니다. sn_vul.vulnerability_admin 또는 sn_vul.admin은 구성을 감독하고 예상 결과를 검증합니다.

프로시저

1. Rapid7 InsightVM 통합 유형의 경우 지역 및 API 키를 준비합니다.
   적절한 지역 및 API 키를 얻으려면 문의하십시오 Rapid7 .
   통합 설정을 완료했습니다 Rapid7 InsightVM . 데이터 웨어하우스 통합에 Rapid7 대한 요구 사항을 검토하지 않은 경우 를 설치하기 Rapid7 취약성 통합전에 및 준비 중 Rapid7 취약성 통합을 참조하십시오데이터 웨어하우스 통합을 위한 Rapid7 설정.
2. 권리를 얻고, 다운로드하고, 설치하는 Rapid7 취약성 통합단계는 문서를 참조하십시오 Rapid7 취약성 통합 설치.

Rapid7 취약성 통합 설치

통합이 취약성 대응제대로 통합되도록 통합 설정 단계를 완료한 후에는 권리를 얻고 인스턴스에 애플리케이션을 ServiceNow AI Platform# 다운로드하여 설치합니다.

시작하기 전에

필요한 역할: admin 다운로드 및 설치의 경우 sn_vuln.admin은 구성을 감독하고 예상 결과를 검증합니다.

1. 의 통합을 위한 Rapid7 InsightVM 설정 통합 유형 및 설정 요구 사항에 Rapid7 취약성 통합대한 자세한 내용은 를 데이터 웨어하우스 통합을 위한 Rapid7 설정 참조하십시오준비 중 Rapid7 취약성 통합.
2. 다운로드 및 설치 전에 다음 설정 검사 목록을 완료합니다. 이러한 설정 작업은 원활한 설치 및 구성을 위해 필요합니다.
3. 애플리케이션이 활성화되면 아래 나열된 단계에 따라 를 Rapid7 취약성 통합구성합니다.

> **주:**
> 이 프로세스는 프로덕션 인스턴스에 다운로드된 애플리케이션에만 적용됩니다. 애플리케이션을 비프로덕션 또는 개발 인스턴스에 다운로드하는 경우에는 권리를 얻을 필요가 없습니다. 로 애플리케이션 활성화 ServiceNow Store계속 진행합니다.

작업 설정	설명
애플리케이션이 설치되고 활성화되었는지 취약성 대응 확인합니다.	이 애플리케이션이 활성화되었는지 확인하려면 다음으로 이동하십시오. 구독 관리 〉 구독

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업 설정	설명
	인스턴스에 있습니다. 목록에 조직이 구매한 구독이 표시됩니다. 애플리케이션이 설치 및 활성화되지 않은 경우 을 참조하십시오 취약성 대응 설치.
인스턴스에 필요한 ServiceNow AI Platform 역할이 있는지 확인합니다.	예상 결과의 설치, 구성 및 검증에 필요한 역할은 다음과 같습니다. 가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응. • 시스템 관리자 〔admin〕가 앱을 설치합니다. 아직 할당되지 않은 경우 관리자는 취약성 관리자 [sn_vul.vulnerability_admin or sn_vul.admin] 역할을 할당합니다. • 취약성 관리자는 구성을 감독하고 예상 결과를 검증합니다. Rapid7 관리자 역할은 (VR) 애플리케이션에서 관리 역할이 취약성 대응 할당되면 상속됩니다.
임포트하려는 취약한 항목 수에 따라 인스턴스 크기를 조정하십시오.	인스턴스 크기가 작으면 로드 시간이 길어질 수 있습니다. 인스턴스 크기를 모르는 경우 에 문의하십시오 고객 서비스 및 지원.
필터링 설정	필터링을 사용하여 초기 임포트에 대한 항목 수를 제한하고 후속 임포트에서 필터를 조정하여 배포를 단계적으로 수행합니다.
취약성 계산기 사용 안 함	정의한 다른 모든 것 외에 취약성 계산기를 사용하지 않는 경우. 사용하지 않는 경우 기본 취약성 계산기 사용 안 함 취약성 계산기는 취약한 항목 기록이 생성되거나 업데이트될 때마다 실행되며 초기 임포트 성능에 영향을 줄 수 있습니다.
실행 사용자에 대한 기본값 유지	각 통합 기록에 대해 구성된 실행 사용자가 있습니다. 이 사용자의 기본값은 VR입니다. 시스템. 이 값은 변경하지 마십시오.
호스트 태그 사용	할당 또는 정정 작업 규칙에서 취약성 대응 호스트 태그를 사용할 계획이라면 규칙을 생성하기 전에 Rapid7 자산 목록 통합을 실행합니다.
기존 데이터 기록 중복 취소	데이터 웨어하우스 통합 유형에서 **InsightVM** 유형으로 마이그레이션할 때 기존 데이터 웨어하우스 기록의 중복을 제거할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업 설정	설명
	자세한 내용은 데이터 웨어하우스 기록 중복 Rapid7 취약성 통합 제거 문서를 참조하십시오.

프로시저

1. 애플리케이션을 설치할 Rapid7 취약성 통합 인스턴스에 로그인합니다.
2. 로 ServiceNow Store 이동하여 로그인합니다.
3. 에서 ServiceNow Store애플리케이션을 검색합니다 Rapid7 취약성 통합 .

   주:
   ServiceNow Store에서는 애플리케이션을 Integration for Security Operations라고 Rapid7 합니다. 이 애플리케이션에는 구독이 필요합니다.

4. 애플리케이션 타일을 클릭합니다.
   설치 중인 애플리케이션에 대한 자세한 정보가 표시됩니다.

   주:
   해당하는 경우 다른 요구 사항 및 종속성 섹션을 읽어보십시오.

5. 앱 요청을 클릭하고 Now Support 로그인 자격 증명을 입력합니다.
6. 가져오기를 클릭합니다.
7. 인스턴스 이름 및 인스턴스 이유를 입력하고 인스턴스 확인을 클릭합니다.
8. 요청을 클릭합니다.
   자세한 설치 지침이 포함된 이메일을 받게 됩니다.
9. 인스턴스에서 ServiceNow AI Platform 다음으로 이동합니다. 시스템 애플리케이션 〉 모든 애플리케이션 〉 모두.
10. 애플리케이션을 찾아서 선택한 다음 설치를 클릭합니다.
    설치 대화 상자에 종속성 상태가 표시됩니다. 의존성 애플리케이션이 필요한 경우 필요한 애플리케이션이 표시됩니다. 대화 상자의 프롬프트에 따라 인스턴스에 애플리케이션을 설치합니다 Rapid7 취약성 통합 .

    주:
    이제 취약성 관리자가 애플리케이션 구성을 완료할 수 있습니다. Rapid7 취약성 통합 구성 문서를 참조하십시오.

Rapid7 취약성 통합 구성

응용 Rapid7 취약성 통합 프로그램이 설치되고 활성화된 ServiceNow AI Platform#후에 구성합니다.

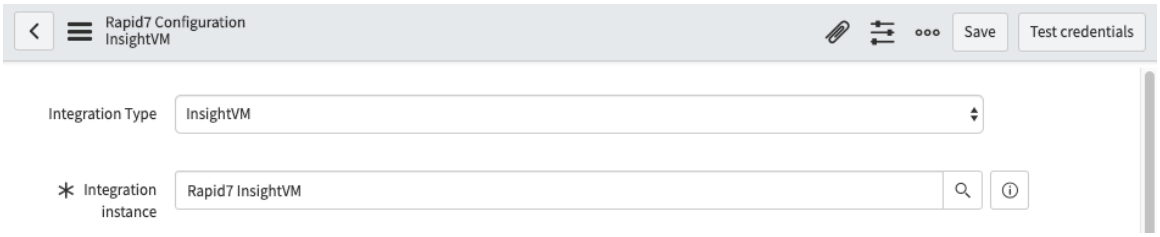
시작하기 전에
필요한 역할: 관리자 〔admin〕가 앱을 다운로드하여 설치합니다. sn_vul.vulnerability_admin 또는 sn_vul.admin은 구성을 감독하고 예상 결과를 검증합니다.

프로시저

1. 애플리케이션이 활성화(설치)된 후 다음으로 이동합니다. **Rapid7** 취약성 통합 〉 관리 〉 구성.
2. 목록에서 통합 유형을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

통합 유형 목록



3. 통합 인스턴스를 선택합니다.
기본적으로 Rapid7 InsightVM 기본 통합 인스턴스가 선택됩니다. 원하는 통합 유형인 경우 다음 단계를 수행합니다. 데이터 웨어하우스 통합 유형을 구성하려면 Rapid7 4단계로 진행합니다.

   a. 표시되는 양식에서 통합 설정 탭을 선택하고 필드에 내용을 입력합니다.

   InsightVM 통합 유형에 대한 통합 설정 탭

필드	설명
InsightVM 지역	사이트에서 가져온 서버 URL입니다 Rapid7 .
API 키	Insight 계정에서 가져온 Rapid7 API 키입니다.
확인 상태	읽기 전용: 자격 증명 확인 프로세스의 상태입니다.

   b. 자격 증명 테스트를 클릭하여 구성이 성공했는지 확인합니다.
   구성 중에 오류 메시지가 표시되면 데이터를 다시 입력합니다.

   c. 테스트가 성공적으로 완료되면 저장을 클릭합니다.

   d. **Import Configuration** 탭을 클릭합니다.

   표시되는 양식의 필드에 내용을 입력합니다.

   InsightVM에 대한 임포트 구성 탭

필드	설명
최소 CVSS 점수	임포트 중에 취약한 항목을 필터링하는 데 사용되는 최소 취약한 항목 CVSS 점수입니다.
최대 CVSS 점수	임포트 중에 취약한 항목을 필터링하는 데 사용되는 최대 취약한 항목 CVSS 점수입니다.
사이트 필터	사이트 목록에서 선택한 사이트로 데이터를 Rapid7 InsightVM 제한합니다. 사이트를 기준으로 Rapid7 필터링 문서를 참조하십시오. 둘 이상의 사이트를 선택할 수 있습니다. 기본값(비어 있음)은 모든 사이트를 가져옵니다. 사이트 목록을 미리 채우려면 이 필드를 설정하기 전에 Rapid7 사이트 통합 — API를 실행합니다. 사이트 필터링 사용에 대한 자세한 내용은 을 참조하십시오 사이트를 기준으로 Rapid7 필터링.
CVE 항목	CVE 항목을 생성하는 시스템 속성은 기본적으로 활성(true)입니다. CVE 자리 표시자는 CVE ID가 없는 경우 Rapid7 지식 수집을 통해 자동으로 생성됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
자동 생성	이 기능을 비활성화하려면 시스템 속성 목록에서 [sn_vul_r7.create_cve_for_vulnerabilities] 속성을 비활성화합니다.
기간별로 해결된 다시 열기	이 옵션을 선택하면 취약한 항목이 해결되었지만 종결되지 않은 일 수가 다음 이후 해결된 다시 열기 필드에 표시된 값과 일치할 때 자동으로 재개됩니다.

e. 저장을 클릭합니다.

통합 유형의 다중 배포의 Rapid7 InsightVM 경우:

f. 통합 인스턴스 필드에서 조회 목록 열고 기존 통합 인스턴스를 선택하거나 팝업 메뉴에서 신규를 클릭합니다.

g. 새로 만들기의 경우 통합 인스턴스의 이름을 입력하고 제출을 클릭합니다.
통합 유형이 구성 양식에 Rapid7 나타납니다.

주:
기본값을 제외한 모든 통합 인스턴스를 삭제할 수 있습니다. 인스턴스를 삭제하면 다음이 삭제됩니다(VI 제외).

- 통합
- 인스턴스 매개변수
- 통합 실행
- 통합 프로세스
- VI의 인스턴스 열이 비어 있는 것으로 표시됩니다.

h. 자격 증명 테스트를 클릭하여 구성이 성공했는지 확인합니다.

i. 테스트가 성공적으로 완료되면 저장을 클릭합니다.

4. 통합 유형 필드에서 목록을 확장하고 데이터 웨어하우스를 클릭합니다.

a. 통합 설정 탭을 선택합니다.

표시되는 양식의 필드에 내용을 입력합니다.

데이터 웨어하우스 통합 유형에 대한 통합 설정 탭

필드	설명
JDBC 자격 증명 이름	데이터 웨어하우스 자격 증명의 이름입니다.
사용자 이름	Rapid7 데이터 웨어하우스 사용자 이름입니다.
암호	Rapid7 데이터 웨어하우스 암호입니다.
확인 상태	읽기 전용: 자격 증명 확인 프로세스의 상태입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
확인 상세 정보	읽기 전용: 데이터 웨어하우스 전용입니다. 테스트 자격 증명을 한 번 이상 클릭한 후 유효성 검사에 대한 추가 정보를 표시합니다. 이는 설정을 디버깅할 때 유용할 수 있습니다(예: MID Server가 잘못 구성되었거나 자격 증명이 잘못되었는지 확인).
데이터베이스 서버 DNS/IP	데이터 웨어하우스의 DNS 또는 IP 주소입니다.
데이터베이스 포트	데이터 웨어하우스 통합에 사용할 포트입니다.
데이터베이스 이름	데이터 웨어하우스의 이름입니다.
데이터 지연 오프셋(일)	데이터 지연 오프셋은 스캐너의 Rapid7 Nexpose 실시간 데이터와 데이터 웨어하우스의 데이터 간의 지연을 고려합니다.
MID 서버	사용할 MID 서버입니다. 독립 실행형 MID Server만 지원됩니다. 클러스터된 MID Server는 지원되지 않습니다.
MID 서버 시간 제한(분)	통합 실행 시간이 초과되기 전에 MID 서버의 응답을 기다리는 시간(분)입니다.

b. 자격 증명 테스트를 클릭하여 구성이 성공했는지 확인합니다.

c. 테스트가 성공적으로 완료되면 저장을 클릭합니다.

d. Import Configuration 탭을 클릭합니다.

표시되는 양식의 필드에 내용을 입력합니다.

데이터 웨어하우스의 임포트 구성 탭

필드	설명
v12.0 이전: CVE 항목 생성 확인란	이 옵션을 선택하면 아직 존재하지 않는 CVE의 자리 표시자가 NVD 기록으로 생성되고 Rapid7에 대한 외부 공급업체 항목에서 참조됩니다. 선택하지 않으면 이러한 CVE는 무시됩니다.
최소 CVSS 점수	임포트 중에 취약한 항목을 필터링하는 데 사용되는 최소 취약한 항목 CVSS 점수입니다.
최대 CVSS 점수	임포트 중에 취약한 항목을 필터링하는 데 사용되는 최대 취약한 항목 CVSS 점수입니다.
사이트 필터	임포트된 사이트 통합 데이터를 선택한 사이트로 제한합니다. 두 개 이상 선택할 수 있습니다. 주: 기본 설정은 모든 사이트에서 데이터를 가져오는 것이므로 모든 사이트를 원하는 경우 필터를 사용할 필요가 없습니다. 이렇게 하면 요청 속도가 느려집니다.
기간별로 해결된 다시 열기	이 옵션을 선택하면 취약한 항목이 해결되었지만 종결되지 않은 일 수가 다음 이후 해결된 다시 열기 필드에 표시된 값과 일치할 때 자동으로 재개됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. 저장을 클릭합니다.
6. 옵션: 취약성 통합 - API 및 Rapid7 취약한 항목 통합 - API 통합 기록에서 시작 날짜를 Rapid7 설정하여 검사에서 Rapid7 처음 임포트하는 동안 기록 데이터를 검색하려면 다음 단계를 수행합니다.
   이 데이터를 사용하여 에 도움이 에서 부실 탐지 종결 취약성 대응될 수 있습니다.

   a. 다음으로 이동 **Rapid7** 취약성 통합 〉 관리 〉 통합.
   Rapid7 통합 목록이 표시됩니다.

   b. 통합 기록 중 하나를 클릭하여 엽니다.

   (Optional) 양식의 위쪽에서 여기 링크를 클릭하여 기록을 편집합니다.

   취약성 통합 - API 및 Rapid7 취약한 항목 통합 - API를 제외하고 Rapid7 통합의 Rapid7임포트 날짜 이후 필드는 기본적으로 비어 있습니다. 이러한 통합의 경우 이러한 필드는 1998-12-31 또는 1999-01-01로 설정됩니다.

   스캔에서 Rapid7 처음 임포트하는 동안 기록 데이터를 검색하려면 적절한 통합 기록에서 시작 날짜를 설정합니다. 이 프로세스는 다음 예외를 제외하고 모든 Rapid7 통합에 대해 작동합니다.

   - 익스플로잇 및 맬웨어 키트 통합은 Rapid7 델타 업데이트를 수행하지 않으므로 해당 필드를 사용하지 않으므로 다음 이후 임포트 필드가 표시되지 않습니다.
   - 자산 목록 통합은 Rapid7 모든 데이터를 검색하려는 의도이므로 필드를 무시합니다.
   - 부실 취약한 항목 자동 종결 모듈이 활성화되고 다음 이후 임포트 필드가 비어 있을 때 포괄적인 취약한 항목 통합 – API의 Rapid7 InsightVM 초기 실행의 경우.

     자동 종결 기능을 활성화하면 Rapid7 포괄적 취약한 항목 통합 또는 Rapid7 포괄적인 취약한 항목 통합 API에서 성공적으로 실행해야 합니다. 이러한 통합은 기본적으로 비활성화되어 있습니다.

     포괄적인 취약한 항목 통합 – API를 Rapid7 InsightVM 사용하도록 설정하는 경우 통합 구성 페이지에서 다음 이후 임포트 필드를 비워 두면 부실 취약한 항목 자동 종결 양식의 일 전 필드에 있는 값이 첫 번째 통합 실행의 다음 이후 임포트 날짜에도 사용됩니다. 부실 취약한 항목 자동 종결의 기본값은 (90일)입니다.

     예를 들어, 부실 취약한 항목 자동 종료 양식의 이전 일 수 필드가 90이고 Rapid7 포괄적인 취약한 항목 통합 – API 구성 페이지의 다음 이후 임포트 필드가 비어 있는 경우 첫 번째 통합 실행은 지난 90일 동안의 데이터를 임포트합니다.

     임포트 시작 날짜와일수 전 필드 간의 관계는 첫 번째 통합 실행에만 적용됩니다. 그 이후에는 부실 취약한 항목 자동 종결 양식에서 일 전 필드를 변경해도 Rapid7 포괄적인 취약한 항목 통합 - API 구성 페이지의 다음 이후 임포트 필드에 영향을 미치지 않습니다. 후속 통합 실행에서 델타 정보만 임포트하도록 필드가 첫 번째 실행의 시작 시간으로 변경됩니다

     다음 이후 임포트 필드는 편집할 수 있으며 각 통합에 대해 원하는 값을 입력할 수 있습니다.

7. 다음으로 이동 모두 〉 **sn_sec_int_impl.list** 〉 **Rapid7 InsightVM**.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. **import_startime_buffer_comprehensive** 통합 인스턴스 매개변수는 다음 이후 임포트 필드에 지정된 시간보다 24시간 전의 버퍼 시간을 설정하여 이 버퍼 시간에서 스캔된 자산을 **Rapid7** 포괄적인 취약한 항목 통합 **- API** 통합 실행 중에 가져오도록 합니다.
요구 사항에 따라 이 버퍼 시간을 수정할 수 있습니다.

b. 옵션: **close_stale_detections** 매개변수를 *true*로 설정하여 **Rapid7** API를 통해 **Rapid7** API를 통해 스캔 및 검색된 자산에 대해 더 이상 Rapid7 API를 통해 들어오지 않는 부실 탐지를 종결합니다.

의 Rapid7 취약성 통합설정, 설치 및 구성 단계를 성공적으로 완료했습니다. 이제 임포트한 데이터를 검토하고 검증할 준비가 되었습니다.

다음에 수행할 작업
Rapid7 및 Qualys 스캐너는 애플리케이션에서 기본적으로 비활성화되어 있습니다취약성 대응. 이러한 애플리케이션을 소스로 사용하는 취약한 항목 또는 정정 작업에서 다시 검색을 수행하려고 하면 다시 검색 버튼을 사용할 수 없습니다.

이러한 스캐너를 활성화하려면 sn_vul.vulnerability_admin 역할을 가진 사용자가 다음과 같이 하십시오.

1. 다음으로 이동 모두 〉 취약성 대응 〉 취약성 스캐닝 〉 스캐너.
2. 활성화할 스캐너 제품을 찾고 기록을 클릭하여 엽니다.
3. 활성 확인란을 선택합니다.
4. 업데이트를 클릭합니다.

활성화한 제품은 다음 임포트 후 취약한 항목 및 정정 작업 기록의 소스 필드에 표시되며, 다시 스캔 은 UI 작업으로 사용할 수 있습니다.

환경에 도메인 분리 가져오기가 필요한 경우 문서를 참조하십시오 통합을 위해 도메인 분리 임포트 작성.

임포트에 앞서 조회 규칙을 만들거나 구체화하려면 다음 문서를 참조하십시오 취약성 대응 CI 조회 규칙 생성.

사이트를 기준으로 **Rapid7** 필터링

통합 유형 및 Rapid7 Nexpose 데이터 웨어하우스 통합 유형에 대해 Rapid7 InsightVM 사이트를 기준으로 필터링합니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)

주:
사이트 필터링을 사용하면 성능에 영향을 줄 수 있습니다. 사이트 필터링을 사용하기 전에 성능 및 기타 고려 사항에 대한 자세한 내용은 KB0789221 참조하십시오.

이 태스크 정보

프로시저

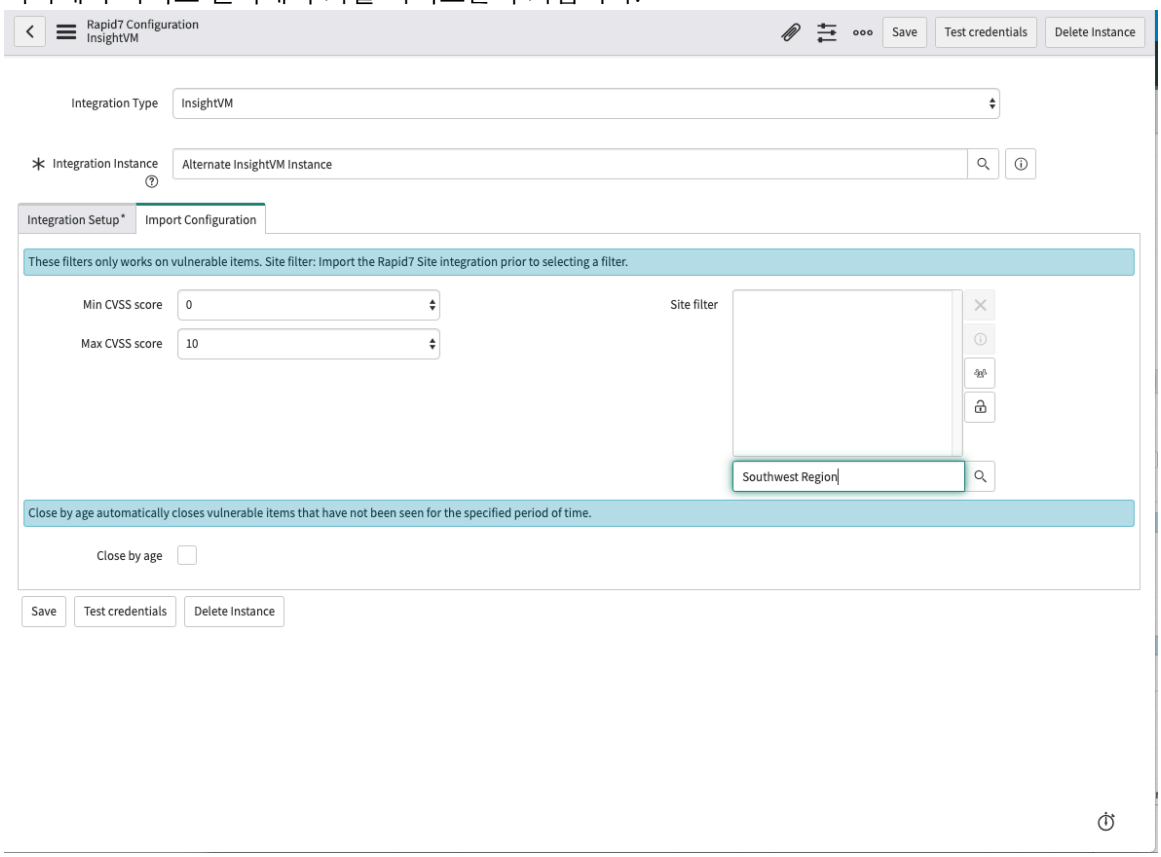
1. 다음으로 이동 모두 〉 **Rapid7** 취약성 통합 〉 구성.
2. 통합 인스턴스를 선택합니다.
3. **Import Configuration** 탭을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
모든 사이트를 원하는 경우 사이트 필터 필드를 비워 둡니다. 사이트 필터 없음은 모든 사이트를 추가하는 것과 같습니다.

사이트는 통합 인스턴스에 따라 다릅니다. 사이트 필터링을 위한 조회 목록에는 데이터 웨어하우스 통합 인스턴스 사이트와 Rapid7 Nexpose 데이터 웨어하우스 통합 인스턴스가 모두 Rapid7 InsightVM 표시됩니다. 선택한 사이트가 선택한 통합 인스턴스와 일치하는지 확인하십시오. 예를 들어 데이터 웨어하우스 사이트를 선택하는 경우 실수로 해당 사이트는 에 의한 Rapid7 InsightVM사이트 필터링에 대해 작동하지 않습니다.

4. 현재 통합 인스턴스에 대한 사이트 기록을 보려면 조회 목록을 클릭하십시오.
5. 목록에서 사이트 필터에 추가할 사이트를 추가합니다.



6. 선택을 반복하여 사이트를 추가합니다.
7. 저장을 클릭합니다.
이러한 사이트는 다음 가져오기 중에 사이트별로 필터링하는 데 사용됩니다. 사이트 데이터에 접두사 SITE를 추가하는 방법에 대한 자세한 내용은 을 참조하십시오 Rapid7 InsightVM 사이트 태그 앞에 사이트 추가 .

Rapid7 InsightVM 사이트 태그 앞에 사이트 추가

사이트 태그에 Rapid7 InsightVM 접두사 SITE를 추가하여 태그 목록에서 강조 표시합니다.

시작하기 전에

필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)
가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
필요한 경우 범위를 보안 운영용 Rapid7 통합으로 전환합니다.

프로시저

1. 왼쪽 탐색 상자에 을(를) *sys_properties.list*입력합니다.
2. 이름에서 다음을 *sn_vul_r7.prefix_site_to_rapid7_tags*검색합니다.
3. *sn_vul_r7.prefix_site_to_rapid7_tags*를 엽니다.
4. 값을예로 변경합니다.
5. 업데이트를 클릭합니다.
   새 사이트 태그와 기존 사이트 태그는 다음에 .Rapid7 InsightVM

Rapid7 취약성 통합 상태 차트 실행

Rapid7 Nexpose센서는 데이터를 수집하고 자동으로 OR Rapid7 InsightVM 제품으로 전송 Rapid7 Nexpose 하여 정보를 지속적으로 분석하고 상관 관계를 지정합니다.

작업 공간의 데이터 시각화 취약성 대응

작업 공간에는 취약성 대응 정정 진행 상황을 모니터링하는 데 도움이 될 수 있는 데이터 시각화가 포함되어 있습니다. 취약성 데이터가 변경될 때 업데이트되는 동적 데이터 시각화에서 조직에 중요한 활성 취약성의 수와 심각도를 확인하여 조직에 대한 위협 수준을 확인할 수 있습니다. 취약성 관리자 작업 공간IT 정정 작업 공간 살펴보기 를 참조취약성 대응 작업 공간하고 사용 가능한 동적 데이터 시각화에 대한 자세한 내용을 확인할 수 있습니다.

Rapid7 취약성 통합 는 취약성을 CI 및 비즈니스 서비스에 쉽게 취약성 대응 매핑하여 잠재적으로 악의적인 위협의 영향과 우선순위를 결정합니다. Rapid7 취약성 통합 실행 상태 모듈은 실행 상태에 Rapid7 취약성 통합 대한 그래픽 보기입니다.

레거시 뷰에서 이 데이터를 보려면 다음으로 이동합니다. 모두 〉 모든 **Rapid7** 취약성 통합 〉 통합 실행 상태.

의 취약성 대응버전 19.0부터 이 대시보드는 New Experience UI에서 사용할 수 있습니다.

주:
Tokyo에 있는 경우 Next Experience UI에서 대시보드를 볼 수 있지만 일부 기능 손실이 있습니다.

이전 버전 취약성 대응

차트에서 원하는 부품(막대형, 원형, 데이터 요소 등)을 가리키면 해당 부품과 관련된 일반 데이터를 볼 수 있습니다. 보고서의 일부를 클릭하면 자세한 정보를 제공하는 목록이 열립니다.

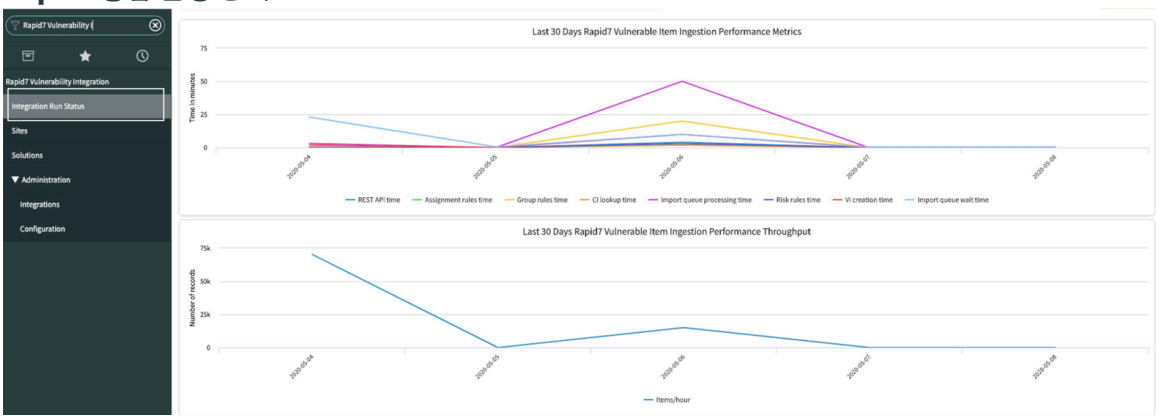
이 데이터를 처리하는 데 걸린 데이터 양 및 시간과 같은 여러 요인이 통합 실행의 성능에 영향을 줄 수 있습니다. 성과 메트릭을 비교하기 위해 두 개의 새로운 그래프가 추가되었습니다.

- Rapid7 취약한 항목 수집 성과 메트릭: 지난 30일 동안 취약한 항목에 대한 담당 규칙, 그룹 규칙, 위험 규칙, 큐 대기 시간, 큐 처리 시간 및 기타 통계에 대한 일일 성과 메트릭을 비교하여 성능 편차의 원인을 식별합니다.
- Rapid7 취약한 항목 수집 성능 처리량: 취약한 항목 통합 - API에 Rapid7 대한 일일 취약한 항목 수집 처리량을 비교합니다. 처리량은 시간당 항목 단위로 측정됩니다.

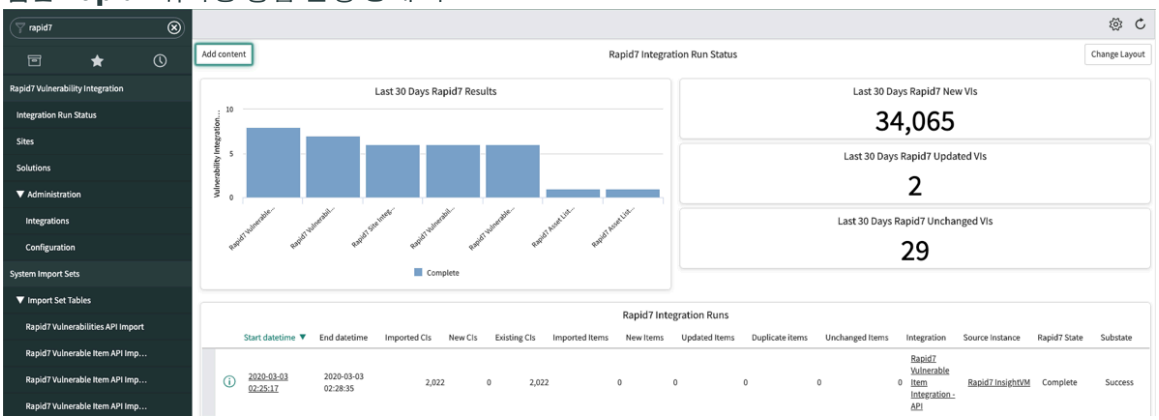
주:
에서 Rapid7이러한 그래프는 Insight VM 통합에 대해서만 지원됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Rapid7 통합 실행 상태



샘플 **Rapid7** 취약성 통합 실행 상태 차트



- 임포트한 항목 열의 값은 통합 실행에서 생성된 총 취약한 항목 수를 나타냅니다.
- 새 항목 열에는 통합 실행에서 생성된 취약한 항목 수가 표시됩니다.
- 중복 항목 열이 더 이상 채워지지 않습니다. 표시에서 이 열을 제거하는 것이 좋습니다.
- 업데이트된 항목 열에는 통합 실행 중에 취약한 항목이 업데이트된 횟수가 표시됩니다. 이 값은 업데이트되는 고유한 취약한 항목 수가 아닙니다. 예를 들어 통합 실행 중에 취약한 항목이 두 번 업데이트되면 두 번 계산되어 2 개의 업데이트된 항목으로 표시됩니다.
- 변경되지 않은 항목 열에는 데이터베이스에 이미 있지만 관련 필드 값이 변경되지 않았기 때문에 업데이트되지 않은 통합 실행 중에 발견된 취약한 항목이 표시됩니다.

주:
통합은 다음 네 가지 값 모두에 대해 0개의 결과로 실행됩니다. 새 **CI**, 기존 **CI,**새 항목 및 업데이트된 항목은**Rapid7** 통합 실행 목록에서 필터링됩니다.

Rapid7 취약성 통합 상태 차트 보고서 실행

이름	설명
지난 30일 Rapid7 결과	각 통합에 대해 완료된 통합 실행 수입니다. 성공한 실행과 실패한 실행을 모두 표시합니다. 시각적 개체 막대에서 실행합니다.
지난 30일 Rapid7 신규 VI	지난 30일 동안 임포트된 새로운 취약한 항목 수입니다. 정수로 표시됩니다.
지난 30일 Rapid7 업데이트된 VI	지난 30일 동안 임포트된 업데이트된 취약한 항목 수입니다. 정수로 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Rapid7 취약성 통합 상태 차트 보고서 실행

이름	설명
지난 30일 Rapid7 중복	지난 30일 동안 임포트된 중복 취약한 항목 수입니다. 정수로 표시됩니다.
Rapid7 통합 실행	통합 실행 기록이 목록에 표시됩니다. 주: **V16.1:** 이 통합에 대한 탐지를 확인하려면 탐지 또는 결과를 ServiceNow 테이블의 탐지 데이터와 *sn_vul_detection* 비교합니다. 통합이 진행되는 동안 탐지 또는 발견 개수가 변경될 수 있습니다. 이 보고서는 통합 실행이 완료된 후 인스턴스의 "종료 날짜 카운트" 열에 탐지 횟수를 표시합니다.
지난 30일 Rapid7 취약한 항목 수집 성과 메트릭	지난 30일 동안과 비교하여 취약한 항목에 대한 일일 성과 메트릭입니다.
지난 30일 Rapid7 취약한 항목 수집 성능 처리량	지난 30일 동안 측정된 취약한 항목 통합 - API에 Rapid7 대한 일일 취약한 항목 수집 처리량입니다.

Rapid7 취약성 통합 임포트 실행 상태 대시보드 보기

Rapid7 취약성 임포트 실행 상태 대시보드를 사용하여 통합 실행의 성공을 확인하고, 문제를 찾고, 정정 결정을 알릴 수 있습니다.

시작하기 전에
필요한 역할: sn_vuln.admin

이 태스크 정보
이 절차에서는 다음과 같이 가정합니다.

- 설치 취약성 대응 및 구성되어 있습니다 Rapid7 취약성 통합 .
- Rapid7 취약성 통합 임포트가 예약되어 실행 중입니다.
- Rapid7 통합 실행 상태 차트가 사용 중입니다.

통합 실행 중에 여러 프로세스가 생성되고 데이터가 페이지 형식으로 수신됩니다. 각 프로세스에는 페이지에 첨부된 데이터가 있는 하나 이상의 임포트 큐 항목이 포함될 수 있습니다. 이러한 항목은 1시간의 시간 제한 내에 데이터를 처리해야 합니다. 그러나 페이로드 크기가 크면 처리 시간이 1시간을 초과하거나 중단되어 통합 시간 제한 오류가 발생할 수 있습니다. 통합은 시간 초과 오류에도 불구하고 데이터를 계속 처리합니다. 이러한 잘못된 통신을 피하기 위해 버전 19.0 취약성 대응부터 큐가 활성 상태이고 데이터를 처리하는지 여부를 나타내기 위해 타임스탬프(하트비트)가 주기적으로 전송됩니다. 임포트 큐 항목 페이지의 처리된 마지막 기록 필드는 임포트 큐가 생성하거나 업데이트하는 기록 수에 따라 업데이트됩니다. 임포트 큐 항목이 1시간의 시간 제한을 초과하는 경우, 시스템은 마지막으로 처리된 기록 필드를 검사하여 1시간보다 오래되었는지도 확인합니다. 이 경우 이는 임포트 큐 항목이 고착되었음을 나타내며 처리 시 더 이상의 지연을 방지하기 위해 시간 초과됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
마지막으로 처리된 기록 필드는 다음 시스템 속성에 정의된 내용에 따라 업데이트됩니다.

- *sn_sec_cmn.record_threshold_heartbeat*: 하트비트(타임스탬프)가 임포트 큐 항목으로 전송된 후 처리된 기록 수를 정의합니다.
- *sn_sec_cmn.maximum_heartbeat_delay*: 임포트 큐 항목을 시간 초과해야 하는 시간을 정의합니다.

프로시저

1. 다음으로 이동 **Rapid7** 〉 통합 실행 상태.

   의 취약성 대응버전 19.0부터 이 대시보드는 New Experience UI에서 사용할 수 있습니다.

   주:
   Tokyo에 있는 경우 Next Experience UI에서 대시보드를 볼 수 있지만 일부 기능 손실이 있습니다.

2. 통합 실행 상태 차트를 사용하지 Rapid7 않는 경우 다음으로 이동합니다. **Rapid7** 〉 통합.
   a. 통합을 선택합니다.
   b. 취약성 통합 실행 관련 목록을 클릭합니다.
3. 모든 임포트가 성공했는지 확인합니다.

   Trouble?

   실행 실패의 가장 일반적인 원인은 다음과 같습니다.

   ○ 네트워크 중단

   ○ 데이터 전송 시 비트 감쇠로 인해 변환 중 데이터가 손상됨
   이러한 모든 조건에 대해 지금 실행을 클릭하고 통합을 다시 실행합니다.

데이터 웨어하우스 기록 중복 **Rapid7** 취약성 통합 제거

데이터 웨어하우스 통합 유형에서 **InsightVM** 통합 유형으로 마이그레이션할 때 기존 데이터 웨어하우스 취약한 항목이 데이터와 Rapid7 InsightVM 동일한 소스 데이터에 속하는 한 중복 제거할 수 있습니다.

시작하기 전에
필요한 역할: sn_vul_r7.admin 또는 sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)
가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

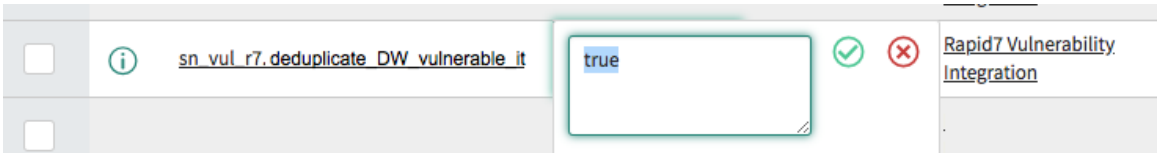
이 태스크 정보
이 중복 제거는 데이터 웨어하우스에서 Rapid7 Nexpose 취약한 항목 통합으로 Rapid7 InsightVM 마이그레이션할 때만 작동합니다.

프로시저

1. 다음으로 이동 모두 〉 고속 **7** 〉 통합.
2. 모든 Rapid7 Nexpose 데이터 웨어하우스 통합 활성 열 설정을 **False**로 설정하여 통합을 비활성화합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 왼쪽 탐색 패널에 sys_properties.list 를 입력합니다.
4. 이름(sn_vul_r7.deduplicate_DW_vulnerable_item)을 검색합니다.
5. 값 필드를 **True**로 변경합니다.



6. 녹색 확인 표시 아이콘 녹색 을 클릭합니다.
   다음 Rapid7 InsightVM 취약한 항목 통합 임포트 중에 기존 데이터 웨어하우스 기록과 일치하면 중복된 취약한 항목이 생성되지 않습니다.

취약성 통합에 **Rapid7** 대한 재스캔 시작

플랫폼에서 재스캔 Rapid7 을 시작하여 예약된 스캔 주기 사이에 취약한 항목이 정정되었는지 확인합니다.

시작하기 전에

주:
데이터 웨어하우스 취약한 항목에 대한 Rapid7 재스캔은 지원되지 않습니다.

취약성 대응 작업 공간에서 다시 스캔을 시작할 수 있습니다. 자세한 내용은 에서 기록 및 정정 작업을 다시 스캔 취약성 관리자 작업 공간 및 에서 취약한 항목 및 정정 작업 다시 스캔 IT 정정 작업 공간 문서를 참조하십시오.

필요한 역할: 필요한 역할: sn_vul.write_all 또는 sn_vul.write_assigned

이 태스크 정보
클래식 환경에서 다시 검색하려면 다음 섹션을 참조하십시오.

재스캔이 지원됩니다. 인스턴스의 통합에서 Rapid7 InsightVM 임포트한 취약한 항목에 대해 요청 시 재검색을 시작할 수 ServiceNow AI Platform# 있습니다.

주:
스캐너는 Rapid7 기본적으로 애플리케이션에서 비활성화되어 있습니다 취약성 대응 . 애플리케이션을 소스로 사용하는 Rapid7 취약한 항목 또는 정정 작업에서 다시 검색을 수행하려고 하면 다시 스캔 버튼을 사용할 수 없습니다.

예약된 전체 검사와 관련된 오버헤드와 볼륨을 줄이기 위해 정정 소유자, IT 전문가, 취약성 분석가 또는 취약성 관리자는 해당 환경에서 자산(구성 항목)의 특정 취약성에 대한 요청 시 대상 재검사를 시작할 수 있습니다. VI(취약한 항목), RT(정정 작업), TPE(외부 공급업체 항목) 또는 인스턴스에서 검색된 항목 기록에서 다시 스캔을 시작할 수 있습니다 ServiceNow AI Platform# .

재검색을 통해 정정 활동, 패치 및 기타 작업이 구성 항목(CI)의 특정 취약성을 성공적으로 수정했는지 확인할 수 있습니다.

예를 들어, 전체 환경은 3주에 한 번씩 검사됩니다. 가장 최근의 전체 검사는 일주일 전에 완료되었지만 중요한 취약성을 수정하기 위해 어제 패치를 적용했습니다. 이 취약성의 특성으로 인해 다음 예약된 검사에서 정정되었는지 확인할 때까지 2주를 기다릴 수 없습니다. 패치가 이전 검사 중에 발견된 중요 취약성을 성공적으로 수정했는지 확인하기 위해 취약한 항목에 대한 Rapid7 대상 재스캔 ServiceNow AI Platform 을 시작할 수 있습니다. 다음에 예약된 취약성 및 취약한 항목 통합 임포트를 Rapid7 InsightVM 통해 취약한 항목에 대한 업데이트된 결과를 볼 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

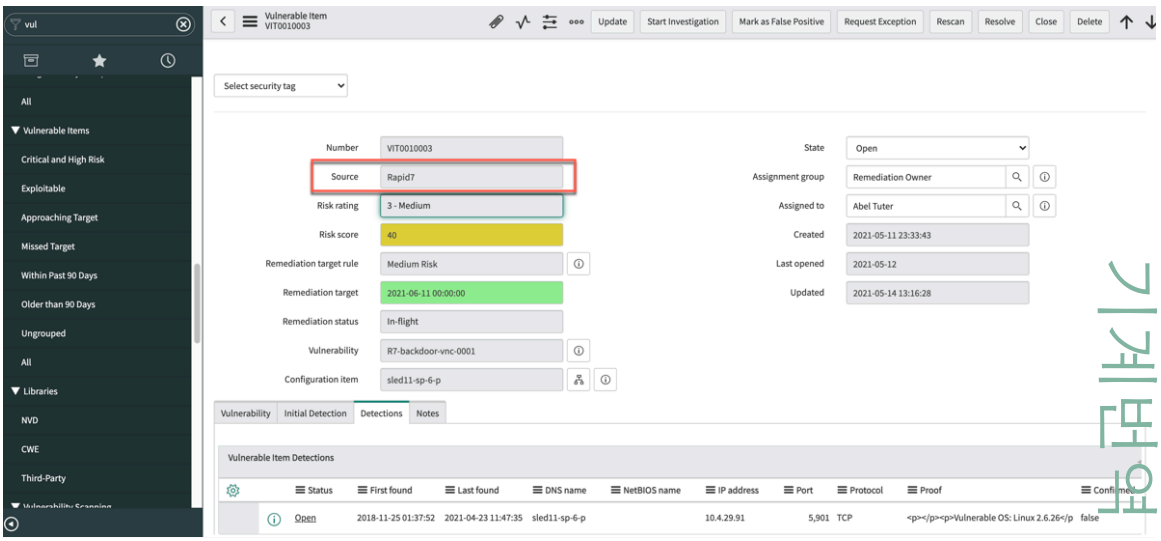
프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 취약한 항목.
2. 다시 스캔을 트리거할 취약한 항목 기록을 찾아 엽니다.

   주:
   소스로 하는 Rapid7 VI에 대한 재스캔을 시작합니다. 확인 Rapid7 이 VI 목록 뷰의 소스 열 또는 개별 기록의 소스 필드에 표시됩니다. 조건 빌더를 사용하여 소스별로 VI를 그룹화할 수 있습니다. 또는 VI 목록 뷰에 소스 열이 표시되지 않으면 목록의 왼쪽 상단에서 톱 니바퀴 아이콘을 클릭하고 소스를 사용 가능 에서 선택됨으로 이동합니다.

   다시 스캔을 시작할 때 여러 소스에서 하나의 소스 ID에 대한 스캔을 동시에 트리거하지 마십시오. 마지막 스캔 요청에 오류가 발생합니다.

   예를 들어 VI 기록에서 VI에 대한 재검색을 시작하고 동일한 VI가 포함된 정정 작업 기록에서 또 다른 재스캔을 요청하는 경우 두 번째 요청이 실패할 가능성이 높습니다.



3. 또는 다음으로 이동합니다. 취약성 대응 〉 정정 작업 또는 취약성 대응 〉 라이브러리 〉 외부 공급업체 각각 다시 검색에 사용할 정정 작업 또는 외부 공급업체 항목 기록의 경우

   선택에 따라 다음 기록에서 다시 스캔 버튼을 사용할 수 있습니다.

   - 단일 VI 기록에서 VI는 제품에서 나온 Rapid7 것이어야 하며 종결 이외의 상태여야 합니다. 여러 VI 레코드의 경우 목록 뷰에서 선택하는 모든 VI는 제품 및 종결 이외의 상태여야 Rapid7 합니다.
   - 정정 작업 기록에서 정정 작업은 종결 이외의 모든 상태일 수 있으며 연결된 모든 VI는 제품에서 가져온 Rapid7 것이어야 합니다.
   - 타사 항목(TPE) 레코드에서 레코드에는 종결 이외의 상태인 제품의 연결된 VI 레코드가 Rapid7 하나 이상 있어야 합니다.
   - 검색된 항목 기록에서 VI는 제품에서 나온 Rapid7 것이어야 하며 종결됨 이외의 상태여야 합니다.

4. 기록의 오른쪽 상단에서 Rescan(다시 스캔)을 클릭합니다.
   목록 뷰의 경우 목록에서 재스캔할 VI를 선택하고 선택한 행 목록의 작업에서재스캔을 선택합니다.
5. 표시되는 팝업에서 재스캔을 확인합니다.
   스캔이 처리 중(큐에 대기 중)임을 나타내는 메시지가 표시됩니다. 메시지에서 상세 정보 보기 링크를 클릭하여 다시 스캔(하위 스캔)의 상태를 확인하고 기록에서 시작된 다른 다시 스캔을 봅니다. 모든 재스캔의 상태는 재스캔을 시작하는 데 사용하는 VI, 정정 작업, TPE 및 검색된 항목 기록 하단의 스캔 관련 목록에서 언제든지 확인할 수 있습니다.

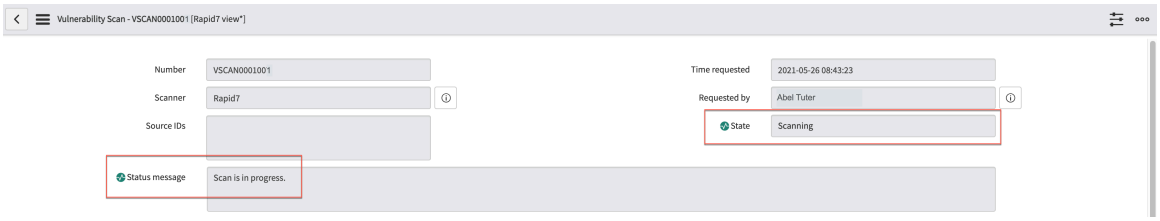
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

검사가 진행 중이면 상태 필드가 검사 중으로 변경되고 상태 메시지 필드에 검사 진행 중이 표시됩니다.

주:
각 재스캔은 스캔당 500개의 자산을 지원합니다. 요청에 500개가 넘는 자산이 있는 경우 더 많은 하위 스캔이 요청됩니다.

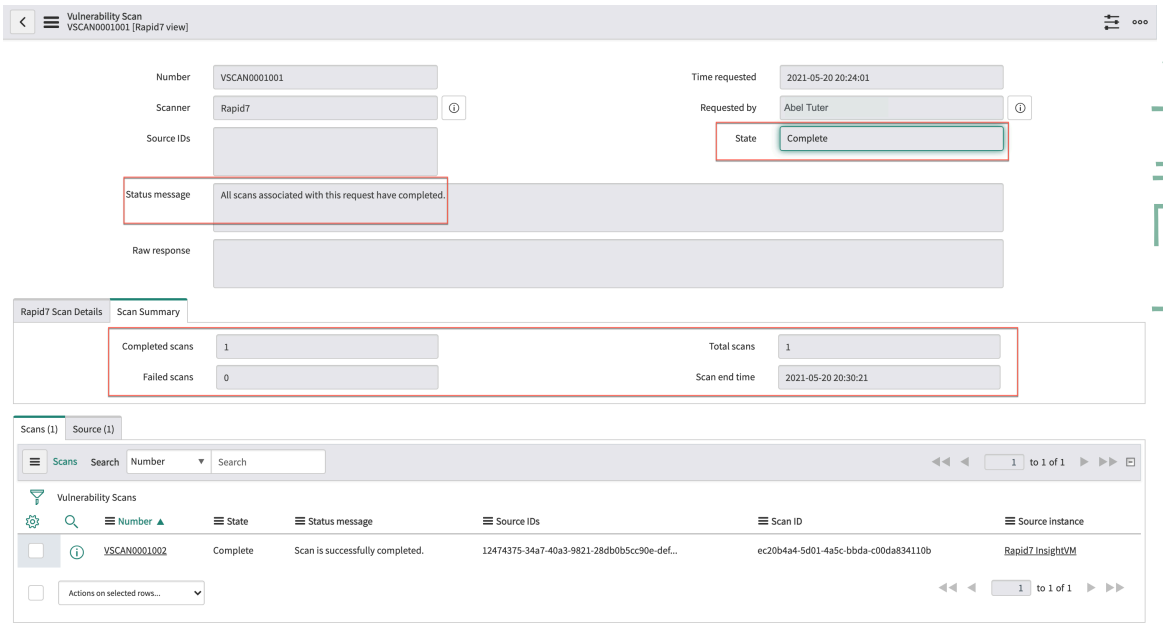
인스턴스는 ServiceNow AI Platform# 재스캔 상태가 성공적으로 완료될 때까지, 또는 설정된 추적 기간이 초과될 때까지(먼저 발생하는 쪽 적용) 재스캔 상태를 추적합니다.

재스캔 처리 중



시간 제한은 검사를 중지하지 않습니다. 시간 제한은 실제 다시 검색이 중지된 시간이 아니라 다시 스캔 상태 추적이 ServiceNow AI Platform# 중지된 시기를 나타냅니다. 종결/고정으로 전환되었거나 전환될 모든 VI는 다음의 Rapid7 예약된 통합 임포트와 함께 임포트됩니다.

재스캔 완료



또는 특정 자산의 특정 취약성에 대한 요청 시 재검색을 시작할 수 있습니다. 스캔을 시작한 새로 고침된 VI, 정정 작업, TPE 및 검색된 항목 기록에서 스캔이 완료되면 이러한 스캔의 결과를 볼 수 있습니다.

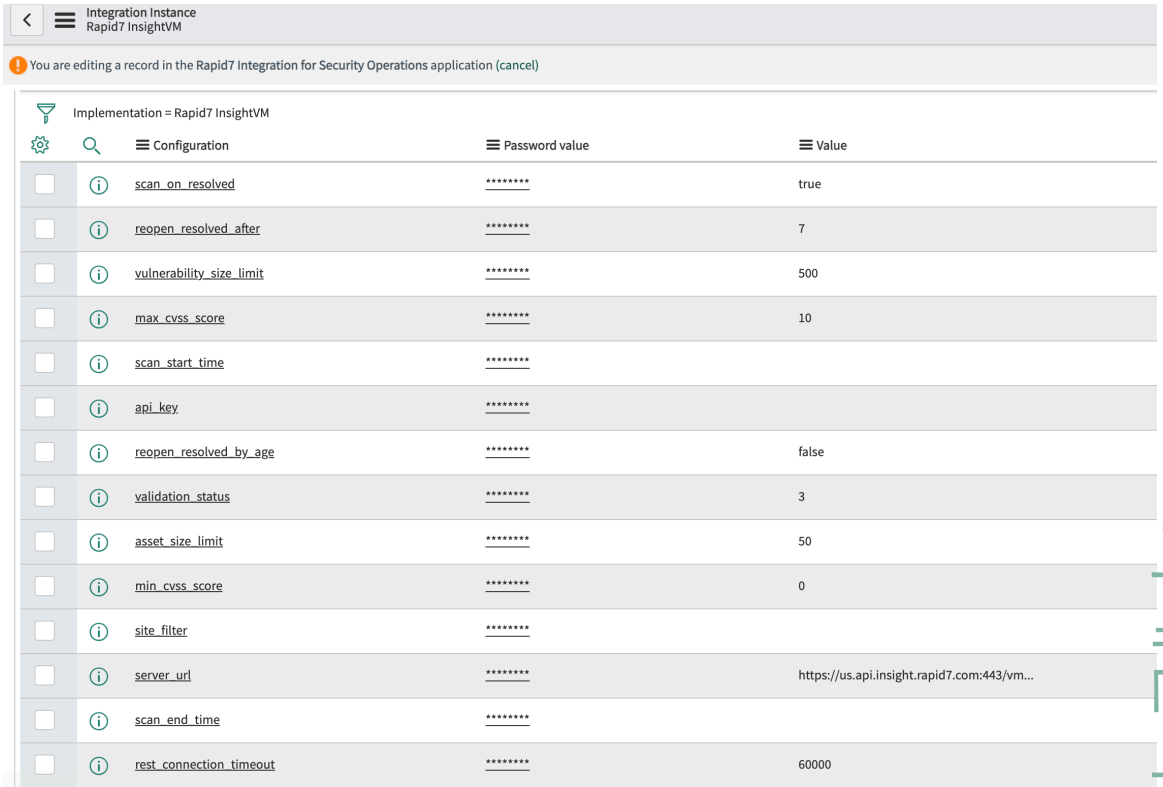
취약성 스캔 기록의 상태 필드 값은 에서 임포트 Rapid7됩니다. 스캔이 성공적으로 완료되면 상태가 완료로 설정됩니다. 스캔이 성공적으로 완료되지 않으면 오류 값이 표시됩니다.

자동 스캔 및 예약된 스캔

취약성 관리자 또는 분석가는 VI 및 RT에 대한 재스캔이 시작되는 시기를 지정하고 예약할 수 있습니다. 해결하도록 설정된 VI 및 정정 작업에 대해 자동 스캔을 활성화할 수도 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

6. 통합 인스턴스의 통합 매개변수를 수정하려면 다음으로 이동합니다. **Rapid7** 취약성 통합 〉 관리 〉 구성.
7. Rapid7 구성 기록의 통합 유형 목록에서 선택되지 않은 경우 **Rapid7 InsightVM**을 선택합니다.
8. 통합 인스턴스 필드 오른쪽에 있는 정보 아이콘을 클릭한 다음 기록 열기를 클릭합니다.
9. 통합 인스턴스 Rapid7 InsightVM 기록에서 스캔을 예약하기 위한 매개변수를 찾고 필요에 따라 편집합니다.



scan_on_resolved 취약성이 해결되면 검사가 시작되는지 나타냅니다. 기본값은 **false**(비활성화)입니다.

이 매개변수가 true로 설정되면 VI 또는 RT가 해결됨으로 설정될 때마다 각 VI 및 정정 작업을 다시 스캔하는 워크플로우가 자동으로 트리거됩니다.

scan_start_time

재스캔을 사용할 수 있도록 하려는 창의 시작 시간에 대해 UTC 시간대의 **HH:mm**(24시간 형식) 안에 스캔 시작 시간을 설정합니다.

기본값은 00:00입니다.

scan_end_time

사용 가능한 스캔 창의 종료 시간에 대한 스캔 종료 시간을 UTC 시간대의 **HH:mm**(24시간 형식) 단위로 설정합니다.

기본값은 23:59입니다.

예약된 기간 내에 스캔이 시작되면 즉시 실행됩니다. 이 기간 밖에서 검사가 시작된 경우에는 예약된 다음 기간 동안 검사가 큐에 대기합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예를 들어 매개변수에 *scan_start_time* 대해 00:00의 시작 시간을 입력하고 *scan_end_time* 같은 날 오전 10:00를 입력하는 경우 자정에서 오전 10시 이외의 시간에 예약되거나 수동으로 실행된 스캔은 큐에 대기하고 다음 날 시간 창 00:00의 시작 시간에 실행됩니다.

같은 예에서 오전 11:00에 수동으로 다시 스캔을 시작하는 경우 재스캔은 사용 가능한 구성된 스캔 시간을 벗어나므로 즉시 시작되지 않습니다. 스캔 요청은 다음 날 기간(이 예에서는 00:00)이 시작될 때까지 큐에 대기된 상태로 남아 있습니다.

임포트에 대한 **Rapid7 InsightVM** 추가 필터 매개변수 설정

를 Rapid7 Integration for Security Operations 사용하여 예약된 쿼리에 대한 필터링 매개변수를 사용자 지정하면 제품과 함께 Rapid7 InsightVM 임포트하는 취약성 데이터를 더욱 세분화할 수 있습니다.

시작하기 전에

사용 사례: 취약성 관리자 또는 분석가는 특정 취약성 상세 정보만 검토할 수 있도록 쿼리에서 데이터를 필터링할 수 있습니다. 예를 들어 임포트한 ## 하고 ### 취약성만 볼 수 있습니다.

이 데이터를 수집하려면 필요한 특정 취약성 상세 정보를 가져오는 데 도움이 되는 매개변수를 추가합니다 Rapid7 .

추가 API 호출이나 코딩을 추가하지 않고 v13.4부터 기능을 사용하면 HTTP 요청 정보를 매개변수로 Rapid7 InsightVM 사용자 지정할 수 있습니다 ServiceNow AI Platform. 다음 Rapid7 InsightVM 통합은 요청 본문에 JSON 컨텐츠를 추가하여 필터링을 지원합니다.

- Rapid7 InsightVM 취약한 항목 통합 API
- Rapid7 InsightVM 취약성 통합 API
- Rapid7 InsightVM

이 기능에 문자열을 사용하는 JSON 방법을 알아야 합니다.

필요한 역할: sn_vul.vulnerability_admin

프로시저

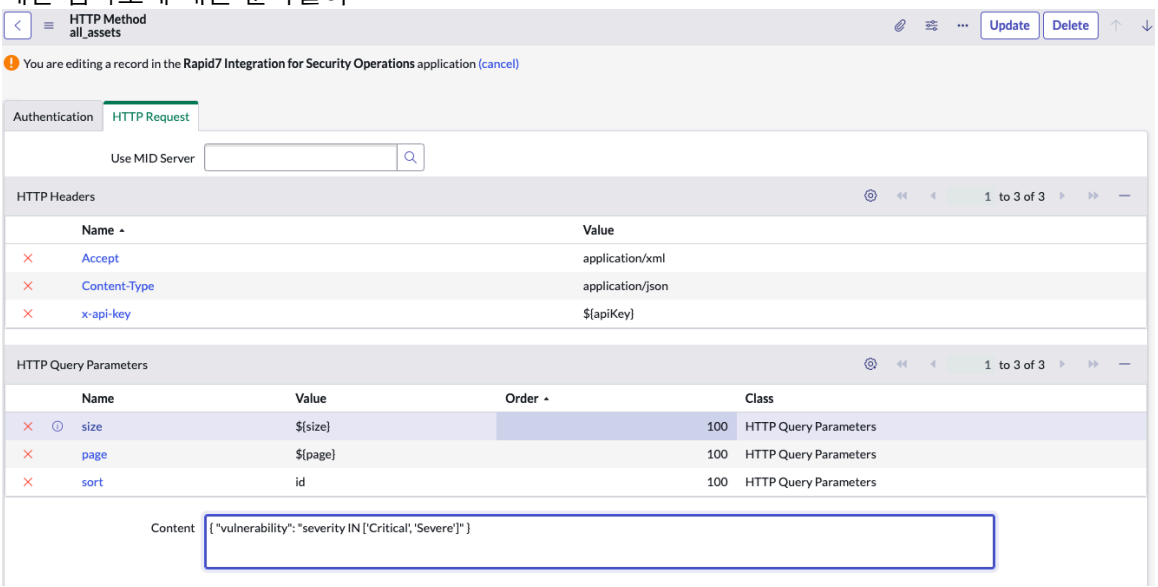
1. 필터링에 사용할 개발자 사이트의 제품 Rapid7 에서 Rapid7 InsightVM 지원하는 매개변수를 찾습니다.

   설명서를 참조하여 요청 본문에 대한 매개변수를 만들 수 있습니다 Rapid7 . 제품에서 Rapid7 InsightVM 입력하는 매개변수와 값은 통합 인스턴스 수준에서만 지원됩니다.

2. 다음으로 이동 모두 〉 **Rapid7** 취약성 통합 〉 관리 〉 통합.
3. Rapid7 통합 목록 페이지에서 열고자 하는 통합의 Rapid7 InsightVM 기록을 클릭합니다.
4. 페이지 오른쪽에서 REST 메시지에 대한 정보 아이콘(I)과 기록 열기를 차례로 클릭합니다.
5. HTTP 요청 탭을 선택한 상태에서 HTTP 메서드의 이름 열에서 항목을 클릭하여 해당 HTTP 쿼리 매개 변수를 엽니다.
6. HTTP 메서드 기록의 HTTP 쿼리 매개변수에서 컨텐츠 필드에 개발자 사이트에서 찾은 Rapid7 매개변수 값을 입력합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음 이미지에는 심각도에 대한 문자열이



추가됩니다.

둘 이상의 매개변수를 입력하려면 각 값을 구분하는 방법에 대한 자세한 내용은 설명서를 참조하십시오 Rapid7 .

7. 업데이트를 클릭합니다.

Shodan 익스플로잇 통합 이해

ServiceNow# Shodan 익스플로잇 통합 애플리케이션은 검색 엔진에서 Shodan 임포트한 데이터를 사용하여 잠재적으로 악의적인 익스플로잇의 영향과 우선순위를 파악하는 데 도움을 줍니다.

스토어에서 앱 요청

ServiceNow Store 웹 사이트를 방문하면 사용 가능한 모든 앱을 확인하고 스토어에 요청을 제출하는 방법에 대한 정보를 참조할 수 있습니다. 출시된 모든 앱의 누적 릴리스 정보는 ServiceNow Store 버전 기록 릴리스 정보를 참조하십시오.

Shodan Exploit Integration

Shodan 검색 엔진은 악용 데이터를 수집하고 Shodan API는 해당 데이터베이스를 ServiceNow AI Platform#. 애플리케이션과 쉽게 통합되어 ServiceNow# 취약성 대응 익스플로잇을 외부 공급업체 취약성에 매핑하여 인스턴스의 익스플로잇 데이터를 보강합니다.

각 통합 기록에 대해 구성된 실행 사용자가 있습니다. 이 사용자의 기본값은 VR입니다. 시스템. 이 값은 변경하지 마십시오.

매일 예약된 작업은 나열된 순서대로 통합을 자동으로 호출합니다. 예약된 개별 작업을 수동으로 실행할 수도 있습니다. 예약된 작업은 인스턴스를 다른 취약성 관리 시스템과 동기화된 상태로 유지하여 취약성 정정 수명주기를 단순화합니다.

사용 가능한 버전

의 릴리스 버전 Yokohama	릴리스 정보
Shodan Exploit 통합 v10.6, 10.7	호환성 정보는 KB0856498 Vulnerability Response 호환성 매트릭스 및

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

의 릴리스 버전 Yokohama	릴리스 정보
	릴리스 스키마 변경을 참조하십시오.

역할

Shodan 악용 통합 작업에는 다음과 같은 역할이 포함됩니다.

- sn_vul_shodan.admin: 이 역할을 가진 사용자는 기록을 읽고, 쓰고, 삭제할 수 있습니다.
- sn_vul_shodan.user: 이 역할을 가진 사용자는 기록을 읽고 쓸 수 있습니다.
- sn_vul_shodan.read: 이 역할을 가진 사용자는 기록을 읽을 수 있습니다.

가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

Shodan 익스플로잇 통합

익스플로잇 통합을 보려면 Shodan 다음으로 이동하십시오. 모두 〉 **Shodan Exploit Integration** 〉 통합.

기본 시스템에는 다음과 같은 통합이 포함됩니다. 이러한 통합은 기본적으로 활성화됩니다.

Shodan 익스플로잇 통합

통합	설명
Shodan ExploitDB 통합	외부 공급업체 취약성 데이터에서 Shodan ExploitDB 데이터를 검색하고 보강합니다. 이 통합은 매일 03:15:00에 실행되도록 설정되었습니다.
Shodan Metasploit 통합	외부 공급업체 취약성 데이터에서 Shodan Metasploit 정보를 검색하고 보강합니다. 이 통합은 매일 01:15:00에 실행되도록 설정됩니다.

예약된 통합 임포트에 대한 기본 시작 시간을 변경하려면 다음 문서를 참조하십시오 악용 통합 임포트 시간 설정 Shodan.

외부 공급업체 취약성에서 악용 데이터를 보려면 을 참조하십시오 취약성 라이브러리 보기 취약성 대응.

다른 Shodan 익스플로잇 통합 설정을 변경하려면 고급 ServiceNow 및 취약성 대응 전문 지식이 필요하며 이는 제품 설명서의 범위를 벗어납니다.

익스플로잇 통합 준비 **Shodan**

익스플로잇 통합에 성공하려면 Shodan 통합 전 작업을 계획하고 신중하게 실행해야 합니다. 다음 작업을 수행하여 통합을 준비합니다. 익스플로잇 통합에서는 Shodan 사용자가 검색 엔진과 API에 Shodan 익숙하다고 가정합니다.

시작하기 전에
익스플로잇 통합에는 Shodan API 키가 필요합니다. 이 키를 얻으려면 무료 구독을 위해 Shodan 웹사이트에 등록하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필요한 역할: 관리자

이 태스크 정보

주:
통합을 실행하기 전에 요구 사항에 따라 필요한 구성을 변경합니다.

- NVD(NIST 취약성 데이터베이스) 데이터를 취약성 대응로 임포트하지 않은 경우 익스플로잇 통합을 설치하기 Shodan 전에 임포트합니다. NVD 데이터를 임포트하면 CVE(Common Vulnerability and Exposure) 데이터가 익스플로잇 기록을 자동으로 채웁니다.

  NVD 데이터가 없으면 익스플로잇 기록에 자리 표시자가 생성되고 다음 NVD 업데이트 때까지 입력되지 않습니다. NVD에 대한 자세한 내용은 를 참조하십시오 NVD 및 CWE 통합을 통해 데이터를 임포트하고 외부 공급업체 라이브러리를 관리합니다.

- 각 통합 기록에 대해 구성된 실행 사용자가 있습니다. 이 사용자의 기본값은 VR입니다. 시스템. 이 값은 변경하지 마십시오.

용 설치 **Shodan Exploit** 통합 및 구성 보안 운영

인스턴스에서 실행하려면 Shodan Exploit 통합 먼저 에서 ServiceNow Store다운로드하여 설치합니다. 이 애플리케이션은 별도의 구독으로 사용할 수 있습니다.

시작하기 전에
설치하기 전에 다음 설정 검사 목록을 완료합니다. 이러한 설정 작업은 원활한 설치 및 구성을 위해 필요합니다.

주:
이 프로세스는 프로덕션 인스턴스에 다운로드된 애플리케이션에만 적용됩니다. 애플리케이션을 비프로덕션 또는 개발 인스턴스에 다운로드하는 경우에는 권리를 얻을 필요가 없습니다. 로 애플리케이션 활성화 ServiceNow Store계속 진행합니다.

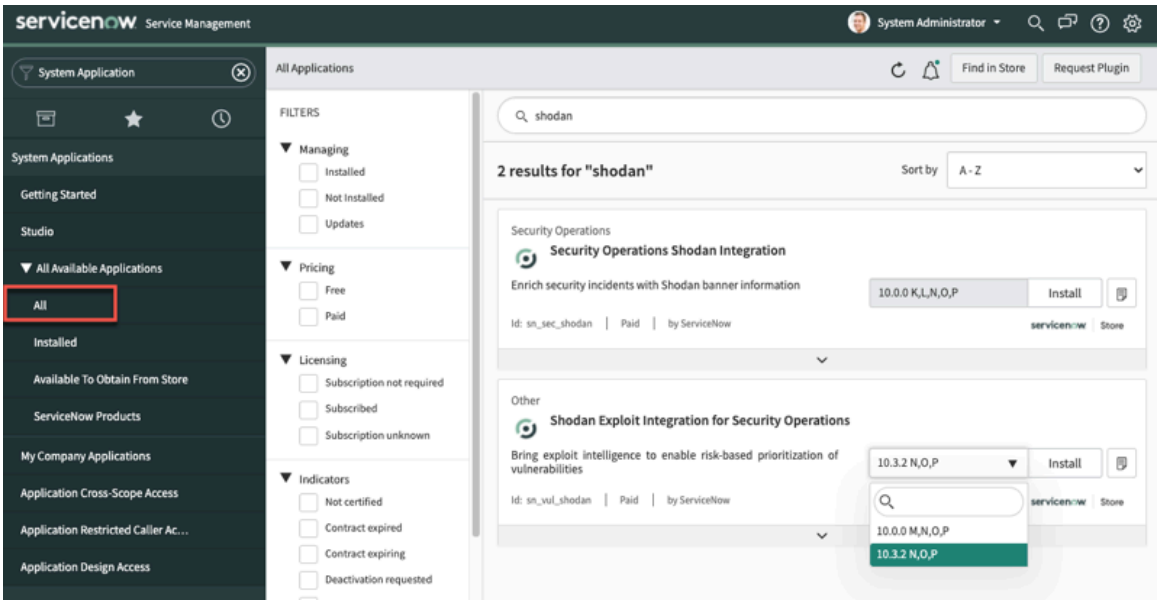
작업 설정	설명
애플리케이션 및 Shodan Exploit 통합 애플리케이션에 대한 보안 운영취약성 대응 유효한 ServiceNow 권리가 있는지 확인합니다.	권리를 확인하려면 다음으로 이동하십시오. 구독 관리 〉 구독 인스턴스에 있습니다. 목록에 조직이 구매한 구독이 표시됩니다. 에서 애플리케이션에 대한 보안 운영 권리를 얻는 방법에 대한 자세한 내용은 을 참조하십시오제품 또는 애플리케이션에 대한 보안 운영 권리 가져오기.ServiceNow Store
(선택 사항) 아직 설치 및 활성화되지 않은 경우 타사 애플리케이션을 설치하기 전에 애플리케이션을 설치하는 취약성 대응 것이 좋습니다.	애플리케이션 설치 및 활성화에 취약성 대응 대한 자세한 내용은 을 참조하십시오 취약성 대응 설치.
Shodan 익스플로잇 통합 API 키를 준비합니다.	익스플로잇 통합 준비 Shodan 문서를 참조하십시오.

필요한 역할: 관리자

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

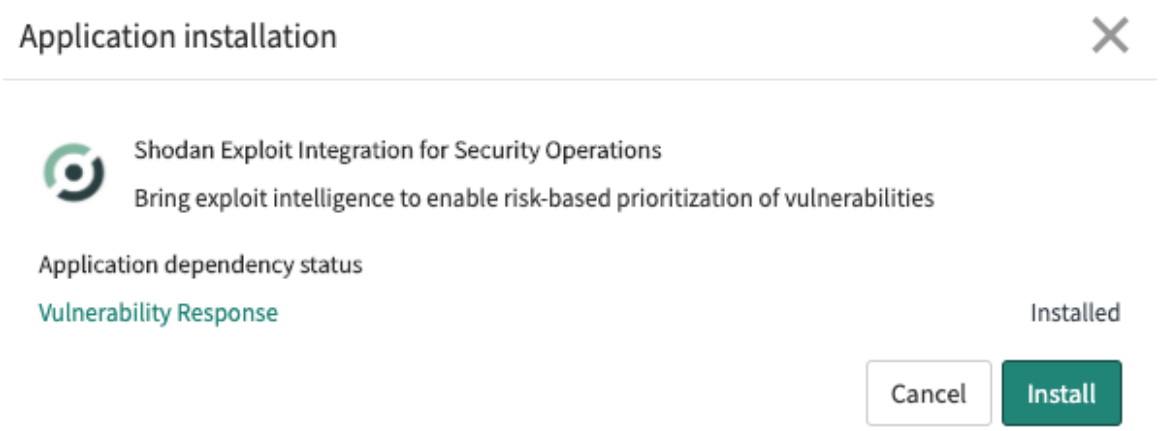
1. 애플리케이션을 설치할 Shodan Exploit 통합 인스턴스에 로그인합니다ServiceNow AI Platform.
2. 다음으로 이동 시스템 애플리케이션 〉 모든 사용 가능 애플리케이션 〉 모두.
3. 용 응용 프로그램을 찾아 Shodan Exploit 통합 원하는 버전을 선택하고 설치를 클릭합니다.보안 운영



주:
이 애플리케이션에 대한 업데이트를 받을 권리가 있는 경우 업데이트 버튼이 표시됩니다.

애플리케이션 설치 대화 상자에 애플리케이션 종속성 상태가 표시됩니다. 아직 설치되지 않은 필수 종속성은 애플리케이션과 함께 자동으로 설치됩니다.

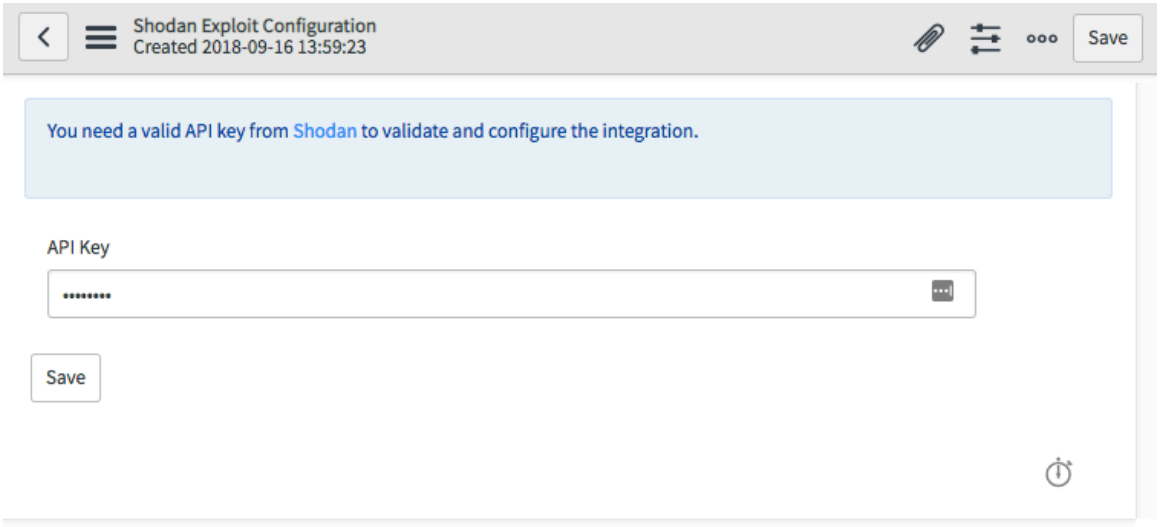
4. 대화 상자에서 Install(설치)을 클릭합니다.



설치 대화 상자에 설치가 성공적으로 완료된 시기가 표시됩니다.

5. 설치 대화 상자를 닫습니다.
6. 다음으로 이동 **Shodan Exploit Integration** 〉 구성.
7. Shodan API 키를 입력합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



8. 저장을 클릭합니다.
   Shodan Exploit 통합 구성이 완료되었습니다.

악용 통합 임포트 시간 설정 **Shodan**

편의를 위해 익스플로잇 통합의 Shodan 시작 시간을 재설정할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
초기 임포트 Shodan 후 익스플로잇 통합은 전체 임포트가 요청되지 않는 한 델타 데이터를 가져옵니다. 전체 임포트에 대한 자세한 내용은 을 참조하십시오 수동 Shodan 익스플로잇 임포트 수행 .

프로시저

1. 다음으로 이동 모두 〉 **Shodan Exploit Integration** 〉 통합.
2. 통합을 선택합니다.
3. 링크를 클릭하여 기록을 편집합니다.
4. 새 실행 및 시간 옵션을 설정합니다.
   시간은 현지 시간의 시간으로 계산됩니다. 익스플로잇 임포트의 Shodan 기본 시간은 03:15:00입니다.
5. 업데이트를 클릭합니다.
   새 시간은 다음으로 예약된 임포트에 사용됩니다.

수동 **Shodan** 익스플로잇 임포트 수행

초기 임포트에 실패했거나 예약된 초기 임포트를 기다리지 않으려면 매일 예약된 작업과 관계없이 전체 데이터 임포트를 수행할 수 있습니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)
가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 **Shodan Exploit Integration** 〉 통합.
2. 통합을 선택합니다.
3. 전체 데이터 가져오기 확인란을 선택합니다.
4. 지금 실행을 클릭합니다.
   임포트가 완료되면 확인란의 선택이 취소되고 델타 임포트가 재개됩니다.

Shodan 익스플로잇 통합 임포트 실행 상태 보기

취약성 통합 실행 관련 목록을 사용하여 통합 실행의 성공을 확인하고, 문제를 찾고, 정정 결정을 알립니다.

시작하기 전에
Shodan 임포트 실행 상태를 보려면 다음을 수행합니다.

- 취약성 대응 애플리케이션과 Shodan 익스플로잇 통합을 설치 및 구성해야 합니다.
- 익스플로잇 통합 임포트가 Shodan 예약되어 실행 중이어야 합니다.

필요한 역할: sn_vuln.admin

이 태스크 정보
통합 실행 중에 여러 프로세스가 생성되고 데이터가 페이지 형식으로 수신됩니다. 각 프로세스에는 페이지에 첨부된 데이터가 있는 하나 이상의 임포트 큐 항목이 포함될 수 있습니다. 이러한 항목은 1시간의 시간 제한 내에 데이터를 처리해야 합니다. 그러나 페이로드 크기가 크면 처리 시간이 1시간을 초과하거나 중단되어 통합 시간 제한 오류가 발생할 수 있습니다. 통합은 시간 초과 오류에도 불구하고 데이터를 계속 처리합니다. 이러한 잘못된 통신을 피하기 위해 버전 18.2.4 취약성 대응부터 큐가 활성 상태이고 데이터를 처리하는지 여부를 나타내기 위해 타임스탬프(하트비트)가 주기적으로 전송됩니다. 임포트 큐 항목 페이지의 처리된 마지막 기록 필드는 임포트 큐가 생성하거나 업데이트하는 기록 수에 따라 업데이트됩니다. 임포트 큐 항목이 1시간의 시간 제한을 초과하는 경우, 시스템은 마지막으로 처리된 기록 필드를 검사하여 1시간보다 오래되었는지도 확인합니다. 이 경우 이는 임포트 큐 항목이 고착되었음을 나타내며 처리 시 더 이상의 지연을 방지하기 위해 시간 초과됩니다.

주:
마지막으로 처리된 기록 필드는 다음 시스템 속성에 정의된 내용에 따라 업데이트됩니다.

- *sn_sec_cmn.record_threshold_heartbeat*: 하트비트(타임스탬프)가 임포트 큐 항목으로 전송된 후 처리된 기록 수를 정의합니다.
- *sn_sec_cmn.maximum_heartbeat_delay*: 임포트 큐 항목을 시간 초과해야 하는 시간을 정의합니다.

프로시저

1. 다음으로 이동 모두 〉 **Shodan Exploit Integration** 〉 통합.
2. 통합을 선택합니다.
3. 취약성 통합 실행 관련 목록을 클릭합니다.
4. 모든 임포트가 성공했는지 확인합니다.

Trouble?

실행 실패의 가장 일반적인 원인은 다음과 같습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 네트워크 중단
- 데이터 전송 시 비트 감쇠로 인해 변환 중 데이터가 손상됨

이러한 조건이 발생하면 전체 데이터 임포트 확인란을 선택하고 지금 실행을 클릭한 다음 통합을 다시 실행합니다.

Tenable 취약성 통합 이해

Vulnerability Response Integration with Tenable Tenable 취약성 통합을 위해 엔지니어링에서 ServiceNow 개발한 애플리케이션은 , Tenable.sc및 Tenable.cs 제품에서 Tenable.io임포트한 데이터를 사용하여 자산의 취약성에 우선순위를 지정하고 정정하는 데 도움을 줍니다. 이 애플리케이션은 .ServiceNow# Store

주:
의 구성 준수v14.9부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v14.9 이전 용어	용어 v14.9 이상
테스트 결과 그룹	정정 작업
그룹 규칙	정정 작업 규칙
정책	테스트 그룹

Tenable 취약성 통합은 세 가지 Tenable 통합, Tenable.io및 Tenable.scTenable.cs를 사용하여 자산 및 취약성에 대한 외부 공급업체 스캐너 데이터를 임포트합니다. 애플리케이션은 Vulnerability Response Integration with Tenable 버전 5.13 Tenable.cs 이상의 제품과 버전 5.0.1 이상의 제품을 지원합니다Tenable.sc.

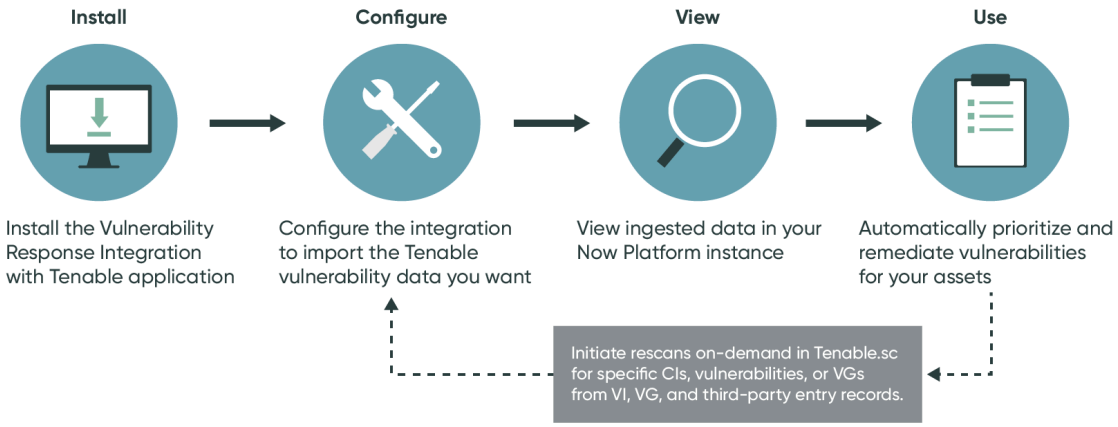
- Tenable.io 은 클라우드 기반 엔터프라이즈 통합입니다.
- Tenable.sc는 제품과 ServiceNow AI Platform 인스턴스가 동일한 환경에 있는 경우 Tenable.sc MID 서버를 사용하는 옵션을 제공하는 온 프레미스 통합입니다.
- Tenable.sc 제품과 ServiceNow AI Platform 인스턴스가 동일한 환경에 있지 않은 경우 MID 서버를 사용해야 합니다.
- Tenable.cs 은 클라우드 기반 엔터프라이즈 통합입니다.

이 Vulnerability Response Integration with Tenable 애플리케이션은 별도의 ServiceNow Store 구독으로 사용할 수 있습니다.

의 통합 Tenable Vulnerability Integration목록 및 설명은 및 Tenable.sc 애플리케이션과의 취약성 대응 통합를 참조하십시오Tenable.io및 구성 준수 애플리케이션과의 취약성 대응 통합.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Tenable 취약성 통합



에 사용 가능한 버전 **Yokohama**

릴리스 버전	릴리스 정보
Vulnerability Response Integration with Tenable v3.13.1, v4.1, v5.0.1	호환성 정보는 KB0856498 Vulnerability Response 호환성 매트릭스 및 릴리스 스키마 변경을 참조하십시오.

통합의 용어 및 주요 기능

취약한 항목 및 취약성

취약한 항목은 다음과 같은 경우에 인스턴스에 ServiceNow AI Platform 생성됩니다.

- 외부 공급업체 스캐너에서 임포트한 취약성이 기존 자산(의 CMDB구성 항목)과 일치합니다. Tenable 제품에서는 이러한 일치 항목을 취약성이라고 합니다.
- 외부 공급업체 스캐너에서 임포트한 취약성이 의 CMDB기존 자산과 일치하지 않습니다. 이 경우 일치하지 않는 CI도 취약한 항목과 함께 생성됩니다.

  일치하지 않는 CI의 경우 기존 CI를 호스트와 일치시킬 수 없을 때 IRE(식별 및 조정 엔진)를 사용하여 두 개의 새 클래스에 CI를 만들 수도 있습니다. 그렇지 않으면 일치하지 않는 CI 클래스에 일치하지 않는 CI가 생성됩니다. 자세한 내용은 식별 및 조정 엔진을 사용하기 위한 취약성 대응 CI 생성 문서를 참조하십시오.

타사 취약성 항목 및 플러그인

외부 공급업체 취약성 항목은 외부 공급업체 스캐너에서 임포트되어 인스턴스의 외부 공급업체 취약성 항목 테이블에 ServiceNow AI Platform 나열됩니다. v24.0 부터 취약성 대응외부 공급업체 취약성 항목 테이블의 소프트웨어 열에 외부 공급업체 항목과 연결된 CPE(공통 플랫폼 열거형)가 채워집니다. Tenable의 외부 공급업체 취약성 항목은 해당 CMDB자산에 취약성 대응 수집되어 해당 목록에 나열된 기존 자산과 일치합니다. Tenable에서는 타사 취약성 항목을 플러그인이라고 합니다.

CI(구성 항목)

구성 항목은 에 나열된 기존 자산입니다.CMDB

검색된 항목

Tenable 자산 임포트에서 수집된 자산은 의 기존 구성 항목 CMDB과 일치합니다. 임포트한 자산이 업데이트됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

일치하는 항목이 없으면 의 일치하지 않는 CI 클래스에 CMDBCI가 만들어집니다. CMDB CI Class Models 플러그인이 활성화되면 IRE(식별 및 조정 엔진)에서 새 클래스를 사용하여 CI를 만듭니다. 자세한 내용은 식별 및 조정 엔진을 사용하기 위한 취약성 대응 CI 생성 문서를 참조하십시오. 일치하지 않는 원래 CI가 재분류되면 검색된 항목 기록이 상태를 반영하도록 업데이트됩니다. 검색된 항목을 통해 자산을 식별하고 의 CI에 매핑하는 방법을 볼 수 있습니다 CMDB.

CI 조회 규칙

외부 공급업체 통합에서 데이터를 가져오면 Vulnerability Response는 자동으로 호스트(자산) 데이터를 사용하여 구성 관리 데이터베이스()CMDB에서 일치하는 항목을 검색합니다. CI 조회 규칙은 정정을 지원하기 위해 VIT가 생성될 때 CI를 식별하고 VI 기록에 추가하는 데 사용됩니다.

재스캔 및 정정 스캔

인스턴스의 취약한 항목, 정정 작업 및 외부 공급업체 취약성 항목 기록 ServiceNow AI Platform 에서 직접 특정 구성 항목, 정정 작업 또는 외부 공급업체 항목에 대해 대상 재스캔 명령을 시작할 수 있습니다. Tenable은 이 재스캔을 정정 검사라고 합니다.

이전 VI 자동 닫기

부실 취약한 항목 자동 종결 모듈을 ServiceNow AI Platform사용하면 외부 공급업체 통합에서 최근에 발견되지 않은 오래된 부실 VI(취약한 항목)를 정리할 수 있습니다. 이러한 VI를 종결 로 이동하면 활성 취약한 항목 및 정정 작업의 CMDB수를 줄이고 . 와의 Vulnerability Response Integration with Tenable 모든 통합을 사용하여 부실 VI를 자동으로 닫을 수 있습니다.

인스턴스

이 용어는 응용 프로그램의 고유한 발생 ServiceNow AI Platform# 을 나타냅니다.

통합

통합은 자산 통합 또는 플러그인 통합과 같은 통합에 대한 제품별 참조입니다 Tenable.ioTenable.sc . 이는 사용자 인스턴스의 Tenable 취약성 통합에 있는 특정 Tenable 제품에 속하는 별도의 통합입니다.

통합 인스턴스

이 용어는 및 Tenable.ioTenable.sc 제품별로 나열된 별도의 Tenable 통합을 나타냅니다.

배포

통합이 다중 소스를 지원하는 경우, 개별적인 단일 통합 존재를 통합의 배포라고 합니다. 이 용어는 환경 전반의 통합 및 제품을 참조하는 데 사용됩니다. 예를 들어, 사용자 환경에서 및 Tenable.sc 제품의 다양한 통합 Tenable.io 이 여러 개 배포되어 있을 수 있습니다.

, Tenable.sc및 Tenable.cs 통합에는 Tenable.io다음과 같은 주요 기능도 포함됩니다.

- 구성 평가 결과, 즉 정책, 구성 테스트(통제) 및 권한이 부여된 소스가 있는 인용과 함께 테스트 결과를 제품과 함께 애플리케이션으로 구성 준수 임포트할 수 있습니다 Tenable.io . 이 통합이 애플리케이션과 작동하는 구성 준수 방식에 대한 자세한 내용은 을 참조하십시오.Tenable.io및 구성 준수 애플리케이션과의 취약성 대응 통합구성 준수 탐색
- 의 Tenable Vulnerability Integrationv2.1부터 동일한 IP 주소를 공유하는 환경의 자산에 대해 서로 다른 네트워크 파티션 식별자를 포함하는 고유한 CI(구성 항목)를 생성합니다. 환경 전반에서 고유한 자산을 식별하고 기존 검색된 항목, 취약한 항목 및 탐지 기록의 CI를 업데이트하여 취약성에 대한 자세한 정보를 제공합니다.
- 모든 Tenable.io및 Tenable.scTenable.cs 통합에 대해 작업을 실행할 시기를 예약할 수 있습니다. 요청 시 예약된 작업을 수동으로 실행할 수도 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 를 사용하여 Tenable.io자산 임포트의 경우 자산 태그를 활성화하여 환경에 나열된 CMDBTenable.io 자산을 구성하고 추적할 수 있습니다.
- Tenable.io및 Tenable.scTenable.cs 통합을 사용하면 CI 조회 규칙을 구성하여 외부 공급업체 소스의 자산 데이터를 사용하여 사용자의 에서 CI(구성 항목)를 식별하는 방법을 정의할 수 있습니다ServiceNow AI Platform CMDB.
- Tenable.io및 Tenable.scTenable.cs 통합을 사용하면 취약성 임포트에 대한 임포트 필터를 설정하여 Tenable에서 원하는 취약성만 임포트할 수 있습니다. 의 경우 Tenable.io취약성 가져오기를 통해 Tenable에서 수정된 취약성을 임포트할 수 있는 옵션이 있습니다.
- 의 경우 Tenable.sc인스턴스의 취약한 항목, 정정 작업 및 외부 공급업체 항목 기록에서 직접 요청 시 재스캔을 시작할 수 있는 ServiceNow AI Platform 옵션이 있습니다. VI가 종결/고정으로 전환되었지만 인스턴스에서 아직 업데이트되지 않은 경우 특정 구성 항목의 취약성이 정정되었는지 확인할 수 있습니다. 통합에 대한 Tenable.sc 재스캔 시작 문서를 참조하십시오.

다음 섹션에는 Tenable 통합에 대한 자세한 내용이 나열되어 있습니다.

필요한 **ServiceNow AI Platform** 역할

통합 작업에는 인스턴스에서 다음 역할이 ServiceNow AI Platform 필요합니다.

관리자

시스템 관리자는 설정 도우미를 Vulnerability Response Integration with Tenable 사용하여 애플리케이션을 설치합니다. 할당되지 않은 경우 관리자는 취약성 관리자(sn_vul.vulnerability_admin) 및 설정 도우미의 다른 역할을 할당합니다.

sn_vul.vulnerability_admin

할당된 취약성 관리자는 설정 도우미에서 Tenable 통합의 구성을 완료합니다. 이 역할은 (VR) 애플리케이션 및 해당 기록에 대한 취약성 대응 전체 액세스 권한을 보유합니다. 취약성 관리자는 설치된 외부 공급업체 통합에 대해 모든 VR 애플리케이션과 규칙을 구성합니다.

sn_vul_tenable.configure_integration

이 역할에는 sn_vul_tenable.read_integration 세분화된 역할이 포함되어 있으며 이 역할을 가진 사용자는 애플리케이션을 구성할 Vulnerability Response Integration with Tenable 수 있습니다.

sn_vul_tenable.read_integration

이 역할을 가진 사용자는 애플리케이션의 기록을 Vulnerability Response Integration with Tenable 보고(읽음) 편집할 수 있지만 편집할 수는 없습니다.

취약성 대응 그룹

기본적으로 취약성 대응 그룹은 설정 도우미에서 사용할 수 있습니다. 취약성 대응 그룹에 할당된 사용자는 sn_vul.read_all 및 sn_vul.remediation_owner 역할을 자동으로 상속합니다.

취약한 항목

취약한 항목은 정정 작업 규칙에 따라 정정 작업으로 그룹화되고 할당 규칙에 따라 정정을 위해 할당됩니다. 자세한 내용은 취약성 대응 정정 작업 및 정정 작업 규칙 개요 및 취약성 대응 할당 규칙 개요 문서를 참조하십시오.

CI(구성 항목) 조회 규칙

CI 조회 규칙은 CI를 식별하고 취약한 항목에 추가할 시기를 결정합니다. CI 조회 규칙의 작동 방식에 대한 자세한 내용은 다음 문서를 참조하십시오 외부 공급업체 취약성 통합에서 취약성 대응 구성 항목을 식별하기 위한 CI 조회 규칙.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
제거된 규칙은 복구할 수 없습니다. 기존 규칙을 제거하는 대신 규칙을 만들 때 사용하지 않도록 설정하십시오.

다음 Tenable.io 조회 규칙은 기본 시스템과 함께 제공됩니다.

- MAC_ADDRESS
- FQDN
- NetBIOS
- 호스트 이름
- DNS
- IP

주:
Tenable.io CI 조회 규칙은 검색된 항목의 일반 FDQN, IPV4 및 MacAddress 값보다 비어 있지 않은 네트워크 인터페이스 값(FDQN, IPV4 및 MacAddress)의 우선순위를 정하고 채웁니다. 이러한 네트워크 인터페이스 값이 비어 있으면 검색된 항목에 대해 일반 FDQN, IPV4 및 MacAddress 값이 채워집니다.

다음 Tenable.sc 조회 규칙은 기본 시스템과 함께 제공됩니다.

- MAC_ADDRESS
- FQDN
- NetBIOS
- IP

주:
자산에 대해 ip_address, mac_address, fqdns 및 network_interfaces에 대한 여러 값이 사용됩니다. 모든 값은 일치를 위한 CI 조회 규칙에서 고려됩니다. 모든 값은 IRE를 사용하여 여러 네트워크 어댑터를 만드는 데 사용됩니다.

조회 규칙 클라우드 자원 ID는 Tenable.cs 기본 시스템과 함께 제공됩니다.

일치하지 않는 클라우드 자원의 분류를 기본 CI 클래스로 구성하는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 일치하지 않는 클라우드 자산에 대한 CI 클래스 업데이트 중.

IP 주소를 무시하는 새 속성

CI 조회 규칙의 일부로 여러 IP 주소나 여러 Mac 주소를 무시하려는 경우 에는 Tenable.io두 가지 속성을 사용할 수 있습니다.

ignoreIPAddress
: CI 조회 및 CI 생성시 무시되는 IP 주소 목록입니다.

ignoreMacAddress
: CI 조회 또는 CI 작성에서 무시할 MAC 주소 목록입니다.

검색된 항목

이 모듈에는 Tenable 취약한 항목 통합 및 Tenable 자산 통합에서 임포트하는 동안 탐지된 구성 항목이 나열됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
이 목록의 기본 필터는 #### ##으로 설정됩니다. 필터를 제거하여 임포트에서 검색된 모든 항목을 볼 수 있습니다.

검색된 항목 모듈에 대한 자세한 내용은 다음 문서를 참조하십시오 검색된 항목.

자산 태그

자산 태그(호스트 태그라고도 함)는 조직의 자산을 구성하고 추적하는 데 사용됩니다. 자산에 태그를 할당할 수 있습니다. 그런 다음 스캔을 시작할 때 스캔하려는 자산과 연결된 태그를 선택할 수 있습니다. 자산 태그 모듈을 사용하면 일정에 따라 인스턴스에서 인스턴스로 Tenable.io 자산 태그 데이터를 다운로드할 수 있습니다. 자산 태그를 포함하는 자산 데이터는 Tenable.io 자산 변환 통합 변환 맵을 사용하여 가져와서 Tenable.io 변환합니다.

모든 자산 태그는 자산 통합의 Tenable.io 일부로 임포트됩니다. 자산 태그는 담당 규칙 및 정정 작업 규칙의 취약성 대응 필터링에 사용됩니다. 검색된 항목 양식에 태그가 표시됩니다.

주:
Tenable.io 취약한 항목을 임포트 및 그룹화하기 전에 해당 규칙에 모든 태그를 사용할 수 있도록 애플리케이션에서 담당 규칙 또는 정정 작업 규칙을 취약성 대응 생성하기 취약성 대응 전에 자산 통합을 실행합니다. 태그에 대한 다음 사항도 참고하십시오.

- 태그 스토리지는 대/소문자를 구분하지 않습니다. 예를 들어 San Diego 위치의 자산을 설명하는 태그를 만들고 San Diego 태그를 만드는 경우 SAN DIEGO 태그를 생성하여 자산 태그 테이블에 저장할 수도 없습니다. San Diego 와 SAN DIEGO 는 시스템에서 동일한 자산 태그로 간주됩니다. 어떤 태그가 먼저 임포트되든 그 태그가 저장되고 인식됩니다.
- 정정 작업 규칙에서 자산 태그를 그룹 키로 사용하면 예기치 않은 결과가 발생할 수 있습니다. 자산 태그는 조건 작성기에서만 사용할 수 있습니다.
- 자산 태그는 전역 시스템 속성 sn_vul.import_asset_tags에 의해 제어됩니다. 이 속성은 기본적으로 true 로 설정됩니다. 태그를 비활성화하면 모든 ServiceNow AI Platform# 인스턴스에서 비활성화됩니다.

데이터 검색 필터

데이터 검색 설정은 Tenable 애플리케이션에서 인스턴스로 ServiceNow AI Platform# 임포트할 데이터의 유형과 범위를 구체적으로 결정하는 데 도움이 됩니다. 가장 일반적으로 사용되는 설정 목록은 문서를 참조하십시오 Tenable 취약성 통합에 대한 데이터 검색 설정.

취약성 우선순위 등급(VPR)

VPR(취약성 우선순위 등급)은 에서 임포트되어 새 기본 위험 계산기 취약성 대응와 함께 사용되는 Tenable 제품의 속성입니다. Tenable 위험 규칙은 의 취약성 계산기취약성 대응에 기본 위험 계산기의 일부로 애플리케이션과 함께 Vulnerability Response Integration with Tenable 설치됩니다.

이 위험 규칙은 기본적으로 비활성 상태입니다.

Tenable 위험 계산기 규칙을 사용하면 임포트한 VPR 값이 취약한 항목의 위험 점수를 계산하는 데 사용됩니다. 이 위험 계산기의 기본 가중치 분포는 VPR = 70%, 자산=15%, 비즈니스 중요도 =15%입니다. 이 Tenable 위험 계산기 규칙을 사용하도록 설정하면 데이터 수집 성능에 영향을 줄 수 있습니다. 계산기 및 Tenable 위험 계산기 규칙에 대한 취약성 대응 자세한 내용은 문서를 참조하십시오 취약성 대응 계산기 및 취약성 계산기 규칙.

설치 및 구성

에서 ServiceNow# Store다운로드한 Vulnerability Response Integration with Tenable 후 의 설치 및 구성은 의 설정 도우미취약성 대응에서 지원됩니다. 자세한 내용은 설정 지원을 사용하여 구성 취약성 대응 하기 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Tenable.io및 구성 준수 애플리케이션과의 취약성 대응 통합

Tenable.io 애플리케이션의 통합 Vulnerability Response Integration with Tenable 은 및 구성 준수 애플리케이션에서 사용할 수 취약성 대응 있습니다.

Tenable.io 통합 목록

모든 Tenable.io 및 Tenable.sc 통합에 대해 다중 소스가 지원됩니다. 의 취약성 대응설정 도우미에서 환경 전체에 다음 통합의 여러 인스턴스를 추가하고 배포할 수 있습니다. 또한 설정 도우미에서 애플리케이션을 설치하고 구성합니다 Vulnerability Response Integration with Tenable .

Tenable.io 은 클라우드 기반 엔터프라이즈 통합입니다. 제품에 대해 Tenable.io 지원되는 통합의 이름과 설명은 다음 표를 참조하십시오.

Tenable.io 규정 준수 결과 통합과 Tenable.io 규정 준수 결과 백필 통합은 기본적으로 비활성 상태입니다.

활성화하려면 다음을 수행합니다.

1. 다음으로 이동 **Tenable** 취약성 통합 〉 관리 〉 통합.
2. Tenable 통합 목록에서 통합 이름을 클릭하여 기록을 열고 활성 확인란을 선택하여 활성화합니다. 이러한 통합을 시작하려면 일정 설정을 기본값으로 두는 것이 좋습니다.

Tenable.io 통합

통합	설명
Tenable.io 자산 통합	• 제품에서 Tenable.io 자산 태그를 포함한 모든 자산 데이터를 검색하고 인스턴스에서 처리합니다. • v3.0부터 준수 결과 통합이 Tenable.io 활성화된 경우 임포트한 자산 데이터와 함께 보안 구성 평가 데이터를 임포트할 수 있습니다. 이 데이터는 자산의 구성 관련 취약성을 식별하고 대응하는 데 도움이 될 수 있습니다. • 일치하지 않는 자산에 대해 고유한 CI를 생성하거나 동일한 IP 주소를 공유하는 환경 전체의 자산에 대한 네트워크 파티션 식별자 속성으로 기존 CI를 업데이트합니다. • 자산 API에 대한 REST 메시지 호출을 조정합니다. • 이 통합의 출력은 검색된 항목입니다. • 데이터는 청크로 임포트되어 [sn_vul_tenable_chunk_status] 테이블에 저장됩니다. 테이블 클리너는 30일 후에 이 테이블에서 저장된 데이터를 자동으로 제거합니다. • v2.2부터는 *Last Scan Time* 취약성이 있는 자산에 대해서만 임포트 및 업데이트됩니다.
Tenable.io 준수 결과 통합	• v3.0부터 준수 결과 통합에서 임포트한 보안 구성 평가 데이터와 자산 통합에서 임포트한 데이터를 통해 자산의 구성 관련 취약성을 식별하고 대응할 수 있습니다. • 사용하도록 설정하면 높은 수준의 보안 구성 평가 데이터를 검색하고 인스턴스에서 ServiceNow AI Platform 처리합니다. 임포트된 데이터에는 정책, 구성 테스트(통제) 및 권한이 부여된 소스의 인용과 함께 테스트 결과가 포함됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Tenable.io 통합

통합	설명
	• 누락된 자산 또는 자산 ID가 없는 자산에 대한 평가 데이터는 임포트되지 않습니다. • 테스트 결과를 임포트하고 해당 자산을 인스턴스에서 일치시킬 수 없는 경우, 테스트 결과가 무시되고 누락된 자산의 ID가 [sn_vul_tenable_missing_asset] 테이블의 임시 기록에 저장됩니다. • 무시된(누락된) 자산의 총 값은 이 통합에 대한 통합 실행 기록의 구성 탭에 있는 무시된 **CI** 필드에 나열됩니다.
Tenable.io 준수 결과 백필 통합	• 활성화되면 자산 통합이 체인 통합 실행의 일부로 성공적으로 완료된 후 이 통합이 자동으로 실행됩니다. 이 통합은 구성 평가 데이터를 [sn_vul_tenable_missing_asset] 테이블에 나열된 누락된 자산과 일치시킵니다. • 자산 통합 임포트가 성공적으로 완료된 후 인스턴스에 발견되거나 존재하는 누락된 자산에 대해 최대 200개의 자산 ID를 임포트합니다. • 자산을 해당 구성 평가 데이터와 일치시킬 수 있는 경우 [sn_vul_tenable_missing_asset] 테이블에서 임시 기록을 제거합니다.
Tenable.io 스캔 자격 증명 통합	• 이 통합은 에서 구성된 검사 자격 증명을 검색합니다.Tenable.io • 자격 증명 API에 대한 REST 메시지 호출을 조정합니다. • 이 통합의 출력은 [sn_vul_tenable_scan_credential] 테이블에 채워진 검사 자격 증명입니다. • 임포트한 자격 증명은 스캔 요청이 에서 시작될 ServiceNow AI Platform때 스캐너에 액세스하는 데 사용됩니다. • 이 통합은 매주 실행되도록 예약되어 있습니다.
Tenable.io 템플릿 통합	다시 스캔하는 동안 템플릿 레코드가 전송됩니다 Tenable.io . 이 통합은 다시 스캔에 사용할 수 있는 Tenable.io 자격 증명을 검색합니다. 자격 증명은 인스턴스에 따라 다르며, 단일 템플릿 기록을 임포트하여 [sn_vul_tenable_io_template] 테이블에 임시로 안전하게 저장합니다.
Tenable.io 플러그인 통합	• 제품에서 Tenable.io 플러그인 데이터를 검색합니다. 검색된 데이터는 통합 실행에 의해 플러그인이 마지막으로 업데이트된 날짜를 기준으로 합니다 Tenable.io . • 이렇게 임포트하면 식별자(ID 10개)가 Tenable.io 최신 상태가 됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Tenable.io 통합

통합	설명
	• 플러그인 API에 대한 REST 메시지 호출을 조정합니다. • 이 통합의 출력은 외부 공급업체 취약성입니다.
Tenable.io 수정된 취약성 통합	• 제품의 심각도 필터를 Tenable.io 기반으로 취약성 데이터를 검색하고 인스턴스에서 처리합니다. 취약한 항목은 오픈 됨 및 다시 열림 상태의 탐지 기록에 대해 생성됩니다. 이러한 기록에는 정정이 필요하기 때문입니다. 탐지가 고정된 경우 기존의 취약한 항목이 Vulnerability Response에 의해 업데이트되지만, Tenable은 완화된 취약성 수정을 고려하기 때문에 기본적으로 고정 탐지에 대한 취약한 항목은 생성되지 않습니다. • 설정 도우미에서 고정 취약성 탐지에 대한 취약 시간 생성 플래그가 활성화되면 새 VI가 고정 상태로 생성되므로 이를 생성한 탐지에 대한 가시성을 확보할 수 있습니다. VI는 인스턴스에 아직 존재하지 않는 고정 탐지를 위해 생성되므로 임포트 성능에 부정적인 영향을 미칠 수 있습니다. 고정 탐지가 기존의 취약한 항목의 상태만 업데이트하도록 이 기능을 비활성화된 상태로 두는 것을 선호할 수 있습니다. • 일치하지 않는 자산에 대해 고유한 CI를 생성하거나 동일한 IP 주소를 공유하는 환경 전체의 자산에 대한 네트워크 파티션 식별자 속성으로 기존 CI를 업데이트합니다. • 취약성 API에 대한 REST 메시지 호출을 조정합니다. • 이 통합의 출력은 종결/고정 취약 항목(VI)입니다. 또한 자산 및 외부 공급업체 항목이 없는 경우 이를 생성합니다. • 데이터는 청크로 임포트되어 [sn_vul_tenable_chunk_status] 테이블에 저장됩니다. 테이블 클리너는 30일 후에 이 테이블에서 저장된 데이터를 자동으로 제거합니다. 이 통합 실행은 예약되어 있습니다. 이는 실행이 성공적으로 완료된 후 아래에 설명된 미해결 취약성 통합이 트리거되는 체인 통합입니다. Tenable v3.3부터 취약성 통합 실행에 대한 다음 정보를 볼 수 있습니다. • 총 청크: Tenable에서 생성되는 총 청크 수 • 사용 가능한 청크: 에 대해 다운로드할 수 있는 청크 수 ServiceNow
Tenable.io 미해결 취약성 통합	• 이 통합은 수정된 취약성 통합이 성공적으로 완료되면 트리거됩니다 Tenable.io . • 제품의 심각도 필터를 Tenable.io 기반으로 취약성 데이터를 검색하고 인스턴스에서 처리합니다. • 일치하지 않는 자산에 대해 고유한 CI를 생성하거나 동일한 IP 주소를 공유하는 환경 전체의 자산에 대한 네트워크 파티션 식별자 속성으로 기존 CI를 업데이트합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Tenable.io 통합

통합	설명
	• 취약성 API에 대한 REST 메시지 호출을 조정합니다. • 이 통합의 출력은 신규/재오픈 된 취약한 항목(VI)입니다. 또한 구성 항목 및 외부 공급업체 항목이 없는 경우 이를 생성합니다. Tenable은 활성 취약성을 누적 (현재)으로 간주합니다. • 데이터는 청크로 임포트되어 [sn_vul_tenable_chunk_status] 테이블에 저장됩니다. 테이블 클리너는 30일 후에 이 테이블에서 저장된 데이터를 자동으로 제거합니다. Tenable v3.3부터 취약성 통합 실행에 대한 다음 정보를 볼 수 있습니다. • 총 청크: Tenable에서 생성되는 총 청크 수 • 사용 가능한 청크: 에 대해 다운로드할 수 있는 청크 수 ServiceNow
Tenable.io/scan 메타데이터 통합	이 통합은 /scans 엔드포인트에서 메타데이터를 검색합니다. 의 Tenable.io기존 자산 데이터에서 last_schedule_id 기반으로 스캔 정보를 끌어옵니다. 에서 Tenable.io /scans 엔드포인트를 통합하려면 다음 구현 단계를 수행해야 합니다. • 테이블 생성: /scans 엔드포인트에서 Tenable.io검색된 스캔 메타데이터를 저장하기 위해 새 사용자 지정 테이블 **sn_vul_tenable_scan**이 생성됩니다. 여기에는 스캔 ID, 이름, 상태, 시작 시간, 종료 시간 및 스캔 유형과 같은 상세 정보가 포함됩니다. • 데이터 연결: 검색된 항목(구성 항목 또는 취약성)과 **sn_vul_tenable_scan** 테이블의 해당 최신 검사 기록 사이에 참조 필드가 설정됩니다. 이 연결을 통해 다음을 수행할 수 있습니다. ○ 검색된 각 항목과 관련된 최근의 스캔 정보를 봅니다. ○ 취약성 분류 및 정정 결정을 위한 컨텍스트를 개선합니다. ○ 스캔 활동의 이력 기록을 유지관리하여 감사 가능성과 보고 기능을 향상시킵니다.

Tenable.sc 애플리케이션과의 취약성 대응 통합

Tenable.sc 애플리케이션의 통합 Vulnerability Response Integration with Tenable

취약성 대응 v20.0부터 에이전트가 자산을 스캔하면 검색된 항목 목록의 "에이전트가 존재함" 열에 값이 "true"로 표시됩니다. 이는 스캔이 진짜임을 나타냅니다.

Tenable.sc 통합 목록

모든 Tenable.io 및 Tenable.sc 통합에 대해 다중 소스가 지원됩니다. 의 취약성 대응설정 도우미에서 환경 전체에 다음 통합의 여러 인스턴스를 추가하고 배포할 수 있습니다. 설정 도우미에서 Vulnerability Response Integration with Tenable 애플리케이션을 설치하고 구성할 수도 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- Tenable.sc는 제품과 ServiceNow AI Platform 인스턴스가 동일한 환경에 있는 경우 Tenable.sc MID 서버를 사용하는 옵션을 제공하는 온 프레미스 통합입니다.
- Tenable.sc 제품과 ServiceNow AI Platform 인스턴스가 동일한 환경에 있지 않은 경우 MID 서버를 사용해야 합니다.

Tenable.sc 통합

통합	설명
Tenable.sc 자산 통합	임포트한 자산 데이터로 검색된 항목이 중복되지 않도록 하기 위해 제품의 자산 통합 Tenable.sc 은 두 가지 통합으로 구성됩니다. Tenable.sc Open Assets 통합 이 통합은 Tenable이 누적 (현재) 또는 오픈으로 간주하는 자산에 대한 취약성 데이터를 임포트합니다. 임포트한 이 자산 데이터로 인스턴스에 생성된 취약한 항목(VI)은 열림(열림) 상태인 것으로 간주됩니다. 이러한 취약한 항목은 조사가 필요하며 수정이 필요할 수 있습니다. 고정 Tenable.sc 자산 통합 이 통합은 Tenable이 완화됨 (더 이상 취약하지 않음) 또는 수정됨으로 간주하는 자산에 대한 취약성 데이터를 임포트합니다. 이러한 자산의 취약한 항목은 검사 결과 더 이상 취약하지 않은 것으로 나타나기 때문에 인스턴스에서 열림 상태에서 종결/고정 상태로 전환됩니다. • 제품에서 Tenable.sc 모든 자산 데이터를 검색하여 인스턴스에서 처리합니다. • 일치하지 않는 자산에 대해 고유한 CI를 생성하거나 IP 주소를 공유하는 환경 전체의 자산에 대한 네트워크 파티션 식별자 속성으로 기존 CI를 업데이트합니다. • 자산 API에 대한 REST 메시지 호출을 조정합니다. • 이 통합의 출력은 검색된 항목입니다. • 설정 도우미에서 선택하는 Tenable 쿼리 필터는 자산 통합에도 Tenable.sc 적용됩니다. 쿼리 필터의 조건과 일치하는 취약성이 있는 자산만 임포트됩니다.
Tenable.sc 플러그인 통합	• 제품에서 Tenable.sc 플러그인 데이터를 검색합니다. 검색된 데이터는 통합 실행에 의해 플러그인이 마지막으로 업데이트된 날짜를 기준으로 합니다 Tenable.sc . • 이렇게 임포트하면 식별자(ID 10개)가 Tenable.sc 최신 상태로 유지되고 활성 상태인 취약성만 임포트됩니다. • 플러그인 API에 대한 REST 메시지 호출을 조정합니다. • 이 통합의 출력은 외부 공급업체 취약성입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Tenable.sc 통합

통합	설명
Tenable.sc 수정된 취약성 통합	• 제품의 심각도 필터를 Tenable.sc 기반으로 취약성 데이터를 검색하고 인스턴스에서 처리합니다. 취약한 항목은 오픈 됨 및 다시 열림 상태의 탐지 기록에 대해 생성됩니다. 이러한 기록에는 정정이 필요하기 때문입니다. 탐지가 고정된 경우 기존 취약한 항목이 취약성 대응에 의해 업데이트되지만, Tenable은 완화된취약성 수정을 고려하기 때문에 기본적으로 고정 탐지에 대해 취약한 항목이 생성되지 않습니다. • 설정 도우미에서 고정 취약성 탐지에 대한 취약 시간 생성 플래그가 활성화되면 **VI** 를 생성한 탐지를 볼 수 있도록 고정 상태의 VI를 생성합니다. VI는 인스턴스에 존재하지 않는 고정 탐지를 위해 생성되므로 임포트 성능에 부정적인 영향을 미칠 수 있습니다. 고정 탐지가 기존의 취약한 항목의 상태만 업데이트하도록 이 기능을 비활성화된 상태로 두는 것을 선호할 수 있습니다. • 일치하지 않는 자산에 대해 고유한 CI를 생성하거나 IP 주소를 공유하는 환경 전체의 자산에 대한 네트워크 파티션 식별자 속성으로 기존 CI를 업데이트합니다. • 취약성 API에 대한 REST 메시지 호출을 조정합니다. 이 통합의 출력은 종결/고정 취약 항목(VI)입니다. 또한 자산 및 외부 공급업체 항목이 없는 경우 이를 생성합니다. 이 통합 실행은 예약된 실행입니다. 이는 실행이 성공적으로 완료된 Tenable.sc 후 다음에 설명된 미해결 취약성 통합이 트리거됨을 의미하는 체인 통합입니다. 주: 기본적으로 제품군 ID 0과 39는 이 통합에서 제외됩니다.
Tenable.sc 미해결 취약성 통합	• 이 통합은 고정된 취약성 통합이 성공적으로 완료될 때 트리거됩니다 Tenable.sc . • 제품에서 Tenable.sc 선택한 쿼리 필터를 기반으로 취약성 데이터를 검색하고 인스턴스에서 처리합니다. • 활성 취약성에 해당하는 취약한 항목을 생성합니다. • 일치하지 않는 자산에 대해 고유한 CI를 생성하거나 IP 주소를 공유하는 환경 전체의 자산에 대한 네트워크 파티션 식별자 속성으로 기존 CI를 업데이트합니다. • 취약성 API에 대한 REST 메시지 호출을 조정합니다. • 이 통합의 출력은 새로운 취약한 항목(VI)이 없는 경우 업데이트/생성 입니다. 또한 구성 항목 및 외부 공급업체 항목이 없는 경우 이를 생성합니다. 주: 기본적으로 제품군 ID 0과 39는 이 통합에서 제외됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Tenable.sc 통합

통합	설명
Tenable.sc 스캔 자격 증명 통합	• 이 통합은 에서 구성된 검사 자격 증명을 검색합니다.Tenable.sc • 자격 증명 API에 대한 REST 메시지 호출을 조정합니다. • 이 통합의 출력은 테이블 〔sn_vul_tenable_scan_credential〕에 채워진 검사 자격 증명입니다. • 임포트한 자격 증명은 스캔 요청이 에서 시작될 ServiceNow AI Platform때 스캐너에 액세스하는 데 사용됩니다. • 이 통합은 매주 실행되도록 예약되어 있습니다.
Tenable.sc 취약성 통합 백필	• 이 채우기 통합은 임포트 중에 누락되었을 수 있는 미해결 취약성과 수정된 취약성을 임포트합니다. • 이 통합은 지난 7일 동안의 미해결된 취약성과 수정된 취약성을 모두 임포트하여 탐지 및 취약한 항목을 업데이트합니다. • 이 통합은 성능에 영향을 줄 수 있습니다. • 이 통합은 기본적으로 비활성 상태입니다. • 취약성 데이터를 업데이트하고 잠재적인 성능 문제를 방지하려면 실행 중인 다른 검사가 없을 때 실행되도록 Tenable.sc 수정된 취약성 및 미해결 취약성 통합을 예약하는 것이 좋습니다. • 이 통합의 출력은 다음과 같습니다. ○ 종결/고정 취약 항목(VI). 또한 자산 및 외부 공급업체 항목이 없는 경우 이를 생성합니다. ○ 취약한 항목(VI)이 없는 경우 업데이트/생성할 수 있습니다. 또한 구성 항목 및 외부 공급업체 항목이 없는 경우 이를 생성합니다.

사용자 인증 및 **Tenable.sc**

사용자 인증은 인스턴스 ServiceNow AI Platform# 와 제품의 버전 5.13 Tenable.sc 에서 지원됩니다. 버전 5.12 및 이전 버전의 제품을 사용하는 경우 사용자 인증이 Tenable.sc 필요합니다.

통합에 Tenable.sc 대한 사용자 인증을 선택하면 통합 실행 중에 토큰이 만료되고 대체될 수 있습니다. 취약성 통합 실행 기록(VIN)의 메모 열에 토큰이 만료될 때 프로세스에 대해 다음 메시지가 표시됩니다. ##: ## ### ### ######. 이 메시지가 표시되는 경우 아무 작업도 필요하지 않습니다. 만료된 토큰은 백그라운드에서 자동으로 새로 고쳐지며 메시지는 통합 프로세스의 일시 중지나 오류를 나타내지 않습니다.

Tenable.cs및 컨테이너 취약성 대응 애플리케이션과의 취약성 대응 통합

Tenable.cs 애플리케이션의 통합 Vulnerability Response Integration with Tenable 은 취약성 대응 및 컨테이너 취약성 대응 애플리케이션에서 사용할 수 있습니다.

v20.0 취약성 대응부터 에이전트가 자산을 스캔하면 검색된 항목 목록의 "에이전트가 존재함" 열에 "true"가 표시되어 스캔이 진짜임을 나타냅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Tenable.cs 통합 목록

모든 Tenable.io, Tenable.sc, 통합 Tenable.cs 에 대해 다중 소스가 지원됩니다. 의 취약성 대응설정 도우미에서 환경 전체에 다음 통합의 여러 인스턴스를 추가하고 배포할 수 있습니다. 설정 도우미에서 Vulnerability Response Integration with Tenable 애플리케이션을 설치하고 구성할 수도 있습니다.

Tenable.cs 은 클라우드 기반 엔터프라이즈 통합입니다. 제품에 대해 Tenable.cs 지원되는 통합의 이름과 설명은 다음 표를 참조하십시오.

Tenable.cs 통합

통합	설명
Tenable.cs 클라우드 컨테이너 자산 통합	• 제품에서 Tenable.cs 모든 컨테이너 자산 데이터를 검색하여 인스턴스에서 처리합니다. • 일치하지 않는 자산에 대해 고유한 CI를 만들거나 기존 CI를 업데이트합니다. 자산 API에 대한 REST 메시지 호출을 조정합니다. 이 통합의 출력은 검색된 컨테이너 이미지, Docker 이미지 및 컨테이너 리포지토리입니다.
Tenable.cs 클라우드 컨테이너 취약성 통합 열기	활성화되면 컨테이너 자산 통합이 체인 통합 실행의 일부로 성공적으로 완료된 후 이 통합이 자동으로 실행됩니다. • 제품의 심각도 필터를 Tenable.cs 기반으로 컨테이너 취약성 데이터를 검색하고 인스턴스에서 처리합니다. • 일치하지 않는 자산에 대해 고유한 CI를 만들거나 기존 CI를 업데이트합니다. • 취약성 API에 대한 REST 메시지 호출을 조정합니다. 이 통합의 출력은 신규/재개시됨컨테이너 CVI(취약한 항목)입니다. 없는 경우 검색된 컨테이너 이미지, Docker 이미지, 컨테이너 리포지토리, 이미지 결과, 타사 항목 및 CVE(Common Vulnerabilities and Exposures)도 생성합니다.
Tenable.cs 클라우드 컨테이너 취약성 통합 수정	이 통합은 Open Cloud Container 취약성 통합이 Tenable.cs 성공적으로 완료될 때 트리거됩니다. • 제품의 심각도 필터를 Tenable.cs 기반으로 컨테이너 취약성 데이터를 검색하고 인스턴스에서 처리합니다. • 일치하지 않는 자산에 대한 고유 CI를 작성하거나 기존 CI를 업데이트합니다 • 취약성 API에 대한 REST 메시지 호출을 조정합니다. 이 통합의 출력은 신규/재오픈된 컨테이너 취약 항목 (CVI)입니다. 없는 경우 컨테이너 이미지 검색, Docker 이미지, 컨테이너 리포지토리, 이미지 결과, 타사 항목 및 CVE도 생성합니다. 이미지 찾기가 종결 상태로 생성됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Tenable.cs 통합

통합	설명
Tenable.cs 클라우드 호스트 취약성 통합 열기	• 제품의 심각도 필터를 Tenable.cs 기반으로 취약성 데이터를 검색하고 인스턴스에서 처리합니다. • 일치하지 않는 자산에 대해 고유한 CI를 만들거나 기존 CI를 업데이트합니다. • 취약성 API에 대한 REST 메시지 호출을 조정합니다. 이 통합의 출력은 신규/재오픈된 취약한 항목(VI)입니다. 없는 경우에는 구성 항목, 타사 항목 및 CVE도 생성됩니다. 취약성 탐지는 오픈 상태로 생성됩니다.
Tenable.cs 클라우드 호스트 취약성 통합 수정	이 통합은 오픈 클라우드 호스트 취약성 통합이 Tenable.cs 성공적으로 완료될 때 트리거됩니다. • 제품의 심각도 필터를 Tenable.cs 기반으로 취약성 데이터를 검색하고 인스턴스에서 처리합니다. • 일치하지 않는 자산에 대해 고유한 CI를 만들거나 기존 CI를 업데이트합니다. • 취약성 API에 대한 REST 메시지 호출을 조정합니다. 이 통합의 출력은 가까운 취약 항목(VI)입니다. 없는 경우에는 구성 항목, 타사 항목 및 CVE도 생성됩니다. 취약성 탐지가 종결 상태로 생성됩니다.

사용자 인증 및 **Tenable.sc**

사용자 인증은 인스턴스 ServiceNow AI Platform# 와 제품의 버전 5.13 Tenable.sc 에서 지원됩니다. 버전 5.12 및 이전 버전의 제품을 사용하는 경우 사용자 인증이 Tenable.sc 필요합니다.

통합에 Tenable.sc 대한 사용자 인증을 선택하면 통합 실행 중에 토큰이 만료되고 대체될 수 있습니다. 취약성 통합 실행 기록(VIN)의 메모 열에 토큰이 만료될 때 프로세스에 대해 다음 메시지가 표시됩니다. ##: ## ### ### ######. 이 메시지가 표시되는 경우 아무 작업도 필요하지 않습니다. 만료된 토큰은 백그라운드에서 자동으로 새로 고쳐지며 메시지는 통합 프로세스의 일시 중지나 오류를 나타내지 않습니다.

Tenable 취약성 통합 준비

ServiceNow# 다음 설정 작업을 수행하여 Tenable 취약성 통합을 준비합니다.

시작하기 전에

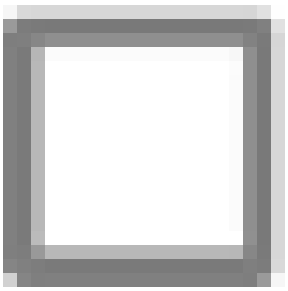
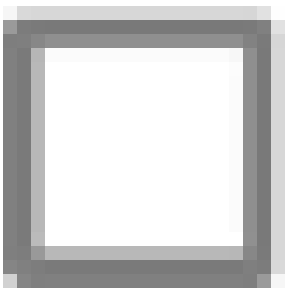
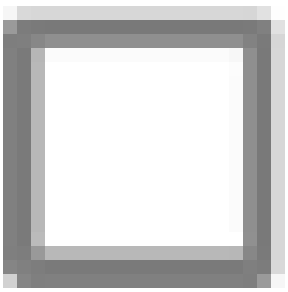
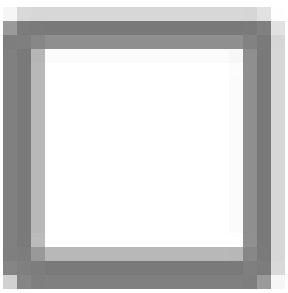
성공적인 통합을 위해서는 통합 전 작업을 계획하고 신중하게 실행해야 합니다. 애플리케이션의 원활한 설치 및 구성을 Vulnerability Response Integration with Tenable 위해 애플리케이션을 설치하고 취약성 데이터를 인스턴스로 ServiceNow AI Platform# 임포트하기 전에 다음 검사 목록을 인쇄하고 나열된 항목이 완료되었는지 확인하는 것이 좋습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

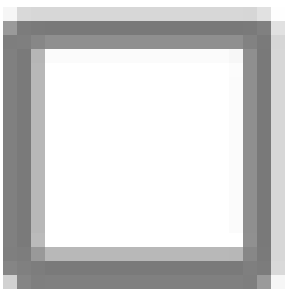
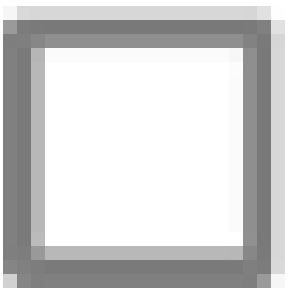
주:
Tenable이 구축한 통합으로 데이터를 임포트해 왔으며 Tenable과의 취약성 대응 통합을 사용하여 ServiceNow# 시작하려는 경우 문서를 참조하십시오.

Tenable이 구축한 통합에서 에서 빌드한 ServiceNow통합으로의 현재 데이터 정리 및 마이그레이션 정보는 Tenable 취약성 대응 통합에서 Tenable과 ServiceNow 취약성 대응 통합으로 마이그레이션하기 위한 가이드라인 (KB0960667) 문서를 참조하십시오.

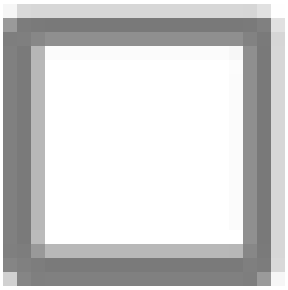
필요한 역할: 애플리케이션을 다운로드하고 설치하기 위한 관리자

작업	설명
	(선택 사항) 아직 설치 및 활성화되지 않은 경우 타사 애플리케이션을 설치하기 전에 애플리케이션을 설치하는 취약성 대응 것이 좋습니다. 애플리케이션 설치 및 활성화에 취약성 대응 대한 자세한 내용은 을 참조하십시오 취약성 대응 설치. 이 통합에는 버전 12.1 취약성 대응 이상이 필요합니다.
	인스턴스에 아직 없는 경우 권리를 얻고 인스턴스에 애플리케이션을 ServiceNow AI Platform# 다운로드합니다Vulnerability Response Integration with Tenable. 애플리케이션은 Vulnerability Response Integration with Tenable 버전 5.13 Tenable.cs 이상의 제품과 버전 5.0.1 이상의 제품을 지원합니다Tenable.sc. .
	임포트할 것으로 예상되는 취약한 항목의 수를 예상합니다. 임포트하려는 취약한 항목 수를 인스턴스가 수락할 수 있는지 확인합니다. 인스턴스 크기가 작으면 로드 시간이 길어질 수 있습니다. 인스턴스 크기를 모르거나 도움이 필요한 경우 기술 지원에 문의하십시오 ServiceNow# .
	통합을 관리하고 취약한 항목을 정정할 그룹 또는 사용자가 있는지 확인합니다. 관리자 시스템 관리자는 설정 도우미를 Vulnerability Response Integration with Tenable 사용하여 애플리케이션을 설치합니다. 할당되지 않은 경우 관리자는 취약성 관리자 (sn_vul.vulnerability_admin) 및 설정 도우미의 다른 역할을 할당합니다. sn_vul.vulnerability_admin 할당된 취약성 관리자는 Tenable 통합의 구성을 완료합니다. 이 역할은 (VR) 애플리케이션 및 해당 기록에 대한 취약성

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업	설명
	대응 전체 액세스 권한을 보유합니다. 모든 VR 애플리케이션 및 규칙을 구성하고 외부 공급업체 통합을 구성합니다. sn_vul_tenable.configure_integration Tenable 취약성 통합을 구성할 수 있습니다. 이 역할에는 sn_vul_tenable.read_integration 세분화된 역할이 포함됩니다. sn_vul_tenable.read_integration Tenable 취약성 통합의 기록을 보거나 읽을 수 있습니다. 취약성 대응 그룹 기본적으로 취약성 대응 그룹은 설정 도우미에서 사용할 수 있습니다. 취약성 대응 그룹에 할당된 사용자는 sn_vul.read_all 및 sn_vul.remediation_owner 역할을 자동으로 상속합니다. 시스템 관리자는 통합을 위해 설정 도우미에서 사용자 및 그룹에 초기 역할 할당을 수행합니다. 기본적으로 취약성 대응 그룹을 사용할 수 있습니다. 아직 생성하지 않은 경우, 설정 도우미를 사용하기 전에 추가 그룹을 생성하고 인스턴스에서 사용자 관리 모듈을 사용하여 사용자를 추가하는 것이 좋습니다. 사용자 그룹 만들기를 참조하십시오. 가상 사용자 및 세분화된 역할을 사용하여 사용자가 Vulnerability Response 애플리케이션에서 확인하고 수행할 수 있는 내용을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할을 처음 할당하려면 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당.
	첫 번째 임포트의 성능을 향상시키려면 인스턴스에서 특정 기능, 규칙 또는 작업을 비활성화하는 것이 좋습니다. • 취약성 계산기를 사용하지 않는 경우 비활성화합니다. 이러한 계산기와 사용자가 정의한 계산기는 취약한 항목 레코드가 생성되거나 업데이트될 때마다 실행됩니다. 취약성 계산기 사용 안 함의 내용을 참조하십시오. • 기록을 처음 임포트하는 동안 특정 알림 관련 비즈니스 규칙으로 인해 많은 알림이 생성되어 성능에 영향을 줄 수 있습니다. 초기 임포트에 앞서 설명된 Tenable 취약성 통합에 대한 수정 사항 임포트대로 알림 관련 비즈니스 규칙을 비활성화하는 것이 좋습니다.
	통합에 필요한 인스턴스의 기능, 규칙, 의존성 플러그인 또는 작업을 활성화했는지 확인합니다. • Tenable.sc는 제품과 ServiceNow AI Platform 인스턴스가 동일한 환경에 있는 경우 Vulnerability Response Integration with Tenable MID 서버를 사용하는 옵션을 제공하는 온 프레미스 통합입니다. Tenable.sc 제품과 ServiceNow AI Platform 인스턴스가 동일한 환경에 있지 않은 경우 MID 서버를 사용해야 합니다. 인스턴스의 MID 서버에 대한 자세한 내용은 MID 서버 단원을 참조하십시오. • 통합 허브 플러그인이 설치되고 활성화되었는지 확인합니다. 이 플러그인을 사용하면 기본 시스템 구성요소에서 통합 API를 사용하여

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업	설명
	외부 시스템을 호출하고 REST와 같은 프로토콜 단계를 활성화할 수 있습니다. 다음으로 이동 시스템 애플리케이션 〉 모든 사용 가능 애플리케이션 〉 모두 플러그인을 찾습니다. 인스턴스에 설치되어 있지 않은 경우 설치하고 활성화합니다.
	Tenable 자격 증명을 얻습니다. Tenable 제품에 액세스할 수 있도록 Tenable 제품에 필요한 계정 이름, 암호 및 기타 서비스 정보가 있는지 확인합니다. Tenable.io 권한 속성이 64 이상인 관리자 액세스 권한이 필요합니다. Tenable.sc 보안 분석가 또는 관리자 액세스 권한이 필요합니다. 주: 의 Vulnerability Response Integration with Tenablev3.8부터는 더 이상 관리자 Tenable.io 권한이 필요하지 않습니다. 권한 속성이 16인 기본 사용자도 제품에 액세스할 수 있습니다.

준비가 완료되었습니다 설정 도우미를 Vulnerability Response Integration with Tenable 사용하여 애플리케이션 설치.

설정 도우미를 **Vulnerability Response Integration with Tenable** 사용하여 애플리케이션 설치

Tenable 취약성 통합을 실행하기 ServiceNow# 전에 에서 ServiceNow Store 애플리케이션을 다운로드하고 Vulnerability Response Integration with Tenable 애플리케이션에서 설정 도우미 취약성 대응 를 사용하여 설치하고 구성해야 합니다.

시작하기 전에
Tenable 애플리케이션을 설치하기 전에 의 Tenable 취약성 통합 준비검사 목록에 있는 모든 항목을 완료했는지 확인하십시오.

주:
이 프로세스는 프로덕션 인스턴스에 다운로드된 애플리케이션에만 적용됩니다. 애플리케이션을 비프로덕션 또는 개발 인스턴스에 다운로드하는 경우에는 권리를 얻을 필요가 없습니다. 로 애플리케이션 활성화 ServiceNow Store계속 진행합니다.

필요한 역할: admin sn_vul.vulnerability_admin 역할의 초기 할당과 설정 도우미에 Tenable 애플리케이션 설치를 위한 admin. 취약성 관리자(sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음))는 애플리케이션을 설치한 후 설정 도우미에서 애플리케이션을 구성할 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 설정 도우미 〉 통합 애플리케이션 설치.

   잠시 후 인스턴스에 설치할 수 있는 애플리케이션이 표시됩니다.

2. **Tenable(Tenable** 플랫폼) 타일을 찾아 설치를 클릭하십시오.

   이 작업은 에서 ServiceNow Store다운로드한 애플리케이션을 설치합니다Vulnerability Response Integration with Tenable.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 설치 도우미에 제공된 프롬프트에 따라 설치를 계속합니다.
4. 설치 도우미를 사용하여 응용 프로그램을 설치하는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 설정 도우미를 사용하여 타사 응용 프로그램 설치 취약성 대응.

다음에 수행할 작업
설정 도우미에서 설치를 완료한 후 설정 도우미에서 통합 구성〉스캐너 통합 으로 이동하여 구성을 계속합니다. 설정 도우미에서 제공되는 프롬프트를 보완하는 자세한 내용은 문서를 참조하십시오 설정 도우미를 사용하여 Tenable 취약성 통합 구성.

Tenable 취약성 통합에 대한 데이터 검색 설정

다음 데이터 검색 설정은 Tenable 취약성 통합에서 ServiceNow# 인스턴스로 ServiceNow AI Platform# 임포트하려는 데이터의 유형과 범위를 구체적으로 결정하는 데 도움이 됩니다.

다음 섹션에 설명된 설정은 가져올 데이터를 제어하는 데 도움이 됩니다. 또한 통합 인스턴스에서 이러한 필터의 값을 설정할 수 있습니다. 통합 인스턴스를 보려면 다음으로 이동하십시오. **Tenable** 취약성 통합 〉 통합 인스턴스 을 클릭하고 통합, Tenable.io, 또는 Tenable.scTenable.cs를 선택합니다.

표시되는 통합 인스턴스 페이지에서 통합 인스턴스 매개변수를 선택하여 매개변수 목록을 표시하거나 일정, REST 상세 정보, 통합 상세 정보, 데이터 소스 및 통합 실행 정보에 대한 취약성 통합 탭을 표시합니다.

, **Tenable.sc** 인스턴스에 **Tenable.cs** 대한 **Tenable.io**공통 심각도 및 검색 설정과 필터 **ServiceNow AI Platform**

인스턴스의 , , 통합에 Tenable.io다음 설정을 사용할 수 있습니다ServiceNow AI Platform.Tenable.csTenable.sc 이러한 구성 설정 및 기타 구성 설정은 인스턴스의 ServiceNow AI Platform 통합 인스턴스 페이지에 표시됩니다. 처음 몇 개의 통합 실행에 대해 이러한 설정을 기본값으로 두는 것이 좋습니다.

Tenable.io

insert_fixed

취약성 임포트 통합을 위해 설정 도우미에서 **insert_fixed** 플래그를 활성화하면 인스턴스에 존재하지 않는 고정 상태의 탐지에 대해 새 VI가 생성됩니다.

severity_critical

이 필터는 기본적으로(예) 활성화되어 미해결 취약성 및 Tenable.io 수정된 취약성 통합에서 중요 심각도 취약성을 수신합니다Tenable.io.

severity_high

이 필터는 기본적으로(예) 활성화되어 미해결 취약성 및 Tenable.io 수정된 취약성 통합에서 높은 심각도 취약성을 수신합니다Tenable.io.

severity_medium

이 필터는 기본적으로 비활성입니다(False). 이 필터를 활성화하여 미해결 취약성 및 Tenable.io 수정된 취약성 통합에서 중간 수준의 심각도 취약성을 수신합니다Tenable.io.

severity_info

이 필터는 기본적으로 비활성입니다(False). 이 필터를 활성화하여 오픈 취약성 및 Tenable.io 수정된 취약성 통합에서 정보 수준의 심각도 취약성을 수신합니다Tenable.io.

severity_low

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 필터는 기본적으로 비활성입니다(False). 이 필터를 활성화하여 오픈 취약성 및 Tenable.io 수정된 취약성 통합에서 낮은 심각도 취약성을 수신합니다Tenable.io.

크기

이 설정은 플러그인 통합의 결과 세트에 Tenable.io 포함할 플러그인 기록 수를 정의합니다. int32 형식이어야 합니다. 기본값은 1,000입니다. 최대 크기는 10,000입니다.

num_assets

수정된 취약성 및 Tenable.io 미해결 취약성 통합에서 익스포트한 Tenable.io 청크당 최대 취약성 수입니다. 기본값은 50입니다.

chunk_size

자산 통합에서 익스포트한 청크당 Tenable.io 자산 수를 지정합니다. 기본값은 1,000입니다.

Tenable.sc

async_request

이 매개변수는 기본적으로 비활성입니다(false). 이 매개변수를 활성화 또는 비활성화하여 각각 비동기 또는 동기 API 호출을 Tenable.sc 수행합니다. 동기 호출의 경우 30초에 시간 제한이 있으면 Tenable 제품에 대한 지원팀에 문의하여 상자를 조정합니다. 이 매개변수는 활성화되면 의 모든 통합 Tenable.sc에 적용할 수 있습니다. 비동기 호출을 사용하는 기존 고객의 경우 기존 Tenable.sc 통합 인스턴스에 새 async_request 매개변수를 추가하는 수정 스크립트를 사용할 수 있습니다. 수정 스크립트를 보려면 다음으로 이동하십시오. 시스템 정의 〉 스크립트 수정.

insert_fixed

취약성 임포트 통합을 위해 설정 도우미에서 **insert_fixed** 플래그를 활성화하면 인스턴스에 존재하지 않는 고정 상태의 탐지에 대해 새 VI가 생성됩니다.

오프셋

하나의 통합 실행에서 임포트되는 자산, 플러그인 및 취약성 수를 지정합니다.

쿼리 필터

쿼리 필터는 Tenable 콘솔 내에서 구성됩니다. 이러한 쿼리 필터에는 설정 도우미 또는 인스턴스의 통합 인스턴스 페이지에서 ServiceNow AI Platform 선택할 수 있는 ID가 있습니다. 이러한 필터는 통합에서 Tenable.sc 데이터를 검색하는 동안 적용됩니다.

Tenable.cs

compute_severity_critical

이 필터는 기본적으로(true) 활성화되어 오픈 클라우드 호스트 취약성 통합 및 Tenable.cs 고정 클라우드 호스트 취약성 통합에서 중요 심각도 취약성을 수신합니다Tenable.cs.

compute_severity_high

이 필터는 기본적으로(true) 활성화되어 Open Cloud Host Vulnerabilities Integration 및 Tenable.cs Fixed Cloud Host Vulnerabilities Integration에서 높은 심각도 취약성을 수신합니다Tenable.cs.

compute_severity_medium

이 필터는 기본적으로 비활성입니다(False). Open Cloud Host Vulnerabilities Integration 및 Tenable.cs Fixed Cloud Host Vulnerabilities Integration에서 중간 수준의 심각도 취약성을 Tenable.cs 수신하려면 이 필터를 활성화합니다.

compute_severity_info

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 필터는 기본적으로 비활성입니다(False). 이 필터를 사용 설정하여 오픈 클라우드 호스트 취약성 통합 및 Tenable.cs 고정 클라우드 호스트 취약성 통합에서 정보 수준의 심각도 취약성을 수신합니다Tenable.cs.

compute_severity_low

이 필터는 기본적으로 비활성입니다(False). 이 필터를 사용 설정하여 오픈 클라우드 호스트 취약성 통합 및 Tenable.cs 고정 클라우드 호스트 취약성 통합에서 낮은 심각도 취약성을 수신합니다Tenable.cs.

container_severity_critical

이 필터는 기본적으로(true) 사용 설정되어 Open Cloud Container Vulnerabilities Integration 및 Tenable.cs Fixed Cloud Container Vulnerabilities Integration에서 중요 심각도 컨테이너 취약성을 수신합니다Tenable.cs.

container_severity_high

이 필터는 기본적으로(true) 활성화되어 Open Cloud Container Vulnerabilities Integration 및 Tenable.cs Fixed Cloud Container Vulnerabilities Integration에서 높은 심각도 컨테이너 취약성을 수신합니다Tenable.cs.

container_severity_medium

이 필터는 기본적으로 비활성입니다(False). Open Cloud Container Vulnerabilities Integration 및 Tenable.cs Fixed Cloud Container Vulnerabilities Integration에서 중간 수준의 심각도 컨테이너 취약성을 수신하려면 Tenable.cs 이 필터를 사용 설정합니다.

container_severity_info

이 필터는 기본적으로 비활성입니다(False). 이 필터를 사용 설정하여 컨테이너에서 정보 수준의 심각도 취약성, 오픈 클라우드 컨테이너 취약성 통합 Tenable.cs 의 Tenable.cs 취약성, 고정 클라우드 컨테이너 취약성 통합을 수신합니다.

container_severity_low

이 필터는 기본적으로 비활성입니다(False). Open Cloud Container Vulnerabilities 통합 및 Tenable.cs 고정 Cloud Container Vulnerabilities 통합에서 낮은 심각도 컨테이너 취약성을 수신하려면 Tenable.cs 이 필터를 사용 설정합니다.

asset_page_limit

이 설정은 클라우드 컨테이너 자산 통합의 Tenable.cs 결과 집합에 포함할 컨테이너 자산 기록 수를 정의합니다. 기본값은 1,000입니다. 최대 크기는 1,000입니다.

vuln_page_limit

이 설정은 오픈 클라우드 호스트 취약성 통합, 고정 클라우드 호스트 취약성 통합, Tenable.csTenable.cs 오픈 클라우드 컨테이너 취약성 통합, 고정 클라우드 컨테이너 취약성 통합의 Tenable.cs 결과 집합에 Tenable.cs 포함할 취약성 레코드 수를 정의합니다. 기본값은 1,000입니다. 최대 크기는 10,000입니다.

Tenable 취약성 통합에 대한 **REST** 메시지

ServiceNow# Tenable 취약성 통합 REST 메시지는 Tenable API를 호출하는 데 사용됩니다.

Tenable.io 자산 **REST** 메시지

Tenable.io 자산 REST 메시지는 자산 통합에 Tenable.io 대한 자산 정보를 검색합니다. REST 메시지 메서드 기록을 변경하면 자산 정보를 검색하기 위한 요청에 Tenable.io 영향을 줍니다. 자산에 대한 익스포트 작업이 다음 필터와 함께 제출됩니다.

- "is_deleted": 거짓
- "is_licensed": 참

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Tenable.io 플러그인 REST 메시지

Tenable.io 플러그인 REST 메시지는 플러그인 통합을 위한 Tenable.io 플러그인 정보를 검색합니다. REST 메시지 메서드 기록에 대한 변경 사항은 플러그인 정보를 검색하기 위한 Tenable.io 요청에 영향을 미칩니다.

Tenable.io 취약성 REST 메시지

Tenable.io 취약성 REST 메시지는 취약성 통합에서 Tenable.io 오픈 및 종결된 취약성 모두에 대한 취약성 정보를 검색합니다. REST 메시지 메서드 기록을 변경하면 취약성 정보 검색 요청에 Tenable.io 영향을 미칩니다.

Tenable.sc 쿼리 REST 메시지

Tenable.sc 쿼리 REST 메시지는 쿼리 필터가 구성된 Tenable.sc 자산 통합 및 Tenable.sc 취약성 통합에 대한 쿼리 필터 정보를 검색합니다.

Tenable.sc 플러그인 REST 메시지

Tenable.sc 플러그인 REST 메시지는 플러그인 통합에 Tenable.sc 대한 플러그인 정보를 검색합니다. REST 메시지 플러그인 메서드 기록 가져오기에 대한 변경은 플러그인 정보를 검색하기 위한 요청에 Tenable.sc 영향을 미칩니다.

매개변수 이름	값	설명
유형	활성	Tenable이 데이터를 가져오는 소스를 나타냅니다. 코드에서 사용됩니다. 변경은 권장되지 않습니다.
필드	id, 설명, cvssVector,cvssV3Vector, cvssV3TemporalVector, 시놉시스, cvssVector, baseScore,temporalScore, cvssV3Vector,cvssV3BaseScore, cvssV3TemporalScore, name, vprScore, vprContext, pluginPubDate, pluginModDate, xrefs, family, riskFactor, cpe, seeAlso, solution, exploitAvailable, exploitFrameworks, type, copyright, version, sourceFile, dependencies, requiredPorts, requiredUDPPorts, srcPort, dstPort,protocol, checkType, cvssVectorBF, stigSeverity, patchPubDate, patchModDate, vulnPubDate, modifiedTime, md5	Tenable에서 임포트한 필드 목록을 나타냅니다.

Tenable.sc 취약성 REST 메시지

Tenable.sc 취약성 REST 메시지는 통합에서 Tenable.sc 취약성 정보를 검색합니다. REST 메시지 취약성 가져오기 또는 패치된 취약성 가져오기 방법에 대한 변경 사항 또는 Tenable 취약성 통합

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

v14.0 취약성 대응 및 v2.2부터 취약성 기록 채우기 가져오기는 취약성 정보를 검색하기 위한 Tenable.sc 요청에 영향을 미칩니다.

Tenable.sc 스캔 자격 증명 REST 메시지

Tenable.sc 정책 REST 메시지

Tenable.sc 정책 POST REST 메시지는 요청된 플러그인에 대한 정책을 추가합니다. 생성된 정책이 스캔 요청에 Tenable.sc 사용됩니다.

Tenable.sc 스캔 REST 메시지

Tenable.sc 스캔 POST REST 메시지는 REST 메시지의 요청 본문에 정의된 액세스 및 권한에 따라 달라지는 스캔을 추가합니다. 스캔 요청에 대한 요청 본문의 정책, 플러그인 ID 및 IP를 사용합니다.

Tenable.sc 스캔 결과 REST 메시지

Tenable.sc 스캔 결과 GET REST 메시지는 스캔 REST 메시지를 사용하여 생성된 스캔의 스캔 상세 정보를 제공합니다. 스캔 REST 메시지의 응답에 scanResultId를 사용하고 트리거된 스캔에 대한 스캔 상세 정보를 검색합니다.

Tenable.sc 스캔 자격 증명

Tenable.sc 검사 자격 증명 REST 메시지는 에서 Tenable.sc자격 증명 정보를 검색합니다. REST 메시지 "임포트" 메서드 기록에 대한 변경은 자격 증명 정보를 검색하기 위한 Tenable.sc 요청에 영향을 미칩니다.

매개변수 이름	값	설명
필드	ID, 이름, 설명, 유형	임포트한 필드 목록을 나타냅니다. Tenable.sc
필터	사용할	통합이 다음에서 사용 가능한 자격 증명만 끌어온다는 것을 나타냅니다. Tenable.sc 매개 변수 중 하나를 변경하는 것은 권장되지 않습니다.

Tenable.cs GraphQl REST 메시지: Tenable.cs GraphQl REST 메시지는 통합을 위해 Tenable.cs 컨테이너 자산 정보, 호스트 및 컨테이너 취약성 정보를 검색합니다. REST 메시지 컨테이너 자산 가져오기, 컨테이너 취약성 가져오기, 계산 취약성 메서드 기록 가져오기에 대한 변경 사항은 자산 및 취약성 정보를 검색하기 위한 Tenable.cs 요청에 영향을 미칩니다.

Tenable 취약성 통합을 위한 데이터 변환

임포트할 데이터를 식별한 후에는 Tenable 제품에서 검색되어 인스턴스의 데이터 소스 및 변환 세트를 통해 처리됩니다.

설치하는 동안 정규화된 심각도 맵이 정규화된 심각도 매핑 모듈에 설치됩니다. 이 맵은 임포트한 Tenable 심각도 수준을 인스턴스에서 처리할 표준 심각도 수준으로 변환합니다. 심각도 맵 생성에 대한 자세한 내용은 설명서의 취약성 대응 심각도 맵 취약성 대응 생성을 참조하십시오.

Tenable.io 자산 임포트

임포트한 자산 데이터는 먼저 Tenable.io 자산 임포트[sn_vul_tenable_io_asset_import] 테이블에 로드됩니다.

Tenable.io 자산 통합 변환 맵은 임포트한 자산 정보를 변환하는 데 사용됩니다. 이 변환을 변경하면 Tenable 자산 임포트의 데이터가 처리되는 방식이 변경됩니다. 이 변환 맵에 액세스하려면 다음으로 이동하십시오. 시스템 임포트 세트 〉 변환 맵. Tenable.io ## ### 검색합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음 표에는 통합별 변환 맵 필드가 나열되어 있습니다.

자산 변환 맵 필드 **Tenable.io**

소스 필드	대상 필드	설명
u_id	source_id	Tenable은 자산에 대한 고유 ID를 제공하고 검색된 항목 기록에 매핑하며 CI 조회에 사용됩니다.
u_ipv4s	ip_address	첫 번째 IP 값을 검색된 항목 기록의 ip_address 필드에 매핑합니다.
u_mac_addresses	mac_address	첫 번째 mac_address 값을 검색된 항목 기록의 mac 주소 필드에 매핑합니다.
u_fqdns	fqdn	첫 번째 fqdn 값을 검색된 항목 기록의 fqdn 필드에 매핑합니다.
u_netbios_names	NetBIOS	첫 번째 netBIOS 값을 검색된 항목 기록의 netBIOS 필드에 매핑합니다.
u_operating_systems	os	첫 번째 OS 값을 검색된 항목 기록의 os 필드에 매핑합니다.
(Tenable 취약성 통합 v14.0 취약성 대응 및 v2.2 이전)u_last_scan_time	last_scan_date	검색된 항목 기록의 last_scan_date 필드에 매핑합니다.
u_last_authenticated_scan_date	last_auth_scan_date	검색된 항목 기록의 last_auth_scan_date 필드에 매핑합니다.
〔스크립트〕	이름	스크립트의 논리를 사용하여 호스트 이름을 매핑합니다.
u_tags		태그는 sn_sec_cmn_host_tag에 저장됩니다. 태그에서 자산으로의 매핑은 sn_sec_cmn_m2m_src_ci_tag에 저장됩니다.

변환 프로세스 중에 실행되는 세 가지 변환 스크립트가 있습니다. 다음 표에는 각 스크립트가 실행되는 시기와 용도가 나와 있습니다.

Tenable.io 자산 변환 맵 스크립트 타이밍 및 목적

스크립트가 실행될 때	목적
onStart(임포트 세트가 변환을 시작한 경우)	통합 프로세스에 대한 import_set의 값을 초기화합니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.
onBefore(임포트 세트가 변환을 완료하기 전)	호스트의 값을 업데이트하고 호스트가 존재하는지 확인합니다. 결과에 따라

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

스크립트가 실행될 때	목적
	import_set의 값을 수정합니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.
onComplete(임포트 세트가 변환을 완료한 경우)	새로 생성된 CI와 업데이트 후 무시된 CI의 값을 설정합니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.

Tenable.io 플러그인 통합

Tenable.io 플러그인 변환 맵은 Tenable.io 에서 임포트한 플러그인을 변환하는 데 사용됩니다.

주:
이 변환 맵을 변경하면 Tenable 플러그인에서 받은 데이터의 처리 방식이 변경됩니다.

이 변환 맵에 액세스하려면 다음으로 이동하십시오. 시스템 임포트 세트 〉 변환 맵. Tenable.io 플러그인 변환을 검색합니다.

tenable.io 플러그인 페이로드에는 sn_vul_tenable_io_plugin_import 테이블의 u_attributes 열에 있는 모든 필드가 포함되어 있습니다. 속성 필드는 다음 표에 나열된 대로 구문 분석되고 외부 공급업체 항목 테이블 기록에 매핑됩니다.

소스 필드	대상 필드	설명
ID	ID	소스의 ID를 매핑하고 여기에 TEN 접두사를 추가합니다. 예를 들어 수신된 ID가 12345인 경우 대상 테이블의 ID는 TEN-12345입니다.
설명	요약	플러그인의 설명을 요약 열에 매핑합니다.
〔스크립트〕	소스	임포트한 외부 공급업체 항목(TPE)의 소스는 Tenable.io 입니다.
〔스크립트〕	source_instance	이 기록을 임포트하는 Tenable 배포에 대한 참조입니다.
제품군	범주	플러그인 제품군을 범주 열에 매핑합니다.
plugin_modification_date	last_modified	plugin_modification_date 마지막으로 수정한 필드에 매핑합니다.
plugin_publication_date	date_published	plugin_publication_date 게시된 날짜에 매핑합니다.
has_patch	remediation_type	has_patch 값에서 정정 유형을 매핑합니다.
시놉시스	위협	이 취약성에 대한 위협 정보를 매핑합니다.
cvss_base__score	점수	CVSS(공통 취약성 평가 시스템) 기본 점수를 외부

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

소스 필드	대상 필드	설명
		공급업체 항목 테이블의 점수 열에 매핑합니다.
솔루션	솔루션	스캐너에서 제공한 솔루션을 외부 공급업체 항목 테이블의 솔루션 열에 매핑합니다.
exploit_available	익스플로잇	스캐너에서 제공한 exploit_available 외부 공급업체 항목 테이블의 익스플로잇 열에 매핑합니다.
vpr.score	source_risk_score	스캐너에서 제공한 VPR 점수를 외부 공급업체 항목 테이블의 source_risk_score 매핑합니다.
〔스크립트〕	source_risk_rating	점수 범위를 기준으로 VPR 점수를 표준 위험 등급에 매핑합니다. • 9–10 – 중요 • 7–9 – 높음 • 4–7 – 중간 • 0–4 - 낮음
vpr.drivers.age_of_vuln	age_of_vuln	스캐너의 취약성 기간을 외부 공급업체 항목 테이블의 age_of_vuln 열에 매핑합니다.
vpr.drivers.exploit_code_maturity	exploit_code_maturity	스캐너에서 외부 공급업체 항목 테이블의 exploit_code_maturity 악용 코드 성숙도를 매핑합니다.
vpr.drivers.product_coverage	product_coverage	스캐너의 제품 범위를 외부 공급업체 항목 테이블의 product_coverage 매핑합니다.
vpr.drivers.threat_sources_last28	threat_sources	스캐너에서 지난 28일 동안의 위협 소스를 외부 공급업체 테이블의 threat_sources 매핑합니다.
vpr.drivers.threat_intensity_last28	threat_intensity	스캐너에서 외부 공급업체 항목 테이블의 threat_intensity 지난 28일 동안의 위협 강도를 매핑합니다.
vpr.drivers.threat_recency	threat_recency	스캐너의 위협 최신성 정보를 외부 공급업체 항목 테이블의 threat_recency 매핑합니다.
vpr.drivers.cvss3_impact_score	v3_impact_subscore	cvss3 영향 점수를 외부 공급업체 항목 테이블의 v3_impact_subscore 열에 매핑합니다.
cvss_temporal_score	cvss_temporal_score	CVSS v2의 임시 점수를 매핑합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

소스 필드	대상 필드	설명
cvss_v3_temporal_score	v3_temporal_score	CVSS v3의 임시 점수를 매핑합니다.
risk_factor	source_severity	외부 공급업체 항목 테이블의 소스 심각도에 매핑합니다.
이름	이름	플러그인의 이름을 외부 공급업체 항목 테이블의 이름에 매핑합니다.
stig_severity	stig_severity	스캐너에서 제공하는 VPR 점수를 외부 공급업체 항목 테이블의 source_risk_score 매핑합니다.
plugin_type	check_type	플러그인 유형을 외부 공급업체 항목 테이블의 check_type에 매핑합니다.
unsupported_by_vendor	unsupported_by_vendor	unsupported_by_vendor 필드를 unsupported_by_vendor 열에 매핑합니다.
〔스크립트〕	exploit_attack_vector	외부 공급업체 항목 테이블의 exploit_attack_vector 열은 열의 exploit_available 및 v3_attack_vector 기준으로 채워집니다.

직접 필드 외에도 다른 정보가 외부 공급업체 항목에 관련 목록으로 추가됩니다.

소스 필드	설명
cve	CVE 관련 데이터를 참조 테이블(sn_vul_nvd_entry)에 삽입합니다. NVD 항목 테이블(sn_vul_nvd_entry)에서 동일한 CVE(Common Vulnerabilities and Exposures)가 발견되면 현재 취약성을 NVD 항목에 연결합니다. 매핑은 sn_vul_m2m_entry_cve에서 찾을 수 있습니다.
입찰	버그 트랙 목록이 참조로 추가됩니다.
see_also	URL 목록이 참조로 추가됩니다.
외부 참조	X-REF 목록이 참조로 추가됩니다.
〔스크립트〕	해당 플러그인에 대한 익스플로잇 목록과 해당 익스플로잇 프레임워크 및 플러그인에 대한 매핑을 sn_vul_m2m_framework_vul 삽입합니다.

변환 프로세스 중에 실행되는 세 가지 변환 스크립트가 있습니다. 다음 표에는 각 스크립트가 실행되는 시기와 용도가 나와 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

스크립트가 실행될 때	목적
onStart(임포트 세트가 변환을 시작한 경우)	통합 프로세스에 대한 import_set의 값을 초기화합니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.
onBefore(임포트 세트가 변환을 완료하기 전)	외부 공급업체 항목의 값을 업데이트하고 외부 공급업체 항목이 있는지 확인합니다. 결과에 따라 외부 공급업체 항목의 값을 수정합니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.
onComplete(임포트 세트가 변환을 완료한 경우)	새로 생성된 CI와 업데이트 후 무시된 CI의 값을 설정합니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.

TenableIOPluginsImportProcessor 스크립트 포함은 onBefore 변환 스크립트에서 호출됩니다. Tenable.io 플러그인 통합에서 출력을 가져와 외부 공급업체 취약성 항목으로 변환합니다 ServiceNow AI Platform . 이 스크립트 포함을 변경하면 외부 공급업체 항목 테이블의 Tenable.io 플러그인 데이터 변환이 변경될 수 있습니다.

Tenable.io 취약성 임포트

Tenable.io 취약한 항목 변환 맵은 Tenable.io 에서 임포트한 미해결 및 수정된 취약성 정보를 변환하는 데 사용됩니다.

주:
이 변환 맵을 변경하면 Tenable 취약성 임포트의 데이터가 처리되는 방식이 변경됩니다.

Tenable.io Fixed Vulnerabilities Integration과 Tenable.io Open Vulnerabilities Integration에 동일한 변환 맵이 사용됩니다. 이 변환 맵에 액세스하려면 다음으로 이동하십시오. 시스템 임포트 세트 〉 변환 맵. Tenable.io ### ## ## ## 검색합니다.

소스 필드	대상 필드	설명
u_asset.uuid	ID	UUID는 cmdb_ci 기록의 ID 필드에 매핑됩니다.
u_asset.ipv4	ip_address	ipv4 필드는 cmdb_ci 기록의 ip 주소 필드에 매핑됩니다.
u_asset.last_authenticated_results	last_auth_scan_date	인증된 마지막 검사 날짜는 cmdb_ci 기록의 마지막 인증 검사 날짜에 매핑됩니다.
u_asset.mac_addess	mac_address	Mac 주소는 cmdb_ci 기록의 호스트 mac 주소 필드에 매핑됩니다.
u_asset.netbios_name	NetBIOS	NetBIOS는 기록의 netbios 필드에 매핑cmdb_ci.
u._plugin.cvss3_base_score	v3_base_score	CVSS v3 기본 점수는 외부 공급업체 항목 기록의 v3 기본 점수에 매핑됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

소스 필드	대상 필드	설명
u._plugin.cvss3_temporal_score	v3_temporal_score	CVSS v3 임시 점수는 외부 공급업체 항목 기록의 v3 임시 점수에 매핑됩니다.
u._plugin.cvss_base_score	점수	CVSS 기본 점수는 외부 공급업체 참가 기록의 점수 필드에 매핑됩니다.
u._plugin.cvss_temporal_score	temporal_score	임시 점수는 외부 공급업체 항목 기록의 임시 점수에 매핑됩니다.
u_plugin.description	요약	설명이 외부 공급업체 항목 기록의 요약 필드에 매핑됩니다.
u_plugin.가족	범주	플러그인 제품군을 외부 공급업체 항목 기록의 범주 열에 매핑합니다.
u_plugin.modification_date	last_modified	마지막 수정 날짜는 외부 공급업체 항목 기록의 플러그인 마지막 수정 날짜에 매핑됩니다.
u_plugin.publication_date	date_published	게시 날짜는 외부 공급업체 항목 기록의 게시된 날짜 필드에 매핑됩니다.
u_plugin.risk_factor	source_severity	위험 요인은 외부 공급업체 항목 기록의 source_severity 필드에 매핑됩니다.
u_plugin.솔루션	솔루션	솔루션은 외부 공급업체 항목 기록의 솔루션 필드에 매핑됩니다.
u_plugin.시놉시스	위협	시놉시스는 외부 공급업체 항목 기록의 위협 필드에 매핑됩니다.
u_severity_id	우선순위	우선순위는 페이로드에서 심각도 ID에 매핑됩니다. 기본값은 5입니다.
u_plugin.exploit_available	익스플로잇	스캐너에서 제공하는 exploit_available 외부 공급업체 항목 테이블의 익스플로잇 열에 매핑합니다.
vpr.score	source_risk_score	스캐너에서 제공하는 VPR 점수를 외부 공급업체 항목 테이블의 source_risk_score 매핑합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

소스 필드	대상 필드	설명
〔스크립트〕	source_risk_rating	점수 범위를 기준으로 VPR 점수를 표준 위험 등급에 매핑합니다. • 9–10 – 중요 • 7–9 – 높음 • 4–7 – 중간 • 0–4 - 낮음
u_plugin.vpr.drivers.age_of_vuln	age_of_vuln	스캐너의 취약성 기간을 외부 공급업체 항목 테이블의 age_of_vuln 매핑합니다.
u_plugin.vpr.drivers.exploit_code_maturity	exploit_code_maturity	스캐너에서 외부 공급업체 항목 테이블의 exploit_code_maturity 악용 코드 성숙도를 매핑합니다.
u_plugin.vpr.drivers.product_coverage	product_coverage	스캐너의 제품 범위를 외부 공급업체 항목 테이블의 product_coverage 매핑합니다.
u_plugin.vpr.drivers.threat_sources_last28	threat_sources	스캐너에서 지난 28일 동안의 위협 소스를 외부 공급업체 항목 테이블의 threat_sources 매핑합니다.
u_plugin.vpr.drivers.threat_intensity_last28	threat_intensity	스캐너에서 외부 공급업체 항목 테이블의 threat_intensity 지난 28일 동안의 위협 강도를 매핑합니다.
u_plugin.vpr.drivers.threat_recency	threat_recency	스캐너의 위협 최신성 정보를 외부 공급업체 항목 테이블의 threat_recency 매핑합니다.
u_plugin.vpr.drivers.cvss3_impact_score	v3_impact_subscore	CVSS3 v3 영향 점수를 외부 공급업체 항목 테이블의 v3_impact_subscore 열에 매핑합니다.
u_plugin.유형	check_type	플러그인 유형을 외부 공급업체 항목 테이블의 check_type에 매핑합니다.
u_plugin.unsupported_by_vendor	unsupported_by_vendor	플러그인의 unsupported_by_vendor 필드를 unsupported_by_vendor 열에 매핑합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

소스 필드	대상 필드	설명
〔스크립트〕	exploit_attack_vector	외부 공급업체 항목 테이블의 exploit_attack_vector 열은 열의 exploit_available 및 v3_attack_vector 기준으로 채워집니다.
u_plugin.family_id	Family_id	플러그인 제품군 ID를 외부 공급업체 항목 테이블의 family_id 열에 매핑합니다.
포트	포트	포트는 취약한 항목 기록의 포트 필드에 매핑됩니다.
프로토콜	프로토콜	프로토콜은 취약한 항목 레코드의 프로토콜 필드에 매핑됩니다.
u_first_found	first_found	첫 번째 발견은 취약한 항목 기록의 처음 발견된 필드에 매핑됩니다.
u_last_found	last_found	마지막 발견은 취약한 항목 기록의 마지막 발견 필드에 매핑됩니다.
u_state	상태	상태는 취약한 항목 레코드의 상태 필드에 매핑됩니다.
〔스크립트〕	소스	통합의 소스가 채워집니다. 이 통합에서 생성된 취약한 항목이 소스로 Tenable.io.
〔스크립트〕	integration_instance	integration_instance은 취약한 항목을 임포트한 인스턴스의 이름입니다.
u_plugin.name	이름	플러그인의 이름을 외부 공급업체 항목 테이블의 이름에 매핑합니다.
u_plugin.stig_severity	stig_severity	플러그인의 stig 심각도를 외부 공급업체 항목 테이블의 stig 심각도 열에 매핑합니다.

직접 필드 외에도 다른 정보가 외부 공급업체 항목에 관련 목록으로 추가됩니다.

소스 필드	설명
cve	CVE 관련 데이터를 참조 테이블(sn_vul_nvd_entry)에 삽입합니다. NVD 항목 테이블(sn_vul_nvd_entry)에서 동일한 CVE가 발견되면 현재 취약성을 NVD 항목에 연결합니다. 매핑은 sn_vul_m2m_entry_cve에서 찾을 수 있습니다.
입찰	버그 트랙 목록이 참조로 추가됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

소스 필드	설명
see_also	URL 목록이 참조로 추가됩니다.
외부 참조	X-REF 목록이 참조로 추가됩니다.
〔스크립트〕	해당 플러그인에 대한 익스플로잇 목록 및 해당 익스플로잇 프레임워크에 대한 매핑 sn_vul_m2m_framework_vul 삽입합니다.

변환 프로세스 중에 실행되는 세 가지 변환 스크립트가 있습니다. 다음 표에는 각 스크립트가 실행되는 시기와 용도가 나와 있습니다.

스크립트가 실행될 때	목적
onStart(임포트 세트가 변환을 시작한 경우)	임포트 세트를 사용하여 Tenable.io 에서 데이터를 임포트하고 각 기록을 CMDB CI 테이블, 취약한 항목 테이블 및 외부 공급업체 취약성 테이블로 로드하는 Trigger Tenable IO 취약성 프로세서입니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.
onBefore(임포트 세트가 변환을 완료하기 전)	외부 공급업체 항목 및 탐지가 있는지 확인합니다. 그렇지 않은 경우 이러한 기록은 해당 테이블에 생성됩니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.
onComplete(임포트 세트가 변환을 완료한 경우)	Tenable.io 에서 임포트한 CI, VIT 및 탐지 수를 업데이트합니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.

Tenable.sc 자산 임포트

Tenable.sc 에서 임포트한 자산 데이터는 먼저 Tenable.sc 자산 임포트 테이블(sn_vul_tenable_sc_asset_import)에 로드됩니다. Tenable.sc 자산 통합 변환 맵은 임포트한 자산 정보를 변환하는 데 사용됩니다. 이 변환을 변경하면 Tenable 자산 임포트의 데이터가 처리되는 방식이 변경됩니다. 이 변환 맵에 액세스하려면 다음으로 이동하십시오. 시스템 임포트 세트 〉 변환 맵. Tenable.sc ## ### 검색합니다.

소스 필드	대상 필드	설명
u_uuid	ID	UUID는 Tenable API에서 채워지지 않으므로 "u_uniqueness" 속성은 자산에 대한 고유 UUID 필드를 만들고 cmdb_ci 기록에 매핑하는 데 사용됩니다.
u_ip	ip_address	API의 IP 필드를 cmdb_ci 기록의 ip_address 필드로 매핑합니다.
u_macaddress	mac_address	API의 MAC 주소 필드를 cmdb_ci 기록의 주소 필드에 매핑합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

소스 필드	대상 필드	설명
u_dnsname	fqdn	API의 dnsname 필드를 cmdb_ci 기록의 fqdn 필드에 매핑합니다.
u_netbiosname	NetBIOS	API의 netbios 필드를 cmdb_ci 기록의 netbios 필드로 매핑합니다.
u_oscpe	os	OS 정보는 페이로드의 oscpe 속성에서 추출되어 cmdb_ci 기록의 os 필드에 매핑됩니다.
u_lastauthrun	last_auth_scan_date	API의 lastauthrun 필드를 검색된 항목 기록의 last_auth_scan_date 필드에 매핑합니다.
u_lastauthrun 및 u_lastunauthrun	last_scan_date	lastauthrun은 Tenable API 또는 lastunauthrun에서 추출됩니다. 검색된 항목 기록의 last_scan_date 필드는 페이로드에 나타나는 값을 기준으로 채워집니다.

변환 프로세스 중에 실행되는 세 가지 변환 스크립트가 있습니다. 다음 표에는 각 스크립트가 실행되는 시기와 용도가 나와 있습니다.

스크립트가 실행될 때	목적
onStart(임포트 세트가 변환을 시작한 경우)	통합 프로세스에 대한 import_set의 값을 초기화합니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.
onBefore(임포트 세트가 변환을 완료하기 전)	호스트의 값을 업데이트하고 호스트가 존재하는지 확인합니다. 결과에 따라 import_set의 값을 수정합니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.
onComplete(임포트 세트가 변환을 완료한 경우)	새로 생성된 CI와 업데이트 후 무시된 CI의 값을 설정합니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.

Tenable.sc 플러그인 임포트

Tenable.sc 에서 임포트한 플러그인 데이터는 먼저 Tenable.sc 플러그인 임포트 테이블(sn_vul_tenable_sc_plugin_import)에 로드됩니다. Tenable.sc 플러그인 변환 맵은 임포트한 플러그인 정보를 변환하는 데 사용됩니다. 이 변환을 변경하면 Tenable 플러그인 임포트의 데이터가 처리되는 방식이 변경됩니다. 이 변환 맵에 액세스하려면 다음으로 이동하십시오. 시스템 임포트 세트 〉 변환 맵. #### ## # Tenable.sc 검색합니다.

소스 필드	대상 필드	설명
u_id	ID	소스에서 ID를 매핑하고 TEN 접두사를 추가합니다. 예를 들어 수신된 ID가 12345인

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

소스 필드	대상 필드	설명
		경우 대상 테이블의 ID는 TEN-12345입니다.
u_description	요약	플러그인의 설명을 요약 열에 매핑합니다.
〔스크립트〕	소스	이 통합에서 임포트한 TPE가 소스로 Tenable.sc.
〔스크립트〕	source_instance	이 기록을 임포트하는 Tenable 배포에 대한 참조입니다.
u_family	범주	플러그인의 패밀리 객체에 있는 이름 필드를 범주 열에 매핑합니다.
u_plugin_modification_date	last_modified	plugin_modification_date 마지막으로 수정한 필드에 매핑합니다.
u_plugin_publication_date	date_published	plugin_publication_date 게시된 날짜에 매핑합니다.
u_has_patch	Remediation_type	has_patch 값에서 정정 유형을 매핑합니다.
u_synopsis	위협	이 취약성에 대한 위협 정보를 매핑합니다.
u_cvss_base_score	점수	CVSS 기본 점수를 외부 공급업체 항목 테이블의 점수 열에 매핑합니다.
u_solution	솔루션	스캐너에서 제공하는 솔루션을 외부 공급업체 항목 테이블의 솔루션 열에 매핑합니다.
u_cvss_temporal_score	cvss_temporal_score	CVSS v2의 임시 점수를 매핑합니다.
u_cvss_v3_temporal_score	v3_temporal_score	CVSS v3의 임시 점수를 매핑합니다.
u_risk_factor	소스 심각도	외부 공급업체 항목 테이블의 소스 심각도에 매핑합니다.
u_cvss_v3_base_score	v3_base_score	외부 공급업체 항목 테이블에 CVSS 기본 점수를 매핑합니다.
u_exploit_available	익스플로잇	스캐너에서 제공하는 exploitAvailable을 외부 공급업체 항목 테이블의 익스플로잇 열에 매핑합니다.
u_vpr_score	source_risk_score	스캐너의 VPR 점수를 외부 공급업체 항목 테이블의 소스 위험 점수에 매핑합니다.
〔스크립트〕	source_risk_rating	점수 범위를 기준으로 VPR 점수를 표준 위험 등급에 매핑합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

소스 필드	대상 필드	설명
		• 9–10 – 중요 • 7–9 – 높음 • 4–7 – 중간 • 0–4 - 낮음
u_vpr_context(id=age_of_vuln)	age_of_vuln	취약성의 기간을 스캐너의 외부 공급업체 항목 테이블에 age_of_vuln 매핑합니다.
u_vpr_context(id=exploit_code_maturity)	exploit_code_maturity	스캐너에서 외부 공급업체 항목 테이블의 exploit_code_maturity 악용 코드 성숙도를 매핑합니다.
u_vpr_context(id=product_coverage)	product_coverage	스캐너의 제품 범위를 외부 공급업체 항목 테이블의 product_coverage 매핑합니다.
u_vpr_context(id="threat_sources_last_28")	threat_sources	지난 28일 동안의 위협 소스를 스캐너에서 외부 공급업체 테이블의 threat_sources 매핑합니다.
u_vpr_context(id="threat_intensity_last_28")	threat_intensity	스캐너에서 외부 공급업체 항목 테이블의 threat_intensity 지난 28일 동안의 위협 강도를 매핑합니다.
u_vpr_context(id="threat_recency")	threat_recency	스캐너의 위협 최신성 정보를 타사 항목 테이블의 threat_recency 매핑합니다.
u_vpr_context(id=cvssV3_impactScore)	v3_impact_subscore	스캐너의 CVSS v3 영향 점수를 외부 공급업체 항목 테이블의 v3_impact_subscore 매핑합니다.
u_name	이름	플러그인 이름을 외부 공급업체 항목 테이블의 이름 열에 매핑합니다.
u_stig_severity	stig_severity	플러그인의 stig_severity 필드를 외부 공급업체 항목 테이블의 stig_severity 매핑합니다.
u_check_type	check_type	검사 유형을 외부 공급업체 항목 테이블의 check_type에 매핑합니다.
u_family.id	family_id	플러그인 family_id 외부 공급업체 항목 테이블의 family_id에 매핑합니다.
〔스크립트〕	exploit_attack_vector	외부 공급업체 항목 테이블의 exploit_attack_vector 열은 열의 exploit_available 및 v3_attack_vector 기준으로 채워집니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

직접 필드 외에도 다른 정보가 외부 공급업체 항목에 관련 목록으로 추가됩니다.

소스 필드	설명
u_cpe	CPE 목록이 참조로 추가됩니다.
u_see_also	URL 목록이 참조로 추가됩니다.
u_exploit_frameworks	해당 플러그인에 대한 익스플로잇 목록과 해당 익스플로잇 프레임워크 및 플러그인에 대한 매핑을 sn_vul_m2m_framework_vul 삽입합니다.

변환 프로세스 중에 실행되는 세 가지 변환 스크립트가 있습니다. 다음 표에는 각 스크립트가 실행되는 시기와 용도가 나와 있습니다.

스크립트가 실행될 때	목적
onStart(임포트 세트가 변환을 시작한 경우)	이 변환은 통합 프로세스에 대한 import_set의 값을 초기화하는 데 사용됩니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.
onBefore(임포트 세트가 변환을 완료하기 전)	외부 공급업체 항목의 값을 업데이트하고 외부 공급업체 항목이 있는지 확인하는 데 사용되는 기능입니다. 결과에 따라 외부 공급업체 항목의 값을 수정합니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.
onComplete(임포트 세트가 변환을 완료한 경우)	이 변환은 만들어지고 무시된 플러그인의 값을 설정하는 데 사용됩니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.

TenableSCPluginsImportProcessor 스크립트 포함은 onBefore 변환 스크립트에서 호출됩니다. Tenable.sc 플러그인 통합에서 출력을 가져와 외부 공급업체 취약성 항목으로 변환합니다 ServiceNow . 이 스크립트 포함을 변경하면 외부 공급업체 항목 테이블의 Tenable.sc 플러그인 데이터 변환이 변경될 수 있습니다.

Tenable.sc 취약성 임포트

Tenable.sc 미해결 취약성 변환 맵은 Tenable.sc 미해결 취약성 통합에서 임포트한 데이터를 변환하는 데 사용되며, Tenable.sc 및 수정된 취약성 변환 맵은 Tenable.sc 해결된 취약성 통합에서 임포트된 데이터를 변환하는 데 사용됩니다.

주:
이러한 변환 맵을 변경하면 고정/미해결 Tenable 취약성 임포트의 데이터가 처리되는 방식이 변경됩니다.

Tenable.sc 미해결 및 수정된 취약성 변환 맵에 접근하려면 다음으로 이동하십시오. **Tenable** 취약성 통합 〉 관리 〉 통합 인스턴스 〉 **Tenable.sc** 고정/미해결 취약성 통합 〉 데이터 소스 〉 **Tenable.sc** 미해결/수정된 취약성 〉 변형.

소스 필드	대상 필드	설명
u_pluginID	ID	플러그인의 식별자로 사용됩니다. 이 필드는

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

소스 필드	대상 필드	설명
		외부 공급업체 항목 기록의 플러그인 ID에 매핑됩니다.
u_riskfactor	source_severity	이 필드는 외부 공급업체 항목 기록의 source_severity에 매핑됩니다.
u_severity	우선순위	우선순위 필드는 심각도와 매핑됩니다. 기본값은 5입니다.
u_hasbeenmitigated	상태	완화됨 취약성 기록의 상태 필드에 매핑됩니다. 수정된 취약성 통합의 경우 모든 VI가 "종결" 상태입니다.
u_ip	ip_address	IP 주소는 cmdb_ci 테이블의 호스트 IP 필드에 매핑됩니다.
u_port	포트	포트는 취약한 항목 기록의 포트 필드에 매핑됩니다.
u_protocol	프로토콜	프로토콜은 취약한 항목 기록의 포트 필드에 매핑됩니다.
u_firstSeen	first_found	첫 번째로 발견된 값은 VI 기록의 첫 번째 발견 필드에 매핑됩니다.
u_lastSeen	last_found	마지막으로 발견된 값은 VI 기록의 마지막으로 발견된 필드에 매핑됩니다.
u_exploitAvailable	익스플로잇	ExploitAvailable은 외부 공급업체 항목 기록의 익스플로잇 필드에 매핑됩니다.
u_synopsis	위협	시놉시스는 외부 공급업체 항목 기록의 위협 필드에 매핑됩니다.
u_description	요약	설명이 외부 공급업체 항목 기록의 요약 필드에 매핑됩니다.
u_solution	솔루션	솔루션은 외부 공급업체 항목 기록의 솔루션 필드에 매핑됩니다.
u_basescore	점수	BaseScore는 외부 공급업체 참가 기록의 점수 필드에 매핑됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

소스 필드	대상 필드	설명
u_temporalScore	temporal_score	임시 점수는 외부 공급업체 항목 기록의 임시 점수에 매핑됩니다.
u_cvssv3basescore	v3_base_score	Cvssv3basescore는 외부 공급업체 항목 레코드의 v3 기본 점수에 매핑됩니다.
u_cvsstemporalscore	v3_temporal_score	Cvssv3temporal 점수는 외부 공급업체 항목 레코드의 v3 temporal 점수에 매핑됩니다.
u_pluginpubdate	date_published	플러그인 게시 날짜는 외부 공급업체 항목 기록의 플러그인 게시 날짜에 매핑됩니다.
u_pluginmoddate	last_modified	마지막 수정 날짜는 외부 공급업체 항목 기록의 플러그인 마지막 수정 날짜에 매핑됩니다.
u_dnsname	fqdn	DnsName은 cmdb_ci 레코드의 FQDN 필드에 매핑됩니다.
u_macaddress	mac_address	MacAddress는 cmdb_ci 기록의 mac_address 필드에 매핑됩니다.
u_netbiosName	NetBIOS	NetbiosName은 cmdb_ci 레코드의 NETBIOS 필드에 매핑됩니다.
u_ip	ip	IP는 cmdb_ci 기록의 IP 필드에 매핑됩니다.
hostUniqueness	uuid	호스트 고유성은 필드에 매핑되지 않지만 호스트의 UUID를 결정하는 데 사용됩니다.
u_family	범주	플러그인의 제품군 객체에 있는 이름 필드를 외부 공급업체 항목 기록의 범주 열에 매핑합니다.
u_plugintext	증명	플러그인 텍스트는 TPE 기록의 증명에 매핑됩니다.
〔스크립트〕	소스	통합의 소스가 채워집니다. 이 통합에서 생성된 취약한 항목이 소스로 Tenable.sc.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

소스 필드	대상 필드	설명
〔스크립트}	integration_instance	integration_instance은 취약한 항목을 임포트한 인스턴스의 이름입니다.
u_vpr_score	source_risk_score	스캐너의 VPR 점수를 외부 공급업체 항목 테이블의 소스 위험 점수에 매핑합니다.
〔스크립트〕	source_risk_rating	점수 범위를 기준으로 VPR 점수를 표준 위험 등급에 매핑합니다. • 9 – 10 – 중요 • 7 – 9 – 높음 • 4–7 – 중간 • 0–4 - 낮음
u_vpr_context〔id=age_of_vuln〕	age_of_vuln	취약성의 기간을 스캐너의 외부 공급업체 항목 테이블에 age_of_vuln 매핑합니다.
u_vpr_context〔id=exploit_code_maturity〕	exploit_code_maturity	스캐너에서 외부 공급업체 항목 테이블의 exploit_code_maturity 악용 코드 성숙도를 매핑합니다.
u_vpr_context〔id=product_coverage〕	product_coverage	스캐너의 제품 범위를 외부 공급업체 항목 테이블의 product_coverage 매핑합니다.
u_vpr_context〔id="threat_sources_last_28〕	threat_sources	스캐너에서 지난 28일 동안의 위협 소스를 외부 공급업체 테이블의 threat_sources 매핑합니다.
u_vpr_context〔id="threat_intensity_last_28〕	threat_intensity	스캐너에서 외부 공급업체 항목 테이블의 threat_intensity 지난 28일 동안의 위협 강도를 매핑합니다.
u_vpr_context〔id="threat_recency"〕	threat_recency	스캐너의 위협 최신성 정보를 타사 항목 테이블의 threat_recency 매핑합니다.
u_vpr_context〔id=cvssV3_impactScore〕	v3_impact_subscore	스캐너의 CVSS v3 영향 점수를 외부 공급업체 항목 테이블의

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

소스 필드	대상 필드	설명
		v3_impact_subscore 매핑합니다.
u_pluginname	이름	플러그인 이름을 외부 공급업체 항목 테이블의 이름 열에 매핑합니다.
u_stigseverity	stig_severity	플러그인의 stig_severity 필드를 외부 공급업체 항목 테이블의 stig_severity 매핑합니다.
u_checktype	check_type	검사 유형을 외부 공급업체 항목 테이블의 check_type에 매핑합니다.
u_family.id	family_id	플러그인 family.id 외부 공급업체 항목 테이블의 family_id에 매핑합니다.
〔스크립트〕	exploit_attack_vector	third_party_entry 테이블의 exploit_attack_vector 열은 열의 exploit_available 및 v3_attack_vector 따라 채워집니다.

소스 필드	설명
u_cve	CVE 관련 데이터를 참조 테이블 (sn_vul_nvd_entry)에 삽입합니다. NVD 항목 테이블(sn_vul_nvd_entry)에서 동일한 CVE가 발견되면 현재 취약성을 NVD 항목에 연결합니다. 매핑은 sn_vul_m2m_entry_cve에서 찾을 수 있습니다.
u_bid	버그 트랙 목록이 참조로 추가됩니다.
u_cpe	CPE 목록이 참조로 추가됩니다.
u_seealso	URL 목록이 참조로 추가됩니다.
u_xrefs	X-REF의 목록이 참조로 추가됩니다.
u_exploitframeworks	해당 플러그인에 대한 익스플로잇 목록 및 해당 익스플로잇 프레임워크에 대한 매핑 sn_vul_m2m_framework_vul 삽입합니다.

변환 프로세스 중에 실행되는 세 가지 변환 스크립트가 있습니다. 다음 표에는 각 스크립트가 실행되는 시기와 용도가 나와 있습니다.

스크립트가 실행될 때	목적
onStart(임포트 세트가 변환을 시작한 경우)	이 변환은 통합 프로세스에 대한 import_set의 값을 초기화하는 데 사용됩니다. 이 스크립트는

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

스크립트가 실행될 때	목적
	내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.
onBefore(임포트 세트가 변환을 완료하기 전)	취약성의 값을 업데이트하고 취약성이 존재하는지 확인하는 데 사용되는 기능입니다. 결과에 따라 취약한 항목 테이블의 값을 수정합니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.
onComplete(임포트 세트가 변환을 완료한 경우)	이 변환은 생성된 새 VI의 값과 업데이트 및 무시된 VI의 값을 설정하는 데 사용됩니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.

Tenable.cs 컨테이너 자산 임포트

임포트한 자산 데이터는 먼저 컨테이너 자산 임포트 [sn_vul_tenable_cs_container_asset_import] 테이블에 로드됩니다 Tenable.cs .

컨테이너 자산 변환 맵은 Tenable.cs 임포트한 자산 정보를 변환하는 데 사용됩니다. 이 변환을 변경하면 컨테이너 자산 임포트의 Tenable.cs 데이터가 처리되는 방식이 변경됩니다. 이 변환 맵에 액세스하려면 시스템 임포트 세트 > 변환 맵으로 이동합니다. Tenable.cs 컨테이너 자산 변환을 검색합니다.

다음 테이블에는 통합별 변환 맵 필드가 나열되어 있습니다.

Tenable.cs 컨테이너 자산 변환 맵 필드

소스 필드	대상 필드	설명
u_digest	Image_id	Tenable은 컨테이너 자산에 대한 고유 다이제스트를 제공하고 검색된 컨테이너 이미지 및 Docker 이미지 기록에 매핑되며 CI 조회에 사용됩니다.
u_digest	Image_digest	Tenable은 컨테이너 자산에 대한 고유 다이제스트를 제공하고 검색된 컨테이너 이미지 및 Docker 이미지 기록에 매핑되며 CI 조회에 사용됩니다.
u_name	이름	Docker 이미지 기록의 이름 필드에 매핑합니다.
u_repositoryuri	이름	컨테이너 리포지토리 기록에 매핑
u_repositoryuri	리포지토리	검색된 컨테이너 이미지 기록에 매핑합니다.
u_virtualmachines	host_list	검색된 컨테이너 이미지 기록에 매핑합니다.
u_labels	Image_labels	첫 번째 OS 값을 검색된 항목 기록의 os 필드에 매핑합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Tenable.cs 컨테이너 자산 변환 맵 필드

소스 필드	대상 필드	설명
u_clusters	image_cluster	검색된 컨테이너 이미지 기록에 매핑합니다.
u_imagetags	태그	검색된 컨테이너 이미지 기록에 매핑합니다.
u_cloudprovider	cloud_providers	검색된 컨테이너 이미지 기록에 매핑합니다.
u_accountid	cloud_account_ids	검색된 컨테이너 이미지 기록에 매핑합니다.
u_region	cloud_regions	검색된 컨테이너 이미지 기록에 매핑합니다.
u_operatingsystem	os	검색된 컨테이너 이미지 기록에 매핑합니다.
u_scantime	last_scan_date	검색된 컨테이너 이미지 기록에 매핑합니다.

변환 프로세스 중에 실행되는 세 가지 변환 스크립트가 있습니다. 다음 표에는 각 스크립트가 실행되는 시기와 용도가 나와 있습니다.

Tenable.cs 컨테이너 자산 변환 맵 스크립트 타이밍 및 목적

스크립트가 실행될 때	목적
onStart(임포트 세트가 변환을 시작한 경우)	이 변환은 통합 프로세스에 대한 import_set의 값을 초기화하는 데 사용됩니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.
onBefore(임포트 세트가 변환을 완료하기 전)	호스트의 값을 업데이트하고 호스트가 존재하는지 확인하는 데 사용되는 함수입니다. 결과에 따라 import_set의 값을 수정합니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.
onComplete(임포트 세트가 변환을 완료한 경우)	이 변환은 새로 생성된 CI와 업데이트 후 무시된 CI의 값을 설정하는 데 사용됩니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.

Tenable.cs 컨테이너 취약성 임포트

임포트된 컨테이너 취약성 데이터는 먼저 컨테이너 취약성 임포트 [sn_vul_tenable_cs_container_vuln_import] 테이블에 로드됩니다 Tenable.cs .

컨테이너 취약성 변환 맵은 Tenable.cs 임포트한 컨테이너 취약성 정보를 변환하는 데 사용됩니다. 이 변환을 변경하면 컨테이너 취약성 임포트의 Tenable.cs 데이터가 처리되는 방식이 변경됩니다. 이 변환 맵에 액세스하려면 다음으로 이동하십시오. 시스템 임포트 세트 〉 변환 맵. Tenable.cs 컨테이너 취약성 변환을 검색합니다.

다음 테이블에는 통합별 변환 맵 필드가 나열되어 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Tenable.cs 컨테이너 취약성 변환 맵 필드

소스 필드	대상 필드	설명
〔스크립트〕	Image_id	다이제스트는 API의 Resource.Id 필드에서 추출되어 검색된 컨테이너 이미지 및 Docker 이미지 기록의 image_id 필드에 매핑됩니다.
〔스크립트〕	Image_digest	다이제스트는 API의 Resource.Id 필드에서 추출되어 검색된 컨테이너 이미지 및 Docker 이미지 기록의 image_digest 필드에 매핑됩니다.
〔스크립트〕	이름	리포지토리 정보는 이름 필드에서 추출되어 Docker 이미지 및 컨테이너 리포지토리 기록에 매핑됩니다.
〔스크립트〕	리포지토리	리포지토리 정보는 이름 필드에서 추출되어 컨테이너 이미지 검색 기록에 매핑됩니다.
u_resource. 레이블	Image_labels	검색된 컨테이너 이미지 기록에 매핑합니다.
u_resource. 클라우드 제공자	cloud_providers	검색된 컨테이너 이미지 기록에 매핑합니다.
u_resource. AccountId	cloud_account_ids	검색된 컨테이너 이미지 기록에 매핑합니다.
u_resource. 부위	cloud_regions	검색된 컨테이너 이미지 기록에 매핑합니다.
u_vulnerability. ID	ID	소스에서 ID를 매핑하고 TEN- 접두사를 추가합니다. 예를 들어 수신된 ID가 12345인 경우 외부 공급업체 항목 테이블의 ID는 TEN-12345입니다.
u_vulnerability. 설명 ID	요약 ID	외부 공급업체 항목 기록에 매핑합니다. 또는 CVE 기록.
u_vulnerability. 심각도	v4_base_severity	외부 공급업체 항목 기록에 매핑합니다.
u_vulnerability. Vpr점수	source_risk_score	외부 공급업체 항목 기록에 매핑합니다.
u_vulnerability. VprSeverity	source_severity	외부 공급업체 항목 기록에 매핑합니다.
u_vulnerability. 공격 벡터	v4_attack_vector	외부 공급업체 항목 기록에 매핑합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Tenable.cs 컨테이너 취약성 변환 맵 필드

소스 필드	대상 필드	설명
u_vulnerability. 악용 성숙도	v4_exploit_maturity	외부 공급업체 항목 기록에 매핑합니다.
〔스크립트〕	소스	수입 TPE의 출처는 Tenable.cs입니다.
u_vulnerability. 아이디	이름	취약성 참조 기록에 매핑
u_vulnerability. 링크	URL	취약성 참조 기록에 매핑
	취약성	취약성 참조 기록의 TPE 또는 CVE 참조
u_software. 이름	이름	컨테이너 이미지 패키지 기록에 매핑
u_software. 버전	버전	컨테이너 이미지 패키지 기록에 매핑
u_software. 형	package_type	컨테이너 이미지 패키지 기록에 매핑
u_softwarepaths	path	컨테이너 이미지 패키지 기록에 매핑
u_resolved	상태	컨테이너 이미지 찾기 기록에 매핑
u_firstscantime	first_found	컨테이너 이미지 찾기 기록에 매핑
u_resource. 스캔 시간	last_found	컨테이너 이미지 찾기 기록에 매핑
u_vulnerability. 묘사	증명	컨테이너 이미지 찾기 기록에 매핑
u_resolved	상태	컨테이너 취약한 항목 기록에 매핑합니다.
u_firstscantime	first_found	컨테이너 취약한 항목 기록에 매핑합니다.
u_resource. 스캔 시간	last_found	컨테이너 취약한 항목 기록에 매핑합니다.
〔스크립트〕	소스	컨테이너 취약한 항목 기록의 소스는 입니다 Tenable.cs.

변환 프로세스 중에 실행되는 세 가지 변환 스크립트가 있습니다. 다음 표에는 각 스크립트가 실행되는 시기와 용도가 나와 있습니다.

Tenable.cs 컨테이너 취약성 변환 맵 스크립트 타이밍 및 목적

스크립트가 실행될 때	목적
onStart(임포트 세트가 변환을 시작한 경우)	임포트 세트를 사용하여 데이터를 Tenable.cs 임포트하고 각 기록을 CMDB CI 테이블, 취약한 항목 테이블, 외부 공급업체 취약성 항목 테이블, 취약성 참조 테이블, 컨테이너 이미지 패키지,

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Tenable.cs 컨테이너 취약성 변환 맵 스크립트 타이밍 및 목적

스크립트가 실행될 때	목적
	컨테이너 이미지 찾기 및 컨테이너 취약한 항목에 로드하는 TenableCS 컨테이너 취약성 프로세서를 트리거합니다. 수정하거나 삭제하는 것은 권장되지 않습니다.
onBefore(임포트 세트가 변환을 완료하기 전)	외부 공급업체 항목 및 이미지 결과가 있는지 확인합니다. 그렇지 않은 경우 이러한 기록은 해당 테이블에 생성됩니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.
onComplete(임포트 세트가 변환을 완료한 경우)	에서 Tenable.cs임포트한 CI, VIT 및 결과 수를 업데이트합니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.

Tenable.cs 취약성 임포트 계산

임포트된 호스트 취약성 데이터는 먼저 취약성 계산 [sn_vul_tenable_cs_compute_vuln_import] 테이블에 로드됩니다 Tenable.cs .

Compute Vuln 변환 맵은 Tenable.cs 임포트한 호스트 취약성 정보를 변환하는 데 사용됩니다. 이 변환을 변경하면 계산 취약성 임포트의 Tenable.cs 데이터가 처리되는 방식이 변경됩니다. 이 변환 맵에 액세스하려면 다음으로 이동하십시오. 시스템 임포트 세트 〉 시스템 임포트 세트. Tenable.cs 계산 취약성 변환을 검색합니다.

다음 표에는 통합별 변환 맵 필드가 나열되어 있습니다.

Tenable.cs 컨테이너 취약성 변환 맵 필드

소스 필드	대상 필드	설명
u_resource. 아이디	object_id	CMDB CI 기록에 매핑됩니다.
u_resource. 이름	이름	CMDB CI 기록에 매핑됩니다.
	asset_category	클라우드는 검색된 항목 기록에서 자산 범주로 매핑됩니다.
U_resource. 클라우드 제공자	cloud_service_provider	검색된 항목 기록에 매핑
u_resource. 부위	cloud_region	검색된 항목 기록에 매핑
u_resource. 계정 ID	cloud_account	검색된 항목 기록에 매핑
u_resource. CloudProvider	cloud_resource_type	검색된 항목 기록에 매핑
u_resource. 아이디	resource_id	검색된 항목 기록에 매핑
u_resource. 이름	resource_name	검색된 항목 기록에 매핑
u_vulnerability. 아이디	ID	소스에서 ID를 매핑하고 TEN- 접두사를 추가합니다. 예를 들어 수신된 ID가 12345인 경우 외부 공급업체 항목 테이블의 ID는 TEN-12345입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Tenable.cs 컨테이너 취약성 변환 맵 필드

소스 필드	대상 필드	설명
		ID를 CVE에도 매핑합니다.
u_vulnerability. 설명	요약	외부 공급업체 항목 기록에 매핑합니다.
u_vulnerability. 심각도	v4_base_severity	외부 공급업체 항목 기록에 매핑합니다.
u_vulnerability. Vpr점수	source_risk_score	외부 공급업체 항목 기록에 매핑합니다.
u_vulnerability. VprSeverity	source_severity	외부 공급업체 항목 기록에 매핑합니다.
u_vulnerability. 공격 벡터	v4_attack_vector	외부 공급업체 항목 기록에 매핑합니다.
u_vulnerability. 악용 성숙도	v4_exploit_maturity	외부 공급업체 항목 기록에 매핑합니다.
〔스크립트〕	소스	수입된 TPE의 출처는 Tenable.cs입니다.
u_vulnerability. 아이디	이름	취약성 참조 기록에 매핑
u_vulnerability. 링크	URL	취약성 참조 기록에 매핑
	취약성	취약성 참조 기록의 TPE 또는 CVE 참조
u_resolved	상태	취약한 항목 탐지 기록에 매핑합니다.
u_firstscantime	first_found	취약한 항목 탐지 기록에 매핑합니다.
u_resource. 스캔 시간	last_found	취약한 항목 탐지 기록에 매핑합니다.
u_softwarepaths	증명	취약한 항목 탐지 기록에 매핑합니다.
u_softwareresolutionversions	solution_summary	취약한 항목 탐지 기록에 매핑합니다.
u_resolved	상태	취약한 항목 기록에 매핑
u_firstscantime	first_found	취약한 항목 기록에 매핑
u_resource. 스캔 시간	last_found	취약한 항목 기록에 매핑
〔스크립트〕	소스	취약한 항목 기록의 소스는 입니다 Tenable.cs.

변환 프로세스 중에 실행되는 세 가지 변환 스크립트가 있습니다. 다음 표에는 각 스크립트가 실행되는 시기와 용도가 나와 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Tenable.cs 취약성 계산 변환 맵 스크립트 타이밍 및 목적

스크립트가 실행될 때	목적
onStart(임포트 세트가 변환을 시작한 경우)	임포트 세트를 사용하여 데이터를 Tenable.cs 임포트하고 각 기록을 CMDB CI 테이블, 취약한 항목 테이블 및 외부 공급업체 취약성 테이블로 로드하는 Tenable CS 계산 취약성 프로세서를 트리거합니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.
onBefore(임포트 세트가 변환을 완료하기 전)	외부 공급업체 항목 및 탐지가 있는지 확인합니다. 그렇지 않은 경우 이러한 기록은 해당 테이블에 생성됩니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.
onComplete(임포트 세트가 변환을 완료한 경우)	에서 Tenable.cs임포트한 CI, VIT 및 탐지 수를 업데이트합니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.

Tenable.cs 컨테이너 취약성 변환 맵 필드

소스 필드	대상 필드	설명
u_digest	Image_id	컨테이너 자산에 대해 Tenable에서 제공하는 고유 다이제스트입니다. 검색된 컨테이너 이미지 및 Docker 이미지 기록에 매핑되며 CI 조회에 사용됩니다.
u_name	이름	Docker 이미지 기록의 이름 필드에 매핑합니다.

임포트에 대한 **Tenable.io** 추가 필터 매개변수 설정

를 Tenable Vulnerability Integration 사용하여 예약된 쿼리에 대한 필터링 매개변수를 사용자 지정하면 제품과 함께 Tenable.io 임포트하는 취약성 데이터를 더욱 세분화할 수 있습니다.

시작하기 전에
사용 사례: 취약성 관리자 또는 분석가는 특정 취약성 상세 정보만 검토할 수 있도록 쿼리에서 데이터를 필터링할 수 있습니다. 예를 들어 , `num_assets`, , `indexed_at`및 로 필터링`cidr_range`되는 임포트된 취약성을 보려고 한다고 `plugin_family`가정해 보겠습니다. 또는 한 실행은 4시간마다 중요한 취약성만 가져오고 다른 실행은 24시간마다 실행하여 중요하지 않은 다른 모든 취약성을 가져오도록 통합을 실행 Tenable.io 하려고 한다고 가정해 보겠습니다.

이 데이터를 수집하는 데 도움이 되도록 필요한 특정 취약성 상세 정보를 가져오는 데 도움이 되는 tenable 지원 매개변수를 추가할 수 있습니다.

이 기능을 사용하면 ServiceNow AI PlatformAPI 호출이나 코딩을 추가하지 않고도 . 다음 Tenable.io 통합은 요청 본문에 JSON 컨텐츠를 제공하여 필터링을 지원합니다.

- 자산 통합
- 수정된 취약성 통합
- 미해결 취약성 통합

이 기능에 문자열을 사용하는 JSON 방법을 알아야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필요한 역할: sn_vul.vulnerability_admin

프로시저

1. 필터링에 사용할 개발자 사이트의 제품에서 Tenable.io 지원하는 매개변수를 찾습니다.

   제품에서 Tenable.io 입력하는 매개변수와 값은 통합 인스턴스 수준에서만 지원됩니다.

2. 다음으로 이동 모두 〉 **Tenable** 취약성 통합 〉 관리 〉 통합.
3. Tenable 통합 목록 페이지에서 열려는 통합에 Tenable.io 대한 기록을 클릭합니다.
4. Tenable REST 메서드 탭을 선택한 상태에서 REST 메서드에 대한 정보 아이콘(i)을 클릭한 다음 기록 열기를 클릭합니다.
5. **HTTP** 요청 탭을 선택합니다.
6. 기록을 편집하려면 페이지 상단에 있는 링크를 클릭하십시오. 기록을 편집하려면 여기를 클릭하십시오.
7. REST 메서드 기록의 컨텐츠 필드에 요청 본문의 일부로 사용할 JSON 컨텐츠를 입력합니다.

   예를 들어, 자산 통합에서 중요한 취약성(CVSS 점수 10.0)만 임포트하도록 임포트한 취약성에 대한 Tenable.io 심각도 매개변수를 다음과 같이 `{"filters": {"severity": ["critical"]}}` 설정할 수 있습니다.

   둘 이상의 매개변수를 입력하려면 각 값을 구분하는 방법에 대한 자세한 내용은 설명서를 참조하십시오 Tenable.io .

8. 업데이트를 클릭합니다.

Tenable 취약성 통합 보고

대시보드에서 취약성 대응 취약성 및 취약한 항목에 대한 보고서를 봅니다.

작업 공간의 데이터 시각화 취약성 대응

작업 공간에는 취약성 대응 정정 진행 상황을 모니터링하는 데 도움이 될 수 있는 데이터 시각화가 포함되어 있습니다. 취약성 데이터가 변경될 때 업데이트되는 동적 데이터 시각화에서 조직에 중요한 활성 취약성의 수와 심각도를 확인하여 조직에 대한 위협 수준을 확인할 수 있습니다. 취약성 관리자 작업 공간 살펴보기IT 정정 작업 공간 살펴보기 를 참조취약성 대응 작업 공간하고 사용 가능한 동적 데이터 시각화에 대한 자세한 내용을 확인할 수 있습니다.

이전 버전 취약성 대응

Vulnerability Response 개요 대시보드(취약성 관리)는 취약성 및 취약한 항목에 대한 경영적 뷰를 제공하여 취약성 관리자가 관심 영역을 신속하게 찾아낼 수 있도록 도와줍니다. 취약성 대응 정정 대시보드(취약성 정정)를 사용하면 정정 전문가가 소유한 정정 작업과 취약한 항목에 집중할 수 있습니다.

자세한 내용은 기본 취약성 대응 대시보드 사용 문서를 참조하십시오.

필요한 역할: 정정 소유자.

가상 사용자 및 세분화된 역할을 사용하여 사용자가 Vulnerability Response 애플리케이션에서 확인하고 수행할 수 있는 내용을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할을 처음 할당하려면 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당.

세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

대시보드를 보려면 다음으로 이동합니다. 취약성 대응 〉 정정 개요.

Tenable 취약성 통합에 대한 통합 실행 상태 차트

Tenable 통합 실행 상태 모듈은 Tenable 통합 실행의 상태에 대한 그래픽 보기를 제공합니다.

차트에서 그래프의 특정 부분을 가리키면 해당 부분과 관련된 데이터 요약이 표시됩니다. 막대 그래프에서 부품을 클릭하면 더 자세한 정보를 제공하는 목록이 열립니다.

필요한 역할: 취약성 관리자.

가상 사용자 및 세분화된 역할을 사용하여 사용자가 Vulnerability Response 애플리케이션에서 확인하고 수행할 수 있는 내용을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할을 처음 할당하려면 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당.

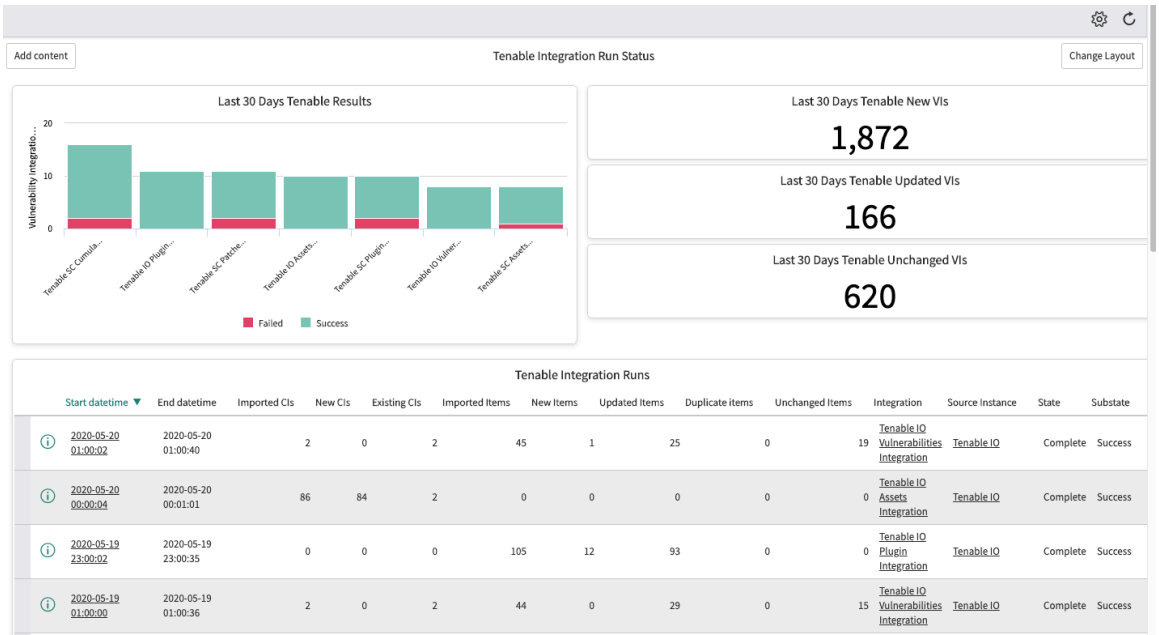
세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

데이터를 보려면 다음으로 이동합니다. 모두 〉 **Tenable** 취약성 통합 〉 통합 실행 상태.

의 취약성 대응버전 19.0부터 이 대시보드는 New Experience UI에서 사용할 수 있습니다.

주:
Tokyo에 있는 경우 Next Experience UI에서 대시보드를 볼 수 있지만 일부 기능 손실이 있습니다.

실행 상태



Tenable 통합 실행 상태 차트 보고서

이름	설명
지난 30일 Tenable 결과	각 통합에 대해 완료된 통합 실행 수입니다. 성공한 실행과 실패한 실행을 모두 표시합니다. 각 실행은 그래프에 막대로 표시됩니다.
지난 30일 Tenable 신규 VI	지난 30일 동안 임포트된 새로운 취약한 항목 수입니다. 정수로 표시됩니다.

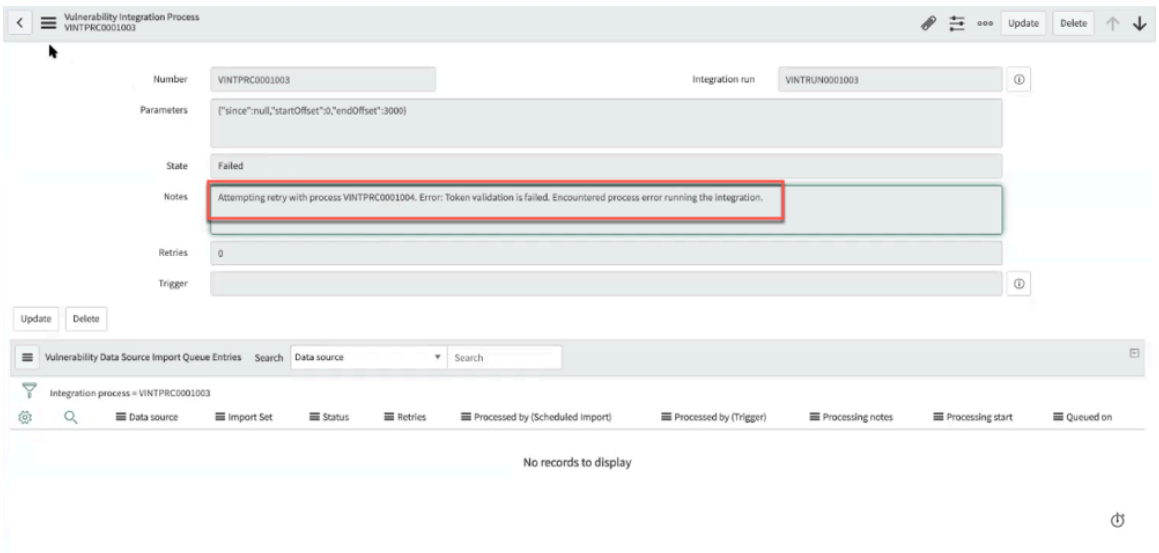
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이름	설명
지난 30일 Tenable 업데이트된 VI	지난 30일 동안 임포트된 업데이트된 취약한 항목 수입니다. 정수로 표시됩니다.
지난 30일 Tenable 미변경 VI	지난 30일 동안 임포트된 중복 취약한 항목 수입니다. 정수로 표시됩니다.
Tenable 통합 실행	통합 실행 기록이 목록에 표시됩니다. 주: **V16.1:** 이 통합에 대한 탐지를 확인하려면 탐지 또는 결과를 ServiceNow 테이블의 탐지 데이터와 *sn_vul_detection* 비교합니다. 통합이 진행되는 동안 탐지 또는 발견 개수가 변경될 수 있습니다. 이 보고서는 통합 실행이 완료된 후 인스턴스의 "종료 날짜 카운트" 열에 탐지 횟수를 표시합니다.

토큰 확인 만료

어떤 이유로든 Tenable.sc 통합 실행이 실패하면 Tenable.sc 에 대한 인증 토큰이 자동으로 만료되고 취약성 통합 프로세스 기록에 메시지가 표시됩니다.

만료된 토큰 메시지



다음 통합 프로세스를 위해 새 토큰이 자동으로 생성됩니다. 모든 통합 프로세스(실패 및 성공)가 취약성 통합 프로세스 기록의 취약성 통합 프로세스 탭에 표시됩니다.

통합에 대한 **Tenable.sc** 재스캔 시작

Tenable 플랫폼에서 다시 스캔을 시작하여 예약된 스캔 주기 사이에 취약한 항목이 정정되었는지 확인합니다. 인스턴스에서 제품의 취약한 항목에 대한 요청 시 재스캔을 Tenable.sc 시작할 수 있습니다 ServiceNow AI Platform# .

시작하기 전에
필요한 역할: sn_vul.write_all 또는 sn_vul.write_assigned

주:
Tenable.sc 은 에이전트 기반 컴퓨터에서 다시 스캔 실행을 지원하지 않습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에 스캐너가 활성화되어 있는지 확인하십시오. 다음으로 이동 취약성 대응 〉 취약성 스캐닝 〉 스캐너.

이 태스크 정보

작업 공간에서 다시 스캔을 시작하려면 다음 문서를 참조하십시오 작업 공간에서 취약성 대응 취약한 항목 다시 스캔 Tenable.ioTenable.sc.

아래 나열된 단계에 따라 클래식 환경에서 재검색을 시작합니다.

예약된 전체 검사와 관련된 오버헤드와 볼륨을 줄이기 위해 정정 소유자, IT 전문가, 취약성 분석가 또는 취약성 관리자는 해당 환경에서 자산(구성 항목)의 특정 취약성에 대한 요청 시 대상 재검사를 시작할 수 있습니다. VI(취약한 항목), RT(정정 작업), TPE(외부 공급업체 항목) 또는 인스턴스에서 검색된 항목 기록에서 다시 스캔을 시작할 수 있습니다 ServiceNow AI Platform .

재검사를 통해 정정 소유자와 취약성 분석가는 정정 활동, 패치 및 기타 작업이 구성 항목(CI)의 특정 취약성을 성공적으로 수정했는지 확인할 수 있습니다.

예를 들어, 전체 환경은 3주에 한 번씩 검사됩니다. 가장 최근의 전체 검사는 일주일 전에 완료되었지만 중요한 취약성을 수정하기 위해 어제 패치를 적용했습니다. 이 취약성의 특성으로 인해 다음 예약된 검사에서 정정되었는지 확인할 때까지 2주를 기다릴 수 없습니다. 패치가 이전 검사 중에 발견된 중요 취약성을 성공적으로 수정했는지 확인하기 위해 취약한 항목에 대한 Tenable.sc 대상 재스캔 ServiceNow AI Platform 을 시작할 수 있습니다.

주:
인스턴스에서 재스캔을 ServiceNow AI Platform# 요청할 때 자격 증명을 선택하는 Vulnerability Response Integration with Tenable 것은 선택 사항입니다. 스캔 자격 증명 통합은 ServiceNow# Tenable.sc 인스턴스의 제품에서 Tenable.sc 스캐너 자격 증명을 임포트하고 업데이트합니다. 이 통합은 매주 실행되어 Tenable 자격 증명 데이터를 임포트하고 안전하게 저장합니다.

임포트된 이 데이터에는 Tenable 암호 또는 기타 민감한 Tenable 계정 정보가 포함되지 않습니다. ServiceNow# Tenable.sc 취약성 통합(Tenable.sc미해결 및 수정된 취약성 통합)을 구성할 때 인스턴스의 설정 도우미 내에서 검사 자격 증명 통합이 자동으로 활성화(##)됩니다Tenable.sc.

임포트하는 자격 증명에 대한 다음 정보를 기록해 두십시오. 그래야 사용자가 인스턴스에서 필요할 ServiceNow AI Platform 때 볼 수 있습니다.

- 관리자 사용자 역할로 만든 자격 증명은 Tenable.sc 모든 조직의 사용자가 사용할 수 있습니다.
- 조직 사용자 역할로 Tenable.sc 만든 자격 증명은 해당 조직 내의 사용자만 사용할 수 있습니다. 이러한 자격 증명은 인스턴스에 연결하는 데 사용되는 사용자 계정과 공유되지 않는 한 작성자의 조직 외부에 있는 사용자용 계정으로 임포트 ServiceNow AI Platform 되지 않습니다.

자세한 내용은 설명서 웹 사이트를 Tenable.sc 참조하십시오.

애플리케이션 구성에 Tenable.sc 대한 자세한 내용은 을 참조하십시오설정 도우미를 사용하여 Tenable 취약성 통합 구성. 검사 자격 증명 통합에 대한 자세한 내용을 보려면 다음으로 이동하십시오. 모두 〉 **Tenable** 취약성 통합 〉 통합 〉 **Tenable.sc** 스캔 자격 증명 통합.

통합 실행 중에 여러 프로세스가 생성되고 데이터가 페이지 형식으로 수신됩니다. 각 프로세스에는 페이지에 첨부된 데이터가 있는 하나 이상의 임포트 큐 항목이 포함될 수 있습니다. 이러한 항목은 1시간의 시간 제한 내에 데이터를 처리해야 합니다. 그러나 페이로드 크기가 크면 처리 시간이 1시간을 초과하거나 중단되어 통합 시간 제한 오류가 발생할 수 있습니다. 통합은 시간 초과 오류에도 불구하고 데이터를 계속 처리합니다. 이러한 잘못된 통신을 피하기 위해 버전 18.2.4 취약성 대응부터 큐가 활성 상태이고 데이터를 처리하는지 여부를 나타내기 위해 타임스탬프(하트비트)가 주기적으로 전송됩니다. 임포트 큐 항목 페이지의 처리된 마지막 기록 필드는 임포트

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

큐가 생성하거나 업데이트하는 기록 수에 따라 업데이트됩니다. 임포트 큐 항목이 1시간의 시간 제한을 초과하는 경우, 시스템은 마지막으로 처리된 기록 필드를 검사하여 1시간보다 오래되었는지도 확인합니다. 이 경우 이는 임포트 큐 항목이 고착되었음을 나타내며 처리 시 더 이상의 지연을 방지하기 위해 시간 초과됩니다.

주:
마지막으로 처리된 기록 필드는 다음 시스템 속성에 정의된 내용에 따라 업데이트됩니다.

- *sn_sec_cmn.record_threshold_heartbeat*: 하트비트(타임스탬프)가 임포트 큐 항목으로 전송된 후 처리된 기록 수를 정의합니다.
- *sn_sec_cmn.maximum_heartbeat_delay*: 임포트 큐 항목을 시간 초과해야 하는 시간을 정의합니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 취약한 항목.
2. 다시 스캔을 트리거할 취약한 항목 기록을 찾아 엽니다.

   주:
   VI Tenable.sc 에 대한 재스캔만 소스로 시작할 수 있습니다. 확인 Tenable.sc 이 VI 목록 뷰의 소스 열 또는 개별 기록의 소스 필드에 표시됩니다. 조건 빌더를 사용하여 소스별로 VI를 그룹화할 수 있습니다. 또는 소스 열이 VI 목록 뷰에 표시되지 않은 경우 목록의 왼쪽 상단에서 목록 개인화 아이콘(기어 아이콘)을 클릭하고 슬러 시버킷을 사용하여 소스를 사용 가능 에서 선택됨으로 이동합니다.

3. 또는 다음으로 이동합니다. 모두 〉 취약성 대응 〉 정정 작업 또는 취약성 대응 〉 라이브러리 〉 외부 공급업체 각각 다시 검색에 사용할 정정 작업 또는 외부 공급업체 항목 기록의 경우

   선택에 따라 다음 기록에서 다시 스캔 버튼을 사용할 수 있습니다.

   - 단일 VI 기록에서 VI는 제품에서 나온 Tenable.sc 것이어야 하며 종결 이외의 상태여야 합니다. 여러 VI 레코드의 경우 모든 VI는 Tenable.sc 제품에서 가져온 것이어야 하며 종결 이외의 상태여야 합니다.
   - RT 레코드에서 정정 작업은 종결 이외의 모든 상태일 수 있으며 연결된 모든 VI는 제품에서 가져와야 Tenable.sc 합니다.
   - 타사 항목(TPE) 레코드에서 레코드에는 종결 이외의 상태인 제품의 연결된 VI 레코드가 Tenable.sc 하나 이상 있어야 합니다.

4. 기록의 오른쪽 상단에서 Rescan(다시 스캔)을 클릭합니다.
   스캐너에 액세스하기 위해 스캐너 자격 증명을 선택하라는 메시지가 표시됩니다. 스캔 자격 증명 통합에서 임포트한 자격 증명입니다 Tenable.sc .
5. 대화 상자에서 원하는 필터와 자격 증명 유형을 선택합니다.
6. 스캔 요청을 클릭합니다.

   스캔이 처리 중임을 나타내는 메시지가 표시됩니다. 모든 재스캔의 상태는 재스캔을 시작하는 데 사용한 VI, RT, TPE 기록의 스캔 관련 목록에서 언제든지 확인할 수 있습니다. 메시지에서 세부 정보 보기를 클릭하여 다시 스캔 상태를 확인하고 지정된 기록에서 시작된 다른 다시 스캔을 봅니다.

   모든 하위 스캔이 성공적으로 완료되면 상위 스캔 기록의 상태 필드가 완료로 표시됩니다. 하위 스캔 임포트 데이터. 상위 스캔 기록은 하위 스캔을 위한 컨테이너입니다.

   인스턴스는 ServiceNow AI Platform# 재스캔 상태가 성공적으로 완료될 때까지, 또는 설정된 추적 기간이 초과될 때까지(먼저 발생하는 쪽 적용) 재스캔 상태를 추적합니다. 시간 제한은 검사를

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

중지하지 않습니다. 시간 제한은 실제 다시 검색이 중지된 시간이 아니라 다시 스캔 상태 추적이 ServiceNow AI Platform# 중지된 시기를 나타냅니다. 종결/고정으로 전환되었거나 전환될 모든 VI는 Tenable.sc Fixed Vulnerabilities Integration의 다음 예약된 임포트와 함께 임포트됩니다.

통합에 대한 **Tenable.io** 재스캔 시작

Tenable 플랫폼에서 다시 스캔을 시작하여 예약된 스캔 주기 사이에 취약한 항목이 정정되었는지 확인합니다. 인스턴스에서 제품의 취약한 항목에 대한 요청 시 재스캔을 Tenable.io 시작할 수 있습니다 ServiceNow AI Platform# .

시작하기 전에
필요한 역할: sn_vul.write_all 또는 sn_vul.write_assigned

시작하기 전에 스캐너가 활성화되어 있는지 확인하십시오. 다음으로 이동 취약성 대응 〉 취약성 스캐닝 〉 스캐너.

이 태스크 정보

- Vulnerability Response 작업 공간에서 다시 스캔을 시작하려면 다음을 에서 기록 및 정정 작업을 다시 스캔 취약성 관리자 작업 공간에서 취약한 항목 및 정정 작업 다시 스캔 IT 정정 작업 공간 참조하십시오.
- 아래 나열된 단계에 따라 클래식 환경에서 재검색을 시작합니다.

주:
Tenable.io 은 에이전트 기반 컴퓨터에서 다시 스캔 실행을 지원하지 않습니다.

예약된 전체 검사와 관련된 오버헤드와 볼륨을 줄이기 위해 정정 소유자, IT 전문가, 취약성 분석가 또는 취약성 관리자는 요청 시 대상 재검사를 시작할 수 있습니다. 사용자 환경에서 자산(구성 항목)의 특정 취약성을 스캔할 수 있습니다. 인스턴스의 VI(취약한 항목), VUL(정정 작업), TPE(외부 공급업체 항목) 또는 SDI(검색된 항목) 기록에서 재스캔을 시작할 수 있습니다 ServiceNow AI Platform . 재검색을 통해 정정 활동, 패치 및 기타 작업이 구성 항목(CI)의 특정 취약성을 성공적으로 수정했는지 확인할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
인스턴스에서 재스캔을 ServiceNow AI Platform# 요청할 때 자격 증명을 선택하는 Vulnerability Response Integration with Tenable 것은 선택 사항입니다. 스캔 자격 증명 통합은 ServiceNow# Tenable.io 인스턴스의 제품에서 Tenable.io 스캐너 자격 증명을 임포트하고 업데이트합니다. 이 통합은 매주 실행되어 Tenable 자격 증명 데이터를 임포트하고 안전하게 저장합니다.

임포트된 이 데이터에는 Tenable 암호 또는 기타 민감한 Tenable 계정 정보가 포함되지 않습니다.

다음 정보는 인스턴스에서 필요할 ServiceNow AI Platform 때 사용자가 볼 수 있도록 임포트하는 자격 증명에 대해 설명합니다.

- 관리자 사용자 역할로 만든 자격 증명은 Tenable.io 모든 조직의 사용자가 사용할 수 있습니다.
- 조직 사용자 역할로 Tenable.io 만든 자격 증명은 해당 조직 내의 사용자만 사용할 수 있습니다. 이러한 자격 증명은 인스턴스에 연결하는 데 사용되는 사용자 계정과 공유되지 않는 한 작성자의 조직 외부에 있는 사용자용 계정으로 임포트 ServiceNow AI Platform 되지 않습니다.

  자세한 내용은 설명서 웹 사이트를 Tenable.io 참조하십시오.

- Tenable.io 재스캔을 시작하기 전에 템플릿 통합과 Tenable.io 스캔 자격 증명 통합을 활성화해야 합니다. 검사 자격 증명 통합에 대한 자세한 내용을 보려면 다음으로 이동하십시오. **Tenable** 취약성 통합 〉 통합 〉 **Tenable.io** 스캔 자격 증명 통합.

  기본적으로 템플릿 및 스캔 자격 증명 통합은 비활성화되어 있습니다. 에 대한 Tenable.io자격 증명을 입력하면 모든 Tenable.io 통합이 자동으로 활성화됩니다. 통합을 수동으로 활성화하거나 비활성화하려면 다음을 수행합니다.

  1. 다음으로 이동 모두 〉 **Tenable** 취약성 통합 〉 관리 〉 통합.
  2. 표시되는 목록에서 원하는 통합 기록을 찾습니다 Tenable.io .
  3. 통합을 활성화하려면 각 기록을 열고 활성 확인란을 선택합니다.
  4. 변경 사항을 저장하려면 업데이트를 클릭합니다.
  5. 설정 도우미로 돌아가 에 취약성 대응대한 Tenable Vulnerability Integration 구성을 계속합니다.

및 제품 구성에 Tenable.io 대한 자세한 내용은 을 Tenable.sc 참조하십시오설정 도우미를 사용하여 Tenable 취약성 통합 구성.

전체 환경이 3주에 한 번씩 스캔된다고 가정해 보겠습니다. 가장 최근의 전체 검사는 일주일 전에 완료되었지만 중요한 취약성을 수정하기 위해 어제 패치를 적용했습니다. 이 취약성의 특성으로 인해 다음 예약된 검사에서 정정되었는지 확인할 때까지 2주를 기다릴 수 없습니다. 패치가 이전 검사 중에 발견된 중요 취약성을 성공적으로 수정했는지 확인하기 위해 취약한 항목에 대한 Tenable.io 대상 재스캔 ServiceNow AI Platform 을 시작할 수 있습니다.

수정된 취약성 통합의 다음 예약된 임포트 후에 검사를 시작한 기록에 대한 업데이트된 결과를 볼 수 있습니다.

통합 실행 중에 여러 프로세스가 생성되고 데이터가 페이지 형식으로 수신됩니다. 각 프로세스에는 페이지에 첨부된 데이터가 있는 하나 이상의 임포트 큐 항목이 포함될 수 있습니다. 이러한 항목은 1시간의 시간 제한 내에 데이터를 처리해야 합니다. 그러나 페이로드 크기가 크면 처리 시간이 1시간을 초과하거나 중단되어 통합 시간 제한 오류가 발생할 수 있습니다. 통합은 시간 초과 오류에도 불구하고 데이터를 계속 처리합니다. 이러한 잘못된 통신을 피하기 위해 버전 18.2.4 취약성 대응부터 큐가 활성 상태이고 데이터를 처리하는지 여부를 나타내기 위해 타임스탬프(하트비트)가 주기적으로 전송됩니다. 임포트 큐 항목 페이지의 처리된 마지막 기록 필드는 임포트 큐가 생성하거나 업데이트하는 기록 수에 따라 업데이트됩니다. 임포트 큐 항목이 1시간의 시간

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

제한을 초과하는 경우, 시스템은 마지막으로 처리된 기록 필드를 검사하여 1시간보다 오래되었는지도 확인합니다. 이 경우 이는 임포트 큐 항목이 고착되었음을 나타내며 처리 시 더 이상의 지연을 방지하기 위해 시간 초과됩니다.

주:
마지막으로 처리된 기록 필드는 다음 시스템 속성에 정의된 내용에 따라 업데이트됩니다.

- *sn_sec_cmn.record_threshold_heartbeat*: 하트비트(타임스탬프)가 임포트 큐 항목으로 전송된 후 처리된 기록 수를 정의합니다.
- *sn_sec_cmn.maximum_heartbeat_delay*: 임포트 큐 항목을 시간 초과해야 하는 시간을 정의합니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 취약한 항목.
2. 다시 스캔을 트리거할 취약한 항목 기록을 찾아 엽니다.

   주:
   스캐너를 Tenable.io 사용하는 경우 VI에 대한 재스캔만 소스로 시작할 Tenable.io 수 있습니다. 확인 Tenable.io 이 VI 목록 뷰의 소스 열 또는 개별 기록의 소스 필드에 표시됩니다. 조건 빌더를 사용하여 소스별로 VI를 그룹화할 수 있습니다. 또는 소스 열이 VI 목록 뷰에 표시되지 않은 경우 목록의 왼쪽 상단에서 목록 개인화 아이콘(기어 아이콘)을 클릭하고 슬러 시버킷을 사용하여 소스를 사용 가능 에서 선택됨으로 이동합니다.

3. 또는 다음으로 이동합니다. 모두 〉 취약성 대응 〉 정정 작업 또는 취약성 대응 〉 라이브러리 〉 외부 공급업체 재스캔에 사용할 기록의 경우.

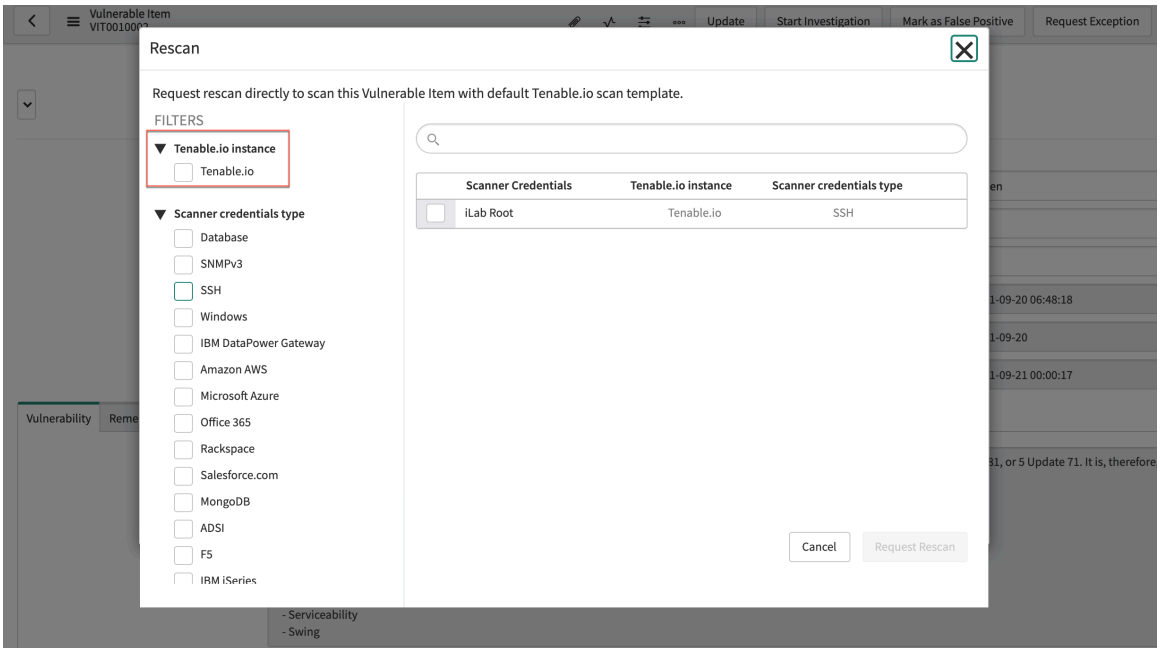
   선택에 따라 다음 기록에서 다시 스캔 버튼을 사용할 수 있습니다.

   - 단일 VI 기록에서 VI는 종결 이외의 상태여야 합니다. 여러 VI 레코드의 경우 모든 VI는 제품에서 가져온 Tenable.io 것이어야 하며 종결 이외의 상태여야 합니다.
   - 정정 작업 기록의 경우 종결 됨 이외의 상태에 있는 정정 작업만 지원됩니다. 연결된 모든 VI는 종결 이외의 상태여야 하며 소스로 사용 Tenable.io 되어야 합니다.
   - 타사 항목(TPE) 레코드에서 레코드에는 종결 이외의 상태인 제품의 연결된 VI 레코드가 Tenable.io 하나 이상 있어야 합니다.
   - 검색된 항목 기록에서 기록에는 종결 이외의 상태인 제품의 연결된 VI 기록 Tenable.io 이 하나 이상 있어야 합니다.
   - 취약한 항목 목록에서 다시 스캔하려는 개별 취약한 항목을 선택할 수 있습니다. 화면 왼쪽 아래에 있는 선택한 행에 대한 작업 메뉴를 사용하여 다시 검색을 시작합니다. 자격 증명을 입력하라는 메시지가 나타납니다.

4. 기록의 오른쪽 상단에서 Rescan(다시 스캔)을 클릭합니다.
   다시 스캔할 인스턴스와 스캐너에 액세스하는 데 사용할 스캐너 자격 증명을 선택하라는 메시지가 표시됩니다. 표시된 자격 증명은 검사 자격 증명 통합에서 Tenable.io 가져온 자격 증명입니다.
5. 대화 상자에서 인스턴스 및/또는 인스턴스와 사용할 자격 증명 유형을 선택합니다.

   다음 이미지에는 하나의 통합 인스턴스 Tenable.io 표시되어 있습니다. 인스턴스가 두 Tenable.io 개 이상인 경우 양식의 Tenable.io 섹션 아래에 모두 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



6. **Request** Rescan(다시 스캔 요청)을 클릭합니다.

스캔이 처리 중이고 상위 스캔 기록이 생성되었음을 나타내는 메시지가 표시됩니다. 모든 하위 스캔의 상태는 다시 스캔을 시작하는 데 사용한 VI, 정정 작업, TPE 및 SDI 기록의 스캔 관련 목록에서 언제든지 확인할 수 있습니다. 메시지에서 세부 정보 보기를 클릭하여 다시 스캔 상태를 확인하고 지정된 기록에서 시작된 다른 다시 스캔을 봅니다.

모든 하위 스캔이 성공적으로 완료되면 상위 스캔 기록의 상태 필드가 완료로 표시됩니다. 하위 스캔 임포트 데이터. 각 스캔은 통합 인스턴스, TPE, IP 및 네트워크 ID의 고유한 조합을 지원합니다. 상위 스캔 기록에 여러 하위 스캔이 표시될 수 있습니다. 예를 들어, 하위 스캔에서 지원할 수 있는 최대 IP 주소 수는 1,000개입니다. 취약한 항목에 대한 IP가 1002개인 경우 요청을 지원하기 위해 두 개의 하위 스캔이 생성되고 스캔 관련 목록에 나열됩니다. 상위 스캔 기록은 하위 스캔을 위한 컨테이너이며 해당 상태는 하위 스캔의 상태를 반영합니다.

인스턴스는 ServiceNow AI Platform# 재스캔 상태가 성공적으로 완료될 때까지, 또는 설정된 추적 기간이 초과될 때까지(먼저 발생하는 쪽 적용) 재스캔 상태를 추적합니다. 시간 제한은 검사를 중지하지 않습니다. 시간 제한은 실제 다시 검색이 중지된 시간이 아니라 다시 스캔 상태 추적이 ServiceNow AI Platform# 중지된 시기를 나타냅니다. 종결/고정으로 전환되었거나 전환될 모든 VI는 고정 취약성 통합의 다음 예약된 임포트와 함께 임포트됩니다Tenable.io.

오류가 발생한 스캔의 경우 상위 스캔 기록에서 하위 스캔을 확인할 수 있습니다. 하위 스캔의 응답 페이로드에서 오류를 봅니다.

수정된 취약성 통합의 다음 예약된 임포트 후에 검사를 시작한 기록에 대한 업데이트된 결과를 볼 수 있습니다.

의 네트워크 파티션 식별자로 구성 항목을 업데이트합니다. **Tenable Vulnerability Integration**

IP 주소를 공유하는 환경의 자산에 대한 고유한 CI(구성 항목)를 생성합니다. 환경 전반에서 고유한 자산을 식별하고 기존 검색된 항목, 취약한 항목 및 탐지 레코드의 CI를 자동으로 업데이트하여 취약성에 대한 자세한 정보를 제공합니다.

시작하기 전에
필요한 역할: 관리자

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보
기본적으로 취약성 대응 애플리케이션에서 자산을 식별하는 한 가지 방법은 IP 주소를 사용하는 것입니다. 경우에 따라 자산은 IP 주소를 공유할 수 있지만 CMDB에 하나의 CI로 저장됩니다.

예를 들어 다음 표와 같이 환경의 여러 자산(CI)은 IP 주소를 공유할 수 있지만 고유한 네트워크 및 리포지토리 ID를 가질 수 있습니다. 그러나 기본적으로 이러한 자산은 일반적으로 IP 주소 조회 중에 단일 CI (CI 1) 로 식별되고 저장됩니다.

기본 **IP** 조회 및 **CI** 생성

소스	**IP** 주소	**Network_id**	구성 항목
Tenable.io: 자산과 고정 및 미해결 취약성 통합	123.12.12.141	03712	CI 1
	123.12.12.141	03713	CI 1

소스	**IP** 주소	**Repository_id**	구성 항목
Tenable.sc: 자산과 고정 및 미해결 취약성 통합	123.12.12.141	12	CI 1
	123.12.12.141	13	CI 1

동일한 IP 주소를 가진 자산에 대해 개별 CI를 생성하여 고유한 자산으로 식별할 수 있습니다. 새로운 데이터 임포트를 시작으로 예약된 작업을 실행하여 네트워크 파티션 식별자(network_partition_identifier)를 포함하는 기존 CI *`Update existing discovered items with network partition identifier`*를 보다 세밀하게 업데이트할 수 있습니다.

이 예약된 작업은 기본적으로 비활성화되어 있습니다. 설정 도우미에서 및 Tenable.sc 제품의 자산과 고정 및 미해결 취약성 통합 Tenable.io 에 대해 이 기능을 활성화하여 기록에서 이 식별자를 봅니다.

이 예약된 작업은 활성화되면 임포트한 데이터의 기존 CI 기록에 네트워크 파티션 식별자(network_partition_identifier)를 추가합니다. IRE에서 만든 기존 CI도 업데이트됩니다. 또한 예약된 작업은 다음 임포트로 시작하는 네트워크 파티션 식별자를 포함하는 CI를 생성합니다. 또는 요청 시 작업을 시작하여 기존 데이터를 업데이트할 수 있습니다.

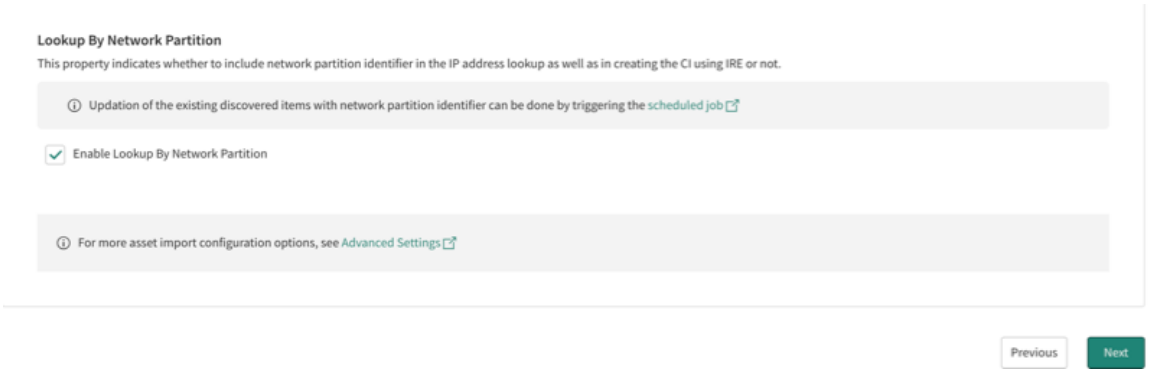
Tenable Vulnerability Integration v14.0 취약성 대응 및 v2.2부터 업그레이드하는 경우 CMDB CI Class Models(1.0.21.)가 지원됩니다. 클래스 모델에는 IRE(식별 및 조정) 식별 규칙에 네트워크 파티션 식별자(network_partition_identifier)가 있습니다.

옵션	설명
요청 시 예약된 작업을 실행합니다.	기존 검색 항목을 업데이트합니다. 네트워크 파티션 식별자 세분성을 포함하도록 기존 Tenable 데이터에 대한 CI가 생성되거나 업데이트됩니다. 검색된 항목, 취약한 항목 및 탐지 기록이 모두 새 CI로 업데이트됩니다.
다음 예약된 작업과의 통합에서 최신 데이터가 임포트될 때까지 기다립니다.	예약된 다음 작업으로 시작하는 네트워크 파티션 식별자를 사용하여 각각의 새 자산에 대한 CI를 생성합니다. CI, 취약한 항목 및 탐지 기록이 모두 새로운 세분성을 포함하도록 업데이트됩니다. 정확히 일치하는 항목이 없으면 새 CI가 만들어집니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 설정 도우미 〉 통합 구성 〉 스캐너 통합.
2. 통합 또는 Tenable.sc 통합을 선택합니다Tenable.io.
3. 필요한 통합을 편집합니다.
4. 선택 자산 임포트 설정.
5. 선택 네트워크 파티션별 조회 사용 의 확인란 네트워크 파티션별 조회 사용 절.



6. 다음을 클릭합니다.

네트워크 파티션 식별자 NETWORK_ID 및 리포지토리 _ID 포함되며 기존 CI를 업데이트하거나 다음 예약된 작업으로 CI를 생성합니다.

IP 조회 및 **CI** 생성에 포함된 네트워크 파티션 식별자 속성

소스	**IP** 주소	**NETWORK_ID**	네트워크 파티션 식별자가 없는 자산에 대한 **CI**	**CI** 네트워크 파티션 식별자가 있는 자산
Tenable.io: 자산과 고정 및 미해결 취약성 통합	123.12.12.141	03712	CI 1	CI 1
	123.12.12.141	03713	CI 1	CI 2

소스	**IP** 주소	**REPOSITORY_ID**	네트워크 파티션 식별자가 없는 자산에 대한 **CI**	**CI** 네트워크 파티션 식별자가 있는 자산
Tenable.sc: 자산과 고정 및 미해결 취약성 통합	123.12.12.141	12	CI 1	CI 1
	123.12.12.141	13	CI 1	CI 2

다음 예약된 작업에서 IP 주소 및 불완전한 IP 주소 CI 식별 조회 규칙에는 및 Tenable.sc 제품에 대한 Tenable.io 자산 및 고정 및 미해결 취약성 통합에서 데이터를 임포트하기 위한 네트워크 파티션 식별자 속성이 자동으로 포함됩니다.

시스템 속성을 활성화하고 기록을 저장한 후 요청 시 예약된 작업을 시작하여 네트워크 파티션 식별자가 포함된 CI로 기존 검색된 항목을 업데이트할 수도 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Tenable 취약성 통합에 대한 수정 사항 임포트

선택적 수정 사항을 구성하고 Tenable 취약성 통합에서 Tenable 취약성 임포트 통합을 위해 특별히 일부 데이터를 간소화합니다 ServiceNow# .

시작하기 전에

필요한 역할: sn_vul.vulnerability_admin

이 태스크 정보

이 작업 집합에는 코딩과 에 대한 ServiceNow AI Platform고급 지식이 필요합니다.

다음 단계에 따라 Tenable 취약성 통합에 대해 도메인 분리된 임포트를 생성합니다. 다음 예는 Tenable.io 미해결 취약성 통합용이지만 이 콘텐츠는 다른 Tenable 통합에 적용할 수 있습니다.

프로시저

1. 도메인을 생성합니다.
2. 생성하는 모든 도메인에 대해 사용자를 생성하고 사용자를 해당 도메인에 할당합니다.

   이 사용자를 Tenable.io 도메인의 run_as 자리 표시자로 생각하십시오.

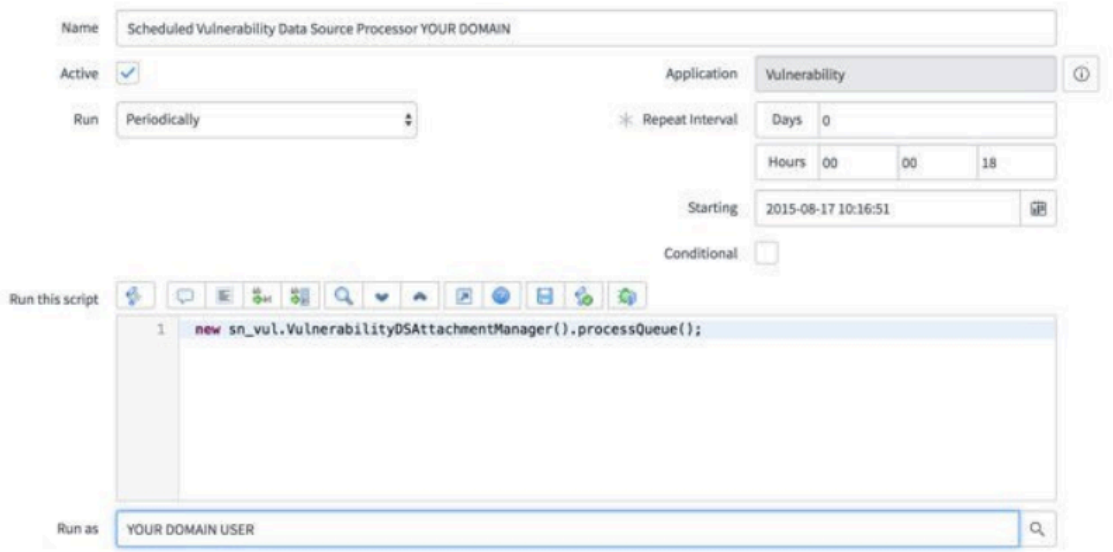
3. 취약성 통합을 엽니다.
   사용자는 VR과 동일합니다. 전역 도메인의 시스템 사용자이며 sn_vul.tenable_configure_integration, import_admin 및 sn_vul.vulnerability_write 역할이 있어야 합니다. 이 사용자는 데이터 소스, 변환 맵 및 취약성 데이터에 액세스할 수 있어야 합니다.

   > **주:**
   > 이 사용자를 이 역할과 관련된 것으로 간주합니다. 사용자에게 다른 목적이 있어서는 안 됩니다.

4. 각 도메인에서 아래에 있는 예약된 취약성 데이터 소스 프로세서를 복사하여 예약된 작업을 생성합니다. 시스템 정의 〉 예약된 작업.
5. 이름에 도메인을 추가하여 예약된 작업을 식별합니다.
6. run_as 사용자를 이전 단계에서 만든 사용자로 변경합니다.

   > **주:**
   > 통합이 run_as 사용자 도메인에서 실행되도록 다음 UI 작업을 편집합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



7. Tenable.io 미해결 취약성 통합에서 지금 실행 UI 작업을 편집하여 이 코드 블록을 파일의 맨 위에 추가합니다.

```
//sys id below is of Tenable.io integration if(current.sys_id ==
"4df3f18d53730010d7f1ddeeff7b12a9"){ current.run_as = gs.getUserID (); }
```

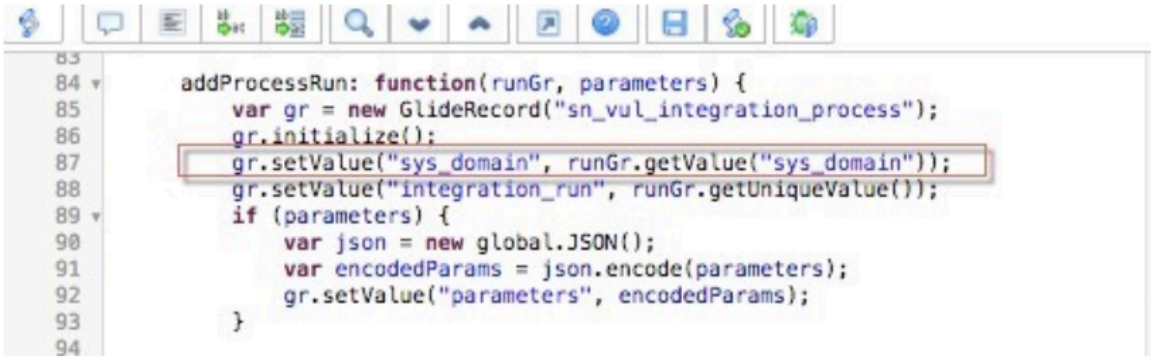
주:
통합이 run_as 사용자 도메인에서 실행되도록 다음 스크립트 포함을 편집합니다.

8. VulnerabilityIntegrationUtils 스크립트 포함 메서드 addIntegrationRun을 편집하여 강조 표시된 코드를 추가합니다.

```
addIntegrationRun: function(integrationGr, optInitialState) {
    if (!optInitialState)
        optInitialState = "ready";
    var importSource = "";
    if ((integrationGr.getValue("name")).indexOf("Qualys") != -1)
        importSource = "Qualys";
    var gr = new GlideRecord("sn_vul_integration_run");
    gr.initialize();
    gr.setValue("integration", integrationGr.getUniqueValue());
    gr.setValue("state", optInitialState);
    gr.setValue("source", importSource);
    var gUser = new GlideRecord("sys_user");
    gUser.get(gs.getUserID());
    gr.setValue("sys_domain",
    gUser.getValue("sys_domain"));
    return gr.insert();
},
```

9. VulnerabilityIntegrationUtils 스크립트 포함 메서드 addProcessRun을 편집하여 강조 표시된 코드를 추가합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



```
addProcessRun: function(runGr, parameters) {
    var gr = new GlideRecord("sn_vul_integration_process");
    gr.initialize();
    gr.setValue("sys_domain", runGr.getValue("sys_domain"));
    gr.setValue("integration_run", runGr.getUniqueValue());
    if (parameters) {
        var json = new global.JSON();
        var encodedParams = json.encode(parameters);
        gr.setValue("parameters", encodedParams);
    }
```

10. DataSourceVulnReportRefreshProcessor 스크립트 포함 메서드 _processFromDataSourceGroups 편집하여 원래 코드를 편집된 _processFromDataSourcesGroups 코드로 원래 _processFromDataSourcesGroups 변경합니다.
11. VulnerabilityDSAttachmentManager 스크립트 포함 메서드인 queueItem을 편집하여 강조 표시된 코드 블록 queueItem, _getNext _processQueueEntry 함수를 추가합니다.

    도메인 분리 호스트 탐지를 임포트할 준비가 되었습니다.

    임포트하기 전에 계산기 사용 안 함

    계산기를 사용하지 않는 경우 다음 단계를 수행하여 기본 계산기를 비활성화합니다. 취약성 계산기를 사용하지 않는 경우 정의한 다른 계산기 외에 기본 계산기를 비활성화하는 것이 가장 좋습니다. 취약성 계산기는 취약한 항목 기록에 액세스할 때마다 실행되며 인스턴스 성능에 영향을 줄 수 있습니다.

    필요한 역할: sn_vul.vulnerability_admin.

12. 다음으로 이동 모두 〉 취약성 〉 관리 〉 취약성 계산기.
13. 취약성 영향 그룹을 엽니다.
14. 점수 및 서비스 기반 영향 계산기를 엽니다.
15. 활성 필드를 선택 취소하여 계산기를 비활성화합니다.
16. 업데이트를 클릭합니다.

    기본 계산기를 사용하지 않도록 설정했습니다.

    초기 임포트 전에 알림 기반 비즈니스 규칙 비활성화

    초기 기록을 임포트하기 전에 알림 관련 비즈니스 규칙을 비활성화하려면 다음 단계를 따르십시오. 기록을 처음 임포트하는 동안 특정 알림 관련 비즈니스 규칙에서 많은 알림이 생성되어 성능에 영향을 줄 수 있습니다. 이러한 비즈니스 규칙은 임포트 중에 비활성화하도록 수정해야 합니다.

    필요한 역할은 sn_vul.vulnerability_admin입니다.

17. 다음으로 이동 모두 〉 시스템 정의 〉 비즈니스 규칙.
18. 영향을 받는 CI 알림을 검색합니다.
19. 비즈니스 규칙을 열고 다음 조건을 *current.sys_class_name != "sn_vul_vulnerable_item"* 삽입합니다.
20. 업데이트를 클릭합니다.
21. 다음 비즈니스 규칙에 대해 이 절차를 반복합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 영향을 받는 비용 센터 알림
- 영향을 받는 그룹 알림
- 영향을 받는 위치 알림

> **주:**
> 초기 기록 임포트가 완료된 후 이러한 비즈니스 규칙을 다시 사용하도록 설정할 수 있습니다. 그러나 비활성화된 상태로 두는 것이 좋습니다. 이로 인해 많은 수의 알림이 생성되고 인스턴스 성능에 영향을 줄 수 있습니다.

초기 시작 날짜 수정

다음 단계에 따라 초기 시작 날짜를 수정합니다. 설정 도우미를 사용하여 설치하는 동안 Tenable 통합의 초기 시작 날짜를 설정합니다. 다음 단계에 표시된 대로 설정 도우미 또는 기본 통합에서 시작 날짜를 재설정할 수 있습니다.

22. 다음으로 이동 모두 〉 **Tenable** 취약성 통합 〉 관리 〉 통합.
23. 통합을 클릭합니다.
24. 통합 상세 정보를 클릭합니다.
25. 시작 시간 필드를 과거의 값으로 설정하면 해당 시간 이후에 스캔되고 탐지된 모든 취약성이 탐지됩니다.

    설정 도우미를 사용하여 Tenable을 구성한 경우, 시작 시간 필드는 처음에는 오늘 날짜의 3개월 전으로, 그 다음에는 오늘 날짜로 미리 채워집니다. 참고: 값을 최대 과거 월로 설정하는 것이 좋습니다. 이렇게 하면 많은 양의 데이터가 Tenable API 속도 제한을 초과하지 않고 실행 시간 초과가 트리거되는 것을 방지할 수 있습니다.
26. 제출 또는 업데이트를 클릭합니다.
27. 옵션: 지금 실행을 클릭하여 즉시 실행합니다.

취약성 인스턴스를 기반으로 **Tenable** 탐지를 분할하여 취약 항목을 분할합니다.

ServiceNow# 취약성 대응을 사용하여 Tenable 스캐너에서 탐지를 분할하여 탐지된 각 취약성 인스턴스에 대해 고유한 취약한 항목(VIT)을 생성할 수 있습니다. 이렇게 분할하면 다양한 정정 팀에 VIT를 할당하여 취약성 관리 및 추적을 강화할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
Tenable 스캐너의 페이로드에는 탐지 데이터가 포함되어 있으며, 증명 내의 각 경로는 탐지를 분할하는 데 사용됩니다. 페이로드의 출력 태그는 취약성의 위치를 식별하여 특정 경로에 따라 취약성을 정확하게 식별하고 관리할 수 있도록 합니다.

프로시저

1. 외부 공급업체 통합 테이블 〔sn_sec_int_integration〕에서 , Tenable.sc, 및 Tenable.cs에 대해 Tenable.ioVI에 증명 포함 키 열 값을 true로 설정합니다.
2. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 **VI** 세분성 구성.
3. 제품의 경우 Tenable.cs탐지 키 구성 〔sn_vul_detection_key_config〕 테이블로 이동하여 기록을 선택하고 Tenable.cs 업데이트합니다.
4. 포트 포함 양식에서 포트 포함 확인란을 선택하고 여기를 클릭 링크(Tenable.io 및 Tenable.sc 에만 적용됨)를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. VI 키에 증명 추가 목록에서 새로 만들기를 선택합니다.

6. VI 키에 증명 추가 - 새 기록 양식의 취약성 필드에서 증명을 포함할 Tenable ID를 추가합니다.

> **주:**
> 경로 정보만을 기준으로 탐지를 분할하거나 경로와 버전 상세 정보를 결합하여 분할할 수 있습니다. 자세한 내용은 이 페이지의 'Tenable 스캐너에서 탐지 분할' 섹션을 참조하십시오.

7. Tenable VIT를 분할하는 정규 표현식 필드에서 다음을 수행합니다.

- Path\s+:\s+([A\n]+)를 입력하여 경로만을 기준으로 탐지를 분할합니다.
- Path\s+:\s+([A\n]+)\n\s+Installed\s+version\s+:\s+([A\n]+)\n\s+Fixed\s+version\s+:\s+([A\n]+)을 입력하여 경로와 설치 및 수정된 버전을 기준으로 탐지를 분할합니다.

8. 제출을 선택합니다.

Example: Tenable 스캐너에서 탐지 분할

Tenable 스캐너에서 다음과 같은 탐지는 경로 및 버전 정보를 모두 포함하는 출력 태그에 증거를 표시합니다.


```
    "results":

            "asset":
                "agent_uuid": *92124caabdb9459baa9d053186df48b9",
               "bios_uuid": "ec2cbbfd-dc9e-efbf-acdd-485daZe8c7df"
               "device_ type": "aws-ec2-instance",
                "fqdn": "ip-ac0a0004. secops.com",
                "hostname": "ip-ac0a0004",
        "uuid": "486acb3b-674f-477a-bc37-660a7bba37b3",
                "ipv4": "18.220.145.158",
                "last_authenticated_results": "2024-05-17T03:34:04.424Z",

                "mac_address": "0a:3e:8b:ed:63:e6",
               "netbios name": "IP-AC0A0094".
               "operating_system": [
                    "Microsoft Windows Server 2019 Datacenter Build 17763"


                "network_id": "00000000-0000-0000-0000-000000000008",

               "tracked": true


            "output": "In                          C: 11 Program Files (x86) \ \Common
Files\\0racle\\Java\\javapath_target_119044062511\n Installed version : 1.8.0_361.9\n Fixed
version
                                                                                Path
            "plugin":
                "bid":
                    123456


                "checks_for_default_account": false,
               "checks_for malware": false,
```


기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
                "coe":
              "cpe:/a:notepad-plus-plus:notepad%5c%2b15ck2b"


               "cvSs3_base_score": 7.8,
              "cvss3 temporal score": 7.0,

              "cvss3_temporal_vector": {
                    "exploitability": "Proof-of-Concept",
                    "remediation level": "Official Fix",
                     "report_confidence": "Confirmed",
                     "raw": "E: P/RL:0/RC: C"
```


Atlassian Jira 와의 통합 이해취약성 대응

Atlassian Jira 와의 취약성 대응 통합을 통해 다양한 문제 추적 및 Agile 관리 도구를 활용하여 취약성 정정 작업을 추적할 수 있습니다.

스토어에서 앱 요청

ServiceNow Store 웹 사이트를 방문하면 사용 가능한 모든 앱을 확인하고 스토어에 요청을 제출하는 방법에 대한 정보를 참조할 수 있습니다. 출시된 모든 앱의 누적 릴리스 정보는 ServiceNow Store 버전 기록 릴리스 정보 를 참조하십시오.

개요

ServiceNow# 취약성 대응 와 Atlassian Jira 통합되어 취약성에 해당하는 문제를 생성하고 문제의 Jira 엔터티와 취약성 항목 엔터티 취약성 대응 를 양방향으로 동기화하여 최신 업데이트를 반영합니다. 취약성 관리자는 에 존재하는 ServiceNow 취약성 대응 취약성 항목을 생성하여 정정 사용자(의 경우 애플리케이션 취약성 대응개발자)에게 기본 기록 시스템 및 문제 관리 도구(예: Atlassian Jira)에 할당해야 합니다. 취약성 관리자가 볼 수 있도록 문제 관리 도구의 취약성에 대해 수행된 모든 진행 상황을 업데이트해야 ServiceNow 취약성 대응 합니다. 또한 취약성 관리자가 취약성 대응 취약성 항목에 대해 수행한 모든 업데이트도 정정 사용자에게 표시되도록 문제 관리 도구에 전달되어야 합니다.

사용 가능한 버전

릴리스 버전	릴리스 정보
취약성 대응	Vulnerability Response Integration 릴리스 정보
컨테이너에 대한 취약성 대응 및 구성 준수	Container Vulnerability Response 릴리스 정보
Jira 스포크	Jira 스포크 릴리스 정보

Jira 취약성 통합

취약성 통합을 보려면 Jira 다음으로 이동하십시오. 모두 〉 VR용 **Agile** 관리 〉 **Agile** 도구 구성 .

기본 시스템에는 다음과 같은 통합이 포함됩니다. 이러한 통합은 기본적으로 모두 활성화되어 있지는 않습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

초기 실행 후에는 매일 예약된 작업이 연결되어 통합을 순서대로 자동으로 실행합니다. 예약된 개별 작업을 수동으로 실행할 수도 있습니다. 예약된 작업은 인스턴스를 다른 취약성 관리 시스템과 동기화된 상태로 유지하여 취약성 정정 수명주기를 단순화합니다.

통합 준비 **Jira** 취약성 대응

취약성을 성공적으로 Jira 통합하려면 통합 전 작업을 계획하고 실행해야 합니다. 다음 작업을 수행하여 통합을 준비합니다. 통합에서는 Jira 취약성 대응 사용자가 제품 및 API에 Jira 익숙하다고 가정합니다.

Agile Integration for 및 **Jira Integration for** 취약성 대응 **Vulnerability** Response와 함께 설치되는 구성요소

Agile Integration for Vulnerability Response 및 Jira Integration for Vulnerability Response 플러그인을 활성화하면 테이블 및 사용자 역할을 비롯한 여러 유형의 구성요소가 설치됩니다.

설치되는 역할

역할 이름 **[name]**	설명
Agile 도구 관리자〔sn_vul_agile.agile_tool_admin〕	Agile Management에 대한 구성 규칙을 생성하여 문제를 생성하거나 업데이트할 수 있습니다. 애자일 관리를 위한 규칙 구성을 생성합니다.
JIRA 관리자〔sn_vul_jira.admin〕	Agile 도구를 선택하여 선택한 엔터티 테이블에 대한 문제를 생성할 수 있습니다.

설치되는 테이블

테이블	설명
Agile 도구 구성〔sn_vul_agile_tool_rule_config〕	Agile 플랫폼에서 문제를 생성하는 구성 규칙을 포함합니다.
Agile 도구 필드 매핑〔sn_vul_agile_tool_field_mapping〕	구성 규칙의 필드 매핑을 포함합니다.
Agile 도구 상태 매핑〔sn_vul_agile_tool_state_mapping〕	애플리케이션 취약한 항목, 컨테이너 취약한 항목, 애플리케이션 정정 작업 및 컨테이너 정정 작업 상태와 Jira 문제 상태의 상태 매핑을 포함합니다.
Agile 도구 매니페스트〔sn_vul_agile_tool_manifest〕	문제 생성을 위한 페이로드를 포함합니다.
Agile 도구 데이터 자원〔sn_vul_agile_tool_data_resource〕	생성된 Jira 문제에 대한 정보를 포함합니다.
JIRA 관리자〔sn_vul_jira.admin〕	Agile 도구를 선택하여 선택한 엔터티 테이블에

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설치되는 테이블

테이블	설명
	대한 문제를 생성할 수 있습니다.

와 **Vulnerability Response** 통합 설치 **Jira**

인스턴스에서 통합을 실행하기 전에 설치 및 구성 단계를 완료 Jira 하여 제품이 .애플리케이션 취약성 대응 이 애플리케이션은 별도의 구독으로 사용할 수 있습니다.

시작하기 전에
필요한 역할: admin.
설치하기 전에 다음 설정 검사 목록을 완료합니다. 이러한 설정 작업은 원활한 설치 및 구성을 위해 필요합니다.

주:
이 프로세스는 프로덕션 인스턴스에 다운로드된 애플리케이션에만 적용됩니다. 애플리케이션을 비프로덕션 또는 개발 인스턴스에 다운로드하는 경우에는 권리를 얻을 필요가 없습니다. 로 애플리케이션 활성화 ServiceNow Store계속 진행합니다.

작업 설정	설명
Vulnerability Response 애플리케이션이 설치되고 활성화되었는지 확인합니다.	• Jira Integration for Vulnerability Response에는 Vulnerability Response 애플리케이션이 필요합니다. • Jira Integration for Vulnerability Response의 최신 버전을 사용하려면 최신 버전의 Vulnerability Response가 설치되어 있는지 확인하십시오. KB0856498 취약성 대응 호환성 매트릭스 및 릴리스 스키마 변경 사항을 참조하십시오. • 애플리케이션이 설치 및 활성화되지 않은 경우 Vulnerability Response 설치를 참조하십시오.
통합 허브 플러그인이 설치되어 있는지 확인합니다.	• Jira 스포크에는 Integration Hub가 필요합니다. • 통합 허브 설치에 대한 KB1112383 참조하십시오. • 자세한 내용은 법무 일정-통합 허브 개요를 참조하십시오.
최신 Jira Spoke 버전이 설치되어 있는지 확인합니다.	Jira 스포크 설치에 대한 KB0792632 참조하십시오.
Agile Management와 취약성 대응 통합이 설치되었는지 확인하십시오.	Atlassian Jira와 취약성 대응 통합에는 이 통합이 필요합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 통합을 설치할 Jira 취약성 대응 인스턴스에 로그인합니다.
2. ServiceNow Store로 이동합니다.
3. 에서 ServiceNow Store애플리케이션과의 Jira 통합을 검색합니다취약성 대응.
4. 애플리케이션 타일을 클릭합니다.
   설치 중인 애플리케이션에 대한 자세한 정보가 표시됩니다.

   주:
   해당하는 경우 다른 요구 사항 및 종속성 섹션을 읽어보십시오.

5. 앱 요청을 클릭하고 Now Support 로그인 자격 증명을 입력합니다.
6. 가져오기를 클릭합니다.
7. 인스턴스 이름 및 인스턴스 이유를 입력하고 인스턴스 확인을 클릭합니다.
8. 요청을 클릭합니다.
   자세한 설치 지침이 포함된 이메일을 받게 됩니다.
9. 다음으로 이동 시스템 애플리케이션 〉 애플리케이션.
10. 애플리케이션을 찾아서 선택한 다음 설치를 클릭합니다.
    애플리케이션이 인스턴스에 자동으로 설치됩니다.

Agile 도구 구성에서 규칙 구성

Jira 애플리케이션 취약한 항목, 컨테이너 취약한 항목, 애플리케이션 정정 작업 및 컨테이너 정정 작업에서 생성된 기록이 Agile 도구 구성에서 생성된 규칙과 일치하면 플랫폼에서 문제가 생성됩니다 Jira .

시작하기 전에
필요한 역할: sn_vul.app_read_all, sn_vul_container.read_all, sn_vul_agile.agile_tool_admin 또는 sn_vul_jira.admin.

프로시저

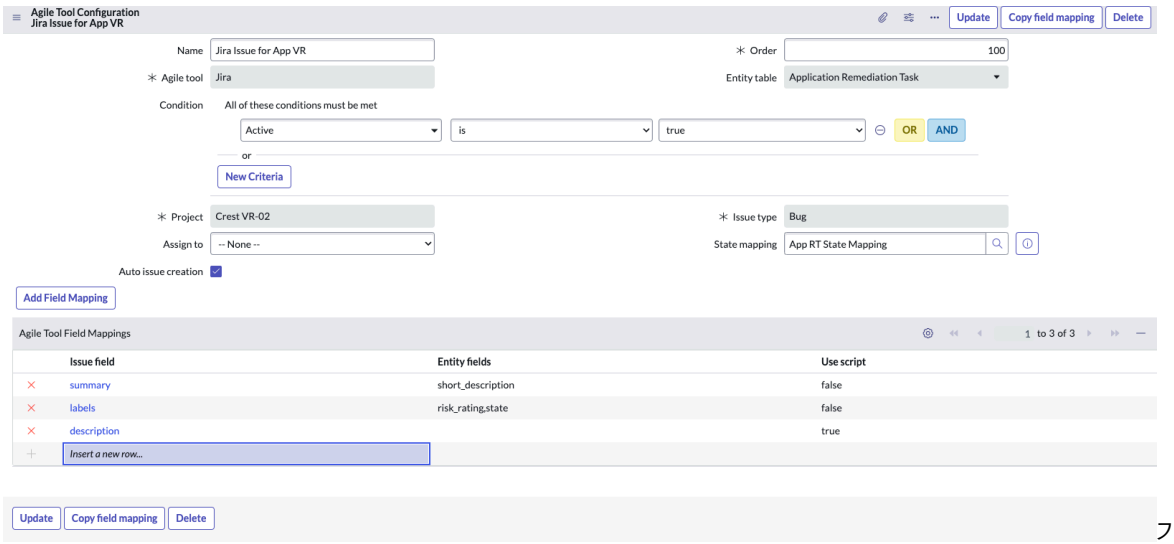
1. 다음으로 이동 모두 〉 VR용 **Agile** 관리 〉 **Agile** 도구 구성.
2. Agile 도구 구성에서 새 구성 규칙을 만들려면 새로 만들기를 선택합니다.
3. 양식에서 필드를 채웁니다.

Agile 도구 구성 양식

필드	설명
이름	Agile 도구 구성의 이름입니다.
순서	Agile 도구 구성의 순서입니다.
Agile 도구	특정 Agile 플랫폼에서 문제를 생성하는 Agile 도구입니다.
엔터티 테이블	구성 규칙을 적용할 테이블입니다.
조건	선택한 엔터티 테이블에서 조건을 필터링하여 Agile 플랫폼에서 문제를 생성합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
자동 문제 생성	선택한 엔터티 테이블에 새 기록이 생성될 때 확인란을 선택한 경우에만 구성 규칙을 쿼리합니다. 주: 사용자는 목록 작업을 사용하여 기존 엔터티 기록에 대한 문제를 생성해야 합니다.
프로젝트	Jira 문제가 생성될 프로젝트입니다.
이슈 유형	특정 프로젝트에서 만들 문제의 유형입니다.
담당자	문제 생성 시 문제를 할당해야 하는 담당자입니다. 생성된 문제를 할당되지 않은 상태로 유지하려면 "없음"을 선택합니다.
상태 매핑	Agile 도구 상태 매핑 테이블의 기존 상태 매핑 또는 Agile Platform의 문제 상태와 엔터티 테이블 상태 간에 새 상태 매핑을 ServiceNow 생성합니다.



기본적으로 애플리케이션이 설치되면 애플리케이션 정정 작업과 컨테이너 정정 작업이 Agile 도구 구성 양식의 엔터티 테이블 필드에 표시됩니다.

4. 엔터티 테이블 선택 목록에 애플리케이션 취약한 항목 및 컨테이너 취약한 항목을 추가하려면 시스템 속성**> sn_vul_agile.tablesToShow** 로 이동하여 값 필드에 모두 추가합니다.

시스템 속성 양식

필드	설명
선택	선택 목록을 표시하는 쉼표로 구분된 값입니다.
값	속성에 대해 원하는 값을 설정합니다. 모든 속성 값은 문자열로 저장됩니다. gs.getProperty() 메서드를 통해 속성을 검색할 때 결과를 문자열로 처리합니다. 예를 들어, True|False 속성은 부울값이 아닌 'True' 또는 'False'(문자열)를 반환합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. 기존 상태 매핑 기록을 선택하거나 Agile 도구 상태 매핑에서 새 상태 매핑을 생성합니다.

Agile 도구 상태 매핑 양식

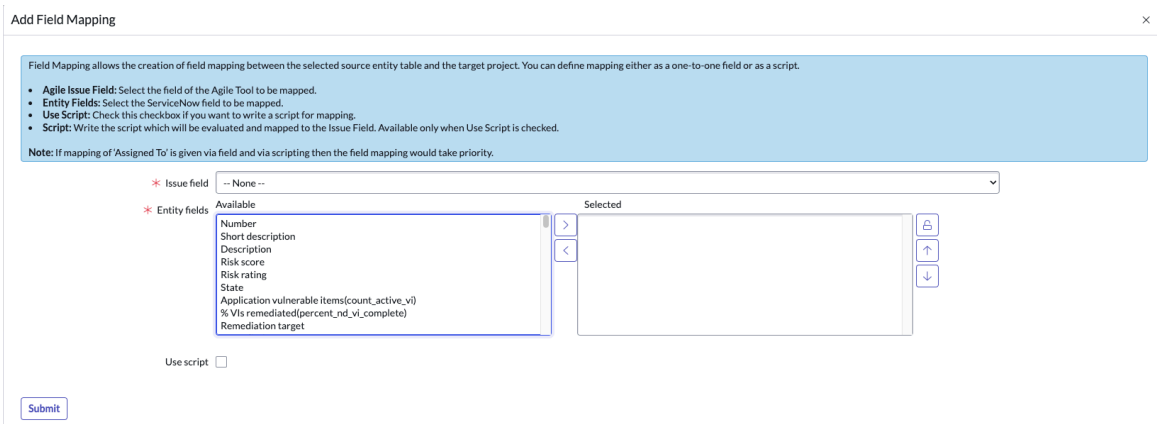
필드	설명
이름	상태 매핑의 고유 이름을 삽입합니다.
Agile 도구	Agile 도구를 선택합니다.
엔터티 테이블	상태 매핑을 생성할 소스 테이블을 선택합니다.
프로젝트	상태가 매핑될 프로젝트를 선택합니다.
ServiceNow 엔터티 상태	Agile 도구 상태와 매핑할 상태를 선택합니다.
Agile 도구 상태	취약한 항목 상태에서 매핑하려는 상태를 선택합니다.

6. 프로젝트 저장 및 가져오기를 클릭하여 프로젝트 필드 구성 규칙에서 프로젝트를 가져오고 Agile 도구의 자격 증명을 확인합니다.

> **팁:**
> 시스템 속성 **projectsPageSize** 를 설정하여 페이지당 특정 수의 프로젝트를 가져올 수 있습니다.

7. 시스템 속성**> sn_vul_jira.projectsPageSize**로 이동하여 Jira Cloud의 값 필드에 페이지당 가져올 프로젝트 수를 추가합니다.
8. 프로젝트를 가져온 후 구성 규칙에서 프로젝트, 문제 유형 및 할당 대상을 선택합니다.

   기본 필드 매핑은 포함된 Agile 도구 필드 매핑 목록에 채워집니다. 기본적으로 문제의 요약 및 설명 필드가 매핑됩니다.
9. 다른 문제 필드를 필드와 ServiceNow 매핑하려면 필드 매핑 추가를 클릭합니다.



> **주:**
> - 문자열 및 선택 유형 필드만 매핑해야 합니다.
> - Agile 도구의 모든 필수 문제 필드가 엔터티 필드와 올바르게 매핑되어 있는지 확인합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Agile 도구 상태 매핑 양식

필드	설명
문제 필드	구성 규칙에서 현재 선택된 프로젝트의 문제 필드와 문제 유형을 포함합니다.
엔터티 필드	구성 규칙에서 선택한 엔터티 테이블의 필드를 포함합니다.
스크립트 사용	문제 필드를 엔터티 필드와 매핑하는 데 스크립트를 사용하려면 선택합니다.
스크립트	문제 필드를 엔터티 필드와 매핑하는 스크립트입니다.

10. Glide 모달에서 제출 을 클릭하여 Agile 도구 필드 매핑 테이블에 필드 매핑 기록을 제출합니다.

    주:
    필수 필드를 매핑하지 않으면 해당 구성 규칙에 대한 문제가 생성되지 않습니다.

    필수 필드는 Agile 도구 구성 양식의 상단에 표시됩니다.
    특정 구성 규칙에 대한 모든 필드 매핑은 Agile 도구 구성 테이블에 있는 Agile 도구 필드 매핑 테이블의 포함된 목록에 표시됩니다.

11. 헤더를 마우스 오른쪽 버튼으로 클릭하여 변경 내용을 저장합니다.
    저장된 기록은 Agile 도구 구성 테이블에 표시됩니다. 애플리케이션 취약한 항목, 컨테이너 취약한 항목, 애플리케이션 정정 작업 및 컨테이너 정정 작업에서 생성된 기록이 임의의 구성 규칙과 일치하면 구성 규칙의 매핑에 따라 기록에 대한 문제가 생성됩니다.

12. 시스템 속성**> sn_vul_jira.cloudBulkSize**로 이동하고 값 필드에 배치당 생성할 문제 수를 설정합니다.

    주:
    Jira Cloud에서 일괄 처리당 생성할 수 있는 최대 문제 수는 50개입니다.

    Jira 서버에서 문제를 생성하기 위한 배치 크기를 설정할 수 있습니다.

13. 시스템 속성**> sn_vul_jira.onPremBulkIssue**로 이동하여 값 필드에 배치당 생성할 문제 수를 설정합니다.
    시스템 속성의 값 필드에서 오류 수를 설정하여 매니페스트 테이블의 기록을 처리하여 특정 오류 수까지 Jira 문제를 생성할 수도 있습니다.

14. 시스템 속성 〉 sn_vul_agile로 이동합니다**. ManifestErrorCount**를 호출하고 오류가 있는 매니페스트를 처리해야 하는 최대 횟수를 설정합니다.

목록 작업을 사용하여 수동으로 **Agile** 문제 생성

목록 작업: Jira 문제 생성이 트리거되면 규칙 구성 기준과 일치하는 기록은 "Jira 문제 생성"에 고려되어야 하며, 이러한 기록은 구성 규칙에서 매핑이 선택된 sn_vul_agile_tool_manifest 테이블로 수집되어야 합니다.

시작하기 전에
필요한 역할: sn_vul_agile.agile_tool_admin 또는 sn_vul_jira.admin, sn_vul.app_read_all, sn_vul_container.read_all.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 작업 공간 〉 취약성 관리자 작업 공간 〉 목록 〉 정정 작업/애플리케이션 취약한 항목/컨테이너 취약한 항목.
2. 여러 기록을 선택하여 Jira 문제를 생성하고 **Jira** 문제 생성을 클릭합니다.
   선택한 기록은 연결된 Agile 도구의 필드 매핑 및 상태 매핑을 고려해야 합니다.
   구성 규칙 조건을 충족하는 선택한 기록은 Jira 문제를 생성할 수 있어야 하며 해당 기록을 테이블에 추가해야 *sn_vul_agile_tool_manifest* 합니다.

양식 작업을 사용하여 수동으로 **Agile** 문제 생성

양식 작업을 사용하여 Agile 문제를 수동으로 생성합니다. 기록이 구성 규칙 조건과 일치하면 구성 규칙에서 선택한 값으로 팝업 상자가 채워지고 기준과 일치하지 않으면 사용자가 미리 정의된 필드의 값을 선택할 수 있습니다.

시작하기 전에
Agile 도구의 모든 필수 문제 필드가 엔터티 필드와 올바르게 매핑되었는지 확인합니다.

필요한 역할: sn_vul_agile.agile_tool_admin 또는 sn_vul_jira.admin, sn_vul.app_read_all sn_vul_container.read_all.

프로시저

1. 다음으로 이동 모두 〉 작업 공간 〉 취약성 관리자 작업 공간 〉 목록 〉 정정 작업/애플리케이션 취약한 항목/컨테이너 취약한 항목.
2. 기록을 선택하여 Agile 문제를 수동으로 생성합니다.
3. **Agile** 문제 생성을 선택합니다.
4. 언급된 필드에 유효한 상세 정보를 삽입합니다.

   기록이 구성 규칙의 조건을 충족하는 경우, 아래 필드를 구성된 값으로 채워야 하며 사용자가 필드 값을 수정할 수 있습니다.

필드	설명
프로젝트	Jira 문제를 생성할 프로젝트를 선택합니다.
이슈 유형	특정 프로젝트에서 만들 문제 유형을 선택합니다.
담당자	문제 생성 시 문제를 할당할 담당자를 선택합니다.
필드 매핑	Agile 도구의 문제 유형 필드를 선택하고 선택한 필드에 대한 직접 값을 삽입합니다.

5. **Agile** 문제 생성을 선택하여 기록을 제출합니다.
   기록을 제출하면 테이블에 기록 항목이 생성됩니다sn_vul_agile_tool_manifest

문제 상태를 **Jira** 수동으로 동기화

양식 컨텍스트 메뉴의 **Agile** 상태 동기화 버튼을 클릭하여 단일 기록의 상태를 업데이트하고, 취약성 관리자 작업 공간에서 애플리케이션 취약한 항목, 컨테이너 취약한 항목 및 정정 작업 테이블의 **Agile** 상태 동기화 목록 작업을 클릭하여 여러 기록의 상태를 업데이트합니다.

시작하기 전에
필요한 역할: sn_vul_agile.agile_tool_admin 또는 sn_vul_jira.admin, sn_vul.app_read_all sn_vul_container.read_all.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보

엔터티 상태가 종결 ServiceNow 되거나 엔터티가 다시 열리면(즉, 상태가 열림) 상태는 Agile 도구에서 ServiceNow Agile 도구로 동기화됩니다. 다른 모든 상태는 Agile 도구 ServiceNow에서 . 사용자는 연결된 구성된 규칙에 상태 매핑이 없는 기록이나 양식 작업에서 직접 생성된 문제에 대한 상태를 동기화할 수 없습니다.

프로시저

1. 다음으로 이동 모두 〉 작업 공간 〉 취약성 관리자 작업 공간 〉 목록 〉 정정 작업/애플리케이션 취약한 항목/컨테이너 취약한 항목.
2. 여러 기록을 선택하여 Jira 문제를 생성하고 **Agile** 상태 동기화를 클릭합니다.
   문제가 이미 생성된 기록의 상태는 기록이 종결 상태가 아니고 구성 규칙에서 선택한 기록에 대한 상태 매핑이 있는 경우 업데이트됩니다.
3. 다음 조건이 충족되는 경우 기록을 열면 **Agile** 동기화 상태가 양식 컨텍스트 메뉴에 표시됩니다.
   - 기록에 대한 문제가 생성되고 기록이 종결 상태가 아닙니다.
   - 기록에 대한 상태 매핑이 있음
4. **Agile** 상태 동기화를 클릭하여 Agile 상태를 매핑된 상태와 동기화합니다.
   시스템 속성을 설정하여 Jira에서 문제 상태를 가져오기 위한 배치 크기를 설정할 수 있습니다.
5. 다음으로 이동 시스템 속성 **> sn_vul_jira.bulkIssueStatusSize**.
   - Jira 서버의 경우 반환할 최대 문제 수입니다(기본값 50). 최대 허용 값은 Jira 속성 'jira.search.views.default.max'에 의해 결정됩니다. 이 숫자보다 큰 값을 지정하면 검색 결과가 잘립니다.
   - 양식 작업에서 문제가 생성되었거나 구성된 규칙에 상태 매핑이 없는 경우 이러한 기록은 상태 동기화에 고려되지 않습니다.

문제를 자동으로 생성하도록 스케줄러 구성

스케줄러가 실행되고 sn_vul_agile_tool_manifest 테이블에 생성된 기록에 대한 문제를 자동으로 생성 Jira 하도록 구성합니다.

시작하기 전에

필요한 역할: admin 또는 schedule_admin.

이 태스크 정보

sn_vul_agile_manifest 테이블에서 생성된 애플리케이션 취약한 항목, 컨테이너 취약한 항목, 애플리케이션 정정 작업 및 컨테이너 정정에 대한 모든 기록은 문제 생성 대상으로 Jira 간주됩니다.

프로시저

1. 다음으로 이동 모두 〉 시스템 정의 〉 예약된 작업 〉 **Jira** 문제 생성.
2. 예약된 스크립트에서 실행, 시간대 및 시간 필드를 수정할 수 있습니다.

예약된 스크립트 실행 양식

필드	설명
실행	예약된 작업을 실행하는 데 사용할 시간 간격: ○ 매일 - 지정된 시간에 매일 실행됩니다. ○ 매주 - 지정된 시간과 요일에 매주 실행됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	○ 매달 - 매월 지정된 시간과 요일에 실행됩니다. ○ 주기적으로–지정된 반복 간격에서 실행됩니다. ○ 한 번 - 한 번만 실행됩니다. ○ 요청 시 - 요청 시 즉시 실행됩니다. ○ 비즈니스 달력: 항목 시작 – 필드에서 선택한 비즈니스 달력의 시작 항목 날짜에 실행됩니다. 예약된 작업은 비즈니스 달력에 정의한 각 비즈니스 항목의 시작 날짜에 실행됩니다. 예를 들어, 비즈니스 달력이 회계 연도를 나타내고 각 항목의 시작 날짜가 회계 월인 경우 예약된 작업은 매월 첫 번째 날에 실행됩니다. ○ 비즈니스 달력: 입력 종료 – 필드에서 선택한 비즈니스 달력의 종료 날짜에 실행됩니다. 이 선택은 연결된 비즈니스 달력 항목의 종료 날짜에 실행된다는 것을 제외하고는 비즈니스 달력: 항목 시작과 같은 방식으로 실행됩니다. **주:** 비즈니스 달력: 항목 시작 또는 비즈니스 달력: 항목 종료를 선택하면 오프셋 요소를 적용하여 작업이 선택한 비즈니스 달력 시간 범위의 전 또는 후에 실행되도록 작업을 예약할 수 있습니다. 자세한 내용은 오프셋 유형(Offset Type) 및 오프셋(Offset) 필드를 참조하십시오. 비즈니스 달력 생성 및 사용과 비즈니스 달력 항목 정의에 대한 자세한 내용은 을 Define business calendar entries 참조하십시오Create a business calendar .
일	예약된 작업이 실행되어야 하는 날입니다. ○ 실행이 매주로 설정되어 있는 경우 주의 어느 한 요일을 선택합니다. 예를 들어 수요일을 선택합니다. ○ 실행이 월간으로 설정되어 있는 경우 달의 어느 한 날을 선택합니다. 예를 들어, 그 달의 25일인 경우 25를 선택합니다. 이 필드는 실행 필드에서 매월 또는 매주를 선택하는 경우에만 나타납니다.
반복 간격	예약된 작업이 매번 실행되는 반복 간격의 기간입니다. 기간을 일, 시간 또는 분 단위의 숫자로 입력합니다. 예:

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	○ 예약된 작업이 4일마다 실행되도록 하려면 일 필드에 04를 입력합니다. ○ 예약된 작업이 26시간마다 실행되도록 하려면 시간 필드에 26을 입력합니다. ○ 13시간 30분 25초 간격으로 작업을 반복해야 하는 경우 시간 필드에 13을 입력한 다음 그 뒤에 레이블이 지정되지 않은 2개의 필드에 30과 25를 입력합니다.
시간	예약된 작업이 실행되어야 하는 날의 시간으로 시간, 분 및 초(24시간제 형식)로 표현됩니다. 시간대 필드에서 선택하는 항목에 따라 이 항목의 시간대가 결정됩니다.
시간대	예약된 작업이 실행되는 시간을 지정할 때 시간 필드 항목에 사용할 시간대입니다. 시간대 항목 선택: ○ 없음: 로그인하여 예약된 작업을 작성하는 사용자에 대해 기본 시간대를 사용합니다. 예를 들어 미국/태평양 표준시가 사용자의 할당 시간대이고 시간 필드에 16:45를 입력하는 경우 예약된 작업은 미국/태평양 표준시 오후 04:45에 실행됩니다. ○ 시스템 시간대 사용: 예약된 작업이 실행되는 인스턴스에 지정된 기본 시스템 시간대를 사용합니다. 예를 들어 유럽/런던 표준시가 인스턴스의 기본 시스템 시간대이고 시간 필드에 22:15를 입력하는 경우 예약된 작업은 런던 표준시 오후 10:15에 실행됩니다. ○ 실제 시간대 ○ 예를 들어 미국/동부를 선택하고 시간 필드에 13:30을 입력하면 예약된 작업은 미국 동부 표준시 오후 1:30에 실행됩니다.
run_as	기본적으로 run_ 필드 값은 비워 두어야 합니다. 사용자는 값을 도메인 사용자 값으로 설정하여 특정 도메인에 대한 문제를 생성할 수 있습니다.

문제를 자동으로 업데이트하도록 스케줄러 구성

sn_vul_agile_tool_manifest 테이블에 추가된 기록에 대해 문제를 자동으로 업데이트 Jira 하도록 스케줄러를 구성합니다.

시작하기 전에
필요한 역할: admin 또는 schedule_admin.

이 태스크 정보
sn_vul_agile_manifest 테이블에서 생성된 애플리케이션 취약한 항목, 컨테이너 취약한 항목, 애플리케이션 정정 작업 및 컨테이너 정정의 모든 기록은 문제 업데이트 대상으로 Jira 간주됩니다. 기록이 종결되고 의견이 추가되면 해당 값도 관련 Jira 문제로 업데이트됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

- 선택한 Agile 문제 프로젝트의 워크플로우가 사용자가 다른 상태에서 상태를 직접 변경하지 못하도록 제한하는 경우 "문제 업데이트" 예약된 작업은 상태를 업데이트 Jira 하지 않습니다.
- 추가 설명이 있는 엔터티 기록을 닫으면 업데이트 시 마지막 설명만 고려되고 다음 업데이트에서는 모든 설명이 연결된 Jira.

프로시저

1. 다음으로 이동 모두 〉 시스템 정의 〉 예약된 작업 〉 **Jira** 문제 업데이트.
2. 예약된 스크립트에서 실행, 시간대 및 시간 필드를 수정할 수 있습니다.

예약된 스크립트 실행 양식

필드	설명
실행	예약된 작업을 실행하는 데 사용할 시간 간격: ○ 매일: 지정된 시간에 매일 실행됩니다. ○ 매주: 매주, 지정된 시간과 요일에 실행됩니다. ○ 매월: 매월, 지정된 시간과 요일에 실행됩니다. ○ 주기적으로: 지정된 반복 기간에 따라 실행됩니다. ○ 한 번: 한 번만 실행됩니다. ○ 요청 시: 요청 시 즉시 실행됩니다. ○ 비즈니스 달력: 항목 시작: 필드에서 선택한 비즈니스 달력 항목 시작 날짜에 실행됩니다. 예약된 작업은 비즈니스 달력에 정의한 각 비즈니스 항목의 시작 날짜에 실행됩니다. 예를 들어, 비즈니스 달력이 회계 연도를 나타내고 각 항목의 시작 날짜가 회계 월인 경우 예약된 작업은 매월 첫 번째 날에 실행됩니다. ○ 비즈니스 달력: 입력 종료: 필드에서 선택한 비즈니스 달력의 종료 날짜에 실행됩니다. 이 선택은 연결된 비즈니스 달력 항목의 종료 날짜에 실행된다는 것을 제외하고는 비즈니스 달력: 항목 시작과 같은 방식으로 실행됩니다. 주: 비즈니스 달력: 항목 시작 또는 비즈니스 달력: 항목 종료를 선택하면 오프셋 요소를 적용하여 작업이 선택한 비즈니스 달력 시간 범위의 전 또는 후에 실행되도록 작업을 예약할 수 있습니다. 자세한 내용은 오프셋 유형(Offset Type) 및 오프셋(Offset) 필드를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	비즈니스 달력 생성 및 사용과 비즈니스 달력 항목 정의에 대한 자세한 내용은 을 Create a business calendar Define business calendar entries 참조하십시오.
일	예약된 작업이 실행되어야 하는 날입니다. ○ 실행이 매주로 설정되어 있는 경우 주의 어느 한 요일을 선택합니다. 예를 들어 수요일을 선택합니다. ○ 실행이 월간으로 설정되어 있는 경우 달의 어느 한 날을 선택합니다. 예를 들어, 그 달의 25일인 경우 25를 선택합니다. 이 필드는 실행 필드에서 매월 또는 매주를 선택하는 경우에만 나타납니다.
반복 간격	예약된 작업이 매번 실행되는 반복 간격의 기간입니다. 기간을 일, 시간 또는 분 단위의 숫자로 입력합니다. 예: ○ 예약된 작업이 4일마다 실행되도록 하려면 일 필드에 04를 입력합니다. ○ 예약된 작업이 26시간마다 실행되도록 하려면 시간 필드에 26을 입력합니다. ○ 13시간 30분 25초 간격으로 작업을 반복해야 하는 경우 시간 필드에 13을 입력한 다음 그 뒤에 레이블이 지정되지 않은 2개의 필드에 30과 25를 입력합니다.
시간	예약된 작업이 실행되어야 하는 날의 시간으로 시간, 분 및 초(24시간제 형식)로 표현됩니다. 시간대 필드에서 선택하는 항목에 따라 이 항목의 시간대가 결정됩니다.
시간대	예약된 작업이 실행되는 시간을 지정할 때 시간 필드 항목에 사용할 시간대입니다. 시간대 항목 선택: ○ 없음: 로그인하여 예약된 작업을 작성하는 사용자에 대해 기본 시간대를 사용합니다. 예를 들어 예약된 작업은 오후 04:45에 실행됩니다. 미국/태평양 표준시 (사용자의 할당 시간대이고 시간 필드에 16:45를 입력하는 경우) ○ 시스템 시간대 사용: 예약된 작업이 실행되는 인스턴스에 지정된 기본 시스템 시간대를 사용합니다. 예를 들어 유럽/런던 표준시가 인스턴스의 기본 시스템 시간대이고 시간 필드에 22:15를 입력하는 경우 예약된 작업은 런던 표준시 오후 10:15에 실행됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	○ 실제 시간대 ○ 예를 들어, 미국/동부를 선택하고 시간 필드에 13:30을 입력하는 경우 예약된 작업은 미국 동부 표준시로 오후 1:30에 실행됩니다.
run_as	기본적으로 **run_** 형식 필드 값은 비어 있습니다. 도메인 사용자에 대한 값을 설정하여 특정 도메인에 대한 문제를 만들 수 있습니다.

상태를 **ServiceNow®** 자동으로 동기화 **Jira** 하도록 스케줄러 구성

문제 상태를 Jira 애플리케이션 취약성 항목, 컨테이너 취약성 항목 및 sn_vul_agile_manifest 테이블의 작업과 동기화하도록 스케줄러를 구성합니다.

시작하기 전에
필요한 역할: schedule_admin 또는 admin

이 태스크 정보
스케줄러는 구성된 일정에 따라 자동으로 실행됩니다. 에서 Jira 생성된 문제가 있는 애플리케이션 취약한 항목, 컨테이너 취약한 항목, 애플리케이션 정정 작업 및 컨테이너 정정 작업 테이블에 생성된 기록의 상태는 구성 규칙의 상태 매핑을 기반으로 플랫폼에서 문제의 Jira 현재 상태에 따라 업데이트됩니다.

sn_vul_agile_manifest 테이블에서 생성된 애플리케이션 취약한 항목, 컨테이너 취약한 항목, 애플리케이션 정정 작업 및 컨테이너 정정에 대한 모든 기록은 문제 생성에 Jira 고려됩니다.

프로시저

1. 다음으로 이동 모두 〉 시스템 정의 〉 예약된 작업 〉 동기화 상태.
2. 예약된 스크립트에서 실행, 시간대 및 시간 필드를 수정할 수 있습니다.

예약된 스크립트 실행 양식

필드	설명
실행	예약된 작업을 실행하는 데 사용할 시간 간격: ○ 매일: 지정된 시간에 매일 실행됩니다. ○ 매주: 매주, 지정된 시간과 요일에 실행됩니다. ○ 매월: 매월, 지정된 시간과 요일에 실행됩니다. ○ 주기적으로: 지정된 반복 기간에 따라 실행됩니다. ○ 한 번: 한 번만 실행됩니다. ○ 요청 시: 요청 시 즉시 실행됩니다. ○ 비즈니스 달력: 항목 시작: 필드에서 선택한 비즈니스 달력 항목 시작 날짜에 실행됩니다. 예약된 작업은 비즈니스 달력에 정의한 각 비즈니스 항목의 시작 날짜에 실행됩니다. 예를 들어, 비즈니스 달력이 회계 연도를

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	나타내고 각 항목의 시작 날짜가 회계 월인 경우 예약된 작업은 매월 첫 번째 날에 실행됩니다. ○ 비즈니스 달력: 입력 종료: 필드에서 선택한 비즈니스 달력의 종료 날짜에 실행됩니다. 이 선택은 연결된 비즈니스 달력 항목의 종료 날짜에 실행된다는 것을 제외하고는 비즈니스 달력: 항목 시작과 같은 방식으로 실행됩니다. **주:** 비즈니스 달력: 항목 시작 또는 비즈니스 달력: 항목 종료를 선택하면 오프셋 요소를 적용하여 작업이 선택한 비즈니스 달력 시간 범위의 전 또는 후에 실행되도록 작업을 예약할 수 있습니다. 자세한 내용은 오프셋 유형(Offset Type) 및 오프셋(Offset) 필드를 참조하십시오. 비즈니스 달력 생성 및 사용과 비즈니스 달력 항목 정의에 대한 자세한 내용은 을 Define business calendar entries 참조하십시오Create a business calendar .
일	예약된 작업이 실행되어야 하는 날입니다. ○ 실행이 매주로 설정되어 있는 경우 주의 어느 한 요일을 선택합니다. 예를 들어 수요일을 선택합니다. ○ 실행이 월간으로 설정되어 있는 경우 달의 어느 한 날을 선택합니다. 예를 들어, 그 달의 25일인 경우 25를 선택합니다. 이 필드는 실행 필드에서 매월 또는 매주를 선택하는 경우에만 나타납니다.
반복 간격	예약된 작업이 매번 실행되는 반복 간격의 기간입니다. 기간을 일, 시간 또는 분 단위의 숫자로 입력합니다. 예: ○ 예약된 작업이 4일마다 실행되도록 하려면 일 필드에 04를 입력합니다. ○ 예약된 작업이 26시간마다 실행되도록 하려면 시간 필드에 26을 입력합니다. ○ 13시간 30분 25초 간격으로 작업을 반복해야 하는 경우 시간 필드에 13을 입력한 다음 그 뒤에 레이블이 지정되지 않은 2개의 필드에 30과 25를 입력합니다.
시간	예약된 작업이 실행되어야 하는 날의 시간으로 시간, 분 및 초(24시간제 형식)로 표현됩니다. 시간대 필드에서 선택하는 항목에 따라 이 항목의 시간대가 결정됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
시간대	예약된 작업이 실행되는 시간을 지정할 때 시간 필드 항목에 사용할 시간대입니다. 시간대 항목 선택: ○ -없음-: 로그인하여 예약된 작업을 생성 중인 사용자에 대해서는 기본 시간대를 사용합니다. 예를 들어 미국/태평양 표준시가 사용자의 할당 시간대이고 시간 필드에 16:45를 입력하는 경우 예약된 작업은 미국/태평양 표준시 오후 04:45에 실행됩니다. ○ 시스템 시간대 사용: 예약된 작업이 실행되는 인스턴스에 지정된 기본 시스템 시간대를 사용합니다. 예를 들어 유럽/런던 표준시가 인스턴스의 기본 시스템 시간대이고 시간 필드에 22:15를 입력하는 경우 예약된 작업은 런던 표준시 오후 10:15에 실행됩니다. ○ 실제 시간대 ○ 예를 들어, 미국/동부를 선택하고 시간 필드에 13:30을 입력하는 경우 예약된 작업은 미국 동부 표준시로 오후 1:30에 실행됩니다.
run_as	기본적으로 run_ 형식 필드 값은 비어 있습니다. 값을 필수 도메인 사용자의 값으로 설정하여 특정 도메인에 대한 문제를 생성할 수 있습니다.

Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute 통합

Prisma Cloud Compute 통합을 사용하면 호스트를 스캔하여 취약성을 감지할 수 있습니다.

의 버전 24.02.0 취약성 대응부터 Prisma Cloud Compute 통합을 사용하여 실행 중인 호스트의 취약성을 임포트할 수 있습니다. Prisma Host API를 사용하면 특정 호스트에 대한 포괄적인 취약성 정보를 검색할 수 있으며 특정 시간에 호스트 취약성에 대한 스냅샷도 제공합니다. 이 API를 사용하면 Prisma와 ServiceNow 인스턴스 간에 정기적인 동기화가 가능합니다. Prisma는 SaaS(Software as a Service) 및 온프레미스 솔루션으로 제공되므로 ServiceNow 인스턴스에서 Prisma API를 호출하려면 MID 서버를 사용해야 합니다. 또한 제품과 ServiceNow AI Platform 인스턴스가 동일한 환경에 있지 않은 경우에도 Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute 사용해야 MID 서버 합니다. 자세한 내용은 MID 서버 시스템 요구 사항을 참조하십시오.

대시보드에서 취약성 및 취약한 항목에 대한 보고서를 볼 수도 있습니다 취약성 대응 . 그런 다음 이러한 취약성의 우선 순위를 지정하고 수정할 수 있습니다.

통합 보기

의 일부인 통합을 볼 수 있습니다 Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute. 통합을 보려면 다음으로 이동합니다. 모두 〉 **Prisma Cloud Compute** 통합 〉 통합.

다음과 같은 통합을 사용할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

실행 시퀀스	일정	통합	설명
1	매일	Prisma Cloud Compute Hosts 통합	호스트 취약성을 검색하고 호스트에 대한 VIT, 탐지 및 검색된 항목을 생성합니다.

주:
Container Vulnerability Response 플러그인이 설치된 경우 Container Vulnerability Response 관련 통합도 볼 수 있습니다.

Prisma 통합 프로세스

실행될 Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute 때 CVE(Common Vulnerability and Exposure)가 NVD(National Vulnerability Database) 테이블에 있는지 확인합니다. 이미 있는 경우 기존 정보가 사용됩니다. 그러나 CVE를 찾을 수 없는 경우 NVD 테이블에 자리 표시자 레코드가 생성됩니다. 이러한 자리 표시자 NVD 레코드를 만들 때는 처음에는 CVE와 해당 이름만 채워집니다. 다른 세부 정보는 NVD 통합이 나중에 이러한 세부 정보를 채운다는 가정하에 채워지지 않습니다. 통합 인스턴스 매개변수 *update_nvd* 가 true로 설정되면 자리 표시자 NVD 기록이 업데이트됩니다. 기본적으로 instance 매개변수는 false로 설정됩니다. 그러나 적어도 NVD 통합이 실행되고 이러한 세부 정보가 채워질 때까지는 심각도 또는 문제에 대한 몇 가지 기본 정보와 같은 CVE에 대한 이해가 필요합니다. 이 요구 사항을 충족하기 위해 익스플로잇 존재 및 정정 메모 필드가 Prisma에서 가져온 세부 정보로 채워집니다. 또한 이 구성은 사용자 지정이 가능하므로 Prisma에서 제공하는 정보를 기반으로 NVD 항목에 채우려는 다른 필드를 지정할 수 있습니다.

준비 중 **Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute**

설정 작업을 수행하여 준비할 Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute 수 있습니다.

시작하기 전에

애플리케이션을 설치하고 구성하려면 Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute 다음 검사 목록을 인쇄할 수 있습니다. 애플리케이션을 설치하고 취약성 데이터를 인스턴스로 ServiceNow AI Platform# 임포트하기 전에 나열된 항목이 완료되었는지 확인합니다.

통합 준비 검사 목록

작업	설명
☐	다음 정보 집합이 있는지 확인합니다. • API 기준 URL • 사용자 이름 및 암호. 이러한 자격 증명은 Prisma Cloud Compute 통합에서 취약성을 가져오는 데 사용됩니다. 자세한 내용은 https://pan.dev/compute/api/ 문서를 참조하십시오. 주: MID 서버 은 선택 사항입니다. Prisma Cloud Compute 통합에 사용되는 사용자 자격 증명에는 이미지를 모니터링할 수 있는 권한이 필요합니다. 다음 코드를 참조하십시오.

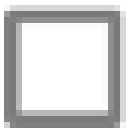
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

통합 준비 검사 목록

작업	설명
	{"permission":"monitorImages","saas":true,"self-hosted":true}
☐	아직 설치 및 활성화되지 않은 경우 타사 애플리케이션을 설치하기 전에 애플리케이션을 설치합니다 취약성 대응 . 애플리케이션 설치 및 활성화에 취약성 대응 대한 자세한 내용은 다음 문서를 참조하십시오 취약성 대응 설치. 이 통합에는 버전 16.1 취약성 대응 이상이 필요합니다.
☐	권리를 얻고 인스턴스에서 애플리케이션을 ServiceNow AI Platform# 다운로드합니다Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute.
☐	임포트할 것으로 예상되는 취약한 항목의 수를 예상합니다. 임포트하려는 취약한 항목 수를 인스턴스가 수락할 수 있는지 확인합니다. 인스턴스 크기가 작으면 로드 시간이 길어질 수 있습니다. 인스턴스 크기를 모르거나 도움이 필요한 경우 기술 지원에 문의하십시오 ServiceNow .
☐	통합을 관리하고 취약한 항목을 정정할 다음 그룹 또는 사용자가 있는지 확인합니다. 관리자 Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute 애플리케이션을 설치합니다. 할당되지 않은 경우 관리자는 컨테이너 취약성 관리자 (sn_vul_container.vulnerability_admin) 및 기타 역할을 할당합니다. sn_vul_container.vulnerability_admin Prisma Cloud Compute 통합 구성을 완료합니다. 이 역할은 (CVR) 애플리케이션 및 해당 기록에 컨테이너 취약성 대응 대한 전체 액세스 권한을 보유합니다. 이 관리자는 다음에서 컨테이너 취약성 대응통합 및 규칙을 구성합니다. 취약성 대응 그룹 기본적으로 취약성 대응 그룹을 사용할 수 있습니다. Vulnerability Response 그룹에 할당된 사용자는 sn_vul.read_all sn_vul_container.read_all을 상속합니다. 컨테이너 정정 소유자 그룹 기본적으로 컨테이너 정정 소유자 그룹을 사용할 수 있습니다. 이 그룹에 할당된 사용자는 sn_vul_container.remediation_owner를 상속합니다. 컨테이너 정정 소유자는 자신 또는 자신이 속한 그룹에 할당된 컨테이너 취약성을 정정합니다. 취약성 분석가 Container Vulnerability Analyst 그룹에 할당된 사용자는 sn_vul.vulnerability_analyst를 상속합니다. 취약성 분석가는 모든 취약한 항목의 정정을 모니터링합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

통합 준비 검사 목록

작업	설명
	아직 생성하지 않은 경우, 추가 그룹을 생성하고 인스턴스에서 사용자 관리 모듈을 사용하여 사용자를 추가하는 것이 좋습니다. 자세한 내용은 사용자 그룹 만들기를 참조하세요.
	취약성 대응 NVD와의 통합을 설치하고 NIST 국가 취약성 데이터베이스 통합 API(CVE만 해당)를 실행합니다.

준비가 되었습니다 Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute 애플리케이션 구성.

Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute 설치

인스턴스에서 통합을 실행하기 전에 설치 및 구성 단계를 완료하여 Prisma Cloud Compute 제품이 및 와 취약성 대응컨테이너 취약성 대응제대로 통합되도록 합니다. 이 애플리케이션은 별도의 구독으로 사용할 수 있습니다.

시작하기 전에
설치하기 전에 다음 설정 검사 목록을 완료합니다. 이러한 설정 작업은 원활한 설치 및 구성을 위해 필요합니다.

주:
이 프로세스는 프로덕션 인스턴스에 다운로드된 애플리케이션에만 적용됩니다. 애플리케이션을 비프로덕션 또는 개발 인스턴스에 다운로드하는 경우에는 권리를 얻을 필요가 없습니다. 로 애플리케이션 활성화 ServiceNow Store계속 진행합니다.

필요한 역할: 관리자

프로시저

1. 설치 Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute 하려는 인스턴스에 로그인합니다.
2. ServiceNow Store로 이동합니다.
3. 에서 ServiceNow Store애플리케이션을 검색합니다 Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute .
4. 애플리케이션 타일을 클릭합니다.
   설치 중인 애플리케이션에 대한 자세한 정보가 표시됩니다.

   주:
   필요한 경우 다른 요구 사항 및 종속성 섹션을 읽으십시오.

5. 앱 요청을 클릭하고 Now Support 로그인 자격 증명을 입력합니다.
6. 가져오기를 클릭합니다.
7. 인스턴스 이름 및 인스턴스 필드의 이유를 업데이트하고 인스턴스 확인을 클릭합니다.
8. 요청을 클릭합니다.
   자세한 설치 지침이 포함된 이메일을 받게 됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

9. 다음으로 이동 시스템 애플리케이션 〉 애플리케이션.
10. 애플리케이션을 찾아서 선택한 다음 설치를 클릭합니다.

결과
애플리케이션이 인스턴스에 자동으로 설치됩니다.

다음에 수행할 작업
사용자 환경에 맞게 구성합니다 Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute . Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute 애플리케이션 구성 문서를 참조하십시오.

Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute
애플리케이션 구성

Prisma Cloud Compute에서 Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute 데이터를 임포트하도록 애플리케이션을 설치하고 구성합니다. 임포트한 데이터를 사용하여 호스트의 취약성 우선순위를 지정하고 정정할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 통합에 대해 받은 이메일을 ServiceNow 엽니다.
2. 인스턴스에 관리자로 로그인합니다.
3. 이메일의 지침에 따라 .Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute
4. 다음으로 이동 모두 〉 **Prisma Cloud Compute** 통합 〉 관리 〉 구성.
   Prisma Cloud Compute 구성 양식에서 필드를 채웁니다. 자세한 내용은 Prisma Cloud Compute 구성 양식 문서를 참조하십시오.
5. 프로젝트 목록에서 모든 프로젝트 또는 특정 프로젝트를 선택하여 모든 프로젝트 또는 선택한 프로젝트를 각각 구성합니다.
   특정 프로젝트를 선택하면 사용 가능 목록에서 프로젝트를 선택할 수 있습니다.
6. 마침 또는 자격 증명 저장 및 테스트를 선택하여 구성을 완료합니다.
   - 프로젝트를 구성한 경우 마침을 선택합니다.
   - 프로젝트를 구성하지 않은 경우 자격 증명 저장 및 테스트를 선택합니다.
7. 새로 생성된 인스턴스를 보려면 다음으로 이동하십시오. **Prisma Cloud Compute** 통합 〉 관리 〉 통합 인스턴스.
8. 통합 인스턴스 매개변수를 선택하여 이전에 구성한 프로젝트를 봅니다.
9. 새로 생성된 통합 인스턴스를 실행하여 취약한 항목을 임포트합니다.
   VIT는 세분성에 따라 추가로 생성됩니다.
10. 취약한 항목의 세분성을 구성합니다.

    a. 다음으로 이동 **Prisma Cloud Compute** 통합 〉 이미지 취약성 키 구성

    b. 필요한 확인란을 선택하여 VIT의 세분성을 구성합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약한 항목은 다음 임포트 중에 선택한 키를 기반으로 생성됩니다.

주:
기본적으로 VIT는 이미지 리포지토리, 취약성 및 이미지 태그의 조합에 대해 생성됩니다. 추가 세분성을 위해 키에 구성요소를 추가할 수 있습니다. 예를 들어 이미지 리포지토리, 취약성, 이미지 태그 및 클러스터의 조합에 대해 CVIT를 생성할 수 있습니다. 취약한 항목 또는 취약한 항목 결과가 생성되면 확인란을 더 이상 편집할 수 없습니다.

Prisma Cloud Compute 통합에 대한 통합 실행 상태 차트

Prisma Cloud Compute 통합 실행 상태 모듈은 Prisma Cloud Compute 통합 실행 상태에 대한 그래픽 보기를 제공합니다.

차트에서 그래프의 특정 부분을 가리키면 해당 부분과 관련된 데이터 요약이 표시됩니다. 막대 그래프에서 부품을 클릭하면 더 자세한 정보를 제공하는 목록이 열립니다.

필요한 역할: 취약성 관리자

가상 사용자 및 세분화된 역할을 사용하여 사용자가 Vulnerability Response 애플리케이션에서 확인하고 수행할 수 있는 내용을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할을 처음 할당하려면 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당.

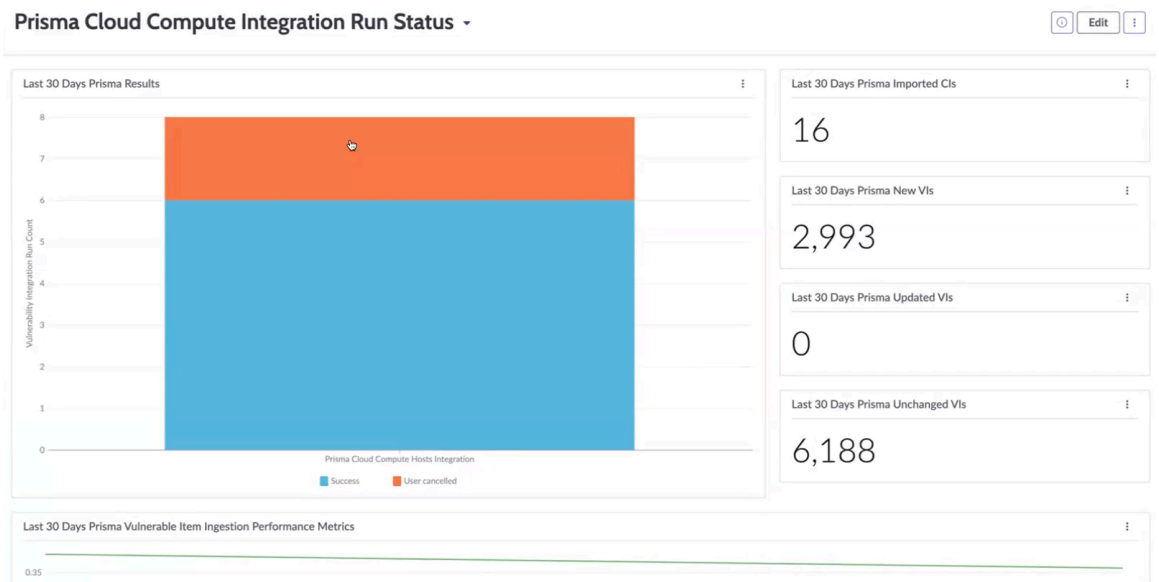
세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

데이터를 보려면 다음으로 이동합니다. 모두 〉 **Prisma Cloud Compute** 통합 〉 통합 실행 상태.

의 취약성 대응버전 19.0부터 이 대시보드는 New Experience UI에서 사용할 수 있습니다.

주:
Tokyo에 있는 경우 Next Experience UI에서 대시보드를 볼 수 있지만 일부 기능 손실이 있습니다.

실행 상태



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Prisma Cloud Compute 통합 실행 상태 차트 보고서

이름	설명
지난 30일 Prisma 결과	통합에 대해 완료된 통합 실행 수입니다. 성공한 실행과 실패한 실행을 모두 표시합니다. 각 실행은 그래프에 막대로 표시됩니다.
지난 30일 Prisma에서 임포트한 CI	지난 30일 동안 Prisma에서 임포트한 구성 항목(CI)의 수입니다. 정수로 표시됩니다.
지난 30일 Prisma 신규 VI	지난 30일 동안 임포트된 새로운 취약한 항목 수입니다. 정수로 표시됩니다.
지난 30일 Prisma 업데이트된 VI	지난 30일 동안 임포트된 업데이트된 취약한 항목(VI) 수입니다. 정수로 표시됩니다.
지난 30일 Prisma 변경 안 된 VI	지난 30일 동안 임포트된 중복 취약한 항목 수입니다. 정수로 표시됩니다.
지난 30일 Prisma 취약한 항목 수집 성과 메트릭	지난 30일 동안과 비교하여 취약한 항목에 대한 일일 성과 메트릭입니다.

Wiz 취약성 대응 통합 이해

취약성 및 규정 준수 데이터를 스캐너에서 Wiz AI Platform 인스턴스로 ServiceNow# 가져오면 클라우드 인프라 위험에 대한 심층적인 통계를 얻을 수 있습니다. 이러한 통합은 전반적인 클라우드 보안 태세에 대한 포괄적인 평가를 제공하고 인스턴스에서 직접 정정 작업을 실행하는 데 도움이 됩니다.

앱과의 통합에 취약성 대응 포함된 통합 Wiz

와의 취약성 대응Wiz 통합에는 취약성 및 규정 준수 데이터를 임포트하는 다음 통합이 포함됩니다.

- Wiz 호스트 취약성 통합
- Wiz 컨테이너 취약성 대응 통합
- Wiz 구성 준수 (테스트 결과) 통합 및 문제 통합

통합의 이점 및 사용자

혜택	Wiz 통합	사용자
호스트 취약성과 실행 중인 호스트의 취약성을 조기에 탐지한 사항을 임포트하고 평가합니다. 호스트 취약성 통합은 클라우드 환경의 가상 머신 및 서버리스 자산과 관련된 결과를 임포트합니다. 이러한 결과는 정정 워크플로우를 지원하기 위해 애플리케이션 내의 호스트 취약 항목(VIT)에 취약성 대응 매핑됩니다.	Wiz 호스트 취약성 통합.	취약성 관리자, 분석가 및 클라우드 보안 팀
클라우드 인프라에서 취약하고 규정을 준수하지 않는 자산에 대한 컨테이너 이미지 취약성 데이터를 임포트하고 평가합니다. 발견 사항은 컨테이너 취약 항목(CVIT)에 매핑되어 컨테이너 기반 워크로드에 대한 분류,	Wiz 컨테이너 취약성 통합.	취약성 관리자, 분석가 및 클라우드 보안 팀

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

혜택	Wiz 통합	사용자
위험 우선순위 지정 및 대상 정정 워크플로우를 지원합니다.		
에서 구성 테스트 결과를 Wiz 임포트하고 평가하여 미준수 클라우드 구성을 탐지합니다. 발견 사항은 애플리케이션의 클라우드 테스트 결과(CTR) 구성 준수 에 매핑되어 클라우드 환경 전체에 보안 정책과 표준을 적용하는 데 도움이 됩니다. 주: 다음의 Wiz 호스트 구성을 임포트하지 않습니다.	Wiz 구성 준수 통합 (Wiz 테스트 결과).	취약성 관리자, 분석가 및 클라우드 보안 팀
임포트 Wiz 취약성 및 잘못된 구성의 유해한 조합에 관련된 자산을 식별하는 문제입니다. 이러한 결과는 CTR에 매핑되고 Wiz Issues 레이블이 소스로 표시되어 복잡한 다중 벡터 위험을 초래할 수 있는 자산을 추적하고 해결하는 데 도움이 됩니다.	Wiz 문제 통합.	취약성 관리자, 분석가 및 클라우드 보안 팀
호스트 취약한 항목(VIT), 컨테이너 취약한 항목(CVT), 클라우드 테스트 결과(CTR) 및 ### 있는 레이블이 지정된 CTR 전반에 걸쳐 정정 단계를 적용합니다.	취약성 대응, 컨테이너 취약성 대응및 애플리케이션.구성 준수	정정 소유자

다음으로 살펴볼 내용

취약성 대응 통합을 사용하여 Wiz 임포트한 데이터를 설치, 구성 및 보는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- 통합 애플리케이션 활성화 Wiz 취약성 대응
- Wiz 취약성 대응 통합 구성
- 호스트 취약성 통합에 Wiz 대한 필터링 설정
- 컨테이너 취약성 통합에 Wiz 대한 필터링 설정
- 테스트 결과 통합에 Wiz 대한 필터링 설정
- 문제 통합에 Wiz 대한 필터링 설정
- 취약성 대응 통합을 위한 Wiz 필드 매핑

통합 애플리케이션 활성화 **Wiz** 취약성 대응

필요한 애플리케이션을 활성화합니다.

시작하기 전에
검사 목록을 검토하고 다음 ServiceNow# 애플리케이션을 설치했는지 확인합니다.

- 취약성 대응 설치 및 지원되는 애플리케이션 여기에는 NVD 통합, 취약성 대응 CISA와의 통합 및 CWE 예약된 작업이 포함됩니다.
- 컨테이너용 Vulnerability Response 및 Configuration Compliance.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 구성 준수.

  이러한 애플리케이션은 별도의 구독으로 사용할 수 있습니다. 스토어 응용 프로그램 설치에 대한 자세한 내용은 을 참조하십시오 Install a ServiceNow Store application .

필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 〉 시스템 애플리케이션 〉 모든 사용 가능 애플리케이션.
2. Wiz 취약성 대응 Integration 애플리케이션을 찾습니다.
3. 카드를 선택하여 열고 설치를 선택합니다.
   스토어 응용 프로그램 설치에 대한 자세한 내용은 을 참조하십시오 Install a ServiceNow Store application .
   종속성 검사 목록 대화 상자가 표시됩니다. 아직 설치하지 않은 필수 종속성을 설치하려면 (설치 필요) 링크를 선택합니다.
4. 애플리케이션 설치 대화 상자에서 설치를 선택합니다.
   애플리케이션이 성공적으로 설치되면 메시지가 표시됩니다. 준비가 완료되었습니다 Wiz 취약성 대응 통합 구성.
5. 다음으로 이동 모두 〉 **Wiz** 취약성 통합 〉 관리 〉 통합.
6. 데이터를 임포트하려는 통합이 활성화되어 있는지 확인합니다(활성 열이 true로 설정됨).
7. 기록을 선택하여 열고 통합을 활성화하거나 비활성화합니다.

Wiz 취약성 대응 통합 구성

서비스 계정에서 통합을 Wiz 구성하고 AI Platform 인스턴스에서 역할을 ServiceNow 할당합니다.

시작하기 전에
이 통합에 대해 생성된 계정에서 미리 선택된 권한으로 통합 타일 Wiz 을 구성해야 합니다. 자세한 내용은 Wiz 제품 설명서를 참조하십시오.

필요한 역할:

- 관리자는 AI Platform 인스턴스에 역할을 ServiceNow 할당합니다.

프로시저

1. AI Platform 인스턴스에서 통합 ServiceNow 과 통합을 지원하는 애플리케이션에 대한 Wiz 역할을 사용자에게 할당합니다.

   a. 다음으로 이동 사용자 관리 〉 사용자

   b. 다음 역할을 할당합니다.

   - sn_vul.vulnerability_admin을 취약성 대응 사용하여 및 컨테이너 취약성 대응 애플리케이션을 구성합니다.
   - sn_vulc.admin
   - sn_vul_wiz.configure_integration을 사용하여 통합을 설정합니다.
   - sn_vul_wiz.read_integration 이 통합에 대한 데이터와 기록을 보려는 조직의 사용자에 대한 것입니다.

   c. 사용자 생성 및 역할 관리에 대한 자세한 내용은 을 참조하십시오 User administration .

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

2. sn_vul_wiz.configure_integration 역할을 가진 사용자로 모두 〉 **Wiz** 취약성 통합 〉 관리 〉 구성 인스턴스에 있습니다.
3. 필드에 내용을 입력합니다.

필드	설명
통합 인스턴스	와 WizVulnerability Response 통합 .
인증 URL	환경에서 입력한 인증 URL입니다 Wiz .
API URL	사용자 환경에 입력한 API URL입니다 Wiz .
클라이언트 ID	사용자 환경에 입력한 Wiz 이 통합에 사용하려는 클라이언트 ID입니다.
클라이언트 비밀	사용자 Wiz 환경에 입력한 이 통합에 사용하려는 클라이언트 비밀입니다.

4. 저장 및 테스트를 선택합니다.
   자격 증명이 성공적으로 저장되고 유효성이 확인되면 메시지가 표시됩니다. 통합 임포트에 대한 필터링을 선택할 수 있습니다.

호스트 취약성 통합에 **Wiz** 대한 필터링 설정

필터링 값을 설정하여 원하는 호스트 취약성 데이터를 임포트합니다.

시작하기 전에
필요한 역할: sn_vul_wiz.configure_integration

프로시저

1. 다음으로 이동 모두 〉 **Wiz** 취약성 통합 〉 관리 〉 구성.
2. 아직 선택하지 않은 경우 호스트 취약성 구성 탭을 선택합니다.
3. 필드에 내용을 입력합니다.
   표시되는 필드는 기본 호스트 취약성 데이터를 임포트하는 필터를 제공합니다. 더 많은 필터링 옵션을 보려면 고급 확인란을 선택하고 다음 표에서 자세한 내용을 참조하십시오.

필드	설명
첫 번째	페이지 매김. 값을 입력합니다. 1000으로 시작하는 것이 좋습니다.
심각도	심각도 찾기. None이 기본값입니다. 선택하면 이 필드에 대한 데이터를 임포트하지 않음을 나타냅니다. 다음과 같이 여러 값을 지정할 수 있습니다. ○ NONE - 사용 가능한 심각도 값이 없는 자산을 반환합니다. ○ 낮음 ○ 보통 ○ 높음 ○ 중요

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
자원 상태	이러한 상태가 있는 자산에 대해 발견한 취약성만 반환합니다. 다음과 같이 여러 값을 지정할 수 있습니다. ○ 없음(기본값) - 이 옵션을 선택하면 이 필드에 대한 데이터를 임포트하지 않음을 나타냅니다. ○ 활성 ○ 오류 ○ 비활성
자원 유형	이러한 객체 유형을 필터링합니다. 두 값을 모두 지정할 수 있습니다. ○ 없음(기본값) - 이 옵션을 선택하면 이 필드에 대한 데이터를 임포트하지 않음을 나타냅니다. ○ VIRTUAL_MACHINE ○ 서버리스

4. 더 많은 필터링 옵션을 보려면 고급 확인란을 선택합니다.

대부분의 필드에 여러 값을 지정할 수 있습니다. --None- -이 (기본값)입니다. 필드에 ## --##--# 선택된 상태로 유지되면 이 필드에 대해 데이터가 임포트되지 않습니다.

필드	설명
상태	찾기 상태를 기준으로 필터링: ○ 열기 ○ 거부됨 ○ 해결됨
탐지 방법	다음 탐지 방법으로 발견한 취약성 결과를 필터링합니다. ○ 패키지 ○ DEFAULT_PACKAGE ○ 라이브러리 ○ OS ○ INSTALLED_PROGRAM ○ INSTALLED_PROGRAM_BY_SERVICE ○ FILE_PATH
관련 문제 심각도	○ 중요 ○ 높음 ○ 정보성

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	○ 낮음 ○ 보통
취약성	입력한 외부 ID와 일치하는 취약성 결과를 필터링합니다(예: CVE-1234-5678, CVE-9110-26117).
공개 익스플로잇 존재 여부	이용 가능한 익스플로잇이 있는 취약성의 취약성 찾기를 필터링합니다(예/아니오).
프로젝트 ID	지정된 프로젝트에 대해 입력한 문자열로 취약성 결과를 필터링합니다.
수정 가능 여부	사용 가능한 수정 사항(예/아니오)으로 취약성 찾기에서 취약성을 필터링합니다.
자원	입력한 자원을 필터링합니다.
자원에 관리자 권한 있음	관리자 권한(예/아니오)이 있는 자산의 취약성 찾기를 필터링합니다.
구독	외부 구독의 경우 다음 문자열에서 결과를 임포트합니다(AWS 계정, Azure 구독, GCP 프로젝트, OCI 구획). 배열에 여러 값을 지정할 수 있습니다. 값을 입력하지 않으면 모든 구독이 반환됩니다.
CISA KEV 익스플로잇 보유 여부	가능한 CISA KEV 익스플로잇(예/아니오)이 있는 취약성에서 취약성 찾기를 필터링합니다.
자원에 높은 권한 있음	높은 권한(예/아니오)이 있는 자산의 취약성 찾기를 필터링합니다.
자원의 인터넷에 광범위하게 노출되어 있음	인터넷 노출이 높은 자산에 대한 취약성 찾기를 필터링합니다(예/아니오).
자원의 인터넷 노출이 제한되어 있음	인터넷 노출이 낮은 자산에 대한 취약성 찾기를 필터링합니다(예/아니오).
처음 표시된 시점(이후)	선택한 날짜로 시작하는 자산을 기준으로 필터링합니다.
해결 시점(이후)	선택한 날짜로 시작하여 해결된 취약성이 있는 자산을 기준으로 필터링합니다.
업데이트 시점(이후)	선택한 날짜로 시작하여 업데이트된 자산을 기준으로 필터링합니다.

5. 저장 및 테스트를 선택합니다.
   자격 증명이 성공적으로 저장되고 유효성이 확인되면 메시지가 표시됩니다. 다른 통합 임포트에 대한 필터링을 선택할 수 있습니다.

컨테이너 취약성 통합에 **Wiz** 대한 필터링 설정

필터링 값을 설정하여 원하는 컨테이너 취약성 데이터를 임포트합니다.

시작하기 전에
필요한 역할: sn_vul_wiz.configure_integration

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 **Wiz** 취약성 통합 〉 관리 〉 구성.
2. 컨테이너 취약성 구성 탭을 선택합니다.
3. 필드에 내용을 입력합니다.

   일부 필드의 경우 여러 값을 지정할 수 있습니다. --None- -이 (기본값)입니다. 필드에 ## --##--# 선택된 상태로 유지되면 이 필드에 대해 데이터가 임포트되지 않습니다.

필드	설명
첫 번째	페이지 매김. 값을 입력합니다. 1000으로 시작하는 것이 좋습니다.
공개 익스플로잇 존재 여부	이용 가능한 익스플로잇이 있는 취약성의 취약성 찾기를 필터링합니다(예/아니오).
구독	외부 구독 ID(AWS 계정, Azure 구독, GCP 프로젝트 및 OCI 구획)에 대해 다음 문자열에서 결과를 임포트합니다. 값을 입력하지 않으면 모든 구독이 반환됩니다.
수정 가능 여부	사용 가능한 수정 사항(참/거짓)으로 취약성에서 발견한 취약성을 임포트합니다.
취약성	외부 ID가 일치하는 취약성 결과(예: CVE-1234-5678, CVE-9110-26117)를 임포트합니다.
CISA KEV 익스플로잇 보유 여부	사용 가능한 CISA KEV 익스플로잇 (예/아니오)이 있는 취약성에 대한 취약성 결과만 임포트합니다.
프로젝트 ID	지정된 프로젝트(문자열)에 대한 취약성 결과만 임포트합니다.
자원에 높은 권한 있음	높은 권한(예/아니오)이 있는 취약성 결과만 반환합니다.
자원 상태	이러한 상태가 있는 결과만 반환합니다. 다음과 같이 여러 값을 지정할 수 있습니다. ○ 활성 ○ 오류 ○ 비활성
자원에 관리자 권한 있음	관리자 권한이 있는 취약성 결과만 반환합니다. (예/아니오)
탐지 방법	다음 탐지 방법으로 발견한 취약성 결과를 필터링합니다. ○ DEFAULT_PACKAGE ○ FILE_PATH ○ INSTALLED_PROGRAM ○ INSTALLED_PROGRAM_BY_SERVICE ○ 라이브러리

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	○ OS ○ 패키지
자원의 인터넷 노출이 제한되어 있음	인터넷 노출이 낮은 취약성 찾기를 필터링합니다(true/false).
취약성 심각도	취약성 심각도별로 결과를 필터링합니다. ○ 중요 ○ 높음 ○ 낮음 ○ 보통
상태	상태별 결과 필터링: ○ 열기 ○ 해결됨

4. 저장 및 테스트를 선택합니다.
   자격 증명이 성공적으로 저장되고 유효성이 확인되면 메시지가 표시됩니다. 다른 통합 임포트에 대한 필터링을 선택할 수 있습니다.
5. 옵션: 키 조합을 지정하여 컨테이너 취약 항목(CVIT)의 세분성을 구성합니다.

   (Optional) CVIT는 기본적으로 이미지 리포지토리, 취약성 및 이미지를 결합하여 생성됩니다. 추가 세분성을 위해 키에 구성요소를 추가할 수 있습니다. 예를 들어 CVIT는 이미지 리포지토리, 취약성, 이미지 및 클러스터의 조합에 대한 것입니다.

   세분성을 구성하려면 다음으로 이동하십시오. 모두 〉 **Wiz** 취약성 통합 〉 관리 〉 **CVR** 기반 **VI** 세분성 구성.

   추가할 키를 선택합니다. 데이터를 임포트하면 키가 고려되고 CVIT가 생성됩니다.

테스트 결과 통합에 **Wiz** 대한 필터링 설정

필터링 값을 설정하여 원하는 클라우드 테스트 결과 데이터를 임포트합니다.

시작하기 전에

필요한 역할: sn_vul_wiz.configure_integration

프로시저

1. 다음으로 이동 모두 〉 **Wiz** 취약성 통합 〉 관리 〉 구성.
2. 테스트 결과 구성 탭을 선택합니다.
3. 필드에 내용을 입력합니다.

   일부 필드의 경우 여러 값을 지정할 수 있습니다. --None- -이 (기본값)입니다. 필드에 ## --##--# 선택된 상태로 유지되면 이 필드에 대해 데이터가 임포트되지 않습니다.

   주:
   다음의 Wiz 호스트 구성을 임포트하지 않습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
심각도	심각도 필터링에 대해 다음 중 하나를 선택합니다. ○ 낮음 ○ 보통 ○ 높음 ○ 중요 ○ NONE - 사용 가능한 심각도 값이 없는 결과를 반환합니다. HIGH 또는 CRITICAL로 시작하여 임포트를 매우 중요한 결과로만 제한하는 것이 좋습니다.
프로젝트 ID	프로젝트에 대한 클라우드 구성 결과(예: "#### ID")만 지정합니다.
클라우드 플랫폼	클라우드 플랫폼별 구성 결과입니다. AWS, GitHub, Terraform, OpenAI, GKE, OKE, EKS, AKS와 같은 여러 값을 지정할 수 있습니다.
구독 ID	구독 ID를 입력하여 지정합니다. 배열에 여러 값을 지정할 수 있습니다.
자원 상태	상태별 지정: ○ 활성 ○ 오류 ○ 비활성
프레임워크 범주	보안 프레임워크, 보안 하위 범주 또는 보안 범주를 입력합니다. 여러 값을 지정할 수 있습니다.
자원 유형	엔터티 유형입니다. 여러 값(예: BUCKET,DATABASE)을 지정할 수 있습니다
네이티브 유형	클라우드 자원의 네이티브 유형(예: ##)을 기준으로 결과를 지정합니다.
정정 가능 여부	정정 지침이 포함되거나(TRUE) 없거나 (FALSE) 결과를 지정합니다.
첫 번째	페이지 매김. 값을 입력합니다. 1000으로 시작하는 것이 좋습니다.
다음 시점 이후 분석	선택한 날짜부터 분석된 결과를 필터링합니다.
상태	상태별 필터링: ○ 열기 ○ 해결됨

4. 저장 및 테스트를 선택합니다.
   자격 증명이 성공적으로 저장되고 유효성이 확인되면 메시지가 표시됩니다. 다른 통합 임포트에 대한 필터링을 선택할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

문제 통합에 **Wiz** 대한 필터링 설정

필터링할 필터링 값을 임포트 Wiz 하도록 설정 취약성 및 잘못된 구성의 유해한 조합에 관련된 자산을 식별하는 문제입니다.

시작하기 전에
필요한 역할: sn_vul_wiz.configure_integration

프로시저

1. 다음으로 이동 모두 〉 **Wiz** 취약성 통합 〉 관리 〉 구성.
2. 문제 구성 탭을 선택합니다.
3. 필드에 내용을 입력합니다.

   일부 필드의 경우 여러 값을 지정할 수 있습니다. --None- -이 (기본값)입니다. 필드에 ## --##--# 선택된 상태로 유지되면 이 필드에 대해 데이터가 임포트되지 않습니다.

필드	설명
심각도	심각도 찾기를 기준으로 필터링합니다. ○ 낮음 ○ 보통 ○ 높음 ○ 중요 ○ 정보성
프로젝트 ID	지정된 프로젝트(문자열)에 대한 결과만 임포트합니다.
문제 유형	문제가 생성된 규칙 유형에 따른 문제입니다. ○ CLOUD_CONFIGURATION ○ THREAT_DETECTION ○ TOXIC_COMBINATION
구독 ID	구독 ID를 입력하여 결과를 지정합니다. 배열에 여러 값을 지정할 수 있습니다.
클라우드 플랫폼	클라우드 플랫폼별 구성 결과입니다. AWS, GitHub, Terraform, OpenAI, GKE, OKE, EKS, AKS와 같은 여러 값을 지정할 수 있습니다.
프레임워크 범주	보안 프레임워크, 보안 하위 범주 또는 보안 범주를 입력합니다. 여러 값을 지정할 수 있습니다.
네이티브 유형	클라우드 자원의 네이티브 유형(예: ##)을 기반으로 한 문제입니다.
첫 번째	페이지 매김. 값을 입력합니다. 1000으로 시작하는 것이 좋습니다.
상태	상태별 필터링:

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	○ 열기 ○ 진행 중 ○ 해결됨

4. 저장 및 테스트를 선택합니다.
   자격 증명이 성공적으로 저장되고 유효성이 확인되면 메시지가 표시됩니다. 다른 통합 임포트에 대한 필터링을 선택할 수 있습니다.

취약성 대응 통합을 위한 **Wiz** 필드 매핑

소스 및 대상 필드를 검토하고 Now Platform AI 인스턴스의 테이블 및 기록에서 임포트한 ServiceNow 데이터를 봅니다.

호스트 취약성 통합 필드 매핑

Wiz 필드	ServiceNow 테이블 열	ServiceNow 필드 열
설명	sn_vul_detection	증명
상태	sn_vul_detection	source_status
lastDetectedAt	sn_vul_detection	last_found
첫 번째 탐지됨	sn_vul_detection	first_found
vulnerableAsset.name	sn_vul_detection	dns
수정	sn_vul_detection	solution_summary
vulnerableAsset.ipAddresses[0]	sn_vul_detection	ip_address
벤더 심각도	sn_vul_detection	source_severity
고정 버전	sn_vul_detection	fixed_version
상태	sn_vul_detection	is_ignored
상태	sn_vul_detection	상태
이름	sn_vul_nvd_entry	ID
점수	sn_vul_nvd_entry	v3_base_score
CVEDescription	sn_vul_nvd_entry	요약
벤더 심각도	sn_vul_nvd_entry	source_severity
cvssv3.attackVector	sn_vul_nvd_entry	v3_attack_vector
cvssv3.attackComplexity	sn_vul_nvd_entry	v3_attack_complexity
cvssv3.기밀성영향	sn_vul_nvd_entry	v3_confidentiality_impact
cvssv3.privileges필수	sn_vul_nvd_entry	v3_privileges_required
cvssv3.무결성영향	sn_vul_nvd_entry	v3_integrity_impact
cvssv3.userInteractionRequired	sn_vul_nvd_entry	v3_user_interaction
익스플로잇 hasExploit	sn_vul_nvd_entry	익스플로잇
hasCisaKevExploit	sn_vul_nvd_entry	cisa_exists

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Wiz 필드	ServiceNow 테이블 열	ServiceNow 필드 열
vulnerableAsset.tags	sn_sec_cmn_src_ci	host_tag
vulnerableAsset.id	sn_sec_cmn_src_ci	source_id
vulnerableAsset.name	sn_sec_cmn_src_ci	이름
vulnerableAsset.region	sn_sec_cmn_src_ci	cloud_region
vulnerableAsset.providerUniqueId	sn_sec_cmn_src_ci	resource_id
vulnerableAsset.cloudPlatform	sn_sec_cmn_src_ci	cloud_service_provider
vulnerableAsset.type	sn_sec_cmn_src_ci	assetType
관련문제분석	sn_sec_cmn_src_ci	source_data
vulnerableAsset.nativeType	sn_sec_cmn_src_ci	cloud_resource_type
vulnerableAsset.subscriptionExternalId	sn_sec_cmn_src_ci	cloud_account
vulnerableAsset.name	sn_sec_cmn_src_ci	resource_name
vulnerableAsset.imageName	sn_sec_cmn_src_ci	image_id
vulnerableAsset.*	sn_sec_cmn_src_ci	source_data
lastDetectedAt	sn_sec_cmn_src_ci	source_data

컨테이너 취약성 통합 필드 매핑

Wiz 필드	ServiceNow 테이블 열	ServiceNow 필드 열
imageId	sn_vul_container_image	image_id
vulnerableAsset.name	sn_vul_container_image	image_name
vulnerableAsset.repository.externalId 이후 ##	sn_vul_container_image	레지스트리
이전의 vulnerableAsset.repository.externalId ##	sn_vul_container_image	리포지토리
vulnerableAsset.tags	sn_vul_container_image	image_labels
프로젝트	sn_vul_container_image	image_projects
vulnerableAsset.region	sn_vul_container_image	cloud_regions
vulnerableAsset.cloudPlatform	sn_vul_container_image	cloud_providers
vulnerableAsset.subscriptionExternalId	sn_vul_container_image	cloud_account_ids
vulnerableAsset.executionControllers	sn_vul_container_image	image_namespace
vulnerableAsset.executionControllers	sn_vul_container_image	image_clusters
vulnerableAsset.executionControllers	sn_vul_container_image_vulnerable_item	image_clusters
vulnerableAsset.executionControllers	sn_vul_container_image_vulnerable_item	image_namespace
이전의 vulnerableAsset.repository.externalId ##	sn_vul_container_image_vulnerable_item	image_repository

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Wiz 필드	ServiceNow 테이블 열	ServiceNow 필드 열
layerMetadata.isBaseLayer	sn_vul_container_image_findings	is_base_image
첫 번째 탐지됨	sn_vul_container_image_findings	first_found
lastDetectedAt	sn_vul_container_image_findings	last_found
상세이름	sn_vul_container_image_package	이름
버전	sn_vul_container_image_package	버전
위치 경로	sn_vul_container_image_package	path
이름	sn_vul_nvd_entry	ID
점수	sn_vul_nvd_entry	v3_base_score
CVEDescription	sn_vul_nvd_entry	요약
벤더 심각도	sn_vul_nvd_entry	source_severity
cvssv3.attackVector	sn_vul_nvd_entry	v3_attack_vector
cvssv3.attackComplexity	sn_vul_nvd_entry	v3_attack_complexity
cvssv3.기밀성영향	sn_vul_nvd_entry	v3_confidentiality_impact
cvssv3.privileges필수	sn_vul_nvd_entry	v3_privileges_required
cvssv3.무결성영향	sn_vul_nvd_entry	v3_integrity_impact
cvssv3.userInteractionRequired	sn_vul_nvd_entry	v3_user_interaction
익스플로잇 hasExploit	sn_vul_nvd_entry	익스플로잇 hasExploit
layerMetadata.isBaseLayer	sn_vul_container_image_layer	기본 레이어
layerMetadata.details	sn_vul_container_image_layer	명령
layerMetadata.id	sn_vul_container_image_layer	ID
상태	sn_vul_container_image_findings	is_ignored
validate_at_runtime	sn_vul_container_image_findings	validate_at_runtime
ID	sn_vul_container_image_findings	unique_key

구성 준수 테스트 결과 통합 필드 매핑

Wiz 필드	ServiceNow 테이블 열	ServiceNow 필드 열
rule.id	sn_vulc_test	source_id
rule.name	sn_vulc_test	short_description
rule.remediationInstructions	sn_vulc_test	수정
rule.description	sn_vulc_test	설명
severity	sn_vulc_test	source_criticality
상태	sn_vulc_result	결과
ID	sn_vulc_result	source_id
분석됨	sn_vulc_result	last_seen
firstSeenAt	sn_vulc_result	first_seen

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Wiz 필드	ServiceNow 테이블 열	ServiceNow 필드 열
rule.remediationInstructions	sn_vulc_result	수정
resource.nativeType	sn_sec_cmn_src_ci	source_data
자원.유형	sn_sec_cmn_src_ci	source_data
ID	sn_vulc_result	설명
ID	sn_vulc_result	source_id
securitySubCategories.category.framework.id	sn_vulc_result_src	source_id
securitySubCategories.category.framework.name	sn_vulc_result_src	short_description
securitySubCategories.category.framework.description	sn_vulc_result_src	설명
securitySubCategories.id	sn_vulc_citation	섹션
securitySubCategories.title	sn_vulc_citation	section_name
resource.projects	sn_sec_cmn_src_ci	프로젝트
상태	sn_vulc_result	is_ignored

문제 통합 필드 매핑

주:
클라우드 테스트 결과(CTR)에 대한 문제 통합을 위해 매핑된 데이터에는 이러한 CTR을 테스트 결과 통합 CTR과 구별하는 데 도움이 되는 소스로 Wiz ## 레이블이 지정됩니다.

Wiz 필드	ServiceNow 테이블 열	ServiceNow 필드 열
sourceRule.id	sn_vulc_test	source_id
sourceRule.name	sn_vulc_test	short_description
sourceRule.resolutionRecommendation/ sourceRule.remediationInstructions	sn_vulc_test	수정
sourceRule.description	sn_vulc_test	설명
severity	sn_vulc_test	source_criticality
createdAt	sn_vulc_result	first_seen
updatedAt	sn_vulc_result	last_seen
상태	sn_vulc_result	결과
ID	sn_vulc_result	source_id
sourceRule.resolutionRecommendation/ sourceRule.remediationInstructions	sn_vulc_result	수정
sourceRule.controlDescription	sn_vulc_result	설명
entitySnapshot.nativeType	sn_sec_cmn_src_ci	source_data
entitySnapshot.type	sn_sec_cmn_src_ci	source_data
Wiz issue'	sn_vulc_result	result_type
ID	sn_vulc_result	설명
severity	sn_vulc_test	source_criticality

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Wiz 필드	ServiceNow 테이블 열	ServiceNow 필드 열
ID	sn_vulc_result	source_id
sourcerule.securitySubCategories.category.framework.id	sn_vulc_category	source_id
sourcerule.securitySubCategories.category.framework.name	sn_vulc_category	short_description
sourcerule.securitySubCategories.category.framework.description	sn_vulc_category	설명
sourcerule.securitySubCategories.id	sn_vulc_citation	섹션
sourcerule.securitySubCategories.title	sn_vulc_citation	section_name
프로젝트	sn_sec_cmn_src_ci	프로젝트
상태	sn_vulc_result	is_ignored

취약한 항목 및 테스트 결과 기록에 매핑

- 호스트 취약성 발견 사항이 호스트 취약 항목(VIT)에 매핑됩니다.
- 컨테이너 취약성 발견 사항은 컨테이너 취약 항목(CVIT)에 매핑됩니다.
- 구성 테스트 결과 결과는 애플리케이션의 클라우드 테스트 결과 기록(CTR)에 매핑됩니다 구성 준수 .
- 문제 발견 사항은 애플리케이션의 클라우드 테스트 결과 기록(CTR)에 매핑됩니다 구성 준수 .

취약성 통합을 수동으로 생성

취약성 통합은 고객과 벤더가 외부 시스템 및 벤더로부터 데이터를 검색하여 인스턴스의 취약성 데이터를 보강할 수 있는 기능을 제공합니다. 이 기능은 인스턴스를 다른 취약성 관리 시스템과 동기화된 상태로 유지하여 취약성 정정 수명주기를 단순화할 수 있습니다.

통합 생성에 대한 자세한 지침은 다음 문서를 참조하십시오 새 취약성 통합 정의.

새 취약성 통합 정의

취약성 통합은 일반적으로 취약성 데이터를 검색하고 데이터 소스 또는 사용자 지정 프로세서를 사용하여 해당 보고 데이터를 처리하기 위해 외부 공급업체 시스템에서 보고서 데이터를 끌어옵니다.

시작하기 전에

가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)

프로시저

1. 다음으로 이동 모두 〉 취약성 〉 관리 〉 통합.
2. 새로 만들기를 클릭합니다.
3. 필요에 따라, 필드를 채웁니다.

취약성 통합

필드	설명
이름	통합에 대한 설명이 포함된 이름입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
활성	통합이 활성 상태인지 여부입니다. 특정 기간 동안 실행되지 않도록 하려면 사용할 매개변수를 설정하고 작업을 비활성화할 수 있습니다.
실행	통합을 실행할 빈도(매일, 매주, 주기적으로 등)입니다. 앞에서 언급했듯이 후속 필드는 이 필드의 설정에 따라 표시되거나 표시되지 않습니다.
일	통합을 실행하려는 날짜입니다. ○ 실행 필드에서 매주를 선택한 경우 이 필드에 요일이 표시됩니다. ○ 실행 필드에서 매월을 선택한 경우 이 필드에 월의 일수가 표시됩니다.
시간	통합을 시작할 시간입니다. 이 필드는 실행 필드에서 매일, 매주 또는 매월을 선택한 경우에만 나타납니다.
애플리케이션	〔읽기 전용〕 이 통합이 생성된 애플리케이션의 이름입니다.
반복 간격	실행 필드에서 주기적으로를 선택한 경우 이 필드에는 통합이 다시 실행되기까지의 일 수와 시간이 표시됩니다.
시작 중	실행 필드에서 주기적으로를 선택한 경우 이 필드에는 주기적인 업데이트의 시작점으로 사용할 날짜 및 시간이 표시됩니다.
조건부	조건부 매개변수를 추가하려면 이 필드를 선택합니다.
조건	조건부 확인란을 선택한 경우 여기에 조건을 입력합니다.
통합 상세 정보	
통합 스크립트	통합이 실행될 때 실행할 VulnerabilityIntegrationBase를 확장하는 스크립트 포함을 선택합니다. 이 스크립트는 타사 시스템에서 데이터를 검색하는 방법을 정의합니다.
통합 공장 스크립트	통합 스크립트에 대해 선택된 스크립트 포함을 구성하는 방법을 정의하는 스크립트를 입력합니다. 자세한 내용은 통합 공장 스크립트 필드 문서를 참조하십시오. **주:** 스크립트에는 두 가지 모두 ServiceNow와 취약성 대응 전문 지식이 필요합니다.
프로세서 전략 보고	통합이 실행될 때 통합 스크립트에서 반환되는 데이터를 처리하는 데 사용하려는 전략을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	○ 데이터 소스를 사용하여 데이터를 처리하려면 데이터 소스 첨부 파일을 선택합니다. ○ 사용자 지정 보고서 프로세서를 선택하여 사용자 지정 프로세서를 선택합니다.
보고서 프로세서	보고서 프로세서 전략 필드에서 사용자 지정 보고서 프로세서를 선택한 경우 통합이 실행될 때 실행되도록 VulnerabilityReportProcessorBase 스크립트 포함을 확장하는 스크립트 포함을 선택합니다. 이 스크립트는 통합 스크립트에서 반환된 데이터의 처리 방법을 정의합니다.
프로세서 공장 스크립트	보고서 프로세서에 대해 선택된 스크립트 포함을 구성하는 방법을 정의하는 스크립트를 입력합니다.

4. 제출을 클릭합니다.

관련 정보

취약성 통합 스크립트

프로세서 전략 보고

통합 공장 스크립트 필드

취약성 통합 수동 실행

취약성 통합 스크립트

취약성 통합 양식에서 통합 스크립트는 VulnerabilityIntegrationBase 스크립트 포함을 확장하는 스크립트 포함에 대한 참조입니다.

이 스크립트에 포함된 기능은 외부 데이터 소스에서 데이터를 검색하는 방법을 관리하기 위해 VulnerabilityIntegrationController에 의해 호출됩니다. VulnerabilityIntegrationBase의 각 하위 클래스는 호출 프로세스에 대한 컨텍스트 정보에 액세스할 수 있습니다. 이 정보는 다음 멤버 변수를 통해 사용할 수 있습니다.

- integrationGr — 통합 실행을 요청한 취약성 통합 기록의 GlideRecord입니다.
- integrationProcessGr — 통합의 현재 프로세스에 대한 컨텍스트 정보를 제공하는 GlideRecord입니다.

취약성 프로세스에는 일반적으로 페이지 매김 목적으로 통합 내에서 사용되는 특수 매개변수가 포함되어 있습니다. 각 취약성 통합 실행(취약성 통합 실행이라고 함)에는 하나 이상의 연관된 취약성 통합 프로세스가 있습니다. 다중 호출 통합의 경우 각 취약성 통합 실행에 대해 하나 이상의 취약성 통합 프로세스 기록이 있습니다.

스크립트 포함은 retrieveData() 메서드에 대한 구현을 제공하고 보고서 프로세서 스크립트에서 처리되는 개체를 반환해야 합니다. retrieveData에서 반환되는 객체는 content, contentType 및 extension에 대한 속성이 있는 간단한 객체입니다.

다음은 VulnerabilityIntegrationBase.retrieveData()의 스크린샷입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

VulnerabilityIntegrationBase.retrieveData()

```
/**
 * Retrieves data (generally from an external system) to be passed to a report processor.
 * Subclasses (i.e. concrete implementations of a Vulnerability Integration) should implement/override this
 * function.
 * The class should return an object structured as follows:
 *
 * {
 *    contents: raw contents of data to process, usually a string.  If the integration creates an attachment
 *              this value should be the attachment sys_id.
 *    contentType: the mimeType of the content.  If the content is an attachment sys_id,
 *                 this should be sys_attachment.  The sys_attachment record itself should have the
 *                 content type specified.
 *    extension: the file extension that should be used for this content in the event the processor
 *               needs to write the contents to a file (such as a new attachment).
 * }
 *
 * For multipage integrations (where multiple calls/integration processes must run), this function should check
 * the integrationProcessGr's parameters.
 */
retrieveData: function() {
    return {contents: "", contentType: "", extension: ""};
},
```

retrieveData()의 논리는 데이터를 검색하는 데 필요한 인터페이스에 따라 다릅니다. 예를 들어 끌어오는 데이터의 원본에 REST API가 있는 경우 이 메서드의 본문은 RESTMessageV2를 통해 REST 엔드포인트를 호출할 수 있습니다. 그런 다음 호출의 응답을 구문 분석하거나 첨부 파일에 넣을 수 있으며 세부 정보를 사용하여 반환 개체를 구성할 수 있습니다.

단일 통화 통합

단일 호출(단일 페이지) 통합 스크립트는 가장 간단한 유형의 통합입니다. 데이터를 검색하려면 종종 외부 데이터 소스에 한 번의 호출이 필요합니다. 단일 페이지/단일 호출 통합의 경우 retrieveData()만 구현해야 합니다.

간단한 단일 호출 통합 스크립트를 보여 주는 샘플은 다음과 같습니다. RESTMessageV2를 생성하고 실행합니다. 그런 다음 응답 본문을 콘텐츠로 사용하여 가정된 contentType 및 확장과 함께 개체를 반환합니다.

단일 호출 통합 스크립트

```
var SingleRunVulnerabilityIntegration = Class.create();
SingleRunVulnerabilityIntegration.prototype = Object.extendsObject(sn_vul.VulnerabilityIntegrationBase, {
    initialize: function() { },

    /**
     * Sample retrieveData() where fictional RESTMessage is executed and XML response body is
     * returned.
     */
    retrieveData: function() {
        var message = new sn_ws.RESTMessageV2("My Vuln REST", "get");
        var response = message.execute();
        var responseBody = response.haveError() ? response.getErrorMessage() : response.getBody();
        return {contents: responseBody, contentType: "application/xml", extension: "xml"};
    },

    type: 'SingleRunVulnerabilityIntegration'
});
```

다중 통화 통합

다중 호출(또는 다중 페이지) 통합 스크립트는 좀 더 복잡합니다. 데이터를 검색하려면 데이터 원본을 여러 번 호출해야 합니다.

단일 호출 통합과 마찬가지로 다중 호출 통합에도 retrieveData()가 구현되어 있어야 합니다. retrieveData()의 본문에서 통합은 VulnerabilityIntegrationBase에서 제공하는 hasMoreData() 및 setNextRunParameters() 메서드를 사용합니다.

hasMoreData() 메서드는 더 많은 데이터를 가져오기 위해 더 많은 프로세스를 삽입하도록 VulnerabilityIntegrationController에 지시하는 단일 부울을 허용합니다. hasMoreData()에 true를 전달하면 setNextRunParameters()를 호출하여 다음 프로세스에 컨텍스트를 제공합니다.

setNextRunParameters() 메서드는 다음에 retrieveData()를 호출할 때 사용할 컨텍스트 정보를 제공하는 단일 객체를 받습니다. 이 객체는 retrieveData()에 대한 후속 호출에 상태를 전달하는 데

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용됩니다. 사용 사례의 예로는 현재 페이지 번호와 페이지 크기를 나타내는 객체를 웹 서비스에 전달하는 것입니다.

여러 호출 통합의 경우 각 retrieveData() 호출은 먼저 현재 프로세스 매개변수를 확인합니다. _getProcessParameters() 메서드는 이전 프로세스에서 설정한 매개변수를 편리하게 가져올 수 있도록 모든 VulnerabilityIntegrationBase에 제공됩니다. 매개변수가 없으면 첫 번째 프로세스임을 나타냅니다.

다음은 샘플 다중 호출 통합 스크립트의 스크린샷입니다. 단일 호출 통합 예제를 확장한 이 스크립트는 기본 페이지 매김 지원이 있는 REST 엔드포인트를 호출하는 방법을 보여줍니다. 한 페이지의 데이터를 가져오고 검색할 데이터가 더 있음을 인식한 다음 다음 프로세스에 검색할 페이지를 지정하는 방법을 보여 줍니다.

다중 호출 통합 스크립트

```
var MultiRunVulnerabilityIntegration = Class.create();
MultiRunVulnerabilityIntegration.prototype = Object.extendsObject(sn_vul.VulnerabilityIntegrationBase, {
    initialize: function() { },

    /**
     * Sample retrieveData() where fictional RESTMessage is executed and XML response body is
     * returned.  This call is paginated, so we need to figure out the range to pull
     * for each call.
     *
     * For simplicity, we'll say that a status code != 200 means we've reached the end of data
     * from the server, or if we cap out past our maxPages member variable.
     */
    maxPages: 5,
    retrieveData: function() {
        var currentParams = this._getProcessParameters();
        var pageSize = 100;
        var page = 1;
        if (currentParams) {
            page = currentParams.page;
        }
        var message = new sn_ws.RESTMessageV2("My Vuln REST", "get");
        message.setQueryParameter("pageSize", pageSize);
        message.setQueryParameter("page", page);
        var response = message.execute();
        var responseBody = response.haveError() ? response.getErrorMessage() : response.getBody();
        if (response.getStatusCode() != 200 || page >= this.maxPages) {
            this.hasMoreData(false);
            this.setNextRunParameters(null);
        } else {
            this.hasMoreData(true);
            this.setNextRunParameters({
                page: page + 1
            });
        }
        return {contents: responseBody, contentType: "application/xml", extension: "xml"};
    },

    type: 'MultiRunVulnerabilityIntegration'
});
```

첨부 파일 **as retrieveData()** 반환 값

때로는 retrieveData()에서 첨부 파일을 반환하는 것이 좋습니다. 첨부 파일을 작성 및/또는 검색하는 논리는 구현에 따라 다르지만 첨부 파일이 알려진 후에는 해당 정보가 반환될 수 있습니다.

첨부 파일을 제공하기 위해 retrieveData() 는 다음과 같은 객체를 반환합니다.

```
{
    contents: "attachment-sys-id",
    contentType: "sys_attachment"
}
```

이전 예를 확장하지만 REST 메시지의 응답 본문을 통합 프로세스 기록에 저장하는 예는 다음과 같습니다. 그런 다음 해당 첨부 파일 식별자를 반환 객체의 내용으로 반환합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

retrieveData에서 첨부 파일 반환

```
var MultiRunAttachVulnerabilityIntegration = Class.create();
MultiRunAttachVulnerabilityIntegration.prototype = Object.extendsObject(sn_vul.VulnerabilityIntegrationBase, {
    initialize: function() { },

    /**
     * Sample retrieveData() where fictional RESTMessage is executed and XML response body is
     * returned.  This call is paginated, so we need to figure out the range to pull
     * for each call.
     *
     * For simplicity, we'll say that a status code != 200 means we've reached the end of data
     * from the server, or if we cap out past our maxPages member variable.
     *
     */
    maxPages: 5,
    retrieveData: function() {
        var currentParams = this._getProcessParameters();
        var pageSize = 100;
        var page = 1;
        if (currentParams) {
            page = currentParams.page;
        }
        var message = new sn_ws.RESTMessageV2("My Vuln REST", "get");
        message.setQueryParameter("pageSize", pageSize);
        message.setQueryParameter("page", page);

        var table = this.integrationProcessGr.getTableName();
        var sysId = this.integrationProcessGr.getUniqueValue();
        var fileName = this.integrationProcessGr.getValue("number") + ".xml";
        message.saveResponseBodyAsAttachment(table, sysId, fileName);
        var response = message.execute();
        var responsSysId = response.getResponseAttachmentSysid();
        if (response.getStatusCode() != 200 || page >= this.maxPages) {
            this.hasMoreData(false);
            this.setNextRunParameters(null);
        } else {
            this.hasMoreData(true);
            this.setNextRunParameters({
                page: page + 1
            });
        }
        return {contents: responsSysId, contentType: "sys_attachment", extension: "xml"};
    },

    type: 'MultiRunAttachVulnerabilityIntegration'
});
```

프로세서 전략 보고

취약성 통합 양식의 프로세서 전략 보고 필드는 취약성 통합 프로세스가 실행될 때 취약성 통합 스크립트에서 반환된 데이터를 처리할 방법을 선택하는 데 사용됩니다.

기본값은 데이터 소스 첨부 파일입니다. 이 메서드는 검색된 데이터를 가져와서 시스템으로 임포트할 데이터 소스에 전달하는 기준선 구현입니다. 사용자 지정 보고서 프로세서를 선택하면 데이터 처리를 위한 사용자 지정 프로세서 스크립트를 선택할 수 있습니다.

데이터 소스 첨부 파일 보고서 프로세서 전략 사용

데이터 소스 첨부 보고서 프로세서 전략은 통합 스크립트에서 검색된 데이터를 구성된 데이터 소스에 전달하는 데 사용됩니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_write

프로시저

1. 다음으로 이동 모두 〉 취약성 〉 관리 〉 통합 을 클릭하고 새 통합을 생성합니다.
2. 보고서 프로세서 전략 필드에서 데이터 소스 첨부 파일을 선택합니다.
3. 양식 머리글을 마우스 오른쪽 버튼으로 클릭하고 저장을 클릭합니다.
4. 취약성 통합 데이터 소스 관련 목록에서 새로 만들기를 클릭합니다.
5. 사용할 데이터 소스를 정의합니다.
6. 제출을 클릭합니다.
7. 추가 데이터 소스가 필요한 경우 4-6단계를 반복합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

순서 필드에서 여러 데이터 소스가 정보를 보내는 순서를 지정해야 합니다.

8. 업데이트를 클릭합니다.

사용자 지정 보고서 프로세서 스크립트 정보

취약성 통합 양식에서 보고서 프로세서는 VulnerabilityReportProcessorBase 스크립트 포함을 확장하는 스크립트 포함에 대한 참조입니다. 이 스크립트에 포함된 기능은 VulnerabilityIntegrationController에 의해 호출되며 통합 스크립트에서 반환되는 데이터를 처리하는 방법을 정의합니다.

VulnerabilityReportProcessorBase의 각 하위 클래스는 호출 프로세스에 대한 컨텍스트 정보에 액세스할 수 있습니다. 이 정보는 다음 멤버 변수를 통해 사용할 수 있습니다.

- integrationGr — 통합 실행을 요청한 취약성 통합 기록의 GlideRecord입니다.
- integrationProcessGr — 통합의 현재 프로세스에 대한 컨텍스트 정보를 제공하는 취약성 프로세스의 GlideRecord입니다.

스크립트 포함은 processReport() 메서드에 대한 구현을 제공해야 합니다. processReport()에 전달된 객체는 retrieveData에 의해 반환된 객체이므로 content, contentType 및 extension에 대한 속성이 있는 간단한 객체입니다. processReport()의 실제 논리는 구현에 따라 다르며 제공된 보고서 데이터에 따라 다릅니다.

다음은 VulnerabilityReportProcessorBase.processReport()의 스크린샷입니다.

사용자 지정 보고서 프로세서 스크립트

```
/*
 * Processes the reportData that was pulled by a Vulnerability Integration's retrieveData().
 * The expectation is that retrieveData() will return an object that matches this function's input parameter.
 *
 * @param reportData = object with the following format:
 *
 * {
 *    contents: raw contents of data to process, usually a string.  If the integration creates an attachment
 *              this value should be the attachment sys_id.
 *    contentType: the mimeType of the content.  If the content is an attachment sys_id,
 *                 this should be sys_attachment.  The sys_attachment record itself should have the
 *                 content type specified.
 *    extension: the file extension that should be used for this content in the event the processor
 *               needs to write the contents to a file (such as a new attachment).
 * }
 *
 */
processReport: function(reportData) {
    return;
},
```

통합 공장 스크립트 필드

취약성 통합 양식에는 통합 공장 스크립트가 포함되며, 사용자 지정 보고서 프로세서 보고서 프로세서 전략을 선택한 경우, 프로세서 공장 스크립트가 포함됩니다. 이러한 필드는 각각 스크립트 포함 참조 필드, 통합 스크립트 및 보고서 프로세서로 정의된 객체를 실제로 인스턴스화하는 논리를 제공하는 데 사용됩니다.

스크립트 포함을 선택하면 두 필드 모두 인수가 없는 생성자 호출로 미리 채워집니다. 종종 이것으로 충분하지만 스크립트 객체를 인스턴스화하는 데 더 많은 논리가 필요한 경우가 있을 수 있습니다.

integrationProcessGr 기록은 필요에 따라 프로세스별 정보를 사용할 수 있도록 공장 스크립트 필드에 노출됩니다.

취약성 통합 수동 실행

에 대한 취약성 대응애플리케이션 취약성 대응 취약성 통합은 예약에 따라 실행되도록 구성됩니다. 그러나 필요한 경우 수동으로 실행할 수 있습니다.

시작하기 전에
필요한 역할:

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- sn_vul.read_integrations()취약성 대응
- sn_vul.app_read_integrations(애플리케이션 취약성 대응)

가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

이 태스크 정보
통합 실행 중에 여러 프로세스가 생성되고 데이터가 페이지 형식으로 수신됩니다. 각 프로세스에는 페이지에 첨부된 데이터가 있는 하나 이상의 임포트 큐 항목이 포함될 수 있습니다. 이러한 항목은 1시간의 시간 제한 내에 데이터를 처리해야 합니다. 그러나 페이로드 크기가 크면 처리 시간이 1시간을 초과하거나 중단되어 통합 시간 제한 오류가 발생할 수 있습니다. 통합은 시간 초과 오류에도 불구하고 데이터를 계속 처리합니다. 이러한 잘못된 통신을 피하기 위해 버전 18.2.4 취약성 대응부터 큐가 활성 상태이고 데이터를 처리하는지 여부를 나타내기 위해 타임스탬프(하트비트)가 주기적으로 전송됩니다. 임포트 큐 항목 페이지의 처리된 마지막 기록 필드는 임포트 큐가 생성하거나 업데이트하는 기록 수에 따라 업데이트됩니다. 임포트 큐 항목이 1시간의 시간 제한을 초과하는 경우, 시스템은 마지막으로 처리된 기록 필드를 검사하여 1시간보다 오래되었는지도 확인합니다. 이 경우 이는 임포트 큐 항목이 고착되었음을 나타내며 처리 시 더 이상의 지연을 방지하기 위해 시간 초과됩니다.

주:
마지막으로 처리된 기록 필드는 다음 시스템 속성에 정의된 내용에 따라 업데이트됩니다.

- *sn_sec_cmn.record_threshold_heartbeat*: 하트비트(타임스탬프)가 임포트 큐 항목으로 전송된 후 처리된 기록 수를 정의합니다.
- *sn_sec_cmn.maximum_heartbeat_delay*: 임포트 큐 항목을 시간 초과해야 하는 시간을 정의합니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 통합.
2. 실행할 통합에 대한 기록을 엽니다.
3. 지금 실행을 클릭합니다.

취약성 수동 수집

스캐너 결과를 기다릴 필요 없이 취약성을 신속하게 정정할 수 있도록 취약성을 취약성 대응 애플리케이션에 수동으로 수집합니다.

와 같은 Rapid7 외부 공급업체 스캐너는 취약성 데이터를 임포트하고 취약성 대응 처리하여 결과를 보고하는 데 도움을 줍니다. 수동 수집 통합을 사용하면 스캐너가 위험에 처한 자산을 보고할 때까지 기다리지 않고 사전 예방적으로 취약성을 수집하여 정정할 수 있습니다. 취약성을 수동으로 수집하면 제로 데이 익스플로잇과 같은 알려지지 않은 위협으로부터 자산을 효과적으로 보호할 수 있습니다.

취약성 수동 수집

다음 파일 형식으로 템플릿을 업로드하여 취약성 데이터를 임포트할 수 있습니다.

- Excel
- 쉼표로 구분된 값(CSV)

템플릿에 액세스하고 다운로드하려면 다음으로 이동하십시오. 모두 〉 취약성 대응 〉 수동 취약성 항목 수집 〉 업로드 파일 **UI**.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

템플릿에서 기록을 채우는 동안 다음 요점을 따라야 합니다.

- 심각도/상태 열 기록에서 입력 오류를 범하지 마십시오. 입력 오류가 있으면 기록을 건너뜁니다.
- 열 이름을 변경하지 마십시오.
- 첫 번째 행을 제외한 어떤 행에도 열 이름을 넣지 마십시오.
- 템플릿에서 Microsoft Excel 시트의 순서를 변경하지 마십시오. 취약성 데이터는 항상 두 번째 시트에 있어야 합니다.
- 입력 수동 탐지 시트를 제외한 모든 시트에 취약성 상세 정보를 넣지 마십시오.
- 대시(-), 마침표(.), 더하기(+), 밑줄(_), 공백, 대괄호 '(' ')' 및 at 기호(@)와 같은 영숫자 및 특수 문자를 제외한 다른 문자도 파일 이름에 사용하지 마십시오.

템플릿의 데이터를 채우는 방법에 대한 지침은 다음 문서를 참조하십시오 취약성 수동 수집을 위한 템플릿.

의 취약성 대응v24.0.6부터 템플릿에 Microsoft Excel 추가 열을 만들 수도 있습니다. 자세한 내용은 KB1646630 문서를 참조하십시오.

수동 수집 통합

통합은 파일이 업로드될 때 트리거됩니다. 업로드된 파일의 유형에 따라 관련 통합이 트리거됩니다.

통합을 보려면 다음으로 이동합니다. 모두 〉 취약성 대응 〉 수동 취약성 항목 수집 〉 통합.

기본적으로 다음과 같은 기본 시스템 수동 수집 통합을 사용할 수 있습니다.

통합

통합 유형	설명
수동 수집 Excel 통합	취약성 수집 푸시 큐 테이블에서 업로드된 최신 Microsoft Excel 파일을 가져와 데이터를 검색하고 해당 통합 실행에 첨부 파일을 복사합니다.
수동 수집 CSV 통합	취약성 수집 푸시 큐 테이블에서 업로드된 최신 CSV 파일을 가져와 데이터를 검색하고 해당 통합 실행에 첨부 파일을 복사합니다.

수동 수집 외부 공급업체 통합은 기본적으로 다음 두 개의 통합 인스턴스 매개변수를 사용하여 통합 인스턴스를 생성합니다.

- max_input_records: 템플릿에서 만들 수 있는 기록 수를 정의합니다. 이 매개변수에 지정된 것보다 많은 기록을 추가하는 경우 추가 기록은 건너뜁니다. 값 열에서 업데이트할 수 있는 기록 수입니다. 템플릿에서 권장되는 기록 생성 수는 1,000개입니다. 이 값을 초과하면 성능 문제가 발생할 수 있습니다.
- insert_fixed: 수정된 취약성 탐지를 임포트합니다.

통합 인스턴스 매개변수를 보려면 다음으로 이동합니다. 모두 〉 취약성 대응 〉 수동 취약성 항목 수집 〉 통합 을 클릭하고 통합의 소스 인스턴스를 클릭합니다. 또는 다음으로 이동할 수 있습니다. 모두 〉 취약성 대응 〉 통합 인스턴스 을 클릭하고 수동 수집을 클릭합니다.

취약성을 수동으로 수집

취약성 데이터가 있는 템플릿을 업로드하여 취약성을 수동으로 수집합니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 수동 취약한 항목 수집 〉 업로드 파일 **UI**.
2. Excel 또는 CSV 링크를 클릭하고 해당 형식으로 템플릿을 다운로드합니다.
3. 템플릿에서 레코드의 취약성 데이터를 입력합니다.
   템플릿의 데이터를 채우는 방법에 대한 지침은 다음 문서를 참조하십시오 취약성 수동 수집을 위한 템플릿.
4. 파일 임포트를 클릭하고 업데이트된 템플릿을 업로드합니다.
5. 제출을 클릭합니다.
   취약성 통합 푸시 큐 페이지가 표시됩니다. 통합 인스턴스 목록, 통합 실행 상태, 통합 실행이 완료된 후의 로그 메모를 볼 수 있습니다.

다음에 수행할 작업

파일을 업로드한 후 모두 〉 취약성 대응 〉 수동 취약한 항목 수집 〉 통합. 통합 실행이 성공했는지 확인합니다.

수동 통합 실행 확인

통합 실행이 성공했는지 확인합니다. 통합 실행으로 인해 생성되거나 업데이트된 개별 탐지 및 VI(취약한 항목) 수를 봅니다.

시작하기 전에

필요한 역할: sn_vul.vulnerability_admin

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 수동 취약한 항목 수집 〉 통합.
2. 업로드된 파일 형식을 기준으로 통합의 이름을 클릭합니다.
3. 취약성 통합 실행 탭을 클릭합니다.
4. 통합 실행 번호를 클릭합니다.
5. 항목 탭을 클릭합니다.
6. 항목 탭의 정보를 검토합니다.

항목 탭

탭/필드	설명
항목 탭	임포트된 VI의 총 수를 표시합니다. 탐지 탭에 나열된 숫자를 추가하여 임포트한 총 탐지를 볼 수 있습니다.
새 항목	이 통합 실행에서 생성된 취약한 항목 수를 표시합니다.
임포트한 항목	이 섹션에 있는 모든 필드의 합계를 표시합니다.
중복 항목	중복 항목을 표시합니다. 이 필드는 더 이상 채워지지 않습니다.
업데이트된 항목	이 통합 실행 중에 취약한 항목이 업데이트된 횟수를 표시합니다. 이 값은 업데이트되는 고유한 취약한 항목 수가 아닙니다. 예를 들어 통합 실행 중에 취약한 항목이 두 번 업데이트되면 두 번 계산되어 2 개의 업데이트된 항목으로 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

탭/필드	설명
변경되지 않은 항목	데이터베이스에 있지만 관련 필드 값이 변경되지 않았기 때문에 업데이트되지 않은 통합 실행 중에 발견된 취약한 항목을 표시합니다.

다음에 수행할 작업
통합 실행이 성공적으로 실행되었는지 확인한 후 모두 〉 취약성 대응 〉 수동 취약한 항목 수집 〉 파일 이력 업로드. 메모에서 실패한 기록이 있는지 확인합니다.

수동 탐지 자동 종결 구성

수동 탐지 자동 종결을 활성화하여 오래된 수동 탐지를 자동으로 종결합니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 수동 취약한 항목 수집 〉 업로드 파일 **UI**.
2. **Change Auto-Close** Configuration(자동 종결 구성 변경)을 클릭합니다.
3. 수동 탐지 탭을 클릭합니다.
4. 수동 탐지 자동 종결 확인란이 선택되어 있는지 확인합니다.
5. 마지막으로 발견된 수동 탐지(일 전) 필드에 수동 탐지를 종결해야 하는 일 수를 입력합니다. 기본값은 90일입니다. 일수에 대한 양수 값을 입력할 수 있습니다.

업로드 상태 확인

취약성 통합 실행이 성공했는지, 부분적으로 성공했는지, 실패했는지 확인합니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 수동 취약한 항목 수집 〉 파일 이력 업로드.
2. 취약성 통합 푸시 큐 테이블의 생성됨 열과 상태 열에서 각각 업로드 시간과 업로드 상태를 확인합니다.
3. 옵션: 메모 필드에서 실패의 이유를 봅니다.

취약성 수동 수집을 위한 템플릿

이 템플릿은 취약성 및 CI(구성 항목) 데이터로 채워야 하는 열을 제공합니다. 템플릿이 채워지고 업로드되면 데이터가 처리됩니다.

템플릿 채우기 지침

템플릿에 세부 정보를 입력하려면 다음 테이블에 제공된 지침을 따릅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

템플릿 지침

열	필수/선택 사항?	문자열 길이(최대)/유효한 값	설명
자산 ID	옵션	255	UUID(범용 고유 식별자) 또는 자산 ID입니다. 스캐너에서 생성된 값일 수 있습니다.
다음 5개 열 중 최소 1개 열에 정보를 입력합니다.			
MAC 주소	필수	24	호스트 또는 자산 정보입니다. 제공된 모든 값의 조합은 자산에 대해 고유해야 합니다.
FQDN	필수	255	
NETBIOS	필수	255	
IP 주소	필수	255	
호스트 이름	필수	255	
나머지 열은 서로 종속되지 않습니다.			
취약성 ID	필수	255	NVD(국가 취약성 데이터베이스)의 취약성 또는 외부 공급업체 스캐너에서 반환된 ID를 나타냅니다.
취약성 요약	옵션	512	취약성에 대한 간략한 설명입니다. 취약성 ID를 사용할 수 없는 경우에만 데이터베이스에 추가됩니다.
심각도	옵션	심각, 높음, 중간, 낮음, 없음	취약성의 심각도입니다. 취약성 ID를 사용할 수 없는 경우에만 데이터베이스에 추가됩니다. 기록이 비어 있으면 기본적으로 중요한 것으로 간주됩니다.
포트	옵션	해당 사항 없음	취약성이 탐지된 포트입니다. 값은 올바른 정수여야 합니다. 잘못된 입력이 있으면 기록을 건너뜁니다.
프로토콜	옵션	40	사용된 네트워크 프로토콜의 유형입니다.
증명	옵션	4000	취약성의 위치 또는 시스템 경로를 나타냅니다.
상태	옵션	열림, 고정됨	탐지 상태입니다. 기록이 비어 있으면 기본적으로 오픈된 것으로 간주됩니다.

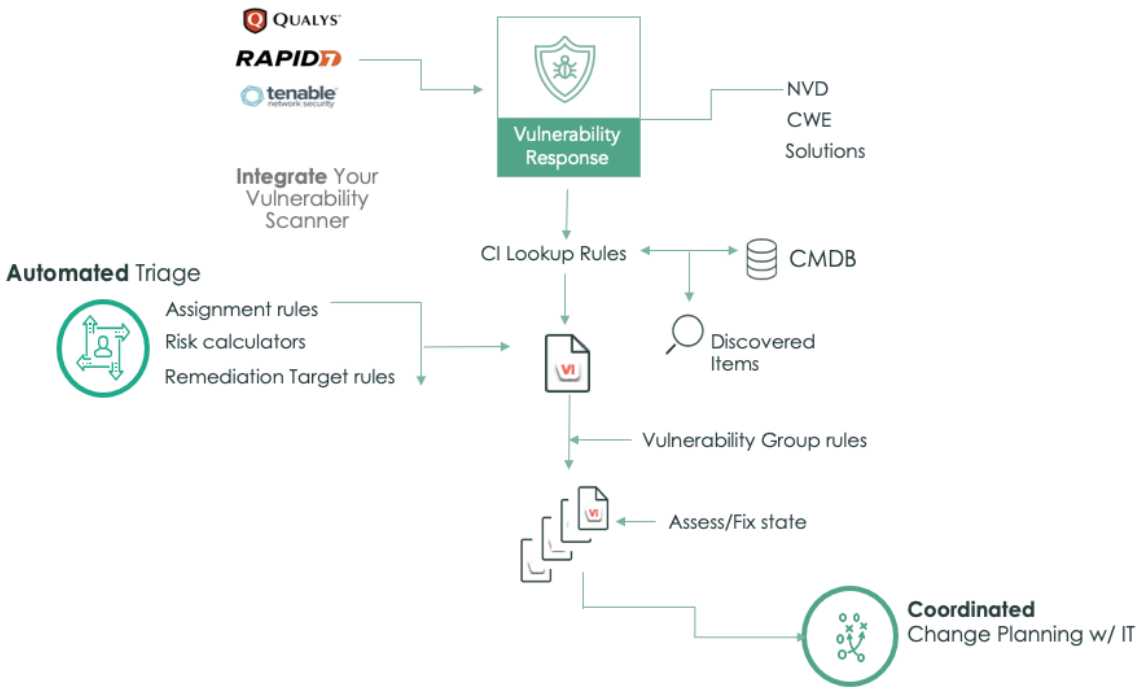
취약성 대응 정정 개요

취약성 대응 정정은 임포트 완료 확인, 새로운 취약성 분류, 완료 진행률 모니터링으로 구성된 단계별 프로세스입니다. 이러한 방식으로 접근하면 개선을 관리할 수 있고 시기적절하며 여러 면에서 자동화됩니다.

회사 자산 전반의 보안 태세를 이해하면 정정할 가장 중요한 취약성을 식별하는 데 도움이 됩니다. 이 정정 프로세스에는 및 설치 Qualys Vulnerability Integration 되고 구성된 것과 같은 외부 공급업체 통합이 필요합니다취약성 대응.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약성 대응 통합 프로세스 흐름



외부 공급업체 통합 임포트가 성공적으로 완료되었는지 확인

이 프로세스의 첫 번째 단계는 모든 것이 올바르게 작동하는지 확인하는 것입니다. 취약성 대응 NVD(국가 취약성 데이터베이스) 및 CWE(일반적인 열거형 약점) 취약성을 다운로드하도록 사전 설정되어 있습니다. 외부 공급업체 임포트는 취약한 항목 및 정정 작업을 생성하는 데 필요한 데이터를 제공합니다. 성공적인 정정은 취약성 및 취약한 항목을 일관되고 성공적으로 임포트하는 데 달려 있습니다.

임포트하는 동안 CI 조회 규칙은 외부 공급업체 자산을 구성 관리 데이터베이스(CMDB). 모든 자산은 검색된 항목 모듈에 저장됩니다. CI 정보는 솔루션 구현에 매우 중요합니다.

주:
외부 공급업체 통합이 설치되고 구성된 후에는 외부 공급업체 공급업체가 API 호출을 제한하는 경우와 같이 임포트에 실패할 수 있는 인스턴스가 거의 없습니다. 수입이 실패하면 즉각적인 주의가 필요합니다.

지원되는 외부 공급업체 통합에 대한 통합 상태 실행 보고서가 애플리케이션과 함께 제공되어 임포트에 대한 그래픽 개요를 제공합니다. 이 보고서를 사용하거나 직접 작성하여 최근 임포트의 성공 여부를 손쉽게 확인할 수 있습니다. 지원되는 통합에 대한 자세한 내용은 다음 문서를 참조하십시오 취약성 대응 통합.

취약성 및 취약한 항목 검토 및 분류

정정의 다음 단계에서는 새로운 취약성 및 취약한 항목을 검토해야 합니다. VI(취약한 항목)는 취약성과 CI(구성 항목)의 감지된 조합입니다. 취약한 항목이 형성되면 VI를 할당하고, VI의 위험을 파악하고, 정정 대상을 설정하는 다양한 규칙이 실행됩니다. 필요한 경우 규칙을 조정하여 취약한 항목을 성공적으로 분류합니다.

기존 취약성 정정 진행 상황 모니터링

정정의 마지막 단계는 진행률 모니터링으로 구성됩니다.

- 표시되지 않은 패치 구현에 대한 임포트 상태를 검토하고 IT 운영을 후속 조치합니다.
- 규정 준수 의무의 진행 상황을 추적하고 완료되었는지 확인합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 지연된 항목 상태를 검토하고 수정을 수정하거나 구현합니다.
- 취약성 관리 대시보드를 모니터링합니다. 추세를 검토하고, 실시간으로 보고서를 보고, 정정 목표 달성률을 추적하는 메트릭을 사용하려면 for Vulnerability Response 애플리케이션을 사용하여 퍼포먼스 분석 프로세스를 모니터링하는 것이 좋습니다.
- 에서 부실 탐지 종결 취약성 대응.

통합 임포트가 성공적으로 완료되었는지 취약성 대응 확인

임포트의 성공 여부를 확인하는 가장 쉬운 방법은 통합 실행 상태 대시보드를 사용하는 것입니다. 통합 실행 상태 대시보드는 외부 공급업체 통합 실행 상태에 대한 그래픽 뷰의 예를 제공합니다.

및 QualysRapid7 취약성 통합에는 통합 실행 상태 대시보드가 있습니다. 차트 내용에 대한 자세한 내용은 을 Rapid7 취약성 통합 상태 차트 실행 참조하십시오Qualys 통합 실행 상태 차트.

주:
에서 제공하지 ServiceNow#않는 통합의 경우 차트는 대시보드의 보고서에서 생성할 수 있지만 전문 지식이 필요할 ServiceNow 수 있습니다. 보고서 및 대시보드 생성에 대한 자세한 내용은 보고서 및 대시보드 시작하기 를 참조하십시오.

취약한 항목 탐지 데이터 보기 취약성 대응

와 취약성 대응 외부 공급업체 스캐너 통합으로 수집된 전체 데이터는 취약한 항목 기록(VIT)의 탐지 및 초기 탐지 탭에 표시됩니다. 인스턴스의 취약한 항목 탐지 목록에 ServiceNow AI Platform# 있는 탐지 기록에도 표시됩니다.

시작하기 전에

외부 공급업체 통합은 취약한 항목 탐지 데이터를 검색합니다. 탐지는 스캐너에서 보고되는 취약성의 명백한 발생입니다. 탐지 데이터는 취약한 항목과 쌍을 이루고 탐지 상태에 따라 VI 상태가 업데이트됩니다. VI를 찾을 수 없는 경우 새 VI가 생성됩니다. 탐지는 스캐너에서 직접 찾은 데이터에 의해서만 열리거나 닫힙니다.

필요한 역할:

- sn_vuln.admin은 통합 실행을 시작하고 취약한 항목 탐지 데이터를 봅니다.
- sn_vul.remediation_owner는 취약한 항목 탐지에서 생성된 취약한 항목을 할당받고 VI 기록에 대한 데이터를 봅니다.

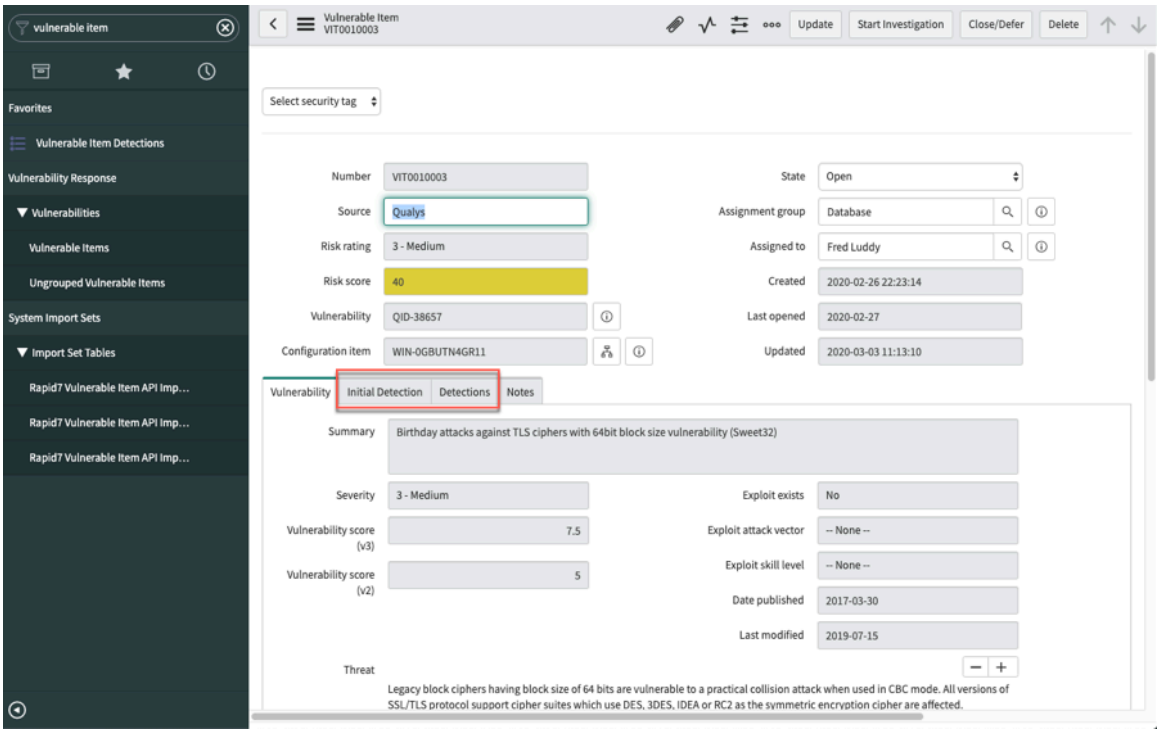
프로시저

1. 취약한 항목 탐지 데이터를 보려면 취약한 항목 기록으로 이동하여 엽니다.

   기록이 초기 탐지 및 탐지 탭과 함께 표시됩니다.

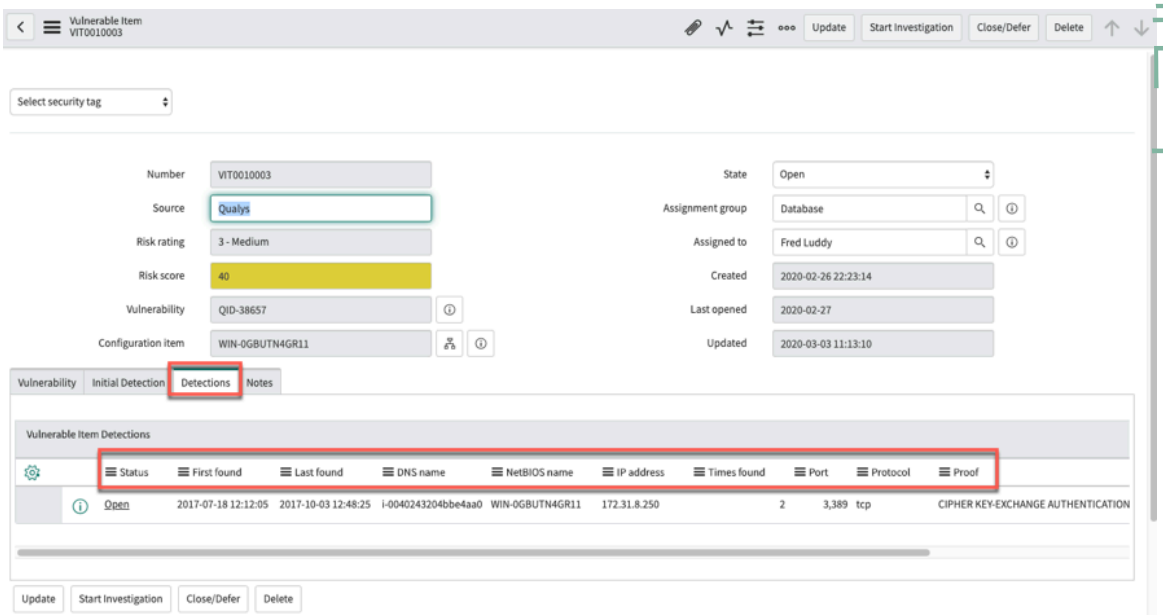
   주:
   이전에 구성 상세 정보 탭에 표시된 데이터가 초기 탐지 및 탐지 탭에 다른 탐지 데이터와 함께 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



2. 탐지 탭을 클릭합니다.

외부 공급업체 검사 결과에서 취약한 항목이 생성되면 다음 그림과 같이 검사 데이터가 탐지 기록에 표시됩니다.



취약한 항목 탐지 섹션의 각 행은 개별 탐지의 데이터를 나타냅니다. 처음 발견 열에는 스캐너에서 취약한 항목을 처음 탐지한 날짜가 표시됩니다. 마지막 발견 열에 가장 최근 탐지 날짜가 표시됩니다. 소스 필드에는 데이터를 검색한 스캐너가 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
의 경우 Qualys취약한 항목 탐지가 있는 경우 다음 필드는 VI 기록에서 사용되지 않으며 더 이상 채워지지 않습니다.

- Qualys 심각도
- 소스에서 마지막으로 업데이트됨

Qualys또한 앞의 그림과 같이 스캔에서 VI가 생성되면 결과에 대한 스캔의 값이 탐지 레코드의 증명 열에 표시됩니다. 그러나 이 값은 VI 레코드의 위쪽 부분에 표시되지 않습니다.

Rapid7의 경우 스캔에서 VI가 생성되면 스캔의 증명 값을 탐지 레코드의 증명 열과 VI 레코드의 상단 부분에 모두 표시할 수 있지만 기본 설정은 아닙니다. 이 값을 VI 기록의 상단 부분에 표시하려면 양식 레이아웃에서 증명 필드를 선택합니다.

3. 옵션: 기록에서 탐지 탭의 레이아웃을 구성하려면 다음 단계를 수행합니다.

a. 기본적으로 탐지 탭에 다음 열이 표시됩니다.

- 상태
- 첫 발견(데이터)
- 마지막 발견(날짜)
- DNS 이름
- 순 BIOS이름
- IP 주소
- 발견 시간
- 포트
- 프로토콜
- 증명
- SSL

주:

(Optional) 참고: 열에 값이 없으면 해당 필드에 대한 데이터가 스캐너에 의해 탐지되지 않은 것입니다.

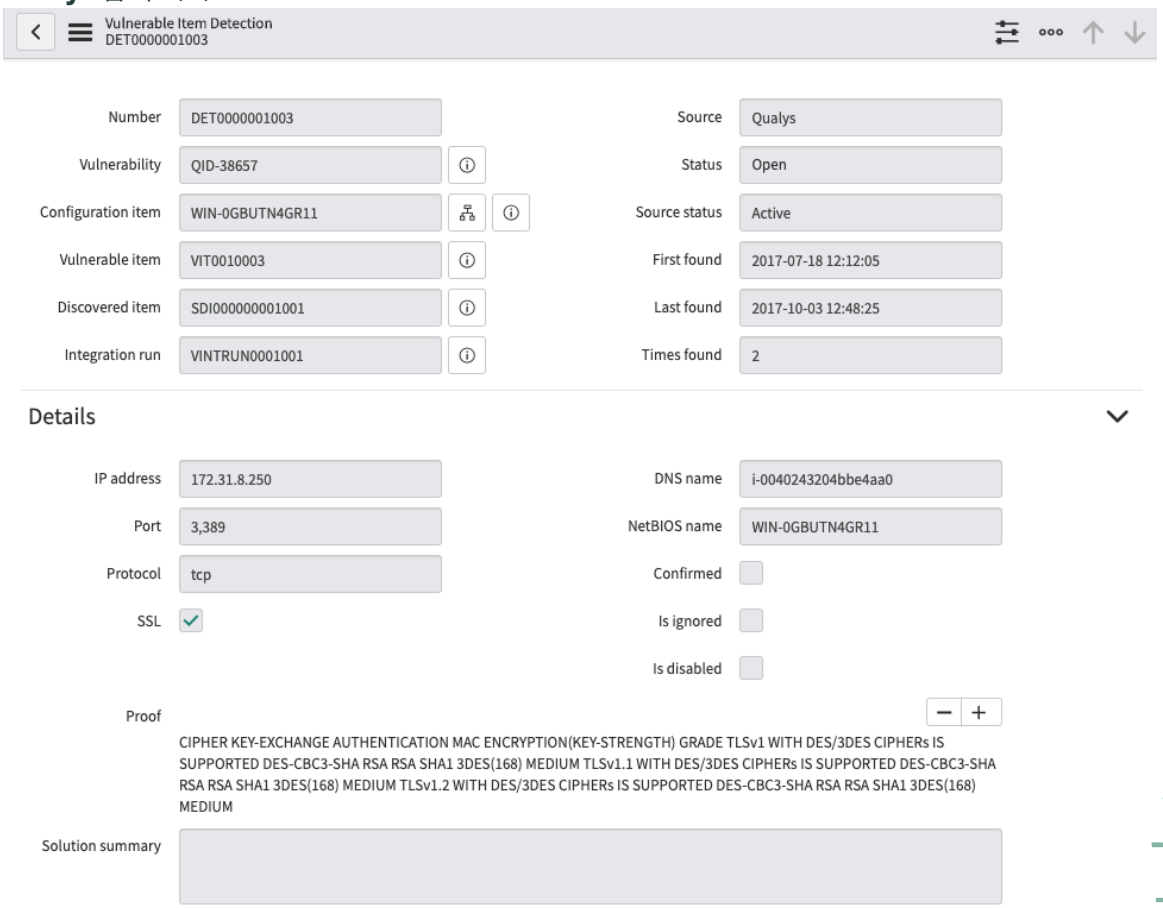
b. 기어 아이콘( )을 클릭하여 뷰를 개인화합니다.

c. 슬러쉬버킷에서 특정 데이터를 표시할 열을 선택하고 확인을 클릭합니다.

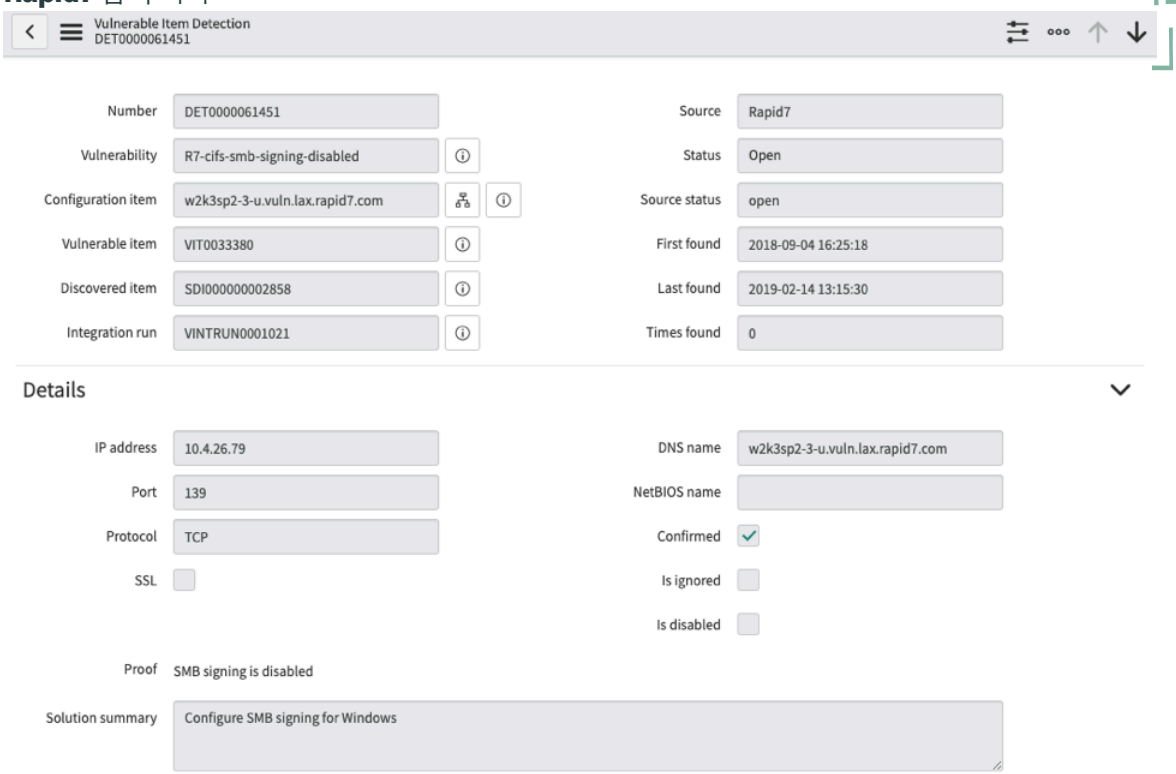
4. 탐지 탭을 선택한 상태의 상태 열에서 항목을 클릭하여 탐지 기록을 열고 솔루션 요약(Rapid7 InsightVM 통합만 해당)을 포함하여 취약한 항목과 연결된 상세 정보를 봅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Qualys 탐지 기록



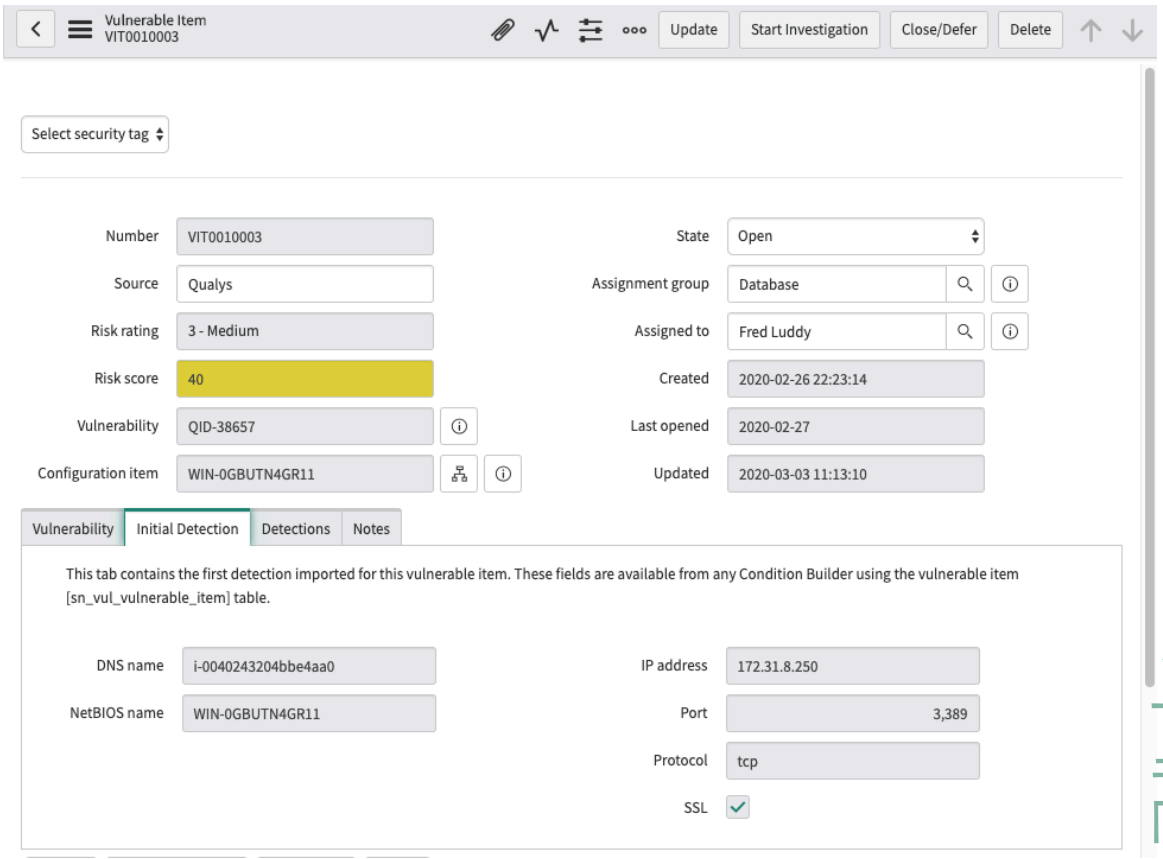
Rapid7 탐지 기록



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

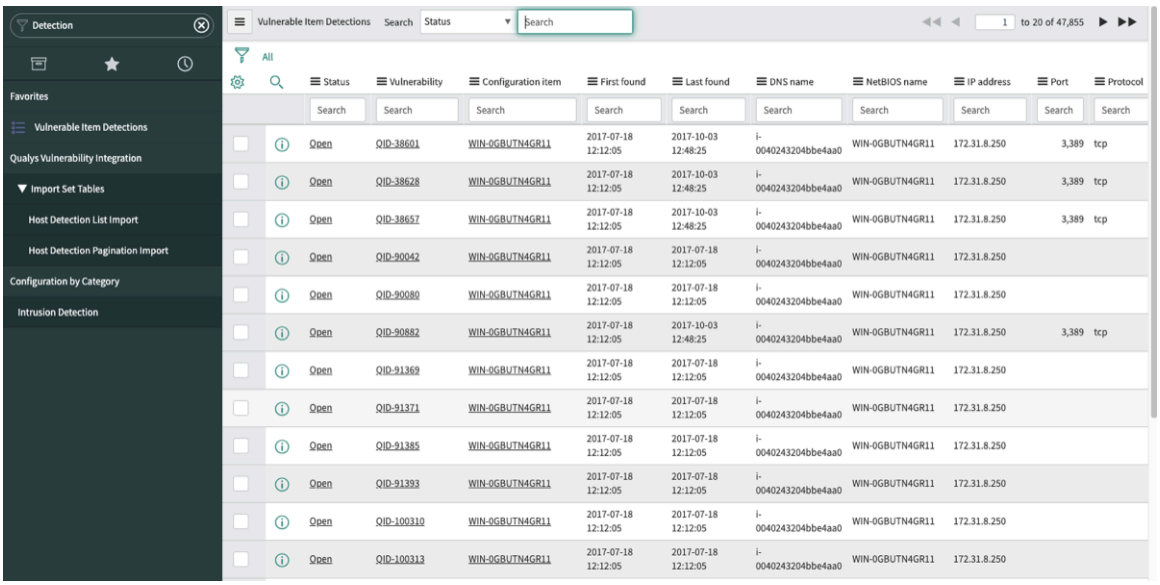
5. 기록으로 돌아가서 초기 탐지 탭을 선택합니다.

초기 탐지 탭에는 탐지가 처음 발생할 때 외부 공급업체 스캐너에서 임포트한 데이터가 표시됩니다. 초기 탐지 탭의 이 정보는 탐지 데이터가 업데이트될 때 변경되지 않습니다.



6. 옵션: 취약한 항목 탐지 목록을 보려면 취약한 항목 탐지로 이동합니다.

(Optional) 취약한 항목 탐지 목록이 표시됩니다. 취약한 항목 탐지 목록의 각 행은 고유한 탐지를 나타냅니다. 열에는 VI 레코드와 동일한 데이터가 표시됩니다.



탐지는 스캐너에서 찾은 데이터에 의해서만 열리거나 닫히며 VI에서 롤다운되지 않습니다. 감지를 가져오면 VI를 생성하고 VI의 상태를 업데이트하는 데 사용됩니다. 취약한 항목에 대한

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모든 탐지가 종결되면 해당 취약한 항목도 종결됩니다. VI 기록에서 상태는 ##되고 하위 상태는 ##입니다.

주:
오류는 다음과 같은 경우에 기록됩니다.

- 스캐너에서 검색된 첨부 파일 처리 중
- 탐지 또는 취약한 항목을 생성하거나 업데이트합니다.

탐지 오류 처리에 대한 자세한 내용은 다음 문서를 참조하십시오 탐지를 위한 오류 처리.

정정 작업에 대해 모든 VI가 닫히면 정정 작업이 종결됩니다.

하위 상태가 고정 또는 부실 인 종결된 VI는 새로운 탐지가 생성되고 VI를 새로운 취약성과 일치시킬 수 있는 경우 다시 열립니다.

인스턴스에서 해결됨 으로 설정되었지만 후속 통합 실행에 의해 종결/수정 됨으로 전환되지 않은 취약한 항목은 재스캔 중에 탐지되면 다시 열립니다.

정정 작업에 대해 모든 VI가 종결되면 기록이 종결됩니다.

인스턴스에서 "해결됨"으로 설정되었지만 후속 통합 실행에 의해 "종결/수정됨"으로 전환되지 않은 취약한 항목은 재스캔 중에 탐지되면 다시 열립니다.

탐지의 경우 Rapid7 , 이제 인스턴스의 Rapid7 구성 페이지에서 해결된 VI를 기간별로 다시 여는 옵션을 사용할 수 있습니다. 활성화된 경우 VI가 해결됨 으로 설정되었지만 후속 스캔에 의해 종결/수정 으로 전환되지 않고 입력한 날짜 수가 지나면 다시 열림 으로 전환됩니다.

탐지의 경우 Qualys 스캐너가 '해결됨'으로 설정되었지만 후속 스캔에서 종결/수정 으로 전환되지 않은 VI를 계속 찾으면 마지막으로 발견된 날짜가 해결 날짜보다 나중일 때 이러한 VI가 다시 열림 으로 이동합니다.

다음에 수행할 작업

항목 및 탐지 횟수를 포함하여 더 많은 데이터를 보려면 다음을 수행하면 됩니다 통합 실행 (VINTRUN) 기록에서 취약한 항목 탐지 데이터 확인 취약성 대응.

통합 실행**(VINTRUN)** 기록에서 취약한 항목 탐지 데이터 확인 취약성 대응

인스턴스의 통합 실행 기록 ServiceNow AI Platform# 에서 스캔 날짜 및 시간을 기준으로 외부 공급업체 통합 취약한 항목 탐지 데이터를 찾을 수 있습니다. 스캔이 성공적으로 완료되었는지 확인하고, 개별 탐지 수(개수)뿐만 아니라 스캔 결과로 직접 생성되거나 업데이트된 취약한 항목(VI)도 봅니다.

시작하기 전에

필요한 역할: sn_vul.vulnerability_admin 또는 sn_vuln.admin(사용하지 않음)
가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

다음 목록에서 특정 기록을 찾는 데 도움이 되도록 통합 실행 정보(검사 날짜 및 시간 또는 취약한 항목 또는 탐지 기록의 통합 실행 기록 번호(VINTRUN#))를 제공하는 것을 선호할 수 있습니다.

프로시저

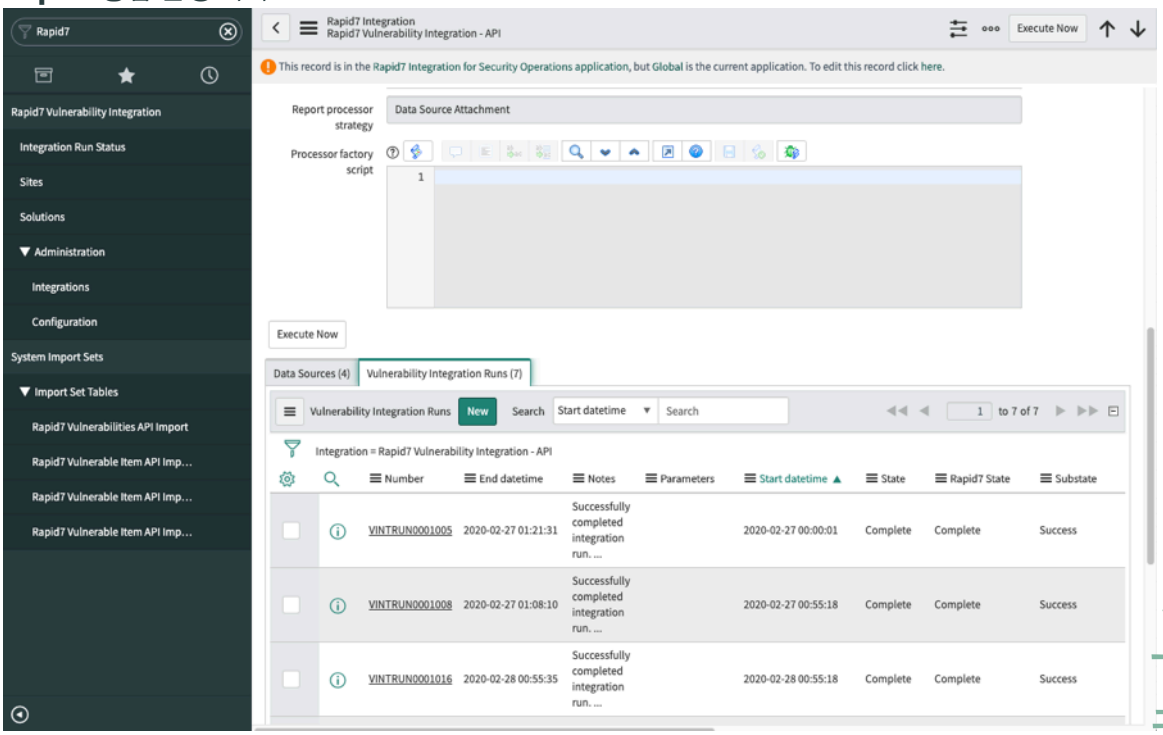
1. 계속하려면 하나를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

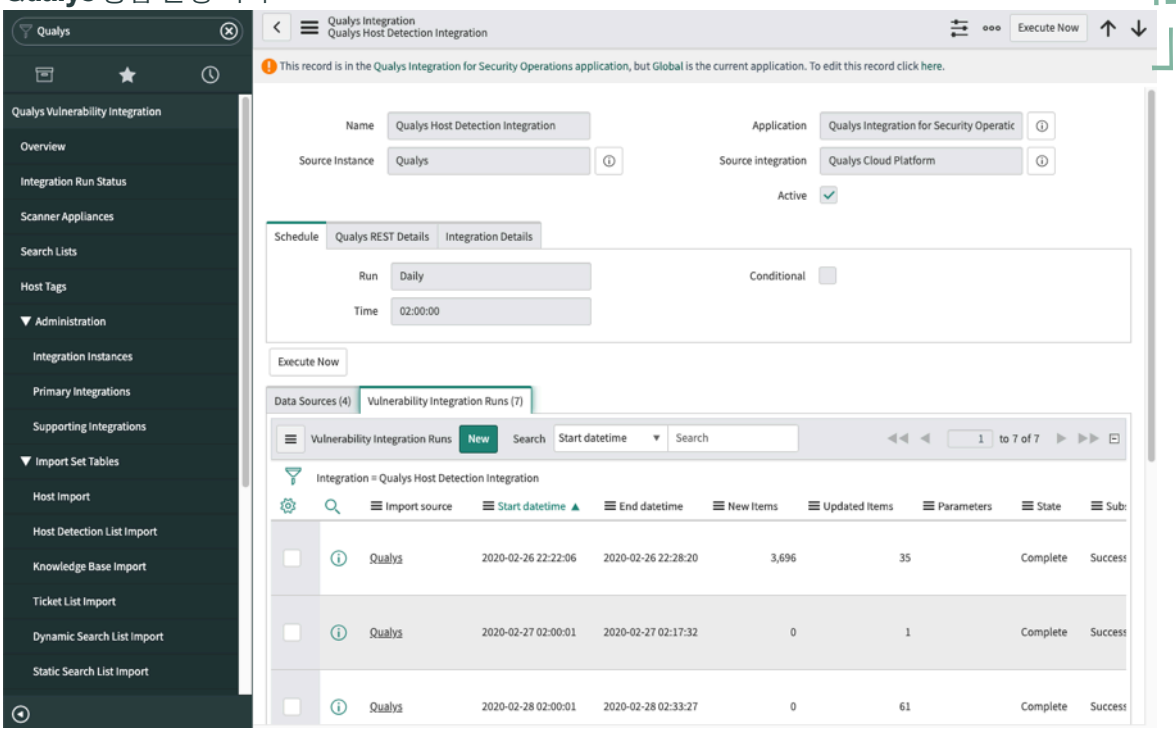
2. 표시되는 페이지 아래쪽에서 취약성 통합 실행 탭을 클릭합니다.
3. 번호 또는 임포트 소스 열에서 항목을 클릭하여 기록을 엽니다.

   통합 실행 기록이 표시됩니다.

Rapid7 통합 실행 기록

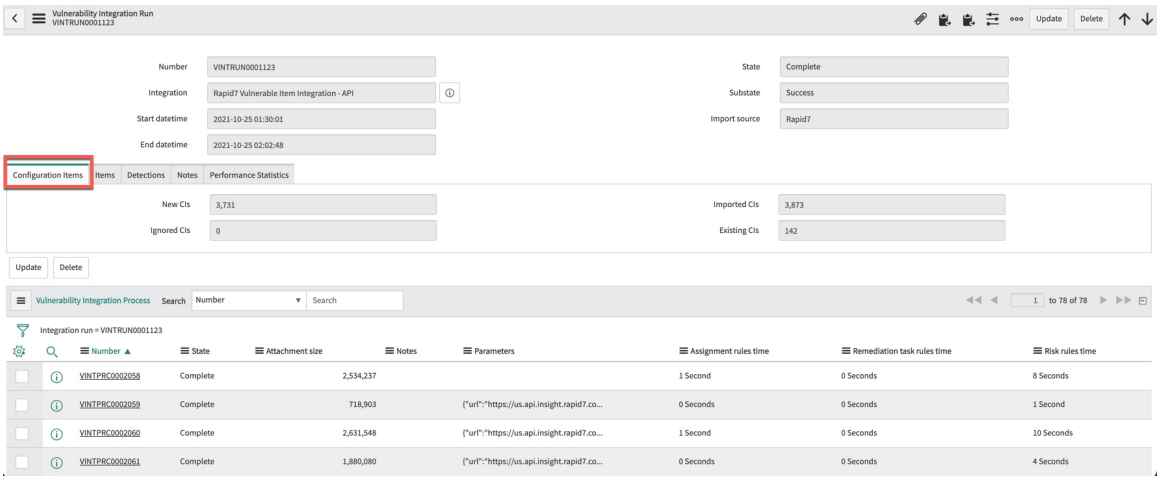


Qualys 통합 실행 기록



통합 실행 기록이 표시됩니다. 상태 필드에서 통합이 성공적으로 실행되었는지 확인할 수 있습니다. 구성 항목 탭을 선택합니다.

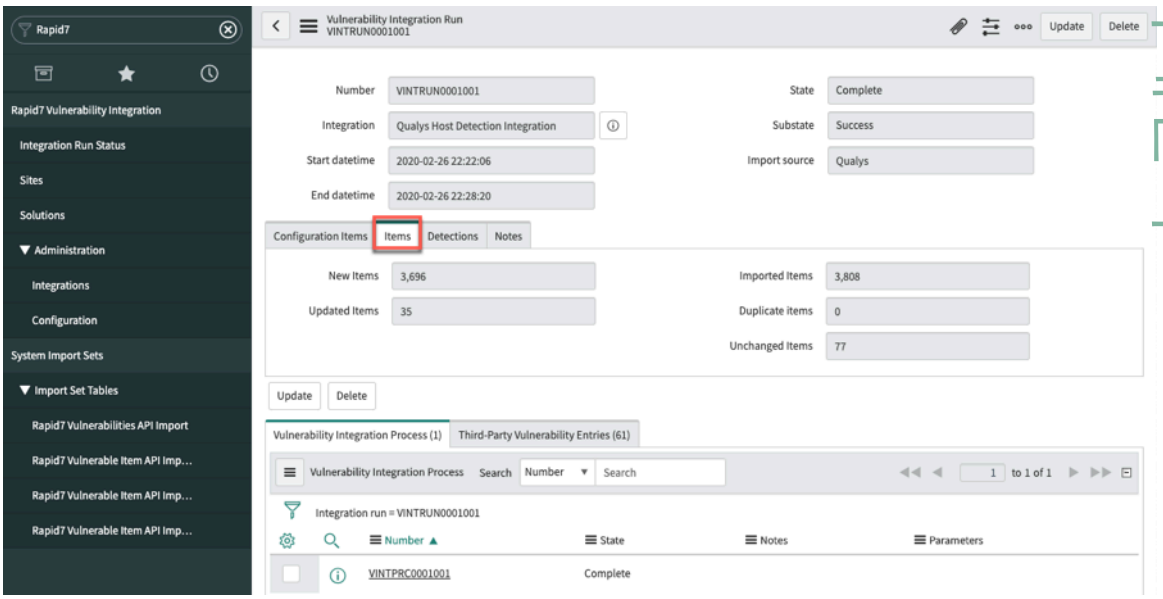
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



구성 항목 탭에는 다음 정보가 표시됩니다.

- 구성 항목 탭에는 임포트된 구성 항목의 총 수가 표시됩니다.
- 새 CI 필드에는 이 통합 실행의 일부로 생성된 CI 수가 표시됩니다.
- 임포트한 CI 필드에는 이 섹션에 있는 모든 CI의 합계가 표시됩니다.
- 무시된 CI 필드의 값은 통합에서 취약성 대응 항상 0입니다.
- 기존 CI 필드에는 이미 존재하는 CI의 총 수가 표시됩니다.

항목 탭을 클릭합니다.



항목 탭에는 다음 정보가 표시됩니다.

- 항목 탭에는 임포트된 VI의 총 개수가 표시됩니다. 탐지 탭에 나열된 숫자를 추가하여 임포트한 총 탐지를 볼 수 있습니다.
- 새 항목 필드에는 이 통합 실행에서 생성된 취약한 항목 수가 표시됩니다.
- 임포트한 항목 필드에는 이 섹션에 있는 모든 필드의 합계가 표시됩니다.
- 중복 항목 필드가 더 이상 채워지지 않습니다.

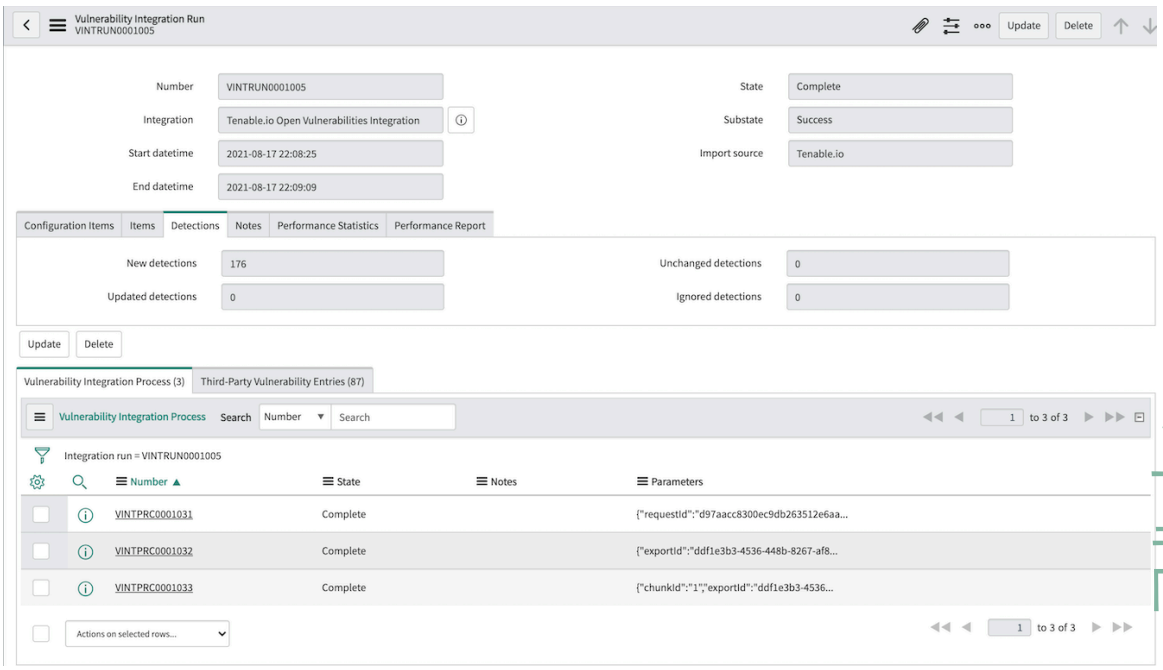
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 업데이트된 항목 필드에는 이 통합 실행 중에 취약한 항목이 업데이트된 횟수가 표시됩니다. 이 값은 업데이트되는 고유한 취약한 항목 수가 아닙니다. 예를 들어 통합 실행 중에 취약한 항목이 두 번 업데이트되면 두 번 계산되어 2 개의 업데이트된 항목으로 표시됩니다.
- 변경되지 않은 항목 필드에는 데이터베이스에 이미 있지만 관련 필드 값이 변경되지 않았기 때문에 업데이트되지 않은 통합 실행 중에 발견된 취약한 항목이 표시됩니다.

4. 탐지 탭을 클릭합니다.

이 탭은 통합 실행에 탐지가 있는 경우에만 표시됩니다. 나열된 숫자를 추가하여 임포트한 총 탐지 수를 확인할 수 있습니다.

VR v15.0의 탐지 탭



주:
v15.0 이전에는 무시된 탐지에 대한 필드가 없었습니다.

탐지 탭에는 다음 정보가 표시됩니다.

- v15부터는 이전에 무시되었던 탐지를 추적하기 위해 새 필드 무시된 탐지가 추가되었습니다. 이 구현을 사용하면 임포트된 탐지 개수와 통합 실행 기록에서 추적되는 개수가 일관성을 갖게 됩니다. 이 기능은 모든 스캐너 Qualys Vulnerability Integration(예: , Rapid7 취약성 통합, Tenable Vulnerability IntegrationMicrosoft 및 TVM)에 대해 구현되었습니다.
- 새 탐지 필드에는 이 통합 실행 중에 생성된 새 탐지가 표시됩니다.
- 변경되지 않은 탐지 필드에는 데이터베이스에 이미 존재하지만 관련 필드 값이 변경되지 않아 업데이트되지 않은 통합 실행 중에 발견된 탐지가 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 업데이트된 탐지 필드에는 이 통합 실행 중에 탐지가 업데이트된 횟수가 표시됩니다. 이 값은 업데이트된 고유 탐지 수가 아닙니다. 예를 들어 통합 실행의 일부로 탐지가 두 번 업데이트되면 두 번 계산되어 2 개의 업데이트된 탐지로 표시됩니다.

  주:
  이 개수에 표시되지 않는 탐지는 기존 VI를 업데이트하는 데 고정 기록이 사용되기 때문에 종결된 상태(고정)의 탐지입니다. 이같은 탐지 기록에 대한 가시성을 높이려면 열린 상태에서 일치하는 기존 VI가 없을 때 생성된 종결된 VI를 표시할 수 있습니다. Qualys 통합을 위해 설정 도우미에서 활성화할 수 있는 고정 상태의 취약성에 대한 자세한 내용은 다음 문서를 참조하십시오 설정 지원을 사용하여 구성 취약성 대응 하기.

5. 번호 또는 임포트 소스 열에서 항목을 클릭하여 기록을 엽니다.

에서 패치 데이터 보기 및 패치 스케줄링 취약성 대응

v16.1 부터취약성 대응는 클래식 환경과 인스턴스의 작업 공간 모두에서 패치의 일정을 예약하고 기록에 대한 솔루션 및 기타 취약성 정보와 함께 패치 데이터를 볼 수 ServiceNow AI Platform 있습니다취약성 대응.

필요한 역할

사용자는 데이터를 보고 패치를 예약하기 위해 패치를 임포트하는 데 사용 중인 패치 오케스트레이션 통합과 관련된 역할이 필요합니다. 자세한 내용은 지원되는 통합을 참조하십시오.

- 와 HCL BigFix 패치 오케스트레이션의 통합 이해 취약성 대응 및 SCCM 취약성 대응 과의 Microsoft 패치 오케스트레이션 통합 이해.
- 대시보드에서 취약성 대응 패치 오케스트레이션 데이터 보기 클래식 환경에서.
- 에서 취약성 대응 작업 공간성과표의 데이터를 봅니다.

패치 일정 예약

다음 기록에서 패치를 예약할 수 있습니다.

- 패치 업데이트(VPU)
- 정정 작업(RT)
- 검색된 항목(SDI)

클래식 환경에서 데이터 패치

애플리케이션의 클래식 환경에서 취약성 대응 :

- 패치 업데이트 기록을 보려면 다음으로 이동하십시오. 모두 〉 취약성 대응 〉 패치.
- 솔루션을 보려면 다음으로 이동하십시오. 모두 〉 취약성 대응 〉 솔루션.
- 패치가 있는 VI를 보려면 다음으로 이동하십시오. 모두 〉 취약성 대응 〉 취약 항목 〉 패치를 사용하여 나에게 할당됨.
- 정정 작업을 보려면 다음으로 이동하십시오. 모두 〉 취약성 대응 〉 취약 항목 〉 패치를 사용하여 나에게 할당됨
- 검색된 항목 기록을 보려면 다음으로 이동하십시오. 모두 〉 보안 운영 〉 검색된 항목.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

의 패치 오케스트레이션에 대한 패치 데이터 및 상태 롤업 취약성 대응

v16.1 취약성 대응 부터는 패치 데이터와 상태가 애플리케이션의 패치 업데이트 및 기타 기록 취약성 대응 으로 롤업됩니다.

패치 클래식 환경의 작업 공간에서 기록 업데이트 취약성 대응

패치, 취약성 솔루션 및 취약성에 대한 정보는 모두 애플리케이션에 연결되어 있습니다 취약성 대응 .

패치 데이터와 패치 롤업 데이터 및 상태가 인스턴스의 기록에 표시됩니다. 패치 기록은 와 취약성 대응통합의 패치 오케스트레이션 기능의 일부로 포함됩니다. IT 정정 작업 공간의 목록 뷰에서 취약성 대응 작업 공간의 패치(VPU) 기록을 봅니다. 클래식 뷰와 Vulnerability Response Workspace의 패치 업데이트 기록에는 다음 데이터가 포함됩니다.

- 취약성 솔루션 관리 애플리케이션에서 임포트한 패치 벤더의 취약성 솔루션 데이터 및 정보입니다.
- 패치로 해결할 수 있는 취약성이 있는 총 장치 수와 업데이트가 누락된 모든 장치를 포함하는 소스 정정 상태입니다.
- 정정된 VI의 비율(%)과 기본 패치로 패치가 있는 총 VI를 포함하는 정정 상태입니다.
- 클래스 뷰의 기록에 대한 관련 링크에 연결된 장치, 취약한 항목, 패치 배포 및 패치 요청. 이 데이터는 취약성 대응 작업 공간 내 기록의 탭에 표시됩니다.
- 정정 소유자가 승인을 위해 제출한 패치 요청입니다.

필요한 역할

사용자는 데이터를 보고 패치를 예약하는 데 사용 중인 패치 오케스트레이션 통합과 관련된 역할이 필요합니다. 자세한 내용은 지원되는 통합을 참조하십시오.

- 와 HCL BigFix 패치 오케스트레이션의 통합 이해 취약성 대응 및 SCCM 취약성 대응 과의 Microsoft 패치 오케스트레이션 통합 이해.
- 대시보드에서 취약성 대응 패치 오케스트레이션 데이터 보기 클래식 환경에서.
- 에서 취약성 대응 작업 공간성과표의 데이터를 봅니다.

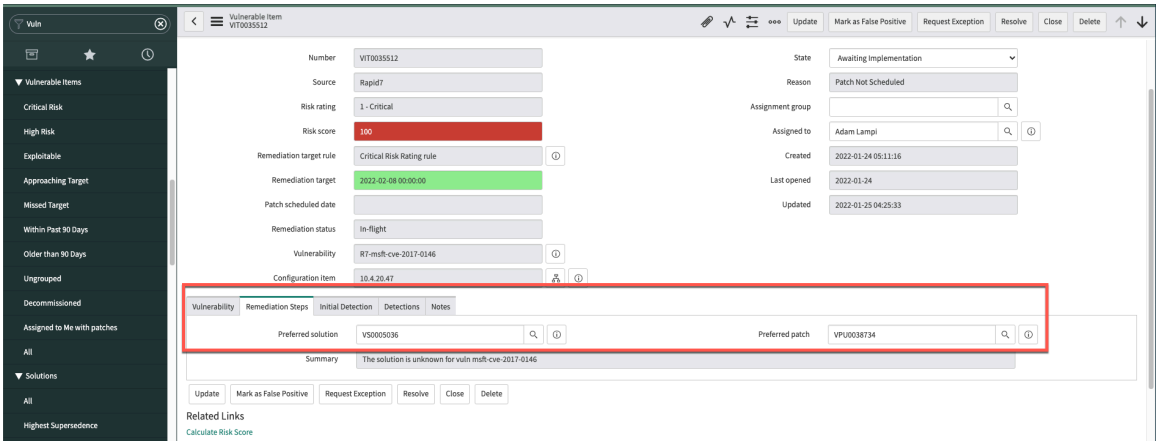
패치 데이터 및 상태 롤업

패치가 있고 클래식 환경에서 사용자에게 할당된 취약한 항목을 보려면 다음으로 이동합니다. 모두 〉 취약성 대응 〉 취약한 항목 〉 패치를 사용하여 나에게 할당됨.

취약한 항목 기록이 기본 패치로 채워지면 VI의 상태가 종결, 해결됨, 연기됨 또는 검토 중이 아닌 경우에만 구현 대기 중으로 자동 전환됩니다. 데이터를 드릴다운하여 기본 솔루션 및 기타 데이터를 보려면 VI 기록에서 정정 탭을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

정정 단계 탭



기본 패치가 있는 VI는 다음과 같은 경우 구현 대기 중 으로 전환됩니다.

- 컬렉션 임포트의 일부인 CI에 패치 배포가 예약되어 있고 CI에 연결된 VI가 있는 경우 VI가 구현 대기 중인 이유는 패치 예약됨 때문입니다.
- 컬렉션 임포트의 일부인 CI에 패치 배포가 예약되어 있고 CI에 연결된 VI가 있으며 정정 목표 날짜(기한)가 TTR(정정 시간) 날짜보다 늦은 경우 VI의 상태는 패치 예약됨(대상 날짜 누락)이라는 이유로 구현 대기 중입니다.
- 컬렉션 임포트의 일부인 CI에 패치 배포가 예약되지 않은 경우 VI의 상태는 패치 예약되지 않음이라는 이유로 구현 대기 중입니다.

기본 패치 정보 아이콘을 클릭하여 패치 업데이트를 열고 관련 링크에서 다음 정보를 확인합니다.

취약한 항목
: 이 패치와 관련된 취약한 항목입니다.

관련 장치
: 업데이트가 있는 장치와 누락된 장치.

패치 배포
: 개별 컴퓨터(자산) 또는 자산 그룹에 이 패치에 대해 예약된 배포입니다.

패치 요청
: 배포 일정이 예약되기 전에 승인을 위해 전송된 패치 요청 목록입니다.

잠재적 패치
: 취약성을 해결할 수 있는 패치입니다.

기본 패치 정보 아이콘을 클릭하여 기록을 열고 다음 패치 업데이트 데이터 외에 이전에 나열된 정보를 봅니다.

소스 정정 상태
: 이 패치가 필요한 총 장치와 패치가 누락된 모든 장치입니다.

정정 상태
: 이 기본 패치가 있는 VI의 상태(총 VI, 정정된 비율, 지연된 VI)입니다.

기본 패치 및 솔루션

임포트한 취약성이 의 구성 관리 데이터베이스(CMDB)자산과 일치하면 에 VI(취약한 항목)가 생성됩니다 취약성 대응. 이 VI와 연결된 CI(구성 항목)도 외부 공급업체 패치 벤더에서 임포트했는데 동일한 취약성에 대한 패치가 누락된 것으로 표시되면 기본 패치가 나열되고 솔루션에 롤업됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 정보를 통해 자산(CI)에 취약성과 가장 일치하는 사용 가능한 패치의 수정 사항이 있음을 알 수 있습니다.

솔루션 없이 패치 보기

임포트 후 사용할 수 있는 취약성 솔루션 데이터가 없으면 패치 업데이트 기록의 취약성 솔루션 필드가 비어 있습니다. 이러한 유형의 패치에 대한 정보를 보는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 에서 솔루션이 없는 패치 보기 취약성 대응.

에서 솔루션이 없는 패치 보기 취약성 대응

의 v16.0 취약성 대응부터 임포트 후에 해결책이 없는 패치의 경우 시스템은 취약성 기록에서 이러한 패치를 볼 수 있도록 취약성 참조 데이터에서 패치 ID를 검색합니다.

솔루션 없는 패치

필요한 역할: sn_vul.vulnerability_admin.

패치 스캐너 통합뿐만 아니라 패치 오케스트레이션 및 취약성 솔루션 애플리케이션에서 임포트한 데이터가 처리, 연결 및 애플리케이션에서 패치 업데이트 기록에 취약성 대응 표시됩니다.

취약성에 대한 솔루션이 존재하는 경우 관련 정보가 인스턴스에서 상호 연관되고 패치에서 취약성 솔루션으로, 취약성으로 롤업됩니다. 이 정보를 보려면 다음으로 이동하십시오. 모두 〉 취약성 대응 〉 패치 〉 모두.

임포트 후 사용할 수 있는 취약성 솔루션 데이터가 없으면 패치 업데이트 기록의 취약성 솔루션 필드가 비어 있습니다. 이러한 패치에 대한 관련 솔루션 정보를 볼 수 있도록 인스턴스에서 시스템 속성 [**sn_vul_patch_orch.no_solution_patch_rollup**]이 기본적으로 활성화됩니다. 이 속성은 스캐너 임포트의 취약성 참조 데이터에서 공지 ID와 문서 ID를 검색합니다. 일치하는 것이 발견되면 관련 데이터가 잠재적 패치 테이블에 채워지고 이 정보는 취약성 기록의 관련 목록에 표시됩니다.

취약성이 많거나 롤업 예약 작업을 완료하는 데 시간이 오래 걸리는 경우 성능 문제를 방지하기 위해 이 시스템 속성을 비활성화하는 것이 좋습니다. 그러나 이 시스템 속성을 비활성화하면 임포트된 솔루션 데이터가 솔루션 없이 검색되거나 취약성으로 롤업되지 않습니다.

sn_vul.vulnerability_admin 역할을 가진 사용자가 시스템 속성을 비활성화하려면 다음 단계를 수행합니다.

1. 다음으로 이동 **sys.properties.list**.
2. **sn_vul_patch_orch.no_solution_patch_rollup**을 찾아 클릭하여 기록을 엽니다.
3. 값 필드에 false를 입력합니다.
4. 업데이트를 클릭합니다.

대시보드에서 취약성 대응 패치 오케스트레이션 데이터 보기

v16.1부터 애플리케이션에 포함된 취약성 대응 대시보드의 클래식 환경에서 패치 업데이트 데이터를 볼 수 있습니다.

작업 공간에는 취약성 대응 정정 진행 상황을 모니터링하는 데 도움이 될 수 있는 데이터 시각화가 포함되어 있습니다. 취약성 데이터가 변경될 때 업데이트되는 동적 데이터 시각화에서 조직에 중요한 활성 취약성의 수와 심각도를 확인하여 조직에 대한 위협 수준을 확인할 수 있습니다. 자세한 내용은 AND IT 정정 작업 공간 살펴보기 문서를 참조하십시오취약성 관리자 작업 공간.

를 구독 퍼포먼스 분석하는 경우 CISO 및 PA(취약성 관리) 대시보드에서도 이 데이터를 볼 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

클래식 환경에서 패치 데이터를 볼 수도 있습니다. 클래식 환경에서 애플리케이션에 포함되어 취약성 대응 있고 별도의 구독이 필요한 대시보드에서 필요한 취약성 대응 역할과 데이터를 보는 방법에 대한 자세한 내용은 기본 취약성 대응 대시보드 사용문서를 참조하십시오.

솔루션 보기

모든 솔루션, 대체 가능성이 가장 높은 솔루션, 취약한 항목과 관련된 솔루션을 보고 정정 활동을 알립니다.

시작하기 전에
필요한 역할: sn_vul.read, sn_vul.vulnerability_admin 또는 sn_vul.remediation_owner
가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

이 태스크 정보
취약성 분석가 또는 정정 소유자는 취약한 항목과 관련된 다양한 솔루션 세트를 볼 수 있습니다.

> **주:**
> 솔루션 기록은 내부 메모 섹션 또는 사용자가 생성한 솔루션의 메모 아래를 제외하고 읽기 전용입니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 솔루션.
2. 솔루션 목록을 선택합니다.

   > **주:**
   > 제품 이름에 와일드카드를 사용하여 솔루션 목록을 필터링할 수 있습니다.

3. 검토하려면 각 항목을 클릭합니다.
4. 옵션: 메모 탭 아래에 메모를 입력하고 마우스 오른쪽 버튼으로 저장을 클릭하여 페이지에 남아 있거나 업데이트를 클릭하여 저장하고 취약성 솔루션 목록으로 돌아갑니다.

   > **주:**
   > sn_vul.read 역할만 있는 경우에는 이 단계를 수행할 수 없습니다.

취약성 솔루션 생성

외부 공급업체 솔루션 컨텐츠에서 다루지 않는 취약성 솔루션을 추적할 수 있도록 취약성 솔루션을 생성합니다.

시작하기 전에
필요한 역할: admin, sn_vul.vulnerability_admin 또는 sn_vul.admin(사용되지 않음) 또는 vulnerability.write
취약성 솔루션 관리 애플리케이션 내에서 취약성 대응 사용할 수 있는 기능입니다. 취약성 솔루션 관리별도의 구독이 필요합니다.

가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보
솔루션 목록에서 솔루션을 만들 수 있습니다. 솔루션을 작성하려면 먼저 취약성 솔루션 관리 애플리케이션을 설치해야 합니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 솔루션.
2. 솔루션 목록(모두, 가장 높은 대체 또는 취약한 항목 포함)을 선택합니다.
3. 새로 만들기를 클릭합니다.
4. 양식의 편집 가능한 필드에 적절한 정보를 입력합니다.
   사용하지 않는 필드는 비워둘 수 있습니다. 개별 필드에 대한 자세한 내용은 다음 문서를 참조하십시오 솔루션 양식 필드.
5. 헤더에서 저장을 마우스 오른쪽 버튼으로 클릭합니다.
   솔루션 기록이 추가되고 기본적으로 모두 및 가장 높은 대체 목록에 나타납니다.
6. 관련 목록이 나타납니다.

   이 솔루션을 취약한 항목, 타사 취약성, **CVE,**대체 솔루션 , 선행 솔루션 등의 관련 목록에 연결할 수 있습니다. 취약성 또는 솔루션을 선택하고 제출을 클릭합니다.

   주:

   취약성 솔루션 관리 취약성 기록이 솔루션과 수동으로 연결되면 취약한 항목 및 정정 작업을 솔루션과 자동으로 연결합니다.

   다른 솔루션에 수동으로 재할당된 취약한 항목은 취약성 수준의 솔루션 변경 내용으로 자동으로 업데이트되지 않습니다.

   정정 중인 CI와 관련이 없거나 사용자 환경의 문제가 되지 않는 외부 공급업체 취약성과 솔루션 간의 관계를 제외하려면 을 참조하십시오 외부 공급업체 기록에서 솔루션을 수동으로 제외하거나 그 반대로 제외.

외부 공급업체 기록에서 솔루션을 수동으로 제외하거나 그 반대로 제외

외부 공급업체 취약성과 솔루션 간의 관계는 정정 중인 CI와 관련이 없거나 사용자 환경의 문제가 되지 않으므로 제외합니다. 외부 공급업체 취약성 또는 솔루션 기록을 사용하여 솔루션을 수동으로 제외합니다.

시작하기 전에
필요한 역할:

- sn_vul.쓰기
- sn_vul.remediation_owner

가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

프로시저

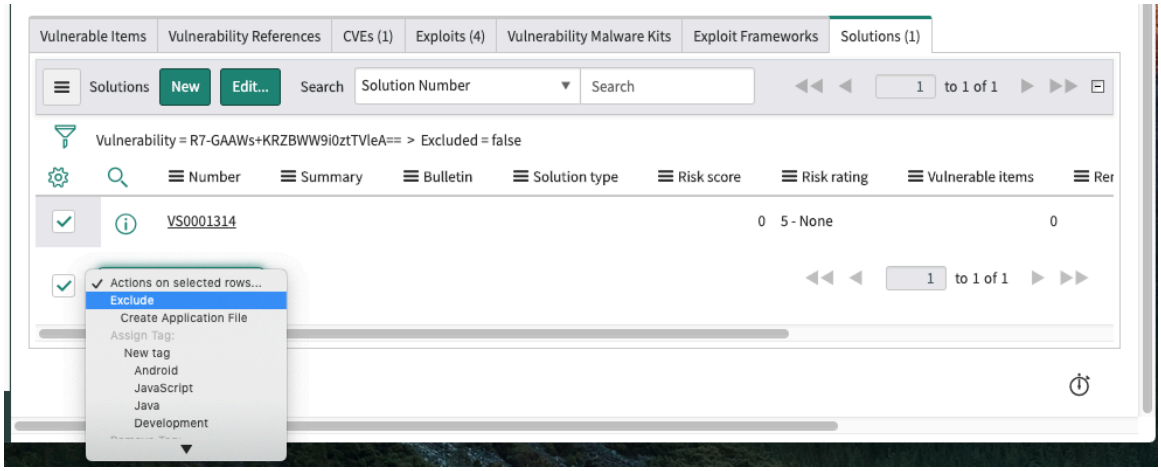
1. 다음으로 이동 모두 〉 취약성 대응 〉 라이브러리 〉 외부 공급업체 또는 취약성 대응 〉 모든 솔루션
2. 타사 취약성 또는 솔루션 기록을 엽니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 외부 공급업체 기록의 경우: 솔루션 관련 탭을 선택합니다.

b. 솔루션 레코드의 경우: 외부 공급업체 취약성 관련 탭을 선택합니다.

3. 제외하려는 각 취약성 또는 솔루션 기록 옆에 있는 확인란을 선택합니다.
4. **Actions on selected** rows(선택한 행에 대한 작업) 드롭다운 메뉴에서 Exclude(제외)를 선택합니다.



외부 공급업체 또는 솔루션 기록이 관련 탭에 더 이상 나타나지 않습니다.

솔루션에 대한 타사 취약성 관계도 솔루션이 업데이트되거나 야간 작업이 활성화된 경우 제외됩니다.

솔루션에 대한 외부 공급업체 취약성 관계는 야간 예약 작업 중에 제외됩니다.

외부 공급업체 취약성을 제외한다는 것은 해당 솔루션이 더 이상 기본 솔루션 평가의 요소가 아니라는 것을 의미합니다. 제외 영향:

- 외부 공급업체 취약성, 취약한 항목(VI) 및 외부 공급업체 취약성에 연결된 CI(구성 항목)는 더 이상 솔루션에 포함되지 않으므로 솔루션에 대한 모든 카운트입니다.
- 외부 공급업체 취약성에 대해 기본 솔루션을 결정하고 더 나아가 연결된 VI 및 VI를 포함하는 정정 작업의 기본 솔루션을 결정합니다.

취약성 자동 분류

성공적인 정정을 위해서는 새로운 취약성을 검토하고 분류하는 것이 필요합니다. 자동화된 VI(취약한 항목) 할당, 위험 계산, 정정 대상 및 VI 그룹화를 사용하여 취약성 임포트를 정정 작업으로 변환합니다.

임포트한 취약성부터 시작하여 CMDB에서 찾을 수 없는 자산을 조정하고, 결과의 우선순위를 지정하고, 이를 자동으로 할당된 정정 활동으로 변환하고, 정정 프로세스를 오케스트레이션하고, 유효성 검사 완료를 확인합니다.

일반적으로 새로운 취약한 항목은 임포트할 때 정정 작업 규칙에 따라 정정 작업으로 분류됩니다. 취약한 항목을 그룹화할 수 없거나 인식된 구성 항목이 없는 경우가 있습니다.

취약성 분류 프로세스의 개요:

- 취약성 대응 인스턴스에 로그인합니다.
- 취약한 항목에 대한 규칙(CI 조회, 할당)이 예상대로 작동하는지 확인합니다. CI 조회 규칙 개정에 대한 자세한 내용은 을 참조하십시오 외부 공급업체 취약성 통합에서 취약성 대응 구성 항목을 식별하기 위한 CI 조회 규칙. 할당 규칙에 대한 자세한 내용은 문서를 참조하십시오 취약성 대응 할당 규칙 개요.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
데이터 임포트의 양이 많기 때문에 자동화된 취약한 항목 할당에 주의해야 합니다.

- 정정 대상이 올바른지 확인합니다. 정정 대상 규칙의 작동 방식과 수정 방법에 대한 자세한 내용은 을 참조하십시오 취약성 대응 정정 대상 규칙 .
- 그룹화되지 않은 취약한 항목을 봅니다.
  - 그룹화되지 않은 취약한 항목을 살펴보면 그룹 규칙을 수정하고 다시 스캔을 수행하는 것이 좋습니다. 자세한 내용은 정정 작업 규칙 생성 또는 편집 취약성 대응 문서를 참조하십시오.
  - 취약한 항목을 수동으로 그룹화합니다. 에서 수동으로 정정 작업 생성 취약성 대응 자세한 내용은.
  - 정정 작업에서 취약한 항목에 대한 위험 점수를 수정합니다. 자세한 내용은 취약성 대응 계산기 및 취약성 계산기 규칙 문서를 참조하십시오.
  - 외부 공급업체 통합에서 최근에 탐지되지 않은 오래된 취약한 항목을 종결합니다. 자세한 내용은 취약한 항목 및 탐지 자동 종결 문서를 참조하십시오.
- 일치하지 않는 구성 항목 보기 및 재분류.
- 개선을 위해 수행해야 할 작업을 조사합니다.

  이 단계에는 다음이 포함될 수 있습니다.

  - 지금 처리해야 할 일과 미룰 수 있는 일을 결정하십시오. 이 결정은 보통 위험 점수, 영향을 받는 시스템 및 변경 기간이 있는 패치를 기반으로 합니다.

    주:
    정정 대상 규칙은 취약한 항목에 속합니다. 이러한 규칙은 취약한 항목을 임포트할 때 실행됩니다. 이러한 규칙은 이전에 설정 도우미에서 생성되었습니다.

  - 필요한 경우 취약한 항목을 새로 고치고 취약한 항목의 정정 대상 상태 취약성 대응 보기.
  - 변경 요청을 생성하고 정정을 위해 할당 그룹(IT 운영)에 정정 작업을 할당합니다.

    주:
    취약성이 보안 인시던트를 구성하며 플러그인(com.snc.security_incident)이 보안 인시던트 응답 활성화된 경우 대신 정정 작업에서 보안 인시던트 기록을 만들 수 있습니다.

  - 하나 이상의 변경 요청을 제출한 후 그룹 상태를 조사 중으로 이동합니다.

에서 취약한 항목을 대량으로 편집 취약성 대응

필드를 선택하고 백그라운드에서 비동기 대량 편집 작업을 실행하여 취약한 항목을 대량 으로 편집하면 시간을 절약할 수 있습니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)

이 태스크 정보
가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

중요사항:
일괄 편집 기능은 의 호스트 취약한 항목에 대해 사용할 수 있습니다 취약성 관리자 작업 공간. 자세한 내용은 에서 대량 편집 사용 취약성 관리자 작업 공간 문서를 참조하십시오.

프로시저

1. 다음으로 이동 모두 〉 취약성 〉 취약성 〉 취약 항목.
2. 다음 작업 중 하나를 수행하여 취약한 항목을 선택합니다.
   - 필드에서 선택한 항목#unique_155_Connect_42_entry-be-record-selection 만 옵션을 사용하려면 각 항목 옆에 있는 확인란을 선택합니다.
   - 필드에서 필터와 일치하는 모든 취약한 항목 옵션을 #unique_155_Connect_42_entry-be-record-selection 사용하려면 필터를 적용합니다.
3. **Bulk** Edit(일괄 편집) 버튼을 선택합니다.
4. 대량 편집 모달의 필드에 내용을 입력합니다.

필드	설명
기록 선택	업데이트할 기록입니다. 선택 항목은 다음과 같습니다. ○ 선택한 취약한 항목만 존재함 ○ 필터와 일치하는 모든 취약한 항목 ○ 정정 작업 ○ 취약성 항목
상태	취약한 항목의 상태에 대한 변경입니다. 선택 항목은 다음과 같습니다. ○ 업데이트하지 마십시오. ○ 오픈 ○ 조사 중 ○ 대기 중인 구현 ○ 연기됨 주: ▪ 이 옵션을 선택하면 이유, 간단한 설명, 기한 및 추가 정보 필드가 나타납니다. ▪ VIT를 연기하면 정정 작업이 생성되고 이 작업은 승인을 위해 전송됩니다. ○ 종결됨 주: ▪ 이 옵션을 선택하여 기록을 긍정 오류로 표시하면 이유, 간단한 설명, 기한 및 추가 정보 필드가 나타납니다. ▪ 기록을 긍정 오류로 표시하면 정정 작업이 생성되고 이 작업이 승인을 위해 전송됩니다. ○ 해결 일시

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
기본 솔루션	대량 편집을 위해 선택된 모든 취약한 항목을 정정하기 위한 대상 솔루션. 취약한 항목(VIT)에서 기본 솔루션 필드에 대한 변경을 선택합니다. 선택한 VIT에 사용할 수 있는 기본 솔루션 조회 목록에서 선택 항목을 선택할 수 있습니다. 주: ○ 사용 가능한 기본 솔루션 집합은 선택한 모든 VIT에서 취약성의 모든 잠재적 솔루션이 교차하는 지점입니다. ○ 를 선택할 때 기록 선택 〉 취약성 항목 대량 편집의 경우 취약성 에 대한 모든 VIT가 선택한 기본 솔루션으로 설정됩니다. 주: 이 작업은 취약성 엔트리 수준에서 기본 솔루션을 설정하지 않습니다. 취약성 엔트리 수준에서 기본 솔루션을 설정하면 앞으로 모든 새 VIT에 대한 기본 솔루션이 설정됩니다. 대량 편집은 현재 VIT 세트만 수정합니다. ○ 선택 기준 전반의 뚜렷한 취약성은 500개로 제한됩니다. 500개 이상의 고유한 취약성이 있는 경우 기본 솔루션을 설정하기 위해 다른 기준을 가진 VIT를 선택하라는 경고 메시지가 표시됩니다. ○ 목록 조회에 표시할 수 있는 총 솔루션 수는 170개로 제한됩니다. 170개가 넘는 솔루션이 있는 경우 경고 메시지가 표시됩니다. 업데이트된 값이 취약한 항목 목록 뷰에 표시됩니다.
기본 패치	대량 편집을 위해 선택된 모든 취약성 항목을 정정하기 위한 대상 패치입니다. 주: ○ 기본 패치 목록을 보려면 패치 오케스트레이션을 설치해야 합니다. ○ 사용 가능한 기본 패치 집합은 선택한 모든 VIT에서 모든 잠재적 패치의 교차점입니다. ○ 선택 기준 전반의 뚜렷한 취약성은 500개로 제한됩니다. 500개 이상의 고유한 취약성이 있는 경우 기본 패치를 설정하기 위해 다른 기준을 가진 VIT를 선택하라는 경고 메시지가 표시됩니다. ○ 조회 목록에 표시할 수 있는 총 패치 수는 170개로 제한됩니다. 패치가 170개 이상이면 경고 메시지가 표시됩니다.
이유	기록을 연기하는 이유: ○ 유지관리 기간을 기다리는 중 ○ 수정 사용 불가 ○ 위험 수락됨 ○ 사용 중인 완화 통제 ○ 기타 기록을 종결하는 이유:

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	○ 긍정 오류 주: ▪ 이 옵션을 선택하면 간단한 설명, 기한 및 추가 정보 필드가 나타납니다. ▪ 기록을 긍정 오류로 표시하고 이 작업이 승인을 위해 전송되면 정정 작업이 생성됩니다. ○ 취소됨 ○ 고정 주: 상태를 연기됨 또는 종결됨으로 선택하면 이 필드가 표시됩니다.
간단한 설명	지연 및 종결-긍정 오류 요청의 이유를 설명하는 간단한 메모입니다. 이 정보는 지연 및 종결-긍정 오류 요청에 대해 생성된 정정 작업의 설명 필드에 반영됩니다. 주: 이 필드는 상태를 연기됨 및 종결됨-긍정 오류로 선택할 때 나타납니다.
다음까지	기록이 지연된 상태로 유지되는 종료 날짜입니다. 주: 이 필드는 상태를 연기됨으로 선택할 때 나타납니다.
추가 정보	기타 필요한 정보입니다. 이 정보는 개요 탭의 추가 정보 필드에 반영됩니다. 연기 요청이 승인되면 이 추가 정보가 VIT 및 정정 작업 모두에서 연기 메모로 나타납니다. 주: 이 필드는 상태를 연기됨 및 종결됨-긍정 오류로 선택할 때 나타납니다.
할당 해제	선택한 모든 항목이 할당 그룹 및 정정 소유자에 대해 할당되지 않습니다. 정정 소유자가 취약한 항목에서 할당을 제거하는 방법에 대한 자세한 내용은 사용자 또는 그룹의 취약한 항목에서 할당 제거를 참조하십시오. 주: ○ 이 필드는 상태를 업데이트 안 함으로 선택할 때 나타납니다. ○ 기록 할당을 해제하면 정정 작업이 생성되고 이 작업이 승인을 위해 전송됩니다.
할당 그룹	VIT에 대한 할당 그룹입니다. 수동으로 선택하거나 활성화된 경우 할당 권장 사항을 사용합니다. 주: 할당 해제 확인란을 선택하면 이 필드가 비활성화됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
작업 메모	변경 내용을 설명하기 위해 입력하는 텍스트입니다.

5. 확인을 선택합니다.
   대량 비동기 편집 작업은 선택한 기록을 업데이트합니다. 링크가 포함된 작업 번호가 취약한 항목 페이지에 표시되며, 여기에서 상태를 볼 수 있습니다. 취약한 항목을 대량으로 연기, 할당 해제 또는 종결(긍정 오류)할 때 선택한 취약한 항목을 가지고 정정 작업이 생성됩니다. 그리고 이 정정 작업은 승인을 위해 전송됩니다.

그룹화되지 취약성 대응 않은 취약한 항목

취약한 항목은 임포트될 때 자동으로 정정 작업에 할당됩니다. 그러나 VI(취약한 항목)가 수동으로 생성되는 경우(예: VI가 고아가 될 수 있음) 경우가 있습니다. 그룹화되지 않은 취약한 항목 모듈은 이러한 취약한 항목을 그룹 없이 나열합니다.

주:
통합 자동화 프로세스는 고아를 생성하지 않으므로 이 사용 사례는 작을 것으로 예상됩니다.

그룹 해제는 취약한 항목이 취약성 없이 생성되었거나 VI를 그룹에 할당하는 정정 작업 규칙이 없는 경우에 발생합니다.

이 경우 다음으로 이동하여 그룹화되지 않은 취약한 항목 목록을 검토하십시오. 모두 〉 취약성 대응 〉 취약한 항목 〉 그룹 해제.

검토 후 선택 항목은 다음과 같습니다.

- 이 목록에 나타나는 모든 항목을 포착할 수 있습니다 정정 작업 규칙 생성 또는 편집 취약성 대응 .
- 이 목록의 항목을 그룹에 수동으로 추가하거나 이러한 항목과 일치하는 조건을 정의할 수 있습니다 에서 수동으로 정정 작업 생성 취약성 대응 .
- 오픈 또는 조사 중인 상태인 기존 정정 작업을 열고 관련 취약한 항목을 그룹에 추가할 수 있습니다.

주:
수동으로 추가된 취약한 항목이 정정 작업 규칙 또는 그룹 조건에 따라 정정 작업에서 자동으로 제거되지 않습니다.

정정 작업 및 작업 규칙의 작동 방식에 대한 자세한 내용은 문서를 참조하십시오 취약성 대응 정정 작업 및 정정 작업 규칙 개요.

그룹화되지 취약성 대응 않은 취약한 항목 보기

그룹에 할당되지 않은 취약한 항목은 볼 수 있는 목록에 배치됩니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)
가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 〉 취약성 〉 그룹화되지 않은 취약한 항목.
2. 목록에서 취약한 항목을 검토합니다.
3. 취약한 항목을 클릭하여 확인하고 그룹에 포함할 방법을 결정합니다.

정정 작업에 취약한 항목을 수동으로 추가

취약한 항목이 그룹화되지 않은 경우 해당 항목을 정정 작업에 추가할 수 있습니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)
가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

프로시저

1. 취약한 번호를 기록합니다.
2. 다음으로 이동 모두 〉 취약성 대응 〉 정정 작업.
3. 취약한 항목에 대한 정정 작업(VUL)을 선택합니다.
4. 오른쪽 하단에서 편집을 선택합니다.
5. 수집 검색 필드에 취약한 항목 번호를 입력합니다.
6. 컬렉션에서 취약한 항목을 선택하고 목록에 추가합니다.
7. 저장을 클릭합니다.

취약한 항목 및 정정 작업에서 할당 제거

, 애플리케이션 취약성 대응및 컨테이너 취약성 대응 애플리케이션의 취약한 항목 기록취약성 대응에서 할당 대상 및 할당 그룹 필드를 지웁니다.

시작하기 전에
필요한 역할:

- 취약한 항목(VIT) 및 정정 작업(VUL)에 대한 sn_vul.remediation_owner 또는 sn_vul.vulnerability_analyst.
- 취약한 항목(AVIT) 및 정정 작업(AVUL)에 대한 애플리케이션 취약성 대응 sn_vul.app_sec_manager.
- 컨테이너 취약한 항목(CVIT) 및 정정 작업(CVUL)에 대한 sn_vul_container.remediation_owner 또는 sn_vul_container.vulnerability_analyst.

이 태스크 정보
UI 할당 해제 작업은 클래식 환경과 작업 공간 모두에서 종결됨 또는 해결됨 이외의 상태인 다음 기록에 대해 지원됩니다.

- 정정 작업(VUL, AVUL 및 CVUL). 이 기능으로 정정 작업이 업데이트되면 동일한 할당 그룹이 있는 연결된 모든 VIT의 할당 대상 및 할당 그룹 필드도 지워집니다.
- 취약한 항목(VIT).
- 애플리케이션 취약 항목(AVIT)입니다.
- 컨테이너 취약 항목(CVIT)입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

중요사항:
에서 호스트 취약한 항목을 대량으로 할당 해제할 수 있습니다 취약성 관리자 작업 공간. 자세한 내용은 에서 대량 편집 사용 취약성 관리자 작업 공간 문서를 참조하십시오.

프로시저

1. 클래식 환경 또는 IT 정정 소유자 작업 공간에서 사용자에게 할당된 종결됨 또는 해결됨 이외의 상태에 있는 취약한 항목(VIT) 기록으로 이동합니다.
2. 클래식 뷰에서 할당 대상 및 할당 그룹 필드를 지우려면 기록 상단에서 할당 취소를 선택합니다.
3. 또는 사용자 또는 사용자 또는 그룹에 할당된 IT 정정 작업 공간에서 취약한 항목(VIT, AVIT 또는 CVIT) 기록으로 이동하고 추가 옵션 메뉴(개)에서 할당 해제를 클릭하여 할당 필드를 지웁니다.
4. 작업 공간에서 사용자 또는 그룹에 할당된 정정 작업 기록의 경우, 기록을 열고 추가 옵션 메뉴 ( )에서 할당 해제를 선택하여 할당 필드를 지웁니다.
5. 취약한 항목과 정정 작업 모두에 대한 할당 해제 대화 상자에서 작업 메모를 제공하고 제출을 선택합니다.
   상태 변경 승인 요청이 승인을 위해 제출됩니다.

   주:
   정정 작업의 경우 모든 정정 작업과 연결된 VIT의 할당 대상 및 할당 그룹 필드도 지워진다는 알림을 받습니다.

   정정 작업에 대한 필드 지우기 요청이 승인되면 동일한 할당 그룹이 있는 취약한 항목의 모든 할당 대상 및 할당 그룹 필드도 할당 해제됩니다. 취약한 항목에 연결된 정정 작업과 다른 할당 그룹이 있는 경우 할당이 취소되지 않습니다. 대부분의 경우 이러한 취약한 항목은 수동으로 할당되었습니다.

6. 다음과 같은 정보를 볼 수 있습니다.
   - 입력한 작업 메모는 메모 섹션에 표시됩니다.
   - 상태 변경 승인 탭에서 상태 변경 승인 기록이 검토 중 상태로 표시되므로 승인 워크플로우를 추적하는 데 도움이 됩니다.
   - 요청된 승인 탭에서 본인 또는 할당 그룹 제거 요청이 요청됨 상태로 표시됩니다.

결과
요청은 기본 1단계 승인 워크플로우를 사용하여 승인됩니다. 자세한 내용은 에서 할당 해제 요청 승인 또는 거부 취약성 대응 문서를 참조하십시오.

- 요청이 승인되면 상태 변경 승인 기록과 요청된 승인 기록이 승인됨 상태로 전환됩니다. 사용자와 사용자의 그룹이 할당 대상 및 할당 그룹 필드에서 제거됩니다. 할당 유형 필드에 #### ##이 표시되고 각 제품의 할당되지 않은 모듈 목록에 정정 작업과 VIT가 표시됩니다.

  기록이 할당되지 않았다는 알림은 할당 해제 알림 그룹의 취약성 관리자 또는 분석가에게 자동으로 전송됩니다. 승인 플래그, 알림 및 기본 할당 그룹을 구성하려면 취약한 항목 및 정정 작업에서 할당 제거를 참조하십시오.

- 요청이 거부됨(Rejected)이면 변경 승인 기록 및 요청된 승인 기록의 상태가 거부됨 상태로 전환됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
취약성 관리자는 시스템 속성을 **false**로 설정하여 *sn_vul.unassign_vr.approval_required* 승인 프로세스를 비활성화할 수 있습니다.

다음에 수행할 작업
및 애플리케이션 취약성 대응 컨테이너 취약성 대응 애플리케이션의 할당되지 않은 모듈 취약성 대응로 이동하여 범위에 속할 수 있는 항목에 대한 할당되지 않은 기록을 모니터링하고 자신에게 다시 할당합니다.

에서 할당 해제 요청 승인 또는 거부 취약성 대응

할당 그룹 또는 애플리케이션의 개별 사용자로부터 취약한 항목을 제거해 달라는 요청을 승인합니다 취약성 대응 .

시작하기 전에
필요한 역할: 미할당 승인의 경우 승인자 – 수준 1 그룹에 한 명의 승인자가 필요합니다.

- sn_vul.unassign_approver for AVITs and VITs
- CVIT에 대한 sn_vul_container.unassign_approver

이 태스크 정보
기본적으로 승인 구성이 제공되고 승인 그룹 할당이 해제됩니다. 승인자 할당 해제 - 수준 1 그룹의 사용자가 요청을 승인할 수 있습니다. 이 그룹에는 기본적으로 할당되지 않은 승인자 역할인 sn_vul.unassign_approver가 포함되어 있습니다. 새 그룹을 수정 또는 생성하고 승인 구성을 업데이트할 수 있습니다. 승인 규칙을 구성하려면 승인 규칙 모듈에서 다음 승인 규칙 중 하나를 선택하고 승인 구성 탭의 승인 구성으로 이동합니다.

- *Vulnerable item field change request* 취약한 항목에 대해.
- *Vulnerability field change request* 정정 작업의 경우.
- *Application vulnerability field change request* 애플리케이션 취약한 항목(AVIT)에 대해 설명합니다.
- *Approval for container management* 컨테이너 취약한 항목(CVIT)에 대해 설명합니다.

승인 규칙 및 구성에 대한 자세한 내용은 다음 문서를 참조하십시오 할당 해제 요청에 대한 승인 워크플로우 구성.

중요사항:
다음에서 요청을 승인하거나 거부할 수 있습니다 취약성 관리자 작업 공간. .

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 내 승인 VIT 및 AVIT용.
   또는 다음으로 이동합니다. 모두 〉 컨테이너 취약성 대응 〉 내 승인 CVIT의 경우.
2. 큐에서 요청을 선택합니다.
3. 적절한 코멘트를 추가하여 요청을 승인하거나 거부합니다.

취약한 항목 및 탐지 자동 종결

자동 종결 규칙 모듈을 사용하여 폐기된 CI와 연결된 부실 탐지 및 취약한 항목(VI)을 자동으로 종결할 수 있습니다.

다음 시나리오에서 부실 탐지 및 VI를 자동으로 종결할 수 있습니다.

- 에서 부실 탐지 자동 종결 취약성 대응
- 폐기된 CI와 관련된 취약한 항목을 자동으로 닫습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

폐기된 구성 항목 작업에 대한 자세한 내용은 을 자동 종결 규칙 생성참조하십시오폐기된 구성 항목 작업.

폐기된 구성 항목 작업

해제된 CI(구성 항목)는 에서 폐기됨, 보관됨 또는 삭제됨 상태로 구성 관리 데이터베이스(CMDB)이동됩니다. 에는 취약성 대응 CI로 구성된 취약한 항목(VI)이 포함되어 있습니다. CI의 상태가 폐기됨으로 업데이트되면 연결된 VI는 하위 상태가 'CI 해제됨'으로 종결됩니다.

주:
v25.0.3 부터 취약성 대응해제된 CI와 관련된 취약 항목 및 탐지를 종결하기 위해 새로운 자동 종결 규칙 'CI 해제됨'이 도입되었습니다.

CMDB가 CI의 수명주기 스테이지 상태를 폐기됨으로 변경하는 경우 연결된 VI를 자동으로 종결하도록 선택할 수 있습니다. 연결된 VI를 자동으로 닫는 방법에 대한 자세한 내용은 문서를 참조하십시오 폐기된 CI와 관련된 취약한 항목을 자동으로 닫습니다..

폐기된 CI는 결국 CMDB.

CI 폐기의 영향:

- 검색된 항목에 미치는 영향: CI가 폐기되면 관련 검색 항목(DI)이 'CI 해제됨'으로 표시됩니다.
- 취약한 항목에 미치는 영향: DI의 상태가 'CI 해제됨'으로 업데이트되면 연결된 VI가 닫히고 메모 섹션이 자동으로 업데이트됩니다.

주:
DI의 상태는 CI의 수명주기 상태가 업데이트될 때마다 자동으로 'CI 해제됨'으로 업데이트됩니다. 반면, 폐기 된 CI에 연결된 **VI** 자동 종결 옵션이 활성화된 경우에만 VI의 상태가 종결로 업데이트됩니다. 연결된 VI를 자동으로 닫는 방법에 대한 자세한 내용은 문서를 참조하십시오 폐기된 CI와 관련된 취약한 항목을 자동으로 닫습니다..

예약된 작업은 *Close detections/VIs for decommissioned CIs* 업데이트된 DI에 대해 매일 실행됩니다. 폐기된 CI에 대해 자동 닫기 구성 옵션이 활성화된 경우 해제된 CI가 포함된 DI를 식별하고 하위 상태가 'CI 해제됨'인 관련 VI를 닫습니다. 정정 작업의 모든 VI가 종결되고 해당 하위 상태가 CI 해제됨인 경우 정정 작업도 하위 상태가 "취소됨"으로 종결됩니다. 해제된 VI를 보려면 다음으로 이동하십시오. 취약성 대응 〉 취약 항목 〉 해제됨.

주:
CI가 '폐기됨' 상태에서 원래 상태로 다시 이동하면 '검색된 항목' 항목도 업데이트됩니다. 스캐너에서 데이터를 다시 수집하면 VI가 자동으로 열립니다.

폐기된 CI와 관련된 취약한 항목을 자동으로 닫습니다.

가 구성 관리 데이터베이스(CMDB) 구성 항목(CI)의 수명 주기 스테이지 상태를 폐기됨으로 변경하는 경우 연결된 취약한 항목(VI) 및 탐지를 자동으로 종결하도록 선택할 수 있습니다.

시작하기 전에
필요한 역할: sn_vul.admin

이 태스크 정보
의 취약성 대응v22.0부터 연결된 VI 및 탐지를 자동으로 닫으려면 시스템 속성을 *sn_vul_cmn.auto_close_vis_linked_retired_cis* 활성화하여 폐기된 CI와 연결된 VI를 자동으로 닫아야 합니다. 이 옵션을 사용하려면 값 필드를 '1'로 설정합니다. 반대로 이 옵션을 비활성화하려면 값 필드를 '0'으로 설정합니다.

업그레이드 중 v21.0 에서 취약성 대응시스템 속성이 *sn_vul_cmn.auto_close_vis_linked_retired_cis* 선택된 경우 값은 '1'로 유지됩니다. 이 옵션을 활성화하면 동일한 CI에 대해 보고된 신규 또는 기존 VI 및 탐지가 자동으로 생성되거나 '종결' 상태로 업데이트됩니다. 이는 스캐너 페이로드의 자산 ID와 검색된 항목 항목의 상태를

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

기반으로 합니다. 폐기된 CI의 영향에 대한 자세한 내용은 다음을 참조하십시오. 폐기된 구성 항목 작업

.

주:

- DI의 상태는 CI의 수명주기 상태가 업데이트될 때마다 'CI 해제됨'으로 업데이트됩니다. 반면, 폐기 된 CI에 연결된 **VI** 자동 종결 옵션이 활성화된 경우에만 VI의 상태가 종결로 업데이트됩니다.
- 다음 절차에 제공된 정보는 의 v22.0 취약성 대응이전 버전에만 적용됩니다. 의 취약성 대응v22.0부터 추가 검색 옵션을 구성할 수 있는 옵션이 있습니다. 자세한 내용은 자동 종결 규칙 생성 문서를 참조하십시오.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 자동 종결 구성 〉 구성 항목 수명 주기.
2. 폐기된 CI와 연결된 취약한 항목을 자동으로 종결하려면 폐기된 CI에 연결된 **VI** 자동 종결 확인란을 선택합니다.
3. 업데이트를 선택합니다.

주:
폐기된 CI에 연결된 **VI** 자동 종결 옵션이 활성화되기 전에 CI가 이미 폐기된 경우, 스캐너의 새로운 탐지에 대해서만 VI가 생성됩니다. 이러한 VI의 상태는 종결이고 하위 상태는 CI 해제됨입니다.

다시 열기 또는 대량 편집 옵션을 사용하여 상태가 CI 해제됨인 VI는 수동으로 다시 열 수 없습니다.

하위 상태가 고정 또는 부실인 종결된 VI는 새로운 탐지가 생성되고 VI를 새로운 취약성과 일치시킬 수 있는 경우 다시 열립니다. 자세한 내용은 탐지, 정정 작업 및 취약한 항목 상태 문서를 참조하십시오.

에서 부실 탐지 종결 취약성 대응

부실 탐지 자동 종결 모듈을 사용하면 외부 공급업체 통합에서 최근에 발견되지 않은 오래된 상태의 취약한 탐지를 자동으로 정리할 수 있습니다. 이러한 탐지를 종결로 이동하면 인스턴스의 활성 취약한 항목 및 정정 작업의 ServiceNow AI Platform 수가 줄어들고 CMDB의 자산을 조정하는 데 도움이 됩니다.

개요 및 주요 용어

탐지 데이터를 취약한 항목에 보다 정확하게 롤업하기 위해 부실 탐지 자동 종결 모듈을 사용하면 외부 공급업체 통합에서 최근에 발견되지 않은 오래된 상태의 취약한 항목 탐지를 정리할 수 있습니다. 이 기능에 대한 자세한 내용은 아래 사용 사례를 참조하십시오.

이전 버전에서 취약성 대응취약한 항목 자동 종결 모듈은 외부 공급업체 스캐너 통합에서 최근에 발견되거나 업데이트되지 않은 취약한 항목을 종결됨 - 부실로 자동 전환했습니다.

부실 탐지 자동 종결 기능을 활성화하기 전에 다음 용어, 취약한 항목 및 정정 작업에 상태가 롤업되는 방식, 탐지 데이터를 임포트하는 외부 공급업체 통합의 필요 조건을 검토하십시오.

이 기능을 활성화하려면 다음 문서를 참조하십시오 에서 부실 탐지 자동 종결 취약성 대응.

주요 용어

부실 탐지

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

오래되어 상당한 시간 동안 외부 공급업체 통합 검사에서 발견, 업데이트 또는 탐지되지 않은 인스턴스의 취약한 항목 ServiceNow AI Platform# 과 관련된 탐지를 나타냅니다.

마지막으로 발견된 탐지

이 검색 옵션은 외부 공급업체 스캐너에서 제공하는 날짜 및 시간을 사용합니다. 이 용어는 스캐너에서 탐지를 다시 발견한 가장 최근 또는 가장 늦은 날짜 및 시간을 나타냅니다.

마지막으로 스캔한 자산

이 검색 옵션은 외부 공급업체 스캐너에서 제공하는 날짜 및 시간을 사용합니다. 이 용어는 외부 공급업체 스캐너에서 자산을 마지막으로 검사한 최신 날짜 및 시간을 나타냅니다.

사용 케이스

때때로 자산(구성 항목)은 사용자 환경에서 해제되거나 외부 공급업체 스캐너에 의해 제거될 수 있으며, 관련 탐지는 취약한 항목 탐지에 의해 업데이트되지 않습니다. 그 결과 탐지 및 관련 취약한 항목이 애플리케이션에서 업데이트되지 취약성 대응 않고 비활성화(부실) 상태가 됩니다.

취약한 항목 데이터가 변경되지 않은 오래된 탐지를 종결하고 활성 VI 및 RT(정정 작업) 수를 줄이려면 부실 탐지 자동 종결을 활성화합니다. 이 기능은 설정한 검색 기준과 기간(일수)에 따라 외부 공급업체 스캐너 통합에서 최근에 발견되거나 업데이트되지 않은 취약한 항목 탐지를 자동으로 종결합니다.

예를 들어 특정 CI(구성 항목)에 여러 개의 자산 ID가 있고 지난 90일 동안 외부 공급업체 스캐너의 탐지에 대해 이러한 ID 중 하나가 임포트되지 않았다고 가정해 보겠습니다. 이 기능은 새로운 취약성 데이터가 없는 이 탐지를 자동으로 종결하므로 연결된 VI를 종결할 수 있습니다.

VI에는 하나 이상의 감지가 연결될 수 있으므로 이 기능은 설정한 파라미터에 의해 오래된 것으로 확인된 감지만 전환합니다. 예를 들어 VI에 4개의 탐지가 연결되어 있고 2개의 탐지가 부실한 경우(지난 90일 동안 새로운 취약성 데이터가 임포트되지 않은 경우) 이 기능은 부실 탐지만 종결합니다. VI를 닫기 전에 먼저 다른 두 개의 미해결 탐지를 정정해야 합니다.

탐지 상태를 VI로 롤업

자동 종결 탐지를 외부 공급업체 스캐너에 의해 종결된 탐지와 구분하기 위해 상태 필드에 대한 새 값인 부실이 추가되었습니다. 이 필드에 사용할 수 있는 값은 오픈, 종결 및 부실입니다. 부실은 탐지 자동 종결 기능으로 탐지가 종결되었음을 나타냅니다.

상태 우선순위: 오픈 > 종결 > 부실.

1. 탐지가 오픈 상태인 경우 연결된 VI 상태는 오픈 상태로 유지됩니다.
2. 탐지가 열려 있지 않고 일부는 종결되고 일부는 부실한 경우 연결된 VI 상태가 종결 - 고정으로 전환됩니다.
3. 모든 탐지가 부실한 경우 연결된 VI 상태가 종결 - 부실로 전환됩니다.

취약성 대응 20.0부터 탐지가 부실이고 관련 VI가 종결 상태인 경우 VI의 상태는 종결됨 - 부실로 전환되지 않습니다. 이는 새로운 탐지가 식별될 때 VI가 다시 열리지 않도록 하여 전체 가양성 요청 및 승인 프로세스를 거치지 않도록 하기 위한 것입니다. 이 동작을 되돌리려면 자동 종결 구성 양식에서 종결된 VI에 대한 부실 탐지 무시 확인란을 선택 해제합니다. 자세한 내용은 에서 부실 탐지 자동 종결 취약성 대응 문서를 참조하십시오.

정정 작업에 **VI** 상태 롤업**(VUL)**

상태 우선순위: 오픈 > 종결 - 고정 > 종결 - 부실.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

1. VUL(정정 작업)의 VI가 열려 있으면 VUL 상태가 변경되지 않습니다.
2. 하나 이상의 VI가 Closed - Fixed이고 나머지는 Closed - Stale인 경우 VUL 상태가 Closed - Fixed로 전환됩니다.
3. VUL의 모든 VI가 종결 - 부실인 경우 VUL 상태가 종결 - 취소됨으로 전환됩니다.
4. VI가 종결 – 긍정 오류로 종결된 경우 VUL이 자동으로 종결되지 않습니다.

상태 롤업 및 롤다운 시나리오에 대한 자세한 내용은 을 참조하십시오 상태 롤업 및 롤다운 시나리오.

자동 종결 탐지 및 외부 공급업체 통합 요구 사항

Microsoft TVM 사용자 및 부실 탐지 자동 종결

검사 목록 항목	설명
Microsoft TVM 취약성 통합	Microsoft TVM 취약성 통합에서 검색 기반으로 마지막으로 발견된 탐지 를 선택하는 경우 이 기능을 사용하려면 지난 7일 이내에 Microsoft TVM 머신 취약성 통합(전체 임포트)을 성공적으로 실행해야 합니다. 이 통합은 매주 실행됩니다. 마지막으로 발견된 탐지에 대해 부실 탐지 자동 종결이 활성화되고 구성되어 있으며 Microsoft TVM 머신 취약성 통합이 비활성화되었거나 지난 7일 이내에 데이터 임포트가 성공적으로 완료되지 않은 경우 탐지를 종결하는 예약된 작업은 계속 매일 실행되지만 일부 부실 탐지가 예상대로 닫히지 않을 수 있습니다. 검색을 기반으로 마지막으로 스캔한 자산을 선택하면 Microsoft TVM 머신 취약성 통합을 실행할 필요가 없습니다. 이 통합을 활성화하려면 다음을 수행합니다. 1. 다음으로 이동 **Microsoft TVM** 취약성 통합 〉 관리 〉 통합. 2. **Microsoft TVM** 머신 취약성 통합(전체 임포트)을 찾아 사용하도록 설정합니다.
(선택 사항) 사용자 환경에 Microsoft TVM 통합의 여러 인스턴스를 배포합니다.	필요에 따라 환경 전체에 통합의 여러 인스턴스를 배포할 수 있습니다. 부실 탐지 자동 종결은 인스턴스별로 다르며 환경 전반에서 활성화되거나 비활성화됩니다. 부실 탐지는 통합 실행을 성공적으로 완료한 인스턴스에서 자동으로 부실로 전환됩니다. 부실 탐지 자동 종결이 활성화되어 있고 인스턴스에서 매주 실행되는 통합을 비활성화하는 경우 탐지를 종결하는 예약된 작업은 계속 매일 실행되지만 일부 탐지는 예상대로 자동으로 부실로 전환되지 않을 수 있습니다.

Qualys 사용자 및 부실 취약한 항목 자동 종결

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 탐지 데이터를 검색하는 활성화된 Qualys 모든 외부 공급업체 통합을 이 모듈로 실행할 수 있습니다. 특정 Qualys 응용 프로그램이 필요하지 않습니다.
- 필요에 따라 환경 전체에 통합의 Qualys 여러 인스턴스를 배포할 수 있습니다.
- 부실 탐지 자동 종결은 인스턴스별로 다르며 환경 전반에서 활성화되거나 비활성화됩니다. 부실 탐지는 모든 인스턴스에서 부실로 자동 전환됩니다.

Rapid7 사용자 및 부실 탐지 자동 종결

검사 목록 항목	설명
Rapid7 취약성 통합	검색 기반으로 마지막으로 발견된 탐지를 선택하는 경우 이 기능을 사용하려면 지난 7일 이내에 포괄적인 취약한 항목 통합 중 Rapid7 하나를 실행해야 합니다. 이러한 포괄적인 통합은 매주 실행됩니다. • 데이터 웨어하우스의 경우 Rapid7 Nexpose 포괄적인 취약한 항목 통합에서 Rapid7 성공적인 실행이 필요합니다. • 의 경우 Rapid7 InsightVM포괄적인 취약한 항목 통합 API에서 Rapid7 성공적으로 실행해야 합니다. 마지막으로 발견된 탐지에 대해 부실 탐지 자동 종결이 활성화되고 구성되어 있으며 포괄적인 취약한 항목 통합이 Rapid7 비활성화되었거나 지난 7일 이내에 데이터 임포트가 성공적으로 완료되지 않은 경우 탐지를 종결하는 예약된 작업은 계속 매일 실행되지만 일부 부실 탐지는 예상대로 닫히지 않을 수 있습니다. 검색 기반으로 마지막으로 스캔한 자산을 선택하는 경우 포괄적인 Rapid7 통합 실행이 필요하지 않습니다. 이러한 통합을 활성화하려면 다음을 수행합니다. **1.** 다음으로 이동 **Rapid7** 취약성 통합 〉 관리 〉 통합. **2.** 필요한 포괄적인 취약한 항목 통합을 찾아서 활성화합니다 Rapid7 . 주: 매주 Rapid7 NexposeRapid7 InsightVM 실행되고 각 통합에는 매일 실행되는 VI 통합, Rapid7 취약한 항목 통합 및 Rapid7 취약한 항목 통합 - API가 있습니다. 매일 및 매주 Rapid7 통합을 모두 사용하는 경우 한 번에 하나의 통합만 실행됩니다. 이러한 통합 작업 중 하나가 실행 중인 경우 다른 통합에 대한 작업은 예약된 다음 작업까지 건너뜁니다.
(선택 사항) 사용자 환경에 통합의 Rapid7 여러 인스턴스를 배포합니다.	필요에 따라 환경 전체에 걸쳐 포괄적인 통합의 여러 인스턴스를 배포할 수 있습니다. 부실 탐지 자동 종결은 인스턴스별로 다르며 환경 전반에서 활성화되거나 비활성화됩니다. 부실 탐지는 통합 실행을 성공적으로 완료한 인스턴스에서 자동으로 부실로 전환됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

검사 목록 항목	설명
	부실 탐지 자동 종결이 활성화되어 있고 인스턴스에서 매주 실행되는 통합을 비활성화하는 경우 탐지를 종결하는 예약된 작업은 계속 매일 실행되지만 일부 탐지는 예상대로 자동으로 부실로 전환되지 않을 수 있습니다.

Tenable 취약성 통합 사용자 및 부실 취약 항목 자동 종결

- 탐지 데이터를 검색하는 Tenable 취약성 통합에서 활성화된 모든 통합을 이 모듈로 실행할 수 있습니다. 특정 Tenable 취약성 통합은 필요하지 않습니다.
- 필요에 따라 환경 전체에 Tenable 취약성 통합의 여러 인스턴스를 배포할 수 있습니다.
- 부실 탐지 자동 종결은 인스턴스별로 다르며 환경 전반에서 활성화되거나 비활성화됩니다. 부실 탐지는 모든 인스턴스에서 부실 로 자동 전환됩니다.

통합이 올바르게 구성되었는지 확인한 후에는 을 참조 에서 부실 탐지 자동 종결 취약성 대응 하여 기능을 활성화합니다.

부실 취약한 항목 자동 종결에서 부실 탐지 자동 종결로 정보 업그레이드

부실 탐지 자동 종결 모듈의 경우, 이전에 부실 취약한 항목 자동 종결을 사용한 경우 다음을 수행합니다.

- 부실 취약한 항목 자동 종결에서 마지막으로 스캔한 자산 옵션에 입력한 일 수에 대한 값은 부실 탐지 자동 종결에서 마지막으로 스캔된 자산 에 대해 자동으로 보존됩니다.
- 부실 취약한 항목 자동 종결에서 마지막으로 발견된 취약한 항목 옵션에 입력한 일 수 값은 부실 탐지 자동 종결에서 마지막으로 발견된 탐지 에 대해 자동으로 보존됩니다.
- 취약한 항목이 종결 상태인 기존 미결 탐지 - 부실은 업그레이드 후 예약된 작업이 실행될 때 *`Auto-Close Stale Detections`* 자동 종결 닫기 구성 설정에 따라 부실로 전환됩니다.

롤업 정보

- 취약한 항목이 업그레이드 전에 종결 - 부실이었고 업그레이드 후 모든 탐지가 부실로 표시된 경우 VI 상태는 종결 - 부실로 유지됩니다.
- 업그레이드 전에 취약한 항목이 종결 - 부실이었으며 업그레이드 후 탐지 중 일부만 부실로 표시되고 나머지는 스캐너에 의해 종결된 경우 취약한 항목은 롤업 논리에 따라 종결 - 수정됨으로 전환됩니다.

에서 부실 탐지 자동 종결 취약성 대응

부실 탐지 자동 종결을 활성화하여 외부 공급업체 통합에서 최근에 발견되지 않은 부실하고 취약한 탐지를 자동으로 종결합니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin 또는 sn_vuln.admin(사용하지 않음) 또는 sn_vul.manage_auto_close_stale_vi 세분화된 역할을 가진 취약성 관리자.

이 기능, 주요 용어 및 탐지 데이터를 임포트하는 외부 공급업체 통합에 필요할 수 있는 설정에 대한 자세한 내용은 문서를 참조하십시오 에서 부실 탐지 종결 취약성 대응 .

주:
다음 절차에 제공된 정보는 의 v22.0 취약성 대응이전 버전에만 적용됩니다. 의 취약성 대응v22.0부터 추가 검색 옵션을 구성할 수 있는 옵션이 있습니다. 자세한 내용은 자동 종결 규칙 생성 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 취약성 대응 〉 관리 〉 자동 종결 구성 〉 부실 탐지.
   부실 구성 자동 종결 양식이 표시됩니다.
2. 필드에 내용을 입력합니다.
3. 부실 탐지 자동 종결 기준 필드의 경우 검색에 사용할 옵션을 하나 선택합니다.

   두 검색 모두 오래된 부실 탐지의 기간을 스캐너에서 제공한 날짜와 일 수로 일치시킵니다.

   주:
   v22.0 부터 취약성 대응마지막으로 발견된 탐지 및 마지막으로 스캔한 자산 옵션이 목록으로 생성됩니다.

   - 마지막으로 발견된 탐지입니다. 이 옵션은 스캐너에서 탐지를 다시 찾은 가장 최근 날짜 또는 최근 날짜를 검색합니다.

     주:
     TVM Microsoft 사용자의 경우 Rapid7 현재 감지 정보가 필요하다는 경고 메시지가 표시됩니다.

     검색의 기반으로 마지막으로 발견된 탐지 를 선택하는 경우 이 기능을 사용하려면 지난 7일 이내에 포괄적인 취약한 항목 통합 중 Rapid7 하나의 통합을 성공적으로 실행해야 합니다.

     검색 기반으로 마지막으로 발견된 탐지를 선택하는 경우 이 기능을 사용하려면 지난 7일 이내에 Microsoft TVM 머신 취약성 통합(전체 임포트)의 통합을 성공적으로 실행해야 합니다.

   - 마지막으로 검사한 자산입니다. 이 옵션은 외부 공급업체 스캐너에서 자산을 마지막으로 검사한 가장 최근 날짜를 검색합니다.
4. 및 Microsoft TVM 사용자의 경우에만 Rapid7 필요한 통합이 활성화되어 있는지 확인합니다.
   자세한 내용은 AND Microsoft Threat and Vulnerability Management 취약성 통합 이해 문서를 참조하십시오Rapid7 취약성 통합 이해.
5. 모듈을 활성화하려면 활성 확인란을 클릭하여 선택합니다.
6. 마지막으로 발견된 탐지(일 전) 필드에 오래된 오래된 오래된 탐지의 기간을 일 수로 입력합니다.

   기본값은 90일입니다. 일수에 대한 양수 값을 입력할 수 있습니다. 이 값은 스캐너에서 제공한 날짜를 일치시키는 데 사용됩니다. 90 및 마지막으로 발견된 탐지 가 표시되면 지난 90일 동안 발견되지 않은 탐지는 자동으로 종결됩니다. 90 및 마지막으로 스캔한 자산 이 표시되면 지난 90일 동안 스캔되지 않은 자산과 연결된 모든 탐지가 자동으로 종결됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

이 기능에 대한 마지막으로 발견된 탐지/마지막으로 검사한 자산(일 전) 필드와 Rapid7 포괄적인 취약한 항목 통합 – API 및 Microsoft TVM 머신 취약성 통합의 다음 이후 임포트 필드 간에는 관계가 있습니다.

이러한 통합의 경우 구성 페이지의 다음 이후 임포트 필드는 기본적으로 비어 있습니다.

값을 입력하지 않거나 필드에 값이 없으면 마지막으로 발견된 탐지/마지막으로 스캔한 자산(일 전) 필드에 구성된 일 수에 대한 데이터가 사용됩니다.

예를 들어 자동 종결 구성 양식에 정의된 일 수가 90이고 다음 이후 임포트 필드가 통합 구성 페이지에서 비어 있는 경우 첫 번째 통합 실행은 지난 90일 동안의 데이터를 임포트합니다. 포괄적인 취약한 항목 통합 - API 및 Microsoft TVM 머신 취약성 통합의 Rapid7다음 이후 임포트 필드를 편집할 수 있으므로 원하는 값을 제공할 수도 있습니다. 자동 종결 기능이 가양성을 종결하지 않도록 필드가 비어 있는 경우 90일 값이 기본값으로 제공됩니다.

이러한 필드 간의 이 관계는 첫 번째 통합 실행에만 적용됩니다. 그 이후에는 부실 취약한 탐지 자동 종결 양식에서 마지막으로 발견된 탐지/마지막으로 스캔한 자산(일 전) 필드를 변경해도 통합 구성 페이지의 다음 이후 임포트 필드에 영향을 미치지 않습니다. 후속 통합 실행에서 델타 정보만 임포트하도록 필드가 첫 번째 실행의 시작 시간으로 변경됩니다.

7. 옵션: 지연된 VI 또는 현재 지연 검토 중인 VI에 매핑된 부실 탐지를 무시하려면 지연 된 VI에 대한 부실 탐지 무시 확인란을 선택합니다.

   (Optional) 이 옵션을 비활성화하면 지연된 VI 또는 지연 검토 중인 VI에 매핑되는 기준과 일치하는 모든 탐지가 종결됩니다. 지연된 VI 또는 이러한 탐지에 해당하는 검토 중인 VI도 롤업 논리에 따라 자동으로 종결됩니다. 롤업 논리에 대한 자세한 내용은 해당 상태 롤업 및 롤다운 시나리오문서를 참조하십시오에서 부실 탐지 종결 취약성 대응.

   이 옵션을 활성화하면 지연된 VI 또는 지연을 위해 검토 중인 VI에 매핑되는 기준과 일치하는 탐지는 자동 종결 중에 건너뜁니다.

8. 옵션: 종결된 VI에 대한 부실 탐지 무시 확인란의 선택을 취소합니다.

   (Optional) 기본적으로 이 확인란은 이 종결된 VI와 관련된 새로운 검출이 식별될 때 종결된 VI가 다시 열리지 않도록 선택됩니다. 롤업 논리에 대한 자세한 내용은 해당 상태 롤업 및 롤다운 시나리오문서를 참조하십시오에서 부실 탐지 종결 취약성 대응 .

9. 변경 사항을 저장하려면 업데이트를 클릭합니다.

   Auto-Close Stale Detections 예약된 작업은 매일 실행됩니다. 이 작업은 탐지가 마지막으로 발견된 날짜 또는 자산을 마지막으로 스캔한 날짜를 선택했는지 여부를 결정합니다. 그런 다음 해당 탐지를 부실 상태로 전환합니다. 부실 탐지 자동 종결 기능은 활성 통합 인스턴스에 대한 부실 탐지만 종결한다는 점에 유의해야 합니다. 활성 통합 인스턴스와 관련된 취약한 항목 및 탐지가 종결됩니다. v22.0 취약성 대응 부터 예약된 작업이 공통 테이블 〔sn_vul_cmn_auto_close_rule〕을 고려하여 수정되었습니다.

   탐지가 부실로 표시된 후 스캐너가 해당 탐지 발견을 다시 보고하면 탐지의 상태 필드가 미결로 전환됩니다. 탐지의 해당 취약한 항목도 다시 열립니다.

   또한 탐지가 부실로 표시되고 스캐너에서 수정됨으로 확인되면 탐지가 종결로 전환됩니다. 상태는 VI로도 롤업됩니다.

자동 종결 규칙 생성

자동 종결 규칙을 사용하여 설정한 필터 조건에 따라 오래된 탐지를 자동으로 종결합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_vul.manage_auto_close_stale_vi

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 자동 종결 규칙.

   기본 시스템은 다음과 같은 자동 종결 규칙을 제공합니다.

   - 마지막으로 검사한 자산: 지난 90일 이내에 검사되지 않은 자산과 연결된 탐지는 부실 상태로 전환됩니다.
   - 마지막으로 발견된 수동 탐지: 지난 90일 이내에 발견되지 않은 수동 탐지입니다. 마지막으로 발견된 탐지 기록을 활성화하는 경우 이 기능을 사용하려면 지난 7일 이내에 포괄적인 취약한 항목 통합 및 Microsoft TVM 머신 취약성 통합(전체 임포트)의 Rapid7 성공적인 통합이 필요합니다.
   - 마지막으로 발견된 탐지: 지난 90일 이내에 발견되지 않은 탐지입니다.

2. 새로 만들기를 선택하여 새 자동 종결 규칙을 만듭니다.
3. 양식에서 필드에 입력합니다.

필드	값
이름	자동 종결 규칙의 이름입니다.
활성	규칙을 활성화하는 옵션입니다. 활성화되면 필터 기준과 일치하는 탐지를 자동으로 종결합니다.
지연된 항목 무시	이 옵션을 선택하면 검토 중 또는 연기됨 상태에 매핑된 모든 탐지가 무시되고 종결되지 않습니다. 이 옵션의 선택을 취소하면 조건과 일치하는 모든 탐지가 종결됩니다.
실행 순서	자동 종결 규칙의 실행을 위한 고유 값입니다. 이 값은 실행 순서를 결정합니다. 기본값은 100입니다.
설명	자동 종결 규칙에 대한 설명입니다.
조건	종결해야 하는 탐지를 식별하는 데 사용되는 필터 조건입니다.

4. 제출을 선택합니다.

   Auto-Close Stale Detections 예약된 작업은 매일 실행됩니다. 지정된 조건에 따라 탐지를 식별하고 일치하는 탐지를 부실 상태로 전환합니다. 이 작업은 다음 시나리오를 처리합니다.

   - 취약한 항목(VIT) 내의 모든 탐지가 부실로 표시되면 하위 상태가 "부실"로 설정된 VIT가 종결됩니다.
   - VIT 내에 열려 있는 탐지가 하나 이상 있고 다른 탐지가 부실 상태인 경우 VIT는 열린 상태로 유지됩니다.
   - VIT 내에 "종결" 및 "부실" 상태의 탐지가 모두 있는 경우 VIT는 하위 상태가 "고정"으로 설정된 상태로 종결됩니다.

   최신 버전의 취약성 대응로 업그레이드하면 자동 종결 규칙에 설정된 조건도 그에 따라 업데이트됩니다. 또한 규칙이 다른 도메인과 연결된 경우 해당 도메인 내에서 규칙이 특별히 생성됩니다.

분류되지 않은 하드웨어 재분류

CI 조회 규칙을 업데이트하여 분류되지 않은 하드웨어를 재분류합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_sec_cmn.admin

이 태스크 정보
호스트 임포트 맵 [sn_sec_cmn_src_cmdb_map] 테이블에는 페이로드의 수신 변수와 검색된 항목 테이블에 해당 할당이 표시됩니다. 경우에 따라 스캐너와 Discovery 간의 명명 규칙이 일치하지 않으면 하드웨어가 분류되지 않은 상태로 남을 수 있습니다. 분류되지 않은 새 하드웨어 CI를 작성하는 동안 페이로드의 이름에 호스트 이름만 포함되어 있는지 확인하십시오. 나중에 Discovery가 자산을 식별하면 적절한 CI 클래스로 다시 분류할 수 있습니다. 필요한 경우 스크립트를 작성하여 Discovery와 CMDB(구성 관리 데이터베이스) 모두의 CI 이름과 일치하는 파생 값을 생성할 수 있습니다.

IRE(식별 및 조정 엔진)가 활성화되면 검색된 항목의 재분류 옵션이 지원되지 않습니다.

프로시저

1. 호스트 임포트 맵 〔sn_sec_cmn_src_cmdb_map〕 테이블로 이동합니다.
2. 소스를 선택합니다.
3. 대상 필드 목록에서 이름을 선택합니다.
   스크립트 사용 확인란이 표시됩니다.

   주:
   - 스크립트는 대상 필드 목록에서 이름을 선택한 경우에만 사용할 수 있습니다.
   - 대상 필드 목록에서 다른 옵션에 대한 스크립트를 추가하려면 다음과 같은 방법으로 UI 정책을 비활성화해야 합니다.
     - '사용 스크립트 설정 아니오'를 비활성화합니다.
     - "스크립트 사용 표시 또는 숨기기"를 비활성화합니다.
     - "스크립트 표시 또는 숨기기 정책"에서 "대상 필드가 이름임" 조건을 제거합니다.
   - 호스트 임포트 맵 테이블이 두 개의 새 열인 스크립트 및 스크립트 사용으로 업데이트됩니다.

4. 스크립트 사용 확인란을 선택합니다.
   스크립트 필드에는 기본 스크립트가 표시되지만 사용자 지정 스크립트를 생성할 수 있는 옵션이 있습니다. 이 필드에서 데이터베이스의 명명 규칙에 맞게 소스 및 파생 값을 지정할 수 있습니다. 스크립트에서 생성된 값은 sourcePayload〔'DERIVED'〕〔rule.source_field〕에 저장됩니다. 해당 테이블을 체크인할 때 소스 페이로드, 파생 및 대상 속성 값을 활용하도록 CI 조회 규칙이 조정되었는지 확인합니다.
5. 이전의 중복 기록에 스크립트를 적용하려면 다음을 수행합니다.

   a. 다음으로 이동 모두 〉 취약성 대응 〉 검색된 항목.

   b. 중복 기록을 선택합니다.

   c. 선택한 행에 대한 작업 목록에서 **CI** 조회 규칙 다시 적용을 선택합니다.
      기존 자산과의 일치 항목을 보여줍니다.

6. 에 대한 Tenable.io스크립트를 적용하려면 다음을 수행합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 다음으로 이동 취약성 대응 호스트 임포트 맵.

b. NetBIOS, 호스트 이름 및 FQDN 이름이 소스 필드인 행에 대한 스크립트를 선택합니다.

c. 각 요소에 대한 스크립트를 업데이트합니다.

주:
의 경우 Tenable.io스캐너는 스크립트가 예상대로 작동하지 않는 NetBIOS, HOSTNAMES 및 FQDNS 이름에 대한 배열을 반환합니다.

의 Tenable.io 호스트 임포트 맵에는 소스 필드에 **netbios_name** 포함되어 있으므로 스크립트를 작성해야 합니다. 조회하는 동안 값 배열이 있는 다른 소스 필드 **NETBIOS** 가 사용됩니다. 따라서 테이블에 새 행이 추가되고 스크립트의 루프에 동일한 논리를 작성해야 합니다. **FQDNS** 및 **HOSTNAMES**의 경우에도 마찬가지입니다.

7. 에 대한 Rapid7스크립트를 적용하려면 다음을 수행합니다.

a. 다음으로 이동 모두 〉 취약성 대응 호스트 임포트 맵.

b. FQDN 및 HostName이 있는 행의 경우 Rapid7 조회 메서드를 스크립트로 업데이트합니다.

주:
의 경우 Rapid7CI 조회 메서드가 FQDN 및 호스트 이름에 대한 필드 일치로 설정되어 스크립트를 사용하지 못하도록 합니다.

에서 수동으로 정정 작업 생성 취약성 대응

정정 작업 규칙 기준 이외의 기준으로 취약한 항목을 그룹화하려면 정정 작업을 수동으로 생성합니다. 예를 들어 특정 관리자에 대한 작업 또는 다양한 취약성이 포함된 랜섬웨어와 같은 활성 상태의 새로운 익스플로잇에 대한 작업을 만들 수 있습니다. 그룹화되지 않은 취약한 항목을 그룹화하는 데 사용할 수도 있습니다.

중요사항:
다음 위치에서 호스트 업데이트 적용 작업을 생성할 수 있습니다.

- 취약성 관리자 작업 공간sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin 역할을 가진 사용자로
- IT 정정 작업 공간 sn_vul.remediation_owner 역할을 가진 사용자로

시작하기 전에
필요한 역할: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin 또는 sn_vul.admin(사용되지 않음)

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 정정 작업.

정정 작업 규칙은 이전에 작동했던 정정 작업 규칙과 동일한 방식으로 작동하며 계속해서 사용할 수 있습니다. 그러나 작업 공간에서 보안 관리자와 IT 팀이 사용할 수 있는 기능에 익숙해지면 정정 작업 규칙을 비활성 상태로 두는 것을 선호할 수 있습니다.

2. 작업 범주 중 하나를 선택하여 목록을 엽니다.

3. 새로 만들기를 클릭합니다.

4. 양식의 필드에 적절히 입력합니다.
특정 필드에 대한 자세한 내용은 다음 문서를 참조하십시오 정정 작업 양식 필드.

5. 제출을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업이 생성되면 조건 또는 필터 그룹 필터 유형을 사용하여 취약한 항목 관련 목록에서 일치하는 모든 취약한 항목을 검색하여 표시합니다.

관련 링크, 취약성 재검사를 사용하여 시작된 검사를 수동으로 트리거 ServiceNow# 할 수 있습니다. 취약성 스캐너를 구성하는 방법에 대한 자세한 내용은 을 참조하십시오 취약성 스캐너 및 검사 구성 및 관리 Qualys.

Qualys 취약성 통합의 경우 취약성 스캐너 모듈에 기본 스캐너가 사전 설치되어 있습니다 . 이 스캐너는 기본적으로 비활성화되어 있습니다. 정정 작업 및 취약한 항목 양식에서 취약성 검사 관련 링크를 통해 작동하도록 Qualys 스캐너를 활성화하려면 활성 및 기본값 확인란을 선택합니다.

업데이트 상태 관련 링크에는 마지막 업데이트의 날짜와 시간이 표시됩니다. 정정 작업의 VI에서 정보를 롤업합니다. 자세한 내용은 정정 작업 양식 필드 문서를 참조하십시오. 특정 취약성을 기반으로 작업이 형성되면 해당 취약성이 정정 작업 양식에 나열됩니다.

연결된 취약한 항목을 열면 연결된 정정 작업 항목이 정정 작업 관련 목록 탭 아래에 나타납니다.

Vulnerability Response 그룹에 사용자 추가

종결/지연 기능을 사용하여 검사 취약성 대응 없이 취약한 항목을 연기하거나 종결하면 요청을 승인하거나 거부하라는 알림이 그룹에 전송됩니다. 적절한 사용자를 할당할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 〉 사용자 관리 〉 그룹.
2. 취약성 대응 그룹을 엽니다.
3. 그룹 구성원 관련 목록을 클릭하고 편집을 클릭합니다.
4. 컬렉션 목록에서 하나 이상의 이름을 선택합니다.
5. 추가를 클릭합니다.
6. 저장을 클릭합니다.

관련 정보

사용자 생성

수동으로 개별 취약한 항목 관리

취약한 항목은 지정된 취약성이 있는 하나의 CI(구성 항목)를 나타냅니다. 취약한 항목은 외부 공급업체 소스에서 임포트하거나 SAM NVD 정보(링크)를 사용하여 취약성 항목을 소프트웨어 자산 관리 모듈에서 검색된 소프트웨어 기록과 비교합니다.

취약한 항목이 취약성 규칙에 의해 정의된 정정 작업에 포함됩니다. 일반적으로 정정 작업은 취약한 항목 그룹이 할당되고 작업되는 위치입니다.

취약한 항목 모듈에서 취약한 항목을 대량으로 보고 편집할 수 있습니다. 취약한 항목 레코드는 취약성 탭에 취약성의 정보를 표시합니다. 이 탭은 공개 또는 활성 익스플로잇이 있는지 여부를 나타낼 수 있습니다. 또한 패치, 구성 변경 또는 둘의 조합을 통해 정정할 수 있는지 여부를 보여줍니다. 중복 제거 중에 발견된 IP 주소가 있으면 관련 목록에 표시됩니다.

CI가 CMDB에서 제거되면 관련된 모든 취약한 항목도 제거됩니다.

취약한 항목이 정정 작업에 추가되면 해당 그룹이 취약한 항목의 정정 작업 목록에 나타납니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약한 항목에 영향을 주는 작업이 생성되면 해당 작업은 취약한 항목의 영향 받는 작업 관련 목록에 나타납니다.

취약한 항목을 수동으로 생성할 수 있습니다. 보안 인시던트 또는 변경 요청을 생성하고 수동으로 종결하거나 지연할 수 있습니다. 수동으로 생성한 취약한 항목에 정정 작업 규칙을 적용할 수 있습니다.

정정 작업 및 정정 작업 규칙이 작업 기능을 인계하도록 개선되었습니다. 취약한 항목을 상위 작업으로 연결할 수 없습니다.

취약한 항목 생성 취약성 대응

여러 방법이 VI(취약한 항목)를 생성합니다. 가장 일반적으로 취약성 스캐너에 대한 통합이 설치되고 야간에 결과를 임포트하도록 구성됩니다. 물리적 보안 취약성과 같이 취약한 항목 레코드를 수동으로 추가하는 것이 더 좋은 경우가 있습니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_write

이 태스크 정보
수동으로 생성한 VI와 자동으로 생성된 VI는 정정 작업 규칙 및 그룹 조건에 따라 정정 작업에서 자동으로 추가되고 제거됩니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 취약 항목.
2. 범주를 선택하여 목록을 엽니다.
3. 새로 만들기를 클릭합니다.
4. 양식의 필드에 적절히 입력합니다.
   취약한 항목 필드에 대한 자세한 내용은 을 참조하십시오 취약성 대응 취약한 항목 양식 필드.
5. 양식 헤더를 마우스 오른쪽 버튼으로 클릭하고 저장을 클릭합니다.

   정정 작업 규칙은 취약한 항목을 평가하고 기존 작업에 추가하거나 새 작업을 생성합니다. 평가에 실패하면 취약한 항목이 그룹화되지 않은 취약한 항목 목록에 추가됩니다.

   취약한 항목을 새로 저장하면 활성화된 모든 계산기가 실행됩니다.

   > **주:**
   > 대상 필드당 한 번에 하나의 계산기만 활성화할 수 있습니다. 하나를 활성화하면 동일한 대상 필드를 가진 다른 항목이 비활성화됩니다.

6. 관련 목록을 클릭하면 추가 정보를 볼 수 있습니다.

   관련 링크, 취약성 검사를 사용하여 시작된 검사를 수동으로 트리거 ServiceNow# 할 수 있습니다. 취약성 스캐너를 구성하는 방법에 대한 자세한 내용은 을 참조하십시오 취약성 스캐너 및 검사 구성 및 관리 Qualys.

   Qualys 취약성 통합의 경우 취약성 스캐너 모듈에 기본 스캐너가 사전 설치되어 있습니다 . 이 스캐너는 기본적으로 비활성화되어 있습니다. 정정 작업 및 취약한 항목 양식에서 취약성 검사 관련 링크를 통해 작동하도록 Qualys 스캐너를 활성화하려면 활성 및 기본값 확인란을 선택합니다.

   헤더 표시줄에서 다음과 같은 편집 및 정정 옵션을 사용할 수 있습니다.

   - 업데이트: 양식에 대한 업데이트를 저장합니다.
   - 보안 인시던트 생성: 보안 인시던트를 생성합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 닫기: 항목을 닫습니다. 해당 그룹의 모든 항목이 닫힌 경우 정정 작업이 자동으로 닫힙니다.
- 예외 요청: 항목 지연 요청을 제출합니다.
- 해결: 항목을 해결합니다.
- 삭제: 취약한 항목을 제거합니다.

관련 정보

에서 취약한 항목을 대량으로 편집 취약성 대응

취약한 항목 지연

취약한 항목(VIT)과 관련된 문제가 위험도가 낮고 추가 분석 없이 즉시 지연될 수 있는 것으로 확인되면 지연 기능을 사용할 수 있습니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)
가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

이 태스크 정보
예약된 작업이 매일 실행되어 재개시 날짜에 도달한 지연된 취약한 항목을 확인합니다. VI의 연기가 만료되도록 설정된 날에 기록이 다시 열립니다.

취약성 대응 v20.0부터 지연된 VI를 다시 열기 전에 ### ## # ## ## ## ## 예약된 작업은 지연된 VI에 적용 가능한 예외 규칙이 있는지 확인하고 예외 규칙에 따라 이유 및 때까지 필드를 업데이트합니다. VI의 상태는 최근 만료 날짜까지 연기됨 상태로 유지됩니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 취약 항목.
2. 취약한 항목을 엽니다.
3. 예외 요청을 클릭합니다.
4. 양식의 필드에 적절히 입력합니다.

필드	설명
다음까지	연기됨 상태가 만료되고 정정 작업이 다시 활성화되는 날짜를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	주: (VR) 버전 18.0 취약성 대응 부터 예외 기간이 만료되기 전에 지연된 취약한 항목을 닫고 스캐너에서 다시 열면 VIT의 상태가 활성 예외 창을 적용하는 지연 상태로 되돌아갑니다. 이 기능을 활성화하려면 시스템 속성 sn_vul.auto_defer_vit_in_active_exception_window의 값을 true로 설정합니다. 또한 지연된 종료 날짜는 취약한 항목이 종결되거나 예외가 만료된 후에도 유지됩니다. 필요한 역할은 읽기와 쓰기 모두에 대해 sn_vul.manage_exception_configuration입니다. 기록이 제출된 후 이메일 알림이 정의되어 있으면 만료 날짜가 1주일 이내이면 그룹 구성원 취약성 대응 은 이메일을 받습니다. 지연 날짜가 만료되면 취약한 항목이 다시 열림으로 설정되고 두 번째 이메일 알림이 전송됩니다.
이유	문제를 지연시키는 이유를 입력합니다. 선택 항목은 다음과 같습니다. ○ 유지관리 기간을 기다리는 중 ○ 긍정 오류 ○ 수정 사용 불가 ○ 수용된 위험 ○ 사용 중인 완화 통제 ○ 기타
추가 정보	기타 관련 정보를 입력합니다.

5. 제출을 클릭합니다.
그룹이 검토 중으로 표시됩니다. 다시 열기 관련 링크가 나타납니다. 재개시된 날짜와 이유는 상태 변경 승인 탭 아래의 작업 메모에 표시됩니다.

지연된 취약한 항목에 대한 연장 요청

지연된 취약한 항목이 지연 종료 기한에 도달하기 전에 해당 항목에 대한 연장을 요청합니다. 정정 소유자는 더 이상 이 요청을 하기 위해 지연된 기한까지 기다릴 필요가 없습니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)

이 태스크 정보
작업 공간에서 연장을 취약성 대응 요청할 수도 있습니다. 자세한 내용은 취약성 관리자 작업 공간에서 지연된 취약한 항목에 대한 연장 요청 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 취약 항목.
2. 지연된 취약한 항목을 엽니다.
3. 연장 요청을 선택합니다.

   주:
   연장 요청 버튼은 취약한 항목의 상태가 연기됨인 경우에만 표시됩니다.

4. 양식의 필드에 적절히 입력합니다.

필드	설명
연장 날짜	정정을 위해 지연된 취약한 항목을 연장해야 하는 종료 날짜를 선택합니다.
이유	문제를 지연시키는 이유를 입력합니다. 선택 항목은 다음과 같습니다. ○ 유지관리 기간을 기다리는 중 ○ 수정 사용 불가 ○ 수용된 위험 ○ 사용 중인 완화 통제 ○ 기타
추가 정보	기타 관련 정보를 입력합니다.

5. 승인 요청을 선택합니다.
   이메일은 요청 제출 및 승인자의 후속 조치 시 트리거됩니다.

   주:
   - 요청은 두 가지 수준의 승인을 거칩니다.
   - 지연된 예외 규칙이 다시 확장되면 백엔드에서 연장 지연 수가 증가합니다.

6. 요청이 승인되면 기한, 이유 및 연기 메모가 업데이트됩니다.

취약 항목 새로 고침 취약성 대응

상태 업데이트 관련 링크는 취약한 항목을 검사하여 정정 작업에 속하는 추가 취약한 항목이 있는지 확인하는 데 사용됩니다. 예약된 작업 외부에서 업데이트가 보장되는 경우 이를 사용합니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_write 또는 sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)
가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보
상태 업데이트 관련 링크는 오픈 또는 조사 중 상태의 정정 작업 양식에서만 필터 그룹을 사용하거나 필터 유형이 조건인 상태로 편집할 수 있습니다. 이 검사는 취약한 항목 자동 새로 고침 확인란의 상태와 관계없이 수행됩니다.

의 취약성 대응v22.0부터 및 IT 정정 작업 공간의 정정 작업에 취약성 관리자 작업 공간 대한 기록 뷰에서 상태 업데이트 버튼을 사용할 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 정정 작업.
2. 오픈 또는 조사 중 상태의 기록을 엽니다.
3. 상태 업데이트**(Update status)** 링크를 클릭합니다.
   취약한 항목 탭 아래에 새로운 취약한 항목이 나타납니다.

외부 공급업체 소프트웨어의 보안 문제 식별 및 에스컬레이션

외부 공급업체 항목에서 반환된 소프트웨어 취약성을 보고 정정을 결정할 수 있습니다. 이 정보를 사용하여 취약한 소프트웨어 항목을 소프트웨어 자산 관리 검색 모델과 매칭합니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_write

가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

프로시저

1. 다음으로 이동 모두 〉 취약성 〉 라이브러리 〉 외부 공급업체.
   다운로드된 취약한 소프트웨어 목록이 표시됩니다.
2. 소프트웨어 기록을 클릭하여 취약성 정보를 봅니다.
3. 다음 관련 목록을 클릭하여 취약성을 식별하기 위한 자세한 정보를 확인합니다.
   취약성이 식별되고 취약한 항목이 생성된 경우 필요에 따라 수행할 수 있습니다 정정 작업 해결.

NVD를 사용하여 보안 문제 식별 및 에스컬레이션

CVE-ID(Common Vulnerability and Exposures Identifier) 레코드가 NVD(국가 취약성 데이터베이스)에서 다운로드되면 소프트웨어 자산 검색 모델로 식별되는 회사 네트워크의 소프트웨어와 비교됩니다. CVE-ID가 네트워크의 취약한 소프트웨어 또는 구성 항목과 일치하면 취약한 항목이 생성됩니다. CVE-ID 기록의 정보를 사용하여 정정을 위해 취약한 항목을 에스컬레이션할지 여부를 결정합니다.

시작하기 전에
가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 라이브러리 〉 **NVD**.
   NVD에서 다운로드한 CVE-ID 목록이 표시됩니다. NVD의 업데이트는 요청 시 또는 다음 위치에 있는 NIST 국가 취약성 데이터베이스 통합 기록에서 예약된 실행에 따라 수행할 수 있습니다. 모두 〉 관리 〉 통합.
2. CVE 기록을 클릭하면 다음 정보를 볼 수 있습니다.
   - CVE-ID에 대한 요약입니다.
   - 해당하는 경우 CWE(Common Weakness Enumeration) 항목에 대한 참조입니다.
   - CVSS(공통 취약성 평가 시스템)에서 CVE-ID의 취약성 점수입니다. CVSS에 대한 자세한 내용은 National Vulnerability Database 웹 사이트를 참조하십시오.
3. 취약성에 대한 자세한 내용을 보려면 관련 목록을 클릭하십시오.

   취약성 참조

   지정된 취약성과 참조 위치에 대한 이름, 설명, URL입니다.

   익스플로잇

   세부 정보.

   약점

   CWE 약점 목록.

4. 다음 관련 목록을 클릭하여 취약성을 식별하기 위한 자세한 정보를 확인합니다.
   취약성이 식별되고 취약한 항목이 생성된 경우 필요에 따라 수행할 수 있습니다 정정 작업 해결.

CWE를 사용하여 보안 문제 식별 및 에스컬레이션

NVD(국가 취약성 데이터베이스)에서 CWE(일반적인 약점 열거) 기록 라이브러리를 보고 CVE(일반적인 취약성 및 노출) 기록과 어떤 관련이 있는지 이해합니다. 그런 다음 이 정보를 사용하여 취약한 소프트웨어 항목을 소프트웨어 자산 관리 검색 모델과 매칭합니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_write

가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

프로시저

1. 다음으로 이동 모두 〉 취약성 〉 라이브러리 〉 **CWE**.
   다운로드된 취약한 소프트웨어 목록이 표시됩니다.
2. 취약성 정보를 보려면 CWE 소프트웨어 기록을 클릭하십시오.
3. 다음 관련 목록을 클릭하여 취약성을 식별하기 위한 자세한 정보를 확인합니다.
   취약성이 식별되고 취약한 항목이 생성된 경우 필요에 따라 수행할 수 있습니다 정정 작업 해결.

취약한 항목의 정정 대상 상태 취약성 대응 보기

취약한 항목이 정정 대상 규칙에 정의된 정정 목표 날짜에 거의 도달하면(또는 지난 경우) 취약한 항목 레코드가 상태로 업데이트됩니다. 이 정보는 분석가가 예정된 정정 활동을 사전에 모니터링하는 데 도움이 될 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할:

- sn_vul.vulnerability_admin
- sn_vul.read_remediation_target_rules〔읽기 전용〕

가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

이 태스크 정보
정정 대상 평가라는 예약된 작업이 하루에 한 번씩 실행되어 연결된 정정 대상 규칙에 지정된 취약한 항목 정정 날짜와 현재 날짜를 비교합니다. 현재 날짜가 정정 기한이 지나기 전 일 수 내에 있으면 정정 상태가 취약한 항목 기록에 추가됩니다.

정정 대상 규칙에 대한 자세한 내용은 다음 문서를 참조하십시오 취약성 대응 정정 대상 규칙.

프로시저

1. 다음으로 이동 모두 〉 취약성 〉 취약 항목.
2. 검토하려는 취약한 항목을 클릭합니다.
   취약한 항목에 대한 정정 날짜가 정정 대상 규칙에 설정된 조건 범위 내에 있으면 정정 대상 상태 탭이 표시됩니다.
3. 정정 대상 상태 탭을 클릭합니다.
4. 정정 대상 상태 기록을 클릭하여 검토합니다.

   주:
   대상에 접근 중, 기내 및 과거 대상에 해당하는 취약한 항목 수를 보려면 을 참조하십시오 기본 취약성 대응 대시보드 사용.

관련 정보

정정 대상 규칙 생성 또는 편집 취약성 대응

일치하지 않는 CI 작업

취약성 관리자이자 분석가는 일치하지 않는 CI(구성 항목)를 확인 및 재분류하고, 일치하지 않는 검색 항목을 조정하고, 선택한 검색 항목에 CI 조회 규칙을 다시 적용하고, 기존 CI의 복제를 제거할 수 있습니다.

일치하지 않는 구성 항목 보기 및 재분류

에서 구성 관리 데이터베이스(CMDB) 찾을 수 없는 구성 항목(CI)은 볼 수 있는 검색된 항목 목록에 배치됩니다. 이 목록을 사용하면 일치하지 않는 CI를 편리하게 재분류할 수 있습니다.

시작하기 전에
필요한 역할:
sn_vul.read(일치하지 않는 CI를 보기 위한 최소값)
및

ITIL 또는 자산(재분류)

가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

이 태스크 정보
취약성 분석가는 일치하지 않는 CI를 볼 수 있습니다.

재분류 작업은 itil 또는 자산 역할이 있는 경우, 클래스 CI에서만 *sn_sec_cmn_unmatched_ci* 사용할 수 있습니다. 재분류된 CI는 UI를 사용하여 재분류할 수 없습니다. CI 양식 또는 CI 목록 뷰에서 클래스 값을 변경하여 재분류할 수 있습니다. 자세한 내용은 다음 문서를 참조하십시오 Reclassify a CI .

프로시저

1. 다음으로 이동 모두 〉 보안 운영 〉 **CMDB** 〉 검색된 항목.
2. 검토하려면 각 항목을 클릭합니다.
3. 검색된 항목 양식 필드의 정보를 수정하려면 이 페이지에서 편집하고 저장을 마우스 오른쪽 버튼으로 클릭하십시오.
   이러한 필드에 추가되거나 남아 있는 모든 데이터는 재분류될 때 결과 구성 항목으로 전송됩니다.
4. 모든 것이 올바르면 재분류를 클릭합니다.
5. 선택 목록에서 클래스 이름을 선택하고 제출을 클릭합니다.
   검색된 항목 클래스가 업데이트되고 상태 필드가 재분류됨으로 변경되며 모든 데이터가 CMDB에 있습니다.

불일치하는 검색 항목을 일치시키기

예약된 작업을 생성하여 불일치하는 검색 항목을 일치시킵니다.

시작하기 전에
필요한 역할: admin

이 태스크 정보
VI(취약한 항목)는 취약성과 CI(구성 항목)로 구성됩니다. VI가 생성되면 생성 시 추가된 CI가 오래된 CI일 수 있습니다. CMDB의 정보가 변경되면 일치하지 않는 CI 정보가 조정되지 않습니다. 조정하려면 CMDB가 최신 CI로 업데이트될 때 일치하지 않는 상태에 있는 항목에 CI(구성 항목) 조회 규칙을 적용합니다.

예약된 작업 요구를 실행하여 일치하지 않는 상태의 검색된 항목에 대한 CI 일치 규칙을 다시 적용할 수 있습니다. 조회 규칙을 다시 적용한 후 CI가 변경되면 검색된 항목이 새 CI로 업데이트됩니다. 영향을 받는 탐지 및 취약한 항목도 업데이트됩니다. 자세한 내용은 검색된 항목에 대한 CI 변경 내용 문서를 참조하십시오.

프로시저

1. 다음으로 이동 모두 〉 **Security Operations >** 불일치하는 검색 항목을 조정하십시오..
2. 백그라운드 작업 페이지에서 조정 작업 만들기를 클릭합니다.
3. 양식에서 필드를 채웁니다.

> **주:**
> 매개변수 필드만 편집할 수 있습니다.

백그라운드 작업 양식

필드	설명
번호	고유한 작업 번호입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
작성자	작업을 생성한 사용자입니다.
매개변수	일치하지 않는 검색 항목을 조정하는 매개변수: ○ limit: 조정할 검색된 항목의 최대 수입니다. 값을 입력하지 않으면 검색된 항목 10,000개가 조정됩니다. ○ firstDiscovereditem: 조정해야 하는 검색된 첫 번째 항목입니다. 값을 입력하지 않으면 검색된 첫 번째 항목에서 조정 프로세스가 시작됩니다.
상태	백그라운드 작업의 현재 상태입니다.
상태 설명	백그라운드 작업의 현재 상태에 대한 설명입니다.
작업 유형	작업의 유형입니다. 값은 일치하지 않는 검색된 항목을 조정합니다.
시작 시간	작업이 시작된 시간입니다.
종료 시간	작업이 완료된 시간입니다.
작업 기간	작업을 완료하는 데 걸린 총 시간입니다.
하위 상태	선택한 상태의 하위 상태입니다.
메모	처리된 기록 수입니다.

4. 제출을 클릭합니다.

주:

- 작업 실행을 중지하려면 취소를 클릭합니다.
- 호스트 또는 취약한 항목을 임포트하는 동안에는 일치하지 않는 CI를 조정하거나 CI 조회 규칙을 다시 적용할 수 없습니다.

5. v26.0.11부터 취약성 대응 검색된 항목 테이블 뷰에서 선택되거나 필터링된 항목에 대해 "조회 규칙 다시 적용"할 수 있습니다.

주:
위에서 언급한 버전부터 일치하지 않는 검색된 항목 조정 예약된 작업이 폐기됩니다.

6. 옵션: 선택 모두 〉 보안 운영 >검색된 항목 테이블에서 선택하거나 필터링된 항목에 대한 조회 규칙을 다시 적용합니다.

주:
필터가 적용되지 않으면 다시 적용 옵션이 비활성화됩니다.

다시 적용한 후 통합이 실행되면 백그라운드 작업 URL 또는 오류 메시지가 팝업됩니다.

선택한 검색 항목에 CI 조회 규칙 재적용

검색된 항목 목록 뷰 선택 작업에서 선택한 검색된 항목에 CI(구성 항목) 조회 규칙을 다시 적용합니다. 규칙을 다시 적용한 후 CI가 변경되면 검색된 항목이 새 CI 및 영향을 받는 탐지로 업데이트됩니다. 취약한 항목도 업데이트됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

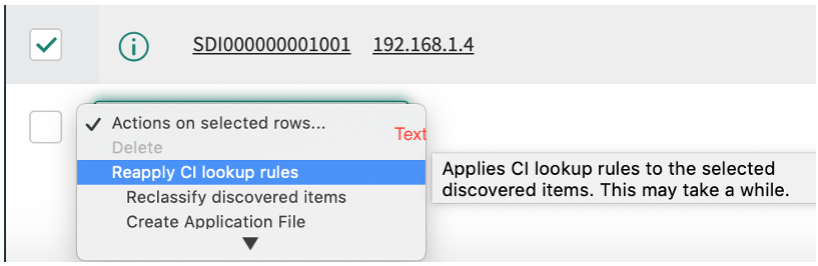
시작하기 전에
필요한 역할: admin

이 태스크 정보
자세한 내용은 검색된 항목에 대한 CI 변경 내용 문서를 참조하십시오.

CI 일치 및 CMDB의 개념, 검색된 항목 조회, 규칙 기반 식별 및 CI 일치 작동 방식에 대한 기타 세부 정보에 대한 자세한 내용은 HI 지식베이스의 취약성 대응에서 CI 일치 (KB0998706) 문서를 참조하십시오.

프로시저

1. 다음으로 이동 모두 〉 보안 운영 〉 **CMDB** 〉 검색된 항목.
2. 필요한 검색 항목을 선택하고 선택한 행에 대해 작업을 클릭합니다.



3. 목록에서 **CI** 조회 규칙 재적용을 선택합니다.

   주:

   v24.0.6부터 취약성 대응 는 시스템 속성을 *sn_sec_cmn.skipItemsWithCIDecommissioned*활성화하여 하위 상태가 'CI 해제됨'인 검색된 항목에 대한 CI 조회 규칙의 재적용을 건너뛸 수 있습니다.

   규칙은 검색된 항목에 다시 적용됩니다.

4. 메시지에서 상태 보기를 클릭합니다.

   백그라운드 작업 양식에 상태가 표시됩니다.

   주:
   메모 필드에서 ### ## ### ### ### # ####. 0이 아닌 값을 가진 속성은 CI 조회 규칙을 다시 적용하는 동안 오류 또는 예외가 발생했음을 나타냅니다. 자세한 내용은 시스템 로그를 확인하십시오.

5. 다시 적용은 **last_scan_date, last_comp_scan_date, non_infra_last_scan_date non_infra_last_comp_scan_date** 열을 기준으로 지난 90일 이내에 스캔한 항목에만 적용됩니다.

   CI 수명주기 상태 열(예: 설치 상태, 운영 상태)을 구성하기 위한 ci_lifecycle_status_source(범위 = sn_sec_cmn) 시스템 속성이 추가되었습니다. CI 폐기에 대한 추가 열을 구성할 수 있습니다.

   열이 백그라운드 작업 목록 뷰에 추가됩니다.

   - 경과 시간(ms): 백그라운드 작업을 처리하는 데 필요한 시간입니다.
   - 처리된 항목: 지금까지 처리된 항목 수입니다.
   - 처리할 총 항목: 처리할 남아 있는 총 항목 수입니다.
   - 완료까지 걸리는 시간(ms): 백그라운드 작업이 처리될 때까지 남은 시간입니다. 이러한 열은 작업 진행 상황에 대한 가시성을 제공하며, 이러한 열은 요구 사항에 따라 추가할 수 있는 각 양식 뷰에서 사용할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

CI 조회 규칙 개선 사항 재적용

OS 및 NetBIOS와 같은 선택된 검색 항목에 CI(구성 항목) 조회 규칙을 다시 적용합니다.

시작하기 전에

필요한 역할: 관리자

이 태스크 정보

- 소스 데이터에 있는 os 및 netBIOS 값은 검색된 항목에서 이러한 필드를 채우는 동안 구성 항목 앞에 채워져야 합니다.
- 소스 데이터에 OS 및 NETBIOS 값이 비어 있는 경우 검색된 항목 테이블의 이러한 필드를 채우는 동안 구성 항목에서 값을 가져옵니다.

프로시저

1. 다음으로 이동 모두 〉 보안 운영 〉 **CMDB** 〉 검색된 항목.
2. 필요한 검색 항목을 선택하고 선택한 행에 대해 작업을 클릭합니다.
3. 목록에서 **CI** 조회 규칙 재적용을 선택합니다.

   규칙은 검색된 항목에 다시 적용됩니다.

CI 조회 규칙을 실행 취약성 대응 한 후 중복 또는 고아 기록을 방지하는 데 도움이 되는 단계

일치하는 항목(내의 구성 항목(CI) CMDB)으로 인해 중복 또는 고아 기록이 생성되지 않도록 조치를 취합니다.

취약성 데이터를 임포트하면 인스턴스에 부담이 가중될 수 있으며 규칙을 신중하게 구성하지 않으면 자원에 성능 문제가 발생할 수 있습니다. CMDB 내에서 반복하고 일치를 수행하는 데 사용되는 논리로 인해 처리 시간이 길어질 수 있습니다. 규칙에서 처리 스크립트를 철저히 테스트하고 디버깅하면 나중에 프로세스에서 발생할 수 있는 문제를 완화하는 데 도움이 됩니다.

중복 기록 또는 고아 기록 방지

- 테스트 중인 CI 조회 규칙과 관련된 데이터의 작은 하위 집합을 사용합니다.
  - 테스트 중인 규칙을 제외한 모든 CI 조회 규칙을 비활성으로 설정합니다.
  - 임포트한 CI를 분석하여 예상되는 동작을 관찰하고 일치가 올바르게 발생하는지 확인합니다.
- 일치하는 CI 검토
  - 일치하는 CI와 일치하지 않는 CI의 수를 검사합니다. 백분율이 허용 가능한지 확인합니다. 첫 번째 페이지만 말고, 그것이 삽입된 첫 번째 페이지일 가능성이 높습니다.
  - 일부 CI를 수동으로 검색합니다.
  - 이름 지정 또는 필드 문제(예: 특정 도메인 검색)가 있는지 확인합니다.

    적절하다고 판단되는 경우 일치 규칙을 추가합니다.
- 일치하지 않는 CI 검토
  - 일치하지 않는 CI 테이블로 이동합니다.
  - 구성 항목 클래스별로 그룹화합니다.
  - 올바르지 않은 클래스(인증서, 네트워크 카드, 이미지)를 검토합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

    - 올바른 CI와 일치하지 않은 이유를 파악합니까?
    - 클래스를 제외해야 합니까?
    - 클래스를 관련 클래스로 상승시켜야 합니까?
- 폐기됨과 같은 CI 상태를 검토합니다.
- 테스트 데이터 제거
    - CI 일치에서 올바름 또는 예상되는 동작을 관찰하기 시작하면 다시 시작하십시오.
    - 다시 시작: 테스트에 사용된 데이터 삭제: (테이블에서 데이터 삭제 섹션 참조)
        - 검색된 항목
        - 취약 항목
        - 정정 작업
    - 모든 CI 일치 규칙을 수동으로 다시 실행합니다.

CI 조회 규칙 및 Qualys에 대한 자세한 내용은 KB0750656 문서를 참조하십시오.

CI 조회 규칙 및 Rapid7에 대한 자세한 내용은 KB0818096 참조하십시오.

테이블에서 데이터 삭제

데이터를 임포트하고 문제가 있음을 깨닫는 경우가 있습니다. 개발 또는 성능 환경에 문제가 있는 경우 더 나은 환경에서 다시 클론할 수 있지만 항상 그렇게 할 수 있는 것은 아닙니다.

주:
이러한 작업을 수행하려면 전문 지식이 필요합니다 ServiceNow .

테이블에서 데이터를 삭제하는 네 가지 옵션이 있습니다.

- 테이블 구성에서 모든 기록 삭제를 사용합니다.
- 자동 플러시(sys_auto_flush.list)로 이동하고 새 자동 플러시 기록을 생성하여 테이블 클리너를 구성합니다.
- 백그라운드 스크립트를 사용하여 gs.truncateTable을 자릅니다.

  를 사용하려면 `truncateTable` 백그라운드 스크립트에서 롤백 기록 확인란을 해제해야 합니다. 그렇지 않으면 테이블 및 관련 계단식 테이블의 복사본이 생성되고 시간이 너무 오래 걸리며 실패할 가능성이 높습니다.

  주:
  프로덕션 환경에서 사용하지 `truncateTable` 마십시오. 프로덕션 또는 공유 환경에서 대용량 삭제를 실행하기 전에 지원 담당자와 상의하십시오.

기존 구성 항목 중복 제거

중복 제거 작업을 통해 CI(구성 항목)가 업데이트될 때마다 해당 CI와 관련된 검색된 항목(DI)도 업데이트됩니다. 취약한 항목(VI) 및 탐지도 CI와 함께 업데이트됩니다.

자세한 내용은 검색된 항목에 대한 CI 변경 내용 문서를 참조하십시오.

관련 정보

중복 제거 작업 정정

정정 작업 해결

에 취약성 대응 내재된 유연성을 통해 보안 조직에 적합한 방식으로 취약성을 수정할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)

이 태스크 정보
변경 요청이 해결되었다는 알림을 받으면 정정 작업 상태를 해결됨으로 옮기고 다음 스캔을 기다립니다. 재스캔은 설정 도우미에 구성된 외부 공급업체 임포트 일정에 의해 자동으로 트리거됩니다.

주:

상태 동기화가 활성화되면 정정 작업(VUL)과 연결된 변경 요청이 구현되어 검토 상태인 후 정정 작업이 자동으로 해결됨 상태로 이동합니다. 를 위한 변경 관리 취약성 대응 문서를 참조하십시오.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 정정 작업 〉 나에게 할당됨.
2. 열림 상태의 기록을 클릭합니다.

   열림 상태는 기록이 아직 작업되지 않았음을 나타냅니다. 양식에는 다음이 표시됩니다.

   - 정정 작업 정보
   - 그룹 구성 상세 정보
   - 메모
   - 관련된 취약 항목
   - 작업 SLA
   - 관련 변경요청
3. 그룹에 대한 분석을 수행합니다.
4. 기록 작업을 시작할 준비가 되면 다음 옵션 중 하나를 선택합니다.

옵션	설명
취약한 항목이 IT 환경에 위험을 초래하는 경우 CHG 기록을 생성하고 변경 관리 팀에 문제를 에스컬레이션합니다.	그룹을 적절한 그룹 또는 개인에 할당하고 변경 생성을 클릭합니다.
취약한 항목이 조직에 잠재적인 보안 위험을 제기하는 경우 보안 인시던트 기록을 생성하고 팀에 문제를 보안 인시던트 응답 에스컬레이션합니다.	보안 인시던트 생성을 클릭합니다. 이 버튼은 활성화된 경우에만 보안 인시던트 응답 표시됩니다. 비즈니스 영향 계산이 적용되고, 인시던트가 할당되고, 보안 인시던트가 생성됩니다.

   변경 요청을 만든 후에는 취약성 그룹 양식의 변경 요청 관련 목록에 해당 기록이 나타납니다.
5. 문제가 위험도가 낮고 지연될 수 있다고 판단되면 예외 요청을 클릭합니다.
   정정 작업을 연기하는 방법에 대한 자세한 내용은 다음 문서를 정정 작업 연기참조하십시오.
6. 추가 분석 없이 문제를 즉시 종결할 수 있다고 판단되면 종결을 클릭합니다.
   정정 작업을 종결하는 방법에 대한 자세한 내용은 다음 문서를 정정 작업 닫기참조하십시오. 의 취약성 대응v23.0부터 정정 작업에 대한 닫기 버튼이 제거되었습니다.

   외부 공급업체 통합의 예약된 작업은 설정된 간격으로 기록을 자동으로 업데이트하고 스캔합니다. 취약한 항목은 다음 예약된 날짜 및 시간에 검사됩니다. 또는 취약성 스캔 관련 링크를 사용하여 취약성 스캔을 수동으로 시작할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

검사에서 구성 항목에서 취약성을 다시 발견하고 고정됨으로 표시하지 않으면 취약한 항목이 조사 중 상태로 돌아갑니다. IT 운영팀에 문의하여 변경 요청을 다시 엽니다.

검사에서 취약성을 찾지 못하고 취약한 항목이 고정됨으로 표시된 것으로 반환되면 취약한 항목이 종결-고정 상태로 전환되고 임포트하는 동안 종결됩니다.

작업의 모든 취약한 항목이 종결-고정 상태인 경우에만 정정 작업이 자동으로 종결됩니다. 고정이 아닌 종결 상태의 취약한 항목이 있는 정정 작업은 수동으로 종결해야 합니다.

정정 작업 연기

정정 작업(VUL)과 관련된 문제가 우선순위가 낮고 추가 분석 없이 즉시 지연될 수 있다고 판단되는 경우 예외 요청 기능을 사용할 수 있습니다.

시작하기 전에

필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)

이 태스크 정보

작업 공간의 정정 작업 기록에서 정정 작업을 연기할 취약성 대응 수 있습니다. 요청을 제출하면 승인을 위해 전송됩니다. 에서 예외 요청 IT 정정 작업 공간 문서를 참조하십시오.

예약된 작업이 매일 실행되어 재개시 날짜에 도달한 지연된 정정 작업을 확인합니다. 작업의 연기가 만료된 날에 작업이 다시 열립니다.

> **주:**
> 상태 동기화를 사용하도록 설정된 해당 기록의 수명주기 상태를 통해 변경 요청 및 정정 작업을 수동으로 이동할 수 있지만, CHG가 상태를 변경했다고 시스템이 등록하거나 CHG를 추가 또는 정정 작업에서 제거하면 상태 동기화가 수동 개입을 재정의할 수 있습니다. 그러나 변경 요청 상태는 정정 작업을 종결 또는 연기됨 상태에서 자동으로 이동하지 않습니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 정정 작업.
2. 기록을 엽니다.
3. 예외 요청을 클릭합니다.
4. 양식의 필드에 적절히 입력합니다.

필드	설명
다음까지	지연 상태가 만료되고 정정 작업이 다시 시작되는 날짜를 선택합니다. 기록이 제출된 후 이메일 알림이 정의되어 있으면 만료 날짜가 1주일 이내이면 그룹 구성원 취약성 대응 은 이메일을 받습니다. 지연 날짜가 만료되면 정정 작업이 다시 열림 으로 설정되고 두 번째 이메일 알림이 전송됩니다.
이유	문제를 지연시키는 이유를 입력합니다. 선택 항목은 다음과 같습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	○ 유지관리 기간을 기다리는 중 ○ 긍정 오류 ○ 수정 사용 불가 ○ 수용된 위험 ○ 사용 중인 완화 통제 ○ 기타
추가 정보	기타 관련 정보를 입력합니다.

5. 제출을 클릭합니다.
   그룹이 검토 중으로 표시됩니다. 다시 열기 관련 링크가 나타납니다. 재개시된 날짜와 이유는 상태 변경 승인 탭 아래의 작업 메모에 표시됩니다.

지연된 정정 작업의 연장을 요청합니다

지연된 기한에 도달하기 전에 지연된 정정 작업(VUL)에 대한 연장을 요청합니다. 정정 소유자는 더 이상 이 요청을 하기 위해 지연된 기한까지 기다릴 필요가 없습니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)

이 태스크 정보
작업 공간에서 연장을 취약성 대응 요청할 수도 있습니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 정정 작업.
2. 지연된 정정 작업을 엽니다.
3. 연장 요청을 선택합니다.
4. 양식의 필드에 적절히 입력합니다.

필드	설명
연장 날짜	지연 상태가 만료되고 정정 작업이 다시 시작되는 날짜를 선택합니다.
이유	문제를 지연시키는 이유를 입력합니다. 선택 항목은 다음과 같습니다. ○ 유지관리 기간을 기다리는 중 ○ 수정 사용 불가 ○ 수용된 위험 ○ 사용 중인 완화 통제 ○ 기타
추가 정보	기타 관련 정보를 입력합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. 승인 요청을 선택합니다.
   요청이 승인되면 정정 작업의 변경 내용이 정정 작업의 일부인 취약한 항목에도 롤다운됩니다. 그러나 취약한 항목은 지연 상태여야 하며 현재 종료 데이터는 업데이트 종료 날짜보다 앞서야 합니다. 요청 제출 및 승인자의 후속 조치 시에도 이메일이 트리거됩니다.

   주:
   - 요청은 두 가지 수준의 승인을 거칩니다.
   - 연장 요청 버튼은 예외 규칙의 일부로 생성된 정정 작업에 사용할 수 없습니다.
   - 지연된 정정 작업이 다시 연장되면 백엔드에서 연장 지연 수가 증가합니다.

정정 작업 닫기

추가 분석 없이 정정 작업과 관련된 문제를 즉시 종결할 수 있는 것으로 확인되면 종결 기능을 사용할 수 있습니다. v23.0 부터 취약성 대응정정 작업에 대한 닫기 버튼이 제거되었으며 스캐너에 의해 정정 작업의 종결이 이루어집니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
취약성 대응 작업 공간에서 정정 작업은 이전 버전의 취약성 대응에서 이전에 수행한 정정 작업과 동일한 상태를 통해 전환됩니다. 정정 작업의 모든 취약한 항목(VIT)이 닫히면 정정 작업이 비활성 상태로 전환됩니다.

중요사항:
상태 동기화를 사용하도록 설정된 해당 기록의 수명주기 상태를 통해 변경 요청 및 정정 작업을 수동으로 이동할 수 있지만, CHG가 상태를 변경했다고 시스템이 등록하거나 CHG를 추가 또는 정정 작업에서 제거하면 상태 동기화가 수동 개입을 재정의할 수 있습니다. 그러나 변경 요청 상태는 정정 작업을 ## 또는 ### 상태에서 자동으로 이동하지 않습니다.

프로시저

1. 검토를 요청할 기록을 엽니다.
2. 종결/지연 버튼을 선택합니다.
3. 양식의 필드에 적절히 입력합니다.

필드	설명
상태	상태를 선택합니다. 선택 항목은 다음과 같습니다. ○ 연기됨 ○ 종결됨
다음까지	지연 상태 팝업에서만 사용할 수 있습니다. 지연 상태가 만료되고 정정 작업이 다시 시작되는 날짜를 선택합니다. 기록이 제출된 후 이메일 알림이 정의되어 있으면 만료 날짜가 1주일 이내이면 그룹 구성원 취약성 대응 은 이메일을 받습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	지연 날짜가 만료되면 취약한 항목이 다시 열림 으로 설정되고 두 번째 이메일 알림이 전송됩니다.
이유	문제를 종결하는 이유를 입력합니다.
추가 정보	기타 관련 정보를 입력합니다.

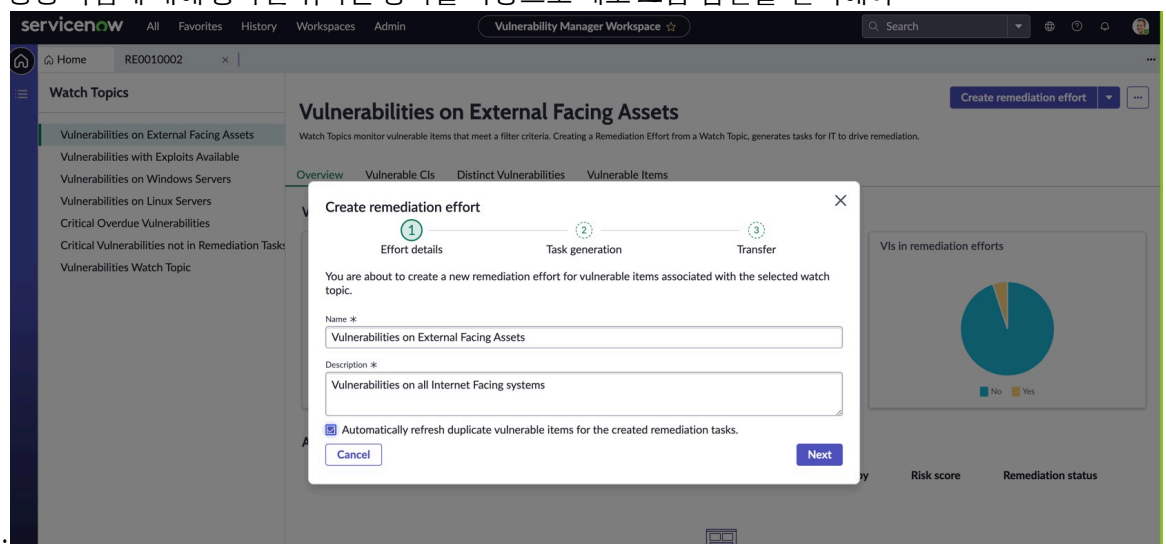
4. 제출을 선택합니다.
   정정 작업이 종결로 표시됩니다.

여러 스캐너에서 중복된 취약한 항목 식별

동일한 자산에서 여러 스캐너를 사용하여 취약성을 탐지하는 경우 여러 VI(취약한 항목)가 생성될 수 있습니다. 이러한 중복 VI를 식별하여 중복 취약성이 정정 소유자에게 할당되지 않도록 할 수 있습니다.

이 해결은 동일한 CVE(Common Vulnerabilities and Exposures)와 같은 동일한 취약성이 검색된 경우에만 가능합니다. 취약성 조합은 사용 중인 스캐너에 따라 다릅니다. 예를 들어 Qualys 및 Tenable에는 고유한 취약성 유형, 즉 TPE(타사 항목)가 있으며 엔드포인트용 Microsoft Defender 같은 다른 스캐너는 CVE를 기반으로 취약성을 검색합니다.

v 17.1부터 정정 작업을 생성하는 동안 생성된 정정 작업에서 중복된 취약한 항목을 자동으로 새로 고칠 수 있습니다. 중복된 취약한 항목을 자동으로 새로 고치려면 생성된 정정 작업에 대해 중복된 취약한 항목을 자동으로 새로 고침 옵션을 선택해야 합니다.



중복 **VI** 표시: 시스템의 여러 스캐너에서 보고된 중복된 취약한 항목을 식별합니다. 중복 VI를 해결됨으로 표시할 수 있습니다. 자세한 내용은 다음 문서를 참조하십시오 중복 취약성 자동 해결. CVE를 사용하여 취약성 조합을 만든 경우에만 중복 항목이 표시됩니다. 자세한 내용은 취약성 대응 정정 작업 및 취약한 항목 상태를 참조하십시오.

다음 취약성 조합에 대해 잠재적인 중복이 식별됩니다.

스캐너 조합	취약성 유형
스캐너 1 및 스캐너 2	CVE
스캐너 1 및 스캐너 2	CVE 및 TPE

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

중복 취약성 자동 해결

(VR) v17.1부터 취약성 대응 자산의 중복 취약성을 자동으로 해결할 수 있습니다.

자산을 여러 스캐너로 스캔할 때 다른 스캐너에서 중복된 취약성과 동일한 취약성을 식별할 가능성이 있습니다. 예를 들어 Qualys 및 Microsoft 스캐너에서 동일한 취약성을 식별하는 경우 중복된 취약성을 자동으로 해결하도록 선택할 수 있습니다.

샘플 시나리오

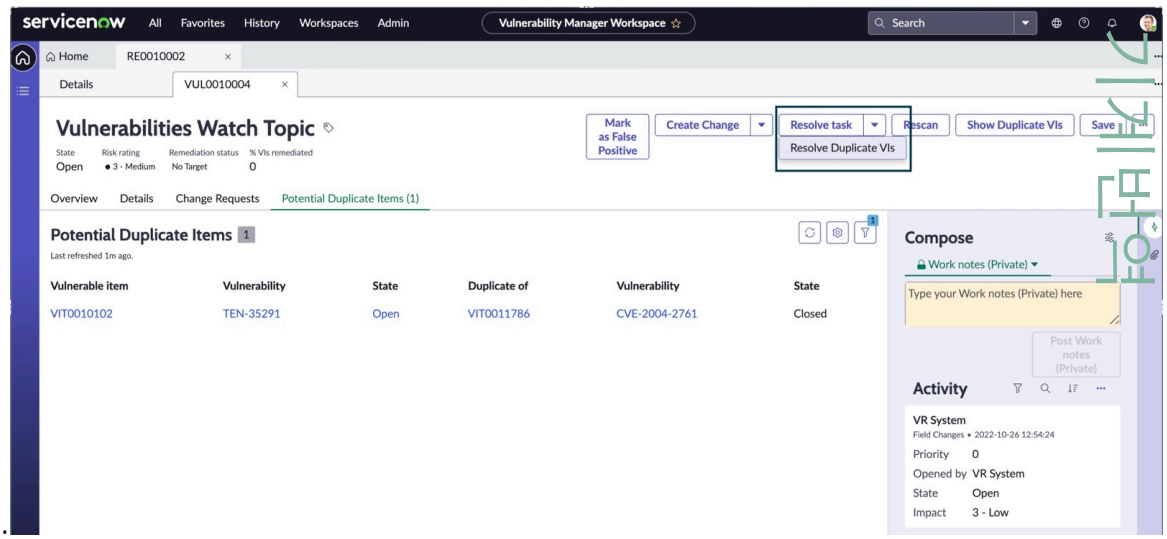
VR은 엔드포인트용 Microsoft Defender 스캐너에서 취약성 1에 대한 레코드(VI1)를 생성합니다. 동일한 취약성에 대해 Qualys 스캐너에서 두 번째 레코드인 VI2가 생성됩니다. 정정 팀은 VI1 및 VI2 기록을 해결할 수 있는 패치를 적용합니다. Qualys 검사 일정을 하루 이상 구성하는 경우 그 때까지 Microsoft Defender는 수정된 취약성 정보를 제공하고 VR은 VI1 레코드를 종결/고정으로 닫습니다.

이 시나리오에서 VI2 레코드는 여전히 오픈 상태이고 VR은 Qualys 스캔 결과를 기다립니다. 이 경우 패치가 적용되고 VI가 다른 스캐너에 의해 수정된 것으로 확인되더라도 두 번째 스캐너의 VI 레코드는 열린 상태로 유지됩니다.

이 상황을 해결하려면 첫 번째 스캐너에서 취약성을 종결한다는 조건에 따라 중복 취약성 레코드를 해결하는 것을 고려할 수 있습니다.

다음과 같은 방법으로 취약성을 해결합니다.

- 요청 시: 정정 작업에서 중복 **VI** 해결 UI 작업을 선택합니다.



- 자동: 시스템 속성 `sn_vul.auto_resolve_duplicate_vit` 를 활성화하여 중복된 취약한 항목을 자동으로 해결합니다. 일일 예약 작업 '정정 작업에서 중복 VIT 새로 고침 및 해결'은 중복 항목을 자동으로 새로 고칩니다.

그러면 중복 VI가 해결됨으로 표시됩니다.

> **주:**
> 해결된 취약성 항목 기록은 스캐너에서 수정되지 않음으로 식별하면 다시 열립니다.

분류 그룹 생성 및 편집

이 그룹의 기본 규칙이 조건을 기반으로 테이블 기록을 분류할 수 있도록 그룹을 생성합니다. 규칙을 사용하여 해당 테이블의 필드를 선택할 수 있습니다.

시작하기 전에

필요한 역할: sn_vul.manage_classification_rule

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 시스템 속성 테이블로 이동합니다.
2. *sn_sec_cmn.classificationTables* 시스템 속성에서 분류 그룹을 생성할 테이블의 이름을 추가합니다.
3. 그룹에 정의된 테이블의 비즈니스 규칙에 다음 코드 스니펫을 추가하여 새 비즈니스 규칙을 작성합니다.
   ```
   var classificationCalc = new sn_vul. ### ###
   (current,true,false,'sn_vul_classification_group','sn_vul_classification_rule');
   classificationCalc.calculate();
   ```

   주:
   검색된 항목 및 취약성 항목 테이블을 수집하는 동안 분류를 실행하기 위해 비즈니스 규칙이 제공됩니다. 다른 테이블의 경우 수집 시 분류 규칙을 사용하려면 비즈니스 규칙을 추가해야 합니다.

4. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 분류 규칙.
5. 분류 그룹 상황에 맞는 메뉴에서 새로 만들기를 클릭합니다.
6. 양식에서 필드를 채웁니다.

취약성 분류 그룹 양식

필드	설명
이름	새 분류 그룹의 이름입니다.
활성	그룹을 활성화하는 옵션입니다.
설명	새 분류 그룹에 대한 설명입니다.
테이블	규칙이 실행되는 기준이 되는 테이블입니다. **주:** 취약성 대응 기본 시스템에는 검색된 항목 및 취약성에 대한 분류 그룹이 포함됩니다.

분류 규칙 생성 및 편집

정정을 위해 수신 취약성을 올바른 팀에 자동으로 분류하는 규칙을 생성합니다.

시작하기 전에
필요한 역할: sn_vul.manage_classification_rule

이 태스크 정보
이러한 규칙은 생성되면 취약성을 플랫폼 또는 애플리케이션에 속하는 것으로 분류합니다. 이러한 규칙을 구성하여 취약성 항목의 특정 필드 값을 대체할 수 있습니다.
컨텐츠를 재사용할 수 있도록 이러한 규칙을 사용하여 계산을 타사 취약성 항목 테이블로 업스트림으로 이동합니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 분류 규칙.
2. 분류 그룹을 보려면 해당 그룹을 클릭합니다.
3. 분류 규칙 상황에 맞는 메뉴에서 새로 만들기를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 양식에서 필드를 채웁니다.

취약성 분류 규칙 양식

필드	설명
이름	새 분류 규칙의 이름입니다.
활성	규칙을 활성화하는 옵션입니다.
설명	새 분류 규칙에 대한 설명입니다.
실행 순서	규칙을 실행해야 하는 순서입니다.
고급 뷰	탭 섹션에서 추가 필드를 볼 수 있는 옵션입니다.
이 조건이 충족될 경우	
조건 유형	규칙에 대한 조건의 유형입니다. 선택 항목은 다음과 같습니다. ○ 필터: 규칙을 사용할지 여부를 결정하는 기본 필터 조건입니다. ○ 필터 그룹: 함께 사용되는 여러 조건의 세트입니다. 필터 그룹에 정의된 조건을 바탕으로 규칙이 평가됩니다. ○ 스크립트: 이 규칙을 적용할 시기를 결정하는 데 사용되는 스크립팅된 조건입니다. 이 필드는 고급 뷰 옵션이 선택된 경우에만 나타납니다.
조건	규칙의 조건입니다. 필수 취약성 항목 열에서 선택한 열을 기준으로 조건을 정의합니다. 여러 조건을 추가하여 규칙을 구체화할 수 있습니다. 이 필드는 조건 유형 필드에서 필터를 선택한 경우에만 나타납니다. **주:** 여러 조건이나 템플릿을 정의할 때는 상위 및 하위 테이블에서만 선택할 수 있습니다. 두 개 이상의 하위 테이블에서 선택할 수 없습니다.
필터 그룹	필터 그룹입니다. 이 그룹은 조건 세트가 여러 위치에서 반복적으로 사용될 때 정의됩니다. 목록 아이콘( )을 사용하여 조회를 클릭하여 필터 그룹을 선택합니다. 자세한 내용은 보안 작업에서 필터 그룹 만들기 및 정의를 참조하십시오. 이 필드는 조건 유형 필드에서 필터 그룹을 선택한 경우에만 표시됩니다.
스크립트	이 규칙을 적용할 시기를 결정하기 위해 평가되는 스크립트입니다. 코드를 작성하고 응답을 true 또는 false로 설정할 수 있습니다. 이 필드는 조건 유형 필드에서 스크립트를 선택한 경우에만 나타납니다

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
이 값 설정	
분류	규칙의 분류입니다. 옵션을 선택하려면 전구 아이콘( )을 클릭합니다. 목록에 플랫폼 및 애플리케이션에 대한 옵션이 표시됩니다. 또는 목록에 없는 사용자 고유의 분류를 입력할 수 있습니다.
분류 유형	분류 유형입니다. 이 필드에는 분류 필드에 대해 선택한 값을 기준으로 필터링된 분류 유형 목록이 표시됩니다.
값 유형	이 규칙을 사용하여 할당되는 값의 유형입니다. 선택 항목은 다음과 같습니다. ○ 템플릿: 템플릿을 선택합니다. 필요한 템플릿을 사용할 수 있습니다. ○ 스크립트: 기존 스크립트를 선택하거나 사용자 지정 스크립트를 직접 작성합니다. 이 필드는 고급 뷰 옵션이 선택된 경우에만 나타납니다.
템플릿	분류 및 분류 유형 필드 외에 규칙에 대한 또 다른 조건입니다. 규칙을 평가할 때 설정할 필드와 값의 조합을 선택합니다. 이 필드는 값 유형 필드에서 템플릿을 선택한 경우에만 나타납니다.
스크립트 값	현재 기록의 값을 설정하는 스크립트입니다. 이 필드는 취약성 항목의 필드에 설정할 값을 정의합니다. 이 필드는 값 유형 필드에서 스크립트를 선택한 경우에만 나타납니다.

5. 새 규칙을 만들려면 제출을 클릭합니다.

Example:
VR 분류 규칙을 사용하여 취약성 및 검색된 항목과 같은 업스트림 테이블에 논리를 추가하고 계산합니다. 출력을 여러 번 재사용할 수 있으므로 담당 규칙과 같은 규칙의 성능이 향상됩니다. 예를 들어, 타사 항목(TPE)을 Java로 분류하고 담당 규칙의 출력을 여러 번 재사용합니다. 샘플 할당 규칙:

```
VI.TPE.Classfication Type
        | IS | Java
```

기존 취약성에 규칙 적용

분류 규칙을 변경하는 경우 모든 취약성 항목에 대한 모든 활성 규칙을 다시 실행합니다. 새로 생성된 분류 규칙을 기존 취약성에 적용하여 기존 취약성을 개조할 수도 있습니다.

시작하기 전에
필요한 역할: sn_vul.manage_classification_rule

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 〉 관리 〉 취약성 분류 규칙.
2. 규칙을 선택하려면 규칙 옆에 있는 확인란을 선택합니다.
3. 변경 내용 적용을 클릭합니다.
4. 다시 적용을 클릭합니다.

분류 규칙 비활성화 또는 삭제

분류 규칙이 더 이상 필요하지 않거나 관련이 없는 경우 비활성화하거나 삭제합니다.

시작하기 전에
필요한 역할: sn_vul.manage_classification_rule

이 태스크 정보
분류 규칙이 비활성화되거나 삭제되면 삭제된 규칙에 따라 분류 및 **Classification_type** 필드에 채워진 데이터는 해당 테이블에 남아 있습니다.

이 데이터를 지우려면 분류 및 **Classification_type** 필드에 빈 값이 있는 규칙을 생성하고 그룹을 다시 적용합니다. 이 새 규칙이 다시 적용되면 규칙의 조건에 따라 이 규칙을 적용할 수 있는 모든 기록에 변경 내용이 반영됩니다.

v24.0.6 중 취약성 대응부터 분류 규칙이 삭제되거나 비활성화되면 검색된 항목 또는 취약성 항목에 더 이상 적용되지 않으며 분류 및 **Classification_type** 필드의 데이터가 지워집니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 〉 관리 〉 취약성 분류 규칙.
2. 삭제할 규칙을 선택하려면 규칙 옆에 있는 확인란을 클릭합니다.
3. 규칙을 삭제하려면 다음 중 하나를 수행합니다.
   - 선택한 행에 대한 작업 목록에서 삭제를 클릭합니다.
   - 규칙을 선택하고 삭제 버튼을 클릭합니다.
4. 변경 내용 적용을 클릭합니다.

   주:
   이 버튼을 클릭하지 않으면 규칙이 시스템에 계속 상주합니다. 규칙에서 참조하는 취약성은 계속해서 이를 참조합니다.

제외 규칙 생성

수집 중에 탐지가 취약한 항목(VIT)으로 변환되지 않도록 필터링하거나 제외하는 규칙을 생성합니다.

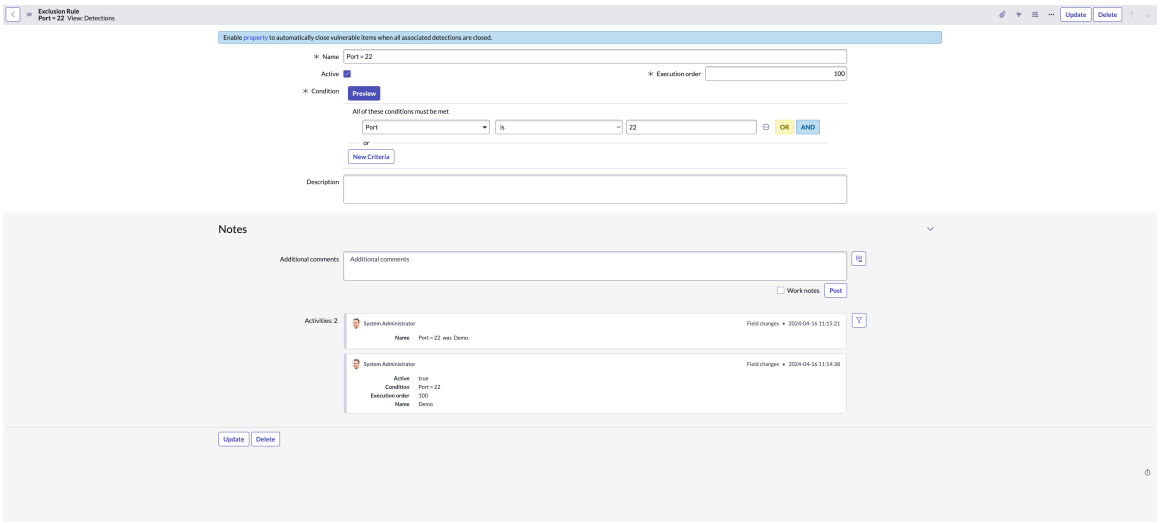
시작하기 전에
필요한 역할: 취약성 관리자

이 태스크 정보

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 제외 규칙.
2. 제외 규칙 기록 페이지에서 새로 만들기를 선택하여 규칙을 생성합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



'연결된 모든 탐지를 닫을 때 취약한 항목을 자동으로 닫을 수 있도록 속성 활성화'라는 메시지가 표시됩니다. 기본적으로 이 속성은 비활성 상태입니다. 사용하려면 속성 링크를 선택하고 값 필드에 값을 True로 입력합니다.

3. 양식에서 필드를 채웁니다.

제외 규칙 양식

필드	설명
이름	제외 규칙의 이름입니다.
활성	제외 규칙을 활성화하는 옵션입니다.
실행 순서	각 제외 규칙의 고유한 순서입니다.
조건	탐지를 처리하는 동안 정의할 수 있는 탐지에 대한 필터 조건입니다. **주:** 제외 규칙 또는 취약성 항목 필드 조건은 선택할 수 없습니다.
설명	제외 규칙에 대한 설명입니다.

4. 제출을 선택합니다.
활동은 시스템에 기록됩니다.

주: 제외 규칙이 생성되면 후속 수집에서 시작되는 탐지에 적용됩니다.

변경 관리 다음에 대한 작업 취약성 대응

정정 작업(RT)에서 변경 요청을 생성하거나, RT를 기존 변경 요청에 연결하거나, 정정 작업을 VI(취약한 항목)의 하위 집합이 있는 새 작업으로 분할합니다.

CMDB에서 지원되는 구성 항목(CI)을 수정하거나 제거하기 위해 모든 종류의 수동 및 제어 프로세스가 필요한 경우 정정 작업에서 직접 변경 요청을 생성하고 관리합니다. 기록에서 직접 변경 요청을 생성하고 관리하면 취약성을 신속하게 조사하고 해결하는 데 도움이 됩니다.

변경 관리가 애플리케이션 및 시스템 요구 사항과 함께 취약성 대응 작동하는 방식에 대한 개요는 을 참조하십시오를 위한 변경 관리 취약성 대응.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

변경 요청을 생성하고, 정정 작업을 기존 변경 요청에 연결하고, 정정 작업을 분리하는 방법은 다음 주제를 참조하십시오. 변경 요청(CHG)의 상태 필드가 정정 작업을 자동으로 해결하는 방법에 대한 자세한 내용은 을 참조하십시오 변경 요청과 정정 작업 간의 상태 동기화 .

정정 작업에서 변경 요청 만들기

IT 정정 소유자는 그룹의 모든 취약한 항목에 대해 정정 작업(VUL)에서 직접 변경 요청(CHG)을 생성합니다. 수동 개입이 필요한 취약성 조사를 신속하게 처리할 기본 솔루션이 포함된 미리 채워진 정보를 사용하여 변경 요청을 생성합니다.

시작하기 전에

필요한 역할: 변경 요청 생성 시: itil 역할이 있는 모든 사용자 itil 역할이 사용자에게 할당되면 sn_vul.remediation_owner 역할도 자동으로 할당됩니다.

필요한 역할: 변경 요청 승인의 경우: itil, admin, sn_change_write change_manager 역할을 가진 사용자.

이 태스크 정보

작업 공간에서 변경 요청을 취약성 대응 생성하는 방법에 대한 자세한 내용은 다음 문서를 에서 변경 요청 만들기 IT 정정 작업 공간참조하십시오.

클래식 환경에서 변경 요청을 만들려면 아래 나열된 단계를 따르십시오.

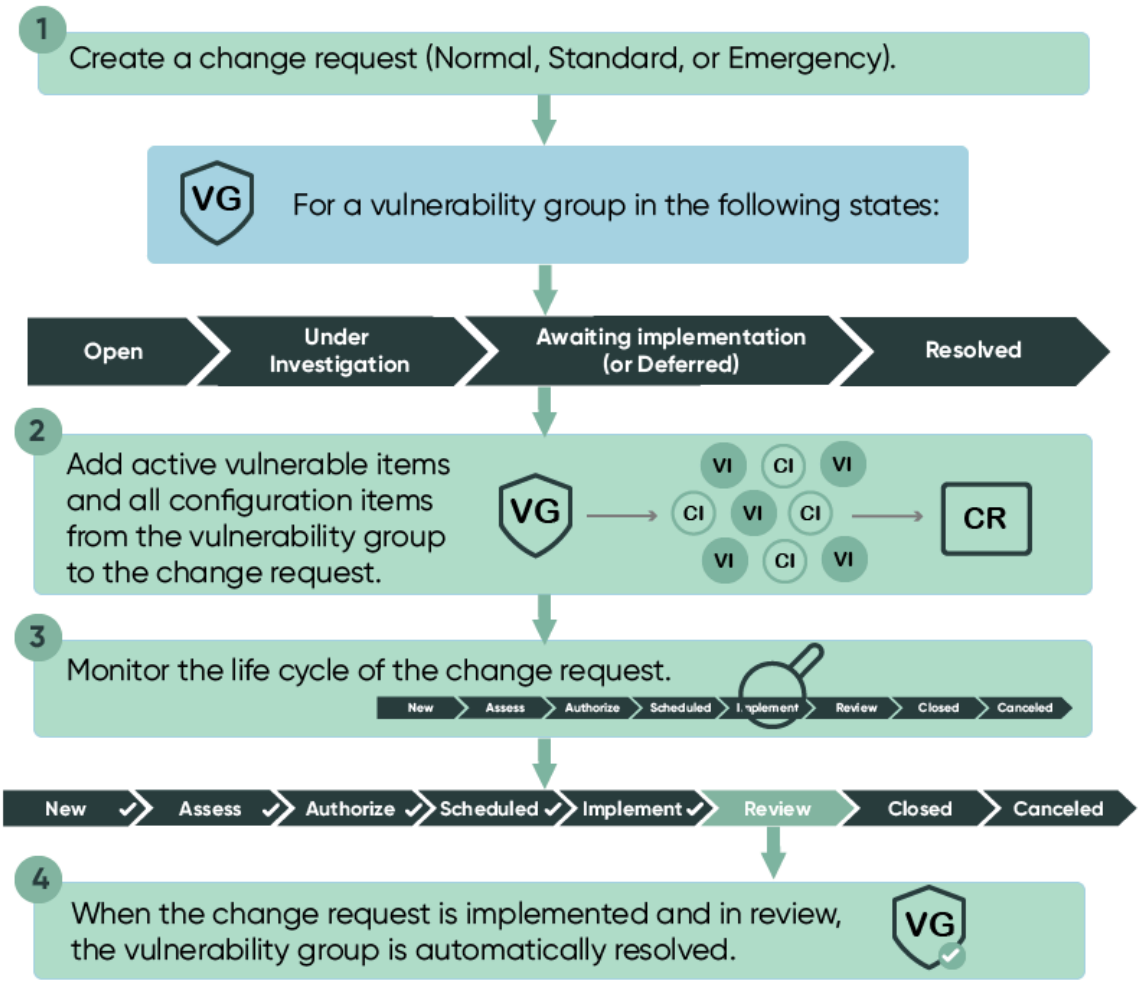
정정 작업에서 직접 변경 요청을 생성, 승인, 구현, 검토 및 종결할 수 있습니다. 정정 작업에서 미리 채워진 정보로 세 가지 유형의 변경 요청을 생성할 수 있습니다.

- 표준. 위험이 적고, 비교적 일반적이며, 지정된 절차나 작업 지시를 따르는 사전 승인된 변경입니다.
- 보통. 일반 변경 요청은 구현, 검토 및 종결 전에 두 가지 수준의 승인이 필요한 후속 대응적 프로세스를 따릅니다.
- 비상. 중요 인시던트를 해결하기 위한 변경입니다.

다음 이미지는 VUL(정정 작업)에서 변경 요청을 생성하는 기본 플로우를 보여줍니다. 이 플로우에 대한 자세한 단계는 이미지를 따릅니다.

다음 섹션에서는 정정 작업 기록을 VUL이라고 합니다. 이전 취약성 대응버전의 에서는 정정 작업을 취약성 그룹(VG)이라고 했습니다. 다음 이미지에서 VG= 정정 작업 또는 VUL 기록입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



주:
새 변경 요청 생성에 대한 주요 포인트:

- ## 상태가 아닌 모든 정정 작업(VUL)에 대한 새 변경 요청을 생성할 수 있습니다.
- 만들거나 VUL에 연결한 표준(사전 승인됨) 이외의 변경 요청에 대한 승인자가 있는지 확인합니다. 이렇게 하면 VUL을 신속하게 해결할 수 있습니다. 사용자 추가에 대한 자세한 내용은 다음 문서를 참조하십시오 Vulnerability Response 그룹에 사용자 추가.
- 정정 작업을 해결하기 전에 변경 요청을 구현하고 ## 상태로 이동할 수 있도록 VUL과 연결된 하나 이상의 CHG에 대한 모든 작업을 완료해야 합니다.

프로시저

1. 기존 정정 작업 기록에서 완전한 변경 요청을 생성하려면 다음으로 이동합니다. 모두 〉 취약성 대응 〉 정정 작업 〉 사용자 그룹에 할당됨.
   할당 그룹에 할당된 정정 작업 목록이 표시됩니다.
2. 옵션: 다음으로 이동 모두 〉 취약성 대응 〉 정정 개요 을 클릭하여 정정 개요 대시보드를 보고 사용자 또는 할당 그룹에 할당된 VUL을 찾습니다.
3. 또는 번호 열에서 정정 작업을 클릭하여 기록을 열고 상세 정보를 봅니다.
   기록이 표시됩니다.
4. 변경 요청을 생성할 VUL 레코드가 표시되면 레코드의 오른쪽 상단에서 변경 생성을 클릭합니다.
   변경 요청 생성 양식이 표시됩니다.
5. 필드에 내용을 입력합니다.

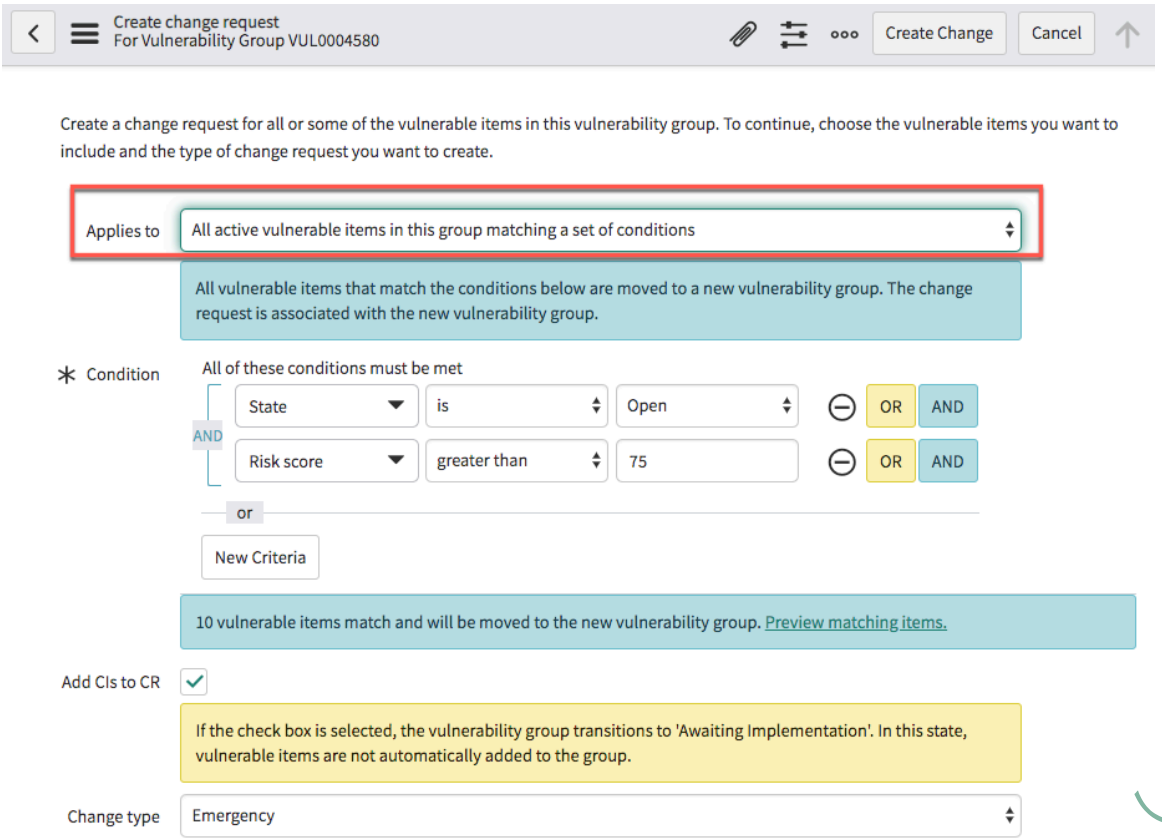
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 적용 대상 필드의 선택 목록에서 하나를 선택하여 계속합니다.

옵션	설명
이 그룹의 모든 활성 취약한 항목	이 항목을 선택한 경우, 변경 생성을 클릭하면 상태가 종결됨이 아닌 이 정정 작업에서 모든 활성 취약한 항목이 변경 요청에 자동으로 추가됩니다.
이 그룹에서 조건 세트와 일치하는 모든 취약한 항목	선택하면 아래 두 번째 그림과 같이 조건 작성기가 표시됩니다. 새 변경 요청에 필요한 취약한 항목을 식별하기 위한 필터 기준을 입력합니다. 필터의 예로는 특정 검색 조건과 일치하는 취약한 항목만 포함될 수 있습니다. 상태가 오픈이고 위험 점수 가 **75** 보다 큽니다. 조건을 입력하면 기준(10)과 일치하는 VI 수와 함께 메시지가 표시됩니다. 일치하는 항목을 미리 볼 수 있는 링크(일치하는 항목 미리 보기)가 표시됩니다. 필터 조건과 일치하는 항목이 없으면 조건 작성기 아래에 필터를 조정하라는 메시지가 표시됩니다. 변경 생성을 클릭하면 이 조건 필터와 일치하는 모든 취약한 항목이 새 정정 작업으로 이동됩니다. 이 변경 요청은 새 정정 작업에 연결됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

조건 세트와 일치하는 작업의 취약한 항목에 대한 변경 요청 양식 생성



b. 옵션: 폼에 디스플레이된 경우, 일치하는 항목 미리보기 링크를 클릭하여 필터 조건과 일치하는 VI 목록을 확인합니다.
정정 작업 목록 미리 보기가 표시됩니다. 이 미리 보기 목록에서 항목을 선택하고 해당 항목에 대한 UI 작업을 수행할 수 있지만 이러한 작업은 VUL에서도 수행됩니다. 예를 들어 미리보기 목록에서 VI를 삭제하면 해당 VI도 VUL에서 삭제됩니다.

c. 미리 보기를 마친 후 브라우저 창을 닫아 변경 요청 양식을 반환합니다.

d. CR에 CI 추가 확인란에서 하나를 선택하여 계속합니다.

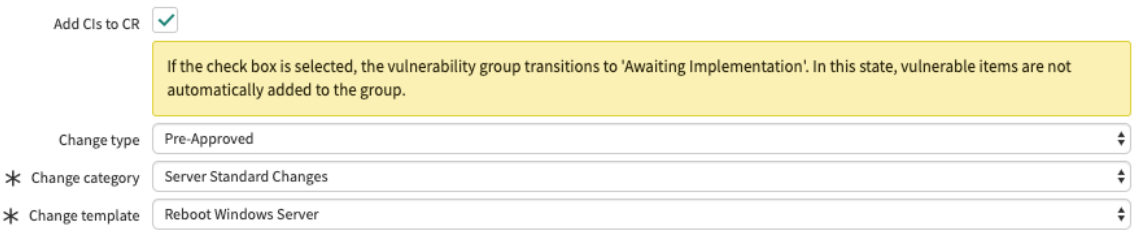
옵션	설명
CR에 CI 추가 확인란 선택됨	기본값은 선택되어 있습니다. 확인란을 선택하면 이 정정 작업의 활성 취약한 항목에 속하는 모든 CI(구성 항목)가 변경 요청에 추가됩니다. VUL은 자동으로 ## ## # 상태로 이동합니다.
CR에 CI 추가 확인란 선택 취소	이 정정 작업의 활성 취약한 항목의 CI가 새 변경 요청에 추가되지 않도록 하려면 확인란의 선택을 취소합니다. 사용하지 않도록 설정하면 변경 요청의 상태가 VUL과 동기화되지 않고 VUL은 현재 상태로 유지됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

e. 변경 유형 필드의 선택 목록에서 하나를 선택하여 계속합니다.

유형 변경	설명
긴급	중요 인시던트를 해결하기 위한 변경입니다.
정상	표준 또는 긴급 변경이 아닌 서비스에 대한 변경을 구현하는 데 사용되는 변경 유형입니다.
표준	자주 구현되는 사전 승인되고 위험도가 낮은 변경 요청입니다. 승인된 표준 변경 요청은 표준 변경을 보다 효율적으로 액세스하고 요청할 수 있도록 템플릿 카탈로그에서 사전 정의될 수 있습니다. 선택하면 다음 그림과 같이 두 개의 필드가 표시됩니다. 각 선택 목록에서 하나를 선택하여 다음 필드를 채웁니다. ▪ 범주 변경: 기존 카탈로그에서 변경할 범주(예: ####, ## ## ##, #####)를 선택합니다. 이 예에서는 ## ## ## ## 이 선택되어 있습니다. ▪ 변경 템플릿: 카탈로그에서 미리 정의된 지원 작업이 있는 변경 요청에 사용할 수 있는 템플릿 하나를 선택합니다. 이 예에서는 Microsoft ## ## ## 템플릿이 선택되어 있습니다. ITSM 변경 요청 범주, 템플릿 및 변경 유형에 대한 자세한 내용은 변경 유형을 참조하십시오.

이 기능은 ITSM Change Management의 카탈로그에 설정한 변경 요청 유형을 자동으로 읽습니다. 예를 들어, ITSM의 표준 변경 요청 이름을 ## 에서 ## ##됨으로 변경하면 다음 그림과 같이 변경 요청 생성 소스의 변경 유형 선택 목록에 새 이름이 자동으로 표시됩니다.



양식의 변경 요청 미리 보기 섹션에 있는 필드는 VUL의 정보로 미리 채워집니다. 필요한 경우 이러한 필드 값을 편집할 수 있습니다. 예를 들어, 다음 그림의 필드에 있는 값을 검토합니다.

계획된 종료 날짜

이 날짜(2019-10-10)는 VUL의 정정 대상 날짜 필드에 표시되는 값과 동일합니다. 이 값은 VUL에 속한 취약한 항목의 가장 빠른 정정 목표 날짜에서 파생됩니다. 이전 정정 날짜가 필요한 중요한 문제에 대한 변경 요청을 생성하는 경우 이 값과 우선순위 필드의 값을 편집하는 것이 좋습니다.

근거

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

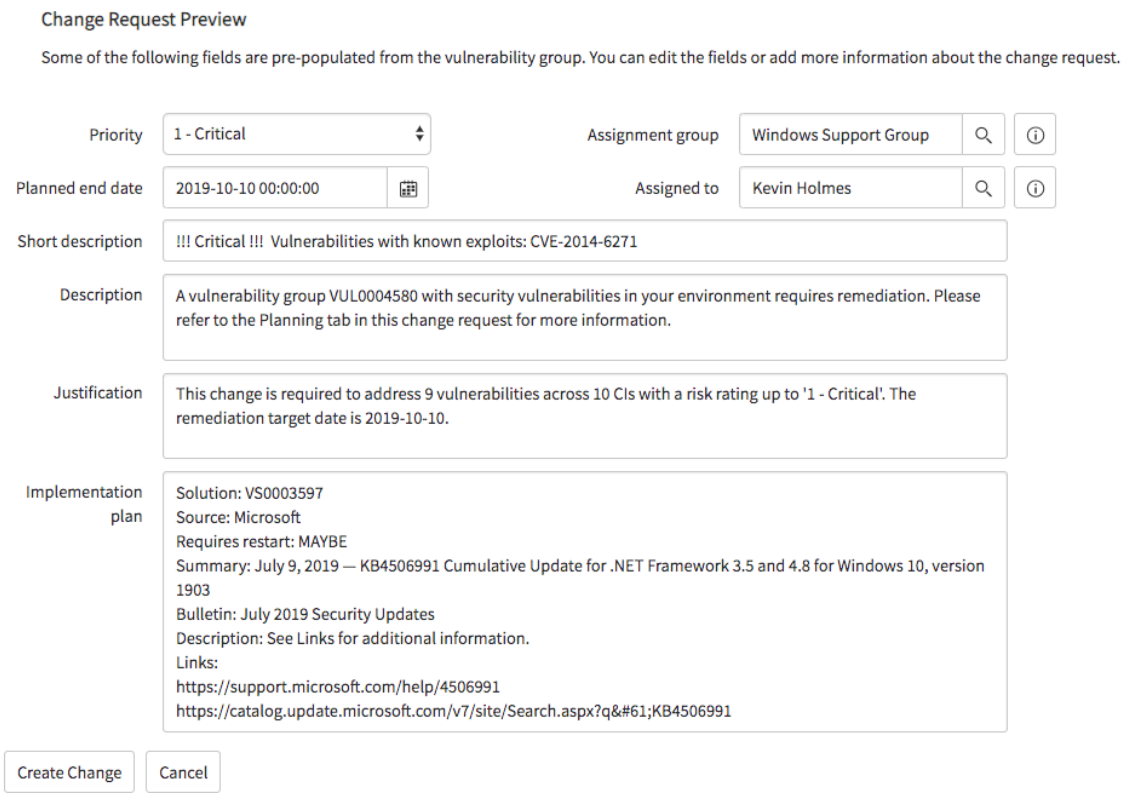
이 필드에는 CHG에 추가된 CI 수가 표시됩니다. 추가 정보를 추가하려면 이 텍스트를 편집하는 것이 좋습니다. 예를 들어, 새 VUL을 생성하는 데 사용한 필터(예: ## ### 75## #)에 대한 메모를 이 필드에 추가할 수 있습니다. 이 텍스트는 새 변경 요청 및 정정 작업을 찾는 데 도움이 됩니다.

구축 계획

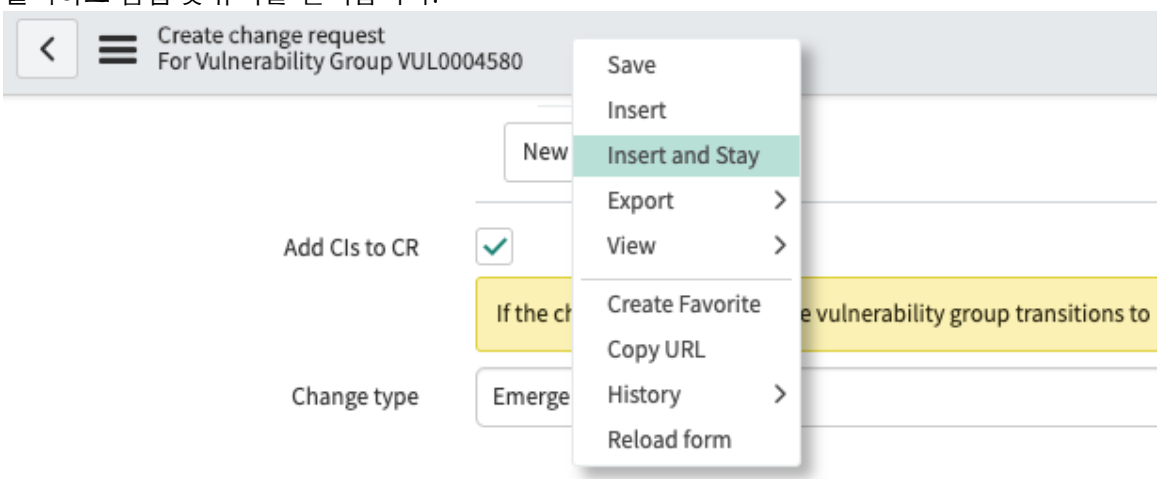
이 필드에는 취약성에 대한 기본 솔루션이 표시됩니다.

할당 그룹 및 할당 대상

할당 그룹을 변경하거나 이 변경 요청을 할당 그룹 중 하나의 사용자에게 재할당하려면 이러한 필드를 편집합니다.

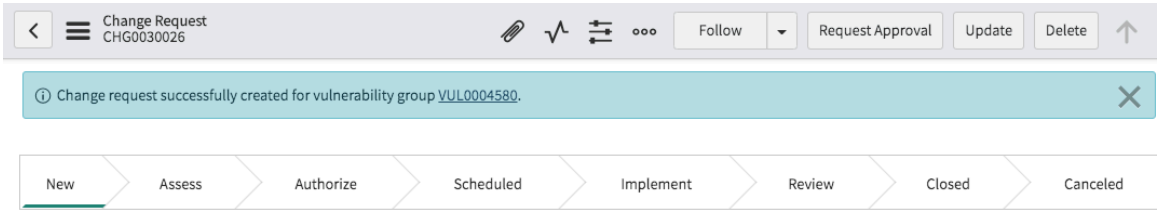


6. 필요에 따라 필드를 계속 미리 보고 편집합니다.
7. 변경 내용을 저장하고 이 페이지에 남아 있으려면 폼 위쪽의 회색 배너를 마우스 오른쪽 버튼으로 클릭하고 삽입 및 유지를 선택합니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

8. 편집을 완료한 후 하나를 선택하여 계속합니다.



주:

할당 그룹 및 할당 대상 필드가 할당되지 않은 ## ### 정정 작업의 경우(비어 있음) 변경 생성을 클릭하면 현재 로그온한 사용자가 작업에 자동으로 할당됩니다. 또한 CR에 CI 추가 확인란을 선택해야 합니다. VUL 상단에 이 할당을 나타내는 파란색 확인 메시지가 표시됩니다.

다음에 수행할 작업

변경 요청 및 변경 작업을 모니터링하여 완료되었고 변경 요청이 구현되었는지 확인합니다. 이 CHG가 구현되고 ## 상태로 이동한 후 상태 동기화가 활성화되면 VUL이 자동으로 ###으로 이동합니다. 상태 동기화에 대한 자세한 내용은 다음 문서를 참조하십시오 변경 요청과 정정 작업 간의 상태 동기화.

정정 작업을 기존 변경 요청에 연결

IT 정정 소유자는 정정 작업(VUL)을 인스턴스에서 이미 사용할 수 있는 변경 요청에 연결하여 정정 작업을 해결할 때 중복 변경 요청(CHG)을 생성하지 않도록 합니다.

시작하기 전에

가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

필요한 역할: itil 역할이 있는 모든 사용자 itil 역할이 할당되면 sn_vul.remediation_owner 역할도 사용자에게 자동으로 할당됩니다.

이 태스크 정보

정정 작업을 기존 변경 요청에 연결하는 방법에 대한 자세한 내용은 다음 문서를 에서 변경 요청 만들기 IT 정정 작업 공간참조하십시오.

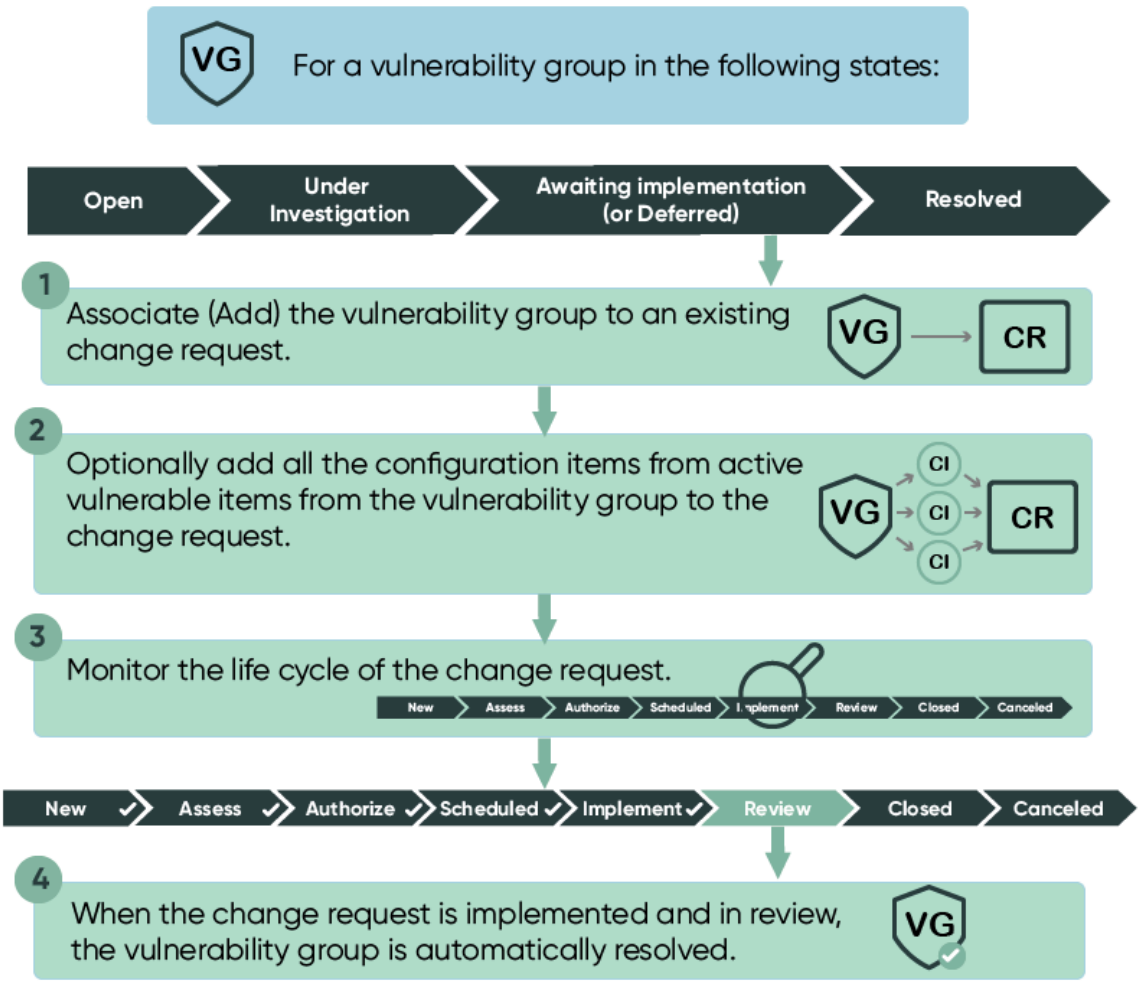
다음 섹션에서는 정정 작업 기록을 VUL이라고 합니다. 이전 버전의 취약성 대응에서는 정정 작업을 취약성 그룹(VG)이라고 했습니다. 다음 이미지에서 VG= 정정 작업 또는 VUL 기록입니다.

정정 작업을 기존 변경 요청에 연결하는 방법에 대한 자세한 내용은 다음 문서를 에서 변경 요청 만들기 IT 정정 작업 공간참조하십시오.

정정 소유자는 본인 또는 할당 그룹에 할당된 정정 작업을 정정 작업 기록에서 직접 기존 변경 요청에 연결할 수 있습니다. 다음 이미지는 변경 요청을 기존 VG(VUL)에 연결하기 위한 기본 플로우를 보여줍니다. 이 플로우에 대한 자세한 단계는 이미지를 따릅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

정정 작업을 기존 변경 요청에 연결하기 위한 워크플로우



주:
모든 상태(오픈, 조사 중, 구현 대기 중, 종결 및 연기됨)의 취약성에 기존 변경 요청을 연결할 수 있습니다. 변경 요청을 기존 VUL에 연결하면 활성 VI만 변경 요청에 추가됩니다.

시작하기 전에 중복 변경 요청의 생성을 방지하기 위해 VUL과 이미 연결된 기존 변경 요청을 보는 것이 좋습니다. 특정 VUL과 관련된 변경 요청 수를 쉽게 추적하려면 정정 작업 목록에서 CR 카운트 열을 참조하십시오. 표시되지 않으면 오른쪽 상단의 설정 아이콘( )을 클릭합니다. CR 카운트 열을 사용 가능에서 선택됨으로 이동하고 확인을 클릭합니다.

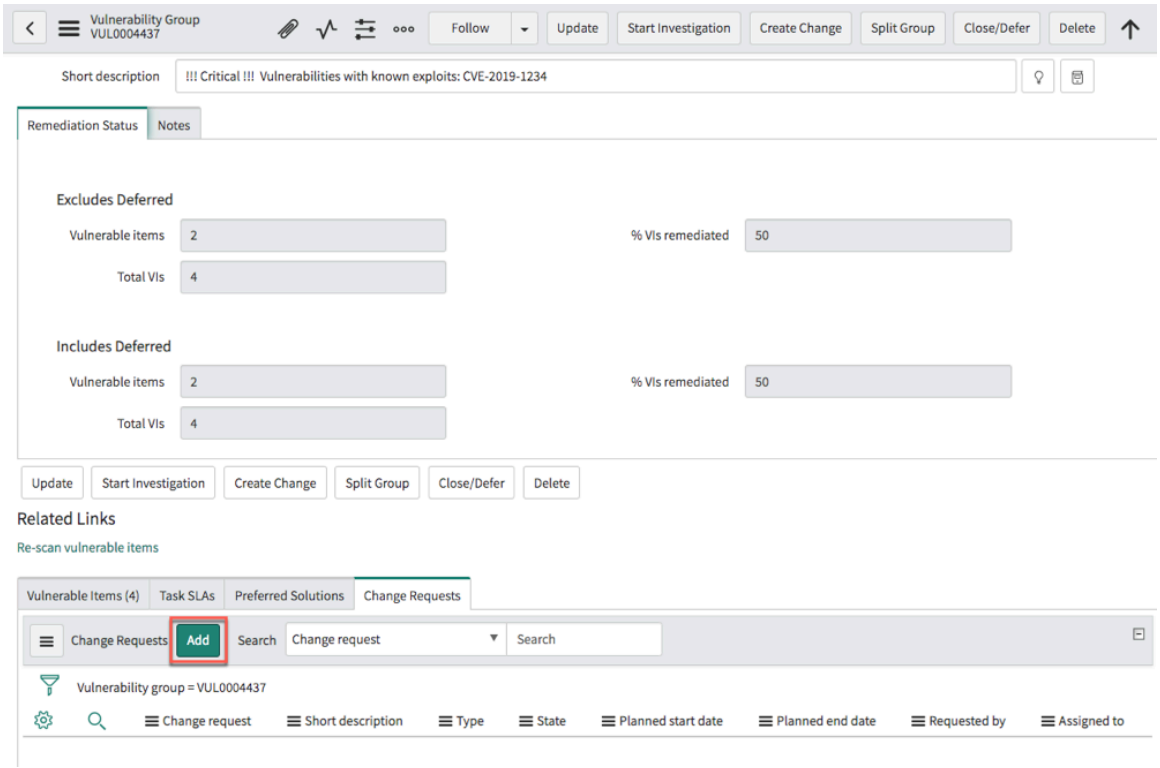
새 열을 자동으로 채우려면 이 테이블에 기존 데이터가 있는 고객의 경우 예약된 작업인 # CR ### # ###를 실행합니다.

프로시저

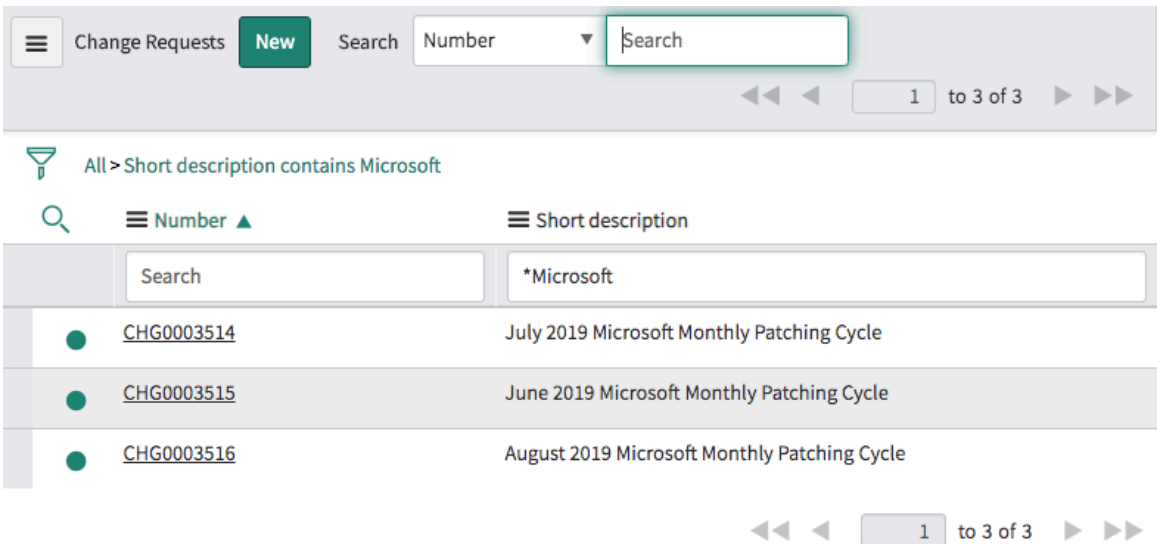
1. 정정 작업을 기존 변경 요청에 연결하려면 다음으로 이동합니다. 모두 〉 취약성 대응 〉 정정 작업.
2. 작업 중인 정정 작업을 찾습니다.
3. 옵션: 다음으로 이동 모두 〉 취약성 대응 〉 정정 개요 을 클릭하여 정정 개요 대시보드를 보고 사용자 또는 할당 그룹에 할당된 VUL을 찾습니다.
4. 번호 열에서 VUL 레코드를 클릭하여 엽니다.
   VUL 레코드가 표시됩니다.
5. 열린 기록이 표시된 상태에서 아직 표시되지 않았다면 변경 요청 관련 목록으로 스크롤하여 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

VUL과 연관된 모든 변경 요청은 추가 단추와 함께 표시됩니다. 다음 그림에는 이 VUL과 이미 연결된 변경 요청이 없습니다.



6. VUL을 기존 CHG와 연결하려면 추가를 클릭합니다.
   정정 작업에 기존 변경 요청 추가 양식이 표시됩니다.
7. 양식에서 검색 아이콘을 클릭합니다.
   다음 그림과 같이 기존 변경 요청의 목록 뷰가 새 창에 표시됩니다.



8. 표시된 목록에서 항목을 선택하거나, 필터(.)을 클릭하고 조건을 입력하여 검색 결과를 제한합니다.
9. CR에 CI 추가 확인란에서 하나를 선택하여 계속합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
이 확인란은 ## 상태의 기존 변경 요청에 대해서만 표시됩니다.

옵션	설명
CR에 CI 추가 확인란 선택됨	기본값은 선택되어 있습니다. 확인란을 선택하면 이 정정 작업의 활성 취약한 항목에 속하는 모든 CI(구성 항목)가 변경 요청에 추가됩니다. 선택하면 변경 요청의 상태가 VUL로 동기화됩니다. 자세한 내용은 변경 요청과 정정 작업 간의 상태 동기화 문서를 참조하십시오.
CR에 CI 추가 확인란 선택 취소	이 정정 작업의 활성 취약한 항목의 CI가 새 변경 요청에 추가되지 않도록 하려면 확인란의 선택을 취소합니다. 사용하지 않도록 설정하면 변경 요청의 상태가 VUL과 동기화되지 않고 VUL은 현재 상태로 유지됩니다.

10. 변경 요청 검색 필드에 표시할 변경 요청 번호를 선택하고 제출을 클릭합니다.
VUL이 표시됩니다. 기록 상단에 선택한 변경 요청이 VUL에 성공적으로 연결되었음을 나타내는 파란색 확인 메시지가 표시됩니다.

주:
할당 그룹 및 할당 대상 필드가 할당되지 않은 ## ### VUL(비어 있음)의 경우, 추가를 클릭하면 현재 로그온한 사용자가 자동으로 취약성에 할당됩니다. 또한 CR에 CI 추가 확인란을 선택해야 합니다. VUL 상단에 현재 사용자가 할당되었음을 나타내는 파란색 확인 메시지가 표시됩니다.

다음에 수행할 작업
VUL 기록을 검토합니다. 변경 요청 관련 목록의 변경 요청 열에서 새 CHG에 대한 링크를 클릭하여 CR 기록을 봅니다. 오픈 CHG 기록에서 변경 요청의 상태를 모니터링할 수 있습니다. 영향을 받는 CI(구성 항목) 및 정정 작업이 영향을 받는 CI 및 정정 작업 관련 목록에 표시됩니다.

정정 작업 분할

IT 정정 소유자는 기존 정정 작업(VUL)에서 새 그룹으로 이동하려는 VI(취약한 항목)의 하위 집합을 식별합니다.

시작하기 전에

주:

기존 VUL에서 새 정정 작업으로 VI를 분할하는 사용 사례에는 다음 예가 포함될 수 있습니다.

- 분할 작업에 대한 변경 요청 또는 변경 요청을 생성하려는 경우
- 할당 그룹의 다른 사용자에게 분할 그룹을 재할당하는 경우
- 특정 CI(구성 항목)의 일부 취약성을 지정된 기간 내에 해결할 수 없다는 것을 알고 있기 때문에 분할 작업에 대한 연기 또는 예외를 요청하는 경우.

필요한 역할: VUL 분할을 위한 itil 역할을 가진 모든 사용자

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
itil 역할이 사용자에게 할당되면 sn_vul.remediation_owner 역할도 자동으로 할당됩니다.

이 태스크 정보
작업 공간에서 정정 작업을 분할하는 취약성 대응 방법에 대한 자세한 내용은 다음 문서를 에서 정정 작업 분할 IT 정정 작업 공간참조하십시오.

클래식 환경 또는 취약성 대응. 버전에서 정정 작업을 분할하려면 다음을 수행합니다.

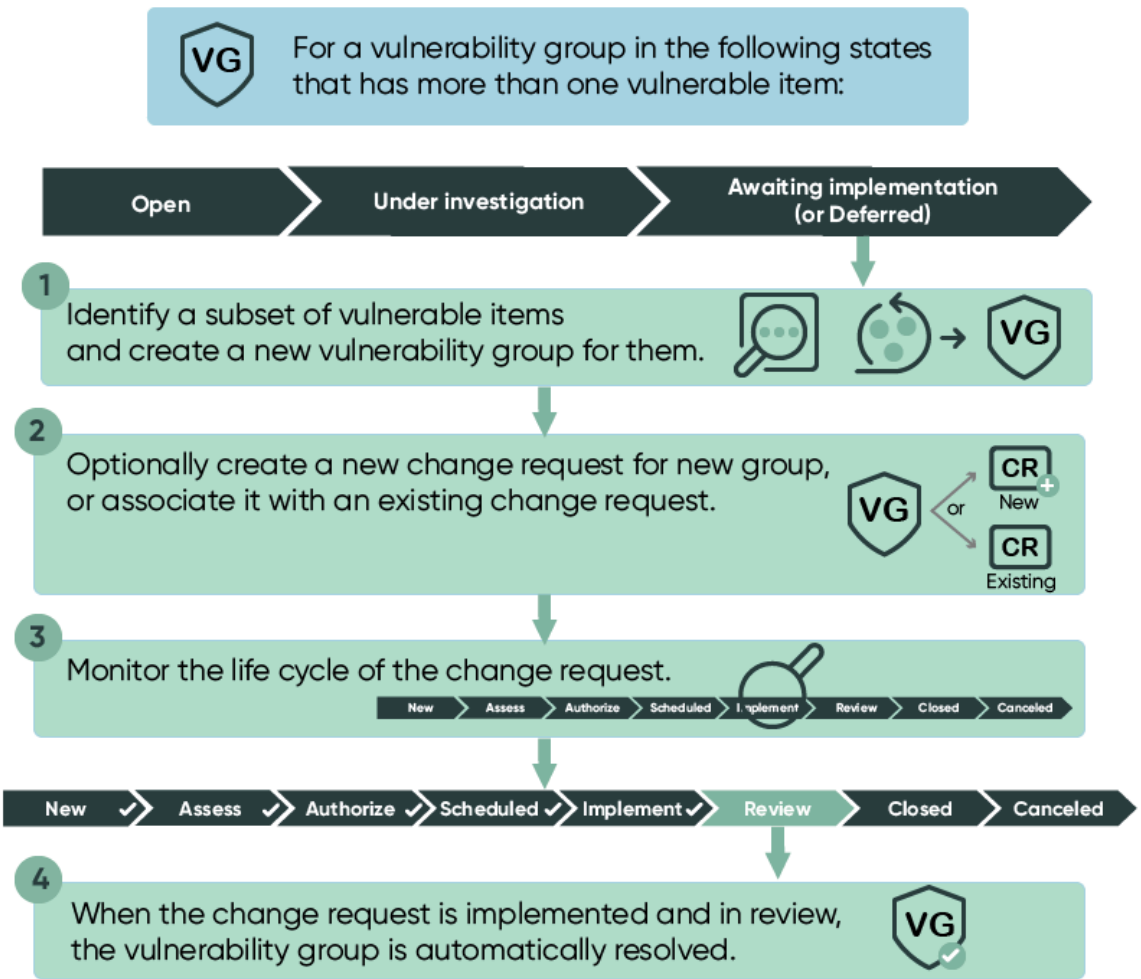
기존 정정 작업을 ##, 조사 중 또는 구현 대기 중 상태에 있는 둘 이상의 취약한 항목으로 분할할 수 있습니다. 특정 기준과 일치하는 취약한 항목을 사용하여 새 취약성을 생성하면 원래 정정 작업에 영향을 주지 않고 특정 그룹의 취약한 항목으로 작업할 수 있습니다.

조건 작성기를 사용하여 새 정정 작업으로 이동할 취약한 항목에 대한 조건을 지정하면 기준과 일치하는 활성 VI만 새 그룹으로 이동됩니다.

VUL을 분할할 때 변경 요청(CHG)을 생성할 필요가 없습니다. 변경 요청을 생성하는 동시에 VUL을 분할하거나 변경 요청을 생성하지 않고 VUL을 분할할 수 있습니다. 다음 이미지는 정정 작업을 분할하기 위한 기본 플로우를 보여줍니다. 이 플로우에 대한 자세한 단계는 이미지를 따릅니다.

다음 섹션에서는 정정 작업 기록을 VUL이라고 합니다. 이전 버전의 취약성 대응에서는 정정 작업을 취약성 그룹(VG)이라고 했습니다. 다음 이미지에서 VG= 정정 작업 또는 VUL 기록입니다.

정정 작업을 분할하기 위한 워크플로우

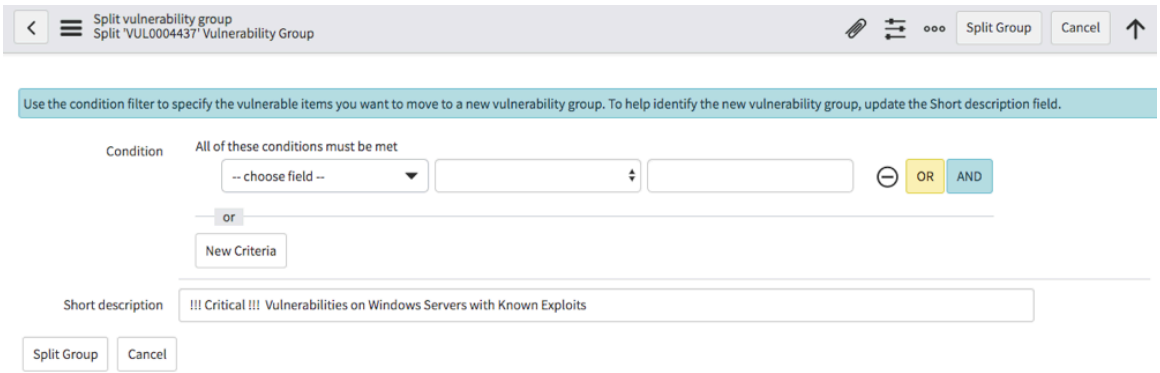


기계 번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 정정 작업 〉 사용자 그룹에 할당됨.
   정정 작업 목록이 표시됩니다.
2. 번호 열에서 기록을 클릭하여 엽니다.
   기록이 표시됩니다.
3. VUL의 오른쪽 상단에서 분할 작업을 클릭합니다.
   분리 정정 작업 양식이 표시됩니다.

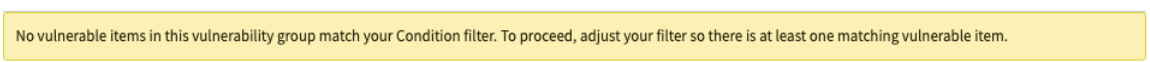


4. 조건 필터가 표시되면 새 작업으로 이동하려는 취약한 항목에 대한 조건을 지정합니다.
   예를 들어 다음 조건과 일치하는 취약한 항목만 필터링하는 것을 선호할 수 있습니다.
   - ## 상태에서.
   - 위험 점수가 80보다 큽니다.
   - 'WINSV'를 포함하는 구성 항목입니다.
   - 샌디에이고에 위치하고 있습니다.

   예를 들어 조건의 경우 다음과 같이 입력할 수 있습니다.
   - 상태 - 다음과 같음 - 열림
   - 위험 점수 - 보다 크거나 같음 - 80
   - 구성 항목입니다. 이름 - 포함 - WINSV
   - 구성 항목입니다. 위치 - 는 - 샌디에이고

   조건을 입력한 후 취약한 항목이 필터와 일치하면 일치하는 취약한 항목 수가 포함된 메시지가 표시됩니다.

   주:
   필터와 일치하는 취약한 항목이 없다는 메시지가 표시되면 하나 이상의 취약한 항목이 필터 기준과 일치하도록 조건을 조정합니다.

5. 옵션: 필요에 따라 필터를 조정합니다.
6. 옵션: 새 VUL이 생성된 후 식별하는 데 도움이 되도록 간단한 설명 필드를 업데이트하는 것이 좋습니다.
   편집된 경우 간단한 설명 필드를 새 VUL에 대한 검색 기준으로 사용하여 생성된 후 찾을 수 있습니다(예: SAN DIEGO# ##).
7. 옵션: 필터 기준과 일치하는 취약한 항목에 대한 세부 정보를 미리 보려면 작업 분할 을 클릭하여 새 VUL을 생성하기 전에 다음 단계를 수행합니다.

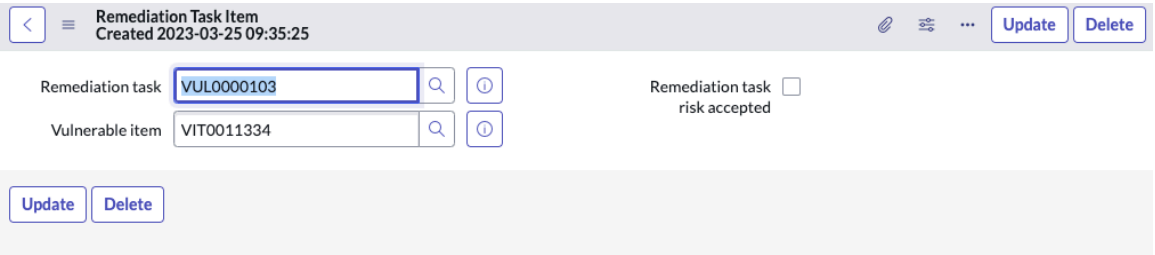
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이러한 상세 정보에는 이 하위 집합과 이미 연결된 기존 변경 요청 및 이러한 취약한 항목이 있는 VUL이 포함됩니다. 미리 보기에서 이 정보를 보면 중복 VUL을 생성하지 못할 수 있습니다.

a. 분리 정정 작업 양식의 파란색 확인 메시지에서 일치하는 항목 미리 보기를 클릭합니다. 정정 작업 항목 목록이 브라우저의 새 창에 조건과 일치하는 취약한 항목 목록과 함께 표시됩니다.

b. 번호 열에서 항목을 클릭하여 기록을 엽니다.

c. 표시되는 레코드에서 취약성 그룹 또는 취약성 항목 필드 오른쪽에 있는 취약한 항목의 정보 아이콘을 클릭하여 기록을 봅니다.



d. 표시되는 대화 상자에서 기록 열기를 클릭합니다. 정정 목표 날짜에 대한 정보가 표시됩니다. 관련 목록 섹션에서 관련 목록을 클릭하여 VI에 대한 자세한 정보를 확인합니다.

8. 조건을 충족하는 VI로 새 VUL을 생성할 준비가 되면 미리보기 창을 닫고 다른 창의 분할 작업 양식으로 돌아가고 양식 상단에서 작업 분할을 클릭합니다.

주:

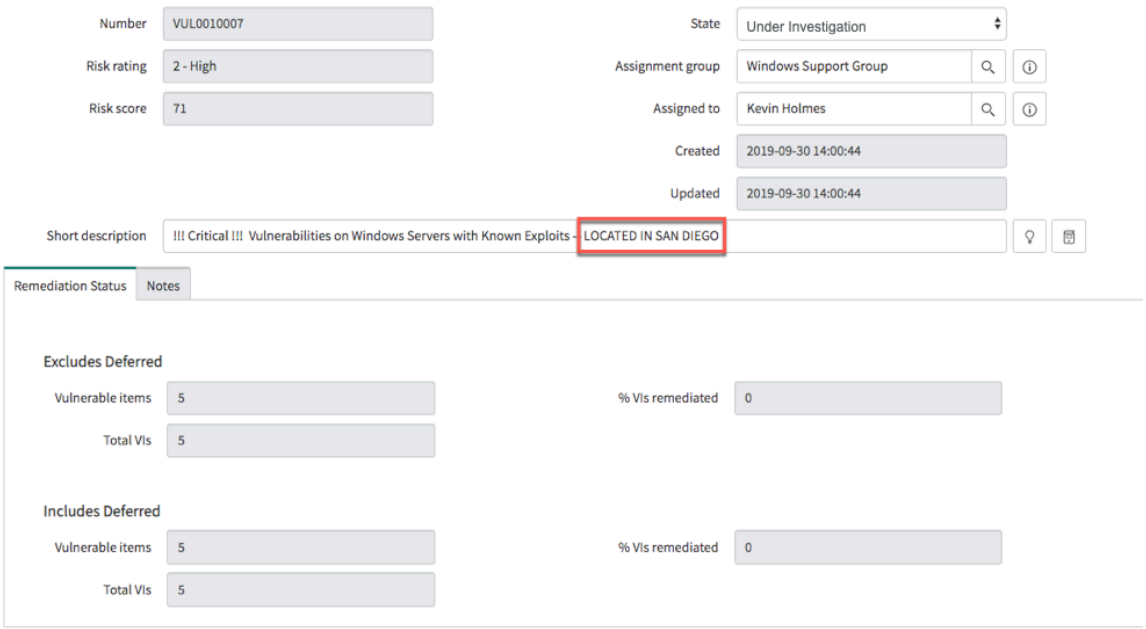
200개 미만의 VI의 경우, 분할 작업은 동기적으로 수행됩니다.

200개 이상의 VI의 경우, 분할 작업은 백그라운드에서 비동기적으로 수행되며, VI가 새로운 그룹에 나타나기까지 몇 초가 걸릴 수 있습니다.

새 그룹으로 이동된 모든 활성 VI를 보여주는 확인 메시지가 표시됩니다. 새 정정 작업 번호도 표시됩니다. 아직 조사 중이 아닌 경우 VUL은 조사 중으로 이동됩니다. (SAN DIEGO# ##)에서 새 VUL에 대해 입력한 텍스트에 대한 간단한 설명 필드를 확인합니다.

새 그룹에 대한 롤업 계산은 새 위험 점수, 정정 대상 날짜 및 기타 필드 값을 계산하기 위해 수행됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



취약한 항목, 기본 솔루션 및 변경 요청이 기록 하단의 관련 목록에 표시됩니다. 정정 작업을 수행할 때와 마찬가지로 이 새 작업을 처리하고 모니터링합니다.

9. 옵션: 메모 관련 목록으로 스크롤한 후 클릭하여 선택합니다.
   원래 정정 작업의 취약한 항목 수가 활동 스트림의 새 그룹으로 이동되었는지 확인합니다.
10. 옵션: 새 VUL에서 취약한 항목 관련 목록에서 VI를 선택하고 다시 한 번 분할하려면 정정 작업 기록의 맨 아래로 스크롤하고, 취약한 항목 관련 목록의 취약한 항목 열에서 이동하려는 VI를 선택한 상태에서 선택한 행 선택 목록에 대한 작업 선택 목록에서 작업 분할을 선택합니다.
    분리 정정 작업 양식이 표시됩니다.
11. 그룹을 다시 분할하고 선택한 항목을 새 그룹으로 이동하려면 작업 분할을 클릭합니다.
    선택한 VI가 다른 정정 작업으로 이동되고 확인 메시지가 표시되며 새 그룹이 표시됩니다.
12. 조사 또는 정정을 계속하려면 하나를 선택합니다.

다음에 수행할 작업

새로운 VUL의 상태를 모니터링하여 해결을 신속하게 처리합니다.

변경 요청과 정정 작업 간의 상태 동기화

제품의 VUL(정정 작업)의 상태 필드와 CHG(변경 요청)의 상태 필드 간에 동기화된 취약성 대응 관계가 있습니다. 변경 요청은 수명주기를 거치면서 관련 정정 작업의 상태도 자동으로 이동합니다.

상태 동기화

다음 섹션에서는 정정 작업 기록을 VUL이라고 합니다. 이전 버전의 취약성 대응에서는 정정 작업을 취약성 그룹(VG)이라고 했습니다. 다음 이미지에서 VG= 정정 작업 또는 VUL 기록입니다.

상태 동기화는 애플리케이션을 다운로드할 때 인스턴스에서 기본적으로 시스템 속성(sn_vul.cr_state_synch)에 취약성 대응 의해 활성화됩니다.

상태 동기화가 활성화되면 다음과 같은 경우 CHG 상태 필드가 정정 작업 상태 필드를 자동으로 변경합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

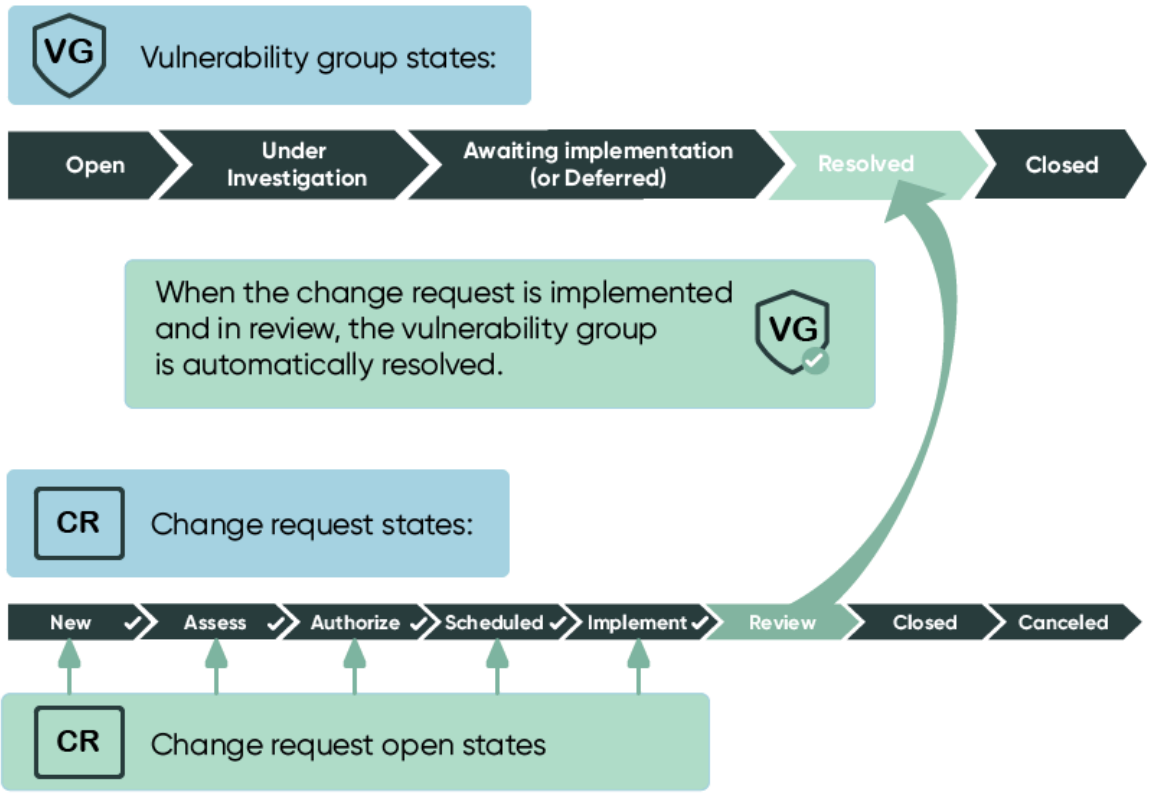
- 정정 작업(VUL)에 대해 새 CHG가 생성될 때 ## ## #이 아닌 경우 VUL 상태는 ## ## #으로 진행됩니다.
- 기존 CHG가 VUL에 연결된 경우 ## ## #이 아닌 경우 VUL 상태는 ## ## #으로 이동합니다.
- CHG의 작업이 완료(###)되고 CHG가 ## 상태로 이동하면 VUL이 ###으로 이동합니다.

상태 동기화에 대한 자세한 내용과 예는 다음 섹션을 참조하십시오.

주:
상태 동기화가 활성화된 상태에서 해당 기록의 수명 주기 상태를 통해 CHG 및 VUL을 수동으로 이동할 수 있지만, CHG가 상태를 변경했다고 시스템이 등록하거나 CHG를 추가하거나 VUL에서 제거하면 상태 동기화가 수동 개입을 재정의할 수 있습니다. 그러나 변경 요청 상태는 VUL을 ## 또는 ### 상태에서 자동으로 이동하지 않습니다.

정방향 상태 동기화

다음 이미지는 CHG 상태가 정방향 수명주기(#, ## 에서 ###)에서 VUL 상태를 자동으로 이동하는 방법을 보여줍니다.



상태가 아닌 모든 정정 작업에 대한 새 변경 요청을 생성할 수 있습니다. 상태 동기화는 VUL# Open, Under Investigation, Awaiting Implementation 및 Resolved 상태를 통해 자동으로 양방향으로 이동합니다. 이 이동은 변경 요청에 대한 상태 필드의 특정 값을 기반으로 합니다. 확인란(CR# CI ##)이 양식에 표시되고 확인란의 선택을 취소하지 않으면 변경 요청과 정정 작업 간의 상태 동기화가 자동으로 호출됩니다.

CHG가 열린 상태일 때 VUL은 ## 됨으로 진행되지 않습니다. 앞의 그림과 같이 ##, ##, ##, ##됨 또는 ##과 같이 수명주기에서 ## 이전 상태의 모든 CHG는 CHG에 대해 오픈 상태로 간주됩니다. CHG에 대한 조사 또는 작업이 완료되지 않았으므로 열린 상태는 VUL의 상태 필드를 이동하지 않습니다. 상태 동기화는 CHG가 VUL에 대해 작성되거나 VUL과 연관되거나 CHG에서 기존 관계의 상태가 변경될 때 호출됩니다. 완료된 CHG 상태는 ## 및 ##### ###입니다. CHG가 성공적으로 종결되면 종결 코드는 ## 또는 ### ## ##이며, 이 경우 VUL은 ###으로 이동합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

역방향 상태 동기화

CHG는 수명 주기 동안 처리되므로 특정 시점에서 취소될 수 있습니다. 이 경우 CHG가 ##되거나 ## 되면(종결 코드가 ## 함) VUL은 자동으로 ## #으로 다시 이동합니다. 취약성을 정정하기 위한 활성 계획이 없기 때문에 VUL이 ## #으로 다시 이동합니다.

VUL이 ### 상태이고 새 CHG를 만들거나 초기 열린 상태 중 하나에서 기존 CHG에 연결하면 VUL은 자동으로 ## ## #으로 다시 전환됩니다. 이제 CHG에 더 많은 작업이 할당되었기 때문에 VUL이 이 상태로 다시 이동합니다.

CHG가 두 개 이상인 **VUL**

VUL에 둘 이상의 CHG가 연결되어 있는 경우 상태 동기화는 수명 주기의 가장 초기 상태에 있는 CHG의 상태를 기반으로 합니다. 예를 들어, 다음 표와 같이 VUL에는 CHG1, CHG2, CHG3 및 CHG4의 4개의 CHG가 연결되어 있습니다.

변경 번호	변경 상태
1	구현
2	취소됨
3	종결됨(실패 종결 ##)
4	종결(종결 코드 ##)

이 경우 CHG와 VUL 간의 상태 동기화는 4개의 CHG 중 가장 초기 상태인 CHG1(##)을 기반으로 합니다. 이 경우 VUL은 ## ## ### 남아 있습니다.

또 다른 예로, VUL이 ### 상태이고 구현되어 ## 상태인 기존 CHG가 있고 새 CHG가 작성되면 VUL이 ### 에서 ## ## #으로 다시 이동합니다. 상태 동기화는 가장 빠른 상태의 CHG인 ## 상태의 CHG를 기반으로 합니다.

변경 번호	변경 상태
1	검토
2	신규

또한 VUL에 둘 이상의 CHG가 있는 경우 VUL의 상태는 다음과 같은 경우에 자동으로 전환됩니다.

- CHG가 ##로 이동할 때 VUL과 연결된 다른 모든 CHG가 ## 또는 ## 상태(성공적인 종결 코드 포함)에 있는 경우 VUL은 자동으로 ###으로 전환됩니다. 취소되거나 성공적으로 종결된 기타 관련 CHG는 무시됩니다.
- CHG가 ## 됨 또는 ## 됨(##의 종결 코드)으로 이동할 때 VUL과 연결된 다른 모든 CHG가 동일한 상태인 경우 VUL은 자동으로 ## #으로 다시 전환됩니다.

정정 작업 상태 및 각 상태에서 수행할 수 있는 작업에 대한 자세한 내용은 다음 문서를 참조하십시오 취약성 대응 정정 작업 및 취약한 항목 상태.

취약한 소프트웨어에 대한 노출 평가

노출 평가 모듈에서 게시자 및 제품 정보를 제공하여 (SAM) Foundation 애플리케이션을 사용하여 취약한 소프트웨어에 대한 자산의 제로 데이(현재 날짜) 노출을 평가할 수 있습니다 ITSM 소프트웨어 자산 관리 .

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

중요사항:
소프트웨어 및 CVE(Common Vulnerabilities and Exposures)별 노출 평가를 수행하여 취약성 평가 작업 공간의 추가 기능을 활용할 수 있습니다. 자세한 내용은 취약성 평가 작업 공간 탐색 문서를 참조하십시오.

시작하기 전에

필요한 역할: 취약성 관리자(sn_vulnerability_write)
가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

평가하려는 취약한 소프트웨어에 대해 다음과 같은 정보를 준비합니다.

- 게시자
- 버전
- 제품
- 에디션

이 태스크 정보

시스템 요구 사항에 대한 자세한 내용은 다음 문서를 참조하십시오 취약성 노출 평가 구성.

소프트웨어 노출 평가 모듈을 보고 인스턴스의 취약한 소프트웨어에 ServiceNow AI Platform# 대한 요청 시 노출 평가 기록을 생성 및 편집합니다.

많은 자산을 담당하는 대규모 운영의 취약성 대응 활동을 관리합니다. 운영 중인 SOC(보안 운영 센터)에서 취약한 것으로 파악된 소프트웨어 버전에 대해 연락합니다. 자산 스캔이 최근에 완료되었으며 이 취약성을 찾지 못했습니다. SOC 팀이 NVD(국가 취약성 데이터베이스), CWE(일반적인 약점 열거) 또는 인스턴스의 다른 외부 공급업체 라이브러리 외부의 신뢰할 수 있는 소스에서 이 취약성에 대해 알게 되었으며, 취약성 스캐너가 아직 해당 플러그인을 추가하지 않은 것이 우려됩니다.

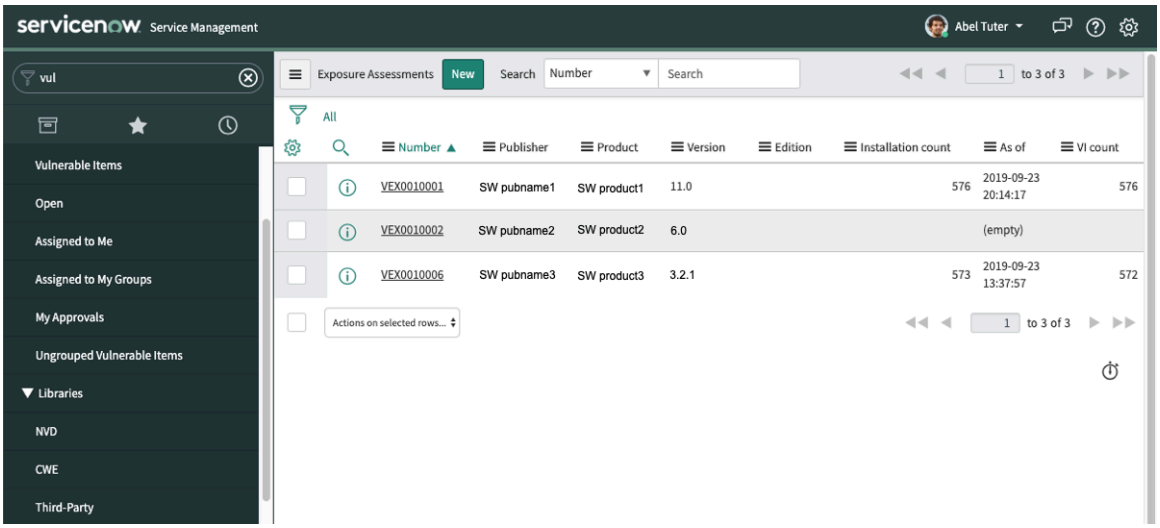
이 취약성에 대한 데이터가 NVD에서 업데이트되고 스캐너가 다음 검사에서 이 취약성을 포착할 수 있도록 곧 가져올 것이라고 확신하지만 잠재적인 노출 범위가 우려되기 때문에 네트워크에 이 소프트웨어가 설치된 자산이 있는지 지금 확인하려고 합니다.

의 취약성 대응v23.0부터 Pro 또는 Enterprise 구독이 있는 경우 모두 메뉴에서 노출 평가 링크를 선택한 역할에 따라 작업 공간의 노출 평가 페이지로 리디렉션됩니다. 자세한 내용은 취약성 노출 평가 구성 문서를 참조하십시오.

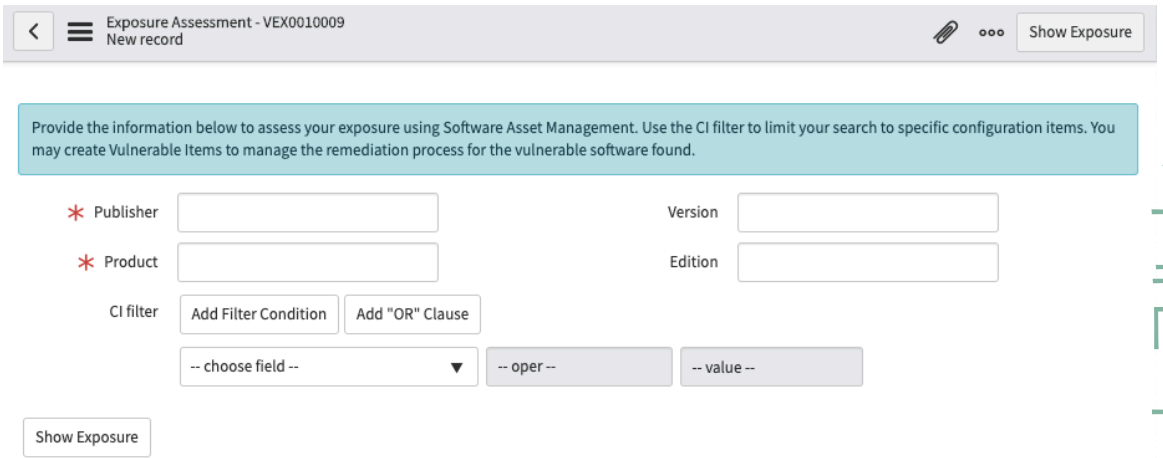
프로시저

1. 새 노출 평가를 생성하려면 다음으로 이동합니다. 모두 〉 취약성 대응 〉 취약성 스캐닝 〉 노출 평가.
   노출 평가 목록이 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



2. 새로 만들기를 선택합니다.
노출 평가 양식이 표시됩니다.

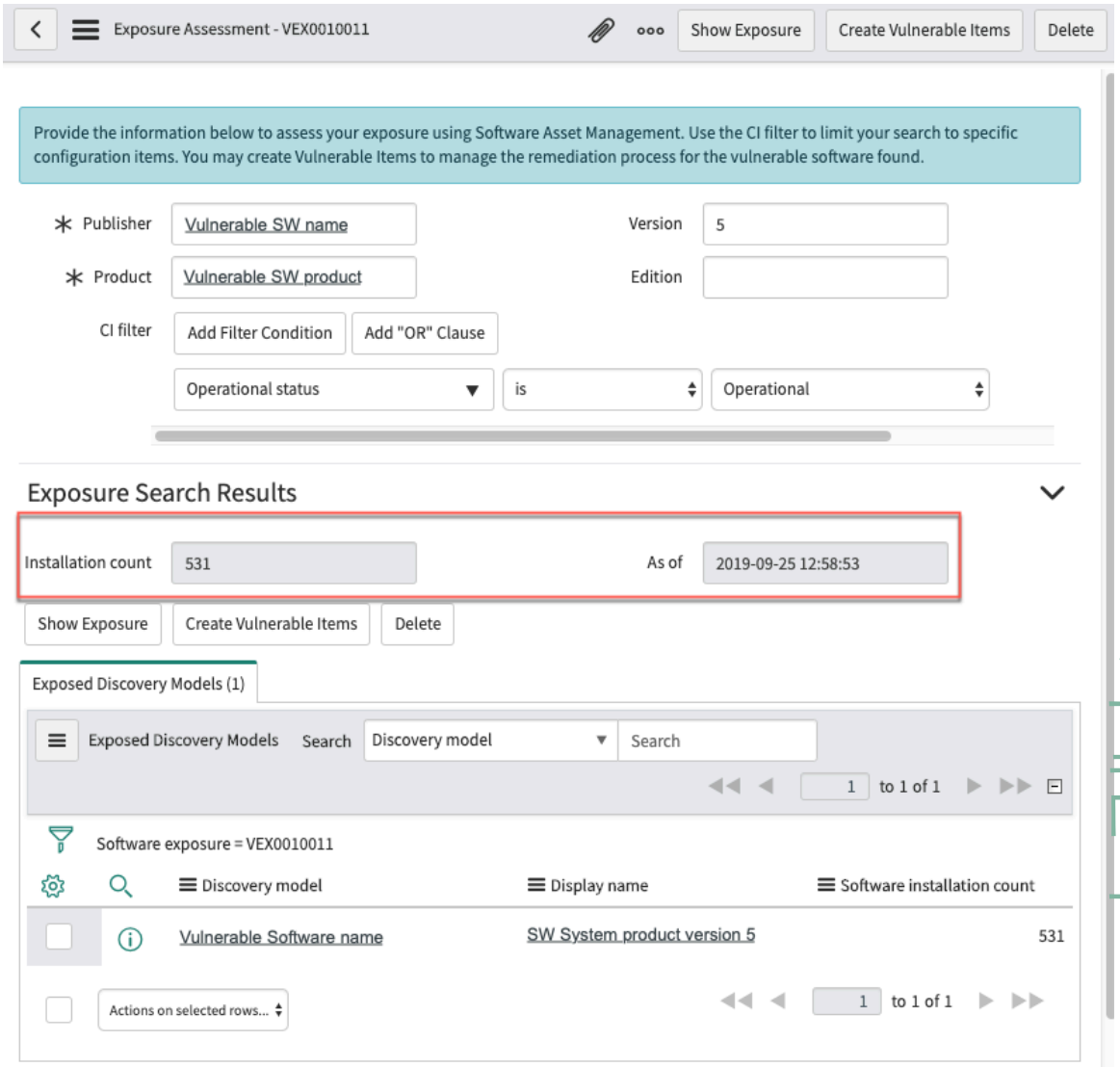


3. 양식을 작성합니다.

필드	설명
게시자	소프트웨어 게시자의 이름입니다.
(선택 사항) 버전	자산에 대한 검색 범위를 좁히는 데 도움이 되는 버전 번호를 입력합니다.
제품	소프트웨어 제품의 이름입니다.
(선택 사항) 판	자산에 대한 검색 범위를 좁히는 데 도움이 되는 에디션을 입력합니다.
CI 필터	CI(구성 항목) 필터의 선택 목록을 사용하여 검색을 특정 구성 항목(자산)으로 제한합니다. 예를 들어, 이 소프트웨어가 설치되어 있을 수 있는 활성 자산에 대해서만 쿼리를 제출할 수 있습니다. ## ### ## ####.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 노출 표시를 선택합니다.
   검색 모델과 특정 날짜를 기준으로 자산의 소프트웨어 설치 수가 포함된 노출 평가 기록이 표시됩니다.



5. 계속하려면 하나를 선택합니다.

6. 옵션: 검색 결과에 취약한 항목을 생성합니다.

   주:
   취약한 항목을 생성한 후에는 이 노출 기록에 대한 검색 기준을 변경할 수 없습니다.

7. 또는 필터 조건을 수정하고 검색 결과를 더 세분화합니다.
8. 취약한 항목을 생성하려면 다음 단계를 수행합니다.

   a. 취약한 항목 생성을 선택합니다.
      취약한 항목 생성 대화 상자가 표시됩니다.

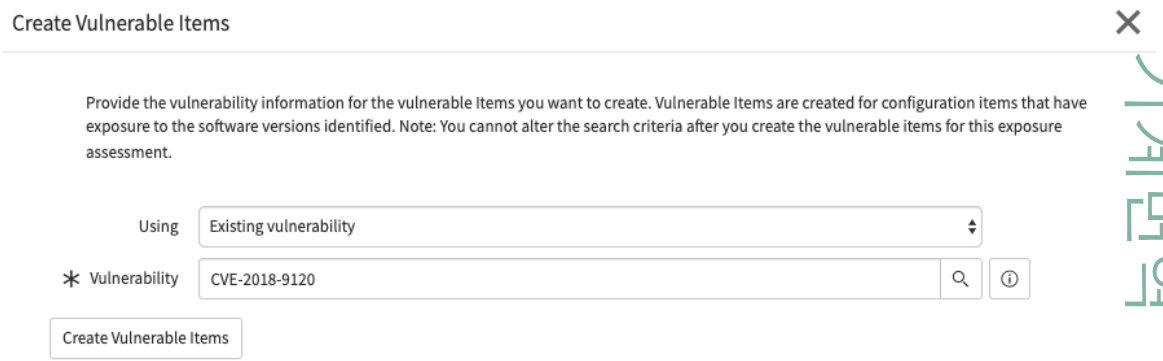
   b. 필드에 내용을 입력합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

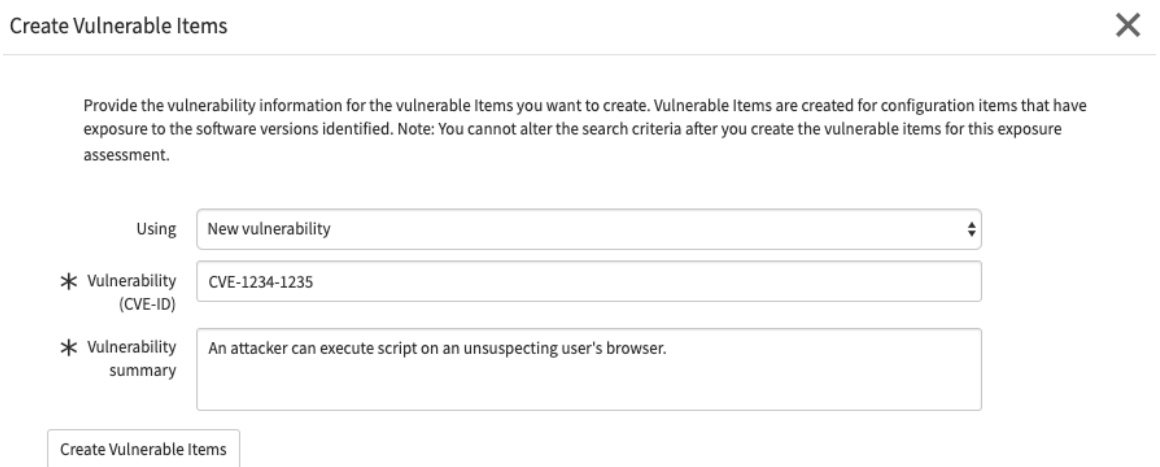
필드	설명
사용	선택 목록을 만들고 계속할 목록을 하나 선택합니다. ▪ 기존 취약성입니다. 취약성 필드 오른쪽에서 검색 아이콘을 클릭합니다. 표시되는 목록에서 CVE-ID를 선택하거나 검색 조건을 입력하여 기존 CVE-ID(예: CVE 2018-9120)를 찾습니다. 주: 이는 NVD 이외의 취약성 데이터베이스의 CVE-ID일 수 있습니다. ▪ 새로운 취약성입니다. 새로운 취약성에 대한 CVE-ID를 xxxx-xxxx, xxxx-xxxxx 또는 xxxx-xxxxxxx 형식으로 입력합니다.
취약성 요약 (새로운 취약성에만 해당)	새로운 취약점에 대한 요약을 입력합니다. 예를 들어, #### #### ## #### ###### ##### ### # ####.

다음 이미지는 기존 취약성과 새로운 취약성에 대해 작성된 양식의 예를 보여줍니다.

기존 취약성



새로운 취약성

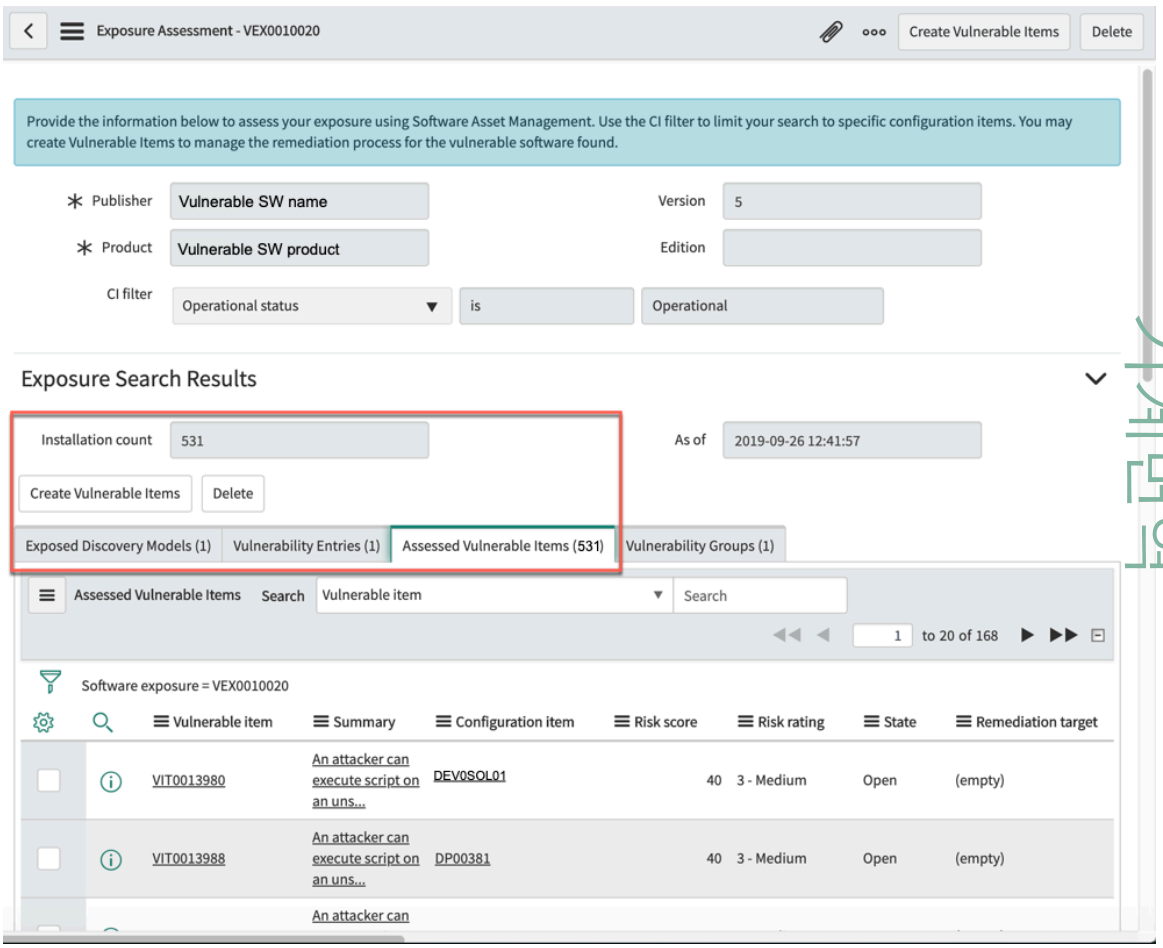


c. 취약한 항목 생성을 선택합니다.
노출 평가 기록은 취약한 항목이 생성되고 있음을 나타내는 상태 메시지와 함께 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

d. 몇 초 후 양식 상단에서 회색 배너를 마우스 오른쪽 버튼으로 클릭하여 페이지를 다시 로드합니다.
새로운 취약한 항목은 평가된 취약한 항목 탭(531)의 다음 그림과 같이 표시됩니다. 이러한 취약한 항목에 대해 생성된 새 정정 작업이 정정 작업 탭 (1)에 표시됩니다.

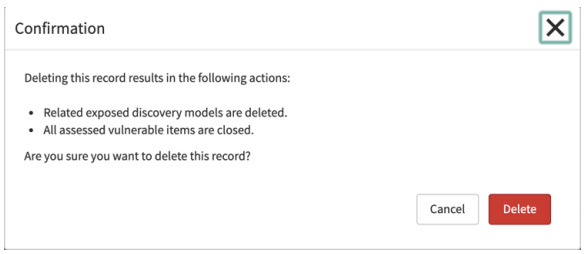
주:
이 예시에서는 취약성이라는 정정 작업 규칙의 그룹 규칙과 조건에 따라 정정 작업이 생성됩니다. 이 그룹 규칙은 인스턴스에 취약성 대응 제품과 ServiceNow AI Platform# 함께 설치되는 기본 정정 작업 규칙입니다. 이 예시에서는 이 그룹 규칙의 조건이 모든 취약한 항목을 단일 정정 작업에 배치했습니다. 노출 평가 검색 결과와 일치하는 취약한 항목에 대해 둘 이상의 정정 작업을 생성하려는 경우 추가 정정 작업 규칙을 설정하는 것이 좋습니다. 정정 작업을 더 많이 생성하면 취약한 항목이 많은 정정 작업이 생성되는 것을 방지할 수 있습니다. 정정 작업 규칙에 대한 자세한 내용은 해당 정정 작업 규칙 생성 또는 편집 취약성 대응문서를 참조하십시오취약성 대응 정정 작업 및 정정 작업 규칙 개요.



9. 계속하려면 하나를 선택합니다.

옵션	설명
정정 작업	정정 작업 탭을 선택한 상태에서, 번호 열에서 기록을 클릭하여 열고 정정 작업을 검토하고 할당합니다. 할당 그룹에 대한 자세한 내용은 다음 문서를 참조하십시오 Creating groups.
평가된 취약성 항목	평가된 취약한 항목 탭을 선택한 상태에서 취약한 항목 열에서 클릭하여 기록을 열고 개별 취약한 항목을 검토하여 할당합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵션	설명
삭제	노출 평가 기록을 삭제합니다. 확인 대화 상자가 표시됩니다. **주:** 취약성 항목을 생성한 후 노출 기록을 삭제하면 다른 노출 기록과 관련이 없는 이 기록에 대해 생성한 모든 취약한 항목이 자동으로 ## 상태로 이동됩니다. 종결 이유가 ###입니다.
	

다음에 수행할 작업
노출 평가에 따라 제로 데이(현재 날짜) 위협에 대응합니다. 의 취약성 대응정정 작업 및 변경 관리에 대한 자세한 내용은 및 을 참조하십시오 취약성 대응 정정 작업 및 정정 작업 규칙 개요를 위한 변경 관리 취약성 대응.

할당 권장 사항 보기

할당 그룹은 일반적으로 할당 규칙을 사용하여 취약한 항목에 할당됩니다. 이러한 규칙은 취약성 관리자가 외부 공급업체 스캐너에서 받은 데이터를 기반으로 올바른 할당 그룹을 할당하도록 구성합니다.

자세한 내용은 취약성 대응 할당 규칙 개요 문서를 참조하십시오. 일치하는 할당 그룹을 사용할 수 없거나 잘못된 경우 을 사용하여 취약점 할당 권장 대체 할당 그룹을 볼 수 있습니다.

다음 작업을 수행하는 데 사용합니다 취약점 할당 권장 .

- 취약한 항목에 대한 할당 그룹 권장 사항 요청.
- 여러 취약한 항목에 대한 할당 그룹 권장 사항 요청.
- 정정 작업에 대한 할당 그룹 권장 사항 요청.

취약한 항목에 대한 할당 그룹 권장 사항 요청

할당 그룹 권장 사항을 볼 수 있도록 요청합니다 취약점 할당 권장 . VI(취약한 항목)에 대해 일치하는 할당 그룹을 사용할 수 없거나 잘못된 경우 권장 사항을 요청할 수 있습니다.

시작하기 전에
필요한 역할: sn_vul.remediation_owner

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 취약 항목 그런 다음 VI를 엽니다.
   항목은 오픈, 연기됨, 조사 중 또는 구현 대기 중 상태여야 합니다.
2. 해당 VI에 대한 할당 제안을 위해 할당 그룹 필드 옆에 있는 권장 아이콘( )을 클릭합니다.
3. 할당 그룹 권장 사항 대화 상자에서 신뢰 점수를 기반으로 하는 권장 사항을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

신뢰 점수는 VI에 대한 일치 항목의 관련성을 예측합니다. 자세한 내용은 용 머신 러닝 솔루션 취약성 대응 문서를 참조하십시오.

4. 할당을 클릭합니다.

결과
선택한 그룹이 할당 그룹 필드에 나타나고 할당 유형이 권장 사항으로 변경됩니다.

여러 취약한 항목에 대한 할당 그룹 권장 사항 요청

대량 편집을 사용하여 여러 VI(취약한 항목)에 대한 할당 그룹 권장 사항을 보는 데 사용합니다 취약점 할당 권장 . 여러 VI를 선택하면 선택한 VI의 무작위 샘플에 대해 예측이 수행됩니다.

시작하기 전에
필요한 역할: sn_vul.remediation_owner

이 태스크 정보
권장 사항과 해당 신뢰도 점수는 선택한 VI에서 가져온 샘플에 따라 발동 간에 약간 다를 수 있습니다. 신뢰 점수는 권장 할당 그룹이 취약성을 해결하는 데 적합하다고 시스템에서 확신하는지 여부를 평가합니다. 대량 편집 옵션을 사용하여 정정 작업(VUL) 및 VI를 요청할 취약점 할당 권장 때 assignment_recommendation_batchsize 시스템 속성을 사용하여 배치 크기를 설정합니다. 이 시스템 속성의 기본값은 최적의 예측 성능을 위해 설정됩니다.

주:
기본값을 늘리면 이러한 케이스에 대한 취약점 할당 권장 응답 시간이 변경될 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 취약한 항목 을 클릭하고 여러 VI를 선택합니다.
   항목은 오픈, 조사 중 또는 구현 대기 중 상태여야 합니다.
2. **Bulk** Edit(벌크 편집)를 클릭합니다.
3. 양식에서 필드를 채웁니다.

대량 취약한 항목 양식

필드	설명
기록 선택	대량 편집을 위해 선택할 기록입니다.
할당 그룹	선택한 취약한 항목에 대해 설정할 할당 그룹입니다. 권장 할당 그룹을 보려면 필드 옆에 있는 권장 아이콘( )을 클릭합니다. 신뢰 점수를 기반으로 하는 권장 사항을 선택하고 할당을 클릭합니다.
작업 메모	추가할 메모입니다.

4. 확인을 클릭합니다.

결과
선택한 그룹이 할당 그룹 필드에 나타나고 할당 유형이 선택한 모든 VI에 대해 권장 사항으로 변경됩니다.

정정 작업에 대한 할당 그룹 권장 사항 요청

정정 작업(VUL)에 대한 할당 그룹 권장 사항을 보는 데 사용합니다 취약점 할당 권장 .

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_vul.remediation_owner

이 태스크 정보
대량 편집 옵션을 사용하여 VUL 및 VI(취약한 항목)를 요청할 취약점 할당 권장 때 assignment_recommendation_batchsize 시스템 속성을 사용하여 배치 크기를 설정합니다. 이 시스템 속성의 기본값은 최적의 예측 성능을 위해 설정됩니다.

주:
기본값을 늘리면 이러한 케이스에 대한 취약점 할당 권장 응답 시간이 변경될 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 정정 작업 을 클릭하고 VUL을 선택합니다.
   그룹은 오픈, 조사 중 또는 구현 대기 중 상태여야 합니다.
2. 선택한 VUL에 대한 할당 그룹 권장 사항에 대한 할당 그룹 필드 옆에 있는 권장 아이콘(.)을 클릭합니다.
   할당 그룹 권장 사항 대화 상자에 해당 그룹의 모든 VI에 대한 평균 신뢰 점수와 함께 권장 할당 그룹이 표시됩니다.
3. 신뢰 점수를 기준으로 할당 그룹 목록에서 권장 사항을 선택합니다.
   신뢰 점수는 선택한 VUL에 대한 일치의 관련성을 예측합니다.
4. 할당을 클릭합니다.
   선택한 그룹이 할당 그룹 필드에 나타납니다.
5. 업데이트된 정보로 정정 작업을 저장합니다.

결과
VUL과 동일한 할당 그룹을 가진 모든 VI가 선택한 할당 그룹에 할당됩니다. 할당 유형이 VUL 및 수정된 모든 VI에 대한 권장 사항으로 변경됩니다.

예외 요청 및 승인

취약한 항목의 정정 또는 정정 작업을 지정된 기간 동안 연기하도록 요청할 수 있습니다. 예를 들어 정정 소유자는 머신에 패치를 사용할 수 없는 경우 예외를 요청할 수 있습니다. 액세스 권한이 있는 승인자는 다른 사용자의 요청을 승인할 수 있습니다.

작업 공간에서 예외를 취약성 대응 요청할 수 있습니다. 에서 예외 요청 IT 정정 작업 공간 문서를 참조하십시오.

- 취약한 항목에 대한 예외 요청
- 정정 작업에 대한 예외 요청
- 대량 예외 요청

다음을 사용하여 GRC: 정책 및 준수 관리정책 예외를 요청할 수도 있습니다.

- 다음을 사용하여 예외 요청 GRC: 정책 및 준수 관리
- 를 사용하여 대량 예외 요청 GRC: 정책 및 준수 관리

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

이메일 알림은 예외 관리의 모든 단계에서 전송되어 요청의 상태 및 기타 세부 정보를 제공합니다. 예를 들어 예외가 요청되면 요청자는 요청이 발생했음을 확인하는 이메일을 받습니다. 또한 승인자는 예외가 요청되었다는 내용의 이메일을 받습니다.

v21.0 부터 취약성 대응설정된 일 수 후에 승인자와 요청자 모두에 대한 이메일 알림과 함께 긍정 오류 및 예외를 승인하기 위한 시간 범위를 구성할 수 있습니다. 요청이 발생하면 취약한 항목이 검토 중 상태로 변경되고 상태 변경 기록이 생성됩니다. 승인자가 구성된 시간 범위 내에 응답하지 않으면 취약한 항목 또는 정정 작업이 열림 상태로 되돌아갑니다. 이전 상태는 **backup_state** 필드에 저장됩니다. 자세한 내용은 예외 관리에 대한 승인 규칙 구성 문서를 참조하십시오.

취약한 항목에 대한 예외 요청

즉시 정정할 수 없는 VI(취약한 항목)에 대한 예외를 요청합니다. 예를 들어 정정 소유자는 머신에 패치를 사용할 수 없는 경우 예외를 요청할 수 있습니다.

시작하기 전에

필요한 역할: sn_vul.remediation_owner

이 태스크 정보

중요사항:
취약성 관리자 및 IT 정정 작업 공간에서 예외를 요청할 수 있습니다. 자세한 내용은 에서 정정 작업 및 기록에 대한 예외 요청 취약성 관리자 작업 공간 및 에서 예외 요청 IT 정정 작업 공간 문서를 참조하십시오.

클래식 환경에서 VI에 대한 예외를 요청할 수도 있습니다.

주:

v21.0 부터 취약성 대응설정된 일 수 후에 승인자와 요청자 모두에 대한 이메일 알림과 함께 긍정 오류 및 예외를 승인하기 위한 시간 범위를 구성할 수 있습니다. 요청이 발생하면 취약한 항목이 검토 중 상태로 변경되고 상태 변경 기록이 생성됩니다. 승인자가 구성된 시간 범위 내에 응답하지 않으면 취약한 항목 또는 정정 작업이 열림 상태로 되돌아갑니다. 이전 상태는 **backup_state** 필드에 저장됩니다. 자세한 내용은 예외 관리에 대한 승인 규칙 구성 문서를 참조하십시오.

프로시저

1. 다음으로 이동 취약성 대응 〉 취약 항목 〉 모두.
2. 예외를 요청할 항목을 선택합니다.
   선택한 항목은 오픈, 조사 중 또는 구현 대기 중 상태여야 합니다.
3. 취약한 항목 양식에서 예외 요청을 클릭합니다.
4. 이 항목을 예외 관리 화면에서 선택한 경우 취약성 대응 예외 요청 양식의 필드에 내용을 입력합니다.

예외 요청 양식

필드	설명
다음까지	예외 요청이 만료되는 날짜입니다. 이 날짜는 에서 선택한 기간 내에 있어야 합니다. 모두 〉 취약성 대응 〉 관리 〉 예외 관리 화면. 예외 요청이 만료되면 그룹은 열림 상태로 되돌아갑니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	주: (VR) 버전 18.0 취약성 대응 부터 예외 관리 기능을 사용하여 취약한 항목의 정정이 지연된 경우 스캐너에서 다시 열 경우 취약성에 설정된 지연 날짜가 계속 유지됩니다. 이 기능을 사용하려면 시스템 속성 *sn_vul.auto_defer_vit_in_active_exception_win* 값을 true로 설정합니다. 또한 지연된 종료 날짜는 취약한 항목이 종결되거나 예외가 만료된 후에도 유지됩니다. 필요한 역할은 읽기와 쓰기 모두에 대해 sn_vul.manage_exception_configuration입니다.
이유	요청 이유입니다. 선택 항목은 다음과 같습니다. ○ 위험 수락됨 ○ 유지관리 기간을 기다리는 중 ○ 수정 사용 불가 ○ 사용 중인 완화 통제 ○ 기타 새 이유 선택 항목을 추가하는 방법을 보려면 다음 문서를 참조하십시오 정책 사유 매핑 정의.
추가 정보	이 요청이 수행되는 이유와 관련된 상세 정보입니다. 이 필수 필드는 정정 소유자가 업데이트해야 합니다.

5. Request Approval을 클릭하여 예외 요청을 제출합니다.

결과
취약한 항목의 상태가 검토 중으로 변경됩니다. 상태 변경 승인 탭을 사용하여 예외 요청의 상태를 추적합니다.

정정 작업에 대한 예외 요청

즉시 해결할 수 없는 경우 지정된 기간 동안 정정 작업을 연기하는 예외를 요청합니다.

시작하기 전에

중요사항:

취약성 관리자 및 IT 정정 작업 공간에서 예외를 요청할 수 있습니다. 에서 예외 요청 IT 정정 작업 공간 문서를 참조하십시오.

가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

필요한 역할: sn_vul.remediation_owner

클래식 환경의 정정 작업에 대한 예외를 요청할 수도 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 정정 작업 〉 모두.
2. 예외를 요청할 그룹을 선택합니다.
   선택한 작업은 오픈, 조사 중 또는 구현 대기 중 상태여야 합니다.
3. 정정 작업 기록(VUL)에서 예외 요청을 선택합니다.
4. 양식에서 필드를 채웁니다.

예외 요청 양식

필드	설명
다음까지	예외 요청이 만료되는 날짜입니다. 이 날짜는 구성에 정의된 예외 기간 내에 있어야 합니다.
이유	예외 요청에 대한 근거입니다.
추가 정보	이 요청이 수행되는 이유와 관련된 상세 정보입니다. 이 필드는 정정 소유자가 업데이트해야 합니다.

5. 승인 요청을 클릭합니다.

대량 예외 요청

대량 편집 옵션을 사용하여 각 항목을 수동으로 선택하는 대신 여러 취약한 항목(VIT)에 대한 예외를 요청합니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_analyst

이 태스크 정보
여러 VIT를 선택하면 이러한 항목으로 정정 작업(VUL)이 형성됩니다. 여러 VIT 편집에 대한 자세한 내용은 을 참조하십시오 에서 취약한 항목을 대량으로 편집 취약성 대응 .

중요사항:
다음에 대한 예외를 요청할 수 있습니다.

- 에서 VIT 취약성 관리자 작업 공간 및 IT 정정 작업 공간. 자세한 내용은 에서 예외 요청 IT 정정 작업 공간 문서를 참조하십시오.
- 의 여러 VIT 취약성 관리자 작업 공간. 자세한 내용은 취약성 관리자 작업 공간에서 대량 예외 요청 문서를 참조하십시오.

프로시저

1. 다음으로 이동 취약성 대응 〉 취약 항목 〉 모두 을 클릭하고 예외를 요청할 항목을 선택합니다.
   선택한 항목은 오픈, 조사 중 또는 구현 대기 중 상태여야 합니다.
2. **Bulk** Edit(벌크 편집)를 클릭합니다.
3. 양식에서 필드를 채웁니다.

취약한 항목 일괄 편집 양식

필드	설명
기록 선택	대량 편집을 위해 선택한 기록입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
상태	취약한 항목의 상태입니다. 선택한 항목에 대한 예외를 요청하려면 연기됨 상태를 선택합니다.
이유	선택한 상태의 하위 상태입니다.
간단한 설명	생성 중인 정정 작업의 이름입니다.
다음까지	예외 요청에 대해 지정한 종료 날짜입니다.
추가 정보	승인자에게 요청 이유를 알리기 위해 언급할 추가 상세 정보입니다.
기본 솔루션	대량 편집을 위해 선택한 모든 취약한 항목을 정정하기 위한 대상 솔루션입니다.
할당 그룹	VI에 대한 할당 그룹입니다. 그룹을 수동으로 선택하거나 해당 기능이 활성화된 경우 할당 권장 사항을 사용할 수 있습니다.
작업 메모	추가할 메모입니다.

4. 확인을 클릭합니다.
   선택한 VI를 포함하는 정정 작업이 생성됩니다. 이 정정 작업은 승인을 위해 제출됩니다.

다음을 사용하여 예외 요청 **GRC:** 정책 및 준수 관리

에서 애플리케이션의 취약성 대응정책 예외 관리 기능을 정책 및 준수 관리 사용하여 GRC 정책 예외를 요청합니다.

시작하기 전에
정책 예외 통합을 사용하여 정책 예외를 요청하려면 먼저 에서 ServiceNow Store애플리케이션을 다운로드 GRC: 정책 및 준수 관리 해야 합니다.

필요한 역할: sn_vul.remediation_owner

클래식 UI에서 예외를 요청할 수도 있습니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 취약 항목 (또는 정정 작업)〉모두로 설정하고 예외를 요청할 항목 또는 그룹을 엽니다.
   선택한 항목 또는 그룹은 오픈, 조사 중 또는 구현 대기 중 상태여야 합니다.
2. 선택한 양식에서 예외 요청을 클릭합니다.
3. 양식에서 필드를 채웁니다.

예외 요청 양식

필드	설명
정책	예외를 요청하는 취약성 관리 정책입니다.
컨트롤 목적	선택한 정책과 연결된 통제 목표입니다. 정책을 선택하지 않으면 모든 통제 목표가 나열됩니다.
유효 기간(시작)	예외가 시작되는 날짜입니다. 기본값은 현재 날짜입니다. 이 날짜는 과거일 수 없습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
유효 기간	정책 예외가 만료되고 취약한 항목 또는 그룹의 상태가 연기됨에서 미결로 변경되는 날짜입니다. 주: 정책 예외가 유효한 일 수는 정책 및 준수에서 정책에 대해 설정한 최대 예외 기간(일) 을 초과할 수 없습니다. 자세한 내용은 정책 만들기를 참조하세요.
이유	예외를 요청하는 이유입니다.
근거	이 요청이 수행되는 이유와 관련된 상세 정보입니다. 이 필수 필드는 정정 소유자가 입력해야 합니다.

4. 제출을 클릭합니다.
   정책 예외 통합 및 정정 소유자와 준수 관리자 간의 핸드오프에 대한 자세한 내용은 정책 및 준수 관리 선택적 설정을 참조하십시오.

를 사용하여 대량 예외 요청 **GRC:** 정책 및 준수 관리

취약한 항목 그룹을 선택하고 대량 예외를 제출합니다.

시작하기 전에
정책 예외 통합을 사용하여 대량 예외를 요청하려면 먼저 에서 ServiceNow Store애플리케이션을 다운로드 GRC: 정책 및 준수 관리 해야 합니다.

주:
이 기능을 사용하려면 업그레이드취약성 대응하기 전에 업그레이드 GRC: 정책 및 준수 관리 해야 합니다. 이전에 GRC: 정책 및 준수 관리이미 업그레이드 취약성 대응 한 경우 이 기능을 사용하려면 업그레이드 절차를 올바른 순서로 다시 수행해야 합니다.

가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

필요한 역할: sn_vul.remediation_owner

의 클래식 환경에서 취약성 대응예외를 요청할 수도 있습니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 취약 항목 〉 모두 을 클릭하고 예외를 요청할 항목을 선택합니다.
   선택한 항목은 오픈, 조사 중 또는 구현 대기 중 상태여야 합니다.
2. **Bulk** Edit(벌크 편집)를 클릭합니다.
3. 양식에서 필드를 채웁니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약한 항목 일괄 편집 양식

필드	설명
기록 선택	대량 편집을 위해 선택한 기록입니다.
상태	취약한 항목의 상태입니다. 선택한 항목에 대한 예외를 요청하려면 연기됨 상태를 선택합니다.
간단한 설명	생성 중인 작업의 이름입니다.
기본 솔루션	대량 편집을 위해 선택한 모든 취약한 항목을 정정하기 위해 대상으로 하는 솔루션입니다.
할당 그룹	VI에 대한 할당 그룹입니다. 그룹을 수동으로 선택하거나 해당 기능이 활성화된 경우 할당 권장 사항을 사용할 수 있습니다.
작업 메모	추가할 메모입니다.

4. 확인을 클릭합니다.
   선택한 취약한 항목을 사용하여 정정 작업이 생성됩니다.
5. 양식에서 필드를 채웁니다.

예외 요청 양식

필드	설명
정책	예외를 요청하는 취약성 관리 정책입니다.
컨트롤 목적	선택한 정책과 연결된 통제 목표입니다. 정책을 선택하지 않으면 모든 통제 목표가 나열됩니다.
유효 기간(시작)	예외가 시작되는 날짜입니다. 기본값은 현재 날짜입니다. 이 날짜는 과거일 수 없습니다.
유효 기간	정책 예외가 만료되고 취약한 항목 또는 그룹의 상태가 연기됨에서 미결로 변경되는 날짜입니다. **주:** 정책 예외가 유효한 일수는 에서 GRC: 정책 및 준수 관리정책에 대해 설정한 최대 예외 기간(일)을 초과할 수 없습니다. 자세한 내용은 정책 만들기를 참조하세요.
이유	예외를 요청하는 이유입니다.
근거	이 요청이 수행되는 이유와 관련된 상세 정보입니다. 이 필수 필드는 정정 소유자가 입력해야 합니다.

6. 제출을 클릭합니다.
   정책 예외 통합 및 정정 소유자와 준수 관리자 간의 핸드오프에 대한 자세한 내용은 정책 및 준수 관리 선택적 설정을 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

에서 예외 요청 승인 또는 거부 취약성 대응

즉시 정정할 수 없는 취약한 항목 또는 정정 작업에 대한 예외 요청을 승인하거나 거부합니다. 이러한 위험 요청을 평가한 다음 정정할 수 있을 때까지 연기하도록 승인해야 합니다.

중요사항:

에서 예외 요청을 승인하거나 거부할 수 있습니다 취약성 관리자 작업 공간.

시작하기 전에
필요한 역할: sn_vul.exception_approver
클래식 환경에서도 예외 요청을 승인할 수 있습니다.

주:

v21.0 부터 취약성 대응설정된 일 수 후에 승인자와 요청자 모두에 대한 이메일 알림과 함께 긍정 오류 및 예외를 승인하기 위한 시간 범위를 구성할 수 있습니다. 요청이 발생하면 취약한 항목이 검토 중 상태로 변경되고 상태 변경 기록이 생성됩니다. 승인자가 구성된 시간 범위 내에 응답하지 않으면 취약한 항목 또는 정정 작업이 열림 상태로 되돌아갑니다. 이전 상태는 **backup_state** 필드에 저장됩니다. 자세한 내용은 예외 관리에 대한 승인 규칙 구성 문서를 참조하십시오.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 내 승인.
2. 큐에서 요청을 선택합니다.
3. 적절한 설명을 사용하여 요청을 승인하거나 거부합니다.

예외 규칙 작업

즉시 수정하거나 연기할 수 없는 취약성, VI(취약한 항목) 또는 CI(구성 항목)에 대한 예외를 요청할 수 있습니다. VI 지연 프로세스를 자동화하면 시스템에서 일치하는 VI를 식별할 때 규칙에 따라 해당 VI를 지연시킬 수 있습니다.

예외 규칙에 대해 다음 작업을 수행할 수 있습니다.

- 예외 규칙 생성
- 예외 규칙 요청 승인
- 예외 규칙 활성화
- 예외 규칙 다시 열기
- 승인된 예외 규칙 업데이트
- 예외 규칙 삭제

주:

v21.0 부터 취약성 대응설정된 일 수 후에 승인자와 요청자 모두에 대한 이메일 알림과 함께 긍정 오류 및 예외를 승인하기 위한 시간 범위를 구성할 수 있습니다. 요청이 발생하면 취약한 항목이 검토 중 상태로 변경되고 상태 변경 기록이 생성됩니다. 승인자가 구성된 시간 범위 내에 응답하지 않으면 취약한 항목 또는 정정 작업이 열림 상태로 되돌아갑니다. 이전 상태는 **backup_state** 필드에 저장됩니다. 자세한 내용은 예외 관리에 대한 승인 규칙 구성 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예외 규칙 생성

취약한 항목(VI) 그룹의 특정 조건에 대한 예외를 자동으로 요청하는 규칙(예: 이러한 VI의 취약성 심각도를 기반으로 하는 조건이 있는 규칙)을 생성합니다. 이 규칙을 사용하면 승인된 규칙 조건과 일치하는 경우 신규 및 기존 VI를 자동으로 연기할 수 있습니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin

이 태스크 정보
규칙은 "유효 기간(시작)"부터 "유효 기간(종료)" 날짜까지 적용됩니다. 규칙이 승인되면 정정 작업(VUL)이 생성됩니다. 이 VUL의 그룹화 방법을 예외 규칙이라고 합니다. VUL은 Deferred(연기됨) 상태로 생성됩니다. 이 VUL을 닫거나, 다시 열거나, 삭제할 수 없습니다. 신규 및 재개된 VI는 "유효 기간(시작)" 날짜부터 그룹이 "유효 기간(종료)" 날짜에 만료될 때까지 연기되고 이 VUL에 추가됩니다.

주:

이메일 알림은 예외 규칙 워크플로우의 모든 단계에서 전송됩니다. 이러한 이메일은 요청의 상태 및 기타 세부 정보를 제공합니다. 예를 들어 예외 규칙이 요청되면 요청자는 요청이 제출되었음을 확인하는 이메일을 받습니다.

주:
규칙이 거부되면 초안 상태에서 다시 열고 업데이트한 다음 승인을 위해 다시 제출할 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 예외 규칙.
2. 예외 규칙 새 기록 페이지에서 새로 만들기를 클릭하여 규칙을 생성합니다.
3. 양식에서 필드를 채웁니다.

예외 규칙 양식

필드	설명
이름	예외 규칙의 이름입니다.
유효 기간(시작)	VI를 연기하기 위해 이 규칙이 활성화되는 날짜입니다.
유효 기간(종료)	정정 작업에서 새 VI 수락을 중지하는 날짜입니다.
이유	이 예외 규칙을 생성하는 이유입니다.
할당 그룹	지연된 VI를 추적하기 위해 생성된 정정 작업이 할당된 그룹입니다.
추가 정보	요청자가 승인자에게 제공하려는 추가 정보입니다. 이 정보는 정정 작업의 설명 필드에 채워집니다.
조건	VI를 처리하는 동안 정의할 수 있는 VI에 대한 필터 조건입니다.
기존 데이터에서 실행	이 규칙을 처음 실행할 때 기존 데이터에 대해 이 규칙을 실행할 수 있도록 하는 옵션입니다.
워크플로우 스테이지	예외 규칙의 현재 승인 상태입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
상태	예외 규칙의 상태입니다.
실행 순서	각 예외 규칙에 대한 고유한 순서입니다.
지연 기한	VUL 및 VI가 지연될 때까지의 날짜입니다. 이 날짜에 생성된 VUL이 종결되고 모든 VI가 그룹 밖으로 이동하며 그룹 규칙이 다시 적용됩니다.

4. 규칙을 생성할 때 할당 그룹을 추가합니다.
5. 승인을 위해 양식을 제출합니다.
   요청 상태가 검토 중으로 변경됩니다. 예외 규칙을 제출할 때까지는 초안 상태로 유지됩니다.

예외 규칙 요청 승인

이러한 요청을 승인하거나 거부할 수 있도록 사용자의 예외 규칙 요청을 평가합니다.

시작하기 전에

필요한 역할: sn_vul.exception_approver

이 태스크 정보

예외 승인자 수준 1 사용자 그룹 구성원은 수준 1 예외 규칙 요청을 승인할 수 있습니다. 마찬가지로 예외 승인자 수준 2 사용자 그룹 구성원은 수준 2 예외 규칙 요청을 승인할 수 있습니다. 두 사용자 그룹 모두 기본적으로 예외 승인자 역할을 상속합니다.

주:

VR 애플리케이션을 처음 배포하는 경우에는 예외 관리용 플로우 디자이너가 기본적으로 활성화되어 있습니다. 워크플로우를 이미 사용 중인 경우 플로우 디자이너로 업데이트할 수 있습니다. 두 경우 모두 다시 워크플로우로 변경할 수 없습니다. 예외 관리 및 가양성에 대한 승인 규칙을 구성하려면 문서를 참조하십시오 예외 관리에 대한 승인 규칙 구성.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 내 승인.
2. 큐에서 요청을 선택합니다.
3. 를 사용하여 요청을 승인 또는 거부하고 요청을 승인하거나 거부한 이유를 설명합니다.
   예외 규칙이 승인되면 기본적으로 지연 상태로 정정 작업(RT)이 생성됩니다. "유효 기간(시작)" 날짜부터 이 규칙은 생성된 모든 VI와 종결 상태에서 오픈 상태로 전환된 VI에서 실행됩니다. 정의된 조건과 일치하는 VI는 RT에 추가되고 지정된 기간 동안 지연됩니다.

   주:
   규칙이 거부되면 초안 상태에서 다시 열고 업데이트한 다음 승인을 위해 다시 제출할 수 있습니다.

예외 규칙 활성화

규칙은 "유효 기간(시작)" 날짜에 활성화됩니다. 활성화 후에는 취약한 항목(VI)에 대한 예외 프로세스를 자동화합니다.

예외 규칙은 다음 수명주기를 따릅니다.

1. 생성하거나 다시 열고 지정된 조건을 충족하는 새로운 취약한 항목(VI)이 지연됩니다. 예외 규칙을 처음 실행할 때 기존 데이터에서 실행 옵션을 활성화하면 예외 규칙 조건과 일치하는 모든 활성 및 지연되지 않은 VI가 새로 생성된 정정 작업(RT)으로 이동되고 상태가 지연됨으로 변경됩니다.
2. 새로 생성된 VI가 예외 규칙 조건과 일치하면 규칙과 연결된 디퍼드 RT로 이동되고 그룹 규칙이 실행되지 않습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. "유효 기간(시작)" 날짜에 기존 데이터에서 실행 옵션을 활성화하면 기존 VI가 추가됩니다.
4. RT는 규칙이 "유효 기간(Valid to)" 날짜에 만료되면 새로운 VI 수락을 중지합니다. RT는 "연기됨" 날짜까지 존재합니다.
5. 예외 규칙은 "유효 기간(종료)" 날짜에 만료됩니다.

예외 규칙에 대한 연장 요청

지연된 예외 규칙이 기한까지 지연되기 전에 해당 규칙의 연장을 요청합니다. 정정 소유자는 더 이상 이 요청을 하기 위해 지연된 기한까지 기다릴 필요가 없습니다.

시작하기 전에

필요한 역할: sn_vul.exception_approver

이 태스크 정보

작업 공간에서 연장을 취약성 대응 요청할 수도 있습니다. 자세한 내용은 취약성 관리자 작업 공간에서 지연된 취약한 항목에 대한 연장 요청 문서를 참조하십시오.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 예외 규칙.
2. 승인된 예외 규칙을 선택합니다.
3. 연장 요청을 선택합니다.
4. 양식의 필드에 적절히 입력합니다.

필드	설명
연장 날짜	예외 규칙을 연장해야 하는 종료 날짜를 선택합니다.
이유	예외 규칙을 지연시키는 이유를 입력합니다. 선택 항목은 다음과 같습니다. ○ 수용된 위험 ○ 유지관리 기간을 기다리는 중 ○ 수정 사용 불가 ○ 사용 중인 완화 통제 ○ 기타
추가 정보	기타 관련 정보를 입력합니다.

5. 승인 요청을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

요청이 승인되면 예외 규칙과 관련 정정 작업 및 취약한 항목에 대해 지연 기한, 이유 및 추가 정보 필드가 업데이트됩니다. 요청 제출 및 승인자의 후속 조치 시에도 이메일이 트리거됩니다.

주:

- 요청은 두 가지 수준의 승인을 거칩니다.
- 연장 요청 버튼은 예외 규칙의 일부로 생성된 정정 작업에 사용할 수 없습니다.
- 지연된 예외 규칙이 다시 확장되면 백엔드에서 연장 지연 수가 증가합니다.
- v21.0 부터 취약성 대응설정된 일 수 후에 승인자와 요청자 모두에 대한 이메일 알림과 함께 긍정 오류 및 예외를 승인하기 위한 시간 범위를 구성할 수 있습니다. 요청이 발생하면 취약한 항목이 검토 중 상태로 변경되고 상태 변경 기록이 생성됩니다. 승인자가 구성된 시간 범위 내에 응답하지 않으면 취약한 항목 또는 정정 작업이 열림 상태로 되돌아갑니다. 이전 상태는 **backup_state** 필드에 저장됩니다. 자세한 내용은 예외 관리에 대한 승인 규칙 구성 문서를 참조하십시오.

예외 규칙 다시 열기

거부되었지만 다시 제출하려는 예외 규칙을 다시 엽니다. 규칙을 다시 열면 초안 상태로 이동합니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin

이 태스크 정보
그런 다음 승인을 위해 규칙을 업데이트하고 다시 제출할 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 예외 규칙.
2. 다시 열려는 규칙을 찾아 다시 열기를 클릭합니다.
3. 승인을 위해 양식을 업데이트하고 다시 제출합니다.

승인된 예외 규칙 업데이트

승인된 규칙을 업데이트하려면 취소합니다. 예를 들어 날짜를 수정하거나 승인된 규칙에 조건을 추가하려면 먼저 정정 작업(VUL)이 삭제되고 취약한 항목(VI)이 오픈 상태로 이동하도록 취소해야 합니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin

이 태스크 정보
그룹 규칙은 이러한 VI에 다시 적용됩니다. 승인 프로세스를 다시 거치도록 변경 후 규칙을 제출합니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 예외 규칙.
2. 취소하려는 예외 규칙을 열고 취소를 클릭합니다.
3. 규칙 취소(Cancel Rule) 대화 상자에서 규칙 취소**(Cancel rule)**를 클릭합니다.
   규칙이 초안 상태로 다시 이동하고 연결된 VUL이 삭제됩니다. 관련 VI가 다시 열리고 그룹 규칙이 개별 VI에 적용됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예외 규칙 삭제

더 이상 필요하지 않은 예외 규칙을 삭제합니다. 예를 들어 수집 중에 VI(취약한 항목)를 지연하지 않으려면 규칙을 삭제할 수 있습니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin

이 태스크 정보
규칙을 삭제하면 연결된 정정 작업(VUL)이 취소됩니다. 관련 VI가 다시 열리고 그룹 규칙이 개별 VI에 적용됩니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 예외 규칙.
2. 삭제하려는 예외 규칙을 열고 삭제를 클릭합니다.
3. Delete Rule(규칙 삭제) 대화 상자에서 **Delete** rule(규칙 삭제)을 클릭하여 선택한 규칙을 삭제합니다.
   연결된 정정 작업도 삭제됩니다. 관련 VI가 다시 열리고 그룹 규칙이 개별 VI에 적용됩니다.

긍정 오류 표시 및 승인

취약한 항목(VI) 및 정정 작업(VUL)은 가양성으로 표시될 수 있습니다. 쓰기 권한이 있는 승인자는 다른 사용자의 이러한 요청을 승인할 수 있습니다.

- 긍정 오류로 표시
- 긍정 오류에 대한 대량 편집
- 긍정 오류 승인 또는 거부

주:

이메일 알림은 가양성 워크플로우의 모든 단계에서 전송되어 요청의 상태 및 기타 세부 정보를 제공합니다. 예를 들어 VI 또는 정정 작업이 긍정 오류로 표시되면 요청자는 확인 이메일을 받게 됩니다. 이와 동시에 승인자는 VI 또는 정정 작업이 긍정 오류로 표시되었다는 내용의 이메일을 받습니다.

v21.0 부터 취약성 대응설정된 일 수 후에 승인자와 요청자 모두에 대한 이메일 알림과 함께 긍정 오류 및 예외를 승인하기 위한 시간 범위를 구성할 수 있습니다. 요청이 발생하면 취약한 항목이 검토 중 상태로 변경되고 상태 변경 기록이 생성됩니다. 승인자가 구성된 시간 범위 내에 응답하지 않으면 취약한 항목 또는 정정 작업이 열림 상태로 되돌아갑니다. 이전 상태는 **backup_state** 필드에 저장됩니다. 자세한 내용은 예외 관리에 대한 승인 규칙 구성 문서를 참조하십시오.

긍정 오류로 표시

스캐너에서 제공한 경고가 실제로 문제가 아닌 경우 VI(취약한 항목) 또는 VUL(정정 작업)을 가양성으로 표시합니다. 예를 들어 구성 항목이 해제되었지만 스캐너에서 여전히 이와 관련된 문제를 제기하는 경우 이를 가양성으로 표시합니다.

시작하기 전에
필요한 역할: 정정 소유자
작업 공간에서 긍정 취약성 대응 오류를 요청할 수 있습니다. 취약한 항목 또는 정정 작업에 대한 가양성 요청 문서를 참조하십시오.

클래식 환경에서 가양성을 요청할 수도 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 취약성 대응 〉 취약한 항목(또는 정정 작업) 〉 모두.
2. 긍정 오류로 표시할 VI 또는 VUL을 열고 긍정 오류로 표시를 클릭합니다.
   VI 또는 VUL은 열림 상태여야 합니다.
3. False Positive(긍정 오류) 양식에서 **Additional** information(추가 정보)에 세부 정보를 입력하고 **Request** Approval(승인 요청)을 클릭합니다.
   승인을 위해 요청이 전송되고 VI 또는 VUL의 상태가 검토 중으로 변경됩니다.

긍정 오류에 대한 대량 편집

대량 편집을 사용하여 여러 취약한 항목(VIT)을 긍정 오류로 표시합니다. 여러 VIT를 선택하면 이러한 항목으로 정정 작업이 형성됩니다.

> **중요사항:**
> 관리자 또는 분석가는 취약성 관리자 작업 공간의 대량 편집 기능을 사용하여 여러 VIT를 가양성으로 표시할 수 있습니다. 자세한 내용은 취약성 관리자 작업 공간에서 가양성에 대한 대량 편집 문서를 참조하십시오.

시작하기 전에
필요한 역할: 정정 소유자
가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

클래식 환경에서 가양성을 요청할 수도 있습니다.

프로시저

1. 다음으로 이동 취약성 대응 〉 취약 항목 〉 모두 을 클릭하고 긍정 오류로 표시할 항목을 선택합니다.
   선택한 항목은 오픈, 조사 중 또는 구현 대기 중 상태여야 합니다.
2. **Bulk** Edit(벌크 편집)를 클릭합니다.
3. 양식에서 필드를 채웁니다.

취약한 항목 일괄 편집 양식

필드	설명
기록 선택	대량 편집을 위해 선택할 기록입니다.
상태	취약한 항목의 상태입니다. 긍정 오류로 표시하려면 종결됨을 선택합니다.
이유	선택한 상태의 하위 상태입니다. 상태를 종결로 선택한 경우 여기에서 긍정 오류를 선택하여 긍정 오류로 표시합니다.
할당 해제	할당 대상 및 할당 그룹 필드를 지우는 요청을 제출합니다.
기본 솔루션	대량 편집을 위해 선택된 모든 취약한 항목을 정정하기 위한 대상 솔루션입니다.
할당 그룹	VI에 대한 할당 그룹입니다. 수동으로 선택하거나 할당 권장 사항(활성화된 경우)을 사용합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
작업 메모	추가할 메모입니다.

4. 확인을 클릭합니다.
   선택한 VI를 포함하는 새 정정 작업이 생성되고 이 작업은 승인을 위해 전송됩니다.

긍정 오류 승인 또는 거부

거짓 양성 승인자는 다른 사용자의 거짓 양성 요청을 승인하거나 거부할 수 있습니다.

중요사항:

거짓 긍정 승인자는 에서 긍정 오류 요청을 승인하거나 거부할 수 있습니다 취약성 관리자 작업 공간.

시작하기 전에
필요한 역할:

- 취약한 항목에 대한 sn_vul.false_positive_approver
- 애플리케이션 취약한 항목에 대한 sn_vul.app_false_positive_approver

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 취약성 〉 내 승인.
2. 큐에서 요청을 선택합니다.
3. 적절한 설명을 사용하여 요청을 승인하거나 거부합니다.

주:
거짓 긍정은 시간 제한이 있을 수 있습니다. 승인자만 종료 날짜를 설정할 수 있습니다.

취약성 대응용 **Analytics and Reporting** 솔루션

취약성 정정 모니터링에는 추세 보기, 위험 관리 및 할당 그룹 모니터링이 포함됩니다. 높은 위험 문제, 할당 그룹 작업 부하, 지연 및 반복되는 취약성을 검토할 수 있습니다. 취약성 대응 는 해당 프로세스의 생산성과 효율성을 높이기 위한 도구, 보고서 및 절차를 제공합니다.

작업 공간의 데이터 시각화 취약성 대응

작업 공간에는 취약성 대응 정정 진행 상황을 모니터링하는 데 도움이 될 수 있는 데이터 시각화가 포함되어 있습니다. 취약성 데이터가 변경될 때 업데이트되는 동적 데이터 시각화에서 조직에 중요한 활성 취약성의 수와 심각도를 확인하여 조직에 대한 위협 수준을 확인할 수 있습니다. 사용 가능한 동적 데이터 시각화에 대한 자세한 내용은 을 IT 정정 작업 공간 살펴보기 참조하십시오취약성 관리자 작업 공간.

취약성 분석가는 다음에서 기본 취약성 대응 대시보드를 사용할 수도 있습니다. 모두 〉 취약성 대응 〉 개요.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

중요사항:

의 취약성 대응버전 19.0부터 이 대시보드는 New Experience UI에서도 볼 수 있습니다. 새 UI에서 대시보드를 보려면 다음으로 이동합니다. 작업 공간 〉 취약성 관리자 작업 공간 을 클릭하고 대시보드 아이콘을 클릭합니다. 역할에 따라 기본 대시보드가 표시됩니다. 다른 대시보드를 보려면 대시보드 이름 옆에 있는 드롭다운을 클릭합니다. 자세한 내용은 취약성 관리자 작업 공간의 대시보드 및 IT 정정 작업 공간의 대시보드를 참조하십시오.

주:
Tokyo에 있는 경우 Next Experience UI에서 대시보드를 볼 수 있지만 일부 기능 손실이 있습니다.

취약성 대응 정정 프로세스

대부분의 취약성 정정은 작업 공간 내의 정정 작업 기록에서 취약성 대응 수행됩니다. 조사 중 상태의 정정 작업(RT)에서 여러 작업을 수행할 수 있습니다.

- 변경 요청을 생성합니다.
- 정정 작업 내의 취약성에 대한 작업 메모 및 설명을 추가합니다.
- 정정 작업과 그 안에 있는 취약한 항목을 나중으로 연기합니다.
- 정정 작업을 닫습니다.
- 일반적으로 시간에 민감한 새로운 규정 준수 의무를 추적합니다.

- 취약성 대응 인스턴스에 로그인합니다.
- 취약성 관리와 타사 대시보드 및 보고서를 검토하여 문제 영역을 찾습니다. 예를 들어 상태별 정정 작업(RT) 에이징 또는 정정 목표 날짜가 지난 고위험 VI(취약한 항목)를 보여주는 대시보드를 볼 수 있습니다.
- 위험 순서대로 정정 작업의 상태를 검토합니다.
- 위험 점수가 올바르게 계산되지 않는 경우 위험 점수 계산기를 조정하거나 필요에 따라 VI 또는 RT를 연기하여 작업의 우선순위를 수정합니다. 이러한 옵션에 대한 자세한 내용은 또는 정정 작업 연기 을 참조하십시오취약성 대응 계산기 및 취약성 계산기 규칙.
- 재개하려고 하는 지연된 취약한 항목을 검토하고 필요에 따라 추가 조치를 취합니다. 자산, 정정 작업 및 해당 취약한 항목에 대한 변경 활동을 시작하고 추적하려면 자세한 내용은 에서 를 위한 변경 관리 취약성 대응추가 작업을 참조하십시오.
- IT 운영팀의 피드백을 검토합니다.

  변경 요청이 해결되었다는 알림을 받으면 다음 스캔을 기다립니다. 스캔은 설정 도우미에 구성된 외부 공급업체 임포트 일정에 의해 자동으로 트리거됩니다.

- 스캔 후 상태가 수정이면 임포트하는 동안 취약한 항목이 자동으로 종결됩니다. 그룹의 모든 취약한 항목이 해결되면 그룹이 닫힙니다.
- 스캔 후 상태가 수정이 아닌 경우 VI는 자동으로 조사 중으로 다시 이동합니다.

- 인스턴스에서 "해결됨"으로 설정되었지만 외부 공급업체 통합 실행에 의해 "종결/수정됨"으로 전환되지 않은 취약한 항목은 재스캔 중에 탐지되면 다시 열립니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

탐지의 경우 Qualys , 스캐너가 '해결됨'으로 설정되었지만 후속 스캔에서 '종결/수정됨'으로 전환되지 않은 VI를 계속 찾으면 마지막으로 발견된 날짜가 해결 날짜보다 나중일 때 이러한 VI가 다시 '오픈'으로 이동합니다.

감지의 경우 Rapid7 , 이제 인스턴스의 구성 페이지에서 해결된 VI를 기간별로 다시 열 수 있는 옵션을 사용할 수 Rapid7 있습니다. 활성화된 경우 VI가 '해결됨'으로 설정되었지만 후속 스캔에서 '종결/수정됨'으로 전환되지 않은 경우 입력한 일수 후에 다시 '오픈'으로 전환됩니다.

취약성 솔루션 관리 배포 진행률

정정 작업 및 취약성 항목에 대한 포괄적인 배포 메트릭은 취약성, 취약한 항목의 정정 상태 아래에 포함되어 취약성 솔루션 관리 있습니다. 해결 진행을 느리게 하는 정정 작업 또는 취약성을 쉽게 식별합니다. 취약성을 식별하는 방법 또는 영향을 받는 자산의 어떤 측면이 정정 문제를 일으킬 수 있는지 드릴다운합니다. 취약성, 솔루션 및 정정 작업 양식에서 상태 업데이트 관련 링크를 사용하여 메트릭 상태를 업데이트합니다.

기본 취약성 대응 대시보드 사용

개요 대시보드(취약성 관리)는 취약성 대응 취약성 및 취약한 항목에 대한 경영진 뷰를 제공하여 취약성 관리자가 관심 영역을 신속하게 찾아낼 수 있도록 도와줍니다. 정정 대시보드(취약성 정정)를 취약성 대응 통해 정정 전문가는 자신이 소유한 정정 작업 및 취약한 항목에 집중할 수 있습니다.

작업 공간의 데이터 시각화 취약성 대응

작업 공간에는 취약성 대응 정정 진행 상황을 모니터링하는 데 도움이 될 수 있는 데이터 시각화가 포함되어 있습니다. 취약성 데이터가 변경될 때 업데이트되는 동적 데이터 시각화에서 조직에 중요한 활성 취약성의 수와 심각도를 확인하여 조직에 대한 위협 수준을 확인할 수 있습니다. 취약성 관리자 작업 공간IT 정정 작업 공간 살펴보기 를 참조취약성 대응 작업 공간하고 사용 가능한 동적 데이터 시각화에 대한 자세한 내용을 확인할 수 있습니다.

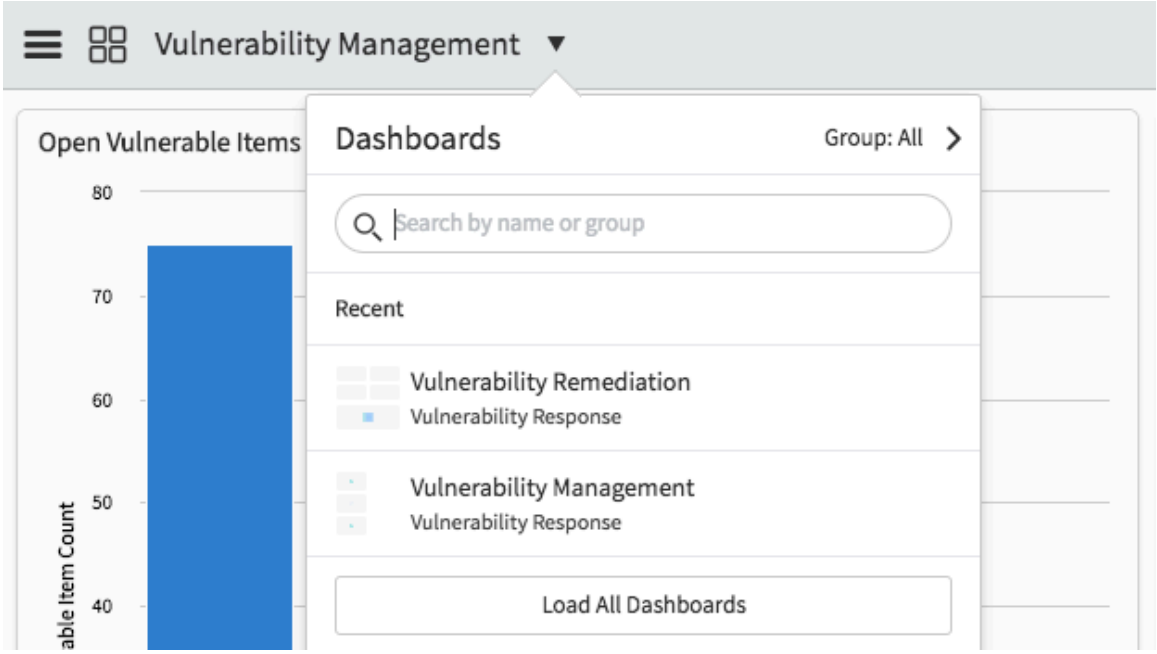
취약성 분석가도 기본 취약성 대응 대시보드를 사용할 수 있습니다.

필요한 역할: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst, sn_vul.vulnerability_read 또는 sn_vul.vulnerability_read 역할을 상속하는 사용자), pa_viewer.

레거시 환경의 기본 취약성 대응 대시보드

이러한 보고서는 애플리케이션의 일부로 취약성 대응용 퍼포먼스 분석 포함되며 별도의 구독이 필요하지 않습니다. 하나를 열려면 선택 목록을 선택하여 확장하고 대시보드를 선택합니다. 또는 검색 필드에 대시보드의 이름을 입력합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



주:

애플리케이션용 취약성 대응 컨텐츠 팩이 퍼포먼스 분석 설치되고 활성화되면 취약성 관리(PA) 대시보드가 개요 모듈에 자동으로 표시됩니다. 이 대시보드에는 취약성 관리 수명주기의 모든 단계를 다루는 보고서가 포함되어 있습니다.

용 취약성 대응퍼포먼스 분석 컨텐츠 팩에 포함된 보고서에 대한 자세한 내용은 취약성 관리 〔PA〕 대시보드를 참조하십시오.

CISO 대시보드 및 스캔 보장 범위 보고서에 대한 자세한 내용은 취약성 관리 CISO 대시보드를 참조하십시오.

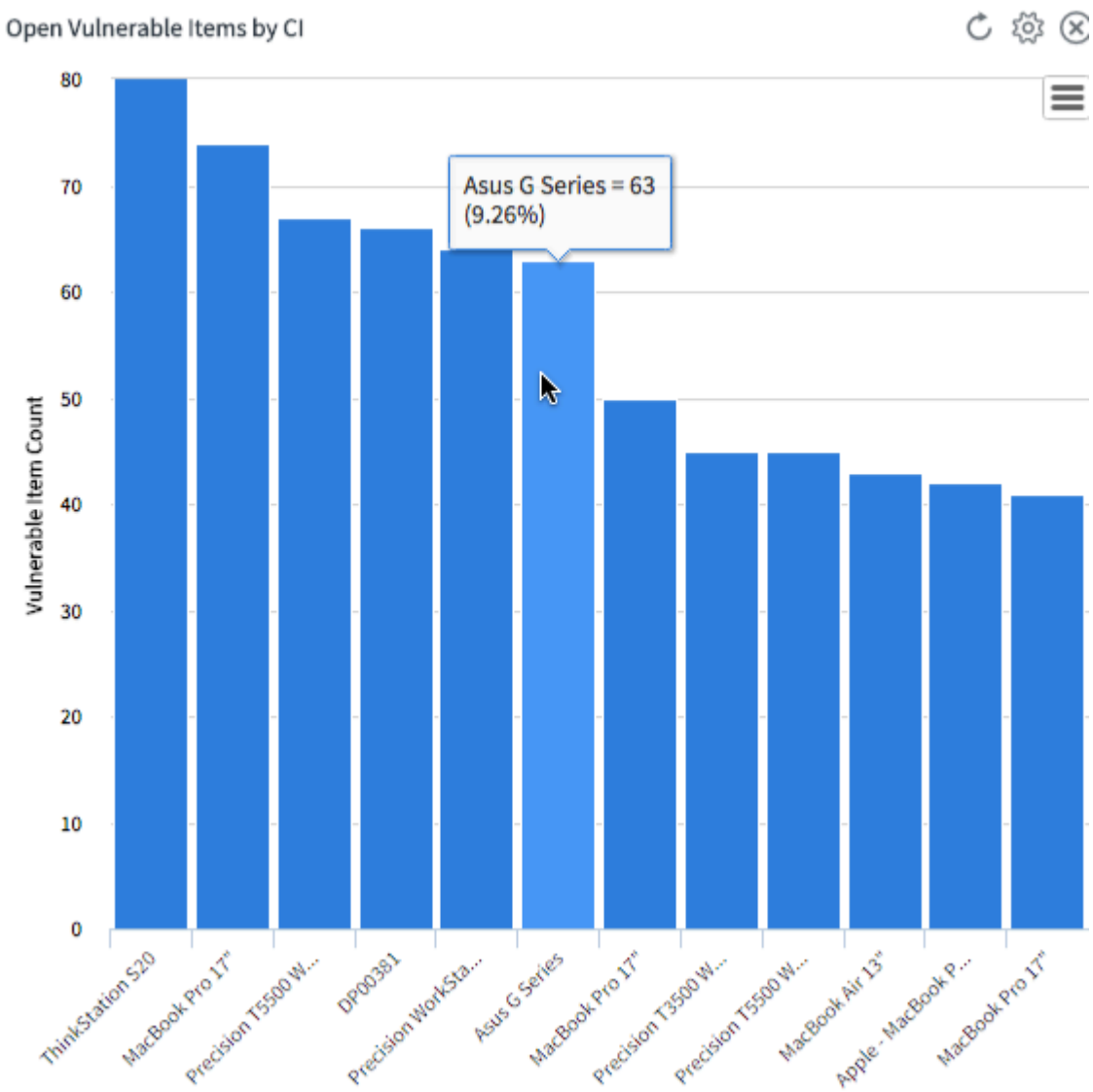
취약성 관리 대시보드

각 차트에서 차트의 특정 부분(막대형, 원형, 데이터 요소 등)을 가리키면 해당 부분과 관련된 일반 데이터를 볼 수 있습니다. 보고서의 일부를 클릭하면 자세한 정보를 제공하는 목록이 열립니다.

주:

사용자 지정 대시보드가 필요한 경우 대시보드 생성 및 사용에서 자세한 내용을 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



취약성 개요 보고서

이름	Visual	설명
CI별 미결된 취약한 항목	막대	각 CI(구성 항목)에 대해 기록된 미해결된 취약한 항목 수를 가장 많은 항목에서 가장 작은 항목 순으로 표시합니다.
정정 대상 상태별 취약한 항목	막대	대상에 접근 중, 비행 중, 과거 대상에 해당하는 취약한 항목 수를 표시합니다. **주:** 지연됨, 해결됨 또는 종결됨 상태의 항목은 포함되지 않습니다.
이번 주에 만료되는 지연된 취약한 항목	그래프	7일 이내에 재활성화되도록 예약된 지연된 취약한 항목 수를 표시합니다.
취약성별 미결된 취약한 항목	막대	각 취약성에 대해 미해결된 취약한 항목 수를 가장 많은 항목에서 가장 작은 항목 순으로 표시합니다.
모델별 취약성	막대	각 모델(CI 클래스)에 대해 기록된 취약한 항목 수를 가장 많은 항목에서 가장 작은 항목 순으로 표시합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약성 개요 보고서

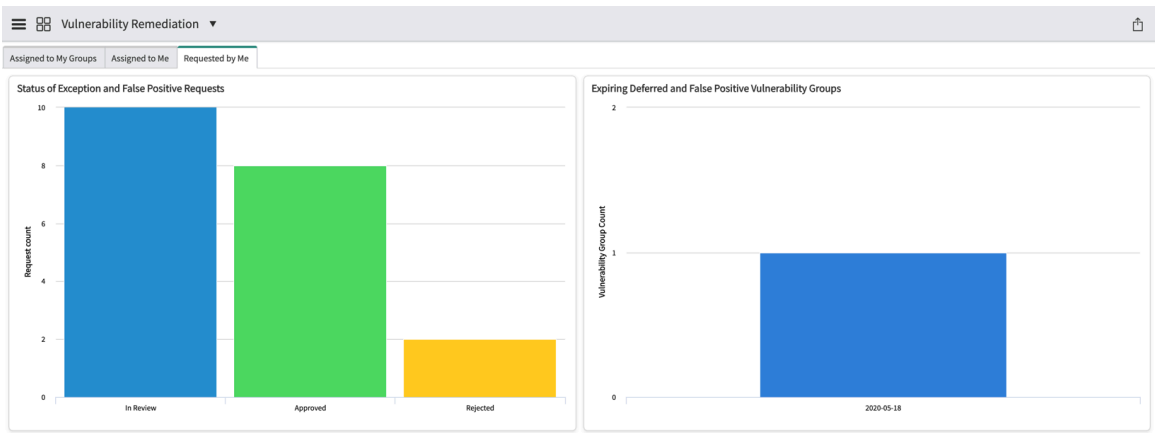
이름	Visual	설명
주간별 취약성	추세	매주 기록된 취약성 항목 수를 표시합니다.
가장 취약한 모델	도넛형	가장 취약한 항목이 있는 모델(CI 클래스)을 표시합니다.
게시자별 취약성	막대	각 게시자에 대해 기록된 취약한 항목 수를 가장 많은 항목에서 가장 작은 항목 순으로 표시합니다.
영향별 취약성	막대	영향을 받는 네트워크 유형에 대한 취약성 항목 수를 표시합니다.
가장 취약한 게시자	도넛형	가장 취약한 항목이 있는 게시자를 표시합니다.
가장 취약한 CI	도넛형	가장 취약한 항목이 있는 CI를 표시합니다.
점수별 취약성	막대	취약성 점수별로 취약성 항목 수를 표시합니다.
다시 개시된 취약한 항목	목록	재개시된 취약한 항목과 해당 기간을 나열합니다.
클래스별 가장 취약한 CI	도넛형	가장 취약한 항목이 있는 CI를 표시합니다.
취약한 항목 기간	목록	취약한 항목이 마지막으로 열린 이후의 일 수를 나열합니다.
날짜별 취약성이 있는 CI	목록	지난 30일 이내에 스캔한 구성 항목을 나열합니다.
스캔되지 않은 CI	목록	취약성을 검사한 적이 없는 구성 항목을 나열합니다.

취약성 개선 대시보드

의 취약성 대응버전 19.0부터 이 대시보드는 New Experience UI에서 사용할 수 있습니다.

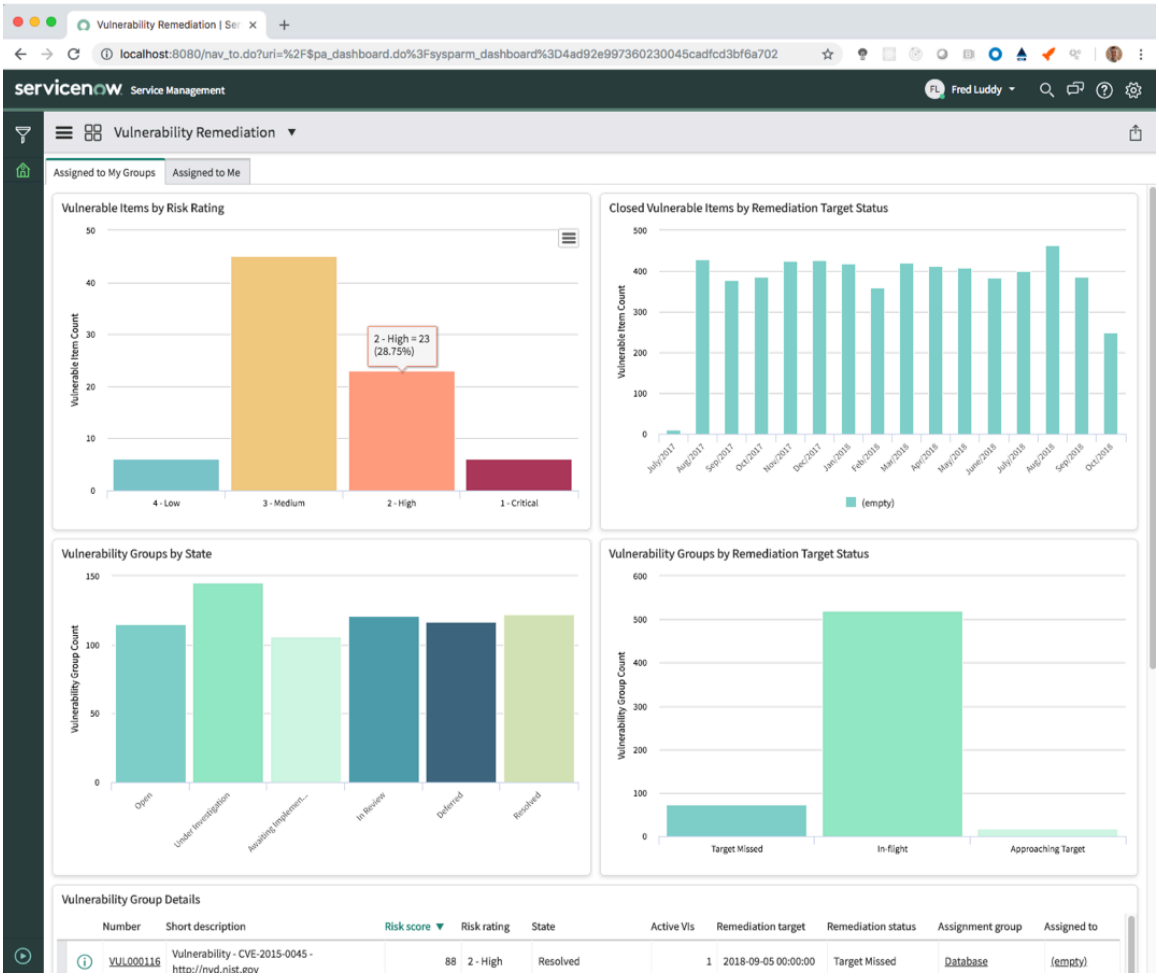
주:
Tokyo에 있는 경우 Next Experience UI에서 대시보드를 볼 수 있지만 일부 기능 손실이 있습니다.

취약성 개선 대시보드에는 내 그룹에 할당됨, 나에게 할당됨 및 내가 요청함 탭이 포함되어 있습니다. 내 그룹에 할당됨 및 나에게 할당됨 탭에 동일한 보고서가 표시됩니다. 전자의 탭은 사용자가 속한 할당 그룹별로 보고하고, 후자는 할당된 취약한 항목 또는 정정 작업별로 보고합니다. 내가 요청함 탭은 요청한 가양성 및 예외를 보고합니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약성 개선 대시보드



보고서

내 그룹에 할당됨 및 나에게 할당됨

이름	Visual	설명
위험 등급별 취약한 항목	막대	선택한 시간 범위 동안 위험 등급별로 그룹화된 활성 취약한 항목 수입니다.
정정 대상 상태별 닫힌 취약한 항목	막대	선택한 시간 범위 동안 정정 목표 상태별로 그룹화된 종결된 취약한 항목 수입니다.
상태별 정정 작업	막대	상태별로 그룹화된 활성 정정 작업(RT) 수입니다.
정정 대상 상태별 정정 작업	막대	정정 대상 상태별로 그룹화된 활성 RT 수입니다. 지연된 취약한 항목은 이 보고서에서 제외됩니다.
정정 작업 세부 정보	목록	목록의 정정 작업 기록 상세 정보.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

내가 요청함

이름	Visual	설명
예외 요청 및 긍정 오류 요청의 상태	막대	활성 요청 수입니다.
만료 지연된 작업 및 긍정 오류 정정 작업	막대	종료 날짜별로 그룹화된 지연된 RT(긍정 오류 정정 작업) 수입니다.

취약성 승인 대시보드

취약성 승인 대시보드에는 예외 승인자 및 긍정 오류 승인자에 대한 다음 보고서가 포함되어 있습니다.

의 취약성 대응버전 19.0부터 이 대시보드는 New Experience UI에서 사용할 수 있습니다.

주:
Tokyo에 있는 경우 Next Experience UI에서 대시보드를 볼 수 있지만 일부 기능 손실이 있습니다.

이름	Visual	설명
내 승인 보류 기간별 예외 요청 및 긍정 오류 요청	막대	생성된 날짜별로 그룹화된 보류 중인 승인 수입니다.
내 승인 및 거부된 예외 요청 및 긍정 오류 요청	막대	승인 상태별로 그룹화된 승인 또는 거부된 승인 요청 수입니다.
승인 보류 중인 위험 등급별 모든 정정 작업	막대	위험 등급별로 그룹화되어 승인 보류 중인 정정 작업 수입니다.
이유별로 그룹화된 모든 보류 중인 승인 요청 및 긍정 오류 승인 요청	막대	이유별로 그룹화된 보류 중인 승인 요청 수입니다.

플랫폼 분석 솔루션 취약성 관리용

플랫폼 분석 솔루션에는 다른 ServiceNow AI Platform 제품과 함께 사용하기 위해 사전 패키징된 퍼포먼스 분석 및 보고 컨텐츠가 포함되어 있습니다. 이 분석 및 보고 솔루션을 사용하면 초기 분석 및 탐지에서 억제 또는 정정에 이르기까지 취약성의 볼륨, 성능 및 진행 상황을 추적할 수 있습니다. 할당 그룹, 익스플로잇, 위험 등급 또는 상태별로 보고서를 필터링할 수 있습니다.

콘텐츠 팩은 취약성 대응용 퍼포먼스 분석 애플리케이션과 함께 취약성 대응 자동으로 설치되지 않습니다. 별도의 구독으로 사용할 수 ServiceNow Store 있습니다.

취약성 대응용 퍼포먼스 분석 에는 다음 두 개의 대시보드가 포함되어 있습니다.

- 취약성 관리(PA) 대시보드
- 취약성 관리 최고 정보 보안 책임자(CISO) 대시보드

필요한 역할, 설치 및 대시보드 보기

이 솔루션과 관련된 역할과 작업은 다음과 같습니다.

- ServiceNow AI Platform 관리자(admin): 이 Analytics and Reporting 솔루션을 설치 및 활성화하고 필요한 변경 사항을 시스템 속성에 적용합니다.
- 퍼포먼스 분석관리자(pa_admin): 표시기, 세부 항목, 위젯 및 대시보드를 검토합니다. 데이터 수집을 설정 및 시작합니다. 적절한 이해 관계자와 대시보드를 공유합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 애플리케이션을 설치하려면 취약성 대응(PA) 애플리케이션을 위한 퍼포먼스 분석 애플리케이션 설치 및 구성을 참조하십시오.

주:
프로덕션에서 사용하도록 설정하기 전에 비프로덕션 인스턴스에서 Analytics and Reporting 솔루션을 설정하고 테스트합니다.

Analytics and Reporting 솔루션은 기본 애플리케이션을 분석하는 데 필요한 모든 구성 기록을 제공합니다. 프로덕션 환경에서 사용할 이러한 기록을 사용자 지정합니다.

취약성 관리(PA) 대시보드를 보려면 다음으로 이동하십시오. 취약성 대응 > 개요 > .

취약성 관리 CISO 대시보드를 보려면 다음으로 이동합니다. 취약성 대응 > **CISO** 대시보드 > .

주요 용어

퍼포먼스 분석(PA)

관리 대시보드를 만들고, KPI 및 메트릭에 대해 보고하고, 핵심 비즈니스 질문에 답하여 품질을 높이고 비용을 절감하는 솔루션입니다.

VI(취약한 항목)

CI(구성 항목)에 있는 외부 공급업체 취약성 스캐너에서 보고된 보안 취약성입니다.

정정 작업

정정 작업은 정정 작업의 취약한 항목과 연결된 그룹에 따라 자동으로 생성되고 IT 팀에 할당됩니다. IT 팀과 정정 소유자는 IT 정정 작업 공간에서 정정 작업을 봅니다. 자세한 내용은 취약성 대응 작업 공간 문서를 참조하십시오.

.

PA 표시기

비즈니스 서비스, 활동 또는 조직 행동에 대해 정기적인 간격으로 수행되는 성과 측정을 정의합니다(예: 연기되지 않은 기한 초과 중요 취약한 항목).

PA 표시기 소스

하나의 테이블 또는 데이터베이스 뷰에서 기록을 필터링하는 데이터 세트(예: VI Active).

실시간으로 데이터 시각화 보기

애플리케이션에서 가장 중요한 항목에 취약성 대응 대해 현재 어떤 일이 일어나고 있는지 확인하기 위해 취약성 관리(PA) 대시보드에서 실시간으로 특정 보고서를 볼 수 있습니다. 이러한 보고서를 즉석에서 확인하면 가장 중요한 취약한 항목(VI)을 관리하고 신속하게 정정할 수 있습니다. 다음 보고서를 실시간으로 볼 수 있습니다.

- 개요 탭 - 할당 그룹별 취약한 항목
- 취약한 CI 탭
  - 소유자가 없는 취약한 CI(구성 항목)
  - 활성 VI가 있는 폐기된 또는 도난당한 CI
- 예외 탭
  - 사유별 연기된 취약한 항목
  - 만료 예정인 연기 요청
  - CIO 관리자가 연기한 취약한 항목
- 정정 탭 - 할당되지 않은 취약한 항목

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

자세한 내용은 실시간으로 취약성 대응(PA)용 퍼포먼스 분석 보고서 보기를 참조하십시오.

취약성 관리 **CISO** 대시보드

취약성 관리 CISO 대시보드를 사용하여 취약성 정정을 위한 핵심성과지표(KPI)와 같은 데이터를 보고, 최고 수준의 위험을 확인하고, 스캔 보장 범위를 확인하고, 위험을 낮추는 방법을 알아봅니다.

필요한 **ServiceNow AI Platform** 역할

- sn_vul.vulnerability_ciso를 사용하여 대시보드를 볼 수 있습니다.
- sn_vul.ciso_write를 사용하여 대시보드를 편집합니다.

CISO 대시보드 활성화

CISO 대시보드를 활성화하려면 해당 퍼포먼스 분석 작업에 대한 취약성 대응 퍼포먼스 분석을 설치하고 활성화해야 합니다. 자세한 내용은 Vulnerability Response를 위한 분석 및 보고 솔루션을 참조하십시오.

사용 사례

사용자	대시보드 사용
최고 정보 보안 책임자(CISO)	최고 정보 보안 책임자(CISO)는 CISO 대시보드를 사용하여 조직의 취약성 관리 프로그램에 대한 인사이트를 얻을 수 있습니다. 대시보드는 데이터를 한눈에 식별하는 데 도움이 되는 데이터를 제공하고, 사용 방법을 사용하여 환경에 대한 취약성을 낮출 수 있습니다.

CISO 대시보드 사용

조직의 최고 정보 보안 책임자(CISO)와 같은 임원 사용자는 취약성 대응의 CISO 대시보드를 보고 취약성 관리 프로그램이 얼마나 효과적인지 파악할 수 있습니다. 다음으로 이동하여 CISO 대시보드를 볼 수 있습니다. 취약성 대응 〉 **CISO** 대시보드. 최상위 필터를 사용하여 위험 등급, 연령대 또는 인터넷 연결을 기준으로 보고서를 필터링합니다. 일부 보고서는 일정 기간 동안의 추세 데이터를 표시합니다. 중요한 메트릭의 정기적인 추세를 보고, 전반적인 비즈니스 보안 위험을 분석하고, 개선이 필요한 영역을 식별할 수 있습니다.

의 취약성 대응버전 19.0부터 이 대시보드는 New Experience UI에서도 볼 수 있습니다. 새 UI에서 대시보드를 보려면 다음으로 이동합니다. 작업 공간 〉 취약성 관리자 작업 공간 을 클릭하고 대시보드 아이콘을 클릭합니다. 역할에 따라 기본 대시보드가 표시됩니다. 다른 대시보드를 보려면 대시보드 이름 옆에 있는 드롭다운을 클릭합니다. 자세한 내용은 취약성 관리자 작업 공간의 대시보드 및 IT 정정 작업 공간의 대시보드를 참조하십시오.

주:
Tokyo에 있는 경우 Next Experience UI에서 대시보드를 볼 수 있지만 일부 기능 손실이 있습니다.

예약된 작업 실행

다음 순서대로 예약된 작업을 실행하여 보고서의 데이터를 업데이트합니다.

1. 대시보드 테이블 업데이트
2. [PA VR] CISO 대시보드

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

CISO 대시보드의 예약된 작업

예약된 작업 이름	설명
대시보드 테이블 업데이트	CISO 데이터를 수집할 수 있도록 〔PA VR〕 CISO 대시보드 작업 전에 실행해야 하는 일별 예약 작업입니다. 이 예약된 작업을 실행하여 스캔 보장 범위 보고서를 업데이트합니다. 업데이트된 정보에는 지난 90일 동안 스캔한 운영 구성 항목(CI), 해당 클래스 및 이러한 클래스에 해당하는 총 운영 CI 수가 포함됩니다. 이 예약된 작업을 실행하면 권장 작업 탭의 보고서도 업데이트됩니다. 주: 운영 CI는 운영 상태가 ##인 CI를 말합니다.
〔PA VR〕 CISO 대시보드	대시보드 테이블 업데이트 예약된 작업이 완료된 후 이 예약된 작업을 실행하여 **CISO** 개요 탭의 모든 보고서를 채웁니다.

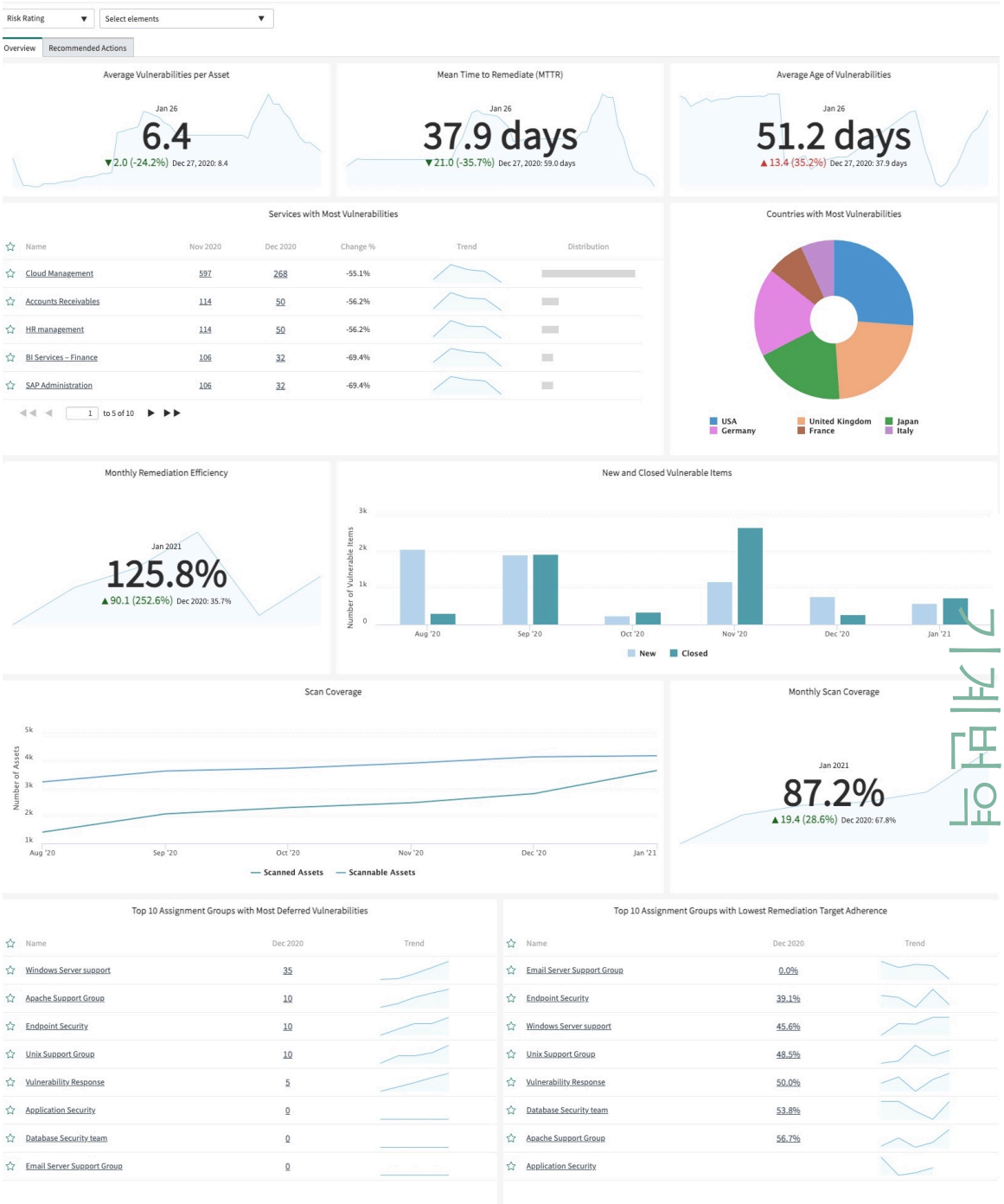
CISO 대시보드 탭

이 대시보드는 취약성 관리에 존재하는 위험에 대한 인사이트를 제공합니다. 지역, 기간, 서비스 및 기타 세부 항목별로 취약성과 관련 데이터를 볼 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

개요 탭

개요 탭에는 조직의 보안 태세를 한 눈에 파악할 수 있는 보고서가 포함되어 있습니다.

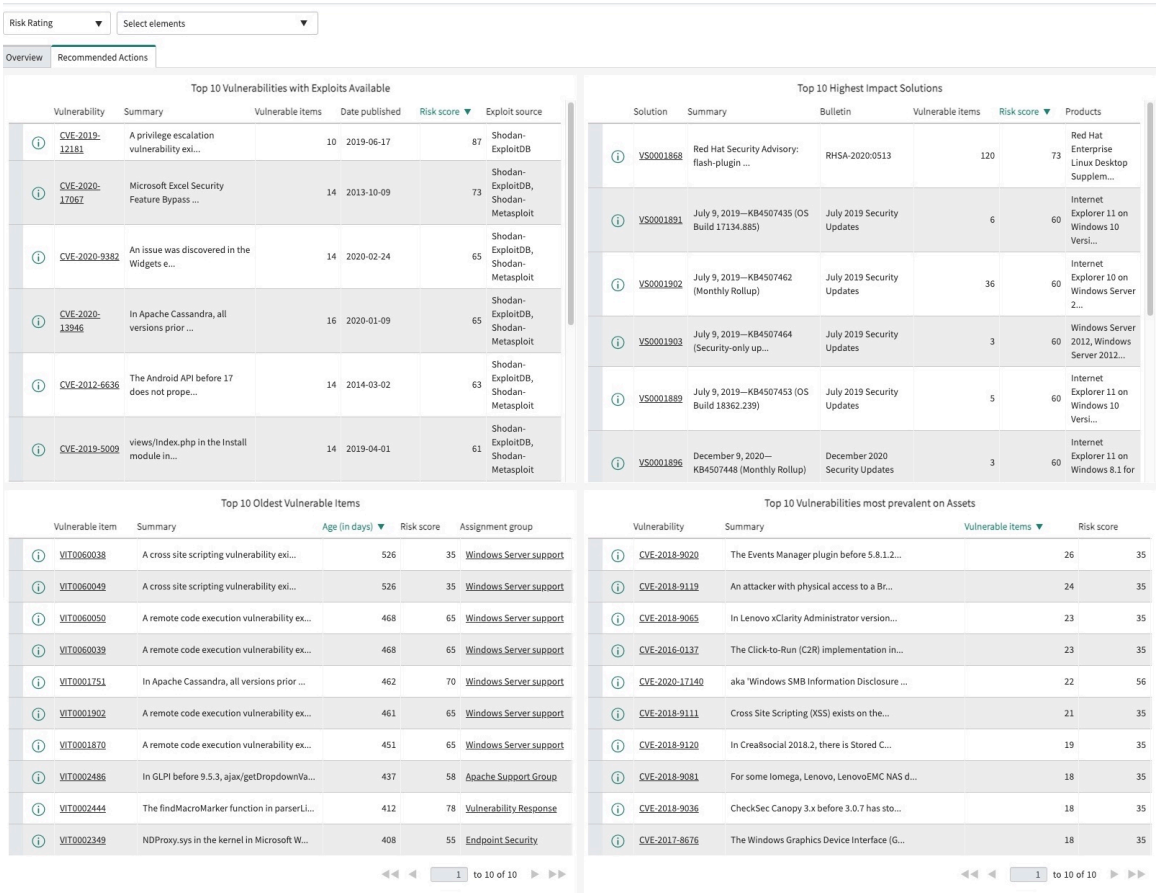


주:
최상위 필터는 일부 보고서에만 사용할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

권장 작업 탭

권장 작업 탭에는 악용 가능, 노후화 및 널리 퍼져 있는 취약성에 대한 인사이트를 제공하는 보고서가 포함되어 있습니다. 또한 위험을 줄이기 위한 작업을 권장하는 솔루션도 포함되어 있습니다. **CISO** 대시보드 테이블 업데이트 예약된 작업을 실행하여 이 탭에서 보고서를 업데이트합니다.



표시기

표시기를 보려면 다음으로 이동하십시오. 퍼포먼스 분석 〉 표시기.

1. 표시기 페이지의 이름 열에서 필요한 표시기 이름을 검색합니다.
2. 표시기 이름을 클릭하여 기록을 열고 상세 정보를 봅니다.

CISO 대시보드의 표시기는 기본적으로 기록을 수집하지 않습니다. 기록 수집 확인란을 선택하여 기록을 수집하도록 선택할 수 있습니다.

닫힌 취약한 항목의 총 기간

종결된 VI의 총 기간은 일 단위로 매일 측정됩니다. 이 표시기의 목표는 점수를 최소화하는 것입니다.

스캔 가능한 자산

스캔한 자산은 매일 # 단위로 측정됩니다. 이 표시기의 목표는 점수를 최대화하는 것입니다.

대부분의 취약성이 포함된 서비스

대부분의 취약성을 갖춘 서비스는 # 단위로 매일 측정됩니다. 이 표시기의 목표는 점수를 최소화하는 것입니다.

자산당 평균 취약성

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

〔〔활성 취약한 항목〕〕/〔〔활성 취약한 구성 항목〕〕

닫힌 취약한 항목

종결된 취약한 항목은 # 단위로 매일 측정됩니다. 이 표시기의 목표는 점수를 최대화하는 것입니다.

정정할 취약한 항목 중위 시간

〔〔종결된 취약한 항목의 합산 기간〕〕/〔〔종결된 취약한 항목〕〕

현재 스캔 보장 범위

백분율로 현재 검사 범위를 계산합니다.

스캔된 자산

스캔한 자산은 매일 # 단위로 측정됩니다. 이 표시기의 목표는 점수를 최대화하는 것입니다.

종결된 취약한 항목(대상 충족)

종결된 취약한 항목(대상 충족)은 # 단위로 매일 측정됩니다. 이 표시기의 목표는 점수를 최대화하는 것입니다.

대상을 충족하는 닫힌 취약한 항목의 비율(%)

〔〔종료된 취약한 항목(목표 충족)/월 합계〕〕 / 〔〔종료된 취약한 항목/월 합계〕〕*100

활성 상태의 취약 항목

활성 취약한 항목은 # 단위로 매일 측정됩니다. 이 표시기의 목표는 점수를 최소화하는 것입니다.

취약한 항목의 평균 기간

활성 VI의 평균 기간은 일 단위로 매일 측정됩니다. 이 표시기의 목표는 점수를 최소화하는 것입니다.

> **주:**
> VI(취약한 항목)에 대한 기간 및 종결된 기간 계산을 사용자 지정하면 이러한 메트릭이 포함된 퍼포먼스 분석(PA) 보고서가 급격히 증가하거나 감소할 수 있습니다. VI의 기간 및 종결 기간 계산을 사용자 지정하는 방법에 대한 자세한 내용은 KB1703270 KB 문서를 참조하십시오.

활성 취약한 구성 항목

활성 취약한 CI는 # 단위로 매일 측정됩니다. 이 표시기의 목표는 점수를 최소화하는 것입니다.

월별 정정 효율성

〔한달간 종결된 취약 항목 수〕 / 〔같은 달에 새로 오픈되거나 재오픈된 취약 항목 수〕

새로운 취약한 항목

새로운 취약한 항목은 # 단위로 매일 측정됩니다. 이 표시기의 목표는 점수를 최소화하는 것입니다.

연기된 취약한 항목

지연된 VI는 매일 # 단위로 측정됩니다. 이 표시기의 목표는 점수를 최소화하는 것입니다.

세부 항목

- 할당 그룹: 일부 VI 보고서에 적용됩니다.
- 위험 등급: VI 보고서에 적용됩니다.
- 연령 범위: VI 보고서에 적용됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 종결 기간: 종결된 VI에 대한 보고서에 적용됩니다.
- 인터넷 접근: CI가 하드웨어 클래스에 속하고 인터넷에 연결되어 있는지 여부를 나타냅니다.
- 지역: 사용되는 CMDB CI 매개변수는 위치입니다. 이 위치는 구성 항목의 원산지 국가를 나타냅니다.

주:
VI(취약한 항목)에 대한 기간 및 종결된 기간 계산을 사용자 지정하면 이러한 메트릭이 포함된 퍼포먼스 분석(PA) 보고서가 급격히 증가하거나 감소할 수 있습니다. VI의 기간 및 종결 기간 계산을 사용자 지정하는 방법에 대한 자세한 내용은 KB1703270 KB 문서를 참조하십시오.

데이터 시각화

이름	유형	설명
자산당 평균 취약성	단일 점수	개별 구성 항목별 취약한 항목의 평균 수입니다.
평균 동작 불가능 시간(MTTR)	단일 점수	취약한 항목을 정정(종결)하기 위한 평균 시간으로, 30일 이동 평균으로 표시됩니다. **주:** 종결 연령의 값은 데이터가 수집될 때 계산됩니다. 값은 마지막으로 오픈한 날짜와 수집 작업의 날짜 및 시간 간의 차이입니다.
취약성의 평균 기간	단일 점수	활성화된 취약한 항목의 평균 기간(일)입니다.
대부분의 취약성이 포함된 서비스	목록 및 라인	조직 내 서비스에 대한 활성 취약한 항목의 월별 평균입니다. **주:** 취약성 대응 보고 및 관련 목록에 표시할 서비스 분류를 정의하는 방법에 대한 자세한 내용은 취약성 관리(PA) 대시보드에서 서비스 탭을 참조하십시오.
대부분의 취약성이 포함된 국가	도넛형	취약 항목 수가 가장 많은 상위 10개 국가입니다.
월별 정정 효율성	단일 점수	이번 달에 종결된 취약한 항목을 새로운 취약한 항목으로 나눈 비율(%)입니다.
새로운 또는 닫힌 취약한 항목	막대	한 달 동안 임포트된 새 취약한 항목 수와 종결된 취약한 항목 수입니다.
스캔 보장 범위	선형	시간 동안 표시된 스캔한 자산의 총 수와 비교하여 스캔한 자산 수입니다. 위젯에 포함된 CI 클래스는 스캔 보장 범위 구성 모듈에 지정됩니다. 스캔 보장 범위 모듈 구성에 대한 자세한 내용은 스캔 보장 범위 보고서 구성을 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이름	유형	설명
월별 스캔 보장 범위	단일 점수	스캔한 자산의 백분율을 현재 월에 스캔 가능한 총 자산 수로 나눈 값입니다. 스캔 보장 범위 모듈 구성에 대한 자세한 내용은 스캔 보장 범위 보고서 구성을 참조하십시오.
취약성이 가장 지연된 상위 10개 담당 그룹	목록 및 라인	지연된 취약한 항목 수가 가장 많은 상위 10개 할당 그룹으로, 월 평균을 기준으로 연기되었습니다.
개선 대상 준수를 가장 이행하지 못한 상위 10개 담당 그룹	목록 및 라인	취약한 항목의 정정 목표 준수율이 가장 낮은 상위 10개 할당 그룹입니다.

권장 작업

이름	유형	소스 테이블	설명
익스플로잇이 가능한 상위 10개 취약성	목록	취약성 상위 항목 [sn_vul_analytics_top_item]	VR 익스플로잇 프레임워크를 사용하는 모든 위협 인텔리전스 벤더에 대해 사용할 수 있는 익스플로잇이 있는 활성 취약성입니다.
가장 영향력이 큰 상위 10개 솔루션	목록	취약성 상위 항목 [sn_vul_analytics_top_item]	활성 취약한 항목에 대한 위험 점수가 가장 높은 기본 솔루션 또는 패치입니다. 이 보고서는 Microsoft 및 Red Hat의 패치를 환경의 취약성과 상호 연관시키는 VSM(취약성 솔루션 관리)의 기능을 사용합니다. VSM은 취약성에 대한 기본 솔루션을 식별하는 데 도움이 됩니다.
가장 오래된 취약한 항목 상위 10개	목록	취약성 상위 항목 [sn_vul_analytics_top_item]	기간이 가장 긴 활성 취약한 항목입니다. 이러한 항목을 해결하여 개요 탭의 평균 취약성 기간을 낮춥니다.
자산에 가장 널리 퍼져 있는 상위 10개 취약성	목록	취약성 상위 항목 [sn_vul_analytics_top_item]	가장 많은 수의 자산에 사용할 수 있는 활성 취약한 항목입니다.

스캔 보장 범위 보고서 구성

사용자가 CISO 대시보드에서 스캔 범위 보고서를 실행할 수 있도록 합니다. 이러한 보고서를 통해 사용자는 일정 기간 동안 조직의 검사 범위를 확인할 수 있습니다.

시작하기 전에

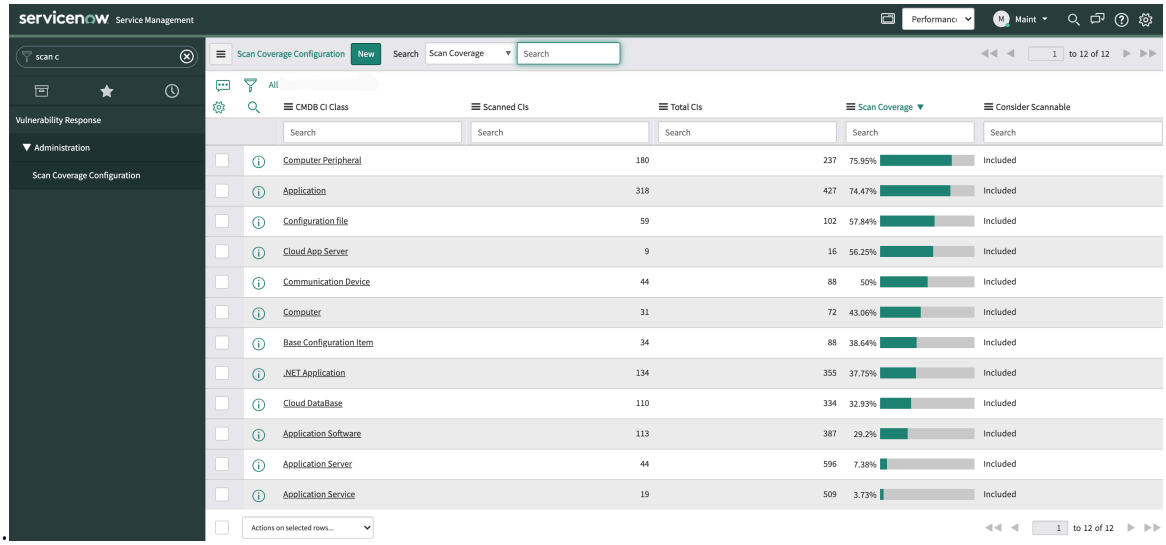
필요한 역할: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

이 태스크 정보

스캔 적용 범위에는 지난 90일 동안 다양한 클래스에 대해 취약성 스캐너에서 스캔한 자산 수가 표시됩니다. 이러한 자산은 에서 구성 관리 데이터베이스(CMDB)스캔 가능한 자산 수와 비교됩니다. 기본적으로 스캔 보장 범위 구성 모듈에는 스캔한 자산이 하나 이상 일치하는 CI 클래스가 포함됩니다 CMDB . 에서 CMDB CISO 대시보드에 표시되는 스캔 범위 보고서에 CI 클래스를

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

추가할 수 있습니다. 스캔 범위 보고서에 나타나는 CI 클래스를 포함하거나 제외 CMDB 할 수 있습니다.



프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 스캔 보장 범위 구성.
2. 새로 만들기를 클릭합니다.
3. 양식에서 필드를 채웁니다.

스캔 보장 범위 구성 양식

필드	설명
CMDB CI 클래스	CISO 대시보드의 검사 범위 보고서에 추가해야 하는 CI 클래스입니다. **주:** 스캔 보장 범위 구성 모듈에 CI 클래스가 이미 있는 경우에는 이 목록에 포함되지 않습니다.
스캔 가능 요소 고려	CI 클래스를 포함해야 하는지 여부를 정의하는 옵션입니다. 스캔 범위 보고서에 해당 데이터를 추가하려면 CI 클래스를 포함합니다. 제외하면 해당 CI 클래스에 대한 데이터가 추가되지 않습니다.

4. 제출을 클릭합니다.

CISO 대시보드의 PA 표시기 구성

인스턴스의 취약성 데이터를 관리할 수 있도록 자동화되고 수식화된 CISO 표시기를 모니터링합니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin

이 태스크 정보
취약성 대응 에는 자동 표시기와 공식화된 표시기가 모두 있습니다.

주요 용어

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

표시기

비즈니스 서비스, 활동 또는 조직 행동에 대해 정기적인 간격으로 수행되는 성과 측정을 정의합니다. 활성 취약한 항목을 예로 들 수 있습니다.

표시기 소스

효율성 향상을 위해 하나의 테이블 또는 데이터베이스 뷰에서 필터링된 기록으로 구성된 데이터 세트. VI.Active(인터넷 접근)를 예로 들 수 있습니다.

세부 항목

세부 항목은 우선순위, 범주 및 할당 그룹과 같은 질적 속성을 사용하여 표시기 점수를 필터링하고 그룹화합니다.

예약된 작업

예약된 작업은 표시기 소스 데이터를 채우기 위해 실행됩니다. [PA VR] CISO 대시보드 일일 예약 작업은 기본적으로 비활성화되어 있습니다. CISO 대시보드에 대한 표시기 점수를 수집하려면 이를 활성화해야 합니다.

프로시저

1. 다음으로 이동 모두 〉 퍼포먼스 분석 〉 표시기 을 클릭하고 다음 중 하나를 선택합니다.
   - 자동 표시기
   - 수식 표시기

   표시기에 대한 자세한 내용은 퍼포먼스 분석 표시기를 참조하십시오.
2. 표시기 페이지의 이름 열에서 필요한 표시기 이름을 검색합니다.
3. 표시기 이름을 클릭하여 기록을 열고 상세 정보를 봅니다.

   CISO 대시보드의 표시기는 기본적으로 기록을 수집하지 않습니다. 기록 수집 확인란을 선택하여 기록을 수집하도록 선택할 수 있습니다.

   주:
   표시기에서 기록 수집을 활성화하면 데이터 수집 작업을 실행하는 데 필요한 시간과 메모리가 훨씬 더 많이 걸리는 등의 성과 문제가 발생할 수 있습니다.

   표시기 소스에 대해 가져올 수 있는 최대 행 수는 1,000,000개입니다.

SecOps Vulnerability Response 상태 대시보드

Vulnerability Response 상태 대시보드는 조직이 Vulnerability Response 애플리케이션의 구현 및 사용에 대한 포괄적인 통찰력을 얻을 수 있도록 설계된 도구입니다.

전체 상태 평가는 구성, 구현, 통합, 성능, 데이터 및 프로세스 전반에 걸쳐 다양한 중요 요인을 집계하여 결정됩니다. 다음 애플리케이션의 각 범주에 대한 집계 대시보드를 봅니다.

- 취약성 대응
- 애플리케이션 취약성 대응
- 컨테이너 취약성 대응
- 구성 준수

SecOps Vulnerability Response 상태 대시보드 설치

인스턴스에 애플리케이션에 ServiceNow AI Platform 대한 취약성 대응 SecOps 취약성 대응 상태 대시보드를 설치하고 구성하려면 SecOps 상태 분석(sn_sec_analytics) 플러그인으로 ServiceNow# Store 이동하여 활성화합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필요한 **ServiceNow AI Platform** 역할

필요한 역할: sn_sec_analytics.admin, sn_sec_analytics.read

예약된 작업

예약된 작업을 보려면 다음으로 이동합니다. 모두 〉 시스템 스케줄러 〉 예약된 작업 〉 상태 대시보드 메트릭 수집. '상태 대시보드 메트릭 수집' 예약된 작업은 매일 00:00시에 실행됩니다. SecOps 취약성 대응 상태 대시보드에 대한 데이터를 생성합니다. 예약된 작업을 수동으로 실행하도록 선택할 수도 있습니다.

사용 사례

조직 내 사람들이 이 대시보드를 사용하는 방법의 예시는 다음 사용 사례를 참조합니다.

사용자	대시보드 사용
취약성 관리자	애플리케이션의 상태 점수를 이해하는 데 도움이 됩니다 취약성 대응 . 개선이 필요한 영역을 강조하는 것도 도움이 됩니다. Vulnerability Response 상태 대시보드는 구현 및 사용 상태만 처리합니다. 취약성 또는 자산 관리에는 도움이 되지 않습니다.
지원 관리자	KPI를 사용하여 성능, 커스터마이제이션 및 구성 문제를 식별하는 데 도움이 됩니다. 애플리케이션 상태에 따라 추가 분석을 수행하거나 사용자에게 권장 사항을 제공할 수 있습니다.
구현 파트너	구성, 추가 기능, 커스터마이제이션 및 통합에 대한 구현 상태를 평가하고 취약성 대응 사용자를 위한 개선 권장 사항을 제공하는 데 도움이 됩니다.

SecOps Vulnerability Response 상태 대시보드 탭

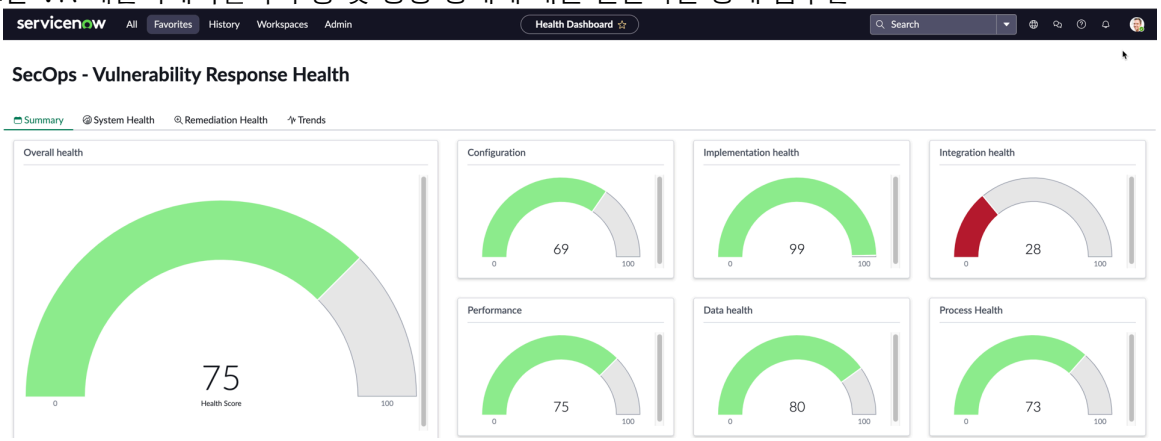
SecOps 취약성 대응 상태 대시보드를 보려면 다음으로 이동합니다. 보안 운영 상태 〉 취약성 대응 상태. 대시보드의 각 색상은 다음을 나타냅니다.

- 녹색: 안전
- 노란색: 경고
- 빨간색: 중요

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

요약 탭

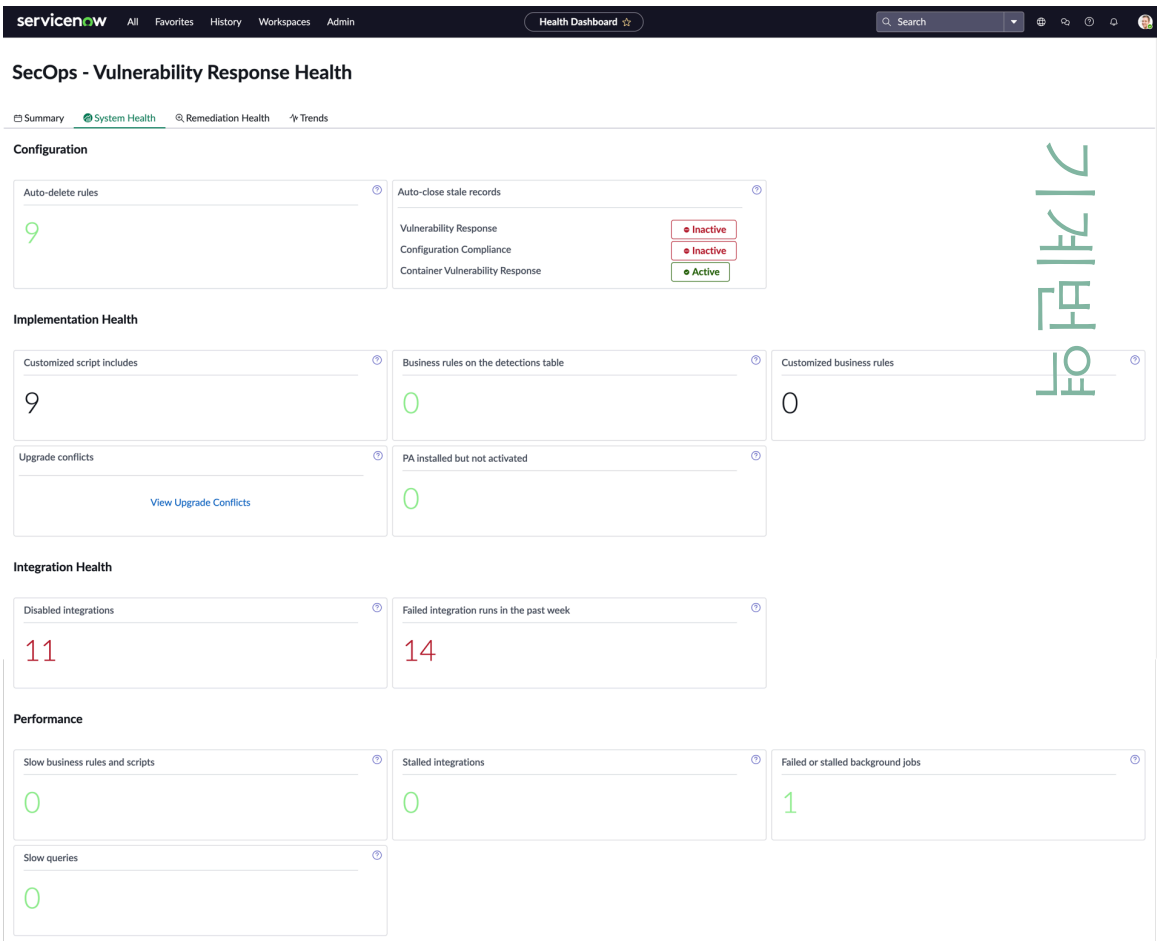
이 대시보드는 VR 애플리케이션의 구성 및 정정 상태에 대한 전반적인 상태 점수를



전달합니다.

시스템 상태 탭

이 대시보드는 구현의 구성 및 통합 상태를 표시합니다. 구현 성과에 대한 전체적인 개요를

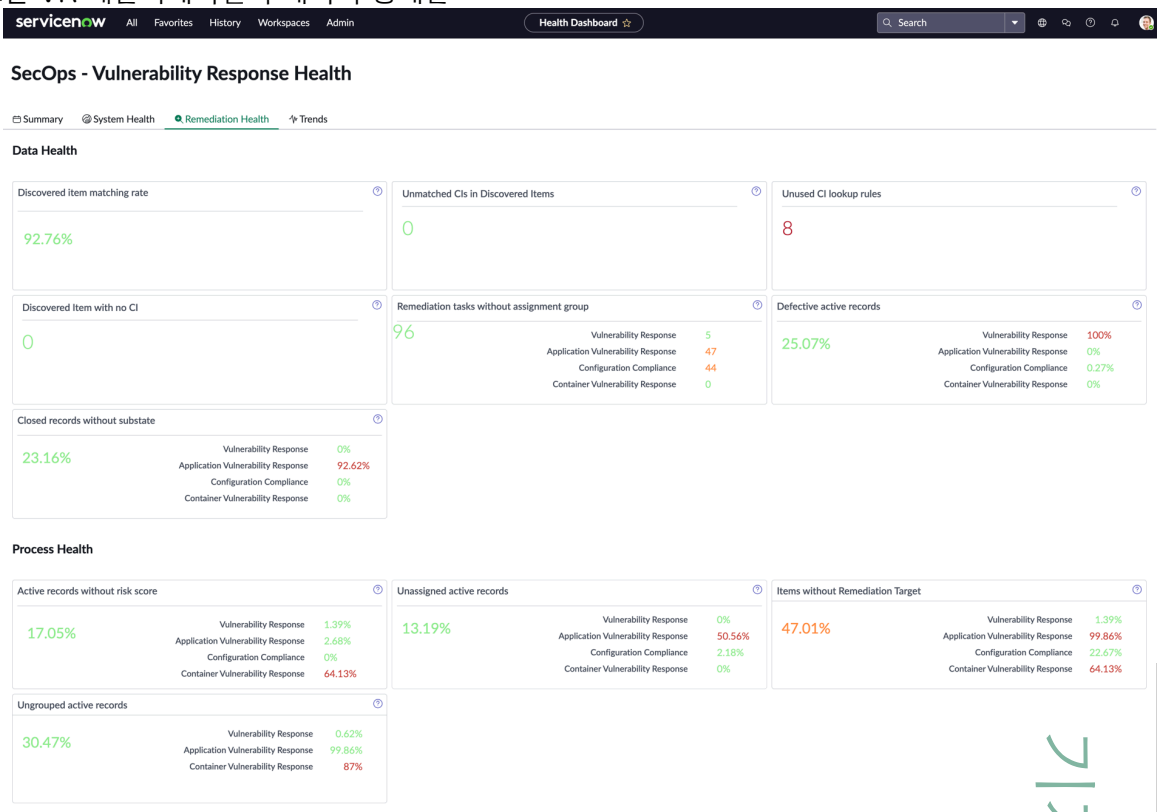


제공합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

정정 상태 탭

이 대시보드는 VR 애플리케이션의 데이터 상태를



표시합니다.

추세 탭

이 대시보드에는 VR 애플리케이션에 대한 지난
30일 동안의 취약한 항목 수집 성과 메트릭의 추세가

표시됩니다.

보고서

주:
임계치 값은 기본 시스템의 일부입니다. 요구 사항에 따라 값을 구성할 수 있습니다.

요약

직위	설명
전반적인 상태	VR 애플리케이션의 전반적인 상태 점수입니다. 자세한 내용은 메트릭 보고서를 참조하십시오.
구성	VR 애플리케이션의 전반적인 구성 상태입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

요약

직위	설명
구현 상태	VR 애플리케이션의 전반적인 구현 상태입니다.
통합 상태	VR 애플리케이션의 전반적인 통합 상태입니다.
성과	VR 애플리케이션의 전반적인 성능 상태 점수입니다.
데이터 상태	VR 애플리케이션의 전반적인 데이터 상태입니다.
프로세스 상태	VR 애플리케이션의 전체 프로세스 상태 점수입니다.

시스템 상태

직위	설명	성능 향상을 위한 고려 사항	임계치 경고	임계치 중요
구성				
자동 삭제 규칙	활성화된 자동 삭제 규칙 수를 표시합니다.	비활성 자동 삭제 규칙을 검토하고 해결합니다.	3	1
부실 기록 자동 종결	부실 탐지를 자동으로 종결합니다. 자세한 내용은 servicenow.com/docs 에서 '취약성 대응에서 부실 탐지 자동 종결' 주제를 참조하십시오.	부실 탐지의 볼륨을 줄입니다. 스캐너에서 종결하지 않은 부실 탐지를 종결하려면 이 옵션을 활성화합니다.	3	1
구현 상태				
사용자 지정된 스크립트 포함	사용자 지정된 "스크립트 포함" 수입니다.	보다 쉬운 업그레이드를 위해 사용자 지정 '스크립트 포함'을 최소화합니다.	10	12
탐지 테이블의 비즈니스 규칙	탐지 테이블의 사용자 지정 비즈니스 규칙 수입니다.	보다 쉬운 업그레이드를 위해 비즈니스 규칙을 최소화합니다.	4	8
사용자 지정 비즈니스 규칙	CMDB에서 기록을 생성하기 전 사용자 지정된 비즈니스 규칙의 수입니다.	기록에 기본 비즈니스 규칙을 사용합니다.	5	8

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시스템 상태

직위	설명	성능 향상을 위한 고려 사항	임계치 경고	임계치 중요
업그레이드 상충	업그레이드 시 식별된 비즈니스 규칙 및 스크립트와 같은 상충.	업그레이드 상충을 검토하고 해결합니다.	10	15
PA가 설치되었지만 활성화되지 않음	퍼포먼스 분석 대시보드가 활성화되지 않았는지 여부를 나타냅니다.	PA 대시보드를 활성화합니다.	10	15
통합 상태				
비활성화된 통합	비활성화된 통합 수입니다.	필요한 통합을 검토하고 활성화합니다.	6	9
지난 주에 실패한 통합 실행	지난 주에 성공하지 못한 통합 실행 수입니다.	실패한 통합 실행의 원인을 검토하고 해결합니다.	9	12
성과				
느린 비즈니스 규칙 및 스크립트	평균 실행 시간이 10ms보다 크고 실행 횟수가 10,000보다 큰 비즈니스 규칙 및 스크립트.	느리게 실행되는 비즈니스 규칙을 검토하고 해결합니다.	10	15
중단된 통합	완료 전에 시간 초과된 통합 수입니다.	중단된 통합의 원인을 검토하고 해결합니다.	10	15
실패 또는 중단된 백그라운드 작업	지난주에 실패하거나 시간 초과된 백그라운드 작업입니다.	실패한 작업의 원인을 검토하고 해결합니다.	5	10
느린 쿼리	평균 실행 시간이 10ms보다 크고 실행 횟수가 10,000회보다 큰 쿼리입니다.	느리게 실행되는 비즈니스 규칙을 검토하고 해결합니다.	10	15

정정 상태

직위	설명	성능 향상을 위한 고려 사항	임계치 경고	임계치 중요
데이터 상태				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

정정 상태

직위	설명	성능 향상을 위한 고려 사항	임계치 경고	임계치 중요
검색된 항목 일치율	기존 CI와 일치하는 검색된 항목 수입니다.	CMDB 및 CI 조회 규칙 논리의 상태를 검토합니다.	50	20
검색된 항목에서 일치하지 않는 CI	일치하지 않는 상태의 검색된 항목입니다.	CMDB 및 CI 조회 규칙 논리의 상태를 검토합니다.	9	12
사용하지 않는 CI 조회 규칙	검색된 항목과 연결되지 않은 CI 조회 규칙입니다.	사용하지 않는 CI 조회 규칙의 상태를 비활성으로 변경합니다.	4	6
CI가 없는 검색된 항목	구성 항목이 없는 검색된 항목입니다.	CI 조회 규칙을 검토하고 다시 적용합니다.	9	12
결함 있는 활성 기록	구성 항목 또는 취약성이 없는 기록입니다.	CMDB CI 수명주기 관리 옵션을 사용하여 CI를 폐기합니다. 주: CI를 직접 삭제하면 VIT가 분리될 수 있습니다.	40	60
할당 그룹이 없는 정정 작업	할당 그룹이 아직 할당되지 않은 활성 정정 작업입니다.	할당 그룹에 정정 작업을 할당하고 기존 할당 규칙을 검토합니다.	40	60
하위 상태 없이 종결된 기록	하위 상태 없이 종결된 기록입니다.	기록을 종결하는 동안 이유 필드에 정보를 제공합니다.	40	50
프로세스 상태				
위험 점수가 없는 활성 기록	위험 점수가 0이거나 위험 점수가 할당되지 않은 활성 기록입니다.	위험 규칙을 검토하고 해결합니다.	40	60
미할당 활성 기록	할당 그룹이 없는 기록입니다.	기록에 그룹을 할당하고 기존 담당 규칙을 검토합니다.	30	50

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

정정 상태

직위	설명	성능 향상을 위한 고려 사항	임계치 경고	임계치 중요
정정 대상이 없는 항목	정정 목표 날짜가 없는 항목입니다.	정정 대상 규칙을 검토하고 해결합니다. 이러한 규칙에는 모든 기록이 포함되어야 합니다.	30	50
그룹화되지 않은 활성 기록	정정 작업 규칙에 포함되지 않은 기록입니다.	정정 작업 규칙을 검토합니다.	40	60

추세

직위	설명
지난 30일 취약한 항목 수집 성과 메트릭	지난 30일 동안 취약한 항목을 수집하고 여러 규칙을 처리하는 데 걸린 평균 시간입니다.

임계치 값 수정

기본 설정에 따라 SecOps VR 상태 대시보드 데이터의 임계값을 수정할 수 있습니다.

시작하기 전에

필요한 역할: 관리자

프로시저

1. 다음으로 이동 보안 운영 상태 〉 구성 〉 메트릭.
2. 상태 대시보드 데이터 페이지에서 수정할 기록을 엽니다.
3. 기록을 업데이트하고 저장합니다.

취약성 관리 **(PA)** 대시보드

초기 분석 및 탐지부터 억제 또는 정정에 이르기까지 취약성의 볼륨, 성능 및 진행 상황을 추적합니다. 예를 들어 할당 그룹, 익스플로잇, 위험 등급 또는 상태별로 보고서를 필터링할 수 있습니다. 취약성 노출과 영향을 받는 비즈니스 서비스에 대한 인사이트를 빠르게 확보합니다.

필요한 **ServiceNow AI Platform** 역할

필요한 역할: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst, sn_vul.vulnerability_read 또는 sn_vul.vulnerability_read 역할을 상속하는 사용자, pa_viewer.

사용 사례

조직 내 다른 사람이 이 대시보드를 사용하는 방법의 예시는 다음 사용 사례를 참조합니다.

사용자	대시보드 사용
IT 관리자, IT 분석가, 취약성 개선 담당자	가장 위험한 취약한 항목을 효율적으로 파악하여 조직이 악용된 취약성으로 인해 증가하는 보안

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용자	대시보드 사용
	인시던트에 대처할 수 있도록 지원합니다. 이러한 대시보드는 취약한 항목 활동에 대한 그래픽 뷰를 제공하며 정정 계획 및 상태 진행률을 설계하는 데 도움이 됩니다. 영향을 받는 중요한 자산 및 가시성이 높은 취약성과 연결된 KPI에 집중할 수 있습니다.

취약성 관리(PA) 대시보드를 보려면 다음으로 이동합니다. 취약성 대응 〉 개요.

시간 경과에 따른 추세 데이터를 보여주는 보고서를 참조하십시오. 실시간 데이터가 포함된 보고서는 다음과 같습니다. 중요한 메트릭의 추세를 정기적으로 확인하여 전체 비즈니스 프로세스를 분석하고 개선 영역을 식별합니다.

실시간 점수로 PA 보고서를 보는 방법에 대한 자세한 내용은 실시간으로 취약성 대응(PA) 보고서를 위한 퍼포먼스 분석 보기의 내용을 참조하십시오.

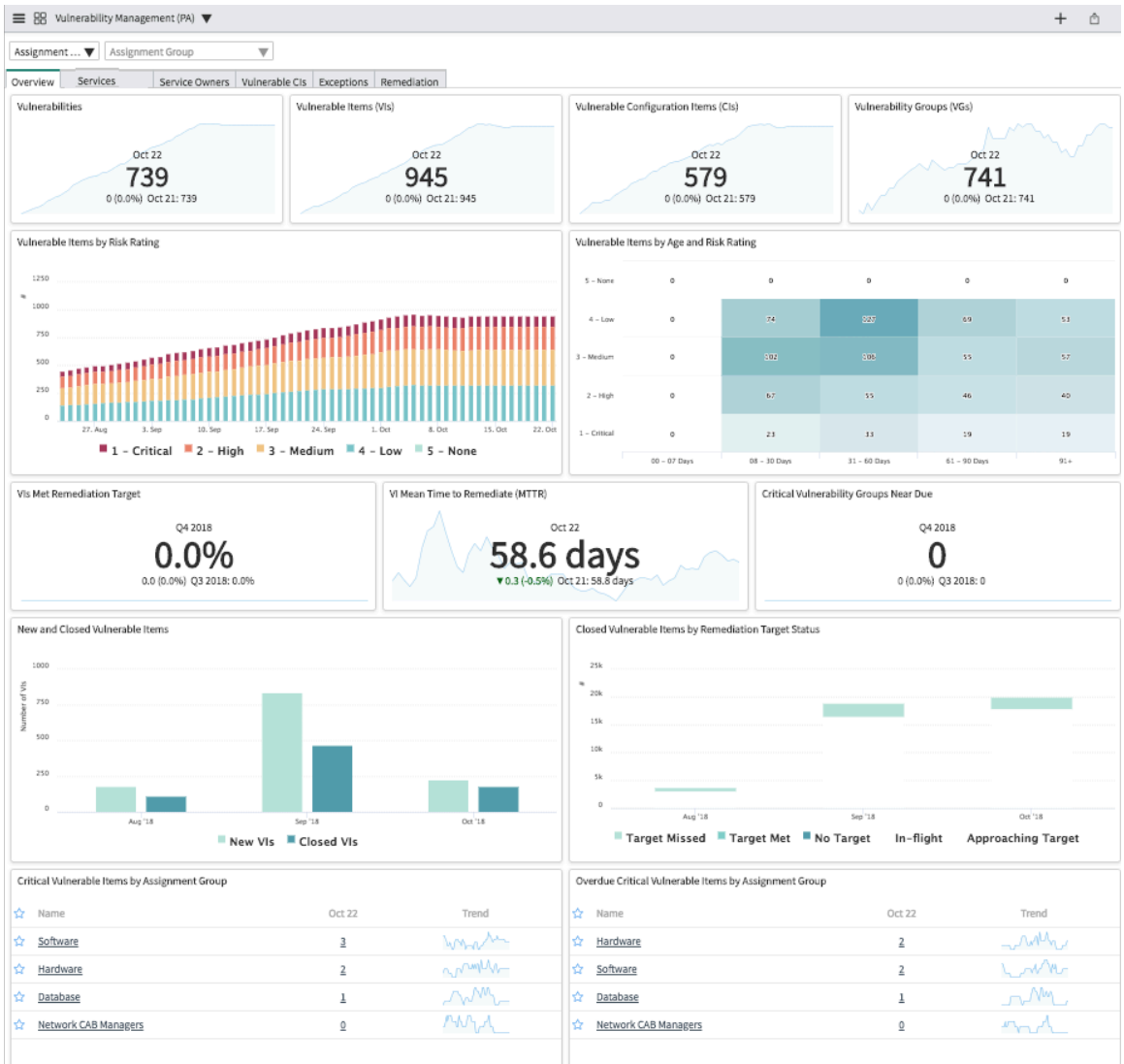
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약성 관리**[PA]** 대시보드 탭

개요 탭

이 대시보드는 취약성 위험 및 확산, 영향을 받는 자산, 정정 대상 준수 및 정정 진행 상황에 대한 KPI를 전달합니다.

개요 탭에서는 예약된 작업에 따라 실행되는 할당 그룹별 중요한 취약한 항목 보고서를 볼 수 있습니다.

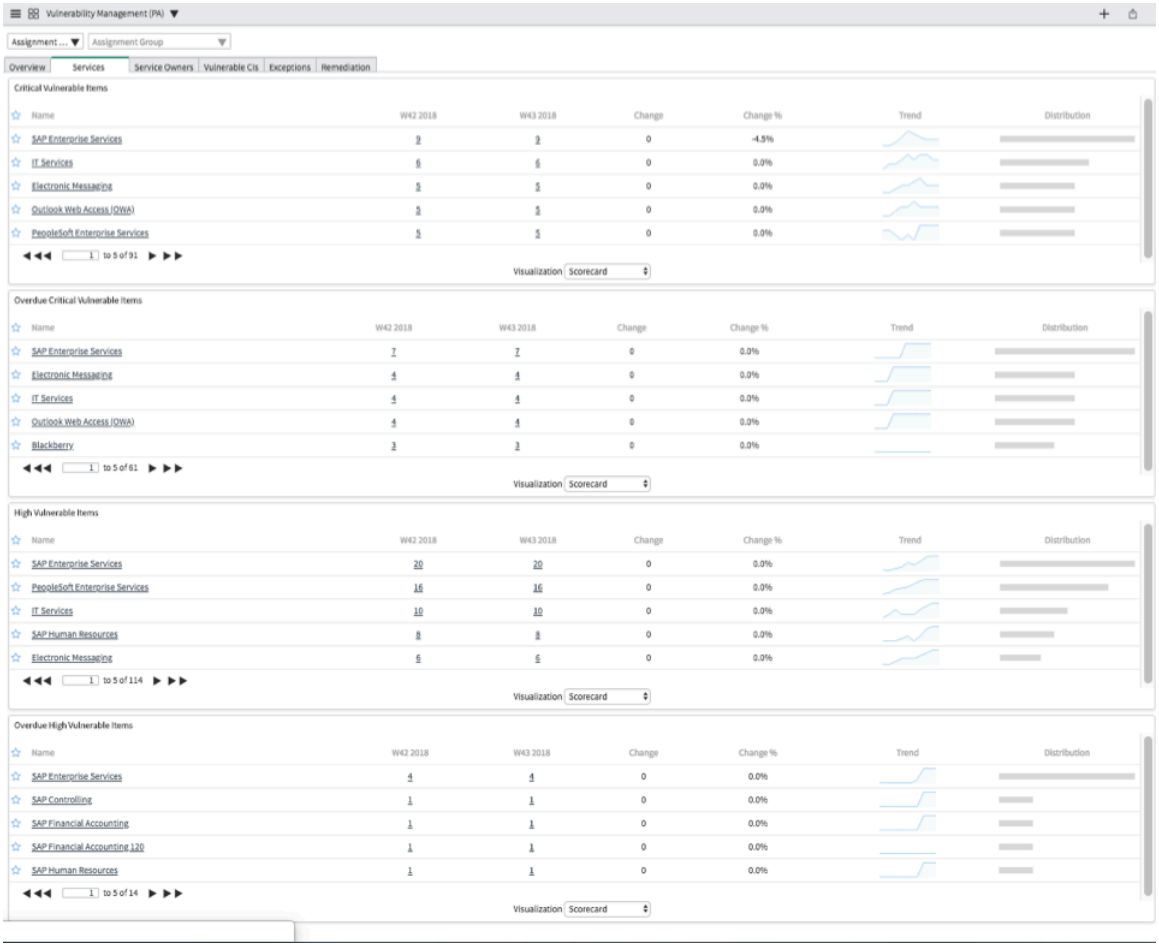


© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

비즈니스 서비스 탭

이 대시보드는 비즈니스 서비스 수준에서 취약성 위험을 노출합니다. 이 정보를 조직 전체에 공유하면 서비스 관리자가 취약성을 신속하고 사전 예방적으로 정정하고 조직을 정보 보안의 공동 책임 모델로 추진할 수 있습니다.

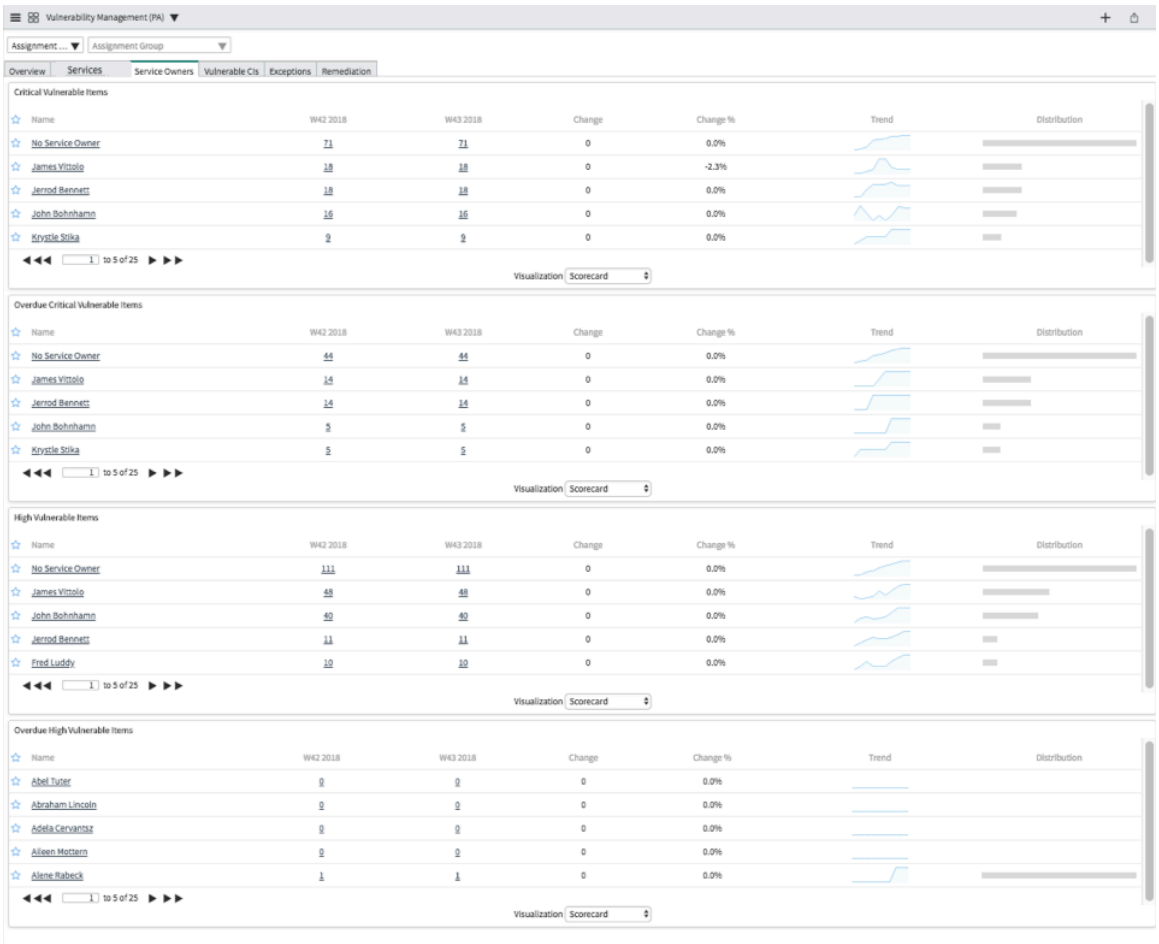
시스템 속성 sn_vul.service_classifications를 사용하여 서비스 클래스를 기술 또는 애플리케이션 서비스로 변경할 수 있습니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

서비스 소유자 탭

이 대시보드는 비즈니스 서비스 수준의 취약성 위험을 서비스 소유자(해당 비즈니스 서비스를 담당하는 임원)에게 집계합니다. 어떤 경영진이 가장 취약한 위험을 감수하고 있는지, 어떤 경영진이 신속한 정정 활동을 장려하는 데 가장 많은 도움이 필요할 수 있는지 보여줍니다.

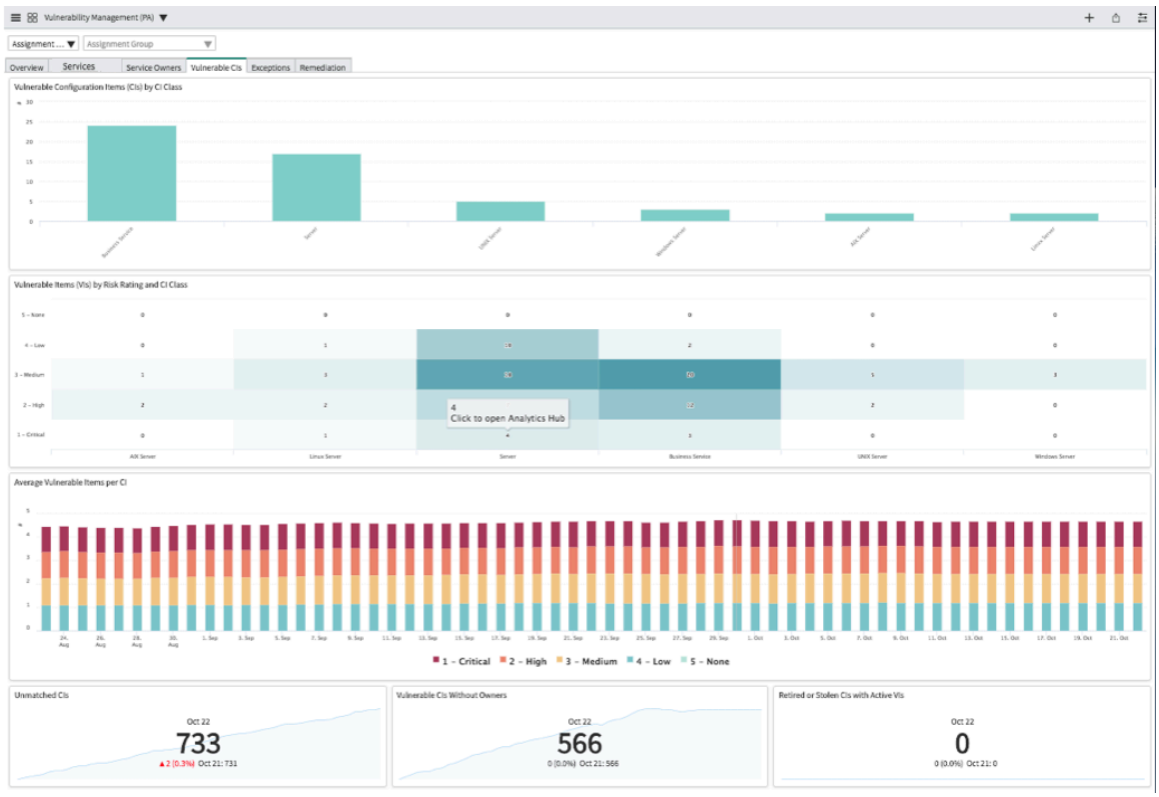


© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약한 CI 탭

이 대시보드는 활성 취약성이 있는 CI의 범위와 구성, 그리고 가장 주의를 요하는 CI 범주를 보여줍니다. 활성 취약한 항목이 있는 폐기된 자산을 식별하고 자산이 해제되었는지 확인합니다. 소유권 정보가 없는 취약한 CI의 수를 확인하여 심각한 취약성이 해당 시스템에 영향을 미치기 전에 이러한 자산의 소유자를 사전 예방적으로 식별할 수 있습니다.

취약한 CI 탭에서 소유자가 없는 취약한 CI 및 활성 VI가 있는 폐기되거나 도난당한 CI 보고서를 실시간으로 볼 수 있습니다.

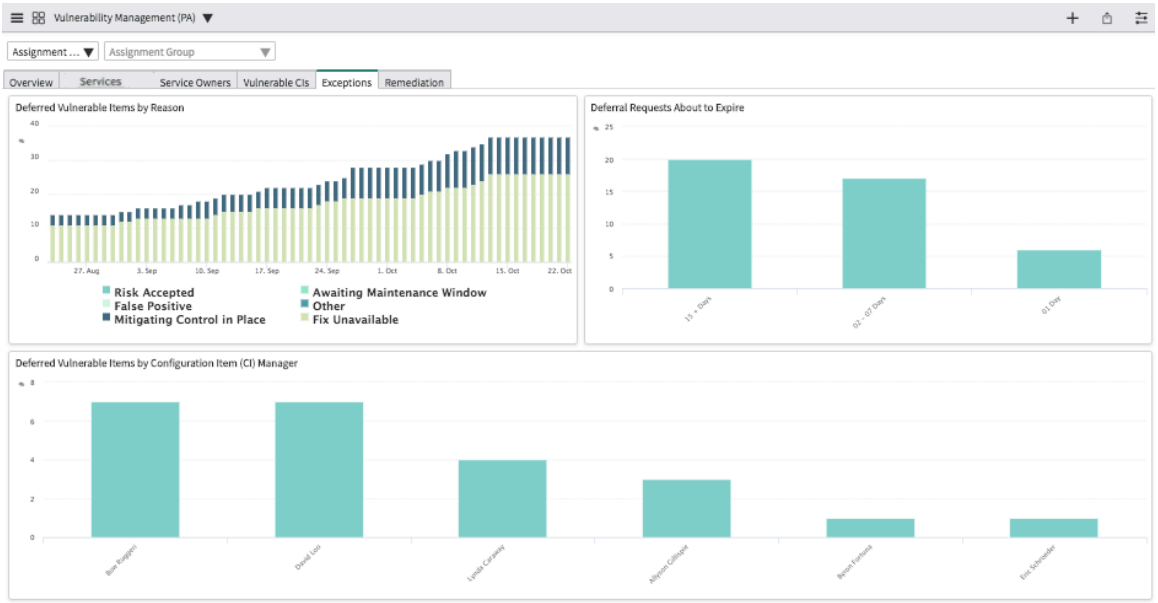


예외 탭

이 대시보드는 잠재적으로 과도한 지연으로 인해 조직이 위험을 감수하는 위치를 이해하고 정정 옵션을 재고하는 데 도움이 됩니다.

사유별, 만료되는 연기 요청별, 할당 그룹별 중요한 취약한 항목에 대한 예외 및 요청자별 예외 요청 보고서에 따라 지연된 취약한 항목을 볼 수 있습니다.

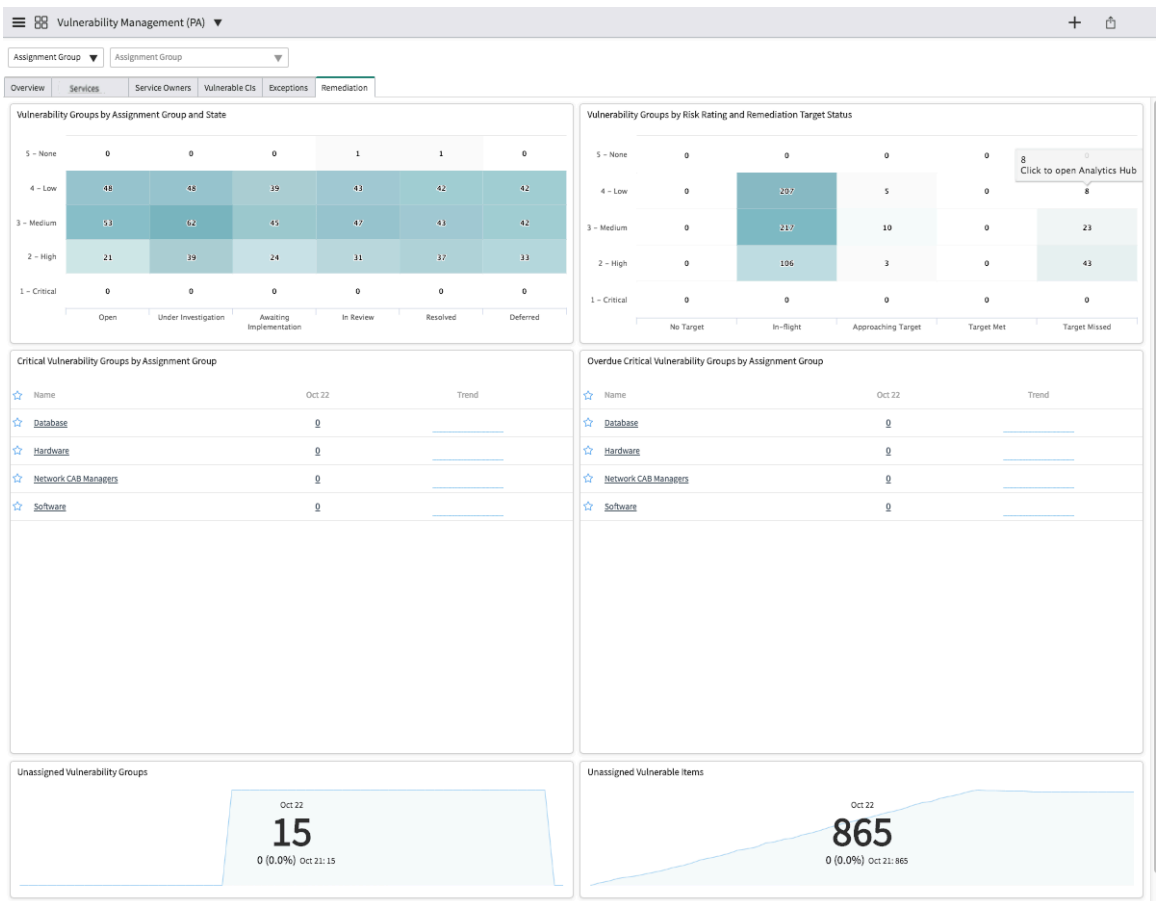
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



정정 탭

이 대시보드를 사용하면 정정 작업의 진행 상황과 완료 시 가장 많은 지원이 필요한 지원 팀을 파악할 수 있습니다.

정정 탭에서 할당되지 않은 취약한 항목 보고서를 실시간으로 볼 수 있습니다.



표시기

취약성 대응 표시기

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

애플리케이션에서 취약성 정정 진행률을 측정하고 추적하는 데 사용되는 여러 표시기가 취약성 대응 있습니다.

표시기에 대한 기록 수집 옵션은 애플리케이션에서 기본적으로 비활성화되어 있습니다 취약성 대응 . 특정 보고서를 실시간으로 볼 수 있도록 이 옵션은 비활성화되어 있습니다. 수동으로 기록 수집을 활성화하고 점수를 구성하는 기록을 보려면 이러한 표시기에서 사용하는 추세 정보를 계속 사용할 수 있습니다.

구별되는 취약성

count_active_vi 〉 0인 뚜렷한 취약성입니다. 목표는 최소화하는 것입니다.

비연기 기한 초과 중요한 취약한 항목

VI.Active 데이터 소스의 개수로, sn_vul_vulnerable_item 테이블을 사용합니다. 목표는 최소화하는 것입니다.

% 취약한 항목이 정정 대상 만족

([[### ### ## > ## ## = ## ##]] / [[### ### ##]]) * 100. 목표는 최대화하는 것입니다.

할당되지 않은 취약한 항목

담당 그룹 필드와 담당자 필드가 모두 비어 있는 모든 활성 취약한 항목입니다. 목표는 최소화하는 것입니다.

중요한 취약한 항목(서비스)

Active VI(서비스) 데이터 소스의 개수입니다. 사용 중인 테이블: sn_vul_analytics_business_services_vi. 목표는 최소화하는 것입니다.

기한 초과가 심각한 취약한 항목(서비스)

Active VI(서비스) 데이터 소스의 개수입니다. 사용 중인 테이블: sn_vul_analytics_business_services_vi. 목표는 최소화하는 것입니다.

할당되지 않은 정정 작업

할당 그룹 필드와 할당 대상 필드가 모두 비어 있는 모든 활성 정정 작업입니다. 목표는 최소화하는 것입니다.

중요한 취약한 항목

VI.Active 데이터 소스의 개수로, sn_vul_vulnerable_item 테이블을 사용합니다. 목표는 최소화하는 것입니다.

취약 항목

VI.Active 데이터 소스의 개수로, sn_vul_vulnerable_item 테이블을 사용합니다. 목표는 최소화하는 것입니다.

새로운 취약한 항목

이 값은 VI.New 데이터 소스의 개수입니다. 사용 중인 테이블: sn_vul_vulnerable_item. 목표는 최소화하는 것입니다.

취약한 구성 항목

이 값은 VI.Active 데이터 소스의 고유 개수로, sn_vul_vulnerable_item 테이블을 사용합니다. 목표는 최소화하는 것입니다.

닫힌 취약한 항목의 합산 기간

이 값은 VI.Closed 데이터 소스의 합계로, sn_vul_vulnerable_item 테이블을 사용합니다. 목표는 최소화하는 것입니다.

연기되지 않은 정정 작업

VG 데이터 소스의 개수입니다. 활성입니다. sn_vul_vulnerability 테이블을 사용합니다. 목표는 최소화하는 것입니다.

정정할 취약한 항목 중위 시간

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

[[### ### ### ## ##]]/[[### ### ##]]

중요한 기한 초과 취약한 항목(서비스)

Active VI(서비스) 데이터 소스의 개수입니다. 사용 중인 테이블: sn_vul_analytics_business_services_vi. 목표는 최소화하는 것입니다.

폐기된 구성 항목

이 값은 VI.Active 데이터 소스의 고유 개수로, sn_vul_vulnerable_item 테이블을 사용합니다. 목표는 최소화하는 것입니다.

연기 요청

활성 지연 요청 데이터 소스의 개수입니다. 사용 중인 테이블: sn_vul_change_approval. 목표는 최소화하는 것입니다.

구성 항목별 취약한 항목

이는 활성 VI가 있는 CIs 데이터 소스의 개수입니다. 사용 중인 테이블: sn_vul_analytics_vi_ci_class. 목표는 최소화하는 것입니다.

닫힌 취약한 항목

종결된 취약한 항목은 # 단위로 매일 측정됩니다. 목표는 최대화하는 것입니다.

일치하지 않는 구성 항목

CMDB의 기존 CI와 일치하지 않는 외부 공급업체 취약성 스캐너를 통해 검색된 호스트를 나열합니다.

연기되지 않은 지연 중요 정정 작업

VG 데이터 소스의 개수입니다. 활성입니다. sn_vul_vulnerability 테이블을 사용합니다. 목표는 최소화하는 것입니다.

지원 그룹이 없는 취약한 구성 항목

이 값은 VI.Open 데이터 소스의 개수이며 사용 중인 테이블: sn_vul_vulnerable_item. 목표는 최소화하는 것입니다.

연기되지 않은 중요 정정 작업

VG 데이터 소스의 개수입니다. 활성입니다. sn_vul_vulnerability 테이블을 사용합니다. 목표는 최소화하는 것입니다.

연기된 취약한 항목

VI.Active 데이터 소스의 개수로, sn_vul_vulnerable_item 테이블을 사용합니다. 목표는 최소화하는 것입니다.

매우 취약한 항목(서비스)

Active VI(서비스) 데이터 소스의 개수입니다. 사용 중인 테이블: sn_vul_analytics_business_services_vi. 목표는 최소화하는 것입니다.

활성 취약한 항목이 있는 고유한 구성 항목

이 값은 활성 VI가 있는 CIs 데이터 소스의 고유 개수입니다. 사용 중인 테이블: sn_vul_analytics_vi_ci_class. 목표는 최소화하는 것입니다.

구성 항목별 취약한 항목의 평균 수

[[## ### ##]]/[[### CI]]. 목표는 최소화하는 것입니다.

정정 작업

VG 데이터 소스의 개수입니다. 활성입니다. sn_vul_vulnerability 테이블을 사용합니다. 목표는 최소화하는 것입니다.

지연된 핵심 취약한 항목

VI.Active 데이터 소스의 개수로, sn_vul_vulnerable_item 테이블을 사용합니다. 목표는 최소화하는 것입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

연기 요청(생성됨)

테이블 sn_vul_change_approval를 사용 중인 데이터 소스 Closed.Requests의 개수입니다. 목표는 최소화하는 것입니다.

세부 항목

다음 세부 항목 이름이 대시보드의 지표에 적용됩니다.

- 기간
- 종결 연령
- 담당 그룹
- CI 클래스
- CI 관리자
- 지연 기간
- 연기 사유
- 예외 요청자
- 공격 벡터 악용
- 악용 존재
- 악용 기술 수준
- 정정 대상 규칙
- 정정 대상 상태
- 정정 대상 상태(닫힘)
- 위험 등급
- 서비스
- 서비스 중요도
- 서비스 소유자
- 심각도
- 상태

주:
VI(취약한 항목)에 대한 기간 및 종결된 기간 계산을 사용자 지정하면 이러한 메트릭이 포함된 퍼포먼스 분석(PA) 보고서가 급격히 증가하거나 감소할 수 있습니다. VI의 기간 및 종결 기간 계산을 사용자 지정하는 방법에 대한 자세한 내용은 KB1703270 KB 문서를 참조하십시오.

세부 항목 소스

- 할당 그룹: VI 또는 RT 보고서에 적용
- 익스플로잇 존재: VI 보고서에 적용됩니다.
- 공격 벡터 악용: VI 보고서에 적용됩니다.
- 악용 기술 수준: VI 보고서에 적용됩니다.
- 정정 대상 상태: VI 및 RT 보고서에 적용됩니다.
- 위험 등급: VI 및 RT 보고서에 적용됩니다.
- 상태: VI 및 RT 보고서에 적용됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

데이터 시각화

제목	유형	설명
취약성	단일 점수	하나 이상의 활성 취약한 항목과 연결된 취약성 수입니다.
취약한 항목(VI)	단일 점수	활성(종결되지 않은) 취약한 항목 수입니다.
취약한 CI(구성 항목)	단일 점수	하나 이상의 활성 취약한 항목과 연결된 구성 항목(CI) 수입니다.
정정 작업	단일 점수	활성(종결 되지 않은) 정정 작업의 수입니다.
위험 등급별 취약한 항목	막대	선택한 시간 범위 동안 위험 등급별로 그룹화된 활성 취약한 항목 수입니다.
연령 및 위험 등급별 취약한 항목	히트맵	위험 등급 및 기간(일)별로 그룹화된 활성 취약한 항목 수입니다.
정정 대상을 만족하는 VI	단일 점수	현재 및 이전 분기에서 정정 목표 날짜를 달성한 종결된 취약한 항목의 비율입니다. 정정 목표는 마지막으로 개시된 날짜와 일 수(24시간 단위로 측정)의 합계로 계산됩니다.
VI 평균 정정 시간(MTTR)	단일 점수	취약한 항목을 정정(종결)하기 위한 평균 시간으로, 30일 이동 평균으로 표시됩니다. **주:** 종결 연령의 값은 데이터가 수집될 때 계산됩니다. 값은 last_opened 날짜와 수집 작업의 날짜 및 시간 차이입니다.
기한이 근접한 중요 정정 작업	단일 점수	정정 목표 날짜에 근접한 활성 정정 작업 수입니다. 정정 작업의 정정 목표 날짜가 그룹의 활성 취약한 항목에 속한 날짜와 가장 근접한 날짜로 설정됩니다. 정정 목표는 마지막으로 개시된 날짜와 일 수(24시간 단위로 측정)의 합계로 계산됩니다. 이 보고서는 지연된 정정 작업을 제외합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

제목	유형	설명
새로운 또는 닫힌 취약한 항목	막대	선택한 시간 범위 동안의 신규 및 종결된 취약한 항목 수입니다. 주: 종결 연령의 값은 데이터가 수집될 때 계산됩니다. 값은 last_opened 날짜와 수집 작업의 날짜 및 시간 차이입니다.
정정 대상 상태별 닫힌 취약한 항목	막대	선택한 시간 범위 동안 정정 목표 상태별로 그룹화된 종결된 취약한 항목 수입니다. 주: 종결 연령의 값은 데이터가 수집될 때 계산됩니다. 값은 last_opened 날짜와 수집 작업의 날짜 및 시간 차이입니다.
담당 그룹별 중요한 취약한 항목	목록 및 라인	담당 그룹별로 그룹화된 위험한 위험 등급의 활성 취약한 항목 수입니다.
담당 그룹별 기한 초과 중요한 취약한 항목	목록 및 라인	위험한 위험 등급의 활성 취약한 항목 수 및 할당 그룹별로 그룹화된 해당 항목의 지난 정정 목표 날짜입니다. 정정 목표는 마지막으로 개시된 날짜와 일 수(24시간 단위로 측정)의 합계로 계산됩니다. 지연된 취약한 항목은 이 보고서에서 제외됩니다.

비즈니스 서비스

이름	유형	설명
중요한 취약한 항목	목록, 라인 및 배포 표시줄	비즈니스 서비스별로 그룹화된 위험한 위험 등급의 활성 취약한 항목 수입니다. 이번 주와 지난 주의 주간 평균, 2주간의 차이(개수 및 백분율) 및 추세를 표시합니다. 분포 표시줄에는 성과표의 현재 페이지에 있는 모든 값 간의 차이가 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

비즈니스 서비스

이름	유형	설명
기한 초과 중요한 취약한 항목	목록, 라인 및 배포 표시줄	위험한 위험 등급의 활성 취약한 항목 수 및 비즈니스 서비스별로 그룹화된 해당 항목의 지난 정정 목표 날짜입니다. 이번 주와 지난 주의 주간 평균, 2주간의 차이(개수 및 백분율) 및 추세를 표시합니다. 분포 표시줄에는 성과표의 현재 페이지에 있는 모든 값 간의 차이가 표시됩니다. 지연된 취약한 항목은 이 보고서에서 제외됩니다.
매우 취약한 항목	목록, 라인 및 배포 표시줄	비즈니스 서비스별로 그룹화된 높은 위험 등급의 활성 취약한 항목 수입니다. 이번 주와 지난 주의 주간 평균, 2주간의 차이(개수 및 백분율) 및 추세를 표시합니다. 분포 표시줄에는 성과표의 현재 페이지에 있는 모든 값 간의 차이가 표시됩니다.
기한 초과 심각한 취약한 항목	목록, 라인 및 배포 표시줄	높은 위험 등급의 활성 취약한 항목 수 및 비즈니스 서비스별로 그룹화된 해당 항목의 지난 정정 목표 날짜입니다. 이번 주와 지난 주의 주간 평균, 2주간의 차이(개수 및 백분율) 및 추세를 표시합니다. 분포 표시줄에는 성과표의 현재 페이지에 있는 모든 값 간의 차이가 표시됩니다. 지연된 취약한 항목은 이 보고서에서 제외됩니다.

서비스 소유자

이름	유형	설명
중요한 취약한 항목	목록, 라인 및 배포 표시줄	비즈니스 서비스 소유자별로 그룹화된 위험한 위험 등급의 활성 취약한 항목 수입니다. 이번 주와 지난 주의 주간 평균, 2주간의 차이(개수 및 백분율) 및 추세를 표시합니다. 분포 표시줄에는 성과표의 현재 페이지에 있는 모든 값 간의 차이가 표시됩니다.
기한 초과 중요한 취약한 항목	목록, 라인 및 배포 표시줄	위험한 위험 등급의 활성 취약한 항목 수 및 비즈니스 서비스 소유자별로 그룹화된 해당 항목의 지난 정정 목표 날짜입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

서비스 소유자

이름	유형	설명
		이번 주와 지난 주의 주간 평균, 2주간의 차이(개수 및 백분율) 및 추세를 표시합니다. 분포 표시줄에는 성과표의 현재 페이지에 있는 모든 값 간의 차이가 표시됩니다. 지연된 취약한 항목은 이 보고서에서 제외됩니다.
매우 취약한 항목	목록, 라인 및 배포 표시줄	비즈니스 서비스 소유자별로 그룹화된 높은 위험 등급의 활성 취약한 항목 수입니다. 이번 주와 지난 주의 주간 평균, 2주간의 차이(개수 및 백분율) 및 추세를 표시합니다. 분포 표시줄에는 성과표의 현재 페이지에 있는 모든 값 간의 차이가 표시됩니다.
기한 초과 심각한 취약한 항목	목록, 라인 및 배포 표시줄	높은 위험 등급의 활성 취약한 항목 수 및 비즈니스 서비스 소유자별로 그룹화된 해당 항목의 지난 정정 목표 날짜입니다. 이번 주와 지난 주의 주간 평균, 2주간의 차이(개수 및 백분율) 및 추세를 표시합니다. 분포 표시줄에는 성과표의 현재 페이지에 있는 모든 값 간의 차이가 표시됩니다. 지연된 취약한 항목은 이 보고서에서 제외됩니다.

취약한 **CI**

이름	유형	설명
CI 클래스별 취약한 CI(구성 항목)	막대	CMDB에서 CI 클래스별로 그룹화된 활성 취약성이 있는 구성 항목 수입니다.
CI 클래스별 취약한 항목(VI)	트리맵	CI 클래스별로 세분화된 활성 VI 수입니다.
CI당 취약한 항목 평균	막대	구성 항목에 속하는 취약한 항목의 평균 개수입니다 (위험 등급별로 그룹화됨).
일치하지 않는 CI	단일 점수	CMDB의 기존 CI와 일치하지 않는 임포트된 구성 항목 수입니다.
지원 그룹이 없는 취약한 CI	단일 점수	할당된 지원 그룹이 없는 취약한 구성 항목 수입니다.
활성 VI가 있는 폐기된 또는 도난당한 CI	단일 점수	활성 취약한 항목이 있는 CMDB에서 폐기 됨 또는 도난 됨으로 표시된 구성 항목 수입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예외

이름	유형	설명
사유별 연기된 취약한 항목	막대	지연 이유별로 그룹화된 지연된 취약한 항목 수입니다.
만료 예정인 연기 요청	막대	검토를 위해 재개시하려는 정정 작업 또는 취약한 항목과 연관된 지연 요청 수입니다. 다시 열릴 때까지 남은 일 수로 그룹화됩니다. 이메일 알림이 정의되어 있으면 이메일이 전송됩니다.
CI(구성 항목) 관리자가 연기한 취약한 항목	막대	연결된 구성 항목에 대해 관리자가 그룹화한 지연된 취약한 항목 수입니다.

정정

이름	유형	설명
위험 등급 및 상태별 정정 작업	히트맵	위험 등급 및 상태별로 그룹화된 활성 정정 작업의 수입니다.
위험 등급 및 정정 대상 상태별 정정 작업	히트맵	위험 등급 및 정정 목표 상태별로 그룹화된 활성 작업 수입니다. 지연된 취약한 항목은 이 보고서에서 제외됩니다.
할당 그룹별 중요 정정 작업	목록 및 라인	할당 그룹별로 그룹화된 위험 등급이 있는 활성 정정 작업의 수입니다. 이 보고서는 지연된 정정 작업을 제외합니다.
할당 그룹별 지연 중요 정정 작업	목록 및 라인	할당 그룹별로 그룹화되어 임계 위험 등급이 있고 수정 대상 날짜가 지난 활성 정정 작업의 수입니다. 이 보고서는 지연된 정정 작업을 제외합니다.
할당되지 않은 정정 작업	단일 점수	담당자 또는 할당 그룹이 없는 활성 정정 작업 수입니다.
할당되지 않은 취약한 항목	단일 점수	담당자 또는 담당 그룹이 없는 활성 취약한 항목 수입니다.

실시간으로 **[PA]** 보고서 보기 취약성 대응용 퍼포먼스 분석

가장 중요한 취약한 항목(VI)을 관리하고 신속하게 정정하려면 취약성 관리(PA) 대시보드에서 요청 시 실시간으로 보고서를 확인합니다. 이 취약성 대응용 퍼포먼스 분석 애플리케이션은 .ServiceNow Store

시작하기 전에

필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)
가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

에 대한 취약성 대응용 퍼포먼스 분석보고서에 대한 자세한 내용은 취약성 관리(PA) 대시보드를 참조하십시오.

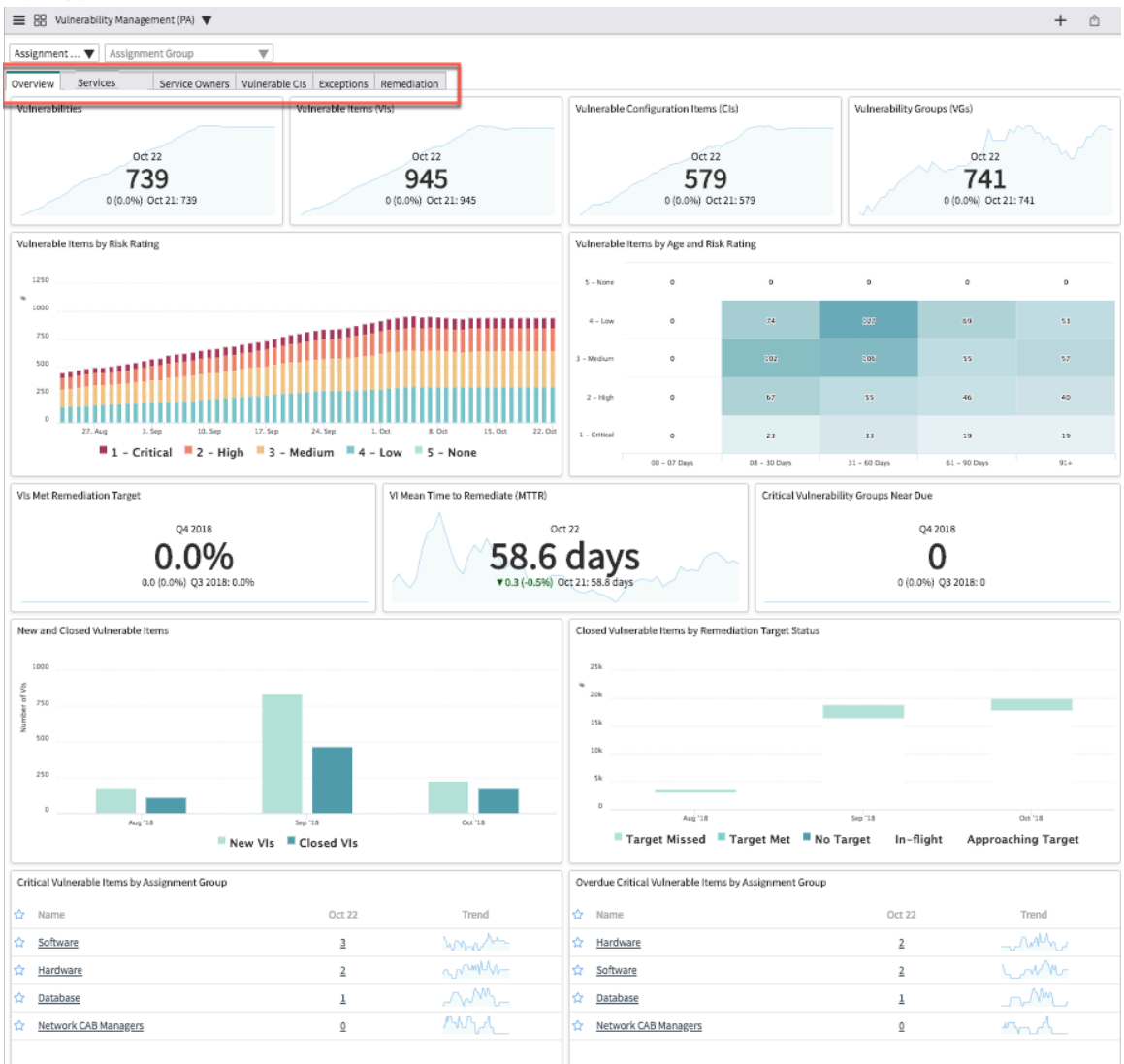
애플리케이션의 설정 및 설치에 취약성 대응용 퍼포먼스 분석 대한 자세한 내용은 문서를 참조하십시오 (PA) 애플리케이션 설치 및 구성 취약성 대응용 퍼포먼스 분석.

표시되지 않은 경우 대시보드를 보려면 취약성 대응 > 개요. 대시보드 상단에 보고서 탭이 표시됩니다.

의 취약성 대응버전 19.0부터 이 대시보드는 New Experience UI에서도 볼 수 있습니다. 새 UI에서 대시보드를 보려면 다음으로 이동합니다. 작업 공간 > 취약성 관리자 작업 공간 을 클릭하고 대시보드 아이콘을 클릭합니다. 역할에 따라 기본 대시보드가 표시됩니다. 다른 대시보드를 보려면 대시보드 이름 옆에 있는 드롭다운을 클릭합니다. 자세한 내용은 취약성 관리자 작업 공간의 대시보드 및 IT 정정 작업 공간의 대시보드를 참조하십시오.

주:
Tokyo에 있는 경우 Next Experience UI에서 대시보드를 볼 수 있지만 일부 기능 손실이 있습니다.

개요 탭



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

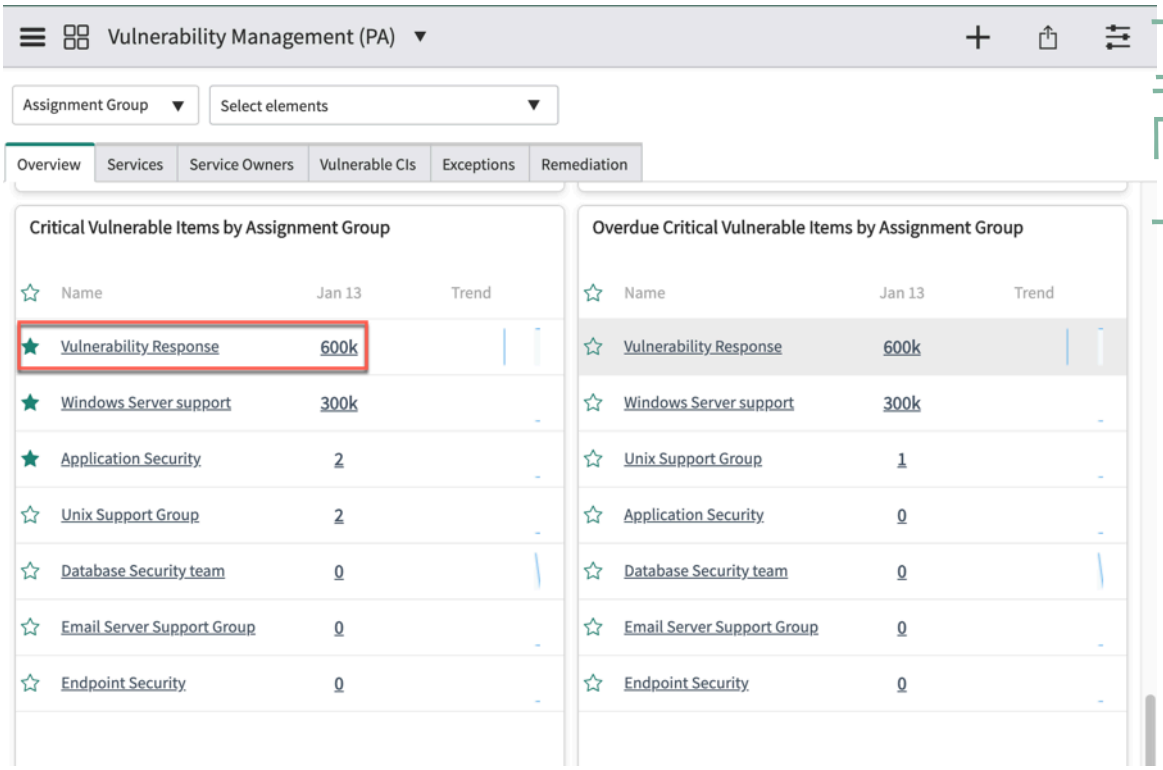
취약성 관리(PA) 대시보드의 탭에서 다음 보고서를 실시간으로 봅니다.

- 개요 탭
  - 담당 그룹별 중요한 취약한 항목
- 취약한 CI 탭:
  - 소유자가 없는 취약한 CI
  - 활성 VI가 있는 폐기된 또는 도난당한 CI
- 예외 탭:
  - 사유별 연기된 취약한 항목
  - 만료 예정인 연기 요청
  - CIO 관리자가 연기한 취약한 항목
- 정정 탭:
  - 할당되지 않은 취약한 항목

실시간 보고서를 포함하는 탭 중 하나를 선택한 상태에서 실시간 점수를 보려면 다음 단계를 수행합니다.

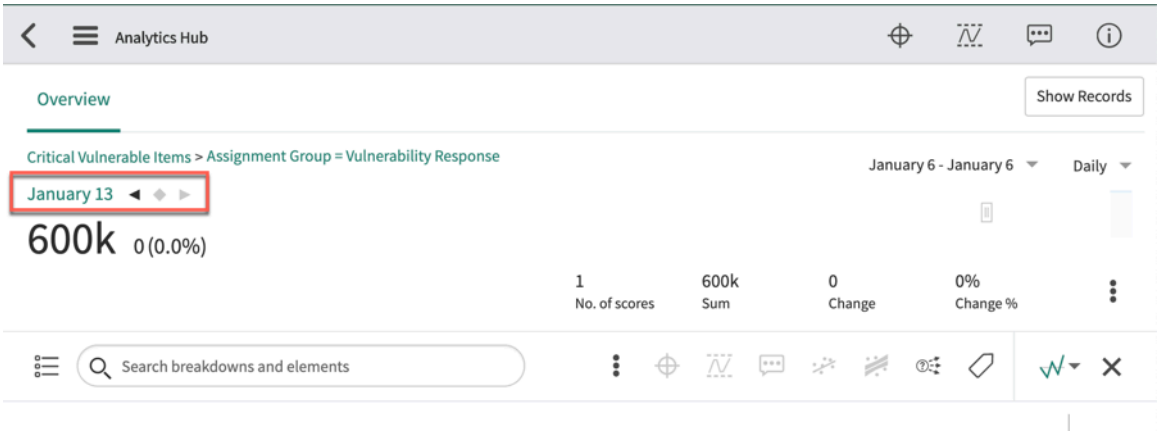
프로시저

1. 보고서(예: 할당 그룹별 중요한 취약한 항목)에서 표시되는 링크 중 하나를 클릭합니다.



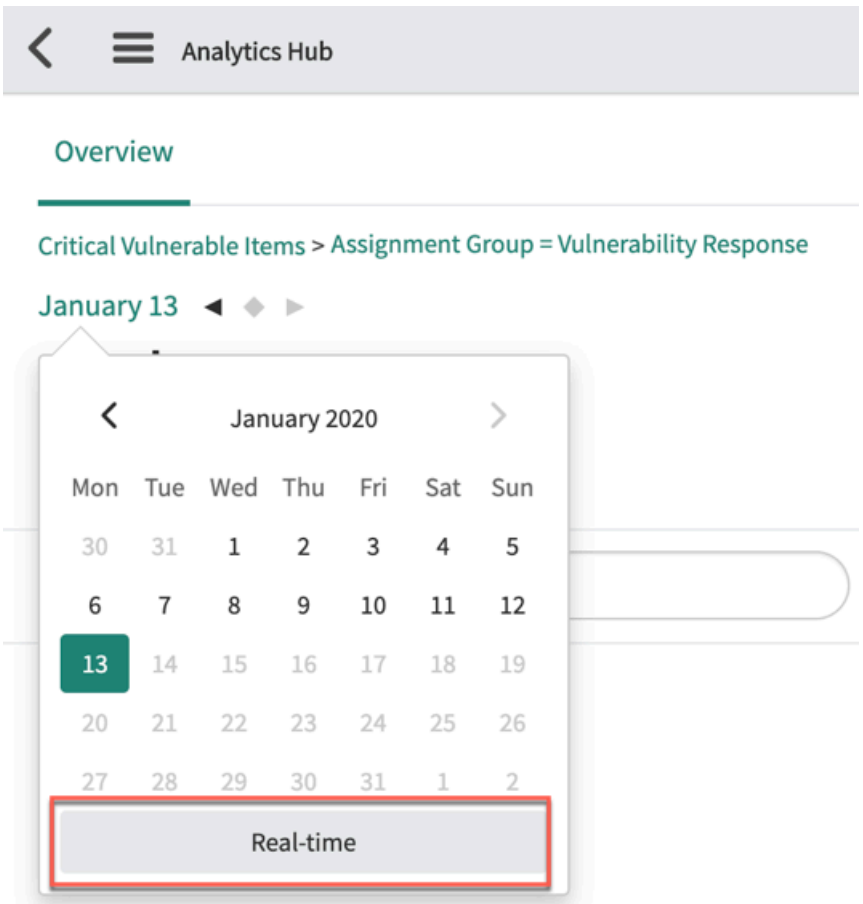
2. 표시되는 기록에서 날짜를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



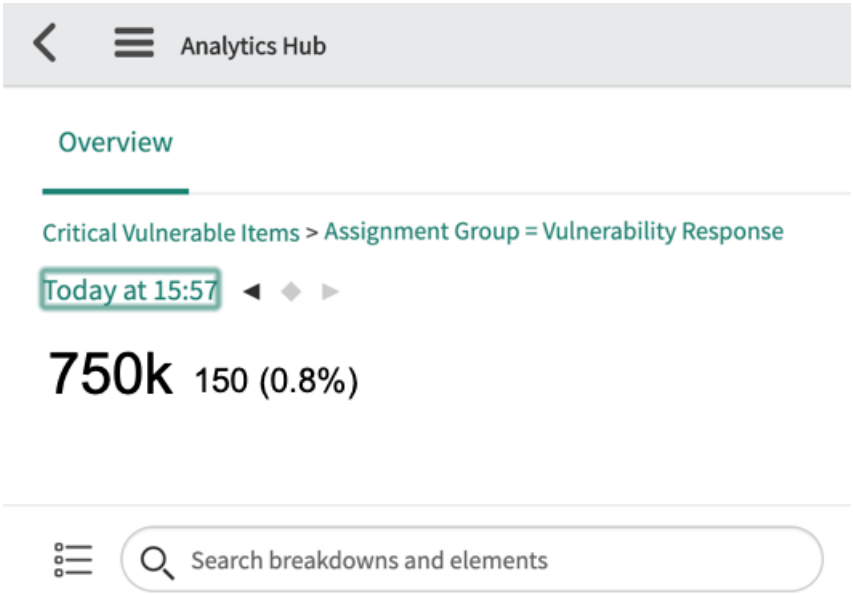
3. 표시되는 달력에서 실시간을 클릭합니다.

보고서에서 실시간 점수를 지원하지 않으면 달력에 실시간 단추가 표시되지 않습니다.



값이 업데이트되는 데 약간의 시간이 걸릴 수 있습니다. 현재 날짜, 기록, 마지막 보고서 이후의 새 기록 수 및 마지막 보고서의 변경 비율도 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 옵션: 실시간 보고서가 표시된 보고서를 구성하는 기록을 보려면 오른쪽 상단에서 기록 표시를 클릭합니다.
   점수를 구성하는 레코드 목록이 표시됩니다.

[PA]에 퍼포먼스 분석 대한 취약성 대응 표시기 보기

인스턴스의 취약성 데이터를 나타내는 자동화되고 공식화된 퍼포먼스 분석 표시기를 봅니다.

시작하기 전에

퍼포먼스 분석 - 콘텐츠 팩 취약성 대응 애플리케이션에서 표시기에 대한 기록 수집 옵션은 기본적으로 비활성 상태입니다. 특정 보고서를 실시간으로 볼 수 있도록 이 옵션은 비활성화되어 있습니다. 수동으로 기록 수집을 활성화하고 점수를 구성하는 기록을 보려면 이러한 표시기에서 사용하는 추세 정보를 계속 사용할 수 있습니다.

주:
표시기에서 기록 수집을 활성화하면 성능에 영향을 미칠 수 있으며 데이터 수집 작업을 실행하는 데 필요한 시간과 메모리가 상당히 길어질 수 있습니다.

가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음) 또는 pa.viewer

이 태스크 정보

취약성 대응 에는 자동 표시기와 공식화된 표시기가 모두 있습니다.

주요 용어

PA 표시기
: 비즈니스 서비스, 활동 또는 조직 행동에 대해 정기적인 간격으로 수행되는 성과 측정을 정의합니다(예: 연기되지 않은 기한 초과 중요 취약한 항목).

PA 표시기 소스
: 하나의 테이블 또는 데이터베이스 뷰에서 기록을 필터링하는 데이터 세트(예: VI Active).

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

기록 수집

이 옵션을 사용하면 메모리에 기록이 저장되고 분석 허브에 액세스할 수 있습니다.

세부 항목

세부 항목은 수집된 기록을 필터링하고 그룹화합니다. 고장은 특히 그 수와 다양성이 증가함에 따라 메모리 사용을 증가시킬 수 있습니다.

세부 항목 제외

제외는 특정 세부 항목을 제거하므로 메모리 소비를 줄일 수 있습니다.

프로시저

1. 자동 표시기를 보려면 다음으로 이동 퍼포먼스 분석 > 표시기 > 자동 표시기.
2. 공식화된 표시기를 보려면 다음으로 이동하십시오. 퍼포먼스 분석 > 수식 표시기.

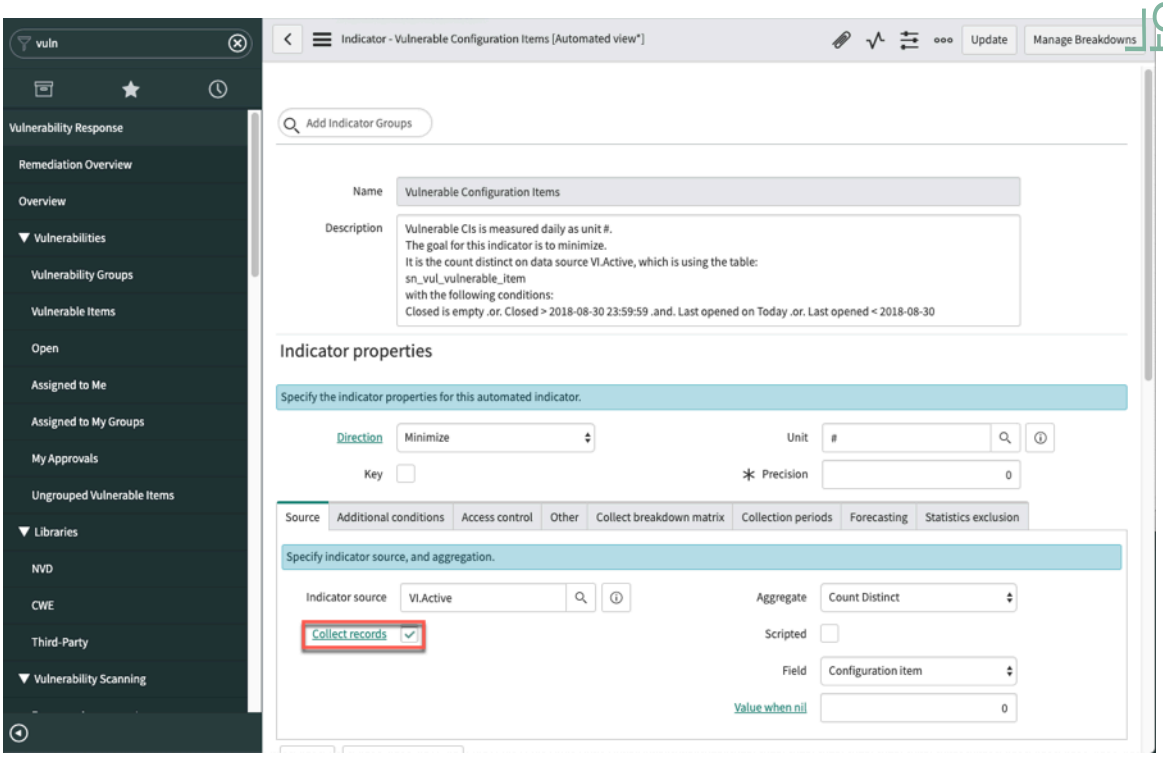
   표시기에 대한 자세한 내용은 퍼포먼스 분석 표시기를 참조하십시오.
3. 두 경우 모두 애플리케이션 > 퍼포먼스 분석.

   주:

   기본 뷰에 없는 경우 페이지의 왼쪽 상단에 있는 기어 아이콘( )을 사용하여 애플리케이션 열을 추가합니다. 그러면 애플리케이션 열이 검색 드롭다운 메뉴에 표시됩니다.
4. 옵션: 퍼포먼스 분석 취약성 대응 표시기에서 기록 수집을 활성화하려면 다음 단계를 따르십시오.

   a. 자동화된 표시기 목록이 표시되면 이름 열에서 기록 수집을 활성화하려는 표시기를 클릭합니다. 표시기 기록이 표시됩니다.

   b. 소스 탭이 선택된 표시기 속성 섹션에서 기록 수집 확인란을 선택합니다.



   c. 계속하려면 하나를 선택합니다.

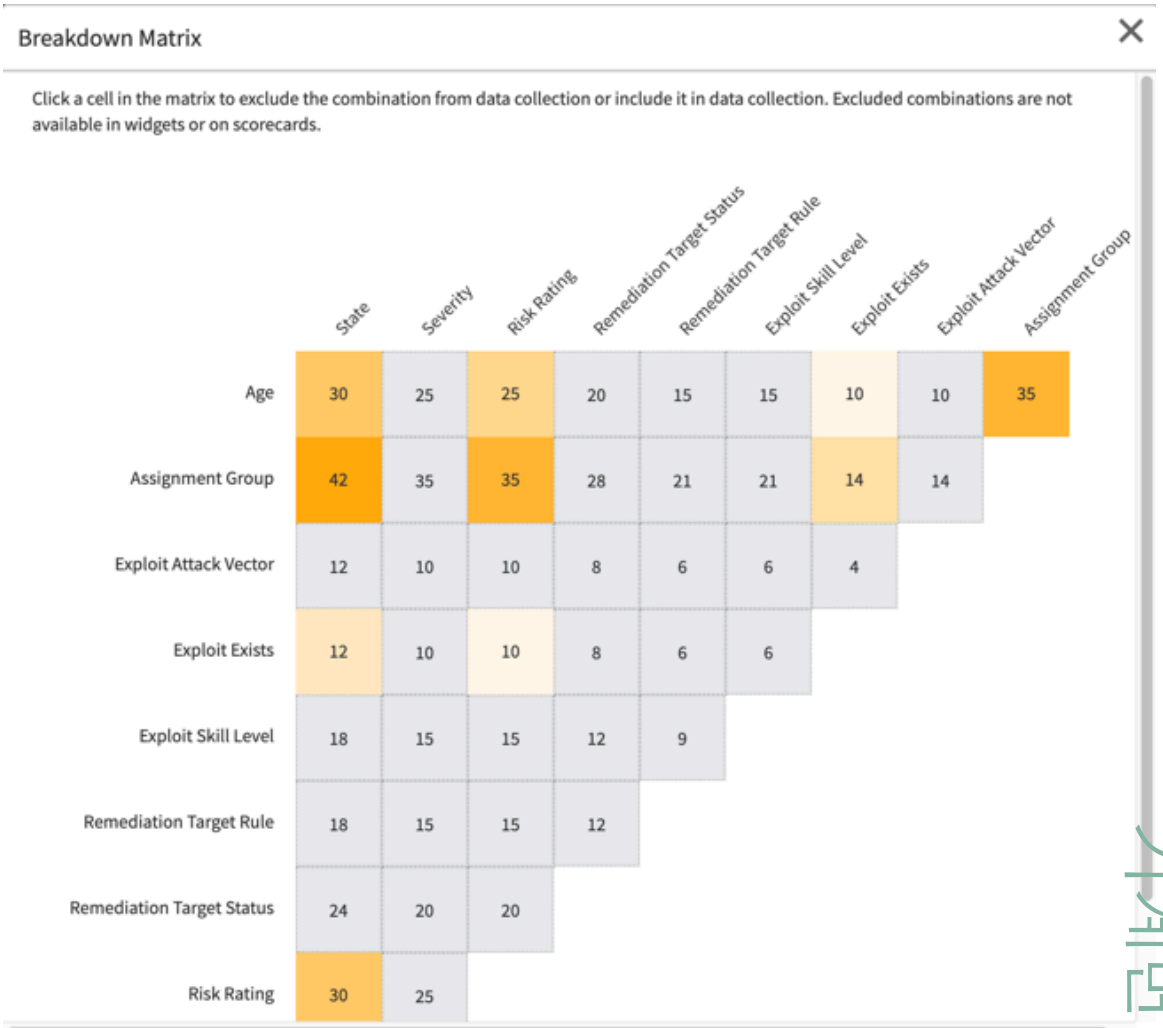
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵션	설명
업데이트	편집 내용을 저장하고 표시기 목록으로 돌아갑니다.
세부 항목 관리 주: 두 번째 수준 세부 항목을 다시 활성화하도록 선택하면 메모리 소비가 크게 증가하고 데이터 수집 작업이 느려질 수 있습니다. 기본적으로 다음 표시기에는 두 번째 수준 세부 항목 제외가 적용되었습니다. ▪ 취약한 구성 항목 ▪ 폐기된 CI ▪ 지연된 VI	나열된 표시기의 두 번째 수준 세부 항목을 다시 활성화하거나 다른 표시기의 세부 항목을 편집합니다. (Optional) 퍼포먼스 분석 세부 항목에 대한 자세한 내용은 퍼포먼스 분석 세부 항목을 참조하십시오.

d. 세부 항목 관리를 클릭합니다.

e. 표시되는 양식에서 세분화 매트릭스 구성을 클릭합니다.
세분화 매트릭스 양식이 표시됩니다. 제외된 조합이 선택되어 다음 그림과 같이 색상으로 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



f. 제외를 제거하고 제외된 조합을 다시 활성화하려면 선택한 셀을 클릭합니다.

g. 양식의 오른쪽 상단에서 닫기 를 클릭하여 세분화 관리 양식을 되돌립니다.

h. 뒤로 화살표를 클릭하여 표시기 기록으로 돌아갑니다.

i. 업데이트를 클릭하여 편집 내용을 저장하고 표시기 목록으로 돌아갑니다.

집계된 보고서 프레임워크

집계된 보고서 프레임워크를 사용하면 성능 향상을 위해 복잡하고 실행 시간이 긴 즉석 쿼리가 포함된 데이터에 대한 보고서를 만들 수 있습니다.

집계된 보고서 프레임워크는 다음을 통해 성과를 개선합니다.

- 더 적은 리소스를 사용하고 보고서를 더 빠르게 렌더링합니다.
- 데이터 집계와 집계 및 세부 항목 재사용(그룹화 기준)
- 데이터베이스에 대한 쿼리 줄이기

취약한 항목이 백만 개 이상 있는 경우 표준 보고서와 함께 Vulnerability Response Common에 제공된 집계 보고서 프레임워크를 사용합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필요한 역할

이 솔루션과 관련된 역할과 작업은 다음과 같습니다.

- ServiceNow AI Platform관리자(admin): 이 플랫폼 분석 솔루션을 설치 및 활성화하고 시스템 속성을 필요에 따라 변경합니다.
- 퍼포먼스 분석 관리자(pa_admin): 집계, 위젯 및 대시보드를 검토합니다. 데이터 수집을 설정 및 시작합니다. 적절한 이해 관계자와 대시보드를 공유합니다.
- 관리자(sn_vul_cmn.admin): 집계를 생성합니다.
- VR write(sn_vul_cmn.write): 집계 및 집계된 결과에서 데이터를 편집합니다.
- VR 읽기(sn_vul_cmn.read): 집계 및 집계된 결과의 데이터를 검토합니다.
- 취약성 분석가(sn_vul.vulnerability_analyst): 집계된 결과를 검토합니다.

관련 정보

소스 데이터에 대한 집계 구성

여러 집계를 동시에 실행

동시에 실행할 수 있는 집계 수 구성

집계를 사용하여 보고서 생성

소스 데이터에 대한 집계 구성

테이블에 기록된 ServiceNow 비즈니스 프로세스에서 특정 패싯의 성과를 분석하려면 패싯과 관련된 집계를 만들고 이 집계에 대한 보고서를 만듭니다.

시작하기 전에
필요한 역할: sn_vul_cmn.admin

프로시저

1. 다음으로 이동 모두 〉 집계된 보고서 〉 집계 정의 〉 모두 을 클릭하고 신규를 클릭합니다.
2. 이름 필드에서 집계에 설명적인 이름을 지정합니다.
3. 설명 필드에 집계에 대한 간략한 설명을 입력합니다.
4. 소스 탭의 필드에 내용을 입력합니다.

소스 탭 필드

필드	설명
테이블	보고서의 데이터를 가져올 테이블입니다. 이 드롭다운에는 앱 보안 공통, app-vul, app-vulc, app-vul-container 및 애플리케이션 취약성 테이블만 포함됩니다.
집계 기능	필드에서 선택한 열에 적용할 기능입니다. ○ 개수: 기록 수입니다. ○ 합계: 필드에서 선택한 열의 값 합계입니다. ○ 평균: 필드에서 선택한 열에 있는 모든 값의 평균입니다. ○ 최대값: 필드에서 선택한 열의 최대값입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	○ 최소: 필드에서 선택한 열의 최소값입니다. ○ 고유 카운트: 필드에서 선택한 열의 고유 값입니다.
필드	기능을 적용할 열입니다. 주: 집계 함수 필드에서 카운트를 선택하면 이 필드가 표시되지 않습니다.

5. 추가 조건 탭에서 조건 필드에 조건을 제공하여 집계된 결과를 가져올 특정 기록 세트를 선택합니다.
6. 그룹화 기준 탭에서 데이터를 그룹화하거나 스택할 테이블의 열을 선택합니다.
   세부 항목을 최대 두 개까지 선택할 수 있습니다.

   필드별 그룹에서 날짜 열을 선택하면 추세 기준 필드가 나타납니다. 추세 기준 필드의 옵션을 선택하여 주, 일, 분 등으로 분류된 집계 결과를 얻을 수 있습니다.
7. 일정 탭에서 집계를 실행하여 데이터를 가져올 수 있는 빈도를 정의하는 집계 일정을 선택하거나 만듭니다.
   집계 일정을 생성하려면 다음 문서를 참조하십시오 여러 집계를 동시에 실행.

   주:
   비활성 집계 정의에 대해 집계 실행을 예약할 수 없습니다.
8. 제출을 클릭하여 집계를 만듭니다.
   집계가 집계 목록에 나타납니다. 미리 정의된 빈도로 집계가 실행되고, 모든 실행에 대한 예약된 실행 관련 목록에 실행 날짜 및 시간과 함께 기록이 생성됩니다.
9. 다음으로 이동 모두 〉 집계된 결과 을 클릭하고 집계를 열어 집계된 결과와 예약된 실행을 확인합니다.
   집계된 결과는 집계된 결과 관련 목록에 나열됩니다. 집계 실행에 실패하면 예약된 실행 관련 목록에서 메모 열을 참조하여 자세한 내용을 확인하십시오.
10. 옵션: 집계 일정에 관계없이 집계 결과를 수집하려면 지금 실행을 선택합니다.
    진행 중일 때 예약된 실행을 종료하면 집계된 결과가 변경되지 않습니다. 집계를 삭제하거나 비활성화할 수도 있습니다.

다음에 수행할 작업

집계를 사용하여 보고서를 생성합니다. 집계를 사용하여 보고서를 만드는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 집계를 사용하여 보고서 생성.

관련 정보

집계된 보고서 프레임워크

여러 집계를 동시에 실행

동시에 실행할 수 있는 집계 수 구성

집계를 사용하여 보고서 생성

여러 집계를 동시에 실행

단일 집계 일정을 사용하여 여러 집계의 실행을 예약할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_vul_cmn.admin

이 태스크 정보
6개의 집계를 동시에 실행하려고 한다고 가정합니다. 집계 일정을 만들고 여기에 모든 집계를 추가합니다. 이러한 집계는 정의된 빈도와 시간에 실행됩니다.

프로시저

1. 다음으로 이동 모두 〉 집계된 보고서 〉 일정.
2. 새로 만들기를 선택합니다.
3. 집계 일정 양식의 필드에 내용을 입력합니다.

필드	설명
일정 이름	집계 일정의 이름입니다.
작업 예약	집계를 실행해야 하는 빈도를 정의하는 예약된 스크립트 실행입니다. 새로 만들기 버튼을 선택하여 일정 작업을 만들 수 있습니다.

4. 제출을 선택합니다.
   집계 일정이 집계 일정 목록에 나타납니다.
5. 집계 일정을 엽니다.
6. 편집을 선택하고, 집계 목록에 집계를 추가하고, 저장을 선택합니다.
   선택한 집계가 집계 관련 목록에 나타납니다.

   주:
   일정에 비활성 집계를 추가하면 예약된 실행이 시작되지 않습니다.

7. 업데이트를 선택합니다.
   이러한 집계는 집계 일정에 정의된 빈도로 실행됩니다.

관련 정보

집계된 보고서 프레임워크

소스 데이터에 대한 집계 구성

동시에 실행할 수 있는 집계 수 구성

집계를 사용하여 보고서 생성

동시에 실행할 수 있는 집계 수 구성

새 프로세서 또는 백그라운드 작업인 집계된 보고 프레임워크 프로세서는 집계된 보고서 프레임워크 테이블과 관련된 예약된 작업을 실행하는 기본 시스템과 함께 제공됩니다. 이렇게 하면 전체 하위 시스템을 백그라운드에서 실행할 수 있으며 시스템 리소스를 사용할 수 있을 때 더 잘 활용할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 백그라운드 작업 구성 – 취약성 대응 공통 집계 결과 계산기.
2. 필드된 최대 동시 스레드 에서 동시에 실행할 집계 수를 정의하고 저장을 선택합니다.
   기본적으로 4개의 집계가 동시에 실행됩니다.
3. 백그라운드 Job Processor 풀 목록으로 이동합니다.
   sn_sec_cmn_background_job_processor_pool.list을 클릭하고 새로 만들기를 선택하여 집계 보고서 프레임워크에 대한 백그라운드 작업 프로세서를 만듭니다.
   백그라운드 작업 프로세서 풀을 만드는 방법에 대한 자세한 내용은 취약성 대응에서 백그라운드 작업에 대한 고급 병렬 처리를 참조하세요.

   주:
   백그라운드 작업 프로세서의 수는 백그라운드 작업 구성 – 취약성 대응 공통 집계 결과 계산기 양식에 제공된 최대 동시 스레드 수와 같아야 합니다. 2단계를 참조하십시오.

관련 정보

- 집계된 보고서 프레임워크
- 소스 데이터에 대한 집계 구성
- 여러 집계를 동시에 실행
- 집계를 사용하여 보고서 생성

집계를 사용하여 보고서 생성

생성한 집계와 관련된 데이터를 시각화하고 분석하려면 조건 작성기에서 집계에 대한 조건을 제공하여 보고서를 생성하십시오.

시작하기 전에
필요한 역할: pa_admin

프로시저

1. 다음으로 이동 모두 〉 보고서 〉 새로 작성.
2. 데이터 탭의 필드에 내용을 입력합니다.

데이터 탭 필드

필드	설명
보고서 이름	보고서 이름
소스 유형	데이터를 가져오는 소스의 유형입니다. 테이블을 선택합니다.
테이블	집계가 생성되는 테이블의 이름입니다. 집계된 결과 테이블 집계된 결과 [sn_vul_cmn_aggregate_result]을(를) 선택합니다.

3. 조건 작성기에서 보고서를 생성할 집계의 조건을 설정합니다.

조건 작성기의 조건

파트	설명
필드	집계를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

파트	설명
운영자	을(를) 선택합니다.
값	집계의 이름입니다.

4. 데이터 탭에서 다음을 선택합니다.
5. 유형 탭에서 데이터를 시각화할 방법을 선택하고 다음을 선택합니다.
   보고서 유형에 대한 자세한 내용은 보고서 만들기를 참조하십시오.

   지원되는 시각화는 막대형 차트, 원형 차트 및 히트맵입니다. 선 그래프 및 기타 추세 시각화를 수정하여 지원되는 시각화를 집계된 결과와 함께 사용하여 동일한 데이터를 나타낼 수 있습니다. 목록 뷰는 지원되지 않습니다.
6. 구성 탭의 필드에 내용을 입력합니다.

필드	설명
그룹화 기준	선택한 필드별로 데이터를 그룹화합니다. 여기에서 집계 탭의 **Grouped by 1** 필드에서 #unique_506_Connect_42_group-by 선택한 필드를 선택합니다.
스택 정렬 기준	선택한 필드를 기준으로 레이어로 데이터를 구성합니다. 여기에서 집계 탭의 **Grouped by 2** 필드에서 #unique_506_Connect_42_group-by 선택한 필드를 선택합니다. 주: 막대형 및 가로 막대형 보고서만 누적 데이터를 사용합니다. 다른 보고서 유형은 그룹화만 허용합니다.
집계	값에최소 또는 최대 기능을 적용합니다.

7. 스타일 탭에서 필드에 적절한 정보를 입력하고 실행을 선택합니다.
   구성 및 스타일 탭의 필드에 대한 자세한 내용은 보고서 만들기 비디오를 참조하십시오.
8. 조건 작성기에서 보고서를 생성할 집계의 조건을 설정하고 실행을 선택합니다.

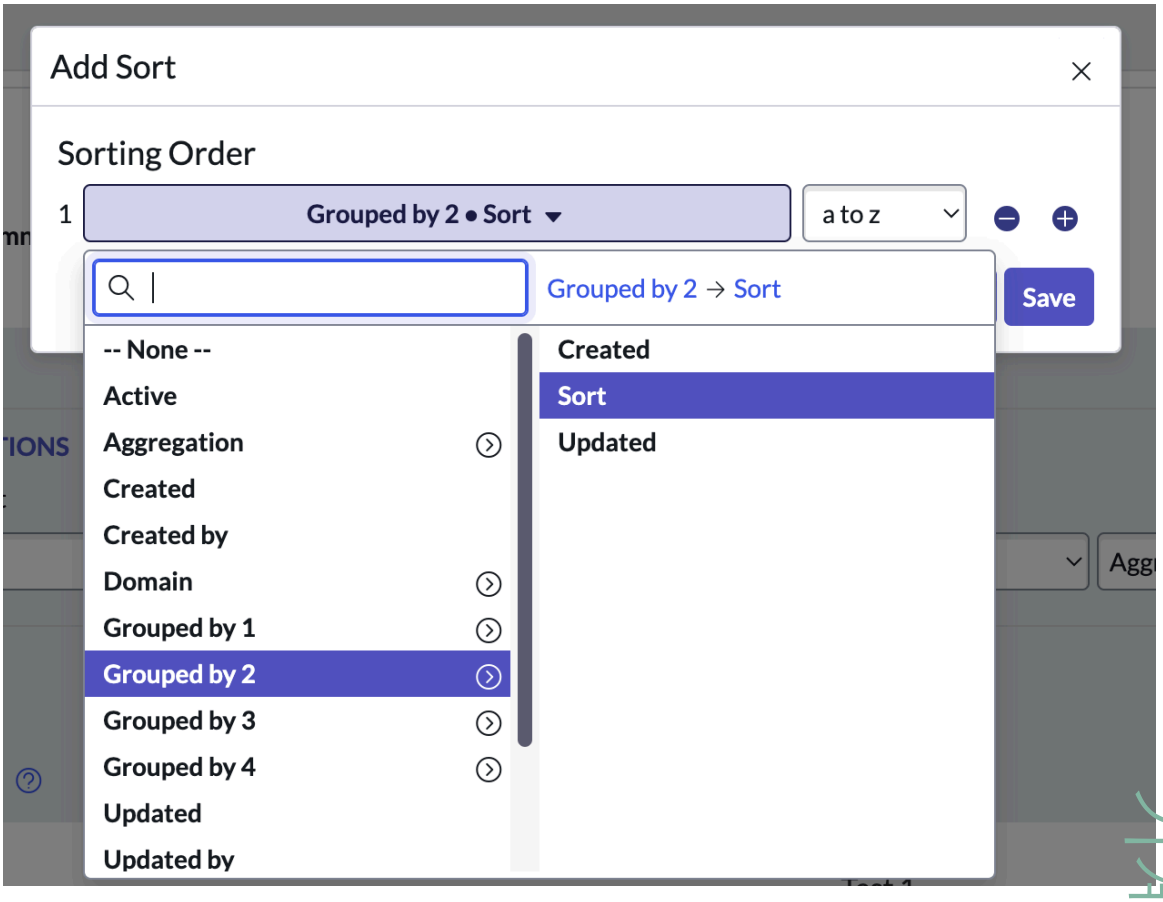
   보고서가 표시됩니다.
9. X축의 값을 정렬하려면 정렬 추가를 선택합니다.

   a. 문자열의 경우 조건을 **Grouped by** > **a-z** 또는 **z-a** 로 제공하여 문자열을 알파벳 순서로 정렬합니다.

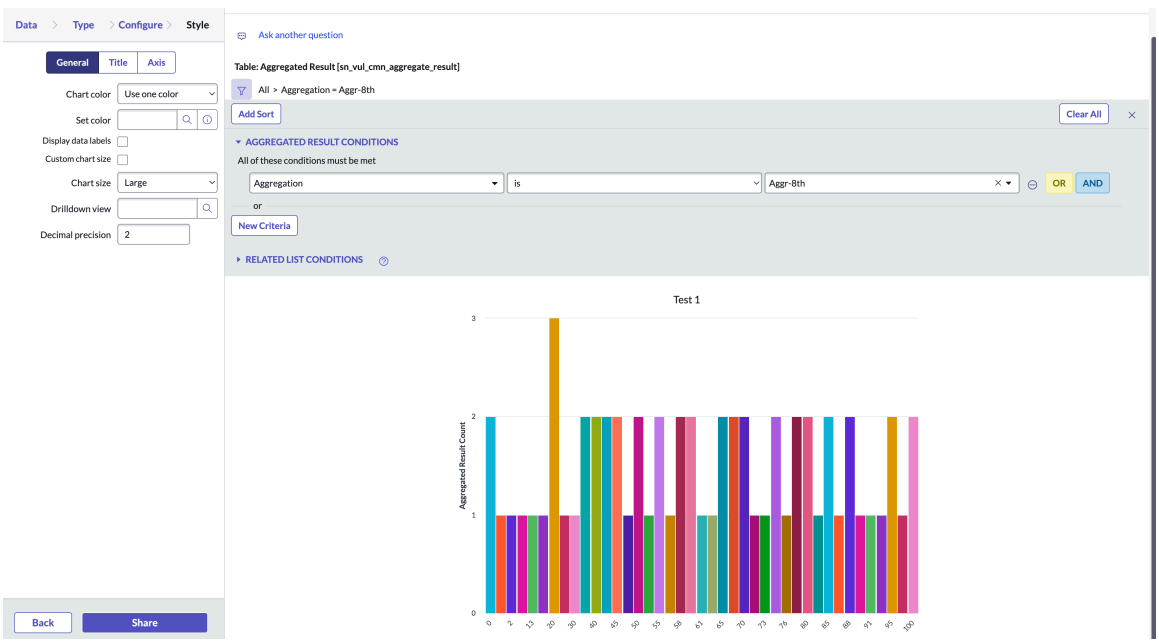
   b. 정수 및 날짜 데이터 형식 값의 경우 조건을 그룹화 기준.정렬 > **a-z** 또는 **z-a** 로 제공하여 값을 각각 오름차순 및 내림차순으로 정렬합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

X축의 정수 정렬



c. 실행을 선택합니다.
정수 및 날짜 값이 X축에서 정렬됩니다.



10. 저장을 선택하여 보고서를 저장합니다.
집계에 대해 생성된 보고서는 각 집계 양식의 결과 탭에 표시됩니다.

11. 옵션: 대시보드에 보고서를 추가합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

대시보드에 보고서를 추가하는 방법에 대한 자세한 내용은 응답 대시보드에 보고서 추가를 참조하세요.

캐시된 보고 프레임워크를 사용하여 생성된 보고서로 구성된 취약성 관리(집계됨) 대시보드는 기본 시스템과 함께 제공됩니다. 이 대시보드를 보려면 다음으로 이동하십시오. 모두 > 퍼포먼스 분석 > 대시보드 > 모두 > 취약성 관리(집계됨). 이 대시보드의 보고서에 해당하는 활성 집계는 기본 시스템과 함께 제공됩니다.

12. 보고서를 다른 사용자와 공유합니다.
보고서를 공유하는 방법에 대한 자세한 내용은 보고서 배포를 참조하십시오.

관련 정보

소스 데이터에 대한 집계 구성

집계된 보고서 프레임워크

여러 집계를 동시에 실행

동시에 실행할 수 있는 집계 수 구성

취약성 대응 참조 정보

다음 항목에서는 링크, 참조 정보, 문제 해결 및 지식 문서를 제공하며 에 취약성 대응있는 양식 및 기록의 필드 데이터도 제공합니다.

아래는 HI 지식베이스의 지원 및 문제 해결 VR/CC에 대한 지식베이스 링크 문서로 시작하는 도움이 될 수 있는 다른 자원에 대한 링크입니다.

- 지원 및 문제 해결 VR/CC에 대한 지식베이스 링크
- 애플리케이션 및 호환성에 대한 자세한 내용은 KB0856498 취약성 대응 호환성 매트릭스 및 릴리스 스키마 변경을 참조하십시오.
- 보안 운영 비디오
- 개발자 교육
- 개발자 설명서
- 구현 전문가와 협력하여 Customer Success Center 에서 원하는 비즈니스 성과를 달성하십시오.
- Vulnerability Response 과정을 수강하여 전문 지식을 쌓고 ROI를 더 빠르게 실현하십시오. 등록하려면 ServiceNow 교육 및 인증 을 참조하십시오.
- 애플리케이션과 함께 설치되는 구성요소 찾기
- 취약성 대응 오케스트레이션
- 통합 작성을 위한 팁
- 보안 운영 커뮤니티에서 질문 또는 답변하기
- 알려진 오류 포털에서 알려진 오류 문서 검색
- 연락처 고객 서비스 및 지원

애플리케이션의 구현 검사 목록 취약성 대응

이 검사 목록에는 인스턴스에서 애플리케이션을 기본적으로 구현하는 데 필요한 단계가 나열되어 있습니다 취약성 대응ServiceNow AI Platform# . 이러한 작업을 완료하면 기본 시스템이 작동 및 검증을 위한 준비가 된 것입니다.

시작하기 전에

필요한 역할: 애플리케이션 다운로드 및 활성화와 역할 할당을 위한 admin, 구성을 취약성 대응위한 sn_vul.vulnerability_admin .

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 작업을 완료하면서 체크 표시를 할 수 있도록 이 검사 목록의 PDF를 만들어 인쇄하는 것이 좋습니다.
2. PDF를 생성하려면 주제 상단에 있는 PDF로 저장 아이콘( )을 클릭하고 선택한 주제를 클릭합니다.

취약성 대응 관리자를 위한 기본 구현 검사 목록 작업

항목	설명
☐	관리자 역할이 있는 사용자로서 권리를 획득하고 인스턴스에서 인스턴스로 ServiceNow AI Platform 다음 애플리케이션을 다운로드(설치)했는지 확인합니다.ServiceNow# Store ○ 취약성 대응 ○ 취약성 대응 NIST 국가 취약성 데이터베이스와 통합 ○ Qualys 보안 운영을 위한 통합 **a.** 인스턴스에서 애플리케이션을 사용할 수 있는지 확인하려면 모두 〉 시스템 애플리케이션 〉 모든 사용 가능 애플리케이션 〉 모두 을 클릭하고 [sn_vul], [sn_vul_nvd] 및 〔sn_vul_qualys〕를 검색합니다. **b.** 애플리케이션을 찾을 수 없는 경우 권리 획득 및 애플리케이션 다운로드에 대한 자세한 내용은 을 참조하십시오 보안 운영 그리고 ServiceNow Store .
☐	관리자 역할이 있는 사용자는 모두 〉 취약성 대응 〉 관리 〉 설정 도우미 〉 통합 애플리케이션 설치 그런 다음 인스턴스에 대한 의존성과 함께 애플리케이션을 활성화(설치) 취약성 대응 합니다 ServiceNow AI Platform . 주: 애플리케이션을 설치하는 취약성 대응 동안 데모 데이터를 설치할 수 있는 옵션이 있습니다. 자동화된 테스트를 실행하여 설치 후 인스턴스가 작동하는지 확인하려면 데모 데이터가 필요합니다. 데이터 손상 및 중단을 방지하려면 개발, 테스트 및 기타 비프로덕션 인스턴스에 대해서만 테스트를 실행하십시오. 데모 데이터 또는 데모 계정이 생성된 경우 비프로덕션 또는 프로덕션에서 인스턴스를 사용하기 전에 모든 데모 데이터를 제거해야 합니다. 에 대한 취약성 대응 설정 도우미는 애플리케이션과 함께 자동으로 설치됩니다. 애플리케이션을 구성하려면 설정 도우미가 취약성 대응 필요합니다. 또한 이 예시에 사용된 Integration for Security Operations 애플리케이션뿐만 아니라 를 지원하고 호환되는 취약성 대응다른 애플리케이션을 설치하고 구성하는 Qualys 데 사용됩니다. 애플리케이션 설치에 취약성 대응 대한 자세한 내용은 다음 문서를 참조하십시오 취약성 대응 설치.
☐	관리자 역할을 가진 사용자는 설정 도우미에서 모두 〉 취약성 대응 사용자 및 그룹 을 클릭하고 필요한 취약성 대응 가상 사용자 역할을 가진 사용자를 할당합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

항목	설명
	a. 설정 도우미 내에서 사용자 관리 모듈 링크를 클릭하여 기존 사용자와 이미 할당된 역할을 봅니다. **b.** 목록에서 사용자 이름을 클릭하여 기록을 열고 역할 관련 목록을 클릭합니다. 이 사용자에게 할당된 모든 역할이 표시됩니다. **c.** (으)로 다시 이동 취약성 대응 사용자 및 그룹 설정 도우미에서 프롬프트에 따라 sn_vul.vulnerability_admin 역할을 할당합니다. 주: 구성을 계속하려면 sn_vul.vulnerability_admin 역할이 필요합니다. 또는 관리자 역할을 가진 사용자로 구성을 계속할 수 있습니다. (선택 사항) CI(구성 항목) 관리자 [sn_vul.ci_manager] 및 예외 승인자 [sn_vul.exception_approver] 역할을 할당할 수도 있지만 나머지 설정 작업에는 이러한 가상 사용자가 필요하지 않습니다. 설정 도우미를 사용하여 가상 사용자 역할을 할당하는 방법에 대한 자세한 내용은 문서를 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당참조하십시오. 사용자 및 사용자 및 그룹에 역할 할당에 대한 자세한 내용은 사용자 관리를 참조하십시오.
☐	**a.** 다음으로 이동 모두 〉 관리 〉 통합 을 클릭하고 **CWE Comprehensive 2000 Integration**이 활성화되었는지 확인하고 예약된 작업을 실행하여 데이터를 임포트합니다. **b.** 관리자 역할이 있는 사용자로서 시스템 애플리케이션 〉 모든 사용 가능 애플리케이션 및 NVD와 취약성 대응 통합 애플리케이션을 활성화(설치)합니다. 외부 공급업체 스캐너 제품을 사용하여 취약성 데이터를 인스턴스로 임포트하기 전에 초기 설정 취약성 대응 의 일부로 NVD 및 CWE 통합을 실행합니다. NVD 및 CWE 라이브러리 설치, 구성 및 보기에 대한 자세한 내용은 을 CWE 기록을 업데이트하기 위해 예약된 작업을 구성하고 실행합니다. 참조하십시오NVD 및 CWE 통합을 통해 데이터를 임포트하고 외부 공급업체 라이브러리를 관리합니다.
☐	관리자 역할이 있는 사용자는 모두 〉 취약성 대응 〉 관리 〉 설정 도우미 〉 통합 애플리케이션 설치 을 클릭하고 Integration for Security Operations 애플리케이션을 활성화합니다 Qualys . 라이브러리가 있는 것과 같은 Qualys 외부 공급업체 스캐너 제품을 설치하고 실행하기 전에 먼저 NVD 및 CWE 통합을 설치하고 실행하여 취약성 데이터를 수집해야 합니다. 자세한 내용은 설정 도우미를 사용하여 타사 응용 프로그램 설치 취약성 대응 문서를 참조하십시오.
☐	(선택 사항) 관리자 역할이 있는 사용자가 애플리케이션과 함께 취약성 대응 데모 데이터를 설치한 경우 ATF 테스트 도구 모음을 취약성 대응 실행하여 애플리케이션이 성공적으로 설치되었는지 확인할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

항목	설명
	주: 데이터 손상 및 중단을 방지하려면 개발, 테스트 및 기타 비프로덕션 인스턴스에 대해서만 테스트를 실행하십시오. 자세한 내용은 에 대해 Automated Test Framework(ATF) 테스트 도구 모음 실행 취약성 대응 문서를 참조하십시오. 자동화된 테스트에 대한 자세한 내용은 Automated Test Framework(ATF) 를 참조하십시오.

3. 취약성 대응 설정 섹션에서 시작하여 애플리케이션 구성을 계속합니다.

   이러한 설정을 검토하면 환경을 계속 설정할 때 작동 방식을 취약성 대응 이해하는 데 도움이 됩니다. 이 예에 사용된 스캐너 통합의 경우 설정을 편집해야 합니다.

   제품에 대해 Qualys 이 구성 예에서 사용하는 개념은 다른 스캐너 애플리케이션에 적용됩니다.

   Qualys 애플리케이션을 구성하려면 자격 증명이 필요합니다. 제품에 필요한 Qualys 계정 이름, 암호 및 기타 서비스 정보가 있는지 확인하여 이에 액세스할 수 있습니다.

   필요한 역할: sn_vul.vulnerability_admin 또는 admin.

   취약성 대응 취약성 관리자를 위한 기본 구현 검사 목록 작업

작업	설명
☐	취약성 할당 규칙을 검토합니다. 담당 규칙은 적절한 할당 그룹에 취약한 항목(VI)을 자동으로 할당합니다. 자세한 내용은 취약성 대응 할당 규칙 개요 문서를 참조하십시오. 설정 도우미를 사용하여 구성하는 취약성 대응 방법에 대한 자세한 내용은 문서를 참조하십시오 설정 지원을 사용하여 구성 취약성 대응 하기.
☐	정정 작업 규칙을 검토합니다. 정정 작업 규칙은 특정 조건에 따라 취약한 항목(VI)이 임포트될 때 자동으로 이 항목을 그룹화합니다. 자세한 내용은 취약성 대응 정정 작업 및 정정 작업 규칙 개요 문서를 참조하십시오.
☐	위험 계산기를 검토합니다. 위험 계산기는 우선순위에 취약한 항목의 점수를 지정합니다. 계산기를 구성하여 취약성 평가(스캐너) 벤더가 보고한 구성 항목(CI), 악용 가능성 및 취약성 심각도의 특성을 통합할 수 있습니다. 자세한 내용은 취약성 대응 계산기 및 취약성 계산기 규칙 문서를 참조하십시오.
☐	정정 대상 규칙을 검토합니다. 정정 대상 규칙은 VI 및 정정 작업에 대한 정정 타임라인을 정의합니다. 자세한 내용은 취약성 대응 정정 대상 규칙 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업	설명
☐	통합 구성 섹션에서 애플리케이션 설정을 검토하고 Qualys 데이터 임포트를 정의하고 예약합니다. **a.** 스캐너 통합을 클릭합니다. **b.** 설치된 애플리케이션 페이지에서 편집을 클릭합니다. **c.** 자격 증명을 입력하고 다음을 클릭합니다. **d.** 지식베이스 구성에 대한 설명을 읽으십시오. **e.** 임포트 설정, CI 조회 규칙 및 임포트 일정에 대한 호스트 탐지 구성 페이지를 검토합니다. **f.** 이 페이지의 설정이 만족스러우면 지금 실행을 클릭하여 데이터를 가져옵니다. 표시되는 세부 정보 보기 링크를 클릭하여 취약성 통합 실행 상태를 확인합니다. **g.** (선택 사항) 구성 설정을 계속 편집합니다. **h.** 마침을 클릭하여 설정 도우미에서 설치 및 구성을 완료합니다. 애플리케이션 구성에 대한 자세한 내용은 다음 문서를 참조하십시오 QualysQualys Vulnerability Integration 설정 도우미 사용 구성.

다음에 수행할 작업
축하합니다! 애플리케이션을 성공적으로 설치하고 취약성 대응 설정 도우미를 사용하여 해당 애플리케이션과 스캐너 애플리케이션을 구성했습니다. 이제 기본 시스템을 작동할 준비가 되었습니다.

에 대한 취약성 대응다른 애플리케이션을 다운로드, 설치 및 구성하려면 이전 검사 목록에 대해 완료한 것과 동일한 단계와 개념을 따릅니다. 자세한 내용은 각 애플리케이션에 대해 제공된 특정 주제를 참조하십시오.

에서 취약성 대응사용할 ServiceNow Store 수 있는 지원되는 애플리케이션에 대한 자세한 내용은 문서를 참조하십시오취약성 대응 설치 및 지원되는 애플리케이션.

사용 취약성 대응방법에 대한 자세한 내용은 을 참조하십시오 애플리케이션 탐색 취약성 대응.

취약성 대응 정정 작업 상태

외부 공급업체 통합은 새로운 취약성 항목(VIT)을 생성하거나 기존 VIT를 업데이트하는 취약한 항목 탐지 데이터를 임포트합니다. 검색 상태는 열려 있거나 닫혀 있는 한 VIT 상태를 업데이트합니다.

탐지 상태가 VIT의 상태에 미치는 영향에 대한 자세한 내용은 를 탐지, 정정 작업 및 취약한 항목 상태참조하십시오.

를 사용하면 를 위한 변경 관리 취약성 대응정정 작업의 상태 필드와 취약성 대응 제품의 변경 요청(CHG)의 상태 필드 간에 동기화된 관계가 있습니다. 변경 요청은 수명주기를 거치면서 관련 정정 작업의 상태도 자동으로 이동합니다. 변경 요청이 구현되면 정정 작업이 자동으로 해결됩니다. 자세한 내용은 변경 요청과 정정 작업 간의 상태 동기화 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
v23.0 취약성 대응부터 :

- Flow Designer에서 정정 작업 상태 승인 워크플로우는 더 이상 사용되지 않으며 플로우 정정 작업 상태 승인으로 대체됩니다.
- 정정 작업에 대한 닫기 버튼이 제거되었으며 스캐너에 의해 정정 작업의 종결이 이루어집니다.

다음 표에는 정정 작업 상태와 각 상태에서 정정 작업에 대해 수행할 수 있는 작업이 나열되어 있습니다.

정정 작업 상태

상태	설명
오픈	생성 시 상태입니다. 이 상태에서 다음을 수행할 수 있습니다. 중복 VI 표시 시스템의 여러 스캐너에서 보고된 중복 VIT를 식별합니다. 중복 VIT를 해결됨 또는 종결됨으로 표시할 수 있습니다. CVE(Common Vulnerabilities and Exposures)를 사용하여 취약성 조합을 만든 경우에만 중복 항목이 표시됩니다. 자세한 내용은 취약성 대응 정정 작업 및 취약한 항목 상태 문서를 참조하십시오. 조사 시작 조사를 시작할 개인 또는 그룹에 이 정정 작업을 할당합니다. 긍정 오류로 표시 스캐너에서 시스템에 취약성이 있다고 보고하지만 실제로는 취약성이 없는 경우 항목 또는 그룹을 가양성으로 표시합니다. 예외 요청 예외, 재개시(종료) 날짜, 이유를 요청하고 선택적으로 추가 정보를 제공합니다. 예외를 요청하는 날짜까지 항목 또는 그룹의 정정을 연기합니다. 해결 해결됨으로 표시 항목 또는 그룹을 해결됨 상태로 이동합니다. 변경 작성 변경 요청을 생성하거나 정정 작업을 기존 변경 요청에 연결합니다. 자세한 내용은 정정 작업에서 변경 요청 만들기 및 정정 작업을 기존 변경 요청에 연결 문서를 참조하십시오. 분리 정정 작업 둘 이상의 취약한 항목이 있는 정정 작업의 경우 조건 세트를 사용하여 취약한 항목의 하위 집합을 필터링하고 정정 작업을 분할합니다. 선택한 항목은 자동으로 새 정정 작업으로 이동됩니다. 자세한 내용은 에서 정정 작업 분할 IT 정정 작업 공간 문서를 참조하십시오. 연기 연기됨 상태, 재개시 날짜, 이유를 선택하고 선택적으로 추가 정보를 제공합니다. 재개시 날짜까지 정정 작업 상태를 연기합니다. 삭제

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

정정 작업 상태

상태	설명
	삭제를 확인합니다. 그룹을 제거합니다.
조사 중	조사 시작 버튼으로 트리거됩니다. 이 상태에서는 다음을 수행할 수 있습니다. 보안 인시던트 생성 자세한 내용은 보안 인시던트 만들기를 참조하십시오. 변경 작성 변경 요청을 생성하거나 정정 작업을 기존 변경 요청에 연결합니다. 자세한 내용은 정정 작업에서 변경 요청 만들기 및 정정 작업을 기존 변경 요청에 연결 문서를 참조하십시오. 작업 분할 둘 이상의 취약한 항목이 있는 정정 작업의 경우 조건 세트를 사용하여 취약한 항목의 하위 집합을 필터링하고 정정 작업을 분할합니다. 선택한 항목은 자동으로 새 정정 작업으로 이동됩니다. 자세한 내용은 정정 작업 분할 문서를 참조하십시오. 변경 요청 생성 자세한 내용은 정정 작업에서 변경 요청 만들기 문서를 참조하십시오. 대기 중인 구현 상태를 구현 대기 중으로 변경합니다. 이 상태는 정정 작업이 외부에서 취약성 대응참조되었음을 나타냅니다. 연기 연기됨 상태, 재개시 날짜, 이유를 선택하고 선택적으로 추가 정보를 제공합니다. 재개시 날짜까지 정정 작업 상태를 연기합니다. 삭제 삭제를 확인합니다. 정정 작업을 제거합니다.
연기됨	예외 요청 버튼으로 트리거됩니다. 승인 워크플로우의 일부로 연기됨 상태는 검토 중이며 승인될 때까지 종결할 수 없습니다. 이 상태에서는 다음을 수행할 수 있습니다. 변경 작성 변경 요청을 생성하거나 정정 작업을 기존 변경 요청에 연결합니다. 자세한 내용은 정정 작업에서 변경 요청 만들기 및 정정 작업을 기존 변경 요청에 연결 문서를 참조하십시오. 작업 분할 둘 이상의 취약한 항목이 있는 정정 작업의 경우 조건 세트를 사용하여 취약한 항목의 하위 집합을 필터링하고 정정 작업을 분할합니다. 선택한 항목은 자동으로 새 VG로 이동됩니다. 정정 작업 분할 문서를 참조하십시오. 보안 인시던트 생성 자세한 내용은 보안 인시던트 만들기를 참조하십시오. 재개설 열림 상태로 다시 전환합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

정정 작업 상태

상태	설명
	삭제 삭제를 확인합니다. 정정 작업을 제거합니다. 연기 정보는 종결/지연 탭에 표시됩니다. 지연 날짜에 그룹은 정정을 위해 다시 열립니다.
대기 중인 구현	구현 대기 중 버튼으로 트리거됩니다. 이 상태에서는 다음을 수행할 수 있습니다. 보안 인시던트 생성 자세한 내용은 보안 인시던트 만들기를 참조하십시오. 변경 작성 변경 요청을 생성하거나 정정 작업을 기존 변경 요청에 연결합니다. 자세한 내용은 정정 작업에서 변경 요청 만들기 및 정정 작업을 기존 변경 요청에 연결 문서를 참조하십시오. 작업 분할 둘 이상의 취약한 항목이 있는 정정 작업의 경우 조건 세트를 사용하여 취약한 항목의 하위 집합을 필터링하고 정정 작업을 분할합니다. 선택한 항목은 자동으로 새 정정 작업으로 이동됩니다. 자세한 내용은 정정 작업 분할 문서를 참조하십시오. 변경 요청 생성 자세한 내용은 정정 작업에서 변경 요청 만들기 문서를 참조하십시오. 연기 연기됨 상태, 재개시 날짜, 이유를 선택하고 선택적으로 추가 정보를 제공합니다. 재개시 날짜까지 정정 작업 상태를 연기합니다. 해결 메모를 추가합니다. 상태가 해결됨이 됩니다. 해결 탭 아래에 메모가 나타납니다. 삭제 삭제를 확인합니다. 정정 작업을 제거합니다.
해결 일시	해결 버튼에서 트리거됩니다. 이 상태에서 다음을 수행할 수 있습니다. 보안 인시던트 생성 자세한 내용은 보안 인시던트 만들기를 참조하십시오. 변경 작성 변경 요청을 생성하거나 정정 작업을 기존 변경 요청에 연결합니다. 자세한 내용은 정정 작업에서 변경 요청 만들기 및 정정 작업을 기존 변경 요청에 연결 문서를 참조하십시오. 재개설 열림 상태로 다시 전환합니다. 삭제 삭제를 확인합니다. 정정 작업을 제거합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

정정 작업 상태

상태	설명
	메모 탭 아래에 메모가 나타납니다. 해결 정보는 해결 탭 아래에 표시됩니다.
종결됨	스캐너에 의해 트리거 됩니다. 이 상태에서는 다음을 수행할 수 있습니다. 보안 인시던트 생성 자세한 내용은 보안 인시던트 만들기를 참조하십시오. 재개설 열림 상태로 다시 전환합니다. 삭제 삭제를 확인합니다. 정정 작업을 제거합니다. 종 결/지연 탭에 종결 정보가 표시됩니다.

- 정정 소유자는 취약한 항목 또는 정정 작업만 해결됨으로 표시할 수 있습니다. 스캐너의 확인에 따라 이 해결된 항목 또는 정정 작업을 종결 또는 재오픈으로 표시할 수 있습니다.
- 수동으로 생성된 취약한 항목이 여러 개 있어 이러한 항목을 종결하거나 삭제해야 하는 경우 관리자가 삭제 버튼을 사용할 수 있습니다.
- 항목이 낮은 위험 수준이거나 변경 시간대 또는 패치를 기다리는 것으로 확인되면 정정 작업을 정의된 시간 동안 빨간색 연기상태로 변경할 수 있습니다.예외 요청 옵션을 사용하여 예외를 요청할 수 있습니다.

  주:
  정정 작업이 연기되거나 종결되면 해결 방법을 지정하여 그 이유를 추가로 정의할 수 있습니다.

- VIT가 수동 또는 자동으로 다시 열리면 다음과 같은 상황이 발생합니다.
  - VIT 상태가 열림으로 변경됩니다. 원래 정정 작업 상태는 업데이트되지 않습니다.
  - VIT가 재평가되어 활성 정정 작업 규칙을 기반으로 하는 새 정정 작업 또는 기존 정정 작업에 배치됩니다.

  이렇게 하면 추가 정정이 가능해지면서 이력이 보존됩니다.

- 정정 작업이 생성되거나(자동 또는 수동으로) 분할되면 상태, 이유 및 종료 필드가 평가됩니다. 분할 작업의 경우 이러한 필드는 이전 및 새 정정 작업 모두에 대해 평가됩니다. VIT가 업데이트되면 연결된 모든 정정 작업의 상태, 이유 및 종료 필드가 평가됩니다.
  - 정정 작업의 모든 VIT가 지연되고 이유가 동일한 경우 정정 작업의 상태가 지연 됨으로 변경되고 VIT의 이유가 정정 작업에 할당됩니다. VIT의 사유가 다르면 정정 작업의 이유가 없음으로 변경됩니다.
  - 모든 VIT의 종료 날짜에 가장 가까운 날짜가 정정 작업의 종료 필드에서 업데이트됩니다.
  - VIT를 다시 열면 정정 작업의 상태가 미해결로 변경됩니다.

  이 평가는 15분마다 실행되는 예약된 작업에 의해 *Rollup vulnerability item values to vulnerability and group* 수행됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

탐지, 정정 작업 및 취약한 항목 상태

외부 공급업체 통합은 취약한 항목 탐지 데이터를 검색합니다. 탐지는 스캐너에서 보고되는 취약성의 명백한 발생입니다.

탐지 데이터는 취약한 항목(VI, VIT)과 쌍을 이루고 VI 상태는 탐지 상태에 따라 업데이트됩니다. VI를 찾을 수 없는 경우 새 VI가 생성됩니다. 탐지는 스캐너에서 직접 찾은 데이터에 의해서만 열리거나 닫힙니다.

취약한 항목에 대한 모든 탐지가 종결되면 해당 취약한 항목이 종결됩니다. VI 기록에서 상태는 종결/고정입니다. 정정 작업에 대해 모든 VI가 닫히면 정정 작업이 종결됩니다. 그렇지 않으면 상태 흐름이 동일하게 유지됩니다.

하위 상태가 고정 또는 부실인 종결된 VI는 새로운 탐지가 생성되고 VI를 새로운 취약성과 일치시킬 수 있는 경우 다시 열립니다.

버전 20.0 취약성 대응부터 감지가 부실이고 연결된 VI가 종결됨 상태인 경우 VI의 상태가 종결됨 - 부실로 전환되지 않습니다. 이는 새로운 탐지가 식별될 때 VI가 다시 열리지 않도록 하여 전체 가양성 요청 및 승인 프로세스를 거치지 않도록 하기 위한 것입니다. 이 동작을 되돌리려면 자동 종결 구성 양식에서 종결된 VI에 대한 부실 탐지 무시 확인란의 선택을 취소하십시오. 자세한 내용은 에서 부실 탐지 자동 종결 취약성 대응 문서를 참조하십시오.

스크립트 포함, *DetectionBase*, 방법에 *_shouldReOpenVI()*따라 VI가 이전에 고정, 부실 또는 CI 해제됨의 하위 상태로 종결된 경우 다시 열리고 탐지가 기존 VIT에 매핑됩니다.

예를 들어 VI의 종결 날짜가 마지막으로 발견된 탐지 날짜보다 나중이라고 가정해 보겠습니다. 이러한 VI 기록은 종결된 상태로 유지될 것으로 예상할 수 있습니다. 그러나 이전에 닫힌 VI가 다시 열린 것으로 확인되면 VI가 이전 탐지에 의해 닫혔고 이후 스캔에서 취약성이 다시 발견되었음을 의미합니다. VI의 구성 항목에 동일한 취약성이 있는 종결된 VIT와 일치하는 새 탐지가 발견되면 VI가 다시 열립니다.

정정 작업 및 취약한 항목 상태

정정 작업과 취약한 항목 상태는 서로 영향을 줄 수 있습니다. 대부분의 경우, 정정 작업 상태는 취약한 항목 상태를 업데이트하며, 그룹의 취약한 항목을 업데이트하는 데 우선순위가 가장 높은 작업 상태가 사용됩니다.

상태 우선 순위는 다음과 같습니다.

종결됨 〉 연기됨 〉 해결 일시 〉 검토 중 〉 대기 중인 구현 〉 조사 중 〉 오픈

- 취약한 항목 그룹이 하나의 정정 작업에 있고 개별 수준에서 변경되지 않는 경우 해당 정정 작업과 상태가 동일합니다.
- 정정 작업이 열림 상태에서 구현 대기 중으로 전환되면 정정 작업의 모든 VI가 구현 대기 중 상태로 전환됩니다.
- 정정 작업이 지연되면 VI도 마찬가지로 지연됩니다. 버전 16.5부터 취약한 항목, 애플리케이션 취약한 항목, 컨테이너 취약한 항목 또는 정정 작업이 지연되는 횟수를 추적할 수 있습니다. 예약된 작업인 *set deferral counts*,는 VR, AVR 및 CVR에 대한 여러 지연 모듈의 지연 횟수 열에 두 번 이상 지연된 기록에 대한 개수를 게시하도록 매일 실행됩니다. 정정 작업이 두 번 이상 지연되는 경우 정정 작업과 연결된 VI에 대한 모든 카운트가 수집되고 게시됩니다.

  정정 작업에 의해서만 업데이트되는 취약한 항목

  항목이 개별적으로 업데이트되지 않은 경우 정정 작업의 상태와 일치하지만 다음 예외가 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 정정 작업 상태가 종결로 변경되고 해결이 취소됨 또는 예외와 함께 수정됨으로 변경되는 경우 항목은 영향을 받지 않으며 해당 항목을 포함하는 다른 모든 정정 작업의 상태를 갖습니다. 취약한 항목이 다른 정정 작업에 없는 경우에는 열림 상태로 되돌아갑니다.
- 취약한 항목 상태가 종결/수정(스캔 또는 임포트에 의해 업데이트됨)인 경우 정정 작업에서 상태가 변경되면 취약한 항목은 종결/고정 상태로 유지됩니다. 이 조건은 정정 작업의 상태에 관계없이 True입니다.

개별적으로 설정된 상태의 취약한 항목

개별적으로 종결되거나 연기된 항목과 같이 항목에 업데이트된 상태의 취약한 항목은 정정 작업의 상태와 자동으로 일치하지 않습니다. 대신 해당 상태를 모든 연관된 그룹과 비교하여 적용할 우선순위가 가장 높은 상태를 찾습니다.

주:
종결/고정 상태는 특수한 경우입니다. 종결/고정 상태로 설정된 취약한 항목의 경우, 스캐너에서 모든 취약성이 정정되었음을 발견하는 경우와 같이 정정 작업 내의 모든 취약한 항목이 종결/수정됨으로 설정된 경우 정정 작업이 자동으로 종결/수정됨으로 표시됩니다.

정정 작업에 빈 할당 필드가 포함되어 있습니다.

정정 작업의 VI 상태가 해결됨에서 오픈으로 변경되면 정정 작업의 상태도 해결됨에서 조사 중으로 업데이트됩니다.

그러나 정정 작업의 할당 대상 및 할당 그룹 필드가 모두 비어 있으면 정정 작업이 해결됨 상태로 유지되고 조사 중으로 이동되지 않습니다.

정정 작업이 업데이트될 때 취약한 항목에 대한 할당 그룹이 항상 업데이트되는 것은 아닙니다.

열림 상태의 VI에 대한 할당 그룹이 수동으로 업데이트되면 정정 작업에 대한 할당 그룹이 업데이트될 때 다시 업데이트되지 않습니다. VI에 대한 할당 그룹이 의도적으로 업데이트되었고 다른 정정 작업의 일부일 수 있으므로 이 정보는 덮어쓰기되지 않습니다.

상태 롤업 및 롤다운 시나리오

상태 롤업 및 롤다운 시나리오는 정정 작업(RT)과 취약 항목(VIT)의 상태를 자동으로 동기화하여 둘 다 실시간 업데이트를 보장합니다. 이러한 동적 상호작용은 수동 추적을 줄이고, 정확도를 높이며, 사용자에게 진행 상황에 대한 최신 뷰를 제공하여 취약성 관리의 효율성을 높이고 사용자가 정보에 입각한 결정을 신속하게 내릴 수 있도록 지원합니다.

롤업 동작

취약한 항목(VIT) 상태가 변경되면 이러한 변경 내용이 정정 작업(RT) 수준까지 전파될 수 있습니다. 다음 표에는 종결 조건, 재할당 및 지연에 따라 취약한 항목(VIT) 상태의 변경이 연결된 RT(정정 작업) 상태에 영향을 줄 수 있는 주요 롤업 시나리오가 요약되어 있습니다.

롤업 시나리오

VIT 상태	**RT** 상태
조사 중인 〉 열기	열린 상태로 유지
열림 〉 종결됨-긍정 오류	열린 상태로 유지
오픈 〉 검토 중	열린 상태로 유지
오픈 〉 지연됨(모든 하위 상태)	오픈 〉 연기됨
오픈 〉 해결됨	열린 상태로 유지

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

롤업 시나리오

VIT 상태	**RT** 상태
오픈 〉 종결-취소됨	열린 상태로 유지
열림 〉 닫힘-고정	열림 〉 닫힘-고정
개방 〉 종결-수정(예외 발생)	오픈 〉 종결됨
종결-고정 〉 열림	종결-고정 유지
개방 〉 폐쇄-고정; (다음 스캔 후) 〉 해결됨	열린 상태로 유지
열림 〉 종결됨-잘못됨	열린 상태로 유지
오픈 〉 종결-부실	열림 〉 종결됨-취소됨
종결-부실 〉 오픈	종결-취소됨으로 유지
오픈 〉 종결 결과가 잘못됨	열린 상태로 유지
열림 〉 종결됨-잘못됨	열린 상태로 유지
오픈 〉 종결됨-CI 해제됨	오픈 〉 종결-취소됨
오픈 〉 구현 대기 중-패치 예약됨	열린 상태로 유지
미해결 〉 구현 대기 중-패치가 예약되지 않음	열린 상태로 유지
오픈 〉 구현 대기 중-패치 일정 예약됨(대상 날짜 누락)	열린 상태로 유지
조사 중 〉 폐쇄-CI 해제됨	RT1: 조사 중 > 종결-취소됨 RT2: 조사 중 > 종결-취소됨
오픈 〉 해결됨; RT = 해결됨; VIT 다시 열기	할당된 경우 RT: 해결 > 조사 중; 기타: 오픈
VIT1: 종결-고정 VIT2: 조사 중 VIT2가 다시 열리고 VIT1이 해결된 상태로 유지되는 경우.	RT1: 조사 중 RT2: 폐쇄-고정
VIT1: 종결-부실 VIT2: 폐쇄형 CI 해제됨	오픈 〉 종결-취소됨
VIT1: 해결됨 VIT2: 폐쇄형 CI 해제됨	열린 상태로 유지
VIT1: 종결-고정	오픈 〉 종결-취소됨

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

롤업 시나리오

VIT 상태	RT 상태
VIT2: 폐쇄형 CI 해제됨	
VIT1: 종결-고정 VIT2: 종결-부실	열림 〉 닫힘-고정
VIT1: 종결〈모든 하위 상태> VIT2: 연기됨	열기> 연기됨 VIT2로 fwd를 수행한 날짜까지

롤다운 동작

정정 작업의 상태가 변경되면 수동 업데이트나 특정 예외에 의해 재정의되지 않는 한 상태가 연결된 VIT로 전파되는 경우가 많습니다. 다음 표에는 우선순위 규칙 및 특수 조건에 따라 RT(정정 작업) 상태의 변경이 연결된 취약한 항목(VIT) 상태에 영향을 줄 수 있는 주요 롤다운 시나리오가 요약되어 있습니다.

롤다운 시나리오

RT 상태	VIT 상태
오픈〉 조사 중	오픈〉 조사 중
열림 〉 종결됨-긍정 오류	열림 〉 종결됨-긍정 오류
오픈 〉 검토 중	오픈 〉 검토 중
오픈 〉 연기됨(하위 상태: 주어진 이유)	오픈 〉 연기됨(하위 상태: 주어진 이유)
오픈 〉 해결됨	오픈 〉 해결됨
오픈 〉 종결-취소됨	열린 상태로 유지
개방 〉 종결-수정(예외 발생)	열린 상태로 유지
RT1: 조사 중인 > 열기 RT2: 열림	조사 중인 〉 열기
RT1: 미해결 > 조사 중 > 구현 대기 중 RT2: 조사 중	미결 〉 조사 중 〉 구현 대기 중
RT1: 구현 대기 중 > 연기됨 RT2: 구현 대기 중	구현 대기 중 〉 연기됨
RT1: 종결-취소됨> 구현 대기 중 RT2: 조사 중	구현 대기 중〉 조사 중

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

롤다운 시나리오

RT 상태	VIT 상태
개방〉종결-수정(예외 발생) 최종 관찰: VIT2는 열려 있습니다.	VIT1: 개방 > 종결-고정 VIT2: 열림
열림〉해결됨 최종 관찰: VIT2: 미결〉해결됨	VIT1: 개방 > 종결-고정 VIT2: 열림
열림〉해결됨 최종 관찰: VIT2 재개; VIT1은 해결 상태를 유지합니다. RT: 해결됨 > 열림	VIT1: 개방 > 종결-고정 VIT2: 열림

여러 그룹의 취약한 항목(VIT)에 대한 정정 작업 상태

VIT가 여러 정정 작업(다음 표의 RT)에 있고 자체 상태가 설정되지 않은 경우 다음 표와 같이 우선순위가 더 높은 그룹 상태가 해당 VIT의 상태를 결정합니다.

취약한 항목 상태 예

정정 작업 상태	취약한 항목 상태
RT 1: 오픈 〉 조사 중 RT 2: 열기	조사 중 RT 1이 조사 중이고 RT 2가 오픈되면 VI가 조사 중으로 변경됩니다. 검색 후 RT 1과 RT 2 사이에서 RT 1은 우선순위가 가장 높은 상태를 갖습니다.
RT 1: 조사 중 RT 2: 오픈 〉 조사 중	조사 중 RT 2가 조사 중이고 RT 1이 조사 중이면 VI는 조사 중으로 유지됩니다. 검색 후 RT 1과 RT 2 사이에서 우선순위가 동일한 상태가 됩니다.
RT 1: 조사 중 RT 2: 조사 중 〉 대기 중인 구현	대기 중인 구현 RT 2가 구현 대기 중이고 RT 1이 조사 중이면 VI가 구현 대기 중으로 변경됩니다. 검색 후 RT 1과 RT 2 사이에서 RT 2는 우선순위가 가장 높은 상태를 갖습니다.
RT 1: 조사 중 〉 연기됨 RT 2: 대기 중인 구현	연기됨 RT 1이 Deferred이고 RT 2가 Awaiting Implementation인 경우 VI가 Deferred로 변경됩니다. 검색 후 RT 1과 RT 2 사이에서 RT 1은 우선순위가 가장 높은 상태를 갖습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

여러 그룹의 취약한 항목 특수 케이스

정정 작업 상태	취약 항목 상태
RT 1: 조사 중 RT 2: 대기 중인 구현 〉 종결(고정 또는 취소됨)	조사 중 RT 2가 종결/고정 또는 종결/취소되고 RT 1이 조사 중이면 VI가 구현 대기 중(이전에 가장 높은 우선순위)에서 조사 중(현재 가장 높은 우선순위)으로 변경됩니다.
RT 1: 모든 상태 RT 2: 모든 상태	취약한 항목 소스 상태가 수정(스캔 또는 임포트에 의해 업데이트됨)인 경우 그룹이 상태를 변경하면 취약한 항목이 종결/수정됨으로 변경됩니다. 이 조건은 다른 관련 그룹이 어떤 상태에 있든 상관없이 True입니다. 그룹 상태에 대한 취약한 항목 검색이 발생하지 않습니다.

VI 상태가 개별적으로 설정되면 다른 정정 작업과 마찬가지로 우선순위를 평가할 때 해당 상태가 고려됩니다. VI가 둘 이상의 정정 작업에 속하는 경우 다음 표에는 수행되는 업데이트가 나열되어 있습니다.

취약한 항목 상태를 개별적으로 설정 특수 케이스

그룹 내 취약한 항목 상태	취약한 항목 최종 상태
RT 1 상태: 조사 중 RT 2 상태: 조사 중 〉 대기 중인 구현 원래 VI 상태: 조사 중 〉 (VI에 설정)	대기 중인 구현 RT 2가 구현 대기 중으로 이동하고 RT 1이 조사 중으로 유지되면 VI가 구현 대기 중(가장 높은 우선순위)으로 변경됩니다.
RT 1: 조사 중 RT 2: 조사 중 〉 대기 중인 구현 원래 VI 상태: 연기됨 〉 (VI에 설정)	연기됨 RT 2가 구현 대기 중으로 이동하고 RT 1이 조사 중으로 남아 있을 때 VI는 지연 상태(가장 높은 우선순위)로 유지됩니다.

다음 표에서는 일반적인 취약한 항목이 있는 두 개의 정정 작업이 지연되면 최신 날짜에 도달할 때까지 상태가 지연됨을 보여줍니다.

취약한 항목 지연 상태 특수 케이스

그룹 내 취약한 항목 상태	취약한 항목 최종 상태
RT 1 상태: 검토 중 (4월 10일까지) RT 2 상태: 조사 중 〉 검토 중 (4월 30일까지) 원래 VI 상태: 검토 중 (4월 10일까지) 〉 (VI에 설정)	연기됨(4월 30일까지) RT 2가 Deferred(4월 30일까지)로 이동하고 RT 1이 Deferred(4월 10일까지)로 유지되면 VI는 Deferred(Apr-05까지)에서 Deferred 상태(Apr-30까지)로 변경됩니다.
RT 1: 검토 중 (7월 15일까지) RT 2: 조사 중 〉 검토 중 (7월 10일까지) 원래 VI 상태: 연기됨 〉 (7월 15일까지)	연기됨(7월 15일까지)

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약한 항목 지연 상태 특수 케이스

그룹 내 취약한 항목 상태	취약한 항목 최종 상태
	RT 2가 Deferred(7월 10일까지)로 이동하고 RT 1이 Deferred(Jul-15)로 유지되면 VI는 Deferred(Jul-15까지)로 유지됩니다.

도메인 분리에 대한 추가 설정

정확한 실행과 결과를 위해서는 에서 도메인을 분리 취약성 대응하기 위해 , 애플리케이션 취약성 대응, , 컨테이너 취약성 대응및 구성 준수에서 다음과 같은 주의사항 및 설정이 필요합니다.

모든 업그레이드에 대해 모든 최신 변경 내용이 업데이트되도록 문제를 방지하기 위해 전역 도메인의 비즈니스 논리 및 프로세스를 수정하지 마십시오. 각 도메인의 모든 비즈니스 논리와 프로세스를 개별적으로 복제하고 전역 도메인에서 비활성 상태인지 확인합니다. 그렇지 않으면 전역 도메인의 비즈니스 논리와 프로세스가 하위 도메인보다 우선합니다. 하위 도메인에서 위험 규칙을 생성했으며 전역 도메인에도 유사한 위험 규칙이 있는 경우 전역 도메인의 규칙이 하위 도메인의 규칙보다 우선한다고 가정해 보겠습니다.

계산기 및 규칙의 재평가

v20.0 이전에는 계산기 또는 규칙을 다시 적용하면 ## ## 플래그가 true로 설정되고 계산기 및 규칙을 다시 적용하는 예약 작업을 실행하도록 비즈니스 규칙이 트리거됩니다. v20.0부터는 ## ## 플래그에 의존할 필요가 없습니다. 계산기 다시 적용 버튼을 클릭하면 계산기 및 규칙을 다시 적용하는 백그라운드 작업이 트리거됩니다. 이렇게 하면 모든 도메인에 대한 계산기와 규칙을 생성할 수 있습니다.

롤업 계산기 설정

도메인에서는 테이블에 대해 하나의 롤업 계산기만 활성화되어 있어야 합니다. 예를 들어, *sn_vul_vulnerability* 롤업 계산기와 함께 전역 도메인의 정정 작업 롤업 과 함께 정정 작업 테이블을 생각해 보십시오. 동일한 도메인에서 동일한 테이블의 가중치를 변경하여 이 롤업 계산기를 복제하면 롤업 계산에 불일치가 발생합니다. 따라서 동일한 도메인에 테이블에 대한 롤업 계산기가 두 개 이상 있는 경우 롤업 계산기를 하나만 활성화해야 합니다.

검색된 항목 양식 필드

자산은 CI 조회 규칙을 사용하여 임포트될 때 CI 구성 관리 데이터베이스(CMDB) (구성 항목)와 자동으로 일치합니다. 일치하지 않는 CI에 대한 기록은 외부 공급업체 취약성 통합 임포트 중에 자동으로 생성되고 검색된 항목에 포함됩니다. 그러나 CL에 CMDB 없는 클라우드 자산의 경우 클라우드 자원 클래스에 레코드가 생성됩니다.

검색된 항목 필드

이러한 기록의 정보는 외부 공급업체 기록에서 수집되어 임포트 중에 분류됩니다.

이러한 필드는 검색된 항목 [sn_sec_cmn_src_ci] 테이블에 나열된 기록에서 찾을 수 있습니다.

다음 테이블에 나열된 필드에서 임포트한 데이터를 보려면 최소한 sn_vul.read_all 역할이 있어야 합니다.

필드	설명
번호	기록에 할당된 식별자입니다.
구성 항목	외부 공급업체 소스 통합에서 임포트한 구성 항목입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	v12.0부터 구성 항목은 해제된 CI를 필터링한 후 CI 목록의 최신 CI입니다.
클래스	에서 취약성 대응임포트하는 동안 CI에 할당되는 클래스입니다.
소스	외부 공급업체 소스 통합에서 임포트한 소스입니다.
CI 일치 규칙	항목을 작성하는 데 사용된 CI 일치 규칙입니다.
V18.0: DI에 대한 일치 유형	검색된 항목을 생성하는 데 사용되는 일치 유형입니다. 옵션은 다음과 같습니다. • VR에 의해 생성 • IRE에 의해 생성 • CI 조회와 일치 • IRE와 일치 • 수동으로 일치 (v24.0.6 부터 취약성 대응이 추가 옵션을 볼 수 있습니다. 검색된 항목 양식에서 CI를 수동으로 업데이트하면 이 옵션이 자동으로 설정됩니다.) 이 정보는 v18.0 이상에 대해 취약성 대응 채워진 데이터에만 사용할 수 있습니다. 기존 데이터에서는 이 열에 값이 포함되지 않습니다. 주: CI 조회 규칙을 다시 적용하면 DI의 일부 CI가 업데이트되어 이 열이 채워질 수 있습니다.
기타 일치 CI	CI 조회 규칙과 일치하는 다른 구성 항목의 목록입니다.
상태	임포트하는 동안 결정되는 CI의 상태입니다. 선택 항목은 다음과 같습니다. • 일치함: CMDB에서 일치하는 구성 항목을 찾았습니다. • 일치하지 않음: CMDB에서 일치하는 항목을 찾을 수 없습니다. 자리 표시자 기록이 생성됩니다.
작성됨	검색된 항목 기록이 생성된 날짜입니다.
업데이트됨	검색된 항목 기록이 업데이트된 날짜입니다.
업데이트한 사람	데이터를 업데이트한 사용자입니다.
호스트 태그	임포트하는 동안 이 검색된 항목에 할당된 호스트 태그입니다. 검색된 항목당 최대 31개의 호스트 태그를 사용할 수 있습니다.
전체 주소 도메인 이름	CMDB에 있는 이 CI와 관련된 데이터입니다.
MAC 주소	CMDB에 있는 이 CI와 관련된 데이터입니다.
운영 체제	이 CI와 연결된 운영 체제입니다.
NetBIOS	타사 소스 통합에서 임포트한 NetBIOS입니다.
IP 주소	CMDB에 있는 이 CI와 관련된 데이터입니다.
소스 데이터	소스에서 이 CI와 연결된 최신 데이터입니다.
V16: 초기 소스 데이터	소스에서 이 CI와 연결된 초기 데이터입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
V16: CI 재평가	스캐너에서 데이터를 수신합니다. 업데이트된 데이터가 있는 경우 값이 true로 설정됩니다. 주: 소스 데이터 값은 최신 소스 데이터에 따라 다시 계산됩니다. 스캐너에서 업데이트된 데이터를 검색하면 소스 데이터가 업데이트됩니다. 기존 소스 데이터 값이 초기 소스 데이터 필드로 이동됩니다. 검색된 항목을 다시 평가하려면 ### ## ## ## #### CI ## ## ## ### 활성화합니다.
에이전트가 존재함	에이전트가 자산에 설치되어 있는지 ### #### true 를 나타냅니다. 소스 데이터 열의 hostUID 및 UUID 값이 비어 있으면 이 값은 true로 채워집니다. 주: 이 필드는 의 v19.0 취약성 대응부터 나타납니다.

의 취약성 대응v23.0부터 테스트 결과 준수 **%(CI)** 열에는 해당 CI를 준수하는 테스트 결과의 백분율이 표시됩니다. 이 값을 얻으려면 정정 메트릭 업데이트 예약된 작업에서 calcTRComplianceForCI를 true로 설정해야 합니다.

주:
테스트 결과 규정 준수 **%(CI)** 값은 마지막 구성 규정 준수 검사 날짜 또는 비 인프라 마지막 규정 준수 검사 날짜 열에 비어 있지 않은 값이 있는 검색된 항목에 대해서만 채워집니다.

버전 18.0취약성 대응부터 , QualysTenable for Vulnerability Response 스캐너 Rapid7 는 클라우드 자산에 대해 다음과 같은 추가 메타데이터를 받을 수 있습니다.

필드	설명
클라우드 서비스 제공자	클라우드 컴퓨팅 서비스를 제공하는 클라우드 서비스 제공자의 이름입니다. 예를 들어 Amazon Web Services ()AWSMicrosoft Azure 및 GCP(Google Cloud Platform).
클라우드 영역	자원이 호스팅된 위치입니다.
클라우드 계정	클라우드 컴퓨팅 서비스에 액세스하기 위해 , GCP등의 클라우드 서비스 제공자AWS가 제공하는 계정입니다.
클라우드 자원 유형	Amazon Elastic Compute Cloud(EC2) 머신, AWS S3 버킷 등 클라우드에 있는 자산 유형입니다.
자원 ID	클라우드 컴퓨팅 환경에서 자원에 할당된 고유 식별자입니다. 이 ID는 자원을 식별하고 관리하는 데 사용됩니다.
자원 이름	클라우드 컴퓨팅 환경에서 자원을 식별하고 관리하는 데 사용되는 사용자 정의 이름입니다.
이미지	가상 머신 이미지 또는 서버 이미지는 운영 체제, 애플리케이션 및 기타 소프트웨어를 포함하는 미리 구성된 가상 머신입니다. 예: Amazon 머신 이미지.

클라우드 메타데이터를 기반으로 클라우드 CI와 일치시키기 위해 새로운 CI 조회 규칙인 '클라우드 자원 ID'가 도입되었습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약성 대응 취약성 양식 필드

NVD(국가 취약성 데이터베이스), CWE(일반적인 약점 열거) 또는 타사 통합에서 레코드를 다운로드하여 의 라이브러리에취약성 대응저장하면 취약성이 자동으로 생성됩니다.

NVD 항목 필드

다음 테이블에 나열된 필드에서 임포트한 데이터를 보려면 최소한 sn_vul.read_all 역할이 있어야 합니다.

이러한 필드는 국가 취약성 데이터베이스 항목 [sn_vul_nvd_entry] 테이블에 나열된 레코드에서 찾을 수 있습니다.

필드	설명
ID	이 취약성 항목의 식별자입니다.
위험 등급	(취약성과 관련된 VIT가 없는 경우 숨겨짐) 취약한 항목을 중요, 높음, 중간, 낮음 및 없음으로 구분하는 정량화된 위험 점수 입니다. 위험 등급에 대한 자세한 내용은 다음 문서를 참조하십시오 취약성 대응 계산기 및 취약성 계산기 규칙. 주: 이 기본 위험 등급은 솔루션 레코드의 위험 등급과 다릅니다.
위험 점수	(취약성과 관련된 VIT가 없는 경우 숨겨짐) 취약한 항목이 환경에 미치는 위험의 계산된 양입니다. 주: 이 기본 위험 점수는 솔루션 기록의 위험 점수와 다릅니다. 자세한 내용은 취약성 대응 계산기 및 취약성 계산기 규칙 문서를 참조하십시오.
심각도	이 취약성의 정규화된 심각도 수준입니다. NVD 및 타사 통합에 ServiceNow 대해 심각도 맵이 제공됩니다. 심각도 맵 생성 및 조정에 대한 자세한 내용은 다음 문서를 참조하십시오 취약성 대응 심각도 맵 생성.
익스플로잇 존재	예, 하나 이상의 익스플로잇이 이 취약성과 관련된 경우 가능합니다.
익스플로잇 기술 수준	이 취약성을 악용하는 데 필요한 가장 낮은 기술 수준입니다.
익스플로잇 공격 벡터	이 취약성에 대한 익스플로잇의 가장 취약한 공격 벡터입니다. SAM NVD가 활성화된 경우에 사용할 수 있습니다.
활성 VI	(취약성과 관련된 VIT가 없는 경우 숨겨짐) 이러한 취약성과 연관된 취약한 항목의 수로, 종결 상태가 아닙니다. 이 취약성에 대한 활성 VI가 없으면 위험 등급 및 위험 점수 가 표시되지 않습니다.
CWE 항목	이 취약성이 가장 적합한 일반 약점 열거형 요소에 대한 참조입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
게시 날짜	취약성이 게시된 날짜입니다.
마지막으로 수정됨	취약성이 마지막으로 수정된 날짜입니다.
요약	취약성에 대한 설명입니다.
Threat Intel(버전 20.0부터 취약성 대응)	위협 인텔리전스 제공: Qualys. 이 데이터를 사용하여 위협 행위자의 동기, 대상 및 공격 동작을 이해할 수 있습니다.
취약성 상세 정보	
CVSS v2	임포트된 CVSS v2 데이터
CVSS v3	2015년 이전에는 사용할 수 없었던 임포트된 CVSS v3 데이터입니다.
기본 솔루션	(취약성과 관련된 VIT가 없는 경우 숨겨짐) 취약성에서 참조하는 솔루션에서 파생된, 체인 내 대체 가능성이 가장 높은 솔루션. 체인에 둘 이상의 최고 대체가 있는 경우 값이 설정되지 않습니다. 수동으로 설정된 값은 후속 임포트에서 덮어쓸 수 있습니다. 취약한 항목에서 이 값을 수동으로 설정해야 합니다.
CISA 익스플로잇 (이 탭은 CISA 애플리케이션이 설치된 경우에만 사용할 수 있습니다.)	
CISA 기한	취약성 해결 기한입니다.
추가된 날짜	취약성이 CISA 카탈로그에 추가된 날짜입니다.
제품	취약성이 식별된 제품입니다.
벤더/프로젝트	식별된 취약성과 관련된 벤더입니다.
알려진 랜섬웨어 의 v21.0 취약성 대응부터 .	랜섬웨어 캠페인에 사용되는 것으로 알려진 필드가 CISA KEV(알려진 악용된 취약성) 카탈로그에서 수집되는 경우 선택됩니다. 플래그는 CVE(Common Vulnerabilities and Exposures) 수준에서 설정되고 TPE(외부 공급업체 항목)로 롤업됩니다.
정정 상태 (취약성과 연관된 VI가 없는 경우 숨겨짐)	
지연 제외	
취약한 항목	이러한 취약성이 있는 활성 취약한 항목의 수. 이 개수에서 지연된 취약한 항목은 제외됩니다.
총 VI	이러한 취약성이 있는 취약한 항목의 총 수. 이 개수에서 지연된 취약한 항목은 제외됩니다.
정정된 VI 비율(%)	이러한 취약성이 있는 취약한 항목의 정정 완료율. 이 개수에서 지연된 취약한 항목은 제외됩니다.
지연 포함	
취약한 항목	이러한 취약성이 있는 활성 취약한 항목의 수.
총 VI	이러한 취약성이 있는 취약한 항목의 총 수.
정정된 VI 비율(%)	이러한 취약성이 있는 취약한 항목의 정정 완료율.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
관련 링크	
상태 업데이트	마지막 업데이트의 날짜 및 시간을 표시합니다. 다음을 업데이트합니다. • 정정 작업 상태 • 위험 점수 및 등급 • 정정 상태 섹션의 활성 VIT, 총 VIT 등의 메트릭
관련 목록	
취약 항목	(취약성과 관련된 VIT가 없는 경우 숨겨짐) 이러한 취약성과 연관된 취약한 항목입니다.
취약성 참조	NVD에서 인용한 외부 소스의 취약성에 대한 정보입니다.
익스플로잇	이 취약성과 관련된 익스플로잇입니다.
솔루션	(취약성과 관련된 VIT가 없는 경우 숨겨짐) 이 취약성과 관련된 모든 취약성 솔루션 관리 통합 솔루션입니다.
약점	CVE(Common Vulnerabilities and Exposures)와 관련된 약점 데이터를 임포트했습니다.
취약한 소프트웨어	(소프트웨어가 CVE와 연결된 경우 숨겨짐) 취약성과 관련된 CPE(공통 플랫폼 열거형) 데이터를 임포트했습니다.
취약성 맬웨어 키트	취약성을 위해 다양한 스캐너 소스에서 임포트된 맬웨어입니다.

CWE 취약성 항목 필드

이러한 필드는 CWE [sn_vul_cwe] 테이블에 나열된 기록에서 찾을 수 있습니다.

필드	설명
CWE-ID	이 취약성 항목의 식별자입니다. 이 식별자는 범주와 약점 모두에 사용되며 두 데이터 세트 간에 고유합니다.
이름	이 CWE-ID에 할당된 설명이 포함된 이름입니다.
악용 가능성	질적 척도에서 약점이 악용될 가능성입니다. 다음 중 하나입니다. • 알 수 없음 • 낮음 • 보통 • 높음
OWASP 상위 10개 위치	OWASP 상위 10개 목록에서 이 취약성의 숫자 위치입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
SANS에서 25 위치로	SAN 상위 25개 목록에서 이 취약성의 숫자 위치입니다.
클래스	약점의 유형
상태	다음 중 하나입니다. • 완료 안 됨 • 초안 • 안정 • 사용하지 않음 • 사용되지 않음 • 불안정
추상화	다음 중 하나입니다. • 변형 • 클래스 • 기본 • 복합
업데이트됨	인스턴스에서 기록이 마지막으로 업데이트된 시간입니다.
기능 영역	영향을 받는 기능 영역의 목록입니다. 예를 들어 파일 처리입니다. 24/862 약점에 대해서만 채워집니다.
영향을 받는 리소스	영향을 받는 자원의 목록입니다. 예를 들어 파일 또는 디렉터리입니다. 51/863 약점에만 적용됩니다.
URL	이 취약성과 관련된 기술 자료 문서입니다.
설명	취약성에 대한 설명입니다.
통합 실행	이 CWE를 임포트한 통합 실행입니다.
섹션	
추가 상세 정보	약점을 추가로 설명하는 소프트웨어 개념 설명입니다. 다음이 포함됩니다. • 확장된 설명 • 백그라운드 세부 정보 • 메모
탐지 방법	애플리케이션에서 이 약점을 감지할 수 있는 방법에 대한 상세 정보입니다.
소개 모드	약점이 도입되는 단계(예: 구현, 아키텍처, 설계 등)입니다.
데모 예제	약점에 대한 코드 예제와 함께 설명이 제공됩니다.
잠재적 완화	애플리케이션 수명주기에서 발생하는 단계와 완화 효과를 포함하여 약점을 방지하는 방법에 대한 상세 정보입니다.
관련 목록	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
관계	이 취약성과 관련된 CWE입니다. 이 CWE와 다른 CWE의 관계를 나열합니다. parent/child, follows/precedes, requiredby/requires(복합 약점의 경우), CanAlsoBe, PeerOf, MemberOf를 포함할 수 있습니다.
관찰 예	이 약점을 대표하는 일부 CVE입니다.
일반적인 결과	범위 및 영향 측면에서 성공적인 익스플로잇의 결과입니다. 예: 범위: 기밀성 영향: 애플리케이션 데이터 읽기
구성원 자격	이러한 취약성이 있는 CWE 회원.
적용 가능 플랫폼	이 취약성과 관련된 플랫폼입니다.
애플리케이션 취약성 항목	이와 연관된 다른 애플리케이션 취약성 항목입니다.
외부 참조	외부 소스에서 얻은 취약성에 대한 정보입니다.

타사 취약성 항목 필드

이러한 필드는 외부 공급업체 취약성 항목 [sn_vul_third_party_entry] 테이블에 나열된 레코드에서 찾을 수 있습니다.

필드	설명
ID	이 취약성 항목의 식별자입니다.
버전 16.0: CVE	이 외부 공급업체 취약성과 연관된 여러 CVE(일반적인 취약성 및 노출)입니다.
소스	취약성의 출처(스캐너 또는 물리적 테스트)입니다.
위험 등급	취약한 항목을 중요, 높음, 중간, 낮음 및 없음으로 구분하는 정량화된 위험 점수 입니다. 위험 등급에 대한 자세한 내용은 을 참조하십시오 취약성 대응 계산기 및 취약성 계산기 규칙. 주: 이 기본 위험 등급은 솔루션 기록의 위험 등급과 같지 않습니다.
위험 점수	위험 점수를 기준으로 취약한 항목이 환경에 미치는 위험의 계산된 양입니다. 주: 이 기본 위험 점수는 솔루션 기록의 위험 점수와 다릅니다. 자세한 내용은 취약성 대응 계산기 및 취약성 계산기 규칙 문서를 참조하십시오.
심각도	이 취약성의 정규화된 심각도 수준입니다. NVD 및 타사 통합에 ServiceNow 대해 심각도 맵이 제공됩니다. 심각도 맵 생성 및 조정에 대한 자세한 내용은 다음 문서를 참조하십시오 취약성 대응 심각도 맵 생성.
익스플로잇 존재	예, 하나 이상의 익스플로잇이 이 취약성과 관련된 경우 가능합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
익스플로잇 기술 수준	이 취약성을 악용하는 데 필요한 가장 낮은 기술 수준입니다.
익스플로잇 공격 벡터	이 취약성에 대한 익스플로잇의 가장 취약한 공격 벡터입니다.
활성 VI	이러한 취약성과 연관된 취약한 항목의 수로, 종결 상태가 아닙니다.
범주	외부 공급업체 통합에서 제공하는 분류입니다. 임무 수행을 돕는다.
정정 유형	정정 작업의 유형입니다. • 패치 • 구성 변경 • 패치 및 구성 변경 • 대책
CWE 항목	이 취약성이 가장 적합한 일반 약점 열거형 요소에 대한 참조입니다.
PCI	이 확인란을 선택하면 결제 정보가 노출될 위험이 크다는 취약성 플래그가 지정됩니다.
PCI 심각도	결제 정보의 노출에 대한 위험 수준입니다. 〔Qualys만 해당.〕
게시 날짜	취약성이 게시된 날짜입니다.
마지막으로 수정됨	취약성이 마지막으로 수정된 날짜입니다.
요약	취약성에 대한 설명입니다.
취약성 상세 정보	
CVSS v2	임포트된 CVSS v2 데이터
CVSS v3	2015년 이전에는 사용할 수 없었던 임포트된 CVSS v3 데이터입니다.
위협	이 취약성으로 인한 위협에 대한 설명입니다.
기본 솔루션	취약성에서 참조하는 솔루션에서 파생된, 체인 내 대체 가능성이 가장 높은 솔루션. 체인에 둘 이상의 최고 대체가 있는 경우 값이 설정되지 않습니다. 수동으로 설정된 값은 후속 임포트에서 덮어쓸 수 있습니다. 취약한 항목에서 이 값을 수동으로 설정해야 합니다.
정정 참고 사항	벤더에서 가져온 정정 솔루션에 대한 설명입니다.
정정 상태	
지연 제외	
취약한 항목	이러한 취약성이 있는 활성 취약한 항목의 수. 이 개수에서 지연된 취약한 항목은 제외됩니다.
총 VI	이러한 취약성이 있는 취약한 항목의 총 수. 이 개수에서 지연된 취약한 항목은 제외됩니다.
정정된 VI 비율(%)	이러한 취약성이 있는 취약한 항목의 정정 완료율. 이 개수에서 지연된 취약한 항목은 제외됩니다.
지연 포함	
취약한 항목	이러한 취약성이 있는 활성 취약한 항목의 수.
총 VI	이러한 취약성이 있는 취약한 항목의 총 수.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
정정된 VI 비율(%)	이러한 취약성이 있는 취약한 항목의 정정 완료율.
관련 링크	
상태 업데이트	마지막 업데이트의 날짜 및 시간을 표시합니다. 다음을 업데이트합니다. • 정정 작업 상태 • 위험 점수 및 등급 • 정정 상태 섹션의 활성 VI, 총 VI와 같은 메트릭
관련 목록	
취약 항목	이러한 취약성과 연관된 취약한 항목입니다.
취약성 참조	NVD에서 인용한 외부 소스의 취약성에 대한 정보입니다.
CVE	이 취약성과 관련된 CVE(일반 취약성 열거형) 기록입니다.
범주	이 취약성과 관련된 범주입니다.
익스플로잇	이 취약성과 관련된 익스플로잇입니다.
취약성 맬웨어 키트	이 취약성과 관련된 맬웨어 키트입니다.
솔루션(Rapid7)	Rapid7 솔루션 통합의 솔루션 정보입니다. 사용 가능한 경우 표시됩니다.
익스플로잇 프레임워크	이 취약성과 관련된 익스플로잇 프레임워크.
솔루션	취약성 솔루션 관리 이 취약성과 연관된 솔루션.
CISA 익스플로잇	
CISA 존재	외부 공급업체 취약성 항목 테이블에 대한 CISA 익스플로잇이 존재합니다.
CISA 기한	취약성 해결 기한입니다.

정정 작업 양식 필드

분석가는 정정 작업을 사용하여 진행 상황을 모니터링하고 중재 프로세스를 보다 효율적으로 추진할 수 있습니다.

이러한 필드는 정정 작업 [sn_vul_vulnerability] 테이블에 나열된 기록에서 찾을 수 있습니다.

다음 테이블에 나열된 필드에서 임포트한 데이터를 보려면 최소한 sn_vul.read_all 역할이 있어야 합니다.

정정 작업 필드

필드	설명
번호	이 기록에 대해 자동으로 생성된 VI(취약한 항목) 번호입니다.
위험 등급	중요, 높음, 중간, 낮음 및 없음의 범위로 구분된 취약한 항목 위험 점수의 롤업입니다. 위험 등급에 대한 자세한 내용은 을 참조하십시오 취약성 대응 계산기 및 취약성 계산기 규칙.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

정정 작업 필드

필드	설명
	주: 이 기본 위험 등급은 솔루션 레코드의 위험 등급과 다릅니다.
위험 점수	이 정정 작업과 연결된 모든 취약한 항목의 위험 점수를 롤업합니다. 취약한 항목이 집합적으로 환경에 미치는 위험의 양입니다. 주: 이 기본 위험 점수는 솔루션 기록의 위험 점수와 다릅니다.
정정 대상	처음 식별된 이후 취약한 항목을 정정해야 하는 날짜입니다. 정정 대상에 대한 자세한 내용은 다음 문서를 참조하십시오 취약성 대응 정정 대상 규칙.
정정 상태	작업에 대한 정정 상태입니다. 기한이 가장 가까운 취약한 항목에 의해 결정됩니다. 공개 그룹의 경우 상태는 다음과 같습니다. • 비행 중 • 대상에 접근 중 • 대상 놓침 종결된 그룹의 경우 상태에는 다음이 포함됩니다. • 대상 없음 • 대상 만족 • 대상 놓침 계산된 정정 대상 날짜의 경우, 작업이 종결되면 모든 종결된 취약한 항목의 전반적인 정정 상태가 작업에 표시됩니다. 이에 따라 작업이 날짜를 지켰는지 여부가 결정됩니다. 종결된 작업 중 정정 대상 날짜가 있는 종결된 항목이 없는 경우 해당 작업의 정정 상태는 대상 없음 입니다. 종결된 항목 중 하나라도 목표 날짜를 놓친 경우 대상 누락 입니다. 하나 이상의 종결된 VI가 목표를 충족하고 다른 VI가 목표를 빗나간 것이 없는 경우 목표 만족 입니다.
상태	작업의 진행 상태입니다. 상태는 다음과 같습니다. • 오픈 • 조사 중 • 대기 중인 구현 • 연기됨 • 검토 중 • 해결 일시 • 종결됨

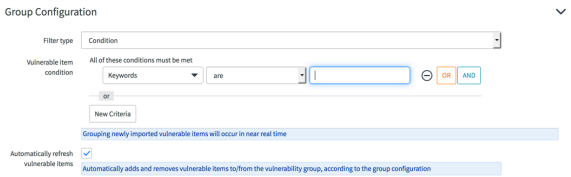
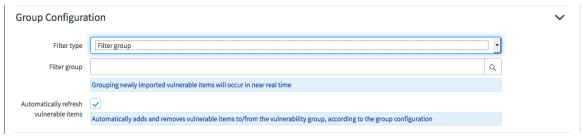
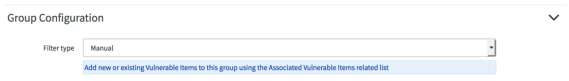
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

정정 작업 필드

필드	설명
	상태에 대한 자세한 내용은 취약성 대응 정정 작업 및 취약한 항목 상태 문서를 참조하십시오.
위험 감소를 위한 종료 날짜	정정 작업에 적용된 보상 통제가 만료되는 날짜입니다. 주: 이 필드는 값을 사용할 수 있는 경우에만 나타납니다.
할당 그룹	이 정정 작업을 수행하도록 선택한 그룹입니다.
담당자	이 취약성에 대해 작업하는 선택한 할당 그룹의 개인입니다.
작성됨	이 정정 작업이 생성된 날짜입니다.
업데이트됨	이 정정 작업이 마지막으로 업데이트된 날짜입니다.
취약성	작업에 적용할 수 있는 취약성입니다. (그룹이 단일 취약성을 기반으로 형성될 때 표시됩니다.)
간단한 설명	이 정정 작업에 대한 간략한 설명입니다.
검토 중 (RT가 검토 중 상태일 때 표시)	
요청한 사람	연기를 요청한 개인입니다.
원하는 이유	지연 사유.
원하는 상태	승인자가 요청한 상태입니다.
원하는 하위 상태	승인자가 요청한 이유입니다.
연기(작업이 연기됨 상태일 때 표시)	
연기한 사람	작업을 연기한 개인입니다.
만료 연기	지연이 만료되는 날짜입니다.
지연 이유	지연 이유입니다.
해결 (RT가 해결됨 상태일 때 표시)	
해결한 사람	정정 작업을 해결한 개인입니다.
해결 날짜	정정 작업이 해결된 날짜입니다.
해결 참고 사항	추가 정보입니다.
닫기 (RT가 닫힘 상태일 때 표시)	
종결한 사람	정정 작업을 해결한 개인입니다.
종결됨	정정 작업이 종결된 날짜입니다.
종결 메모	추가 정보입니다.
그룹 구성 (모든 상태에서 표시)	
필터 유형	그룹의 취약성을 선택하는 데 사용되는 필터링 유형입니다. 조건

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

정정 작업 필드

필드	설명
	 **주:** 한 시간에 한 번 새로 고침됩니다. 필터 그룹  **주:** 한 시간에 한 번 새로 고침됩니다. 수동 
정정 상태	
지연 제외	
취약한 항목	이 작업 내의 활성 취약한 항목 수입니다. 이 개수에서 지연된 취약한 항목은 제외됩니다.
총 VI	이 작업 내 총 취약한 항목 수입니다. 이 개수에서 지연된 취약한 항목은 제외됩니다.
정정된 VI 비율(%)	이 작업 내 취약한 항목의 정정 완료율입니다. 이 개수에서 지연된 취약한 항목은 제외됩니다.
지연 포함	
취약한 항목	이 작업 내의 활성 취약한 항목 수입니다.
총 VI	이 작업 내 총 취약한 항목 수입니다.
정정된 VI 비율(%)	이 작업 내 취약한 항목의 정정 완료율입니다.
메모 (모든 상태에서 표시)	
설명	그룹 또는 정정 작업에 대한 설명입니다.
추가 의견	추가 정보입니다.
활동	시스템 참고.
관련 링크	
취약한 항목 재검사	취약한 항목의 재검사를 트리거하여 문제가 해결되었는지 확인합니다.
상태 업데이트	마지막 업데이트의 날짜 및 시간을 표시합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

정정 작업 필드

필드	설명
	작업의 VI에서 다음을 롤업합니다. • 정정 작업 상태 • 위험 점수 및 위험 등급 • 정정 목표 날짜 및 상태(해당하는 경우) • 정정 상태 섹션의 활성 VI, 총 VI와 같은 메트릭
관련 목록	
취약한 항목	이 작업의 취약한 항목입니다.
작업 SLA	이 작업과 연결된 플랫폼 SLA입니다.
기본 설정 솔루션	이 작업에서 취약한 항목의 기본 솔루션입니다.
관련 변경요청	이 작업과 연결된 변경 요청입니다.
요청된 승인	(작업이 검토 중 상태인 경우 표시됩니다.) 승인자 목록입니다. 지연이 승인되면 정정 작업이 연기됨 상태로 전환됩니다.

질문서 구성 양식 필드

VR 예외 관리 설정 양식의 VR 질문서 구성 섹션에서 취약성 또는 정정 작업을 각각 필터링하여 고유한 취약성 또는 정정 작업 모음에 대한 고유한 질문서를 정의할 수 있습니다.

VR 예외 관리 설정 양식의 VR 질문서 구성 섹션에서 새로 만들기 버튼을 선택하면 질문서 구성 양식이 나타납니다.

질문서 구성 양식 필드

필드	설명
이름	질문서의 이름입니다.
승인 규칙	질문서를 적용할 수 있는 승인 규칙입니다. • 취약성 그룹에 대한 예외 요청 • 취약한 항목에 대한 예외 요청 • 취약성 그룹에 대한 가양성 • 취약한 항목에 대한 가양성 • 정정 작업의 위험 감소 요청에 대한 취약한 그룹에 대한 보상 통제에 대한 질문서입니다. • 취약한 항목의 위험 감소 요청에 취약한 항목에 대한 보상 통제에 대한 질문서입니다.
설명	질문서 구성에 대한 짧은 설명입니다.
순서	요청 중에 순서가 가장 낮은 질문서가 나타납니다.
활성	기본적으로 활성화되며, 이는 질문서가 사용 중임을 나타냅니다.
테이블	승인 규칙을 적용할 수 있는 테이블입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

질문서 구성 양식 필드

필드	설명
	• 취약한 항목 〔취약한 항목과 관련된 승인 규칙에 대한 sn_vul_vulnerable_item. • 정정 작업과 관련된 승인 규칙에 대한 정정 작업 〔sn_vul_vulnerability〕입니다.
조건	질문서가 표시되어야 하는 기록의 조건입니다. 이유를 제외한 취약한 항목 및 정정 작업의 모든 필드에 조건을 적용할 수 있습니다.
질문서	정정 소유자가 예외, 가양성 또는 위험 감소를 요청할 때 나타나는 질문서

관련 정보

에 대한 예외 관리 구성 취약성 대응

위험 감소를 위한 질문서 구성

취약성 대응 취약한 항목 양식 필드

타사 취약성 통합 임포트 중에 취약한 항목이 자동으로 생성됩니다.

취약한 항목 필드

다음 테이블에 나열된 필드에서 임포트한 데이터를 보려면 최소한 sn_vul.read_all 역할이 있어야 합니다.

이러한 필드는 취약한 항목 [sn_vul_vulnerable_item] 테이블에 나열된 기록에서 찾을 수 있습니다.

SAM NVD 취약성 스캔 을 활성화한 경우 기록이 사용 중인 구성 관리 데이터베이스(CMDB) 소프트웨어와 비교되고 취약한 소프트웨어 또는 CI(구성 항목)와 일치하는 항목을 찾을 수 있습니다.

필드	설명
보안 태그 선택	기록에 메타데이터를 추가하거나 이 보안 인시던트 기록에 접근할 수 있는 사람을 식별하는 보안 태그입니다. 이 필드는 취약한 항목이 저장된 후에만 나타납니다.
번호	이 기록에 대해 자동으로 생성된 취약한 항목 번호입니다.
소스	이 취약한 항목을 발견한 스캐너입니다.
위험 등급	취약한 항목을 중요, 높음, 중간, 낮음 및 없음으로 구분하는 정량화된 위험 점수 입니다. 위험 등급에 대한 자세한 내용은 다음 문서를 참조하십시오 취약성 대응 계산기 및 취약성 계산기 규칙. 주: 이 기본 위험 등급은 솔루션 기록의 위험 등급과 다릅니다.
위험 점수	취약한 항목이 환경에 미치는 위험의 계산된 양입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	주: 이 기본 위험 점수는 솔루션 기록의 위험 점수와 다릅니다. 자세한 내용은 취약성 대응 계산기 및 취약성 계산기 규칙 문서를 참조하십시오.
취약성	이 취약한 항목과 관련된 취약성 ID입니다.
구성 항목	영향을 받는 자산입니다.
상태	이 필드는 기본적으로 공개로 설정되지만 취약성을 즉시 정정할 준비가 되면 조사 중 으로 변경할 수 있습니다.
위험 감소를 위한 종료 날짜	취약한 항목에 적용된 보상 통제가 만료되는 날짜입니다. 주: 이 필드는 원래 위험 점수 값을 사용할 수 있는 경우에만 나타납니다.
할당 그룹	이 정정 작업을 수행하도록 선택한 그룹입니다.
담당자	이 취약성에 대해 작업하는 선택한 할당 그룹의 개인입니다.
작성됨	인스턴스에서 이 취약한 항목이 생성된 날짜입니다.
마지막으로 시작한 시간	인스턴스에서 취약한 항목이 가장 최근에 열린 날짜입니다. 처음에는 취약한 항목의 생성 날짜와 동일하지만 취약한 항목이 종결된 후 다시 열린 경우 마지막으로 시작한 날짜에는 재오픈된 날짜 및 시간이 포함됩니다.
업데이트됨	마지막 검사 날짜입니다.
기간	VI가 마지막으로 열린 날짜 이후 활성화된 기간입니다. VI가 닫혀 있으면 Age 필드의 값이 0으로 설정됩니다. Age 필드에 대한 자세한 내용은 다음 문서를 참조하십시오 취약한 항목 기간 계산 및 표시. 연령 기간 계산을 사용자 지정하는 방법에 대한 자세한 내용은 KB1703270 문서를 참조하십시오.
취약성	
요약	취약성에 대한 설명입니다.
심각도	이 취약성의 정규화된 심각도 수준입니다. NVD 및 타사 통합에 ServiceNow 대해 심각도 맵이 제공됩니다. 심각도 맵 생성 및 조정에 대한 자세한 내용은 다음 문서를 참조하십시오 취약성 대응 심각도 맵 생성.
취약성 점수(v3)	CVSS v3 점수입니다.
취약성 점수(v2)	CVSS v2 점수입니다.
익스플로잇 존재	예, 하나 이상의 익스플로잇이 이 취약한 항목과 관련된 취약성과 관련된 경우 가능합니다.
익스플로잇 공격 벡터	이 취약한 항목과 관련된 취약성을 악용한 가장 취약한 공격 벡터입니다.
익스플로잇 기술 수준	이 취약한 항목과 연관된 취약성을 악용하는 데 필요한 가장 낮은 기술 수준입니다.
게시 날짜	취약성이 게시된 날짜입니다.
마지막으로 수정됨	취약성이 마지막으로 수정된 날짜입니다.
위협	위협에 대한 관련 정보입니다. 취약한 항목 기록에서 끌어옵니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	주: 여기에서 변경한 내용은 취약한 항목 기록을 업데이트합니다.
정정 참고 사항	취약한 항목 기록에서 가져온 위협에 대한 관련 솔루션입니다.
정정 에서만 사용할 수 있습니다 취약성 솔루션 관리.	
기본 솔루션	취약성 기록에서 임포트한 기본 솔루션입니다. 주: 여기에서 수동으로 변경해도 취약성 기록은 변경되지 않으며 후속 임포트 시 VI에서 변경되지 않은 상태로 유지됩니다.
요약	솔루션 기록에서 요약을 임포트했습니다.
솔루션 유형	잠재적 또는 기본 솔루션입니다.
초기 탐지	
DNS 이름	도메인 이름 서비스 이름의 이름입니다. CI가 제공되지 않은 경우 이 필드는 일치하는 CI를 조회하는 데 사용됩니다(있는 경우).
NetBIOS 이름	NetBIOS의 이름입니다. CI가 제공되지 않은 경우 이 필드는 일치하는 CI를 조회하는 데 사용됩니다(있는 경우).
IP 주소	IPv4 또는 IPv6 주소입니다. CI가 제공되지 않은 경우 이 필드는 일치하는 CI를 조회하는 데 사용됩니다(있는 경우).
포트	포트 주소
프로토콜	프로토콜의 이름입니다.
SSL	SSL 암호화 사용 여부.
탐지	
상태	탐지 상태입니다.
첫 발견	외부 공급업체 소스가 이 자산에서 탐지를 처음 발견한 날짜입니다.
마지막 발견	외부 공급업체 소스가 이 자산에서 마지막으로 탐지를 발견한 날짜입니다.
DNS 이름	도메인 이름 서비스 이름의 이름입니다. CI가 제공되지 않은 경우 이 필드는 일치하는 CI를 조회하는 데 사용됩니다(있는 경우).
NetBIOS 이름	NetBIOS의 이름입니다. CI가 제공되지 않은 경우 이 필드는 일치하는 CI를 조회하는 데 사용됩니다(있는 경우).
IP 주소	IPv4 또는 IPv6 주소입니다. CI가 제공되지 않은 경우 이 필드는 일치하는 CI를 조회하는 데 사용됩니다(있는 경우).
포트	포트 주소
프로토콜	프로토콜의 이름입니다.
SSL	SSL 암호화 사용 여부.
발견 시간	외부 공급업체 소스에서 이 자산에 대해 이러한 취약성을 탐지한 횟수입니다.
통합 실행	탐지를 임포트한 통합 실행입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
종결 취약한 항목이 정정되고 종결된 후에 사용할 수 있습니다. 이 섹션의 항목은 읽기 전용입니다.	
종결한 사람	취약한 항목을 종결한 사람입니다.
종결됨	취약한 항목이 종결된 날짜입니다.
종결 메모	종결에 포함된 정보입니다.
종결 기간	VI가 종결된 후의 기간입니다. VI가 다시 열리면 Age closed 필드의 값이 0으로 설정됩니다. Age 종결 필드에 대한 자세한 내용은 을 참조하십시오 취약한 항목 기간 계산 및 표시. 종결 기간 기간 계산을 사용자 지정하는 방법에 대한 자세한 내용은 KB1703270 문서를 참조하세요.
메모	
추가 의견/작업 메모	관련 정보입니다. 추가 코멘트를 추가하려면 확인란을 선택합니다. 취약성 대응 v20.0부터는 지연된 취약한 항목에 대한 메모 섹션에 작업 메모를 추가할 수 있습니다.
활동	작업 메모가 생성된 경우에만 나타납니다.
관련 링크	
위험 점수 계산	취약성 심각도 또는 위험 점수 계산기를 사용하도록 설정하면 위험 점수 필드가 업데이트됩니다.

취약 항목 관련 목록은 다음과 같습니다.

관련 목록	설명
정정 작업	이 취약한 항목과 연결된 작업입니다.
영향 받는 작업	이 취약한 항목과 연결된 작업입니다.
연결된 IP 주소	취약성 통합 애플리케이션이 설치된 경우 Qualys Vulnerability Integration 사용할 수 있습니다. 중복을 제거하는 동안 발견되는 IP 주소입니다.
영향을 받는 서비스	이 취약한 항목의 영향을 받는 비즈니스 서비스입니다. CMDB 기록에서 이 정보를 사용할 수 있는 경우에 표시됩니다. 이 정보는 수동으로 입력하거나 애플리케이션을 사용하여 입력할 수 있습니다 ServiceNow# 서비스 매핑 . 자세한 내용은 서비스 매핑 을 참조하십시오. 취약한 항목과 연결된 영향을 받는 CI가 추가되거나 업데이트되면 기록이 저장될 때 이 관련 목록의 정보가 자동으로 업데이트됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관련 목록	설명
상태 변경 승인	VIT와 연관된 변경 요청 및 기타 승인 정보의 상태입니다.
Qualys 티켓	Qualys 이 취약한 항목과 연결된 티켓 통합 정보입니다.

솔루션 양식 필드

솔루션은 외부 공급업체 솔루션 통합에서 기록을 다운로드하여 의 취약성 대응솔루션에 저장하면 자동으로 생성됩니다.

솔루션 통합 항목 필드

이 테이블에서 임포트한 필드는 읽기 전용입니다.

필드	설명
번호	솔루션에 할당된 식별자입니다.
소스	솔루션의 출처입니다.
소스 ID	이 솔루션의 소스 식별자입니다.
위험 등급	솔루션 기록 위험 점수를 중요에서 없음까지 구분합니다. 솔루션 위험 등급에 대한 자세한 내용은 을 참조하십시오취약성 솔루션 관리. 주: 솔루션 위험 등급 은 취약한 항목, 타사 취약성 항목 및 정정 작업 기록의 위험 등급과 동일하지 않습니다.
위험 점수	이 솔루션을 기본 솔루션으로 사용하는 취약한 항목의 수와 위험 점수를 기준으로 한 가중 계산입니다. 솔루션 위험 점수에 대한 자세한 내용은 다음 문서를 참조하십시오 취약성 솔루션 관리. 주: 솔루션 기록 위험 점수 가 취약한 항목, 타사 취약성 항목 및 정정 작업 기록과 같지 않습니다. 위험 점수. SAM NVD가 활성화된 경우에 사용할 수 있지만 취약성과 연결된 활성 VI(취약한 항목)가 없는 경우 솔루션 위험 점수 는 0으로 설정됩니다.
가장 높은 대체	이를 대체할 솔루션이 없음을 나타냅니다.
솔루션 유형	솔루션의 종류입니다. 선택 항목은 다음과 같습니다. • 임시 해결책 • 완화 • 벤더 수정 • 패치 • 롤업 • 권리

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	• 수정하지 않을 예정 • 사용할 수 있는 항목 없음
다시 시작해야 함	다시 시작해야 합니다. 선택 항목은 다음과 같습니다. • 예 • 아니요 • 아마도
게시 날짜	소스에서 취약성을 게시한 날짜입니다.
마지막으로 수정됨	소스에서 취약성이 마지막으로 수정된 날짜입니다.
요약	솔루션의 정정 요약입니다.
공지	솔루션과 관련된 보안 게시판입니다.
제품 범주	솔루션이 적용되는 제품 범주입니다.
제품	솔루션이 적용되는 제품입니다.
솔루션 상세 정보	
설명	솔루션 소스에서 사용할 수 있는 콘텐츠가 없는 경우 자세한 내용을 보려면 다른 관련 섹션 또는 솔루션으로 이동하게 됩니다.
링크	솔루션과 연결된 임포트한 인터넷 자원입니다.
취약성 상세 정보	
취약성 참고 사항	솔루션으로 정정된 취약성의 요약입니다.
정정 상태	
기본 솔루션 대상 취약한 항목 및 취약한 항목의 고유 CI(구성 항목)에 대한 정정 상태로, 기본 솔루션입니다. 주: 고유 CI는 연결된 VI 수에 관계없이 한 번만 계산되는 CI입니다.	
취약 항목	정정에 이 솔루션이 기본인 활성(종결되지 않음) 취약한 항목 수. 이 개수에서 지연된 취약한 항목은 제외됩니다.
총 VI	정정에 이 솔루션이 기본인 활성 및 종결된 취약한 항목 수. 이 개수에서 지연된 취약한 항목은 제외됩니다.
정정된 VI 비율(%)	VI(취약한 항목) 정정에 대한 완료율입니다. 이 솔루션이 기본인 VI에 적용됩니다. 이 개수에서 지연된 VI는 제외됩니다.
남아 있는 CI	정정에 이 솔루션이 기본인 하나 이상의 활성 취약한 항목과 연결된 고유 CI 수. 이 개수에서 지연된 취약한 항목의 CI는 제외됩니다.
총 CI	정정에 이 솔루션이 기본인 하나 이상의 활성 및 종결된 취약한 항목과 연결된 고유 CI 수. 이 개수에서 지연된 취약한 항목의 CI는 제외됩니다.
정정된 CI 비율(%)	정정된 고유 CI의 완료율(해당 CI와 이 솔루션에 대한 모든 VI가 정정됨을 의미). 기본 솔루션이 있는 취약한 항목에 연결된 총 고유 CI 수에 대해

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	정정된 CI 수에 따라 결정됩니다. 이 개수에서 지연된 취약한 항목의 CI는 제외됩니다.
기본 솔루션 대상(지연 포함) 취약한 항목 및 취약한 항목의 고유 CI(지연됨)에 대한 정정 상태로, 선호되는 솔루션입니다.	
취약 항목	정정에 이 솔루션이 기본인 활성(종결되지 않음) 취약한 항목 수.
총 VI	정정에 이 솔루션이 기본인 활성 및 종결된 취약한 항목 수.
정정된 VI 비율(%)	VI(취약한 항목) 정정에 대한 완료율입니다. 이 솔루션이 기본인 VI에 적용됩니다.
남아 있는 CI	정정에 이 솔루션이 기본인 하나 이상의 활성 취약한 항목과 연결된 고유 CI 수.
총 CI	정정에 이 솔루션이 기본인 하나 이상의 활성 및 종결된 취약한 항목과 연결된 고유 CI 수.
정정된 CI 비율(%)	정정된 고유 CI의 완료율(해당 CI와 이 솔루션에 대한 모든 VI가 정정됨을 의미). 기본 솔루션이 있는 취약한 항목에 연결된 총 고유 CI 수에 대해 정정된 CI 수에 따라 결정됩니다. 이 개수에서 지연된 취약한 항목의 CI는 제외됩니다.
잠재적 솔루션 대상 이 솔루션과 관련된 취약성이 있는 취약한 항목 및 해당 고유 CI에 대한 정정 상태입니다.	
취약한 항목	이 솔루션이 정정을 위한 잠재적 솔루션인 활성(종결되지 않음) 취약한 항목 수. 이 개수에서 지연된 취약한 항목은 제외됩니다.
남아 있는 CI	이 솔루션이 정정을 위한 잠재적 솔루션인 하나 이상의 활성 취약한 항목과 연결된 고유 CI 수. 이 개수에서 지연된 취약한 항목은 제외됩니다.
잠재적 솔루션 대상(지연 포함) 취약한 항목 및 해당 고유 CI(지연됨 포함)에 대한 정정 상태이며, 기본 솔루션 수를 포함하여 이 솔루션으로 정정할 수 있는 취약성이 있습니다.	
취약한 항목	이 솔루션이 정정을 위한 잠재적 솔루션인 활성(종결되지 않음) 취약한 항목 수.
남아 있는 CI	이 솔루션이 정정을 위한 잠재적 솔루션인 하나 이상의 활성 취약한 항목과 연결된 고유 CI 수.
메모	
내부 메모	정정 전문가에게 제공되는 편집 가능한 필드입니다.
관련 링크	
상태 업데이트	정정 상태가 마지막으로 업데이트된 날짜 및 시간입니다. 다음을 업데이트합니다. • 정정 작업 상태 • 위험 점수 및 등급 • 정정 상태 섹션의 메트릭
관련 목록	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
취약 항목	정정을 위한 기본 솔루션으로 이 솔루션과 연결된 취약한 항목입니다.
외부 공급업체 취약성	이 솔루션과 연결된 외부 공급업체 취약성입니다.
CVE	이 솔루션과 관련된 CVE(일반적인 취약성 및 노출) 취약성입니다.
정정 작업	정정에 선호되는 이 솔루션의 관련 취약한 항목을 포함하는 정정 작업입니다.
이전 솔루션	이 솔루션의 취약성 중 하나 이상을 해결하는 이전 솔루션입니다.
대체 솔루션	이 솔루션의 모든 취약성을 해결하는 최신 솔루션입니다. 가장 높은 대체 확인란을 선택하면 이 목록이 비어 있습니다.

할당 해제 요청에 대한 승인 워크플로우 구성

사용자와 그룹의 취약한 항목(VI, VIT), 정정 작업, AVIT(애플리케이션 취약한 항목) 및 CVIT(컨테이너 취약한 항목)에서 할당을 제거하기 위한 승인 워크플로우를 설계할 수 있습니다.

VIT, 정정 작업, AVIT 및 CVIT에는 각각 기본 승인 규칙이 있습니다. 각 승인 규칙에는 기본 승인 구성이 있습니다. 각 승인 구성에는 기본 승인자 수준이 있습니다. VIT, 정정 작업, AVIT 및 CVIT에 대한 승인 규칙은 기본적으로 활성화되어 있습니다. 관리자는 다음으로 이동하여 다음 작업을 수행할 수 있습니다. 모두 〉 취약성 대응 〉 내 승인 〉 승인 규칙 적절한 승인 규칙을 선택합니다.

- 승인 규칙을 사용하거나 사용하지 않도록 설정합니다.
- 승인 구성을 만들고 업데이트합니다.
- 승인 규칙이 적용되는 취약한 항목 및 정정 작업에 대한 조건을 정의합니다.
- 여러 승인자 수준을 생성하고 업데이트합니다.

다음 테이블에는 기본 시스템과 함께 제공되는 VIT, 정정 작업, AVIT 및 CVIT에 대한 기본 승인 규칙, 승인 구성 및 승인자 수준이 나와 있습니다.

기본 승인 규칙, 승인 구성 및 승인자 수준

유형	승인 규칙	승인 구성	승인자 수준
VIT 또는 VI	취약한 항목 필드 변경 요청	취약한 항목 필드 변경 요청	VI에 대한 수준 1 요청 할당 해제
정정 작업	취약성 그룹 필드 변경 요청	취약성 필드 변경 요청	수준 1 - VG에 대한 요청 할당 해제
AVIT	애플리케이션 취약한 항목 필드 변경 요청	애플리케이션 취약성 필드 변경 요청	앱 취약성 항목 할당 해제
CVIT	컨테이너 관리 승인	기본 구성 할당 해제 CVIT	CVIT 미할당 승인 수준 - 1

할당 해제 요청을 승인하는 방법에 대한 자세한 내용은 문서를 참조하십시오 에서 할당 해제 요청 승인 또는 거부 취약성 대응.

취약성 대응 정정 작업 규칙의 예

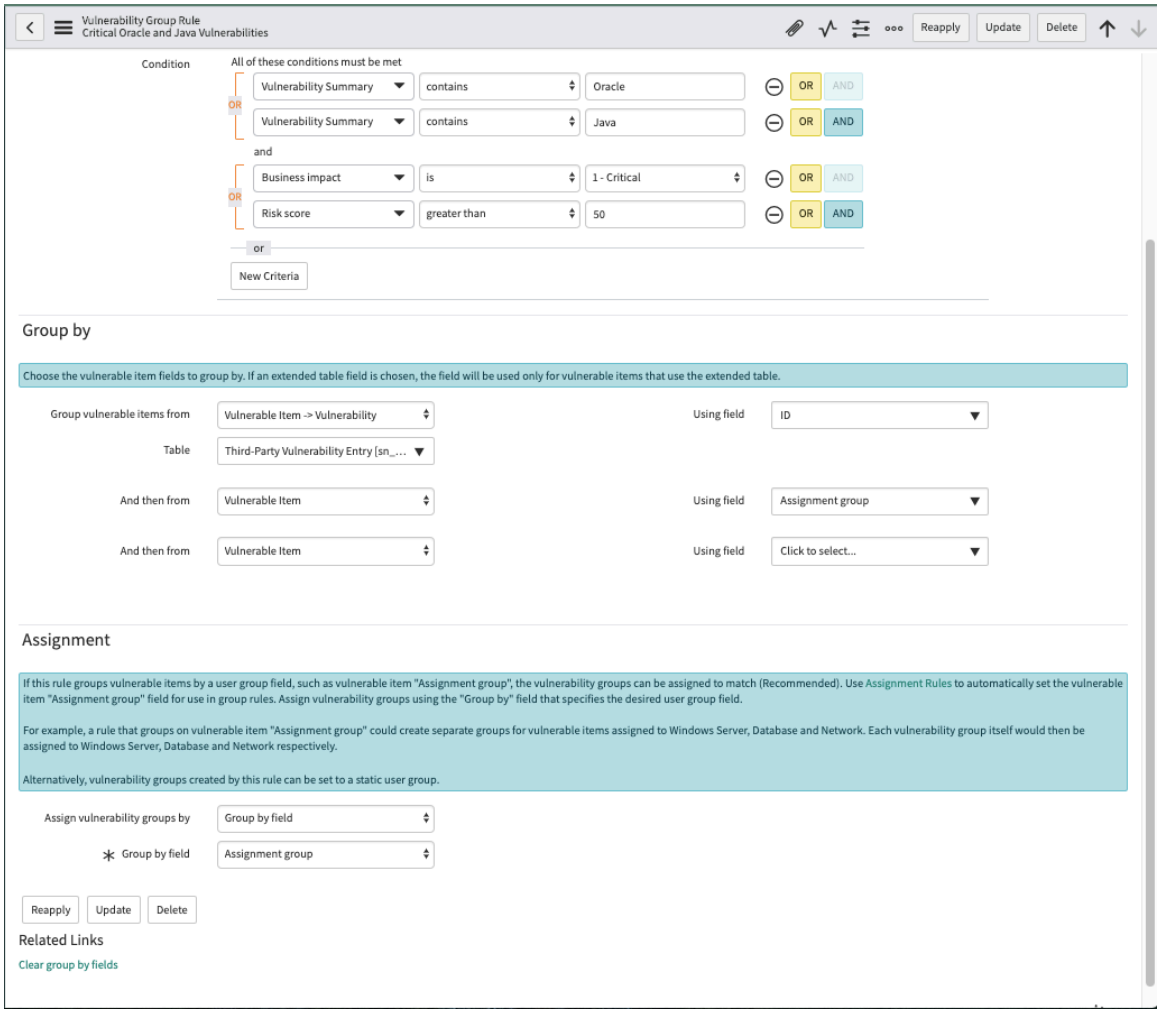
취약성 및 위험 또는 영향 또는 CI(구성 항목)를 사용하는 정정 작업 규칙의 예입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

고위험 **Java** 및 **Oracle** 취약한 항목을 그룹화하기 위한 정정 작업 규칙

이 예에서는 Java 및 Oracle 취약한 항목을 취약성별로 그룹화하고 해당 지원 그룹에 할당하는 규칙의 워크스루를 보여줍니다.

정정 작업 규칙 예시

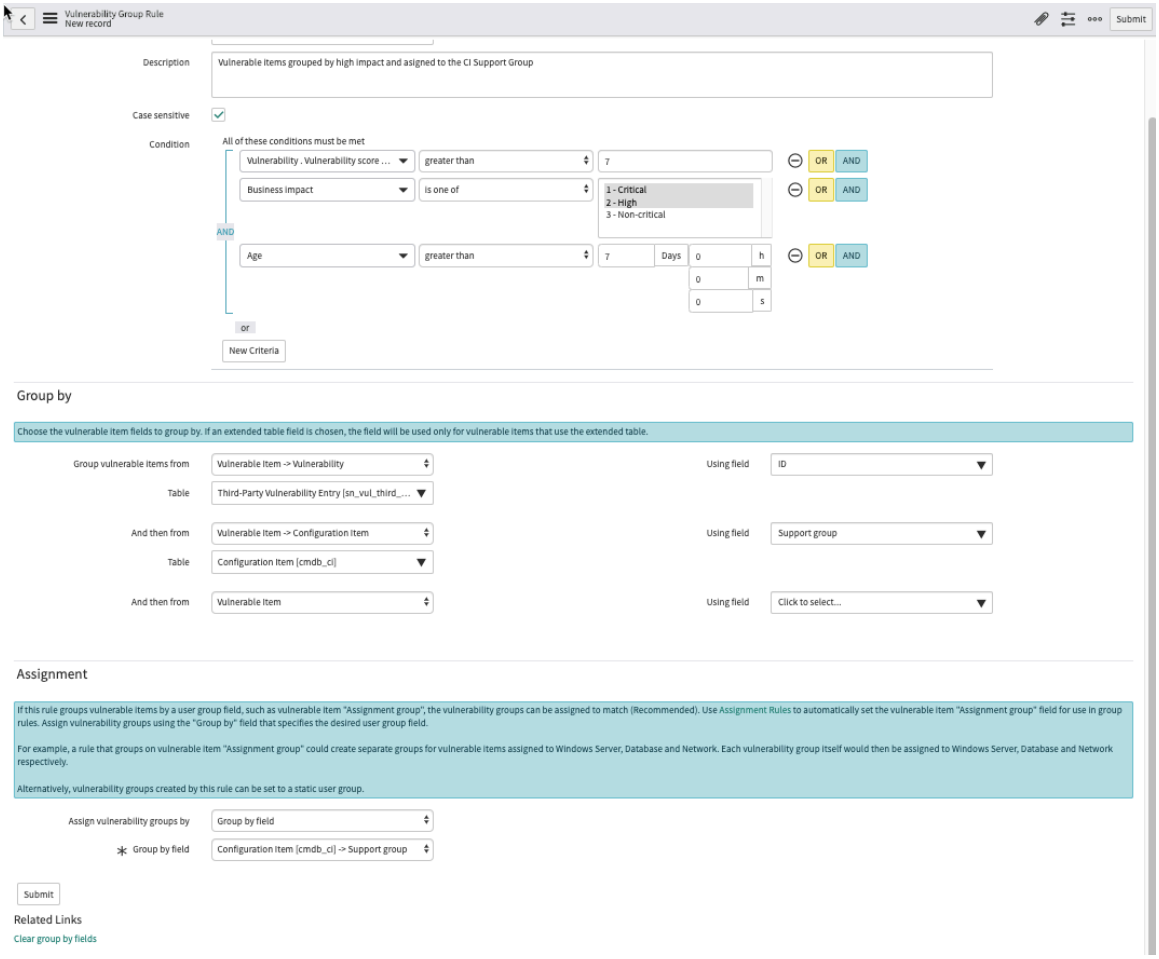


저장하려면 헤더를 마우스 오른쪽 버튼으로 클릭합니다.

영향도가 높은 모든 취약한 항목을 취약성 및 **CI** 지원 그룹별로 그룹화하는 정정 작업 규칙

이 예에서는 CI 지원 그룹에 할당되는 영향도가 높은 취약한 항목의 그룹 규칙에 대한 양식 필드 설정을 보여줍니다.

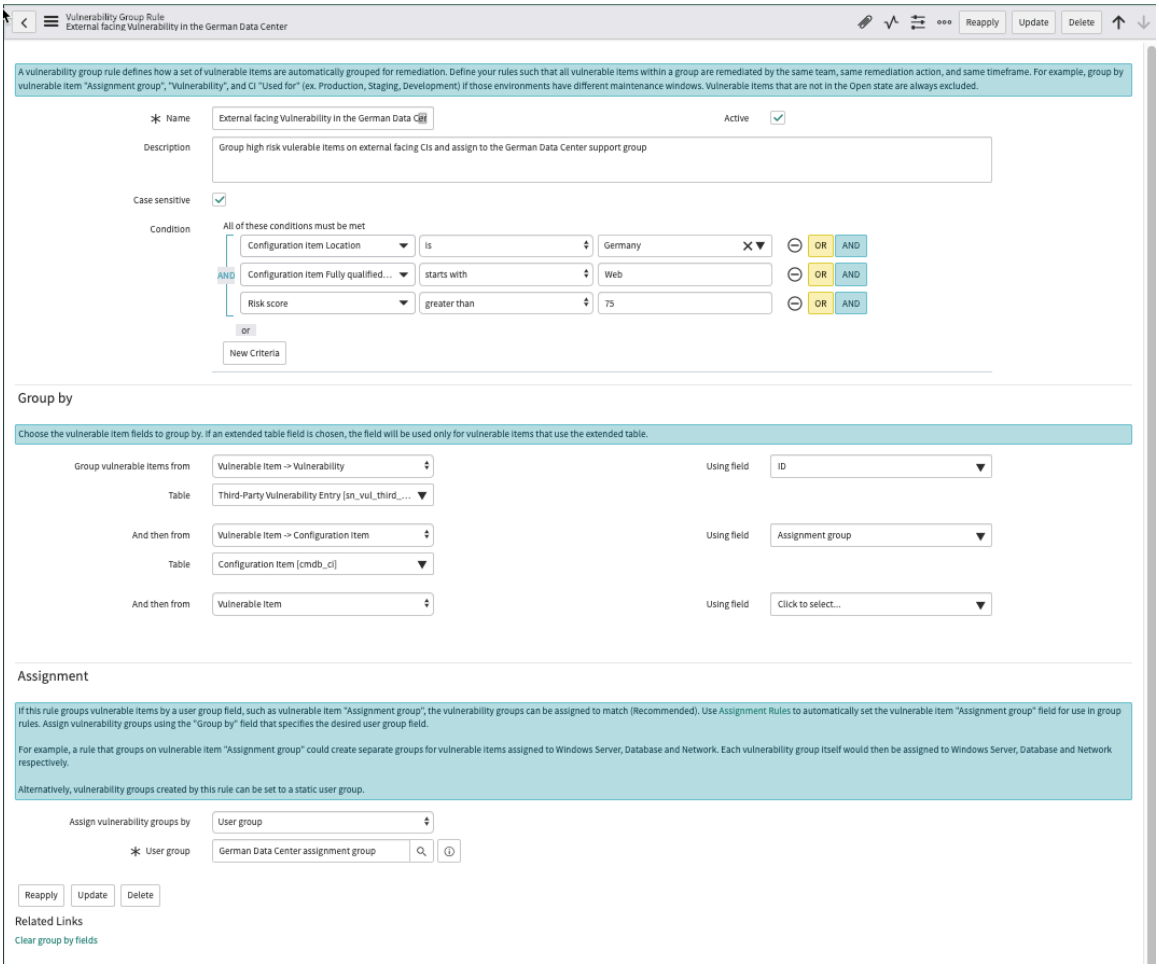
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



독일 데이터 센터의 외부 연결 CI에 대한 모든 고위험 취약성을 그룹화하는 정정 작업 규칙

이 예는 독일 데이터 센터의 외부 연결 CI에 대한 고위험 취약성의 그룹 규칙에 대한 양식 필드 설정을 보여줍니다. 독일 데이터 센터 할당 그룹에 할당됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



에 대한 위험 점수 계산 예 취약성 대응

위험 점수 계산기를 결정하여 조직 고유의 취약성 및 자산 데이터를 사용하는 위험 점수를 생성할 수 있습니다.

위험 규칙 계산기 점수 결정의 예

다음 예는 위험 규칙 계산기의 점수가 결정되는 방법을 보여줍니다.

위험 규칙 계산기가 다음 테이블의 필드로 구성되어 있다고 가정합니다.

필드	가중치	가중치 세부 항목
취약성.심각도	50	기본값: 20 1 - 매우 중요: 100 2 - 높음: 80 3 - 보통: 60 4 - 낮음: 40 5 - 없음: 20
취약성.악용 존재	50	기본값: 50

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	가중치	가중치 세부 항목
		예: 100 아니요: 0

또한 다음 표에 표시된 취약한 항목이 시스템에 있다고 가정합니다.

ID	취약성 심각도	취약성 익스플로잇 존재
VIT00001	1 - 위험	1 - 예
VIT00002	2 - 높음	1 - 예
VIT00003	3 - 보통	2 - 아니요
VIT00004	4 - 낮음	2 - 아니요
VIT00005	5 - 없음	2 - 아니요

취약한 항목에 대한 위험 점수 계산은 다음 수식에 따라 계산됩니다.

`## ## = (W(###) * FV(###). + W(##### ##) * FV(##### ##)) / 100`

여기서 **W** 는 가중치이고 **FV** 는 필드 값의 가중치 백분율입니다.

이러한 취약한 항목에 대한 결과 위험 점수는 다음 표에 설명되어 있습니다.

ID	취약성 심각도**(50%)**	취약성 악용 존재**(50%)**	결과 위험 점수
VIT00001	1 – 중요(50% x 100)	1 – 예(50% x 100)	100
VIT00002	2 – 높음(50% x 80)	1 – 예(50% x 100)	90
VIT00003	3 – 중간(50% x 60)	2 – 아니요(50% x 0)	30
VIT00004	4 – 낮음(50% x 40)	2 – 아니요(50% x 0)	20
VIT00005	5 - 없음(50% x 20)	2 – 아니요(50% x 0)	10

주:
VIT00005의 경우 심각도 값이 비어 있기 때문에 기본 가중치가 적용됩니다.

필드 값 중 하나에 대해 가중치 백분율이 변경된 경우 결과는 다음 표를 참조하십시오.

필드	가중치	가중치 세부 항목
취약성.심각도	50	• 기본값: 20 • 1 - 매우 중요: 100 • **2 -** 높음: **70** *수정된 값 • 3 - 보통: 60 • 4 - 낮음: 40

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	가중치	가중치 세부 항목
취약성.악용 존재	50	• 기본값: 50 • 예: 100 • 아니요: 0

계산기를 다시 적용한 후 취약한 항목에 대한 위험 점수가 다음 테이블에 표시됩니다.

ID	취약성 심각도(50%)	취약성 악용 존재(50%)	결과 위험 점수
VIT00001	1 – 중요(50% x 100)	1 – 예(50% x 100)	100
VIT00002	**2 – 높음(50% x 70)** *수정된 값	1 – 예(50% x 100)	**85** *수정된 값
VIT00003	3 – 중간(50% x 60)	2 – 아니요(50% x 0)	30
VIT00004	4 – 낮음(50% x 40)	2 – 아니요(50% x 0)	20
VIT00005	5 - 없음(50% x 20)	2 – 아니요(50% x 0)	10

탐지를 위한 오류 처리

첨부 파일을 처리하는 동안 탐지를 생성하거나 취약한 항목을 생성 및 업데이트하는 동안 오류가 기록됩니다. 취약성 통합 프로세스가 실패하면 '취약성 통합 로그' 탭에 오류가 기록됩니다.

이러한 오류는 다음 범주 중 하나로 기록됩니다.

필드	설명
VI 생성	탐지를 생성하거나 업데이트하는 동안 오류가 발생했습니다.
탐지	탐지를 생성하는 동안 오류가 발생했습니다.

취약성 대응용 모바일 환경

정정 소유자는 Android 또는 iOS 모바일 장치로 ServiceNow AI Platform# 인스턴스의 취약성 대응(VR) 애플리케이션에 액세스할 수 있습니다.

스토어에서 앱 요청

ServiceNow Store 웹 사이트를 방문하면 사용 가능한 모든 앱을 확인하고 스토어에 요청을 제출하는 방법에 대한 정보를 참조할 수 있습니다. 출시된 모든 앱의 누적 릴리스 정보는 ServiceNow Store 버전 기록 릴리스 정보를 참조하십시오.

취약성 대응

취약성 대응의 개념과 이 제품이 조직에 어떻게 도움이 될 수 있는지 숙지하려면 취약성 대응 이해를 참조하십시오.

주:
모바일을 Vulnerability Response Mobile 앱 설치하기 전에 다음 사항을 숙지하십시오. 모바일 에이전트.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

개요

정정 소유자 역할(sn_vul.remediation_ownerVulnerability Response Mobile 앱)을 가진 사용자는 사용자 Android 또는 iOS 모바일 장치에서 직접 인스턴스의 취약성, 정정 작업 및 할당을 보고 검색할 수 ServiceNow AI Platform 있습니다.

정정 작업(RT) 또는 VI가 사용자 또는 할당 그룹에 할당되면 알림을 받습니다. 이 앱은 정정 소유자가 데스크톱에 연결되지 않고 유연하게 필드를 재할당, 편집하고 정정을 시작할 수 있도록 합니다.

취약성, 취약성 항목, 모듈 및 모든 솔루션에 액세스할 수 있습니다. 모바일 장치에서 다음 작업을 수행할 수 있습니다.

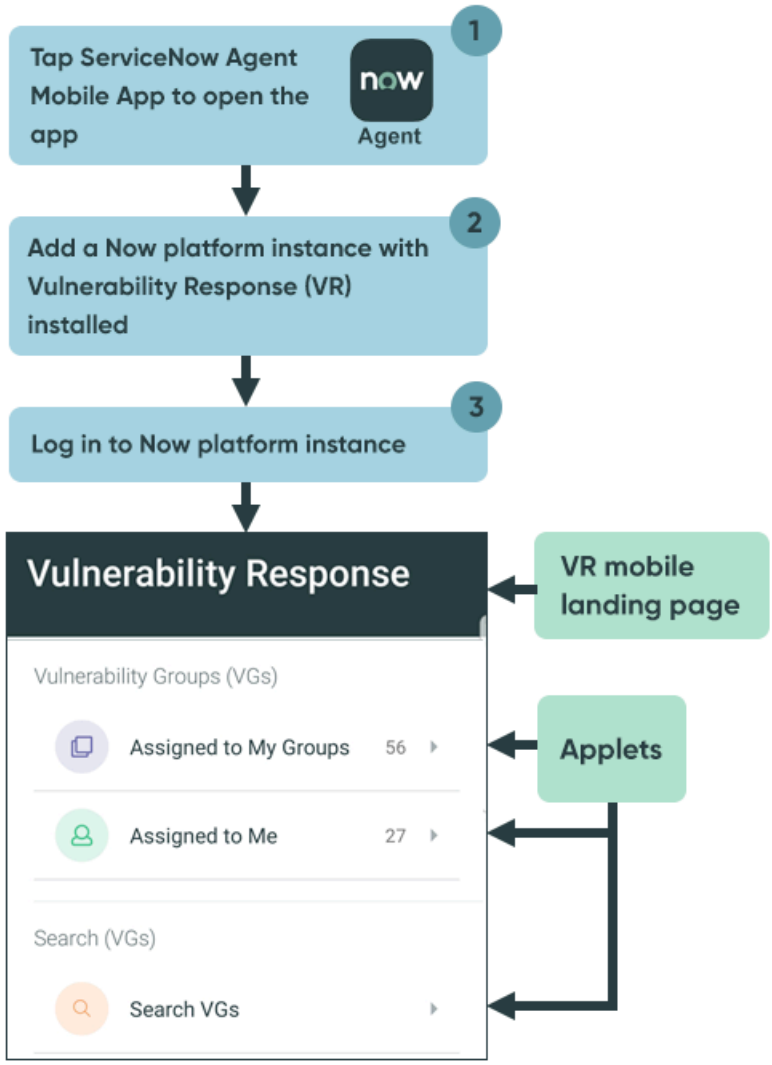
- 정정 작업을 보고 업데이트합니다.
- 변경 요청을 봅니다.
- 정정 작업 또는 취약성 항목을 할당 그룹의 다른 구성원에게 재할당합니다.
- 중요 정정 작업이 사용자 또는 할당 그룹 중 하나에 할당될 때 알림을 봅니다.
- 정정 작업 기록에서 필드의 하위 집합을 편집합니다.
- 특정 검색 기준과 일치하는 정정 작업을 검색합니다.

다음 그림은 모바일 장치에서 인스턴스에 로그인하는 ServiceNow AI Platform 방법과 로그인 후 표시되는 방문 화면을 Vulnerability Response Mobile 앱 보여줍니다.

인스턴스를 설정하고 ServiceNow AI Platform 설치하는 Vulnerability Response Mobile 앱방법에 대한 단계별 지침은 문서를 에 대한 검사 목록 설정 Vulnerability Response Mobile 앱참조하십시오. 로그인 방법에 대한 지침은 문서를 참조하십시오 에 로그인 Vulnerability Response Mobile 앱.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Vulnerability Response Mobile 앱



애플리케이션

ServiceNow 애플리케이션은 (SIR), 취약성 대응 (VR), 거버넌스, 리스크 및 컴플라이언스 ()GRC와 같은 보안 인시던트 응답 소프트웨어 구성요소와 인스턴스 내에서 ServiceNow AI Platform 특정 특성 및 기능성을 제공하는 기타 ServiceNow 제품입니다. 인스턴스에 모바일 앱이 ServiceNow AI Platform 있는 핵심 애플리케이션을 설치하면 이러한 애플리케이션이 모바일 장치 하단에 아이콘으로 표시됩니다.

모바일 장치의 취약성 대응 아이콘

폴더

각 ServiceNow# 모바일 애플리케이션에는 범주별로 애플릿을 구분하는 폴더가 있습니다. 위의 이미지에서 정정 작업 및 검색(VG)은 의 Vulnerability Response Mobile 앱폴더입니다.

애플릿

애플릿은 애플리케이션 내의 다른 옵션입니다. 앞의 이미지에서 정정 작업 및 검색(VG) 아래의 아이콘은 에 Vulnerability Response Mobile 앱사용할 수 있는 애플릿입니다.

의 Vulnerability Response Mobile 앱애플릿에 대한 자세한 내용은 다음 항목을 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

에 대한 검사 목록 설정 **Vulnerability Response Mobile** 앱

다음 검사 목록에는 를 Vulnerability Response Mobile 앱사용하기 전에 인스턴스 ServiceNow AI Platform[#] 와 모바일 장치에서 완료해야 하는 설정 작업이 포함되어 있습니다.

시작하기 전에

추가 정보는 오른쪽 열의 각 단계를 따릅니다. 이 작업의 예상 완료 시간: 15-20분.

필요한 역할: admin, sn_vul.remediation_owner

에 Vulnerability Response Mobile 앱대한 모바일 장치를 성공적으로 설정했습니다. 다음 단계는 에 Vulnerability Response Mobile 앱 로그인하여 모바일 장치에 인스턴스를 추가하는 ServiceNow AI Platform 것입니다.

프로시저

1. 옵션으로, 이 검사 목록을 인쇄하고 이를 사용하여 .Vulnerability Response Mobile 앱
2. 인스턴스에 로그인하여 Vulnerability Response Mobile 앱ServiceNow AI Platform 추가할 수 있도록 목록의 각 항목이 완료되었는지 확인합니다.

모바일 검사 목록

항목	설명
☐	관리자 역할이 있는 사용자는 인스턴스에 코어 애플리케이션이 설치되어 ServiceNow AI Platform 있는지 취약성 대응 확인합니다. 모바일 장치에서 보는 인스턴스입니다 ServiceNow AI Platform . **주:** 취약성 대응 핵심 애플리케이션과 ServiceNow AI Platform 인스턴스는 동일한 제품군 릴리스에 속해야 합니다. **a.** 인스턴스에 핵심 애플리케이션이 설치되었는지 확인하려면 플러그인으로 이동하여 을 검색합니다 취약성 대응. **b.** 취약성 대응 코어 애플리케이션이 아직 설치되지 않은 경우 설치를 클릭하여 설치합니다. 핵심 애플리케이션 설치에 취약성 대응 대한 자세한 내용은 다음 문서를 참조하십시오 취약성 대응 설치. 에서 핵심 애플리케이션을 ServiceNow Store얻고, 권리를 얻고, 핵심 애플리케이션을 설치하고, 종속성을 취약성 대응 활성화하는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오보안 운영 그리고 ServiceNow Store.
☐	관리자 역할이 있는 사용자는 모바일 장치에서 보려는 인스턴스에 가 Vulnerability Response Mobile 앱 설치되어 ServiceNow AI Platform 있는지 확인합니다. **주:** 및 Vulnerability Response Mobile 앱ServiceNow AI Platform 인스턴스는 동일한 제품군 릴리스에 속해야 합니다. 및 Vulnerability Response Mobile 앱취약성 대응 응용 프로그램은 호환되어야 합니다. Vulnerability Response 애플리케이션 호환성에 대한 자세한 내용은 Vulnerability Response 및 Configuration Compliance 호환성 매트릭스를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

항목	설명
	에서 ServiceNow Store 다운로드하여 Vulnerability Response Mobile 앱 인스턴스의 ServiceNow AI Platform 에 설치합니다. 를 Vulnerability Response Mobile 앱설치하면 해당 종속성, com.glide.sg 및 com.glide.sg.agent_native_client도 설치됩니다. 이러한 종속성이 설치되어 있는지 확인하려면 다음을 수행합니다. **a.** 다음으로 이동 모두 〉 플러그인. **b.** 플러그인 ID(com.glide.sg 및 com.glide.sg.agent_native_client)를 검색합니다. **c.** 활성화되지 않은 경우 이러한 플러그인을 활성화합니다. 이러한 플러그인은 에 Vulnerability Response Mobile 앱필요합니다. 에서 ServiceNow Store애플리케이션을 얻고, 권리를 얻고, 애플리케이션을 설치하고, 종속성을 Vulnerability Response Mobile 앱 활성화하는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오보안 운영 그리고 ServiceNow Store.
☐	관리자 역할을 ServiceNow AI Platform 가진 사용자는 인스턴스에서 필요한 ServiceNow AI Platform 역할을 가진 모바일 사용자를 할당했는지 확인합니다. **a.** 사용자에게 할당된 역할을 보려면 다음으로 이동합니다. 모두 〉 관리 〉 사용자. **b.** 사용자 이름과 역할 관련 목록을 차례로 선택합니다. 이 사용자에게 할당된 모든 역할이 표시됩니다. **c.** 사용자가 할당되었는지 확인하거나 사용자에게 IT 인프라 라이브러리 역할(itil)을 할당합니다. itil 역할을 가진 사용자는 변경 요청과 정정 작업을 생성, 오픈, 업데이트 및 종결할 수 있습니다. itil 역할을 가진 사용자만 작업을 할당할 수 있습니다. **d.** 사용자가 할당되었는지 확인하거나 정정 소유자 역할(sn_vul.remediation_owner)을 가진 사용자를 할당합니다. sn_vul.remediation_owner 역할을 가진 사용자는 취약성 및 솔루션 기록을 읽을 수 있습니다. itil 역할을 할당하면 이 역할이 자동으로 추가됩니다. **e.** 필요한 할당 그룹을 생성하고 모바일 사용자를 해당 그룹에 할당했는지 확인합니다. 주: 모바일 애플리케이션의 사용자가 많은 경우 그룹에 sn_vul.remediation_owner 역할을 할당할 수도 있습니다. 그룹에 추가하는 각 사용자는 이 역할을 상속합니다. 담당 규칙 및 그룹에 대한 자세한 내용은 문서를 참조하십시오 취약성 대응 할당 규칙 개요. 사용자 및 사용자 및 그룹에 역할 할당에 대한 자세한 내용은 사용자 관리를 참조하십시오.
☐	정정 소유자 역할(sn_vul.remediation_owner)을 가진 사용자는 모바일 장치에 최신 ServiceNow# 에이전트 앱을 다운로드합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

항목	설명
	 최신 에이전트 앱은 Apple iOS App Store와 Play 스토어에서 사용할 수 있습니다 Google .
☐	sn_vul.remediation_owner 역할을 가진 사용자는 모바일 장치와 ServiceNow AI Platform 인스턴스에서 알림을 사용할 수 있는지 확인합니다. 알림은 중요 정정 작업이 사용자 또는 할당 그룹에 할당될 때 알려줍니다. 적시에 정정할 수 있도록 지원하려면, 알림을 활성화한 후 에서 Vulnerability Response Mobile 앱 알림을 클릭하고 기록으로 직접 이동합니다. 모바일 장치에 표시되도록 인스턴스에서 알림을 ServiceNow AI Platform 활성화하려면 다음 단계를 따르십시오. **a.** 인스턴스에 다운로드하여 Vulnerability Response Mobile 앱ServiceNow AI Platform 설치했는지 확인합니다. **b.** 인스턴스의 시스템 설정에 ServiceNow AI Platform 있는 알림에서 **ServiceNow Mobile** 애플리케이션을 활성화했는지 확인합니다. 알림 설정에 대한 자세한 내용은 문서를 참조하십시오 Setting notification preferences in Core UI . ServiceNow AI Platform 알림은 모바일 장치의 메시지 화면에도 표시됩니다. 모바일 장치의 설정에서도 알림이 활성화되어 있는지 확인합니다.

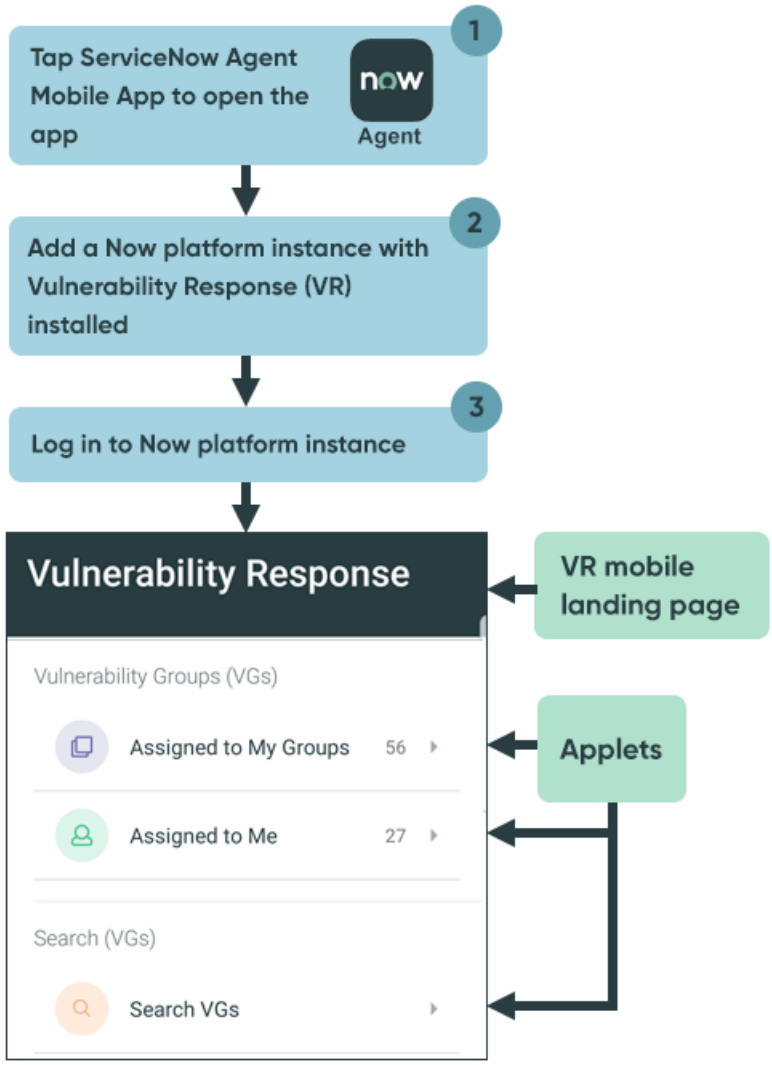
에 로그인 **Vulnerability Response Mobile** 앱

취약성 대응 모바일 앱을 열고 취약성 대응이 ServiceNow AI Platform 포함된 인스턴스를 모바일 장치에 추가하십시오.

시작하기 전에
설명된 에 대한 검사 목록 설정 Vulnerability Response Mobile 앱설정 단계를 완료했는지 확인합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Vulnerability Response Mobile 앱

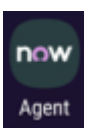


필요한 역할: 정정 소유자(sn_vul.remediation_owner)

이 태스크 정보
작업 완료 시간: 5-7분.

프로시저

1. 모바일 장치에서 **ServiceNow Agent** 앱을 누릅니다.



인스턴스에 아직 로그인 ServiceNow AI Platform 하지 않은 경우 인스턴스 화면이 표시됩니다.

2. ServiceNow AI Platform 코어 애플리케이션이 있는 취약성 대응 인스턴스가 모바일 장치에 아직 추가되지 않은 경우 다음 단계에 따라 추가합니다.

a. 표시되는 인스턴스(Instances) 화면에서 더하기 아이콘( )을 누릅니다.
인스턴스의 주소를 ServiceNow AI Platform 입력하고 저장하라는 메시지가 표시되는 화면이 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

b. 필드에 내용을 입력합니다.

필드 이름	설명
인스턴스 주소를 입력하거나 QR 코드를 스캔합니다.	계속하려면 하나를 선택합니다. ▪ .service-now.com 앞에 인스턴스의 이름ServiceNow AI Platform(예: vrmobilenewyorkagent)을 입력합니다. ▪ 주소를 입력합니다. 이 주소는 모바일 장치에서 보려는 인스턴스의 URL ServiceNow AI Platform 입니다. ▪ QR 코드를 스캔합니다.
(선택 사항) 별칭 입력	이 인스턴스의 별칭을 입력합니다. 장치에 여러 인스턴스가 추가된 경우 별칭을 사용하면 인스턴스를 빠르게 찾을 수 있습니다 ServiceNow AI Platform .

c. 저장 및 로그인을 누릅니다.

3. ServiceNow 표시되는 로그인 화면에서 추가할 인스턴스의 사용자 이름과 암호를 ServiceNow AI Platform 입력하고 로그인을 누릅니다.
Vulnerability Response 방문 화면이 표시됩니다. 에 Vulnerability Response Mobile 앱 성공적으로 로그인했습니다!

4. 로그인한 후 에서 Vulnerability Response Mobile 앱알림이 활성화되었는지 확인합니다.

a. 하단의 방문 화면에서 알림을 탭합니다.

b. 알림 화면에서 활성화되지 않은 경우 알림 활성화 를 누릅니다.
의 ServiceNow AI Platform 알림은 의 Vulnerability Response Mobile 앱알림 화면에 표시됩니다.

5. 모바일 장치의 인스턴스에 로그인하면 이 인스턴스가 장치의 기본 ServiceNow AI Platform 인스턴스가 됩니다.
장치에서 다른 ServiceNow AI Platform 항목을 보려면 기본 인스턴스에서 로그아웃해야 합니다. 로그아웃하려면 다음을 수행합니다.

a. 설정 아이콘을 누릅니다.

b. 로그아웃을 누릅니다.
인스턴스 화면은 모바일 장치에 추가한 모든 ServiceNow AI Platform 인스턴스와 함께 표시됩니다.

c. 옵션: 다른 인스턴스를 눌러 로그인하거나, 이전 단계에 따라 다른 인스턴스를 추가합니다.

결과
장치에서 **ServiceNow** 에이전트 앱을 탭한 후 에 대한 Vulnerability Response Mobile 앱 인스턴스 화면이 표시되지 않으면 장치에서 **ServiceNow** 에이전트가 신뢰할 수 있는 앱으로 허용되는지 확인하십시오. 신뢰할 수 있는 앱으로 액세스를 허용하려면 장치의 설정 및 일반 장치 관리로 이동하고 옵션(Trust 앱 등)을 탭하여 액세스를 허용합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

로그인 화면에 자격 증명을 입력한 후에 오류 메시지가 표시되면 인스턴스의 사용자 이름과 암호가 ServiceNow AI Platform 올바른지 확인하십시오.

방문 화면을 보는 데 문제가 있는 경우 네트워크 연결을 확인합니다.

ServiceNow 에이전트 앱을 탭한 후 인스턴스 화면을 볼 수 없으면 장치에서 앱을 제거해 보십시오. Apple iOS App Store 또는 Google Play 스토어에서 최신 버전의 앱이 있는지 확인하고 다시 설치해 보십시오.

를 사용하여 정정 작업 보기, 할당 및 편집 **Vulnerability Response Mobile** 앱

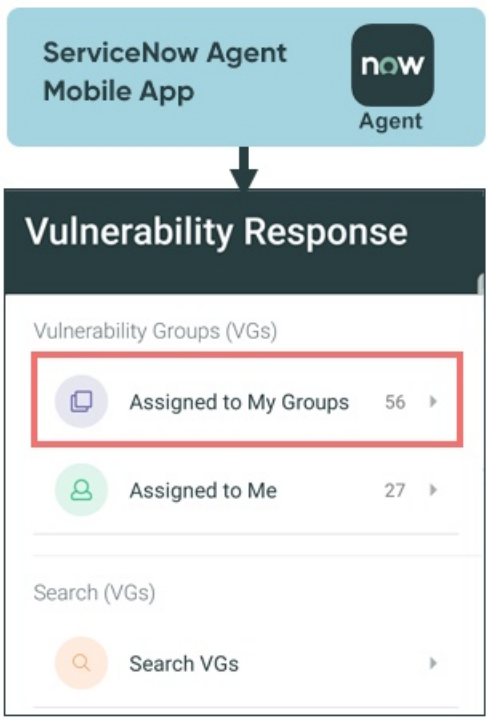
그룹에 할당된 정정 작업(RT) 기록의 필드를 보거나 할당하거나 편집합니다. 취약성, 취약성 항목, 솔루션 기록과 관련 목록을 탐색하여 솔루션, 배포 메트릭, 해결할 항목을 봅니다.

시작하기 전에
필요한 역할: 정정 소유자(sn_vul.remediation_owner)

이 태스크 정보
RT(VUL) 기록을 자신에게 할당하거나 그룹의 다른 구성원에게 다시 할당합니다. 또는 편집, 할당 또는 정정 전에 활성 정정 작업 기록, VI(취약한 항목), NVD 취약성 및 솔루션에 대한 상세 정보를 봅니다. 이 작업 완료 시간: 5-10분.

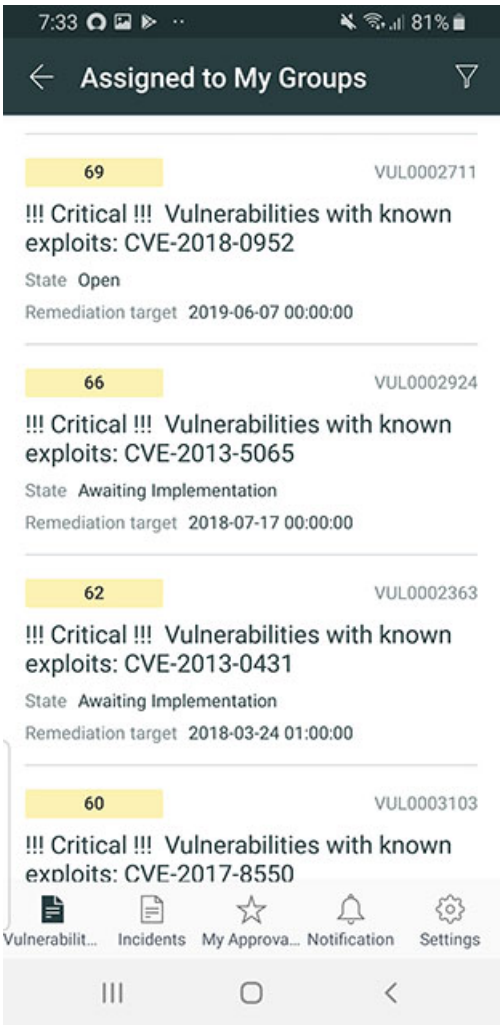
프로시저

1. 모바일 장치에서 인스턴스에 로그인 ServiceNow AI Platform 하지 않은 경우, 자세한 내용은 문서를 에 로그인 Vulnerability Response Mobile 앱참조하십시오.
2. Vulnerability Response 방문 화면이 표시되면 내 그룹에 할당됨을 누릅니다.
   로그인한 후 다른 Vulnerability Response Mobile 앱 곳으로 이동할 경우 언제든지 Now Agent 앱을 탭하여 마지막으로 표시한 화면으로 돌아갈 수 있습니다.



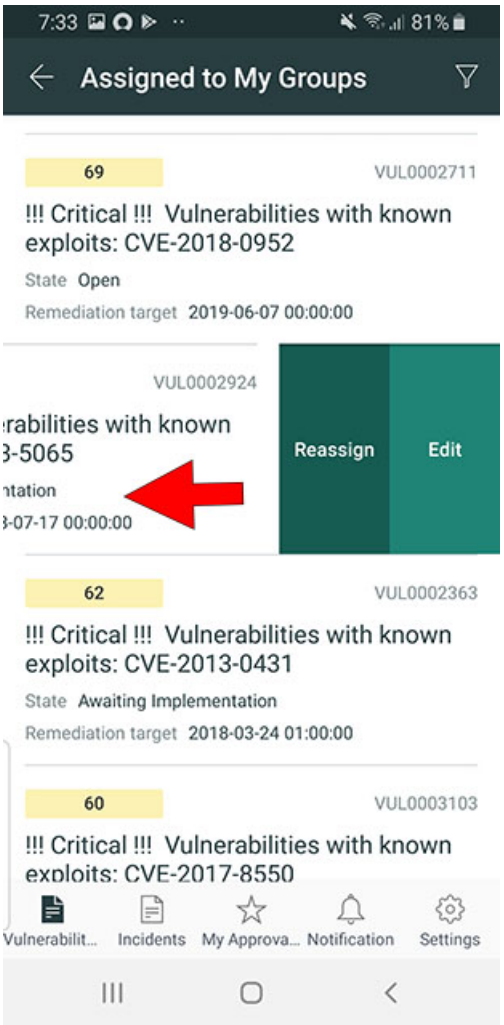
그룹에 할당된 미결 기록 목록이 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



3. 옵션: 를 참조하여 를 사용하여 정정 작업 검색 Vulnerability Response Mobile 앱 특정 기준과 일치하는 기록을 검색합니다.
4. 또는 필터 아이콘( )이 표시되면 필터를 설정하여 목록의 기록 수를 제한합니다 . 모바일 앱의 화면에서 기록을 필터링하는 것은 에서 ServiceNow AI Platform조건 작성기로 필터링하는 것과 비슷합니다.
5. 목록에서 직접 기록을 재할당하거나 편집하려면 열려 있는 기록 목록이 표시된 상태에서 기록을 왼쪽으로 밀어 메뉴를 엽니다.

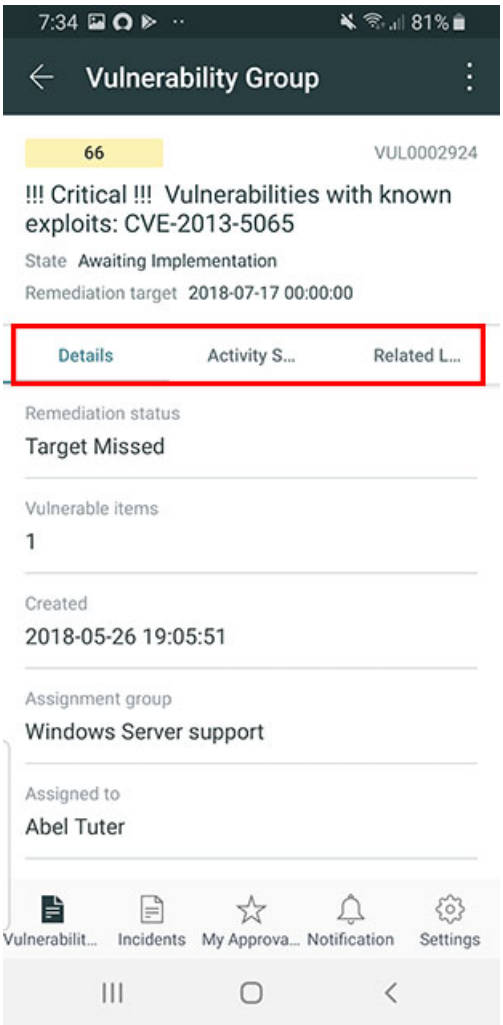
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



6. 표시되는 메뉴에서 하나를 선택하여 계속합니다.

7. 또는 열려 있는 취약성 레코드의 상세 정보를 보고 연결된 레코드 및 관련 목록을 더 많이 보려면 내 그룹에 할당 화면이 표시된 상태에서 목록에서 레코드를 누릅니다.
8. 표시되는 열린 정정 작업 기록에서 다음 표의 옵션 하나를 선택하여 작업 메모 또는 관련 목록을 봅니다.

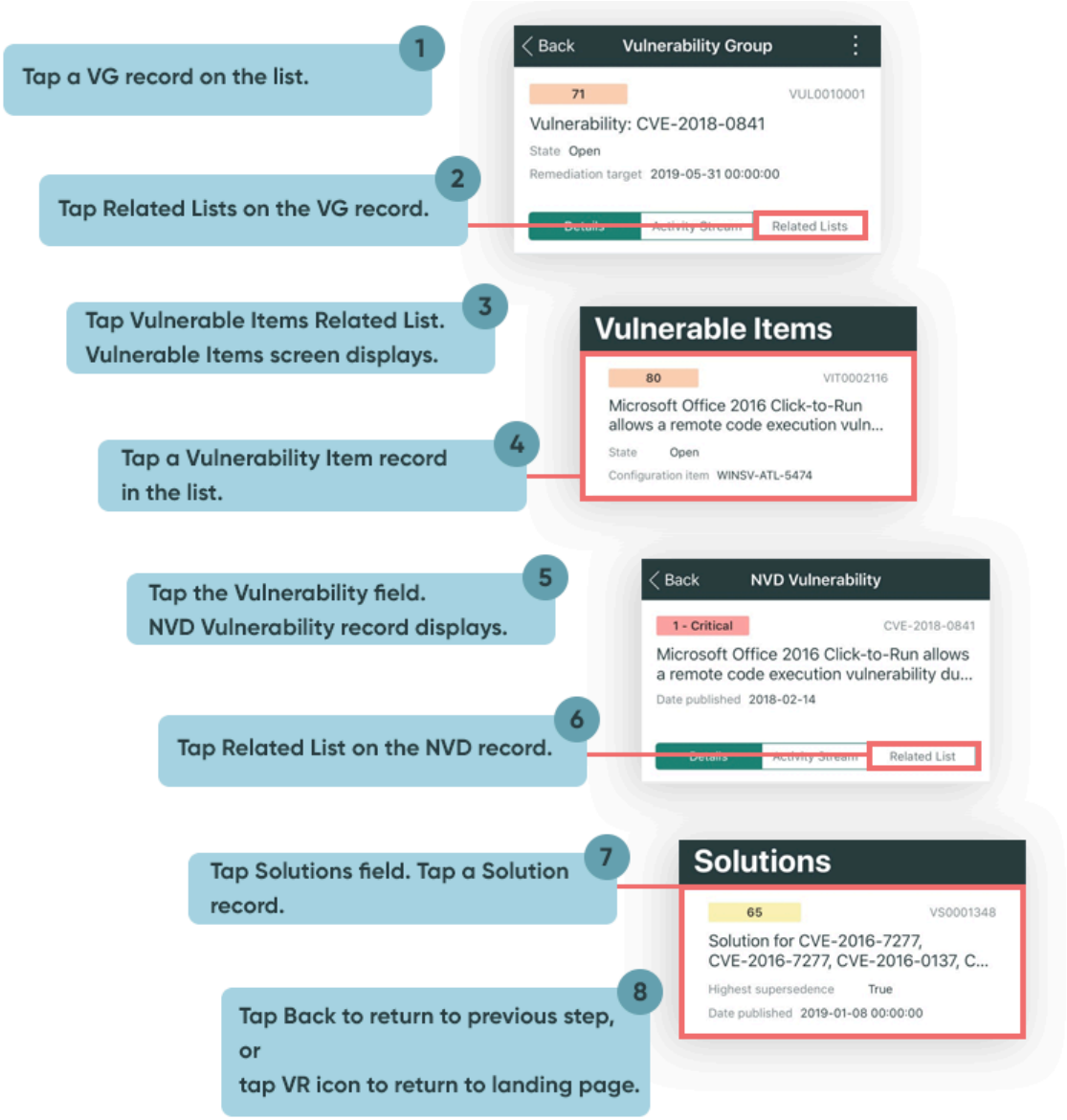
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



다음 이미지는 선택한 취약성에 대한 정정 작업 기록에서 기본 솔루션 기록까지의 탐색 경로를 보여줍니다. 기록과 관련 목록을 탐색하여 솔루션, 배포 메트릭, 해결할 항목을 봅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

정정 작업에서 솔루션 기록을 통한 탐색 경로



9. 검토, 편집 또는 정정한 후 계속하려면 하나를 선택합니다.

를 사용하여 사용자에게 할당된 정정 작업 보기, 재할당 및 편집 **Vulnerability Response Mobile** 앱

나에게 할당된 정정 작업 기록의 필드를 보거나 할당하거나 편집합니다. 기록 및 관련 목록을 탐색하여 솔루션, 배포 메트릭 및 해결할 항목을 봅니다.

시작하기 전에

필요한 역할: 정정 소유자(sn_vul.remediation_owner)

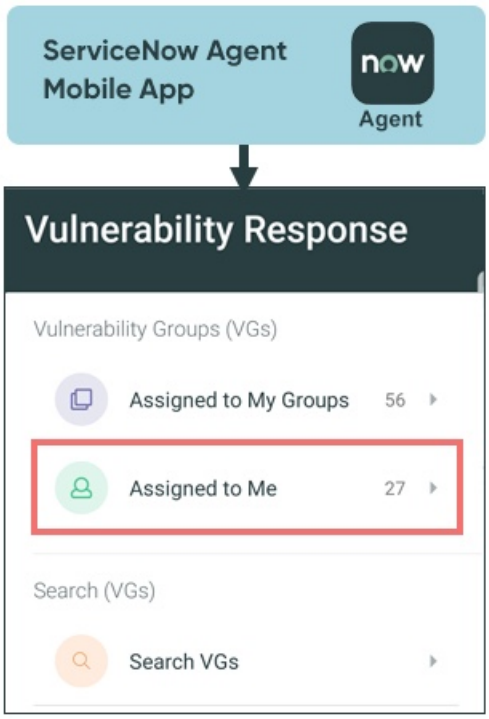
이 태스크 정보

자신에게 할당된 기록을 재할당하거나 편집합니다. 편집, 할당 또는 정정 전에 활성 정정 작업 기록, VI(취약한 항목) 기록, 취약성 및 솔루션의 상세 정보를 봅니다. 이 작업 완료 시간: 5-10분.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

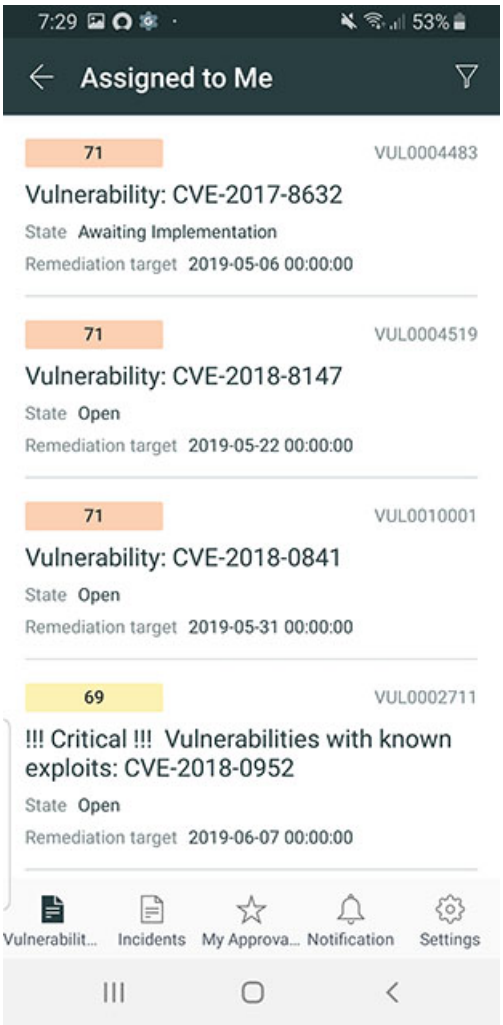
프로시저

1. 모바일 장치에서 인스턴스에 로그인 ServiceNow AI Platform 하지 않은 경우, 자세한 내용은 문서를 에 로그인 Vulnerability Response Mobile 앱참조하십시오.
2. **Vulnerability Response** 방문 화면이 표시되면 '나에게 할당됨'을 누릅니다.
   로그인한 후 다른 Vulnerability Response Mobile 앱 곳으로 이동할 경우 언제든지 Now Agent 앱을 탭하여 마지막으로 표시한 화면으로 돌아갈 수 있습니다.



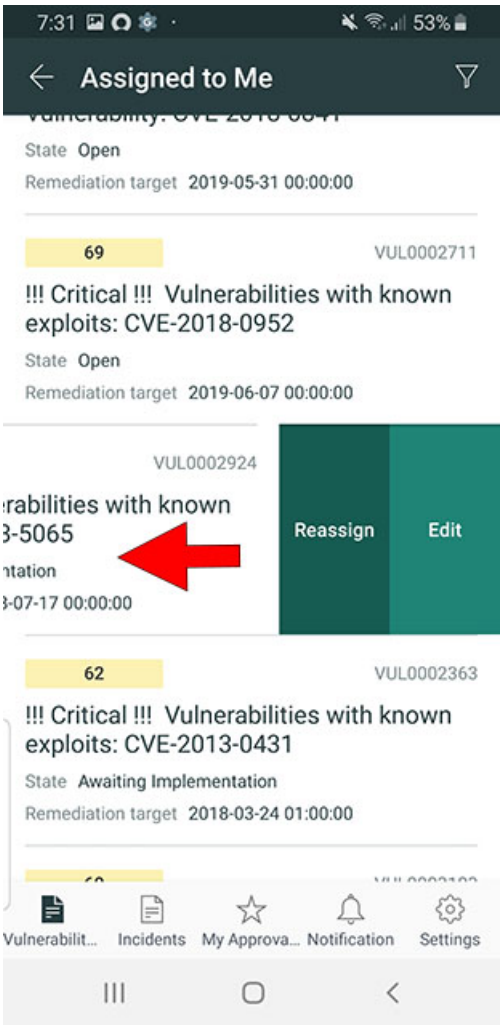
사용자에게 할당된 정정 작업 기록 목록이 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



3. 옵션: 를 참조하여 를 사용하여 정정 작업 검색 Vulnerability Response Mobile 앱 특정 기준과 일치하는 기록을 검색합니다.
4. 또는 필터 아이콘( )이 표시되면 필터를 설정하여 목록의 기록 수를 제한합니다 . 모바일 앱의 화면에서 기록을 필터링하는 것은 에서 ServiceNow AI Platform조건 작성기로 필터링하는 것과 비슷합니다.
5. 목록에서 직접 기록을 재할당하거나 편집하려면 나에게 할당 화면이 표시된 상태에서 기록을 왼쪽으로 살짝 밀어 메뉴를 엽니다.

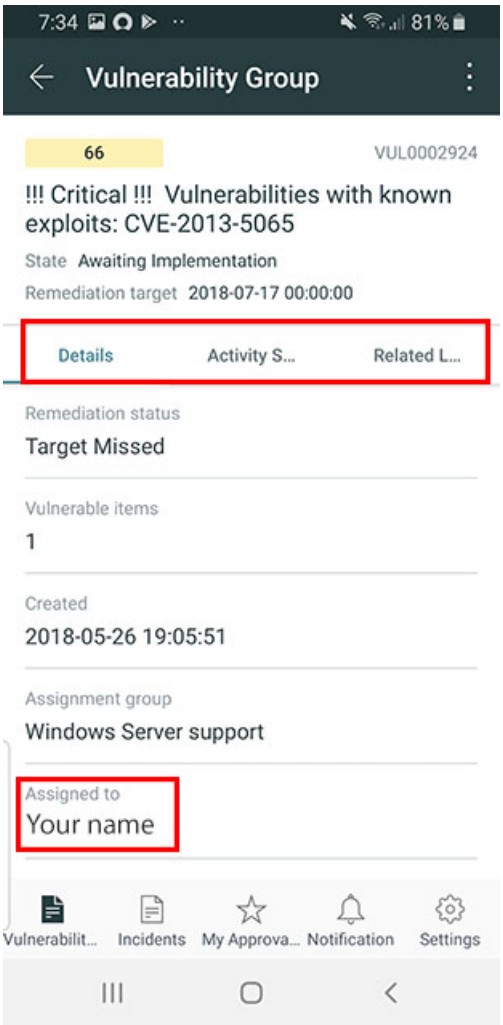
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



6. 계속하려면 하나를 선택합니다.

7. 또는 열려 있는 기록의 상세 정보를 보고 연결된 기록 및 관련 목록을 더 많이 보려면 나에게 할당 화면이 표시된 상태에서 목록에서 기록을 누릅니다.
8. 표시되는 열린 정정 작업 기록에서 다음 표의 옵션 하나를 선택하여 작업 메모 또는 관련 목록을 봅니다.

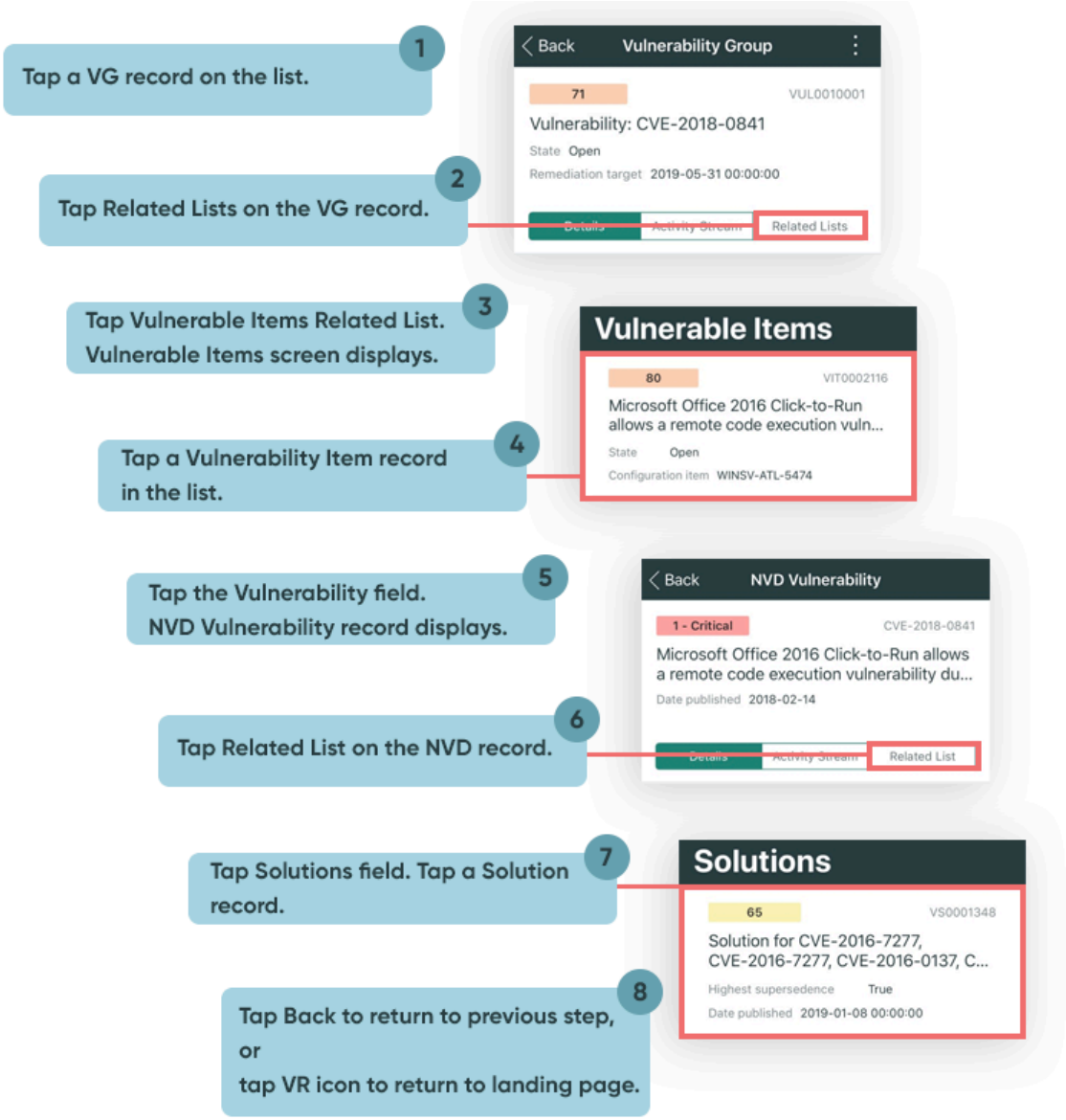
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



다음 이미지는 선택한 취약성에 대한 정정 작업 기록에서 기본 솔루션 기록까지의 탐색 경로를 보여줍니다. 기록과 관련 목록을 탐색하여 솔루션, 배포 메트릭, 해결할 항목을 봅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

RT에서 솔루션 기록을 통한 탐색 경로



9. 계속하려면 하나를 선택합니다.

를 사용하여 정정 작업 검색 **Vulnerability Response Mobile** 앱

선택한 특정 검색 기준과 일치하는 정정 작업을 검색합니다.

시작하기 전에

필요한 역할: 정정 소유자(sn_vul.remediation_owner)

이 태스크 정보

작업 완료 시간: 5-7분.

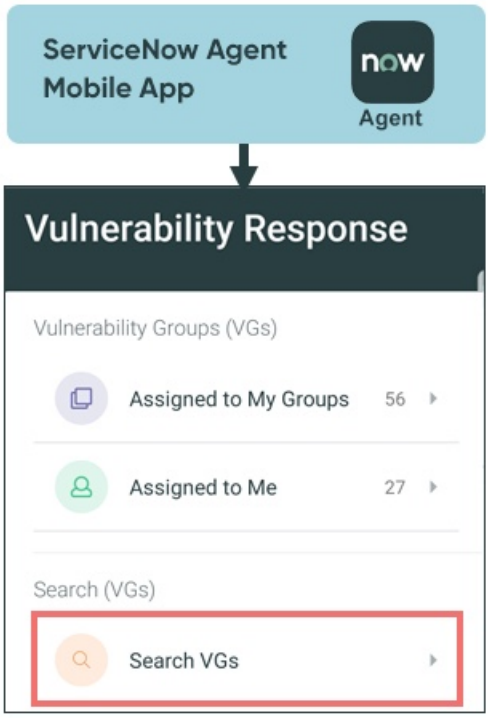
프로시저

1. 모바일 장치에서 인스턴스에 로그인 ServiceNow AI Platform 하지 않은 경우, 자세한 내용은 문서를 에 로그인 Vulnerability Response Mobile 앱참조하십시오.

2. Vulnerability Response 방문 화면이 표시되면 **RT** 검색을 누릅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

로그인한 후 다른 Vulnerability Response Mobile 앱 곳으로 이동할 경우 언제든지 Now Agent 앱을 탭하여 마지막으로 표시한 화면으로 돌아갈 수 있습니다.



3. 표시되는 검색 화면에서 필드를 누르고 원하는 검색 기준으로 양식을 채웁니다.

표 뒤의 지침에 따라 검색 기준을 편집하거나, 검색 기준을 지우거나, 검색을 제출합니다.

이 필드 누르기	장치에 항목을 Android 추가하려면	장치에 항목을 iOS 추가하려면
번호	화면을 탭하고 RT 번호(예: (VUL0002372)를 입력합니다. 이 번호는 RT 레코드의 오른쪽 상단에 표시됩니다. 확인 표시 아이콘을 눌러 항목을 추가하고 RT 검색 화면으로 돌아갑니다. 닫기 아이콘(X)을 눌러 입력을 취소하고 RT 검색 필드로 돌아갑니다.	RT 번호(예: (VUL0002372))를 입력합니다. 이 번호는 RT 레코드의 오른쪽 상단에 표시됩니다. 완료를 눌러 RT 검색 화면으로 돌아갑니다. 확장된 필드에서 취소 를 눌러 항목을 지우고 RT 검색 화면으로 돌아갑니다.
위험 등급	하나 이상의 항목을 누른 다음 확인 표시 아이콘을 눌러 항목을 추가하고 RT 검색 화면으로 돌아갑니다. 닫기 아이콘(X)을 눌러 입력을 취소하고 RT 검색 필드로 돌아갑니다.	항목을 추가하려면 하나 이상의 항목을 탭하거나, 검색 아이콘을 탭하고 검색 필드에 항목을 입력합니다. 완료를 눌러 RT 검색 화면으로 돌아갑니다. 확장된 필드에서 취소 를 눌러 항목을 지우고 RT 검색 화면으로 돌아갑니다.
정정 상태	하나 이상의 항목을 누른 다음 확인 표시 아이콘을 눌러 항목을 추가하고 RT 검색 화면으로 돌아갑니다.	항목을 추가하려면 하나 이상의 항목을 탭하거나, 검색 아이콘을 탭하고 검색 필드에 항목을

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 필드 누르기	장치에 항목을 Android 추가하려면	장치에 항목을 iOS 추가하려면
	닫기 아이콘(X)을 눌러 입력을 취소하고 RT 검색 필드로 돌아갑니다.	입력합니다. 완료를 눌러 RT 검색 화면으로 돌아갑니다. 확장된 필드에서 취소 를 눌러 항목을 지우고 RT 검색 화면으로 돌아갑니다.
상태	하나 이상의 항목을 누른 다음 확인 표시 아이콘을 눌러 항목을 추가하고 RT 검색 화면으로 돌아갑니다. 닫기 아이콘(X)을 눌러 입력을 취소하고 RT 검색 필드로 돌아갑니다.	항목을 추가하려면 하나 이상의 항목을 탭하거나, 검색 아이콘을 탭하고 검색 필드에 항목을 입력합니다. 완료를 눌러 RT 검색 화면으로 돌아갑니다. 확장된 필드에서 취소 를 눌러 항목을 지우고 RT 검색 화면으로 돌아갑니다.
이유	하나 이상의 항목을 누른 다음 확인 표시 아이콘을 눌러 항목을 추가하고 RT 검색 화면으로 돌아갑니다. 닫기 아이콘(X)을 눌러 입력을 취소하고 RT 검색 필드로 돌아갑니다.	항목을 추가하려면 하나 이상의 항목을 탭하거나, 검색 아이콘을 탭하고 검색 필드에 항목을 입력합니다. 완료를 눌러 RT 검색 화면으로 돌아갑니다. 확장된 필드에서 취소 를 눌러 항목을 지우고 RT 검색 화면으로 돌아갑니다.
할당 그룹	목록에서 하나를 선택하거나 검색 아이콘을 누르고 검색 필드에 항목을 입력합니다. 할당 그룹 및 할당 대상 필드의 값을 지우려면 항목 없음에 대해 없음을 선택합니다.	목록에서 하나를 선택하거나 검색 아이콘을 누르고 검색 필드에 항목을 입력합니다. 할당 그룹 및 할당 대상 필드의 값을 지우려면 항목 없음에 대해 없음을 선택합니다.
담당자	목록에서 하나를 선택하거나 검색 아이콘을 누르고 검색 필드에 항목을 입력합니다. 할당 그룹 및 할당 대상 필드의 값을 지우려면 항목 없음에 대해 없음을 선택합니다.	목록에서 하나를 선택하거나 검색 아이콘을 누르고 검색 필드에 항목을 입력합니다. 할당 그룹 및 할당 대상 필드의 값을 지우려면 항목 없음에 대해 없음을 선택합니다.
간단한 설명	화면을 탭하고 텍스트를 입력합니다. 이 기능은 이 필드의 텍스트 문자열과 부분 텍스트 문자열을 인식하지만 와일드카드(*)는 허용되지 않습니다. 대문자는 필요하지 않습니다. 확인 표시 아이콘을 눌러 항목을 추가하고 RT 검색 화면으로 돌아갑니다.	화면에 텍스트를 입력합니다. 이 기능은 이 필드의 텍스트 문자열과 부분 텍스트 문자열을 인식하지만 와일드카드(*)는 허용되지 않습니다. 대문자는 필요하지 않습니다. 완료를 눌러 RT 검색 화면으로 돌아갑니다. 확장된 필드에서 취소 를 눌러 항목을 지우고 RT 검색 화면으로 돌아갑니다.
설명	화면을 탭하고 텍스트를 입력합니다. 이 기능은 이 필드의 텍스트 문자열과	화면에 텍스트를 입력합니다. 이 기능은 이 필드의 텍스트 문자열과

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 필드 누르기	장치에 항목을 Android 추가하려면	장치에 항목을 iOS 추가하려면
	부분 텍스트 문자열을 인식하지만 와일드카드(*)는 허용되지 않습니다. 대문자는 필요하지 않습니다. 확인 표시 아이콘을 눌러 항목을 추가하고 RT 검색 화면으로 돌아갑니다.	부분 텍스트 문자열을 인식하지만 와일드카드(*)는 허용되지 않습니다. 대문자는 필요하지 않습니다. 완료를 눌러 RT 검색 화면으로 돌아갑니다. 확장된 필드에서 취소 를 눌러 항목을 지우고 SearchRT 화면으로 돌아갑니다.

장치의 경우 Android RT 검색 화면이 표시되고 모든 조건을 입력한 상태에서 하나를 선택하여 계속합니다.

4. 장치의 경우 iOS RT 검색 화면이 표시된 상태에서 하나를 선택하여 계속합니다.

5. 옵션: 검색에서 여러 레코드를 반환하는 경우 검색 결과를 세분화할 수 있습니다 를 사용하여 기록 필터링 Vulnerability Response Mobile 앱 .

를 사용하여 기록 필터링 **Vulnerability Response Mobile** 앱

화면에 표시되는 기록 수를 제한하려면 추가 필터를 설정합니다. 모바일 앱에서 기록을 필터링하는 것은 ServiceNow AI Platform에서 조건 작성기로 필터링하는 것과 비슷합니다.

시작하기 전에
필요한 역할: 정정 소유자(sn_vul.remediation_owner)

이 태스크 정보
작업 완료 시간: 5분.

프로시저

1. 검색 결과를 더 구체화하거나 표시되는 레코드 목록에 추가 필터 조건을 입력하려면 필터 아이콘( )을 누릅니다.
2. 필터 화면이 표시되면 필드를 눌러 확장합니다.
   정정 작업 기록에 대한 검색 기준을 입력하는 일반적인 필드는 상태 필드입니다.
3. 표시되는 옵션에서 확인란을 누르거나 필터의 항목을 누릅니다.
   많은 필터가 여러 옵션을 선택할 수 있습니다.
4. 뒤로 아이콘(Back.) 또는 완료 를 눌러 필드에 대한 변경 내용을 저장합니다.
   선택한 기준이 필터 화면에 표시됩니다. 조건과 일치하는 기록 수도 화면 위쪽에 표시됩니다.
   재설정을 눌러 필터를 제거하고 기본 설정을 복원합니다.
5. 옵션: 필터 화면이 표시된 상태로 1-4단계를 반복하여 필터 조건을 계속 설정합니다.
6. 교차로 아이콘(.)을 눌러 AND 조건을 만듭니다.
7. 또는 교차로 아이콘(.)을 눌러 OR 조건을 만듭니다.
8. 원하는 조건을 모두 추가한 후 필터 화면이 표시되면 완료를 누릅니다.
   화면에는 필터 조건과 일치하는 기록만 표시됩니다.

관련 정보

를 사용하여 정정 작업 검색 Vulnerability Response Mobile 앱

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약성 대응 오케스트레이션

워크플로우 및 활동을 사용하면 취약성 대응 오케스트레이션 워크플로우 오케스트레이션을 사용하여 Windows 또는 UNIX 기반 시스템 및 환경에서 데이터를 검색하고 상호작용할 수 있습니다. 데이터를 보강하여 정정 수명주기를 단축할 수 있습니다.

워크플로우 편집 또는 사용자 지정 워크플로우 생성에 대한 자세한 내용은 다음 항목을 참조하십시오 Exploring flows .

취약성 스캔 워크플로우

는 취약성 대응 〉 취약성 검사 워크플로우가 정정 작업을 다시 스캔합니다.

시작하기 전에
필요한 역할: 없음

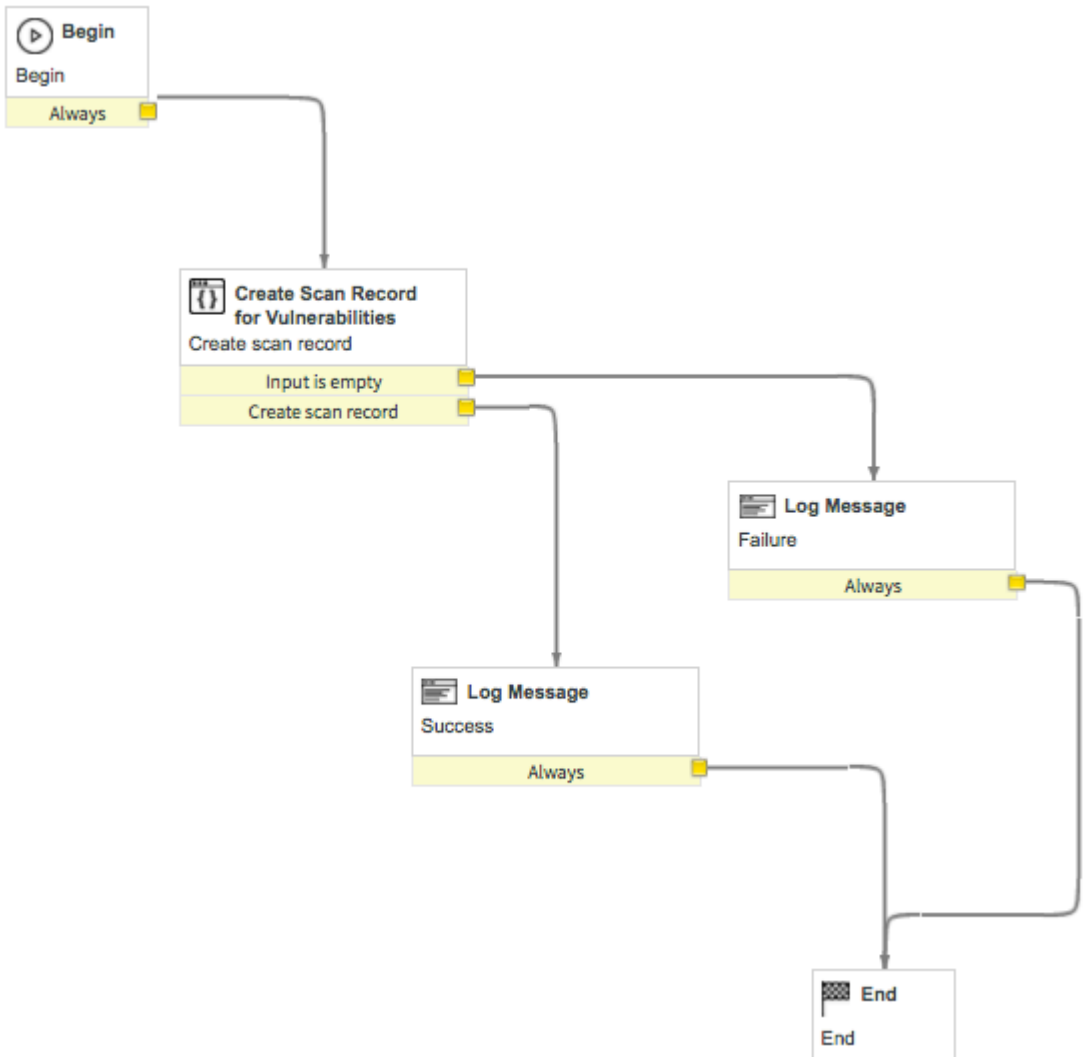
이 태스크 정보
이 워크플로우는 종결/무시 작업 중 취약 그룹 다시 스캔에 의해 트리거됩니다.

워크플로우 프로세스 활동에는 다음이 포함됩니다.

취약성에 대한 검사 기록 생성 활동에 대한 변수

로그 메시지

취약성 스캔 워크플로우



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 정정 작업.
2. 작업 기록(VUL)을 엽니다.
3. 닫기를 클릭합니다.
4. 원하는 상태에 대해 Closed(종결됨)를 선택합니다.
5. 하위 상태에 대해 고정을 선택합니다.
6. "지금 종료하시겠습니까?"에 대해 다음 검색에서 확인 대기를 선택합니다.
   정정 작업 및 취약한 항목의 경우 상태가확인 보류 중으로 변경되고, 하위 상태가수정됨으로 변경되며, 다시 스캔이 실행됩니다.

취약성 항목 검사 워크플로우

는취약한 응답 〉 취약성 항목 검사 워크플로우가 취약한 항목을 다시 스캔합니다.

시작하기 전에
필요한 역할: 없음

이 태스크 정보
이 워크플로우는 종결/무시 작업 중 재스캔 취약성에 의해 트리거됩니다.

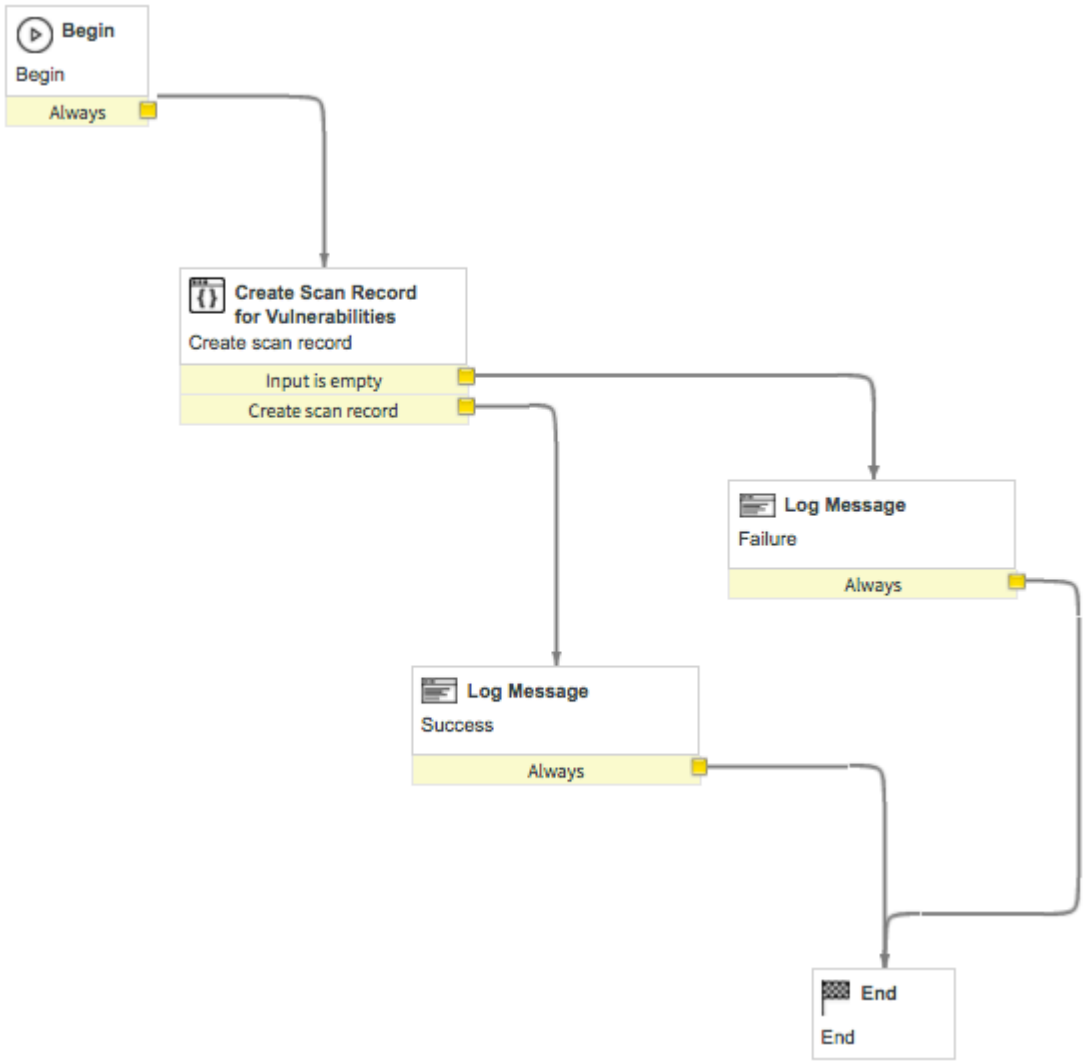
워크플로우 프로세스 활동에는 다음이 포함됩니다.

취약성에 대한 검사 기록 생성 활동에 대한 변수

로그 메시지

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약성 스캔 워크플로우



프로시저

1. 다음으로 이동 취약성 〉 취약성 〉 취약 항목.
2. 취약성 항목을 엽니다.
3. 닫기/무시를 클릭합니다.
4. 원하는 상태에 대해 Closed(종결됨)를 선택합니다.
5. 하위 상태에 대해 고정을 선택합니다.
   그룹의 상태가확인 보류 중으로 변경되고, 하위 상태가고정으로 변경되며, 다시 검색이 실행됩니다.

취약성에 대한 검사 기록 생성 활동에 대한 변수

단일 또는 여러 취약한 항목에 대한 취약성 스캔은 기본 시스템에 포함된 취약성 검사 기록 생성 워크플로우 활동을 사용하여 실행할 수 있습니다. 입력이 활동에 전달되면 스캔 기록이 생성됩니다.

입력 변수

입력 변수는 활동의 초기 동작을 결정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

입력 변수

변수	설명
taskids 〔문자열〕	예상 입력을 정의하는 쉼표로 구분된 sysId의 문자열입니다. 이 필드는 필수입니다.

출력 변수

출력 변수에는 후속 활동에 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
scanResult 〔부울〕	입력이 비어 있지 않으면 True를 반환합니다. taskId에 대한 스캔 기록이 생성됩니다.

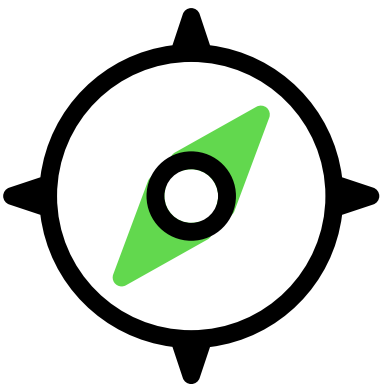
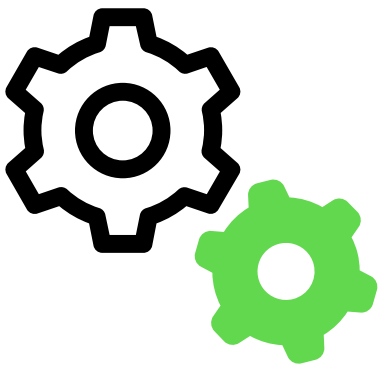
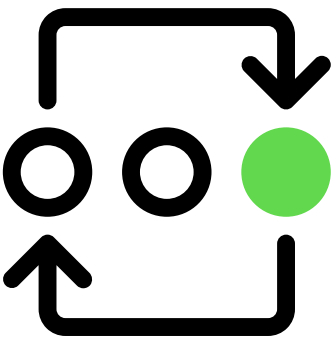
애플리케이션 취약성 대응

애플리케이션 취약성 대응 애플리케이션의 (AVR) 기능은 애플리케이션 취약한 항목(AVIT)을 ServiceNow# 취약성 대응 임포트하고 규칙에 따라 애플리케이션 취약성을 정정할 수 있도록 합니다. 취약성 대응 는 별도의 구독을 통해 사용할 수 있습니다.

AVR v19.0부터 일부 키 테이블 및 열 이름이 업데이트되었습니다. 따라서 설명서에서 이전 이름과 최신 이름 모두에 대한 참조를 볼 수 있습니다. 업데이트된 용어의 전체 목록은 다음 문서를 애플리케이션 취약성 대응 제품 뷰참조하십시오.

의 취약성 대응v19.0부터 SCA(소프트웨어 구성 분석) 및 SBOM(소프트웨어 자재 명세서) 취약성 데이터를 수집하여 소프트웨어 애플리케이션의 약점을 식별할 수 있습니다. 자세한 내용은 애플리케이션 취약성 대응 탐색 및 Veracode Vulnerability Integration 문서를 참조하십시오.

애플리케이션 취약성 대응

탐색	구성	통합
		
Application Vulnerability Response 개념 및 기능에 대해 알아봅니다.	애플리케이션 취약성 대응을 구성합니다.	다른 애플리케이션과 통합하여 Application Vulnerability Response를 확장합니다.

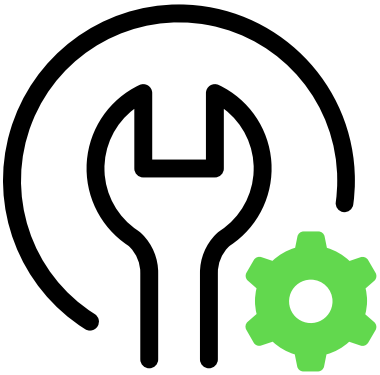
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

애플리케이션 취약성 대응

Vulnerability Response
작업 공간 사용

취약성 관리자, IT 정정 및 취약성 평가 작업 공간에서 AVIT를 모니터링, 관리 및 정정하는 방법에 대해 알아봅니다.

정정

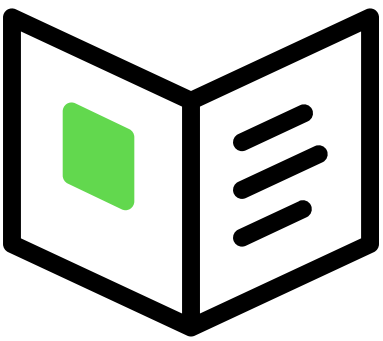


애플리케이션 취약성을 정정하는 방법을 알아봅니다.

분석 및 보고

Application Vulnerability Response 분석 보기

참조



필드, 테이블 및 속성과 같은 애플리케이션 취약성 대응 구성요소에 대한 상세 정보를 얻습니다.

문제 해결 및 도움 받기

- Security Operations 리소스 라이브러리
- Security Operations 커뮤니티
- 알려진 오류 포털에서 알려진 오류 문서 검색
- 연락처 고객 서비스 및 지원

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

애플리케이션 취약성 대응 탐색

애플리케이션 취약성은 애플리케이션의 개발 수명주기 동안 검사되는 사용자 지정 소프트웨어 애플리케이션의 취약성입니다.

개요 애플리케이션 취약성 대응 및 사용 가능한 버전

애플리케이션 취약성 대응 (AVR)은 애플리케이션 취약성을 처리하는 애플리케이션의 일부입니다 취약성 대응 .

사용 가능한 버전

릴리스 버전	릴리스 정보
취약성 대응 v23.0 취약성 대응 v22.0 취약성 대응 v21.0 취약성 대응 v20.0 취약성 대응 v19.0 취약성 대응 v18.2	Application Vulnerability Response release notes 호환성 정보는 KB0856498 Vulnerability Response 호환성 매트릭스 및 릴리스 스키마 변경을 참조하십시오.

작동 원리

취약성 데이터는 CWE(Common Weakness Enumeration) 또는 타사 통합과 같은 내부 및 외부 소스에서 임포트됩니다. 데이터를 임포트한 후에는 사용자의 구성 관리 데이터베이스 (CMDB) 애플리케이션 데이터와 비교되고 애플리케이션에서 처리됩니다 애플리케이션 취약성 대응 . 임포트한 애플리케이션 취약성 데이터와 CMDB의 데이터 간에 일치하는 항목이 있으면 AVIT(애플리케이션 취약한 항목)가 생성됩니다.

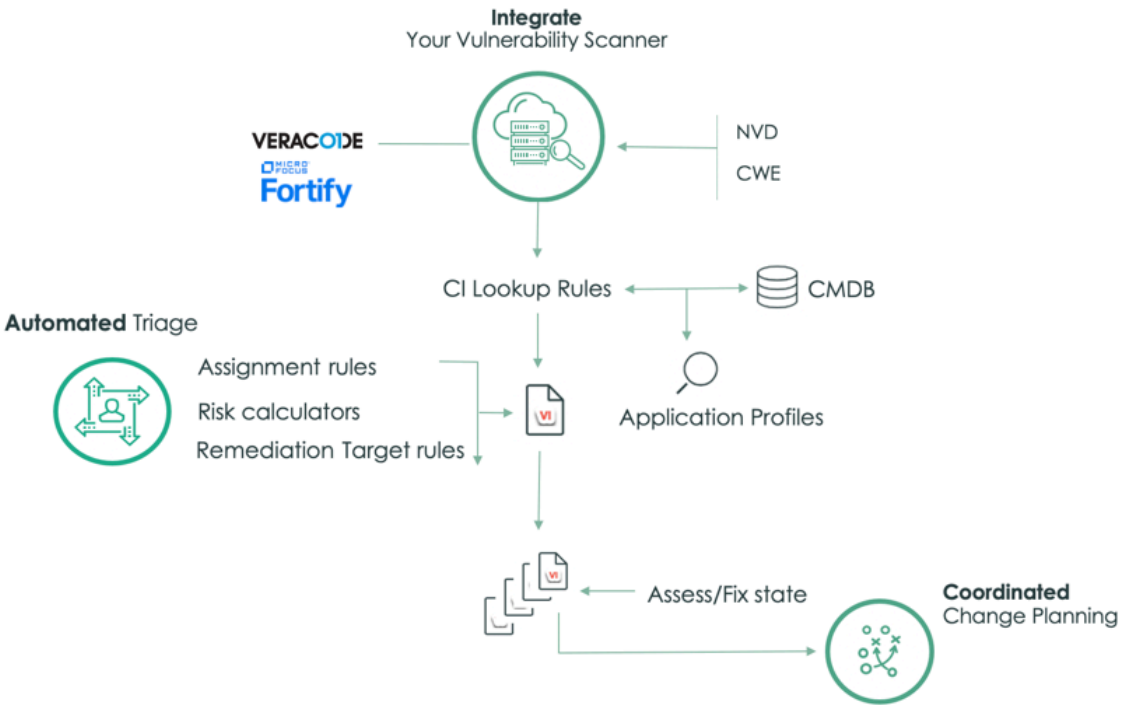
여기에는 애플리케이션 취약성 대응 다음과 같은 주요 기능이 포함됩니다.

- 지원되는 외부 공급업체 스캐너와 통합하여 취약성 데이터를 임포트합니다.
- 애플리케이션 취약성 관련 데이터를 비교하고 애플리케이션에서 애플리케이션 취약성이 발견되었는지 확인합니다.
- 애플리케이션 취약한 항목(AVIT)의 우선순위를 지정하고 정정하며 관리합니다. 각 애플리케이션 취약성은 CWE 또는 외부 공급업체 라이브러리의 취약성 항목을 나타냅니다.
- 의 취약성 대응버전 18.0부터 및 에서 각각 AVIT를 취약성 관리자 작업 공간 모니터링하고 정정할 수 있습니다 IT 정정 작업 공간 . 자세한 내용은 취약성 관리자 작업 공간 및 IT 정정 작업 공간 문서를 참조하십시오.
- 계산기와 라이브러리를 사용하여 데이터의 상관 관계를 지정하면 애플리케이션 취약성 대응 다음 작업을 수행하는 데 도움이 됩니다.
  - **CI** 조회 규칙을 사용하여 애플리케이션 취약한 항목을 자동으로 생성합니다. 임포트하는 동안 타사 취약성이 CWE에 연결되어 AVIT를 생성합니다.
  - 담당 규칙을 생성하여 애플리케이션 취약한 항목 할당을 자동화합니다.
  - 계산기 그룹을 사용하여 비즈니스 영향을 결정하거나, 필터를 사용하여 다양한 조건을 지정하거나, 단순 계산을 적용하거나, 스크립트를 사용할 수 있습니다.
  - 예정된 정정 활동을 모니터링할 수 있도록 애플리케이션 취약한 항목을 정정하기 위한 예상 시간 범위를 정의하는 정정 대상 규칙을 생성합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 단일 외부 공급업체 취약성을 여러 CWE 항목과 연관시키고 취약성의 기본 CWE를 찾아서 위험을 판단하는 데 도움을 줍니다. 기본 **CWE**에 대한 자세한 내용은 다음 문서를 참조하십시오애플리케이션 취약성 필드.
- CWE 데이터베이스에서 다운로드하거나 외부 공급업체 통합에서 임포트한 CWE 기록을 참조용으로 사용하면 취약성을 에스컬레이션해야 하는지 여부를 결정하는 데 도움이 됩니다. 각 CWE 기록에는 약점을 설명하는 관련 지식 문서도 포함되어 있습니다.

통합에서 조사, 그리고 해결에 이르는 정보의 흐름을 따라가는 데 사용합니다 애플리케이션 취약성 대응 .



임포트된 취약성 데이터의 유형

애플리케이션 취약성 대응 는 다음과 같은 유형의 임포트된 애플리케이션 취약성 데이터를 지원합니다.

주:
v19.0 이전에는 SAST, SCA, IAST 및 침투 테스트 데이터가 수집되지 않았으며 에 표시되는 것과 에 FortifyInvicti 표시되는 Veracode애플리케이션 취약성 대응내용 간의 차이를 설명할 수 있습니다.

동적 애플리케이션 보안 테스트(DAST)

DAST 스캔은 애플리케이션에 입력을 보내고 실행 중인 응답을 모니터링하여 취약성 애플리케이션을 찾습니다. 이 접근 방식은 외부 공격을 모방할 수 있습니다. 동적 검사 중에는 실행 중인 서비스(URL)에 취약성이 있는지 검사합니다. 취약성 결과에는 발견된 취약성의 URL 위치가 포함됩니다.

정적 애플리케이션 보안 테스트(SAST)

SAST 스캔은 저장 중인 애플리케이션의 소스 코드를 검토하고 코드를 작성한 방식에서 취약점을 찾는 데 도움이 됩니다. SAST 스캔은 컴파일되지 않은 소스 코드에서 수행되므로 애플리케이션 서비스와 독립적으로 존재합니다. 반환되는 결과에는 발견된 취약성의 파일 및 라인 번호, 위치가 포함됩니다.

인터랙티브 애플리케이션 보안 테스트(IAST)

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

IAST 스캔은 프로그램이 실행되는 동안 프로그램과 상호 작용하여 소프트웨어 취약성을 탐지합니다. 사람의 관찰, 자동화된 테스트 및 센서가 함께 사용되어 애플리케이션과 상호작용하여 취약성을 찾습니다.

소프트웨어 구성 분석(SCA)

의 취약성 대응v19.0부터 SCA(소프트웨어 구성 분석) 취약성을 수집할 수 있습니다. SCA 취약성 데이터는 소프트웨어 애플리케이션에서 사용 중인 오픈 소스 소프트웨어의 약점을 식별하는 데 도움이 됩니다.

침투 테스트

에서 애플리케이션 취약성 대응 침투 테스트 평가 요청을 구성하면 애플리케이션 약점이 있는 위치와 이를 수정하기 위해 수행할 수 있는 작업을 이해하는 데 도움이 됩니다.

소프트웨어 자재 명세서

(SBOM) 데이터를 업로드 소프트웨어 자재 명세서 하여 오픈 소스 구성요소의 취약성을 식별합니다. 자세한 내용은 소프트웨어 자재 명세서 탐색 문서를 참조하십시오.

사용 사례

다음 DAST 사용 사례 중 일부가 지원됩니다.

- 스캔 결과의 각 취약성을 일종의 cmdb_ci(하위 클래스)에 연결합니다.
- 원본 디스커버리 또는 외부 공급업체 통합에 CMDB 기록이 있는 경우 DAST 스캔 결과를 기존 애플리케이션과 연결합니다.
- 새 애플리케이션이 이전에 CMDB에서 식별 및/또는 저장되지 않은 경우 DAST 스캔 결과를 새로 삽입된 스캔한 애플리케이션과 연관시킵니다.
- 가 아닌 ServiceNow#다른 제품에서 애플리케이션을 관리할 때 CMDB에 대한 DAST 스캔 결과를 저장합니다.
- 이전에 다른 용도로 사용자 지정한 경우 CMDB에 대한 DAST 스캔 결과를 저장합니다.
- 소스 코드 리포지토리에 대한 애플리케이션을 수동으로 생성합니다.

지원되는 SAST 사용 사례 중 일부가 지원됩니다.

- 스캔 결과의 각 취약성을 일종의 cmdb_ci(하위 클래스)에 연결합니다.
- 소스 코드 리포지토리에 대한 CI를 수동으로 생성합니다.
- 관련 애플리케이션 서비스가 없는 SAST 스캔 결과를 저장합니다.

[store-future: BEGIN review]다음 IAST 사용 사례 중 일부가 지원됩니다.[End]

[store-future: BEGIN review]지원되는 SCA 사용 중 일부가 지원됩니다.[End]

외부 공급업체 통합

에서 애플리케이션 취약성 대응 지원하는 타사 통합은 에서 별도의 애플리케이션으로 사용할 수 있습니다 ServiceNow Store. 자세한 내용은 다른 애플리케이션과 애플리케이션 취약성 대응의 통합 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주요 기능

- 공유 API는 DAST, SAST, IAST 및 SCA 데이터와 수동 펜 테스트 결과를 가져옵니다. 침투 테스트 문서를 참조하십시오.
- SBOM 데이터를 임포트하는 데 별도의 API가 사용됩니다. 자세한 내용은 소프트웨어 자재 명세서 탐색 및 Veracode Vulnerability Integration 문서를 참조하십시오.

CI 조회 규칙

에서 일치하는 구성 관리 데이터베이스(CMDB)항목에 대한 애플리케이션 데이터를 자동으로 검색합니다.

할당 규칙

사용자 그룹, 사용자 그룹 필드 및 스크립트를 기반으로 애플리케이션 취약성을 자동으로 할당합니다.

위험 계산기

조건 필터를 사용하여 기준에 따라 계산기를 사용하여 AVIT의 영향에 자동으로 우선순위를 지정하고 등급을 지정합니다.

심각도 매핑

애플리케이션 취약한 항목 필드의 초기 값을 자동으로 계산합니다. 취약성 항목에는 소스 심각도와 정규화된 심각도(심각도 매핑 기반)가 모두 있습니다. 심각도는 CWE(일반적인 약점 열거)와 관련이 있습니다.

정정 대상 규칙

애플리케이션 취약한 항목을 정정하기 위한 예상 시간 범위를 정의합니다.

보고

보안 태세, 문제 해결 추세 및 가장 중요한 AVIT를 갖춘 상위 10개 애플리케이션 또는 비즈니스 단위에 대한 인사이트를 빠르게 확보합니다.

두 스캔 유형의 공통점은 애플리케이션 릴리스입니다. **Name** 문자열을 정의하는 애플리케이션 릴리스는 스캐너 측에서 스캔된 취약성 결과를 그룹화하기 위한 연결 지점입니다. 이러한 방식으로 AVR은 통합을 통해 스캔 결과를 임포트할 때 결과가 속한 애플리케이션 릴리스를 알 수 있습니다.

애플리케이션 및 범위에 구성 항목 [cmdb_ci] 하위 테이블인 스캔한 애플리케이션 〔sn_vul_app_scanned_application〕이 취약성 대응 생성되었습니다. 이 테이블은 애플리케이션 릴리스 추상화를 저장하고 CMDB 관계를 통해 서비스 그래프 기능을 제공합니다. 다음에서 볼 수 있습니다. 모두 〉 애플리케이션 취약성 대응 〉 관리 〉 애플리케이션 모듈. 스캔한 애플리케이션의 목록 뷰에는 설치 중에 추가된 부서 및 지원 그룹이 포함되어 있습니다.

애플리케이션 취약 항목**(AVIT)**

애플리케이션 취약성의 경우 AVR은 취약성을 애플리케이션에 연결하여 AVIT(애플리케이션 취약한 항목) 기록을 생성합니다. CMDB 애플리케이션 취약성 대응 에서 애플리케이션을 구성하는 항목에 대한 정의가 여러 가지이므로 애플리케이션을 검사된 애플리케이션으로 제한합니다. 스캔한 애플리케이션은 AVR에 의해 이름 및 **ID**로 식별되는 사용자 환경에서 스캔된 애플리케이션입니다. AVIT는 스캐너에서 수정 이 확인될 때까지 최신 검사 요약을 기반으로 합니다. AVIT를 더 이상 찾을 수 없으면 마지막으로 표시된 검사 요약에 연결된 상태로 유지됩니다.

다음에서 애플리케이션 취약 항목을 볼 수 있습니다. 모두 〉 애플리케이션 취약성 대응 〉 취약성 〉 취약 항목 모듈.

애플리케이션이 CMDB에서 제거되면 연결된 모든 AVIT가 닫힙니다.

AVIT 양식 필드에 대한 자세한 내용은 문서를 참조하십시오 애플리케이션 취약한 항목 필드.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

의 사용자 그룹 및 역할 애플리케이션 취약성 대응

팀이 함께 작업하여 애플리케이션 취약성 관리를 생성, 관리 및 감독하는 경우가 많습니다. 팀 구성원들 중에는 운영 역할뿐만 뿐만 아니라, 전략적 역할도 가집니다. 대부분의 조직에서는 두 가지 이상의 역할에 참여하고 다른 사람과 역할을 공유할 수도 있습니다. 애플리케이션 취약성 대응 은 세분화된 역할을 포함하는 세 개의 사용자 그룹(App-Sec 관리자, 애플리케이션 보안 챔피언 및 개발자)을 사용합니다. 이러한 그룹 및 역할에 대한 자세한 내용은 을 참조하십시오 애플리케이션 취약성 대응 사용자 그룹 및 역할 .

애플리케이션 취약성 대응 상태

애플리케이션 취약성 대응 은 애플리케이션 취약 항목(AVIT)의 상태에 대한 상태 모델을 제공하며 AVIT를 정정하는 시기와 방법을 결정하는 데 도움을 줍니다.

애플리케이션 취약한 항목에는 여러 가지 상태가 있을 수 있습니다. 자세한 내용은 를 참조하십시오 애플리케이션 취약한 항목(AVI) 상태 .

취약성 대응 애플리케이션 및 **CSDM** 테이블

, 취약성 대응애플리케이션 취약성 대응, 타사 취약성 통합 및 소프트웨어 자재 명세서 애플리케이션은 테이블을 관리(데이터 기여) CSDM 합니다. 이러한 애플리케이션은 다른 애플리케이션이 생성하는 테이블의 데이터 CSDM 도 사용합니다. 따라서 여러 ServiceNow 제품이 이러한 보안 운영 애플리케이션의 이점을 누리고 가치를 더합니다. 자세한 내용은 취약성 대응 애플리케이션 및 CSDM 테이블 문서를 참조하십시오.

애플리케이션 취약성 대응 구성

인스턴스에서 실행하기 애플리케이션 취약성 대응ServiceNow AI Platform 전에 먼저 구성해야 합니다.

애플리케이션 취약성 대응 구성

구성이 완료되었는지 확인할 수 있도록 구성 전에 다음 설정 단계를 수행합니다.

시작하기 전에

작업 설정	설명
애플리케이션이 설치되고 활성화되었는지 취약성 대응 확인합니다.	활성화되었는지 확인하려면 구독 관리 〉 구독 인스턴스에 있습니다. 목록에 조직이 구매한 구독이 표시됩니다. 애플리케이션이 설치 및 활성화되지 않은 경우 문서를 참조하십시오 취약성 대응 설치.
보고서를 보려면 애플리케이션 취약성 대응 이(가취약성 대응용 퍼포먼스 분석) 설치되고 활성화되었는지 확인합니다.	활성화되었는지 확인하려면 구독 관리 〉 구독 인스턴스에 있습니다. 목록에 조직이 구매한 구독이 표시됩니다. 애플리케이션이 설치 및 활성화되지 않은 경우 문서를 참조하십시오 〔PA〕 애플리케이션 설치 및 구성 취약성 대응용 퍼포먼스 분석.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업 설정	설명
가 Veracode Vulnerability Integration 설치, 활성화 및 구성되어 있는지 확인합니다. (이 시점에서는 통합을 실행하지 마십시오.)	활성화되었는지 확인하려면 구독 관리 〉 구독 인스턴스에 있습니다. 목록에 조직이 구매한 구독이 표시됩니다. 애플리케이션이 설치 및 활성화되지 않은 경우 문서를 참조하십시오 ServiceNow 와 Vulnerability Response 통합 설치Veracode.
버전 14.0: 가 Fortify 취약성 통합 설치, 활성화 및 구성되어 있는지 확인합니다. (이 시점에서는 통합을 실행하지 마십시오.)	활성화되었는지 확인하려면 구독 관리 〉 구독 인스턴스에 있습니다. 목록에 조직이 구매한 구독이 표시됩니다. 애플리케이션이 설치 및 활성화되지 않은 경우 및 Fortify 취약성 통합 구성를 참조하십시오ServiceNow 와 Vulnerability Response 통합 설치Fortify.
CWE 2000 통합이 에서 실행 취약성 대응중인지 확인합니다.	통합을 확인하려면 다음 문서를 참조하십시오 NVD 기록을 업데이트하기 위한 예약된 작업이 실행 중인지 확인.
〔선택사항〕 NVD 통합이 에서 실행 취약성 대응중인지 확인합니다.	확인하려면 다음 문서를 참조하십시오 CWE 기록 업데이트를 위한 예약된 작업이 실행 중인지 확인.
인스턴스에 필요한 ServiceNow 역할이 있는지 확인합니다.	예상 결과의 설치, 구성 및 검증에 필요한 역할은 다음과 같습니다. • 아직 할당되지 않은 경우 관리자 역할의 사용자가 애플리케이션을 설치하고 사용자를 App-Sec 관리자, 보안 챔피언 및 개발자 사용자 그룹에 할당합니다. 그룹 역할에 대한 자세한 내용은 다음 문서를 참조하십시오 애플리케이션 취약성 대응 사용자 그룹 및 역할. • App-Sec 관리자 그룹은 구성을 감독하고 예상 결과를 검증합니다. 주: 애플리케이션 취약성 대응 의 설정 도우미 기능 취약성 대응에서는 구성을 사용할 수 없습니다.

필요한 역할: App-Sec 관리자 사용자 그룹

프로시저

1. 다음으로 이동 보안 운영 〉 **CMDB** 〉 조회 규칙.
   사용자 환경에 대한 CI 조회 규칙을 작성 또는 수정하려면 을(를) 참조하십시오 CI 조회 규칙 생성 .
2. 다음으로 이동 애플리케이션 취약성 대응 〉 관리.
3. 할당 규칙을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용자 환경에 맞게 애플리케이션 할당 규칙을 생성하거나 수정하려면 을(를) 참조하십시오 담당 규칙 생성 또는 편집 애플리케이션 취약성 대응 .

4. 취약성 계산기를 선택합니다.
   사용자 환경에 맞게 애플리케이션 취약성 계산기를 만들거나 수정하려면 을(를) 참조하십시오 자동으로 위험 애플리케이션 취약성 대응 계산 .
5. 정정 대상 규칙을 선택합니다.
   사용자 환경에 맞게 애플리케이션 정정 대상을 만들거나 수정하려면 을(를) 참조하십시오 애플리케이션 정정 대상 규칙 생성 또는 편집 .
6. 정규화된 심각도 맵을 선택합니다.
   사용자 환경에 대한 심각도 맵 작성 또는 수정을 참조하십시오 애플리케이션 취약한 항목의 심각도를 자동으로 매핑 .
7. 다음 중 하나로 이동합니다. **Veracode Vulnerability Integration** 〉 통합 또는 **Fortify** 취약성 통합 〉 통합.
8. Veracode 애플리케이션 목록 통합 또는 Fortify 요청 시 애플리케이션 목록 통합을 엽니다.
9. 아직 실행되지 않은 경우 지금 실행을 선택합니다.

   주:
   다른 Veracode 또는 Fortify 통합은 기본적으로 비활성 상태입니다.

   통합 실행 상태에 대한 자세한 내용은 또는 Fortify 취약성 통합 임포트 실행 상태 보기을 참조하십시오Veracode 애플리케이션 취약성 통합 임포트 실행 상태 보기.
10. Veracode 또는 Fortify 요청 시 애플리케이션 목록 통합의 실행이 완료되면 애플리케이션 취약성 대응 〉 관리 〉 애플리케이션.
11. 각 애플리케이션에 대해 지원 그룹 (할당 규칙에 사용됨) 및 부서 (보고에 사용됨)에 대한 값을 입력합니다.
    여러 항목을 업데이트하려면 목록 편집기를 사용하여 목록에서 여러 기록을 편집 하여 작업을 대량으로 완료하기를 참고하세요.

    주:
    자동 업데이트된 비즈니스 단위를 보려면 페이지를 새로 고치십시오. 스캔한 애플리케이션 양식 필드에 대한 자세한 내용은 을 참조하십시오 스캔한 애플리케이션 필드.

12. 통합 목록으로 돌아가 다른 Veracode 하나 또는 Fortify 통합을 활성화합니다.
    델타 데이터 통합 임포트를 설정하려면 을(를) 통합 활성화 애플리케이션 취약성 대응 참조하십시오.

    Veracode 및 Fortify 통합은 체인으로 연결되며 활성화되면 연속적으로 실행됩니다.

13. 옵션: 다음으로 이동 애플리케이션 취약성 대응 〉 관리 〉 담당 규칙.

    a. 옵션: 이전에 담당 규칙을 만들거나 편집할 때 구성 항목:사용자 그룹에 대한 지원 그룹 필드를 선택한 경우 검사한 애플리케이션 목록 보기에 추가한 값을 지금 사용할 수 있습니다.
    담당 규칙이 편집됩니다.

    b. 업데이트를 선택합니다.

    c. 취약성 담당 규칙 목록 보기에서 변경 내용 적용을 선택하여 담당 규칙을 AVI에 다시 적용합니다.

결과
애플리케이션 취약성 대응 이제 구성이 완료되었습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 수행할 작업
다음으로 이동 애플리케이션 취약성 대응 〉 개요 전반적인 보안 태세에 대한 자세한 내용은 PA(애플리케이션 취약성 관리) 대시보드를 참조하십시오.

CWE 기록 업데이트를 위한 예약된 작업이 실행 중인지 확인

취약성을 에스컬레이션해야 하는지 여부를 결정할 때 CWE 데이터베이스에서 다운로드한 CWE(일반적인 약점 열거) 기록을 참조용으로 사용합니다. 정기적으로 Common Weakness Enumeration 데이터베이스에서 일반 약점 기록을 업데이트합니다. 기본 스크립트를 업데이트하거나 필요에 따라 스크립트를 직접 작성할 수도 있습니다.

시작하기 전에
필요한 역할: App-Sec 관리자 그룹
각 CWE 기록에는 약점을 설명하는 관련 지식 문서도 포함되어 있습니다.

프로시저

1. 다음으로 이동 모두 〉 애플리케이션 취약성 대응 〉 관리 〉 통합.
2. **CWE Comprehensive 2000 Integration** 예약 작업을 선택합니다.
3. 활성 확인란이 선택되었는지 확인합니다.

   주:
   이 양식의 설정은 및 애플리케이션 취약성 대응에 의해 취약성 대응 공유됩니다. 통합 설정을 수정하려면 및 ServiceNow에 대한 취약성 대응 조정 및 전문 지식이 필요합니다.

4. 상자가 선택되어 있으면 작업이 완료된 것입니다.

   주:
   상자가 선택되어 있지 않으면 에서 이 통합을 구성해야 취약성 대응할 수 있습니다. 선택하기 전에 자세한 내용을 참조하십시오 NVD 및 CWE 통합을 통해 데이터를 임포트하고 외부 공급업체 라이브러리를 관리합니다 .

필요한 경우 임포트한 항목을 보려면 을 참조하십시오 취약성 라이브러리 보기 .

기본 **CWE** 필드에는 CWE 항목이 포함되어 있습니다. 취약성과 관련된 CWE가 두 개 이상 있는 경우 에서 기본 CWE가 결정되는 방식에 대한 자세한 내용을 참조하십시오 애플리케이션 취약성 필드 .

NVD 기록을 업데이트하기 위한 예약된 작업이 실행 중인지 확인

정기적으로 업데이트할 리포지토리를 식별합니다. 예약된 작업을 실행하여 NVD(국가 취약성 데이터베이스) 레코드를 야간 또는 매주 업데이트할 수 있습니다. 아직 실행 중이 아닌 경우 작업을 사용하도록 설정할 수 있습니다

시작하기 전에
필요한 역할: App-Sec 관리자 그룹

NVD 통합은 기본적으로 월요일 00:00:00에 예약된 작업으로 실행됩니다.

프로시저

1. 다음으로 이동 모두 〉 애플리케이션 취약성 대응 〉 관리 〉 통합.
2. **NIST** 국가 취약성 데이터베이스 예약된 작업을 선택합니다.
3. 활성 확인란이 선택되었는지 확인합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
이 양식의 설정은 및 애플리케이션 취약성 대응에 의해 취약성 대응 공유됩니다. 통합 설정을 수정하려면 및 ServiceNow에 대한 취약성 대응 조정 및 전문 지식이 필요합니다.

4. 상자가 선택되어 있으면 작업이 완료된 것입니다.

주:
상자가 선택되어 있지 않으면 에서 이 통합을 구성해야 취약성 대응할 수 있습니다. 선택하기 전에 자세한 내용을 참조하십시오 NVD 및 CWE 통합을 통해 데이터를 임포트하고 외부 공급업체 라이브러리를 관리합니다 .

필요한 경우 임포트한 항목을 보려면 을 참조하십시오 취약성 라이브러리 보기 .

통합 활성화 애플리케이션 취약성 대응

통합을 활성화 애플리케이션 취약성 대응 하여 정기적인 업데이트를 수행합니다.

시작하기 전에
필요한 역할: App-Sec 관리자

프로시저

1. 다음으로 이동 모두 〉 애플리케이션 취약성 대응 〉 통합.
2. 통합을 선택합니다.
3. 활성 확인란을 선택합니다.
4. 업데이트를 선택합니다.
5. 각 통합에 필요한 만큼 반복합니다.
   초기 실행 후 통합은 후속 실행에 대한 델타 임포트를 수행하도록 연결됩니다.

이메일 알림 정의 애플리케이션 취약성 대응

가양성 요청 승인 및 거부와 같은 중요한 업데이트 및 활동에 대한 유용한 정보를 공유하도록 이메일 알림을 설정합니다. 이메일 알림을 생성하려면 알림 전송 시기, 받는 사람 및 포함된 항목 지정이 포함됩니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 이메일 템플릿.
2. 새로 만들기를 선택합니다.

   이메일 알림 생성에 대한 자세한 지침은 문서를 참조하십시오 Create an email notification .

결과
v21.0 of 취약성 대응부터 수신자가 이메일 알림의 링크를 클릭하면 역할에 따라 기록이 OR IT 정정 작업 공간 에서 취약성 관리자 작업 공간 열립니다.

- sn_vul.app_sec_manager 역할을 가진 사용자에 대해 에서 취약성 관리자 작업 공간 열리는 링크입니다.
- 역할, sn_vul.app_security_champion 또는 sn_vul.app_developer가 있는 사용자에 대해 링크에서 열립니다IT 정정 작업 공간.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

수신자에게 위의 역할이 없는 경우 이메일 알림의 링크가 클래식 UI에서 열립니다.

에서 정정 대상 알림 생성 또는 편집 애플리케이션 취약성 대응

취약성 관리자는 정정 대상 알림을 편집하거나 새로 추가하여 알림 전송 시기, 알림 수신자, 알림의 내용을 지정할 수 있습니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 알림.
2. 정정 대상 알림 기록을 선택하거나 새로 만들기를 선택합니다.
3. 양식의 필드에 적절히 입력합니다.
   양식 필드에 대한 자세한 내용은 Create an email notification 문서를 참조하십시오.
4. 메시지를 보려면 알림 미리 보기를 선택합니다.

결과
v21.0 of 취약성 대응부터 수신자가 이메일 알림의 링크를 클릭하면 역할에 따라 기록이 OR IT 정정 작업 공간 에서 취약성 관리자 작업 공간 열립니다.

- 역할이 있는 사용자에 대해 sn_vul.app_sec_manager 에서 취약성 관리자 작업 공간열리는 링크입니다.
- 역할, sn_vul.app_security_champion 또는 sn_vul.app_developer가 있는 사용자에 대해 링크에서 열립니다IT 정정 작업 공간.

수신자에게 위의 역할이 없는 경우 이메일 알림의 링크가 클래식 UI에서 열립니다.

의 예외 관리 애플리케이션 취약성 대응

조직이 게시된 취약성 관리 또는 보안 정책, 표준 또는 가이드라인을 준수할 수 없는 경우 예외를 요청할 수 있습니다. 예외 관리에는 정책에 따라 정정할 수 없는 AVIT(애플리케이션 취약한 항목)에 대한 예외를 요청, 검토, 승인 또는 거부하는 작업이 포함됩니다.

일부 취약성에는 기존 패치, 수정 프로그램 또는 솔루션이 없을 수 있습니다. 예외가 승인되면 취약성을 수정하지 않은 결과를 인정하고 이에 동의하기 때문에 위험을 수락한다는 의미이기도 합니다.

주:

v21.0 부터 애플리케이션 취약성 대응설정된 일 수 후에 승인자와 요청자 모두에 대한 이메일 알림과 함께 긍정 오류 및 예외를 승인하기 위한 시간 범위를 구성할 수 있습니다. 요청이 발생하면 애플리케이션 취약한 항목이 검토 중 상태로 변경되고 상태 변경 기록이 생성됩니다. 승인자가 구성된 시간 범위 내에 응답하지 않으면 애플리케이션 취약한 항목 또는 정정 작업이 열림 상태로 되돌아갑니다. 이전 상태는 **backup_state** 필드에 저장됩니다. 자세한 내용은 예외 관리에 대한 승인 규칙 구성 문서를 참조하십시오.

예외의 수명주기

예외의 정의

예외는 지정된 기간 동안 AVI 수정을 연기하는 요청입니다. 예를 들어 개발자는 머신에 패치를 사용할 수 없는 경우 예외를 요청할 수 있습니다.

예외 요청

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

개발자는 예외 관리 프로세스를 사용하여 AVI에 대한 면제를 요청할 수 있습니다. 애플리케이션 보안 분석가가 이 요청을 승인하면 AVI가 지연 상태로 전환됩니다.

> **중요사항:**
> AVTI 및 RT에 대한 예외를 각각 취약성 관리자 작업 공간 및 IT 정정 작업 공간에서 요청할 수 있습니다. 자세한 내용은 에서 정정 작업 및 기록에 대한 예외 요청 취약성 관리자 작업 공간 및 에서 예외 요청 IT 정정 작업 공간 문서를 참조하십시오.

예외 규칙

v20부터는 규칙의 조건과 일치하는 경우 특정 기간 동안 기존 및 신규 애플리케이션 취약한 항목(AVI)을 자동으로 연기하는 예외 규칙을 생성할 수 있습니다. 예외 규칙을 사용하여 AVI를 자동으로 연기하면 서비스 수준 계약이 누락될 위험이 최소화됩니다. 이 규칙은 수동 개입을 제거하므로 여러 항목을 관리하는 데 도움이 될 수 있습니다. 예외 규칙 만들기를 참조하십시오.

예외 규칙에 대한 연장 요청

v20부터는 예외 규칙의 연기 날짜에 대한 연장 요청을 제출할 수 있습니다. 규칙에 의해 생성된 많은 수의 기록이 지연 날짜(정정 작업에서 새 AVI 수락을 중지하는 날짜)로 해결되지 않는 경우 규칙에 대한 연장을 요청할 수 있습니다. 이 확장은 예외 규칙을 업데이트하여 기존 규칙의 지연 날짜를 자동으로 연장합니다. 현재 날짜로부터 최대 1년까지의 날짜를 입력할 수 있으며 연장 사유를 포함해야 합니다. 연장 요청에는 별도의 승인 그룹에서 2단계 승인이 필요합니다.

예외 요청 승인

즉시 정정할 수 없는 AVIT는 애플리케이션 보안 분석가가 검토하고, 위험을 평가하고, 정정할 수 있을 때까지 연기 승인을 받습니다. 예외 요청 승인은 2단계 플로우일 수 있습니다. 첫 번째 수준 승인자만 있는 경우 예외를 요청하고 승인할 수 있습니다. 그러나 첫 번째 수준 승인자가 없으면 예외를 요청할 수 없습니다. 자세한 내용은 에 대한 예외 승인자 추가 애플리케이션 취약성 대응 문서를 참조하십시오.

> **중요사항:**
> 취약성 관리자 작업 공간에서 예외 요청을 승인하거나 거부할 수 있습니다. 자세한 내용은 에서 요청 승인 또는 거부 취약성 관리자 작업 공간 문서를 참조하십시오.

주:

AVIT에 대한 예외 요청이 승인된 후 다음 작업을 수행할 수 있습니다.

- 재개설
- 자세한 내용 가져오기

예외 요청 추적

예외를 발생시킨 후 AVIT의 상태 변경 승인 탭을 사용하여 상태를 추적할 수 있습니다.

예외 요청의 만료 및 예외 규칙의 연장 요청

특정 AVI에 대한 예외 요청이 만료되면 영향을 받는 AVI가 열림 상태로 되돌아갑니다.

그러나 v20부터는 예외 규칙에서 지연 날짜 연장 요청을 제출할 수 있습니다.

에 대한 예외 관리 구성 애플리케이션 취약성 대응

모듈을 사용하여 요청된 예외의 기간을 제한 하고 예외 또는 긍정 오류 요청에 질문서를 추가합니다 . 기본적으로, 예외를 설정하면 모듈을 사용하여 요청됩니다 ServiceNow# 애플리케이션 취약성 대응 . 통합을 사용하여 예외를 요청할 수도 있습니다 GRC: 정책 및 준수 관리 .

기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_vul.app_manage_exception_configuration

이 태스크 정보
가 활성화된 경우 취약성 대응 예외를 요청할 수 있는 기간을 제한할 수 있습니다. 마찬가지로 모듈이 설치되어 있으면 GRC: 정책 및 준수 관리 구성 화면에서 선택할 GRC: 정책 및 준수 관리 수 있습니다. 이 옵션을 사용하면 에서 정책 및 제어 목표를 GRC지정하는 예외를 요청할 수 있습니다.

질문서를 추가하면 예외 또는 가양성 요청을 제기하는 사람에게 전송됩니다. 기본 질문서를 사용하거나 요구 사항에 따라 만들 수 있습니다.

예외 승인자가 예외를 요청하는 이유를 이해하는 것이 좋습니다.

프로시저

1. 다음으로 이동 모두 〉 애플리케이션 취약성 대응 〉 관리 〉 예외 관리.
2. 예외 관리 구성 양식의 다음을 사용하여 예외 관리 목록에서 옵션을 선택하여 예외를 관리할 방법을 선택합니다.

   주:
   버전 17.1부터 취약성 대응 또는 GRC: 정책 및 준수 관리를 선택할 취약성 대응 수 있습니다. 예외를 요청하는 데 사용할 GRC: 정책 및 준수 관리 플러그인을 활성화해야 GRC 합니다. 구성을 변경해도 기존 데이터에는 영향을 주지 않습니다.

3. 선택한 옵션에 따라 양식의 필드를 채웁니다.
   - 옵션을 선택한 취약성 대응 경우 양식의 필드에 내용을 입력합니다.

     VR 예외 관리 설정 양식

필드	설명
지속 시간	예외를 요청할 수 있는 기간입니다.
단위	지정된 기간의 시간 단위입니다.
예외를 요청하려면 질문서 사용	제기 중인 예외 요청에 질문서를 추가하는 옵션입니다.
예외를 요청하기 위한 질문서	예외를 요청하기 위해 선택한 질문서를 표시하는 옵션입니다. 예외 질문서가 기본적으로 표시됩니다.
긍정 오류로 표시하려면 질문서 사용	제기 중인 긍정 오류 요청에 질문서를 추가하는 옵션입니다.
긍정 오류를 표시하기 위한 질문서	긍정 오류로 표시하기 위해 선택한 질문서를 표시하는 옵션입니다. 긍정 오류 요청에 대한 질문서가 기본적으로 표시됩니다.

   - 옵션을 선택한 GRC: 정책 및 준수 관리 경우 양식의 필드에 내용을 입력합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

VR 예외 관리 설정 양식

필드	설명
긍정 오류로 표시하려면 질문서 사용	제기 중인 긍정 오류 요청에 질문서를 추가하는 옵션입니다.
긍정 오류를 표시하기 위한 질문서	긍정 오류로 표시하기 위해 선택한 질문서를 표시하는 옵션입니다. 긍정 오류 요청에 대한 질문서가 기본적으로 표시됩니다.

4. 저장을 선택합니다.

예외 관리에 대한 승인 규칙 구성

v15.0부터 애플리케이션 취약성 대응 플로우 디자이너를 사용하여 예외 관리, 예외 규칙 및 긍정 오류 관리에 대한 예외 요청을 승인합니다. AVR(처음 배포 애플리케이션 취약성 대응)하는 경우 Flow Designer가 기본적으로 활성화됩니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin

이 태스크 정보
기존 VR 사용자인 경우 기본 옵션은 워크플로우입니다.
v15.0 이상을 배포 애플리케이션 취약성 대응 한 경우 시스템 속성의 *sn_vul.flow_designer_activation* 값이 true로 설정됩니다. 즉, Flow Designer가 기본적으로 활성화됩니다.

v15.0 이전 버전을 이미 사용 애플리케이션 취약성 대응 중인 경우 이 시스템 속성의 값은 false로 설정됩니다. 값을 true로 변경하여 플로우 디자이너를 활성화할 수 있습니다.

> **주:**
> Flow Designer를 활성화한 후에는 워크플로우 사용으로 되돌릴 수 없습니다. 워크플로우와 Flow Designer를 자세히 비교하려면 다음 항목을 참조하십시오 예외 관리 워크플로우와 Flow Designer 비교.

플로우 디자이너를 사용하려면 승인 규칙 모듈을 사용하여 규칙을 생성합니다. 이 모듈을 사용하여 다음의 각 예외 관리 워크플로우에 대한 승인 규칙을 구성할 수 있습니다.

- 정정 작업에 대한 예외 요청
- 애플리케이션 취약한 항목에 대한 예외 요청
- 예외 규칙
- 정정 작업에 대한 긍정 오류
- 애플리케이션 취약한 항목에 대한 가양성

> **주:**
> 규칙 내에 여러 수준의 승인을 포함하는 조건을 정의할 수도 있습니다. Flow Designer는 이 모듈에서 생성된 규칙을 자동으로 상속하고 일치하는 승인 워크플로우를 처리합니다.

프로시저

1. 다음으로 이동 모두 〉 애플리케이션 취약성 대응 〉 관리 〉 승인 규칙.

2. 승인 규칙 페이지에서 승인 규칙을 설정할 그룹을 선택합니다.

3. 양식에서 필드를 채웁니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

승인 규칙 양식

필드	설명
이름	승인 구성 이름입니다.
테이블	규칙이 적용되는 테이블입니다.
애플리케이션	기본값은 취약성 대응입니다.
규칙 유형	규칙 유형을 지정합니다. 예를 들어 예외 관리, 가양성 또는 예외 규칙이 있습니다.
활성	기본적으로 활성화되며, 승인 규칙이 사용 중임을 나타냅니다.
설명	승인 규칙에 대한 간단한 설명입니다.
승인 만료Y (일) v21.0 of 애플리케이션 취약성 대응	승인자가 요청을 승인할 수 있을 때까지의 날짜입니다.
승인자에게 알림(일) v21.0 of 애플리케이션 취약성 대응	승인자에게 조치를 취하라는 알림이 전송된 날짜입니다.

4. 업데이트를 선택합니다.
   승인 구성 탭에는 기본적으로 두 가지 수준의 승인자가 설정됩니다. 규칙을 선택하여 규칙 내의 다양한 사용 사례를 기반으로 조건을 정의할 수 있습니다.

   주:
   각 구성 페이지에서 여러 승인 수준을 생성할 수 있습니다.

Example:
다양한 사용 사례를 기반으로 서로 다른 구성 항목에서 발견된 동일한 취약성에 대해 서로 다른 승인 프로세스를 정의할 수 있습니다.

에서 정정 연기 애플리케이션 취약성 대응

v20.0부터 애플리케이션 취약한 항목(AVI) 및 정정 작업의 수명주기 동안 사용할 수 있는 구현 대기 중 상태의 정정을 연기할 수 있습니다. AVI에서 구현 대기 중 과 조사 중 상태의 정정 작업 기록을 선택하여 기록을 이 상태로 수동 전환할 수만 있습니다.

사용 케이스

정정 전문가는 기록을 구현 대기 중 으로 이동하여 작업에 대한 조사 및 작업이 완료되었음을 팀에 알릴 수 있습니다. 수정 사항을 구현할 준비가 되었지만 사용할 수 없는 경우 이 업데이트를 선택할 수 있습니다. 사용할 수 없는 수정 사항의 예로는 소프트웨어 패치가 있습니다. 조사를 마쳤을 때 패치에 대한 유지 관리 기간을 사용할 수 없는 경우 패치를 배포할 수 있을 때까지 작업을 구현 대기 중 으로 이동할 수 있습니다.

필수 필드

구현 대기 중 상태에 있는 AVI 및 정정 작업 기록에는 편집 가능한 필수 필드 2개가 있습니다.

정정 약정 날짜

계획된 정정 날짜입니다.

정정 계획

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

정정을 위한 정정 계획에 대한 설명입니다. 이 텍스트는 기록의 메모에 표시됩니다.

필드 및 시스템 속성

기록을 구현 대기 중으로 전환할 때 나타나는 모달에 대해 기본적으로 # 가지 시스템 속성이 true로 설정됩니다. 기본 설정으로 유지되는 경우:

sn_vul.remediation_fields

정정 약정 날짜 및 정정 계획을 필수 필드로 설정합니다. false로 설정된 경우 이러한 필드는 선택 사항입니다.

sn_vul.awaiting_implementation

기록에서 구현 대기 중을 선택하면 정정 약정 날짜, 정정 계획 필드가 있는 모달이 표시됩니다. false로 설정하면 약정 날짜 또는 계획을 입력하라는 프롬프트 없이 AVI의 상태를 구현 대기 중으로 변경할 수 있습니다.

누락된 정정 약정 날짜 모듈

누락된 정정 약정 날짜 모듈에서 정정 약정 날짜가 누락된 AVI를 봅니다. 이동 애플리케이션 취약성 대응 〉 취약한 항목 〉 누락된 정정 약정 날짜 을 클릭하여 목록을 봅니다.

정정 작업에서 AVI로 상태 롤다운

기록을 구현 대기 중 으로 전환하는 UI 작업 버튼은 조사 중 상태의 애플리케이션 취약한 항목 및 정정 작업 기록에서만 표시됩니다. 상태 롤다운의 경우 정정 작업에서 구현 대기 중 을 선택할 때 나타나는 모달에는 기존 AVI를 재정의하는 옵션이 있습니다.

옵션	설명
기존 **AVI** 재정의를 선택합니다.	이 옵션을 선택하면 이미 구현 대기 중 상태에 있는 작업의 모든 정정 약정 날짜 및 정정 계획을 재정의할 수 있습니다. 선택하는 경우 이 기능은 정정 작업의 날짜 및 계획 데이터를 AVI로 롤다운합니다.
기존 **AVI** 재정의를 비활성화된 상태로 둡니다.	이미 구현 대기 중 상태에 있는 작업의 기존 AVI에 대한 날짜와 계획 값을 그대로 유지하려면 이 옵션을 비활성화된 상태로 둡니다. 비활성화하면 이미 구현 대기 중 상태에 있는 AVI는 기존 날짜와 계획 데이터를 유지하며 상태 롤다운의 영향을 받지 않습니다.

롤다운 예시

작업의 약정 날짜를 업데이트하고 소프트웨어 패치 유지관리 기간에 대한 정보를 계획할 수 있도록 정정 작업을 미결 에서 구현 대기 중 으로 전환하려 한다고 가정해 보겠습니다. 이 작업에 구현 대기 중 상태의 AVI가 있고 정정 작업과 일치하도록 약정 날짜 및 계획 정보를 업데이트하려 한다고 가정합니다.

정정 작업과 일치하도록 AVI 날짜 및 계획 데이터를 덮어쓰려면 메시지가 표시될 때 기존 **AVI** 재정의 확인란을 선택합니다. AVI의 날짜 및 계획 값은 구현 대기 중을 선택할 때 프롬프트에서 작업에 대해 입력하는 계획 및 날짜 값이 됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 경우 재정의 옵션을 선택하지 않고 구현 대기 중 AVI가 있는 경우 AVI의 원래 날짜 및 계획 데이터는 그대로 유지됩니다. 구현 대기 중을 선택할 때 프롬프트에서 작업에 대해 입력하는 계획 및 날짜 값은 작업의 구현 대기 중 상태에 있는 AVI에 사용되지 않습니다.

작업의 AVI가 해결 됨 또는 종결 고정 상태이고 작업을 구현 대기 중으로 전환하는 경우 기존 **AVI** 재정의 를 선택해도 상태 우선순위가 더 높기 때문에 AVI가 종결-고정 및 해결 됨에서 구현 대기 중으로 변경되지 않습니다.

작업을 구현 대기 중 으로 이동하는 동안 재정의를 선택하지 않았고 구현 대기 중인 AVI가 이미 있는 경우 작업을 다시 오픈 또는 조사 중으로 이동하면 AVI는 구현 대기 중 상태로 유지됩니다.

에 대한 예외 승인자 추가 애플리케이션 취약성 대응

예외를 요청할 수 있도록 승인자 그룹에 사용자를 추가합니다.

시작하기 전에
필요한 역할: sn_vul.app_exception_approver

이 태스크 정보
애플리케이션 취약한 항목에 대한 예외 요청은 기본 2단계 승인 플로우를 사용하여 승인됩니다. 요청은 두 가지 수준의 승인자가 승인할 수 있습니다. 사용자를 첫 번째 수준 그룹에 추가해야 합니다. 두 번째 수준에 사용자가 없는 경우, 요청은 첫 번째 수준 승인 후에 승인됩니다.

프로시저

1. 다음으로 이동 모두 〉 사용자 관리 〉 그룹.
2. 이름 열에서 예외를 검색하고 애플리케이션 예외 승인자 - 수준 **1**을 클릭합니다.

   주:
   v12.8.1부터 애플리케이션 취약성 대응 시스템 속성〔sys_properties〕테이블의 워크플로우를 통해 예외 승인을 위해 기본 시스템에 제공된 시스템 속성을 사용할 수 있습니다. 따라서 워크플로우를 통해 예외 또는 가양성 요청이 발생하면 승인을 위해 시스템 속성에 정의된 그룹 ID로 전송됩니다. 다음으로 이동 모두 〉 시스템 속성 및 , *sn_vul.app_exception_approver_L2*, 또는 *sn_vul.app_false_positive_approver_group* 을 선택하여 *sn_vul.app_exception_approver_L1*속성 값을 변경합니다.

3. 그룹 애플리케이션 예외 승인자 - 수준 1 양식에서 그룹 구성원 관련 목록을 클릭합니다.
4. 새로 만들기를 클릭하여 목록을 만듭니다.
5. 양식에서 필드를 채웁니다.

사용자 양식

필드	설명
사용자 ID	사용자의 고유 식별자입니다.
이름	사용자의 이름입니다.
성	사용자의 성입니다.
직위	사용자의 직함입니다. 직함 또는 직무 설명을 입력하거나 목록에서 선택합니다.
부서	사용자의 부서입니다.
암호	사용자에게 할당된 암호입니다. 이 암호는 영구적이거나 임시적일 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
암호 다시 설정 필요	사용자가 보안을 보장하기 위해 암호를 재설정할 수 있도록 하는 옵션입니다.
잠겨 있음	사용자를 인스턴스에서 잠그고 사용자의 모든 활성 세션을 종료하는 옵션입니다. 시스템은 관리자 역할을 가진 사용자가 자신을 잠그는 것을 방지합니다.
활성	이 사용자를 활성화하는 옵션입니다. 다음 영역에서는 비활성 사용자만 볼 수 있습니다. ○ 사용자 목록 ○ 참조 필드의 선택 목록(돋보기 아이콘) ○ 참조 필드에 입력할 때 나타나는 자동 완성 목록
웹 서비스 접근만 허용	이 사용자를 비대화형 사용자로 지정하는 옵션입니다.
내부 통합 사용자	이 사용자를 내부 통합 사용자로 지정하는 옵션입니다.
이메일	사용자의 이메일 주소입니다.
언어	사용자의 기본 설정 언어입니다.
달력 통합	작업 일정을 관리하는 데 사용되는 달력입니다. 예를 들어 Outlook입니다.
시간대	이 사용자의 위치에 대한 시간대입니다.
날짜 형식	사용자가 선호하는 날짜 형식입니다.
직장 전화번호	사용자의 직장 전화 번호입니다.
휴대폰	사용자의 휴대폰입니다.
사진	추가하려면 클릭...을 클릭하여 업로드할 수 있는 사진입니다.

6. 제출을 클릭합니다.
7. 옵션: 1-5단계를 반복하여 애플리케이션 예외 승인자 - 수준 2를 만듭니다.
   승인자는 애플리케이션 취약성 대응 〉 내 승인 으로 이동하여 요청을 승인해야 합니다.

에서 예외 요청 및 승인 애플리케이션 취약성 대응

지정된 기간 동안 애플리케이션 취약한 항목 및 정정 작업의 정정을 연기하도록 요청할 수 있습니다.

예를 들어 개발자는 머신에 패치를 사용할 수 없는 경우 예외를 요청할 수 있습니다. 액세스 권한이 있는 승인자는 다른 사용자의 요청을 승인할 수 있습니다.

또한 예외 규칙을 생성하고 예외 규칙에 대한 예외 확장을 요청할 수 있습니다. 기본적으로 지연, 예외 규칙 및 예외 연장 요청에는 두 가지 수준의 승인이 필요합니다.

예외를 요청하거나 승인하려면 다음을 참조하십시오.

- 애플리케이션 취약한 항목에 대한 예외 요청
- 를 사용하여 애플리케이션 취약성에 대한 예외 요청 GRC: 정책 및 준수 관리

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 에서 예외 규칙 및 예외 규칙 확장 요청 승인 애플리케이션 취약성 대응
- 에서 예외 규칙에 대한 연장 요청 애플리케이션 취약성 대응

주:

이메일 알림은 예외 관리의 모든 단계에서 전송되어 요청의 상태 및 기타 세부 정보를 제공합니다. 예를 들어 예외가 요청되면 요청자는 요청이 발생했음을 확인하는 이메일을 받습니다. 또한 승인자는 예외가 요청되었다는 내용의 이메일을 받습니다.

v21.0 부터 애플리케이션 취약성 대응설정된 일 수 후에 승인자와 요청자 모두에 대한 이메일 알림과 함께 긍정 오류 및 예외를 승인하기 위한 시간 범위를 구성할 수 있습니다. 요청이 발생하면 애플리케이션 취약한 항목이 검토 중 상태로 변경되고 상태 변경 기록이 생성됩니다. 승인자가 구성된 시간 범위 내에 응답하지 않으면 애플리케이션 취약한 항목 또는 정정 작업이 열림 상태로 되돌아갑니다. 이전 상태는 **backup_state** 필드에 저장됩니다. 자세한 내용은 예외 관리에 대한 승인 규칙 구성 문서를 참조하십시오.

애플리케이션 취약한 항목에 대한 예외 요청

즉시 정정할 수 없는 애플리케이션 취약한 항목에 대한 예외를 요청합니다. 예를 들어 개발자는 머신에 패치를 사용할 수 없는 경우 예외를 요청할 수 있습니다.

중요사항:
취약성 관리자 작업 공간 및 IT 정정 작업 공간에서 애플리케이션 취약한 항목 및 정정 작업에 대한 예외를 요청할 수 있습니다. 자세한 내용은 에서 정정 작업 및 기록에 대한 예외 요청 취약성 관리자 작업 공간 및 에서 예외 요청 IT 정정 작업 공간 문서를 참조하십시오.

시작하기 전에
필요한 역할: 개발자 그룹

프로시저

1. 다음으로 이동 애플리케이션 취약성 대응 〉 애플리케이션 취약한 항목 〉 모두 을 클릭하고 예외를 요청할 항목을 선택합니다.
   선택한 항목은 오픈 또는 조사 중 상태여야 합니다.

   주:

   v21.0 of 애플리케이션 취약성 대응부터 애플리케이션 취약한 항목의 이전 상태가 **backup_state** 필드에 저장됩니다.

2. 애플리케이션 취약한 항목 양식에서 예외 요청을 클릭합니다.

   주:
   취약성 대응 선택되었는지 또는 GRC: 정책 및 준수 관리 에 따라 애플리케이션 취약성 대응 〉 예외 관리 화면에 예외 요청 양식이 변경됩니다. 만약 GRC: 정책 및 준수 관리에 , 참조 를 사용하여 애플리케이션 취약성에 대한 예외 요청 GRC: 정책 및 준수 관리

3. 이 항목을 예외 관리 화면에서 선택한 경우 취약성 대응 예외 요청 양식의 필드에 내용을 입력합니다.

   예외 요청 양식

필드	설명
다음까지	예외 요청이 만료되는 날짜입니다. 이 날짜는 에서 선택한 기간 내에 있어야 합니다. 모두 〉

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	애플리케이션 취약성 대응 〉 관리 〉 예외 관리 화면. 예외 요청이 만료되면 그룹은 열림 상태로 되돌아갑니다. 주: (AVR) 버전 18.0 애플리케이션 취약성 대응 부터 지연된 애플리케이션 취약한 항목을 스캐너에서 닫고 다시 열 수 있습니다. 예외 기간이 만료되기 전에 항목이 다시 열리면 AVIT의 상태가 활성 예외 창을 적용하는 지연 상태로 되돌아갑니다. 이 기능을 사용 설정하려면 시스템 속성 sn_vul.auto_defer_avit_in_active_exception_window의 값을 true로 설정합니다. 또한 지연된 종료 날짜는 AVIT가 종결되거나 예외가 만료된 후에도 유지됩니다. 필요한 역할은 읽기와 쓰기 모두에 대해 sn_vul.app_manage_exception_configuration입니다.
이유	이유를 선택합니다. 선택 항목은 다음과 같습니다. ○ 위험 수락됨 ○ 유지관리 기간을 기다리는 중 ○ 수정 사용 불가 ○ 사용 중인 완화 통제 ○ 기타 새 이유 선택 사항을 추가하는 방법을 보려면 을 참조하십시오 정책 사유 매핑 정의.
추가 정보	이 요청이 수행되는 이유와 관련된 상세 정보입니다. 이 필수 필드는 정정 소유자가 업데이트해야 합니다.

4. 승인 요청을 클릭하여 예외 요청을 제출합니다.
애플리케이션 취약성 항목의 상태가 검토 중으로 변경됩니다. 상태 변경 승인 탭을 사용하여 예외 요청의 상태를 추적합니다.

를 사용하여 애플리케이션 취약성에 대한 예외 요청 **GRC:** 정책 및 준수 관리

에서 애플리케이션의 애플리케이션 취약성 대응정책 예외 관리 기능을 정책 및 준수 관리 사용하여 GRC 정책 예외를 요청합니다.

시작하기 전에
정책 예외 통합을 사용하여 정책 예외를 요청하려면 먼저 에서 ServiceNow Store애플리케이션을 다운로드 GRC: 정책 및 준수 관리 해야 합니다.

필요한 역할: sn_vul.remediation_owner

클래식 UI에서 예외를 요청할 수도 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 애플리케이션 취약성 대응 〉 애플리케이션 취약한 항목 (또는 정정 작업)〉모두로 설정하고 예외를 요청할 항목 또는 그룹을 엽니다.
   선택한 항목 또는 그룹은 오픈, 조사 중 또는 구현 대기 중 상태여야 합니다.
2. 선택한 양식에서 예외 요청을 클릭합니다.
3. 이 항목을 예외 관리 화면에서 선택한 경우 GRC: 정책 및 준수 관리 예외 요청 양식의 필드에 내용을 입력합니다.

   예외 요청 양식

필드	설명
정책	예외를 요청하는 취약성 관리 정책입니다.
컨트롤 목적	선택한 정책과 연결된 통제 목표입니다. 정책을 선택하지 않으면 모든 통제 목표가 나열됩니다.
유효 기간(시작)	예외가 시작되는 날짜입니다. 기본값은 현재 날짜입니다. 이 날짜는 과거일 수 없습니다.
유효 기간	정책 예외가 만료되고 취약한 항목 또는 그룹의 상태가 연기됨에서 미결로 변경되는 날짜입니다. **주:** 정책 예외가 유효한 일 수는 정책 및 준수에서 정책에 대해 설정한 최대 예외 기간(일) 을 초과할 수 없습니다. 자세한 내용은 정책 만들기를 참조하세요.
이유	예외를 요청하는 이유입니다.
근거	이 요청이 수행되는 이유와 관련된 상세 정보입니다. 이 필수 필드는 정정 소유자가 입력해야 합니다.

   a. 승인 요청을 클릭하여 예외 요청을 제출합니다.
   취약한 항목의 상태가 검토 중으로 변경되고 정책 예외가 생성됩니다. 상태 변경 승인 탭을 사용하여 예외 요청의 상태를 추적합니다.

   b. 정책 예외를 보려면 정책 예외 관련 목록을 클릭합니다.

   c. 정책 예외 번호를 클릭합니다.

   d. 승인자 필드에서 승인자의 이름을 선택합니다.

   e. 소스 탭을 클릭하고 통제 목표 필드에서 통제 목표를 선택합니다.

   f. 위험 평가 탭을 클릭하고 위험 등급 필드에서 위험 등급을 선택합니다.

   g. 양식을 저장합니다.

   h. 영향을 받는 컨트롤 탭을 클릭하고 추가를 클릭하여 컨트롤을 추가합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

i. 양식을 저장합니다.

> 주:
> 규정 준수 검토 요청을 클릭하여 규정 준수 검토를 제기할 수 있습니다.

j. 승인 양식이 승인자에게 전송됩니다.

k. 승인자는 승인을 클릭하여 요청을 승인하거나 추가 승인 요청을 클릭하여 추가 승인을 요청할 수 있습니다.
기록 상태가 연기됨으로 변경됩니다. 명시된 이유는 예외 요청을 제기할 때 선택한 이유입니다. 지연 탭에는 기록에 대한 추가 메모가 제공됩니다.

> 주:
> 요청이 거부되면 기록이 이전 상태로 이동합니다.

4. 제출을 클릭합니다.
정책 예외 통합 및 정정 소유자와 준수 관리자 간의 핸드오프에 대한 자세한 내용은 정책 및 준수 관리 선택적 설정을 참조하십시오.

애플리케이션 정정 작업에 대한 예외 요청

애플리케이션 정정 작업을 즉시 해결할 수 없는 경우 예외를 요청하여 지정된 기간 동안 애플리케이션 정정 작업을 연기합니다.

시작하기 전에

작업 공간에서 예외를 취약성 대응 요청할 수 있습니다. 에서 예외 요청 IT 정정 작업 공간 문서를 참조하십시오.

가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

필요한 역할: sn_vul.remediation_owner, sn_vul.app_security_champion 또는 sn_vul_container.remediation_owner.

클래식 환경에서 애플리케이션 정정 작업에 대한 예외를 요청할 수도 있습니다.

프로시저

1. 다음으로 이동 모두 〉 애플리케이션 취약성 대응 〉 정정 작업 〉 모두.
2. 예외를 요청할 그룹을 선택합니다.
선택한 작업은 오픈, 조사 중 또는 구현 대기 중 상태여야 합니다.
3. 애플리케이션 정정 작업 기록에서 예외 요청을 선택합니다.
4. 양식에서 필드를 채웁니다.

예외 요청 양식

필드	설명
다음까지	예외 요청이 만료되는 날짜입니다. 이 날짜는 구성에 정의된 예외 기간 내에 있어야 합니다.
이유	예외 요청에 대한 근거입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
추가 정보	이 요청이 수행되는 이유와 관련된 상세 정보입니다. 이 필드는 정정 소유자가 업데이트해야 합니다.

5. 승인 요청을 클릭합니다.

에서 예외 규칙 및 예외 규칙 확장 요청 승인 애플리케이션 취약성 대응

즉시 정정할 수 없는 애플리케이션 취약한 항목에 대한 예외 요청을 승인합니다. 이러한 위험 요청을 평가한 다음 정정할 수 있을 때까지 연기하도록 승인해야 합니다.

시작하기 전에
필요한 역할: sn_vul.app_exception_approver

프로시저

1. 다음으로 이동 모두 〉 애플리케이션 취약성 대응 〉 내 승인.
2. 큐에서 요청을 선택합니다.
3. 적절한 설명을 사용하여 요청을 승인하거나 거부합니다.

정책 사유 매핑 정의

예외를 요청하는 모든 사용자가 사용할 수 있는 이유 선택 항목을 정의할 수 있습니다.

시작하기 전에
GRC: Policy and Compliance Management 애플리케이션이 설치되어 있어야 합니다. 이 애플리케이션은 별도의 구독을 통해 사용할 ServiceNow# Store 수 있습니다.

시스템 요구 사항과 제품군 호환성에 대한 자세한 내용은 ServiceNow Store 웹 사이트에서 애플리케이션 목록을 참조하십시오.

필요한 역할: sn_vul.compliance.manager 및 sn_vul.vulnerability_admin

프로시저

1. 다음으로 이동 모두 〉 정책 및 준수 〉 정책 예외 〉 통합 레지스트리.

   주:
   이유 선택 테이블에 있는 이유 선택 항목에서 이유를 선택하거나 새 이유를 추가할 수 있습니다.

2. 애플리케이션의 통합 레지스트리(예: 애플리케이션 취약성 대응, 취약성 대응 등)를 클릭합니다.
3. 기존 이유 선택을 추가하려면 다음 단계를 수행합니다.
   a. 이유 선택 목록에서 새로 만들기를 클릭합니다.
   b. 돋보기 아이콘을 클릭하여 이유를 선택합니다.
4. 이유 선택 테이블에 새 이유 선택 사항을 추가하려면 다음 단계를 수행합니다.
   a. 이유 선택 목록에서 새로 만들기를 클릭합니다.
   b. 돋보기 아이콘을 클릭합니다.
   c. 새로 만들기를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

d. 양식에서 필드를 채웁니다.

이유 선택 목록 양식

필드	설명
레이블	이 선택 항목의 고유 레이블입니다.
값	이 선택 항목의 고유 값입니다. 이 값은 각 애플리케이션에 대한 정책 예외 이유 매핑 테이블에 매핑됩니다. 이 테이블로 이동하려면 sn_vul_policy_reason_mapping를 입력하십시오. 필터 탐색기의 LIST.
순서	이 선택 항목에 대한 순서입니다. 이유는 이 숫자를 기준으로 정렬됩니다.
기본값	요청 시 정책 예외가 요청될 때마다 이 이유 선택을 사용할 수 있음을 나타내는 옵션입니다. 통합 레지스트리에 애플리케이션별 선택 항목이 포함되어 있지 않으면 기본 필드가 선택된 모든 이유 선택 항목을 사용할 수 있습니다.
활성	이유 선택 목록에 선택 항목을 표시하는 옵션입니다.

5. 제출을 클릭합니다.

에서 예외 규칙에 대한 연장 요청 애플리케이션 취약성 대응

지연된 예외 규칙이 기한까지 지연되기 전에 해당 규칙의 연장을 요청합니다. 정정 소유자는 더 이상 이 요청을 하기 위해 지연된 기한까지 기다릴 필요가 없습니다.

시작하기 전에

필요한 역할: App-Sec 관리자 sn_vul.app_sec_manager, 보안 챔피언 sn_vul.app_security_champion.

이 태스크 정보

연장 규칙 기록에서 규칙이 승인됨 상태인 경우에만 연기된 종료 날짜에 대한 연장을 요청할 수 있습니다. 규칙에 의해 생성된 많은 수의 기록이 지연 종료 날짜, 즉 정정 작업에서 새 AVI 수락을 중지하는 날짜로 해결되지 않는 경우 규칙에 대한 이 확장을 요청할 수 있습니다. 이 확장은 예외 규칙을 업데이트하여 기존 규칙의 지연 날짜를 자동으로 연장합니다.

작업 공간에서 연장을 취약성 대응 요청할 수도 있습니다. 자세한 내용은 취약성 관리자 작업 공간에서 지연된 취약한 항목에 대한 연장 요청 문서를 참조하십시오.

프로시저

1. 다음으로 이동 모두 〉 애플리케이션 취약성 대응 〉 예외 규칙.

2. 승인된 예외 규칙을 선택합니다.

3. 연장 요청을 선택합니다.

4. 양식의 필드에 적절히 입력합니다.

필드	설명
연장 날짜	예외 규칙을 연장해야 하는 종료 날짜를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
이유	예외 규칙을 지연시키는 이유를 입력합니다. 선택 항목은 다음과 같습니다. ○ 수용된 위험 ○ 유지관리 기간을 기다리는 중 ○ 수정 사용 불가 ○ 사용 중인 완화 통제 ○ 기타
추가 정보	기타 관련 정보를 입력합니다.

5. 승인 요청을 선택합니다.
요청이 승인되면 예외 규칙과 관련 정정 작업 및 애플리케이션 취약한 항목에 대해 지연 기한, 이유 및 추가 정보 필드가 업데이트됩니다. 요청 제출 및 승인자의 후속 조치 시에도 이메일이 트리거됩니다.

주:

- 요청은 두 가지 수준의 승인을 거칩니다.
- 연장 요청 버튼은 예외 규칙의 일부로 생성된 정정 작업에 사용할 수 없습니다.
- 지연된 예외 규칙이 다시 확장되면 백엔드에서 연장 지연 수가 증가합니다.

에서 지연된 정정 작업에 대한 연장 요청 애플리케이션 취약성 대응

지연된 기한에 도달하기 전에 지연된 정정 작업(VUL)에 대한 연장을 요청합니다. 정정 소유자는 더 이상 이 요청을 하기 위해 지연된 기한까지 기다릴 필요가 없습니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)

이 태스크 정보
작업 공간에서 연장을 취약성 대응 요청할 수도 있습니다. 자세한 내용은 취약성 관리자 작업 공간에서 지연된 취약한 항목에 대한 연장 요청 문서를 참조하십시오.

프로시저

1. 다음으로 이동 모두 〉 애플리케이션 취약성 대응 〉 정정 작업.
2. 지연된 정정 작업을 엽니다.
3. 연장 요청을 선택합니다.
4. 양식의 필드에 적절히 입력합니다.

필드	설명
연장 날짜	지연 상태가 만료되고 정정 작업이 다시 시작되는 날짜를 선택합니다.
이유	문제를 지연시키는 이유를 입력합니다. 선택 항목은 다음과 같습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	○ 유지관리 기간을 기다리는 중 ○ 수정 사용 불가 ○ 수용된 위험 ○ 사용 중인 완화 통제 ○ 기타
추가 정보	기타 관련 정보를 입력합니다.

5. 승인 요청을 선택합니다.
   요청이 승인되면 정정 작업의 일부인 애플리케이션 취약한 항목에도 변경 사항이 롤다운됩니다. 그러나 애플리케이션 취약한 항목은 지연 상태이고 현재 종료 데이터는 업데이트 종료 날짜 이전이어야 합니다. 요청 제출 및 승인자의 후속 조치 시에도 이메일이 트리거됩니다.

   주:
   - 요청은 두 가지 수준의 승인을 거칩니다.
   - 연장 요청 버튼은 예외 규칙의 일부로 생성된 정정 작업에 사용할 수 없습니다.
   - 지연된 정정 작업이 다시 연장되면 백엔드에서 연장 지연 수가 증가합니다.

에서 지연된 애플리케이션 취약한 항목에 대한 연장 요청 애플리케이션 취약성 대응

지연된 애플리케이션 취약한 항목이 지연 기한에 도달하기 전에 해당 항목에 대한 연장을 요청합니다. 정정 소유자는 더 이상 이 요청을 하기 위해 지연된 기한까지 기다릴 필요가 없습니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)

이 태스크 정보
작업 공간에서 연장을 취약성 대응 요청할 수도 있습니다. 자세한 내용은 취약성 관리자 작업 공간에서 지연된 취약한 항목에 대한 연장 요청 문서를 참조하십시오.

프로시저

1. 다음으로 이동 모두 〉 애플리케이션 취약성 대응 〉 취약 항목.
2. 지연된 애플리케이션 취약한 항목을 엽니다.
3. 연장 요청을 선택합니다.

   주:
   연장 요청 버튼은 애플리케이션 취약한 항목의 상태가 연기됨인 경우에만 표시됩니다.

4. 양식의 필드에 적절히 입력합니다.

필드	설명
연장 날짜	정정을 위해 지연된 애플리케이션 취약한 항목을 연장해야 하는 종료 날짜를 선택합니다.
이유	문제를 지연시키는 이유를 입력합니다. 선택 항목은 다음과 같습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	○ 유지관리 기간을 기다리는 중 ○ 수정 사용 불가 ○ 수용된 위험 ○ 사용 중인 완화 통제 ○ 기타
추가 정보	기타 관련 정보를 입력합니다.

5. 승인 요청을 선택합니다.
이메일은 요청 제출 및 승인자의 후속 조치 시 트리거됩니다.

주:

- 요청은 두 가지 수준의 승인을 거칩니다.
- 지연된 예외 규칙이 다시 확장되면 백엔드에서 연장 지연 수가 증가합니다.

6. 요청이 승인되면 기한, 이유 및 연기 메모가 업데이트됩니다.

에 대한 예외 규칙 생성, 삭제 및 취소 애플리케이션 취약성 대응

특정 조건을 충족하는 애플리케이션 취약한 항목(AVI)에 대해 자동으로 예외를 요청하는 규칙을 생성합니다.

시작하기 전에
예를 들어, 즉시 해결할 수 없는 알려진 특정 취약성 또는 중요 취약성을 기반으로 하는 조건으로 규칙을 만들 수 있습니다. 이 규칙을 사용하면 승인된 규칙 조건과 일치하는 경우 신규 및 기존 AVI를 자동으로 연기할 수 있습니다.

- 예외 규칙은 유효 기간(시작)부터 규칙 기록에 입력한 유효 기간(종료) 날짜까지 적용됩니다.
- 정정 작업(AVUL)은 지연 됨 상태의 일치하는 AVI에 대한 규칙이 승인된 후에 생성됩니다.
- 이 AVUL의 그룹화 방법을 예외 규칙이라고 합니다.
- 이 AVUL을 닫거나, 다시 열거나, 삭제할 수 없습니다. 신규 및 다시 열린 AVI는 유효 기간 **(Valid)** 시작 날짜부터 유효 기간**(Valid)** 종료 날짜에 그룹이 만료될 때까지 지연되고 이 AVUL에 추가됩니다.

주:

이메일 알림은 예외 규칙 워크플로우의 모든 단계에서 전송됩니다. 이러한 이메일은 요청의 상태 및 기타 세부 정보를 제공합니다. 예를 들어 예외 규칙이 요청되면 요청자는 요청이 제출되었음을 확인하는 이메일을 받습니다.

규칙이 거부되면 초안 상태에서 다시 열고 업데이트한 다음 승인을 위해 다시 제출할 수 있습니다.

필요한 역할: 앱 SEC 관리자 sn_vul.app_sec_manager 및 보안 챔피언 sn_vul.app_security_champion.

프로시저

1. 다음으로 이동 모두 〉 애플리케이션 취약성 대응 〉 관리 〉 예외 규칙.
2. 예외 규칙 새 기록 페이지에서 새로 만들기를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 필드에 내용을 입력합니다.

필드	설명
이름	예외 규칙의 이름입니다.
상태	읽기 전용: 초안
유효 기간(시작)	AVI 연기를 위해 이 규칙이 활성화되는 날짜입니다.
실행 순서	각 예외 규칙에 대한 고유한 순서입니다. 낮은 값이 높은 값보다 우선합니다.
유효 기간(종료)	정정 작업에서 새 AVI 수락을 중지한 날짜입니다.
지연 기한	정정 작업 및 AVI가 지연될 때까지의 날짜입니다. 이 날짜에 AVUL이 종결되고 모든 AVI가 작업에서 나갔다가 다시 열립니다. 그룹 규칙은 이러한 AVI에 다시 적용됩니다.
이유	이 예외 규칙을 생성하는 이유입니다.
할당 그룹	지연된 AVI를 추적하기 위해 정정 작업이 할당된 그룹입니다.
추가 정보	요청자가 승인자에게 제공하려는 추가 정보입니다. 이 정보는 정정 작업의 설명 필드에 채워집니다.
조건	이 규칙과 일치하는 AVI를 지정하는 필터 조건입니다.
기존 데이터에서 실행	이 규칙을 처음 실행할 때 기존 데이터에 대해 이 규칙을 실행할 수 있도록 하는 옵션입니다. 이 옵션을 비활성화하면 새 데이터로 시작하는 예약된 작업에 *`Associate existing AVIs with Auto Exception Rule`* 따라 규칙이 매일 실행됩니다. 기존 데이터에서 실행 옵션을 활성화하면 예약된 작업이 유효 기간(시작) 날짜에 기존 데이터에 대해 한 번 실행됩니다.

4. 규칙을 생성할 때 할당 그룹을 추가합니다.
5. 하나를 선택합니다.

   규칙이 승인되면 승인됨 상태로 전환됩니다. 규칙은 작업을 통해 AVI를 *`Associate existing AVIs with Auto Exception Rule scheduled`* 평가합니다. 기존 데이터에서 실행을 선택한 경우 기존 AVI를 평가합니다. 규칙에 대한 정정 작업이 자동으로 생성되고 해당 조건을 충족하는 일치하는 AVI가 작업과 연결됩니다.

   예약된 작업은 기존 데이터에 대해 예외 규칙을 한 번 실행합니다. AVI를 찾을 수 없는 경우에도 기존 데이터에서 규칙이 다시 실행되지 않습니다. 규칙과 일치하는 기존 AVI가 이미 지연되었기 때문에 새 데이터만 평가합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

6. 규칙을 삭제하려면 예외 규칙 기록에서 삭제를 선택합니다.
   다음과 같은 메시지가 나타납니다. ### #### ### ## ### #### ### ### ### ## ####. ### ## ## ### ## AVI# #### ## ### #####.
7. 중지하려면 규칙 유지를 선택하고, 계속하려면 규칙 삭제를 선택합니다.
8. 규칙을 비활성화하되 예외 규칙 목록에 유지하려면 취소를 선택합니다.
   다음과 같은 메시지가 나타납니다. # ### #### ### ## ### #### ### ### ### ## ####. ## ## ### ## ### ### #### ## ### ## ### #####.
9. 규칙을 초안으로 이동하고 비활성화하려면규칙 유지를 선택하여 중지하거나 취소를 선택합니다.

애플리케이션 취약성 대응 정정 작업 및 작업 규칙 개요

분석가 및 정정 전문가가 애플리케이션 취약한 항목(AVI)을 구성하고 대량으로 분석할 수 있도록 정정 작업(AVUL)을 구성합니다. AVI가 정정 작업에 자동으로 할당되도록 정정 작업이 구성되는 기준이 구성됩니다. 정정 작업을 사용하여 진행 상황을 모니터링하고 정정 프로세스를 보다 효율적으로 추진할 수 있습니다.

애플리케이션 취약한 항목 및 정정 작업에 대한 지연 수 추적

취약한 항목, 애플리케이션 취약한 항목, 컨테이너 취약한 항목 또는 정정 작업이 지연된 횟수를 추적합니다. `set deferral counts` 예약된 작업은 매일 실행되어 지연 수 열에 두 번 이상 지연된 기록에 대한 수를 게시합니다. 기록은 VR, AVR 및 CVR에 대한 여러 지연 모듈에 표시됩니다.

정정 작업 규칙 이해

정정 작업 규칙을 사용하면 애플리케이션 취약한 항목을 자동으로 그룹화하고 할당하는 방법을 정의할 수 있습니다. 기본 규칙 취약성 은 취약성을 기반으로 AVI를 수집하는 기본 시스템에 포함됩니다. 그러나 AVI에서 액세스할 수 있는 열의 다른 값 집합을 기준으로 그룹화할 수 있습니다. 이러한 값에는 CI(구성 항목), 취약성 항목 등이 포함될 수 있습니다.

활성화 시 사용할 수 있는 애플리케이션에 포함된 취약성 대응 Application Vulnerability Response에 대한 작업 규칙이 있습니다.

조건 작성기를 사용하여 여러 조건을 생성할 수 있습니다. 그룹화 기준 섹션에서 필드 쌍을 설정하면 다른 행이 나타납니다. 최대 6개의 그룹화 기준 선택 항목을 가질 수 있습니다. 그룹 할당을 자동화할 수도 있습니다. 자세한 내용은 AND 내부 필터링 취약성 대응 문서를 참조하십시오에서 애플리케이션 취약 항목 애플리케이션 취약성 대응 자동으로 할당.

예를 들어 애플리케이션 취약한 항목을 구성 항목 또는 제품 모델별로 그룹화할 수 있습니다. 심각도가 낮은 취약성 또는 위험도가 낮은 CI에 대해 하나의 작업 규칙을 가질 수 있습니다. 중요한 서버와 회사를 더 많은 위험에 노출시키는 취약성에 대한 또 다른 작업 규칙이 있을 수 있습니다. 사용할 수 있는 옵션에 대한 자세한 내용은 을 참조하십시오 정정 작업 규칙 생성, 편집 및 삭제 애플리케이션 취약성 대응 .

회사를 더 큰 위험에 노출시키는 애플리케이션 취약한 항목에 대해 다른 규칙 집합을 사용할 수 있습니다. 정정 작업 이름이 정정 작업 규칙 그룹화 기준 값에 추가되어 새 기록에 대한 짧은 설명을 작성합니다.

새 애플리케이션 취약한 항목이 생성되거나, 임포트되거나, 종결된 후 다시 열리면 해당 항목에 대해 규칙이 평가됩니다. AVI는 닫힌 후 다시 열리거나 규칙이 수동으로 다시 적용되지 않는 한 자동으로 한 번만 평가됩니다.

새 AVI 또는 다시 열린 각 AVI에 대해 다음 프로세스가 사용됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 각 정정 작업 규칙에 대해 AVI는 정정 작업 규칙 필터와 비교됩니다.

- 정정 작업 규칙 조건이 일치하는 각 규칙에 대해 규칙은 AVI의 그룹화 기준 선택 항목에서 데이터를 가져옵니다. 그룹 이름과 필드를 빌드합니다. 이 경우 고위험: **QID-32342:** *QID-3242 ##* (이름: 취약성 ID: 취약성 요약)입니다.

  주:
  간단한 설명 필드는 160자로 제한됩니다. 긴 취약성 요약은 잘립니다.

  이 규칙은 AVI와 동일한 할당 그룹에 할당된 일치하는 미해결 정정 작업이 있는지 확인합니다.

  - 작업이 발견되면 AVI가 열림 상태의 기존 작업에 추가됩니다.
  - 열림 상태의 작업을 찾을 수 없는 경우 규칙은 높은 위험: **QID-32342** 작업을 생성하고 AVI와 동일한 할당 그룹에 할당한 다음 정정 작업에 AVI를 배치합니다.

서로 다른 종류의 취약성을 그룹화하도록 둘 이상의 정정 작업 규칙을 정의할 수 있습니다. 각 취약성은 정정 작업에 넣기 전에 정정 작업 규칙 조건과 비교되므로 규칙이 너무 많으면 성능에 영향을 줄 수 있습니다. 조건이 중복 정정 작업의 생성을 방지하는 데 도움이 되도록 작업 규칙을 설정합니다.

기본적으로 정정 작업 규칙은 항목을 그룹화할 때 AVI의 담당 규칙에 의해 설정된 할당 그룹을 사용하고 AVI와 일치하도록 정정 작업을 할당합니다.

기본 작업 규칙의 일부로 이러한 정정 작업의 할당은 할당 규칙 모듈의 규칙에 의해 제어됩니다. 담당 규칙에 대한 자세한 내용은 다음 문서를 참조하십시오 취약성 대응 할당 규칙 개요.

작업 규칙이 양식 또는 목록 뷰에서 삭제되면 해당 규칙에 따라 생성된 모든 미결 작업을 삭제할 수 있습니다. 열림 상태가 아닌 작업은 제외됩니다.

정정 작업 규칙 다시 적용

정정 작업 규칙을 변경하려면 정정 작업 규칙 페이지의 다시 적용 버튼을 사용하여 해당 규칙에 의해 생성된 모든 활성 미결 정정 작업에서 변경된 규칙을 다시 실행합니다. 변경된 규칙에 따라 정정 작업을 자동으로 삭제하고 다시 생성합니다.

다시 적용 은 기존 정정 작업만 확인합니다.

다시 적용을 선택하면 다음 메시지가 표시됩니다. *# ## ## ### ## #### # ### ## ## ### #### ## #####. ## ### ## ## ### ##*되지 않습니다.

정정 작업 생성 및 **AVI** 수동 추가

다른 애플리케이션 정정 작업 기록에서 AVUL(애플리케이션 정정 작업)을 생성하고 애플리케이션 취약한 항목(AVIT)을 수동으로 추가합니다. 자세한 내용은 에서 수동으로 애플리케이션 정정 작업 생성 애플리케이션 취약성 대응 문서를 참조하십시오.

정정 작업 규칙과 **AVI** 생성 및 업데이트

검사의 CI 또는 제품 모델이 알려진 취약성과 연결되면 AVI가 생성됩니다. AVI가 생성되면 일치에 대한 정정 작업 규칙의 조건에 대해 평가됩니다. 기존 정정 작업과 일치하는 항목이 있으면 AVI가 추가됩니다. 일치하는 정정 작업을 찾을 수 없는 경우 AVI에 대해 작업이 하나 만들어집니다.

정정 작업 필터링 조건에 캡처된 속성이 AVI에서 업데이트되거나 변경되면 업데이트된 AVI도 일치에 대한 정정 작업 규칙에 대해 평가됩니다. 기존 정정 작업과 일치하는 항목이 있으면 AVI가 추가됩니다. 일치하는 정정 작업을 찾을 수 없는 경우 AVI에 대해 작업이 하나 만들어집니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

상태 롤업 및 롤다운

정정 작업을 미결로 업데이트하거나 미결에서 조사 중으로 업데이트하면 새 상태가 연결된 모든 AVI로 롤다운됩니다. 상태 롤다운은 상태를 변경한 직후에 발생합니다.

AVI에서 정정 작업으로의 상태 롤업은 작업의 모든 AVI가 연기 됨 또는 종결 고정 상태인 경우에만 발생합니다. 롤업은 15분마다 실행되는 예약된 작업으로 수행됩니다 ***Rollup application vulnerable item values to vulnerability and group*** . 작업이 실행될 때까지 상태가 롤업되지 않습니다. AVI에서 정정 작업으로 상태가 롤업되려면 모든 AVI가 동일한 상태여야 합니다.

정정 작업 규칙 생성, 편집 및 삭제 애플리케이션 취약성 대응

필터 조건에 따라 자동으로 AVI(애플리케이션 취약한 항목)를 AVUL(정정 작업)로 그룹화하는 규칙을 생성할 수 있습니다. 이러한 규칙은 AVI를 가져오거나 수동으로 만들 때 자동으로 그룹화합니다.

시작하기 전에

새 규칙을 만들면 기존 데이터에 적용되지 않습니다. 제출한 후에는 새 가져오기에 대해 실행됩니다.

필요한 역할: sn_vul.app_sec_manager

프로시저

1. 다음으로 이동 모두 〉 애플리케이션 취약성 대응 〉 관리 〉 정정 작업 규칙.
2. 규칙을 열거나 새로 만들기를 선택합니다.
3. 양식의 필드에 내용을 입력하거나 편집합니다.

정정 작업 규칙

필드	설명
이름	작업 규칙의 이름입니다.
활성	작업이 활성 상태인지 여부를 나타냅니다.
설명	규칙에 대한 설명입니다.
대소문자 구분	조건이 대/소문자를 구분하는지 여부를 결정합니다. 주: 기본값은 대/소문자를 구분하지 않습니다.
조건	규칙에 대한 선택적 필터 조건입니다. 기본적으로 (대/소문자 구분 확인란이 선택되지 않음) 작업 규칙 기록 및 양식의 조건 작성기에서 입력하는 검색 텍스트는 대소문자를 구분하지 않습니다. 작업 기록 및 양식에서 대/소문자 구분 검색을 사용하도록 설정할 수 있습니다. 예시 조건은 다음과 같습니다. 취약성 〉 다음과 같음 〉 **VULNENT123451** (알려진 임포트 취약성). 이 취약성이 있는 모든 AVI가 이 조건과 일치합니다.
그룹화 기준(최대 6개의 조건 세트 사용 가능)	
다음 중 애플리케이션 취약한 항목 그룹화	규칙에서 AVI를 그룹화하는 데 사용하는 테이블입니다. 트리에서 요소를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	○ 애플리케이션 취약한 항목 [sn_vuln_vulnerable_item] ○ 애플리케이션 취약한 항목 구성 항목 [cmdb_ci] ○ 애플리케이션 취약한 항목 애플리케이션 취약성[sn_vul_third_party_entry] ○ 애플리케이션 취약한 항목 제품 모델 주: 확장된 테이블을 선택하면 해당 확장된 테이블을 사용하는 애플리케이션 취약한 항목에만 사용 필드가 적용됩니다.
필드 사용	규칙이 AVI를 그룹화하는 데 사용하는 테이블의 필드입니다. 트리에서 조건을 선택합니다. 주: 데이터를 공유하는 모든 AVI가 동일한 정정 작업에 할당되지 않도록 조건별로 그룹을 생성할 수 있습니다. 예를 들어 할당 그룹 및 IP 주소를 사용 필드로 선택하고 여러 AVI가 초기 필터링 조건 취약성과 일치하는 경우 그룹화 기준 섹션에서 사용할 수 있는 여러 옵션을 사용하여 수정을 위해 이러한 AVI를 고유한 할당 그룹에 할당할 수 있습니다. 조건별로 그룹화하면 일부 데이터를 공유하더라도 다른 그룹에 할당할 수 있는 고유한 정정 작업을 유연하게 생성할 수 있습니다.
할당	
정정 작업 할당자	정정 작업을 자동으로 할당하면 취약한 항목을 그룹화하기 위해 그룹화 기준 선택 사항과 함께 할당 선택 항목이 사용됩니다. 필요에 따라 새 작업이 생성되므로 각 AVI는 일치하는 할당 그룹 집합이 있는 작업에 배치됩니다. 이 규칙을 기반으로 생성된 작업의 할당을 자동화하려면 사용 가능한 옵션 중 하나를 선택합니다. ○ 필드별로 그룹화: 그룹화 기준섹션의 필드 값 사용 섹션에서 사용자 그룹 필드를 선택한 경우 드롭다운 메뉴에 표시됩니다. ○ 사용자 그룹: 조회 목록을 사용하여 정적 사용자 그룹을 선택합니다.

양식 또는 목록 뷰에서 규칙을 삭제하는 경우 해당 규칙에 의해 생성된 모든 미해결 정정 작업을 삭제할 수 있습니다. 오픈 상태가 아닌 그룹은 제외됩니다.

4. 새 규칙에 대해 제출 을 선택합니다.
제출을 선택하면 정정 작업 규칙 목록 〔sn_vul_grouping_rule〕에 규칙이 표시됩니다. 다음과 같은 상황에서 규칙이 시작됩니다.
   - 새 AVI가 생성될 때
   - 다시 적용을 선택하는 경우. 재적용을 선택하면 기존 정정 작업에 대한 작업 규칙만 평가할 수 있습니다.
   - 사용자 또는 시스템에 의해 AVI가 업데이트되는 경우.

     AVI가 업데이트되면 작업 규칙이 기존 정정 작업과 일치하는지 평가됩니다. 규칙 검사를 시작하는 몇 가지 일반적인 업데이트는 다음과 같습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 상태가 종결에서 오픈으로 변경되거나 종결에서 조사 중으로 변경되는 경우
- CI(구성 항목)가 변경됩니다.
- 취약성이 변경되었습니다.

시스템은 모든 작업 규칙이 업데이트된 AVI와 일치하는지 확인합니다. 규칙의 조건이 정정 작업의 조건과 일치하면 일치하는 AVI가 할당됩니다.

일치하는 항목이 없으면 새 정정 작업이 만들어집니다.

AVI에서 정정 작업으로의 상태 롤업 및 정정 작업에서 AVI로의 상태 롤다운에 대한 자세한 내용은 다음 문서를 참조하십시오 애플리케이션 취약성 대응 정정 작업 및 작업 규칙 개요.

정정 작업 규칙의 예는 다음 문서를 애플리케이션 취약성 대응 정정 작업 규칙의 예참조하십시오.

5. 작업 규칙을 삭제하려면 정정 작업 규칙 목록에서 규칙을 선택하고 삭제를 선택합니다.
다음 메시지가 표시됩니다. ### ## ## ### ## #### #######. ## ## # n## ## #####.

옵션	설명
확인란이 비활성화되었습니다(기본값).	규칙만 삭제합니다. 열림 상태가 아닌 작업은 제외됩니다.
확인란이 선택되었습니다.	정정 작업 규칙을 삭제할 때 오픈 상태의 정정 작업을 포함합니다. 열림 상태의 규칙 및 모든 정정 작업을 삭제합니다.

6. 하나의 옵션을 선택하고 삭제를 선택합니다.

에서 수동으로 애플리케이션 정정 작업 생성 애플리케이션 취약성 대응

다른 애플리케이션 정정 작업 기록에서 AVUL(애플리케이션 정정 작업)을 생성하고 애플리케이션 취약한 항목(AVIT)을 수동으로 추가합니다.

시작하기 전에
필요한 역할: sn_vul.app_sec_manager

프로시저

1. 다음으로 이동 모두 〉 애플리케이션 취약성 대응 〉 정정 작업 〉 모두.
2. 페이지 오른쪽 상단에서 새로 만들기를 선택합니다.
3. Group Configuration(그룹 구성) 탭에서 Grouping method(그룹화 방법)에 대해 Manual(수동)을 선택합니다.
4. 제출을 선택합니다.
5. 애플리케이션 정정 작업 〔sn_vul_app_vulnerability〕 테이블에서 새 작업 기록(AVUL)을 찾습니다. 기록이 열림 상태로 생성됩니다.
6. 기록을 열고 애플리케이션 취약 항목 관련 목록(편집 또는 추가)을 사용하여 이 그룹에 신규 또는 기존 애플리케이션 취약 항목을 추가합니다.
7. 업데이트를 선택하여 기록을 저장하거나 다른 UI 작업을 선택하여 기록을 다른 상태로 전환합니다.

자동 종결 규칙 생성

자동 종결 규칙을 사용하여 설정한 필터 조건에 따라 이전 AVIT를 자동으로 종결합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_vul.app_manage_auto_close_rules

프로시저

1. 다음으로 이동 모두 〉 애플리케이션 취약성 대응 〉 관리 〉 자동 종결 규칙.
   기본 시스템은 다음과 같은 자동 종결 규칙을 제공합니다.

   마지막으로 검사한 애플리케이션 취약성 지난 90일 이내에 보고되지 않은 취약성은 부실 상태로 전환됩니다.

2. 새로 만들기를 선택하여 새 자동 종결 규칙을 만듭니다.
3. 양식에서 필드에 입력합니다.

필드	값
이름	자동 종결 규칙의 이름입니다.
활성	규칙을 활성화하는 옵션입니다. 활성화되면 필터 기준과 일치하는 탐지를 자동으로 종결합니다.
실행 순서	자동 종결 규칙의 실행을 위한 고유 값입니다. 이 값은 실행 순서를 결정합니다. 기본값은 100입니다.
통합 유형	애플리케이션 취약성 통합
설명	자동 종결 규칙에 대한 설명입니다.
조건	종결해야 하는 탐지를 식별하는 데 사용되는 필터 조건입니다.

4. 제출을 선택합니다.

   규칙 프로세서 자동 종결 예약된 작업은 야간에 실행됩니다. 지정된 조건에 따라 AVIT를 식별하고 일치하는 항목을 부실 상태로 전환합니다. "종결" 상태와 "부실" 상태가 모두 있는 AVIT가 있는 경우 AVIT는 하위 상태가 고정으로 설정된 상태로 종결됩니다.

침투 테스트 구성

침투 테스트 평가 유형에 대한 스프린트 기간 및 예상 작업량을 구성할 수 있습니다. 이는 애플리케이션 소유자를 위한 예약 기능을 제공하여 침투 테스트 평가 요청에 대한 잠정적 시간 범위를 결정하는 데 도움이 됩니다.

시작하기 전에
필요한 역할: 윤리적 해커

이 태스크 정보
윤리적 해킹 팀에 대한 침투 테스트 평가 설정을 구성하면 침투 테스트 평가 요청을 수신하는 그룹 및 연락 창구를 결정하는 데에도 도움이 됩니다.

의 v19.0 취약성 대응부터 를 사용하는 Veracode Vulnerability Integration경우 의 침투 평가 테스트는 Veracode Vulnerability Integration 의 수동 결과 Veracode입니다. 에서 구성하는 애플리케이션 취약성 대응침투 테스트 평가 요청에는 연결되지 않습니다. 의 Veracode침투 테스트 평가에 대한 자세한 내용은 를 Veracode Vulnerability Integration참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 애플리케이션 취약성 대응 〉 관리 〉 침투 테스트 구성.
2. 첫 번째 섹션을 사용하여 할당 그룹을 구성합니다.
3. 양식에서 필드를 채웁니다.

침투 테스트 구성 양식

필드	설명
침투 테스트 팀 사용자 그룹	침투 테스트 평가 요청이 할당된 그룹입니다.
침투 테스트 평가 요청에 대한 기본 할당자	침투 테스트 평가 요청에 대한 연락 창구입니다.

4. 업데이트를 선택합니다.
5. 두 번째 섹션을 사용하여 스프린트를 구성합니다.
   자세한 내용은 침투 테스트를 위한 스프린트 구성 문서를 참조하십시오.
6. 세 번째 섹션을 사용하여 평가 유형을 구성합니다.
   자세한 내용은 침투 테스트에 대한 평가 유형 구성 문서를 참조하십시오.

침투 테스트를 위한 스프린트 구성

침투 테스트 평가를 위한 스프린트 용량을 관리할 수 있도록 윤리적 해킹 팀의 스프린트 기간 및 용량을 구성합니다.

시작하기 전에
필요한 역할: 윤리적 해킹

프로시저

1. 다음으로 이동 모두 〉 애플리케이션 취약성 대응 〉 관리 〉 침투 테스트 구성.
2. 스프린트 구성에 대한 구성 옵션을 선택합니다.
3. 양식에서 필드를 채웁니다.

스프린트 구성 양식

필드	설명
스프린트 기간(일)	스프린트의 일 수입니다.
시작 날짜	스프린트 기간의 시작 날짜입니다.
스프린트 수	스프린트 범위의 시작 및 종료 날짜를 기준으로 생성할 수 있는 스프린트 수입니다.
종료 날짜	스프린트 기간의 종료 날짜입니다.
스프린트 용량	
스프린트 용량(시간)	스프린트의 용량(시간)입니다.

4. 스프린트 생성을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

생성된 스프린트를 보려면 스프린트 보기를 선택합니다.

> **주:**
> 스프린트가 생성되고 진행 중인 후 동일한 기간 동안 스프린트 생성을 선택하면 현재 스프린트가 평소와 같이 완료됩니다. 나머지 스프린트는 업데이트된 스프린트 구성에 따라 다시 계산됩니다.

침투 테스트에 대한 평가 유형 구성

침투 테스트 평가의 각 유형에 대한 예상 작업량을 구성합니다. 이렇게 하면 각 평가 유형에 필요한 작업량을 추정하여 각 스프린트의 용량을 관리할 수 있습니다.

시작하기 전에
필요한 역할: 윤리적 해킹

이 태스크 정보
각 스프린트는 침투 테스트 요청에 할당됩니다. 평가 유형에 대한 예상 작업량에 따라 스프린트의 균형 시간을 반영하도록 시간이 조정됩니다.

프로시저

1. 다음으로 이동 모두 〉 애플리케이션 취약성 대응 〉 관리 〉 침투 테스트 구성.
2. 의 취약성 대응v19.0부터 구성을 선택하여 평가 유형, 애플리케이션 크기 및 예상 작업량을 표시합니다.
3. 옵션: 평가 유형 기록을 선택하여 필요에 따라 필드를 업데이트하거나 새 기록을 생성합니다.

   (Optional) 애플리케이션 크기 값은 테스트 시간과 노력을 보다 정확하게 예측하는 데 도움이 되는 추가 옵션을 제공합니다. 이러한 기록의 시간을 편집하거나 새로 만들기를 선택하여 고유한 조합을 만들 수 있습니다.

   스프린트 용량과 일치하도록 테스트를 예약할 수 있도록 기존 침투 테스트 요청 기록의 값에 대한 평가 유형 및 애플리케이션 크기를 수정할 수 있습니다. 예를 들어 테스트 요청을 작성하는 경우 일부 스프린트가 이미 테스트를 위해 수행되었기 때문에 구성한 스프린트 수가 표시되지 않을 수 있습니다. 스프린트의 예상 작업 시간이 테스트의 유형 및 크기에 필요한 조합과 일치하면 새 요청에 사용할 수 없습니다.

   침투 테스트 스프린트 목록의 기록에 대한 테스트 요청에 할당된 스프린트는 다음 위치에서 볼 수 있습니다. 모두 〉 애플리케이션 취약성 대응 〉 관리 〉 침투 테스트 구성 〉 스프린트 구성. 스프린트 구성에 대한 자세한 내용은 을 참조하십시오 침투 테스트를 위한 스프린트 구성 .

   평가 유형, 애플리케이션 크기, 예상 작업량의 기준값은 다음과 같습니다.

침투 테스트 평가 유형 구성 양식

평가 유형	애플리케이션 크기	예상 작업(시)
집중 테스트	작게	20
집중 테스트	중간	30
집중 테스트	크게	40
집중 테스트	표준	40
재테스트	작게	10
재테스트	중간	15
재테스트	크게	20

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

평가 유형	애플리케이션 크기	예상 작업(시)
재테스트	표준	20
전체 침투 테스트	작게	60
전체 침투 테스트	중간	70
전체 침투 테스트	크게	80
전체 침투 테스트	표준	80

4. 업데이트를 선택하여 변경 내용을 저장하거나 새 기록을 위해 제출을 선택합니다.
5. v19.0 이전에는 평가 유형 구성에 대한 구성 옵션을 선택합니다.
6. 필요에 따라 평가 유형에 대한 값을 업데이트합니다.
   기준값은 다음과 같습니다.

   침투 테스트 평가 유형 구성 양식

평가 유형	예상 작업(시)
집중 테스트	40
재테스트	20
전체 침투 테스트	80

7. 변경 내용을 저장합니다.

다른 애플리케이션과 애플리케이션 취약성 대응의 통합

취약성 대응 에는 외부 공급업체 통합에 대한 지원이 포함됩니다.

외부 공급업체 통합

애플리케이션 취약성 통합은 외부 시스템 및 벤더로부터 데이터를 검색하여 인스턴스의 애플리케이션 취약성 데이터를 보강하는 데 도움이 됩니다. 지원되는 통합에 대한 자세한 내용은 다음 개요 주제를 참조하십시오.

- Fortify 취약성 통합
- GitHub 애플리케이션 취약성 통합
- Invicti 취약성 통합
- Veracode Vulnerability Integration
- Vulnerability Response Integration with Black Duck
- Application Vulnerability Response의 취약성 수동 수집
- Atlassian Jira 통합

> **중요사항:**
> 취약성 관리자 작업 공간에서 목록 작업 및 양식 작업을 사용하여 Agile 문제를 수동으로 생성하여 AVIT 및 RT의 정정을 추적할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

에서 다중 소스 통합은 지원되지 애플리케이션 취약성 대응않습니다. 타사 통합은 별도로 처리됩니다. 사용자 환경에서 둘 이상의 외부 공급업체 통합 애플리케이션을 사용하는 경우 통합 전반에 걸쳐 애플리케이션 취약한 항목(AVI) 중복 제거가 없습니다.

다음 테이블에는 취약성을 임포트하고 취약한 항목을 생성하기 위해 만든 통합 및 파트너가 제공하는 ServiceNow# 통합 목록이 애플리케이션 취약성 대응 나와 있습니다.

Vulnerability Response - 인프라 통합

벤더	벤더 제품	통합 요약	스토어 링크	주요 기능	작성자
Veracode	Veracode 동적 분석	임포트 테스트, 정책, 결과 DAST 결과 임포트 SAST 결과 임포트 SCA 결과 임포트			ServiceNow#
Qualys WAS					ServiceNow#
					ServiceNow#
					파트너
					ServiceNow#
					ServiceNow#
					파트너
					파트너
					파트너
					파트너
					파트너
					파트너
					파트너
					파트너
					파트너
					파트너
					파트너
					파트너
					파트너
					파트너
					파트너
					파트너
					파트너

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약성 대응 애플리케이션 및 **CSDM** 테이블

, 취약성 대응애플리케이션 취약성 대응, 타사 취약성 통합 및 소프트웨어 자재 명세서 애플리케이션은 테이블을 관리(데이터 기여) CSDM 합니다. 이러한 애플리케이션은 다른 애플리케이션이 생성하는 테이블의 데이터 CSDM 도 사용합니다. 따라서 여러 ServiceNow 제품이 이러한 보안 운영 애플리케이션의 이점을 누리고 가치를 더합니다. 자세한 내용은 취약성 대응 애플리케이션 및 CSDM 테이블 문서를 참조하십시오.

통합에 대한 추가 참고 사항

통합 실행 중에 여러 프로세스가 생성되고 데이터가 페이지 형식으로 수신됩니다. 각 프로세스에는 페이지에 첨부된 데이터가 있는 하나 이상의 임포트 큐 항목이 포함될 수 있습니다. 이러한 항목은 1시간의 시간 제한 내에 데이터를 처리해야 합니다. 그러나 페이로드 크기가 크면 처리 시간이 1시간을 초과하거나 중단되어 통합 시간 제한 오류가 발생할 수 있습니다. 통합은 시간 초과 오류에도 불구하고 데이터를 계속 처리합니다. 이러한 잘못된 통신을 피하기 위해 버전 18.2.4 애플리케이션 취약성 대응부터 큐가 활성 상태이고 데이터를 처리하는지 여부를 나타내기 위해 타임스탬프(하트비트)가 주기적으로 전송됩니다. 임포트 큐 항목 페이지의 처리된 마지막 기록 필드는 임포트 큐가 생성하거나 업데이트하는 기록 수에 따라 업데이트됩니다. 임포트 큐 항목이 1시간의 시간 제한을 초과하는 경우, 시스템은 마지막으로 처리된 기록 필드를 검사하여 1시간보다 오래되었는지도 확인합니다. 이 경우 이는 임포트 큐 항목이 고착되었음을 나타내며 처리 시 더 이상의 지연을 방지하기 위해 시간 초과됩니다.

주:
마지막으로 처리된 기록 필드는 다음 시스템 속성에 정의된 내용에 따라 업데이트됩니다.

- *sn_sec_cmn.record_threshold_heartbeat*: 하트비트(타임스탬프)가 임포트 큐 항목으로 전송된 후 처리된 기록 수를 정의합니다.
- *sn_sec_cmn.maximum_heartbeat_delay*: 임포트 큐 항목을 시간 초과해야 하는 시간을 정의합니다.

취약성 애플리케이션 취약성 대응 통합은 예약에 따라 실행되도록 구성됩니다. 그러나 필요한 경우 수동으로 실행할 수 있습니다.

필요한 역할: sn_vul.app_read_integrations

1. 다음으로 이동 모두 〉 애플리케이션 취약성 대응 〉 관리 〉 통합.
2. 실행할 통합에 대한 기록을 엽니다.
3. 지금 실행을 클릭합니다.

Vulnerability Response Integration with Black Duck

와의 Vulnerability Response Integration with Black Duck 통합은 취약성 대응 Black Duck SCA(소프트웨어 컴포지션 분석) 도구에서 임포트한 데이터를 사용하여 코드 결함의 영향과 우선순위를 결정하는 데 도움을 줍니다.

통합 개요

를 Vulnerability Response Integration with Black Duck사용하여 SCA를 수집하고 해당 데이터를 ServiceNow AI Platform. 의 v22.0.5 부터 취약성 대응SCA 취약성 데이터를 인스턴스로 임포트하여 소프트웨어 애플리케이션의 취약성을 식별할 수 있습니다. 자세한 내용은 소프트웨어 자재 명세서 탐색 문서를 참조하십시오.

공유 API는 SCA 데이터를 수집합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
각 통합 기록에는 구성된 실행 사용자가 있습니다. 이 사용자의 기본값은 VR 시스템입니다. 이 값을 변경하지 마십시오.

매일 예약된 작업은 나열된 순서대로 통합을 자동으로 호출합니다. 예약된 개별 작업을 수동으로 실행할 수도 있습니다. 예약된 작업은 인스턴스를 다른 취약성 관리 시스템과 동기화된 상태로 유지하여 취약성 정정 수명주기를 단순화합니다.

사용 가능한 버전

Black Duck 통합 사용 가능한 버전

릴리스 버전	릴리스 정보
Vulnerability Response Integration with Black Duck 1.0.5	Application Vulnerability Response release notes

사용자 그룹 및 역할

관리자 Vulnerability Response Integration with Black Duck 역할의 사용자가 설치하고 App-Sec 관리자 그룹의 구성원이 구성합니다. 자세한 내용은 애플리케이션 취약성 대응 사용자 그룹 및 역할 문서를 참조하십시오.

통합 실행 상태는 다음을 참조하십시오. Vulnerability Response Integration with Black Duck 임포트 실행 상태 보기

타사 취약성의 데이터를 보려면 을 참조하십시오 취약성 라이브러리 보기.

다음에 대한 사전 통합 작업 준비 **Vulnerability Response Integration with Black Duck**

통합이 성공할 수 있도록 에 Vulnerability Response Integration with Black Duck 대한 사전 통합 작업을 계획하고 실행합니다. 여기서는 Vulnerability Response Integration with Black Duck 사용자가 Black Duck SCA(소프트웨어 구성 분석) 애플리케이션 및 API에 익숙하다고 가정합니다.

시작하기 전에

를 Vulnerability Response Integration with Black Duck설치하고 구성하기 전에 에서 사용되는 애플리케이션 취약성 대응CWE(Common Weakness Enumeration) 통합을 실행하고 설치해야 합니다. CWE 통합은 기본적으로 와 함께 취약성 대응 설치됩니다.

주:
NVD(NIST 취약성 데이터베이스) 데이터는 Black Duck 애플리케이션 취약성 통합을 설치하는 데 필요하지 않지만 있으면 유용할 것입니다. NVD에 대한 자세한 내용은 문서를 참조하십시오 NVD 및 CWE 통합을 통해 데이터를 임포트하고 외부 공급업체 라이브러리를 관리합니다.

각 통합 기록에는 구성된 실행 사용자가 있습니다. 이 사용자의 기본값은 VR입니다. 체계. 이 값을 변경하지 마십시오.

필요한 역할: App-Sec 관리자 그룹

이 태스크 정보

주:
통합을 실행하기 전에 요구 사항에 따라 필요한 구성을 변경합니다.

임포트할 것으로 예상되는 애플리케이션 취약한 항목 수를 기준으로 인스턴스 크기를 확인합니다. 인스턴스 크기가 작으면 로드 시간이 길어질 수 있습니다. 인스턴스 크기를 모르는 경우 에 문의하십시오 고객 서비스 및 지원.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Vulnerability Response Integration with Black Duck API URL과 API 토큰이 필요합니다.

프로시저

API 토큰 및 키 자격 증명을 생성합니다.

a. Black Duck 플랫폼에 로그인합니다.

b. 사용자 계정 메뉴로 이동하여 **API** 자격 증명을 선택합니다.

c. API 자격 증명 생성을 선택합니다.

d. 나중에 사용할 수 있도록 자격 증명을 기록합니다.

설치 **ServiceNow Vulnerability Response Integration with Black Duck**

인스턴스에서 통합을 실행하기 전에 Black Duck 소프트웨어 구성 분석(SCA) 도구가 와 제대로 통합 애플리케이션 취약성 대응되도록 설치 및 구성 단계를 완료해야 합니다.

시작하기 전에
설치하기 전에 다음 설정 검사 목록을 완료합니다. Black Duck SCA(소프트웨어 컴퍼지션 분석) 도구가 .애플리케이션 취약성 대응

> **주:**
> 이 프로세스는 프로덕션 인스턴스에 다운로드된 애플리케이션에만 적용됩니다. 애플리케이션을 비프로덕션 또는 개발 인스턴스에 다운로드하는 경우에는 권리를 얻을 필요가 없습니다. 로 애플리케이션 활성화 ServiceNow Store계속 진행합니다.

작업 설정

작업 설정	설명
애플리케이션이 설치되고 활성화되었는지 취약성 대응 확인합니다.	이 애플리케이션이 활성화되었는지 확인하려면 다음으로 이동하십시오. 구독 관리 〉 구독 인스턴스에 있습니다. 목록에 조직이 구매한 구독이 표시됩니다. 애플리케이션이 설치 및 활성화되지 않은 경우 문서를 참조하십시오 취약성 대응 설치.
인스턴스에 필요한 ServiceNow 역할이 있는지 확인합니다.	예상 결과의 설치, 구성 및 검증에 필요한 역할은 다음과 같습니다. • 아직 할당되지 않은 경우 관리자 역할을 가진 사용자가 애플리케이션을 설치하고 사용자를 App-Sec 관리자 그룹에 할당합니다. 그룹 역할에 대한 자세한 내용은 다음 문서를 참조하십시오 애플리케이션 취약성 대응 사용자 그룹 및 역할. • App-Sec 관리자 그룹은 구성을 감독하고 예상 결과를 검증합니다.

필요한 역할: 관리자

이 태스크 정보
이 SCA 도구는 별도의 구독으로 사용할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 설치 Vulnerability Response Integration with Black Duck 하려는 인스턴스에 로그인합니다.
2. ServiceNow Store로 이동합니다.
3. ServiceNow Store에서 Vulnerability Response Integration with the Black Duck 애플리케이션을 검색합니다.
4. 애플리케이션 타일을 선택합니다.
   설치 중인 애플리케이션에 대한 상세 정보가 표시됩니다.

   주:
   해당하는 경우 다른 요구 사항 및 종속성 섹션을 읽어보십시오.

5. 요청 앱을 선택하고 로그인 자격 증명을 입력합니다Now Support.
6. 가져오기를 선택합니다.
7. 인스턴스 이름과 인스턴스의 이유를 입력하고 인스턴스 확인을 선택합니다.
8. 요청을 선택합니다.
   자세한 설치 지침이 포함된 이메일을 받게 됩니다.
9. 다음으로 이동 시스템 애플리케이션 〉 애플리케이션.
10. 응용 프로그램을 찾아서 선택하고 설치를 선택합니다.
    애플리케이션이 인스턴스에 자동으로 설치됩니다.

다음에 수행할 작업
사용자 환경에 맞게 구성합니다 Vulnerability Response Integration with Black Duck . Vulnerability Response Integration with Black Duck 구성 문서를 참조하십시오.

Vulnerability Response Integration with Black Duck 구성

인스턴스에서 실행하기 Vulnerability Response Integration with Black Duck 전에 Black Duck SCA(소프트웨어 컴포지션 분석) 도구가 애플리케이션과 제대로 통합 애플리케이션 취약성 대응 되도록 설치 및 구성 단계를 완료해야 합니다.

시작하기 전에
필요한 역할: App-Sec 관리자 사용자 그룹

이 태스크 정보
별도의 Vulnerability Response Integration with Black Duck 구독으로 사용할 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 **Blackduck** 취약성 통합 〉 구성.
2. 기본 인증 유형을 선택합니다.
   기본 인증에는 온프레미스에 있는 인스턴스에 대한 a MID 서버 가 필요합니다. Black Duck 계정에서 기본 인증에 필요한 API 토큰을 생성할 수 있습니다.
3. 양식에서 필드를 채웁니다.
   기본 인증

필드	설명
API URL	엔터프라이즈 또는 온프레미스 인스턴스에 대한 Black Duck API URL입니다. 온-프레미스 인스턴스는 Black Duck 끝점 URL입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
API 토큰	Black Duck 콘솔에서 생성한 토큰입니다.
MID 서버	MID 서버 이는 기본 인증을 위해 온 프레미스에 있는 인스턴스에 필요합니다.
SCA 포함	기본적으로 포함된 SCA(소프트웨어 구성 분석) 검사의 취약성입니다. SCA 검사는 오픈 소스 구성 요소의 취약성을 식별합니다.
ServiceNow에서 긍정 오류를 관리하는 옵션을 선택합니다.	ServiceNow 긍정 오류 관리 옵션. 소스 상태가 긍정 오류 또는 잠재 긍정 오류로 표시된 임포트한 AVI(애플리케이션 취약한 항목)를 분류하려면 이 옵션을 활성화된 상태로 둡니다. 일반적으로 인스턴스에서 종결됨 상태로 매핑되는 이러한 소스 상태를 가진 AVI는 **Open**에 매핑됩니다. AVI 기록에서 긍정 오류를 요청할 수 있습니다. ○ 스캐너에서 임포트한 소스 상태를 유지하려면 옵션 중 하나 또는 둘 다를 비활성화합니다. ○ 비활성화하면 예외 요청 및 가양성 작업이 AVI에 표시되지 않습니다.
통합 인스턴스	데이터를 임포트하는 데 사용하는 인스턴스입니다.

4. 자격 증명 저장 및 테스트를 선택합니다.
5. 다른 통합을 실행하기 전에 **Black Duck** 프로젝트 목록 통합을 실행하십시오.
   Black Duck 애플리케이션 목록 통합 및 Black Duck 애플리케이션 취약한 항목 통합과 같은 다른 Black Duck 통합은 프로젝트 목록 통합에서 임포트한 현재 프로젝트 및 애플리케이션 데이터에 따라 달라집니다.

Vulnerability Response Integration with Black Duck 임포트 실행 상태 보기

취약성 통합 실행 관련 목록을 보면서 통합 실행의 성공을 확인하고, 문제를 찾고, 정정 결정을 확인합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 〉 **Blackduck** 취약성 통합 〉 통합.
2. 통합을 선택합니다.
3. 취약성 통합 실행 관련 목록을 선택합니다.
4. 모든 임포트가 성공했는지 확인합니다.
   문제 해결:

   실행 실패의 가장 일반적인 원인은 다음과 같습니다.

   ○ 네트워크 중단.

   ○ 변환 중에 데이터가 손상되는 데이터 전송 문제입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이러한 조건이 발생하면 지금 실행을 선택하고 통합을 다시 실행합니다.

5. 통합 목록으로 이동하고 Black Duck 통합 기록을 선택하여 임포트한 리포지토리를 봅니다.
6. 취약성 통합 실행 관련 목록을 선택하고 기록을 엽니다.

에 대한 데이터 변환 **Vulnerability Response Integration with Black Duck**

임포트할 데이터를 식별한 후에는 데이터 Vulnerability Response Integration with Black Duck소스에서 데이터가 검색되고 데이터 소스 세트를 통해 처리되어 인스턴스에서 변환됩니다.

Vulnerability Response Integration with Black Duck

API의 데이터는 먼저 Black Duck AppVul 항목 임포트 [sn_vul_blackduck_appvul_item_import] 테이블에 로드되고 Black Duck AppVul 항목 변환을 사용하여 임포트된 정보를 변환합니다.

이 변환 맵에 액세스하려면 다음으로 이동하십시오. 시스템 임포트 세트 〉 변환 맵 을 클릭하고 **Black Duck AppVul Item Transform**을 검색합니다. 다음 표에는 통합별 변환 맵 필드가 나열되어 있습니다.

Black Duck AppVul 항목 변환 맵 필드

소스 필드	대상 필드	설명
app_id	source_app_id	애플리케이션 ID입니다.
문제 ID	source_avit_id	AVIT ID입니다.
app_name	app_name	애플리케이션 이름입니다.
버전	app_version	애플리케이션 버전입니다.
build_id	source_scan_id	애플리케이션의 빌드 ID입니다.
account_id	account_id	계정 ID
sandbox_id	sandbox_id	샌드박스 ID입니다.
last_update_time	last_scan_date	마지막 업데이트 시간입니다.
app_name + last_scan_date	scan_summary_name	검사 요약입니다.
life_cycle_stage	source_sdlc_status	소스 SDLC 상태입니다.
수준	source_severity	소스 심각도
category_name	범주	범주입니다.
source_severity	source_severity	소스 심각도
category_id + " CWE-" + cweId	source_entry_id	소스 항목 ID입니다.
source_vulnerability_summary	source_vulnerability_summary	소스 취약성 요약.
source_recommendation	source_recommendation	소스 권장 사항.
설명	설명	소스의 설명입니다.
설명	source_vulnerability_explanation	소스 취약성 설명.
mitigation_status_desc	source_mitigation_status	소스 완화 상태입니다.
remediation_status	source_remediation_status	소스 정정 상태입니다.
라인	line_number	결함이 발견된 선입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Black Duck AppVul 항목 변환 맵 필드

소스 필드	대상 필드	설명
모듈	application_module	애플리케이션 모듈입니다.
소스 파일	source_notes	출처 메모.
affects_policy_compliance	complies_with_policy	소스 정보가 true 또는 false인지에 따라 값이 Yes 또는 No가 될 수 있습니다.
소스 파일 경로 + 소스 파일	위치	정적 결함인 위치 매핑입니다.
URL	위치	동적 결함에 대한 위치 매핑.
범위, 유형, exploitLevel	source_additional_info	정적 결함에 대한 소스의 값으로 채워진 이름 값 필드입니다.

다음 테이블에는 변환 프로세스 중에 실행되는 변환 스크립트가 나와 있습니다.

Black Duck 변환 맵 스크립트 타이밍 및 목적

Black Duck 변환 맵 스크립트

스크립트가 실행될 때	목적
onStart (임포트 세트에서 변환을 생성한 경우)	기록을 처리하고 생성, 업데이트 또는 변경되지 않은 엔터티 수와 이 통합의 일부로 임포트되는 엔터티 수를 업데이트하는 데 사용되는 스크립트입니다. 이 스크립트는 내부용이며 수정하거나 삭제하면 안 됩니다.
onBefore (임포트 세트가 변환을 완료하기 전)	잘못되어 무시해야 하는 기록의 동작을 정의하는 데 사용되는 스크립트입니다. 또한 기록 처리를 위한 전역 객체를 정의하는 데 사용됩니다. 이 스크립트는 내부용이며 수정하거나 삭제하면 안 됩니다.

Black Duck 통합 상태 매핑

다음 테이블에는 Black Duck 취약성 통합의 소스 상태와 인스턴스의 대상 상태가 나와 있습니다.

Black Duck 소스 상태 및 해당 **ServiceNow AI Platform** 상태

Black Duck 소스 상태	소스 상태 설명	의 대상 상태 ServiceNow AI Platform
신규	취약성은 이 구성요소 버전에 영향을 미칩니다.	오픈
검토 필요	취약성이 이 구성요소 버전에 영향을 주는지 확인할 수 없습니다.	오픈
정정 필요	이 버전에 대한 정정이 필요합니다.	오픈
정정 완료	이 취약성에 대한 정정이 완료되었습니다.	종결됨

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Black Duck 소스 상태 및 해당 **ServiceNow AI Platform** 상태

Black Duck 소스 상태	소스 상태 설명	의 대상 상태 ServiceNow AI Platform
완화	취약성이 완화되었습니다.	종결됨
패치	취약성에 패치가 적용되었습니다.	종결됨
무시됨	취약성은 무시되었습니다.	종결됨

Black Duck 통합 인스턴스에서 프로젝트 정보 임포트

Black Duck 통합 인스턴스에서 프로젝트 정보를 임포트하여 취약성 통합이 순차적으로 실행되도록 합니다. 통합에 성공하면 애플리케이션 취약한 항목(AVI)을 식별하고 수집할 수 있습니다.

시작하기 전에

필요한 역할: App-Sec 관리자 그룹

이 태스크 정보

〔sn_vul_blackduck_project〕 Black Duck 프로젝트 테이블에서 모든 프로젝트 정보를 Vulnerability Response Integration with Black Duck 임포트할 수 있습니다. 다른 버전의 프로젝트를 쿼리하는 데 필요한 모든 필수 속성(예: 프로젝트 GUID)은 〔sn_vul_blackduck_project〕 Black Duck projects 테이블에 캡처됩니다.

프로시저

1. 다음으로 이동 모두 〉 **Blackduck** 취약성 통합 〉 통합.
2. 통합을 선택합니다.
   예를 들어 **Black Duck** 프로젝트 목록 통합을 선택할 수 있습니다.
3. 지금 실행을 선택합니다.

   > **주:**
   > 각각 Vulnerability Response Integration with Black Duck 은 가장 완전한 데이터 검색을 제공하기 위한 것입니다. 이러한 통합을 순서대로 실행하지 않으면 불완전한 데이터와 요구 ServiceNow 사항 및 Application Vulnerability Response 전문 지식이 발생할 수 있습니다.

   임포트가 완료되면 [sn_vul_blackduck_project] Black Duck 프로젝트 테이블에서 프로젝트 상세 정보를 볼 수 있습니다.
4. 통합 실행 상태에 대해서는 다음 문서를 참조하십시오 Vulnerability Response Integration with Black Duck 임포트 실행 상태 보기.
5. 옵션: 다른 통합 매개변수를 수정하려면 통합 인스턴스로 이동해야 합니다.

검색된 애플리케이션 테이블로 프로젝트 버전 임포트 **Vulnerability Response Integration with Black Duck**

Black Duck 취약성 통합이 순차적으로 실행되도록 Black Duck 프로젝트 버전과 취약성 대응 통합을 검색된 애플리케이션 [sn_vul_release] 테이블로 임포트합니다. 통합에 성공하면 애플리케이션 취약한 항목(AVI)을 식별하고 수집할 수 있습니다.

시작하기 전에

필요한 역할: App-Sec 관리자 그룹

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보
검색된 애플리케이션 [sn_vul_release] 테이블에서 임포트 Vulnerability Response Integration with Black Duck 한 프로젝트의 다른 버전(Black Duck 프로젝트 테이블의 상세 정보 참조)을 모두 추가하고 볼 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 **Blackduck** 취약성 통합 〉 통합 .
2. 통합을 선택합니다.
   예를 들어 **Black Duck** 애플리케이션 목록 통합을 선택할 수 있습니다.
3. 지금 실행을 선택합니다.

   주:
   통합의 각 프로젝트 버전은 가장 완전한 데이터 검색을 제공하기 위한 것입니다. 이러한 통합을 순서대로 실행하지 않으면 불완전한 데이터가 생성될 수 있으며 ServiceNow 및 Application Vulnerability Response 전문 지식이 필요합니다.

   임포트가 완료되면 검색된 애플리케이션 [sn_vul_release] 테이블에서 프로젝트의 다양한 버전을 볼 수 있습니다. CI 조회 규칙을 사용하는 경우 검색된 애플리케이션은 구성 항목 [cmdb_ci] 테이블에 연결됩니다.
4. 통합 실행의 상태를 확인합니다.
   자세한 내용은 Vulnerability Response Integration with Black Duck 임포트 실행 상태 보기 문서를 참조하십시오.

다음에서 애플리케이션 취약 항목 임포트 **Vulnerability Response Integration with Black Duck**

통합이 순차적으로 실행되도록 Black Duck과의 취약성 대응 통합에서 애플리케이션 취약한 항목(AVI)을 임포트합니다. 통합에 성공하면 AVI를 식별하고 수집할 수 있습니다.

시작하기 전에
필요한 역할: App-Sec 관리자 그룹

이 태스크 정보
에서 Vulnerability Response Integration with Black Duck검사 결과를 보고, 인스턴스에 AVI를 삽입하고, 타사 취약성 데이터를 보강할 수 있습니다. 기본적으로 스캐너 기록이 종결 상태인 경우 AVI가 생성되지 않습니다. 속성 sn_vul_create_closed 사용하여 기존 AVI를 제어할 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 **Black Duck** 취약성 통합 〉 통합.
2. 통합을 선택합니다.
   예를 들어 **Black Duck** 애플리케이션 취약한 항목 통합을 선택할 수 있습니다.
3. 지금 실행을 선택합니다.

   주:
   가장 Vulnerability Response Integration with Black Duck 완벽한 데이터 검색을 제공하기 위한 것입니다. 이러한 통합을 순서대로 실행하지 않으면 불완전한 데이터와 요구 ServiceNow 사항 및 애플리케이션 취약성 대응 전문 지식이 발생할 수 있습니다.

   에서 Vulnerability Response Integration with Black Duck모든 SCA 취약성을 임포트한 후 AVI 및 타사 취약성 데이터를 볼 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

에 대한 임포트 시간 설정 **Vulnerability Response Integration with Black Duck**

임포트의 Vulnerability Response Integration with Black Duck 시작 시간을 설정합니다. 더 나은 성능과 더 빠른 임포트 실행을 얻을 수 있도록 통합을 미리 설정할 수 있습니다.

시작하기 전에
필요한 역할: App-Sec 관리자 그룹

이 태스크 정보
초기 임포트 후 Black Duck 취약성 통합은 실행될 때마다 전체 임포트를 수행합니다.

프로시저
1. 다음으로 이동 모두 〉 **Black Duck** 취약성 통합 〉 통합.
2. 통합을 선택합니다.
3. 새 시작 시간을 설정합니다.
   시간은 현지 시간의 시간으로 계산됩니다. Black Duck 애플리케이션 목록 통합 임포트의 기본 시간은 00:00:00입니다. 다른 통합은 요청 시 및 체인으로 연결되어 있으므로 Black Duck 애플리케이션 목록 통합 후 실행되는 시퀀스를 따릅니다. 시작 시간을 변경하려면 고급 ServiceNow 및 애플리케이션 취약성 관리 전문 지식이 필요합니다.
4. 업데이트를 선택합니다.
   새 시간은 다음으로 예약된 임포트에 사용됩니다.

종결된 **Black Duck** 애플리케이션 취약 항목 포함

종결된 애플리케이션 취약한 항목(AVI)은 기본적으로 통합 임포트 중에 생성되지 않으므로 Black Duck 취약한 항목 통합 임포트 중에 포함합니다. 만들려면 시스템 속성을 변경해야 합니다.

시작하기 전에
이(가 Vulnerability Response Integration with Black Duck) 설치되어 실행 중인지 확인하십시오.

필요한 역할: 관리자

프로시저
1. 탐색 필터에 sys_properties.list를 입력합니다.
2. 목록의 이름 필드에 sn_vul.create_closed를 입력합니다.
3. 값 필드를 두 번 클릭하고 **True**로 설정합니다.
4. 녹색 확인 표시 아이콘을 선택하여 저장합니다. 녹색
   다음 Black Duck 임포트에서 종결됨 상태의 기록은 애플리케이션 취약성 대응.

Fortify 취약성 통합

Fortify 취약성 통합 에서는 제품에서 Fortify 임포트한 데이터를 사용하여 코드 내 결함의 영향과 우선순위를 파악하는 데 도움을 줍니다.

Fortify 취약성 통합

Fortify 제품은 스캐너 데이터를 수집하고 해당 데이터를 ServiceNow AI Platform#. 타사 취약성을 매핑하는 기능과 취약성 대응 쉽게 통합되어 ServiceNow# 애플리케이션 취약성 대응 인스턴스의 데이터를 보강합니다.

각 통합 기록에 대해 구성된 실행 사용자가 있습니다. 이 사용자의 기본값은 VR입니다. 시스템. 이 값은 변경하지 마십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예약된 작업은 매일 통합을 자동으로 호출합니다. 모든 통합이 활성화되면 순서대로 실행되도록 연결됩니다. 예약된 개별 작업을 수동으로 실행할 수도 있습니다. 예약된 작업은 인스턴스를 다른 취약성 관리 시스템과 동기화된 상태로 유지하여 취약성 정정 수명주기를 단순화합니다.

사용 가능한 버전

릴리스 버전	릴리스 정보
와 Vulnerability Response 통합 Fortify v2.4 Fortify v2.3 Fortify v2.2 Fortify v2.1	Application Vulnerability Response release notes 호환성 정보는 KB0856498 Vulnerability Response 호환성 매트릭스 및 릴리스 스키마 변경을 참조하십시오.

Fortify 취약성 통합

을(를 Fortify 취약성 통합) 보려면 다음으로 이동하십시오. **Fortify** 취약성 통합 〉 통합.

기본 시스템에는 다음과 같은 통합이 포함됩니다. 이러한 통합은 기본적으로 모두 활성화되어 있지는 않습니다.

초기 실행 후에는 매일 예약된 작업이 연결되어 통합을 순서대로 자동으로 실행합니다. 예약된 개별 작업을 수동으로 실행할 수도 있습니다. 예약된 작업은 인스턴스를 다른 취약성 관리 시스템과 동기화된 상태로 유지하여 취약성 정정 수명주기를 단순화합니다.

Fortify 취약성 통합

통합	설명
Fortify 요청 시 애플리케이션 목록 통합	애플리케이션 스캐너 데이터(취약성, 메타데이터)를 검색하고 Fortify 외부 공급업체 애플리케이션 데이터를 보강합니다. 이 통합은 매일 00:00:00에 실행되도록 설정됩니다. 이 옵션은 기본적으로 활성화됩니다.
Fortify 요청 시 검사 요약 통합	에서 스캔 기록을 조회합니다 Fortify. 이 통합은 활성화 시 요청 시 애플리케이션 목록 통합에 Fortify 따라 실행되도록 연결됩니다. 기본적으로 비활성 상태입니다.
Fortify 요청 시 애플리케이션 취약한 항목 통합	에서 Fortify검사 결과를 검색하고, AVIT를 삽입하고, 외부 공급업체 취약성 데이터를 보강합니다. 스캐너 기록이 종결 상태인 경우 AVIT가 생성되지 않습니다. 기존 AVIT는 여전히 업데이트됩니다. v2.3부터 총 처리 시간, 사전 및 사후 통합 실행 프로세스의 평균 시간과 같은 상세 정보, 애플리케이션 취약한 항목 통합에 대한 통합 실행 기록에 대한 보고서를 볼 수 있습니다. 이 통합은 활성화될 때 요청 시 검사 요약 통합 다음에 Fortify 실행되도록 연결됩니다. 기본적으로 비활성 상태입니다.

통합 실행 상태는 문서를 참조하십시오 Fortify 취약성 통합 임포트 실행 상태 보기.

외부 공급업체 취약성의 데이터를 보려면 을 참조하십시오 취약성 라이브러리 보기.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

준비 중 **Fortify** 취약성 통합

성공 Fortify 취약성 통합 하려면 통합 전 작업의 계획과 실행이 필요합니다. 다음 작업을 수행하여 통합을 준비합니다. 여기서는 Fortify 취약성 통합 사용자가 제품과 API에 Fortify 익숙하다고 가정합니다.

시작하기 전에
CWE(Common Weakness Enumeration) 통합도 에서 애플리케이션 취약성 대응 사용되며 를 설치 및 구성 Fortify 취약성 통합하기 전에 실행해야 합니다.

주:
NVD(NIST 취약성 데이터베이스) 데이터는 설치에 Fortify 취약성 통합필요하지 않지만 보강 기능을 제공하므로 있으면 유용합니다.

NVD에 대한 자세한 내용은 문서를 참조하십시오 NVD 및 CWE 통합을 통해 데이터를 임포트하고 외부 공급업체 라이브러리를 관리합니다.

각 통합 기록에 대해 구성된 실행 사용자가 있습니다. 이 사용자의 기본값은 VR입니다. 시스템. 이 값은 변경하지 마십시오.

필요한 역할: App-Sec 관리자

이 태스크 정보
주:
통합을 실행하기 전에 요구 사항에 따라 필요한 구성을 변경합니다.

임포트하려는 것으로 예상되는 애플리케이션 취약한 항목 수에 따라 인스턴스 크기를 확인합니다. 인스턴스 크기가 작으면 로드 시간이 길어질 수 있습니다. 인스턴스 크기를 모르는 경우 에 문의하십시오 고객 서비스 및 지원.

요청 Fortify 취약성 통합 시 계정에서 사용할 수 Fortify 있는 API 키, API 비밀 및 API 루트 URL이 필요합니다.

프로시저

API 비밀 키를 작성하려면 다음을 수행합니다.

a. 온디맨드 Fortify 포털에 로그인합니다.

b. 다음으로 이동 모두 〉 관리 〉 설정 〉 **API**.

c. ServiceNow를 애플리케이션으로 추가합니다.

d. 새 비밀을 클릭하여 API 비밀을 작성합니다.

e. 나중에 사용할 수 있도록 API 비밀을 기록합니다.

ServiceNow® 와 **Vulnerability Response** 통합 설치**Fortify**

인스턴스에서 통합을 실행하기 전에 설치 및 구성 단계를 완료 Fortify 하여 제품이 .애플리케이션 취약성 대응 이 애플리케이션은 별도의 구독으로 사용할 수 있습니다.

시작하기 전에
설치하기 전에 다음 설정 검사 목록을 완료합니다. 이러한 설정 작업은 원활한 설치 및 구성을 위해 필요합니다.

주:
이 프로세스는 프로덕션 인스턴스에 다운로드된 애플리케이션에만 적용됩니다. 애플리케이션을 비프로덕션 또는 개발 인스턴스에 다운로드하는 경우에는 권리를 얻을 필요가 없습니다. 로 애플리케이션 활성화 ServiceNow Store계속 진행합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업 설정	설명
애플리케이션이 설치되고 활성화되었는지 취약성 대응 확인합니다.	이 애플리케이션이 활성화되었는지 확인하려면 다음으로 이동하십시오. 구독 관리 〉 구독 인스턴스에 있습니다. 목록에 조직이 구매한 구독이 표시됩니다. 애플리케이션이 설치 및 활성화되지 않은 경우 을 참조하십시오 취약성 대응 설치.
인스턴스에 필요한 ServiceNow 역할이 있는지 확인합니다.	예상 결과의 설치, 구성 및 검증에 필요한 역할은 다음과 같습니다. • 아직 할당되지 않은 경우 시스템 관리자〔admin〕가 애플리케이션을 설치하고 사용자를 App-Sec Manager 그룹에 할당합니다. 그룹 역할에 대한 자세한 내용은 문서를 참조하십시오 애플리케이션 취약성 대응 사용자 그룹 및 역할. • App-Sec 관리자 그룹은 구성을 감독하고 예상 결과를 검증합니다.

필요한 역할: App-Sec 관리자

프로시저

1. 설치 Fortify 취약성 통합 하려는 인스턴스에 로그인합니다.
2. ServiceNow Store로 이동합니다.
3. ServiceNow Store에서 애플리케이션과 취약성 대응 통합을 Fortify 검색합니다.
4. 애플리케이션 타일을 클릭합니다.
   설치 중인 애플리케이션에 대한 자세한 정보가 표시됩니다.

   주:
   해당하는 경우 다른 요구 사항 및 종속성 섹션을 읽어보십시오.

5. 앱 요청을 클릭하고 Now Support 로그인 자격 증명을 입력합니다.
6. 가져오기를 클릭합니다.
7. 인스턴스 이름 및 인스턴스 이유를 입력하고 인스턴스 확인을 클릭합니다.
8. 요청을 클릭합니다.
   자세한 설치 지침이 포함된 이메일을 받게 됩니다.
9. 다음으로 이동 시스템 애플리케이션 〉 애플리케이션.
10. 애플리케이션을 찾아서 선택한 다음 설치를 클릭합니다.
    애플리케이션이 인스턴스에 자동으로 설치됩니다.

다음에 수행할 작업

사용자 환경에 맞게 구성합니다 Fortify 취약성 통합 . Fortify 취약성 통합 구성 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Fortify 취약성 통합 구성

인스턴스에서 통합을 실행하기 전에 설치 및 구성 단계를 완료하여 제품이 의 기능과 취약성 대응제대로 통합 애플리케이션 취약성 대응 되도록 Fortify 해야 합니다. 이 애플리케이션은 별도의 구독으로 사용할 수 있습니다.

시작하기 전에
필요한 역할: App-Sec 관리자

설치하기 전에 다음 설정 검사 목록을 완료합니다. 이러한 설정 작업은 원활한 설치 및 구성을 위해 필요합니다.

주:
이 프로세스는 프로덕션 인스턴스에 다운로드된 애플리케이션에만 적용됩니다. 애플리케이션을 비프로덕션 또는 개발 인스턴스에 다운로드하는 경우에는 권리를 얻을 필요가 없습니다. 로 애플리케이션 활성화 ServiceNow Store계속 진행합니다.

작업 설정	설명
애플리케이션이 설치되고 활성화되었는지 취약성 대응 확인합니다.	이 애플리케이션이 활성화되었는지 확인하려면 다음으로 이동하십시오. 구독 관리 〉 구독 인스턴스에 있습니다. 목록에 조직이 구매한 구독이 표시됩니다. 애플리케이션이 설치 및 활성화되지 않은 경우 을 참조하십시오 취약성 대응 설치.
애플리케이션과의 Fortify 통합이 취약성 대응 설치되고 활성화되었는지 확인합니다.	이 애플리케이션이 활성화되었는지 확인하려면 다음으로 이동하십시오. 구독 관리 〉 구독 인스턴스에 있습니다. 목록에 조직이 구매한 구독이 표시됩니다. 애플리케이션이 설치 및 활성화되지 않은 경우 을 참조하십시오 ServiceNow 와 Vulnerability Response 통합 설치Fortify.
인스턴스에 필요한 ServiceNow 역할이 있는지 확인합니다.	예상 결과의 설치, 구성 및 검증에 필요한 역할은 다음과 같습니다. • 아직 할당되지 않은 경우 시스템 관리자 〔admin〕가 앱을 설치하고 사용자를 App-Sec 관리자 그룹에 할당합니다. • App-Sec 관리자는 구성을 감독하고 예상 결과를 검증합니다.
Fortify 취약성 통합의 경우 **API ID**와 **API** 키를 준비합니다.	**API ID** 및 **API** 키를 얻으려면 연락처에 문의하십시오Fortify.

프로시저

1. 애플리케이션 취약성 통합을 설치할 Fortify 인스턴스에 로그인합니다.
2. ServiceNow Store로 이동합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 에서 ServiceNow Store애플리케이션과의 Fortify 통합을 검색합니다취약성 대응.
4. 애플리케이션 타일을 클릭합니다.
   설치 중인 애플리케이션에 대한 자세한 정보가 표시됩니다.

   주:
   해당하는 경우 다른 요구 사항 및 종속성 섹션을 읽어보십시오.

5. 앱 요청을 클릭하고 Now Support 로그인 자격 증명을 입력합니다.
6. 가져오기를 클릭합니다.
7. 인스턴스 이름 및 인스턴스 이유를 입력하고 인스턴스 확인을 클릭합니다.
8. 요청을 클릭합니다.
   자세한 설치 지침이 포함된 이메일을 받게 됩니다.
9. 다음으로 이동 시스템 애플리케이션 〉 애플리케이션.
10. 애플리케이션을 찾아서 선택한 다음 설치를 클릭합니다.
    애플리케이션이 인스턴스에 자동으로 설치됩니다.
11. 설치가 완료되면 다음으로 이동합니다. **Fortify** 취약성 통합 〉 **FoD** 구성.
12. 양식에서 필드를 채웁니다.

Fortify on Demand 구성 양식

필드	설명
API 루트 URL	사용자의 Fortify 인스턴스 URL입니다.
API 키	API에 전송되는 고유 식별자입니다 Fortify .
API 비밀	에서 제공하는 클라이언트 비밀입니다 Fortify.
DAST 포함	DAST 검사의 취약성을 포함하는 옵션입니다. DAST 스캔은 전체 애플리케이션 동작의 취약성을 식별합니다.
SAST 포함	SAST 검사의 취약성을 포함하는 옵션입니다. SAST 검사는 코드의 취약성을 식별합니다.
ServiceNow에서 예외 및 긍정 오류 분류 (Vulnerability Response v20.0부터 시작)	임포트 시 워크플로우를 통해 ServiceNow AVI에 대한 예외 관리 및 긍정 오류를 관리하는 옵션을 선택합니다. 이러한 옵션은 기본적으로 활성화됩니다. 사용 사례 예제는 다음 문서를 에서 지연 및 긍정 오류에 대한 상태 매핑 관리 애플리케이션 취약성 대응참조하십시오. 다음에서 예외 관리 ServiceNow 지연됨 상태로 표시된 임포트된 AVI를 분류하려면 이 옵션을 활성화된 상태로 둡니다. 소스 상태가 있는 AVI는 일반적으로 인스턴스에서 지연됨 상태로 매핑됩니다. 대신 오픈에 매핑됩니다. AVI 기록 에서 예외를 요청합니다 .

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	에서 긍정 오류 관리 ServiceNow 소스 상태가 긍정 오류 또는 잠재적 긍정 오류로 표시된 임포트된 AVI를 분류하려면 이 옵션을 활성화된 상태로 둡니다. 일반적으로 인스턴스에서 종결됨 상태로 매핑되는 이러한 소스 상태를 가진 AVI는 **Open**에 매핑됩니다. AVI 기록에서 긍정 오류를 요청합니다. ○ 스캐너에서 임포트한 소스 상태를 유지하려면 확인란 하나 또는 둘 다를 비활성화합니다. ○ 이러한 AVI는 임포트될 때 대상 상태 및 대상 이유 상태에 매핑되지만 예외 및 가양성 워크플로우에 의해 분류되지 않습니다. 예외 요청 및 긍정 오류 작업은 AVI에 표시되지 않습니다.
ServiceNow에서 환자 분류(Vulnerability Response v20.0 이전)	인스턴스에서 애플리케이션 취약성 분류를 ServiceNow 관리합니다. ○ 내에서 AVI ServiceNow를 분류하려면 확인란을 선택합니다. 이 옵션을 선택하면 AVI가 열림 상태로 임포트됩니다. 그런 다음 예외를 요청하거나 AVI를 가양성으로 표시할 수 있습니다. ○ 소스 상태, 즉 스캐너에서 임포트한 상태를 유지하려면 이 확인란이 선택되어 있지 않아야 합니다. 주: 긍정 오류로 표시 및 예외 요청 옵션은 내에서 분류ServiceNow되는 AVI에 대해서만 사용할 수 있습니다.

13. 자격 증명 저장 및 테스트를 선택합니다.

다음에 수행할 작업
환경에 도메인 분리 가져오기가 필요한 경우 문서를 참조하십시오 통합을 위해 도메인 분리 임포트 작성.

초기 설치 시 자세한 지침은 을 참조하십시오 애플리케이션 취약성 대응 구성 .

초기 설치 후 수정 사항은 를 Fortify 취약성 통합 수정 및 활동참조하십시오.

Fortify 취약성 통합 임포트 실행 상태 보기

취약성 통합 실행 관련 목록을 사용하여 통합 실행의 성공을 확인하고, 문제를 찾고, 정정 결정을 알립니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
임포트 실행 상태를 보려면 Fortify 다음을 수행합니다.

- 취약성 대응 및 Fortify 취약성 통합 애플리케이션을 설치하고 구성해야 합니다.
- 임포트가 Fortify 취약성 통합 예약되어 실행 중이어야 합니다.

필요한 역할: App-Sec 관리자

이 태스크 정보
통합 실행 중에 여러 프로세스가 생성되고 데이터가 페이지 형식으로 수신됩니다. 각 프로세스에는 페이지에 첨부된 데이터가 있는 하나 이상의 임포트 큐 항목이 포함될 수 있습니다. 이러한 항목은 1시간의 시간 제한 내에 데이터를 처리해야 합니다. 그러나 페이로드 크기가 크면 처리 시간이 1시간을 초과하거나 중단되어 통합 시간 제한 오류가 발생할 수 있습니다. 통합은 시간 초과 오류에도 불구하고 데이터를 계속 처리합니다. 이러한 잘못된 통신을 피하기 위해 버전 18.2.4 애플리케이션 취약성 대응부터 큐가 활성 상태이고 데이터를 처리하는지 여부를 나타내기 위해 타임스탬프(하트비트)가 주기적으로 전송됩니다. 임포트 큐 항목 페이지의 처리된 마지막 기록 필드는 임포트 큐가 생성하거나 업데이트하는 기록 수에 따라 업데이트됩니다. 임포트 큐 항목이 1시간의 시간 제한을 초과하는 경우, 시스템은 마지막으로 처리된 기록 필드를 검사하여 1시간보다 오래되었는지도 확인합니다. 이 경우 이는 임포트 큐 항목이 고착되었음을 나타내며 처리 시 더 이상의 지연을 방지하기 위해 시간 초과됩니다.

주:
마지막으로 처리된 기록 필드는 다음 시스템 속성에 정의된 내용에 따라 업데이트됩니다.

- *sn_sec_cmn.record_threshold_heartbeat*: 하트비트(타임스탬프)가 임포트 큐 항목으로 전송된 후 처리된 기록 수를 정의합니다.
- *sn_sec_cmn.maximum_heartbeat_delay*: 임포트 큐 항목을 시간 초과해야 하는 시간을 정의합니다.

프로시저

1. 다음으로 이동 모두 〉 **Fortify** 취약성 통합 〉 통합.
2. 통합을 선택합니다.
3. 취약성 통합 실행 관련 목록을 클릭합니다.
4. 모든 임포트가 성공했는지 확인합니다.
5. v2.3부터 총 처리 시간, 사전 및 사후 통합 실행 프로세스의 평균 시간과 같은 상세 정보, 애플리케이션 취약한 항목 통합의 통합 실행 기록에 대한 보고서를 볼 수 있습니다.

Fortify 취약성 통합 수정 및 활동

특히 에 대한 Fortify 취약성 통합선택적 수정 사항을 구성합니다.

주:
여기에 나열된 설정 이외의 다른 Fortify 취약성 통합 설정을 변경하려면 고급 ServiceNow 전문 애플리케이션 취약성 대응 지식이 필요하며 이는 제품 설명서에서 다루지 않습니다.

수동 **Fortify** 애플리케이션 취약성 임포트 수행

초기 임포트에 실패했거나 예약된 초기 임포트를 기다리지 않으려면 매일 예약된 작업과 관계없이 전체 데이터 임포트를 수행할 수 있습니다.

시작하기 전에
필요한 역할: App-Sec 관리자

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 **Fortify** 취약성 통합 〉 통합.
2. 통합(예: 애플리케이션 목록 통합)을 Fortify 선택합니다.
3. 지금 실행을 선택합니다.

> **주:**
> 완전한 데이터 검색을 위해 Fortify 애플리케이션 취약성 통합을 순서대로 실행합니다.

를 사용하여 데이터 임포트 **Fortify** 취약성 통합

Fortify 스캐너에서 데이터를 임포트하여 애플리케이션 취약한 항목(AVI)을 매핑함으로써 인스턴스의 데이터를 보강합니다.

시작하기 전에

필요한 역할: App-Sec 관리자

이 태스크 정보

초기 임포트 Fortify 후 취약성 통합은 실행될 때마다 델타 임포트를 수행하여 최신 데이터를 검색합니다. 전체 임포트에 대한 자세한 내용은 을 참조하십시오 수동 Fortify 애플리케이션 취약성 임포트 수행 .

프로시저

1. 다음으로 이동 모두 〉 **Fortify** 취약성 통합 〉 통합.
2. 통합을 선택합니다.
3. 양식에서 필드를 채웁니다.

필드	설명
이름	통합 실행의 이름입니다.
활성	통합을 활성화하는 옵션입니다.
실행	통합 실행 빈도입니다.
시간	
애플리케이션	이 기록이 포함된 애플리케이션입니다.
소스 통합	이 통합에 대한 소스 통합입니다.
소스 인스턴스	이 통합에 대한 소스 인스턴스입니다.
다음 통합	현재 통합 실행 후 실행할 다음 순서 통합입니다.
시작 시간	마지막으로 성공한 통합 실행의 시작 날짜 및 시간입니다. 시간은 현지 시간으로 시간으로 계산됩니다. 초기 실행의 기본 시간은 00:00:00입니다.
통합 상세 정보	
통합 스크립트	통합이 실행될 때 실행되도록 확장하는 *VulnerabilityIntegrationBase* 스크립트 포함입니다. 이 스크립트는 타사 시스템에서 데이터를 검색하는 방법을 정의합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
통합 공장 스크립트	통합 스크립트에 대해 선택된 스크립트 포함을 구성하는 방법을 정의하는 스크립트입니다.
프로세서 전략 보고	통합이 실행될 때 통합 스크립트에서 반환된 데이터를 처리하는 데 사용하려는 전략입니다.

4. 통합을 실행하려면 지금 실행을 선택합니다.

종결된 **Fortify** 요청 시 애플리케이션 취약 항목 포함

기본적으로 종결 된 애플리케이션 취약한 항목(AVIT)은 취약한 항목 통합 임포트 중에 Fortify 생성되지 않습니다. 만들려면 시스템 속성을 변경해야 합니다.

시작하기 전에
이(가) Fortify 취약성 통합 설치되어 실행 중이어야 합니다.

필요한 역할: App-Sec 관리자

프로시저

1. 왼쪽 탐색 필터 탐색기 텍스트 상자에 sys_properties.list를 입력합니다.
2. 목록의 이름 검색 상자에 sn_vul.create_closed를 입력합니다.
3. 값 필드를 두 번 클릭하고 **True**로 설정합니다.
4. 저장 확인 표시 아이콘을 클릭합니다.
   다음 Fortify 임포트에서 종결 상태의 기록은 에 AVIT애플리케이션 취약성 대응로 생성됩니다.

GitHub 애플리케이션 취약성 통합

이 임포트는 GitHub 애플리케이션 취약성 통합 사용자 환경의 리포지토리 GitHub 에서 취약성 경보를 보는 데 도움이 되는 SAST(정적 애플리케이션 보안 테스트) 및 SCA(소프트웨어 구성 분석) 데이터를 가져옵니다.

GitHub 애플리케이션 취약성 통합

는 GitHub 애플리케이션 취약성 통합 스캐너 데이터를 수집하고 해당 데이터를 ServiceNow AI Platform#. 인스턴스의 외부 공급업체 취약성 및 GitHub 경보를 매핑하는 기능과 취약성 대응 쉽게 통합됩니다ServiceNow# 애플리케이션 취약성 대응.

환경은 GitHub 여러 조직을 지원합니다. 이러한 조직(온 프레미스 및 엔터프라이즈)에는 엔지니어링, 품질, 설명서 등 다양한 부서가 포함될 수 있습니다. 각 조직은 차례로 여러 리포지토리를 지원할 수 있습니다. 리포지토리 통합을 사용하여 GitHub 애플리케이션 데이터를 임포트한 후에는 이러한 리포지토리에서 취약성 및 경보 데이터를 임포트할 수 있습니다. 임포트한 데이터는 애플리케이션에서 애플리케이션처럼 애플리케이션 취약성 대응 처리됩니다. 스캐너가 취약성을 탐지하고 리포지토리에 대한 경보를 생성하면 에 애플리케이션 취약성 대응취약성이 생성됩니다.

각 통합 기록에 대해 구성된 실행 사용자가 있습니다. 이 사용자의 기본값은 VR입니다. 시스템. 이 값은 변경하지 마십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용 가능한 버전

릴리스 버전	릴리스 정보
GitHub 애플리케이션 취약성 통합 v1.2, v1.1, 1.0	Application Vulnerability Response release notes 호환성 정보는 KB0856498 Vulnerability Response 호환성 매트릭스 및 릴리스 스키마 변경을 참조하십시오.

GitHub 통합

통합	설명
GitHub 리포지토리 통합	v1.1부터 온 프레미스 및 클라우드(엔터프라이즈) 계정에 대한 모든 애플리케이션 데이터를 임포트합니다 GitHub . 통합은 조직(온프레미스) 또는 엔터프라이즈(클라우드) 환경에 대해 구성한 리포지토리에서 애플리케이션을 임포트합니다. 다른 통합은 리포지토리 통합에서 임포트된 현재 애플리케이션 데이터에 종속되므로 실행을 GitHub 전에 이 통합을 실행합니다.
GitHub CodeScan 통합	리포지토리에서 GitHub 보안 취약성 및 코딩 오류에 대한 Code scanning 취약성 경보를 검색합니다. 임포트한 데이터는 인스턴스의 SAST 결과에 매핑됩니다.
GitHub Dependabot 통합	리포지토리에서 알려진 취약성이 있는 종속성에 대한 Dependabot 경보를 검색합니다. 임포트한 데이터는 인스턴스의 SCA 결과에 매핑됩니다.
GitHub 비밀 스캔	애플리케이션 보안 테스트 결과와 함께 조직 코드에서 비밀을 검색합니다. 데이터가 인스턴스의 SCA 결과에 매핑됩니다.
GitHub 비밀 스캔 위치	조직 코드에서 스캔한 비밀의 위치와 라인 번호를 검색하여 개발자가 정정할 수 있도록 지원합니다.

리포지토리에서 GitHub 파일 ServiceNow AI Platform® 업로드 SBOM

CI/CD(지속적 통합 및 지속적 제공/배포) 파이프라인에서 생성된 파일이 인스턴스에서 성공적으로 큐에 대기 ServiceNow AI Platform# 했는지 확인합니다SBOM.

- 환경에서 시작하는 GitHub 작업을 사용하여 GitHub 소프트웨어 개발 주기 동안 잠재적으로 유해한 구성 요소로부터 환경을 보호합니다.
- GitHub Marketplace에서 업로드하는 데 SBOM 필요한 GitHub 작업을 가져옵니다.

SBOM 애플리케이션은 파일을 업로드 SBOM 하는 데 필요합니다. 자세한 내용은 소프트웨어 자재 명세서 탐색 문서를 참조하십시오.

임포트한 데이터 보기

리포지토리 통합에서 임포트한 GitHub 애플리케이션 데이터가 검색된 애플리케이션 [sn_vul_app_release] 테이블에 표시됩니다. 먼저 이 통합을 실행합니다.

리포지토리 통합은 설정 메뉴에서 계정의 리포지토리 GitHub 에 대해 구성한 태그와 주제를 가져옵니다. 모든 사용자 지정 속성은 리포지토리 아래의 메뉴에 있습니다. 속성에 대해 설정한 값은 키-값 쌍으로 임포트됩니다. 인스턴스에서 이 정보를 볼 수 있는 위치에 대한 자세한 내용은

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음 문서를 GitHub 애플리케이션 취약성 통합 임포트 실행 상태 및 임포트한 리포지토리 데이터 보기참조하십시오.

Dependabot 통합에서 임포트한 데이터(결과)는 GitHub 다음 테이블에 표시됩니다.

- 검색된 애플리케이션 [sn_vul_app_release].
- 애플리케이션 취약성 검사 요약 [sn_vul_app_vul_scan_summary].
- 애플리케이션 취약한 항목 [sn_vul_app_vulnerable_item]
- 패키지 [sn_vul_app_package].

GitHub CodeScan 통합에서 가져온 데이터가 다음 테이블에 표시됩니다.

- 검색된 애플리케이션 [sn_vul_app_release].
- 애플리케이션 취약성 검사 요약 [sn_vul_app_vul_scan_summary].
- 애플리케이션 취약성 항목 [sn_vul_app_vul_entry]
- 애플리케이션 취약한 항목 [sn_vul_app_vulnerable_item]

준비 중 **GitHub** 애플리케이션 취약성 통합

다음 작업을 수행하여 통합을 준비합니다. 여기서는 GitHub 애플리케이션 취약성 통합 사용자가 GitHub 제품 및 API에 익숙하다고 가정합니다.

각 통합 기록에 대해 구성된 실행 사용자가 있습니다. 이 사용자의 기본값은 VR입니다. 시스템. 이 값은 변경하지 마십시오.

필요한 역할:

- 관리자는 애플리케이션을 다운로드, 설치, 활성화하고 역할을 할당합니다.
- GitHub 관리자는 GitHub 콘솔에서 자격 증명을 얻고 토큰을 생성합니다.
- 관리자는 인스턴스에서 연결 및 별칭 기록을 설정합니다.

작업 설정

작업 설정	설명
애플리케이션이 설치되고 활성화되었는지 취약성 대응 확인합니다.	이 애플리케이션이 활성화되었는지 확인하려면 다음으로 이동하십시오. 구독 관리 〉 구독 인스턴스에 있습니다. 목록에 조직이 구매한 구독이 표시됩니다. 애플리케이션이 설치 및 활성화되지 않은 경우 을 참조하십시오 취약성 대응 설치.
이(가) GitHub 애플리케이션 취약성 통합 설치되고 활성화되었는지 확인합니다.	이 애플리케이션이 활성화되었는지 확인하려면 다음으로 이동하십시오. 구독 관리 〉 구독 인스턴스에 있습니다. 목록에 조직이 구매한 구독이 표시됩니다. 애플리케이션이 설치 및 활성화되지 않은 경우 을 참조하십시오 설치 ServiceNow GitHub 애플리케이션 취약성 통합.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업 설정

작업 설정	설명
인스턴스에 필요한 ServiceNow 역할이 있는지 확인합니다.	구성 및 예상 결과 검증에 필요한 역할은 다음과 같습니다. • 아직 할당되지 않은 경우 시스템 관리자〔admin〕가 앱을 설치하고 사용자를 App-Sec Manager 사용자 그룹에 할당합니다. • App-Sec 관리자는 구성을 감독하고 예상 결과를 검증합니다. • sn_vul_github_config_integration App-Sec Manager 사용자 그룹이 상속합니다. 이 역할에는 connection_admin 및 oauth_admin 역할이 포함되어 있습니다.
GitHub 자격 증명 및 계정 정보를 가져옵니다.	인증을 위해 생성하는 기록에는 계정 정보가 필요합니다. 필요한 세부 정보 및 OAuth 인증에 필요한 기록 설정에 대한 자세한 내용은 을 참조하십시오 앱에 대한 GitHub OAuth 2.0 자격 증명 생성 - JWT for the GitHub 애플리케이션 취약성 통합 .
CWE(Common Weakness Enumeration) 데이터를 임포트하고 있는지 확인합니다.	CWE(일반적인 약점 열거형) 통합도 GitHub 취약성 통합을 설치하고 구성하기 전에 사용되며 애플리케이션 취약성 대응 그 전에 실행해야 합니다. 기본적으로 와 함께 취약성 대응설치됩니다. 주: NVD(NIST 취약성 데이터베이스) 데이터는 GitHub 취약성 통합을 설치하는 데 필요하지 않지만 보강 기능을 제공하므로 유용합니다. NVD에 대한 자세한 내용은 문서를 참조하십시오 NVD 및 CWE 통합을 통해 데이터를 임포트하고 외부 공급업체 라이브러리를 관리합니다.

앱에 대한 **GitHub OAuth 2.0** 자격 증명 생성 **- JWT for the GitHub** 애플리케이션 취약성 통합

에 대한 GitHub 애플리케이션 취약성 통합JWT 전달자 토큰을 사용하여 앱을 통합 GitHub 하려면 다음 단계를 수행합니다.

필요한 역할:

- sn_vul.app_sec_manager 및 관리자 의 기록에 ServiceNow AI Platform대한 .
- 계정의 작업에 GitHub 필요한 인스턴스 역할이 없습니다.
- 이 설정 단계의 컨텍스트에 대한 자세한 내용은 OAuth 2.0 프로토콜을 참조하세요.

에 대한 앱 생성 및 구성 **GitHubGitHub** 애플리케이션 취약성 통합

계정에서 사용자 지정 GitHub 앱을 GitHub 생성하여 인스턴스에서 OAuth GitHub 애플리케이션 취약성 통합 2.0 인증을 활성화합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: 인스턴스 역할이 필요하지 않음

이 태스크 정보
계정에서 GitHub 이 단계를 완료합니다. 참조 건물 GitHub 앱 (개발자 사이트)에서 GitHub 사용자 지정 애플리케이션을 만들고 구성하는 방법에 대한 지침을 확인할 수 있습니다.

프로시저

1. GitHub 계정에서 다음으로 이동하여 앱을 생성합니다GitHub. 개발자 설정 〉 **GitHub** 앱.
2. 홈페이지 **URL** 필드에 https://<instance-name>.service-now.com 을 입력합니다.
3. 사용자 권한 부여 콜백 **URL** 필드에 https://<instance-name>.service-now.com/oauth_redirect.do 을 입력합니다.
4. 사용자 식별 및 권한 부여 섹션에서 사용자 인증 토큰 만료 필드의 선택을 취소합니다.
5. 웹후크 섹션에서 활성 필드를 선택합니다.
6. 웹후크 **URL** 필드에 https://instance-name>.service-now.com/ # 입력합니다.
7. 나머지 필드는 비워 둡니다(기본값).
8. 리포지토리 권한 섹션에서 다음 설정을 구성합니다.

코드 스캔	읽기 전용
컨텐츠	읽기 전용
사용자 지정 속성	읽기 전용
Dependabot alerts	읽기 전용
메타데이터	읽기 전용

주:
GitHub 앱을 이미 사용 중이고 권한을 업데이트하는 경우 GitHub 앱에 대한 해당 권한을 검토하고 수락해야 합니다. 앱으로 이동하여 구성 > 검토 요청 > 새 권한 수락을 선택할 수 있습니다.

9. 나머지 권한은 ## ## ## (기본값)으로 둡니다.
10. 이벤트 구독 섹션에서 배포 보호 규칙 옵션을 선택합니다.
11. 헤더를 마우스 오른쪽 버튼으로 클릭하여 변경 내용을 저장합니다.
12. 새로 만든 GitHub 앱을 선택한 계정에 설치합니다.
    a. GitHub 앱 설정 페이지에서 앱을 선택합니다.
    b. 왼쪽 사이드바에서 앱 설치를 선택합니다.
    c. 올바른 리포지토리가 포함된 조직 또는 개인 계정 옆에 있는 설치를 선택합니다.
    d. 모든 리포지토리에 앱을 설치하거나 리포지토리를 선택합니다.
    자세한 내용은 GitHub 앱 설치를 참조하세요.
13. 설치 후 앱의 설정(톱니바퀴 아이콘)을 선택하고 다음 정보를 적어 두거나 기록해 둡니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이러한 상세 정보는 인스턴스에서 애플리케이션 레지스트리 ServiceNow AI Platform 를 생성할 때 필요합니다.

- 앱 ID
- 클라이언트 ID
- 클라이언트 비밀입니다.
- URL에서 토큰을 기록해 둡니다. 인스턴스의 토큰 URL에 입력하는 토큰 ID입니다.

14. 페이지를 아래로 스크롤하여 새 개인 키를 생성하고 컴퓨터에 저장합니다.

에 대한 **JKS** 인증서 생성 **GitHub** 애플리케이션 취약성 통합

에 대한 GitHub 애플리케이션 취약성 통합JWT 인증을 위한 JKS 인증서를 생성합니다.

시작하기 전에
.jks 파일(KeyStore 암호)을 생성하는 데 사용하는 암호를 기록해 두어야 합니다.

필요한 역할: sn_vul.app_sec_manager

프로시저

1. 앱 개인 키를 사용하여 GitHub CA 서명 인증서를 만듭니다.

```
openssl req -new -x509 -key <file-name>.pem -out <certificate-name>.pem -days 1095
```

2. 필요한 상세 정보를 입력합니다.
3. 앱 개인 키 및 CA 서명 인증서를 사용하여 GitHub PKCS 12 파일을 생성합니다.

```
openssl pkcs12 -export -in <certificate-name>.pem -inkey <file-name>.pem -certfile
 <certificate-name>.pem -out <PKCS-12-file-name>.p12
```

4. 익스포트 암호를 제공합니다.
5. JKS 파일을 생성합니다.

```
keytool -importkeystore -srckeystore <PKCS-12-file-name>.p12 -srcstoretype pkcs12
 -destkeystore <JKS-certificate-filename>.jks -deststoretype JKS
```

6. 대상 및 소스 키 저장소 암호를 제공합니다.

Java 키 스토어 인증서를 인스턴스에 첨부 **GitHub** 하여 **GitHub** 애플리케이션 취약성 통합

유효한 GitHub Java KeyStore(JKS) 인증서를 인스턴스에 연결하여 JWT 전달자 Grant 토큰 인증을 활성화합니다.

시작하기 전에
유효한 Java KeyStore 인증서입니다.

필요한 역할: sn_vul.app_sec_manager

프로시저

1. 다음으로 이동 모두 〉 시스템 정의 〉 인증서.
2. 새로 만들기를 선택합니다.
3. 양식에서 필드를 채웁니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

X.509 인증서 양식 필드

필드	설명
이름	기록을 고유하게 식별하는 이름입니다. 예를 들어 AVR# # GitHub # ######.
만료 시 알림	인증서가 만료될 때 알림을 받을 사용자를 지정하는 옵션입니다.
만료되기 전 경고	인증서가 만료되기 전에 알림을 보낼 일 수입니다.
활성	인증서를 활성화하는 옵션입니다.
유형	인증서 유형을 선택하는 옵션입니다. **Java** 키 스토어를 선택합니다.
며칠 후 만료	인증서가 만료될 때까지의 일 수입니다.
키 스토어 암호	인증서와 관련된 암호입니다(힌트: 이전에 작성한 대상 KeyStore 암호).
간단한 설명	인증서에 대한 요약입니다.

4. 첨부 파일 아이콘을 선택하고 JKS 인증서를 첨부합니다.
5. **Validate Stores/**Certificates(스토어/인증서 확인)를 선택합니다.
   유효한 인증서 파일에 대해 유효한 key_store 메시지가 표시됩니다.

JKS 인증서에 대한 **GitHub JWT** 서명 키 만들기 **GitHub** 애플리케이션 취약성 통합

Java KeyStore 인증서에 GitHub 할당할 JWT(JSON Web Token) 서명 키를 생성합니다.

시작하기 전에
필요한 역할:

- 관리자
- sn_vul.app_sec_manager

프로시저

1. 다음으로 이동 모두 〉 시스템 **OAuth** 〉 **JWT** 키.
2. 새로 만들기를 선택합니다.
3. 양식에서 필드를 채웁니다.

JWT 키 양식 필드

필드	설명
이름	JWT 서명 키를 고유하게 식별하는 이름입니다. 예를 들어 AVR# # GitHub # JWT #입니다.
서명 키 스토어	이전 작업에서 첨부한 유효한 JKS 인증서를 선택합니다.
키 ID	이 필드는 비워둡니다.
서명 알고리즘	이 값을 RSA 256으로 둡니다.
서명 키 암호	서명 키와 연결된 암호입니다. JKS 파일을 생성하는 데 사용한 암호입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
활성	키를 활성화하는 옵션입니다.

4. 페이지의 회색 머리글 아무 곳이나 마우스 오른쪽 버튼으로 클릭하고 저장을 선택합니다.

의 서명 키에 대한 **GitHub JWT** 제공자 생성 **GitHub** 애플리케이션 취약성 통합

에 대한 GitHub인스턴스에 JSON 웹 토큰(JWT) 제공자 ServiceNow 를 추가합니다.

시작하기 전에
필요한 역할:

- 관리자
- sn_vul.app_sec_manager

프로시저

1. 다음으로 이동 모두 〉 시스템 **OAuth** 〉 **JWT** 제공자.
2. 새로 만들기를 선택합니다.
3. 양식에서 필드를 채웁니다.

JWT 제공자 양식 필드

필드	설명
이름	JWT 제공자를 고유하게 식별하는 이름입니다. 예를 들어 AVR# # GitHub # JWT ###입니다.
만료 간격(초)	JWT 제공자 토큰의 수명을 설정할 숫자(초)입니다. 이 설정을 기본값으로 둘 수 있습니다.
서명 구성	이전 단계에서 만든 JWT 키를 선택합니다.

4. 양식 헤더를 마우스 오른쪽 버튼으로 클릭하고 저장을 선택합니다.
5. GitHub 표준 클레임 관련 목록에서 **iss** 클레임 값에 대한 앱 앱 **ID**를 입력합니다.
   이전 단계에서 만든 콘솔의 GitHubGitHub 앱의 앱 ID입니다.
6. **aud** 및 **sub** 값을 비워 둡니다(기본값).
7. 양식 헤더를 마우스 오른쪽 버튼으로 클릭하고 저장을 선택합니다.

에 대한 **OAuth** 제공자(JWT)로 등록 **GitHubGitHub** 애플리케이션 취약성 통합

앱 계정 구성 중에 GitHub 생성된 정보를 사용하여 OAuth 공급자로 등록 GitHub 하고 인스턴스가 OAuth 2.0 토큰을 요청하도록 허용합니다.

시작하기 전에
필요한 역할:

- 관리자
- sn_vul.app_sec_manager

프로시저

1. 다음으로 이동 모두 〉 시스템 **OAuth** 〉 애플리케이션 레지스트리.
2. 새로 만들기를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

어떤 종류의 **OAuth** 애플리케이션입니까? 메시지가 표시됩니다.

3. 외부 공급업체 **OAuth** 제공자에 연결을 선택합니다.
4. 양식에서 필드를 채웁니다.

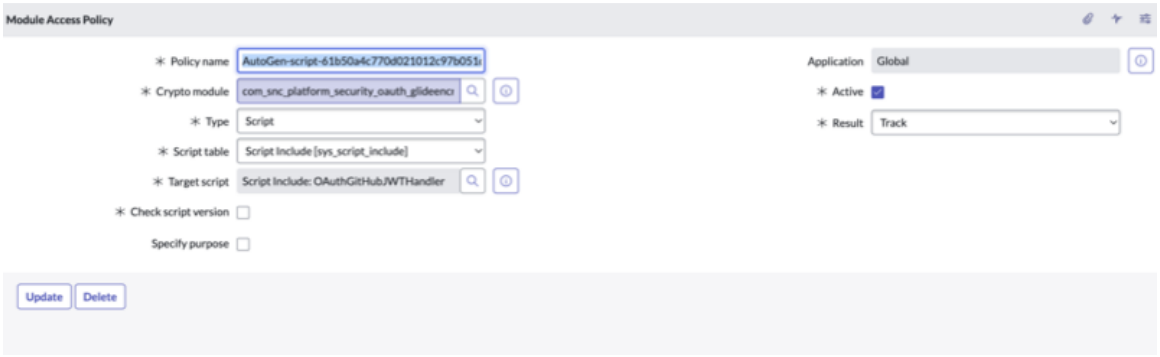
애플리케이션 레지스트리 양식 필드

필드	설명
이름	기록을 고유하게 식별하는 이름입니다. 예를 들어 # GitHub App Provider for AVR# 입력합니다.
클라이언트 ID	앱의 클라이언트 ID입니다 GitHub . 클라이언트 ID는 이전 단계에서 만든 콘솔의 GitHub 애플리케이션에서 가져옵니다GitHub. 이 ID는 의 앱 구성 정보 섹션에서 GitHub 사용할 수 있습니다 GitHub.
접근 가능	이 설정을 현재 값으로 둡니다.
클라이언트 비밀	앱의 클라이언트 비밀입니다 GitHub . 클라이언트 암호는 이전 단계에서 만든 콘솔의 GitHub 애플리케이션에서 가져온 GitHub 것입니다. 이 ID는 의 앱 구성 정보 섹션에서 GitHub 사용할 수 있습니다 GitHub.
활성	키를 활성화하는 옵션입니다. 이 항목을 선택된 상태로 둡니다.
인증 URL	이 URL은 자동으로 생성됩니다.
토큰 URL	인스턴스가 토큰을 검색하고 새로 고치는 데 사용하는 토큰 엔드포인트의 위치입니다. 앱의 URL GitHub 에서 토큰을 입력합니다. 앱이 에 설치된 GitHub후 URL에 표시되는 토큰입니다. 의 GitHub 앱 구성에 GitHub있는 앱 설치 섹션에서 기어를 선택합니다. 토큰이 웹 페이지 URL에 표시됩니다. ○ 클라우드의 경우: https://api.github.com/app/installations/49374672/access_tokens . 설치 ID: 9374672. ○ 온 프레미스의 경우: https://github-372.secops-eng.com/api/v3/app/installations/7/access_tokens/api/v3 .
OAuth API 스크립트	수정된 OAuthUtil 스크립트 포함을 참조할 수 있는 옵션입니다. **OAuthGitHubJWTHandler**를 선택합니다.
기본 부여 유형	애플리케이션 레지스트리와 연결된 권한 부여 유형입니다. **JWT** 전달자를 선택합니다.

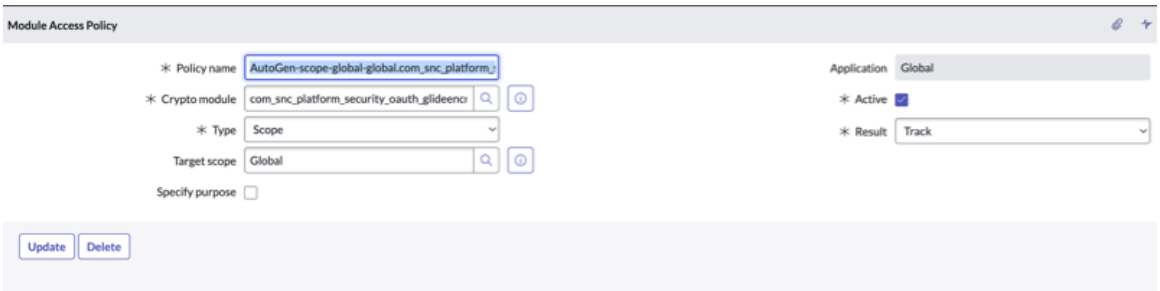
5. 나머지 양식 필드는 기본값으로 둡니다.
6. 양식 헤더를 마우스 오른쪽 버튼으로 클릭하고 저장을 선택합니다.
7. **OAuth** 엔터티 프로파일 관련 목록으로 스크롤하여 선택한 다음 목록에서 생성된 기본 프로파일을 엽니다.
8. **JWT** 제공자 필드를 이전에 작성한 JWT 제공자로 채우고 양식을 저장합니다.
9. 애플리케이션 레지스트리 파일로 돌아가서 저장합니다.
10. 다음으로 이동 주요 운영 〉 모듈 접근 정책 〉 모두.
11. com_snc_platform_security_oauth_glideencrypter암호화 모듈 필드 값으로 표시되고 대상 스크립트 필드에 OAuthGitHubJWTHandler가 스크립트 포함이 되도록 정책을 선택합니다.

    다음 이미지에서는 com_snc_platform_security_oauth_glideencrypter 이 암호화 모듈 필드의 값으로 선택되어 있습니다. 스크립트 테이블 필드## #### ## [sys_script_include] 테이블이 표시되고 대상 스크립트 필드 값은 OAuthGitHubJWTHandler입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



12. 업데이트를 선택합니다.



앞의 이미지에 표시된 것처럼 정책 이름 필드의 값이 변경되고 스크립트 테이블 및 대상 스크립트 필드가 더 이상 표시되지 않습니다.

13. 결과 필드가 ##으로 설정되어 있는지 확인하고 변경 내용을 저장합니다.

에 대한 자격 증명 및 연결 생성 **GitHub** 애플리케이션 취약성 통합

이전에 앱 제공자에게 GitHub 자격 증명 기록을 생성하여 작업을 승인합니다.

시작하기 전에
필요한 역할:

- 관리자
- sn_vul.app_sec_manager

프로시저

1. 다음으로 이동 자격 증명 및 연결 〉 자격 증명.
2. 새로 만들기를 선택합니다.
3. **OAuth 2.0** 자격 증명을 선택합니다.
4. 새로 만들기를 선택하고 필드를 채웁니다.
5. 페이지 헤더의 아무 곳이나 마우스 오른쪽 버튼으로 클릭하고 저장을 선택합니다.
   자격 증명 목록이 표시됩니다.
6. 방금 생성한 기록을 열고 **OAuth** 토큰 가져오기 관련 링크를 선택합니다.
   OAuth 토큰을 성공적으로 가져왔다는 메시지가 표시됩니다.
7. 다음으로 이동 자격 증명 및 연결 〉 연결.
8. 새로 만들기를 선택합니다.
9. **HTTP(s)** 연결을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

10. 새로 만들기를 선택하고 필드를 채웁니다.

11. 제출을 선택합니다.
    연결 및 자격 증명 별칭 목록이 표시됩니다.
12. 기록을 열고 연결 관련 목록 탭에서 새로 만들기를 선택한 다음 HTTP 연결 기록의 필드를 채웁니다.

13. 제출을 선택합니다.
    연결 및 자격 증명 별칭 목록이 표시됩니다. 이제 에 대한 GitHub 애플리케이션 취약성 통합 구성단계를 완료할 준비가 되었습니다. 연결 필드에 이전 단계에서 생성한 자격 증명을 입력합니다.

설치 **ServiceNow® GitHub** 애플리케이션 취약성 통합

인스턴스에서 통합을 실행하기 전에 설치 및 구성 단계를 완료하여 와 GitHub 애플리케이션 취약성 통합 올바르게 통합 애플리케이션 취약성 대응되도록 해야 합니다. 이 애플리케이션은 별도의 구독으로 사용할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 설치 GitHub 애플리케이션 취약성 통합 하려는 인스턴스에 로그인합니다.
2. ServiceNow Store로 이동합니다.
3. 에서 ServiceNow Store애플리케이션을 검색합니다 GitHub 애플리케이션 취약성 통합 .
4. 애플리케이션 타일을 선택합니다.
   설치 중인 애플리케이션에 대한 자세한 정보가 표시됩니다.

   > **주:**
   > 해당하는 경우 다른 요구 사항 및 종속성 섹션을 읽어보십시오.

5. 요청 앱을 선택하고 로그인 자격 증명을 입력합니다Now Support.
6. 가져오기를 선택합니다.
7. 인스턴스의 인스턴스 이름과이유를 입력하고 인스턴스 확인을 선택합니다.
8. 요청을 선택합니다.
   자세한 설치 지침이 포함된 이메일을 받게 됩니다.
9. 다음으로 이동 시스템 애플리케이션 〉 애플리케이션.
10. 응용 프로그램을 찾아서 선택하고 설치를 선택합니다.
    애플리케이션이 인스턴스에 자동으로 설치됩니다.

GitHub 애플리케이션 취약성 통합 구성

인스턴스에서 통합을 실행하기 전에 GitHub 제품이 와 제대로 통합 애플리케이션 취약성 대응되도록 설치 및 구성 단계를 완료해야 합니다. 이 애플리케이션은 별도의 구독으로 사용할 수 있습니다.

시작하기 전에
필요한 역할:

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- App-Sec 관리자 사용자 그룹
- OAuth 설정에 필요한 sn_vul.app_sec_manager

프로시저

1. 다음으로 이동 모두 〉 **Github** 취약성 통합 〉 구성.
2. 인증 유형으로 기본 인증 또는 **OAuth** 를 선택합니다.
   - 기본 인증에는 온프레미스 인스턴스에 대한 MID 서버가 필요합니다. 계정에서 기본 인증 GitHub 에 필요한 API 토큰을 생성합니다.
   - OAuth에는 에 설명된 앱에 대한 GitHub OAuth 2.0 자격 증명 생성 - JWT for the GitHub 애플리케이션 취약성 통합OAuth 앱, 자격 증명 및 연결 설정이 필요합니다.
3. 선택한 유형에 따라 필드를 채웁니다.
   기본 인증

필드	설명
API URL	엔터프라이즈 또는 온프레미스에 적합한 GitHub API URL입니다. 기본 URL은 입니다 https://api.github.com . 온프레미스는 엔드포인트 URL입니다 GitHub .
API 토큰	콘솔에서 생성한 토큰입니다 GitHub .
API 유형	다음 중 하나를 선택합니다. 조직 특정 조직의 데이터를 이름으로 임포트하려는 경우 이 옵션을 선택합니다. 환경은 GitHub 여러 조직을 지원합니다. 각 조직은 여러 리포지토리를 지원할 수 있습니다. 조직을 입력하면 해당 조직의 데이터만 임포트됩니다. 기업용 엔터프라이즈 환경은 여러 조직을 지원합니다. 엔터프라이즈 (클라우드) 환경의 모든 조직에서 취약성 데이터를 임포트하려면 이 옵션을 선택합니다.
조직 이름	리포지토리의 GitHub 이름입니다. 입력한 조직의 데이터만 임포트됩니다.
MID 서버	기본 인증을 위한 온 프레미스 인스턴스의 경우 MID 서버가 필요합니다.
예외 관리 및 긍정 오류를 관리하는 옵션을 선택합니다.	임포트 시 워크플로우를 사용하여 ServiceNow 예외 관리 및 애플리케이션 취약한 항목 (AVI)에 대한 긍정 오류를 관리하는 옵션을 선택합니다. 다음에서 예외 관리 ServiceNow

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	지연됨 상태로 표시된 임포트된 AVI를 분류하려면 이 옵션을 활성화된 상태로 둡니다. 소스 상태가 있는 AVI는 일반적으로 인스턴스에서 지연됨 상태로 매핑됩니다. 대신 오픈에 매핑됩니다. AVI 기록 에서 예외를 요청합니다 . 에서 긍정 오류 관리 ServiceNow 소스 상태가 긍정 오류 또는 잠재적 긍정 오류로 표시된 임포트된 AVI를 분류하려면 이 옵션을 활성화된 상태로 둡니다. 일반적으로 인스턴스에서 종결됨 상태로 매핑되는 이러한 소스 상태를 가진 AVI는 **Open**에 매핑됩니다. AVI 기록에서 긍정 오류를 요청합니다. ○ 스캐너에서 임포트한 소스 상태를 유지하려면 확인란 하나 또는 둘 다를 비활성화합니다. ○ 비활성화하면 예외 요청 및 긍정 오류 작업이 AVI에 표시되지 않습니다.
통합 인스턴스	데이터를 임포트하는 인스턴스입니다.

OAuth

필드	설명
API URL	엔터프라이즈 또는 온프레미스에 적합한 GitHub API URL입니다. 기본 URL은 입니다 https://api.github.com . 온프레미스는 엔드포인트 URL입니다 GitHub .
연결	생성한 연결은 다음에 설명되어 있습니다 앱에 대한 GitHub OAuth 2.0 자격 증명 생성 - JWT for the GitHub 애플리케이션 취약성 통합.
API 유형	다음 중 하나를 선택합니다. 조직 특정 조직의 데이터를 이름으로 임포트하려는 경우 이 옵션을 선택합니다. 환경은 GitHub 여러 조직을 지원합니다. 각 조직은 여러 리포지토리를 지원할 수

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	있습니다. 조직을 입력하면 해당 조직의 데이터만 임포트됩니다. 기업용 엔터프라이즈 환경은 여러 조직을 지원합니다. 엔터프라이즈 (클라우드) 환경의 모든 조직에서 취약성 데이터를 임포트하려면 이 옵션을 선택합니다. **주:** GitHub 앱은 엔터프라이즈 수준 API를 지원하지 않습니다.
조직 이름	리포지토리의 GitHub 조직 이름입니다. 입력한 조직의 리포지토리에 있는 데이터만 가져옵니다.
예외 관리 및 긍정 오류를 관리하는 옵션을 선택합니다.	임포트 시 워크플로우를 사용하여 ServiceNow 예외 관리 및 애플리케이션 취약한 항목 (AVI)에 대한 긍정 오류를 관리하는 옵션을 선택합니다. 다음에서 예외 관리 ServiceNow 지연됨 상태로 표시된 임포트된 AVI를 분류하려면 이 옵션을 활성화된 상태로 둡니다. 소스 상태가 있는 AVI는 일반적으로 인스턴스에서 지연됨 상태로 매핑됩니다. 대신 오픈에 매핑됩니다. AVI 기록 에서 예외를 요청합니다 . 에서 긍정 오류 관리 ServiceNow 소스 상태가 긍정 오류 또는 잠재적 긍정 오류로 표시된 임포트된 AVI를 분류하려면 이 옵션을 활성화된 상태로 둡니다. 일반적으로 인스턴스에서 종결됨 상태로 매핑되는 이러한 소스 상태를 가진 AVI는 **Open**에 매핑됩니다. AVI 기록에서 긍정 오류를 요청합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	○ 스캐너에서 임포트한 소스 상태를 유지하려면 확인란 하나 또는 둘 다를 비활성화합니다. ○ 비활성화하면 예외 요청 및 긍정 오류 작업이 AVI에 표시되지 않습니다.

4. 자격 증명 저장 및 테스트를 선택합니다.
5. GitHub 다른 통합을 실행하기 전에 리포지토리 통합을 실행합니다.
   다른 GitHub 통합은 리포지토리 통합에서 임포트한 현재 애플리케이션 데이터에 따라 다릅니다.
   리포지토리 통합의 데이터는 검색된 애플리케이션 [sn_vul_app_release] 테이블에 저장됩니다.
   자세한 내용은 GitHub 애플리케이션 취약성 통합 임포트 실행 상태 및 임포트한 리포지토리 데이터 보기 문서를 참조하십시오.

GitHub 애플리케이션 취약성 통합 임포트 실행 상태 및 임포트한 리포지토리 데이터 보기

취약성 통합 실행 관련 목록을 사용하여 통합 실행의 성공을 확인하고, 문제를 찾고, 정정 결정을 알립니다.

시작하기 전에
필요한 역할: sn_vul.app_sec_manager

프로시저

1. 다음으로 이동 모두 〉 **GitHub** 취약성 통합 〉 통합.
2. 통합을 선택합니다.
3. 취약성 통합 실행 관련 목록을 선택합니다.
4. 모든 임포트가 성공했는지 확인합니다.

   Trouble?

   실행 실패의 가장 일반적인 원인은 다음과 같습니다.

   ○ 네트워크 중단.

   ○ 데이터 전송 문제로 인해 변환 중에 데이터가 손상되었습니다.
   이러한 조건이 발생하면 지금 실행을 선택하고 통합을 다시 실행합니다.
5. 임포트한 리포지토리를 보려면 통합 목록으로 다시 이동하여 리포지토리 통합 기록을 선택합니다 GitHub .
6. 취약성 통합 실행 관련 목록을 선택하고 기록을 엽니다.
   통합 실행으로 임포트한 리포지토리 수가 임포트한 항목 열에 표시됩니다.

   설정 메뉴에서 계정의 리포지토리 GitHub 에 대해 구성한 모든 태그와 주제가 임포트됩니다.
   임포트한 모든 사용자 지정 속성은 리포지토리 아래 메뉴에 있습니다.

   태그, 주제 및 사용자 지정 속성은 계정에서 구성된 GitHub 경우에만 인스턴스로 임포트됩니다.

   임포트한 경우 이 GitHub 정보는 검색된 애플리케이션 [sn_vul_app_release] 테이블의 소스 추가 정보 열과 검색된 애플리케이션 기록의 소스 추가 정보 섹션에 표시됩니다. 사용자 지정 속성은 키-값 쌍으로 표시되고 태그와 주제는 배열로 표시됩니다.

임포트 세트 보기 GitHub 애플리케이션 취약성 통합

에 GitHub 애플리케이션 취약성 통합대한 임포트 정보의 상세 정보를 봅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_vul.app_sec_manager

프로시저

1. 다음으로 이동합니다. **GitHub** 취약성 통합 〉 임포트 세트 테이블.
2. 통합할 기록을 선택합니다.
3. 다음 정보를 보려면 관련 링크를 선택합니다.
   - 임포트 세트
   - 변환 맵
   - 변환 이력

Invicti 취약성 통합

는 Invicti 취약성 통합 Invicti 제품에서 임포트한 애플리케이션 데이터를 사용하여 코드 결함의 영향과 우선순위를 파악하는 데 도움을 줍니다.

Invicti 취약성 통합

는 Invicti 취약성 통합 스캐너 데이터를 수집하고 해당 데이터를 ServiceNow AI Platform#. 임포트한 ServiceNow# 애플리케이션 취약성 대응 외부 공급업체 애플리케이션 취약성 정보를 인스턴스에 매핑하는 기능과 취약성 대응 쉽게 통합됩니다.

통합은 다음과 같은 유형의 스캔 데이터를 임포트합니다.

- 동적 애플리케이션 보안 테스트(DAST)
- 인터랙티브 애플리케이션 보안 테스트(IAST)

DAST 및 IAST에 대한 자세한 내용은 문서를 참조하십시오 애플리케이션 취약성 대응 탐색.

사용 가능한 버전

릴리스 버전	릴리스 정보
Invicti 취약성 통합 v1.1 Invicti 취약성 통합 1.0	Application Vulnerability Response release notes 호환성 정보는 KB0856498 Vulnerability Response 호환성 매트릭스 및 릴리스 스키마 변경을 참조하십시오.

통합

기본 시스템에는 다음과 같은 통합이 포함됩니다. 통합은 하나의 통합이 성공적으로 완료된 후 다음 통합이 시작되도록 체인으로 연결됩니다. 통합은 다음 표에 나열된 순서대로 실행됩니다.

초기 실행 후에는 매일 예약된 작업이 연결되어 이러한 통합을 순서대로 자동으로 실행합니다. 예약된 개별 작업을 수동으로 실행할 수도 있습니다. 예약된 작업은 인스턴스를 다른 취약성 관리 시스템과 동기화된 상태로 유지하여 취약성 정정 수명주기를 단순화합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Invicti 애플리케이션 취약성 통합

통합	설명
Invicti 애플리케이션 목록 애플리케이션	CI 조회 규칙 기록에 대해 시스템 속성이 설정된 방식에 *sn_vul.use_product_model* 따라 Invicti에서 스캔한 애플리케이션을 검색된 애플리케이션〔sn_vul_app_release〕 테이블 또는 스캔한 애플리케이션〔sn_vul_app_scanned_application〕 테이블로 임포트합니다. • 제품 모델 속성을 true로 설정하면 애플리케이션이 검색된 애플리케이션 릴리스 테이블에 삽입됩니다. • 제품 모델 속성이 false로 설정되면 스캔한 애플리케이션 테이블에 애플리케이션이 삽입됩니다. 시스템 속성을 수정하여 CI(구성 항목)를 조회 대상으로 사용하는 조회 규칙을 활성화하도록 선택할 수 있습니다. 수정하는 경우 조회 대상과 일치하도록 CI 조회 규칙도 활성화해야 합니다. 자세한 내용은 다음을 참조하십시오. • Invicti 취약성 통합 구성 • CI 조회 규칙 생성 • 에서 CI 조회 규칙 다시 적용 애플리케이션 취약성 대응
Invicti 스캔 목록 통합	이 통합은 애플리케이션 목록 통합이 성공적으로 완료된 후에 시작됩니다. 이 통합은 스캔이 실행된 날짜 및 시간에 대한 데이터를 임포트합니다.
Invicti 애플리케이션 취약한 항목 통합	이 통합은 스캔 목록 통합이 성공적으로 완료된 후에 시작됩니다. v1.1부터 총 처리 시간, 통합 실행 전 및 사후 프로세스의 평균 시간, 애플리케이션 취약한 항목 통합의 통합 실행 기록에 대한 보고서와 같은 상세 정보를 볼 수 있습니다. Invicti의 각 취약성에는 **DirectoryListing**과 같은 유형이 있습니다. 이 유형은 인스턴스에서 고유 ID로 매핑되고 애플리케이션 취약한 항목(AVI) 기록인 **Invicti-DirectoryListing**의 취약성 필드에 값의 일부로 표시됩니다. 매핑에 대한 자세한 내용은 다음 문서를 참조하십시오 Invicti 취약성 통합 상태 매핑.

세 가지 통합 모두에 대한 페이지당 항목의 상한은 200입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음을 위한 준비 **Invicti** 취약성 통합

성공적인 통합을 위해서는 통합 전 작업을 계획하고 실행해야 합니다. 다음 작업을 수행하여 통합을 준비합니다. Invicti Invicti 취약성 통합 제품 및 API에 익숙하다고 가정합니다.

CWE(일반적인 약점 열거) 통합도 Invicti 취약성 통합을 설치 및 구성하기 전에 사용되며 애플리케이션 취약성 대응 실행되어야 합니다.

주:
NVD(NIST 취약성 데이터베이스) 데이터는 통합을 설치하는 데 필요하지 않지만 취약성 보강을 제공하며 유용합니다.

NVD에 대한 자세한 내용은 문서를 참조하십시오 NVD 및 CWE 통합을 통해 데이터를 임포트하고 외부 공급업체 라이브러리를 관리합니다.

각 통합 기록에 대해 구성된 실행 사용자가 있습니다. 이 사용자의 기본값은 VR입니다. 시스템. 이 값은 변경하지 마십시오.

주:
통합을 실행하기 전에 요구 사항에 따라 필요한 구성을 변경합니다.

임포트하려는 것으로 예상되는 애플리케이션 취약한 항목 수에 따라 인스턴스 크기를 확인합니다. 인스턴스 크기가 작으면 로드 시간이 길어질 수 있습니다. 인스턴스 크기를 모르는 경우 에 문의하십시오 고객 서비스 및 지원. 인스턴스에 애플리케이션을 ServiceNow AI Platform 설치하고 구성하려면 관리자 역할이 필요합니다.

Invicti 콘솔에서 API 자격 증명과 API 토큰을 가져옵니다. Invicti 제품 웹 사이트의 API 개요 에서 사용할 수 있는 정보를 검토합니다.

Invicti와 **ServiceNow® Vulnerability Response** 통합 설치

인스턴스에서 통합을 실행하기 전에 설치 및 구성 단계를 완료 Invicti 취약성 통합 하여 애플리케이션이 .애플리케이션 취약성 대응 이 애플리케이션은 별도의 구독으로 사용할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 설치 Invicti 취약성 통합 하려는 인스턴스에 로그인합니다.
2. ServiceNow Store로 이동합니다.
3. 에서 ServiceNow Store애플리케이션을 검색합니다 Invicti 취약성 통합 .
4. 애플리케이션 타일을 선택합니다.
   설치 중인 애플리케이션에 대한 자세한 정보가 표시됩니다.

   주:
   해당하는 경우 다른 요구 사항 및 종속성 섹션을 읽어보십시오.

5. 요청 앱을 선택하고 로그인 자격 증명을 입력합니다Now Support.
6. 가져오기를 선택합니다.
7. 인스턴스의 인스턴스 이름과이유를 입력하고 인스턴스 확인을 선택합니다.
8. 요청을 선택합니다.
   자세한 설치 지침이 포함된 이메일을 받게 됩니다.
9. 다음으로 이동 모두 〉 시스템 애플리케이션 〉 모든 사용 가능 애플리케이션 〉 모두.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

10. 애플리케이션을 찾아서 선택하고 설치를 선택하여 활성화합니다.
애플리케이션이 인스턴스에 자동으로 설치됩니다.

Invicti 취약성 통합 구성

인스턴스에서 통합을 실행하기 전에 의 기능으로 취약성 대응제대로 작동하도록 애플리케이션 취약성 대응 설치 및 구성 단계를 완료해야 Invicti 취약성 통합 합니다.

시작하기 전에
필요한 역할:

- 애플리케이션을 설치하고 활성화하는 관리자
- 통합을 구성할 App-Sec Manager 사용자 그룹

설치하기 전에 다음 설정 검사 목록을 완료합니다. 이러한 설정 작업은 원활한 설치 및 구성을 위해 필요합니다.

애플리케이션이 설치되고 활성화되었는지 취약성 대응 확인합니다.	이 애플리케이션이 활성화되었는지 확인하려면 다음으로 이동하십시오. 구독 관리 〉 구독 인스턴스에 있습니다. 목록에 조직이 구매한 구독이 표시됩니다. 애플리케이션이 설치 및 활성화되지 않은 경우 을 참조하십시오 취약성 대응 설치.
이(가) Invicti 취약성 통합 설치되고 활성화되었는지 확인합니다.	이 애플리케이션이 활성화되었는지 확인하려면 다음으로 이동하십시오. 구독 관리 〉 구독 인스턴스에 있습니다. 목록에 조직이 구매한 구독이 표시됩니다. 애플리케이션이 설치 및 활성화되지 않은 경우 을 참조하십시오 Invicti와 ServiceNow Vulnerability Response 통합 설치.
인스턴스에 필요한 ServiceNow 역할이 있는지 확인합니다.	예상 결과의 설치, 구성 및 검증에 필요한 역할은 다음과 같습니다. • 아직 할당되지 않은 경우 시스템 관리자 〔admin〕가 앱을 설치하고 사용자를 App-Sec 관리자 그룹에 할당합니다. • App-Sec 관리자는 구성을 감독하고 예상 결과를 검증합니다.
Inviciti 취약성 통합의 경우 사용자 **ID** 와 **API** 토큰을 준비합니다.	사용자 ID 및 API 토큰을 모르는 경우 Invicti 관리자에게 문의하여 사용자 **ID** 및 **API** 토큰을 얻습니다. 자세한 내용은 API 개요 에서 Invicti 제품 웹 사이트를 참조하세요.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 **Invicti** 〉 **Invicti** 구성.
2. 필드를 작성합니다.

필드	설명
API URL	사용자의 Invicti의 인스턴스 URL입니다. 이것은 에서 얻은 다음을 위한 준비 Invicti 취약성 통합정보입니다.
사용자 ID	고유 사용자 ID입니다.
API 토큰	Invicti 콘솔에서 생성한 API 토큰입니다. 이것은 에서 얻은 다음을 위한 준비 Invicti 취약성 통합정보입니다.
스캔 유형을 선택합니다. 하나 이상을 선택해야 합니다.	
DAST 임포트	DAST 검사의 취약성을 포함하는 옵션입니다. DAST 스캔은 애플리케이션이 실행되는 동안 동적으로 취약성을 찾습니다. 이 접근 방식은 외부 공격을 모방할 수 있습니다.
IAST 임포트	IAST 스캔의 취약성을 포함하는 옵션입니다. IAST 스캔은 프로그램이 실행되는 동안 프로그램과 상호 작용하여 소프트웨어 취약성을 탐지합니다. 사람의 관찰, 자동화된 테스트 및 센서가 함께 사용되어 애플리케이션과 상호작용하여 취약성을 찾습니다.
날짜 형식	시작 시간을 Invicti 애플리케이션 취약한 항목 통합에 사용되는 Invicti API에서 지원하는 형식으로 변환하는 매개변수입니다. 이 매개 변수는 Invicti 계정에서 정의하거나 선택한 형식(예: **dd/MM/yyyy**)과 일치해야 합니다. Invicti 콘솔의 날짜 및 시간 형식이 인스턴스의 날짜 형식에 ServiceNow AI Platform 대해 입력한 형식과 일치하는지 확인합니다. Invicti 콘솔에서 이 형식을 변경하려면: **a.** Invicti 로그인 에 로그인합니다. **b.** 오른쪽 상단에서 사용자 이름을 선택합니다. **c.** 다음으로 이동 사용자 설정 〉 날짜 및 시간 형식. 주: 인스턴스에 잘못된 날짜 형식을 입력하면 임포트 실패가 발생할 수 있습니다 ServiceNow AI Platform . 인스턴스에 Invicti 콘솔의 날짜 형식과 다른 유효한 형식을 입력하면 Invicti는 빈 페이로드를 반환합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
ServiceNow에서 예외 관리	다음 중 하나를 선택합니다. 활성화됨(선택됨) 인스턴스에서 지연될 수 있는 **Present** 및 **AcceptedRisk** 와 같은 상태가 있는 Invicti의 애플리케이션 취약 항목(AVIT)은 대신 자동으로 열기 에 매핑됩니다. 비활성화됨(선택하지 않음) Invicti에서 임포트한 AVIT(애플리케이션 취약 항목)에 대한 소스 상태는 유지됩니다. AVIT 기록에서 이러한 AVIT에 대한 예외를 관리(지연)해야 합니다. Invicti 소스 상태 및 대상 필드에 대한 자세한 내용은 다음 문서를 참조하십시오 Invicti 취약성 통합 상태 매핑.
ServiceNow에서 긍정 오류 관리	다음 중 하나를 선택합니다. 활성화됨(선택됨) 인스턴스에서 종결됨으로 전환될 수 있는 현재 및 긍정 오류와 같은 Invicti의 상태가 있는 AVIT는 대신 자동으로 오픈에 매핑됩니다. 비활성화됨(선택하지 않음) Invicti에서 가져온 AVIT 상태는 유지됩니다. AVIT 기록에서 이러한 AVIT에 대한 가양성 또는 잠재적 가양성을 관리해야 합니다.

3. 자격 증명 저장 및 테스트를 선택합니다.
4. 옵션: 구성 항목을 기반으로 하도록 조회 규칙을 수정합니다.

   (Optional) 기본적으로 제품 모델을 기준으로 [sn_sec_cmn_ci_lookup_rule] 테이블에 나열된 조회 규칙에 대해 **sn_vul.use_product_model** 시스템 속성이 활성화됩니다(true로 설정). 이 규칙이 활성화되면 다음을 수행합니다.

   - 이 규칙은 임포트한 데이터와 제품 모델을 기반으로 사용자의 구성 관리 데이터베이스(CMDB) 데이터 간의 일치 항목을 식별합니다.
   - 검색된 애플리케이션 [sn_vul_app_release] 테이블에 기록이 생성되거나 업데이트됩니다.
   - Invicti에 대한 조회 규칙을 생성하거나 편집하면 규칙 양식의 조회 대상 필드에 제품 모델이 표시됩니다.

   구성 항목을 기반으로 하도록 규칙을 수정하려면 **sn_vul.use_product_model** 시스템 속성을 수동으로 비활성화(false로 설정)해야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 다음으로 이동 모두 〉 시스템 속성 을 클릭하고 **sn_vul.use_product_model** 기록을 찾아 값을 false로 설정합니다.

b. 업데이트를 선택합니다.

c. 다음으로 이동 모두 〉 보안 운영 〉 **CMDB** 〉 조회 규칙.

d. 조회 대상이 구성 항목인 애플리케이션 이름 및 소스 애플리케이션 ID 규칙을 찾습니다.

e. 이러한 규칙에 대한 활성 확인란을 선택합니다.

f. 업데이트를 선택합니다.
Invicti에 대한 조회 규칙을 생성하거나 편집할 때 규칙 양식의 조회 대상 필드에 구성 항목이 표시됩니다. 검사한 애플리케이션 〔sn_vul_app_scanned_application〕 테이블에 기록이 생성되거나 업데이트됩니다.

임포트 실행 상태 및 기록 보기 **Invicti** 취약성 통합

취약성 통합 실행 관련 목록을 사용하여 통합 실행의 성공을 확인하고, 문제를 찾고, 정정 결정을 알립니다.

임포트 상태, 임포트 세트 및 기록 보기

임포트 상태를 보려면 App-Sec Manager 사용자 그룹의 사용자로서 모두 〉 **Invicti** 취약성 통합 〉 통합 을 클릭하고 통합 기록을 선택합니다. 취약성 통합 실행 관련 목록을 선택합니다.

v1.1부터 총 처리 시간, 통합 실행 전 및 사후 프로세스의 평균 시간, 애플리케이션 취약한 항목 통합의 통합 실행 기록에 대한 보고서와 같은 상세 정보를 볼 수 있습니다.

임포트 세트를 보려면 다음으로 이동하십시오. 모두 〉 **Invicti** 취약성 통합 〉 통합 〉 임포트 세트 테이블 을 클릭하고 통합을 선택합니다.

애플리케이션 목록 통합은 조회 대상에 따라 기록을 생성하거나 업데이트합니다.

- 제품 모델: 검색된 애플리케이션 [sn_vul_app_release] 테이블
- 구성 항목: 검사한 애플리케이션 [sn_vul_app_scanned_application] 테이블

스캔 목록 통합은 스캔한 애플리케이션 [sn_vul_app_scan_summary] 테이블에 기록을 생성하거나 업데이트합니다.

애플리케이션 취약한 항목 통합은 애플리케이션 취약한 항목 [sn_vul_app_vulnerable_item] 및 CWE [sn_vul_cwe] 테이블에 기록을 생성하거나 업데이트합니다.

주:
Invicti의 각 취약점에는 '유형'(예: ProductDirectoryListing)이 있습니다. 이 유형은 인스턴스에 고유 ID로 매핑되어 임포트되고 AVIT(애플리케이션 취약한 항목) 기록의 취약성 필드에 값의 일부로 표시됩니다. 이 예에서 값은 Invicti-ProductDirectoryListing이며, 이 값은 애플리케이션 취약성 항목 레코드에도 고유 ID로 표시됩니다. Invicti AVIT는 여러 CWE(Common Weakness Enumeration) 항목을 지원하므로 CWE는 고유한 ID로 사용되지 않습니다. CWE는 AVIT 기록에도 표시됩니다.

Invicti AVIT의 경우 Invicti에 취약성에 대한 중복 유형이 있는 경우 값에 '사용자 지정'이라는 단어가 삽입됩니다(예: Invicti-custom-ProductDirectoryListing). 취약성에 대한 사용자 지정 유형을 만드는 경우 취약성 ID는 Invicti-Custom-<title of vulnerability>일 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

새 필드: ## ## = Invicti의 경우 영향을 받는 매개변수 및 사용자 지정 필드에 취약성을 이해하고 해결하는 데 도움이 될 수 있는 데이터가 포함될 수 있습니다. 데이터가 없으면 이러한 필드는 AVIT에 표시되지 않습니다.

Invicti 취약성 통합 상태 매핑

소스 상태의 Invicti 취약성 통합 소스 상태와 인스턴스의 대상 상태가 다음 테이블에 나열됩니다.

Invicti 소스 상태 및 해당 **ServiceNow AI Platform** 상태

Invicti 소스 상태	소스 상태 설명	의 대상 상태 ServiceNow AI Platform
현존	문제가 식별되었습니다.	오픈
존재, 수락된 위험, 부활됨	이 문제가 고려되었으며 저위험 취약성으로 표시됩니다.	연기됨
현재, 긍정 오류	문제가 고려되었으며 진정한 취약성이 아닌 것으로 표시되었습니다.	종결됨
고정 미확인, 고정 미확인	이 문제는 수정되었지만 Invicti Enterprise에서 확인하지 않았습니다.	해결 일시
고정(확인됨), FixedConfirmed, FixedConfirmed, AcceptedRisk, FixedConfirmed, False Positive	이 문제는 Invicti Enterprise에 의해 수정 및 확인되었으며 추가 조치가 필요하지 않습니다.	종결됨
수정됨(다시 테스트할 수 없음)	문제가 식별되었지만 Invicti는 문제가 해결되었는지 여부를 확인하기 위해 다시 테스트할 수 없습니다.	해결 일시
부활	이 문제는 이전 검사에서 수정되었지만 다시 발견되었습니다.	오픈
지연됨, 무시됨	사용자가 문제를 무시했습니다. Invicti Enterprise에서 문제를 무시하기 위해 사용자는 상태를 "수락된 위험"으로 업데이트합니다.	위험 수락됨

애플리케이션 릴리스 매핑

소스 필드	대상 필드 ServiceNow AI Platform
ID	source_app_id
CreatedAt	app_creation_date
UpdatedAt	app_updation_date
이름	app_name
RootUrl	Source_additional_info
설명	설명
태그	태그

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약성 매핑

소스 필드	대상 필드 ServiceNow AI Platform
유형	범주 이름
취약성 상세 정보	요약
영향도	위협
소스 참조	웹 참조
소스 권장 사항	솔루션
유형	source_entry_id/ID
심각도	source_severity
분류["Cwe"]	CWE 목록
Cvss벡터 문자열	CVVS v3 필드

검사 요약 매핑

소스 필드	대상 필드
소스	소스
TotalVulnerabilityCount	Detected_flaw_count
개시 날짜	동적 검사 날짜
ID	source_scan_id

AVIT(애플리케이션 취약한 항목) 매핑

소스 필드	대상 필드 ServiceNow AI Platform
유형	스캔 유형
웹 사이트 ID	소스 앱 ID
ID	소스 AVIT ID
마지막으로 본 날짜	마지막 발견
처음 본 날짜	첫 발견
마지막 업데이트 날짜	마지막 검사 날짜
parameters	영향을 받는 매개변수
URL	영향을 받는 URL
심각도	소스 심각도
URL	소스 링크
취약성 상세 정보	소스 취약성 요약
외부 참조	소스 참조
Remedy + Remedy 참조	소스 권장 사항
상태	소스 정정 상태

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

영향도	소스 취약성 설명

Veracode Vulnerability Integration

애플리케이션과의 Veracode 통합은 취약성 대응Veracode 제품에서 임포트한 데이터를 사용하여 코드 내 결함의 영향과 우선순위를 파악하는 데 도움을 줍니다.

Veracode Vulnerability Integration

이 Veracode 제품은 DAST(동적 애플리케이션 보안 테스트), SAST(정적 애플리케이션 보안 테스트) 및 수동 스캐너 데이터를 수집하고 해당 데이터를 ServiceNow AI Platform#. 타사 취약성을 매핑하는 기능과 취약성 대응 쉽게 통합되어 애플리케이션 취약성 대응 인스턴스의 데이터를 보강합니다.

의 취약성 대응v19.0부터 소프트웨어 애플리케이션의 약점을 식별하는 데 도움이 되는 소프트웨어 구성 분석(SCA) 취약성 및 소프트웨어 자재 명세서 (SBOM) 취약성 데이터를 임포트할 수 있습니다. 자세한 내용은 소프트웨어 자재 명세서 탐색 문서를 참조하십시오.

공유 API는 DAST, SAST, SCA 데이터 및 수동 침투 테스트 결과를 수집합니다.

각 통합 기록에 대해 구성된 실행 사용자가 있습니다. 이 사용자의 기본값은 VR입니다. 시스템. 이 값은 변경하지 마십시오.

매일 예약된 작업은 나열된 순서대로 통합을 자동으로 호출합니다. 예약된 개별 작업을 수동으로 실행할 수도 있습니다. 예약된 작업은 인스턴스를 다른 취약성 관리 시스템과 동기화된 상태로 유지하여 취약성 정정 수명주기를 단순화합니다.

에서 자세한 내용 가져오기 **Veracode**

v4.2부터 애플리케이션 취약 항목[sn_vul_app_vulnerable_item] 테이블 또는 취약성 대응 작업 공간의 목록 뷰에서 소스로 있는 Veracode 애플리케이션 취약 항목(AVIT)에 대한 상세 정보 가져오기를 선택하여 다음 Veracode 데이터를 확인합니다.

- 동적 애플리케이션 보안 테스트(DAST) 스캔에 대한 HTTP 소스 요청 및 소스 응답 상세 정보가 HTTP 요청/응답 관련 목록에 표시됩니다.
- Veracode의 솔루션 권장 사항이 결과 관련 목록에 표시됩니다.
- HTTP 소스 요청, 소스 응답 및 권장 사항이 취약성 대응 취약성 대응 작업 공간의 상세 정보 탭에 표시됩니다.
- 설명 열은 애플리케이션 취약 항목 [sn_vul_app_vulnerable_item] 테이블에서 지원됩니다.

사용 가능한 버전

릴리스 버전	릴리스 정보
Veracode v4.3 Veracode v4.2 Veracode v4.1	Application Vulnerability Response release notes 호환성 정보는 KB0856498 Vulnerability Response 호환성 매트릭스 및 릴리스 스키마 변경을 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용자 그룹 및 역할

는 Veracode Vulnerability Integration 시스템 관리자(admin)가 설치하고 App-Sec Manager 그룹의 구성원이 구성합니다. 자세한 내용은 애플리케이션 취약성 대응 사용자 그룹 및 역할 문서를 참조하십시오.

Veracode Vulnerability Integration

취약성 통합을 보려면 Veracode 다음으로 이동하십시오. 모두 〉 **Veracode Vulnerability Integration** 〉 통합.

기본 시스템에는 다음과 같은 통합이 포함됩니다.

Veracode Vulnerability Integration

통합	설명
v4.1부터: Veracode 프로젝트 연결 통합	이 통합은 기본적으로 활성화됩니다. 에서 각 애플리케이션에 Veracode대해 연결된 모든 프로젝트를 검색합니다. 애플리케이션의 애플리케이션에 여러 프로젝트가 Veracode 있을 수 있습니다. 이 통합에서 임포트한 데이터는 다음 기록에 표시됩니다. • 마지막 **SCA** 검사 날짜, 앱 생성 날짜 및 앱 업데이트 날짜가검색된 애플리케이션의 기록에 나열됩니다. • 애플리케이션 취약성 검사 요약 기록 및 애플리케이션 취약 항목(AVIT)에 소스 **SDLC** 상태 (소프트웨어 개발 수명 주기)가 표시됩니다. • 소스 악용 가능성 은 애플리케이션 취약한 항목(AVI) 기록에 표시됩니다.
Veracode 애플리케이션 목록 통합 (JSON)	이 통합은 기본적으로 비활성 상태입니다. 애플리케이션 스캐너 데이터(취약성, 메타데이터)를 검색하고 Veracode 애플리케이션 데이터를 보강합니다. JSON 기반 API를 Veracode 통해 스캔 기록을 검색합니다.
Veracode 애플리케이션 목록 통합 (XML)	이 통합은 기본적으로 비활성 상태입니다. 이 통합의 XML 기반 버전이 비활성화되었습니다(사용하지 않음). 애플리케이션 스캐너 데이터(취약성, 메타데이터)를 검색하고 Veracode 애플리케이션 데이터를 보강합니다. 이 통합은 매일 00:00:00에 실행되도록 설정됩니다. 주: JSON 기반 API Veracode 는 애플리케이션 목록을 검색하는 데 사용됩니다. 이 API는 이러한 애플리케이션에 대한 "마지막 정책 준수 검사 날짜"를 임포트하여 이러한 애플리케이션이 에서 마지막으로 검사 Veracode된 시기를 나타냅니다.
Veracode 소프트웨어 자재 명세서 (SBOM) 통합	버전 4.3 Veracode Vulnerability Integration 에는 다음과 같은 Veracode SBOM 파일 개선 사항이 포함되어 있습니다. • SBOM Response를 설치한 경우 업로드하는 SBOM 파일에 대해 Veracode 발견된 취약성을 포함할 수 있습니다. • Veracode 이(가) SBOM 파일에 대한 자재 명세서[sn_sbom_doc] 테이블에 있는 기록의 소스 필드에 매핑됩니다 Veracode . 이 통합은 기본적으로 활성화됩니다. v4.2부터 생성된 Veracode CycloneDX 및 SPDX 형식의 파일을 임포트 소프트웨어 자재 명세서 하고 인스턴스에서 구문

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Veracode Vulnerability Integration

통합	설명
	분석하기 위해 큐에 대기합니다. 이 데이터를 임포트하고 보려면 애플리케이션이 설치되어 있어야 합니다 소프트웨어 자재 명세서 .
Veracode 검사 요약 통합(JSON)	이 통합은 기본적으로 비활성 상태입니다. JSON 기반 API를 Veracode 통해 스캔 기록을 검색합니다. 이 통합은 XML 기반 API 통합을 대체합니다. 이 플러그인은 체인으로 연결되고 활성화되면 애플리케이션 목록 통합을 따릅니다 Veracode .
Veracode 검사 요약 (XML)	이 통합은 기본적으로 비활성 상태입니다. 이 통합의 XML 기반 버전이 비활성화되었습니다(사용하지 않음). 에서 스캔 기록을 조회합니다 Veracode. 이 통합은 연결되며 활성화되면 애플리케이션 목록 통합을 따릅니다 Veracode . 주: 활성화될 때 애플리케이션 목록 통합을 자동으로 따릅니다 Veracode . 의 Veracode애플리케이션에 대한 "마지막 정책 준수 확인 날짜"를 사용하여 이 통합은 이 통합의 "delta_start_time" 후에 스캔된 애플리케이션에 대해서만 데이터를 검색합니다.
Veracode 애플리케이션 취약한 항목 JSON 통합	v4.2부터 총 처리 시간, 사전 및 사후 통합 실행 프로세스의 평균 시간과 같은 상세 정보, 애플리케이션 취약한 항목 통합에 대한 통합 실행 기록에 대한 보고서를 볼 수 있습니다. 이 통합은 기본적으로 비활성 상태입니다. 에서 XML 기반 통합 Veracode보다 더 많은 취약성 데이터가 포함된 검사 결과를 검색합니다. AVI를 삽입하고 외부 공급업체 취약성 데이터를 보강합니다.
Veracode 애플리케이션 취약한 항목 통합(XML)	v4.2부터 총 처리 시간, 사전 및 사후 통합 실행 프로세스의 평균 시간과 같은 상세 정보, 애플리케이션 취약한 항목 통합에 대한 통합 실행 기록에 대한 보고서를 볼 수 있습니다. 이 통합은 기본적으로 비활성 상태입니다. 에서 Veracode검사 결과를 검색하고 AVIT(애플리케이션 취약한 항목)를 삽입하며 외부 공급업체 취약성 데이터를 보강합니다. 기본적으로 스캐너 기록이 종결 상태인 경우 AVIT가 생성되지 않습니다. 기존 AVIT는 여전히 업데이트됩니다. 이 통합은 연결되며 활성화되면 검사 요약 통합을 따릅니다 Veracode . XML 기반 API는 검사 요약 JSON 통합에 Veracode 사용되지 않습니다. 주: 은 Veracode 검사 요약 통합을 자동으로 따릅니다. 의 Veracode애플리케이션에 대한 "마지막 정책 준수 확인 날짜"를 사용하여 이 통합은 이 통합의 "delta_start_time" 후에 스캔된 애플리케이션에 대해서만 데이터를 검색합니다.
Veracode 범주 통합	이 통합은 기본적으로 비활성 상태입니다. 에서 Veracode향상된 범주 데이터를 검색합니다.
Veracode CWE 통합	이 통합은 기본적으로 활성화됩니다. 위협 정보 및 정정 권장 사항에 대한 특정 CWE(일반적인 약점 열거) 데이터를 검색합니다 Veracode . 이러한 데이터는 애플리케이션 취약성 항목 기록에서 채워지고 업데이트됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Veracode Vulnerability Integration

통합	설명
	이 CWE 통합은 애플리케이션에 대해 활성화하는 CWE Comprehensive 2000 Integration의 취약성 대응 예약된 작업과는 독립적으로 작동합니다. CWE 통합 및 CWE Comprehensive 2000 통합이 Veracode 활성화되어 있으면 데이터가 복제되지 않습니다.
Veracode DevOps 통합	이 통합은 기본적으로 비활성 상태입니다. 통합은 의 애플리케이션 취약성 대응애플리케이션 취약성 통합 목록에서 볼 수 있습니다. DevOps 변경 속도 라이센스가 있는 경우 이 기능은 DevOps 사용자가 타사 취약성 검사에 대한 요약 상세 정보를 보기 위해 SecOps 라이센스가 없어도 사용할 수 있도록 구성되어 있습니다. 에 애플리케이션 취약성 대응대한 영향이나 변경 사항은 없습니다.

통합 실행 상태는 문서를 참조하십시오 Veracode 애플리케이션 취약성 통합 임포트 실행 상태 보기.

외부 공급업체 취약성의 데이터를 보려면 을 참조하십시오 취약성 라이브러리 보기.

준비 중 **Veracode Vulnerability Integration**

성공 Veracode Vulnerability Integration 하려면 통합 전 작업의 계획과 실행이 필요합니다. 다음 작업을 수행하여 통합을 준비합니다. 여기서는 Veracode Vulnerability Integration 사용자가 제품과 API에 Veracode 익숙하다고 가정합니다.

시작하기 전에
CWE(Common Weakness Enumeration) 통합도 에서 애플리케이션 취약성 대응 사용되며 를 설치 및 구성 Veracode Vulnerability Integration하기 전에 실행해야 합니다. 기본적으로 와 함께 취약성 대응설치됩니다.

주:
NVD(NIST 취약성 데이터베이스) 데이터는 애플리케이션 취약성 통합을 설치하는 Veracode 데 필요하지 않지만 보강 기능을 제공하므로 보유하면 유용할 것입니다. NVD에 대한 자세한 내용은 문서를 참조하십시오 NVD 및 CWE 통합을 통해 데이터를 임포트하고 외부 공급업체 라이브러리를 관리합니다.

각 통합 기록에 대해 구성된 실행 사용자가 있습니다. 이 사용자의 기본값은 VR입니다. 시스템. 이 값은 변경하지 마십시오.

필요한 역할: App-Sec 관리자 그룹

이 태스크 정보
주:
통합을 실행하기 전에 요구 사항에 따라 필요한 구성을 변경합니다.

임포트하려는 것으로 예상되는 애플리케이션 취약한 항목 수에 따라 인스턴스 크기를 확인합니다. 인스턴스 크기가 작으면 로드 시간이 길어질 수 있습니다. 인스턴스 크기를 모르는 경우 에 문의하십시오 고객 서비스 및 지원.

Veracode Vulnerability Integration API ID와 API 키가 필요합니다.

프로시저

API ID 및 키 자격 증명을 작성하려면 다음을 수행하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 플랫폼에 로그인합니다 Veracode .

b. 사용자 계정 메뉴로 이동하여 **API** 자격 증명을 선택합니다.

c. **API** 자격 증명 생성을 클릭합니다.

d. 나중에 사용할 수 있도록 자격 증명을 기록합니다.

ServiceNow® 와 **Vulnerability Response** 통합 설치**Veracode**

인스턴스에서 통합을 실행하기 전에 설치 및 구성 단계를 완료 Veracode 하여 제품이 .애플리케이션 취약성 대응 이 애플리케이션은 별도의 구독으로 사용할 수 있습니다.

시작하기 전에

설치하기 전에 다음 설정 검사 목록을 완료합니다. 이러한 설정 작업은 원활한 설치 및 구성을 위해 필요합니다.

주:
이 프로세스는 프로덕션 인스턴스에 다운로드된 애플리케이션에만 적용됩니다. 애플리케이션을 비프로덕션 또는 개발 인스턴스에 다운로드하는 경우에는 권리를 얻을 필요가 없습니다. 로 애플리케이션 활성화 ServiceNow Store계속 진행합니다.

작업 설정	설명
애플리케이션이 설치되고 활성화되었는지 취약성 대응 확인합니다.	이 애플리케이션이 활성화되었는지 확인하려면 다음으로 이동하십시오. 구독 관리 〉 구독 인스턴스에 있습니다. 목록에 조직이 구매한 구독이 표시됩니다. 애플리케이션이 설치 및 활성화되지 않은 경우 을 참조하십시오 취약성 대응 설치.
인스턴스에 필요한 ServiceNow 역할이 있는지 확인합니다.	예상 결과의 설치, 구성 및 검증에 필요한 역할은 다음과 같습니다. • 아직 할당되지 않은 경우 시스템 관리자 〔admin〕가 애플리케이션을 설치하고 사용자를 App-Sec Manager 그룹에 할당합니다. 그룹 역할에 대한 자세한 내용은 문서를 참조하십시오 애플리케이션 취약성 대응 사용자 그룹 및 역할. • App-Sec 관리자 그룹은 구성을 감독하고 예상 결과를 검증합니다.

필요한 역할: 관리자

프로시저

1. 설치 Veracode Vulnerability Integration 하려는 인스턴스에 로그인합니다.

2. ServiceNow Store로 이동합니다.

3. ServiceNow Store에서 애플리케이션과 취약성 대응 통합을 Veracode 검색합니다.

4. 애플리케이션 타일을 클릭합니다.
설치 중인 애플리케이션에 대한 자세한 정보가 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
해당하는 경우 다른 요구 사항 및 종속성 섹션을 읽어보십시오.

5. 앱 요청을 클릭하고 Now Support 로그인 자격 증명을 입력합니다.
6. 가져오기를 클릭합니다.
7. 인스턴스 이름 및 인스턴스 이유를 입력하고 인스턴스 확인을 클릭합니다.
8. 요청을 클릭합니다.
   자세한 설치 지침이 포함된 이메일을 받게 됩니다.
9. 다음으로 이동 시스템 애플리케이션 〉 애플리케이션.
10. 애플리케이션을 찾아서 선택한 다음 설치를 클릭합니다.
    애플리케이션이 인스턴스에 자동으로 설치됩니다.

다음에 수행할 작업
사용자 환경에 맞게 구성합니다 Veracode Vulnerability Integration . Veracode Vulnerability Integration 구성 문서를 참조하십시오.

Veracode Vulnerability Integration 구성

인스턴스에서 통합을 실행하기 전에 설치 및 구성 단계를 완료 Veracode 하여 제품이 .애플리케이션 취약성 대응 이 애플리케이션은 별도의 구독으로 사용할 수 있습니다.

시작하기 전에
설치하기 전에 다음 설정 검사 목록을 완료합니다. 이러한 설정 작업은 원활한 설치 및 구성을 위해 필요합니다.

주:
이 프로세스는 프로덕션 인스턴스에 다운로드된 애플리케이션에만 적용됩니다. 애플리케이션을 비프로덕션 또는 개발 인스턴스에 다운로드하는 경우에는 권리를 얻을 필요가 없습니다. 로 애플리케이션 활성화 ServiceNow Store계속 진행합니다.

작업 설정	설명
애플리케이션이 설치되고 활성화되었는지 취약성 대응 확인합니다.	이 애플리케이션이 활성화되었는지 확인하려면 다음으로 이동하십시오. 구독 관리 〉 구독 인스턴스에 있습니다. 목록에 조직이 구매한 구독이 표시됩니다. 애플리케이션이 설치 및 활성화되지 않은 경우 을 참조하십시오 취약성 대응 설치.
애플리케이션과의 Veracode 통합이 취약성 대응 설치되고 활성화되었는지 확인합니다.	이 애플리케이션이 활성화되었는지 확인하려면 다음으로 이동하십시오. 구독 관리 〉 구독 인스턴스에 있습니다. 목록에 조직이 구매한 구독이 표시됩니다. 애플리케이션이 설치 및 활성화되지 않은 경우 을 참조하십시오 ServiceNow 와 Vulnerability Response 통합 설치Veracode.
인스턴스에 필요한 ServiceNow 역할이 있는지 확인합니다.	구성 및 예상 결과 검증에 필요한 역할은 다음과 같습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업 설정	설명
	• 아직 할당되지 않은 경우 시스템 관리자(admin)가 앱을 설치하고 사용자를 App-Sec Manager 사용자 그룹에 할당합니다. • App-Sec 관리자는 구성을 감독하고 예상 결과를 검증합니다.
애플리케이션 취약성 통합의 Veracode 경우 **API ID** 와 **API** 키를 준비합니다.	**API ID** 및 **API** 키를 얻으려면 연락처에 문의하십시오Veracode. 준비 중 Veracode Vulnerability Integration 문서를 참조하십시오. 버전 4.0부터 를 사용하는 Veracode Vulnerability Integration경우 의 침투 평가 테스트는 Veracode Vulnerability Integration 의 수동 결과 Veracode입니다. 이러한 결과는 에서 애플리케이션 취약성 대응구성하는 침투 테스트 평가 요청과 연결되지 않습니다. 의 애플리케이션 취약성 대응침투 테스트 요청에 대한 자세한 내용은 문서를 참조하십시오 침투 테스트 구성.

필요한 역할: App-Sec 관리자 사용자 그룹

프로시저

1. 다음으로 이동 모두 〉 **Veracode Vulnerability Integration** 〉 구성.
2. **API ID** 및 **API** 키 필드를 입력합니다.
3. 테스트 결과를 선택합니다.

옵션	설명
버전 4.0:	**a.** 임포트에 포함할 **DAST** 또는 **SAST** 데이터 유형을 선택합니다. 주: 둘 중 하나 또는 둘 다를 선택할 수 있지만 하나 이상을 선택해야 합니다. **b.** SCA(소프트웨어 구성 분석) 취약성을 임포트하려면 **SCA** 를 선택합니다. **c.** 에서 수동 침투 테스트 결과를 Veracode임포트하려면 수동 포함을 선택합니다. 이러한 결과에 대해 AVIT가 생성됩니다.
버전 3.0	임포트에 포함할 **DAST** 또는 **SAST** 데이터 유형을 선택합니다. 주: 둘 중 하나 또는 둘 다를 선택할 수 있지만 하나 이상을 선택해야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵션	설명
버전 1.0:	동적 애플리케이션 보안 테스트 결과가 기본적으로 선택됩니다.

4. Veracode 심각도 수준을 추가하여 임포트한 데이터를 필터링합니다.
   이 값은 다음에서 Veracode임포트됩니다. 필드에 여러 값을 추가할 수 있습니다. 채워지면 임포트는 추가한 심각도 수준과 일치하는 데이터만 수집합니다.
5. 선택 사항을 저장하고 확인합니다.

옵션	설명
버전 3.0:	자격 증명 저장 및 테스트를 클릭합니다. 주: 오류 메시지가 표시되지 않는 한 구성이 성공적으로 완료된 것입니다. 구성 중에 오류 메시지가 표시되면 데이터를 다시 입력합니다.
버전 1.0:	저장을 클릭합니다. 자격 증명 테스트를 클릭하여 구성이 올바른지 확인합니다. 주: 오류 메시지가 표시되지 않는 한 구성이 성공적으로 완료된 것입니다. 구성 중에 오류 메시지가 표시되면 데이터를 다시 입력합니다.

6. 임포트 시 AVIT에 대한 예외 및 가양성을 관리하는 방법을 선택합니다.
   예외 관리 및 긍정 오류 워크플로우를 사용하여 임포트 시 AVIT를 ServiceNow 관리하는 옵션이 기본적으로 활성화됩니다. 워크플로우는 AVIT의 소스 상태가 인스턴스에서 매핑되는 방식에 따라 트리거됩니다. 사용 사례 예제는 다음 문서를 에서 지연 및 긍정 오류에 대한 상태 매핑 관리 애플리케이션 취약성 대응참조하십시오.
7. v4.3부터 다음 매개 변수에 대한 설정을 선택하거나 확인합니다.
8. 자격 증명 저장 및 테스트를 선택합니다.

다음에 수행할 작업
환경에 도메인 분리 가져오기가 필요한 경우 문서를 참조하십시오 통합을 위해 도메인 분리 임포트 작성.

초기 설치 시 추가 지침을 참조하십시오 애플리케이션 취약성 대응 구성 .

초기 설치 후 수정 사항은 를 Veracode Vulnerability Integration 수정 및 활동참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Veracode 애플리케이션 취약성 통합 임포트 실행 상태 보기

취약성 통합 실행 관련 목록을 사용하여 통합 실행의 성공을 확인하고, 문제를 찾고, 정정 결정을 알립니다.

시작하기 전에

임포트 실행 상태를 보려면 Veracode Vulnerability Integration 다음을 수행합니다.

- 애플리케이션 취약성 대응 그리고 설치하고 Veracode Vulnerability Integration 구성해야 합니다.
- 임포트가 Veracode Vulnerability Integration 예약되어 실행 중이어야 합니다.

필요한 역할: App-Sec 관리자 그룹

이 태스크 정보

통합 실행 중에 여러 프로세스가 생성되고 데이터가 페이지 형식으로 수신됩니다. 각 프로세스에는 페이지에 첨부된 데이터가 있는 하나 이상의 임포트 큐 항목이 포함될 수 있습니다. 이러한 항목은 1시간의 시간 제한 내에 데이터를 처리해야 합니다. 그러나 페이로드 크기가 크면 처리 시간이 1시간을 초과하거나 중단되어 통합 시간 제한 오류가 발생할 수 있습니다. 통합은 시간 초과 오류에도 불구하고 데이터를 계속 처리합니다. 이러한 잘못된 통신을 피하기 위해 버전 18.2.4 애플리케이션 취약성 대응부터 큐가 활성 상태이고 데이터를 처리하는지 여부를 나타내기 위해 타임스탬프(하트비트)가 주기적으로 전송됩니다. 임포트 큐 항목 페이지의 처리된 마지막 기록 필드는 임포트 큐가 생성하거나 업데이트하는 기록 수에 따라 업데이트됩니다. 임포트 큐 항목이 1시간의 시간 제한을 초과하는 경우, 시스템은 마지막으로 처리된 기록 필드를 검사하여 1시간보다 오래되었는지도 확인합니다. 이 경우 이는 임포트 큐 항목이 고착되었음을 나타내며 처리 시 더 이상의 지연을 방지하기 위해 시간 초과됩니다.

주:
마지막으로 처리된 기록 필드는 다음 시스템 속성에 정의된 내용에 따라 업데이트됩니다.

- *sn_sec_cmn.record_threshold_heartbeat*: 하트비트(타임스탬프)가 임포트 큐 항목으로 전송된 후 처리된 기록 수를 정의합니다.
- *sn_sec_cmn.maximum_heartbeat_delay*: 임포트 큐 항목을 시간 초과해야 하는 시간을 정의합니다.

프로시저

1. 〔store-future: BEGIN review〕통합 실행 상태 차트를 〔End〕 다음으로 이동합니다. 모두 〉 **Veracode Vulnerability Integration** 〉 통합.
2. 통합을 선택합니다.
3. 취약성 통합 실행 관련 목록을 클릭합니다.
4. 모든 임포트가 성공했는지 확인합니다.

   Trouble?

   실행 실패의 가장 일반적인 원인은 다음과 같습니다.

   ○ 네트워크 중단.

   ○ 데이터 전송 문제로 인해 변환 중에 데이터가 손상되었습니다.
   이러한 조건이 발생하면 지금 실행을 클릭하고 통합을 다시 실행합니다.
5. v4.2부터 총 처리 시간, 사전 및 사후 통합 실행 프로세스의 평균 시간과 같은 상세 정보, 애플리케이션 취약한 항목 통합의 통합 실행 기록에 대한 보고서를 볼 수 있습니다.
   에서 임포트한 Veracode추가 상세 정보를 보는 방법에 대한 자세한 내용은 을 참조하십시오 Veracode Vulnerability Integration.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

검사 요약 보기 **Veracode**

취약성 통합에 대한 Veracode 검사 요약 정보에 대한 상세 정보를 봅니다.

시작하기 전에
필요한 역할: App-Sec 관리자 그룹

프로시저

1. 애플리케이션 취약성 검사 요약 〔sn_vul_app_vul_scan_summary_list〕 테이블로 이동합니다.
2. 스캔할 Veracode 기록을 선택합니다.
3. Veracode 취약성 통합 v19.0 취약성 대응 및 v4.0부터 목록 개인화 아이콘(기어 아이콘)을 사용하여 다음 열을 표시합니다.
   - 정적 검사 크기
   - 외부 공급업체 라이브러리 수
   - 외부 공급업체 취약성 라이브러리 수
   - 심각도별 외부 공급업체 결함 수
   - 외부 공급업체 라이브러리 문제 수
   - 외부 공급업체 라이센스 문제 수
   - 혼합 결함 수
   - 완화된 결함 수
   - 완화되지 않은 결함 수
   - 심각도별 정직 결함 수
   - 심각도별 새 결함 수
   - 심각도별 완화되지 않은 결함 수
   - 심각도별 총 결함 수
   - 마지막 SCA 검사 등급
   - 마지막 SCA 검사 날짜
   - 게시된 날짜 검사
   - 태그

취약성 통합을 위한 **Veracode** 데이터 변환

임포트할 데이터를 식별하면 애플리케이션에서 데이터가 검색 Veracode 되어 데이터 소스 세트를 통해 처리되고 인스턴스에서 변환됩니다.

Veracode 애플리케이션 취약한 항목 통합

API의 데이터는 먼저 AppVul 항목 임포트[sn_vul_veracode_appvul_item_import] 테이블에 로드 Veracode 되고 Veracode AppVul 항목 변환을 사용하여 임포트된 정보를 변환합니다.

이 변환 맵에 액세스하려면 AppVul 항목 변환으로 *System Import Sets > Transform Maps* 이동하여 검색합니다 Veracode . 다음 표에는 통합별 변환 맵 필드가 나열되어 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Veracode AppVul 항목 변환 맵 필드

소스 필드	대상 필드	설명
app_id	source_app_id	애플리케이션 ID입니다.
문제 ID	source_avit_id	AVIT ID입니다.
app_name	app_name	애플리케이션 이름입니다.
버전	app_version	애플리케이션 버전입니다.
build_id	source_scan_id	애플리케이션의 빌드 ID입니다.
account_id	account_id	계정 ID
sandbox_id	sandbox_id	샌드박스 ID입니다.
last_update_time	last_scan_date	마지막 업데이트 시간입니다.
app_name + last_scan_date	scan_summary_name	검사 요약입니다.
life_cycle_stage	source_sdlc_status	소스 SDLC 상태입니다.
수준	source_severity	소스 심각도
category_name	범주	범주입니다.
source_severity	source_severity	소스 심각도
category_id + " CWE-" + cweId	source_entry_id	소스 항목 ID입니다.
source_vulnerability_summary	source_vulnerability_summary	소스 취약성 요약.
source_recommendation	source_recommendation	소스 권장 사항.
설명	설명	소스의 설명입니다.
설명	source_vulnerability_explanation	소스 취약성 설명.
mitigation_status_desc	source_mitigation_status	소스 완화 상태입니다.
remediation_status	source_remediation_status	소스 정정 상태입니다.
라인	line_number	결함이 발견된 선입니다.
모듈	application_module	애플리케이션 모듈입니다.
소스 파일	source_notes	출처 메모.
affects_policy_compliance	complies_with_policy	소스 정보가 true 또는 false인지에 따라 값이 Yes 또는 No가 될 수 있습니다.
소스 파일 경로 + 소스 파일	위치	결함이 있는 경우 위치 매핑.`static`
URL	위치	결함이 있는 경우 위치 매핑.`dynamic`
범위, 유형, exploitLevel	source_additional_info	정적 결함이 있는 경우 소스의 값으로 채워진 이름 값 필드입니다.

변환 프로세스 중에 다음 변환 스크립트가 실행됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Veracode 변환 맵 스크립트 타이밍 및 목적

스크립트가 실행될 때	목적
onComplete(임포트 세트가 변환을 완료한 경우)	데이터 소스를 처리하고 생성, 업데이트 또는 변경되지 않은 AVIT 수와 에서 이 통합의 일부로 임포트된 AVIT 수를 업데이트하는 데 사용되는 스크립트입니다 Veracode. 이 스크립트는 내부용이며 수정하거나 삭제하면 안 됩니다.

Veracode Vulnerability Integration 수정 및 활동

특히 에 대한 Veracode Vulnerability Integration선택적 수정 사항을 구성합니다.

에서 임포트한 추가 데이터 보기 Veracode Vulnerability Integration

주:
여기에 나열된 설정 이외의 다른 Veracode Vulnerability Integration 설정을 변경하려면 고급 ServiceNow 전문 애플리케이션 취약성 대응 지식이 필요하며 이는 제품 설명서에서 다루지 않습니다.

에서 자세한 내용 가져오기 Veracode

v4.2부터 애플리케이션 취약 항목[sn_vul_app_vulnerable_item] 테이블 또는 취약성 대응 작업 공간의 목록 뷰에서 소스로 있는 Veracode 애플리케이션 취약 항목(AVIT)에 대한 상세 정보 가져오기를 선택하여 다음 Veracode 데이터를 확인합니다.

- 동적 애플리케이션 보안 테스트(DAST) 스캔에 대한 HTTP 소스 요청 및 소스 응답 상세 정보가 HTTP 요청/응답 관련 목록에 표시됩니다.
- Veracode의 솔루션 권장 사항이 결과 관련 목록에 표시됩니다.
- HTTP 소스 요청, 소스 응답 및 권장 사항이 취약성 대응 취약성 대응 작업 공간의 상세 정보 탭에 표시됩니다.
- 설명 열은 애플리케이션 취약 항목 [sn_vul_app_vulnerable_item] 테이블에서 지원됩니다.

통합 인스턴스 매개변수 수정 Veracode

초기 설치 후 통합 인스턴스에서 통합에 대한 Veracode 매개변수를 수정할 수 있습니다 Veracode .

시작하기 전에
필요한 역할: App-Sec 관리자 그룹

이 태스크 정보
인스턴스에서 통합에 대한 매개변수를 수정하여 수집할 데이터 유형을 결정할 수 있습니다. 이러한 설정 중 일부의 경우 통합의 구성 페이지에서 이러한 매개변수를 수정할 수도 있습니다.

프로시저

1. 다음으로 이동 모두 〉 애플리케이션 취약성 대응 〉 관리 〉 통합.
2. 수정하려는 통합에 Veracode 대해 소스 인스턴스 열에서 **Veracode** 애플리케이션 취약성을 선택합니다.
3. 통합 인스턴스 매개변수 탭을 선택하고 값 열의 필드를 두 번 클릭하여 값을 수정합니다.

   의 취약성 대응 v19.0 및 의 Veracode Vulnerability Integrationv4.0부터 통합에 대해 다음 매개변수를 구성할 수 있습니다 Veracode .

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

수동 임포트

##Veracode수동 침투 테스트 결과를 임포트하려면 true를 입력합니다. 통합 구성 페이지에서 이 값을 수정할 수도 있습니다.

침투 평가 테스트는 Veracode Vulnerability Integration 의 수동 결과 Veracode입니다. 이러한 결과는 에서 애플리케이션 취약성 대응구성하는 침투 테스트 평가 요청과 연결되지 않습니다. 의 애플리케이션 취약성 대응침투 테스트 요청에 대한 자세한 내용은 문서를 참조하십시오 침투 테스트 구성.

import_sca

SCA(소프트웨어 구성 분석) 취약성을 임포트하려면 true 를 입력합니다. 통합 구성 페이지에서 이 값을 수정할 수도 있습니다.

상태

원하는 상태의 결과를 임포트하려면 ## 또는 ## 됨을 입력합니다. 이 필드를 비워 두면 통합에서 열림 상태와 종결됨 상태 모두에 대한 결과를 임포트합니다.

policy_sandbox

정책 또는 샌드박스에 해당하는 기록을 임포트하려면 ## 이나 #### 를 입력합니다. 이러한 기록은 사용자 환경에서 애플리케이션을 테스트하는 방법과 관련이 있을 수 있습니다.

policy_rule_passed

정책 규칙을 통과한 기록을 임포트하려면 true 또는 false 를 입력합니다. 이러한 기록은 사용자 환경에서 애플리케이션을 테스트하는 방법과 관련이 있을 수 있습니다.

4. 업데이트를 선택하여 변경 내용을 저장합니다.

수동 **Veracode** 애플리케이션 취약성 임포트 수행

초기 임포트에 실패했거나 예약된 초기 임포트를 기다리지 않으려면 매일 예약된 작업과 관계없이 전체 데이터 임포트를 수행할 수 있습니다.

시작하기 전에
필요한 역할: App-Sec 관리자 그룹

프로시저

1. 다음으로 이동 모두 〉 **Veracode Vulnerability Integration** 〉 통합.
2. 통합(예: 애플리케이션 목록 통합)을 Veracode 선택합니다.
3. 지금 실행을 클릭합니다.

   주:
   Veracode 각 애플리케이션 취약성 통합은 가장 완벽한 데이터 검색을 제공하기 위한 것입니다. 순서를 벗어나면 전문 지식이 필요하며 ServiceNow애플리케이션 취약성 대응 불완전한 데이터가 발생할 수 있습니다.

   임포트가 완료되면 예약된 임포트가 다시 시작됩니다.
4. 통합 실행 상태는 문서를 참조하십시오 Veracode 애플리케이션 취약성 통합 임포트 실행 상태 보기.
5. 다른 통합 매개변수를 수정하려면 통합 인스턴스로 이동해야 합니다.

임포트 시간 설정 **Veracode Vulnerability Integration**

편의를 위해 의 시작 시간을 재설정할 수 있습니다 Veracode Vulnerability Integration.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: App-Sec 관리자 그룹

이 태스크 정보
초기 임포트 후에는 취약성 통합이 Veracode 실행될 때마다 전체 임포트를 수행합니다. 임포트 수행에 대한 자세한 내용은 을 참조하십시오 수동 Veracode 애플리케이션 취약성 임포트 수행 .

프로시저

1. 다음으로 이동 모두 〉 **Veracode Vulnerability Integration** 〉 통합.
2. 통합을 선택합니다.
3. 새 시작 시간을 설정합니다.
   시간은 현지 시간의 시간으로 계산됩니다. 애플리케이션 목록 통합 임포트의 Veracode 기본 시간은 00:00:00입니다. 다른 통합은 요청 시 이며 애플리케이션 목록 통합 후 실행되도록 체인으로 연결되어 있습니다 Veracode . 이 중 하나의 시작 시간을 변경하려면 고급 ServiceNow 및 애플리케이션 취약성 관리 전문 지식이 필요합니다.
4. 업데이트를 클릭합니다.
   새 시간은 다음으로 예약된 임포트에 사용됩니다.

종결된 **Veracode** 애플리케이션 취약 항목 포함

기본적으로 종결 된 애플리케이션 취약한 항목(AVI)은 취약한 항목 통합 임포트 중에 Veracode 생성되지 않습니다. 만들려면 시스템 속성을 변경해야 합니다.

시작하기 전에
이(가) Veracode Vulnerability Integration 설치되어 실행 중이어야 합니다.

필요한 역할: 관리자

프로시저

1. 왼쪽 탐색 필터 탐색기 텍스트 상자에 `sys_properties.list`를 입력합니다.
2. 목록의 이름 검색 상자에 `sn_vul.create_closed`를 입력합니다.
3. 값 필드를 두 번 클릭하고 **True**로 설정합니다.
4. 저장 확인 표시 아이콘을 클릭합니다.
   다음 Veracode 임포트에서 종결 상태의 기록은 에 AVI애플리케이션 취약성 대응로 생성됩니다.

Application Vulnerability Response의 취약성 수동 수집

보안 전문가와 애플리케이션 테스터는 침투 테스트 작업 공간 내에서 애플리케이션 침투 테스트 결과를 생성하고 관리할 수 있습니다.

침투 테스트 양식은 침투 테스트 작업 공간에서 핵심 비즈니스 애플리케이션에서 식별된 취약성을 문서화하는 데 사용할 수 있습니다.

보안 전문가와 애플리케이션 테스터는 Excel 또는 CSV 형식으로 제공된 템플릿을 사용하여 외부 소스 및 플랫폼에서 결과를 수동으로 임포트할 수 있습니다. 모든 취약성 발견 사항은 침투 테스트 작업 공간에서 사용할 수 있습니다.

침투 테스트 작업 공간에 업로드하기 위한 템플릿에 액세스하고 다운로드하려면 다음으로 이동하십시오. 모두 〉 수동 **AVIT** 수집 〉 업로드 파일 **UI**.

각 애플리케이션에 대한 모든 파일 업로드에 대해 새로운 침투 테스트 양식이 생성됩니다. 해당 업로드 내의 모든 취약성 발견 사항은 동일한 침투 테스트 양식에 연결됩니다. 애플리케이션 이름은 다음 테이블의 기록과 일치해야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 애플리케이션 테이블
- 비즈니스 애플리케이션 테이블
- 스캔한 애플리케이션 테이블

애플리케이션 이름은 침투 테스트 양식과 관련된 애플리케이션 내에 존재하는 취약성을 식별하기 위해 템플릿에 있는 필수 필드입니다. 애플리케이션 이름이 누락된 기록은 취약성을 생성하는 동안 처리되지 않고 건너뜁니다.

주:
침투 테스트 결과를 처리하려면 템플릿의 필수 필드가 필요합니다. 침투 테스트 결과를 처리하는 동안 문제를 방지하려면 템플릿의 모든 필드가 손상되지 않았는지 확인해야 합니다.

침투 테스트 결과 생성을 위한 템플릿의 일부로 필요한 필수 필드

열 이름	필수	설명	사용 가능한 옵션/문자열의 최대 문자 수
위험 등급	필수	애플리케이션 취약한 항목의 심각도	중요 높음 보통 낮음 없음(기본값)
요청한 사람	필수	요청한 사람	151
CWE 범주	필수(하나의 열만 입력)	CWE ID	255
취약성 ID	필수(하나의 열만 입력)	취약성 ID	255
애플리케이션	필수	애플리케이션 이름	255
애플리케이션 목적	필수	애플리케이션 목적	4000
중요한 데이터 유형	필수	애플리케이션에서 액세스할 수 있는 민감한 데이터의 목록 유형	40
규정 준수 프로그램 목록	필수	규정 준수 프로그램 목록	4000
기술 스택 상세 정보	필수	기술 스택 상세 정보	4000
애플리케이션 팀	필수	애플리케이션 팀 이름; 소프트웨어 애플리케이션 개발 및 유지관리를 담당하는 그룹	100
테스트할 URL	필수	테스트할 URL	4000
재현 단계	필수	재현 단계	1000

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

침투 테스트 결과 생성을 위한 템플릿의 일부로 필요한 필수 필드

열 이름	필수	설명	사용 가능한 옵션/문자열의 최대 문자 수
기술 상세 정보	필수	기술 상세 정보	1000
담당자	필수	할당 대상(침투 테스트 수행 및 보안 결과 생성을 담당하는 개인)	151
할당 그룹	필수	할당 그룹(침투 테스트 수행 및 보안 결과 생성을 담당하는 그룹)	151

템플릿 파일을 사용하여 애플리케이션 취약성 업로드

템플릿 파일을 사용하여 애플리케이션 취약성을 업로드합니다. 템플릿에 액세스하고 다운로드하려면 다음으로 이동하십시오. 모두 〉 수동 **AVIT** 수집 〉 업로드 파일 **UI**.

시작하기 전에

필요한 역할: 윤리적 해커 **sn_vul.app_pen_tester**

프로시저

1. 다음으로 이동 모두 〉 수동 **AVIT** 수집 〉 업로드 파일 **UI**.
2. Excel 또는 CSV 링크를 선택하고 해당 형식으로 템플릿을 다운로드합니다.
3. 템플릿에서 레코드의 취약성 데이터를 입력합니다.
   템플릿의 데이터를 채우는 방법에 대한 지침은 템플릿의 "예" 시트를 참조하십시오.
4. 파일 임포트를 선택하고 업데이트된 템플릿을 업로드합니다.
5. 제출을 선택합니다.

   취약성 통합 푸시 큐 페이지가 표시됩니다. 상태를 추적하고 제출과 관련된 로그 메모를 볼 수 있습니다.

   주:
   발생하는 오류의 경우:
   - 오류 로그 파일은 관련 푸시 큐 기록에 직접 첨부됩니다.
   - 추가 오류 세부 정보는 동일한 푸시 큐 기록의 로그 메모 섹션에서도 찾을 수 있습니다.
   - 이 접근 방식을 통해 윤리적 해커는 더 심층적인 시스템 수준 통합 세부 정보에 액세스할 필요 없이 제출을 쉽게 모니터링하고 문제를 해결할 수 있습니다.

통합 실행 확인

통합 실행에 성공하면 개별 탐지 수와 생성 또는 업데이트된 침투 테스트 결과를 검토합니다.

시작하기 전에

필요한 역할: admin

프로시저

1. 다음으로 이동 모두 〉 수동 **AVIT** 수집 〉 통합.
2. 업로드된 파일 형식에 따라 통합의 이름을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 취약성 통합 실행 탭을 선택합니다.
4. 통합 실행 번호를 선택합니다.
5. 항목 탭을 선택합니다.
   항목 탭의 정보를 검토합니다.

결과

항목 탭

탭/필드	설명
항목 탭	임포트된 총 AVIT 수를 표시합니다.
새 항목	이 통합 실행에서 생성된 애플리케이션 취약한 항목 수를 표시합니다.
임포트한 항목	이 섹션에 있는 모든 필드의 합계를 표시합니다.
중복 항목	중복 항목을 표시합니다. 이 필드는 더 이상 채워지지 않습니다.
변경되지 않은 항목	데이터베이스에 있지만 관련 필드 값이 변경되지 않아 업데이트되지 않은 통합 실행 중에 발견된 애플리케이션 취약 항목을 표시합니다.

주:
통합 실행이 성공했음을 확인한 후 푸시 큐 기록으로 이동하여 제출 상태를 추적합니다. 푸시 큐 기록은 다음과 같은 상세 정보를 제공합니다.

- 로그 메모: 레코드 처리 정보로 구성됩니다.
- 오류 파일: 밀어넣는 동안 발생한 오류 세부 정보로 구성됩니다.

업로드 상태 확인

취약성 통합 실행이 성공했는지, 부분적으로 성공했는지, 실패했는지 확인합니다.

시작하기 전에
필요한 역할: sn_vul.app_pen_tester

프로시저

1. 다음으로 이동 모두 〉 수동 **AVIT** 수집 〉 파일 이력 업로드.
2. 업로드 상태 검토: 애플리케이션 취약성 통합 푸시 큐 테이블에서 업로드 타임스탬프에 대한 생성됨 열과 업로드 상태에 대한 상태 열을 검사합니다.
3. 옵션: 성공 확인: 메모 필드에서 성공 마사지를 보고 모든 기록이 성공적으로 처리되었는지 확인합니다.
4. 오류 처리(실패/부분 성공)
   - "실패" 또는 "부분 성공" 상태의 업로드의 경우 오류 로그 파일이 생성됩니다.
   - 관리자 사용자는 이 파일을 보고 업로드 실패 이유를 이해할 수 있습니다.
   - app_pen_tester 역할을 가진 사용자는 푸시 큐 기록 및 관련 오류 상세 정보를 볼 수 있습니다.
   - 오류 로그 파일에는 처리에 실패한 결과만 포함되어 수정 및 재수집을 위한 특정 정보를 제공합니다.
5. 재섭취 지침:

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 성공적으로 처리된 결과를 다시 수집하면 중복 기록이 생성됩니다.
- 중복을 방지하려면 오류 로그 파일에 나열된 결과만 다시 수집합니다.

취약성 정정 애플리케이션 취약성 대응

모니터링 정정은 상태 검토로 시작하여 AVIT(애플리케이션 취약한 항목)를 종결하는 프로세스입니다. 애플리케이션 취약성 대응 는 해당 프로세스를 보다 생산적이고 효율적으로 만드는 도구와 절차를 제공합니다.

애플리케이션 취약성 대응 정정 프로세스

애플리케이션 취약한 항목 정정은 수동으로 수행됩니다.

프로세스 개요:

- 애플리케이션 취약성 대응 인스턴스에 로그인합니다.
- 애플리케이션 취약한 항목에 대한 규칙(CI 조회, 할당)이 예상대로 작동하는지 확인합니다. CI 조회 규칙 개정에 대한 자세한 내용은 을 참조하십시오 자동으로 지원서 애플리케이션 취약성 대응 식별. 할당 규칙에 대한 자세한 내용은 문서를 참조하십시오 에서 애플리케이션 취약 항목 애플리케이션 취약성 대응 자동으로 할당.
- 정정 대상이 올바른지 확인합니다. 정정 대상 규칙의 작동 방식과 수정 방법에 대한 자세한 내용은 을 참조하십시오 에서 정정 대상 추적 자동화 애플리케이션 취약성 대응 . 애플리케이션 취약한 항목의 정정 대상 상태 보기.

  주:
  정정 대상 규칙은 AVIT에 속합니다. 이러한 규칙은 AVIT를 가져올 때 실행됩니다.

- 대시보드 또는 보고서를 검토합니다. 예를 들어 상태별 에이징 AVIT를 보여주는 대시보드를 볼 수 있습니다.

  주:

  애플리케이션(com.snc.vulnerability.analytics)이 취약성 대응용 퍼포먼스 분석 활성화되면 특정 역할을 가진 사용자가 App-Sec 관리자 및 보안 챔피온 그룹의 구성원이 관심을 갖는 데이터를 볼 수 있습니다.

  App-Sec 관리자의 취약성 대응용 퍼포먼스 분석 경우 관심 영역을 모니터링하는 데 도움이 될 수 있는 개요가 애플리케이션 취약성 대응 포함되어 있습니다. 애플리케이션 취약성 대응 및 애플리케이션 취약성 관리(PA) 대시보드에 대한 분석 및 보고 솔루션을 참조하십시오.

  애플리케이션 버전 13.0부터 다음을 수행합니다 취약성 대응 . 보안 챔피온 취약성 대응용 퍼포먼스 분석 의 경우 관심 영역을 모니터링하는 데 도움이 될 수 있는 내 애플리케이션 취약성 대시보드가 포함되어 있습니다. 내 애플리케이션 취약성 대시보드를 참조하십시오.

  애플리케이션의 버전 13.0 취약성 대응 부터 다음을 수행합니다. 보고서 또는 관련 목록에 대해 수집되는 데이터의 양을 제한하려면 을 참조하십시오 보고 및 관련 목록에 대한 취약성 대응 서비스 분류 정의.

- AVIT의 상태를 우선순위 순으로 검토하고 변경된 내용을 검색합니다.
- 필요한 경우 AVIT에 대한 위험을 수정합니다. 자세한 내용은 애플리케이션 취약성 계산기 생성 문서를 참조하십시오.
- 필요한 경우 정정을 위해 할당 그룹에 AVIT를 재할당합니다.
- 재스캔은 외부 공급업체 임포트 일정에 의해 자동으로 트리거됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 재스캔 후 상태가 고정인 경우 임포트하는 동안 AVIT가 자동으로 종결됩니다.
- 스캔 후 상태가 고정이 아닌 경우 AVIT가 다시 열립니다.

에서 자세한 내용 가져오기 **Veracode**

다음 데이터를 보려면 Veracode 애플리케이션 취약 항목[sn_vul_app_vulnerable_item] 테이블 또는 취약성 대응 작업 공간의 목록 뷰에서 소스로 있는 Veracode 애플리케이션 취약한 항목(AVIT)에 대한 상세 정보 가져오기를 선택합니다.

- 동적 애플리케이션 보안 테스트(DAST) 스캔에 대한 HTTP 소스 요청 및 소스 응답 상세 정보가 HTTP 요청/응답 관련 목록에 표시됩니다.
- Veracode의 솔루션 권장 사항이 결과 관련 목록에 표시됩니다.
- HTTP 소스 요청, 소스 응답 및 권장 사항이 취약성 대응 취약성 대응 작업 공간의 상세 정보 탭에 표시됩니다.
- 설명 열은 애플리케이션 취약 항목 [sn_vul_app_vulnerable_item] 테이블에서 지원됩니다.

취약성 라이브러리 보기

NVD(국가 취약성 데이터베이스), CWE(일반적인 약점 열거) 또는 타사에서 임포트한 취약성 데이터를 보고 정정 작업을 에스컬레이션할지 여부를 결정할 수 있습니다.

시작하기 전에
필요한 역할: App-Sec 관리자 그룹

프로시저

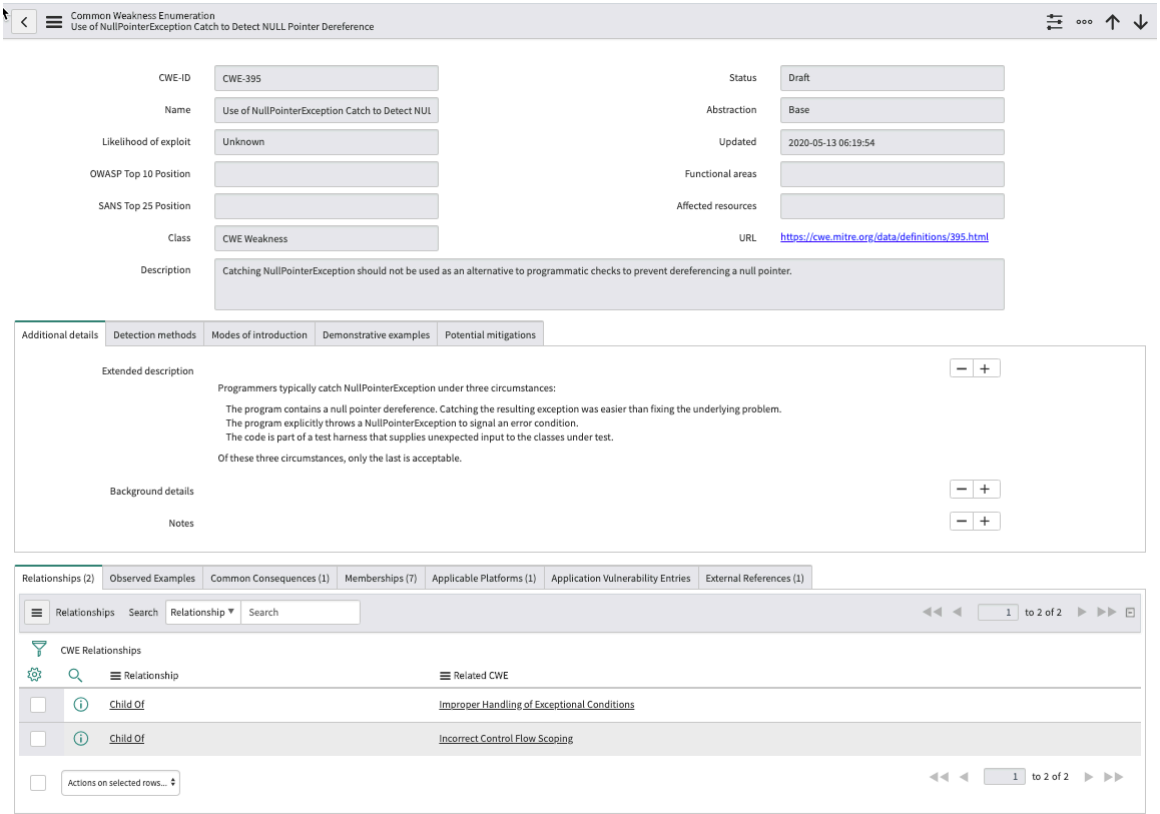
1. 다음으로 이동 모두 〉 애플리케이션 취약성 대응 〉 도서관을 위해.

   다음 라이브러리를 사용할 수 있습니다.

라이브러리	설명
NVD	NVD에서 발견한 취약성 목록으로, 보안 검사 목록, 보안 관련 소프트웨어 결함, 잘못된 구성, 제품 이름 및 익스플로잇을 포함한 영향 메트릭이 포함됩니다.
CWE	커뮤니티에서 개발한 소프트웨어 약점 유형 목록입니다. 각 CWE 기록에는 약점을 설명하는 관련 지식 문서도 포함되어 있습니다. 일반 약점 열거 화면에서 취약성을 에스컬레이션할 수 없으며 참조용으로만 사용해야 합니다.
외부 공급업체	인스턴스에 임포트한 외부 공급업체 취약성의 목록입니다. 관련 참조, 취약한 항목, 익스플로잇, CWE 및 CVE 목록을 포함합니다.

2. 취약성을 확인할 라이브러리를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



특정 필드에 대한 자세한 내용은 다음 문서를 참조하십시오 애플리케이션 취약성 필드.

애플리케이션 취약성 필드

NVD(국가 취약성 데이터베이스), CWE(일반적인 약점 열거) 또는 타사 통합에서 기록을 다운로드하면 취약성이 자동으로 생성됩니다. NVD 및 CWE는 의 라이브러리취약성 대응 또는 취약점애플리케이션 취약성 대응아래에 저장됩니다.

CWE 취약성 항목 필드

이 테이블의 필드는 읽기 전용입니다.

필드	설명
CWE-ID	이 취약성 항목의 식별자입니다. 이 식별자는 범주와 약점 모두에 사용되며 두 데이터 세트 간에 고유합니다.
이름	이 CWE-ID에 할당된 설명이 포함된 이름입니다.
악용 가능성	질적 척도에서 약점이 악용될 가능성입니다. 다음 중 하나입니다. • 낮음 • 보통 • 높음
OWASP 상위 10개 위치	OWASP 상위 10개 목록에서 이 취약성의 숫자 위치입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
SANS에서 25 위치로	SAN 상위 25개 목록에서 이 취약성의 숫자 위치입니다.
클래스	약점의 유형
상태	다음 중 하나입니다. • 완료 안 됨 • 초안 • 안정 • 사용하지 않음 • 사용되지 않음 • 불안정
추상화	다음 중 하나입니다. • 변형 • 클래스 • 기본 • 복합
업데이트됨	인스턴스에서 기록이 마지막으로 업데이트된 시간입니다.
기능 영역	영향을 받는 기능 영역의 목록입니다. 예를 들어 파일 처리입니다. 24/862 약점에 대해서만 채워집니다.
영향을 받는 리소스	영향을 받는 자원의 목록입니다. 예를 들어 파일 또는 디렉터리입니다. 51/863 약점에만 적용됩니다.
URL	이 취약성과 관련된 기술 자료 문서입니다.
설명	취약성에 대한 설명입니다.
통합 실행	이 CWE를 임포트한 통합 실행입니다.
섹션	
추가 상세 정보	약점을 추가로 설명하는 소프트웨어 개념 설명입니다. 다음이 포함됩니다. • 확장된 설명 • 백그라운드 세부 정보 • 메모
탐지 방법	애플리케이션에서 이 약점을 감지할 수 있는 방법에 대한 상세 정보입니다.
소개 모드	약점이 도입되는 단계(예: 구현, 아키텍처 및 설계 등)입니다.
데모 예제	약점에 대한 코드 예제와 함께 설명이 제공됩니다.
잠재적 완화	취약점이 발생하는 애플리케이션 수명주기 단계 및 완화 효과를 포함하여 약점을 방지하는 방법에 대한 상세 정보입니다.
관련 목록	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
관계	이 취약성과 관련된 CWE입니다. 이 CWE와 다른 CWE의 관계를 나열합니다. parent/child, follows/precedes, requiredby/requires(복합 약점의 경우), CanAlsoBe, PeerOf, MemberOf를 포함할 수 있습니다.
관찰 예	이 약점을 대표하는 일부 CVE입니다.
일반적인 결과	범위 및 영향 측면에서 성공적인 익스플로잇의 결과입니다. 예: 범위: 기밀성 영향: 애플리케이션 데이터 읽기
구성원 자격	이러한 취약성이 있는 CWE 회원.
적용 가능 플랫폼	이 취약성과 관련된 플랫폼입니다.
애플리케이션 취약성 항목	이와 연관된 다른 애플리케이션 취약성 항목입니다.
외부 참조	외부 소스에서 얻은 취약성에 대한 정보입니다.

애플리케이션 취약성 항목 필드

이 테이블의 필드는 읽기 전용입니다.

필드	설명
ID	이 취약성 항목의 식별자입니다.
소스	취약성의 출처(스캐너 또는 물리적 테스트)입니다.
심각도	이 취약성의 정규화된 심각도 수준입니다. NVD 및 타사 통합에 ServiceNow 대해 심각도 맵이 제공됩니다. 심각도 맵 생성 및 조정에 대한 자세한 내용은 다음 문서를 참조하십시오 애플리케이션 취약한 항목의 심각도를 자동으로 매핑.
버전 13.0: 기본 CWE 버전 12.1: CWE 항목	이 취약성이 가장 적합한 일반 약점 열거형 요소에 대한 참조입니다. 취약성과 관련된 CWE가 둘 이상인 경우 기본 CWE는 다음과 같이 결정됩니다. • CWE가 OWASP 상위 10개 항목에 매핑되어 있습니까? 그렇다면 이 CWE를 사용합니다. 그렇지 않은 경우 계속합니다. • CWE가 SAN 상위 25개 항목에 매핑됩니까? 그렇다면 이 CWE를 사용합니다. 그렇지 않은 경우 계속합니다. • CWE의 심각도가 가장 높습니까? 그렇다면 이 CWE를 사용하십시오. 그렇지 않은 경우 계속합니다. • 모든 CWE 중 최신 CW를 선택합니다. 최신 CWE는 CWE 기록에서 최신 업데이트된 필드 값이 있는 CWE입니다.
범주 이름	외부 공급업체 통합에서 제공하는 분류입니다. 임무 수행을 돕는다.
취약성 상세 정보	
위협	이 취약성으로 인한 위협에 대한 설명입니다.
완화 설명	취약성을 완화하기 위해 수행할 수 있는 단계에 대한 설명입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
관련 목록	
버전 13.0 : CWE	이 취약성과 연관된 CWE 목록입니다. 에는 Veracode Vulnerability Integration적용되지 않음.

NVD 항목 필드

이 테이블에서 임포트한 필드는 읽기 전용입니다.

주:

NVD 데이터는 사용되지 애플리케이션 취약성 대응 않으며 항목은 데이터만 나타냅니다 취약성 대응 .

에서 사용되는 애플리케이션 취약성 대응CWE는 약점의 예로 NVD 항목을 가리킬 수 있으며 여기서는 정보 제공의 목적으로만 제공됩니다.

필드	설명
ID	이 취약성 항목의 식별자입니다.
위험 등급	(취약성과 관련된 취약한 항목(VI)이 없는 취약성 대응 경우 숨겨짐) VI를 중요, 높음, 중간, 낮음 및 없음으로 구분하는 정량화된 위험 점수 입니다.
위험 점수	(취약성과 연관된 VI가 없는 경우 숨겨짐) 취약한 항목이 환경에 미치는 위험의 계산된 양입니다.
심각도	에서 이 취약성의 정규화된 심각도 .취약성 대응 NVD 및 타사 통합에 ServiceNow 대해 심각도 맵이 제공됩니다. 애플리케이션 취약성 대응 심각도는 NVD가 아닌 임포트된 소스 심각도에서 파생됩니다. 심각도 매핑에 대한 애플리케이션 취약성 대응 자세한 내용은 다음 문서를 참조하십시오 애플리케이션 취약한 항목의 심각도를 자동으로 매핑.
익스플로잇 존재	예, 하나 이상의 익스플로잇이 이 취약성과 관련된 경우 가능합니다.
익스플로잇 기술 수준	이 취약성을 악용하는 데 필요한 가장 낮은 기술 수준입니다.
익스플로잇 공격 벡터	이 취약성에 대한 익스플로잇의 가장 취약한 공격 벡터입니다.
활성 VI	(취약성과 연관된 VI가 없는 경우 숨겨짐) 이러한 취약성과 연관된 취약한 항목의 수로, 종결 상태가 아닙니다. 이 취약성에 대한 활성 AVI가 없으면 위험 등급 및 위험 점수 가 표시되지 않습니다.
CWE 항목	NVD에 따라 이 취약성이 가장 적합한 Common Weakness Enumeration 요소에 대한 참조입니다.
게시 날짜	취약성이 게시된 날짜입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
마지막으로 수정됨	취약성이 마지막으로 수정된 날짜입니다.
요약	취약성에 대한 설명입니다.
취약성 상세 정보	
CVSS v2	임포트된 CVSS v2 데이터
CVSS v3	2015년 이전에는 사용할 수 없었던 임포트된 CVSS v3 데이터입니다.
기본 솔루션	(취약성과 연관된 VI가 없는 경우 숨겨짐) 취약성에서 참조하는 솔루션에서 파생된, 체인 내 대체 가능성이 가장 높은 솔루션. 체인에 둘 이상의 최고 대체가 있는 경우 값이 설정되지 않습니다. 수동으로 설정된 값은 후속 임포트에서 덮어쓸 수 있습니다. 취약한 항목에서 이 값을 수동으로 설정해야 합니다.
정정 상태 (취약성과 연관된 VI가 없는 경우 숨겨짐)	
지연 제외	
취약한 항목	이러한 취약성이 있는 활성 애플리케이션 취약한 항목의 수입니다. 이 개수에서 지연된 취약한 항목은 제외됩니다.
총 VI	이러한 취약성이 있는 취약한 항목의 총 수. 이 개수에서 지연된 취약한 항목은 제외됩니다.
정정된 VI 비율(%)	이러한 취약성이 있는 취약한 항목의 정정 완료율. 이 개수에서 지연된 취약한 항목은 제외됩니다.
지연 포함	
취약한 항목	이러한 취약성이 있는 활성 취약한 항목의 수.
총 VI	이러한 취약성이 있는 취약한 항목의 총 수.
정정된 VI 비율(%)	이러한 취약성이 있는 취약한 항목의 정정 완료율.
관련 링크	
v13.0 이전: 소프트웨어 취약성 임포트 강제 적용 주: v13.0에서 제거됨	(사용 안 함) NVD의 정보를 기반으로 제품 매핑을 ITSM 소프트웨어 자산 관리 다시 계산합니다. 취약한 소프트웨어 라이브러리를 업데이트합니다.
상태 업데이트	마지막 업데이트의 날짜 및 시간을 표시합니다. 다음을 업데이트합니다. • 정정 작업 상태 • 위험 점수 및 등급 • 정정 상태 섹션의 활성 VI, 총 VI와 같은 메트릭
관련 목록	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
취약 항목	(취약성과 연관된 VI가 없는 경우 숨겨짐) 이러한 취약성과 연관된 취약한 항목입니다.
취약성 참조	NVD에서 인용한 외부 소스의 취약성에 대한 정보입니다.
익스플로잇	이 취약성과 관련된 익스플로잇입니다.
솔루션	(취약성과 연관된 VI가 없는 경우 숨겨짐) 이 취약성과 관련된 모든 취약성 솔루션 관리 통합 솔루션입니다.
버전 13.0 : 약점	CVE(Common Vulnerabilities and Exposures)와 관련된 CWE 약점 데이터를 임포트했습니다.
버전 13.0 : 취약한 소프트웨어	(취약성과 연관된 VI가 없는 경우 숨겨짐) 취약성과 관련된 CPE(공통 플랫폼 열거형) 데이터를 임포트했습니다.

자동으로 지원서 애플리케이션 취약성 대응 식별

외부 공급업체 통합에서 데이터를 임포트하면 에서 애플리케이션 취약성 대응 애플리케이션 데이터를 사용하여 에서 일치하는 항목을 구성 관리 데이터베이스(CMDB)검색합니다. 이는 **CI** 조회 규칙을 사용합니다. 이러한 규칙은 정정에 도움이 되는 애플리케이션 취약한 항목(AVI) 기록에 대한 애플리케이션을 식별합니다.

애플리케이션을 임포트하면 검사한 애플리케이션에서 조회가 수행됩니다. [sn_vul_app_scanned_application] source_app_id 및 app_name 사용하여 이전 임포트의 애플리케이션과 일치하는 항목을 찾을 수 있습니다. 애플리케이션 ID 일치가 발견되면 해당 값이 애플리케이션 취약한 항목 기록의 애플리케이션 및 앱 릴리스 필드에 사용됩니다.

일치하는 항목을 찾을 수 없거나 애플리케이션 ID 필드가 비어 있는 경우 규칙은 다른 애플리케이션 정보를 사용하여 애플리케이션을 올바르게 식별하려고 시도합니다. 그래도 일치하는 항목이 없으면 애플리케이션 이름 및 애플리케이션 **ID** 필드만 사용하여 자리 표시자 스캔된 애플리케이션 기록이 생성됩니다.

소스 애플리케이션 **ID** 및 애플리케이션 이름 조회 규칙은 기본적으로 와 Veracode Vulnerability Integration함께 제공됩니다.

> **주:**
> 에 대한 애플리케이션 취약성 대응 기본 CI 조회 규칙은 취약성 통합에만 Veracode 사용할 수 있습니다.

일치를 시도할 때 조회 규칙은 가장 낮은 순서 값으로 먼저 평가됩니다. 규칙이 단일 CI를 일치로 반환하면 중지됩니다.

> **주:**
> 둘 이상의 CI를 반환하는 방식으로 규칙이 생성되면 첫 번째 일치 항목만 사용됩니다.

일치하는 문제를 쉽게 찾을 수 있도록 일치하는 항목이 발견되면 이를 찾는 데 사용되는 CI 조회 규칙이 스캔된 애플리케이션에 대한 **CI** 일치 규칙 필드에 추가됩니다. 스캔한 애플리케이션 목록 뷰의 상단에 있는 개인화된 목록 업데이트 기어 아이콘을 클릭하여 뷰에 추가합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
제거된 규칙은 복구할 수 없습니다. 기존 규칙을 제거하는 대신 새 규칙을 만들 때 비활성화하십시오.

CI 조회 규칙은 도메인으로 분리될 수 있으며 소스에 따라 다릅니다. 지원되는 경우 각 소스에는 여러 배포가 있을 수 있습니다. 예를 들어 취약성 통합에는 Veracode 취약성 통합의 여러 배포가 있을 수 있습니다 Veracode . 각 배포에는 고유한 CI 조회 규칙 세트가 있습니다.

주:
CI 조회 규칙은 취약성 통합의 모든 배포에서 공유됩니다. 규칙이 삭제되거나 수정되면 삭제 또는 변경이 취약성 통합의 모든 배포에 영향을 줍니다.

취약성 데이터를 임포트하면 인스턴스에 부담이 가중될 수 있으며 규칙을 신중하게 구성하지 않으면 자원에 성능 문제가 발생할 수 있습니다. 반복을 수행하고 일치를 수행하는 데 사용되는 논리로 CMDB 인해 처리 시간이 길어질 수 있습니다. 자원의 잠재적 저하나 성능 저하를 방지하려면 사용자 지정 작성된 CI 조회 규칙을 테스트하거나 사전 정의된 **CI** 조회 규칙을 수정하십시오. 고아 기록 중복 방지, 데이터 삭제 및 데이터 정리에 대한 자세한 내용은 을 참조하십시오 Application Vulnerability Response CI 조회 규칙을 실행한 후 중복 또는 고아 기록 방지 .

관련 정보

Configuration Management 및 CMDB

CI 조회 규칙 생성

CI 조회 규칙 모듈에는 에 일치하는 데이터가 있는 필드를 정의하는 규칙이 포함되어 있습니다구성 관리 데이터베이스(CMDB). 이러한 규칙은 애플리케이션 및 애플리케이션 릴리스를 식별하고 정정에 도움이 되도록 애플리케이션 취약한 항목(AVI) 기록에 추가하는 데 사용됩니다.

시작하기 전에
필요한 역할: App-Sec 관리자 그룹

이 태스크 정보
CI 조회 규칙을 생성하려면 고급 ServiceNow 전문 애플리케이션 취약성 관리 지식이 필요합니다. 기존 조회 규칙 중 하나를 수정하지 말고 복사하여 복사본을 수정하는 것이 좋습니다. 새 규칙이 원하는 작업을 수행한다고 생각되면 원래 규칙을 비활성화합니다.

주:
제거된 규칙은 복구할 수 없습니다. 기존 규칙을 제거하는 대신 새 규칙을 만들 때 비활성화하십시오.

프로시저

1. 다음으로 이동 모두 〉 보안 운영 〉 **CMDB** 〉 **CI** 조회 규칙.
2. 새로 만들기를 클릭합니다.
3. 양식에서 필드를 채웁니다.

CI 조회 규칙 양식

필드	설명
이름	규칙의 이름입니다.
조회 메서드	일치에 사용되는 메서드입니다. 선택 항목은 다음과 같습니다. ○ 스크립트: 사전 구축 또는 사용자 지정 스크립트입니다. ○ 필드 일치: CMDB의 테이블 또는 필드를 검색합니다.

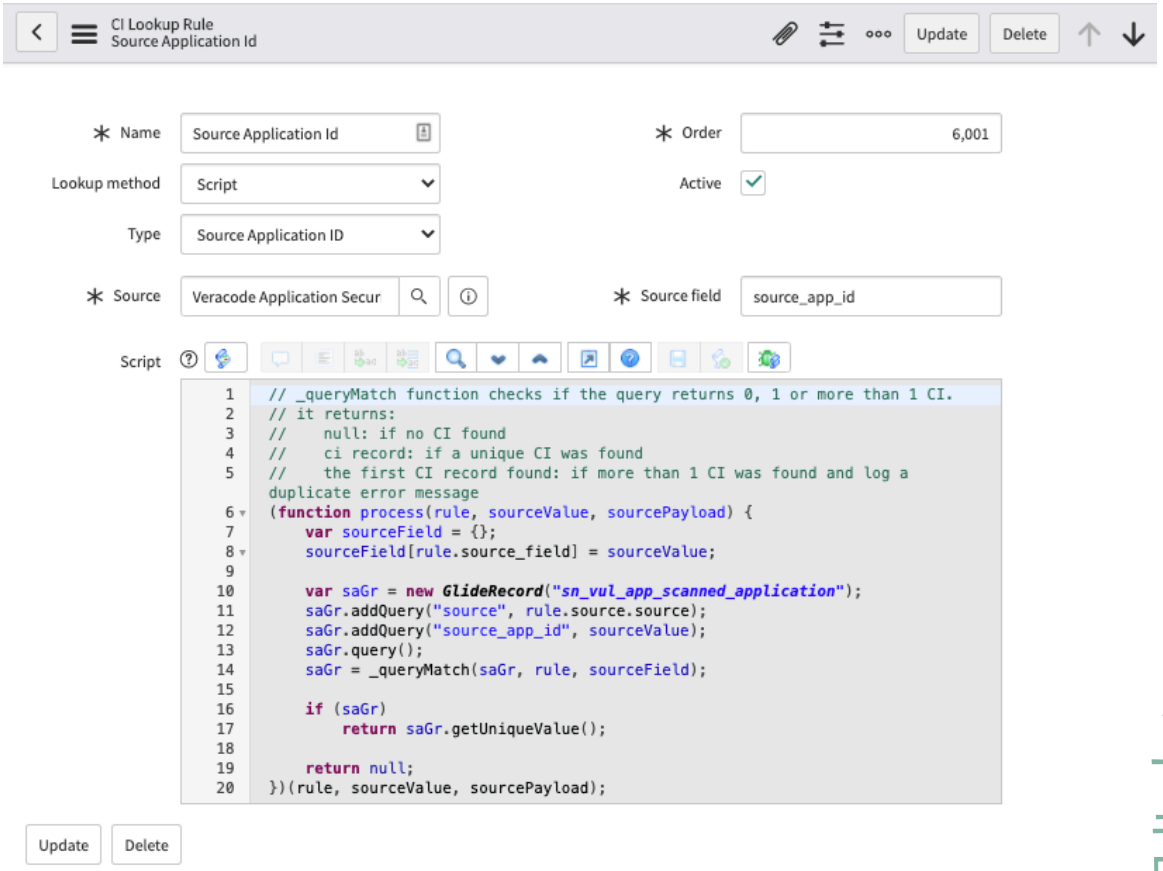
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
유형	스크립트 조회 메서드에 사용되는 유형입니다.
순서	규칙의 우선순위 순서입니다. 순서가 가장 낮은 일치 항목이 먼저 평가됩니다.
활성	규칙의 활성 또는 사용 안 함 여부에 대한 확인란입니다.
소스	이 규칙에 대한 입력으로 사용되는 소스입니다. 선택하면 조건 필터가 나타납니다.
소스 필드	이 규칙에 대한 입력으로 사용되는 소스 필드입니다. 필드는 문자열 또는 숫자여야 합니다.
설명	규칙을 설명하는 텍스트입니다.
V19.0: 조회 대상	따르려는 조회 접근 방식입니다. 다음 중에서 선택합니다. ○ 구성 항목 ○ 제품 모델
스크립트	유형에 따라 편집 가능한 샘플 스크립트가 표시됩니다. 기본 기능의 템플릿에 포함된 설명에 따라 사용자 지정 스크립트를 구현합니다. 주: process 함수에는 세 개의 매개 변수가 있습니다. *rulesourceValuesourcePayload*
CI 테이블에서 검색	CMDB 내에서 검색할 테이블입니다. 필드 일치 조회 메서드와 함께 사용됩니다.
V19.0: 제품 테이블에서 검색	제품 모델 조회 대상을 선택하면 기본값은 애플리케이션 모델입니다.
CI 필드 검색	CI를 찾는 데 사용할 수 있는 정보가 담긴 필드입니다. 필드 일치 조회 메서드와 함께 사용됩니다. 이 필드는 CI 기록 또는 네트워크 어댑터와 같은 관련 기록에 있을 수 있습니다.
V19.0: 제품 모델 필드에서 검색	제품 모델 조회 대상을 선택하는 경우 기본값은 이름입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 제출을 클릭합니다.

스크립트를 사용한 **CI** 조회 규칙의 예



관련 정보

애플리케이션 취약한 항목 필드

에서 **CI** 조회 규칙 다시 적용 애플리케이션 취약성 대응

CI(구성 항목) 조회 규칙을 다시 적용하여 검색된 애플리케이션 기록의 기존 CI(스캔한 애플리케이션 및 제품 모델)를 업데이트할 수 있습니다.

조회 규칙 다시 적용

검색된 애플리케이션 테이블에서 선택되거나 필터링된 항목에 대해 "조회 규칙을 다시 적용"할 수 있습니다.

필터가 적용되지 않으면 다시 적용 옵션이 비활성화됩니다. 다시 적용한 후 통합이 실행 중인 경우 사용자가 백그라운드 작업 URL 또는 오류 메시지를 받을 수 있습니다.

기존 디스커버리된 애플리케이션에 규칙을 다시 적용하려면 다음으로 이동하십시오. 모두 〉 보안 운영 〉 **CMDB** 〉 조회 규칙.

주:
v25.0.3 부터 애플리케이션 취약성 대응해제된 CI와 관련된 취약 항목 및 탐지를 종결하기 위해 새로운 자동 종결 규칙 'CI 해제됨'이 도입되었습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

조회 대상 설정

기본적으로 *sn_vul.use_product_model* 시스템 속성이 활성화되어 있습니다(**true**로 설정). CI 조회 규칙 기록에서 시스템 속성이 설정된 방식에 따라 검색된 애플리케이션 기록은 다음과 같은 방식으로 업데이트됩니다.

- 값 필드가 **true**로 설정되면 제품 모델이 CI 조회 규칙의 조회 대상이 되고 검색된 애플리케이션이 제품 모델로 업데이트됩니다.
- 값 필드가 **false**로 설정되면 구성 항목(스캔한 앱)이 조회 대상이 되고 검색된 애플리케이션이 구성 항목(스캔된 애플리케이션)으로 업데이트됩니다.

구성 항목이 대상으로 사용되도록 시스템 속성을 수정 *sn_vul.use_product_model* 하려면 다음을 수행합니다.

1. sn_vul.app_sec_manager 역할을 가진 사용자로, 모두 〉 시스템 속성 〉 모두
2. 를 찾습니다 *sn_vul.use_product_model*.
3. 기록을 엽니다.
4. 유형 필드를 **false**로 설정합니다.
5. 업데이트를 선택합니다.

이 시스템 속성을 재설정하는 경우 조회 대상이 시스템 속성 설정과 일치하도록 규칙을 수정해야 합니다. 예를 들어, 구성 항목을 대상으로 사용하도록 시스템 속성을 재설정하는 경우 조회 대상이 구성 항목으로 있는 규칙을 찾습니다.

1. 이러한 규칙의 활성 확인란을 선택하고 업데이트를 선택합니다.
2. 제품 모델을 대상으로 사용하는 규칙을 찾아 활성 확인란의 선택을 취소하고 업데이트를 선택하여 비활성화합니다.

새 조회 규칙을 만드는 경우 규칙 양식에서 규칙에 대한 조회 대상을 설정합니다. 자세한 내용은 CI 조회 규칙 생성 문서를 참조하십시오.

Application Vulnerability Response CI 조회 규칙을 실행한 후 중복 또는 고아 기록 방지

일치하는 항목(CI) 내의 CMDB중복 기록 또는 고아 기록이 발생하지 않도록 조치를 취합니다.

취약성 데이터를 임포트하면 인스턴스에 부담이 가중될 수 있으며 규칙을 신중하게 구성하지 않으면 자원에 성능 문제가 발생할 수 있습니다. CMDB 내에서 반복하고 일치를 수행하는 데 사용되는 논리로 인해 처리 시간이 길어질 수 있습니다. 규칙에서 처리 스크립트를 철저히 테스트하고 디버깅하면 나중에 프로세스에서 발생할 수 있는 문제를 완화하는 데 도움이 됩니다.

중복 기록 또는 고아 기록 방지

- 테스트 중인 CI 조회 규칙과 관련된 데이터의 작은 하위 집합을 사용합니다.
  - 테스트 중인 규칙을 제외한 모든 **CI** 조회 규칙을비활성으로 설정합니다.
  - 임포트한 애플리케이션 및 CI(구성 항목)를 분석하여 예상되는 동작을 관찰하고 일치가 올바르게 발생하는지 확인합니다.
- 폐기됨과 같은 CI 상태를 검토합니다.
- 테스트 데이터를 제거합니다. CI 일치에서 올바름 또는 예상되는 동작을 관찰하기 시작하면 다시 시작하십시오. 이 작업은 다음을 통해 수행할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 테스트에 사용되는 데이터 삭제: (테이블에서 데이터 삭제 섹션 참조)
  - 검사한 애플리케이션
  - 애플리케이션 취약한 항목(AVI)
- 통합을 수동으로 다시 실행합니다.

.

테이블에서 데이터 삭제

데이터를 임포트하고 문제가 있음을 깨닫는 경우가 있습니다. 개발 또는 성능 환경에서 이 문제가 발생하는 경우 더 나은 환경에서 다시 복제할 수 있지만 항상 가능한 것은 아닙니다.

주:
이러한 작업을 수행하려면 고급 ServiceNow 전문 지식이 필요합니다.

테이블에서 데이터를 삭제하는 네 가지 옵션이 있습니다.

- 테이블 구성에서 모든 기록 삭제를 사용합니다.
- 자동 플러시(sys_auto_flush.list)로 이동하고 새 자동 플러시 기록을 생성하여 테이블 클리너를 구성합니다.
- 백그라운드 스크립트를 사용하여 gs.truncateTable을 자릅니다.

  주:
  프로덕션 환경에서 사용하지 *`truncateTable`* 마십시오. 프로덕션 또는 공유 환경에서 대용량 삭제를 실행하기 전에 지원 담당자에게 문의하십시오.

- HI에서 데이터를 삭제하도록 요청을 생성합니다.

에서 애플리케이션 취약 항목 애플리케이션 취약성 대응 자동으로 할당

애플리케이션 태그 또는 구성 항목 [cmdb_ci] 또는 플랫폼 할당 그룹의 할당 그룹을 기반으로 애플리케이션 취약성을 자동으로 할당하여 평균 할당 시간을 줄입니다.

애플리케이션 취약한 항목 자동으로 할당

다음을 사용하여 할당을 사용하여 AVI를 할당하는 방법에는 세 가지가 있습니다.

주:
의 취약성 대응 할당 권장 사항 기능은 에 사용할 애플리케이션 취약성 대응수 없습니다.

- 사용자 그룹: 이 옵션을 사용하면 기존 ServiceNow AI Platform# 사용자 그룹을 선택할 수 있습니다.
- 사용자 그룹 필드: 이 옵션을 사용하면 cmdb_ci 테이블을 사용하여 사용할 수 있는 할당 그룹 필드를 선택할 수 있습니다. 기본적으로 사용자 그룹 필드 아래의 목록 메뉴에는 다음 세 개의 그룹 필드가 표시됩니다.
  - 없음: 이 필수 필드의 기본값이 없음을 나타냅니다.
  - 구성 항목: 승인 그룹
  - 구성 항목: 담당 그룹
  - 구성 항목: 지원 그룹
- 스크립트: 이 옵션을 사용하면 스크립트를 사용하여 조건을 정의할 수 있습니다. 이 옵션을 사용하려면 코딩 또는 고급 ServiceNow 전문 지식이 필요합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

우선 순위가 높은 규칙(특별한 처리가 필요하거나 위험이 중요하거나 규정 준수에서 AVI를 처리해야 하는 항목)을 먼저 실행합니다. 다음으로, 특별한 처리가 필요하지 않은 일반 규칙을 실행하고 누가 이를 담당해야 하는지 알 수 있습니다. 마지막으로, 그룹에 AVI를 할당하여 속해야 하는 할당 그룹을 파악하는 기본 규칙을 만듭니다. 이 그룹은 그들의 결정을 다루기 위해 또 다른 규칙을 추가할 수 있습니다. 이 기본 규칙은 마지막에 실행됩니다.

할당 규칙 평가 프로세스

종결된 후 새 AVI를 생성, 임포트 또는 다시 열면 담당 규칙이 이에 대해 평가됩니다. AVI는 종결된 후 다시 열리지 않는 한 한 한 번만 평가됩니다. 변경 후 수동으로 규칙을 다시 적용할 수 있습니다.

새 AVI, 업데이트 또는 다시 열린 각 AVI에 대해 다음 프로세스가 사용됩니다.

- 각 취약성 할당 규칙에 대해 AVI는 할당 필터와 비교됩니다. 가장 낮은 순서의 규칙이 먼저 적용됩니다.
- 조건이 일치하는 경우 AVI에 할당 그룹이 할당됩니다. 조회가 중지됩니다.
- 조건이 다른 모든 규칙 간에 일치하는 항목을 찾지 못하면 기본 규칙이 있으면 AVI가 기본 할당 그룹에 할당됩니다.

> **주:**
> 기본 규칙이 없으면 AVI는 할당되지 않은 상태로 유지됩니다.

할당 유형(애플리케이션 취약한 항목(AVI) 양식의 양식 레이아웃 슬러시버킷에서 수동 또는 규칙 및 할당 규칙을 사용할 수 있는지 여부. 원래 규칙에 의해 할당되었지만 나중에 수동으로 다시 할당된 모든 AVI에는 원래 규칙에 대한 참조가 포함되어 있습니다. 할당 규칙 및 할당 유형 정보를 사용하여 담당 규칙이 의도한 수신자에 대한 올바른 일치 항목을 찾지 못한 케이스를 식별합니다. 또는 재할당이 가장 많은 규칙.

> **주:**
> 담당 규칙은 수동으로 생성된 할당을 다시 평가하지 않습니다.

담당 규칙 다시 적용

할당 규칙을 변경할 때 할당 규칙 목록 뷰의 변경 내용 적용 단추를 사용하여 수동으로 할당된 규칙 제외의 모든 활성 AVI에 대해 변경된 모든 규칙을 다시 실행합니다.

> **주:**
>
> ***Reapply all vulnerability assignment rules***변경 적용을 처음 사용하기 전에 예약된 작업이 실행되지 않은 경우 수동으로 할당된 AVI를 제외한 모든 Open AVI에 대해 모든 담당 규칙이 실행됩니다. 이후에는 변경 내용 적용을 이후에 사용할 때마다 변경된 규칙과 종속 규칙만 다시 실행됩니다. 한 규칙을 변경하면 AVI가 수정되지 않은 다른 규칙과 일치할 수 있습니다. 〔store-future: BEGIN review〕담당 규칙을 다시 적용해도 취약한 항목은 다시 그룹화되지 않습니다.〔End〕
>
> 예약된 작업 [***Reapply all assignment rules***〕은 기본적으로 비활성 상태입니다. 활성화되면 수동으로 할당된 AVI를 제외한 모든 열린 AVI에 모든 규칙이 적용됩니다. 매일, 매주, 매월, 주기적으로, 한 번 또는 요청 시에 실행할 수 있습니다. 환경에 있는 활성 AVI 수에 따라 성능에 영향을 주지 않도록 초기 실행 후 실행 필드를 적절하게 설정해야 합니다.

담당 규칙 생성 또는 편집 애플리케이션 취약성 대응

필터 조건에 따라 애플리케이션 취약한 항목(AVI)을 자동으로 할당하는 규칙을 생성할 수 있습니다. 이러한 규칙은 AVI를 임포트하거나 수동으로 만들 때 AVI를 할당합니다.

시작하기 전에
필요한 역할: App-Sec 관리자 그룹

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보
담당 규칙을 사용하여 할당 조건과 실행 순서를 정의합니다. AVI가 규칙 조건과 일치하면 할당 조회가 중지됩니다. 자세한 내용은 내부 필터링 애플리케이션 취약성 관리 문서를 참조하십시오.

프로시저

1. 다음으로 이동 모두 〉 애플리케이션 취약성 대응 〉 관리 〉 담당 규칙.
2. 새로 만들기를 클릭합니다.
3. 새로 만들기인 경우 양식의 필드에 적절한 정보를 입력합니다.

애플리케이션 취약성 담당 규칙

필드	설명
이름	그룹 규칙의 이름입니다.
활성	할당 규칙이 활성 상태인지 여부를 나타냅니다.
실행 순서	규칙이 평가되는 순서입니다. 우선 순위가 높은 규칙, 특별한 처리가 필요한 항목, 위험이 중요한 경우 또는 규정 준수에서 AVI를 처리해야 하는 항목이 먼저 실행됩니다. 다음으로, 특별한 처리가 필요하지 않은 일반 규칙을 실행하고 누가 책임을 져야 하는지 알 수 있습니다. 마지막으로, 그룹에 AVI를 할당하여 속해야 하는 할당 그룹을 파악하는 기본 규칙을 만듭니다. 이 그룹은 그들의 결정을 다루기 위해 또 다른 규칙을 추가할 수 있습니다. 이 기본 규칙은 마지막에 실행됩니다.
설명	할당 규칙에 대한 설명입니다.
조건	
조건 필드	충족되어야 하는 조건입니다.
새 기준	선택할 조건 필터 필드를 더 추가합니다.
할당 사용	이 규칙에 따라 생성된 그룹의 할당을 자동화하려면 사용 가능한 옵션 중 하나를 선택합니다. ○ 사용자 그룹: 조회 테이블에서 사용자 그룹을 선택합니다. ○ 사용자 그룹 필드: 목록 메뉴에서 사용자 그룹 필드를 선택합니다. ○ 스크립트: 스크립트를 만들거나 편집합니다. 주: 스크립트를 만들거나 편집하려면 전문 지식이 필요합니다 ServiceNow .

4. 제출을 클릭합니다.
새 규칙이나 업데이트된 규칙은 다음 임포트 시 평가됩니다.

취약한 항목 및 정정 작업에서 할당 애플리케이션 취약성 대응 제거

사용자 또는 그룹에 잘못 할당되었을 수 있는 애플리케이션 취약한 항목 및 정정 작업 기록에서 취약한 항목의 할당 대상 및 할당 그룹 필드를 애플리케이션 취약성 대응 직접 지울 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

워크플로우 개요

취약한 항목(AVIT) 및 정정 작업(AVUL)이 정정 범위에 속하지 않는 것으로 확인 애플리케이션 취약성 대응 되거나 기록이 사용자 또는 소속 그룹에 잘못 할당되었다고 생각되는 경우, AVIT 및 AVUL 기록의 할당 대상 및 할당 그룹 필드에서 본인 또는 그룹을 제거할 수 있습니다.

할당 해제 워크플로우는 AVIT 및 AVUL에 대한 클래식 및 작업 공간 뷰에서 지원됩니다.

승인을 위해 할당 필드를 지우는 요청을 보낼 수 있습니다. 자세한 내용은 에서 할당 해제 요청 승인 또는 거부 취약성 대응 문서를 참조하십시오.

- 할당 해제 버튼은 AVIT 및 AVUL 기록에 종결됨 또는 해결됨 이외의 모든 상태로 표시됩니다.
- 필드 지우기 요청이 승인되면 동일한 할당 그룹이 있는 AVUL과 연결된 AVIT의 모든 할당 대상 및 할당 그룹 필드도 할당 취소됩니다. 애플리케이션 취약한 항목에 연결된 정정 작업과 다른 할당 그룹이 있는 경우 할당되지 않습니다. 대부분의 경우 이러한 애플리케이션 취약한 항목은 수동으로 할당되었습니다. 자세한 내용은 취약한 항목 및 정정 작업에서 할당 제거 문서를 참조하십시오.
- UI 작업으로 업데이트하거나 수동으로 업데이트하는 모든 기록은 에 대한 애플리케이션 취약성 대응할당되지 않은 모듈에 표시됩니다.
- 목록에서 여러 AVIT에 대한 할당 필드를 지울 수 있습니다. AVIT를 선택하고 대량 편집을 선택한 후 표시되는 대화 상자에서 할당 취소 확인란을 선택합니다.

할당 필드를 지우는 방법에 대한 자세한 단계는 을 참조하십시오 취약한 항목 및 정정 작업에서 할당 제거 .

시스템 속성 및 승인 알림

정정 소유자가 기록에서 할당 해제 를 선택하면 기본적으로 sn_vul.unassign_vr.approval_required 시스템 속성이 승인 플로우를 트리거하고 검토 상태에서 상태 변경 승인 기록을 생성하며, 요청은 승인을 위해 라우팅됩니다. 요청은 sn_vul_.unassign_approver가 있는 사용자의 내 승인 목록에 표시됩니다.

주:
취약성 관리자(sn_vul.vulnerability_admin)는 *sn_vul.unassign_vr.approval_required* 시스템 속성을 **false** 로 설정하여 승인 프로세스를 비활성화할 수 있습니다.

또한 할당 필드가 지워지면 특정 그룹이 할당되도록 시스템 속성의 값을 *sn_vul.default_assignment_group* 변경할 수 있습니다. 예를 들어 사용자가 기록에서 할당 해제 를 클릭하고 검토를 위해 특정 그룹으로 리디렉션하려는 경우 시스템 속성의 값 필드에 선택한 그룹의 시스템 ID를 추가할 수 있습니다.

주:
이 값을 변경하면 할당되지 않은 모든 VIT, AVIT 및 CVIT에 대한 알림이 지정한 그룹으로 전송됩니다.

시스템 속성 변경에 대한 자세한 내용은 을 참조하십시오 취약한 항목 및 정정 작업에서 할당 제거 .

자동으로 위험 애플리케이션 취약성 대응 계산

애플리케이션 취약성 계산기는 애플리케이션 취약한 항목(AVI)의 필드에 대한 초기 위험 값 계산을 자동화합니다. 위험 계산은 정정 우선순위에 대한 인사이트를 제공합니다. 각 계산기의 조건은 순서대로 평가되며 첫 번째로 일치하는 계산기가 사용됩니다.

애플리케이션 취약성 계산기

기본 시스템에는 애플리케이션 취약성 대응 애플리케이션 취약한 항목에 대한 기본 위험 점수를 설정하는 두 가지 취약성 계산기가 포함되어 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 기본 위험 계산기
- 고급 위험 계산기

조건 필터를 사용하여 모든 기준에 따라 AVI의 영향에 우선순위를 지정하고 평가하도록 애플리케이션 취약성 계산기를 빌드할 수 있습니다. 취약성이 비즈니스에 미치는 영향, CI(구성 항목)의 클래스, AVI의 기간 등에 관계없이 추가 취약성 계산기를 만들어 AVI의 다른 필드를 설정할 수 있습니다. 또는 기존 취약성 계산기를 사용자 지정할 수 있습니다. 계산기는 우선순위 집합을 반영하도록 작성할 수 있습니다. 자세한 내용은 내부 필터링 애플리케이션 취약성 관리 문서를 참조하십시오.

AVI에는 위험 계산기에서 파생된 위험 점수 값이 포함되어 있습니다.

주:
AVI는 소스 심각도 를 표시하지만 정규화된 심각도는 표시하지 않습니다. 정규화된 심각도는 계산기에서 위험 점수 값을 가져오는 데 사용되지만 AVI에는 표시되지 않습니다.

각 계산기에는 규칙 적용 시기를 결정하는 조건과 함께 계산기 규칙 목록이 포함되어 있습니다. 계산기를 실행하면 각 계산기 규칙의 조건이 순서대로 평가되고 첫 번째로 일치하는 계산기 규칙이 사용됩니다.

활성화된 모든 취약성 계산기는 AVI가 생성될 때마다, 연결된 CI 또는 취약성이 변경될 때마다 선택한 필드를 설정합니다.

기본 위험 계산기는 정규화된 취약성 심각도를 사용하여 AVI에 대한 위험 점수를 계산합니다.

주:
대상 필드(위험 점수)당 한 번에 하나의 계산기만 활성화할 수 있습니다.

기본 위험은 기본적으로 활성화되어 있습니다. 고급 위험 계산기는 기본적으로 비활성 상태입니다.

애플리케이션 취약성 계산기 규칙

기본 시스템 기본 위험 계산기 계산기에는 심각도에 따라 위험 점수 에 대한 각 심각도 수준(없음에서 위험)을 할당하는 계산기 규칙이 포함되어 있습니다. 알 수 없는 심각도 에는 위험 점수 100이 자동으로 할당됩니다. 이러한 값은 조정할 수 있으며 고급 위험 계산기와 마찬가지로 새 계산기 규칙이나 새 위험 규칙을 만들 수 있습니다.

주:
의 애플리케이션 취약성 대응v23.0부터 AVIT에서 위험 점수가 업데이트될 때마다 메모 섹션이 다음 세부 정보로 업데이트됩니다.

- 계산기 그룹 이름
- 계산기 이름: 계산기 규칙이 템플릿 또는 스크립트를 기반으로 하는지 여부에 따라 괄호 안에 이름이 세부 정보와 함께 추가됩니다. 계산기 규칙의 기초를 수정하거나 보려면 규칙을 선택하고 고급 보기 확인란을 선택합니다. 값 유형 드롭다운 상자에서 필요한 옵션을 선택합니다. 템플릿을 선택하면 규칙에 지정된 조건에 따라 위험 점수가 업데이트됩니다. 스크립트를 선택한 경우 기존 스크립트를 추가하거나 업데이트할 수 있습니다. 시스템 속성은 *sn_sec_cmn.risk_score_changes_add_worknotes* 작업 메모 섹션을 채우는 데 도움이 됩니다. 의 애플리케이션 취약성 대응v25.0.3부터 시스템 속성은 *sn_sec_cmn.risk_score_changes_add_worknotes* 기본적으로 비활성입니다. 이 기능을 사용하도록 설정한 경우에만 작업 메모 섹션에서 애플리케이션 취약한 항목의 위험 점수와 관련된 모든 변경 내용을 볼 수 있습니다. 또한 위험 점수가 변경된 경우에만 작업 메모가 업데이트됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

기본 시스템 고급 위험 계산기 계산기에는 기본 위험 규칙이라는 특수한 취약성 계산기 규칙이 포함되어 있습니다. 여러 값을 기준으로 위험 점수를 계산합니다.

- 취약성 심각도
- OWASP 상위 10개
- SAN 상위 25개

기본 위험 규칙의 기준을 사용자 지정할 수 있습니다. 자세한 내용은 위험 규칙에 대한 필드와 가중치 정의 문서를 참조하십시오.

기본 위험 규칙에 사용할 값과 이러한 각 값에 지정할 가중치를 조정할 수 있습니다. 가중치는 위험 점수를 설정할 때 각 요소 수를 조정하는 데 사용됩니다.

각 규칙에는 순서 설정이 있지만 조건과 일치하는 첫 번째 규칙이 AVI의 위험 점수 필드를 업데이트합니다. 일반적으로 스크립트되지 않은 계산기 규칙은 스크립트된 계산기 규칙보다 성능에 미치는 영향이 적습니다.

취약성 위험 점수 가중치

모든 취약성에는 심각도, 중요도, 악용 정보 등의 요인에 따라 위험 점수와 등급이 할당됩니다. 취약한 항목 테이블의 비즈니스 규칙은 *`Update Risk Rating from Risk Score`* 위험 등급 계산을 담당합니다. 위험 점수가 변경될 때마다 취약한 항목에 대한 위험 등급이 계산되어 채워집니다. (VR) 애플리케이션 버전 17.1 취약성 대응 이전에는 하드 코딩된 스크립트 포함 VulnerabilityUtils의 일부로 다음 위험 등급이 제공되었습니다.

값(위험 등급)	가중치(위험 점수)
1	90–100
2	70–89
3	40–69
4	1–39
5	0

의 18.0 버전 취약성 대응부터

- 위험 등급 유형은 기본 테이블에 avr_risk_rating으로 제공됩니다. 이러한 유형은 위험 등급이 계산되는 각 테이블에서 비즈니스 규칙의 일부로 전달됩니다.
- 위험 등급 계산을 위해 위험 점수 가중치 테이블 값의 항목을 쿼리할 수 있도록 스크립트가 수정됩니다.
- 기존 형식에 대한 항목을 추가하거나 새 형식을 만듭니다. 새 유형을 만들 때는 새 위험 등급에 대한 레이블을 추가하고 관련 스크립트 및 비즈니스 규칙도 수정해야 합니다. 또한 새 위험 점수에 대한 새 스타일을 추가해야 합니다.
- 스크립트를 수정하여 기본 테이블의 기록을 쿼리합니다.

필터 탐색기에 sn_sec_cmn_risk_score_weight 입력하여 위험 점수 가중치 테이블에 액세스할 수 있습니다.

또한 다음 시나리오에서는 위험 점수가 자동으로 다시 계산됩니다.

- CI(구성 항목)가 비인터넷 연결에서 인터넷 연결로 변경되는 경우
- 취약성 항목(VI)에 대한 관련 CVE(알반적인 취약성 및 노출) 또는 외부 공급업체 항목(TPE)이 CVE Known Exploit 취약성(KEV)에 연결되는 경우

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

위험 규칙에 대한 필드와 가중치 정의

조직에 고유한 취약성 및 자산 데이터를 사용하는 위험 점수를 생성할 수 있도록 위험 규칙의 매개변수와 가중치를 사용자 지정합니다. 위험 규칙에 포함된 필드를 선택하여 효과적인 위험 점수 매기기 프레임워크를 정의할 수 있습니다.

시작하기 전에

필요한 역할: sn_vul.app_manage_risk_score_configuration

프로시저

1. 다음으로 이동 모두 〉 애플리케이션 취약성 대응 〉 관리 〉 취약성 계산기.
2. 취약성 계산기 페이지에서 고급 위험 계산기를 클릭합니다.
3. 다음으로 이동 취약성 계산기 페이지 〉 취약성 계산기 규칙 탭 〉 기본 위험 규칙.
4. 옵션: 취약성 위험 규칙 페이지의 위험 계산기 기준 섹션에서 전체 위험 점수 계산에서 중요도에 따라 각 기준의 가중치를 설정합니다.
5. 규칙을 비활성화하려면 활성 확인란의 선택을 취소해야 합니다.
6. 위험 계산 기준에 위험 규칙 필드를 추가하려면 기준 추가를 클릭합니다.
7. 양식에서 필드를 채웁니다.

위험 규칙 필드 양식

필드	설명
참조 테이블 선택	위험 점수 가중치를 정의하는 데 사용하는 테이블입니다. 다음 옵션 중 하나를 선택할 수 있습니다. ○ 애플리케이션 취약한 항목: VI(취약한 항목)에서 직접 닷워킹 가능한 필드를 추가합니다. ○ 애플리케이션 취약한 항목 - 구성 항목: 하드웨어 테이블과 같은 기본 테이블 확장의 일부인 dot-walkable 필드를 추가합니다. 이러한 필드는 기본 테이블(cmdb_ci)의 일부가 아닙니다. ○ 애플리케이션 취약한 항목 - 취약성: 기본 테이블을 확장하는 테이블의 일부인 dot-walkable 필드를 추가합니다(예: 외부 공급업체 항목). 이러한 필드는 취약성 항목 기본 테이블에 속하지 않습니다. ○ 애플리케이션 취약한 항목 참조 테이블: 관련 테이블(m2m) 또는 취약한 항목에 대한 참조가 있는 테이블(m2m)의 일부인 필드를 추가합니다. 이 필드는 VI에서 직접 닷워킹할 수 없습니다. ○ 구성 항목 참조 테이블: cmdb_ci에 대한 참조가 있는 cmdb_ci 또는 테이블의 관련 테이블(m2m)에 속하는 필드를 추가합니다. 이 필드는 VI에서 직접 닷워킹할 수 없습니다. ○ 취약성 참조 테이블: sn_vul_entry에 대한 참조가 있는 sn_vul_entry 또는 테이블의 관련 테이블(m2m)에 속하는 필드를

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	추가합니다. 이 필드는 VI에서 직접 닷워킹할 수 없습니다. ○ 사용자 지정 조건: 조건을 평가하여 규칙에 가중치를 할당하려면 이 옵션을 사용합니다. 예를 들어 인터넷 연결 필터는 CI(구성 항목)가 외부인지 내부인지를 결정합니다.
테이블	참조 테이블 선택에서 다음 옵션 중 하나를 선택한 경우에만 나타나는 필드입니다. ○ 애플리케이션 취약한 항목 -> 구성 항목 ○ 애플리케이션 취약한 항목 -> 취약성 ○ 애플리케이션 취약한 항목 참조 테이블 ○ 구성 항목 참조 테이블 ○ 취약성 참조 테이블
필드	이 규칙에 대한 위험 점수 계산에 사용할 필드입니다.
집계	참조 테이블 선택에서 참조 테이블을 선택한 경우에만 나타나는 필드입니다. 관련 테이블(m2m)에서 필드를 선택할 때 계산에 고려할 최소값 또는 최대값을 선택합니다.
가중치	위험 규칙 내에서 이 필드의 가중치입니다. 값은 0에서 100 사이의 정수여야 합니다.
값 가중치 정의	각 필드 값에 가중치를 할당하는 구성요소입니다. 숫자 필드의 경우 필드 값을 범위(예: 1-5)로 정의할 수 있습니다. 가중치는 0에서 100 사이의 정수여야 합니다. 주: 참조 테이블 선택에서 사용자 지정 조건 옵션을 선택한 경우에는 이 필드가 표시되지 않습니다.
조건 테이블	참조 테이블 선택에서 사용자 지정 조건을 선택한 경우에만 나타나는 필드입니다. 목록에서 조건을 선택합니다.
필드 이름	참조 테이블 선택에서 사용자 지정 조건을 선택한 경우에만 나타나는 필드입니다. 위험 기준의 이름을 입력합니다.
조건	참조 테이블 선택에서 사용자 지정 조건을 선택한 경우에만 나타나는 필드입니다. 정의된 조건과 일치하는 이 테이블의 항목을 미리 봅니다.

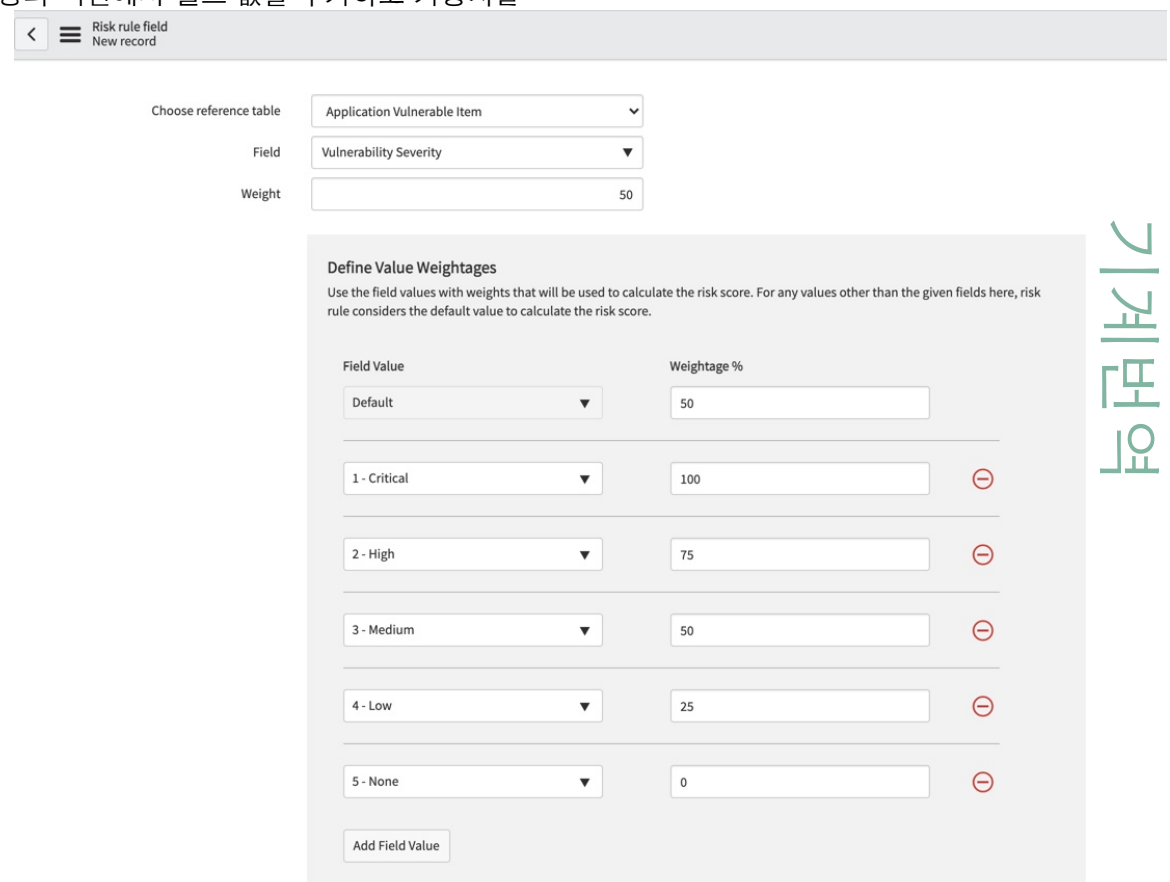
8. 제출을 클릭합니다.
9. 규칙 페이지에서 규칙을 활성화하고 다시 적용하여 활성 취약한 항목의 위험 점수를 다시 평가합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Example:
소스 심각도를 위험 규칙의 기준으로 추가합니다.

사용 사례: Qualys 및 Tenable과 같은 외부 공급업체 벤더는 자체 점수를 제공합니다. 이러한 점수는 sn_vul_entry 테이블의 소스 심각도 필드에 채워집니다. 이 필드는 위험 점수 계산에 사용합니다. 이 점수를 사용하여 위험 점수를 계산하려면 다음을 수행합니다.

1. 위험 규칙 페이지로 이동합니다.
2. 규칙을 비활성화하려면 활성 확인란의 선택을 취소합니다.
3. 위험 계산 기준에 위험 규칙 필드를 추가하려면 기준 추가를 클릭합니다.
4. 참조 테이블 선택 목록에서 애플리케이션 취약한 항목을 선택합니다.
5. 필드 목록에서 **Vulnerability.Severity**를 선택합니다.
6. 가중치 필드에 위험 규칙 내에서 이 필드의 상대적 중요도를 입력합니다. 값은 0에서 100 사이의 정수여야 합니다.
7. 값 가중치 정의 섹션에서 필드 값을 추가하고 가중치를



할당합니다. Submit Cancel
8. 제출을 클릭합니다.

관련 정보

Vulnerability Response 계산기 및 취약성 계산기 규칙

애플리케이션 취약성 계산기 생성

애플리케이션 취약성 계산기는 특정 조건이 충족될 때 대상 필드를 계산하는 미리 정의된 수식입니다. 애플리케이션 취약한 항목(AVI) 위험 점수를 계산하는 계산기에는 위험 규칙이 포함될 수 있습니다. 위험 계산은 정정 우선순위를 정하는 데 통찰력을 제공합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: App-Sec 관리자 그룹

주:
스크립트가 포함된 애플리케이션 취약성 계산기를 실행할 때 성능이 저하될 수 있습니다.

가장 간단한 규칙을 먼저 실행하도록 규칙을 정렬하십시오. 조건 및 템플릿 값 또는 위험 규칙으로 처리할 수 없는 항목에 대해서만 스크립트를 실행합니다.

프로시저

1. 다음으로 이동 모두 〉 애플리케이션 취약성 대응 〉 관리 〉 취약성 계산기.
2. 새로 만들기를 클릭합니다.
3. 양식의 필드에 적절히 입력합니다.

취약성 계산기 양식

필드	설명
이름	애플리케이션 취약성 계산기의 이름입니다.
테이블	AVI 테이블의 이름으로 자동으로 채워집니다.
애플리케이션	로 취약성 대응자동 채워집니다.
대상 필드	계산할 필드입니다.
설명	계산기에 대한 텍스트 설명입니다.
활성	계산기를 켜거나 끕니다.

4. 저장하려면 헤더를 마우스 오른쪽 버튼으로 클릭합니다.
취약성 계산기 규칙 섹션이 나타납니다.
5. 새로 만들기를 클릭하여 계산기에 대한 규칙을 생성합니다.

주:
새 위험 규칙 양식(대상 필드가위험 점수인 경우에만 사용 가능)은 10단계를 참조하십시오.

6. 필드에 적절한 정보를 입력합니다.

취약성 계산기 규칙 양식

필드	설명
이름	계산기 규칙의 이름입니다.
순서	취약성 계산기를 실행하는 순서입니다. 주문 항목이 100인 계산기는 주문 항목이 200인 계산기 앞에 실행됩니다.
계산기	상위 계산기로 자동으로 채워집니다.
활성	기본적으로 활성 확인란이 선택되어 있으며, 이는 계산기 규칙이 활성 상태임을 의미합니다. 이 확인란의 선택을 취소하면 시스템에서 생성된 새로운 취약한 항목에 이 규칙이 적용되지 않습니다.
고급 뷰	이 옵션을 선택하면 조건 유형 및 값 유형에서 스크립팅된 조건 및 스크립팅된 값을 선택할 수 있습니다.

7. 이 조건이 충족되는 경우 탭의 필드에 적절한 정보를 입력합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 조건이 충족될 경우 탭

필드	설명
조건 유형	고급 뷰를 선택한 경우에 사용할 수 있습니다. 선택 항목은 다음과 같습니다. ○ 필터: 필터 조건을 사용합니다. ○ 필터 그룹: 필터 그룹 생성 및 정의를 참조하여 계산기 기준을 정의합니다. ○ 스크립트: 이 계산기를 적용할 시기를 결정하는 데 사용되는 스크립트 조건입니다. 주: 계산기 적용 시기를 결정하기 위한 스크립트를 작성하기 전에 애플리케이션 취약성 계산기 목록으로 돌아가십시오. 기본 시스템과 함께 제공된 취약성 계산기 기록을 살펴봅니다.
조건	계산기 사용 여부를 결정하는 기본 필터 조건을 정의합니다. 필터 그룹 또는 스크립트 조건 유형을 선택하면 이 필드가 숨겨집니다.

8. 이 값 설정 탭을 클릭하고 양식의 필드에 적절한 정보를 입력합니다.

이 필드 탭 설정

필드	설명
값 유형	고급 뷰를 선택한 경우에 사용할 수 있습니다. 선택 항목은 다음과 같습니다. ○ 템플릿: 각 필드에 설정할 값을 정의합니다. ○ 스크립트: 각 필드의 값을 설정하는 데 사용됩니다.
스크립트 값	스크립트 값 유형을 선택한 경우 사용할 수 있습니다. 계산에 적용할 값을 정의합니다.
템플릿	계산기에 사용할 필드와 값을 선택합니다. 스크립트 값 유형 중 하나를 선택하면 이 필드가 숨겨집니다.

9. 모든 항목을 완료했으면 제출을 클릭합니다.

주:
기존 계산기를 편집하고 기존 점수를 모두 업데이트하려는 경우 계산기 다시 적용 버튼을 사용할 수 있습니다. 모든 활성 AVI를 통해 실행되며 해당 계산기를 사용하여 값을 설정하는 경우 해당 AVI의 값을 다시 계산합니다. 계산기를 다시 적용하는 데 시간이 오래 걸릴 수 있으므로 예약된 작업이 이를 처리합니다.

10. 새 위험 규칙 양식의 경우 필드에 적절한 정보를 입력합니다.

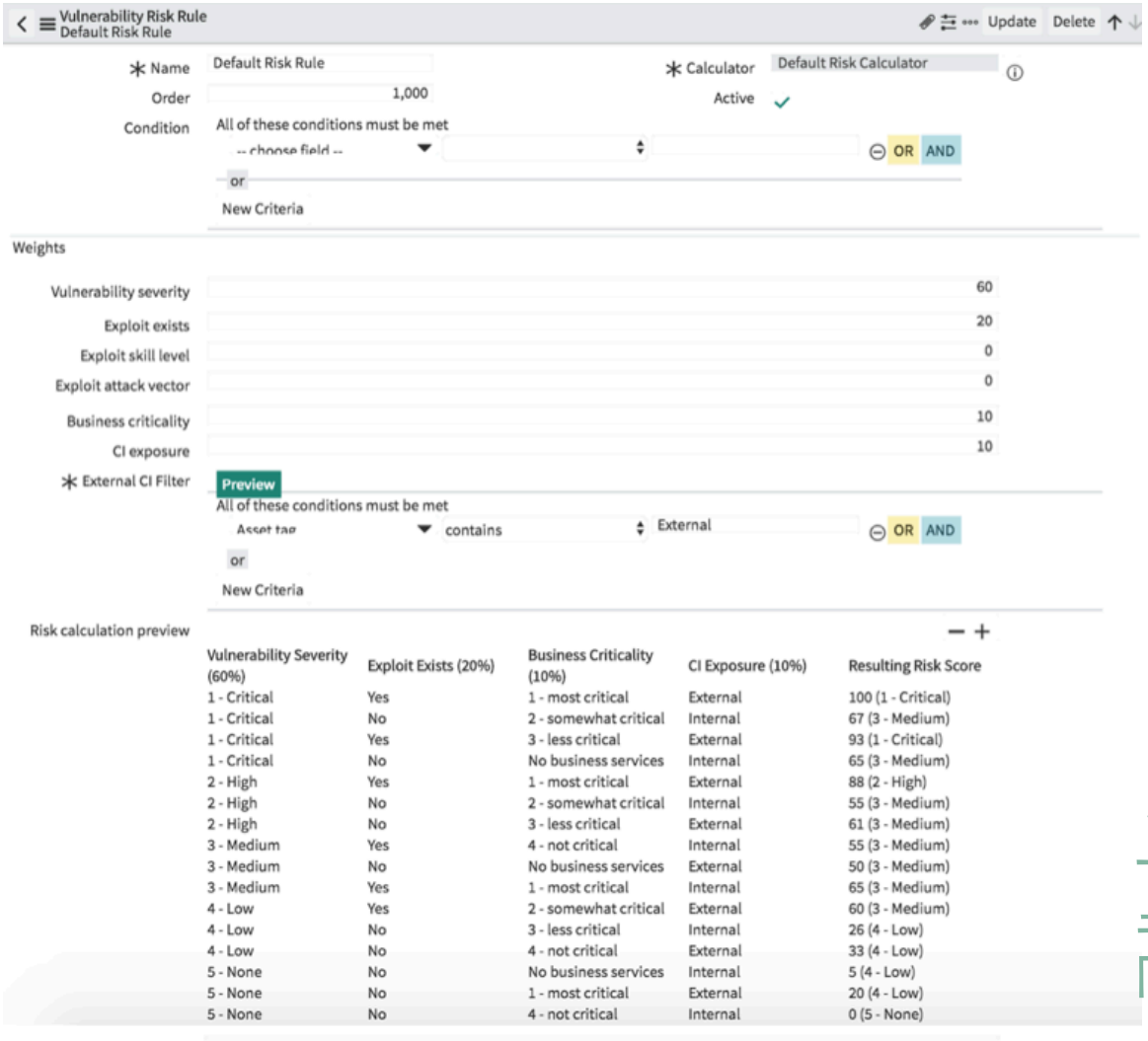
해당 값에서 가져와야 하는 결과의 백분율에 따라 각 가중치를 설정합니다. 스캐너가 제공하지 않는 데이터 또는 위험 점수의 일부가 아니어야 하는 데이터의 경우 가중치를 0으로 설정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

가중치를 업데이트하면 시나리오에 남은 가중치와 예상 위험 점수 결과가 표시됩니다.

필드	설명
이름	계산기 규칙의 이름입니다.
순서	계산기를 실행하는 순서입니다. 주문 항목이 100인 계산기는 주문 항목이 200인 계산기 앞에 실행됩니다.
계산기	상위 계산기로 자동으로 채워집니다.
활성	기본적으로 활성 확인란이 선택되어 있으며, 이는 계산기 규칙이 활성 상태임을 의미합니다. 이 확인란의 선택을 취소하면 시스템에서 생성된 새로운 취약한 항목에 이 규칙이 적용되지 않습니다.
조건	계산기 사용 여부를 결정하는 기본 필터 조건을 정의합니다. 필터 그룹 또는 스크립트 조건 유형을 선택하면 이 필드가 숨겨집니다.
가중치	
취약성 심각도	심각도에서 비롯된 결과의 백분율입니다.
OWASP 상위 10개	OWASP 상위 10개 목록에 취약성이 있을 때 발생하는 결과의 백분율입니다. 이 정보가 취약성에 없으면 가중치를 0으로 설정합니다.
SAN 상위 25개	SANS 상위 25개 목록에 취약성이 있을 때 발생하는 결과의 백분율입니다. 이 정보가 취약성에 없으면 가중치를 0으로 설정합니다.
누계	자동 계산된 백분율 합계. 이 값이 100에 도달하면 시나리오 미리 보기에 여러 시나리오의 샘플 위험 점수가 표시됩니다.
예제 시나리오	모든 가중치의 합계가 100%이면 위험 점수 시나리오가 표시되어 일부 가능한 시나리오에서 위험 점수의 미리 보기를 제공합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



11. 제출을 클릭합니다.

애플리케이션 취약한 항목의 심각도를 자동으로 매핑

애플리케이션 취약성 대응 심각도 매핑은 외부 공급업체 소스 심각도 필드를 내부의 인식 가능한 필드 취약성 대응로 변환합니다.

시작하기 전에
필요한 역할: App-Sec 관리자 그룹

이 태스크 정보
애플리케이션 취약성 대응 설치 시 심각도 매핑 제공과 같은 Veracode Vulnerability Integration 외부 공급업체 통합. 이러한 맵은 기존 맵의 필드를 변경하여 조정할 수 있습니다.

심각도 맵을 만들거나 편집하는 것은 사용자 환경에서 사용자 지정된 또는 비표준 외부 공급업체 매핑에만 사용되며 전문 지식이 필요합니다 애플리케이션 취약성 대응ServiceNow .

프로시저

1. 다음으로 이동 모두 〉 애플리케이션 취약성 대응 〉 관리 〉 표준화된 심각성 매핑.

2. 새로 만들기를 클릭합니다.

3. 양식의 필드에 적절히 입력합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드 매핑

필드	설명
소스	심각도 매핑에 대한 소스의 이름입니다.
소스 값	소스 심각도 값입니다.
대상 값	대상 심각도 값입니다. 선택 항목은 다음과 같습니다. ○ 1 - 심각 ○ 2 - 높음 ○ 3 - 보통 ○ 4 - 낮음 ○ 5 - 없음

4. 각 소스 심각도 수준에 대해 3단계를 반복합니다.
5. 제출을 클릭합니다.

내부 필터링 애플리케이션 취약성 관리

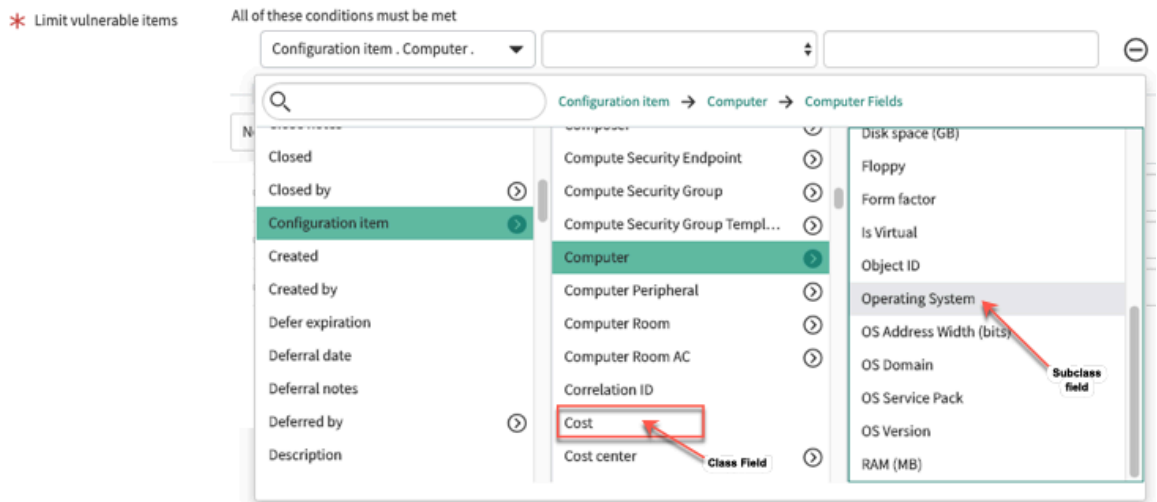
계산기 및 할당 규칙은 임포트 중 조건 작성기를 사용하여 생성된 조건을 사용합니다. 이러한 필터를 사용하여 각 기록을 평가하므로 기준을 변경하면 성능에 영향을 줄 수 있습니다.

기본 시스템과 함께 제공되는 규칙과 계산기는 성능에 최적화되어 있습니다. 규칙 또는 계산기를 편집하거나 생성할 때는 주의가 필요하며 두 가지 모두 ServiceNow 와 애플리케이션 취약성 대응 전문 지식이 필요할 수 있습니다. 즉, 몇 가지 지침을 사용할 수 있습니다.

하위 클래스 필드를 기준으로 필터링하지 마십시오.

일부 테이블은 확장을 지원합니다. CMDB CI [cmdb_ci] 테이블이 그 예입니다. cmdb_ci_hardware 및 cmdb_ci_computer와 같은 테이블은 이 테이블을 확장합니다. 상위 테이블에 없는 필드를 기준으로 필터링하는 경우 해당 필터를 구성하고 평가하는 데 비용이 많이 들 수 있습니다.

조건 필터 드롭다운 메뉴



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예를 들어 필터링: 구성 항목 〉 비용 **Cost**는 구성 항목의 하위 클래스 필드가 아니라 클래스 필드이므로 성능에 부정적인 영향을 주지 않습니다.

구성 항목 〉 컴퓨터그러나 다른 필드(이 경우 운영 체제)로 닷워킹이 필요한 하위 클래스입니다. 이 프로세스는 수백만 개의 취약한 항목을 임포트할 때 빠르게 추가되어 성능에 영향을 주는 몇 밀리초 정도 걸릴 수 있습니다.

주:
〔contains〕 조건을 사용하는 것은 와일드카드 검색과 비슷하며 성능에 영향을 줄 수 있습니다. 가능하면 〔is〕를 사용하는 것이 더 효율적입니다.

에서 정정 대상 추적 자동화 애플리케이션 취약성 대응

애플리케이션 정정 대상 규칙은 애플리케이션 취약한 항목(AVI)을 정정하기 위한 예상 기간을 정의하여 취약성 자체를 정정하기 위한 시간 범위를 제공합니다. 예를 들어 애플리케이션 취약한 항목에 위험한 위험 등급이 포함되어 있으면 해당 항목에 대한 취약성을 15일 이내에 수정해야 합니다.

App-Sec 관리자는 다음을 정의하여 애플리케이션 정정 대상 규칙을 생성할 수 있습니다.

- 정정 대상입니다.
- 미리 알림 대상입니다.
- [store-future: BEGIN review〕미리 알림 및 알림 수신자 - AVI가 미리 알림 또는 정정 목표 날짜가 지났고 정정되지 않은 경우 알림을 받아야 하는 사람입니다.[End]

애플리케이션 보안 관리자는 AVI 양식 및 목록 뷰에서 정정 목표 날짜를 볼 수 있지만 지연됨, 해결됨 또는 종결 됨 상태의 AVI에 대해서는 날짜가 업데이트되지 않습니다.

정정 목표 날짜는 다음과 같이 AVI 목록 뷰에 점으로 구분되어 있습니다.

- 알림 날짜에 도달하지 않은 AVI는 녹색으로 표시됩니다.
- 정정 목표 날짜에 근접한 AVI는 주황색으로 표시됩니다.
- 정정 목표 날짜가 지난 AVI는 빨간색으로 표시됩니다.

[store-future: BEGIN review〕하나 이상의 AVI가 정정 목표 날짜에 근접하거나 정정 목표 날짜가 지난 경우 애플리케이션 정정 대상 규칙에 따라 요약 이메일이 전송됩니다.[End]

기본 규칙

애플리케이션 취약성 대응 에는 기본적으로 비활성화되어 있는 세 가지 기본 규칙이 제공됩니다.

- 중요 위험 등급 규칙: 1 -중요 위험 등급이 있고 15일의 정정 목표이며 목표 날짜 **7** 일 전의 미리 알림이 있는 정정 대상입니다.
- 중간-높음 위험 등급 규칙: 2 -높음 또는 3-중간 위험 등급이 있고 30일의 정정 목표이며 목표 날짜 7일 전 의 미리 알림을 포함하는 정정 대상입니다.
- 덜 중요한 위험 등급 규칙: 위험 등급이 4-낮음 이고, 정정 목표가 45일이며, 목표 날짜 7일 전에 미리 알림을 제공하는 정정 대상입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

정정 대상 규칙은 비활성화하거나 삭제할 수 있습니다.

규칙이 비활성화되면 규칙이 적용된 AVI의 현재 정정 대상 날짜가 지워집니다. AVI가 활성 규칙을 만족하면 해당 규칙이 적용되고, 그렇지 않으면 AVI에 규칙 또는 대상 날짜가 없으며 해당 상태는 대상 없음입니다.

규칙이 삭제되면 종결된 AVI의 정정 대상 날짜와 관련 필드는 유지됩니다. 종결되지 않은 AVI의 정정 목표 날짜와 관련 필드가 지워지고 모든 종속 규칙이 다시 적용됩니다.

정정 규칙 시나리오

동일한 AVI에 여러 정정 대상 규칙이 적용되면 가장 제한적인 규칙이 적용됩니다.

예를 들어 AVI가 두 애플리케이션 정정 대상 규칙에 대한 조건을 충족하는 경우:

시나리오: AVI는 2018년 3월 1일 10:00:00에 마지막으로 열렸습니다.

- 애플리케이션 정정 대상 규칙 1: 2018년 3월 7일에 마지막으로 오픈되었습니다. 정정 목표는 마지막으로 오픈된 이후 15일입니다. 계산된 정정 목표 날짜는 03/16/2018 10:00:00입니다.
- 애플리케이션 정정 대상 규칙 2: 2018년 3월 10일에 마지막으로 오픈되었습니다. 정정 목표는 마지막으로 오픈된 이후 10일입니다. 계산된 정정 목표 날짜는 03/11/2018 10:00:00입니다.

이 시나리오에서는 애플리케이션 정정 대상 규칙 2가 더 제한적인 날짜를 가지고 있으므로 AVI에 적용됩니다. AVI가 처음 식별된 이후 10일 대 15일.

주:
애플리케이션 정정 목표는 마지막으로 개시 된 날짜와 일 수(24시간 단위로 측정)의 합계로 계산됩니다. 양식 레이아웃 슬러시버킷에서 AVI 양식에 이 필드를 추가할 수 있습니다. 인스턴스에서 AVI가 가장 최근에 열린 날짜입니다.

V17.1부터 정정 대상은 대상(날짜)부터 계산됩니다. 기본값은 마지막 개시 날짜로 유지됩니다.

주:
애플리케이션 정정 대상 규칙이 정의되면 예약된 작업 또는 정정 대상 규칙 목록 뷰의 변경 내용 적용 버튼에 의해 *Evaluate remediation targets* 정정 대상 날짜가 계산됩니다.

정정 대상 평가 예약된 작업 정보

Evaluate remediation targets 매일 4:00:00에 한 번 실행됩니다.

Evaluate remediation targets 정정 목표 날짜가 가장 빠른 규칙부터 시작하여 활성 상태인 모든 취약성 규칙을 반복합니다. 다음과 같은 모든 AVI를 살펴봅니다.

- 종결, 연기됨 또는 해결됨 상태가 아닙니다.
- 정정 대상 날짜가 없습니다.
- 정정 목표 날짜가 애플리케이션 정정 대상 규칙의 날짜보다 나중이어야 합니다.

Evaluate remediation targets 정정 목표 날짜가 없거나 이 규칙이 기록에 있는 날짜보다 이전 날짜를 포함하는 경우 정정 목표 날짜를 추가합니다. 마지막으로 AVI 양식의 정정 목표 날짜 및 정정 상태 필드를 업데이트합니다. 비활성 규칙의 경우 정정 대상 평가 는 AVI의 정정 필드를 지웁니다.

정정 대상 규칙 다시 적용

정정 대상 규칙을 변경할 때 정정 대상 규칙 목록 페이지의 변경 내용 적용 버튼을 사용하여 종결, 연기 또는 해결됨 상태의 AVI를 제외한 모든 활성 AVI에서 변경된 모든 규칙을 다시 실행합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

예약된 작업이 실행 중인 *Evaluate remediation targets* 경우 다시 적용 프로세스를 시작할 수 없습니다. 그러나 다시 적용 프로세스가 이미 실행 중이고 예약된 작업이 트리거되면 병렬로 실행됩니다.

의 재적용 프로세스는 취약성 대응 독립적 애플리케이션 취약성 대응 이며 병렬로 실행할 수 있습니다.

애플리케이션 정정 대상 규칙 생성 또는 편집

애플리케이션 취약한 항목(AVI) 수준에서 정정 대상 규칙을 설정하여 고위험 취약성을 적시에 정정합니다.

시작하기 전에

필요한 역할: App-Sec 관리자 그룹

주:
기본 시스템에는 세 가지 정정 대상 규칙이 함께 제공됩니다.

- 중요 위험 등급 규칙
- 위험하지 않음 위험 등급 규칙
- 중간-높음 위험 등급 규칙

이러한 규칙은 기본적으로 비활성화되어 있습니다. 새 항목을 만드는 대신 하나를 편집하도록 선택하는 경우 저장하기 전에활성 상자를 선택해야 합니다.

프로시저

1. 다음으로 이동 모두 〉 애플리케이션 취약성 대응 〉 관리 〉 정정 대상 규칙.
2. 새로 만들기를 클릭합니다.
3. 양식의 필드에 적절히 입력합니다.

필드	설명
이름	규칙의 이름입니다.
목표(일수)	마지막으로 열린 이후 AVI를 정정해야 하는 일 수를 지정합니다.
V17.1: 대상 시작일(날짜)	목표 SLA가 계산된 시작 날짜입니다. 날짜 또는 날짜 및 시간 유형 필드만 지정할 수 있습니다. 기본값은 마지막으로 열린 날짜입니다. 이 필드의 값을 사용자 지정하려면 KB1642413 문서를 참조하십시오.
활성	기본적으로 활성 확인란이 선택되어 있으며, 이는 정정 대상 규칙이 활성 상태임을 의미합니다. 이 확인란의 선택을 취소하면 이 규칙은 시스템에서 생성된 새 AVI에 적용되지 않습니다.
알림(기한 이전 남은 일수)	미리 알림을 설정할 대상 정정 시간 이전의 일 수입니다. 이 값을 사용하여 계산된 알림 날짜는 정정 상태 및 색상 코딩을 표시하는 데 사용됩니다. 날짜가 알림 날짜 이전인 경우 정정 상태는 "전송 중"입니다. 알림 날짜를 지나 정정 목표 날짜 이전이면 상태가 목표에 임박한 것으로 표시됩니다. 주: 이 필드를 0으로 설정하면 대상 누락 알림만 설정됩니다.
규칙 적용 대상	조건 필터를 사용하여 AVI에 규칙을 적용하기 위한 기준을 선택합니다. 성능 영향을 방지하려면 전체 생산 규모에서 조건을 테스트하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	테스트를 통해 의 조건과 규모에 따라 정정 대상 평가 작업을 실행하는 데 걸리는 시간을 확인할 수 있습니다 구성 관리 데이터베이스(CMDB).
업데이트 이력	
활동	규칙을 처음 생성하는 데 사용되지 않습니다. 이어서 시스템 작업 메모가 여기에 로깅됩니다.

4. 제출을 클릭합니다.
   이 규칙은 예약된 작업 ***Evaluate remediation targets***, 의 다음 실행 중에 적용됩니다. 기존 규칙이 업데이트되거나 정정 대상 규칙 목록 뷰에서 변경 내용 적용 버튼을 사용하는 경우에도 마찬가지입니다. 기존 규칙이 업데이트될 때도 마찬가지입니다. 예약된 작업 및 변경 적용 에 대한 자세한 내용은 문서를 참조하십시오 에서 정정 대상 추적 자동화 애플리케이션 취약성 대응.

애플리케이션 취약한 항목의 정정 대상 상태 보기

애플리케이션 취약한 항목(AVI)이 정정 대상 규칙에 정의된 정정 목표 날짜에 거의 도달했거나 지났을 경우 AVI 기록이 상태로 업데이트됩니다. 이 정보는 예정된 정정 활동을 사전에 모니터링하는 데 도움이 될 수 있습니다.

시작하기 전에
필요한 역할: App-Sec 관리자 그룹

이 태스크 정보
정정 대상 평가 예약된 작업은 하루에 한 번씩 실행되어 현재 날짜를 연결된 정정 대상 규칙에 지정된 취약한 항목 정정 날짜와 비교합니다. 현재 날짜가 정정 기한이 지나기 전 일 수 내에 있으면 정정 상태가 취약한 항목 기록에 추가됩니다.

프로시저

다음으로 이동 모두 〉 애플리케이션 취약성 대응 〉 취약 항목.
AVI에 대한 정정 날짜가 정정 대상 규칙에 설정된 조건 범위 내에 있는 경우 취약한 항목 목록 뷰에 표시되는 정정 대상 상태 열을 확인합니다. AVI에 대한 정정 목표 날짜가 지난 경우 AVI 양식에 주석이 나타납니다.

> **주:**
> 대상, 진행중 및과거 대상에 접근하는 AVI 수를 보려면 애플리케이션 취약성 관리(PA) 대시보드를 참조하십시오.

관련 정보

애플리케이션 정정 대상 규칙 생성 또는 편집

정정 작업 닫기

애플리케이션 정정 작업과 관련된 문제를 추가 분석 없이 즉시 종결할 수 있는 것으로 확인되면 종결 기능을 사용할 수 있습니다. v23.0 부터 취약성 대응애플리케이션 정정 작업에 대한 닫기 버튼이 제거되었습니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
취약성 대응 작업 공간에서 정정 작업은 이전 버전의 취약성 대응에서 이전에 수행한 정정 작업과 동일한 상태를 통해 전환됩니다. 정정 작업의 모든 취약한 항목(VIT)이 닫히면 정정 작업이 비활성 상태로 전환됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

중요사항:
상태 동기화를 사용하도록 설정된 해당 기록의 수명주기 상태를 통해 변경 요청 및 정정 작업을 수동으로 이동할 수 있지만, CHG가 상태를 변경했다고 시스템이 등록하거나 CHG를 추가 또는 정정 작업에서 제거하면 상태 동기화가 수동 개입을 재정의할 수 있습니다. 그러나 변경 요청 상태는 정정 작업을 ## 또는 ### 상태에서 자동으로 이동하지 않습니다.

프로시저

1. 검토를 요청할 기록을 엽니다.
2. 닫기 단추를 선택합니다.
3. 양식의 필드에 적절히 입력합니다.

필드	설명
상태	상태를 종결로 선택합니다.
이유	문제를 종결하는 이유를 입력합니다.
추가 정보	기타 관련 정보를 입력합니다.

4. 제출을 선택합니다.
정정 작업이 종결로 표시됩니다.

애플리케이션 취약성 대응용 **Change Management**

애플리케이션 취약성 대응 애플리케이션의 정정 작업에서 변경 요청을 생성하여 수동 개입이 필요한 AVIT(애플리케이션 취약성)에 대한 조사를 신속하게 처리합니다.

CI(구성 항목)로 분류된 검사한 애플리케이션에 대해 미리 채워진 정보로 변경 요청을 생성하면 수동 개입이 필요한 AVIT(애플리케이션 취약성)에 대한 조사를 신속하게 처리할 수 있습니다.

- 의 애플리케이션 취약성 대응 변경 요청 워크플로우는 에서 취약성 대응지원하는 워크플로우와 유사합니다.
- 변경 요청 워크플로우에 취약성 대응 대한 자세한 내용은 다음 문서를 참조하십시오 를 위한 변경 관리 취약성 대응.

애플리케이션 정정 작업에 대한 변경 요청 생성

애플리케이션 보안 관리자 또는 보안 챔피온은 애플리케이션 취약성 대응 애플리케이션의 정정 작업에서 변경 요청을 생성할 수 있습니다.

시작하기 전에
필요한 역할:

취약성 관리자 관리자 작업 공간에서: sn_vul.app_sec_manager

ITRem 소유자 작업 공간에서: sn_vul.app_sec_champion 또는 sn_vul.app_developer, itil 역할.

이 태스크 정보
클래식 환경에서 변경 요청을 만들려면 아래 나열된 단계를 따르십시오.

정정 작업에서 직접 변경 요청을 생성, 승인, 구현, 검토 및 종결할 수 있습니다. 정정 작업에서 미리 채워진 정보로 세 가지 유형의 변경 요청을 생성할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 표준. 위험이 적고, 비교적 일반적이며, 지정된 절차나 작업 지시를 따르는 사전 승인된 변경입니다.
- 보통. 일반 변경 요청은 구현, 검토 및 종결 전에 두 가지 수준의 승인이 필요한 후속 대응적 프로세스를 따릅니다.
- 비상. 중요 인시던트를 해결하기 위한 변경입니다.

주:
검색된 애플리케이션이 CI(구성 항목)와 연결된 경우에만 애플리케이션 취약성 대응에 대한 변경 요청이 지원되며, 이는 제품 모델 사용 〔sn_vul.use_product_model〕 시스템 속성에서 '제품 모델'을 '아니오'로 설정한 경우에만 발생합니다.

프로시저

1. 기존 정정 작업 기록에서 완전한 변경 요청을 생성하려면 다음으로 이동합니다. 모두 〉 애플리케이션 취약성 대응 〉 정정 작업 〉 사용자 그룹에 할당됨.
   할당 그룹에 할당된 정정 작업 목록이 표시됩니다.
2. 옵션: 다음으로 이동 모두 〉 애플리케이션 취약성 대응 〉 정정 개요 을 클릭하여 정정 개요 대시보드를 보고 사용자 또는 할당 그룹에 할당된 VUL을 찾습니다.
3. 또는 번호 열에서 정정 작업을 클릭하여 기록을 열고 상세 정보를 봅니다.
   기록이 표시됩니다.
4. 변경 요청을 생성할 APP-VUL 레코드가 표시되면 레코드의 오른쪽 상단에서 변경 생성을 클릭합니다.
   변경 요청 생성 양식이 표시됩니다.
5. 필드에 내용을 입력합니다.

   a. 적용 대상 필드의 선택 목록에서 하나를 선택하여 계속합니다.

옵션	설명
이 그룹의 모든 활성 애플리케이션 취약한 항목	이 항목을 선택한 경우, 변경 생성을 클릭하면 상태가 종결됨이 아닌 이 정정 작업에서 모든 활성 애플리케이션 취약한 항목이 변경 요청에 자동으로 추가됩니다.
이 그룹에서 조건 세트와 일치하는 모든 애플리케이션 취약한 항목	선택하면 아래 두 번째 그림과 같이 조건 작성기가 표시됩니다. 새 변경 요청에 필요한 취약한 항목을 식별하기 위한 필터 기준을 입력합니다. 필터의 예로는 특정 검색 조건과 일치하는 취약한 항목만 포함될 수 있습니다. 상태가 오픈이고 위험 점수 가 **75** 보다 큽니다. 조건을 입력하면 기준(10)과 일치하는 AVIT 수와 함께 메시지가 표시됩니다. 일치하는 항목을 미리 볼 수 있는 링크(일치하는 항목 미리 보기)가 표시됩니다. 필터 조건과 일치하는 항목이 없으면 조건 작성기 아래에 필터를 조정하라는 메시지가 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵션	설명
	변경 생성을 클릭하면 이 조건 필터와 일치하는 모든 애플리케이션 취약한 항목이 새 정정 작업으로 이동합니다. 이 변경 요청은 새 정정 작업에 연결됩니다.

조건 세트와 일치하는 작업의 애플리케이션 취약한 항목에 대한 변경 요청 양식 생성

b. 옵션: 양식에 표시되면 일치하는 항목 미리 보기 링크를 클릭하여 필터 기준과 일치하는 AVIT 목록을 확인합니다.
정정 작업 목록 미리 보기가 표시됩니다. 이 미리 보기 목록에서 항목을 선택하고 UI 작업을 수행할 수 있지만 이러한 작업은 APP-VUL에서도 수행됩니다. 예를 들어 미리 보기 목록에서 VI를 삭제하면 해당 AVIT도 APP-VUL에서 삭제됩니다.

c. 미리 보기를 마친 후 브라우저 창을 닫아 변경 요청 양식을 반환합니다.

d. CR에 CI 추가 확인란에서 하나를 선택하여 계속합니다.

옵션	설명
CR에 CI 추가 확인란 선택됨	기본값은 선택되어 있습니다. 확인란을 선택하면 이 정정 작업의 활성 취약한 항목에 속하는 모든 CI(구성 항목)가 변경 요청에 추가됩니다. APP-VUL은 자동으로 ## ## # 상태로 이동합니다.
CR에 CI 추가 확인란 선택 취소	이 정정 작업의 활성 애플리케이션 취약한 항목의 CI가 새 변경 요청에 추가되지 않도록 하려면 확인란의 선택을 취소합니다. 사용하지 않도록 설정하면 변경 요청의 상태가 APP-VUL과 동기화되지 않고 APP-VUL은 현재 상태로 유지됩니다.

e. 변경 유형 필드의 선택 목록에서 하나를 선택하여 계속합니다.

유형 변경	설명
긴급	중요 인시던트를 해결하기 위한 변경입니다.
정상	표준 또는 긴급 변경이 아닌 서비스에 대한 변경을 구현하는 데 사용되는 변경 유형입니다.
표준	자주 구현되는 사전 승인되고 위험도가 낮은 변경 요청입니다. 승인된 표준 변경 요청은 표준 변경을 보다 효율적으로 액세스하고 요청할 수 있도록 템플릿 카탈로그에서 사전 정의될 수 있습니다. 선택하면 두 개의 필드가 표시됩니다. 각 선택 목록에서 하나를 선택하여 다음 필드를 채웁니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

유형 변경	설명
	▪ 범주 변경: 기존 카탈로그에서 변경할 범주(예: ####, ## ## ##, #####)를 선택합니다. 이 예에서는 ## ## ## ## 이 선택되어 있습니다. ▪ 변경 템플릿: 카탈로그에서 미리 정의된 지원 작업이 있는 변경 요청에 사용할 수 있는 템플릿 하나를 선택합니다. 이 예에서는 Microsoft ## ## ## 템플릿이 선택되어 있습니다. ITSM 변경 요청 범주, 템플릿 및 변경 유형에 대한 자세한 내용은 변경 유형을 참조하십시오.

이 기능은 ITSM Change Management의 카탈로그에 설정한 변경 요청 유형을 자동으로 읽습니다. 예를 들어, ITSM의 표준 변경 요청 이름을 ## 에서 ## ##됨으로 변경하면 다음 그림과 같이 변경 요청 생성 소스의 변경 유형 선택 목록에 새 이름이 자동으로 표시됩니다.

양식의 변경 요청 미리 보기 섹션에 있는 필드는 APP-VUL의 정보로 미리 채워집니다. 필요한 경우 이러한 필드 값을 편집할 수 있습니다. 예를 들어, 다음 그림의 필드에 있는 값을 검토합니다.

계획된 종료 날짜

이 날짜(2019-10-10)는 APP-VUL의 정정 대상 날짜 필드에 표시되는 값과 동일합니다. 이 값은 APP-VUL에 속한 애플리케이션 취약한 항목의 가장 빠른 정정 목표 날짜에서 파생됩니다. 이전 정정 날짜가 필요한 중요한 문제에 대한 변경 요청을 생성하는 경우 이 값과 우선순위 필드의 값을 편집하는 것이 좋습니다.

근거

이 필드에는 CHG에 추가된 CI 수가 표시됩니다. 추가 정보를 추가하려면 이 텍스트를 편집하는 것이 좋습니다. 예를 들어, 새 APP-VUL을 생성하는 데 사용한 필터(예: ## ### 75## #)에 대한 메모를 이 필드에 추가하는 것을 선호할 수 있습니다. 이 텍스트는 새 변경 요청 및 정정 작업을 찾는 데 도움이 됩니다.

구축 계획

이 필드에는 취약성에 대한 기본 솔루션이 표시됩니다.

할당 그룹 및 할당 대상

할당 그룹을 변경하거나 이 변경 요청을 할당 그룹 중 하나의 사용자에게 재할당하려면 이러한 필드를 편집합니다.

6. 필요에 따라 필드를 계속 미리 보고 편집합니다.
7. 변경 내용을 저장하고 이 페이지에 남아 있으려면 폼 위쪽의 회색 배너를 마우스 오른쪽 버튼으로 클릭하고 삽입 및 유지를 선택합니다.
8. 편집을 완료한 후 하나를 선택하여 계속합니다.

주:

할당 그룹 및 할당 대상 필드가 할당되지 않은 ## ### 정정 작업의 경우(비어 있음) 변경 생성을 클릭하면 현재 로그온한 사용자가 작업에 자동으로 할당됩니다. 또한 CR에 CI 추가 확인란을 선택해야 합니다. VUL 상단에 이 할당을 나타내는 파란색 확인 메시지가 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 수행할 작업
변경 요청 및 변경 작업을 모니터링하여 완료되었고 변경 요청이 구현되었는지 확인합니다. 이 CHG가 구현되고 ## 상태로 이동한 후 상태 동기화가 활성화되면 APP-VUL이 자동으로 ###으로 이동합니다.

정정 작업을 기존 변경 요청에 연결

AppSec 관리자 또는 보안 챔피온은 정정 작업(APP-VUL)을 인스턴스에서 이미 사용할 수 있는 변경 요청에 연결하여 정정 작업을 해결할 때 중복 변경 요청(CHG)을 생성하지 않도록 합니다.

시작하기 전에
필요한 역할:

취약성 관리자 관리자 작업 공간에서: sn_vul.app_sec_manager

ITRem 소유자 작업 공간에서: sn_vul.app_sec_champion 또는 sn_vul.app_developer, itil 역할.

이 태스크 정보
정정 소유자는 본인 또는 할당 그룹에 할당된 정정 작업을 정정 작업 기록에서 직접 기존 변경 요청에 연결할 수 있습니다. 다음 이미지는 변경 요청을 기존 APP-VUL(VG)에 연결하는 기본 플로우를 보여줍니다.

주:
기존 변경 요청은 모든 상태(Open, Under Investigation, Awaiting Implementation, Closed 및 Deferred)의 APP-VUL에 연결할 수 있습니다. 변경 요청을 기존 VUL에 연결하면 활성 VI만 변경 요청에 추가됩니다.

시작하기 전에 중복 변경 요청의 생성을 방지하기 위해 APP-VUL과 이미 연결된 기존 변경 요청을 보는 것이 좋습니다. 특정 APP-VUL과 관련된 변경 요청 수를 쉽게 추적하려면 정정 작업 목록에서 CR 카운트 열을 참조하십시오. 표시되지 않으면 오른쪽 상단에 있는 설정 아이콘()을 클릭합니다. CR 카운트 열을 사용 가능에서 선택됨으로 이동하고 확인을 클릭합니다.

새 열을 자동으로 채우려면 이 테이블에 기존 데이터가 있는 고객의 경우 예약된 작업인 # CR ### # ###를 실행합니다.

프로시저

1. 정정 작업을 기존 변경 요청에 연결하려면 다음으로 이동합니다. 모두 〉 애플리케이션 취약성 대응 〉 정정 작업.
2. 작업 중인 정정 작업을 찾습니다.
3. 옵션: 다음으로 이동 모두 〉 애플리케이션 취약성 대응 〉 정정 개요 을 클릭하여 정정 개요 대시보드를 보고 사용자 또는 할당 그룹에 할당된 APP-VUL을 찾습니다.
4. 번호 열에서 APP-VUL 레코드를 클릭하여 엽니다.
   APP-VUL 레코드가 표시됩니다.
5. 열린 기록이 표시된 상태에서 아직 표시되지 않았다면 변경 요청 관련 목록으로 스크롤하여 선택합니다.
   APP-VUL과 관련된 모든 변경 요청은 추가 버튼과 함께 표시됩니다. 다음 그림에는 이 APP-VUL과 이미 연결된 변경 요청이 없습니다.
6. APP-VUL을 기존 CHG와 연결하려면 추가를 클릭합니다.
   정정 작업에 기존 변경 요청 추가 양식이 표시됩니다.
7. 양식에서 검색 아이콘을 클릭합니다.
   다음 그림과 같이 기존 변경 요청의 목록 뷰가 새 창에 표시됩니다.
8. 표시된 목록에서 항목을 선택하거나, 필터()를 클릭하고 조건을 입력하여 검색 결과를 제한합니다.
9. CR에 CI 추가 확인란에서 하나를 선택하여 계속합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
이 확인란은 ## 상태의 기존 변경 요청에 대해서만 표시됩니다.

옵션	설명
CR에 CI 추가 확인란 선택됨	기본값은 선택되어 있습니다. 확인란을 선택하면 이 정정 작업의 활성 취약한 항목에 속하는 모든 CI(구성 항목)가 변경 요청에 추가됩니다. 선택하면 변경 요청의 상태가 APP-VUL로 동기화됩니다. 자세한 내용은 변경 요청과 정정 작업 간의 상태 동기화 문서를 참조하십시오.
CR에 CI 추가 확인란 선택 취소	이 정정 작업의 활성 취약한 항목의 CI가 새 변경 요청에 추가되지 않도록 하려면 확인란의 선택을 취소합니다. 사용하지 않도록 설정하면 변경 요청의 상태가 APP-VUL과 동기화되지 않고 APP-VUL은 현재 상태로 유지됩니다.

10. 변경 요청 검색 필드에 표시할 변경 요청 번호를 선택하고 제출을 클릭합니다.
APP-VUL이 표시됩니다. 기록 상단에 선택한 변경 요청이 APP-VUL에 성공적으로 연결되었음을 나타내는 파란색 확인 메시지가 표시됩니다.

주:
할당 그룹 및 할당 대상 필드가 할당되지 않은 ## 상태의 APP-VUL의 경우(비어 있음) 추가를 클릭하면 현재 로그온한 사용자가 APP-VUL에 자동으로 할당됩니다. 또한 CR에 CI 추가 확인란을 선택해야 합니다. APP-VUL 상단에 현재 사용자가 할당되었음을 나타내는 파란색 확인 메시지가 표시됩니다.

다음에 수행할 작업
APP-VUL 기록을 검토합니다. 변경 요청 관련 목록의 변경 요청 열에서 새 CHG에 대한 링크를 클릭하여 CR 기록을 봅니다. 오픈 CHG 기록에서 변경 요청의 상태를 모니터링할 수 있습니다. 영향을 받는 CI(구성 항목) 및 정정 작업이 영향을 받는 CI 및 정정 작업 관련 목록에 표시됩니다.

침투 테스트

의 애플리케이션 취약성 대응 침투 테스트를 통해 애플리케이션 소유자는 애플리케이션의 보안 태세를 평가할 수 있습니다. 윤리적 해킹 팀이 애플리케이션을 수동으로 테스트하는 것입니다.

필요한 역할

침투 테스트에는 다음과 같은 역할이 필요합니다.

App-Sec 관리자: 침투 테스트 평가 요청을 관리하는 보안 관리자 및 애플리케이션 소유자를 포함합니다. 여기에는 다음과 같은 세분화된 역할이 포함됩니다.

- sn_vul.app_관리_pen_테스트_요청
- sn_vul.app_read_all
- cmdb_read

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

윤리적 해커: 애플리케이션의 침투 테스트를 수행하는 윤리적 해킹 팀의 구성원을 포함합니다. 여기에는 다음과 같은 세분화된 역할이 포함됩니다.

- sn_vul.app_update_assignment_group입니다.
- sn_vul.app_update_assigned_to
- sn_vul.app_manage_manual_avits
- sn_vul.app_manage_pen_test_request_config
- itil
- sn_vul.app_read_all
- sn_vul.app_관리_pen_테스트_요청
- sn_vul.app_update_state입니다.

이러한 역할에 대한 자세한 내용은 다음 문서를 참조하십시오 애플리케이션 취약성 대응 사용자 그룹 및 역할.

의 v19.0 취약성 대응부터 를 사용하는 Veracode Vulnerability Integration경우 의 침투 평가 테스트는 Veracode Vulnerability Integration 의 수동 결과 Veracode입니다. 에서 구성하는 애플리케이션 취약성 대응침투 테스트 평가 요청에는 연결되지 않습니다. 의 Veracode침투 테스트 평가에 대한 자세한 내용은 를 Veracode Vulnerability Integration참조하십시오.

침투 테스트 수명 주기

애플리케이션 소유자는 윤리적 해킹 팀에 애플리케이션의 침투 테스트 평가를 요청할 수 있습니다. 윤리적 해킹 팀은 이 요청에 따라 조치를 취하고 침투 테스트 결과를 생성합니다. 이러한 결과는 수동으로 생성된 애플리케이션 취약한 항목(AVI)입니다.

침투 테스트 워크플로우는 테스트 요청 제기부터 윤리적 해킹 팀의 결과 해결에 이르기까지 침투 테스트 수명주기를 다룹니다.

침투 테스트 평가 요청

v19.0부터 다음 위치에서 새 요청을 생성하거나 기존 요청을 복사할 수 있습니다. 모두 〉 침투 테스트 평가 요청 〉 모두.

v19.0 이전에는 애플리케이션 소유자가 ITSM 서비스 카탈로그를 사용하여 애플리케이션에 대한 침투 테스트 평가를 요청할 수 있었습니다.

침투 테스트 평가 요청 검토

윤리적 해킹 팀은 침투 테스트 평가 요청의 애플리케이션과 범위를 검토하고 평가하여 기존 백로그에 추가합니다.

환경 준비

그런 다음 윤리적 해킹 팀은 애플리케이션 소유자에게 테스트를 시작할 수 있는 환경을 제공하라는 요청을 보냅니다. 환경이 준비되면 애플리케이션 소유자는 윤리적 해킹 팀에 알립니다.

테스트 요청 구성에 대한 자세한 내용은 다음 문서를 참조하십시오 침투 테스트 구성.

침투 테스트 결과 테스트 및 보고

윤리적 해킹 팀은 애플리케이션을 테스트하고 그 결과를 애플리케이션 소유자에게 보고합니다. 또한 윤리적 해킹 팀은 정정 목표 날짜를 사용하여 침투 테스트 결과에 대한 서비스 수준 계약(SLA)을

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

정의합니다. 이러한 결과는 수동으로 생성된 AVI입니다. 애플리케이션 소유자는 윤리적 해킹 팀에서 만든 AVI를 검토합니다. 수정 사항을 계획하고 애플리케이션 팀에 할당합니다.

주:
정정 대상 규칙은 침투 테스트 결과에 적용되지 않습니다.

윤리적 해킹 팀은 AVE(애플리케이션 취약성 항목) 라이브러리를 생성하여 AVI를 보고하는 동안 재사용할 수 있습니다. 또한 침투 테스트 결과의 상태를 추적할 수도 있습니다.

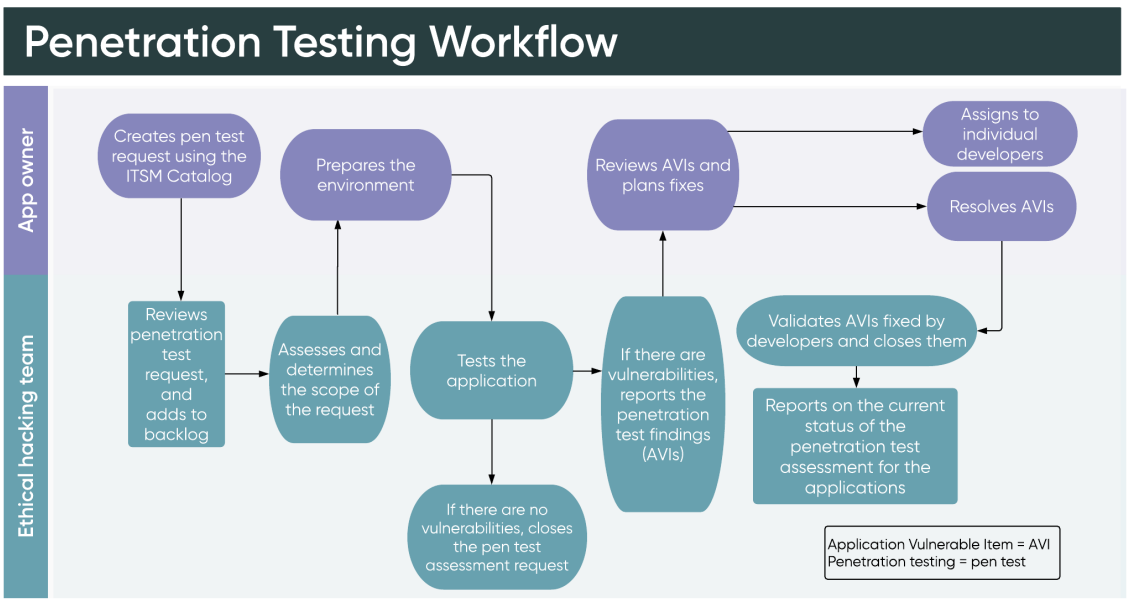
침투 테스트 결과 수정 및 검증

침투 테스트 결과가 애플리케이션 팀에 의해 수정되고 해결되면 수정 사항이 수동으로 검증되고 윤리적 해킹 팀에 의해 종결됩니다.

애플리케이션 취약성 관리 보고서

PA 대시보드에서 애플리케이션 취약성 관리 제공되는 보고서를 사용하여 침투 테스트 결과를 추적합니다.

침투 테스트 수명주기



기존 요청에서 침투 테스트 평가 요청 생성**(v19.0)**

v19.0부터는 기존 요청 목록에서 직접 침투 테스트 평가 요청을 생성합니다. 이 목록에서 종결 상태의 기존 요청을 복사하여 요청을 생성할 수도 있습니다.

시작하기 전에
필요한 역할: App-Sec 관리자

이 태스크 정보
의 v19.0 취약성 대응부터 를 사용하는 Veracode Vulnerability Integration경우 의 침투 평가 테스트는 Veracode Vulnerability Integration 의 수동 결과 Veracode입니다. 에서 구성하는 애플리케이션 취약성 대응침투 테스트 평가 요청에는 연결되지 않습니다. 의 Veracode침투 테스트 평가에 대한 자세한 내용은 를 Veracode Vulnerability Integration참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 침투 테스트 평가 요청 〉 모두.
2. 옵션: 또는 종결된 요청을 복제하여 요청을 생성할 수 있습니다.
   원래 요청의 모든 값이 새 양식에 보존됩니다. 활성 AVI(애플리케이션 취약한 항목)가 새 요청에 자동으로 복사됩니다. 종결 상태의 기록에서 요청 복사 및 생성을 선택합니다.
3. 새로 만들기를 선택하고 필드를 입력합니다.

침투 테스트 평가 요청 양식

필드	설명
번호	침투 테스트 평가 요청에 대해 생성된 고유 식별자입니다.
상태	요청 상태에 따라 값을 선택합니다.
요청한 사람	애플리케이션 평가를 요청하는 사람입니다.
할당 그룹	침투 테스트 결과에 대한 작업을 위해 선택된 그룹입니다. App-Sec 관리자가 수동으로 추가하거나 편집할 수 있습니다. 그룹을 구성하려면 다음 문서를 참조하십시오 침투 테스트 구성.
애플리케이션	검색 옵션을 사용하여 애플리케이션을 선택합니다.
담당자	침투 테스트 결과에 대해 작업하는 선택된 할당 그룹의 개인입니다. App-Sec 관리자가 수동으로 추가하거나 편집할 수 있습니다.
애플리케이션 유형	다음 옵션 중에서 선택합니다. ○ 웹 서비스(v16.1 이전에는 API라고 함) ○ 웹 애플리케이션 ○ Thick 클라이언트 ○ 모바일(모바일을 선택하면 모바일 탭이 추가 필드와 함께 양식 하단에 표시됨)
스프린트	선택한 평가 유형 필드에 따라 평가 요청을 수용하는 데 사용할 수 있는 대역폭이 있는 스프린트를 표시합니다. 스프린트 용량 및 테스트 범위 수정에 대한 자세한 내용은 을 참조하십시오 침투 테스트를 위한 스프린트 구성침투 테스트에 대한 평가 유형 구성 .
v19.0: 애플리케이션 크기	테스트할 애플리케이션의 크기를 선택합니다. ○ 작게 ○ 보통 ○ 크게 ○ 표준(크기를 잘 모를 경우 이 옵션 선택)

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	스프린트 용량을 수정하고 애플리케이션 크기 및 스프린트 용량으로 범위를 테스트하는 방법에 대한 자세한 침투 테스트 구성 내용을 참조하십시오.
작성됨	요청이 생성된 날짜 및 시간입니다.
평가 유형	다음에서 평가 유형을 선택합니다. ○ 전체 침투 테스트 ○ 집중 테스트 ○ 다시 테스트 테스트 조합 및 테스트 범위에 대한 자세한 내용은 다음 문서를 참조하십시오 침투 테스트에 대한 평가 유형 구성.
업데이트됨	요청이 마지막으로 업데이트된 날짜 및 시간입니다.
데모 날짜	이 애플리케이션을 시연할 수 있는 날짜입니다.
계획된 제품 배포	이 애플리케이션을 프로덕션 환경에 배포하기로 계획된 날짜입니다.
배포의 애플리케이션 버전/계획된 릴리스	프로덕션 배포를 위해 계획된 애플리케이션의 버전입니다.
v19.0: 외부 공급업체 또는 합작 투자 업체가 소유한 애플리케이션 탭 이 필드에 대해 예를 선택하면 벤더/합작 투자 업체 정보 탭이 표시됩니다. 추가 필드를 채웁니다.	
펜 테스트를 수행할 수 있는 조항이 있습니까?	'조항'이라는 용어는 추가하려는 둘 이상의 당사자 간에 존재하는 모든 계약을 포함하는 테스트 표준을 나타낼 수 있습니다. 예를 선택하는 경우 절을 추가합니다.
펜 테스트를 수행할 수 있는 권한을 인용하는 조항	
벤더의 전체 법적 이름 및 주소	
침입 탐지 시스템	
벤더의 기술 연락처	
로그된 정보가 악성 활동에서 검토되었습니까?	
애플리케이션이 다른 외부 공급업체 벤더에 의해 호스팅됩니까?	
펜 테스트에 서명할 벤더의 연락처	
애플리케이션 상세 정보 탭	
애플리케이션 목적	애플리케이션의 기능에 대한 설명입니다.
기술 스택 상세 정보	프론트엔드에서 백엔드, 데이터베이스 및 기타 핵심 기술에 이르는 완전한 기술 스택.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
외부 공급업체 애플리케이션입니까?	이 애플리케이션이 외부 공급업체 벤더의 소유인지 확인합니다.
애플리케이션에서 액세스할 수 있는 민감한 데이터의 목록 유형	애플리케이션에서 액세스할 수 있는 민감한 데이터의 유형입니다. PII 데이터, PHI 데이터, 신용 카드 번호 등의 재무 데이터를 예로 들 수 있습니다.
인증 유형	이 애플리케이션이 LDAP 인증, 자체 기본 인증 또는 기타 인증 양식을 사용하는지 여부를 지정합니다.
애플리케이션이 모든 준수 프로그램의 범위에 있습니까?	이 애플리케이션이 PCI와 같은 준수 프로그램에 영향을 주는지 여부를 지정합니다.
애플리케이션 팀 연락처	질문이 있는 경우 윤리적 해킹 팀에서 연락할 애플리케이션 팀 구성원입니다.
규정 준수 프로그램 목록	
관련 외부 공급업체 인터페이스 또는 애플리케이션	
IP 주소	
프로덕션 중인 사용자의 대략적인 수?	
자동화된 스크립트가 있습니까?	
이 앱의 프로덕션 버전이 외부에 연결되어 있습니까?	
v 19.0: 비즈니스 영향	
재정적 손상	목록에서 하나를 선택합니다.
미준수	목록에서 하나를 선택합니다.
평판 손상	목록에서 하나를 선택합니다.
개인정보 보호 위반	목록에서 하나를 선택합니다.
테스트 상세 정보 탭	
테스트할 URL	침투 테스트에 포함되어야 하는 URL입니다.
제외할 URL	침투 테스트에서 제외되어야 하는 URL입니다.
이 애플리케이션이 이전에 테스트되었습니까?	이 애플리케이션이 이미 침투 테스트를 거쳤는지 여부를 지정합니다.
재시도 이유	애플리케이션이 이전에 테스트된 경우 침투 테스트 재평가를 요청하는 이유입니다.
애플리케이션은 언제 테스트되었습니까?	애플리케이션이 침투 테스트를 거친 시간 범위입니다.
테스트 계정 상세 정보	윤리적 해킹 팀에서 침투 테스트에 사용할 수 있는 테스트 계정의 상세 정보입니다.
애플리케이션 역할	해당 사용자에 대해 애플리케이션에서 지원하는 역할입니다.
가장 많이 사용된 역할	애플리케이션에서 가장 일반적으로 사용되는 역할입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
추가 의견 탭	
작업 메모	

4. 저장을 선택하여 편집 내용을 저장하거나 제출을 선택하여 요청을 시작합니다.

침투 테스트 평가 요청 생성(v19.0 이전)

웹 애플리케이션 또는 API에 대한 침투 테스트 평가 요청을 시작합니다. 이러한 요청은 윤리적 해킹 팀에 제출되며, 윤리적 해킹 팀은 이러한 애플리케이션을 테스트하고 침투 테스트 결과를 수동으로 보고합니다.

시작하기 전에
필요한 역할: App-Sec 관리자

이 태스크 정보
애플리케이션 소유자는 침투 테스트 평가 요청을 제기하여 애플리케이션 또는 API를 수동으로 스캔합니다. 윤리적 해킹 팀은 애플리케이션을 테스트하고 침투 테스트 결과를 수동으로 생성합니다. 이러한 결과는 수동으로 생성된 애플리케이션 취약한 항목(AVI)입니다.

침투 테스트 결과에 대한 기본 할당 그룹은 연결된 침투 테스트 평가 요청의 "애플리케이션 팀" 필드에 구성된 그룹입니다. 침투 테스트 결과의 할당 유형은 수동입니다. 할당 규칙은 이러한 침투 테스트 결과의 할당을 재정의할 수 없습니다.

v19.0부터 침투 테스트 평가 요청[sn_vul_pen_test_assessment_request_list] 테이블에서 직접 침투 테스트 평가 요청을 생성할 수 있습니다. 자세한 내용은 기존 요청에서 침투 테스트 평가 요청 생성(v19.0) 문서를 참조하십시오.

프로시저

1. v19.0 이전 버전: 모두 〉 **Self-Service** 〉 서비스 카탈로그 〉 서비스 〉 침투 테스트 평가 요청.
2. 옵션: 또는 종결된 요청을 복제하여 요청을 생성할 수 있습니다.
   원래 요청의 모든 값이 보존됩니다. 활성 AVI(애플리케이션 취약한 항목)가 새 요청에 자동으로 복사됩니다.
3. 양식에서 필드를 채웁니다.

침투 테스트 평가 요청 양식

필드	설명
번호	침투 테스트 평가 요청에 대해 생성된 고유 식별자입니다.
요청한 사람	애플리케이션 평가를 요청하는 사람입니다.
상위 평가 요청	하위 요청을 생성하는 데 사용되는 원본 침투 테스트 평가 요청입니다. 종결된 평가 요청을 사용하여 생성됩니다. 하위 평가 요청 양식에만 표시됩니다.
애플리케이션	검색 옵션을 사용하여 애플리케이션을 선택합니다.
애플리케이션 유형	다음 옵션 중에서 선택합니다. ○ 웹 서비스(v16.1 이전에는 API로 알려짐) ○ 웹 애플리케이션

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	○ Thick 클라이언트 ○ 모바일(모바일을 선택하면 모바일 탭이 추가 필드와 함께 양식 하단에 표시됨)
v19.0: 애플리케이션 크기	테스트할 애플리케이션의 크기를 선택합니다. ○ 작게 ○ 보통 ○ 크게 ○ 표준(크기를 잘 모를 경우 이 옵션 선택)
평가 유형	다음에서 평가 유형을 선택합니다. ○ 전체 침투 테스트 ○ 집중 테스트 ○ 다시 테스트 자세한 내용은 침투 테스트에 대한 평가 유형 구성 문서를 참조하십시오.
애플리케이션 목적	애플리케이션의 기능에 대한 설명입니다.
기술 스택 상세 정보	프론트엔드에서 백엔드, 데이터베이스 및 기타 핵심 기술에 이르는 완전한 기술 스택.
외부 공급업체 애플리케이션입니까?	이 애플리케이션이 외부 공급업체 벤더의 소유인지 확인합니다.
애플리케이션에서 액세스할 수 있는 민감한 데이터의 목록 유형	애플리케이션에서 액세스할 수 있는 민감한 데이터의 유형입니다. PII 데이터, PHI 데이터, 신용 카드 번호 등의 재무 데이터를 예로 들 수 있습니다.
인증 유형	이 애플리케이션이 LDAP 인증, 자체 기본 인증 또는 기타 인증 양식을 사용하는지 여부를 지정합니다.
애플리케이션이 모든 준수 프로그램의 범위에 있습니까?	이 애플리케이션이 PCI와 같은 준수 프로그램에 영향을 주는지 여부를 지정합니다.
애플리케이션 팀 연락처	질문이 있는 경우 윤리적 해킹 팀에서 연락할 애플리케이션 팀 구성원입니다.
데모 날짜	이 애플리케이션을 시연할 수 있는 날짜입니다.
계획된 제품 배포	이 애플리케이션을 프로덕션 환경에 배포하기로 계획된 날짜입니다.
배포의 애플리케이션 버전/계획된 릴리스	프로덕션 배포를 위해 계획된 애플리케이션의 버전입니다.
v19.0: 외부 공급업체 또는 합작 투자 업체가 소유한 애플리케이션	이 필드에 대해 예를 선택하면 추가 필드와 함께 벤더/합작 투자 업체 정보 탭이 표시됩니다. '조항'이라는 용어는 둘 이상의 당사자 간에 존재하는 모든 계약을 포함하는 테스트 표준을 나타낼 수 있습니다.
상태	요청 상태에 따라 값을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
할당 그룹	침투 테스트 결과에 대한 작업을 위해 선택된 그룹입니다. App-Sec 관리자가 수동으로 추가하거나 편집할 수 있습니다.
담당자	침투 테스트 결과에 대해 작업하는 선택된 할당 그룹의 개인입니다. App-Sec 관리자가 수동으로 추가하거나 편집할 수 있습니다.
스프린트	선택한 평가 유형 필드에 따라 평가 요청을 수용하는 데 사용할 수 있는 대역폭이 있는 스프린트를 표시합니다.
작성됨	요청이 생성된 날짜 및 시간입니다.
테스트 시작 날짜	테스트가 시작되는 날짜 및 시간입니다.
업데이트됨	요청이 마지막으로 업데이트된 날짜 및 시간입니다.
테스트 상세 정보	
테스트할 URL	침투 테스트에 포함되어야 하는 URL입니다.
제외할 URL	침투 테스트에서 제외되어야 하는 URL입니다.
이 애플리케이션이 이전에 테스트되었습니까?	이 애플리케이션이 이미 침투 테스트를 거쳤는지 여부를 지정합니다.
재시도 이유	애플리케이션이 이전에 테스트된 경우 침투 테스트 재평가를 요청하는 이유입니다.
애플리케이션은 언제 테스트되었습니까?	애플리케이션이 침투 테스트를 거친 기간입니다.
테스트 계정 상세 정보	윤리적 해킹 팀에서 침투 테스트에 사용할 수 있는 테스트 계정의 상세 정보입니다.
애플리케이션 역할	해당 사용자에 대해 애플리케이션에서 지원하는 역할입니다.
가장 많이 사용된 역할	애플리케이션에서 가장 일반적으로 사용되는 역할입니다.

4. 제출을 선택합니다.
   윤리적 해킹 팀에 관련 애플리케이션에 대한 요청이 생성되었다는 이메일 알림이 전송됩니다.

종결 상태의 침투 테스트 요청 복제

종결 상태의 요청을 복제하여 침투 테스트 평가 요청을 생성합니다. 활성 AVI(애플리케이션 취약한 항목)가 새 요청에 복사됩니다.

시작하기 전에
필요한 역할: 애플리케이션 팀

프로시저

1. 다음으로 이동 모두 〉 애플리케이션 취약성 대응 〉 침투 테스트 평가 요청 〉 모두.
2. 종결 상태의 요청을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 요청 복사 및 생성을 선택합니다.
   새 요청이 생성되고 활성 AVI가 업데이트된 데이터와 함께 이 요청에 복사됩니다. 상위 요청에서 AVI의 원래 상태를 보려면 침투 테스트 결과 스냅샷 탭으로 이동합니다.

평가 요청에 기반하여 침투 테스트 결과 생성(v19.0 이전)

침투 테스트 평가 요청을 기반으로 침투 테스트 결과를 생성합니다. 이러한 발견 사항은 수동으로 생성된 애플리케이션 취약성 항목(AVI)입니다.

시작하기 전에

필요한 역할: 윤리적 해커

프로시저

1. 다음으로 이동 모두 〉 **Self-Service** 〉 서비스 카탈로그 〉 서비스 〉 침투 테스트 평가 요청.
2. 침투 테스트 평가 요청에 대한 AVI를 생성하려면 관련 요청을 선택합니다.
3. 애플리케이션 취약한 항목 섹션에서 새로 만들기를 선택합니다.
4. 양식에서 필드를 채웁니다.

애플리케이션 취약한 항목 양식(침투 테스트 뷰)

필드	설명
번호	이 기록에 대해 자동으로 생성된 AVI 식별자입니다.
평가 요청	이 AVI가 연결된 침투 테스트 평가 요청입니다.
취약성	검색 옵션을 사용하여 취약성 항목 테이블에서 선택한 취약성입니다.
위험 등급	취약한 항목을 중요, 높음, 중간, 낮음 및 없음으로 구분하는 정량화된 위험 점수 입니다. 위험 등급에 대한 자세한 내용은 다음 문서를 참조하십시오 자동으로 위험 애플리케이션 취약성 대응 계산. V16.1부터 이 값은 취약성의 심각도와 동일합니다.
규정 준수 프로그램에 영향을 미칩니까?	규정 준수 프로그램에 영향이 있는지 여부를 확인합니다. 선택 사항은 예 및 아니요입니다.
영향을 받는 규정 준수 프로그램 목록	이 필드는 "모든 준수 프로그램에 영향을 미침" 필드의 값이 로 설정된 *Yes*경우에 표시됩니다. 영향을 받는 규정 준수 프로그램을 나열합니다.
계획된 릴리스/수정 버전	침투 테스트 결과를 해결해야 하는 시점까지 해제합니다.
상태	AVI가 생성되면 기본값은 열림 입니다. 상태가 매핑되는 방법에 대한 자세한 내용은 을 참조하십시오 애플리케이션 취약한 항목(AVI) 상태 .
할당 그룹	이 AVI에서 작업하기 위해 선택한 그룹입니다. App-Sec 관리자가 수동으로 추가하거나 편집할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
담당자	이 AVI에서 작업하는 선택한 할당 그룹의 개인입니다. App-Sec 관리자가 수동으로 추가하거나 편집할 수 있습니다.
정정 대상	처음 식별된 이후 AVI를 정정해야 하는 날짜입니다. 이 필드는 해당하는 경우에만 나타납니다. 정정 대상에 대한 자세한 내용은 다음 문서를 에서 정정 대상 추적 자동화 애플리케이션 취약성 대응참조하십시오.
작성됨	애플리케이션 취약한 항목(AVI)이 생성된 타임스탬프입니다.
업데이트됨	애플리케이션 취약한 항목(AVI)이 업데이트된 타임스탬프입니다.
개설자	이 침투 테스트 결과를 생성한 사용자입니다.
보안 팀 연락처	윤리적 해킹 팀의 연락 창구입니다.
간단한 설명	침투 테스트 결과에 대한 간략한 설명입니다.
상세 정보	
기술 상세 정보	침투 테스트 결과의 기술적 세부 사항.
영향도	침투 테스트 결과의 영향 평가입니다.
재현 단계	침투 테스트 결과를 재현하고 검토하는 단계를 문서화합니다.
권장 사항	이 필드에 권장 작업을 기록합니다.
메모	
작업 메모	상태 전환 및 기타 필드 업데이트에 대한 정보를 전달하기 위한 메모를 추가합니다.
V16.1: 영향을 받는 URL	영향을 받는 URL과 관련된 추가 정보입니다.
V16.1: 영향을 받는 매개변수	영향을 받는 매개변수와 관련된 추가 정보입니다.
V16.1: 영향을 받는 기능	영향을 받는 기능과 관련된 추가 정보입니다.

5. 양식을 저장하려면 제출을 선택합니다.

애플리케이션 취약성 항목 생성

침투 테스트 결과에 대해 지정된 취약성에 대한 애플리케이션 취약성 항목을 생성합니다. 애플리케이션 취약성은 사용자 지정 소프트웨어 애플리케이션의 취약성입니다.

시작하기 전에
필요한 역할: 윤리적 해커

이 태스크 정보
애플리케이션 취약성 대응 취약성을 애플리케이션에 연결하여 침투 테스트 결과를 생성합니다. 이러한 결과는 수동으로 생성된 애플리케이션 취약한 항목(AVI)입니다. 침투 테스트 중 기존 항목을 다시 사용하거나 각 취약성에 대해 수동으로 항목을 만들 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 애플리케이션 취약성 대응 〉 라이브러리 〉 외부 공급업체.
2. 애플리케이션 취약성 항목 페이지에서 새로 만들기를 선택합니다.
3. 양식에서 필드를 채웁니다.

애플리케이션 취약성 입력 양식(침투 테스트 뷰)

필드	설명
ID	이 취약성 항목의 식별자입니다.
심각도	이 취약성의 정규화된 심각도 수준입니다. 심각도 맵은 NVD 및 ServiceNow 외부 공급업체 통합과 함께 제공됩니다. 심각도 맵 생성 및 조정에 대한 자세한 내용은 다음 문서를 참조하십시오 애플리케이션 취약한 항목의 심각도를 자동으로 매핑.
기본 CVE	이 취약성이 가장 적합한 일반 약점 열거형 요소에 대한 참조입니다.
범주 이름	외부 공급업체 통합에서 제공하는 분류입니다. 임무 수행을 돕는다.
취약성 상세 정보	
공격 벡터	이 취약성에 대한 가장 취약한 공격 벡터입니다.
공격 복잡성	취약성을 악용하기 위해 존재해야 하는 공격자의 통제를 벗어난 조건을 설명하는 메트릭입니다.
범위	소프트웨어 취약성이 자원을 평균 이상으로 영향을 미칠 수 있는지 측정하는 메트릭입니다.
무결성	악용된 취약성의 무결성에 미치는 영향을 측정하는 메트릭입니다.
CVSS 벡터	소프트웨어 취약성의 특성과 심각도를 파악하는 개방형 프레임워크입니다.
필요한 권한	취약성을 성공적으로 악용하기 전에 공격자에게 있어야 하는 권한 수준입니다.
사용자 상호작용	취약성을 성공적으로 악용하기 위한 인간 상호작용에 대한 요구 사항입니다.
기밀성	악용된 취약성이 정보 자원의 기밀성에 미치는 영향입니다. 이러한 자원은 소프트웨어 구성요소에 의해 관리됩니다.
가용성	악용된 취약성이 영향을 받는 구성요소의 가용성에 미치는 영향입니다.
CVSS 기준 점수	애플리케이션 취약성 항목의 심각도를 숫자(0-10)로 나타냅니다.
위협	이 취약성으로 인한 위협에 대한 설명입니다.
완화 설명	취약성을 완화하는 단계에 대한 설명입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 양식을 저장하려면 제출을 선택합니다.

> **주:**
> AVE는 sn_vul_app_vul_entry(애플리케이션 취약성 항목) 테이블에 생성됩니다. 애플리케이션 취약성 항목 테이블은 취약성 항목()*sn_vul_entry* 테이블의 하위 항목입니다. 따라서 생성된 AVE는 취약성 항목 테이블에도 추가됩니다.

침투 테스트 작업 공간

Application Vulnerability Response의 침투 테스트 작업 공간은 고객이 침투 테스트 평가 요청을 요청하고 워크플로우를 사용하여 이를 추적하는 데 도움이 됩니다. 이를 통해 애플리케이션 소유자는 애플리케이션의 보안 태세를 평가할 수 있습니다. 윤리적 해킹 팀이 애플리케이션을 수동으로 테스트하는 것입니다.

필요한 역할

침투 테스트에는 다음과 같은 역할이 필요합니다.

sn_vul.app_pen_tester: 애플리케이션 침투 테스트의 일부로 펜 테스트 결과를 생성하는 펜 테스터를 나타냅니다.

sn_vul.app_pen_test_requester: 작업에 대한 기록 선택: sn_vul.app_pen_test_requester.

침투 테스트의 수명주기

애플리케이션 소유자는 윤리적 해킹 팀에 애플리케이션의 침투 테스트 평가를 요청할 수 있습니다. 윤리적 해킹 팀은 이 요청에 따라 조치를 취하고 침투 테스트 결과를 생성합니다. 이러한 결과는 수동으로 생성된 애플리케이션 취약한 항목(AVI)입니다.

침투 테스트 워크플로우는 테스트 요청 제기부터 윤리적 해킹 팀의 결과 해결에 이르기까지 침투 테스트 수명주기를 다룹니다.

침투 테스트 평가 요청을 생성합니다.

웹 애플리케이션, 모바일 애플리케이션 또는 API에 대한 침투 테스트 평가 요청을 시작합니다. 이러한 요청은 윤리적 해킹 팀에 제출되며, 윤리적 해킹 팀은 이러한 애플리케이션을 테스트하고 침투 테스트 결과를 수동으로 보고합니다.

시작하기 전에
필요한 역할: App-Sec 관리자

프로시저

1. 다음으로 이동 침투 테스트 작업 공간.
2. 침투 테스트 평가 요청 양식의 필드에 내용을 입력합니다.
3. 제출을 선택합니다.
   윤리적 해킹 팀에 관련 애플리케이션에 대한 요청이 생성되었다는 이메일 알림이 전송됩니다.
4. 양식이 제출되면 윤리적 해킹 팀이 범위 지정을 시작할 수 있습니다.
5. 범위 지정 후 애플리케이션 소유자는 테스트 환경을 준비하고 윤리적 해킹 팀은 테스트를 시작할 수 있습니다.
6. 요청에서 세부 정보를 확인해야 하는 경우 보류 중 버튼을 선택하여 테스트 단계를 보류로 표시할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

7. 테스트가 완료되면 침투 테스트 테스트 결과 탭에서 AVIT를 볼 수 있습니다.

> **주:**
> 기존 요청에서 요청을 복제할 수 있습니다. 복제되면 상위 요청에 연결된 AVIT가 중복된 요청으로 이동(복사되지 않음)됩니다.

평가 질문서를 기반으로 침투 테스트 결과 생성

침투 테스트 워크플로우에 MASVS 질문서의 인식된 표준에 맞게 테스트를 조정하는 침투 테스트 결과를 생성합니다. 이러한 발견 사항은 수동으로 생성된 애플리케이션 취약성 항목(AVI)입니다.

시작하기 전에
필요한 역할: App-sec 관리자

프로시저

1. 다음으로 이동 침투 테스트 결과 탭.
2. 애플리케이션에 따라 게시된 질문서를 선택합니다.
3. 테스트를 검토하고 테스트 단계를 완료됨으로 표시합니다.
4. 위 단계가 완료되면 요청을 종결합니다.

> **주:**
> 이전 단계는 윤리적 해킹 팀의 구성원이 수행할 수 있습니다.

평가 질문서 게시

모바일 애플리케이션을 테스트하기 위해 테스터가 제품의 버그를 식별하는 데 도움이 되도록 OAS 커뮤니티에서 개발한 특정 표준이 있습니다. 평가 작업 공간으로 이동하여 원하는 질문서를 생성합니다. 평가 요청 양식에서 볼 수 있도록 게시합니다.

시작하기 전에
필요한 역할: sn_vul.app_pen_test_requester

침투 테스트에 필요한 역할 요청자 및 테스터:

sn_vul.app_manage_pen_test_request:

포함: sn_smart_asmt.assessment_reader sn_smart_asmt:assessment_admin sn_smart_asmt.actor.

sn_vul.app_pen_tester

포함: sn_smart_asmt.assessment_reader sn_smart_asmt:actor.

> **주:**
> 스마트 평가 엔진 기능의 일부로 위의 역할을 추가했습니다. 이러한 역할은 침투 테스트 요청자와 테스터가 질문서를 보고 제출하는 데 필수적입니다.

프로시저

1. 다음으로 이동 평가 작업 공간.
2. 각 질문서 내에는 가이드라인이 있습니다. 질문서를 검토하고, 필요한 경우 조직의 테스트 요구 사항에 맞게 변경한 후 테스트를 완료할 수 있습니다.
   질문서는 기본적으로 MASVS 표준을 따릅니다. 자세한 내용은 다음을 방문하십시오.
3. 질문서를 게시하고 침투 테스트 평가 요청 양식의 테스트 상세 정보 섹션 아래 목록에서 게시된 질문서를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
침투 테스트 요청 평가 요청 양식에서 볼 수 있도록 질문서를 게시합니다.

4. 그런 다음 테스트를 수행하는 가상 사용자는 침투 테스트 요청 양식의 평가 탭에서 테스트를 통과 또는 실패 또는 해당 사항 없음으로 표시할 수 있습니다.

평가 질문서 사용

평가 질문서를 작성한 후 이러한 질문서를 테스트 목적으로 사용할 수 있습니다.

시작하기 전에
필요한 역할: sn_vul.app_pen_tester

프로시저

1. 다음으로 이동 침투 테스트 요청 형.
2. 양식에 언급된 지침을 따르십시오.
3. 침투 테스트 요청을 선택합니다.
4. 평가 탭으로 이동합니다.
5. 탭을 열고 질문서에 응답한 후 제출합니다.

주:
침투 테스트 요청에 할당된 가상 사용자가 요청을 제출할 수 있습니다.

침투 테스트 대시보드

개인 침투 테스트 대시보드에서 침투 테스트 요청 및 수동 결과에 대한 개요를 확인합니다. 침투 테스트 작업 공간에서 팀의 진행률을 볼 수 있습니다. 대시보드는 침투 테스트 결과에 대한 개요를 제공하고, 주의가 필요한 테스트를 보고 우선순위를 지정하고, 테스트 결과를 추적하고, 할당을 확인합니다.

침투 테스트 관리자/윤리적 해킹 팀 리더는 침투 테스트 요청 모니터링과 같은 주요 메트릭을 식별 및 분석하고 침투 테스트 작업 공간에서 팀의 전반적인 진행률을 볼 수 있습니다. 펜 테스트 관리자/윤리적 해킹 팀 리더는 다음과 같은 인사이트도 볼 수 있습니다.

- 전략적 의사 결정을 알리기 위해 상태 및 평가 유형별로 분류된 수동 결과의 개요입니다.
- 더 나은 용량 계획을 위해 개인 전체에 할당된 침투 테스트 배포
- 진행 상황에 따라 기한이 지난 결과의 우선순위를 지정하여 해결 효율성을 높입니다.
- 비판적 분포를 기반으로 한 침투 테스트 결과의 환경을 이해합니다.

침투 대시보드 구성요소

팀의 진행률과 데이터를 시각적으로 분석하고 개인 대시보드의 구성요소를 활용하여 비즈니스 성과를 도출합니다.

중요 항목 표시기

할당되지 않은 긴급 릴리스, 개요 날짜가 지난 테스트, 할당되지 않은 테스트 및 보류 중인 중요 확인을 봅니다.

- 할당되지 않은 긴급 릴리스: "긴급 릴리스" 평가 유형에 대한 할당되지 않은 침투 테스트 요청의 총 수를 나타냅니다.
- 테스트 지연: 기한이 지난 테스트의 총 수를 나타냅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 할당되지 않은 테스트: 팀에 할당되지 않은 테스트의 총 수를 나타냅니다.
- 중요 확인 보류 중: "확인 보류 중" 상태의 모든 요청에 대한 총 AVIT 수를 나타냅니다.

주:
각 타일을 선택하여 항목 목록을 보고 필요한 작업을 수행합니다.

침투 테스트 요청

상태별 테스트 요청, 지연된 테스트 및 릴리스 승인별 테스트를 봅니다.

- 상태별 테스트 요청: 침투 테스트 주기의 이러한 다양한 상태의 테스트 요청 수를 나타냅니다. 색상이 지정된 각 타일을 클릭하여 다양한 상태의 테스트 요청 목록을 보고 이동할 수 있습니다. 탭의 오른쪽 상단 섹션에 있는 필터 드롭다운에서 월을 선택하여 다음 6개월 동안의 테스트 상태를 볼 수도 있습니다. 다음은 여러 테스트 요청 상태입니다.
  - Open: 열린 테스트 요청 수입니다.
  - 범위 지정 진행 중:
  - 범위 지정 완료:
  - 환경 준비:
  - 테스트할 수 있는 환경:
  - 테스트 진행 중:
  - 가득 차있는 침투 시험:
  - 버그 바운티 프로그램: 윤리적 해커에게 보안 취약점을 찾아 보고할 수 있는 보상을 제공합니다.
  - 집중 테스트:
  - 경영진 관심사: 조직 내 중요 프로젝트에 대한 고위 경영진의 참여 및 지원에 대해 보고합니다.
  - 일회성 검토: 정기 개발 및 릴리스 주기가 아닌 특정 프로젝트를 평가하여 성과를 평가하고 개선 사항을 구현합니다.
  - 긴급 릴리스: 보안 취약성과 같은 중요한 문제를 해결하기 위해 신속한 소프트웨어 업데이트에 필요한 긴급 릴리스를 지원합니다.
- 테스트 지연:: 특정 기간 동안 보류 중인 테스트를 나타냅니다. 테스트 결과를 보려는 타임라인을 선택할 수 있으며 드롭다운 옵션은 어제 기한, 이번 주 기한, 지난주 기한, 지난달 기한 및 지난달 기한 입니다.
- 릴리스 승인별 테스트: 릴리스 준비가 완료된 테스트의 승인 상태를 나타냅니다. 또한 새 소프트웨어를 배포하기 전에 필요한 모든 검사가 완료되었는지 확인합니다. 탭의 오른쪽 상단 섹션에 있는 필터 드롭다운에서 월을 선택하여 다음 6개월 동안의 테스트 상태를 볼 수도 있습니다.

정보

확인 보류 중인 AVIT 수와 함께 보고된 AVIT(Open 침투 테스트 결과) 수를 나타냅니다. 색상이 지정된 각 타일을 선택하여 다양한 상태의 결과 목록을 보고 탐색할 수 있습니다. 이 섹션에서 볼 수 있는 데이터는 다음과 같습니다.

- 위험 등급별 열린 결과**(AVIT)**
- 발견 사항에 대한 확인 보류 중**(AVIT)**

팀 개요

다음 6개월 동안 팀 구성원에게 할당된 테스트를 나타냅니다. 다른 상태는 다음과 같습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 범위 지정 진행 중
- 오픈
- 범위 지정 완료됨
- 테스트할 준비가 된 환경
- 테스트 진행 중
- 환경 준비

애플리케이션 취약성 대응 용 플랫폼 분석 솔루션

플랫폼 분석 솔루션에는 다른 ServiceNow AI Platform 제품과 함께 사용하기 위해 사전 패키징된 플랫폼 분석 컨텐츠가 포함되어 있습니다. 이는 플랫폼 분석 솔루션 애플리케이션 취약성 관리 프로세스를 분석하는 데 중요한 메트릭을 제공합니다.

개요

Performance Analytics for Vulnerability Response 콘텐츠 팩은 별도의 ServiceNow# Store 구독으로 사용할 수 있습니다. 애플리케이션은 취약성 대응 애플리케이션과 함께 자동으로 설치되지 않습니다. Application Vulnerability Response 콘텐츠 팩은 Performance Analytics for Vulnerability Response 콘텐츠 팩의 일부입니다.

취약성 대응을 위한 퍼포먼스 분석 애플리케이션의 설정, 설치 및 구성에 대한 자세한 내용은 취약성 대응을 위한 퍼포먼스 분석(PA) 애플리케이션 설치 및 구성의 내용을 참조하십시오.

주요 용어

퍼포먼스 분석(PA)

: 관리 대시보드를 만들고, KPI 및 메트릭에 대해 보고하고, 핵심 비즈니스 질문에 답하여 품질을 높이고 비용을 절감하는 솔루션입니다.

애플리케이션 취약한 항목(AVI)

: CI(구성 항목)에 있는 외부 공급업체 취약성 스캐너에서 보고하는 애플리케이션 취약성입니다.

PA 표시기

: 활동 또는 조직 행동에 대해 정기적인 간격으로 수행되는 성과 측정을 정의합니다(예: 가장 중요한 애플리케이션 취약한 항목이 있는 상위 10개 애플리케이션).

PA 표시기 소스

: 하나의 테이블 또는 데이터베이스 뷰에서 기록을 필터링하는 데이터 세트입니다(예: AVI Active).

- 내 애플리케이션 취약성 대시보드는 초기 분석/탐지부터 억제 또는 정정에 이르기까지 애플리케이션 취약성의 볼륨, 성능 및 진행 상황을 추적합니다.
- 정정 목표 달성률을 확인하고 조직에 가장 큰 위험을 초래하는 애플리케이션 취약한 항목(AVI)을 효율적으로 파악합니다.

필요한 역할

이 솔루션과 관련된 역할과 작업은 다음과 같습니다.

- ServiceNow AI Platform 관리자(admin): 이 Analytics and Reporting 솔루션을 설치 및 활성화하고 필요한 변경 사항을 시스템 속성에 적용합니다.
- 퍼포먼스 분석관리자(pa_admin): 표시기, 세부 항목, 위젯 및 대시보드를 검토합니다. 데이터 수집을 설정 및 시작합니다. 적절한 이해 관계자와 대시보드를 공유합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음 대시보드는 정정 계획 및 상태 진행률을 확인하는 데 도움이 되는 AVI 활동에 대한 그래픽 보기를 제공합니다. 영향을 받는 중요한 애플리케이션 및 가시성이 높은 취약성과 연결된 KPI에 집중할 수 있습니다.

- 애플리케이션 취약성 관리(PA) 대시보드는 취약성 위험 및 확산, 영향을 받는 애플리케이션, 정정 추세 및 정정 진행 상황에 대한 KPI를 전달합니다. 추세의 기본값은 3개월이지만 7일, 1개월, 3개월, 6개월, YTD, 1년 또는 모두로 변경할 수 있습니다.
- 내 애플리케이션 취약성 대시보드는 초기 분석/탐지부터 억제 또는 정정에 이르기까지 애플리케이션 취약성의 볼륨, 성능 및 진행 상황을 추적합니다.

> **주:**
> 내 애플리케이션 취약성 대시보드는 개요 대시보드의 하위 집합이며 보안 챔피언 사용자 그룹의 구성원이 인스턴스에 로그인한 경우에만 사용할 수 있습니다. 내 애플리케이션 취약성 대시보드에 대한 자세한 내용은 내 애플리케이션 취약성 대시보드를 참조하십시오.

애플리케이션 취약성 관리 **(PA)** 대시보드

초기 분석 및 탐지부터 억제 또는 정정에 이르기까지 애플리케이션 취약성의 볼륨, 성능 및 진행 상황을 추적합니다.

사용 사례

사용자	대시보드 사용
취약성 관리자	취약성 관리는 애플리케이션 취약성 관리 대시보드를 사용하여 조직에 가장 큰 위험을 초래하는 애플리케이션 취약한 항목(AVI)을 확인할 수 있습니다. 이러한 대시보드는 AVI 활동에 대한 그래픽 보기를 제공하여 정정 계획 및 상태 진행률을 결정하는 데 도움이 됩니다. 영향을 받는 중요한 애플리케이션 및 가시성이 높은 취약성과 연관된 KPI에 집중합니다.

필요한 **ServiceNow AI Platform** 역할, 설정 및 대시보드 탭

애플리케이션 취약성 관리(PA) 대시보드는 취약성 대응을 위한 퍼포먼스 분석 컨텐츠 팩의 일부로 포함되어 있습니다. Performance Analytics for Vulnerability Response 컨텐츠 팩은 애플리케이션과 함께 취약성 대응 자동으로 설치되지 않습니다. 별도의 구독으로 사용할 수 ServiceNow# Store 있습니다.

취약성 대응을 위한 퍼포먼스 분석 애플리케이션의 설정, 설치 및 구성에 대한 자세한 내용은 취약성 대응을 위한 퍼포먼스 분석〔PA〕 애플리케이션 설치 및 구성의 내용을 참조하십시오.

대시보드를 보려면 보안 챔피온, App-Sec 관리자 또는 개발자 사용자 그룹에 할당된 사용자로서 애플리케이션 취약성 대응 〉 개요.

> **주:**
> 내 애플리케이션 취약성 대시보드는 개요 대시보드의 하위 집합이며 보안 챔피언 사용자 그룹의 구성원이 인스턴스에 로그인한 경우에만 사용할 수 있습니다. 내 애플리케이션 취약성 대시보드에 대한 자세한 내용은 을 참조하십시오 내 애플리케이션 취약성 대시보드.

의 애플리케이션 취약성 대응버전 19.0부터 이 대시보드는 New Experience UI에서도 볼 수 있습니다. 새 UI에서 대시보드를 보려면 다음으로 이동합니다. 작업 공간 〉 취약성 관리자 작업

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

공간 을 클릭하고 대시보드 아이콘을 클릭합니다. 역할에 따라 기본 대시보드가 표시됩니다. 다른 대시보드를 보려면 대시보드 이름 옆에 있는 드롭다운을 클릭합니다. 자세한 내용은 대시보드 페이지의 취약성 관리자 작업 공간 및 대시보드 페이지의 IT 정정 작업 공간 문서를 참조하십시오.

개요 대시보드는 취약성 위험 및 보급, 영향을 받는 애플리케이션, 정정 추세 및 정정 진행 상황에 대한 KPI를 전달합니다. 추세의 기본값은 3개월이지만 7일, 1개월, 3개월, 6개월, YTD, 1년 또는 모두로 변경할 수 있습니다.

대시보드의 애플리케이션 취약성 관리 데이터를 스캔 유형, 애플리케이션 또는 비즈니스 단위별로 분류합니다. 이러한 각 선택 항목에는 선택 항목을 구체화하기 위한 추가 필터인 요소 선택이 있습니다. v15.0부터 애플리케이션 취약성 대응 비즈니스 및 CI 애플리케이션이 애플리케이션 필터의 선택 항목에 추가되었습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

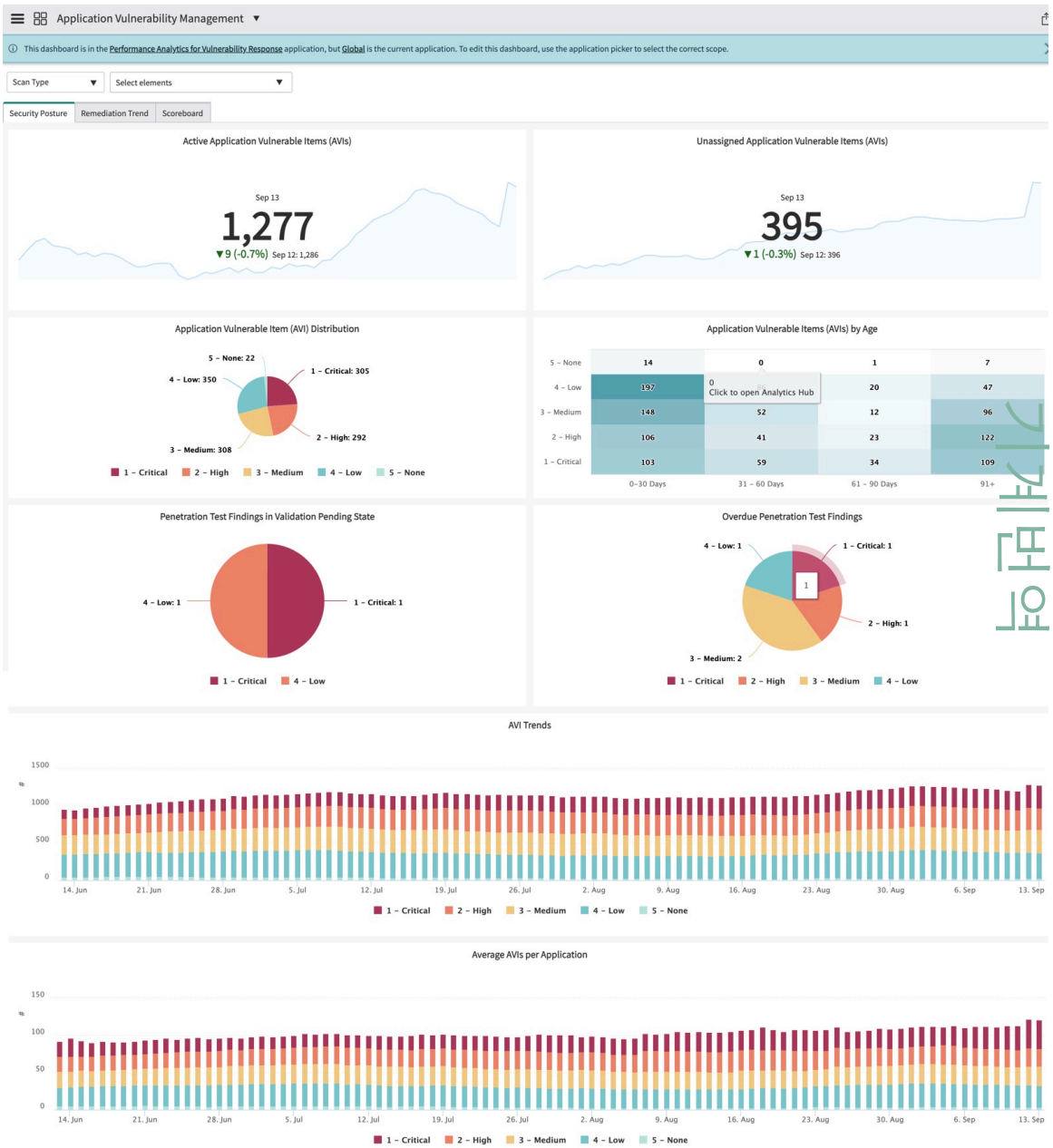
보안 태세 탭

보안 태세 탭은 보안 태세와 정정 작업의 진행 상황을 이해하는 데 도움이 됩니다.

v15.0부터 애플리케이션 취약성 대응 침투 테스트 결과 보고서를 볼 수 있습니다. 침투 테스트 결과는 침투 테스트 평가 요청에 따라 수동으로 생성된 애플리케이션 취약한 항목(AVI)입니다.

주:
이러한 위젯의 스캔 유형은 수동입니다.

AVM 대시보드의 보안 태세 탭



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

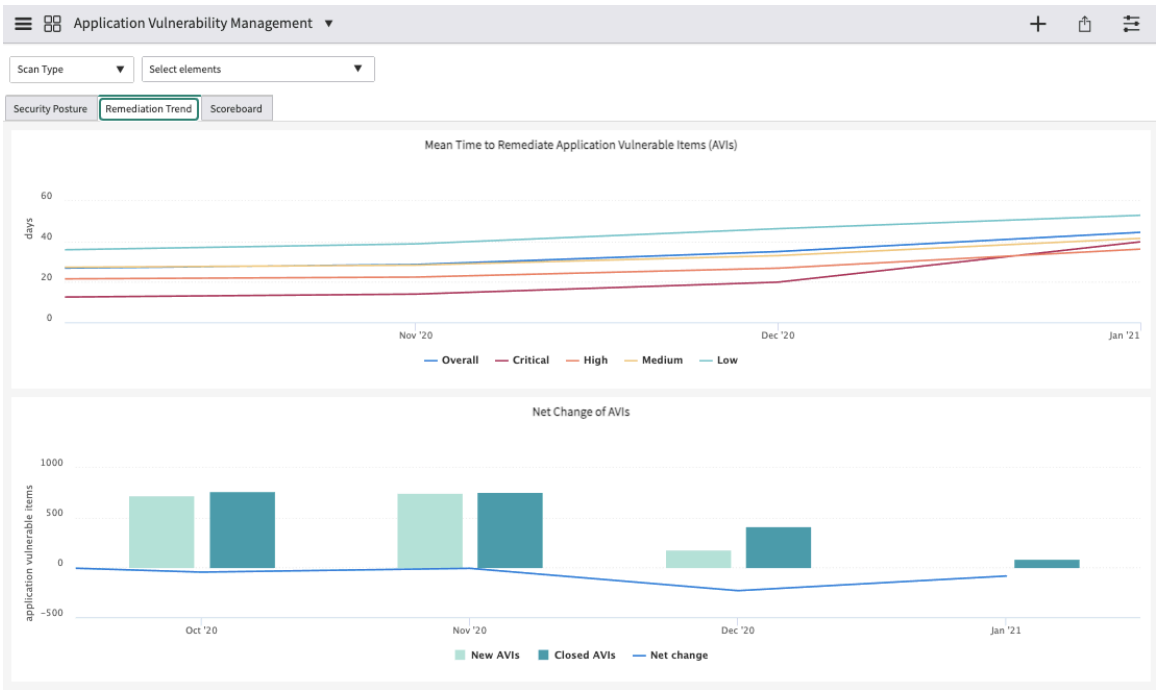
예외 탭

이 대시보드는 잠재적으로 과도한 지연으로 인해 조직이 위험을 감수하는 위치를 이해하고 정정 옵션을 재고하는 데 도움이 됩니다.

사유별로 연기된 애플리케이션 취약한 항목, AVI에 대한 연기 요청 만료, 할당 그룹별로 중요한 애플리케이션 취약한 항목에 대한 예외, 요청자별 AVI 예외 요청을 볼 수 있습니다.

정정 추세 탭

정정 추세 탭은 정정 작업의 진행 상황을 이해하는 데 도움이 됩니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

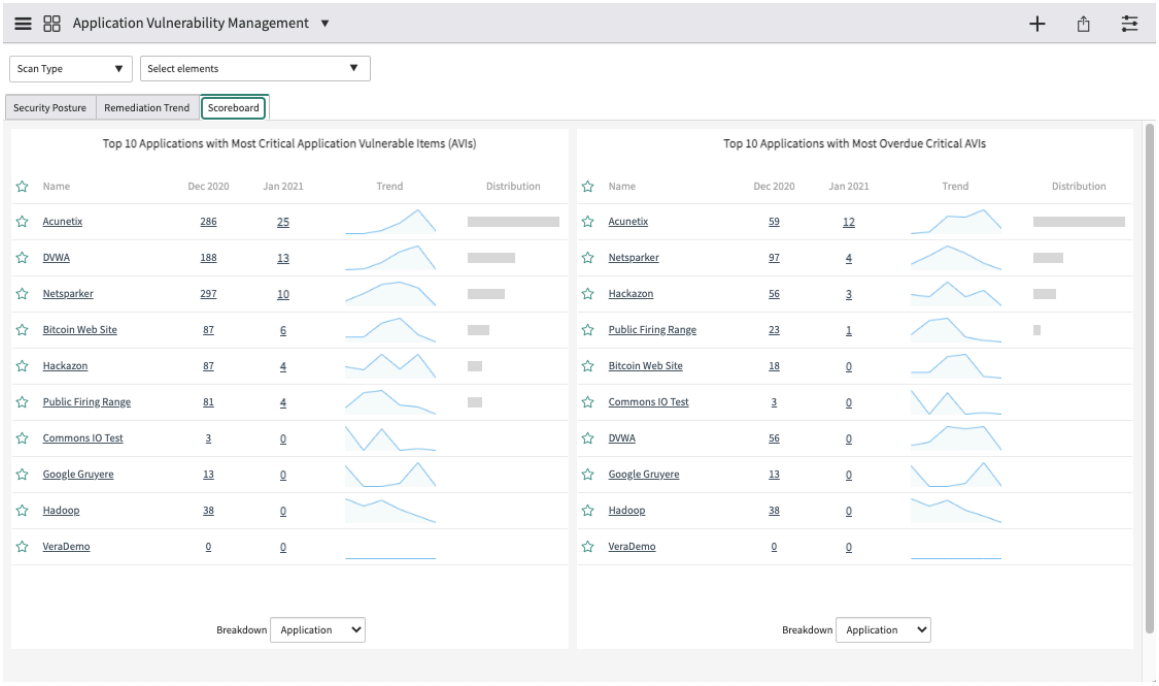
점수판 탭

점수판 탭은 정정 작업의 진행률과 완료 시 가장 많은 지원이 필요한 AVI를 이해하는 데 도움이 됩니다.

스캔 유형 요소:

- 동적: 동적 데이터 임포트의 메트릭만 사용
- 정적: 정적 데이터 임포트의 메트릭만 사용합니다.

둘 중 하나 또는 둘 다를 선택할 수 있습니다.



표시기

낮은 AVI 정정 평균 시간

[[### ###### ### ### ## ## > ## ## = 4 - ##]] / [[### ###### ### ## > ## ## = 4 - ##]]. 목표는 최소화하는 것입니다.

애플리케이션 릴리스

AVI와 응용 프로그램의 고유 수입니다. 활성입니다. sn_vul_app_vulnerable_item 테이블을 사용합니다. 목표는 최소화하는 것입니다.

애플리케이션 취약한 항목

앱 취약한 항목 AVI의 수입니다. 활성입니다. sn_vul_app_vulnerable_item 테이블을 사용합니다. 목표는 최소화하는 것입니다.

애플리케이션당 평균 AVI

[## ###### ### ##]]/[[###### ###]]. 목표는 최소화하는 것입니다.

할당되지 않은 VI

표시기 소스 AVI의 개수입니다. 활성입니다. sn_vul_app_vulnerable_item 테이블을 사용합니다. 목표는 최소화하는 것입니다.

AVI 정정 평균 시간

[[### ###### ### ### ## ##]]/[[### ###### ### ##]]. 목표는 최소화하는 것입니다.

높은 AVI 정정 평균 시간

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

[[### ###### ### ### ## ## > ## ## = 2 - ##]] / [[### ###### ### ## > ## ## = 2 - ##]]. 목표는 최소화하는 것입니다.

닫힌 애플리케이션 취약한 항목

표시기 소스 AVI의 개수입니다. 종결됨. 사용 중인 테이블: sn_vul_app_vulnerable_item. 목표는 최대화하는 것입니다.

핵심 AVI 정정 평균 시간

[[### ###### ### ### ## ## > ## ## = 1 - ##]] / [[### ###### ### ## > ## ## = 1- ##]]. 목표는 최소화하는 것입니다.

새 애플리케이션 취약한 항목

표시기 소스 AVI의 개수입니다. New. 사용 중인 테이블: sn_vul_app_vulnerable_item. 목표는 최소화하는 것입니다.

보통 AVI 정정 평균 시간

[[### ###### ### ### ## ## > ## ## = 3 - ##]] / [[### ###### ### ## > ## ## = 3 - ##]]. 목표는 최소화하는 것입니다.

VI의 순 변경

[[# ###### ### ##]] - [[## ###### ### ##]]. 목표는 최소화하는 것입니다.

닫힌 애플리케이션 취약한 항목의 합산 기간

표시기 소스 AVI의 개수입니다. 종결됨. 사용 중인 테이블: sn_vul_app_vulnerable_item. 목표는 최소화하는 것입니다.

핵심 지연 애플리케이션 취약한 항목

데이터 소스 AVI의 개수입니다. 활성입니다. sn_vul_app_vulnerable_item 테이블을 사용합니다. 목표는 최소화하는 것입니다.

핵심 애플리케이션 취약한 항목

이 값은 sn_vul_analytics_app_ci_dept_bu 테이블을 사용 중인 활성 AVI가 있는 표시기 소스 애플리케이션의 개수입니다. 목표는 최소화하는 것입니다.

세부 항목

- 기간
- 종결 연령
- 애플리케이션
- 비즈니스 단위
- 위험 등급
- 스캔 유형

주:
애플리케이션 취약한 항목(AVI)에 대한 기간 및 종결된 기간 계산을 사용자 지정하면 이러한 메트릭을 포함하는 퍼포먼스 분석(PA) 보고서가 급격히 증가하거나 감소할 수 있습니다. AVI에 대한 연령 및 종결 연령 계산을 사용자 지정하는 방법에 대한 자세한 내용은 KB1703270 KB 문서를 참조하세요.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

데이터 시각화

보안 태세

이름	유형	설명
V15.0: 유효성 확인 보류 중인 상태의 침투 테스트 결과	원형 차트	침투 테스트 결과가 해결됨 상태이지만 유효성 검사가 보류 중이며 위험 등급별로 그룹화되어 있습니다.
V15.0: 지연된 침투 테스트 결과	원형 차트	정정 목표 날짜를 놓친 중요 침투 테스트 결과로, 위험 등급별로 그룹화됩니다.
활성 애플리케이션 취약한 항목 (AVI)	단일 점수	활성 (비-종결된) 애플리케이션 취약한 항목의 수(AVI)
할당되지 않은 애플리케이션 취약한 항목 (AVI)	단일 점수	담당자 또는 할당 그룹이 없는 활성 취약한 항목 수입니다.
애플리케이션 취약한 항목 (AVI) 배포	원형 차트	위험 등급에 따라 그룹화된 활성 AVI(애플리케이션 취약한 항목)의 분포입니다.
기간 별 애플리케이션 취약한 항목 (AVIs)	히트맵	위험 등급 및 기간(일)별로 그룹화된 활성 AVI(애플리케이션 취약한 항목) 수입니다. **주:** 애플리케이션 취약한 항목(AVI)에 대한 기간 및 종결된 기간 계산을 사용자 지정하면 이러한 메트릭을 포함하는 퍼포먼스 분석(PA) 보고서가 급격히 증가하거나 감소할 수 있습니다. AVI에 대한 연령 및 종결 연령 계산을 사용자 지정하는 방법에 대한 자세한 내용은 KB1703270 KB 문서를 참조하세요.
AVI 추세	추세	위험 등급에 따라 그룹화된 활성 AVI(애플리케이션 취약한 항목)의 추세입니다.
애플리케이션당 평균 AVI	추세	위험 등급에 따라 그룹화된 평균 AVI(애플리케이션 취약한 항목)의 추세입니다.

정정 추세

이름	유형	설명
애플리케이션 취약한 항목(AVI) 정정 평균 시간	선형	위험 등급에 따른 애플리케이션 취약한 항목(AVI)의 평균 정정 시간 추세입니다.
AVI의 순 변경	추세	새 AVI(애플리케이션 취약한 항목) 대 월별 종결의 추세입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

득점판

이름	유형	설명
가장 중요한 애플리케이션 취약한 항목(AVI)이 있는 상위 10개의 애플리케이션	점수 카드 및 분포 표시줄	가장 중요한 애플리케이션 취약한 항목(AVI)의 최다 부문이 있는 애플리케이션
가장 기한이 지난 중요한 애플리케이션 취약한 항목(AVI)이 있는 상위 10개의 애플리케이션	점수 카드 및 분포 표시줄	정정 대상 날짜가 지난 활성 애플리케이션 취약한 항목(AVI) 수가 가장 많은 애플리케이션입니다.

내 애플리케이션 취약성 대시보드

이 대시보드는 정정 목표 달성률 보기와 같은 애플리케이션 취약성 관리 프로세스를 분석하는 데 중요한 메트릭을 제공합니다.

필요한 **ServiceNow AI Platform** 역할 및 대시보드 보기

주:

- 이 대시보드는 Application Vulnerability Response 콘텐츠 팩의 일부입니다. Application Vulnerability Response 콘텐츠 팩은 Performance Analytics for Vulnerability Response 콘텐츠 팩의 일부입니다.
- Performance Analytics for Vulnerability Response 콘텐츠 팩은 별도의 ServiceNow# Store 구독으로 사용할 수 있습니다.
- Performance Analytics for Vulnerability Response 콘텐츠 팩은 Vulnerability Response 애플리케이션과 함께 자동으로 설치되지 않습니다.

내 애플리케이션 취약성 대시보드는 보안 챔피언 사용자 그룹의 구성원이 인스턴스에 로그인하는 경우에만 사용할 수 있습니다. 개요 대시보드에 대한 자세한 내용은 PA〔애플리케이션 취약성 관리〕 대시보드를 참조하십시오.

대시보드를 보려면 다음으로 이동합니다. 애플리케이션 취약성 대응 〉 내 애플리케이션 취약성.

의 애플리케이션 취약성 대응버전 19.0부터 이 대시보드는 New Experience UI에서도 볼 수 있습니다. 새 UI에서 대시보드를 보려면 다음으로 이동합니다. 작업 공간 〉 취약성 관리자 작업 공간 을 클릭하고 대시보드 아이콘을 클릭합니다. 역할에 따라 기본 대시보드가 표시됩니다. 다른 대시보드를 보려면 대시보드 이름 옆에 있는 드롭다운을 클릭합니다. 자세한 내용은 대시보드 페이지의 취약성 관리자 작업 공간 및 대시보드 페이지의 IT 정정 작업 공간 문서를 참조하십시오.

시간 경과에 따른 추세 데이터를 보여주는 보고서를 봅니다. 중요한 메트릭의 추세를 정기적으로 확인하여 전체 비즈니스 프로세스를 분석하고 개선 영역을 식별합니다.

내 애플리케이션 취약성 대시보드는 Performance Analytics for Vulnerability Response 컨텐츠 팩에 포함되어 있습니다. Performance Analytics for Vulnerability Response 컨텐츠 팩은 애플리케이션과 함께 취약성 대응 자동으로 설치되지 않습니다. 별도의 구독으로 사용할 수 ServiceNow# Store 있습니다.

사용 사례

사용자	대시보드 사용
자신 또는 자신이 속한 그룹에 할당된 취약성을 정정하는 IT 전문가, 정정 소유자 또는 분석가입니다.	보안 챔피온은 내 애플리케이션 취약성 대시보드를 사용하여 애플리케이션 취약성에

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용자	대시보드 사용
	대한 정정 볼륨, 성능 및 진행 상황을 추적합니다. 조직에 가장 큰 위험을 초래하는 애플리케이션 취약한 항목(AVI)을 효율적으로 결정합니다. 이러한 대시보드는 AVI 활동에 대한 그래픽 보기를 제공하여 정정 계획 및 상태 진행률을 확인하는 데 도움이 됩니다. 영향을 받는 중요한 애플리케이션 및 가시성이 높은 취약성과 연결된 KPI에 집중할 수 있습니다. 취약성 노출 및 보안 태세에 대한 인사이트를 빠르게 확보합니다. 초기 분석 및 탐지부터 억제 또는 정정에 이르기까지 추적합니다.

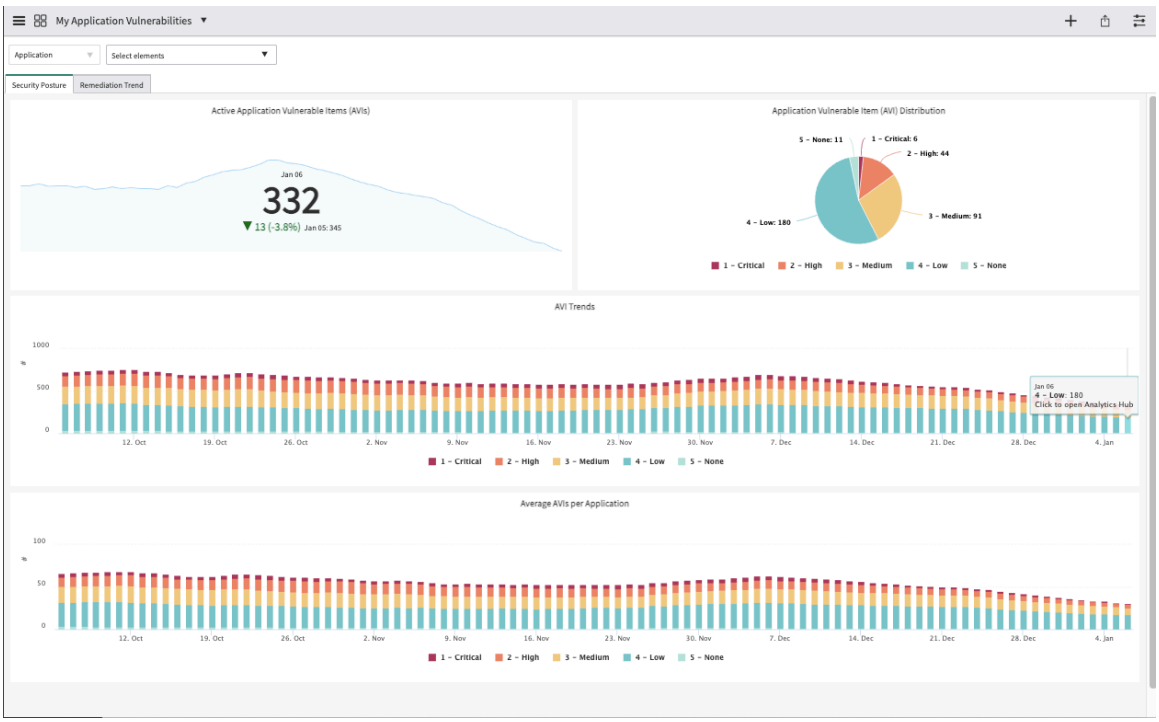
내 애플리케이션 취약성 **[PA]** 대시보드 탭

내 애플리케이션 취약성 대시보드는 취약성 위험 및 보급, 영향을 받는 애플리케이션, 정정 추세 및 정정 진행 상황에 대한 KPI를 전달합니다. 추세의 기본값은 3개월이지만 7일, 1개월, 3개월, 6개월, YTD, 1년 또는 모두로 변경할 수 있습니다.

데이터는 대시보드에서 애플리케이션별로 세분화됩니다. 요소 선택 목록을 사용하여 선택 항목을 구체화합니다.

보안 태세 탭

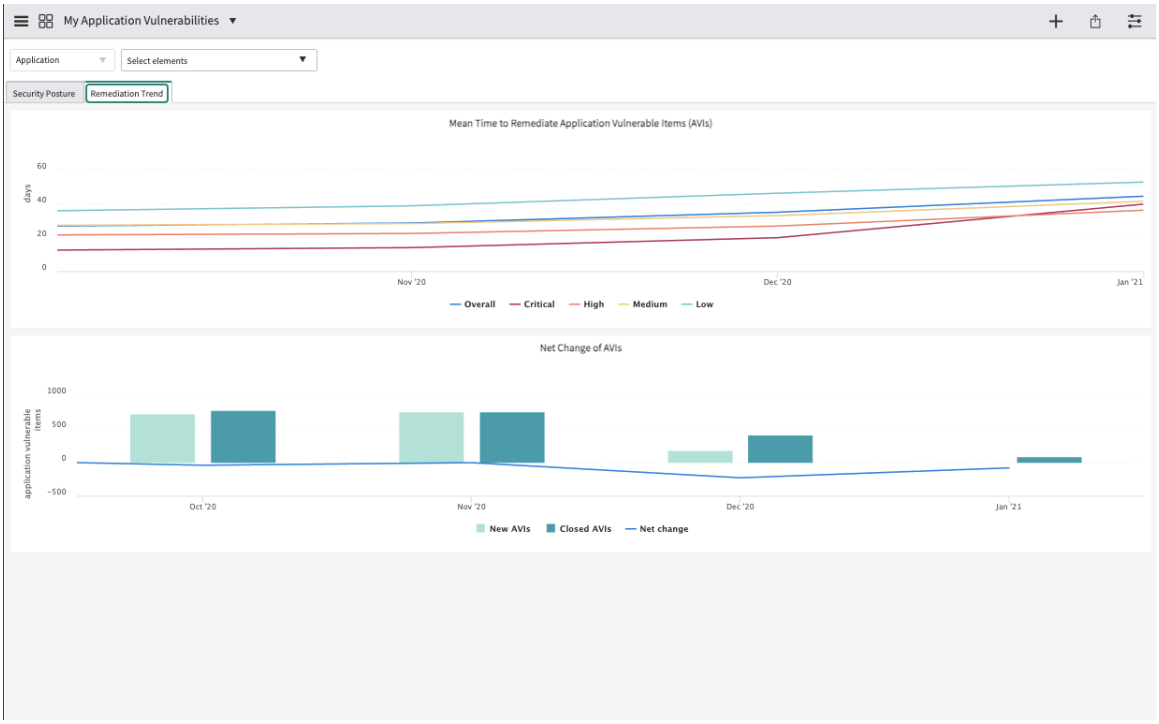
보안 태세 탭은 보안 태세와 정정 작업의 진행 상황을 이해하는 데 도움이 됩니다. 애플리케이션 취약성 관리 대시보드의 데이터를 스캔 유형, 애플리케이션 또는 비즈니스 단위별로 분류합니다. 이러한 각 선택 항목에는 선택 항목을 구체화하기 위한 추가 필터인 요소 선택이 있습니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

정정 추세 탭

정정 추세 탭은 정정 작업의 진행 상황을 이해하는 데 도움이 됩니다.



표시기

낮은 AVI 정정 평균 시간

[[### ###### ### ### ## ## > ## ## = 4 - ##]] / [[### ###### ### ## > ## ## = 4 - ##]]. 목표는 최소화하는 것입니다.

애플리케이션 릴리스

AVI와 응용 프로그램의 고유 수입니다. 활성입니다. sn_vul_app_vulnerable_item 테이블을 사용합니다. 목표는 최소화하는 것입니다.

애플리케이션 취약한 항목

앱 취약한 항목 AVI의 수입니다. 활성입니다. sn_vul_app_vulnerable_item 테이블을 사용합니다. 목표는 최소화하는 것입니다.

애플리케이션당 평균 AVI

[## ###### ### ##]]/[[###### ###]]. 목표는 최소화하는 것입니다.

할당되지 않은 VI

표시기 소스 AVI의 개수입니다. 활성입니다. sn_vul_app_vulnerable_item 테이블을 사용합니다. 목표는 최소화하는 것입니다.

AVI 정정 평균 시간

[[### ###### ### ### ## ##]]/[[### ###### ### ##]]. 목표는 최소화하는 것입니다.

높은 AVI 정정 평균 시간

[[### ###### ### ### ## ## > ## ## = 2 - ##]] / [[### ###### ### ## > ## ## = 2 - ##]]. 목표는 최소화하는 것입니다.

닫힌 애플리케이션 취약한 항목

표시기 소스 AVI의 개수입니다. 종결됨. 사용 중인 테이블: sn_vul_app_vulnerable_item. 목표는 최대화하는 것입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

핵심 AVI 정정 평균 시간

[[### ###### ### ### ## ## > ## ## = 1 - ##]] / [[### ###### ### ## > ## ## = 1-##]]. 목표는 최소화하는 것입니다.

새 애플리케이션 취약한 항목

표시기 소스 AVI의 개수입니다. New. 사용 중인 테이블: sn_vul_app_vulnerable_item. 목표는 최소화하는 것입니다.

보통 AVI 정정 평균 시간

[[### ###### ### ### ## ## > ## ## = 3 - ##]] / [[### ###### ### ## > ## ## = 3 - ##]]. 목표는 최소화하는 것입니다.

VI의 순 변경

[[# ###### ### ##]] - [[## ###### ### ##]]. 목표는 최소화하는 것입니다.

닫힌 애플리케이션 취약한 항목의 합산 기간

표시기 소스 AVI의 개수입니다. 종결됨. 사용 중인 테이블: sn_vul_app_vulnerable_item. 목표는 최소화하는 것입니다.

핵심 지연 애플리케이션 취약한 항목

데이터 소스 AVI의 개수입니다. 활성입니다. sn_vul_app_vulnerable_item 테이블을 사용합니다. 목표는 최소화하는 것입니다.

핵심 애플리케이션 취약한 항목

이 값은 sn_vul_analytics_app_ci_dept_bu 테이블을 사용 중인 활성 AVI가 있는 표시기 소스 애플리케이션의 개수입니다. 목표는 최소화하는 것입니다.

세부 항목

- 기간
- 종결 연령
- 애플리케이션
- 비즈니스 단위
- 위험 등급
- 스캔 유형

주:
애플리케이션 취약한 항목(AVI)에 대한 기간 및 종결된 기간 계산을 사용자 지정하면 이러한 메트릭을 포함하는 퍼포먼스 분석(PA) 보고서가 급격히 증가하거나 감소할 수 있습니다. AVI에 대한 연령 및 종결 연령 계산을 사용자 지정하는 방법에 대한 자세한 내용은 KB1703270 KB 문서를 참조하세요.

데이터 시각화

보안 태세

이름	유형	설명
활성 애플리케이션 취약한 항목(AVI)	단일 점수	활성 (비-종결된) 애플리케이션 취약한 항목의 수(AVI)
애플리케이션 취약한 항목(AVI) 배포	원형 차트	위험 등급에 따라 그룹화된 활성 AVI(애플리케이션 취약한 항목)의 분포입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 태세

이름	유형	설명
AVI 추세	추세	위험 등급에 따라 그룹화된 활성 AVI(애플리케이션 취약한 항목)의 추세입니다.
애플리케이션당 평균 AVI	추세	위험 등급에 따라 그룹화된 평균 AVI(애플리케이션 취약한 항목)의 추세입니다.

정정 추세

이름	유형	설명
애플리케이션 취약한 항목(AVI) 정정 평균 시간	선형	위험 등급에 따른 애플리케이션 취약한 항목(AVI)의 평균 정정 시간 추세입니다.
AVI의 순 변경	추세	새 AVI(애플리케이션 취약한 항목) 대 월별 종결의 추세입니다.

에 대한 집계 보고서 프레임워크 애플리케이션 취약성 대응

집계된 보고서 프레임워크를 사용하면 성능 향상을 위해 복잡하고 실행 시간이 긴 즉석 쿼리가 포함된 데이터에 대한 보고서를 만들 수 있습니다.

집계된 보고서 프레임워크는 다음을 통해 성과를 개선합니다.

- 더 적은 리소스를 사용하고 보고서를 더 빠르게 렌더링합니다.
- 데이터 집계와 집계 및 세부 항목 재사용(그룹화 기준)
- 데이터베이스에 대한 쿼리 줄이기

애플리케이션 취약 항목(AVIT)이 100만 개 이상인 경우 표준 보고서와 함께 집계된 보고서 프레임워크를 사용합니다.

필요한 역할

이 솔루션과 관련된 역할과 작업은 다음과 같습니다.

- ServiceNow AI Platform관리자(admin): 이 플랫폼 분석 솔루션을 설치 및 활성화하고 시스템 속성을 필요에 따라 변경합니다.
- 퍼포먼스 분석 관리자(pa_admin): 집계, 위젯 및 대시보드를 검토합니다. 데이터 수집을 설정 및 시작합니다. 적절한 이해 관계자와 대시보드를 공유합니다.
- 관리자(sn_vul_cmn.admin): 집계를 생성합니다.
- VR write(sn_vul_cmn.write): 집계 및 집계된 결과에서 데이터를 편집합니다.
- VR 읽기(sn_vul_cmn.read): 집계 및 집계된 결과의 데이터를 검토합니다.
- 취약성 분석가(sn_vul.vulnerability_analyst): 집계된 결과를 검토합니다.

관련 정보

- 소스 데이터에 대한 집계 구성
- 여러 집계를 동시에 실행
- 동시에 실행할 수 있는 집계 수 구성
- 집계를 사용하여 보고서 생성

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

애플리케이션 취약성 대응 참조

애플리케이션과 함께 설치되는 테이블, 역할 및 속성에 대한 정보가 포함된 참조 주제입니다 애플리케이션 취약성 대응 .

자세한 내용은 다음을 참조하십시오.

- 애플리케이션 취약성 대응 사용자 그룹 및 역할
- 애플리케이션 취약성 대응와 함께 설치되는 구성요소
- 애플리케이션 취약한 항목(AVI) 상태
- 스캔한 애플리케이션 필드
- 애플리케이션 취약한 항목 필드
- 애플리케이션 취약성 필드
- 침투 테스트 상태

애플리케이션 취약성 대응 사용자 그룹 및 역할

(AVR)을 사용하여 애플리케이션 취약성 대응 취약성을 성공적으로 정정하려면 먼저 사용자 그룹에 사용자를 할당해야 합니다.

역할은 사용자와 사용자의 그룹이 에서 보고 수행할 애플리케이션 취약성 대응수 있는 것을 취약성 대응용 퍼포먼스 분석, 및 와의 애플리케이션 취약성 대응외부 공급업체 통합을 정의합니다.

사용자 그룹

지원하는 애플리케이션 취약성 대응기본 사용자 그룹은 다음과 같습니다.

- App-Sec Manager: 보안 관리자를 포함합니다. v15.0부터 애플리케이션 취약성 대응 는 침투 테스트 평가 요청을 관리하는 애플리케이션 소유자도 포함됩니다.
- 보안 챔피언: 개발 그룹과 보안 관리자 간의 연락 담당자를 포함합니다.
- 개발자: 개별 기여자를 포함합니다.
- V15.0: 윤리적 해커: 애플리케이션의 침투 테스트를 수행하는 윤리적 해킹 팀의 구성원을 포함합니다.

시스템 관리자 [admin] 역할은 사용자 관리 모듈을 사용하여 기본 사용자 그룹에 사용자를 애플리케이션 취약성 대응 할당하는 데 필요합니다.

주:

AVR 사용자를 애플리케이션 취약성 대응 의 애플리케이션 취약성 대응 사용자 그룹에 할당하는 것은 설정 도우미 기능에서 취약성 대응 사용할 수 없습니다. 역할만 취약성 대응 할당됩니다.

다음 표에는 사용 가능한 애플리케이션 취약성 대응 사용자 그룹 및 해당 그룹과 연결된 역할이 나열되어 있습니다. 이 테이블을 사용하여 어떤 사용자에게 어떤 그룹을 할당해야 하는지 결정합니다.

사용자 그룹	이 그룹에서의 역할
보안 챔피언 이 그룹의 구성원은 다음을 수행할 수 있습니다.	• sn_vul.app_read_assigned • sn_vul.app_write_assigned • sn_vul.app_update_assignment_group입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용자 그룹	이 그룹에서의 역할
• 사용자에게 할당된 애플리케이션 취약한 항목(AVI)을 읽고 씁니다. • 사용자에게 할당된 AVI를 다른 개인 또는 그룹에 할당합니다. • V20.0: 예외 규칙 만들기, 업데이트, 삭제 및 취소(비활성화)	• sn_vul.app_update_assigned_to • sn_vul.app_manage_auto_exception_rule
App-Sec 관리자 이 그룹의 구성원은 다음을 수행할 수 있습니다. • V20.0: 예외 규칙 만들기, 업데이트, 삭제 및 취소(비활성화) • 애플리케이션 정정 작업 규칙에 대한 읽기, 쓰기, 삭제 및 모든 작업 • 모든 AVI를 읽고 씁니다. • 규칙, 계산기 및 심각도 맵을 생성하고 관리하여 AVR을 구성합니다. • 통합을 구성합니다. • AVI를 삭제합니다. • 개인 또는 그룹에 AVI를 할당합니다. • 애플리케이션을 관리합니다. • 애플리케이션 모듈에 액세스할 수 있습니다. • 통합 예약, 구성, 실행. • 통합을 읽고 실행합니다. • AVR 퍼포먼스 분석 대시보드 및 보고서를 확인합니다. • V15.0: 침투 테스트 평가 요청을 관리합니다.	• sn_vul.app_manage_auto_exception_rule • sn_vul.app_manage_group_rules • sn_vul.app_read_all • sn_vul.app_write_all • sn_vul.app_update_assignment_group입니다. • sn_vul.app_update_assigned_to • sn_vul.app_configure_integrations 주: 기본적으로 이 역할에는 외부 공급업체 통합 구성에 대한 세분화된 역할이 포함됩니다. 단일 또는 특정 통합으로 App-Sec Manager 사용자 그룹을 정의하거나 편집하려면 문서를 취약성 대응 가상 사용자 및 세분화된 역할참조하십시오. • sn_vul.app_manage_assignment_rules • sn_vul.app_manage_remediation_target_rules • sn_vul.app_manage_risk_score_configurations • sn_vul.app_manage_applications • sn_vul.app_manage_app_vul_permissions • sn_vul.app_manage_normalized_severity • 버전 13.0: sn_vul.app_manage_app_sc • 버전 12.0에만 해당: sn_vul.app_read_application_release 〔v12.1에서 제거되었습니다. 사용하지 마십시오.〕 • sn_sec_int.admin • 버전 13.0: pa_power_user • pa_viewer 주: v13.0부터 취약성 대응 pa_viewer pa_power_user에 포함되어 더 이상 자체적으로 필요하지 않습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용자 그룹	이 그룹에서의 역할
	• V15.0: sn_vul.app_manage_pen_test_request • V15.0: sn_vul.app_update_state • V15.0: cmdb_read
개발자 이 그룹의 구성원은 다음을 수행할 수 있습니다. • 할당된 AVR 기록을 읽고 씁니다. • 사용자에게 할당된 AVI를 다른 개인 또는 그룹에 할당합니다.	• sn_vul.app_read_assigned • sn_vul.app_write_assigned • sn_vul.app_update_assignment_group입니다. • sn_vul.app_update_assigned_to • sn_vul.app_pa_sc_뷰
V15.0: 윤리적 해커 이 그룹의 구성원은 다음을 수행할 수 있습니다. • 침투 테스트 평가 요청에 대한 기본 담당 그룹 및 담당자를 구성합니다. • 침투 테스트 결과를 관리합니다. • 침투 테스트 평가 요청을 관리합니다. • 애플리케이션 취약한 항목을 봅니다. • 애플리케이션 취약한 항목에 대한 할당을 업데이트합니다.	• V15.0: sn_vul.app_update_state • V15.0: sn_vul.app_manage_pen_test_request • V15.0: itil • V15.0: sn_vul.app_read_all • V15.0: sn_vul.app_manage_pen_test_request_config • V15.0: sn_vul.app_manage_manual_avits • V15.0: sn_vul.app_update_assigned_to • V15.0: sn_vul.app_update_assignment_group

에서 사용자 그룹에 사용자 할당 애플리케이션 취약성 대응

인스턴스에서 사용자 관리 모듈을 사용하여 그룹에 사용자를 할당합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

그룹에서 사용자를 할당하거나 제거하려면 다음과 같이 하십시오.

a. 다음으로 이동 관리 〉 그룹.

b. 적절한 그룹(예: **App-Sec Manager**)을 찾아 엽니다.
그룹 기록이 표시됩니다.

c. 그룹 구성원 탭을 선택합니다.
그룹의 현재 구성원이 표시됩니다.

d. 편집을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

구성원 편집 양식이 표시됩니다.

e. 컬렉션 목록에서 그룹에 추가하거나 그룹에서 제거할 사용자를 선택합니다.

f. 모든 사용자가 그룹 구성원 목록에 추가되거나 제거되면 저장을 클릭합니다.
그룹 구성원 탭으로 돌아갑니다.

g. 업데이트를 클릭하여 변경 내용을 저장하고 그룹 목록으로 돌아갑니다.

관련 정보

애플리케이션 취약성 대응와 함께 설치되는 구성요소

애플리케이션 취약성 대응와 함께 설치되는 구성요소

기능을 활성화하면 테이블, 사용자 역할, 예약된 작업을 포함한 여러 유형의 구성요소가 애플리케이션 취약성 대응 설치됩니다.

의 애플리케이션 취약성 대응v24.0.6부터 가장 자주 사용되는 시스템 속성에 애플리케이션 내에서 액세스할 수 있습니다 애플리케이션 취약성 대응 . 이러한 시스템 속성을 보려면 다음으로 이동합니다. 모두애플리케이션 취약성 대응속성.

주:
애플리케이션 파일 테이블에는 이 애플리케이션과 함께 설치되는 구성요소가 나열됩니다. 이 테이블에 액세스하는 방법에 대한 지침은 애플리케이션과 함께 설치되는 구성요소 찾기 를 참조하십시오.

이 기능에 대한 데모 데이터를 사용할 수 있습니다.

설치되는 역할

의 애플리케이션 취약성 대응 세분화된 역할은 기본적으로 특정 사용자 그룹에 할당됩니다.

주:
이러한 사용자 그룹 외부에서 세분화된 역할을 사용하려면 코딩과 고급 애플리케이션 취약성 대응 또는 ServiceNow 전문 지식이 필요합니다.

역할 이름 **[name]**	설명	포함하는 역할
V20.0: sn_vul.app_manage_auto_exception_rule	예외 규칙을 생성, 업데이트, 삭제 및 취소(비활성화)합니다.	sn_vul.app_read_auto_excep
sn_vul.app_manage_group_rules	애플리케이션 정정 작업 규칙에 대한 읽기, 쓰기, 삭제 및 모든 작업	• sn_vul.app_read_all • sn_vul.app_read_group_
V20.0: sn_vul.app_exception_approver	예외 규칙 및 예외 규칙 연장 요청을 승인합니다. v20.0부터 이 역할에 대한 세분화된 역할인 sn_vul.app_read_all이 제거되었으므로, 사용자는 모든 애플리케이션 취약한 항목 및 정정 작업 대신 사용자와 그룹에 할당된 애플리케이션 취약 항목 및 정정 작업에 액세스할 수 있습니다.	• sn_vul.app_read_auto_ex • sn_vul.view_manager_wo

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

역할 이름 **[name]**	설명	포함하는 역할
sn_vul.app_false_positive_approver	긍정 오류 요청을 승인하거나 거부합니다.	sn_vul.view_manager_works
sn_vul.app_read_assigned	사용자에게 할당된 애플리케이션 취약한 항목(AVI)을 클래식 UI 및 IT 정정 작업 공간. 중요사항: 의 취약성 대응v24.0부터 sn_vul.app_read_assigned 역할은 에 액세스할 IT 정정 작업 공간수 있는 권한이 있습니다.	sn_vul.view_rem_workspace
sn_vul.app_read_all	클래식 UI 또는 취약성 관리자 작업 공간에서 모든 AVI 및 관련 정보를 봅니다. 중요사항: 의 취약성 대응v24.0부터 sn_vul.app_read_all 역할은 에 액세스할 수 있는 취약성 관리자 작업 공간권한이 있습니다.	sn_vul.view_manager_works
sn_vul.app_write_assigned	할당된 AVI를 업데이트합니다.	
sn_vul.app_write_all	모든 AVI 및 관련 정보를 업데이트합니다.	
sn_vul.app_update_assignment_group입니다.	AVI 할당 그룹을 업데이트합니다.	주: 기본 사용자 그룹 외부에 경우 sn_vul.app_write_a sn_vul.app_write_assign
sn_vul.app_update_assigned_to	AVI 담당자를 업데이트합니다.	주: 기본 사용자 그룹 외부에 경우 sn_vul.app_write_a sn_vul.app_write_assign
sn_vul.app_configure_integrations	외부 공급업체 통합을 구성합니다.	sn_vul.app_read_all sn_vul.app_read_integratio sn_sec_int.admin sn_vul_veracode.configure sn_vul.configure_nvd_admi [store-future: BEGIN review]sn_vul_fortify.confi

기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

역할 이름 **[name]**	설명	포함하는 역할
		주: 단일 또는 특정 통합으로 사용자 그룹을 정의하거 문서를 취약성 대응 가상 역할참조하십시오.
sn_vul.app_read_integrations	모든 외부 공급업체 통합을 봅니다.	
sn_vul_veracode.configure_integration	Veracode 통합을 정의, 업데이트 및 삭제합니다.	
sn_vul.app_manage_assignment_rules	AVI 담당 규칙을 정의, 업데이트 및 삭제합니다.	sn_vul.app_read_all sn_vul.app_read_assignme
sn_vul.app_read_assignment_rules	담당 규칙을 봅니다.	
sn_vul.app_manage_remediation_target_rules	AVI 정정 대상 규칙을 정의, 업데이트 및 삭제합니다.	sn_vul.app_read_all sn_vul.app_read_remediati
sn_vul.app_manage_risk_score_configurations	AVR 계산기 및 위험 규칙을 정의, 업데이트 및 삭제합니다.	sn_vul.app_read_all sn_vul.app_read_risk_score sn_sec_cmn.calc.write
sn_vul.app_read_risk_score_configuration	AVR 계산기 및 위험 규칙을 봅니다.	
sn_vul.app_manage_applications	애플리케이션 기록을 보고, 업데이트하고, 삭제합니다.	
sn_vul.app_manage_app_sc	보안 챔피언에게 검사한 애플리케이션 관련 목록에서 자신을 추가하거나 제거할 수 있는 기능을 제공합니다.	
sn_vul.app_pa_sc_뷰	특정 보안 챔피언에 대한 관련 뷰를 제공합니다.	
sn_vul.app_manage_app_vul_permissions	〔내부〕 sn_vul.app_manage_applications에서 사용됩니다.	
sn_vul.app_manage_normalized_severity	매핑을 정규화된 심각도로 업데이트합니다.	sn_vul.app_read_normalized_
sn_vul.app_read_normalized_severity 〔v12.1에서 제거되었습니다. 사용하지 마세요.〕	정규화된 심각도 기록을 봅니다.	
sn_vul.app_read_application_release	애플리케이션 릴리스 기록을 봅니다.	
sn_sec_int.admin	통합에 대한 액세스를 제공합니다.	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

역할 이름 **[name]**	설명	포함하는 역할
pa_power_user	보고서에 대한 액세스를 제공합니다.	pa_viewer
sn_vul.app_sec_manager	애플리케이션 취약한 항목의 우선순위를 지정하고 관리합니다.	
sn_vul.app_developer	애플리케이션 취약성을 수정할 책임이 있는 개발자입니다.	
sn_vul.app_create_watch_topic	애플리케이션 취약성에 대한 감시 주제를 생성합니다.	
sn_vul.app_read_watch_topic	애플리케이션 취약성에 대한 주시 주제를 읽어보십시오.	
sn_vul.app_edit_watch_topic	애플리케이션 취약성에 대한 감시 주제를 편집합니다.	
sn_vul_blackduck.configure_integration	외부 공급업체 통합을 구성합니다.	sn_vul_blackduck.configure_i

설치되는 예약된 작업

취약성 대응 공유 예약된 작업은 문서를 참조하십시오취약성 대응 앱과 함께 설치되는 구성요소.

예약된 작업	설명
기존 AVI를 자동 예외 규칙과 연결	애플리케이션 취약한 항목이 예외 규칙과 일치하는지 평가합니다.
항목 및 CVE M2M 채우기	기존 기록을 여러 CWE 기록과 일치시킵니다. 업그레이드 후 한 번 실행하여 채운 다음 비활성화합니다.
기본 CWE 재동기화	사용자 지정된 기본 CWE 계산의 경우. 업그레이드 후 한 번 실행하여 다시 동기화한 다음 비활성화합니다.
애플리케이션 취약한 항목 값을 취약성 및 그룹에 롤업	애플리케이션 취약한 항목에 대한 취약성 및 그룹 롤업을 계산합니다. 주: 의 애플리케이션 취약성 대응v23.0부터 예약된 작업이 개선되어 멀티스레딩 기능이 있는 백그라운드 작업을 생성할 수 있습니다. 이 업그레이드에는 작업을 여러 개의 더 작은 하위 작업으로 분할하는 작업이 포함되며, 이러한 작업은 병렬로 또는 동시에 실행됩니다. 이렇게 수정하면 여러 기록을 동시에 처리할 수 있으므로 전체 작업 속도가 크게 향상됩니다.
Black Duck 프로젝트 목록 통합	데이터를 Black Duck 프로젝트 테이블로 끌어오고 수집합니다.
Black Duck 애플리케이션 목록 통합	프로젝트 테이블의 Black Duck 통합에서 사용할 수 있는 모든 프로젝트 버전에 대해 애플리케이션을 검색된 애플리케이션 테이블로 임포트합니다.
Black Duck 애플리케이션 취약한 항목 통합	시스템에서 검색된 모든 애플리케이션에 대해 스캐너가 탐지한 취약성을 기반으로 취약한 항목을 ServiceNow 애플리케이션으로 수집합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설치되는 테이블

테이블	설명
애플리케이션 릴리스 [sn_vul_app_release]	애플리케이션 버전 정보를 포함합니다.
버전 13.0 : 애플리케이션 보안 챔피온 [sn_vul_app_m2m_app_sc]	애플리케이션 취약성 대응 보안 챔피언 그룹 기록을 포함합니다.
애플리케이션 취약성 항목 [sn_vul_app_vul_entry]	애플리케이션 취약성 항목을 포함합니다.
애플리케이션 취약성 통합 [sn_vul_app_integration]	통합 기록을 포함합니다 애플리케이션 취약성 대응 .
애플리케이션 취약성 통합 검사 위치 [sn_vul_app_vul_scan_location]	타사 검사 위치 정보를 포함합니다.
애플리케이션 취약성 검사 요약 [sn_vul_app_vul_scan_summary]	외부 공급업체 검사 요약 정보를 포함합니다.
애플리케이션 취약한 항목 [sn_vul_app_vulnerable_item]	AVI 기록을 포함합니다. v19.0부터 소프트웨어 자재 명세서에 다음 열이 추가됩니다. • sn_sbm_config_rule • sn_sbom_component • vex_justification • vex_detail • vex_response • vex_state • sca_type(SBOM-SCA)
검사한 애플리케이션 [sn_vul_app_scanned_application]	애플리케이션 정보를 포함합니다.
상태 맵 [sn_vul_app_state_map]	외부 공급업체 통합에서 애플리케이션 취약한 항목(AVI) 상태로의 상태 매핑을 포함합니다.
취약성 CWE [sn_vul_m2m_entry_cwe]	CVE 데이터를 애플리케이션 취약한 항목에 연결합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테이블	설명
애플리케이션 정정 작업 매니페스트 sn_vul_app_rt_manifest	정정 작업에 대한 업데이트는 예약된 작업에 따라 이 매니페스트 테이블을 사용하여 수행됩니다.
애플리케이션 정정 작업 sn_vul_app_vulnerability	애플리케이션 정정 작업을 포함합니다.
애플리케이션 정정 작업 항목 sn_vul_app_m2m_vul_group_item	AVI와 애플리케이션 정정 작업 간의 M2M 테이블입니다.
버전 21.0: 애플리케이션 취약한 항목 sn_vul_app_vulnerable_item	AVI 기록을 포함합니다.
버전 21.0: 패키지 [sn_vul_app_package]	애플리케이션 패키지 상세 정보를 포함합니다.
버전 21.0: 라이센스 sn_vul_app_license	애플리케이션 라이센스를 포함합니다.
버전 21.0: 애플리케이션 정정 작업 sn_vul_app_vulnerability	애플리케이션 정정 작업을 포함합니다.
sn_vul_blackduck_config	Black Duck 통합 구성 상세 정보를 포함합니다.
sn_vul_blackduck_project	Black Duck에서 제공되는 프로젝트의 세부 정보가 포함되어 있습니다.
sn_vul_blackduck_project_import	Black Duck 프로젝트 수집을 위한 임포트 세트 테이블입니다.
sn_vul_blackduck_app_import	Black Duck 애플리케이션 수집을 위한 임포트 세트 테이블입니다.
sn_vul_blackduck_avit_import	Black Duck AVIT 수집을 위한 임포트 세트 테이블입니다.

애플리케이션 취약한 항목**(AVI)** 상태

애플리케이션 취약성 대응 는 언제든지 애플리케이션 취약한 항목(AVI)의 상태에 대한 상태 모델을 제공합니다. 각 상태가 서로 어떻게 관련되고 영향을 미치는지 알면 AVI를 정정하는 시기와 방법을 결정하는 데 도움이 됩니다.

애플리케이션 취약한 항목 상태

상태의 작동 방식을 이해하면 애플리케이션 취약한 항목(AVI) 규칙을 생성하거나 편집하는 데 도움이 됩니다. AVI에는 외부 공급업체 통합에서 가져온 정정 상태에서 매핑되는 몇 가지 가능한 상태가 있습니다. AVI에서 상태 필드는 읽기 전용입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

애플리케이션 취약성 대응 상태 플로우 다이어그램

상태	설명
오픈	생성 시 상태입니다. 이 상태에서 다음을 수행할 수 있습니다. V16: 자세한 내용 가져오기 Fortify에서 임포트한 AVI에 대한 다음 정보를 가져옵니다. • 취약성 요약 • 취약성 설명 • 권장 사항 • 참조 • 요청 • 응답 V16: 긍정 오류로 표시 스캐너에서 시스템에 취약성이 있다고 보고하지만 실제로는 취약성이 없는 경우 항목을 가양성으로 표시합니다. V16: 예외 요청 예외, 재개시(종료) 날짜, 이유를 요청하고 선택적으로 추가 정보를 제공합니다. 예외가 요청되는 날짜까지 항목 정정을 연기합니다. V15: 닫기 취약한 항목 닫기 대화 상자에서 원인인 종결 상태를 선택하고 추가 정보를 제공합니다. AVI를 닫습니다. V15: 해결 열려 있는 AVI를 해결됨으로 표시하여 해결됨 상태로 이동합니다. 애플리케이션 취약한 항목 해결 대화 상자에서 해결 메모를 추가해야 합니다.
연기됨	**V15:** 이는 예외 요청 옵션에 의해 트리거됩니다. 승인 워크플로우의 일부로 연기됨 상태는 검토 중이며 승인될 때까지 종결될 수 없습니다. 이 상태에서 다음을 수행할 수 있습니다. V16: 자세한 내용 가져오기 Fortify에서 임포트한 AVI에 대한 다음 정보를 가져옵니다. • 취약성 요약 • 취약성 설명

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

애플리케이션 취약성 대응 상태 플로우 다이어그램

상태	설명
	• 권장 사항 • 참조 • 요청 • 응답 재개설 종결되거나 해결된 AVI를 다시 오픈 상태로 전환합니다. 닫기 종결 상태, 이유를 선택하고 추가 정보를 제공합니다. AVI를 닫습니다.
조사 중	상태 목록에서 이 옵션을 선택합니다. 이 상태에서 다음을 수행할 수 있습니다. V20.0 정정 작업 또는 AVI 기록을 구현 대기 중으로 수동 전환합니다. V16: 자세한 내용 가져오기 Fortify에서 임포트한 AVI에 대한 다음 정보를 가져옵니다. • 취약성 요약 • 취약성 설명 • 권장 사항 • 참조 • 요청 • 응답 V16: 긍정 오류로 표시 스캐너에서 시스템에 취약성이 있다고 보고하지만 실제로는 취약성이 없는 경우 항목을 가양성으로 표시합니다. V16: 예외 요청 예외, 재개시(종료) 날짜, 이유를 요청하고 선택적으로 추가 정보를 제공합니다. 예외가 요청되는 날짜까지 항목 정정을 연기합니다. V15: 닫기 취약한 항목 닫기 대화 상자에서 원인인 종결 상태를 선택하고 추가 정보를 제공합니다. AVI를 닫습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

애플리케이션 취약성 대응 상태 플로우 다이어그램

상태	설명
	V15: 해결 열려 있는 AVI를 해결됨으로 표시하여 해결됨 상태로 이동합니다. 애플리케이션 취약한 항목 해결 대화 상자에서 해결 메모를 추가해야 합니다.
대기 중인 구현	AVI에서 구현 대기 중과 조사 중 상태의 정정 작업 기록을 선택하여 기록을 이 상태로 수동 전환할 수만 있습니다. 이 상태에서 다음을 수행할 수 있습니다. 오픈 AVI를 다시 오픈 상태로 전환합니다. 조사 중 해결에 대한 자세한 정보를 가져옵니다. 조사 중으로 전환됩니다. 해결 열려 있는 AVI를 해결됨으로 표시하여 해결됨 상태로 이동합니다. 애플리케이션 취약한 항목 해결 대화 상자에서 해결 메모를 추가해야 합니다. 닫기 취약한 항목 닫기 대화 상자에서 원인인 종결 상태를 선택하고 추가 정보를 제공합니다. AVI를 닫습니다. 이 상태에서는 작업에 대한 조사 및 작업이 완료되고 수정 사항을 구현할 준비가 되었지만 아직 사용할 수 없는 경우 기록을 구현 대기 중으로 전환합니다. 정정 약정 날짜 및 정정 계획 필드를 설정합니다. 구현 후 기록을 해결하거나 종결합니다.
해결 일시	해결 버튼에서 트리거됩니다. 이 상태에서 다음을 수행할 수 있습니다. V16: 자세한 내용 가져오기 Fortify에서 임포트한 AVI에 대한 다음 정보를 가져옵니다. • 취약성 요약 • 취약성 설명 • 권장 사항

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

애플리케이션 취약성 대응 상태 플로우 다이어그램

상태	설명
	• 참조 • 요청 • 응답 재개설 열림 상태로 다시 전환됩니다 . 닫기 종결 상태, 이유를 선택하고 추가 정보를 제공합니다. 그룹을 닫습니다. 메모 및 해결 정보는 메모 탭 아래에 표시됩니다.
종결됨	닫기 버튼에서 트리거됩니다. 이 상태에서 다음을 수행할 수 있습니다. 다시 열기: 다시 열림 상태로 전환됩니다.

주:
AVI를 기반으로 한 다양한 통합을 이해하려면 다른 애플리케이션과 애플리케이션 취약성 대응 통합을 참조하십시오.

애플리케이션 정정 작업 상태

애플리케이션 정정 작업의 생성부터 종결까지, 애플리케이션 정정 작업은 전체 정정 프로세스 동안 여러 상태를 통해 전환됩니다.

상태 우선순위는 다음과 같습니다.

종결됨 〉 연기됨 〉 해결 일시 〉 검토 중 〉 대기 중인 구현 〉 조사 중 〉 오픈

상태 전환은 지연, 오픈, 종결 등 다양한 작업을 수행할 때 발생합니다.

특정 상태의 애플리케이션 업데이트 적용 작업에서 수행할 수 있는 작업은 호스트 업데이트 적용 작업의 작업과 유사합니다. 따라서 자세한 내용은 취약성 대응 정정 작업 상태 설명서의 및 상태 롤업 및 롤다운 시나리오취약성 대응 문서를 참조하십시오.

주:
v23.0 부터 취약성 대응스캐너가 정정 작업의 종결을 구동하도록 닫기 버튼이 제거되었습니다.

애플리케이션 취약성 대응 정정 작업 규칙의 예

조건 작성기를 사용하는 정정 작업 규칙의 예입니다.

취약성, 제품 모델, **IP** 주소 및 할당 그룹을 사용하는 정정 작업 규칙

1. 새 기록의 조건 작성기에서 조건을 다음과 같이 설정합니다. 취약성 〉 다음과 같음 알려진 취약성을 입력합니다.

   취약성은 다음에 애플리케이션 취약성 대응 구성설명된 대로 NVD(국가 취약성 데이터베이스) 및 CWE(일반적인 약점 열거) 통합에서 임포트됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

2. 그룹화 기준 섹션에서 필드에서 애플리케이션 취약한 항목 그룹화에 대해 애플리케이션 취약한 항목을 선택합니다.
3. 사용 필드에서 할당 그룹을 선택합니다.

   할당 규칙을 사용하여 정정 작업 규칙에 사용할 할당 그룹 필드를 자동으로 설정합니다. 애플리케이션과 함께 제공된 규칙을 사용하거나 고유한 담당 규칙을 설정할 수 있습니다. 자세한 내용은 에서 애플리케이션 취약 항목 애플리케이션 취약성 대응 자동으로 할당 문서를 참조하십시오.

4. 다른 조건(예: 그룹 애플리케이션 취약한 항목 시작 필드의 애플리케이션 취약한 항목 구성 항목, 사용 필드의 IP 주소 또는 제품 모델)을 선택합니다.
5. 할당 섹션의 필드별로 정정 작업 할당에서 필드별로 그룹화를 선택합니다.
6. 그룹화 기준 필드에서 할당 그룹을 선택합니다.

   이 섹션에 설명된 대로 이 선택 항목은 그룹화 기준 섹션에서 설정한 조건에 따라 다양한 그룹에 취약한 항목을 할당합니다. AVI는 취약성을 공유하지만 CI 제품 모델 또는 IP 주소에 따라 다른 그룹에 할당됩니다.

7. 제출을 선택하여 규칙을 저장합니다.

스캔한 애플리케이션 필드

애플리케이션은 임포트하는 동안 관리 〉 검색된 애플리케이션 in 애플리케이션 취약성 대응.

스캔한 애플리케이션 필드

이 테이블에서 임포트한 필드는 달리 지정하지 않는 한 읽기 전용입니다. 부서 및 지원 그룹 항목은 App-Sec 관리자가 수동으로 추가하거나 편집할 수 있습니다.

필드	설명
이름	애플리케이션의 임포트된 이름입니다.
버전	애플리케이션의 임포트한 버전(해당하는 경우).
운영 상태	애플리케이션의 임포트된 운영 상태입니다.
부서	애플리케이션이 속한 임포트한 부서입니다. 비어 있는 경우 수동으로 추가할 수 있습니다.
비즈니스 단위	부서가 속한 임포트한 비즈니스 단위입니다. 부서 필드가 채워지면 이 필드는 자동으로 부서가 속한 비즈니스 단위로 채워집니다. 그렇지 않으면 비어 있고 읽기 전용으로 남습니다.
지원 그룹	애플리케이션이 속한 임포트한 지원 그룹입니다. 비어 있는 경우 수동으로 추가할 수 있습니다.
설명	애플리케이션에 대한 임포트한 설명입니다.
마지막 정책 준수 확인 날짜	정책 준수를 위해 Veracode에서 애플리케이션을 마지막으로 검사한 날짜입니다. 이 날짜를 각 통합의 델타 시작 시간과 비교하여 애플리케이션에 대한 델타 수집을 지원할 수 있는 애플리케이션 목록 통합의 연결된 통합에 사용됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	주: Veracode에서 애플리케이션에 대한 데이터가 검색되며, "마지막 정책 준수 확인 날짜" 값이 연결된 통합의 "시작 시간"(delta_start_time)보다 크거나 같습니다.
관련 목록**(App-Sec** 관리자 또는 보안 챔피언에게만 표시)	
보안 챔피언	보안 챔피언과 연결된 애플리케이션을 나열합니다. App-Sec 관리자는 목록에서 구성원을 추가하거나 제거할 수 있습니다.

애플리케이션 취약한 항목 필드

애플리케이션 취약 항목(AVIT)은 타사 취약성 통합 임포트 중에 자동으로 생성됩니다.

애플리케이션 취약한 항목 필드

할당 그룹, 할당 대상 필드 및 메모를 제외한 AVIT의 다른 모든 필드는 읽기 전용입니다.

필드	설명
번호	이 기록에 대해 자동으로 생성된 AVIT 식별자입니다.
스캔 유형	이 AVIT를 찾은 스캐너의 유형입니다. 선택 항목은 다음과 같습니다. • 동적 • 정적 • SCA
위험 등급	취약한 항목을 중요, 높음, 중간, 낮음 및 없음으로 구분하는 정량화된 위험 점수 입니다. 위험 등급에 대한 자세한 내용은 을 참조하십시오 자동으로 위험 애플리케이션 취약성 대응 계산.
위험 점수	AVI가 사용자 환경에 미치는 위험의 계산된 양입니다. 자세한 내용은 자동으로 위험 애플리케이션 취약성 대응 계산 문서를 참조하십시오.
정정 약정 날짜	날짜 AVIT가 조사 중으로 이동한 후 수정되어야 합니다. 이 필드는 AVIT가 조사 중인 경우에만 나타납니다.
정정 대상	처음 식별된 이후 AVIT를 정정해야 하는 날짜입니다. 해당하는 경우에만 나타납니다. 정정 대상에 대한 자세한 내용은 다음 문서를 에서 정정 대상 추적 자동화 애플리케이션 취약성 대응참조하십시오.
정정 상태	AVIT에 대한 정정 상태입니다. 해당하는 경우 기한이 가장 가까운 AVIT에 의해 결정됩니다. 상태는 다음과 같습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	• 비행 중 • 대상에 접근 중 • 과거 대상
범주 이름	취약성 범주의 이름입니다.
취약성	이 애플리케이션 취약한 항목과 관련된 취약성 ID입니다.
애플리케이션 릴리스	애플리케이션 버전입니다.
애플리케이션 모듈	DAST 스캔에서 영향을 받는 애플리케이션입니다. SAST 스캔을 위해 숨겨집니다.
위치 버전 14.0: SAST	다스트: 애플리케이션 내 취약성의 URL 위치입니다. SAST: 애플리케이션 내 취약성에 대한 파일 경로 및 라인 번호입니다.
상태	이 필드는 생성 시 기본적으로 열림 으로 설정됩니다. 상태가 매핑되는 방법에 대한 자세한 내용은 을 참조하십시오 애플리케이션 취약한 항목(AVI) 상태 .
이유	〔AIV가 종결 상태일 때만 표시됩니다.〕 상태에 대한 설명입니다.
할당 그룹	이 AVIT에서 작업하도록 선택한 그룹입니다. App-Sec 관리자가 수동으로 추가하거나 편집할 수 있습니다.
담당자	이 AVI에서 작업하는 선택한 할당 그룹의 개인입니다. App-Sec 관리자가 수동으로 추가하거나 편집할 수 있습니다.
첫 발견	외부 공급업체 소스에서 애플리케이션 취약한 항목을 처음 발견한 날짜입니다.
마지막 발견	외부 공급업체 소스에서 애플리케이션 취약한 항목을 마지막으로 발견한 날짜입니다.
종결됨	〔AVIT가 종결 상태인 경우에만 표시됩니다.〕 AVI가 종결된 날짜입니다.
종결한 사람	〔AVIT가 종결 상태인 경우에만 표시됩니다.〕 AVIT를 종결한 엔터티입니다.
요약	임포트한 취약성 설명입니다.
정보 외부 공급업체 통합에서 임포트한 읽기 전용 데이터입니다.	
소스 AVIT ID	소스 AVIT에 대해 임포트한 식별자입니다.
소스 심각도	소스 애플리케이션에서 심각도를 임포트했습니다.
소스 대상 수정 날짜	소스에서 AVIT가 정정될 것으로 예상하는 임포트한 날짜입니다.
소스 완화 상태	소스 애플리케이션에서 임포트한 완화 상태입니다.
소스 정정 상태	소스 애플리케이션에서 임포트한 정정 상태입니다.
소스 결과 상태	〔채워진 경우에만 표시〕 소스 애플리케이션에서 임포트한 문제 상태입니다.
SDLC 상태	임포트된 소프트웨어 개발 수명주기 상태.
정책 준수	임포트된 준수 상태입니다. 상태가 제공되지 않은 경우 이 필드는 해당 사항 없음으로 설정됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
소스 링크	소스 AVIT에 대한 URL입니다.
소스 메모	소스에서 임포트한 메모입니다.
취약성 요약	소스에서 요약을 임포트했습니다.
취약성 설명	소스에서 임포트한 설명입니다.
권장 사항	소스에서 임포트한 권장 사항입니다.
참조	소스에서 임포트한 참조입니다.
HTTP 요청/응답**(DAST** 스캔에 대해서만 표시)	
소스 요청	HTTP 요청
소스 응답	HTTP 응답
메모	
정정 계획	AVIT를 정정하는 방법에 대한 상세 정보입니다. 계획은 정정 약정 날짜까지 구현되어야 합니다. 이 필드는 AVIT가 조사 중인 경우에만 나타납니다.
추가 의견/작업 메모	관련 정보입니다. 정보를 추가하려면 작업 메모의 텍스트 상자를 선택합니다. 취약성 대응 v20.0부터는 지연된 애플리케이션 취약한 항목에 대한 메모 섹션에 작업 메모를 추가할 수 있습니다.

AVIT의 기간 계산:

- AVIT 목록의 기간 열에는 AVIT가 활성화된 기간(형식: 일 HH:MM:SS)이 표시됩니다. 종결된 AVIT의 연령 값은 0입니다.
- AVIT 목록의 종결 기간 열에는 AVI가 종결되기 전에 활성 상태인 기간(형식: 일 HH:MM:SS)이 표시됩니다. 종결됨 상태가 아닌 AVIT의 경우 종결 기간 값은 0입니다.

Age 및 Age 종결 기간의 계산을 사용자 지정하는 방법에 대한 자세한 내용은 KB1703270 문서를 참조하십시오.

침투 테스트 상태

애플리케이션 소유자는 애플리케이션에 대한 침투 테스트 평가를 요청하고 요청이 해결될 때까지 윤리적 해킹 팀의 진행 상황을 모니터링할 수 있습니다.

침투 테스트 평가 요청은 해결될 때까지 다음 전환 상태를 통과합니다.

침투 테스트 평가 요청의 스테이지

필드	설명
침투 테스트 상태	
오픈	애플리케이션 소유자가 평가 요청을 만든 경우의 상태입니다.
범위 지정	윤리적 해킹 팀이 애플리케이션의 요청과 범위를 평가합니다.
환경 준비	애플리케이션 소유자는 역할 및 기타 정보가 포함된 환경을 생성하고 테스트를 위해 윤리적 해킹 팀에 제공합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

침투 테스트 평가 요청의 스테이지

필드	설명
테스트	윤리적 해킹 팀은 애플리케이션을 수동으로 테스트하여 침투 테스트 결과를 식별합니다.
V16.1: 테스트 진행 중	윤리적 해킹 팀은 현재 테스트가 진행 중임을 나타냅니다. 이 상태를 선택하면 양식에서 보류 중 테스트 옵션을 사용할 수 있게 됩니다.
V16.1: 보류 중 테스트	이 필드는 테스트 진행 중 상태가 선택된 경우에만 표시됩니다. 윤리적 해킹 팀은 필요한 경우 이 상태를 선택하여 침투 테스트 평가 요청의 서비스 수준 계약(SLA)을 제어합니다. 이렇게 하면 정확한 SLA가 보고됩니다.
V16.1: 검토 중인 테스트	윤리적 해킹 팀은 테스트가 완료되었으며 주제 전문가의 검토를 받고 있음을 나타냅니다.
종결됨	윤리적 해킹 팀은 침투 테스트 결과가 보고된 후 침투 테스트 평가 요청을 종결합니다. 주: V16.1부터 양식의 요청 복사 및 작성 옵션을 사용하여 종결 상태의 요청을 복제하고 새 요청을 작성할 수 있습니다. 자세한 내용은 종결 상태의 침투 테스트 요청 복제 문서를 참조하십시오.
V16.1: 취소됨	애플리케이션 소유자가 침투 테스트 평가 요청을 취소합니다.
V16.1: 초안	애플리케이션 소유자는 요청을 생성하고 요청을 제출하기 전에 초안으로 저장합니다.
애플리케이션 취약한 항목 상태	
오픈	윤리적 해킹 팀이 침투 테스트 결과를 식별하고 생성하면 해당 상태는 Open입니다.
해결 일시	애플리케이션 팀이 침투 테스트 결과를 해결하면 상태가 해결됨으로 이동됩니다. 주: 침투 테스트 결과가 해결되었지만 윤리적 해킹 팀에서 아직 검증되지 않은 경우 하위 상태는 *Validation Pending*입니다.
종결됨	윤리적 해킹 팀은 침투 테스트 결과가 해결되었는지 확인하고 상태를 종결로 전환합니다.

에서 지연 및 긍정 오류에 대한 상태 매핑 관리 애플리케이션 취약성 대응

에서 Veracode Vulnerability IntegrationFortify 취약성 통합 임포트한 애플리케이션 취약한 항목(AVI)의 소스 상태가 임포트되고 임포트 후 인스턴스에서 매핑되는 방식을 관리할 수 있습니다.

v20.0 부터 취약성 대응워크플로우를 사용하여 ServiceNow 임포트한 AVI를 분류할 수 있는 더 많은 옵션이 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용자 Fortify 취약성 통합 구성 또는 통합 Veracode Vulnerability Integration 구성구성 페이지에서는 인스턴스의 예외 및 긍정 오류를 관리하는 데 도움이 되는 두 가지 옵션을 제공합니다.

- 다음에서 예외 관리 ServiceNow
- 에서 긍정 오류 관리 ServiceNow

필요한 역할: App-Sec 관리자.

예외 관리 사용 사례

AVI는 소스 상태와의 이러한 통합에서 임포트됩니다. 스캐너의 소스 상태와 인스턴스에서 사용하는 상태가 정확히 일치하지 않는 경우가 있기 때문에 임포트 시 이러한 상태는 인스턴스의 대상 및 대상 이유 상태에 매핑됩니다.

예를 들어, '수정하지 않을 것', '정정 지연', '수용된 위험', '완화된Fortify 취약성 통합 위험'과 같은 소스 상태는 인스턴스에 위험 수락됨 또는 완화 통제의 하위 상태가 있는 '지연됨' 상태에 매핑됩니다.

이러한 통합에 대한 구성 페이지에는 다음 옵션이 있습니다.

옵션	확인란 선택됨	설명
다음에서 예외 관리 ServiceNow	Y(기본값)	이 옵션을 선택한 상태로 두면 AVI 레코드에서 예외를 요청해야 합니다. 지연됨 상태로 표시된 임포트된 AVI는 예외 관리 워크플로우를 ServiceNow 통해 분류됩니다. 일반적으로 지연됨 상태에 매핑되는 소스 상태가 있는 AVI는 열림 상태의 대상 환자 분류 상태에 매핑됩니다.
	N	이 확인란을 비활성화하면 스캐너에서 임포트한 소스 상태가 유지됩니다. 이러한 AVI는 대상 상태에지연됨으로 매핑되고 인스턴스의 대상 이유 상태에 매핑됩니다. 대상 분류 상태 및 대상 분류 이유 상태에 매핑되지 않으므로 예외 워크플로우에 의해 분류되지 않습니다. 기록이 이미 대상 지연 상태이므로 AVI 기록에서 예외 요청 UI 작업을 사용할 수 없습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

긍정 오류 사용 케이스

예를 들어 긍정 Veracode Vulnerability Integration 오류의 경우, 긍정 오류 또는 잠재적 긍정 오류와 같은 소스 상태는 하위 상태가 긍정 오류인 종결된 대상 상태에 매핑됩니다.

옵션	확인란 선택됨	설명
에서 긍정 오류 관리 ServiceNow	Y(기본값)	이 옵션을 선택한 상태로 두면 AVI 기록에서 긍정 오류를 요청해야 합니다. 긍정 오류 또는 잠재적 긍정 오류 상태로 표시된 임포트된 AVI는 예외 관리 워크플로우를 ServiceNow 통해 분류됩니다. 일반적으로 종결 대상 상태에 매핑되는 소스 상태가 있는 AVI는 열림의 대상 분류 상태에 매핑됩니다. 가양성 UI 작업은 AVI 기록에서 사용할 수 있습니다.
	N	이 확인란을 비활성화하면 스캐너에서 임포트한 소스 상태가 유지됩니다. 이러한 AVI는 인스턴스에서 대상 상태에종결 됨으로 매핑되고 대상 이유 상태는 긍정 오류로 매핑됩니다. 긍정 오류 워크플로우에 의해 분류되지 않습니다. 기록이 이미 대상 종결 상태이므로 AVI 기록에서 긍정 오류 UI 작업을 사용할 수 없습니다.

애플리케이션 취약성 대응 참조

에서 사용되는 용어는 애플리케이션 취약성 대응다음과 같습니다.

애플리케이션 취약한 항목(AVI)

회사 환경에서 취약성 항목과 잠재적으로 취약한 애플리케이션의 쌍입니다.

할당 규칙

정의된 기준에 따라 AVI를 할당하는 데 사용되는 규칙입니다.

CPE(공통 플랫폼 열거형)

정보 기술 시스템, 소프트웨어 및 패키지에 대한 NIST NVD의 구조적 명명 체계입니다.

CVE(일반적인 취약성 및 노출)

공개적으로 알려진 정보 보안 취약성 및 노출 사전입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

CWE(일반적인 약점 열거)

커뮤니티에서 개발한 소프트웨어 약점 유형 목록입니다.

통합

취약성 데이터를 검색하기 위해 CWE 또는 외부 공급업체 시스템에서 Veracode보고서 데이터를 끌어오는 예약된 작업입니다.

주:
에서 취약성 대응 NIST 국가 취약성 데이터베이스 통합이 활성화되고 구성된 경우 CWE에 대해 CVE 보강을 사용할 수 있지만 필수는 아닙니다. NIST 국가 취약성 데이터베이스 통합에 대한 자세한 내용은 문서를 참조하십시오 NVD 및 CWE 통합을 통해 데이터를 임포트하고 외부 공급업체 라이브러리를 관리합니다.

NVD(국가 취약성 데이터베이스)

SCAP(Security Content Automation Protocol)를 사용하여 표시되는 표준 기반 취약성 관리 데이터의 미국 정부 리포지토리입니다.

정정 대상 규칙

정의된 기준에 따라 정정할 AVI 대상 날짜를 할당하는 데 사용되는 규칙입니다.

취약성 계산기

정의된 기준에 따라 애플리케이션 취약성의 우선순위를 지정하고 분류하는 데 사용되는 계산기입니다.

에 대한 예외 규칙 예 애플리케이션 취약성 대응

예외 규칙에 대한 알려진 취약성을 기반으로 하는 예시 규칙입니다.

필드	설명
이름	목적을 식별하고 규칙을 쉽게 찾을 수 있는 고유한 이름입니다(예: Veracode-1 cwe-22 exception).
상태	읽기 전용: 초안
유효 기간(시작)	AVI를 연기하기 위해 이 규칙이 활성화되는 날짜입니다.
실행 순서	각 예외 규칙에 대한 고유한 순서입니다. 낮은 값이 높은 값보다 우선합니다.
유효 기간(종료)	정정 작업에서 새 VI 수락을 중지한 날짜입니다.
지연 기한	정정 작업 및 AVI가 지연되는 날짜입니다. 이 날짜에 AVUL이 종결되고 모든 AVI가 작업에서 벗어나 다시 열립니다. 그룹 규칙은 이러한 AVI에 다시 적용됩니다.
이유	이 예외 규칙을 생성하는 이유입니다. 목록에서 하나를 선택합니다(예: 수정 사용 불가능).
할당 그룹	지연된 VI를 추적하기 위해 할당된 그룹(예: APP 보안 관리자).
추가 정보	요청자가 승인자에게 제공하려는 추가 정보입니다. 이 정보는 정정 작업의 설명 필드에 채워집니다. 이 예에서는 ###(Veracode-1-22)## AVI# #####.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
조건	이 규칙과 일치하는 AVI를 지정하는 필터 조건입니다. 이 예에서 `####` Veracode-1-22`###`.
기존 데이터에서 실행	이 규칙을 처음 실행할 때 기존 데이터에 대해 이 규칙을 실행할 수 있도록 하는 옵션입니다. 이 옵션을 비활성화하면 새 데이터로 시작하는 예약된 작업에 ***Associate existing AVIs with Auto Exception Rule*** 따라 규칙이 매일 실행됩니다. 기존 데이터에서 실행 옵션을 활성화하면 예약된 작업이 유효 기간(시작) 날짜에 기존 데이터에 대해 한 번 실행됩니다.

애플리케이션 취약성 대응 제품 뷰

AVR(Application Vulnerability Response) 제품은 애플리케이션 보안 테스트 도구에서 탐지된 약점과 취약성을 수집하고 환경에 있는 모든 애플리케이션의 보안 상태를 이해할 수 있는 단일 창을 제공합니다.

AVR을 사용하면 정정 워크플로우로 위험을 줄일 수 있습니다. 이 제품 뷰의 목적은 AVR 키 엔터티가 핵심 CSDM 프레임워크에서 작동하는 방식을 이해하는 데 도움을 주는 것입니다.

업데이트된 용어

AVR v19.0부터 다음 키 테이블 및 열 이름이 업데이트되었습니다. 따라서 설명서에서 이전 이름과 최신 이름 모두에 대한 참조를 볼 수 있습니다.

AVR에 대한 용어, 테이블 및 필드 이름 목록이 업데이트되었습니다.

AVR v19.0 이전	**AVR** v19.0부터
CI 조회 규칙	조회 규칙
CI 조회 규칙 양식	조회 규칙 양식
CI 일치 규칙	일치 규칙
테이블에서 검색	CI 테이블에서 검색
필드 검색	CI 필드 검색
애플리케이션 릴리스	검색된 애플리케이션
애플리케이션 릴리스 테이블	검색된 애플리케이션 테이블
비즈니스 중요도	소스 비즈니스 중요도

필수 구성요소

다음 애플리케이션의 최신 버전을 설치합니다.

- Security Support Common
- 취약성 대응
- 보안 통합 프레임워크

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 보안 지원 오케스트레이션
- Veracode 및 Fortify와 같은 스캐너 통합

AVR 및 CSDM 4.0

AVR v19.0 이전에는 애플리케이션 취약성이 수집될 때 CI 조회 규칙을 사용하여 취약성이 수집된 애플리케이션을 스캔된 애플리케이션(sn_vul_app_scanned_application)에 대해 조회했습니다. 애플리케이션 이름 기록이 없으면 항목이 만들어집니다.

AVR v19.0부터 CSDM 4.0 프레임워크에 맞추기 위해 스캔한 애플리케이션 테이블 대신 제품 모델 테이블이 사용됩니다. 애플리케이션에 버전이 있는 경우 조회는 소프트웨어 모델 테이블을 대상으로 합니다. 버전이 없는 경우 조회는 애플리케이션 모델 테이블을 대상으로 합니다. 애플리케이션 모델과 소프트웨어 모델은 모두 제품 모델 테이블의 하위 테이블이며 CMDB의 기초 테이블입니다. 다음 스크린샷에서는 제품 모델에 대해 설명합니다.

시스템 속성

CSDM 4.0 제품 모델 기반 조회 프로세스를 사용하려면 시스템 속성을 *sn_vul.use_product_modeltrue*로 설정합니다.

시스템 속성 고려 사항

시스템 속성 이름	시스템 속성 값	조회 대상 값	고려 사항
sn_vul.use_product_model	예	값 선택 제품 모델	신규 사용자는 CSDM 4.0 프레임워크의 제품 모델 조회 규칙을 사용하려면 제품 모델 값을 선택해야 합니다.
	아니오	값 선택 구성 항목	기존 사용자는 CI 조회 프로세스와 기존 **CI** 조회 규칙을 계속 사용할 수 있습니다.

주:
조회 대상 값을 설정하려면 조회 규칙 페이지 **> [AVR** 통합 조회 규칙〕 〉 조회 대상 필드로 이동합니다.

AVR의 조회 규칙

CSDM 4.0 프레임워크에서는 CI 조회 규칙 대신 제품 모델 기반 조회 규칙을 사용하여 각 제품 모델 클래스에 항목을 생성합니다. 스크립트와 마찬가지로 CSDM 4.0 모델의 프레임워크 내에서 조회 규칙을 정의할 수 있습니다.

AVR v19.0부터 조회 규칙을 생성할 때 조회 대상 필드를 사용하여 구성 항목 또는 제품 모델 접근 방식을 사용할지 여부를 정의해야 합니다. 자세한 내용은 CI 조회 규칙 생성 문서를 참조하십시오.

검색된 애플리케이션

다음으로 이동 모두 〉 검색된 애플리케이션. 검색된 애플리케이션 테이블에는 스캐너에서 수집된 애플리케이션이 표시됩니다. 시스템 속성이 *sn_vul.use_product_model* 로 설정된 *true*경우 애플리케이션에 해당하는 제품 모델을 볼 수 있습니다.

AVR 고려 사항

중복 **CI** 또는 제품 모델 기록의 존재

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

조회 프로세스에 대해 시스템 속성이 *sn_vul.use_product_model* 올바르게 구성되었는지 확인합니다. 조회 규칙 양식을 구성하는 동안 구성 항목 또는 제품 모델을 조회 대상으로 선택해야 합니다.

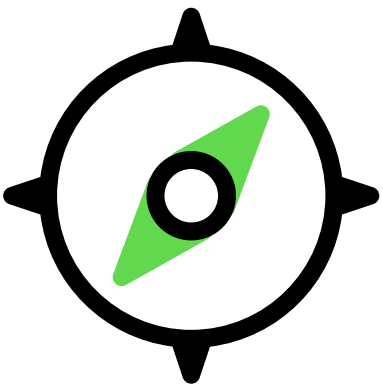
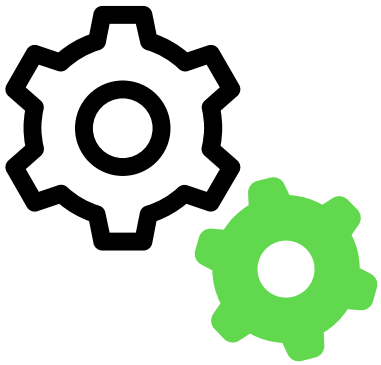
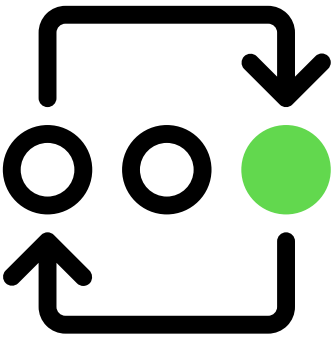
컨테이너 취약성 대응

애플리케이션은 ServiceNow# 컨테이너 취약성 대응 컨테이너 취약한 항목 (CVIT) 을 임포트하고 규칙에 따라 컨테이너 취약성을 정정할 수 있습니다. 취약성 데이터는 NVD(국가 취약성 데이터베이스) 또는 타사 통합과 같은 내부 및 외부 소스에서 끌어옵니다.

스토어에서 앱 요청

ServiceNow Store 웹 사이트를 방문하면 사용 가능한 모든 앱을 확인하고 스토어에 요청을 제출하는 방법에 대한 정보를 참조할 수 있습니다. 출시된 모든 앱의 누적 릴리스 정보는 ServiceNow Store 버전 기록 릴리스 정보를 참조하십시오.

컨테이너 취약성 대응

탐색	구성	통합
		
Container Vulnerability Response 개념 및 기능에 대해 알아봅니다.	컨테이너 취약성 대응을 구성합니다.	다른 애플리케이션과 통합하여 컨테이너 취약성 대응을 확장합니다.

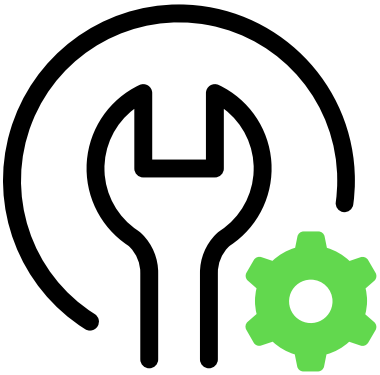
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

컨테이너 취약성 대응

Vulnerability Response
작업 공간 사용

취약성 관리자, IT 정정 및 취약성 평가 작업 공간에서 CVIT를 모니터링, 관리 및 정정하는 방법을 알아봅니다.

정정

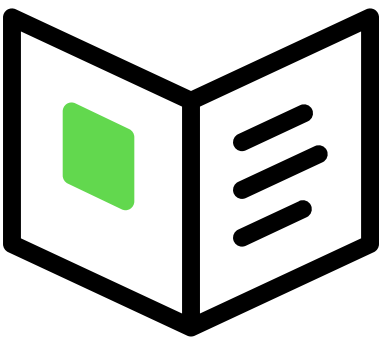


컨테이너 취약성을 정정하는 방법을 알아봅니다.

분석 및 보고

컨테이너 취약성 대응 분석 보기

참조



필드, 테이블 및 속성과 같은 컨테이너 취약성 대응 구성요소에 대한 상세 정보를 얻습니다.

이점

컨테이너 취약성 대응 애플리케이션은 다음과 같은 주요 이점을 제공합니다.

- Palo Alto Networks의 Prisma Cloud Compute 같은 외부 공급업체 컨테이너 보안 제품과 통합됩니다.
- 런타임에 배포된 이미지의 취약성 데이터를 임포트하고 런타임 컨텍스트 정보(호스트, Kubernetes 클러스터, 서비스 및 네임스페이스)로 취약성 데이터를 보강합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- Kubernetes 디스커버리 사용 ServiceNow 의 구성 관리 데이터베이스(CMDB) 관련 Kubernetes 엔터티에 취약성에서 생성된 참조 목록을 제공합니다.
- 취약성 및 정정 추세에 대한 인사이트를 제공하는 포괄적인 보고 대시보드를 제공합니다.

주요 기능

컨테이너 취약성 대응 애플리케이션은 컨테이너에서 감지된 취약성을 관리합니다. 다음과 같은 기능을 제공합니다.

- 컨테이너를 실행하는 대신 CVIT에서 소스 Docker 이미지를 가리킵니다.
- 이미지, Kubernetes 클러스터, 네임스페이스 또는 서비스 수준에서 추적하도록 CVIT의 세분성을 구성합니다.
- 새 이미지 버전을 추적하여 수정된 취약성을 식별합니다. 이전 버전에서 보고된 취약성은 런타임에 새 이미지 버전이 배포될 때 자동으로 해결 ServiceNow 됩니다.
- 애플리케이션 이미지와 별도로 기본 이미지의 CVIT를 추적하여 독립적인 정정을 가능하게 합니다.
- 다단계 승인자 프로세스를 통해 검토할 수 있는 예외 요청 또는 긍정 오류 요청을 제기합니다.
- CVIT를 자동으로 연기하도록 예외 규칙을 정의합니다.

사용 사례

컨테이너는 오버헤드를 줄이고 이식성을 높이면서 여러 환경에서 애플리케이션을 배포하고 확장할 수 있는 좋은 방법입니다. 그러나 컨테이너 이미지의 취약성은 기본 호스트와 궁극적으로 이러한 이미지에서 컨테이너가 시작된 인프라에 위험을 초래할 수 있습니다. 컨테이너 이미지에서 취약성을 검사하는 컨테이너 보안 제품이 많이 있지만 취약성 수정과 관련된 몇 가지 고려 사항과 문제가 있습니다. 컨테이너 취약성 대응 는 컨테이너 이미지 취약성 정정과 관련된 다양한 문제 또는 사용 사례를 해결하는 데 도움이 될 수 있습니다. 모듈을 활용하는 방법을 살펴보십시오.컨테이너 취약성 대응

런타임 컨텍스트

컨테이너 이미지의 취약성은 애플리케이션 수명주기의 다음 스테이지에서 이미지를 검사하여 검색할 수 있습니다.

- 스테이지 1: CI/CD 파이프라인에서 이미지를 빌드하는 경우.
- 스테이지 2: 이미지가 레지스트리에 게시될 때
- 스테이지 3: 이미지가 런타임에 배포될 때

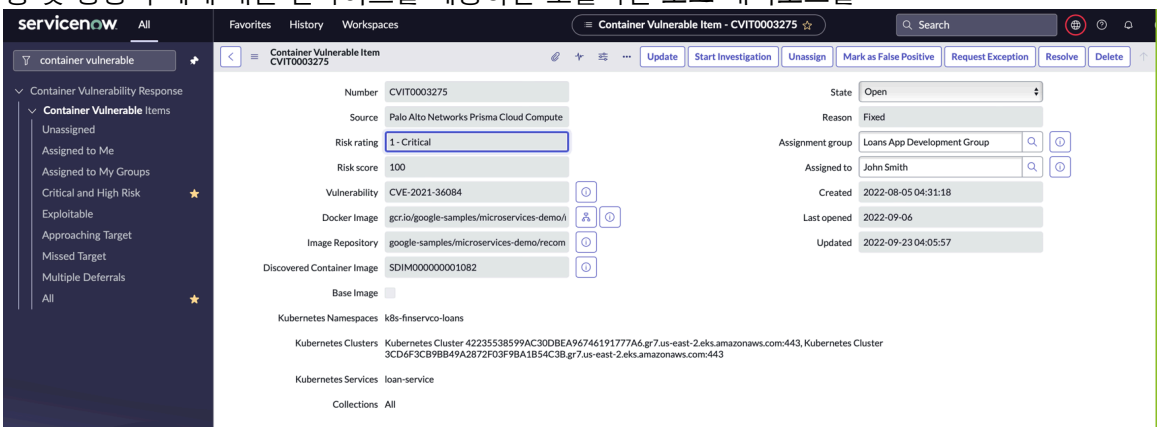
1단계와 2단계에서 가능한 한 빨리 취약성을 식별하는 것이 중요하지만 런타임 환경에 배포된 이미지를 검사하는 것도 똑같이 중요합니다. 다음과 같은 이점을 제공합니다.

- 게시된 새로운 CVE(Common Vulnerabilities and Exposures)를 식별합니다.
- 배포된 애플리케이션의 위험 태세에 대한 정확한 가시성을 제공합니다.
- 해결해야 하는 취약성의 우선순위 지정. 취약성으로 인해 영향을 받는 애플리케이션 서비스 또는 비즈니스 서비스와 관련된 런타임 컨텍스트는 우선순위 지정에 도움이 될 수 있습니다.

컨테이너 취약성 대응 에서 Prisma Cloud Compute Palo Alto Networks 와 같은 컨테이너 보안 제품과 통합하여 런타임에 배포된 이미지의 취약성 데이터를 끌어오고 이러한 컨테이너 이미지가 배포되는 호스트, Kubernetes 클러스터, 서비스 및 네임스페이스와 같은 런타임 컨텍스트 정보로 취약성 데이터를 보강합니다. Kubernetes 검색을 사용하는 ServiceNow 고객은 취약성에서 생성된 참조를 해당 구성 관리 데이터베이스(CMDB). 메타데이터를 ServiceNow 보강할 뿐만

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

아니라 취약성 및 정정 추세에 대한 인사이트를 제공하는 포괄적인 보고 대시보드를 제공합니다.



소유권 식별

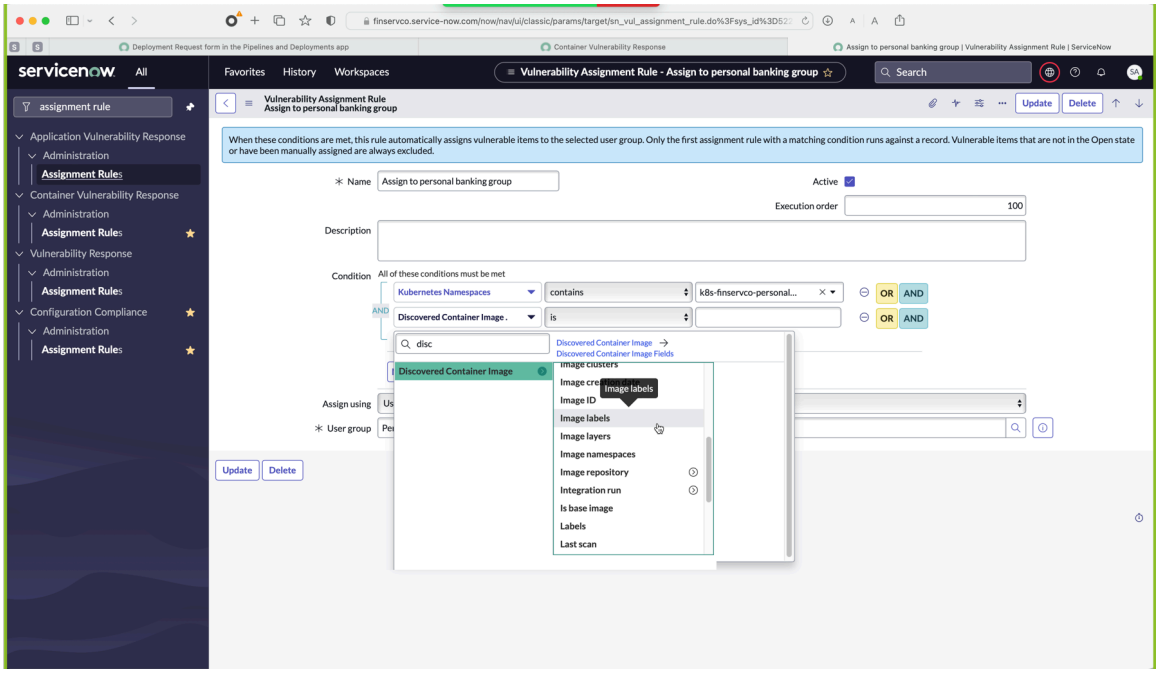
필수 구성 요소

- **Kubernetes** 메타데이터 및 참조: 컨테이너 취약성 대응 Kubernetes 메타데이터(네임스페이스, 클러스터 등) 및 항목 참조를 구성 관리 데이터베이스(CMDB) 채우려면 (ITOM)에서 Information Technology Operations Management Kubernetes 검색을 구현해야 합니다. Kubernetes 검색은 Docker 이미지, 실행 중인 Docker 컨테이너, 포드, Kubernetes 클러스터 등을 CMDB컨테이너 취약성 대응 . 이미지 ID를 기반으로 Docker CMDB 이미지를 식별한 다음, 관련 Kubernetes 엔터티를 식별하고 취약한 항목에서 해당 엔터티에 대한 참조를 채웁니다.
- 클라우드 메타데이터 및 **Docker** 이미지 레이블: 컨테이너 취약성 대응 Docker 이미지 레이블, 클라우드 계정 ID, 이미지가 배포되는 지역도 채웁니다. 이 데이터는 취약한 항목과 연결된 "탐색한 컨테이너 이미지" 기록에 유지됩니다. 이 데이터를 채우기 위한 필수 조건은 없습니다. 컨테이너 취약성 대응 는 컨테이너 보안 제품(예: Palo Alto Prisma Cloud Compute)에서 반환한 데이터를 사용하여 이러한 항목을 채웁니다.

컨테이너 이미지의 취약성을 패치하기 위한 소유권은 조직마다 다를 수 있습니다. 이 정보는 다른 위치에서 캡처될 수 있습니다. 일부 조직에서는 특정 컨테이너 이미지를 소유하는 애플리케이션 팀을 식별하는 방법으로 Docker 이미지 레이블을 사용하는 반면, 다른 조직에서는 Kubernetes 네임스페이스 또는 컨테이너 이미지가 배포된 클라우드 계정을 사용하여 올바른 소유자를 식별할 수 있습니다.

컨테이너 취약성 대응 은 '할당 규칙' 모듈에서 Docker 이미지 레이블, Kubernetes 클러스터/서비스/네임스페이스 메타데이터 또는 클라우드 계정 메타데이터(클라우드 계정 ID, 지역, 제공자 등)를 캡처 및 사용하고 이미지 또는 런타임 환경의 메타데이터를 기반으로 올바른 애플리케이션 팀에 취약성을 자동으로 할당하는 데 필요한 데이터 모델 요소를 제공합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



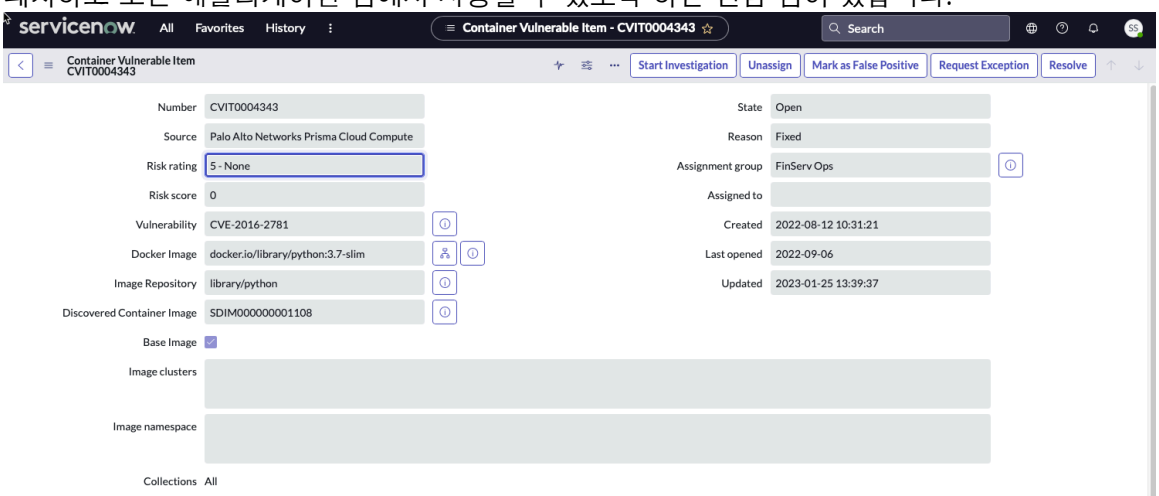
기본 이미지의 취약성 추적

필수 구성 요소

"기본 이미지" 속성을 채우 컨테이너 취약성 대응려면 기본 이미지를 콘솔에서 명시적으로 Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute 구성해야 합니다. Prisma Cloud에서 기본 이미지를 구성하는 방법에 대한 자세한 내용은 https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin - compute/vulnerability_management/base_images를 참조하십시오.

컨테이너 취약성 대응 다른 팀에 할당할 수 있도록 기본 계층에 대한 별도의 취약성 기록을 생성할 수 있습니다.

컨테이너 이미지의 다른 계층에서 검색된 취약성에서 Alpine과 같은 기본 OS 이미지에서 식별된 취약성을 추적합니다. 많은 조직에는 기본 OS 이미지를 패치하고 모든 애플리케이션 팀에서 사용할 수 있도록 하는 전담 팀이 있습니다.

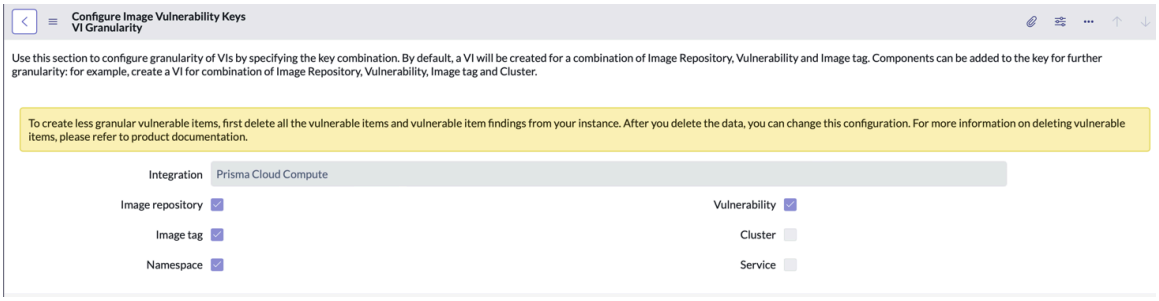


취약한 항목에 대한 세분성 정의

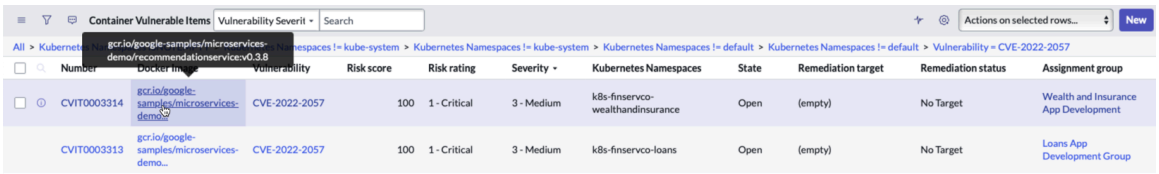
필수 구성 요소

다음으로 이동하여 CVIT의 세분성을 구성합니다. 모두 〉 컨테이너 취약성 대응 〉 관리 〉 **VI** 세분성 구성.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



기본적으로 CVE 및 Docker 이미지 버전(참조 + 태그)의 모든 고유한 조합에 대해 취약한 항목이 생성됩니다. 그러나 몇 개의 Docker 이미지는 둘 이상의 Kubernetes 네임스페이스에 배포될 수 있으며 각 네임스페이스는 다른 비즈니스 단위 또는 팀이 소유할 수 있습니다. 각 팀은 취약성을 수정하기 위해 새 버전의 컨테이너 이미지를 롤아웃하기 위해 고유한 주기를 따를 수 있습니다. 이 시나리오를 수용하기 위해 다음을 컨테이너 취약성 대응 수행하여 취약한 항목에 대한 세분성을 정의할 수 있습니다. Docker 이미지 버전 및 취약성의 모든 고유한 조합에 대해 각 Kubernetes 네임스페이스/클러스터/서비스에 대해 하나의 취약한 항목을 생성해야 하는지 여부입니다.



이 예에서는 동일한 Docker 이미지 및 CVE 조합에 대해 생성된 두 개의 취약한 항목을 볼 수 있습니다. 하나는 Kubernetes 네임스페이스 'k8s-finservco-loans'에 대한 것이고 다른 하나는 'k8s-finservco-wealthandinsurance'에 대한 것입니다.

태그 기반 서비스 식별을 사용하여 영향을 받는 서비스 식별

필수 구성 요소

- 애플리케이션에서 다양한 서비스를 식별하고 해당 서비스를 나타내는 태그/키-값 쌍을 정의합니다.
- 해당 태그 또는 레이블을 사용하여 Docker 이미지 및 Kubernetes 포드를 배포합니다.
- ITOM Kubernetes 디스커버리 배포 올바른 태그로 '태그 기반 서비스'를 정의합니다.
- ITOM Kubernetes 디스커버리 배포
- 올바른 태그 또는 키-값 쌍을 사용하여 "태그 기반 서비스"를 정의합니다.
- 를 사용하여 취약성 데이터 ServiceNow 임포트 컨테이너 취약성 대응

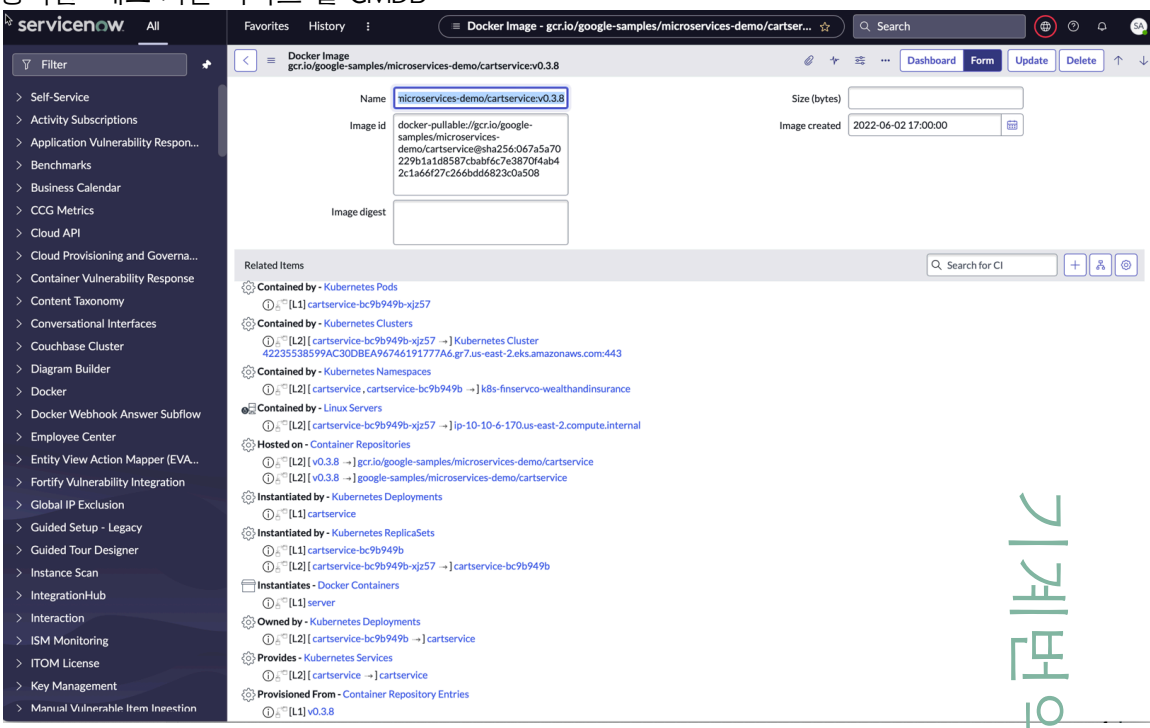
취약한 항목에 대한 위험 계산은 CI(Docker 이미지) 및 에서 관련 서비스의 CMDB중요도를 확인하여 수행할 수 있습니다. 그러나 영향을 받는 서비스를 보다 쉽게 식별할 수 있도록 에서는 컨테이너 취약성 대응 태그 기반 서비스 식별을 제공합니다.

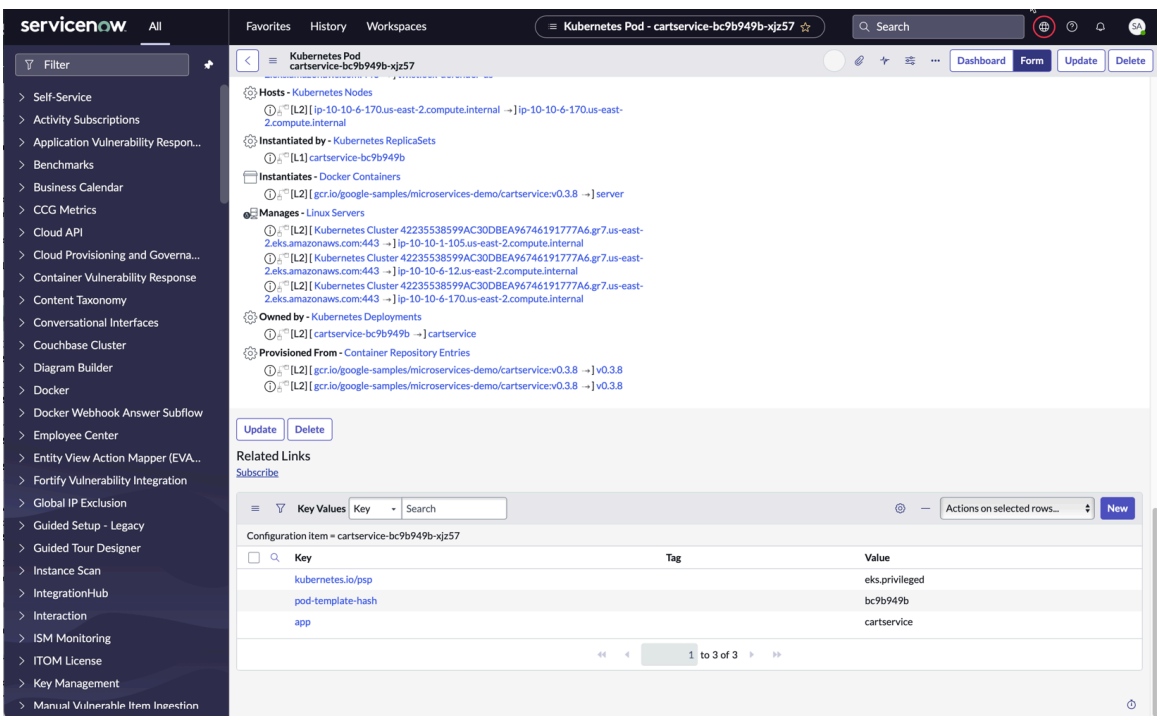
Kubernetes 포드 또는 엔티티가 의 ServiceNow"태그 기반 서비스"에 정의된 키 값과 일치하는 키 값 또는 레이블과 함께 게시되면 는 컨테이너 취약성 대응 Docker 이미지와 영향을 받는 애플리케이션 서비스 간의 관계를 자동으로 설정하고 위험 계산에 해당 애플리케이션 서비스의 중요도를 사용합니다.

플로우는 다음과 같습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

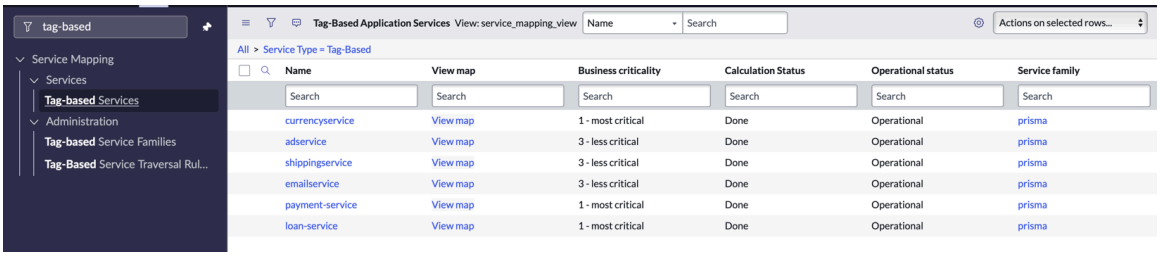
1. 컨테이너 취약성 대응 컨테이너 보안 제품에서 취약성 데이터를 임포트합니다.
2. 각 컨테이너 취약한 항목에 컨테이너 취약성 대응 대해 취약성이 있는 Docker 이미지를 CMDB 채웁니다.
3. 컨테이너 취약성 대응 그런 다음, Docker 이미지 레이블 또는 이 이미지가 배포된 Kubernetes 포드와 함께 게시된 레이블/키-값을 확인합니다. Kubernetes 디스커버리가 실행 중인 경우 이 CMDB 이미지를 사용할 수 있습니다.
4. 컨테이너 취약성 대응 그런 다음 동일한 일치하는 키-값 쌍이 정의된 "태그 기반 서비스"를 CMDB 검색합니다.

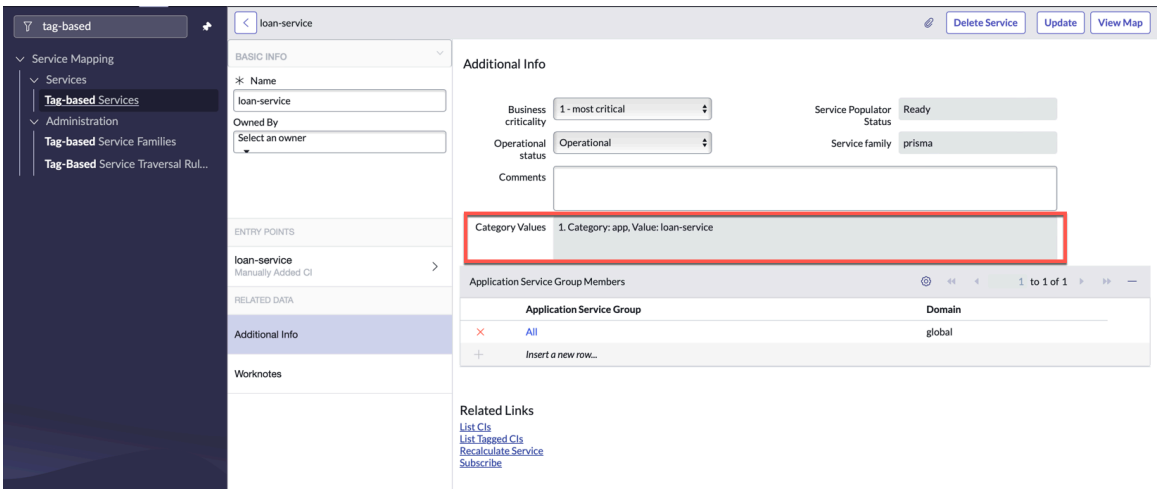




5. 컨테이너 취약성 대응 는 일치하는 "태그 기반 서비스"(있는 경우)의 "비즈니스 중요도"를 사용하여 컨테이너 취약한 항목의 위험을 계산합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

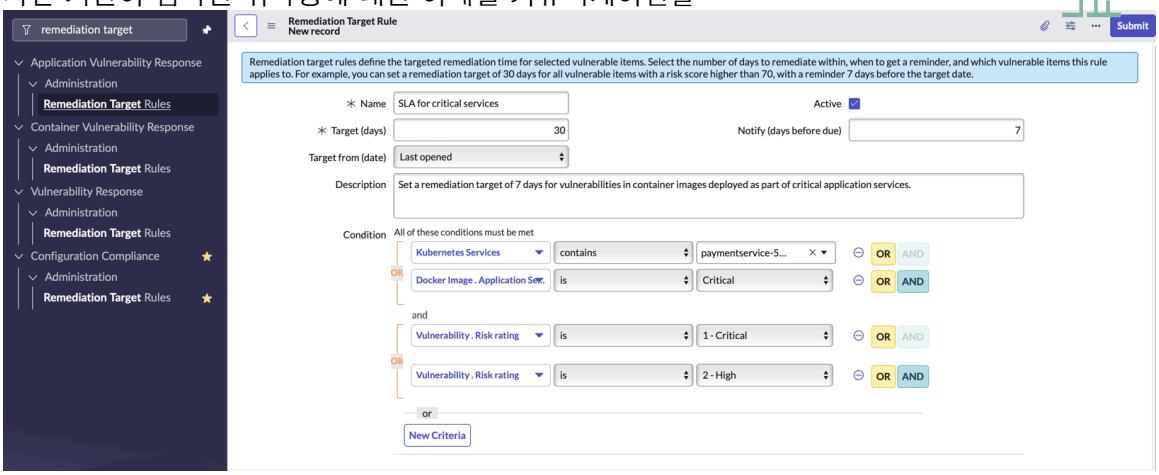




취약성 추적

정정 대상 설정

ServiceNow 를 사용하면 취약성 관리자가 컨테이너 이미지에서 발견된 취약성을 수정하기 위한 SLA(서비스 수준 계약)를 정의할 수 있도록 '정정 대상 규칙'을 정의할 수 있습니다. 정정 목표 날짜는 이미지 메타데이터 또는 취약성 정보에 대한 조건/기준을 기반으로 정의할 수 있습니다. 정정 소유자는 기한이 임박한 취약성에 대한 이메일 커뮤니케이션을 받습니다.



수정된 취약성 식별

호스트에 패치를 적용하여 해결할 수 있는 호스트 취약점과 달리 컨테이너 취약점은 패치가 불가능합니다. 이전 버전을 대체하려면 새 버전의 컨테이너 이미지를 생성하고 배포해야 합니다. 새 버전은 이전 버전과 달리 식별자(이미지 ID)가 다르기 때문에 이미 수정된 취약점을 추적하기가 어렵습니다.

ServiceNow 는 이전 버전의 컨테이너 이미지에서 보고되었지만 최신 버전의 이미지에서 해결된 취약성을 식별하고 해당 취약성을 자동으로 "종결/고정" 상태로

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

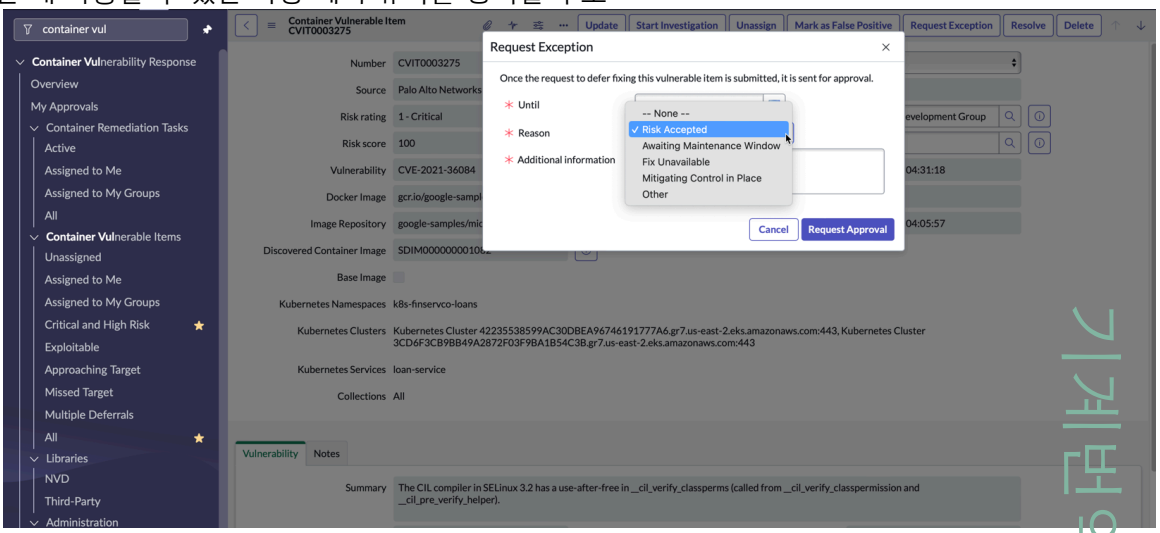
전환하여 보안 팀이 항상 최신 위험 태세에 대한 정확한 가시성을 확보할 수 있도록 합니다.

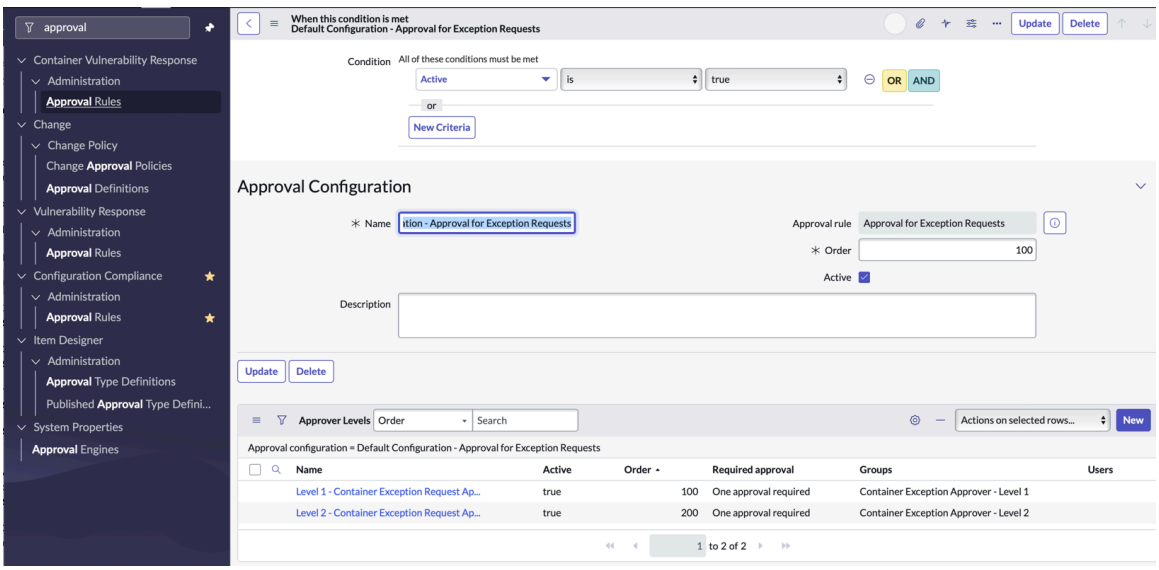
예외 관리

취약성에 대한 애플리케이션 팀 또는 정정 소유자는 다음과 같은 이유로 예외를 요청하는 기능이 필요할 수 있습니다.

- 완화 통제가 이미 시행 중입니다.
- 수용된 위험
- 수정 사항을 푸시하기 위해 유지관리 기간을 기다리는 중입니다.

ServiceNow 보안 관리자가 예외 요청에 대해 여러 수준의 승인자를 정의할 수 있습니다. 지정된 조건과 일치하는 취약성을 자동으로 지연시키는 데 사용할 수 있는 자동 예외 규칙을 정의할 수도 있습니다.





새로운 기능

의 새로운 기능과 변경된 Yokohama내용에 대한 자세한 내용은 릴리스 정보를 참조하십시오 Yokohama .

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기

- 인스턴스에 대한 보안 운영ServiceNow AI Platform 개요는 보안 운영 이해를 참조하십시오.
- 에서 다운로드할 수 있는 보안 운영 모든 애플리케이션에 대한 자세한 내용은 보안 운영 및 ServiceNow Store를 참조하십시오.ServiceNow Store

컨테이너 취약성 대응 탐색

애플리케이션이 CVIT(컨테이너 취약한 항목)를 컨테이너 취약성 대응 임포트합니다. 규칙에 따라 이 기능을 사용하면 컨테이너 취약성을 해결할 수 있습니다. 컨테이너 취약성 대응 는 별도의 구독을 통해 사용할 수 있습니다.

기존 애플리케이션과 달리 컨테이너는 모든 애플리케이션 소스 코드를 의존성과 함께 컨테이너 이미지라는 바이너리 파일로 패키징합니다. 이미지는 레지스트리에 게시되어 모든 플랫폼에서 이 이미지를 애플리케이션 또는 컨테이너 인스턴스로 실행하는 옵션을 제공합니다. 컨테이너 사전 배포 수명주기의 단계는 다음과 같습니다.

1. 컨테이너 이미지 작성: 컨테이너 이미지가 구성되고 소스 코드 또는 종속 라이브러리를 가리킵니다.
2. 컨테이너 이미지 구축
3. 컨테이너 이미지 게시: 컨테이너 이미지 파일이 레지스트리에 게시됩니다. 각 이미지에는 이미지 내용에 따라 고유한 ID가 있습니다. 이러한 이미지는 배포 후 모드에서 레지스트리에서 런타임 환경으로 끌어옵니다. 그런 다음 이미지는 프로덕션 환경의 호스트에서 컨테이너 인스턴스로 실행됩니다.

컨테이너 이미지 스캔

컨테이너 이미지는 배포 전후에 취약성을 검사할 수 있습니다. 배포 전 단계에서 컨테이너 이미지를 검사하면 즉각적인 주의가 필요하지 않을 수 있는 많은 취약성 경고를 받을 수 있습니다. 그러나 배포 후 단계에서 취약성을 검사하면 다음과 같은 더 큰 이점을 얻을 수 있습니다.

- 배포된 애플리케이션과 관련된 위험에 대한 가시성을 제공합니다.
- 프로덕션 환경의 이미지에 대해서만 포커스형 뷰를 제공합니다.
- 즉시 조치를 취해야 하는 취약성을 식별하고 우선순위를 지정합니다.
- 이미지의 메타데이터를 기반으로 취약성을 그룹화하고 할당합니다. 예를 들어 이미지 리포지토리, 이미지 레이블 및 컨테이너 이미지와 관련된 기타 속성을 그룹화 및 할당 규칙에 사용할 수 있습니다.

각 컨테이너 이미지에는 다음과 같은 주요 구성요소가 있습니다.

- 컨테이너 또는 이미지 리포지토리: 지정된 리포지토리 또는 이름으로 Docker 이미지를 나타냅니다. 이미지의 모든 버전을 호스팅합니다.
- Docker 이미지: 빌드 Docker 이미지의 특정 버전을 나타냅니다.
- Docker 컨테이너: 실행 중인 Docker 이미지의 인스턴스를 나타냅니다. 각 버전에는 고유한 ID가 있으며 프로덕션 환경에서 실행되는 컨테이너의 여러 인스턴스가 있습니다.

컨테이너 취약성 대응 모듈

이 컨테이너 취약성 대응 모듈은 다음에 대한 상세 정보를 제공합니다.

컨테이너 취약한 항목

컨테이너 취약한 항목(CVIT)은 할당, 중요도, 악용 가능성 및 정정 상태를 기준으로 그룹화되고 나열됩니다.

라이브러리

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

NVD(국가 취약성 데이터베이스) 및 외부 공급업체 라이브러리에 액세스합니다. NVD 라이브러리는 취약성 항목 ID로 제한된 정보를 제공하지만 타사 라이브러리는 취약성 항목에 대한 대부분의 상세 정보를 제공합니다. NVD 화면의 정보는 NVD 통합이 트리거될 때만 채워집니다.

관리

관리 모듈은 취약한 항목의 할당 규칙, 정정 대상 규칙 및 컨테이너 취약성 통합에 대한 정보를 제공합니다. 또한 취약한 항목을 자동으로 종결해야 하는 기간을 구성할 수도 있습니다. VI 세분성 구성 섹션을 사용하여 키 조합을 지정하여 CVIT의 세분성을 구성할 수 있습니다. 기본적으로 CVIT는 이미지 리포지토리, 이미지 태그 및 취약성의 조합에 대해 생성됩니다. 추가 세분성을 위해 키에 추가 구성 요소를 추가할 수 있습니다. 예를 들어 이미지 리포지토리, 이미지 태그, 취약성 및 클러스터의 조합에 대해 CVIT를 생성할 수 있습니다.

사용 가능한 버전

릴리스 버전	릴리스 정보
컨테이너 취약성 대응 v2.1 컨테이너 취약성 대응 V2.06 컨테이너 취약성 대응 v2.0.4	Container Vulnerability Response 릴리스 정보 호환성 정보는 KB0856498 취약성 대응 호환성 매트릭스 및 릴리스 스키마 변경을 참조하십시오.

컨테이너 취약성 대응 정정 작업 및 컨테이너 취약한 항목 상태

컨테이너 취약성 대응 애플리케이션에서 상태 모델을 사용하여 언제든지 정정 작업의 상태를 볼 수 있습니다. 각 상태가 서로 어떻게 관련되고 영향을 미치는지 알면 컨테이너 취약한 항목(CVIT)을 정정하는 시기와 방법을 결정하는 데 도움이 됩니다.

정정 작업 상태

복잡한 사용 사례로 인해 컨테이너 취약한 항목이 정정 작업과 다른 상태가 되는 경우가 있습니다. 상태의 작동 방식을 이해하면 이 동작을 설명하는 데 도움이 되며, 정정 작업 생성 및 정정 작업 규칙 생성 또는 편집에 도움이 됩니다.

정정 작업에는 다음 다이어그램과 같이 여러 가지 가능한 상태가 있습니다.

컨테이너 취약성 대응 상태 플로우

주:

- 컨테이너 취약한 항목은 수동으로 닫을 수 없습니다.
- 각 작업 양식에는 작업의 표준 ServiceNow 인 팔로우 및 업데이트 버튼이 있습니다.

정정 작업 및 **CVIT** 상태 전환 및 선행 순서

정정 작업과 취약한 항목 상태는 서로 영향을 줄 수 있습니다. 대부분의 경우, 정정 작업 상태는 취약한 항목 상태를 업데이트하며, 그룹의 취약한 항목을 업데이트하는 데 우선순위가 가장 높은 작업 상태가 사용됩니다.

컨테이너 정정 작업의 생성부터 종결까지 전체 정정 프로세스 동안 다양한 상태를 통해 전환됩니다.

상태 우선순위는 다음과 같습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

종결됨 〉 연기됨 〉 해결 일시 〉 검토 중 〉 대기 중인 구현 〉 조사 중 〉 오픈

상태 전환은 지연, 오픈, 종결 등 다양한 작업을 수행할 때 발생합니다.

특정 상태의 컨테이너 업데이트 적용 작업에서 수행할 수 있는 작업은 호스트 업데이트 적용 작업의 작업과 유사합니다. 따라서 자세한 내용은 취약성 대응 정정 작업 상태 설명서의 및 상태 롤업 및 롤다운 시나리오취약성 대응 문서를 참조하십시오.

컨테이너 취약성 대응 구성

인스턴스에서 실행하기 컨테이너 취약성 대응ServiceNow AI Platform 전에 먼저 구성해야 합니다.

컨테이너용 **Vulnerability Response** 및 **Configuration Compliance** 설치

인스턴스에서 애플리케이션을 ServiceNow AI Platform 실행하려면 컨테이너용 Vulnerability Response 및 Configuration Compliance 먼저 권리를 얻고 에서 애플리케이션을 ServiceNow Store다운로드해야 합니다. 인스턴스에 애플리케이션을 ServiceNow AI Platform 설치하고 설정 도우미에서 몇 가지 설치 단계를 완료합니다.

시작하기 전에
설치하기 전에 다음 설정 검사 목록을 완료합니다. 이러한 설정 작업은 원활한 설치 및 구성을 위해 필요합니다.

주:
이 프로세스는 프로덕션 인스턴스에 다운로드된 애플리케이션에만 적용됩니다. 애플리케이션을 비프로덕션 또는 개발 인스턴스에 다운로드하는 경우에는 권리를 얻을 필요가 없습니다. 로 애플리케이션 활성화 ServiceNow Store계속 진행합니다.

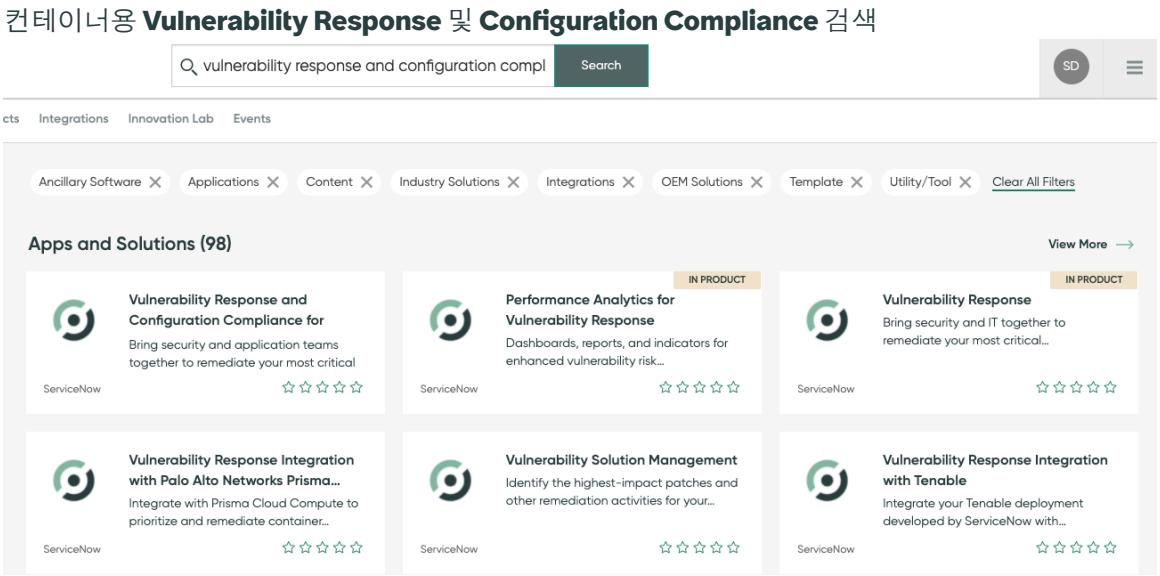
작업 설정	설명
애플리케이션이 설치되고 활성화되었는지 확인합니다.	활성화되었는지 확인하려면 다음으로 이동하십시오. 구독 관리 〉 구독 인스턴스에 있습니다. 목록에 조직이 구매한 구독이 표시됩니다. 애플리케이션이 설치 및 활성화되지 않은 경우 을 참조하십시오 취약성 대응 설치.
인스턴스에 필요한 ServiceNow 역할이 할당되어 있는지 확인합니다.	설치하려면 관리자 역할이 필요합니다. 아직 할당되지 않은 경우 시스템 관리자 〔admin〕는 취약성 관리자인 sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)〕 역할도 할당합니다.

필요한 역할: 관리자

프로시저

1. 권리를 얻고 애플리케이션을 다운로드하려면 컨테이너용 Vulnerability Response 및 Configuration Compliance 로 ServiceNow Store이동하십시오.
2. 페이지 오른쪽 상단에서 로그인을 클릭합니다.
3. 검색 창에 를 입력합니다 컨테이너용 Vulnerability Response 및 Configuration Compliance.
4. Apps and Solutions(앱 및 솔루션)에서 타일을 컨테이너용 Vulnerability Response 및 Configuration Compliance 클릭합니다.

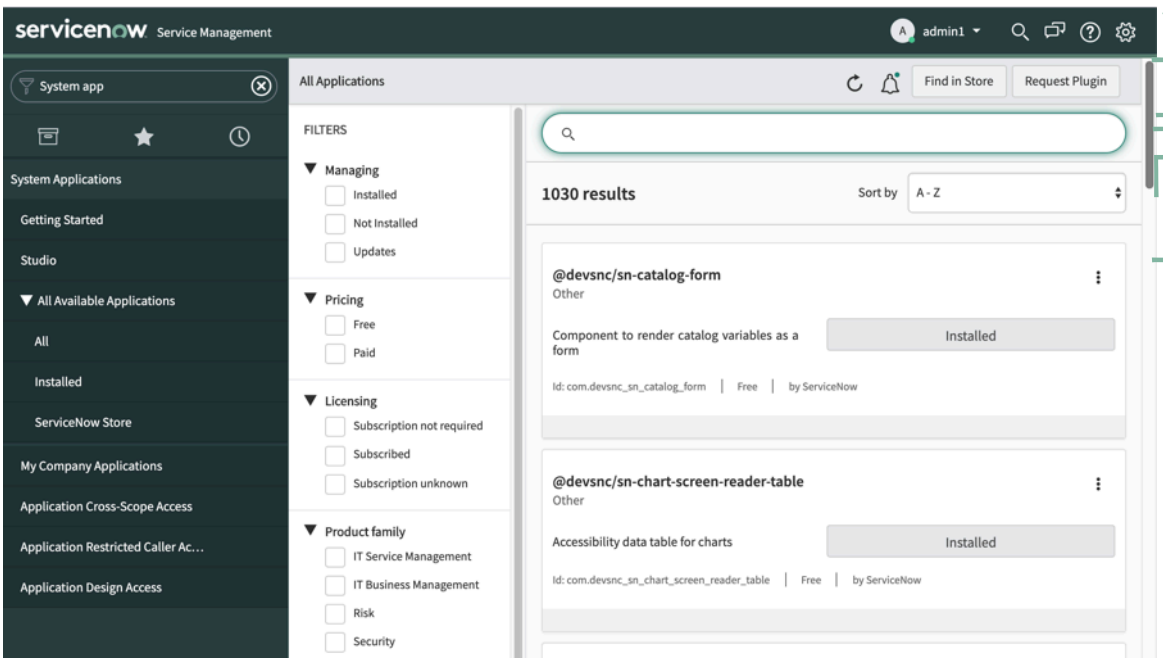
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



5. 설치 요청을 클릭합니다.

6. ServiceNow AI Platform 애플리케이션을 설치할 컨테이너용 Vulnerability Response 및 Configuration Compliance 인스턴스에 로그인합니다.

7. 다음으로 이동 시스템 애플리케이션 〉 모든 사용 가능 애플리케이션 〉 모두.



8. 나열된 응용 프로그램에서 응용 프로그램을 찾아 컨테이너용 Vulnerability Response 및 Configuration Compliance 목록에서 버전을 선택하고 설치를 클릭합니다.
애플리케이션 설치 대화 상자가 표시됩니다. 설치된 모든 종속성이 표시됩니다.

9. 닫기를 클릭합니다.

이메일 알림 정의 컨테이너 취약성 대응

가양성 요청 승인 및 거부와 같은 중요한 업데이트 및 활동에 대한 유용한 정보를 공유하도록 이메일 알림을 설정합니다. 이메일 알림을 생성하려면 알림 전송 시기, 받는 사람 및 포함된 항목 지정이 포함됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 이메일 템플릿.
2. 새로 만들기를 선택합니다.

   이메일 알림 생성에 대한 자세한 지침은 문서를 참조하십시오 Create an email notification .

결과
v21.0 of 취약성 대응부터 수신자가 이메일 알림의 링크를 클릭하면 역할에 따라 기록이 OR IT 정정 작업 공간 에서 취약성 관리자 작업 공간 열립니다.

- 역할이 있는 사용자(sn_vul_container.vulnerability_analyst 또는 sn_vul_container.vulnerability_admin)에 대해 링크가 열립니다취약성 관리자 작업 공간.
- 역할이 있는 사용자에게 sn_vul_container.remediation_owner에서 링크가 열립니다IT 정정 작업 공간.

수신자에게 위의 역할이 없는 경우 이메일 알림의 링크가 클래식 UI에서 열립니다.

정정 대상 알림 만들기 또는 편집

취약성 관리자는 정정 대상 알림을 편집하거나 새로 추가하여 알림 전송 시기, 알림 수신자, 알림의 내용을 지정할 수 있습니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 알림.
2. 정정 대상 알림 기록을 선택하거나 새로 만들기를 선택합니다.
3. 양식의 필드에 적절히 입력합니다.
   양식 필드에 대한 자세한 내용은 Create an email notification 문서를 참조하십시오.
4. 메시지를 보려면 알림 미리 보기를 선택합니다.

결과
v21.0 of 취약성 대응부터 수신자가 이메일 알림의 링크를 클릭하면 역할에 따라 기록이 OR IT 정정 작업 공간 에서 취약성 관리자 작업 공간 열립니다.

- 역할이 있는 사용자(sn_vul_container.vulnerability_analyst 또는 sn_vul_container.vulnerability_admin)에 대해 링크에서 열립니다취약성 관리자 작업 공간.
- 역할이 있는 사용자에게 sn_vul_container.remediation_owner 링크가 열립니다IT 정정 작업 공간.

수신자에게 위의 역할이 없는 경우 이메일 알림의 링크가 클래식 UI에서 열립니다.

에 대한 예외 관리 구성 컨테이너 취약성 대응

모듈을 사용하여 컨테이너 취약성 대응 요청된 예외의 기간을 제한하고 예외 또는 긍정 오류 요청에 질문서를 추가합니다. 기본적으로, 예외를 설정하면 모듈을 사용하여 요청됩니다 ServiceNow# 컨테이너 취약성 대응 . 통합을 사용하여 예외를 요청할 수도 있습니다 GRC: 정책 및 준수 관리 .

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_vul_container.manage_exception_configuration

이 태스크 정보
가 활성화된 경우 컨테이너 취약성 대응 예외를 요청할 수 있는 기간을 제한할 수 있습니다. 마찬가지로 모듈이 설치되어 있으면 GRC: 정책 및 준수 관리 구성 화면에서 선택할 GRC: 정책 및 준수 관리 수 있습니다. 이 옵션을 사용하면 에서 정책 및 제어 목표를 GRC지정하는 예외를 요청할 수 있습니다.

질문서를 추가하면 예외 또는 긍정 오류 요청을 제기하는 사람에게 전송됩니다. 기본 질문서를 사용하거나 요구 사항에 따라 만들 수 있습니다. 입니다.

예외 승인자가 예외를 요청하는 이유를 이해하는 것이 좋습니다.

프로시저

1. 다음으로 이동 모두 〉 컨테이너 취약성 대응 〉 관리 〉 예외 관리.
2. 예외 관리 구성 양식의 다음을 사용하여 예외 관리 목록에서 옵션을 선택하여 예외를 관리할 방법을 선택합니다.
   또는 GRC: 정책 및 준수 관리를 선택할 취약성 대응 수 있습니다.
3. 옵션을 선택한 취약성 대응 경우 다음 정보를 입력합니다.

취약성 대응 필드

필드	설명
지속 시간	예외를 요청할 수 있는 기간입니다.
단위	지정된 기간의 시간 단위입니다.
긍정 오류로 표시하려면 질문서 사용	제기 중인 긍정 오류 요청에 질문서를 추가하는 옵션입니다.
예외를 요청하려면 질문서 사용	제기 중인 예외 요청에 질문서를 추가하는 옵션입니다.
예외를 요청하기 위한 질문서	예외를 요청하기 위해 선택한 질문서가 표시됩니다. 예외 질문서가 기본적으로 표시됩니다.

주:
을 선택하면 GRC: 정책 및 준수 관리해당 플로우를 처리하면서 거버넌스, 리스크 및 컴플라이언스 기간 및 단위 필드가 사라집니다.

4. 저장을 선택합니다.

예외 관리에 대한 승인 규칙 구성

v15.0부터 취약성 대응 플로우 디자이너를 사용하여 예외 관리, 예외 규칙 및 긍정 오류 관리에 대한 예외 요청을 승인합니다. 처음 배포 취약성 대응 (VR)하는 경우 Flow Designer가 기본적으로 활성화됩니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin

이 태스크 정보
플로우 디자이너를 사용하려면 승인 규칙 모듈을 사용하여 규칙을 생성합니다. 이 모듈을 사용하여 다음의 각 예외 관리 워크플로우에 대한 승인 규칙을 구성할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 정정 작업에 대한 예외 요청
- 컨테이너 취약한 항목에 대한 예외 요청
- 예외 규칙
- 정정 작업에 대한 긍정 오류
- 컨테이너 취약한 항목에 대한 가양성

규칙 내에 여러 수준의 승인을 포함하는 조건을 정의할 수도 있습니다. Flow Designer는 이 모듈에서 생성된 규칙을 자동으로 상속하고 일치하는 승인 워크플로우를 처리합니다.

프로시저

1. 다음으로 이동 모두 〉 컨테이너 취약성 대응 〉 관리 〉 승인 규칙.
2. 승인 규칙 페이지에서 승인 규칙을 설정할 그룹을 선택합니다.
3. 양식에서 필드를 채웁니다.

승인 규칙 양식

필드	설명
이름	승인 구성 이름입니다.
테이블	규칙이 적용되는 테이블입니다.
애플리케이션	기본값은 취약성 대응입니다.
규칙 유형	규칙 유형을 지정합니다. 예를 들어 예외 관리, 가양성 또는 예외 규칙이 있습니다.
활성	기본적으로 활성화되며, 승인 규칙이 사용 중임을 나타냅니다.
설명	승인 규칙에 대한 간단한 설명입니다.
승인 만료Y (일) v2.5 of 컨테이너 취약성 대응	승인자가 요청을 승인할 수 있을 때까지의 날짜입니다.
승인자에게 알림(일) v2.5 of 컨테이너 취약성 대응	승인자에게 조치를 취하라는 알림이 전송된 날짜입니다.

4. 업데이트를 선택합니다.
   승인 구성 탭에는 기본적으로 두 가지 수준의 승인자가 설정됩니다. 규칙을 선택하여 규칙 내의 다양한 사용 사례를 기반으로 조건을 정의할 수 있습니다. 자세한 내용은 승인 규칙에 대한 구성 생성 문서를 참조하십시오.

   주:
   각 구성 페이지에서 여러 승인 수준을 생성할 수 있습니다. 자세한 내용은 예외 관리에 대한 승인 수준 생성 문서를 참조하십시오.

Example:
다양한 사용 사례를 기반으로 서로 다른 구성 항목에서 발견된 동일한 취약성에 대해 서로 다른 승인 프로세스를 정의할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

컨테이너 취약성 대응에 대한 빠른 시작 테스트

업그레이드 적용 또는 애플리케이션 개발과 같이 구성 변경 후에도 컨테이너 취약성 대응 앱이 계속 작동하는지 확인합니다. 인스턴스별 데이터를 사용할 때 통과하도록 이러한 빠른 시작 테스트를 복사하여 사용자 지정합니다.

테스트 실행 속성은 프로덕션 시스템에서 테스트를 실행할 수 없도록 기본적으로 비활성화되어 있습니다. 개발, 테스트 및 기타 비프로덕션 인스턴스에 대해서만 테스트를 실행합니다. 데모 데이터 또는 데모 계정이 생성된 경우 비프로덕션 또는 프로덕션에서 인스턴스를 사용하기 전에 모든 데모 데이터를 제거해야 합니다. 에 대한 컨테이너 취약성 대응테스트 도구 모음 설정 및 실행에 대한 자세한 내용은 을 참조하십시오에 대해 Automated Test Framework(ATF) 테스트 도구 모음 실행 취약성 대응.

컨테이너 취약성 대응 빠른 시작 테스트를 하려면 컨테이너 취약성 대응 애플리케이션(sn_vul_container)을 활성화합니다.

컨테이너 취약성 대응 테스트

테스트	설명	릴리스 버전
CVR: 담당 규칙	담당 규칙의 예시 집합이 정정을 위해 할당 그룹에 컨테이너의 취약 항목을 성공적으로 자동 할당할 수 있는지 여부를 확인합니다.	Vancouver
CVR: 예외 규칙	테스트 예외 규칙입니다.	Vancouver
CVR: 오탐지 플로우로 표시	컨테이너 취약 항목에서 오탐지 플로우 표시가 작동하는지 테스트합니다.	Vancouver
CVR: 정정 대상 규칙	정정 대상 규칙을 만듭니다.	Vancouver
CVR: 요청 예외 플로우	요청 예외 플로우가 예상대로 작동하는지 여부를 테스트합니다.	Vancouver
CVR: 취약성 계산기	컨테이너 취약성 계산기를 테스트합니다.	Vancouver

관련 정보

빠른 시작 테스트

에 대해 **Automated Test Framework(ATF)** 테스트 도구 모음 실행 컨테이너 취약성 대응

애플리케이션을 설치하거나 업그레이드한 후 Automated Test Framework(ATF) 테스트 도구 모음을 컨테이너 취약성 대응 실행합니다.

시작하기 전에

설치가 성공적으로 되었고 인스턴스가 설계된 대로 작동하는지 확인합니다.

테스트 실행 속성은 프로덕션 시스템에서 테스트를 실행할 수 없도록 기본적으로 비활성화되어 있습니다. 개발, 테스트 및 기타 비프로덕션 인스턴스에 대해서만 테스트를 실행합니다. 데모 데이터 또는 데모 계정이 생성된 경우 비프로덕션 또는 프로덕션에서 인스턴스를 사용하기 전에 모든 데모 데이터를 제거해야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 테스트를 활성화하려면 다음 단계를 수행합니다.
  1. 다음으로 이동 모두 〉 **ATF(Automated Test Framework)** 〉 관리 〉 속성.
  2. 선택하지 않은 경우 테스트/테스트 도구 모음 실행 사용 확인란을 선택합니다.
  3. 저장을 클릭합니다.
  4. 헤더에서 범위가 컨테이너 취약성 대응 으로 설정되지 않았거나 헤더에 범위가 표시되지 않으면 설정 아이콘을 클릭합니다.
  5. 시스템 설정 창에서 개발자를 클릭합니다.
  6. 선택하지 않은 경우 헤더에 애플리케이션 선택기 표시를 클릭하고 창을 닫습니다.
  7. ### ### 옆에 표시되는 목록에서 해당 필드에 대해 컨테이너 취약성 대응을 클릭합니다.

필요한 역할: admin 또는 atf_test_admin

프로시저

1. 다음으로 이동 모두 〉 **ATF(Automated Test Framework)** 〉 테스트.
2. 패키지 목록에서 컨테이너에 대한 취약성 대응 및 구성 준수를 찾습니다.
3. 테스트를 선택하여 기록을 엽니다.
4. 열려 있는 기록에서 활성 확인란을 선택합니다.
5. 테스트 단계 관련 목록의 활성 열에서 true를 선택합니다.
6. 업데이트를 클릭합니다.
7. 테스트를 다시 열고 여기에서 테스트 및 테스트 도구 모음 실행 사용을 클릭합니다.
8. 테스트/테스트 도구 모음 속성 및 테스트 디버깅 속성을 활성화합니다.
9. 저장을 클릭합니다.
10. 테스트 실행 버튼이 표시되지 않으면 화면을 새로 고치고 기록을 다시 연 다음 테스트 실행을 클릭하여 테스트를 시작합니다.
    잠시 후 테스트 실행 대화 상자에 테스트가 성공적으로 완료되었다고 표시됩니다. 자세한 내용은 결과로 이동을 클릭합니다.

다음에 수행할 작업
축하합니다! 의 컨테이너 취약성 대응구성을 계속할 수 있습니다.

자동화된 테스트 및 자동화된 테스트, 테스트 도구 모음 및 자동화된 테스트 만들기에 대한 컨테이너 취약성 대응 자세한 내용은 Automated Test Framework(ATF) 를 참조하십시오.

다른 애플리케이션과 컨테이너 취약성 대응의 통합

다른 애플리케이션과 통합하여 기능을 컨테이너 취약성 대응 확장합니다.

컨테이너 취약성 대응 컨테이너 보안 제품과 통합하여 런타임에 배포된 이미지에 대한 취약성 데이터를 끌어옵니다. 그런 다음, 호스트, Kubernetes 클러스터, 서비스 및 이러한 컨테이너 이미지가 배포되는 네임스페이스와 같은 런타임 컨텍스트 정보로 취약성 데이터를 보강합니다. ServiceNow의 Kubernetes 디스커버리를 사용하면 취약성에서 생성된 참조를 사용자의 구성 관리 데이터베이스(CMDB). ServiceNow는 메타데이터를 보강할 뿐만 아니라 포괄적인 보고 대시보드를 제공하여 취약성 및 정정 추세에 대한 인사이트를 제공합니다.

컨테이너 취약성 대응는 다음 애플리케이션과의 통합을 제공합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute 통합
- Atlassian Jira 와의 통합 이해취약성 대응
- Tenable 취약성 통합 이해

- **중요사항:**
  취약성 관리자 작업 공간에서 목록 작업 및 양식 작업을 사용하여 Agile 문제를 수동으로 생성하여 CVIT 및 RT의 정정을 추적할 수 있습니다.

통합에 대한 추가 참고 사항

통합 실행 중에 여러 프로세스가 생성되고 데이터가 페이지 형식으로 수신됩니다. 각 프로세스에는 페이지에 첨부된 데이터가 있는 하나 이상의 임포트 큐 항목이 포함될 수 있습니다. 이러한 항목은 1시간의 시간 제한 내에 데이터를 처리해야 합니다. 그러나 페이로드 크기가 크면 처리 시간이 1시간을 초과하거나 중단되어 통합 시간 제한 오류가 발생할 수 있습니다. 통합은 시간 초과 오류에도 불구하고 데이터를 계속 처리합니다. 이러한 잘못된 통신을 피하기 위해 버전 2.1.2 컨테이너 취약성 대응부터 큐가 활성 상태이고 데이터를 처리하는지 여부를 나타내기 위해 타임스탬프(하트비트)가 주기적으로 전송됩니다. 임포트 큐 항목 페이지의 처리된 마지막 기록 필드는 임포트 큐가 생성하거나 업데이트하는 기록 수에 따라 업데이트됩니다. 임포트 큐 항목이 1시간의 시간 제한을 초과하는 경우, 시스템은 마지막으로 처리된 기록 필드를 검사하여 1시간보다 오래되었는지도 확인합니다. 이 경우 이는 임포트 큐 항목이 고착되었음을 나타내며 처리 시 더 이상의 지연을 방지하기 위해 시간 초과됩니다.

주:
마지막으로 처리된 기록 필드는 다음 시스템 속성에 정의된 내용에 따라 업데이트됩니다.

- *sn_sec_cmn.record_threshold_heartbeat*: 하트비트(타임스탬프)가 임포트 큐 항목으로 전송된 후 처리된 기록 수를 정의합니다.
- *sn_sec_cmn.maximum_heartbeat_delay*: 임포트 큐 항목을 시간 초과해야 하는 시간을 정의합니다.

Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute 통합

Prisma Cloud Compute 통합을 사용하면 컨테이너 이미지를 스캔하여 취약성을 탐지할 수 있습니다.

버전 23.0 취약성 대응부터 애플리케이션에서 를 Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute컨테이너 취약성 대응 사용하여 실행 중인 호스트의 취약성을 임포트할 수 있습니다. Prisma Host API를 사용하면 특정 호스트에 대한 포괄적인 취약성 정보를 검색할 수 있으며 특정 시간에 호스트 취약성에 대한 스냅샷도 제공합니다. 이 API를 사용하면 Prisma와 ServiceNow 인스턴스 간에 정기적인 동기화가 가능합니다. Prisma는 SaaS(Software as a Service) 및 온프레미스 솔루션으로 제공되므로 ServiceNow 인스턴스에서 Prisma API를 호출하려면 MID 서버를 사용해야 합니다.

버전 16.1 취약성 대응부터 애플리케이션을 사용하여 Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute컨테이너 취약성 대응 배포된 컨테이너에 대한 컨테이너 이미지 취약성 데이터를 임포트할 수 있습니다. 그런 다음 대시보드에서 취약성 및 취약한 항목에 대한 보고서를 볼 수 있습니다 취약성 대응 . 그런 다음 이러한 취약성의 우선 순위를 지정하고 수정할 수 있습니다.

Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute 제품과 ServiceNow AI Platform 인스턴스가 동일한 환경에 있지 않은 경우 MID 서버를 사용해야 합니다. 자세한 내용은 MID 서버 시스템 요구 사항을 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

통합 보기

의 일부인 통합을 볼 수 있습니다 Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute. 통합을 보려면 다음으로 이동합니다. 모두 〉 **Prisma Cloud Compute** 통합 〉 통합.

다음과 같은 통합을 사용할 수 있습니다.

실행 시퀀스	일정	통합	설명
1	매일	Prisma 클라우드 컴퓨팅 기본 이미지 통합	Prisma API에서 기본 이미지의 취약성을 검색하고 기본 이미지 취약성을 별도로 보고합니다. 또한 기본 이미지를 가리키는 이미지 결과 및 취약한 항목을 생성합니다.
2	매일	Prisma Cloud Compute 취약성 통합	컨테이너 취약성을 검색합니다. 찾기 결과 및 컨테이너 취약 항목(CVIT) 및 검색된 컨테이너 이미지를 생성합니다.
3	요청 시	Prisma Cloud Compute Container Counts 통합	기본이 아닌 각 이미지에 대한 컨테이너 수를 검색합니다.
4	매일	Prisma Cloud Compute 레지스트리 통합	Prisma 레지스트리 검사 및 수집 컨테이너 취약성 대응에서 얻은 정적 이미지 찾기를 검색합니다.

Prisma의 기본 이미지 구성

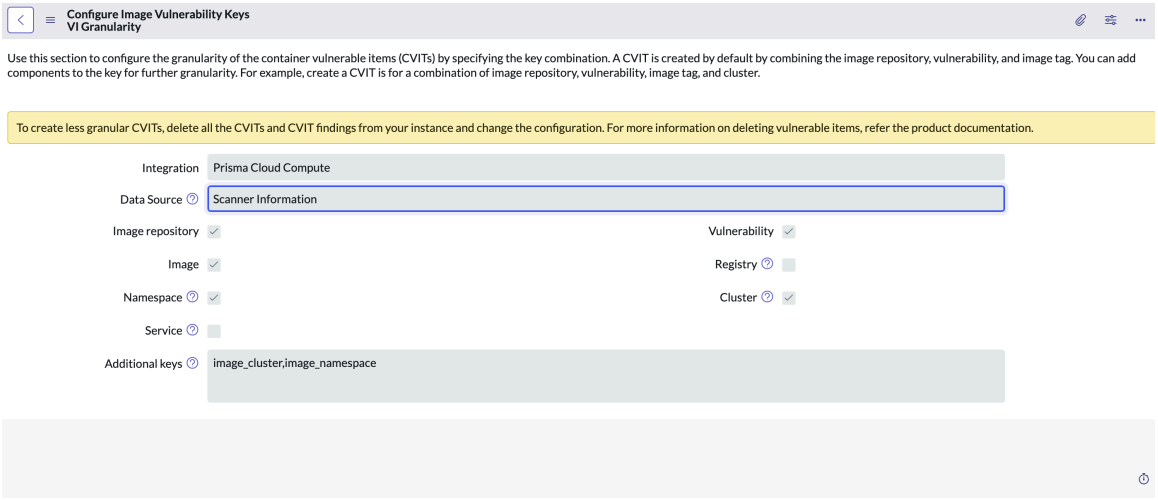
Prisma 콘솔에서 레지스트리를 구성한 다음 해당 레지스트리에서 기본 이미지를 구성할 수 있습니다. 기본 이미지에 취약성이 있는 경우 Prisma Cloud Compute 기본 이미지 통합을 실행하면 기본 이미지에 취약성이 있음을 나타내는 기본 이미지 확인란이 선택됩니다.

CVR 기반 **VI** 세분성 구성

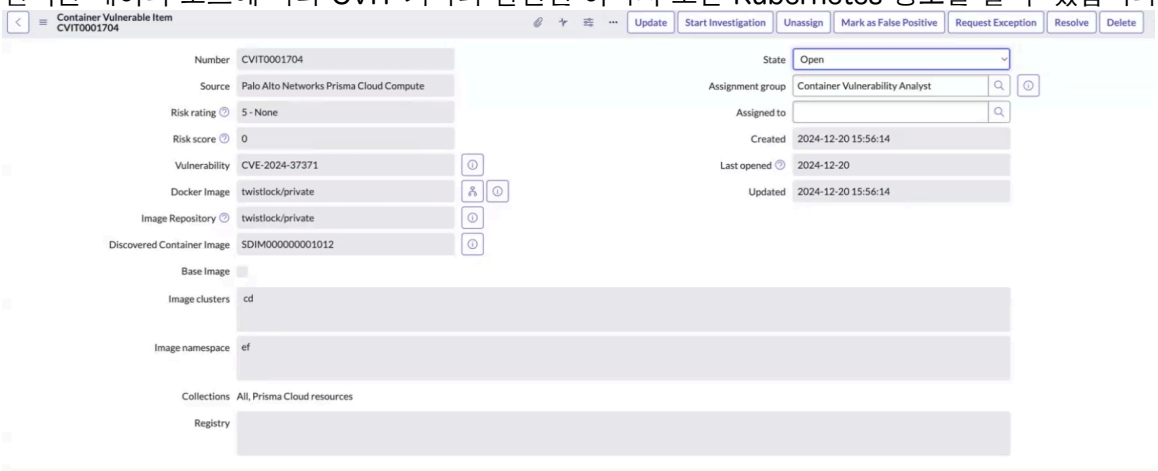
CVIT의 세분성을 구성하려면 다음으로 이동합니다. 모두 〉 **Prisma Cloud Compute** 통합 〉 **CVR** 기반 **VI** 세분성 구성 을 클릭하고 키 조합을 지정합니다. 기본적으로 CVIT는 이미지 리포지토리, 이미지 및 취약성의 조합에 대해 생성됩니다. 추가 세분성을 위해 키에 추가 구성 요소를 추가할 수 있습니다. 예를 들어 이미지 리포지토리, 이미지, 취약성 및 클러스터의 조합에 대한 CVIT를 생성할 수 있습니다.

의 컨테이너 취약성 대응v2.12.1부터 레지스트리 정보 및 데이터 소스를 사용하여 CVIT(컨테이너 취약한 항목)의 세분성을 구성할 수도 있습니다. 네임스페이스 및 클러스터 정보는 스캐너와 디스커버리. 이 정보만 디스커버리원하는 경우 데이터 소스 필드에서 **Discovery** 정보를 선택할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



선택한 데이터 소스에 따라 CVIT 기록과 관련된 이미지 또는 Kubernetes 정보를 볼 수 있습니다.



스캐너 정보를 선택하면 CVIT 기록에 이미지 클러스터 및 이미지 네임스페이스 필드가 표시됩니다.

검색 정보를 선택하면 CVIT 기록에 **Kubernetes** 클러스터 및 **Kubernetes** 네임스페이스 필드가 표시됩니다.

Prisma 통합 프로세스

실행될 Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute 때 CVE(Common Vulnerability and Exposure)가 NVD(National Vulnerability Database) 테이블에 있는지 확인합니다. 이미 있는 경우 기존 정보가 사용됩니다. 그러나 CVE를 찾을 수 없는 경우 NVD 테이블에 자리 표시자 레코드가 생성됩니다. 이러한 자리 표시자 NVD 레코드를 만들 때는 처음에는 CVE와 해당 이름만 채워집니다. 다른 세부 정보는 NVD 통합이 나중에 이러한 세부 정보를 채운다는 가정하에 채워지지 않습니다. 통합 인스턴스 매개변수 *update_nvd* 가 true로 설정되면 자리 표시자 NVD 기록이 업데이트됩니다. 기본적으로 instance 매개변수는 false로 설정됩니다. 그러나 적어도 NVD 통합이 실행되고 이러한 세부 정보가 채워질 때까지는 문제에 대한 심각도 또는 기타 세부 정보와 같은 CVE에 대한 이해가 필요합니다. 이 요구 사항을 충족하기 위해 익스플로잇 존재 및 정정 메모 필드가 Prisma에서 가져온 세부 정보로 채워집니다. 또한 이 구성은 사용자 지정이 가능하므로 Prisma에서 제공하는 정보를 기반으로 NVD 항목에 채우려는 다른 필드를 지정할 수 있습니다.

준비 중 **Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute**

설정 작업을 수행하여 준비할 Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에

애플리케이션을 설치하고 구성하려면 Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute 다음 검사 목록을 인쇄할 수 있습니다. 애플리케이션을 설치하고 취약성 데이터를 인스턴스로 ServiceNow AI Platform# 임포트하기 전에 나열된 항목이 완료되었는지 확인합니다.

통합 준비 검사 목록

작업	설명
☐	다음 정보 집합이 있는지 확인합니다. • API 기준 URL • 사용자 이름 및 암호. 이러한 자격 증명은 Prisma Cloud Compute 통합에서 취약성을 가져오는 데 사용됩니다. 자세한 내용은 https://pan.dev/compute/api/ 문서를 참조하십시오. 주: MID 서버는 선택 사항입니다. Prisma Cloud Compute 통합에 사용되는 사용자 자격 증명에는 이미지를 모니터링할 수 있는 권한이 필요합니다. 다음 코드를 참조하십시오. `{"permission":"monitorImages","saas":true,"self-hosted":true}`
☐	아직 설치 및 활성화되지 않은 경우 타사 애플리케이션을 설치하기 전에 애플리케이션을 설치합니다 취약성 대응 . 애플리케이션 설치 및 활성화에 취약성 대응 대한 자세한 내용은 다음 문서를 참조하십시오 취약성 대응 설치. 이 통합에는 버전 16.1 취약성 대응 이상이 필요합니다.
☐	권리를 얻고 인스턴스에서 애플리케이션을 ServiceNow AI Platform# 다운로드합니다Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute.
☐	임포트할 것으로 예상되는 취약한 항목의 수를 예상합니다. 임포트하려는 취약한 항목 수를 인스턴스가 수락할 수 있는지 확인합니다. 인스턴스 크기가 작으면 로드 시간이 길어질 수 있습니다. 인스턴스 크기를 모르거나 도움이 필요한 경우 기술 지원에 문의하십시오 ServiceNow .
☐	통합을 관리하고 취약한 항목을 정정할 다음 그룹 또는 사용자가 있는지 확인합니다. 관리자 Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute 애플리케이션을 설치합니다. 할당되지 않은 경우 관리자는 컨테이너 취약성 관리자 (sn_vul_container.vulnerability_admin) 및 기타 역할을 할당합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

통합 준비 검사 목록

작업	설명
	sn_vul_container.vulnerability_admin Prisma Cloud Compute 통합 구성을 완료합니다. 이 역할은 (CVR) 애플리케이션 및 해당 기록에 컨테이너 취약성 대응 대한 전체 액세스 권한을 보유합니다. 이 관리자는 다음에서 컨테이너 취약성 대응통합 및 규칙을 구성합니다. 취약성 대응 그룹 기본적으로 취약성 대응 그룹을 사용할 수 있습니다. Vulnerability Response 그룹에 할당된 사용자는 sn_vul.read_all sn_vul_container.read_all을 상속합니다. 컨테이너 정정 소유자 그룹 기본적으로 컨테이너 정정 소유자 그룹을 사용할 수 있습니다. 이 그룹에 할당된 사용자는 sn_vul_container.remediation_owner를 상속합니다. 컨테이너 정정 소유자는 자신 또는 자신이 속한 그룹에 할당된 컨테이너 취약성을 정정합니다. 취약성 분석가 Container Vulnerability Analyst 그룹에 할당된 사용자는 sn_vul.vulnerability_analyst를 상속합니다. 취약성 분석가는 모든 취약한 항목의 정정을 모니터링합니다. 아직 생성하지 않은 경우, 추가 그룹을 생성하고 인스턴스에서 사용자 관리 모듈을 사용하여 사용자를 추가하는 것이 좋습니다. 자세한 내용은 사용자 그룹 만들기를 참조하세요.
☐	취약성 대응 NVD와의 통합을 설치하고 NIST 국가 취약성 데이터베이스 통합 API(CVE만 해당)를 실행합니다.

준비가 되었습니다 Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute 애플리케이션 구성.

Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute 설치

인스턴스에서 통합을 실행하기 전에 설치 및 구성 단계를 완료하여 Prisma Cloud Compute 제품이 및 와 취약성 대응컨테이너 취약성 대응제대로 통합되도록 합니다. 이 애플리케이션은 별도의 구독으로 사용할 수 있습니다.

시작하기 전에
설치하기 전에 다음 설정 검사 목록을 완료합니다. 이러한 설정 작업은 원활한 설치 및 구성을 위해 필요합니다.

주:
이 프로세스는 프로덕션 인스턴스에 다운로드된 애플리케이션에만 적용됩니다. 애플리케이션을 비프로덕션 또는 개발 인스턴스에 다운로드하는 경우에는 권리를 얻을 필요가 없습니다. 로 애플리케이션 활성화 ServiceNow Store계속 진행합니다.

필요한 역할: 관리자

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 설치 Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute 하려는 인스턴스에 로그인합니다.
2. ServiceNow Store로 이동합니다.
3. 에서 ServiceNow Store애플리케이션을 검색합니다 Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute .
4. 애플리케이션 타일을 클릭합니다.
   설치 중인 애플리케이션에 대한 자세한 정보가 표시됩니다.

   주:
   필요한 경우 다른 요구 사항 및 종속성 섹션을 읽으십시오.

5. 앱 요청을 클릭하고 Now Support 로그인 자격 증명을 입력합니다.
6. 가져오기를 클릭합니다.
7. 인스턴스 이름 및 인스턴스 필드의 이유를 업데이트하고 인스턴스 확인을 클릭합니다.
8. 요청을 클릭합니다.
   자세한 설치 지침이 포함된 이메일을 받게 됩니다.
9. 다음으로 이동 시스템 애플리케이션 〉 애플리케이션.
10. 애플리케이션을 찾아서 선택한 다음 설치를 클릭합니다.

결과
애플리케이션이 인스턴스에 자동으로 설치됩니다.

다음에 수행할 작업
사용자 환경에 맞게 구성합니다 Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute . Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute 애플리케이션 구성 문서를 참조하십시오.

Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute
애플리케이션 구성

애플리케이션을 설치하고 구성합니다 Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute . Prisma Cloud Compute에서 데이터를 임포트합니다. 임포트한 데이터를 사용하여 Docker 이미지 및 호스트의 취약성에 우선순위를 지정하고 정정할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 통합에 대해 받은 이메일을 ServiceNow 엽니다.
2. 인스턴스에 관리자로 로그인합니다.
3. 이메일의 지침에 따라 .Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute
4. 다음으로 이동 모두 〉 **Prisma Cloud Compute** 통합 〉 관리 〉 구성.
   Prisma Cloud Compute 구성 양식에서 필드를 채웁니다. 자세한 내용은 Prisma Cloud Compute 구성 양식 문서를 참조하십시오.
5. 프로젝트 목록에서 모든 프로젝트 또는 특정 프로젝트를 선택하여 모든 프로젝트 또는 선택한 프로젝트를 각각 구성합니다.
   특정 프로젝트를 선택하면 사용 가능 목록에서 프로젝트를 선택할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

6. 마침 또는 자격 증명 저장 및 테스트를 선택하여 구성을 완료합니다.
   - 프로젝트를 구성한 경우 마침을 선택합니다.
   - 프로젝트를 구성하지 않은 경우 자격 증명 저장 및 테스트를 선택합니다.
7. 새로 생성된 인스턴스를 보려면 다음으로 이동하십시오. **Prisma Cloud Compute** 통합 〉 관리 〉 통합 인스턴스.
8. 통합 인스턴스 매개변수를 선택하여 이전에 구성한 프로젝트를 봅니다.
9. 새로 생성된 통합 인스턴스를 실행하여 다음 데이터를 임포트합니다.
   - Docker 이미지: IRE(식별 및 조정 엔진)를 사용하여 생성된 Docker 이미지를 나열합니다. 각 Docker 이미지는 리포지토리와 설치된 버전 간의 관계에 대한 정보도 제공합니다.
   - 검색된 컨테이너 이미지: 검색된 컨테이너 이미지 모듈은 이미지 ID, Docker 이미지 및 이미지 리포지토리에 대한 정보를 제공합니다. 또한 계층 정보를 저장하고 검색된 이미지와 연결합니다. 여기에서 프로젝트 및 컨테이너 수를 볼 수도 있습니다. 검색된 컨테이너 이미지의 경우 클라우드 제공자, 클라우드 지역, 클라우드 계정 ID 및 클라우드 자원 ID와 같은 클라우드 메타데이터를 볼 수 있습니다.
   - 컨테이너 이미지 패키지: 취약성이 있는 패키지에 대한 정보를 제공합니다. 이진 패키지 상세 정보도 쉼표로 구분된 값으로 제공됩니다.
   - 컨테이너 이미지 레이어: 이 화면에는 각 이미지 레이어에 대한 레코드가 표시됩니다.
   - 컨테이너 이미지 결과: 이 화면에는 관련 취약성, 이미지 계층, Docker 이미지, 이미지 리포지토리 및 검색된 이미지에 대한 정보와 함께 결과 목록이 표시됩니다. 현재 취약성 정보는 ID로만 제한됩니다. NVD(국가 취약성 데이터베이스) 통합이 트리거되면 추가 정보가 채워집니다.
   - 컨테이너 취약한 항목: 각 발견 사항에는 해당하는 취약성이 있습니다. CVIT는 세분성에 따라 추가로 생성됩니다.
10. 취약한 항목의 세분성을 구성합니다.

    a. 다음으로 이동 모두 〉 **Prisma Cloud Compute** 통합 〉 이미지 취약성 키 구성

    b. 필요한 확인란을 선택하여 CVIT의 세분성을 구성합니다.
    취약한 항목은 다음 임포트 중에 선택한 키를 기반으로 생성됩니다.

    > **주:**
    > 기본적으로 CVIT는 이미지 리포지토리, 취약성 및 이미지 태그의 조합에 대해 생성됩니다. 추가 세분성을 위해 키에 구성요소를 추가할 수 있습니다. 예를 들어 이미지 리포지토리, 취약성, 이미지 태그 및 클러스터의 조합에 대해 CVIT를 생성할 수 있습니다. 취약한 항목 또는 취약한 항목 결과가 생성되면 확인란을 더 이상 편집할 수 없습니다.

컨테이너 취약성 통합 탐색 **Wiz**

통합에 포함된 컨테이너 취약성 통합을 사용하여 Wiz 컨테이너 취약성 데이터를 임포트합니다 Wiz 취약성 대응 .

Wiz 컨테이너 취약성 통합 개요

컨테이너 취약성 통합은 Wiz 취약성 스캐너에서 식별된 컨테이너 이미지 취약성을 임포트합니다 Wiz . 데이터를 임포트하면 ServiceNow AI Platform 인스턴스의 자동화된 워크플로우를 통해 정정을 위해 컨테이너 취약성을 식별하고, 우선순위를 지정하고, 할당할 수 있습니다.

발견 사항은 컨테이너 취약 항목(CVIT)에 매핑되어 컨테이너 기반 워크로드에 대한 분류, 위험 우선순위 지정 및 대상 정정 워크플로우를 지원합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

통합과 설치 및 구성 단계에 포함된 Wiz 취약성 대응 다른 통합에 대한 자세한 내용은 문서를 Wiz 취약성 대응 통합 이해참조하십시오.

컨테이너 취약성 정정

모니터링 정정은 상태 검토로 시작하여 CVIT(컨테이너 취약한 항목)를 종결하는 프로세스입니다. 컨테이너 취약성 대응 는 해당 프로세스를 보다 생산적이고 효율적으로 만드는 도구와 절차를 제공합니다.

컨테이너 취약성 대응 계산기 규칙

취약성 계산기는 컨테이너 취약한 항목의 필드에 대한 초기 값 계산을 자동화합니다. 각 계산기의 조건은 순서대로 평가되며 첫 번째로 일치하는 계산기가 사용됩니다.

취약성 계산기를 보고 생성하려면 다음으로 이동하십시오. 모두 〉 컨테이너 취약성 대응 〉 관리 〉 취약성 계산기.

기본 시스템에는 컨테이너 취약성 대응 컨테이너 취약한 항목에 대한 기본 위험 점수를 설정하는 두 가지 취약성 계산기가 포함되어 있습니다. 기본 시스템에서 사용할 수 있는 계산기 그룹은 다음과 같습니다.

- 취약성 심각도: 정규화된 취약성 심각도를 사용하여 취약한 항목에 대한 위험 점수를 계산합니다.
- 기본 위험 계산기: 위험 규칙을 기반으로 합니다.

주:
버전 2.10 컨테이너 취약성 대응부터 다음의 경우:

- 기본 위험 계산기 규칙: 컨테이너 취약한 항목(CVIT)의 위험 점수가 변경될 때마다 다음 상세 정보가 CVIT의 메모 섹션에 문서화됩니다.
  - 계산기 그룹 이름
  - 계산기 이름
  - 가중치가 1보다 크고 위험 점수가 기여하는 필드 값입니다.
  - 최종 위험 점수
- 취약성 심각도 위험 규칙: CVIT에서 위험 점수가 업데이트될 때마다 메모 섹션이 다음 상세 정보로 업데이트됩니다.
  - 계산기 그룹 이름
  - 계산기 이름: 계산기 규칙이 템플릿 또는 스크립트를 기반으로 하는지 여부에 따라 괄호 안에 이름이 세부 정보와 함께 추가됩니다. 계산기 규칙의 기초를 수정하거나 보려면 규칙을 선택하고 고급 보기 확인란을 선택합니다. 값 유형 드롭다운 상자에서 필요한 옵션을 선택합니다. 템플릿을 선택하면 규칙에 지정된 조건에 따라 위험 점수가 업데이트됩니다. 스크립트를 선택한 경우 기존 스크립트를 추가하거나 업데이트할 수 있습니다. 시스템 속성은 `sn_sec_cmn.risk_score_changes_add_worknotes` 작업 메모 섹션을 채우는 데 도움이 됩니다. 의 컨테이너 취약성 대응v2.12.2부터 시스템 속성은 `sn_sec_cmn.risk_score_changes_add_worknotes` 기본적으로 비활성 상태입니다. 이 기능을 사용하도록 설정한 경우에만 작업 메모 섹션에서 컨테이너 취약한 항목의 위험 점수와 관련된 모든 변경 내용을 볼 수 있습니다. 또한 위험 점수가 변경된 경우에만 작업 메모가 업데이트됩니다.

취약성 위험 점수 가중치

모든 취약성에는 심각도, 중요도, 악용 정보 등의 요인에 따라 위험 점수와 등급이 할당됩니다. 컨테이너 취약한 항목 테이블의 비즈니스 규칙은 `Update Risk Rating from Risk Score` 위험 등급 계산을 담당합니다. 위험 점수가 변경될 때마다 컨테이너 취약한 항목에 대한 위험 등급이

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

계산되어 채워집니다. (VR) 애플리케이션 버전 17.1 취약성 대응 이전에는 하드 코딩된 스크립트 포함 VulnerabilityUtils의 일부로 다음 위험 등급이 제공되었습니다.

값(위험 등급)	가중치(위험 점수)
1	90–100
2	70–89
3	40–69
4	1–39
5	0

의 18.0 버전 취약성 대응부터

- 위험 등급 유형은 기본 테이블 위험 점수 가중치 〔sn_sec_cmn_risk_scorew_weights〕에 cvr_risk_rating로 제공됩니다. 이러한 유형은 위험 등급이 계산되는 각 테이블에 비즈니스 규칙 또는 스크립트 포함의 일부로 전달됩니다.
- 위험 등급 계산을 위해 위험 점수 가중치 테이블 값의 항목을 쿼리할 수 있도록 스크립트가 수정됩니다.
- 기존 형식에 대한 항목을 추가하거나 새 형식을 만듭니다. 새 유형을 만들 때는 새 위험 등급에 대한 레이블을 추가하고 관련 스크립트 및 비즈니스 규칙도 수정해야 합니다. 또한 새 위험 점수에 대한 새 스타일을 추가해야 합니다.
- 스크립트를 수정하여 기본 테이블의 기록을 쿼리합니다.

필터 탐색기에 sn_sec_cmn_risk_score_weight 입력하여 위험 점수 가중치 테이블에 액세스할 수 있습니다.

또한 다음 시나리오에서는 위험 점수가 자동으로 다시 계산됩니다.

- CI(구성 항목)가 비인터넷 연결에서 인터넷 연결로 변경되는 경우
- 취약성 항목(VI)에 대한 관련 CVE(알반적인 취약성 및 노출) 또는 외부 공급업체 항목(TPE)이 CVE Known Exploit 취약성(KEV)에 연결되는 경우

자세한 내용은 취약성 대응 계산기 및 취약성 계산기 규칙 문서를 참조하십시오.

컨테이너 취약성 대응 할당 규칙

정정을 위해 컨테이너 취약한 항목이 할당 그룹에 자동으로 할당되는 기준을 정의합니다.

컨테이너 취약한 항목에 대한 담당 규칙을 생성하고 보려면 다음으로 이동하십시오. 모두 〉 컨테이너 취약성 대응 〉 관리 〉 담당 규칙. 할당 규칙을 만들 때 조건을 설정할 수 있습니다. 이러한 조건이 충족되면 규칙은 선택한 사용자 그룹에 컨테이너 취약한 항목을 자동으로 할당합니다. 일치하는 조건이 있는 첫 번째 할당 규칙만 기록에 대해 실행됩니다. 담당 규칙에 대한 자세한 내용은 을 참조하십시오 취약성 대응 할당 규칙 개요 .

필요한 역할: 규칙을 정의하고 업데이트하기 위한 sn_vul_container.manage_assignment_rules 및 규칙을 다시 적용하기 위한 sn_vul_container.container_reapply.

버전 2.13부터 스캐너 정보에 대한 필드가 검색된 컨테이너 이미지[sn_vul_container_image] 테이블의 기록에 추가되었습니다. 컨테이너 CVIT(이미지 취약한 항목)에 대한 할당 규칙을 생성하거나 업데이트할 때 다음 값을 조건으로 사용하여 컨테이너 환경 전체에서 소유권을 추적할 수 있습니다.

- 클라우드 계정 ID
- 이미지 네임스페이스

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 레지스트리
- 호스트
- 레이블
- 상태(해결된 취약성에 대한 벤더 상태)

> **주:**
> 컨테이너 이미지 찾기〔sn_vul_container_image_findings〕테이블의 이 값은 취약성이 해결된 버전(예: 6.2.1## ##됨)을 나타냅니다. 이 값은 에서 Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute 통합가져옵니다.

> **주:**
> 오픈 상태가 아니거나 수동으로 할당된 컨테이너 취약 항목(CVIT)은 항상 담당 규칙에서 제외됩니다. 이러한 스캐너 필드의 값을 담당 규칙에 추가하고 규칙을 다시 실행하면 할당 유형이 ### 아닌 한 취약한 항목이 재할당되지 않습니다. ### manual인 항목은 담당 규칙에서 고려되지 않습니다.

> **중요사항:**
> 취약성 관리자 및 분석가는 에서 선택한 CVIT에 대한 최신 할당을 얻을 수 있습니다 취약성 관리자 작업 공간. 이 방법은 시간이 많이 걸리는 프로세스인 UI의 클래식 모든 CVIT에 대한 할당 규칙을 다시 적용하는 것보다 더 효율적입니다. 자세한 내용은 에 있는 기록의 정정 속성 재평가 취약성 관리자 작업 공간 문서를 참조하십시오.

컨테이너 취약성 대응 정정 대상 규칙

정정 대상 규칙은 컨테이너 취약한 항목(CVIT)을 정정하기 위한 예상 기간을 정의합니다. 이러한 규칙은 SLA가 취약성 자체를 정정하기 위한 시간 범위를 제공하는 방식과 유사합니다.

컨테이너 취약성에 대한 정정 대상 규칙을 만들고 보려면 다음으로 이동하십시오. 모두 〉 컨테이너 취약성 대응 〉 관리 〉 정정 대상 규칙.

정정 대상 규칙은 선택한 CVIT(컨테이너 취약한 항목)에 대한 대상 정정 시간을 정의합니다. 정정 일수를 선택하여 취약성 정정 기한을 설정합니다. 정정에 대한 미리 알림을 설정하고 규칙이 적용되는 컨테이너 취약한 항목을 설정합니다. 정정이 필요한 일수에 대한 정정 대상을 설정하고 목표 날짜에 도달하기 전에 미리 알림을 설정할 수도 있습니다. 자세한 내용은 취약성 대응 정정 대상 규칙 문서를 참조하십시오.

> **중요사항:**
> 취약성 관리자 및 분석가는 다음에서 선택한 CVIT에 대한 최신 정정 목표 날짜를 확인할 수 있습니다 취약성 관리자 작업 공간. 이 방법은 시간이 많이 걸리는 프로세스인 UI의 클래식 모든 CVIT에 대해 정정 대상 규칙을 실행하는 것보다 더 효율적입니다. 자세한 내용은 에 있는 기록의 정정 속성 재평가 취약성 관리자 작업 공간 문서를 참조하십시오.

의 예외 관리 컨테이너 취약성 대응

조직이 게시된 취약성 관리 또는 보안 정책, 표준 또는 가이드라인을 준수할 수 없는 경우 예외를 요청할 수 있습니다. 예외 관리에는 정책에 따라 정정할 수 없는 컨테이너 취약한 항목(CVIT)에 대한 예외를 요청, 검토, 승인 또는 거부하는 작업이 포함됩니다.

일부 컨테이너 취약성(CVIT)에는 기존 패치, 수정 사항 또는 솔루션이 없을 수 있습니다. 예외가 승인되면 취약성을 수정하지 않은 결과를 인정하고 이에 동의하기 때문에 위험을 수락한다는 의미이기도 합니다.

예외의 수명주기

예외의 정의

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예외는 지정된 기간 동안 CVIT 또는 RT의 수정을 연기해 달라는 요청입니다. 예를 들어 정정 소유자는 머신에 패치를 사용할 수 없는 경우 예외를 요청할 수 있습니다.

예외 요청

정정 소유자는 예외 관리 프로세스를 사용하여 CVIT 또는 RT에 대한 면제를 요청할 수 있습니다. 예외 승인자가 이 요청을 승인하면 CVIT 또는 RT가 지연 상태로 전환됩니다.

예외 요청 승인

즉시 정정할 수 없는 CVIT 또는 RT는 취약성 분석가가 검토하고, 위험을 평가하고, 정정할 수 있을 때까지 연기 승인을 받습니다. 예외 요청 승인은 2단계 워크플로가 될 수 있습니다. 첫 번째 수준 승인자만 있는 경우 예외를 요청하고 승인할 수 있습니다. 그러나 첫 번째 수준 승인자가 없으면 예외를 요청할 수 없습니다. 자세한 내용은 예외 승인자 추가 문서를 참조하십시오.

주:

v15.0부터 취약성 대응 VR 애플리케이션을 처음 배포하는 경우 예외 관리용 플로우 디자이너가 기본적으로 활성화됩니다. 워크플로우를 이미 사용 중인 경우 플로우 디자이너로 업데이트할 수 있습니다. 두 경우 모두 다시 워크플로우로 변경할 수 없습니다. 예외 관리 및 가양성에 대한 승인 규칙을 구성하려면 문서를 참조하십시오 예외 관리에 대한 승인 규칙 구성.

CVIT 또는 RT에 대한 예외 요청이 승인되면 다음 작업을 수행할 수 있습니다.

- 재개설
- 삭제
- 할당 대상 또는 할당 그룹 필드 업데이트

예외 요청 추적

예외를 발생시킨 후 CVIT 또는 RT의 상태 변경 승인 탭을 사용하여 해당 상태를 추적할 수 있습니다. RT에서 작업이 수행되면 해당 RT에서 개별 CVIT의 상태를 추적할 수 없습니다.

예외 요청의 만료

특정 CVIT 또는 RT에 대한 예외 요청이 만료되면 영향을 받는 CVIT 또는 RT가 열림 상태로 되돌아갑니다.

단일 CVIT 또는 RT의 모든 CVIT가 다음 스캔을 통과하면 CVIT 및 RT 상태 필드(해당하는 경우)가 하위 상태가 고정된상태로 종결됨으로 변경됩니다.

승인 규칙 구성

다음으로 이동하여 승인 규칙 보기 및 구성 모두 〉 컨테이너 취약성 대응 〉 관리 〉 승인 규칙. 영향을 받는 취약성, CI(구성 항목) 또는 CVIT를 식별하여 즉시 정정하거나 연기할 수 없는 CVIT에 대한 예외를 요청합니다. CVIT 연기 프로세스를 자동화합니다. 시스템에서 이러한 CVIT를 식별할 때 이러한 규칙에 따라 일치하는 CVIT를 연기합니다.

기본적으로 다음과 같은 승인 규칙이 제공됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 예외 요청에 대한 승인: 기본 시스템에는 두 가지 승인 수준이 있는 기본 구성이 제공됩니다. 취약한 항목에 대한 예외 요청이 있을 때마다 수준 1에 있는 사용자 또는 그룹으로 승인 요청이 전송됩니다. 수준 1 승인자가 승인하면 수준 2 승인자에게 전송됩니다.

  주:
  기본 수준을 변경하고 필요에 따라 편집할 수 있습니다. v2.0.6부터 컨테이너 취약성 대응 시스템 속성 [sys_properties] 테이블의 워크플로우를 통해 예외 승인에 기본 시스템에 제공된 시스템 속성을 사용할 수 있습니다. 따라서 워크플로우를 통해 예외 또는 가양성 요청이 발생하면 승인을 위해 시스템 속성에 정의된 그룹 ID로 전송됩니다. 다음으로 이동 모두 〉 시스템 속성 및 , *sn_vul_container.container_exception_approver_L2*, 또는 *sn_vul_container.container_false_positive_approver_group* 을 선택하여 *sn_vul_container.container_exception_approver_L1*속성 값을 변경합니다.

- 예외 규칙에 대한 승인: 구성은 없지만 두 가지 승인 수준이 있습니다.
- 긍정 오류에 대한 승인: 하나의 승인 수준이 있는 하나의 구성이 있습니다.

주:
의 컨테이너 취약성 대응v2.5부터 설정된 일 후에 승인자와 요청자 모두에게 이메일 알림과 함께 긍정 오류 및 예외를 승인하기 위한 시간 범위를 구성할 수 있습니다. 요청이 발생하면 컨테이너 취약한 항목이 검토 중 상태로 변경되고 상태 변경 기록이 생성됩니다. 승인자가 구성된 시간 범위 내에 응답하지 않으면 컨테이너 취약한 항목 또는 정정 작업이 열림 상태로 되돌아갑니다. 이전 상태는 **backup_state** 필드에 저장됩니다. 자세한 내용은 예외 관리에 대한 승인 규칙 구성 문서를 참조하십시오.

에서 예외 요청 및 승인 컨테이너 취약성 대응

지정된 기간 동안 컨테이너 취약한 항목(CVIT)의 정정을 연기하도록 요청할 수 있습니다. 예를 들어 개발자는 머신에 패치를 사용할 수 없는 경우 예외를 요청할 수 있습니다. 액세스 권한이 있는 승인자는 다른 사용자의 요청을 승인할 수 있습니다.

예외를 요청하거나 승인하려면 다음을 참조하십시오.

- 컨테이너 취약한 항목에 대한 예외 요청
- 를 사용하여 컨테이너 취약성에 대한 예외 요청 GRC: 정책 및 준수 관리

주:

이메일 알림은 예외 관리의 모든 단계에서 전송되어 요청의 상태 및 기타 세부 정보를 제공합니다. 예를 들어 예외가 요청되면 요청자는 요청이 발생했음을 확인하는 이메일을 받습니다. 또한 승인자는 예외가 요청되었다는 내용의 이메일을 받습니다. 의 컨테이너 취약성 대응v2.5부터 설정된 일 후에 승인자와 요청자 모두에게 이메일 알림과 함께 긍정 오류 및 예외를 승인하기 위한 시간 범위를 구성할 수 있습니다. 요청이 발생하면 컨테이너 취약한 항목이 검토 중 상태로 변경되고 상태 변경 기록이 생성됩니다. 승인자가 구성된 시간 범위 내에 응답하지 않으면 컨테이너 취약한 항목 또는 정정 작업이 열림 상태로 되돌아갑니다. 이전 상태는 **backup_state** 필드에 저장됩니다. 자세한 내용은 예외 관리에 대한 승인 규칙 구성 문서를 참조하십시오.

컨테이너 취약한 항목에 대한 예외 요청

즉시 정정할 수 없는 컨테이너 취약한 항목(CVIT)에 대한 예외를 요청합니다. 예를 들어 정정 소유자는 머신에 패치를 사용할 수 없는 경우 예외를 요청할 수 있습니다.

시작하기 전에
필요한 역할: 개발자 그룹

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보
의 취약성 관리자 작업 공간대량 편집 기능을 사용하여 여러 CVIT에 대한 예외를 동시에 요청할 수 있습니다. 자세한 내용은 취약성 관리자 작업 공간에서 대량 예외 요청 문서를 참조하십시오.

프로시저

1. 다음으로 이동 컨테이너 취약성 대응 〉 컨테이너 취약한 항목 〉 모두.
2. 예외를 요청할 항목을 선택합니다.
   선택한 항목은 오픈 또는 조사 중 상태여야 합니다.
3. 컨테이너 취약한 항목 양식에서 예외 요청을 클릭합니다.
   〔store-future: BEGIN review〕

   주:
   또는 GRC: 정책 및 준수 관리 에서 선택되었는지 여부에 취약성 대응 따라 컨테이너 취약성 대응 〉 예외 관리 화면에 예외 요청 양식이 변경됩니다.

   〔End〕
4. 〔store-future: BEGIN review〕이 항목을 예외 관리 화면에서 선택한 경우 취약성 대응 다음을 수행합니다.〔End〕

   a. 양식에서 필드를 채웁니다.

예외 요청 양식

필드	설명
다음까지	예외 요청이 만료되는 날짜입니다. 이 날짜는 에서 선택한 기간 내에 있어야 합니다. 모두 〉 컨테이너 취약성 대응 〉 관리 〉 예외 관리 화면. 예외 요청이 만료되면 그룹은 열림 상태로 되돌아갑니다. 주: 의 컨테이너 취약성 대응버전 1.2부터 예외 관리 기능을 사용하여 취약한 항목의 정정이 지연된 경우 스캐너에서 다시 열 경우 취약성에 설정된 지연 날짜가 계속 유지됩니다. 이 기능을 사용하려면 시스템 속성 *sn_vul.container.auto_defer_cvit_in_active_e* 값을 true로 설정합니다. 또한 지연된 날짜는 CVIT가 종결되거나 예외가 만료된 후에도 유지됩니다. 필요한 역할은 읽기와 쓰기 모두에 대해 sn_vul_container.manage_exception_configuration입니다.
이유	예외 이유입니다. 선택 항목은 다음과 같습니다. ▪ 위험 수락됨 ▪ 유지관리 기간을 기다리는 중 ▪ 수정 사용 불가

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	▪ 사용 중인 완화 통제 ▪ 기타 새 이유 선택 항목을 추가하는 방법을 보려면 다음 문서를 참조하십시오 정책 이유 매핑 정의.
추가 정보	이 요청이 수행되는 이유와 관련된 상세 정보입니다. 이 필드는 정정 소유자가 업데이트해야 합니다.

b. **Request Approval**을 클릭하여 예외 요청을 제출합니다.
컨테이너 취약한 항목의 상태가 검토 중으로 변경됩니다. 상태 변경 승인 탭을 사용하여 예외 요청의 상태를 추적합니다.

컨테이너 정정 작업에 대한 예외 요청

즉시 해결할 수 없는 경우 지정된 기간 동안 컨테이너 정정 작업을 연기하는 예외를 요청합니다.

시작하기 전에

작업 공간에서 예외를 취약성 대응 요청할 수 있습니다. 에서 예외 요청 IT 정정 작업 공간 문서를 참조하십시오.

필요한 역할:

sn_vul.remediation_owner, sn_vul.app_security_champion 또는 sn_vul_container.remediation_owner.

클래식 환경에서 컨테이너 정정 작업에 대한 예외를 요청할 수도 있습니다.

프로시저

1. 다음으로 이동 모두 〉 컨테이너 취약성 대응 〉 정정 작업 〉 모두.
2. 예외를 요청할 그룹을 선택합니다.
선택한 작업은 오픈, 조사 중 또는 구현 대기 중 상태여야 합니다.
3. 컨테이너 정정 작업 기록에서 예외 요청을 선택합니다.
4. 양식에서 필드를 채웁니다.

예외 요청 양식

필드	설명
다음까지	예외 요청이 만료되는 날짜입니다. 이 날짜는 구성에 정의된 예외 기간 내에 있어야 합니다.
이유	예외 요청에 대한 근거입니다.
추가 정보	이 요청이 수행되는 이유와 관련된 상세 정보입니다. 이 필드는 정정 소유자가 업데이트해야 합니다.

5. 승인 요청을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

를 사용하여 컨테이너 취약성에 대한 예외 요청 **GRC:** 정책 및 준수 관리

에서 애플리케이션의 컨테이너 취약성 대응정책 예외 관리 기능을 정책 및 준수 관리 사용하여 GRC 정책 예외를 요청합니다.

시작하기 전에

정책 예외 통합을 사용하여 정책 예외를 요청하려면 먼저 에서 ServiceNow Store애플리케이션을 다운로드 GRC: 정책 및 준수 관리 해야 합니다.

필요한 역할: sn_vul.remediation_owner

클래식 UI에서 예외를 요청할 수도 있습니다.

프로시저

1. 다음으로 이동 모두 〉 컨테이너 취약성 대응 〉 컨테이너 취약한 항목 (또는 정정 작업)〉모두로 설정하고 예외를 요청할 항목 또는 그룹을 엽니다.
   선택한 항목 또는 그룹은 오픈, 조사 중 또는 구현 대기 중 상태여야 합니다.
2. 선택한 양식에서 예외 요청을 클릭합니다.

   주:
   이 항목을 예외 관리 화면에서 선택한 경우 GRC: 정책 및 준수 관리 예외 요청 양식의 필드에 내용을 입력합니다. 양식 필드에 대한 자세한 내용은 예외 요청 양식 문서를 참조하십시오.

   a. **Request Approval**을 클릭하여 예외 요청을 제출합니다.
   취약한 항목의 상태가 검토 중으로 변경되고 정책 예외가 생성됩니다. 상태 변경 승인 탭을 사용하여 예외 요청의 상태를 추적합니다.

   b. 정책 예외 관련 목록을 클릭하여 정책 예외를 봅니다.

   c. 정책 예외 번호를 클릭합니다.

   d. 승인자 필드에서 승인자의 이름을 선택합니다.

   e. 소스 탭을 클릭하고 통제 목표 필드에서 통제 목표를 선택합니다.

   f. 위험 평가 탭을 클릭하고 위험 등급 필드에서 위험 등급을 선택합니다.

   g. 양식을 저장합니다.

   h. 영향을 받는 컨트롤 탭을 클릭합니다.

   i. 추가를 클릭하여 컨트롤을 추가합니다.

   j. 양식을 저장합니다.

   주:
   규정 준수 검토 요청을 클릭하여 규정 준수 검토를 제기할 수 있습니다.

   승인 양식이 승인자에게 전송됩니다.

   승인자는 승인을 클릭하여 요청을 승인하거나 추가 승인 요청을 클릭하여 추가 승인을 요청할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

기록 상태가 연기됨으로 변경됩니다. 명시된 이유는 예외 요청을 제기할 때 선택한 이유입니다. 지연 탭에는 기록에 대한 추가 메모가 제공됩니다.

> **주:**
> 요청이 거부되면 기록이 이전 상태로 이동합니다.

3. 제출을 클릭합니다.
   정책 예외 통합 및 정정 소유자와 준수 관리자 간의 핸드오프에 대한 자세한 내용은 정책 및 준수 관리 선택적 설정을 참조하십시오.

정책 이유 매핑 정의

예외를 요청하는 모든 사용자가 사용할 수 있는 이유 선택 항목을 정의합니다.

시작하기 전에
필요한 역할: sn_vul.compliance.manager 및 sn_vul_container.manage_exception_configuration

프로시저

1. 다음으로 이동 모두 〉 정책 및 준수 〉 정책 예외 〉 통합 레지스트리.

   > **주:**
   > 이유 선택 테이블에 있는 이유 선택 항목에서 이유를 선택하거나 새 이유를 추가할 수 있습니다.

2. 컨테이너 취약성 대응 - CVIT 통합 레지스트리를 클릭합니다.
3. 이유 선택 목록에서 새로 만들기를 클릭합니다.
4. 돋보기 아이콘을 클릭합니다.
5. 기존 이유 선택 항목을 추가하여 새 이유 선택을 만듭니다.
   - 기존 이유 선택을 추가하려면 이유를 선택합니다.
   - 이유 선택 테이블에 새 이유 선택을 추가하려면 새로 만들기를 클릭하고 양식의 필드를 채웁니다.

이유 선택 목록 양식

필드	설명
레이블	이 선택 항목의 고유 레이블입니다.
값	이 선택 항목의 고유 값입니다. 이 값은 각 애플리케이션의 정책 사유 매핑 테이블에 매핑됩니다. 이 테이블로 이동하려면 sn_vul_policy_reason_mapping를 입력합니다 . ## 탐색기의 LIST.
순서	이 선택 항목에 대한 순서입니다. 이유는 이 숫자를 기준으로 정렬됩니다.
기본값	요청 시 정책 예외가 요청될 때마다 이 이유 선택을 사용할 수 있음을 나타내는 옵션입니다. 통합 레지스트리에 애플리케이션별 선택 항목이 포함되어 있지 않으면 기본 필드가 선택된 모든 이유 선택 항목을 사용할 수 있습니다.
활성	이유 선택 목록에 선택 항목을 표시하는 옵션입니다.

6. 제출을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

결과
이유 선택 항목이 추가됩니다. 이유 선택은 선택한 애플리케이션에 대한 정책 예외 요청 양식의 이유 필드에서 사용할 수 있습니다.

에서 예외 요청 승인 컨테이너 취약성 대응

즉시 정정할 수 없는 컨테이너 취약한 항목 또는 정정 작업에 대한 예외 요청을 승인합니다. 이러한 위험 요청을 평가한 다음 정정할 수 있을 때까지 연기하도록 승인해야 합니다.

시작하기 전에
필요한 역할: sn_vul.exception_approver

이 태스크 정보
에서 예외 및 긍정 오류 요청을 승인할 수 있습니다 취약성 관리자 작업 공간.

클래식 환경에서도 예외 요청을 승인할 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 컨테이너 취약성 대응 〉 내 승인.
2. 큐에서 요청을 선택합니다.
3. 적절한 설명을 사용하여 요청을 승인하거나 거부합니다.

에서 컨테이너 취약한 항목 연기 컨테이너 취약성 대응

컨테이너 취약한 항목(CVIT)과 관련된 문제가 위험도가 낮고 추가 분석 없이 즉시 지연될 수 있다고 판단되면 지연 기능을 사용할 수 있습니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)
가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

이 태스크 정보
예약된 작업이 매일 실행되어 재개시 날짜에 도달한 지연된 취약한 항목을 확인합니다. CVIT의 연기가 만료되는 날에 기록이 다시 열립니다.

프로시저

1. 다음으로 이동 모두 〉 컨테이너 취약성 대응 〉 컨테이너 취약한 항목.
2. 취약한 항목을 엽니다.
3. 예외 요청을 클릭합니다.
4. 양식의 필드에 적절히 입력합니다.

필드	설명
다음까지	연기됨 상태가 만료되고 정정 작업이 다시 활성화되는 날짜를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	주: 버전 18.0 컨테이너 취약성 대응부터 예외 기간이 만료되기 전에 스캐너에서 지연된 컨테이너 취약한 항목(CVIT)을 닫고 다시 열면 CVIT의 상태가 활성 예외 창을 적용하는 지연 상태로 되돌아갑니다. 이 기능을 사용하려면 시스템 속성 *sn_vul.container.auto_defer_cvit_in_active_ex* 값을 true로 설정합니다. 또한 지연된 종료 날짜는 취약한 항목이 종결되거나 예외가 만료된 후에도 지속됩니다. 필요한 역할은 읽기와 쓰기 모두에 대해 sn_vul_container.manage_exception_configuration입니다. 기록이 제출된 후 이메일 알림이 정의되어 있으면 만료 날짜가 1주일 이내이면 그룹 구성원 컨테이너 취약성 대응 은 이메일을 받습니다. 지연 날짜가 만료되면 취약한 항목이 다시 열림으로 설정되고 두 번째 이메일 알림이 전송됩니다.
이유	문제를 지연시키는 이유를 입력합니다. 선택 항목은 다음과 같습니다. ○ 유지관리 기간을 기다리는 중 ○ 긍정 오류 ○ 수정 사용 불가 ○ 수용된 위험 ○ 사용 중인 완화 통제 ○ 기타
추가 정보	기타 관련 정보를 입력합니다.

5. 제출을 클릭합니다.
그룹이 검토 중으로 표시됩니다. 다시 열기 관련 링크가 나타납니다. 재개시된 날짜와 이유는 상태 변경 승인 탭 아래의 작업 메모에 표시됩니다.

   컨테이너 취약성 대응 v2.3부터는 지연된 컨테이너 취약한 항목에 대한 메모 섹션의 작업 메모 필드에 관련 정보를 추가할 수 있습니다.

지연된 컨테이너 취약한 항목에 대한 연장 요청

지연된 컨테이너 취약한 항목이 지연 기한에 도달하기 전에 해당 항목에 대한 연장을 요청합니다. 정정 소유자는 더 이상 이 요청을 하기 위해 지연된 기한까지 기다릴 필요가 없습니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)

이 태스크 정보
작업 공간에서 연장을 취약성 대응 요청할 수도 있습니다. 자세한 내용은 취약성 관리자 작업 공간에서 지연된 취약한 항목에 대한 연장 요청 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 컨테이너 취약성 대응 〉 컨테이너 취약한 항목.
2. 지연된 컨테이너 취약한 항목을 엽니다.
3. 연장 요청을 선택합니다.

   주:
   연장 요청 버튼은 컨테이너 취약한 항목의 상태가 연기됨인 경우에만 표시됩니다.

4. 양식의 필드에 적절히 입력합니다.

필드	설명
연장 날짜	정정을 위해 지연된 컨테이너 취약한 항목을 연장해야 하는 종료 날짜를 선택합니다.
이유	문제를 지연시키는 이유를 입력합니다. 선택 항목은 다음과 같습니다. ○ 유지관리 기간을 기다리는 중 ○ 수정 사용 불가 ○ 수용된 위험 ○ 사용 중인 완화 통제 ○ 기타
추가 정보	기타 관련 정보를 입력합니다.

5. 승인 요청을 선택합니다.
   이메일은 요청 제출 및 승인자의 후속 조치 시 트리거됩니다.

   주:
   - 요청은 두 가지 수준의 승인을 거칩니다.
   - 지연된 컨테이너 취약한 항목이 다시 확장되면 백엔드에서 연장 지연 수가 증가합니다.

6. 요청이 승인되면 기한, 이유 및 연기 메모가 업데이트됩니다.

에서 예외 규칙 작업 컨테이너 취약성 대응

즉시 수정하거나 연기할 수 없는 컨테이너 취약한 항목(CVIT)에 대한 예외를 요청할 수 있습니다. VI 지연 프로세스를 자동화하면 시스템에서 일치하는 CVIT를 식별할 때 규칙에 따라 해당 CVIT를 지연시킬 수 있습니다.

예외 규칙에 대해 다음 작업을 수행할 수 있습니다.

- 에서 예외 규칙 생성 컨테이너 취약성 대응
- 에서 예외 규칙 요청 승인 컨테이너 취약성 대응
- 에서 예외 규칙 활성화 컨테이너 취약성 대응
- 에서 예외 규칙 다시 열기 컨테이너 취약성 대응
- 에서 승인된 예외 규칙 업데이트 컨테이너 취약성 대응

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 에서 예외 규칙 삭제 컨테이너 취약성 대응
- 에서 컨테이너 취약한 항목 연기 컨테이너 취약성 대응

주:
의 컨테이너 취약성 대응v2.5부터 설정된 일 후에 승인자와 요청자 모두에게 이메일 알림과 함께 긍정 오류 및 예외를 승인하기 위한 시간 범위를 구성할 수 있습니다. 요청이 발생하면 컨테이너 취약한 항목이 검토 중 상태로 변경되고 상태 변경 기록이 생성됩니다. 승인자가 구성된 시간 범위 내에 응답하지 않으면 컨테이너 취약한 항목 또는 정정 작업이 열림 상태로 되돌아갑니다. 이전 상태는 **backup_state** 필드에 저장됩니다. 자세한 내용은 예외 관리에 대한 승인 규칙 구성 문서를 참조하십시오.

에서 예외 규칙 생성 컨테이너 취약성 대응

컨테이너 취약한 항목 그룹(CVIT)의 특정 조건에 대한 예외를 자동으로 요청하는 규칙(예: 이러한 CVIT의 취약성 심각도를 기반으로 하는 조건이 있는 규칙)을 생성합니다. 이 규칙을 사용하면 승인된 규칙 조건과 일치하는 경우 신규 및 기존 CVIT를 자동으로 연기할 수 있습니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin

이 태스크 정보
규칙은 "유효 기간(시작)"부터 "유효 기간(종료)" 날짜까지 적용됩니다. 규칙이 승인되면 정정 작업(VUL)이 생성됩니다. 이 VUL의 그룹화 방법을 예외 규칙이라고 합니다. VUL은 Deferred(연기됨) 상태로 생성됩니다. 이 VUL을 닫거나, 다시 열거나, 삭제할 수 없습니다. 신규 및 재개된 CVIT는 "유효 기간(시작)" 날짜부터 그룹이 "유효 기간(종료)" 날짜에 만료될 때까지 연기되고 이 VUL에 추가됩니다.

주:

이메일 알림은 예외 규칙 워크플로우의 모든 단계에서 전송됩니다. 이러한 이메일은 요청의 상태 및 기타 세부 정보를 제공합니다. 예를 들어 예외 규칙이 요청되면 요청자는 요청이 제출되었음을 확인하는 이메일을 받습니다.

주:
규칙이 거부되면 초안 상태에서 다시 열고 업데이트한 다음 승인을 위해 다시 제출할 수 있습니다.

프로시저
1. 다음으로 이동 모두 〉 컨테이너 취약성 대응 〉 관리 〉 예외 규칙.
2. 예외 규칙 새 기록 페이지에서 새로 만들기를 클릭하여 규칙을 생성합니다.
3. 예외 규칙 양식의 필드에 내용을 입력합니다.

   주:
   양식 필드에 대한 자세한 내용은 예외 규칙 양식 문서를 참조하십시오.

4. 규칙을 생성할 때 할당 그룹을 추가합니다.
5. 승인을 위해 양식을 제출합니다.
   요청 상태가 검토 중으로 변경됩니다. 예외 규칙을 제출할 때까지는 초안 상태로 유지됩니다.
6. 그룹을 보고 작성하여 예외 규칙을 관리하려면 다음을 수행합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 다음으로 이동 모두 〉 사용자 관리 〉 그룹.

b. 예외 규칙에서 요청된 승인 탭을 클릭하여 요청 상태를 봅니다.
예약된 작업이 매일 실행되어 기존 데이터에 대한 예외 규칙이 실행됩니다. 조건과 일치하는 모든 취약한 항목이 지연 상태로 이동됩니다. 승인된 예외 규칙이 삭제되면 지연된 모든 취약한 항목이 이전 상태로 되돌아갑니다. 자세한 내용은 예외 규칙 작업 문서를 참조하십시오.

에서 예외 규칙 요청 승인 컨테이너 취약성 대응

이러한 요청을 승인하거나 거부할 수 있도록 사용자의 예외 규칙 요청을 평가합니다.

시작하기 전에
필요한 역할: sn_vul.exception_approver

이 태스크 정보
예외 승인자 수준 1 사용자 그룹 구성원은 수준 1 예외 규칙 요청을 승인할 수 있습니다. 마찬가지로 예외 승인자 수준 2 사용자 그룹 구성원은 수준 2 예외 규칙 요청을 승인할 수 있습니다. 두 사용자 그룹 모두 기본적으로 예외 승인자 역할을 상속합니다.

주:

VR 애플리케이션을 처음 배포하는 경우에는 예외 관리용 플로우 디자이너가 기본적으로 활성화되어 있습니다. 워크플로우를 이미 사용 중인 경우 플로우 디자이너로 업데이트할 수 있습니다. 두 경우 모두 다시 워크플로우로 변경할 수 없습니다. 예외 관리 및 가양성에 대한 승인 규칙을 구성하려면 문서를 참조하십시오 예외 관리에 대한 승인 규칙 구성.

프로시저

1. 다음으로 이동 모두 〉 컨테이너 취약성 대응 〉 내 승인.
2. 큐에서 요청을 선택합니다.
3. 를 사용하여 요청을 승인 또는 거부하고 요청을 승인하거나 거부한 이유를 설명합니다.
예외 규칙이 승인되면 기본적으로 지연 상태로 정정 작업(RT)이 생성됩니다. 이 규칙은 "유효 기간(시작)" 날짜부터 생성된 모든 CVIT와 종결 상태에서 오픈 상태로 전환된 CVIT에 대해 실행됩니다. 정의된 조건과 일치하는 CVIT가 RT에 추가되고 지정된 기간 동안 지연됩니다.

주:
규칙이 거부되면 초안 상태에서 다시 열고 업데이트한 다음 승인을 위해 다시 제출할 수 있습니다.

에서 예외 규칙 활성화 컨테이너 취약성 대응

규칙은 "유효 기간(시작)" 날짜에 활성화됩니다. 활성화 후에는 컨테이너 취약한 항목(CVIT)에 대한 예외 프로세스를 자동화합니다.

예외 규칙은 다음 수명주기를 따릅니다.

1. 생성하거나 다시 열고 지정된 조건을 충족하는 새 CVIT가 지연됩니다. 예외 규칙을 처음 실행할 때 기존 데이터에서 실행 옵션을 사용하도록 설정하면 예외 규칙 조건과 일치하는 모든 활성 및 지연되지 않은 CVIT가 새로 생성된 RT(정정 작업)로 이동되고 상태가 연기됨으로 변경됩니다.
2. 새로 생성된 CVIT가 예외 규칙 조건과 일치하면 규칙과 연결된 지연된 RT로 이동되고 그룹 규칙이 실행되지 않습니다.
3. "유효 기간(시작)" 날짜에 기존 데이터에서 실행 옵션을 활성화하면 기존 CVIT가 추가됩니다.
4. RT는 규칙이 "유효 기간(Valid to)" 날짜에 만료되면 새 CVIT 수락을 중지합니다. RT는 "연기됨" 날짜까지 존재합니다.
5. 예외 규칙은 "유효 기간(종료)" 날짜에 만료됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

에서 예외 규칙 다시 열기 컨테이너 취약성 대응

거부되었지만 다시 제출하려는 예외 규칙을 다시 엽니다. 규칙을 다시 열면 초안 상태로 이동합니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin

이 태스크 정보
그런 다음 승인을 위해 규칙을 업데이트하고 다시 제출할 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 컨테이너 취약성 대응 〉 관리 〉 예외 규칙.
2. 다시 열려는 규칙을 찾아 다시 열기를 클릭합니다.
3. 승인을 위해 양식을 업데이트하고 다시 제출합니다.

에서 승인된 예외 규칙 업데이트 컨테이너 취약성 대응

승인된 규칙을 업데이트하려면 취소합니다. 예를 들어 날짜를 수정하거나 승인된 규칙에 조건을 추가하려면 먼저 VUL(정정 작업)이 삭제되고 CVIT(컨테이너 취약한 항목)가 열림 상태로 이동하도록 취소해야 합니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin

이 태스크 정보
그룹 규칙은 이러한 CVIT에 다시 적용됩니다. 승인 프로세스를 다시 거치도록 변경 후 규칙을 제출합니다.

프로시저

1. 다음으로 이동 모두 〉 컨테이너 취약성 대응 〉 관리 〉 예외 규칙.
2. 취소하려는 예외 규칙을 열고 취소를 클릭합니다.
3. 규칙 취소(Cancel Rule) 대화 상자에서 규칙 취소**(Cancel rule)**를 클릭합니다.
   규칙이 초안 상태로 다시 이동하고 연결된 VUL이 삭제됩니다. 관련 CVIT가 다시 열리고 그룹 규칙이 개별 CVIT에 적용됩니다.

에서 예외 규칙 삭제 컨테이너 취약성 대응

더 이상 필요하지 않은 예외 규칙을 삭제합니다. 예를 들어 수집 중에 CVIT(컨테이너 취약한 항목)를 지연하지 않으려면 규칙을 삭제할 수 있습니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin

이 태스크 정보
규칙을 삭제하면 연결된 정정 작업(VUL)이 취소됩니다. 관련 CVIT가 다시 열리고 그룹 규칙이 개별 CVIT에 적용됩니다.

프로시저

1. 다음으로 이동 모두 〉 컨테이너 취약성 대응 〉 관리 〉 예외 규칙.
2. 삭제하려는 예외 규칙을 열고 삭제를 클릭합니다.
3. Delete Rule(규칙 삭제) 대화 상자에서 **Delete** rule(규칙 삭제)을 클릭하여 선택한 규칙을 삭제합니다.
   연결된 정정 작업도 삭제됩니다. 관련 CVIT가 다시 열리고 그룹 규칙이 개별 CVIT에 적용됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

에서 지연된 정정 작업에 대한 연장 요청 컨테이너 취약성 대응

지연된 기한에 도달하기 전에 지연된 정정 작업(VUL)에 대한 연장을 요청합니다. 정정 소유자는 더 이상 이 요청을 하기 위해 지연된 기한까지 기다릴 필요가 없습니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)

이 태스크 정보
작업 공간에서 연장을 취약성 대응 요청할 수도 있습니다. 자세한 내용은 취약성 관리자 작업 공간에서 지연된 취약한 항목에 대한 연장 요청 문서를 참조하십시오.

프로시저
1. 다음으로 이동 모두 〉 컨테이너 취약성 대응 〉 정정 작업.
2. 지연된 정정 작업을 엽니다.
3. 연장 요청을 선택합니다.
4. 양식의 필드에 적절히 입력합니다.

필드	설명
연장 날짜	지연 상태가 만료되고 컨테이너 취약한 항목이 다시 활성화되는 날짜를 선택합니다.
이유	문제를 지연시키는 이유를 입력합니다. 선택 항목은 다음과 같습니다. ○ 유지관리 기간을 기다리는 중 ○ 수정 사용 불가 ○ 수용된 위험 ○ 사용 중인 완화 통제 ○ 기타
추가 정보	기타 관련 정보를 입력합니다.

5. 승인 요청을 선택합니다.
   요청이 승인되면 정정 작업의 일부인 컨테이너 취약한 항목에도 변경 사항이 롤다운됩니다. 그러나 컨테이너 취약한 항목은 지연 상태여야 하며 현재 종료 데이터는 업데이트 종료 날짜 이전이어야 합니다. 요청 제출 및 승인자의 후속 조치 시에도 이메일이 트리거됩니다.

   주:
   - 요청은 두 가지 수준의 승인을 거칩니다.
   - 연장 요청 버튼은 예외 규칙의 일부로 생성된 정정 작업에 사용할 수 없습니다.
   - 지연된 정정 작업이 다시 연장되면 백엔드에서 연장 지연 수가 증가합니다.

에서 예외 규칙에 대한 연장 요청 컨테이너 취약성 대응

지연된 예외 규칙이 기한까지 지연되기 전에 해당 규칙의 연장을 요청합니다. 정정 소유자는 더 이상 이 요청을 하기 위해 지연된 기한까지 기다릴 필요가 없습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_vul.exception_approver

이 태스크 정보
작업 공간에서 연장을 취약성 대응 요청할 수도 있습니다. 자세한 내용은 취약성 관리자 작업 공간에서 지연된 취약한 항목에 대한 연장 요청 문서를 참조하십시오.

프로시저

1. 다음으로 이동 모두 〉 컨테이너 취약성 대응 〉 예외 규칙.
2. 지연된 예외 규칙을 선택합니다.
3. 연장 요청을 선택합니다.
4. 양식의 필드에 적절히 입력합니다.

필드	설명
연장 날짜	예외 규칙을 연장해야 하는 종료 날짜를 선택합니다.
이유	예외 규칙을 지연시키는 이유를 입력합니다. 선택 항목은 다음과 같습니다. ○ 수용된 위험 ○ 유지관리 기간을 기다리는 중 ○ 수정 사용 불가 ○ 사용 중인 완화 통제 ○ 기타
추가 정보	기타 관련 정보를 입력합니다.

5. 승인 요청을 선택합니다.
요청이 승인되면 예외 규칙 및 컨테이너 취약한 항목에 대해 지연 기한, 이유 및 추가 정보 필드가 업데이트됩니다. 요청 제출 및 승인자의 후속 조치 시에도 이메일이 트리거됩니다.

주:
- 요청은 두 가지 수준의 승인을 거칩니다.
- 연장 요청 버튼은 예외 규칙의 일부로 생성된 정정 작업에 사용할 수 없습니다.
- 지연된 예외 규칙이 다시 확장되면 백엔드에서 연장 지연 수가 증가합니다.

긍정 오류 컨테이너 취약성 항목 표시 및 승인

컨테이너 취약한 항목(CVIT) 및 정정 작업(VUL)은 가양성으로 표시할 수 있습니다. 쓰기 권한이 있는 승인자는 다른 사용자의 이러한 요청을 승인할 수 있습니다.

- 에서 긍정 오류로 표시 컨테이너 취약성 대응
- 긍정 오류 승인

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

이메일 알림은 가양성 워크플로우의 모든 단계에서 전송되어 요청의 상태 및 기타 세부 정보를 제공합니다. 예를 들어 CVIT 또는 정정 작업이 긍정 오류로 표시되면 요청자는 확인 이메일을 받게 됩니다. 이와 동시에 승인자는 CVIT 또는 정정 작업이 긍정 오류로 표시되었다는 내용의 이메일을 받습니다. 의 컨테이너 취약성 대응v2.5부터 설정된 일 후에 승인자와 요청자 모두에게 이메일 알림과 함께 긍정 오류 및 예외를 승인하기 위한 시간 범위를 구성할 수 있습니다. 요청이 발생하면 컨테이너 취약한 항목이 검토 중 상태로 변경되고 상태 변경 기록이 생성됩니다. 승인자가 구성된 시간 범위 내에 응답하지 않으면 컨테이너 취약한 항목 또는 정정 작업이 열림 상태로 되돌아갑니다. 이전 상태는 **backup_state** 필드에 저장됩니다. 자세한 내용은 예외 관리에 대한 승인 규칙 구성 문서를 참조하십시오.

중요사항:
취약성 분석가 및 정정 소유자는 각각 취약성 관리자 작업 공간과IT 정정 작업 공간에서 가양성을 요청하고 승인할 수 있습니다.

에서 긍정 오류로 표시 컨테이너 취약성 대응

스캐너에서 제공한 경고가 실제로 문제가 되지 않으면 컨테이너 취약한 항목(CVIT) 또는 정정 작업을 긍정 오류로 표시합니다. 예를 들어, CVIT가 해제되었지만 스캐너에서 여전히 이와 관련된 문제를 제기하는 경우 이를 가양성으로 표시합니다.

중요사항:
취약성 분석가 및 정정 소유자는 취약성 관리자 작업 공간과IT 정정 작업 공간에서 각각 가양성을 요청할 수 있습니다.

시작하기 전에
필요한 역할: 정정 소유자

프로시저

1. 다음으로 이동 모두 〉 컨테이너 취약성 대응(또는 정정 작업) 〉 모두.
2. 긍정 오류로 표시할 CVIT를 열고 긍정 오류로 표시를 클릭합니다.
   CVIT는 열림 상태여야 합니다.
3. False Positive(긍정 오류) 양식에서 **Additional** information(추가 정보)에 세부 정보를 입력하고 **Request** Approval(승인 요청)을 클릭합니다.
   승인을 위해 요청이 전송되고 CVIT의 상태가 검토 중으로 변경됩니다. 요청자와 승인자 모두 이메일을 통해 알림을 받습니다.

긍정 오류 승인

거짓 양성 승인자는 다른 사용자의 거짓 양성 요청을 승인할 수 있습니다.

중요사항:
에서 긍정 오류 요청을 승인하거나 거부할 수 있습니다 취약성 관리자 작업 공간.

시작하기 전에
필요한 역할: false_positive_approver
클래식 환경에서 예외 및 긍정 오류 요청을 승인할 수도 있습니다.

프로시저

1. 다음으로 이동 모두 〉 컨테이너 취약성 대응 〉 내 승인.
2. 큐에서 요청을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 적절한 설명을 사용하여 요청을 승인하거나 거부합니다.

> **주:**
> 거짓 긍정은 시간 제한이 있을 수 있습니다. 승인자만 종료 날짜를 설정할 수 있습니다.

컨테이너 취약성 대응 정정 작업 및 작업 규칙 개요

분석가 및 정정 전문가가 컨테이너 취약한 항목(CVIT)을 구성하고 대량으로 분석할 수 있도록 정정 작업(CVUL)을 구성합니다. 정정 작업의 기준이 되는 기준은 CVIT가 정정 작업에 자동으로 할당되도록 구성됩니다. 정정 작업을 사용하여 진행 상황을 모니터링하고 정정 프로세스를 보다 효율적으로 추진할 수 있습니다.

컨테이너 취약한 항목 및 정정 작업에서 할당 제거

버전 2.13부터는 사용자 또는 그룹에 잘못 할당되었을 수 있다고 판단되는 CVIT 및 정정 작업 기록에서 CVIT(컨테이너 취약한 항목)의 할당 대상 및 할당 그룹 필드를 직접 지울 수 있습니다.

자세한 내용은 AND 취약한 항목 및 정정 작업에서 할당 제거 문서를 참조하십시오컨테이너 취약한 항목 및 정정 작업에서 할당 제거.

컨테이너 취약한 항목 및 정정 작업에 대한 지연 수 추적

취약한 항목, 애플리케이션 취약한 항목, 컨테이너 취약한 항목 또는 정정 작업이 지연된 횟수를 추적합니다. 지연 수 설정 예약된 작업은 매일 실행되어 지연 수 열에 두 번 이상 지연된 기록에 대한 수를 게시합니다. 기록은 VR, AVR 및 CVR에 대한 여러 지연 모듈에 표시됩니다.

정정 작업 규칙 이해

정정 작업 규칙을 사용하면 컨테이너 취약한 항목을 자동으로 그룹화하고 할당하는 방법을 정의할 수 있습니다. 기본 규칙 취약성 은 취약성을 기반으로 CVIT를 수집하는 기본 시스템에 포함됩니다. 그러나 CVIT에서 액세스할 수 있는 열의 다른 값 집합을 기준으로 그룹화할 수 있습니다. 이러한 값에는 CI(구성 항목), 취약성 항목 등이 포함될 수 있습니다.

활성화 시 사용할 수 있는 취약성 대응 애플리케이션에 포함된 컨테이너 취약성 대응에 대한 작업 규칙이 있습니다.

조건 작성기를 사용하여 여러 조건을 생성할 수 있습니다. 그룹화 기준 섹션에서 필드 쌍을 설정하면 다른 행이 나타납니다. 최대 6개의 그룹화 기준 선택 항목을 가질 수 있습니다. 그룹 할당을 자동화할 수도 있습니다.

예를 들어 컨테이너 취약한 항목을 구성 항목 또는 제품 모델별로 그룹화할 수 있습니다. 심각도가 낮은 취약성 또는 위험도가 낮은 CI에 대해 하나의 작업 규칙을 가질 수 있습니다. 중요한 서버와 회사를 더 많은 위험에 노출시키는 취약성에 대한 또 다른 작업 규칙이 있을 수 있습니다. 사용할 수 있는 옵션에 대한 자세한 내용은 을 참조하십시오 컨테이너 취약성 대응 정정 작업 규칙 생성, 편집 및 삭제 .

회사를 더 큰 위험에 노출시키는 컨테이너 취약한 항목에는 다른 규칙 집합을 사용할 수 있습니다. 정정 작업 이름이 정정 작업 규칙 그룹화 기준 값에 추가되어 새 기록에 대한 짧은 설명을 작성합니다.

컨테이너에 취약한 새 항목이 생성되거나, 임포트되거나, 종결된 후 다시 열리면 해당 항목에 대해 규칙이 평가됩니다. CVIT는 종결된 후 다시 열리거나 규칙이 수동으로 다시 적용되지 않는 한 자동으로 한 번만 평가됩니다.

새 CVIT 또는 다시 열린 각 CVIT에 대해 다음 프로세스가 사용됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 각 정정 작업 규칙에 대해 CVIT는 정정 작업 규칙 필터와 비교됩니다.
- 정정 작업 규칙 조건이 일치하는 각 규칙에 대해 규칙은 CVIT의 선택 항목별 그룹에서 데이터를 가져옵니다. 그룹 이름과 필드를 빌드합니다. 이 경우 고위험: **QID-32342: QID-3242** 요약 (이름: 취약성 ID: 취약성 요약)입니다.

  주:
  간단한 설명 필드는 160자로 제한됩니다. 긴 취약성 요약은 잘립니다.

이 규칙은 CVIT와 동일한 할당 그룹에 할당된 일치하는 미해결 정정 작업이 있는지 확인합니다.

- 작업이 발견되면 CVIT가 열림 상태의 기존 작업에 추가됩니다.
- 열림 상태의 작업을 찾을 수 없는 경우 규칙은 높은 위험: **QID-32342** 작업을 생성하고 CVIT와 동일한 할당 그룹에 할당한 다음 정정 작업에 CVIT를 배치합니다.

서로 다른 종류의 취약성을 그룹화하도록 둘 이상의 정정 작업 규칙을 정의할 수 있습니다. 각 취약성은 정정 작업에 넣기 전에 정정 작업 규칙 조건과 비교되므로 규칙이 너무 많으면 성능에 영향을 줄 수 있습니다. 조건이 중복 정정 작업의 생성을 방지하는 데 도움이 되도록 작업 규칙을 설정합니다.

기본적으로 정정 작업 규칙은 항목을 그룹화할 때 CVIT의 할당 규칙에 의해 설정된 할당 그룹을 사용하고 CVIT와 일치하도록 정정 작업을 할당합니다.

기본 작업 규칙의 일부로 이러한 정정 작업의 할당은 할당 규칙 모듈의 규칙에 의해 제어됩니다. 담당 규칙에 대한 자세한 내용은 취약성 대응 담당 규칙 개요를 참조하십시오.

작업 규칙이 양식 또는 목록 뷰에서 삭제되면 해당 규칙에 따라 생성된 모든 미결 작업을 삭제할 수 있습니다. 오픈 상태가 아닌 작업은 제외됩니다.

정정 작업 규칙 다시 적용

정정 작업 규칙을 변경하려면 정정 작업 규칙 페이지의 다시 적용 버튼을 사용하여 해당 규칙에 의해 생성된 모든 활성 미결 정정 작업에서 변경된 규칙을 다시 실행합니다. 변경된 규칙에 따라 정정 작업을 자동으로 삭제하고 다시 생성합니다.

다시 적용 은 기존 정정 작업만 확인합니다.

다시 적용을 선택하면 다음 메시지가 표시됩니다. 이 정정 작업 규칙을 다시 적용하면 이 규칙에 대한 정정 작업이 삭제되고 다시 생성됩니다. 열림 상태가 아닌 정정 작업은 삭제되지 않습니다.

중요사항:
취약성 관리자와 분석가는 에서 선택한 취약한 항목에 대한 정정 작업 규칙을 평가할 수 있습니다 취약성 관리자 작업 공간. 이 방법은 시간이 오래 걸리는 프로세스인 클래식 UI에서 정정 작업 규칙을 다시 적용하는 것보다 더 효율적입니다. 자세한 내용은 에 있는 기록의 정정 속성 재평가 취약성 관리자 작업 공간 문서를 참조하십시오.

정정 작업 규칙 및 **CVIT** 생성 및 업데이트

검사의 CI가 알려진 취약성과 연결된 경우 CVIT가 생성됩니다. CVIT가 생성되면 일치에 대한 정정 작업 규칙의 조건에 대해 평가됩니다. 기존 정정 작업과 일치하는 항목이 있으면 CVIT가 추가됩니다. 일치하는 정정 작업을 찾을 수 없는 경우 CVIT에 대해 작업이 하나 생성됩니다.

정정 작업 필터링 조건에 캡처된 속성이 CVIT에서 업데이트되거나 변경되면 업데이트된 AVI도 일치에 대한 정정 작업 규칙과 비교하여 평가됩니다. 기존 정정 작업과 일치하는 항목이 있으면 CVIT가 추가됩니다. 일치하는 정정 작업을 찾을 수 없는 경우 CVIT에 대해 작업이 하나 생성됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

상태 롤업 및 롤다운

정정 작업을 오픈 또는 오픈에서 조사 중으로 업데이트하면 새 상태가 연결된 모든 CVIT로 롤다운됩니다. 상태 롤다운은 상태를 변경한 직후에 발생합니다.

CVIT에서 정정 작업으로의 상태 롤업은 작업의 모든 CVIT가 연기됨 또는 종결 고정 상태인 경우에만 발생합니다. 롤업은 취약성에 대한 컨테이너 취약한 항목 값 롤업과 15분마다 실행되는 그룹 예약 작업으로 수행됩니다. 작업이 실행될 때까지 상태가 롤업되지 않습니다. CVIT에서 정정 작업으로 발생하도록 상태를 롤업하려면 모든 CVIT가 동일한 상태여야 합니다.

컨테이너 취약성 대응 정정 작업 규칙 생성, 편집 및 삭제

필터 조건에 따라 컨테이너 취약한 항목(CVIT)을 정정 작업(CVUL)으로 자동 그룹화하는 규칙을 생성할 수 있습니다. 이러한 규칙은 CVIT를 가져오거나 수동으로 생성할 때 자동으로 그룹화합니다.

시작하기 전에

새 규칙을 만들면 기존 데이터에 적용되지 않습니다. 제출한 후에는 새 가져오기에 대해 실행됩니다.

필요한 역할: App-Sec 관리자

프로시저

1. 다음으로 이동 모두 〉 컨테이너 취약성 대응 〉 관리 〉 정정 작업 규칙..
2. 규칙을 열거나 새로 만들기를 선택합니다.
3. 양식의 필드에 내용을 입력하거나 편집합니다.

정정 작업 규칙

필드	설명
이름	작업 규칙의 이름입니다.
활성	작업이 활성 상태인지 여부를 나타냅니다.
설명	규칙에 대한 설명입니다.
대소문자 구분	조건이 대/소문자를 구분하는지 여부를 결정합니다. 주: 기본값은 대/소문자를 구분하지 않습니다.
조건	규칙에 대한 선택적 필터 조건입니다. 기본적으로 (대/소문자 구분 확인란이 선택되지 않음) 작업 규칙 기록 및 양식의 조건 작성기에서 입력하는 검색 텍스트는 대소문자를 구분하지 않습니다. 작업 기록 및 양식에서 대/소문자 구분 검색을 사용하도록 설정할 수 있습니다. 예시 조건은 다음과 같습니다. 취약성 〉 다음과 같음 〉 **VULNENT123451** (알려진 임포트 취약성). 이 취약성이 있는 모든 CVIT가 이 조건과 일치합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
그룹화 기준(최대 6개의 조건 세트 사용 가능)	
다음에서 컨테이너 취약한 항목 그룹화	규칙에서 CVIT를 그룹화하는 데 사용하는 테이블입니다. 트리에서 요소를 선택합니다. ○ 컨테이너 취약한 항목 [sn_vuln_vulnerable_item] ○ 컨테이너 취약한 항목 - Docker 이미지 ○ 컨테이너 취약한 항목 - 컨테이너 취약성 주: 확장된 테이블을 선택하면 해당 확장된 테이블을 사용하는 애플리케이션 취약한 항목에만 사용 필드가 적용됩니다.
필드 사용	규칙이 CVIT를 그룹화하는 데 사용하는 테이블의 필드입니다. 트리에서 조건을 선택합니다.
할당	
정정 작업 할당자	정정 작업을 자동으로 할당하면 취약한 항목을 그룹화하기 위해 그룹화 기준 선택 사항과 함께 할당 선택 항목이 사용됩니다. 필요에 따라 새 작업이 생성되어 각 CVIT가 일치하는 할당 그룹 집합이 있는 작업에 배치됩니다. 이 규칙을 기반으로 생성된 작업의 할당을 자동화하려면 사용 가능한 옵션 중 하나를 선택합니다. ○ 필드별로 그룹화: 그룹화 기준 섹션의 필드 값 사용 섹션에서 사용자 그룹 필드를 선택한 경우 드롭다운 메뉴에 표시됩니다. ○ 사용자 그룹: 조회 목록을 사용하여 정적 사용자 그룹을 선택합니다.

주:
양식 또는 목록 뷰에서 규칙을 삭제하는 경우 해당 규칙에 의해 생성된 모든 미해결 정정 작업을 삭제할 수 있습니다. 오픈 상태가 아닌 그룹은 제외됩니다.

4. 새 규칙에 대해 제출 을 선택합니다.
제출을 선택하면 정정 작업 규칙 목록 (sn_vul_grouping_rule)에 규칙이 표시됩니다. 다음과 같은 상황에서 규칙이 시작됩니다.
   - 새 CVIT가 생성될 때.
   - 다시 적용을 선택하는 경우. 재적용을 선택하면 기존 정정 작업에 대한 작업 규칙만 평가할 수 있습니다.
   - 사용자 또는 시스템에 의해 CVIT가 업데이트되는 경우.

     CVIT가 업데이트되면 작업 규칙이 기존 정정 작업과 일치하는지 평가됩니다. 규칙 검사를 시작하는 몇 가지 일반적인 업데이트는 다음과 같습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 상태가 종결에서 오픈으로 변경되거나 종결에서 조사 중으로 변경되는 경우
- CI(구성 항목)가 변경됩니다.
- 취약성이 변경되었습니다.

시스템은 모든 작업 규칙이 업데이트된 CVIT와 일치하는지 확인합니다. 규칙의 조건이 정정 작업의 조건과 일치하면 일치하는 CVIT가 할당됩니다.

일치하는 항목이 없으면 새 정정 작업이 만들어집니다.

CVIT에서 정정 작업으로의 상태 롤업 및 정정 작업에서 CVIT로의 상태 롤다운에 대한 자세한 내용은 Container Vulnerability Response 정정 작업 및 작업 규칙 개요를 참조하십시오.

정정 작업 규칙의 예는 애플리케이션 취약성 대응 정정 작업 규칙의 예를 참조하십시오.

5. 작업 규칙을 삭제하려면 정정 작업 규칙 목록에서 규칙을 선택하고 삭제를 선택합니다. 다음 메시지가 표시됩니다. ### ## ## ### ## #### #######. ## ## # n## ## #####.

옵션	설명
확인란이 비활성화되었습니다(기본값).	규칙만 삭제합니다. 열림 상태가 아닌 작업은 제외됩니다.
확인란이 선택되었습니다.	정정 작업 규칙을 삭제할 때 오픈 상태의 정정 작업을 포함합니다. 열림 상태의 규칙 및 모든 정정 작업을 삭제합니다.

6. 하나의 옵션을 선택하고 삭제를 선택합니다.

에 대한 자동 종결 규칙 생성 컨테이너 취약성 대응

자동 종결 규칙을 사용하여 설정한 필터 조건에 따라 오래된 컨테이너 취약 항목(CVIT)을 자동으로 종결합니다.

시작하기 전에
필요한 역할: sn_vul.container_manage_auto_close_stale_vi

프로시저

1. 다음으로 이동 모두 〉 컨테이너 취약성 대응 〉 컨테이너 취약한 항목 〉 자동 종결 규칙.

   기본 시스템은 다음과 같은 자동 종결 규칙을 제공합니다. 마지막으로 검사된 컨테이너 취약성: 지난 90일 이내에 보고되지 않은 취약성은 부실 상태로 전환됩니다.

2. 새로 만들기를 선택하여 자동 종결 규칙을 생성합니다.
3. 양식에서 필드에 입력합니다.

필드	값
이름	자동 종결 규칙의 이름입니다.
활성	규칙을 활성화하는 옵션입니다. 활성화되면 필터 기준과 일치하는 탐지를 자동으로 종결합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	값
실행 순서	자동 종결 규칙의 실행을 위한 고유 값입니다. 이 값은 실행 순서를 결정합니다. 기본값은 100입니다.
통합 유형	컨테이너 취약성 통합 주: Prisma Cloud Compute 통합을 사용하여 호스트 취약성을 스캔하려면 취약성 스캐너 통합을 선택합니다.
설명	자동 종결 규칙에 대한 설명입니다.
조건	종결해야 하는 탐지를 식별하는 데 사용되는 필터 조건입니다.

4. 제출을 선택합니다.
   자동 종결 규칙 예약된 작업은 매일 실행됩니다. 지정된 조건에 따라 CVIT를 식별하고 일치하는 CVIT를 부실 상태로 전환합니다. 종결 상태와 부실 상태가 모두 있는 CVIT가 있는 경우 CVIT는 하위 상태가 고정으로 설정된 상태로 종결됩니다.

컨테이너 취약한 항목 및 정정 작업에서 할당 제거

사용자 또는 그룹에 잘못 할당되었다고 판단되는 컨테이너 취약한 항목 및 정정 작업 기록에서 직접 컨테이너 취약한 항목의 할당 대상 및 할당 그룹 필드를 지울 수 있습니다.

워크플로우 개요

컨테이너 취약한 항목(CVIT) 및 정정 작업(CVUL)이 정정 범위에 속하지 않는 것으로 확인되거나 기록이 사용자 또는 소속 그룹에 잘못 할당되었다고 생각되는 경우, CVIT 및 CVUL 기록의 할당 대상 및 할당 그룹 필드에서 본인 또는 그룹을 제거할 수 있습니다.

할당 해제 워크플로우는 작업 공간에서 지원되며, CVIT 및 CVUL의 클래식 뷰와 작업 공간 뷰 모두에서 지원됩니다.

승인을 위해 할당 필드를 지우는 요청을 보낼 수 있습니다. 자세한 내용은 AND 취약한 항목 및 정정 작업에서 할당 제거 문서를 참조하십시오에서 할당 해제 요청 승인 또는 거부 취약성 대응.

- 할당 해제 UI 작업은 종결 또는 해결됨 이외의 모든 상태의 CVIT 및 CVUL 기록에 표시됩니다.

  주:
  CVUL에 대한 필드 지우기 요청이 승인되면 동일한 할당 그룹이 있는 CVIT의 모든 할당 대상 및 할당 그룹 필드가 할당 해제됩니다. CVUL의 CVIT에 연관된 CVUL과 다른 지정 그룹이 있는 경우 할당 해제되지 않습니다. 대부분의 경우 이러한 CVIT는 수동으로 할당되었습니다. 자세한 내용은 AND 취약한 항목 및 정정 작업에서 할당 제거 문서를 참조하십시오컨테이너 취약성 대응 정정 작업 및 작업 규칙 개요.

- UI 작업으로 업데이트하거나 수동으로 업데이트하는 모든 기록은 컨테이너 취약성 대응의 할당되지 않은 모듈에 표시됩니다.

할당 필드를 지우는 방법에 대한 자세한 단계는 을 참조하십시오 취약한 항목 및 정정 작업에서 할당 제거 .

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시스템 속성 및 승인 알림

정정 소유자가 기록에서 할당 해제 를 선택하면 기본적으로 sn_vul.unassign_vr.approval_required 시스템 속성이 승인 플로우를 트리거하고 검토 상태에서 상태 변경 승인 기록을 생성하며, 요청은 승인을 위해 라우팅됩니다. 이 요청은 sn_vul_container.unassign_approver가 있는 사용자의 내 승인 목록에 표시됩니다.

주:
취약성 관리자(sn_vul.vulnerability_admin)는 *sn_vul.unassign_vr.approval_required* 시스템 속성을 **false** 로 설정하여 승인 프로세스를 비활성화할 수 있습니다.

또한 할당 필드가 지워지면 특정 그룹이 할당되도록 시스템 속성의 값을 *sn_vul.default_assignment_group* 변경할 수 있습니다. 예를 들어 사용자가 기록에서 할당 해제 를 클릭하고 검토를 위해 특정 그룹으로 리디렉션하려는 경우 시스템 속성의 값 필드에 선택한 그룹의 시스템 ID를 추가할 수 있습니다.

주:
이 값을 변경하면 할당되지 않은 모든 VIT, AVIT 및 CVIT에 대한 알림이 지정한 그룹으로 전송됩니다.

정정 작업 닫기

애플리케이션 정정 작업과 관련된 문제를 추가 분석 없이 즉시 종결할 수 있는 것으로 확인되면 종결 기능을 사용할 수 있습니다. v2.10 부터 컨테이너 취약성 대응컨테이너 정정 작업에 대한 닫기 버튼이 제거되었습니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
취약성 대응 작업 공간에서 정정 작업은 이전 버전의 취약성 대응에서 이전에 수행한 정정 작업과 동일한 상태를 통해 전환됩니다. 정정 작업의 모든 취약한 항목(VIT)이 닫히면 정정 작업이 비활성 상태로 전환됩니다.

중요사항:
상태 동기화를 사용하도록 설정된 해당 기록의 수명주기 상태를 통해 변경 요청 및 정정 작업을 수동으로 이동할 수 있지만, CHG가 상태를 변경했다고 시스템이 등록하거나 CHG를 추가 또는 정정 작업에서 제거하면 상태 동기화가 수동 개입을 재정의할 수 있습니다. 그러나 변경 요청 상태는 정정 작업을 ## 또는 ### 상태에서 자동으로 이동하지 않습니다.

프로시저

1. 검토를 요청할 기록을 엽니다.
2. 닫기 단추를 선택합니다.
3. 양식의 필드에 적절히 입력합니다.

필드	설명
상태	상태를 종결로 선택합니다.
이유	문제를 종결하는 이유를 입력합니다.
추가 정보	기타 관련 정보를 입력합니다.

4. 제출을 선택합니다.
정정 작업이 종결로 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

IT Operations Management 및 패턴 **Discovery**

검색이 활성화되면 (ITOM) 팀으로부터 Information Technology Operations Management 정보를 받습니다. 검색이 ITOM 활성화되면 컨테이너 취약한 항목(CVIT)을 열 때 Kubernetes 네임스페이스, Kubernetes 클러스터 및 Kubernetes 서비스를 볼 수 있습니다. 그렇지 않으면 Prisma 페이로드 정보를 볼 수 있습니다.

Prisma 페이로드의 이미지 레이블은 Docker 이미지 아래에 키 값 쌍으로 저장됩니다. Prisma 페이로드의 레이블은 cmdb_key_value 테이블에 저장됩니다. 이 기능을 사용할 수 있도록 ITOM 팀에서 cmdb_ci_docker_image 식별 규칙을 제공합니다. Docker 이미지를 열어 관련 항목 목록을 봅니다. 대부분의 항목은 팀에서 ITOM 채웁니다. Docker 이미지의 식별 항목은 값을 키 값 쌍으로 표시하기 위해 제공됩니다.

비즈니스 중요도는 팀에서 ITOM 받은 서비스 중요도 정보에 따라 결정됩니다. 예약된 작업이 실행되어 이미지와 연결된 모든 서비스에서 데이터를 끌어옵니다. 서비스 매핑을 기반으로 비즈니스 중요도를 계산합니다. 위험 점수는 비즈니스 중요도에 따라 달라질 수 있으므로 위험 점수도 이를 기반으로 계산됩니다.

를 위한 분석 및 보고 솔루션 컨테이너 취약성 대응

여기에는 플랫폼 분석 솔루션 다른 ServiceNow AI Platform 제품과 함께 사용하기 위해 사전 패키징된 플랫폼 분석 콘텐츠가 포함됩니다. 이는 플랫폼 분석 솔루션 다양한 차트를 통해 취약성이 어떻게 관리되는지에 대한 노출을 제공합니다.

필요한 역할

이 솔루션과 관련된 역할과 작업은 다음과 같습니다.

- ServiceNow AI Platform 관리자(admin): 이 Analytics and Reporting 솔루션을 설치 및 활성화하고 필요한 변경 사항을 시스템 속성에 적용합니다.
- 플랫폼 분석관리자(pa_admin): 표시기, 세부 항목, 위젯 및 대시보드를 검토합니다. 데이터 수집을 설정 및 시작합니다. 적절한 이해 관계자와 대시보드를 공유합니다.

컨테이너 취약성 대응 대시보드

Analytics and Reporting 솔루션에는 다른 ServiceNow AI Platform 제품과 함께 사용하기 위해 사전 패키징된 퍼포먼스 분석 및 보고 컨텐츠가 포함되어 있습니다. 이를 플랫폼 분석 솔루션 통해 초기 분석 및 탐지에서 억제 또는 정정에 이르기까지 취약성의 볼륨, 성능 및 진행 상황을 추적할 수 있습니다. 할당 그룹, 익스플로잇, 위험 등급 또는 상태별로 보고서를 필터링할 수 있습니다.

필요한 **ServiceNow AI Platform** 역할

- ServiceNow AI Platform 관리자(admin): 이 Analytics and Reporting 솔루션을 설치 및 활성화하고 필요한 변경 사항을 시스템 속성에 적용합니다.
- 퍼포먼스 분석관리자(pa_admin): 표시기, 세부 항목, 위젯 및 대시보드를 검토합니다. 데이터 수집을 설정 및 시작합니다. 적절한 이해 관계자와 대시보드를 공유합니다.

컨테이너 취약성 대응 대시보드에 액세스

대시보드를 열려면 다음으로 이동합니다. 모두 〉 컨테이너 취약성 대응 〉 개요.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

중요사항:

의 컨테이너 취약성 대응버전 2.2부터 이 대시보드는 넥스트 경험 UI에서도 볼 수 있습니다. 새 UI에서 대시보드를 보려면 다음으로 이동합니다. 작업 공간 〉 취약성 관리자 작업 공간 을 클릭하고 대시보드 아이콘을 선택합니다. 역할에 따라 기본 대시보드가 표시됩니다. 다른 대시보드를 보려면 대시보드 이름 옆에 있는 드롭다운을 선택합니다. 자세한 내용은 대시보드 페이지의 취약성 관리자 작업 공간 및 대시보드 페이지의 IT 정정 작업 공간 문서를 참조하십시오.

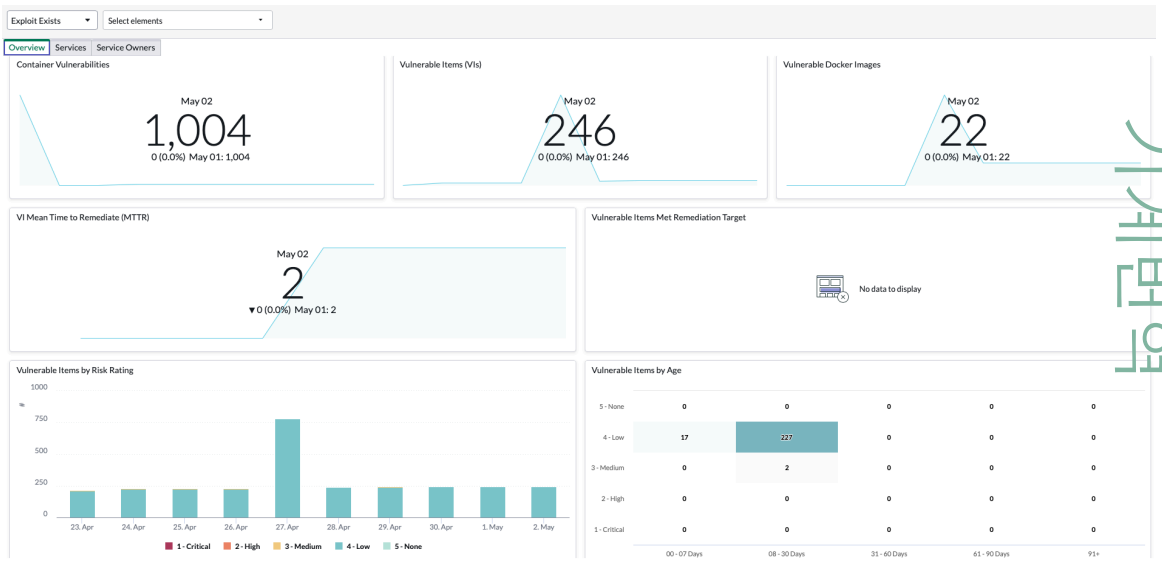
주:

- 새 사용자인 경우 작업 공간에서만 대시보드를 볼 수 있습니다.
- Tokyo에 있는 경우 Next Experience UI에서 대시보드를 볼 수 있지만 일부 기능 손실이 있습니다.

컨테이너 취약성 관리 탭

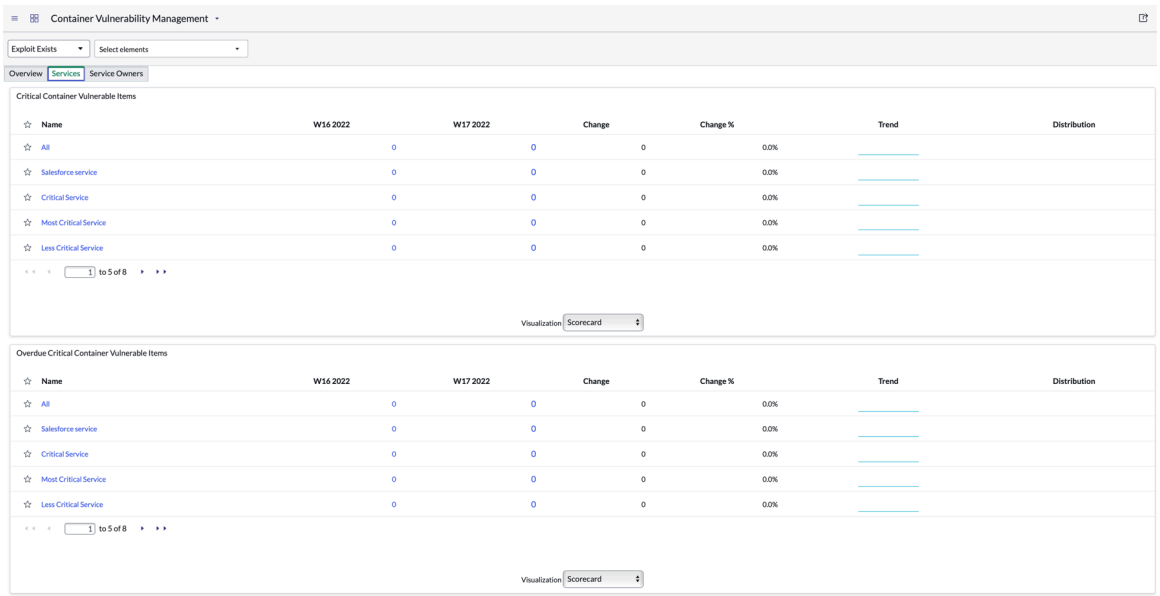
이 대시보드에서는 컨테이너에 있는 취약성을 볼 수 있습니다. 취약성과 관련 데이터를 지역, 기간, 서비스 및 기타 세부 항목별로 볼 수 있습니다.

개요 탭에서는 시스템의 컨테이너 취약성 관리에 대한 전반적인 상태를 제공합니다.

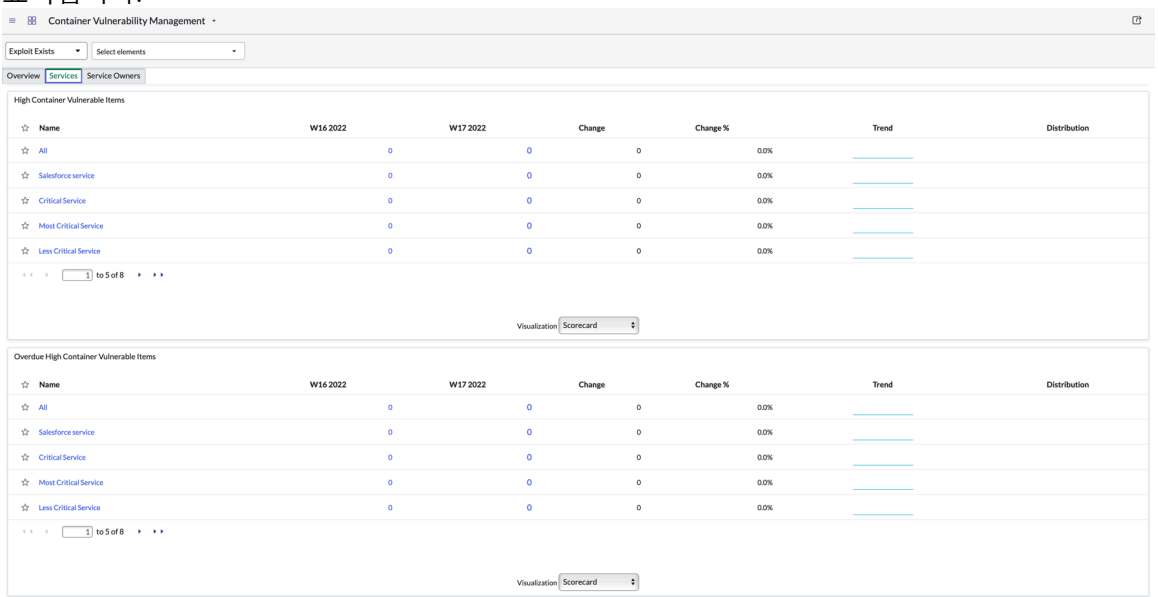


© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

서비스 탭에는 애플리케이션 서비스에 영향을 주는 컨테이너 취약한 항목이

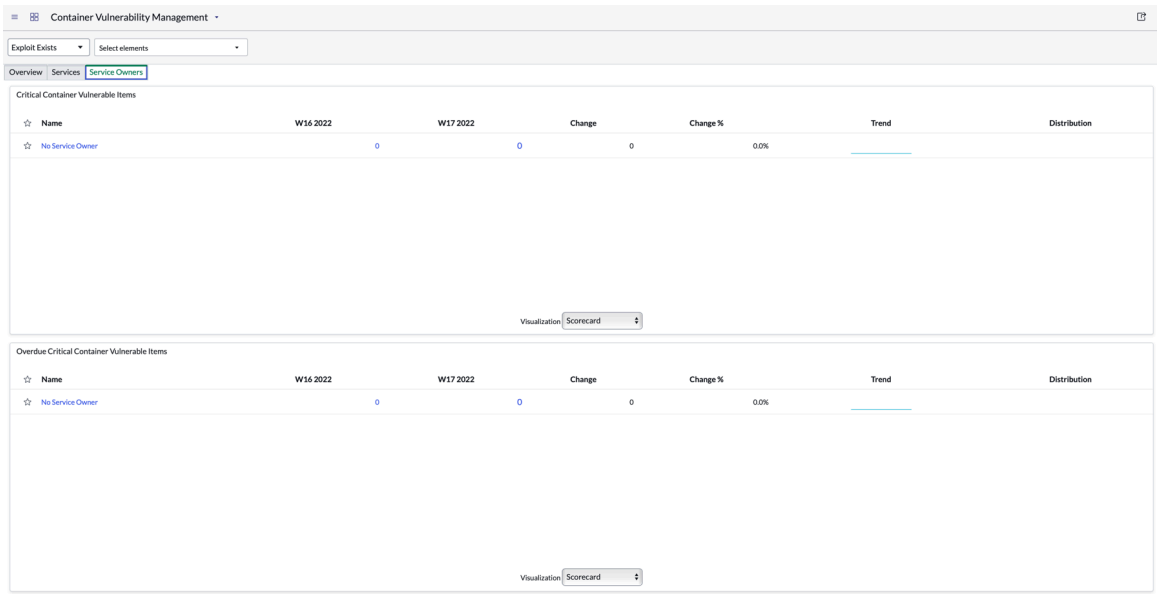


표시됩니다.

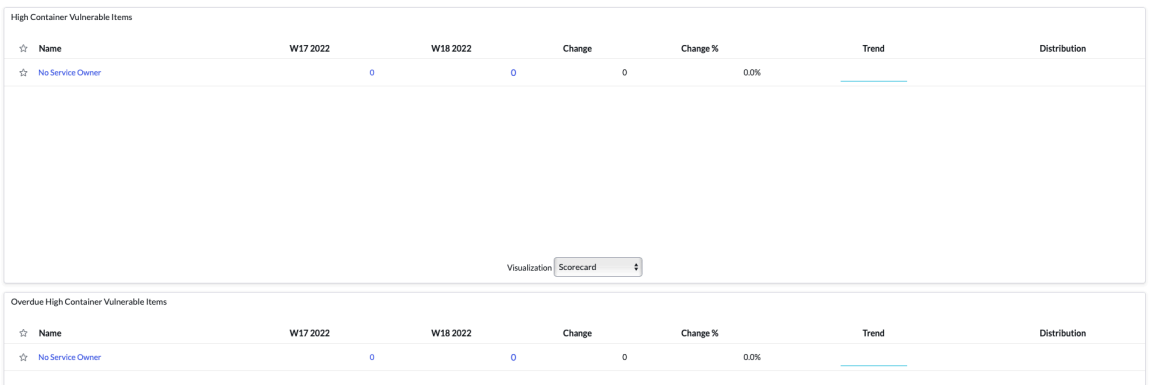


© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

서비스 소유자 탭에는 서비스 소유자에게 영향을 미치는 컨테이너 취약한 항목이



표시됩니다.



세부 항목

- 악용 존재
- 공격 벡터 악용
- 악용 기술 수준
- 정정 대상 상태
- 위험 등급
- 상태
- 할당 그룹

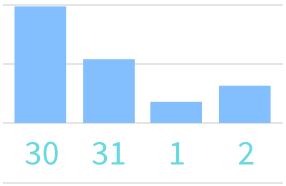
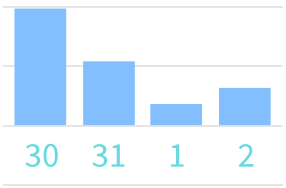
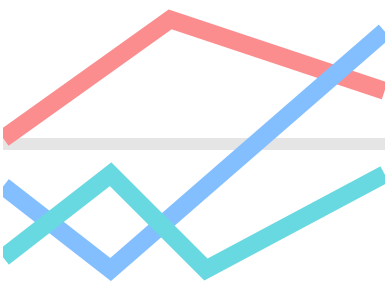
기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

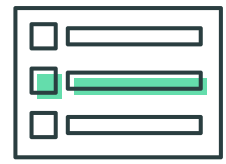
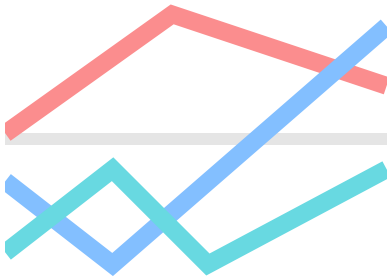
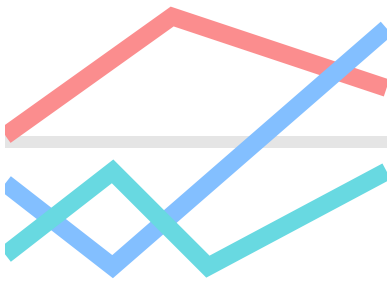
데이터 시각화

이름	유형	설명
컨테이너 취약성	단일 점수	하나 이상의 컨테이너에 취약한 활성 항목과 연결된 컨테이너 취약성 수입니다.
취약한 항목(VI)	단일 점수	활성(종결되지 않은) 컨테이너 취약한 항목 수입니다.
취약한 Docker 이미지	단일 점수	활성 컨테이너 취약한 활성 항목과 연결된 도커 이미지 수입니다.
VI 평균 정정 시간(MTTR)	단일 점수	취약한 항목을 정정(종결)하기 위한 평균 시간으로, 30일 이동 평균으로 표시됩니다.
취약한 항목이 정정 대상 만족	단일 점수	현재 및 이전 분기에서 정정 대상 날짜를 달성한 종결된 컨테이너 취약한 항목의 비율입니다. 정정 대상은 마지막으로 개시된 날짜와 일수로 계산됩니다.

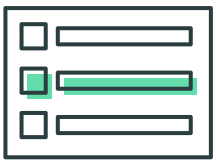
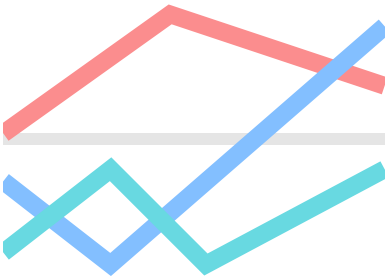
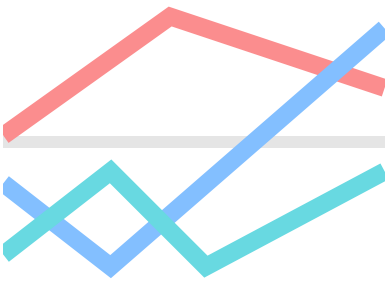
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이름	유형	설명
위험 등급별 취약한 항목	막대 	선택한 시간 범위 동안 위험 등급별로 그룹화된 컨테이너에 취약한 활성 항목 수입니다.
연령별 취약한 항목	막대 	위험 등급 및 기간(일)별로 그룹화된 컨테이너에 취약한 활성 항목 수입니다. **주:** 컨테이너 취약한 항목(CVI)에 대한 기간 및 종결된 기간 계산을 사용자 지정하면 이러한 메트릭이 포함된 퍼포먼스 분석(PA) 보고서가 급격히 증가하거나 감소할 수 있습니다. CVI에 대한 연령 및 종결 연령 계산을 사용자 지정하는 방법에 대한 자세한 내용은 KB1703270 KB 문서를 참조하십시오.
중요한 컨테이너 취약한 항목	목록 및 라인 	서비스별로 그룹화된 위험한 위험 등급의 컨테이너에 취약한 활성 항목 수입니다.

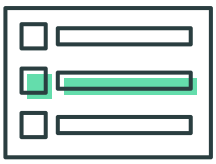
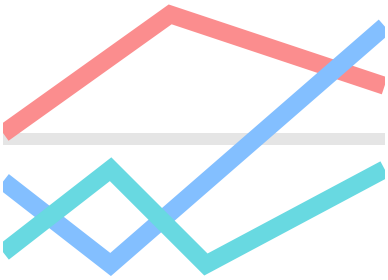
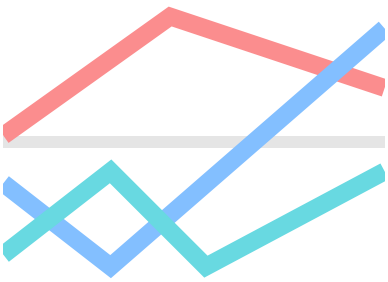
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이름	유형	설명
기한 초과 중요 컨테이너 취약한 항목	목록 및 라인  	위험 등급의 컨테이너에 취약한 활성 항목 수 및 서비스별로 그룹화된 해당 항목의 지난 정정 목표 날짜입니다.
상위 컨테이너 취약한 항목	목록 및 라인 	서비스별로 그룹화된 높은 위험 등급의 컨테이너에 취약한 활성 항목 수입니다.

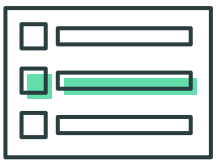
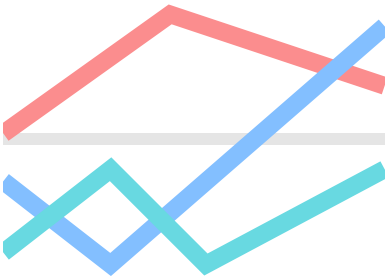
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이름	유형	설명
기한 초과 상위 컨테이너 취약한 항목	목록 및 라인  	높은 위험 등급의 활성 취약한 항목 수 및 서비스별로 그룹화된 해당 항목의 지난 정정 목표 날짜입니다.
중요한 컨테이너 취약한 항목	목록 및 라인 	서비스 소유자별로 그룹화된 위험한 위험 등급의 컨테이너에 취약한 활성 항목 수입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이름	유형	설명
기한 초과 중요 컨테이너 취약한 항목	목록 및 라인  	위험 등급의 컨테이너에 취약한 활성 항목 수 및 서비스 소유자별로 그룹화된 해당 항목의 지난 정정 목표 날짜입니다.
상위 컨테이너 취약한 항목	목록 및 라인 	서비스 소유자별로 그룹화된 높은 위험 등급의 컨테이너에 취약한 활성 항목 수입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이름	유형	설명
기한 초과 상위 컨테이너 취약한 항목	목록 및 라인  	높은 위험 등급의 활성 취약한 항목 수 및 서비스 소유자별로 그룹화된 해당 항목의 지난 정정 목표 날짜입니다.

에 대한 집계 보고서 프레임워크 컨테이너 취약성 대응

집계된 보고서 프레임워크를 사용하면 성능 향상을 위해 복잡하고 실행 시간이 긴 즉석 쿼리가 포함된 데이터에 대한 보고서를 만들 수 있습니다.

집계된 보고서 프레임워크는 다음을 통해 성과를 개선합니다.

- 더 적은 리소스를 사용하고 보고서를 더 빠르게 렌더링합니다.
- 데이터 집계와 집계 및 세부 항목 재사용(그룹화 기준)
- 데이터베이스에 대한 쿼리 줄이기

100만 개가 넘는 CVIT(컨테이너 취약한 항목)가 있는 경우 표준 보고서와 함께 집계된 보고서 프레임워크를 사용합니다.

필요한 역할

이 솔루션과 관련된 역할과 작업은 다음과 같습니다.

- ServiceNow AI Platform관리자(admin): 이 플랫폼 분석 솔루션을 설치 및 활성화하고 시스템 속성을 필요에 따라 변경합니다.
- 퍼포먼스 분석 관리자(pa_admin): 집계, 위젯 및 대시보드를 검토합니다. 데이터 수집을 설정 및 시작합니다. 적절한 이해 관계자와 대시보드를 공유합니다.
- 관리자(sn_vul_cmn.admin): 집계를 생성합니다.
- VR write(sn_vul_cmn.write): 집계 및 집계된 결과에서 데이터를 편집합니다.
- VR 읽기(sn_vul_cmn.read): 집계 및 집계된 결과의 데이터를 검토합니다.
- 취약성 분석가(sn_vul.vulnerability_analyst): 집계된 결과를 검토합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관련 정보

- 소스 데이터에 대한 집계 구성
- 여러 집계를 동시에 실행
- 동시에 실행할 수 있는 집계 수 구성
- 집계를 사용하여 보고서 생성

컨테이너 취약성 대응 참조

와 컨테이너 취약성 대응함께 설치되는 테이블, 역할 및 속성에 대한 정보가 포함된 참조 항목입니다.

컨테이너 취약성 대응 앱과 함께 설치되는 구성요소

컨테이너 취약성 대응 애플리케이션을 활성화하면 테이블, 사용자 역할, 예약된 작업을 포함하여 여러 유형의 구성요소가 설치됩니다.

주:
애플리케이션 파일 테이블에는 이 애플리케이션과 함께 설치되는 구성요소가 나열됩니다. 이 테이블에 액세스하는 방법에 대한 지침은 애플리케이션과 함께 설치되는 구성요소 찾기 를 참조하십시오.

이 기능에 대한 데모 데이터를 사용할 수 있습니다.

v2.11 of 부터 컨테이너 취약성 대응가장 자주 사용되는 시스템 속성에 애플리케이션 내에서 액세스할 수 있습니다 컨테이너 취약성 대응 . 이러한 시스템 속성을 보려면 다음으로 이동합니다. 모두컨테이너 취약성 대응속성.

컨테이너 취약성 대응 앱과 함께 설치되는 역할

컨테이너 취약성 대응가 활성화되면 역할이 추가됩니다.

가상 사용자와 세분화된 역할을 사용하여 사용자와 그룹이 애플리케이션에서 보고 수행할 취약성 대응 수 있는 것을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할의 초기 할당에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당. 세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

주:

업그레이드 고객인 경우 v10.3 이전 권한인 sn_vul.vulnerability_read 및 sn_vul.vulnerability_write 권한으로 할당한 사용자 및 그룹에 대한 액세스는 변경되지 않습니다. 사용자와 그룹은 변경할 때까지 이러한 역할을 계속 할당받은 상태로 유지됩니다. 그러나 v10.3부터는 사용자 및 그룹이 애플리케이션에서 수행하고 볼 수 있는 것을 보다 세밀하게 제어하기 위해 세분화된 역할을 할당하는 취약성 대응 것을 선호할 수 있습니다. 이러한 역할을 관리하는 방법에 대한 개요 및 자세한 내용은 해당 의 가상 사용자 및 세분화된 역할 관리 취약성 대응문서를 참조하십시오취약성 대응 가상 사용자 및 세분화된 역할.

역할 제목**[name]**	설명
V2.10: sn_vul_container.delete	소스 기록을 삭제합니다. sn_v 및 sn_vul_container.delete_vi 포함합니다.
sn_vul_container.ci_manager	일치하지 않는 구성 항목(CI)의 관리합니다.
sn_vul_container.configure_integrations	컨테이너 통합을 구성합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

역할 제목[name]	설명
sn_vul_container.configure_vi_granularity	컨테이너 취약한 항목 세분성을
sn_vul_container.create_vi	컨테이너에 취약한 항목을 수동 수 있습니다.
sn_vul_container.delete_vi	수동으로 생성된 컨테이너 취약 삭제할 수 있습니다.
sn_vul_container.exception_approver	컨테이너 취약한 항목의 예외, 종결을 승인합니다. sn_vul.view_manager_works 포함합니다. v2.3부터 이 역할에 대한 세분 sn_vul_container.read_all이 저 컨테이너 취약한 항목 및 정정 사용자와 그룹에 할당된 컨테이 항목 및 정정 작업에 액세스할
sn_vul_container.false_positive_approver	컨테이너 취약한 항목을 긍정 종결하는 것을 승인하거나 거부 sn_vul.view_manager_works 포함합니다.
sn_vul_container.manage_assignment_rules	컨테이너 취약한 항목 담당 규 업데이트합니다.
sn_vul_container.manage_auto_close_stale_vi	부실 컨테이너 취약 항목 자동
sn_vul_container.관리_자동_예외_규칙	예외 규칙 관리(만들기/읽기/ 삭제)
sn_vul_container.manage_normalized_severity	매핑을 업데이트하여 심각도를 있습니다.
sn_vul_container.manage_permissions	사용자에게 컨테이너 취약성 대 할당할 수 있습니다.
sn_vul_container.manage_remediation_targ...	컨테이너 정정 대상 규칙을 정 업데이트합니다.
sn_vul_container.manage_risk_score_confi...	위험 점수 정의 및 업데이트 컨 취약한 항목에 대한 계산기, 위 취약성 롤업 계산기입니다.
sn_vul_container.모두 읽기	모든 컨테이너 취약한 항목 및 볼 수 있습니다. sn_vul.view_manager_works 포함
sn_vul_container.read_assigned	클래식 UI 또는 IT 정정 작업 공 사용자 또는 사용자의 그룹에 컨테이너 취약한 항목을 볼 수 sn_vul.view_rem_workspace 포함합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

역할 제목**[name]**	설명
	중요사항: 의 취약성 대응v24.0부터 sn_vul_container.read_as 역할은 에 액세스할 수 있 작업 공간권한이 있습니다
sn_vul_container.read_assignment_rules	컨테이너 취약한 항목을 볼 수 담당 규칙.
sn_vul_container.read_auto_exception_rule	예외 규칙 읽기
sn_vul_container.read_discovered_이미지	검색된 항목을 볼 수 있습니다
sn_vul_container.read_integrations	통합 실행의 결과를 볼 수 있습
sn_vul_container.read_normalized_severity	정규화된 심각도 매핑을 볼 수
sn_vul_container.read_remediation_target...	정정 대상 규칙을 볼 수 있습니
sn_vul_container.read_risk_score_configu...	컨테이너 취약한 항목에 대한 계산기, 위험 규칙 및 취약성 를 볼 수 있습니다.
sn_vul_container.remediation_owner	할당된 컨테이너 취약한 항목을 씁니다. 취약성 기록은 이 역할 사용자도 읽을 수 있습니다.
sn_vul_container.update_assigned_to	컨테이너 취약한 항목의 할당을 수 있습니다. sn_vul_container.write_all 또 sn_vul_container.write_assign 필요합니다.
sn_vul_container.update_assignment_group	컨테이너 취약한 항목에 대한 업데이트할 수 있습니다. sn_vul_container.write_all 또 sn_vul_container.write_assign 필요합니다.
sn_vul_container.update_state입니다.	취약한 항목의 상태를 업데이트 있습니다. sn_vul_container.write_all 또 sn_vul_container.write_assign 필요합니다.
sn_vul_container.vulnerability_admin	제품에 대한 컨테이너 취약성 규칙, 통합 등을 구성합니다.
sn_vul_container.vulnerability_analyst	모든 컨테이너 취약한 항목의 모니터링합니다.
sn_vul_container.write_all	모든 컨테이너 취약한 항목 및 업데이트할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

역할 제목**[name]**	설명
sn_vul_container.write_assigned	나 또는 내 그룹에 할당된 컨테 항목 또는 정정 작업을 업데이 있습니다.
sn_vul_container.read_watch_topic	컨테이너 취약성에 대한 주시 수 있습니다.
sn_vul_container.create_watch_topic	컨테이너 취약성에 대한 감시 수 있습니다.
sn_vul_container.edit_watch_topic	컨테이너 취약성에 대한 감시 수 있습니다.
sn_vul_container.관리_예외_구성	예외 관리 구성을 관리할 수 있

컨테이너 취약성 대응 앱과 함께 설치되는 테이블

(CVR)이 컨테이너 취약성 대응 활성화되면 테이블이 추가됩니다.

테이블	설명
컨테이너 이미지 찾기 sn_vul_container_image_findings	관련 취약성, 이미지 계층, Docker 이미지, 이미지 리포지토리 및 검색된 이미지에 대한 정보를 저장합니다. 의 컨테이너 취약성 대응v2.11.3부터 찾은 결과가 표시되는 경로를 볼 수도 있습니다.
컨테이너 이미지 계층 sn_vul_container_image_layer	각 이미지 레이어의 정보를 포함합니다. 이미지는 컴퓨팅 시스템에서 컨테이너를 만들 수 있는 실행 코드가 있는 정적 파일입니다.
컨테이너 이미지 패키지 sn_vul_container_image_package	취약성이 있는 패키지에 대한 정보를 제공합니다. 이진 패키지 상세 정보도 쉼표로 구분된 값으로 제공됩니다. 의 컨테이너 취약성 대응v2.11.3부터는 패키지 URL(PURL)도 볼 수 있습니다.
컨테이너 취약한 항목 sn_vul_container_image_vulnerable_item	각 발견 사항과 해당 취약성에 대한 상세 정보를 포함합니다. 의 컨테이너 취약성 대응v2.11.3부터 컨테이너로 실행되는 이미지의 마지막 스캔 날짜에 대한 정보도 볼 수 있습니다.
취약성 항목(v2.11.3) sn_vul_entry	CVE의 심각도에 대한 정보와 Prisma에서 보낸 추가 정보를 제공합니다.
탐색한 컨테이너 이미지 sn_vul_container_image	이미지 ID, Docker 이미지 및 이미지 리포지토리에 대한 정보를 제공합니다. 또한 계층 정보를 저장하고 검색된 이미지와 연결합니다. v2.11.3 of 부터 컨테이너 취약성 대응도커 이미지의 이미지 다이제스트와 컨테이너 및

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테이블	설명
	레지스트리로 실행되는 이미지의 마지막 스캔 날짜에 대한 정보도 제공합니다.
매핑 찾기 sn_vul_container_finding_m2m_vul_item	컨테이너 이미지 결과와 컨테이너 취약한 항목(CVIT)의 M2M 관계입니다.
취약한 항목 자동 종결 sn_vul_container_image_auto_close_config	부실 컨테이너 이미지 찾기를 종결하고 상태를 CVIT에 롤업하는 방법에 대한 정보를 포함합니다.
컨테이너 이미지 취약성 키 sn_vul_container_image_vulnerability_keys	컨테이너 이미지 결과에서 CVIT를 생성하기 위한 세분성 구성을 포함합니다.
Docker 관련 서비스 sn_vul_container_m2m_ci_services	컨테이너 이미지와 관련된 모든 비즈니스 서비스를 포함합니다.
VR 컨테이너 수 sn_vul_container_vr_container_counts	지난 90일 동안 컨테이너 이미지에서 분리된 컨테이너 인스턴스의 롤링 평균을 포함합니다.
컨테이너 정정 작업 항목 sn_vul_container_m2m_vul_group_item	CVIT와 컨테이너 정정 작업 간의 M2M 테이블입니다.
컨테이너 정정 작업 sn_vul_container_vulnerability	컨테이너 정정 작업을 포함합니다.
컨테이너 정정 작업 메니페스트 sn_vul_container_rt_manifest	정정 작업에 대한 업데이트는 예약된 작업에 따라 이 매니페스트 테이블을 사용하여 수행됩니다.

컨테이너 취약성 대응 앱과 함께 설치되는 예약된 작업

컨테이너 취약성 대응가 활성화되면 예약된 작업이 추가됩니다.

주:
애플리케이션 파일 테이블에는 이 애플리케이션과 함께 설치되는 구성요소가 나열됩니다. 이 테이블에 액세스하는 방법에 대한 지침은 애플리케이션과 함께 설치되는 구성요소 찾기 를 참조하십시오.

이 기능에 대한 데모 데이터를 사용할 수 있습니다.

예약된 작업	설명
기존 컨테이너 VI를 자동 예외 규칙과 연결	자동 예외 규칙을 기존 컨테이너 취약 항목(CVIT)과 자동으로 연결합니다.
컨테이너 취약한 항목 연기 만료 확인	컨테이너 취약한 항목 또는 컨테이너 취약성이 만료된 경우(그리고 1주일 후 만료되는 경우) 알림을 보냅니다.
취약성 대응 컨테이너 수	매일 실행하여 컨테이너의 90일 이동 평균을 계산하는 sn_vul_container_vr_container_counts 테이블을 채웁니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예약된 작업	설명
(애플리케이션 - 컨테이너에 대한 취약성 대응 및 구성 준수)	
CVIT 자동 종결	자동 종결 구성에 정의된 조건과 일치하는 컨테이너 취약성 항목을 자동으로 종결합니다. 상태가 '수정됨'으로 변경됩니다.
CVIT에 대한 비즈니스 중요도 계산	모든 활성 CVIT를 처리하고 CVIT의 Docker 이미지의 영향을 받는 서비스를 기반으로 비즈니스 중요도 필드를 업데이트합니다.
Docker 이미지가 연결되지 않은 취소 CVIT 닫기	연결된 CI가 없는 CVIT를 자동으로 만료합니다. 해당 상태는 종결로 설정되고 하위 상태는 취소됨으로 설정됩니다.
컨테이너 정정 작업에 대한 관련 VI 수 계산	컨테이너 정정 작업 기록의 개수를 계산합니다.
컨테이너 취약한 항목 값을 취약성 및 그룹에 롤업	컨테이너 취약한 항목에 대한 취약성 및 그룹 롤업을 계산합니다. 주: 의 컨테이너 취약성 대응v2.10부터 예약된 작업이 개선되어 멀티스레딩 기능이 있는 백그라운드 작업을 생성할 수 있습니다. 이 업그레이드에는 작업을 여러 개의 더 작은 하위 작업으로 분할하는 작업이 포함되며, 이러한 작업은 병렬로 또는 동시에 실행됩니다. 이렇게 수정하면 여러 기록을 동시에 처리할 수 있으므로 전체 작업 속도가 크게 향상됩니다.

컨테이너 취약성 대응 용어집

에 고유한 용어와 개념에 컨테이너 취약성 대응대해 알아봅니다.

주요 용어

컨테이너

애플리케이션이 한 컴퓨팅 환경에서 다른 컴퓨팅 환경으로 원활하고 안정적으로 실행될 수 있도록 코드와 코드의 모든 의존성을 패키지화하는 소프트웨어 단위입니다.

컨테이너 이미지

컴퓨팅 시스템에서 컨테이너를 만들 수 있는 실행 코드가 포함된 정적 파일입니다. 컨테이너 이미지는 변경할 수 없으므로 어떤 환경에서도 일관되게 배포할 수 있습니다.

클러스터

컨테이너화된 애플리케이션을 실행하는 노드라고 하는 작업자 머신 집합입니다.

Docker

서버와 클라우드에서 애플리케이션 컨테이너를 생성, 배포 및 관리하는 소프트웨어입니다.

Docker 이미지

코드, 필수 라이브러리, 구성 등을 포함하는 템플릿 파일입니다. 이 파일은 컨테이너 인스턴스를 시작하는 데 사용됩니다. 계층화된 파일 시스템의 조합으로 구성됩니다.

Dockerfile

여러 레이어를 추가하여 컨테이너 이미지를 생성하는 지침이 포함된 텍스트 파일입니다. 예를 들어 기본 Ubuntu, Nginx 및 앱 코드의 계층화입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Docker 작성

Docker로 복잡한 애플리케이션을 정의하고 실행하기 위한 도구입니다. Compose를 사용하면 단일 파일에 다중 컨테이너 애플리케이션을 정의할 수 있습니다.

Docker 컨테이너

Docker 컨테이너는 Docker 이미지에서 시작되는 런타임 인스턴스입니다.

이미지 계층

레이어는 이미지를 수정한 것입니다. Dockerfile의 명령으로 표시됩니다. 레이어는 기본 이미지에 순서대로 적용되어 최종 이미지를 만듭니다.

이미지 리포지토리

태그 또는 버전이 다른 Docker 이미지 컬렉션입니다.

이미지 레이블

이미지와 함께 메타데이터로 저장되는 키-값 쌍 집합입니다.

네임스페이스

Kubernetes에서 단일 클러스터 내에서 자원 그룹의 격리를 지원하는 데 사용하는 추상화입니다.

포드

실행 중인 컨테이너 집합(컨테이너 위에 있는 또 다른 추상화)입니다.

레지스트리

이미지 리포지토리를 포함하는 호스팅된 서비스입니다.

서비스

포드 집합에서 실행되는 애플리케이션을 네트워크 서비스로 노출하는 추상적인 방법입니다.

태그

태그는 지정된 이미지 리포지토리의 Docker 이미지에 적용되는 레이블입니다. 태그는 리포지토리의 다양한 이미지가 서로 구별되는 방법입니다.

컨테이너 취약 항목(CVIT)은 외부 공급업체 취약성 통합 임포트 중에 자동으로 생성됩니다.

컨테이너 취약한 항목 양식 필드

CVIT의 할당 그룹, 할당 대상 필드 및 메모를 제외한 다른 모든 필드는 읽기 전용입니다.

필드	설명
번호	이 기록에 대해 자동으로 생성된 CVIT 식별자입니다.
소스	취약성을 식별한 스캐너입니다.
위험 등급	취약한 항목을 중요, 높음, 중간, 낮음 및 없음으로 구분하는 정량화된 위험 점수 입니다.
위험 점수	CVIT가 환경에 미치는 위험의 계산된 양입니다.
정정 대상 규칙	정정 목표 날짜가 계산되는 정정 대상 규칙입니다.
정정 대상	처음 식별된 이후 CVIT를 정정해야 하는 날짜입니다. 해당하는 경우에만 나타납니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
정정 상태	CVIT의 정정 상태입니다.
취약성	이 애플리케이션 취약한 항목과 관련된 취약성 ID입니다.
Docker 이미지	코드, 필수 라이브러리, 구성 등이 포함된 템플릿 파일입니다. 이 파일은 컨테이너 인스턴스를 시작하는 데 사용됩니다. 계층화된 파일 시스템의 조합으로 구성됩니다.
탐색한 컨테이너 이미지	각 이미지 ID에 대한 고유 기록입니다.
기본 이미지	필수 운영 체제와 라이브러리를 포함하는 컨테이너화된 애플리케이션을 생성하는 데 사용되는 기본 이미지입니다. 이는 Docker와 같은 환경에서 애플리케이션을 빌드하고 사용자 지정하기 위한 시작점 역할을 합니다.
이미지 클러스터	머신 러닝에서 유사한 이미지를 클러스터링하거나 리포지토리에서 이미지를 컨테이너로 클러스터링하는 등 다양한 컨텍스트에서 사용되는 관련 이미지 그룹입니다.
이미지 네임스페이스	레지스트리 내에서 컨테이너 이미지를 구성하고 격리하여 여러 팀 또는 프로젝트에서 별도의 컬렉션을 유지 관리할 수 있도록 하는 데 사용됩니다.
상태	이 필드는 생성 시 기본적으로 열림 으로 설정됩니다. 상태가 매핑되는 방법에 대한 자세한 내용은 을 참조하십시오 애플리케이션 취약한 항목(AVI) 상태 .
할당 그룹	이 CVIT에서 작업하도록 선택한 그룹입니다.
담당자	이 CVIT에서 작업하는 선택된 할당 그룹의 개인입니다. App-Sec 관리자가 수동으로 추가하거나 편집할 수 있습니다.
작성됨	CVIT가 생성된 날짜 및 시간입니다.
마지막으로 열림	CVIT가 재개된 가장 늦은 날짜 및 시간입니다.
업데이트됨	CVIT가 마지막으로 수정된 날짜 및 시간입니다.
첫 발견(v2.12.1)	취약성이 처음 발견된 날짜입니다. v2.12.1부터는 처음 검색된 정확한 날짜와 시간을 볼 수 있으므로 명확성을 보장하고 다른 시간대를 설명할 수 있습니다. 처음 발견된 날짜 및 시간 상세 정보를 채우려면 통합을 다시 실행해야 합니다.
마지막 발견 (v2.12.1)	취약성이 마지막으로 발견된 날짜입니다. v2.12.1부터는 마지막으로 발견된 정확한 날짜와 시간을 볼 수 있으므로 명확성을 보장하고 다른 시간대를 설명할 수 있습니다. 마지막으로 찾은 날짜 및 시간 상세 정보를 채우려면 통합을 다시 실행해야 합니다.
해결 날짜 (v2.12.1)	취약성이 해결된 날짜입니다. v2.12.1부터는 해결된 정확한 날짜 및 시간을 볼 수 있으므로 명확성을 보장하고 여러 시간대를 고려할 수 있습니다. CVIT가 워크플로우의 일부로 해결되면 해결 날짜가 채워집니다.
마지막으로 열림 (v2.12.1)	취약성이 마지막으로 열린 날짜입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	v2.12.1부터는 마지막으로 열린 정확한 날짜와 시간을 볼 수 있으므로 명확성을 보장하고 다른 시간대를 설명할 수 있습니다. 예약된 작업이 *Add default values for last_opened_dt_tm from last _opened* 이 필드의 데이터를 채웁니다. 요청 시 한 번만 실행해야 합니다.
취약성	
요약	취약성에 대한 설명입니다.
심각도	이 취약성의 정규화된 심각도 수준입니다. 심각도 맵은 NVD(국가 취약성 데이터베이스) 및 ServiceNow 외부 공급업체 통합과 함께 제공됩니다.
취약성 점수(v3)	CVSS(공통 취약성 평가 시스템) v3 점수입니다.
취약성 점수(v2)	CVSS v2 점수입니다.
익스플로잇 존재	예, 하나 이상의 익스플로잇이 이 취약한 항목과 관련된 취약성과 관련된 경우 가능합니다.
익스플로잇 공격 벡터	이 취약한 항목과 관련된 취약성을 악용한 가장 취약한 공격 벡터입니다.
익스플로잇 기술 수준	이 취약한 항목과 연관된 취약성을 악용하는 데 필요한 가장 낮은 기술 수준입니다.
게시 날짜	취약성이 게시된 날짜입니다.
마지막으로 수정됨	취약성이 마지막으로 수정된 날짜입니다.
위협	위협에 대한 관련 정보입니다. 취약한 항목 기록에서 끌어옵니다. **주:** 여기에서 변경한 내용은 취약한 항목 기록을 업데이트합니다.
정정 참고 사항	취약한 항목 기록에서 가져온 위협에 대한 관련 솔루션입니다.
메모	
작업 메모	관련 정보입니다. 정보를 추가하려면 작업 메모의 텍스트 상자를 선택합니다.
이미지 결과	컨테이너 이미지에서 취약성을 검사한 결과입니다.
요청된 승인	CVIT에 대해 제기된 승인 요청입니다.
상태 변경 승인	CVIT에 대해 발생한 상태 변경 승인 요청입니다.

CVIT의 연령 계산:

- CVIT 목록의 기간 열에는 CVIT가 활성화되는 기간(형식: 일 HH:MM:SS)이 표시됩니다. 종결된 CVIT의 경우 연령 값은 0입니다.
- CVIT 목록의 종결 기간 열에는 CVIT가 종결되기 전에 활성 상태인 기간(형식: 일수 HH:MM:SS)이 표시됩니다. 종결 상태가 아닌 CVIT의 경우 종결 기간 값은 0입니다.

Age 및 Age 종결 기간의 계산을 사용자 지정하는 방법에 대한 자세한 내용은 KB1703270 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Prisma Cloud Compute 구성 양식

Prisma Cloud Compute 구성 양식은 Prisma Cloud Compute 통합 모듈 내에서 액세스할 수 있습니다.

Prisma Cloud Compute 구성 양식을 보려면 다음으로 이동합니다. 모두 〉 **Prisma Cloud Compute** 통합 〉 관리 〉 구성.

Prisma Cloud Compute 구성

필드	설명
통합 인스턴스	새 통합 인스턴스의 이름입니다. 인스턴스를 만들거나 조회 아이콘을 클릭하여 기존 인스턴스를 선택할 수 있습니다.
API 기준 URL	Prisma Cloud Compute와 통합할 URL입니다.
사용자 이름	Prisma Cloud Compute에 액세스하기 위한 사용자 이름입니다.
암호	Prisma Cloud Compute에 액세스하기 위한 암호입니다.
Mid Server	로컬 네트워크의 서버에서 Windows 서비스 또는 UNIX 디먼으로 실행되는 Java 애플리케이션입니다. MID 서버를 사용하면 인스턴스와 외부 애플리케이션, 데이터 소스 및 서비스 간의 데이터 이동 및 ServiceNow 통신을 수행할 수 있습니다.
프로젝트 사용	프로젝트를 구성하는 옵션입니다. 이 확인란을 선택하면 구성 페이지에서 프로젝트를 선택하고 프로젝트별 상세 정보를 채우도록 구성된 프로젝트를 기반으로 통합을 실행할 수 있습니다. **주:** 이 확인란을 선택하면 프로젝트 구성 탭이 활성화됩니다. 다음을 클릭하여 프로젝트 구성을 진행합니다.

예외 요청 양식

에서 애플리케이션의 컨테이너 취약성 대응정책 예외 관리 기능을 정책 및 준수 관리 사용하여 GRC 정책 예외를 요청합니다.

Prisma Cloud Compute 구성 양식을 보려면 다음으로 이동합니다. 모두 〉 컨테이너 취약성 대응 〉 컨테이너 취약한 항목 (또는 정정 작업)>모두로 설정하고 예외를 요청할 항목 또는 그룹을 엽니다.

예외 요청 양식

필드	설명
정책	예외를 요청하는 취약성 관리 정책입니다.
컨트롤 목적	선택한 정책과 연결된 통제 목표입니다. 정책을 선택하지 않으면 모든 통제 목표가 나열됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예외 요청 양식

필드	설명
유효 기간(시작)	예외가 시작되는 날짜입니다. 기본값은 현재 날짜입니다. 이 날짜는 과거일 수 없습니다.
유효 기간	정책 예외가 만료되고 취약한 항목 또는 그룹의 상태가 연기됨에서 미결로 변경되는 날짜입니다. 주: 정책 예외가 유효한 일 수는 정책 및 준수에서 정책에 대해 설정한 최대 예외 기간(일) 을 초과할 수 없습니다. 자세한 내용은 정책 만들기를 참조하세요.
이유	예외를 요청하는 이유입니다.
근거	이 요청이 수행되는 이유와 관련된 상세 정보입니다. 정정 소유자가 이 필드를 입력해야 합니다.

예외 규칙 양식

컨테이너 취약한 항목 그룹(CVIT)의 특정 조건에 대한 예외를 자동으로 요청하는 규칙(예: 이러한 CVIT의 취약성 심각도를 기반으로 하는 조건이 있는 규칙)을 생성합니다. 이 규칙을 사용하면 승인된 규칙 조건과 일치하는 경우 신규 및 기존 CVIT를 자동으로 연기할 수 있습니다.

예외 규칙 양식을 보려면 다음으로 이동하십시오. 모두 〉 컨테이너 취약성 대응 〉 관리 〉 예외 규칙.

예외 규칙 양식

필드	설명
이름	예외 규칙의 이름입니다.
유효 기간(시작)	CVIT를 연기하기 위해 이 규칙이 활성화되는 날짜입니다.
유효 기간(종료)	정정 작업에서 새 CVIT 수락을 중지하는 날짜입니다.
이유	이 예외 규칙을 생성하는 이유입니다.
할당 그룹	지연된 CVIT를 추적하기 위해 생성된 정정 작업이 할당된 그룹입니다.
추가 정보	요청자가 승인자에게 제공하려는 추가 정보입니다. 이 정보는 정정 작업의 설명 필드에 채워집니다.
조건	CVIT를 처리하는 동안 정의할 수 있는 CVIT에 대한 필터 조건입니다.
기존 데이터에서 실행	이 규칙을 처음 실행할 때 기존 데이터에 대해 이 규칙을 실행할 수 있도록 하는 옵션입니다.
워크플로우 스테이지	예외 규칙의 현재 승인 상태입니다.
상태	예외 규칙의 상태입니다.
실행 순서	각 예외 규칙에 대한 고유한 순서입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예외 규칙 양식

필드	설명
지연 기한	VUL 및 CVIT가 지연될 때까지의 날짜입니다. 이 날짜에 생성된 VUL이 닫히고 모든 CVIT가 그룹 외부로 이동하며 그룹 규칙이 다시 적용됩니다.

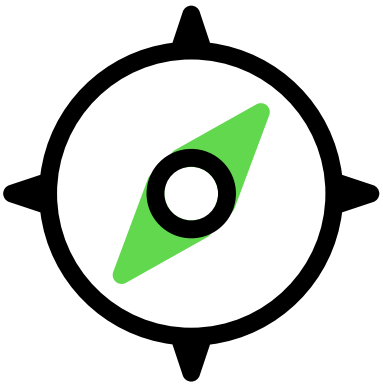
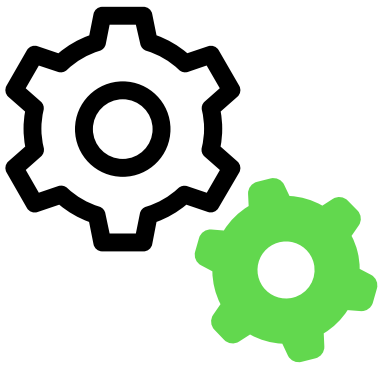
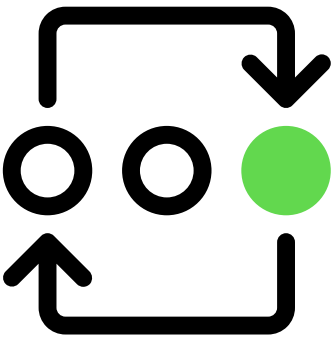
구성 준수

이 ServiceNow# 구성 준수 애플리케이션은 외부 공급업체 구성 검사 애플리케이션과의 통합에서 검사 결과를 집계하는 보안 구성 평가(SCA) 애플리케이션입니다. 를 사용하여 구성 관리 데이터베이스(CMDB)구성 준수 문제의 우선순위를 지정할 수 있습니다. 는 구성 준수 IT 변경 관리 프로세스와 긴밀하게 통합되어 미준수 구성을 정정합니다.

스토어에서 앱 요청

ServiceNow Store 웹 사이트를 방문하면 사용 가능한 모든 앱을 확인하고 스토어에 요청을 제출하는 방법에 대한 정보를 참조할 수 있습니다. 출시된 모든 앱의 누적 릴리스 정보는 ServiceNow Store 버전 기록 릴리스 정보 를 참조하십시오.

구성 준수

탐색	설정, 설치 및 구성	통합
		
Configuration Compliance 개념 및 기능에 대해 알아보기	구성 준수 구성	다른 애플리케이션과 통합하여 구성 준수 확장

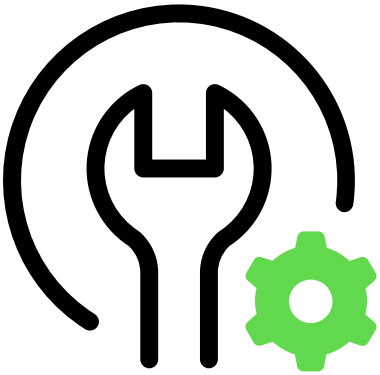
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

구성 준수

Vulnerability Response
작업 공간 사용

취약성 관리자, IT 정정 및 취약성 평가 작업 공간에서 구성 문제를 모니터링, 관리 및 정정하는 방법을 알아봅니다.

정정

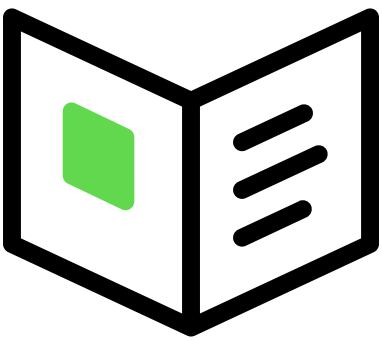


구성 준수를 사용하여 미준수 자산을 정정하는 방법 알아보기

분석 및 보고서

Configuration Compliance에서 보고서 및 대시보드 보기

참조



필드, 테이블 및 속성과 같은 구성 준수 구성요소에 대한 상세 정보 가져오기

문제 해결 및 도움 받기

- Security Operations 리소스 라이브러리
- Security Operations 커뮤니티
- 알려진 오류 포털에서 알려진 오류 문서 검색
- 연락처 고객 서비스 및 지원

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

구성 준수 탐색

외부 공급업체 보안 구성 평가(SCA) 통합에서 얻은 테스트 결과를 사용하여 보안 또는 회사 정책을 준수하는지 확인합니다. 미준수 구성 항목을 식별하고, 우선순위를 지정하고, 정정합니다.

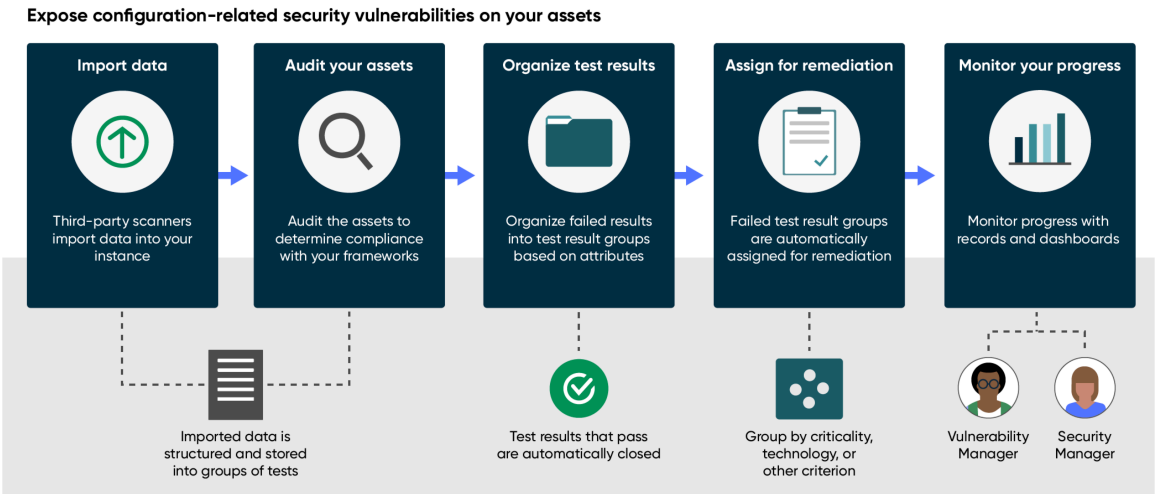
주:
의 구성 준수v14.9부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v14.9 이전 용어	용어 **v14.9** 이상
테스트 결과 그룹	정정 작업
그룹 규칙	정정 작업 규칙
정책	테스트 그룹

구성 준수의 정의

이 ServiceNow# 구성 준수 애플리케이션을 사용하면 사용자 환경에서 가장 중요한 구성 관련 취약성의 우선순위를 지정하고 빠르고 효율적으로 정정할 수 있습니다. 구성 준수 에서 구독을 통해 사용할 수 있습니다 ServiceNow# Store.



구성 준수의 주요 기능

에서 ServiceNow AI Platform# 를 구성 관리 데이터베이스(CMDB) 사용하여 가장 중요한 구성 관련 보안 취약성을 노출하고 수정할 수 있습니다. 위험 감소가 가장 큰 활동에 정정 자원을 집중하십시오. 보안, IT 및 비즈니스 프로세스 이해 관계자 전반에 걸쳐 정정 프로세스를 간소화합니다. 이 애플리케이션에는 구성 준수 다음과 같은 주요 기능이 포함되어 있습니다.

- 지원되는 외부 공급업체 통합을 사용하면 정책, 테스트, 권한이 부여된 소스 및 기술을 자동으로 임포트할 수 있습니다. 지원되는 통합에 대한 자세한 내용은 을 참조하십시오 구성 준수 통합 .
- 정책과 테스트를 구성 항목(자산)의 상관관계를 지정하여 구성 관련 취약성을 식별하고 자산이 정책과 통제를 준수하는지 확인하는 데 도움이 됩니다.
- 모든 자산에서 구성 평가, 할당 및 정정을 통합합니다.
- 구성 스캔 콘텐츠는 선도적인 SCA(Secure Configuration Assessment) 에코시스템 통합 애플리케이션에서 임포트할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 구성 결과, 테스트 실패는 정정 전문가 기술 세트 및 책임 영역을 기반으로 자동으로 그룹화 및 라우팅할 수 있습니다. 변경 관리와의 긴밀한 통합과 지능형 워크플로우를 통해 그룹 간에 원활한 작업 핸드오프가 가능합니다.
- ()GRC 애플리케이션과 함께 ServiceNow 거버넌스, 리스크 및 컴플라이언스 사용할 경우 의 구성 준수 구성 테스트를 해당 GRC 컨트롤로 롤업할 수 있습니다.
- 향상된 변경 관리를 사용하여 IT 구성 준수 에 대해 미리 채워진 변경 요청을 직접 생성하여 추가 자원이 필요한 정정 작업에 도움을 줄 수 있습니다.
- 대시보드를 사용하여 정정 작업, 준수 테스트 및 정책 기록에 대한 정정 상태 메트릭을 봅니다.

구성 준수 사용자

구성 준수 활동에는 여러 수준의 관리가 포함될 수 있습니다.

- 시스템 관리자
- 취약성 관리자
- 취약성 관리자
- 취약성 분석가
- 규정 준수 관리자

구성 준수 작업에는 다음과 같은 역할이 포함됩니다.

- sn_vulc.admin - 읽기, 쓰기, 삭제 가능
- sn_vulc.write — 읽고 쓸 수 있습니다.
- sn_vulc.remediation_owner - 할당된 기록을 읽고 업데이트할 수 있습니다.

> **주:**
> 모든 사용자에게 itil 역할이 할당되면 sn_vulc.remediation_owner 역할도 자동으로 할당됩니다.

- sn_vulc.read — 읽을 수 있음

구성 준수과 보안 운영

및 Qualys Vulnerability Integration 가 Tenable Vulnerability Integration 설치되면 에 액세스할 취약성 대응 수 있게 됩니다. 이러한 통합은 여러 번 배포할 수 있습니다. 각 배포에서 소싱된 데이터가 식별되고 의 단일 인스턴스에서 GRC사용할 수 있습니다.

에 사용 가능한 버전 **Yokohama**

릴리스 버전	릴리스 정보
구성 준수 v15.4	구성 준수 릴리스 정보 . 호환성 정보는 KB0856498 Vulnerability Response 호환성 매트릭스 및 릴리스 스키마 변경을 참조하십시오. 애플리케이션 활성화에 대한 자세한 내용은 을 참조하십시오 애플리케이션 설정, 설치 및 구성 구성 준수 .

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

구성 준수 임포트된 데이터

애플리케이션은 구성 준수 외부 공급업체 통합에서 정책, 테스트, 권한 있는 소스 및 테스트 결과를 임포트하여 볼 수 있도록 모듈에 저장합니다.

주:
의 구성 준수v14.9부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v14.9 이전 용어	용어 **v14.9** 이상
테스트 결과 그룹	정정 작업
그룹 규칙	정정 작업 규칙
정책	테스트 그룹

지원되는 통합

외부 공급업체 통합은 구성 평가 결과, 테스트 그룹, 테스트, 기술, 권한이 부여된 소스 및 테스트 결과를 애플리케이션으로 임포트합니다 구성 준수 . 취약성 관리자 또는 취약성 분석가는 이 데이터를 사용하여 자산의 구성 관련 취약성을 식별하고 대응할 수 있습니다.

지원되는 통합에 대한 자세한 내용은 다음 문서를 참조하십시오 구성 준수 통합.

테스트 그룹

테스트 그룹은 권한이 부여된 문서 및 테스트 기록과 관련이 있습니다. 구성 테스트 그룹은 테스트 그룹을 정의합니다. 테스트 그룹은 일반적으로 Windows, Oracle 데이터베이스, Cisco IOS와 같은 기술 클래스에 부합하며 종종 기본 산업 표준에서 파생됩니다. 조직의 필요에 맞게 테스트 그룹을 수정할 수 있습니다. 단일 구성 테스트는 여러 테스트 그룹에 속할 수 있습니다.

통합	설명
Qualys Vulnerability Integration	테스트 그룹이 검색되고 오전 1:00에 예약된 작업인 **Qualys PC** 정책에 의해 통제 ID가 채워집니다. 다음으로 이동하여 예약된 작업을 볼 수 있습니다. **Qualys** 취약성 통합 〉 기본 통합 〉 **Qualys PC** 정책. 주: 통합을 수동으로 실행하려는 경우 먼저 **Qualys PC** 정책을 실행합니다.
Tenable Vulnerability Integration	예약된 작업 Tenable.io 준수 결과 통합이 정책을 임포트합니다. 통합을 수동으로 실행하기로 선택한 경우 무시된 자산이 평가 데이터로 조정될 때까지 다음 순서로 통합을 실행합니다. • Tenable.io 자산 통합 • Tenable.io 준수 결과 통합 • Tenable.io 준수 결과 백필 통합

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

통합	설명
	• Tenable.io 자산 통합 • Tenable.io 준수 결과 백필 통합 정책 기록을 보려면 다음으로 이동합니다. 모두 〉 구성 준수 〉 테스트 그룹. 테스트 그룹 기록을 올바르게 식별하고 생성하기 위해 테스트 그룹에 대한 감사 정보가 임포트되어 간단한 설명 필드에 표시됩니다.

테스트

테스트는 컴퓨팅 자산의 스캔을 구성하는 데이터 기록 라이브러리입니다. 구성 테스트는 기술 자산 클래스를 관리하는 방법을 정의합니다.

구성 준수 테스트는 외부 공급업체 통합 애플리케이션이 취약성 유형별로 자산을 그룹화하는 데 사용하는 메커니즘입니다. Qualys와 같은 일부 타사 VA 스캔 솔루션에는 권한이 부여된 소스의 정책 및 "프레임워크"에 매핑되는 매우 큰 테스트 라이브러리(최대 8,000개)가 있습니다.

테스트에는 일대다, 예상 대 실제 등 많은 값이 있을 수 있습니다. 테스트란 규정을 준수하지 않는 소프트웨어 또는 하드웨어 자산의 클래스를 식별하는 데 사용할 수 있는 것입니다. 예를 들면 릴리스 또는 하드웨어 번호입니다.

통합	설명
Qualys Vulnerability Integration	예약된 작업인 **Qualys PC Controls**가 테스트를 검색합니다. 다음으로 이동하여 예약된 작업을 볼 수 있습니다. **Qualys** 취약성 통합 〉 기본 통합 〉 **Qualys PC** 컨트롤. 주: 통합을 수동으로 실행하도록 선택하는 경우 **Qualys PC** 정책 다음에 **Qualys PC** 컨트롤을 실행합니다.
Tenable Vulnerability Integration	예약된 작업 Tenable.io 준수 결과 통합은 구성 테스트(테스트)를 임포트합니다. 통합을 수동으로 실행하기로 선택한 경우 무시된 자산이 평가 데이터로 조정될 때까지 다음 순서로 통합을 실행합니다. • Tenable.io 자산 통합 • Tenable.io 준수 결과 통합 • Tenable.io 준수 결과 백필 통합 • Tenable.io 자산 통합 • Tenable.io 준수 결과 백필 통합 구성 테스트 기록을 보려면 다음으로 이동합니다. 구성 준수 〉 테스트. 기록에서 임포트한 데이터는 간단한 설명 필드와 정정

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

통합	설명
	상태, 설명 및 정정 탭에 표시됩니다. 데이터는 인용, 정책 및 테스트 결과 관련 링크에도 표시됩니다.

기술

타사 취약성 스캐너에서 분석을 위한 소프트웨어 및 하드웨어 구성 항목의 테스트 그룹을 생성하는 데 사용하는 기술 중 하나는 이를 기술별로 구성하는 것입니다. 기술은 정책과 연결된 OS, 네트워크 장치, 데이터베이스 및 앱의 가져온 라이브러리입니다. 테스트에는 서로 다른 기술에 대한 여러 구현이 있습니다. 정정은 기술별로 다릅니다.

테스트에 적용 가능한 기술을 확인하여 컨트롤을 적용할 수 있는 소프트웨어 또는 하드웨어 자산의 종류를 더 잘 이해할 수 있습니다. 컨트롤에 적용할 수 있는 기술의 예로는 CentOS 7.x, Windows 8.1, Windows 2016 Server 등이 있습니다. 기술 목록은 읽기 전용이며 애플리케이션에 정의된 Qualys Cloud Platform 기술과 일치합니다.

데이터베이스 관련 구성 평가를 위해서만 기술을 임포트합니다. *db_type* 임포트의 (비어 있지 않은 경우)는 기술을 생성하는 데 사용됩니다. 구성 테스트 기록, 테스트 결과 기록, 정책 기록 등의 기술 섹션에 채워진 기술을 봅니다. 구성 준수 〉 지원 데이터 〉 기술.

권한이 부여된 소스

구성 준수 는 테스트에 대한 취약성 경보를 생성할 때 권한이 부여된 소스와 인용을 사용합니다. 신뢰할 수 있는 소스는 일반적으로 "NIST 800-53 버전 3(2009) 3: 2009, SA-4″와 같은 게시된 산업 표준의 섹션에 매핑됩니다.

주:
Qualys Vulnerability Integration에서는 이 조합을 프레임워크라고 합니다.

권한이 부여된 출처와 인용(의무라고도 함)은 외부 공급업체 취약성 스캐너에서 임포트됩니다.

권한이 부여된 소스 기록에는 컴퓨터 보안 분야의 전문가가 알려준 알려진 소프트웨어 및 하드웨어 구성 문제에 대한 정보에 대한 참조가 포함되어 있습니다. 보안 정책 및 절차에 대한 요구 사항을 정의합니다. 구성 테스트는 인용을 통해 여러 권한이 부여된 출처를 참조할 수 있습니다. 권위 있는 출처는 감사를 준비하기 위해 주어진 표준에 대한 준수에 대해 보고할 수 있습니다.

통합	설명
Qualys Vulnerability Integration	예약된 작업인 **Qualys PC** 정책 상세 정보는 권한이 부여된 소스와 인용을 검색합니다. 다음으로 이동하여 이 예약된 작업을 볼 수 있습니다. **Qualys** 취약성 통합 〉 기본 통합 〉 **Qualys PC** 정책 상세 정보. **주:** 통합을 수동으로 실행하려는 경우 **Qualys PC** 정책다음에 **Qualys PC** 정책 상세 정보를 실행합니다.
Tenable Vulnerability Integration	예약된 작업 Tenable.io 준수 결과 통합은 인용 데이터의 일부로 권한이 부여된 소스를 임포트합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

통합	설명
	통합을 수동으로 실행하기로 선택한 경우 무시된 자산이 평가 데이터로 조정될 때까지 다음 순서로 통합을 실행합니다. • Tenable.io 자산 통합 • Tenable.io 준수 결과 통합 • Tenable.io 준수 결과 백필 통합 • Tenable.io 자산 통합 • Tenable.io 준수 결과 백필 통합 데이터는 구성 테스트 기록의 인용 관련 링크에 표시됩니다.

테스트 결과

구성 준수 는 테스트 결과를 계산하지 않지만 외부 공급업체 통합의 일부로 가져옵니다. 에서 볼 수 구성 준수있게 되면 정정 작업을 사용하여 정정됩니다. 자세한 내용은 구성 준수 상관 문서를 참조하십시오.

통합	설명
Qualys Vulnerability Integration	다음 방법 중 하나로 테스트 결과를 검색할 수 있습니다. 예약된 작업인 **Qualys PC** 결과가 테스트 결과를 검색합니다. 다음으로 이동하여 이 예약된 작업을 볼 수 있습니다. **Qualys** 취약성 통합 〉 기본 통합 〉 **Qualys PC** 결과. 주: 통합을 수동으로 실행하려는 경우 **Qualys PC** 정책 및 **Qualys PC** 정책 상세 정보 다음에 **Qualys PC** 결과를 실행합니다. **Qualys PC** 결과 임포트는 통합 상세 정보 탭의 *`Start Time`* 매개변수를 사용합니다. 다른 구성 준수 모든 임포트는 에 *`Start Time`*관계없이 사용 가능한 모든 데이터를 가져옵니다. **Qualys PC** 결과 가져오기가 완료되면 가져오기 종료 계산을 트리거하는 이벤트가 발생합니다. 자세한 내용은 구성 준수 상태 문서를 참조하십시오. 또는 V14.5부터 다음 통합을 실행하여 테스트 결과를 검색할 수도 있습니다. • Qualys PCRS 정책 호스트 통합 - 각 정책의 호스트 ID를 검색합니다. 이 예약된 작업을 보려면 Qualys 취약성 통합 > 기본 통합 > Qualys PCRS 정책 호스트 통합으로 이동합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

통합	설명
	주: 통합을 수동으로 실행하려는 경우 Qualys PC 정책 및 Qualys PC 정책 상세 정보 다음에 Qualys PCRS 정책 호스트 통합을 실행합니다. 이 예약된 작업이 완료되면 Qualys PCRS 테스트 결과 통합이 자동으로 트리거됩니다. • Qualys PCRS 테스트 결과 통합 - 각 호스트 ID에 대한 테스트 결과를 검색합니다. 이 예약된 작업을 보려면 Qualys 취약성 통합 > 기본 통합 > Qualys PCRS 테스트 결과 통합으로 이동합니다. 주: 통합을 수동으로 실행하는 경우 Qualys PC 정책, Qualys PC 정책 상세 정보 및 Qualys PCRS 정책 호스트 통합 후 Qualys PCRS 테스트 결과 통합을 실행합니다. 이 통합은 통합 상세 정보 탭의 시작 시간 매개변수를 사용합니다.
Tenable Vulnerability Integration	예약된 작업 Tenable.io 준수 결과 통합은 테스트 결과를 임포트합니다. 통합을 수동으로 실행하기로 선택한 경우 무시된 자산이 평가 데이터로 조정될 때까지 다음 순서로 통합을 실행합니다. • Tenable.io 자산 통합 • Tenable.io 준수 결과 통합 • Tenable.io 준수 결과 백필 통합 • Tenable.io 자산 통합 • Tenable.io 준수 결과 백필 통합 구성 테스트 기록을 보려면 다음으로 이동합니다. 구성 준수 〉 테스트 결과. 기록의 임포트한 데이터가테스트 및 구성 항목 필드에 표시됩니다. 데이터는 예상 값, 실제 값 및 정정 탭에도 표시됩니다. 정 정 작업 및 테스트 결과 이력 관련 링크가 채워집니다.

구성 준수 검색

구성 준수 데이터는 외부 공급업체 SCA 스캐너 애플리케이션에서 임포트됩니다. 소프트웨어 및 하드웨어 테스트 그룹을 데이터 레코드로 구조화하여 평가를 신속하게 수행합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
의 구성 준수v14.9부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v14.9 이전 용어	용어 **v14.9** 이상
테스트 결과 그룹	정정 작업
그룹 규칙	정정 작업 규칙
정책	테스트 그룹

임포트가 완료되면 임포트 종료 작업을 나타내는 이벤트가 전송됩니다. 모든 활성 정정 작업에 대해 다음 작업이 수행됩니다.

- 실패한 결과가 있는 해결된 정정 작업은 구현 대기 중 상태로 돌아갑니다.
- 모든 결과가 통과된 정정 작업은 종결됩니다.
- 활성 정정 작업에 있는 테스트 결과의 상태가 업데이트됩니다.
- 결과가 활성 정정 작업의 일부인지 여부를 나타내는 플래그가 업데이트됩니다.

구성 준수 상관

구성 준수 미준수 문제의 정정을 지원하기 위해 우선순위 지정 및 테스트 결과 그룹화 (정정 작업으로)를 제공합니다.

주:
의 구성 준수v14.9부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v14.9 이전 용어	용어 **v14.9** 이상
테스트 결과 그룹	정정 작업
그룹 규칙	정정 작업 규칙
정책	테스트 그룹

자산 중심 우선순위 지정

구성 스캔을 통해 많은 수의 결과가 생성될 수 있습니다. 위험을 최대한 줄이기 위해 결과의 우선순위를 지정합니다. 우선순위에는 구성 테스트 중요도와 자산 중요도가 모두 포함됩니다. 구성 테스트 결과 우선순위는 0-100 규모의 위험 점수로 표현됩니다. 계산기 그룹은 위험 점수를 계산하며 사용자 지정할 수 있습니다.

외부 공급업체 임포트가 완료되면 는 구성 준수 이벤트를 전송하여 임포트 종료 작업을 나타냅니다. 모든 활성 결과 그룹에 대해 다음 작업이 수행됩니다.

- 실패한 결과가 있는 해결된 정정 작업은 구현 대기 중 상태로 돌아갑니다.
- 전달된 모든 결과가 종결된 정정 작업입니다.
- 활성 정정 작업에 있는 테스트 결과의 상태가 업데이트됩니다.
- 결과가 활성 정정 작업의 일부인지 여부를 나타내는 플래그가 업데이트됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

정정 작업 우선순위

테스트 결과가 둘 이상의 그룹에 속하는 경우 테스트 결과의 상태는 우선순위에 따라 파생됩니다.

구성 테스트 양식의 상태 및 해결 필드와 테스트 결과 양식의 결과 필드는 다음 우선 순위에 따라 계산됩니다.

주:

그룹 구성원 자격 우선순위는 항목이 구성 테스트를 통과하지 못한 항목에만 적용됩니다. 통과된 항목은 항상 종결-고정 상태입니다.

결과 값에 따라 상태가 결정됩니다. 종결-고정 및 종결-취소됨 상태의 정정 작업은 무시됩니다. 항목 상태는 해당 항목이 속한 다른 모든 정정 작업의 상태로부터 계산되거나 항목에 대한 다른 그룹이 없는 경우 미결로 설정됩니다.

Order of Precedence for Test Results belonging to multiple Test Result Groups						
Group A	**Group B**					
	Open	**Under Investigation**	**Awaiting Implementation**	**Resolved**	**Deferred**	**Closed-Invalid**
Open	Open	Under Investigation	Awaiting Implementation	Resolved	Deferred	Closed-Invalid
Under Investigation	Under Investigation	Under Investigation	Awaiting Implementation	Resolved	Deferred	Closed-Invalid
Awaiting Implementation	Awaiting Implementation	Awaiting Implementation	Awaiting Implementation	Resolved	Deferred	Closed-Invalid
Resolved	Resolved	Resolved	Resolved	Resolved	Deferred	Closed-Invalid
Deferred	Deferred	Deferred	Deferred	Deferred	Deferred	Closed-Invalid
Closed-Invalid	Closed-Invalid	Closed-Invalid	Closed-Invalid	Closed-Invalid	Closed-Invalid	Closed-Invalid

정정 작업 생성

구성 준수 정정 작업은 수동으로 생성됩니다.

정정 작업을 생성하고 채우는 방법에는 두 가지가 있습니다.

- 정정 작업 모듈에서 테스트 결과 탭을 자동으로 채우는 필터를 사용합니다.

  이 방법은 사용하려는 필터링을 알고있을 때 유용합니다. 예를 들어, 보통 이상의 중요도이고, Windows 기반 인프라에 영향을 미치며, SAP 공급망 애플리케이션에만 적용되는 모든 실패한 테스트 결과를 캡처합니다.

- 테스트 결과 목록에서 테스트 결과를 선택하고 선택한 행에 대해 수행할 동작... 메뉴에서 정정 작업을 만듭니다.

  이 방법은 쉽게 필터링할 수 없는 결과나 정정할 테스트 결과를 지정하려는 상황에 적합합니다. 예를 들어, 공통점이 없는 이상값이 있습니다.

주:
테스트 결과 목록에서 정정 작업을 생성한 후 나중에 해당 정정 작업에 필터를 사용하기로 결정한 경우, 원래 항목이 제거되고 필터 결과로 바뀝니다.

그룹화되지 않은 테스트 결과

그룹화되지 않은 테스트 결과 에는 활성(종결되지 않은) 정정 작업의 구성원이 아닌 모든 테스트에 통과하지 못한 테스트 결과가 포함됩니다. 이 모듈은 임포트할 때마다 그리고 테스트 결과가 정정 작업에서 추가되거나 제거될 때마다 업데이트됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대해 검색된 항목 구성 준수

자산은 호스트 및 테스트 결과 통합을 사용하여 임포트될 때 CI 조회 규칙을 사용하여 구성 항목(CI)과 자동으로 일치합니다. 검색된 항목을 통해 자산 식별이 의 CI에 매핑되는 방식을 볼 수 있습니다 CMDB.

검색된 항목은 일치,일치하지 않음 또는 재분류된 것으로 간주됩니다. 식별된 CI가 일치함 상태입니다.

잠재적인 일치 문제를 쉽게 찾을 수 있도록 CI와 일치하는 CI 조회 규칙이 **CI** 일치 규칙 필드에 나타납니다.

주:
CI 일치 규칙 필드 지원은 통합에만 Qualys 사용할 수 있습니다.

일치하는 항목이 없으면 의 CMDB#### ## *CI* 클래스 [sn_sec_cmn_unmatched_ci],[cmdb_ci_unclassed_hardware] 또는 [cmdb_ci_incomplete_ip]에 CI가 작성됩니다. 원래 일치하지 않는 CI가 재분류된 경우 검색된 항목 기록이 해당 상태를 반영하도록 업데이트됩니다. 자세한 내용은 일치하지 않는 CI를 참조하고 자세한 내용은 일치하지 않는 구성 항목을 보고 재분류 하십시오.

기본적으로 보안 운영 〉 **CMDB** 〉 검색된 항목 모듈에는 일치하지 않는 구성 항목이 나열됩니다. 필터를 제거하여 임포트에서 검색된 모든 항목을 볼 수 있습니다.

검색된 항목의 필드에 대한 설명은 검색된 항목 양식 필드를 참조하십시오.

에 대한 검색된 항목의 **CI** 변경 내용 구성 준수

sn_sec_cmn.update_on_ci_change의 기본값은 true입니다. 따라서 검색된 항목에 대한 CI(구성 항목)가 업데이트되면 테스트 결과도 업데이트됩니다.

주:
의 구성 준수v14.9부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v14.9 이전 용어	용어 **v14.9** 이상
테스트 결과 그룹	정정 작업
그룹 규칙	정정 작업 규칙
정책	테스트 그룹

테스트 결과의 외부 ID가 업데이트되고 위험 점수, 할당 규칙, 정정 작업 규칙, 정정 대상 규칙이 다시 평가됩니다. 테스트 및 CI가 동일한 테스트 결과가 있는 경우 테스트 결과는 기존 테스트 결과로 업데이트되고 현재 테스트 결과는 ## ## invalidCI로 종결됩니다. 이에 따라 작업 메모가 추가됩니다.

기존 테스트 결과에 대해 CI를 업데이트하지 않으려면 속성을 false로 설정하십시오. 이 경우 CI가 변경되면 새 테스트 결과가 생성되고 기존 테스트 결과는 ### CI로 종결됩니다.

에 대해 일치하지 않는 검색된 항목을 일치시킵니다. 구성 준수

일치하지 않는 검색 항목을 조정하기 위한 예약 작업을 생성합니다. 테스트 결과가 생성되면 생성 시 추가된 CI(구성 항목)가 오래된 것일 수 있습니다.

시작하기 전에
필요한 역할: 관리자

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보
CMDB의 정보가 변경되면 일치하지 않는 CI 정보가 조정되지 않습니다. 조정하려면 CMDB가 최신 CI로 업데이트될 때 일치하지 않는 상태에 있는 테스트 결과에 CI 조회 규칙을 적용합니다. 요청 시 예약 작업이 실행되어 일치하지 않는 상태의 검색된 항목에 대한 CI 일치 규칙을 다시 적용합니다. 조회 규칙을 다시 적용한 후 CI가 변경되면 검색된 항목이 새 CI로 업데이트됩니다. 영향을 받는 테스트 결과도 업데이트됩니다. 자세한 내용은 에 대한 검색된 항목의 CI 변경 내용 구성 준수 문서를 참조하십시오.

주:

구성 준수 v24부터는 시스템 속성을 *sn_sec_cmn.skipItemsWithCIDecommissioned*활성화하여 하위 상태가 'CI 해제됨'인 검색된 항목에 대한 CI 조회 규칙의 재적용을 건너뛸 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 **Security Operations >** 불일치하는 검색 항목을 조정하십시오..
2. 백그라운드 작업 페이지에서 조정 작업 만들기를 클릭합니다.
3. 양식에서 필드를 채웁니다.

주:
매개변수 필드만 편집할 수 있습니다.

백그라운드 작업

필드	설명
번호	고유한 작업 번호입니다.
작성자	작업을 생성한 사용자입니다.
매개변수	일치하지 않는 검색 항목을 조정하는 매개변수: ○ limit: 조정할 검색된 항목의 최대 수입니다. 값을 입력하지 않으면 검색된 항목 10,000개가 조정됩니다. ○ firstDiscovereditem: 조정해야 하는 검색된 첫 번째 항목입니다. 값을 입력하지 않으면 검색된 첫 번째 항목에서 조정 프로세스가 시작됩니다.
상태	백그라운드 작업의 현재 상태입니다.
상태 설명	백그라운드 작업의 현재 상태에 대한 설명입니다.
작업 유형	작업의 유형입니다. 값은 일치하지 않는 검색된 항목을 조정합니다.
시작 시간	작업이 시작된 시간입니다.
종료 시간	작업이 완료된 시간입니다.
작업 기간	작업을 완료하는 데 걸린 총 시간입니다.
하위 상태	선택한 상태의 하위 상태입니다.
메모	처리된 기록 수입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 제출을 클릭합니다.

주:

- 작업 실행을 중지하려면 취소를 클릭합니다.
- 호스트 또는 테스트 결과를 임포트하는 동안에는 일치하지 않는 CI를 조정하거나 CI 조회 규칙을 다시 적용할 수 없습니다.

에 대해 선택한 검색 항목에 **CI** 조회 규칙을 다시 적용합니다. 구성 준수

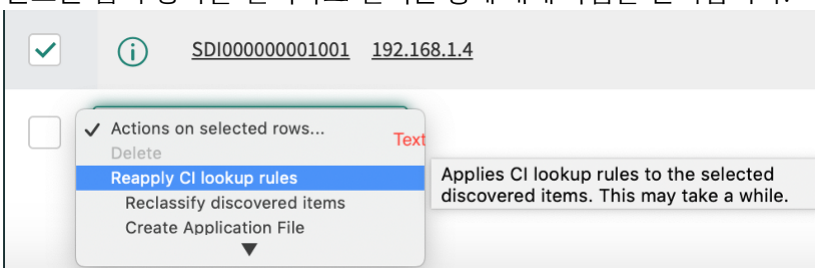
검색된 항목 목록 뷰에서 선택한 검색된 항목에 CI(구성 항목) 조회 규칙을 다시 적용합니다. 작업을 선택합니다. 관리자는 여러 가지 이유로 조회 규칙을 편집하거나 업데이트해야 할 수 있습니다. 조회 규칙이 변경되면 검색된 항목에 다시 적용할 수 있습니다.

시작하기 전에
필요한 역할:

이 태스크 정보
CI 조회 규칙을 다시 적용한 후 CI가 변경되면 검색된 항목이 새 CI 및 테스트 결과로 업데이트됩니다. 자세한 내용은 에 대한 검색된 항목의 CI 변경 내용 구성 준수 문서를 참조하십시오.

프로시저

1. 다음으로 이동 모두 〉 보안 운영 〉 **CMDB** 〉 검색된 항목.
2. 필요한 검색 항목을 선택하고 선택한 행에 대해 작업을 클릭합니다.



3. 목록에서 **CI** 조회 규칙 재적용을 선택합니다.

규칙은 검색된 항목에 다시 적용됩니다.

주:

구성 준수 v15.1.5부터는 시스템 속성을 *sn_sec_cmn.skipItemsWithCIDecommissioned*활성화하여 하위 상태가 'CI 해제됨'인 검색된 항목에 대한 CI 조회 규칙의 재적용을 건너뛸 수 있습니다.

와 **Tenable Vulnerability Integration** 함께 구성 준수

Tenable.io 애플리케이션에서 처리하기 위한 정책, 통제(테스트 결과) 및 구성 테스트를 임포트한 결과물 Tenable Vulnerability Integration 입니다구성 준수.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
의 구성 준수v14.9부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v14.9 이전 용어	용어 **v14.9** 이상
테스트 결과 그룹	정정 작업
그룹 규칙	정정 작업 규칙
정책	테스트 그룹

Tenable.io

가 Tenable Vulnerability Integration 지원됩니다.

임포트한 데이터를 사용하여 다음을 수행할 수 있습니다.

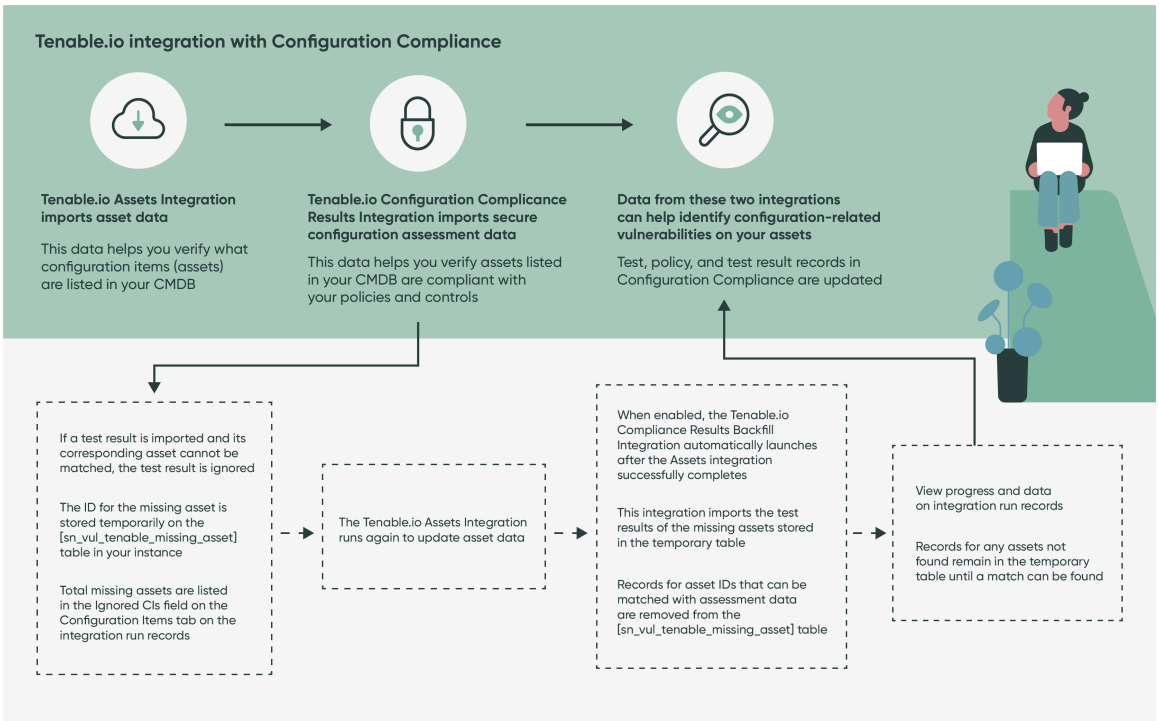
- 다음에 나열된 자산에 대한 구성 관련 취약성 식별 구성 관리 데이터베이스(CMDB)
- 자산이 정책 및 통제를 준수하는지 확인합니다.

다음 통합을 통해 자산 데이터, 정책, 통제(테스트 결과) 및 구성 테스트를 임포트합니다.

- Tenable.io 자산 통합
- Tenable.io 준수 결과 통합
- Tenable.io 준수 결과 백필 통합

다음 이미지는 통합이 함께 작동하여 자산 및 구성 평가 데이터를 임포트하고 임포트 중에 간과된 무시된 CI를 조정하는 방법을 보여줍니다.

보안 구성 평가 결과를 위한 임포트 플로우



데이터를 임포트 및 업데이트하여 애플리케이션의 테스트 결과, 정책 및 구성 테스트 기록에 구성 준수 표시합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

경우에 따라 임포트된 구성 항목(CI)의 수가 자산 통합 및 규정 준수 결과 통합에 따라 Tenable.io 다를 수 있습니다 Tenable.io . 이 경우 무시된 자산 ID에 대한 임시 기록이 생성되고 저장됩니다. 이러한 기록은 나중에 규정 준수 결과 백필 통합에서 임포트하여 임포트한 평가 데이터와 일치시킬 수 있습니다.

예를 들어 자산 통합은 통합 실행 시 80개의 자산을 임포트하지만 준수 결과 통합은 100개를 임포트한다고 가정해 보겠습니다.

주:
다음으로 이동하여 통합 실행에서 무시된 CI 수를 확인할 수 있습니다. **Tenable** 취약성 통합 〉 관리 〉 통합. 통합 이름을 클릭하여 기록을 엽니다. 취약성 통합 실행 관련 링크에서 통합 실행 기록을 열고 항목 탭을 선택하여 무시된 **CI** 필드의 값을 확인합니다. 이 필드는 임포트에서 무시된(누락된) 자산의 총계를 추적합니다.

각 통합 실행 기록에서 무시된 **CI** 필드의 값을 비교하면 무시된 CI가 20개 차이납니다. 결과적으로 백필 통합은 이전 이미지와 같이 자동으로 실행됩니다. 이 통합은 준수 결과 통합에서 찾았지만 자산 통합에서 누락된 추가 20개 자산에 대한 구성 평가 정보를 임포트합니다. 누락된 자산에 대한 평가 데이터는 임포트되지 않으므로 준수 결과 백필 통합은 Tenable.io 통합 실행당 최대 200개의 자산 ID를 임포트하여 누락된 자산을 해당 평가 데이터와 조정합니다. 이러한 자산과 해당 데이터가 일치하면 누락되거나 무시된 자산에 대해 생성되고 임시 테이블에 나열된 모든 기록이 삭제됩니다.

주:
무시된 모든 자산을 임포트하려면 이러한 통합을 여러 번 실행해야 할 수 있습니다.

자산 통합을 활성화하고 구성하는 Tenable.io 방법에 대한 자세한 내용은 문서를 참조하십시오 설정 도우미를 사용하여 Tenable 취약성 통합 구성. 통합에 대한 자세한 내용은 을 참조하십시오 Tenable 취약성 통합 이해 .

Tenable.io 규정 준수 결과 통합과 Tenable.io 규정 준수 결과 백필 통합은 기본적으로 비활성 상태입니다.

활성화하려면 다음을 수행합니다.

1. 다음으로 이동 **Tenable** 취약성 통합 〉 관리 〉 통합.
2. Tenable 통합 목록에서 통합 이름을 클릭하여 기록을 열고 활성 확인란을 선택하여 활성화합니다. 이러한 통합을 시작하려면 일정 설정을 기본값으로 두는 것이 좋습니다.

외부 공급업체 취약성 통합에서 구성 준수 구성 항목을 식별하기 위한 CI 조회 규칙

외부 공급업체 통합에서 데이터를 임포트하면 에서 구성 준수 일치하는 항목을 구성 관리 데이터베이스(CMDB)찾기 위해 자동으로 호스트 데이터를 사용합니다. 이는 **CI** 조회 규칙을 사용합니다. 이러한 규칙은 구성 항목(CI)을 식별하고 정정에 도움이 되도록 테스트 결과 기록에 추가하는 데 사용됩니다.

자산을 임포트할 때 검색된 항목 목록에서 먼저 외부 공급업체 ID를 사용하여 조회가 수행되어 이전 임포트의 구성 항목(CI)과 일치하는 항목을 찾습니다. 호스트 ID 일치가 발견되면 테스트 결과 기록의 구성 항목 필드로 사용됩니다.

검색된 항목 목록을 사용하여 임포트한 자산이 CI에 매핑되는 방식을 볼 수 있습니다. 일치하는 항목을 찾을 수 없거나 cmdb_ci 필드가 비어 있는 경우 규칙은 다른 호스트 정보를 사용하여 CI를 올바르게 식별하려고 시도합니다. 그래도 일치하는 항목이 없으면 자리 표시자 CI가 만들어지고 일치하지 않는 **CI**로 지정됩니다. 이러한 CI 처리 방법에 대한 자세한 내용은 일치하지 않는 CI를 참조하십시오.

검색된 새 항목이 생성되고 이 CI에 매핑됩니다.

주:
CI 조회 규칙은 보안 운영 통합에만 Qualys 사용할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

CI 조회 규칙은 도메인으로 분리될 수 있으며 소스에 따라 다릅니다. 각 소스에는 여러 배포가 있을 수 있습니다. Qualys에는 Qualys 통합의 여러 배포가 있을 수 있습니다. 각 배포에는 고유한 CI 조회 규칙 세트가 있습니다.

주:
CI 조회 규칙은 취약성 통합의 모든 배포에서 공유됩니다. 규칙이 삭제되거나 수정되면 삭제 또는 변경이 취약성 통합의 모든 배포에 영향을 줍니다.

일치를 시도할 때 첫 번째 단계는 벤더 ID를 조회하여 소스, source_instance 및 벤더 ID 간에 정확히 일치하는 항목을 찾습니다. 그런 다음, 조회 규칙이 가장 낮은 규칙에서 가장 높은 순서로 실행되고 규칙이 일치하는 CI를 하나만 반환하면 중지됩니다. 둘 이상의 CI를 반환하는 방식으로 규칙이 생성되면 첫 번째 일치 항목만 사용됩니다.

주:
낮은 수준의 네트워킹 요소에서 일치하지 않도록 하기 위해 일치하는 CI가 dscy_switchport, cmdb_ci_network_adapter, cmdb_ci_nic 또는 cmdb_ci_ip_address 중 하나이면 상위 CI가 반환됩니다.

CI 클래스를 제외하는 시스템 속성을 사용할 수 있습니다. 이 속성은 업그레이드에 사용할 수 없습니다. 속성 설정에 대한 업그레이드 정보 및 지침을 참조하십시오 CI 클래스 무시 .

일치하는 문제를 쉽게 찾을 수 있도록 일치하는 항목을 찾으면 이를 찾는 데 사용되는 CI 조회 규칙이 **CI** 일치 규칙 필드의 검색된 항목 기록에 추가됩니다. 조회 규칙은 가장 낮은 순서 값으로 먼저 평가됩니다.

Qualys 다음은 기본 시스템과 함께 제공되는 CI 조회 규칙의 일부입니다.

- QUALYS 호스트 ID
- FQDN
- NetBIOS
- DNS
- IP

기본 시스템과 함께 제공되는 Microsoft Defender CI 조회 규칙 중 일부는 다음과 같습니다.

- S3 버킷
- 이름
- 자원 ID

다음은 기본 시스템과 함께 제공되는 Palo Alto Prisma Cloud CI 조회 규칙의 일부입니다.

- S3 버킷
- 이름
- 자원 ID

테스트 결과 데이터를 임포트하는 것은 인스턴스에 부담이 될 수 있으며 규칙을 신중하게 구성하지 않으면 자원과 관련된 성능 문제가 발생할 수 있습니다. 반복을 수행하고 일치를 수행하는 데 사용되는 논리로 CMDB 인해 처리 시간이 길어질 수 있습니다. 자원의 잠재적 저하나 성능 저하를 방지하려면 사용자 지정 작성된 CI 조회 규칙을 테스트하거나 사전 정의된 **CI** 조회 규칙을 수정하십시오. 고아 기록 중복 방지, 데이터 삭제 및 데이터 정리에 대한 자세한 내용은 을 참조하십시오 CI 조회 규칙을 실행 취약성 대응 한 후 중복 또는 고아 기록을 방지하는 데 도움이 되는 단계 .

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

업데이트된 CI 조회 규칙 다시 적용

CI 조회 규칙을 변경할 때 CI 조회 규칙 목록 페이지에서 변경 내용 적용을 클릭하여 검색된 항목에 대해 다음과 같은 모든 규칙을 다시 실행합니다.

- 업데이트된 규칙과 일치함
- 어떤 규칙과도 일치하지 않습니다.

조회 규칙을 다시 적용한 후 CI(구성 항목)가 변경되면 검색된 항목이 새 CI로 업데이트됩니다. 테스트 결과도 업데이트됩니다. 자세한 내용은 에 대한 검색된 항목의 CI 변경 내용 구성 준수 문서를 참조하십시오.

에 대한 기존 구성 항목 중복 제거 구성 준수

중복 제거 작업에 대한 Duplicate CI Remediator가 `sn_sec_cmn_src_ci.cmdb_ci` 속성으로 업데이트됩니다.

중복 제거 작업을 사용하여 CI(구성 항목)를 업데이트할 때마다 해당 CI와 관련된 검색된 항목도 업데이트됩니다. 따라서 테스트 결과가 CI로 업데이트됩니다. 자세한 내용은 에 대한 검색된 항목의 CI 변경 내용 구성 준수 문서를 참조하십시오.

식별 및 조정 엔진을 사용하기 위한 구성 준수 CI 생성

11.1부터 구성 준수 IRE(식별 및 조정 엔진) API를 사용하여 CI 구성 관리 데이터베이스(CMDB)(구성 항목)를 생성할 수 있습니다. IRE API를 사용하여 CI를 생성하면 중복 CI가 생성되는 것을 방지할 수 있으며 신뢰할 수 있는 데이터 소스만 에 쓸 CMDB수 있도록 하여 CI 속성을 조정할 수 있습니다.

CI 클래스(테이블)는 인스턴스 데이터베이스의 원래 테이블 이름입니다. CMDB 에는 CI에 대한 데이터를 저장하는 기본 시스템 클래스가 포함되어 있습니다.

CI 생성에 IRE 사용

버전 11.1 이전에는 검색된 항목 목록 또는 CMDB에서 일치하는 CI를 찾을 수 없는 경우 일치하지 않는 CI 클래스(sn_sec_cmn_unmatched_ci)에 CI가 생성되었습니다.

자세한 내용은 일치하지 않는 CI를 참조하십시오.

버전 11.1부터 IRE API를 사용하여 에서 CMDBCI를 생성할 수 있습니다. 일치하지 않는 CI 클래스를 사용하는 대신 분류되지 않은 하드웨어 또는 불완전한 IP 식별 장치 클래스에 CI가 생성됩니다.

CMDB CI 클래스

주:
새 클래스를 사용하려면 CI Class Models 플러그인을 활성화하십시오 CMDB . 그렇지 않으면 CI가 Unmatched CI 클래스에 생성됩니다.

버전 11.1부터 외부 공급업체 스캐너에서 임포트한 호스트를 검색된 항목 목록에서 CMDB찾을 수 없거나 다음과 같은 새 CMDB CI 클래스 중 하나에 저장됩니다.

CMDB CI 클래스

CMDB CI 클래스	설명
불완전한 IP 식별 장치(cmdb_ci_incomplete_ip)	스캐너에서 받은 호스트 정보에서 IP 주소만 사용할 수 있는 경우 이 테이블에 CI가 생성됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

CMDB CI 클래스

CMDB **CI** 클래스	설명
분류되지 않은 하드웨어 (cmdb_unclassed_hardware_ci)	스캐너에서 받은 호스트 정보에서 다음 정보를 사용할 수 있는 경우 이 테이블에 CI가 생성됩니다. • 호스트 이름 • IP 주소 • DNS • NETBIOS • MAC 주소 주: MAC 주소를 사용할 수 있으면 네트워크 어댑터 항목이 생성되고 분류되지 않은 하드웨어 CI와 연관됩니다. IP 주소와 MAC 주소를 모두 사용할 수 있는 경우 IP 주소 CI도 생성되고 분류되지 않은 하드웨어 CI와 연결됩니다.

다음 중 하나가 발생할 경우 시스템에서 자동으로 일치하지 않는 CI 클래스를 사용합니다.

- CI 클래스 플러그인이 CMDB 활성화되지 않았습니다.
- IRE는 새 CI를 생성하는 동안 예외를 발생합니다.

관련 정보

CMDB CI Class Models 스토어 앱

IRE(식별 및 조정 엔진)

구성 준수 할당 규칙 개요

정정을 위해 할당 그룹에 테스트 결과가 자동으로 할당되는 기준을 정의합니다.

주:
의 구성 준수v14.9부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v14.9 이전 용어	용어 **v14.9** 이상
테스트 결과 그룹	정정 작업
그룹 규칙	정정 작업 규칙
정책	테스트 그룹

기본 할당 규칙인 **CI** 지원 그룹에 할당은 **CI** 지원 그룹에 테스트 결과를 할당하는 기본 시스템에 포함됩니다. 기본적으로 비활성 상태입니다.

할당 규칙에 의해 설정된 할당 그룹은 정정 작업 규칙 에서 소유자를 RT(정정 작업)에 할당하는 데 사용됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테스트 결과 자동 할당

할당을 사용하여 테스트 결과를 할당하는 방법에는 세 가지가 있습니다.

- 할당 그룹: 이 옵션을 사용하면 기존 ServiceNow AI Platform# 사용자 그룹을 선택할 수 있습니다.
- 할당 그룹 필드: 이 옵션을 사용하면 cmdb_ci 테이블을 사용하여 사용 가능한 할당 그룹 필드를 선택할 수 있습니다. 기본적으로 다음과 같은 세 개의 그룹 필드가 표시됩니다.
  - 없음: 이 필수 필드의 기본값이 없음을 나타냅니다.
  - 구성 항목: 승인 그룹
  - 구성 항목: 담당 그룹
  - 구성 항목: 지원 그룹
- 스크립트: 이 옵션을 사용하면 스크립트를 사용하여 조건을 정의할 수 있습니다. 이 옵션을 사용하려면 코딩 또는 고급 ServiceNow# 전문 지식이 필요합니다.

담당 규칙 생성에 대한 자세한 내용은 을 참조하십시오 담당 규칙 생성 또는 편집 구성 준수 .

sn_vulc.remediation_owner 역할을 사용하면 사용자 또는 자신의 할당 그룹에 할당된 테스트 결과 및 정정 작업을 보고 업데이트할 수 있습니다. 모듈을 보려면 다음으로 이동하십시오. 모두 〉 구성 준수 〉 테스트 결과 〉 열린 사용자 테스트 결과또는 구성 준수 〉 정정 작업 〉 내 오픈 작업.

sn_vulc.remediation_owner 역할은 사용자에게 직접 할당하거나 사용자에게 itil 역할을 할당할 때 자동으로 할당됩니다.

할당 규칙 평가 프로세스

새 테스트 결과를 임포트하거나 종결 후 다시 열면 담당 규칙이 이에 대해 평가됩니다. 담당 규칙은 CI 일치 및 위험 점수 계산 후에 평가됩니다. 테스트 결과는 종결 후 다시 열리지 않는 한, 초기 임포트 시와 규칙이 변경될 때만 자동으로 평가됩니다. 변경 후 수동으로 규칙을 다시 적용할 수 있습니다.

새 테스트 결과 또는 다시 열린 테스트 결과마다 다음 프로세스가 사용됩니다.

- 각 테스트 결과 할당 규칙에 대해 테스트 결과는 가장 낮은 순서의 규칙이 먼저 할당 필터와 비교됩니다.
- 조건이 일치하면 테스트 결과에 할당 그룹이 할당됩니다. 조회가 중지됩니다.
- 조건이 모든 규칙 중에서 일치하는 항목을 찾지 못하면 테스트 결과는 할당되지 않은 상태로 유지됩니다.

담당 규칙 다시 적용

할당 규칙을 변경할 때 할당 규칙 목록 페이지의 변경 내용 적용 버튼을 사용하여 수동으로 할당된 테스트 결과를 제외하고 모든 활성 테스트 결과에 대해 변경된 모든 규칙을 다시 실행합니다.

주:
담당 규칙은 수동으로 생성된 할당을 다시 평가하지 않습니다.

예약된 작업 [*Reapply all assignment rules*]은 기본적으로 비활성 상태입니다. 활성화되면 수동으로 할당된 규칙을 제외한 모든 활성 규칙에 대해 열려 있는 모든 테스트 결과가 평가됩니다. 매일, 매주, 매월, 주기적으로, 한 번 또는 요청 시에 실행할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

중요사항:
관리자 및 분석가는 에서 취약성 관리자 작업 공간선택한 테스트 결과에 대한 최신 할당을 얻을 수 있습니다. 이 방법은 시간이 오래 걸리는 프로세스인, UI의 클래식 모든 테스트 결과에 대해 할당 규칙을 다시 적용하는 것보다 더 효율적입니다. 자세한 내용은 에 있는 기록의 정정 속성 재평가 취약성 관리자 작업 공간 문서를 참조하십시오.

담당 규칙 및 정정 작업 할당

일반적으로 정정 작업(RT)을 테스트 결과와 동일한 할당 그룹에 할당합니다. 기본적으로 정정 작업 규칙이 수행하는 작업입니다.

예를 들어, RT가 구성 항목 클래스별로 그룹화된 경우, 생성된 정정 작업은 다른 할당 그룹에 의해 분리될 수 있습니다. Oracle Database TRG는 그룹 1에 지정되고 Oracle Database TRG는 그룹 2에 지정될 수 있습니다.

할당 그룹이 정정 작업 수준에서 변경되면 할당 그룹이 동일한 정정 작업의 모든 테스트 결과가 새 할당 그룹으로 업데이트됩니다. 테스트 결과는 수동으로 할당된 것으로 표시되며 추가 규칙 평가에 해당되지 않습니다.

정정 작업에서 할당 구성 준수 제거

사용자 또는 그룹에 잘못 할당되었을 수 있다고 판단되는 테스트 결과 기록 및 정정 작업에서 바로 정정 작업 및 관련 테스트 결과의 할당 대상 및 할당 그룹 필드를 지울 수 있습니다.

워크플로우 개요

정정 소유자는 할당 해제 버튼으로 재할당을 위해 기록을 업데이트할 수 있습니다.

sn_vulc.remediation_owner 사용 케이스

RT 및 관련 테스트 결과가 정정 범위 내에 있지 않다고 판단되거나 기록이 사용자 또는 그룹에 잘못 할당되었다고 생각되는 경우 해당 정정 작업 기록의 할당 대상 및 할당 그룹 필드에서 자신 또는 그룹을 제거할 수 있습니다.

모듈 할당 해제

할당 해제 버튼은 종결됨 또는 해결됨 상태를 제외한 모든 상태의 정정 작업 및 테스트 결과 기록에 표시됩니다.

할당 취소를 선택하면 정정 작업과 연결된 모든 테스트 결과가 다시 할당되고 할당되지 않은 할당 유형으로 전환된다는 메시지가 표시됩니다.

주:
정정 작업의 테스트 결과에 정정 작업과 다른 할당 그룹이 있는 경우 할당 해제되지 않습니다. 대부분의 경우 이러한 테스트 결과는 수동으로 할당되었습니다.

UI 버튼을 사용하거나 수동으로 업데이트하는 모든 기록은 할당되지 않은 모듈의 에 표시됩니다 구성 준수.

UI 작업을 사용하여 기록을 재할당하는 *`Unassigned`* 단계는 다음 문서를 사용자 또는 그룹에 대한 정정 작업에서 할당 제거참조하십시오.

시스템 속성 및 알림

sn_vulc.vulnerability_admin 역할을 가진 관리자인 경우 기록에서 할당 해제 를 선택하면 기본적으로 시스템 속성이 *`sn_vulc.unassign_test_result_group.approval_required`* 상태 변경 승인 기록 및 요청된 승인 기록을 트리거합니다. 또한 요청은 승인자의 내 승인 목록에 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
취약성 관리자는 시스템 속성을 **false**로 설정하여 *sn_vulc.unassign_test_result_group.approval_required* 승인 프로세스를 비활성화할 수 있습니다.

- 승인자가 요청을 승인하면 기본적으로 시스템 속성 *sn_vulc.default_assignment_group* 에서 할당 대상 및 할당 그룹 필드를 지우고 할당 유형 필드를 할당되지 않음으로 채웁니다. 취약성 관리자는 할당 필드를 지우고 특정 그룹을 할당하도록 시스템 속성의 값을 *sn_vulc.default_assignment_group* 변경할 수 있습니다. 예를 들어 사용자가 기록에서 할당 해제 를 선택하고 검토를 위해 특정 그룹으로 리디렉션하려는 경우 시스템 속성의 값 필드에 선택한 그룹의 시스템 ID를 추가할 수 있습니다.
- 승인자가 요청을 거부하면 메모 탭에 거부 사유가 표시됩니다.

또는 특정 그룹에 대해 구성되지 않은 경우 *sn_vulc.default_assignment_group* 기본적으로 할당되지 않은 알림 사용자 그룹에 추가한 사용자는 기록이 할당되지 않을 때 경보를 받습니다. 시스템 속성으로, *sn_vulc.default_notification_group* 이 그룹에 대한 알림을 결정합니다.

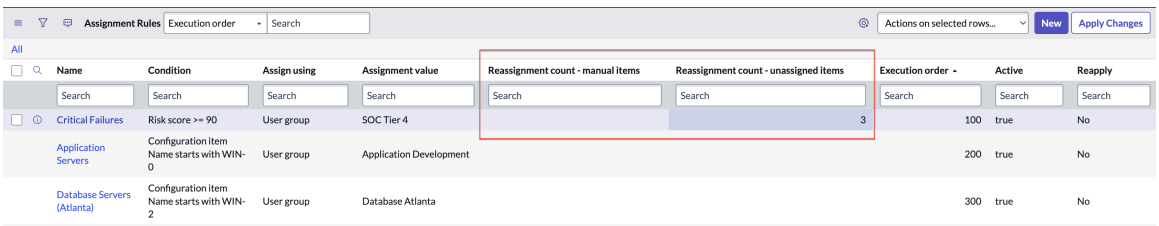
할당 유형(수동, 규칙 또는 미할당)은 RT 레코드와 목록 뷰에서 사용할 수 있습니다. 할당되지 않은 할당 유형은 기능의 시스템 속성에 의해 할당 대상 및 할당 그룹 필드가 지워진 후에 표시됩니다.

이 기능에 대해 예약된 작업으로 담당 규칙 모니터링

일일 예약 작업은 할당되지 않은 할당 유형으로 전환될 때의 기록을 계산합니다. 이 개수로 취약성 분석가는 할당되지 않은 RT가 더 많은 할당 규칙을 기반으로 제대로 수행되지 않을 수 있는 할당 규칙을 모니터링하고 조정할 수 있습니다.

Reassignment count for assignment rules 예약된 작업은 매일 실행되며 특정 할당 규칙에 대해 이 기능에 의해 할당되지 않은 총 RT 수를 게시합니다.

이 작업은 수동으로 할당되지 않은 모든 기록도 계산합니다. 수동 개수와 이 기능으로 수집된 개수는 모두 취약성 할당 규칙 목록의 두 열 *Reassignment count - manual items* (및 *Reassignment count - unassigned items*.



1. 취약성 관리자는 다음으로 이동하여 이러한 개수를 볼 수 있습니다. 구성 준수 〉 관리 〉 담당 규칙.
2. 목록의 오른쪽 상단에 있는 기어 아이콘을 선택하고 재할당 횟수 - 수동 항목 및 재할당 횟수 - 할당되지 않은 항목을 선택하여 표시합니다.
3. 원래 규칙에 의해 할당되었지만 나중에 자동 또는 수동으로 재할당된 모든 RT에는 목록 보기에 원래 규칙에 대한 참조가 포함됩니다.

구성 준수 정정 작업 및 정정 작업 규칙 개요

정정 작업 규칙을 사용하여 결과를 대량으로 분석하도록 정정 작업(RT)을 자동으로 생성합니다. 테스트 결과를 정정 작업에 수동으로 할당할 필요가 없도록 작업이 구성되는 기준이 구성됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
의 구성 준수v14.9부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v14.9 이전 용어	용어 **v14.9** 이상
테스트 결과 그룹	정정 작업
그룹 규칙	정정 작업 규칙
정책	테스트 그룹

정정 작업 이해

정정 작업은 정정할 테스트 결과 집합을 나타냅니다. 테스트 결과를 그룹화하면 여러 가지 장점이 있습니다. 정정 상태를 통해 테스트 결과를 이동하고, 조사 중인 것으로 표시하고, 지연시키고, 그룹을 사용하여 일괄적으로 해결하도록 표시할 수 있습니다. 지정된 결과, 기술, 위험 점수 및 테스트 결과와 관련된 다른 모든 데이터를 포함하는 모든 결과를 자동으로 그룹화하는 조건을 만들 수 있습니다. 테스트 결과는 하나 이상의 정정 작업에 속할 수 있으므로 한 정정 작업을 적극적으로 수행하고 다른 작업을 모니터링할 수 있는 유연성이 제공됩니다. 그것은 모두 조직의 요구에 달려 있습니다. 예를 들어, 할당별로 그룹화하고 기술을 포함하는 그룹을 만들 수도 있습니다.

다음과 같이 정정 작업이 생성됩니다.

- 두 옵션 중 하나를 사용하여 수동으로 테스트 결과를 그룹에 추가합니다.
  - 수동: 항목이 없는 정정 작업을 생성합니다. 테스트 결과는 수동으로 추가해야 합니다.
  - 필터: 정정 작업을 만들고 조건을 사용하여 해당 정정 작업에 테스트 결과를 자동으로 추가합니다.

  주:
  수동으로 추가된 테스트 결과는 정정 작업 규칙 또는 정정 작업 조건에 따라 정정 작업에서 자동으로 제거되지 않습니다.

- 정정 작업 규칙을 사용하여 자동으로 수행됩니다. 이 옵션은 가장 쉬운 옵션입니다. 일단 구성되면 정정 작업 규칙이 원하는 모든 정정 작업을 생성합니다.

정정 작업에서 테스트 결과 그룹을 사용자에게 할당하고, 나중으로 연기하고, 변경 요청을 만드는 데 사용하는 등의 작업을 수행할 수 있습니다.

주:

sn_vulc.remediation_owner 역할을 사용하면 사용자 또는 할당 그룹에 할당된 테스트 결과 및 정정 작업을 보고 업데이트할 수 있습니다. 모듈을 보려면 다음으로 이동하십시오. 모두 〉 구성 준수 〉 테스트 결과 〉 열린 사용자 테스트 결과또는 구성 준수 〉 정정 작업 〉 내 오픈 작업.

새 테스트 결과를 정정 작업에 추가할 수 있는 것으로 확인되면 테스트 결과가 정정 작업의 테스트 결과 관련 목록에 포함됩니다.

정정 작업의 상태를 업데이트할 때 관련 테스트 결과의 상태가 이 정정 작업과 일치하도록 업데이트될 수 있습니다. 상태 변경에 대한 자세한 내용은 다음 문서를 참조하십시오 구성 준수 상태.

정정 작업 규칙 이해

정정 작업 규칙을 사용하면 테스트 결과를 자동으로 그룹화하고 할당하는 방법을 정의할 수 있습니다. 기본 규칙인 할당 그룹인 테스트는 테스트 결과 할당 그룹 및 테스트 필드를 기반으로 테스트 결과를 그룹화하는 기본 시스템에 포함됩니다. 이 규칙은 기본적으로 사용되지 않습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테스트 결과에서 액세스할 수 있는 열의 다른 값 집합을 기준으로 그룹화할 수 있습니다. 최대 6개의 키와 원하는 수의 조건을 사용할 수 있습니다. 자세한 내용은 정정 작업 규칙 생성 또는 편집 구성 준수 문서를 참조하십시오.

중요사항:
관리자와 분석가는 취약성 관리자 작업 공간에서 선택한 테스트 결과에 대한 정정 작업 규칙을 평가할 수 있습니다. 이 방법은 시간이 오래 걸리는 프로세스인 클래식 UI에서 정정 작업 규칙을 다시 적용하는 것보다 더 효율적입니다. 자세한 내용은 에 있는 기록의 정정 속성 재평가 취약성 관리자 작업 공간 문서를 참조하십시오.

예를 들어 할당 그룹 또는 기술 및 CI(구성 항목)별로 테스트 결과를 그룹화할 수 있습니다. 회사를 더 많은 위험에 노출시키는 테스트 결과에 대해 다른 규칙 집합을 사용할 수 있습니다. 심각도가 낮거나 위험도가 낮은 CI에 대해 하나의 정정 작업 규칙을 가질 수 있습니다. 사용 가능한 필드에 대한 자세한 내용은 을 참조하십시오 테스트 결과 보기 구성 준수 .

새 테스트 결과를 임포트하거나 종결했다가 다시 열면 정정 작업 규칙이 이에 대해 평가됩니다. 테스트 결과는 종결 후 다시 열리지 않는 한 한 번만 평가됩니다.

정정 작업 규칙은 CI 일치, 위험 점수 계산 및 할당 규칙 후에 평가됩니다.

새 테스트 결과 또는 다시 열린 테스트 결과마다 다음 프로세스가 사용됩니다.

- 각 정정 작업 규칙의 테스트 결과는 조건 필터와 비교됩니다.
- 규칙 조건이 일치하는 각 규칙에 대해 테스트 결과의 그룹 키 열에서 데이터를 끌어옵니다. 이 규칙은 테스트 결과와 동일한 할당 그룹에 할당된 일치하는 미해결 정정 작업이 있는지 확인합니다.

  정정 작업이 발견되면 테스트 결과가 열림 상태의 기존 정정 작업에 추가됩니다.

- 열림 상태의 정정 작업이 없는 경우, 규칙에서 정정 작업을 생성하고 규칙의 사용자 그룹 또는 키 값에 따라 할당한 후 테스트 결과를 배치합니다.

여러 종류의 결과를 그룹화하기 위해 두 개 이상의 테스트 결과 규칙을 정의할 수 있습니다. 각 결과는 정정 작업에 배치하기 전에 규칙 조건과 비교되므로 규칙이 너무 많으면 성능에 영향을 줄 수 있습니다.

정정 작업 규칙이 삭제되면 규칙에 의해 생성된 모든 열린 작업을 삭제할 수 있습니다. 이는 규칙 양식 뷰와 목록 뷰 모두에 적용됩니다.

정정 작업 할당이 수행되거나 변경되면 테스트 결과가 RT와 다른 할당 그룹이 있는 경우를 제외하고 할당 그룹 및 할당 대상 필드가 모든 테스트 결과로 롤다운됩니다. 담당 규칙에 대한 자세한 내용은 다음 문서를 참조하십시오 구성 준수 할당 규칙 개요. 이러한 할당은 다음 임포트 시 이 그룹에 대해 자동으로 사용됩니다.

테스트 결과 및 정정 작업에 대한 지연 수 추적

v14.3부터 여러 지연 모듈에서 테스트 결과 또는 정정 작업이 지연되는 횟수를 추적합니다. 지연 수 설정이라는 예약된 작업은 매일 실행되어 여러 지연 모듈에 나열된 기록의 지연 수 열에 두 번 이상 지연된 기록에 대한 개수를 게시합니다.

용 계산기 그룹 및 계산기 구성 구성 준수

구성 준수 계산기는 사전 정의된 조건이 충족될 때 기록 값을 업데이트하는 데 사용됩니다. 계산기는 기록 업데이트 방법을 결정하는 데 사용되는 기준에 따라 그룹화됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
의 구성 준수v14.9부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v14.9 이전 용어	용어 **v14.9** 이상
테스트 결과 그룹	정정 작업
그룹 규칙	정정 작업 규칙
정책	테스트 그룹

구성 준수 계산기

구성 준수 애플리케이션에는 위험 계산기와 위험 점수 롤업 계산기라는 두 가지 유형의 계산기가 포함되어 있습니다. 이러한 계산기 그룹은 기본적으로 활성화됩니다.

위험 점수 계산기 그룹의 이름이 위험 계산기로 변경되었습니다.

위험 점수 롤업 계산기에는 구성 테스트 및 정정 작업에 대한 롤업 계산기가 포함되어 있습니다.

테스트 결과 및 정정 작업의 정정을 위한 위험 및 롤업 계산기 구성에는 다음 작업이 포함됩니다.

- 위험 계산기 생성
- 위험 점수 롤업 계산기 생성

위험 계산기를 생성한 후에는 다음 데이터 수집 시 계산에 사용할 수 있습니다. 생성한 후 요청 시 적용하는 것을 선호할 수도 있습니다.

계산기 및 계산기 그룹에 대한 자세한 내용은 다음 문서를 참조하십시오 구성 준수 계산기 그룹.

구성 준수 예외 관리 개요

조직이 게시된 취약성 관리 또는 보안 정책, 표준 또는 가이드라인을 준수할 수 없는 경우 예외를 요청할 수 있습니다. 예외 관리에는 정책에 따라 정정할 수 없는 정정 작업에 대한 예외를 요청, 검토, 승인 또는 거부하는 작업이 포함됩니다.

중요사항:
예외 관리는 취약성 관리자 작업 공간 및 IT 정정 작업 공간에서 지원됩니다.

주:
의 구성 준수v14.9부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v14.9 이전 용어	용어 **v14.9** 이상
테스트 결과 그룹	정정 작업
그룹 규칙	정정 작업 규칙
정책	테스트 그룹

일부 취약성에는 기존 패치, 수정 프로그램 또는 솔루션이 없을 수 있습니다. 예외가 승인되면 구성 관련 취약성을 수정하지 않은 결과를 인정하고 이에 동의하기 때문에 위험을 수락한다는 의미이기도 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예외의 수명주기

예외는 지정된 기간 동안 정정 작업의 정정을 연기해 달라는 요청입니다.

예외의 수명주기는 다음과 같습니다.

- 예외 요청
- 예외 요청 승인
- 예외 요청 추적
- 예외 요청의 만료

예외 요청

정정 소유자는 예외 관리 프로세스를 사용하여 정정 작업에 대한 면제를 요청할 수 있습니다. 승인 프로세스 중에 정정 작업은 검토 중 상태로 유지됩니다. 예외 승인자가 이 요청을 승인하면 정정 작업이 연기됨 상태로 전환됩니다.

중요사항:
IT 정정 작업 공간에서 예외를 요청할 수 있습니다. 자세한 내용은 에서 예외 요청 IT 정정 작업 공간 문서를 참조하십시오.

예외 요청 승인

즉시 정정할 수 없는 정정 작업은 검토되고, 위험에 대해 평가되며, 정정될 수 있을 때까지 연기 승인됩니다. 예외 요청 승인은 2단계 워크플로가 될 수 있습니다. 첫 번째 수준 승인자만 있는 경우 예외를 요청하고 승인할 수 있습니다. 그러나 첫 번째 수준 승인자가 없으면 예외를 요청할 수 없습니다. 자세한 내용은 에 대한 예외 승인자 추가 구성 준수 문서를 참조하십시오.

중요사항:
취약성 관리자 작업 공간에서 예외 요청을 승인하거나 거부할 수 있습니다. 자세한 내용은 에서 정정 작업 및 기록에 대한 예외 요청 취약성 관리자 작업 공간 문서를 참조하십시오.

주:

v13.0부터 구성 준수 CC 애플리케이션을 처음 배포하는 경우 예외 관리용 플로우 디자이너가 기본적으로 활성화됩니다. 워크플로우를 이미 사용 중인 경우 플로우 디자이너로 업데이트할 수 있습니다. 두 경우 모두 다시 워크플로우로 변경할 수 없습니다.

정정 작업에 대한 예외 요청이 승인되면 다음 작업을 수행할 수 있습니다.

- 재개설
- 삭제

주:
거부 설명은 정정 작업의 작업 메모에 표시됩니다. 예외 요청이 거부되면 이 정정 작업은 이전 상태로 되돌아갑니다.

예외 요청 추적

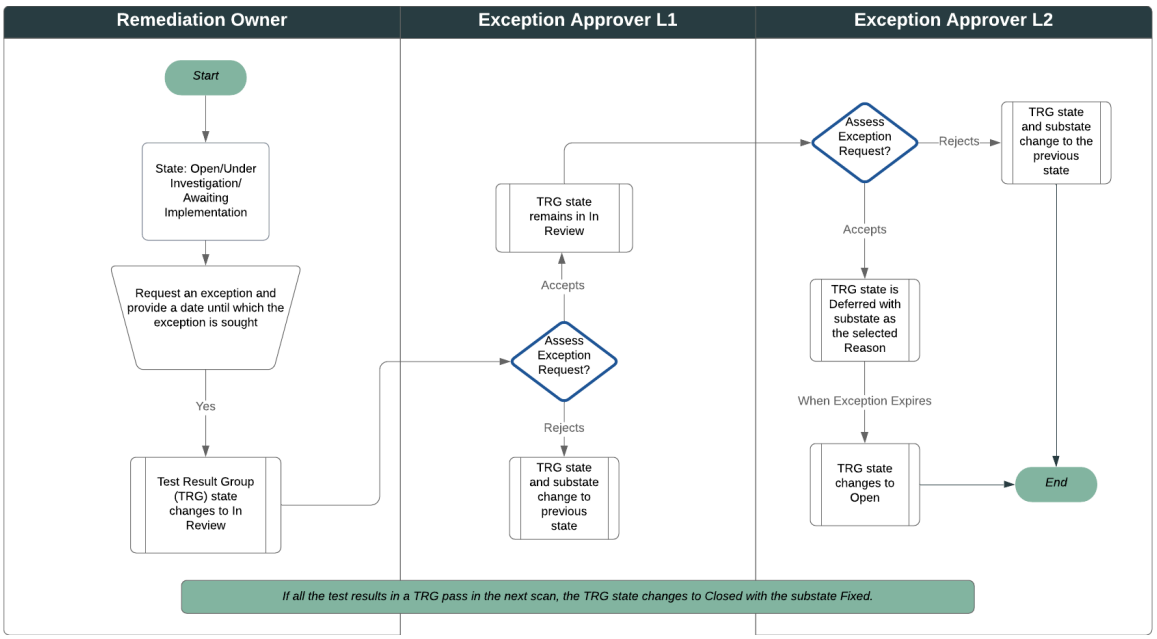
예외를 제기한 후에는 정정 작업의 상태 변경 승인 탭을 사용하여 해당 상태를 추적할 수 있습니다. 정정 작업에 대해 작업이 수행된 경우 해당 정정 작업에서 개별 테스트 결과의 상태를 추적할 수 없습니다.

예외 요청의 만료

정정 작업에 대한 예외 요청이 만료되면 정정 작업이 열림 상태로 되돌아갑니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

CC v13.0 이전의 예외 관리 승인 프로세스



구성 준수 변경 관리

IT 정정 소유자는 애플리케이션의 RT(정정 작업)에서 직접 CHG(변경 요청)를 생성하고 관리할 수 있습니다 구성 준수 .

주:
의 구성 준수v14.9부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v14.9 이전 용어	용어 **v14.9** 이상
테스트 결과 그룹	정정 작업
그룹 규칙	정정 작업 규칙
정책	테스트 그룹

변경 요청 및 구성 준수 워크플로우

변경 요청 및 변경 관리는 워크플로우 정정 프로세스의 구성 준수 일부입니다. 이 정정 단계 중에 변경 요청을 사용하여 테스트 결과의 우선순위를 지정하고 테스트 결과를 추적하며 정정할 수 있습니다.

이 구성 준수 애플리케이션은 IT 변경 관리 프로세스와 함께 ServiceNow AI Platform# 작동하여 환경에서 미준수 소프트웨어 및 기술을 정정할 수 있도록 지원합니다.

애플리케이션에서 Change Management를 구성 준수 사용하면 테스트 결과를 기존 변경 요청에 연결하거나, 정정 작업을 분할하여 선택한 테스트 결과에 대해서만 새 정정 작업을 생성할 수 있습니다.

자세한 내용은 구성 준수에서 변경 요청 만들기 문서를 참조하십시오.

주요 용어

테스트

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테스트는 컴퓨팅 자산의 스캔을 구성하는 데이터 기록 라이브러리입니다. 구성 테스트는 기술 자산 클래스를 관리하는 방법을 정의합니다. 테스트는 규정을 준수하지 않는 소프트웨어 클래스 또는 하드웨어 자산을 식별하는 데 사용할 수 있는 것입니다.

테스트 결과

테스트 결과는 외부 공급업체 통합을 통해 임포트됩니다. 에서 볼 수 구성 준수있게 되면 정정 작업을 사용하여 정정됩니다. 할당 규칙에 따라 정정을 위해 그룹이 할당됩니다.

주:
버전 14.9 구성 준수부터 테스트 결과의 레이블은 *Finding*입니다.

정정 작업

테스트 결과는 할당 규칙에 따라 정정 작업으로 그룹화되고 정정을 위해 정정 소유자에게 자동으로 할당됩니다.

주:
의 구성 준수버전 14.9부터 테스트 결과에는 정정 작업 레이블이 지정됩니다.

테스트 그룹

테스트 그룹은 권한이 부여된 문서 및 테스트 레코드와 관련이 있습니다. 구성 테스트 그룹이 테스트 그룹을 정의합니다.

관련 변경요청

변경 요청은 정정을 위해 제어된 프로세스를 구현하는 데 도움이 됩니다. 의 구성 준수 정정 작업과 함께 변경 요청을 사용하면 추가 자원이 필요하거나 지연 대상으로 할 수 있는 미준수 자산(구성 항목)을 식별, 추적 및 해결하는 데 도움이 될 수 있습니다.

테스트 결과 및 정정 작업에 대한 자세한 내용은 다음 문서를 구성 준수 정정 작업 및 정정 작업 규칙 개요참조하십시오.

에서 변경 요청을 사용하는 경우 구성 준수

변경 요청은 테스트 결과에 대한 정정 활동을 시작하고 추적하는 데 도움이 됩니다. 정정 소유자에게 정정되지 않은 테스트 결과 또는 구성 항목이 다수 있는 경우 변경 요청을 사용하여 지연에 대한 테스트 결과를 식별할 수 있습니다. 또는 원래 정정 작업에서 처음에 파악한 것보다 더 많은 자원을 필요로 하는 테스트 결과 및 구성 항목을 식별하고 다시 그룹화할 수 있습니다.

정정 작업에서 변경 요청 생성

정정 작업의 모든 테스트 결과에 대해 정정 작업에서 직접 변경 요청을 생성하거나 필터링을 사용하여 특정 기준과 일치하는 테스트 결과만 식별합니다. 수동 개입이 필요한 테스트 결과에 대한 조사를 신속하게 처리할 수 있도록 미리 채워진 정보로 변경 요청을 생성합니다.

정정 작업 분할

기존 정정 작업에서 새 정정 작업으로 이동하려는 테스트 결과의 하위 집합을 식별합니다. 새 TRG를 만들면 원래 정정 작업에 영향을 주지 않고 특정 테스트 결과 그룹을 사용할 수 있습니다.

테스트 결과를 기존 변경 요청에 연결

정정 작업을 해결할 때 중복 변경 요청이 생성되지 않도록 테스트 결과를 기존 작업에 연결합니다. 정정 작업을 인스턴스에서 이미 사용할 수 있는 변경 요청에 연결하면 기존 작업 목록을 사용할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

정정 작업에 대한 변경 요청의 유형

자신에게 할당된 정정 작업에서 직접 변경 요청을 생성, 승인, 구현, 검토 및 종결할 수 있습니다. 정정 작업에서 미리 채워진 정보로 세 가지 유형의 변경 요청을 생성할 수 있습니다.

- 표준. 위험이 적고, 비교적 일반적이며, 지정된 절차나 작업 지시를 따르는 사전 승인된 변경입니다.
- 보통. 일반 변경 요청은 구현, 검토 및 종결 전에 두 가지 수준의 승인이 필요한 후속 대응적 프로세스를 따릅니다.
- 비상. 중요 인시던트를 해결하기 위한 변경입니다.

애플리케이션 설정, 설치 및 구성 구성 준수

인스턴스에서 애플리케이션을 ServiceNow AI Platform# 실행하기 전에 먼저 에서 애플리케이션을 ServiceNow# Store다운로드하고 설치해야 구성 준수 합니다. 이 애플리케이션은 별도의 구독으로 사용할 수 있습니다.

설치하기 전에 다음 표에 나열된 다음 설정 검사 목록 단계를 완료합니다. 이러한 설정 작업은 원활한 설치 및 구성을 위해 필요합니다.

애플리케이션의 릴리스 버전 구성 준수 , 외부 공급업체 및 ServiceNow 이와 호환되는 애플리케이션에 대한 자세한 내용은 HI 지식베이스에서 취약성 대응 호환성 매트릭스 및 릴리스 스키마 변경 (KB0856498) 문서를 참조하십시오.

스토어 앱에 대한 권리를 얻는 방법에 대한 자세한 내용은 다음을 참조하십시오 보안 운영 그리고 ServiceNow Store.

검사 목록 작업 설정

작업 설정	설명
인스턴스에 필요한 ServiceNow 역할이 있는지 확인합니다.	예상 결과의 설치, 구성 및 검증에 필요한 역할은 다음과 같습니다. • 아직 할당되지 않은 경우 시스템 관리자 (admin)가 애플리케이션을 설치하고 구성 준수 관리자 [sn_vulc.admin] 역할을 할당합니다. • 구성 준수 관리자 (sn_vulc.admin)는 구성을 감독하고 예상 결과를 검증합니다. • 정정 소유자 (sn_vulc.remediation_owner)는 할당된 기록을 읽고 업데이트합니다. 모든 사용자에게 itil 역할이 할당되면 sn_vulc.remediation_owner 역할도 자동으로 할당됩니다.
지원되는 통합	를 사용하여 구성 준수 구성 항목을 정정하려면 먼저 타사 스캐너 통합을 설치하고 하나 이상의 네트워크 스캔을 수행해야 합니다. 취약성 대응 지원되는 외부 공급업체 통합을 구성하기 전에 애플리케이션이 설치되고 활성화되었는지 확인하십시오. 취약성 대응 설치 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

검사 목록 작업 설정

작업 설정	설명
	통합 애플리케이션이 설치되고 활성화되었는지 확인하려면 다음으로 이동하십시오. 구독 관리 〉 구독 인스턴스에 있습니다. 목록에 조직이 구매한 구독이 표시됩니다. 타사 통합 및 지원되는 제품 목록에 대한 자세한 내용은 문서를 참조하십시오 구성 준수 통합.

Qualys Vulnerability Integration

- 시스템에 Qualys Vulnerability Integration 이미 설치되어 있고 API 자격 증명이 사용하려는 구성 준수자격 증명과 다른 경우 설정 도우미(의 취약성 대응)로 이동하여 각 **Qualys PC** 통합에 할당합니다.
- 다음으로 이동 **Qualys** 취약성 통합 〉 기본 통합 을 클릭하고 **Qualys REST** 상세 정보 탭 아래의 **Qualys API** 자격 증명 필드를 편집합니다.

에 Qualys Vulnerability Integration대한 자세한 내용은 문서를 참조하십시오 Qualys Vulnerability Integration 이해.

이제 애플리케이션을 설치할 구성 준수 준비가 되었습니다. 구성 준수 설치 문서를 참조하십시오.

구성 준수 설치

인스턴스에서 실행하려면 구성 준수ServiceNow AI Platform# 먼저 에서 ServiceNow Store애플리케이션을 다운로드하고 설치해야 구성 준수 합니다. 이 애플리케이션은 별도의 구독으로 사용할 수 있습니다.

시작하기 전에
설치하기 전에 설명된 애플리케이션 설정, 설치 및 구성 구성 준수 설정 검사 목록을 완료합니다. 이러한 설정 작업은 원활한 설치 및 구성을 위해 필요합니다.

필요한 역할: 관리자

프로시저

1. 제품을 옵트인 ServiceNow 하려면 다음 Opt in to the ServiceNow Store products 의 단계를 따르십시오.
2. 에서 ServiceNow Store구입한 애플리케이션을 설치하려면 다음 Install a ServiceNow Store application 의 단계를 따르십시오.
3. 옵션: 또는 다른 ServiceNow AI Platform 인스턴스에서 애플리케이션에 대한 구성 준수 권리를 관리하려면 다음Manage entitlements from your ServiceNow instance 의 단계를 따릅니다.
4. 애플리케이션을 이미 설치 구성 준수 했고 업데이트하려는 경우 문서를 참조하십시오 Install an update to a ServiceNow Store application .
5. 지원되는 애플리케이션을 설치합니다.

   별도의 외부 공급업체 애플리케이션은 에서 구성 준수데이터를 획득하고 변환합니다. 를 사용하여 구성 준수 구성 항목을 정정하려면 먼저 타사 스캐너 통합을 설치하고 하나 이상의 네트워크 스캔을 수행해야 합니다.

   에 대한 구성 준수외부 공급업체 통합 설치에 대한 자세한 내용은 문서를 참조하십시오 구성 준수 통합.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

담당 규칙 생성 또는 편집 구성 준수

필터 조건에 따라 테스트 결과를 자동으로 할당하는 규칙을 생성합니다. 이러한 규칙은 테스트 결과를 가져올 때 할당합니다.

시작하기 전에
필요한 역할: sn_vulc.admin

이 태스크 정보
기본 시스템에는 **CI** 지원 그룹과 동일한 할당 그룹에 테스트 결과를 할당하는 CI 지원 그룹에 할당이라는 하나의 구성 준수 할당 규칙이 함께 제공됩니다. 이 규칙은 기본적으로 비활성 상태입니다. 필터 조건 사용을 수정할 수 있습니다. 담당 규칙을 사용하여 하나 이상의 할당 조건과 실행 순서를 정의합니다. 테스트 결과가 규칙 조건과 일치하면 할당 조회가 중지됩니다.

주:
새 규칙이나 업데이트된 규칙은 다음 임포트 시 자동으로 평가되거나 담당 규칙 목록의 변경 내용 적용 단추를 사용하여 수동으로 평가됩니다.

프로시저

1. 다음으로 이동 모두 〉 구성 준수 〉 관리 〉 담당 규칙.
2. CI에 할당 지원 그룹 규칙을 열거나 새로 만들기를 클릭합니다.
3. CI에 할당 지원 그룹 규칙을 편집하거나, 신규인 경우 양식의 필드에 적절한 정보를 입력합니다.

구성 준수 할당 규칙

필드	설명
이름	할당 규칙의 이름입니다.
실행 순서	규칙이 평가되는 순서입니다. 가장 낮은 숫자가 먼저 평가됩니다. 우선 순위가 높은 규칙, 특별한 처리가 필요한 테스트 결과, 위험이 중요한 경우 또는 규정 준수에서 처리해야 하는 테스트 결과를 먼저 실행해야 합니다. 다음으로, 특별한 처리가 필요하지 않은 일반 규칙을 실행하고 누가 이를 담당해야 하는지 알 수 있습니다. 마지막으로, 어떤 할당 그룹에 속해야 하는지 파악하는 그룹에 테스트 결과를 할당하는 기본 규칙을 생성합니다. 이 그룹은 그들의 결정을 다루기 위해 또 다른 규칙을 추가할 수 있습니다. 이 기본 규칙은 마지막에 실행됩니다.
활성	할당 규칙이 활성 상태인지 여부를 나타냅니다.
조건	
조건 필드	충족되어야 하는 조건입니다. 조건 작성기에 입력한 검색 텍스트의 대소문자 구분은 이 기록이나 양식에서 지원되지 않습니다.
새 기준	선택할 조건 필터 필드를 더 추가합니다.
설명	할당 규칙을 설명하는 텍스트입니다.
할당 사용	이 규칙에 따라 생성된 그룹의 할당을 자동화하려면 사용 가능한 옵션 중 하나를 선택합니다. ○ 사용자 그룹: 조회 테이블에서 사용자 그룹을 선택합니다 ○ 사용자 그룹 필드: 드롭다운 메뉴에서 사용자 그룹 필드를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	○ 스크립트: 스크립트를 만들거나 편집합니다. 주: 스크립트를 만들거나 편집하려면 전문 지식이 필요합니다 ServiceNow .
사용자 그룹	의 조건과 일치하는 테스트 정정을 담당하는 사용자 그룹을 선택합니다.

4. 제출을 클릭합니다.

구성 준수 정정 대상 규칙

정정 대상 규칙을 사용하여 테스트 결과를 정정하기 위한 예상 시간 범위를 설정할 수 있습니다. 목표 날짜가 가까워지거나 기한이 지났을 때 사용자와 그룹에 알림을 보낼 수 있습니다.

중요사항:
구성 준수 관리자 또는 분석가는 취약성 관리자 작업 공간에서 특정 테스트 결과 집합에 대한 최신 정정 목표 날짜를 얻을 수 있습니다. 이 방법은 시간이 오래 걸리는 프로세스인 클래식 UI에서 모든 테스트 결과에 대해 정정 대상 규칙을 실행하는 것보다 더 효율적입니다. 자세한 내용은 에 있는 기록의 정정 속성 재평가 취약성 관리자 작업 공간 문서를 참조하십시오.

필요한 역할: 구성 준수 관리자(sn_vulc_admin) 또는 sn_vulc.manage_remediation_target_rules 역할을 가진 관리자.

주:
의 구성 준수v14.9부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v14.9 이전 용어	용어 **v14.9** 이상
테스트 결과 그룹	정정 작업
그룹 규칙	정정 작업 규칙
정책	테스트 그룹

정정 대상 규칙

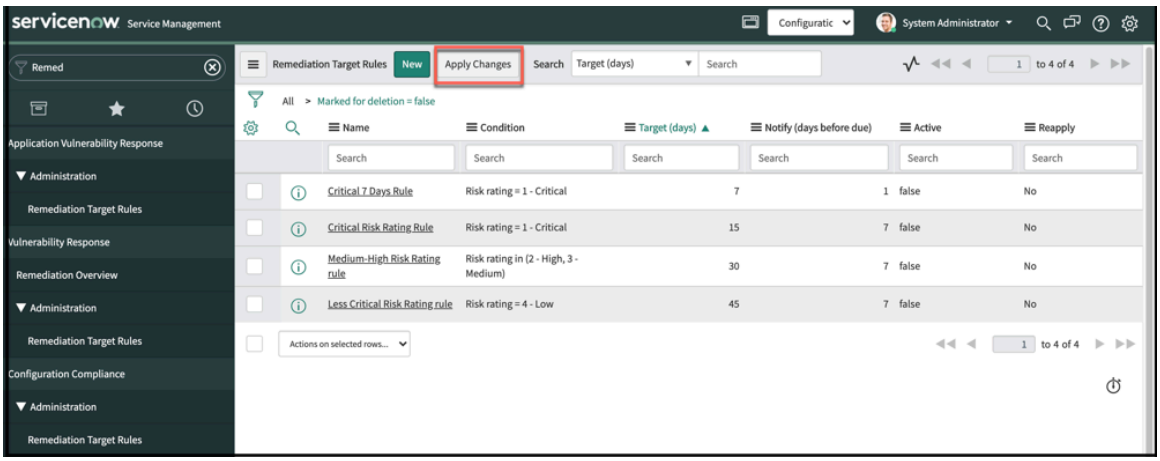
예약된 작업 *Evaluate and notify remediation targets*은 매일 실행되며 활성 정정 대상 규칙을 사용하여 활성 테스트 결과 기록을 평가합니다. 정정 작업과 연결된 테스트 결과 기록이 업데이트되거나 변경될 때마다 대상 규칙에 따라 수정된 값이 평가되고 변경 내용이 롤업되어 관련 정정 작업에 표시됩니다.

기존 정정 대상 규칙을 편집, 비활성화 또는 삭제하고 새 규칙을 생성할 수 있습니다. 새 규칙을 변경, 비활성화 또는 생성할 때 정정 대상 규칙 목록 보기에서 변경 내용 적용을 클릭하고 예약된 다음 작업 전에 도입한 변경 내용을 수동으로 적용할 수 있습니다. 이 옵션을 사용하면 기다릴 필요 없이 테스트 결과 기록을 다시 평가할 수 있습니다. 변경 내용을 수동으로 적용하도록 선택하지 않으면 다음 일일 예약 작업에서 변경 내용을 선택하고 적용합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

1. 다음으로 이동 모두 〉 구성 준수 〉 관리 〉 정정 대상 규칙 을 클릭하여 정정 대상 규칙을 봅니다.

정정 대상 규칙 목록 뷰에 변경 내용 적용



2. 이름 열에서 규칙을 클릭하여 해당 기록을 엽니다.
3. 정정 대상 규칙 기록에서 활성 확인란을 선택하여 비활성화된 규칙(true)을 활성화(true)합니다.

대상 규칙을 변경하거나 추가할 때마다 변경 내용을 수동으로 적용하도록 선택하든 예약된 다음 작업을 기다리든 관계없이 변경 내용은 변경 내용의 영향을 받는 다른 대상 규칙과 함께 모든 활성 테스트 결과를 평가하는 데 사용됩니다. 변경 내용을 수동으로 적용하기로 선택한 경우 변경의 영향을 받는 모든 규칙이 평가에 사용되므로 활성 테스트 결과의 양이 많은 경우 이 평가에 약간의 시간이 걸릴 수 있습니다.

예를 들어 대상 정정일 기본값은 30입니다. 대상 정정 일수가 30일인 새 규칙을 생성하면 이 규칙과 대상 날짜가 30일 이상인 대상 규칙이 각각 테스트 결과에 적용됩니다.

비활성화 및 삭제된 대상 규칙

규칙이 활성 상태이면 정정 대상 규칙 목록 뷰의 활성 열에 true 가 표시됩니다. 규칙이 비활성화되면 (false) 새 테스트 결과에 더 이상 적용되지 않습니다. 그러나 예약된 작업은 규칙이 적용된 기존 테스트 결과를 계속 추적합니다. 비활성화된 규칙이 이후에 다시 활성화되면 정정 대상 날짜 필드가 비어 있는 테스트 결과가 다시 활성화된 규칙에 대해 평가됩니다. 여기에는 규칙이 비활성화된 동안 생성된 테스트 결과가 포함됩니다.

규칙을 삭제해도 종결된 테스트 결과의 정정 목표 날짜 와 관련 필드는 유지됩니다. 종결되지 않은 테스트 결과의 정정 목표 날짜 와 관련 필드가 지워지고 모든 종속 규칙이 다시 적용됩니다.

규칙을 비활성화하려면 정정 대상 규칙 기록에서 활성 확인란을 비활성화하고 업데이트를 클릭합니다. False 가 정정 대상 규칙 목록 뷰의 활성 열에 표시됩니다.

규칙을 삭제하려면 양식에서 삭제를 클릭하거나, 목록 보기에서 규칙을 선택하고 행의 작업 목록에서 삭제를 클릭합니다. 해당 규칙은 더 이상 목록에 표시되지 않으며 작업 순서의 다음 규칙이 삭제된 규칙을 대체합니다.

규칙을 비활성화 또는 삭제하고 예약된 다음 작업 전에 변경 내용을 적용하도록 선택하면 규칙 참조가 필드에서 지워지지만 정정 날짜와 상태 데이터는 보존됩니다. 변경 내용을 수동으로 적용하지 않으면 다음 예약된 작업이 있는 필드에서 규칙 참조가 지워집니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

대상 규칙 및 정정 대상 평가 및 알림 예약된 작업 정보

Evaluate and notify remediation targets 예약된 작업은 매일 4:30:00에 한 번 실행됩니다. 활성 정정 대상 규칙을 선택하고 정정 대상 날짜가 가장 빠른 테스트 결과부터 시작하여 모든 활성 테스트 결과를 평가합니다. 다음 기준을 충족하는 모든 테스트 결과를 평가합니다.

- 종결 상태가 아닙니다.
- 정정 대상 날짜가 없습니다.
- 정정 대상 날짜가 정정 대상 규칙의 날짜보다 나중입니다.
- 스캐너 임포트가 완료된 후에 생성됩니다. 예약된 작업은 임포트의 결과로 생성된 새 테스트 결과를 선택하고 평가합니다.

대상 규칙이 정의되면 예약된 작업에 따라 *Evaluate and notify remediation targets* 정정 대상 날짜가 계산됩니다. 예약된 작업은 정정 목표 날짜가 없는 경우 이를 추가하거나, 이 규칙에 기록에 있는 날짜보다 이전 날짜가 포함되어 있는 경우 기존 대상 날짜를 업데이트합니다.

대상 규칙과 일치하는 만료된 기록 및 미리 알림 날짜가 작업에서 선택되고 알림이 전송됩니다. 사용하지 않도록 설정된 규칙의 경우 이 작업은 테스트 결과 기록의 정정 필드를 지우고 알림 전송을 중지합니다.

이 sn_sec_cmn.evaluate_targetmissed_records 속성을 활성화하면 예약된 작업이 대상 누락된 테스트 결과를 평가할 수 없습니다 *Evaluate and notify remediation targets* . 이 속성은 기본적으로 사용하도록 설정됩니다.

목록 및 양식 뷰에서 대상 날짜와 상태 보기

구성 준수 관리자는 테스트 결과 양식과 목록 뷰 모두에서 정정 목표 날짜를 볼 수 있습니다. 스캐너를 임포트한 후에도 정정 대상 규칙이 실행되고 테스트 결과가 다시 열리는 경우 다시 실행됩니다.

예약된 작업은 테스트 결과 목록 뷰에서 정정 대상 및 정정 상태를 업데이트하고 테스트 결과 양식의 정정 대상 규칙, 정정 대상 및 정정 상태 필드를 업데이트합니다.

주:
기본적으로 정정 대상 및 정정 상태 열은 테스트 결과 목록 뷰에 표시되지 않습니다. 이러한 열을 표시하려면 목록 뷰에도 추가해야 합니다. 마찬가지로 테스트 결과 양식에 정정 대상 규칙, 정정 대상 및 정정 상태 필드를 추가합니다.

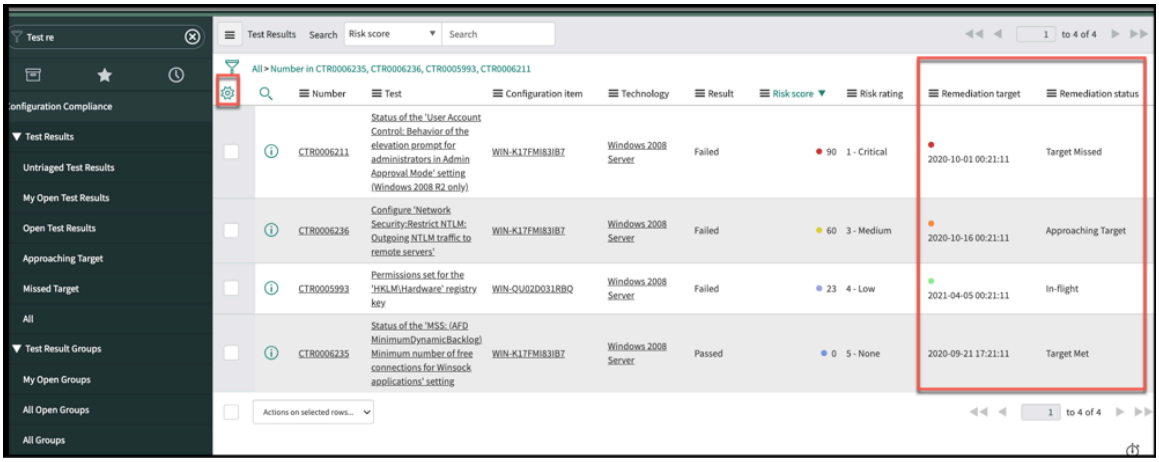
다음 이미지와 같이 설정 및 추가 작업 메뉴에서 슬러쉬버킷을 각각 사용하여 이러한 열과 필드를 표시합니다. 테스트 결과 기록의 추가 작업 메뉴에서 메뉴 아이콘을 클릭한 다음 구성 및 양식 레이아웃을 클릭하여 슬러시버킷을 보고 필드를 사용 가능 에서 선택됨으로 옮깁니다.

정정 목표 날짜는 테스트 결과 목록 뷰에 색상으로 표시된 점으로 표시됩니다.

- 알림 날짜에 도달하지 않은 테스트 결과는 녹색으로 표시됩니다.
- 정정 목표 날짜에 근접한 테스트 결과가 주황색으로 표시됩니다.
- 정정 목표 날짜가 지난 테스트 결과는 빨간색으로 표시됩니다.

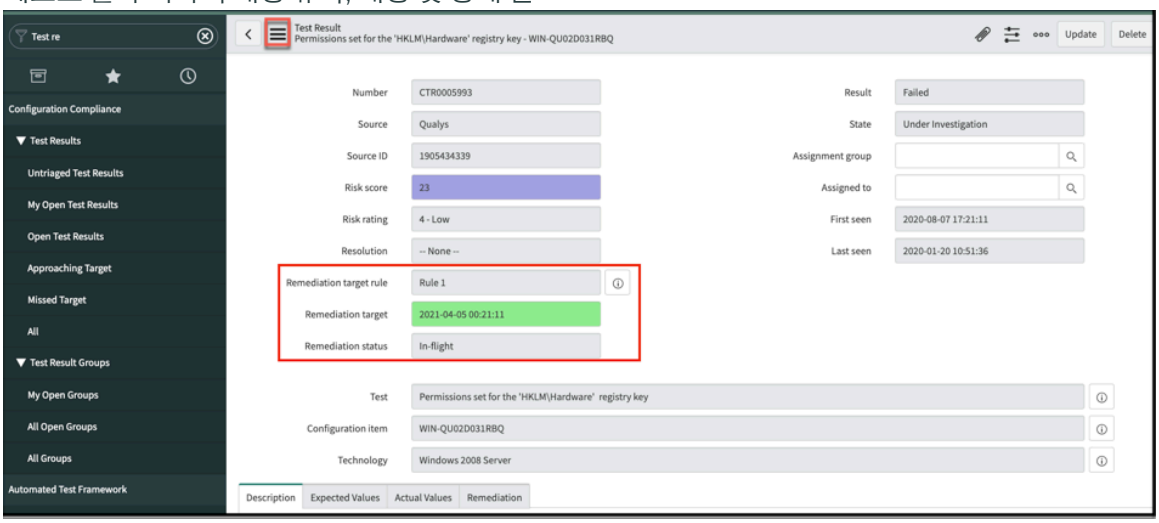
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테스트 결과 목록 뷰의 정정 대상 및 상태 열



- ## ##: 대상 날짜가 지났습니다.
- ## #: 테스트 결과가 진행 중입니다.

테스트 결과 기록의 대상 규칙, 대상 및 상태 필드



테스트 결과 기록은 대시보드에도 구성 준수 시각적으로 표시됩니다. 다음으로 이동 모두 〉 구성 준수 〉 개요 대시보드에서 상태를 확인합니다. 개요에는 기존 위젯 및 정정 상태가 포함됩니다. 그래프의 색상은 테스트 결과 목록 뷰 및 테스트 결과 기록에 표시되는 색상과 일치합니다.

정정 대상 규칙 시나리오

동일한 테스트 결과에 여러 정정 대상 규칙이 적용되면 가장 제한적인 규칙이 적용됩니다.

예를 들어 2018년 3월 1일에 처음 식별된 테스트 결과가 두 가지 정정 대상 규칙의 조건을 충족하는 경우:

- 정정 대상 규칙 1: 2018년 3월 7일에 정의됨; 개선 목표는 처음 발견된 후 15일입니다. 계산된 정정 목표 날짜는 03/16/2018 10:00:00입니다.
- 정정 대상 규칙 2: 2018년 3월 10일에 정의됨; 정정 목표는 처음 발견 후 10일입니다. 계산된 정정 목표 날짜는 03/11/2018 10:00:00입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

정정 목표는 마지막으로 표시된 날짜와 일 수(24시간 단위로 측정)의 합계로 계산됩니다.

V14.5부터 정정 대상은 대상(날짜)부터 계산됩니다. 기본값은 마지막으로 발견됨으로 유지됩니다. v14.12부터 기본값은 마지막 통과입니다.

이 시나리오에서는 테스트 결과가 처음 식별된 이후 10일과 15일로 더 제한적인 날짜가 있기 때문에 정정 대상 규칙 2가 테스트 결과에 적용됩니다.

대상 규칙을 생성 또는 수정하고 변경 내용을 다시 적용합니다.

1. 다음으로 이동 모두 〉 구성 준수 〉 관리 〉 정정 대상 규칙 을 사용하여 새 정정 대상 규칙을 보고, 편집하고, 생성합니다.
2. 이름 열에서 규칙을 클릭하여 대상 규칙을 열고 기록을 편집하거나, 또는 새로 만들기를 클릭하여 새 대상 규칙을 만듭니다.
3. 폼을 작성하여 예상 정정 기간을 정의하고, 조건을 사용하여 이 규칙이 적용될 테스트 결과를 지정하고, 미리 알림을 사용자나 그룹 또는 둘 다에 보낼 시기를 결정합니다.

정정 대상 규칙 양식

필드	설명
이름	규칙의 이름입니다.
활성	규칙을 사용하거나 사용하지 않도록 설정합니다. 이 규칙은 기본적으로 자동으로 활성화(true)되며 수동으로 또는 예약된 다음 작업 후에 변경 내용을 적용하도록 선택하면 테스트 결과에 적용됩니다.
목표(일수)	정정 대상 기한 날짜를 일 수로 설정합니다. 대상 정정 기간의 기본값은 30입니다. 예를 들어 대상 값에 대해 30이 있는 새 규칙을 만드는 경우 새 규칙과 대상 날짜가 30일 이상인 다른 기존 규칙이 테스트 결과에 적용됩니다.
대상 시작 날짜	대상 날짜를 계산하는 시작 날짜입니다. 날짜 또는 날짜 및 시간 유형 필드만 지정할 수 있습니다. v14.12 부터 기본값은 마지막 통과입니다. 다음 중 하나를 선택합니다. ○ 마지막으로 발견됨 ○ 처음 발견됨 ○ 작성됨 ○ 마지막 통과 마지막 패스가 비어 있으면 생성 날짜가 정정 대상 계산에 고려됩니다. ○ 마지막으로 열림 이 필드의 값을 사용자 지정하려면 KB1642413 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
알림(기한 이전 남은 일수)	사용자와 그룹에 이를 알리기 위해 기한 날짜 전의 일 수를 설정합니다.
설명	규칙에 대한 짧은 설명입니다.
조건	조건 작성기를 사용하여 이 규칙이 적용되는 테스트 결과를 지정합니다. 예를 들어, 위험 점수가 70보다 큰 모든 테스트 결과에 대해 정정 목표 날짜를 30일로 설정합니다. 정정 날짜 7일 전에 사용자나 그룹 또는 두 그룹 모두에게 미리 알림을 보냅니다. 조건 작성기에 입력한 검색 텍스트의 대소문자 구분은 이 기록이나 양식에서 지원되지 않습니다. v 12.0 이전에는 조건 작성기에 입력하는 검색 텍스트에 대해 대소문자 구분이 지원됩니다.
사용자 및 사용자 그룹 또는 둘 다	사용자 또는 그룹 또는 둘 다를 선택하여 설정한 목표 날짜가 임박했거나 기한이 지난 날짜에 대한 알림을 보냅니다.

4. 제출을 클릭합니다. 또는 편집된 규칙을 저장하려면 업데이트를 클릭합니다.

   목록 뷰가 업데이트된 규칙 또는 새 규칙과 함께 표시됩니다. 목록에 있는 규칙은 정정 대상 날짜가 가장 낮은 규칙부터 순서가 지정되고 실행됩니다. 규칙을 사용하지 않도록 설정하거나 삭제하면 순서 순서의 다음 규칙이 비활성 또는 삭제된 규칙을 대체합니다.

5. 새 변경 내용을 지금 적용하려면 변경 적용을 클릭합니다.

구성 준수 계산기 그룹

구성 준수 계산기는 사전 정의된 조건이 충족될 때 기록 값을 업데이트하는 데 사용됩니다. 계산기는 기록 업데이트 방법을 결정하는 데 사용되는 기준에 따라 그룹화됩니다.

주:
의 구성 준수v14.9부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v14.9 이전 용어	용어 **v14.9** 이상
테스트 결과 그룹	정정 작업
그룹 규칙	정정 작업 규칙
정책	테스트 그룹

구성 준수 계산기 그룹

기본 위험 계산기 기록에서 계산기 규칙을 영향을 받는 모든 테스트 결과 및 요청 시 수집에 적용할 수 있습니다. 취약성 관리자는 이 기능을 사용하여 위험 계산기 구성을 조정할 수 있습니다. 배포 초기에 여러 우선순위 지정 체계를 실험하고 이러한 변경 내용을 요청 시 적용하여 임포트 결과에 미치는 영향을 확인할 수 있습니다.

위험 점수 계산기 그룹의 이름이 위험 계산기로 변경되었습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

위험 점수 롤업 계산기는 에 포함되어 있습니다.구성 준수 개별 롤업 계산기에는 두 가지 유형이 있습니다.

구성 테스트 위험 롤업

구성 테스트에 대한 전체 위험 점수를 제공하기 위해 동일한 구성 테스트를 통해 모든 테스트 결과에 대한 위험 점수를 롤업하는 계산기 롤업된 값이 위험 점수 필드에 표시됩니다.

정정 작업 위험 점수 롤업

이러한 계산기는 정정 작업의 모든 테스트 결과에 대한 위험 점수를 롤업하여 해당 정정 작업에 대한 전체 위험 점수를 제공합니다. 롤업된 값이 위험 점수 필드에 표시됩니다.

위험 점수 계산기 그룹과 위험 점수 롤업 계산기 그룹은 기본적으로 모두 활성화되어 있습니다.

자세한 내용은 계산기에 대한 구성 준수 다음 주요 용어를 검토하십시오.

테스트 결과

테스트 결과는 CI(구성 항목) 및 관련 기술에 대한 구성 테스트의 결과입니다. 실패, 오류 및 알 수 없는 상태의 테스트 결과는 정책을 준수하지 않는 하드웨어, 소프트웨어 및 자산을 식별합니다.

정정 작업

테스트 결과는 미리 정의된 정정 작업 규칙에 따라 데이터를 임포트할 때 함께 그룹화됩니다. 이러한 정정 작업은 의 취약성 대응취약성 그룹과 유사합니다. 정정 작업은 대량 분석을 위해 테스트 결과를 그룹으로 구성하고 정정할 항목 집합을 나타냅니다.

테스트 결과의 위험 점수

자산의 비즈니스 컨텍스트 및 관련 테스트의 심각도를 기반으로 하는 위험 점수 계산기로 계산되는 값입니다. CMDB에 정의된 영향을 받는 자산의 비즈니스 중요도 및 스캐너에서 전달한 테스트 심각도의 평균입니다.

각 자산에는 여러 서비스가 연결될 수 있습니다. 자산의 비즈니스 중요도는 중요도가 가장 높은 서비스에 의해 결정됩니다.

계산된 값은 테스트 결과의 위험 점수 필드에 표시됩니다. 점수는 0-100 범위의 값을 표시합니다. 또한 필드는 색상으로 구분되어 심각도를 한 눈에 파악할 수 있습니다.

정정 작업의 위험 점수

이 점수는 정정 작업 기록에 표시되며 정정 작업의 모든 활성 테스트 결과에 대한 위험 점수의 롤업 값입니다. 정정 작업에서 테스트 결과가 정정되면 이 점수가 변경됩니다.

구성 테스트의 위험 점수

이 점수는 구성 테스트에 표시되며 해당 구성 테스트의 모든 활성 테스트 결과에 대한 위험 점수의 롤업된 값입니다. 이 구성 테스트와 연결된 테스트 결과가 정정되면 이 점수가 변경됩니다.

위험 등급

실패한 테스트 결과가 시스템에 미치는 위험의 양입니다. 이 점수는 위험을 위험(1)에서 없음(5)으로 평가하는 1-5 숫자 척도의 위험 점수 범위를 기반으로 합니다. 점수는 위험 점수의 범위를 기반으로 하며 위험 등급 필드에 표시됩니다.

위험 등급 범위

위험 등급	위험 점수
1 - 심각	90에서 100
2- 높음	70에서 89

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

위험 등급 범위

위험 등급	위험 점수
3- 중간	40에서 69
4- 낮음	1에서 39
5- 없음	0

위험 점수 롤업 계산기

롤업 계산기에는 두 가지 유형이 있습니다.

- 구성 테스트 위험 롤업: 이 계산기는 구성 테스트에 대한 전체 위험 점수를 제공하기 위해 동일한 구성 테스트를 통해 모든 테스트 결과에 대한 위험 점수를 롤업합니다. 롤업된 값이 위험 점수 필드에 표시됩니다. 이러한 계산기의 가중치 및 점수에 대한 스크립트 값을 편집할 수 있습니다.
- 정정 작업 위험 점수 롤업: 이 계산기는 정정 작업의 모든 테스트 결과에 대한 위험 점수를 롤업하여 해당 정정 작업에 대한 전체 위험 점수를 제공합니다. 롤업된 값이 위험 점수 필드에 표시됩니다. 이러한 계산기의 가중치 및 점수에 대한 스크립트 값을 편집할 수 있습니다. 위험 점수 롤업 계산기와 이 계산기의 점수 계산 방법에 대한 예는 문서를 참조하십시오 (v15.0 이전)에 대한 구성 준수 위험 롤업 계산 예.

이력 위험 점수

통과한 모든 테스트 결과의 고유 위험 점수는 정정 작업에 포함됩니다. 이 필드에는 테스트 그룹에서 정정한 위험의 양이 표시되며 테스트 그룹이 "종결" 상태이고 위험 점수가 0인 후에만 표시됩니다.

위험 점수가 변경될 때마다 또는 정정 작업에서 테스트 결과가 추가되거나 제거될 때 점수가 계산됩니다.

주:
이 스크립트가 제대로 작동하려면 플러그인이 서비스 매핑 필요합니다. 서비스 매핑 은 별도의 구독으로 사용할 수 있으며 담당자가 ServiceNow 활성화해야 합니다.

구성 준수 계산기 그룹 생성

구성 준수 계산기 그룹은 원하는 사용 방법에 따라 계산기를 그룹화하는 데 사용됩니다.

시작하기 전에
필요한 역할: sn_vulc.admin

이 태스크 정보
기본 시스템에는 구성 준수위험 점수라는 하나의 계산기 그룹이 포함됩니다. 다른 계산기를 만들 때 이 그룹에 추가하거나 다른 그룹 및 계산기를 만들 수 있습니다. 각 그룹 내에서 테스트 결과와 일치하는 첫 번째 계산기가 실행됩니다.

애플리케이션에는 구성 준수 두 개의 계산기 그룹이 포함되어 있습니다.

- 위험 계산기
- 위험 점수 롤업 계산기

위험 계산기는 테스트 결과의 위험 점수와 위험 등급을 계산합니다.

위험 점수 롤업 계산기는 전체 위험 점수를 제공하기 위해 동일한 구성 테스트를 통해 모든 테스트 결과 및 정정 작업에 대한 위험 점수를 롤업합니다.

또한 이러한 그룹에서 직접 새 계산기를 생성할 수도 있습니다.

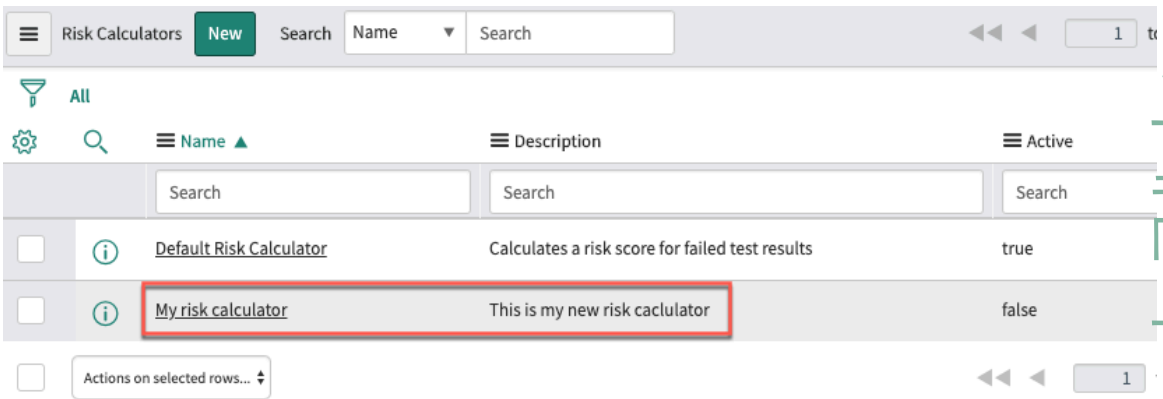
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 구성 준수 〉 관리 〉 계산기 그룹.
2. 다음으로 이동 모두 〉 구성 준수 〉 관리 을 클릭하고 위험 계산기 또는 위험 점수 롤업 계산기를 선택합니다.
3. 새로 만들기를 클릭합니다.
4. 양식의 필드에 적절히 입력합니다.

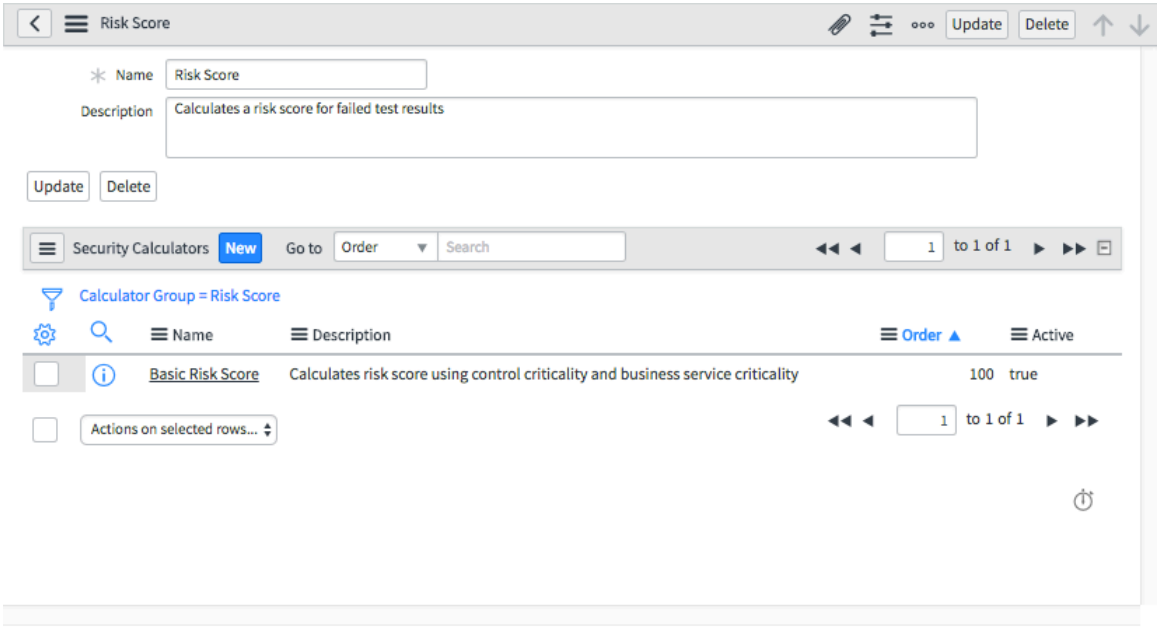
필드	설명
이름	계산기의 이름입니다.
설명	이 계산기 그룹에 대한 설명입니다.
활성	계산기 그룹을 활성화하거나 비활성화합니다.

5. 양식 헤더에서 저장을 마우스 오른쪽 버튼으로 클릭하거나 제출을 클릭합니다.
새 계산기 그룹이 다른 계산기와 함께 그룹 목록에 표시됩니다. 새 계산기 그룹의 이름을 클릭하여 기록을 엽니다. 조건 및 표시된 값을 설정하고 계산기를 다시 적용하는 방법에 대한 자세한 내용은 을 참조하십시오 에 대한 위험 계산기 생성, 편집 및 다시 적용 구성 준수 .



보안 계산기 관련 목록이 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



6. 새로 만들기를 클릭하여 해당 조건과 함께 계산기를 그룹에 추가합니다.

조건 작성기에 입력한 검색 텍스트의 대소문자 구분은 이 기록이나 양식에서 지원되지 않습니다.

구성 준수 계산기 및 계산기 규칙

구성 준수 테스트 결과 필드의 초기 값 계산을 자동화합니다. 각 계산기의 조건은 순서대로 평가되며 첫 번째로 일치하는 계산기가 사용됩니다.

구성 준수 계산기

구성 준수 기본 시스템에는 테스트 결과에서 기본 위험 점수를 설정하는 하나의 구성 준수 계산기(기본 위험 계산기)가 포함되어 있습니다. 구성 준수 계산기는 조건 필터를 사용하여 임의의 기준에 따라 테스트 결과의 영향도에 우선순위를 지정하고 평가하도록 빌드할 수 있습니다. 취약성의 비즈니스 영향, CI(구성 항목) 클래스 등에 관계없이 추가 구성 준수 계산기를 만들어 테스트 결과의 다른 필드를 설정하거나 기존 구성 준수 계산기를 사용자 지정할 수 있습니다. 계산기는 우선순위 집합을 반영하도록 작성할 수 있습니다.

각 계산기에는 규칙 적용 시기를 결정하는 조건과 함께 계산기 규칙 목록이 포함되어 있습니다. 계산기를 실행하면 각 계산기 규칙의 조건이 순서대로 평가되고 첫 번째로 일치하는 계산기 규칙이 사용됩니다.

활성화된 모든 구성 준수 계산기는 테스트 결과가 생성될 때마다, 연결된 CI 또는 구성 테스트가 변경될 때 또는 테스트 결과에서 위험 점수 계산 관련 링크가 사용될 때마다 선택한 필드를 설정합니다. 예를 들어, 임포트된 테스트 결과에서 control.criticality 값이 업데이트되면 테스트 결과 기록에서 위험 점수가 자동으로 업데이트됩니다. 테스트 결과 가져오기에서 테스트 결과 점수를 업데이트한 후 계산기 다시 적용 단추를 선택하여 테스트 결과의 위험 점수를 다시 계산할 수 있습니다.

기존 테스트 결과에서 위험 점수 계산 관련 링크를 선택하고 계산기 중 하나를 사용하도록 설정하면 테스트 결과의 위험 점수 필드가 업데이트됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

- 위험 점수 계산 관련 링크는 하나 이상의 구성 준수 계산기가 활성화된 경우에만 표시됩니다.
- v22.0 부터 취약성 대응기록 뷰에서 위험 점수 계산 버튼을 선택하여 취약성 관리자 작업 공간 및 IT 정정 작업 공간에서 테스트 결과에 대한 위험 점수를 업데이트할 수 있습니다.
- 의 버전 14.13 구성 준수부터는 테스트 결과의 위험 점수가 변경될 때마다 테스트 결과의 메모 섹션에 다음 상세 정보가 문서화됩니다.
  - 계산기 그룹 이름
  - 계산기 이름: 계산기 규칙이 템플릿 또는 스크립트를 기반으로 하는지 여부에 따라 괄호 안에 이름이 세부 정보와 함께 추가됩니다. 계산기 규칙의 기초를 수정하거나 보려면 규칙을 선택하고 고급 보기 확인란을 선택합니다. 값 유형 드롭다운 상자에서 필요한 옵션을 선택합니다. 템플릿을 선택하면 규칙에 지정된 조건에 따라 위험 점수가 업데이트됩니다. 스크립트를 선택한 경우 기존 스크립트를 추가하거나 업데이트할 수 있습니다.
  - 가중치 및 위험 점수 기여도가 있는 필드 값
  - 최종 위험 점수
  - 시스템 속성은 *sn_sec_cmn.risk_score_changes_add_worknotes* 작업 메모 섹션을 채우는 데 도움이 됩니다. 의 구성 준수v15.2.1부터 시스템 속성은 *sn_sec_cmn.risk_score_changes_add_worknotes* 기본적으로 비활성 상태입니다. 이 기능을 사용하도록 설정한 경우에만 작업 메모 섹션에서 테스트 결과의 위험 점수와 관련된 모든 변경 내용을 볼 수 있습니다. 또한 위험 점수가 변경된 경우에만 작업 메모가 업데이트됩니다.

구성 준수 계산기 규칙

기본적으로 기본 시스템 기본 위험 계산기 가 제공됩니다. 이 계산기에 대한 위험 규칙을 생성하려면 기본 위험 계산기 의 대상 필드를 위험 점수로 설정해야 합니다. 새 위험 규칙 버튼을 선택하여 새 위험 규칙을 만듭니다. 이렇게 하면위험 규칙이라는 특수 테스트 결과 계산기 규칙이 생성되어 여러 값을 기반으로 위험 점수 가 계산됩니다. 기본적으로 위험 점수를 계산하기 위해 다음 값이 고려됩니다.

- 비즈니스 중요도
- 중요도

기본 위험 규칙에 사용할 값과 이러한 각 값에 지정할 가중치를 조정할 수 있습니다. 가중치는 기본 위험 점수를 설정할 때 각 요소의 수를 조정하는 데 사용됩니다.

버전 13.0부터 구성 준수 기본 위험 규칙의 기준을 사용자 지정할 수 있습니다. 자세한 내용은 위험 규칙에 대한 필드 및 가중치 정의를 참조하십시오.

가중치 백분율 할당

필드 값 수준에서 가중치 백분율(0-100)을 할당할 수도 있습니다. 예를 들어, 심각도의 각 수준에 가중치 백분율을 할당할 수 있습니다(없음에서 중요). 위험 규칙에 대해 중요도 가중치가 50이고 중요도 수준에 대해 다음 가중치 값이 할당된 경우:

가중치 백분율 할당

중요도	위험 점수
중요	100
높음	50

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

가중치 백분율 할당

중요도	위험 점수
중간	20
안 함	0

중요도가 중요한 경우 해당하는 가중치는 50입니다. 중요도가 높으면 가중치가 25이고, 중요도가 중간이면 가중치는 10입니다. 중요도가 없음이면 해당 가중치는 0입니다. 자세한 내용은 구성 준수에 대한 위험 점수 계산 예시를 참조하십시오.

각 규칙에는 순서 설정이 있으며 조건과 일치하는 첫 번째 규칙이 테스트 결과의 위험 점수 필드를 업데이트합니다. 일반적으로 스크립트되지 않은 계산기 규칙은 스크립트된 계산기 규칙보다 성능에 미치는 영향이 적습니다.

기본 시스템 구성 준수 계산기에는 심각도에 따라 위험 점수 에 대한 각 중요도 수준(없음에서 위험)을 할당하는 계산기 규칙이 포함되어 있습니다. 알 수 없는 심각도에는 위험 점수 100이 자동으로 할당됩니다. 이러한 값은 기본 위험 계산기처럼 조정할 수 있으며, 새 계산기 규칙 또는 새 위험 규칙을 만들 수 있습니다.

취약성 위험 점수 가중치

모든 취약성에는 심각도, 중요도, 악용 정보 등의 요인에 따라 위험 점수와 등급이 할당됩니다. 취약한 항목 테이블의 비즈니스 규칙은 *`Update Risk Rating from Risk Score`* 위험 등급 계산을 담당합니다. 위험 점수가 변경될 때마다 취약한 항목에 대한 위험 등급이 계산되어 채워집니다. (VR) 애플리케이션 버전 17.1 취약성 대응 이전에는 하드 코딩된 스크립트 포함 VulnerabilityUtils의 일부로 다음 위험 등급이 제공되었습니다.

값(위험 등급)	가중치(위험 점수)
1	90–100
2	70–89
3	40–69
4	1–39
5	0

의 18.0 버전 취약성 대응부터

- 위험 등급 유형은 기본 테이블에 cc_risk_rating으로 제공됩니다. 이러한 유형은 위험 등급이 계산되는 각 테이블에서 비즈니스 규칙의 일부로 전달됩니다.
- 위험 등급 계산을 위해 위험 점수 가중치 테이블 값의 항목을 쿼리할 수 있도록 스크립트가 수정됩니다.
- 기존 형식에 대한 항목을 추가하거나 새 형식을 만듭니다. 새 유형을 만들 때는 새 위험 등급에 대한 레이블을 추가하고 관련 스크립트 및 비즈니스 규칙도 수정해야 합니다. 또한 새 위험 점수에 대한 새 스타일을 추가해야 합니다.
- 스크립트를 수정하여 기본 테이블의 기록을 쿼리합니다.

필터 탐색기에 sn_sec_cmn_risk_score_weight 입력하여 위험 점수 가중치 테이블에 액세스할 수 있습니다.

또한 다음 시나리오에서는 위험 점수가 자동으로 다시 계산됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- CI(구성 항목)가 비인터넷 연결에서 인터넷 연결로 변경되는 경우
- 취약성 항목(VI)에 대한 관련 CVE(알반적인 취약성 및 노출) 또는 외부 공급업체 항목(TPE)이 CVE Known Exploit 취약성(KEV)에 연결되는 경우

위험 규칙에 대한 필드와 가중치 정의

조직에 고유한 테스트 및 자산 데이터를 사용하는 위험 점수를 생성할 수 있도록 위험 규칙의 매개변수와 가중치를 사용자 지정합니다. 위험 규칙에 포함된 필드를 선택하여 효과적인 위험 점수 매기기 프레임워크를 정의할 수 있습니다.

시작하기 전에

필요한 역할: sn_vulc.admin

프로시저

1. 다음으로 이동 모두 〉 구성 준수 〉 관리 〉 위험 계산기.
2. 기본 위험 계산기를 클릭합니다.
3. 대상 필드를 위험 점수로 선택합니다.
   계산기 규칙 테이블에 새 위험 규칙 버튼이 표시됩니다.
4. 새 위험 규칙 버튼을 클릭하여 구성 준수 위험 규칙 양식으로 이동합니다.
5. 위험 계산기 기준 섹션에서 전체 위험 점수 계산에서 중요도에 따라 각 기준의 가중치를 설정합니다.
6. 활성 확인란의 선택을 취소하여 규칙을 비활성화합니다.
7. 위험 계산 기준에 위험 규칙 필드를 추가하려면 기준 추가를 클릭합니다.
8. 양식에서 필드를 채웁니다.

위험 규칙 필드 양식

필드	설명
참조 테이블 선택	위험 점수 가중치를 정의하는 데 사용하는 테이블입니다. 다음 옵션 중에서 선택합니다. ○ 테스트 결과: 테스트 결과(TR)에서 직접 닷워킹할 수 있는 필드를 추가합니다. ○ 테스트 결과 - 구성 항목: 하드웨어 테이블과 같은 기본 테이블 확장의 일부인 dot walkable 필드를 추가합니다. 이러한 필드는 기본 cmdb_ci 테이블의 일부가 아닙니다. ○ 테스트 결과 - 테스트: 기본 테이블을 확장하는 테이블의 일부인 dot-walkable 필드를 추가합니다(예: 외부 공급업체 항목). 이러한 필드는 구성 테스트 기본 테이블의 일부가 아닙니다. ○ 테스트 결과 참조 테이블: 관련 테이블(m2m) 또는 테스트 결과에 대한 참조가 있는 테이블의 일부인 필드를 추가합니다. 이러한

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	필드는 테스트 결과에서 직접 닷워킹할 수 없습니다. ○ 구성 항목 참조 테이블: cmdb_ci에 대한 참조가 있는 cmdb_ci의 관련 테이블(m2m)에 속하는 필드를 추가합니다. 이러한 필드는 TR에서 직접 닷워킹할 수 없습니다. ○ 테스트 참조 테이블: sn_vulc_test에 대한 참조가 있는 sn_vulc_test 또는 테이블의 관련 테이블(m2m)에 속하는 필드를 추가합니다. 이러한 필드는 TR에서 직접 닷워킹할 수 없습니다. ○ 사용자 지정 조건: 조건을 평가하여 규칙에 가중치를 할당하려면 이 옵션을 사용합니다. 예를 들어 인터넷 연결 필터는 CI(구성 항목)가 외부인지 내부인지를 결정합니다.
필드	이 규칙의 위험 점수 계산에 사용되는 필드입니다.
가중치	위험 규칙 내에서 이 필드의 가중치입니다. 값은 0에서 100 사이의 정수여야 합니다.
테이블	○ 구성 항목에 > 테스트 결과 ○ 테스트 결과 > 테스트 ○ 테스트 결과 참조 테이블 ○ 구성 항목 참조 테이블 ○ 테스트 참조 테이블 이 필드는 참조 테이블 선택 필드에서 나열된 옵션 중 하나를 선택한 경우에만 나타납니다.
집계	관련 테이블(m2m)에서 필드를 선택할 때 계산에 고려할 최소값 또는 최대값을 선택합니다. 이 필드는 참조 테이블 선택 필드에서 참조 테이블을 선택한 경우에만 나타납니다.
값 가중치 정의	각 필드 값에 가중치를 할당하는 구성요소입니다. 숫자 필드의 경우 필드 값을 범위(예: 1-5)로 정의합니다. 값은 0에서 100 사이의 정수여야 합니다. 참조 테이블 선택 필드에서 사용자 지정 조건 옵션을 선택한 경우에는 이 필드가 표시되지 않습니다.
조건 테이블	목록에서 조건을 선택합니다. 이 필드는 참조 테이블 선택 필드에서 사용자 지정 조건 옵션을 선택한 경우에만 나타납니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
필드 이름	위험 기준의 이름을 입력합니다. 이 필드는 참조 테이블 선택 필드에서 사용자 지정 조건을 선택한 경우에만 나타납니다.
조건	정의된 조건과 일치하는 이 테이블의 항목을 미리 봅니다. 이 필드는 참조 테이블 선택 필드에서 사용자 지정 조건을 선택한 경우에만 나타납니다.

9. 제출을 클릭합니다.

다음에 수행할 작업

규칙 페이지에서 규칙을 활성화하고 다시 적용하여 활성 테스트 결과의 위험 점수를 다시 평가합니다.

에 대한 위험 롤업 계산기 편집 구성 준수

기존 위험 롤업 계산기를 편집합니다.

시작하기 전에

필요한 역할: 필요한 역할: sn_vulc.admin

프로시저

1. 다음으로 이동 모두 〉 구성 준수 〉 관리 을 클릭하고 위험 점수 롤업 계산기를 선택합니다.

2. 위험 점수 롤업 계산기 목록이 표시되면 계산기를 클릭하여 기록을 열고 양식을 편집합니다.

필드	설명
이름	구성 테스트 또는 정정 작업 롤업 계산기의 이름입니다.
설명	위험 롤업 계산기에 대한 설명입니다.
테이블	롤업 계산기가 적용되는 테이블입니다.
연기 포함	위험 점수를 롤업하는 동안 지연된 테스트 결과를 포함합니다.

3. 다음 방법 중 하나로 가중치를 정의합니다.

- 롤업 가중치 섹션에서 다음에 대한 가중치를 할당합니다.

롤업 가중치

필드	설명	기본 가중치
최대 위험 점수	테스트 결과의 최대 위험 점수가 고려됩니다.	85
평균 위험 점수	고려된 모든 테스트 결과의 위험 점수 집계입니다.	0
테스트 결과 수	테스트 결과 수입니다.	15

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 고급 뷰 확인란을 선택하고 스크립트 값 편집기에서 필요에 따라 스크립트의 값을 편집합니다.

  주:
  스크립트를 편집하려면 구성 준수 및 ServiceNow AI Platform 애플리케이션에 대한 고급 지식이 필요합니다.

4. 업데이트를 클릭하여 편집 내용을 저장합니다.

롤업 계산기는 변경 내용을 적용하기 위해 매시간 실행되는 예약된 작업입니다. 이러한 예약된 작업은 구성 테스트 및 정정 작업에 대한 전반적인 위험 점수이기도 합니다. 롤업된 값이 위험 점수 필드에 표시됩니다.

위험 롤업 계산기가 점수를 결정하는 방법의 예는 다음 문서를 참조하십시오 (v15.0 이전)에 대한 구성 준수 위험 롤업 계산 예.

에 대한 위험 계산기 생성, 편집 및 다시 적용 구성 준수

계산기 규칙은 영향을 받는 모든 테스트 결과 및 수집에 요청 시 적용할 수 있습니다. 취약성 관리자는 이 기능을 사용하여 위험 계산기 구성을 조정하고 요청 시 변경 내용을 적용하여 결과를 임포트할 수 있습니다.

시작하기 전에
필요한 역할: sn_vulc.admin

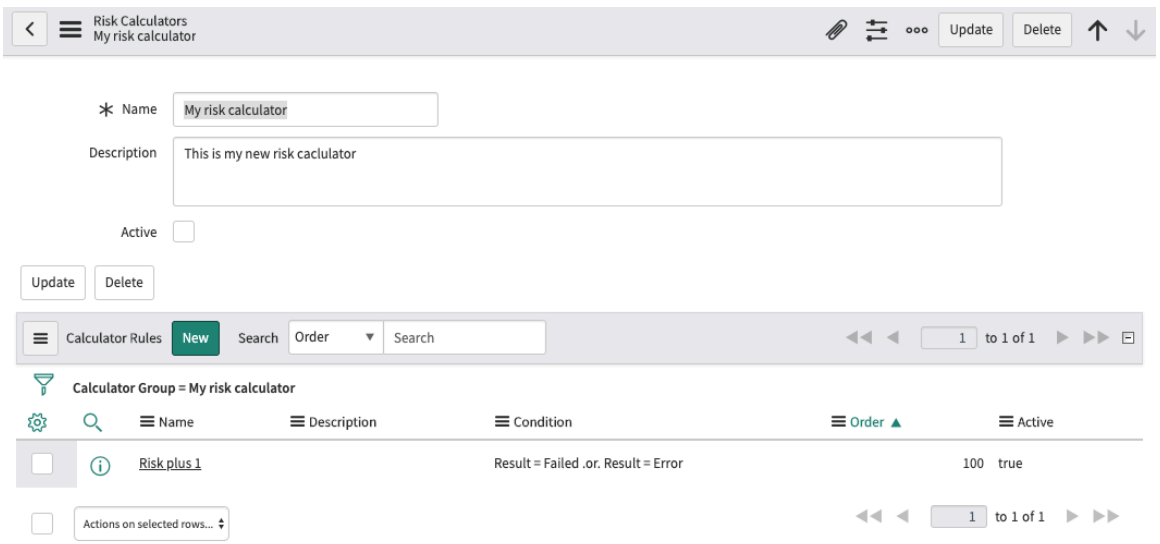
프로시저

1. 새 위험 계산기를 만들려면 다음 단계를 수행합니다.

   a. 다음으로 이동 모두 〉 구성 준수 〉 관리 을 클릭하고 위험 계산기를 선택합니다.

   b. 위험 계산기 목록에서 새로 만들기를 클릭합니다.

   c. 새 계산기의 이름과 설명을 입력하고 제출을 클릭합니다.
   새 계산기가 위험 계산기 목록에 표시됩니다.



   d. 목록에서 새 계산기를 클릭하여 계산기가 실행되는 조건을 만들고 테스트 결과 기록 및 정정 작업에 표시할 필드와 값을 지정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

e. 표시되는 레코드에서 **New**를 클릭합니다.

f. 탭의 필드를 적절하게 입력합니다.

탭	설명
이 조건이 충족될 경우	조건 작성기를 사용하여 계산기가 실행되는 조건을 만듭니다. 예를 들면 다음과 같습니다. ### ##### ### #####.
이 값 설정	템플릿을 사용하여 표시할 필드와 값을 선택합니다.

g. 제출을 클릭합니다.
새 계산기 규칙과 해당 규칙이 속한 그룹과 함께 기록이 표시됩니다.

2. 기존 계산기를 테스트 결과에 다시 적용하거나 기존 위험 계산기의 규칙과 표시된 값을 편집하려면 다음 단계를 수행합니다.

a. 위험 계산기 또는 위험 롤업 계산기 목록에서 편집할 계산기를 선택합니다.

b. 기록의 기존 테스트 결과 데이터에 위험 계산기를 다시 적용하려면 계산기 다시 적용을 클릭합니다.
계산기의 조건을 충족하는 모든 테스트 결과가 업데이트됩니다.

> **주:**
> 테스트 결과 수에 따라 이 업데이트에는 시간이 걸릴 수 있습니다.

c. 조건과 값을 편집하려면 왼쪽 아래의 이름 열에서 계산기 이름을 클릭합니다.
위험 계산기의 경우 기록과 이 조건이 충족되는 경우 및 다음 값 설정 탭이 표시됩니다.

d. 양식을 적절하게 작성합니다.

탭	필드 설명
이 조건이 충족될 경우	필터 조건 빌더를 사용하여 계산기를 실행할 조건을 생성합니다.
이 값 설정	계속하려면 하나를 선택합니다. ▪ 값 유형 - 템플릿입니다. 목록에서 필드와 해당 값을 선택합니다. ▪ 스크립트 - 편집기를 사용하여 변경 내용을 입력합니다. **주:** 스크립트를 편집하려면 구성 준수 및 ServiceNow AI Platform 애플리케이션에 대한 고급 지식이 필요합니다.

3. 옵션: 요청 시 기존 테스트 결과 데이터에 새 규칙을 적용하려면 다음 단계를 수행합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 위험 계산기 목록이 표시되면 적용할 계산기를 클릭합니다.
기록이 표시됩니다.

b. 계산기 다시 적용을 클릭하여 요청 시 변경 내용을 임포트 결과에 적용하고 테스트하십시오.

4. 테스트 결과의 변경 내용을 보고 필요한 경우 계산기를 계속 편집합니다.

위험 점수 계산의 구성 준수 예

의 구성 준수v13.0부터 기본 위험 규칙의 기준을 사용자 지정할 수 있습니다. 위험 점수 계산에 Qualys 및 Tenable과 같은 외부 공급업체 벤더가 제공하는 위험 점수를 사용합니다.

Qualys 및 Tenable과 같은 외부 공급업체 벤더는 자체 점수를 제공합니다. 이러한 점수는 sn_vulc_test 테이블의 중요도 필드에 채워집니다. 이 필드는 위험 점수 계산에 사용합니다. 이 점수를 사용하여 위험 점수를 계산하려면 다음 절차를 따르십시오.

소스 중요도를 위험 규칙의 기준으로 추가

외부 공급업체 벤더가 제공한 중요도를 기준으로 점수를 사용하여 위험 점수를 계산합니다.

시작하기 전에
필요한 역할: sn_vulc.admin

이 태스크 정보
Qualys 및 Tenable과 같은 외부 공급업체 벤더는 자체 위험 점수를 제공합니다. 이러한 점수는 sn_vulc_test 테이블의 중요도 필드에 채워집니다. 이 필드는 위험 점수를 계산하고 위험 점수를 계산하는 데 사용합니다.

프로시저

1. 다음으로 이동 모두 〉 구성 준수 〉 관리 〉 위험 계산기.

2. 위험 규칙 양식으로 이동합니다.

3. 활성 확인란의 선택을 취소하여 규칙을 비활성화합니다.

4. **Add** Criteria(기준 추가)를 클릭합니다.

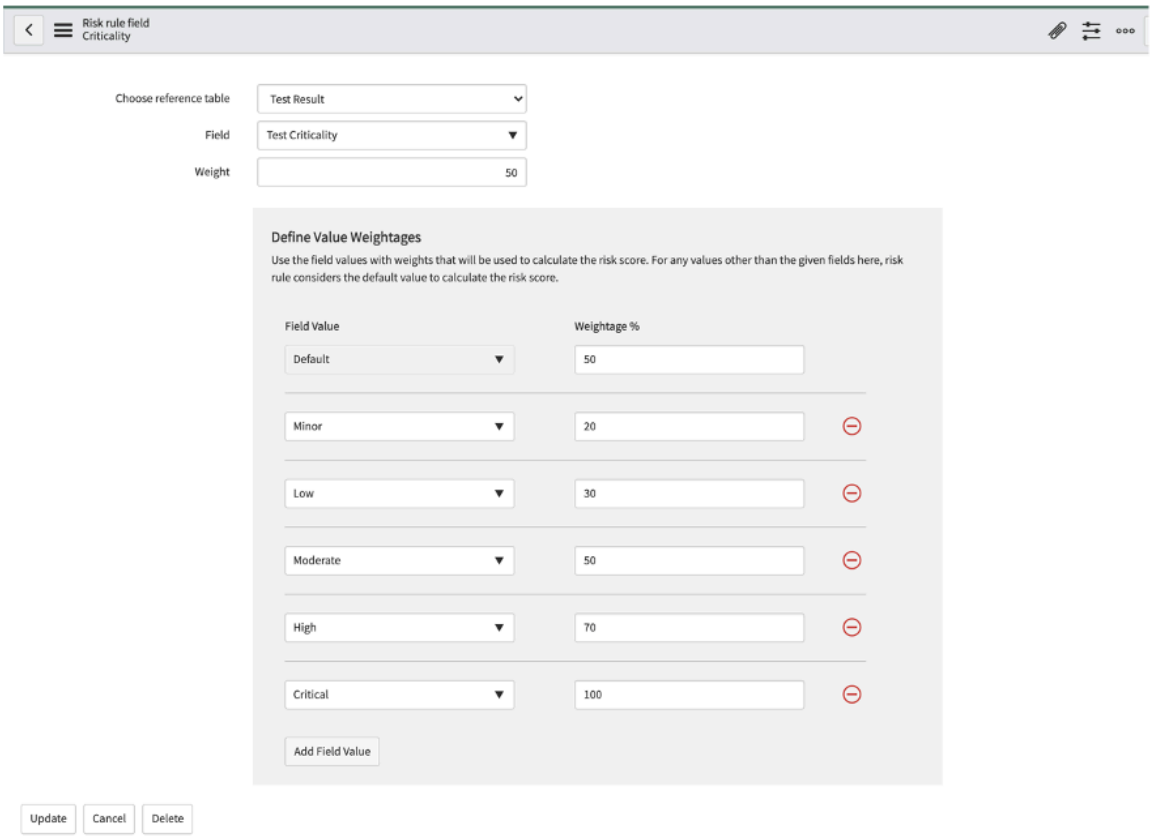
5. 참조 테이블 선택 목록에서 테스트 결과를 선택합니다.

6. 필드 목록에서 **Test.Criticality**를 선택합니다.

7. 가중치 필드에서 이 필드의 상대적 중요도를 지정합니다.
값은 0에서 100 사이의 정수여야 합니다.

8. 값 가중치 정의 섹션에서 필드 값을 추가하고 필드에 가중치 백분율을 할당합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



9. 제출을 클릭합니다.

위험 규칙의 기준으로 비즈니스 중요도 추가

비즈니스 서비스에 대한 중요도 값을 지정하고 비즈니스 중요도를 사용하여 위험 점수를 계산합니다.

시작하기 전에

필요한 역할: sn_vulc.admin

이 태스크 정보

조직에 많은 비즈니스 서비스가 있고 다음 서비스에서 CI(구성 항목)를 사용한다고 가정합니다.

비즈니스 서비스의 중요도

비즈니스 서비스	중요도
클라우드 관리	1 - 가장 중요함
전자 상거래	2 - 다소 중요함
클라이언트 서비스	3 - 덜 중요함
출장 및 경비	4 - 중요하지 않음

CI와 서비스 간의 매핑은 서비스 [cmdb_ci_services] 테이블에 저장됩니다. CI가 구성 테스트를 통과하지 못하면 테스트 결과(TR)가 생성됩니다. 영향을 받는 서비스의 비즈니스 중요도 값을 사용하여 이 TR의 위험 점수를 계산할 수 있습니다. 절차에 따라 이러한 서비스의 중요도 값을 사용하여 위험 점수를 계산합니다.

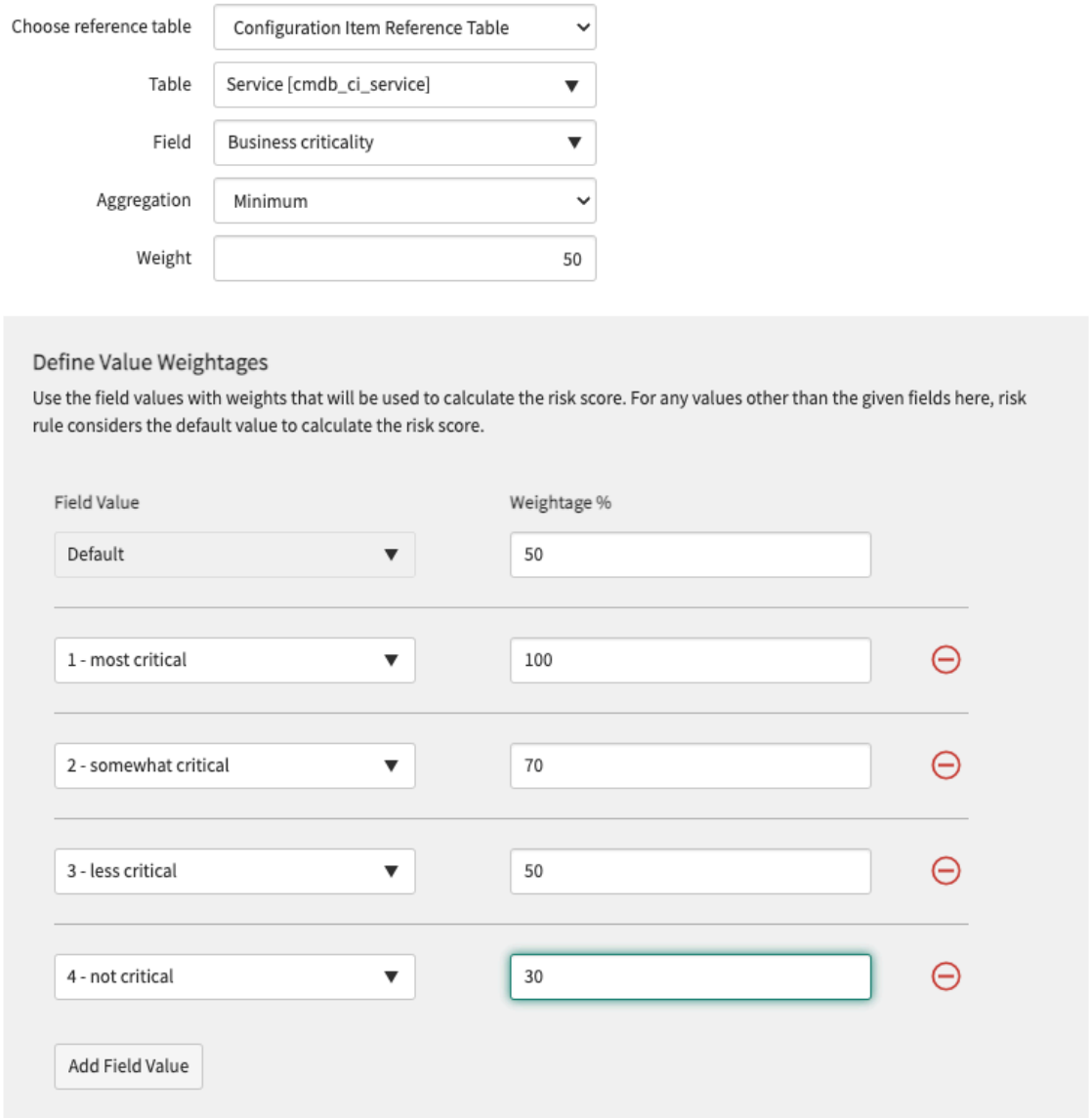
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 구성 준수 〉 관리 〉 위험 계산기.
2. 계산기 규칙 섹션에서 위험 규칙 양식으로 이동합니다.
3. 활성 확인란의 선택을 취소하여 규칙을 비활성화합니다.
4. **Add** Criteria(기준 추가)를 클릭합니다.
5. 참조 테이블 선택 목록에서 구성 항목 참조 테이블을 선택합니다.
6. 테이블 목록에서 서비스 [cmdb_ci_service]를 선택합니다.
7. 필드 목록에서 비즈니스 중요도를 선택합니다.
8. 집계 필드에서 최소를 선택하여 이 사용 사례에 대해 가장 중요한 서비스(1 - 가장 중요한 값)를 검색하거나 최대를 선택하여 이 사용 사례에 대해 가장 중요하지 않은 서비스(4 - 중요하지 않은 값)를 검색합니다.
9. 가중치 필드에서 이 필드의 상대적 중요도를 지정합니다.
   값은 0에서 100 사이의 정수여야 합니다.
10. 값 가중치 정의 섹션에서 필드 값을 추가하고 가중치를 할당합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용자 지정 비즈니스 중요도 위험 규칙 가중치



11. 제출을 클릭합니다.

위험 계산기에 조건부 기준 추가

위험 점수 계산을 위해 위험 규칙에 사용자 지정 조건을 사용합니다.

시작하기 전에
필요한 역할: sn_vulc.admin

이 태스크 정보
조직에 여러 개의 구성 항목(CI)이 있고 그 중 일부만 외부 사용자가 액세스할 수 있다고 가정합니다. 사용자는 이러한 외부 방향 CI에 대해 위험 점수 가중치를 추가할 수 있습니다.

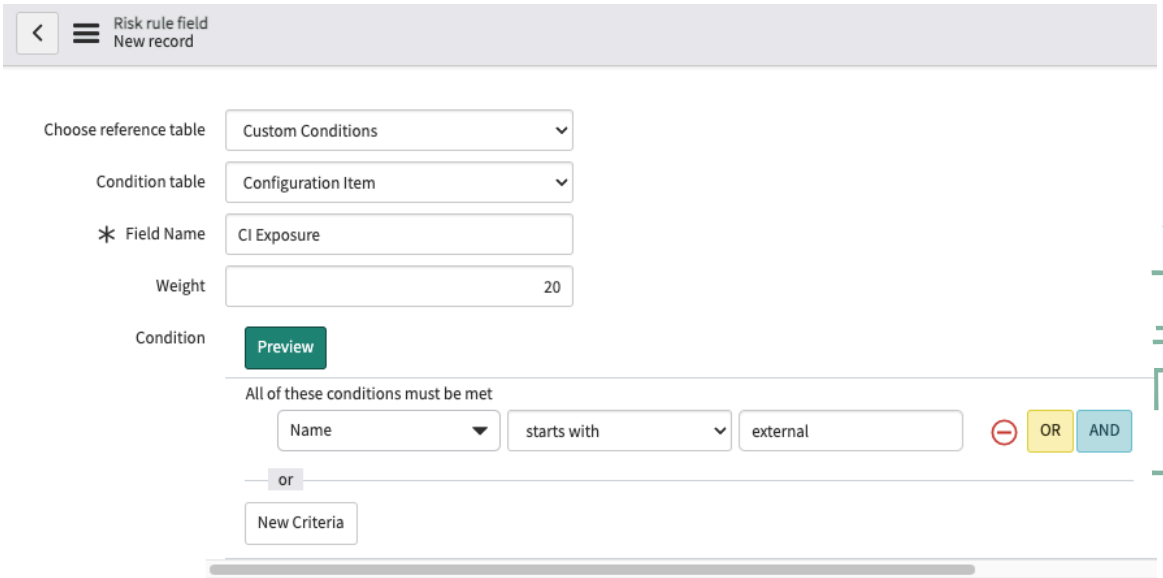
주:
이러한 CI는 이름으로 식별할 수 있습니다. 이름은 'external'로 시작합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 구성 준수 〉 관리 〉 위험 계산기.
2. 위험 규칙 양식으로 이동합니다.
3. 활성 확인란의 선택을 취소하여 규칙을 비활성화합니다.
4. **Add** Criteria(기준 추가)를 클릭합니다.
5. 참조 테이블 선택 목록에서 사용자 지정 조건을 선택합니다.
6. 조건 테이블 목록에서 구성 항목을 선택합니다.
7. 필드 이름 필드에 CI Exposure를 입력합니다.
8. 가중치 필드에서 이 필드의 상대적 중요도를 지정합니다.
   값은 0에서 100 사이의 정수여야 합니다.
9. 조건 필드에서 다음으로 시작하는 **>** 이름을 선택하고 값을 ##로 지정합니다.

새 위험 규칙에 대한 사용자 지정 조건



10. 제출을 클릭합니다.

관련 정보

구성 준수 계산기 그룹

에 대한 위험 점수 계산 예 구성 준수

위험 점수 계산기를 결정하여 해당 조직과 관련된 테스트 및 자산 데이터를 사용하는 위험 점수를 생성합니다.

위험 규칙 계산기 점수 결정의 예

다음 예는 위험 규칙 계산기의 점수가 결정되는 방법을 보여줍니다. 이 테이블의 필드로 위험 규칙 계산기가 구성되어 있다고 가정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

위험 규칙 계산기 점수 결정

필드	가중치	가중치 세부 항목
통제.중요도	50	기본값: 0 부: 20 낮음: 30 보통: 50 높음: 70 중요: 100
Business_Criticality	50	기본값: 0 부: 20 낮음: 30 보통: 50 높이: 70 중요: 100

이 표에 표시된 테스트 결과가 시스템에 있다고 가정합니다.

테스트 결과 매핑

ID	비즈니스 중요도	통제 중요도
CTR0000001	1 - 가장 중요	경미
CTR0000002	1 - 가장 중요	낮음
CTR0000003	2 - 다소 중요	경미
CTR0000004	2 - 다소 중요	보통
CTR0000005	3 - 덜 중요	낮음

테스트 결과에 대한 위험 점수 계산은 다음 수식에 따라 계산됩니다.

위험 점수 = (W(통제.중요도) * FV(통제.중요도). + W(business_criticality) * FV(business_criticality)) / 100, 여기서 W는 가중치이고 FV는 필드 값의 가중치 백분율입니다.

이러한 테스트 결과에 대한 결과 위험 점수는 다음 표에 설명되어 있습니다.

테스트 결과에 따른 위험 점수

ID	비즈니스 중요도(50%)	통제 중요도(50%)	결과 위험 점수
CTR0000001	1 – 가장 중요(50% x100)	경미(50% x 20)	60

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테스트 결과에 따른 위험 점수

ID	비즈니스 중요도(50%)	통제 중요도(50%)	결과 위험 점수
CTR0000002	1 – 가장 중요(50% x100)	낮음(50% x 30)	65
CTR0000003	2 - 다소 중요(50% x 70)	경미(50% x 30)	45
CTR0000004	2 - 다소 중요(50% x 70)	보통(50% x 50)	60
CTR0000005	3 – 덜 중요(50% x 50)	낮음(50% x 30)	40

필드 값 중 하나에 대해 가중치 백분율이 변경된 경우 결과는 다음 표를 참조하십시오.

변경된 가중치 백분율에 대한 결과

필드	가중치	가중치 세부 항목
통제.중요도	50	기본값: 0 부: 20 낮음: 30 보통: 60 높이: 70 중요: 100
Business_Criticality	50	기본값: 50 1 – 가장 중요: 100 2 – 다소 비판적: 70 3 – 덜 중요: 20 4 – 중요하지 않음: 30

계산기를 다시 적용한 후 테스트 결과에 대한 위험 점수는 다음 표에 표시됩니다.

계산기 재적용 시 TR에 대한 위험 점수

ID	비즈니스 중요도(50%)	통제 중요도(50%)	결과 위험 점수
CTR0000001	1 – 가장 중요(50% x 100)	경미(50% x 20)	60
CTR0000002	1 – 가장 중요(50% x 100)	낮음(50% x 30)	65
CTR0000003	2 - 다소 중요(50% x 70)	경미(50% x 30)	45
CTR0000004	2 - 다소 중요(50% x 70)	보통(50% x 60) *수정된 값	65 *수정된 값

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

계산기 재적용 시 TR에 대한 위험 점수

ID	비즈니스 중요도(50%)	통제 중요도(50%)	결과 위험 점수
CTR0000005	3 - 덜 중요(50% x 20) *수정된 값	낮음(50% x 30)	25 *수정된 값

(v15.0 이전)에 대한 구성 준수 위험 롤업 계산 예

다음 예는 위험 롤업 계산기의 점수가 결정되는 방식을 보여줍니다.

다음 정정 작업 롤업 계산기에서 정정 작업 위험 점수를 계산하는 수식은 다음과 같습니다.

(최대 위험 점수/100) * 85 + (계수 * 15).

위 방정식의 요인은 다음 표와 같이 테스트 결과 수에 따라 결정됩니다.

테스트 결과 수	요인
〈10	0.2
10-99	0.4
100-1000	0.6
1001-9999	0.8
〉10000	1

다음 정정 작업의 경우, TRG0003066, 세 개의 테스트 결과 위험 점수가 있는 경우 최대 점수는 90입니다.

번호	위험 점수	정정 작업	결과	상태
CTR000123	90	TRG0003066	실패함	오픈
CTR000124	70	TRG0003066	실패함	오픈
CTR000125	40	TRG0003066	실패함	오픈

정정 작업의 경우 다음을 TRG0003066.

위험 점수는 79, (90/100) * 85 + 0.2 * 15 = Math.floor (76.5 +3) = 79입니다.

정정 작업이 아직 "오픈" 상태이므로 이력 위험 점수가 null입니다.

데이터 수집 후 테스트 결과가 '통과'되고 다음 표와 같이 정정 작업이 '종결'로 전환됩니다.

번호	위험 점수(v15.0 이전)	정정 작업	결과	상태
CTR000123	0	TRG0003066	통과함	종결됨
CTR000124	0	TRG0003066	통과함	종결됨
CTR000125	0	TRG0003066	통과함	종결됨

테스트 결과 기록은 다음 표에 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

번호	위험 점수	최신 결과	결과
CTRH000111	90	CTR000123	실패함
CTRH000112	70	CTR000124	실패함
CTRH000113	40	CTR000125	실패함

정정 작업에 활성 테스트 결과가 없기 때문에 위험 점수는 0입니다.

정정 작업의 경우 다음을 TRG0003066.

과거 위험 점수는 79: (90/100) * 85 + 0.2 * 15 = Math.floor (76.5 +3) =79입니다.

에 대한 구성 준수 위험 롤업 계산 예 **(v15.0** 이상)

다음 예는 위험 롤업 계산기의 점수가 결정되는 방식을 보여줍니다.

다음 정정 작업 롤업 계산기에서 정정 작업 위험 점수를 계산하는 수식은 다음과 같습니다.

(최대 위험 점수* 80/100) + (평균 위험 점수* 5/100) + (요인 * 15)

여기서 가중치는 다음과 같습니다.

- 최대 위험 점수: 80
- 평균 위험 점수: 5
- 계수: 15

평균 위험 점수의 기본 가중치는 0입니다. 가중치를 설정하는 방법에 대한 자세한 내용은 문서를 참조하십시오 에 대한 위험 롤업 계산기 편집 구성 준수.

위 방정식의 요인은 다음 표와 같이 테스트 결과 수에 따라 결정됩니다.

테스트 결과 수	요인
〈10	0.2
10-99	0.4
100-1000	0.6
1001-9999	0.8
〉10000	1

다음 정정 작업 TRG0003066의 경우, 세 가지 테스트 결과가 위험 점수인 경우 최대 위험 점수는 90이고 평균 위험 점수는 66.67입니다.

번호	위험 점수	정정 작업	결과	상태
CTR000123	90	TRG0003066	실패함	오픈
CTR000124	70	TRG0003066	실패함	오픈
CTR000125	40	TRG0003066	실패함	오픈

정정 작업의 경우 다음을 TRG0003066.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

위험 점수는 81, (90* 80/100) + (66.67* 5/100) + (0.2 * 15) = Math.floor (78.3 +3) = 81입니다.

정정 작업이 아직 "오픈" 상태이므로 이력 위험 점수가 null입니다.

데이터 수집 후 테스트 결과가 '통과'되고 다음 표와 같이 정정 작업이 '종결'로 전환됩니다. 의 구성 준수v15.0부터 완화된 위험을 결정하기 위해 통과된 테스트 결과의 위험 점수가 채워집니다.

번호	위험 점수	정정 작업	결과	상태
CTR000123	90	TRG0003066	통과함	종결됨
CTR000124	70	TRG0003066	통과함	종결됨
CTR000125	40	TRG0003066	통과함	종결됨

테스트 결과 기록은 다음 표에 표시됩니다.

번호	위험 점수	최신 결과	결과
CTRH000111	90	CTR000123	실패함
CTRH000112	70	CTR000124	실패함
CTRH000113	40	CTR000125	실패함

정정 작업에 활성 테스트 결과가 없기 때문에 정정 작업의 위험 점수는 0입니다.

정정 작업의 경우 다음을 TRG0003066.

과거 위험 점수는 81입니다: (90* 80/100) + (66.67* 5/100) + (0.2 * 15) = Math.floor (78.3 +3) = 81.

정정 작업 규칙 생성 또는 편집 구성 준수

필터 조건에 따라 테스트 결과를 자동으로 그룹화하는 규칙을 만들 수 있습니다. 이러한 규칙은 테스트 결과를 가져올 때 자동으로 그룹화합니다. 익스플로잇이 있는 모든 테스트 결과 선택과 같이 이 규칙으로 그룹화되는 테스트 결과를 제한하려면 필터를 사용합니다.

시작하기 전에
필요한 역할: sn_vulc.admin

이 태스크 정보
기본 시스템에는 할당 그룹(할당 규칙에서 미리 채워짐) 및 테스트 결과 테스트 필드별로 테스트 결과를 그룹화하는 할당 그룹, 테스트 등 하나의 정정 작업 규칙이 함께 제공됩니다. 이 규칙은 필터 조건과 그룹 키를 사용하여 수정할 수 있습니다. 그룹 키는 테스트 결과 테이블의 열입니다. 테스트 결과를 그룹화하는 데 사용해야 하는 값을 나타내려면 최대 6개의 키를 선택합니다.

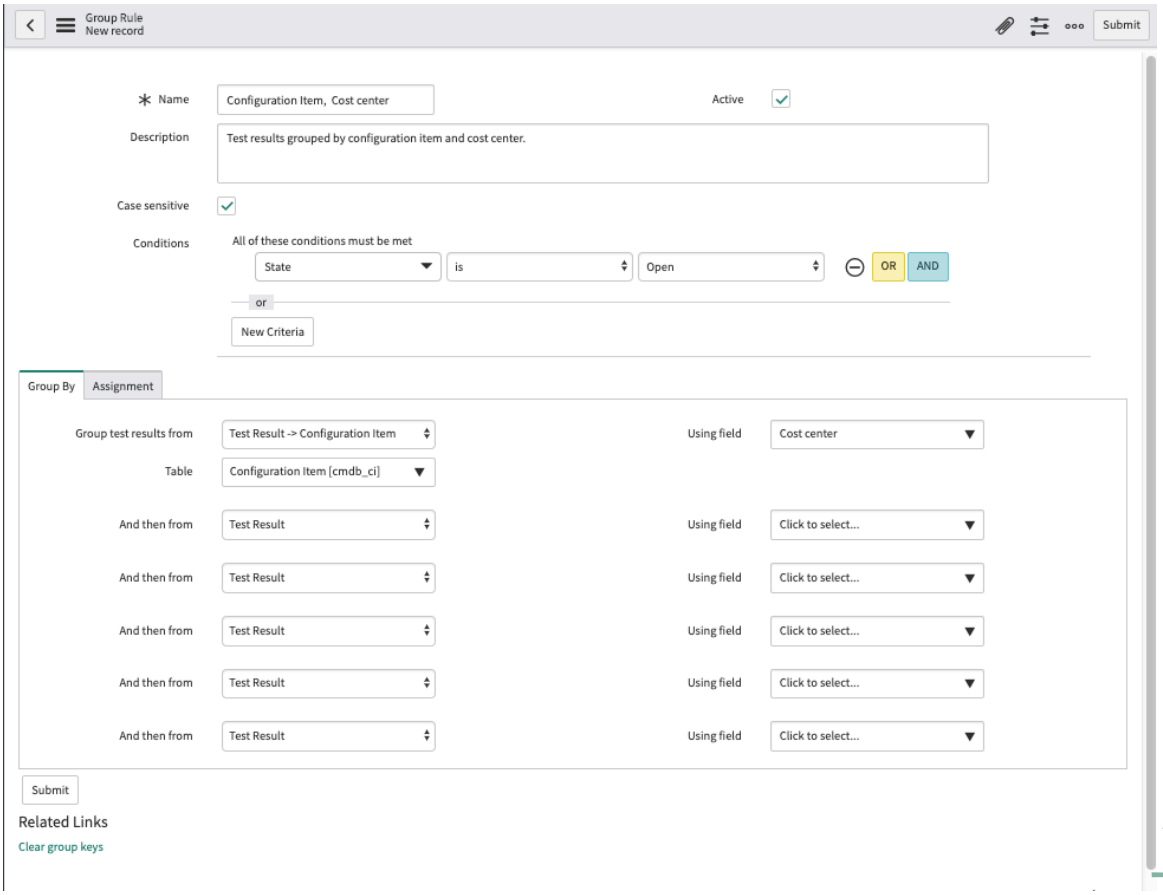
의 버전 14.7 구성 준수부터는 새 구현에 대해 할당 그룹, 테스트 정정 작업 규칙이 비활성화됩니다.

> **주:**
> 새 규칙이나 업데이트된 규칙은 다음 임포트 시 자동으로 평가되거나 정정 작업 규칙 양식의 다시 적용 버튼을 사용하여 수동으로 평가됩니다.

프로시저

1. 다음으로 이동 모두 〉 구성 준수 〉 관리 〉 정정 작업 규칙.
2. 할당 그룹, 테스트 규칙을 열거나 새로 만들기를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



3. 새로 만들기인 경우 양식의 필드에 적절한 정보를 입력합니다.

구성 준수 정정 작업 규칙

필드	설명
이름	정정 작업 규칙의 이름입니다.
활성	정정 작업 규칙이 활성 상태인지 여부를 나타냅니다.
설명	이 정정 작업 규칙에 대한 텍스트 설명입니다.
대소문자 구분	규칙 일치가 대/소문자를 구분하는지 여부를 결정합니다. 주: 기본값은 대/소문자를 구분하지 않습니다.
조건	충족되어야 하는 조건입니다. 기본적으로 (대/소문자 구분 확인란 비활성화됨) 정정 작업 규칙 기록 및 양식의 조건 작성기에 입력하는 검색 텍스트는 대소문자를 구분하지 않습니다. 그룹 기록 및 양식에서 대/소문자 구분 검색을 사용하도록 설정할 수 있습니다.
그룹화 기준	
다음의 테스트	이 규칙에 따라 그룹 생성을 자동화합니다. 사용 가능한 옵션 중 하나를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
결과 그룹화	○ 테스트 결과 | 필드 사용 ○ 테스트 결과->구성 항목 | 테이블 | 필드 사용 확장된 테이블 필드를 선택하면 해당 확장 테이블을 사용하지 않는 테스트 결과가 별도의 정정 작업으로 그룹화됩니다.
할당	
테스트 결과 그룹 할당 기준	이 규칙에 따라 생성된 그룹의 할당을 자동화합니다. 사용 가능한 옵션 중 하나를 선택합니다. ○ 그룹 키 선택하면 키 값 필드가 나타나고 드롭다운 메뉴에 사용 가능한 필드가 나열됩니다. ○ 사용자 그룹 선택하면 사용자 그룹 조회 필드가 나타납니다.

4. 제출을 클릭합니다.

> **주:**
> 키별 그룹화 지우기 관련 링크는 양식의 그룹화 기준 탭에서 그룹 키를 제거합니다.

정정 작업에 대해 요청된 예외의 기간 지정

시스템 속성을 사용하여 정정 작업에 대해 예외를 요청하는 기간을 제한합니다. 정정 작업의 정정이 지정된 기간 동안 지연됩니다.

시작하기 전에
필요한 역할: sn_vulc.admin

이 태스크 정보
sn_vulc.exception_max_request_days 속성은 정정 작업에 대한 예외를 요청할 수 있는 최대 일수를 지정하는 데 사용됩니다. 기본값은 365일입니다.

> **주:**
> 필요하지 않은 경우 sn_vulc.exception_approval_required 속성을 사용하여 정정 작업에 대한 예외 승인 작업 플로우를 비활성화할 수 있습니다. 기본적으로 이 속성은 사용하도록 설정되어 있으며 해당 값은 true입니다.

프로시저

1. 다음으로 이동 모두 〉 시스템 속성 〉 모든 속성.

2. 시스템 속성 페이지에서 sn_vulc.exception_max_request_days를 검색합니다.

3. 속성 이름을 클릭하여 시스템 속성 기록을 엽니다.

4. 이 기록을 편집하려면 이 구성 준수 항목이 현재 애플리케이션으로 선택되어 있어야 합니다.

5. 양수 값을 입력하고 업데이트를 클릭합니다.
기록이 업데이트되고 저장됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

에 대한 예외 관리 구성 구성 준수

모듈을 사용하여 구성 준수 요청된 예외의 기간을 제한하고 예외에 질문서를 추가합니다. 기본적으로, 예외를 설정하면 모듈을 사용하여 요청됩니다 ServiceNow# 취약성 대응 . 통합을 사용하여 예외를 요청할 수도 있습니다 GRC: 정책 및 준수 관리 .

시작하기 전에

필요한 역할: sn_vulc.admin

이 태스크 정보

가 활성화된 경우 취약성 대응 예외를 요청할 수 있는 기간을 제한할 수 있습니다. 마찬가지로 모듈이 설치되어 있으면 GRC: 정책 및 준수 관리 구성 화면에서 선택할 GRC: 정책 및 준수 관리 수 있습니다. 이 옵션을 사용하면 에서 정책 및 제어 목표를 GRC지정하는 예외를 요청할 수 있습니다.

질문서를 추가하면 예외 또는 가양성 요청을 제기하는 사람에게 전송됩니다. 기본 질문서를 사용하거나 요구 사항에 따라 만들 수 있습니다.

예외 승인자가 예외를 요청하는 이유를 이해하는 것이 좋습니다.

프로시저

1. 다음으로 이동 모두 〉 구성 준수 〉 관리 〉 예외 관리.
2. 예외 관리 구성 양식의 다음을 사용하여 예외 관리 목록에서 옵션을 선택하여 예외를 관리할 방법을 선택합니다.
   - 취약성 대응

     주:
     의 취약성 대응22.0부터 옵션에 대한 취약성 대응 긍정 오류 요청에 대한 질문서를 설정할 수도 있습니다.

   - GRC: 정책 및 준수 관리

     주:
     예외를 요청하는 데 사용할 GRC: 정책 및 준수 관리 플러그인을 활성화해야 GRC 합니다.

   주:
   구성을 변경해도 기존 데이터에는 영향을 주지 않습니다.

3. 양식의 필드에 내용을 입력합니다.

참조 예외 관리 양식 설정

필드	설명
지속 시간	예외를 요청할 수 있는 기간입니다.
단위	지정된 기간의 시간 단위입니다.
예외를 요청하려면 질문서 사용	제기 중인 예외 요청에 질문서를 추가하는 옵션입니다.
예외를 요청하기 위한 질문서	예외를 요청하기 위해 선택한 질문서를 표시하는 옵션입니다. 예외 질문서가 기본적으로 표시됩니다.
긍정 오류로 표시하려면 질문서 사용	제기 중인 긍정 오류 요청에 질문서를 추가하는 옵션입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
긍정 오류를 표시하기 위한 질문서	긍정 오류로 표시하기 위해 선택한 질문서를 표시하는 옵션입니다. 긍정 오류 요청에 대한 질문서가 기본적으로 표시됩니다.

4. 저장을 선택합니다.

에 대한 예외 승인자 추가 구성 준수

의 정정 작업에 구성 준수대한 예외를 요청할 수 있도록 승인자 그룹에 사용자를 추가합니다.

시작하기 전에
필요한 역할: sn_vulc.admin

이 태스크 정보
정정 작업에 대한 예외 요청은 기본 2단계 승인 워크플로우를 사용하여 승인됩니다. 사용자를 첫 번째 수준 그룹에 추가해야 합니다. 두 번째 수준에 사용자가 없는 경우, 요청은 첫 번째 수준 승인 후 자동으로 승인됩니다.

주:
첫 번째 수준 승인자가 없으면 예외를 요청할 수 없습니다.

주:
v13.0까지는 구성 준수 첫 번째 수준 승인자가 없으면 예외를 요청할 수 없습니다. 그러나 v13.0부터 구성 준수 CC 애플리케이션을 처음 배포하는 경우 예외 관리용 Flow Designer가 기본적으로 활성화됩니다. 워크플로우를 이미 사용 중인 경우 플로우 디자이너로 업데이트할 수 있습니다. 두 경우 모두 다시 워크플로우로 변경할 수 없습니다.

프로시저

1. 다음으로 이동 모두 〉 시스템 보안 〉 사용자 및 그룹 〉 그룹.
2. 이름 열에서 예외를 검색하고 예외 승인자 - 수준 1 참조를 클릭합니다.

주:
v14.7.5부터 구성 준수 시스템 속성〔sys_properties〕 테이블의 워크플로우를 통해 예외 승인을 위해 기본 시스템에 제공된 시스템 속성을 사용할 수 있습니다. 따라서 워크플로우를 통해 예외 요청이 발생하면 승인을 위해 시스템 속성에 정의된 그룹 ID로 전송됩니다. 다음으로 이동 모두 〉 시스템 속성 및 또는 `sn_vulc.exception_approver_L2_CC` 을 선택하여 `sn_vulc.exception_approver_L1_CC` 속성 값을 변경합니다.

3. 그룹 예외 승인자 - 수준 1 참조 양식에서 다음으로 이동합니다. 그룹 구성원 〉 신규 (또는 편집)을 클릭합니다.
4. 양식에서 필드를 채웁니다.

사용자 양식

필드	설명
사용자 ID	사용자의 고유 식별자입니다.
이름	사용자의 이름입니다.
성	사용자의 성입니다.
직위	사용자의 직함입니다. 직함 또는 직무 설명을 입력하거나 목록에서 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
부서	사용자의 부서입니다.
암호	사용자에게 할당된 암호입니다. 이 암호는 영구적이거나 임시적일 수 있습니다.
암호 다시 설정 필요	사용자가 보안을 보장하기 위해 암호를 재설정할 수 있도록 하는 옵션입니다.
잠겨 있음	사용자를 인스턴스에서 잠그고 사용자의 모든 활성 세션을 종료하는 옵션입니다. 시스템은 관리자 역할을 가진 사용자가 자신을 잠그는 것을 방지합니다.
활성	이 사용자를 활성화하는 옵션입니다. 다음 영역에서는 비활성 사용자만 볼 수 있습니다. ○ 사용자 목록 ○ 참조 필드의 선택 목록(돋보기 아이콘) ○ 참조 필드에 입력할 때 나타나는 자동 완성 목록
웹 서비스 접근만 허용	이 사용자를 비대화형 사용자로 지정하는 옵션입니다.
내부 통합 사용자	이 사용자를 내부 통합 사용자로 지정하는 옵션입니다.
이메일	사용자의 이메일 주소입니다.
언어	사용자의 기본 설정 언어입니다.
달력 통합	작업 일정을 관리하는 데 사용되는 달력입니다. 예를 들어 Outlook입니다.
시간대	이 사용자의 위치에 대한 시간대입니다.
날짜 형식	사용자가 선호하는 날짜 형식입니다.
직장 전화번호	사용자의 직장 전화 번호입니다.
휴대폰	사용자의 휴대폰입니다.
사진	추가하려면 클릭...을 클릭하여 업로드할 수 있는 사진입니다.

5. 제출을 클릭합니다.
6. 옵션: 1-5단계를 반복하여 예외 승인자 - 수준 2 참조를 생성합니다.

   주:
   두 번째 수준 승인자를 생성하는 동안 예외 승인자 - 수준 **2** 참조를 선택합니다.

7. 옵션: 편집을 선택하는 경우 사용자를 컬렉션에서 그룹 구성원 패널로 이동하고 저장을 클릭합니다.
   승인자는 다음으로 이동해야 합니다. 모두 〉 구성 준수 〉 내 승인 요청을 승인합니다.

구성 준수 중요도 맵 생성

구성 준수 중요도 매핑은 외부 공급업체 소스 중요도 필드에 대한 변환 맵을 심각도의 구성 준수 인식 가능한 필드로 제공합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_vulc.admin

프로시저

1. 다음으로 이동 모두 〉 구성 준수 〉 관리 〉 중요도 매핑.
2. 새로 만들기를 클릭합니다.
3. 양식의 필드에 적절히 입력합니다.

필드 매핑

필드	설명
소스	중요도 매핑에 대한 소스의 이름입니다.
소스 값	소스 중요도 값입니다.
대상 값	대상 값입니다. 선택 항목은 다음과 같습니다. 중요 컨트롤과 관련된 구성 문제로 인해 하나 이상의 비즈니스 크리티컬 CI가 중단됩니다. 높음 컨트롤과 관련된 구성 문제는 위협이지만 중요한 네트워크 리소스의 종료를 일으키지는 않습니다. 보통 통제와 관련된 구성 문제는 위험하지만 즉각적인 위협은 아닙니다. 낮음 제어와 연결된 구성 문제는 낮은 수준의 위협이며 더 큰 위험에 처한 CI를 위해 무시할 수 있습니다. 경미 컨트롤과 관련된 구성 문제는 사소한 위험이며 필요한 경우 무시할 수 있습니다.

4. 제출을 클릭합니다.

이메일 알림 만들기

취약성 관리자는 알림을 보내거나 새로 추가하여 알림 전송 시기, 알림 수신자, 알림의 내용을 지정할 수 있습니다.

시작하기 전에
필요한 역할: sn_vulc.admin

이 태스크 정보
다양한 유형의 이메일 알림에 대한 이메일 템플릿을 생성할 수 있습니다. 이메일 템플릿을 만드는 방법에 대한 자세한 내용은 문서를 참조하십시오 이메일 템플릿 정의 취약성 대응.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 알림.
2. 정정 대상 알림 기록을 선택하거나 새로 만들기를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 양식의 필드에 적절히 입력합니다.
   양식 필드에 대한 자세한 내용은 Create an email notification 문서를 참조하십시오.
4. 메시지를 보려면 알림 미리 보기를 선택합니다.

결과
의 구성 준수v14.11부터 수신자가 이메일 알림의 링크를 클릭하면 역할에 따라 기록이 OR IT 정정 작업 공간 에서 취약성 관리자 작업 공간 열립니다.

- 에서 sn_vulc.admin 역할을 가진 사용자에게 링크가 열립니다 취약성 관리자 작업 공간 .
- sn_vulc.remediation IT 정정 작업 공간 _owner 역할을 가진 사용자에 대해 링크에서 열립니다.

수신자에게 위의 역할이 없는 경우 이메일 알림의 링크가 클래식 UI에서 열립니다.

에서 예외 관리에 대한 승인 규칙 구성 구성 준수

Flow Designer를 사용하여 예외 관리 및 예외 규칙에 대한 예외 요청을 승인합니다. 처음 배포하는 구성 준수 경우에는 Flow Designer가 기본적으로 활성화되어 있습니다.

시작하기 전에
필요한 역할: sn_vulc.admin

이 태스크 정보
시스템 속성의 *sn_vulc.flow_designer_activation* 값이 true로 설정됩니다. 즉, Flow Designer가 기본적으로 활성화됩니다.

> **주:**
> Flow Designer를 활성화한 후에는 워크플로우 사용으로 되돌릴 수 없습니다. 워크플로우와 Flow Designer를 자세히 비교하려면 다음 항목을 참조하십시오 의 예외 관리 워크플로우와 Flow Designer 비교 구성 준수.

플로우 디자이너를 사용하려면 승인 규칙 모듈을 사용하여 규칙을 생성합니다. 이 모듈을 사용하여 다음의 각 예외 관리 워크플로우에 대한 승인 규칙을 구성할 수 있습니다.

- 정정 작업에 대한 예외 승인 규칙
- 자동 예외 규칙에 대한 승인 규칙

> **주:**
> 규칙 내에 여러 수준의 승인을 포함하는 조건을 정의할 수도 있습니다. Flow Designer는 이 모듈에서 생성된 규칙을 자동으로 상속하고 일치하는 승인 워크플로우를 처리합니다. 승인 수준 구성에 대한 자세한 내용은 다음 문서를 참조하십시오 에서 예외 관리에 대한 승인 수준 생성 구성 준수.

프로시저

1. 다음으로 이동 모두 〉 구성 준수 〉 관리 〉 승인 규칙 〉 정정 작업에 대한 예외 승인 규칙.
2. 승인 규칙 페이지에서 승인 규칙을 설정할 그룹을 선택합니다.
3. 양식에서 필드를 채웁니다.

승인 규칙 양식

필드	설명
이름	승인 구성 이름입니다.
테이블	규칙이 적용되는 테이블입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
애플리케이션	기본값은 입니다 구성 준수.
규칙 유형	규칙 유형을 지정합니다. 예를 들어 예외 관리 또는 예외 규칙이 있습니다.
활성	기본적으로 활성화되며, 승인 규칙이 사용 중임을 나타냅니다.
설명	승인 규칙에 대한 간단한 설명입니다.
승인 만료Y (일)	승인자가 요청을 승인할 수 있을 때까지의 날짜입니다.
승인자에게 알림(일)	승인자에게 조치를 취하라는 알림이 전송된 날짜입니다.

4. 업데이트를 선택합니다.
승인 구성 탭에는 기본적으로 두 가지 수준의 승인자가 설정됩니다. 규칙을 선택하여 규칙 내의 다양한 사용 사례를 기반으로 조건을 정의할 수 있습니다. 자세한 내용은 에서 승인 규칙에 대한 구성 생성 구성 준수 문서를 참조하십시오.

주:
각 구성 페이지에서 여러 승인 수준을 생성할 수 있습니다. 자세한 내용은 에서 예외 관리에 대한 승인 수준 생성 구성 준수 문서를 참조하십시오.

Example:
다양한 사용 사례를 기반으로 서로 다른 정정 작업에서 발견된 동일한 테스트 결과에 대해 서로 다른 승인 프로세스를 정의할 수 있습니다.

에서 승인 규칙에 대한 구성 생성 구성 준수

승인 수준에 대해 일치하는 정정 작업을 필터링하는 조건을 정의합니다.

시작하기 전에
필요한 역할: sn_vulc.admin

이 태스크 정보
승인 구성 모듈에서 서로 다른 구성에 대해 여러 수준의 승인을 구성할 수 있습니다. 각 규칙에 여러 수준의 승인이 포함된 조건 기반 규칙을 정의합니다.

주:
승인 규칙 모듈을 사용하여 예외 관리 워크플로우에 대한 승인 규칙을 구성합니다. 승인 규칙 구성에 대한 자세한 내용은 문서를 참조하십시오 에서 예외 관리에 대한 승인 수준 생성 구성 준수.

프로시저

1. 다음으로 이동 모두 〉 구성 준수 〉 관리 〉 승인 규칙.
2. 승인 규칙을 선택하고 승인 구성 탭으로 이동합니다.
3. 구성을 선택합니다.
4. 양식에서 필드를 채웁니다.

승인 구성 양식

필드	설명
이름	승인 구성 이름입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
승인 규칙	승인 규칙에 대한 테이블 및 유형 상세 정보를 포함합니다.
순서	규칙 내에서 다양한 구성의 실행 순서입니다. 예를 들어 주문 항목이 100인 구성은 주문 항목이 200인 구성보다 먼저 실행됩니다.
활성	기본적으로 활성화되며, 승인 구성이 사용 중임을 나타냅니다.
설명	승인 구성 수준에 대한 짧은 설명입니다.

5. 다음 방법 중 하나로 테스트 결과 또는 정정 작업에 대한 조건을 설정합니다.

필드	설명
조건	일치하는 테스트 결과 또는 정정 작업을 식별합니다.
고급 조건	테스트 결과 또는 정정 작업에 대한 조건을 정의하는 스크립트입니다. **주:** 이 필드는 고급 확인란을 선택할 때 나타납니다.

6. 업데이트를 선택합니다.
규칙 내에서 여러 수준의 승인을 포함하는 조건을 정의할 수 있습니다. Flow Designer는 이 모듈에서 생성된 규칙을 자동으로 상속하고 일치하는 승인 워크플로우를 처리합니다. 승인 수준 구성에 대한 자세한 내용은 다음 문서를 참조하십시오 에서 예외 관리에 대한 승인 수준 생성 구성 준수.

Example:
다양한 유형의 정정 작업에 대해 서로 다른 승인 경로를 정의할 수 있습니다.

에서 예외 관리에 대한 승인 수준 생성 구성 준수

예외 요청을 승인할 사용자 및 사용자 그룹의 수준을 정의합니다.

시작하기 전에
필요한 역할: sn_vulc.admin

프로시저

1. 다음으로 이동 모두 〉 구성 준수 〉 관리 〉 승인 규칙.

2. 승인 규칙을 선택하고 승인 구성 탭으로 이동합니다.

3. 구성을 선택합니다.

4. 승인자 수준 섹션에서 승인자 수준을 선택합니다.

5. 양식에서 필드를 채웁니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

승인자 수준 양식

필드	설명
이름	승인 수준 이름입니다.
필요한 승인	선택한 수준에 필요한 승인 수를 선택합니다. ○ 승인자 1명 필요 ○ 모든 사용자의 승인 필요
활성	기본적으로 활성화되며, 승인 수준이 사용 중임을 나타냅니다.
순서	규칙 내에서 다양한 구성의 실행 순서입니다. 예를 들어 주문 항목이 100인 구성은 주문 항목이 200인 구성보다 먼저 실행됩니다.
승인 규칙	승인 규칙에 대한 테이블 및 유형 상세 정보를 포함합니다. 이 필드는 읽기 전용입니다.
승인 구성	승인 구성을 포함합니다. 이 필드는 읽기 전용입니다.
할당 사용	다음 옵션 중에서 선택합니다. ○ 사용자 및 사용자 그룹 ○ 승인 테이블 필드 ○ 스크립트
그룹	여러 사용자로 구성된 승인자 수준 그룹입니다. 사용자는 예외 관리 및 예외 규칙에 대해 다음 역할 중 하나가 있어야 합니다. ○ sn_vulc.exception_approver ○ sn_vulc.읽기 ○ sn_vulc.read_auto_exception_rule
사용자	그룹에 나열된 사용자를 편집합니다.

6. 변경 내용을 저장하려면 업데이트를 선택합니다.

주:
v13.0 이전에는 예외 수준 1의 사용자만 있는 경우 워크플로우 프로세스가 작동합니다. 단, v13.0부터는 각 레벨에 최소 한 명의 사용자가 있어야 합니다.

v13.0 이전에는 워크플로우에서 두 번째 수준에 사용자가 없으면 정정 작업이 지연되었습니다. 그러나 v13.0 이상에서는 두 번째 수준에 사용자가 없으면 승인 요청이 자동으로 거부됩니다.

Example:
Linux 및 Windows 서버의 정정 작업에 대한 승인 수준은 다를 수 있습니다.

의 예외 관리 워크플로우와 **Flow Designer** 비교 구성 준수

구성 준수 (CC) v13.0부터 CC를 처음 배포하는 경우 예외 관리에서 예외 요청을 승인하기 위한 Flow Designer가 기본적으로 활성화됩니다. 기존 참조 사용자인 경우 기본 옵션은 워크플로우입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

워크플로우와 **Flow Designer** 비교

고려 사항	워크플로우	**Flow Designer**
버전	CC v13.0 이전	CC의 v13.0부터
기본 옵션	기존 참조 사용자인 경우 기본 옵션입니다.	v13.0부터 새 CC 사용자에 대한 기본 옵션입니다.
승인 프로세스 설정	예외 관리에는 예외 규칙과 함께 예외 요청이 포함됩니다.	다양한 수준을 정의하고 다양한 사용 사례에 대해 서로 다른 승인자를 추가하는 작업이 포함됩니다. 워크플로우보다 구현하기 쉽습니다. 예외 관리에는 예외 규칙과 함께 예외 요청이 포함됩니다.
Flow Designer로 업그레이드	워크플로우에서 Flow Designer로 업그레이드할 수 있습니다. 그러나 기존 요청은 워크플로우를 사용해야만 승인할 수 있습니다.	플로우 디자이너는 기본적으로 활성화되어 있습니다.
시스템 속성 *sn_vulc.flow_designer_activated*	v13.0 이전의 예외 관리에 워크플로우를 사용한 경우 시스템 속성이 false로 설정됩니다. 플로우 디자이너를 활성화하려면 이 속성을 true로 설정합니다. **주:** Flow Designer를 활성화한 후에는 워크플로우 사용으로 되돌릴 수 없습니다.	v13.0 이상에 대해 CC를 처음 사용하는 경우 시스템 속성 값은 기본적으로 true로 설정됩니다.
승인 규칙 모듈	시스템 속성을 true로 설정하면 모듈 승인 규칙 사용 예약된 작업이 24시간 이내에 실행됩니다. 이 예약된 작업은 승인 규칙 모듈을 활성화합니다. 이 모듈을 즉시 활성화하려면 이 작업을 수동으로 실행하십시오.	CC v13.0에서 CC를 처음 배포한 경우 기본적으로 이 모듈을 사용할 수 있습니다.
승인 수준	승인자 수준을 두 개만 설정하는 옵션을 제공합니다.	원하는 수의 구성 및 승인자 수준 설정 및 각 규칙에 대한 승인자를 동적으로 추가하는 등 다양한 옵션을 제공합니다.

구성 준수 통합

외부 공급업체 통합은 구성 평가 결과, 정책, 테스트, 기술, 권한이 부여된 소스, 테스트 결과를 기타 취약성 데이터와 함께 애플리케이션으로 임포트합니다 구성 준수 .

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
의 구성 준수v14.9부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v14.9 이전 용어	용어 **v14.9** 이상
테스트 결과 그룹	정정 작업
그룹 규칙	정정 작업 규칙
정책	테스트 그룹

이 구성 준수 애플리케이션은 다음과 같은 외부 공급업체 통합을 지원합니다.

- v14.11부터는 결과를 애플리케이션에 테스트 결과로 구성 준수 게시하여 보안 태세 통제 애플리케이션에서 식별한 엔터프라이즈 자산의 보안 격차를 해결합니다. 보안 태세 통제 애플리케이션과 지원되는 애플리케이션은 에서 별도의 구독으로 사용할 수 있습니다 ServiceNow# Store. 자세한 내용은 보안 태세 통제 문서를 참조하십시오.
- 보안 운영에 대한 Microsoft Defender for Cloud Integration
- Palo Alto Prisma 클라우드 취약성 통합
- Qualys 및 구성 준수 통합
- Tenable.ioTenable 취약성 통합의 산물

통합에 대한 추가 참고 사항

통합 실행 중에 여러 프로세스가 생성되고 데이터가 페이지 형식으로 수신됩니다. 각 프로세스에는 페이지에 첨부된 데이터가 있는 하나 이상의 임포트 큐 항목이 포함될 수 있습니다. 이러한 항목은 1시간의 시간 제한 내에 데이터를 처리해야 합니다. 그러나 페이로드 크기가 크면 처리 시간이 1시간을 초과하거나 중단되어 통합 시간 제한 오류가 발생할 수 있습니다. 통합은 시간 초과 오류에도 불구하고 데이터를 계속 처리합니다. 이러한 잘못된 통신을 피하기 위해 버전 14.8.5 구성 준수부터 큐가 활성 상태이고 데이터를 처리하는지 여부를 나타내기 위해 타임스탬프(하트비트)가 주기적으로 전송됩니다. 임포트 큐 항목 페이지의 처리된 마지막 기록 필드는 임포트 큐가 생성하거나 업데이트하는 기록 수에 따라 업데이트됩니다. 임포트 큐 항목이 1시간의 시간 제한을 초과하는 경우, 시스템은 마지막으로 처리된 기록 필드를 검사하여 1시간보다 오래되었는지도 확인합니다. 이 경우 이는 임포트 큐 항목이 고착되었음을 나타내며 처리 시 더 이상의 지연을 방지하기 위해 시간 초과됩니다.

주:
마지막으로 처리된 기록 필드는 다음 시스템 속성에 정의된 내용에 따라 업데이트됩니다.

- *sn_sec_cmn.record_threshold_heartbeat*: 하트비트(타임스탬프)가 임포트 큐 항목으로 전송된 후 처리된 기록 수를 정의합니다.
- *sn_sec_cmn.maximum_heartbeat_delay*: 임포트 큐 항목을 시간 초과해야 하는 시간을 정의합니다.

보안 운영에 대한 **Microsoft Defender for Cloud Integration**

이 Microsoft Defender for Cloud Integration 제품은 클라우드 환경의 보안 태세를 강화하는 인프라 보안 관리 시스템입니다.

Microsoft Defender for Cloud Integration 용 보안 운영 애플리케이션과 구성 준수 통합하여 테스트를 CI(구성 항목)에 매핑하여 테스트 결과를 생성합니다. 워크로드 전반에 배포된 새로운 클라우드 자원을 지속적으로 검색하고 CIS(Center for Internet Security)와 같은 보안 표준에 따라 구성되었는지 확인합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

버전 2.2부터 Microsoft Azure Security Center의 이름이 for 보안 운영로 바 Microsoft Defender for Cloud Integration 뀝니다.

사용 가능한 버전

애플리케이션	버전
Microsoft Defender for Cloud Integration 때문에 보안 운영	2.3
구성 준수	14.3
Security Support Common	13.2
취약성 대응	16.2

플랫폼의 다중 배포 **Microsoft Defender for Cloud**

플랫폼 애플리케이션을 여러 개 배포하는 Microsoft Defender for Cloud 경우 각 배포에 대한 통합을 추가할 수 있습니다. 여러 외부 공급업체 배포로 식별되는 자원은 .구성 관리 데이터베이스(CMDB) 이러한 통합은 여러 배포 간에 스캔 프로세스가 겹치는 경우에도 수행됩니다.

ServiceNow Microsoft Defender for Cloud 통합

for 보안 운영 는 Microsoft Defender for Cloud Integration 에서 Microsoft Defender for Cloud데이터를 검색하여 인스턴스의 규정 준수 데이터를 보강합니다. 일련의 예약된 작업이 통합을 자동으로 호출합니다. 이러한 예약된 작업을 수동으로 실행할 수도 있습니다. 예약된 작업은 인스턴스를 와 동기화 Microsoft Defender for Cloud된 상태로 유지하여 테스트 결과 정정 수명주기를 단순화합니다.

각 통합 기록에 대해 기본값이 VR로 구성된 실행 사용자가 있습니다 .시스템. 이 값은 동일해야 합니다.

주:
유효한 실행 사용자를 설정하지 않으면 데이터 소스 기록에 대해 중복 또는 여러 개의 데이터 검색 첨부 파일이 생성됩니다. 통합이 실행될 때마다 첨부 파일 수가 증가합니다. 이렇게 하면 처리 시간이 늘어나 일관되지 않은 변환 결과가 발생합니다.

Microsoft Defender for Cloud 플랫폼 통합 작업에는 다음과 같은 역할이 포함됩니다.

- sn_vul_asc.configure_integration: 기록을 읽고, 쓰고, 삭제하는 기능입니다.
- sn_vul_asc.read_integration: 기록을 읽을 수 있는 기능입니다.

통합 보기 **Microsoft Defender for Cloud**

다음으로 이동하여 통합을 봅니다. 모두 〉 클라우드 통합을 위한 **Microsoft Defender** 〉 통합.

기본 시스템에는 다음과 같은 통합이 포함됩니다.

통합	설명
정책 정의 통합	정책을 검색하고 인스턴스에 정책 항목을 생성합니다.
평가 메타데이터 통합	평가 메타데이터를 검색하고 인스턴스에서 테스트를 생성합니다.
규정 준수 표준 및 통제 통합	표준 및 통제를 검색하고 인증 소스와 인용을 생성합니다. 그런 다음 생성된 테스트에 연결합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

통합	설명
평가 통합	평가를 검색하고 인스턴스에서 처리합니다. 이 통합의 출력은 테스트 결과입니다.

식별 및 조정 엔진을 사용하여 CI 생성

기존 CI를 외부 공급업체 스캐너에서 임포트한 호스트와 일치시킬 수 없는 경우 IRE(식별 및 조정 엔진)를 사용하여 CI를 생성합니다.

CI가 CMDB에서 일치하지 않으면 클래스에 CI가 *cmdb_ci_cmp_resource* 생성됩니다. 나중에 검색에서 동일한 CI를 찾으면 CI를 보강하거나 다른 CI를 생성합니다.

주:
클라우드 자원에 대해서는 자동 조정이 발생하지 않습니다.

에 대한 설치 및 구성 Microsoft Defender for Cloud Integration보안 운영

에서 임포트 Microsoft Defender for Cloud 한 데이터를 사용하여 자산의 잘못된 구성의 우선순위를 지정하고 정정할 수 있도록 for 보안 운영를 Microsoft Defender for Cloud Integration 설치하고 구성합니다.

시작하기 전에

Azure Active Directory에 대한 Microsoft Defender for Cloud Integration새 앱 등록을 만듭니다. Azure Active Directory에 새 응용 프로그램을 등록하는 방법에 대한 자세한 내용은 Microsoft 제품 설명서 사이트를 참조하세요. Azure 역할에 대한 자세한 내용은 Azure 역할을 참조하세요.

필요한 역할: sn_vulc.admin

프로시저

1. 다음으로 이동 모두 〉 시스템 정의 〉 플러그인.
2. 검색 창에서 ## ### ## ##### Microsoft Defender ### 검색합니다.
3. 설치를 선택합니다.

   설치될 모든 종속성이 표시됩니다.
4. 다음으로 이동 모두 〉 클라우드 통합을 위한 **Microsoft Defender** 〉 관리 〉 구성 〉 클라우드 구성을 위한 **Microsoft Defender**.
5. 양식에서 필드를 채웁니다.

Microsoft Defender for Cloud 구성 양식

필드	설명
API URL	인스턴스의 자원 URL입니다. 예: https://management.azure.com (Azure 퍼블릭 클라우드)
테넌트 ID	조직의 테넌트 ID입니다.
통합 인스턴스	기본 인스턴스입니다. 여러 Microsoft Defender 테넌트 또는 구독에서 데이터를 가져오기 위한 인스턴스를 만들 수도 있습니다.
클라이언트 ID	애플리케이션을 등록한 후 Microsoft Defender for Cloud Integration 생성되는 클라이언트 ID입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
클라이언트 비밀	애플리케이션을 등록한 후 생성되는 클라이언트 비밀입니다 Microsoft Defender for Cloud Integration .
다음에서 결과 임포트	검색할 선택한 관리 그룹 ID 및 구독 ID에 해당하는 자원 및 평가입니다.
관리 그룹 ID	검색할 관리 그룹 ID에 해당하는 자원 및 평가입니다. 주: 이 필드는 다음에서 결과 임포트 필드에서 특정 관리 그룹을 선택하는 경우에만 나타납니다.
구독 ID	자원 및 평가를 검색할 구독의 식별 번호입니다. 주: 이 필드는 다음에서 결과 임포트 필드에서 특정 구독을 선택하는 경우에만 나타납니다.
확인 상태	제공된 자격 증명과 구독 ID가 유효한지 여부입니다.

6. 저장 및 테스트를 선택하여 통합을 구성하거나 실행합니다.

구성 준수 다음에 대해 임포트된 데이터 **Microsoft Defender for Cloud Integration**

구성 준수 는 외부 공급업체 통합에서 정책, 테스트, 권한 있는 소스 및 테스트 결과를 임포트하고 볼 수 있도록 모듈에 저장합니다.

주:
의 구성 준수v14.9부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v14.9 이전 용어	용어 **v14.9** 이상
테스트 결과 그룹	정정 작업
그룹 규칙	정정 작업 규칙
정책	테스트 그룹

테스트 그룹

구성 테스트 그룹이 테스트 그룹을 구성합니다. 테스트 그룹은 권한이 부여된 문서 및 테스트 레코드와 관련이 있으며 조직의 요구 사항에 맞게 수정할 수 있습니다. 하나의 구성 테스트가 여러 테스트 그룹에 속할 수 있습니다.

가 Microsoft Defender for Cloud Integration 설치되면 테스트 그룹이 검색되고 예약된 작업인 정책 정의 통합에 의해 채워집니다. 다음으로 이동하여 예약된 작업을 볼 수 있습니다. 모두 〉 클라우드 통합을 위한 **Microsoft Defender** 〉 관리 〉 통합 〉 정책 정의 통합.

주:
통합을 수동으로 실행하도록 선택하는 경우 먼저 정책 정의 통합을 실행합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테스트

테스트는 컴퓨팅 자산의 스캔을 구성하는 데이터 기록 라이브러리입니다. 구성 테스트는 자산을 관리하는 방법을 정의합니다.

테스트는 구성 준수 외부 공급업체 통합 애플리케이션에서 테스트 결과 유형별로 자산을 그룹화하는 데 사용하는 메커니즘입니다.

가 Microsoft Defender for Cloud Integration 설치된 경우 예약된 작업인 평가 메타데이터 통합이 테스트를 검색합니다. 다음으로 이동하여 예약된 작업을 볼 수 있습니다. 통합 〉 기본 통합 〉 평가 메타데이터 통합.

주:
통합을 수동으로 실행하려는 경우 정책 정의 통합 후 평가 메타데이터 통합을 실행합니다.

의 구성 준수v15.0부터 테스트가 속한 테스트 그룹이 테스트 목록의 테스트 그룹 열에 채워집니다.

권한이 부여된 소스

구성 준수 테스트는 테스트에 대한 취약성 경보를 생성할 때 신뢰할 수 있는 출처와 인용을 사용합니다. 권한이 부여된 소스는 일반적으로 **ISO 27001** 및 **PCI DSS 3.2.1**과 같은 게시된 산업 표준의 섹션에 매핑됩니다.

이러한 원본 기록에는 컴퓨터 보안 분야의 전문가가 제공한 알려진 소프트웨어 및 하드웨어 구성 문제에 대한 정보에 대한 참조가 포함되어 있습니다. 보안 정책 및 절차에 대한 요구 사항을 정의합니다.

가 Microsoft Defender for Cloud Integration 설치된 경우 예약된 작업인 준수 표준 및 통제가 권한이 부여된 소스와 인용을 검색합니다. 다음으로 이동하여 이 예약된 작업을 볼 수 있습니다. 모두 〉 클라우드 통합을 위한 **Microsoft Defender** 〉 통합 〉 규정 준수 표준 및 통제 통합.

주:
통합을 수동으로 실행하려는 경우 평가 메타데이터 통합 후 준수 표준 및 통제 통합을 실행합니다.

자산

평가 통합은 자원 태그 및 클라우드 속성과 같은 중요한 정보를 제공합니다. 이 정보는 검색된 항목 양식에 표시됩니다. #할당및 정정 작업 규칙에서 구성 준수 필터링하는 데 주로 사용됩니다.

- 자원 태그: 모든 클라우드 자원 태그는 평가 통합의 일부로 호스트 태그로 임포트됩니다. 자원이 호스트인지 여부에 관계없이 모든 클라우드 자원 유형에 대한 클라우드 태그가 여기에 저장됩니다.
  - 태그 스토리지는 대/소문자를 구분하지 않습니다. Tokyo 태그가 생성되면 호스트 태그 테이블에 **TOKYO** 태그를 저장할 수 없습니다. **Tokyo** 와 **TOKYO** 는 동일한 호스트 태그로 간주됩니다. 먼저 가져온 태그가 우선합니다.
  - 그룹 규칙에서 호스트 태그를 그룹 키로 사용하면 예기치 않은 결과가 발생할 수 있습니다. 호스트 태그는 조건 작성기에서만 사용할 수 있습니다.
- 자산에 대한 클라우드 속성: 다음은 통합이 검색하는 클라우드 속성입니다.Microsoft Defender for Cloud
  - 클라우드 계정
  - 클라우드 영역
  - 클라우드 자원 유형
  - 클라우드 서비스 제공자

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테스트 결과

구성 준수 는 테스트 결과를 계산하지 않지만 외부 공급업체 통합의 일부로 가져옵니다. 에서 볼 수 구성 준수있게 되면 정정 작업을 사용하여 정정됩니다.

통합이 Microsoft Defender for Cloud 설치되면 예약된 작업인 평가 통합이 테스트 결과를 검색합니다. 다음으로 이동하여 이 예약된 작업을 볼 수 있습니다. 모두 〉 클라우드 통합을 위한 **Microsoft Defender** 〉 통합 〉 평가 통합.

평가 통합 임포트는 통합 상세 정보 탭의 `Start Time` 매개변수를 사용하는 유일한 통합입니다. 다른 구성 준수 모든 임포트는 에 `Start Time`관계없이 사용 가능한 모든 데이터를 가져옵니다.

평가 통합 임포트가 완료되면 임포트 종료 계산을 트리거하는 이벤트가 시작됩니다.

평가 통합은 기본적으로 지난 1일 동안 마지막으로 성공한 통합 실행에서 상태가 변경된 경우에만 데이터 평가를 가져옵니다. 따라서 지난 며칠 동안 평가가 계속 실패하면 평가에 대한 상태 변경이 없으므로 통합에서 평가를 가져오지 않습니다. Defender 평가를 통해 테스트 결과를 최신 상태로 유지하기 위해 지난 7일 동안의 데이터를 가져오는 새로운 종합 평가 통합 이 추가되었습니다. 매주 실행되며 통과되지 않은 모든 테스트 결과를 가져옵니다.

통합에서 **Microsoft Defender for Cloud** CI를 식별하기 위한 **CI** 조회 규칙

외부 공급업체 통합 구성 준수 에서 데이터를 임포트하면 은 CI 조회 규칙을 통해 에서 일치 항목을 구성 관리 데이터베이스(CMDB)검색하기 위해 자동으로 자원 데이터를 사용합니다. 이러한 규칙은 CI(구성 항목)를 식별하고 정정에 도움이 되도록 테스트 결과 기록에 추가하는 데 사용됩니다. 자원 ID, 이름 및 S3 버킷에 기본 시스템 CI 조회 규칙을 사용할 수 있습니다. CI 조회 규칙에 대한 자세한 내용은 보안 작업을 위한 클라우드 통합용 Microsoft Defender 대한 CI 잠금 규칙을 참조하세요.

Vulnerability Response Integration with Palo Alto Prisma Cloud 이해

Prisma Cloud는 API 기반 클라우드 인프라 보안 솔루션입니다. 클라우드 환경에 연결하고 공용 클라우드 환경에 배포된 자원(Amazon Web Services 예: (AWS) Microsoft Azure)을 모니터링합니다. 퍼블릭 클라우드 인프라 내의 위험에 대한 완벽한 가시성과 통제를 얻을 수 있습니다.

이 Vulnerability Response Integration with Palo Alto Prisma Cloud 애플리케이션을 사용하면 Prisma Cloud에서 정책과 경보를 애플리케이션에서 각각 테스트 및 테스트 결과로 쉽게 수집할 수 있습니다 구성 준수 . 올바른 구성을 사용하면 적절한 위험 점수를 할당하고 그룹화하여 관련 사용자 및 그룹에 할당하여 테스트 결과를 원활하게 관리할 수 있습니다.

사용 가능한 버전

이 테이블에는 애플리케이션의 버전과 함께 종속된 Vulnerability Response Integration with Palo Alto Prisma Cloud 애플리케이션이 나열됩니다.

애플리케이션	버전
보안 운영용 Prisma 클라우드 통합	2.3
구성 준수	14.7
Security Support Common	13.5
취약성 대응	18.0

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

ServiceNow Prisma 클라우드 통합

이 Vulnerability Response Integration with Palo Alto Prisma Cloud 애플리케이션을 사용하면 Prisma 데이터를 인스턴스로 ServiceNow 임포트하여 인스턴스를 보강하여 더 나은 관리를 할 수 있습니다. 일련의 예약된 작업이 통합을 자동으로 호출합니다. 이러한 예약된 작업을 수동으로 실행할 수도 있습니다. 예약된 작업은 Prisma Cloud에서 주기적으로 데이터를 검색하여 인스턴스를 업데이트된 상태로 유지하여 테스트 결과 정정 수명주기를 단순화합니다.

Prisma 클라우드 통합 작업에는 다음 역할이 포함됩니다.

- sn_vul_prismacloud.configure_integration: 기록을 읽고, 쓰고, 삭제하는 기능입니다.
- sn_vul_prismacloud.read_integration: 기록 읽기 기능입니다.

통합 보기

로 이동하여 통합의 일부인 Vulnerability Response Integration with Palo Alto Prisma Cloud 통합을 볼 수 있습니다. **Prisma** 클라우드 통합 〉 통합.

기본 시스템에서 다음 통합을 사용할 수 있습니다.

실행 시퀀스	일정	통합	설명
1	주별	Prisma 정책 통합	• Prisma Cloud에서 정책을 검색하고 인스턴스에 테스트 항목을 생성합니다. • 증분 지원은 제공하지 않습니다. 지난 10일 동안 통합을 실행하면 이전 통합 실행에 대한 결과도 표시됩니다.
2	매일	Prisma 경보 통합	• Prisma Cloud에서 경보를 검색하고 인스턴스에 테스트 결과 항목을 생성합니다. • 증분 지원을 제공합니다. 통합은 마지막 통합 실행 시간 이후에 매일 실행됩니다.

설치 준비 중 **Vulnerability Response Integration with Palo Alto Prisma Cloud**

설정 작업을 수행하여 설치를 준비합니다 Vulnerability Response Integration with Palo Alto Prisma Cloud .

시작하기 전에

Vulnerability Response를 Palo Alto Prisma Cloud와 통합하려면 정책 및 경보 데이터에 대한 읽기 전용 액세스를 제공하는 Prisma에서 권한 그룹을 할당받아야 합니다. 권한 그룹에 대한 자세한 내용은 Prisma 클라우드 관리자 역할 에서 확인할 수 있습니다.

다른 권한 그룹에 할당된 역할에 대한 자세한 내용은 Prisma 클라우드 관리자 권한 페이지를 참조하십시오.

또한 경보를 읽을 수 있도록 접근 키를 생성해야 합니다. 접근 키 생성에 대한 자세한 내용은 접근 키 생성 및 관리 단원을 참조하십시오.

를 Vulnerability Response Integration with Palo Alto Prisma Cloud설치하고 구성하려면 다음 검사 목록을 사용합니다. 애플리케이션을 설치하기 전에 나열된 항목이 완료되었는지 확인합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

통합 준비 검사 목록

작업	설명
☐	다음 정보 집합이 있는지 확인합니다. • API 기준 URL • 접근 키 ID • 비밀 키 • Prisma Cloud에 액세스하기 위한 사용자 이름 및 암호입니다. 이러한 자격 증명은 인스턴스에서 Prisma Cloud 인스턴스에 ServiceNow AI Platform# 연결하는 데 사용됩니다. 등록 후 Prisma Cloud 포털에서 액세스 키 ID와 비밀 키를 생성해야 합니다.
☐	아직 설치 및 활성화되지 않은 경우 애플리케이션을 설치하기 전에 애플리케이션을 설치합니다 취약성 대응Vulnerability Response Integration with Palo Alto Prisma Cloud . 애플리케이션 설치 및 활성화에 취약성 대응 대한 자세한 내용은 다음 문서를 참조하십시오 취약성 대응 설치. 이 통합에는 버전 15.2.0취약성 대응 이상이 필요합니다.
☐	인스턴스에 아직 애플리케이션이 없는 경우 권리를 얻고 인스턴스에 애플리케이션을 ServiceNow AI Platform# 다운로드합니다Vulnerability Response Integration with Palo Alto Prisma Cloud. 문서를 참조하십시오.
☐	원활한 통합 실행을 위해 다음 플러그인을 설치했는지 확인합니다. • 취약성 대응 • 구성 준수 • Vulnerability Response Integration with Palo Alto Prisma Cloud 다음 플러그인은 선택 사항이지만 유용할 수 있습니다. • Cloud Provisioning and Governance • 디스커버리 및 서비스 매핑 패턴
☐	임포트할 것으로 예상되는 테스트 결과 수를 예상합니다. 임포트하려는 테스트 결과 수를 인스턴스가 수락할 수 있는지 확인합니다. 인스턴스 크기가 작으면 로드 시간이 길어질 수 있습니다. 인스턴스 크기를 모르거나 도움이 필요한 경우 기술 지원에 문의하십시오 ServiceNow .
☐	통합을 관리하고 테스트 결과를 정정할 관리자가 있는지 확인합니다. 관리자가 애플리케이션을 설치합니다 Vulnerability Response Integration with Palo Alto Prisma Cloud . 할당되지 않은 경우 관리자는 취약성 관리자(sn_vul.vulnerability_admin) 및 기타 역할을 할당합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

준비가 되었습니다 애플리케이션 설치 및 구성 Vulnerability Response Integration with Palo Alto Prisma Cloud.

애플리케이션 설치 및 구성 **Vulnerability Response Integration with Palo Alto Prisma Cloud**

Vulnerability Response Integration with Palo Alto Prisma Cloud Prisma Cloud에서 임포트한 데이터를 사용하려면 애플리케이션을 설치합니다. 이 데이터를 사용하여 자산의 잘못된 구성의 우선순위를 지정하고 정정합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 시스템 정의 > 플러그인.
2. 검색 창에서 Palo Alto Prisma Cloud## ### ## ### 검색합니다.
3. 설치를 클릭합니다.

   설치될 모든 종속성이 표시됩니다.
4. 다음으로 이동 모두 > **Prisma** 클라우드 통합 > 관리 > 구성 > **Prisma** 클라우드 구성.
5. 양식에서 필드를 채웁니다.

필드	설명
통합 인스턴스	새 통합 인스턴스의 이름입니다. 인스턴스를 만들거나 조회 아이콘을 클릭하여 기존 인스턴스를 선택할 수 있습니다.
API URL	Prisma 클라우드와 통합할 URL입니다.
접근 키 ID	Prisma 클라우드에 대한 액세스 요청을 인증하는 고유 키입니다. 주: Prisma Cloud 포털에 로그인한 후 키를 생성해야 합니다.
비밀 키	Prisma 클라우드에 대한 액세스 요청을 인증하는 개인 키입니다. 주: Prisma Cloud 포털에 로그인한 후 비밀 키를 생성해야 합니다.

6. 저장 및 테스트를 클릭합니다.

다음에 수행할 작업
설치를 완료한 후 **Prisma** 클라우드 통합 > 구성 구성을 계속합니다.

Vulnerability Response Integration with Palo Alto Prisma Cloud 애플리케이션 구성

Vulnerability Response Integration with Palo Alto Prisma Cloud 애플리케이션을 구성합니다. Prisma Cloud에서 임포트한 데이터를 사용하여 자산의 잘못된 구성의 우선순위를 지정하고 정정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 **Prisma** 클라우드 통합 〉 구성.
2. 양식에서 필드를 채웁니다.

Prisma 클라우드 구성

필드	설명
통합 인스턴스	새 통합 인스턴스의 이름입니다. 인스턴스를 만들거나 조회 아이콘을 클릭하여 기존 인스턴스를 선택할 수 있습니다.
API URL	Prisma Cloud와 통합할 URL입니다.
접근 키 ID	Prisma 클라우드에 대한 액세스 요청을 인증하는 고유 키입니다. Prisma Cloud 포털에 로그인한 후 키를 생성해야 합니다.
비밀 키	Prisma 클라우드에 대한 액세스 요청을 인증하기 위한 개인 키입니다. Prisma Cloud 포털에 로그인한 후 비밀 키를 생성해야 합니다.

3. 저장 및 테스트를 클릭합니다.

다음에 수행할 작업
구성을 완료한 후 **Prisma** 클라우드 통합 〉 통합 통합 실행이 성공했는지 확인합니다.

Vulnerability Response Integration with Palo Alto Prisma Cloud 임포트 실행 상태 확인

Vulnerability Response Integration with Palo Alto Prisma Cloud 임포트 실행 상태를 사용하여 통합 실행의 성공을 확인하고 문제를 식별합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
통합 실행 중에 여러 프로세스가 생성되고 데이터가 페이지 형식으로 수신됩니다. 각 프로세스에는 페이지에 첨부된 데이터가 있는 하나 이상의 임포트 큐 항목이 포함될 수 있습니다. 이러한 항목은 1시간의 시간 제한 내에 데이터를 처리해야 합니다. 그러나 페이로드 크기가 크면 처리 시간이 1시간을 초과하거나 중단되어 통합 시간 제한 오류가 발생할 수 있습니다. 통합은 시간 초과 오류에도 불구하고 데이터를 계속 처리합니다. 이러한 잘못된 통신을 피하기 위해 버전 14.8.5 구성 준수부터 큐가 활성 상태이고 데이터를 처리하는지 여부를 나타내기 위해 타임스탬프(하트비트)가 주기적으로 전송됩니다. 임포트 큐 항목 페이지의 처리된 마지막 기록 필드는 임포트 큐가 생성하거나 업데이트하는 기록 수에 따라 업데이트됩니다. 임포트 큐 항목이 1시간의 시간 제한을 초과하는 경우, 시스템은 마지막으로 처리된 기록 필드를 검사하여 1시간보다 오래되었는지도 확인합니다. 이 경우 이는 임포트 큐 항목이 고착되었음을 나타내며 처리 시 더 이상의 지연을 방지하기 위해 시간 초과됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
마지막으로 처리된 기록 필드는 다음 시스템 속성에 정의된 내용에 따라 업데이트됩니다.

- *sn_sec_cmn.record_threshold_heartbeat*: 하트비트(타임스탬프)가 임포트 큐 항목으로 전송된 후 처리된 기록 수를 정의합니다.
- *sn_sec_cmn.maximum_heartbeat_delay*: 임포트 큐 항목을 시간 초과해야 하는 시간을 정의합니다.

프로시저

1. 다음으로 이동 **Prisma** 클라우드 통합 〉 통합.
2. **Prisma** 정책 통합을 클릭합니다.
3. 지금 실행을 클릭합니다.
   이 통합이 실행되면 다음 테이블이 다음 순서로 채워집니다.
   a. sn_vulc_test.list(구성 테스트)
   b. sn_vulc_auth_src(권한이 부여된 소스)
   c. sn_vulc_citation(인용)
4. 항목 탭에서 취약성 통합 실행을 클릭하여 생성, 업데이트 및 무시된 새 테스트 수를 봅니다.

   주:
   정책은 선택한 클라우드 인스턴스에 대해 Prisma Cloud에 정의됩니다. 정의된 정책에 따라 인스턴스가 검사됩니다.

5. **Prisma** 경보 통합을 클릭합니다.
6. 지금 실행을 클릭합니다.
   다음 테이블은 통합에 따라 채워집니다.
   - 테스트 결과
   - 검색된 항목: 시스템에서 구성 항목을 사용할 수 없는 경우 새로 만들어집니다. 클래스는 항상 클라우드 자원입니다. 검색된 항목 페이지에 클라우드 자원 유형, 클라우드 서비스 제공자 및 자산 범주라는 세 개의 새 필드가 생성됩니다.

     항목 탭에서 취약성 통합 실행을 클릭하여 임포트, 업데이트 및 무시된 새 테스트 결과 수를 확인합니다. 또한 구성 항목 탭은 생성된 테스트 결과 수에 따라 채워집니다.

데이터 매핑

Prisma Cloud의 데이터가 인스턴스의 모듈 ServiceNow 로 구성 준수 임포트됩니다.

주:
의 구성 준수v14.9부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v14.9 이전 용어	용어 **v14.9** 이상
테스트 결과 그룹	정정 작업
그룹 규칙	정정 작업 규칙
정책	테스트 그룹

Prisma Cloud의 데이터는 표에 나와 있는 대로 다른 구성 준수 이름으로 임포트됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

구성 준수에서 **Prisma** 클라우드 데이터 매핑

Prisma 클라우드	구성 준수
정책	테스트
경보	테스트 결과
준수 표준	권한이 부여된 소스
섹션	인용
자산	디스커버리 항목/CI(구성 항목)

테스트

Prisma Cloud의 정책은 에서 구성 준수테스트로 임포트됩니다. 정책은 권한이 부여된 문서 및 테스트 레코드와 관련이 있으며 조직의 요구 사항에 맞게 수정할 수 있습니다. 다음으로 이동하여 테스트를 볼 수 있습니다. 구성 준수 〉 테스트.

Palo Alto Prisma Cloud와의 취약성 대응 통합이 설치된 경우 통합 작업이 *`Prisma Policy Integration`* 테스트를 검색합니다. 다음으로 이동하여 이 통합 작업을 볼 수 있습니다. 모두 〉 **Prisma** 클라우드 통합 〉 **Prisma** 정책 통합.

테스트 결과

Prisma Cloud의 경보는 다음의 구성 준수테스트 결과로 임포트됩니다. 경보는 정정 작업을 사용하여 정정됩니다. 다음으로 이동하여 테스트 결과를 볼 수 있습니다. 구성 준수 〉 테스트 결과.

외부 공급업체 통합의 구성 준수 일부로 테스트 결과를 임포트합니다. 애플리케이션에서 볼 수 있게 구성 준수 된 후에는 정정 작업을 사용하여 정정됩니다.

Palo Alto Prisma Cloud와의 취약성 대응 통합이 설치된 경우 통합 작업 **Prisma** 경보 통합이 테스트 결과를 검색합니다. 다음으로 이동하여 이 통합 작업을 볼 수 있습니다. 모두 〉 **Prisma** 클라우드 통합 〉 통합 〉 **Prisma** 경보 통합.

Prisma 경보 통합은 매일 실행되는 통합 작업이며 통합 탭의 시작 시간 필드에 정의된 시간 후에 상태 변경이 있는 테스트 결과를 끌어옵니다.

주:
통합 작업인 **Prisma** 경보 통합을 수동으로 실행하는 경우 통합 작업인 **Prisma Policy Integration**을 실행한 후 실행합니다.

Prisma 경보 통합이 데이터 임포트를 완료하면 임포트 종료 계산을 트리거하는 이벤트가 시작됩니다. 지난 며칠 동안 경보가 계속 실패하면 경보에 대한 상태 변경이 없으므로 통합에서 경보를 가져오지 않습니다. 따라서 Prisma 경보를 사용하여 테스트 결과 데이터를 최신 상태로 유지하기 위해 지난 7일 동안 업데이트된 경보를 가져오는 새로운 통합 작업인 **Prisma Comprehensive Alert Integration** 이 추가됩니다. 매주 실행되며 통과되지 않은 모든 테스트 결과를 가져옵니다.

권한이 부여된 소스

구성 준수 테스트는 테스트에 대한 취약성 경보를 생성할 때 신뢰할 수 있는 출처와 인용을 사용합니다. 권한이 부여된 소스는 일반적으로 ISO 27001 및 PCI DSS 3.2.1과 같은 게시된 산업 표준의 섹션에 매핑됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이러한 원본 기록에는 컴퓨터 보안 분야의 전문가가 제공한 알려진 소프트웨어 및 하드웨어 구성 문제에 대한 정보에 대한 참조가 포함되어 있습니다. 참조는 보안 정책 및 절차에 대한 요구 사항을 정의합니다. 다음으로 이동 구성 준수 〉 권한이 부여된 소스 권한이 부여된 소스를 볼 수 있습니다.

자산

가 Vulnerability Response Integration with Palo Alto Prisma Cloud 설치된 경우 예약된 작업은 *Prisma Alerts Integration* 검색된 항목 모듈 또는 테이블의 경보 관련 정보를 캡처합니다. 다음으로 이동하여 이 예약된 작업을 볼 수 있습니다. **Prisma** 클라우드 통합 〉 통합.

Prisma 경보 통합은 테이블에 저장된 자원 태그 및 클라우드 속성과 같은 추가 유형의 정보를 임포트합니다. 이 정보는 검색된 항목 양식에 표시됩니다.

- 호스트 태그: 자원에는 여러 태그가 있을 수 있습니다. 호스트 태그는 키 값 쌍 형식으로 사용할 수 있습니다. 예를 들어 운영 체제는 Windows 10이고 Java 버전은 1.8입니다.
- 자산에 대한 클라우드 속성: 다음과 같은 클라우드 속성을 사용할 수 있습니다.
  - 클라우드 계정: 통합의 계정 ID를 제공합니다. 이 정보는 클라우드 계정 [sn_sec_cmn_cloud_account. LIST] 테이블에 있습니다.
  - 클라우드 영역: 자원이 호스팅된 위치를 제공합니다. 이 정보는 클라우드 영역 [sn_sec_cmn_region. LIST] 테이블에 있습니다.
  - 클라우드 자원 유형: 자원 유형에 대한 정보(예: 가상 머신인지 데이터베이스 인스턴스인지 등)를 제공합니다. 이 정보는 클라우드 자원 유형 [sn_sec_cmn_cloud_resource_type. LIST] 테이블에 있습니다.
  - 클라우드 서비스 제공자: AWS(Amazon Web Services), Oracle Cloud 등 클라우드 서비스 제공자에 대한 정보를 제공합니다. 이 정보는 클라우드 서비스 제공자 [sn_sec_cmn_cloud_service_provider. LIST] 테이블에 있습니다.
  - 클라우드 계정 그룹: 계정 그룹에 대한 정보를 제공합니다. 이 정보는 클라우드 계정 그룹 [sn_vul_prismacloud_account_group.list] 테이블에서 채워집니다.

    주:
    클라우드 계정 그룹 속성은 Prisma에만 사용할 수 있습니다.

CI 조회 규칙

기본 시스템 CI 조회 규칙은 자원 ID, 이름 및 S3 버킷에 사용할 수 있습니다. CI 조회 규칙에 대한 자세한 내용은 다음 문서를 참조하십시오 에 대한 Microsoft Defender for Cloud Integration보안 운영 및 CI 조회 규칙 Palo Alto Prisma Cloud.

Prisma 클라우드 REST 메시지

Prisma REST 메시지는 규정 준수 데이터를 가져오기 위해 Prisma API(애플리케이션 프로그래밍 인터페이스)를 호출하는 데 사용됩니다.

다음 REST 메시지가 기본 시스템과 함께 제공됩니다.

Prisma Cloud 통합

모든 Prisma Cloud 통합은 인증 및 권한 부여에 JWT(JSON Web Token)를 사용합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Prisma 로그인 **REST** 메시지

엔드포인트	설명	방법	본문	**API** 문서 링크
/로그인	모든 후속 통합에 사용할 JWT 토큰을 가져옵니다.	##	{ "username": <<access key id >>, "password": <<secret access key>>}	https://pan.dev/prisma-cloud/api/cspm/app-login/

Prisma 새로 고침 토큰 **REST** 메시지

엔드포인트	설명	방법	본문	**API** 문서 링크
/auth_token/확장	만료 시 JWT 토큰을 자동으로 갱신합니다. 토큰 만료의 기본 기간은 60분입니다.	####	해당 사항 없음	https://pan.dev/prisma-cloud/api/cspm/extend-session/

Prisma 정책 **REST** 메시지

엔드포인트	설명	방법	본문	**API** 문서 링크
/v2/정책	Prisma에서 모든 정책 데이터를 검색합니다.	####	해당 사항 없음	https://pan.dev/prisma-cloud/api/cspm/get-policies/

Prisma 경보 **REST** 메시지

엔드포인트	설명	방법	본문	**API** 문서 링크
/v2/alert	Prisma에서 모든 경보를 검색합니다.	##	{ "detailed": "false", "filters": [{ "name": "timeRange.type", "operator": "=", "value": "ALERT_STATUS_UPDATED" }], "sortBy": ["resource.id"], "pageToken": "", "offset": 0, "limit": 2000, "timeRange": { "type": "absolute", "value": { "startTime": <<Import since at integration level>>,	https://pan.dev/prisma-cloud/api/cspm/post-alerts/

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Prisma 경보 **REST** 메시지

엔드포인트	설명	방법	본문	**API** 문서 링크
			"endTime": << Current integration run time>> } } }	

Prisma 이해 경보 통합의 경우 위 POST 본문의 필터를 다음과 같이 교체해야 합니다.

```
"filters": [
 {
                "name": "alert.status",
                "operator": "=",
                "value": "open"
            },
            {
                "name": "alert.status",
                "operator": "=",
                "value": "dismissed"
            },
            {
                "name": "alert.status",
                "operator": "=",
                "value": "snoozed"
            },
            {
                "name": "alert.status",
                "operator": "=",
                "value": "pending_resolution"
            },
            {
                "name": "timeRange.type",
                "operator": "=",
                "value": "ALERT_UPDATED"
            }

  ],
```

Qualys 및 구성 준수 통합

정책 준수는 Qualys 데이터를 수집하여 자동으로 애플리케이션에 전송 Qualys 하며, 애플리케이션은 정보를 지속적으로 분석하고 상관 관계를 지정합니다. 통합 for Security Operations로 Qualys 쉽게 통합되어 구성 결과를 CI 및 비즈니스 서비스에 매핑하여 잠재적인 구성 오류의 영향과 우선순위를 결정합니다.

애플리케이션 배포가 Qualys Cloud Platform 여러 개 있는 경우 각 배포에 대한 통합을 추가할 수 있습니다. 여러 외부 공급업체 배포 및 해당 취약성으로 식별된 자산이 CMDB와 통합되고 조정됩니다. 이러한 통합은 여러 배포 간에 스캔 프로세스가 겹치는 경우에도 발생합니다. 각 배포에서 소싱된 데이터가 식별되고 의 단일 인스턴스에서 취약성 대응사용할 수 있습니다.

주:
원래 취약성 통합을 삭제할 수는 없지만 사용하지 않도록 설정할 수는 있습니다. 비활성 템플릿에서 생성된 통합은 기본적으로 비활성화됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

호스트 태그

호스트 목록 통합의 Qualys 일부로 모든 호스트 태그가 임포트됩니다. 호스트 태그는 할당 및 정정 작업 규칙의 필터링에 취약성 대응 주로 사용됩니다. 검색된 항목 양식에 표시됩니다.

주:
호스트 목록 통합은 Qualys 할당 또는 정정 작업 규칙을 취약성 대응 생성하기 전에 실행되어야 모든 태그가 규칙에 포함될 수 있고 취약한 항목을 임포트 및 그룹화할 수 있습니다.

- 태그 스토리지는 대/소문자를 구분하지 않습니다. **San Diego** 태그가 생성되면 호스트 태그 테이블에 **SAN DIEGO** 태그를 저장할 수 없습니다. 'San Diego'와 'SAN DIEGO'는 동일한 호스트 태그로 간주됩니다. 먼저 가져온 태그가 우선합니다.
- 정정 작업 규칙에서 호스트 태그를 그룹 키로 사용하면 예기치 않은 결과가 발생할 수 있습니다. 호스트 태그는 조건 작성기에서만 사용할 수 있습니다.
- 호스트 태그는 전역 시스템 속성 sn_vul.import_host_tags에 의해 제어됩니다. 이 속성은 기본적으로 true로 설정됩니다. 태그를 끄면 모든 인스턴스에서 태그가 꺼집니다.

호스트 태그(자산 태그라고도 함)는 조직의 자산을 구성하고 추적하는 데 사용됩니다. 호스트 자산에 태그를 할당할 수 있습니다. 그런 다음 검사를 시작할 때 검사할 호스트와 연결된 태그를 선택할 수 있습니다. 호스트 태그 모듈을 사용하면 일정에 따라 인스턴스에서 인스턴스로 Qualys 호스트 태그 데이터를 다운로드할 수 있습니다.

테스트를 테스트 그룹과 연결

테스트 양식의 테스트 그룹 필드를 채우려면 시스템 속성을 활성화합니다 *sn_vulc.add_policy_as_key* . 테스트가 테스트 그룹과 연결되는 방식, 이 시스템 속성 활성화의 영향 및 필수 구성 요소에 대한 자세한 내용은 KB1644268 문서를 참조하십시오.

경고:
시스템 속성을 활성화한 후에는 비활성화 *sn_vulc.add_policy_as_key* 할 수 없습니다. 따라서 이 시스템 속성을 활성화하기 전에 KB1644268 문서의 영향 섹션을 검토하십시오.

이 시스템 속성을 활성화하면 다음 수집 후에 테스트 그룹 필드가 테스트 테이블에 추가되고 테스트가 속한 테스트 그룹이 채워집니다. 따라서 다음을 쉽게 수행할 수 있습니다.

- 테스트에서 테스트 그룹으로 닷워킹하여 테스트 결과가 속한 테스트 그룹을 식별합니다.
- 다른 테스트 그룹과 연결된 동일한 테스트 ID로 테스트 기록을 구별합니다.

애플리케이션과 통합 **QualysServiceNow®** 구성 준수

시스템에 Qualys Vulnerability Integration 이미 설치되어 있고 API 자격 증명이 사용하려는 구성 준수자격 증명과 다른 경우 설정 도우미(의 취약성 대응)로 이동하여 각 **Qualys PC** 통합에 할당합니다.

다음으로 이동 모두 〉 **Qualys** 취약성 통합 〉 기본 통합 을 클릭하고 **Qualys REST** 상세 정보 탭 아래의 **Qualys API** 자격 증명 필드를 편집합니다.

PCRS 매개변수 구성

의 Qualys Integration for Security Operationsv12.6.3부터 PCRS 정책 호스트 통합 및 Qualys PCRS 테스트 결과 통합을 사용하여 Qualys 새 API 세트 Qualys 로 테스트 결과를 임포트할 수 있습니다. 이러한 통합에는 정보를 Qualys가져올 게이트웨이 URL이 필요합니다.

시작하기 전에
필요한 역할: 관리자

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보
를 설치할 Qualys Integration for Security Operations 때 for 취약성 대응에서 새 PCRS 통합구성 준수에 대한 **gateway_url** 구성할 수 있습니다. API URL에 대한 게이트웨이 URL을 찾는 방법에 대한 자세한 내용은 Qualys 플랫폼 식별 을 참조하세요.

인스턴스에 게이트웨이 URL을 추가해야 ServiceNow 합니다.

프로시저

1. 다음으로 이동 모두 〉 **Qualys** 취약성 통합 〉 관리 〉 통합 인스턴스.

   주:
   현재 범위가 Security Operations용 Qualys인지 확인하십시오.

2. PCRS 통합에 사용되는 인스턴스를 엽니다.
3. 통합 인스턴스 매개변수 탭에서 gateway_url 구성에 대한 게이트웨이 URL 을 추가합니다.

   주:
   Qualys PCRS 테스트 결과 통합은 Qualys PCRS 정책 호스트 통합에 종속됩니다. 따라서 통합 Qualys PCRS 테스트 결과를 소급 적용하는 경우 동일한 순서로 다시 실행해야 할 수 있습니다.

Qualys Integration for Security Operations와 함께 설치되는 구성요소

다음 역할, 예약된 작업 및 테이블이 Qualys Integration for Security Operations와 함께 설치됩니다.

주:
애플리케이션 파일 테이블에는 이 애플리케이션과 함께 설치되는 구성요소가 나열됩니다. 이 테이블에 액세스하는 방법에 대한 지침은 애플리케이션과 함께 설치되는 구성요소 찾기 를 참조하십시오.

애플리케이션과 함께 설치된 구성요소에 대해 필터링된 목록 보기

애플리케이션과 함께 설치되는 역할, 예약된 작업 및 테이블만 표시되도록 애플리케이션 파일 테이블을 필터링합니다. 해당 파일이 인스턴스와 메타데이터 테이블에 로드되도록 이러한 구성요소를 보려는 애플리케이션을 설치해야 합니다. 다음 단계에 따라 애플리케이션 파일 테이블에서 필터링된 목록을 봅니다.

1. 필터 탐색기에서 **sys_metadata.list** 를 입력하여 메타데이터 테이블로 이동합니다.
2. 조건 작성기(필터 아이콘)를 선택하고 애플리케이션 〉 다음과 같음 다음에 애플리케이션 이름이 표시됩니다. 예: 애플리케이션 〉 다음과 같음 〉 취약성 대응.
3. 조건 작성기에서 두 번째 필터를 추가하려면 **AND**를 선택한 뒤 클래스 〉 다음 중 하나 을 클릭하고 목록에서 역할, 예약된 작업 또는 테이블 클래스 중 하나를 선택합니다.
4. 실행을 선택합니다.

선택한 클래스의 결과가 필터링된 목록에 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설치되는 역할

역할 이름 **[name]**	설명	포함하는 역할
sn_vul_qualys.읽기	기록에 Qualys Vulnerability Integration 대한 읽기 권한이 있습니다.	
sn_vul_qualys.user	에 대한 사용자입니다 Qualys Vulnerability Integration. 기록을 읽고 쓸 수 있습니다.	sn_vul_qualys.읽기
sn_vul_qualys.admin	관리자.Qualys Vulnerability Integration 예를 들어 통합 시작 날짜를 수정하고 일부 고급 구성 설정을 수행할 수 있습니다.	• sn_vul_qualys.user • sn_vul.vulnerability_analyst
sn_vul.configure_qualys_integration	구성할 수 있는 항목 Qualys Vulnerability Integration	sn_vul_qualys.admin

설치되는 예약된 작업

예약된 작업	설명
Qualys PC 정책	에서 Qualys정책을 검색합니다. 출력은 sn_vulc_policy 테이블에 저장됩니다. 이 통합에 사용된 API는 페이지 매김을 지원하지 않으므로 모든 정책이 단일 페이지에서 다운로드됩니다.
Qualys PC 정책 상세 정보	예를 들어 기술 및 섹션과 같은 전체 정책 상세 정보를 검색합니다.
Qualys PC 컨트롤	에서 Qualys다른 통제 ID에 대한 준수 통제 정보를 검색합니다.
Qualys PC 결과	에서 Qualys규정 준수 태세 기록을 검색합니다. 이 통합의 출력은 테스트 결과입니다. 기본적으로 매개변수 상세 정보는 호스트 정보, 마지막 스캔 날짜/시간, 통제 ID 및 증거 정보를 임포트하기 위해 전달됩니다.
Qualys PC 종합 결과	통과되지 않은 테스트 결과의 마지막 평가 날짜를 기준으로 규정 준수 태세 기록을 Qualys 검색합니다. 이 작업은 일주일에 한 번 실행됩니다. 이 통합의 출력은 테스트 결과입니다. 기본적으로 호스트 정보, 마지막 스캔 날짜/시간, 통제 ID 및 증거 정보를 임포트하기 위해 매개변수 상세 정보가 전달됩니다.
Qualys PCRS 정책 호스트 통합	호스트 데이터를 Qualys 검색하여 인스턴스에서 처리합니다. 이 통합의 출력은 정책 호스트 ID입니다 . Qualys 이 통합에서 호스트 데이터가 임포트됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예약된 작업	설명
	주: • 이 예약된 작업은 가 설치된 경우에만 구성 준수 나타납니다. • 이 통합을 실행하기 전에 gateway_url 및 pcrs_page_size 통합 인스턴스 매개변수를 구성합니다. 이 두 통합은 비활성 OOB가 됩니다. 이러한 통합 중 하나를 활성화하면 PC 결과 통합이 비활성화됩니다. 이 두 통합은 Qualys의 새로운 스트리밍 API를 기반으로 추가됩니다.
Qualys PCRS 테스트 결과 통합	각 호스트 ID에 대한 테스트 결과를 검색합니다. 이 통합은 통합 상세 정보 탭의 시작 시간 매개변수를 사용합니다. 주: • 이 예약된 작업은 가 설치된 경우에만 구성 준수 나타납니다. • 이 통합을 실행하기 전에 gateway_url 및 pcrs_page_size 통합 인스턴스 매개변수를 구성합니다. • 통합을 수동으로 실행하도록 선택하는 경우 PC 정책, Qualys PC 정책 세부 정보 및 Qualys PCRS 정책 호스트 통합 후 Qualys PCRS 테스트 결과 통합을 실행합니다Qualys.

주:
Qualys PCRS 정책 호스트 및 Qualys PCRS 테스트 결과 통합은 기본적으로 비활성 상태입니다. 이 두 통합은 의 새로운 스트리밍 API Qualys를 기반으로 합니다. 이러한 통합 중 하나를 활성화하면 PC 결과 통합이 비활성화되며 그 반대의 경우도 마찬가지입니다.

설치되는 테이블

테이블	설명
Qualys PC 결과 임포트 sn_vul_qualys_pc_result_import	임포트 세트 행을 확장하는 테이블입니다. 필드 맵 변환을 건너뛰고 응답 첨부 파일이 onComplete 스크립트로 직접 처리됩니다.
정책 호스트 ID sn_vul_qualys_policy_host_id	정책과 이 정책이 스캔된 호스트 간의 매핑을 저장하는 테이블입니다. 이 테이블은 새 Qualys PCRS 통합에 사용됩니다. 주: 이 테이블은 가 설치된 경우에만 구성 준수 나타납니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테이블	설명
Qualys PCRS 정책 호스트 임포트 sn_vul_qualys_pcrs_policy_host_import	임포트 세트 행을 확장하는 테이블입니다. 필드 맵 변환을 건너뛰고 응답 첨부 파일이 onComplete 스크립트로 직접 처리됩니다. 주: 이 테이블은 가 설치된 경우에만 구성 준수 나타납니다.
Qualys PC 정책 임포트 sn_vul_qualys_pc_policy_import	임포트 세트 행을 확장하는 테이블입니다. 필드 맵 변환을 건너뛰고 응답 첨부 파일이 onComplete 스크립트로 직접 처리됩니다.

Qualys 통합을 위한 네트워크 파티션 식별자로 구성 항목 업데이트

IP 주소를 공유하는 환경의 자산에 대한 고유한 CI(구성 항목)를 생성합니다. 환경 전반에서 고유한 자산을 식별하고 기존 검색된 항목, 취약한 항목 및 탐지 레코드의 CI를 자동으로 업데이트하여 취약성에 대한 자세한 정보를 제공합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
기본적으로 취약성 대응 애플리케이션에서 자산을 식별하는 한 가지 방법은 IP 주소를 사용하는 것입니다. 경우에 따라 자산은 IP 주소를 공유할 수 있지만 CMDB에 하나의 CI로 저장됩니다.

예를 들어 다음 표와 같이 환경의 여러 자산(CI)은 IP 주소를 공유할 수 있지만 고유한 네트워크 및 리포지토리 ID를 가질 수 있습니다. 그러나 기본적으로 이러한 자산은 일반적으로 IP 주소 조회 중에 단일 CI (CI 1) 로 식별되고 저장됩니다.

기본 **IP** 조회 및 **CI** 생성

소스	**IP** 주소	**NETWORK_ID**	구성 항목
Qualys Vulnerability Integration: 자산과 고정 및 미해결 취약성 통합	123.12.12.141	03712	CI 1
	123.12.12.141	03713	CI 1

소스	**IP** 주소	**REPOSITORY_ID**	구성 항목
Qualys Vulnerability Integration: 자산과 고정 및 미해결 취약성 통합	123.12.12.141	12	CI 1
	123.12.12.141	13	CI 1

동일한 IP 주소를 가진 자산에 대해 개별 CI를 생성하여 고유한 자산으로 식별할 수 있습니다. 새로운 데이터 임포트를 시작으로 예약된 작업을 실행하여 네트워크 파티션 식별자(network_partition_identifier)를 포함하는 기존 CI *`Update existing discovered items with network partition identifier`*를 보다 세밀하게 업데이트할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 예약된 작업은 기본적으로 비활성화되어 있습니다. 설정 도우미에서 자산 및 고정 및 미해결 취약성 통합 Qualys Vulnerability Integration 에 대해 이 기능을 활성화하여 기록에서 이 식별자를 봅니다.

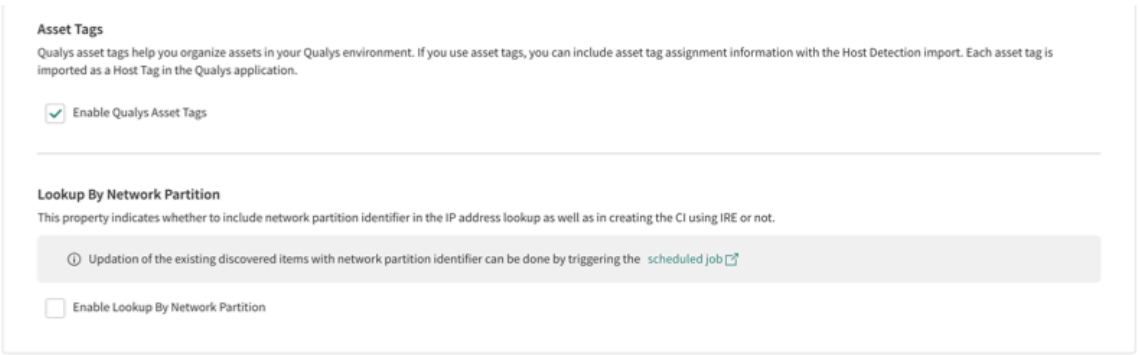
이 예약된 작업은 활성화되면 임포트한 데이터의 기존 CI 기록에 네트워크 파티션 식별자 〔network_partition_identifier〕를 추가합니다. IRE에서 만든 기존 CI도 업데이트됩니다. 또한 예약된 작업은 다음 임포트로 시작하는 네트워크 파티션 식별자를 포함하는 CI를 생성합니다. 또는 요청 시 작업을 시작하여 기존 데이터를 업데이트할 수 있습니다.

취약성 통합 v14.0 취약성 대응 및 v12.1 Qualys Vulnerability Integration 부터 CMDB CI Class Models(1.0.21.)가 지원됩니다. 클래스 모델에는 IRE(식별 및 조정) 식별 규칙에 네트워크 파티션 식별자 〔network_partition_identifier〕가 있습니다.

옵션	설명
요청 시 예약된 작업을 실행합니다.	기존 검색 항목을 업데이트합니다. 기존 Qualys Vulnerability Integration 데이터에 대한 CI는 네트워크 파티션 식별자 세분성을 포함하도록 생성되거나 업데이트됩니다. 검색된 항목, 취약한 항목 및 탐지 기록이 모두 새 CI로 업데이트됩니다.
다음 예약된 작업과의 통합에서 최신 데이터가 임포트될 때까지 기다립니다.	예약된 다음 작업으로 시작하는 네트워크 파티션 식별자를 사용하여 각각의 새 자산에 대한 CI를 생성합니다. CI, 취약한 항목 및 탐지 기록이 모두 새로운 세분성을 포함하도록 업데이트됩니다. 정확히 일치하는 항목이 없으면 새 CI가 만들어집니다.

프로시저

1. 다음으로 이동 취약성 대응 〉 설정 도우미 〉 통합 구성 〉 스캐너 통합.
2. 을(를) 선택합니다 Qualys Vulnerability Integration.
3. 필요한 통합을 편집합니다.
4. 선택 호스트 탐지 구성.
5. 선택 네트워크 파티션별 조회 사용 의 확인란 네트워크 파티션별 조회



절.

6. 마침을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

네트워크 파티션 식별자 **NETWORK_ID** 및 리포지토리_**ID IP** 조회 및 **CI** 생성에 포함됩니다.

소스	**IP** 주소	**NETWORK_ID**	네트워크 파티션 식별자가 없는 자산에 대한 **CI**	**CI** 네트워크 파티션 식별자가 있는 자산
Qualys Vulnerability Integration: 자산과 고정 및 미해결 취약성 통합	123.12.12.141	03712	CI 1	CI 1
	123.12.12.141	03713	CI 1	CI 2

소스	**IP** 주소	**REPOSITORY_ID**	네트워크 파티션 식별자가 없는 자산에 대한 **CI**	**CI** 네트워크 파티션 식별자가 있는 자산
Qualys: 자산 및 고정 및 미해결 취약성 통합	123.12.12.141	12	CI 1	CI 1
	123.12.12.141	13	CI 1	CI 2

IP 주소 및 불완전한 IP 주소 CI 식별 조회 규칙에는 자산 및 의 고정 및 미해결 취약성 통합 Qualys Vulnerability Integration에서 데이터를 임포트하기 위한 네트워크 파티션 식별자 속성이 자동으로 포함됩니다.

예약된 작업을 활성화하고 기록을 저장한 후 요청 시 예약된 작업을 시작하여 네트워크 파티션 식별자가 포함된 CI로 기존 검색된 항목을 업데이트할 수도 있습니다. 기존 검색된 항목, 취약한 항목 및 탐지 기록의 CI가 자동으로 업데이트됩니다.

임포트에 대한 **Qualys** 추가 필터 매개변수 설정

지원되는 Qualys Vulnerability IntegrationQualys 통합을 통해 임포트하는 취약성 데이터를 더욱 구체화할 수 있도록 예약된 쿼리에 대한 필터링 매개변수를 사용자 지정합니다.

시작하기 전에

사용 사례: 취약성 관리자 또는 분석가는 특정 취약성 상세 정보만 검토할 수 있도록 쿼리에서 데이터를 필터링할 수 있습니다. 예를 들어 특정 IP 또는 IP 범위별로 필터링되는 임포트된 취약성을 보려는 경우를 가정해 보겠습니다. 또는 사용자 범위 내에 있는 컴퓨터만 가져오려는 경우(예: 외부 장치가 아닌 회사 네트워크 내의 컴퓨터만 가져오려는 경우)

이 데이터를 수집하는 데 도움이 되도록 필요한 특정 취약성 상세 정보를 가져오는 데 도움이 되는 매개변수를 추가할 Qualys 수 있습니다.

이 기능을 사용하면 API 호출이나 코딩을 추가하지 않고도 HTTP 요청 정보를 QualysServiceNow AI Platform. 지원되는 Qualys 통합 Qualys Vulnerability Integration에 대한 REST 메서드 아래의 HTTP 메서드 기록에서 이러한 값을 수정하거나 추가합니다.

필요한 역할: sn_vul.vulnerability_admin

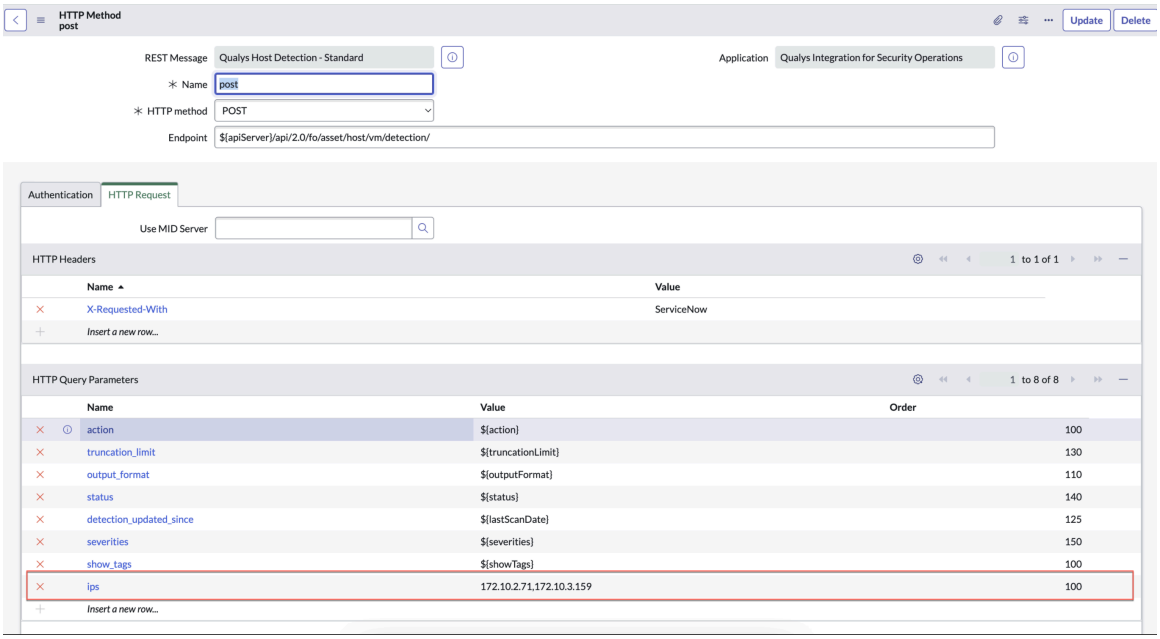
프로시저

1. 필터링에 사용할 개발자 사이트의 제품에서 Qualys 지원하는 매개변수를 찾습니다.
   제품에서 Qualys 입력하는 매개변수와 값은 의 통합 인스턴스 수준 ServiceNow AI Platform에서만 지원됩니다. 모든 Qualys 통합은 쿼리 매개변수를 사용한 필터링을 지원합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

2. 다음으로 이동 모두 〉 **Qualys** 취약성 통합 〉 관리 〉 기본 통합.
3. Qualys 통합 목록 페이지에서 기록을 열고자 하는 통합에 대한 기록을 클릭합니다.
4. Qualys REST 상세 정보 탭을 선택한 상태에서 REST 메서드에 대한 정보 아이콘(I)과 기록 열기를 차례로 찾아 클릭하여 HTTP 메서드 기록을 엽니다.
5. **HTTP** 요청 탭을 선택합니다.
6. 요청 본문에 대한 HTTP 쿼리 매개변수에서 개발자 사이트에서 가져온 Qualys 값을 추가합니다.

   예를 들어 다음 이미지에서는 특정 IP 주소/범위 *ips={value}* 만 수집하는 매개 변수가 추가되었습니다. 이 경우 값은 지정한 하나 이상의 IP/범위입니다. 여러 항목은 쉼표로 구분되고 (172.10.2.71, 172.10.3.159) 범위는 하이픈(10.10.10.1-10.10.10.100)으로 지정됩니다. Qualys 자세한 내용은 개발자 사이트를 참조하십시오.



   둘 이상의 매개변수를 입력하려면 각 값을 구분하는 방법에 대한 자세한 내용은 설명서를 참조하십시오 Qualys .

   > **주:**
   > API 요구 사항을 알고 있어야 합니다. 이러한 API 속성을 쿼리 매개변수 또는 본문 콘텐츠에 추가해야 할 수 있습니다.

   개발자 사이트에서 유용할 수 있는 몇 가지 다른 매개변수:Qualys

   - *ag_ids* - 검색할 자산 그룹 목록 ID입니다. 이 매개변수를 사용하면 사용자 범위 아래에 있는 컴퓨터만 가져올 수 있습니다.
   - *qids* - 이 매개변수는 특정 취약점(외부 공급업체 항목 테이블의 QID)으로만 결과를 제한합니다. 이 설정은 시스템에 정보 레코드가 넘쳐나는 것을 방지합니다.
7. 업데이트를 클릭합니다.

Qualys 테스트 결과 세분성 구성

선택한 구성 키를 기반으로 시스템이 결과를 더 자세히 임포트할 수 있도록 Qualys 테스트 결과 세분성을 구성합니다. 기본 키 외에도 요구 사항에 따라 추가 키를 구성하여 세분성을 높일 수 있습니다. 세분화된 임포트를 통해 팀은 각 자산을 독립적으로 관리하고 여러 기록이 공통 식별자를 공유할 때 데이터를 덮어쓰는 일을 방지할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할:

- sn_vulc.admin

프로시저

1. 다음으로 이동 모두 〉 **Qualys** 테스트 결과 세분성 구성.
2. 키 구성 양식에서 다음 사항을 확인합니다.
   - 소스 통합 은 Qualys #### ######.
   - 테이블이### ### 설정됩니다.
3. 구성 키 섹션에서 고유한 테스트 결과를 생성할 필드를 선택합니다.
   예를 들어, 선택하면 *instance* 데이터베이스 내의 각 인스턴스에 대해 고유한 테스트 결과가 생성됩니다.

   주:
   이 기능은 주의해서 사용해야 합니다. 각 추가 구성 키는 통합 시간을 증가시킵니다. 최적의 성능을 유지하려면 3개 이하의 추가 키로 사용을 제한하십시오.

4. 세분성을 활성화하려면 옆에 예를 입력하고, 사용하지 않으려면 아니오를 *instance* 입력합니다.
5. 업데이트를 선택하여 변경 내용을 저장합니다.

〔store-future: BEGIN review〕

에서 테스트 결과를 테스트 그룹과 연결 **Qualys**구성 준수

테스트 그룹에 매핑 Qualys 하여 테스트 및 구성 준수 테스트 결과를 생성합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
Qualys 사용자 지정 정책 및 통제를 생성할 수 있도록 하는 동시에 기본 정책 및 통제 라이브러리를 유지합니다. 이러한 통제는 정책에 매핑되어 IT 자산의 보안 태세를 평가하기 위한 포괄적인 프레임워크를 제공할 수 있습니다. 자산에 대해 평가될 때 정책은 태세를 생성 Qualys 하며, 이는 의 테스트 결과로 구성 준수변환됩니다. 정책에 매핑된 컨트롤이 라이브러리에 있는 QualysQualys 기본 컨트롤과 다릅니다. 이를 통해 정책 수준에서 통제에 대한 중요도, 상태(활성 또는 비활성) 및 기술과 같은 속성을 유연하게 정의할 수 있습니다.

이전에는 구성 준수에서 일반적으로 테스트에 매핑된 통제가 아닌 라이브러리 통제에 Qualys 대해 Qualys 생성되었습니다. 테스트 결과는 테스트 그룹 매핑이 없는 테스트를 참조합니다. 따라서 의 Qualys자세에 비해 의 구성 준수 테스트 결과가 적을 수 있습니다.

테스트 그룹에 매핑하여 테스트 구성 준수 및 테스트 결과를 생성하기 위해 테스트 수준에 새 열 "테스트 그룹"이 추가되었습니다. 이 열의 채우기는 시스템 속성 *sn_vulc.add_policy_as_key*에 의해 제어됩니다. 이 시스템 속성을 활성화하면 구성 준수 라이브러리 통제(테스트 그룹이 비어 있음)와 정책에 매핑된 통제(테스트 그룹이 정책 ID가 됨) 모두에 대한 테스트가 생성됩니다. 테스트 결과는 정책 매핑이 있는 테스트를 참조합니다.

모든 테스트 결과가 테스트 그룹 매핑을 사용하여 새 테스트로 마이그레이션되도록 하려면 다음을 수행합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. sn_vulc.add_policy_as_key 시스템 속성을 활성화합니다.
   a. 필터 탐색기에서 sys_properties.list를 입력하여 인스턴스에 대한 시스템 속성 목록을 표시합니다.
   b. sn_vulc.add_policy_as_key 시스템 속성을 검색하여 엽니다.
   c. 경고 메시지의 링크를 선택하여 시스템 속성을 편집합니다.
   d. sn_vulc.add_policy_as_key 시스템 속성을 활성화하려면 값 필드를 True로 설정합니다.
2. 옵션: 구성 준수에 기존 데이터(테스트 및 테스트 결과)가 있는 고객의 경우:
   a. sn_vulc.add_policy_as_key 시스템 속성의 시작 시간 필드를 지웁니다.
   b. 다음 순서로 통합을 실행합니다.
      - Qualys PC 정책
      - Qualys PC 컨트롤
      - Qualys PC 정책 상세 정보
      - Qualys PC 결과/Qualys PCRS 테스트 결과 통합
3. 다음을 확인합니다.
   - Qualys PC 정책을 실행한 후 테스트 그룹 참조를 사용하여 새 테스트가 생성되었는지 확인합니다.
   - Qualys PC 결과/Qualys PCRS 테스트 결과 통합을 실행한 후 모든 테스트 결과가 채워진 테스트 그룹 참조가 있는 새 테스트를 가리키는지 확인합니다.

결과

- 테스트 그룹에 대한 참조를 사용하여 새 테스트가 생성됩니다. 새 테스트에 대한 테스트 그룹 관련 목록이 채워지지 않습니다. 새로운 테스트는 의 Qualys정책에 매핑된 통제를 기반으로 하며, 정책 수준에서 통제의 중요도, 상태(활성 또는 비활성) 및 기술을 반영합니다.
- 테스트 그룹 참조가 없는 테스트는 라이브러리의 Qualys 컨트롤을 반영합니다.
- 모든 테스트 결과는 테스트 그룹 매핑이 있는 새 테스트를 가리킵니다. 관련 테스트로 닷워킹하여 테스트 결과에 대한 테스트 그룹을 식별할 수 있습니다.

〔End〕

취약성 통합 문제 해결 **Qualys**

일반적으로 발생하는 몇 가지 문제와 임시 해결책에 대해 논의합니다.

임포트 후 첨부 파일이 표시되지 않음

외부 공급업체 통합을 임포트한 후 데이터 소스 또는 보안 인시던트에 첨부 파일이 예상대로 표시되지 않으면 IP 제한을 확인하십시오.

IP 액세스 제한으로 인해 안전한 IP에서 로그인하지 않으면 첨부 파일을 볼 수 없습니다. 가져올 때마다 새 첨부 파일이 추가되므로 제거해야 하는 중복이 발생할 수 있습니다.

예를 들어 타사 호스트 임포트 통합을 실행할 때 데이터 소스에 첨부 파일이 표시되지 않으면 IP 제한을 확인하고 임포트하기 전에 사용자를 허용 목록에 추가하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

변환 맵 수정

변환 맵은 기본 구성으로 제공되며 일반적으로 충분합니다. 조직의 필요에 따라 변환 매핑을 수정할 수 있습니다.

시작하기 전에
필요한 역할: sn_vul_qualys.admin + import_admin

프로시저

1. 다음으로 이동 모두 〉 시스템 임포트 세트 〉 관리 〉 변환 맵 을 클릭하여 REST 메시지를 봅니다.
2. 결과 목록을 애플리케이션별로 필터링하고 목록을 **Qualys** 취약성 통합 애플리케이션으로 제한합니다.
3. 고객 요구사항에 따라 변환 맵을 수정합니다.

   Qualys API에서 제공하는 데이터에 대한 자세한 내용은 Qualys API 문서를 참조하십시오.

XML 첨부 파일 속성 크기 확인

XML 첨부 파일 속성이 큰 파일에 충분한지 확인합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 〉 시스템 속성 〉 임포트 익스포트.
2. 까지 아래로 스크롤합니다. 임포트 속성 〉 **XML** 형식 페이지 하단에 있습니다.

3. 필요한 경우 값을 250으로 변경하고 저장을 클릭합니다.

관련 정보

사용 가능한 시스템 속성

데이터 검색 제한 사항

기본적으로 Qualys에서 데이터를 검색하는 방법에는 제한이 없습니다. 많은 기록이 고객이 취약성 대응 프로세스를 사용하여 정정하지 않으려는 낮은 심각도 취약성과 관련될 수 있습니다. 해당 REST 메시지/메서드 매개변수를 업데이트하면 이 동작을 수정할 수 있습니다.

이 업데이트를 담당하는 REST 메시지/메서드는 **Qualys** 호스트 탐지 – 표준/게시입니다. 값을 업데이트하려면 다음 값을 사용하여 post 메서드에 새 HTTP 쿼리 매개변수를 추가합니다.

- 이름: severities
- 값: 3-5(또는 원하는 적절한 심각도)

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Qualys 기술 자료 통합에 실패했습니다.

에서 Qualys 수신되는 페이로드 첨부 파일 크기를 지정된 한도로 줄여 지식베이스 통합 실패를 해결합니다Qualys.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin

프로시저

1. 페이로드 첨부 파일 크기가 지정된 한도 내에 있는지 확인합니다.
   a. 다음으로 이동 모두 〉 **Qualys** 취약성 통합 〉 통합 인스턴스.
   b. 통합 인스턴스 매개변수 탭을 선택합니다.
   c. **max_delta_days** 선택하고 기본값을 3으로 수정합니다.
2. 통합이 계속 실패하면 다음 단계를 수행합니다.
   a. 다음으로 이동 모두 〉 **Qualys** 취약성 통합 〉 기본 통합.
   b. **Qualys** 기술 자료를 선택합니다.
   c. 통합 세부 정보 탭을 선택합니다.
   d. 시작 시간 필드에서 현재 날짜를 선택하여 해당 날짜의 실행 실행을 건너뜁니다.
   e. 다음으로 이동 모두 〉 **Qualys** 취약성 통합 〉 통합 인스턴스.
   f. 통합 인스턴스 매개변수 탭을 선택합니다.
   g. **kb_backfill_full_import** 선택하고 기본값을 true로 수정합니다.

결과
Qualys 지식베이스 백필 통합을 실행하면 시스템의 모든 타사 항목(TPE)이 업데이트됩니다. Qualys 호스트 탐지 통합이 자리 표시자 항목을 생성하는 동안 Qualys 지식베이스 백필 통합이 이를 업데이트합니다.

Qualys 통합 실행 상태 차트

Qualys 통합 실행 상태 모듈은 통합 실행 상태에 Qualys 대한 그래픽 뷰입니다.

통합 실행의 상태를 보려면 다음으로 이동합니다. **Qualys** 취약성 통합 〉 통합 실행 상태.

의 취약성 대응버전 19.0부터 이 대시보드는 New Experience UI에서 사용할 수 있습니다.

> **주:**
> Tokyo에 있는 경우 Next Experience UI에서 대시보드를 볼 수 있지만 일부 기능 손실이 있습니다.

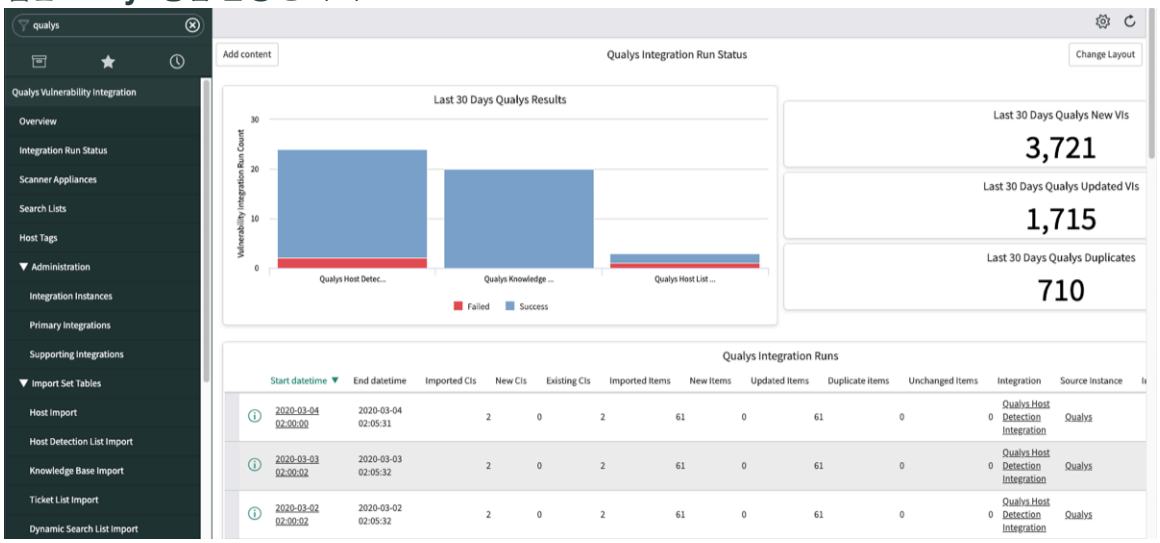
차트에서 원하는 부품(막대형, 원형, 데이터 요소 등)을 가리키면 해당 부품과 관련된 일반 데이터를 볼 수 있습니다. 보고서의 일부를 클릭하면 자세한 정보를 제공하는 목록이 열립니다.

통합 실행 상태에는 Qualys 지난 30일 동안의 취약성 통합 실행 상태가 표시됩니다. Qualys[qualys] 업데이트된 VI 수는 동일한 자산 내 고유 탐지 수를 나타냅니다. 그런 다음 VI가 새로운 감지로 업데이트됩니다.

> **주:**
> 취약성 통합 실행 횟수는 활성 상태로 설정된 통합에 대해서만 표시됩니다. 다음으로 이동 **Qualys** 취약성 통합 〉 관리 〉 기본 통합 을 클릭하고 상태를 활성으로 설정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

샘플 **Qualys** 통합 실행 상태 차트



- 임포트한 항목 열의 값은 통합 실행에서 생성된 총 기록 수를 나타냅니다.
- 새 항목 열에는 통합 실행에서 생성된 기록 수가 표시됩니다.
- 중복 항목 열이 더 이상 채워지지 않습니다. 표시에서 이 열을 제거하는 것이 좋습니다.
- 업데이트된 항목 열에는 통합 실행 중에 기록 이 업데이트된 횟수가 표시됩니다. 이 값은 업데이트되는 고유 기록 수가 아닙니다. 예를 들어 통합 실행 중에 기록 이 두 번 업데이트되면 두 번 계산되어 2 개의 업데이트된 항목으로 표시됩니다.
- 변경되지 않은 항목 열에는 데이터베이스에 이미 있지만 관련 필드 값이 변경되지 않았기 때문에 업데이트되지 않은 통합 실행 중에 발견된 기록 이 표시됩니다.

주:
통합은 다음 네 가지 값 모두에 대해 0개의 결과로 실행됩니다. 새 **CI,**기존 **CI,**새 항목 및 업데이트된 항목은**Qualys** 통합 실행 목록에서 필터링됩니다.

Qualys 통합 실행 상태 차트 보고서

이름	설명
지난 30일 Qualys 결과	각 통합에 대해 완료된 통합 실행 수입니다. 성공한 실행과 실패한 실행을 모두 표시합니다. 시각적 개체 막대에서 실행합니다.
지난 30일 Qualys 신규 VI	지난 30일 동안 임포트한 새 기록 수입니다. 정수로 표시됩니다.
지난 30일 Qualys 업데이트된 VI	지난 30일 동안 임포트한 업데이트된 기록 수입니다. 정수로 표시됩니다.
지난 30일 Qualys 중복	지난 30일 동안 임포트된 중복 기록 수입니다. 정수로 표시됩니다.
Qualys 통합 실행	통합 실행 기록이 목록에 표시됩니다.

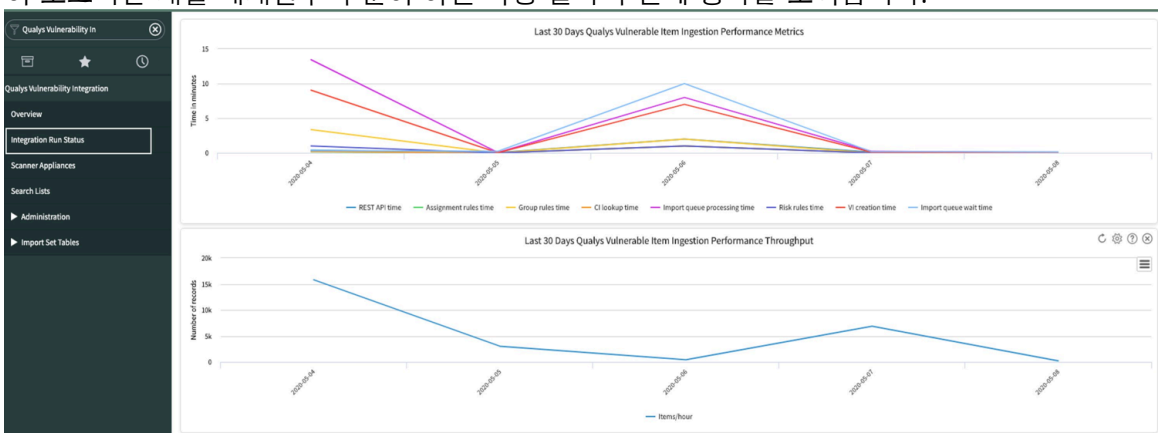
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Qualys 통합 실행 상태 차트 보고서

이름	설명
	주: **V16.1:** 이 통합에 대한 탐지를 확인하려면 탐지 또는 결과를 ServiceNow 테이블의 탐지 데이터와 *sn_vul_detection* 비교합니다. 통합이 진행되는 동안 탐지 또는 발견 개수가 변경될 수 있습니다. 이 보고서는 통합 실행이 완료된 후 인스턴스의 "종료 날짜 카운트" 열에 탐지 횟수를 표시합니다.
지난 30일 Qualys 취약한 항목 수집 성과 메트릭	지난 30일 동안과 비교하여 취약한 항목에 대한 일일 성과 메트릭입니다.
지난 30일 Qualys 취약한 항목 수집 성능 처리량	지난 30일 동안 호스트 탐지 통합에 대해 측정된 일일 취약한 항목 수집 처리량입니다 Qualys .

이 데이터를 처리하는 데 걸린 데이터 양 및 시간과 같은 여러 요인이 통합 실행의 성능에 영향을 줄 수 있습니다. 두 그래프는 성과 메트릭을 비교합니다.

- Qualys 취약한 항목 수집 성과 메트릭: 지난 30일 동안 취약한 항목에 대한 담당 규칙, 그룹 규칙, 위험 규칙, 큐 대기 시간, 큐 처리 시간 및 기타 통계에 대한 일일 성과 메트릭을 비교하여 성능 편차의 원인을 식별합니다. 성과는 각 활동에 소요된 시간을 기준으로 계산됩니다. 이러한 매개변수는 통합 실행 수준에서 계산되고 연결됩니다. 각 매개변수는 쉽게 식별할 수 있도록 색상으로 구분되어 있습니다.
- Qualys 취약한 항목 수집 성능 처리량: 호스트 탐지 통합에 Qualys 대한 일일 취약한 항목 수집 처리량을 비교합니다. 처리량은 시간당 항목 단위로 측정됩니다. 이 보고서는 개별 매개변수 수준이 아닌 특정 날짜의 전체 성과를 보여줍니다.



Qualys REST 메시지

Qualys REST 메시지는 준수 데이터를 가져오기 위해 Qualys API 를 호출하는 데 사용됩니다.

다음 REST 메시지는 기본 시스템과 함께 제공됩니다.

Qualys PC 정책 REST 메시지

Qualys PC 정책 REST 메시지는 Qualys에서 정책 데이터를 검색합니다. REST 메시지 메서드 기록에 대한 변경은 정책 정보를 검색하기 위해 Qualys에 대한 요청에 영향을 줍니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Qualys PC 정책 **REST** 메시지 매개변수

매개변수 이름	값	설명
작업	list	요청된 작업의 유형을 나타냅니다. 필수 매개변수입니다.
상세 정보	모두	검색된 정책에 대해 표시되는 상세 정보 수준을 나타냅니다. 요구 사항에 따라 수정하는 것이 안전합니다.

Qualys PC 통제 **REST** 메시지

Qualys PC 통제 REST 메시지는 Qualys에서 다른 통제 ID에 대한 준수 통제 정보를 검색합니다.

Qualys PC 통제 **REST** 메시지 매개변수

매개변수 이름	값	설명
작업	list	요청된 작업의 유형을 나타냅니다. 필수 매개변수입니다.
상세 정보	모두	검색된 컨트롤에 대해 표시되는 상세 정보 수준을 나타냅니다. 요구 사항에 따라 수정하는 것이 안전합니다.

Qualys PC 정책 상세 정보 **REST** 메시지

Qualys PC 정책 상세 정보 REST 메시지는 기술 및 섹션과 같은 전체 정책 상세 정보를 검색합니다.

Qualys PC 정책 세부사항 **REST** 메시지 매개변수

매개변수	값	설명
작업	list	요청 중인 작업의 유형을 나타냅니다. 필수 매개변수입니다.
show_user_controls	부울	• XML 출력에 UDC(사용자 정의 컨트롤)를 포함하려면 1로 설정합니다. • 지정하지 않으면 UDC가 포함되지 않습니다. 이는 선택적 매개변수입니다. 요구 사항에 따라 수정하는 것이 안전합니다.
show_appendix	부울	(선택 사항) XML 출력에 부록 섹션을 표시하려면 1로 설정합니다. 지정되지 않은 경우.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Qualys PC 결과 REST 메시지

Qualys PC 결과 REST 메시지는 Qualys에서 규정 준수 태세 기록을 검색합니다.

Qualys PC 결과 REST 메시지 매개변수

소스 필드	값	설명
작업	list	요청된 작업의 유형을 나타냅니다. 필수 매개변수입니다. 변경하지 않는 것이 좋습니다.
show_extended_evidence	부울	• 출력에 확장된 증거 정보를 표시하려면 1로 설정합니다. • 0으로 설정하거나 지정하지 않으면 확장된 증거 정보가 출력에 표시되지 않습니다. 주: • 동일한 요청에서 show_extended_evidence=1 을 hide_evidence=1로 지정할 수 없습니다. 이로 인해 오류가 발생합니다. 확장된 증거는 증거 데이터의 일부이며 증거 데이터가 표시될 때만 표시됩니다. • 이 매개변수는 기본 시스템과 함께 제공되지 않습니다.
cause_of_failure	부울	'1'을 통과하면 Qualys는 실패의 원인을 반환합니다. '0'을 전달하면 Qualys는 이러한 속성을 반환하지 않습니다. 주: 이 매개변수는 기본 시스템과 함께 제공되지 않습니다.
policy_id		지정된 정책에 대한 규정 준수 태세 정보 기록을 표시합니다. 유효한 정책 ID가 필요합니다.
상세 정보	모두	검색된 자세에 대해 표시되는 상세 정보 수준을 나타냅니다. 요구 사항에 따라 수정하는 것이 안전합니다.
show_remediation_info		(선택 사항) 정정 정보를 XML 또는 CSV 출력으로 표시하려면 1로 설정합니다. 기본적으로 출력에는 정정 정보가 포함되지 않습니다. 지정하지 않으면 정정 정보가 출력에 포함되지 않습니다.

Qualys PCRS 정책 호스트 통합 REST 메시지

Qualys PCRS 정책 호스트 통합은 Qualys에서 호스트 데이터를 검색하여 인스턴스에서 처리합니다.

Qualys PCRS 정책 호스트 통합 REST 메시지 매개변수

매개변수 이름	값	설명
policyId	${lastRunDatetime}	준수 평가를 위한 정책 ID입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Qualys PCRS 테스트 결과 통합

테이블에 전송되는 요청 매개변수가 표시됩니다.

Qualys PCRS 테스트 결과 통합 REST 메시지 매개변수

매개변수 이름	값	설명
evidenceRequired	${lastRunDatetime}	• 기본값은 0이며, 이는 호스트 상태에 대한 증거 데이터가 검색되지 않음을 나타냅니다. • 증거 데이터를 검색하려면 값을 1로 설정합니다. 주: 값을 1로 변경하면 상태 데이터를 가져오는 데 필요한 시간이 늘어납니다.
압축필수		• 기본값은 1이며, 출력이 압축됨을 나타냅니다. • 데이터가 압축되지 않도록 하려면 값을 0으로 설정합니다. 주: 데이터를 압축하지 않으면 상태 데이터를 가져오는 데 필요한 시간이 늘어납니다.

Tenable 취약성 통합 이해

Vulnerability Response Integration with Tenable Tenable 취약성 통합을 위해 엔지니어링에서 ServiceNow 개발한 애플리케이션은 , Tenable.sc및 Tenable.cs 제품에서 Tenable.io임포트한 데이터를 사용하여 자산의 취약성에 우선순위를 지정하고 정정하는 데 도움을 줍니다. 이 애플리케이션은 .ServiceNow# Store

주:
의 구성 준수v14.9부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v14.9 이전 용어	용어 v14.9 이상
테스트 결과 그룹	정정 작업
그룹 규칙	정정 작업 규칙
정책	테스트 그룹

Tenable 취약성 통합은 세 가지 Tenable 통합, Tenable.io및 Tenable.scTenable.cs를 사용하여 자산 및 취약성에 대한 외부 공급업체 스캐너 데이터를 임포트합니다. 애플리케이션은 Vulnerability Response Integration with Tenable 버전 5.13 Tenable.cs 이상의 제품과 버전 5.0.1 이상의 제품을 지원합니다Tenable.sc.

- Tenable.io 은 클라우드 기반 엔터프라이즈 통합입니다.
- Tenable.sc는 제품과 ServiceNow AI Platform 인스턴스가 동일한 환경에 있는 경우 Tenable.sc MID 서버를 사용하는 옵션을 제공하는 온 프레미스 통합입니다.

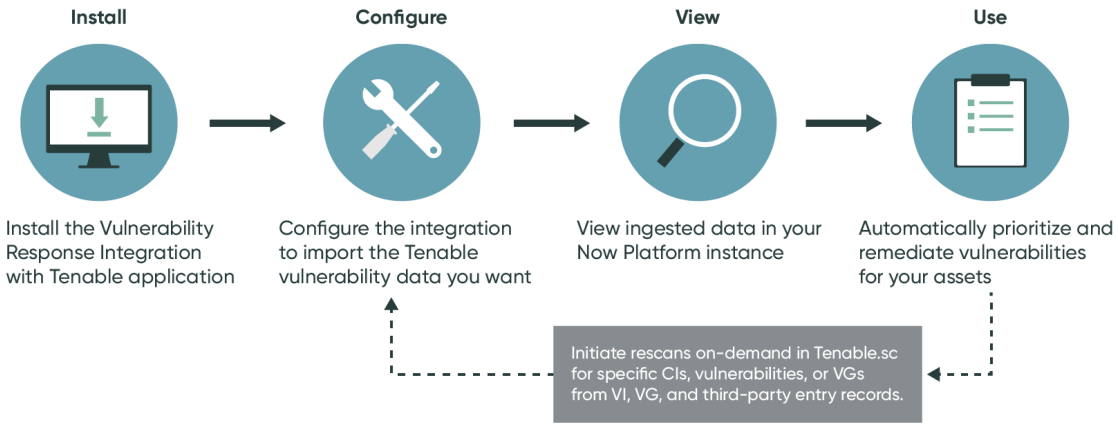
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- Tenable.sc 제품과 ServiceNow AI Platform 인스턴스가 동일한 환경에 있지 않은 경우 MID 서버를 사용해야 합니다.
- Tenable.cs 은 클라우드 기반 엔터프라이즈 통합입니다.

이 Vulnerability Response Integration with Tenable 애플리케이션은 별도의 ServiceNow Store 구독으로 사용할 수 있습니다.

의 통합 Tenable Vulnerability Integration목록 및 설명은 및 Tenable.sc 애플리케이션과의 취약성 대응 통합를 참조하십시오Tenable.io및 구성 준수 애플리케이션과의 취약성 대응 통합.

Tenable 취약성 통합



에 사용 가능한 버전 **Yokohama**

릴리스 버전	릴리스 정보
Vulnerability Response Integration with Tenable v3.13.1, v4.1, v5.0.1	호환성 정보는 KB0856498 Vulnerability Response 호환성 매트릭스 및 릴리스 스키마 변경을 참조하십시오.

통합의 용어 및 주요 기능

취약한 항목 및 취약성

취약한 항목은 다음과 같은 경우에 인스턴스에 ServiceNow AI Platform 생성됩니다.

- 외부 공급업체 스캐너에서 임포트한 취약성이 기존 자산(의 CMDB구성 항목)과 일치합니다. Tenable 제품에서는 이러한 일치 항목을 취약성이라고 합니다.
- 외부 공급업체 스캐너에서 임포트한 취약성이 의 CMDB기존 자산과 일치하지 않습니다. 이 경우 일치하지 않는 CI도 취약한 항목과 함께 생성됩니다.

  일치하지 않는 CI의 경우 기존 CI를 호스트와 일치시킬 수 없을 때 IRE(식별 및 조정 엔진)를 사용하여 두 개의 새 클래스에 CI를 만들 수도 있습니다. 그렇지 않으면 일치하지 않는 CI 클래스에 일치하지 않는 CI가 생성됩니다. 자세한 내용은 식별 및 조정 엔진을 사용하기 위한 취약성 대응 CI 생성 문서를 참조하십시오.

타사 취약성 항목 및 플러그인

외부 공급업체 취약성 항목은 외부 공급업체 스캐너에서 임포트되어 인스턴스의 외부 공급업체 취약성 항목 테이블에 ServiceNow AI Platform 나열됩니다. v24.0 부터

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약성 대응외부 공급업체 취약성 항목 테이블의 소프트웨어 열에 외부 공급업체 항목과 연결된 CPE(공통 플랫폼 열거형)가 채워집니다. Tenable의 외부 공급업체 취약성 항목은 해당 CMDB자산에 취약성 대응 수집되어 해당 목록에 나열된 기존 자산과 일치합니다. Tenable에서는 타사 취약성 항목을 플러그인이라고 합니다.

CI(구성 항목)

구성 항목은 에 나열된 기존 자산입니다.CMDB

검색된 항목

Tenable 자산 임포트에서 수집된 자산은 의 기존 구성 항목 CMDB과 일치합니다. 임포트한 자산이 업데이트됩니다.

일치하는 항목이 없으면 의 일치하지 않는 CI 클래스에 CMDBCI가 만들어집니다. CMDB CI Class Models 플러그인이 활성화되면 IRE(식별 및 조정 엔진)에서 새 클래스를 사용하여 CI를 만듭니다. 자세한 내용은 식별 및 조정 엔진을 사용하기 위한 취약성 대응 CI 생성 문서를 참조하십시오. 일치하지 않는 원래 CI가 재분류되면 검색된 항목 기록이 상태를 반영하도록 업데이트됩니다. 검색된 항목을 통해 자산을 식별하고 의 CI에 매핑하는 방법을 볼 수 있습니다 CMDB.

CI 조회 규칙

외부 공급업체 통합에서 데이터를 가져오면 Vulnerability Response는 자동으로 호스트(자산) 데이터를 사용하여 구성 관리 데이터베이스()CMDB에서 일치하는 항목을 검색합니다. CI 조회 규칙은 정정을 지원하기 위해 VIT가 생성될 때 CI를 식별하고 VI 기록에 추가하는 데 사용됩니다.

재스캔 및 정정 스캔

인스턴스의 취약한 항목, 정정 작업 및 외부 공급업체 취약성 항목 기록 ServiceNow AI Platform 에서 직접 특정 구성 항목, 정정 작업 또는 외부 공급업체 항목에 대해 대상 재스캔 명령을 시작할 수 있습니다. Tenable은 이 재스캔을 정정 검사라고 합니다.

이전 VI 자동 닫기

부실 취약한 항목 자동 종결 모듈을 ServiceNow AI Platform사용하면 외부 공급업체 통합에서 최근에 발견되지 않은 오래된 부실 VI(취약한 항목)를 정리할 수 있습니다. 이러한 VI를 종결 로 이동하면 활성 취약한 항목 및 정정 작업의 CMDB수를 줄이고 . 와의 Vulnerability Response Integration with Tenable 모든 통합을 사용하여 부실 VI를 자동으로 닫을 수 있습니다.

인스턴스

이 용어는 응용 프로그램의 고유한 발생 ServiceNow AI Platform# 을 나타냅니다.

통합

통합은 자산 통합 또는 플러그인 통합과 같은 통합에 대한 제품별 참조입니다 Tenable.ioTenable.sc . 이는 사용자 인스턴스의 Tenable 취약성 통합에 있는 특정 Tenable 제품에 속하는 별도의 통합입니다.

통합 인스턴스

이 용어는 및 Tenable.ioTenable.sc 제품별로 나열된 별도의 Tenable 통합을 나타냅니다.

배포

통합이 다중 소스를 지원하는 경우, 개별적인 단일 통합 존재를 통합의 배포라고 합니다. 이 용어는 환경 전반의 통합 및 제품을 참조하는 데 사용됩니다. 예를 들어, 사용자 환경에서 및 Tenable.sc 제품의 다양한 통합 Tenable.io 이 여러 개 배포되어 있을 수 있습니다.

, Tenable.sc및 Tenable.cs 통합에는 Tenable.io다음과 같은 주요 기능도 포함됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 구성 평가 결과, 즉 정책, 구성 테스트(통제) 및 권한이 부여된 소스가 있는 인용과 함께 테스트 결과를 제품과 함께 애플리케이션으로 구성 준수 임포트할 수 있습니다 Tenable.io . 이 통합이 애플리케이션과 작동하는 구성 준수 방식에 대한 자세한 내용은 을 참조하십시오.Tenable.io및 구성 준수 애플리케이션과의 취약성 대응 통합구성 준수 탐색
- 의 Tenable Vulnerability Integrationv2.1부터 동일한 IP 주소를 공유하는 환경의 자산에 대해 서로 다른 네트워크 파티션 식별자를 포함하는 고유한 CI(구성 항목)를 생성합니다. 환경 전반에서 고유한 자산을 식별하고 기존 검색된 항목, 취약한 항목 및 탐지 기록의 CI를 업데이트하여 취약성에 대한 자세한 정보를 제공합니다.
- 모든 Tenable.io및 Tenable.scTenable.cs 통합에 대해 작업을 실행할 시기를 예약할 수 있습니다. 요청 시 예약된 작업을 수동으로 실행할 수도 있습니다.
- 를 사용하여 Tenable.io자산 임포트의 경우 자산 태그를 활성화하여 환경에 나열된 CMDBTenable.io 자산을 구성하고 추적할 수 있습니다.
- Tenable.io및 Tenable.scTenable.cs 통합을 사용하면 CI 조회 규칙을 구성하여 외부 공급업체 소스의 자산 데이터를 사용하여 사용자의 에서 CI(구성 항목)를 식별하는 방법을 정의할 수 있습니다ServiceNow AI Platform CMDB.
- Tenable.io및 Tenable.scTenable.cs 통합을 사용하면 취약성 임포트에 대한 임포트 필터를 설정하여 Tenable에서 원하는 취약성만 임포트할 수 있습니다. 의 경우 Tenable.io취약성 가져오기를 통해 Tenable에서 수정된 취약성을 임포트할 수 있는 옵션이 있습니다.
- 의 경우 Tenable.sc인스턴스의 취약한 항목, 정정 작업 및 외부 공급업체 항목 기록에서 직접 요청 시 재스캔을 시작할 수 있는 ServiceNow AI Platform 옵션이 있습니다. VI가 종결/고정으로 전환되었지만 인스턴스에서 아직 업데이트되지 않은 경우 특정 구성 항목의 취약성이 정정되었는지 확인할 수 있습니다. 통합에 대한 Tenable.sc 재스캔 시작 문서를 참조하십시오.

다음 섹션에는 Tenable 통합에 대한 자세한 내용이 나열되어 있습니다.

필요한 **ServiceNow AI Platform** 역할

통합 작업에는 인스턴스에서 다음 역할이 ServiceNow AI Platform 필요합니다.

관리자

시스템 관리자는 설정 도우미를 Vulnerability Response Integration with Tenable 사용하여 애플리케이션을 설치합니다. 할당되지 않은 경우 관리자는 취약성 관리자(sn_vul.vulnerability_admin) 및 설정 도우미의 다른 역할을 할당합니다.

sn_vul.vulnerability_admin

할당된 취약성 관리자는 설정 도우미에서 Tenable 통합의 구성을 완료합니다. 이 역할은 (VR) 애플리케이션 및 해당 기록에 대한 취약성 대응 전체 액세스 권한을 보유합니다. 취약성 관리자는 설치된 외부 공급업체 통합에 대해 모든 VR 애플리케이션과 규칙을 구성합니다.

sn_vul_tenable.configure_integration

이 역할에는 sn_vul_tenable.read_integration 세분화된 역할이 포함되어 있으며 이 역할을 가진 사용자는 애플리케이션을 구성할 Vulnerability Response Integration with Tenable 수 있습니다.

sn_vul_tenable.read_integration

이 역할을 가진 사용자는 애플리케이션의 기록을 Vulnerability Response Integration with Tenable 보고(읽음) 편집할 수 있지만 편집할 수는 없습니다.

취약성 대응 그룹

기본적으로 취약성 대응 그룹은 설정 도우미에서 사용할 수 있습니다. 취약성 대응 그룹에 할당된 사용자는 sn_vul.read_all 및 sn_vul.remediation_owner 역할을 자동으로 상속합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약한 항목

취약한 항목은 정정 작업 규칙에 따라 정정 작업으로 그룹화되고 할당 규칙에 따라 정정을 위해 할당됩니다. 자세한 내용은 취약성 대응 정정 작업 및 정정 작업 규칙 개요 및 취약성 대응 할당 규칙 개요 문서를 참조하십시오.

CI(구성 항목) 조회 규칙

CI 조회 규칙은 CI를 식별하고 취약한 항목에 추가할 시기를 결정합니다. CI 조회 규칙의 작동 방식에 대한 자세한 내용은 다음 문서를 참조하십시오 외부 공급업체 취약성 통합에서 취약성 대응 구성 항목을 식별하기 위한 CI 조회 규칙.

주:
제거된 규칙은 복구할 수 없습니다. 기존 규칙을 제거하는 대신 규칙을 만들 때 사용하지 않도록 설정하십시오.

다음 Tenable.io 조회 규칙은 기본 시스템과 함께 제공됩니다.

- MAC_ADDRESS
- FQDN
- NetBIOS
- 호스트 이름
- DNS
- IP

주:
Tenable.io CI 조회 규칙은 검색된 항목의 일반 FDQN, IPV4 및 MacAddress 값보다 비어 있지 않은 네트워크 인터페이스 값(FDQN, IPV4 및 MacAddress)의 우선순위를 정하고 채웁니다. 이러한 네트워크 인터페이스 값이 비어 있으면 검색된 항목에 대해 일반 FDQN, IPV4 및 MacAddress 값이 채워집니다.

다음 Tenable.sc 조회 규칙은 기본 시스템과 함께 제공됩니다.

- MAC_ADDRESS
- FQDN
- NetBIOS
- IP

주:
자산에 대해 ip_address, mac_address, fqdns 및 network_interfaces에 대한 여러 값이 사용됩니다. 모든 값은 일치를 위한 CI 조회 규칙에서 고려됩니다. 모든 값은 IRE를 사용하여 여러 네트워크 어댑터를 만드는 데 사용됩니다.

조회 규칙 클라우드 자원 ID는 Tenable.cs 기본 시스템과 함께 제공됩니다.

일치하지 않는 클라우드 자원의 분류를 기본 CI 클래스로 구성하는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 일치하지 않는 클라우드 자산에 대한 CI 클래스 업데이트 중.

IP 주소를 무시하는 새 속성

CI 조회 규칙의 일부로 여러 IP 주소나 여러 Mac 주소를 무시하려는 경우 에는 Tenable.io두 가지 속성을 사용할 수 있습니다.

ignoreIPAddress

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

CI 조회 및 CI 생성시 무시되는 IP 주소 목록입니다.

ignoreMacAddress

CI 조회 또는 CI 작성에서 무시할 MAC 주소 목록입니다.

검색된 항목

이 모듈에는 Tenable 취약한 항목 통합 및 Tenable 자산 통합에서 임포트하는 동안 탐지된 구성 항목이 나열됩니다.

주:
이 목록의 기본 필터는 #### ##으로 설정됩니다. 필터를 제거하여 임포트에서 검색된 모든 항목을 볼 수 있습니다.

검색된 항목 모듈에 대한 자세한 내용은 다음 문서를 참조하십시오 검색된 항목.

자산 태그

자산 태그(호스트 태그라고도 함)는 조직의 자산을 구성하고 추적하는 데 사용됩니다. 자산에 태그를 할당할 수 있습니다. 그런 다음 스캔을 시작할 때 스캔하려는 자산과 연결된 태그를 선택할 수 있습니다. 자산 태그 모듈을 사용하면 일정에 따라 인스턴스에서 인스턴스로 Tenable.io 자산 태그 데이터를 다운로드할 수 있습니다. 자산 태그를 포함하는 자산 데이터는 Tenable.io 자산 변환 통합 변환 맵을 사용하여 가져와서 Tenable.io 변환합니다.

모든 자산 태그는 자산 통합의 Tenable.io 일부로 임포트됩니다. 자산 태그는 담당 규칙 및 정정 작업 규칙의 취약성 대응 필터링에 사용됩니다. 검색된 항목 양식에 태그가 표시됩니다.

주:
Tenable.io 취약한 항목을 임포트 및 그룹화하기 전에 해당 규칙에 모든 태그를 사용할 수 있도록 애플리케이션에서 담당 규칙 또는 정정 작업 규칙을 취약성 대응 생성하기 취약성 대응 전에 자산 통합을 실행합니다. 태그에 대한 다음 사항도 참고하십시오.

- 태그 스토리지는 대/소문자를 구분하지 않습니다. 예를 들어 San Diego 위치의 자산을 설명하는 태그를 만들고 San Diego 태그를 만드는 경우 SAN DIEGO 태그를 생성하여 자산 태그 테이블에 저장할 수도 없습니다. San Diego 와 SAN DIEGO 는 시스템에서 동일한 자산 태그로 간주됩니다. 어떤 태그가 먼저 임포트되든 그 태그가 저장되고 인식됩니다.
- 정정 작업 규칙에서 자산 태그를 그룹 키로 사용하면 예기치 않은 결과가 발생할 수 있습니다. 자산 태그는 조건 작성기에서만 사용할 수 있습니다.
- 자산 태그는 전역 시스템 속성 sn_vul.import_asset_tags에 의해 제어됩니다. 이 속성은 기본적으로 true 로 설정됩니다. 태그를 비활성화하면 모든 ServiceNow AI Platform# 인스턴스에서 비활성화됩니다.

데이터 검색 필터

데이터 검색 설정은 Tenable 애플리케이션에서 인스턴스로 ServiceNow AI Platform# 임포트할 데이터의 유형과 범위를 구체적으로 결정하는 데 도움이 됩니다. 가장 일반적으로 사용되는 설정 목록은 문서를 참조하십시오 Tenable 취약성 통합에 대한 데이터 검색 설정.

취약성 우선순위 등급(VPR)

VPR(취약성 우선순위 등급)은 에서 임포트되어 새 기본 위험 계산기 취약성 대응와 함께 사용되는 Tenable 제품의 속성입니다. Tenable 위험 규칙은 의 취약성 계산기취약성 대응에 기본 위험 계산기의 일부로 애플리케이션과 함께 Vulnerability Response Integration with Tenable 설치됩니다.

이 위험 규칙은 기본적으로 비활성 상태입니다.

Tenable 위험 계산기 규칙을 사용하면 임포트한 VPR 값이 취약한 항목의 위험 점수를 계산하는 데 사용됩니다. 이 위험 계산기의 기본 가중치 분포는 VPR = 70%, 자산=15%, 비즈니스 중요도

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

=15%입니다. 이 Tenable 위험 계산기 규칙을 사용하도록 설정하면 데이터 수집 성능에 영향을 줄 수 있습니다. 계산기 및 Tenable 위험 계산기 규칙에 대한 취약성 대응 자세한 내용은 문서를 참조하십시오 취약성 대응 계산기 및 취약성 계산기 규칙.

설치 및 구성

에서 ServiceNow# Store다운로드한 Vulnerability Response Integration with Tenable 후 의 설치 및 구성은 의 설정 도우미취약성 대응에서 지원됩니다. 자세한 내용은 설정 지원을 사용하여 구성 취약성 대응 하기 문서를 참조하십시오.

Tenable.io및 구성 준수 애플리케이션과의 취약성 대응 통합

Tenable.io 애플리케이션의 통합 Vulnerability Response Integration with Tenable 은 및 구성 준수 애플리케이션에서 사용할 수 취약성 대응 있습니다.

Tenable.io 통합 목록

모든 Tenable.io 및 Tenable.sc 통합에 대해 다중 소스가 지원됩니다. 의 취약성 대응설정 도우미에서 환경 전체에 다음 통합의 여러 인스턴스를 추가하고 배포할 수 있습니다. 또한 설정 도우미에서 애플리케이션을 설치하고 구성합니다 Vulnerability Response Integration with Tenable .

Tenable.io 은 클라우드 기반 엔터프라이즈 통합입니다. 제품에 대해 Tenable.io 지원되는 통합의 이름과 설명은 다음 표를 참조하십시오.

Tenable.io 규정 준수 결과 통합과 Tenable.io 규정 준수 결과 백필 통합은 기본적으로 비활성 상태입니다.

활성화하려면 다음을 수행합니다.

1. 다음으로 이동 **Tenable** 취약성 통합 〉 관리 〉 통합.
2. Tenable 통합 목록에서 통합 이름을 클릭하여 기록을 열고 활성 확인란을 선택하여 활성화합니다. 이러한 통합을 시작하려면 일정 설정을 기본값으로 두는 것이 좋습니다.

Tenable.io 통합

통합	설명
Tenable.io 자산 통합	• 제품에서 Tenable.io 자산 태그를 포함한 모든 자산 데이터를 검색하고 인스턴스에서 처리합니다. • v3.0부터 준수 결과 통합이 Tenable.io 활성화된 경우 임포트한 자산 데이터와 함께 보안 구성 평가 데이터를 임포트할 수 있습니다. 이 데이터는 자산의 구성 관련 취약성을 식별하고 대응하는 데 도움이 될 수 있습니다. • 일치하지 않는 자산에 대해 고유한 CI를 생성하거나 동일한 IP 주소를 공유하는 환경 전체의 자산에 대한 네트워크 파티션 식별자 속성으로 기존 CI를 업데이트합니다. • 자산 API에 대한 REST 메시지 호출을 조정합니다. • 이 통합의 출력은 검색된 항목입니다. • 데이터는 청크로 임포트되어 [sn_vul_tenable_chunk_status] 테이블에 저장됩니다. 테이블 클리너는 30일 후에 이 테이블에서 저장된 데이터를 자동으로 제거합니다. • v2.2부터는 *Last Scan Time* 취약성이 있는 자산에 대해서만 임포트 및 업데이트됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Tenable.io 통합

통합	설명
Tenable.io 준수 결과 통합	• v3.0부터 준수 결과 통합에서 임포트한 보안 구성 평가 데이터와 자산 통합에서 임포트한 데이터를 통해 자산의 구성 관련 취약성을 식별하고 대응할 수 있습니다. • 사용하도록 설정하면 높은 수준의 보안 구성 평가 데이터를 검색하고 인스턴스에서 ServiceNow AI Platform 처리합니다. 임포트된 데이터에는 정책, 구성 테스트(통제) 및 권한이 부여된 소스의 인용과 함께 테스트 결과가 포함됩니다. • 누락된 자산 또는 자산 ID가 없는 자산에 대한 평가 데이터는 임포트되지 않습니다. • 테스트 결과를 임포트하고 해당 자산을 인스턴스에서 일치시킬 수 없는 경우, 테스트 결과가 무시되고 누락된 자산의 ID가 [sn_vul_tenable_missing_asset] 테이블의 임시 기록에 저장됩니다. • 무시된(누락된) 자산의 총 값은 이 통합에 대한 통합 실행 기록의 구성 탭에 있는 무시된 **CI** 필드에 나열됩니다.
Tenable.io 준수 결과 백필 통합	• 활성화되면 자산 통합이 체인 통합 실행의 일부로 성공적으로 완료된 후 이 통합이 자동으로 실행됩니다. 이 통합은 구성 평가 데이터를 [sn_vul_tenable_missing_asset] 테이블에 나열된 누락된 자산과 일치시킵니다. • 자산 통합 임포트가 성공적으로 완료된 후 인스턴스에 발견되거나 존재하는 누락된 자산에 대해 최대 200개의 자산 ID를 임포트합니다. • 자산을 해당 구성 평가 데이터와 일치시킬 수 있는 경우 [sn_vul_tenable_missing_asset] 테이블에서 임시 기록을 제거합니다.
Tenable.io 스캔 자격 증명 통합	• 이 통합은 에서 구성된 검사 자격 증명을 검색합니다.Tenable.io • 자격 증명 API에 대한 REST 메시지 호출을 조정합니다. • 이 통합의 출력은 [sn_vul_tenable_scan_credential] 테이블에 채워진 검사 자격 증명입니다. • 임포트한 자격 증명은 스캔 요청이 에서 시작될 ServiceNow AI Platform때 스캐너에 액세스하는 데 사용됩니다. • 이 통합은 매주 실행되도록 예약되어 있습니다.
Tenable.io 템플릿 통합	다시 스캔하는 동안 템플릿 레코드가 전송됩니다 Tenable.io . 이 통합은 다시 스캔에 사용할 수 있는 Tenable.io 자격 증명을 검색합니다. 자격 증명은 인스턴스에 따라 다르며, 단일 템플릿 기록을 임포트하여 [sn_vul_tenable_io_template] 테이블에 임시로 안전하게 저장합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Tenable.io 통합

통합	설명
Tenable.io 플러그인 통합	• 제품에서 Tenable.io 플러그인 데이터를 검색합니다. 검색된 데이터는 통합 실행에 의해 플러그인이 마지막으로 업데이트된 날짜를 기준으로 합니다 Tenable.io . • 이렇게 임포트하면 식별자(ID 10개)가 Tenable.io 최신 상태가 됩니다. • 플러그인 API에 대한 REST 메시지 호출을 조정합니다. • 이 통합의 출력은 외부 공급업체 취약성입니다.
Tenable.io 수정된 취약성 통합	• 제품의 심각도 필터를 Tenable.io 기반으로 취약성 데이터를 검색하고 인스턴스에서 처리합니다. 취약한 항목은 오픈 됨 및 다시 열림 상태의 탐지 기록에 대해 생성됩니다. 이러한 기록에는 정정이 필요하기 때문입니다. 탐지가 고정된 경우 기존의 취약한 항목이 Vulnerability Response에 의해 업데이트되지만, Tenable은 완화된 취약성 수정을 고려하기 때문에 기본적으로 고정 탐지에 대한 취약한 항목은 생성되지 않습니다. • 설정 도우미에서 고정 취약성 탐지에 대한 취약 시간 생성 플래그가 활성화되면 새 VI가 고정 상태로 생성되므로 이를 생성한 탐지에 대한 가시성을 확보할 수 있습니다. VI는 인스턴스에 아직 존재하지 않는 고정 탐지를 위해 생성되므로 임포트 성능에 부정적인 영향을 미칠 수 있습니다. 고정 탐지가 기존의 취약한 항목의 상태만 업데이트하도록 이 기능을 비활성화된 상태로 두는 것을 선호할 수 있습니다. • 일치하지 않는 자산에 대해 고유한 CI를 생성하거나 동일한 IP 주소를 공유하는 환경 전체의 자산에 대한 네트워크 파티션 식별자 속성으로 기존 CI를 업데이트합니다. • 취약성 API에 대한 REST 메시지 호출을 조정합니다. • 이 통합의 출력은 종결/고정 취약 항목(VI)입니다. 또한 자산 및 외부 공급업체 항목이 없는 경우 이를 생성합니다. • 데이터는 청크로 임포트되어 [sn_vul_tenable_chunk_status] 테이블에 저장됩니다. 테이블 클리너는 30일 후에 이 테이블에서 저장된 데이터를 자동으로 제거합니다. 이 통합 실행은 예약되어 있습니다. 이는 실행이 성공적으로 완료된 후 아래에 설명된 미해결 취약성 통합이 트리거되는 체인 통합입니다. Tenable v3.3부터 취약성 통합 실행에 대한 다음 정보를 볼 수 있습니다. • 총 청크: Tenable에서 생성되는 총 청크 수 • 사용 가능한 청크: 에 대해 다운로드할 수 있는 청크 수 ServiceNow

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Tenable.io 통합

통합	설명
Tenable.io 미해결 취약성 통합	• 이 통합은 수정된 취약성 통합이 성공적으로 완료되면 트리거됩니다 Tenable.io . • 제품의 심각도 필터를 Tenable.io 기반으로 취약성 데이터를 검색하고 인스턴스에서 처리합니다. • 일치하지 않는 자산에 대해 고유한 CI를 생성하거나 동일한 IP 주소를 공유하는 환경 전체의 자산에 대한 네트워크 파티션 식별자 속성으로 기존 CI를 업데이트합니다. • 취약성 API에 대한 REST 메시지 호출을 조정합니다. • 이 통합의 출력은 신규/재오픈 된 취약한 항목(VI)입니다. 또한 구성 항목 및 외부 공급업체 항목이 없는 경우 이를 생성합니다. Tenable은 활성 취약성을 누적 (현재)으로 간주합니다. • 데이터는 청크로 임포트되어 [sn_vul_tenable_chunk_status] 테이블에 저장됩니다. 테이블 클리너는 30일 후에 이 테이블에서 저장된 데이터를 자동으로 제거합니다. Tenable v3.3부터 취약성 통합 실행에 대한 다음 정보를 볼 수 있습니다. • 총 청크: Tenable에서 생성되는 총 청크 수 • 사용 가능한 청크: 에 대해 다운로드할 수 있는 청크 수 ServiceNow
Tenable.io/scan 메타데이터 통합	이 통합은 /scans 엔드포인트에서 메타데이터를 검색합니다. 의 Tenable.io기존 자산 데이터에서 last_schedule_id 기반으로 스캔 정보를 끌어옵니다. 에서 Tenable.io /scans 엔드포인트를 통합하려면 다음 구현 단계를 수행해야 합니다. • 테이블 생성: /scans 엔드포인트에서 Tenable.io검색된 스캔 메타데이터를 저장하기 위해 새 사용자 지정 테이블 **sn_vul_tenable_scan**이 생성됩니다. 여기에는 스캔 ID, 이름, 상태, 시작 시간, 종료 시간 및 스캔 유형과 같은 상세 정보가 포함됩니다. • 데이터 연결: 검색된 항목(구성 항목 또는 취약성)과 **sn_vul_tenable_scan** 테이블의 해당 최신 검사 기록 사이에 참조 필드가 설정됩니다. 이 연결을 통해 다음을 수행할 수 있습니다. ○ 검색된 각 항목과 관련된 최근의 스캔 정보를 봅니다. ○ 취약성 분류 및 정정 결정을 위한 컨텍스트를 개선합니다. ○ 스캔 활동의 이력 기록을 유지관리하여 감사 가능성과 보고 기능을 향상시킵니다.

Tenable.sc 애플리케이션과의 취약성 대응 통합

Tenable.sc 애플리케이션의 통합 Vulnerability Response Integration with Tenable

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약성 대응 v20.0부터 에이전트가 자산을 스캔하면 검색된 항목 목록의 "에이전트가 존재함" 열에 값이 "true"로 표시됩니다. 이는 스캔이 진짜임을 나타냅니다.

Tenable.sc 통합 목록

모든 Tenable.io 및 Tenable.sc 통합에 대해 다중 소스가 지원됩니다. 의 취약성 대응설정 도우미에서 환경 전체에 다음 통합의 여러 인스턴스를 추가하고 배포할 수 있습니다. 설정 도우미에서 Vulnerability Response Integration with Tenable 애플리케이션을 설치하고 구성할 수도 있습니다.

- Tenable.sc는 제품과 ServiceNow AI Platform 인스턴스가 동일한 환경에 있는 경우 Tenable.sc MID 서버를 사용하는 옵션을 제공하는 온 프레미스 통합입니다.
- Tenable.sc 제품과 ServiceNow AI Platform 인스턴스가 동일한 환경에 있지 않은 경우 MID 서버를 사용해야 합니다.

Tenable.sc 통합

통합	설명
Tenable.sc 자산 통합	임포트한 자산 데이터로 검색된 항목이 중복되지 않도록 하기 위해 제품의 자산 통합 Tenable.sc 은 두 가지 통합으로 구성됩니다. Tenable.sc Open Assets 통합 이 통합은 Tenable이 누적 (현재) 또는 오픈으로 간주하는 자산에 대한 취약성 데이터를 임포트합니다. 임포트한 이 자산 데이터로 인스턴스에 생성된 취약한 항목(VI)은 열림(열림) 상태인 것으로 간주됩니다. 이러한 취약한 항목은 조사가 필요하며 수정이 필요할 수 있습니다. 고정 Tenable.sc 자산 통합 이 통합은 Tenable이 완화됨 (더 이상 취약하지 않음) 또는 수정됨으로 간주하는 자산에 대한 취약성 데이터를 임포트합니다. 이러한 자산의 취약한 항목은 검사 결과 더 이상 취약하지 않은 것으로 나타나기 때문에 인스턴스에서 열림 상태에서 종결/고정 상태로 전환됩니다. • 제품에서 Tenable.sc 모든 자산 데이터를 검색하여 인스턴스에서 처리합니다. • 일치하지 않는 자산에 대해 고유한 CI를 생성하거나 IP 주소를 공유하는 환경 전체의 자산에 대한 네트워크 파티션 식별자 속성으로 기존 CI를 업데이트합니다. • 자산 API에 대한 REST 메시지 호출을 조정합니다. • 이 통합의 출력은 검색된 항목입니다. • 설정 도우미에서 선택하는 Tenable 쿼리 필터는 자산 통합에도 Tenable.sc 적용됩니다. 쿼리 필터의 조건과 일치하는 취약성이 있는 자산만 임포트됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Tenable.sc 통합

통합	설명
Tenable.sc 플러그인 통합	• 제품에서 Tenable.sc 플러그인 데이터를 검색합니다. 검색된 데이터는 통합 실행에 의해 플러그인이 마지막으로 업데이트된 날짜를 기준으로 합니다 Tenable.sc . • 이렇게 임포트하면 식별자(ID 10개)가 Tenable.sc 최신 상태로 유지되고 활성 상태인 취약성만 임포트됩니다. • 플러그인 API에 대한 REST 메시지 호출을 조정합니다. • 이 통합의 출력은 외부 공급업체 취약성입니다.
Tenable.sc 수정된 취약성 통합	• 제품의 심각도 필터를 Tenable.sc 기반으로 취약성 데이터를 검색하고 인스턴스에서 처리합니다. 취약한 항목은 오픈 됨 및 다시 열림 상태의 탐지 기록에 대해 생성됩니다. 이러한 기록에는 정정이 필요하기 때문입니다. 탐지가 고정된 경우 기존 취약한 항목이 취약성 대응에 의해 업데이트되지만, Tenable은 완화된취약성 수정을 고려하기 때문에 기본적으로 고정 탐지에 대해 취약한 항목이 생성되지 않습니다. • 설정 도우미에서 고정 취약성 탐지에 대한 취약 시간 생성 플래그가 활성화되면 **VI** 를 생성한 탐지를 볼 수 있도록 고정 상태의 VI를 생성합니다. VI는 인스턴스에 존재하지 않는 고정 탐지를 위해 생성되므로 임포트 성능에 부정적인 영향을 미칠 수 있습니다. 고정 탐지가 기존의 취약한 항목의 상태만 업데이트하도록 이 기능을 비활성화된 상태로 두는 것을 선호할 수 있습니다. • 일치하지 않는 자산에 대해 고유한 CI를 생성하거나 IP 주소를 공유하는 환경 전체의 자산에 대한 네트워크 파티션 식별자 속성으로 기존 CI를 업데이트합니다. • 취약성 API에 대한 REST 메시지 호출을 조정합니다. 이 통합의 출력은 종결/고정 취약 항목(VI)입니다. 또한 자산 및 외부 공급업체 항목이 없는 경우 이를 생성합니다. 이 통합 실행은 예약된 실행입니다. 이는 실행이 성공적으로 완료된 Tenable.sc 후 다음에 설명된 미해결 취약성 통합이 트리거됨을 의미하는 체인 통합입니다. 주: 기본적으로 제품군 ID 0과 39는 이 통합에서 제외됩니다.
Tenable.sc 미해결 취약성 통합	• 이 통합은 고정된 취약성 통합이 성공적으로 완료될 때 트리거됩니다 Tenable.sc . • 제품에서 Tenable.sc 선택한 쿼리 필터를 기반으로 취약성 데이터를 검색하고 인스턴스에서 처리합니다. • 활성 취약성에 해당하는 취약한 항목을 생성합니다. • 일치하지 않는 자산에 대해 고유한 CI를 생성하거나 IP 주소를 공유하는 환경 전체의 자산에 대한 네트워크 파티션 식별자 속성으로 기존 CI를 업데이트합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Tenable.sc 통합

통합	설명
	• 취약성 API에 대한 REST 메시지 호출을 조정합니다. • 이 통합의 출력은 새로운 취약한 항목(VI)이 없는 경우 업데이트/생성 입니다. 또한 구성 항목 및 외부 공급업체 항목이 없는 경우 이를 생성합니다. 주: 기본적으로 제품군 ID 0과 39는 이 통합에서 제외됩니다.
Tenable.sc 스캔 자격 증명 통합	• 이 통합은 에서 구성된 검사 자격 증명을 검색합니다.Tenable.sc • 자격 증명 API에 대한 REST 메시지 호출을 조정합니다. • 이 통합의 출력은 테이블 〔sn_vul_tenable_scan_credential〕에 채워진 검사 자격 증명입니다. • 임포트한 자격 증명은 스캔 요청이 에서 시작될 ServiceNow AI Platform때 스캐너에 액세스하는 데 사용됩니다. • 이 통합은 매주 실행되도록 예약되어 있습니다.
Tenable.sc 취약성 통합 백필	• 이 채우기 통합은 임포트 중에 누락되었을 수 있는 미해결 취약성과 수정된 취약성을 임포트합니다. • 이 통합은 지난 7일 동안의 미해결된 취약성과 수정된 취약성을 모두 임포트하여 탐지 및 취약한 항목을 업데이트합니다. • 이 통합은 성능에 영향을 줄 수 있습니다. • 이 통합은 기본적으로 비활성 상태입니다. • 취약성 데이터를 업데이트하고 잠재적인 성능 문제를 방지하려면 실행 중인 다른 검사가 없을 때 실행되도록 Tenable.sc 수정된 취약성 및 미해결 취약성 통합을 예약하는 것이 좋습니다. • 이 통합의 출력은 다음과 같습니다. ○ 종결/고정 취약 항목(VI). 또한 자산 및 외부 공급업체 항목이 없는 경우 이를 생성합니다. ○ 취약한 항목(VI)이 없는 경우 업데이트/생성할 수 있습니다. 또한 구성 항목 및 외부 공급업체 항목이 없는 경우 이를 생성합니다.

사용자 인증 및 **Tenable.sc**

사용자 인증은 인스턴스 ServiceNow AI Platform# 와 제품의 버전 5.13 Tenable.sc 에서 지원됩니다. 버전 5.12 및 이전 버전의 제품을 사용하는 경우 사용자 인증이 Tenable.sc 필요합니다.

통합에 Tenable.sc 대한 사용자 인증을 선택하면 통합 실행 중에 토큰이 만료되고 대체될 수 있습니다. 취약성 통합 실행 기록(VIN)의 메모 열에 토큰이 만료될 때 프로세스에 대해 다음 메시지가 표시됩니다. ##: ## ### ### ######. 이 메시지가 표시되는 경우 아무 작업도 필요하지

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

않습니다. 만료된 토큰은 백그라운드에서 자동으로 새로 고쳐지며 메시지는 통합 프로세스의 일시 중지나 오류를 나타내지 않습니다.

Tenable.cs및 컨테이너 취약성 대응 애플리케이션과의 취약성 대응 통합

Tenable.cs 애플리케이션의 통합 Vulnerability Response Integration with Tenable 은 취약성 대응 및 컨테이너 취약성 대응 애플리케이션에서 사용할 수 있습니다.

v20.0 취약성 대응부터 에이전트가 자산을 스캔하면 검색된 항목 목록의 "에이전트가 존재함" 열에 "true"가 표시되어 스캔이 진짜임을 나타냅니다.

Tenable.cs 통합 목록

모든 Tenable.io, Tenable.sc, 통합 Tenable.cs 에 대해 다중 소스가 지원됩니다. 의 취약성 대응설정 도우미에서 환경 전체에 다음 통합의 여러 인스턴스를 추가하고 배포할 수 있습니다. 설정 도우미에서 Vulnerability Response Integration with Tenable 애플리케이션을 설치하고 구성할 수도 있습니다.

Tenable.cs 은 클라우드 기반 엔터프라이즈 통합입니다. 제품에 대해 Tenable.cs 지원되는 통합의 이름과 설명은 다음 표를 참조하십시오.

Tenable.cs 통합

통합	설명
Tenable.cs 클라우드 컨테이너 자산 통합	• 제품에서 Tenable.cs 모든 컨테이너 자산 데이터를 검색하여 인스턴스에서 처리합니다. • 일치하지 않는 자산에 대해 고유한 CI를 만들거나 기존 CI를 업데이트합니다. 자산 API에 대한 REST 메시지 호출을 조정합니다. 이 통합의 출력은 검색된 컨테이너 이미지, Docker 이미지 및 컨테이너 리포지토리입니다.
Tenable.cs 클라우드 컨테이너 취약성 통합 열기	활성화되면 컨테이너 자산 통합이 체인 통합 실행의 일부로 성공적으로 완료된 후 이 통합이 자동으로 실행됩니다. • 제품의 심각도 필터를 Tenable.cs 기반으로 컨테이너 취약성 데이터를 검색하고 인스턴스에서 처리합니다. • 일치하지 않는 자산에 대해 고유한 CI를 만들거나 기존 CI를 업데이트합니다. • 취약성 API에 대한 REST 메시지 호출을 조정합니다. 이 통합의 출력은 신규/재개시됨컨테이너 CVI(취약한 항목)입니다. 없는 경우 검색된 컨테이너 이미지, Docker 이미지, 컨테이너 리포지토리, 이미지 결과, 타사 항목 및 CVE(Common Vulnerabilities and Exposures)도 생성합니다.
Tenable.cs 클라우드 컨테이너 취약성 통합 수정	이 통합은 Open Cloud Container 취약성 통합이 Tenable.cs 성공적으로 완료될 때 트리거됩니다. • 제품의 심각도 필터를 Tenable.cs 기반으로 컨테이너 취약성 데이터를 검색하고 인스턴스에서 처리합니다. • 일치하지 않는 자산에 대한 고유 CI를 작성하거나 기존 CI를 업데이트합니다 • 취약성 API에 대한 REST 메시지 호출을 조정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Tenable.cs 통합

통합	설명
	이 통합의 출력은 신규/재오픈된 컨테이너 취약 항목(CVI)입니다. 없는 경우 컨테이너 이미지 검색, Docker 이미지, 컨테이너 리포지토리, 이미지 결과, 타사 항목 및 CVE도 생성합니다. 이미지 찾기가 종결 상태로 생성됩니다.
Tenable.cs 클라우드 호스트 취약성 통합 열기	• 제품의 심각도 필터를 Tenable.cs 기반으로 취약성 데이터를 검색하고 인스턴스에서 처리합니다. • 일치하지 않는 자산에 대해 고유한 CI를 만들거나 기존 CI를 업데이트합니다. • 취약성 API에 대한 REST 메시지 호출을 조정합니다. 이 통합의 출력은 신규/재오픈된 취약한 항목(VI)입니다. 없는 경우에는 구성 항목, 타사 항목 및 CVE도 생성됩니다. 취약성 탐지는 오픈 상태로 생성됩니다.
Tenable.cs 클라우드 호스트 취약성 통합 수정	이 통합은 오픈 클라우드 호스트 취약성 통합이 Tenable.cs 성공적으로 완료될 때 트리거됩니다. • 제품의 심각도 필터를 Tenable.cs 기반으로 취약성 데이터를 검색하고 인스턴스에서 처리합니다. • 일치하지 않는 자산에 대해 고유한 CI를 만들거나 기존 CI를 업데이트합니다. • 취약성 API에 대한 REST 메시지 호출을 조정합니다. 이 통합의 출력은 가까운 취약 항목(VI)입니다. 없는 경우에는 구성 항목, 타사 항목 및 CVE도 생성됩니다. 취약성 탐지가 종결 상태로 생성됩니다.

사용자 인증 및 **Tenable.sc**

사용자 인증은 인스턴스 ServiceNow AI Platform# 와 제품의 버전 5.13 Tenable.sc 에서 지원됩니다. 버전 5.12 및 이전 버전의 제품을 사용하는 경우 사용자 인증이 Tenable.sc 필요합니다.

통합에 Tenable.sc 대한 사용자 인증을 선택하면 통합 실행 중에 토큰이 만료되고 대체될 수 있습니다. 취약성 통합 실행 기록(VIN)의 메모 열에 토큰이 만료될 때 프로세스에 대해 다음 메시지가 표시됩니다. ##: ## ### ### ######. 이 메시지가 표시되는 경우 아무 작업도 필요하지 않습니다. 만료된 토큰은 백그라운드에서 자동으로 새로 고쳐지며 메시지는 통합 프로세스의 일시 중지나 오류를 나타내지 않습니다.

Tenable 취약성 통합 준비

ServiceNow# 다음 설정 작업을 수행하여 Tenable 취약성 통합을 준비합니다.

시작하기 전에

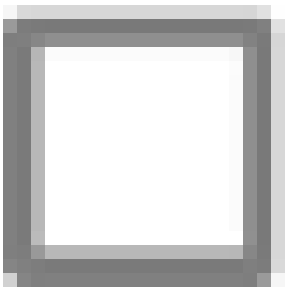
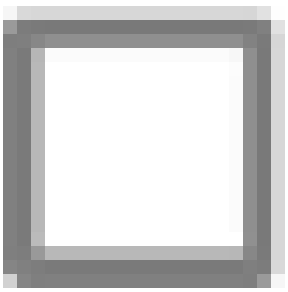
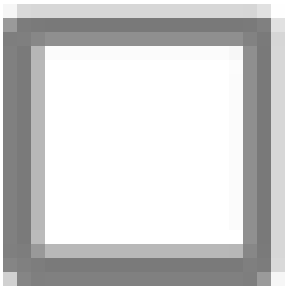
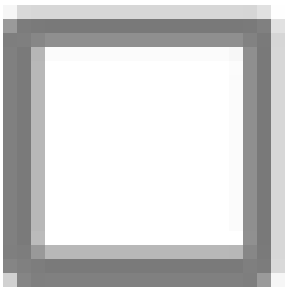
성공적인 통합을 위해서는 통합 전 작업을 계획하고 신중하게 실행해야 합니다. 애플리케이션의 원활한 설치 및 구성을 Vulnerability Response Integration with Tenable 위해 애플리케이션을 설치하고 취약성 데이터를 인스턴스로 ServiceNow AI Platform# 임포트하기 전에 다음 검사 목록을 인쇄하고 나열된 항목이 완료되었는지 확인하는 것이 좋습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

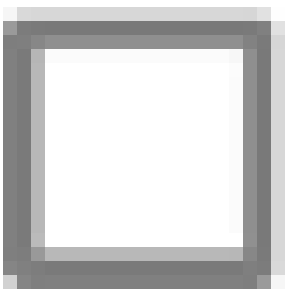
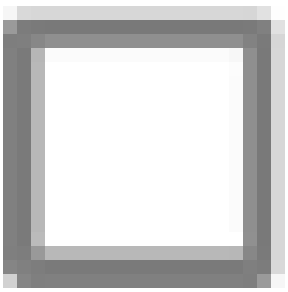
주:
Tenable이 구축한 통합으로 데이터를 임포트해 왔으며 Tenable과의 취약성 대응 통합을 사용하여 ServiceNow# 시작하려는 경우 문서를 참조하십시오.

Tenable이 구축한 통합에서 에서 빌드한 ServiceNow통합으로의 현재 데이터 정리 및 마이그레이션 정보는 Tenable 취약성 대응 통합에서 Tenable과 ServiceNow 취약성 대응 통합으로 마이그레이션하기 위한 가이드라인 (KB0960667) 문서를 참조하십시오.

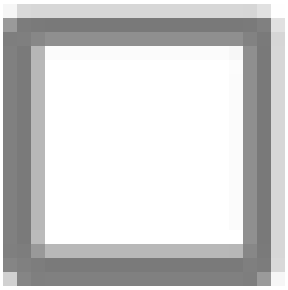
필요한 역할: 애플리케이션을 다운로드하고 설치하기 위한 관리자

작업	설명
	(선택 사항) 아직 설치 및 활성화되지 않은 경우 타사 애플리케이션을 설치하기 전에 애플리케이션을 설치하는 취약성 대응 것이 좋습니다. 애플리케이션 설치 및 활성화에 취약성 대응 대한 자세한 내용은 을 참조하십시오 취약성 대응 설치. 이 통합에는 버전 12.1 취약성 대응 이상이 필요합니다.
	인스턴스에 아직 없는 경우 권리를 얻고 인스턴스에 애플리케이션을 ServiceNow AI Platform# 다운로드합니다Vulnerability Response Integration with Tenable. 애플리케이션은 Vulnerability Response Integration with Tenable 버전 5.13 Tenable.cs 이상의 제품과 버전 5.0.1 이상의 제품을 지원합니다Tenable.sc. .
	임포트할 것으로 예상되는 취약한 항목의 수를 예상합니다. 임포트하려는 취약한 항목 수를 인스턴스가 수락할 수 있는지 확인합니다. 인스턴스 크기가 작으면 로드 시간이 길어질 수 있습니다. 인스턴스 크기를 모르거나 도움이 필요한 경우 기술 지원에 문의하십시오 ServiceNow# .
	통합을 관리하고 취약한 항목을 정정할 그룹 또는 사용자가 있는지 확인합니다. 관리자 시스템 관리자는 설정 도우미를 Vulnerability Response Integration with Tenable 사용하여 애플리케이션을 설치합니다. 할당되지 않은 경우 관리자는 취약성 관리자 (sn_vul.vulnerability_admin) 및 설정 도우미의 다른 역할을 할당합니다. sn_vul.vulnerability_admin 할당된 취약성 관리자는 Tenable 통합의 구성을 완료합니다. 이 역할은 (VR) 애플리케이션 및 해당 기록에 대한 취약성

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업	설명
	대응 전체 액세스 권한을 보유합니다. 모든 VR 애플리케이션 및 규칙을 구성하고 외부 공급업체 통합을 구성합니다. sn_vul_tenable.configure_integration Tenable 취약성 통합을 구성할 수 있습니다. 이 역할에는 sn_vul_tenable.read_integration 세분화된 역할이 포함됩니다. sn_vul_tenable.read_integration Tenable 취약성 통합의 기록을 보거나 읽을 수 있습니다. 취약성 대응 그룹 기본적으로 취약성 대응 그룹은 설정 도우미에서 사용할 수 있습니다. 취약성 대응 그룹에 할당된 사용자는 sn_vul.read_all 및 sn_vul.remediation_owner 역할을 자동으로 상속합니다. 시스템 관리자는 통합을 위해 설정 도우미에서 사용자 및 그룹에 초기 역할 할당을 수행합니다. 기본적으로 취약성 대응 그룹을 사용할 수 있습니다. 아직 생성하지 않은 경우, 설정 도우미를 사용하기 전에 추가 그룹을 생성하고 인스턴스에서 사용자 관리 모듈을 사용하여 사용자를 추가하는 것이 좋습니다. 사용자 그룹 만들기를 참조하십시오. 가상 사용자 및 세분화된 역할을 사용하여 사용자가 Vulnerability Response 애플리케이션에서 확인하고 수행할 수 있는 내용을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할을 처음 할당하려면 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당.
	첫 번째 임포트의 성능을 향상시키려면 인스턴스에서 특정 기능, 규칙 또는 작업을 비활성화하는 것이 좋습니다. • 취약성 계산기를 사용하지 않는 경우 비활성화합니다. 이러한 계산기와 사용자가 정의한 계산기는 취약한 항목 레코드가 생성되거나 업데이트될 때마다 실행됩니다. 취약성 계산기 사용 안 함의 내용을 참조하십시오. • 기록을 처음 임포트하는 동안 특정 알림 관련 비즈니스 규칙으로 인해 많은 알림이 생성되어 성능에 영향을 줄 수 있습니다. 초기 임포트에 앞서 설명된 Tenable 취약성 통합에 대한 수정 사항 임포트대로 알림 관련 비즈니스 규칙을 비활성화하는 것이 좋습니다.
	통합에 필요한 인스턴스의 기능, 규칙, 의존성 플러그인 또는 작업을 활성화했는지 확인합니다. • Tenable.sc는 제품과 ServiceNow AI Platform 인스턴스가 동일한 환경에 있는 경우 Vulnerability Response Integration with Tenable MID 서버를 사용하는 옵션을 제공하는 온 프레미스 통합입니다. Tenable.sc 제품과 ServiceNow AI Platform 인스턴스가 동일한 환경에 있지 않은 경우 MID 서버를 사용해야 합니다. 인스턴스의 MID 서버에 대한 자세한 내용은 MID 서버 단원을 참조하십시오. • 통합 허브 플러그인이 설치되고 활성화되었는지 확인합니다. 이 플러그인을 사용하면 기본 시스템 구성요소에서 통합 API를 사용하여

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업	설명
	외부 시스템을 호출하고 REST와 같은 프로토콜 단계를 활성화할 수 있습니다. 다음으로 이동 시스템 애플리케이션 〉 모든 사용 가능 애플리케이션 〉 모두 플러그인을 찾습니다. 인스턴스에 설치되어 있지 않은 경우 설치하고 활성화합니다.
	Tenable 자격 증명을 얻습니다. Tenable 제품에 액세스할 수 있도록 Tenable 제품에 필요한 계정 이름, 암호 및 기타 서비스 정보가 있는지 확인합니다. Tenable.io 권한 속성이 64 이상인 관리자 액세스 권한이 필요합니다. Tenable.sc 보안 분석가 또는 관리자 액세스 권한이 필요합니다. 주: 의 Vulnerability Response Integration with Tenablev3.8부터는 더 이상 관리자 Tenable.io 권한이 필요하지 않습니다. 권한 속성이 16인 기본 사용자도 제품에 액세스할 수 있습니다.

준비가 완료되었습니다 설정 도우미를 Vulnerability Response Integration with Tenable 사용하여 애플리케이션 설치.

설정 도우미를 **Vulnerability Response Integration with Tenable** 사용하여 애플리케이션 설치

Tenable 취약성 통합을 실행하기 ServiceNow# 전에 에서 ServiceNow Store 애플리케이션을 다운로드하고 Vulnerability Response Integration with Tenable 애플리케이션에서 설정 도우미 취약성 대응 를 사용하여 설치하고 구성해야 합니다.

시작하기 전에
Tenable 애플리케이션을 설치하기 전에 의 Tenable 취약성 통합 준비검사 목록에 있는 모든 항목을 완료했는지 확인하십시오.

주:
이 프로세스는 프로덕션 인스턴스에 다운로드된 애플리케이션에만 적용됩니다. 애플리케이션을 비프로덕션 또는 개발 인스턴스에 다운로드하는 경우에는 권리를 얻을 필요가 없습니다. 로 애플리케이션 활성화 ServiceNow Store계속 진행합니다.

필요한 역할: admin sn_vul.vulnerability_admin 역할의 초기 할당과 설정 도우미에 Tenable 애플리케이션 설치를 위한 admin. 취약성 관리자(sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음))는 애플리케이션을 설치한 후 설정 도우미에서 애플리케이션을 구성할 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 설정 도우미 〉 통합 애플리케이션 설치.

   잠시 후 인스턴스에 설치할 수 있는 애플리케이션이 표시됩니다.

2. **Tenable(Tenable** 플랫폼) 타일을 찾아 설치를 클릭하십시오.

   이 작업은 에서 ServiceNow Store다운로드한 애플리케이션을 설치합니다Vulnerability Response Integration with Tenable.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 설치 도우미에 제공된 프롬프트에 따라 설치를 계속합니다.
4. 설치 도우미를 사용하여 응용 프로그램을 설치하는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 설정 도우미를 사용하여 타사 응용 프로그램 설치 취약성 대응.

다음에 수행할 작업
설정 도우미에서 설치를 완료한 후 설정 도우미에서 통합 구성〉스캐너 통합 으로 이동하여 구성을 계속합니다. 설정 도우미에서 제공되는 프롬프트를 보완하는 자세한 내용은 문서를 참조하십시오 설정 도우미를 사용하여 Tenable 취약성 통합 구성.

Tenable 취약성 통합에 대한 데이터 검색 설정

다음 데이터 검색 설정은 Tenable 취약성 통합에서 ServiceNow# 인스턴스로 ServiceNow AI Platform# 임포트하려는 데이터의 유형과 범위를 구체적으로 결정하는 데 도움이 됩니다.

다음 섹션에 설명된 설정은 가져올 데이터를 제어하는 데 도움이 됩니다. 또한 통합 인스턴스에서 이러한 필터의 값을 설정할 수 있습니다. 통합 인스턴스를 보려면 다음으로 이동하십시오. **Tenable** 취약성 통합 〉 통합 인스턴스 을 클릭하고 통합, Tenable.io, 또는 Tenable.scTenable.cs를 선택합니다.

표시되는 통합 인스턴스 페이지에서 통합 인스턴스 매개변수를 선택하여 매개변수 목록을 표시하거나 일정, REST 상세 정보, 통합 상세 정보, 데이터 소스 및 통합 실행 정보에 대한 취약성 통합 탭을 표시합니다.

, **Tenable.sc** 인스턴스에 **Tenable.cs** 대한 **Tenable.io**공통 심각도 및 검색 설정과 필터 **ServiceNow AI Platform**

인스턴스의 , , 통합에 Tenable.io다음 설정을 사용할 수 있습니다ServiceNow AI Platform.Tenable.csTenable.sc 이러한 구성 설정 및 기타 구성 설정은 인스턴스의 ServiceNow AI Platform 통합 인스턴스 페이지에 표시됩니다. 처음 몇 개의 통합 실행에 대해 이러한 설정을 기본값으로 두는 것이 좋습니다.

Tenable.io

insert_fixed

취약성 임포트 통합을 위해 설정 도우미에서 **insert_fixed** 플래그를 활성화하면 인스턴스에 존재하지 않는 고정 상태의 탐지에 대해 새 VI가 생성됩니다.

severity_critical

이 필터는 기본적으로(예) 활성화되어 미해결 취약성 및 Tenable.io 수정된 취약성 통합에서 중요 심각도 취약성을 수신합니다Tenable.io.

severity_high

이 필터는 기본적으로(예) 활성화되어 미해결 취약성 및 Tenable.io 수정된 취약성 통합에서 높은 심각도 취약성을 수신합니다Tenable.io.

severity_medium

이 필터는 기본적으로 비활성입니다(False). 이 필터를 활성화하여 미해결 취약성 및 Tenable.io 수정된 취약성 통합에서 중간 수준의 심각도 취약성을 수신합니다Tenable.io.

severity_info

이 필터는 기본적으로 비활성입니다(False). 이 필터를 활성화하여 오픈 취약성 및 Tenable.io 수정된 취약성 통합에서 정보 수준의 심각도 취약성을 수신합니다Tenable.io.

severity_low

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 필터는 기본적으로 비활성입니다(False). 이 필터를 활성화하여 오픈 취약성 및 Tenable.io 수정된 취약성 통합에서 낮은 심각도 취약성을 수신합니다Tenable.io.

크기

이 설정은 플러그인 통합의 결과 세트에 Tenable.io 포함할 플러그인 기록 수를 정의합니다. int32 형식이어야 합니다. 기본값은 1,000입니다. 최대 크기는 10,000입니다.

num_assets

수정된 취약성 및 Tenable.io 미해결 취약성 통합에서 익스포트한 Tenable.io 청크당 최대 취약성 수입니다. 기본값은 50입니다.

chunk_size

자산 통합에서 익스포트한 청크당 Tenable.io 자산 수를 지정합니다. 기본값은 1,000입니다.

Tenable.sc

async_request

이 매개변수는 기본적으로 비활성입니다(false). 이 매개변수를 활성화 또는 비활성화하여 각각 비동기 또는 동기 API 호출을 Tenable.sc 수행합니다. 동기 호출의 경우 30초에 시간 제한이 있으면 Tenable 제품에 대한 지원팀에 문의하여 상자를 조정합니다. 이 매개변수는 활성화되면 의 모든 통합 Tenable.sc에 적용할 수 있습니다. 비동기 호출을 사용하는 기존 고객의 경우 기존 Tenable.sc 통합 인스턴스에 새 async_request 매개변수를 추가하는 수정 스크립트를 사용할 수 있습니다. 수정 스크립트를 보려면 다음으로 이동하십시오. 시스템 정의 〉 스크립트 수정.

insert_fixed

취약성 임포트 통합을 위해 설정 도우미에서 **insert_fixed** 플래그를 활성화하면 인스턴스에 존재하지 않는 고정 상태의 탐지에 대해 새 VI가 생성됩니다.

오프셋

하나의 통합 실행에서 임포트되는 자산, 플러그인 및 취약성 수를 지정합니다.

쿼리 필터

쿼리 필터는 Tenable 콘솔 내에서 구성됩니다. 이러한 쿼리 필터에는 설정 도우미 또는 인스턴스의 통합 인스턴스 페이지에서 ServiceNow AI Platform 선택할 수 있는 ID가 있습니다. 이러한 필터는 통합에서 Tenable.sc 데이터를 검색하는 동안 적용됩니다.

Tenable.cs

compute_severity_critical

이 필터는 기본적으로(true) 활성화되어 오픈 클라우드 호스트 취약성 통합 및 Tenable.cs 고정 클라우드 호스트 취약성 통합에서 중요 심각도 취약성을 수신합니다Tenable.cs.

compute_severity_high

이 필터는 기본적으로(true) 활성화되어 Open Cloud Host Vulnerabilities Integration 및 Tenable.cs Fixed Cloud Host Vulnerabilities Integration에서 높은 심각도 취약성을 수신합니다Tenable.cs.

compute_severity_medium

이 필터는 기본적으로 비활성입니다(False). Open Cloud Host Vulnerabilities Integration 및 Tenable.cs Fixed Cloud Host Vulnerabilities Integration에서 중간 수준의 심각도 취약성을 Tenable.cs 수신하려면 이 필터를 활성화합니다.

compute_severity_info

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 필터는 기본적으로 비활성입니다(False). 이 필터를 사용 설정하여 오픈 클라우드 호스트 취약성 통합 및 Tenable.cs 고정 클라우드 호스트 취약성 통합에서 정보 수준의 심각도 취약성을 수신합니다Tenable.cs.

compute_severity_low

이 필터는 기본적으로 비활성입니다(False). 이 필터를 사용 설정하여 오픈 클라우드 호스트 취약성 통합 및 Tenable.cs 고정 클라우드 호스트 취약성 통합에서 낮은 심각도 취약성을 수신합니다Tenable.cs.

container_severity_critical

이 필터는 기본적으로(true) 사용 설정되어 Open Cloud Container Vulnerabilities Integration 및 Tenable.cs Fixed Cloud Container Vulnerabilities Integration에서 중요 심각도 컨테이너 취약성을 수신합니다Tenable.cs.

container_severity_high

이 필터는 기본적으로(true) 활성화되어 Open Cloud Container Vulnerabilities Integration 및 Tenable.cs Fixed Cloud Container Vulnerabilities Integration에서 높은 심각도 컨테이너 취약성을 수신합니다Tenable.cs.

container_severity_medium

이 필터는 기본적으로 비활성입니다(False). Open Cloud Container Vulnerabilities Integration 및 Tenable.cs Fixed Cloud Container Vulnerabilities Integration에서 중간 수준의 심각도 컨테이너 취약성을 수신하려면 Tenable.cs 이 필터를 사용 설정합니다.

container_severity_info

이 필터는 기본적으로 비활성입니다(False). 이 필터를 사용 설정하여 컨테이너에서 정보 수준의 심각도 취약성, 오픈 클라우드 컨테이너 취약성 통합 Tenable.cs 의 Tenable.cs 취약성, 고정 클라우드 컨테이너 취약성 통합을 수신합니다.

container_severity_low

이 필터는 기본적으로 비활성입니다(False). Open Cloud Container Vulnerabilities 통합 및 Tenable.cs 고정 Cloud Container Vulnerabilities 통합에서 낮은 심각도 컨테이너 취약성을 수신하려면 Tenable.cs 이 필터를 사용 설정합니다.

asset_page_limit

이 설정은 클라우드 컨테이너 자산 통합의 Tenable.cs 결과 집합에 포함할 컨테이너 자산 기록 수를 정의합니다. 기본값은 1,000입니다. 최대 크기는 1,000입니다.

vuln_page_limit

이 설정은 오픈 클라우드 호스트 취약성 통합, 고정 클라우드 호스트 취약성 통합, Tenable.csTenable.cs 오픈 클라우드 컨테이너 취약성 통합, 고정 클라우드 컨테이너 취약성 통합의 Tenable.cs 결과 집합에 Tenable.cs 포함할 취약성 레코드 수를 정의합니다. 기본값은 1,000입니다. 최대 크기는 10,000입니다.

Tenable 취약성 통합에 대한 **REST** 메시지

ServiceNow# Tenable 취약성 통합 REST 메시지는 Tenable API를 호출하는 데 사용됩니다.

Tenable.io 자산 **REST** 메시지

Tenable.io 자산 REST 메시지는 자산 통합에 Tenable.io 대한 자산 정보를 검색합니다. REST 메시지 메서드 기록을 변경하면 자산 정보를 검색하기 위한 요청에 Tenable.io 영향을 줍니다. 자산에 대한 익스포트 작업이 다음 필터와 함께 제출됩니다.

- "is_deleted": 거짓
- "is_licensed": 참

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Tenable.io 플러그인 REST 메시지

Tenable.io 플러그인 REST 메시지는 플러그인 통합을 위한 Tenable.io 플러그인 정보를 검색합니다. REST 메시지 메서드 기록에 대한 변경 사항은 플러그인 정보를 검색하기 위한 Tenable.io 요청에 영향을 미칩니다.

Tenable.io 취약성 REST 메시지

Tenable.io 취약성 REST 메시지는 취약성 통합에서 Tenable.io 오픈 및 종결된 취약성 모두에 대한 취약성 정보를 검색합니다. REST 메시지 메서드 기록을 변경하면 취약성 정보 검색 요청에 Tenable.io 영향을 미칩니다.

Tenable.sc 쿼리 REST 메시지

Tenable.sc 쿼리 REST 메시지는 쿼리 필터가 구성된 Tenable.sc 자산 통합 및 Tenable.sc 취약성 통합에 대한 쿼리 필터 정보를 검색합니다.

Tenable.sc 플러그인 REST 메시지

Tenable.sc 플러그인 REST 메시지는 플러그인 통합에 Tenable.sc 대한 플러그인 정보를 검색합니다. REST 메시지 플러그인 메서드 기록 가져오기에 대한 변경은 플러그인 정보를 검색하기 위한 요청에 Tenable.sc 영향을 미칩니다.

매개변수 이름	값	설명
유형	활성	Tenable이 데이터를 가져오는 소스를 나타냅니다. 코드에서 사용됩니다. 변경은 권장되지 않습니다.
필드	id, 설명, cvssVector,cvssV3Vector, cvssV3TemporalVector, 시놉시스, cvssVector, baseScore,temporalScore, cvssV3Vector,cvssV3BaseScore, cvssV3TemporalScore, name, vprScore, vprContext, pluginPubDate, pluginModDate, xrefs, family, riskFactor, cpe, seeAlso, solution, exploitAvailable, exploitFrameworks, type, copyright, version, sourceFile, dependencies, requiredPorts, requiredUDPPorts, srcPort, dstPort,protocol, checkType, cvssVectorBF, stigSeverity, patchPubDate, patchModDate, vulnPubDate, modifiedTime, md5	Tenable에서 임포트한 필드 목록을 나타냅니다.

Tenable.sc 취약성 REST 메시지

Tenable.sc 취약성 REST 메시지는 통합에서 Tenable.sc 취약성 정보를 검색합니다. REST 메시지 취약성 가져오기 또는 패치된 취약성 가져오기 방법에 대한 변경 사항 또는 Tenable 취약성 통합

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

v14.0 취약성 대응 및 v2.2부터 취약성 기록 채우기 가져오기는 취약성 정보를 검색하기 위한 Tenable.sc 요청에 영향을 미칩니다.

Tenable.sc 스캔 자격 증명 REST 메시지

Tenable.sc 정책 REST 메시지

Tenable.sc 정책 POST REST 메시지는 요청된 플러그인에 대한 정책을 추가합니다. 생성된 정책이 스캔 요청에 Tenable.sc 사용됩니다.

Tenable.sc 스캔 REST 메시지

Tenable.sc 스캔 POST REST 메시지는 REST 메시지의 요청 본문에 정의된 액세스 및 권한에 따라 달라지는 스캔을 추가합니다. 스캔 요청에 대한 요청 본문의 정책, 플러그인 ID 및 IP를 사용합니다.

Tenable.sc 스캔 결과 REST 메시지

Tenable.sc 스캔 결과 GET REST 메시지는 스캔 REST 메시지를 사용하여 생성된 스캔의 스캔 상세 정보를 제공합니다. 스캔 REST 메시지의 응답에 scanResultId를 사용하고 트리거된 스캔에 대한 스캔 상세 정보를 검색합니다.

Tenable.sc 스캔 자격 증명

Tenable.sc 검사 자격 증명 REST 메시지는 에서 Tenable.sc자격 증명 정보를 검색합니다. REST 메시지 "임포트" 메서드 기록에 대한 변경은 자격 증명 정보를 검색하기 위한 Tenable.sc 요청에 영향을 미칩니다.

매개변수 이름	값	설명
필드	ID, 이름, 설명, 유형	임포트한 필드 목록을 나타냅니다. Tenable.sc
필터	사용할	통합이 다음에서 사용 가능한 자격 증명만 끌어온다는 것을 나타냅니다. Tenable.sc 매개 변수 중 하나를 변경하는 것은 권장되지 않습니다.

Tenable.cs GraphQl REST 메시지: Tenable.cs GraphQl REST 메시지는 통합을 위해 Tenable.cs 컨테이너 자산 정보, 호스트 및 컨테이너 취약성 정보를 검색합니다. REST 메시지 컨테이너 자산 가져오기, 컨테이너 취약성 가져오기, 계산 취약성 메서드 기록 가져오기에 대한 변경 사항은 자산 및 취약성 정보를 검색하기 위한 Tenable.cs 요청에 영향을 미칩니다.

Tenable 취약성 통합을 위한 데이터 변환

임포트할 데이터를 식별한 후에는 Tenable 제품에서 검색되어 인스턴스의 데이터 소스 및 변환 세트를 통해 처리됩니다.

설치하는 동안 정규화된 심각도 맵이 정규화된 심각도 매핑 모듈에 설치됩니다. 이 맵은 임포트한 Tenable 심각도 수준을 인스턴스에서 처리할 표준 심각도 수준으로 변환합니다. 심각도 맵 생성에 대한 자세한 내용은 설명서의 취약성 대응 심각도 맵 취약성 대응 생성을 참조하십시오.

Tenable.io 자산 임포트

임포트한 자산 데이터는 먼저 Tenable.io 자산 임포트[sn_vul_tenable_io_asset_import] 테이블에 로드됩니다.

Tenable.io 자산 통합 변환 맵은 임포트한 자산 정보를 변환하는 데 사용됩니다. 이 변환을 변경하면 Tenable 자산 임포트의 데이터가 처리되는 방식이 변경됩니다. 이 변환 맵에 액세스하려면 다음으로 이동하십시오. 시스템 임포트 세트 〉 변환 맵. Tenable.io ## ### 검색합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음 표에는 통합별 변환 맵 필드가 나열되어 있습니다.

자산 변환 맵 필드 **Tenable.io**

소스 필드	대상 필드	설명
u_id	source_id	Tenable은 자산에 대한 고유 ID를 제공하고 검색된 항목 기록에 매핑하며 CI 조회에 사용됩니다.
u_ipv4s	ip_address	첫 번째 IP 값을 검색된 항목 기록의 ip_address 필드에 매핑합니다.
u_mac_addresses	mac_address	첫 번째 mac_address 값을 검색된 항목 기록의 mac 주소 필드에 매핑합니다.
u_fqdns	fqdn	첫 번째 fqdn 값을 검색된 항목 기록의 fqdn 필드에 매핑합니다.
u_netbios_names	NetBIOS	첫 번째 netBIOS 값을 검색된 항목 기록의 netBIOS 필드에 매핑합니다.
u_operating_systems	os	첫 번째 OS 값을 검색된 항목 기록의 os 필드에 매핑합니다.
(Tenable 취약성 통합 v14.0 취약성 대응 및 v2.2 이전)u_last_scan_time	last_scan_date	검색된 항목 기록의 last_scan_date 필드에 매핑합니다.
u_last_authenticated_scan_date	last_auth_scan_date	검색된 항목 기록의 last_auth_scan_date 필드에 매핑합니다.
〔스크립트〕	이름	스크립트의 논리를 사용하여 호스트 이름을 매핑합니다.
u_tags		태그는 sn_sec_cmn_host_tag에 저장됩니다. 태그에서 자산으로의 매핑은 sn_sec_cmn_m2m_src_ci_tag에 저장됩니다.

변환 프로세스 중에 실행되는 세 가지 변환 스크립트가 있습니다. 다음 표에는 각 스크립트가 실행되는 시기와 용도가 나와 있습니다.

Tenable.io 자산 변환 맵 스크립트 타이밍 및 목적

스크립트가 실행될 때	목적
onStart(임포트 세트가 변환을 시작한 경우)	통합 프로세스에 대한 import_set의 값을 초기화합니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.
onBefore(임포트 세트가 변환을 완료하기 전)	호스트의 값을 업데이트하고 호스트가 존재하는지 확인합니다. 결과에 따라

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

스크립트가 실행될 때	목적
	import_set의 값을 수정합니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.
onComplete(임포트 세트가 변환을 완료한 경우)	새로 생성된 CI와 업데이트 후 무시된 CI의 값을 설정합니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.

Tenable.io 플러그인 통합

Tenable.io 플러그인 변환 맵은 Tenable.io 에서 임포트한 플러그인을 변환하는 데 사용됩니다.

주:
이 변환 맵을 변경하면 Tenable 플러그인에서 받은 데이터의 처리 방식이 변경됩니다.

이 변환 맵에 액세스하려면 다음으로 이동하십시오. 시스템 임포트 세트 〉 변환 맵. Tenable.io 플러그인 변환을 검색합니다.

tenable.io 플러그인 페이로드에는 sn_vul_tenable_io_plugin_import 테이블의 u_attributes 열에 있는 모든 필드가 포함되어 있습니다. 속성 필드는 다음 표에 나열된 대로 구문 분석되고 외부 공급업체 항목 테이블 기록에 매핑됩니다.

소스 필드	대상 필드	설명
ID	ID	소스의 ID를 매핑하고 여기에 TEN 접두사를 추가합니다. 예를 들어 수신된 ID가 12345인 경우 대상 테이블의 ID는 TEN-12345입니다.
설명	요약	플러그인의 설명을 요약 열에 매핑합니다.
〔스크립트〕	소스	임포트한 외부 공급업체 항목(TPE)의 소스는 Tenable.io 입니다.
〔스크립트〕	source_instance	이 기록을 임포트하는 Tenable 배포에 대한 참조입니다.
제품군	범주	플러그인 제품군을 범주 열에 매핑합니다.
plugin_modification_date	last_modified	plugin_modification_date 마지막으로 수정한 필드에 매핑합니다.
plugin_publication_date	date_published	plugin_publication_date 게시된 날짜에 매핑합니다.
has_patch	remediation_type	has_patch 값에서 정정 유형을 매핑합니다.
시놉시스	위협	이 취약성에 대한 위협 정보를 매핑합니다.
cvss_base__score	점수	CVSS(공통 취약성 평가 시스템) 기본 점수를 외부

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

소스 필드	대상 필드	설명
		공급업체 항목 테이블의 점수 열에 매핑합니다.
솔루션	솔루션	스캐너에서 제공한 솔루션을 외부 공급업체 항목 테이블의 솔루션 열에 매핑합니다.
exploit_available	익스플로잇	스캐너에서 제공한 exploit_available 외부 공급업체 항목 테이블의 익스플로잇 열에 매핑합니다.
vpr.score	source_risk_score	스캐너에서 제공한 VPR 점수를 외부 공급업체 항목 테이블의 source_risk_score 매핑합니다.
〔스크립트〕	source_risk_rating	점수 범위를 기준으로 VPR 점수를 표준 위험 등급에 매핑합니다. • 9–10 – 중요 • 7–9 – 높음 • 4–7 – 중간 • 0–4 - 낮음
vpr.drivers.age_of_vuln	age_of_vuln	스캐너의 취약성 기간을 외부 공급업체 항목 테이블의 age_of_vuln 열에 매핑합니다.
vpr.drivers.exploit_code_maturity	exploit_code_maturity	스캐너에서 외부 공급업체 항목 테이블의 exploit_code_maturity 악용 코드 성숙도를 매핑합니다.
vpr.drivers.product_coverage	product_coverage	스캐너의 제품 범위를 외부 공급업체 항목 테이블의 product_coverage 매핑합니다.
vpr.drivers.threat_sources_last28	threat_sources	스캐너에서 지난 28일 동안의 위협 소스를 외부 공급업체 테이블의 threat_sources 매핑합니다.
vpr.drivers.threat_intensity_last28	threat_intensity	스캐너에서 외부 공급업체 항목 테이블의 threat_intensity 지난 28일 동안의 위협 강도를 매핑합니다.
vpr.drivers.threat_recency	threat_recency	스캐너의 위협 최신성 정보를 외부 공급업체 항목 테이블의 threat_recency 매핑합니다.
vpr.drivers.cvss3_impact_score	v3_impact_subscore	cvss3 영향 점수를 외부 공급업체 항목 테이블의 v3_impact_subscore 열에 매핑합니다.
cvss_temporal_score	cvss_temporal_score	CVSS v2의 임시 점수를 매핑합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

소스 필드	대상 필드	설명
cvss_v3_temporal_score	v3_temporal_score	CVSS v3의 임시 점수를 매핑합니다.
risk_factor	source_severity	외부 공급업체 항목 테이블의 소스 심각도에 매핑합니다.
이름	이름	플러그인의 이름을 외부 공급업체 항목 테이블의 이름에 매핑합니다.
stig_severity	stig_severity	스캐너에서 제공하는 VPR 점수를 외부 공급업체 항목 테이블의 source_risk_score 매핑합니다.
plugin_type	check_type	플러그인 유형을 외부 공급업체 항목 테이블의 check_type에 매핑합니다.
unsupported_by_vendor	unsupported_by_vendor	unsupported_by_vendor 필드를 unsupported_by_vendor 열에 매핑합니다.
〔스크립트〕	exploit_attack_vector	외부 공급업체 항목 테이블의 exploit_attack_vector 열은 열의 exploit_available 및 v3_attack_vector 기준으로 채워집니다.

직접 필드 외에도 다른 정보가 외부 공급업체 항목에 관련 목록으로 추가됩니다.

소스 필드	설명
cve	CVE 관련 데이터를 참조 테이블(sn_vul_nvd_entry)에 삽입합니다. NVD 항목 테이블(sn_vul_nvd_entry)에서 동일한 CVE(Common Vulnerabilities and Exposures)가 발견되면 현재 취약성을 NVD 항목에 연결합니다. 매핑은 sn_vul_m2m_entry_cve에서 찾을 수 있습니다.
입찰	버그 트랙 목록이 참조로 추가됩니다.
see_also	URL 목록이 참조로 추가됩니다.
외부 참조	X-REF 목록이 참조로 추가됩니다.
〔스크립트〕	해당 플러그인에 대한 익스플로잇 목록과 해당 익스플로잇 프레임워크 및 플러그인에 대한 매핑을 sn_vul_m2m_framework_vul 삽입합니다.

변환 프로세스 중에 실행되는 세 가지 변환 스크립트가 있습니다. 다음 표에는 각 스크립트가 실행되는 시기와 용도가 나와 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

스크립트가 실행될 때	목적
onStart(임포트 세트가 변환을 시작한 경우)	통합 프로세스에 대한 import_set의 값을 초기화합니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.
onBefore(임포트 세트가 변환을 완료하기 전)	외부 공급업체 항목의 값을 업데이트하고 외부 공급업체 항목이 있는지 확인합니다. 결과에 따라 외부 공급업체 항목의 값을 수정합니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.
onComplete(임포트 세트가 변환을 완료한 경우)	새로 생성된 CI와 업데이트 후 무시된 CI의 값을 설정합니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.

TenableIOPluginsImportProcessor 스크립트 포함은 onBefore 변환 스크립트에서 호출됩니다. Tenable.io 플러그인 통합에서 출력을 가져와 외부 공급업체 취약성 항목으로 변환합니다 ServiceNow AI Platform . 이 스크립트 포함을 변경하면 외부 공급업체 항목 테이블의 Tenable.io 플러그인 데이터 변환이 변경될 수 있습니다.

Tenable.io 취약성 임포트

Tenable.io 취약한 항목 변환 맵은 Tenable.io 에서 임포트한 미해결 및 수정된 취약성 정보를 변환하는 데 사용됩니다.

주:
이 변환 맵을 변경하면 Tenable 취약성 임포트의 데이터가 처리되는 방식이 변경됩니다.

Tenable.io Fixed Vulnerabilities Integration과 Tenable.io Open Vulnerabilities Integration에 동일한 변환 맵이 사용됩니다. 이 변환 맵에 액세스하려면 다음으로 이동하십시오. 시스템 임포트 세트 〉 변환 맵. Tenable.io ### ## ## ## 검색합니다.

소스 필드	대상 필드	설명
u_asset.uuid	ID	UUID는 cmdb_ci 기록의 ID 필드에 매핑됩니다.
u_asset.ipv4	ip_address	ipv4 필드는 cmdb_ci 기록의 ip 주소 필드에 매핑됩니다.
u_asset.last_authenticated_results	last_auth_scan_date	인증된 마지막 검사 날짜는 cmdb_ci 기록의 마지막 인증 검사 날짜에 매핑됩니다.
u_asset.mac_addess	mac_address	Mac 주소는 cmdb_ci 기록의 호스트 mac 주소 필드에 매핑됩니다.
u_asset.netbios_name	NetBIOS	NetBIOS는 기록의 netbios 필드에 매핑cmdb_ci.
u._plugin.cvss3_base_score	v3_base_score	CVSS v3 기본 점수는 외부 공급업체 항목 기록의 v3 기본 점수에 매핑됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

소스 필드	대상 필드	설명
u._plugin.cvss3_temporal_score	v3_temporal_score	CVSS v3 임시 점수는 외부 공급업체 항목 기록의 v3 임시 점수에 매핑됩니다.
u._plugin.cvss_base_score	점수	CVSS 기본 점수는 외부 공급업체 참가 기록의 점수 필드에 매핑됩니다.
u._plugin.cvss_temporal_score	temporal_score	임시 점수는 외부 공급업체 항목 기록의 임시 점수에 매핑됩니다.
u_plugin.description	요약	설명이 외부 공급업체 항목 기록의 요약 필드에 매핑됩니다.
u_plugin.가족	범주	플러그인 제품군을 외부 공급업체 항목 기록의 범주 열에 매핑합니다.
u_plugin.modification_date	last_modified	마지막 수정 날짜는 외부 공급업체 항목 기록의 플러그인 마지막 수정 날짜에 매핑됩니다.
u_plugin.publication_date	date_published	게시 날짜는 외부 공급업체 항목 기록의 게시된 날짜 필드에 매핑됩니다.
u_plugin.risk_factor	source_severity	위험 요인은 외부 공급업체 항목 기록의 source_severity 필드에 매핑됩니다.
u_plugin.솔루션	솔루션	솔루션은 외부 공급업체 항목 기록의 솔루션 필드에 매핑됩니다.
u_plugin.시놉시스	위협	시놉시스는 외부 공급업체 항목 기록의 위협 필드에 매핑됩니다.
u_severity_id	우선순위	우선순위는 페이로드에서 심각도 ID에 매핑됩니다. 기본값은 5입니다.
u_plugin.exploit_available	익스플로잇	스캐너에서 제공하는 exploit_available 외부 공급업체 항목 테이블의 익스플로잇 열에 매핑합니다.
vpr.score	source_risk_score	스캐너에서 제공하는 VPR 점수를 외부 공급업체 항목 테이블의 source_risk_score 매핑합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

소스 필드	대상 필드	설명
〔스크립트〕	source_risk_rating	점수 범위를 기준으로 VPR 점수를 표준 위험 등급에 매핑합니다. • 9–10 – 중요 • 7–9 – 높음 • 4–7 – 중간 • 0–4 - 낮음
u_plugin.vpr.drivers.age_of_vuln	age_of_vuln	스캐너의 취약성 기간을 외부 공급업체 항목 테이블의 age_of_vuln 매핑합니다.
u_plugin.vpr.drivers.exploit_code_maturity	exploit_code_maturity	스캐너에서 외부 공급업체 항목 테이블의 exploit_code_maturity 악용 코드 성숙도를 매핑합니다.
u_plugin.vpr.drivers.product_coverage	product_coverage	스캐너의 제품 범위를 외부 공급업체 항목 테이블의 product_coverage 매핑합니다.
u_plugin.vpr.drivers.threat_sources_last28	threat_sources	스캐너에서 지난 28일 동안의 위협 소스를 외부 공급업체 항목 테이블의 threat_sources 매핑합니다.
u_plugin.vpr.drivers.threat_intensity_last28	threat_intensity	스캐너에서 외부 공급업체 항목 테이블의 threat_intensity 지난 28일 동안의 위협 강도를 매핑합니다.
u_plugin.vpr.drivers.threat_recency	threat_recency	스캐너의 위협 최신성 정보를 외부 공급업체 항목 테이블의 threat_recency 매핑합니다.
u_plugin.vpr.drivers.cvss3_impact_score	v3_impact_subscore	CVSS3 v3 영향 점수를 외부 공급업체 항목 테이블의 v3_impact_subscore 열에 매핑합니다.
u_plugin.유형	check_type	플러그인 유형을 외부 공급업체 항목 테이블의 check_type에 매핑합니다.
u_plugin.unsupported_by_vendor	unsupported_by_vendor	플러그인의 unsupported_by_vendor 필드를 unsupported_by_vendor 열에 매핑합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

소스 필드	대상 필드	설명
〔스크립트〕	exploit_attack_vector	외부 공급업체 항목 테이블의 exploit_attack_vector 열은 열의 exploit_available 및 v3_attack_vector 기준으로 채워집니다.
u_plugin.family_id	Family_id	플러그인 제품군 ID를 외부 공급업체 항목 테이블의 family_id 열에 매핑합니다.
포트	포트	포트는 취약한 항목 기록의 포트 필드에 매핑됩니다.
프로토콜	프로토콜	프로토콜은 취약한 항목 레코드의 프로토콜 필드에 매핑됩니다.
u_first_found	first_found	첫 번째 발견은 취약한 항목 기록의 처음 발견된 필드에 매핑됩니다.
u_last_found	last_found	마지막 발견은 취약한 항목 기록의 마지막 발견 필드에 매핑됩니다.
u_state	상태	상태는 취약한 항목 레코드의 상태 필드에 매핑됩니다.
〔스크립트〕	소스	통합의 소스가 채워집니다. 이 통합에서 생성된 취약한 항목이 소스로 Tenable.io.
〔스크립트〕	integration_instance	integration_instance은 취약한 항목을 임포트한 인스턴스의 이름입니다.
u_plugin.name	이름	플러그인의 이름을 외부 공급업체 항목 테이블의 이름에 매핑합니다.
u_plugin.stig_severity	stig_severity	플러그인의 stig 심각도를 외부 공급업체 항목 테이블의 stig 심각도 열에 매핑합니다.

직접 필드 외에도 다른 정보가 외부 공급업체 항목에 관련 목록으로 추가됩니다.

소스 필드	설명
cve	CVE 관련 데이터를 참조 테이블(sn_vul_nvd_entry)에 삽입합니다. NVD 항목 테이블(sn_vul_nvd_entry)에서 동일한 CVE가 발견되면 현재 취약성을 NVD 항목에 연결합니다. 매핑은 sn_vul_m2m_entry_cve에서 찾을 수 있습니다.
입찰	버그 트랙 목록이 참조로 추가됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

소스 필드	설명
see_also	URL 목록이 참조로 추가됩니다.
외부 참조	X-REF 목록이 참조로 추가됩니다.
〔스크립트〕	해당 플러그인에 대한 익스플로잇 목록 및 해당 익스플로잇 프레임워크에 대한 매핑 sn_vul_m2m_framework_vul 삽입합니다.

변환 프로세스 중에 실행되는 세 가지 변환 스크립트가 있습니다. 다음 표에는 각 스크립트가 실행되는 시기와 용도가 나와 있습니다.

스크립트가 실행될 때	목적
onStart(임포트 세트가 변환을 시작한 경우)	임포트 세트를 사용하여 Tenable.io 에서 데이터를 임포트하고 각 기록을 CMDB CI 테이블, 취약한 항목 테이블 및 외부 공급업체 취약성 테이블로 로드하는 Trigger Tenable IO 취약성 프로세서입니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.
onBefore(임포트 세트가 변환을 완료하기 전)	외부 공급업체 항목 및 탐지가 있는지 확인합니다. 그렇지 않은 경우 이러한 기록은 해당 테이블에 생성됩니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.
onComplete(임포트 세트가 변환을 완료한 경우)	Tenable.io 에서 임포트한 CI, VIT 및 탐지 수를 업데이트합니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.

Tenable.sc 자산 임포트

Tenable.sc 에서 임포트한 자산 데이터는 먼저 Tenable.sc 자산 임포트 테이블(sn_vul_tenable_sc_asset_import)에 로드됩니다. Tenable.sc 자산 통합 변환 맵은 임포트한 자산 정보를 변환하는 데 사용됩니다. 이 변환을 변경하면 Tenable 자산 임포트의 데이터가 처리되는 방식이 변경됩니다. 이 변환 맵에 액세스하려면 다음으로 이동하십시오. 시스템 임포트 세트 〉 변환 맵. Tenable.sc ## ### 검색합니다.

소스 필드	대상 필드	설명
u_uuid	ID	UUID는 Tenable API에서 채워지지 않으므로 "u_uniqueness" 속성은 자산에 대한 고유 UUID 필드를 만들고 cmdb_ci 기록에 매핑하는 데 사용됩니다.
u_ip	ip_address	API의 IP 필드를 cmdb_ci 기록의 ip_address 필드로 매핑합니다.
u_macaddress	mac_address	API의 MAC 주소 필드를 cmdb_ci 기록의 주소 필드에 매핑합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

소스 필드	대상 필드	설명
u_dnsname	fqdn	API의 dnsname 필드를 cmdb_ci 기록의 fqdn 필드에 매핑합니다.
u_netbiosname	NetBIOS	API의 netbios 필드를 cmdb_ci 기록의 netbios 필드로 매핑합니다.
u_oscpe	os	OS 정보는 페이로드의 oscpe 속성에서 추출되어 cmdb_ci 기록의 os 필드에 매핑됩니다.
u_lastauthrun	last_auth_scan_date	API의 lastauthrun 필드를 검색된 항목 기록의 last_auth_scan_date 필드에 매핑합니다.
u_lastauthrun 및 u_lastunauthrun	last_scan_date	lastauthrun은 Tenable API 또는 lastunauthrun에서 추출됩니다. 검색된 항목 기록의 last_scan_date 필드는 페이로드에 나타나는 값을 기준으로 채워집니다.

변환 프로세스 중에 실행되는 세 가지 변환 스크립트가 있습니다. 다음 표에는 각 스크립트가 실행되는 시기와 용도가 나와 있습니다.

스크립트가 실행될 때	목적
onStart(임포트 세트가 변환을 시작한 경우)	통합 프로세스에 대한 import_set의 값을 초기화합니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.
onBefore(임포트 세트가 변환을 완료하기 전)	호스트의 값을 업데이트하고 호스트가 존재하는지 확인합니다. 결과에 따라 import_set의 값을 수정합니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.
onComplete(임포트 세트가 변환을 완료한 경우)	새로 생성된 CI와 업데이트 후 무시된 CI의 값을 설정합니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.

Tenable.sc 플러그인 임포트

Tenable.sc 에서 임포트한 플러그인 데이터는 먼저 Tenable.sc 플러그인 임포트 테이블(sn_vul_tenable_sc_plugin_import)에 로드됩니다. Tenable.sc 플러그인 변환 맵은 임포트한 플러그인 정보를 변환하는 데 사용됩니다. 이 변환을 변경하면 Tenable 플러그인 임포트의 데이터가 처리되는 방식이 변경됩니다. 이 변환 맵에 액세스하려면 다음으로 이동하십시오. 시스템 임포트 세트 〉 변환 맵. #### ## # Tenable.sc 검색합니다.

소스 필드	대상 필드	설명
u_id	ID	소스에서 ID를 매핑하고 TEN 접두사를 추가합니다. 예를 들어 수신된 ID가 12345인

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

소스 필드	대상 필드	설명
		경우 대상 테이블의 ID는 TEN-12345입니다.
u_description	요약	플러그인의 설명을 요약 열에 매핑합니다.
〔스크립트〕	소스	이 통합에서 임포트한 TPE가 소스로 Tenable.sc.
〔스크립트〕	source_instance	이 기록을 임포트하는 Tenable 배포에 대한 참조입니다.
u_family	범주	플러그인의 패밀리 객체에 있는 이름 필드를 범주 열에 매핑합니다.
u_plugin_modification_date	last_modified	plugin_modification_date 마지막으로 수정한 필드에 매핑합니다.
u_plugin_publication_date	date_published	plugin_publication_date 게시된 날짜에 매핑합니다.
u_has_patch	Remediation_type	has_patch 값에서 정정 유형을 매핑합니다.
u_synopsis	위협	이 취약성에 대한 위협 정보를 매핑합니다.
u_cvss_base_score	점수	CVSS 기본 점수를 외부 공급업체 항목 테이블의 점수 열에 매핑합니다.
u_solution	솔루션	스캐너에서 제공하는 솔루션을 외부 공급업체 항목 테이블의 솔루션 열에 매핑합니다.
u_cvss_temporal_score	cvss_temporal_score	CVSS v2의 임시 점수를 매핑합니다.
u_cvss_v3_temporal_score	v3_temporal_score	CVSS v3의 임시 점수를 매핑합니다.
u_risk_factor	소스 심각도	외부 공급업체 항목 테이블의 소스 심각도에 매핑합니다.
u_cvss_v3_base_score	v3_base_score	외부 공급업체 항목 테이블에 CVSS 기본 점수를 매핑합니다.
u_exploit_available	익스플로잇	스캐너에서 제공하는 exploitAvailable을 외부 공급업체 항목 테이블의 익스플로잇 열에 매핑합니다.
u_vpr_score	source_risk_score	스캐너의 VPR 점수를 외부 공급업체 항목 테이블의 소스 위험 점수에 매핑합니다.
〔스크립트〕	source_risk_rating	점수 범위를 기준으로 VPR 점수를 표준 위험 등급에 매핑합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

소스 필드	대상 필드	설명
		• 9–10 – 중요 • 7–9 – 높음 • 4–7 – 중간 • 0–4 - 낮음
u_vpr_context(id=age_of_vuln)	age_of_vuln	취약성의 기간을 스캐너의 외부 공급업체 항목 테이블에 age_of_vuln 매핑합니다.
u_vpr_context(id=exploit_code_maturity)	exploit_code_maturity	스캐너에서 외부 공급업체 항목 테이블의 exploit_code_maturity 악용 코드 성숙도를 매핑합니다.
u_vpr_context(id=product_coverage)	product_coverage	스캐너의 제품 범위를 외부 공급업체 항목 테이블의 product_coverage 매핑합니다.
u_vpr_context(id="threat_sources_last_28")	threat_sources	지난 28일 동안의 위협 소스를 스캐너에서 외부 공급업체 테이블의 threat_sources 매핑합니다.
u_vpr_context(id="threat_intensity_last_28")	threat_intensity	스캐너에서 외부 공급업체 항목 테이블의 threat_intensity 지난 28일 동안의 위협 강도를 매핑합니다.
u_vpr_context(id="threat_recency")	threat_recency	스캐너의 위협 최신성 정보를 타사 항목 테이블의 threat_recency 매핑합니다.
u_vpr_context(id=cvssV3_impact_score)	v3_impact_subscore	스캐너의 CVSS v3 영향 점수를 외부 공급업체 항목 테이블의 v3_impact_subscore 매핑합니다.
u_name	이름	플러그인 이름을 외부 공급업체 항목 테이블의 이름 열에 매핑합니다.
u_stig_severity	stig_severity	플러그인의 stig_severity 필드를 외부 공급업체 항목 테이블의 stig_severity 매핑합니다.
u_check_type	check_type	검사 유형을 외부 공급업체 항목 테이블의 check_type에 매핑합니다.
u_family.id	family_id	플러그인 family_id 외부 공급업체 항목 테이블의 family_id에 매핑합니다.
〔스크립트〕	exploit_attack_vector	외부 공급업체 항목 테이블의 exploit_attack_vector 열은 열의 exploit_available 및 v3_attack_vector 기준으로 채워집니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

직접 필드 외에도 다른 정보가 외부 공급업체 항목에 관련 목록으로 추가됩니다.

소스 필드	설명
u_cpe	CPE 목록이 참조로 추가됩니다.
u_see_also	URL 목록이 참조로 추가됩니다.
u_exploit_frameworks	해당 플러그인에 대한 익스플로잇 목록과 해당 익스플로잇 프레임워크 및 플러그인에 대한 매핑을 sn_vul_m2m_framework_vul 삽입합니다.

변환 프로세스 중에 실행되는 세 가지 변환 스크립트가 있습니다. 다음 표에는 각 스크립트가 실행되는 시기와 용도가 나와 있습니다.

스크립트가 실행될 때	목적
onStart(임포트 세트가 변환을 시작한 경우)	이 변환은 통합 프로세스에 대한 import_set의 값을 초기화하는 데 사용됩니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.
onBefore(임포트 세트가 변환을 완료하기 전)	외부 공급업체 항목의 값을 업데이트하고 외부 공급업체 항목이 있는지 확인하는 데 사용되는 기능입니다. 결과에 따라 외부 공급업체 항목의 값을 수정합니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.
onComplete(임포트 세트가 변환을 완료한 경우)	이 변환은 만들어지고 무시된 플러그인의 값을 설정하는 데 사용됩니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.

TenableSCPluginsImportProcessor 스크립트 포함은 onBefore 변환 스크립트에서 호출됩니다. Tenable.sc 플러그인 통합에서 출력을 가져와 외부 공급업체 취약성 항목으로 변환합니다 ServiceNow . 이 스크립트 포함을 변경하면 외부 공급업체 항목 테이블의 Tenable.sc 플러그인 데이터 변환이 변경될 수 있습니다.

Tenable.sc 취약성 임포트

Tenable.sc 미해결 취약성 변환 맵은 Tenable.sc 미해결 취약성 통합에서 임포트한 데이터를 변환하는 데 사용되며, Tenable.sc 및 수정된 취약성 변환 맵은 Tenable.sc 해결된 취약성 통합에서 임포트된 데이터를 변환하는 데 사용됩니다.

주:
이러한 변환 맵을 변경하면 고정/미해결 Tenable 취약성 임포트의 데이터가 처리되는 방식이 변경됩니다.

Tenable.sc 미해결 및 수정된 취약성 변환 맵에 접근하려면 다음으로 이동하십시오. **Tenable** 취약성 통합 〉 관리 〉 통합 인스턴스 〉 **Tenable.sc** 고정/미해결 취약성 통합 〉 데이터 소스 〉 **Tenable.sc** 미해결/수정된 취약성 〉 변형.

소스 필드	대상 필드	설명
u_pluginID	ID	플러그인의 식별자로 사용됩니다. 이 필드는

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

소스 필드	대상 필드	설명
		외부 공급업체 항목 기록의 플러그인 ID에 매핑됩니다.
u_riskfactor	source_severity	이 필드는 외부 공급업체 항목 기록의 source_severity에 매핑됩니다.
u_severity	우선순위	우선순위 필드는 심각도와 매핑됩니다. 기본값은 5입니다.
u_hasbeenmitigated	상태	완화됨 취약성 기록의 상태 필드에 매핑됩니다. 수정된 취약성 통합의 경우 모든 VI가 "종결" 상태입니다.
u_ip	ip_address	IP 주소는 cmdb_ci 테이블의 호스트 IP 필드에 매핑됩니다.
u_port	포트	포트는 취약한 항목 기록의 포트 필드에 매핑됩니다.
u_protocol	프로토콜	프로토콜은 취약한 항목 기록의 포트 필드에 매핑됩니다.
u_firstSeen	first_found	첫 번째로 발견된 값은 VI 기록의 첫 번째 발견 필드에 매핑됩니다.
u_lastSeen	last_found	마지막으로 발견된 값은 VI 기록의 마지막으로 발견된 필드에 매핑됩니다.
u_exploitAvailable	익스플로잇	ExploitAvailable은 외부 공급업체 항목 기록의 익스플로잇 필드에 매핑됩니다.
u_synopsis	위협	시놉시스는 외부 공급업체 항목 기록의 위협 필드에 매핑됩니다.
u_description	요약	설명이 외부 공급업체 항목 기록의 요약 필드에 매핑됩니다.
u_solution	솔루션	솔루션은 외부 공급업체 항목 기록의 솔루션 필드에 매핑됩니다.
u_basescore	점수	BaseScore는 외부 공급업체 참가 기록의 점수 필드에 매핑됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

소스 필드	대상 필드	설명
u_temporalScore	temporal_score	임시 점수는 외부 공급업체 항목 기록의 임시 점수에 매핑됩니다.
u_cvssv3basescore	v3_base_score	Cvssv3basescore는 외부 공급업체 항목 레코드의 v3 기본 점수에 매핑됩니다.
u_cvsstemporalscore	v3_temporal_score	Cvssv3temporal 점수는 외부 공급업체 항목 레코드의 v3 temporal 점수에 매핑됩니다.
u_pluginpubdate	date_published	플러그인 게시 날짜는 외부 공급업체 항목 기록의 플러그인 게시 날짜에 매핑됩니다.
u_pluginmoddate	last_modified	마지막 수정 날짜는 외부 공급업체 항목 기록의 플러그인 마지막 수정 날짜에 매핑됩니다.
u_dnsname	fqdn	DnsName은 cmdb_ci 레코드의 FQDN 필드에 매핑됩니다.
u_macaddress	mac_address	MacAddress는 cmdb_ci 기록의 mac_address 필드에 매핑됩니다.
u_netbiosName	NetBIOS	NetbiosName은 cmdb_ci 레코드의 NETBIOS 필드에 매핑됩니다.
u_ip	ip	IP는 cmdb_ci 기록의 IP 필드에 매핑됩니다.
hostUniqueness	uuid	호스트 고유성은 필드에 매핑되지 않지만 호스트의 UUID를 결정하는 데 사용됩니다.
u_family	범주	플러그인의 제품군 객체에 있는 이름 필드를 외부 공급업체 항목 기록의 범주 열에 매핑합니다.
u_plugintext	증명	플러그인 텍스트는 TPE 기록의 증명에 매핑됩니다.
〔스크립트〕	소스	통합의 소스가 채워집니다. 이 통합에서 생성된 취약한 항목이 소스로 Tenable.sc.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

소스 필드	대상 필드	설명
〔스크립트}	integration_instance	integration_instance은 취약한 항목을 임포트한 인스턴스의 이름입니다.
u_vpr_score	source_risk_score	스캐너의 VPR 점수를 외부 공급업체 항목 테이블의 소스 위험 점수에 매핑합니다.
〔스크립트〕	source_risk_rating	점수 범위를 기준으로 VPR 점수를 표준 위험 등급에 매핑합니다. • 9 – 10 – 중요 • 7 – 9 – 높음 • 4–7 – 중간 • 0–4 - 낮음
u_vpr_context〔id=age_of_vuln〕	age_of_vuln	취약성의 기간을 스캐너의 외부 공급업체 항목 테이블에 age_of_vuln 매핑합니다.
u_vpr_context〔id=exploit_code_maturity〕	exploit_code_maturity	스캐너에서 외부 공급업체 항목 테이블의 exploit_code_maturity 악용 코드 성숙도를 매핑합니다.
u_vpr_context〔id=product_coverage〕	product_coverage	스캐너의 제품 범위를 외부 공급업체 항목 테이블의 product_coverage 매핑합니다.
u_vpr_context〔id="threat_sources_last_28〕	threat_sources	스캐너에서 지난 28일 동안의 위협 소스를 외부 공급업체 테이블의 threat_sources 매핑합니다.
u_vpr_context〔id="threat_intensity_last_28〕	threat_intensity	스캐너에서 외부 공급업체 항목 테이블의 threat_intensity 지난 28일 동안의 위협 강도를 매핑합니다.
u_vpr_context〔id="threat_recency"〕	threat_recency	스캐너의 위협 최신성 정보를 타사 항목 테이블의 threat_recency 매핑합니다.
u_vpr_context〔id=cvssV3_impactScore〕	v3_impact_subscore	스캐너의 CVSS v3 영향 점수를 외부 공급업체 항목 테이블의

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

소스 필드	대상 필드	설명
		v3_impact_subscore 매핑합니다.
u_pluginname	이름	플러그인 이름을 외부 공급업체 항목 테이블의 이름 열에 매핑합니다.
u_stigseverity	stig_severity	플러그인의 stig_severity 필드를 외부 공급업체 항목 테이블의 stig_severity 매핑합니다.
u_checktype	check_type	검사 유형을 외부 공급업체 항목 테이블의 check_type에 매핑합니다.
u_family.id	family_id	플러그인 family.id 외부 공급업체 항목 테이블의 family_id에 매핑합니다.
〔스크립트〕	exploit_attack_vector	third_party_entry 테이블의 exploit_attack_vector 열은 열의 exploit_available 및 v3_attack_vector 따라 채워집니다.

소스 필드	설명
u_cve	CVE 관련 데이터를 참조 테이블(sn_vul_nvd_entry)에 삽입합니다. NVD 항목 테이블(sn_vul_nvd_entry)에서 동일한 CVE가 발견되면 현재 취약성을 NVD 항목에 연결합니다. 매핑은 sn_vul_m2m_entry_cve에서 찾을 수 있습니다.
u_bid	버그 트랙 목록이 참조로 추가됩니다.
u_cpe	CPE 목록이 참조로 추가됩니다.
u_seealso	URL 목록이 참조로 추가됩니다.
u_xrefs	X-REF의 목록이 참조로 추가됩니다.
u_exploitframeworks	해당 플러그인에 대한 익스플로잇 목록 및 해당 익스플로잇 프레임워크에 대한 매핑 sn_vul_m2m_framework_vul 삽입합니다.

변환 프로세스 중에 실행되는 세 가지 변환 스크립트가 있습니다. 다음 표에는 각 스크립트가 실행되는 시기와 용도가 나와 있습니다.

스크립트가 실행될 때	목적
onStart(임포트 세트가 변환을 시작한 경우)	이 변환은 통합 프로세스에 대한 import_set의 값을 초기화하는 데 사용됩니다. 이 스크립트는

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

스크립트가 실행될 때	목적
	내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.
onBefore(임포트 세트가 변환을 완료하기 전)	취약성의 값을 업데이트하고 취약성이 존재하는지 확인하는 데 사용되는 기능입니다. 결과에 따라 취약한 항목 테이블의 값을 수정합니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.
onComplete(임포트 세트가 변환을 완료한 경우)	이 변환은 생성된 새 VI의 값과 업데이트 및 무시된 VI의 값을 설정하는 데 사용됩니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.

Tenable.cs 컨테이너 자산 임포트

임포트한 자산 데이터는 먼저 컨테이너 자산 임포트 [sn_vul_tenable_cs_container_asset_import] 테이블에 로드됩니다 Tenable.cs .

컨테이너 자산 변환 맵은 Tenable.cs 임포트한 자산 정보를 변환하는 데 사용됩니다. 이 변환을 변경하면 컨테이너 자산 임포트의 Tenable.cs 데이터가 처리되는 방식이 변경됩니다. 이 변환 맵에 액세스하려면 시스템 임포트 세트 > 변환 맵으로 이동합니다. Tenable.cs 컨테이너 자산 변환을 검색합니다.

다음 테이블에는 통합별 변환 맵 필드가 나열되어 있습니다.

Tenable.cs 컨테이너 자산 변환 맵 필드

소스 필드	대상 필드	설명
u_digest	Image_id	Tenable은 컨테이너 자산에 대한 고유 다이제스트를 제공하고 검색된 컨테이너 이미지 및 Docker 이미지 기록에 매핑되며 CI 조회에 사용됩니다.
u_digest	Image_digest	Tenable은 컨테이너 자산에 대한 고유 다이제스트를 제공하고 검색된 컨테이너 이미지 및 Docker 이미지 기록에 매핑되며 CI 조회에 사용됩니다.
u_name	이름	Docker 이미지 기록의 이름 필드에 매핑합니다.
u_repositoryuri	이름	컨테이너 리포지토리 기록에 매핑
u_repositoryuri	리포지토리	검색된 컨테이너 이미지 기록에 매핑합니다.
u_virtualmachines	host_list	검색된 컨테이너 이미지 기록에 매핑합니다.
u_labels	Image_labels	첫 번째 OS 값을 검색된 항목 기록의 os 필드에 매핑합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Tenable.cs 컨테이너 자산 변환 맵 필드

소스 필드	대상 필드	설명
u_clusters	image_cluster	검색된 컨테이너 이미지 기록에 매핑합니다.
u_imagetags	태그	검색된 컨테이너 이미지 기록에 매핑합니다.
u_cloudprovider	cloud_providers	검색된 컨테이너 이미지 기록에 매핑합니다.
u_accountid	cloud_account_ids	검색된 컨테이너 이미지 기록에 매핑합니다.
u_region	cloud_regions	검색된 컨테이너 이미지 기록에 매핑합니다.
u_operatingsystem	os	검색된 컨테이너 이미지 기록에 매핑합니다.
u_scantime	last_scan_date	검색된 컨테이너 이미지 기록에 매핑합니다.

변환 프로세스 중에 실행되는 세 가지 변환 스크립트가 있습니다. 다음 표에는 각 스크립트가 실행되는 시기와 용도가 나와 있습니다.

Tenable.cs 컨테이너 자산 변환 맵 스크립트 타이밍 및 목적

스크립트가 실행될 때	목적
onStart(임포트 세트가 변환을 시작한 경우)	이 변환은 통합 프로세스에 대한 import_set의 값을 초기화하는 데 사용됩니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.
onBefore(임포트 세트가 변환을 완료하기 전)	호스트의 값을 업데이트하고 호스트가 존재하는지 확인하는 데 사용되는 함수입니다. 결과에 따라 import_set의 값을 수정합니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.
onComplete(임포트 세트가 변환을 완료한 경우)	이 변환은 새로 생성된 CI와 업데이트 후 무시된 CI의 값을 설정하는 데 사용됩니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.

Tenable.cs 컨테이너 취약성 임포트

임포트된 컨테이너 취약성 데이터는 먼저 컨테이너 취약성 임포트 [sn_vul_tenable_cs_container_vuln_import] 테이블에 로드됩니다 Tenable.cs .

컨테이너 취약성 변환 맵은 Tenable.cs 임포트한 컨테이너 취약성 정보를 변환하는 데 사용됩니다. 이 변환을 변경하면 컨테이너 취약성 임포트의 Tenable.cs 데이터가 처리되는 방식이 변경됩니다. 이 변환 맵에 액세스하려면 다음으로 이동하십시오. 시스템 임포트 세트 〉 변환 맵. Tenable.cs 컨테이너 취약성 변환을 검색합니다.

다음 테이블에는 통합별 변환 맵 필드가 나열되어 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Tenable.cs 컨테이너 취약성 변환 맵 필드

소스 필드	대상 필드	설명
〔스크립트〕	Image_id	다이제스트는 API의 Resource.Id 필드에서 추출되어 검색된 컨테이너 이미지 및 Docker 이미지 기록의 image_id 필드에 매핑됩니다.
〔스크립트〕	Image_digest	다이제스트는 API의 Resource.Id 필드에서 추출되어 검색된 컨테이너 이미지 및 Docker 이미지 기록의 image_digest 필드에 매핑됩니다.
〔스크립트〕	이름	리포지토리 정보는 이름 필드에서 추출되어 Docker 이미지 및 컨테이너 리포지토리 기록에 매핑됩니다.
〔스크립트〕	리포지토리	리포지토리 정보는 이름 필드에서 추출되어 컨테이너 이미지 검색 기록에 매핑됩니다.
u_resource. 레이블	Image_labels	검색된 컨테이너 이미지 기록에 매핑합니다.
u_resource. 클라우드 제공자	cloud_providers	검색된 컨테이너 이미지 기록에 매핑합니다.
u_resource. AccountId	cloud_account_ids	검색된 컨테이너 이미지 기록에 매핑합니다.
u_resource. 부위	cloud_regions	검색된 컨테이너 이미지 기록에 매핑합니다.
u_vulnerability. ID	ID	소스에서 ID를 매핑하고 TEN- 접두사를 추가합니다. 예를 들어 수신된 ID가 12345인 경우 외부 공급업체 항목 테이블의 ID는 TEN-12345입니다.
u_vulnerability. 설명 ID	요약 ID	외부 공급업체 항목 기록에 매핑합니다. 또는 CVE 기록.
u_vulnerability. 심각도	v4_base_severity	외부 공급업체 항목 기록에 매핑합니다.
u_vulnerability. Vpr점수	source_risk_score	외부 공급업체 항목 기록에 매핑합니다.
u_vulnerability. VprSeverity	source_severity	외부 공급업체 항목 기록에 매핑합니다.
u_vulnerability. 공격 벡터	v4_attack_vector	외부 공급업체 항목 기록에 매핑합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Tenable.cs 컨테이너 취약성 변환 맵 필드

소스 필드	대상 필드	설명
u_vulnerability. 악용 성숙도	v4_exploit_maturity	외부 공급업체 항목 기록에 매핑합니다.
〔스크립트〕	소스	수입 TPE의 출처는 Tenable.cs입니다.
u_vulnerability. 아이디	이름	취약성 참조 기록에 매핑
u_vulnerability. 링크	URL	취약성 참조 기록에 매핑
	취약성	취약성 참조 기록의 TPE 또는 CVE 참조
u_software. 이름	이름	컨테이너 이미지 패키지 기록에 매핑
u_software. 버전	버전	컨테이너 이미지 패키지 기록에 매핑
u_software. 형	package_type	컨테이너 이미지 패키지 기록에 매핑
u_softwarepaths	path	컨테이너 이미지 패키지 기록에 매핑
u_resolved	상태	컨테이너 이미지 찾기 기록에 매핑
u_firstscantime	first_found	컨테이너 이미지 찾기 기록에 매핑
u_resource. 스캔 시간	last_found	컨테이너 이미지 찾기 기록에 매핑
u_vulnerability. 묘사	증명	컨테이너 이미지 찾기 기록에 매핑
u_resolved	상태	컨테이너 취약한 항목 기록에 매핑합니다.
u_firstscantime	first_found	컨테이너 취약한 항목 기록에 매핑합니다.
u_resource. 스캔 시간	last_found	컨테이너 취약한 항목 기록에 매핑합니다.
〔스크립트〕	소스	컨테이너 취약한 항목 기록의 소스는 입니다 Tenable.cs.

변환 프로세스 중에 실행되는 세 가지 변환 스크립트가 있습니다. 다음 표에는 각 스크립트가 실행되는 시기와 용도가 나와 있습니다.

Tenable.cs 컨테이너 취약성 변환 맵 스크립트 타이밍 및 목적

스크립트가 실행될 때	목적
onStart(임포트 세트가 변환을 시작한 경우)	임포트 세트를 사용하여 데이터를 Tenable.cs 임포트하고 각 기록을 CMDB CI 테이블, 취약한 항목 테이블, 외부 공급업체 취약성 항목 테이블, 취약성 참조 테이블, 컨테이너 이미지 패키지,

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Tenable.cs 컨테이너 취약성 변환 맵 스크립트 타이밍 및 목적

스크립트가 실행될 때	목적
	컨테이너 이미지 찾기 및 컨테이너 취약한 항목에 로드하는 TenableCS 컨테이너 취약성 프로세서를 트리거합니다. 수정하거나 삭제하는 것은 권장되지 않습니다.
onBefore(임포트 세트가 변환을 완료하기 전)	외부 공급업체 항목 및 이미지 결과가 있는지 확인합니다. 그렇지 않은 경우 이러한 기록은 해당 테이블에 생성됩니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.
onComplete(임포트 세트가 변환을 완료한 경우)	에서 Tenable.cs임포트한 CI, VIT 및 결과 수를 업데이트합니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.

Tenable.cs 취약성 임포트 계산

임포트된 호스트 취약성 데이터는 먼저 취약성 계산 [sn_vul_tenable_cs_compute_vuln_import] 테이블에 로드됩니다 Tenable.cs .

Compute Vuln 변환 맵은 Tenable.cs 임포트한 호스트 취약성 정보를 변환하는 데 사용됩니다. 이 변환을 변경하면 계산 취약성 임포트의 Tenable.cs 데이터가 처리되는 방식이 변경됩니다. 이 변환 맵에 액세스하려면 다음으로 이동하십시오. 시스템 임포트 세트 〉 시스템 임포트 세트. Tenable.cs 계산 취약성 변환을 검색합니다.

다음 표에는 통합별 변환 맵 필드가 나열되어 있습니다.

Tenable.cs 컨테이너 취약성 변환 맵 필드

소스 필드	대상 필드	설명
u_resource. 아이디	object_id	CMDB CI 기록에 매핑됩니다.
u_resource. 이름	이름	CMDB CI 기록에 매핑됩니다.
	asset_category	클라우드는 검색된 항목 기록에서 자산 범주로 매핑됩니다.
U_resource. 클라우드 제공자	cloud_service_provider	검색된 항목 기록에 매핑
u_resource. 부위	cloud_region	검색된 항목 기록에 매핑
u_resource. 계정 ID	cloud_account	검색된 항목 기록에 매핑
u_resource. CloudProvider	cloud_resource_type	검색된 항목 기록에 매핑
u_resource. 아이디	resource_id	검색된 항목 기록에 매핑
u_resource. 이름	resource_name	검색된 항목 기록에 매핑
u_vulnerability. 아이디	ID	소스에서 ID를 매핑하고 TEN- 접두사를 추가합니다. 예를 들어 수신된 ID가 12345인 경우 외부 공급업체 항목 테이블의 ID는 TEN-12345입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Tenable.cs 컨테이너 취약성 변환 맵 필드

소스 필드	대상 필드	설명
		ID를 CVE에도 매핑합니다.
u_vulnerability. 설명	요약	외부 공급업체 항목 기록에 매핑합니다.
u_vulnerability. 심각도	v4_base_severity	외부 공급업체 항목 기록에 매핑합니다.
u_vulnerability. Vpr점수	source_risk_score	외부 공급업체 항목 기록에 매핑합니다.
u_vulnerability. VprSeverity	source_severity	외부 공급업체 항목 기록에 매핑합니다.
u_vulnerability. 공격 벡터	v4_attack_vector	외부 공급업체 항목 기록에 매핑합니다.
u_vulnerability. 악용 성숙도	v4_exploit_maturity	외부 공급업체 항목 기록에 매핑합니다.
〔스크립트〕	소스	수입된 TPE의 출처는 Tenable.cs입니다.
u_vulnerability. 아이디	이름	취약성 참조 기록에 매핑
u_vulnerability. 링크	URL	취약성 참조 기록에 매핑
	취약성	취약성 참조 기록의 TPE 또는 CVE 참조
u_resolved	상태	취약한 항목 탐지 기록에 매핑합니다.
u_firstscantime	first_found	취약한 항목 탐지 기록에 매핑합니다.
u_resource. 스캔 시간	last_found	취약한 항목 탐지 기록에 매핑합니다.
u_softwarepaths	증명	취약한 항목 탐지 기록에 매핑합니다.
u_softwareresolutionversions	solution_summary	취약한 항목 탐지 기록에 매핑합니다.
u_resolved	상태	취약한 항목 기록에 매핑
u_firstscantime	first_found	취약한 항목 기록에 매핑
u_resource. 스캔 시간	last_found	취약한 항목 기록에 매핑
〔스크립트〕	소스	취약한 항목 기록의 소스는 입니다 Tenable.cs.

변환 프로세스 중에 실행되는 세 가지 변환 스크립트가 있습니다. 다음 표에는 각 스크립트가 실행되는 시기와 용도가 나와 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Tenable.cs 취약성 계산 변환 맵 스크립트 타이밍 및 목적

스크립트가 실행될 때	목적
onStart(임포트 세트가 변환을 시작한 경우)	임포트 세트를 사용하여 데이터를 Tenable.cs 임포트하고 각 기록을 CMDB CI 테이블, 취약한 항목 테이블 및 외부 공급업체 취약성 테이블로 로드하는 Tenable CS 계산 취약성 프로세서를 트리거합니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.
onBefore(임포트 세트가 변환을 완료하기 전)	외부 공급업체 항목 및 탐지가 있는지 확인합니다. 그렇지 않은 경우 이러한 기록은 해당 테이블에 생성됩니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.
onComplete(임포트 세트가 변환을 완료한 경우)	에서 Tenable.cs임포트한 CI, VIT 및 탐지 수를 업데이트합니다. 이 스크립트는 내부용이며 수정하거나 삭제하는 것은 권장되지 않습니다.

Tenable.cs 컨테이너 취약성 변환 맵 필드

소스 필드	대상 필드	설명
u_digest	Image_id	컨테이너 자산에 대해 Tenable에서 제공하는 고유 다이제스트입니다. 검색된 컨테이너 이미지 및 Docker 이미지 기록에 매핑되며 CI 조회에 사용됩니다.
u_name	이름	Docker 이미지 기록의 이름 필드에 매핑합니다.

임포트에 대한 **Tenable.io** 추가 필터 매개변수 설정

를 Tenable Vulnerability Integration 사용하여 예약된 쿼리에 대한 필터링 매개변수를 사용자 지정하면 제품과 함께 Tenable.io 임포트하는 취약성 데이터를 더욱 세분화할 수 있습니다.

시작하기 전에
사용 사례: 취약성 관리자 또는 분석가는 특정 취약성 상세 정보만 검토할 수 있도록 쿼리에서 데이터를 필터링할 수 있습니다. 예를 들어 , `num_assets`, , `indexed_at`및 로 필터링`cidr_range`되는 임포트된 취약성을 보려고 한다고 `plugin_family`가정해 보겠습니다. 또는 한 실행은 4시간마다 중요한 취약성만 가져오고 다른 실행은 24시간마다 실행하여 중요하지 않은 다른 모든 취약성을 가져오도록 통합을 실행 Tenable.io 하려고 한다고 가정해 보겠습니다.

이 데이터를 수집하는 데 도움이 되도록 필요한 특정 취약성 상세 정보를 가져오는 데 도움이 되는 tenable 지원 매개변수를 추가할 수 있습니다.

이 기능을 사용하면 ServiceNow AI PlatformAPI 호출이나 코딩을 추가하지 않고도 . 다음 Tenable.io 통합은 요청 본문에 JSON 컨텐츠를 제공하여 필터링을 지원합니다.

- 자산 통합
- 수정된 취약성 통합
- 미해결 취약성 통합

이 기능에 문자열을 사용하는 JSON 방법을 알아야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필요한 역할: sn_vul.vulnerability_admin

프로시저

1. 필터링에 사용할 개발자 사이트의 제품에서 Tenable.io 지원하는 매개변수를 찾습니다.

   제품에서 Tenable.io 입력하는 매개변수와 값은 통합 인스턴스 수준에서만 지원됩니다.

2. 다음으로 이동 모두 〉 **Tenable** 취약성 통합 〉 관리 〉 통합.
3. Tenable 통합 목록 페이지에서 열려는 통합에 Tenable.io 대한 기록을 클릭합니다.
4. Tenable REST 메서드 탭을 선택한 상태에서 REST 메서드에 대한 정보 아이콘(i)을 클릭한 다음 기록 열기를 클릭합니다.
5. **HTTP** 요청 탭을 선택합니다.
6. 기록을 편집하려면 페이지 상단에 있는 링크를 클릭하십시오. 기록을 편집하려면 여기를 클릭하십시오.
7. REST 메서드 기록의 컨텐츠 필드에 요청 본문의 일부로 사용할 JSON 컨텐츠를 입력합니다.

   예를 들어, 자산 통합에서 중요한 취약성(CVSS 점수 10.0)만 임포트하도록 임포트한 취약성에 대한 Tenable.io 심각도 매개변수를 다음과 같이 `{"filters": {"severity": ["critical"]}}` 설정할 수 있습니다.

   둘 이상의 매개변수를 입력하려면 각 값을 구분하는 방법에 대한 자세한 내용은 설명서를 참조하십시오 Tenable.io .

8. 업데이트를 클릭합니다.

Tenable 취약성 통합 보고

대시보드에서 취약성 대응 취약성 및 취약한 항목에 대한 보고서를 봅니다.

작업 공간의 데이터 시각화 취약성 대응

작업 공간에는 취약성 대응 정정 진행 상황을 모니터링하는 데 도움이 될 수 있는 데이터 시각화가 포함되어 있습니다. 취약성 데이터가 변경될 때 업데이트되는 동적 데이터 시각화에서 조직에 중요한 활성 취약성의 수와 심각도를 확인하여 조직에 대한 위협 수준을 확인할 수 있습니다. 취약성 관리자 작업 공간 살펴보기IT 정정 작업 공간 살펴보기 를 참조취약성 대응 작업 공간하고 사용 가능한 동적 데이터 시각화에 대한 자세한 내용을 확인할 수 있습니다.

이전 버전 취약성 대응

Vulnerability Response 개요 대시보드(취약성 관리)는 취약성 및 취약한 항목에 대한 경영적 뷰를 제공하여 취약성 관리자가 관심 영역을 신속하게 찾아낼 수 있도록 도와줍니다. 취약성 대응 정정 대시보드(취약성 정정)를 사용하면 정정 전문가가 소유한 정정 작업과 취약한 항목에 집중할 수 있습니다.

자세한 내용은 기본 취약성 대응 대시보드 사용 문서를 참조하십시오.

필요한 역할: 정정 소유자.

가상 사용자 및 세분화된 역할을 사용하여 사용자가 Vulnerability Response 애플리케이션에서 확인하고 수행할 수 있는 내용을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할을 처음 할당하려면 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당.

세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

대시보드를 보려면 다음으로 이동합니다. 취약성 대응 〉 정정 개요.

Tenable 취약성 통합에 대한 통합 실행 상태 차트

Tenable 통합 실행 상태 모듈은 Tenable 통합 실행의 상태에 대한 그래픽 보기를 제공합니다.

차트에서 그래프의 특정 부분을 가리키면 해당 부분과 관련된 데이터 요약이 표시됩니다. 막대 그래프에서 부품을 클릭하면 더 자세한 정보를 제공하는 목록이 열립니다.

필요한 역할: 취약성 관리자.

가상 사용자 및 세분화된 역할을 사용하여 사용자가 Vulnerability Response 애플리케이션에서 확인하고 수행할 수 있는 내용을 관리할 수 있습니다. 설정 도우미에서 가상 사용자 역할을 처음 할당하려면 문서를 참조하십시오 설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당.

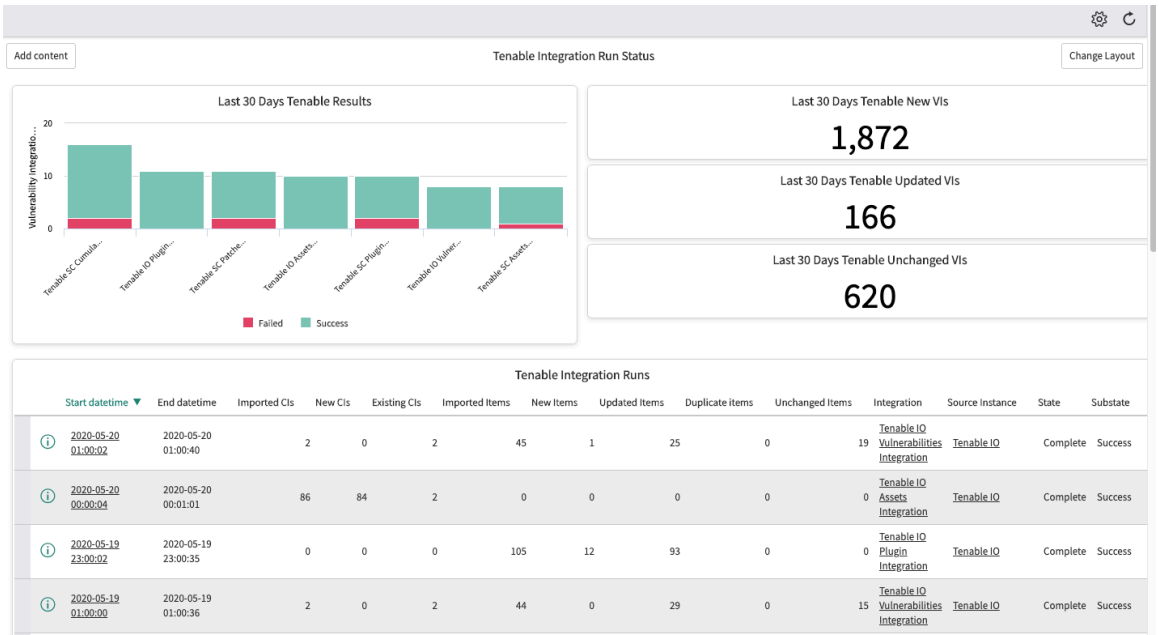
세분화된 역할 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 의 가상 사용자 및 세분화된 역할 관리 취약성 대응.

데이터를 보려면 다음으로 이동합니다. 모두 〉 **Tenable** 취약성 통합 〉 통합 실행 상태.

의 취약성 대응버전 19.0부터 이 대시보드는 New Experience UI에서 사용할 수 있습니다.

주:
Tokyo에 있는 경우 Next Experience UI에서 대시보드를 볼 수 있지만 일부 기능 손실이 있습니다.

실행 상태



Tenable 통합 실행 상태 차트 보고서

이름	설명
지난 30일 Tenable 결과	각 통합에 대해 완료된 통합 실행 수입니다. 성공한 실행과 실패한 실행을 모두 표시합니다. 각 실행은 그래프에 막대로 표시됩니다.
지난 30일 Tenable 신규 VI	지난 30일 동안 임포트된 새로운 취약한 항목 수입니다. 정수로 표시됩니다.

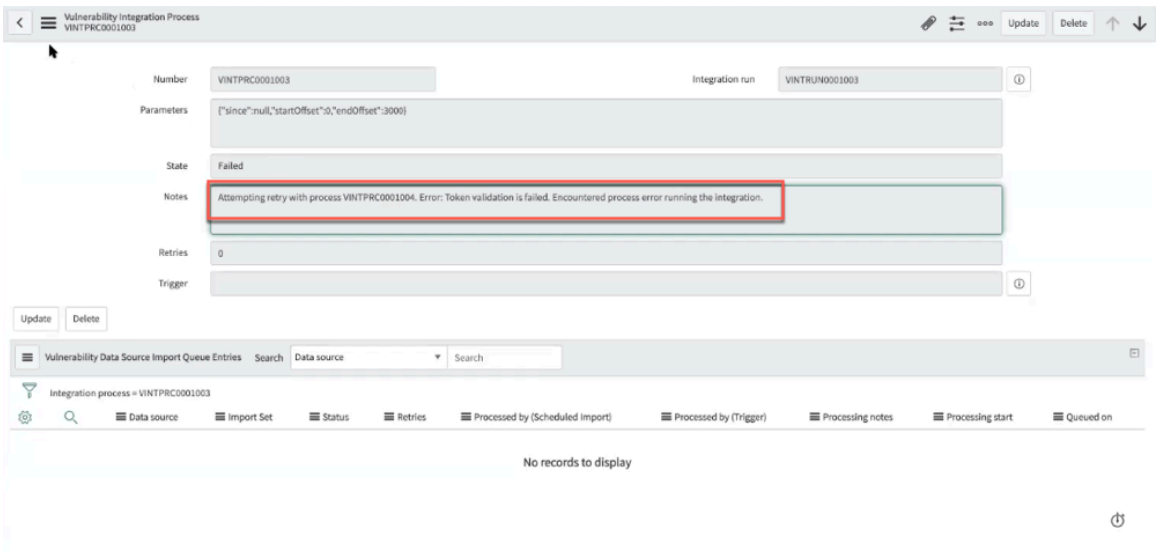
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이름	설명
지난 30일 Tenable 업데이트된 VI	지난 30일 동안 임포트된 업데이트된 취약한 항목 수입니다. 정수로 표시됩니다.
지난 30일 Tenable 미변경 VI	지난 30일 동안 임포트된 중복 취약한 항목 수입니다. 정수로 표시됩니다.
Tenable 통합 실행	통합 실행 기록이 목록에 표시됩니다. 주: **V16.1:** 이 통합에 대한 탐지를 확인하려면 탐지 또는 결과를 ServiceNow 테이블의 탐지 데이터와 *sn_vul_detection* 비교합니다. 통합이 진행되는 동안 탐지 또는 발견 개수가 변경될 수 있습니다. 이 보고서는 통합 실행이 완료된 후 인스턴스의 "종료 날짜 카운트" 열에 탐지 횟수를 표시합니다.

토큰 확인 만료

어떤 이유로든 Tenable.sc 통합 실행이 실패하면 Tenable.sc 에 대한 인증 토큰이 자동으로 만료되고 취약성 통합 프로세스 기록에 메시지가 표시됩니다.

만료된 토큰 메시지



다음 통합 프로세스를 위해 새 토큰이 자동으로 생성됩니다. 모든 통합 프로세스(실패 및 성공)가 취약성 통합 프로세스 기록의 취약성 통합 프로세스 탭에 표시됩니다.

통합에 대한 **Tenable.sc** 재스캔 시작

Tenable 플랫폼에서 다시 스캔을 시작하여 예약된 스캔 주기 사이에 취약한 항목이 정정되었는지 확인합니다. 인스턴스에서 제품의 취약한 항목에 대한 요청 시 재스캔을 Tenable.sc 시작할 수 있습니다 ServiceNow AI Platform# .

시작하기 전에
필요한 역할: sn_vul.write_all 또는 sn_vul.write_assigned

주:
Tenable.sc 은 에이전트 기반 컴퓨터에서 다시 스캔 실행을 지원하지 않습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에 스캐너가 활성화되어 있는지 확인하십시오. 다음으로 이동 취약성 대응 〉 취약성 스캐닝 〉 스캐너.

이 태스크 정보

작업 공간에서 다시 스캔을 시작하려면 다음 문서를 참조하십시오 작업 공간에서 취약성 대응 취약한 항목 다시 스캔 Tenable.ioTenable.sc.

아래 나열된 단계에 따라 클래식 환경에서 재검색을 시작합니다.

예약된 전체 검사와 관련된 오버헤드와 볼륨을 줄이기 위해 정정 소유자, IT 전문가, 취약성 분석가 또는 취약성 관리자는 해당 환경에서 자산(구성 항목)의 특정 취약성에 대한 요청 시 대상 재검사를 시작할 수 있습니다. VI(취약한 항목), RT(정정 작업), TPE(외부 공급업체 항목) 또는 인스턴스에서 검색된 항목 기록에서 다시 스캔을 시작할 수 있습니다 ServiceNow AI Platform .

재검사를 통해 정정 소유자와 취약성 분석가는 정정 활동, 패치 및 기타 작업이 구성 항목(CI)의 특정 취약성을 성공적으로 수정했는지 확인할 수 있습니다.

예를 들어, 전체 환경은 3주에 한 번씩 검사됩니다. 가장 최근의 전체 검사는 일주일 전에 완료되었지만 중요한 취약성을 수정하기 위해 어제 패치를 적용했습니다. 이 취약성의 특성으로 인해 다음 예약된 검사에서 정정되었는지 확인할 때까지 2주를 기다릴 수 없습니다. 패치가 이전 검사 중에 발견된 중요 취약성을 성공적으로 수정했는지 확인하기 위해 취약한 항목에 대한 Tenable.sc 대상 재스캔 ServiceNow AI Platform 을 시작할 수 있습니다.

주:
인스턴스에서 재스캔을 ServiceNow AI Platform# 요청할 때 자격 증명을 선택하는 Vulnerability Response Integration with Tenable 것은 선택 사항입니다. 스캔 자격 증명 통합은 ServiceNow# Tenable.sc 인스턴스의 제품에서 Tenable.sc 스캐너 자격 증명을 임포트하고 업데이트합니다. 이 통합은 매주 실행되어 Tenable 자격 증명 데이터를 임포트하고 안전하게 저장합니다.

임포트된 이 데이터에는 Tenable 암호 또는 기타 민감한 Tenable 계정 정보가 포함되지 않습니다. ServiceNow# Tenable.sc 취약성 통합(Tenable.sc미해결 및 수정된 취약성 통합)을 구성할 때 인스턴스의 설정 도우미 내에서 검사 자격 증명 통합이 자동으로 활성화(##)됩니다Tenable.sc.

임포트하는 자격 증명에 대한 다음 정보를 기록해 두십시오. 그래야 사용자가 인스턴스에서 필요할 ServiceNow AI Platform 때 볼 수 있습니다.

- 관리자 사용자 역할로 만든 자격 증명은 Tenable.sc 모든 조직의 사용자가 사용할 수 있습니다.
- 조직 사용자 역할로 Tenable.sc 만든 자격 증명은 해당 조직 내의 사용자만 사용할 수 있습니다. 이러한 자격 증명은 인스턴스에 연결하는 데 사용되는 사용자 계정과 공유되지 않는 한 작성자의 조직 외부에 있는 사용자용 계정으로 임포트 ServiceNow AI Platform 되지 않습니다.

자세한 내용은 설명서 웹 사이트를 Tenable.sc 참조하십시오.

애플리케이션 구성에 Tenable.sc 대한 자세한 내용은 을 참조하십시오설정 도우미를 사용하여 Tenable 취약성 통합 구성. 검사 자격 증명 통합에 대한 자세한 내용을 보려면 다음으로 이동하십시오. 모두 〉 **Tenable** 취약성 통합 〉 통합 〉 **Tenable.sc** 스캔 자격 증명 통합.

통합 실행 중에 여러 프로세스가 생성되고 데이터가 페이지 형식으로 수신됩니다. 각 프로세스에는 페이지에 첨부된 데이터가 있는 하나 이상의 임포트 큐 항목이 포함될 수 있습니다. 이러한 항목은 1시간의 시간 제한 내에 데이터를 처리해야 합니다. 그러나 페이로드 크기가 크면 처리 시간이 1시간을 초과하거나 중단되어 통합 시간 제한 오류가 발생할 수 있습니다. 통합은 시간 초과 오류에도 불구하고 데이터를 계속 처리합니다. 이러한 잘못된 통신을 피하기 위해 버전 18.2.4 취약성 대응부터 큐가 활성 상태이고 데이터를 처리하는지 여부를 나타내기 위해 타임스탬프(하트비트)가 주기적으로 전송됩니다. 임포트 큐 항목 페이지의 처리된 마지막 기록 필드는 임포트

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

큐가 생성하거나 업데이트하는 기록 수에 따라 업데이트됩니다. 임포트 큐 항목이 1시간의 시간 제한을 초과하는 경우, 시스템은 마지막으로 처리된 기록 필드를 검사하여 1시간보다 오래되었는지도 확인합니다. 이 경우 이는 임포트 큐 항목이 고착되었음을 나타내며 처리 시 더 이상의 지연을 방지하기 위해 시간 초과됩니다.

주:
마지막으로 처리된 기록 필드는 다음 시스템 속성에 정의된 내용에 따라 업데이트됩니다.

- *sn_sec_cmn.record_threshold_heartbeat*: 하트비트(타임스탬프)가 임포트 큐 항목으로 전송된 후 처리된 기록 수를 정의합니다.
- *sn_sec_cmn.maximum_heartbeat_delay*: 임포트 큐 항목을 시간 초과해야 하는 시간을 정의합니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 취약한 항목.
2. 다시 스캔을 트리거할 취약한 항목 기록을 찾아 엽니다.

   주:
   VI Tenable.sc 에 대한 재스캔만 소스로 시작할 수 있습니다. 확인 Tenable.sc 이 VI 목록 뷰의 소스 열 또는 개별 기록의 소스 필드에 표시됩니다. 조건 빌더를 사용하여 소스별로 VI를 그룹화할 수 있습니다. 또는 소스 열이 VI 목록 뷰에 표시되지 않은 경우 목록의 왼쪽 상단에서 목록 개인화 아이콘(기어 아이콘)을 클릭하고 슬러 시버킷을 사용하여 소스를 사용 가능 에서 선택됨으로 이동합니다.

3. 또는 다음으로 이동합니다. 모두 〉 취약성 대응 〉 정정 작업 또는 취약성 대응 〉 라이브러리 〉 외부 공급업체 각각 다시 검색에 사용할 정정 작업 또는 외부 공급업체 항목 기록의 경우

   선택에 따라 다음 기록에서 다시 스캔 버튼을 사용할 수 있습니다.

   - 단일 VI 기록에서 VI는 제품에서 나온 Tenable.sc 것이어야 하며 종결 이외의 상태여야 합니다. 여러 VI 레코드의 경우 모든 VI는 Tenable.sc 제품에서 가져온 것이어야 하며 종결 이외의 상태여야 합니다.
   - RT 레코드에서 정정 작업은 종결 이외의 모든 상태일 수 있으며 연결된 모든 VI는 제품에서 가져와야 Tenable.sc 합니다.
   - 타사 항목(TPE) 레코드에서 레코드에는 종결 이외의 상태인 제품의 연결된 VI 레코드가 Tenable.sc 하나 이상 있어야 합니다.

4. 기록의 오른쪽 상단에서 Rescan(다시 스캔)을 클릭합니다.
   스캐너에 액세스하기 위해 스캐너 자격 증명을 선택하라는 메시지가 표시됩니다. 스캔 자격 증명 통합에서 임포트한 자격 증명입니다 Tenable.sc .
5. 대화 상자에서 원하는 필터와 자격 증명 유형을 선택합니다.
6. 스캔 요청을 클릭합니다.

   스캔이 처리 중임을 나타내는 메시지가 표시됩니다. 모든 재스캔의 상태는 재스캔을 시작하는 데 사용한 VI, RT, TPE 기록의 스캔 관련 목록에서 언제든지 확인할 수 있습니다. 메시지에서 세부 정보 보기를 클릭하여 다시 스캔 상태를 확인하고 지정된 기록에서 시작된 다른 다시 스캔을 봅니다.

   모든 하위 스캔이 성공적으로 완료되면 상위 스캔 기록의 상태 필드가 완료로 표시됩니다. 하위 스캔 임포트 데이터. 상위 스캔 기록은 하위 스캔을 위한 컨테이너입니다.

   인스턴스는 ServiceNow AI Platform# 재스캔 상태가 성공적으로 완료될 때까지, 또는 설정된 추적 기간이 초과될 때까지(먼저 발생하는 쪽 적용) 재스캔 상태를 추적합니다. 시간 제한은 검사를

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

중지하지 않습니다. 시간 제한은 실제 다시 검색이 중지된 시간이 아니라 다시 스캔 상태 추적이 ServiceNow AI Platform# 중지된 시기를 나타냅니다. 종결/고정으로 전환되었거나 전환될 모든 VI는 Tenable.sc Fixed Vulnerabilities Integration의 다음 예약된 임포트와 함께 임포트됩니다.

통합에 대한 **Tenable.io** 재스캔 시작

Tenable 플랫폼에서 다시 스캔을 시작하여 예약된 스캔 주기 사이에 취약한 항목이 정정되었는지 확인합니다. 인스턴스에서 제품의 취약한 항목에 대한 요청 시 재스캔을 Tenable.io 시작할 수 있습니다 ServiceNow AI Platform# .

시작하기 전에
필요한 역할: sn_vul.write_all 또는 sn_vul.write_assigned

시작하기 전에 스캐너가 활성화되어 있는지 확인하십시오. 다음으로 이동 취약성 대응 〉 취약성 스캐닝 〉 스캐너.

이 태스크 정보

- Vulnerability Response 작업 공간에서 다시 스캔을 시작하려면 다음을 에서 기록 및 정정 작업을 다시 스캔 취약성 관리자 작업 공간에서 취약한 항목 및 정정 작업 다시 스캔 IT 정정 작업 공간 참조하십시오.
- 아래 나열된 단계에 따라 클래식 환경에서 재검색을 시작합니다.

주:
Tenable.io 은 에이전트 기반 컴퓨터에서 다시 스캔 실행을 지원하지 않습니다.

예약된 전체 검사와 관련된 오버헤드와 볼륨을 줄이기 위해 정정 소유자, IT 전문가, 취약성 분석가 또는 취약성 관리자는 요청 시 대상 재검사를 시작할 수 있습니다. 사용자 환경에서 자산(구성 항목)의 특정 취약성을 스캔할 수 있습니다. 인스턴스의 VI(취약한 항목), VUL(정정 작업), TPE(외부 공급업체 항목) 또는 SDI(검색된 항목) 기록에서 재스캔을 시작할 수 있습니다 ServiceNow AI Platform . 재검색을 통해 정정 활동, 패치 및 기타 작업이 구성 항목(CI)의 특정 취약성을 성공적으로 수정했는지 확인할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
인스턴스에서 재스캔을 ServiceNow AI Platform# 요청할 때 자격 증명을 선택하는 Vulnerability Response Integration with Tenable 것은 선택 사항입니다. 스캔 자격 증명 통합은 ServiceNow# Tenable.io 인스턴스의 제품에서 Tenable.io 스캐너 자격 증명을 임포트하고 업데이트합니다. 이 통합은 매주 실행되어 Tenable 자격 증명 데이터를 임포트하고 안전하게 저장합니다.

임포트된 이 데이터에는 Tenable 암호 또는 기타 민감한 Tenable 계정 정보가 포함되지 않습니다.

다음 정보는 인스턴스에서 필요할 ServiceNow AI Platform 때 사용자가 볼 수 있도록 임포트하는 자격 증명에 대해 설명합니다.

- 관리자 사용자 역할로 만든 자격 증명은 Tenable.io 모든 조직의 사용자가 사용할 수 있습니다.
- 조직 사용자 역할로 Tenable.io 만든 자격 증명은 해당 조직 내의 사용자만 사용할 수 있습니다. 이러한 자격 증명은 인스턴스에 연결하는 데 사용되는 사용자 계정과 공유되지 않는 한 작성자의 조직 외부에 있는 사용자용 계정으로 임포트 ServiceNow AI Platform 되지 않습니다.

  자세한 내용은 설명서 웹 사이트를 Tenable.io 참조하십시오.

- Tenable.io 재스캔을 시작하기 전에 템플릿 통합과 Tenable.io 스캔 자격 증명 통합을 활성화해야 합니다. 검사 자격 증명 통합에 대한 자세한 내용을 보려면 다음으로 이동하십시오. **Tenable** 취약성 통합 〉 통합 〉 **Tenable.io** 스캔 자격 증명 통합.

  기본적으로 템플릿 및 스캔 자격 증명 통합은 비활성화되어 있습니다. 에 대한 Tenable.io자격 증명을 입력하면 모든 Tenable.io 통합이 자동으로 활성화됩니다. 통합을 수동으로 활성화하거나 비활성화하려면 다음을 수행합니다.

  1. 다음으로 이동 모두 〉 **Tenable** 취약성 통합 〉 관리 〉 통합.
  2. 표시되는 목록에서 원하는 통합 기록을 찾습니다 Tenable.io .
  3. 통합을 활성화하려면 각 기록을 열고 활성 확인란을 선택합니다.
  4. 변경 사항을 저장하려면 업데이트를 클릭합니다.
  5. 설정 도우미로 돌아가 에 취약성 대응대한 Tenable Vulnerability Integration 구성을 계속합니다.

및 제품 구성에 Tenable.io 대한 자세한 내용은 을 Tenable.sc 참조하십시오설정 도우미를 사용하여 Tenable 취약성 통합 구성.

전체 환경이 3주에 한 번씩 스캔된다고 가정해 보겠습니다. 가장 최근의 전체 검사는 일주일 전에 완료되었지만 중요한 취약성을 수정하기 위해 어제 패치를 적용했습니다. 이 취약성의 특성으로 인해 다음 예약된 검사에서 정정되었는지 확인할 때까지 2주를 기다릴 수 없습니다. 패치가 이전 검사 중에 발견된 중요 취약성을 성공적으로 수정했는지 확인하기 위해 취약한 항목에 대한 Tenable.io 대상 재스캔 ServiceNow AI Platform 을 시작할 수 있습니다.

수정된 취약성 통합의 다음 예약된 임포트 후에 검사를 시작한 기록에 대한 업데이트된 결과를 볼 수 있습니다.

통합 실행 중에 여러 프로세스가 생성되고 데이터가 페이지 형식으로 수신됩니다. 각 프로세스에는 페이지에 첨부된 데이터가 있는 하나 이상의 임포트 큐 항목이 포함될 수 있습니다. 이러한 항목은 1시간의 시간 제한 내에 데이터를 처리해야 합니다. 그러나 페이로드 크기가 크면 처리 시간이 1시간을 초과하거나 중단되어 통합 시간 제한 오류가 발생할 수 있습니다. 통합은 시간 초과 오류에도 불구하고 데이터를 계속 처리합니다. 이러한 잘못된 통신을 피하기 위해 버전 18.2.4 취약성 대응부터 큐가 활성 상태이고 데이터를 처리하는지 여부를 나타내기 위해 타임스탬프(하트비트)가 주기적으로 전송됩니다. 임포트 큐 항목 페이지의 처리된 마지막 기록 필드는 임포트 큐가 생성하거나 업데이트하는 기록 수에 따라 업데이트됩니다. 임포트 큐 항목이 1시간의 시간

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

제한을 초과하는 경우, 시스템은 마지막으로 처리된 기록 필드를 검사하여 1시간보다 오래되었는지도 확인합니다. 이 경우 이는 임포트 큐 항목이 고착되었음을 나타내며 처리 시 더 이상의 지연을 방지하기 위해 시간 초과됩니다.

주:
마지막으로 처리된 기록 필드는 다음 시스템 속성에 정의된 내용에 따라 업데이트됩니다.

- *sn_sec_cmn.record_threshold_heartbeat*: 하트비트(타임스탬프)가 임포트 큐 항목으로 전송된 후 처리된 기록 수를 정의합니다.
- *sn_sec_cmn.maximum_heartbeat_delay*: 임포트 큐 항목을 시간 초과해야 하는 시간을 정의합니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 취약한 항목.
2. 다시 스캔을 트리거할 취약한 항목 기록을 찾아 엽니다.

   주:
   스캐너를 Tenable.io 사용하는 경우 VI에 대한 재스캔만 소스로 시작할 Tenable.io 수 있습니다. 확인 Tenable.io 이 VI 목록 뷰의 소스 열 또는 개별 기록의 소스 필드에 표시됩니다. 조건 빌더를 사용하여 소스별로 VI를 그룹화할 수 있습니다. 또는 소스 열이 VI 목록 뷰에 표시되지 않은 경우 목록의 왼쪽 상단에서 목록 개인화 아이콘(기어 아이콘)을 클릭하고 슬러 시버킷을 사용하여 소스를 사용 가능 에서 선택됨으로 이동합니다.

3. 또는 다음으로 이동합니다. 모두 〉 취약성 대응 〉 정정 작업 또는 취약성 대응 〉 라이브러리 〉 외부 공급업체 재스캔에 사용할 기록의 경우.

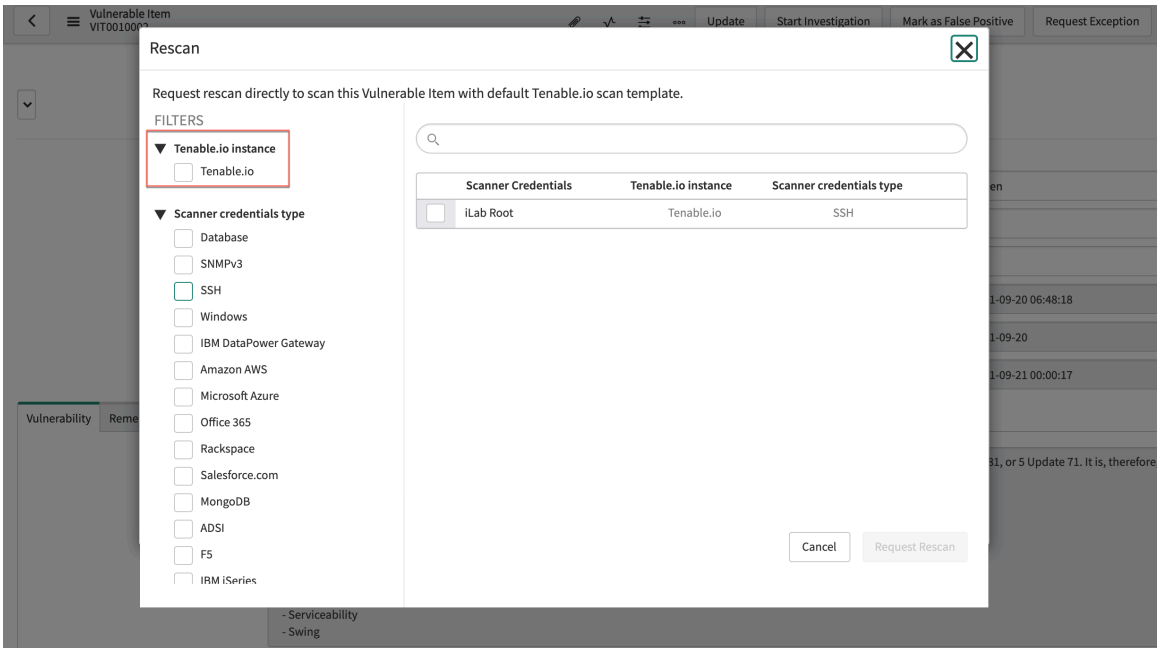
   선택에 따라 다음 기록에서 다시 스캔 버튼을 사용할 수 있습니다.

   - 단일 VI 기록에서 VI는 종결 이외의 상태여야 합니다. 여러 VI 레코드의 경우 모든 VI는 제품에서 가져온 Tenable.io 것이어야 하며 종결 이외의 상태여야 합니다.
   - 정정 작업 기록의 경우 종결 됨 이외의 상태에 있는 정정 작업만 지원됩니다. 연결된 모든 VI는 종결 이외의 상태여야 하며 소스로 사용 Tenable.io 되어야 합니다.
   - 타사 항목(TPE) 레코드에서 레코드에는 종결 이외의 상태인 제품의 연결된 VI 레코드가 Tenable.io 하나 이상 있어야 합니다.
   - 검색된 항목 기록에서 기록에는 종결 이외의 상태인 제품의 연결된 VI 기록 Tenable.io 이 하나 이상 있어야 합니다.
   - 취약한 항목 목록에서 다시 스캔하려는 개별 취약한 항목을 선택할 수 있습니다. 화면 왼쪽 아래에 있는 선택한 행에 대한 작업 메뉴를 사용하여 다시 검색을 시작합니다. 자격 증명을 입력하라는 메시지가 나타납니다.

4. 기록의 오른쪽 상단에서 Rescan(다시 스캔)을 클릭합니다.
   다시 스캔할 인스턴스와 스캐너에 액세스하는 데 사용할 스캐너 자격 증명을 선택하라는 메시지가 표시됩니다. 표시된 자격 증명은 검사 자격 증명 통합에서 Tenable.io 가져온 자격 증명입니다.
5. 대화 상자에서 인스턴스 및/또는 인스턴스와 사용할 자격 증명 유형을 선택합니다.

   다음 이미지에는 하나의 통합 인스턴스 Tenable.io 표시되어 있습니다. 인스턴스가 두 Tenable.io 개 이상인 경우 양식의 Tenable.io 섹션 아래에 모두 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



6. **Request** Rescan(다시 스캔 요청)을 클릭합니다.

스캔이 처리 중이고 상위 스캔 기록이 생성되었음을 나타내는 메시지가 표시됩니다. 모든 하위 스캔의 상태는 다시 스캔을 시작하는 데 사용한 VI, 정정 작업, TPE 및 SDI 기록의 스캔 관련 목록에서 언제든지 확인할 수 있습니다. 메시지에서 세부 정보 보기를 클릭하여 다시 스캔 상태를 확인하고 지정된 기록에서 시작된 다른 다시 스캔을 봅니다.

모든 하위 스캔이 성공적으로 완료되면 상위 스캔 기록의 상태 필드가 완료로 표시됩니다. 하위 스캔 임포트 데이터. 각 스캔은 통합 인스턴스, TPE, IP 및 네트워크 ID의 고유한 조합을 지원합니다. 상위 스캔 기록에 여러 하위 스캔이 표시될 수 있습니다. 예를 들어, 하위 스캔에서 지원할 수 있는 최대 IP 주소 수는 1,000개입니다. 취약한 항목에 대한 IP가 1002개인 경우 요청을 지원하기 위해 두 개의 하위 스캔이 생성되고 스캔 관련 목록에 나열됩니다. 상위 스캔 기록은 하위 스캔을 위한 컨테이너이며 해당 상태는 하위 스캔의 상태를 반영합니다.

인스턴스는 ServiceNow AI Platform# 재스캔 상태가 성공적으로 완료될 때까지, 또는 설정된 추적 기간이 초과될 때까지(먼저 발생하는 쪽 적용) 재스캔 상태를 추적합니다. 시간 제한은 검사를 중지하지 않습니다. 시간 제한은 실제 다시 검색이 중지된 시간이 아니라 다시 스캔 상태 추적이 ServiceNow AI Platform# 중지된 시기를 나타냅니다. 종결/고정으로 전환되었거나 전환될 모든 VI는 고정 취약성 통합의 다음 예약된 임포트와 함께 임포트됩니다Tenable.io.

오류가 발생한 스캔의 경우 상위 스캔 기록에서 하위 스캔을 확인할 수 있습니다. 하위 스캔의 응답 페이로드에서 오류를 봅니다.

수정된 취약성 통합의 다음 예약된 임포트 후에 검사를 시작한 기록에 대한 업데이트된 결과를 볼 수 있습니다.

의 네트워크 파티션 식별자로 구성 항목을 업데이트합니다. **Tenable Vulnerability Integration**

IP 주소를 공유하는 환경의 자산에 대한 고유한 CI(구성 항목)를 생성합니다. 환경 전반에서 고유한 자산을 식별하고 기존 검색된 항목, 취약한 항목 및 탐지 레코드의 CI를 자동으로 업데이트하여 취약성에 대한 자세한 정보를 제공합니다.

시작하기 전에
필요한 역할: 관리자

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보
기본적으로 취약성 대응 애플리케이션에서 자산을 식별하는 한 가지 방법은 IP 주소를 사용하는 것입니다. 경우에 따라 자산은 IP 주소를 공유할 수 있지만 CMDB에 하나의 CI로 저장됩니다.

예를 들어 다음 표와 같이 환경의 여러 자산(CI)은 IP 주소를 공유할 수 있지만 고유한 네트워크 및 리포지토리 ID를 가질 수 있습니다. 그러나 기본적으로 이러한 자산은 일반적으로 IP 주소 조회 중에 단일 CI (CI 1) 로 식별되고 저장됩니다.

기본 **IP** 조회 및 **CI** 생성

소스	**IP** 주소	**Network_id**	구성 항목
Tenable.io: 자산과 고정 및 미해결 취약성 통합	123.12.12.141	03712	CI 1
	123.12.12.141	03713	CI 1

소스	**IP** 주소	**Repository_id**	구성 항목
Tenable.sc: 자산과 고정 및 미해결 취약성 통합	123.12.12.141	12	CI 1
	123.12.12.141	13	CI 1

동일한 IP 주소를 가진 자산에 대해 개별 CI를 생성하여 고유한 자산으로 식별할 수 있습니다. 새로운 데이터 임포트를 시작으로 예약된 작업을 실행하여 네트워크 파티션 식별자(network_partition_identifier)를 포함하는 기존 CI *`Update existing discovered items with network partition identifier`*를 보다 세밀하게 업데이트할 수 있습니다.

이 예약된 작업은 기본적으로 비활성화되어 있습니다. 설정 도우미에서 및 Tenable.sc 제품의 자산과 고정 및 미해결 취약성 통합 Tenable.io 에 대해 이 기능을 활성화하여 기록에서 이 식별자를 봅니다.

이 예약된 작업은 활성화되면 임포트한 데이터의 기존 CI 기록에 네트워크 파티션 식별자(network_partition_identifier)를 추가합니다. IRE에서 만든 기존 CI도 업데이트됩니다. 또한 예약된 작업은 다음 임포트로 시작하는 네트워크 파티션 식별자를 포함하는 CI를 생성합니다. 또는 요청 시 작업을 시작하여 기존 데이터를 업데이트할 수 있습니다.

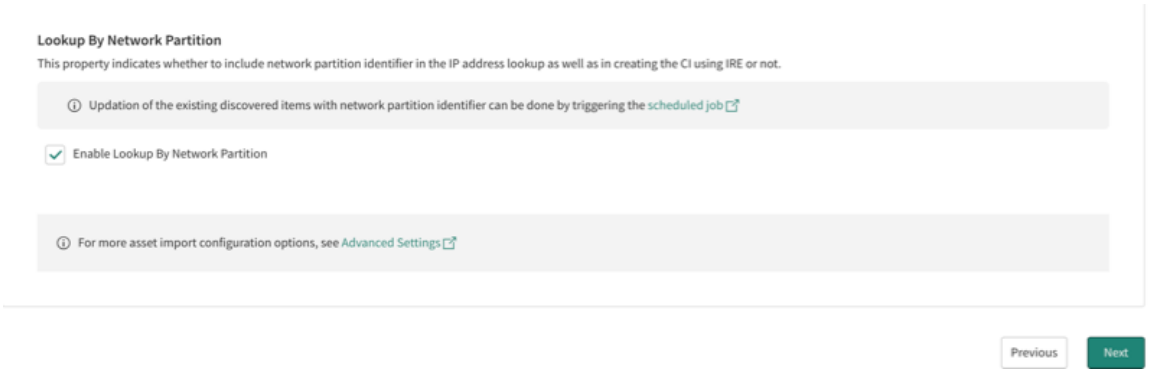
Tenable Vulnerability Integration v14.0 취약성 대응 및 v2.2부터 업그레이드하는 경우 CMDB CI Class Models(1.0.21.)가 지원됩니다. 클래스 모델에는 IRE(식별 및 조정) 식별 규칙에 네트워크 파티션 식별자(network_partition_identifier)가 있습니다.

옵션	설명
요청 시 예약된 작업을 실행합니다.	기존 검색 항목을 업데이트합니다. 네트워크 파티션 식별자 세분성을 포함하도록 기존 Tenable 데이터에 대한 CI가 생성되거나 업데이트됩니다. 검색된 항목, 취약한 항목 및 탐지 기록이 모두 새 CI로 업데이트됩니다.
다음 예약된 작업과의 통합에서 최신 데이터가 임포트될 때까지 기다립니다.	예약된 다음 작업으로 시작하는 네트워크 파티션 식별자를 사용하여 각각의 새 자산에 대한 CI를 생성합니다. CI, 취약한 항목 및 탐지 기록이 모두 새로운 세분성을 포함하도록 업데이트됩니다. 정확히 일치하는 항목이 없으면 새 CI가 만들어집니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 설정 도우미 〉 통합 구성 〉 스캐너 통합.
2. 통합 또는 Tenable.sc 통합을 선택합니다Tenable.io.
3. 필요한 통합을 편집합니다.
4. 선택 자산 임포트 설정.
5. 선택 네트워크 파티션별 조회 사용 의 확인란 네트워크 파티션별 조회 사용 절.



6. 다음을 클릭합니다.

네트워크 파티션 식별자 NETWORK_ID 및 리포지토리 _ID 포함되며 기존 CI를 업데이트하거나 다음 예약된 작업으로 CI를 생성합니다.

IP 조회 및 **CI** 생성에 포함된 네트워크 파티션 식별자 속성

소스	**IP** 주소	**NETWORK_ID**	네트워크 파티션 식별자가 없는 자산에 대한 **CI**	**CI** 네트워크 파티션 식별자가 있는 자산
Tenable.io: 자산과 고정 및 미해결 취약성 통합	123.12.12.141	03712	CI 1	CI 1
	123.12.12.141	03713	CI 1	CI 2

소스	**IP** 주소	**REPOSITORY_ID**	네트워크 파티션 식별자가 없는 자산에 대한 **CI**	**CI** 네트워크 파티션 식별자가 있는 자산
Tenable.sc: 자산과 고정 및 미해결 취약성 통합	123.12.12.141	12	CI 1	CI 1
	123.12.12.141	13	CI 1	CI 2

다음 예약된 작업에서 IP 주소 및 불완전한 IP 주소 CI 식별 조회 규칙에는 및 Tenable.sc 제품에 대한 Tenable.io 자산 및 고정 및 미해결 취약성 통합에서 데이터를 임포트하기 위한 네트워크 파티션 식별자 속성이 자동으로 포함됩니다.

시스템 속성을 활성화하고 기록을 저장한 후 요청 시 예약된 작업을 시작하여 네트워크 파티션 식별자가 포함된 CI로 기존 검색된 항목을 업데이트할 수도 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Tenable 취약성 통합에 대한 수정 사항 임포트

선택적 수정 사항을 구성하고 Tenable 취약성 통합에서 Tenable 취약성 임포트 통합을 위해 특별히 일부 데이터를 간소화합니다 ServiceNow# .

시작하기 전에

필요한 역할: sn_vul.vulnerability_admin

이 태스크 정보

이 작업 집합에는 코딩과 에 대한 ServiceNow AI Platform고급 지식이 필요합니다.

다음 단계에 따라 Tenable 취약성 통합에 대해 도메인 분리된 임포트를 생성합니다. 다음 예는 Tenable.io 미해결 취약성 통합용이지만 이 콘텐츠는 다른 Tenable 통합에 적용할 수 있습니다.

프로시저

1. 도메인을 생성합니다.
2. 생성하는 모든 도메인에 대해 사용자를 생성하고 사용자를 해당 도메인에 할당합니다.

   이 사용자를 Tenable.io 도메인의 run_as 자리 표시자로 생각하십시오.

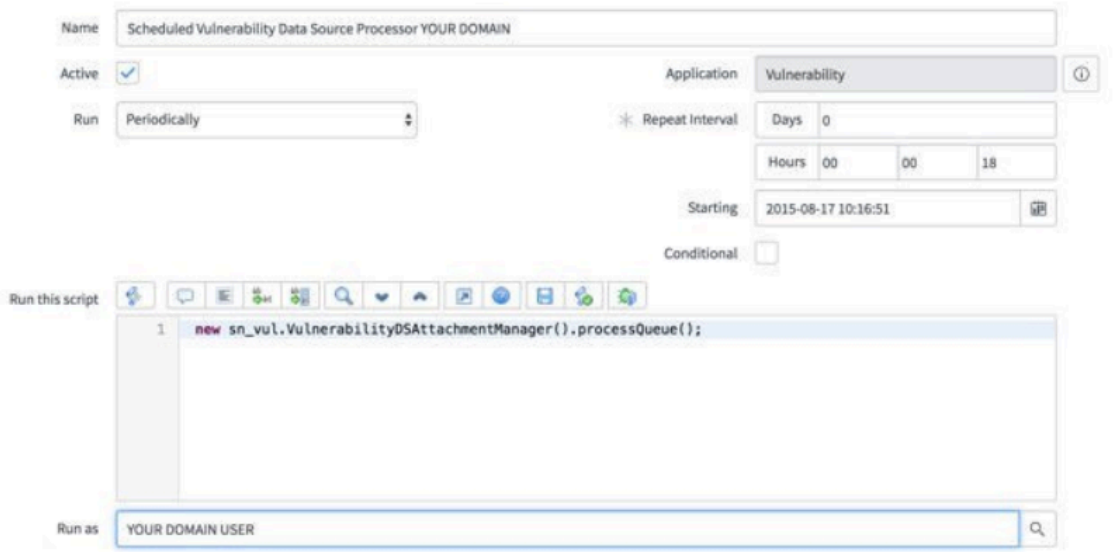
3. 취약성 통합을 엽니다.
   사용자는 VR과 동일합니다. 전역 도메인의 시스템 사용자이며 sn_vul.tenable_configure_integration, import_admin 및 sn_vul.vulnerability_write 역할이 있어야 합니다. 이 사용자는 데이터 소스, 변환 맵 및 취약성 데이터에 액세스할 수 있어야 합니다.

   > **주:**
   > 이 사용자를 이 역할과 관련된 것으로 간주합니다. 사용자에게 다른 목적이 있어서는 안 됩니다.

4. 각 도메인에서 아래에 있는 예약된 취약성 데이터 소스 프로세서를 복사하여 예약된 작업을 생성합니다. 시스템 정의 〉 예약된 작업.
5. 이름에 도메인을 추가하여 예약된 작업을 식별합니다.
6. run_as 사용자를 이전 단계에서 만든 사용자로 변경합니다.

   > **주:**
   > 통합이 run_as 사용자 도메인에서 실행되도록 다음 UI 작업을 편집합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



7. Tenable.io 미해결 취약성 통합에서 지금 실행 UI 작업을 편집하여 이 코드 블록을 파일의 맨 위에 추가합니다.

```
//sys id below is of Tenable.io integration if(current.sys_id ==
"4df3f18d53730010d7f1ddeeff7b12a9"){ current.run_as = gs.getUserID (); }
```

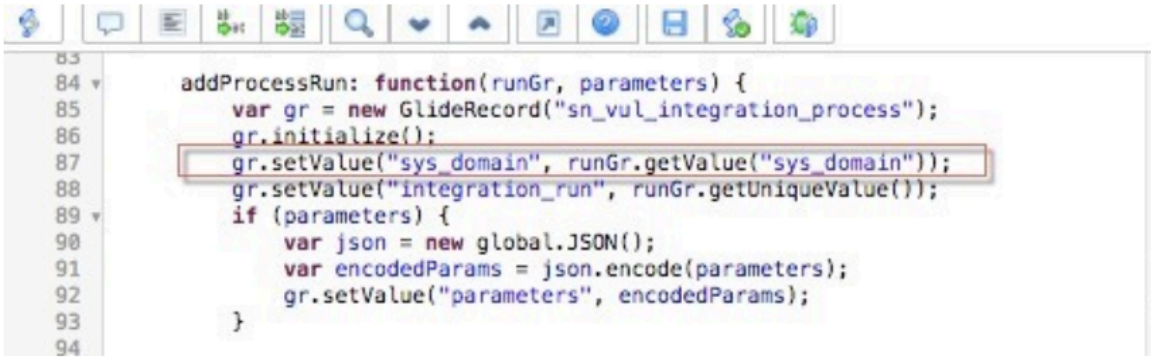
주:
통합이 run_as 사용자 도메인에서 실행되도록 다음 스크립트 포함을 편집합니다.

8. VulnerabilityIntegrationUtils 스크립트 포함 메서드 addIntegrationRun을 편집하여 강조 표시된 코드를 추가합니다.

```
addIntegrationRun: function(integrationGr, optInitialState) {
    if (!optInitialState)
        optInitialState = "ready";
    var importSource = "";
    if ((integrationGr.getValue("name")).indexOf("Qualys") != -1)
        importSource = "Qualys";
    var gr = new GlideRecord("sn_vul_integration_run");
    gr.initialize();
    gr.setValue("integration", integrationGr.getUniqueValue());
    gr.setValue("state", optInitialState);
    gr.setValue("source", importSource);
    var gUser = new GlideRecord("sys_user");
    gUser.get(gs.getUserID());
    gr.setValue("sys_domain",
    gUser.getValue("sys_domain"));
    return gr.insert();
},
```

9. VulnerabilityIntegrationUtils 스크립트 포함 메서드 addProcessRun을 편집하여 강조 표시된 코드를 추가합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



```
addProcessRun: function(runGr, parameters) {
    var gr = new GlideRecord("sn_vul_integration_process");
    gr.initialize();
    gr.setValue("sys_domain", runGr.getValue("sys_domain"));
    gr.setValue("integration_run", runGr.getUniqueValue());
    if (parameters) {
        var json = new global.JSON();
        var encodedParams = json.encode(parameters);
        gr.setValue("parameters", encodedParams);
    }
```

10. DataSourceVulnReportRefreshProcessor 스크립트 포함 메서드 _processFromDataSourceGroups 편집하여 원래 코드를 편집된 _processFromDataSourcesGroups 코드로 원래 _processFromDataSourcesGroups 변경합니다.
11. VulnerabilityDSAttachmentManager 스크립트 포함 메서드인 queueItem을 편집하여 강조 표시된 코드 블록 queueItem, _getNext _processQueueEntry 함수를 추가합니다.

    도메인 분리 호스트 탐지를 임포트할 준비가 되었습니다.

    임포트하기 전에 계산기 사용 안 함

    계산기를 사용하지 않는 경우 다음 단계를 수행하여 기본 계산기를 비활성화합니다. 취약성 계산기를 사용하지 않는 경우 정의한 다른 계산기 외에 기본 계산기를 비활성화하는 것이 가장 좋습니다. 취약성 계산기는 취약한 항목 기록에 액세스할 때마다 실행되며 인스턴스 성능에 영향을 줄 수 있습니다.

    필요한 역할: sn_vul.vulnerability_admin.

12. 다음으로 이동 모두 〉 취약성 〉 관리 〉 취약성 계산기.
13. 취약성 영향 그룹을 엽니다.
14. 점수 및 서비스 기반 영향 계산기를 엽니다.
15. 활성 필드를 선택 취소하여 계산기를 비활성화합니다.
16. 업데이트를 클릭합니다.

    기본 계산기를 사용하지 않도록 설정했습니다.

    초기 임포트 전에 알림 기반 비즈니스 규칙 비활성화

    초기 기록을 임포트하기 전에 알림 관련 비즈니스 규칙을 비활성화하려면 다음 단계를 따르십시오. 기록을 처음 임포트하는 동안 특정 알림 관련 비즈니스 규칙에서 많은 알림이 생성되어 성능에 영향을 줄 수 있습니다. 이러한 비즈니스 규칙은 임포트 중에 비활성화하도록 수정해야 합니다.

    필요한 역할은 sn_vul.vulnerability_admin입니다.

17. 다음으로 이동 모두 〉 시스템 정의 〉 비즈니스 규칙.
18. 영향을 받는 CI 알림을 검색합니다.
19. 비즈니스 규칙을 열고 다음 조건을 *current.sys_class_name != "sn_vul_vulnerable_item"* 삽입합니다.
20. 업데이트를 클릭합니다.
21. 다음 비즈니스 규칙에 대해 이 절차를 반복합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 영향을 받는 비용 센터 알림
- 영향을 받는 그룹 알림
- 영향을 받는 위치 알림

> **주:**
> 초기 기록 임포트가 완료된 후 이러한 비즈니스 규칙을 다시 사용하도록 설정할 수 있습니다. 그러나 비활성화된 상태로 두는 것이 좋습니다. 이로 인해 많은 수의 알림이 생성되고 인스턴스 성능에 영향을 줄 수 있습니다.

초기 시작 날짜 수정

다음 단계에 따라 초기 시작 날짜를 수정합니다. 설정 도우미를 사용하여 설치하는 동안 Tenable 통합의 초기 시작 날짜를 설정합니다. 다음 단계에 표시된 대로 설정 도우미 또는 기본 통합에서 시작 날짜를 재설정할 수 있습니다.

22. 다음으로 이동 모두 〉 **Tenable** 취약성 통합 〉 관리 〉 통합.
23. 통합을 클릭합니다.
24. 통합 상세 정보를 클릭합니다.
25. 시작 시간 필드를 과거의 값으로 설정하면 해당 시간 이후에 스캔되고 탐지된 모든 취약성이 탐지됩니다.

    설정 도우미를 사용하여 Tenable을 구성한 경우, 시작 시간 필드는 처음에는 오늘 날짜의 3개월 전으로, 그 다음에는 오늘 날짜로 미리 채워집니다. 참고: 값을 최대 과거 월로 설정하는 것이 좋습니다. 이렇게 하면 많은 양의 데이터가 Tenable API 속도 제한을 초과하지 않고 실행 시간 초과가 트리거되는 것을 방지할 수 있습니다.
26. 제출 또는 업데이트를 클릭합니다.
27. 옵션: 지금 실행을 클릭하여 즉시 실행합니다.

취약성 인스턴스를 기반으로 **Tenable** 탐지를 분할하여 취약 항목을 분할합니다.

ServiceNow# 취약성 대응을 사용하여 Tenable 스캐너에서 탐지를 분할하여 탐지된 각 취약성 인스턴스에 대해 고유한 취약한 항목(VIT)을 생성할 수 있습니다. 이렇게 분할하면 다양한 정정 팀에 VIT를 할당하여 취약성 관리 및 추적을 강화할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
Tenable 스캐너의 페이로드에는 탐지 데이터가 포함되어 있으며, 증명 내의 각 경로는 탐지를 분할하는 데 사용됩니다. 페이로드의 출력 태그는 취약성의 위치를 식별하여 특정 경로에 따라 취약성을 정확하게 식별하고 관리할 수 있도록 합니다.

프로시저

1. 외부 공급업체 통합 테이블 〔sn_sec_int_integration〕에서 , Tenable.sc, 및 Tenable.cs에 대해 Tenable.ioVI에 증명 포함 키 열 값을 true로 설정합니다.
2. 다음으로 이동 모두 〉 취약성 대응 〉 관리 〉 **VI** 세분성 구성.
3. 제품의 경우 Tenable.cs탐지 키 구성 〔sn_vul_detection_key_config〕 테이블로 이동하여 기록을 선택하고 Tenable.cs 업데이트합니다.
4. 포트 포함 양식에서 포트 포함 확인란을 선택하고 여기를 클릭 링크(Tenable.io 및 Tenable.sc 에만 적용됨)를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. VI 키에 증명 추가 목록에서 새로 만들기를 선택합니다.
6. VI 키에 증명 추가 - 새 기록 양식의 취약성 필드에서 증명을 포함할 Tenable ID를 추가합니다.

   주:
   경로 정보만을 기준으로 탐지를 분할하거나 경로와 버전 상세 정보를 결합하여 분할할 수 있습니다. 자세한 내용은 이 페이지의 'Tenable 스캐너에서 탐지 분할' 섹션을 참조하십시오.

7. **Tenable** VIT를 분할하는 정규 표현식 필드에서 다음을 수행합니다.
   - Path\s+:\s+([A\n]+)를 입력하여 경로만을 기준으로 탐지를 분할합니다.
   - Path\s+:\s+([A\n]+)\n\s+Installed\s+version\s+:\s+([A\n]+)\n\s+Fixed\s+version\s+:\s+([A\n]+)을 입력하여 경로와 설치 및 수정된 버전을 기준으로 탐지를 분할합니다.
8. 제출을 선택합니다.

Example: Tenable 스캐너에서 탐지 분할

Tenable 스캐너에서 다음과 같은 탐지는 경로 및 버전 정보를 모두 포함하는 출력 태그에 증거를 표시합니다.


```
    "results":


            "asset":
                "agent_uuid": *92124caabdb9459baa9d053186df48b9",
               "bios_uuid": "ec2cbbfd-dc9e-efbf-acdd-485daZe8c7df"
               "device_ type": "aws-ec2-instance",
                "fqdn": "ip-ac0a0004. secops.com",
                "hostname": "ip-ac0a0004",
        "uuid": "486acb3b-674f-477a-bc37-660a7bba37b3",
                "ipv4": "18.220.145.158",
                "last_authenticated_results": "2024-05-17T03:34:04.424Z",

                "mac_address": "0a:3e:8b:ed:63:e6",
               "netbios name": "IP-AC0A0094".
               "operating_system": [
                     "Microsoft Windows Server 2019 Datacenter Build 17763"


                "network_id": "00000000-0000-0000-0000-000000000008",

               "tracked": true


            "output": "In                          C: 11 Program Files (x86) \ \Common Files\\0racle\\Java\\javapath_target_119044062511\n Installed version : 1.8.0_361.9\n Fixed version
                                                                    Path
            "plugin":
                  "bid":
                        123456


                "checks_for_default_account": false,
              "checks_for malware": false,
```


기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
                    "coe":
                "cpe:/a:notepad-plus-plus:notepad%5c%2b15ck2b"


                 "cvSs3_base_score": 7.8,
                "cvss3 temporal score": 7.0,

                "cvss3_temporal_vector": {
                      "exploitability": "Proof-of-Concept",
                      "remediation level": "Official Fix",
                       "report_confidence": "Confirmed",
                       "raw": "E: P/RL:0/RC: C"
```

Wiz 테스트 결과 및 문제 탐색 앱과의 통합 구성 준수

통합에 Wiz 취약성 대응 포함된 Wiz 테스트 결과 및 문제 통합을 구성 준수 사용하여 클라우드 구성 데이터를 임포트합니다.

Wiz 테스트 결과 통합

다음에서 Wiz 구성 테스트 결과를 임포트하여 미준수 클라우드 구성을 탐지하고 클라우드 환경 전체에 걸쳐 보안 정책과 표준을 적용할 수 있습니다.

결과는 애플리케이션의 클라우드 테스트 결과(CTR)에 매핑됩니다 구성 준수 .

주:
다음의 Wiz 호스트 구성을 임포트하지 않습니다.

Wiz 문제 통합

취약성 관리자, 분석가, 클라우드 보안 및 위험 팀이 클라우드 인프라에서 잠재적인 공격 경로를 드러낼 수 있는 취약성 조합을 식별할 수 있도록 문제 데이터를 Wiz 임포트합니다.

또한 이러한 결과는 애플리케이션에서 소스 구성 준수 로 레이블이 지정된 Wiz ### 있는 CTR에 매핑되어 복잡한 다중 벡터 위험을 초래할 수 있는 자산을 추적하고 정정하는 데 도움이 됩니다.

통합과 설치 및 구성 단계에 포함된 Wiz 취약성 대응 다른 통합에 대한 자세한 내용은 문서를 Wiz 취약성 대응 통합 이해참조하십시오.

구성 준수 정정

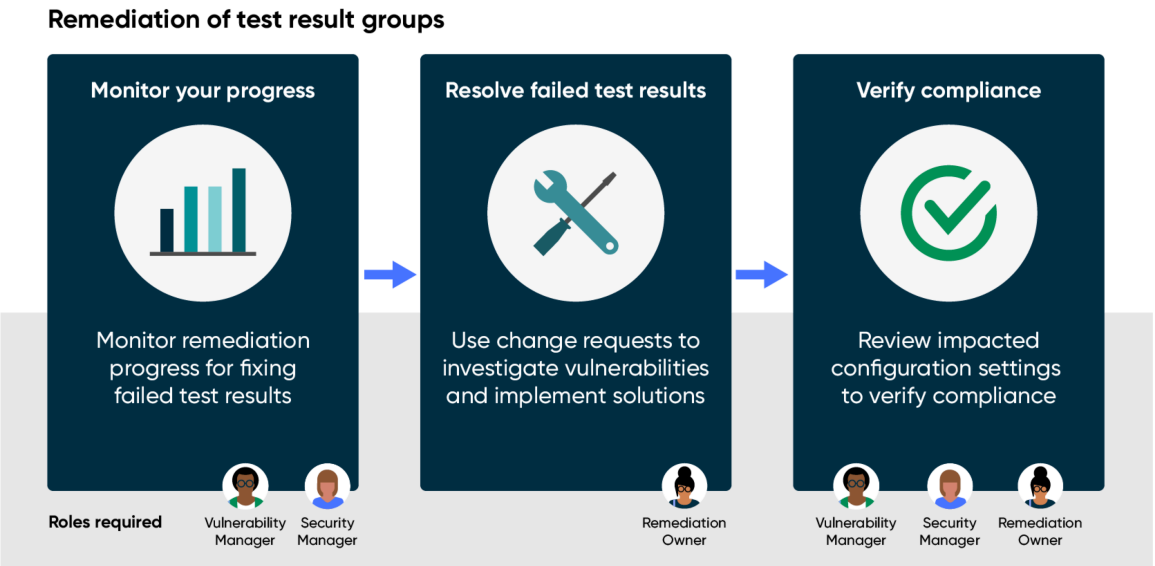
구성 준수 정정은 주로 예약된 작업(통합), 정정 작업, 워크플로우 및 변경 요청에 의해 보강되는 수동 프로세스입니다.

주:
의 구성 준수v14.9부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v14.9 이전 용어	용어 **v14.9** 이상
테스트 결과 그룹	정정 작업
그룹 규칙	정정 작업 규칙
정책	테스트 그룹

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



별도의 외부 공급업체 SCA 플러그인은 에서 구성 준수데이터를 수집하고 변환합니다. 를 사용하여 구성 준수 구성 항목을 정정하려면 먼저 타사 스캐너 통합을 설치하고 하나 이상의 네트워크 스캔을 수행해야 합니다.

변경 요청을 사용하여 정정 작업에서 실패한 개별 테스트 정정을 정정합니다.

관련 변경 요청이 를 사용하여 변경 요청과 정정 작업 간의 상태 동기화수명주기를 통해 이동함에 따라 정정 작업의 상태가 자동으로 전환됩니다. itil 역할을 가진 사용자는 정정 작업에서 직접 변경 요청을 생성하고 관리할 수 있습니다.

관련 정보

- 수동으로 정정 작업 생성 구성 준수
- 테스트 결과 목록에서 정정 작업을 수동으로 생성 구성 준수
- 구성 준수에서 변경 요청 만들기
- 정정 작업을 기존 변경 요청에 연결
- 사용자 또는 그룹에 대한 정정 작업에서 할당 제거
- 테스트 결과 자동 종결
- 정정 작업 닫기
- 에서 예외 관리에 대한 승인 규칙 구성 구성 준수

수동으로 정정 작업 생성 구성 준수

정정 작업 모듈에서 정정 작업을 수동으로 생성하고 정정을 수행할 수 있습니다.

중요사항:
다음에서 정정 작업을 생성할 수 있습니다.

- 취약성 관리자 작업 공간 sn_vulc.admin 역할을 가진 사용자로
- IT 정정 작업 공간 sn_vulc.remediation_owner 역할을 가진 사용자로

시작하기 전에

필요한 역할: sn_vulc.admin

이 태스크 정보

정정 작업 규칙을 사용하면 테스트 결과 탭이 자동으로 채워집니다. 수동 생성은 규칙이 필요하지 않거나 반복할 필요가 없는 정정 작업에 유용합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
의 구성 준수v14.9부터 다음 용어의 이름이 변경되었습니다.

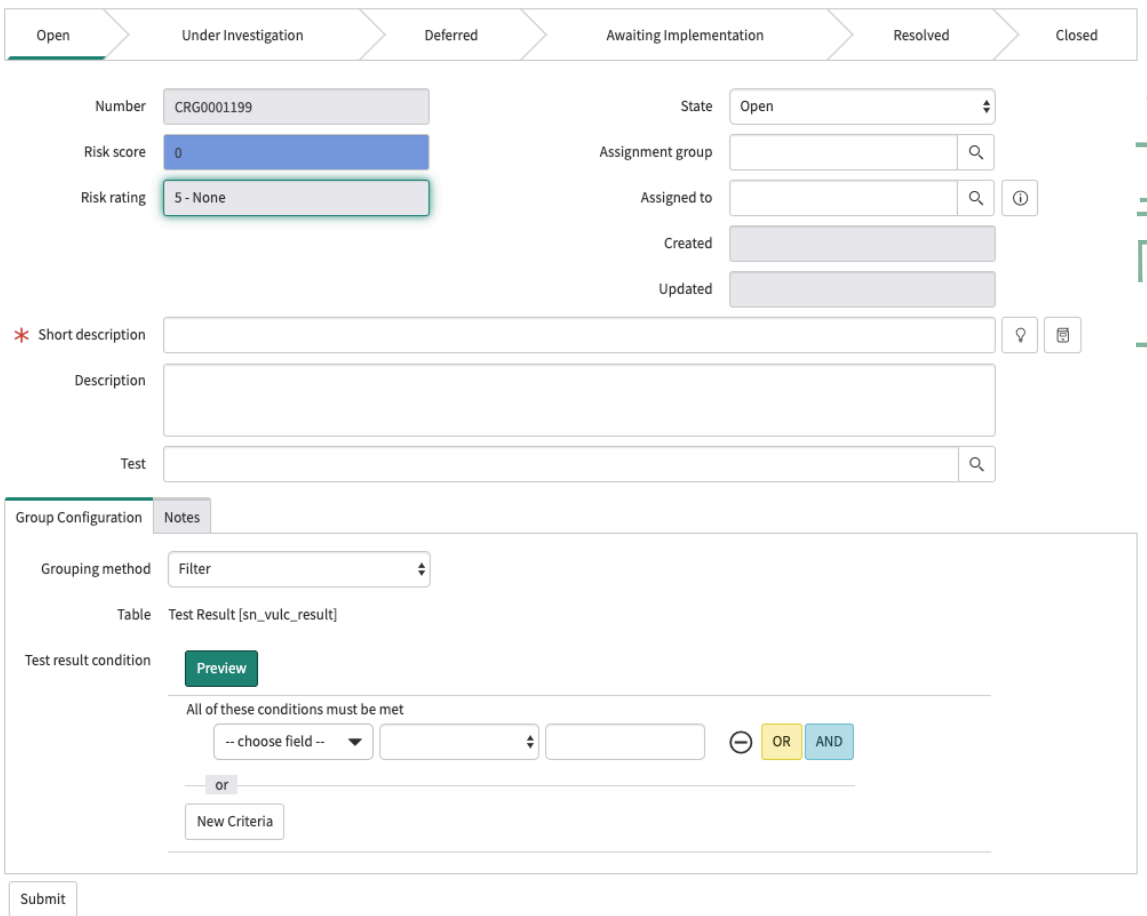
용어 변경

v14.9 이전 용어	용어 **v14.9** 이상
테스트 결과 그룹	정정 작업
그룹 규칙	정정 작업 규칙
정책	테스트 그룹

프로시저

1. 다음으로 이동 모두 〉 구성 준수 〉 정정 작업.
2. 탐색 패널에서 내 오픈 작업 또는 모든 오픈 작업을 클릭하여 목록을 봅니다.
3. 새로 만들기를 클릭합니다.

정정 작업 양식



4. 정정 작업 양식의 필드에 적절히 입력합니다.

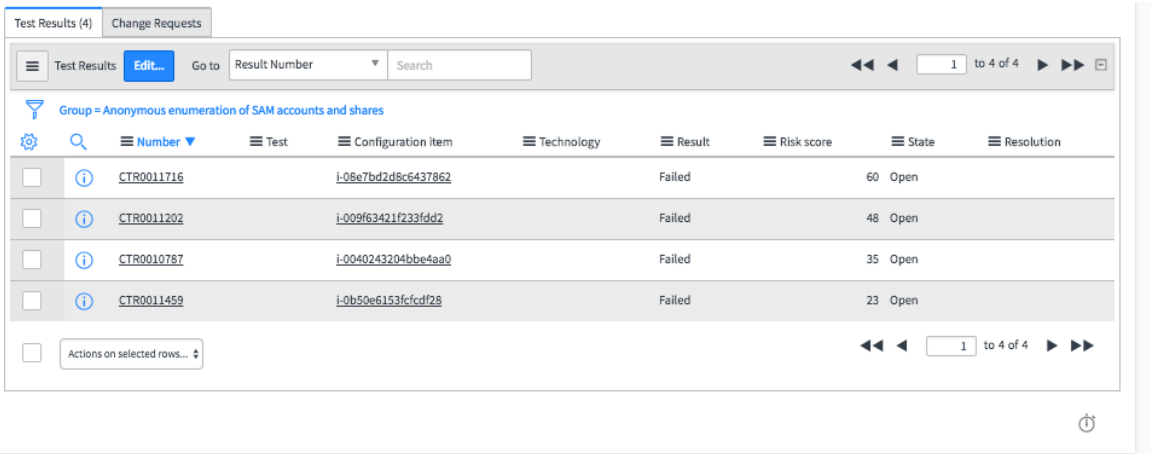
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

정정 작업 양식

필드	설명
번호	시스템에서 자동으로 할당된 ID입니다.
위험 점수	위험 점수 계산기로 자동으로 채워집니다. 롤업 위험 점수입니다. 이 위험 점수는 가중치가 적용되며, "종결"이 아닌 모든 테스트 결과(오픈, 조사 중, 구현 대기 중, 연기됨, 해결됨)의 최대 위험 점수 점수의 85%와 "종결됨"이 아닌 테스트 결과 수의 점수의 15%입니다.
위험 등급	위험 점수 계산기로 자동으로 채워집니다. 1-5 숫자 척도의 위험 점수 범위를 기준으로 1 - 중요에서 5 - 없음까지의 위험 점수 범위에 따라 전체 위험을 평가합니다. 이 필드는 이전 버전의 우선순위 필드를 대체합니다.
상태	첫 시작은 정정 작업의 정정 상태입니다. 자세한 내용은 구성 준수 상태 문서를 참조하십시오.
할당 그룹	정정 그룹에 정정 작업을 할당합니다.
담당자	정정 작업을 정정할 직원을 할당합니다.
작성됨	이 정정 작업을 생성한 날짜입니다.
업데이트됨	이 정정 작업을 업데이트한 날짜입니다.
간단한 설명	정정 작업의 이름입니다.
설명	이 정정 작업에 대한 설명입니다.
테스트	이 정정 작업에 대한 구성 테스트를 선택하십시오.
관련 탭	
그룹 구성	사용할 그룹화 방법: ○ 수동(기본값): ○ 필터 또는 그룹 규칙: 테이블: 테스트 결과로 사전 선택됨 [sn_vulc_result] 테스트 결과 조건: 사용할 필터를 선택합니다. 주: 필터 조건 위의 기록이 조건과 일치함 링크에 선택한 테스트 결과 기록이 새 창에 표시됩니다. 미리 보기를 클릭하여 새 그룹을 저장하기 전에 필터 기준에서 반환하는 결과 수를 확인합니다. 테스트 결과 관련 탭에서 편집 단추를 클릭하여 테스트 결과 관련 목록을 수동으로 만들어야 합니다.
메모	이 정정 작업과 관련된 작업 메모입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. 헤더를 마우스 오른쪽 버튼으로 클릭하여 저장 하거나 제출 을 클릭하여 저장하고 정정 작업 목록으로 돌아갑니다.
   테스트 결과 및 변경 요청 관련 목록을 표시합니다.



테스트 결과 목록에서 정정 작업을 수동으로 생성 구성 준수

테스트 결과 목록에서 정정 작업을 수동으로 생성하고 그에 따른 정정 작업에서 정정을 수행할 수 있습니다.

시작하기 전에
필요한 역할: sn_vulc.admin

이 태스크 정보
이 방법을 사용하려면 포함할 테스트 결과를 선택하고 선택한 행에 대해 수행할 동작... 메뉴에서 그룹을 생성해야 합니다. 이 방법은 쉽게 필터링할 수 없는 결과 또는 정정할 테스트 결과를 지정하려는 상황에 적합합니다.

주:
의 구성 준수v14.9부터 다음 용어의 이름이 변경되었습니다.

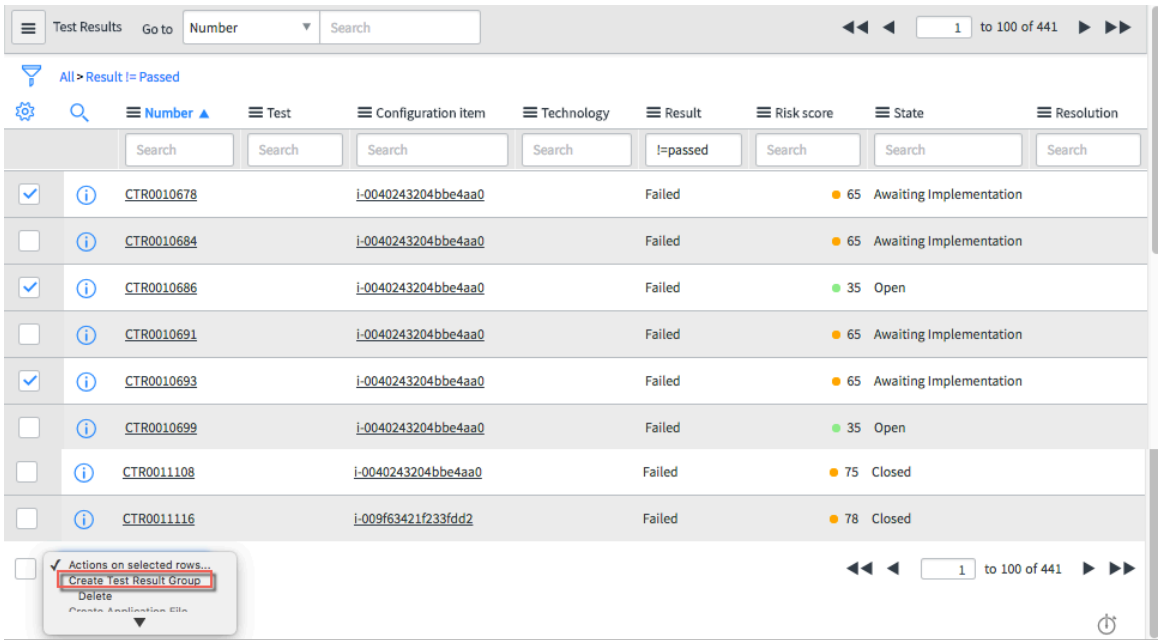
용어 변경

v14.9 이전 용어	용어 **v14.9** 이상
테스트 결과 그룹	정정 작업
그룹 규칙	정정 작업 규칙
정책	테스트 그룹

프로시저

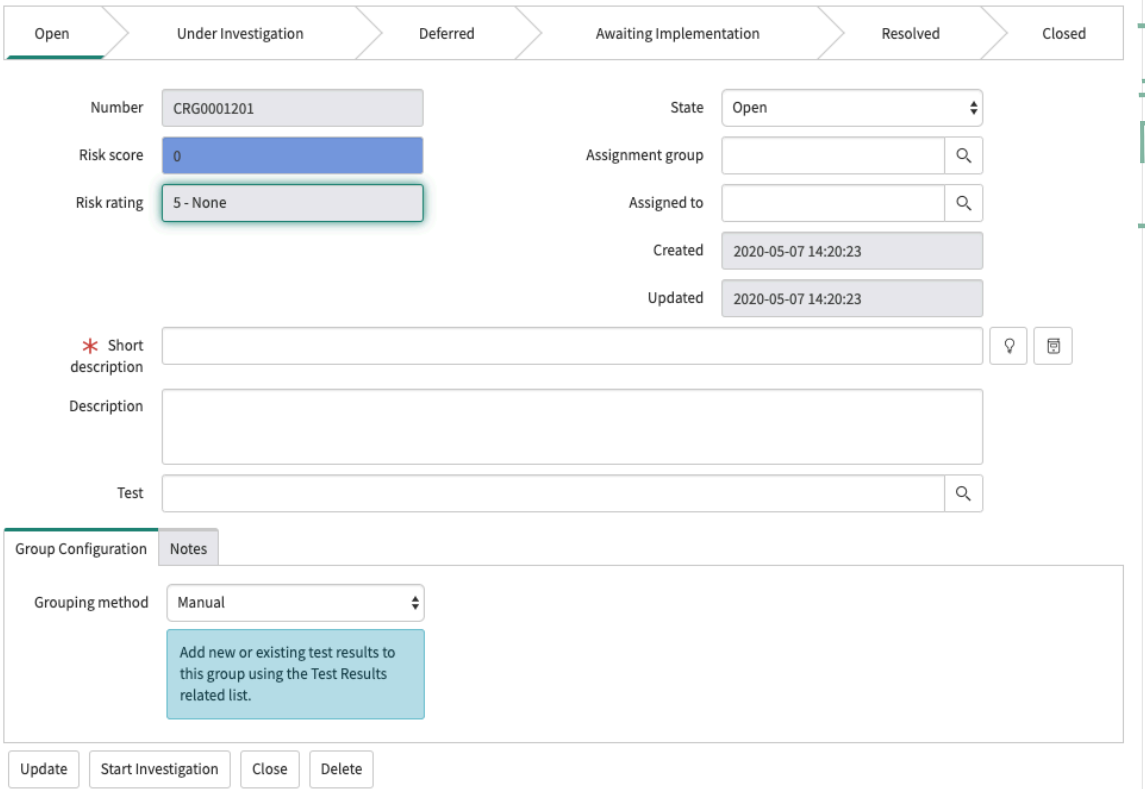
1. 다음으로 이동 모두 〉 구성 준수 〉 테스트 결과.
2. 탐색 패널에서 테스트 결과 모듈을 선택하여 목록을 엽니다.
3. 각 테스트 결과 옆에 있는 확인란을 선택하여 정정 작업에 포함할 테스트 결과를 선택합니다.
4. 목록 하단에 있는 선택한 행에 대해 수행할 작업... 메뉴를 엽니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



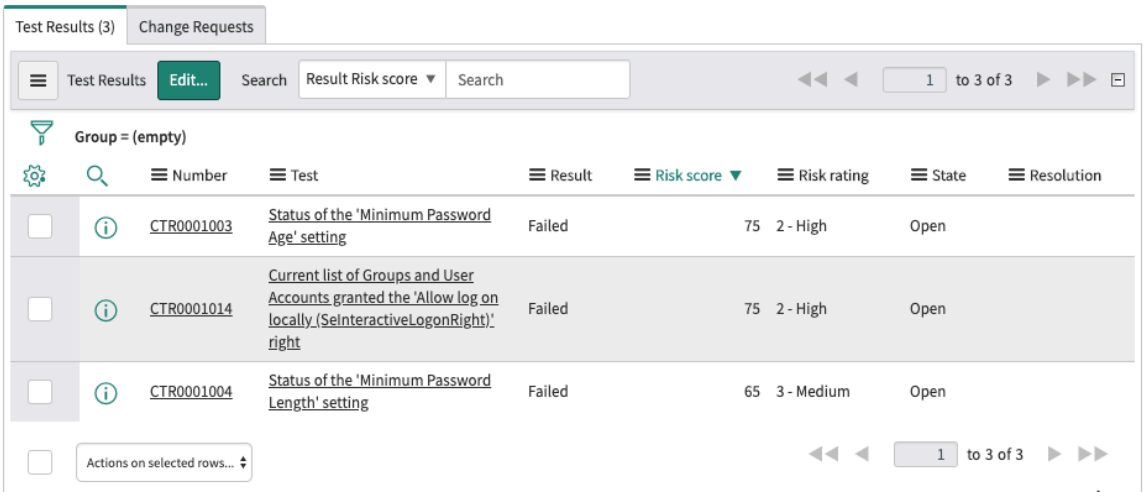
5. **[Create Remediation Task]**를 선택합니다.
정정 작업이 생성되고 열립니다.

정정 작업 양식



정정 작업에 대해 선택한 테스트 결과가 관련 변경 요청과 함께 테스트 결과 관련 목록에 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



6. 양식의 필드에 적절히 입력합니다.

필드	설명
번호	시스템에서 자동으로 할당된 ID입니다.
포인트	위험 점수 롤업 계산기로 자동으로 채워집니다. 롤업 위험 점수입니다. 이 위험 점수는 가중치가 적용되며, "종결"이 아닌 모든 테스트 결과(오픈, 조사 중, 구현 대기 중, 연기됨, 해결됨)의 최대 위험 점수 점수의 85%와 "종결됨"이 아닌 테스트 결과 수의 점수의 15%입니다.
평가 등급	위험 점수 롤업 계산기로 자동으로 채워집니다. 1-5 숫자 척도의 위험 점수 범위를 기준으로 1 - 중요에서 5 - 없음까지의 위험 점수 범위에 따라 전체 위험을 평가합니다. 이 필드는 이전 버전의 우선순위 필드를 대체합니다.
이력 위험 점수	위험 점수 롤업 계산기로 자동으로 채워집니다. 통과한 모든 테스트 결과의 고유 위험 점수는 정정 작업에 포함됩니다. 이 필드에는 테스트 그룹에서 정정한 위험의 양이 표시되며 테스트 그룹이 "종결" 상태이고 위험 점수가 0인 후에만 표시됩니다.
상태	첫 시작은 정정 작업의 정정 상태입니다. 자세한 내용은 구성 준수 상태 문서를 참조하십시오.
할당 그룹	정정 그룹에 정정 작업을 할당합니다.
담당자	정정 작업을 정정할 직원을 할당합니다.
작성됨	이 정정 작업을 생성한 날짜입니다.
업데이트됨	이 정정 작업을 업데이트한 날짜입니다.
간단한 설명	정정 작업의 이름입니다.
설명	이 정정 작업에 대한 텍스트 설명입니다.
	이 정정 작업에 대한 구성 테스트를 선택하십시오.
관련 탭	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
그룹 구성	사용할 그룹화 방법: ○ 수동(기본값) ○ 필터 테이블: 테스트 결과로 미리 선택됨 테스트 결과 조건: 사용할 필터를 선택합니다. 주: 필터 조건 위의 기록이 조건과 일치함 링크에 선택한 테스트 결과 기록이 새 창에 표시됩니다. 미리 보기를 클릭하여 새 정정 작업을 저장하기 전에 필터 기준이 반환하는 결과 수를 확인합니다.
메모	이 정정 작업과 관련된 작업 메모입니다.
관련 목록	
테스트 결과	이 정정 작업에 포함된 테스트 결과입니다.
관련 변경요청	이 정정 작업과 연결된 변경 요청입니다.

7. 헤더를 마우스 오른쪽 버튼으로 클릭하여 저장 하거나 제출 을 클릭하여 저장하고 정정 작업 목록으로 돌아갑니다.

구성 준수에서 변경 요청 만들기

애플리케이션의 정정 작업에서 변경 요청을 생성할 수 있습니다 구성 준수 .

시작하기 전에
필요한 역할: itil 역할을 가진 사용자

이 태스크 정보
IT 또는 정정 전문가는 정정 작업에서 모든 테스트 결과에 대한 변경 요청(CHG)을 직접 생성합니다. 수동 개입이 필요한 취약성 조사를 신속하게 처리할 수 있도록 미리 채워진 정보로 변경 요청을 생성합니다.

자신에게 할당된 정정 작업에서 직접 변경 요청을 생성, 승인, 구현, 검토 및 종결할 수 있습니다. 정정 작업에서 미리 채워진 정보로 세 가지 유형의 변경 요청을 생성할 수 있습니다.

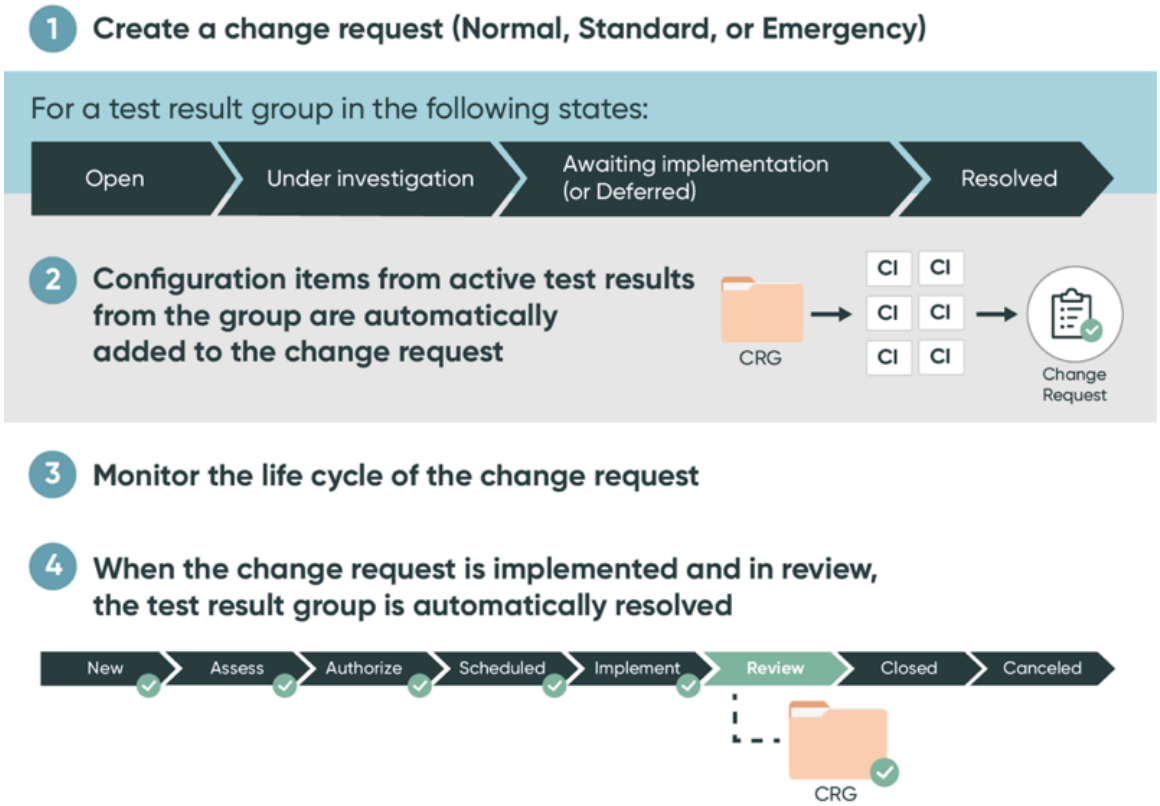
표준
: 위험이 적고, 비교적 일반적이며, 지정된 절차나 작업 지시를 따르는 사전 승인된 변경입니다.

정상
: 일반 변경 요청은 구현, 검토 및 종결 전에 두 가지 수준의 승인이 필요한 후속 대응적 프로세스를 따릅니다.

긴급
: 중요 인시던트를 해결하기 위한 변경입니다.

다음 이미지는 정정 작업에서 변경 요청을 생성하는 기본 플로우를 보여줍니다. 이 플로우에 대한 자세한 단계는 이미지를 따릅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



버전 19.0 취약성 대응부터 IT 정정 작업 공간에서 정정 작업에 대한 변경 요청을 생성할 수 있습니다. 자세한 내용은 에서 변경 요청 만들기 IT 정정 작업 공간 문서를 참조하십시오.

주:
의 구성 준수v14.9부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v14.9 이전 용어	용어 **v14.9** 이상
테스트 결과 그룹	정정 작업
그룹 규칙	정정 작업 규칙
정책	테스트 그룹

프로시저

1. 다음으로 이동 모두 〉 구성 준수 〉 정정 작업 〉 내 오픈 작업.
   그룹에 할당된 정정 작업 목록이 표시됩니다.
2. 번호 열에서 변경 요청을 생성할 정정 작업을 클릭합니다.
   종결 또는 검토 중 이외의 상태에 있는 정정 작업에서 변경 요청을 생성할 수 있습니다.

   정정 작업 기록이 표시됩니다.
3. 기록의 오른쪽 상단에서 **Create** Change(변경 생성)를 클릭합니다.
   변경 요청 양식이 표시됩니다.
4. 필드에 내용을 입력합니다.
   a. 적용 대상 필드 목록에서 하나를 선택하여 계속합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. CR에 **CI** 추가 확인란에서 하나를 선택하여 계속합니다.

6. 변경 유형 필드 목록에서 하나를 선택하여 계속합니다.

   이 기능은 ITSM Change Management의 카탈로그에 설정한 변경 요청 유형을 자동으로 읽습니다. 예를 들어, ITSM의 표준 변경 요청 이름을 ## 에서 ## ###으로 변경하면 변경 요청 생성 양식의 변경 유형 목록에 새 이름이 자동으로 표시됩니다.

7. 양식의 변경 요청 미리 보기 섹션에 있는 필드는 정정 작업의 정보로 미리 채워져 있습니다. 필요한 경우 해당 필드를 편집합니다.

8. 변경 생성을 클릭합니다.
   변경 요청이 표시됩니다. 영향을 받는 CI 관련 목록에 기준과 일치하는 테스트 결과의 CI가 표시됩니다. 변경 요청에 승인이 필요한 경우 승인 요청 버튼이 표시됩니다.

   변경 요청이 생성되면 테스트 결과 그룹이 구현 대기 중 상태로 전환됩니다. 이 정정 작업에 대한 변경 요청이 해결되고 이 정정 작업과 연결된 다른 미해결 변경 요청이 없으면 정정 작업도 해결됨 상태로 이동합니다.

   자세한 내용은 변경 요청과 정정 작업 간의 상태 동기화 문서를 참조하십시오.

   주:
   상태 동기화가 활성화된 상태에서 각 기록의 수명주기 상태를 통해 변경 요청 및 정정 작업을 수동으로 이동할 수 있지만, 시스템에서 변경 요청의 상태가 변경되었음을 등록하거나 변경 요청을 추가하거나 정정 작업에서 제거하는 경우 상태 동기화가 수동 개입을 재정의할 수 있습니다. 그러나 변경 요청 상태는 정정 작업을 ## 또는 ### 상태에서 자동으로 이동하지 않습니다.

정정 작업을 기존 변경 요청에 연결

애플리케이션의 정정 작업을 구성 준수 기존 변경 요청에 연결합니다.

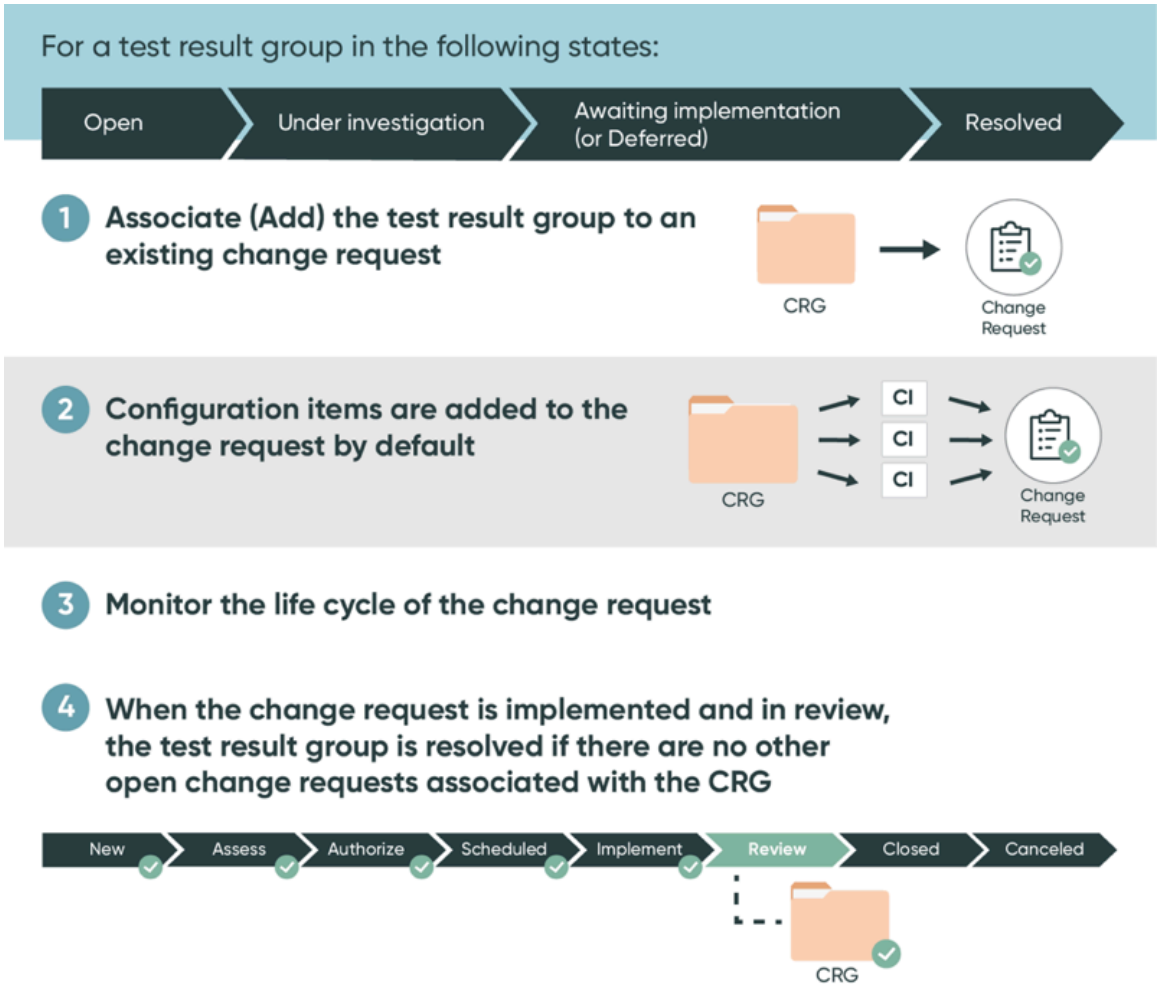
시작하기 전에
필요한 역할: itil 역할을 가진 사용자

이 태스크 정보
IT 또는 정정 전문가는 정정 작업(RT)을 인스턴스에서 이미 사용할 수 있는 변경 요청에 연결하여 정정 작업을 해결할 때 중복 변경 요청(CHG)을 생성하지 않도록 합니다.

정정 작업 기록에서 직접 본인 또는 할당 그룹에 할당된 정정 작업을 기존 변경 요청에 연결할 수 있습니다. 다음 이미지는 기존 변경 요청을 정정 작업에 연결하기 위한 기본 플로우를 보여줍니다. 이 플로우에 대한 자세한 단계는 이미지를 따릅니다.

주:
기존 변경 요청을 취소 됨 이외의 상태(오픈, 조사 중, 구현 대기 중, 종결 및 연기됨)의 모든 정정 작업에 연결할 수 있습니다. 지난 90일 내에 종결된 요청을 포함하여 변경 요청을 양식에서 연결할 수 있습니다. 변경 요청을 기존 정정 작업에 연결하면 활성 테스트 결과와 해당 구성 항목만 변경 요청에 추가됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



주:
의 구성 준수v14.9부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v14.9 이전 용어	용어 **v14.9** 이상
테스트 결과 그룹	정정 작업
그룹 규칙	정정 작업 규칙
정책	테스트 그룹

프로시저

1. 다음으로 이동 모두 〉 구성 준수 〉 정정 작업 〉 내 오픈 작업.
   그룹에 할당된 정정 작업 목록이 표시됩니다.
2. 번호 열에서 변경 요청을 생성할 정정 작업을 클릭합니다.

   정정 작업 기록이 표시됩니다.
3. 기록의 오른쪽 상단에서 **Create** Change(변경 생성)를 클릭합니다.
   변경 요청 양식이 표시됩니다.
4. 변경 요청 관련 목록으로 스크롤하여 선택합니다.
   정정 작업과 연결된 모든 변경 요청이 추가 단추와 함께 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. 추가를 클릭합니다.
   정정 작업에 기존 변경 요청 추가 대화 상자가 표시됩니다.
6. 검색 아이콘을 클릭하고 목록에서 항목을 선택합니다.
   표시되는 목록을 필터링하여 검색 범위를 좁힐 수 있습니다.
7. 제출을 클릭합니다.
   TRG는 변경 요청이 정정 작업에 성공적으로 연결되었음을 나타내는 메시지와 함께 표시됩니다. 변경 요청 관련 목록 아래에 새 변경 요청이 표시됩니다. 업데이트 적용 작업의 CI가 기본적으로 변경 요청에 추가되어 영향을 받는 CI 관련 목록에 표시됩니다. 이 관련 목록에서 변경 요청에 CI를 추가할 수도 있습니다. 메시지가 새 정정 작업으로 이동한 테스트 결과 수를 나타내고 새 RT가 표시됩니다.

   주:
   테스트 결과가 200개 미만인 경우 분할 작업이 동기식으로 수행되고 테스트 결과가 새 정정 작업에 표시됩니다.

   200개가 넘는 테스트 결과의 경우 분할 작업이 백그라운드에서 비동기적으로 수행되며 테스트 결과가 새 정정 작업에 표시되는 데 몇 초가 걸릴 수 있습니다. 다음 메시지도 표시됩니다. n ## ### ### TRGxxxxxxx## # ## ## GRCxxxxx(#)# # #####.

   변경 요청을 정정 작업에 연결할 수 있지만 다음과 같은 예외가 있습니다.

   - 취소됨 상태의 변경 요청.
   - 90일이 넘은 종결 상태의 변경 요청.
   - RT와 이미 연결된 변경 요청입니다. 시스템에서는 RT에 이미 연결된 변경 요청을 연결할 수 없습니다.

   이 정정 작업에 대한 변경 요청이 해결되고 이 정정 작업과 연결된 다른 미해결 변경 요청이 없으면 정정 작업도해결됨 상태로 이동합니다.

   주:
   상태 동기화가 활성화된 상태에서 각 기록의 수명주기 상태를 통해 변경 요청 및 정정 작업을 수동으로 이동할 수 있지만, 시스템에서 변경 요청의 상태가 변경되었음을 등록하거나 변경 요청을 추가하거나 정정 작업에서 제거하는 경우 상태 동기화가 수동 개입을 재정의할 수 있습니다. 그러나 변경 요청 상태는 정정 작업을 ## 또는 ### 상태에서 자동으로 이동하지 않습니다.

   자세한 내용은 변경 요청과 정정 작업 간의 상태 동기화 문서를 참조하십시오.

정정 작업 분할

애플리케이션의 기존 정정 작업에서 구성 준수 새 정정 작업으로 이동하려는 테스트 결과의 하위 집합을 식별합니다.

중요사항:
관리자와 정정 소유자는 각각 취약성 관리자 작업 공간 및 IT 정정 작업 공간에서 정정 작업을 분할할 수 있습니다.

시작하기 전에
필요한 역할: itil 역할을 가진 사용자

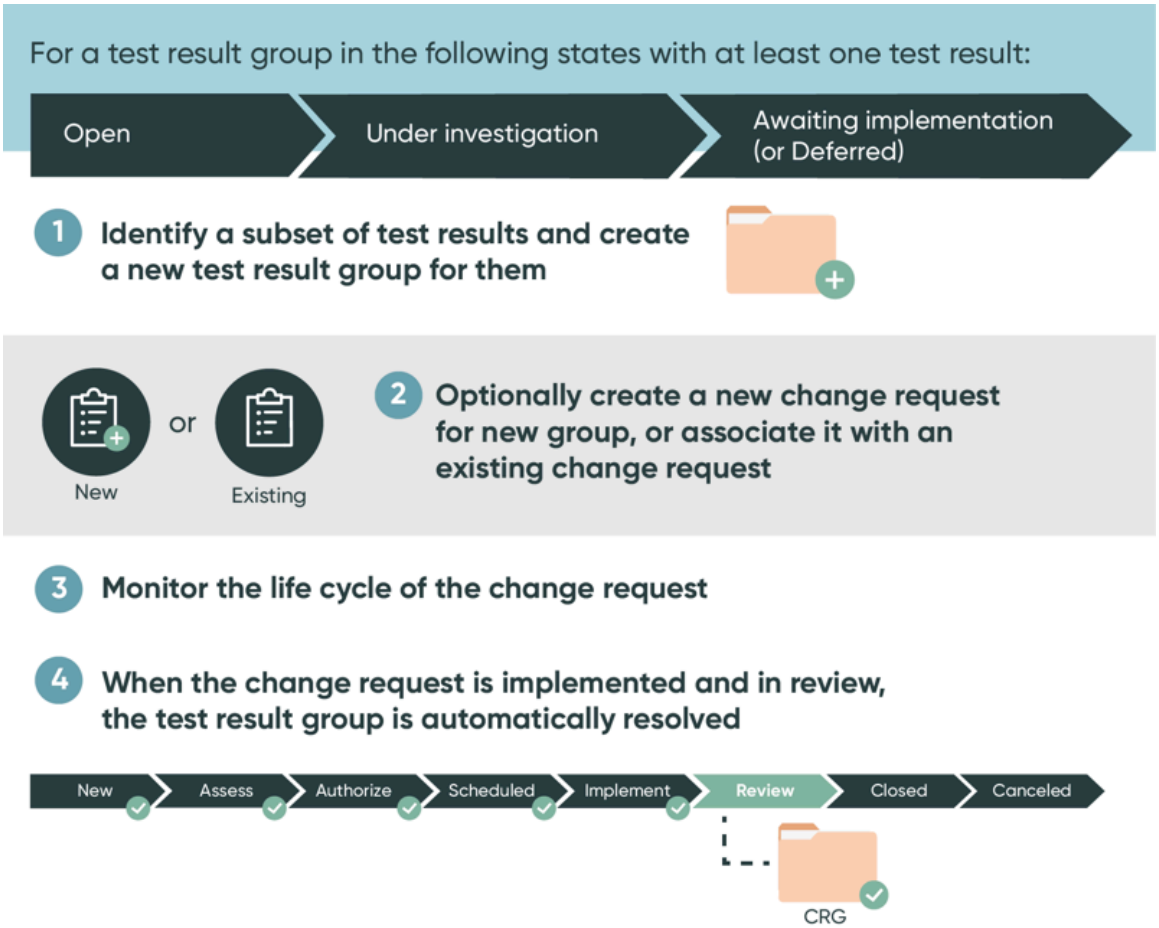
이 태스크 정보
IT 또는 정정 전문가는 두 개 이상의 테스트 결과를 통해 오픈, 조사 중 또는 구현 대기 중 상태의 기존 정정 작업을 분할할 수 있습니다. 특정 기준과 일치하는 테스트 결과로 새 정정 작업을 생성하면 원래 정정 작업에 영향을 주지 않고 특정 테스트 결과 그룹으로 작업할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

조건 작성기를 사용하여 새 정정 작업으로 이동할 테스트 결과의 조건을 지정하면 기준과 일치하는 활성 테스트 결과만 새 작업으로 이동됩니다. 정정 작업을 분할할 때 변경 요청(CHG)을 생성할 필요가 없습니다. 변경 요청을 생성하는 동시에 정정 작업을 분할하거나, 변경 요청을 생성하지 않고 정정 작업을 분할할 수 있는 옵션이 있습니다.

다음 이미지는 정정 작업을 분할하기 위한 기본 플로우를 보여줍니다. 이 플로우에 대한 자세한 단계는 이미지를 따릅니다.

정정 작업을 분할하기 위한 플로우



기존 정정 작업의 테스트 결과를 새 작업으로 분할하는 사용 사례에는 다음 예가 포함될 수 있습니다.

- 분할 작업에 대한 변경 요청 또는 변경 요청을 생성하려는 경우
- 할당 그룹의 다른 사용자에게 분할 작업을 재할당하는 경우
- 특정 CI(구성 항목)에 대한 일부 테스트 결과를 지정된 기간 내에 정정할 수 없다는 것을 알고 있기 때문에 분할 작업에 대한 연기 또는 예외를 요청하는 경우

[store-future: BEGIN review)의 취약성 대응버전 19.0부터 IT 정정 작업 공간에서 정정 작업을 분할할 수 있습니다.[End]

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
의 구성 준수v14.9부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v14.9 이전 용어	용어 **v14.9** 이상
테스트 결과 그룹	정정 작업
그룹 규칙	정정 작업 규칙
정책	테스트 그룹

프로시저

1. 다음으로 이동 모두 〉 구성 준수 〉 테스트 〉 정정 작업 〉 내 오픈 작업.
   그룹에 할당된 정정 작업 목록이 표시됩니다.
2. 번호 열에서 분할할 정정 작업을 클릭합니다.

   정정 작업 기록이 표시됩니다.
3. 특정 조건과 일치하는 새 작업에 대한 테스트 결과의 하위 집합을 만들려면 다음 단계를 수행합니다.

   기록의 오른쪽 상단에서 작업 분할을 클릭합니다.

   여러 테스트 결과가 있는 대규모 그룹에서 작업하는 경우 새 정정 작업을 생성하는 이 방법을 선호할 수 있습니다.

   분리 정정 작업 양식이 표시됩니다.
4. 조건 작성기가 표시되면 새 정정 작업으로 이동할 테스트 결과의 조건을 지정합니다.

   예를 들어, 다음 조건과 일치하는 테스트 결과만 필터링하는 것을 선호할 수 있습니다.

   - 열림 상태.
   - 위험 점수가 75보다 큽니다.
   - 결과는 실패입니다.

   조건을 입력한 후 테스트 결과가 필터와 일치하면 일치하는 테스트 결과 수와 함께 메시지가 표시됩니다.

   필터와 일치하는 테스트 결과가 없거나 모든 테스트 결과가 조건과 일치한다는 메시지가 표시되면 하나 이상의 테스트 결과가 필터 조건과 일치하도록 조건을 조정합니다.
5. 항목 미리 보기를 클릭하여 일치하는 테스트 결과를 확인합니다.
   새 창인 정정 작업에 항목이 표시됩니다.
6. 필터 조건과 일치하는 테스트 결과에 대한 세부 정보를 미리 보려면 작업 분할 을 클릭하여 새 그룹을 만들기 전에 다음 단계를 수행합니다.
   이러한 상세 정보에는 할당 그룹 및 테스트 결과가 할당된 대상이 포함됩니다. 미리 보기에서 이 정보를 보면 새 작업이 제대로 할당되었는지 확인하는 데 도움이 될 수 있습니다.

   a. 미리 보기에 정정 목록이 표시되면 결과 열에서 항목을 클릭합니다.
   테스트 결과 기록이 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

b. 할당 그룹 및 할당 대상 필드가 올바른지 확인합니다.

c. 업데이트를 클릭합니다.

7. 새 정정 작업을 생성할 준비가 되면 작업 분할을 클릭합니다.
메시지가 새 정정 작업으로 이동된 테스트 결과 수를 나타내고 새 정정 작업이 표시됩니다. 새 작업을 식별하는 데 도움이 되도록 간단한 설명 필드의 텍스트를 편집하고 필요한 경우 할당 그룹 또는 할당 대상 필드를 다시 편집할 수 있습니다.

> **주:**
> 테스트 결과가 200개 미만인 경우 분할 작업이 동기적으로 수행되고 테스트 결과가 새 작업에 표시됩니다.
>
> 200개가 넘는 테스트 결과의 경우 분할 작업은 백그라운드에서 비동기적으로 수행되며 테스트 결과가 새 작업에 표시되는 데 몇 초가 걸릴 수 있습니다. 다음 메시지도 표시됩니다. n ## ### ### TRGxxxxxxx## # ## ## GRCxxxxx(#)# # #####.

8. 또는 정정 작업의 테스트 결과 관련 목록에서 직접 테스트 결과를 선택하여 새 정정 작업을 생성할 수 있습니다.

정정 작업에 테스트 결과가 몇 개밖에 없거나 새 정정 작업으로 이동하려는 테스트를 정확히 알고 있는 경우 이 방법을 사용하는 것이 좋습니다.

a. 정정 작업 기록이 표시되면 테스트 결과 관련 목록으로 스크롤합니다.

b. 맨 왼쪽 열에서 새 정정 작업을 만들 테스트 결과의 확인란을 선택합니다.

c. 기록의 왼쪽 아래에 있는 선택한 행에 대한 작업 목록에서 작업 분할을 클릭합니다.

d. 표시되는 분리 정정 작업 양식에서 새 그룹을 쉽게 식별할 수 있도록 간단한 설명 필드의 텍스트를 편집하는 것이 좋습니다.

e. 작업 분할을 클릭합니다.
메시지가 새 작업으로 이동한 테스트 결과 수를 나타내고 새 정정 작업이 표시됩니다.

이 정정 작업에 대한 변경 요청이 해결되고 이 정정 작업과 연결된 다른 미해결 변경 요청이 없으면 정정 작업도 해결됨 상태로 이동합니다.

> **주:**
> 상태 동기화가 활성화된 상태에서 각 기록의 수명주기 상태를 통해 변경 요청 및 정정 작업을 수동으로 이동할 수 있지만, 시스템에서 변경 요청의 상태가 변경되었음을 등록하거나 변경 요청을 추가하거나 정정 작업에서 제거하는 경우 상태 동기화가 수동 개입을 재정의할 수 있습니다. 그러나 변경 요청 상태는 정정 작업을 ## 또는 ### 상태에서 자동으로 이동하지 않습니다.

자세한 내용은 변경 요청과 정정 작업 간의 상태 동기화 문서를 참조하십시오.

다음에 수행할 작업

새 정정 작업에 대한 변경 요청을 생성하거나 연결할 수 있습니다. 자세한 내용은 정정 작업을 기존 변경 요청에 연결 및 구성 준수에서 변경 요청 만들기 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용자 또는 그룹에 대한 정정 작업에서 할당 제거

기록이 사용자 또는 그룹에 잘못 할당된 경우 애플리케이션에서 테스트 결과 기록을 구성 준수 재할당합니다.

시작하기 전에
필요한 역할: sn_vulc.remediation_owner

이 태스크 정보
정정 작업(RT) 및 관련 테스트 결과가 정정 범위 내에 있지 않다고 판단되거나 기록이 사용자 또는 그룹에 잘못 할당되었다고 생각되는 경우 RT 기록의 할당 대상 및 할당 그룹 필드에서 자신 또는 그룹을 제거할 수 있습니다.

할당 해제 버튼은 종결 또는 해결됨 상태를 제외한 모든 정정 작업 기록에 표시됩니다.

프로시저

1. 사용자에게 할당된 종결 또는 해결됨 이외의 상태에 있는 정정 작업 기록으로 이동합니다.
2. 할당 대상 및 할당 그룹 필드를 지우려면 기록 상단에서 할당 취소를 선택합니다.
3. 할당 해제 대화 상자에서 작업 메모를 제공하고 제출을 선택합니다.
   - 입력한 작업 메모는 메모 섹션에 표시됩니다.
   - 상태 변경 승인 탭의 상태 변경 승인 기록(CA#)이 검토 중 상태를 표시하므로 승인 워크플로우를 추적할 수 있습니다.
   - 요청된 승인 탭에서 본인 또는 할당 그룹 제거 요청이 요청됨 상태로 표시됩니다.
4. 옵션: 또는 추가 옵션 메뉴에서 할당 해제 ( )를 선택하여 할당 필드를 지웁니다.

결과
요청은 기본 1단계 승인 워크플로우를 사용하여 승인됩니다. 자세한 내용은 Configuration Compliance에서 할당 취소 요청 승인을 참조하세요.

- 요청이 승인되면 상태 변경 승인 기록과 요청된 승인 기록이 승인됨으로 전환됩니다. 사용자와 사용자의 그룹이 할당 대상 및 할당 그룹 필드에서 제거됩니다. 할당 유형 필드에 #### ##이 표시되고, 애플리케이션의 할당되지 않은 모듈 구성 준수 목록에 정정 작업이 표시됩니다.

  기록이 할당되지 않았다는 알림은 할당 해제 알림 그룹의 취약성 관리자 또는 분석가에게 자동으로 전송됩니다. 이 기능의 알림 및 속성에 대한 자세한 내용은 구성 준수 테스트 결과 그룹에서 할당 제거를 참조하십시오.

- 요청이 거부되면 상태 변경 승인 기록과 요청된 승인 기록이 거부됨으로 전환됩니다.

> **주:**
> 취약성 관리자는 시스템 속성을 **false**로 설정하여 *sn_vulc.unassign_test_result_group.approval_required* 승인 프로세스를 비활성화할 수 있습니다.

다음에 수행할 작업
애플리케이션의 할당되지 않은 모듈 구성 준수 로 이동하여 범위에 속할 수 있는 항목에 대한 할당되지 않은 기록을 모니터링한 다음 자신에게 다시 할당합니다.

에서 할당 해제 요청 승인 구성 준수

애플리케이션의 할당 그룹 또는 개별 사용자의 정정 작업 제거 요청을 승인합니다 구성 준수 .

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_vulc.unassign_approver

이 태스크 정보
기본적으로 승인 구성이 제공됩니다. 미할당 승인의 경우 승인자 - 수준 1 승인 그룹에 한 명의 승인자가 필요합니다. 기본적으로 승인 그룹 할당 해제(### ## ## ## - ## 1)가 생성되고 이 그룹에 속한 사용자가 요청을 승인할 수 있습니다. 기본적으로 이 그룹에는 할당되지 않은 승인자 역할인 sn_vulc.unassign_approver가 포함되어 있습니다. 다음으로 이동하여 그룹을 수정하거나 생성하고 승인 구성을 업데이트할 수 있습니다. 모두 〉 구성 준수 〉 관리 〉 승인 규칙 〉 정정 작업 필드 변경 요청 〉 정정 작업 할당 해제.

프로시저

1. 다음으로 이동 모두 〉 구성 준수 〉 내 승인.

2. 큐에서 요청을 선택합니다.

3. 적절한 코멘트를 추가하여 요청을 승인하거나 거부합니다.

테스트 결과 자동 종결

폐기된 CI(구성 항목)와 연결된 테스트 결과(TR)를 자동으로 닫을 수 있습니다.

자동 종결 옵션을 구성하려면 시스템 속성 **sn_vulc.auto_close_test_results_linked_to_retired_CIs** 로 이동하여 true로 설정합니다. 폐기된 CI와 관련된 TR을 자동으로 종결하려면 문서를 폐기된 CI와 관련된 테스트 결과 자동 종결참조하십시오.

폐기된 구성 항목 작업에 대한 자세한 내용은 다음 문서를 참조하십시오 Configuration Compliance에서 폐기된 구성 항목 작업.

주:
의 구성 준수v14.9부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v14.9 이전 용어	용어 **v14.9** 이상
테스트 결과 그룹	정정 작업
그룹 규칙	정정 작업 규칙
정책	테스트 그룹

Configuration Compliance에서 폐기된 구성 항목 작업

해제된 CI(구성 항목)는 에서 폐기, 보관 또는 삭제됨 상태로 구성 관리 데이터베이스(CMDB)이동됩니다. 에는 구성 준수 CI로 구성된 테스트 결과(TR)가 포함되어 있습니다. CI의 상태가 폐기됨으로 업데이트되면 연결된 TR은 하위 상태가 'CI 해제됨'으로 종결됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
의 구성 준수v14.9부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v14.9 이전 용어	용어 **v14.9** 이상
테스트 결과 그룹	정정 작업
그룹 규칙	정정 작업 규칙
정책	테스트 그룹

CMDB가 CI의 수명주기 스테이지 상태를 폐기됨으로 변경하는 경우 연결된 TR을 자동으로 닫도록 선택할 수 있습니다. 연결된 테스트 결과 자동 닫기에 대한 자세한 내용은 다음 문서를 참조하십시오 폐기된 CI와 관련된 테스트 결과 자동 종결.

폐기된 CI는 결국 CMDB.

CI 폐기의 영향:

- 검색된 항목에 미치는 영향: CI가 폐기되면 관련 DI가 'CI 해제됨'으로 표시됩니다.
- 테스트 결과에 미치는 영향: DI의 상태가 'CI 해제됨'으로 업데이트되면 연결된 TR이 종결되고 메모 섹션이 자동으로 업데이트됩니다.

주:
DI의 상태는 CI의 수명주기 상태가 업데이트될 때마다 자동으로 'CI 해제됨'으로 업데이트됩니다. 반면에 **sn_vulc.auto_close_test_results_linked_to_retired_CIs** 속성이 true로 설정된 경우에만 TR의 상태가 종결됨으로 업데이트됩니다. 연결된 테스트 결과 자동 닫기에 대한 자세한 내용은 다음 문서를 참조하십시오 폐기된 CI와 관련된 테스트 결과 자동 종결.

예약된 작업은 *`Close Test Results for decommissioned CIs`* 업데이트된 DI에 대해 매일 실행됩니다. 폐기된 CI에 대해 자동 종결 구성 옵션이 활성화된 경우 해제된 CI가 포함된 DI를 식별하고 하위 상태가 'CI 해제됨'인 관련 TR을 종결합니다. 정정 작업의 모든 TR이 종결되고 하위 상태가 CI 해제됨인 경우 정정 작업도 하위 상태가 '취소됨'으로 종결됩니다.

주:
CI가 '폐기됨' 상태에서 원래 상태로 다시 이동하면 '검색된 항목' 항목도 업데이트됩니다. 스캐너에서 데이터를 다시 수집하면 TR이 자동으로 열립니다.

폐기된 CI와 관련된 테스트 결과 자동 종결

이 구성 관리 데이터베이스(CMDB) CI(구성 항목)의 수명 주기 스테이지 상태를 폐기됨으로 변경하는 경우 관련 테스트 결과(TR)를 자동으로 종결하도록 선택할 수 있습니다.

시작하기 전에
필요한 역할: sn_vulc.admin

이 태스크 정보
연결된 TR을 자동으로 종결하려면 시스템 속성 **sn_vulc.auto_close_test_results_linked_to_retired_CIs** 를 활성화하여 폐기된 CI와 연결된 TR을 자동으로 종결해야 합니다. 이 옵션을 사용하면 동일한 CI에 대해 보고된 신규 및 기존 TR이 자동으로 "종결" 상태로 생성되거나 업데이트됩니다. 이는 스캐너 페이로드의 자산 ID와 검색된 항목 항목 상태를 기반으로 합니다. 폐기된 CI의 영향에 대한 자세한 내용은 다음 문서를 참조하십시오 Configuration Compliance에서 폐기된 구성 항목 작업.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
DI의 상태는 CI의 수명주기 상태가 업데이트될 때마다 'CI 해제됨'으로 업데이트됩니다. 반면에 **sn_vulc.auto_close_test_results_linked_to_retired_CIs** 시스템 속성이 활성화된 경우에만 TR의 상태가 종결됨으로 업데이트됩니다.

프로시저

1. 다음으로 이동 시스템 속성 〉 모든 속성 을 클릭하고 이름 열에서 필터링 *sn_vulc.auto_close_test_results_linked_to_retired_CIs* 합니다.
2. 속성을 선택합니다.
3. 폐기된 CI와 관련된 테스트 결과를 자동으로 종결하려면 속성 값을 true로 설정합니다.

에서 부실 테스트 결과 자동 종결 구성 준수

부실 테스트 결과 자동 종결 기능을 활성화하여 외부 공급업체 통합에서 최근에 발견되지 않은 오래된 테스트 결과를 자동으로 종결할 수 있습니다. 이러한 테스트 결과를 종결-부실 로 이동하면 인스턴스의 활성 테스트 결과 및 정정 작업 수가 줄어들고 구성 관리 데이터베이스(CMDB).

주:
의 구성 준수v14.9부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v14.9 이전 용어	용어 **v14.9** 이상
테스트 결과 그룹	정정 작업
그룹 규칙	정정 작업 규칙
정책	테스트 그룹

개요

부실 테스트 결과 자동 종결 모듈을 사용하면 외부 공급업체 통합에서 최근에 발견되지 않은 오래된 부실 테스트 결과를 자동으로 종결할 수 있습니다. 조건 작성기에서 설정한 조건에 따라 테스트 결과가 종결-부실 로 이동됩니다.

주요 용어

테스트 결과

테스트 결과는 기술 자산 클래스를 관리하는 방법을 정의하는 프레임워크, 정책 및 권한 있는 소스에 매핑된 구성 테스트 라이브러리에서 가져온 결과입니다. 애플리케이션은 구성 준수 테스트 결과를 계산하지 않지만 외부 공급업체 통합을 통해 결과를 임포트합니다.

마지막으로 검사한 자산 날짜

테스트 결과와 관련된 검색된 항목 테이블의 마지막 구성 준수 검사 날짜 열 값을 나타냅니다. 이 날짜는 외부 공급업체 스캐너에서 자산을 마지막으로 검사한 가장 현재 날짜 및 시간을 나타냅니다.

마지막 실패 날짜

결과 필드 값이 〔실패〕일 때 테스트 결과 테이블의 마지막으로 본 열 날짜를 참조합니다.

부실 테스트 결과

오래되어 상당한 시간 동안 외부 공급업체 통합 검사에서 발견, 업데이트 또는 탐지되지 않은 인스턴스의 테스트 결과를 나타냅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

마지막으로 발견된 테스트 결과

이 검색 옵션은 외부 공급업체 스캐너에서 제공하는 날짜 및 시간을 사용합니다. 이 용어는 스캐너에서 테스트 결과를 다시 찾은 가장 최근 또는 최근 날짜(며칠 전)를 나타냅니다. 이 매개변수를 구성할 수 있습니다.

사용 케이스

때때로 자산(구성 항목)이 사용자 환경에서 폐기되거나 외부 공급업체 스캐너에 의해 제거될 수 있습니다. 이 경우 자산과 관련된 구성 테스트 결과가 임포트한 탐지에 의해 애플리케이션에서 업데이트되지 구성 준수 않고 비활성화(부실) 상태가 됩니다.

인스턴스에서 활성 테스트 결과(TR) 및 정정 작업(RT)의 수를 줄이려면 부실 테스트 결과 자동 종결 기능을 활성화합니다. 이 기능은 상태가 변경되지 않았거나 통합에서 최근에 임포트되지 않은 오래된 테스트 결과를 자동으로 종결합니다.

예를 들어 특정 CI(구성 항목)에 여러 개의 자산 ID가 있고 지난 90일 동안 외부 공급업체 스캐너에서 탐지된 경우 이러한 ID 중 하나를 임포트하지 않았다고 가정해 보겠습니다. 부실 테스트 결과 자동 종결 모듈에서 지난 90일 이상 발견되거나 업데이트되지 않은 테스트 결과를 종결하도록 조건 작성기를 설정하면 이 기능이 이 필터링과 일치하는 모든 테스트 결과를 자동으로 종결합니다.

주:
이 기능은 조건 작성기에서 설정하고 외부 공급업체 스캐너 통합에 의해 탐지되는 필터 조건에 따라서만 테스트 결과 탐지를 종결합니다.

해결 필드

제품 등의 외부 공급업체 스캐너 Qualys 에 의해 종결된 탐지와 인스턴스의 부실 테스트 결과 자동 종결 기능을 구분하기 위해 해결 필드 〔종결-부실〕에 대한 새 값이 추가되었습니다.Tenable.io 종결-부실 은 TR이 자동 종결 기능에 의해 종결되었음을 나타냅니다. 종결 또는 고정-종결 은 TR이 스캐너에 의해 닫혔음을 나타냅니다.

자동 종결 기능을 사용하여 **TR** 상태를 TRG로 롤업

테스트 결과의 상태 진행률 및 우선순위는 다음과 같습니다. 오픈 〉 종결됨 〉 고정-종결 〉 종결-부실.

1. TRG의 TR이 오픈인 경우 TRG 상태는 변경되지 않습니다.
2. 하나 이상의 TR이 종결 - 고정 이고 나머지는 종결 - 부실인 경우 TRG 상태가 종결 - 고정으로 전환됩니다.
3. TRG의 모든 TR이 종결 - 부실인 경우 TRG 상태가 종결 - 취소됨으로 전환됩니다.

지원되는 통합

이 기능을 지원하는 외부 공급업체 통합에 대한 자세한 내용은 해당 Tenable.io및 구성 준수 애플리케이션과의 취약성 대응 통합문서를 참조하십시오Qualys Vulnerability Integration 이해.

부실 테스트 결과 자동 종결 사용 구성 준수

부실 테스트 결과 자동 종결(TR)을 활성화하여 설정한 필터 조건에 따라 오래된 테스트 결과를 자동으로 종결합니다.

시작하기 전에
이 기능, 주요 용어 및 테스트 결과 데이터를 임포트하는 외부 공급업체 통합에 필요할 수 있는 설정에 대한 자세한 내용은 문서를 에서 부실 테스트 결과 자동 종결 구성 준수참조하십시오.

필요한 역할: sn_vulc.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 구성 준수 〉 관리 〉 부실 테스트 결과 자동 종결.
2. 필드에 내용을 입력합니다.

필드	값
이름	이 구성 기록의 이름입니다.
활성	선택하면 이 기록이 활성화되고 필터 기준과 일치하는 테스트 결과가 있으면 자동으로 종결됩니다.
지연된 TR에 대한 부실 TR 무시	선택하는 경우 검토 중 또는 연기됨 상태에 매핑된 모든 TR이 무시되고 종결되지 않습니다. 이 옵션의 선택을 취소하면 기준과 일치하는 모든 TR이 종결됩니다.
실행 순서	기본값은 100입니다. 이 값은 부실 테스트 결과를 찾아 표시하는 데 사용되는 각 구성 기록의 실행 순서를 오름차순으로 결정합니다.
설명	이 기록에 대한 설명입니다. 이 텍스트는 더 많은 수의 기록을 생성할 경우 쉽게 다시 찾을 수 있도록 도와줍니다.
조건	닫으려는 TR을 찾는 데 사용되는 필터링 조건입니다. 기본 필터는 검색된 항목 〉 마지막 검사.

3. 제출을 클릭합니다.

   예약된 작업 이(가) *Auto-Close Stale Test Results*매일 실행됩니다. 이 작업은 사용자가 제공한 조건을 기반으로 TR을 식별하고 상태: 종결됨과 일치하는 TR을 전환합니다.

   TR이 상태: 종결-부실로 표시된 후 스캐너가 이러한 TR을 다시 찾으면 테스트 결과가 다시 열리고 상태가다시 오픈으로 전환됩니다.

   TR이 상태: 종결-부실로 표시되고 스캐너에서 수정된 것으로 확인되면(해상도: 수정됨) TR이 상태: 종결 됨 해결: 수정됨으로 전환됩니다. **Result**: **Pass**가 있는 TR은 State: **Closed** **Resolution**: **Fixed**로 유지됩니다. 또한 상태는 다음 목록에 설명된 대로 정정 작업으로 롤업됩니다.

   a. 정정 작업의 TR이 열려 있으면 정정 작업 상태가 변경되지 않습니다.
   b. 하나 이상의 TR이 상태: 종결 됨 해결: 수정 됨이고 나머지는 종결-부실인 경우 정정 작업 상태는 종결 됨 해결: 수정됨으로 전환됩니다.
   c. 정정 작업의 모든 테스트 결과가 종결 해결: 수정인 경우 TRG 상태가 상태: 종결 됨 해결: 취소됨으로 전환됩니다.

   상태 전환에 대한 자세한 내용은 다음 문서를 참조하십시오 애플리케이션의 테스트 결과 및 정정 작업 상태 전환 구성 준수.

정정 작업 닫기

추가 분석 없이 정정 작업과 관련된 문제를 즉시 종결할 수 있는 것으로 확인되면 종결 기능을 사용할 수 있습니다.

시작하기 전에
필요한 역할:

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- sn_vulc.admin
- sn_vulc.remediation_owner

> 주:
> sn_vulc.remediation_owner 역할을 사용하여 사용자 또는 할당 그룹에 할당된 정정 작업을 재할당하거나 종결할 수 있습니다.

이 태스크 정보
의 구성 준수v15.0부터 정정 작업에 대한 닫기 버튼이 제거되었습니다.

정정 작업을 해결하면 해결 메모 는 모든 테스트 결과의 작업 메모에 반영됩니다.

프로시저

1. 정정 작업 기록을 엽니다.
2. 닫기 단추를 선택합니다.
3. 팝업 창에서 문제가 종결되는 이유를 설명합니다.
4. 닫기를 선택합니다.

관련 정보

구성 준수 상태

정정 작업에 대한 예외 요청 및 승인

지정된 기간 동안 정정 작업의 정정을 연기하도록 요청할 수 있습니다. 승인자 그룹에 속한 사용자는 예외 요청을 승인할 수 있습니다.

> 주:
> 의 구성 준수v14.9부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v14.9 이전 용어	용어 **v14.9** 이상
테스트 결과 그룹	정정 작업
그룹 규칙	정정 작업 규칙
정책	테스트 그룹

예외 요청을 요청하거나 승인하려면 다음을 참조하십시오.

- 의 정정 작업에 대한 예외 요청 구성 준수
- 에서 예외 요청 승인 구성 준수

> 주:
>
> 이메일 알림은 예외 관리의 모든 단계에서 전송되어 요청의 상태 및 기타 세부 정보를 제공합니다. 예를 들어 예외가 요청되면 요청자는 요청이 발생했음을 확인하는 이메일을 받습니다. 또한 승인자는 예외가 요청되었다는 내용의 이메일을 받습니다.
>
> 의 구성 준수v14.11 부터 일정 기간(일) 후에 승인자와 요청자 모두에게 이메일 알림을 보내고, 예외를 승인하기 위한 시간 범위를 구성할 수 있습니다. 요청이 발생하면 테스트 결과가 검토 중 상태로 변경되고 상태 변경 기록이 생성됩니다. 승인자가 구성된 시간 범위 내에 응답하지 않으면 테스트 결과가 열림 상태로 되돌아갑니다. 이전 상태는 **backup_state** 필드에 저장됩니다. 자세한 내용은 예외 관리에 대한 승인 규칙 구성 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

의 정정 작업에 대한 예외 요청 구성 준수

즉시 정정할 수 없는 경우 지정된 기간 동안 정정 작업의 정정을 연기하는 예외를 요청합니다.

시작하기 전에
필요한 역할: sn_vulc.remediation_owner

이 태스크 정보

중요사항:
다음에 대한 예외를 요청할 수 있습니다.

- 의 정정 작업 취약성 관리자 작업 공간 및 IT 정정 작업 공간. 자세한 내용은 에서 예외 요청 IT 정정 작업 공간 문서를 참조하십시오.
- 에서 취약성 관리자 작업 공간동시에 여러 테스트 결과가 . 자세한 내용은 취약성 관리자 작업 공간에서 대량 예외 요청 문서를 참조하십시오.

주:
의 구성 준수v14.9부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v14.9 이전 용어	용어 **v14.9** 이상
테스트 결과 그룹	정정 작업
그룹 규칙	정정 작업 규칙
정책	테스트 그룹

프로시저

1. 다음으로 이동 모두 〉 구성 준수 〉 정정 작업 〉 모든 작업.
2. 예외를 요청하려는 정정 작업을 선택합니다.
   선택한 작업은 오픈, 조사 중 또는 구현 대기 중 상태여야 합니다.
3. 정정 작업 양식에서 예외 요청을 클릭합니다.

   주:
   또는 GRC: 정책 및 준수 관리 에서 선택되었는지 여부에 취약성 대응 따라 구성 준수 〉 예외 관리 화면에 예외 요청 양식이 변경됩니다. 에 대한 예외 관리 구성 구성 준수 문서를 참조하십시오.

4. 이 옵션을 선택한 경우 취약성 대응 예외 관리 화면에서 다음을 수행합니다.

   a. 양식에서 필드를 채웁니다.

예외 요청 양식

필드	설명
다음까지	예외 요청이 만료되는 날짜입니다. 이 날짜는 에서 선택한 기간 내에 있어야 합니다. 모두 〉 구성 준수 〉 관리 〉 예외 관리 화면. 예외 요청이 만료되면 정정 작업이 열림 상태로 되돌아갑니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	주: (CC) 버전 14.7 구성 준수 부터 예외 기간이 만료되기 전에 스캐너에서 지연된 정정 작업을 다시 열면 정정 작업의 상태가 열림에서 연기됨으로 변경됩니다. 이 기능은 기본적으로 비활성화되어 있습니다. 이 기능을 사용하려면 시스템 속성 *sn_vulc.auto_defer_test_result_in_active_exc* 값을 true로 설정합니다. 또한 만료 날짜 이후 정정 작업이 다시 열린 후에도 연기된 종료 날짜가 유지됩니다.
이유	예외 이유입니다. 선택 항목은 다음과 같습니다. ▪ 위험 수락됨 ▪ 유지관리 기간을 기다리는 중 ▪ 수정 사용 불가 ▪ 사용 중인 완화 통제 ▪ 기타 새 이유 선택 항목을 추가하는 방법을 보려면 다음 문서를 참조하십시오 정책 이유 매핑 정의.
추가 정보	이 요청이 수행되는 이유와 관련된 상세 정보입니다. 이 필드는 정정 소유자가 업데이트해야 합니다.

b. Request Approval을 클릭하여 예외 요청을 제출합니다.

결과
정정 작업의 상태가 검토 중으로 변경됩니다. 상태 변경 승인 탭을 사용하여 예외 요청의 상태를 추적합니다.

정정 작업 연장 요청

지연된 정정 작업이 지연 기한에 도달하기 전에 해당 작업에 대한 연장을 요청합니다. 정정 소유자는 더 이상 이 요청을 하기 위해 지연된 기한까지 기다릴 필요가 없습니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)

이 태스크 정보
작업 공간에서 연장을 취약성 대응 요청할 수도 있습니다. 자세한 내용은 취약성 관리자 작업 공간에서 지연된 취약한 항목에 대한 연장 요청 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
의 구성 준수v14.9부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v14.9 이전 용어	용어 **v14.9** 이상
테스트 결과 그룹	정정 작업
그룹 규칙	정정 작업 규칙
정책	테스트 그룹

프로시저

1. 다음으로 이동 모두 〉 구성 준수 〉 정정 작업.
2. 지연된 정정 작업을 엽니다.
3. 연장 요청을 선택합니다.
4. 양식의 필드에 적절히 입력합니다.

필드	설명
연장 날짜	지연 상태가 만료되고 정정 작업이 다시 시작되는 날짜를 선택합니다.
이유	문제를 지연시키는 이유를 입력합니다. 선택 항목은 다음과 같습니다. ○ 유지관리 기간을 기다리는 중 ○ 수정 사용 불가 ○ 수용된 위험 ○ 사용 중인 완화 통제 ○ 기타
추가 정보	기타 관련 정보를 입력합니다.

5. 승인 요청을 선택합니다.

주:
- 요청은 두 가지 수준의 승인을 거칩니다.
- 연장 요청 버튼은 예외 규칙의 일부로 생성된 정정 작업에 사용할 수 없습니다.
- 지연된 정정 작업이 다시 연장되면 백엔드에서 연장 지연 수가 증가합니다.

에서 예외 규칙에 대한 연장 요청 구성 준수

지연된 예외 규칙이 기한까지 지연되기 전에 해당 규칙의 연장을 요청합니다. 정정 소유자는 더 이상 이 요청을 하기 위해 지연된 기한까지 기다릴 필요가 없습니다.

시작하기 전에
필요한 역할: sn_vul.exception_approver

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보
작업 공간에서 연장을 취약성 대응 요청할 수도 있습니다. 자세한 내용은 취약성 관리자 작업 공간에서 지연된 취약한 항목에 대한 연장 요청 문서를 참조하십시오.

주:
의 구성 준수v14.9부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v14.9 이전 용어	용어 **v14.9** 이상
테스트 결과 그룹	정정 작업
그룹 규칙	정정 작업 규칙
정책	테스트 그룹

프로시저

1. 다음으로 이동 모두 〉 구성 준수 〉 예외 규칙.
2. 승인된 예외 규칙을 선택합니다.
3. 연장 요청을 선택합니다.
4. 양식의 필드에 적절히 입력합니다.

필드	설명
연장 날짜	예외 규칙을 연장해야 하는 종료 날짜를 선택합니다.
이유	예외 규칙을 지연시키는 이유를 입력합니다. 선택 항목은 다음과 같습니다. ○ 수용된 위험 ○ 유지관리 기간을 기다리는 중 ○ 수정 사용 불가 ○ 사용 중인 완화 통제 ○ 기타
추가 정보	기타 관련 정보를 입력합니다.

5. 승인 요청을 선택합니다.
요청이 승인되면 예외 규칙 및 관련 정정 작업에 대해 지연 기한, 이유 및 추가 정보 필드가 업데이트됩니다. 요청 제출 및 승인자의 후속 조치 시에도 이메일이 트리거됩니다.

주:
- 요청은 두 가지 수준의 승인을 거칩니다.
- 지연된 예외 규칙이 다시 확장되면 백엔드에서 연장 지연 수가 증가합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

를 사용하여 정정 작업에 대한 예외 요청 **GRC:** 정책 및 준수 관리

에서 애플리케이션의 구성 준수정책 예외 관리 기능을 정책 및 준수 관리 사용하여 GRC 정책 예외를 요청합니다.

시작하기 전에

정책 예외 통합을 사용하여 정책 예외를 요청하려면 먼저 에서 ServiceNow Store애플리케이션을 다운로드 GRC: 정책 및 준수 관리 해야 합니다.

필요한 역할: sn_vulc.remediation_owner

클래식 UI에서 예외를 요청할 수도 있습니다.

이 태스크 정보

중요사항:
관리자와 정정 소유자는 각각 취약성 관리자 작업 공간 및 IT 정정 작업 공간의 정정 작업(RT)에 대한 정책 예외를 요청할 수 있습니다.

주:
의 구성 준수v14.9부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v14.9 이전 용어	용어 **v14.9** 이상
테스트 결과 그룹	정정 작업
그룹 규칙	정정 작업 규칙
정책	테스트 그룹

프로시저

1. 다음으로 이동 모두 〉 애플리케이션 취약성 대응 〉 애플리케이션 취약한 항목 (또는 정정 작업)〉모두로 설정하고 예외를 요청할 항목 또는 그룹을 엽니다.
   선택한 항목 또는 그룹은 오픈, 조사 중 또는 구현 대기 중 상태여야 합니다.
2. 선택한 양식에서 예외 요청을 클릭합니다.
3. 이 옵션을 선택한 경우 GRC: 정책 및 준수 관리 예외 관리 화면에서 다음을 수행합니다.

   a. 양식에서 필드를 채웁니다.

예외 요청 양식

필드	설명
정책	예외를 요청하는 취약성 관리 정책입니다.
컨트롤 목적	선택한 정책과 연결된 통제 목표입니다. 정책을 선택하지 않으면 모든 통제 목표가 나열됩니다.
유효 기간(시작)	예외가 시작되는 날짜입니다. 기본값은 현재 날짜입니다. 이 날짜는 과거일 수 없습니다.
유효 기간	정책 예외가 만료되고 취약한 항목 또는 그룹의 상태가 연기됨에서 미결로 변경되는 날짜입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	주: 정책 예외가 유효한 일 수는 정책 및 준수에서 정책에 대해 설정한 최대 예외 기간(일) 을 초과할 수 없습니다. 자세한 내용은 정책 만들기를 참조하세요.
이유	예외를 요청하는 이유입니다.
근거	이 요청이 수행되는 이유와 관련된 상세 정보입니다. 정정 소유자가 이 필드를 입력해야 합니다.

b. **Request Approval**을 클릭하여 예외 요청을 제출합니다.
정정 작업의 상태가 검토 중으로 변경되고 정책 예외가 생성됩니다. 상태 변경 승인 탭을 사용하여 예외 요청의 상태를 추적합니다.

c. 정책 예외 관련 목록을 클릭하여 정책 예외를 봅니다.

d. 정책 예외 번호를 클릭합니다.

e. 승인자 필드에서 승인자의 이름을 선택합니다.

f. 소스 탭을 클릭하고 통제 목표 필드에서 통제 목표를 선택합니다.

g. 위험 평가 탭을 클릭하고 위험 등급 필드에서 위험 등급을 선택합니다.

h. 양식을 저장합니다.

i. 영향을 받는 컨트롤 탭을 클릭합니다.

j. 추가를 클릭하여 컨트롤을 추가합니다.

k. 양식을 저장합니다.

주:
규정 준수 검토 요청을 클릭하여 규정 준수 검토를 제기할 수 있습니다.

승인 양식이 승인자에게 전송됩니다.

승인자는 승인을 클릭하여 요청을 승인하거나 추가 승인 요청을 클릭하여 추가 승인을 요청할 수 있습니다.

기록 상태가 연기됨으로 변경됩니다. 명시된 이유는 예외 요청을 제기할 때 선택한 이유입니다. 지연 탭에는 기록에 대한 추가 메모가 제공됩니다.

주:
요청이 거부되면 기록이 이전 상태로 이동합니다.

4. 제출을 클릭합니다.
정책 예외 통합 및 정정 소유자와 준수 관리자 간의 핸드오프에 대한 자세한 내용은 정책 및 준수 관리 선택적 설정을 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

에서 예외 요청 승인 구성 준수

즉시 정정할 수 없는 정정 작업에 대한 예외 요청을 승인합니다. 이러한 위험 요청을 평가한 다음 정정할 수 있을 때까지 연기하도록 승인해야 합니다.

중요사항:
관리자 또는 분석가는 취약성 관리자 작업 공간에서 예외 요청을 승인하거나 거부할 수 있습니다.

시작하기 전에
필요한 역할: sn_vulc.exception_approver

프로시저

1. 다음으로 이동 모두 〉 구성 준수 〉 내 승인.
2. 큐에서 요청을 선택합니다.
3. 적절한 설명을 사용하여 요청을 승인하거나 거부합니다.

주:
2단계 승인 워크플로우의 경우, 첫 번째 수준 승인 후 추가 승인을 위해 요청이 두 번째 수준으로 제출됩니다. 두 번째 수준에 사용자가 없는 경우, 요청은 첫 번째 수준 승인 후 자동으로 승인됩니다.

요청이 승인되면 정정 작업이 연기됨 상태로 전환됩니다. 거부되는 경우 정정 작업은 이전 상태로 되돌아갑니다.

정책 이유 매핑 정의

예외를 요청하는 모든 사용자가 사용할 수 있는 이유 선택 항목을 정의할 수 있습니다.

시작하기 전에
필요한 역할: sn_vul.compliance.manager 및 sn_vulc.admin

프로시저

1. 다음으로 이동 모두 〉 정책 및 준수 〉 정책 예외 〉 통합 레지스트리.

주:
이유 선택 테이블에 있는 이유 선택 항목에서 이유를 선택하거나 새 이유를 추가할 수 있습니다.

2. 컨테이너 취약성 대응 - CVIT 통합 레지스트리를 클릭합니다.
3. 기존 이유 선택을 추가하려면 다음 단계를 수행합니다.
   a. 이유 선택 목록에서 새로 만들기를 클릭합니다.
   b. 돋보기 아이콘을 클릭하여 이유를 선택합니다.
4. 이유 선택 테이블에 새 이유 선택 사항을 추가하려면 다음 단계를 수행합니다.
   a. 이유 선택 목록에서 새로 만들기를 클릭합니다.
   b. 돋보기 아이콘을 클릭합니다.
   c. 새로 만들기를 클릭합니다.
   d. 양식에서 필드를 채웁니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이유 선택 목록 양식

필드	설명
레이블	이 선택 항목의 고유 레이블입니다.
값	이 선택 항목의 고유 값입니다. 이 값은 각 애플리케이션에 대한 정책 예외 이유 매핑 테이블에 매핑됩니다. 이 테이블로 이동하려면 sn_sec_cmn_policy_reason_mapping를 입력합니다. 필터 탐색기의 LIST.
순서	이 선택 항목에 대한 순서입니다. 이유는 이 숫자를 기준으로 정렬됩니다.
기본값	요청 시 정책 예외가 요청될 때마다 이 이유 선택을 사용할 수 있음을 나타내는 옵션입니다. 통합 레지스트리에 애플리케이션별 선택 항목이 포함되어 있지 않으면 기본 필드가 선택된 모든 이유 선택 항목을 사용할 수 있습니다.
활성	이유 선택 목록에 선택 항목을 표시하는 옵션입니다.

5. 제출을 클릭합니다.

구성 준수에 대한 분석 및 보고

모니터링을 위해 다음 보고서가 제공됩니다.

개요 보고서에서 정책, CI, 테스트 및 테스트 결과를 구성 준수 봅니다.

주:
의 구성 준수v14.9부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v14.9 이전 용어	용어 **v14.9** 이상
테스트 결과 그룹	정정 작업
그룹 규칙	정정 작업 규칙
정책	테스트 그룹

구성 준수 보고

홈페이지는 구성 준수 정책, CI, 테스트 및 테스트 결과에 대한 경영진 뷰를 제공하여 보안 직원이 관심 영역을 신속하게 파악할 수 있도록 도와줍니다. 구성 준수 필요에 따라 유의성 차트를 추가할 수 있습니다. 전역 검색 기능을 사용하여 관련 정보를 반환할 구성 준수 수도 있습니다.

주:
의 구성 준수v14.9부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v14.9 이전 용어	용어 **v14.9** 이상
테스트 결과 그룹	정정 작업
그룹 규칙	정정 작업 규칙
정책	테스트 그룹

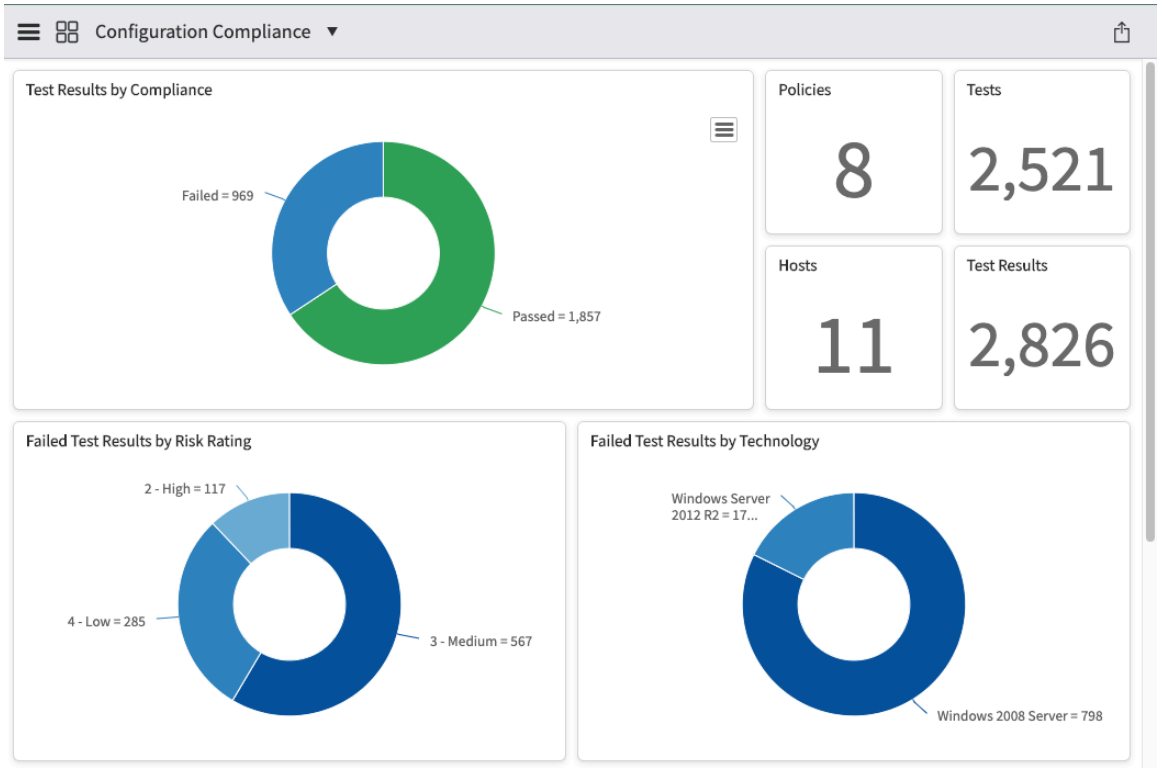
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

각 차트에서 차트의 특정 부분(막대형, 원형, 데이터 요소)을 가리키면 차트의 해당 부분과 관련된 일반 데이터를 볼 수 있습니다. 보고서의 일부를 클릭하면 자세한 정보를 제공하는 목록이 열립니다.

주:

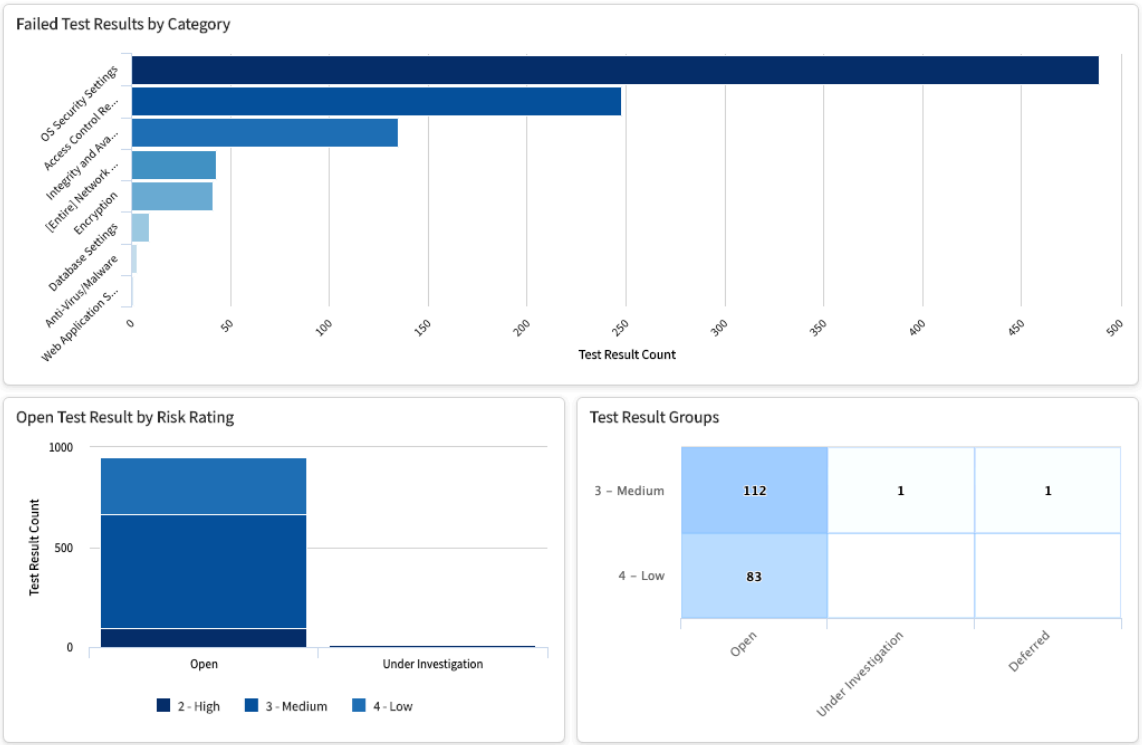
- 홈페이지의 구성 준수 대시보드는 구성 준수용 퍼포먼스 분석 애플리케이션이 활성화된 경우에만 사용할 수 있습니다. 이 애플리케이션을 활성화하는 단계는 문서를 참조하십시오 구성 준수용 퍼포먼스 분석 활성화.
- sn_vulc.read 역할을 가진 사용자는 누구나 대시보드를 볼 수 있습니다. sn_vulc.write 또는 sn_vulc.admin 역할의 모든 사용자가 대시보드를 만들고 편집할 수 있습니다. sn_vulc.admin만 대시보드를 삭제할 수 있습니다.

취약성 개요 보고서



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

구성 준수 보고서



취약성 개요 보고서

이름	Visual	설명
준수별 테스트 결과	도넛형	통과 또는 실패한 오픈 테스트 수를 표시합니다.
정책을	번호	실패한 테스트 결과가 있는 정책 수입니다.
테스트	번호	실패한 테스트 결과가 있는 테스트의 수입니다.
호스트	번호	실패한 테스트 결과가 있는 호스트 수입니다.
테스트 결과	번호	테스트 결과 수를 표시합니다.
위험 등급별 실패한 테스트 결과	도넛형	위험 등급별로 실패한 테스트 수를 표시합니다.
기술별 실패한 테스트 결과	도넛형	실패한 테스트가 있는 모델을 표시합니다.
범주별 실패한 테스트 결과	막대	가장 많이 실패한 테스트 결과가 있는 범주를 표시합니다.
위험 등급별 열린 테스트 결과	막대	위험 등급별로 열린 테스트 결과 수를 표시합니다.
정정 작업	차트	상태 및 위험 등급별로 정정 작업을 표시합니다.

구성 준수 대시보드

여기에는 플랫폼 분석 솔루션 다른 ServiceNow AI Platform 제품과 함께 사용할 사전 패키징 퍼포먼스 분석 된 보고 컨텐츠가 포함됩니다. 이를 플랫폼 분석 솔루션 통해 미준수 호스트 수준 및 클라우드 제어부 구성에 대한 가시성을 제공합니다.

이 플랫폼 분석 솔루션에는 다른 ServiceNow AI Platform 제품과 함께 사용하기 위해 사전 패키징된 퍼포먼스 분석 및 보고 컨텐츠가 포함되어 있습니다. 이 플랫폼 분석 솔루션은 미준수 호스트 수준 및 클라우드 컨트롤 플레인 구성에 대한 가시성을 제공합니다.

구성 준수용 퍼포먼스 분석 대시보드에는 다양한 차원의 데이터를 제공하는 여러 위젯이 포함되어 있습니다. 규정 준수 추세, 구성 문제, 정정 추세 및 예외 관리에 대한 포괄적인 뷰를 제공합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
퍼포먼스 분석 프레임워크에서 넥스트 경험 (PA) 대시보드를 보려면 구성 준수 for 구성 준수 플러그인을 설치해야 합니다. 설치되어 있지 않은 경우 보고 프레임워크를 사용하여 작성된 기존 대시보드를 볼 수 있습니다.

구성 준수용 퍼포먼스 분석 활성화

플랫폼 분석 솔루션용 콘텐츠 팩 ServiceNow Store 애플리케이션을 활성화합니다.

시작하기 전에

이 플랫폼 분석 솔루션을 활성화하는 인스턴스에서 퍼포먼스 분석의 전체 구독 버전을 활성화합니다. 구독을 구입하지 않아도 비프로덕션 인스턴스에서 퍼포먼스 분석를 활성화할 수 있습니다. 자세한 내용은 퍼포먼스 분석 구독 활성화 를 참조하십시오.

고려 중인 인스턴스에 대한 애플리케이션을 요청하려면 계정과 권한이 필요합니다 Now Support . Now Support 계정과 인스턴스는 동일한 회사에 속해 있어야 합니다. 자세한 내용은 ServiceNow Store의 ServiceNow 제품 설치 를 참조하십시오.

필요한 역할: 관리자

이 태스크 정보

대시보드에 구성 준수 사용하여 퍼포먼스 분석 정정 작업, 준수 상태, 정정 작업 및 예외 요청에 대한 보고서를 생성합니다.

프로시저

1. 다음으로 이동 모두 〉 시스템 애플리케이션 〉 모든 애플리케이션 〉 **ServiceNow Store**.
2. 유효한 권리가 퍼포먼스 분석구성 준수 있는지 찾아보고 확인합니다.
3. ## ### ## #### ### 검색합니다.
4. 애플리케이션을 설치합니다.

   이 애플리케이션을 설치하면 애플리케이션도 구성 준수 활성화됩니다.

용 구성 준수 대시보드 보기 퍼포먼스 분석

(PA) 대시보드에서 보고서를 확인하여 가장 중요한 구성 문제를 관리하고 신속하게 정정할 수 있습니다 구성 준수 퍼포먼스 분석 .

주:
의 구성 준수v14.9부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v14.9 이전 용어	용어 **v14.9** 이상
테스트 결과 그룹	정정 작업
그룹 규칙	정정 작업 규칙
정책	테스트 그룹

필요한 **ServiceNow AI Platform** 역할

대시보드에 구성 준수 퍼포먼스 분석 필요한 역할은 다음과 같습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 관리자: 관리자는 를 구성 준수 설치 및 활성화 퍼포먼스 분석 하고 시스템 속성을 변경할 수 있습니다.
- pa_admin: Performance Analytics 관리자는 백그라운드 작업, 표시기, 세부 항목, 위젯 및 대시보드를 만들고 검토할 수 있습니다. 이 관리자는 데이터 수집을 설정하고 시작할 수도 있습니다.
- sn_vulc.read: 읽기 역할이 있는 사용자가 대시보드 데이터를 검토할 수 있습니다.

대시보드에 구성 준수 액세스

대시보드를 열려면 다음으로 이동합니다. 모두 〉 구성 준수 〉 개요.

중요사항:

의 구성 준수버전 14.9부터 이 대시보드는 Next Experience UI에서도 볼 수 있습니다. 새 UI에서 대시보드를 보려면 다음으로 이동합니다. 작업 공간 〉 취약성 관리자 작업 공간 을 클릭하고 대시보드 아이콘을 클릭합니다. 역할에 따라 기본 대시보드가 표시됩니다. 다른 대시보드를 보려면 대시보드 이름 옆에 있는 드롭다운을 클릭합니다. 자세한 내용은 취약성 관리자 작업 공간의 대시보드 와 IT 정정 작업 공간의 대시보드를 참조하십시오.

주:
Tokyo에 있는 경우 Next Experience UI에서 대시보드를 볼 수 있지만 일부 기능 손실이 있습니다.

구성 준수 **[PA]** 대시보드 탭

개요 탭

개요 탭에는 5개의 필터가 있습니다. 이러한 필터는 자산 범주, 클라우드 자원 유형, 클라우드 서비스 제공자, 클라우드 계정 및 클라우드 영역이며, 적용된 필터에 대한 보고서를 시각화하는 데 적용할 수 있습니다. 범주를 선택하고 변경 내용을 적용하면 범주를 지원하는 모든 위젯이 새로 고쳐집니다. 각 위젯은 하단에 적용된 필터와 위젯의 필터 아이콘에 적용된 필터 수를 표시합니다. 위젯에서 보고서를 클릭하면 **KPI** 세부 정보 탭에 대한 추가 정보를 볼 수 있습니다. **KPI** 세부 정보 탭에서 다음을 수행할 수 있습니다.

- 기록을 표시합니다.
- 기록을 비교합니다.
- 차트 유형을 변경합니다.
- 날짜 범위를 선택합니다.
- 기간을 기준으로 한 추세를 봅니다.
- 개요 탭에서 사용할 수 없는 필터를 포함하여 추가 필터를 적용합니다. Host 태그를 예로 들 수 있습니다.

다음 예에서는 개요 탭에서 필터를 적용하고 **KPI** 세부 정보 탭에서 작업을 수행하는 방법을 보여줍니다.

구성 준수 대시보드의 개요 탭

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

준수 탭

규정 준수 탭에는 HIPAA(Health Insurance Portability and Accountability Act) 및 DISA(Data Interchange Standards Association)와 같은 다양한 권한 있는 소스에 대한 규정 준수 비율이 표시됩니다. 열 헤더 필터를 사용하고 범주를 선택하여 이 목록을 구체화할 수 있습니다.

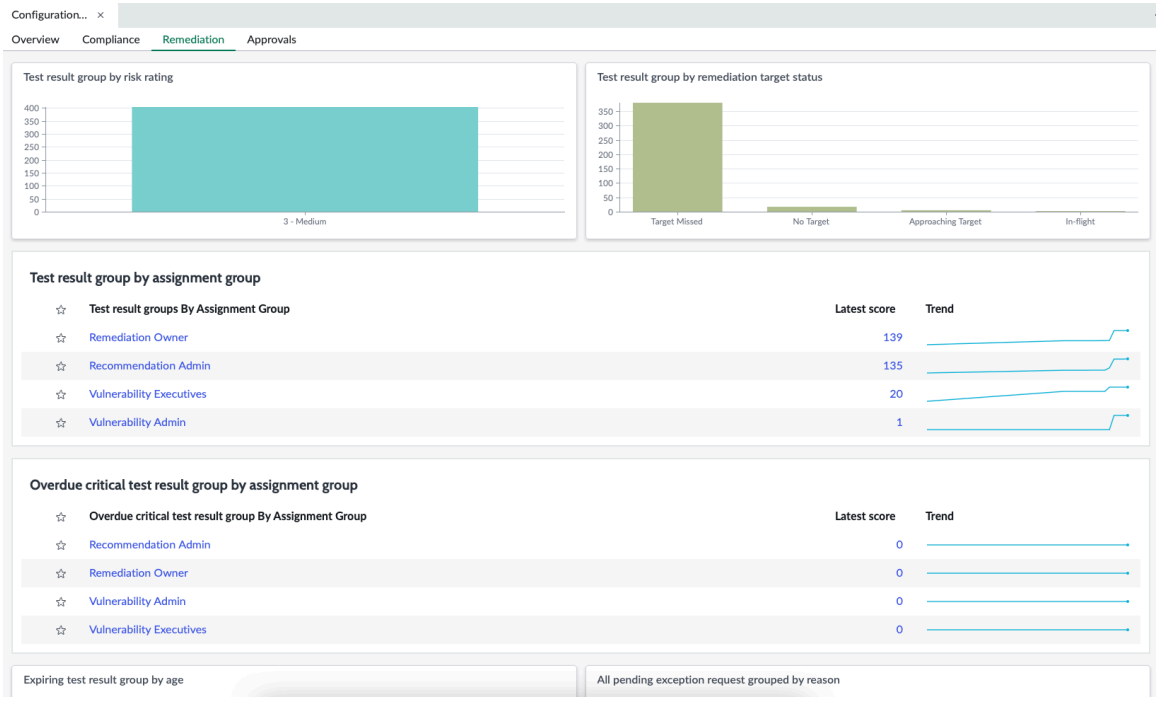
다음 예제에서는 규정 준수 탭에서 데이터를 필터링할 수 있는 방법을 보여 줍니다.

구성 준수 대시보드의 준수 탭

정정 탭

정정 탭에는 정정 진행 상황에 대한 정보가 표시됩니다. 이 탭을 사용하여 잘못된 구성 정정 위생을 확인할 수 있습니다.

다음 예는 정정 탭을 보여줍니다.

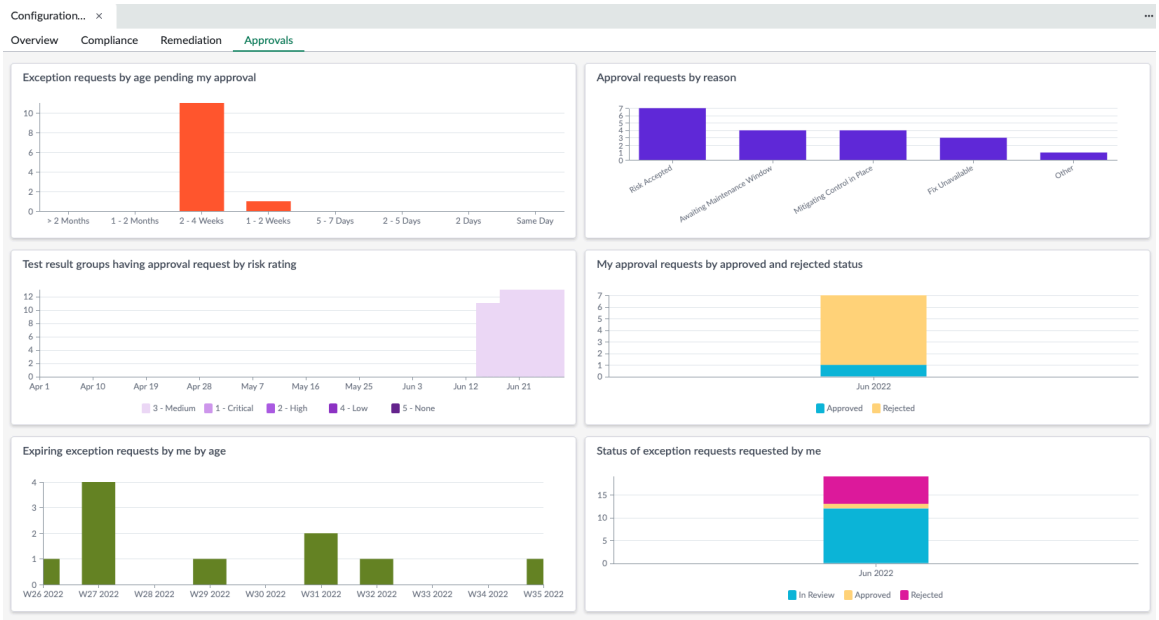


© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

승인 탭

승인 탭의 보고서에는 예외 요청 및 승인 상태에 대한 정보가 표시됩니다.

다음 예는 승인 탭을 보여줍니다.



세부 항목

표시기에서 사용하는 세부 항목은 다음과 같습니다.

- 지연 이유
- 기간
- 할당 그룹
- 정정 상태
- 결과
- 위험 등급
- 자산 범주
- 호스트 태그
- 구성 테스트
- 클라우드 서비스 제공자
- 클라우드 영역
- 클라우드 계정
- 클라우드 자원 유형

주:
테스트 결과에 대한 기간 및 종결된 기간 계산을 사용자 지정하면 이러한 메트릭을 포함하는 퍼포먼스 분석(PA) 보고서가 급격히 증가하거나 감소할 수 있습니다. 테스트 결과에 대한 연령 및 종결 연령의 계산을 사용자 지정하는 방법에 대한 자세한 내용은 KB1703270 KB 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필터

개요 탭에서 다음 필터를 위젯에 적용하여 필터링된 데이터를 시각화할 수 있습니다.

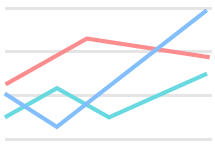
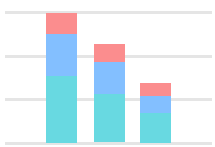
이름	유형	설명
자산 범주	선택	자산의 유형입니다. 네 가지 옵션은 다음과 같습니다. • 클라우드 • 컨테이너 • 인프라 • OT
클라우드 자원 유형	선택	자원의 유형입니다. 가상 머신을 예로 들 수 있습니다. 통합을 실행할 때 필터의 데이터가 채워집니다.
클라우드 서비스 제공자	선택	클라우드의 서비스 제공자입니다. 세 가지 옵션은 다음과 같습니다. • Amazon Web Services (AWS • Microsoft Azure • GCP(Google Cloud Platform)
클라우드 계정	선택	클라우드 서비스에서 계정을 만들 때 만들어지는 계정 ID입니다. 예: AWS. 계정 ID 데이터는 통합을 실행할 때 필터에 채워집니다.
클라우드 영역	선택	자원이 호스팅되는 위치입니다.

주:
필터에서 여러 옵션을 선택하고 적용을 선택할 수 있습니다. 각 위젯에는 적용된 필터와 적용되지 않은 필터가 표시됩니다. 사용 가능한 데이터에 따라 보고서가 생성됩니다. 위젯에는 지원되는 필터 수도 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

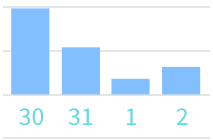
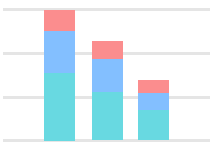
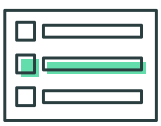
데이터 시각화

개요 탭 시각화

보고서 이름	유형	소스 테이블	설명
준수 추세	꺾은선형 차트 	테스트 결과	준수 추세에 대한 정보: • 자원: 시스템에서 사용할 수 있는 총 자원 수입니다. • 실패: 실패한 테스트 결과가 하나 이상 있는 자원 수입니다. • 통과: 모든 테스트 결과가 통과 상태인 자원 수입니다.
정정 작업	단일 점수	테스트 결과	시스템에 있으며 활성 상태인 정정 작업의 수입니다.
기한이 근접한 중요 정정 작업	단일 점수	테스트 결과	위험 등급이 "위험"이고 정정 상태가 "대상에 접근 중"인 정정 작업의 수입니다.
위험 등급별 테스트 결과	막대 	테스트 결과	위험 등급에 따라 그룹화된 실패 상태의 테스트 결과입니다.
연령별 테스트 결과	막대	테스트 결과	테스트 결과가 생성된 시기에 따라 그룹화되는 실패 상태의 테스트 결과입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

개요 탭 시각화

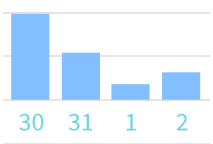
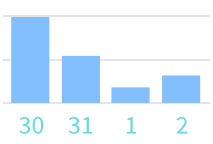
보고서 이름	유형	소스 테이블	설명
			주: 테스트 결과에 대한 기간 및 종결된 기간 계산을 사용자 지정하면 이러한 메트릭을 포함하는 퍼포먼스 분석(PA) 보고서가 급격히 증가하거나 감소할 수 있습니다. 테스트 결과에 대한 연령 및 종결 연령의 계산을 사용자 지정하는 방법에 대한 자세한 내용은 KB1703270 KB 문서를 참조하십시오.
정정 대상 준수로 종결된 테스트 결과	막대 	테스트 결과	테스트 결과가 통과됨 상태로 표시되며, 이는 이 테스트가 종결되었음을 나타냅니다.
담당 그룹별 중요 테스트 결과 지연	목록 및 점수 	테스트 결과	위험 등급이 "심각"이고 정정 상태가 "대상 누락"인 테스트 결과의 수. 이 보고서는 테스트 결과가 오픈 상태임을 나타냅니다. 테스트 결과가 정정 목표 날짜를 초과하면 기한이 지난 것으로 간주됩니다.
지연된 테스트 결과 - 서비스	목록, 점수 및 추세	서비스용 PA 대시보드 데이터베이스 뷰	정정 상태가 "대상 누락"인 서비스에 대한 테스트 결과 수입니다. 이 보고서는 테스트 결과가 가장 높은 서비스 또는 부서의 이름도 표시합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

개요 탭 시각화

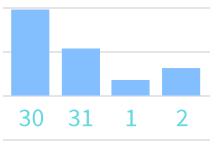
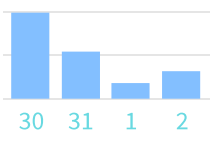
보고서 이름	유형	소스 테이블	설명
지연된 테스트 결과 - 서비스 소유자	목록, 점수 및 추세	서비스용 PA 대시보드 데이터베이스 뷰	정정 상태가 "대상 누락"인 서비스 소유자의 테스트 결과 수입니다. 이 보고서는 테스트 결과가 가장 높은 서비스 또는 부서의 이름도 표시합니다.

정정 탭 시각화

직위	유형	소스 테이블	설명
위험 등급별 정정 작업	막대 	정정 작업	활성 상태인 모든 테스트 결과 그룹의 위험 등급에 대한 세부 항목입니다.
정정 대상 상태별 정정 작업	막대 	정정 작업	대상을 놓쳤고 대상이 없으며 대상에 근접하고 있는 모든 테스트 결과 그룹의 정정 대상 세부 항목입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

정정 탭 시각화

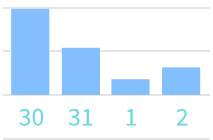
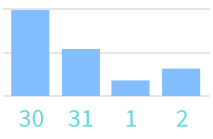
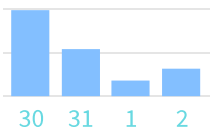
직위	유형	소스 테이블	설명
할당 그룹별 정정 작업	목록, 점수 및 추세	정정 작업	할당 그룹을 기반으로 하는 정정 작업의 세부 항목입니다.
할당 그룹별 지연된 중요 정정 작업	목록, 점수 및 추세	정정 작업	할당 그룹을 기반으로 하는 정정 작업의 세부 항목입니다. 이러한 정정 작업의 위험 등급이 "심각"이며 정정 목표가 충족되지 않았습니다.
기간별 만료되는 정정 작업	막대 	정정 작업	특정 기간 내에 만료되는 정정 작업입니다. 최대 10개의 기간 버킷을 생성할 수 있습니다.
보류 중인 모든 예외 요청이 사유별로 그룹화됨	막대 	상태 변경 승인	예외의 이유별로 그룹화된 상태 변경 승인 요청입니다.
담당 그룹별 테스트 결과에 대한 중요한 예외	목록, 점수 및 추세	테스트 결과	지연됨 및 중요 상태이며 할당 그룹을

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

정정 탭 시각화

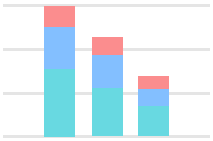
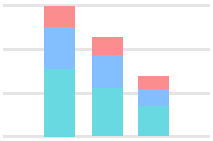
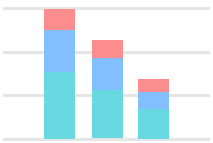
직위	유형	소스 테이블	설명
			기반으로 그룹화된 테스트 결과입니다.

승인 탭 시각화

보고서	유형	소스 테이블	설명
내 승인 보류 기간별 예외 요청	막대 	승인	사용자가 생성하고 승인 보류 중인 예외 요청입니다. 요청은 요청 기간에 따라 그룹화됩니다.
이유별 승인 요청	막대 	상태 변경 승인	예외 생성에 대한 상태 변경 승인 요청이며 예외의 이유를 포함합니다.
위험 등급별 승인 요청이 있는 정정 작업	막대 	정정 작업	중요도에 기반한 승인 요청이 있는 정정 작업입니다.
승인됨 및 거부됨 상태별 내 승인 요청	막대	상태 변경 승인	승인됨 및 거부됨 상태별로 그룹화된 예외 요청입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

승인 탭 시각화

보고서	유형	소스 테이블	설명
			
기간별 만료되는 예외 요청	막대 	상태 변경 승인	앞으로 몇 주 안에 만료될 예외 요청입니다. 예외 요청은 주를 기준으로 그룹화됩니다. 예외 요청이 생성될 때마다 예외 요청의 유효성을 위한 날짜가 선택됩니다. 요청 기간에 대한 계산은 이 날짜를 기준으로 합니다.
내가 요청한 예외 요청의 상태	막대 	상태 변경 승인	사용자가 생성하고 다음 상태에 따라 그룹화된 예외 요청: • 검토중 • 승인됨 • 거부됨

에 대한 집계 보고서 프레임워크 구성 준수

집계된 보고서 프레임워크를 사용하면 성능 향상을 위해 복잡하고 실행 시간이 긴 즉석 쿼리가 포함된 데이터에 대한 보고서를 만들 수 있습니다.

집계된 보고서 프레임워크는 다음을 통해 성과를 개선합니다.

- 더 적은 리소스를 사용하고 보고서를 더 빠르게 렌더링합니다.
- 데이터 집계와 집계 및 세부 항목 재사용(그룹화 기준)
- 데이터베이스에 대한 쿼리 줄이기

구성 테스트 결과가 100만 개 이상인 경우 표준 보고서와 함께 집계된 보고서 프레임워크를 사용합니다.

필요한 역할

이 솔루션과 관련된 역할과 작업은 다음과 같습니다.

- ServiceNow AI Platform관리자(admin): 이 플랫폼 분석 솔루션을 설치 및 활성화하고 시스템 속성을 필요에 따라 변경합니다.
- 퍼포먼스 분석 관리자(pa_admin): 집계, 위젯 및 대시보드를 검토합니다. 데이터 수집을 설정 및 시작합니다. 적절한 이해 관계자와 대시보드를 공유합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 관리자(sn_vul_cmn.admin): 집계를 생성합니다.
- VR write(sn_vul_cmn.write): 집계 및 집계된 결과에서 데이터를 편집합니다.
- VR 읽기(sn_vul_cmn.read): 집계 및 집계된 결과의 데이터를 검토합니다.
- 취약성 분석가(sn_vul.vulnerability_analyst): 집계된 결과를 검토합니다.

관련 정보

소스 데이터에 대한 집계 구성

여러 집계를 동시에 실행

동시에 실행할 수 있는 집계 수 구성

집계를 사용하여 보고서 생성

구성 준수 참조 정보

애플리케이션을 활성화하면 구성 준수 테이블, 예약된 작업, 사용자 역할 등 여러 유형의 구성요소가 설치됩니다.

다음 항목에서는 에 있는 구성 준수양식 및 기록의 필드 데이터 외에도 참조 정보, 문제 해결 정보를 제공합니다.

- 구성 준수와 함께 설치되는 구성요소
- 테스트 결과 양식 필드
- 임포트 문제 해결 구성 준수
- Qualys PC 결과 시작 날짜 수정

구성 준수와 함께 설치되는 구성요소

구성 준수 플러그인을 활성화하면 테이블 및 사용자 역할을 포함한 여러 유형의 구성요소가 설치됩니다.

의 구성 준수v15.1.5부터 가장 자주 사용되는 시스템 속성에 애플리케이션 내에서 액세스할 수 있습니다 구성 준수 . 이러한 시스템 속성을 보려면 다음으로 이동합니다. 모두구성 준수속성.

주:
애플리케이션 파일 테이블에는 이 애플리케이션과 함께 설치되는 구성요소가 나열됩니다. 이 테이블에 액세스하는 방법에 대한 지침은 애플리케이션과 함께 설치되는 구성요소 찾기 를 참조하십시오.

이 기능에 대한 데모 데이터를 사용할 수 있습니다.

주:
의 구성 준수v14.9부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v14.9 이전 용어	용어 **v14.9** 이상
테스트 결과 그룹	정정 작업
그룹 규칙	정정 작업 규칙
정책	테스트 그룹

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

애플리케이션과 함께 설치된 구성요소에 대해 필터링된 목록 보기

애플리케이션과 함께 설치되는 역할, 예약된 작업 및 테이블만 표시되도록 애플리케이션 파일 테이블을 필터링합니다. 해당 파일이 인스턴스와 메타데이터 테이블에 로드되도록 이러한 구성요소를 보려는 애플리케이션을 설치해야 합니다. 다음 단계에 따라 애플리케이션 파일 테이블에서 필터링된 목록을 봅니다.

1. 필터 탐색기에서 **sys_metadata.list** 를 입력하여 메타데이터 테이블로 이동합니다.
2. 조건 작성기(필터 아이콘)를 선택하고 애플리케이션 〉 다음과 같음 다음에 애플리케이션 이름이 표시됩니다. 예: 애플리케이션 〉 다음과 같음 〉 취약성 대응.
3. 조건 작성기에서 두 번째 필터를 추가하려면 **AND**를 선택한 뒤 클래스 〉 다음 중 하나 을 클릭하고 목록에서 역할, 예약된 작업 또는 테이블 클래스 중 하나를 선택합니다.
4. 실행을 선택합니다.

선택한 클래스의 결과가 필터링된 목록에 표시됩니다.

설치되는 역할

역할 이름 **[name]**	설명	포함하는 역할
구성 준수 관리자 [sn_vulc.admin]	애플리케이션 속성, 구성, 업데이트 규칙, 애플리케이션 통합을 구성 준수 수정할 수 있습니다. v15.0부터 admin 사용자는 Expliots, CVE 등과 같은 소스 기록을 삭제할 수 없습니다.	sn_vulc.쓰기 **주:** Configuration Compliance 애플리케이션의 기록 관리에 필요한 역할을 상속합니다.
읽음 〔sn_vulc.읽기〕	Configuration Compliance에서 목록 및 기록을 읽습니다. **중요사항:** 의 취약성 대응v24.0부터 sn_vulc.read 역할은 취약성 관리자 작업 공간.	• sn_sec_cmn.calc_read • sn_vul.view_manager_workspace
쓰기 〔sn_vulc.쓰기〕	Configuration Compliance에서 목록 및 기록을 작성합니다.	• sn_vulc.읽기 • sn_vulc.remediation_owner
쓰기 할당 [sn_vulc.write_assignment	테스트 결과 할당 필드에 쓰기	sn_vulc.remediation_owner 역할에 포함되어 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

역할 이름 **[name]**	설명	포함하는 역할
정정 소유자 sn_vulc.remediation_owner	사용자 또는 그룹에 할당된 테스트 결과에 대한 권한을 확인하고 업데이트합니다.	itil 역할에 포함되어 있습니다. 포함: • sn_sec_cmn.읽기 • sn_vulc.write_assignment • sn_vul.view_rem_workspace
CC.시스템 sn_vulc.import_admin	구성 준수 애플리케이션에서 모든 예약된 작업을 실행합니다. 주: 이 사용자는 구성 준수에서 모든 예약된 작업에 대한 기본 실행 사용자입니다.	• sn_vulc.쓰기 • import_admin • sn_vul_tenable.read_integration
VRCommon.시스템 sn_vul_cmn.admin	취약성 대응 공통 애플리케이션의 모든 예약된 작업에 대한 기본 실행 사용자입니다.	• sn_vul_cmn.쓰기 • sn_sec_cmn.admin • report_admin
SecCommon.System sn_sec_cmn.admin	보안 지원 공통 애플리케이션의 백그라운드 작업 역량에 사용되는 모든 예약된 작업에 대한 기본 실행 사용자	• sn_sec_cmn.int_write • sn_sec_cmn.쓰기 • workflow_admin • sn_sec_cmn.calc_write • sn_sec_core.read_dictionary • sn_sec_cmn.승인_규칙 관리 • sn_sec_int.admin • sn_sec_cmn.cap_email_write • sn_sec_cmn.관리_분류_규칙 • sn_sec_cmn.배경_관리_작업
V14.7: sn_vulc.edit_watch_topic	구성 준수에 대한 주시 주제를 편집합니다.	sn_vulc.read_watch_topic
V14.7: sn_vulc.read_watch_topic	구성 준수에 대한 주시 주제를 읽어보십시오.	cmdb_read

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

역할 이름 **[name]**	설명	포함하는 역할
V14.7: sn_vulc.create_watch_topic	구성 준수에 대한 주시 주제를 생성합니다.	sn_vulc.read_watch_topic
sn_vulc.auditor	모든 구성 준수 모듈에 대해 읽기 허용	sn_vulc.읽기 sn_vulc.고급_읽기
sn_vulc.고급_읽기	모든 구성 준수 관리 모듈에 대해 읽기 허용	sn_vulc.read_auto_close_rules sn_vulc.read_exception_configuration sn_vulc.read_assignment_rules sn_vulc.read_task_rules sn_vulc.read_auto_exception_rule sn_vulc.read_notifications sn_vulc.read_risk_score_configuration sn_vulc.read_test_criticality_mapping sn_sec_cmn.read_approval_rules sn_vulc.read_auto_delete sn_vulc.read_remediation_target_rules
sn_vulc.read_test_criticality_mapping	테스트 중요도 매핑에 대한 읽기 허용	
sn_vulc.read_task_rules	정정 작업 규칙에 대한 읽기 허용	
sn_vulc.read_assignment_rules	담당 규칙에 대한 읽기 허용	
sn_vulc.read_risk_score_configuration	위험 점수 구성에 대한 읽기 허용	
sn_vulc.read_auto_close_rules	자동 종결 구성에 대한 읽기 허용	
sn_vulc.false_positive_approver	정정 작업 긍정 오류로 종결 승인/거부 허용	sn_vul.view_manager_workspace
sn_vulc.exception_approver	예외 요청을 승인하거나 거부합니다.	sn_vul.view_manager_workspace
sn_vulc.삭제	소스 기록을 삭제합니다.	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설치되는 예약된 작업

예약된 작업	설명
V15.0: 구성 테스트에서 테스트 그룹 업데이트	Tenable 및 Microsoft Defender 소스에 대한 테스트에서 테스트 그룹을 업데이트합니다. 이것은 일회성 작업입니다.
V15.0: 기존 테스트 결과 필드 채우기	테스트 결과 테이블, 저장된 필터 및 모듈에 새로 추가된 열(예: 연령, 연령 종결, 활성 등)에 값을 업데이트합니다. 이것은 일회성 작업입니다.
V15.0: 취약한 CI 테이블 채우기 - 테스트 결과 삭제 및 다시 채우기	취약한 CI 테이블의 총 기록을 채웁니다. 이것은 일회성 작업입니다.
버전 12.0 모든 테스트 결과 그룹에 대한 정정 메트릭 계산	정정 작업 기록의 상태 메트릭 값을 계산하고 업데이트합니다.
버전 12.0: 모든 테스트 결과에 대한 정정 메트릭 계산	테스트 결과 기록의 상태 메트릭 값을 계산하고 업데이트합니다.
버전 12.0: 변경 요청 상태 동기화	기존의 모든 정정 작업(RT)의 상태를 변경 요청(CHG)과 동기화하는 주문형 작업입니다. 변경 요청은 수명주기를 거치면서 관련 정정 작업의 상태도 자동으로 이동합니다. 앞으로 상태 동기화를 활성화합니다.
버전 11.1: 테스트 결과 그룹 연기 확인 만료	정정 작업이 만료된 경우(그리고 1주일 후에 만료되는 경우) 알림을 보냅니다.
구성 준수 CI 수	구성 항목 수〔sn_vulc_cc_configuration_item_count〕 테이블에 고유한 CI(구성 항목) 카운트와 90일 이동 평균을 입력합니다.
버전 11.1: 정정 대상 평가 및 알림	모든 테스트 결과에 대한 정정 목표 날짜를 설정하거나 업데이트합니다. 규칙에 대한 정정 목표 날짜의 상태를 결정합니다. 알림 전송
V14.7: 통합 정정 작업에 테스트 결과 그룹 삽입	클래식 UI에서 만든 모든 정정 작업을 sn_vul_remediation_task(통합 정정 작업)에 삽입하는 일회성 예약 작업입니다.
버전 12.0: CR 및 CR-Parent에 대한 CR-TRG m2m 채우기	정정 작업에 대한 변경 요청을 채웁니다.
v11.1에서 제거됨: 지연된 테스트 결과 그룹 다시 열기 **주:** 11.1 이전 버전에서는 사용되지 않습니다. 사용하지 마십시오.	기한이 지나면 지연된 그룹을 다시 엽니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예약된 작업	설명
모든 담당 규칙 다시 적용	모든 담당 규칙을 다시 적용합니다.
버전 14.3: 담당 규칙의 재할당 횟수	매일 실행되며 특정 할당 규칙에 대해 이 기능에 의해 할당되지 않은 테스트 결과 및 정정 작업의 총 수를 게시합니다.
테스트 결과 그룹의 상태 재평가	**assess_state**가 false인 항목에 대한 정정 작업의 상태를 재평가합니다. 15분마다 실행됩니다.
테스트 결과 그룹 및 구성 테스트에 테스트 결과 위험 점수를 롤업	매시간 실행되고 변경된 구성 테스트 및 정정 작업에 대한 롤업 점수를 계산합니다. • sn_vulc_test_manifest의 모든 테스트에 대한 롤업 위험 점수를 계산하고 완료 시 매니페스트 기록을 삭제합니다. • sn_vulc_result_group_manifest의 모든 테스트에 대한 롤업 위험 점수를 계산하고 완료 시 매니페스트를 삭제합니다.
버전 12.0: 정책 정정 메트릭 업데이트	의 구성 준수v15.0부터 이 예약된 작업의 이름이 정정 메트릭 업데이트로 변경되었습니다. • 정책 기록의 상태 메트릭 값을 계산하고 업데이트합니다. • 검색된 항목에 대한 CI의 테스트 결과 준수 %를 계산합니다.
버전 14.3: 지연 수 설정	테스트 결과 또는 정정 작업이 지연된 횟수를 수집합니다.
테스트 결과에 대한 위험 등급 업데이트	테스트 결과의 위험 등급을 업데이트합니다.
종결되지 않은 모든 결과 그룹 및 구성 테스트에 대한 롤업 위험 점수를 업데이트합니다.	종결되지 않은 모든 결과 그룹 및 구성 준수 테스트에 대한 롤업 위험 점수를 업데이트합니다.

설치되는 테이블

테이블	설명
할당 규칙 [sn_vulc_assignment_rule]	테스트 결과에 할당 그룹을 설정하기 위해 평가된 규칙 집합을 포함합니다.
권한이 부여된 소스 [sn_vulc_auth_src]	임포트한 권한이 부여된 소스를 저장합니다.
계산기 [sn_vulc_calculator_risk_score]	특정 조건이 충족될 때 특정 테스트 결과 필드를 설정하는 계산기가 포함되어 있습니다.
참조 구성 항목 수	구성 항목의 총 수를 포함합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테이블	설명
[sn_vulc_cc_configuration_item_count]	
버전 12.0: 변경 요청 연결 [sn_vulc_action_associate_cr]	변경 요청을 정정 작업에 연결하는 데 사용되는 스테이징 테이블입니다.
버전 12.0: 변경 요청 생성 [sn_vulc_action_create_cr]	변경 요청 양식을 생성하는 데 사용되는 스테이징 테이블입니다.
버전 12.0: 변경 요청 양식 [sn_vulc_cr_form]	변경 요청 관리의 기본 테이블입니다.
인용 [sn_vulc_citation]	임포트된 인용 포함
구성 테스트 [sn_vulc_test]	임포트한 구성 테스트 데이터를 포함합니다.
구성 테스트 매니페스트 [sn_vulc_test_manifest]	롤업 위험 점수를 계산해야 하는 구성 테스트를 포함합니다.
버전 12.2 자산 테이블 〔sn_vul_missing_asset〕 누락	일치하지 않는 자산이 있는 임포트된 구성 준수 평가 데이터에 대한 임시 자산 기록을 포함합니다.
구성 테스트 기술 [sn_vulc_test_technology]	임포트한 구성 테스트 기술을 포함합니다.
정정 작업 규칙 [sn_vulc_grouping_rule]	테스트 결과 세트에 대해 그룹을 자동으로 만드는 기준을 정의하는 규칙을 포함합니다.
테스트 그룹 [sn_vulc_policy]	임포트한 정책을 포함합니다.
정책 구성 테스트 [sn_vulc_policy_test]	임포트한 정책 구성 테스트 데이터를 포함합니다.
정정 대상 규칙 [sn_vulc_ttr_rule]	테스트 결과를 정정하기 위한 예상 시간 범위를 정의합니다.
위험 계산기	계산기 그룹화 구성 준수 를 포함합니다. 계산기 그룹의 순서에 따라 가장 먼저 평가되는 그룹이 결정되며, 각 그룹에서 최대 하나의 계산기가 사용됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테이블	설명
[sn_vulc_calculator_group]	
위험 점수 롤업 계산기 [sn_vulc_risk_score_rollup]	롤업 계산기 구성을 포함합니다.
분리 정정 작업 [sn_vulc_action_split_trg]	정정 작업을 분할하는 데 사용되는 스테이징 테이블입니다.
상태 변경 승인 [sn_vulc_state_change_approval]	승인 상태 프로세스 데이터를 포함합니다.
기술 [sn_vulc_technology]	수입된 기술을 포함합니다.
테스트 중요도 맵 [sn_vulc_test_criticality_map]	중요도 맵 데이터를 포함합니다.
테스트 결과 [sn_vulc_result]	임포트한 테스트 결과를 포함합니다.
정정 작업 [sn_vulc_result_group]	임포트한 정정 작업을 포함합니다.
버전 12.0: 정정 작업 변경 요청	정정 작업에 대한 변경 요청을 포함합니다.
정정 작업 매니페스트 [sn_vulc_result_group_manifest]	롤업 위험 점수를 계산해야 하는 정정 작업을 포함합니다.
정정 작업 [sn_vulc_m2m_result_result_group]	정정 작업 데이터를 포함합니다.
테스트 결과 이력 [sn_vulc_result_history]	임포트한 테스트 결과 이력을 포함합니다.
테스트 결과 정정 상태	가장 근접하게 적용된 정정 대상 규칙에 대한 테스트 결과의 상태입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테이블	설명
V14.7: 주시 주제 테스트 수 [sn_vulc_wt_test_counts]	취약성 관리자 작업 공간의 구별되는 구성 테스트 탭에 대한 캐시 테이블입니다.

테스트 그룹 보기 구성 준수

외부 공급업체 스캔 결과를 인스턴스로 임포트한 후에는 테스트 그룹 수준에서 테스트 준수를 확인할 수 있습니다. 해당 테스트 그룹과 관련된 모든 테스트 기록을 감사하기 전에 이 뷰를 사용하십시오.

시작하기 전에
필요한 역할: 보려면 sn_vulc.read 및 sn_vulc.remediation_owner

이 태스크 정보
테스트 그룹은 임포트한 기록이므로 애플리케이션에서 편집할 구성 준수 수 없습니다.

프로시저

1. 다음으로 이동 모두 〉 구성 준수 〉 테스트 그룹.
   테스트 결과 목록이 표시됩니다. 의 구성 준수v15.0부터 테스트 결과 준수 비율**(%)** 열에는 테스트 그룹의 테스트를 준수하는 테스트 결과의 백분율이 표시됩니다.

   테스트 결과 준수 비율(%) = (테스트 그룹에서 종결된 테스트 결과 수/테스트 그룹과 관련된 총 테스트 결과 수) * 100

2. 보려는 테스트 그룹의 짧은 설명을 클릭합니다.

구성 준수 테스트 그룹 양식 필드

필드	설명
소스	외부 공급업체 스캐너의 시스템 이름 또는 와 통신구성 준수하는 데 사용되는 API의 플러그인에 ServiceNow 입력된 이름입니다.
기술	외부 공급업체 스캐너 애플리케이션의 테스트 그룹과 연결된 기술 목록입니다.
소스 ID	외부 공급업체 스캐너에서 이 테스트 그룹에 할당한 식별자입니다.
소스 작성됨	외부 공급업체 스캐너 애플리케이션에서 테스트 그룹이 정의된 날짜 및 시간입니다.
소스 업데이트됨	타사 정책 스캐너 애플리케이션에서 테스트 그룹을 마지막으로 수정한 날짜 및 시간입니다.
간단한 설명	외부 공급업체 스캐너 애플리케이션에서 테스트 그룹에 할당된 요약 설명 또는 제목입니다.
설명	외부 공급업체 스캐너 애플리케이션에 정의된 테스트 그룹에 대한 자세한 설명입니다.
테스트	이 테스트 그룹을 참조하는 테스트 목록입니다. 외부 공급업체 스캐너에서 임포트했습니다. 필요한 경우 목록을 탐색하여 특정 테스트에 대한 자세한 정보를 확인할 수 있습니다.
정정 상태(버전 **12.0)**	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
지연 제외	이러한 값은 지연된 테스트 결과의 CI를 포함하지 않습니다. ○ 남아 있는 **CI**: 이 정책에 대한 활성 테스트 결과(종결 이외의 상태)가 있는 구성 항목(CI)의 수(수)입니다. ○ 정정된 **CI** 비율**(%)**: 이 테스트 그룹의 준수 CI 비율(%)입니다. 이 숫자는 테스트 결과가 지연된 CI를 제외합니다. ○ 총 **CI:** 이 테스트 그룹의 영향을 받은 총 CI 수입니다. 이 카운트에서 지연된 테스트 결과는 제외됩니다.
지연 포함	값은 모든 활성 테스트 결과(종결 상태 이외의 모든 상태)의 CI를 나타냅니다. ○ 나머지 **CI:** 이 테스트 그룹이 적용되었으며 종결되지 않은 하나 이상의 테스트 결과와 연결된 고유 CI 수입니다. ○ 정정된 **CI** 비율**(%)**: 이 테스트 그룹의 준수 CI 비율(%)입니다. ○ 총 **CI:** 이 테스트 그룹의 영향을 받은 총 CI 수입니다.

버전 12.0부터 요청 시 이러한 값을 업데이트하려면 정정 상태 탭 아래에서 상태 업데이트 관련 링크를 클릭합니다. 데이터가 새로 고침되고 있음을 나타내는 메시지가 표시됩니다. 상태 보기 링크를 클릭하여 업데이트 진행률을 확인합니다. 잠시 후 마지막으로 예약된 작업 이후 변경되거나 업데이트된 모든 데이터가 기록에서 새로 고쳐집니다. 업데이트된 필드 값이 새로 고쳐집니다.

3. 옵션: 임포트 사용 안 함 단추를 선택하여 테스트 그룹에 대한 테스트 결과 임포트를 비활성화합니다.

   (Optional) 임포트가 비활성화됨 열의 값이 *true*로 변경됩니다. 테스트 그룹에 대한 테스트 결과는 예정된 수집에서 임포트되지 않습니다.

   주:
   가져오기 사용 안 함 버튼은 스캐너에서 얻은 테스트 결과에만 사용할 수 있습니다Qualys.

   v23.0 취약성 대응부터 :

   ○ 에서 취약성 관리자 작업 공간테스트 그룹에 대한 Qualys 테스트 결과 임포트를 활성화하거나 비활성화할 수 있습니다. 자세한 내용은 테스트 그룹에 대한 Qualys 테스트 결과 임포트 활성화 또는 비활성화 문서를 참조하십시오.

   ○ 사용하지 않음 표시 단추의 이름이 임포트 사용 안 함으로 변경되었습니다.

   ○ 사용하지 않음 열의 이름이 임포트가 비활성화됨으로 변경되었습니다.

권한이 부여된 소스 보기 구성 준수

이 모듈을 사용하여 권한이 부여된 각 소스에 대한 요약 정보를 보고 레코드를 생성하는 데 사용된 소스 게시글을 조사할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할:

- 업데이트할 sn_vulc.admin
- sn_vulc.remediation_owner

프로시저

1. 다음으로 이동 모두 〉 구성 준수 〉 지원 데이터 〉 권한이 부여된 소스.
2. 보려는 권한이 부여된 소스에 대한 짧은 설명을 클릭합니다.

구성 준수 권한이 부여된 소스 양식 필드

필드	설명
번호	임포트 프로세스 동안 인스턴스에서 권한이 부여된 소스에 할당한 ID 번호입니다.
소스	외부 공급업체 스캐너 애플리케이션의 시스템 이름 또는 와 통신 구성 준수하는 API의 스캐너 플러그인에 입력된 이름입니다.
소스 ID	외부 공급업체 스캐너가 권한이 부여된 소스에 할당한 식별자입니다.
간단한 설명	외부 공급업체 스캐너에서 이 권한이 부여된 소스에 지정된 이름입니다.
게시자	이 권한이 부여된 소스에 대한 정보의 원래 소스였던 조직 또는 출판물의 이름입니다.
인용	테스트 결과에 대해 인용된 정보 목록입니다. 외부 공급업체 스캐너에서 임포트했습니다. 필요한 경우 이 목록을 탐색하여 특정 테스트에 대한 자세한 정보를 확인할 수 있습니다.

3. 옵션: 게시자를 추가합니다.
4. 업데이트를 클릭합니다.
5. 삭제를 클릭하여 이 기록을 삭제할 수 있습니다.
   인스턴스에서 기록을 제거합니다. 외부 공급업체 통합에서 아직 사용 중이면 다음 임포트에서 반환됩니다.

기술 보기 구성 준수

이 모듈을 사용하여 권한이 부여된 각 출처 및 인용(Qualys에서는 프레임워크라고도 함)에 대한 요약 정보를 볼 수 있습니다. 기록을 생성하는 데 사용된 소스 게시글을 조사할 수 있습니다.

시작하기 전에
필요한 역할:

- 업데이트할 sn_vulc.admin
- sn_vulc.remediation_owner

프로시저

1. 다음으로 이동 모두 〉 구성 준수 〉 지원 데이터 〉 기술.
2. 보려는 권한이 부여된 소스에 대한 짧은 설명을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

구성 준수 권한이 부여된 소스 양식 필드

필드	설명
번호	임포트 프로세스 동안 인스턴스에서 권한이 부여된 소스에 할당한 ID 번호입니다.
소스	외부 공급업체 스캐너의 시스템 이름 또는 와 구성 준수통신하는 API에 대한 외부 공급업체 스캐너 플러그인에 입력된 이름입니다.
소스 ID	외부 공급업체 스캐너가 권한이 부여된 소스에 할당한 식별자입니다.

3. 삭제를 클릭하여 이 기록을 삭제할 수 있습니다.
   인스턴스에서 기록을 제거합니다. 외부 공급업체 통합에서 아직 사용 중이면 다음 임포트에서 반환됩니다.

테스트 보기 구성 준수

이 모듈을 사용하여 이러한 테스트에 대한 자세한 정보를 조사합니다. 여기에는 생성 시 사용된 전문가 소스 인용, 사용 중인 타사 구성 정책 및 검사에서 얻은 결과가 포함됩니다.

시작하기 전에
필요한 역할:

- 업데이트할 sn_vulc.admin
- sn_vulc.remediation_owner

주:
의 구성 준수v14.9부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v14.9 이전 용어	용어 **v14.9** 이상
테스트 결과 그룹	정정 작업
그룹 규칙	정정 작업 규칙
정책	테스트 그룹

프로시저

1. 다음으로 이동 모두 〉 구성 준수 〉 통제.
2. 다음으로 이동 모두 〉 구성 준수 〉 테스트
3. 목록에서 보려는 컨트롤(컴플라이언스 테스트)을 엽니다.

   버전 12.0부터 요청 시 이러한 값을 업데이트하려면 정정 상태 탭 아래에서 상태 업데이트 관련 링크를 클릭합니다. 데이터가 새로 고침되고 있음을 나타내는 메시지가 표시됩니다. 상태 보기 링크를 클릭하여 업데이트 진행률을 확인합니다. 잠시 후 마지막으로 예약된 작업 이후 변경되거나 업데이트된 모든 데이터가 기록에서 새로 고쳐집니다. 위험 점수, 위험 등급, 정정 목표 날짜, 상태 및 정정 상태 탭의 필드와 같은 필드 값이 새로 고쳐집니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

구성 준수 테스트 양식 필드

필드	설명
번호	임포트 프로세스 동안 통제에 할당된 번호입니다.
결과	검사 상태입니다. 통과 또는 실패. 이 테스트가 여러 정정 작업에 속하는 경우 해당 상태는 우선순위에 따라 결정됩니다.
소스	외부 공급업체 통합 애플리케이션의 시스템 이름 또는 와 통신 구성 준수하는 데 사용되는 API의 플러그인에 입력된 이름입니다.
중요도	구성 문제의 심각도 또는 외부 공급업체 통합에 정의된 통제와 관련된 문제입니다. 중요도 수준은 에서 취약성 대응사용할 수 있는 유사한 취약성 표시기의 세분성과 일치하도록 조정됩니다. 가능한 수준은 다음과 같습니다. 중요 컨트롤과 관련된 구성 문제로 인해 하나 이상의 비즈니스 크리티컬 CI가 중단됩니다. 높음 컨트롤과 관련된 구성 문제는 위협이지만 중요한 네트워크 리소스의 종료를 일으키지는 않습니다. 보통 통제와 관련된 구성 문제는 위험하지만 즉각적인 위협은 아닙니다. 낮음 제어와 연결된 구성 문제는 낮은 수준의 위협이며 더 큰 위험에 처한 CI를 위해 무시할 수 있습니다. 경미 컨트롤과 관련된 구성 문제는 사소한 위험이며 필요한 경우 무시할 수 있습니다.
소스 ID	외부 공급업체 통합에 의해 제어에 할당된 식별자입니다.
범주	외부 공급업체 벤더가 이 유형의 통제에 부여한 주 분류 범주입니다.
위험 점수	롤업 위험 점수입니다. 이 위험 점수는 가중치가 적용되며, "종결"이 아닌 모든 테스트 결과(오픈, 조사 중, 구현 대기 중, 연기됨, 해결됨)의 최대 위험 점수 점수의 85%와 "종결됨"이 아닌 테스트 결과 수의 점수의 15%입니다. 테스트 결과의 비즈니스 중요도

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	및 테스트 중요도 값을 기반으로 하는 위험 점수 계산기로 계산된 값입니다.
하위 범주	외부 공급업체 벤더가 이 테스트 클래스에 할당한 하위 범주입니다.
위험 등급	1-5 숫자 척도의 위험 점수 범위를 기준으로 1 - 중요에서 5 - 없음까지의 위험 점수 범위에 따라 전체 위험을 평가합니다. 이 필드는 이전 버전의 우선순위 필드를 대체합니다.
기술	이 테스트에서 다루는 기술 목록입니다.
소스 작성됨	외부 공급업체 통합에서 테스트가 처음 정의된 날짜입니다.
소스 업데이트됨	외부 공급업체 통합에서 테스트가 마지막으로 업데이트된 날짜입니다.
간단한 설명	외부 공급업체 통합에서 테스트에 입력되었거나 할당된 요약 설명 또는 제목입니다.
정정 상태**(v 12.0)**	
지연 제외	이러한 값에는 지연된 테스트 결과가 포함되지 않습니다. ○ 오픈 테스트 결과: 이 구성 테스트에 대한 활성(종결 상태 이외의 모든 상태) 테스트 결과의 수(수)입니다. ○ 정정된 테스트 결과의 비율**(%)**: 이 정정 작업에 대한 정정된 테스트 결과의 백분율입니다. ○ 총 테스트 결과: 이 정정 작업에 대한 총 테스트 결과 수입니다.
지연 포함	이러한 값에는 지연된 테스트 결과가 포함됩니다. ○ 오픈 테스트 결과: 이 정정 작업에 대한 모든 활성(종결 이외의 상태) 테스트 결과의 수(수)입니다. ○ 정정된 테스트 결과의 비율**(%)**: 이 정정 작업에 대한 정정된 테스트 결과의 백분율입니다. ○ 총 테스트 결과: 이 정정 작업에 대한 총 테스트 결과 수입니다.
설명	테스트에 대한 자세한 설명입니다. Qualys 취약성 통합의 경우 이 필드는 기본적으로 커버 페이지의 컨텐츠 Qualys Cloud Platform 로 설정됩니다.
정정	단계 미준수를 정정하는 방법을 설명하는 지침입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
관련 탭	
인용	테스트와 관련된 각 권한이 부여된 출처에 대해 입력한 인용 목록입니다.
테스트 그룹	구성 준수 이 테스트를 사용하는 테스트 그룹 목록입니다.
테스트 결과	구성 문제의 영향을 받는 CI 목록 또는 이 테스트와 관련된 문제입니다. 필요한 경우 개별 테스트, ServiceNow 구성 항목 또는 영향을 받는 기술 목록에 액세스할 수 있습니다.
GRC 정책 설명	플러그인이 GRC 정책 및 준수 관리 설치되어 있으면 이 탭에 관련 GRC 정책이 포함됩니다. 이 목록을 편집하여 정책 설명을 추가하거나 제거할 수 있습니다.

테스트 결과 보기 구성 준수

감사 및 정정에 대한 테스트 결과를 봅니다 구성 준수 . 테스트 결과는 타사 취약성 통합 임포트 중에 자동으로 생성됩니다.

중요사항:
취약성 관리자 작업 공간에서 타사 취약성 통합 임포트 중에 생성된 테스트 결과를 볼 수 있습니다. 자세한 내용은 의 목록 페이지 취약성 관리자 작업 공간 문서를 참조하십시오.

시작하기 전에
필요한 역할:

- sn_vulc.보려면 읽기
- sn_vulc.remediation_owner 보고 업데이트하기
- sn_vulc.삭제하여 삭제

이 태스크 정보
구성 준수 는 테스트 결과를 만들거나 업데이트하지 않지만 외부 공급업체 통합의 일부로 가져옵니다. 에서 볼 수 구성 준수있게 되면 테스트 결과 그룹을 사용하여 정정됩니다.

주:
의 구성 준수v14.9부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v14.9 이전 용어	용어 **v14.9** 이상
테스트 결과 그룹	정정 작업
그룹 규칙	정정 작업 규칙
정책	테스트 그룹

프로시저

1. 다음으로 이동 모두 〉 구성 준수 〉 테스트 결과.
   v15.0 부터 구성 준수테스트 결과 목록에 다음 열이 나타납니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테스트 결과 목록

열	설명
활성	테스트 결과가 활성 상태인지 나타냅니다. 테스트 결과는 다음과 같이 표시됩니다. ○ True: 상태가 종결되지 않은 경우입니다. ○ False: 상태가 종결된 경우.
기간	테스트 결과가 마지막으로 오픈된 이후 활성 상태로 유지되는 기간입니다. 종결된 테스트 결과의 경우 이 필드는 비어 있습니다. 형식: 일 HH:MM: SS 나이 계산을 사용자 지정하는 방법에 대한 자세한 내용은 KB1703270 문서를 참조하세요.
종결 기간	테스트 결과가 '종결됨'으로 전환되기 전에 활성 상태였던 기간입니다. 테스트 결과가 '종결됨'으로 전환되면 연령 열의 값이 오래된 종결 필드에 표시됩니다. 활성 테스트 결과에 대한 이 필드는 비어 있습니다. 형식: 일 HH:MM: SS 종결된 나이 계산을 사용자 지정하는 방법에 대한 자세한 내용은 KB1703270 문서를 참조하세요.
종결됨	테스트 결과가 종결되는 타임스탬프입니다. 형식: YYYY-MM-DD HH:MM: SS
마지막으로 시작한 시간	테스트 결과가 열리는 타임스탬프, 즉 활성 필드 값이 *true*로 변경되는 타임스탬프입니다.

2. 보려는 컨트롤을 엽니다.

구성 준수 테스트 결과 양식 필드

필드	설명
번호	임포트 프로세스 동안 테스트에 할당된 번호입니다.
소스	써드파티 SCA 애플리케이션의 시스템 이름 또는 와 통신 구성 준수하는 데 사용되는 API의 애플리케이션 플러그인에 입력된 이름입니다.
소스 ID	SCA 애플리케이션에서 제어에 할당한 식별자입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
결과	통과, 실패, 오류 또는 알 수 없음. Qualys에서 임포트했습니다.
위험 점수	이 테스트의 계산기 결과입니다. v15.0 이전에는 구성 준수통과한 테스트 결과의 위험 점수가 '0'으로 설정되었습니다. 의 구성 준수v15.0부터 완화된 위험을 추정할 수 있도록 통과된 테스트 결과의 위험 점수가 '0'으로 변경되지 않습니다. 통과된 테스트 결과의 위험 점수는 정정 작업의 위험 점수를 계산하는 데 포함되지 않습니다.
위험 등급	1-5 숫자 척도의 위험 점수 범위를 기준으로 1 - 중요에서 5 - 없음까지의 위험 점수 범위에 따라 전체 위험을 평가합니다. 이 필드는 이전 버전의 우선순위 필드를 대체합니다.
상태	테스트 결과가 속한 정정 작업에서 계산됩니다. 테스트 결과가 여러 그룹에 속한 경우 상태를 결정하기 위해 우선순위가 적용됩니다.
해결	테스트 결과가 속한 정정 작업에서 계산됩니다. 테스트 결과가 여러 그룹에 속한 경우 해결 방법을 결정하기 위해 우선순위가 적용됩니다.
처음 발견됨	로 처음 가져온 날짜입니다 구성 준수. v13.1.1부터 처음 발견됨 필드에 스캐너에서 제공한 날짜가 표시됩니다. 그렇지 않으면 로 처음 가져온 구성 준수날짜가 표시됩니다.
마지막으로 발견됨	로 마지막으로 가져온 날짜입니다 구성 준수. v13.1.1부터 마지막 발견됨 필드에 스캐너에서 제공한 날짜가 표시됩니다. 그렇지 않으면 마지막으로 로 임포트한 구성 준수날짜가 표시됩니다.
마지막 통과	테스트 결과가 통과된 가장 최근 날짜입니다.
테스트	테스트의 이름입니다.
구성 항목	테스트에 첨부된 CI의 이름입니다.
기술	CI에서 실행되는 소프트웨어 버전입니다.
설명	테스트에 대한 설명
예상값	Qualys에서 구성되고 에서 임포트한 구성 준수예상 값입니다. 이 값은 true로 계산될 때 테스트 결과가 통과되는 부울 식입니다. 표현식은 논리, 집합 또는 정규 표현식 연산자의 조합일 수 있습니다.
실제 값	테스트에서 반환된 값입니다. 이러한 값은 예상 값 부울 식에 삽입되어 결과를 통과해야 하는지 또는 실패해야 하는지 여부를 결정합니다. Qualys에서 가져옵니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	버전 구성 준수14.9부터 확장된 증거 및 실패 원인 값이 실제 값 열에 추가됩니다.
정정	정정 지침입니다.
관련 탭	
정정 작업	이 테스트 결과와 연결된 정정 작업입니다.
테스트 결과 이력	동일한 CI/기술/테스트에 대한 합격/불합격 결과 이력을 보여주는 테스트 결과 관련 목록입니다.

정정 작업 보기

정정 작업을 보거나, 생성하고 정정을 수행할 수도 있습니다.

중요사항:
취약성 관리자 작업 공간에서 정정 작업을 볼 수 있습니다. 자세한 내용은 의 목록 페이지 취약성 관리자 작업 공간 문서를 참조하십시오.

시작하기 전에
필요한 역할:

- sn_vulc.admin 업데이트하거나 작성할
- sn_vulc.remediation_owner

주:
의 구성 준수v14.9부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v14.9 이전 용어	용어 **v14.9** 이상
테스트 결과 그룹	정정 작업
그룹 규칙	정정 작업 규칙
정책	테스트 그룹

프로시저

1. 다음으로 이동 모두 〉 구성 준수 〉 정정 작업.
2. 목록에서 보려는 기록을 클릭합니다.
3. 또는 새로 만들기를 클릭하여 새 정정 작업을 만들고 필드를 채웁니다.

구성 준수 정정 작업 양식 필드

필드	설명
번호	이 기록에 대해 자동으로 생성된 번호입니다.
상태	정정 작업의 진행 상태입니다. ○ 오픈 ○ 조사 중

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	○ 대기 중인 구현 ○ 연기됨 ○ 해결 일시 ○ 종결됨
위험 점수	이 점수는 정정 작업의 모든 활성 테스트 결과에 대한 위험 점수의 롤업된 값입니다. 정정 작업에서 테스트 결과가 정정되면 이 점수가 변경됩니다.
할당 그룹	이 정정 작업을 수행하도록 선택한 그룹입니다.
위험 등급	실패한 테스트 결과가 시스템에 미치는 위험의 양입니다. 이 점수는 위험을 위험(1)에서 없음(5)으로 평가하는 1-5 숫자 척도의 위험 점수 범위를 기반으로 합니다.
담당자	이 작업 세트에 대해 작업하는 선택한 할당 그룹의 개인입니다.
정정 대상	처음 파악된 이후 테스트 결과를 수정해야 하는 날짜입니다.
작성됨	이 정정 작업이 생성된 날짜 및 시간입니다.
정정 상태	그룹의 정정 상태입니다. 기한이 가장 가까운 테스트 결과에 따라 결정됩니다. 공개 그룹의 경우 상태에는 In-flight, Approaching Target 및 Target Missed가 포함됩니다. 종결된 그룹의 경우 상태에는 대상 없음, 대상 충족됨 및 대상 놓침이 포함됩니다. 계산된 정정 대상 날짜의 경우, 정정 작업이 종결되면 종결된 모든 테스트 결과의 전반적인 정정 상태가 정정 작업에 표시됩니다. 이 결정은 그룹이 날짜를 지켰는지 여부를 결정합니다. 종결된 정정 작업 정정 종결된 결과에 정정 대상 날짜가 있는 결과가 없는 경우 상태는 대상 없음 입니다. 종결된 결과 중 하나라도 목표 날짜를 놓친 경우 목표 누락 입니다. 하나 이상의 종결된 결과가 목표를 충족하고 다른 결과로 놓친 결과가 없는 경우 목표 충족 입니다.
업데이트됨	이 기록이 마지막으로 수정된 날짜 및 시간입니다.
간단한 설명	이 정정 작업에 대한 간략한 설명입니다.
설명	이 정정 작업과 연결된 소프트웨어 목록이 포함된 정정 작업에 대한 긴 설명입니다.
테스트	이 정정 작업과 연결된 구성 테스트입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
정정 상태(버전 **12.0**)	
지연 제외	이러한 값에는 지연된 테스트 결과가 포함되지 않습니다. ○ 오픈 테스트 결과: 이 정정 작업에 대한 활성(종결 이외의 상태) 테스트 결과의 수(수)입니다. ○ 정정된 테스트 결과의 비율**(%)**: 이 정정 작업에 대한 정정된(종결된) 테스트 결과의 백분율입니다. ○ 총 테스트 결과: 이 정정 작업에 대한 총 테스트 결과 수입니다.
지연 포함	값은 모든 활성 테스트 결과(종결 이외의 모든 상태)를 나타냅니다. ○ 오픈 테스트 결과: 이 정정 작업에 대한 활성(종결 이외의 상태) 테스트 결과의 수(수)입니다. ○ 정정된 테스트 결과의 비율**(%)**: 이 정정 작업에 대한 정정된(종결된) 테스트 결과의 백분율입니다. ○ 총 테스트 결과: 이 정정 작업에 대한 총 테스트 결과 수입니다.
그룹 구성	정정 작업에 대한 테스트 결과를 선택하는 데 사용되는 필터링 유형입니다.
그룹화 방법	사용된 메서드의 이름입니다.
그룹 규칙	사용된 그룹 규칙의 이름입니다.
메모	기록과 연결된 시스템 메모입니다.
관련 링크	버전 **12.0:** 업데이트 상태 링크. 요청 시 테스트 결과 기록의 값을 업데이트합니다. 마지막으로 예약된 작업 이후 변경되었거나 업데이트된 모든 데이터를 봅니다.
테스트 결과	이 정정 작업의 테스트 결과입니다.
변경 요청**(v 12.0)**	이 정정 작업과 연결된 변경 요청의 목록입니다.
상태 변경 승인**(v 12.0)**	이 정정 작업과 관련된 변경 요청 승인의 상태입니다.

애플리케이션의 테스트 결과 및 정정 작업 상태 전환 구성 준수

테스트 결과 기록이 연기, 해결, 재개되고 다른 정정 작업(RE)으로 이전되면 구성 테스트 기록의 상태 및 관련 정정 작업(RT)이 영향을 받습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테스트 결과와 정정 작업 간의 상태 전환 시나리오

주:
의 구성 준수v14.9부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v14.9 이전 용어	용어 **v14.9** 이상
테스트 결과 그룹	정정 작업
그룹 규칙	정정 작업 규칙
정책	테스트 그룹

다음 표에서는 구성 테스트 결과와 정정 작업 간에 상태 및 하위 상태가 전환되는 방법을 자세히 설명합니다.

정정 작업 상태가 다음에서 전환되는 경우...	... 종료 상태/하위 상태	관련 테스트 결과 상태 전환...	... 종료 상태/하위 상태	설명
오픈	조사 중	오픈	조사 중	상태는 양방향으로 전환됩니다.
오픈	검토 중	오픈	검토 중	상태는 양방향으로 전환됩니다.
오픈	지연됨/해결을 위해 선택된 이유가 있는 경우	오픈	연기됨	테스트 결과의 해결 사유는 정정 작업과 동일하게 유지됩니다.
지연됨/해결 이유 없음	오픈	테스트 결과가 지연됨 상태로 유지		테스트 결과는 정정 작업과 동일한 해상도를 유지합니다.
오픈	해결됨/수정됨	오픈	해결 일시	상태/하위 상태는 양방향으로 전환됩니다.
오픈	해결됨 및 해결됨에서 종결됨/수정됨으로	오픈	해결 일시	정정 작업이 종결/고정으로 전환되면 다시 열림으로 전환할 수 있습니다. 작업이 열림으로 전환되면 관련 테스트 결과가 해결됨에서 열림으로 다시 전환됩니다.
오픈	해결 일시	오픈	해결 일시	상태/하위 상태는 양방향으로 전환됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

정정 작업 상태가 다음에서 전환되는 경우...	... 종료 상태/하위 상태	관련 테스트 결과 상태 전환...	... 종료 상태/하위 상태	설명
오픈	해결됨/취소됨	오픈	해결 일시	상태/하위 상태는 양방향으로 전환됩니다.
오픈	해결됨 및 해결됨에서 종결됨으로	오픈	해결 일시	정정 작업이 자동으로 종결로 전환되면 관련 테스트 결과가 다시 열림으로 전환될 수 있습니다.
오픈	해결됨 및 해결됨에서 종결됨/잘못된 결과	오픈	해결됨 및 해결됨에서 종결됨/잘못된 결과	정정 작업이 해결됨으로 전환되면 다시 열림으로 전환할 수 있습니다. 정정 작업이 종결/잘못된 결과로 전환되면 해당 작업 및 관련 테스트 결과를 다시 열 수 없습니다.
오픈	종결/고정	테스트 결과 오픈 상태 유지		

주:

- v14.12 of 부터 구성 준수모달 닫기의 해결 필드에서 잘못된 결과 옵션이 제거됩니다.
- 의 구성 준수v14.12부터 정정 작업 상태 승인 워크플로우는 더 이상 사용되지 않으며 플로우 디자이너의 플로우 정정 작업 상태 승인으로 대체됩니다.

변경 요청과 정정 작업 간의 상태 동기화

애플리케이션에서 정정 작업의 상태 필드와 변경 요청(CHG)의 상태 필드 간에 동기화된 구성 준수 관계가 있습니다.

주:
의 구성 준수v14.9부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v14.9 이전 용어	용어 **v14.9** 이상
테스트 결과 그룹	정정 작업
그룹 규칙	정정 작업 규칙
정책	테스트 그룹

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

변경 요청은 수명주기를 거치면서 관련 정정 작업의 상태도 자동으로 이동합니다. 상태 동기화는 v12.0부터 애플리케이션을 ServiceNow Store 다운로드할 구성 준수 때 인스턴스에서 기본적으로 시스템 속성(sn_vulc.cr_state_sync)에 의해 활성화됩니다.

상태 동기화가 활성화되면 다음과 같은 경우 CHG 상태 필드가 정정 작업 상태 필드를 자동으로 변경합니다.

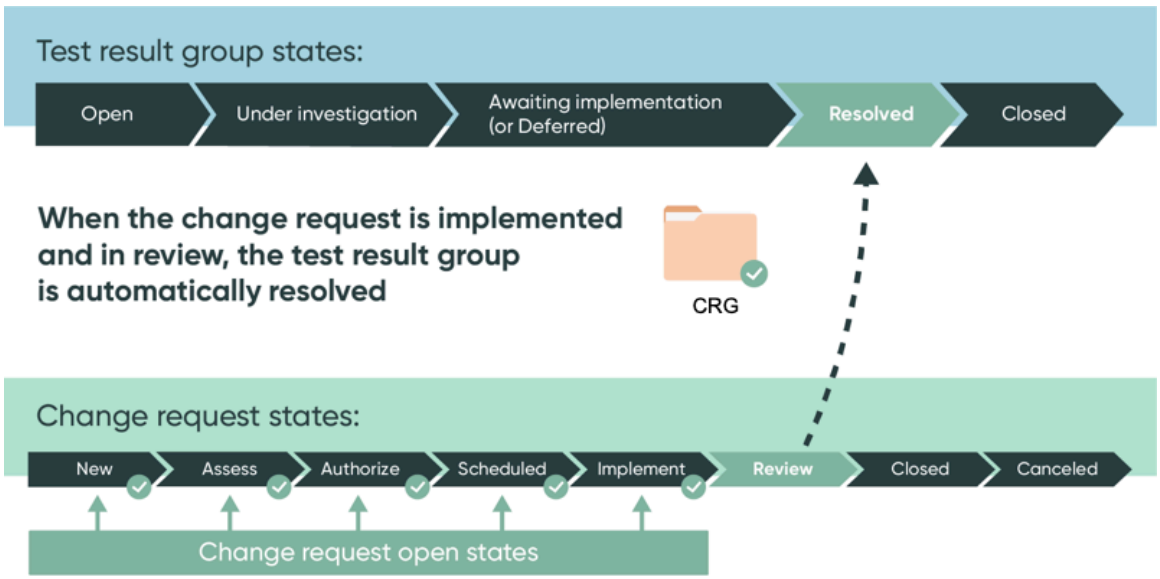
- 정정 작업에 대한 새 변경 요청이 생성될 때 변경 요청이 구현 대기 중이 아닌 경우 정정 작업 상태는 구현 대기 중으로 진행됩니다.
- 기존 변경 요청이 정정 작업에 연결될 때 구현 대기 중이 아닌 경우 정정 작업 상태는 구현 대기 중으로 진행됩니다.
- 변경 요청에 대한 작업이 완료(###)되고 CHG가 검토 상태로 이동하면 정정 작업이 해결됨으로 진행됩니다.

상태 동기화에 대한 자세한 내용과 예는 다음 섹션을 참조하십시오.

주:
상태 동기화가 활성화된 상태에서 각 기록의 수명주기 상태를 통해 변경 요청 및 정정 작업을 수동으로 이동할 수 있지만, 시스템에서 변경 요청의 상태가 변경되었음을 등록하거나 변경 요청을 추가하거나 정정 작업에서 제거하는 경우 상태 동기화가 수동 개입을 재정의할 수 있습니다. 그러나 변경 요청 상태는 정정 작업을 자동으로 종결에서 이동하지 않습니다.

정방향 상태 동기화

다음 이미지는 CHG 상태가 정정 작업 상태를 정정 수명주기(즉, 열림 에서 해결됨)로 자동으로 이동하는 방법을 보여줍니다.



해결됨 또는 종결됨 이외의 상태인 정정 작업에 대한 새 변경 요청을 생성할 수 있습니다. 상태 동기화는 TRG를 오픈, 조사 중, 구현 대기 중 및 해결됨 상태를 통해 자동으로 양방향으로 이동합니다. 이 이동은 변경 요청에 대한 상태 필드의 특정 값을 기반으로 합니다. 확인란(CR에 **CI** 추가)이 양식에 표시되고 확인란의 선택을 취소하지 않으면 변경 요청과 정정 작업 간의 상태 동기화가 자동으로 호출됩니다.

CHG가 열린 상태일 때는 정정 작업이 해결됨 으로 진행되지 않습니다. 앞의 그림과 같이 신규, 평가, 승인, 예약됨 또는 구현과 같이 수명주기에서 검토 이전 상태의 모든 CHG는 CHG에 대해 오픈 상태로 간주됩니다. CHG에 대한 조사 또는 작업이 완료되지 않았으므로 열린 상태는 정정 작업의 상태 필드를 이동하지 않습니다. 상태 동기화는 정정 작업에 대해 CHG가 생성되거나 정정 작업에

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

연결된 경우 또는 CHG에서 기존 관계의 상태가 변경될 때 호출됩니다. 완료된 CHG 상태는 검토 및 성공적으로 종결됨입니다. CHG가 성공적으로 종결되면 종결 코드는 성공 또는 문제와 함께 성공이며, 이 경우 정정 작업은 해결됨으로 진행됩니다.

역방향 상태 동기화

CHG는 수명 주기 동안 처리되므로 특정 시점에서 취소될 수 있습니다. 이 경우 CHG가 취소됨 또는 종결 되면(종결 코드가 실패함) 정정 작업이 자동으로 조사 중으로 다시 이동합니다. 취약성을 정정할 활성 계획이 없기 때문에 정정 작업이 조사 중으로 다시 이동합니다.

정정 작업이 해결됨 상태이고 새 CHG를 만들거나 초기 오픈 상태 중 하나에서 기존 CHG에 연결하면 정정 작업이 자동으로 구현 대기 중으로 다시 전환됩니다. 이제 CHG에 더 많은 작업이 할당되었기 때문에 정정 작업이 이 상태로 다시 전환됩니다.

둘 이상의 CHG가 포함된 정정 작업

구현 대기 중 상태의 정정 작업에 둘 이상의 CHG가 연결되어 있는 경우 상태 동기화는 수명 주기의 가장 초기 상태에 있는 CHG의 상태를 기반으로 합니다. 예를 들어 다음 표와 같이 정정 작업에 CHG1, CHG2, CHG3, CHG4 등 4개의 CHG가 연결되어 있다고 가정해 보겠습니다.

변경 번호	변경 상태
1	구현
2	취소됨
3	종결됨(실패 종결 코드)
4	종결됨(종결 코드 실패)

이 경우 CHG와 정정 작업 간의 상태 동기화는 4개의 CHG 중 가장 초기 상태인 CHG1(구현)을 기반으로 합니다. 이 경우 정정 작업은 구현 대기 중 상태로 유지됩니다.

또 다른 예로, 정정 작업이 해결됨 상태이고 구현되어 검토 상태인 기존 CHG가 있는 경우 새 CHG가 생성되면 정정 작업이 해결됨 에서 구현 대기 중으로 다시 전환됩니다. 상태 동기화는 가장 빠른 상태의 CHG인 신규 상태의 CHG를 기반으로 합니다.

변경 번호	변경 상태
1	검토
2	신규

또한 정정 작업에 둘 이상의 CHG가 있는 경우 다음과 같은 경우에 정정 작업의 상태가 자동으로 전환됩니다.

- CHG가 검토로 이동할 때 정정 작업과 연결된 다른 모든 CHG가 검토 또는 종결 상태(성공적인 종결 코드 포함)인 경우 정정 작업은 자동으로 해결됨으로 전환됩니다. 취소되거나 성공적으로 종결된 기타 관련 CHG는 무시됩니다.
- CHG가 취소 됨 또는 종결 (실패의 종결 코드)로 이동할 때 정정 작업과 연결된 다른 모든 CHG가 동일한 상태인 경우 정정 작업은 자동으로 다시 조사 중으로 전환됩니다.

정정 작업 상태 및 각 상태에서 수행할 수 있는 작업에 대한 자세한 내용은 다음 문서를 참조하십시오 구성 준수 상태.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

도메인 분리 및 구성 준수

구성 준수에서는 도메인 분리가 지원됩니다. 도메인 분리를 사용하여 데이터, 프로세스 및 관리 작업을 도메인이라는 논리적 그룹으로 분할할 수 있습니다. 어떤 사용자가 데이터를 보고 액세스할 수 있는지를 포함하여 이러한 분리의 여러 측면을 제어할 수 있습니다.

주:
의 구성 준수v14.9부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v14.9 이전 용어	용어 **v14.9** 이상
테스트 결과 그룹	정정 작업
그룹 규칙	정정 작업 규칙
정책	테스트 그룹

지원 수준: 표준

- 기본 수준 지원의 모든 측면을 포함합니다.
- 애플리케이션 속성이 필요에 따라 도메인을 인식합니다.
- 비즈니스 논리: 서비스 제공자(SP)가 고객별로 프로세스를 만들거나 수정합니다. 사용 사례는 여러 SP 고객이 단일 인스턴스에서 애플리케이션을 올바르게 사용하는 것을 반영합니다.
- 인스턴스 소유자는 특정 애플리케이션에 필요한 대로 테넌트별 최소 실행 가능한 제품(MVP) 비즈니스 논리 및 데이터 매개변수를 구성해야 합니다.

샘플 사용 사례: 관리자가 한 테넌트에 대해서는 기록이 닫히지만 다른 테넌트에 대해서는 기록이 닫히지 않는 경우 설명이 필요하도록 설정할 수 있어야 합니다.

지원 수준에 대한 자세한 내용은 도메인 분리를 위한 애플리케이션 지원 을 참조하십시오.

구성 준수에서 도메인 분리가 작동하는 방식

도메인 분리를 사용하면 서비스를 제공하는 고객 기반 전체에서 ()구성 준수 절차를 표준화하여 운영 비용을 절감하고 서비스 품질을 높일 수 있습니다.

워크플로우, 대시보드, 보고서 등을 위한 별도의 고객 작업 공간을 사용하면 고객 데이터가 분리되어 다른 클라이언트에게 노출되지 않습니다.

버전 릴리스별 구성 준수 도메인 분리 지원

릴리스	지원 수준	메모
Orlando	표준	
파리	표준	
Quebec	표준	
Rome	표준	
San Diego	표준	
Tokyo	표준	
유타	표준	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

버전 릴리스별 구성 준수 도메인 분리 지원

릴리스	지원 수준	메모
밴쿠버	표준	

애플리케이션의 도메인 분리는 구성 준수 다음 제품 기능을 포함합니다.

- 올바른 도메인의 외부 공급업체 스캐너(Qualys)에서 테스트 결과를 수집합니다.

  통합 사용자의 데이터와 동일한 도메인에서 데이터 수집으로, 해당 자격 증명이 통합에 사용됩니다.

- 요청된 도메인의 특정 호스트를 구성 준수 다시 스캔합니다.
- CMDB CI 조회 프로세스를 사용하여 스캐너의 CI 정보가 통합 사용자 도메인의 CMDB에 있는 CI와 일치하는지 확인합니다.
- 통합 사용자와 동일한 도메인에 정의된 위험 점수 계산기에 따라 테스트 결과 수준에서 위험 점수를 계산합니다.
- 정정 작업 규칙은 통합 사용자의 도메인과 동일한 도메인에서 정의, 할당 및 유지될 수 있습니다.
- 문서 정정 작업 규칙을 사용하여 생성된 정정 작업은 정정 작업 규칙이 생성된 도메인과 동일한 도메인에 유지됩니다.
- 연기 워크플로우는 연기가 요청되는 동일한 도메인에서 승인 프로세스를 진행합니다.
- 보고서와 대시보드에는 테스트 결과의 경과 기간, CI별 열린 테스트 결과, 속한 도메인의 영향에 따른 테스트 결과 등의 테스트 결과 상태가 표시됩니다.
- 외부 공급업체 스캐너(Qualys)의 지식은 전역 도메인에서 수집할 수 있으며 여러 클라이언트에서 데이터를 공유할 수 있습니다.

주:
위의 모든 경우에 NOW Platform에서 분리된 도메인 분리의 가시성에 대한 중요한 원칙이 적용됩니다.

사용 사례

애플리케이션은 구성 준수 테스트 결과의 수명 주기를 엔드투엔드로 관리합니다. 다음 사용 사례는 도메인 분리를 인식합니다.

- 다음에서 테스트 결과 수집Qualys
  - 여러 인스턴스에서 데이터 수집
  - 테스트 결과 중복 제거
  - CMDB CI와 매칭
- 위험 점수로 테스트 결과 보강
  - 자산 보강(CMDB)
  - 위험 점수
- 테스트 결과를 그룹화하고 정정 작업 할당
  - 테스트 결과 자동 그룹화
  - 정정 작업 자동으로 할당
- 정정

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 정정 작업으로 할당된 정정 작업
- 포괄적인 정정 수명주기
- 연기 워크플로우

- 조직 및 규정 준수 관리 프로그램의 보안 태세 측정
  - 규정 준수, 범주, 중요도 및 기술별 결과 추세
  - 정책, 테스트, 호스트, 테스트 결과 및 위험 점수의 상태 및 분포

설정

의 구성 준수 도메인 분리를 설정하는 데는 추가 단계가 필요하지 않습니다. 모든 구성 준수 테이블은 인스턴스가 도메인으로 분리된 후 도메인 열을 획득합니다. 테스트 결과 통합을 특정 도메인으로 임포트하도록 지시할 수 있습니다. 자세한 내용은 통합을 위해 도메인 분리 임포트 작성 문서를 참조하십시오. 추가 주의 사항 및 설정에 대한 자세한 내용은 문서를 참조하십시오 도메인 분리에 대한 추가 설정.

도메인 분리 데이터

데이터는 도메인으로 분리될 수 있으며 이는 다음을 의미합니다.

- 외부 공급업체 스캐너에서 수집된 테스트 결과는 통합 사용자의 도메인과 동일한 도메인에 유지되며 다른 도메인에서 액세스할 수 없습니다.
- 한 도메인의 테스트 결과나 호스트는 다른 도메인에서 볼 수 없습니다.
- 위험 점수 산정 알고리즘 및 테스트 결과 그룹 규칙은 도메인 외부의 사용자가 볼 수 없습니다.
- 한 도메인에서 생성된 지연 워크플로우는 다른 도메인에 표시되지 않습니다.
- 모든 이메일 알림은 자신이 속한 도메인에 포함됩니다.

규정 준수 분석가가 자신의 애플리케이션 데이터를 관리하는 방법

- 분석가는 자체 애플리케이션 설치, 다중 소스 애플리케이션 관리 및 CI 조회 규칙을 생성합니다.
- 분석가는 도메인 내에서만 사용할 특정 통합을 구성할 수 있습니다.
- 분석가는 고유한 지연 및 변경 관리 워크플로우를 생성할 수 있습니다.
- 분석가는 자체 정정 작업 규칙, 위험 점수 산정 로직을 생성하여 결과의 우선순위를 정확하게 지정하고 정정 작업을 자동으로 할당하고 올바른 할당 그룹에 할당할 수 있습니다.
- 도메인 사용자가 수동 정정 작업을 생성한 다음 닫습니다.

인스턴스 소유자가 도메인 분리할 수 있는 비즈니스 로직 및 프로세스

- 구성 준수 사용자 및 그룹
- 구성 준수 통합(Madrid 릴리스부터 시작)
- 전체 설정 구성(사용자 및 그룹 관리, 애플리케이션 설치, 다중 소스 애플리케이션 관리, CI 조회 규칙, 정정 작업 규칙, 위험 계산기 등)
- 지연을 포함한 전체 정정 수명주기

관련 정보

서비스 제공자용 도메인 분리

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

구성 준수 중요도 맵

구성 준수 중요도 매핑은 중요도 필드를 소스에서 의 필드 구성 준수로 변환합니다.

구성 준수 기본 시스템은 표준에 Qualys Cloud PlatformServiceNow 대한 매핑과 함께 제공됩니다. 중요도 맵을 만들거나 편집하는 작업은 사용자 환경에서 사용자 지정되거나 표준이 아닌 외부 공급업체 매핑에만 사용할 수 있습니다.

구성 준수 상태

를 사용하면 구성 준수상태 모델을 확인하여 주어진 시간의 정정 작업 상태를 파악할 수 있습니다. 정정 작업 상태는 테스트 결과 상태를 우선순위에 따라 제어합니다.

주:
의 구성 준수v14.9부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v14.9 이전 용어	용어 **v14.9** 이상
테스트 결과 그룹	정정 작업
그룹 규칙	정정 작업 규칙
정책	테스트 그룹

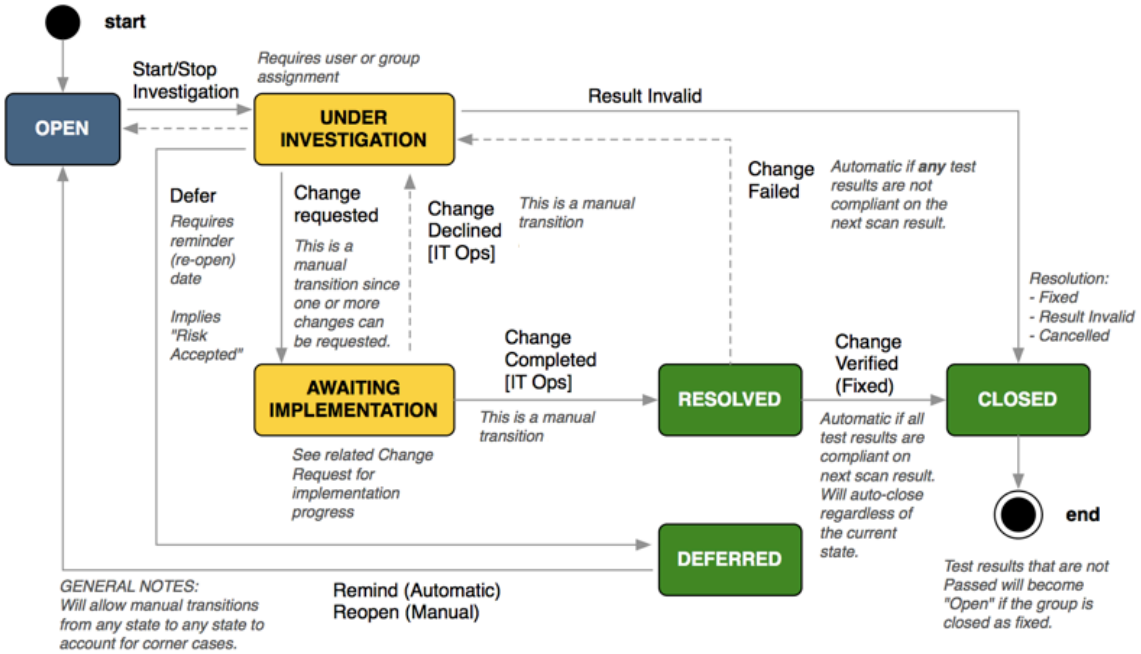
정정 작업 상태

RT(정정 작업)에는 여러 가지 상태가 있을 수 있습니다. 자동 전환은 다음 스캔 결과에 따라 해결됨 상태에서 사용할 수 있습니다. 다음 스캔에서 모든 테스트 결과가 통과되면 정정 작업이 종결됩니다. 그렇지 않으면 조사 중 상태로 전환됩니다. 시스템은 종결 상태를 확인하지만 테스트 결과가 정정 작업에 추가되거나 정정 작업에서 삭제되면 정정 작업 상태를 다시 평가합니다. 작업 메모는 전환을 반영하도록 업데이트됩니다.

다음 그림은 정정 작업의 상태가 열림 상태에서 종결됨 상태로 전환되는 방식을 보여줍니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

구성 준수 상태 플로우 **(v15.0** 이전)



주:

- 각 정정 작업 양식에는 작업의 표준 ServiceNow 인 팔로우 및 업데이트 버튼이 포함되어 있습니다.
- 의 구성 준수v15.0부터 다음이 제거되었습니다.
  - 닫기 버튼
  - 해결 모달의 해결 필드

다음 표에는 상태가 나열되어 있습니다 구성 준수 .

구성 준수 상태

상태	설명
오픈	생성 시 상태입니다.
조사 중	조사 시작 버튼으로 트리거됩니다. 이 상태에서는 다음을 수행할 수 있습니다. 변경 요청 생성 자세한 내용은 구성 준수에서 변경 요청 만들기 문서를 참조하십시오. 예외 요청 이유를 입력하고 재개시 날짜를 선택합니다. 삭제 삭제를 확인합니다. 정정 작업을 제거합니다. 긍정 오류로 표시 이유와 메모를 제공합니다. 정정 작업을 긍정 오류로 표시합니다.
검토 중	다음 동작에 대한 정정 작업을 평가할 때 트리거됩니다. 일반적으로 구현 전에 조사 결과를 확인하거나 제안된 변경/예외를 승인하는 데 사용됩니다. 이 상태에서는 승인 또는 거부에 따라 다음 중 하나로 전환할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

구성 준수 상태

상태	설명
	대기 중인 구현 승인된 경우 구현 대기 중으로 전환 조사 중 추가 분석이 필요한 경우 조사 중으로 다시 전환합니다. 삭제 삭제를 확인합니다. 정정 작업을 제거합니다.
연기됨	지연 버튼으로 트리거됩니다. 이 상태에서 다음을 수행할 수 있습니다. 재개설 열림 상태로 다시 전환합니다. 삭제 삭제를 확인합니다. 그룹을 제거합니다. 연기 정보는 연기/종결 관련 탭에 표시됩니다. 지연 날짜에 그룹은 정정을 위해 다시 열립니다.
대기 중인 구현	구현 대기 중 버튼으로 트리거됩니다. 이 상태에서 다음을 수행할 수 있습니다. 보안 인시던트 생성 자세한 내용은 보안 인시던트 만들기를 참조하십시오. 변경 요청 생성 자세한 내용은 구성 준수에서 변경 요청 만들기 문서를 참조하십시오. 해결 해결 메모에 정정 작업을 해결하는 이유를 추가합니다. 상태가 해결됨이 됩니다. 메모는 해결 관련 탭 아래에 표시됩니다. 삭제 삭제를 확인합니다. 정정 작업을 제거합니다.
해결 일시	해결 버튼에서 트리거됩니다. 이 상태에서 다음을 수행할 수 있습니다. 보안 인시던트 생성 자세한 내용은 보안 인시던트 만들기를 참조하십시오. 재개설 열림 상태로 다시 전환합니다. 삭제 삭제를 확인합니다. 정정 작업을 제거합니다. 메모 관련 탭 아래에 메모가 나타납니다. 해결 정보는 해결 관련 탭 아래에 표시됩니다. 메모는 정정 작업과 연결된 모든 테스트 결과의 작업 메모 에 반영됩니다.
종결됨	닫기 버튼 또는 긍정 오류로 표시 버튼에서 트리거됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

구성 준수 상태

상태	설명
	v14.12 of 구성 준수부터 정정 작업을 긍정 오류로 표시하여 종결할 수 있습니다. 이 상태에서 다음을 수행할 수 있습니다. 재개설 열림 상태로 다시 전환합니다. 삭제 삭제를 확인합니다. 그룹을 제거합니다. 종결 정보는 연기/종결 관련 탭에 표시됩니다. 메모는 정정 작업과 연결된 모든 테스트 결과의 작업 메모 에 반영됩니다.

- 정정 작업이 종결 또는 수정됨으로 표시되고 추가된 테스트 결과 자체가 종결 또는 수정됨이 아닌 경우 테스트 결과 상태는 변경되지 않고 정정 작업 상태가 미결로 변경됩니다.
- 새 정정 작업을 생성하거나 정정 작업을 분리하면 새 정정 작업과 이전 정정 작업에 대해 이유 및 종료 필드가 다시 평가됩니다. 모든 테스트 결과의 상태가 연기됨이면 이유 및 **Until** 필드의 값이 정정 작업으로 롤업됩니다.
  - 정정 작업의 모든 테스트 결과가 지연되고 이유가 동일한 경우 정정 작업에 동일한 이유가 할당됩니다. 그렇지 않으면 이유 필드가 없음으로 변경됩니다.
  - 종료 필드의 날짜는 테스트 결과가 속한 모든 정정 작업의 종료 날짜와 가장 가까운 날짜로 업데이트됩니다.

  주:
  이 평가는 1시간마다 실행되는 예약된 작업에 의해 *Rollup test result values to test result RT1nd configuration test* 수행됩니다.

- 마지막으로 본 시간이 해결된 테스트 결과의 해결 날짜보다 크면 테스트 결과가 다시 오픈됩니다. 해결된 정정 작업에서 수집 중에 하나 이상의 테스트 결과가 다시 열리면 정정 작업이 조사 중 상태로 전환됩니다.

테스트 결과 상태

정정 작업의 상태는 관련 테스트 결과의 상태도 변경합니다. 이 메커니즘에는 두 가지 경우가 있습니다.

하나의 정정 작업에만 속하는 테스트 결과

결과는 다음 세 가지 예외를 제외하고 정정 작업의 상태와 일치합니다.

- 정정 작업의 상태가 종결로 변경되고 해결(하위 상태)이 수정됨으로 변경되면 항목은 해당 변경을 무시하고 열림 상태로 돌아갑니다.
- 정정 작업의 상태가 종결로 변경되고 해결(하위 상태)이 취소됨으로 변경되면 항목은 해당 변경을 무시하고 열림 상태로 돌아갑니다.
- 테스트 결과 소스 상태가 수정(스캔 또는 임포트에 의해 업데이트됨)인 경우 정정 작업의 상태가 변경되면 정정 작업의 상태에 관계없이 테스트 결과가 상태를 종결(고정)로 변경합니다.

여러 정정 작업에 속한 테스트 결과

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테스트 결과가 정정 작업의 상태와 자동으로 일치하지 않습니다. 대신 연관된 모든 그룹 중에서 검색하여 적용할 우선순위가 가장 높은 상태를 찾습니다. 우선순위 상태는 다음과 같습니다.

종결됨 〉 종결(하위 상태: 긍정 오류) 〉 연기됨 〉 해결 일시 〉 검토 중 〉 대기 중인 구현 〉 조사 중 〉 오픈 〉 종결됨(하위 상태: 취소됨) 〉 종결됨(하위 상태: 고정됨)

주:
종결됨(하위 상태: 고정됨) 과 종결됨(하위 상태: 취소됨) 은 두 가지 특별한 경우입니다.

주:
의 구성 준수v15.0부터 잘못된 결과 하위 상태가 더 이상 사용되지 않습니다.

정정 작업 상태 예

예:

정정 작업 상태	테스트 결과 상태
RT1: 오픈 〉 조사 중 RT2: 열림	조사 중 RT1이 조사 중이고 RT2가 오픈인 경우 검색 후 RT1과 RT2 사이에서 RT1의 우선순위가 가장 높은 상태가 되기 때문에 테스트 결과가 조사 중으로 변경됩니다.
RT1: 조사 중 RT2: 오픈 〉 조사 중	조사 중 RT2가 조사 중이고 RT1이 조사 중인 경우 검색 후 RT1과 RT2 사이에서 우선순위가 동일한 상태를 가지므로 테스트 결과는 조사 중으로 유지됩니다.
RT1: 조사 중 RT2: 조사 중 〉 대기 중인 구현	대기 중인 구현 RT2가 구현 대기 중이고 RT1이 조사 중인 경우 검색 후 RT1과 RT2 사이에서 RT2의 우선 순위가 가장 높은 상태가 있으므로 테스트 결과가 구현 대기 중으로 변경됩니다.
RT1: 조사 중 〉 연기됨 RT2: 대기 중인 구현	연기됨 RT1이 지연되고 RT2가 구현 대기 중이면 검색 후 항목 1이 RT1과 RT2 사이에서 RT1의 우선순위가 가장 높은 상태를 가지는 것을 발견했기 때문에 테스트 결과가 지연됨으로 변경됩니다
RT1: 연기됨 RT2: 대기 중인 구현 〉 종결됨(잘못된 결과)	종결됨(잘못된 결과) 〉 연기됨 RT2가 종결되고 해결(하위 상태)이 잘못된 결과이고 RT1이 지연되면 검색 후 RT1과 RT2 사이에서 RT2의 우선순위가 가장 높은 상태가 되므로 테스트 결과가 종결(잘못된 결과)으로 변경됩니다.
RT1: 연기됨 RT2: 종결됨(잘못된 결과) 〉 오픈(다시 오픈을 통해)	연기됨

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

정정 작업 상태	테스트 결과 상태
	RT2가 다시 열리고 상태가 열림으로 변경되고 RT1이 지연되면 검색 후 RT1과 RT2 사이에서 RT1의 우선순위가 가장 높은 상태가 되기 때문에 테스트 결과가 지연됨으로 변경됩니다.
RT1: 연기됨 RT2: 대기 중인 구현 〉 종결(긍정 오류)	종결(긍정 오류) RT2가 종결되고 해결 방법(하위 상태)이 긍정 오류이고 RT1이 지연되면 검색 후 RT1과 RT2 사이에서 RT2의 우선 순위가 가장 높은 상태가 되기 때문에 테스트 결과가 종결(긍정 오류)로 변경됩니다.

테스트 결과 상태 특수 케이스

정정 작업 상태	테스트 결과 상태
RT1: 조사 중 RT2: 대기 중인 구현 〉 종결(고정 또는 취소됨)	조사 중 RT2가 종결(하위 상태 고정 또는 하위 상태 취소됨)이고 RT1이 조사 중이면 테스트 결과가 구현 대기 중(이전에는 가장 높은 우선 순위)에서 조사 중(현재 가장 높은 우선 순위)으로 변경됩니다.
RT1: 모든 상태 RT2: 모든 상태	테스트 결과 소스 상태가 수정(스캔 또는 임포트에 의해 업데이트됨)인 경우 정정 작업의 상태가 변경되면 다른 관련 정정 작업의 상태에 관계없이 테스트 결과가 종결(고정)로 변경됩니다. 정정 작업 상태에 대한 테스트 결과 검색이 발생하지 않습니다.

상태 롤업 및 롤다운 시나리오

상태 롤업 및 롤다운 시나리오는 정정 작업(RT)과 구성 테스트 결과(CTR)의 상태를 자동으로 동기화하여 둘 다에 대한 실시간 업데이트를 보장합니다. 이러한 동적 상호작용은 수동 추적을 줄이고 정확도를 높이며 사용자에게 진행 상황에 대한 최신 뷰를 제공하여 구성 규정 준수를 보다 효율적으로 만들고 사용자가 정보에 입각한 결정을 신속하게 내릴 수 있도록 지원합니다.

롤업 동작

구성 테스트 결과(CTR) 상태가 변경되면 이러한 변경 내용이 RT(정정 작업) 수준까지 전파될 수 있습니다.

다음 표에는 종결 조건, 재할당 및 지연에 따라 구성 테스트 결과(CTR) 상태의 변경이 관련 정정 작업(RT) 상태에 영향을 줄 수 있는 주요 롤업 시나리오가 요약되어 있습니다.

롤업 시나리오

CTR 상태	**RT** 상태
열림 〉 닫힘-고정	열림 〉 닫힘-고정
오픈 〉 종결-부실	오픈 〉 종결-취소됨

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

롤다운 동작

정정 작업의 상태가 변경될 때 수동 업데이트나 예외에 의해 재정의되지 않는 한 상태가 연결된 CTR로 전파되는 경우가 많습니다.

다음 표에는 우선순위 규칙 및 특수 조건에 따라 RT(정정 작업) 상태의 변경이 연결된 CTR(구성 테스트 결과) 상태에 영향을 줄 수 있는 주요 롤업 시나리오가 요약되어 있습니다.

롤업 시나리오

RT 상태	**CTR** 상태
조사 중인 〉 열기	조사 중인 〉 열기
오픈 〉 검토 중	오픈 〉 검토 중
오픈 〉 연기됨	오픈 〉 연기됨
지연 〉 오픈	연기된 상태로 유지
해결됨-수정 〉 열기	해결됨-수정 〉 열기
열림 〉 해결됨-수정 〉 종결됨-고정	열림 〉 해결됨-수정 〉 종결됨-고정
해결됨-결과가 잘못된 오픈 〉	해결됨-결과가 잘못된 오픈 〉
오픈 〉 해결됨-취소됨	오픈 〉 해결됨-취소됨
오픈 〉 해결됨-취소됨 〉 종결됨	오픈 〉 해결됨-취소됨 〉 종결됨
오픈 〉 해결됨-결과 유효하지 않음 〉 종결됨-결과 유효하지 않음	오픈 〉 해결됨-결과 유효하지 않음 〉 종결됨-결과 유효하지 않음
열림 〉 닫힘-고정	열림 〉 닫힘-고정

임포트 문제 해결 구성 준수

외부 공급업체 통합 임포트 문제를 해결합니다.

문제 해결 임포트

문제	해결
테스트 결과가 누락되었습니다.	*Start Time*Qualys PC 결과 통합을 확인합니다. 충분히 뒤로 물러나지 않을 수도 있습니다. Qualys PC 결과 시작 날짜 수정 문서를 참조하십시오.
통합에 실패했습니다.	취약성 통합 실행 상태를 확인합니다. 개별 통합 프로세스 항목에는 임포트한 XML이 포함되며, 예기치 않은 정보가 있는지 검사할 수 있습니다. 다음으로 이동 **Qualys** 취약성 통합 〉 기본 통합 〉 **QualysPC** 결과 〉 취약성 통합 실행 관련 탭. 최신 실행을 선택합니다. 관련 목록 취약성 통합 프로세스에 있는 항목의 상태와 메모를 검사하여 이상 징후를 확인합니다. .

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Qualys PC 결과 시작 날짜 수정

Qualys PC 결과 임포트의 시작 날짜에 데이터가 누락된 경우 수정할 수 있습니다.

시작하기 전에
필요한 역할: sn_vul_qualys.admin

프로시저

1. 다음으로 이동 모두 〉 **Qualys** 취약성 통합 〉 관리 〉 기본 통합.
2. **Qualys PC** 결과 통합을 클릭합니다.
3. 통합 상세 정보를 클릭합니다.
4. 시작 시간 필드를 과거 값으로 설정하면 해당 시간 이후에 스캔되고 탐지된 모든 테스트 결과가 검색됩니다.

   주:
   날짜를 비워 두면 첫 번째 실행에서 데이터가 반환되지 않습니다. 이 값을 최대 과거 월로 설정합니다. 이 설정은 많은 양의 데이터가 Qualys API 속도 제한을 초과하지 않도록 하고 실행 시간 제한을 트리거하지 않도록 합니다.

5. 제출 또는 업데이트를 클릭합니다.
6. 옵션: 지금 실행을 클릭하여 즉시 실행합니다.

에 대한 Microsoft Defender for Cloud Integration보안 운영 및 CI 조회 규칙 Palo Alto Prisma Cloud

및 Palo Alto Prisma Cloud 통합에 대한 Microsoft Defender for Cloud Integration CI(구성 항목) 조회 규칙을 사용하여 에서 일반적으로 사용되는 자원 유형에 대한 올바른 일치 항목을 찾을 수 있습니다구성 관리 데이터베이스(CMDB).

개요

CI 조회 규칙 모듈에는 에 일치하는 데이터가 있는 필드를 정의하는 데 도움이 되는 규칙이 포함되어 있습니다 구성 관리 데이터베이스(CMDB). 이러한 규칙을 사용하여 애플리케이션 및 애플리케이션 릴리스를 식별할 수 있습니다. 모든 Microsoft Defender for Cloud Integration 자산과 Palo Alto Prisma Cloud 자산은 플랫폼에서 객체 ID, 클라우드 계정 및 논리 데이터센터의 ServiceNow 조합으로 고유하게 식별됩니다. ServiceNow 검색은 다양한 자원 유형에 대해 서로 다른 형식으로 의 Object_id 열에 CMDB 있는 자원 ID를 채웁니다. 다음 표에서는 검색 서비스가 CI의 Object_id 열을 채우는 데 사용하는 일반적으로 사용되는 자원 유형의 객체 ID 형식을 보여줍니다. 특정 리소스 유형의 자산을 조회하려는 모든 스캐너는 올바른 개체 ID 형식을 사용하여 검색해야 합니다. 해당 CMDB CI 클래스의 객체 ID 열을 조사한 다음 스캐너에서 받은 값을 사용하여 객체 ID를 구성하여 올바른 객체 ID 형식을 얻을 수 있습니다.

다양한 자원 유형에 대한 객체 **ID** 형식

자원 유형	형식
AWS::EC2::Instance	객체 ID
AWS::ElasticLoadBalancing::LoadBalancer	부하 분산 장치 이름
AWS::S3::Bucket	arn:aws:s3:::〈버킷 이름〉

조회 규칙에 동일한 형식의 `object_id` 사용하지 않으면 테스트 결과에 대한 CI 일치를 정확하게 구성 관리 데이터베이스(CMDB) 찾지 못할 수 있습니다. 대부분의 경우 OOB CI 조회 규칙은 및 Palo Alto Prisma Cloud에 대해 Microsoft Defender for Cloud Integration 가장 일반적으로 사용되는 자원

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

유형에 대한 일치 항목을 찾습니다. 다음 CI 조회 규칙이 테스트 결과에서 CMDB CI를 찾지 못하는 경우 자원 유형에 대한 CI 조회 규칙을 만들 수 있습니다. CI 조회 규칙을 생성하는 방법에 대한 자세한 내용은 CI 조회 규칙 생성을 참조하십시오.

CI 조회 규칙

다음 CI 조회 규칙은 Microsoft Defender for Cloud Integration 및 Palo Alto Prisma Cloud.

S3 버킷

이 조회 규칙은 arn:aws:s3::: 및 자원 이름을 연결하여 얻은 값으로 에서 CI CMDB 를 찾으려고 시도합니다. 얻은 값은 cmdb_ci_cloud_object_storage 테이블의 object_id 열에서 조회됩니다. 이 조회 규칙은 자원 유형이 AWS::S3::Bucket인 경우에만 적용됩니다.

이름

이 조회 규칙은 이름순으로 CMDB CI를 찾으려고 시도합니다. CI 클래스의 Object_id 열에서 조회되는 이름은 sn_capi_resource_type 테이블의 자원 유형에 해당합니다.

> **주:**
> Palo Alto Prisma Cloud 애플리케이션의 경우 이 CI 조회 규칙은 AWS::RDS::DBInstance, AWS::ElasticLoadBalancing::LoadBalancer 및 AWS::CloudTrail::Trail 자원 유형에 대해서만 실행됩니다. 이 CI 조회 규칙을 실행하려는 자원 유형을 추가할 수 있습니다.

자원 **ID**

이 조회 규칙은 자원 ID로 CI CMDB 를 찾으려고 시도합니다. CI 클래스의 Object_id 열에서 조회되는 자원 ID는 sn_capi_resource_type 테이블의 자원 유형에 해당합니다.

> **주:**
> 순서 필드에서 CI 조회 규칙의 우선순위를 설정할 수 있습니다. 순서 값이 가장 작은 CI 조회 규칙이 먼저 실행됩니다.

취약성 대응 작업 공간

Vulnerability Response Workspace는 생산성을 높이고 시간을 절약함으로써 동일한 창 내에서 멀티태스킹을 수행할 수 있는 기능에 대한 통합 보기를 제공합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약성 대응 작업 공간

취약성 관리자 작업 공간	**IT** 정정 작업 공간	취약성 평가 작업 공간
취약성 관리자 작업 공간에 대해 알아보기	IT 정정 작업 공간에 대해 알아보기	취약성 평가 작업 공간에 대해 알아보기

시작하기 전에

작업 공간을 사용하려면 다음을 수행합니다.

- 몇 가지 구성 작업을 수행해야 합니다. 자세한 내용은 취약성 대응 작업 공간 구성 문서를 참조하십시오.
- 에서 취약성 대응 정정 작업 및 정정 작업 규칙에 대한 작업 공간 및 업데이트정정 작업, 정정 작업 규칙, 작업 공간에 대한 주요 용어 및 개념에 대한 업데이트에 대한 중요한 정보를 검토합니다.

문제 해결 및 도움 받기

- Security Operations on ServiceNow 커뮤니티
- 알려진 오류 포털에서 알려진 오류 문서 검색
- 연락처 고객 서비스 및 지원

취약성 대응 작업 공간 개요

취약성 관리자 및 IT 정정 작업 공간은 , 애플리케이션 취약성 대응, 컨테이너 취약성 대응및 구성 준수를 지원합니다취약성 대응.

취약성 관리자, **IT** 정정 및 취약성 평가 작업 공간

취약성 관리자 작업 공간

취약성 관리자는 멀웨어 및 악의적인 공격으로부터 회사의 자산을 보호합니다. 애플리케이션의 단일 작업 영역 ServiceNow AI Platform#취약성 대응 에서, 취약성 라이브러리 및 외부 공급업체 스캐너 데이터 애플리케이션에서 인스턴스로 임포트한 현재 취약성 데이터와 함께 중요한 취약성과 잘못된 구성을 식별하고 우선순위를 지정한 다음 전문가가 조치를 취할 수 있도록 정정 작업 목록을 IT 부서에 보냅니다.

IT 정정 작업 공간

IT 전문가는 취약성 관리자가 보낸 목록 또는 정정 작업(RT)을 사용하여 사용자 또는 그룹에 할당된 중요한 취약성을 모니터링하고 해결합니다. 패치, 솔루션,

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약성 재검색, 변경 요청, 예외 및 취약한 항목을 정정하고 결과를 모두 한 위치에서 테스트하는 기타 도구를 사용하여 취약한 항목 그룹을 수정합니다.

취약성 평가 작업 공간

취약성 이벤트 관리자는 노출 평가를 수행하고 특히 제로 데이 이벤트와 같은 중요한 취약성 이벤트 중에 중요한 취약성 이벤트를 사전에 관리합니다.

주요 기능

작업 공간에는 취약성 대응 다음과 같은 기능과 향상된 기능이 포함되어 있습니다.

- 의 취약성 관리자 작업 공간 대량 편집 기능을 사용하여 여러 기록을 동시에 업데이트합니다. 자세한 내용은 에서 대량 편집 사용 취약성 관리자 작업 공간 문서를 참조하십시오.
- 취약성 관리자 작업 공간의 대시보드 페이지에서 Next Experience UI에 취약성 관리(PA), 취약성 승인, CISO, 컨테이너 취약성 관리 개요, 애플리케이션 취약성 관리 대시보드, 통합 취약성 대응 및 상태 대시보드를 봅니다. 자세한 내용은 대시보드 페이지의 취약성 관리자 작업 공간 문서를 참조하십시오.
- IT 정정 작업 공간의 대시보드 페이지에서 Next Experience UI의 취약성 정정 대시보드를 봅니다. 자세한 내용은 대시보드 페이지의 IT 정정 작업 공간 문서를 참조하십시오.
- 및 IT 정정 작업 공간에서 수동으로 정정 작업(VUL, AVUL, CBULB 또는 CRG)을 생성합니다취약성 관리자 작업 공간. 자세한 내용은 에서 수동으로 정정 작업 생성 취약성 관리자 작업 공간 및 에서 수동으로 정정 작업 생성 IT 정정 작업 공간 문서를 참조하십시오.
- 및 에서 정정 작업(VUL, AVUL, CBULB 및 CRG) 취약성 관리자 작업 공간 을 분할합니다 IT 정정 작업 공간. 자세한 내용은 AND 에서 정정 작업 분할 IT 정정 작업 공간 문서를 참조하십시오에서 정정 작업 및 기록에 대한 예외 요청 취약성 관리자 작업 공간.
- 취약성 관리자 및 IT 정정 작업 공간에서 취약한 항목(VIT, AVIT 및 CVIT) 및 정정 작업(VUL, AVUL, CVUL 및 CRG)에 대한 정책 예외를 요청합니다. 자세한 내용은 AND 에서 사용하는 예외 GRC: 정책 및 준수 관리 요청 IT 정정 작업 공간 문서를 참조하십시오에서 정정 작업 및 기록에 대한 예외 요청 취약성 관리자 작업 공간.
- VCM(취약성 위기 관리)을 통해 중요한 취약성 이벤트를 생성하고 추적합니다. 자세한 내용은 취약성 평가 작업 공간 탐색 문서를 참조하십시오.
- 의 Compensating controls 라이브러리에 compensating controls를 취약성 관리자 작업 공간추가합니다. 자세한 내용은 라이브러리에 보정 통제 추가 문서를 참조하십시오.
- IT 정정 작업 공간에서 호스트 취약한 항목 및 정정 작업에 대한 위험 감소를 요청합니다. 자세한 내용은 취약한 항목 또는 정정 작업에 대한 위험 감소 요청 문서를 참조하십시오.
- 에서 취약성 관리자 작업 공간애플리케이션 및 컨테이너 취약한 항목에 대한 Agile 문제 및 Jira 문제를 생성합니다. 자세한 내용은 양식 작업을 사용하여 수동으로 Agile 문제 생성 및 목록 작업을 사용하여 수동으로 Agile 문제 생성 문서를 참조하십시오.

제품군 릴리스와의 버전 호환성에 대한 자세한 내용은 HI 지식베이스에서 KB0856498 Vulnerability Response 호환성 매트릭스 및 릴리스 스키마 변경 문서를 참조하십시오.

작업 공간으로 취약성 대응 오케스트레이션 패치

를 사용한 취약성 대응Patch 오케스트레이션을 사용하여 대규모 자산 그룹의 중요한 취약성에 대한 패치 및 패치 배포를 관리할 수 있습니다.

작업 공간의 **Patch** 오케스트레이션

애플리케이션을 사용한 취약성 대응 패치 오케스트레이션은 타사 솔루션 통합, 패치 벤더 및 취약성 스캐너에서 예약된 임포트를 사용합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

애플리케이션을 사용한 취약성 대응 패치 오케스트레이션은 클래식 환경과 취약성 대응 작업 공간 모두에서 지원됩니다. 상관 관계가 있는 데이터가 롤업되어 작업 공간과 클래식 환경 모두에 표시됩니다. 클래식 환경의 패치 오케스트레이션에 대한 기능, 요구 사항 및 정보에 대한 개요는 다음 문서를 다음으로 오케스트레이션 패치 취약성 대응참조하십시오.

- 패치 벤더와의 지원되는 통합에 대한 자세한 내용은 해당 SCCM 취약성 대응 과의 Microsoft 패치 오케스트레이션 통합 이해문서를 참조하십시오와 HCL BigFix 패치 오케스트레이션의 통합 이해 취약성 대응.
- 작업 공간에서 패치 양식 레코드를 예약하는 방법에 대한 자세한 내용은 해당 패치 오케스트레이션 통합으로 취약성 대응 패치 예약 HCL BigFix문서를 참조하십시오와 SCCM의 Microsoft 통합으로 패치 예약 취약성 대응.

패치 오케스트레이션 통합에 필요한 애플리케이션 및 의존성의 사용 가능한 버전

의 취약성 대응작업 공간에서 패치 오케스트레이션 데이터와 사용 가능한 업데이트(패치)를 보려면 다음 애플리케이션이 필요합니다. 나열된 모든 애플리케이션은 에서 사용할 수 있습니다 ServiceNow# Store. 일부 애플리케이션에는 별도의 구독이 필요합니다. 다음으로 오케스트레이션 패치 취약성 대응 문서를 참조하십시오.

필요한 역할

작업 공간에 필요한 취약성 대응 sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin 역할 외에도 사용자에게는 데이터를 보고 패치를 예약하는 데 사용 중인 패치 오케스트레이션 통합과 관련된 역할이 필요합니다. 이러한 역할에 대한 자세한 내용은 다음 지원되는 통합을 참조하십시오.

와 HCL BigFix 패치 오케스트레이션의 통합 이해 취약성 대응 및 SCCM 취약성 대응 과의 Microsoft 패치 오케스트레이션 통합 이해 문서를 참조하십시오.

작업 공간의 패치 데이터 취약성 대응

IT 정정 작업 공간의 작업 공간에 있는 패치 데이터를 볼 수 있습니다.

- 홈 뷰에서 성과표를 클릭하여 VI의 기본 솔루션, 취약한 CI 및 VI의 기본 설정 패치에 대한 기록을 봅니다.
- 목록 뷰에서 모든 VPU(패치 업데이트 기록)와 사용 가능한 링크의 패치가 있는 사용자에게 할당된 취약한 항목을 봅니다.

다음 기록에서 패치를 예약할 수 있습니다.

- 패치 업데이트(VPU)
- 정정 작업(RT)
- 검색된 항목(SDI)

안에 취약성 관리자 작업 공간, 패치를 볼 수 있습니다.

- 취약한 항목 탭의 감시 주제에 대한 홈 뷰에서 기본 및 잠재적 패치, 패치 일정 날짜 및 기타 정보를 볼 수 있습니다.
- 정정 작업 기록의 목록 뷰에서 취약한 항목 탭의 VIT 기록에 대한 패치 데이터를 볼 수 있습니다.

취약성 대응 정정 작업 및 정정 작업 규칙에 대한 작업 공간 및 업데이트

작업 공간의 정정 작업 번들 기록(VIT, ABIT, CVIT 또는 CTR).취약성 대응

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업 공간의 주요 용어 취약성 대응

취약성 대응 작업 공간 또는 작업 공간

취약성 대응 는 취약성 대응 작업 공간을 지원합니다. 클래식 코어 UI 환경 또는 작업 공간을 사용할 수 있습니다.

클래식(레거시) UI

경험을 참조합니다 코어 UI . 클래식 환경에서 일부 작업을 수행하고 몇 가지 목록을 볼 수 있습니다.

취약성 관리자 작업 공간

이 작업 공간에서 관리자는 대상 취약성을 모니터링하고 IT에 할당할 VI 및 테스트 결과를 선택합니다.

IT 정정 작업 공간

이 작업 공간에서 IT 팀은 보안에 의해 할당된 가장 중요한 취약성에 집중할 수 있습니다. 영향을 받는 고유한 CI(구성 항목), 솔루션, 정정 진행률을 포함하는 IT 중심 정보를 정정 소유자는 이 작업 공간에서 쉽게 사용할 수 있습니다.

취약성 평가 작업 공간

이 작업 공간에서 취약성 분석가는 제로 데이 취약성 분석 중 취약성 평가를 수행할 수 있습니다. 제로 데이 취약성이 식별되면 취약성과 관련된 잠재적 영향 및 위험을 평가할 수 있습니다. 분석가는 영향을 받는 시스템, 애플리케이션 또는 네트워크 구성요소를 분석하여 조직 내의 심각도와 가능한 공격 벡터를 이해할 수 있습니다.

주시 주제

감시 주제는 취약성 관리자와 분석가가 취약성 관리자 작업 공간에서 모니터링하려는 취약한 항목의 세그먼트를 정의합니다. 감시 주제는 추세, CI 및 취약성 관련 통계가 포함된 VI 세그먼트 및 테스트 결과 와 관련된 보고서의 집중적인 개요 세트를 보여줍니다. 이러한 주제의 대시보드를 사용하여 추세를 모니터링할 수 있습니다. 대시보드는 관리자에게 다음과 같은 도움을 줄 수 있습니다.

- 중요 항목에 대한 정정 진행률 보기
- 중요 시스템에 취약성 존재 확인
- 새로운 익스플로잇이 언제 나오는지 확인
- 특정 취약성 세트를 해결하기 위한 신속한 대응 추진

정정 작업(RE)

취약성 관리자는 IT 부서가 감시 주제에 나열된 취약성을 수정해야 할 시기라고 판단할 때 정정 작업을 생성합니다. 취약성 관리자와 분석가는 할당 그룹 및 취약성 등에 따라 정정 작업을 생성하는 방법을 선택할 수 있습니다. 정정 작업은 정정 작업에 포함됩니다.

정정 작업(VUL)

IT 팀은 정정 작업을 사용하여 보안에 의해 할당된 취약성을 정정합니다. 정정 작업은 취약성을 수정하는 데 필요한 작업 목록입니다. 정정 작업은 보안 관리자가 정정 작업을 생성할 때 자동으로 생성됩니다.

작업 공간 개발

이전 버전의 취약성 대응에서는 보안 및 취약성 분석가가 기록 세트(VIT, VIT, CVIT 또는 CTR)를 모니터링하는 두 가지 옵션이 있었습니다.

- 모든 VI를 요약하는 개요 대시보드
- 정정 작업

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

미리 정의된 정정 작업 규칙에 따라 취약한 항목이 정정 작업으로 자동 정렬되었습니다. 정정 작업은 IT 팀이 관리 가능한 취약한 항목 청크를 정정할 수 있도록 지원하기 위해 설계되었습니다.

이 자동화를 통해 대량 할당 및 수정을 위해 매우 많은 수의 기록을 자동으로 그룹화할 수 있습니다. 그러나 취약성 분석가와 관리자는 정정 작업에서 전체 기록 세트를 모니터링하는 것이 어렵다는 것을 알게 되었습니다. 대규모 그룹의 성능 문제 외에도 가장 중요한 취약성만 필터링하는 기능적 정정 작업 규칙을 생성하는 것이 어려울 수 있습니다.

취약성 대응 작업 공간:

- 보안 관리자가 시간 경과에 따라 활성 VI 및 테스트 결과를 필터링하고 모니터링하며 가장 중요하다고 판단한 취약성에 대한 정정을 추진할 수 있도록 지원합니다.
- IT 팀이 보안에 의해 할당된 취약성을 수정하는 데 사용할 수 있는 IT 중심 정보를 한 곳에서 제공합니다.

작업 공간의 정정 작업에 대한 업데이트

취약성 관리자 작업 공간에서 취약성 분석가와 관리자는 정정을 위해 VI를 모니터링하고 할당하는 두 가지 새로운 방법으로 감시 주제 및 정정 노력을 사용합니다.

취약성 그룹의 이름이 정정 작업*(Remediation Tasks)*으로 변경되었습니다. 이 변경 사항은 레거시 UI와 작업 공간 모두에서 목록, 기록 및 규칙의 레이블에 적용됩니다. 정정 작업은 IT 팀이 IT 정정 작업 공간에서 작업할 수 있도록 설정됩니다. 다음 목록에서는 취약성 관리자 또는 취약성 분석가가 취약성 및 테스트 결과를 모니터링하고, 필터링하고, 할당하는 방법을 보여줍니다.

1. 취약성 관리자 작업 공간에서 관리자는 감시 주제에 대해 임포트된 취약성과 잘못된 구성을 모니터링합니다. 관리자와 분석가는 감시 주제를 사용하여 시간 경과에 따라 가장 중요하다고 생각되는 필터링된 기록의 동적 세트를 모니터링합니다.
2. 감시 주제를 통해 보안 관리자는 정정 작업(RE)에서 IT 팀에 넘겨줄 VI의 시기와 종류를 결정할 수 있습니다. 이러한 RE는 보안에서 IT 팀이 수정하기를 원하는 VI의 정적 목록입니다.

   정정 작업에서 관리자는 기록을 정정 작업(VUL, AVUL, CVUL 또는 CRG)에 번들로 묶는 방법에 대한 네 가지 옵션을 사용할 수 있습니다. 정정 작업은 원래 기록과 연결된 할당 그룹에 따라 IT 팀에 자동으로 할당됩니다.
3. IT 팀은 모든 기록을 정렬할 필요 없이 IT 정정 작업 공간에서 정정 작업을 수행합니다.

   정정 작업은 이전 버전의 취약성 대응에서 정정 작업이 수행하는 것과 동일한 상태를 통해 전환됩니다. 정정 작업의 모든 기록이 종결되면 정정 작업이 종결되고 비활성으로 설정됩니다.

   정정 진행률은 감시 주제 및 IT 정정 홈페이지의 데이터 시각화에서 업데이트됩니다.

작업 공간의 정정 작업 규칙 업데이트

취약성 그룹 규칙을 정정 작업 규칙이라고 합니다. 이 변경 사항은 레거시 UI와 작업 공간 모두에서 목록, 기록 및 규칙의 레이블에 적용됩니다.

테이블 이름(예: 〔sn_vul_m2m_vul_group_item〕)은 변경되지 않습니다.

이전 버전의 취약성 대응에서 취약성 그룹 규칙을 생성한 경우 정정 작업 규칙으로 레이블이 지정된 상태로 계속 사용할 수 있습니다.

그러나 작업 공간에서 정정 작업 규칙은 더 이상 대량의 기록을 정정 작업으로 구성하는 기본 방법으로 사용되지 않습니다. 작업 공간에 익숙해지면 정정 작업 규칙을 비활성 상태로 두는 것을 선호할 수 있습니다.

대신 작업 공간을 점진적으로 사용하는 취약성 대응 것을 선호할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

1. 이전 버전의 취약성 대응 업데이트 적용 작업 규칙으로 업그레이드하는 경우 기존 정정 작업 규칙이 유지됩니다. 작업 공간에서 계속 사용할 수 있습니다. 기본 그룹 규칙인 취약성은 기본적으로 비활성 상태입니다.
2. 담당 규칙과 원하는 경우 위험 규칙을 구성한 다음 임포트를 수행합니다.
3. 취약성 관리자 또는 분석가는 취약성 관리자 작업 공간의 감시 주제에서 모니터링할 세그먼트를 선택할 수 있습니다. 주시 주제를 독립 실행형 기능으로 사용할 수 있습니다. 기록의 하위 집합을 선택하고 이에 대한 대시보드를 사용하여 추세를 모니터링합니다. 이를 통해 개선 노력을 집중할 위치와 시기를 결정할 수 있습니다.
4. 취약성 관리자 또는 분석가는 기록의 하위 세트를 정정할 시기가 결정되면 감시 주제에서 정정 작업을 생성합니다. 또한 정정 작업을 생성할 때 IT에 전달되도록 정정 작업이 자동으로 생성됩니다.
5. 시간이 지남에 따라 취약성 관리자 또는 분석가는 정정 작업 규칙으로 자동으로 처리할 수 있는 몇 가지 일상적인 패턴을 발견할 수 있습니다.

정정 작업 규칙을 보려면 **,**애플리케이션 취약성 대응, 컨테이너 취약성 대응및 구성 준수 모두 메뉴에서 각 정정 작업 규칙 모듈취약성 대응로 이동합니다.

작업 공간의 담당 규칙, 정정 작업 규칙, 정정 작업 및 취약한 항목에 대한 취약성 대응 자세한 내용

- 정정 작업 기록은 클래식 환경과 작업 공간 모두에서 목록과 기록에 표시됩니다.
- 정정 작업은 취약성 그룹과 동일한 상태를 통해 전환됩니다. 정정 작업의 모든 기록이 종결되면 정정 작업이 비활성 상태로 전환됩니다.
- 팀의 정정 작업을 돕기 위해 취약한 항목은 한 가지 정정 작업에만 포함될 수 있습니다. 일단 정정 작업에 들어가면 취약한 항목은 사용자가 생성하는 다른 정정 작업에 추가되지 않습니다.
- 정정 작업을 삭제하면 정정 작업이 비활성화되고 새로운 정정 작업에 활성 VI를 사용할 수 있습니다.
- 기록(VIT, AVIT, CVIT 또는 CTR)은 여러 정정 작업에 있을 수 있습니다.
- 정정 작업은 정정 작업의 취약한 항목과 연결된 할당 그룹에 따라 IT 팀에 자동으로 할당됩니다. 요청 시 정정 작업을 생성하는 경우 할당 그룹을 선택합니다.
- 이전 버전에서 취약성 대응업그레이드하는 경우 담당 규칙이 레거시 UI에서 보존됩니다.
- 이전 버전에서 취약성 대응업그레이드하는 경우 현재 사용자와 그룹이 상속되고 작업 공간에서 액세스할 수 있습니다.

정정 작업의 수명주기에 대한 자세한 내용은 다음 문서를 취약성 대응 작업 공간의 정정 작업, 정정 작업 및 기록의 수명주기참조하십시오.

작업 공간의 구성 및 설정 취약성 대응

담당 규칙 및 정정 작업 규칙에 대한 자세한 내용은 해당 취약성 대응 할당 규칙 개요문서를 참조하십시오취약성 대응 작업 공간 구성.

신규 고객이고 아직 추가하지 않은 경우 취약한 항목 및 정정 작업이 원하는 정정 그룹에 할당되도록 사용자와 그룹을 설정해야 합니다. 취약성 대응 담당 규칙은 그룹에 작업을 할당하는 데 사용됩니다.

취약성 대응 작업 공간 구성

작업 공간을 사용하려면 먼저 다음 설정 작업을 완료했는지 확인합니다.

시작하기 전에

필요한 역할: 사용자 및 그룹에 역할을 할당하고 사용자를 그룹에 할당하기 위한 관리자

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

sn_vul.vulnerability_admin을 취약성 대응 사용하여 규칙을 편집하고 생성하고 애플리케이션을 구성할 수 있습니다.

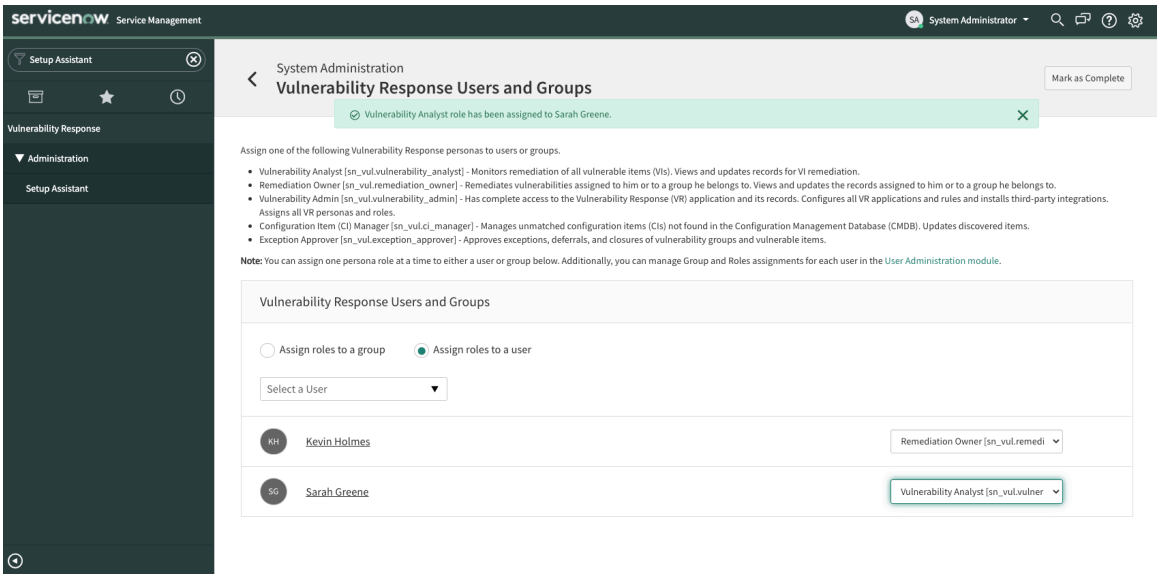
다음 설정 작업을 완료했는지 확인합니다. 이러한 작업을 수행하는 방법에 대한 자세한 내용은 목록 다음 단계를 참조하십시오.

작업	설명
☐	아직 할당되지 않은 경우 작업 공간에 액세스할 수 있도록 적절한 역할을 가진 사용자와 그룹을 할당합니다. 필요한 역할: admin. 자세한 내용은 아래 단계를 참조하십시오.
☐	취약한 항목이 정정을 위해 적절한 그룹에 할당되도록 담당 규칙을 설정합니다. 필요한 역할: sn_vul.vulnerability_admin. 담당 규칙에 대한 자세한 내용은 다음 문서를 참조하십시오 취약성 대응 할당 규칙 개요. 클래식 환경에서 담당 규칙을 만들고 편집합니다.
☐	(선택 사항): 정정 작업 규칙을 편집하거나 생성합니다. 필요한 역할: sn_vul.vulnerability_admin. 주: 기능적으로 정정 작업 규칙은 이전 버전의 취약성 대응에서 정정 작업 규칙과 동일하게 작동합니다. 그러나 정정 작업 규칙에서 자동으로 생성된 취약성 그룹과 달리 정정 작업은 정정 작업을 생성할 때 생성됩니다. 다음과 같은 옵션을 사용하여 정정 작업의 취약한 항목을 정정 작업에 번들로 묶을 수 있습니다. • 할당 그룹별 • 할당 그룹 및 구성 항목별 • 할당 그룹 및 취약성별 • 없음 - 정정 작업에 VI를 수동으로 추가하려면 이 옵션을 사용합니다. 자세한 내용은 의 정정 작업에서 요청 시 정정 작업 생성 취약성 관리자 작업 공간 문서를 참조하십시오. VI가 자동으로 그룹화되는 방법 및 클래식 환경에서 그룹 규칙이 다시 적용되는 방법에 대한 자세한 내용은 문서를 참조하십시오 취약성 대응 정정 작업 및 정정 작업 규칙 개요.
☐	정정 대상 규칙을 편집합니다. 필요한 역할: sn_vul.vulnerability_admin. 클래식 환경에서 정정 대상 규칙을 추가합니다. 정정 대상 규칙에 대한 자세한 내용은 다음 문서를 정정 대상 규칙 생성 또는 편집 취약성 대응참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 애플리케이션을 설치하고 활성화 취약성 대응 한 후 클래식 환경에서 관리자 역할의 사용자로 모두 〉 취약성 대응 〉 관리 〉 설정 도우미.



2. 설정 도우미에서 사용자를 다음 그룹에 할당합니다.

> **주:**
> 1000은 Vulnerability Response 작업 공간에서 사용자를 할당할 수 있는 사용자 그룹 수의 제한입니다.

애플리케이션과 함께 취약성 대응 제공되며 작업 공간에서 사용되는 그룹은 다음과 같습니다. 설정 도우미에서 사용자를 할당할 수 있습니다.

- 정정 소유자 - 이 그룹은 IT 정정 작업 공간의 IT 정정 소유자를 위한 그룹입니다. 이 역할이 있는 사용자는 정정 작업에서 자신에게 할당된 취약성을 수정합니다.

  > **주:**
  >
  > 정정 소유자가 IT 정정 작업 공간 및 클래식 환경에서 변경 요청을 생성하고 보고 취약한 CI(구성 항목) 데이터를 볼 수 있도록 하려면 ITIL 역할을 할당합니다. 그룹의 모든 구성원 대신 개별 사용자에게 itil 역할을 할당하는 것이 좋습니다. cmdb_read 역할은 사용자가 작업 공간에서 CI 데이터를 볼 수 있는 옵션이기도 합니다.

- v16.1부터 IT 정정 소유자에게 이메일 미리 알림을 설정할 수 있습니다. 작업 공간에 대한 이메일 알림을 설정하려면 문서를 작업 공간에서 이메일 알림 취약성 대응 설정참조하십시오.
- 취약성 관리자 - 이 그룹은 취약성 관리자용입니다. 이 역할은 설정 도우미에서 애플리케이션을 구성합니다 취약성 대응 . 이 역할에는 예외 및 긍정 오류 요청을 처리할 권한도 있습니다.
- 취약성 분석가 - 이 그룹은 취약성 관리자 작업 공간의 보안 관리자, 취약성 관리자 및 분석가를 위한 그룹입니다. 이 역할은 취약성을 모니터링하고, 주시 주제 및 정정 작업을 생성하고, 정정 진행 상황을 모니터링합니다.
- 거짓 긍정 승인자 - 이 그룹의 사용자는 취약한 항목 또는 정정 작업에 대한 가양성 요청을 처리합니다. 긍정 오류 요청에는 단일 수준 승인 프로세스가 필요합니다. 사용자 관리의 설정 도우미 외부에서 이 그룹에 대한 사용자 할당을 관리할 수 있습니다.
- 예외 승인자 - 취약한 항목 또는 정정 작업에 대한 예외 요청은 기본 2단계 승인 워크플로우를 사용하여 승인됩니다. 예외 요청에는 두 가지 수준의 승인자가 필요합니다. 두 승인 그룹

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

(예외 승인자 - 수준 1 및 예외 승인자 수준 - 2)에 사용자를 추가합니다. 요청이 수준 1 승인자에 의해 승인되면 두 번째 수준 승인자에게 전송됩니다. 사용자 관리의 설정 도우미 외부에서 이 그룹에 대한 사용자 할당을 관리합니다.

> **주:**
> 긍정 오류 및 예외 요청을 제출하기 전에 승인 그룹에 사용자를 추가합니다. 사용자에게 승인 권한을 할당하기 전에 요청을 생성하면 요청이 표시되지 않을 수 있습니다.

또는 사용자 관리 링크를 눌러 다음과 같은 세분화된 역할을 관리하고 사용자 및 기존 그룹에 할당합니다. 이러한 역할을 통해 사용자는 애플리케이션 및 작업 공간 내에서 취약성 대응 특정 작업을 수행할 수 있습니다.

- sn_vul.vulnerability_admin
- sn_vul.vulnerability_analyst
- sn_vul.remediation_owner
- IT 정정 작업 공간과 클래식 환경에서 변경 요청을 생성하고 보려면 itil 역할을 할당합니다.

사용자에게 가상 사용자 역할을 할당하고 사용자를 그룹에 할당하는 방법에 대한 자세한 내용은 을 참조하십시오 취약성 대응 가상 사용자 및 세분화된 역할설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당 .

3. 정정 작업은 생성될 때 처리를 위해 IT 정정 할당 그룹에 자동으로 전달됩니다.
   - 할당 그룹별
   - 할당 그룹 및 구성 항목별
   - 할당 그룹 및 취약성별
   - 없음 - 정정 작업에 VI를 수동으로 추가하려면 이 옵션을 사용합니다.

     > **주:**
     > 의 버전 18.0 취약성 대응에서는 없음 옵션을 사용할 수 없습니다.

   이전 버전에서 취약성 대응업그레이드하는 경우 할당 그룹은 유지됩니다. 그러나 주시 주제 및 정정 작업의 작동 방식에 익숙해질 때까지 취약한 항목이 특정 할당 그룹과 연결되도록 이러한 그룹을 편집하는 것이 좋습니다. 예를 들어 제품 또는 지역별로 할당 그룹을 만들 수 있지만 조직에 가장 적합한 조건을 사용할 수 있습니다.

   할당 규칙을 사용하여 그룹에 정정 작업을 할당할 수도 있습니다. 다음 항목에 대해 높은 우선순위 규칙만 실행하는 것을 선호할 수 있습니다.
   - 특별 처리가 필요한 항목
   - 위험이 중요하거나 VI에서 규정 준수를 통해 처리해야 하는 항목

   애플리케이션과 함께 제공되는 다음 담당 규칙은 기본적으로 활성화됩니다.
   - 폐기된 CI 할당 규칙
   - CI 지원 그룹에 할당
   - 워크스테이션 할당 규칙
   - 데이터베이스 할당 규칙
   - 웹 애플리케이션 할당 규칙
   - Windows Server 할당 규칙
   - 비 Windows Server 할당 규칙
   - 예비 연락망 할당 규칙

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

담당 규칙에 대한 자세한 내용은 다음 문서를 참조하십시오 취약성 대응 할당 규칙 개요. 클래식 환경에서 담당 규칙을 만들고 편집합니다.

4. 옵션: 정정 작업 규칙을 편집하거나 생성합니다.

   (Optional) 작업 공간에서 정정 작업은 정정 작업을 생성할 때 생성됩니다. 다음과 같은 옵션을 사용하여 정정 작업의 취약한 항목을 정정 작업에 번들로 묶을 수 있습니다.

   - 할당 그룹별
   - 할당 그룹 및 구성 항목별
   - 할당 그룹 및 취약성별
   - 없음 - 정정 작업에 VI를 수동으로 추가하려면 이 옵션을 사용합니다. 자세한 내용은 의 정정 작업에서 요청 시 정정 작업 생성 취약성 관리자 작업 공간 문서를 참조하십시오.

     주:
     의 버전 18.0취약성 대응에서는 없음 옵션을 사용할 수 없습니다.

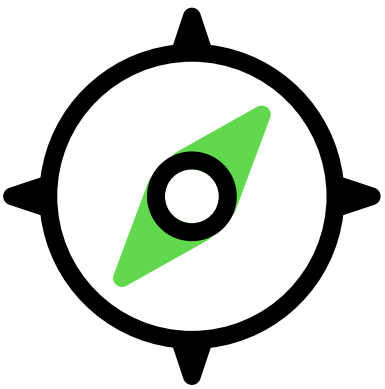
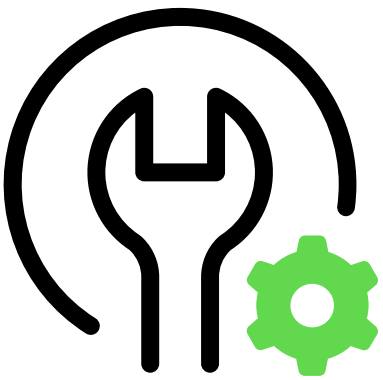
   VI가 자동으로 그룹화되는 방법 및 클래식 환경에서 그룹 규칙이 다시 적용되는 방법에 대한 자세한 내용은 문서를 참조하십시오 취약성 대응 정정 작업 및 정정 작업 규칙 개요.

취약성 관리자 작업 공간

이를 취약성 관리자 작업 공간 통해 취약성 관리자와 분석가는 가장 중요하게 여기는 취약성과 잘못된 구성을 모니터링하고 수정을 위해 IT 팀에 보낼 취약성을 전략적으로 결정할 수 있습니다.

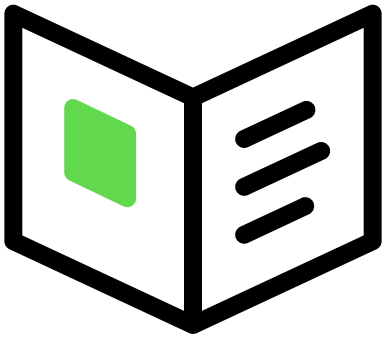
V18.0 취약성 관리자 작업 공간 데모

시작하기

탐색	모니터링 및 관리	정정
		
의 기능에 대해 알아보기 취약성 관리자 작업 공간	취약한 항목(VIT, AVIT 및 CVIT)과 테스트 결과를 모니터링하고 관리하는 방법에 대해 알아봅니다. 취약성 관리자 작업 공간	취약한 항목(VIT, AVIT 및 CVIT)을 정정하고 결과를 테스트하는 방법에 대해 알아봅니다. 취약성 관리자 작업 공간

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

참조



를 사용하는 데 필요한
추가 정보에 대해
자세히 알아보기 취약성
관리자 작업 공간

문제 해결 및 도움 받기

- Security Operations on ServiceNow 커뮤니티
- 알려진 오류 포털에서 알려진 오류 문서 검색
- 연락처 고객 서비스 및 지원

취약성 관리자 작업 공간 살펴보기

취약성 관리자와 분석가는 의 취약성 관리자 작업 공간모든 취약성 유형에 대한 통합 뷰를 얻습니다. 호스트, 애플리케이션 및 컨테이너 취약성 및 구성 문제를 확인하고, 이러한 취약성 및 잘못된 구성에 대한 주시 주제를 생성하고, 정정 작업 및 정정 작업을 생성할 수 있습니다.

주:
의 취약성 대응v19.0부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v19.0 이전 용어	용어집 **v19.0** 이상
테스트 결과 그룹	정정 작업
구성 문제	구성 테스트 결과
정책	테스트 그룹

다음으로 이동하여 볼 취약성 관리자 작업 공간 수 있습니다. 작업 공간 〉 취약성 관리자 작업 공간.

다음 취약성 관리자 작업 공간 페이지로 구성됩니다.

홈페이지

호스트 취약성, 애플리케이션 취약성, 컨테이너 취약성 및 구성 테스트 결과의 요약을 시각화하는 데 사용되는 미리 정의된 필터로 구성됩니다.

홈페이지에 대한 자세한 내용은 다음 문서를 참조하십시오 의 홈페이지 취약성 관리자 작업 공간.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
의 취약성 대응v21.0부터 감시 주제가 감시 주제 페이지에 나타납니다.

주시 주제 페이지

호스트 취약성, 애플리케이션 취약성, 컨테이너 취약성 및 구성 테스트 결과의 네 가지 모듈로 분류되는 감시 주제 목록으로 구성됩니다.

감시 주제에 대한 자세한 내용은 다음 문서를 참조하십시오 의 주시 주제 페이지 취약성 관리자 작업 공간.

대시보드 페이지

취약성 관리, 취약성 관리(PA), 취약성 승인, CISO, 컨테이너 취약성 관리 개요, 애플리케이션 취약성 관리, 통합 취약성 대응 및 상태 대시보드로 구성됩니다.

자세한 내용은 대시보드 페이지의 취약성 관리자 작업 공간 문서를 참조하십시오.

주:
대시보드 페이지는 의 버전 19.0 취약성 대응부터 나타납니다.

목록 페이지

정정 작업, 정정 작업, 호스트 취약한 항목, 애플리케이션 취약한 항목, 컨테이너 취약한 항목, 구성 테스트 결과, 예외, 승인 및 라이브러리에 대한 기본 및 사용자 지정 목록 페이지로 구성됩니다.

자세한 내용은 의 목록 페이지 취약성 관리자 작업 공간 문서를 참조하십시오.

의 홈페이지 취약성 관리자 작업 공간

의 취약성 관리자 작업 공간 홈페이지는 위험 등급, 정정 진행률, 할당 그룹에 할당, 정정 작업의 기록, 클라우드 자원의 취약성에 대한 시각화를 보여 주는 활성 기록 요약을 제공합니다.

홈 페이지에서 사전 필터링된 호스트 취약한 항목, 컨테이너 취약한 항목, 애플리케이션 취약한 항목 및 구성 테스트 결과에 대한 시각화를 볼 수 있습니다. 필터를 만들고 적용하여 원하는 기록 세트에 대한 시각화를 볼 수도 있습니다. 필터를 생성, 업데이트, 적용 및 삭제하는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 활성 기록 요약(VIT, ABIT, CVIT 및 CTR) 필터 생성 및 적용.

팁:

sn_vul_cmn_ws.navigate_to_workspace 관리자가 시스템 속성을 true로 설정한 경우 모두 메뉴의 취약한 항목, 애플리케이션 취약한 항목, 컨테이너 취약한 항목 및 테스트 결과 모듈에서 미리 정의된 필터 링크를 선택하면 이러한 링크가 의 홈페이지에서 취약성 관리자 작업 공간열리고 해당하는 저장된 필터가 자동으로 선택됩니다.

예를 들어 다음으로 이동하여 높은 위험을 선택하는 경우 모두 〉 취약성 대응 〉 취약한 항목, 이 링크는 호스트 취약성 탭에서 높은 위험 필터의 자동 선택이 있는 홈페이지 취약성 관리자 작업 공간 로 리디렉션됩니다.

홈페이지에서 다음을 수행할 수 있습니다.

- 데이터를 드릴다운하고 시각화를 클릭하여 기록 목록을 봅니다.
- 클래식 목록 보기 링크를 선택하여 클래식 UI에서 활성 기록 목록으로 이동합니다.
- 뷰 기준 드롭다운 옆에 있는 활성 기록 카운트를 선택하여 활성 기록 취약성 관리자 작업 공간 목록을 엽니다.
- 선택한 저장된 필터 새로 고침 아이콘을 선택하여 시각화를 업데이트합니다.
- 위젯의 점 3개 메뉴에서 새로 고침 옵션을 선택하여 최신 정보를 봅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

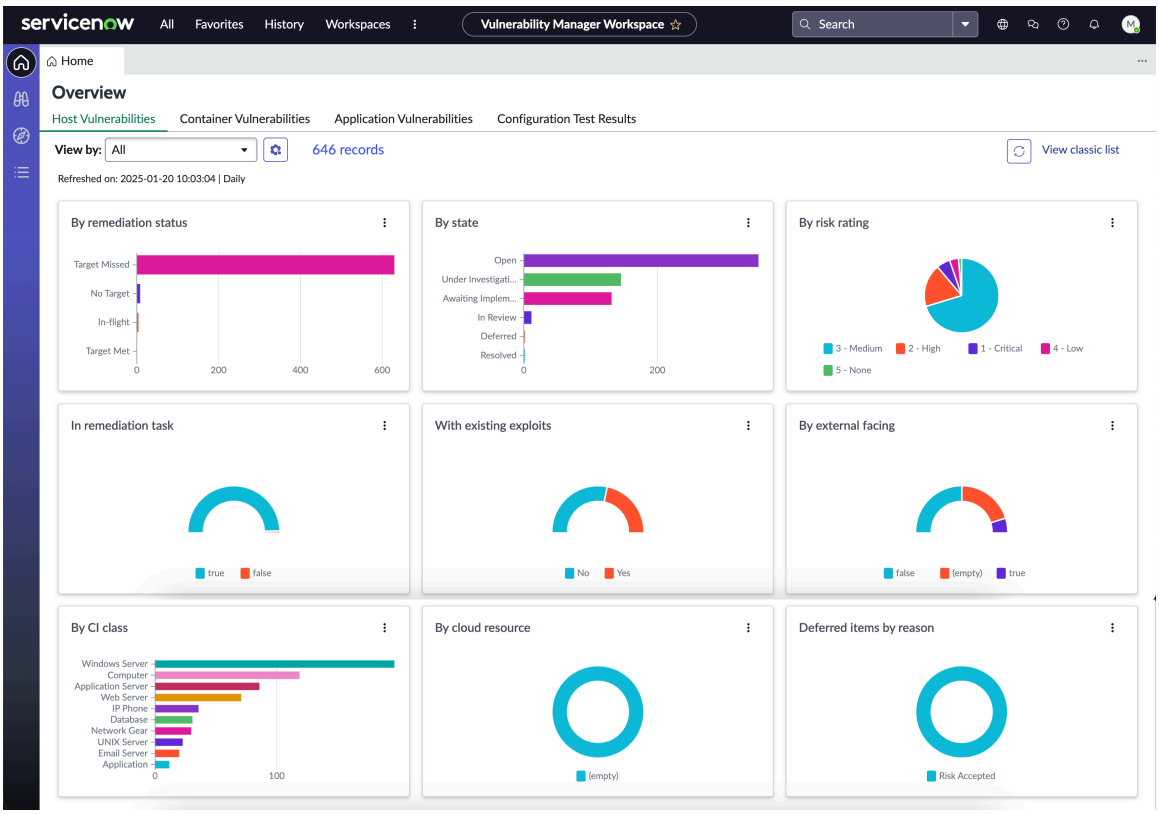
호스트 취약성

Host Vulnerabilities(호스트 취약성) 탭에는 활성 호스트 취약성에 대한 전체 요약을 제공하는 시각화가 포함되어 있습니다.

필요한 역할:

- sn_vul.vulnerability_analyst 및 sn_vul.vulnerability_admin을 사용하여 필터를 적용하여 시각화를 보고 필터를 생성합니다.
- sn_vul.read_all 필터를 적용하여 시각화를 볼 수 있는 세분화된 역할입니다.

호스트 취약성 탭



다음 표에서는 홈 페이지의 호스트 취약성 탭에 있는 시각화에 대해 설명합니다. 이러한 시각화를 선택하여 해당 기록 목록을 가져옵니다.

홈페이지의 호스트 취약성 탭에 있는 시각화

시각화	유형	설명
할당 그룹 및 정정 상태별	배포 표시줄	정정 상태별로 그룹화된 다양한 할당 그룹에 할당된 활성 기록입니다.
상태별	막대	다양한 상태(오픈, 조사 중, 구현 대기 중, 검토 중, 해결됨 및 연기됨)로 분류된 활성 기록입니다.
위험 등급별	원형 차트	위험 등급(1 - 매우 높음, 2 - 높음, 3 - 중간, 4 - 낮음, 5 - 없음)으로 분류된 활성 기록

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

홈페이지의 호스트 취약성 탭에 있는 시각화

시각화	유형	설명
정정 작업 중	반원 도넛형	정정 작업의 일부인 활성 기록과 포함되지 않은 활성 기록입니다.
기존 익스플로잇 있음	반원 도넛형	알려진 익스플로잇이 있거나 없는 활성 기록입니다.
외부 연결별	반원 도넛형	자산이 인터넷에 노출되어 분류된 활성 기록입니다.
CI 클래스별	막대	CI 클래스별로 분류된 활성 기록입니다.
클라우드 자원 기준	도넛형 차트	다양한 클라우드 자원별로 분류된 활성 기록입니다.
사유별 연기된 항목	도넛형 차트	이유별로 그룹화된 활성 지연 기록입니다.

컨테이너 취약성

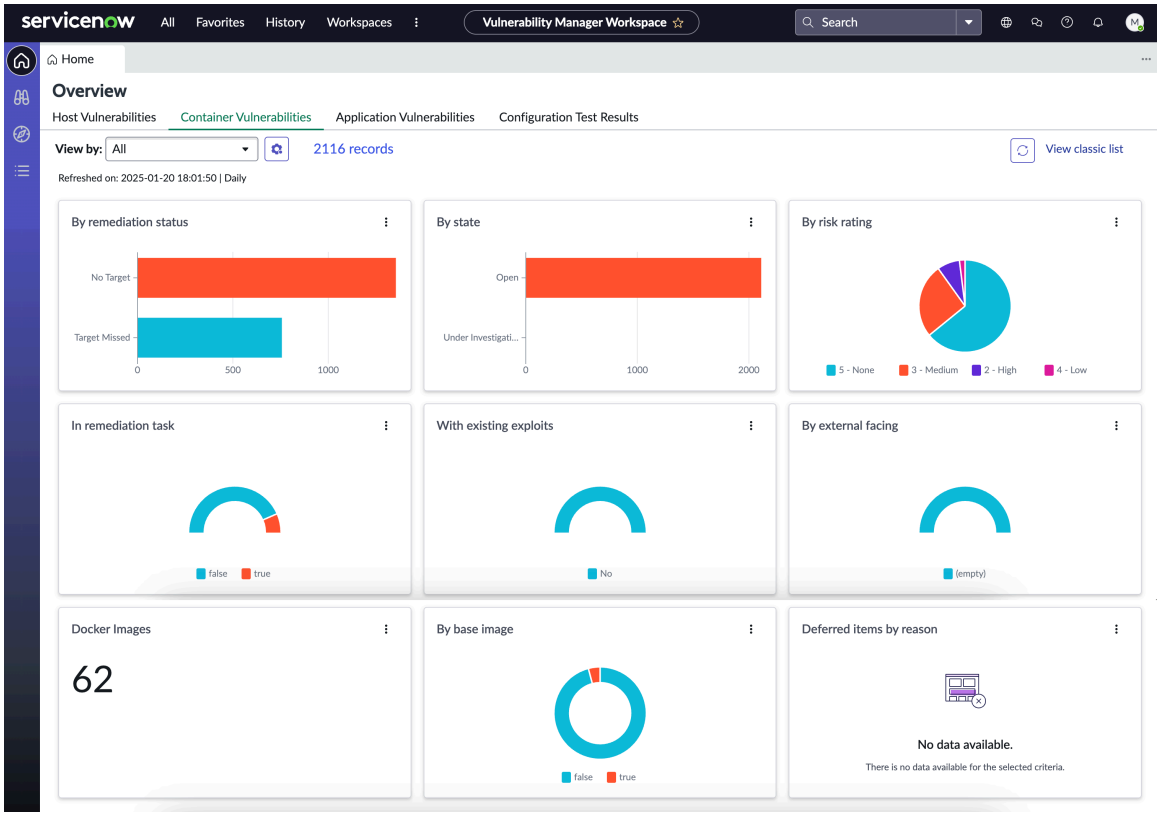
컨테이너 취약성 탭에는 활성 컨테이너 취약한 항목에 대한 전체 요약을 제공하는 시각화가 포함되어 있습니다.

필요한 역할:

- sn_vul_container.vulnerability_analyst 또는 sn_vul_container.vulnerability_admin - 필터를 적용하여 시각화를 보고 필터를 생성합니다.
- 필터를 적용하여 시각화를 볼 수 있는 sn_vul_container.read_all 세분화된 역할입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

컨테이너 취약성 탭



다음 표에서는 홈 페이지의 호스트 취약성 탭에 있는 시각화에 대해 설명합니다. 이러한 시각화를 선택하여 해당 기록 목록을 가져옵니다.

홈페이지의 컨테이너 취약성 탭에 있는 시각화

시각화	유형	설명
할당 그룹 및 정정 상태별	배포 표시줄	정정 상태별로 그룹화된 다양한 할당 그룹에 할당된 활성 기록입니다.
상태별	막대	다양한 상태(오픈, 조사 중, 구현 대기 중, 검토 중, 해결됨 및 연기됨)로 분류된 활성 기록입니다.
위험 등급별	원형 차트	위험 등급(1 - 매우 높음, 2 - 높음, 3 - 중간, 4 - 낮음, 5 - 없음)으로 분류된 활성 기록
정정 작업 중	반원 도넛형	정정 작업의 일부인 활성 기록과 포함되지 않은 활성 기록입니다.
기존 익스플로잇 있음	반원 도넛형	알려진 익스플로잇이 있거나 없는 활성 기록입니다.
외부 연결별	반원 도넛형	자산으로 분류된 활성 기록, 인터넷에 대한 노출입니다.
Docker 이미지	카운트	고유한 Docker 이미지 수입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

홈페이지의 컨테이너 취약성 탭에 있는 시각화

시각화	유형	설명
기본 이미지 기준	도넛형 차트	이미지 유형별로 분류된 활성 기록입니다.
사유별 연기된 항목	도넛형 차트	이유별로 그룹화된 활성 지연 기록입니다.

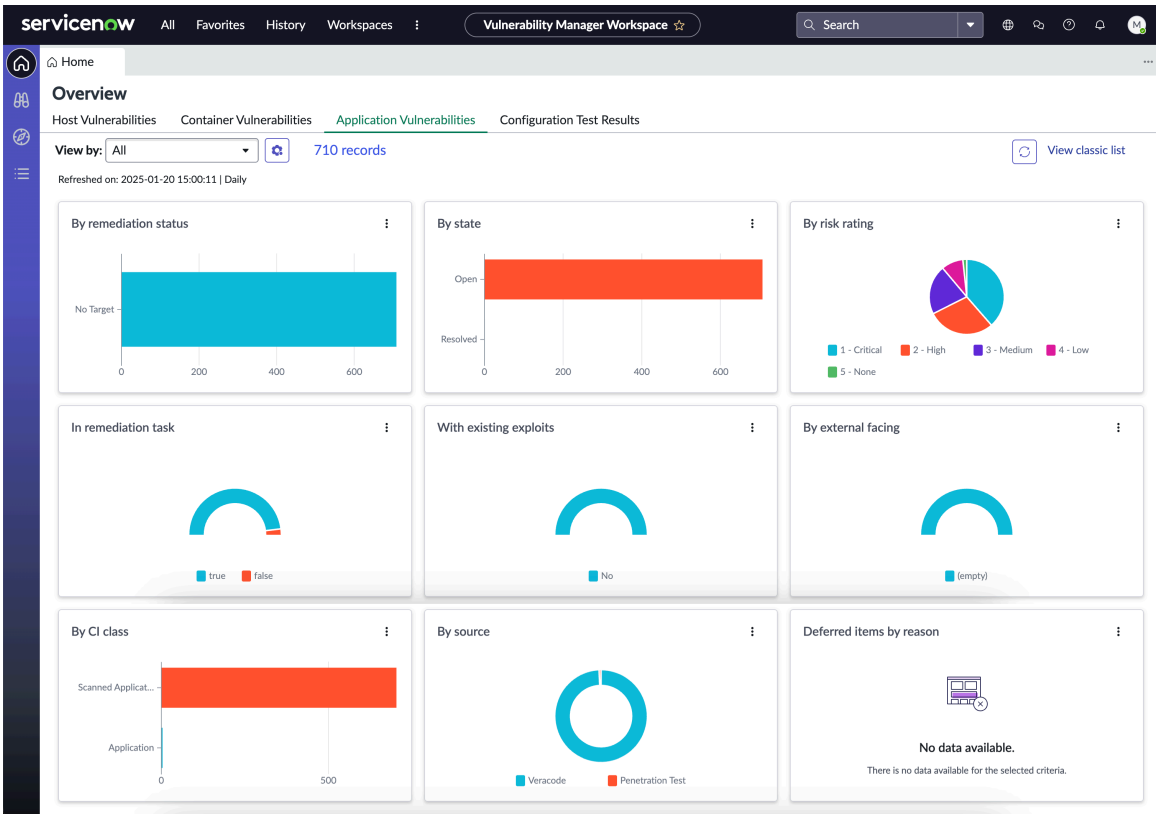
애플리케이션 취약성

애플리케이션 취약성 탭에는 애플리케이션 취약성에 대한 전반적인 요약을 제공하는 시각화가 포함되어 있습니다.

필요한 역할:

- sn_vul.app_sec_manager를 사용하여 필터를 적용하여 시각화를 보고 필터를 생성합니다.
- 필터를 적용하여 시각화를 볼 수 있는 sn_vul.app_read_all 세분화된 역할입니다.

애플리케이션 취약성 탭



다음 표에서는 홈 페이지의 호스트 취약성 탭에 있는 시각화에 대해 설명합니다. 이러한 시각화를 선택하여 해당 기록 목록을 가져옵니다.

홈페이지의 애플리케이션 취약성 탭에 있는 시각화

시각화	유형	설명
할당 그룹 및 정정 상태별	배포 표시줄	정정 상태별로 그룹화된 다양한 할당 그룹에 할당된 활성 기록입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

홈페이지의 애플리케이션 취약성 탭에 있는 시각화

시각화	유형	설명
상태별	막대	다양한 상태(오픈, 조사 중, 구현 대기 중, 검토 중, 해결됨 및 연기됨)로 분류된 활성 기록입니다.
위험 등급별	원형 차트	위험 등급(1 - 매우 높음, 2 - 높음, 3 - 중간, 4 - 낮음, 5 - 없음)으로 분류된 활성 기록
정정 작업 중	반원 도넛형	정정 작업의 일부인 활성 기록과 포함되지 않은 활성 기록입니다.
기존 익스플로잇 있음	반원 도넛형	알려진 익스플로잇이 있거나 없는 활성 기록입니다.
외부 연결별	반원 도넛형	자산이 인터넷에 노출되어 분류된 활성 기록입니다.
CI 클래스별	막대	CI 클래스별로 분류된 활성 기록입니다.
클라우드 자원 기준	도넛형 차트	다양한 클라우드 자원별로 분류된 활성 기록입니다.
사유별 연기된 항목	도넛형 차트	이유별로 그룹화된 활성 지연 기록입니다.

구성 테스트 결과

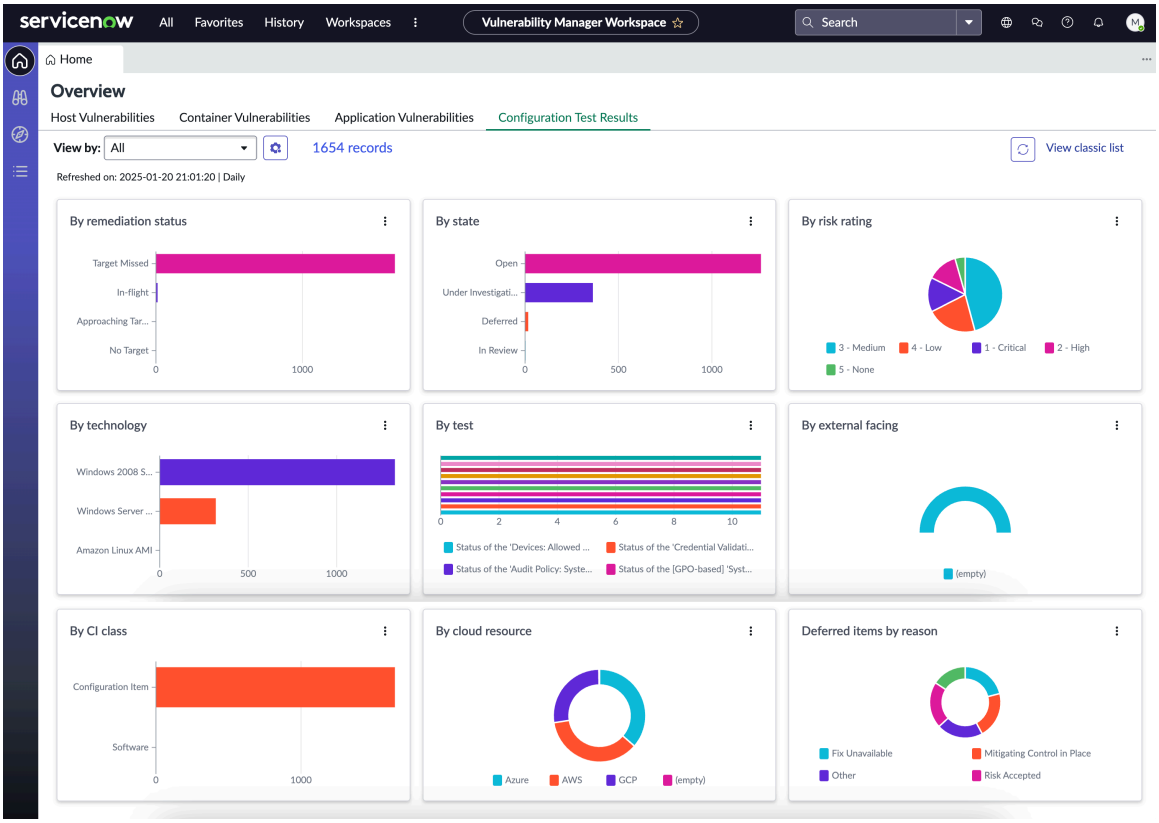
구성 테스트 결과 탭에는 조직 내 자산의 활성 상태인 잘못된 구성에 대한 전체 요약을 제공하는 시각화가 포함되어 있습니다.

필요한 역할:

- sn_vulc.admin을 사용하여 필터를 적용하여 시각화를 보고 필터를 생성합니다.
- sn_vulc.필터를 적용하여 시각화를 보려면 세분화된 역할을 읽습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

구성 테스트 결과 탭



다음 표에서는 홈 페이지의 구성 테스트 결과 탭에 있는 시각화에 대해 설명합니다. 이러한 시각화를 선택하여 해당 기록 목록을 가져옵니다.

홈페이지의 구성 테스트 결과 탭에 있는 시각화

시각화		설명
할당 그룹 및 정정 상태별	배포 표시줄	정정 상태별로 그룹화된 다양한 할당 그룹에 할당된 활성 기록입니다.
상태별	막대	다양한 상태(오픈, 조사 중, 구현 대기 중, 검토 중, 해결됨 및 연기됨)로 분류된 활성 기록입니다.
위험 등급별	원형 차트	위험 등급(1 - 매우 높음, 2 - 높음, 3 - 중간, 4 - 낮음, 5 - 없음)으로 분류된 활성 기록
기술별	막대	기술별로 분류된 활성 기록입니다.
테스트별	막대	테스트별로 분류된 활성 기록입니다.
외부 연결별	반원 도넛형	자산이 인터넷에 노출되어 분류된 활성 기록입니다.
CI 클래스별	막대	CI 클래스별로 분류된 활성 기록입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

홈페이지의 구성 테스트 결과 탭에 있는 시각화

시각화		설명
클라우드 자원 기준	도넛형 차트	다양한 클라우드 자원별로 분류된 활성 기록입니다.
사유별 연기된 항목	도넛형 차트	이유별로 그룹화된 활성 지연 기록입니다.

의 주시 주제 페이지 취약성 관리자 작업 공간

의 취약성 관리자 작업 공간 감시 주제 페이지에서는 감시 주제를 생성하고 편집할 수 있습니다. 감시 주제는 조직에서 특정 관심사 또는 우선순위를 가질 수 있는 대시보드에서 시간 경과에 따라 필터링된 기록 세트(VIT, ABIT, CVIT 및 CTR)를 모니터링할 수 있는 데이터 시각화 세트입니다.

필요한 역할:

- 호스트 취약 항목(VIT)의 경우 sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin
- 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_sec_manager
- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.vulnerability_analyst 또는 sn_vul_container.vulnerability_admin
- 구성 테스트 결과(CTR)에 대한 sn_vulc.admin

감시 주제의 데이터 시각화에 표시되는 데이터는 임포트 시 취약성 데이터가 변경되면 동적으로 업데이트됩니다. 대시보드를 사용하여 선택한 감시 주제에 대한 취약성과 구성 항목의 추세, 범위, 유형을 모니터링합니다. 이 정보는 각 감시 주제의 취약성이 환경에 미치는 영향을 확인하는 데 도움이 됩니다. 감시 주제 페이지는 호스트 취약성, 컨테이너 취약성, 애플리케이션 취약성, 구성 테스트 결과 및 비활성의 네 가지 모듈로 구성됩니다. 감시 항목의 관련 항목 탭과 시각화에 대한 자세한 내용은 문서를 참조하십시오 주시 주제의 관련 항목 목록 및 시각화.

다음 감시 주제는 감시 주제 페이지의 호스트 취약성 모듈에서 기본 시스템과 함께 제공됩니다.

- 외부 연결 자산의 취약성
- 악용이 가능한 취약성
- Windows 서버의 취약성
- LINUX 서버의 취약성
- 중요한 지연 취약성
- 정정 작업에 없는 중요한 취약성

주:
데이터 시각화에 해당 범주에 대한 기록이 없다고 표시되지만 그래프 아이콘을 클릭하면 기록 목록을 볼 수 있는 경우 표시되는 목록에서 감시 주제 이름이 있는 열을 선택합니다. 감시 주제의 열에 나열된 모든 기록(예: 인터넷 접근)의 값이 false인지 확인합니다. 이 예제의 이 값은 이 감시 주제에 대한 인터넷 연결 기록이 없음을 나타냅니다.

정정을 시작하거나 감시 주제에 있는 기록에 중요한 필요가 발생하는 경우 감시 주제에서 정정 작업을 생성할 수 있습니다. 자세한 내용은 에서 정정 작업 생성 취약성 관리자 작업 공간 문서를 참조하십시오.

관련 정보

주시 주제의 관련 항목 목록 및 시각화

의 주시 주제 사용취약성 관리자 작업 공간

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

에서 주시 주제 생성 취약성 관리자 작업 공간

에서 주시 주제를 편집하거나 삭제합니다. 취약성 관리자 작업 공간

주시 주제 비활성화 또는 활성화

주시 주제의 관련 항목 목록 및 시각화

의 취약성 관리자 작업 공간감시 주제 페이지에서 호스트 취약성, 컨테이너 취약성, 애플리케이션 취약성 및 구성 테스트 결과의 4개 모듈로 분류되는 감시 주제를 생성할 수 있습니다. 주시 주제의 관련 항목 탭은 모듈마다 다릅니다.

필요한 역할:

- 호스트 취약 항목(VIT)의 경우 sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin
- 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_sec_manager
- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.vulnerability_analyst 또는 sn_vul_container.vulnerability_admin
- 구성 테스트 결과(CTR)에 대한 sn_vulc.admin

감시 주제 페이지의 탐색 창에는 다음 모듈이 포함되어 있습니다.

- 호스트 취약성: 호스트 취약한 항목을 포함하는 감시 주제를 표시합니다.
- 컨테이너 취약성: 컨테이너 취약한 항목이 포함된 감시 주제를 표시합니다.
- 애플리케이션 취약성: 애플리케이션 취약한 항목이 포함된 감시 주제를 표시합니다.
- 구성 테스트 결과: 구성 항목이 포함된 주시 주제를 표시합니다.
- 비활성: 4개 모듈 모두에서 비활성 감시 주제를 표시합니다.

다음 테이블에는 다양한 감시 주제 모듈에 사용할 수 있는 관련 항목 탭이 나와 있습니다.

주시 주제 및 관련 항목

주시 주제	관련 항목 탭
호스트 취약성	개요, 영향을 받는 CI, 구별되는 취약성 및 취약한 항목
컨테이너 취약성	개요, 영향을 받는 CI, 구별되는 취약성 및 취약한 항목
애플리케이션 취약성	개요 및 취약한 항목
구성 테스트 결과	개요, 영향을 받는 CI, 고유한 구성 테스트 및 구성 테스트 결과

다음 테이블에서는 감시 항목의 관련 항목 탭과 시각화에 대한 설명을 제공합니다.

감시 주제의 관련 항목 탭 및 시각화

관련 항목 탭 및 시각화	설명
개요	
시간 경과에 따른 활성 취약한 항목	시간 경과에 따른 활성 취약한 항목(VI)의 수입니다. 지난 30일 동안의 이 데이터의 추세를 모니터링할 수 있습니다. 자산 범주 필터를 사용하여 데이터를 필터링할 수도 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

감시 주제의 관련 항목 탭 및 시각화

관련 항목 탭 및 시각화	설명
VI 정정 작업 중	이미 활성 정정 작업에 있는 총 VI 수 중 활성 VI 수입니다.
활성 정정 작업	활성 상태의 정정 작업 목록입니다.
영향을 받는 **CI**	
고유 CI	이러한 취약성의 영향을 받는 구성 항목 (CI) (자산) 수입니다.
CI 클래스당 VI	각 구성 관리 데이터베이스(CMDB) CI 클래스의 VI(취약한 항목) 수입니다. 주: 이 위젯은 호스트, 애플리케이션 및 컨테이너 취약성 모듈의 감시 주제에 대해서만 나타납니다.
CI 클래스별 구성 문제	각 구성 관리 데이터베이스(CMDB) CI 클래스의 CI 수입니다. 주: 이 위젯은 구성 문제 모듈의 감시 주제에 대해서만 나타납니다.
인터넷 연결 VI	인터넷에 노출된 자산의 총 VI 수 중 활성 VI 수입니다. 주: 이 위젯은 호스트, 애플리케이션 및 컨테이너 취약성 모듈의 감시 주제에 대해서만 나타납니다.
인터넷 연결 구성 문제	인터넷에 노출된 자산의 총 CI 수 중 활성 CI 수입니다. 주: 이 위젯은 구성 문제 모듈의 감시 주제에 대해서만 나타납니다.
구별되는 취약성	
기존 익스플로잇이 포함된 VI	알려진 익스플로잇이 있는 활성 VI입니다.
구별되는 취약성	자산과 연결된 고유한 개별 취약성 수입니다. 문제 유형을 기준으로 구별되는 취약성을 필터링할 수 있습니다.
PCI 취약성이 있는 VI	PCI(지불 카드 산업) 취약성이 있는 활성 VI가 있는 고유한 개별 자산 수입니다.
취약한 항목	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

감시 주제의 관련 항목 탭 및 시각화

관련 항목 탭 및 시각화	설명
호스트 취약한 항목	모든 호스트 취약한 항목의 목록입니다. 보려는 기록만 표시되도록 이 목록을 필터링할 수 있습니다. 주: 이 목록은 호스트 취약성 모듈의 감시 주제에 대해서만 나타납니다.
애플리케이션 취약한 항목	모든 애플리케이션 취약한 항목의 목록입니다. 보려는 기록만 표시되도록 이 목록을 필터링할 수 있습니다. 주: 이 목록은 애플리케이션 취약성 모듈의 감시 주제에 대해서만 나타납니다.
컨테이너 취약한 항목	모든 컨테이너 취약한 항목의 목록입니다. 이 목록을 필터링하여 표시하면 원하는 기록만 표시되도록 할 수 있습니다. 주: 이 목록은 컨테이너 취약성 모듈의 주시 주제에만 표시됩니다.
구성 테스트 결과 모듈 아래 주시 주제의 개요 탭	
시간 경과에 따른 활성 구성 테스트 결과	시간 경과에 따른 활성 구성 테스트 결과 수입니다. 지난 30일 동안의 이 데이터의 추세를 모니터링할 수 있습니다.
정정 작업의 구성 테스트 결과	이미 활성 정정 작업에 있는 총 기록 수 중에서 활성 구성 테스트 결과의 수입니다.
활성 정정 작업	활성 상태의 정정 작업 목록입니다.
구성 테스트 결과 모듈 아래 주시 주제의 구별되는 구성 테스트 탭	
테스트 중요도를 통한 구성 테스트 결과	문제의 중요도를 기반으로 하는 구성 테스트 결과입니다.
구별되는 구성 테스트	고유한 구성 테스트 수.
구성 테스트 결과 모듈 아래 주시 주제의 구성 테스트 결과 탭	구성 테스트 결과 목록입니다.

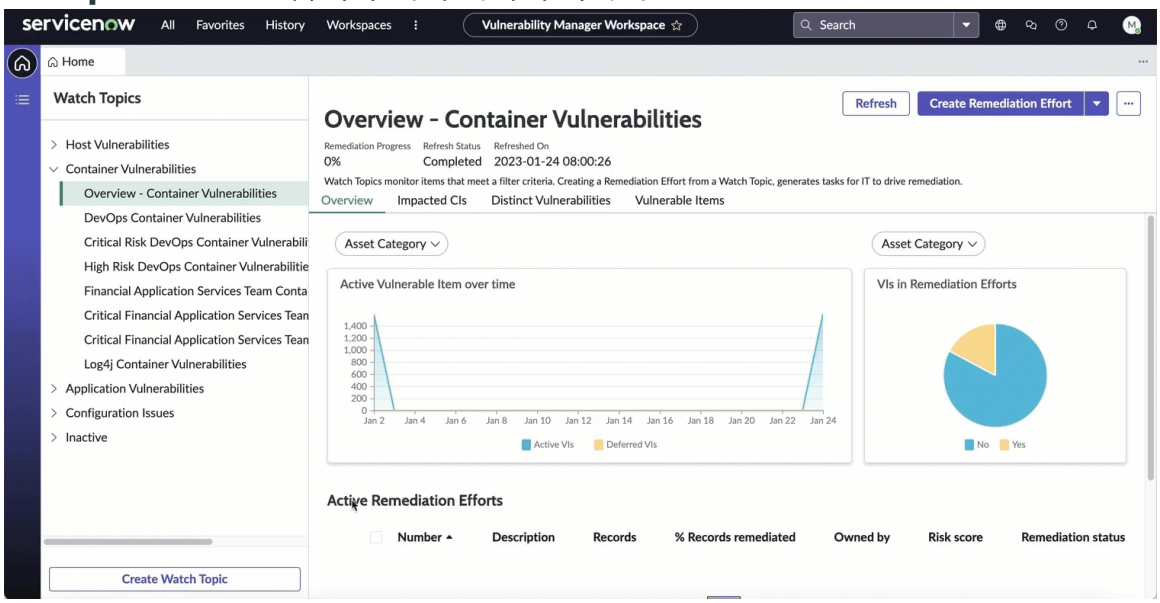
새로 고침 버튼을 선택하여 주시 주제의 최신 세부 정보를 가져올 수 있습니다. 최신 새로 고침 상태 및 타임스탬프가 감시 주제 이름 아래에 표시됩니다. 감시 주제를 새로 고치면 차트 및 정정 작업을 포함하여 감시 주제의 모든 상세 정보가 업데이트됩니다. 감시 주제는 생성되거나 업데이트될 때 자동으로 새로 고침됩니다.

주:
비활성 감시 주제는 새로 고칠 수 없으므로 비활성 감시 주제에 대해 새로 고침 버튼이 비활성화됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

기록에 대한 추가 정보를 보려면 위젯의 데이터 그림을 클릭합니다.

Example: 버전 **18.0** 감시 주제의 데이터 시각화



의 정정 작업 취약성 관리자 작업 공간

정정 작업은 감시 주제와 연결된 기록 세트입니다. 정정 작업에 나열된 기록은 정적입니다. 새 임포트 데이터 또는 주시 주제에 대한 변경 내용으로 업데이트되지 않습니다.

필요한 역할:

- 호스트 취약 항목(VIT)의 경우 sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin
- 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_sec_manager
- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.vulnerability_analyst 또는 sn_vul_container.vulnerability_admin
- 구성 테스트 결과(CTR)에 대한 sn_vulc.admin

목록 페이지의 정정 작업 목록에서 활성을 선택한 상태에서 정정 작업 링크를 클릭하여 엽니다. 정정 작업을 호스트 취약한 항목(VIT), 애플리케이션 취약한 항목(AVIT), 컨테이너 취약한 항목(CVIT) 및 구성 테스트 결과(CTR)로 분류하려면 기록 유형 열에서 점 3개 메뉴를 선택한 다음 기록 유형별 그룹화를 선택합니다.

정정 작업 기록의 관련 목록 항목을 사용하면 연결된 기록의 전반적인 정정 진행률과 상태를 볼 수 있습니다.

- 개요 탭에서 이 정정 작업과 관련되어 시간이 지남에 따라 종결된 기록을 모니터링합니다. 기록 오른쪽에 있는 그래프의 필터 아이콘을 클릭하여 데이터 시각화에 적용된 필터를 봅니다.
- 상세 정보 탭에서 관련 주시 주제 및 상태(활성 또는 비활성)를 포함하여 정정 작업에 대한 상세 정보를 봅니다. 이 페이지에서 정정 작업을 비활성화할 수 있습니다. 모든 기록이 종결되기 전에 정정 작업량을 비활성화하면 새 정정 작업에 추가할 수 있는 활성 기록이 됩니다.
- 정정 작업 탭에서 이 정정 작업과 연결된 정정 작업을 봅니다. 이 작업과 관련되어 정정된 기록의 백분율을 봅니다.
- 취약한 항목 탭에서 이 정정 작업과 연결된 기록을 봅니다. 정정 작업의 모든 기록이 완료되고 닫히면 정정 작업이 비활성으로 전환됩니다. 정정 작업이 비활성 상태이면 정정 작업과 연결된 모든 종결된 기록을 새 정정 작업에 추가할 수 없습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

> **주:**
> 취약한 항목 탭은 호스트 취약성, 애플리케이션 취약성 및 컨테이너 취약성 모듈의 감시 주제와 연결된 정정 작업에 대해 나타납니다.

- 구성 테스트 결과 탭에서 정정 작업과 연결된 구성 테스트 결과를 봅니다. 정정 작업의 모든 기록이 완료되고 닫히면 정정 작업이 비활성으로 전환됩니다. 정정 작업이 비활성 상태이면 정정 작업과 연결된 모든 종결된 기록을 새 정정 작업에 추가할 수 없습니다.

> **주:**
> 구성 테스트 결과 탭은 구성 테스트 결과 모듈의 감시 주제와 연결된 정정 작업에 대해 나타납니다.

정정 작업에서 수행할 수 있는 UI 작업 및 자세한 내용은 문서를 참조하십시오 정정 작업 기록 사용.

관련 정보

취약성 대응 작업 공간의 정정 작업, 정정 작업 및 기록의 수명주기

에서 정정 작업 생성 취약성 관리자 작업 공간

의 정정 작업에서 요청 시 정정 작업 생성 취약성 관리자 작업 공간

에서 반복 정정 작업 생성 취약성 관리자 작업 공간

의 정정 작업으로 기록 전송 취약성 관리자 작업 공간

취약성 대응 작업 공간의 정정 작업, 정정 작업 및 기록의 수명주기

기록이 연기, 해결, 재개되고 다른 RE(정정 작업)로 이전되면 기록 상태 및 관련 RT(정정 작업)가 영향을 받습니다.

필요한 역할:

- 호스트 취약 항목(VIT)의 경우 sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin
- 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_sec_manager
- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.vulnerability_analyst 또는 sn_vul_container.vulnerability_admin
- 구성 테스트 결과(CTR)에 대한 sn_vulc.admin

정정 작업 생성

정정 작업, 정정 작업 및 기록의 상태와 수명주기가 영향을 받는 방식은 정정 작업이 생성되는 방식, 생성 시기 및 비활성화 여부에 따라 달라집니다.

감시 주제의 오른쪽 상단 목록에서 정 정 작업량 생성 또는 반복 작업량 생성을 클릭하여 정정 작업량을 생성할 수 있습니다. 감시 주제당 하나의 반복 정정 작업을 생성할 수 있습니다. 반복 정정 작업을 생성하면 설정한 기준에 따라 연결된 감시 주제에 대한 후속 정정 작업이 자동으로 생성됩니다. 두 경우 모두:

- 수정을 용이하게 하기 위해 활성 기록만 정정 작업에 추가됩니다.
- 새 정정 작업의 모든 기록은 새 정정 작업에 배치됩니다. 기록은 여러 정정 작업에 존재할 수 있지만 하나의 기록만 정정 작업과 연결할 수 있습니다.

> **주:**
> 활성 기록이 없는 경우 정정 작업이 자동으로 비활성화됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

기록 이전 또는 기록 이월

다른 활성 정정 작업에서 일치하는 기록 전송 확인란을 선택하여 정정 작업을 생성할 때 한 정정 작업에서 다른 정정 작업으로 기록을 이전할 수 있습니다. 기록을 전송하는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 의 정정 작업으로 기록 전송 취약성 관리자 작업 공간. 기록이 정정 작업에서 이전되거나 반복적인 정정 작업으로 이월되는 경우:

동일한 감시 주제의 새로운 정정 노력으로

- 이전 정정 작업의 모든 정정 작업이 새 정정 작업으로 이동됩니다.
- 이전에는 정정 작업의 일부가 아니었던 기록에 대해 선택한 그룹화 기준에 따라 새 정정 작업이 생성됩니다.
- 이전 정정 작업이 비활성화됩니다.

다른 감시 주제의 새로운 정정 노력으로

이전 정정 작업의 모든 기록이 새 정정 작업으로 이동되고 선택한 그룹화 기준에 따라 정정 작업이 생성됩니다.

- 이전 정정 작업과 연결된 정정 작업의 모든 기록이 이전되면 이러한 정정 작업이 종결-취소됩니다.
- 기록의 하위 세트만 전송되면 이전 정정 작업과 연결된 정정 작업이 분할되어 활성 상태로 유지됩니다.

이전 정정 작업과 연결된 종결된 정정 작업은 영향을 받지 않습니다.

주:
반복되는 정정 작업의 기록을 새 정정 작업으로 이전할 수 없습니다. 그러나 기존의 반복되지 않는 정정 작업에서 새 정정 작업으로 기록을 이전할 수 있습니다. 기록 이전에 대한 자세한 내용은 을 참조하십시오 의 정정 작업으로 기록 전송 취약성 관리자 작업 공간 .

대시보드 페이지의 취약성 관리자 작업 공간

의 대시보드 페이지에서 취약성 관리자 작업 공간UI로 넥스트 경험 대시보드를 볼 수 있으며 이러한 대시보드를 사용하여 취약성을 추적하고 분석할 수 있습니다.

필요한 역할:

- 호스트 취약 항목(VIT)의 경우 sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin
- 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_sec_manager
- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.vulnerability_analyst 또는 sn_vul_container.vulnerability_admin
- 구성 테스트 결과(CTR)에 대한 sn_vulc.admin

다음으로 이동하여 대시보드 취약성 관리자 작업 공간 에 액세스합니다. 작업 공간 〉 취약성 관리자 작업 공간 을 클릭하고 대시보드 아이콘을 선택합니다. 역할에 따라 기본 대시보드가 표시됩니다.

다음 테이블에는 특정 역할에 대해 표시되는 기본 대시보드가 나와 있습니다.

기본 대시보드

기본 대시보드	역할
통합 대시보드	sn_vul_cmn_vulnerability_admin 또는 sn_vul_cmn_vulnerability_analyst

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

기본 대시보드

기본 대시보드	역할
취약성 PA 대시보드	sn_vul_vulnerability_admin 또는 sn_vul_vulnerability_analyst
애플리케이션 개요	sn_vul_app_sec_manager
컨테이너 개요	sn_vul_container_vulnerability_admin 또는 sn_vul_container_analyst

대시보드 페이지의 드롭다운에서 선택하여 수행하려는 작업에 대한 다음 대시보드를 볼 수 있습니다.

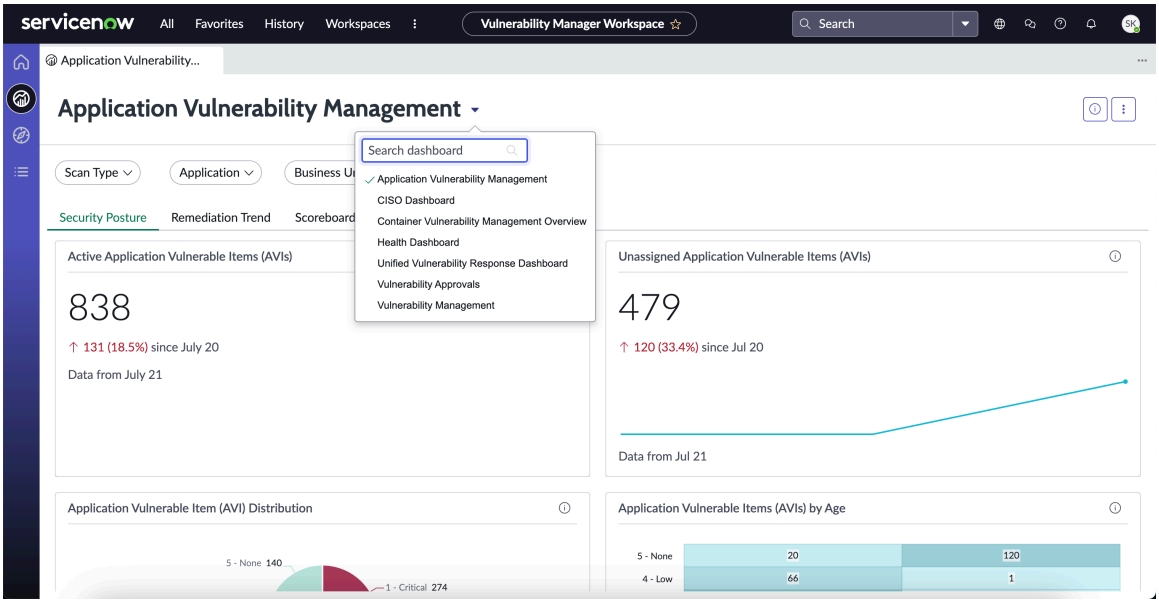
의 대시보드 취약성 관리자 작업 공간

대시보드	설명
취약성 관리(PA)	초기 분석 및 탐지부터 억제 또는 정정에 이르기까지 호스트 취약성의 볼륨, 성능 및 진행 상황을 추적합니다. 자세한 내용은 취약성 관리(PA) 대시보드 문서를 참조하십시오.
취약성 승인	승인, 거부 및 보류 중인 승인 요청 수를 봅니다. 자세한 내용은 기본 취약성 대응 대시보드 사용 문서를 참조하십시오.
CISO 대시보드	보안 취약성 및 인시던트를 포함하여 조직의 전반적인 보안 태세를 드러냅니다. 자세한 내용은 취약성 관리 CISO 대시보드 문서를 참조하십시오.
컨테이너 취약성 관리 개요	초기 분석 및 탐지부터 억제 또는 정정에 이르기까지 컨테이너 취약성의 볼륨, 성능 및 진행 상황을 추적합니다. 자세한 내용은 컨테이너 취약성 대응 대시보드 문서를 참조하십시오.
애플리케이션 취약성 관리 대시보드	초기 분석 및 탐지부터 억제 또는 정정에 이르기까지 애플리케이션 취약성의 볼륨, 성능 및 진행 상황을 추적합니다. 자세한 내용은 애플리케이션 취약성 관리 (PA) 대시보드 문서를 참조하십시오.
통합 취약성 대응 대시보드	여러 취약성 스캐너 및 보안 도구의 가시성을 제공하여 조직의 취약성과 위험에 대한 포괄적인 뷰를 제공합니다. 자세한 내용은 통합 취약성 대응 대시보드에 대한 분석 및 보고 솔루션 문서를 참조하십시오.
Vulnerability Response 상태 대시보드	취약성 대응 애플리케이션의 전체 상태 점수를 표시합니다. 자세한 내용은 SecOps Vulnerability Response 상태 대시보드 문서를 참조하십시오.

다음 이미지는 의 취약성 관리자 작업 공간대시보드 페이지를 보여줍니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

버전 **19.0** 대시보드의 취약성 관리자 작업 공간



추가 옵션 아이콘 ⋮ 선택한 다음 새 대시보드 만들기를 선택하여 사용자 지정 대시보드를 만들 수도 있습니다.

의 목록 페이지 취약성 관리자 작업 공간

취약성 및 보안 관리자와 분석가는 목록 페이지에서 취약성 관리자 작업 공간 기록의 정정 진행 상황을 보고, 기록을 드릴다운하고, 승인 요청 및 예외의 상태를 볼 수 있습니다.

필요한 역할:

- 호스트 취약 항목(VIT)의 경우 sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin
- 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_sec_manager
- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.vulnerability_analyst 또는 sn_vul_container.vulnerability_admin
- 구성 테스트 결과(CTR)에 대한 sn_vulc.admin

이러한 목록과 링크를 통해 기록과 작업에 쉽게 액세스할 수 있습니다. 여기에는 두 개의 탭이 있습니다.

- 목록 탭: 정정 작업, 정정 작업, 취약한 항목, 구성 테스트 결과, 솔루션, 예외 및 라이브러리에 대한 기본 목록을 표시합니다.
- 내 목록 탭: 목록 탭에서 이름을 변경한 목록과 생성한 모든 목록을 표시합니다.

  정정 진행률을 모니터링하기 위해 고유한 목록을 만들 수도 있습니다. 자세한 내용은 사용자 지정 기록 목록 만들기 문서를 참조하십시오.

목록 탭

다음 테이블에는 목록 페이지의 목록 탭에서 사용할 수 있는 목록이 나와 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

팁:

sn_vul_cmn_ws.navigate_to_workspace 관리자가 시스템 속성을 true로 설정한 경우 모두 메뉴에서 취약성 대응, 애플리케이션 취약성 대응, 컨테이너 취약성 대응 및 구성 준수 모듈에 있는 미리 정의된 필터 링크를 선택하면 이러한 링크가 역할에 따라 목록 페이지에서 취약성 관리자 작업 공간 열립니다.

예를 들어, 다음으로 이동하여 내 그룹에 할당 됨을 선택하는 경우 모두 〉 취약성 대응 〉 정정 작업 〉 사용자 그룹에 할당됨, 이 링크는 로 리디렉션됩니다 취약성 관리자 작업 공간. 취약성 관리자 또는 분석가 역할이 있는 경우 정정 작업 모듈의 내 그룹에 할당됨 목록이 취약성 관리자 작업 공간의 목록 페이지에서 열립니다. 호스트 업데이트 적용 작업을 보려면 기록 유형별로 작업을 그룹화합니다.

시스템 속성을 사용하여 목록에서 기록 수를 숨길 수 있습니다 *glide.ui.list.seismic.omit.count* . 목록에서 기록 카운트를 해제/설정하는 방법에 대한 자세한 내용은 KBB0010402 KB 문서를 참조하십시오.

목록

목록 항목	설명	모듈	필요한 역할
정정 작업(RE)	할당 그룹에 할당된 활성 RE 및 모든 RE의 목록입니다. 정정 작업을 기록 유형 별로 그룹화하여 호스트 취약한 항목, 애플리케이션 취약한 항목, 컨테이너 취약한 항목 및 구성 테스트 결과별로 분류합니다.	취약성 대응, 애플리케이션 취약성 대응, 컨테이너 취약성 대응및 구성 준수	• 호스트 취약 항목(VIT)의 경우 sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin • 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_sec_manager • 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.vulnerability_analy 또는 sn_vul_container.vulnerability_admi • 구성 테스트 결과(CTR)에 대한 sn_vulc.admin
정정 작업	다음 목록이 포함되어 있습니다. • 활성: 모든 활성 호스트, 애플리케이션, 컨테이너 및 테스트 결과 정정 작업의 목록입니다. • 모두: 활성 및 비활성 호스트, 애플리케이션, 컨테이너 및 테스트	취약성 대응, 애플리케이션 취약성 대응, 컨테이너 취약성 대응및 구성 준수	• 호스트 취약 항목(VIT)의 경우 sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin • 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_sec_manager • 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.vulnerability_analy

기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

목록

목록 항목	설명	모듈	필요한 역할
	결과 정정 작업의 목록입니다. • 나에게 할당됨: 정정을 위해 사용자에게 할당된 정정 작업 목록입니다. • 내 그룹에 할당: 정정을 위해 할당 그룹에 할당된 정정 작업입니다. 정정 작업을 기록 유형 별로 그룹화하여 호스트 취약한 항목, 애플리케이션 취약한 항목, 컨테이너 취약한 항목 및 구성 테스트 결과별로 분류합니다. 주: 정정 작업 목록에는 에서 정정 작업을 생성하는 취약성 관리자 작업 공간동안 생성된 작업과 클래식 UI에서 정정 작업 규칙 및 기타 프로세스에 의해 수동으로 생성된 작업이 포함됩니다. 정정 작업의 일부로 생성되지 않은 모든 정정 작업에 대해 정정 작업 열이 비어 있습니다.		또는 sn_vul_container.vulnerability_admin • 구성 테스트 결과(CTR)에 대한 sn_vulc.admin
호스트 취약한 항목	다음 목록이 포함되어 있습니다 • 활성: 모든 활성 호스트 취약한 항목의 목록입니다. • 모두: 활성 및 비활성 호스트 취약한 항목의 목록입니다.	취약성 대응	sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

목록

목록 항목	설명	모듈	필요한 역할
	• 나에게 할당됨: 정정을 위해 사용자에게 할당된 호스트 취약한 항목 목록입니다. • 내 그룹에 할당됨: 정정을 위해 할당 그룹에 할당된 호스트 취약한 항목의 목록입니다.		
애플리케이션 취약한 항목	다음 목록이 포함되어 있습니다. • 활성: 모든 활성 애플리케이션 취약한 항목의 목록입니다. • 모두: 활성 및 비활성 애플리케이션 취약한 항목의 목록입니다. • 나에게 할당됨: 정정을 위해 사용자에게 할당된 애플리케이션 취약한 항목 목록입니다. • 내 그룹에 할당됨: 정정을 위해 할당 그룹에 할당된 애플리케이션 취약한 항목의 목록입니다. 새로 만들기 버튼을 선택하여 새 애플리케이션 취약한 항목을 만들 수 있습니다.	애플리케이션 취약성 대응	sn_vul.app_sec_manager
컨테이너 취약한 항목	다음 목록이 포함되어 있습니다. • 활성: 모든 활성 컨테이너 취약한 항목의 목록입니다. • 모두: 활성 및 비활성 컨테이너 취약한 항목의 목록입니다. • 나에게 할당됨: 정정을 위해 사용자에게 할당된	컨테이너 취약성 대응	sn_vul_container.vulnerability_analyst 또는 sn_vul_container.vulnerability_admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

목록

목록 항목	설명	모듈	필요한 역할
	컨테이너 취약한 항목 목록입니다. • 내 그룹에 할당됨: 정정을 위해 할당 그룹에 할당된 컨테이너 취약한 항목 목록입니다.		
구성 테스트 결과	다음 목록이 포함되어 있습니다. • 활성: 모든 활성 테스트 결과의 목록입니다. • 모두: 활성 및 비활성 테스트 결과의 목록입니다. • 나에게 할당됨: 정정을 위해 사용자에게 할당된 테스트 결과 목록입니다. • 내 그룹에 할당: 정정을 위해 할당 그룹에 할당된 테스트 결과 목록입니다.	구성 준수	sn_vulc.admin
솔루션	다음 목록이 포함되어 있습니다. • 모두 - 호스트 취약한 항목을 정정하는 데 사용할 수 있는 모든 사용 가능한 솔루션을 표시합니다. • 가장 높은 대체 - 기본 솔루션을 채우는 데 사용되는 모든 솔루션을 표시합니다. • 취약한 항목 포함 - 취약한 항목에서 기본 솔루션으로 사용되고 있는 솔루션을 표시합니다.	취약성 대응	sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

목록

목록 항목	설명	모듈	필요한 역할
예외	할당 그룹과 연결된 모든 예외 요청 및 긍정 오류 요청에 대한 승인 상태를 표시합니다. • 모두: VIT, AVIT 및 CVIT와 관련된 예외, 가양성 및 할당 해제 승인 요청 및 해당 정정 작업(VUL, AVUL 및 CVUL)의 목록입니다. • 모두(구성 준수): 예외, 가양성 및 할당 해제 승인 요청 관련 테스트 결과 및 정정 작업(CTR#)의 목록입니다. 예외를 기록 유형별로 그룹화하여 호스트 취약한 항목, 애플리케이션 취약한 항목, 컨테이너 취약한 항목 및 구성 테스트 결과별로 분류합니다.	취약성 대응, 애플리케이션 취약성 대응, 컨테이너 취약성 대응및 구성 준수	• 호스트 취약 항목(VIT)의 경우 sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin • 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_sec_manager • 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.vulnerability_analy 또는 sn_vul_container.vulnerability_admi • 구성 테스트 결과(CTR)에 대한 sn_vulc.admin
승인	나에게 할당됨: 처리를 위해 사용자에게 할당된 승인 요청을 표시합니다. 작업 공간에서 승인을 처리하려면 다음 문서를 참조하십시오 에서 요청 승인 또는 거부 취약성 관리자 작업 공간.	취약성 대응, 애플리케이션 취약성 대응, 컨테이너 취약성 대응및 구성 준수	• 호스트 취약 항목(VIT)의 경우 sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin • 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_sec_manager • 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.vulnerability_analy 또는 sn_vul_container.vulnerability_admi • 구성 테스트 결과(CTR)에 대한 sn_vulc.admin
라이브러리	는 다음 목록으로 구성됩니다. • CVE(NVD) - , 애플리케이션 취약성 대응, 컨테이너	취약성 대응, 애플리케이션 취약성 대응, 컨테이너 취약성 대응및 구성 준수	• 호스트 취약 항목(VIT)의 경우 sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

목록

목록 항목	설명	모듈	필요한 역할
	취약성 대응의 모든 CVE(Common Vulnerability and Exposures)취약성 대응의 목록입니다. • TPE - 인스턴스에 임포트한 외부 공급업체 취약성의 목록입니다. 관련 참조, 취약한 항목, 익스플로잇 및 CVE 목록을 포함합니다. • CWE - , 애플리케이션 취약성 대응, 및 컨테이너 취약성 대응의 모든 CWE(일반적인 약점 열거형) 취약성 대응목록입니다. • 앱 취약성 - 모든 외부 공급업체 애플리케이션 취약성 항목의 목록입니다. • 테스트 그룹 - 모든 구성 준수 테스트 그룹의 목록입니다. 기록 뷰에서 테스트 그룹에 대한 CI 준수 및 테스트 결과 준수 백분율을 볼 수 있습니다. • 테스트 - 의 구성 준수모든 테스트 목록입니다. 기록 뷰에서 테스트의 테스트 결과 준수 백분율을 볼 수 있습니다. • 보상 통제 - 위험 감소 요청에 사용할 수 있는 모든 보상 통제 목록입니다. 새로 만들기를 클릭하여 보상 컨트롤을 추가할 수 있습니다. 보정 컨트롤을 추가하는 방법에 대한 자세한 내용은		• 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_sec_manager • 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.vulnerability_analy 또는 sn_vul_container.vulnerability_admin • 구성 테스트 결과(CTR)에 대한 sn_vulc.admin

기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

목록

목록 항목	설명	모듈	필요한 역할
	을 참조하십시오 라이브러리에 보정 통제 추가.		
CMDB	다음 목록이 포함되어 있습니다 • 검색된 항목: 검색된 모든 항목의 목록입니다. • 검색된 컨테이너 이미지: 컨테이너 이미지의 목록입니다. 이러한 컨테이너 이미지는 계층 정보와 함께 이미지 ID, Docker 이미지 및 이미지 리포지토리에 대한 정보를 제공합니다. • 취약성 관리자 작업 공간 뷰에 추가된 검색된 애플리케이션 테이블입니다. 작업 공간에서 선택하거나 필터링된 검색된 항목 또는 애플리케이션에 다시 적용할 수 있습니다.	취약성 대응, 애플리케이션 취약성 대응, 컨테이너 취약성 대응및 구성 준수	• 호스트 취약 항목(VIT)의 경우 sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin • 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_sec_manager • 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.vulnerability_analy 또는 sn_vul_container.vulnerability_admin • 구성 테스트 결과(CTR)에 대한 sn_vulc.admin
침투 테스트 평가 요청	다음 목록이 포함되어 있습니다. • 활성: 활성 침투 테스트 평가 요청의 목록입니다. • 모두: 활성 및 비활성 침투 테스트 평가 요청 목록 • 나에게 할당됨: 사용자가 제기한 침투 테스트 평가 요청 목록입니다. • 내 그룹에 할당: 할당 그룹의 사용자가 제기한 침투 테스트 평가 요청 목록입니다.	애플리케이션 취약성 대응	sn_vul.app_sec_manager

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

목록

목록 항목	설명	모듈	필요한 역할
	침투 테스트 평가 요청을 생성하는 방법에 대한 자세한 내용은 문서를 참조하십시오 침투 테스트 평가 요청을 생성합니다..		
침투 테스트 결과	다음 목록이 포함되어 있습니다. • 활성: 모든 활성 침투 테스트 결과의 목록입니다. • 모두: 활성 및 비활성 침투 테스트 결과 목록입니다. • 나에게 할당됨: 정정을 위해 사용자에게 할당된 침투 테스트 결과 목록입니다. • 내 그룹에 할당: 정정을 위해 할당 그룹에 할당된 침투 테스트 결과 목록입니다. 침투 테스트 결과를 생성하는 방법에 대한 자세한 내용은 문서를 참조하십시오 평가 질문서를 기반으로 침투 테스트 결과 생성.	애플리케이션 취약성 대응	sn_vul.app_sec_manager
패치	모두: 호스트 취약한 항목을 정정하는 데 사용할 수 있는 모든 패치의 목록입니다.	취약성 대응	sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin
지원 데이터	다음 목록이 포함되어 있습니다. • 신뢰할 수 있는 출처: 소스 출판물을 조사하는 데 유용한 요약 정보를 제공하는 신뢰할 수 있는 출처 목록입니다. • 기술: 각 권위 있는 출처 및	구성 준수	sn_vulc.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

목록

목록 항목	설명	모듈	필요한 역할
	인용에 대한 요약 정보를 제공하는 기술 목록입니다(Qualys에서는 프레임워크라고도 함).		

관련 정보

에서 목록 뷰 사용 취약성 관리자 작업 공간

에서 대량 편집 취약성 관리자 작업 공간

에서 취약성 관리자 작업 공간벌크 편집 기능을 사용하면 여러 취약한 항목(VIT, AVIT 또는 CVIT) 또는 구성 테스트 결과(TR)를 동시에 업데이트하여 관리 및 정정 프로세스를 간소화할 수 있습니다.

대량 편집을 사용하면 여러 취약성을 선택하고 정정 소유자 할당, 상태 업데이트, 작업 메모 추가, 예외 요청 및 가양성 요청과 같은 일관된 변경 내용을 적용할 수 있습니다. 이렇게 하면 취약한 항목을 개별적으로 편집할 필요가 없으므로 시간과 노력이 절약되고 취약성을 효율적이고 일관되게 관리할 수 있습니다.

대량 편집 기능은 다음에 사용할 수 있습니다.

- 의 v21.0부터 시작하는 호스트 취약 항목(VIT)입니다 취약성 대응.
- 의 v22.0 취약성 대응부터 시작하는 AVIT(애플리케이션 취약 항목) 및 CVIT(컨테이너 취약 항목)입니다.
- 의 v23.0 취약성 대응부터 시작하는 테스트 결과(TR).

필요한 역할:

- 호스트 취약 항목(VIT)의 경우 sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin
- 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_sec_manager
- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.vulnerability_analyst 또는 sn_vul_container.vulnerability_admin
- 구성 테스트 결과(CTR)에 대한 sn_vulc.admin

의 대량 편집 기능을 사용하여 다음 작업을 수행할 수 있습니다.취약성 관리자 작업 공간

- 할당 그룹에 기록을 대량으로 할당
- 취약성 관리자 작업 공간에서 대량 예외 요청
- 호스트 취약한 항목에 대한 할당을 대량으로 제거
- 취약성 관리자 작업 공간에서 가양성에 대한 대량 편집
- 에서 기록을 대량으로 종결 취약성 관리자 작업 공간

위험 감소를 위한 보상 통제 이해

보상 통제는 즉시 패치할 수 없는 취약성으로 인한 위험을 줄이기 위해 취하는 조치입니다. 악용이 성공할 가능성이나 영향을 완화하는 데 사용할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
보상 제어 기능은 호스트 취약성에 대해서만 사용할 수 있습니다.

보상 통제를 적용하면 취약성의 위험을 줄이는 데 도움이 될 수 있습니다.

다음 표에서는 보상 컨트롤의 사용 사례를 보여 줍니다.

보상 통제 사용 사례

사용 케이스	보상 통제
공격자가 임의 코드를 실행할 수 있는 웹 서버의 취약성입니다.	WAF(웹 애플리케이션 방화벽)를 구현하여 웹 서버에 대한 악의적인 요청을 차단합니다.
공격자가 권한을 에스컬레이션하여 루트로 만들 수 있는 운영 체제의 취약성입니다.	애플리케이션 제어를 구현하여 호스트 시스템에서 애플리케이션의 실행을 제한합니다.
공격자가 중요한 데이터에 액세스할 수 있도록 하는 데이터베이스 서버의 취약성입니다.	네트워크 세그멘테이션을 구현하여 데이터베이스 서버를 다른 호스트 및 중요한 시스템으로부터 격리합니다.

보상 통제가 취약한 항목 및 정정 작업의 위험 점수에 미치는 영향에 대한 자세한 내용은 다음 문서를 참조하십시오 보상 통제가 위험 점수 및 만료 날짜에 미치는 영향.

관련 정보

라이브러리에 보정 통제 추가

위험 감소 요청을 위해 CVE 또는 TPE와 보상 통제 연결

CVE 또는 TPE에 대한 위험 감소 사용 안 함 또는 사용

통합 취약성 대응 대시보드에 대한 분석 및 보고 솔루션

통합 취약성 대응 대시보드는 여러 취약성 스캐너 및 보안 도구의 가시성을 제공하여 조직의 취약성과 위험에 대한 포괄적인 뷰를 제공하는 중앙 집중식 집계 대시보드입니다.

필요한 역할

이 솔루션과 관련된 역할과 작업은 다음과 같습니다. 보고서를 보고 공유하는 데 필요합니다.

- sn_vul.app_sec_manager
- sn_vul.vulnerability_admin
- sn_vul.vulnerability_analyst
- sn_vulc.admin
- sn_vul_container.vulnerability_admin
- sn_vul_container.vulnerability_analyst
- sn_vul.app_developer
- sn_vulc.vulnerability_analyst

통합 취약성 대응 대시보드

통합 취약성 대응 대시보드는 조직의 취약성 및 위험에 대한 포괄적인 뷰를 제공합니다. 인프라, 클라우드, 애플리케이션 및 컨테이너와 관련된 취약성을 중앙 집중식 대시보드에서 볼 수 있으므로 가시성과 정정을 개선할 수 있습니다.

이 4분짜리 비디오를 보고 통합 취약성 대응 대시보드에 대해 알아보십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

https://player.vimeo.com/video/1046083623?h=74c3349c9c&badge=0&autopause=0&player_id=0&app_id=58479

필요한 **ServiceNow AI Platform** 역할

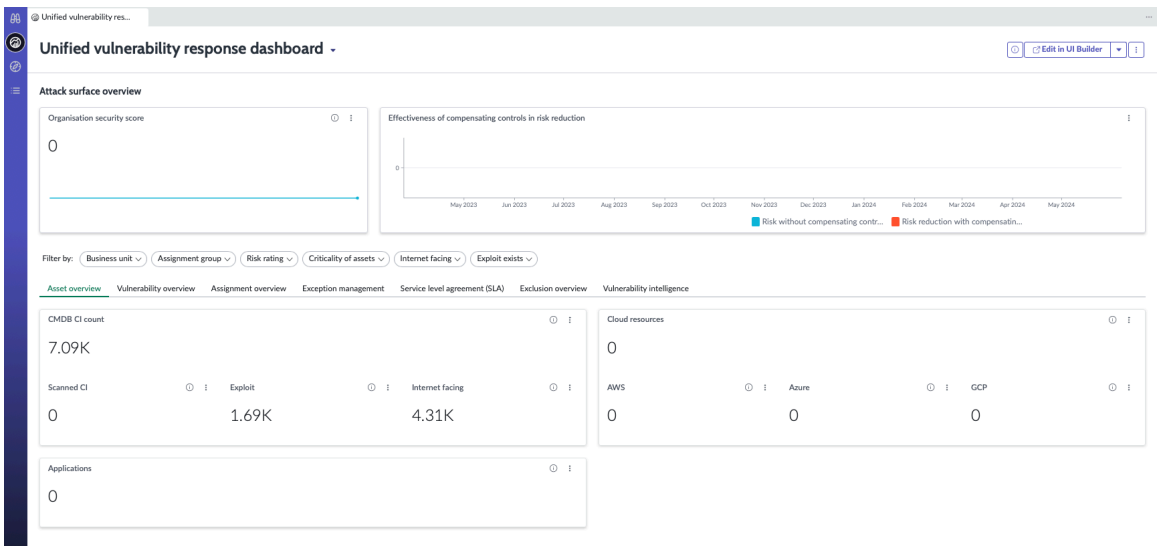
이 솔루션과 관련된 역할은 다음과 같습니다. 보고서를 보고, 편집하고, 공유하는 데 필요합니다.

- sn_vul.app_sec_manager
- sn_vul.vulnerability_admin
- sn_vul.vulnerability_analyst
- sn_vulc.admin
- sn_vul_container.vulnerability_admin
- sn_vul_container.vulnerability_analyst
- sn_vul.app_developer
- sn_vulc.vulnerability_analyst

통합 취약성 대응 대시보드에 액세스

대시보드를 열려면 다음 중 하나로 이동합니다.

- 모두 〉 취약성 대응 〉 취약성 관리자 작업 공간 을 클릭하고 대시보드 아이콘을 선택합니다. 역할에 따라 기본 대시보드가 표시됩니다. 통합 취약성 대응 대시보드를 보려면 대시보드 이름 옆에 있는 드롭다운을 선택합니다.
- 작업 공간 〉 플랫폼 분석 작업 공간 〉 대시보드 〉 통합 취약성 대응 대시보드.



사용 사례

조직 내 다른 사람이 이 대시보드를 사용하는 방법의 예시는 다음 사용 사례를 참조합니다.

사용자	대시보드 사용
• 취약성 관리자 • 취약성 분석가	• 인프라, 애플리케이션, 구성 및 컨테이너에 존재하는 위험에 대한 실시간 가시성을 제공합니다. 취약성 관리자와 취약성 분석가가

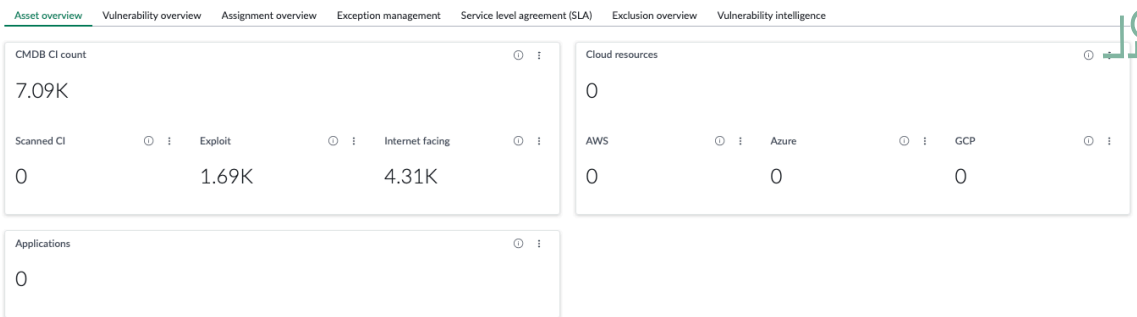
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용자	대시보드 사용
	적시에 취약성의 우선순위를 지정하고 정정할 수 있습니다. • 정정 진행률과 노력을 추적하는 데 사용할 수 있는 중요한 자산에 대한 공격 표면 개요를 제공합니다. • 비즈니스 단위(BU) 전반의 위험에 대한 개요를 제공합니다. 필터를 사용하여 BU를 선택하고 진행률을 비교하여 필요에 따라 자원을 재할당할 수 있습니다. BU 헤드에 역할 수준 액세스 권한을 제공해야 합니다. • BU의 잠재적 영향에 대한 가시성을 제공합니다. CVE(일반적인 취약성 및 노출) 필터를 사용하여 조직 전체의 노출을 식별할 수 있습니다. • 애플리케이션, 호스트 및 컨테이너 취약한 항목에 대한 CISA KEV 카탈로그에 있는 취약한 항목이 획득한 EPSS 점수에 대한 가시성을 제공합니다.

통합 취약성 대응 대시보드 탭

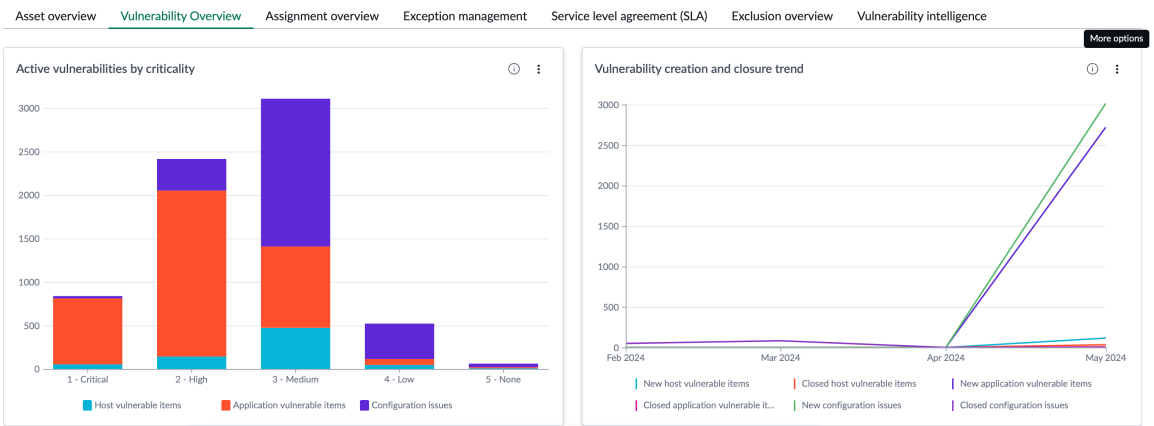
이 대시보드를 통해 호스트, 클라우드, 구성, 애플리케이션 및 컨테이너에 존재하는 취약성 또는 문제를 볼 수 있습니다. 비즈니스 단위, 할당 그룹, 위험 등급, 중요도 및 취약성에 대한 익스플로잇 존재 여부를 기준으로 취약성을 볼 수 있습니다.

자산 개요 탭에서는 시스템에 있는 구성 항목(CI)의 전반적인 상태를



제공합니다.

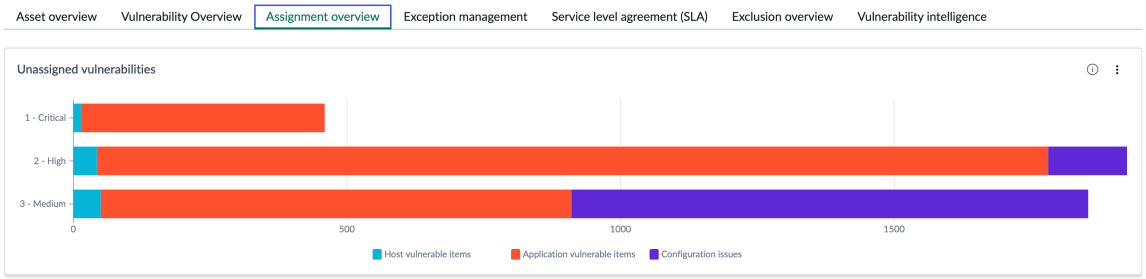
취약성 개요 탭은 호스트, 애플리케이션, 컨테이너와 같은 취약성 유형에 대한 상태를



제공합니다.

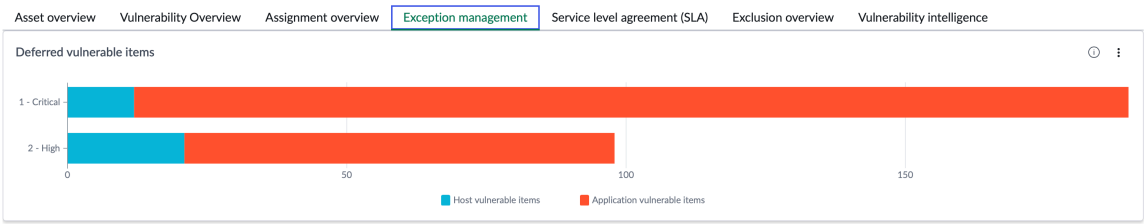
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

할당 개요 탭은 취약성 할당에 대한 상태를



제공합니다.

예외 관리 탭은 지연된 취약성에 대한 상태를

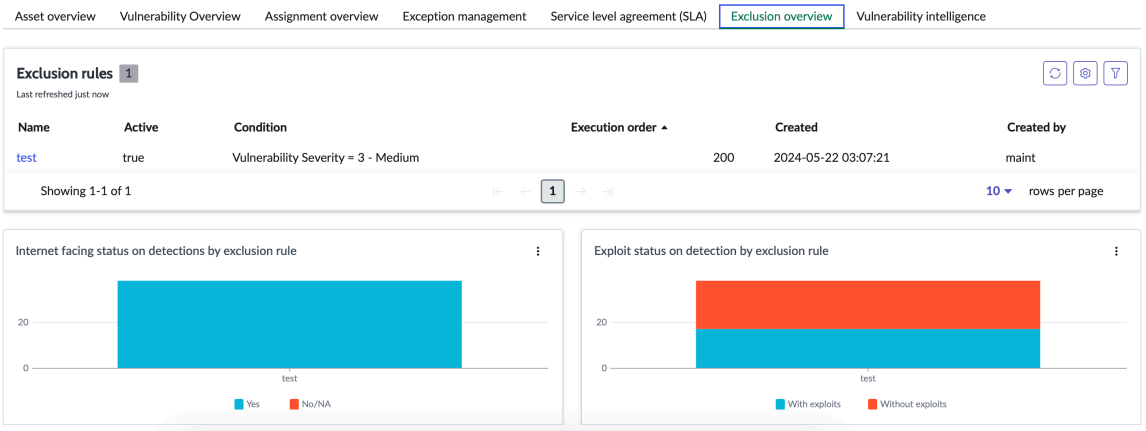


제공합니다.

서비스 수준 계약**(SLA)** 탭은 여러 할당 그룹이 획득한 서비스 수준 계약의 상태를

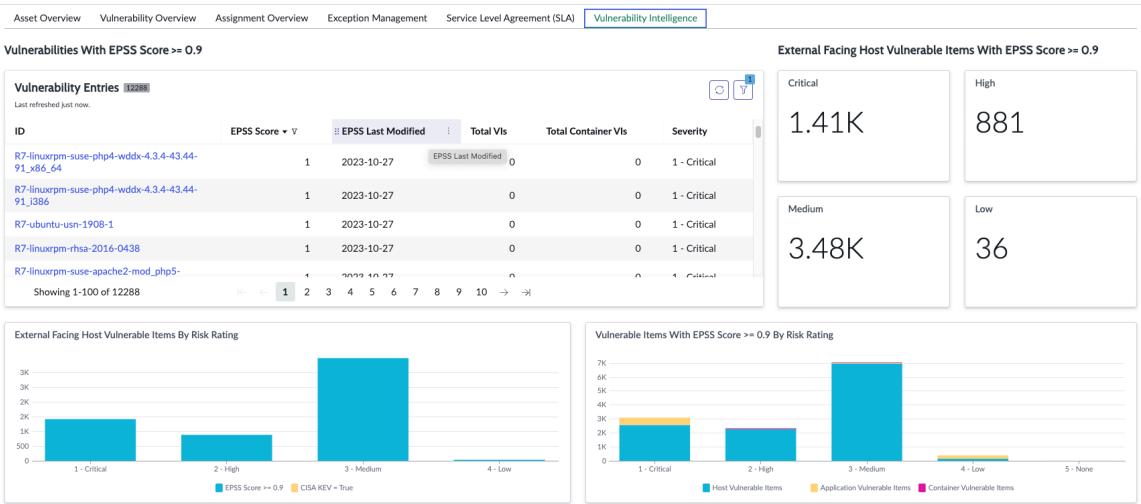
제공합니다.

제외 개요 탭은 사용자가 생성한 제외 규칙의 상태뿐만 아니라 인터넷에 연결되어 있고 이용 가능한 익스플로잇이 있는 탐지에 영향을 주는 규칙의 상태를 제공합니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약성 인텔리전스 탭은 애플리케이션, 호스트 및 컨테이너 취약한 항목에 대해 CISA KEV 플래그가 true이고 EPSS 점수 >= 0.9인 취약성이 획득한 EPSS 점수의 상태를



제공합니다.

필터

다음을 기준으로 위젯을 필터링할 수 있습니다.

- 비즈니스 단위
- 할당 그룹
- 위험 등급
- 자산 중요도
- 인터넷 연결
- 익스플로잇 존재

필터를 선택하면 모든 위젯의 데이터가 업데이트됩니다. 그러나 필터를 위젯에 적용할 수 없는 경우에는 필터 이름 옆에 십자 기호가 표시됩니다.

주:
에서 Tokyo비즈니스 단위 및 할당 그룹 필터만 사용할 수 있습니다. 모든 필터는 이제부터 Utah 사용할 수 있습니다.

표시기

스캔된 자산

지난 60일 동안 스캔한 자산에 대한 수식 표시기입니다. 스캔한 검색 항목 자산, 스캔한 애플리케이션 릴리스 자산, 스캔한 검색 컨테이너 이미지 자산을 기여 표시기로 포함합니다.

자산 - 익스플로잇 존재

취약성에 익스플로잇이 존재하는 자산에 대한 수식 표시기입니다. 호스트 자산 포함 - 익스플로잇 존재, 애플리케이션 자산 - 익스플로잇 존재, 컨테이너 자산 - 익스플로잇이 기여 표시기로 존재합니다.

인프라 자산 - 인터넷 연결

인터넷에 연결된 자산 수를 가져오기 위한 표시기입니다.

클라우드 자원 유형을 기반으로 검색된 항목

클라우드와 같은 자산 범주가 있는 자산의 수를 가져오기 위한 표시기입니다.

기본 이미지

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

기본 이미지 수를 가져오기 위한 표시기입니다.

CISA KEV 자산 유형

취약성에 CISA KEV(BOD 22-01) 플래그가 예로 설정된 컨테이너 및 호스트 취약한 항목의 수를 제공하는 수식 표시기입니다. CISA가 CVR을 존재하고, CISA가 기여 표시기로 취약성 항목을 존재합니다.

CISA 취약한 항목 존재 – 할당되지 않음

취약성에 CISA KEV(BOD 22-01) 플래그가 true로 설정되고 취약한 항목이 할당되지 않은 컨테이너 및 호스트 취약한 항목의 수를 제공하는 수식 표시기입니다. 할당되지 않은 컨테이너 취약한 항목, 할당되지 않은 호스트 취약한 항목을 기여 표시기로 포함합니다.

CISA 취약한 항목 존재 - 대상 놓침

취약성에 CISA KEV(BOD 22-01) 플래그가 true로 설정되어 있고 취약한 항목이 대상을 놓친 컨테이너 및 호스트 취약한 항목의 수를 제공하는 수식 표시기입니다. CISA가 취약한 항목을 포함하고, CISA가 기여 표시기로 CVR을 존재합니다.

활성 호스트 VIT

활성 호스트 취약한 항목(VIT)의 수입니다.

활성 애플리케이션 VIT

활성 애플리케이션 취약한 항목(AVIT)의 수입니다.

활성 컨테이너 VIT

활성 컨테이너 취약한 항목 (CVIT)의 수입니다.

새 VIT

당일에 오픈된 VIT 수입니다.

새 AVIT

하루에 오픈한 AVIT 수입니다.

새 CVIT

하루에 열린 CVIT 수입니다.

새 테스트 결과

하루에 생성된 테스트 결과(TR) 수입니다.

종결된 AVIT

하루에 종결된 VIT 수입니다.

종결된 VIT

하루에 종결된 AVIT 수입니다.

종결된 CVIT

하루에 종결된 CVIT 수입니다.

종결된 테스트 결과

하루에 종결된 TR 수입니다.

미해결 구성 문제 - 테스트 결과

실패 상태의 모든 열린 테스트 결과 수입니다.

조직 위험 점수

롤업 애플리케이션 위험 점수 테이블에 있는 조직의 위험 점수입니다.

할당되지 않은 애플리케이션 취약한 항목

할당 그룹 또는 할당 대상이 없는 AVIT

할당되지 않은 호스트 취약한 항목

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

할당 그룹 또는 할당 대상이 없는 VIT

할당되지 않은 컨테이너 취약한 항목

할당 그룹 또는 할당 대상이 없는 CVIT입니다.

할당되지 않은 구성 문제

담당 그룹 또는 할당 대상이 없는 TR입니다.

지연된 VIT

지연됨 상태의 VIT입니다.

지연된 AVIT

지연 상태의 AVIT입니다.

지연된 CVIT

지연된 상태의 CVIT입니다.

호스트 SLA - 종결됨

종결된 VIT의 평균 종결 연령입니다.

애플리케이션 SLA - 종결됨

종결된 AVIT의 평균 종결 기간입니다.

컨테이너 SLA - 종결됨

종결된 CVIT의 평균 종결 기간입니다.

SLA 테스트 결과 - 통과함

통과된 TR의 평균 종결 기간입니다.

호스트 SLA - 종결됨(중요 및 높음)

종결된 중요 VIT와 높은 VIT의 평균 종결 기간입니다.

애플리케이션 SLA - 종결됨(중요 및 높음)

중요 및 높은 AVIT의 평균 종결 기간입니다.

컨테이너 SLA - 종결됨(중요 및 높음)

종결된 중요한 CVIT와 높은 CVIT의 평균 종결 기간입니다.

SLA 테스트 결과 - 통과함(중요 및 높음)

통과된 중요 TR 및 높은 TR의 평균 종결 기간입니다.

MTTR 집계

종결된 VIT, ABIT, VIT 및 TR의 평균 종결 기간입니다.

SLA 누락

종결 및 대상 누락 VIT, ABIT, CVIT 및 TR의 평균 종결 기간입니다.

EPSS 점수가 >= 0.9인 취약성

EPSS 점수가 0.9 이상인 취약성 항목 수입니다.

세부 항목

- VIT 유형(통합)
- 인터넷 연결(통합)
- 위험 등급(통합)
- 익스플로잇 존재(통합)
- 검색된 항목 클라우드 자원 유형(통합)

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- CISA 존재(통합)
- CMDB 클래스(통합)
- 비즈니스 단위(통합)
- 비즈니스 중요도(통합)
- 지연 이유(통합)
- 담당 그룹(통합)
- 정정 상태(통합)

데이터 시각화

자산 개요 탭

직위	유형	설명
공격 표면 개요	단일 점수 	조직 보안의 집계 점수를 나타내는 숫자입니다.
CMDB CI 수	단일 점수 	에 구성 관리 데이터베이스(CMDB)등록되고 추적되는 조직의 CI 수입니다. 다음 CI의 세부 항목을 제공합니다. • 스캔한 CI: 스캔한 CI 수 • 익스플로잇: 사용 가능한 익스플로잇 수 • 인터넷 연결: 인터넷 연결 CI 수
클라우드 자원	단일 점수 	클라우드와 같은 자산 범주가 있는 CI의 수입니다. 다음 클라우드 자산의 세부 항목을 제공합니다. • AWS • Azure • GCP

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

자산 개요 탭

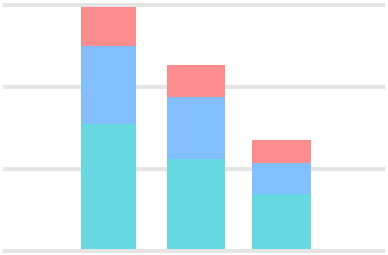
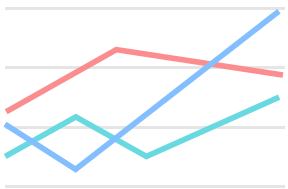
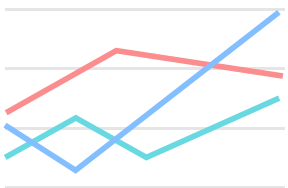
직위	유형	설명
Docker 이미지	단일 점수	기본 이미지 수를 포함한 Docker 이미지 수입니다.
애플리케이션	단일 점수	조직의 애플리케이션 수입니다.

취약성 개요 탭

직위	유형	설명
CISA KEV	원형 차트	카탈로그 및 CISA와 관련된 취약성 수입니다. 이는 사실로 플래그가 CISA 지정됩니다. 다음을 기반으로 세부 항목을 제공합니다. • CISA 취약성: CISA 플래그가 true인 취약성 유형 • 호스트 CI - 인터넷 연결: 인터넷 연결 CI • 할당되지 않은 VIT: CISA 플래그가 예인 할당되지 않은 VIT • VIT 대상 누락: CISA 플래그가 예인 대상을 놓친 VIT

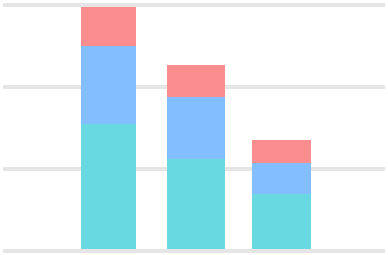
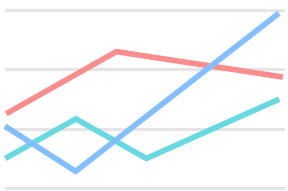
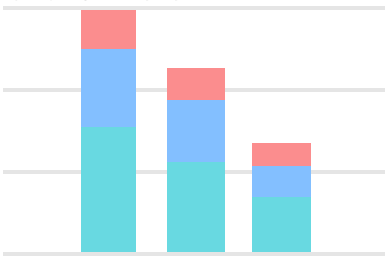
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약성 개요 탭

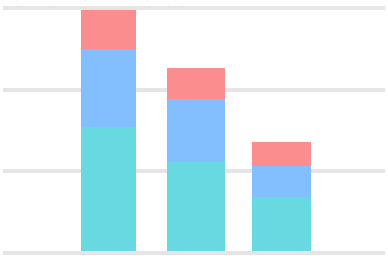
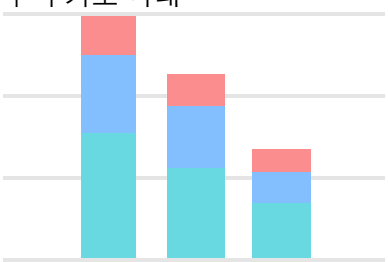
직위	유형	설명
중요도별 활성 취약성	누적 가로 막대 	중요도에 따른 활성 VIT, AVIT 및 CVIT 수입니다.
취약성 생성 및 종결 추세	다중 라인 	모든 애플리케이션에 대해 새로 추가되거나 종결된 취약성 수입니다. 지난 3개월 동안의 추세를 제공합니다.
클라우드 플랫폼별 잘못된 구성	다중 라인 	각 클라우드 자산의 위험 등급에 따른 구성 문제 수입니다.
클라우드 준수	테이블	다음 상세 정보와 함께 자산 범주가 클라우드인 자원 목록: • 자원 이름 • 클래스 • 취약성 문제: 위험 등급에 따라 집계된 자원에 있는 문제 수입니다. • 구성 문제: 위험 등급과 함께 구성 문제가 있는 자원 수입니다. • 클라우드 계정: 클라우드 계정 ID. • 클라우드 영역: 클라우드 자원의 위치입니다. • 클라우드 제공자: 클라우드 제공자의 이름입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

할당 개요 탭

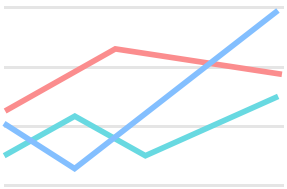
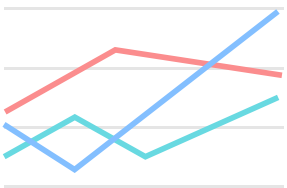
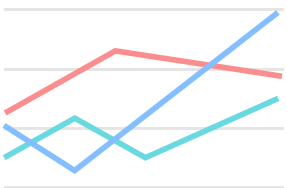
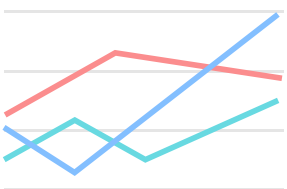
직위	유형	설명
할당되지 않은 VIT	누적 가로 막대 	위험 등급과 함께 그룹이나 개인에게 할당되지 않은 취약성 수입니다.
할당 그룹별 MTTR - 상위 10개	다중 라인 	할당 그룹이 보안 취약성 또는 문제를 식별하고 정정하는 데 걸린 평균 시간입니다. 평균 정정 시간이 가장 긴 상위 10개 할당 그룹이 표시됩니다.
SLA가 누락된 상위 10개 담당 그룹(중요 및 높은 취약성)	누적 가로 막대 	중요 및 높은 취약성의 정정 목표 날짜를 놓친 상위 10개 할당 그룹입니다.

예외 관리 탭

직위	유형	설명
지연된 VIT	누적 가로 막대 	위험 등급에 따른 지연됨 상태의 취약성 수입니다.
할당 그룹별 중요 및 높은 지연된 VIT	누적 가로 막대 	할당 그룹에 따라 분류된 지연됨 상태의 심각 및 높은 위험 등급의 취약성 수입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

서비스 수준 계약**(SLA)** 탭

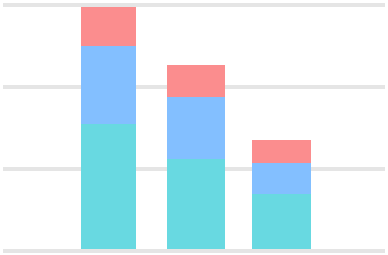
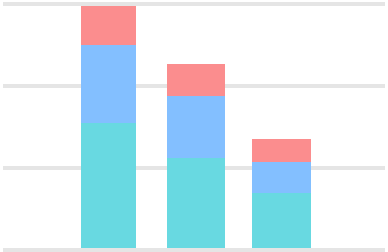
직위	유형	설명
호스트 취약성: 할당 그룹별 SLA 달성	다중 라인 	할당 그룹이 호스트 취약성을 정정하는 데 걸린 시간입니다. 지난 10개월 동안의 추세를 제공합니다.
준수 문제: 할당 그룹별 SLA 달성	다중 라인 	할당 그룹이 규정 준수 문제를 해결하는 데 걸린 시간입니다. 지난 10개월 동안의 추세를 제공합니다.
애플리케이션 취약성: 할당 그룹별 SLA 달성	다중 라인 	할당 그룹이 애플리케이션 취약성을 정정하는 데 걸린 시간입니다. 지난 10개월 동안의 추세를 제공합니다.
컨테이너 취약성: 할당 그룹별 SLA 달성	다중 라인 	할당 그룹이 컨테이너 취약성을 정정하는 데 걸린 시간입니다. 지난 10개월 동안의 추세를 제공합니다.

제외 개요 탭

직위	유형	설명
제외 규칙	테이블	생성한 모든 제외 규칙의 목록입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

제외 개요 탭

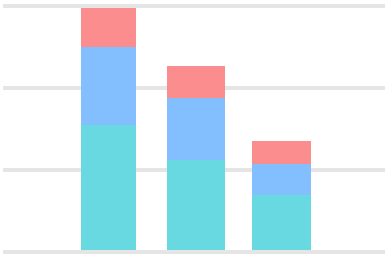
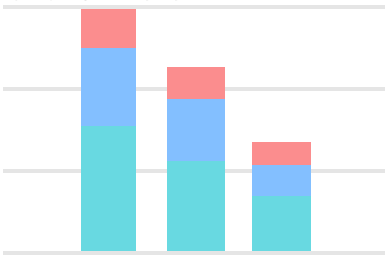
직위	유형	설명
제외 규칙과 인터넷 연결 비교	누적 가로 막대 	인터넷 연결 자산에 속하는 탐지에 영향을 주는 제외 규칙입니다.
제외 규칙 및 익스플로잇 존재	누적 가로 막대 	기존 익스플로잇에 취약한 탐지에 영향을 주는 제외 규칙입니다.

취약성 인텔리전스 탭

직위	유형	설명
EPSS 점수가 >= 0.9인 취약성	테이블	EPSS 점수가 0.9 이상인 모든 취약한 항목(CVE 또는 TPE)과 다음 상세 정보의 전체 목록 뷰입니다. • ID: 취약성의 CVE ID • EPSS 점수 • EPSS 마지막으로 수정됨 • CISA KEV BOD 22-01: CISA KEV BOD에 항목이 있는지 나타냅니다 (바인딩 운영 지침 22-01). • 총 VI: 이 취약성 항목에 대해 존재하는 총 VI 수입니다. • 총 컨테이너 VI: 이 취약성 항목에 대해 존재하는 컨테이너 VI의 총 수입니다. • 심각도

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약성 인텔리전스 탭

직위	유형	설명
EPSS 점수가 〉= 0.9인 외부 연결 호스트 취약 항목	단일 점수 	EPSS 점수가 0.9 이상인 외부 연결 호스트 취약한 항목의 집계 수를 나타내는 번호입니다. 위험 등급의 심각도별로 정렬된 단일 점수를 제공합니다.
위험 등급별 외부 연결 호스트 취약 항목	누적 가로 막대 	위험 등급별 외부 연결 호스트 취약한 항목 수입니다. 스택 막대는 EPSS 점수 〉=0.9 및 CISA KEV = True로 분류됩니다.
EPSS 점수가 위험 등급 기준 〉= 0.9인 취약 항목	누적 가로 막대 	위험 등급별로 정렬된 EPSS 점수가 0.9 이상인 취약성 수입니다. 호스트 취약한 항목, 애플리케이션 취약한 항목 및 컨테이너 취약한 항목별로 세부 항목을 제공합니다.

데이터 수집을 위한 예약된 작업

데이터 수집 작업에서는 자동 표시기와 세분화에 대한 점수가 자동으로 수집됩니다. 다음 예약된 작업이 실행되어 새 데이터에 대한 점수를 자동으로 수집합니다.

⚠ 경고:
기본적으로 기본 시스템에서는 다음 데이터 수집 작업이 비활성화되어 있습니다.

- 통합 대시보드 일별 데이터 수집
- 통합 대시보드 주간 데이터 수집
- 통합 대시보드 기록 데이터 수집

작업을 활성화하기 전에 KB 를 참조하십시오.

예약된 작업	빈도	설명
통합 대시보드 기록 데이터 수집	한 번	기존 기록의 점수와 스냅샷을 수집합니다.
통합 대시보드 주간 데이터 수집	주별	매주 데이터를 수집합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예약된 작업	빈도	설명
통합 대시보드 일별 데이터 수집	매일	매일 데이터를 수집합니다.
조직에 위험 점수 롤업	매일	조직에 대해 집계된 위험 점수를 수집합니다.
클라우드 준수 일일 카운트 채우기	매일	클라우드 규정 준수를 위해 데이터를 수집합니다.
EPSS 일일 작업	매일	First.org 에서 EPSS 데이터를 수집합니다.

취약성 공통 범위에 새 테이블 롤업 애플리케이션 위험 점수(sn_vul_cmn_rollup_app_risk_score)가 생성됩니다. 이 테이블은 매일 예약된 작업을 통해 다음 롤업 계산기를 사용하여 채워집니다.

롤업 계산기 이름	설명
조직 위험 점수 롤업	조직의 모든 취약한 항목 및 구성 문제에 대한 위험 점수를 롤업합니다. 조직의 전반적인 위험 점수를 제공합니다.
취약한 항목 롤업	조직의 모든 취약한 항목에 대한 위험 점수를 롤업하여 조직의 전체 위험 점수에 기여합니다.
애플리케이션 취약한 항목 롤업	조직의 전체 위험 점수에 기여하기 위해 조직의 모든 애플리케이션 취약한 항목에 대한 위험 점수를 롤업합니다.
컨테이너 취약한 항목 롤업	조직의 전체 위험 점수에 기여하기 위해 조직의 모든 컨테이너 취약한 항목에 대한 위험 점수를 롤업합니다.
테스트 결과 롤업	조직의 전체 위험 점수에 기여하기 위해 조직의 모든 테스트 결과에 대한 위험 점수를 롤업합니다.
NVD에서 TPE로 EPSS 점수 롤업	NVD에서 TPE로 EPSS 점수를 롤업하여 조직의 전체 위험 점수에 기여합니다.

에서 워크플로우 예시 보기 취약성 관리자 작업 공간

에서 취약성 관리자 작업 공간엔드 투 엔드 워크플로우의 예를 봅니다. 취약성 관리자 또는 분석가가 작업 공간을 사용하여 중요한 기록을 모니터링하고 IT에 전달할 정정 작업을 생성하는 방법을 알아봅니다.

시작하기 전에
필요한 역할:

- 호스트 취약 항목(VIT)의 경우 sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin
- 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_sec_manager
- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.vulnerability_analyst 또는 sn_vul_container.vulnerability_admin
- 구성 테스트 결과(CTR)에 대한 sn_vulc.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

워크플로우의 단계를 보려면 다음 비디오를 클릭하십시오.
취약성 관리자 작업 공간 데모

이전 비디오에는 다음 작업이 포함되어 있습니다.

a. 대시보드에서 데이터를 보려면 작업 공간의 감시 주제 페이지에서 감시 주제를 클릭합니다.

b. 필터 조건을 사용하여 주시 주제를 생성하고 일치하는 기록을 미리 봅니다. 감시 주제를 생성하는 방법에 대한 자세한 내용은 문서를 참조하십시오 에서 주시 주제 생성 취약성 관리자 작업 공간.

c. 감시 주제의 영향을 받는 **CI** 탭에서 기록 및 관련 구성 항목에 대한 데이터를 봅니다. 시각화에 대한 자세한 내용은 다음 문서를 참조하십시오 주시 주제의 관련 항목 목록 및 시각화.

d. 감시 주제의 구별되는 취약성 탭에서 취약성에 대한 데이터를 봅니다.

e. 취약한 항목의 감시 주제 또는 감시 주제의 구성 테스트 결과 탭에서 감시 주제와 연결된 기록을 봅니다. 오른쪽으로 스크롤하여 정정 작업 열에서 이미 정정 작업에 있는 기록을 봅니다.

f. 특정 유형의 기록에 대한 작업을 생성하고 정정을 위해 IT에 할당할 준비가 되면 감시 주제에 대한 정정 작업 생성을 선택합니다. 정정 작업을 만드는 방법에 대한 자세한 내용은 을 참조하십시오 에서 정정 작업 생성 취약성 관리자 작업 공간.

g. 목록 뷰를 선택하여 정정 작업, 정정 작업, 기록, 예외 및 승인 목록을 확인합니다. 목록 페이지에 대한 자세한 내용은 다음 문서를 참조하십시오 의 목록 페이지 취약성 관리자 작업 공간.

h. 목록 뷰에서 활성 정정 작업 목록을 선택하여 정정 작업 기록을 열고 기록에 대한 상태 및 정보를 봅니다. 자세한 내용은 의 목록 페이지 취약성 관리자 작업 공간 문서를 참조하십시오.

i. 정정 기록에서 정정 작업 탭을 선택하여 정정 기록과 연결된 정정 작업을 봅니다. 자세한 내용은 의 목록 페이지 취약성 관리자 작업 공간 문서를 참조하십시오.

j. 각 정정 작업 기록에서 취약한 항목 탭, 애플리케이션 취약한 항목 탭, 컨테이너 취약한 항목 탭 또는 구성 테스트 결과 탭을 선택하여 정정 작업과 연결된 기록 목록을 봅니다. 자세한 내용은 의 목록 페이지 취약성 관리자 작업 공간 문서를 참조하십시오.

k. 기록의 하위 집합에 대한 정정 작업에서 요청 시 새 정정 작업을 생성하려면 이동할 기록을 선택하고 정정 작업 생성을 클릭합니다. 자세한 내용은 의 정정 작업에서 요청 시 정정 작업 생성 취약성 관리자 작업 공간 문서를 참조하십시오.

다음에서 취약한 항목 및 테스트 결과를 모니터링하고 관리합니다. 취약성 관리자 작업 공간

이를 취약성 관리자 작업 공간 통해 감시 주제를 사용하여 취약한 항목(VIT, AVIT 및 CVIT) 및 테스트 결과(TR)를 모니터링하고, 정정 작업을 생성하여 정정 진행률을 추적 및 관리할 수 있습니다.

다음에서 검색 결과 열기 취약성 관리자 작업 공간

애플리케이션 범위를 변경하여 클래식 UI 대신 검색 결과를 취약성 관리자 작업 공간 엽니다.

시작하기 전에
필요한 역할:

- 호스트 취약 항목(VIT)에 대한 sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin 또는 sn_vul.read_all
- 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_sec_manager 또는 sn_vul.app_read_all
- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.vulnerability_analyst, sn_vul_container.vulnerability_admin 또는 sn_vul_container.read_all
- 구성 테스트 결과(TR)에 대한 sn_vulc.admin 또는 sn_vulc.read

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보
예: 애플리케이션 범위를 취약성 관리자 작업 공간로 설정하여 검색 필드에서 호스트 취약한 항목을 해당 번호로 검색하면 VIT취약성 관리자 작업 공간가 의 기록 뷰에서 열립니다.

프로시저

1. 통합 탐색 모음에서 지구본 아이콘 선택합니다.
2. 애플리케이션 범위를 선택합니다.
3. 범위를 취약성 관리자 작업 공간으로 설정합니다.

다음에 수행할 작업
통합 탐색 모음의 검색 필드에서 VIT, 정정 작업, 상태 변경 승인 등의 기록을 검색하면 에서 취약성 관리자 작업 공간기록이 열립니다.

범위가 전역이 아닌 경우 지구본 아이콘에 빨간색 링이 있는 표시됩니다. 범위를 변경하려면 다시 선택합니다.

활성 기록 요약(VIT, ABIT, CVIT 및 CTR) 필터 생성 및 적용

취약성 관리자와 분석가는 원하는 레코드를 필터링하여 의 홈 페이지에 취약성 관리자 작업 공간요약을 시각화할 수 있습니다.

시작하기 전에
필요한 역할:

- 호스트 취약 항목(VIT)의 경우 sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin
- 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_sec_manager
- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.vulnerability_analyst 또는 sn_vul_container.vulnerability_admin
- 구성 테스트 결과(CTR)에 대한 sn_vulc.admin

프로시저

1. 다음으로 이동 작업 공간 〉 취약성 관리자 작업 공간 〉 홈페이지.
2. 기어 아이콘 선택한 다음 호스트 취약성, 컨테이너 취약성, 애플리케이션 취약성 또는 구성 테스트 결과 탭에서 필터 생성을 선택합니다.
3. 필터 생성 팝업 창에서 필드에 내용을 입력합니다.

필터 생성 팝업 창

필드	설명
필터 이름	필터의 이름입니다.
조건	시각화를 보려는 기록만 표시하는 조건입니다.
매일 새로 고침	시각화 정보를 매일 업데이트합니다.

4. 저장을 선택합니다.
5. 보기 기준 필드에서 새 필터를 선택하여 필터링된 기록에 대한 시각화를 봅니다.
   위젯에 대한 자세한 내용은 의 홈페이지 취약성 관리자 작업 공간 문서를 참조하십시오.
6. 필터를 업데이트하거나 삭제하려면:

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 기어 아이콘 선택한 다음 필터 편집을 선택합니다.

b. 저장된 필터 팝업 창에서 업데이트하거나 삭제할 필터를 선택합니다.

c. 필터를 업데이트하거나 삭제합니다.

작업	단계
필터를 삭제합니다.	삭제를 선택합니다.
필터 이름 수정	필터 이름을 편집하고 업데이트를 선택합니다.
필터 조건 변경	특정 기록에 대한 정보만 표시하도록 조건을 편집하고 업데이트를 선택합니다.
매일 새로 고침	시각화 정보를 매일 새로 고칠지 여부를 결정하고 업데이트를 선택합니다.

관련 정보

의 홈페이지 취약성 관리자 작업 공간

의 주시 주제 사용취약성 관리자 작업 공간

의 취약성 관리자 작업 공간 감시 주제를 사용하여 설정한 기준에 따라 임포트한 데이터에서 필터링된 취약성 및 잘못된 구성을 봅니다. 이 정보를 사용하여 각 감시 주제의 취약성과 잘못된 구성이 환경에 어떤 영향을 미칠 수 있는지 확인할 수 있습니다.

시작하기 전에
필요한 역할:

- 호스트 취약 항목(VIT)의 경우 sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin
- 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_sec_manager
- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.vulnerability_analyst 또는 sn_vul_container.vulnerability_admin
- 구성 테스트 결과(CTR)에 대한 sn_vulc.admin

이 태스크 정보
감시 주제 페이지에서 다음 작업을 수행할 수 있습니다.

- 정정 작업 및 기록(VIT, ABIT, CVIT 및 TR) 수를 모니터링하여 취약성 정정 진행 상황을 확인합니다.
- 기존 감시 주제를 편집하거나 삭제하고 감시 주제를 생성합니다.
- 정정 작업을 생성하고 수정하려는 취약성에 대해서만 정정 작업을 IT 팀에 자동으로 전달합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
의 취약성 대응v19.0부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v19.0 이전 용어	용어집 **v19.0** 이상
테스트 결과 그룹	정정 작업
구성 문제	구성 테스트 결과
정책	테스트 그룹

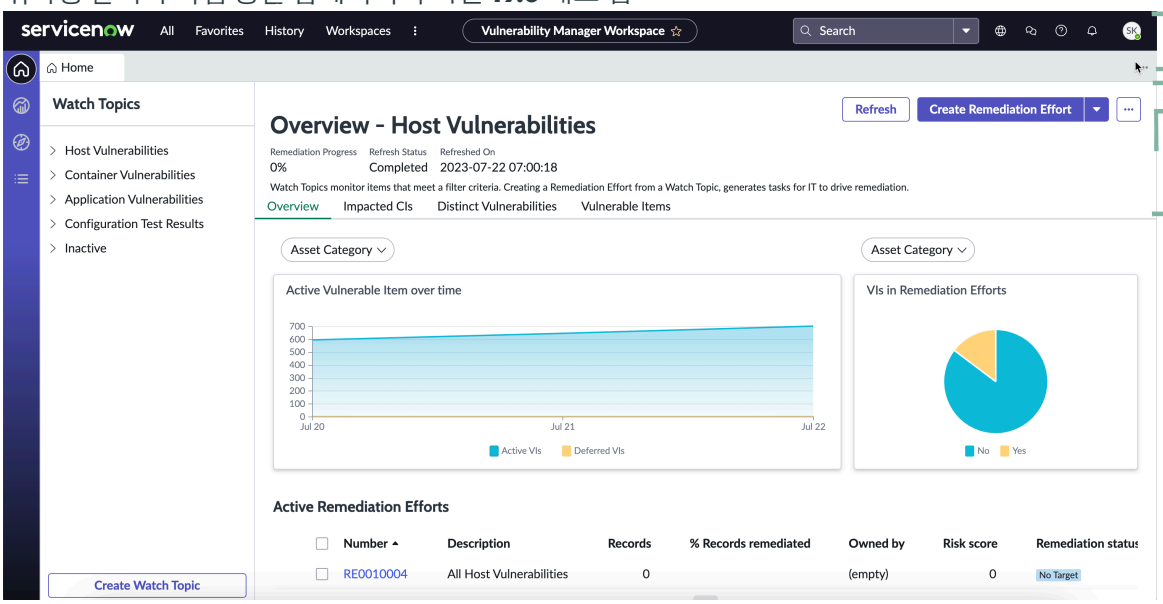
프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 취약성 관리자 작업 공간.
2. 주시 주제 아이콘을 선택합니다.
3. 감시 주제 페이지의 호스트 취약성, 컨테이너 취약성, 애플리케이션 취약성 또는 구성 테스트 결과 탭에서 감시 주제를 선택합니다.

   감시 주제를 선택하면 기본적으로 개요 탭이 표시됩니다.

   감시 주제에 대한 자세한 내용은 문서를 참조하십시오 의 주시 주제 페이지 취약성 관리자 작업 공간.

   취약성 관리자 작업 공간 홈페이지의 버전 **19.0** 개요 탭



   대시보드는 임포트 시 동적이며 새로운 취약성 데이터가 업데이트됩니다.

4. 더 많은 데이터를 보려면 관련 항목 탭을 선택하십시오.

   감시 항목의 관련 항목 목록 및 시각화에 대한 자세한 내용은 을 참조하십시오 주시 주제의 관련 항목 목록 및 시각화.

5. 주시 주제 페이지에서 UI 작업을 수행합니다.

6. 옵션: 기록을 선택하여 자세한 내용을 봅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

에서 주시 주제 생성 취약성 관리자 작업 공간

취약성 관리자와 분석가는 일련의 조건을 사용하여 감시 주제를 생성하여 모니터링하려는 기록의 하위 집합(VIT, AVITs, CVIT 또는 CTR)을 필터링할 수 있습니다.

시작하기 전에

필요한 역할:

- 호스트 취약 항목(VIT)의 경우 sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin
- 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_sec_manager
- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.vulnerability_analyst 또는 sn_vul_container.vulnerability_admin
- 구성 테스트 결과(CTR)에 대한 sn_vulc.admin

이 태스크 정보

감시 주제의 개요 탭에서, 다른 보고서와 함께 야간에 업데이트되는 추세 보고서는 해당 감시 주제에 대한 기록의 현재 상태를 보여줍니다.

주:
의 취약성 대응v19.0부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v19.0 이전 용어	용어집 **v19.0** 이상
테스트 결과 그룹	정정 작업
구성 문제	구성 테스트 결과
정책	테스트 그룹

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 취약성 관리자 작업 공간 〉 주시 주제.
2. 옵션: 또는 Create remediation effort 버튼 오른쪽에 있는 세 개의 점 클릭한 다음 편집을 클릭하여 기존 주시 주제를 수정합니다.

   주:
   필터링을 변경한 후 주시 주제에 대한 현재 데이터가 표시되기까지 지연이 발생할 수 있습니다.

3. 페이지 왼쪽 하단에서 주시 주제 생성을 선택합니다.
4. 표시되는 모달의 필드에 내용을 입력합니다.
   주시 주제 생성 모달 필드에 대한 자세한 내용은 문서를 참조하십시오주시 주제 양식 필드 생성.
5. 선택한 기록 범주에 대한 조건을 정의합니다.

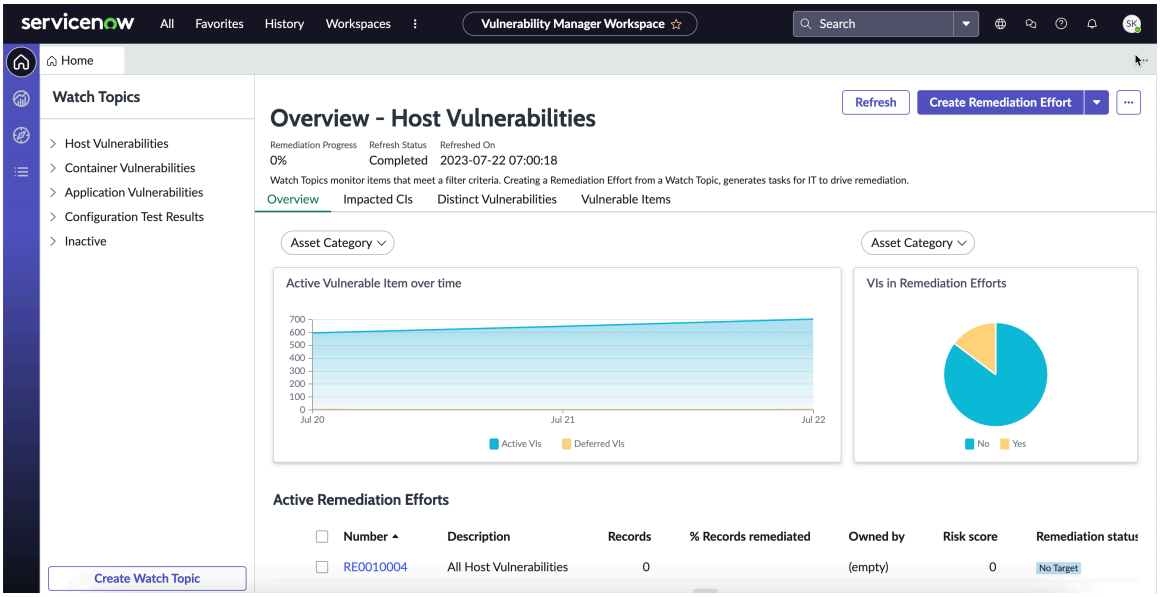
   주:
   감시 주제에서 조건을 설정하지 않으면 데이터가 대시보드로 끌어오지 않습니다.

6. 제출을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

새 주시 주제가 홈 방문 페이지에 표시됩니다. 감시 주제는 탐색 창에서 기록 유형별로 분류됩니다.

버전 **19.0** 취약성 관리자 작업 공간 홈페이지



다음에 수행할 작업
정정 작업량을 생성합니다.

에서 주시 주제를 편집하거나 삭제합니다. 취약성 관리자 작업 공간

에서 기존 감시 주제를 편집하거나 삭제할 수 있습니다 취약성 관리자 작업 공간.

시작하기 전에
필요한 역할:

- 호스트 취약 항목(VIT)의 경우 sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin
- 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_sec_manager
- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.vulnerability_analyst 또는 sn_vul_container.vulnerability_admin
- 구성 테스트 결과(CTR)에 대한 sn_vulc.admin

이 태스크 정보
기존 감시 주제를 편집하는 경우:

- 대시보드의 데이터가 업데이트되어 변경 내용이 반영됩니다.
- 현재 기존 정정 작업에 있는 기록은 변경되지 않은 상태로 유지됩니다.
- 현재 정정 작업에 없는 기록은 조건 작성기에 입력한 기준에 따라 표시됩니다.

연관된 모든 기록이 수정되기 전에 감시 주제를 삭제해도 해당 감시 주제와 함께 표시되는 기록은 영향을 받지 않습니다.

프로시저

1. 다음으로 이동 작업 공간 〉 취약성 관리자 작업 공간 〉 주시 주제.
2. 편집하려는 주시 주제를 여십시오.
3. 점 세 개 ... 클릭하고 편집을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
비활성 감시 주제는 편집할 수 없습니다.

4. 주시 주제 편집 모달에서 필드를 수정합니다.
5. 제출을 클릭합니다.

주:
필터링을 변경한 후 주시 주제에 대한 현재 데이터가 표시되기까지 지연이 발생할 수 있습니다.

기존의 반복 정정 작업을 편집할 수도 있습니다. 감시 주제에 대한 기존 반복 정정 작업이 있는 경우 메뉴에서 반복 작업 편집을 사용할 수 있습니다. 반복 작업을 편집하려면 이 옵션을 선택합니다.

변경 사항을 적용하고 정정 작업 기록에 저장해도 감시 주제에서 이미 생성한 다른 정정 작업에는 영향을 주지 않습니다.

6. 옵션: 감시 주제를 삭제하려면 감시 주제에서 점 3개 메뉴 선택하고 삭제를 선택합니다.

주시 주제 비활성화 또는 활성화

취약성 관리자 작업 공간에서 감시 주제를 비활성화하거나 활성화할 수 있습니다.

시작하기 전에

필요한 역할:

- 호스트 취약 항목(VIT)의 경우 sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin
- 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_sec_manager
- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.vulnerability_analyst 또는 sn_vul_container.vulnerability_admin
- 구성 테스트 결과(CTR)에 대한 sn_vulc.admin

이 태스크 정보

- 모든 비활성 주시 주제가 탐색 창의 비활성 모듈에 표시됩니다.
- 비활성 감시 주제에 대한 정정 작업 또는 반복 정정 작업을 생성할 수 없습니다.
- 비활성 주시 주제는 새로 고칠 수 없습니다.
- 비활성 주시 주제 및 관련 정정 작업의 상세 정보는 업데이트되지 않습니다.

프로시저

1. 다음으로 이동 작업 공간 〉 취약성 관리자 작업 공간 〉 주시 주제.
2. 비활성화하려는 주시 주제를 엽니다.
3. 세 개의 점을 클릭하고 비활성화를 클릭합니다.
   주시 주제가 비활성 모듈에 나타납니다.
4. 감시 주제를 활성화하려면 비활성 모듈에서 감시 주제를 선택하고 점 3개 메뉴를 선택한 다음 활성화를 선택합니다.
   활성화된 감시 주제가 탐색 창의 해당 모듈로 이동합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

정정 작업 기록 사용

취약성 관리자와 분석가가 RE(정정 작업)를 생성하면 정정 작업(VUL, AVUL, CVUL 및 CRG)이 정정을 위해 IT 팀에 자동으로 할당됩니다.

시작하기 전에

정정 작업의 정정 진행률을 모니터링하는 데 사용하려면 먼저 정정 작업량을 생성해야 합니다.

필요한 역할:

- 호스트 취약 항목(VIT)의 경우 sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin
- 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_sec_manager
- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.vulnerability_analyst 또는 sn_vul_container.vulnerability_admin
- 구성 테스트 결과(CTR)에 대한 sn_vulc.admin

프로시저

1. 선택하지 않은 경우 왼쪽 상단에서 목록 아이콘을 클릭합니다.

   활성 정정 작업 기록이 있는 목록 뷰가 표시됩니다.

2. Record Type(기록 유형) 열에서 점 3개 메뉴를 선택하고 **Group by Record** type(기록 유형별 그룹화)을 선택합니다.
   정정 작업은 호스트 취약한 항목, 애플리케이션 취약한 항목, 컨테이너 취약한 항목 및 구성 테스트 결과로 분류됩니다.
3. 목록 뷰 방문 페이지의 필터링된 목록에서 활성 정정 작업이 선택된 상태에서 기록을 클릭하여 엽니다.
   기록이 표시됩니다. 선택한 정정 작업과 연결된 정정 작업 및 기록을 볼 수 있습니다.
4. 정정 작업 기록에서 수행할 수 있는 작업에 대해서는 다음 테이블을 참조하십시오.

   기록을 생성한 후 정정 작업과 많은 수의 기록이 표시되는 데 몇 분 정도 걸릴 수 있습니다.

UI 작업	설명
태그 추가	헤더 오른쪽에 있는 작은 태그 아이콘을 클릭합니다. 이 기록을 식별하는 데 도움이 되는 텍스트를 추가할 수 있습니다. 예를 들어 이 기록에 PCI 또는 기타 중요한 데이터가 있는 태그를 추가할 수 있습니다.
기록에 작업 메모 추가	화면 맨 오른쪽에서 활동 아이콘(번개 아이콘)을 클릭하고 작업 메모를 입력합니다. 패널을 전환하려면 아이콘을 클릭합니다.
기록 업데이트	상세 정보 탭에서 편집 가능한 모든 필드에 대해 필드를 클릭하여 선택하고 변경한 다음 저장을 클릭하여 기록을 업데이트합니다.
표시되면 필터 아이콘을 클릭하여 표시된 페이지의 데이터를 구체화합니다.	정정 작업, 취약한 항목 또는구성 테스트 결과 탭 중 하나를 선택한 상태에서 맨 오른쪽에 있는 필터 아이콘을 클릭하여 탭에 적용되는 필터를 표시합니다. 표시되는 패널에서 고급 보기를 클릭하여 페이지의 항목에 대한 필터 조건을 추가하거나

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

UI 작업	설명
	변경합니다. 변경 사항을 저장하려면 업데이트를 클릭합니다. 예를 들어 취약한 항목 탭에서 연령 필드를 추가하고 특정 기간의 기록만 표시하는 범위를 입력할 수 있습니다. 설정한 조건과 일치하는 기록이 목록에 표시됩니다.
열의 항목에 대한 필터 구체화	열을 선택하고 세 개의 세로 점 메뉴를 클릭한 다음 확장하여 열의 데이터를 구체화하고 그룹화할 조건을 입력합니다.
열의 행에서 항목 또는 일치 항목을 필터링합니다.	예를 들어 특정 취약성이 있는 레코드만 보려고 한다고 가정해 보겠습니다. 기록 목록의 요약 열에서 기록 행을 선택합니다. 표시되는 세로 점 메뉴를 클릭하고 다음 중 하나를 선택합니다. ○ 일치 표시 - 이러한 취약성이 있는 다른 모든 기록을 표시합니다. ○ 필터링 - 이 취약성이 없는 모든 기록을 표시합니다.

5. 정정 작업, 취약한 항목 및 구성 테스트 결과 탭에서 개별 정정 작업(VUL, AVUL, CVUL 또는 CRG), 취약한 항목(VIT, AVIT 또는 CVIT) 및 테스트 결과(CTR) 기록을 각각 드릴다운할 수 있습니다.

다음에 수행할 작업

정정 작업에서 요청 시 정정 작업을 생성하려면 다음 문서를 참조하십시오 의 정정 작업에서 요청 시 정정 작업 생성 취약성 관리자 작업 공간. 정정 진행률을 모니터링하는 데 도움이 될 수도 사용자 지정 기록 목록 만들기 있습니다.

에서 정정 작업 생성 취약성 관리자 작업 공간

정정 작업 기록은 의 취약성 관리자 작업 공간감시 주제에서 생성하는 기록의 정적 목록입니다.

시작하기 전에

필요한 역할:

- 호스트 취약 항목(VIT)의 경우 sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin
- 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_sec_manager
- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.vulnerability_analyst 또는 sn_vul_container.vulnerability_admin
- 구성 테스트 결과(CTR)에 대한 sn_vulc.admin

이 태스크 정보

정정 작업을 사용하여 IT 팀이 취약성과 잘못된 구성을 수정하는 데 사용하는 작업을 전달합니다.

- 기존 정정 작업을 편집할 수 있습니다.
- 설정한 날짜 및 시간에 자동으로 생성되는 정정 작업을 생성합니다.
- 기존 정정 작업에서 새 정정 작업으로 기록을 이전합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

버전 18.0부터는 비활성 감시 주제에 대한 정정 작업량을 생성할 수 없으므로 정 정 작업량 생성 버튼이 비활성화됩니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 취약성 관리자 작업 공간 〉 주시 주제.
2. 감시 주제 페이지에서 정정 작업을 생성할 감시 주제를 선택합니다.
3. 선택한 감시 주제와 연결된 기록을 보려면 기록 헤더 아래에서 해당 감시 주제의 취약한 항목, 애플리케이션 취약한 항목, 컨테이너 취약한 항목 또는 구성 테스트 결과 탭을 클릭합니다.

   기록이 표시됩니다.

   예를 들어 취약한 항목 탭 아래의 헤더에서 이 감시 주제에 있는 총 기록 수를 볼 수 있습니다.

   다음과 같은 열과 데이터가 표시됩니다.

취약한 항목 탭의 열

열	설명
번호	기록 번호입니다.
요약	취약성에 대한 설명입니다.
구성 항목	취약성과 연결된 자산입니다.
위험 등급	기록을 중요, 높음, 중간, 낮음 및 없음으로 구분하는 정량화된 위험 점수입니다.
상태	기록의 상태입니다.
정정 상태	기록의 정정 상태입니다.
할당 그룹	정정을 담당하는 할당 그룹입니다. 그룹에 대한 기록 할당은 생성하는 담당 규칙에 따라 수행됩니다.
정정 작업	정정 작업에 할당된 경우 각 기록에는 할당된 정정 작업이 나열됩니다. 정정 작업에 추가된 후에는 사용자가 생성하는 다른 정정 작업에 기록이 추가되지 않습니다.
할당 그룹	정정을 담당하는 할당 그룹입니다. 그룹에 대한 기록 할당은 생성하는 담당 규칙에 따라 수행됩니다.
정정 작업	정정 작업에 할당된 경우 각 기록에는 할당된 정정 작업이 나열됩니다. 정정 작업에 추가된 후에는 사용자가 생성하는 다른 정정 작업에 기록이 추가되지 않습니다.
정정 작업 중	true인 경우 이 값은 기록이 이미 정정 작업에 있음을 나타냅니다. 기록은 여러 정정 작업에 있을 수 있지만 기록은 하나의 정정 작업에만 추가할 수 있습니다.
익스플로잇 존재	기록에 대해 알려진 익스플로잇이 존재하는지 나타냅니다.
마지막으로 시작한 시간	에서 ServiceNow AI Platform기록이 마지막으로 열린 날짜입니다. 기록을 종결한

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

열	설명
	다음 다시 열었다면 기록이 마지막으로 다시 열렸습니다.

4. 정정 작업량을 생성하려면 정 정 작업량 생성을 클릭합니다.

   정정 작업을 생성하면 기존 정정 작업에 이미 있는 기록이 이 감시 주제에서 생성하는 새 정정 작업에 추가되지 않습니다.

   감시 주제에 기록이 업데이트되거나 새 기록이 생성되면 정정 작업을 생성할 수 있습니다.

5. 또는 다음을 수행할 수 있습니다 에서 반복 정정 작업 생성 취약성 관리자 작업 공간.

   편집 버튼은 기존 정정 작업에 대한 메뉴에서 사용할 수 있습니다. 표시되는 모달에서 필드와 조건을 수정할 수 있는 옵션이 있습니다. 변경하고 정정 작업 기록에 저장해도 감시 주제에서 이미 생성한 다른 정정 작업에는 영향을 주지 않습니다.

6. 정정 작업 생성 모달의 1단계에서 필드에 내용을 입력합니다.

   간단한 설명 필드에 반복되는 정정 작업을 설명하고 작업 목록에서 이를 찾아 추적하는 데 도움이 되는 텍스트를 입력합니다.

   설명 필드에 정정 작업 목록에서 쉽게 찾을 수 있도록 작업의 컨텍스트에 대한 추가 텍스트를 입력합니다.

7. 2단계, 작업 생성의 목록에서 한 가지 방법을 선택하여 이 정정 작업이 생성된 후 생성하는 정정 작업의 기록을 번들로 묶습니다.

8. 중복 호스트 취약한 항목을 자동으로 새로 고치려면 생성된 정정 작업에 대해 중복된 취약한 항목을 자동으로 새로 고침 확인란을 선택해야 합니다.

   주:
   이 확인란은 호스트 취약성에 대해서만 사용할 수 있습니다.

9. 3단계, 이전에서 정정 작업에 추가할 기록 수를 확인하고 다른 활성 정정 작업에서 이전할 수 있는 기록 수를 확인합니다.

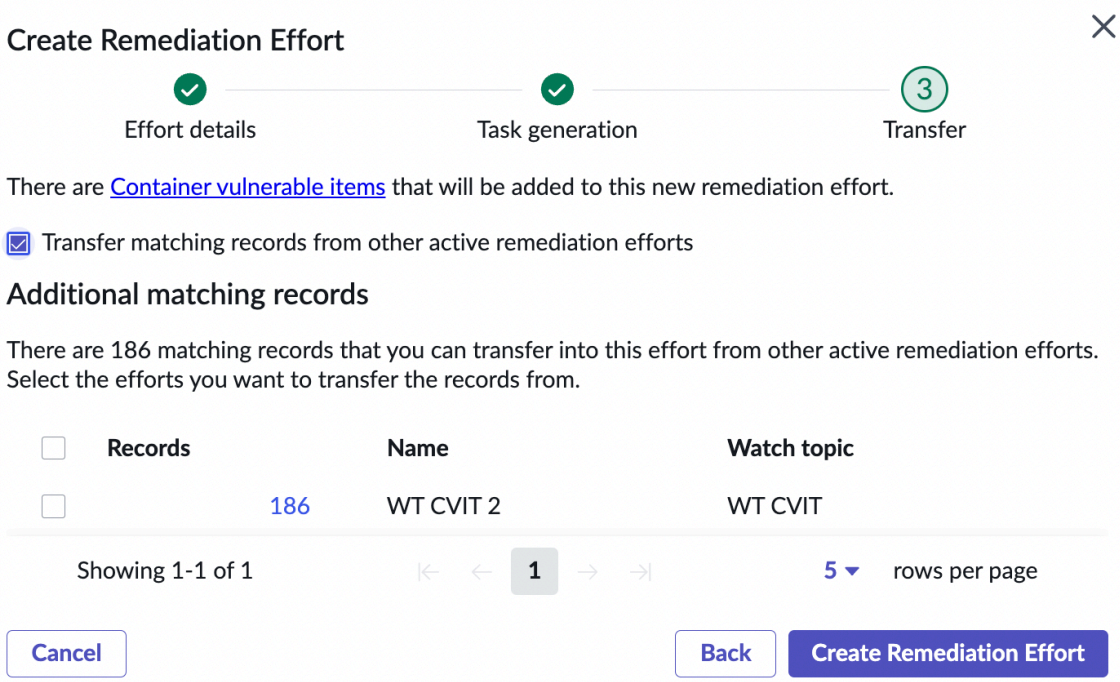
   추가할 새 활성 기록이 없는 경우 다음 텍스트가 표시됩니다.

   # ### ## ### ### # ## ## ### ## ### ####.

   이 작업으로 이전할 수 있는 추가 기록은 #### ## ## 아래에 나열됩니다 .

   다른 활성 정정 작업에서 일치하는 기록 전송 확인란을 선택한 다음, 다른 활성 정정 작업에서 이전할 기록의 확인란을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



정정 작업량 생성을 클릭하면 잠시 후 새로운 정정 작업이 표시됩니다. 기록 수에 따라 새 기록을 채우는 데 시간이 걸릴 수 있습니다. 기록이 아직 채워지고 있는지는 메시지가 표시됩니다.

새 정정 작업은 기존 작업에서 이전하기 위해 선택한 기록 외에 새 정정 작업을 생성하는 데 사용된 감시 주제에서 사용할 수 있는 모든 기록을 사용하여 생성됩니다.

기존 작업에서 이전할 기록을 선택하고 기존 작업이 모든 기록을 새 작업으로 이전하는 경우, 기록을 이동한 원본 정정 작업이 종결됩니다. 정정 작업과 연결된 정정 작업이 기록 전송으로 인해 어떤 영향을 받는지에 대한 자세한 내용은 다음 문서를 취약성 대응 작업 공간의 정정 작업, 정정 작업 및 기록의 수명주기참조하십시오.

주:
감시 주제에서 사용할 수 있는 기록이 없거나 이전을 위해 선택한 기록이 없는 경우 정정 작업량 생성 버튼이 비활성화됩니다.

Populate Efforts 예약된 작업은 10분마다 실행되어 선택한 조건에 따라 위젯에 데이터를 채웁니다.

정정 진행률 탭을 클릭하여 정정 진행률을 확인합니다. 기록 유형, 위험 점수, 위험 등급, 정정된 기록의 백분율, 지연 및 비지연 상태의 기록, 총 기록 수, 감시 주제에 사용된 조건, 정정 상태 등의 상세 정보를 보려면 항목을 클릭하십시오. 정정 대상 및 정정 상태와 같은 정정 상태 정보는 취약한 항목 테이블에서 롤업됩니다. 가장 높은 기록 위험 점수는 취약성 계산기 테이블에서 롤업되고 위험 점수는 취약성 롤업 계산기 〉 정정 작업 롤업.

정정 작업 탭에는 모든 유형의 문제에 대한 작업이 표시됩니다. 다음 예약된 작업이 실행될 때 필드가 채워집니다. 15분마다 자동으로 실행됩니다.

- 애플리케이션 취약한 항목 값을 취약성 및 그룹에 롤업합니다.
- 컨테이너 취약한 항목 값을 취약성 및 그룹에 롤업합니다.
- 테스트 결과 값을 테스트 결과 그룹 및 구성 테스트에 롤업합니다.
- 취약한 항목 값을 취약성 및 그룹에 롤업합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

목록 뷰에서 정정 작업, 정정 작업, 취약한 항목, 구성, 테스트 결과 등을 볼 수 있습니다. 정정 작업 또는 취약한 항목을 열고 상세 정보 페이지를 볼 수 있습니다. 추가 작업 줄임표를 클릭하고 조사 시작을 클릭하여 정정 작업을 해결합니다.

10. 옵션: 기존의 반복 정정 작업을 편집할 수도 있습니다.

    (Optional) 감시 주제에 대한 기존 반복 정정 작업이 있는 경우, 감시 주제의 오른쪽 상단에 있는 메뉴에서 반복 작업 편집을 사용할 수 있습니다. 반복 작업을 편집하려면 이 옵션을 선택합니다.

    변경하고 정정 작업 기록에 저장해도 감시 주제에서 이미 생성한 다른 정정 작업에는 영향을 주지 않습니다.

의 정정 작업에서 요청 시 정정 작업 생성 취약성 관리자 작업 공간

정정 작업에서 요청 시 정정 작업을 생성합니다. 요청 시 정정 작업을 생성하는 경우 추가할 기록을 수동으로 선택합니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin

이 태스크 정보
버전 18.0 취약성 대응의 경우 정정 작업의 기록 뷰에서 정정 작업을 생성할 수 없습니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 취약성 관리자 작업 공간.
2. 홈페이지가 표시된 작업 공간의 왼쪽 상단에서 목록 뷰 아이콘을 클릭하여 목록 방문 페이지를 표시합니다.
3. 정정 작업에서 활성 또는 모두를 클릭합니다.
4. 표시되는 목록에서 기록을 클릭하여 엽니다.
   기록의 개요 탭이 표시됩니다.
5. 취약한 항목 탭을 클릭합니다.
   기록 목록이 표시됩니다.
6. 새 정정 작업을 생성하려면 번호 열에서 추가할 기록을 선택합니다.
7. 정정 작업 생성을 클릭합니다.
8. 표시되는 모달의 필드에 내용을 입력합니다.
9. 생성을 클릭합니다.
10. 새 정정 작업이 선택한 활성 기록과 함께 표시됩니다.

에서 반복 정정 작업 생성 취약성 관리자 작업 공간

설정한 날짜 및 시간에 자동으로 생성되는 반복적인 정정 작업을 생성하고 예약할 수 있습니다.

시작하기 전에
필요한 역할:

- 호스트 취약 항목(VIT)의 경우 sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin
- 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_sec_manager

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.vulnerability_analyst 또는 sn_vul_container.vulnerability_admin
- 구성 테스트 결과(CTR)에 대한 sn_vulc.admin

이 태스크 정보
발생할 수 있는 취약성을 추적하여 즉각적이고 지속적인 주의가 필요한 주기적인 정정 작업을 일정에 따라 자동으로 생성할 수 있습니다.

버전 18.0부터는 비활성 감시 주제에 대해 반복적인 정정 작업을 생성할 수 없으므로 반복 작업 생성 옵션이 비활성화됩니다. 반복 작업이 이미 예약된 감시 주제를 비활성화하면 감시 주제가 활성화될 때까지 새 정정 작업이 생성되지 않습니다. 또한 오른쪽 상단에 작업량 반복 및 다음 반복 날짜 상세 정보가 사라집니다. 주시 주제를 활성화하면 예정된 일정에 따라 정정 작업이 생성됩니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 취약성 관리자 작업 공간 〉 주시 주제.
2. 감시 주제 페이지에서 반복 정정 작업을 생성할 감시 주제를 선택합니다.

   감시 주제당 하나의 반복 정정 작업을 생성할 수 있습니다.

   주:
   반복되는 정정 작업의 기록을 새 정정 작업으로 이전할 수 없습니다. 그러나 기존의 반복되지 않는 정정 작업에서 새 정정 작업으로 기록을 이전할 수 있습니다. 기록 이전에 대한 자세한 내용은 을 참조하십시오 의 정정 작업으로 기록 전송 취약성 관리자 작업 공간 .

3. 감시 주제의 정정 작업 생성 목록에서 오른쪽 위에 있는 반복 작업 생성을 선택합니다.

   반복 작업 생성 모달이 표시됩니다.

4. 1단계, 작업 상세 정보에서 필수 필드를 입력합니다.

   간단한 설명 필드에 반복 정정 작업을 설명하는 텍스트를 입력하여 해당 작업을 찾고 작업 목록에서 추적하는 데 도움이 됩니다.

   설명 필드에 정정 작업 목록에서 쉽게 찾을 수 있도록 작업의 컨텍스트에 대한 추가 텍스트를 입력합니다. 예를 들어, ## ## ### ###입니다.

5. 다음을 클릭합니다.
   작업 생성 상세 정보가 표시됩니다.
6. 2단계, 작업 생성의 목록에서 한 가지 방법을 선택하여 이 정정 작업이 생성된 후 생성하는 정정 작업에 취약한 항목을 번들로 묶습니다.
   - 할당 그룹별
   - 할당 그룹 및 구성 항목별
   - 할당 그룹 및 취약성별
   - 없음(정정 작업이 생성되지 않음). 이 작업에 대한 정정 작업에 수동으로 기록을 추가하려면 이 방법을 사용합니다. 의 정정 작업에서 요청 시 정정 작업 생성 취약성 관리자 작업 공간 문서를 참조하십시오.
7. 중복 호스트 취약한 항목을 자동으로 새로 고치려면 생성된 정정 작업에 대해 중복된 취약한 항목 자동 새로 고침 옵션을 선택해야 합니다.

   주:
   이 확인란은 호스트 취약성에 대해서만 사용할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

8. 다음을 클릭하여 계속합니다.
9. 3단계, 반복에서 빈도를 선택합니다.

   a. 반복 일정을 정의합니다.

      목록을 사용하여 정정 작업을 생성할 월/일/시간/분을 선택합니다. 일정을 예약할 시간대는 기본적으로 사용자의 시간대입니다.

      주:
      취약성이 많은 경우 업무 외 시간에 생성을 설정하는 것이 좋습니다.

      달의 마지막 날에 작업을 생성하려는 경우 예약된 작업은 달의 마지막 날에 반복 정정 작업을 생성합니다. 월이 31일로 되어 있지 않으면 메시지가 표시됩니다.

   b. 옵션: 이 정정 작업에서 취약성을 활성 취약성으로 이월 을 선택하여 생성되는 각 후속 정정 작업으로 이월합니다.

10. 되풀이 예약을 클릭합니다.
    반복 정정 기록이 생성되었다는 메시지가 표시됩니다. 새 정정 작업은 즉시 표시되지 않으며 예약했을 때 생성됩니다. 예약된 작업에 의해 생성된 후 목록에 표시됩니다.

    정정 작업이 생성될 날짜는 해당 감시 주제에 표시됩니다. 정정 작업과 연결된 정정 작업이 기록 전송에 의해 어떤 영향을 받는지에 대한 자세한 내용은 다음 문서를 참조하십시오 취약성 대응 작업 공간의 정정 작업, 정정 작업 및 기록의 수명주기.

의 정정 작업으로 기록 전송 취약성 관리자 작업 공간

에서 기존 정정 작업의 기록을 새 정정 작업으로 이전할 수 있습니다 취약성 관리자 작업 공간.

시작하기 전에
신속하게 해결하려는 제로 데이 위협 또는 매우 중요한 취약성에 직면한 경우 이 취약성에 대해 이미 가지고 있는 활성 레코드를 하나의 정정 작업으로 통합할 수 있습니다. 그러나 각 기록은 하나의 작업으로만 이루어질 수 있으며 기록은 감시 주제 간에 겹칠 수 있습니다. 따라서 이러한 기록을 모두 수집하려면 여러 기존 작업에서 하나의 정정 작업으로 이러한 기록을 이전해야 합니다.

예를 들어 우선순위가 높은 취약성이 하나 있는 정정 노력을 만들었다고 가정해 보겠습니다. 이 취약성은 광범위하고 사용자 환경의 다른 영역에 잠재적으로 영향을 미치기 때문에 기존 정정 작업에 이미 이 취약성과 연결된 기록이 있을 수 있습니다. 이러한 기록을 모두 하나의 정정 작업에 통합하려면 기존 정정 작업의 기록을 새 정정 작업으로 이전할 수 있습니다.

주:
반복되는 정정 작업의 기록을 새 정정 작업으로 이전할 수 없습니다. 자세한 내용은 에서 반복 정정 작업 생성 취약성 관리자 작업 공간 문서를 참조하십시오.

필요한 역할:

- 호스트 취약 항목(VIT)의 경우 sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin
- 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_sec_manager
- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.vulnerability_analyst 또는 sn_vul_container.vulnerability_admin
- 구성 테스트 결과(CTR)에 대한 sn_vulc.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 취약성 관리자 작업 공간.
2. 주시 주제 아이콘을 선택합니다.
3. 감시 주제 페이지에서 반복 정정 작업을 생성할 감시 주제를 선택합니다.
4. 정정 작업량 생성을 클릭합니다.
   정정 작업량 생성 모달이 표시됩니다.
5. 1단계, '작업 상세 정보'에서 필수 필드를 입력합니다.

   간단한 설명 필드에 반복 정정 작업을 설명하는 텍스트를 입력하여 해당 작업을 찾고 작업 목록에서 추적하는 데 도움이 됩니다.

   설명 필드에 정정 작업 목록에서 쉽게 찾을 수 있도록 작업의 컨텍스트에 대한 추가 텍스트를 입력합니다. 예를 들어 `## Log4J ######`.

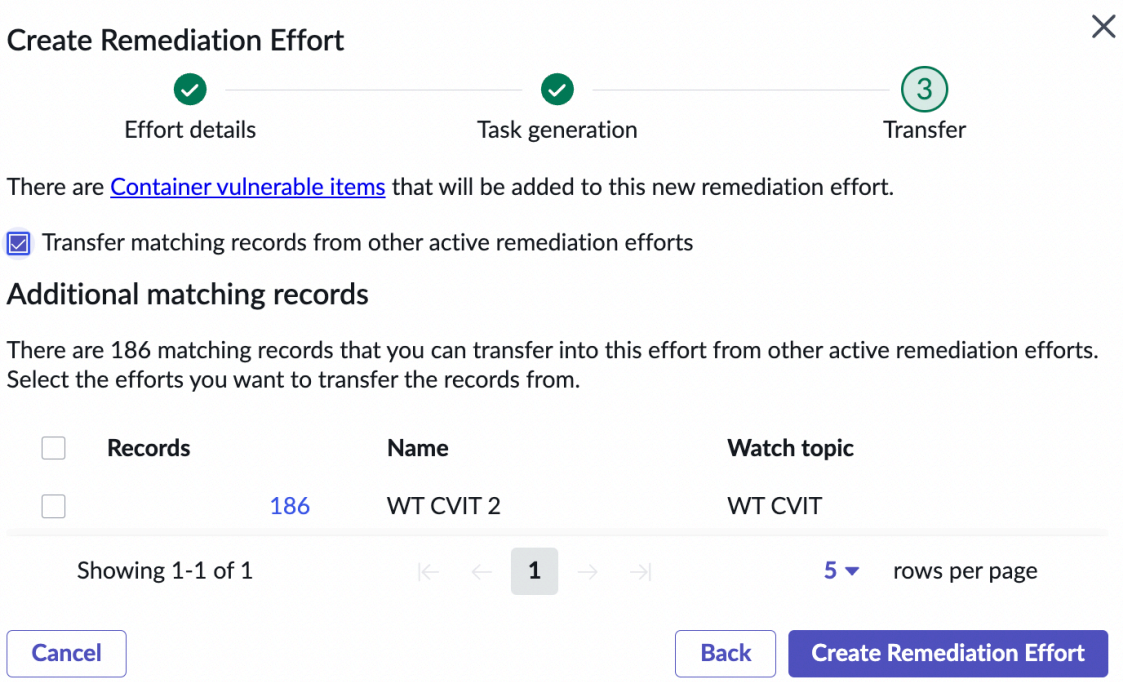
   a. 이름 필드에 새 정정 작업의 이름을 입력합니다.
      기본적으로 주시 주제 이름이 표시됩니다.

   b. 설명 필드에 정정 작업 목록에서 이 정정 작업을 쉽게 찾을 수 있는 텍스트를 입력합니다.

6. 다음을 클릭합니다.
   작업 생성 상세 정보가 표시됩니다.
7. 2단계, 작업 생성의 목록에서 한 가지 방법을 선택하여 이 정정 작업이 생성된 후 생성하는 정정 작업의 기록을 번들로 묶습니다.
   - 할당 그룹별
   - 할당 그룹 및 구성 항목별
   - 할당 그룹 및 취약성별
   - 없음(정정 작업이 생성되지 않음). 이 작업에 대한 정정 작업에 수동으로 기록을 추가하려면 이 방법을 사용합니다. 의 정정 작업에서 요청 시 정정 작업 생성 취약성 관리자 작업 공간 문서를 참조하십시오.
8. 중복된 취약한 항목을 자동으로 새로 고치려면 생성된 정정 작업에 대해 중복된 취약한 항목을 자동으로 새로 고침 옵션을 선택해야 합니다.
9. 다음을 클릭합니다.
10. 3단계, '이전'에서 정정 작업에 추가할 기록 수를 확인하고 다른 활성 정정 작업에서 이전할 수 있는 기록 수를 확인합니다.
11. 다른 작업에서 기록을 이전하려면 목록에서 원하는 기록의 확인란을 선택합니다.

    다른 활성 정정 작업에서 일치하는 기록 전송 확인란을 선택한 다음, 다른 활성 정정 작업에서 이전할 기록의 확인란을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



12. 정정 작업량 생성을 클릭합니다.

잠시 후 새 정정 작업이 표시됩니다. 기록 수에 따라 시간이 걸릴 수 있습니다. 기록이 채워지고 있다는 메시지가 표시됩니다.

새 정정 작업은 기존 작업에서 이전하기 위해 선택한 기록 외에 새 정정 작업을 생성하는 데 사용된 감시 주제에서 사용할 수 있는 모든 기록을 사용하여 생성됩니다.

기존 작업에서 이전할 기록을 선택하고 기존 작업이 모든 기록을 새 작업으로 이전하는 경우, 기록을 이동한 원본 정정 작업이 종결됩니다.

주:
감시 주제에서 사용할 수 있는 기록이나 이전을 위해 선택한 기록이 없는 경우 정정 작업량 생성 버튼이 비활성화됩니다.

정정 작업과 연결된 정정 작업이 기록 전송에 의해 어떤 영향을 받는지에 대한 자세한 내용은 기록 전송 또는 기록 이월을 참조하십시오.

라이브러리에 보정 통제 추가

취약성 관리자 또는 분석가는 호스트 취약한 항목의 위험 감소와 정정 작업에 적용할 수 있는 보상 통제 목록을 의 취약성 관리자 작업 공간보상 통제 라이브러리에 추가합니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin

이 태스크 정보
일반적으로 사용되는 일부 보상 컨트롤은 기본 시스템과 함께 제공됩니다. 다음으로 이동하여 이러한 보상 컨트롤을 볼 수 있습니다. 작업 공간 〉 취약성 관리자 작업 공간 〉 목록 〉 라이브러리 〉 보상 통제. 요구 사항에 따라 이러한 보상 통제를 활성화하거나 비활성화할 수 있습니다.

주:
보상 제어 기능은 호스트 취약성에 대해서만 사용할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 작업 공간 〉 취약성 관리자 작업 공간.
2. 목록 페이지의 라이브러리 아래에서 보상 컨트롤을 선택합니다.
3. 새로 만들기를 클릭합니다.
4. 보상 통제 생성 양식의 필드에 내용을 입력합니다.

보상 통제 양식 필드 생성

필드	설명
이름	예외 요청 모달의 보상 통제 드롭다운에 옵션으로 표시되는 보상 통제의 이름입니다.
설명	보상 통제에 대한 세부 정보를 제공하는 간략한 정보입니다.
활성	보상 통제의 상태입니다. 활성 통제만 예외 요청 모달의 보상 통제 드롭다운에 나타납니다.

5. 저장을 선택합니다.
6. 라이브러리 아래의 보상 컨트롤 목록에서 원하는 보상 컨트롤을 선택하고 보상 컨트롤 편집, 활성화 또는 비활성화를 선택한 다음 저장을 클릭하여 보상 컨트롤을 수정합니다.
   모든 활성 보상 통제는 위험 감소 요청에 대한 예외 요청 모달의 보상 통제 드롭다운에 옵션으로 나타납니다.

다음에 수행할 작업

v21.0 of 취약성 대응부터 라이브러리에 보상 컨트롤을 추가한 후 보상 컨트롤을 CVE 또는 TPE와 연결할 수 있습니다. 보상 컨트롤을 연결하는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 위험 감소 요청을 위해 CVE 또는 TPE와 보상 통제 연결.

관련 정보

위험 감소를 위한 보상 통제 이해

CVE 또는 TPE에 대한 위험 감소 사용 안 함 또는 사용

위험 감소 요청을 위해 CVE 또는 TPE와 보상 통제 연결

보상 통제가 위험 점수 및 만료 날짜에 미치는 영향

위험 감소 요청을 위해 **CVE** 또는 TPE와 보상 통제 연결

취약성 관리자 또는 분석가는 취약성으로 인한 위험을 줄이는 데 사용할 수 있는 CVE(공통 취약성 항목) 또는 TPE(외부 공급업체 항목) 취약성 관리자 작업 공간와 관련 보상 통제를 연결할 수 있습니다.

시작하기 전에

필요한 역할: sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin

이 태스크 정보

- 보상 통제를 CVE 또는 TPE에 연결하지 않으면 모든 활성 통제가 예외 요청 양식의 보상 통제 선택 필드에 나타납니다.
- 보상 통제를 CVE에 연결하면 이 보상 통제는 CVE에 매핑된 TPE와 자동으로 연결됩니다.

주:
보상 제어 기능은 호스트 취약성에 대해서만 사용할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 작업 공간 〉 취약성 관리자 작업 공간.
2. 목록 페이지의 라이브러리에서 컨트롤을 연결할 다음 중 하나를 엽니다.
   - CVE 목록의 **CVE**.
   - TPE 목록의 **TPE**입니다.
3. 컨트롤 연결을 선택합니다.

   주:
   통제 연결 버튼은 CVE 또는 TPE에 대해 위험 감소가 활성화된 경우에만 나타납니다. 즉, CVE 또는 TPE에 대해 위험 감소가 활성화된 경우에만 보상 통제를 연결할 수 있습니다. 컨트롤 연결 버튼이 표시되지 않으면 위험 감소 사용을 선택합니다.

4. 통제 연결 모달에서 위험 감소를 위해 CVE 또는 TPE와 관련된 취약성에 적용할 수 있는 보상 통제를 선택합니다.
5. 제출을 선택합니다.
   - 연결된 보상 통제는 CVE 및 TPE의 기록 뷰에 있는 적용 가능한 보상 통제 탭에 나타납니다.
   - 정정 소유자가 위험 감소를 요청하는 동안 이러한 관련 보상 통제는 예외 요청 모달의 보상 통제 선택 필드에 표시됩니다.

관련 정보

위험 감소를 위한 보상 통제 이해

CVE 또는 TPE에 대한 위험 감소 사용 안 함 또는 사용

라이브러리에 보정 통제 추가

보상 통제가 위험 점수 및 만료 날짜에 미치는 영향

CVE 또는 TPE에 대한 위험 감소 사용 안 함 또는 사용

취약성 관리자 및 분석가는 의 CVE(공통 취약성 항목) 또는 TPE(외부 공급업체 항목)와 연관된 호스트 취약성에 대한 위험 감소 요청을 비활성화하거나 활성화할 수 있습니다 취약성 관리자 작업 공간.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
CVE 및 TPE에 대한 위험 감소는 기본적으로 활성화되어 있습니다.

주:
보상 제어 기능은 호스트 취약성에 대해서만 사용할 수 있습니다.

프로시저

1. 다음으로 이동 작업 공간 〉 취약성 관리자 작업 공간.
   목록 페이지의 라이브러리에서 위험 감소 요청을 비활성화하려는 다음 중 하나를 엽니다.
   - CVE 목록의 **CVE**.
   - TPE 목록의 **TPE**입니다.
2. 위험 감소 비활성화를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

정정 소유자는 이 CVE 또는 TPE와 관련된 호스트 취약한 항목에 대한 위험 감소를 요청할 수 없습니다. 즉, 이유 가 예외 요청 모달에서 ## ## ## ##로 선택되면 위험 감소 요청 확인란이 표시되지 않습니다.

3. 호스트 취약한 항목에 대한 위험 감소 요청을 활성화하려면 위험 감소 활성화를 선택합니다.

관련 정보

위험 감소를 위한 보상 통제 이해

라이브러리에 보정 통제 추가

위험 감소 요청을 위해 CVE 또는 TPE와 보상 통제 연결

보상 통제가 위험 점수 및 만료 날짜에 미치는 영향

에서 기록 및 정정 작업을 다시 스캔 취약성 관리자 작업 공간

예약된 스캔 주기 사이에 정정 작업 및 기록이 해결되었는지 확인하려면 요청 시 다시 스캔을 ServiceNow AI Platform 시작합니다.

필요한 역할: sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin

재검색을 통해 정정 활동, 패치 및 기타 작업이 구성 항목(CI)의 특정 취약성을 성공적으로 수정했는지 확인할 수 있습니다.

Rapid7 및 Qualys 스캐너는 애플리케이션에서 기본적으로 비활성화되어 있습니다취약성 대응. 이러한 애플리케이션을 소스로 사용하는 취약한 항목 또는 정정 작업에서 다시 검색을 수행하려고 하면 다시 검색 버튼을 사용할 수 없습니다.

이러한 스캐너를 활성화하려면 sn_vul.vulnerability_admin 역할을 가진 사용자가 다음과 같이 하십시오.

1. 다음으로 이동 모두 〉 취약성 대응 〉 취약성 스캐닝 〉 스캐너.
2. 활성화할 스캐너 제품을 찾고 레코드를 클릭하여 엽니다.
3. 활성 확인란을 선택합니다.
4. 업데이트를 클릭합니다.

활성화한 제품은 다음 임포트 후 취약한 항목 및 정정 작업 기록의 소스 필드에 표시되며, 다시 스캔 은 UI 작업으로 사용할 수 있습니다.

재스캔은 다음 취약성 관리자 작업 공간의 통합을 통해 기록 및 정정 작업에 대해 지원됩니다. 자세한 내용은 다음 항목을 참조하십시오.

- 작업 공간에서 취약한 항목 취약성 대응 다시 스캔 Rapid7
- 작업 공간에서 취약한 항목 취약성 대응 다시 스캔 Qualys
- 작업 공간에서 취약성 대응 취약한 항목 다시 스캔 Tenable.ioTenable.sc

취약한 항목 및 정정 작업 기록에서 취약성 관리자 작업 공간 재스캔을 시작하려면 기록에 지원되는 스캐너가 소스로 필요합니다.

소스별로 기록을 표시하는 필터링된 목록을 만드는 것이 좋습니다. 목록을 만드는 방법에 대한 예는 을 참조하십시오 사용자 지정 기록 목록 만들기 .

에 있는 기록의 정정 속성 재평가 취약성 관리자 작업 공간

의 취약성 관리자 작업 공간기록 세트(VIT, VIT, CVIT 또는 TR)에 대한 할당, 정정 목표 날짜, 정정 작업, 예외 및 위험 점수를 평가합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할:

- 호스트 취약 항목(VIT)의 경우 sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin
- 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_sec_manager
- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.vulnerability_analyst 또는 sn_vul_container.vulnerability_admin
- 구성 테스트 결과(CTR)에 대한 sn_vulc.admin

이 태스크 정보
Vulnerability Response 버전 23.0 이전에는 최신 할당, 정정 목표 날짜, 위험 점수 및 정정 작업을 얻기 위해 모든 기록에 규칙을 적용해야 했으며, 이는 시간이 많이 걸리는 프로세스였습니다. 버전 23.0부터 특정 기록에 대해 이러한 속성을 선택적으로 평가하고 업데이트하여 처리 시간을 단축할 수 있습니다. 또한 이러한 업데이트된 속성을 기반으로 정정 프로세스를 구체화할 수 있습니다. Vulnerability Response v24.0.6부터 에서 선택한 기록 취약성 관리자 작업 공간에 대한 예외 규칙을 평가할 수 있습니다.

프로시저

1. 다음으로 이동 작업 공간 〉 취약성 관리자 작업 공간.
2. 목록 페이지의 다음 목록 중 하나에서 활성 또는 모두 목록을 엽니다.
   - 호스트 취약한 항목
   - 애플리케이션 취약한 항목
   - 컨테이너 취약한 항목
   - 구성 테스트 결과
3. 옵션: 모달에서 선택한 항목 옵션을 선택하여 선택한 기록만 업데이트하려는 기록의 확인란을 선택합니다.
4. 재평가 버튼을 선택합니다.
5. 정정 속성 재평가 및 업데이트 모달에서 선택한 기록에 대해 업데이트할 속성을 선택합니다.

   주:
   속성을 선택하면 종속 속성이 자동으로 선택됩니다.

6. 적용을 선택합니다.

결과
선택한 기록의 속성이 업데이트됩니다. 업데이트된 정정 속성의 이전 값과 최신 값에 대한 기록의 작업 메모를 확인할 수 있습니다.

정정 작업 생성 없이 예외 규칙에 따른 취약한 항목(VIT)의 직접 연기

예외 규칙은 취약한 항목(VIT)에 직접 적용되므로 정정 작업을 생성하는 프로세스가 제거됩니다. 자동 예외 규칙 열이 양식 뷰에 추가되어 취약한 항목(VIT)에 적용된 현재 예외 규칙이 채워집니다

예외 규칙/재적용 승인:

특정 취약한 항목(VIT)에 대해 예외 규칙이 생성됩니다. 이 항목은 오픈, 조사 중, 초기 구현 대기 중 상태에 있습니다. 규칙이 승인되면 예외 규칙을 다시 적용하는 매일, 매일 밤 예약된 작업에 의해 처리됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예약된 작업이 실행될 때 VIT가 예외 규칙에 잘못 매핑되어 VIT가 지연(연기)되는 경우 예약된 작업은 VIT를 다시 열어 새 예외 규칙을 다시 적용합니다.

이후 실행 순서가 있는 새 규칙을 활성화하여 이전 규칙을 대체할 수도 있습니다.

주:
연기 종료 날짜는 기본적으로 12개월로 설정되어 있으며 예외 관리 구성 설정 페이지에서 필요에 따라 편집할 수 있습니다. 기본 날짜 이후의 지연 날짜를 선택하려고 하면 시스템에서 오류가 발생합니다.

취소 또는 삭제된 예외 규칙 처리:

이전 예외 규칙이 취소되거나 삭제되면 다음을 위한 백그라운드 작업이 트리거됩니다.

- 연결된 모든 VIT를 엽니다.
- 규칙이 취소되면 예외 규칙을 초안 상태로 이동합니다.
- VIT에 새 예외 규칙을 적용합니다. (적용 가능한 예외 규칙이 있는 경우 VIT가 해당 규칙과 연결되고 VIT 상태가 지연됩니다.)

새 **VIT** 작성(삽입):

새 VIT가 생성되면(예: 수집) 예외 규칙이 자동으로 할당됩니다. 새 VIT도 예외 규칙이 취소될 때와 동일한 프로세스에 따라 동일한 추론 및 종료 날짜로 지연됩니다.

VM 관리자 작업 공간에서 클릭 가능한 링크를 사용하여 예외 규칙에 직접 액세스할 수 있으며, 이를 통해 사용자는 지정된 VIT에 영향을 주는 예외 규칙을 확인할 수 있습니다.

에서 목록 뷰 사용 취약성 관리자 작업 공간

취약성 및 보안 관리자와 분석가는 목록 취약성 관리자 작업 공간 뷰를 사용하여 기록의 정정 진행률을 보고, 취약성 대응 기록을 드릴다운하고, 승인 요청 및 예외의 상태를 볼 수 있습니다.

시작하기 전에
필요한 역할:

- 호스트 취약 항목(VIT)의 경우 sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin
- 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_sec_manager
- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.vulnerability_analyst 또는 sn_vul_container.vulnerability_admin
- 구성 테스트 결과(CTR)에 대한 sn_vulc.admin

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 취약성 관리자 작업 공간.
2. 홈페이지가 표시된 작업 공간의 왼쪽 상단에서 목록 아이콘을 클릭합니다.
3. 옵션: 내 목록을 클릭하여 목록을 만듭니다.
   목록을 만드는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 사용자 지정 기록 목록 만들기.
4. 목록 페이지에서 수행할 수 있는 작업은 다음 테이블을 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

UI 작업	설명
정정 작업량 열기	정정 작업 목록에서 활성을 선택한 상태에서 정정 작업 링크를 클릭하여 엽니다. 정정 작업은 감시 주제와 연결된 기록 세트입니다. 정정 작업에 나열된 기록은 정적입니다. 새 임포트 데이터 또는 주시 주제에 대한 변경 내용으로 업데이트되지 않습니다. 정정 작업 기록의 관련 목록 항목을 사용하면 연결된 기록의 전반적인 정정 진행률과 상태를 볼 수 있습니다. 정정 작업에서 수행할 수 있는 UI 작업 및 자세한 내용은 문서를 참조하십시오 정정 작업 기록 사용.
목록이 표시된 번호 열의 왼쪽에서 행을 롤오버하고 기록에 대한 작은 정보 아이콘 **(i)** 을 클릭합니다.	기록에 대한 상세 정보는 페이지의 오른쪽 패널에 표시됩니다. 자세한 내용은 다음과 같습니다. ○ 할당 그룹 ○ 취약성 ○ 담당자 ○ 짧은 설명 ○ 설명 필드를 편집할 수 있습니다. 활성 확인란이 표시되면 기록을 활성화하거나 비활성화할 수 있습니다. 업데이트를 클릭하여 변경 내용을 저장합니다.
목록 새로 고침	페이지 오른쪽 위에 있는 새로 고침 아이콘을 사용하여 현재 페이지를 다시 로드합니다.
너비 재설정	기어 아이콘을 클릭하여 목록의 열 너비를 조정합니다. 원본 목록의 사본이 내 목록 아래에 저장됩니다.
표시된 페이지의 URL을 복사합니다.	다른 곳에서 사용할 URL을 복사합니다.
페이지 익스포트	모달에서 파일 및 배달 유형을 입력하고 내보내기를 클릭합니다.
페이지의 데이터에 대한 필터를 구체화합니다.	열을 선택하고 세 개의 세로 점 메뉴를 확장하여 열의 데이터를 추가로 필터링하는 옵션을 봅니다. 예를 들어, 활성 정정 작업 목록에서 할당 그룹 열을 특정 할당 그룹을 기준으로 필터링하는 것을 선호할 수 있습니다.
열의 행에서 항목 또는 일치 항목을 필터링합니다.	열에서 셀을 선택하고 다음 중 하나를 선택하여 표시된 데이터를 구체화합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

UI 작업	설명
	○ 일치 표시 - 열에서 선택한 셀과 일치하는 항목만 표시합니다. ○ 필터링 - 열에서 선택한 셀과 일치하는 항목을 열에서 필터링합니다.

5. 오른쪽 위에 있는 새로 만들기 버튼을 클릭하여 아래의 *Application Vulnerable items*활성 또는 모두 목록에서 애플리케이션 취약한 항목을 생성합니다.

사용자 지정 기록 목록 만들기

에서 사용자 지정 목록을 생성할 수 있습니다 취약성 관리자 작업 공간.

시작하기 전에
필요한 역할:

- 호스트 취약 항목(VIT)의 경우 sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin
- 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_sec_manager
- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.vulnerability_analyst 또는 sn_vul_container.vulnerability_admin
- 구성 테스트 결과(CTR)에 대한 sn_vulc.admin

프로시저

1. 다음으로 이동 작업 공간 〉 취약성 관리자 작업 공간.
2. 목록 아이콘을 선택하고 내 목록을 클릭합니다.
3. 새 목록을 선택합니다.
4. 새 목록 모달에서 기존 목록에서 시작을 클릭하고 목록 선택 목록에서 템플릿으로 사용할 기존 목록을 검색합니다.
5. 목록 이름을 편집합니다.
6. 필터를 추가합니다.
   예를 들어, 재스캔을 모니터링하려는 특정 스캐너에 대한 활성 기록 목록을 생성할 수 있습니다. Active# true이고 Source contains (### ##) 필터를 사용할 수 있습니다.
7. 목록에 표시할 열을 편집합니다.
8. 생성을 클릭합니다.
   새 목록이 표시됩니다.
9. 또는 **Create your** own(직접 생성)을 클릭하고 이름을 입력한 다음 **Select** Source(소스 선택)를 클릭합니다.
10. 필드에 입력을 시작하고 새 목록에 대해 표시되는 소스 중에서 선택합니다.
11. 생성을 클릭합니다.
    새 목록이 표시됩니다.

    > **주:**
    > 목록 모듈을 나가면 종료할 때 표시되는 목록이 돌아올 때 표시되는 목록입니다.

12. 목록을 삭제하려면 목록이 표시된 상태에서 페이지 오른쪽 상단의 기어 아이콘을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

에서 수동으로 정정 작업 생성 취약성 관리자 작업 공간

의 취약성 대응v25.0.4부터 의 목록 페이지에 취약성 관리자 작업 공간있는 호스트 취약한 항목, 애플리케이션 취약한 항목, 컨테이너 취약한 항목 및 구성 테스트 결과 목록에서 수동으로 업데이트 적용 작업을 생성할 수 있습니다. 홈페이지에서 시각화를 클릭할 때 나타나는 드릴다운 목록에서 정정 작업을 만들 수도 있습니다.

시작하기 전에

필요한 역할:

- 호스트 취약 항목(VIT)에 대한 sn_vul.write_all, sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin
- 애플리케이션 취약한 항목(AVIT)의 경우 sn_vul.app_write_all 또는 sn_vul.app_sec_manager
- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.write_all, sn_vul_container.vulnerability_analyst 또는 sn_vul_container.vulnerability_admin
- 구성 테스트 결과(TR)의 경우 sn_vulc.write 또는 sn_vulc.admin

이 태스크 정보

에서 취약성 관리자 작업 공간 정정 작업(RT)을 수동으로 생성하면 기록(VIT, CVIT, AVIT 또는 TR)을 실시간으로 동적으로 정정 작업으로 그룹화할 수 있으므로 정정 작업 관리를 세부적으로 제어할 수 있습니다.

정정 작업을 수동으로 생성할 때 다음 작업을 수행할 수 있습니다.

- 정정 작업 규칙 기준 이외의 기준으로 취약한 항목을 그룹화합니다. 예를 들어 특정 관리자에 대한 정정 작업을 만들거나 다른 취약성을 포함하는 랜섬웨어와 같은 새로운 활성 익스플로잇에 대한 정정 작업을 만들 수 있습니다.
- 그룹화되지 않은 기록을 그룹화합니다.
- 정정 작업 규칙이 비활성 상태입니다.

프로시저

1. 다음으로 이동 작업 공간 〉 취약성 관리자 작업 공간 〉 목록.
2. 목록 페이지의 다음 목록 중 하나에서 활성 또는 모두 목록을 엽니다.
   - 호스트 취약한 항목
   - 애플리케이션 취약한 항목
   - 컨테이너 취약한 항목
   - 구성 테스트 결과
3. 옵션: 업데이트할 기록의 확인란을 선택한 다음, 정정 작업 생성 모달의 기록 선택 필드에서 선택한 항목 옵션을 선택합니다.
4. 정정 작업 생성을 선택합니다.
5. 정정 작업 생성 모달에서 다음 상세 정보를 입력합니다.

정정 작업 모달 생성

필드	설명
기록 선택	○ 선택한 항목: 선택한 기록만 업데이트합니다. ○ 모든 항목: 목록의 모든 기록을 업데이트합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
간단한 설명	정정 작업에 대한 간략한 메모입니다.
그룹화 기준	선택 항목은 다음과 같습니다. ○ 할당 그룹: 할당 그룹이 동일한 기록은 하나의 정정 작업으로 그룹화됩니다. ○ 할당 그룹 및 구성 항목: 할당 그룹 및 구성 항목이 동일한 기록이 하나의 정정 작업으로 그룹화됩니다. ○ 할당 그룹 및 취약성: 할당 그룹 및 취약성이 동일한 기록은 하나의 정정 작업으로 그룹화됩니다. ○ 할당 그룹 및 위험 등급: 할당 그룹 및 위험 등급이 동일한 기록은 하나의 정정 작업으로 그룹화됩니다.
다른 정정 작업의 기록 관리	선택 항목은 다음과 같습니다. ○ 새 정정 작업에 대한 기록 건너뛰기: 다른 정정 작업의 일부인 기록에 대해서는 아무 작업도 수행되지 않습니다. ○ 새 정정 작업으로 이동: 다른 정정 작업의 일부인 기록은 새 정정 작업으로 전송됩니다. ○ 현재 및 새 정정 작업 모두에 유지: 다른 정정 작업의 일부인 기록은 이전 정정 작업과 새 정정 작업 모두에 유지됩니다.

6. 정정 작업 생성을 선택합니다.

결과
정정 작업은 그룹화 기준에 따라 생성됩니다. 할당 그룹의 정정 소유자에게 정정 작업이 생성되어 해당 그룹에 할당되었음을 알리는 이메일 알림이 전송됩니다. 그룹화 기준에 따라 정정 작업이 생성되는 방식에 대한 예는 다음 문서를 의 정정 작업 생성 취약성 관리자 작업 공간 예시 및 IT 정정 작업 공간참조하십시오.

테스트 그룹에 대한 **Qualys** 테스트 결과 임포트 활성화 또는 비활성화

의 취약성 대응v23.0부터 테스트 그룹의 기록 뷰에서 사용할 수 있는 임포트 사용/사용 안 함 버튼을 사용하여 테스트 그룹의 테스트에 Qualys 대한 테스트 결과 임포트를 제어합니다.

시작하기 전에
필요한 역할: sn_vulc.admin

프로시저

1. 다음으로 이동 작업 공간 〉 취약성 관리자 작업 공간 〉 목록.
2. 라이브러리의 테스트 그룹 목록 아래에 있는 레코드 뷰에서 테스트 그룹을 엽니다 Qualys .
3. 임포트 사용 안 함 버튼을 선택하여 테스트 그룹과 연결된 Qualys 테스트 결과의 임포트를 비활성화합니다.
   예정된 데이터 수집에서 테스트 그룹에 대한 Qualys 테스트 결과는 임포트되지 않습니다.
   임포트가 비활성화됨 필드의 값이 *true*로 변경됩니다.
4. 옵션: 임포트 사용 단추를 선택하여 테스트 결과 임포트를 사용하도록 설정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

CVE 또는 TPE의 심각도 수정

취약성 관리자 또는 분석가는 취약성 관리자 작업 공간에서 CVE(일반적인 취약성 항목) 또는 TPE(외부 공급업체 항목)의 심각도 수준을 수정할 수 있습니다.

시작하기 전에

필요한 역할:

- 호스트 취약 항목(VIT)의 경우 sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin
- sn_vul.app_sec_manager, sn_vul.app_developer 애플리케이션 취약 항목(AVIT)
- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.vulnerability_analyst 또는 sn_vul_container.vulnerability_admin

프로시저

1. 다음으로 이동 작업 공간 〉 취약성 관리자 작업 공간 〉 목록 〉 라이브러리.
2. 적절한 항목을 엽니다.
   - **CVE(NVD):** CVE의 심각도를 수정합니다.
   - **TPE: TPE**의 심각도를 수정합니다.
3. 추가 작업 아이콘 ellipsis_icon에서 심각도 수정을 선택합니다
4. 드롭다운에서 새 심각도 수준을 선택합니다.
5. 업데이트에 대한 근거를 제공합니다.
6. 제출을 선택합니다.

주:

- 추가 작업 메뉴의 심각도 재설정 옵션을 사용하여 원래 소스 심각도로 되돌릴 수 있습니다. 이 옵션은 심각도를 수정한 후에만 나타납니다.
- 수정된 심각도 필드는 소스 심각도를 변경할 때만 나타납니다. 원래 값으로 재설정하면 필드가 제거됩니다.
- 시스템은 예약된 다음 작업부터 위험 계산에 수정된 심각도 를 사용합니다. 심각도가 재설정되면 원래 소스 심각도가 대신 적용됩니다.

에서 요청 승인 또는 거부 취약성 관리자 작업 공간

정정 소유자가 제출한 요청을 승인하거나 거부합니다.

시작하기 전에

필요한 역할:

다양한 승인 요청에 필요한 승인자 역할

승인 유형	승인 수준 필요	승인자 역할	추가 정보
가양성 승인	1	• sn_vul.false_positive_approver 취약한 항목(VIT)에 대한 세분화된 역할입니다. • 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_false_positive_approver 역할	-

기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다양한 승인 요청에 필요한 승인자 역할

승인 유형	승인 수준 필요	승인자 역할	추가 정보
		• 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.false_positive_approver 역할 • 구성 테스트 결과에 대한 sn_vulc.false_positive_approver 또는 승인자는 False Positive Approver 사용자 그룹에 있어야 합니다.	
예외 승인(연기)	2	• 승인자 - 수준 1 그룹에는 한 명의 승인자가 필요합니다. • 승인자 - 수준 2 그룹에는 한 명의 승인자가 필요합니다.	기록 또는 정정 작업에 대한 예외 요청은 기본 2단계 승인 워크플로우를 사용하여 승인됩니다. 예외 요청에는 두 가지 수준의 승인자가 필요합니다. 요청이 수준 1 승인자에 의해 승인되면 두 번째 수준 승인자에게 전송된 다음 승인자 2의 큐에 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다양한 승인 요청에 필요한 승인자 역할

승인 유형	승인 수준 필요	승인자 역할	추가 정보
승인 할당 취소	승인자 – 수준 1 그룹에는 한 명의 승인자가 필요합니다.	• sn_vul.unassign_appr for AVITs and VITs • CVIT에 대한 sn_vul_container.unas • 구성 문제에 대한 sn_vulc.unassign_app	주: 기본적으로 승인 구성이 제공되고 승인 그룹 할당이 해제됩니다. 이 그룹의 사용자 (승인자 할당 해제 - 수준 1)가 요청을 승인할 수 있습니다. 이 그룹에는 기본적으로 할당되지 않은 승인자 역할인 sn_vul.unassign_approver가 포함되어 있습니다. 새 그룹을 수정 또는 생성하고 승인 구성을 업데이트할 수 있습니다. 승인 규칙을 구성하려면 해당 승인 규칙 모듈로 이동하여 다음 승인 규칙 중 하나를 선택하고 승인 구성 탭의 승인 구성으로 이동합니다. • *Vulnerable item field change request* 취약한 항목에 대해. • *Vulnerability field change request* 정정 작업의 경우. • *Application vulnerability field change request* 애플리케이션 취약한 항목 (AVIT)에 대해 설명합니다. • *Approval for*

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다양한 승인 요청에 필요한 승인자 역할

승인 유형	승인 수준 필요	승인자 역할	추가 정보
위험 감소 승인	2	• 승인자 - 수준 1 그룹에는 한 명의 승인자가 필요합니다. • 승인자 - 수준 2 그룹에는 한 명의 승인자가 필요합니다.	위험 감소를 위한 승인 플로우는 예외 승인(지연)과 동일합니다.

사용자에게 가상 사용자 역할을 할당하고 사용자를 그룹에 할당하는 방법에 대한 자세한 내용은 을 참조하십시오 취약성 대응 가상 사용자 및 세분화된 역할설정 도우미를 취약성 대응 사용하여 가상 사용자 역할 할당 .

주:
승인 요청을 제출하기 전에 승인 그룹에 사용자를 추가하십시오. 승인 그룹에 사용자를 추가하기 전에 요청을 생성하면 승인 권한이 있는 사용자에게는 요청이 표시되지 않을 수 있습니다.

프로시저

1. 다음으로 이동 작업 공간 〉 취약성 관리자 작업 공간.
   승인자가 작업 공간에 액세스할 수 없는 경우 다음에서 승인을 처리할 수 있습니다. 취약성 대응 〉 내 승인 클래식 환경에서.
2. 목록 뷰 아이콘(.)을 선택합니다.
   목록 페이지가 표시됩니다.
3. 필터링된 승인 목록에서 나에게 할당을 선택합니다.
4. 처리할 요청을 찾은 다음 상태 열에서 링크를 선택합니다.
   취약성 상태 변경 승인 기록(VCA#)이 표시됩니다.
5. 다음 옵션 중 하나를 선택하여 요청을 승인하거나 거부합니다.

작업 공간에서 이메일 알림 취약성 대응 설정

정정 소유자 사용자 그룹의 사용자에게 전송되는 자동 이메일 미리 알림에 대한 사용자를 식별합니다.

시작하기 전에

필요한 역할: 관리자

이 기능은 정정 소유자 사용자 그룹의 사용자에 대한 이메일 다이제스트를 자동으로 생성합니다. 설명된 취약성 대응 작업 공간에서 이메일 다이제스트 사용대로 이메일 알림을 받을 사용자를 추가합니다.

사용자의 사용자 기록에 입력된 활성 이메일 주소가 있는지, 그리고 정정 소유자 사용자 그룹에 추가했는지 확인합니다.

이메일의 배달 빈도, 날짜 또는 시간을 변경하거나 기능을 비활성화하려면 다음 단계를 수행합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 예약된 작업.
2. 정정 다이제스트 생성을 찾은 후 클릭하여 기록을 엽니다.

   알림이 전송되고 있는지 확인할 때까지 필드를 기본 설정으로 두는 것이 좋습니다. 기본적으로 이메일은 매주 월요일 오전 9:00에 작업을 실행하는 인스턴스의 시간대로 전송됩니다.

3. 양식의 필드를 수정합니다.
   양식 필드에 대한 자세한 내용은 정정 다이제스트 양식 필드 생성 문서를 참조하십시오.
4. 업데이트를 클릭합니다.

다음에 수행할 작업
이전에 나열된 모든 정보가 올바른지 확인한 후 정정 소유자 사용자 그룹에 사용자가 있지만 이메일이 예상대로 전송되지 않는 경우 이메일 알림을 수신하도록 활성화된 채널이 있는지 확인합니다. Create notification channels 문서를 참조하십시오.

다음에서 취약한 항목 및 테스트 결과 정정 보안 노출 관리 작업 공간

에서 취약성 관리자 작업 공간조건을 정의하여 취약한 항목과 테스트 결과를 감시 주제별로 정정할 수 있으며, 정정 작업을 생성하여 정정 진행률을 추적할 수 있습니다.

에서 대량 편집 사용 취약성 관리자 작업 공간

에서 취약성 관리자 작업 공간대량 편집 기능을 사용하여 기록의 상태를 업데이트하고, 예외 및 긍정 오류를 요청하고, 할당 그룹에 여러 취약한 항목(VIT, AVIT 또는 CVIT)에 기록을 동시에 할당할 수 있습니다.

대량 편집 기능은 다음에 사용할 수 있습니다.

- 의 v21.0부터 시작하는 호스트 취약 항목(VIT)입니다 취약성 대응.
- 의 v22.0 취약성 대응부터 시작하는 AVIT(애플리케이션 취약 항목) 및 CVIT(컨테이너 취약 항목)입니다.
- 의 v23.0 취약성 대응부터 시작하는 테스트 결과.

에서 기록 상태를 대량으로 업데이트 취약성 관리자 작업 공간

의 취약성 관리자 작업 공간대량 편집 기능을 사용하여 정정 진행률에 따라 여러 기록(VIT, AVIT 또는 CVIT)의 상태를 동시에 업데이트합니다.

시작하기 전에
필요한 역할:

- 호스트 취약한 항목의 경우 sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin
- 애플리케이션 취약한 항목에 대한 sn_vul.app_sec_manager
- 컨테이너 취약한 항목의 sn_vul_container.vulnerability_analyst 또는 sn_vul_container.vulnerability_admin

프로시저

1. 다음으로 이동 작업 공간 〉 취약성 관리자 작업 공간 〉 목록.
2. 목록 페이지의 다음 목록 중 하나에서 활성 또는 모두 목록을 엽니다.
   - 호스트 취약한 항목
   - 컨테이너 취약한 항목
   - 애플리케이션 취약한 항목

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 다음 중 하나를 수행합니다.
   - 기록 선택 필드에서 선택한 항목만 옵션을 사용하려면 각 항목 옆에 있는 확인란을 선택합니다.
   - 기록 선택 필드의 필터와 일치하는 모든 취약한 항목 옵션을 사용하려면 필터를 적용합니다.
4. **Bulk** Edit(일괄 편집) 버튼을 선택합니다.
5. 대량 편집 모달에서 다음 필드를 입력하여 기록의 상태를 업데이트합니다.

모달 필드 대량 편집

필드	설명
기록 선택	업데이트할 기록입니다. 선택 항목은 다음과 같습니다. ○ 선택한 항목만: 확인란을 사용하여 선택한 기록을 업데이트하려면 이 옵션을 선택합니다. ○ 필터와 일치하는 모든 취약한 항목: 필터링된 기록을 업데이트하려면 이 옵션을 선택합니다. ○ 정정 작업: 정정 작업의 기록을 업데이트한 다음 정정 작업 필드에서 원하는 정정 작업을 선택하려면 이 옵션을 선택합니다. ○ 취약성 항목: CVE(일반적인 취약한 항목)에 특정한 기록을 업데이트하려는 경우 이 옵션을 선택한 다음 취약성 항목 필드에서 CVE를 선택합니다. **주:** 잘못된 CI 또는 CI가 해제된 기록은 업데이트되지 않습니다.
상태	기록의 상태에 대한 변경입니다. 선택 항목은 다음과 같습니다. ○ 업데이트하지 마십시오. ○ 오픈 ○ 조사 중 ○ 대기 중인 구현 ○ 연기됨 자세한 내용은 취약성 관리자 작업 공간에서 대량 예외 요청 문서를 참조하십시오. ○ 종결됨 자세한 내용은 취약성 관리자 작업 공간에서 가양성에 대한 대량 편집 문서를 참조하십시오. ○ 해결 일시 **주:** 상태 전환이 유효한 기록만 업데이트됩니다.
작업 메모	변경 내용을 설명하기 위해 입력하는 텍스트입니다.

6. 편집을 선택합니다.

대량 비동기 편집 작업은 선택한 기록을 업데이트합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

패치 및 솔루션으로 호스트 취약 항목 대량 편집

의 대량 편집 기능을 취약성 관리자 작업 공간사용하여 여러 호스트 취약한 항목에 대한 패치 또는 솔루션을 동시에 사용합니다.

시작하기 전에

필요한 역할: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin 및 sn_vul.bulk_edit 세분화된 역할이 있는 모든 역할.

이 태스크 정보

대량 편집 모달에서 기본 솔루션 및 패치를 추가하는 동안 여러 호스트 취약한 항목(VIT)을 할당 그룹에 동시에 할당 해제하거나 할당할 수도 있습니다.

프로시저

1. 다음으로 이동 작업 공간 〉 취약성 관리자 작업 공간.

> **주:**
> 선택한 기록은 오픈, 조사 중 또는 구현 대기 중 상태여야 합니다.

2. 목록 페이지의 호스트 취약한 항목 아래에서 활성 또는 모두 목록을 엽니다.

3. 다음 중 하나를 수행합니다.

- 기록 선택 필드에서 선택한 항목만 옵션을 사용하려면 각 항목 옆에 있는 확인란을 선택합니다.
- 기록 선택 필드의 필터와 일치하는 모든 취약한 항목 옵션을 사용하려면 필터를 적용합니다.
- 대량 편집 모달의 기록 선택 필드에서 선택한 항목만 옵션을 사용하려면 각 항목 옆에 있는 확인란을 선택합니다.
- 대량 편집 모달의 기록 선택 필드에서 필터와 일치하는 모든 취약한 항목 옵션을 사용하려면 필터를 적용합니다.

4. **Bulk** Edit(일괄 편집) 버튼을 선택합니다.

5. 대량 편집 모달에서 여러 호스트 취약한 항목에 대한 패치 또는 솔루션을 권장하는 필드를 입력합니다.

모달 필드 대량 편집

필드	설명
기록 선택	업데이트할 기록입니다. 선택 항목은 다음과 같습니다. ○ 선택한 항목만: 확인란을 사용하여 선택한 기록을 업데이트하려면 이 옵션을 선택합니다. ○ 필터와 일치하는 모든 취약한 항목: 필터링된 기록을 업데이트하려면 이 옵션을 선택합니다. ○ 정정 작업: 정정 작업의 기록을 업데이트한 다음 정정 작업 필드에서 원하는 정정 작업을 선택하려면 이 옵션을 선택합니다. ○ 취약성 항목: CVE(일반적인 취약한 항목)에 특정한 기록을 업데이트하려는 경우 이 옵션을 선택한 다음 취약성 항목 필드에서 CVE를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	주: ○ 잘못된 CI 또는 CI가 해제된 기록은 업데이트되지 않습니다. ○ 오픈, 조사 중 또는 구현 대기 중 상태의 기록(VIT)만 업데이트됩니다.
상태	호스트 취약한 항목의 상태에 대한 변경입니다. 다음 상태를 선택하는 경우에만 기본 솔루션 및 패치를 추가할 수 있습니다. ○ 업데이트하지 마십시오. ○ 오픈 ○ 조사 중 ○ 대기 중인 구현
기본 솔루션	대량 편집을 위해 선택된 모든 취약한 항목을 정정하기 위한 대상 솔루션. 취약한 항목의 기본 솔루션 필드에 대한 변경 사항을 선택합니다. 선택한 VIT에 사용할 수 있는 기본 솔루션 조회 목록에서 선택 항목을 선택할 수 있습니다. 주: ○ 사용 가능한 기본 솔루션 집합은 선택한 모든 VIT에서 취약성의 모든 잠재적 솔루션이 교차하는 지점입니다. ○ 를 선택할 때 기록 선택 〉 취약성 항목 대량 편집의 경우 취약성에 대한 모든 VIT가 선택한 기본 솔루션으로 설정됩니다. 주: 이 작업은 취약성 엔트리 수준에서 기본 솔루션을 설정하지 않습니다. 취약성 엔트리 수준에서 기본 솔루션을 설정하면 앞으로 모든 새 VIT에 대한 기본 솔루션이 설정됩니다. 대량 편집은 현재 VIT 세트만 수정합니다. ○ 선택 기준 전반의 뚜렷한 취약성은 500개로 제한됩니다. 500개 이상의 고유한 취약성이 있는 경우 기본 솔루션을 설정하기 위해 다른 기준을 가진 VIT를 선택하라는 경고 메시지가 표시됩니다. ○ 목록 조회에 표시할 수 있는 총 솔루션 수는 170개로 제한됩니다. 170개가 넘는 솔루션이 있는 경우 경고 메시지가 표시됩니다. 업데이트된 값이 취약한 항목 목록 뷰에 표시됩니다.
기본 패치	대량 편집을 위해 선택된 모든 취약성 항목을 정정하기 위한 대상 패치입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	주: ○ 기본 패치 목록을 보려면 패치 오케스트레이션을 설치해야 합니다. ○ 사용 가능한 기본 패치 집합은 선택한 모든 VIT에서 모든 잠재적 패치의 교차점입니다. ○ 선택 기준 전반의 뚜렷한 취약성은 500개로 제한됩니다. 500개 이상의 고유한 취약성이 있는 경우 기본 패치를 설정하기 위해 다른 기준을 가진 VIT를 선택하라는 경고 메시지가 표시됩니다. ○ 조회 목록에 표시할 수 있는 총 패치 수는 170개로 제한됩니다. 패치가 170개 이상이면 경고 메시지가 표시됩니다.
할당 해제	선택한 모든 항목이 할당 그룹 및 정정 소유자에게 할당되지 않았습니다. 주: ○ 이 필드는 상태를 업데이트 안 함으로 선택할 때 나타납니다. ○ 기록 할당을 해제하면 승인을 위해 전송되는 정정 작업이 생성됩니다. 자세한 내용은 호스트 취약한 항목에 대한 할당을 대량으로 제거 문서를 참조하십시오.
할당 그룹	기록에 대한 할당 그룹입니다. 모든 활성 할당 그룹이 이 필드에 표시됩니다. 주: 할당 해제 확인란을 선택하면 이 필드는 비활성화됩니다.
작업 메모	변경 내용을 설명하기 위해 입력하는 텍스트입니다.

6. 편집을 선택합니다.

결과
대량 비동기 편집 작업은 선택한 호스트 취약한 항목(VIT)을 업데이트합니다. 기본 솔루션 및 패치가 관련 호스트 취약한 항목(VIT)에 추가됩니다. 호스트 취약한 항목을 열고 상세 정보 탭의 업데이트 적용 섹션에서 기본 솔루션 및 패치를 확인합니다.

할당 그룹에 기록을 대량으로 할당

의 취약성 관리자 작업 공간대량 편집 기능을 사용하여 여러 기록(VIT, VIT, VIT 또는 TR)을 할당 그룹에 동시에 할당합니다.

시작하기 전에
필요한 역할:

- 호스트 취약 항목(VIT)의 경우 sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin
- 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_sec_manager
- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.vulnerability_analyst 또는 sn_vul_container.vulnerability_admin
- 구성 테스트 결과(CTR)에 대한 sn_vulc.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 작업 공간 〉 취약성 관리자 작업 공간 〉 목록.
2. 목록 페이지의 다음 목록 중 하나에서 활성 또는 모두 목록을 엽니다.
   - 호스트 취약한 항목
   - 컨테이너 취약한 항목
   - 애플리케이션 취약한 항목
   - 구성 테스트 결과
3. 다음 중 하나를 수행합니다.
   - 기록 선택 필드에서 선택한 항목만 옵션을 사용하려면 각 항목 옆에 있는 확인란을 선택합니다.
   - 기록 선택 필드에서 필터와 일치하는 모든 기록 옵션을 사용하려면 필터를 적용합니다.
4. **Bulk** Edit(일괄 편집) 버튼을 선택합니다.
5. 양식의 필드에 내용을 입력하여 기록을 할당 그룹에 할당합니다.

모달 필드 대량 편집

필드	설명
기록 선택	업데이트할 기록입니다. 선택 항목은 다음과 같습니다. ○ 선택한 항목만: 확인란을 사용하여 선택한 기록을 업데이트하려면 이 옵션을 선택합니다. ○ 필터와 일치하는 모든 기록: 필터링된 기록을 업데이트하려면 이 옵션을 선택합니다. ○ 정정 작업: 정정 작업의 기록을 업데이트한 다음 정정 작업 필드에서 원하는 정정 작업을 선택하려면 이 옵션을 선택합니다. ○ 취약성 항목: 취약성항목에 특정한 기록을 업데이트하려는 경우 이 옵션을 선택한 다음 취약성 항목 필드에서 CVE 또는 TPE를 선택합니다. **주:** 이 필드는 호스트 취약한 항목, 애플리케이션 취약한 항목 및 컨테이너 취약한 항목에 대해 표시됩니다. ○ 구성 테스트: 테스트와 관련된 테스트 결과를 업데이트하려는 경우 이 옵션을 선택한 다음 구성 테스트 필드에서 테스트를 선택합니다. **주:** 이 옵션은 구성 테스트 결과에만 나타납니다. **주:** ○ 잘못된 CI 또는 CI가 해제된 기록은 업데이트되지 않습니다. ○ 오픈, 조사 중, 구현 대기 중 또는 연기됨 상태의 기록만 업데이트됩니다.
할당 그룹	기록에 대한 할당 그룹입니다. 모든 활성 할당 그룹이 이 필드에 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	주: VIT에 대한 할당 해제 확인란을 선택하면 이 필드가 비활성화됩니다.
작업 메모	변경 내용을 설명하기 위해 입력하는 텍스트입니다.

6. 편집을 클릭합니다.

결과
할당 그룹을 업데이트한 기록을 열고 개요 탭으로 이동하면 기록이 할당된 사용자 그룹이 할당 그룹 필드에 나타납니다.

호스트 취약한 항목에 대한 할당을 대량으로 제거

기록이 정정 범위 내에 있지 않거나 기록이 사용자 또는 그룹에 잘못 할당되었다고 생각되면 호스트 취약 항목(VIT) 또는 정정 작업(VUL)의 할당 대상 및 할당 그룹 필드에서 자신 또는 그룹을 제거합니다.

시작하기 전에
필요한 역할: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin

이 태스크 정보
할당 해제 기능은 종결 또는 해결됨 이외의 모든 상태에 있는 기록에 적용할 수 있습니다. 대량 편집 기능을 사용하여 호스트 취약한 항목에 대한 할당을 제거하면 관련 기록만 업데이트됩니다.

프로시저

1. 다음으로 이동 작업 공간 〉 취약성 관리자 작업 공간.
2. 목록 페이지의 호스트 취약한 항목 아래에서 활성 또는 모두 목록을 엽니다.
3. 다음 중 하나를 수행합니다.
   - 기록 선택 필드에서 선택한 항목만 옵션을 사용하려면 각 항목 옆에 있는 확인란을 선택합니다.
   - 기록 선택 필드의 필터와 일치하는 모든 취약한 항목 옵션을 사용하려면 필터를 적용합니다.
4. **Bulk** Edit(일괄 편집) 버튼을 선택합니다.
5. 양식의 필드에 내용을 입력하여 할당을 대량으로 제거합니다.

모달 필드 대량 편집

필드	설명
기록 선택	업데이트할 기록입니다. 선택 항목은 다음과 같습니다. ○ 선택한 항목만: 확인란을 사용하여 선택한 기록을 업데이트하려면 이 옵션을 선택합니다. ○ 필터와 일치하는 모든 취약한 항목: 필터링된 기록을 업데이트하려면 이 옵션을 선택합니다. ○ 정정 작업: 정정 작업의 기록을 업데이트한 다음 정정 작업 필드에서 원하는 정정 작업을 선택하려면 이 옵션을 선택합니다. ○ 취약성 항목: CVE(일반적인 취약한 항목)에 특정한 기록을 업데이트하려는 경우 이 옵션을 선택한 다음 취약성 항목 필드에서 CVE를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	주: ○ 잘못된 CI 또는 CI가 해제된 기록은 업데이트되지 않습니다. ○ 오픈, 조사 중, 구현 대기 중 또는 연기됨 상태의 기록만 업데이트됩니다.
상태	업데이트 안 함으로 상태를 선택합니다.
할당 해제	선택한 모든 취약한 항목이 할당 그룹 및 정정 소유자로부터 할당되지 않았습니다. 주: ○ 이 필드는 상태를 업데이트 안 함으로 선택할 때 나타납니다. ○ 기록 할당을 해제하면 승인을 위해 전송되는 정정 작업이 생성됩니다.
작업 메모	변경 내용을 설명하기 위해 입력하는 텍스트입니다.

6. 편집을 클릭합니다.
   선택한 호스트 취약한 항목(VIT)을 사용하여 업데이트 적용 작업이 생성됩니다.

   요청이 승인을 위해 제출되고 승인자는 요청에 대한 이메일 알림을 받습니다.

   호스트 취약한 항목(VIT) 및 정정 작업(VUL)의 상태가 검토 중으로 전환됩니다. 이 기능으로 정정 작업이 업데이트되면 요청이 승인될 때 연결된 모든 VIT의 할당 대상 및 할당 그룹 필드도 지워집니다.

결과
취약성 관리자 작업 공간의 목록 페이지에서 예외 요청 〉 모두 을 클릭하고 해당 상태 변경 승인 기록(VCA#)을 열고 승인 상태 열에서 요청 상태를 확인합니다.

승인 상태	결과
승인됨	모든 호스트 취약한 항목의 할당 대상 및 할당 그룹 필드가 지워집니다.
거부됨	모든 호스트 취약한 항목의 할당 대상 및 할당 그룹 필드가 업데이트되지 않습니다.

기록 또는 정정 작업의 활동 스트림 에서 요청의 전체 워크플로우를 볼 수 있습니다.

취약성 관리자 작업 공간에서 대량 예외 요청

각 기록을 수동으로 선택하는 대신 대량 편집 기능을 사용하여 여러 기록(VIT, VIT, CVIT 또는 TR)에 대한 예외를 동시에 요청합니다.

시작하기 전에
필요한 역할:

- 호스트 취약 항목(VIT)의 경우 sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin
- 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_sec_manager

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.vulnerability_analyst 또는 sn_vul_container.vulnerability_admin
- 구성 테스트 결과(CTR)에 대한 sn_vulc.admin

이 태스크 정보

대량 편집 모달에서 하나 이상의 기록에 대한 예외를 요청하면 선택한 기록과 함께 정정 작업이 생성됩니다.

주:
ServiceNow에서 예외 관리 매개변수가 false로 설정된 스캐너의 애플리케이션 취약한 항목(AVIT)이 업데이트되지 않습니다.

- 다양한 스캐너에서 AVIT를 선택하는 경우(일부는 ServiceNow에서 예외 관리 매개변수가 true로 설정되고 다른 일부는 false로 설정됨) ServiceNow에서 예외 관리 매개변수가 false로 설정된 스캐너에 연결된 AVIT는 업데이트되지 않습니다.
- ServiceNow에서 예외 관리 매개변수가 false로 설정된 스캐너에서만 AVIT를 선택하면 대량 편집 모달의 상태 필드에 지연 옵션이 나타나지 않습니다.

프로시저

1. 다음으로 이동 작업 공간 〉 취약성 관리자 작업 공간.
2. 목록 페이지의 다음 목록 중 하나에서 활성 또는 모두 목록을 엽니다.
   - 호스트 취약한 항목
   - 컨테이너 취약한 항목
   - 애플리케이션 취약한 항목
   - 구성 테스트 결과
3. 다음 중 하나를 수행합니다.
   - 기록 선택 필드에서 선택한 항목만 옵션을 사용하려면 각 항목 옆에 있는 확인란을 선택합니다.
   - 기록 선택 필드에서 필터와 일치하는 모든 기록 옵션을 사용하려면 필터를 적용합니다.
4. **Bulk** Edit(일괄 편집) 버튼을 선택합니다.
5. 양식에서 다음 필드를 입력하여 여러 기록(VIT, VIT, CVIT 또는 TR)에 대한 예외를 동시에 요청합니다.

모달 필드 대량 편집

필드	설명
기록 선택	업데이트할 기록입니다. 선택 항목은 다음과 같습니다. ○ 선택한 항목만: 확인란을 사용하여 선택한 기록을 업데이트하려면 이 옵션을 선택합니다. ○ 필터와 일치하는 모든 기록: 필터링된 기록을 업데이트하려면 이 옵션을 선택합니다. ○ 정정 작업: 정정 작업의 기록을 업데이트한 다음 정정 작업 필드에서 원하는 정정 작업을 선택하려면 이 옵션을 선택합니다. ○ 취약성 항목: 취약성 과 관련된 기록을 업데이트하려는 경우 이 옵션을 선택한 다음 취약성 항목 필드에서 CVE 또는 TPE를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	주: 이 필드는 호스트 취약한 항목, 애플리케이션 취약한 항목 및 컨테이너 취약한 항목에 대해 표시됩니다. ○ 구성 테스트: 테스트와 관련된 테스트 결과를 업데이트하려는 경우 이 옵션을 선택한 다음 구성 테스트 필드에서 테스트를 선택합니다. 주: 이 옵션은 구성 테스트 결과에만 나타납니다. 주: ○ 잘못된 CI 또는 CI가 해제된 기록은 업데이트되지 않습니다. ○ 오픈, 조사 중 또는 구현 대기 중 상태의 기록만 업데이트됩니다.
상태	선택한 기록에 대한 예외를 요청하려면 연기됨 상태를 선택합니다. 주: ○ 이 옵션을 선택하면 이유, 간단한 설명, 기한 및 추가 정보 필드가 나타납니다. ○ 기록을 연기하면 정정 작업이 생성되고 이 작업은 승인을 위해 전송됩니다.
이유	기록을 연기하는 이유: ○ 유지관리 기간을 기다리는 중 ○ 수정 사용 불가 ○ 위험 수락됨 ○ 사용 중인 완화 통제 ○ 기타 주: 상태를 연기됨으로 선택하면 이유 필드가 나타납니다.
간단한 설명	연기 요청의 이유를 설명하는 간단한 메모입니다. 이 정보는 지연 요청에 대해 생성된 정정 작업의 설명 필드에 반영됩니다. 주: 이 필드는 상태를 연기됨 및 종결됨-긍정 오류로 선택할 때 나타납니다.
다음까지	기록이 지연된 상태로 유지되는 종료 날짜입니다. 주: 이 필드는 상태를 연기됨으로 선택할 때 나타납니다.
추가 정보	기타 필요한 정보입니다. 이 정보는 지연 및 종결 긍정 오류 요청에 대해 생성된 정정 작업의 개요 탭에 있는 추가 정보 필드에 반영됩니다. 연기

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	요청이 승인되면 이 추가 정보가 VIT 및 정정 작업 모두에 대한 연기 메모로 표시됩니다. 주: 이 필드는 상태를 연기됨 및 종결됨-긍정 오류로 선택할 때 나타납니다.
작업 메모	변경 내용을 설명하기 위해 입력하는 텍스트입니다.

6. 편집을 클릭합니다.
7. 질문서 수행 모달에서 질문에 답하고 제출을 클릭합니다.

   선택한 기록을 포함하는 정정 작업이 생성됩니다. 요청이 승인을 위해 제출되고 기록 상태가 검토 중으로 변경됩니다.

   주:
   질문서 사용 모달은 예외 관리 양식에서 예외 요청에 대해 질문서가 활성화된 경우에만 나타납니다. 예외 요청에 대한 질문서 구성에 대한 자세한 내용은 , , 에 대한 예외 관리 구성 컨테이너 취약성 대응, 및 구성 준수 예외 관리 개요를 참조하십시오에 대한 예외 관리 구성 취약성 대응. 에 대한 예외 관리 구성 애플리케이션 취약성 대응

   승인자는 요청에 대한 이메일 알림을 받습니다.

결과
취약성 관리자 작업 공간의 목록 페이지에서 예외 〉 모두에서 해당하는 상태 변경 승인 기록(VCA#)을 열고 승인 상태 열에서 요청 상태를 확인합니다.

승인 상태	결과
승인됨	정정 작업의 상태가 지연됨으로 전환되며 지정된 이유가 하위 상태로 표시됩니다. 상태 및 이유가 기록으로 롤다운됩니다.
거부됨	정정 작업 및 해당 기록의 상태는 변경되지 않습니다.

기록 또는 정정 작업의 활동 스트림 에서 요청의 전체 워크플로우를 볼 수 있습니다.

취약성 관리자 작업 공간에서 가양성에 대한 대량 편집

각 항목을 수동으로 선택하는 대신 취약성 관리자 작업 공간의 대량 편집 기능을 사용하여 하나 이상의 기록(VIT, VIT, CVIT 또는 TR)을 동시에 긍정 오류로 표시합니다.

시작하기 전에
필요한 역할:

- 호스트 취약 항목(VIT)의 경우 sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin
- 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_sec_manager
- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.vulnerability_analyst 또는 sn_vul_container.vulnerability_admin
- 구성 테스트 결과(CTR)에 대한 sn_vulc.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보
대량 편집 모달에서 하나 이상의 기록에 대해 긍정 오류 요청을 제기하면 선택한 기록과 함께 정정 작업이 생성됩니다.

주:
대량 편집 기능을 사용하여 애플리케이션 취약 항목(AVIT)에 대해 긍정 오류 요청을 제기하면 ServiceNow로 허위 양성 관리 매개변수가 false로 설정된 스캐너의 AVIT가 업데이트되지 않습니다.

- 다양한 스캐너에서 AVIT를 선택하는 경우, 일부는 Servicenow로 거짓 양성 관리 매개변수가 true로 설정되고 다른 일부는 false로 설정된 경우 Servicenow로 거짓 양성 관리 매개변수가 false로 설정된 스캐너에 연결된 AVIT가 업데이트되지 않습니다.
- Servicenow로 거짓 양성 관리 매개변수가 false로 설정된 스캐너에서만 AVIT를 선택하면 대량 편집 모달의 이유 필드에 긍정 오류 옵션이 나타나지 않습니다.

프로시저

1. 다음으로 이동 작업 공간 〉 취약성 관리자 작업 공간 〉 목록.

   주:
   선택한 기록은 오픈, 조사 중 또는 구현 대기 중 상태여야 합니다.

2. 목록 페이지의 다음 목록 중 하나에서 활성 또는 모두 목록을 엽니다.
   - 호스트 취약한 항목
   - 컨테이너 취약한 항목
   - 애플리케이션 취약한 항목
   - 구성 테스트 결과
3. 다음 중 하나를 수행합니다.
   - 기록 선택 필드에서 선택한 항목만 옵션을 사용하려면 각 항목 옆에 있는 확인란을 선택합니다.
   - 기록 선택 필드에서 필터와 일치하는 모든 기록 옵션을 사용하려면 필터를 적용합니다.
4. **Bulk** Edit(일괄 편집) 버튼을 선택합니다.
5. 양식에서 필드를 입력하여 여러 기록에 대한 긍정 오류를 요청합니다.

모달 필드 대량 편집

필드	설명
기록 선택	업데이트할 기록입니다. 선택 항목은 다음과 같습니다. ○ 선택한 항목만: 확인란을 사용하여 선택한 기록을 업데이트하려면 이 옵션을 선택합니다. ○ 필터와 일치하는 모든 기록: 필터링된 기록을 업데이트하려면 이 옵션을 선택합니다. ○ 정정 작업: 정정 작업의 기록을 업데이트한 다음 정정 작업 필드에서 원하는 정정 작업을 선택하려면 이 옵션을 선택합니다. ○ 취약성 항목: 취약성 과 관련된 기록을 업데이트하려는 경우 이 옵션을 선택한 다음 취약성 항목 필드에서 CVE 또는 TPE를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	주: 이 필드는 호스트 취약한 항목, 애플리케이션 취약한 항목 및 컨테이너 취약한 항목에 대해 표시됩니다. ○ 구성 테스트: 테스트와 관련된 테스트 결과를 업데이트하려는 경우 이 옵션을 선택한 다음 구성 테스트 필드에서 테스트를 선택합니다. 주: 이 옵션은 구성 테스트 결과에만 나타납니다. 주: ○ 잘못된 CI 또는 CI가 해제된 기록은 업데이트되지 않습니다. ○ 오픈, 조사 중 또는 구현 대기 중 상태의 기록만 업데이트됩니다.
상태	종결 상태를 선택합니다.
이유	이유를 긍정 오류로 선택합니다. 주: ○ 이 옵션을 선택하면 간단한 설명 및 추가 정보 필드가 나타납니다. ○ 기록을 긍정 오류로 표시하고 이 작업이 승인을 위해 전송되면 정정 작업이 생성됩니다. 주: 상태를 연기됨 또는 종결됨으로 선택하면 이유 필드가 나타납니다.
간단한 설명	종결-긍정 오류 요청의 이유를 설명하는 간단한 메모입니다. 이 정보는 종결-긍정 오류 요청에 대해 생성된 정정 작업의 설명 필드에 반영됩니다. 주: 이 필드는 상태를 연기됨 또는 종결됨-긍정 오류로 선택할 때 나타납니다.
추가 정보	기타 필요한 정보입니다. 이 정보는 종결-긍정 오류 요청에 대해 생성된 정정 작업의 개요 탭에 있는 추가 정보 필드에 반영됩니다. 긍정 오류 요청이 승인되면 이 추가 정보가 VIT 및 정정 작업 모두에 대한 메모로 표시됩니다. 주: 이 필드는 상태를 연기됨 또는 종결됨-긍정 오류로 선택할 때 나타납니다.
작업 메모	변경 내용을 설명하기 위해 입력하는 텍스트입니다.

6. 편집을 클릭합니다.
7. 질문서 수행 모달에서 질문에 답하고 제출을 선택합니다.
   선택한 기록과 함께 정정 작업이 생성됩니다. 요청이 승인을 위해 제출되고 정정 작업의 상태가 검토 중으로 변경됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
질문서 사용 모달은 예외 관리 양식에서 긍정 오류 요청에 대해 질문서가 활성화된 경우에만 나타납니다. 긍정 오류 요청에 대한 질문서를 구성하는 방법에 대한 자세한 내용은 , 에 대한 예외 관리 구성 애플리케이션 취약성 대응, 및 에 대한 예외 관리 구성 컨테이너 취약성 대응을 참조하십시오에 대한 예외 관리 구성 취약성 대응.

승인자는 요청에 대한 이메일 알림을 받습니다.

결과
취약성 관리자 작업 공간의 목록 페이지에서 예외 〉 모두에서 해당하는 상태 변경 승인 기록(VCA#)을 열고 승인 상태 열에서 요청 상태를 확인합니다.

승인 상태	결과
승인됨	정정 작업의 상태가 긍정 오류로 이유와 함께 종결됨으로 전환됩니다. 상태 및 이유가 기록으로 롤다운됩니다.
거부됨	정정 작업 및 해당 기록의 상태는 변경되지 않습니다.

기록 또는 정정 작업의 활동 스트림 에서 요청의 전체 워크플로우를 볼 수 있습니다.

에서 기록을 대량으로 종결 취약성 관리자 작업 공간

의 취약성 관리자 작업 공간대량 편집 기능을 사용하여 여러 기록(VIT, AVIT 또는 CVIT)을 동시에 닫습니다.

시작하기 전에
필요한 역할:

- 호스트 취약 항목(VIT)의 경우 sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin
- 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_sec_manager
- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.vulnerability_analyst 또는 sn_vul_container.vulnerability_admin

프로시저

1. 다음으로 이동 작업 공간 〉 취약성 관리자 작업 공간 〉 목록.
2. 목록 페이지의 다음 목록 중 하나에서 활성 또는 모두 목록을 엽니다.
   - 호스트 취약한 항목
   - 컨테이너 취약한 항목
   - 애플리케이션 취약한 항목
3. 다음 중 하나를 수행합니다.
   - 기록 선택 필드에서 선택한 항목만 옵션을 사용하려면 각 항목 옆에 있는 확인란을 선택합니다.
   - 기록 선택 필드의 필터와 일치하는 모든 취약한 항목 옵션을 사용하려면 필터를 적용합니다.
4. **Bulk** Edit(일괄 편집) 버튼을 선택합니다.
5. 양식의 필드에 내용을 입력하여 선택한 기록을 닫습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모달 필드 대량 편집

필드	설명
기록 선택	업데이트할 기록입니다. 선택 항목은 다음과 같습니다. ○ 선택한 항목만: 확인란을 사용하여 선택한 기록을 업데이트하려면 이 옵션을 선택합니다. ○ 필터와 일치하는 모든 취약한 항목: 필터링된 기록을 업데이트하려면 이 옵션을 선택합니다. ○ 정정 작업: 정정 작업의 기록을 업데이트한 다음 정정 작업 필드에서 원하는 정정 작업을 선택하려면 이 옵션을 선택합니다. ○ 취약성 항목: CVE(일반적인 취약한 항목)에 특정한 기록을 업데이트하려는 경우 이 옵션을 선택한 다음 취약성 항목 필드에서 CVE를 선택합니다. **주:** ○ 잘못된 CI 또는 CI가 해제된 기록은 업데이트되지 않습니다. ○ 오픈, 조사 중 또는 구현 대기 중 상태의 기록만 업데이트됩니다.
상태	상태를 종결로 선택합니다.
이유	기록을 종결하는 이유: ○ 긍정 오류 **주:** 이 옵션을 선택하여 기록을 긍정 오류로 표시하면 이유, 간단한 설명 및 추가 정보 필드가 나타납니다. 가양성의 대량 편집에 대한 자세한 내용은 다음 문서를 참조하십시오 취약성 관리자 작업 공간에서 가양성에 대한 대량 편집. ○ 취소됨 ○ 고정 **주:** 그 이유, 취소됨 및 수정됨은 CVIT에 적용되지 않습니다.
작업 메모	변경 내용을 설명하기 위해 입력하는 텍스트입니다.

6. 편집을 클릭합니다.

대량 편집 비동기 작업은 관련 기록을 업데이트합니다.

에서 정정 작업 및 기록에 대한 예외 요청 취약성 관리자 작업 공간

취약성 관리자 작업 공간에서 취약성 관리자와 분석가는 정정 작업(VUL, AVUL, CVUL 또는 CRG) 및 기록(VIT, CVIT, AVIT 또는 CTR)에 대한 예외 및 가양성을 요청할 수 있습니다. 정정 작업을 분할하여 변경 요청을 생성할 수도 있습니다.

필요한 역할:

- 호스트 취약 항목(VIT)의 경우 sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin
- 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_sec_manager

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.vulnerability_analyst 또는 sn_vul_container.vulnerability_admin
- 구성 테스트 결과(CTR)에 대한 sn_vulc.admin

주:
의 취약성 대응v19.0부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v19.0 이전 용어	용어집 **v19.0** 이상
테스트 결과 그룹	정정 작업
구성 문제	구성 테스트 결과
정책	테스트 그룹

에서 취약성 관리자 작업 공간기록 및 정정 작업에 대해 다음을 수행할 수 있습니다.

- 정정 작업(VUL, AVUL, CVUL 및 CRG)을 분할합니다.
- 기록(VIT, AVIT 또는 CVIT) 또는 정정 작업(VUL, AVUL, CVUL 또는 CRG)에 대한 예외를 요청합니다.
- 기록(VIT, AVIT 또는 CVIT) 또는 정정 작업(VUL, AVUL, CVUL 또는 CRG)에 대한 정책 예외를 요청합니다.
- 호스트 취약한 항목(VIT) 및 정정 작업(VUL)에 대한 위험 감소 요청
- 정정 작업에 대한 변경 요청(VUL, CVUL 또는 CRG)을 생성합니다.
- 기록(VIT, AVIT 또는 CVIT) 또는 정정 작업(VUL, AVUL, CVUL 또는 CRG)에 대해 긍정 오류를 요청합니다.

주:
정정 작업(CRG)에서 일련의 테스트 결과에 대해 긍정 오류 요청을 제기할 수 있습니다.

의 기록 취약성 관리자 작업 공간에서 이러한 UI 작업을 시작할 수 있으며, 이는 정정 소유자가 에서 이러한 작업을 IT 정정 작업 공간수행하는 방식과 동일합니다.

자세한 내용은 다음 항목을 참조하십시오.

- 취약한 항목 또는 정정 작업에 대한 가양성 요청
- 에서 예외 요청 IT 정정 작업 공간
- 취약한 항목 또는 정정 작업에 대한 위험 감소 요청
- 에서 정정 작업 분할 IT 정정 작업 공간
- 에서 변경 요청 만들기 IT 정정 작업 공간
- 에서 사용하는 예외 GRC: 정책 및 준수 관리 요청 IT 정정 작업 공간
- 일련의 테스트 결과에 대해 긍정 오류 요청

관련 정보

예외 관리 개요

구성 준수 예외 관리 개요

취약성 관리자 작업 공간에서 대량 예외 요청

취약성 관리자 작업 공간에서 가양성에 대한 대량 편집

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약성 관리자 작업 공간에서 지연된 취약한 항목에 대한 연장 요청

지연된 취약한 항목이 지연 종료 기한에 도달하기 전에 해당 항목에 대한 연장을 요청합니다. 정정 소유자는 더 이상 이 요청을 하기 위해 지연된 기한까지 기다릴 필요가 없습니다.

시작하기 전에

필요한 역할: sn_vul.vulnerability_admin 또는 sn_vul.admin(사용하지 않음)

이 태스크 정보

클래식 환경에서 연장을 요청할 수도 있습니다.

동일한 절차에 따라 애플리케이션 취약한 항목, 컨테이너 취약한 항목, 테스트 결과 그룹 및 정정 작업에 대한 연장을 요청합니다.

프로시저

1. 다음으로 이동 작업 공간 〉 취약성 관리자 작업 공간.
2. 목록을 선택합니다.
3. 호스트 취약한 항목에서 모두를 선택합니다.
4. 상태 열에서 지연됨을 선택하여 목록을 필터링합니다.
5. 지연된 취약한 항목을 선택합니다.

   주:
   연장 요청 버튼은 취약한 항목의 상태가 연기됨인 경우에만 표시됩니다.

6. 연장 요청 버튼을 선택합니다.
7. 양식의 필드에 적절히 입력합니다.

필드	설명
연장 날짜	정정을 위해 지연된 취약한 항목을 연장해야 하는 종료 날짜를 선택합니다.
이유	문제를 지연시키는 이유를 입력합니다. 선택 항목은 다음과 같습니다. ○ 유지관리 기간을 기다리는 중 ○ 수정 사용 불가 ○ 수용된 위험 ○ 사용 중인 완화 통제 ○ 기타
추가 정보	기타 관련 정보를 입력합니다.

8. 연장 요청을 선택합니다.
   이메일은 요청 제출 및 승인자의 후속 조치 시 트리거됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

- 요청은 두 가지 수준의 승인을 거칩니다.
- 지연된 취약한 항목이 다시 확장되면 백엔드에서 연장 지연 수가 증가합니다.

9. 요청이 승인되면 기한, 이유 및 연기 메모가 업데이트됩니다.

취약성 관리자 작업 공간 참조 정보

다음 항목에서는 링크, 참조 정보 외에 에 있는 취약성 관리자 작업 공간양식 및 기록의 필드 데이터를 제공합니다.

주시 주제 양식 필드 생성

다음 표에서는 의 주시 주제 생성 양식에 있는 취약성 관리자 작업 공간필드를 설명합니다.

필드	설명
이름	감시 주제의 이름(예: ## VI)
소유자	감시 주제를 소유한 사용자의 이름입니다.
표시 순서	100에서 1000 사이의 값을 입력합니다. 기본값은 100입니다. 100부터 시작하는 낮은 값은 목록에서 오름차순으로 표시됩니다.
소유 그룹	감시 주제를 소유한 그룹의 이름입니다.
활성	주시 주제를 활성화 또는 비활성화합니다. 기본값은 선택되어 있습니다(활성).
관찰 목록	알림을 수신하고 주시 주제를 볼 수 있는 사용자의 이름을 추가합니다.
설명	주시 주제를 설명하는 텍스트입니다. 이 텍스트는 이 감시 주제에서 정정 작업을 생성할 때 설명 필드에 표시됩니다.
범주	감시 주제가 생성되는 기록의 유형입니다.

관련 정보

에서 주시 주제 생성 취약성 관리자 작업 공간

GRC 요청 예외 양식 필드

다음 테이블에는 GRC 요청 예외 양식에 대한 필드 설명이 나와 있습니다.

예외 요청 양식

필드	설명
정책	예외를 요청하는 취약성 관리 정책입니다.
컨트롤 목적	선택한 정책과 연결된 통제 목표입니다. 정책을 선택하지 않으면 모든 통제 목표가 나열됩니다.
유효 기간(시작)	예외가 시작되는 날짜입니다. 기본값은 현재 날짜입니다. 이 날짜는 과거일 수 없습니다.
유효 기간	정책 예외가 만료되고 취약한 항목 또는 그룹의 상태가 연기됨에서 미결로 변경되는 날짜입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예외 요청 양식

필드	설명
	주: 정책 예외가 유효한 일 수는 정책 및 준수에서 정책에 대해 설정한 최대 예외 기간(일) 을 초과할 수 없습니다. 자세한 내용은 정책 만들기를 참조하세요.
이유	예외를 요청하는 이유입니다.
근거	이 요청이 수행되는 이유와 관련된 상세 정보입니다. 정정 소유자가 이 필드를 입력해야 합니다.

정정 다이제스트 양식 필드 생성

다음 표에서는 정정 다이제스트 생성 양식의 필드를 보여줍니다.

정정 다이제스트 필드 생성

필드	설명
활성 확인란	이 확인란은 기본적으로 활성화되어 있습니다. 이메일 알림을 보내지 않으려면 이 필드를 비활성화합니다.
실행	기본값은 매주입니다. 목록에서 옵션을 선택합니다.
일	월요일이 기본값입니다. 목록에서 옵션을 선택합니다.
시간	이메일을 전송할 시간을 설정합니다. 작업을 실행하는 인스턴스에서 사용하는 시간대가 아닌 다른 시간대를 원하는 경우 시간대를 선택합니다.

보상 통제가 위험 점수 및 만료 날짜에 미치는 영향

업데이트 적용 소유자는 호스트 취약한 항목 또는 업데이트 적용 작업에 대한 위험 감소를 요청할 수 있습니다. 그리고 취약성 관리자 또는 분석가는 이러한 위험 감소 요청을 승인할 수 있습니다.

위험 감소를 요청하고 위험 감소 승인을 승인하는 방법에 대한 자세한 내용은 각각 문서를 참조하십시오 취약한 항목 또는 정정 작업에 대한 위험 감소 요청에서 요청 승인 또는 거부 취약성 관리자 작업 공간 .

위험 감소 요청이 승인되면 상태 변경 승인(VCA#) 기록의 원하는 값 (위험 등급)에 따라 위험 점수가 낮아집니다. 위험 감소 요청이 승인되면 원하는 위험 등급의 가장 높은 위험 점수가 기록에 할당됩니다. 다음 예는 보상 통제가 적용될 때 위험 점수와 원래 위험 점수가 업데이트되는 방식을 보여줍니다. 다음 예에서는 위험 등급의 기본 최고 위험 점수가 사용됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보상 통제가 위험 점수 및 원래 위험 점수에 미치는 영향

시나리오	위험 등급	위험 점수	원래 위험 점수 (계산된 위험 점수)
v20.0 이전 데이터	2 - 높음	80	v20.0 이전에는 이 필드를 사용할 수 없습니다.
v20.0으로 업그레이드한 후	2 - 높음	80	영
수집 중에 계산된 위험 점수가 90으로 변경됩니다.	1 - 위험	90	영
보상 통제를 적용할 때	3 - 보통	69	90
수집 중에 계산된 위험 점수가 70으로 변경됩니다.	3 - 보통	69	70
수집 중 계산된 위험 점수가 50으로 변경됩니다.	3 - 보통	50	50
수집 중 계산된 위험 점수가 80으로 변경됩니다.	3 - 보통	50	80
보상 통제가 위험 감소를 위한 종료 날짜에 만료되는 경우	2 - 높음	80	영

보상 통제가 정정 작업에 미치는 영향

정정 작업에 대한 위험 감소 요청이 승인되면 보상 통제가 취약한 항목에 미치는 영향은 다음과 같습니다.

- 정정 작업에 적용된 보상 통제는 정정 작업의 상태 변경 승인에서 필요한 값에 해당하는 위험 점수보다 큰 위험 점수를 가진 취약한 항목(종결 상태의 항목 제외)에 적용됩니다. 그리고 이러한 취약한 항목의 위험 점수는 원하는 값에 따라 감소합니다.
- 보상 통제가 이미 적용된 취약한 항목에 대해 위험 감소를 위한 종료 날짜가 변경되지 않고 유지됩니다. 정정 작업의 위험 감소를 위한 종료 날짜 로 업데이트되지 않습니다.
- 이전에 취약한 항목에 보상 통제가 적용되지 않은 경우에만 위험 감소를 위한 종료 날짜가 취약한 항목으로 롤다운됩니다. 정정 작업에 보상 통제를 다시 적용하면 취약한 항목의 위험 감소를 위한 기존 종료 날짜가 우선시되므로 위험 감소를 위한 종료 날짜가 취약한 항목으로 롤다운되지 않습니다.
- 보상 통제가 이미 적용된 정정 작업에 새 취약한 항목이 추가되면 위험이 취약한 항목으로 롤다운되지 않습니다.

취약한 항목에 대한 보상 통제의 영향

취약한 항목에 대한 위험 감소 요청이 승인되면 다음을 수행합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 새 위험 점수가 위험 점수 필드에 표시되고 이전 위험 점수(계산된 위험 점수)는 원래 위험 점수 필드로 이동합니다. 이 변경은 위험 감소의 종료 날짜 필드에 지정된 날짜까지 유지됩니다.
- 취약한 항목에 보상 통제가 이미 적용되어 있는 경우 수집 중:
  - 계산된 위험 점수가 위험 점수보다 크면 위험 점수가 동일하게 유지되고 원래 위험 점수가 계산된 위험 점수로 업데이트됩니다.
  - 계산된 위험 점수가 위험 점수보다 낮으면 위험 점수와 원래 위험 점수가 모두 계산된 위험 점수로 업데이트됩니다.
- 보상 통제가 이미 적용된 취약한 항목에 대해 CI(구성 항목)가 변경된 경우:
  - 시스템 속성이 true로 설정되어 있으므로 기본적으로 취약한 항목에 대한 CI가 *sn_sec_cmn.update_on_ci_change* 업데이트됩니다.

    보상 통제는 취약한 항목에 계속 적용할 수 있습니다.
  - 시스템 속성이 false로 설정된 경우 *sn_sec_cmn.update_on_ci_change* 취약한 항목이 종결되고 새로운 취약한 항목이 생성됩니다.

    이전 취약한 항목에 적용된 보상 통제가 새로운 취약한 항목에 적용되며 위험 감소를 위한 종료 날짜, 원래 위험 점수 및 위험 점수 는 동일하게 유지됩니다.
- 스캐너에서 취약한 항목을 다시 열고 보상 통제가 이미 적용된 경우, 재개된 후에도 동일한 보상 통제가 적용됩니다.

관련 정보

위험 감소를 위한 보상 통제 이해

라이브러리에 보정 통제 추가

위험 감소 요청을 위해 CVE 또는 TPE와 보상 통제 연결

CVE 또는 TPE에 대한 위험 감소 사용 안 함 또는 사용

#unique_159_Connect_42_li-risk-reduction-vmws

의 정정 작업 생성 취약성 관리자 작업 공간 예시 및 **IT** 정정 작업 공간

및 IT 정정 작업 공간에서 수동으로 취약성 관리자 작업 공간 정정 작업을 생성하면 선택한 그룹화 기준에 따라 기록이 정정 작업으로 그룹화됩니다.

정정 작업 생성을 위해 10개의 기록이 선택된 다음 예를 생각해 보십시오. 기록 선택 상세 정보와 간략한 설명을 입력한 후 요구 사항에 따라 그룹화 기준을 선택한 다음 이미 기존 정정 작업의 일부인 기록을 관리할 방법을 선택합니다.

Example: 그룹화 기준에 따라 정정 작업 생성

정정 작업 생성을 위해 선택한 취약한 항목

취약한 항목 **ID**	기존 정정 작업	할당 그룹	구성 항목	취약성	위험 등급
VIT10001	VUL10021, VUL10022	정정 관리자	APSVR-NY-1672	CVE-2018-9024	10
VIT10002	-	취약성 대응	DEV-IBM-NY-682	CVE-2018-9022 (영문)	10
VIT10003	VUL10021	LDAP 관리자	DEV-IBM-NY-682	CVE-2012-5357	7

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

정정 작업 생성을 위해 선택한 취약한 항목

취약한 항목 ID	기존 정정 작업	할당 그룹	구성 항목	취약성	위험 등급
VIT10004	-	정정 관리자	CRMBK-SD-4210	CVE-2013-1714	10
VIT10005	VUL10022	취약성 대응	DEV-IBM-NY-682	CVE-2018-9022 (영문)	20
VIT10006	-	정정 관리자	CRMBK-SD-4210	CVE-2013-1712 (영문)	20
VIT10007	-	LDAP 관리자	DEV-SAP-SD-9388	CVE-2013-3906	6
VIT10008	-	LDAP 관리자	DEV-IBM-NY-682	CVE-2013-3906 (영문)	6
VIT10009	-	정정 관리자	CRMBK-SD-4210	CVE-2013-1712 (영문)	20
VIT10010	-	LDAP 관리자	DEV-SAP-SD-9388	CVE-2013-3904 (영문)	6

다음 목록에서는 정정 작업을 생성할 때 선택한 그룹화 기준에 따라 기록이 정정 작업으로 그룹화되는 방식을 보여줍니다.

시나리오 1: 그룹화 기준이 "할당 그룹"으로 선택되고 다른 정정 작업의 기록 관리가 "새 정정 작업에 대한 기록 건너뛰기"로 선택됩니다.

할당 그룹이 동일한 기록은 하나의 정정 작업으로 그룹화됩니다. 이미 기존 정정 작업에 일부인 기록은 새 정정 작업에 추가되지 않습니다. 여기에서 정 정 관리자, **LDAP** 관리자 및 취약성 대응 할당 그룹에 할당된 기록을 포함하는 세 가지 정정 작업이 생성됩니다.

시나리오 1에서 생성된 정정 작업

정정 작업 생성됨	정정 작업의 기록
정정 작업 1 - VUL10001	이 정정 작업에는 정정 관리자 할당 그룹에 할당된 기록이 포함되어 있습니다. • VIT10004 • VIT10006 • VIT10009 VIT10001 기록은 VUL10001 정정 작업으로 이동되지 않습니다.
정정 작업 2 - VUL10002	이 정정 작업에는 취약성 대응 할당 그룹에 할당된 VIT10002 기록이 포함되어 있습니다. VIT10005 기록은 VUL10002 작업으로 이동되지 않습니다.
정정 작업 3 - VUL10003	이 정정 작업에는 **LDAP** 관리자 할당 그룹에 할당된 기록이 포함되어 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시나리오 1에서 생성된 정정 작업

정정 작업 생성됨	정정 작업의 기록
	• VIT10007 • VIT10008 • VIT10010 VIT10003 기록은 VUL10003 정정 작업으로 이동되지 않습니다.

시나리오 2: 그룹화 기준이 "할당 그룹 및 구성 항목"으로 선택되고 다른 정정 작업의 기록 관리가 "새 정정 작업으로 기록 이전"으로 선택됩니다.

동일한 할당 그룹에 할당된 동일한 구성 항목이 있는 기록은 정정 작업으로 그룹화됩니다. VIT10001, VIT10003 및 VIT10005 기록이 이전 정정 작업에서 제거되고 새 정정 작업으로 이동됩니다. 여기에 5개의 정정 작업이 만들어집니다.

시나리오 2에서 생성된 정정 작업

정정 작업 생성됨	정정 작업의 일부 기록
정정 작업 1 - VUL10004	이 정정 작업에는 정정 소유자 할당 그룹에 할당되고 **APSVR-NY-1672** 구성 항목과 함께 할당된 기록이 포함되어 있습니다. • VIT10001 • [store-future: BEGIN review][End] VIT10001 기록이 VUL10021에서 제거되고 정정 작업이 VUL10022됩니다.
정정 작업 2 - VUL10005	이 정정 작업에는 취약성 대응 담당 그룹 및 **DEV-IBM-NY-682** 구성 항목과 함께 할당된 기록이 포함되어 있습니다. • VIT10002 • VIT10005 VIT10005 기록이 VUL10022 정정 작업에서 제거됩니다.
정정 작업 3 - VUL10006	이 정정 작업에는 **LDAP** 관리자 할당 그룹에 할당된 기록이 **DEV-IBM-NY-682** 구성 항목과 함께 포함되어 있습니다. • VIT10003 • VIT10008 VIT10003 기록이 VUL10021 정정 작업에서 제거됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시나리오 2에서 생성된 정정 작업

정정 작업 생성됨	정정 작업의 일부 기록
정정 작업 4 - VUL10007	이 정정 작업에는 정정 관리자 할당 그룹에 할당된 기록이 **CRMBK-SD-4210** 구성 항목과 함께 포함되어 있습니다. • VIT10004 • VIT10006 • VIT10009
정정 작업 5 - VUL10008	이 정정 작업에는 **LDAP** 관리자 할당 그룹에 할당된 기록이 **DEV-SAP-SD-9388** 구성 항목과 함께 포함되어 있습니다. • VIT10007 • VIT10010

시나리오 3: 그룹화 기준이 "할당 그룹 및 취약성"으로 선택되고 다른 정정 작업의 기록 관리가 "현재 및 새 정정 작업 모두에 기록 유지"로 선택됩니다.

동일한 할당 그룹에 할당된 동일한 취약성의 기록은 정정 작업으로 그룹화됩니다. VIT10001, VIT10003 및 VIT10005 기록은 이전 정정 작업에서 제거되지 않고 각각의 새 정정 작업에 추가됩니다. 여기에 5개의 정정 작업이 만들어집니다.

시나리오 3에서 생성된 정정 작업

정정 작업 생성됨	정정 작업의 일부 기록
정정 작업 1 - VUL10009	이 정정 작업에는 정정 소유자 할당 그룹에 할당되고 **CVE-2018-9020** 취약성이 있는 기록이 포함되어 있습니다. • VIT10001 • [store-future: BEGIN review][End] VIT10001 기록은 VUL10021의 일부로 유지되며 VUL10022 정정 작업도 포함됩니다.
정정 작업 2 - VUL10010	이 정정 작업에는 취약성 대응 할당 그룹에 할당되고 **CVE-2018-9020** 취약성이 있는 기록이 포함되어 있습니다. • VIT10002 • VIT10005 VIT10005 기록도 정정 작업의 일부로 유지됩니다VUL10022.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시나리오 3에서 생성된 정정 작업

정정 작업 생성됨	정정 작업의 일부 기록
정정 작업 3 - VUL10011	이 정정 작업에는 **LDAP** 관리자 할당 그룹에 할당된 기록과 **CVE-2012-5357** 취약성이 포함되어 있습니다. • VIT10003 • [store-future: BEGIN review][End] VIT10003 기록은 계속해서 VUL10021 정정 작업의 일부가 됩니다.
정정 작업 4 - VUL10012	이 정정 작업에는 정정 관리자 할당 그룹에 할당된 기록이 포함되어 있으며 **CVE-2013-1710** 취약성이 있습니다. • VIT10004 • VIT10006 • VIT10009
정정 작업 5 - VUL10013	이 정정 작업에는 **LDAP** 관리자 할당 그룹에 할당된 기록이 포함되어 있으며 **CVE-2013-3906** 취약성이 있습니다. • VIT10007 • VIT10008 • VIT10010

시나리오 4: 그룹화 기준을 "할당 그룹 및 위험 등급"으로 선택하고 다른 정정 작업의 기록 관리를 "현재 및 새 정정 작업 모두에 기록 유지"로 선택합니다.

동일한 할당 그룹에 할당된 동일한 위험 등급의 기록은 정정 작업으로 그룹화됩니다. VIT10001, VIT10003 및 VIT10005 기록은 이전 정정 작업에서 제거되지 않고 각각의 새 정정 작업에 추가됩니다. 여기에 5개의 정정 작업이 만들어집니다.

시나리오 4에서 생성된 정정 작업

정정 작업 생성됨	정정 작업의 일부 기록
정정 작업 1 - VUL10014	이 정정 작업에는 정정 소유자 할당 그룹에 할당되고 위험 등급이 **4** 인 기록이 포함되어 있습니다. • VIT10001 • VIT10004 VIT10001 기록은 계속해서 VUL10021 및 VUL10022 정정 작업의 일부입니다.
정정 작업 2 - VUL10015	이 정정 작업에는 취약성 대응 담당 그룹에 할당되고 위험 등급이 **2** 인 기록이 포함되어 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시나리오 4에서 생성된 정정 작업

정정 작업 생성됨	정정 작업의 일부 기록
	• VIT10002 • VIT10005 VIT10005 기록은 계속해서 정정 작업의 일부가 됩니다VUL10022.
정정 작업 3 - VUL10016	이 정정 작업에는 **LDAP** 관리자 할당 그룹에 할당되고 위험 등급이 **1** 인 기록이 포함되어 있습니다. • VIT10003 • VIT10007 • VIT10008 VIT10003 기록은 계속해서 정정 작업의 일부가 됩니다VUL10021.
정정 작업 4 - VUL10017	이 정정 작업에는 정정 관리자 할당 그룹에 할당되고 위험 등급이 **2** 인 기록이 포함되어 있습니다. • VIT10006 • VIT10009
정정 작업 5 - VUL10018	이 정정 작업에는 **LDAP** 관리자 할당 그룹에 할당되고 위험 등급이 **4** 인 기록이 포함되어 있습니다. • VIT10010 • [store-future: BEGIN review][End]

관련 정보

에서 수동으로 정정 작업 생성 취약성 관리자 작업 공간

에서 수동으로 정정 작업 생성 IT 정정 작업 공간

에서 선택한 기록에 대한 예외 재평가 취약성 관리자 작업 공간

에서 취약성 관리자 작업 공간정정 속성 재평가 및 업데이트 모달의 기록 세트에 대한 예외 규칙을 평가하면 해당 지연 상태와 지연 종료 날짜가 최신 예외 규칙에 따라 업데이트됩니다.

시나리오

다음에서 취약성 관리자 작업 공간정정 속성 모달을 재평가하고 업데이트할 때 선택한 기록 세트에 대한 예외를 평가할 때 다음과 같은 시나리오가 발생할 수 있습니다.

시나리오 **1:** 선택한 기록이 이미 수동으로 지연되고 예외 규칙의 조건과 일치하는 경우 이러한 기록은 변경 없이 지연 상태로 유지됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시나리오 **2:** 선택한 기록이 예외 규칙의 조건과 일치하고 이러한 기록이 지연이 아닌 상태(예: 오픈, 검토 중, 조사 중)인 경우 이러한 기록은 예외 규칙에 정의된 날짜까지 지연됩니다.

시나리오 **3:** 선택한 기록이 이미 지연 상태(예외 규칙 A를 사용하여 지연됨)에 있는 경우 다음 시나리오에서 지연됨 상태로 유지됩니다.

- 예외 규칙이 만료되고 기록이 조건과 일치하지 않습니다.
- 예외 규칙이 만료되고 기록이 조건과 일치하는 경우
- 예외 규칙 A가 만료되고 기록이 다른 예외 규칙 B의 조건과 일치합니다.

시나리오 **4:** 기록이 예외 규칙을 사용하여 지연되는 것을 고려하십시오. 기록의 지연 상태가 더 이상 유효하지 않도록 예외 규칙 조건을 변경한 다음 이러한 기록에 대한 예외 규칙을 다시 평가하는 경우:

- 기록이 열림 상태로 이동합니다
- 종료 날짜, 지연 날짜, 지연 수 및 기타 필드가 업데이트됩니다.

Example: 다음 호스트 취약한 항목(VIT)에 대한 예외를 평가하고 있다고 가정해 보겠습니다

다음과 같은 세부 정보가 있는 예외 규칙을 고려하십시오.

예외 규칙 상세 정보

필드	설명	값
이름	예외 규칙의 이름입니다.	중요 VIT 연기
유효 기간(시작)	VI를 연기하기 위해 이 규칙이 활성화되는 날짜입니다.	20-08-2024
유효 기간(종료)	정정 작업에서 새 VI 수락을 중지하는 날짜입니다.	30-11-2024
이유	이 예외 규칙을 생성하는 이유입니다.	위험 수락됨
할당 그룹	지연된 VI를 추적하기 위해 생성된 정정 작업이 할당된 그룹입니다.	정정 그룹 1
추가 정보	요청자가 승인자에게 제공하려는 추가 정보입니다. 이 정보는 정정 작업의 설명 필드에 채워집니다.	이 규칙은 중요 VIT를 자동으로 연기하기 위해 생성되었습니다.
조건	VI를 처리하는 동안 정의할 수 있는 VI에 대한 필터 조건입니다.	위험 등급 = 5 - 심각
기존 데이터에서 실행	이 규칙을 처음 실행할 때 기존 데이터에 대해 이 규칙을 실행할 수 있도록 하는 옵션입니다.	예
상태	예외 규칙의 상태입니다.	승인됨
실행 순서	각 예외 규칙에 대한 고유한 순서입니다.	100

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예외 규칙 상세 정보

필드	설명	값
지연 기한	VUL 및 VI가 지연될 때까지의 날짜입니다. 이 날짜에 생성된 VUL이 종결되고 모든 VI가 그룹 밖으로 이동하며 그룹 규칙이 다시 적용됩니다.	2024-12-23 16:10:29

다음 표는 여러 VIT에 대해 예외 규칙을 동시에 재평가할 때 상태가 어떻게 변경되는지 보여줍니다.

예외를 재평가하는 기록

VIT 번호	상태	위험 등급	예외 - 1을 재평가한 후 상태가 업데이트됨	종료 날짜 - **1**
VIT120067	오픈	2 - 낮음	오픈	-
VIT120068	검토 중	3 - 보통	검토 중	-
VIT120069	조사 중	5 - 중요	연기됨	2024-12-23 16:10:29
VIT120070	연기됨	5 - 중요	연기됨	2024-12-23 16:10:29
VIT120071	연기됨	2 - 낮음	연기됨	2024-10-02 16:10:29 (수동으로 연기됨)
VIT120072	종결됨	5 - 중요	종결됨	-

이전 예외 규칙의 조건이 `## ## = 2 - ##` 으로 수정되고 지연 기한 이 `2024-12-31 14:10:23` 으로 수정되면 기록이 다음과 같이 업데이트됩니다.

예외를 재평가하는 기록

VIT 번호	예외 - 1을 재평가한 후 상태가 업데이트됨	위험 등급	예외를 재평가한 후 상태 업데이트됨 - **2**	종료 날짜 - **2**
VIT120067	오픈	2 - 낮음	연기됨	2024-12-31 14:10:23
VIT120068	검토 중	3 - 보통	검토 중	-
VIT120069	연기됨	5 - 중요	연기됨	2024-12-23 16:10:29
VIT120070	연기됨	5 - 중요	연기됨	2024-12-23 16:10:29
VIT120071	연기됨	2 - 낮음	지연됨(상태 변경 없음)	2024-10-02 16:10:29 (종료일 변경 없음)
VIT120072	종결됨	5 - 중요	종결됨	-

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관련 정보

에 있는 기록의 정정 속성 재평가 취약성 관리자 작업 공간

예외 규칙 개요

구성 준수 예외 관리 개요

〔store-future: BEGIN review〕

모두 메뉴에서 리디렉션 중 취약성 관리자 작업 공간

관리자가 시스템 속성을 true로 설정하면 *sn_vul_cmn_ws.navigate_to_workspace*모두 메뉴의 , 애플리케이션 취약성 대응, 컨테이너 취약성 대응및 구성 준수 모듈에서 취약성 대응미리 정의된 필터 링크를 선택하면 다음으로 취약성 관리자 작업 공간 리디렉션됩니다.

의 홈페이지로 리디렉션 중 취약성 관리자 작업 공간

sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin 역할을 가진 사용자가 취약한 항목 모듈에서 다음과 같이 미리 정의된 필터 링크를 선택하면 모두 〉 취약성 대응 〉 취약 항목, 다음 링크는 호스트 취약성 탭에서 저장된 해당 필터의 자동 선택과 함께 의 홈 페이지에서 열립니다 취약성 관리자 작업 공간.

- 중요 위험
- 누락된 대상
- 여러 지연
- 90일 경과
- 미할당
- 그룹 해제
- 높은 위험
- 지난 90일 이내
- 해제됨
- 대상에 접근 중
- 악용 가능

sn_vul_container.vulnerability_analyst 또는 sn_vul_container.vulnerability_admin 역할을 가진 사용자가 컨테이너 취약한 항목 모듈에서 다음과 같이 미리 정의된 필터 링크를 선택하는 경우 모두 〉 컨테이너 취약성 대응 〉 컨테이너 취약한 항목, 이러한 링크는 의 홈 페이지에서 열리 취약성 관리자 작업 공간며 컨테이너 취약성 탭에 저장된 해당 필터가 자동으로 선택됩니다.

- 미할당
- 중요 및 높은 위험
- 악용 가능
- 대상에 접근 중
- 누락된 대상
- 여러 지연
- 모두

sn_vul.app_sec_manager 역할을 가진 사용자가 다음으로 이동하여 애플리케이션 취약한 항목 모듈에서 다음과 같이 미리 정의된 필터 링크를 선택하면 모두 〉 애플리케이션 취약성 대응 〉

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약한 항목, 다음 링크는 애플리케이션 취약성 탭에서 저장된 해당 필터의 자동 선택과 함께 의 홈 페이지에서 열립니다 취약성 관리자 작업 공간.

- 활성
- 누락된 정정 약정 날짜
- 여러 지연
- 미할당
- 모두

sn_vulc.admin 역할을 가진 사용자가 다음으로 이동하여 테스트 결과 모듈에서 다음과 같이 미리 정의된 필터 링크를 선택하는 경우 모두 〉 구성 준수 〉 테스트 결과, 구성 테스트 결과 탭에 저장된 필터의 자동 선택과 함께 의 홈 페이지에 링크가 열립니다 취약성 관리자 작업 공간.

- 우선순위가 부여되지 않은 테스트 결과
- 테스트 결과 오픈
- 대상에 접근 중
- 누락된 대상
- 여러 지연
- 미할당
- 모두

의 목록 페이지로 리디렉션 중 취약성 관리자 작업 공간

sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin 역할을 가진 사용자가 취약성 대응 모듈에서 다음과 같이 미리 정의된 필터 링크를 선택하는 경우 모두 〉 취약성 대응, 이러한 링크는 다음의 취약성 관리자 작업 공간목록 페이지에서 열립니다.

- 정정 작업 - 활성, 나에게 할당됨, 내 그룹에 할당됨, 모두
- 취약한 항목 - 나에게 할당됨 및 내 그룹에 할당됨
- 라이브러리 - NVD, CWE, 외부 공급업체 및 취약한 소프트웨어
- 솔루션 - 모두, 가장 높은 대체 및 취약한 항목 포함
- 내 승인

sn_vul_container.vulnerability_analyst 또는 sn_vul_container.vulnerability_admin 역할을 가진 사용자가 컨테이너 취약성 대응 모듈에서 다음과 같이 미리 정의된 필터 링크를 선택하는 경우 모두 〉 컨테이너 취약성 대응, 이러한 링크는 다음의 취약성 관리자 작업 공간목록 페이지에서 열립니다.

- 컨테이너 정정 작업 - 활성, 나에게 할당됨, 내 그룹에 할당됨 및 전체
- 컨테이너 취약한 항목 - 나에게 할당됨 및 내 그룹에 할당됨
- 라이브러리 - NVD, CWE 및 외부 공급업체
- 내 승인

sn_vul.app_sec_manager 역할을 가진 사용자가 다음으로 이동하여 애플리케이션 취약성 대응 모듈에서 다음과 같이 미리 정의된 필터 링크를 선택하는 경우 모두 〉 애플리케이션 취약성 대응, 이러한 링크는 다음의 취약성 관리자 작업 공간목록 페이지에서 열립니다.

- 정정 작업 - 활성, 나에게 할당됨, 내 그룹에 할당됨 및 모두
- 취약한 항목 - 나에게 할당됨 및 내 그룹에 할당됨

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 내 승인
- 라이브러리 - NVD, CWE 및 외부 공급업체
- 침투 테스트 평가 요청 - 활성, 모두 나에게 할당됨, 내 그룹에 할당됨
- 침투 테스트 결과 - 활성, 확인 보류 중, 나에게 할당됨, 내 그룹에 할당됨, 모두

sn_vul.app_sec_manager 역할을 가진 사용자가 다음으로 이동하여 구성 준수 모듈에서 다음과 같이 미리 정의된 필터 링크를 선택하는 경우 모두 〉 구성 준수, 이러한 링크는 다음의 취약성 관리자 작업 공간목록 페이지에서 열립니다.

- 정정 작업 - 내 오픈 작업, 모든 오픈 작업, 여러 지연 및 모든 작업
- 테스트
- 테스트 그룹
- 지원 데이터 - 권한이 부여된 소스 및 기술

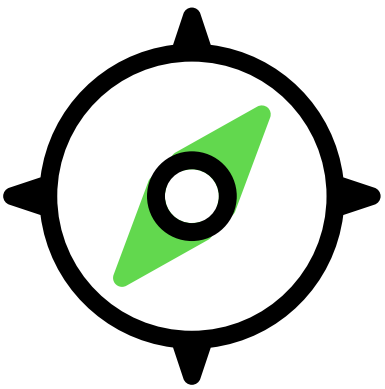
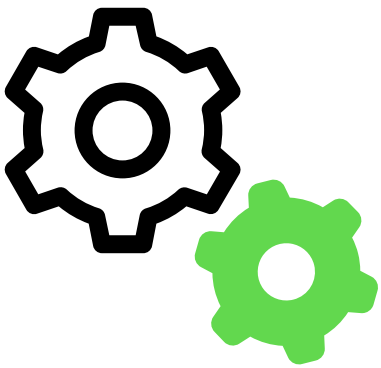
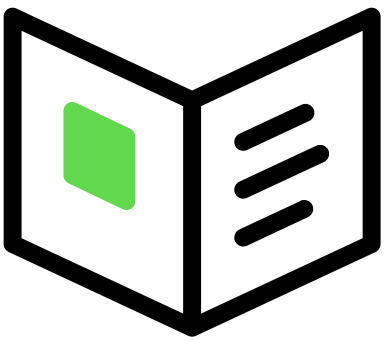
〔End〕

IT 정정 작업 공간

IT 팀은 변경 요청을 쉽게 생성하고, 취약한 항목을 다시 스캔하고, 에서 예외 요청을 제출하여 IT 관련 취약성을 해결하는 시간을 절약할 수 있습니다 IT 정정 작업 공간.

v18.0 IT 정정 작업 공간 데모

시작하기

탐색	정정	참조
		
다음에 대해 알아보기 IT 정정 작업 공간	에서 취약성 및 잘못된 구성을 정정하는 방법을 알아봅니다. IT 정정 작업 공간	구성 및 관리에 사용하는 추가 정보 가져오기 IT 정정 작업 공간

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

문제 해결 및 도움 받기

- Security Operations on ServiceNow 커뮤니티
- 알려진 오류 포털에서 알려진 오류 문서 검색
- 연락처 고객 서비스 및 지원

IT 정정 작업 공간 살펴보기

IT IT 정정 작업 공간 정정 소유자와 IT 그룹을 위한 것입니다. 이는 홈 및 목록 뷰뿐만 아니라, 클릭할 수 있는 데이터 시각화로 구성되며, 이를 통해 할당된 정정 작업과 할당된 솔루션 기록 수를 확인할 수 있습니다.

필요한 역할:

- 호스트 취약 항목(VIT)에 대한 sn_vul.remediation_owner
- 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_security_champion
- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.remediation_owner
- 구성 테스트 결과(CTR)에 대한 sn_vulc.remediation_owner

주:
의 취약성 대응v19.0부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v19.0 이전 용어	용어집 **v19.0** 이상
테스트 결과 그룹	정정 작업
구성 문제	구성 테스트 결과
정책	테스트 그룹

이 목록은 IT 정정 작업 공간 다음 페이지, 목록 및 양식으로 구성됩니다.

방문(홈) 페이지

홈페이지는 할당된 정정 작업 카드, VI 카드의 기본 솔루션, 영향을 받는 CI 카드, VI 카드의 기본 설정 패치 및 정정 작업 목록으로 구성됩니다. 홈페이지에 대한 자세한 내용은 다음 문서를 참조하십시오 의 홈페이지 IT 정정 작업 공간.

대시보드 페이지

대시보드 페이지는 취약성 개선 대시보드로 구성됩니다. 대시보드 페이지에 대한 자세한 내용은 다음 문서를 참조하십시오 대시보드 페이지의 IT 정정 작업 공간.

목록 페이지

이 뷰는 정정 작업, 호스트 취약한 항목, 애플리케이션 취약한 항목, 컨테이너 취약한 항목, 사용자에게 할당된 구성 테스트 결과 및 솔루션, 예외 요청 등의 기본 및 사용자 지정 목록으로 구성됩니다. 목록 페이지에 대한 자세한 내용은 문서를 참조하십시오 의 목록 페이지 IT 정정 작업 공간. 이 페이지에서 수행할 수 있는 작업에 대한 자세한 내용은 다음 문서를 참조하십시오 에서 목록 생성 IT 정정 작업 공간.

에서 워크플로우 예시 보기 IT 정정 작업 공간

에서 IT 정정 작업 공간엔드 투 엔드 워크플로우의 예를 봅니다. IT 전문가가 작업 공간을 사용하여 중요한 취약 항목(VIT, ABIT 및 CVIT) 및 테스트 결과(TR)를 모니터링하고 할당된 취약성을 정정하는 방법을 알아봅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할:

- 호스트 취약 항목(VIT)에 대한 sn_vul.remediation_owner
- 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_security_champion
- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.remediation_owner
- 구성 테스트 결과(CTR)에 대한 sn_vulc.remediation_owner

프로시저

워크플로우의 단계를 보려면 다음 이미지를 클릭하십시오.
IT 정정 작업 공간 데모

이미지에는 다음 작업이 포함되어 있습니다.

- 홈페이지(IT 정정 소유자 방문 페이지)에서 사용자에게 할당된 정정 작업을 봅니다. 사용자와 그룹에 할당된 작업 간에 전환합니다. 솔루션이 있는 호스트 업데이트 적용 작업을 참조하십시오. 홈페이지에 대한 자세한 내용은 다음 문서를 참조하십시오 의 홈페이지 IT 정정 작업 공간.
- 목록 보기를 선택하여 할당된 작업의 목록을 확인합니다.
- 정정 작업 목록에서 내 그룹에 할당 목록을 선택한 목록 뷰에서 작업을 식별하고 자신에게 할당합니다. 목록 페이지에 대한 자세한 내용은 문서를 참조하십시오 의 목록 페이지 IT 정정 작업 공간.
- 기록 유형별로 정정 작업 그룹화: 기록 유형 열에서 점 3개 메뉴를 선택한 다음 기록 유형별로 그룹화를 선택합니다.
- 미해결 정정 작업(VUL, AVUL, CVUL 및 CRG)에서:
  - 개요 탭을 선택하여 기록과 연결된 기록(VIT, VIT, CVIT 및 TR) 및 영향을 받는 CI(구성 항목)를 확인합니다.
  - 솔루션 탭을 선택하여 호스트 업데이트 적용 작업에 대한 기본 솔루션과 잠재적 솔루션을 확인합니다.
  - 상세 정보 탭을 선택하여 상태, 할당 그룹, 할당 대상 및 간단한 설명과 같은 편집 가능한 필드를 수정하고 정정 작업에서 수행된 작업을 봅니다.
  - 상태 변경 승인 탭을 선택하여 승인 워크플로우를 추적하는 데 도움이 되는 상태 변경 승인 기록(CA#)을 확인합니다.
  - 변경 요청 탭을 선택하여 변경 요청의 승인 상태를 확인하고 새로 만들기 버튼을 선택하여 새 변경 요청을 생성합니다.
  - UI 작업 선택: 긍정 오류로 표시, 변경 생성, 작업 분할, 상태 업데이트, 예외 요청, 삭제 등. 정정에 도움이 되도록 대화 상자의 프롬프트를 따릅니다.

의 홈페이지 IT 정정 작업 공간

의 IT 정정 작업 공간 홈페이지는 사용자와 할당 그룹에 할당된 호스트, 애플리케이션, 컨테이너 및 테스트 결과 정정 작업의 통합 목록을 제공합니다.

- 호스트 취약 항목(VIT)에 대한 sn_vul.remediation_owner
- 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_security_champion
- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.remediation_owner
- 구성 테스트 결과(CTR)에 대한 sn_vulc.remediation_owner

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

홈페이지는 다음과 같은 카드와 사용자와 할당 그룹에 할당된 정정 작업 목록, 솔루션이 있는 기록으로 구성됩니다.

할당된 정정 작업 카드

사용자에게 할당된 활성 정정 작업의 수입니다. 타일을 선택하여 정정 작업 목록을 봅니다.

VI 카드의 기본 솔루션

호스트 취약한 항목을 정정하는 데 사용할 수 있는 기본 솔루션 수입니다. Vulnerability Solution Management 애플리케이션이 설치된 경우 솔루션 목록이 표시됩니다. 이 카드는 취약한 항목에 대한 외부 공급업체 벤더의 솔루션 데이터, 잠재적 및 기본 솔루션을 보여줍니다.

영향을 받는 CI 카드

사용자 또는 그룹에 할당된 VI가 있는 구성 항목의 수입니다. 자세한 내용은 에서 취약성이 있는 구성 항목 보기 IT 정정 작업 공간 문서를 참조하십시오.

VI 카드의 기본 패치

호스트 취약한 항목을 정정하는 데 사용할 수 있는 기본 패치 수입니다.

정정 작업 목록

사용자와 할당 그룹에 할당된 정정 작업의 목록입니다. 나에게 할당됨 및 내 그룹에 할당됨 옵션을 선택하여 기록을 필터링할 수 있습니다.

정정 작업을 클릭하여 상세 정보를 보고 조사를 시작할 수 있습니다. 목록 뷰에서 정정 작업, 취약한 항목, 구성, 테스트 결과 등을 볼 수 있습니다. 정정 작업을 열고 나에게 할당을 클릭하여 자신에게 작업을 할당하고 조사를 시작할 수 있습니다.

주:
정정 작업에서 자신에게 작업을 할당하지 않으면 기록 수준에서 UI 작업을 볼 수 없습니다.

추가 작업 줄임표를 클릭하고 조사 시작을 클릭하여 정정 작업을 해결합니다.

홈페이지에서 수행할 수 있는 작업에 대한 자세한 내용은 문서를 참조하십시오 다음의 정정 작업 기록 사용 IT 정정 작업 공간.

대시보드 페이지의 **IT** 정정 작업 공간

의 IT 정정 작업 공간 대시보드 페이지는 정정 작업 및 취약한 항목에 집중하는 데 사용할 수 있는 UI의 넥스트 경험 취약성 정정 대시보드를 제공합니다.

정정 소유자(sn_vul.remediation_owner)는 다음으로 이동하여 취약성 정정 대시보드에 액세스할 수 있습니다. 작업 공간 〉 **IT** 정정 작업 공간 을 클릭하고 대시보드 아이콘을 선택합니다. 취약성 개선 대시보드에 대한 자세한 내용은 다음 문서를 참조하십시오 기본 취약성 대응 대시보드 사용.

추가 옵션 아이콘 ⋮ 선택하고 새로 만들기를 선택하여 사용자 지정 대시보드를 만들 수 있습니다.

의 목록 페이지 **IT** 정정 작업 공간

정정 소유자의 목록 뷰는 IT 정정 작업 공간 정정 소유자가 자신과 할당 그룹에 할당된 기록(VIT, ABIT, CVIT 및 TR)을 보고 이러한 취약성과 잘못된 구성을 정정할 수 있도록 허용합니다. 호스트 취약한 항목(VIT) 업데이트 적용에 권장되는 기본 솔루션 목록을 볼 수도 있습니다. 이러한 목록과 함께 사용자가 제기한 예외 요청 및 침투 테스트 평가 요청 목록, 침투 테스트 평가 요청과 관련된 침투 테스트 결과, 지원되는 라이브러리 및 기타 지원되는 데이터를 볼 수 있습니다.

필요한 역할:

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 호스트 취약 항목(VIT)에 대한 sn_vul.remediation_owner
- 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_security_champion
- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.remediation_owner
- 구성 테스트 결과(CTR)에 대한 sn_vulc.remediation_owner

목록 페이지의 목록과 링크를 통해 기록과 작업에 쉽게 액세스할 수 있습니다. 여기에는 두 개의 탭이 있습니다.

- 목록 탭: 정정 작업, 정정 작업, 취약한 항목(VIT, AVIT 또는 CVIT), 솔루션, 예외 및 구성 테스트 결과(TR) 등에 대한 기본 목록을 표시합니다. 자세한 내용은 다음 테이블을 참조하십시오.
- 내 목록 탭: 목록 탭에서 이름을 변경한 목록과 생성한 모든 목록을 표시합니다.

  기록 목록을 직접 생성할 수도 있습니다. 자세한 내용은 에서 목록 생성 IT 정정 작업 공간 문서를 참조하십시오.

팁:

sn_vul_cmn_ws.navigate_to_workspace 관리자가 시스템 속성을 true로 설정한 경우 모두 메뉴의 , 애플리케이션 취약성 대응, 컨테이너 취약성 대응및 테스트 결과 모듈 구성 준수에서 취약성 대응미리 정의된 필터 링크를 선택하면 이러한 IT 정정 작업 공간링크가 의 목록 페이지에서 열립니다.

예를 들어, 다음으로 이동하여 내 그룹에 할당 됨을 선택하는 경우 모두 〉취약성 대응 〉정정 작업 〉사용자 그룹에 할당됨, 이 링크는 로 리디렉션됩니다 IT 정정 작업 공간. 정정 소유자 역할이 있는 경우 정정 작업 모듈의 내 그룹에 할당 목록이 IT 정정 작업 공간의 목록 페이지에서 열립니다. 호스트 업데이트 적용 작업을 보려면 기록 유형별로 작업을 그룹화합니다.

시스템 속성을 사용하여 목록에서 기록 수를 숨길 수 있습니다 *glide.ui.list.seismic.omit.count* . 목록에서 기록 수 표시를 해제/설정하는 방법에 대한 자세한 내용은 KBB0010402 KB 문서를 참조하십시오.

목록 탭

다음 목록이 표시됩니다.

목록

목록 항목	설명	필요한 애플리케이션	필요한 역할
정정 작업	정정 작업 목록을 보고 원하는 작업으로 이동하여 작업을 시작합니다. 다음과 같은 목록을 사용할 수 있습니다. • 나에게 할당됨: 할당된 모든 호스트, 애플리케이션, 컨테이너 및 테스트 결과 정정 작업을 나열합니다. • 내 그룹에 할당: 사용자가 속한	취약성 대응, 애플리케이션 취약성 대응, 컨테이너 취약성 대응및 구성 준수	• 호스트 취약 항목(VIT)에 대한 sn_vul.remediation_owner • 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_security_champion • 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.remediation_owne • 구성 테스트 결과(CTR)에 대한 sn_vulc.remediation_owner

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

목록

목록 항목	설명	필요한 애플리케이션	필요한 역할
	할당 그룹에 할당된 모든 호스트, 애플리케이션, 컨테이너 및 테스트 결과 정정 작업을 나열합니다. 작업을 기록 유형별로 그룹화하여 호스트, 애플리케이션, 컨테이너 및 구성 테스트 결과 정정 작업으로 분류합니다. 클래식 UI의 정정 작업 규칙에 의해 생성된 정정 작업에는 빈 정정 작업량이 있습니다.		
영향을 받은 자산	영향을 받는 자산의 목록을 봅니다. 다음과 같은 목록을 사용할 수 있습니다. • 나에게 할당됨: 나에게 할당된 영향을 받는 구성 항목 목록 • 내 그룹에 할당: 할당 그룹에 할당된 영향을 받는 구성 항목의 목록입니다.	취약성 대응, 애플리케이션 취약성 대응, 컨테이너 취약성 대응및 구성 준수	• 호스트 취약 항목(VIT)에 대한 sn_vul.remediation_owner • 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_security_champion • 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.remediation_owne • 구성 테스트 결과(CTR)에 대한 sn_vulc.remediation_owner
호스트 취약한 항목	호스트 취약한 항목의 목록을 보고 원하는 항목으로 이동하여 작업을 시작합니다. 이 목록을 사용할 수 있습니다. • 나에게 할당됨: 정정을 위해 사용자에게 할당된 호스트 취약한 항목 목록입니다. • 내 그룹에 할당됨: 사용자가 속한 할당 그룹에 할당된 호스트 취약한 항목의 목록입니다.	취약성 대응	호스트 취약 항목(VIT)에 대한 sn_vul.remediation_owner

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

목록

목록 항목	설명	필요한 애플리케이션	필요한 역할
애플리케이션 취약한 항목	호스트 취약한 항목의 목록을 보고 원하는 항목으로 이동하여 작업을 시작합니다. 다음과 같은 목록을 사용할 수 있습니다. • 나에게 할당됨: 정정을 위해 사용자에게 할당된 애플리케이션 취약한 항목 목록입니다. • 내 그룹에 할당: 사용자가 속한 할당 그룹에 할당된 애플리케이션 취약한 항목의 목록입니다.	애플리케이션 취약성 대응	sn_vul.app_security_champion
컨테이너 취약한 항목	컨테이너 취약한 항목 목록을 보고 원하는 항목으로 이동하여 작업을 시작합니다. 이 목록 뷰에는 다음이 포함됩니다. • 나에게 할당됨: 정정을 위해 사용자에게 할당된 컨테이너 취약한 항목 목록입니다. • 내 그룹에 할당: 사용자가 속한 할당 그룹에 할당된 컨테이너 취약한 항목의 목록입니다.	컨테이너 취약성 대응	sn_vul_container.remediation_owner 사후 인시던트 검토를 수행하는 데 필요한 평가 목록을 봅니다.
구성 테스트 결과	테스트 결과 목록을 보고 원하는 기록으로 이동하여 작업을 시작합니다. 이 목록 뷰에는 다음이 포함됩니다. • 나에게 할당됨: 정정을 위해 사용자에게 할당된 구성 테스트 결과 목록입니다. • 내 그룹에 할당: 사용자가 속한	구성 준수	sn_vulc.remediation_owner

기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

목록

목록 항목	설명	필요한 애플리케이션	필요한 역할
	할당 그룹에 할당된 구성 테스트 결과 목록입니다.		
솔루션	솔루션 관리 애플리케이션의 솔루션을 나열합니다. Vulnerability Solution Management 애플리케이션이 설치된 경우 솔루션 목록이 표시됩니다. • 모두: 호스트 취약한 항목을 정정하는 데 사용하는 사용 가능한 모든 솔루션을 표시합니다. • 가장 높은 대체: 기본 솔루션을 채우는 데 사용되는 모든 솔루션을 표시합니다. • 취약한 항목 포함: 취약한 항목에서 기본 솔루션으로 사용되고 있는 솔루션을 표시합니다.	취약성 대응	sn_vul.remediation_owner
예외 요청	• 내 요청: 호스트, 애플리케이션 및 컨테이너 취약한 항목과 해당 정정 작업에 대해 사용자가 제기한 모든 예외, 가양성 및 할당 해제 승인 요청 목록입니다. • 내 요청(구성 준수): 테스트 결과와 작업 중인 정정 작업에 대해 사용자가 제기한 모든 예외,	취약성 대응, 애플리케이션 취약성 대응, 컨테이너 취약성 대응및 구성 준수	• 호스트 취약 항목(VIT)에 대한 sn_vul.remediation_owner • 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_security_champion • 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.remediation_owne • 구성 테스트 결과(CTR)에 대한 sn_vulc.remediation_owner

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

목록

목록 항목	설명	필요한 애플리케이션	필요한 역할
	가양성 및 할당 해제 승인 요청의 목록입니다.		
라이브러리	다음 목록이 포함되어 있습니다. • **NVD**: NIST(National Institute of Standards and Technology)에서 유지 관리하는 포괄적인 취약성 인텔리전스 라이브러리입니다. NVD에서 발견한 취약성 목록으로, 보안 검사 목록, 보안 관련 소프트웨어 결함, 잘못된 구성, 제품 이름 및 익스플로잇을 포함한 영향 메트릭이 포함됩니다. • **CWE**: 커뮤니티에서 개발한 소프트웨어 약점 유형의 목록입니다. 각 CWE 기록에는 약점을 설명하는 관련 지식 문서도 포함되어 있습니다. • 앱 취약성: 모든 외부 공급업체 애플리케이션 취약성 항목의 목록입니다. • **TPE:** 인스턴스에서 임포트한 외부 공급업체 취약성의 목록입니다. 관련 참조, 취약한 항목, 익스플로잇 및 CVE 목록을 포함합니다. • 테스트: 테스트 결과가 준수해야 하는 외부 공급업체 통합에서 임포트한 테스트입니다.	취약성 대응, 애플리케이션 취약성 대응, 컨테이너 취약성 대응및 구성 준수	• 호스트 취약 항목(VIT)에 대한 sn_vul.remediation_owner • 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_security_champion • 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.remediation_owne • 구성 테스트 결과(CTR)에 대한 sn_vulc.remediation_owner

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

목록

목록 항목	설명	필요한 애플리케이션	필요한 역할
	• 테스트 그룹: 외부 공급업체 통합에서 임포트한 테스트 그룹/정책 목록입니다. 테스트 그룹에는 테스트 세트가 포함되어 있습니다.		
CMDB	• 검색된 항목: 검색된 모든 항목의 목록입니다. • 검색된 컨테이너 이미지:	취약성 대응, 애플리케이션 취약성 대응, 컨테이너 취약성 대응및 구성 준수	• 호스트 취약 항목(VIT)에 대한 sn_vul.remediation_owner • 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_security_champion • 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.remediation_owne • 구성 테스트 결과(CTR)에 대한 sn_vulc.remediation_owner
침투 테스트 평가 요청	비즈니스 애플리케이션의 보안 평가를 수행하기 위해 사용자가 보안 팀에 제출하는 침투 테스트 평가 요청입니다. 이 목록에는 다음이 포함됩니다. • 나에게 할당됨: 사용자가 제기한 침투 테스트 평가 요청 목록입니다. • 내 그룹에 할당: 할당 그룹의 사용자가 제기한 침투 테스트 평가 요청 목록입니다.	애플리케이션 취약성 대응	sn_vul.app_security_champion
침투 테스트 결과	보안 팀에서 펜 테스트 평가를 수행하는 동안 식별된 취약성 목록: • 나에게 할당됨: 정정을 위해 사용자에게 할당된	애플리케이션 취약성 대응	sn_vul.app_security_champion

기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

목록

목록 항목	설명	필요한 애플리케이션	필요한 역할
	침투 테스트 결과 목록입니다. • 내 그룹에 할당됨: 정정을 위해 할당 그룹에 할당된 침투 테스트 결과 목록입니다.		
지원 데이터	이 목록 뷰에는 다음이 포함됩니다. • 권한이 부여된 소스: 기록을 생성하는 데 사용된 소스 게시글을 조사하는 데 유용한 요약 정보를 제공하는 신뢰할 수 있는 소스 목록입니다. • 기술: 각 권위 있는 출처 및 인용에 대한 요약 정보를 제공하는 기술 목록입니다 (Qualys에서는 프레임워크라고도 함).	구성 준수	sn_vulc.remediation_owner

관련 정보

에서 목록 뷰 사용 취약성 관리자 작업 공간

IT 정정 작업 공간 사용

사용자와 IT 정정 작업 공간 그룹에 할당된 호스트 취약성, 애플리케이션 취약성, 컨테이너 취약성 및 잘못된 구성의 통합 목록을 제공합니다. 이 작업 공간을 사용하여 취약성 및 잘못된 구성에 대한 정정 및 예외를 요청할 수 있습니다.

다음에서 검색 결과 열기 IT 정정 작업 공간

애플리케이션 범위를 변경하여 클래식 UI 대신 검색 결과를 IT 정정 작업 공간 열려면 애플리케이션 범위를 로 IT 정정 작업 공간 설정합니다.

시작하기 전에
필요한 역할:

- 호스트 취약 항목(VIT)에 대한 sn_vul.remediation_owner
- 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_security_champion
- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.remediation_owner
- 구성 테스트 결과(CTR)에 대한 sn_vulc.remediation_owner

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보
예를 들어 애플리케이션 범위를 IT 정정 작업 공간로 설정하여 검색 필드에서 호스트 취약한 항목을 해당 번호와 함께 검색하면 VIT가 의 기록 뷰IT 정정 작업 공간에서 열립니다.

프로시저

1. 통합 탐색 모음에서 지구본 아이콘 선택합니다.
2. 애플리케이션 범위를 선택한 다음 범위를 **IT** 정정 작업 공간으로 설정합니다.

결과
통합 탐색 모음의 검색 필드에서 VIT, 정정 작업, 상태 변경 승인 등의 기록을 검색하면 에서 IT 정정 작업 공간기록이 열립니다.

범위가 전역이 아닌 경우 지구본 아이콘에 빨간색 링이 있는 표시됩니다. 범위를 변경하려면 다시 선택합니다.

취약성 대응 작업 공간에서 이메일 다이제스트 사용

이메일 알림을 사용하여 정정 진행률을 보고 작업이 SLA에 근접했거나 SLA가 지난 시기를 알 수 있습니다.

시작하기 전에
필요한 역할:

- 호스트 취약 항목(VIT)에 대한 sn_vul.remediation_owner
- 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_security_champion
- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.remediation_owner
- 구성 테스트 결과(CTR)에 대한 sn_vulc.remediation_owner

이 태스크 정보
정정 소유자는 작업 영역에 들어와서 이메일 알림을 작업의 요약으로 봅니다. 달성한 것, 다가오고 있는 것, 기한이 지난 것을 확인합니다. 알림을 사용하면 중요한 정정 작업을 구성하고 우선순위를 지정할 수 있습니다. 이메일의 링크를 클릭하면 작업 공간으로 바로 연결됩니다. 알림은 IT 전문가가 작업 상태를 한눈에 파악하는 데 도움이 될 수 있습니다. 취약성 관리자는 IT 전문가가 정정 작업을 위해 이메일 서비스에서 직접 플랫폼으로 들어갈 수 있도록 지원합니다.

이 기능을 구성하는 방법에 대한 자세한 내용은 을 참조하십시오 작업 공간에서 이메일 알림 취약성 대응 설정 .

기본적으로 이메일에는 종결한 작업, 사용자와 그룹에 할당된 총 활성 작업, 새로 할당된 작업, 종결된 VIT 및 기타 정보가 표시됩니다.

프로시저

1. 이메일로 이동하여 알림을 찾은 다음 클릭하여 엽니다.
   작업 상태에 대한 정보가 포함된 알림이 표시됩니다.
2. 작업 공간으로 이동을 클릭하여 작업 영역으로 이동합니다.

에서 목록 생성 **IT** 정정 작업 공간

의 IT 정정 작업 공간목록 뷰를 사용하면 사용자와 그룹에 할당된 정정 작업과 기록을 볼 수 있습니다. 또한 정정 작업(VUL, AVUL, CVUL 및 CRG), 취약한 항목(VIT, AVIT 및 CVIT) 및 테스트 결과(TR)에 대한 예외 및 긍정 오류 요청을 추적하고 솔루션을 볼 수 있습니다.

시작하기 전에
필요한 역할:

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 호스트 취약 항목(VIT)에 대한 sn_vul.remediation_owner
- 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_security_champion
- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.remediation_owner
- 구성 테스트 결과(CTR)에 대한 sn_vulc.remediation_owner

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 **IT** 정정 작업 공간.
2. 목록 아이콘( )을 선택합니다.
   목록 뷰가 표시됩니다.
   - 필터링된 목록을 클릭하면 사용자 또는 그룹에 할당된 총 활성 정정 작업 또는 기록 수를 볼 수 있습니다. 이러한 기록에서 수행할 수 있는 작업에 대한 자세한 내용은 을 참조하십시오 다음의 정정 작업 기록 사용 IT 정정 작업 공간 .
   - 본인 또는 솔루션이 있는 그룹에 할당된 총 VI 수를 봅니다. VI 카드 에서 기본 솔루션을 클릭하여 목록을 표시합니다.
   - 취약한 **CI** 탭 또는 목록 뷰에서 나와 내 그룹에 할당된 취약한 CI 목록에서 사용자와 그룹에 할당된 취약성이 있는 취약한 CI를 확인합니다.
3. 내 목록 탭을 선택합니다.
4. 새 목록 추가를 선택합니다.
5. 기존 목록 또는 자체 설정을 기반으로 목록을 생성합니다.
6. 옵션: 필터링된 목록을 생성합니다.
   a. 열 선택 필드에서 표시하지 않으려는 필드를 삭제하여 목록에 표시할 열을 결정합니다.
   b. 목록을 필터링할 조건을 제공합니다.
      (Optional) 둘 이상의 조건을 추가하려면 새 조건 세트를 선택합니다.
      예를 들어 모니터링하려는 스캐너에 활성 취약한 항목의 목록을 생성하려면 **[Active][is][true]** 및 **[Source][contains][scanner-name]** 조건을 입력할 수 있습니다.
   c. 생성을 선택합니다.
      새 목록이 표시됩니다.

      주:
      목록 모듈을 나가면 종료할 때 표시되는 목록이 돌아올 때 표시되는 목록입니다. 생성한 사용자 지정 목록을 삭제하려면 목록이 표시된 상태에서 창 오른쪽에 있는 기어 아이콘을 선택한 다음 삭제를 선택합니다.
7. 목록 뷰에서 수행할 수 있는 작업은 다음 테이블을 참조하십시오.

다음의 기록 사용 **IT** 정정 작업 공간

기록을 사용하면 정정 진행률 및 자산에 대한 취약한 항목의 영향을 보는 데 도움이 됩니다.

시작하기 전에
필요한 역할:

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 호스트 취약 항목(VIT)에 대한 sn_vul.remediation_owner
- 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_security_champion
- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.remediation_owner
- 구성 테스트 결과(CTR)에 대한 sn_vulc.remediation_owner

프로시저

1. 인스턴스에서 ServiceNow AI Platform 다음으로 이동합니다. 작업 공간 〉 **IT** 정정 작업 공간.
   홈 방문 페이지가 표시됩니다.
2. 취약한 항목 기록으로 이동한 다음 홈 방문 페이지 또는 목록 뷰에서 엽니다.

   상세 정보 탭에는 취약성의 특성과 관련된 정보가 맨 위에 있는 양식 헤더에 포함되어 있습니다 (예: LINUX-DAL-4331## ### CVE-2013-5014). 양식 헤더 아래에 상태, 위험 등급, 정정 목표 날짜 값이 표시됩니다.
3. 정정 작업 기록에서 수행할 수 있는 UI 작업은 다음 테이블을 참조하십시오.

에서 수동으로 정정 작업 생성 **IT** 정정 작업 공간

의 취약성 대응v25.0.4부터 의 목록 페이지에 IT 정정 작업 공간있는 호스트 취약 항목, 애플리케이션 취약 항목, 컨테이너 취약 항목 및 구성 테스트 결과 목록에서 수동으로 업데이트 적용 작업을 생성할 수 있습니다.

시작하기 전에
필요한 역할:

- 호스트 취약 항목(VIT)에 대한 sn_vul.write_assigned 또는 sn_vul.remediation_owner
- 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_write_assigned 또는 sn_vul.app_security_champion
- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.writer_assigned 또는 sn_vul_container.remediation_owner
- 구성 테스트 결과(CTR)에 대한 sn_vulc.remediation_owner

프로시저

1. 다음으로 이동 작업 공간 〉 **IT** 정정 작업 공간 〉 목록.
2. 목록 페이지의 다음 목록 중 하나에서 활성 또는 모두 목록을 엽니다.
   - 호스트 취약한 항목
   - 애플리케이션 취약한 항목
   - 컨테이너 취약한 항목
   - 구성 테스트 결과
3. 업데이트할 기록의 확인란을 선택한 다음, 정정 작업 생성 모달의 기록 선택 필드에서 선택한 항목 옵션을 선택합니다.
4. 정정 작업 생성을 선택합니다.
5. 정정 작업 생성 모달에서 다음 상세 정보를 입력합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

정정 작업 모달 생성

필드	설명
기록 선택	선택한 항목: 선택한 기록만 업데이트합니다.
간단한 설명	정정 작업에 대한 간략한 메모입니다.
그룹화 기준	선택 항목은 다음과 같습니다. ○ 할당 그룹: 할당 그룹이 동일한 기록은 하나의 정정 작업으로 그룹화됩니다. ○ 할당 그룹 및 구성 항목: 할당 그룹 및 구성 항목이 동일한 기록이 하나의 정정 작업으로 그룹화됩니다. ○ 할당 그룹 및 취약성: 할당 그룹 및 취약성이 동일한 기록은 하나의 정정 작업으로 그룹화됩니다. ○ 할당 그룹 및 위험 등급: 할당 그룹 및 위험 등급이 동일한 기록은 하나의 정정 작업으로 그룹화됩니다.
다른 정정 작업의 기록 관리	선택 항목은 다음과 같습니다. ○ 새 정정 작업에 대한 기록 건너뛰기: 다른 정정 작업의 일부인 기록에 대해서는 아무 작업도 수행되지 않습니다. ○ 새 정정 작업으로 이동: 다른 정정 작업의 일부인 기록은 새 정정 작업으로 전송됩니다. ○ 현재 및 새 정정 작업 모두에 유지: 다른 정정 작업의 일부인 기록은 이전 정정 작업과 새 정정 작업 모두에 유지됩니다.

6. 정정 작업 생성을 선택합니다.

결과
정정 작업은 그룹화 기준에 따라 생성됩니다. 할당 그룹의 정정 소유자에게 정정 작업이 생성되어 해당 그룹에 할당되었음을 알리는 이메일 알림이 전송됩니다. 그룹화 기준 및 기록 관리 기준에 따라 정정 작업이 생성되는 방식에 대한 예는 다음 문서를 의 정정 작업 생성 취약성 관리자 작업 공간 예시 및 IT 정정 작업 공간참조하십시오.

다음의 정정 작업 기록 사용 **IT** 정정 작업 공간

정정 작업은 정정 작업을 통해 자동으로 생성되고 할당됩니다. IT 팀과 정정 소유자는 에서 IT 정정 작업 공간정정 작업을 볼 수 있습니다.

시작하기 전에
필요한 역할:

- 호스트 취약 항목(VIT)에 대한 sn_vul.remediation_owner
- 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_security_champion
- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.remediation_owner
- 구성 테스트 결과(CTR)에 대한 sn_vulc.remediation_owner

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보
취약성 관리자와 분석가가 정정을 추진하기 위해 정정 작업을 생성하면 정정 작업이 자동으로 생성되고 정정 작업의 기록 과 연결된 그룹을 기반으로 IT 팀에 할당됩니다.

취약한 **CI** 탭 또는 목록 뷰에서 나와 내 그룹에 할당된 취약한 CI 목록에서 사용자와 그룹에 할당된 취약성이 있는 취약한 CI를 확인합니다.

프로시저

1. 인스턴스에서 ServiceNow AI Platform 다음으로 이동합니다. 취약성 대응 〉 **IT** 정정 작업 공간.
   홈 방문 페이지가 표시됩니다.
2. 정정 작업 섹션에서 정정 작업을 클릭하여 엽니다.
3. 옵션: 또는 홈 페이지의 왼쪽 상단에 있는 목록 아이콘을 클릭하여 사용자 및 사용자 그룹에 할당된 모든 정정 작업(VUL, AVUL, CVUL 및 CRG) 및 기록(VIT, VIT, CVIT 및 TR) 을 볼 수 있습니다.
   목록 뷰를 사용하는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 에서 목록 생성 IT 정정 작업 공간.
4. 홈페이지 또는 목록 뷰에서 정정 작업을 클릭하여 엽니다.

   상세 정보 탭에서 할당 그룹, 상태, 간단한 설명 등과 같은 기록의 일부 정보를 업데이트할 수 있습니다. 저장을 클릭하여 변경 사항을 적용합니다.

5. 정정 작업 기록에서 수행할 수 있는 UI 작업은 다음 테이블을 참조하십시오.

   호스트 업데이트 적용 작업의 솔루션 탭에는 업데이트 적용 작업과 관련된 취약성과 가장 일치하는 기본 설정 및 잠재적 솔루션 정보가 모두 표시됩니다. 솔루션은 IT 팀이 취약성을 해결하기 위해 적용하는 패치입니다.

   취약성 솔루션 관리 애플리케이션이 설치된 경우 기본 솔루션은 취약한 항목에 적용되는 가장 높은 대체 솔루션입니다. 솔루션 목록은 호스트 업데이트 적용 작업의 취약한 항목을 기반으로 합니다.

   잠재적 솔루션은 호스트 업데이트 적용 작업에서 VIT에 사용할 수 있는 모든 솔루션 목록입니다.

   다음으로 이동하여 정정 작업에서 이 취약성의 영향을 받는 CI(자산)를 볼 수 있습니다. 개요 〉 영향을 받는 **CI**.

에서 자신에게 정정 작업 또는 기록 할당 **IT** 정정 작업 공간

작업 공간의 목록 페이지에서 IT 정정 작업 공간 정정 작업(VUL, AVUL, CVUL 또는 CRG) 또는 기록(VIT, AVIT, CVIT 또는 TR)을 자신에게 할당합니다.

시작하기 전에
필요한 역할:

- 호스트 취약 항목(VIT)에 대한 sn_vul.remediation_owner
- 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_security_champion
- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.remediation_owner
- 구성 테스트 결과(CTR)에 대한 sn_vulc.remediation_owner

프로시저

1. 다음으로 이동 작업 공간 〉 **IT** 정정 작업 공간 〉 목록 〉 정정 작업 〉 내 그룹에 할당.
2. 정정 작업 목록에서 정정 작업(VUL, AVUL, CVUL 또는 CRG)을 엽니다.
3. 오른쪽에 있는 UI 작업 버튼에서 나에게 할당을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

나에게 할당 버튼은 기록이 아직 사용자에게 할당되지 않은 경우에만 사용할 수 있습니다.

정정 작업은 정정 작업의 나에게 할당됨 목록에 표시됩니다.

4. 열려 있는 기록과 동일한 단계에 따라 자신에게 기록(VIT, AVIT, CVIT 또는 TR)을 할당할 수도 있습니다.
나에게 할당 버튼은 기록이 아직 사용자에게 할당되지 않은 경우에만 사용할 수 있습니다.

에서 취약성이 있는 구성 항목 보기 **IT** 정정 작업 공간

애플리케이션 버전 16.1 취약성 대응 을 사용하여 정정 작업에 다음과 같은 개선 사항이 추가되었습니다.

시작하기 전에
필요한 역할:

- 호스트 취약 항목(VIT)에 대한 sn_vul.remediation_owner
- 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_security_champion
- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.remediation_owner
- 구성 테스트 결과(CTR)에 대한 sn_vulc.remediation_owner

작업 공간에서 CI 데이터를 보려면 itil 또는 cmdb_read 역할도 필요합니다.

이 태스크 정보
자신에게 할당된 구성 항목 중 취약성이 있는 CI(구성 항목)를 확인합니다. 영향받는 **CI** 성과표를 클릭합니다. 왼쪽 상단의 필터 목록을 클릭하여 나에게 할당 됨 및 내 그룹에 할당됨 간에 전환합니다. 목록 뷰에서 링크를 클릭합니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 **IT** 정정 작업 공간.
홈 방문 페이지가 표시됩니다.
2. 또는 목록 뷰의 링크에서 또는 해당 모듈로 이동하여 이러한 목록을 볼 수 있습니다. 예를 들어, 모두 〉 취약성 대응 〉 정정 작업.
3. 계속하려면 하나를 선택합니다.
필터 토글에서 선택한 항목에 따라, 사용자 또는 사용자와 그룹에 할당된 다음 기록의 목록을 봅니다.
4. 영향을 받는 **CI** 성과표를 클릭합니다.

   CI 기록 목록이 표시됩니다.
5. 구성 항목을 클릭하여 해당 기록을 엽니다.
기록이 표시됩니다.

   관련 목록을 사용하면 상세 정보 및 다양한 관련 기록을 볼 수 있습니다. 이번 릴리스에서 이 기록에 대해 사용 가능한 새로운 데이터는 다음과 같습니다.
   - 이 기록에 대한 최근 활동을 보여주는 타임라인입니다.
   - 이 CI와 연결된 모든 변경 요청입니다.
   - 성과표로 쉽게 이동하고 이 CI와 연관된 정정 작업, 취약한 항목 및 기본 솔루션을 봅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 성과표로 이동하여 이 CI와 관련된 기본 패치를 볼 수 있습니다. 기본 패치는 취약한 항목과 연결된 패치입니다. 관련 목록의 패치 탭에는 CI에 대해 설치된 패치와 누락된 패치가 표시됩니다.
- 클래스, 위치, 인터넷 접근, 환경 및 유지관리 일정을 포함하는 CI에 대한 정보입니다.

에서 변경 요청 만들기 **IT** 정정 작업 공간

정정 작업(VUL, AVUL, CVUL 또는 CRG)에서 변경 요청을 생성합니다. 또는 기존 변경 요청에 정정 작업을 추가합니다.

시작하기 전에
필요한 역할:

- 호스트 취약 항목(VIT)에 대한 sn_vul.remediation_owner
- 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_security_champion
- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.remediation_owner
- 구성 테스트 결과(CTR)에 대한 sn_vulc.remediation_owner

주:
에서 변경 요청을 IT 정정 작업 공간제출하려면 itli 역할이 필요합니다.

이 태스크 정보
정정 작업에 대한 변경 요청을 생성하려는 이유는 여러 가지가 있을 수 있습니다. 일반적으로 조사에 취약성을 수정하기 위해 수동 개입이 필요하기 때문입니다.

클래식 환경에서 변경 요청 및 변경 요청을 만드는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 를 위한 변경 관리 취약성 대응.

주:
의 취약성 대응v19.0부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v19.0 이전 용어	용어집 **v19.0** 이상
테스트 결과 그룹	정정 작업
구성 문제	구성 테스트 결과
정책	테스트 그룹

프로시저

1. 다음으로 이동 작업 공간 〉 **IT** 정정 작업 공간.
2. 목록 아이콘을 선택합니다.
3. 목록 페이지의 정정 작업 목록에서 변경 요청을 생성할 정정 작업(VUL, AVUL, CVUL 또는 CRG)을 찾습니다.
4. 오른쪽의 UI 작업 버튼에서 목록을 확장하고 다음 중 하나를 선택합니다.
   - 변경 작성 클릭
   - 기존 변경에 추가
5. 새 변경 요청을 생성하려면 표시되는 모달의 필드에 내용을 입력합니다.
   양식 필드에 대한 자세한 내용은 변경 요청 양식 필드 생성 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

6. 변경 요청 생성을 선택합니다.
   정정 작업 기록이 표시되고 변경 요청이 성공적으로 생성되었음을 나타내는 메시지가 표시됩니다.

   기록과 연결된 모든 변경 요청을 보려면 기록에서 변경 요청 관련 링크를 클릭합니다.

7. 또는 이 정정 작업을 기존 변경 요청에 추가하려면 다음 단계를 수행합니다.

   a. 아래쪽 화살표를 클릭하여 변경 생성 버튼의 목록을 확장합니다.

   b. 기존 변경에 추가를 선택합니다.

   c. 표시되는 모달에서 검색 아이콘을 클릭하여 기존 변경 요청 목록을 봅니다.

   d. 변경 요청 목록에 초점을 맞추는 조건을 목록에 추가하려면 모달의 오른쪽 상단에서 필터 아이콘(깔때기형)을 클릭합니다.

   e. 표시되는 새 창에서 고급 보기를 클릭합니다.

   f. 조건 작성기를 사용하여 조건을 생성합니다.

   g. 업데이트를 선택합니다.

   h. 목록에서 변경 요청을 클릭하여 선택합니다.
      업데이트된 모달이 선택한 내용과 함께 표시됩니다.

   i. 옵션: 모달에서 CR에 CI 추가 확인란을 선택하여 모든 활성 취약한 항목의 구성 항목을 변경 요청에 추가합니다.

   j. 변경 내용 추가를 선택합니다.
      정정 기록이 표시되고 변경 요청이 성공적으로 생성되어 승인을 위해 제출되었다는 메시지가 표시됩니다.
      - 메시지의 변경 뷰 링크를 클릭하여 변경 요청(CHG) 기록을 엽니다.
      - 정정 작업 기록에서 변경 요청 관련 항목 메뉴 링크를 선택하여 기록과 연결된 모든 변경 요청을 봅니다.

      또는 클래식 환경에서 셀프 서비스 〉 내 요청. 변경 내용을 제출하고 구현한 후 상태 동기화를 사용하면 정정 작업이 #### ###으로 이동합니다. 변경 요청의 상태 및 상태 동기화에 대한 자세한 내용은 다음 문서를 참조하십시오 정정 작업에서 변경 요청 만들기.

에서 정정 작업 분할 **IT** 정정 작업 공간

정정 작업(VUL, AVUL, CVUL 또는 CRG)에서 기록의 하위 집합을 식별하고 해당 기록에 대한 새 정정 작업을 생성합니다.

시작하기 전에
필요한 역할:

- 호스트 취약 항목(VIT)에 대한 sn_vul.remediation_owner
- 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_security_champion
- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.remediation_owner
- 구성 테스트 결과(CTR)에 대한 sn_vulc.remediation_owner

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보

정정 작업의 개요 탭에서 개별 기록을 선택하고 새 정정 작업으로 이동할 수 있습니다.

기존 정정 작업에서 새 작업으로 기록(VIT, ABIT, CVIT 또는 CTR)을 분할하는 사용 사례에는 다음 예가 포함될 수 있습니다.

- 분할 작업에 대한 변경 요청 또는 변경 요청을 만들려고 합니다.
- 할당 그룹의 다른 사용자에게 분할 작업을 재할당하려고 합니다.
- 특정 CI(구성 항목)의 일부 취약성을 대상 날짜까지 해결할 수 없다는 것을 알고 있기 때문에 분할 작업에 대한 연기 또는 예외를 요청합니다.

클래식 환경 및 v15.0 이전 버전에서 취약성 대응 변경 요청 및 정정 작업 분할에 대한 자세한 내용은 문서를 참조하십시오 정정 작업 분할.

주:
의 취약성 대응v19.0부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v19.0 이전 용어	용어집 **v19.0** 이상
테스트 결과 그룹	정정 작업
구성 문제	구성 테스트 결과
정책	테스트 그룹

프로시저

1. 다음으로 이동 작업 공간 〉 **IT** 정정 작업 공간.
2. 홈페이지 또는 목록 페이지에서 정정 작업(VUL, AVUL, CVUL 또는 CRG)을 엽니다.
3. 개요 탭에서 새 정정 작업으로 이동할 기록(VIT, ABIT, VIT 또는 CTR)을 선택합니다.
4. 작업 분할을 클릭합니다.
5. 표시되는 대화 상자에 목록에서 선택한 기록(VIT, ABIT, CVIT 또는 CTR) 수가 표시됩니다.
6. 작업 분할을 다시 클릭합니다.
   새 정정 작업에 대한 링크가 포함된 확인 메시지가 표시됩니다.

   또는 조건 작성기를 사용하여 기록(VIT, VIT, CVIT 또는 CTR)을 필터링할 수 있습니다.
7. 분할할 정정 작업을 찾습니다.
8. 오른쪽의 UI 작업 버튼에서 작업 분할을 클릭합니다.
   잠시 후 조건 작성기가 표시됩니다.
9. 표시되는 모달에서 조건 작성기를 사용하여 새 정정 작업에 추가하려는 기록의 하위 세트(VIT, ABIT, CVIT 또는 CTR)를 식별합니다.
10. 작업 분할을 클릭합니다.
    조건과 일치하는 기록이 없다는 메시지가 표시되면 기준을 조정하고 작업 분할 을 다시 클릭해야 합니다. 필요에 따라 간단한 설명 필드를 편집합니다. 이 필드는 새 정정 작업을 생성한 후에 찾는 데 도움이 될 수 있습니다.

    기록이 조건과 일치하면 일치하는 기록 수가 메시지에 표시됩니다.
11. 옵션: 항목 미리 보기 링크를 클릭하여 필터 조건과 일치하는 기록을 봅니다.
    새 정정 작업이 새 탭으로 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약한 항목 또는 정정 작업에 대한 가양성 요청

에서 IT 정정 작업 공간호스트 취약한 항목(VIT), 애플리케이션 취약한 항목(AVIT), 컨테이너 취약한 항목(CVIT) 또는 정정 작업(VUL, AVUL, CVUL 또는 CRG)에 대한 긍정 오류 요청을 나타냅니다. 가양성은 잘못된 분류, 부적절한 논리 또는 스캐너의 알고리즘과 같은 상황으로 인해 시스템에 취약성이 있다고 스캐너가 잘못 보고하는 조건입니다.

시작하기 전에

필요한 역할:

- 호스트 취약 항목(VIT)에 대한 sn_vul.remediation_owner
- 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_security_champion
- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.remediation_owner
- 구성 테스트 결과(CTR)에 대한 sn_vulc.remediation_owner

이 태스크 정보

일련의 테스트 결과에 대해 가양성을 요청하는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 일련의 테스트 결과에 대해 긍정 오류 요청.

프로시저

1. 다음으로 이동 작업 공간 〉 **IT** 정정 작업 공간.
2. 목록 아이콘( )을 선택합니다.
3. 정정 작업(VUL, AVUL, CVUL 또는 CRG) 또는 취약한 항목(VIT, AVIT 또는 CVIT)을 선택합니다.
4. 긍정 오류로 표시를 선택합니다.
5. 요청에 대한 정보를 입력합니다.
6. 승인 요청을 선택합니다.
7. 승인자에게 요청에 대한 추가 정보를 제공하고 제출을 선택합니다.

> **주:**
> 질문서 사용 모달은 예외 관리 구성 양식에서 질문서를 사용하여 긍정 오류로 표시 확인란이 선택된 경우에만 나타납니다. 자세한 내용은 ,에 대한 예외 관리 구성 애플리케이션 취약성 대응, 에 대한 예외 관리 구성 컨테이너 취약성 대응및 에 대한 예외 관리 구성 구성 준수를 참조하십시오에 대한 예외 관리 구성 취약성 대응.

결과

취약한 항목(VIT, AVIT 또는 CVIT) 또는 정정 작업(VUL, AVUL 또는 CVUL)의 상태가 검토 중으로 전환됩니다.

요청이 승인을 위해 제출되고 승인자는 요청에 대한 이메일 알림을 받습니다.

요청을 승인하거나 거부하면 이메일 알림을 받게 됩니다.

다음에 수행할 작업

IT 정정 작업 공간의 목록 페이지에서 예외 요청 〉 내 요청 을 클릭하고 해당 상태 변경 승인 기록(VCA#)을 열고 승인 상태 열에서 요청 상태를 확인합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

승인 상태	기록(**VIT, AVIT** 또는 **CVIT**)	정정 작업(**VUL, AVUL, CVUL** 또는 **CRG**)
승인됨	기록의 상태가 긍정 오류로 이유가 표시된 상태로 종결됨으로 전환됩니다.	정정 작업의 상태가 긍정 오류로 이유가 표시된 상태로 종결됨으로 전환됩니다. 이에 따라 상태가 정정 작업의 기록으로 롤다운됩니다. 정정 작업의 상세 정보 탭으로 이동하고 필요한 경우 때까지 필드에서 긍정 오류에 대한 만료 날짜를 설정합니다. 정정 작업은 지정된 날짜 후에 열림 상태로 되돌아가고 상태는 테스트 결과로 롤다운됩니다.
거부됨	기록의 상태는 변경되지 않습니다.	정정 작업 및 해당 기록의 상태가 이전 상태로 되돌아갑니다.

기록 또는 정정 작업의 활동 스트림 에서 긍정 오류 요청의 전체 워크플로우를 볼 수 있습니다.

관련 정보

긍정 오류 개요

일련의 테스트 결과에 대해 긍정 오류 요청

의 IT 정정 작업 공간정정 작업 내에 있는 테스트 결과 집합에 대해 긍정 오류 요청을 제기합니다.

이 태스크 정보

정정 작업 내의 테스트 결과 집합에 대해 긍정 오류를 요청하려면 다음 조건이 충족되어야 합니다.

- 버전 22.0 취약성 대응 이 설치되어 있어야 합니다.
- 선택한 테스트 결과가 하나 이상 활성 상태여야 합니다.
- 정정 작업에는 두 개 이상의 테스트 결과가 있어야 합니다.
- 하나 이상의 테스트 결과가 선택되지 않았습니다.

시작하기 전에

필요한 역할: sn_vulc.remediation_owner

프로시저

1. 다음으로 이동 작업 공간 〉 **IT** 정정 작업 공간.
2. 목록 아이콘( )을 선택합니다.
3. 목록 페이지에서 정정 작업을 선택합니다 구성 준수 .
4. 개요 관련 목록의 테스트 결과 탭에서 긍정 오류로 표시할 테스트 결과를 선택합니다.
5. 구성 테스트 결과 탭에서 긍정 오류로 표시 단추를 선택합니다.
6. 표시되는 대화 상자에서 요청에 대한 정보를 입력하고 승인 요청을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

7. 질문서 사용 모달에서 질문에 응답하여 승인자에게 요청에 대한 추가 정보를 제공하고 제출을 선택합니다.

   주:
   질문서 사용 모달은 예외 관리 구성 양식에서 질문서를 사용하여 긍정 오류로 표시 확인란이 선택된 경우에만 나타납니다. 질문서 구성 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 에 대한 예외 관리 구성 구성 준수.

결과
선택한 테스트 결과가 새 정정 작업으로 이동되고 승인을 위해 요청이 제출됩니다. 작업 번호는 이전 정정 작업의 활동 스트림 에 나타납니다. 승인자는 요청에 대한 이메일 알림을 받습니다.

요청 승인 또는 거부에 대한 이메일 알림이 전송됩니다. 테스트 결과 또는 정정 작업의 활동 스트림에서 긍정 오류 요청의 전체 워크플로우를 볼 수 있습니다.

다음에 수행할 작업

1. IT 정정 작업 공간목록 페이지에서 예외 요청 〉 내 요청.
2. 해당 상태 변경 승인 기록(VCA#)을 열고 승인 상태 열에서 요청 상태를 확인합니다.

승인 상태	결과
승인됨	새 정정 작업의 상태가 긍정 오류로 이유가 표시된 상태로 종결됨으로 전환됩니다.
거부됨	새 정정 작업의 상태가 미해결로 변경됩니다.

3. 요청이 승인되면 새 정정 작업의 상세 정보 탭으로 이동하고 필요한 경우 때까지 필드에서 긍정 오류에 대한 만료 날짜를 설정합니다.

   정정 작업은 지정된 날짜 후에 열림 상태로 되돌아가고 상태는 테스트 결과로 롤다운됩니다.

에서 예외 요청 **IT** 정정 작업 공간

에서 IT 정정 작업 공간호스트 취약한 항목(VIT), 애플리케이션 취약한 항목(AVIT), 컨테이너 취약한 항목(CVIT) 및 정정 작업(VUL, AVUL, CVUL 또는 CRG)에 대한 예외를 요청합니다.

시작하기 전에
필요한 역할:

- 호스트 취약 항목(VIT)에 대한 sn_vul.remediation_owner
- 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_security_champion
- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.remediation_owner
- 구성 테스트 결과(CTR)에 대한 sn_vulc.remediation_owner

이 태스크 정보
일부 취약성에는 기존 패치, 수정 프로그램 또는 솔루션이 없을 수 있습니다. 또는 정정 작업을 목표 날짜까지 해결할 수 없다고 판단할 수 있습니다. 정정이 게시된 취약성 관리 또는 보안 정책, 표준 또는 가이드라인을 준수할 수 없는 경우 예외를 요청할 수 있습니다.

할당된 정 IT 정정 작업 공간 정 작업(VUL, AVUL, CVUL 또는 CRG) 및 취약한 항목(VIT, AVIT 또는 CVIT)에 대한 예외를 요청할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
의 취약성 대응v19.0부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v19.0 이전 용어	용어집 **v19.0** 이상
테스트 결과 그룹	정정 작업
구성 문제	구성 테스트 결과
정책	테스트 그룹

버전 18.0부터 애플리케이션 취약성 항목 및 컨테이너 취약성 항목에 대한 예외를 요청할 수 있습니다.

클래식 환경에서 예외를 요청하는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 정정 작업에 대한 예외 요청.

프로시저

1. 다음으로 이동 모두 〉 취약성 대응 〉 **IT** 정정 작업 공간.
2. 목록 아이콘을 선택합니다.
3. 정정 작업 목록에서 예외를 요청하려는 정정 작업(VUL, AVUL, CVUL 또는 CRG) 또는 기록(VIT, AVIT 또는 CVIT)을 엽니다.
4. 오른쪽의 UI 작업 버튼에서 예외 요청을 클릭합니다.
5. 표시되는 대화 상자에서 예외의 종료 날짜를 입력하고 목록에서 이유를 선택한 후 기타 필수 정보를 추가합니다.
6. 예외 요청을 클릭합니다.
7. 질문서 수행 모달에서 질문에 답하고 제출을 클릭합니다.

   주:
   질문서 사용 모달은 예외 관리 구성 양식에서 예외를 요청하기 위해 질문서 사용 확인란을 선택한 경우에만 나타납니다.

   요청이 승인을 위해 성공적으로 제출되었음을 알리는 메시지가 표시됩니다.

   정정 작업에 대한 예외 요청은 기본 2단계 승인 워크플로우를 사용하여 승인됩니다. 요청이 수준 1 승인자에 의해 승인되면 수준 2 승인자에게 전송됩니다.

   - 예외 요청이 열려 있는 동안 정정 작업 또는 기록이 검토 중으로 전환됩니다.
   - 요청이 승인되면 정정 작업 또는 기록이 지연됨으로 전환됩니다.
   - 예외 요청이 승인된 후 예외 요청 기록(VCA#)이 종결됩니다.

   승인 요청의 상태를 보려면 목록 페이지의 예외 요청에서 내 요청을 클릭합니다. 목록에서 기록 또는 정정 작업을 열면 요청 번호(VCA#)가 표시됩니다.

   - 요청이 거부되면 요청 기록(VCA#)이 내 요청 아래 목록 뷰의 승인 상태 열에 거부됨 으로 표시됩니다.
   - 이 항목을 계속 연기하려면 새 예외 요청을 제출해야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

에서 사용하는 예외 **GRC:** 정책 및 준수 관리 요청 **IT** 정정 작업 공간

에서 IT 정정 작업 공간호스트 취약한 항목(VIT), 애플리케이션 취약한 항목(AVIT), 컨테이너 취약한 항목(CVIT) 또는 정정 작업(VUL, AVUL, CVUL 또는 CRG)에 대한 정책 예외를 요청합니다.

시작하기 전에

필요한 역할:

- 호스트 취약 항목(VIT)에 대한 sn_vul.remediation_owner
- 애플리케이션 취약 항목(AVIT)에 대한 sn_vul.app_security_champion
- 컨테이너 취약한 항목(CVIT)에 대한 sn_vul_container.remediation_owner
- 구성 테스트 결과(CTR)에 대한 sn_vulc.remediation_owner

이 태스크 정보

주:
의 취약성 대응v19.0부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v19.0 이전 용어	용어집 **v19.0** 이상
테스트 결과 그룹	정정 작업
구성 문제	구성 테스트 결과
정책	테스트 그룹

프로시저

1. 다음으로 이동 작업 공간 〉 **IT** 정정 작업 공간.
2. 애플리케이션 네비게이터에서 목록 아이콘(.)을 선택합니다.
3. 목록 페이지의 호스트 취약한 항목, 애플리케이션 취약한 항목, 컨테이너 취약한 항목 또는 정정 작업(VUL, AVUL, CVOL 또는 CRG)에서 예외를 요청할 기록을 선택합니다.
   선택한 기록은 오픈, 조사 중 또는 구현 대기 중 상태여야 합니다.
4. 예외 요청 버튼을 선택합니다.
5. 양식에서 필드를 채웁니다.
   양식 필드에 대한 자세한 내용은 정책 예외에 대한 예외 양식 필드 요청 문서를 참조하십시오.
6. 예외 요청을 선택합니다.
7. 질문서 수행 모달에서 질문에 응답하여 요청에 대한 추가 정보를 제공하고 제출을 선택합니다.

   주:
   질문서 사용 모달은 질문서 상세 정보가 해당 통합 레지스트리에 추가되는 경우에만 나타납니다.

   요청이 승인을 위해 성공적으로 제출되었다는 메시지가 나타납니다.

   정책 예외 통합 및 정정 소유자와 준수 관리자 간의 핸드오프에 대한 자세한 내용은 정책 및 준수 관리 선택적 설정을 참조하십시오.

취약한 항목 또는 정정 작업에 대한 위험 감소 요청

에서 IT 정정 작업 공간호스트 취약한 항목 또는 정정 작업에 대한 위험 감소를 요청합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_vul.remediation_owner

이 태스크 정보
의 취약성 대응v21.0부터 다음 항목에 대해서만 위험 감소를 요청할 수 있습니다.

- CVE에 대해 위험 감소가 활성화되었는지 여부에 관계없이 모든 취약한 항목이 동일한 CVE(공통 취약성 항목)에연결된 경우에만 정정 작업입니다.
- 위험 감소가 활성화된 외부 공급업체(TPE)입니다.

주:
보상 제어 기능은 호스트 취약성에 대해서만 사용할 수 있습니다.

프로시저

1. 다음으로 이동 작업 공간 〉 **IT** 정정 작업 공간.
2. 목록 아이콘( )을 선택합니다.
3. 목록 페이지에서 호스트 취약한 항목 또는 업데이트 적용 작업을 엽니다.
4. 추가 옵션 아이콘을 선택하고 예외 요청을 선택합니다.
5. 예외 요청 양식의 필드에 내용을 입력합니다.
   필드 값에 대한 설명은 위험 감소를 위한 예외 요청 양식 문서를 참조하십시오.
6. 예외 요청을 선택합니다.
7. 질문서 사용 모달이 표시되면 질문에 응답하여 요청에 대한 추가 정보를 제공하고 제출을 선택합니다.

   주:
   질문서 사용 모달은 예외 관리에 대해 질문서를 사용할 때만 나타납니다. 자세한 내용은 에 대한 예외 관리 구성 취약성 대응 문서를 참조하십시오.

결과
요청이 승인을 위해 성공적으로 제출되었다는 메시지가 나타납니다. 요청에 대한 알림이 승인자에게 전송됩니다.

- 연기 및 위험 감소를 요청하는 경우:
  - 지연 및 위험 감소를 위해 두 개의 상태 변경 승인(VCA#)이 생성됩니다.
  - 기록의 상태가 검토 중으로 변경됩니다.
- 요청이 위험 감소만을 위한 것인 경우:
  - 상태 변경 승인(VCA#)이 생성됩니다.
  - 상태는 변하지 않습니다.

요청이 승인되거나 거부되면 알림을 받게 됩니다. 승인 프로세스에 대한 자세한 내용은 다음 문서를 참조하십시오 에서 요청 승인 또는 거부 취약성 관리자 작업 공간.

위험 감소 요청이 승인될 때 정정 작업 및 취약한 항목에 대해 위험 감소를 위한 종료 날짜가 업데이트되는 방식에 대한 자세한 내용은 문서를 보상 통제가 위험 점수 및 만료 날짜에 미치는 영향참조하십시오.

관련 정보

위험 감소를 위한 보상 통제 이해

CVE 또는 TPE에 대한 위험 감소 사용 안 함 또는 사용

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

라이브러리에 보정 통제 추가

보상 통제가 위험 점수 및 만료 날짜에 미치는 영향

에서 취약한 항목 및 정정 작업 다시 스캔 **IT** 정정 작업 공간

예약된 검사 주기 사이에 취약한 항목이 정정되었는지 확인합니다. 온디맨드에서 IT 정정 작업 공간 다시 스캔을 ServiceNow AI Platform 시작합니다.

재검색을 통해 정정 활동, 패치 및 기타 작업이 구성 항목(CI)의 특정 취약성을 성공적으로 수정했는지 확인할 수 있습니다.

다시 스캔은 에서 IT 정정 작업 공간다음 통합에 대해 지원됩니다. 자세한 내용은 다음 항목을 참조하십시오.

- 작업 공간에서 취약한 항목 취약성 대응 다시 스캔 Qualys
- 작업 공간에서 취약한 항목 취약성 대응 다시 스캔 Rapid7
- 작업 공간에서 취약성 대응 취약한 항목 다시 스캔 Tenable.ioTenable.sc

필요한 역할: sn_vul.remediation_owner for the IT 정정 작업 공간.

작업 공간에서 취약한 항목 취약성 대응 다시 스캔 **Qualys**

예약된 검사 주기 사이에 취약한 항목이 정정되었는지 확인합니다. 인스턴스에서 요청 IT 정정 작업 공간ServiceNow AI Platform 시 제품의 재스캔을 Qualys 시작합니다.

시작하기 전에
클래식 환경에서 제품에 대한 Qualys 재검색을 시작하려면 문서를 참조하십시오 다음에 대한 재스캔 시작 Qualys Vulnerability Integration.

스캐너는 Qualys 애플리케이션에서 기본적으로 비활성화되어 있습니다 취약성 대응 . 이러한 애플리케이션을 소스로 사용하는 취약한 항목 또는 정정 작업에서 다시 검색을 수행하려고 하면 다시 검색 버튼을 사용할 수 없습니다.

이러한 스캐너를 활성화하려면 sn_vul.vulnerability_admin 역할을 가진 사용자가 다음과 같이 하십시오.

1. 다음으로 이동 모두 〉 취약성 대응 〉 취약성 스캐닝 〉 스캐너.
2. 활성화할 스캐너 제품을 찾고 기록을 클릭하여 엽니다.
3. 활성 확인란을 선택합니다.
4. 업데이트를 클릭합니다.

   활성화한 제품은 다음 임포트 후 취약한 항목 및 정정 작업 기록의 소스 필드에 표시되며, 다시 스캔 은 UI 작업으로 사용할 수 있습니다.

스캐너 설정에 Qualys 대한 자세한 내용은 해당 고급 Qualys 구성 및 수정문서를 참조하십시오스캐너 장치 설정.

- 에서 제품을 소스로 사용하는 Qualys 취약한 항목 및 정정 작업에 대한 요청 시 재스캔을 시작할 수 있습니다ServiceNow AI Platform.IT 정정 작업 공간
- 정정 작업 기록에서 기록은 종결 이외의 상태일 수 있으며 연결된 모든 VI는 제품에서 가져온 Qualys 것이어야 합니다.
- 취약한 항목 및 정정 작업 기록에서 IT 정정 작업 공간에서 다시 스캔을 시작하려면 이러한 기록을 사용자에게 할당해야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필요한 역할:

- sn_vul.remediation_owner입니다 IT 정정 작업 공간.
- 취약성 관리자 작업 공간의 sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin

프로시저

1. 취약한 항목 또는 할당된 정정 작업으로 이동하여 엽니다.

   주:
   재스캔을 시작하기 위해 정정 작업을 선택하면 해당 기록과 연결된 모든 VI가 스캔됩니다.

2. 기록의 오른쪽 상단에서 Rescan(다시 스캔)을 클릭합니다.
3. 다시 스캔 모달에서 옵션 프로필을 선택합니다.
   옵션 프로파일은 에서 ServiceNow AI Platform#스캔을 Qualys 시작할 때 필요합니다. 옵션 프로파일에는 검사 설정이 포함되어 Qualys 있습니다.
4. 다시 스캔 모달에서 다시 스캔 요청을 클릭합니다.
   ## ### ## #이라는 메시지가 표시됩니다.
5. 메시지에서 상태 보기 링크를 클릭하여 스캔 진행률을 봅니다.

   스캔 기록(VSCAN#)이 표시됩니다. 스캔 번호가 있는 기록 헤더 아래에 있는 관련 항목 목록에 다음 정보가 표시됩니다.

   - 상세 정보 목록에는 상위 스캔의 스캔 번호, 스캐너 소스 및 상태가 표시됩니다. 검사 요약 섹션에서 완료된 검사와 실패한 검사를 봅니다.
   - 스캔 목록에는 모든 하위 스캔과 해당 상태가 표시됩니다. 모든 하위 스캔이 완료되면 상위 스캔의 상태가 완료로 전환됩니다.
   - 소스 목록에는 검사에 사용되는 취약한 항목, 관련 구성 항목 및 취약성, VI 상태 및 정정 상태가 표시됩니다.

   인스턴스는 ServiceNow AI Platform# 재스캔 상태가 성공적으로 완료될 때까지, 또는 설정된 추적 기간이 초과될 때까지(먼저 발생하는 쪽 적용) 재스캔 상태를 추적합니다.

   시간 제한은 검사를 중지하지 않습니다. 시간 제한은 실제 다시 검색이 중지된 시간이 아니라 다시 스캔 상태 추적이 ServiceNow AI Platform# 중지된 시기를 나타냅니다.

   종결/고정으로 전환되었거나 전환될 모든 VI는 다음의 Qualys 예약된 통합 임포트와 함께 임포트됩니다.

작업 공간에서 취약한 항목 취약성 대응 다시 스캔 **Rapid7**

예약된 검사 주기 사이에 취약한 항목이 정정되었는지 확인합니다. 인스턴스의 IT 정정 작업 공간에서 ServiceNow AI Platform 요청 시 제품 재스캔 Rapid7 을 시작합니다.

시작하기 전에
클래식 환경에서 제품에 대한 재검색을 시작하려면 문서를 참조하십시오 취약성 통합에 Rapid7 대한 재스캔 시작. 이 주제에는 통합 인스턴스에서 통합 매개변수를 사용하여 스캔을 예약하는 방법에 대한 정보도 포함되어 있습니다 Rapid7 .

스캐너는 Rapid7 애플리케이션에서 기본적으로 비활성화되어 있습니다 취약성 대응 .
애플리케이션을 소스로 사용하는 Rapid7 취약한 항목 또는 정정 작업에서 다시 검색을 수행하려고 하면 다시 스캔 버튼을 사용할 수 없습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이러한 스캐너를 활성화하려면 sn_vul.vulnerability_admin 역할을 가진 사용자가 다음과 같이 하십시오.

1. 다음으로 이동 모두 〉 취약성 대응 〉 취약성 스캐닝 〉 스캐너.
2. 활성화할 스캐너 제품을 찾고 기록을 클릭하여 엽니다.
3. 활성 확인란을 선택합니다.
4. 업데이트를 클릭합니다.

활성화한 제품은 다음 임포트 후 취약한 항목 및 정정 작업 기록의 소스 필드에 표시되며, 다시 스캔 은 UI 작업으로 사용할 수 있습니다.

- 소스로 제품이 있는 Rapid7 InsightVM 취약한 항목 및 정정 작업에 대한 요청 시 다시 스캔을 시작할 수 있습니다 ServiceNow AI Platform.
- 정정 작업 기록에서 기록은 종결 이외의 상태일 수 있으며 연결된 모든 VI는 제품에서 가져온 Rapid7 것이어야 합니다.
- 취약한 항목 및 정정 작업 기록에서 IT 정정 작업 공간의 재스캔을 시작하려면 이러한 기록을 사용자에게 할당해야 합니다.

필요한 역할:

- IT 정정 작업 공간에 대한 sn_vul.remediation_owner
- 취약성 관리자 작업 공간의 sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin

프로시저

1. 취약한 항목 또는 할당된 정정 작업으로 이동하여 엽니다.

   주:
   재스캔을 시작하기 위해 정정 작업을 선택하면 해당 기록과 연결된 모든 VI가 스캔됩니다.

2. 기록의 오른쪽 상단에서 Rescan(다시 스캔)을 클릭합니다.
3. 다시 스캔 확인 모달에서 다시 스캔 요청을 클릭합니다.
   ## ### ## #이라는 메시지가 표시됩니다.
4. 메시지에서 상태 보기 링크를 클릭하여 스캔 진행률을 봅니다.

   스캔 기록(VSCAN#)이 표시됩니다. 스캔 번호가 있는 기록 헤더 아래에 있는 관련 항목 목록에 다음 정보가 표시됩니다.

   - 상세 정보 목록에는 상위 스캔의 스캔 번호, 스캐너 소스 및 상태가 표시됩니다. 검사 요약 섹션에서 완료된 검사와 실패한 검사를 봅니다.
   - 스캔 목록에는 모든 하위 스캔과 해당 상태가 표시됩니다. 모든 하위 스캔이 완료되면 상위 스캔의 상태가 완료로 전환됩니다.
   - 소스 목록에는 검사에 사용되는 취약한 항목, 관련 구성 항목 및 취약성, VI 상태 및 정정 상태가 표시됩니다.

   인스턴스는 ServiceNow AI Platform# 재스캔 상태가 성공적으로 완료될 때까지, 또는 설정된 추적 기간이 초과될 때까지(먼저 발생하는 쪽 적용) 재스캔 상태를 추적합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시간 제한은 검사를 중지하지 않습니다. 시간 제한은 실제 다시 검색이 중지된 시간이 아니라 다시 스캔 상태 추적이 ServiceNow AI Platform# 중지된 시기를 나타냅니다.

종결/고정으로 전환되었거나 전환될 모든 VI는 다음의 Rapid7 예약된 통합 임포트와 함께 임포트됩니다.

작업 공간에서 취약성 대응 취약한 항목 다시 스캔 **Tenable.ioTenable.sc**

예약된 검사 주기 사이에 취약한 항목이 정정되었는지 확인합니다. 인스턴스의 IT 정정 작업 공간에서 ServiceNow AI Platform 온디맨드로 제품 재스캔 Tenable.ioTenable.sc 을 시작합니다.

시작하기 전에
의 클래식 환경에서 및 제품에 대한 Tenable.io 재검색을 시작하려면 및 통합에 대한 Tenable.io 재스캔 시작를 참조하십시오통합에 대한 Tenable.sc 재스캔 시작.Tenable.sc취약성 대응

에서 ServiceNow AI Platform재스캔을 수행하려면 Tenable 자격 증명이 필요합니다. 스캐너 Tenable.sc 를 설정하고 Tenable.io Tenable에서 자격 증명을 가져오는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오설정 도우미를 사용하여 Tenable 취약성 통합 구성.

- 소스로 또는 제품이 있는 Tenable.io 취약한 항목 및 정정 작업에 대한 요청 시 다시 검색을 사용자의 IT 정정 작업 공간에서 시작할 수 있습니다ServiceNow AI Platform.Tenable.sc
- 정정 작업 기록에서 기록은 종결 이외의 상태일 수 있으며 연결된 모든 VI는 또는 Tenable.sc 제품에서 생성된 Tenable.io 것이어야 합니다.
- 취약한 항목 및 정정 작업 기록에서 IT 정정 작업 공간 다시 스캔을 시작하려면 이러한 기록을 사용자에게 할당해야 합니다.

필요한 역할:

- sn_vul.remediation_owner IT 정정 작업 공간
- 취약성 관리자 작업 공간의 sn_vul.vulnerability_analyst 또는 sn_vul.vulnerability_admin

프로시저

1. 취약한 항목 또는 할당된 정정 작업으로 이동하여 엽니다.

   주:
   재스캔을 시작하기 위해 정정 작업을 선택하면 해당 기록과 연결된 모든 VI가 스캔됩니다.

2. 기록의 오른쪽 상단에서 Rescan(다시 스캔)을 클릭합니다.
   다시 스캔할 인스턴스와 스캐너에 액세스하는 데 사용할 스캐너 자격 증명을 선택하라는 메시지가 표시됩니다. 표시된 자격 증명은 및 Tenable.sc 검사 자격 증명 통합에서 Tenable.io 임포트한 자격 증명입니다.
3. 모달에서 검색 아이콘을 클릭합니다.

   표시되는 스캔 자격 증명 선택 모달에서 열 제목의 필터를 사용하여 이름, 인스턴스 및/또는 인스턴스, 사용할 자격 증명 유형을 선택합니다.

   자세한 내용은 다음 테이블을 참조하십시오.

4. 업데이트된 다시 스캔 모달에서 **Request** rescan(재스캔 요청)을 클릭합니다.
   ## ### ## #이라는 메시지가 표시됩니다.
5. 메시지에서 상태 보기 링크를 클릭하여 스캔 진행률을 봅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

스캔 기록(VSCAN#)이 표시됩니다. 스캔 번호가 있는 기록 헤더 아래에 있는 관련 항목 목록에 다음 정보가 표시됩니다.

- 상세 정보 목록에는 상위 스캔의 스캔 번호, 스캐너 소스 및 상태가 표시됩니다. 검사 요약 섹션에서 완료된 검사와 실패한 검사를 봅니다.
- 스캔 목록에는 모든 하위 스캔과 해당 상태가 표시됩니다. 모든 하위 스캔이 완료되면 상위 스캔의 상태가 완료로 전환됩니다.
- 소스 목록에는 검사에 사용되는 취약한 항목, 관련 구성 항목 및 취약성, VI 상태 및 정정 상태가 표시됩니다.

인스턴스는 ServiceNow AI Platform# 재스캔 상태가 성공적으로 완료될 때까지, 또는 설정된 추적 기간이 초과될 때까지(먼저 발생하는 쪽 적용) 재스캔 상태를 추적합니다.

시간 제한은 검사를 중지하지 않습니다. 시간 제한은 실제 다시 검색이 중지된 시간이 아니라 다시 스캔 상태 추적이 ServiceNow AI Platform# 중지된 시기를 나타냅니다.

종결/고정으로 전환되었거나 전환될 모든 VI는 OR Tenable.sc 통합의 Tenable.io 다음 예약된 임포트와 함께 임포트됩니다.

IT 정정 작업 공간 참조 정보

다음 항목에서는 링크, 참조 정보 외에 에 있는 IT 정정 작업 공간양식 및 기록의 필드 데이터를 제공합니다.

〔store-future: BEGIN review〕

모두 메뉴에서 리디렉션 중 IT 정정 작업 공간

관리자가 시스템 속성을 true로 설정하면 *sn_vul_cmn_ws.navigate_to_workspace*모두 메뉴의 , 애플리케이션 취약성 대응, 컨테이너 취약성 대응및 구성 준수 모듈에서 취약성 대응미리 정의된 필터 링크를 선택하면 다음으로 IT 정정 작업 공간 리디렉션됩니다.

의 목록 페이지로 리디렉션 중 IT 정정 작업 공간

sn_vul.remediation_owner 역할을 가진 사용자가 취약성 대응 모듈에서 다음과 같이 미리 정의된 필터 링크를 선택할 때 모두 〉 취약성 대응, 이러한 링크는 다음의 IT 정정 작업 공간목록 페이지에서 열립니다.

- 정정 작업 - 나에게 할당됨 및 내 그룹에 할당됨
- 취약한 항목 - 나에게 할당됨 및 내 그룹에 할당됨
- 라이브러리 - NVD, CWE 및 외부 공급업체
- 솔루션 - 모두, 가장 높은 대체 및 취약한 항목 포함
- 내 승인

sn_vul_container.remediation_owner 역할을 가진 사용자가 컨테이너 취약성 대응 모듈에서 다음과 같이 미리 정의된 필터 링크를 선택하는 경우 모두 〉 컨테이너 취약성 대응, 이러한 링크는 다음의 IT 정정 작업 공간목록 페이지에서 열립니다.

- 컨테이너 정정 작업 - 활성, 나에게 할당됨, 내 그룹에 할당됨 및 전체
- 컨테이너 취약한 항목 - 나에게 할당됨 및 내 그룹에 할당됨
- 내 승인
- 라이브러리 - NVD, CWE 및 외부 공급업체

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

sn_vul.app_security_champion 역할을 가진 사용자가 다음으로 이동하여 애플리케이션 취약성 대응 모듈에서 다음과 같이 미리 정의된 필터 링크를 선택하는 경우 모두 〉 애플리케이션 취약성 대응, 이러한 링크는 다음의 IT 정정 작업 공간목록 페이지에서 열립니다.

- 정정 작업 - 활성, 나에게 할당됨, 내 그룹에 할당됨 및 모두
- 취약한 항목 - 나에게 할당됨 및 내 그룹에 할당됨
- 내 승인
- 라이브러리 - NVD, CWE 및 외부 공급업체
- 침투 테스트 평가 요청 - 활성, 모두 나에게 할당됨 및 내 그룹에 할당됨
- 침투 테스트 결과 - 활성, 확인 보류 중, 나에게 할당됨, 내 그룹에 할당됨, 모두

sn_vulc.remediation_owner 역할을 가진 사용자가 다음으로 이동하여 구성 준수 모듈에서 다음과 같이 미리 정의된 필터 링크를 선택하는 경우 모두 〉 구성 준수, 이러한 링크는 다음의 IT 정정 작업 공간목록 페이지에서 열립니다.

- 정정 작업 - 내 오픈 작업, 모든 오픈 작업, 여러 지연 및 모든 작업
- 테스트
- 테스트 그룹
- 지원 데이터 - 권한이 부여된 소스 및 기술

〔End〕

변경 요청 양식 필드 생성

다음 테이블에는 변경 요청 생성 양식의 필드와 해당 설명이 표시됩니다.

필드	설명
유형 변경	Normal – Normal이 기본값입니다. 표준 - 두 개의 추가 필드가 표시됩니다. 표준 변경 범주 - 목록에서 범주를 선택합니다. 표준 변경 템플릿 – 선택 목록에서 이 변경 요청에 사용할 템플릿을 선택합니다. 긴급 - 중요 우선순위
변경 요청에 CI 추가	기본값은 사용 설정입니다. 활성화하면 변경 요청은 이 정정 작업의 활성 취약한 항목에 속하는 모든 CI(구성 항목)가 이 변경 요청에 추가됩니다.
우선순위	높음이 기본값입니다. 목록에서 우선순위를 선택합니다.
할당 그룹	할당 그룹은 기본적으로 감시 주제에서 가져옵니다. 검색 아이콘을 클릭하고 모달에서 다른 할당 그룹을 선택합니다.
계획된 종료 날짜	달력 아이콘을 클릭하여 계획된 종료 날짜를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
담당자	기본적으로 현재 사용자가 정정 작업에 할당됩니다. 검색 아이콘을 클릭하고 모달에서 다른 사용자를 선택합니다.
간단한 설명	짧은 설명은 정정 작업에서 가져온 것입니다. 편집할 텍스트를 클릭합니다.
설명	설명은 정정 작업에서 가져온 것입니다. 편집할 텍스트를 클릭합니다.
근거	정정 작업에서 가져온 근거입니다. 편집할 텍스트를 클릭합니다.
구축 계획	기본 솔루션 정보(사용 가능한 경우)로 미리 채워집니다. 솔루션을 보거나 근거 계획을 입력합니다.

관련 정보

에서 변경 요청 만들기 IT 정정 작업 공간

정책 예외에 대한 예외 양식 필드 요청

다음 테이블에는 정책 예외에 대한 예외 요청 양식에서 작성해야 하는 필드가 나와 있습니다.

예외 요청 양식

필드	설명
정책	예외를 요청하는 취약성 관리 정책입니다.
컨트롤 목적	선택한 정책과 연결된 통제 목표입니다. 정책을 선택하지 않으면 모든 통제 목표가 나열됩니다.
유효 기간(시작)	예외가 시작되는 날짜입니다. 기본값은 현재 날짜입니다. 이 날짜는 과거일 수 없습니다.
유효 기간	정책 예외가 만료되고 취약한 항목 또는 그룹의 상태가 연기됨에서 미결로 변경되는 날짜입니다. **주:** 정책 예외가 유효한 일수는 정책에 대해 설정한 최대 예외 기간(일) 필드의 값을 초과할 수 없습니다. 자세한 내용은 정책 만들기를 참조하세요.
이유	예외를 요청하는 이유입니다.
근거	이 예외가 요청되는 이유와 관련된 상세 정보입니다. 정정 소유자가 이 필드를 입력해야 합니다.

관련 정보

에서 사용하는 예외 GRC: 정책 및 준수 관리 요청 IT 정정 작업 공간

위험 감소를 위한 예외 요청 양식

다음 테이블에는 위험 감소 요청에 대한 예외 요청 양식에서 작성해야 하는 필드가 나와 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예외 요청 양식

필드	설명
이유	예외 요청의 이유입니다. 위험 감소 요청에 대한 완화 통제를 선택합니다. 새 이유 선택 항목을 추가하는 방법을 보려면 다음 문서를 참조하십시오 정책 사유 매핑 정의.
연기 요청	기록을 연기합니다. 이 필드는 기본적으로 선택되어 있습니다. 주: 이 필드는 이유 필드에서 사용 중인 완화 통제 옵션을 선택한 경우에만 나타납니다.
위험 감소 요청	위험 점수 감소를 요청할 수 있습니다. 주: 이 확인란은 이유 필드에서 사용 중인 완화 통제 옵션을 선택한 경우에만 나타납니다.
현재 위험 등급	위험의 현재 심각도입니다. 주: 이 필드는 위험 감소 요청 확인란이 선택된 경우에만 나타납니다.
원하는 위험 등급	기록에 할당할 새 위험 등급입니다. 요청이 승인되면 이 위험 등급 범위에서 가장 높은 위험 점수가 기록에 적용됩니다. 주: 이 필드는 위험 감소 요청 확인란이 선택된 경우에만 나타납니다.
보상 통제 선택	위험 등급을 낮추도록 요청한 이유입니다.
다음까지	연기 또는 위험 감소 요청이 만료되는 날짜입니다. 예외 요청이 만료되는 경우: • 기록이 열림 상태로 되돌아갑니다. • 보상 통제가 만료됩니다. • 계산된 점수는 감소된 점수 대신 적용됩니다.
근거 메모	이 요청이 수행되는 이유와 관련된 상세 정보입니다.

관련 정보

취약한 항목 또는 정정 작업에 대한 위험 감소 요청

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약성 평가 작업 공간 탐색

취약성 평가 작업 공간은 취약성 이벤트 관리자가 노출 평가를 수행하고, 특히 제로 데이 이벤트와 같은 중요한 취약성 이벤트 중에 중요한 취약성 이벤트를 사전 예방적으로 관리할 수 있도록 설계되었습니다.

중요 취약성이 식별되면 취약성 이벤트 관리자가 취약성과 연관된 잠재적 영향 및 위험을 평가할 수 있습니다. 분석가는 영향을 받는 시스템, 애플리케이션 또는 네트워크 구성 요소를 분석하여 조직 내의 심각도와 가능한 공격 벡터를 이해할 수 있습니다.

취약성 평가 작업 공간에는 다음이 포함됩니다.

노출 평가 페이지

취약성 및 취약한 소프트웨어에 노출된 자산에 대한 자세한 가시성을 제공합니다. 노출 평가 기능은 다음을 제공합니다.

- 취약성 및 영향을 받는 소프트웨어에 대해 영향을 받는 자산에 대한 가시성
- 단일 CVE 또는 취약한 소프트웨어에 대해 독립 실행형 평가를 수행하는 능력
- CISA의 영향을 받는 자산에 대한 가시성 알려진 악용 취약성 CVE
- 추가 디스커버리 모델 및 자산의 노출에 대한 가시성
- 취약한 항목을 생성할 수 있는 기능

취약성 평가 페이지

취약성 위기 관리 워크플로우를 사용하여 평가에서 해결까지 취약성 위기 이벤트를 처리할 수 있는 취약성 평가 페이지입니다. 워크플로우를 통해 관심 있는 취약성 이벤트를 추적하고, 관련 위험을 분석하고, 여러 인벤토리(예: 소프트웨어 설치 인벤토리)에 대한 노출 평가를 수행하고, 높은 대응 참여에 대한 위기로 선언할 수 있습니다. 그런 다음 취약성 평가 레코드를 중요 보안 인시던트에 연결하고 보안 인시던트 응답 팀이 위기에 대응하도록 지원할 수 있습니다.

- 중요 취약성 이벤트에 대한 취약성 평가 생성 및 수정
- 취약성의 주요 속성을 기록하여 위험 계산
- 취약성 평가를 수행하여 노출 수준과 우선순위를 결정합니다.
- 취약성 평가를 중요 이벤트로 선언
- 취약성 평가를 주요 보안 인시던트에 연결, 제안 또는 승격하여 취약성 평가를 중요 보안 인시던트에 연결합니다.

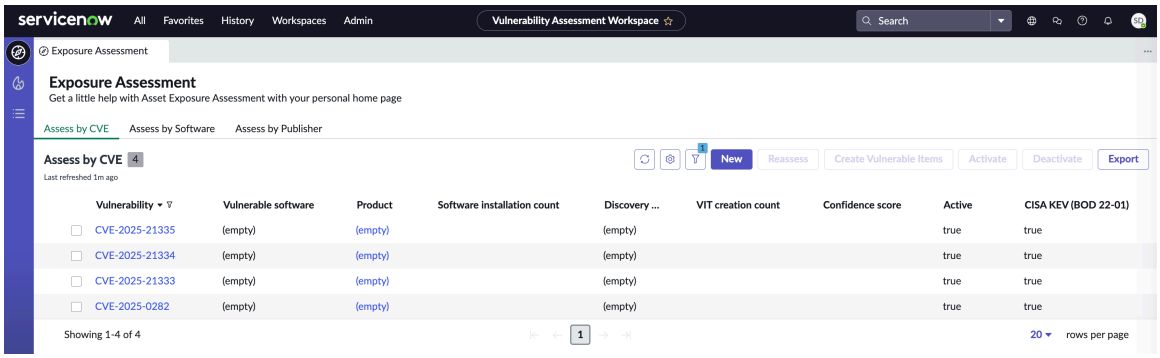
목록 페이지

목록 페이지는 다음을 포함하는 라이브러리로 구성됩니다.

- CVE
- TPE
- CWE

다음 이미지는 취약성 평가 작업 공간 홈페이지를 보여줍니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



노출 평가 살펴보기

노출 평가는 CVE(Common Vulnerabilities and Exposures) 시스템의 일부인 CPE(Common Platform Enumeration) 프레임워크를 사용하여 취약성 소프트웨어에 대한 자산의 취약성 노출을 평가합니다. 이 평가는 소프트웨어 검색 모델을 사용하여 수행됩니다.

매칭 알고리즘을 사용하면 관련 CPE가 소프트웨어 검색 모델에 연결되고 매핑되어 잠재적 노출을 식별할 수 있습니다.

CVE 또는 소프트웨어의 노출 평가를 사용하여 다음 시나리오에 대한 잠재적 취약성에 대한 노출을 식별할 수 있습니다.

- 기존 스캐너로 식별할 수 없는 취약성
- 스캐너가 취약성 탐지를 위한 서명을 제공하기 전 제로 데이 취약성

노출 평가는 이러한 취약성을 정정하고 취약성 관리 프로그램의 성숙도를 개선하기 위한 조기 경고를 제공합니다.

노출 평가를 위한 전제 조건

사용 가능한 버전

애플리케이션	버전
취약성 위기 관리 플러그인	1.0
취약성 대응	20.0
취약성 대응 NVD 포함	1.3
Vulnerability Response Integration with CISA	1.2
NVD와 취약성 대응 통합 **주:** 자세한 내용은 NVD 통합 이해 문서를 참조하십시오.	1.3
소프트웨어 자산 관리	Software Asset Management Foundation 플러그인 또는 소프트웨어 자산 관리 전문가 플러그인

사용 사례

취약성 분석가 조직에서 취약성 노출 평가 작업 공간을 사용하는 방법의 예시는 다음 사용 사례를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

평가 유형	사용
CVE별 평가	CVE별로 취약성을 평가하여 (SAM) 및 디스커버리 데이터를 사용하여 소프트웨어 자산 관리 영향을 받는 시스템의 영향과 노출을 완전히 파악합니다. 수동 VIT를 생성하고 정정 소유자에게 할당하여 즉각적인 정정 작업을 수행합니다. 스캐너가 영향을 받는 모든 시스템을 디스커버리 탐지하지 못할 수 있지만 일반적으로 공격 표면에 있는 대부분의 소프트웨어를 식별하기 때문에 CVE로 평가하는 것이 유용합니다.
소프트웨어별 평가	CVE를 사용하여 소프트웨어가 설치된 CI 수를 식별할 수 없는 경우 소프트웨어별 영향을 평가합니다. 소프트웨어별로 평가하면 수동으로 VIT를 생성하고 공식적으로 게시되기 전에 또는 스캐너에서 식별하기 전에 정정 소유자에게 할당하여 제로 데이 또는 중요 취약성에 대해 사전 예방적으로 조치를 취할 수 있습니다.
게시자별 평가	소프트웨어 벤더의 취약성을 평가하여 벤더가 기간 내에 게시한 CVE에 대해 영향을 받는 시스템의 영향과 노출을 파악합니다. 게시자별 평가는 벤더 위험 및 중요 취약성을 평가하고 사전 예방적 정정을 가능하게 하는 데 도움이 됩니다.

호환성 및 시스템 요구 사항

취약성 대응 응용 프로그램은 에서 사용할 수 있습니다ServiceNow Store. 노출 평가 모듈에는 애플리케이션(com.snc.asset_management)이 ITSM 소프트웨어 자산 관리 필요합니다. 이 애플리케이션은 모든 자산과 소프트웨어 라이센스를 관리하며SAM Foundation, 이 애플리케이션의 버전은 에서 다운로드하는 ServiceNow Store애플리케이션의 일부입니다취약성 대응.

중요사항:
노출 평가 애플리케이션은 다음 플러그인과 함께 작동합니다.

- Software Asset Management Foundation 플러그인(com.snc.sams)
- 소프트웨어 자산 관리 전문가 (com.snc.pa.samp)
- 소프트웨어 자산 관리 플러그인 (com.snc.software_asset_management)

애플리케이션이 인스턴스에 설치되었는지 확인하려면 SAM Foundation 다음으로 이동합니다. 시스템 애플리케이션 〉 모든 사용 가능 애플리케이션 〉 모두 을 클릭하고 com.snc.asset_management 검색합니다. 애플리케이션이 설치되지 않은 경우 설치를 선택합니다. 취약성 노출 평가 애플리케이션은 인스턴스의 자산 데이터에 ServiceNow AI Platform# 액세스해야 하므로 자산 관리 애플리케이션에는 참조할 데이터가 있어야 합니다. 소프트웨어 검색 모델 테이블(cmdb_sam_sw_discovery_model)과 소프트웨어 설치(cmdb_sam_sw_install)에는 데이터가 필요합니다.

소프트웨어 검색 모델의 일치 알고리즘 필드

이 소프트웨어 자산 관리 전문가 애플리케이션을 사용하면 소프트웨어 검색 모델을 편집하여 소프트웨어 검색 모델 양식에서 완전히 정규화되지 않은(부분적으로 정규화됨, 게시자 정규화됨

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

또는 일치하는 항목을 찾을 수 없음) 검색된 소프트웨어를 조정할 수 있도록 수동으로 정규화할 수 있습니다. 버전 취약성 대응 20.0부터 는 에서 소프트웨어 자산 관리 전문가가져온 정규화된 검색 모델을 지원합니다. 다음 필드는 소프트웨어 검색 모델의 일치 알고리즘에 사용됩니다.

CPE(소프트웨어 모델)	**SAM** 기초	**SAM** 전문가용
벤더	기본 키	기본 키
제품	표시 이름	표시 이름
버전	검색된 게시자	검색된 게시자
에디션	검색된 제품	검색된 제품
	검색된 버전	검색된 버전
		표준화된 게시자
		표준화된 제품
		표준화된 버전

주:
SAM Professional 애플리케이션은 핵심 취약성 대응ServiceNow Store 제품에 속하지 않으며 별도의 구독이 필요합니다.

시스템 속성

노출 평가를 위해 CISA가 악용한 취약성을 자동으로 처리하려면 시스템 속성을 *sn_vul_analyst.enable_exposure_for_cisa*true로 설정하십시오. 기본값은 *false*입니다.

예약된 작업

예약된 작업은 다음과 같습니다.

예약된 작업 이름	설명
잠재적 취약성 노출 확인	델타 CVE, 소프트웨어 및 설치를 처리하여 노출을 가져옵니다. **주:** 이 예약된 작업은 12시간마다 실행됩니다. 예약된 다른 작업보다 더 오랜 기간 실행됩니다.
CISA 악용 CVE를 노출 구성에 삽입	주문형. CISA CVE를 노출 구성 테이블에 삽입하여 노출을 계산합니다.
구성된 CVE에 대한 노출 평가 실행	주문형. 노출 구성 테이블의 모든 CVE 기록에 대한 노출을 계산합니다.
소프트웨어 노출 실행	주문형. 노출 구성 테이블의 모든 소프트웨어 기록에 대한 노출을 계산합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주요 용어

- 신뢰도 점수: 신뢰 점수는 필드에 대한 권장 사항을 제공할 때의 신뢰성을 측정한 것입니다. 점수가 높을수록 권장 사항의 신뢰성이 높아집니다. 샘플 계산은 다음 문서를 참조하십시오 신뢰 점수 계산 예.
- 소프트웨어 설치 횟수: 취약성의 영향을 받는 소프트웨어 자산 수입니다.
- 소프트웨어 모델: 제품과 연결된 소프트웨어 모델입니다. 소프트웨어 모델 결과를 보려면 소프트웨어 모델을 드릴다운합니다. 자세한 내용은 Software Asset Management Foundation plugin discovery models and software installations 문서를 참조하십시오.

소프트웨어 설치 개수 필드는 검색 모델의 활성 또는 비활성 상태와 관계없이 총 소프트웨어 설치 수를 제공합니다. 의 취약성 대응v22.0부터 노출 평가〔store-future: BEGIN review〕 또는 VCM(취약성 위기 관리)〔End〕을 위해 비활성 소프트웨어 설치를 필터링해야 하는지 여부를 결정하기 위해 새로운 시스템 속성인 `sn_vul.filter_inactive_sw_installs`가 도입되었습니다. 기본적으로 이 속성은 기본 시스템에서 사용하도록 설정됩니다. 필터를 활성화하면 활성 설치만 표시됩니다.

소프트웨어 검색 모델 테이블의 기본 active=true 필터를 기준으로 필터링된 비활성 소프트웨어 설치의 수는 검색 모델 필드로 표시됩니다. 이 필드의 개수는 소프트웨어 설치 개수 필드에 표시된 필터링된 개수와 일치해야 합니다. 소프트웨어 설치 필드의 개수는 시스템 속성을 업데이트해도 유지됩니다. 업데이트된 개수를 얻으려면 예약된 작업 `Run exposure assessment for configured CVEs` 및 `Run software exposure that updates the count`를 실행해야 합니다.

CVE의 노출 평가

노출 평가에서는 CVE(일반적인 취약성 및 노출)를 사용하여 소프트웨어 검색 모델을 사용하여 자산의 노출을 평가합니다. CVE의 노출 평가를 사용하여 잠재적인 취약성에 대한 노출을 식별할 수 있습니다.

CVE에 의한 노출 평가에 대한 자세한 내용은 다음을 참조하세요.

- CVE를 추가하여 노출 평가
- 노출 평가를 위해 CVE에 대한 VI 생성
- 노출 평가를 위해 CVE 활성화 또는 비활성화
- 노출 평가를 위해 영향을 받는 CI 익스포트
- 신뢰 점수 계산 예

CVE를 추가하여 노출 평가

노출 평가에서 CVE의 노출 구성 목록에 CVE(Common Vulnerabilities and Exposures)를 추가하여 새로운 취약성 또는 제로 데이 취약성의 영향을 평가합니다.

시작하기 전에

필요한 역할: sn_vul_analyst.vul_event_manager

프로시저

1. 다음으로 이동 작업 공간 〉 취약성 평가 작업 공간 〉 노출 평가 〉 CVE별 평가.
2. 추가를 선택합니다.
3. CVE 추가 대화 상자에서 목록에 추가할 CVE를 선택하고 추가 옵션을 선택합니다.
   목록에 이미 있는 CVE는 다시 추가되지 않습니다. 나머지는 CVE 목록에 추가됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
필터 아이콘을 선택하여 고급 뷰 로 이동하고 보려는 CVE를 지정합니다.

4. 목록에 이미 있는 CVE의 영향을 평가하려면 다음을 수행합니다.

   a. 재평가할 CVE의 확인란을 선택합니다.

   b. 다시 평가 버튼을 선택합니다.
   업데이트된 상세 정보가 각 열에 표시됩니다.

노출 평가를 위해 CVE에 대한 **VI** 생성

노출 평가 페이지에서 취약한 항목(VI)을 생성합니다. 그런 다음 취약성 이벤트 관리자는 이 VI 목록을 분석하고 IT 팀이 이러한 취약성을 패치하는 데 도움이 되는 솔루션과 패치를 권장합니다.

시작하기 전에
필요한 역할: sn_vul_analyst.vul_event_manager

이 태스크 정보
노출이 평가되면 잠재적 평가 목록이 CI(구성 항목) 수와 함께 노출 평가 기록에 표시됩니다. 기록을 선택하고 목록 작업에서 취약한 항목 생성을 선택하여 취약한 소프트웨어가 있는 CI와 CVE(알반적인 취약성 및 노출)에 대한 VI(취약한 항목)를 생성할 수 있습니다. VI는 백그라운드에서 생성됩니다. 이 프로세스에는 다소 시간이 걸릴 수 있습니다. 항목이 생성되면 VI 테이블로 이동하여 생성된 기록을 볼 수 있습니다.

프로시저

1. 다음으로 이동 작업 공간 〉 취약성 평가 작업 공간 〉 노출 평가 〉 CVE별 평가.
2. 필요한 CVE를 선택하고 취약한 항목 생성 옵션을 선택합니다.
3. 취약한 항목 생성 대화 상자에서 취약한 항목 생성 옵션을 선택합니다.
4. VI를 생성하는 데 사용되는 백그라운드 작업의 상태를 보려면 상태 보기 링크를 선택합니다.

노출 평가를 위해 **CVE** 활성화 또는 비활성화

CVE의 델타 처리를 위해 CVE를 활성화하여 CVE의 활성 목록에 추가할 수 있습니다.

시작하기 전에
필요한 역할: sn_vul_analyst.vul_event_manager

주:
취약성 노출 평가 버전 4.0.1부터 CVE(일반 취약성 항목)가 업데이트되지 않았거나 지난 30일 동안 생성된 VIT(취약한 항목)가 있는 경우 해당 CVE에 대한 노출 평가 기록이 자동으로 비활성으로 표시됩니다. 그러나 이러한 기록을 수동으로 활성화하거나 비활성화할 수 있습니다. 또한 예약된 작업이 *Check potential vulnerability exposure* 계속 실행되어 이러한 CVE를 스캔하여 비활성으로 지정합니다.

프로시저

1. 다음으로 이동 작업 공간 〉 취약성 평가 작업 공간 〉 노출 평가 〉 CVE별 평가.
2. 필요한 활성 CVE를 선택하고 비활성화 옵션을 선택합니다.
   CVE가 비활성화됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
소프트웨어를 활성화하려면 동일한 프로세스에 따라 활성화 옵션을 선택합니다.

3. 페이지를 새로 고치면 활성 열에서 업데이트된 상태(False)가 표시됩니다.

노출 평가를 위해 영향을 받는 CI 익스포트

노출 평가 기록과 관련된 CI(구성 항목)를 Excel 시트로 익스포트하여 새 CVE의 영향을 받은 자산 목록을 추적할 수 있습니다. 이 시트는 자산 상세 정보 및 소유자를 공유하여 제로 데이 취약성에 대해 알려진 영향을 받는 자산으로 인시던트를 생성하는 데 사용할 수 있습니다.

시작하기 전에
필요한 역할: sn_vul_analyst.vul_event_manager

프로시저

1. 다음으로 이동 작업 공간 〉 취약성 평가 작업 공간 〉 노출 평가 〉 CVE별 평가.
2. 익스포트하려는 CI가 있는 기록의 검색 모델을 선택합니다.
   소프트웨어 설치 탭에는 소프트웨어 기록과 관련된 활성 CI가 포함되어 있습니다. 이러한 CI는 설치 대상 열에 저장됩니다.
3. 익스포트 옵션을 선택합니다.
4. 익스포트 대화 상자에서 파일 유형 및 제공 유형을 선택하여 관련 CI를 익스포트합니다.
5. 익스포트 옵션을 선택합니다.

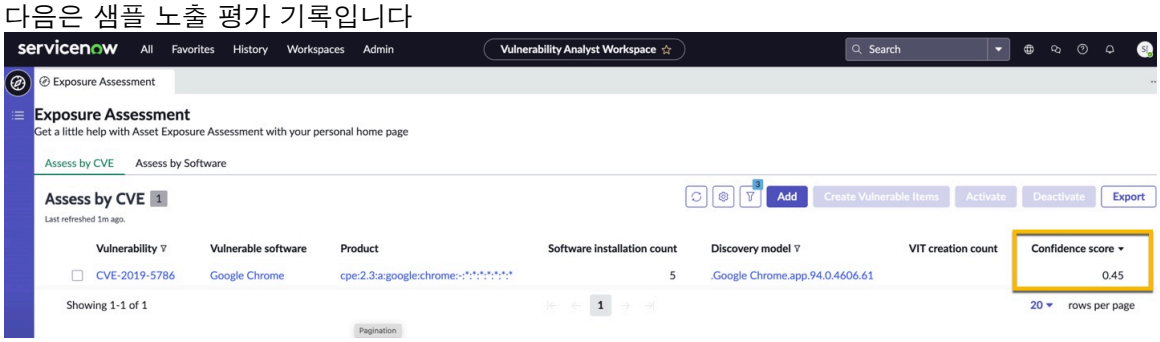
신뢰 점수 계산 예

CVE(Common Vulnerabilities and Exposures) 정보를 기반으로 제로 데이 취약성에 대한 신뢰도를 계산하는 예입니다.

다음은 **CVE-2019-5786**의 CPE(Common Platform Enumeration) 정보에서 신뢰도 점수를 계산하는 예입니다.

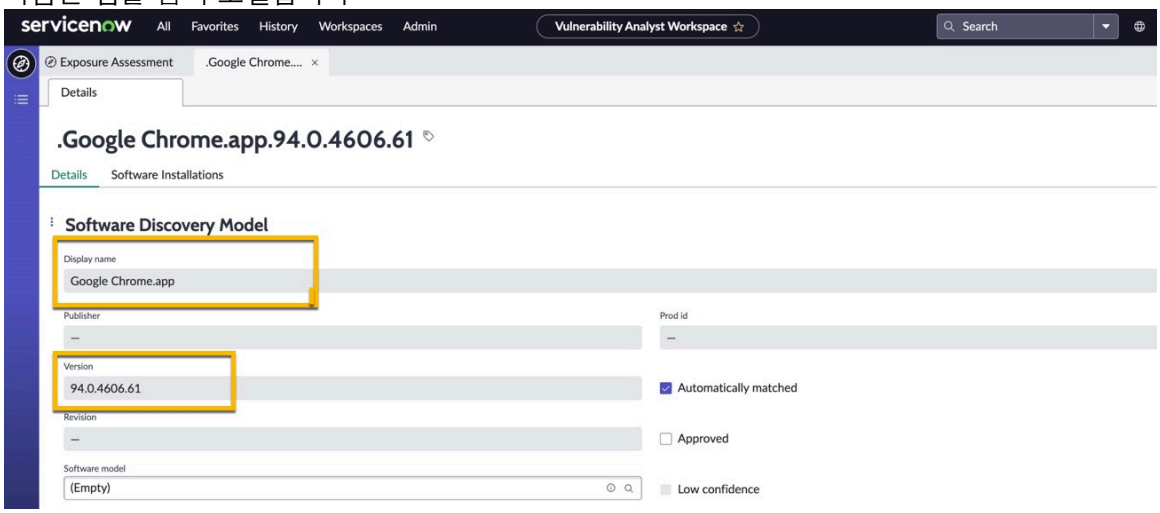
주:
CPE를 보려면 취약성 열을 취약성별로 그룹화하면 됩니다. 취약한 소프트웨어 상세 정보 보기에 대한 자세한 내용은 문서를 참조하십시오 취약한 소프트웨어 상세 정보 보기.

다음은 샘플 노출 평가 기록입니다



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음은 샘플 검색 모델입니다



신뢰 점수를 계산하는 방법

신뢰 점수 범위는 0–1입니다. CPE 정보를 기반으로 신뢰 점수는 다음 수식을 사용하여 계산됩니다.

```
((BASE SCORE) + (publisher score) +(product score) + (version score) + (edition score) + (display name score)) / 100
```

=

```
((25) + (10) + (10)) / 100
```

=

```
45 / 100
```

=

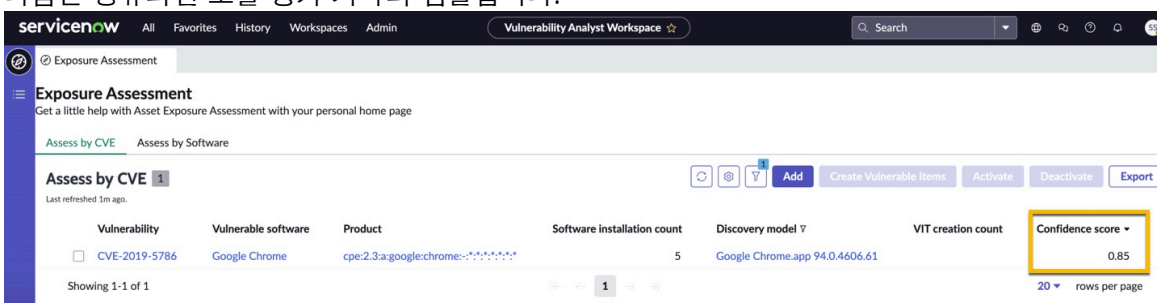
```
.45
```

주:
신뢰 점수를 계산하는 데 사용되는 값을 참조하려면 문서를 참조하십시오 노출 평가를 위한 신뢰 점수 참조 테이블.

소프트웨어 모델이 정규화된 검색 모델과 일치할 때 신뢰 점수를 계산하는 중

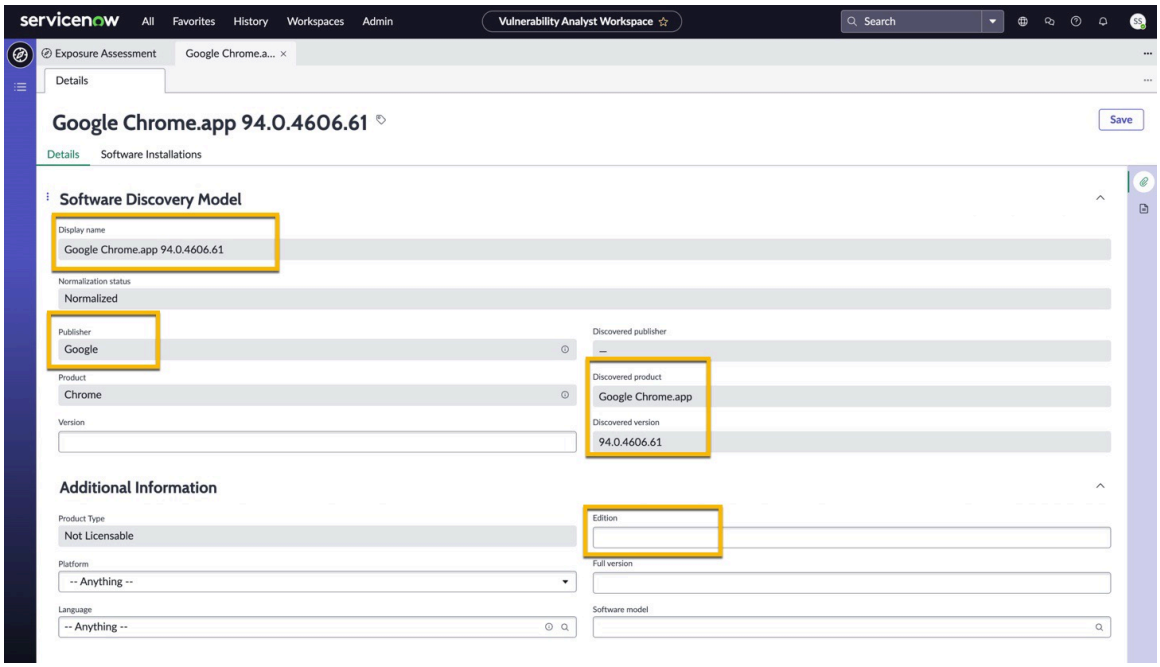
정규화된 검색 모델을 사용하는 경우 소프트웨어 검색 모델에 사용할 수 있는 추가 정보가 향상된 신뢰도 점수를 제공합니다. 다음은 샘플 계산입니다.

다음은 정규화된 노출 평가 기록의 샘플입니다.



다음은 샘플 정규화된 검색 모델입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.




```
((BASE SCORE) + (publisher score) + (product score) + (version score) + (edition score) + (display name score)) / 100
```

=

```
((25) + (20) + (15) + (15) + (0) + (10)) / 100
```

=

```
85 / 100
```

=

```
.85
```

주:
신뢰 점수를 계산하는 데 사용되는 값을 참조하려면 문서를 참조하십시오 노출 평가를 위한 신뢰 점수 참조 테이블.

취약한 소프트웨어 상세 정보 보기

취약한 소프트웨어(이 경우 Google Chrome)의 상세 정보를 봅니다. 검색 모델 및 CPE(공통 플랫폼 열거형)와 일치합니다. 이 CPE 버전은 모든 Google Chrome 버전에 영향을 줍니다.

시작하기 전에
필요한 역할: sn_vul_analyst.vul_event_manager

프로시저

1. 모두로 이동하여 를 입력합니다*sn_vul_software.LIST*.
2. 취약한 소프트웨어 목록에서 **cpe:2.3:a:google:chrome:-:*:*:*:*:*:*:*** 를 검색하여 정보를 봅니다.

노출 평가를 위한 신뢰 점수 참조 테이블

신뢰 점수를 계산하는 데 사용되는 참조 값입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

참조 테이블

신뢰 점수 계산 참조 테이블

취약한 소프트웨어 세그먼트	검색 모델 세그먼트	포인트	디스커버리 모델 정확히 일치 세그먼트	정확한 일치 점수
게시자	표시 이름	15	게시자	5
모델	표시 이름	15	모델	5
버전	표시 이름	10	버전	5
에디션	표시 이름	3	정규화된 에디션	2
표시 이름	표시 이름	10	표시 이름	5

신뢰 점수 요약 테이블

포인트	값
모든 점수의 합계	75%
최저 점수 주: 일치하는 모든 검색 모델에 제공되는 최소 점수입니다.	25
총점	100

소프트웨어별 노출 평가

자산 또는 구성 항목에 대한 CVE(알반적인 취약성과 노출)를 사용할 수 없는 경우 제로 데이 취약성에 대한 노출 평가 소프트웨어 검색 모델을 통해 소프트웨어 정보를 사용하여 노출을 평가합니다.

소프트웨어별 노출 평가에 대한 자세한 내용은 다음을 참조하십시오.

- 노출 평가를 위한 소프트웨어 추가
- 노출 평가를 위한 소프트웨어에 대한 VI 생성
- 노출 평가를 위한 소프트웨어 활성화 또는 비활성화
- 취약성 평가 작업 공간에서 소프트웨어의 영향을 받은 CI 익스포트

노출 평가를 위한 소프트웨어 추가

새로운 취약성 또는 제로 데이 취약성의 영향을 평가하기 위해 노출 평가 모듈에 새 소프트웨어를 추가합니다.

시작하기 전에
필요한 역할: sn_vul_analyst.vul_event_manager

프로시저

1. 다음으로 이동 작업 공간 〉 취약성 평가 작업 공간 〉 노출 평가 〉 소프트웨어별 평가 〉 추가.
2. 양식에서 필드를 채웁니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
게시자	소프트웨어 게시자입니다.
제품	소프트웨어의 제품 이름입니다.
버전	소프트웨어 제품의 버전입니다.
에디션	소프트웨어의 에디션입니다.

주:
상태가 '아니오'인 테이블에 있는 소프트웨어에 대한 노출을 추가하려고 하면 중복 기록이 생성되지 않습니다. 기존 소프트웨어의 상태가 "true"로 업데이트됩니다.

3. 추가 옵션을 선택합니다.
4. 목록에 이미 있는 소프트웨어의 영향을 평가하려면 다음을 수행합니다.
   a. 재평가할 소프트웨어의 확인란을 선택합니다.
   b. 다시 평가 버튼을 선택합니다.
   업데이트된 상세 정보가 각 열에 표시됩니다.

노출 평가를 위한 소프트웨어에 대한 VI 생성

노출 평가 페이지에서 취약한 항목(VI)을 생성합니다. 그런 다음 취약성 이벤트 관리자는 이 VI 목록을 분석하고 IT 팀이 이러한 취약성을 패치하는 데 도움이 되는 솔루션과 패치를 권장합니다.

시작하기 전에
필요한 역할: sn_vul_analyst.vul_event_manager

프로시저

1. 다음으로 이동 작업 공간 〉 취약성 평가 작업 공간 〉 노출 평가 〉 소프트웨어별 평가.
2. VI를 생성할 기록을 선택합니다.
3. 취약한 항목 생성 옵션을 선택합니다.
4. 취약한 항목 생성 대화 상자에서 다음 중 하나를 선택합니다.
   - 기존 취약성
   - 새로운 취약성
5. 취약한 항목 생성 옵션을 선택합니다.

노출 평가를 위한 소프트웨어 활성화 또는 비활성화

소프트웨어의 추가 델타 처리를 중지하려면 소프트웨어를 비활성화하도록 선택하여 활성 소프트웨어 목록에서 제거할 수 있습니다.

시작하기 전에
필요한 역할: sn_vul_analyst.vul_event_manager

프로시저

1. 다음으로 이동 작업 공간 〉 취약성 평가 작업 공간 〉 노출 평가 〉 소프트웨어별 평가.
2. 비활성화하려면 필요한 활성 소프트웨어를 선택하고 비활성화 옵션을 선택합니다.
   소프트웨어가 비활성화되었습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
소프트웨어를 활성화하려면 동일한 프로세스에 따라 활성화 옵션을 선택합니다.

3. 페이지를 새로 고치면 활성 열에서 업데이트된 상태(False)가 표시됩니다.

취약성 평가 작업 공간에서 소프트웨어의 영향을 받은 CI 익스포트

노출 평가 기록과 관련된 CI(구성 항목)를 Excel 시트로 익스포트하여 새 소프트웨어의 영향을 받은 자산 목록을 추적할 수 있습니다. 이 시트는 자산 상세 정보 및 소유자를 공유하여 제로 데이 취약성에 대해 알려진 영향을 받는 자산으로 인시던트를 생성하는 데 사용할 수 있습니다.

시작하기 전에
필요한 역할: sn_vul_analyst.vul_event_manager

프로시저

1. 다음으로 이동 작업 공간 〉 취약성 평가 작업 공간 〉 노출 평가 〉 소프트웨어별 평가.
2. 익스포트하려는 CI가 있는 기록의 검색 모델을 선택합니다.
   소프트웨어 설치 탭에는 소프트웨어 기록과 관련된 활성 CI가 포함되어 있습니다. 이러한 CI는 설치 대상 열에 저장됩니다.
3. 익스포트 옵션을 선택합니다.
4. 익스포트 대화 상자에서 파일 유형 및 제공 유형을 선택하여 관련 CI를 익스포트합니다.
5. 익스포트 옵션을 선택합니다.

게시자 소프트웨어별 노출 평가

자산 또는 구성 항목에 대한 CVE(알반적인 취약성과 노출)를 사용할 수 없는 경우 제로 데이 취약성에 대한 노출을 평가합니다. 소프트웨어 검색 모델을 통해 소프트웨어 정보를 사용하여 노출을 평가합니다.

소프트웨어별 노출 평가에 대한 자세한 내용은 다음을 참조하십시오.

- 노출 평가를 위해 게시자에 의한 소프트웨어 추가
- 노출 평가를 위해 게시자가 소프트웨어에 대한 VI 생성
- 노출 평가를 위해 게시자가 소프트웨어를 활성화 또는 비활성화합니다.
- 취약성 평가 작업 공간에서 게시자의 영향을 받는 소프트웨어 CI 익스포트

노출 평가를 위해 게시자에 의한 소프트웨어 추가

노출 평가 모듈에 게시자별 소프트웨어를 추가하여 새로운 취약성 또는 제로 데이 취약성의 영향을 평가합니다.

시작하기 전에
필요한 역할: sn_vul_analyst.vul_event_manager

프로시저

1. 다음으로 이동 작업 공간 〉 취약성 평가 작업 공간 〉 노출 평가 〉 게시자별 평가 〉 새로 작성함.
2. 새 평가 창에서 평가를 수행할 게시자를 선택합니다.
3. **CVE** 게시 위치 필드에서 날짜를 선택합니다.
   선택한 날짜 이후에 소프트웨어와 관련된 CVE(일반 취약성 항목)가 수정되면 해당 소프트웨어는 노출 평가 대상으로 간주됩니다.
4. **CVE** 심각도 섹션에서 CVE의 심각도 수준을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. 평가 시작을 선택합니다.
   작업이 완료되면 선택한 기록이 생성됩니다.

노출 평가를 위해 게시자가 소프트웨어에 대한 VI 생성

노출 평가 페이지에서 VI(취약한 항목)를 생성하여 VI 목록을 분석하고 IT 팀이 취약성을 패치하는 데 도움이 될 수 있는 솔루션과 패치를 추천합니다.

시작하기 전에
필요한 역할: sn_vul_analyst.vul_event_manager

프로시저

1. 다음으로 이동 작업 공간 〉 취약성 평가 작업 공간 〉 노출 평가 〉 게시자별 평가.
2. VI를 생성할 기록을 선택합니다.
3. 취약한 항목 생성 옵션을 선택합니다.
4. 취약한 항목 생성 대화 상자에서 다음 중 하나를 선택합니다.
   - 기존 취약성
   - 새로운 취약성
5. 취약한 항목 생성 옵션을 선택합니다.

노출 평가를 위해 게시자가 소프트웨어를 활성화 또는 비활성화합니다.

게시자가 소프트웨어를 활성화 또는 비활성화하여 소프트웨어의 델타 처리를 중지하고 활성 소프트웨어 목록에서 제거합니다.

시작하기 전에
필요한 역할: sn_vul_analyst.vul_event_manager

프로시저

1. 다음으로 이동 작업 공간 〉 취약성 평가 작업 공간 〉 노출 평가 〉 게시자별 평가.
2. 비활성화하려면 게시자가 필요한 활성 소프트웨어를 선택하고 다시 평가 버튼 아래에서 비활성화 옵션을 선택합니다.
   게시자가 비활성화되었습니다.

   주:
   게시자가 소프트웨어를 활성화하려면 동일한 프로세스에 따라 활성화 옵션을 선택합니다.

3. 페이지를 새로 고치면 활성 열에서 업데이트된 상태(False)가 표시됩니다.

취약성 평가 작업 공간에서 게시자의 영향을 받는 소프트웨어 CI 익스포트

노출 평가 기록과 관련된 CI(구성 항목)를 Excel 시트로 익스포트하여 새 소프트웨어의 영향을 받은 자산 목록을 추적할 수 있습니다. 이 시트는 자산 상세 정보 및 소유자를 공유하여 제로 데이 취약성에 대해 알려진 영향을 받는 자산으로 인시던트를 생성하는 데 사용할 수 있습니다.

시작하기 전에
필요한 역할: sn_vul_analyst.vul_event_manager

프로시저

1. 다음으로 이동 작업 공간 〉 취약성 평가 작업 공간 〉 노출 평가 〉 게시자별 평가.
2. 익스포트하려는 CI가 있는 기록의 검색 모델을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

소프트웨어 설치 탭에는 소프트웨어 기록과 관련된 활성 CI가 포함되어 있습니다. 이러한 CI는 설치 대상 열에 저장됩니다.

3. 익스포트 옵션을 선택합니다.
4. 익스포트 대화 상자에서 파일 유형 및 제공 유형을 선택하여 관련 CI를 익스포트합니다.
5. 익스포트 옵션을 선택합니다.

취약성 평가 탐색

Vulnerability Assessment Workspace는 Vulnerability Event Manager가 특히 제로 데이 취약성 분석 중에 취약성 이벤트를 생성하고 취약성 평가를 수행하도록 설계되었습니다.

취약성 평가 작업 공간을 사용하여 다음과 같은 중요한 취약성을 관리할 수 있습니다.

- 심각 또는 높은 심각도의 제로데이 취약성
- 취약성에 대해 식별된 새로운 위협 인텔리전스
- 심각 또는 높은 심각도의 취약성을 신속하게 악용합니다.

Vulnerability Assessment Workspace 및 Vulnerability Crisis Management

취약성 이벤트 관리자는 관심 있는 취약성에 대한 취약성 이벤트 기록을 식별하고 생성합니다. 취약한 이벤트를 생성한 후에는 위험 평가를 수행하고, 위험 속성을 수동으로 업데이트하고, 위험 점수를 자동으로 계산할 수 있습니다. 취약성 평가 작업 공간을 사용하면 다음 작업을 수행하여 취약성 위기 이벤트를 처음부터 해결까지 처리할 수 있습니다.

- 취약성 평가 기록 생성
- 취약성 평가 기록 수정
- 취약성 평가 수행
- 평가 상세 정보 검토
- 취약성 평가 기록에 우선순위 및 노출 수준 할당
- 평가 기록에 영향을 받는 CI 추가
- 영향을 받는 CI 또는 영향을 받는 소프트웨어 구성요소에 대한 취약한 항목 생성
- 의 중요 보안 인시던트에 취약성 평가 기록 연결 중요 보안 인시던트 관리

취약성 평가를 위한 필수 조건

사용 가능한 버전

애플리케이션	버전
취약성 위기 관리 플러그인	1.0
취약성 대응	20.0
취약성 대응 NVD 포함 주: 자세한 내용은 NVD 통합 이해 문서를 참조하십시오.	1.4.2
Vulnerability Response Integration with CISA	1.2

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용 가능한 버전

애플리케이션	버전
SBOM을 위한 데이터 모델	1.1.2
소프트웨어 자재 명세서 Core	2.0.2
소프트웨어 자산 관리	Software Asset Management Foundation 플러그인 또는 소프트웨어 자산 관리 전문가 플러그인
중요 보안 인시던트 관리	2.2.5

예약된 작업

다음은 예약된 작업입니다.

예약된 작업 이름	설명
취약성 평가	평가 후 취약한 항목(VIT 또는 AVIT)이 생성되면 영향을 받는 구성 항목 테이블과 CI 소스를 업데이트합니다. **주:** 이 예약된 작업은 매일 실행됩니다. 예약된 다른 작업보다 더 오랜 기간 실행됩니다.

관련 정보

취약성 위기 관리

취약성 평가 기록 생성

관심 있는 취약성에 대한 평가 기록을 생성합니다. 평가를 생성한 후에는 초기 위험 평가를 시작하고, 기록을 수동으로 업데이트하고, 위험 점수를 자동으로 계산할 수 있습니다.

시작하기 전에

취약성 평가와 관련된 작업을 수행할 수 있으려면 기본 시스템 취약성 평가 이벤트 관리자 할당 그룹에 속해 있어야 합니다.

필요한 역할: sn_vul_analyst.vul_event_manager, sn_vul_analyst.emergency_response

이 태스크 정보

이벤트 레코드를 기본 CVE 또는 영향을 받는 제품에 연결하여 관심 있는 취약성에 대한 취약성 평가 레코드를 만들 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 작업 공간 〉 취약성 평가 작업 공간.
2. 취약성 평가 아이콘을 선택합니다.
3. 새로 만들기를 선택합니다.
4. 제목 필드에 적절한 제목을 입력합니다.
5. 옵션: 기본 CVE 필드에서 새 평가 기록과 연결할 기본 **CVE** 를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
평가 기록의 모든 예비 상세 정보는 선택하거나 생성하는 제품 또는 기록과 연결한 기본 CVE에 따라 채워집니다.

6. 제출을 선택합니다.
입력한 제목의 취약성 평가 기록이 생성되고 새 취약성 평가 탭에 표시됩니다. 기본적으로 취약성 평가 기록은 상세 정보 탭에 표시됩니다.

주:
기본적으로 연결/매핑된 기본 CVE의 상세 정보가 표시됩니다.

- 취약성 평가 이벤트 기록 생성 중에 기본 CVE가 선택되지 않은 경우 기본 기록이 생성됩니다.
- 기본 CVE에 연결된 CVE가 있는 경우 관련 CVE가 취약성 항목 탭에 채워집니다. 취약성 항목 탭에서 연결된 CVE를 더 추가할 수 있습니다.

7. 영향을 받는 제품 탭으로 이동합니다.

a. 새로 만들기를 선택합니다.

b. 양식의 필드에 내용을 입력합니다.

필드	설명
게시자	소프트웨어 게시자입니다. 필수 필드입니다.
제품	소프트웨어의 제품 이름입니다. 필수 필드입니다.
버전	소프트웨어 제품의 버전입니다.
에디션	소프트웨어의 에디션입니다.

주:
상태가 '아니오'인 테이블에 있는 소프트웨어에 대한 취약성을 추가하려고 하면 중복 기록이 생성되지 않습니다. 기존 소프트웨어의 상태가 "true"로 업데이트됩니다.

c. 확인을 선택합니다.

8. 저장을 선택합니다.

취약성 평가 자동 플러시 기록 업데이트

취약성 평가 자동 플러시 기록을 업데이트합니다.

시작하기 전에
필요한 역할: sn_vul_analyst.vul_event_manager

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보

기본 시스템에서 취약성 평가 기록 보존 기간은 6개월로 설정됩니다. 취약성 평가 기록 상태가 종결인 경우 취약성 평가 기록은 정의된 보존 기간까지만 저장되고 해당 평가의 관련 기록은 6개월 후에 모든 관련 테이블에서 제거됩니다.

프로시저

1. 다음으로 이동 모두 〉 자동 플러시.
2. 테이블 sn_vul_analyst_vulnerability_assessment가 있는 기록을 엽니다.
3. 취약성 평가 기록에 대한 자동 플러시 옵션을 활성화하려면 활성 확인란을 선택합니다.
4. 업데이트를 클릭합니다.

취약성 평가 기록 수정

취약성 평가 기록을 생성한 후 업데이트합니다. 필드의 값을 기준으로 위험 점수를 계산할 수 있습니다.

시작하기 전에

필요한 역할: sn_vul_analyst.vul_event_manager

이 태스크 정보

취약성 평가에 기본 CVE가 추가되면 기록이 평가 보류 중 상태로 이동됩니다. 취약성 항목탭에서 다른 관련 CVE를 추가로 추가하거나 영향을 받는 제품 탭에서 이 취약성의 영향을 받는 제품을 추가할 수 있습니다. 위험 평가 필드를 추가로 수정할 수 있으며 이에 따라 평가 기록의 위험 점수가 자동으로 업데이트됩니다.

프로시저

1. 다음으로 이동 모두 〉 취약성 평가 작업 공간 〉 취약성 평가.
2. 상세 정보 탭에서 필드를 업데이트합니다.

필드	설명
직위	취약성 이벤트 기록을 설명하는 제목입니다.
기본 CVE	이벤트 기록과 연결한 기본 CVE입니다.
상태	이벤트 기록의 현재 상태입니다.
우선순위	1-5의 척도에서 이벤트 기록의 우선순위입니다.
경보 소스	잠재적 취약성 이벤트의 소스입니다.
위험 점수	자동으로 계산된 위험 점수 기본적으로 편집할 수 없습니다.
노출 수준	1-5의 척도에서 취약성 이벤트의 노출 수준입니다.
담당 그룹	이벤트 기록이 할당된 할당 그룹입니다.
담당자	이벤트 기록이 할당된 사용자입니다.
설명	이벤트 기록에 대한 자세한 설명입니다.

3. 취약성 항목 탭으로 이동하여 관련 또는 관련 CVE를 추가합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 새로 만들기를 선택합니다.

b. 취약성 항목 필드에서 기록을 검색합니다.

c. 평가 기록과 연결할 취약성 기록을 선택합니다.

d. 옵션: 찾아보기를 선택하여 파일을 찾아 첨부합니다.

e. 저장을 선택합니다.
선택한 취약성 레코드가 평가 기록에 추가되고 취약성 항목 탭에 표시됩니다.

4. 옵션: 영향을 받는 제품을 추가합니다.

5. 평가 기록에 관련 링크 추가.

6. 취약성 평가 이벤트 기록과 연결된 기본 CVE에 대한 위험 속성을 수정합니다.

필드	설명
메모리 손상	이 이벤트 기록이 메모리를 손상시킬 수 있는지 여부를 나타냅니다.
원격 코드 실행 파일	원격 코드 실행이 가능한지 나타냅니다.
로컬 권한 에스컬레이션	로컬 권한 에스컬레이션 취약성이 있는지 나타냅니다.
무단 접근	무단 액세스 취약성이 있는지 나타냅니다.
DDOS	잠재적 이벤트에 분산 서비스 거부가 포함될 수 있는지 여부를 나타냅니다.
공격 복잡성	첨부 파일의 복잡성을 나타냅니다. 옵션은 낮음, 중간 또는 높음입니다.
공격 벡터	잠재적인 공격 경로 또는 방법을 나타냅니다. 옵션은 네트워크, 인접 네트워크, 로컬, 물리적, 없음입니다.
필요한 권한	공격자가 취약성을 악용하는 데 필요한 권한 수준을 나타냅니다. 옵션은 없음, 낮음 또는 높음입니다.
사용자 상호작용	취약성을 악용하는 데 사용자 상호작용이 필요한지 여부를 나타냅니다.
기밀성 영향	취약성의 기밀성에 대한 잠재적 영향의 측정값을 나타냅니다. 옵션은 없음, 낮음 또는 높음입니다.
범위 변경	평가가 변경된 경우 범위를 나타냅니다.
가용성 영향	악용된 오용 취약성의 가용성에 대한 잠재적 영향을 나타냅니다. 가용성은 정보 자원의 접근성을 나타냅니다. 옵션은 없음, 낮음 또는 높음입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
무결성 영향	악용된 오용 취약성의 무결성에 대한 잠재적 영향을 나타냅니다. 무결성은 정보의 신뢰성과 보장된 진실성을 나타냅니다. 옵션은 없음, 낮음 또는 높음입니다.
정정 수준	취약성에 대한 정정 상태 또는 가용성을 나타냅니다. 옵션으로 공식 수정, 임시 수정, 임시 해결책, 사용할 수 없음, 정의되지 않음 등이 있습니다.
익스플로잇 코드 성숙도	기존 악용 기술 및 코드 가용성의 상태를 기준으로 취약성이 악용될 가능성을 나타냅니다. 옵션으로 증명되지 않음, 개념 증명, 기능적, 높음 및 정의되지 않음이 있습니다.
보고서 신뢰도	취약성이 존재한다고 확신하는 정도를 나타냅니다.

7. 작성 필드에 관련 의견을 입력합니다.
   - 작업 메모(비공개) 필드에 작업 메모를 입력합니다.
   - 의견 필드에 의견(모든 사람이 볼 수 있음)을 입력합니다.
8. 평가 기록을 저장합니다.
   기본 CVE 또는 평가 기록과 연결된 영향을 받는 제품에 대한 위험 속성 필드의 업데이트에 따라 위험 점수 필드가 자동으로 업데이트됩니다.

   주:
   기본 시스템 위험 점수 계산기 규칙 또는 기준을 수정하려면 다음으로 이동합니다. 모두 〉 취약성 평가 계산기 〉 취약성 평가 위험 계산기 〉 취약성 평가 위험 규칙. 필요에 따라 기준을 추가하고 필드 수준 가중치를 기존 기준으로 수정할 수 있습니다.

다음에 수행할 작업
이벤트 기록에 대한 초기 평가를 수행합니다.

취약성 평가 기록에서 관련 **CVE** 또는 영향을 받는 제품 삭제

더 이상 필요하지 않은 경우 취약성 이벤트 기록을 삭제합니다.

시작하기 전에
필요한 역할: sn_vul_analyst.vul_event_manager

이 태스크 정보
취약성 평가 기록과 연결된 CVE 또는 영향을 받는 제품을 삭제할 수 있습니다. 취약성 항목/관련 CVE 또는 영향을 받는 제품이 신규 또는 보류 중인 평가 상태인 경우에만 삭제할 수 있습니다.

프로시저
1. 다음으로 이동 모두 〉 작업 공간 〉 취약성 평가.
2. 취약성 평가 기록을 선택합니다.
3. 취약성 항목 탭 또는 영향을 받는 제품 탭을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 연결된 CVE 또는 영향을 받는 제품 기록을 선택합니다.
5. 삭제를 선택합니다.

> **주:**
> 삭제 버튼은 평가 기록이 신규 또는 보류 중인 평가 상태일 때만 표시됩니다.

평가 기록에 관련 링크 추가

평가 기록과 관련된 추가 링크 및 정보를 추가합니다.

시작하기 전에
필요한 역할: sn_vul_analyst.vul_event_manager

프로시저
1. 다음으로 이동 작업 공간 〉 취약성 평가 작업 공간.
2. 평가 기록 항목을 선택합니다.
3. 관련 링크 탭을 선택합니다.
4. 설명 필드에 관련 설명을 입력합니다.
5. 링크 필드에 URL을 입력합니다.
6. 확인을 선택합니다.
   관련 링크가 추가되고 관련 링크 탭에 나열됩니다.

평가 수행

취약성 평가 기록을 생성하고 위험 속성 필드를 업데이트한 후 이벤트 기록에 대한 평가를 실행합니다.

시작하기 전에
필요한 역할: sn_vul_analyst.vul_event_manager

이 태스크 정보
관심 취약성에 대한 이벤트가 생성되고 시스템 및 데이터에 위험을 나타내는 것으로 확인된 후 초기 평가를 수행합니다. 이 활동의 목적은 심층적인 노출 평가로 위험 평가를 업데이트하여 위협을 추가로 분석하는 것입니다.

프로시저
1. 다음으로 이동 작업 공간 〉 취약성 평가 작업 공간 〉 취약성 평가.
2. 취약성 평가 이벤트 기록 목록에서 관련 기록을 선택합니다.
3. 평가를 선택하여 취약성 평가를 실행합니다.
   Vulnerability Response - 취약성 평가 프로세스 이벤트 백그라운드 작업이 시작되고 관련 알림이 표시됩니다.
4. 알림에서 상태 보기를 선택하여 실행 중인 작업의 상태를 봅니다.
5. 저장을 선택합니다.

   평가 탭에 평가 상세 정보가 표시됩니다. 평가가 처리되면 취약한 항목 또는 CVE와 연결된 VIT 또는 AVIT가 취약한 항목 또는 애플리케이션 취약한 항목 탭에 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

결과

- 관련된 CVE와 관련된 취약한 항목 또는 TPE는 평가 중에 가져옵니다. 취약한 항목과 관련된 CI도 식별되어 영향을 받는 구성 항목 테이블에 표시됩니다.
- 연결된 CI가 영향을 받는 CI 테이블에 없는 경우, 식별된 CI가 테이블에 추가되고 취약한 항목 있음 필드 값은 **True**로 설정되며 소스 필드의 값은 스캐너로 설정됩니다.
- 영향을 받는 CI 테이블에 CI가 이미 있는 경우 취약한 항목 있음 필드 값만 **True** 로 설정되고 CI에 대한 소스 필드 값은 평가 레코드가 생성되었을 때와 동일하게 유지됩니다.
- 평가 후에 취약한 항목이 생성되면 영향을 받는 CI 테이블과 CI의 소스를 업데이트하기 위해 취약성 평가 예약된 작업이 실행됩니다.

다음에 수행할 작업

- 취약성 평가 기록에 우선순위 및 노출 수준 할당
- 평가 기록에 영향을 받는 CI 추가
- 영향을 받는 CI 또는 영향을 받는 소프트웨어 구성요소에 대한 취약한 항목 생성
- 평가 기록에 관련 링크 추가

관련 정보

평가 탭

개요 탭

평가 탭

평가 탭에서 평가 결과를 검토합니다. 취약성 이벤트에 대한 평가를 수행한 후에는 기록이 데이터의 소프트웨어 자재 명세서소프트웨어 자산 관리 상관관계를 파악하고 시각화를 통해 표시됩니다.

평가 탭은 생성한 평가 기록을 기반으로 데이터(사용 가능한 경우)를 채우고 CMDB의 소프트웨어 자산 관리 평가 및 소프트웨어 자재 명세서 구성요소 데이터와 상세 정보를 상호 연관시킵니다.

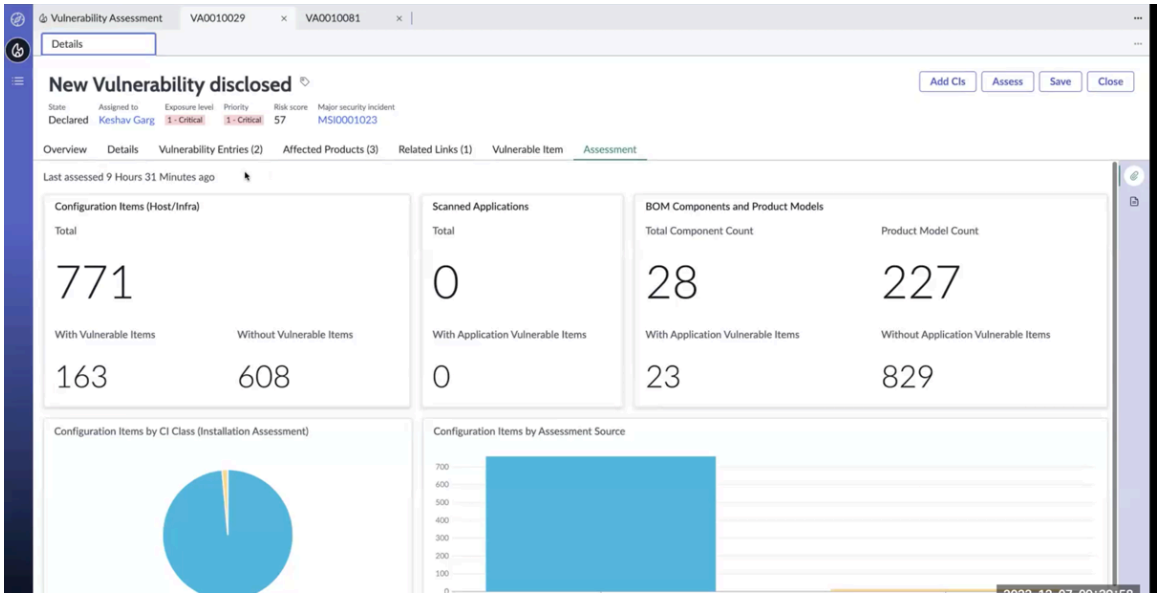
평가 작동 방식

평가 버튼을 선택하면 데이터와 SBOM 데이터를 모두 소프트웨어 자산 관리 사용하는 모든 관련 CVE 및 영향을 받는 제품에 대한 평가가 시작됩니다. 백그라운드 작업이 트리거되고 평가가 처리되면 취약한 항목 또는 CVE와 연결된 VIT 또는 AVIT가 취약한 항목 및 애플리케이션 취약한 항목 탭에 표시됩니다.

- CVE와 관련된 모든 취약한 항목 또는 TPE가 식별됩니다.
- 취약한 항목과 관련된 구성 항목(CI)도 식별되어 영향을 받는 구성 항목 테이블에 표시됩니다.
- 영향을 받는 CI 테이블에 CI가 없는 경우 식별된 CI가 테이블에 추가되고 취약한 항목 있음 플래그가 True로 바뀌며 소스 필드의 값이 스캐너로 설정됩니다.
- 영향을 받는 구성 항목 테이블에 CI가 이미 있는 경우 취약한 항목 있음 플래그만 true로 설정되고 소스 는 평가 레코드가 생성되었을 때와 변경되지 않은 상태로 유지됩니다.
- 평가 후에 취약한 항목이 생성되면 영향을 받는 CI 테이블과 CI의 소스를 업데이트하기 위해 취약성 평가 예약된 작업이 실행됩니다.
- 평가 작업 공간에서 타임스탬프를 보고 이벤트의 마지막 평가를 볼 수 있습니다. 평가 탭은 새 평가가 생성될 때만 표시됩니다. 평가가 진행 중 상태인 경우 평가가 진행 중으로 마지막 평가 상태가 나타납니다. 업데이트된 평가 상태를 보려면 페이지를 새로 고쳐야 합니다. 평가가 완료되면 사용자는 해당 평가에 대한 모든 관련 탭을 볼 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약성 평가 작업 공간 - 평가 탭



다음 위젯에 대한 평가 상세 정보가 표시됩니다.

- 구성 항목(호스트/인프라)
- 검사한 애플리케이션
- BOM 구성요소 및 제품 모델
- CI 클래스별 구성 항목(설치 평가)
- 평가 소스별 구성 항목 - 영향을 받는 구성 항목 목록을 표시합니다.

데이터 시각화

이름	유형	설명
구성 항목(호스트/인프라)	단일 점수	VI가 있는 CI 수와 없는 CI 수를 표시합니다. 구성 항목 위젯에는 평가 기록과 연결된 것으로 검색된 CI의 총 수가 표시됩니다. 또한 위젯에는 취약한 항목이 있는 구성 항목과 취약한 항목이 없는 구성 항목이 표시됩니다.
검사한 애플리케이션	카운트	AVIT로 검사한 총 애플리케이션 수입니다. **주:** 기본 및 보조 CVE 모두에 대해 검사한 애플리케이션 수를 볼 수 있습니다.
BOM 구성요소 및 제품 모델	단일 점수	총 구성요소 수, 제품 모델 수, 애플리케이션 취약한 항목 포함, 애플리케이션 취약한 항목 수 제외.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이름	유형	설명
평가 소스별 구성 항목	누적 가로 막대형	평가 소스에 의해 누적된 영향을 받는 구성 항목입니다.
CI 클래스별 구성 항목 (설치 평가)	원형 차트	CI 클래스별로 누적된 구성 항목입니다.

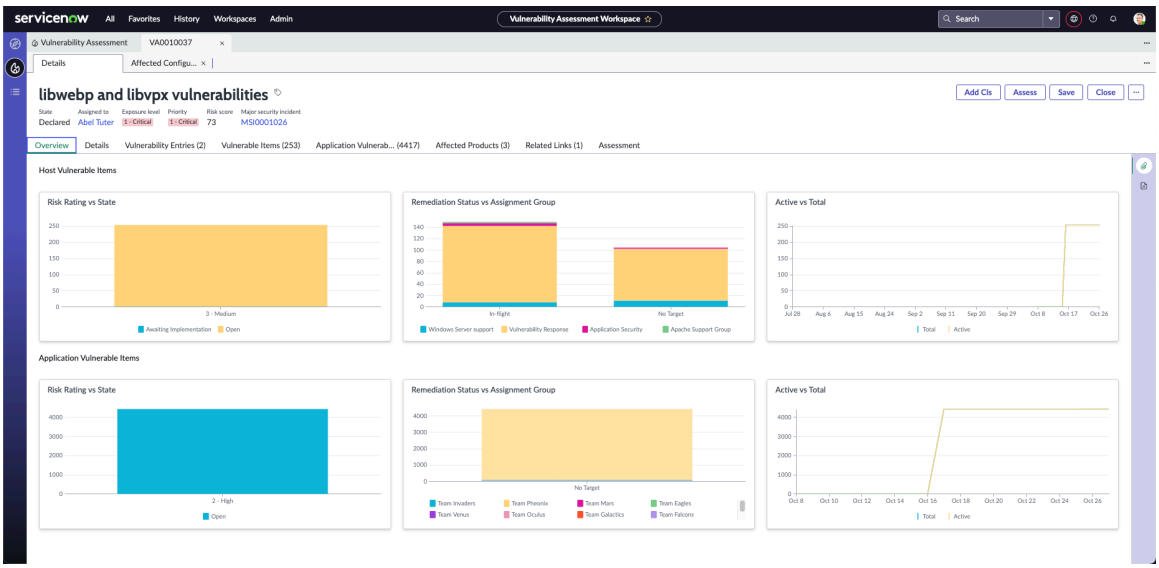
개요 탭

개요 탭에 평가 상세 정보의 개요가 표시됩니다. 초기 평가를 수행한 후에는 기록이 기존 소프트웨어 자재 명세서소프트웨어 자산 관리 데이터와 상호 연관되고 시각화와 함께 표시됩니다.

개요 탭

개요 탭은 생성한 평가 기록에 따라 데이터(사용 가능한 경우)를 채우고 CMDB의 소프트웨어 자산 관리 평가 및 소프트웨어 자재 명세서 데이터와 상세 정보의 상관 관계를 지정합니다. 는

취약성 평가-개요 탭



다음 위젯에 대한 평가 상세 정보가 표시됩니다.

- 호스트 취약 항목(호스트/인프라)
  - 위험 등급 대 상태
  - 정정 상태 대 담당 그룹
  - 활성 대 총
- 애플리케이션 취약한 항목
  - 위험 등급 대 상태
  - 정정 상태 대 담당 그룹
  - 활성 대 총

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

데이터 시각화

호스트 취약한 항목

이름	유형	설명
위험 등급 대 상태	누적 가로 막대형	위험 등급별로 누적된 취약한 항목의 상태입니다.
정정 상태 대 담당 그룹	누적 가로 막대형	할당 그룹별로 누적된 취약한 항목의 정정 상태입니다.
활성 대 총	목록 및 라인	이 항목과 연결된 총 취약한 항목 대 활성 취약한 항목입니다.

애플리케이션 취약한 항목

이름	유형	설명
위험 등급 대 상태	누적 가로 막대형	위험 등급에 따라 누적된 애플리케이션 취약한 항목의 상태입니다.
정정 상태 대 담당 그룹	누적 가로 막대형	할당 그룹별로 누적된 애플리케이션 취약한 항목의 정정 상태입니다.
활성 대 총	목록 및 라인	이 항목과 연결된 총 애플리케이션 취약한 항목 대 활성 취약한 항목입니다.

취약성 평가 기록에 우선순위 및 노출 수준 할당

취약성 평가 기록에 우선순위 및 노출 수준을 수동으로 할당합니다.

시작하기 전에
필요한 역할: sn_vul_analyst.vul_event_manager

프로시저

1. 다음으로 이동 작업 공간 〉 취약성 평가 작업 공간.
2. 취약성 평가 기록을 선택합니다.
3. 상세 정보 탭에서 위험 속성으로 이동합니다.
4. 옵션 목록에서 우선순위 를 선택합니다.
5. 옵션 목록에서 노출 수준을 선택합니다.
6. 저장을 선택합니다.

평가 기록에 영향을 받는 CI 추가

취약성 평가 기록과 연결해야 하지만 초기 평가 후 영향을 받는 CI에 표시되지 않는 조직 내 CI를 수동으로 추가합니다.

시작하기 전에
필요한 역할: sn_vul_analyst.vul_event_manager

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보

영향을 받았을 수 있지만 평가가 완료된 후 나타나지 않는 CI를 추가합니다. 평가 기록이 선언됨 또는 보류 중인 평가 상태인 경우에만 CI를 추가할 수 있습니다.

프로시저

1. 다음으로 이동 작업 공간 〉 취약성 평가 작업 공간.
2. 목록에서 필요한 평가 기록을 선택합니다.
3. **CI** 추가를 선택합니다.
4. 구성 항목 대화 상자에서 구성 항목을 선택합니다.
5. **CI** 추가를 선택합니다.
   Vulnerability Response - 이벤트에 구성 항목 추가 백그라운드 작업이 시작되고 관련 알림이 표시됩니다.
6. 알림에서 상태 보기를 선택하여 실행 중인 작업의 상태를 봅니다.

결과

소스가 #### 설정된 영향을 받는 구성 항목 테이블에 기록이 추가됩니다.

다음에 수행할 작업

평가 탭으로 이동하고 구성 항목(호스트/인프라) 위젯을 새로 고쳐 추가한 CI를 확인합니다.

영향을 받는 **CI** 또는 영향을 받는 소프트웨어 구성요소에 대한 취약한 항목 생성

취약성 평가 작업 공간에서 VI(취약한 항목) 또는 AVIT(애플리케이션 취약한 항목)를 생성합니다. 취약성 분석가는 VI 목록을 분석하고 IT 팀이 이러한 취약성을 패치하는 데 도움이 되는 솔루션과 패치를 권장합니다.

취약성 이벤트 관리자는 하나 또는 여러 개 또는 모든 노출 검색 결과를 선택하여 취약성 항목을 만들 수 있어야 합니다.

- AVIT가 연결되지 않은 SBOM 평가 결과에 대한 애플리케이션 취약 항목
- VIT가 연결되지 않은 구성 항목의 취약한 항목
- 취약성 항목에 기본 CVE를 연결합니다.

취약한 항목이 연결되지 않은 구성 항목에 대한 **VI** 생성

취약한 항목 생성 취약성 평가를 통해 식별되었지만 기록과 연결된 VIT가 없는 구성 항목에 대한 VIT.

시작하기 전에

필요한 역할: 관리자

프로시저

1. 다음으로 이동 작업 공간 〉 취약성 평가 작업 공간 〉 평가.
2. VIT를 생성해야 하는 평가 기록을 선택합니다.
3. 평가 탭을 선택합니다.
4. 구성 항목(호스트 인프라) 위젯에서 구성 항목 수 제외를 선택합니다.
5. 영향을 받는 구성 항목 목록에서 VIT를 생성할 구성 항목을 선택합니다.
6. 취약한 항목 생성을 선택합니다.
   Vulnerability Response - 수동 VIT 생성 취약성 평가 백그라운드 작업이 시작되고 관련 알림이 표시됩니다.
7. 알림에서 상태 보기를 선택하여 실행 중인 작업의 상태를 봅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

선택한 영향을 받는 구성 항목에 해당하는 취약한 항목이 생성됩니다.

이제 구성 항목(호스트 인프라) 위젯에 취약한 항목 포함 개수에 동일한 CI가 표시됩니다.

연결된 애플리케이션 취약 항목이 없는 영향을 받는 제품, 모델 또는 구성요소에 대한 애플리케이션 취약 항목**(AVIT)** 생성

영향을 받는 제품 또는 구성요소에 대한 애플리케이션 취약 항목(AVIT)을 생성합니다. 취약성 평가를 통해 식별되었지만 기록과 연결된 AVIT가 없는 항목입니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 작업 공간 〉 취약성 평가 작업 공간 〉 평가.
2. VIT를 생성해야 하는 평가 기록을 선택합니다.
3. 평가 탭을 선택합니다.
4. **BOM** 구성요소 및 제품 모델 위젯에서 애플리케이션 취약 항목 수 제외를 선택합니다.
5. 영향을 받는 제품 모델 목록에서 AVIT를 생성할 영향을 받는 제품 모델을 선택합니다.
6. 애플리케이션 취약한 항목 생성을 선택합니다.
   Vulnerability Response - 수동 VIT 생성 취약성 평가 백그라운드 작업이 시작되고 관련 알림이 표시됩니다.
7. 알림에서 상태 보기를 선택하여 실행 중인 작업의 상태를 봅니다.
   영향을 받는 제품 모델에 대한 애플리케이션 취약한 항목이 선택한 항목이 생성됩니다. 기록과 연결된 기본 CVE의 경우.

   이제 **BOM** 구성요소 및 제품 모델 위젯에 애플리케이션 취약한 항목 포함 개수에 동일한 제품 모델 또는 구성요소가 표시됩니다.

의 중요 보안 인시던트에 취약성 평가 기록 연결 중요 보안 인시던트 관리

애플리케이션에 대한 액세스 중요 보안 인시던트 관리 권한이 있는 경우 중요 보안 인시던트 평가 기록을 연결, 제안 또는 승격할 수 있습니다.

시작하기 전에
필요한 역할: sn_vul_analyst.vul_event_manager, sn_si.analyst, sn_msi.workspace_admin

이 태스크 정보
평가 기록을 기존의 중요 보안 인시던트와 연결되도록 이동하거나, 평가 기록에서 새 MSI를 생성하거나, 취약성 평가 기록을 중요 보안 인시던트로 승격할 수 있습니다. 및 Microsoft SharePoint와의 통합과 같은 기능을 활용 중요 보안 인시던트 관리 합니다Microsoft Teams.

취약성 관리자 작업 공간에서 취약한 항목에 대한 주요 보안 인시던트에 대한 링크를 볼 수도 있습니다. 이 MSIM 링크는 취약성 항목 및 의 다른 작업 공간에 취약성 대응표시될 취약한 평가에 연결됩니다.

프로시저

1. 다음으로 이동 작업 공간 〉 취약성 평가 작업 공간.
2. 중요 보안 인시던트에 연결할 평가 기록을 선택합니다.
3. 세부 정보 탭에서 추가 작업 아이콘을 선택합니다.
4. 다음 중 하나를 선택하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵션	설명
중요 보안 인시던트에 연결	중요 보안 인시던트 목록에서 기존 MSI 기록을 선택합니다. 취약성 평가 기록은 기존 중요 보안 인시던트에 연결됩니다.
중요 보안 인시던트로 제안	다음 상세 정보를 입력하고 제안을 선택합니다. ○ 탐지 날짜 ○ 근거 ○ 잠재적 영향
중요 보안 인시던트로 승격	다음 상세 정보를 입력하고 승격을 선택합니다. ○ 탐지 날짜 ○ 예상 해결 날짜 ○ 근거 ○ 잠재적 영향

5. 저장을 선택합니다.

다음에 수행할 작업
MSI 기록을 선택하여 뷰에서 중요 보안 인시던트 관리 기록을 엽니다.

관련 정보

중요 보안 인시던트에 연결

다음으로 제안 중요 보안 인시던트로 승격 중요 보안 인시던트

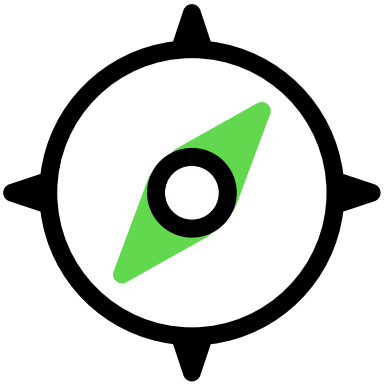
소프트웨어 자재 명세서

애플리케이션 개발에 사용 중인 오픈 소스 및 타사 소프트웨어 구성요소 목록을 봅니다. 인스턴스에 업로드하는 (SBOM) 파일의 소프트웨어 라이센스, 버전 정보 및 구성요소 소프트웨어 자재 명세서 의 알려진 취약성에 대한 인사이트를 얻습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

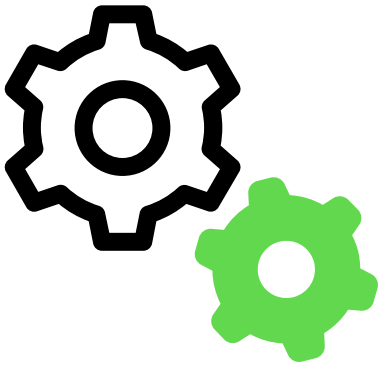
시작하기

탐색



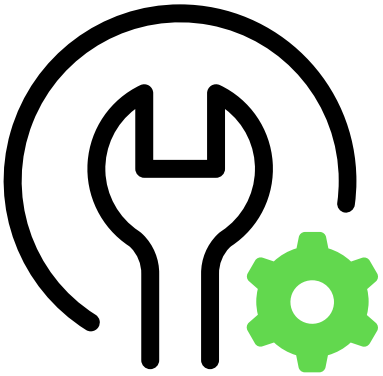
개념과 기능에 대해 SBOM 알아봅니다.

구성



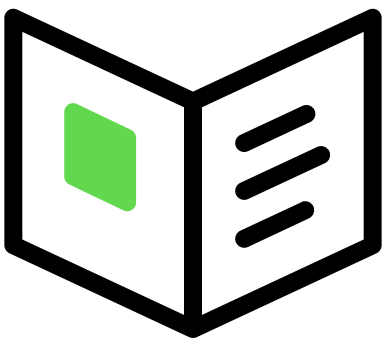
애플리케이션을 구성합니다 SBOM .

사용



작업 공간에서 구성요소를 가져오고 SBOM 데이터를 보는 방법을 알아봅니다.

참조



양식, 필드, 테이블 및 속성에 대한 SBOM 상세 정보를 얻습니다.

문제 해결 및 도움 받기

- Security Operations 커뮤니티
- CycloneDX - 소프트웨어 자재 명세서(SBOM).
- SPDX 입니다.
- 알려진 오류 포털에서 알려진 오류 문서 검색.
- 연락처 고객 서비스 및 지원.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

소프트웨어 자재 명세서 탐색

인스턴스에 업로드하는 (SBOM) 파일에서 조직의 애플리케이션에 소프트웨어 자재 명세서 사용되는 구성요소를 식별합니다. 오픈 소스 소프트웨어 사용과 관련된 위험을 파악하여 잠재적 노출을 확인하고, 라이센스 준수를 확인하고, 취약성을 수정합니다.

소프트웨어 자재 명세서 개요

타사 및 오픈 소스 구성요소는 소프트웨어 프로젝트를 신속하게 작성하고 릴리스할 수 있도록 여러 가지 이점을 제공합니다. 그러나 다음과 같이 공개적으로 액세스할 수 있는 구성 요소를 사용하는 것과 관련된 위험이 있는 경우도 있습니다.

- 구성요소 무결성에 대한 가시성 부족
- 오픈 소스 소프트웨어의 취약성
- 오픈 소스 소프트웨어용 패키지 인텔리전스
- 규정 미준수 소프트웨어 라이센스

API를 통해 또는 수동으로 소프트웨어 BOM 파일을 업로드할 수 있습니다. 엔터티로 임포트한 파일을 봅니다. 이 파일은 소프트웨어에서 사용되는 타사 구성요소 라이브러리의 인벤토리이며 여기에는 전이적 종속성 및 사용 가능한 라이선싱 정보가 포함됩니다.

CycloneDX 및 SPDX SBOM의 소프트웨어 인벤토리에 포함된 내용에 대한 자세한 내용은 CycloneDX - 소프트웨어 자재 명세서(SBOM) 및 SPDX 를 참조하세요.

소프트웨어 자재 명세서 사용자

사용자

사용자	설명
취약성 관리자 및 분석가	업로드된 소프트웨어 자재 명세서 파일을 기록, 데이터 시각화, (SBOM) 작업 공간에서 향상된 취약성 인텔리전스로 볼 수 있습니다 소프트웨어 자재 명세서 . 취약성 관리자와 분석가는 이 정보를 사용하여 소프트웨어 라이선싱 준수 및 오픈 소스 소프트웨어 사용으로 인한 잠재적 위험 노출을 확인하는 데 도움을 줍니다.
다음을 포함할 수 있지만 이에 국한되지 않는 사용자: • 기술 또는 소프트웨어 변호사 • IT 관리자 • 감사자 • 소프트웨어 자산 관리자 및 팀	업로드된 SBOM 파일의 구성요소에 대해 업로드된 독점 및 오픈 소스 소프트웨어 라이센스를 봅니다. 구성요소에 대한 독점 및 오픈 소스 소프트웨어 라이센스의 데이터베이스를 구축합니다. 내부 또는 규제 정책에 따라 누락된 정보가 있는 라이센스를 검토하고 분류합니다. 구성요소를 라이센스와 매칭하고 전반적인 라이센스 준수를 파악하여 금지, 제한 또는 누락된 라이센스에 대한 잠재적 위험 노출을 확인합니다.

소프트웨어 자재 명세서 워크플로우

SBOM 애플리케이션을 사용하면 소프트웨어 자재 명세서(SBOM) 작업 공간에서 엔터티, 구성 요소 인벤토리, 취약성 및 소프트웨어 라이선스 정보에 대한 파일을 업로드하고 세부 정보를 볼 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- API를 사용하거나 수동으로 파일을 업로드합니다 SBOM .
- 작업 공간에서 업로드한 파일의 구성요소 SBOM 를 SBOM 검토합니다.
- 업로드된 SBOM 파일에서 구성요소 라이센스 정보를 검토하고 분류하여 제한되거나 금지된 라이센스에 대한 노출을 식별하는 데 도움이 됩니다.
- 위험 노출을 평가하고 연관된 취약성이 있는 구성요소에 대한 취약한 항목을 생성합니다.
- 작업 공간의 홈페이지에서 보고서와 대시보드뿐 아니라 업로드된 SBOM 구성요소에 대한 전반적인 라이센스 준수도 볼 수 SBOM 있습니다.

소프트웨어 자재 명세서 이점

다음과 같은 세 가지 소프트웨어 자재 명세서 애플리케이션을 사용하여 소프트웨어 구성요소 및 관련 위험의 정확한 인벤토리를 볼 수 있습니다.

- 에 대한 데이터 모델 SBOM
- SBOM Core
- SBOM 응답

호환성 정보는 KB0856498 취약성 대응 호환성 매트릭스 및 릴리스 스키마 변경을 참조하십시오.

SBOM 이점

혜택	애플리케이션	지원되는 버전
이 애플리케이션은 데이터를 저장하는 SBOM 데 사용되는 테이블을 제공합니다. 이 애플리케이션은 필수입니다. 여기에는 데이터를 읽는 SBOM 데 필요한 테이블, ACL 및 역할이 포함됩니다.	에 대한 데이터 모델 SBOM	v4.0, v3.0, v2.0
이 애플리케이션은 필수입니다. 여기에는 문서를 업로드 SBOM 하는 데 필요한 API와 해당 문서의 데이터를 구문 분석하고 인스턴스로 임포트하는 데 필요한 비즈니스 논리가 포함됩니다. 작업 공간에서 소프트웨어 구성요소의 인벤토리를 볼 수 SBOM 있지만 방문 페이지에서 데이터 시각화를 볼 수는 없습니다. CycloneDX 및 SPDX 표준으로 소프트웨어 BOM 파일을 업로드, 구문 분석 및 처리합니다. 이러한 제품에 지원되는 파일 형식 및 버전에 대해서는 지원되는 버전 열을 참조하십시오. BOM(자재 명세서) 엔터티 및 소프트웨어 구성요소의 인벤토리를 봅니다. BOM 엔터티는 SBOM 파일의 루트 수준 구성요소입니다. 예를 들어 메타데이터에 CycloneDX SBOM나열된 구성 요소는 BOM 엔터티로 간주됩니다.	SBOM Core	v6.0, v5.0, v4.0 버전 4.0 SBOM 부터 Core는 다음을 지원합니다. • CycloneDX의 XML 및 JSON 버전 1.0에서 1.6까지. • SPDX의 JSON 버전 2.2에서 2.3까지.
• SBOMSBOM 작업 공간의 방문 페이지에서 기능 및 데이터 시각화에 액세스하려면 응답이 필요합니다. • SBOM 응답하려면 취약성 대응 애플리케이션이 필요합니다.	SBOM 응답	v6.0, v5.0, v4.0

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

SBOM 이점

혜택	애플리케이션	지원되는 버전
• 구성요소 인벤토리를 보고 작업 공간에서의 위험 노출을 SBOM 평가합니다. 애플리케이션 취약 항목(AVIT)을 자동으로 생성하고 워크플로우를 애플리케이션 취약성 대응 통해 정정하는 규칙을 설정합니다. • 라이센스 관리 모듈에서 파일과 함께 SBOM 업로드되는 구성요소 라이센스 정보를 봅니다. 파일에 업로드 애플리케이션 취약성 대응 하는 구성요소를 분류하고 해결(일치)하여 전반적인 라이센스 준수 상태를 확인할 수 있습니다. • 응답 버전 4.0 애플리케이션 취약성 대응 부터 작업 공간에서 사용할 수 있는 PaCE(Policy as Code Engine) 인터페이스에서 부실하거나 '미준수'로 중단된 구성요소를 SBOM 볼 수 있습니다. • OSV.dev 및 Deps.dev 통합은 Response를 설치할 SBOM 때 포함됩니다. ○ OSV.dev 는 패키지 또는 라이브러리의 특정 버전에 대한 취약성 인텔리전스 정보를 제공하는 오픈 소스 API입니다. ○ Deps.dev 는 지정된 패키지 또는 라이브러리에 대한 버전 목록을 제공하고 부실 및 중단됨 상태에 있는 구성 요소를 식별하는 오픈 소스 API입니다. 자세한 내용은 용 Deps.dev, OSV.dev 및 PaCE 통합 구성 소프트웨어 자재 명세서 문서를 참조하십시오. PaCE 및 PaCE 정책에 대한 자세한 내용은 을 참조하십시오 Integrating PaCE with other applications .		
지속적 통합과 지속적 배포 개발 주기 동안 소프트웨어에 대한 파일을SBOM 생성하고 (소프트웨어 자재 명세서)합니다.	SBOM 응답	• 데이터 SBOM모델 : v1.4 이상. • SBOM Core: v3.0 이상. • SBOM 응답: v4.0 이상.

취약성 대응 애플리케이션 및 **CSDM** 테이블

, 취약성 대응애플리케이션 취약성 대응, 타사 취약성 통합 및 소프트웨어 자재 명세서 애플리케이션은 테이블을 관리(데이터 기여) CSDM 합니다. 이러한 애플리케이션은 다른

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

애플리케이션이 생성하는 테이블의 데이터 CSDM 도 사용합니다. 따라서 여러 ServiceNow 제품이 이러한 보안 운영 애플리케이션의 이점을 누리고 가치를 더합니다. 자세한 내용은 취약성 대응 애플리케이션 및 CSDM 테이블 문서를 참조하십시오.

다음으로 살펴볼 내용

소프트웨어 자재 명세서 구성 및 사용에 대한 자세한 내용은 다음을 참조하십시오.

- 에 대해 지원되는 애플리케이션 탐색 소프트웨어 자재 명세서
- 소프트웨어 자재 명세서 구성
- 작업 공간에서 파일 SBOM 업로드 및 보기 SBOM
- 작업 공간에서 보고서 및 대시보드 소프트웨어 자재 명세서 보기

에 대해 지원되는 애플리케이션 탐색 소프트웨어 자재 명세서

타사 취약성 인텔리전스 및 애플리케이션과의 소프트웨어 자재 명세서 기타 통합을 통해 업로드된 파일의 데이터를 향상시킬 수 있습니다.

지원되는 애플리케이션의 이점

타사 취약성 인텔리전스 및 애플리케이션과의 소프트웨어 자재 명세서 기타 통합을 통해 부실 및 중단된 것으로 간주되는 구성요소의 개수와 구성요소와 연관된 취약성을 수정할 수 있는지에 대한 정보를 볼 수 있습니다.

ServiceNow# 다음 테이블에 나열된 애플리케이션 및 외부 공급업체 통합은 애플리케이션에서 지원됩니다SBOM. 이러한 애플리케이션은 SBOM 파일과 관련된 취약성을 보고 우선순위를 지정하는 데 도움이 될 수 있는 풍부한 취약성 데이터, 취약성 인텔리전스 및 기타 주요 정보를 제공합니다. 이러한 모든 애플리케이션 및 통합은 에서 사용할 수 있습니다 ServiceNow# Store.

지원되는 애플리케이션 및 외부 공급업체 통합

혜택	애플리케이션	지원되는 버전	사용자
취약성 대응 응답 애플리케이션을 설치하는 SBOM 경우 필요합니다. 취약성 대응 SBOM 응답을 설치하기 전에 애플리케이션을 설치합니다. 애플리케이션 취약성 대응 기능은 와 함께 취약성 대응설치됩니다. 이러한 기능을 사용하면 애플리케이션의 취약성 관리자 작업 공간과 취약성 대응 취약성 워크플로우에 액세스하여 AVIT(애플리케이션 취약한	취약성 대응	호환성 정보는 KB0856498 취약성 대응 호환성 매트릭스 및 릴리스 스키마 변경을 참조하십시오.	

기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

지원되는 애플리케이션 및 외부 공급업체 통합

혜택	애플리케이션	지원되는 버전	사용자
항목)를 정정할 수 있습니다.			
향상된 NVD 취약성 및 심각도 데이터를 봅니다. NVD 및 CWE 통합에서 임포트한 데이터를 보고 SBOM 데이터에서 찾을 수 있는 취약성 데이터를 보강합니다. 자세한 내용은 NVD 및 CWE 통합을 통해 데이터를 임포트하고 외부 공급업체 라이브러리를 관리합니다 문서를 참조하십시오.	NVD 및 SBOM Response와의 취약성 대응 통합	호환성 정보는 KB0856498 취약성 대응 호환성 매트릭스 및 릴리스 스키마 변경을 참조하십시오.	
를 사용하여 Veracode Vulnerability Integration자재 명세서 파일을 가져옵니다. 여기에는 Veracode Vulnerability Integration SBOM 파일에 대한 다음과 같은 Veracode 개선 사항이 포함됩니다. • Response를 설치한 SBOM 경우 업로드하는 파일에 대해 SBOM 발견 SBOM 된 취약점을 포함할 수 있는 옵션이 있습니다. • SBOM 이(가) 업로드하는 파일의 자재 명세서 [sn_sbom_doc] 테이블에 SBOM SBOM 있는 기록의 소스 필드에 매핑됩니다. 자세한 내용은 Veracode Vulnerability Integration 문서를 참조하십시오.	Veracode 취약성 통합 및 SBOM Response	버전 4.3 Veracode Vulnerability Integration부터 . Veracode Vulnerability Integration 이미 설치되어 있는 경우 Core 버전 v3.0 SBOM 부터 CycloneDX(JSON 및 XML) 및 SPDX(XML) 형식으로 가져온 Veracode SBOM 데이터를 업로드할 수도 있습니다. 호환성 정보는 KB0856498 취약성 대응 호환성 매트릭스 및 릴리스 스키마 변경을 참조하십시오.	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

지원되는 애플리케이션 및 외부 공급업체 통합

혜택	애플리케이션	지원되는 버전	사용자
GitHub 리포지토리에서 로 파일을 ServiceNow AI Platform 업로드합니다SBOM. CI/CD(지속적 통합 및 지속적 제공/배포) 파이프라인에서 생성된 파일이 인스턴스에서 성공적으로 큐에 대기 ServiceNow AI Platform 했는지 확인합니다SBOM. GitHub 환경에서 시작하는 GitHub Actions를 사용하여 소프트웨어 개발 주기 동안 잠재적으로 유해한 구성 요소로부터 환경을 보호합니다.	GitHub Marketplace에서 업로드하는 데 SBOM 필요한 GitHub Actions를 가져옵니다.	Core 버전 4.0 SBOM 부터.	

소프트웨어 자재 명세서 구성

파일을 업로드 SBOM 하기 전에 ()SBOM 애플리케이션에 필요한 소프트웨어 자재 명세서 애플리케이션을 다운로드하고 활성화하십시오.

구성 개요

1. ServiceNow Store에서 원하는 SBOM 필수 애플리케이션과 지원되는 추가 애플리케이션 및 통합을 ServiceNow 인스턴스로 다운로드합니다. 지원되는 애플리케이션에 대한 자세한 내용은 을 에서 처음으로 애플리케이션 ServiceNow Store 다운로드 참조하십시오소프트웨어 자재 명세서 탐색.

   Response에는 SBOM 취약성 대응 애플리케이션이 필요합니다. Response를 설치하기 SBOM 전에 취약성 대응 애플리케이션을 설치하십시오.

2. 다운로드한 SBOM 애플리케이션을 찾아 설치를 선택하여 다음 순서로 종속성과 함께 활성화합니다. 에 대해 지원되는 애플리케이션 설치 소프트웨어 자재 명세서 문서를 참조하십시오.

   - Vulnerability Response 및 해당 종속성
   - NVD와 취약성 대응 통합
   - 에 대한 데이터 모델 SBOM
   - SBOM Core
   - SBOM 응답: SBOM 작업 공간의 OSV.dev 및 Deps.dev 통합과 Policy as Code Engine(PaCE) 기능에 대한 액세스가 포함됩니다.

3. Deps.dev 및 OSV.dev 통합을 구성합니다. 이러한 통합은 Response 애플리케이션에 포함되어 SBOM 있으며 자동으로 설치 및 활성화됩니다. 통합 기록에서 OSV.dev 통합 - 포괄적인 요청

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시를 시작해야 합니다. 자세한 내용은 AND 소프트웨어 자재 명세서 탐색 문서를 참조하십시오용 Deps.dev, OSV.dev 및 PaCE 통합 구성 소프트웨어 자재 명세서.

Deps.dev 통합은 파일에 업로드 SBOM 하는 패키지 또는 라이브러리의 지정된 버전에 대해 부실 및 중단됨 상태에 있는 구성요소에 대한 정보를 제공합니다.

OSV.dev 는 오픈 소스 데이터베이스에서 파일에 업로드 SBOM 하는 패키지 또는 라이브러리 버전에 대한 취약성 데이터를 가져옵니다.

4. 제품 설명서를 참조하여 사용자가 설치한 추가 지원되는 애플리케이션 및 통합을 구성하십시오. 취약성 대응 통합 및 다른 애플리케이션과 애플리케이션 취약성 대응의 통합 문서를 참조하십시오.

에 대해 지원되는 애플리케이션 설치 소프트웨어 자재 명세서

파일을 업로드하기 전에 ()SBOM 애플리케이션에 필요한 소프트웨어 자재 명세서 애플리케이션을 다운로드하고 활성화하십시오.

시작하기 전에
필요한 역할: admin 인스턴스에서 모든 애플리케이션과 역할 할당을 다운로드, 설치 및 활성화합니다.

이 태스크 정보

프로시저

1. 필요한 SBOM 애플리케이션을 ServiceNow Store 인스턴스에서 인스턴스 ServiceNow 로 다운로드합니다.

   이러한 애플리케이션을 사용하여 인스턴스에 파일을 업로드하고 임포트 SBOM 할 수 있습니다. Core가 설치된 경우 SBOM 작업 공간에서 BOM 엔터티 및 구성요소 데이터를 SBOM 볼 수 있습니다.

   Response가 설치된 경우 SBOM 작업 공간에서 BOM 엔터티, 구성요소 데이터 및 데이터 시각화를 SBOM 볼 수 있습니다.

   - 에 대한 데이터 모델 SBOM
   - SBOM Core

   애플리케이션 다운로드 및 활성화에 대한 자세한 내용은 다음을 참조하십시오.

   - Install a ServiceNow Store application
   - Install an update to a ServiceNow Store application

2. 옵션: 작업 공간에서 데이터를 보고SBOM, 임포트한 외부 공급업체 취약성 인텔리전스를 SBOM 보고, 위험 노출을 평가하고, 및 취약성 대응 워크플로우를 사용하여 애플리케이션 취약성 대응 취약성을 정정하려면 다음 애플리케이션을 다운로드합니다.

   - 취약성 대응 및 의존성
   - NVD와 취약성 대응 통합
   - SBOM 응답

   이러한 애플리케이션 및 지원되는 SBOM 다른 애플리케이션에 대한 자세한 내용은 다음 문서를 참조하십시오 소프트웨어 자재 명세서 탐색.

3. 애플리케이션을 다운로드한 후 모두 〉 시스템 애플리케이션 〉 모든 사용 가능 애플리케이션 〉 모두.
4. 다운로드한 애플리케이션을 찾아 SBOM설치를 선택하여 해당 종속성과 함께 활성화합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

애플리케이션이 성공적으로 활성화되면 메시지가 표시됩니다. 다음 순서로 애플리케이션을 활성화합니다.

- 취약성 대응 및 의존성
- NVD와 취약성 대응 통합
- 에 대한 데이터 모델 SBOM
- SBOM Core
- SBOM 응답: OSV.dev 및 Deps.dev 통합을 포함하고 작업 공간에서 PaCE(Policy as Code Engine) 인터페이스를 SBOM 지원합니다.

응답을 설치한 SBOM 후 이러한 통합 애플리케이션을 구성하는 방법에 대한 자세한 내용은 을 참조하십시오용 Deps.dev, OSV.dev 및 PaCE 통합 구성 소프트웨어 자재 명세서.

5. 옵션: 로 이동하여 통합 활성화 모두 〉 시스템 애플리케이션 〉 모든 사용 가능 애플리케이션 〉 모두을 클릭하고 설치를 선택합니다.

   (Optional) 이러한 통합 및 통합에서 제공하는 역량에 대한 자세한 내용은 다음 문서를 참조하십시오 소프트웨어 자재 명세서 탐색.

   - Veracode와의 취약성 대응 통합. 자세한 내용은 ServiceNow 와 Vulnerability Response 통합 설치Veracode 문서를 참조하십시오.
   - NVD와의 취약성 대응 통합으로, 업로드된 구성요소와 관련된 취약성에 대한 향상된 데이터를 보려면 필요합니다. 자세한 내용은 NVD 통합 이해 문서를 참조하십시오.
   - CWE Comprehensive 2000 통합. 이 예약된 작업 활성화에 대한 자세한 내용은 을 참조하십시오 CWE 기록을 업데이트하기 위해 예약된 작업을 구성하고 실행합니다. .

   애플리케이션이 성공적으로 활성화되면 메시지가 표시됩니다.

6. 사용자에게 다음 역할을 할당합니다.
   - sn_sbom_dm.app_create
   - sn_sbom_dm.app_read
   - sn_sbom_dm.app_write
   - sn_sbom_core.sbom_ingest
   - sn_sbom_core.admin
   - sn_sbom_resp.sbom_analyst
   - sn_sbom_resp.manage_avi_rule
   - sn_sbom_response.managelicense
   - sn_sbom_response.licenseresolver
7. 옵션: 임포트 SBOM 한 데이터의 취약성에 대한 애플리케이션 취약한 항목을 생성하는 경우 사용자를 App-Sec 관리자 그룹에 할당합니다.

   (Optional) App-Sec 관리자 그룹에 할당된 사용자는 애플리케이션 취약한 항목의 우선순위를 지정하고 관리합니다. 이 그룹의 사용자는 기록을 읽고 편집하며 애플리케이션 및 정정 워크플로우에서 지원하는 애플리케이션을 구성하는 데 필요한 많은 역할을 상속받습니다 애플리케이션 취약성 대응 .

8. 옵션: 종결된 AVIT가 자동으로 오픈 상태로 다시 전환되는 것을 원하지 않으면 탐지된 경우 AVIT 다시 열기(*sn_sbom_resp.reopen_avits_if_detected*) 시스템 속성을 비활성화합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

(Optional) 다음과 같은 조건이 존재하면 관련된 취약성이 있는 구성요소에 대해 종결된 AVIT(애플리케이션 취약한 항목)가 자동으로 다시 열리고(오픈으로 설정) SBOM 작업 공간에 표시됩니다.

- 연관된 취약성이 있는 AVIT가 외부 공급업체 통합의 취약성 검사에 의해 다시 탐지되거나 취약성이 있는 구성요소가 후속 SBOM 업로드의 일부입니다.
- 탐지된 경우 AVIT 다시 열기 (*sn_sbom_resp.reopen_avits_if_detected*) 시스템 속성을 비활성화하지 않았습니다. 이 시스템 속성은 기본적으로 활성화되어 있습니다.
- 종결된 AVIT의 하위 상태가 완화 통제가 있음, 영향을 받지 않음 또는 가양성 중 하나가 아닙니다. 이러한 하위 상태가 있는 AVIT는 시스템 속성에 의해 다시 열리지 않습니다.

다음에 수행할 작업
SBOM 파일을 업로드합니다. 자세한 내용은 AND REST API를 사용하여 파일 업로드 소프트웨어 자재 명세서 문서를 참조하십시오수동으로 파일 업로드 소프트웨어 자재 명세서.

용 **Deps.dev, OSV.dev** 및 **PaCE** 통합 구성 소프트웨어 자재 명세서

Deps.dev 및 OSV.dev 통합에 대한 일부 매개변수를 편집할 수 있습니다. 또한 이러한 통합에는 내부 워크플로우에만 사용되는 두 가지 코드 트리거 버전이 있으며 이러한 통합을 요청 시 시작하면 안 됩니다. 또한 예약된 작업을 활성화하여 Policy as Code Engine(PaCE)을 사용하여 정책을 생성할 수 있습니다.

내부 워크플로우에 대한 코드 트리거 통합

응답 v3.2 SBOM 부터 두 가지 OSV.dev 및 Deps.dev 코드 트리거 통합이 추가되어 성능이 향상되었습니다.

- OSV 통합(요청 시 코드 트리거)
- Deps.dev 통합(요청 시 코드 트리거)

이러한 통합은 내부 워크플로우에 의해 자동으로 시작되며 내부용으로만 사용됩니다. 찾을 수는 있지만 통합 기록에서 지금 실행 버튼을 사용하여 요청 시 이러한 통합을 시작해서는 안 됩니다.

Deps.dev 통합의 실행 일정 구성

Deps.dev 통합 은 응답과 함께 SBOM 설치됩니다. 통합은 기본적으로 활성화되고(통합 기록에서 활성 확인란 선택됨) 매주 실행되도록 예약됩니다. 이는 온디맨드 Deps.dev 코드 트리거 통합이 아니며, 통합 기록에서 일정을 편집하고 온디맨드 방식으로 예약된 작업을 시작할 수 있습니다. 입니다.

일정을 수정하려면 다음으로 이동하십시오. 모두 〉 취약성 대응 〉 관리 〉 통합 〉 **Deps.dev** 통합. 이 통합의 일정을 편집하려면 sn_vul.app_configure_integrations 역할이 필요합니다.

이 Deps.dev 통합은 부실 및 중단됨 상태에 있는 구성요소를 식별하는 데 사용됩니다. 부실 구성 요소의 버전은 최신 버전보다 두 개 이상의 주요 버전이며 최신 버전보다 2년 뒤처져 있습니다. 버려진 구성 요소가 2년 이상 업데이트되지 않았습니다. 2년 및 2개의 버전 임계치는 시스템 속성으로 편집할 수 있습니다. 이러한 매개변수를 편집하려면 모두 〉 시스템 속성 〉 모든 속성 을 클릭하고 다음 기록을 찾습니다.

- sn_sbom_resp.pkg_abandoned_threshold
- sn_sbom_resp.pkg_stale_threshold
- sn_sbom_resp.pkg_stale_version_threshold

중단됨 및 부실에 대한 임계값은 개월 단위입니다. 버전의 임계값은 숫자입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업공간의 홈 페이지와 BOM 큐 모듈에서 임포트한 데이터를 볼 수 있습니다. 임포트한 데이터는 패키지 그룹 [sn_sbom_pkg_group] 테이블에 저장됩니다.

OSV.dev 통합 구성 및 시작 **-** 포괄적

OSV.dev 통합 - 포괄적 통합이 Response와 함께 SBOM 설치됩니다. 통합은 기본적으로 활성화됩니다(통합 기록에서 활성 확인란 선택됨). 이는 요청 시 OSV.dev 코드 트리거 통합이 아니며 통합 기록에서 요청 시 이 통합을 시작해야 합니다.

이 통합을 구성하고 시작하려면 다음으로 이동하십시오. 모두 〉 취약성 대응 〉 관리 〉 통합 〉 **OSV.dev** 통합 **-** 포괄적. sn_vul.app_configure_integrations 역할이 필요합니다.

임포트한 데이터는 작업 공간의 홈페이지, 취약성 탭, 엔터티 목록의 기록, 라이브러리 모듈에서 볼 수 있습니다. 임포트된 데이터는 애플리케이션 취약 항목 [sn_vul_app_vul_entry] 및 국가 취약성 데이터베이스 항목 [sn_vul_nvd_entry] 테이블에 저장됩니다.

주:
에 있는 오픈 소스 취약성 인스턴스의 통합 매개변수 탭에서 OSV.dev의 *batchSize* 통합 매개변수를 구성할 수 있습니다. 모두 〉 취약성 대응 〉 관리 〉 통합 〉 취약성 통합 〉 오픈 소스 취약성 인스턴스. 기본값은 API 호출당 75 PURL입니다.

이 값을 기본 설정으로 두는 것이 좋습니다. 값을 변경하면 성능에 영향을 줄 수 있습니다.

PaCE 활성화

응답 버전 4.0 SBOM 부터 작업 공간에서 사용할 수 있는 PaCE(Policy as Code Engine) 인터페이스에서 부실하거나 '미준수'로 중단된 구성요소를 SBOM 볼 수 있습니다.

- 구성요소가 부실하거나 예약된 작업으로 중단되었는지 *Run PaCE policies for SBOM Response* 확인합니다. 이 예약된 작업은 기본적으로 비활성화되어 있습니다.
- 작업 공간에서 사용할 수 있고 볼 수 있는 PaCE 인터페이스에서 부실하거나 규정 미준수로 중단된 구성요소를 SBOM 봅니다.

PaCE 및 PaCE 정책에 대한 자세한 내용은 을 참조하십시오 Integrating PaCE with other applications .

작업 공간에서 파일 **SBOM** 업로드 및 보기 **SBOM**

이 SBOM 애플리케이션을 사용하면 파일을 업로드하고 소프트웨어 자재 명세서 작업 공간에서 엔터티, 구성 요소 인벤토리, 라이센스 정보 및 기타 세부 사항에 대한 세부 정보를 볼 수 있습니다.

파일 업로드 **SBOM** 개요

API를 통해 또는 수동으로 소프트웨어 BOM 파일을 업로드할 수 있습니다. 엔터티로 임포트한 파일을 봅니다. 이는 소프트웨어에서 사용되는 외부 공급업체 구성요소 라이브러리의 인벤토리입니다(전이적 종속성 포함).

- REST API를 사용하여 파일 업로드 소프트웨어 자재 명세서.

  업로드 API는 파일(CycloneDX/SPDX)을 SBOM 인스턴스에 업로드하고 수집하는 데 사용됩니다.

- 수동으로 파일 업로드 소프트웨어 자재 명세서.

  소프트웨어 자재 명세서 파일을 수동으로 업로드합니다. 파일을 업로드하는 데 사용하는 방법은 Core 또는 SBOM Response 애플리케이션이 설치되어 있는지 여부에 SBOM 따라 다릅니다.

- DevOps SBOM 파일에 대한 업로드 소프트웨어 자재 명세서.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

지속적인 통합과 지속적인 배포 개발 주기 전반에 걸쳐 소프트웨어에 대한 파일을 생성하고 업로드합니다 SBOM .

- 라이센스 관리 모듈에서 구성요소 라이센스를 분류하고 해결합니다.

  내부 또는 규제 정책에 따라 파일에 업로드 SBOM 하는 구성요소에 대한 라이센스 정보를 검토, 분류 및 해결(할당)합니다. 구성요소를 라이센스와 매칭하고 전체 라이센스 준수를 파악하여 금지, 제한 또는 누락된 라이센스에 대한 잠재적 위험 노출을 확인할 수 있습니다.

- 작업 공간에서 보고서 및 대시보드 소프트웨어 자재 명세서 보기

  취약성 분석가와 관리자는 업로드된 소프트웨어 자재 명세서 파일과 기록, 데이터 시각화, 향상된 취약성 인텔리전스 및 라이센스 정보()SBOM 작업 공간에서 소프트웨어 자재 명세서 중요한 데이터를 볼 수 있습니다.

  > **주:**
  > 작업 공간의 랜딩(홈) 페이지에서 데이터 시각화를 보려면 Response를 설치해야 SBOM 합니다.

REST API를 사용하여 파일 업로드 소프트웨어 자재 명세서

API를 사용하여 파일을 업로드 소프트웨어 자재 명세서 하기 전에 다음 정보를 검토합니다.

REST API 사용

API를 사용하여 SBOM 파일을 업로드하려면 sn_sbom_core.sbom_ingest 역할이 필요합니다.

API를 업로드합니다.

이 API는 SBOM 파일(CycloneDX/SPDX)을 인스턴스에 업로드하고 수집하는 데 사용됩니다.

Core 버전 4.0 SBOM 은 다음을 지원합니다.

- CycloneDx의 XML 및 JSON(버전 1.0~1.6).
- SPDX의 JSON(버전 2.2-2.3)

- > **주:**
  > 32MB를 초과하는 파일은 제대로 로드되지 않을 수 있습니다.

HTTP 메서드: (POST)

API URL: `<host_name>/api/sbom/core/upload`

> **주:**
> ServiceNow 인스턴스 이름은 `<host_name>`입니다.

아래의 모든 요청 매개변수는 선택 사항입니다. 요청 본문은 SBOM 파일 내용입니다. DevOps를 개발 프로세스의 일부로 사용하는 경우 "requestedBy" 값은 "devops"여야 합니다. DevOps에 대한 자세한 내용은 을 참조하십시오 DevOps SBOM 파일에 대한 업로드 소프트웨어 자재 명세서 . 'requestedby' 값이 'devops'(개발 작업)인 경우 다음 매개변수는 필수입니다.

- 빌드 ID
- lifecycleStage

또한 'requestedBy'가 'devops'인 경우 fetchVulenrabilityInfo, fetchPackageInfo에 대한 데이터가 포함됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- buildId- 전송하는 문자열
- lifecycleStage- 두 개의 값, 프로덕션 또는 pre_production
- fetchVulenrabilityInfo- t/f
- fetchPackageInfo-t/f

매개변수 요청	가능한 값	설명
productModelId	시스템 ID	지정된 SBOM의 루트 애플리케이션과 매핑할 제품 모델의 시스템 ID입니다.
비즈니스 애플리케이션 ID	시스템 ID	지정된 SBOM루트 애플리케이션과 매핑할 비즈니스 애플리케이션의 시스템 ID입니다.
businessApplicationName(사용하지 않음)	비즈니스 애플리케이션 이름	지정된 SBOM루트 애플리케이션과 매핑할 비즈니스 애플리케이션의 이름입니다.
sbomSource	예를 들어 다음과 같은 Veracode제품	파일의 소스입니다 SBOM .
requestedBy	도구 또는 방법론 이름 (Jenkins)입니다. "devops"를 사용하는 경우 buildId 및 lifecycleStage 는 필수입니다.	업로드 요청자
빌드 ID	요청자가 문자열 요청자를 보냅니다.	빌드의 빌드 ID입니다 SBOM .
lifecycleStage	생산 또는 pre_production	엔터티의 수명 주기 스테이지입니다.
fetchVulenrabilityInfo	티/에프	true일 경우 취약성 인텔리전스 통합을 트리거합니다.
fetchPackage 정보	티/에프	true이면 패키지 인텔리전스 통합을 트리거합니다.

업로드 API 응답: "상태" 성공/실패, "메시지"(문자열), "bomRecordId"(성공적인 SBOM 업로드를 위해 업로드 API를 통해 반환되는 SBOM의 시스템 ID임)가 포함되었습니다.

```
{

"result": {

"status": "success",

"message": "Queued for processing.",

"bomRecordId": "f207059b4393c290629aa597cbb8f247"

}

}
```


© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

상태 API

이 API는 수집을 위해 큐에 대기 중인 SBOM의 상태 및 요약을 가져옵니다.

- API URL: */api/sbom/core/upload/status*
- HTTP 메서드(GET)

매개변수 요청	가능한 값	설명
bomRecordId	시스템 ID	성공적인 SBOM 업로드를 위해 업로드 API를 통해 반환되는 SBOM 기록 ID입니다.

상태 API 기본 응답 예시.

```
{
  "result": {
    "bomRecordId": "0407c0fea3e70a505df340f5251e617e",
    "uploadStatus": "processed",
    "additionalInfoStatus": "not_requested",
    "uploadSummary": {
      "components": {
        "added": 0,
        "removed": 0,
        "total": 70
      }
    }
  }
}
```

추가 매개변수가 있는 상태 API 응답 예시. 해당 SBOM에 대한 fetchVulenrabilityInfo를 요청한 경우 응답의 일부로 취약성 세부 항목이 표시됩니다.

```
{
 "result": {
  "bomRecordId": "93af349b4393c290629aa597cbb8f258",
  "uploadStatus": "processed",
  "additionalInfoStatus": "complete",
  "uploadSummary": {
   "components": {
    "added": 0,
    "removed": 0,
    "total": 3
   },
  "vulnerabilityInfo": {
```


© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
  "critical": 0,
  "high": 0,
  "medium": 0,
  "low": 0,
  "none": 0
 }
},
"buildId": "1"
}
}
```


해당 SBOM에 대해 fetchPackageInfo를 요청한 경우 응답의 일부로 부실 및 중단된 개수가 표시됩니다.

성공적으로 SBOM 처리된 후 업로드된 기록을 보는 위치는 사용 중인 애플리케이션에 따라 다릅니다.

- 응답을 사용하는 SBOM 경우 작업 공간의 BOM 큐 모듈에 있는 수집 상태 목록에 BOM 엔터티 기록이 표시됩니다 SBOMSBOM .
- SBOM Core를 사용하는 경우 **SBOM Core** 〉 **BOM** 수집 상태.

지원되는 **SBOM** 표준 및 일반 사용 정보에 대한 개선 사항

Core 버전 4.0 SBOM 은 다음을 지원합니다.

- CycloneDx의 XML 및 JSON(버전 1.0~1.6).
- SPDX의 JSON(버전 2.2-2.3)

- **주:**
  32MB를 초과하는 파일은 제대로 로드되지 않을 수 있습니다.

코어 v4.0 SBOM 부터 버전 1.0 - 1.6에 대한 CycloneDx 표준을 지원하기 위해 다음과 같은 개선 사항이 적용되었습니다.

- (sn_sbom_core.collect_properties) 속성을 사용하여 CycloneDX SBOM 파일의 추가 정보를 임포트합니다. 이 속성은 기본적으로 비활성화되어 있습니다. 속성을 활성화하여 일반적으로 지원되지 않는 정보를 임포트합니다. 이러한 속성에서 임포트한 모든 정보는 다음에 대한 SBOM 구성요소 속성 [sn_sbom_comp_property] 테이블로 업로드됩니다.
  - 업로드된 SBOM 파일
  - 메타데이터
  - 개별 취약성
  - 구성 요소
- 두 개의 새 라이선스 필드에서 CycloneDX 버전 1.4 이상에서 SBOM 파일에 대한 선언 및 종료된 라이선스에 대해 임포트된 구성요소 데이터를 봅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 선언함
- 결론

- SBOM 구문 분석 지원은 다음 CycloneDX 구성 요소 유형에 대해 확장됩니다.
  - 버전 1.5: 플랫폼, 데이터, 장치 드라이버, 기계 학습 모델
  - 버전 1.6: 암호화

Core 버전 3.0 SBOM 은 다음을 지원합니다.

- CycloneDx의 XML 및 JSON(버전 1.4까지).
- SPDX의 JSON(v2.3까지).

호출 사용자가 성공적으로 인증되고 인스턴스에서 sn_sbom_core.sbom_ingest 역할을 ServiceNow 가지고 있는 경우 인스턴스 외부에서 API에 액세스하여 데이터를 업로드할 SBOM 수 있습니다.

데이터가 업로드되면 구문 분석됩니다. 데이터를 구문 분석하기 전에 다음 요구 사항을 확인합니다.

- 수신 데이터가 유효한 JSON 또는 XML인지 검사합니다.
- BOM 형식이 지원됩니다. Core v2.1 SBOM 부터 CycloneDX(JSON 및 XML) 및 SPDX(XML) 형식이 지원됩니다.
- 데이터를 구문 분석할 수 있도록 최소 필드를 사용할 수 있습니다.

이러한 검사가 확인되면 수신 SBOM 데이터가 첨부 파일로 포함된 자재 명세서[sn_sbom_doc] 테이블에 항목이 생성됩니다.

`Process BOM file` 비즈니스 규칙은 기록 삽입 및 데이터 구문 분석의 결과로 자동으로 트리거됩니다.

주:
이 비즈니스 규칙은 기본적으로 Core를 SBOM 설치하는 동안 활성화됩니다.

에 SBOM 나열된 모든 구성 요소에는 정의된 ### 있습니다.

- SBOM 파일이 업로드된 구성요소는 BOM 엔터티로 간주됩니다.
- type=library로 나열된 구성요소는 외부 공급업체 구성요소로 간주됩니다.

관련 정보

파일의 업로드 상태 소프트웨어 자재 명세서 보기

작업 공간에서 보고서 및 대시보드 소프트웨어 자재 명세서 보기

수동으로 파일 업로드 소프트웨어 자재 명세서

(SBOM) 파일을 수동으로 업로드합니다 소프트웨어 자재 명세서 .

시작하기 전에
버전 4.0부터 SBOM Core는 다음을 지원합니다.

- CycloneDX 버전 1.0 - 1.6의 XML 및 JSON.
- SPDX 버전 2.2 - 2.3의 JSON.

필요한 역할: sn_sbom_core.sbom_ingest

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 파일을 수동으로 업로드합니다.

   파일을 업로드하는 데 사용하는 방법은 Core 또는 SBOM Response 애플리케이션이 설치되어 있는지 여부에 SBOM 따라 다릅니다.

2. 옵션: 에서 Veracode Vulnerability Integration임포트한 파일을 업로드 SBOM 하십시오.

   주:
   와의 통합을 애플리케이션 취약성 대응설치하고 활성화 Veracode 한 경우에만 CycloneDX(JSON 및 XML) 및 SPDX(XML) 형식의 파일을 업로드할 Veracode 수 있습니다. 자세한 내용은 을 Veracode Vulnerability Integration 참조하십시오.

결과
성공적으로 SBOM 처리된 후 업로드 상태를 보는 위치는 사용 중인 애플리케이션에 따라 달라집니다.

- 응답을 사용하는 SBOM 경우 작업 공간의 BOM 큐 모듈에 있는 수집 상태 목록에 BOM 엔터티 기록이 표시됩니다 SBOMSBOM .
- Core를 사용하는 SBOM 경우 **SBOM Core** 〉 **BOM** 수집 상태.

관련 정보

REST API를 사용하여 파일 업로드 소프트웨어 자재 명세서

DevOps SBOM 파일에 대한 업로드 소프트웨어 자재 명세서

지속적인 통합과 지속적인 배포 개발 주기 전반에 걸쳐 소프트웨어에 대한 파일을 생성하고 업로드합니다 소프트웨어 자재 명세서 SBOM .

DevOps 및 SBOM 파일

SBOM 파일은 소프트웨어 지속적 통합 및 지속적 배포(CI/CD) 개발 수명주기 전반에 걸쳐 여러 스테이지에서 생성될 수 있습니다. 조직의 대부분의 소프트웨어 개발 운영(DevOps)은 릴리스 후 발생할 수 있는 비용이 많이 드는 버그를 식별하고 방지하는 데 도움이 되는 일종의 CI/CD 프로세스를 사용합니다. DevOps는 CI/CD 파이프라인 전반에 걸쳐 SBOM 파일을 생성하고 취약성 및 위험에 처한 구성 요소를 사전에 확인할 수 있습니다. 이러한 검사를 통해 조직은 더 나은 소프트웨어 품질을 달성하고 나중에 비용이 많이 드는 유지 관리를 방지할 수 있습니다. 파일 생성 SBOM 은 CI/CD 개발 중에 정확한 빌드 평가를 성공적으로 구현하고 자동화하는 데 중요합니다.

개발 파이프라인에서 SBOM 파일을 업로드하는 것은 다음 버전의 SBOM 애플리케이션부터 지원됩니다.

지원되는 버전

애플리케이션	지원되는 버전
에 대한 데이터 모델 SBOM	v3.0, v2.0
SBOM Core	v5.0, v4.0, v3.0
SBOM 응답	v5.0, v4.0, v3.2, 3.1

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용 사례

DevOps 빌드 파이프라인의 일부로 파일을 생성하고 SBOM SBOM 업로드 API를 통해 전송하면 파이프라인의 성공 또는 실패 여부를 결정하는 다음 개수를 제공할 수 있습니다.

- 추가된 구성요소
- 제거된 구성요소
- 취약성 정보
- 패키지 정보(중단된/부실 구성 요소)

파이프라인의 성공 또는 실패에 대한 DevOps 정책 및 규칙은 상태 API에서 수신되는 취약성 수와 부실 및 중단된 구성 요소 수 임계값에 SBOM 의해 정의될 수 있습니다.

실패한 파이프라인의 경우 DevOps 사용자는 인스턴스에서 실패한 빌드 ServiceNow# 에 대한 정보에 액세스하여 취약성의 근본 원인과 출처를 더 잘 이해할 수 있습니다.

업로드 및 상태 API의 (POST) 및 (GET) 매개변수와 URL에 대한 자세한 내용은 을 참조하십시오 REST API를 사용하여 파일 업로드 소프트웨어 자재 명세서 .

도메인 분리

SBOM 애플리케이션의 모든 테이블은 도메인으로 분리됩니다.

작업 공간에서 소프트웨어 자재 명세서 라이센스 분류 및 구성요소 라이센스 해결

라이센스를 분류하고 구성요소와 해결(일치)하거나 작업 공간의 SBOM 라이센스 관리 모듈에서 라이센스를 생성합니다. 라이센스를 분류하고 구성요소에 매칭하면 파일에 업로드하는 독점, 오픈 소스 및 벤더 제공 소프트웨어 구성요소에 대한 라이센스 준수 여부를 확인할 수 있습니다 SBOM .

라이센스 데이터 및 타사 소프트웨어

조직이 자체 소프트웨어 애플리케이션을 더 많이 구축함에 따라 오픈 소스 구성 요소와 벤더 제공 소프트웨어를 사용하고 있습니다. 타사 및 오픈 소스 구성 요소를 사용하면 소프트웨어 프로젝트를 신속하게 만들고 릴리스할 수 있는 여러 가지 이점이 있지만 이러한 구성 요소를 사용하면 다음과 같은 라이선스 위험이 따릅니다.

- 오픈 소스 및 벤더 제공 소프트웨어 구성요소는 때때로 다른 구성요소에 대한 종속성을 가지며 각 구성요소에는 고유한 라이선스 요구 사항이 있을 수 있습니다.
- 애플리케이션의 구성 요소 및 소프트웨어에 대한 라이선스 조건을 준수하지 않는 경우 실수로 내부 정책 및 규제 라이선스 요구 사항을 위반하는 코드를 제공할 수 있습니다.

라이센스 관리 모듈

SBOM 작업 공간의 라이센스 관리 모듈을 사용하면 다음 작업을 수행할 수 있습니다.

- 파일과 함께 SBOM 업로드하는 구성요소에 필요한 라이센스를 분류합니다.
- 분류한 각 라이센스를 특정 구성요소로 해결합니다.
- 홈페이지에서 데이터 시각화를 준수하지 않는 구성 요소의 비율을 확인합니다. 이 정보를 사용하여 전반적인 보안 태세와 잠재적 위험 노출을 확인할 수 있습니다.

SBOM 업로드하는 파일에 라이선스 정보가 포함되어 있으면 각 SBOM 업로드 시 고유한 라이선스가 관찰되므로 라이선스 데이터베이스가 자동으로 확장됩니다. 각 SBOM 업로드를 통해 업로드된 라이선스의 데이터베이스를 구축한 다음, 필요한 경우 작업 공간의 라이선스 관리 모듈을 사용하여 분류할 수 있습니다 SBOM . 라이센스를 다음 범주 중 하나로 분류한 후 구성요소에 할당할 수 있도록 라이센스 인벤토리를 작성합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 허용됨
- 제한함
- 금지됨
- 분류되지 않음

법무 담당자, 라이센스 관리자, 규정 준수 및 규제 관리자는 라이센스 관리 모듈에서 작업을 수행합니다.

업로드된 라이센스 데이터 보기

다음 옵션을 사용하여 SBOM 작업 공간에서 구성요소와 함께 업로드한 라이센스 정보를 볼 수 있습니다.

- 다음으로 이동 작업 공간 〉 **SBOM** 작업 공간 〉 구성 요소.

  구성요소 페이지에서 구성요소의 라이센스 분류 카드에는 다음 범주와 함께 전체 라이센스 준수에 대한 시각화가 표시됩니다.

범주	설명
금지됨	라이센스 사용은 허용되지 않습니다.
분류 필요	라이센스가 아직 분류되지 않아 검토가 필요합니다.
허용됨	라이선스 사용은 제한 없이 허용됩니다.
제한함	특정 사용 사례에서는 라이센스 사용이 허용되지 않습니다.

  이 스냅샷은 라이센스 관리 모듈에 입력한 분류 및 확인된 라이센스 정보를 사용하여 전반적인 라이센스 준수를 계산합니다.

  이 목록에서 구성요소 기록을 선택하면 상태 필드의 다른 정보와 함께 구성요소의 라이센스 정보를 볼 수 있습니다.

- 또는 다음으로 이동합니다. 작업 공간 〉 **SBOM** 작업 공간 〉 라이센스 관리 〉 라이센스 분류.

  이 페이지는 업로드한 SBOM 파일에서 탐지된 고유 라이선스의 총 수를 추적합니다. 또한 다음 범주의 페이지 상단에 있는 카드로 필터링합니다.

  - 분류되지 않음 - 라이선스에 검토 및 분류가 필요합니다.
  - 금지됨 - 라이선스 사용이 허용되지 않습니다.
  - 제한됨 - 특정 사용 케이스에서는 라이센스가 허용되지 않습니다.
  - 허용됨 - 라이선스 사용이 제한 없이 허용됩니다.
  - 모든 라이센스 - 라이센스의 총 카운트.

  조직의 모든 구성요소가 이 페이지에 나열된 라이센스 중 하나를 사용하고 있습니다. SBOM 업로드에서 새 라이센스가 탐지되면 기록이 생성되어 SBOM 라이센스 [sn_sbom_license] 테이블에 저장되고 이 목록에 추가됩니다. 기본 분류는 분류 필수입니다. 전체 라이센스 준수가 정확하게 계산되도록 이 상태의 라이센스 기록을 검토 및 분류한 후 구성요소와 해결(일치)해야 합니다.

  라이센스를 분류하는 방법에 대한 자세한 내용은 문서를 참조하십시오 작업 공간에서 임포트한 라이센스 소프트웨어 자재 명세서 분류.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

역할

새 라이센스는 sn_sbom_response.managelicense 역할을 가진 사용자가 분류해야 합니다. 이 사용자는 업로드된 라이센스 정보를 보고 허용되는 라이센스와 금지된 라이센스를 결정합니다. 이 역할을 가진 사용자는 sn_sbom_response.licenseresolver 역할이 없으면 구성요소 라이선스 해결 모듈을 볼 수 없습니다.

분류 후에는 전반적인 라이센스 준수를 확인할 수 있도록 sn_sbom_response.licenseresolver 역할을 가진 사용자가 라이센스를 해결해야 합니다. 이 사용자는 구성요소에 대한 라이센스를 해결합니다. 이 역할을 가진 사용자는 sn_sbom_response.managelicense 역할이 없으면 라이센스 분류 모듈을 볼 수 없습니다.

새 라이센스 정보를 분류하는 것은 지속적인 프로세스입니다. 미분류 카드에 표시되는 총 수를 낮게 유지하는 것이 좋습니다. 라이선스 관리자는 며칠에 한 번씩 그리고 SBOM 파일을 업로드한 후에 분류가 필요한 라이선스를 확인하는 것이 좋습니다.

라이센스 해결자는 며칠에 한 번씩 업데이트된 분류 라이센스를 확인하는 것이 좋습니다.

작업 공간에서 임포트한 라이센스 소프트웨어 자재 명세서 분류

라이센스 분류 기능을 사용하여 파일과 함께 SBOM 업로드하는 구성요소 라이센스를 분류합니다.

시작하기 전에

새 라이센스 정보를 분류하는 것은 지속적인 프로세스입니다. 미분류 카드에 표시되는 총 수를 낮게 유지하는 것이 좋습니다. 라이선스 관리자는 며칠에 한 번씩 그리고 SBOM 파일을 업로드한 후에 분류가 필요한 라이선스를 확인하는 것이 좋습니다.

필요한 역할: sn_sbom_response.managelicense

프로시저

1. 다음으로 이동 작업 공간 〉 **SBOM** 작업 공간 〉 라이센스 관리 〉 라이센스 분류.

   주:
   sn_sbom_response.licenseresolver 역할이 없으면 라이센스 분류 탭만 표시됩니다.

2. 옵션: 분류를 기준으로 라이센스를 필터링하려면 카드를 선택합니다.
3. 라이센스를 분류하려면 하나를 선택합니다.
4. 라이센스를 분류한 후에는 분류된 라이센스를 구성요소로 해결할 준비가 된 것입니다.

작업 공간의 구성요소 소프트웨어 자재 명세서 에 대한 라이센스 해결

구성요소 라이센스 해결 기능을 사용하여 분류된 라이센스를 특정 구성요소로 해결(할당)합니다. 정보가 누락되었거나 잘못된 라이센스 정보가 있는 구성요소에 라이센스를 할당하거나 새 라이센스를 생성하여 전체 라이센스 준수를 계산할 수 있습니다.

시작하기 전에

필요한 역할: sn_sbom_response.licenseresolver

프로시저

1. 다음으로 이동 작업 공간 〉 **SBOM** 작업 공간 〉 라이센스 관리 〉 구성요소 라이센스 해결.

   주:
   sn_sbom_response.managelicense 역할이 없으면 구성요소 라이센스 해결 탭만 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 페이지에서는 고유 라이센스의 총 수와 업로드한 SBOM 파일에서 탐지된 라이센스 합계를 한눈에 볼 수 있는 뷰를 추적합니다. 이 페이지에 표시된 라이센스는 구성 요소와 관련하여 크게 두 가지 범주에 속합니다.

- 구성요소의 모든 인스턴스가 라이센스에 동의합니다.
- 단일 라이센스에 대한 불일치가 있으며 구성요소에 대해 둘 이상의 라이센스가 있습니다.

두 번째 경우에는 단일 라이센스가 단일 구성요소로 해결되도록 이러한 라이센스를 조정해야 합니다. 라이센스 준수는 구성 요소당 해결된 라이센스 하나를 기준으로 계산됩니다.

이 페이지의 라이선스는 해결하는 데 도움이 되도록 다음 범주로 필터링됩니다.

값	설명
해결되지 않은 라이센스가 있는 구성요소	구성요소에 라이센스가 할당되지 않았으며 해결이 필요합니다. (## ##) 이 이러한 구성요소의 해결된 라이센스 열에 표시됩니다. 누락된 라이센스와 여러 라이센스 합계가 모두 이 범주의 일부로 나열됩니다.
누락된 라이센스가 있는 구성 요소입니다.	해결이 필요한 누락된 라이센스 정보가 있는 구성요소입니다.
여러 라이센스가 있는 구성요소	라이센스가 다르고 해결이 필요한 여러 엔터티에서 볼 수 있는 구성요소입니다.
모든 구성 요소	조직에서 추적하는 총 구성요소 목록입니다. 이 필터링된 목록에서 라이센스를 변경할 수 있습니다.

2. 카드를 선택합니다.
3. 라이센스를 해결하려면 하나를 선택합니다.

4. SBOM 작업 공간의 홈페이지로 이동하여 구성 요소의 라이센스 분류 시각화에서 사용 중인 구성 요소의 몇 퍼센트가 규정을 준수하지 않는지 확인합니다.
이 시각화에 대한 데이터는 BOM 구성요소의 라이센스 세부 항목 예약된 작업에 의해 매일 업데이트됩니다. 이 작업은 매일 실행되는 SBOM 보고서 데이터 수집기 예약 작업의 일부입니다.

작업 공간에서 보고서 및 대시보드 소프트웨어 자재 명세서 보기

취약성 분석가는 업로드된 소프트웨어 자재 명세서 파일을 기록, 데이터 시각화, (SBOM) 작업 공간에서 향상된 취약성 인텔리전스로 볼 수 있습니다 소프트웨어 자재 명세서 .

SBOM Core

BOM 엔티티와 업로드한 컴포넌트 목록을 홈(방문) 페이지와 작업공간의 컴포넌트 모듈에서 볼 수 있습니다 SBOM .

SBOM 응답

SBOM 응답 애플리케이션은 작업 공간의 홈(방문) 페이지에서 BOM 엔터티, 취약성이 있는 엔터티 및 활성 애플리케이션 취약 항목에 대한 자세한 정보가 포함된 데이터 시각화를 SBOM 제공합니다. 응답이 있는 SBOM 작업 공간에는 다음 모듈이 포함되어 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 홈페이지 - 데이터 시각화 및 향상된 취약성 상세 정보입니다.
- 구성요소 - 구성요소 및 구성요소의 라이센스 분류에 대한 버전 및 수정 사항 정보입니다.
- AVIT(애플리케이션 취약 항목) 생성 규칙 - 애플리케이션 취약 항목(AVIT)이 생성되는 경우의 조건입니다.
- BOM 큐 - 파일 업로드 상태 및 이력입니다.
- 목록 - 취약한 구성요소 및 라이브러리(NVD, CWE 및 애플리케이션 취약성)에 대한 AVIT 기록입니다.

다음 항목에서는 작업 공간에서 구성 요소에 소프트웨어 자재 명세서 대한 세부 정보를 찾는 방법에 대한 자세한 정보를 제공합니다.

- 작업 공간에서 홈페이지 소프트웨어 자재 명세서 검토
- 작업 공간에서 소프트웨어 자재 명세서 구성요소 모듈 검토
- 파일의 업로드 상태 소프트웨어 자재 명세서 보기
- 엔터티에 소프트웨어 자재 명세서 취약성이 있는지 확인 중
- 작업 공간에서 소프트웨어 자재 명세서 라이센스 분류 및 구성요소 라이센스 해결

작업 공간에서 홈페이지 소프트웨어 자재 명세서 검토

업로드된 데이터는 ()SBOM 작업 공간의 방문(홈) 페이지에 있는 시각화로 소프트웨어 자재 명세서 롤업됩니다. 취약성 분석가가 추세를 확인하고 구성요소에 대한 현재 정보를 검토할 수 있도록 파일을 업로드한 후 데이터가 수정됩니다.

시작하기 전에

필요한 역할: sn_sbom_resp.sbom_analyst

프로시저

1. 다음으로 이동 작업 공간 〉 **SBOM** 작업 공간.
   기본적으로 방문 페이지(홈)가 표시됩니다.

   모듈에서 볼 수 있는 내용은 설치한 애플리케이션에 따라 다릅니다.

   임포트된 데이터는 라이브 쿼리에 의해 계산되고 채워지지 않습니다. 홈 및 구성요소 페이지의 점수는 매일 한 번 업데이트되며 보고서 성과가 개선되었습니다. 이 향상된 기능을 통해 작업 공간의 홈 및 구성요소 모듈에서 성과표를 로드하는 시간이 더 빨라질 수 있습니다 SBOM .

   이러한 향상된 기능은 데이터 저장 방법 또는 위치에 영향을 주지 않습니다.

설치된 애플리케이션	설명
Core를 설치한 SBOM 경우	모든 BOM 도면요소입니다. 목록에는 각 엔터티의 이름, 분류 규칙(애플리케이션, 컨테이너, 라이브러리 등) 및 구성요소 수가 포함됩니다. BOM 엔터티는 문서가 생성되고 업로드된 파일의 루트 수준 구성요소 SBOM 를 SBOM 나타냅니다. 작업 공간의 홈 페이지로 이동하여 BOM 엔터티 목록을 확인합니다.
Response를 설치한 SBOM 경우	다음과 같은 데이터 시각화가 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설치된 애플리케이션	설명
	○ 모든 BOM 엔터티 - 유형(애플리케이션, 컨테이너, 라이브러리 및 기타)별 BOM 엔터티에 대한 세부 항목입니다. BOM 엔터티는 문서가 생성되고 업로드된 파일의 루트 수준 구성요소 SBOM 를 SBOM 나타냅니다. ○ BOM 취약성이 있는 엔터티 - 종속된 구성요소와 연관된 취약성이 있는 엔터티입니다. 엔터티 종속성에 중요 취약성이 하나 있는 경우 해당 엔터티의 심각도는 중요한 것으로 간주됩니다. ○ 활성 AVI - 매일 생성된 애플리케이션 취약한 항목(AVI) 수에 대한 추세입니다. 데이터 시각화는 지난 30일 동안의 데이터를 표시합니다. 30일 범위는 편집할 수 없습니다. 이 데이터는 애플리케이션 취약한 항목에 대한 생성 규칙을 검토하고 설정한 후에 사용할 수 있습니다. 자세한 내용은 작업 공간에서 애플리케이션 취약한 항목에 소프트웨어 자재 명세서 대한 규칙 생성 문서를 참조하십시오.

2. 데이터 시각화 카드를 선택하여 기록 목록을 표시합니다.

3. 홈 탭을 선택하여 방문 페이지로 돌아갑니다.

4. 또는**BOM** 엔터티 목록에서 기록을 선택합니다.

엔터티 이름과 버전이 기록 상단에 표시됩니다(예: SNC-SECOPS-SIR2.0).

주:
라이센스 관리 모듈을 사용하면 엔터티-라이센스 관계가 이 목록에 표시되지 않습니다. 구성요소가 사용되는 엔터티를 보려면 구성요소 모듈로 이동하여 구성요소 기록을 엽니다. 구성요소 기록에서 해결되지 않음 또는 분류되지 않음 상태를 볼 수 있습니다.

5. 엔터티 기록에서 탭을 선택하여 데이터를 검토합니다.

a. 선택하지 않은 경우 개요 탭을 선택합니다.

데이터를 검토합니다. 이 기록에 필드가 채워지지 않으면 업로드한 파일에 데이터가 포함되지 SBOM 않은 것입니다.

이름	설명
이름	엔터티 이름입니다.
분류 규칙	엔터티 유형(예: 애플리케이션, 구성요소 또는 라이브러리)
버전	엔터티의 버전 번호입니다.
공급자	엔터티를 공급한 제품입니다.
제품 모델	기존 제품 모델이 없거나 API를 통해 업로드할 때 SBOM 포함하지 않은 경우 모델이

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이름	설명
	생성됩니다. 엔터티 이름은 제품 모델 기록에 사용됩니다(예: SNC-SECOPS-SIR2.0).

b. 종속 대상 탭을 선택합니다.

이 엔터티의 모든 종속성과 분류 규칙(예: #####)이 나열됩니다. 버전 번호, #### 및 기타 정보가 표시됩니다.

이 목록에서 링크를 선택하면 기록이 열립니다. 해당 탭은 홈 및 엔터티 기록 탭 아래에 표시됩니다. 여는 기록에는 검토할 수 있는 개요, 해시, BOM 엔터티, 취약성 및 애플리케이션 취약한 항목(AVIT)과 같은 관련 목록이 포함될 수 있습니다.

BOM 엔터티 관련 목록에는 이 표시된 항목이 사용되는 모든 엔터티가 표시됩니다.

c. 취약성 탭을 선택하여 이 엔터티의 종속성과 관련된 취약성을 확인합니다.

엔터티에 대해 표시되는 취약성에 대한 자세한 내용은 다음 문서를 참조하십시오 파일의 업로드 상태 소프트웨어 자재 명세서 보기.

d. AVI 탭을 선택하여 이 엔터티에 대한 애플리케이션 취약한 항목이 있는지 확인합니다.

6. 옵션: 기록을 검토한 후 더 이상 필요하지 않은 것으로 확인되면 하나 이상의 BOM 엔터티 기록을 삭제할 수 있습니다.

> **주:**
> BOM 엔터티 기록을 삭제하면 해당 엔터티 기록 및 해당 구성요소 관계가 영구적으로 제거됩니다. BOM 엔터티와 연결된 모든 AVIT(애플리케이션 취약 항목)가 종결로 전환됩니다. 나중에 삭제한 레코드 및 컴포넌트 관계를 BOM 엔티티 목록에서 다시 사용하고 작업공간에서 사용할 수 있도록 하려면 이러한 BOM 엔티티를 다시 업로드해야 합니다.

a. 홈페이지에 없는 경우 홈 탭을 선택하여 홈페이지로 돌아갑니다.

b. BOM 엔터티 목록에서 삭제할 기록을 선택합니다.

c. 삭제를 선택합니다.

작업 공간에서 소프트웨어 자재 명세서 구성요소 모듈 검토

(SBOM) 작업 공간의 구성요소 모듈 소프트웨어 자재 명세서 에는 임포트한 구성요소의 취약, 부실, 중단됨 및 고위험 조합에 대한 현재 정보가 표시됩니다.

구성요소 모듈 보기

필요한 역할: sn_sbom_resp.sbom_analyst

다음으로 이동 작업 공간 〉 **SBOM** 작업 공간 〉 구성 요소.

모듈에서 볼 수 있는 내용은 설치한 애플리케이션에 따라 다릅니다.

임포트된 데이터는 라이브 쿼리에 의해 계산되고 채워지지 않습니다. 홈 및 구성요소 페이지의 점수는 매일 한 번 업데이트되며 보고서 성과가 개선되었습니다. 이 향상된 기능을 통해 작업 공간의 홈 및 구성요소 모듈에서 성과표를 로드하는 시간이 더 빨라질 수 있습니다 SBOM .

이러한 향상된 기능은 데이터 저장 방법 또는 위치에 영향을 주지 않습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설치된 애플리케이션	설명
Core를 설치한 SBOM 경우	다음 정보를 포함하는 업로드된 모든 구성요소의 인벤토리입니다. • 이름 • 설명 • 버전 • BOM 엔터티 수
Response를 설치한 SBOM 경우	그래프에서 그래프 또는 숫자를 선택하여 연결된 기록 목록을 봅니다. 모든 구성 요소 부실 및 중단된 구성요소 목록과 전체 구성요소 수에 하나 이상의 취약성이 있는 구성요소입니다. 이러한 개수는 주의가 필요한 구성요소를 식별하는 데 도움이 될 수 있습니다. 모든 구성요소가 이러한 범주에 맞지 않을 수 있기 때문에 이러한 구성요소 하위 세트가 총 구성요소 수와 일치하지 않을 수 있습니다. • 부실 구성 요소의 버전은 최신 버전보다 두 개 이상의 주요 버전이며 최신 버전보다 2년 뒤처져 있습니다. • 버려진 구성 요소가 2년 이상 업데이트되지 않았습니다. • 취약한 구성 요소는 심각도가 높음 이상인 취약성이 있는 구성 요소입니다. 고위험 조합 고위험 구성 요소는 즉각적인 주의가 필요할 수 있습니다. 응답 애플리케이션을 설치할 SBOM 때 설치되는 Deps.dev 통합은 부실 및 중단됨 상태의 구성 요소에 대한 패키지 인텔리전스를 제공합니다. 임포트된 고위험 조합은 업데이트, 교체 또는 다른 유형의 복구를 통해 수정할 수 있는 심각한 (심각 또는 높음) 취약성이 하나 이상 있는 부실 및 중단된 구성 요소로 구성됩니다. 완전히 수정 가능 상태는 구성 요소에 문제를 해결할 수 있는 사용 가능한 버전이 있음을 의미합니다. 수정 가능한

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설치된 애플리케이션	설명
	버전이 있는 고위험 구성 요소의 총 수의 백분율이 표시됩니다. 취약한 구성 요소의 적합성 중요, 높음, 보통 및 낮음 취약성이 있는 구성요소의 합계 및 세부 항목과 취약성의 일부 또는 전부를 해결할 수 있는지 여부입니다. 구성요소에 둘 이상의 취약성이 있는 경우 가장 중요한 취약성이 우선합니다. 고정성 상태: • 완료 - 구성요소의 현재 버전과 관련된 모든 취약성에 대한 수정 버전이 있습니다. • 부분 - 구성요소의 현재 버전과 연관된 취약성 중 적어도 하나에 대한 수정 버전이 있지만 모든 취약성과 관련된 것은 아닙니다. 구성요소의 라이센스 분류 라이센스 분류에 따른 구성요소의 합계 및 세부 항목입니다. 시각화 아래의 구성요소 목록을 사용하면 이름, 설명, 버전 및 엔터티 수를 볼 수 있습니다. 오른쪽 패널에서 버전 기록을 볼 수 있습니다. 현재 버전이 버전 이력에서 강조 표시됩니다. **CVE(**Common Vulnerabilities and Exposure) 및 **Fixability** 열도 표시됩니다.

취약성 인텔리전스로 위험 평가

작업 공간에서 취약성 인텔리전스 데이터를 검토하는 방법에 대한 자세한 내용은 을 참조하십시오 엔터티에 소프트웨어 자재 명세서 취약성이 있는지 확인 중 .

라이센스 준수로 위험 평가

데이터에 라이센스를 부여하는 방법, 구성요소를 사용하여 임포트하는 방법 및 작업 공간에서 전반적인 라이센스 준수를 보는 방법에 대한 자세한 내용은 을 참조하십시오 작업 공간에서 소프트웨어 자재 명세서 라이센스 분류 및 구성요소 라이센스 해결 .

작업 공간에서 애플리케이션 취약한 항목에 소프트웨어 자재 명세서 대한 규칙 생성

소프트웨어 자재 명세서(SBOM) 작업 공간에서 AVIT(애플리케이션 취약 항목)를 보려면 먼저 AVIT가 생성되는 조건을 설정해야 합니다.

작업 공간의 **AVIT SBOM**

응답 애플리케이션을 설치하고 활성화 SBOM 한 경우 가져온 데이터 중 하나라도 기존 AVIT 생성 규칙의 조건과 일치하면 파일에 대한 SBOM AVIT가 생성됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

SBOM 대응 및 취약성 대응 애플리케이션은 애플리케이션 취약한 항목(AVIT)을 자동으로 생성하고 워크플로우를 애플리케이션 취약성 대응 통해 정정하기 위한 규칙을 설정해야 합니다. 자세한 내용은 소프트웨어 자재 명세서 탐색 문서를 참조하십시오.

sn_sbom_resp.manage_avi_rule 역할을 가진 사용자는 수집된 SBOM 데이터에서 발견된 취약성에 대한 AVIT를 생성하기 전에 작업 공간에 AVIT 생성 규칙을 SBOM 추가해야 합니다. AVIT를 사용하면 애플리케이션에서 타사 구성 요소의 무결성을 평가할 수 있습니다. 애플리케이션이 연관된 취약성이 있는 구성요소와 일치할 때 인스턴스에 AVIT가 생성됩니다.

SBOM 작업 공간에서는 SBOM AVIT만 볼 수 있습니다. 그러나 의 취약성 관리자 작업 공간에서 다른 유형의 취약한 항목과 함께 AVIT를 볼 SBOM 수 있습니다 취약성 대응. 목록 모듈의 SBOM 작업 공간에서 생성된 모든 AVIT를 볼 수 있습니다. 목록 모듈에는 모든 NVD 및 CWE 항목과 애플리케이션 취약점도 포함됩니다.

NVD(국가 취약성 데이터베이스)와 같은 알려진 취약성 목록의 권장 사항에 따라 정정을 위해 AVIT를 할당할 수도 있습니다. 예약된 작업이 트리거되고 생성 규칙의 조건이 수집된 데이터와 일치하면 AVIT가 생성됩니다.

사용자 지정 규칙을 설정하여 AVIT를 추적하고 정정할 수 있습니다.

규칙을 만드는 방법에 대한 자세한 내용은 을 참조하십시오 작업 공간에서 애플리케이션 취약한 항목 규칙 소프트웨어 자재 명세서 생성 .

SBOM의 AVIT 취약성 관리자 작업 공간취약성 대응

작업 공간에서 생성된 SBOM 모든 SBOM AVIT를 액세스할 수 있는 경우 해당 취약성 관리자 작업 공간 AVIT를 볼 수 있습니다.

> **주:**
> 모든 AVIT가 아닌 애플리케이션 취약 항목 목록의 취약성 관리자 작업 공간 AVIT만 SBOM 보려면 애플리케이션 취약 항목 〔sn_vul_app_vulnerable_item〕 테이블에서 〔소스〕 〔다음과 같음〕 **[SBOM]** 및 〔스캔 유형〕 〔다음과 같음〕 **[SBOM-SCA]** 조건을 설정합니다. 테이블을 보려면 인스턴스에서 모두 로 이동한 다음 필터 탐색기에 **sn_vul_app_vulnerable_item.list** 를 입력합니다.
>
> 취약성 관리자 작업 공간, 감시 주제, 애플리케이션 정정 작업 및 애플리케이션에서 구성된 취약성 대응 AVIT에 대한 애플리케이션 정정 작업 규칙을 보는 방법에 대한 자세한 내용은 을 취약성 관리자 작업 공간참조하십시오 의 주시 주제 사용취약성 관리자 작업 공간.

AVUL(정정 작업)은 AVIT에서 생성되며 할당 규칙에 따라 정정을 위해 그룹에 자동으로 할당됩니다. 이러한 규칙을 만드는 방법에 대한 자세한 내용은 다음 항목을 참조하세요.

- 담당 규칙 생성 또는 편집 취약성 대응
- 정정 작업 규칙 생성 또는 편집 취약성 대응 및 에서 정정 작업 생성 취약성 관리자 작업 공간.

SBOM 응답에서 애플리케이션 취약 항목 다시 열기

다음과 같은 조건이 존재하면 연관된 취약성이 있는 구성요소에 대해 종결된 AVIT(애플리케이션 취약한 항목)가 자동으로 다시 열리고 작업 공간에 표시됩니다 SBOM .

- 연관된 취약성이 있는 AVIT가 외부 공급업체 통합의 취약성 검사에 의해 다시 탐지되거나 취약성이 있는 구성요소가 후속 SBOM 업로드의 일부입니다.
- 탐지된 경우 AVIT 다시 열기 (*sn_sbom_resp.reopen_avits_if_detected*) 시스템 속성을 비활성화하지 않았습니다. 이 시스템 속성은 기본적으로 활성화되어 있습니다.
- 종결된 AVIT의 하위 상태가 완화 통제가 있음, 영향을 받지 않음 또는 가양성 중 하나가 아닙니다. 이러한 하위 상태가 있는 AVIT는 시스템 속성에 의해 다시 열리지 않습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

종결된 AVIT가 자동으로 다시 열리지 않도록 하려는 경우에만 이 시스템 속성을 비활성화합니다.

파일의 업로드 상태 소프트웨어 자재 명세서 보기

(SBOM) 작업 공간의 소프트웨어 자재 명세서 BOM 큐 모듈에 업로드하는 소프트웨어 자재 명세서 ()SBOM 파일의 업로드 상태를 확인합니다. 성공적으로 업로드한 파일, 업로드 이력 및 오류를 추적합니다.

시작하기 전에

필요한 역할: sn_sbom_resp.sbom_analyst

프로시저

1. 업로드 상태를 봅니다.

   업로드 상태를 확인하는 데 사용하는 방법은 설치한 애플리케이션에 따라 다릅니다.

옵션	설명
SBOM Core	**a.** 다음으로 이동 모두 〉 **SBOM Core** 〉 **BOM** 수집 상태. **b.** BOM 목록에서 상태, **BOM** 생성 시간 및 생성됨 열과 같은 열을 검토하여 자세한 내용을 확인합니다.
SBOM 응답	**a.** 다음으로 이동 모두 〉 **SBOM** 작업 공간 〉 **BOM** 큐. **b.** 시각화 카드를 선택하여 업로드된 파일의 범주에 대한 다음 상세 정보를 검토합니다. ▪ 지난 30일 동안의 BOM 업데이트 - 지난 30일 동안 성공적으로 업로드되고 구문 분석된 총 BOM 엔터티입니다. ▪ 소스 업로드 - 성공적으로 업로드된 SBOM 총 파일 수 및 해당 파일을 수집하는 데 사용되는 방법의 세부 항목(API 또는 수동)입니다. ▪ 범주별 업로드 오류 - 업로드 오류의 상위 5개 범주입니다. 이 시각화에 데이터가 나타나지 않으면 모든 파일이 성공적으로 업로드된 SBOM 것입니다.

BOM 테이블〔sn_sbom_doc_list〕과 BOM 큐 모듈의 상태 정보에는 모두 BOM 형식, 수집 상태 및 BOM 생성 시간이 포함됩니다. BOM 수집을 위한 상태 열에는 다음 상태가 포함됩니다.

- 큐에 대기 중 - SBOM 데이터가 업로드되었습니다.
- 처리 중 - 구성요소 데이터가 임포트의 일부로 처리되고 있습니다.
- 처리됨 - 데이터 수집이 성공적으로 완료되었습니다.
- 오류 - 처리하는 동안 오류가 발생했습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

업로드된 파일의 상태 외에도 BOM 엔터티 기록을 선택하여 수집한 구성 요소 목록을 볼 수 있습니다.

2. 옵션: 기어 아이콘, 선택하고 오류 범주 및 오류 상세 정보와 같은 필드를 추가하여 오류 및 업로드 상태에 대한 자세한 정보에 액세스합니다.

엔터티에 소프트웨어 자재 명세서 취약성이 있는지 확인 중

취약성이 업로드된 소프트웨어 자재 명세서 ()SBOM 파일의 구성요소와 연결되어 있는지 확인합니다.

먼저 다음 애플리케이션을 설치하고 활성화해야 취약성 및 강화된 취약성 데이터를 볼 수 있습니다.

- SBOM 응답
- NVD 및 CWE 작업과의 취약성 대응 통합
- 취약성 대응

자세한 내용은 소프트웨어 자재 명세서 탐색 문서를 참조하십시오.

필요한 역할: sn_sbom_resp.sbom_analyst

1. 다음으로 이동 모두 〉 **SBOM** 작업 공간 〉 구성 요소.
2. 시각화 또는 구성요소 레코드를 통해 취약성 정보를 볼 수 있습니다.

방법	작업
취약성이 있는 BOM 엔터티 시각화	취약성이 있는 **BOM** 엔터티 시각화 그래프를 선택합니다. ○ 취약성이 이 구성요소와 연결된 경우 총계가 목록의 CVE 및 CWE 열에 표시됩니다. 구성요소에는 둘 이상의 취약성이 있을 수 있습니다. 사용 가능한 경우 이 목록의 고정성 열에서 항목을 확인할 수 있습니다. ○ 이 구성요소와 연결된 취약성이 없는 경우 이 열에는 구성요소에 대한 값이 0 또는 전혀 표시되지 않습니다. CVE, CWE 및 Fixibilty 열이 표시되지 않는 경우 페이지 오른쪽 상단의 기어 아이콘 과 편집 열을 선택하여 페이지에 추가할 수 있습니다. 사용 가능 열 목록에서 선택하고 확인을 선택합니다.
구성요소 기록	**a.** 시각화 아래 목록에서 기록을 선택합니다. **b.** 기록에서 취약성 탭을 선택합니다. **i.** 데이터가 표시되지 않으면 보고된 취약성이 기록과 연결되지 않은 것입니다. **ii.** 데이터가 표시되면 취약성을 해결하기 위한 애플리케이션 취약성 대응 정정 워크플로우의 단계를 확인하고 작업

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

방법	작업
	공간에서 소프트웨어 자재 명세서 구성요소 모듈 검토 따릅니다. 자세한 내용은 취약성 정정 애플리케이션 취약성 대응 문서를 참조하십시오.

취약성 인텔리전스로 위험 평가

구성요소 레코드에 대한 응답을 사용하여 SBOM 향상된 취약성 데이터를 더 많이 봅니다. SBOM지원되는 애플리케이션에 설명된 Response 애플리케이션, Vulnerability Response, NVD(National Vulnerability Database) Integration 및 CWE(Common Weakness Enumeration) 예약된 작업을 설치하고 활성화해야 합니다.

1. 모든 구성요소 시각화를 선택하여 관련 기록 목록을 봅니다.
2. 이름 열에서 링크를 선택하여 기록을 엽니다.

   상태, 부실, 중단됨 및 취약 이 구성요소 이름 아래에 표시됩니다. 구성요소에는 이러한 상태의 조합이 있을 수 있습니다. 상태가 표시되지 않으면 구성요소가 부실하거나, 중단되거나, 취약하지 않은 상태입니다.

   현재 버전과 최근에 게시된 버전을 검토합니다. 오른쪽 패널에서 버전 기록을 볼 수 있습니다. 현재 버전은 버전 이력에서 강조 표시되며, 목록에 있는 해당 버전은 구성요소가 부실, 중단됨 및 취약한 이유를 파악할 수 있습니다. 예를 들어 이전 버전의 구성요소를 사용할 수 있습니다.

3. 기록에서 개요, 해시, **BOM** 엔터티, 취약성 및 **AVI** 관련 탭을 선택합니다.
   - 개요 - 구성요소 상세 정보의 요약입니다.
   - BOM 엔터티 - 이 구성요소와 연결된 엔터티 목록입니다.
   - 해시 - 임포트한 경우 해시가 표시됩니다.
   - 취약성 - 이 구성요소와 연관된 알려진 취약성에 대한 정보입니다. 이 목록이 비어 있으면 알려진 취약성이 없는 것입니다.

     목록이 채워지면 탭을 선택하여 이 기록과 연관된 CVE(일반적인 취약성 및 노출) 및 CWE(일반적인 약점 열거) 데이터에 대한 취약성 ID, 요약 및 기타 취약성 정보를 봅니다. CVE는 심각도에 따라 분류되고 CWE는 구성요소가 악용될 수 있는 가능성에 따라 분류됩니다. 취약성 ID 링크를 선택하여 OR 애플리케이션 취약성 대응 애플리케이션에서 향상된 취약성 기록을 취약성 대응 볼 수 있습니다.

   - AVI(AVIT) - COMPONENT 를 알려진 취약성과 일치시키는 AVIT 생성 규칙을 생성한 경우 이 구성요소와 연결된 애플리케이션 취약 항목입니다. AVR(애플리케이션 취약성 대응 애플리케이션)은 취약성을 애플리케이션에 연결하여 AVI 기록을 생성합니다. 자세한 내용은 작업 공간에서 애플리케이션 취약한 항목에 소프트웨어 자재 명세서 대한 규칙 생성 문서를 참조하십시오.

소프트웨어 자재 명세서 애플리케이션과 함께 설치되는 구성요소

애플리케이션을 활성화하면 소프트웨어 자재 명세서 테이블, 사용자 역할, 예약된 작업을 포함한 여러 유형의 구성요소가 설치됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설치되는 역할

역할 이름 **[name]**	설명	포함하는 역할
sn_sbom_response.managelicense	이 역할은 응답 애플리케이션과 함께 SBOM 설치됩니다. 이 역할을 사용하면 구성요소에 대한 라이센스를 해결할 수 있습니다.	안 함
sn_sbom_response.licenseresolver	이 역할은 응답 애플리케이션과 함께 SBOM 설치됩니다. 이 역할을 통해 업로드된 라이센스 정보를 볼 수 있으며 허용되는 라이센스와 금지된 라이센스를 결정할 수 있습니다.	안 함
SBOM 쓰기 [sn_sbom_dm.app_write], SBOM 생성 [sn_sbom_dm.app_create], SBOM 읽기 [sbom_dm.app_read]	이러한 역할은 애플리케이션용 SBOM 데이터 모델과 함께 설치됩니다. 이를 통해 테이블의 기록을 읽고, 만들고, 편집할 수 SBOM 있습니다.	안 함
SBOM 코어 수집 [sn_sbom_core.sbom_ingest] 및 SBOM 코어 관리자 [sn_sbom_core.admin]	이러한 역할은 코어 애플리케이션과 함께 SBOM 설치됩니다. sn_sbom_core.sbom_ingest 역할을 사용하면 REST API를 통해 수동으로 SBOM을 업로드할 수 있습니다. sn_sbom_core.admin 역할을 통해 SBOM을 생성, 읽기, 편집하고 업로드할 수 있습니다. 또한 이 역할을 통해 인스턴스의 핵심 모듈에 액세스할 SBOM 수 있습니다. 애플리케이션에 대한 SBOM 데이터 모델에서 역할을 상속합니다.	• sn_sbom_dm.app_write • sn_sbom_dm.app_create • sn_ sbom_dm.app_read

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

역할 이름 **[name]**	설명	포함하는 역할
SBOM 분석가 [sn_sbom_resp.sbom_analyst]	이 역할은 응답 애플리케이션과 함께 SBOM 설치됩니다. 이는 sn_sbom_core.admin 역할을 상속하며 작업 공간에 액세스할 SBOM 수 있도록 합니다.	• sn_sbom_core.admin • sn_sbom_dm.app_write • sn_sbom_dm.app_create • sn_ sbom_dm.app_read • sn_sbom_resp.manage_avi_rule • sn_sbom_config_rule 테이블

애플리케이션과 함께 설치되는 **SBOM** 테이블

다음 테이블에 나열된 테이블은 애플리케이션용 SBOM 데이터 모델과 함께 설치됩니다.

테이블의 데이터 모델 **SBOM**

테이블	설명
SBOM 문서 [sn_sbom_doc]	업로드한 BOM 엔터티를 포함합니다.
SBOM 구성요소 [sn_sbom_component]	상위 구성요소에 포함된 임포트한 SBOM 구성요소, 분류 규칙 및 버전을 포함합니다.
SBOM 구성요소 관계 [sn_sbom_comp_relationship]	구성요소와 해당 종속성을 포함합니다.
SBOM M2M BOM 구성요소 [sn_sbom_m2m_bom_comp]	BOM 구성요소 매핑을 포함합니다.
SBOM 라이센스 [sn_sbom_license]	구성요소에 사용되는 오픈 소스 라이센스 ID를 포함합니다.
SBOM 공급 업체 [sn_sbom_supplier]	구성요소를 제공한 조직(제조업체, 배포자 또는 재패키지 업체일 수 있음)을 포함합니다.
SBOM 구성요소 ID [sn_sbom_comp_id]	구성요소 식별자를 포함합니다.
SBOM 구성요소 속성	구성요소 이름-값 속성을 포함합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테이블의 데이터 모델 **SBOM**

테이블	설명
[sn_sbom_comp_property]	
SBOM 해시 [sn_sbom_hash]	구성요소 해시 알고리즘을 포함합니다.
SBOM 접촉 [sn_sbom_contact]	공급자의 연락처 정보를 포함합니다.
SBOM 외부 참조 [sn_sbom_comp_external_ref]	관련될 수 있지만 에 포함되지 SBOM않은 시스템, 사이트 및 정보를 문서화하는 구성요소, 구성요소 유형 및 외부 URL을 포함합니다.
SBOM 패키지 그룹 [sn_sbom_pkg_group]	모든 구성요소에 대한 패키지 그룹 정보를 포함합니다. 애플리케이션 전체에서 여러 버전의 라이브러리를 사용할 수 있습니다. 동일한 구성 요소의 버전이 그룹화되어 이 테이블에 추가되어 동일한 데이터를 여러 번 끌어오지 않습니다.

다음 테이블에 나열된 테이블은 응답 애플리케이션과 함께 SBOM 설치됩니다

SBOM 응답 테이블

테이블	설명
SBOM 생성 규칙 구성 [sn_sbom_config_rule]	작업 공간에서 사용되는 SBOM AVIT 생성 규칙을 포함합니다.
SBOM M2M 구성요소 취약성 [sn_sbom_m2m_comp_vuln]	구성요소 및 관련 취약성을 포함합니다.
구성요소 취약성 수정 정보 [sn_sbom_comp_vuln_fix_info]	구성요소 버전과 연결된 각 외부 공급업체 취약성의 수정 버전을 포함합니다.
구성 요소 보고서 인사이트 [sn_sbom_comp_report_insight]	구성요소의 부실, 중단됨 및 고정성 데이터에 대한 인사이트를 포함합니다.
Deps 통합 임포트 [sn_sbom_deps_integration_import]	지정된 패키지 또는 라이브러리에 대해 임포트한 버전 목록 정보를 포함합니다.
OSV 통합 임포트 [sn_sbom_osv_integration_import]	주어진 패키지 또는 라이브러리 버전에 대한 취약성 인텔리전스 정보를 포함합니다.
구성 요소 버전 목록	구성요소에 대한 버전 정보 및 게시된 날짜를 포함합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

SBOM 응답 테이블

테이블	설명
[sn_sbom_st_version_list]	

예약된 작업

작업	설명
구성요소 고정성 및 취약성 계산	취약성이 있는 구성 요소를 수정하는 방법과 구성 요소를 수정할 수 있는 가능성에 대한 정보를 계산합니다.
OSV 통합 새 구성요소	마지막 통합 실행 후 임포트된 패키지(라이브러리)와 관련하여 공개적으로 알려진 모든 취약성을 검색합니다.
OSV 통합 종합	임포트된 모든 패키지와 관련하여 공개적으로 알려진 모든 취약성을 검색합니다.
Deps.dev 통합	패키지에 대해 공개적으로 알려진 모든 버전을 검색하고 부실 및 중단됨 상태의 구성요소를 식별하는 데 사용됩니다.
BOM 구성요소의 vuln_based_criticality 업데이트	취약성이 있는 구성 요소의 중요도를 업데이트합니다.

작업 공간에서 애플리케이션 취약한 항목 규칙 소프트웨어 자재 명세서 생성

(SBOM) 작업 공간의 AVI 생성 규칙 모듈에서 애플리케이션 취약 항목(AVIT)이 소프트웨어 자재 명세서 자동으로 생성되는 조건을 설정합니다.

시작하기 전에

SBOM 애플리케이션 취약한 항목을 생성하려면 응답 애플리케이션이 필요합니다. 자세한 내용은 소프트웨어 자재 명세서 탐색 문서를 참조하십시오.

필요한 역할: sn_sbom_resp.manage_avi_rule.

프로시저

1. 다음으로 이동 **SBOM** 작업 공간 〉 **AVI** 생성 규칙.
2. 새로 만들기를 선택합니다.
3. 필드를 작성합니다.

필드	설명
이름	규칙의 이름입니다.
활성	생성 규칙이 활성화되었는지 여부를 나타냅니다.
실행 순서	규칙이 평가되는 순서입니다. 숫자 값이 가장 낮은 규칙이 먼저 실행됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	예를 들어 특별한 처리가 필요하거나 위험이 중요한 항목에 대해 우선 순위가 높은 규칙을 만들어 먼저 실행할 수 있습니다. 다음으로, 특별한 처리가 필요하지 않은 항목에 대한 일반 규칙을 생성합니다. 마지막으로, 취약성이 있는 모든 구성 요소를 포착하는 기본 규칙을 생성합니다.
설명	다른 규칙과 구별하는 데 도움이 되는 규칙에 대한 설명입니다.
조건	애플리케이션 취약한 항목(AVI)이 생성되는 조건을 만듭니다. 예를 들어 **[Vulnerability > Severity][is][1-Critical]** 을 선택하여 위험이 높고 사용자에게 심각한 영향을 미칠 수 있는 취약성이 있는 구성 요소에 대한 AVIT를 만들 수 있습니다. 조건을 더 추가할 수 있습니다.

4. 저장을 선택합니다.
   생성 규칙은 다음 업로드 후 자동으로 실행되며 조건과 일치하는 구성요소에 대한 AVI를 생성합니다. 지금 실행을 선택하여 AVI 만들기 규칙 모듈에서 요청 시 규칙을 실행할 수도 있습니다.

결과
AVIT가 생성된 후 AVI 기록에서 소스 및 스캔 유형 필드의 값을 확인하여 AVIT가 데이터에 대해 SBOM 특별히 생성되었는지 확인할 수 있습니다.

필드	값
소스	SBOM
스캔 유형	SBOM-SCA

엔터프라이즈 보안 케이스 관리 애플리케이션

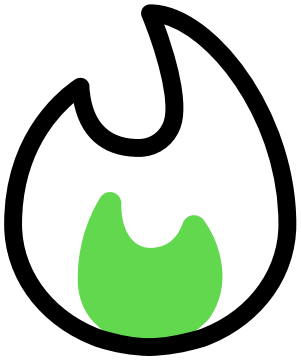
엔터프라이즈 보안 케이스 관리 애플리케이션에는 엔터프라이즈 보안 운영을 최적화하고 오케스트레이션하는 동시에 진화하는 위협에 신속하게 대응할 수 있도록 지원하는 보안 오케스트레이션 및 자동화 응답(SOAR) 솔루션이 포함됩니다 보안 인시던트 응답. 시스템, 팀 및 책임 전반에 걸친 수동 핸드오프에 내재된 오류와 마찰을 제거합니다.

시작하기

다음 보안 인시던트 응답 애플리케이션은 ServiceNow# Store. 앱을 찾고, 권리를 얻고, 인스턴스에 다운로드하는 방법에 대한 자세한 내용은 문서를 참조하십시오 보안 운영 그리고 ServiceNow Store .

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 인시던트 응답



Security Incident Response 애플리케이션에 대해 알아보기

중요 보안 인시던트 관리

Major Security Incident Management 애플리케이션에 대해 알아보기

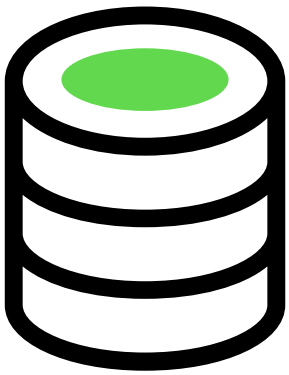
위협 인텔리전스

Threat Intelligence 애플리케이션에 대해 알아보기

위협 인텔리전스 보안 센터

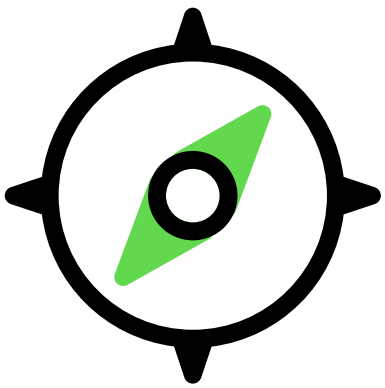
위협 인텔리전스 보안 센터 애플리케이션에 대해 알아보기

데이터 손실 방지 인시던트 응답



Data Loss Prevention 애플리케이션에 대해 알아보기

Security Incident Response 애플리케이션의 공유 기능



Security Incident Response 애플리케이션 간에 공유되는 기능에 대해 알아보기

문제 해결 및 도움 받기

- Security Operations 리소스 라이브러리
- Security Operations 커뮤니티
- 알려진 오류 포털에서 알려진 오류 문서 검색
- 연락처 고객 서비스 및 지원

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

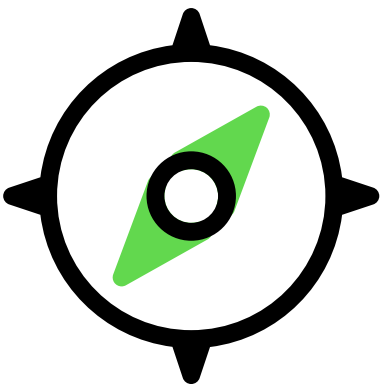
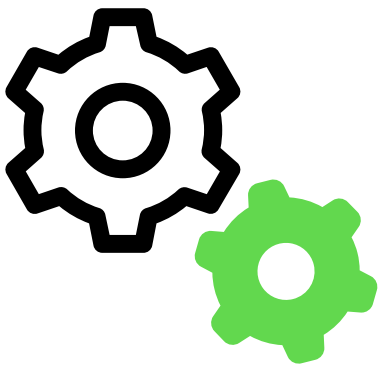
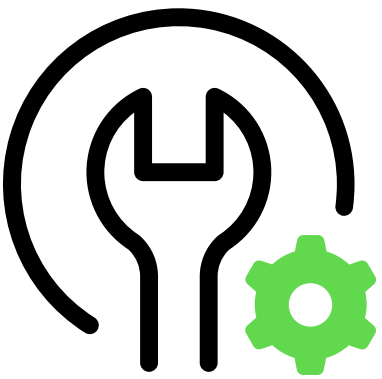
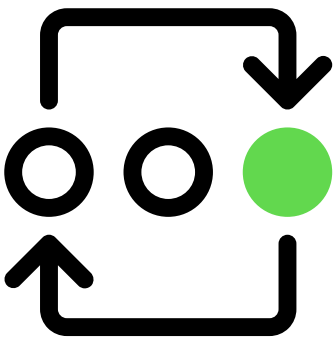
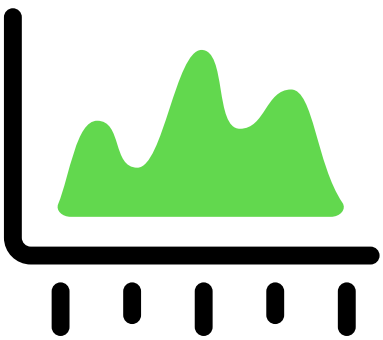
보안 인시던트 응답

이 ServiceNow# 보안 인시던트 응답 애플리케이션은 검색 및 초기 분석부터 방지, 근절 및 복구를 거쳐 최종 사후 인시던트 검토, 지식베이스 문서 생성 및 종결에 이르기까지 보안 인시던트의 진행 상황을 추적합니다.

스토어에서 앱 요청

ServiceNow Store 웹 사이트를 방문하면 사용 가능한 모든 앱을 확인하고 스토어에 요청을 제출하는 방법에 대한 정보를 참조할 수 있습니다. 출시된 모든 앱의 누적 릴리스 정보는 ServiceNow Store 버전 기록 릴리스 정보를 참조하십시오.

보안 인시던트 응답

탐색	설정 및 구성	관리자
		
Security Incident Response의 기능에 대해 알아보기	보안 인시던트 응답 애플리케이션 설치 및 설정	보안 인시던트 관리 및 사용자 지정
통합	보안 인시던트 응답 작업 공간 사용	분석 및 보고
		
다른 애플리케이션과 통합하여 Security Incident Response 확장	Security Incident Response 및 IT 정정 작업 공간 사용 방법 알아보기	정정 진행률 모니터링

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 인시던트 응답에
대한 추가 정보 가져오기

스토어에서 보안 운영 앱 요청

패치 6 이상의 신규 고객 London 인 보안 운영 경우 ServiceNow Store 사용 가능한 모든 앱을 보고 스토어에 요청을 제출하는 방법을 확인할 수 있는 웹 사이트입니다.

문제 해결 및 도움 받기

- Security Operations 리소스 라이브러리
- Security Operations 커뮤니티
- 알려진 오류 포털에서 알려진 오류 문서 검색
- 연락처 고객 서비스 및 지원

보안 인시던트 응답 이해

(SIR)을 사용하면 보안 인시던트 응답 초기 분석부터 억제, 근절, 복구에 이르기까지 보안 인시던트의 수명주기를 관리할 수 있습니다. Security Incident Response를 사용하면 분석가가 수행한 인시던트 응답 절차를 포괄적으로 이해하고 분석 기반 대시보드 및 보고를 통해 해당 절차의 추세와 병목 현상을 이해할 수 있습니다.

애플리케이션 사용을 시작하는 방법을 보여주는 보안 인시던트 응답에 대한 소개입니다.

이 9분짜리 비디오를 통해 탐색기에서 보안 인시던트 응답 공격을 차단하고 보안 활동을 보는 방법을 사용하는 SIR 프로세스에 보안 인시던트 응답 대해 알아보십시오.

타사 사이버 보안 솔루션과의 기본 제공 통합 및 Store의 ServiceNow 파트너 개발 통합을 통해 보안 자동화 및 오케스트레이션을 통해 효율적이고 정확한 인시던트 대응을 지원합니다.

조사를 보호하고 보안 인시던트를 비공개로 보안 인시던트 응답 유지하기 위해 는 시스템에 대한 액세스를 특정 보안 관련 역할 및 ACL로 제한할 수 있는 수단을 제공합니다. 비보안 관리자는 명시적으로 허용하지 않는 한 액세스가 제한될 수 있습니다.

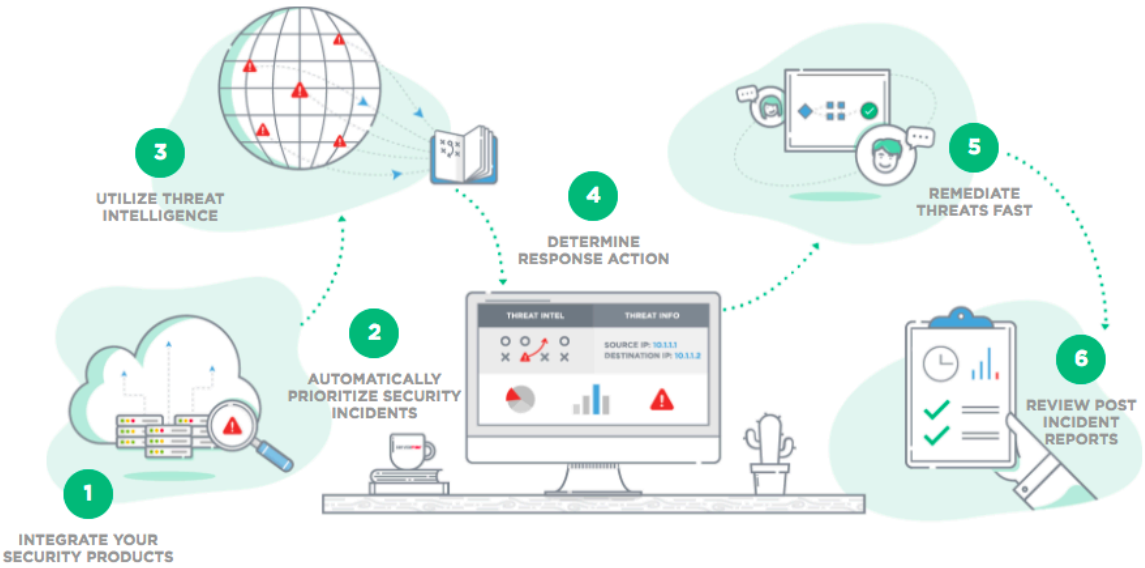
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
IT 시스템 관리자 (admin)는 ServiceNow 사용자로 가장할 수 있습니다. 그러나 보안 인시던트 응답에 대한 애플리케이션 관리자 역할이 있는 사용자를 가장하면 관리자는 보안 인시던트 및 프로파일 정보를 포함하여 해당 역할이 부여하는 기능에 액세스할 수 없습니다. 탐색 모음의 모듈 및 애플리케이션에 대한 액세스도 제한됩니다. 또한 관리자는 보안 인시던트 응답에 대한 애플리케이션 관리자 역할이 있는 사용자의 암호를 변경할 수 없습니다.

보안 인시던트 응답 정보 플로우

Security Incident Response는 통합에서 조사, 그리고 해결 및 검토에 이르기까지 다음과 같은 정보 흐름을 사용합니다.

주:
이것은 대화형 인포그래픽이므로 이미지의 아이콘이나 단계를 클릭하여 해당 프로세스나 작업에 대해 알아볼 수 있습니다.



1. SIR 통합에 대해 알아보려면 이 이미지를 클릭하십시오.
2. 보안 인시던트 생성에 대해 알아보려면 이 이미지를 클릭하십시오.
3. 위협 인텔리전스에 대해 알아보려면 이 이미지를 클릭하십시오.
4. SIR 작업 공간에 대해 알아보려면 이 이미지를 클릭하십시오.
5. MITRE 공격 기능에 대해 알아보려면 이 이미지를 클릭하십시오.
6. 사후 인시던트 검토 활동에 대해 알아보려면 이 이미지를 클릭하십시오.

디스커버리

다음과 같은 방법으로 보안 인시던트를 기록하거나 생성할 수 있습니다.

- 보안 인시던트 양식에서
- 내부에서 생성되거나 경보 규칙을 통해 외부 모니터링 또는 취약성 추적 시스템에서 생성하거나 수동으로 생성된 이벤트에서
- 외부 모니터링 또는 추적 시스템에서
- 서비스 카탈로그에서 제출

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

분석

선택한 뷰(기본값, 비 IT 보안, 보안 ITIL 등)에 따라 보안 인시던트 양식은 영향을 받는 CI 및 영향을 받는 CI 그룹의 취약성, 인시던트, 변경 사항, 문제, 작업의 조합을 표시할 수 있습니다. 시스템은 NIST(National Institute of Standards and Technology) 데이터베이스 또는 기타 타사 탐지 소프트웨어를 상호 참조하여 맬웨어, 바이러스 및 기타 취약성 영역을 식별할 수 있습니다. 보안 인시던트가 해결되면 아무 인시던트든 나중에 참조할 수 있도록 보안 지식베이스 문서를 만들 수 있습니다.

비즈니스 서비스 맵을 사용하여 추가 분석을 수행하여 감염되었을 수 있는 영향을 받는 다른 시스템 또는 비즈니스 서비스를 찾습니다.

방지, 근절 및 복구

취약성을 모니터링하고 분석하면서 작업을 생성하고 다른 부서에 할당할 수 있습니다. 비즈니스 서비스 맵을 사용하여 영향을 받는 모든 시스템, 문서, 활동, SMS 메시지, 브리지 통화 등에 대한 작업, 문제 또는 변경 사항을 만들 수 있습니다.

검토

인시던트가 해결되면 종결되기 전에 다른 단계를 수행할 수 있습니다. 인시던트 사후 검토를 수행할 수 있습니다. 지식베이스 문서를 생성하면 향후 유사한 인시던트에 도움이 될 수 있습니다. 중요한 인시던트는 사후 인시던트 해결 검토가 필요할 수 있습니다. 이 검토는 여러 가지 형태를 취할 수 있습니다. 예:

- 회의를 수행하여 인시던트에 대해 논의하고 응답을 수집합니다.
- 인시던트의 각 범주 또는 우선순위에 대해 디자인된 해결 검토 질문 목록을 작성하여 인시던트 담당 팀에 배포합니다.
- 인시던트 관리자는 직접 보고서를 작성하고 정보를 수집할 수 있습니다.

다음을 포함하는 인시던트 해결 검토 보고서를 자동으로 생성할 수 있습니다.

1. 수행한 작업에 대한 요약
2. 타임라인
3. 발생한 보안 인시던트의 유형
4. 모든 관련 인시던트, 변경 사항, 문제, 작업, CI 그룹
5. 해결의 세부 정보

또한 자동화된 보안 인시던트 해결 검토 설문 조사 시스템을 사용할 수 있습니다. 보안 인시던트에 할당된 모든 사용자의 이름을 수집하고 사용자 지정 설문 조사를 전송하여 인시던트 처리에 대한 데이터를 수집합니다. 그런 다음 이 데이터를 생성된 보안 인시던트 검토 보고서에 제공할 수 있으며, 이 보고서는 최종 초안으로 편집할 수 있습니다. 유사한 데이터를 지식베이스 문서에 추가하여 학습한 교훈과 향후 유사한 문제를 해결하기 위해 수행할 단계를 포함할 수 있습니다.

스토어에서 앱 요청

ServiceNow Store 웹 사이트를 방문하면 사용 가능한 모든 앱을 확인하고 스토어에 요청을 제출하는 방법에 대한 정보를 참조할 수 있습니다. 출시된 모든 앱의 누적 릴리스 정보는 ServiceNow Store 버전 기록 릴리스 정보를 참조하십시오.

Security Incident Response 용어

에서 사용되는 용어는 보안 인시던트 응답다음과 같습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

용어	정의
활성	종결되거나 취소됨 상태가 아닌 모든 보안 인시던트
관리자 잠금	보안 관련 역할 및 ACL이 있는 직원에 대한 액세스를 제한하는 보안 인시던트 응답 기능.
인바운드 보안 요청	새 전자 배지 요청과 같이 영향이 적은 보안 요구에 대해 제출된 요청입니다.
사후 인시던트 활동 관리	보안 인시던트의 기원 및 처리에 대한 검토입니다. 최종 결과물은 수행된 모든 작업과 수행 이유를 문서화하는 사후 인시던트 보고서입니다.
응답 작업	위협에 대응한 작업을 추적하기 위해 보안 인시던트에 할당된 작업입니다.
보안 인시던트 계산기 이해	미리 구성된 조건이 충족될 때 기록 값을 업데이트하는 데 사용되는 계산기입니다.
보안 인시던트 트리맵	중첩된 사각형 형태로 보안 인시던트 데이터를 계층적으로 표시하는 차트 유형입니다.
위협 조회	파일, URL 및 IP 주소에서 맬웨어를 검사하기 위해 보안 인시던트 카탈로그에서 제출된 요청입니다.
취약성 검사	영향을 받는 자원(서버, 컴퓨터 및 기타 구성 항목)에 취약성이 있는지 검사하기 위해 보안 인시던트 양식에서 시작된 요청입니다.

도메인 분리 및 보안 인시던트 응답

보안 인시던트 응답에서는 도메인 분리가 지원됩니다. 도메인 분리를 사용하여 데이터, 프로세스 및 관리 작업을 도메인이라는 논리적 그룹으로 분할할 수 있습니다. 어떤 사용자가 데이터를 보고 액세스할 수 있는지를 포함하여 이러한 분리의 여러 측면을 제어할 수 있습니다.

지원 수준: 표준

- 기본 수준 지원의 모든 측면을 포함합니다.
- 애플리케이션 속성이 필요에 따라 도메인을 인식합니다.
- 비즈니스 논리: 서비스 제공자(SP)가 고객별로 프로세스를 만들거나 수정합니다. 사용 사례는 여러 SP 고객이 단일 인스턴스에서 애플리케이션을 올바르게 사용하는 것을 반영합니다.
- 인스턴스 소유자는 특정 애플리케이션에 필요한 대로 테넌트별 최소 실행 가능한 제품(MVP) 비즈니스 논리 및 데이터 매개변수를 구성해야 합니다.

샘플 사용 사례: 관리자가 한 테넌트에 대해서는 기록이 닫히지만 다른 테넌트에 대해서는 기록이 닫히지 않는 경우 설명이 필요하도록 설정할 수 있어야 합니다.

지원 수준에 대한 자세한 내용은 도메인 분리를 위한 애플리케이션 지원 을 참조하십시오.

개요

애플리케이션에서 서비스 제공자(SP)는 도메인 분리를 보안 인시던트 응답 통해 서비스를 제공하는 고객 기반 전체에서 SOC(보안 운영 센터) 및 보안 인시던트 응답(SIR) 절차를 표준화하여 운영 비용을 절감하고 서비스 품질을 높일 수 있습니다. 워크플로우, 대시보드, 보고서 등을 위한 별도의 고객 작업 공간을 통해 고객 데이터가 분리되어 다른 클라이언트에게 노출되지 않도록 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

버전 릴리스별 보안 인시던트 응답의 도메인 분리 지원

릴리스	지원 수준	메모
제네바, 헬싱키	지원 안 함	데이터 수준 도메인 분리 시작
Istanbul	데이터만	
Jakarta	수준 2(데이터, 요청자, 이행자)	새로운 기능: 위협 인텔리전스 통합을 포함한 통합의 단일 인스턴스에서 수준 2 도메인 분리를 통한 외부 공급업체 통합 지원
Kingston	수준 2(데이터, 요청자, 이행자)	새로운 기능: SIR용 사이팅 검색 통합은 여러 인스턴스에서 활성화되지만 모든 인스턴스는 여전히 단일 도메인에 있습니다. 예: Splunk 통합의 두 인스턴스(SplunkCLOUD 및 SplunkCORP)가 구성된 경우 둘 다 구현이 원래 구성된 단일 도메인에서 인시던트 응답 활동에 계속 활용됩니다.
London	수준 2(데이터, 요청자, 이행자)	새로운 기능: 모든 통합이 여러 도메인에 걸쳐 있음
Madrid	수준 2(데이터, 요청자, 이행자)	이제 모든 통합이 여러 도메인에 걸쳐 상주할 수 있습니다. 위의 예에서 SplunkCloud는 domain1 및 SplunkCORP domain2일 수 있습니다.
New York	수준 2(데이터, 요청자, 이행자)	모든 통합은 여러 도메인에 걸쳐 있습니다.
Orlando	표준	모든 통합은 여러 도메인에 걸쳐 있습니다.
파리	표준	모든 통합은 여러 도메인에 걸쳐 있습니다.

애플리케이션의 도메인 분리는 보안 인시던트 응답 다음 제품 기능을 포함합니다.

- 보안 경보는 ID/자격 증명/범위가 인시던트를 생성하고 보안 인시던트로 등록된 사용자의 해당 도메인으로 전달됩니다.
- 경보는 상태 저장 속성 또는 측정 가능한 이벤트를 나타내는 "옵저버블"을 생성합니다. 보안 인시던트 도메인의 보안 워크플로우는 응답을 오케스트레이션하는 데 사용됩니다.
- 통합은 응답 자동화를 위한 보안 인시던트의 도메인에서 구성됩니다.
- 기능은 응답 자동화를 위한 보안 인시던트의 도메인에 구성됩니다. 이러한 기능(Kingston 릴리스 기준)은 다음과 같습니다.
  - 위협 조회
  - 옵저버블 보강
  - 구성 항목 보강
  - 실행 중인 프로세스 가져오기

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

  - 네트워크 통계 가져오기
  - 요청 차단
  - 호스트 격리
  - 검색 찾기
  - 이메일 검색 및 삭제
  - 감시 목록에 게시
- 응답 자동화(예: 위협 조회 또는 사이팅 검색)의 결과는 보안 인시던트의 도메인에 저장됩니다.
- 다른 보안 인시던트는 공유 옵저버블 집합을 기반으로 보안 인시던트의 동일한 도메인에서 상호 참조됩니다.
- 다른 사용자는 보안 인시던트의 도메인에서 상호 참조됩니다.
- 구성 항목은 보안 인시던트와 동일한 도메인에서 상호 참조됩니다.
- 수동 응답 작업은 보안 인시던트의 도메인에 추가됩니다.
- 지식베이스 문서와 실행 지침서는 보안 인시던트의 도메인에서 참조됩니다.
- 도메인의 인시던트와 관련된 보안 인시던트 응답 메트릭이 대시보드와 보고에 표시됩니다.

주:
앞의 경우 NOW Platform에서 분리된 도메인의 가시성에 대한 중요한 원칙이 적용됩니다. 항상 그렇듯이 상위 도메인의 인시던트는 하위 도메인의 아티팩트를 참조할 수 있지만 그 반대의 경우는 불가능합니다.

Security Incident Response에서 도메인 분리 작동 방식

애플리케이션은 보안 인시던트 응답 보안 인시던트의 수명주기를 엔드투엔드로 관리합니다. 다음 사용 사례는 도메인 분리를 인식합니다.

- 이벤트 및 경보를 수집 하여 고객 SOC의 분석가 또는 MSP가 응답할 수 있는 보안 인시던트를 생성합니다.
  - 이메일 파서(플랫폼 기반, 사용자 보고 피싱, 사용자 지정)
  - 인시던트 생성 전 중복 제거 이벤트/경보
  - 옵저버블 자동 추출
  - 외부 공급업체 SIEM 저장소의 애플리케이션
- 인시던트에 관련된 아티팩트 보강(IP, URL, 도메인, 파일 해시):
  - 자산 보강(CMDB)
  - 사용자(플랫폼)
  - 자동화: 옵저버블 보강(예: WhoIs)
- 아티팩트 및 아티팩트의 평판 또는 알려진 위협과의 연관성을 활용하여 인시던트 조사
  - 오케스트레이션: Playbook 및 지식베이스 문서
  - 자동화: 위협 조회(예: VirusTotal), 사이팅 검색(예: Splunk), 실행 중인 프로세스 가져오기(예: Carbon Black)
- 수행된 조사를 기반으로 인시던트에 관련된 위협 관련 아티팩트 근절
  - 오케스트레이션: Playbook 및 지식베이스 문서
  - 자동화: 이메일 검색 및 삭제(예: Microsoft Exchange), IP 차단(예: Palo Alto 방화벽)

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 인시던트 응답 운영의 효율성 측정
  - Performance Analytics 대시보드: 생산성 및 인시던트 추세
  - 작업 메모에서 인시던트 조사 단계 재구성
  - 사후 인시던트 검토

도메인 분리 설정

의 보안 인시던트 응답 도메인 분리를 설정하는 데는 추가 단계가 필요하지 않습니다. 모든 보안 인시던트 응답 테이블은 인스턴스가 도메인으로 분리된 후 도메인 열을 획득합니다.

도메인 분리 데이터

데이터는 도메인으로 구분될 수 있으며 이는 다음을 의미합니다.

- 한 도메인의 보안 인시던트를 다른 도메인에서 볼 수 없습니다.
- 보안 인시던트에서 추출된 옵저버블은 동일한 도메인에 배치되며 다른 도메인에서 볼 수 없습니다.
- Kingston 릴리스까지 구성된 타사 통합이 전역 도메인에 존재하며 인스턴스의 다른 모든 도메인에서 액세스할 수 있습니다.
- Madrid 릴리스에서는 도메인별로 외부 공급업체 통합을 구성하고 활성화할 수 있습니다. 즉, 한 도메인에서 활성화되고 구성된 통합을 다른 도메인에서 활용할 수 없습니다.
- 외부 공급업체 통합(위협 조사, 억제 또는 근절을 위해)을 사용하여 옵저버블에서 실행되는 자동화는 결과를 보안 인시던트의 도메인에 배치하고 다른 도메인에서 결과를 볼 수 없습니다.
- 한 도메인에서 생성된 오케스트레이션 워크플로우는 다른 도메인에서 볼 수 없습니다.
- 호출되는 기능(이전 기능 기능 목록에 설명되어 있음)은 호출되는 기능의 도메인별 구현을 통해 도메인 간에 일반 상태를 유지합니다. 예를 들어, IP에 대한 사이팅 검색은 한 도메인에서 Splunk 구현을 호출하고 다른 도메인에서 QRadar 구현을 호출할 수 있습니다.

구성

제품 구성의 모든 측면은 도메인 분리 환경에 포함되어 있습니다. 개별 도메인에 맞게 설정을 조정할 수 있습니다.

> **주:**
> 아래 #2-5의 비즈니스 논리와 프로세스는 테넌트 도메인 내에서 관리할 수 있습니다.

다음 작업을 구성해야 합니다.

1. 시스템 관리
   - 사용자 및 사용자 그룹에 역할을 할당합니다. 보안 인시던트 응답과 함께 설치되는 사용자 역할
   - 하나 보안 인시던트 응답이상의 외부 공급업체 통합 플러그인을 설치하여 작업합니다. 보안 인시던트 응답 통합
2. 보안 인시던트 응답 관리
   - 역할 추가 또는 검토: 보안 인시던트 응답와 함께 설치되는 구성요소
   - 그룹 및 사용자를 구성합니다. 보안 인시던트 그룹 생성
   - 인시던트 에스컬레이션 설정: 보안 인시던트 에스컬레이션
   - 보안 인시던트 위험 점수 계산기 설정: 보안 인시던트 계산기 이해
   - 서비스 수준 계약을 설정합니다. SLA 생성 보안 인시던트 응답

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 보안 인시던트 프로세스 정의를 설정합니다. Security Incident Response 프로세스 정의 이해
- 사후 인시던트 검토 프로세스를 설정합니다. 사후 인시던트 활동 관리

3. 보안 인시던트 이메일 설정
   - 이메일 구문 분석 수신함 설정: 보안 운영 이메일 구문 분석
   - 경보 수집을 위한 이메일 파서 설정: 보안 운영에서 이메일 파서 생성
   - 사용자가 보고한 피싱에 대한 이메일 일치 규칙을 설정합니다. 사용자가 보고한 피싱 공격을 확인하는 규칙 생성
   - 이메일 인바운드 작업 설정:인바운드 이메일 작업
4. 보안 인시던트 Playbook 설정
   - Runbook 문서를 검토하고 설정합니다. 보안 인시던트 응답 Runbook 생성
   - 보안 인시던트 워크플로우 설정: 보안 운영 공통 기능
5. 역량 구성
   - 차단 요청: 보안 운영 통합 - 차단 요청 기능
   - 이메일 검색 및 삭제: 보안 운영 통합 - 이메일 검색 및 삭제 기능
   - 구성 항목 보강: 보안 운영 통합 - CI 기능 보강
   - 옵저버블 보강: 보안 운영 통합 - 옵저버블 보강 기능
   - 네트워크 통계 가져오기: 보안 운영 통합 - 네트워크 통계 기능 가져오기
   - 실행 중인 프로세스 가져오기: 보안 운영 통합 - 실행 중인 프로세스 가져오기 기능
   - 호스트 격리: 보안 운영 통합 - 호스트 격리 기능
   - 주요 업데이트 공유자에 게시: 보안 운영 통합 - 감시 목록에 게시 기능
   - 사이팅 검색: 보안 운영 통합 - 사이팅 검색 역량
   - 위협 조회: 보안 운영 통합 - 위협 조회 기능

테넌트 도메인이 자체 애플리케이션 데이터를 관리하는 방법

- 테넌트 도메인 소유자는 보안 인시던트를 수집하기 위한 고유한 이메일 구문 분석 규칙을 생성합니다.
- 테넌트 도메인 소유자는 도메인 내에서만 사용할 특정 통합을 구성할 수 있습니다.
- 테넌트 도메인 소유자는 고유한 인시던트 응답 워크플로우를 만들 수 있습니다.
- 테넌트 도메인 소유자는 인시던트 응답 워크플로우와 연결할 고유한 인시던트 범주, 인시던트 응답 지식베이스 문서 및 Runbook을 생성할 수 있습니다.
- 테넌트 도메인 사용자가 자체 보안 인시던트를 생성하고 종결합니다.

인스턴스 소유자가 도메인을 분리할 수 있는 비즈니스 논리 및 프로세스

- 보안 인시던트 응답 사용자 및 그룹
- 보안 인시던트 응답 통합(Madrid 릴리스부터 시작)
- 인시던트 생성을 위한 이메일 구문 분석 규칙
- 여러 이벤트 또는 경보를 보안 인시던트로 통합하는 비즈니스 규칙
- 인시던트 응답 오케스트레이션을 위한 워크플로우

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 보안 인시던트 위험 점수 계산기
- 보안 인시던트 에스컬레이션 경로
- 보안 인시던트 SLA
- 보안 인시던트 프로세스 정의
- 보안 인시던트 사후 인시던트 검토 프로세스

관련 정보

서비스 제공자용 도메인 분리

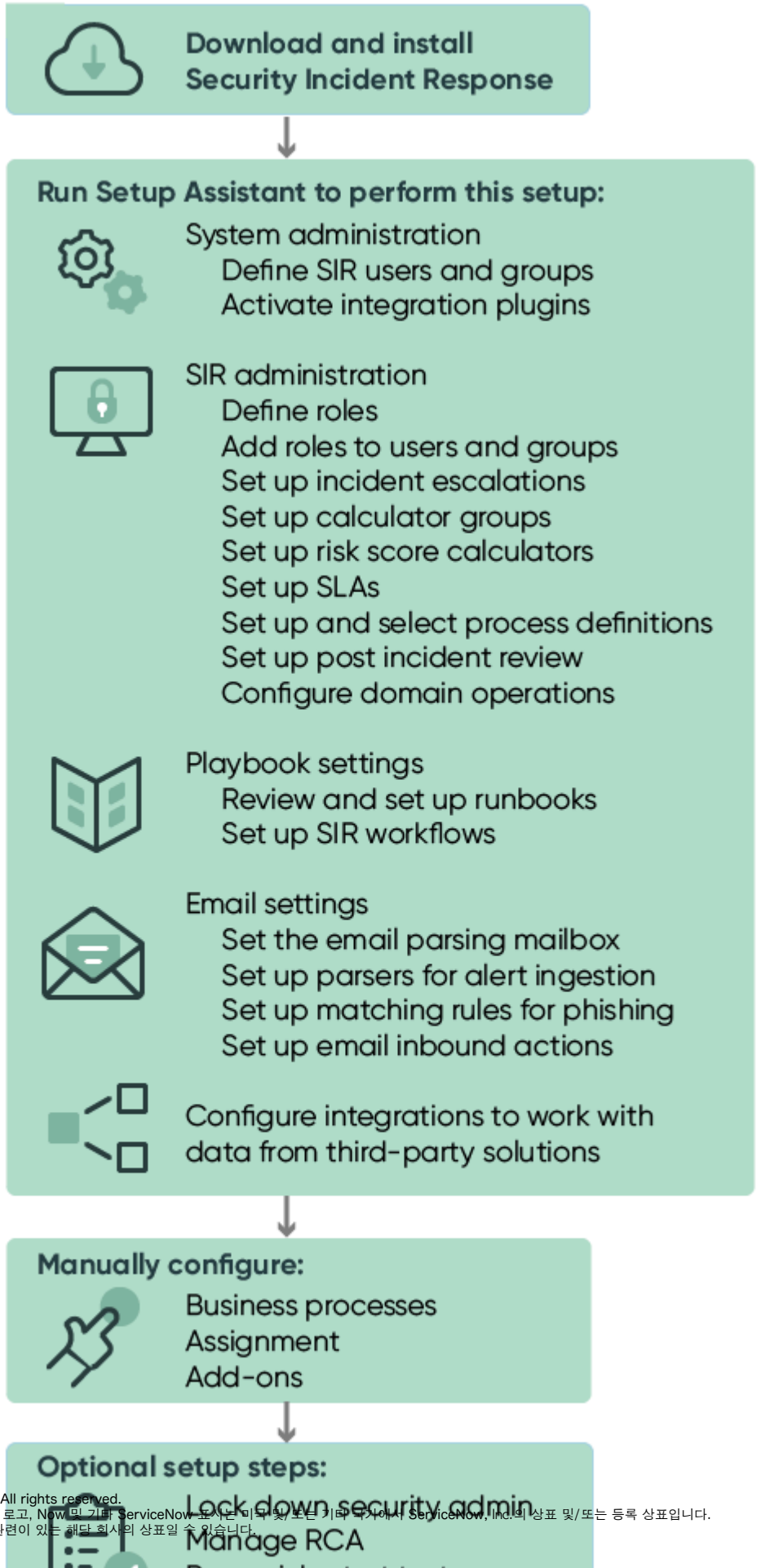
보안 인시던트 응답 설정

설정에는 보안 인시던트 응답 특정 요구 사항에 따라 몇 가지 필수 단계와 몇 가지 선택적 단계가 포함됩니다. 에서 ServiceNow Store 다운로드하여 보안 인시던트 응답 설치한 후에는 설정 도우미를 실행하여 타사 통합에 대한 보안 인시던트 응답 기본 구성을 수행할 수 있습니다.

보안 인시던트 응답 설정 프로세스

다음 다이어그램에서는 설정 프로세스를 보여 줍니다. 이는 애플리케이션을 다운로드하고 구성하는 보안 인시던트 응답 두 개의 하위 프로세스로 구분됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

첫 번째 설정 단계는 다음을 수행하는 것입니다. 다운로드 보안 인시던트 응답 애플리케이션의 ServiceNow Store. 다운로드가 완료되면 설정 도우미를 비롯한 여러 종속 응용 프로그램이 로드되어 에 보안 인시던트 응답사용할 준비가 됩니다.

설정 도우미

설정 도우미는 보안 인시던트 응답 기본 보안 인시던트 응답 인스턴스 설정을 단계별로 안내하는 마법사와 같은 애플리케이션입니다.

설정 단계는 매우 자명합니다. 그러나 추가 설명이 필요한 경우 설정 도우미 참조에서 추가 지원을 찾을 수 있습니다. 설정 도우미를 사용하여 설정을 완료한 후 필요에 따라 다른 선택적 설정 절차를 수행할 수 있습니다. 이러한 절차에는 다음에 대한 옵션이 포함됩니다.

- 요청 수명주기 설정
- 카탈로그 및 요청 생성
- 알림 구성
- 수동 및 자동 할당 설정
- 지식베이스, 관리 대상 문서 및 작업 활동 사용

새롭게 향상된 보안 인시던트 응답 작업 공간을 사용할 수 있습니다. 자세한 내용은 보안 인시던트 응답 작업 공간 문서를 참조하십시오.

보안 인시던트 응답 설치 및 구성

인스턴스에서 실행하려면 보안 인시던트 응답 먼저 에서 ServiceNow Store 다운로드하여 구성 단계를 완료해야 합니다.

시작하기 전에

필요한 역할: 관리자

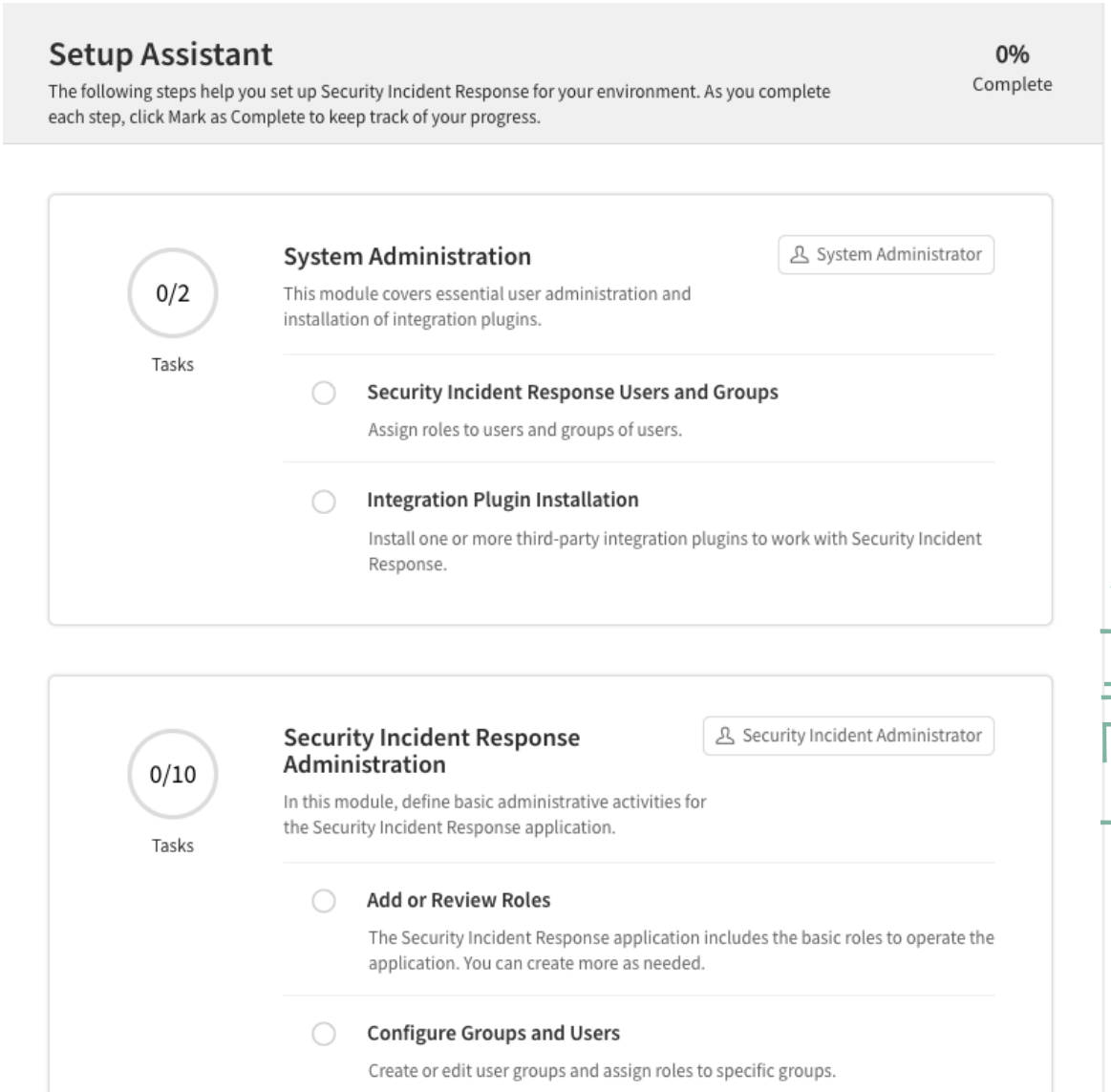
중요사항:

- 보안 인시던트 응답 에서 ServiceNow Store 13.4.5 버전 이상을 설치하면 기본적으로 (sn_si_aw) 1.5.1 버전 이상이 자동으로 설치됩니다 보안 인시던트 응답 작업 공간 . 종속 애플리케이션에 대한 자세한 내용은 이 SIR Workspace 플러그인 및 역할 섹션을 참조하십시오.
- 보안 인시던트 응답 작업 공간 버전 1.5.1 이상은 보안 인시던트 응답의 설치/업그레이드를 통해서만 설치/업그레이드할 수 있으며 독립적으로 설치할 수 없습니다.
- 의 보안 인시던트 응답 최신 기능은 에서만 사용할 수 있습니다 보안 인시던트 응답 작업 공간. 교대조 핸드오버, 위험 점수 계산기 등과 같은 기능에 액세스하고 활용하려면 최신 보안 인시던트 응답 버전을 보안 인시던트 응답 작업 공간 설치하거나 업그레이드하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음에 대한 지침을 따릅니다. 에서 애플리케이션 다운로드 ServiceNow Store.
2. 애플리케이션과 모든 의존성 애플리케이션을 다운로드한 보안 인시던트 응답 후 보안 인시던트 〉 분석가 작업 공간 설정 〉 설정 도우미.



3. 양식의 지침에 따라 기본 시스템을 구성합니다 보안 인시던트 응답 .
   좀 더 복잡한 설정 작업에 대한 자세한 내용은 필요에 따라 문서를 참조하십시오 설정 도우미 참조.

보안 분석가 작업 공간 다운로드 및 설치

인스턴스에서 새 UI를 보안 인시던트 응답 실행하려면 먼저 에서 ServiceNow# Store 다운로드하여 설치해야 합니다.

시작하기 전에
원활한 설치를 위해 인스턴스에 필요한 ServiceNow 역할이 있는지 확인하십시오. 예상 결과의 설치, 구성 및 검증에 필요한 역할은 다음과 같습니다.

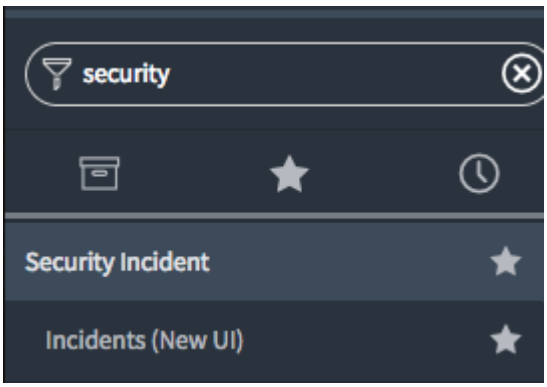
- 아직 할당되지 않은 경우 시스템 관리자 〔admin〕이 애플리케이션을 설치하고 보안 인시던트 응답 관리자 [sn_si.admin] 역할을 할당합니다.
- 보안 인시던트 응답 관리자 〔sn_si.admin〕는 구성을 감독하고 예상 결과를 검증합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필요한 역할: 관리자

프로시저

1. 다음에 대한 지침을 따릅니다. 에서 애플리케이션 다운로드 ServiceNow Store 보안 인시던트 응답 **UI** 애플리케이션을 설치합니다.
2. 설치가 완료되면 다음으로 이동하여 보안 분석가 작업 공간을 열 수 있습니다. 보안 인시던트 〉 인시던트(신규 **UI)**



보안 인시던트 응답와 함께 설치되는 구성요소

애플리케이션을 다운로드하고 활성화하면 보안 인시던트 응답 사용자 역할, 테이블, 속성, 예약된 작업을 포함한 여러 유형의 구성요소가 설치됩니다.

주:
애플리케이션 파일 테이블에는 이 애플리케이션과 함께 설치되는 구성요소가 나열됩니다. 이 테이블에 액세스하는 방법에 대한 지침은 애플리케이션과 함께 설치되는 구성요소 찾기 를 참조하십시오.

이 기능에 대한 데모 데이터를 사용할 수 있습니다.

설치되는 속성

시스템 관리자 [admin] 역할을 가진 사용자는 속성을 볼 수 있습니다. 보안 관리자 [sn_si.admin] 역할이 있는 사용자는 이를 수정할 수 있습니다.

속성	사용량
작업 공간 내의 관계 그래프 탭에 표시되는 기본 범주 노드입니다. 기본값은 관련 기록에 해당하는 테이블 이름을 나타냅니다. sn_si_aw.defaultCategories	• 유형: 문자열 • 기본값: sn_ti_m2m_task_observables,sn_si_m2m_task_affected_user,s
일정이 설정되지 않은 경우 모든 에이전트에 대한 기본 시작 시간(08:00 형식) sn_si.default.start.time	• 유형: 문자열 • 기본값: 08:00 • 위치: 보안 인시던트 〉 관리 〉 속성

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	사용량
일정이 설정되지 않은 경우 모든 에이전트에 대한 기본 종료 시간(17:00 형식) sn_si.default.end.time	• 유형: 문자열 • 기본값: 17:00 • 위치: 보안 인시던트 〉 관리 〉 속성
다른 컨텍스트 유형 옵저버블과 함께 대상 유형 옵저버블을 보안 인시던트 사용자 및 CI 관계에 포함 sn_si.link_dest_ip	컨텍스트 유형이 대상인 보안 인시던트 옵저버블을 구성 항목 또는 영 사용자 탭 아래에 표시할지 여부를 결정합니다. 기본적으로 대상 컨텍 옵저버블은 제외됩니다. 옵저버블을 포함하려면 Yes(예)를 선택합니
보안 인시던트에서 문제 또는 변경 요청을 생성할 때 사용자 지정 허용 sn_si.팝업	문제나 변경이 생성되면 이 속성은 요청을 수정하기 위한 팝업 창을 엽 이 속성이 **false**로 설정되면 문제 또는 변경 요청의 우선순위, 짧은 설 설명이 보안 인시던트와 동일하며 해당 필드를 추가하거나 편집할 수 없습니다. • 유형: true | false • 기본값: True • 위치: 보안 인시던트 〉 관리 〉 속성
사이팅 검색 결과를 CMDB의 CI와 연결합니다. sn_si.associate_ci_with_sighting_search	true로 설정하면 사이팅 검색 결과에 CMDB에 있는 관련 구성 항목이 • 유형: true | false • 기본값: True • 위치: 보안 인시던트 〉 관리 〉 속성
범위의 위험 점수가 0-49 형식으로 녹색으로 강조 표시됩니다. sn_si.risk.score.green	보안 인시던트 목록에서 위험 점수가 0에서 49 사이인 보안 인시던트 점이 표시됩니다.
범위의 위험 점수가 50-79 형식으로 주황색으로 강조 표시됩니다. sn_si.risk.score.orange	보안 인시던트 목록에서 위험 점수가 50에서 79 사이인 보안 인시던트 점이 표시됩니다.
범위의 위험 점수가 80-100 형식으로 빨간색으로 강조 표시됩니다. sn_si.risk.score.red	보안 인시던트 목록에서 위험 점수가 80에서 100 사이인 보안 인시던 빨간색 점이 표시됩니다.
이 매개변수는 이 기능을 구현한 사이팅 검색 구성을 활성화하거나 비활성화합니다. sn_si.enable_sighting_search	true로 설정하면 활성화된 통합에서 사이팅 검색을 수행할 수 있습니다 • 유형: true | false • 기본값: True • 위치: 보안 인시던트 〉 관리 〉 속성
사이팅 검색이 수행될 때 저장되는 원시 데이터의 행 수입니다. 범위 0-100	이 속성은 기본적으로 원시 데이터의 50개 행으로 설정됩니다. 결과 행 검색 시간 범위의 시작부터, 나머지 절반은 검색 시간 범위의 끝에서 보

개요 보기

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	사용량
sn_si.sighting_search_raw_data_rows	따라서 50개의 행을 선택하면 25개는 검색 시간 범위의 시작부터, 25 시간 범위의 끝에서 가져옵니다.
응답 작업이 진행 중으로 진행되면 인시던트 상태를 포함으로 자동 진행 sn_si.롤업_작업_상태	플로우 또는 워크플로우를 사용하는 동안 이 속성을 **false**로 설정하는 좋습니다. 이렇게 하면 플로우 또는 워크플로우 내에서 인시던트 상태 있습니다. 또한 한 인시던트 상태에서 다른 인시던트 상태로 전환하는 수 있는 상충을 방지할 수 있습니다. • 유형: true | false • 기본값: True • 위치: 보안 인시던트 〉 관리 〉 속성
보안 인시던트 응답에 대한 할당 속성	
위치 가중치 sn_si.위치.무게	보안 분석가를 자동으로 할당하는 데 사용할 기준을 계산할 때 사용되 등급입니다. 예를 들어 작업에 위치를 고려하면 위치 가중치 값이 보안 등급에 추가됩니다. • 유형: 정수 • 기본값: 10 • 위치: 보안 인시던트 〉 관리 〉 속성
기술 가중치 sn_si.기술.가중치	보안 분석가를 자동으로 할당하는 데 사용할 기준을 계산할 때 사용되 등급입니다. 예를 들어 작업에 대해 기술을 고려하는 경우 기술 가중치 분석가 등급에 추가됩니다. • 유형: 정수 • 기본값: 10 • 위치: 보안 인시던트 〉 관리 〉 속성
자동 할당에서 한 번에 처리할 보안 분석가의 최대 수 설정 sn_si.max.agents.processed	이 시스템의 절대 보안 분석가 수는 300명입니다. 300 초과를 지정하 수준으로 설정됩니다. 시스템은 구성된 값보다 많은 보안 분석가가 포 그룹에 대한 작업을 자동 디스패치할 수 없습니다. • 유형: 정수 • 기본값: 100 • 위치: 보안 인시던트 〉 관리 〉 속성
시간대 가중치 sn_si.timezone.weight	보안 분석가를 자동으로 할당하는 데 사용할 기준을 계산할 때 사용되 등급입니다. 예를 들어 작업에 보안 분석가 시간대를 고려하면 시간대 보안 분석가 등급에 추가됩니다. • 유형: 정수 • 기본값: 10 • 위치: 보안 인시던트 〉 관리 〉 속성
작업 종료 및 다음 이동 시작 사이에 추가하는 시간입니다(단위: 분).	유효한 시간 값의 예는 10입니다.

PDF 미리보기

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	사용량
sn_si.작업.간격	• 유형: 정수 • 기본값: 0 • 위치: 보안 인시던트 〉 관리 〉 속성
컨텐츠를 HTML로 렌더링하는 ## 태그를 포함하는 지정된 저널 필드입니다. sn_si.journal_field.html_enabled	• 유형: 문자열 • 기본값: work_notes, 설명 • 위치: 보안 인시던트 〉 관리 〉 속성
백그라운드에서 영향을 받는 서비스를 계산합니다. sn_si.refresh_impacted.event	영향을 받는 서비스/영향을 받는 CI 관련 목록은 이벤트를 통해 생성됩 옵션을 사용하면 새로 고침이 백그라운드에서 실행되고 인시던트에 보 추가됩니다. 백그라운드에서 작업을 수행하려면 값을 **true** 로 설정합니다. • 유형: true | false • 기본값: false • 위치: 보안 인시던트 〉 관리 〉 속성
미리 계산된 데이터에서 중요한 서비스를 검색합니다. sn_si.critical_service.calculator.use_cache	중요한 서비스 계산기에서 구성 항목의 미리 계산된 데이터를 사용할 합니다. 미리 계산된 데이터에서 조회하려면 값을 예 로 설정합니다. • 유형: true | false • 기본값: false • 위치: 보안 인시던트 〉 관리 〉 속성

기계번역

설치되는 역할

역할 이름 **[name]**	설명	포함하는 역할
보안 인시던트 관리자 [sn_si.admin]	모든 보안 인시던트 응답 데이터에 대한 완전한 제어. 또한 필요에 따라 영역과 기술을 관리합니다. 주: 기본 시스템에서 관리자는 sn_si.admin에 대한 액세스 권한도 갖습니다. 보안 인시던트 응답 한 명 이상의 다른 사용자에게 보안 관리자 역할이 할당되어 있는 한 관리자로부터 제한할 수 있습니다.	• assessment_admin • catalog_admin • decision_table_admin • decision_table_reader • filter_admin • flow_designer • pd_author • pd_content_author • pd_operator • skill_admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

역할 이름 **[name]**	설명	포함하는 역할
		• skill_model_admin • sn_si.analyst • sn_si.ingestion_profile_admin • sn_si.knowledge_admin • sn_si.manager • sn_sec_cmn.admin • sn_si.restriction_access_manag • sn_si.special_access_read_mana • sn_si.special_access_write_man • sn_ti.malicious_attachment_acc • sn_ti.observable.admin • tags_admin • template_admin • territory_admin • treemap_admin • user_admin
프로파일 관리자 [sn_si.ingestion_profile_admin]	플러그인을 구성하고 Splunk, Splunk ES 및 보안 운영용 Azure Sentinel 통합 애플리케이션에 대한 프로파일을 생성, 편집, 삭제 및 관리합니다. 주: sn_si.admin 역할은 기본적으로 필수 권한을 상속하므로 sn_si.admin 역할을 가진 사용자는 프로필 관리자가 사용할 수 있는 모든 작업을 수행할 수 있습니다. sn_si.ingestion_profile_admin 역할은 sn_si.admin이 사용자에게 할당할 수 있습니다.	해당 사항 없음
보안 인시던트 분석가 〔sn_si.분석가〕	보안 인시던트를 관리합니다. 기본 보안 액세스에 대한 기본 역할입니다. 이 역할을 가진 사용자는 보안 인시던트, 요청 및 작업은 물론 인시던트와 관련된 문제, 변경 및 중단을 생성하고 업데이트할 수 있습니다.	• pd_operator • snc_platform_rest_api_access • sn_msi.promoter • sn_msi.제안자

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

역할 이름 **[name]**	설명	포함하는 역할
		• sn_si.basic • sn_ti.malicious_attachment_acc
보안 인시던트 기본 〔sn_si.기본〕	기본 보안 액세스에 대한 기본 역할입니다. 이 역할을 가진 사용자는 보안 인시던트, 요청 및 작업은 물론 인시던트와 관련된 문제, 변경 및 중단을 생성하고 업데이트할 수 있습니다.	• canvas_user • document_management_user • email_composer • flow_operator • inventory_user • pa_viewer • service_fullfiller • skill_user • sn_sec_cmn.쓰기 • sn_si.read • sn_ti.observable.read • sn_ti.observable.write • sn_ti.읽기 • task_activity_writer • task_editor • treemap_user
CISO(최고 정보 보안 책임자) [sn_si.ciso]	CISO 대시보드를 보고 조작합니다. 또한 플러그인이 취약성 대응 활성화된 경우 이 역할을 가진 사용자는 대시보드에 취약성 유의성 정의 트리맵을 추가할 수 있습니다. 플러그인으로도 보안 인시던트 응답 동일한 작업을 수행할 수 있습니다.	• pa_viewer • sn_si.basic • sn_si.read
보안 인시던트 외부 〔sn_si.외부〕	특정 그룹에 속한 모든 보안 인시던트를 봅니다.	service_fulfiller

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

역할 이름 **[name]**	설명	포함하는 역할
	주: 다음 두 규칙은 범위가 지정된 관리자 또는 범위 지정 앱에 관계없이 적용할 ServiceNow 수 있습니다. • 그룹에 사용자를 추가하면 해당 그룹에도 역할이 할당됩니다. 마찬가지로 그룹에서 사용자를 제거하면 상속된 역할도 제거됩니다. • 모든 역할은 우선순위가 더 높은 역할에 의해 할당될 수 있습니다.	
보안 인시던트 통합 사용자 [sn_si.integration_user]	외부 도구는 새로운 보안 인시던트 기록을 제공하고 보안 인시던트 기록을 업데이트할 수 있습니다.	import_transformer
보안 인시던트 지식 관리자 [sn_si.knowledge_admin]	보안 인시던트 지식베이스에서 정보를 관리, 업데이트 및 삭제합니다.	• knowledge_admin • sn_si.read
보안 인시던트 관리자 〔sn_si.관리자〕	보안 분석가와 동일한 액세스 권한입니다.	• pd_author • pd_operator • sn_si.basic
보안 인시던트 읽기 〔sn_si.읽기〕	보안 인시던트를 읽습니다.	• canvas_user • sn_sec_cmn.읽기 • sn_templated_snip.template_sni • sn_ti.observable.read • workspace_user
보안 제한 액세스 관리자 〔sn_si.restriction_access_manager〕	사용자 또는 그룹이 보안 인시던트에 '제한 적용'을 할 수 있습니다. 이는 필드 변경에만 적용됩니다.	해당 사항 없음
보안 인시던트 특별 액세스 sn_si.special_access	보안 운영 조직 외부의 사용자에게 특정 보안 인시던트에 대한 액세스를 제공합니다.	해당 사항 없음
보안 특수 액세스 인에이블러 〔sn_si.special_access_enabler〕	보안 운영 조직 외부의 사용자에게 특정 보안 인시던트에 대한 특별 액세스 역할을 제공합니다.	해당 사항 없음
보안 인시던트 특수 액세스 읽기 관리자 〔sn_si.special_access_read_manager〕	보안 인시던트 특수 액세스 〔sn_si.special_access〕 역할을 관리합니다. 이 역할을 사용하여 보안 인시던트 양식의 읽기 액세스	sn_si.special_access_enabler

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

역할 이름 **[name]**	설명	포함하는 역할
	필드를 수정합니다. 이 역할은 sn_si.admin에 의해 할당됩니다.	
보안 인시던트 특수 액세스 작성자 관리자 〔sn_si.special_access_write_manager〕	보안 인시던트 특수 액세스 〔sn_si.special_access〕 역할을 관리합니다. 이 역할을 사용하여 보안 인시던트 양식의 권한 있는 액세스 필드를 수정합니다. 이 역할은 sn_si.admin에 의해 할당됩니다.	sn_si.special_access_enabler

설치되는 예약된 작업

예약된 작업	설명
보안 인시던트 옵저버블 조회	사용자 정의 일정에 따라 옵저버블 조회를 수행합니다.

설치되는 테이블

테이블	설명
뉴스 피드 구성 [sn_si_feed_configuration]	보안 인시던트 뉴스 피드에 표시되는 콘텐츠를 정의하는 데 사용되는 구성 기록입니다.
사후 인시던트 검토 할당 규칙 [sn_si_pir_condition]	보안 인시던트가 종결되면 사후 인시던트 검토 설문 조사 참가자 선택을 자동화합니다.
보안 인시던트 [sn_si_incident]	보안 인시던트, 인시던트에 대한 응답, 연결된 모든 작업, 변경 사항, 문제 및 이 보안 인시던트와 관련된 인시던트를 저장합니다.
보안 인시던트 공격 벡터 [sn_si_attack_vector]	공격 벡터 옵션.
보안 인시던트 감사 로그 [sn_si_audit_log]	보안 인시던트 보강 감사 로그를 저장합니다.
보안 인시던트 계산기 [sn_si_calculator]	특정 조건이 충족될 때 특정 보안 인시던트 필드를 설정하는 계산기입니다.
보안 인시던트 계산기 그룹 [sn_si_calculator_group]	보안 인시던트 계산기 그룹입니다. 계산기 그룹의 순서에 따라 가장 먼저 평가되는 그룹이 결정되며, 각 그룹에서 최대 하나의 계산기가 사용됩니다.
보안 인시던트 보강 방화벽 [sn_si_enrichment_firewall]	기본 테이블 (sn_sec_cmn_enrichment_data_base)에서 확장되며 Palo Alto Networks 방화벽과 관련된 모든 보강 기록을 포함합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테이블	설명
보안 인시던트 보강 맬웨어 결과 [sn_si_enrichment_malware]	기본 테이블 (sn_sec_cmn_enrichment_data_base)에서 확장되며 맬웨어와 관련된 모든 보강 기록을 포함합니다.
보안 인시던트 보강 네트워크 통계 [sn_si_enrichment_network_statistics]	기본 테이블 (sn_sec_cmn_enrichment_data_base)에서 확장되며 네트워크 통계와 관련된 모든 보강 기록을 포함합니다.
보안 인시던트 보강 실행 중인 프로세스 [sn_si_enrichment_running _processes]	기본 테이블 (sn_sec_cmn_enrichment_data_base)에서 확장되며 실행 중인 프로세스와 관련된 모든 보강 기록을 포함합니다.
보안 인시던트 보강 실행 서비스 [sn_si_enrichment_running_service]	기본 테이블 (sn_sec_cmn_enrichment_data_base)에서 확장되며 실행 중인 서비스와 관련된 모든 보강 기록을 포함합니다.
보안 인시던트 이메일 검색 [sn_si_m2m_incident_email_search]	이메일 검색 기록을 보안 인시던트에 매핑합니다.
보안 인시던트 임포트 [sn_si_incident_import]	보안 인시던트에 대한 테이블을 임포트합니다. 외부 시스템에서 보안 인시던트를 만드는 데 사용됩니다.
보안 인시던트 프로세스 정의 [sn_si_process_definition]	보안 인시던트 프로세스 플로우에 대한 구성을 저장합니다.
보안 인시던트 프로세스 정의 선택기 [sn_si_process_definition_selector]	보안 인시던트에 사용할 보안 인시던트 프로세스 정의를 저장합니다.
보안 인시던트와 관련된 고객 서비스 케이스 [sn_si_m2m_incident_customerservice_case]	고객 서비스 케이스 및 보안 인시던트를 매핑합니다.
보안 인시던트와 관련된 보강 데이터 [sn_si_m2m_incident_enrichment]	보안 인시던트 및 관련 보강 데이터 기록을 매핑합니다.
작업 보안 인시던트 응답개 [sn_si_task]	보안 인시던트 처리와 관련된 하위 작업을 관리합니다. 이러한 작업은 보안 담당자 또는 다른 부서의 사람에게 할당하여 부서 간 통신 및 작업 추적을 관리할 수 있습니다.
보안 인시던트 응답 작업 템플릿 [sn_si_task_template]	작업을 작성하는 보안 인시던트 응답 데 사용됩니다. 이러한 템플릿은 카탈로그 항목에 자주 사용되어 특정 유형의 보안 인시던트에 적합한 하위 작업 집합을 자동으로 만듭니다.
보안 인시던트 Runbook 문서 [sn_si_runbook_document]	보안 인시던트 조건 또는 필터를 지식 문서와 연결합니다. 보안 인시던트 정정을 위한 Runbook 절차를 지정하는 데 사용됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테이블	설명
보안 인시던트 템플릿 [sn_si_incident_template]	보안 인시던트를 만드는 데 사용됩니다. 이러한 템플릿은 종종 카탈로그 항목에서 사전 구축된 보안 인시던트를 만드는 데 사용됩니다.
보안 요청 [sn_si_request]	보안 팀에 대한 보안 관련 요청입니다.
보안 스캔 요청 [sn_si_scan_request]	위협 조회 요청입니다.
심각도 계산기 sn_si_severity_calculator	보안 인시던트의 심각도, 영향, 위험 및 중요도 값을 정의합니다.
작업에 영향을 받는 사용자 [sn_si_m2m_task_affected_user]	보안 인시던트와 영향을 받는 사용자를 연결하는 다대다 테이블입니다.
템플릿 워크플로우 활동 결과 평가자 [sn_si_wf_activity_outcome_evaluator]	평가 스크립트로 역량을 매핑합니다. 분석가가 수동으로 설정하는 대신 템플릿 워크플로우에 새 하위 플로우를 추가하여 응답 작업 결과를 설정할 수 있습니다.

기타 추가 보안 인시던트 응답 설정 작업

전역 도메인의 관리자인 경우 일상적인 작업의 처리 방법을 보안 인시던트 응답 구성합니다.

시작하기 전에
필요한 역할: sn_si.admin

주:

이러한 옵션은 많은 서비스 관리 애플리케이션에서 표준이므로 서비스 관리 용어를 사용합니다. 예를 들어 요청은 주 작업(즉, 보안 인시던트)에 사용되고 작업은 하위 작업 또는 응답 작업에 사용됩니다.

전역 도메인보다 낮은 도메인의 관리자인 경우 구성 화면을 볼 수 있지만 설정을 수정할 수는 없습니다.

프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 관리 〉 구성.
   애플리케이션을 구성하는 옵션은 다음 탭에서 구성됩니다.
   - 비즈니스 프로세스 탭에는 요청 수명주기 설정, 카탈로그와 요청 생성, 알림 구성 옵션이 있습니다.
   - 할당 탭에는 수동과 자동 할당을 설정하는 옵션이 있습니다.
   - 추가 기능 탭에는 지식베이스, 관리 대상 문서, 작업 활동을 사용하도록 설정하는 옵션이 있습니다.
2. 비즈니스 프로세스 탭의 필드에 내용을 입력합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

구성 화면 - 비즈니스 프로세스 탭

필드	설명
수명주기	
요청 또는 작업을 종결하거나 취소하려면 작업 메모가 필요함	보안 인시던트 또는 응답 작업을 종결하거나 취소하기 전에 사용자가 작업 메모를 입력하도록 요구하려면 이 옵션을 활성화합니다.
요청할 작업 메모 복사	응답 작업 작업 메모를 보안 인시던트의 작업 메모와 동기화하려면 이 옵션을 활성화합니다. 따라서 작업에 작업 메모가 추가되면 상위 보안 인시던트에 동일한 작업 메모가 나타납니다.
카탈로그 및 요청 생성	
인바운드 이메일을 통해 요청 작성 또는 업데이트	인바운드 이메일에서 보안 인시던트를 만들거나 업데이트하려면 이 옵션을 활성화합니다.
다음을 사용하여 요청이 생성됨	카탈로그나 정규 양식을 선택하여 카탈로그를 활성화하고 보안 인시던트 템플릿을 카탈로그에 자동으로 게시하도록 설정합니다. 카탈로그를 비활성화하고 보안 인시던트 템플릿이 카탈로그에 자동으로 게시되는 것을 비활성화하려면 정규 양식만을 선택합니다.
템플릿에서 전용 카탈로그 항목 작성	애플리케이션에 대한 카탈로그 항목의 자동 게시를 활성화하려면 이 옵션을 활성화합니다.
알림	
요청 또는 작업의 경우 선택한 필드가 변경되면 수신자에게 알림을 보냅니다.	보안 인시던트 및 응답 작업에서 선택한 필드가 변경될 때 특정 수신자에게 알림이 전송되도록 구성할 수 있습니다. **a.** 테이블에서요청(보안 인시던트 또는 작업(응답 작업)을 선택합니다. **b.** 필드에서 알림을 생성하는 데 사용할 필드를 선택합니다. 선택한 필드가 변경되면 식별된 수신자에게 알림이 전송됩니다. **c.** 수신자에서 하나 이상의 수신자를 선택합니다. **d.** 특정 사용자 또는 특정 그룹을 선택하면 사용자 또는 그룹을 선택하는 메시지가 사용자에게 표시됩니다. **e.** 다른 필드나 수신자를 사용하여 더 많은 알림을 정의하려면 다음 알림 설정 집합에 대해 이전 단계를 반복합니다. **f.** 알림을 제거하려면 알림 ⊖ 아이콘을 클릭합니다.

3. 할당 탭을 클릭하고 필드를 채웁니다.

구성 화면 – 할당 탭

필드	설명
요청에 대한 할당 방법	보안 인시던트 할당 방법을 선택합니다. ○ 자동 할당 사용: 보안 인시던트가 자동으로 할당됩니다. ○ 워크플로우 사용: 선택한 워크플로우가 보안 인시던트를 할당합니다. ○ 수동으로: 보안 인시던트를 수동으로 할당합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
이 워크플로우를 사용하여 요청 할당	보안 인시던트를 디스패치하기 위한 워크플로우를 선택합니다. 이 필드는 요청에 대한 할당 방법 목록에서 워크플로우 사용이 선택될 때 나타납니다.
작업에 대한 할당 방법	대응 작업을 할당할 방법을 선택합니다. ○ 자동 할당 사용: 응답 작업이 자동으로 할당됩니다. ○ 워크플로우 사용: 선택한 워크플로우가 응답 작업을 할당합니다. ○ 수동으로: 응답 작업이 수동으로 할당됩니다.
이 워크플로우를 사용하여 작업 할당	응답 작업을 할당하기 위한 워크플로우를 선택합니다. 이 필드는 작업 할당 방법 목록에서 워크플로우 사용이 선택될 때 나타납니다.
평가 그룹 범위 영역을 기준으로 요청 또는 작업 할당	이 옵션을 사용하여 보안 인시던트 및 응답 작업의 할당을 작업 위치를 담당하는 그룹으로 제한합니다.
스케줄링	
에이전트의 자동 선택은 작업에 대한 시간대를 고려함	작업을 할당할 때 에이전트의 시간대를 고려하려면 이 옵션을 활성화합니다. 보안 인시던트 또는 응답 작업에 대해 자동 할당을 선택하면 이 필드가 나타납니다.
추가 요인	
에이전트의 자동 선택은 에이전트의 위치를 고려함	작업을 할당할 때 작업 위치에 더 가까운 에이전트를 우선적으로 사용하려면 이 옵션을 활성화합니다. 보안 인시던트 또는 응답 작업에 대해 자동 할당을 선택하면 이 필드가 나타납니다.
작업에 대한 에이전트의 자동 선택을 사용하려면 에이전트가 기술을 보유해야 함	자동 할당을 결정할 때 에이전트의 기술을 작업과 일치시켜야 하는 정도를 선택합니다. ○ 할당된 에이전트가 작업을 수행하는 데 필요한 모든 기술을 보유하도록 요구하려면 모두를 선택합니다. 기술이 하나라도 부족한 에이전트는 제거됩니다. ○ 작업을 수행하는 데 필요한 대부분의 기술을 보유한 에이전트를 원하면 일부를 선택합니다. ○ 기술을 고려하지 않고 에이전트를 자동으로 할당하려면 없음을 선택합니다. 보안 인시던트 또는 응답 작업에 대해 자동 할당을 선택하면 이 필드가 나타납니다.
자동 선택을 통해 동일한 에이전트를 요청의 모든 작업에 할당하려고 함	보안 인시던트에 대한 모든 응답 작업을 동일한 에이전트에 자동으로 할당하려면 이 옵션을 활성화합니다.

4. 추가 기능 탭을 클릭하고 필드를 채웁니다.

구성 화면 — 추가 기능 탭

필드	설명
설명서	
전용 지식베이스 (KB) 사용	에 대한 보안 인시던트 응답지식베이스를 활성화하려면 이 옵션을 활성화합니다.
관리 대상 문서 사용	관련 목록을 관리 대상 문서에 추가하려면 이 옵션을 활성화합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
작업 활동 사용	전화 통화 및 이메일 메시지와 같은 작업 상호작용 및 통신을 기록하려면 이 옵션을 활성화합니다.

5. 저장을 클릭합니다.

보안 관리 잠금

조사를 보호하고 보안 인시던트를 비공개로 유지하기 위해 보안 관련 역할 및 ACL에 대한 액세스를 제한할 보안 인시던트 응답 수 있습니다. 비보안 관리자는 명시적으로 허용하지 않는 한 액세스가 제한될 수 있습니다.

시작하기 전에

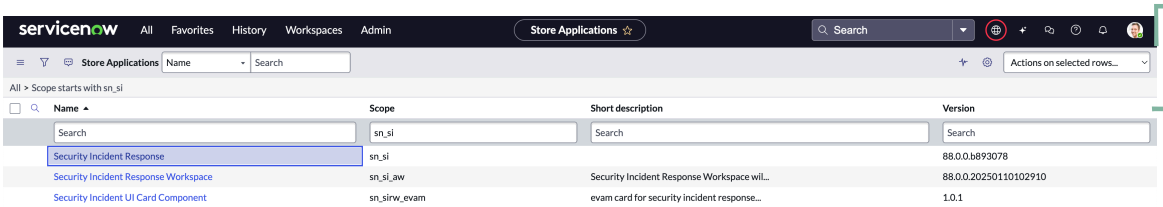
보안 인시던트 응답 애플리케이션이 활성화되면 시스템 관리자 사용자에게 기본적으로 sn_si.admin 역할이 부여됩니다. 시스템 관리자는 보안 그룹 및 사용자를 설정할 수 있는 유일한 관리자입니다.

기능 및 기록에 보안 인시던트 응답 액세스하려면 보안 역할이 필요합니다.

필요한 역할: sn_si.admin

프로시저

1. 플러그인이 보안 인시던트 응답 활성화되면 관리자 역할의 사용자는 한 명 이상의 사용자에게 범위 지정 관리자(sn_si.admin) 역할을 할당합니다.
2. 관리자 역할을 가진 사용자가 보안 인시던트 범위로 변경됩니다.
3. 다음으로 이동 모두 〉 **sys_store_app.list**.
4. 범위 필드에 **sn_si** 입력합니다.



5. 보안 인시던트 응답을 클릭합니다.
6. 아래로 스크롤하여 관련 링크로 이동하고 관리자에게 포함된 역할에서 제거를 클릭합니다.
7. 로그아웃했다가 다시 로그인합니다.
   관리자 사용자는 애플리케이션에 액세스할 보안 인시던트 응답 수 없습니다.

관련 정보

애플리케이션 관리

제한된 호출자 접근 관리

RCA(제한된 호출자 접근) 기능을 사용하면 관리자가 애플리케이션 또는 애플리케이션 자원에 대한 교차 범위 액세스를 정의하고 액세스 요청을 허용하거나 거부할 수 있습니다. 이 기능은 보안 분석가가 중요한 보안 관련 정보를 보호할 수 있도록 기본적으로 활성화되어 보안 인시던트 응답 있습니다.

호출자 접근이라는 필드가 의 모든 테이블 및 스크립트 포함보안 인시던트 응답에 추가되었으며 필드는 기본적으로 호출자 추적으로 설정됩니다. 이 설정은 애플리케이션 범위에서 테이블 및 스크립트 포함에 액세스할 수 보안 인시던트 응답 있음을 의미합니다. 그러나 추적 레코드는 각

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

레코드에 대해 생성되고 제한된 호출자 접근 권한 [sys_restricted_caller_access] 테이블에 저장됩니다.

주:
기록을 호출자 추적에서 호출자 제한으로 변경할 때 주의하십시오. 이 상태의 기록은 관리자가 수동으로 액세스를 허용할 때까지 액세스할 수 없습니다. 관리자는 다음으로 이동해야 합니다. 시스템 애플리케이션 〉 애플리케이션 제한된 호출자 접근, 액세스가 요청된 테이블 또는 스크립트 포함을 찾은 다음 상태 필드를 요청됨 에서 허용됨으로 변경합니다.

관련 정보

제한된 호출자 접근 권한 설정

애플리케이션 범위, 애플리케이션 자원 및 이벤트 액세스 설정

보안 인시던트 응답에 대한 빠른 시작 테스트 실행

업그레이드 적용 또는 애플리케이션 개발과 같이 구성 변경 후에도 보안 인시던트 응답가 계속 작동하는지 확인합니다. 인스턴스별 데이터를 사용할 때 통과하도록 이러한 빠른 시작 테스트를 복사하여 사용자 지정합니다.

보안 인시던트 응답 빠른 시작 테스트를 하려면 보안 인시던트 응답 플러그인 (com.snc.security_incident)을 활성화하고 데모 데이터를 로드해야 합니다.

보안 인시던트 응답 테스트

테스트	설명	릴리스 버전
SIR: 보안 인시던트 생성	사용자가 보안 인시던트 양식에서 보안 인시던트를 성공적으로 만들 수 있는지 여부를 결정합니다.	Madrid
SIR: 보안 인시던트 카탈로그를 통해 보안 인시던트 생성	사용자가 카탈로그에서 보안 인시던트를 성공적으로 만들 수 있는지 여부를 결정합니다.	Madrid
SIR: 보안 인시던트 수명주기	정책 위반 워크플로우의 응답 작업을 확인합니다.	Madrid
SIR: PIR 평가 OOTB 구성 테스트	이 테스트를 사용하여 PIR 평가 및 기본 시스템 구성의 유효성을 확인합니다.	Tokyo
SIR: PIR 평가 조건부 구성 테스트	사후 인시던트 평가를 완료하지 않으면 필수 조건 규칙과 일치하는 보안 인시던트가 종결되지 않는지 확인합니다. 사후 인시던트 평가를 완료하지 않고도 선택적 조건 규칙과 일치하는 보안 인시던트를 종결할 수 있는지 확인합니다. 어떤 규칙과도 일치하지 않는 보안 인시던트에 대해서는 평가가 생성되지 않는지 확인합니다.	Tokyo

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 인시던트 응답 테스트

테스트	설명	릴리스 버전
SIR: PIR 실행 시간 경험	PIR 보고서가 새 설계에 따라 구성되어 보안 인시던트에 첨부되어 있는지 검증합니다.	Tokyo
SIR: PIR 설계 시간 경험	관리자 구성에 따라 보안 인시던트가 보고서 템플릿과 매핑되어 있는지 검증합니다.	Tokyo
SIR: 보안 인시던트를 기존의 중요 보안 인시던트와 연결	보안 인시던트를 기존의 중요 보안 인시던트에 연결하고 중요 보안 인시던트로 롤업된 보안 인시던트의 데이터를 확인합니다.	Tokyo
SIR: 보안 인시던트를 중요 보안 인시던트로 승격	보안 인시던트를 중요 보안 인시던트로 승격하고 중요 보안 인시던트로 롤업된 보안 인시던트의 데이터를 확인합니다.	Tokyo
SIR: 보안 인시던트를 중요 보안 인시던트로 제안	보안 인시던트를 중요 보안 인시던트로 제안하고 중요 보안 인시던트로 롤업된 보안 인시던트의 데이터를 확인합니다.	Tokyo
SIR: 보안 인시던트 수명주기	정책 위반 응답 작업 워크플로우로 보안 인시던트 수명주기를 확인합니다.	Yokohama
SIR: 보안 케이스 생성	보안 인시던트 양식에서 보안 케이스를 생성합니다.	Yokohama
제한 적용이 켜지면 허용된 구성원만 보안 인시던트에 액세스할 수 있는지 확인합니다.	제한 적용이 활성화되면 허용된 구성원만 보안 인시던트에 액세스할 수 있는지 확인합니다.	Yokohama
"제한 적용"으로 활성화된 보안 인시던트가 어떤 사용자에게도 표시되지 않는지 확인	"제한 적용"이 활성화된 보안 인시던트가 어떤 사용자에게도 표시되지 않는지 확인합니다.	Yokohama
읽기 액세스 확인	보기 액세스 권한을 확인합니다.	Yokohama
쓰기 액세스 확인	편집 액세스 권한을 확인합니다.	Yokohama
SIR 작업 공간: 읽기 액세스	읽기 액세스 사용자가 작업 공간에서도 보안 역할이 없이도 보안 인시던트를 볼 수 있는지 확인합니다.	Yokohama
SIR 작업 공간: 쓰기 권한	쓰기 액세스 사용자가 보안 역할 없이 보안 인시던트를 업데이트할 수 있는지 확인합니다.	Yokohama

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 인시던트 응답 테스트

테스트	설명	릴리스 버전
SIR 작업 공간: 새 보안 인시던트 생성	작업 공간에서 새 보안 인시던트를 생성합니다.	Yokohama
SIR 작업 공간: 응답 작업 생성	기존 보안 인시던트에서 새 응답 작업을 생성합니다.	Yokohama
보안용 Now Assist: 활성 보안 인시던트 요약	활성 보안 인시던트를 요약하고 표시된 섹션의 유효성을 확인합니다.	Zurich
보안용 Now Assist: 작업 메모에 Summarization_Share된 보안 인시던트	생성된 요약을 작업 메모에 공유합니다.	Zurich
보안용 Now Assist: 종결된 보안 인시던트 요약	종결된 보안 인시던트를 요약하고 표시된 섹션을 확인합니다.	Zurich

관련 정보

빠른 시작 테스트

설정 도우미 참조

설정 도우미는 기본 시스템을 설정하기 보안 인시던트 응답 위해 수행해야 하는 단계를 안내합니다. 이 섹션에서는 자세한 설명이 필요할 수 있는 복잡한 단계에 대한 추가 정보를 제공합니다.

보안 인시던트 응답 프로세스 정의 생성

보안 인시던트가 한 상태에서 다음 상태로 전환하는 방식을 정의하는 프로세스 정의를 생성할 수 있습니다. 프로세스 정의는 서비스 데스크와 최종 사용자에게 수명주기 동안 문제를 추적하는 데 도움을 줍니다.

시작하기 전에
필요한 역할: sn.si_admin

프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 관리 〉 프로세스 정의.
2. 새로 만들기를 클릭합니다.
3. 필드에 적절한 정보를 입력합니다.

프로세스 정의 생성

필드	설명
이름	스크립트 포함 파일에 인코딩된 프로세스를 설명하는 기록의 이름입니다. 이름은 프로세스 정의 선택기 목록에 선택 항목으로 표시됩니다.
스크립트 포함	프로세스의 정의를 포함하는 스크립트 포함의 이름(sn_si. 접두사 포함)입니다. 스크립트는 sn_si(보안 인시던트) 애플리케이션 범위에 있어야 합니다. 자세한 내용은 사용자 지정 보안 인시던트 응답 프로세스 정의 스크립트 포함

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	생성 문서를 참조하십시오. 이 필드에 유효한 스크립트 포함 이름이 포함되어 있지 않으면 기본 ProcessDefinition_NIST_Stateful 정의가 사용됩니다.
설명	스크립트 포함에 대한 유용한 정보입니다.
순서	프로세스 정의 목록에서의 위치를 결정합니다.
활성	선택하면 프로세스 정의 선택기 페이지에서 이 프로세스 정의를 선택할 수 있습니다.

4. 제출을 클릭합니다.

관련 정보

보안 인시던트 응답 프로세스 선택

Security Incident Response 프로세스 정의 이해

Security Incident Response 프로세스 정의 이해

보안 인시던트 응답 프로세스 정의 상태 플로우를 대체하고 최종 사용자와 서비스 데스크에 문제의 상태를 제공합니다. 프로세스 정의는 수명주기를 통해 문제를 추적하는 데 도움이 됩니다. 보안 인시던트 응답 는 고유한 상태 세트가 있는 SM(서비스 관리) 애플리케이션입니다. 잘못된 상태는 의 프로세스 선택일부로 보고됩니다.

보안 인시던트 응답 프로세스 정의

기본 프로세스 정의(NIST 상태 저장)는 다음과 같은 인시던트 상태를 정의합니다.

주:
사용 가능한 상태는 인시던트의 현재 상태에 따라 달라집니다.

보안 인시던트 프로세스 정의 상태

상태	설명
초안	요청 개시자가 보안 인시던트에 대한 정보를 추가하지만 아직 처리할 준비가 되지 않았습니다.
분석	인시던트가 할당되었고 문제를 분석하는 중입니다.
포함	문제가 확인되었으며 보안 직원이 이를 억제하고 피해 통제를 수행하기 위해 노력하고 있습니다. 이러한 작업에는 서버를 오프라인으로 전환하고, 장비를 인터넷에서 분리하고, 백업이 있는지 확인하는 작업이 포함될 수 있습니다.
근절	문제가 억제되었으며 보안 직원이 문제를 해결하기 위한 조치를 취하고 있습니다.
복구	문제가 해결되고 영향을 받는 시스템의 운영 준비 상태가 검증되고 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 인시던트 프로세스 정의 상태

상태	설명
검토	보안 인시던트가 완료되고 모든 시스템이 정상 작동 상태로 돌아왔지만 여전히 사후 인시던트 검토가 필요합니다.
종결됨	인시던트가 완료되었지만 보안 인시던트를 종결하려면 먼저 종결 처리 정보 탭의 정보를 입력해야 합니다.

보안 인시던트 작업 프로세스 정의

다음 프로세스 정의는 보안 인시던트 작업에 사용됩니다.

작업 프로세스 정의 상태

상태	설명
준비	작업이 에이전트에 할당되면 작업할 준비가 됩니다.
할당됨	작업이 에이전트에게 할당됩니다.
작업 진행 중	할당된 에이전트가 작업을 수행 중입니다.
완료	작업이 완료되었습니다.
취소됨	작업이 취소되었습니다.

NIST는 다음 두 가지 모델을 지원합니다.

- **NIST** 상태 저장

  이 프로세스 정의를 사용하면 분석가가 단계를 건너뛰지 않고 한 상태에서 다른 상태로 순차적으로 이동할 수 있습니다. 예를 들어 분석가가 초안 상태로 시작하는 경우 이 프로세스 정의의 순차 순서는 초안>분석>포함>근절>복구입니다. 따라서 NIST 상태 저장 프로세스 정의는 단방향이며 분석가는 정방향 상태로만 진행할 수 있습니다.

  또 다른 예로, 분석가가 분석 상태로 시작하는 경우 이 프로세스 정의의 순차 순서는 분석>포함>근절>복구입니다.

- **NIST** 오픈

  이 프로세스 정의를 통해 분석가는 한 상태에서 다른 상태로 앞으로 또는 뒤로 이동할 수 있습니다. 예를 들어 분석가가 분석 상태로 시작하는 경우 프로세스 정의의 순서는 분석>포함>근절>복구 또는 분석>초안일 수 있습니다. 따라서 NIST Open 프로세스 정의는 양방향이며 분석가가 요구 사항에 따라 정방향 또는 역방향 상태로 이동할 수 있습니다.

보안 인시던트 응답 프로세스 선택

보안 인시던트 응답 프로세스 선택 보안 인시던트 및 응답 작업에 대해 잘못된 상태가 있는 프로세스를 나열합니다.

관리자는 수동으로 또는 스크립트를 사용하여 인시던트나 작업을 올바른 상태로 수정할 수 있습니다. 관련 목록이 비어 있으면(인시던트 없음, 작업 없음) 모든 활성 작업이 유효한 상태임을 나타냅니다. 사용 가능한 상태는 인시던트의 현재 상태에 따라 달라집니다. 자세한 내용은 프로세스 정의를 사용하여 잘못된 보안 인시던트 또는 작업 상태 정정 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 인시던트 응답 프로세스 정의 선택

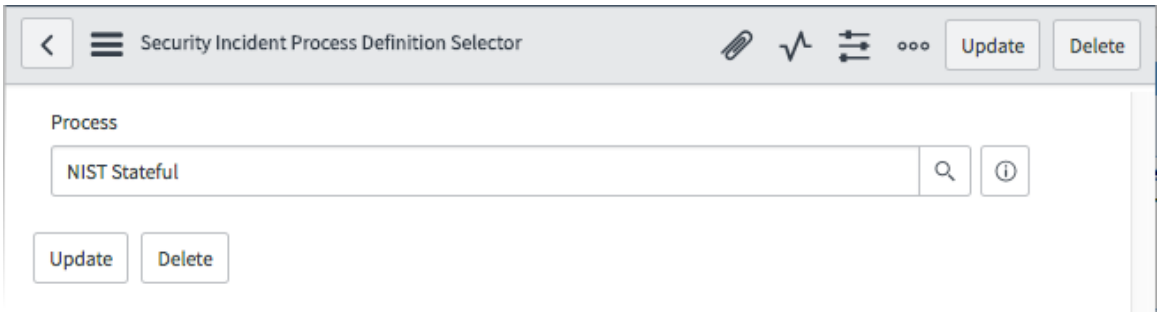
회사 보안 인시던트 및 응답 작업의 적절한 상태에 사용할 프로세스 정의를 선택할 수 있습니다.

시작하기 전에
필요한 역할: admin 및 sn_si.admin

이 태스크 정보

프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 응답 〉 관리 〉 프로세스 선택.
2. 사용 가능한 프로세스 정의를 나열하려면 검색 아이콘을 클릭합니다.



3. 프로세스 정의를 선택합니다.
4. 업데이트를 클릭합니다.

사용자 지정 보안 인시던트 응답 프로세스 정의 스크립트 포함 생성

회사 보안 인시던트 및 응답 작업의 적절한 상태에 대한 사용자 지정 프로세스 정의 스크립트를 만듭니다.

시작하기 전에
필요한 역할: sn_si.admin

이 태스크 정보
sn_si. ProcessDefinition 메인 스크립트에는 컨트롤, 프로세스 정의가 포함됩니다. 프로세스 정의 는 사용 중인 정의를 결정합니다(프로세스 선택 사용). 적절한 스크립트 포함 파일을 호출하여 보안 인시던트와 응답 작업 모두에 대한 초기 상태와 전환을 확인합니다.

프로시저

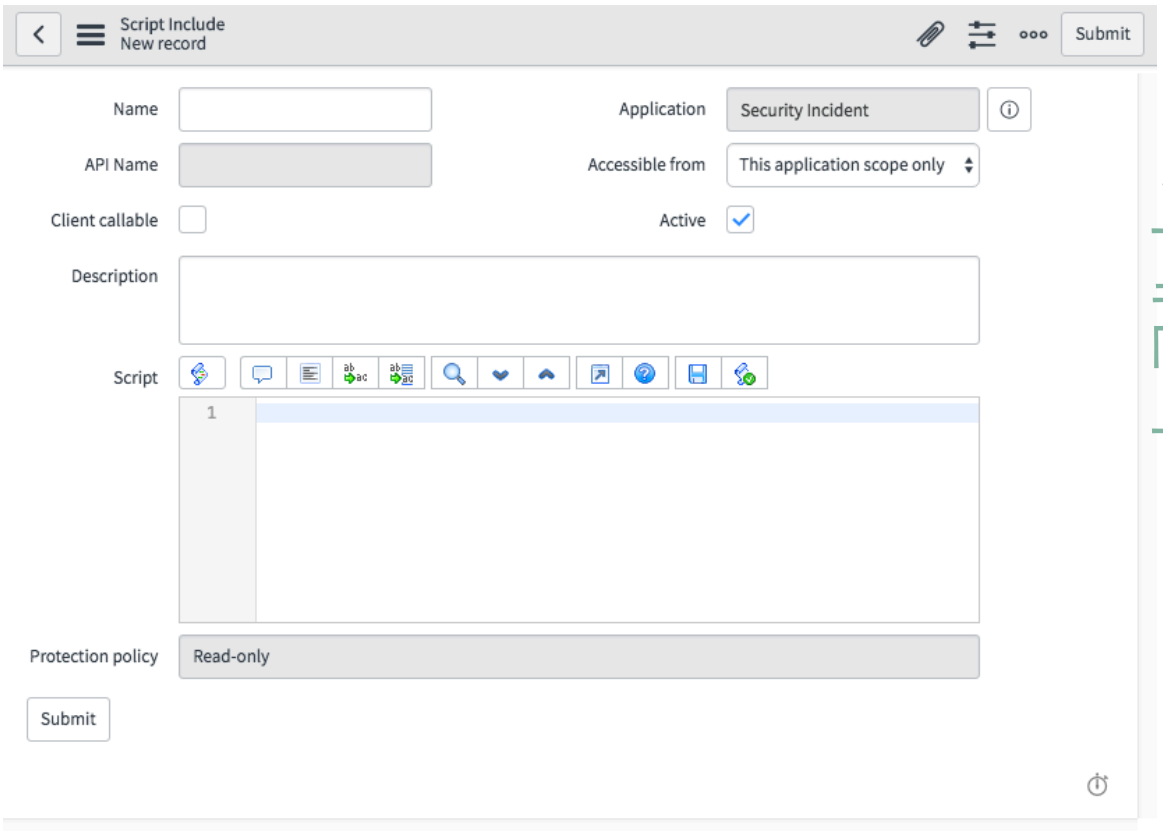
1. 다음으로 이동 모두 〉 시스템 정의 〉 스크립트 포함.
2. 새로 만들기를 클릭합니다.
3. 필드에 적절한 정보를 입력합니다.

프로세스 정의 생성

필드	설명
이름	이 스크립트 포함의 이름입니다.
API 이름	스크립트 포함의 이름을 기반으로 생성됩니다.
클라이언트 호출 가능	스크립트 포함을 클라이언트 스크립트, 목록 및 보고서 필터, 참조 한정자 또는 지정된 경우 URL의 일부로 사용할 수 있도록 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
애플리케이션	보안 인시던트
다음에서 접근 가능	이 애플리케이션 범위만을 선택하십시오.
활성	선택하면 프로세스 정의 페이지에서 이 스크립트 포함을 선택할 수 있습니다.
설명	스크립트 포함에 대한 유용한 정보입니다.
스크립트	다른 스크립트에서 호출될 때 실행할 서버 측 스크립트를 정의합니다. 스크립트는 단일 JavaScript 클래스 또는 전역 함수를 정의해야 합니다. 클래스 또는 함수 이름은 이름 필드와 일치해야 합니다. 스크립트 내용에 대한 자세한 내용은 다음 문서를 참조하십시오 프로세스 정의 스크립트 포함.



4. 제출을 클릭합니다.

관련 정보

프로세스 정의 스크립트 포함

프로세스 정의 스크립트 포함

프로세스 정의 스크립트 포함은 프로세스 정의를 정의하기 위한 메서드를 제공합니다.

여기에 설명된 상수, 속성, 배열 및 메서드 호출을 구현하여 프로세스 정의 스크립트 포함을 사용자 지정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용처

이 스크립트 포함을 사용하여 프로세스 정의를 생성합니다.

스크립트 포함 본문

스크립트 포함 본문은 다음 세 개의 섹션으로 구성됩니다.

- 상수: 초기 상태 정의
- 보안 인시던트 및 응답 작업: 프로세스 정의 배열
- 메서드 호출: 정보 검색

상수

상수는 보안 인시던트 및 응답 작업의 초기 상태를 정의하는 데 사용됩니다.

상수의 사용은 선택 사항이지만 가독성을 위해 권장됩니다. 예:

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

나중에 다음 메서드에서 사용됩니다.

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

다음 상수 세트는 보안 인시던트와 응답 작업 모두의 상태를 정의합니다.

각 배열에는 인시던트나 작업이 특정 상태에 있을 때 사용할 수 있는 상태에 대한 정의도 포함되어 있습니다.

예:

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

예제는 객체 배열입니다. 각 객체는 상태와 가능한 전환 상태를 정의합니다.

상태 객체의 순서에 따라 원하는 플로우 순서가 결정됩니다.

작업이 '초안' 상태(값 1)인 경우 가능한 상태는 1(초안, 변경 없음) 및 10(준비, 프로세스의 다음 단계)입니다.

상태를 벗어나는 전환 횟수에는 제한이 없습니다. '종결 완료' 및 '취소됨' 상태는 최종 상태이므로 가능한 상태 전환이 없습니다.

개체의 특성 순서는 중요하지 않습니다. 정의가 더 명확해지면 레이블을 먼저 넣으십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성

상태 정의 객체의 필수 속성은 다음과 같습니다.

- 상태: 상태의 숫자 값
- 레이블: 상태와 관련된 사람이 읽을 수 있는 텍스트
- 선택: 상태가 전환될 수 있는 상태 값의 배열(상태 드롭다운의 콘텐츠 결정)

선택적 속성은 다음과 같습니다.

- 필수: 이 상태에서 필수가 되는 필드 ID의 목록
- 읽기 전용: 이 상태에서 읽기 전용이 되는 필드 ID의 목록입니다.
- visible: 이 상태로 표시되는 필드 ID의 목록
- notmandatory: 이 상태에서 필수가 아닌 필드 ID의 목록
- notVisible: 이 상태에서 더 이상 표시할 수 없는 필드 ID의 목록

주:

선택적 속성이 사용되는 경우 상태 간에 필드가 적절하게 표시/표시되지 않음, 필수/필수가 아님, 표시/숨김 또는 읽기 전용이 되도록 하는 것은 작성자의 책임입니다.

예를 들어, 한 상태에서 필드를 숨기면 'visible' 속성을 사용하지 않는 한 나중에 다른 상태로 표시되지 않습니다.

프로세스 흐름 정의 배열

프로세스 플로우 포매터(보안 인시던트 및 응답 작업 양식 상단의 막대)에 표시되는 정보를 정의하려면 시스템에서 각 상태에 대해 표시할 내용에 대한 정보가 필요합니다.

예:

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

TASK_PF 배열은 프로세스 포매터 표시줄에 표시되는 텍스트(순서 및 활동 포함)를 결정하는 데 사용되는 레이블, 조건 및 설명의 컬렉션입니다.

이 예에서 '준비' 텍스트는 표시된 두 번째 항목입니다. 작업이 '상태=10^EQ' 조건을 충족하면 강조 표시됩니다.

포인터가 텍스트 위에 있으면 '보안 인시던트 대응 작업을 할당할 준비가 되었습니다'라는 설명이 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

상태를 단일 포매터 상태로 결합할 수 있습니다.

이 예에서는 '종결 완료' 상태와 '취소됨' 상태가 모두 상단 표시줄에 '종결됨'으로 표시됩니다.

메서드 호출

다음 메서드는 sn_si에서 사용되므로 스크립트 포함에 있어야 합니다. 프로세스 정의:

수익 유형	메서드 요약	설명
문자열	getInitialIncidentState: 함수 ()	초기 인시던트 상태 숫자 값 반환
문자열	getInitialTaskState: 함수():	초기 작업 상태 숫자 값 반환
문자열 배열	getIncidentStates: 함수():	인시던트 상태 배열 반환
문자열 배열	getTaskStates: 함수():	작업 상태의 배열 반환
객체 배열	getIncidentProcessFlows: 함수():	인시던트 프로세스 흐름 정의 배열 반환
객체 배열	getTaskProcessFlows: 함수():	작업 프로세스 흐름 정의 배열 반환

다음 메서드 집합은 인시던트나 작업이 업데이트될 때마다 호출되며 특정 변경 전환에 대해 수행할 수 있는 작업을 허용합니다.

수익 유형	메서드 요약	설명
void	performIncidentStateChange: 함수(현재, 이전)	예제에서 이 방법은 SM 관련 값을 설정하고 누군가가 할당되었을 때 인시던트가 "초안"에서 벗어나도록 하는 데 사용됩니다.
void	performTaskStateChange: 함수(현재, 이전)	이 예에서는 타임스탬프(할당 및 종결 시)를 업데이트하고 assigned_to 필드가 채워지면 작업을 '준비'에서 '할당됨'으로 진행하기 위해 이 방법을 사용합니다.

비즈니스 규칙을 사용하면 이 두 가지 방법으로 수행되는 동일한 작업을 수행할 수 있습니다. 스크립트 포함에서 정의하면 프로세스 정의 전환이 더 쉬워집니다.

프로세스 정의를 사용하여 잘못된 보안 인시던트 또는 작업 상태 정정

관리자는 수동으로 또는 스크립트를 사용하여 보안 인시던트 또는 작업을 올바른 상태로 수정할 수 있습니다. 사용 가능한 상태는 인시던트의 현재 상태에 따라 달라집니다.

시작하기 전에
필요한 역할: 관리자

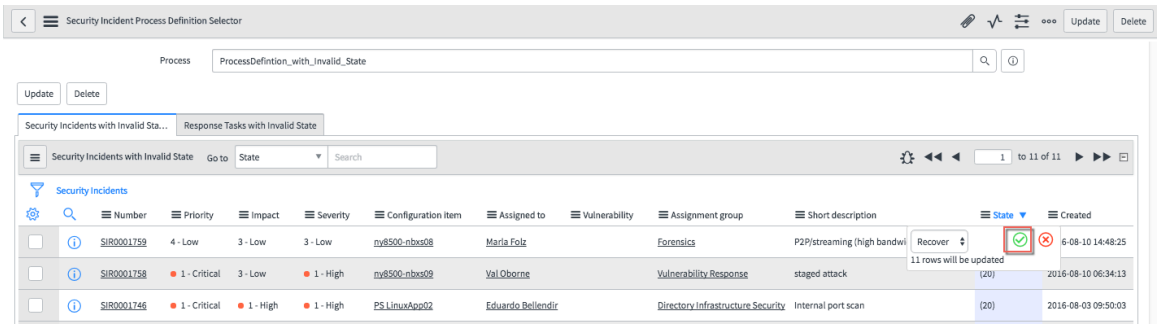
이 태스크 정보
프로세스 정의를 전환한 후 새 정의가 일부 이전 상태를 지원하지 않을 수 있습니다. 고아 상태의 인시던트 또는 작업 상태를 수정하려면 프로세스 정의를 변경하거나, 스크립트 포함을 편집하거나, 각 인시던트 또는 작업을 수동으로 열어 상태를 업데이트할 수 있습니다. 일반적으로 상태 업데이트(대량으로 수행할 수 있음)가 가장 쉬운 솔루션입니다.

상태를 대량으로 변경하려면 다음을 수행합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 프로세스 선택.
2. 변경하려는 인시던트나 작업의 상태 필드를 강조 표시합니다.
3. 첫 번째 기록의 상태 필드를 두 번 클릭하고 새 상태를 선택한 다음 녹색 확인 표시( )를 클릭하여 변경을 완료합니다.



4. 업데이트를 클릭합니다.

보안 인시던트 그룹 생성

보안 인시던트 그룹을 설정하고 적절한 역할과 사용자를 그룹에 할당합니다.

시작하기 전에

필요한 역할:

- user_admin 역할이 있는 경우 보안 인시던트 할당 그룹을 만들 수 있습니다.
- sn_si.admin 역할이 있는 경우 보안 인시던트 할당 그룹을 생성하고 편집할 수 있습니다.

이 태스크 정보

그룹의 사용자는 그룹의 역할을 상속하므로 각 사용자에게 개별적으로 역할을 할당할 필요가 없습니다.
조직에서 필요한 만큼 그룹을 생성하는 것이 좋습니다. 또한 관리자용 그룹을 하나 생성한 다음 이 그룹에만 관리자 역할을 할당하는 것이 좋습니다.

프로시저

1. 다음으로 이동 모두 〉 사용자 관리 〉 그룹 또는 보안 인시던트 〉 설정 〉 그룹.
2. 새로 만들기를 클릭합니다.
3. 양식에서 필드를 채웁니다.

   주:

   자세한 내용은 사용자 그룹 만들기를 참조하세요.

4. 이 그룹에 대한 보안 인시던트 유형을 선택해야 합니다.
   a. 유형 필드가 표시되지 않으면 양식을 구성하여 추가합니다 .
   b. 유형 필드 옆에 있는 잠금 아이콘을 클릭합니다.
   c. 참조 조회 아이콘(조회)을 클릭합니다.
   d. 보안 인시던트 유형을 검색하여 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. 양식 헤더를 마우스 오른쪽 버튼으로 클릭하고 저장을 선택합니다.
6. 역할 관련 목록에서 이 그룹의 각 구성원이 받는 역할을 추가합니다.
   예를 들어 팀 구성원에 대한 보안 인시던트 응답 그룹을 만드는 경우 sn_si.analyst를 추가합니다.
   관리자용 보안 인시던트 응답 그룹을 만드는 경우 sn_si.admin을 추가합니다.
7. 그룹 구성원 관련 목록에서 이 그룹에 사용자를 추가합니다.
8. 업데이트를 클릭합니다.

보안 인시던트 계산기 그룹 생성

보안 인시던트 계산기 그룹은 계산기를 그룹화하는 데 사용됩니다.

시작하기 전에
필요한 역할: sn_si.admin

프로시저
1. 다음으로 이동 모두 〉 보안 인시던트 〉 설정 〉 보안 인시던트 계산기 그룹.
2. 새로 만들기를 클릭합니다.
3. 양식의 필드에 적절히 입력합니다.

필드	설명
이름	보안 인시던트 계산기의 이름입니다.
애플리케이션	이 기록을 포함하는 애플리케이션입니다.
순서	보안 인시던트 계산기가 실행되는 순서입니다. 주문 항목이 100인 계산기는 주문 항목이 200인 계산기 앞에 실행됩니다.
설명	이 계산기 그룹에 대한 설명입니다.
작성자	생성한 사용자의 이름 입력

4. 제출을 클릭합니다.

보안 인시던트 계산기 생성

보안 인시던트 계산기를 사용하면 미리 정의된 수식에 따라 보안 인시던트의 심각도를 계산할 수 있습니다. 필요에 따라 고유한 보안 인시던트 계산기를 정의할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.admin

프로시저
1. 다음으로 이동 모두 〉 보안 인시던트 〉 설정 〉 보안 인시던트 계산기 그룹.
2. 계산기를 생성할 그룹의 이름을 클릭하거나 계산기 그룹을 생성할 수 있습니다.
3. 새로 만들기를 클릭합니다.
4. 양식의 필드에 적절히 입력합니다.

필드	설명
이름	보안 인시던트 계산기의 이름입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
계산기 그룹	이 계산기가 속한 그룹의 이름입니다. 주: 계산기 그룹을 만들거나 변경하는 작업은 이름과테이블을 입력한 후에 수행할 수 있습니다.
테이블	이 계산기에 사용할 테이블을 선택합니다. 취약성 [sn_vul_vulnerability] 및 취약한 항목 [sn_vul_vulnerable_item] 이외의 테이블에 계산기를 추가하는 경우 해당 테이블에 비즈니스 규칙과 UI 작업을 추가해야 합니다. 예를 보려면 다음을 수행합니다. ○ 다음으로 이동 시스템 정의 〉 비즈니스 규칙, 취약한 항목 [sn_vul_vulnerable_item] 테이블에서 심각도 계산 비즈니스 규칙을 찾습니다. ○ 다음으로 이동 시스템 **UI** 〉 **UI** 작업, 취약한 항목 [sn_vul_vulnerable_item] 테이블에서 심각도 계산 UI 작업을 찾습니다. 또한 취약성 관리자 역할에는 계산기에서 사용하는 테이블에 대한 전체 읽기, 쓰기(또는 save_as_template) 기능이 부여되어야 템플릿에 적용할 값이 제대로 표시됩니다.
애플리케이션	계산기가 속한 범위가 지정된 애플리케이션입니다.
순서	보안 인시던트 계산기가 실행되는 순서입니다. 주문 항목이 100인 계산기는 주문 항목이 200인 계산기 앞에 실행됩니다.
활성	계산기를 켜거나 끕니다.
설명	이 계산기에 대한 설명입니다.

5. 양식 헤더를 마우스 오른쪽 버튼으로 클릭하고 저장을 선택합니다.
적용할 조건 및 값 탭이 나타납니다.
6. 조건 탭의 필드에 적절한 정보를 입력합니다.

필드	설명
필터 그룹 이용	미리 정의된 필터 그룹을 사용하거나 새 필터 그룹을 생성하여 계산 기준을 정의하려면 이 확인란을 선택합니다.
필터 그룹	계산기를 정의하는 데 사용할 필터 그룹을 선택합니다. 이 필드는 필터 그룹 사용 확인란을 선택한 경우에만 나타납니다.
고급 조건 사용	이 계산기가 적용되는 시기를 결정하는 데 스크립트 조건이 사용됨을 나타내려면 이 확인란을 선택합니다. 확인란을 선택하면 고급 조건 스크립팅 필드가 나타납니다. 필터 그룹 사용 확인란을 선택한 경우 이 필드는 숨겨집니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	주: 고급 조건을 정의하고 보안 인시던트 계산기가 적용되는 시기를 결정하기 위한 스크립트를 작성하기 전에 보안 인시던트 계산기 목록으로 돌아가십시오. 기본 시스템과 함께 제공된 계산기 기록을 살펴봅니다.
조건	계산기 사용 여부를 결정하는 기본 필터 조건을 정의합니다. 필터 그룹 사용 또는 고급 조건 사용 확인란을 선택한 경우 이 필드는 숨겨집니다.

7. 적용할 값 탭을 클릭하고 양식의 필드에 적절한 정보를 입력합니다.
계산에 적용할 값을 정의하는 스크립트를 만들거나 선택한 테이블의 필드를 기반으로 템플릿을 정의할 수 있습니다.

필드	설명
스크립트 값 사용	스크립트로 필드 값을 정의하려면 이 확인란을 선택합니다.
스크립트 값	계산에 적용할 값을 정의합니다. 이 필드는 스크립트 값 사용 확인란을 선택한 경우에만 나타납니다.
템플릿	양식 헤더를 마우스 오른쪽 버튼으로 클릭하고 저장을 선택합니다. 계산기에 사용할 필드와 값을 선택합니다.

8. 모든 항목을 완료했으면 제출을 클릭합니다.

보안 인시던트 계산기 이해

보안 인시던트 계산기는 사전 정의된 조건이 충족될 때 기록 값을 업데이트하는 데 사용됩니다. 계산기는 기록 업데이트 방법을 결정하는 데 사용되는 기준에 따라 그룹화됩니다.

기본 시스템에는 보안 인시던트 응답 다음과 같은 보안 인시던트 계산기 그룹 및 계산기가 포함됩니다. 각 그룹 내에서 조건과 일치하는 첫 번째 계산기를 실행합니다.

기본 시스템의 보안 인시던트 계산기

보안 인시던트 계산기 그룹 이름	그룹에 포함된 계산기	설명
비즈니스 영향	심각도 계산기에서 집계	이 계산기는 다른 필드의 값에 가중치를 부여하여 중요도를 결정하는 보안 중요도 계산기에 위임합니다.
심각도	영향을 받는 비즈니스	이 심각도 계산기는 간단한 조건 작성기를 사용하여 선택 기준을 정의합니다.
	중요한 서비스가 영향을 받음	이 심각도 계산기는 고급 조건을 사용하여 선택 기준을 정의합니다. 보안 인시던트의 구성 항목이 매우 중요한 비즈니스 서비스와 연결된

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

기본 시스템의 보안 인시던트 계산기

보안 인시던트 계산기 그룹 이름	그룹에 포함된 계산기	설명
		경우 위험 점수, 비즈니스 영향 및 우선순위 필드가 계산기에 정의된 대로 상승됩니다.
	중요한 서비스 변경	이 심각도 계산기는 고급 조건을 사용하여 선택 기준을 정의합니다. 보안 인시던트가 조건을 충족하면 필드가 상승되는 수준을 정의하기 위해 스크립트가 실행됩니다. 보안 인시던트의 구성 항목이 가장 중요하거나 상당히 중요한 비즈니스 서비스와 연결된 경우 위험 점수, 비즈니스 영향 및 우선순위 필드가 계산기에 정의된 대로 상승됩니다.
	다중 공격 벡터	이 심각도 계산기는 간단한 조건 작성기를 사용하여 선택 기준을 정의합니다. 보안 인시던트의 구성 항목이 웹, 이메일 및 가장 공격 벡터와 연결된 경우 위험 점수, 비즈니스 영향 및 우선순위 필드가 계산기에 정의된 대로 상승됩니다.

	범주 및 서비스로 우선순위 설정	이 심각도 계산기는 고급 조건 작성기를 사용하여 선택 기준을 정의합니다.
		
		다음 조건이 충족되면 보안 인시던트 우선순위가 **1 - 중요** 로 설정됩니다.
		• 보안 인시던트에는 영향을 받는 서비스가 연결되어 있으며 그 중 하나가 중요합니다.
		• 보안 인시던트 범주는 다음 중 하나입니다.
		  ○ DoS(서비스 거부)
		  ○ 스피어 피싱
		  ○ 악성 코드 활동
		
		주: 이 계산기는 Starter Security Operation 가격 책정 계층이 있는 경우 기본 시스템에서 사용할 수 있습니다.

	옵저버블로 우선순위 설정	이 심각도 계산기는 고급 조건 작성기를 사용하여 선택 기준을 정의합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

기본 시스템의 보안 인시던트 계산기

보안 인시던트 계산기 그룹 이름	그룹에 포함된 계산기	설명
		다음 조건이 충족되면 보안 인시던트 우선순위가 **1 - 중요** 로 설정됩니다. • 보안 인시던트에는 영향을 받는 서비스가 연결되어 있으며 그 중 하나가 중요합니다. • 보안 인시던트 범주는 다음 중 하나입니다. ○ DoS(서비스 거부) ○ 스피어 피싱 ○ 악성 코드 활동 • 연결된 옵저버블 또는 표시기 중 하나의 사이팅 수가 활성 표시기가 있는 사이팅 2개를 초과합니다 (즉, 옵저버블 또는 표시기가 여러 소스에서 잘못된 것으로 확인됨). **주:** 이 계산기는 고급 보안 운영 가격 책정 계층이 있고 위협 피드 플러그인을 활성화하는 경우 기본 시스템에서 사용할 수 있습니다.
사용자 중요도	사용자 중요도 가져오기	이 심각도 계산기는 간단한 조건 작성기를 사용하여 선택 기준을 정의합니다. 이 심각도 계산기는 부서 필드가 재무로 변경될 때 사용자 비즈니스 중요도를 **1 - 중요**로 변경합니다.
	사용자 그룹 중요도 가져오기	이 심각도 계산기는 고급 조건 작성기를 사용하여 선택 기준을 정의합니다. 이 심각도 계산기는 관련 목록의 데이터에서 실행되는 계산기의 예를 제공합니다.

심각도 계산기

보안 인시던트를 만들면 위험 점수, 비즈니스 영향 및 우선순위 필드에 기본값이 포함됩니다. 인시던트를 저장하면 비즈니스 규칙이 각 활성 심각도 계산기에 정의된 조건을 기준으로 보안 인시던트의 정보를 자동으로 확인합니다. 각 계산기의 순서 필드에 정의된 순서대로 한 번에 하나의 보안 계산기에 대한 유효성이 검사됩니다. 보안 인시던트의 정보가 계산기 중 하나에 정의된 조건과 일치하면 계산기에 설정된 규칙에 따라 심각도 필드 값이 업데이트됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예를 들어 영향을 받는 CI에 대한 보안 인시던트를 생성했으며 CI가 매우 중요하다고 가정해 보겠습니다. 보안 인시던트가 저장되면 CI 정보가 심각도 계산기에 정의된 조건과 비교됩니다. 중요 서비스의 영향을 받는 심각도 계산기에 대해 보안 인시던트가 확인되면 심각도 필드가 자동으로 업데이트되고 보안 인시던트 상단에 다음과 유사한 메시지가 표시됩니다.

Severity Calculation applied: Critical service changes; Risk: High; impact: 1 - High; Priority: 1 - Critical; Severity: 1 - High

이러한 심각도 계산기를 그대로 사용하거나 비즈니스 요구 사항을 보다 근접하게 충족하도록 편집할 수 있습니다. 예를 들어 재무 사업부와 관련된 웹 및 이메일 위협을 식별하려면 다중 공격 벡터 계산기의 조건을 변경할 수 있습니다.

- 〔공격 벡터〕〔포함〕〔편물〕
- 〔공격 벡터〕〔포함〕〔이메일〕
- 〔비즈니스 단위〕〔포함〕〔재무〕

기록을 열고 심각도 계산 관련 링크를 클릭하여 기존 보안 인시던트의 심각도 값을 언제든지 업데이트할 수도 있습니다.

보안 인시던트 위험 점수 계산기

범주 및 서비스로 우선순위 설정 및 옵저버블로 우선순위 설정 계산기는 보안 인시던트의 위험 점수를 계산하는 데 사용됩니다.

사용자 중요도 계산기

사용자 중요도 그룹에 있는 두 가지 계산기(사용자 중요도 가져오기 및 사용자 그룹 중요도 가져오기)는 사용자 기록에 정의된 기준 또는 사용자가 속한 그룹을 기반으로 중요도를 높이는 방법의 예를 제공합니다.

필요에 따라 편집하거나 새 사용자 중요도 계산기를 만들 수 있습니다.

사용자 중요도 가져오기 계산기를 사용하면 부서 필드가 재무로 변경될 때 사용자의 비즈니스 중요도가 **1 - 중요**로 변경됩니다.

사용자 그룹 중요도 계산기를 사용하면 사용자가 데이터베이스 그룹에 추가될 때 사용자의 비즈니스 중요도가 **1 - 중요**로 변경됩니다.

주:
사용자 그룹 중요도 가져오기 는 관련 목록의 데이터에 대해 실행되는 계산기의 예입니다. 그룹을 더 추가하여 중요도 변경을 시작하려면 스크립트의 첫 번째 줄에 그룹 sys_ids 목록을 추가하고, 쉼표로 구분합니다. 예: `var CRITICAL_GROUPS = [group1_sys_id, group2_sys_id, group3_sys_id];`.

보안 인시던트 위험 점수 계산

위험 점수는 보안 인시던트의 우선순위, 보안 인시던트 유형(서비스 거부, 스피어 피싱 또는 악성 코드 활동) 및 표시기에서 실패한 평판 점수를 트리거한 소스 수를 기반으로 위험을 나타내는 산술 평균으로 계산됩니다.

위험 점수는 분석가가 보안 인시던트 작업의 우선순위를 정하는 데 도움이 됩니다.

중요사항:
새 위험 점수 계산기를 사용하려면 을 참조하십시오 새 위험 점수 계산기 규칙 정의.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

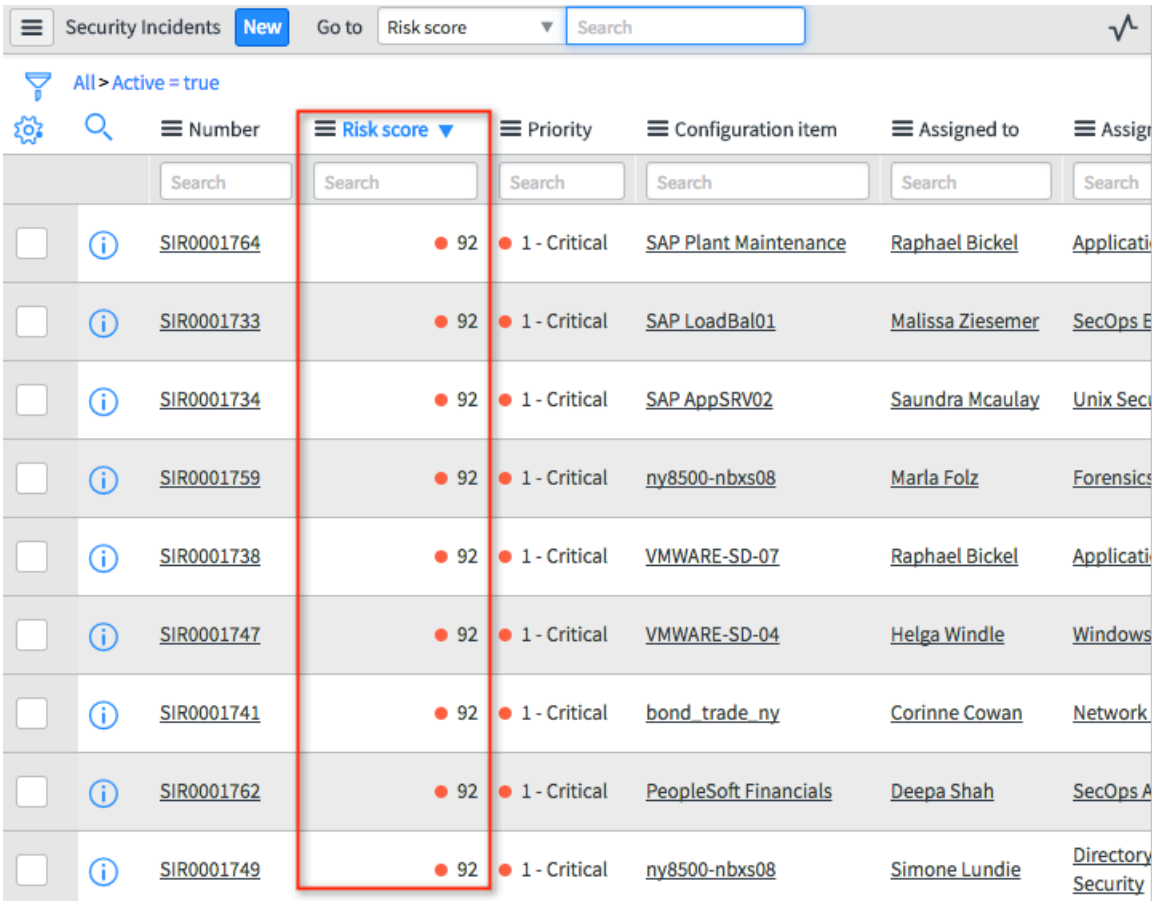
범주 및 서비스로 우선순위 설정 및 옵저버블로 우선순위 설정 보안 인시던트 계산기는 보안 인시던트의 위험 점수를 계산하는 데 사용됩니다. 또한 다음 비즈니스 규칙은 위험 점수의 자동 계산을 트리거합니다.

- 심각도 계산
- 위험 점수 업데이트
- SI 위험 점수 업데이트

주:
기본 시스템에서 사용할 수 있는 위험 계산기는 보안 운영 가격 책정 계층에 따라 달라집니다.

기본 시스템의 보안 인시던트 목록을 살펴보면 위험 점수 열을 확인할 수 있습니다.

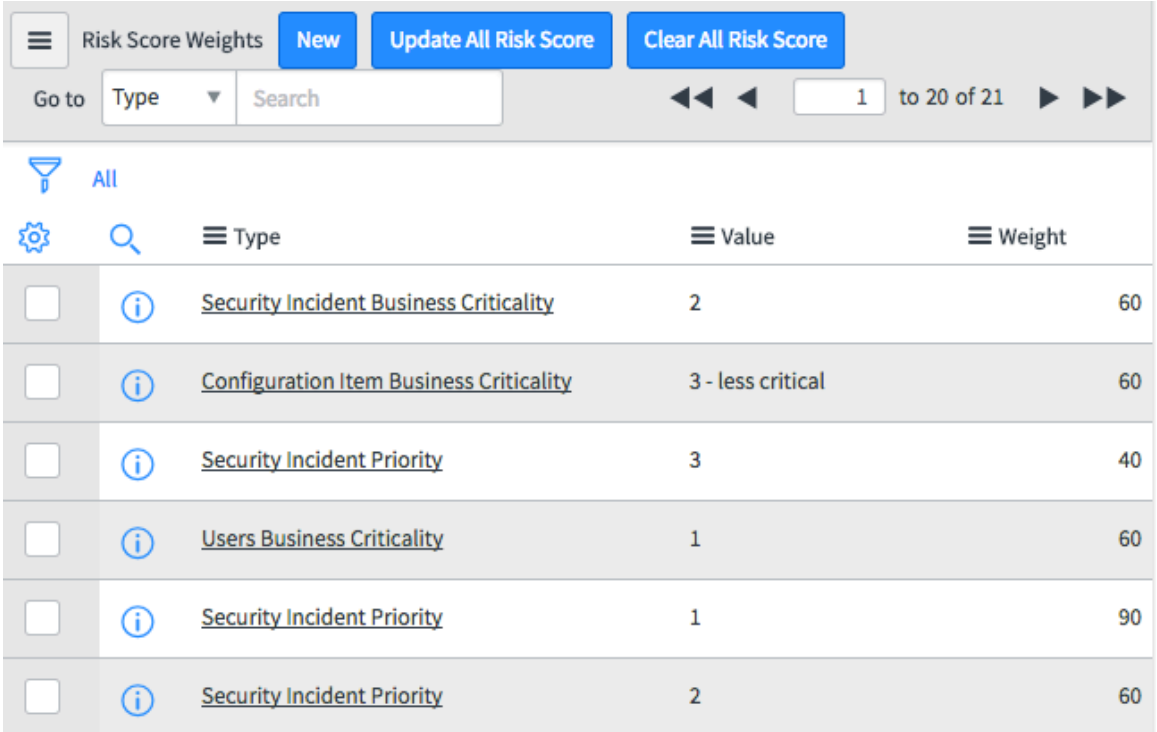
보안 인시던트



위험 점수는 위험 점수 구성에 정의된 가중치를 사용하여 계산됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

위험 점수 구성



예를 들어, 보안 인시던트의 비즈니스 영향 이 2-높음 으로 설정되고 우선순위 가 3-보통으로 설정된 경우 위험 점수 가중치 테이블의 각 가중치가 조회되고 계산되는 것은 다음과 같습니다.

값이 2인 보안 인시던트 비즈니스 영향 = 가중치 60.

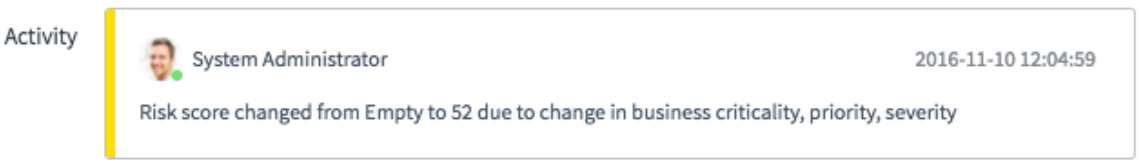
값이 3인 보안 인시던트 우선순위 = 가중치 40.

(60 + 40)/2 = 위험 점수 50.

업데이트된 위험 점수에 따라 보안 인시던트 목록의 보안 인시던트 위치가 다시 정렬됩니다.

위 예시에서 보안 인시던트의 비즈니스 영향 또는 우선순위 가 변경되면 위험 점수가 다시 계산되고 변경 내용이 작업 메모에 반영됩니다.

작업 메모



다음 필드가 변경되면(위험 점수가 업데이트됨) 작업 메모가 업데이트됩니다.

- 보안 인시던트 양식에 대한 비즈니스 영향
- 보안 인시던트 양식에 대한 우선순위
- 보안 인시던트 양식의 심각도(기본적으로 숨겨져 있음)
- 영향을 받는 사용자 관련 목록에 대한 비즈니스 영향
- 영향을 받는 서비스 관련 목록에 대한 비즈니스 영향
- 취약 항목 관련 목록의 취약성에 대한 비즈니스 영향

또한 다음과 같은 상황에서 작업 메모가 업데이트됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 영향을 받는 사용자와 보안 인시던트 간의 연결이 생성되거나 수정되는 경우
- 영향을 받는 서비스와 보안 인시던트 간의 연결이 생성되거나 수정되는 경우
- 취약한 항목과 보안 인시던트 간의 연결이 생성되거나 수정되는 경우

또한 위험 점수 가중치 양식에서 모든 위험 점수 업데이트 및 모든 위험 점수 지우기를 클릭할 때마다 작업 메모가 업데이트됩니다.

위험 점수 가중치 유지

보안 인시던트에서 위험 점수를 계산하는 데 사용되는 위험 점수 가중치는 개별적으로 제거하거나 업데이트할 수 있습니다. 또한 모든 보안 인시던트에 대해 제거하거나 업데이트할 수도 있습니다. 보안 인시던트에서 제거하는 기능은 가중치 값을 변경할 때 유용합니다.

시작하기 전에

필요한 역할: sn_sec_cmn.admin

주:
sn_si.read 역할을 가진 사용자는 다음에서 보안 인시던트 응답위험 점수 구성을 볼 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 설정 〉 위험 점수 구성.

   주:
   sn_si.read 역할을 가진 사용자는 다음으로 이동하여 위험 점수 구성을 볼 수 있습니다. 보안 인시던트 〉 경보 및 이벤트 〉 위험 점수 구성.

2. 새 위험 점수 가중치를 추가하려면 새로 만들기를 클릭하고 필드에 정보를 입력합니다.

필드	설명
유형	정의하려는 위험 점수 유형을 선택합니다.
값	선택한 유형과 연결된 값을 지정합니다. 유형에 여러 값을 사용할 수 있는 경우 여러 위험 점수 가중치 기록을 정의할 수 있습니다. 예를 들어 값이 1인 보안 인시던트 우선순위, 값이 2인 보안 인시던트 우선순위 등이 있습니다.
가중치	선택한 유형/값 쌍과 연결된 가중치입니다. 유효한 항목은 0에서 100 사이이며 0은 가장 낮은 가중치이고 100은 가장 높은 가중치입니다.

3. 제출을 클릭합니다.
4. 필요에 따라 다음 단계를 수행합니다.
   - 위험 점수 가중치 기록을 지우려면 목록에서 열고 삭제를 클릭합니다.
   - 모든 위험 점수 가중치 기록을 지우려면 모든 위험 점수 지우기를 클릭합니다.
   - 모든 위험 점수 가중치 기록을 업데이트하려면 모든 위험 점수 업데이트를 클릭하십시오.

SLA 생성 보안 인시던트 응답

에 대한 보안 인시던트 응답서비스 수준 계약(SLA)을 정의할 수 있습니다.

시작하기 전에

필요한 역할: sn_si.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 설정 〉 **SLA**.
2. 새로 만들기를 클릭합니다.
   필드 설명과 자세한 지침은 다음 문서를 참조하십시오 Create an SLA definition .

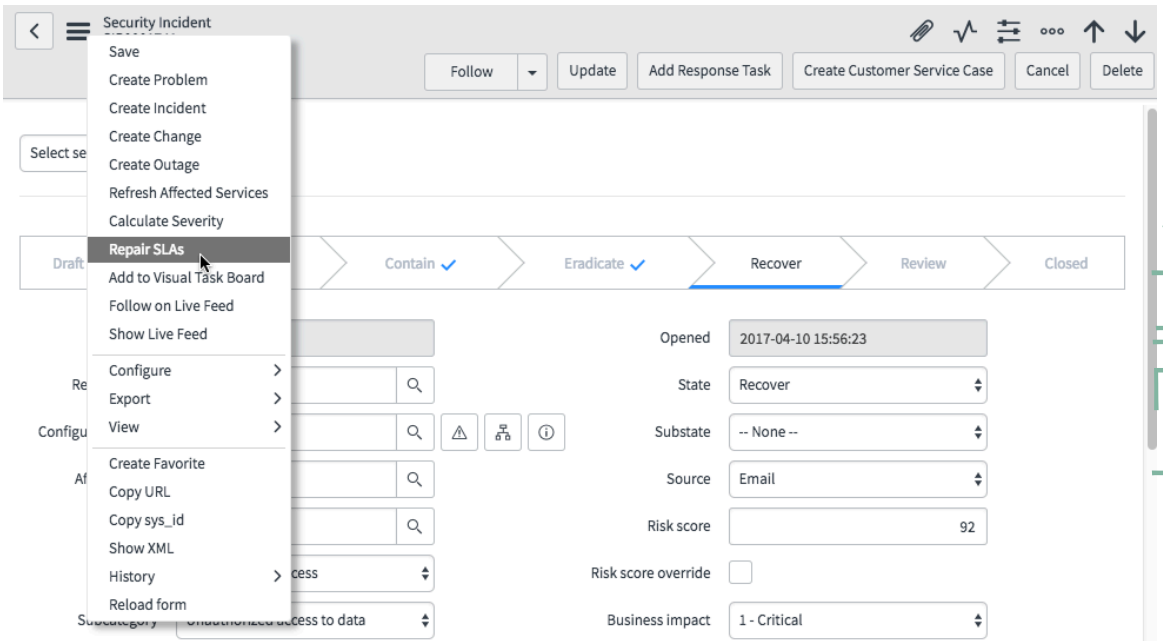
보안 인시던트 **SLA** 복구

SLA 기록을 복구하여 SLA 타이밍 및 기간 정보가 정확해지도록 할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.basic

프로시저

1. 아직 열려 있지 않으면 SLA를 복구하려는 보안 인시던트를 엽니다.
2. 양식 헤더 컨텍스트 메뉴를 클릭하고 **SLA** 복구를 선택합니다.



3. 경고 확인 상자에서 확인을 클릭합니다.
   자세한 내용은 SLA 복구를 참조하십시오.

보안 인시던트 응답 **Runbook** 생성

Runbook은 게시된 지식 문서와 특정 작업 간의 연결입니다. 작업을 수행하는 동안 Runbook의 지식 문서가 자동으로 열리고 작업과 관련된 정보가 제공됩니다.

시작하기 전에
Runbook 지식베이스에 보안 인시던트 응답 기존 지식 문서가 있어야 합니다. 보안 인시던트 지식 문서를 생성할 때 지식베이스 필드에서 보안 인시던트 응답 **Runbook**을 선택해야 합니다. 문서를 게시한 후 **Runbook** 만들기 단추를 클릭할 수 있습니다.

필요한 역할: sn.si.knowledge_admin

이 태스크 정보
보안 인시던트 또는 응답 작업 생성 프로세스 중에 Runbook을 사용하거나, Runbook의 지식베이스 문서를 Playbook의 작업과 연결할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 수동 **Runbook** 〉 새 **Runbook** 생성.
2. 필드에 적절한 정보를 입력합니다.

필드	설명
지식 문서	Runbook에 포함할 지식 문서를 선택합니다.
활성	필터 탐색기에서 Runbook을 사용할 수 있도록 하려면 확인란을 선택합니다.
필터 그룹 이용	미리 정의된 필터 그룹을 사용하거나 새 필터 그룹을 만들어 Runbook 조건을 정의하려면 이 확인란을 선택합니다.
필터 그룹	Runbook을 정의하는 데 사용할 필터 그룹을 선택합니다. 이 필드는 필터 그룹 사용 확인란을 선택한 경우에만 나타납니다.
테이블	보안 인시던트(sn_si_incident) 또는 보안 인시던트 응답 작업(sn_si_task)을 선택합니다. 필터 그룹 사용 확인란을 선택하고 필터 그룹을 선택한 경우 이 필드는 기본적으로 선택한 필터 그룹과 연결된 테이블로 설정됩니다.
조건	이 Runbook을 인시던트나 작업에 연결하는 조건을 설정합니다. 필터 그룹 사용 확인란을 선택하고 필터 그룹을 선택한 경우 조건 필드가 표시되지 않습니다.

3. 양식 헤더를 마우스 오른쪽 버튼으로 클릭하고 저장을 선택합니다.
   지식 문서 상세 정보 탭과 일련의 버튼이 나타납니다.
4. Runbook의 세부 정보를 보려면 기술 자료 세부 정보 탭을 클릭합니다.
5. 사용자에게 표시되는 대로 지식 문서를 보려면 문서 보기를 클릭합니다.
6. ~ 지식 문서의 세부 사항을 편집하고 문서 편집을 클릭합니다.

사용자가 보고한 피싱 공격을 확인하는 규칙 생성

직원이 피싱 공격으로 보이는 이메일을 받으면 피싱 이메일 주소를 사용하여 보고할 수 있습니다. 의심스러운 이메일은 조직에서 정의한 규칙을 사용하여 확인됩니다.

시작하기 전에

이메일 일치 규칙을 사용하여 잠재적인 피싱 공격을 식별하려면 먼저 직원이 전달한 이메일이 처리를 위해 전송될 이메일 주소를 정의합니다. 다음과 같은 옵션으로 이 이메일 주소를 정의할 수 있습니다(회사 이메일 도메인이 acme.com 것으로 가정).

- 이메일 주소(예: **acme+phishing@service-now.com**)를 정의합니다. +피싱 태그는 필터링을 활성화하기 위해 SMTP에서 지원되며 인스턴스에서 전송된 이메일을 받을 수 있습니다.
- **phishing@acme.com**(Exchange 사서함)와 같은 이메일 주소를 정의하면 이 주소가 **acme +phishing@service-now.com**(메일 전달 규칙을 통해 정의된 인스턴스 사서함)으로 전달됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필요한 역할: sn_sec_cmn.write

이 태스크 정보
직원이 의심스러운 이메일을 발견하면 피싱 이메일 주소에 첨부 파일로 전달해야 합니다. 첨부된 이메일이 위협을 정의하는 규칙과 일치하면 보안 인시던트가 생성됩니다.

프로시저
1. 다음으로 이동 모두 〉 보안 운영 〉 이메일 처리 〉 사용자가 보고한 피싱.
2. 새로 만들기를 클릭합니다.
3. 필요에 따라, 필드를 채웁니다.

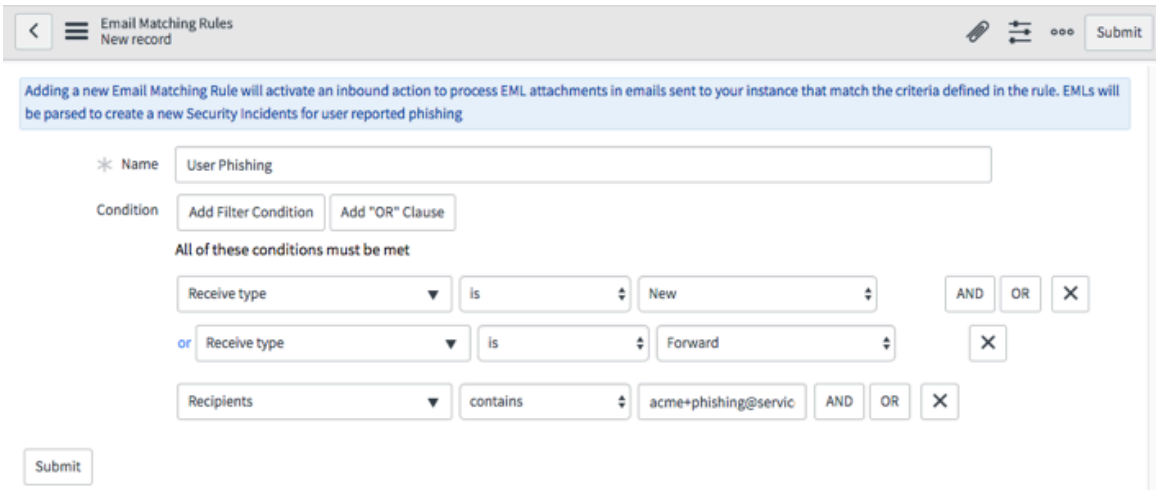
이메일 일치 규칙 양식

필드	설명
이름	이 이메일 일치 규칙의 이름입니다. 예를 들어 사용자가 보고한 피싱입니다.
조건	다음 사용 회사 피싱 이메일 주소로 전송된 이메일이 피싱 공격인지 여부를 확인하는 조건 작성기 입니다. 다음 예를 참조하십시오.

4. 제출을 클릭합니다.

Example:
이 예에서는 사용자가 보고한 피싱을 처리하기 위한 일치 규칙을 보여 줍니다.

이메일 일치 규칙의 예



보안 분석가 작업 공간 구성
에서 보안 분석가 작업 공간 인시던트 기록의 사용자 인터페이스를 구성하여 표시할 필드를 지정합니다.

시작하기 전에
필요한 역할: sn_si.analyst

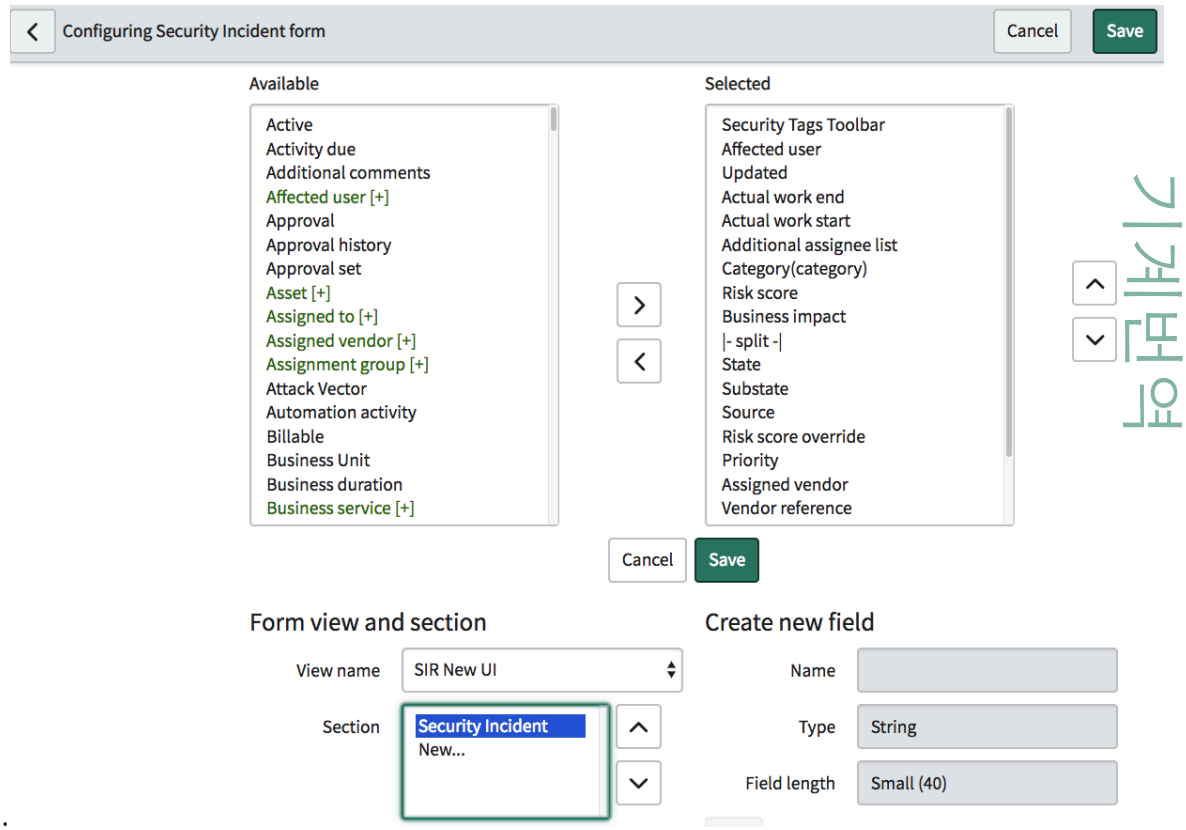
이 태스크 정보
인시던트 기록에 표시할 필드와 보안 인시던트 양식 및 응답 작업 양식에 필드가 표시되어야 하는 순서를 지정합니다. 표시할 필드 수에 제한을 설정할 수도 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
특정 양식에 사용할 뷰를 결정하는 규칙을 만들 수 있습니다. 기본 시스템에는 기본 및 SIR New UI 뷰를 포함해 여러 뷰가 포함되어 있습니다. 기타 모든 응답 작업 규칙을 포함하여 여러 뷰 규칙도 기본 시스템과 함께 제공됩니다. 이 규칙은 뷰 규칙에 지정된 조건이 충족될 때 응답 작업 양식에 기본 뷰를 적용합니다. 보안 분석가 작업 공간 SIR 새 UI 뷰를 사용합니다. 에 표시된 보안 분석가 작업 공간 양식 필드가 클래식 환경의 양식 필드와 일치하지 않으면 뷰 규칙이 적용될 가능성이 높습니다. 양식에 **SIR** 새 **UI** 뷰를 사용하려면 뷰 규칙을 비활성화해야 합니다. 자세한 내용은 Control when the system displays a view 를 참조하십시오.

프로시저

1. 보안 인시던트 목록(예: 모두 〉 보안 인시던트 〉 인시던트 〉 모든 인시던트 표시).
2. 보안 인시던트 기록을 열려면 보안 인시던트 링크를 클릭합니다.
3. 보안 인시던트 구성 양식 페이지로 이동하려면 메뉴 아이콘을 클릭하고 구성 〉 양식 레이아웃.
4. 이름 보기 목록에서 **SIR** 새 **UI**를 선택합니다.
5. 섹션 필드에서 적절한 섹션을 선택합니다.
   이는 보안 인시던트 또는 보안 인시던트 응답 작업일 수



있습니다.

6. 새 UI의 인시던트 배너에 표시할 필드와 순서를 선택합니다.
7. 저장을 클릭합니다.

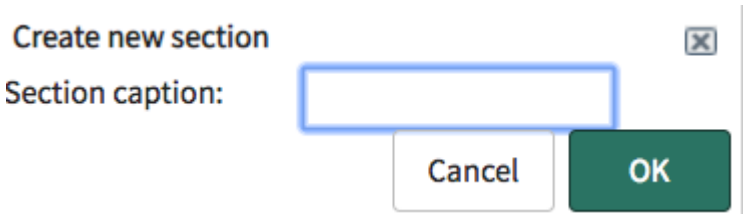
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

- 일부 필드는 기본적으로 인시던트 및 응답 작업 배너에서 숨겨져 있습니다. 설명된 대로 보안 분석가 작업 공간 속성sn_app_secops_ui.form.excluded_fields.incident 및 sn_app_secops_ui.form.excluded_fields.response_task 속성을 수정하여 숨기거나 표시되는 필드를 변경합니다.
- 다음 속성을 설정하여 인시던트 및 응답 작업 배너와 인시던트 배너의 첫 번째 라인에 표시할 수 있는 필드의 수를 지정합니다.
  - sn_app_secops_ui.task_summary.single_summary.limit.incident
  - sn_app_secops_ui.task_summary.single_summary.limit.response_task
  - sn_app_secops_ui.task_summary.single_summary.limit.incident.first_line

8. 예를 들어, 인시던트 기록의 필드 값 옆에 표시되는 점선 원의 스타일을 구성하려면 다음으로 이동합니다. 시스템 **UI** 〉 필드 스타일 을 클릭하고 특정 테이블 및 필드 이름에 대한 새 스타일 기록을 수정하거나 생성합니다.
   스타일 기록의 스타일 필드에 있는 속성 background-color에 따라 점선 원의 색상이 결정됩니다.
9. 업데이트된 인시던트 배너를 보려면 다음을 클릭합니다. 보안 인시던트 〉 인시던트(신규 **UI)** 의 인시던트 기록 보안 분석가 작업 공간 으로 이동하고 페이지를 새로 고쳐 업데이트된 인시던트 배너를 확인합니다.
10. 인시던트 기록에서 응답 작업 배너를 구성하려면 다음으로 이동하십시오. 보안 인시던트 〉 응답 작업 〉 모든 작업 표시 을 클릭하고 단계를 반복합니다.
11. 기본 보안 인시던트 응답 작업 테이블에서 확장되는 새 작업 테이블을 생성하는 경우 SIR 새 UI 뷰를 테이블에 추가해야 합니다.

    a. 뷰 이름 목록에서 새로 만들기를 선택합니다.



    b. 새 뷰 만들기 창에 **SIR** 새 **UI** (대/소문자 구분)를 입력하고 확인을 클릭합니다.

결과
보안 인시던트 및 응답 작업 배너는 ()를 사용하여 보안 위협 관리 보안 분석가 작업 공간에서 보안 분석가 작업 공간 업데이트됩니다.

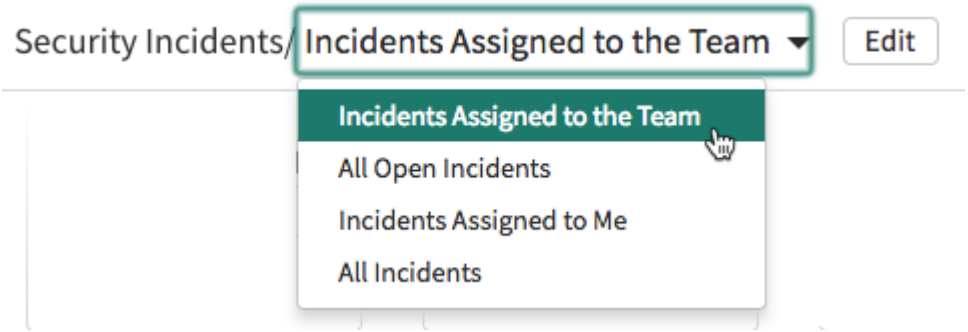
에 대한 기본 및 보조 필터 설정 보안 분석가 작업 공간

보안 분석가 작업 공간 기본 시스템에는 분석할 보안 인시던트 목록의 범위를 좁히기 위한 기본 필터 세트(사용자에게 할당된 보안 인시던트, 모든 미해결 인시던트 등)와 목록 범위를 더 좁힐 수 있는 빠른(또는 보조) 필터 세트(새 인시던트, 미해결 인시던트, 중요한 인시던트만 등)가 포함되어 있습니다.

시작하기 전에
클래식 환경을 사용하여 추가 기본 및 보조 필터를 정의할 수 있습니다.

에서 보안 분석가 작업 공간사용할 필터를 정의할 때 태그를 할당하여 기본 또는 보조 필터로 사용할 수 있는지 여부를 나타낼 수 있습니다. 기본 필터는 보안 인시던트 목록의 맨 위에 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



빠른 필터 옵션 옆에 있는 편집을 클릭하여 보조(또는 빠른) 필터를 선택합니다.

필요한 역할: admin 또는 sn_sec_cmn.write

프로시저

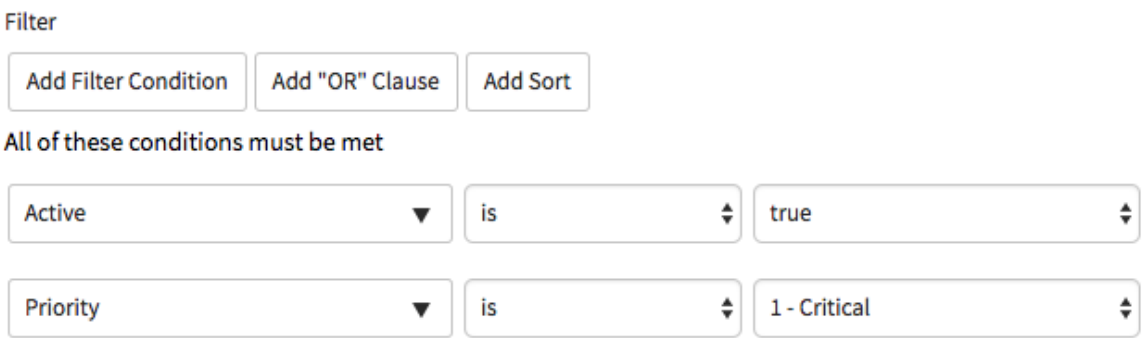
1. 다음으로 이동 모두 〉 시스템 정의 〉 필터.

2. 새로 만들기를 클릭하고 다음 단계를 완료합니다.

a. 제목을 입력합니다.

b. 테이블 선택 목록에서 보안 인시던트 **[sn_si_incident]**를 선택합니다.

c. 필터 조건을 추가합니다.
예를 들어, 우선순위 **=** 중요인 미해결 인시던트 필터는 다음 조건을 사용합니다.



d. 제출을 클릭합니다.

3. 태그 열이 필터 목록에 표시되지 않으면 기어 아이콘을 클릭하고 뷰를 개인화하여 추가합니다.

4. 생성한 필터를 찾아 다음 태그 중 하나를 추가하여 필터가 에 보안 분석가 작업 공간표시되는 방식을 나타냅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- **SN_SI_Primary**: 이 태그를 선택하면 의 보안 분석가 작업 공간기본 필터 슬러시버킷에서 필터를 선택할 수 있습니다.
- **SN_SI_Primary_OOB**: 이 태그를 선택하면 필터가 기본적으로 기본 필터 슬러시버킷의 선택됨 쪽에 나타납니다.
- **SN_SI_Secondary**: 이 태그를 선택하면 보조(빠른) 필터 슬러시버킷에서 필터를 선택할 수 있습니다.
- **SN_SI_Secondary_OOB**: 이 태그를 선택하면 필터가 기본적으로 기본 필터 슬러시버킷의 선택됨 쪽에 나타납니다.

관련 정보

필터 생성 및 편집

보안 분석가 작업 공간 속성

이러한 시스템 속성은 보안 분석가 작업 공간을 구성하는 데 사용됩니다.

다음과 같은 두 가지 유형의 속성이 있습니다.

- 일반적으로 수정되지 않는 속성입니다(예: sys_ids 및 제품 키).
- 긴 폴링 간격 및 사용자 인터페이스 구성처럼 필요에 따라 수정되는 속성입니다.

주:
보안 분석가 작업 공간 속성은 다음 위치에 있습니다. 보안 인시던트 〉 분석가 작업 공간 설정 〉 분석가 작업 공간 속성.

보안 분석가 작업 공간 속성

속성 이름	설명
응답 작업 배너에서 기본적으로 숨겨져 있는 필드입니다. sn_app_secops_ui.form.excluded_fields.response_task	• 유형: 문자열 • 기본값: ○ 번호 ○ 간단한 설명 ○ 설명 ○ work_notes ○ comments_and_work_notes ○ work_notes_list ○ automation_activity
인시던트 배너에서 기본적으로 숨겨져 있는 필드입니다. sn_app_secops_ui.form.excluded_fields.incident	• 유형: 문자열 • 기본값: ○ 번호 ○ 간단한 설명 ○ 설명 ○ work_notes

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 분석가 작업 공간 속성

속성 이름	설명
	○ comments_and_work_notes ○ work_notes_list ○ automation_activity ○ security_tags
배경색 스타일은 여기에 나열된 필드에 적용됩니다. sn_app_secops_ui.form.color_coded_fields	• 유형: 문자열 • 기본값: ○ 비즈니스 중요도 ○ 영향도 ○ 우선순위 ○ risk_score ○ severity
예일 경우 sn_si_task 기본 응답 작업 테이블에서 확장된 테이블은 기본 응답 작업 테이블에 대해 작성된 이메일 템플릿에도 액세스할 수 있습니다. sn_app_secops_ui.extend.base.response_task.email_templates	• 유형: true | false • 기본값: True
각 응답 작업 배너에서 각 요약 필드의 너비를 설정합니다. sn_app_secops_ui.task_summary.single_summary.width.response_task	• 유형: 정수 • 기본값: 10
각 인시던트 배너에서 각 요약 필드의 너비를 설정합니다. sn_app_secops_ui.task_summary.single_summary.width.incident	• 유형: 정수 • 기본값: 15
인시던트 배너에 허용되는 요약 필드 수를 제한합니다. sn_app_secops_ui.task_summary.single_summary.limit.incident	• 유형: 정수 • 기본값: 12
응답 작업 배너에 허용되는 요약 필드 수에 대한 제한을 설정합니다. sn_app_secops_ui.task_summary.single_summary.limit.response_task	• 유형: 정수 • 기본값: 12

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 분석가 작업 공간 속성

속성 이름	설명
인시던트 배너의 첫 줄에 허용되는 요약 필드 수를 제한합니다. sn_app_secops_ui.task_summary.single_summary.limit.incident.first_line	• 유형: 정수 • 기본값: 3

사용자 사진이 있을 수 있는 쉼표로 구분된 필드 목록입니다.
 	
sn_app_secops_ui.form.user_fields
	• 유형: 문자열
	• 기본값:
	  ○ affected_user
	  ○ caller
	  ○ sys_updated_by
	  ○ sys_created_by
	  ○ opened_by
	  ○ closed_by
	  ○ submitted_by

각 인시던트 엿보기 뷰에서 각 요약 필드의 너비를 설정합니다. sn_app_secops_ui.task_summary.single_summary.width.incident_peek	• 유형: 정수 • 기본값: 13.5

시간을 표시하는 쉼표로 구분된 필드 목록입니다.
 	
sn_app_secops_ui.form.time_fields
	• 유형: 문자열
	• 기본값:
	  ○ opened_at
	  ○ sys_created_on
	  ○ sys_updated_on

사이팅 검색 결과를 새로 고치는 빈도(밀리초)를 제어합니다. sn_app_secops_ui.poller_interval.search_action	• 유형: 정수 • 기본값: 30000 최소: 15000
카운트 또는 쿼리 데이터를 새로 고치는 빈도(밀리초)를 제어합니다. sn_app_secops_ui.poller_interval.related_list	• 유형: 정수 • 기본값: 30000 최소: 15000

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 분석가 작업 공간 속성

속성 이름	설명
플레이북의 경우 결과 데이터를 새로 고치는 빈도(밀리초)를 제어합니다. sn_app_secops_ui.poller_interval.playbook_tasks	• 유형: 정수 • 기본값: 30000 최소: 15000
보안 운영 통합 - 호스트 격리 워크플로우의 ID입니다. sn_app_secops_ui.workflow.id.isolate_host	• 유형: 문자열 • 기본값: d72041f1ff203200c68c84648e94fa5e
보안 운영 통합 - 감시 목록 워크플로우의 ID입니다. sn_app_secops_ui.workflow.id.publish_to_watchlist	• 유형: 문자열 • 기본값: 35800c0eff343200c68c84648e94fa85
보안 운영 통합 - 차단 요청 워크플로우의 ID입니다. sn_app_secops_ui.workflow.id.block_request	• 유형: 문자열 • 기본값: 11a6a5270b9032008f9108e3c5673a24
sn_si_analyst 사용자 역할의 ID입니다. sn_app_secops_ui.roles.id.sn_si.write	• 유형: 문자열 • 기본값: 66878663ff123100158bffffffffff8d
sn_si_read 사용자 역할의 ID입니다. sn_app_secops_ui.roles.id.sn_si.read	• 유형: 문자열 • 기본값: ae878663ff123100158bffffffffff8e
sn_si_admin 사용자 역할의 ID입니다. sn_app_secops_ui.roles.id.sn_si.admin	• 유형: 문자열 • 기본값: 22878663ff123100158bffffffffff8d
Microsoft Exchange - 이메일 검색 수행 및 삭제 워크플로우의 ID입니다. sn_app_secops_ui.email.phishing.manual.workflow	• 유형: 문자열 • 기본값: ed9f289cc310220031fbdccdf3d3aeb4
탐색 보안 분석가 작업 공간탭 아래에 있는 거부 목록에 추가 사용자 지정 작업의 ID입니다. sn_app_secops_ui.explore.action.direct.id.deny_list	• 유형: 문자열 • 기본값: DENY_e9bd0ac50b632200263a089b37673a0b

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 분석가 작업 공간 속성

속성 이름	설명
탐색 탭 아래에 있는 허용 목록에 추가 사용자 지정 작업의 ID 보안 분석가 작업 공간 sn_app_secops_ui.explore.action.direct.id.allow_list	• 유형: 문자열 • 기본값: ALLOWLIST_e9bd0ac50b632200263a089b37673a0b
위협 조회 실행 UI 작업의 ID입니다. sn_app_secops_ui.explore.action.id.run_threat_lookup	• 유형: 문자열 • 기본값: da5ff4420b540300263a089b37673ae7
위협 조회 통합 역량의 ID입니다. sn_app_secops_ui.explore.capability.id.threat_lookup	• 유형: 문자열 • 기본값: 39344d4f0b273200263a089b37673ab1
의 보안 분석가 작업 공간탐색 탭 아래에 있는 옵저버블 보강 사용자 지정 작업에 대한 ID입니다. sn_app_secops_ui.explore.action.id.observable_enrichment	• 유형: 문자열 • 기본값: OBS_ENRICHMENT_54e2f5d60b5003009f66e94685673
옵저버블 보강 통합 역량의 ID입니다. sn_app_secops_ui.explore.capability.id.observable_enrichment	• 유형: 문자열 • 기본값: 9ad183640b1003009f66e94685673af4
감시 목록에 게시 UI 작업의 ID입니다. sn_app_secops_ui.explore.action.id.publish_to_watchlist	• 유형: 문자열 • 기본값: 8ee94002ff743200c68c84648e94faf9
차단 요청 UI 작업의 ID입니다. sn_app_secops_ui.explore.action.id.block_request	• 유형: 문자열 • 기본값: 7158f6e40b2032008f9108e3c5673adf
사이팅 검색 실행 UI 작업의 ID입니다. sn_app_secops_ui.explore.action.id.sightings_search	• 유형: 문자열 • 기본값: 43f91a6f0b032200b97c67d985673a2c
하위 보안 인시던트 생성 UI 작업의 ID입니다. sn_app_secops_ui.explore.action.id.create_child_incident	• 유형: 문자열 • 기본값: 5a68826453635300 99d5ddeeff7b1272

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 분석가 작업 공간 속성

속성 이름	설명
보안 주석 추가 UI 작업의 ID입니다. sn_app_secops_ui.explore.action.id.add_security_annotation	• 유형: 문자열 • 기본값: 1e3a3e723b5332005a9149a4d2efc4eb
의 탐색 탭 아래에 있는 CI 보강 사용자 지정 작업의 ID입니다 보안 분석가 작업 공간. sn_app_secops_ui.explore.action.id.ci_enrichment	• 유형: 문자열 • 기본값: CI_ENRICHMENT_54e2f5d60b5003009f66e94685673a1
호스트 격리 UI 작업의 ID입니다. sn_app_secops_ui.explore.action.id.isolate_host	• 유형: 문자열 • 기본값: d6244e0aff203200c68c84648e94fad3
복수 옵저버블 추가 UI 작업의 ID입니다. sn_app_secops_ui.explore.action.id.multiple_observable	• 유형: 문자열 • 기본값: 138de478d78322007a6de294de6103aa
ag-Grid-Enterprise의 제품 키입니다. sn_app_secops_ui.ag-grid-license	• 유형: 문자열 • 기본값:ServiceNow_ServiceNow_5Devs2_August_2018__M

기계번역

추가 보안 분석가 작업 공간 구성

보안 분석가 작업 공간 필터, UI 작업 및 관련 목록을 구성하고 정의합니다.

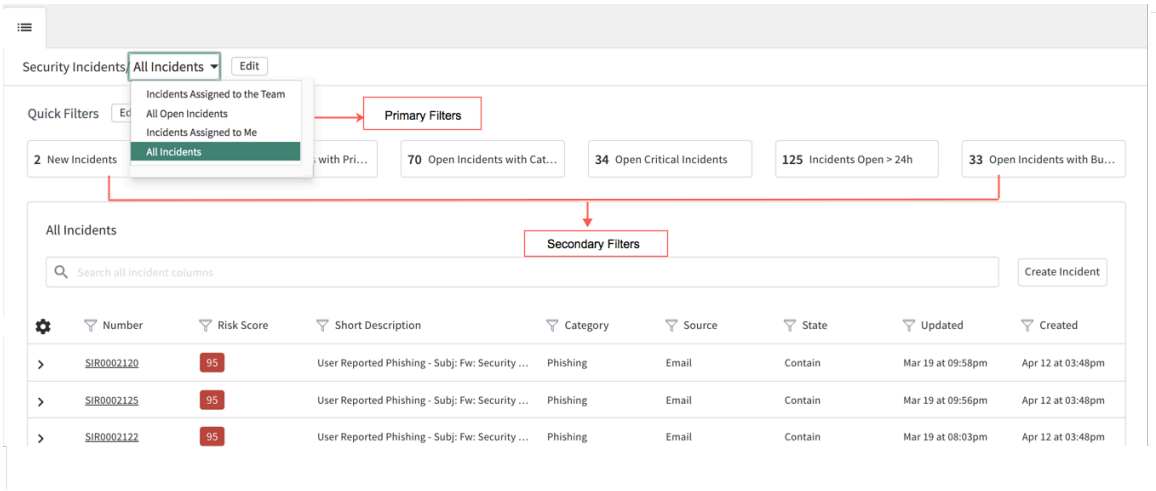
- 방문 페이지 필터 구성
- UI 작업 사용
- 양식 UI 작업
- 관련 목록 구성
- 관련 목록 UI 작업
- 양식 구성 시스템 속성
- 분석가 선택을 위해 플레이북 사용

방문 페이지 필터 구성

에 나타나는 새 필터를 추가하거나 기존 필터를 수정할 수 있습니다 보안 분석가 작업 공간.

에는 보안 분석가 작업 공간 분석하려는 보안 인시던트를 빠르게 찾을 수 있도록 보안 인시던트 목록을 필터링할 수 있는 기본 및 보조 필터가 있습니다. 자세한 내용은 를 참조하십시오 를 사용하여 보안 위협 관리 보안 분석가 작업 공간.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



새 필터 작성

1. 다음으로 이동 보안 인시던트 〉 분석가 작업 공간 설정(신규 **UI**) 〉 방문 페이지 필터 구성.
2. 새로 만들기를 클릭합니다.
3. 필터 제목을 입력하고 필터 조건을 지정한 후 제출 을 클릭하여 이전 페이지로 돌아갑니다.

   페이지에 새로 추가된 필터가 표시됩니다.
4. 이 필터에 대한 태그를 추가하여 기본 필터인지 보조 필터인지 나타냅니다. 다음과 같은 태그를 사용할 수 있습니다.
   - SN_SI_Primary
   - SN_SI_Secondary

기존 필터 편집

다음을 수행할 수도 있습니다.

- 기존 필터 수정하기: 기존 필터의 제목을 클릭하십시오. 제목과 필터 조건을 수정하고 업데이트를 클릭합니다.
- 태그 수정: 필터를 선택하고 방문 페이지 필터 구성에서 태그 열을 클릭합니다. 기존 태그를 삭제하거나 필터에 대한 새 태그를 추가할 수 있습니다.

UI 작업 사용

UI 작업을 구성하기 전에 에서 구성에 사용할 수 있도록 특정 단계를 수행하여 활성화해야 합니다 보안 분석가 작업 공간.

> **주:**
> UI 작업을 수정하려면 다음 역할을 가진 사용자로 로그인하십시오.
>
> - ui_action_admin
> - ui_page_admin
> - web_service_admin

다음에 대해 구성할 수 있는 UI 작업에는 두 가지 유형이 있습니다.보안 분석가 작업 공간

- 대화 상자 기반 UI 작업
- 서버 측 UI 동작

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

대화 상자 기반 **UI** 작업

에서 보안 분석가 작업 공간대화 상자 기반 UI 작업을 사용하려면 해당 표준 UI 작업과 연결된 UI 페이지를 다음과 같이 변경합니다.

1. **HTML** 섹션: *##* 입력 태그를 포함하도록 HTML 섹션을 수정합니다. *##* 입력 태그 값은 클라이언트 스크립트 섹션에서 UI 페이지가 에서 시작보안 분석가 작업 공간되었는지 식별하는 데 사용됩니다. 예를 들면 다음과 같습니다.

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

2. 클라이언트 스크립트: *##* 플래그가 예일 때 클라이언트 스크립트에 추가 논리를 작성해야 합니다. 이는 대화 상자의 일부로 표시되는 제출 및 취소 버튼 이벤트를 처리하는 데 필요합니다.

   a. onCancel() 이벤트 핸들러는 다음에서 'SIR_WORKBENCH_POPUP_CANCEL' 이벤트를 디스패치해야 합니다. 보안 분석가 작업 공간

   b. onSubmit() 이벤트 핸들러는 다음에서 'SIR_WORKBENCH_POPUP_SUBMIT' 이벤트를 디스패치해야 합니다. 보안 분석가 작업 공간

3. *##* 입력 태그 값이 예일 때 "onSubmit" 작업이 아니오를 반환하도록 수정되었으므로 처리 스크립트의 실행을 컨텍스트에서 건너뜁니다보안 분석가 작업 공간. 처리 스크립트의 논리는 클라이언트 호출 가능 스크립트(GlideAjax API를 통해 호출됨) 또는 REST 자원 엔드포인트를 통해 처리되어야 합니다.

자세한 내용은 다음 샘플 UI 페이지를 참조하십시오.

- 관련 목록 UI 작업 예: 감시 목록에 게시(UI 페이지 이름: publish_to_watchlist)
- 양식 UI 작업 예: 문제 생성(UI 페이지 이름: create_prb_change_inc)

서버 측 **UI** 작업

서버 측 UI 작업을 사용하려면 다음을 수행해야 합니다.

표준 UI 작업 스크립트의 논리는 스크립팅된 REST 자원의 일부로 처리되어야 합니다.

자세한 내용은 다음 샘플 양식 UI 작업을 참조하십시오.

- 중단 작성
- 취소

양식 **UI** 작업

에 표시되는 UI 작업을 구성할 수 있습니다 보안 분석가 작업 공간.

필수 구성 요소:

UI 작업을 구성하기 전에 에서 구성에 사용할 수 있도록 특정 단계를 수행하여 활성화해야 합니다 보안 분석가 작업 공간. 자세한 내용은 UI 작업 사용 문서를 참조하십시오.

에 보안 분석가 작업 공간대한 양식 UI 작업을 구성하려면 다음 단계를 따르십시오.

1. 다음으로 이동 보안 인시던트 〉 분석가 작업 공간 설정(신규 **UI)** 〉 양식 **UI** 작업.
2. 다음 상세 정보를 입력합니다.

필드 이름	설명
작업	선택 목록에서 UI 작업을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드 이름	설명
유형	작업 유형을 선택합니다. 다음과 같을 수 있습니다. ○ 대화 상자 기반 작업: 이 유형의 작업은 특정 비즈니스 논리를 실행하기 위해 사용자 상호 작용 또는 입력이 필요한 경우에 사용됩니다. ○ 서버 측 작업: 이 작업은 추가 사용자 입력 없이 필요한 비즈니스 논리를 실행합니다. 주: UI 작업을 구성하기 전에 에서 구성에 사용할 수 있도록 특정 단계를 수행하여 활성화해야 합니다 보안 분석가 작업 공간. 자세한 내용은 UI 작업 사용 문서를 참조하십시오.
애플리케이션	UI 작업이 추가되는 애플리케이션 범위(보안 인시던트 응답 UI)의 이름이 여기에 표시됩니다.
대화 상자 기반 작업 유형 필드에서 대화 상자 기반 작업을 선택하는 경우 다음 상세 정보를 입력합니다.	
UI 페이지	작업과 연결된 UI 페이지를 선택합니다.
대화 상자 제목	대화 상자 작업의 제목을 입력합니다.
대화 상자 너비 및 높이	대화 상자의 높이와 너비를 픽셀 단위로 입력합니다.
스크립트	선택한 UI 페이지에 대해 여기에서 추가 쿼리 매개변수를 지정할 수 있습니다. 기본 시스템과 함께 제공되는 템플릿은 sysparm_sys_id 매개변수만 생성하고 반환합니다. 여기에서 다른 매개변수를 지정하여 이를 재정의할 수 있습니다.
서버 측 작업 유형 필드에서 서버 측 작업을 선택하는 경우 다음 상세 정보를 입력합니다.	
스크립팅된 REST 자원	작업을 정의하는 스크립팅된 REST 자원을 선택합니다. 주: **SIR UI ANALYST** ACL을 REST 자원에 추가해야 합니다.

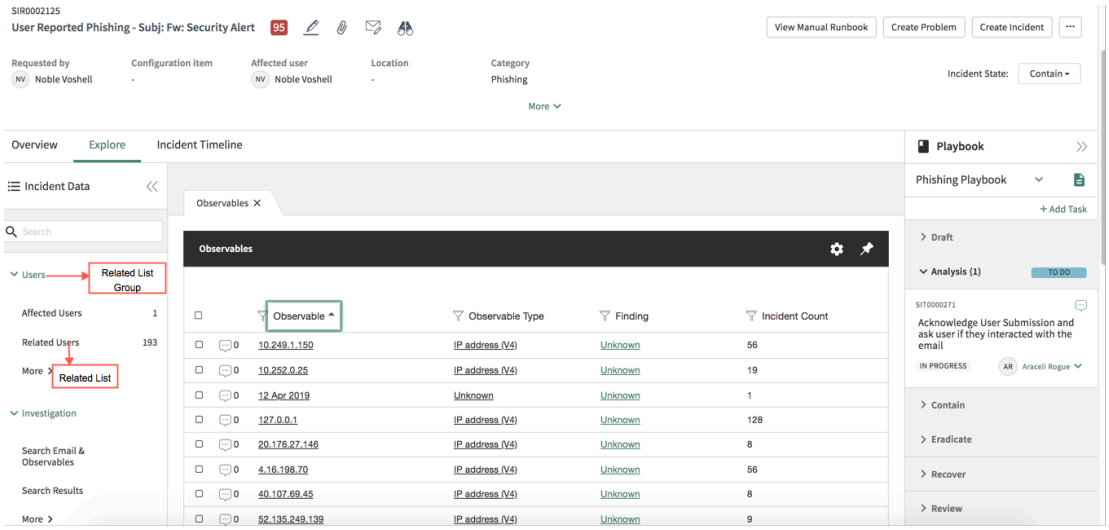
3. 제출을 클릭합니다.
4. 다음으로 이동 보안 인시던트 〉 인시던트(신규 **UI)** 페이지.
5. 보안 인시던트 기록을 보려면 보안 인시던트 번호를 클릭하십시오. 페이지 상단에서 새 UI 작업을 확인할 수 있습니다.

기존 양식 UI 작업을 수정하려면 작업 이름을 클릭하여 양식 UI 작업 페이지로 이동합니다. 선택한 유형을 기반으로 작업 이름, 유형 및 나머지 필드를 수정할 수 있습니다.

관련 목록 구성

새 관련 목록 또는 새 관련 목록 그룹을 추가하고 에 표시되는 기존 그룹 또는 관련 목록을 수정할 수 있습니다 보안 분석가 작업 공간.

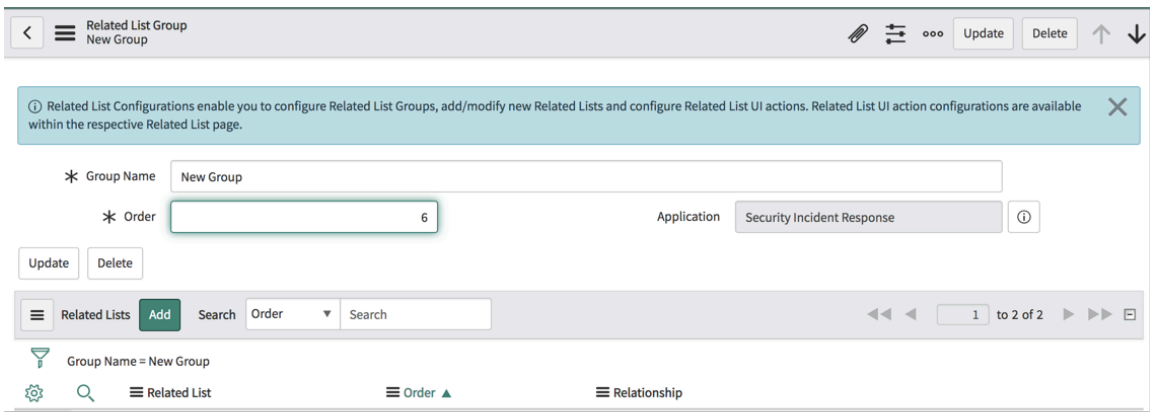
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



관련 목록 그룹 추가

관련 목록 그룹을 추가하려면 다음 단계를 수행합니다.

1. 다음으로 이동 보안 인시던트 〉 분석가 작업 공간 설정(신규 **UI)** 〉 관련 목록 구성.
2. 새로 만들기를 클릭하여 새 관련 목록 그룹을 추가합니다. 그룹 이름과 인시던트(새 UI) 페이지에 표시되는 순서를 입력합니다.
3. 제출을 클릭합니다. 새로 추가된 그룹이 관련 목록 그룹 페이지에 나타납니다.



관련 목록 추가

새 관련 목록을 추가하려면 다음 단계를 수행합니다.

1. 관련 목록 그룹 링크를 클릭합니다.
2. 관련 목록 섹션에서 추가를 클릭하여 새 관련 목록을 추가합니다.

   추가 버튼이 보이지 않으면 관련 목록 그룹과 동일한 애플리케이션 범위에 있는지 확인합니다.
3. 그룹에 포함할 관련 목록을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
특정 관련 목록이 표시되지 않으면 다음을 수행합니다.

a. 다음으로 이동 시스템 **UI** 〉 관련 목록 *# #### sn_si_incident* 테이블에 있는 관련 목록을 검색합니다.

b. **SIR** 새 **UI**뷰와 연결된 *sn_si_incident* 테이블을 클릭합니다.

c. 관련 목록 항목 섹션에서 새로 만들기를 클릭하여 **SIR** 새 **UI** 뷰에 관련 목록을 추가합니다.

4. 표시되는 순서를 지정하고 제출을 클릭합니다.

추가한 관련 목록이 에 나타납니다 보안 분석가 작업 공간.

기존 관련 목록 그룹을 수정하려면 그룹 이름을 클릭하여 관련 목록 그룹 페이지로 이동합니다. 그룹 이름, 순서를 수정하고 그룹에서 관련 목록을 추가 또는 삭제할 수 있습니다.

관련 목록 **UI** 작업

에 보안 분석가 작업 공간표시되는 관련 목록에 새 UI 작업을 추가할 수 있습니다.

필수 구성 요소:

UI 작업을 구성하기 전에 에서 구성에 사용할 수 있도록 특정 단계를 수행하여 활성화해야 합니다 보안 분석가 작업 공간. 자세한 내용은 UI 작업 사용 문서를 참조하십시오.

새 관련 목록 UI 작업을 추가하려면 다음 단계를 따르십시오.

1. 다음으로 이동 보안 인시던트 〉 분석가 작업 공간 설정(신규 **UI**) 〉 관련 목록 구성.
2. 그룹 이름을 클릭합니다. 관련 목록 그룹 구성 페이지가 표시됩니다.
3. UI 작업을 추가할 관련 목록을 클릭합니다.
4. 관련 목록 UI 작업 섹션에서 추가를 클릭합니다.
5. 다음 상세 정보를 입력합니다.

필드 이름	설명
작업	선택 목록에서 UI 작업을 선택합니다.
유형	작업 유형을 선택합니다. 다음과 같을 수 있습니다. ○ 대화 상자 기반 작업: 이 유형의 작업은 특정 비즈니스 논리를 실행하기 위해 사용자 상호 작용 또는 입력이 필요한 경우에 사용됩니다. ○ 서버 측 작업: 이 작업은 추가 사용자 입력 없이 필요한 비즈니스 논리를 실행합니다. 주: UI 작업을 구성하기 전에 에서 구성에 사용할 수 있도록 특정 단계를 수행하여 활성화해야 합니다 보안 분석가 작업 공간. 자세한 내용은 UI 작업 사용 문서를 참조하십시오.
애플리케이션	UI 작업이 추가되는 애플리케이션 범위(보안 인시던트 응답 UI)의 이름이 여기에 표시됩니다.
대화 상자 기반 작업	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드 이름	설명
유형 필드에서 대화 상자 기반 작업을 선택하는 경우 다음 상세 정보를 입력합니다.	
UI 페이지	작업과 연결된 UI 페이지를 선택합니다.
대화 상자 제목	대화 상자 작업의 제목을 입력합니다.
대화 상자 너비 및 높이	대화 상자의 높이와 너비를 픽셀 단위로 입력합니다.
스크립트	선택한 UI 페이지에 대해 여기에서 추가 쿼리 매개변수를 지정할 수 있습니다. 기본 시스템과 함께 제공되는 템플릿은 sysparm_incident_id, sysparm_record_table 및 sysparm_related_sys_ids 매개변수만 구성하고 반환합니다. 여기에서 다른 매개변수를 지정하여 재정의할 수 있습니다.
서버 측 작업 유형 필드에서 서버 측 작업을 선택하는 경우 다음을 지정합니다.	
스크립팅된 REST 자원	작업을 정의하는 스크립팅된 REST 자원을 선택합니다. 주: **SIR UI ANALYST** ACL을 REST 자원에 추가해야 합니다.

6. 제출을 클릭합니다.
7. 다음으로 이동 보안 인시던트 〉 인시던트(신규 **UI)** 페이지.
8. 보안 인시던트 기록을 보려면 보안 인시던트 번호를 클릭하십시오. 해당 관련 목록을 시작하여 새 UI 작업을 확인합니다.

양식 구성 시스템 속성

이러한 시스템 속성은 플레이북 작업에 대한 양식 새로 고침 간격을 정의합니다.

이러한 속성을 구성하려면 다음으로 이동합니다. 분석가 작업 공간 설정(신규 **UI)** 〉 분석가 작업 공간 속성.

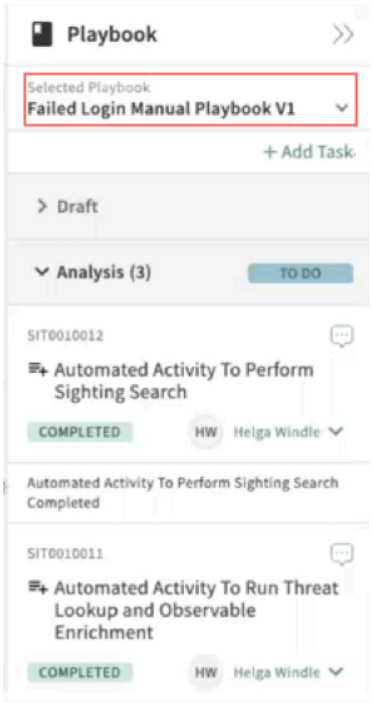
속성	기본값	설명
sn_app_secops_ui.poller_interval.playbook_tasks	10000 밀리세컨드	구성된 모든 간격 시간에 대해 응답 작업을 새로 고침하기 위해 플레이북 구성요소에서 사용하는 간격 시간입니다.
sn_app_secops_ui.poller_interval_count.playbook_tasks	3 회	Playbook 구성요소가 응답 작업을 폴링하는 횟수입니다.
sn_app_secops_ui.poller_interval.related_list	30000 밀리세컨드	이 간격 시간은 탐색 구성요소에서 구성된 모든 간격 시간에 대해 관련 목록 수를 새로 고치는 데 사용됩니다.

분석가 선택을 위해 플레이북 사용

플레이북 선택 목록에 새 플레이북을 추가합니다.

()를 사용하여 보안 위협 관리 보안 분석가 작업 공간에서 보안 분석가 작업 공간 적절한 플레이북을 선택하여 보안 인시던트를 조사할 수 있습니다. 플레이북 선택 옵션은 플로우 디자이너를 사용하여 설계된 플레이북만 지원합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



Flow Designer를 사용하여 플레이북을 생성한 후 다음 단계에 따라 선택한 플레이북 선택 목록에 포함합니다.

1. *sys_hub_flow* 테이블로 이동합니다.
2. Flow Designer를 사용하여 만든 새 플레이북을 검색합니다.
3. 선택한 플레이북 선택 목록에 포함하려는 플레이북에 **sir_playbook** 태그를 추가합니다.

주:
워크플로우에서 Flow Designer로 마이그레이션되지 않은 이전 Playbook이 있는 경우에는 목록에 표시되지 않습니다. 그러나 워크플로우를 사용하여 생성된 플레이북이 트리거 조건 또는 수동 선택(클래식 환경에서 오케스트레이션 실행 옵션 사용)에 의해 보안 인시던트에 할당된 경우, 에서 보안 인시던트 보안 분석가 작업 공간를 열면 이 플레이북이 시작됩니다.

Security Incident Response 문제 해결

이 섹션에서는 보안 인시던트 응답과 관련된 중요한 문제 해결 팁과 자주 묻는 질문을 다룹니다.

접근 제어 규칙 문제

접근 제어 규칙은 다음 세 조건이 모두 충족될 경우 지정된 자원에 대한 접근을 허용합니다.

- 사용자가 역할 목록에 지정된 역할 중 하나를 가지고 있거나 목록이 비어 있습니다.
- 조건 필드의 조건이 true로 평가되거나 조건이 비어 있습니다.
- 스크립트 필드(고급)의 스크립트가 true로 평가되거나, 변수 대답을 true로 설정하거나, 비어 있습니다.

접근 제어 규칙에 대한 자세한 내용은 다음을 참조하십시오. Explore Access Control Lists

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

중요사항:
보안 인시던트 테이블에 대해 관리자 무효화 옵션이 선택 취소되어 있고 관리자가 보안 인시던트 테이블에 액세스할 수 있는 경우 문서를 참조하십시오 KB1444673

보안 인시던트 응답 플랫폼 분석 솔루션

플랫폼 분석 솔루션에는 사전 구성된 대시보드가 포함되어 있습니다. 대시보드는 새로운 보안 인시던트 또는 미해결 보안 인시던트의 평균 연령과 같은 프로세스를 분석하는 보안 인시던트 응답에 중요한 메트릭을 제공합니다.

플랫폼 분석 데이터 시각화는 퍼포먼스 분석 표시기 데이터를 사용하여 시간 경과에 따른 데이터를 표시함으로써 비즈니스 프로세스를 분석하고 개선 영역을 식별하는 데 도움이 됩니다. 플랫폼 분석 솔루션을 사용하면 최소한의 설정으로 애플리케이션에 대한 퍼포먼스 분석을 통해 가치를 얻을 수 있습니다. 또한 사용자 고유의 개체를 만들 수도 있습니다.

보안 인시던트 응답 퍼포먼스 분석 솔루션은 에서 사용할 수 있습니다ServiceNow Store. 이 애플리케이션의 다운로드 및 설치에 대한 자세한 내용은 보안 운영 및 ServiceNow Store를 참조하십시오.

주:
기능을 평가하기 위해 퍼포먼스 분석의 라이센스가 부여되지 않은 인스턴스에서 퍼포먼스 분석 솔루션 및 양식 내 분석을 활성화할 수 있습니다. 그러나 다음과 같은 제한 사항이 있습니다.

- 새 표시기를 만들 수 없습니다.
- 180일 이상된 데이터는 수집할 수 없습니다.

모든 기능을 사용하려면 퍼포먼스 분석 라이센스가 필요합니다. 자세한 내용은 퍼포먼스 분석 구독 활성화 를 참조하십시오.

중요사항:
기본적으로 퍼포먼스 분석의 *(com.snc.pa.dc.max_records)* 속성에 대한 데이터 수집 제한은 기록 5,000개로 설정됩니다. 그러나 요구 사항에 따라 이 한도를 늘릴 수 있습니다(예: 기록 50,000개). 그러나 이 제한을 늘리면 데이터 수집 중 또는 스냅샷 테이블에서 작업을 수행할 때 성능에 영향을 줄 수 있습니다. 퍼포먼스 분석 속성에 대한 자세한 내용은 다음 문서를 참조하십시오 Performance Analytics properties .

관련 정보

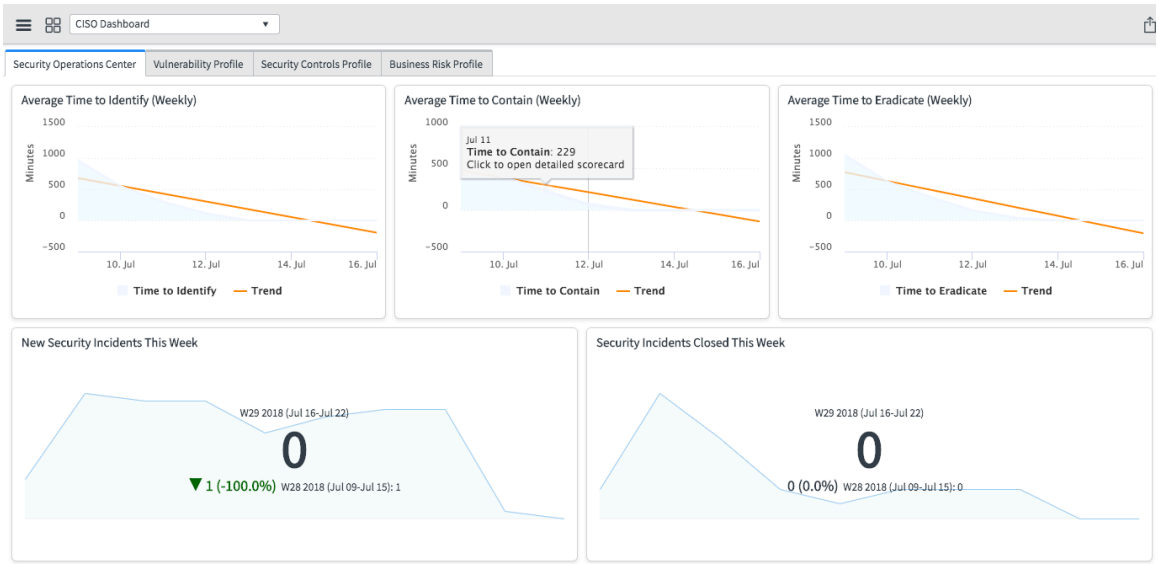
퍼포먼스 분석 구독 활성화

CISO 대시보드

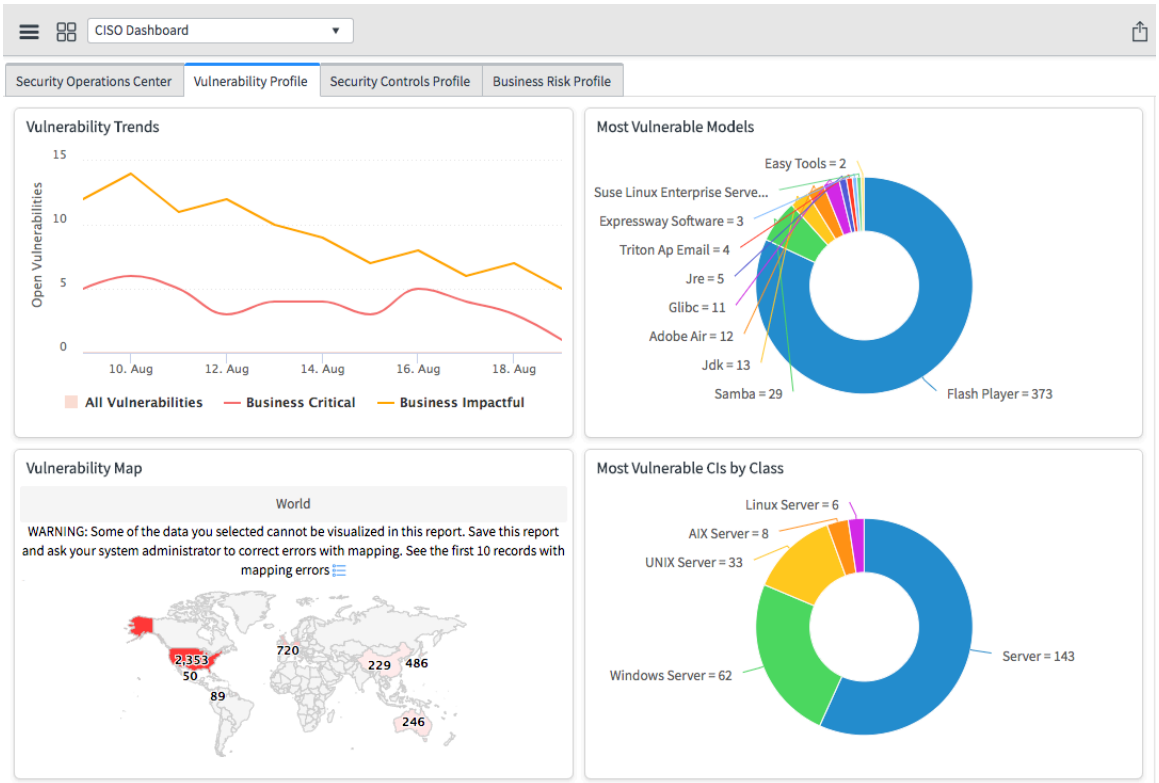
이 대시보드는 보안 취약성 및 인시던트를 포함하여 조직의 전반적인 보안 태세를 보여줍니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 운영 센터 탭

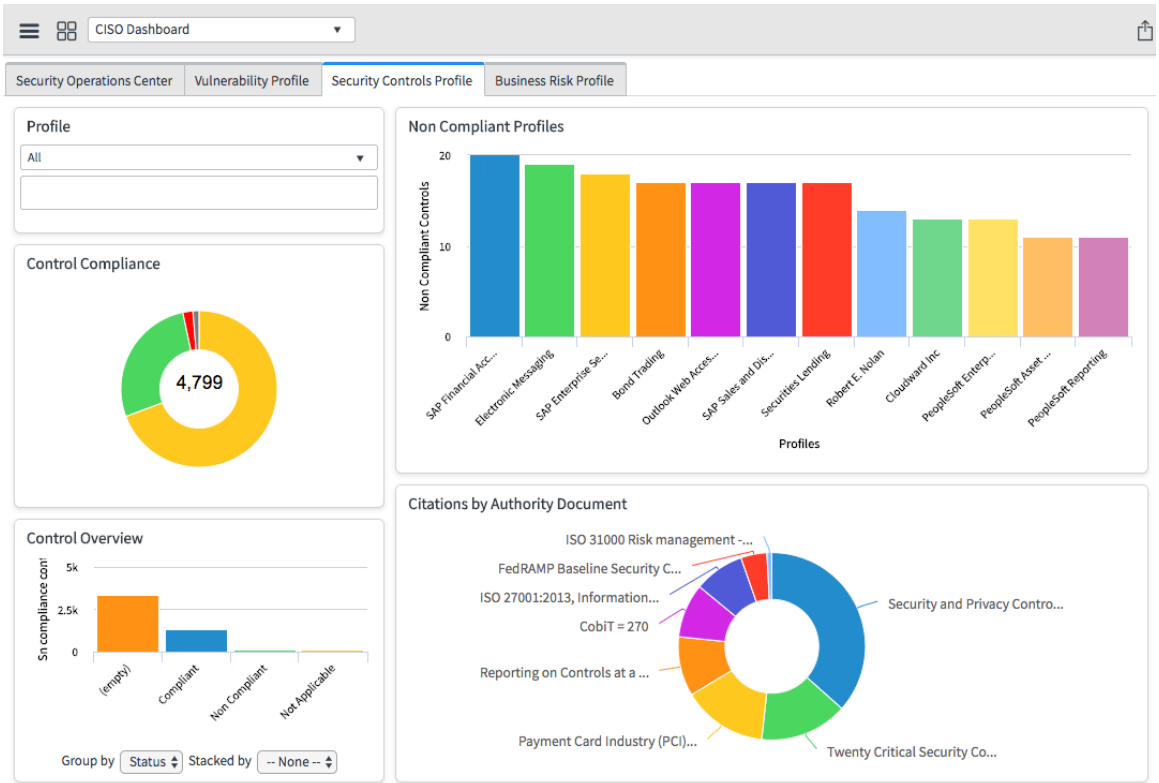


취약성 프로파일 탭

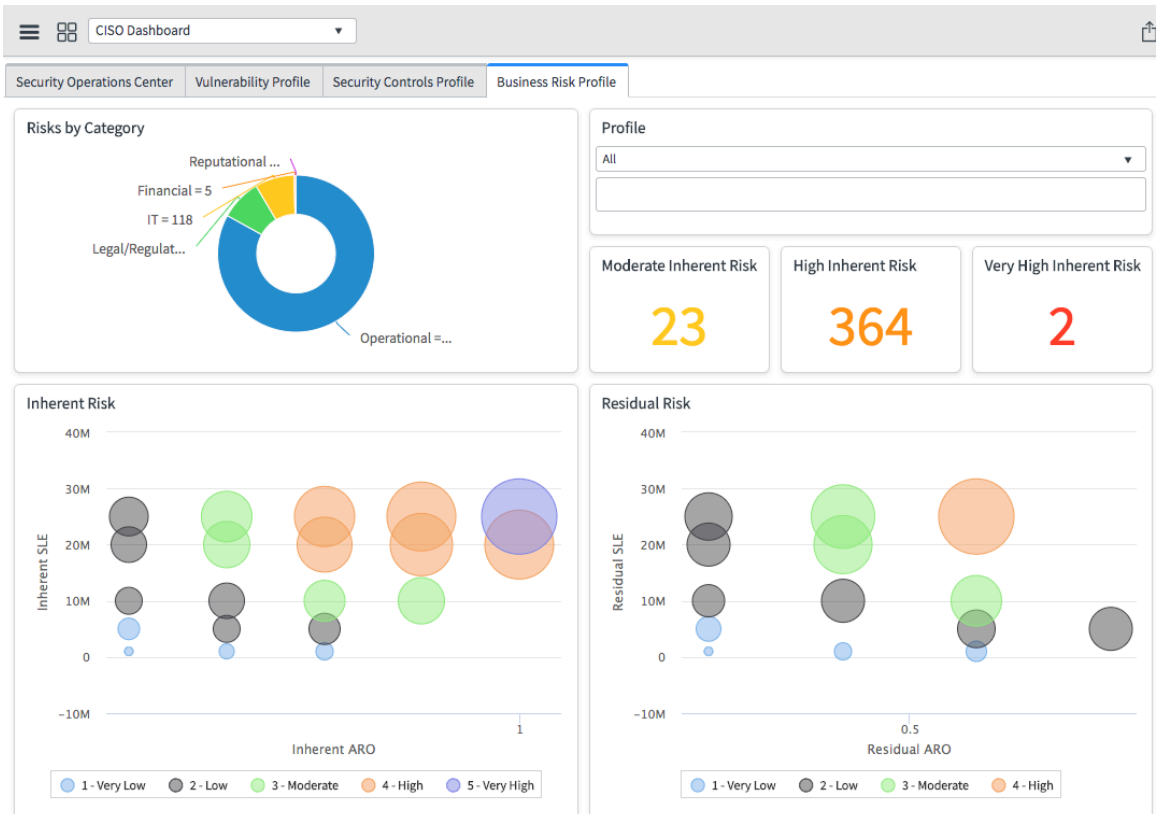


© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 통제 프로파일 탭



비즈니스 위험 프로파일 탭



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

최종 사용자 및 역할

최종 사용자 및 목표	필요한 역할
CISO: 전체 조직의 현재 보안 태세에 대한 명확한 가시성이 필요합니다.	sn_si.ciso

CISO 대시보드 표시기

CISO 대시보드에는 다음과 같은 핵심성과지표가 표시됩니다.

SI - 평균 식별 시간

보안 인시던트를 식별하는 데 걸리는 7일 평균 시간(분)으로, 매일 계산됩니다.

평균 포함 시간

보안 인시던트를 억제하는 데 걸리는 7일 평균 시간(분)으로, 매일 계산됩니다.

평균 근절 시간

보안 인시던트를 근절하는 데 걸리는 7일 평균 시간(분)으로, 매일 계산됩니다. 평균 포함 시간과 평균 근절 시간은 모두 SI - 보안 인시던트 상태별 평균 기간 시간 표시기를 기반으로 합니다.

새 보안 인시던트 금주

일일 새 보안 인시던트 수 표시기 점수의 주간 합계입니다.

종결된 보안 인시던트(주간)

일일 종결된 보안 인시던트 수 표시기의 7일 실행 합계입니다.

우선순위별 새 보안 인시던트

우선순위별 새로운 보안 인시던트 수 표시기의 일일 세부 항목입니다.

신규 보안 인시던트 대 종결된 보안 인시던트(주간) 볼륨

종결된 인시던트 수 표시기의 7일 실행 합계 시계열에 대해 차트로 표시된 새 인시던트 수 표시기의 7일 실행 합계 시계열

보안 인시던트 히트맵

각 국가의 미해결 보안 인시던트 수를 보여주는 글로벌 맵입니다.

보안 인시던트 트리맵

다음을 확인하기 위해 선택할 수 있는 대화형 트리맵:

- 비즈니스 중요도별로 세분화된 비즈니스 서비스별 보안 인시던트
- 인시던트의 범주 또는 하위 범주별로 세분화된 보안 인시던트
- 할당 그룹별 또는 담당자별 보안 인시던트
- 영향을 받는 자원 또는 영향을 받는 사용자당 보안 인시던트의 "피해자 통계"

세부 항목

다음 세부 항목은 대시보드의 지표에 적용됩니다.

- 비즈니스 중요도
- 보안 그룹
- 보안 인시던트 기간
- 보안 인시던트 범주
- 보안 인시던트 종결 코드

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 보안 인시던트 우선순위
- 보안 인시던트 상태
- SI - 비즈니스 서비스
- 취약성

데이터 시각화

대시보드에는 다음과 같은 시각화가 있습니다.

제목	유형	설명
담당 그룹 및 상태별 30일 이상된 보안 인시던트	히트맵	가장 취약한 항목이 있는 모델을 표시합니다.
범주별 위험	도넛형	재개시된 취약한 항목의 기간을 나열합니다.
권한 문서에 의한 인용	도넛형	활성 취약성 수
활성 상태가 아닌 담당자가 있는 보안 인시던트	히트맵	취약성과 관련된 미해결된 취약한 항목 (CVE(일반적인 취약성 열거형) 레코드)의 수를 가장 많은 항목에서 가장 작은 항목 순으로 표시합니다.
할당 그룹 및 상태별 30일 이상 업데이트되지 않은 보안 인시던트	히트맵	가장 취약한 항목이 있는 게시자를 표시합니다.
취약성 맵	맵	위치별 취약성을 보여주는 월드 맵
가장 취약한 모델	도넛형	취약성이 가장 많은 애플리케이션
클래스별 가장 취약한 CI	도넛형	서버 유형별 CI
중요 중요 취약성이 있는 서비스	목록	
규정 미준수 프로필	막대	프로파일별 규정 미준수 통제
통제 개요	막대	준수 및 미준수 통제의 수
정책 예외	목록	우선순위, 소유자 및 짧은 설명이 있는 정책 예외
범주별 위험	도넛형	위험의 각 범주에 있는 위험의 수
고유 위험	거품형	고유 SLE 대 고유 ARO
남은 위험	거품형	잔여 SLE 대 잔여 ARO

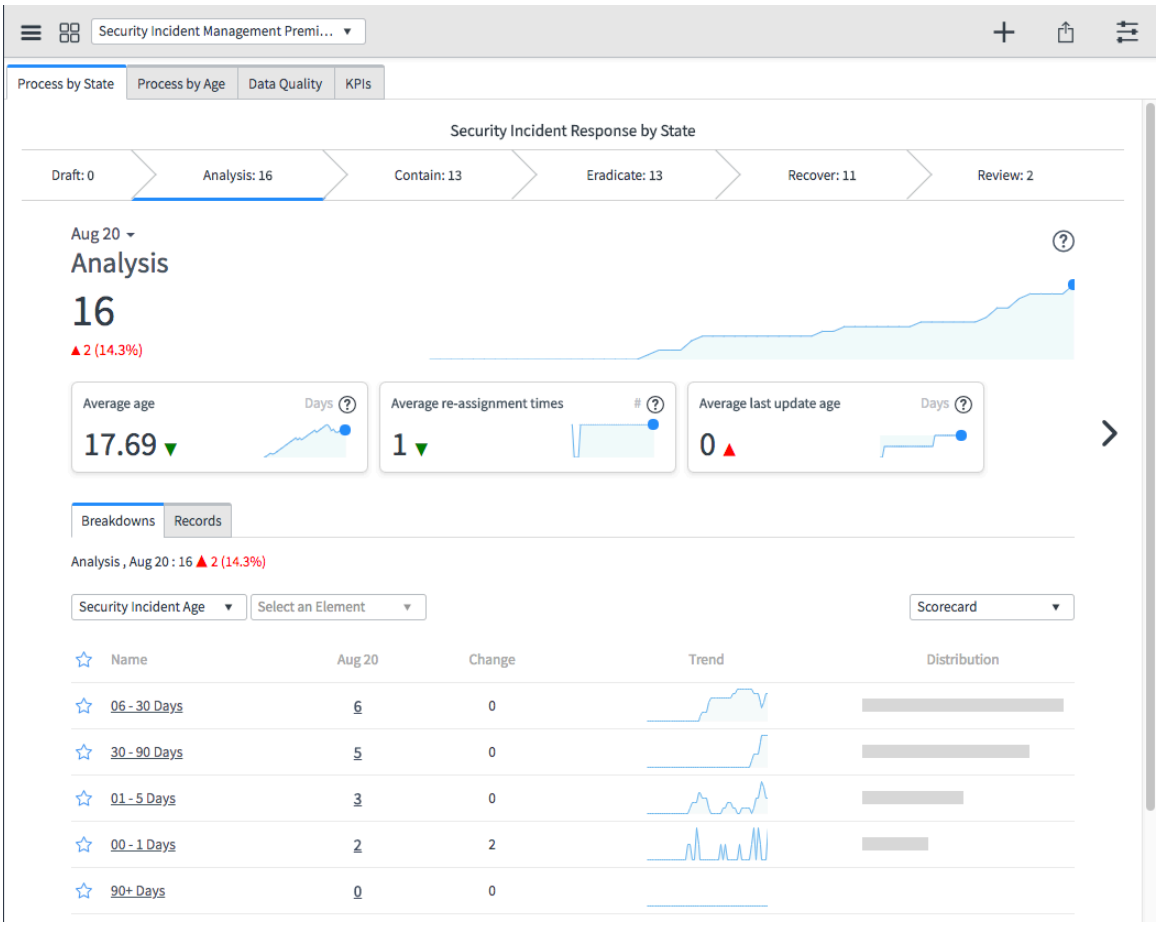
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

제목	유형	설명
보통, 높음 및 매우 높은 위험	점수	보통 위험, 높은 위험 및 매우 높은 위험의 수 각각
프로파일별 위험	누적 가로 막대형	그룹화 기준과 스택 기준으로 선택할 수 있는 위험 수

Security Incident Management 프리미엄 대시보드

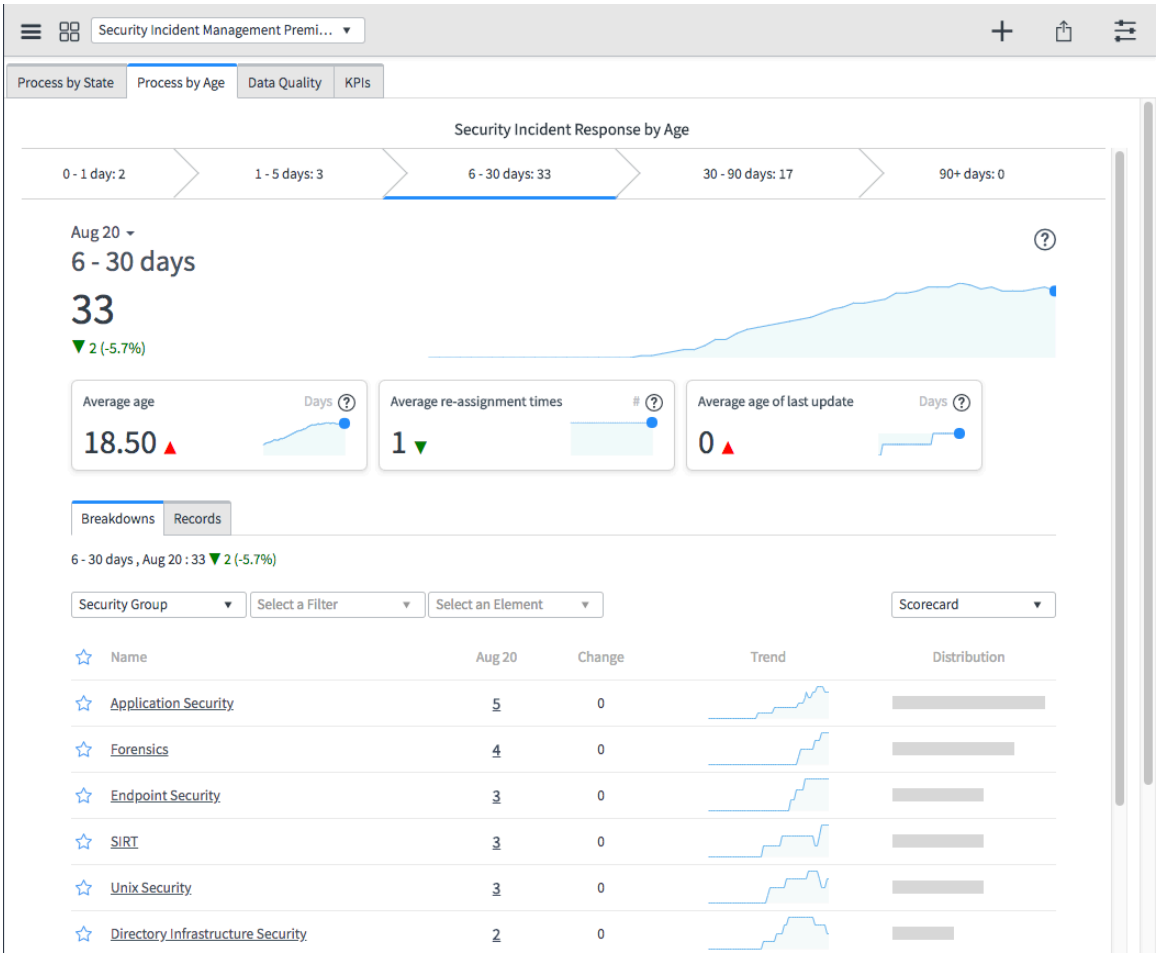
이 대시보드는 고급 플랫폼 분석 시각화를 사용하여 보안 관리자가 초기 분석/탐지에서 억제, 근절 및 복구에 이르기까지 보안 인시던트의 볼륨, 성능 및 진행 상황을 추적할 수 있도록 지원합니다. 따라서 라이센스가 퍼포먼스 분석 부여된 버전이 필요합니다.

상태별 보안 인시던트 응답



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

연령별 보안 인시던트 응답



최종 사용자 및 역할

최종 사용자 및 목표	필요한 역할	혜택
보안 응답 관리자: 애플리케이션 및 서비스와 관련된 보안 인시던트의 전체 상태와 볼륨에 대한 명확한 가시성이 필요합니다.	sn_si.manager	할당 그룹의 구성원을 조정할 수 있는 기능을 사용하여 전반적인 보안 태세를 검토할 수 있습니다.
보안 응답 관리자: 관심 영역을 신속하게 찾아내고 필요에 따라 영역과 기술을 관리하면서 모든 보안 인시던트 응답 데이터를 완전히 제어할 수 있어야 합니다.	sn_si.admin	위험 계산 매개변수를 조정하여 조직과 가장 관련된 취약한 항목을 먼저 처리할 수 있습니다.
보안 응답 분석가: 조직에 대한 중요도에 따라 집중할 취약성의 우선순위를 신속하게 결정해야 합니다.	sn_si.analyst	계층 1 및 2 보안 분석가가 보안 인시던트에 대해 작업합니다. 보안 인시던트, 요청 및 작업은 물론 인시던트와 관련된 문제, 변경 및 중단을 생성하고 업데이트할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Security Incident Management 프리미엄 표시기

상태별 프로세스 및 연령별 프로세스 탭에는 다음 표시기가 있는 워크벤치 위젯이 포함되어 있습니다.

평균 기간

미해결 보안 인시던트의 평균 연령 표시기는 [[### ## ##### ## ##]] / [[### ## #### #]] / 24 수식을 사용하여 일 단위 결과를 제공합니다.

평균 재할당 시간

미해결 보안 인시던트의 평균 재할당 표시기는 ### ## ##### ### ## / ### ## #### # 수식을 사용합니다.

마지막 업데이트의 평균 연령

미해결 보안 인시던트의 마지막 업데이트 평균 연령 표시기는 ### ## ##### ### #### ## ## / ### ## #### # / 24 수식을 사용하여 일 단위로 결과를 제공합니다.

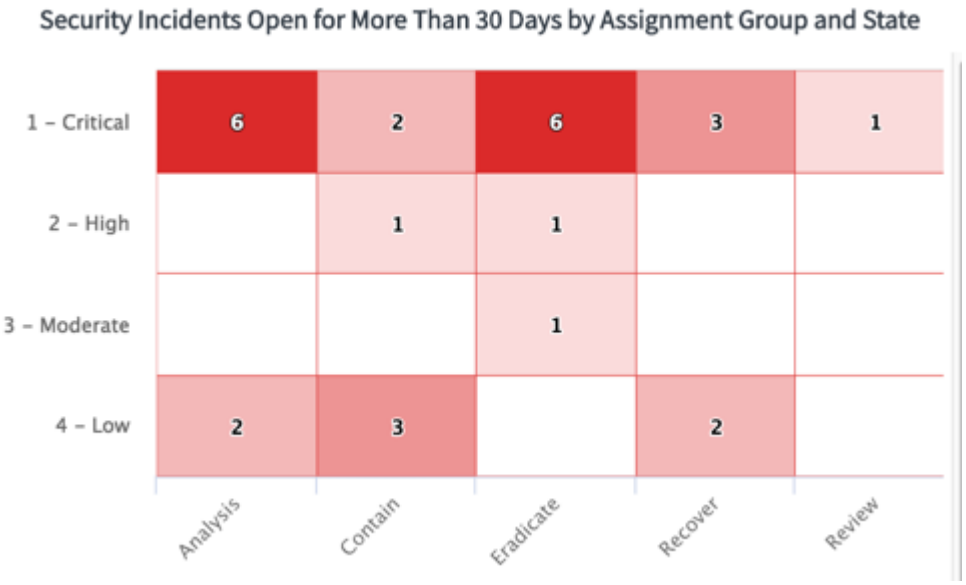
5일 동안 업데이트하지 않은 비율(%)

지난 5일 동안 업데이트하지 않은 미해결 보안 인시던트의 비율(%) 표시기는 ([[## 5# ## ###### ## ### ## #### #]] / [[### ## #### #]]) * 100 수식을 사용합니다.

데이터 품질 탭에는 보안 인시던트의 범주와 위험, 우선순위 및 심각도 수준에 대한 대화형 필터가 있습니다. 이러한 필터는 다음 표시기에 동시에 적용됩니다.

담당 그룹 및 상태별 30일 이상된 보안 인시던트

30일 동안 필터링되고 할당 그룹 및 상태별로 구분된 미해결 보안 인시던트 수입니다.



활성 상태가 아닌 담당자가 있는 보안 인시던트

담당자가 없거나 활성 상태가 아닌 미해결 보안 인시던트 수입니다.

담당 그룹 및 상태별 30일 이상된 보안 인시던트

할당 그룹 및 상태별로 구분된 지난 30일 동안 업데이트되지 않은 미해결 보안 인시던트 수 표시기입니다.

KPI 탭에는 다음과 같은 추가 표시기가 있습니다.

- 새 중요 보안 인시던트 비율(%)
- 오픈 보안 인시던트의 평균 연령
- 보안 인시던트 평균 종결 시간

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 재할당된 보안 인시던트 비율(%)
- 첫 할당에서 종결된 보안 인시던트 비율(%)
- 셀프 서비스로 종결된 보안 인시던트 비율(%)
- 해결되지 않은 보안 인시던트 비율(%)
- 보안 인시던트 작업의 평균 종결 시간

세부 항목

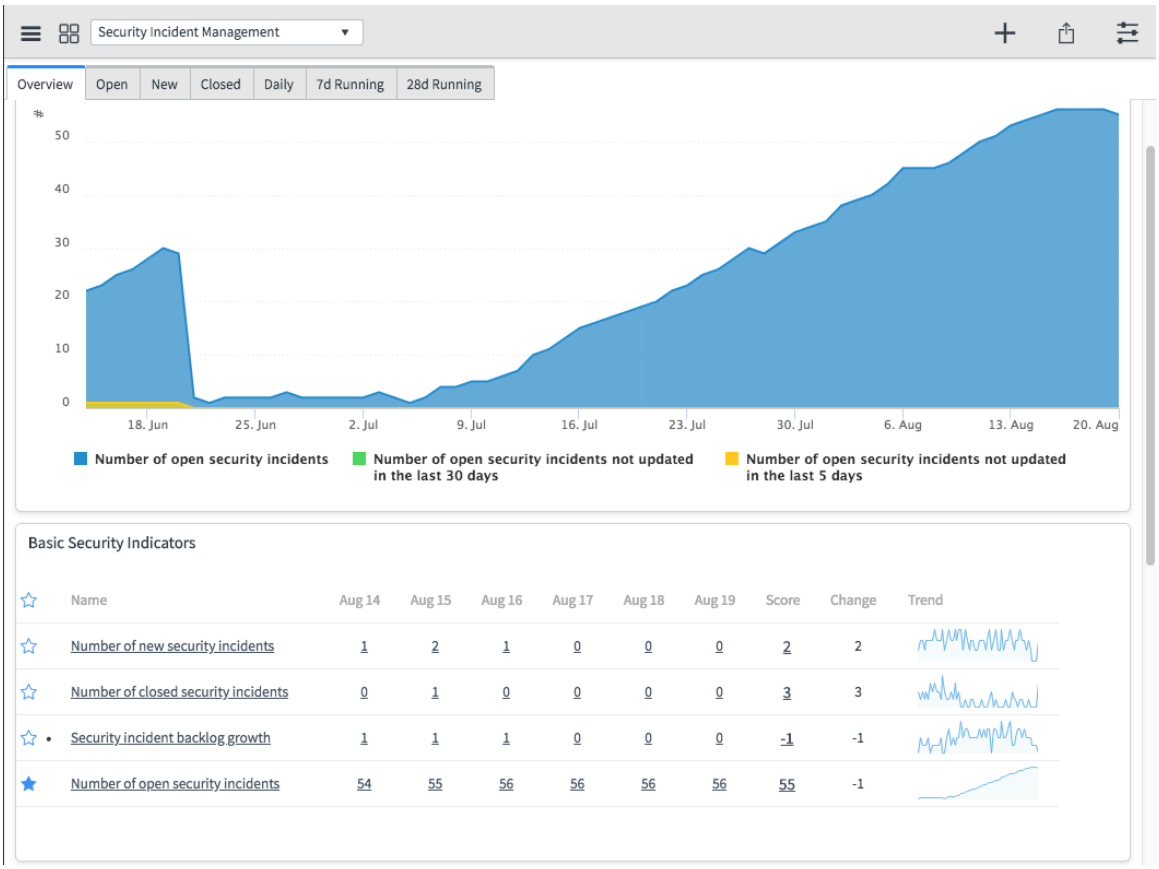
다음 세부 항목은 대시보드의 지표에 적용됩니다.

- 보안 그룹
- 보안 인시던트 기간
- 보안 인시던트 범주
- 보안 인시던트 우선순위
- 보안 인시던트 상태

Security Incident Management 대시보드

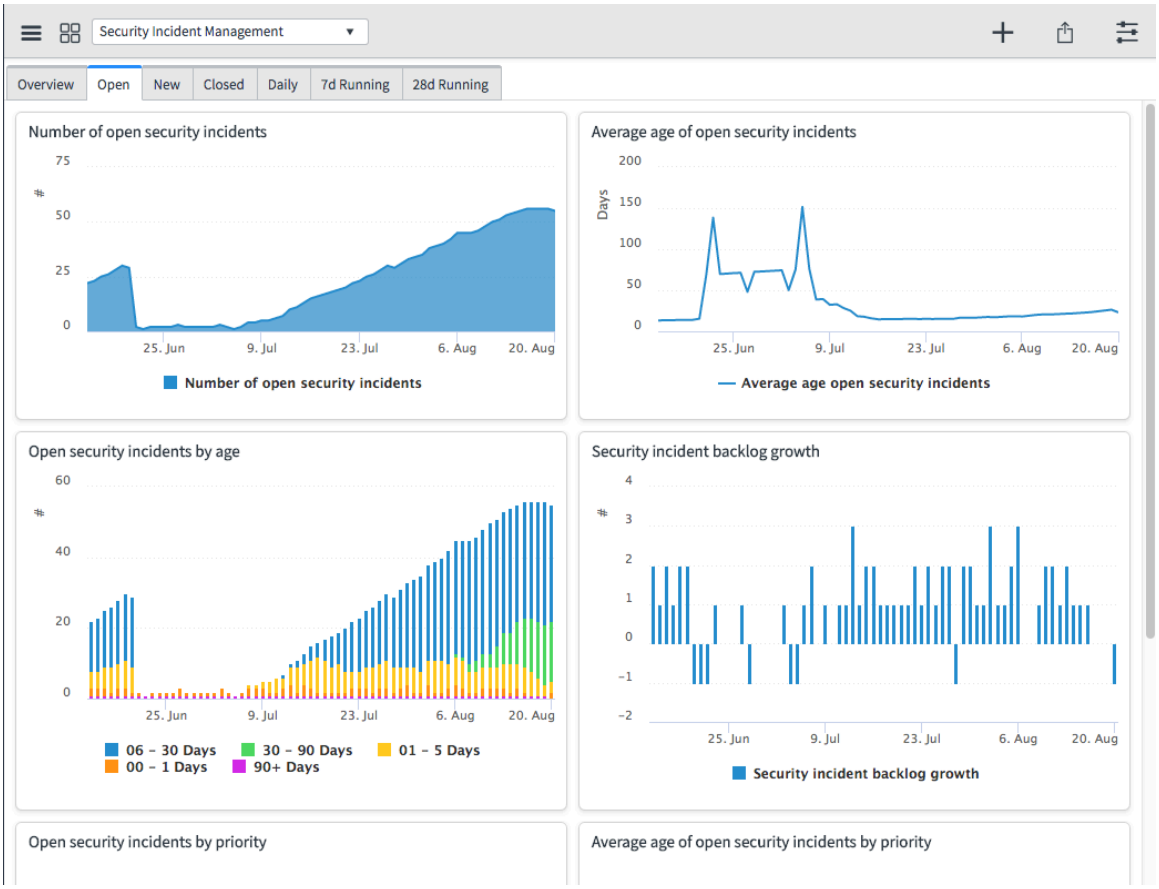
이 대시보드를 통해 보안 관리자는 초기 분석/탐지에서 억제, 근절 및 복구에 이르기까지 보안 인시던트의 볼륨, 성능 및 진행 상황을 쉽게 추적할 수 있습니다.

개요 탭

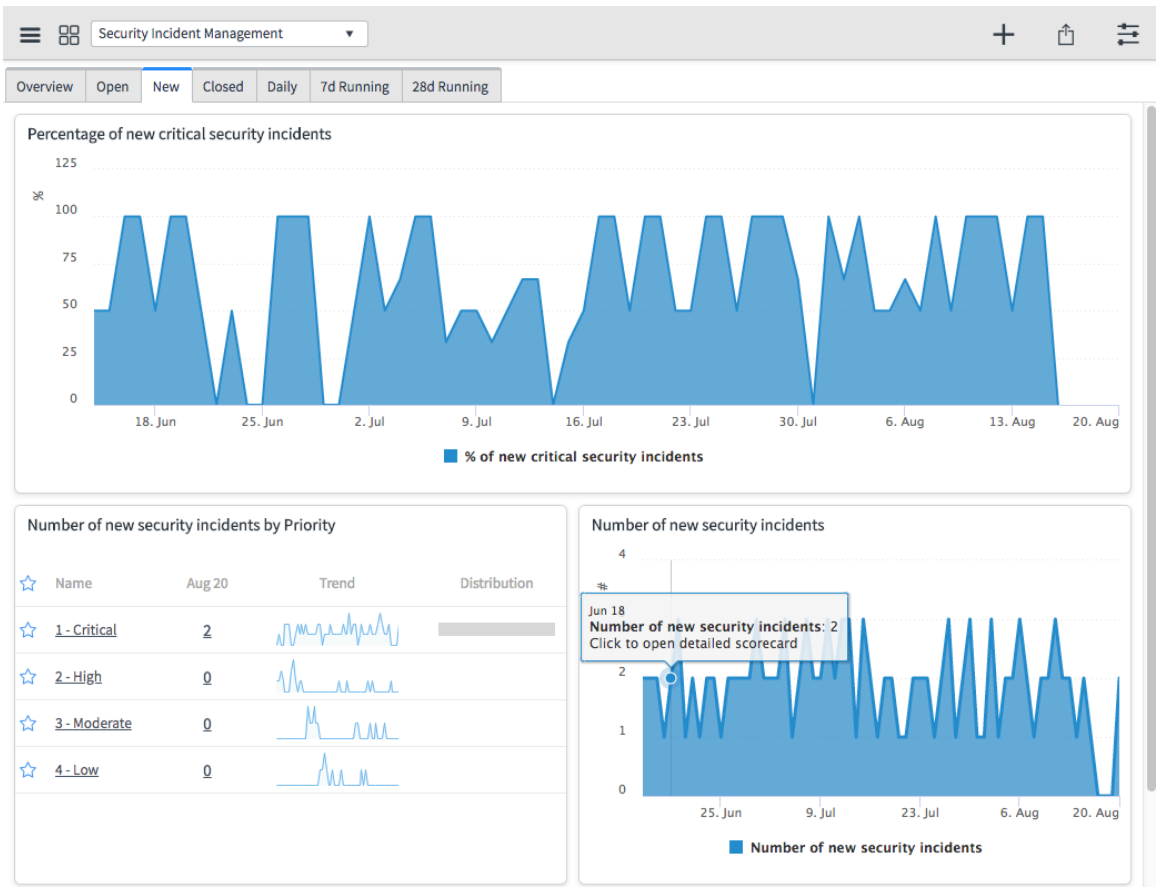


© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 인시던트 탭 열기



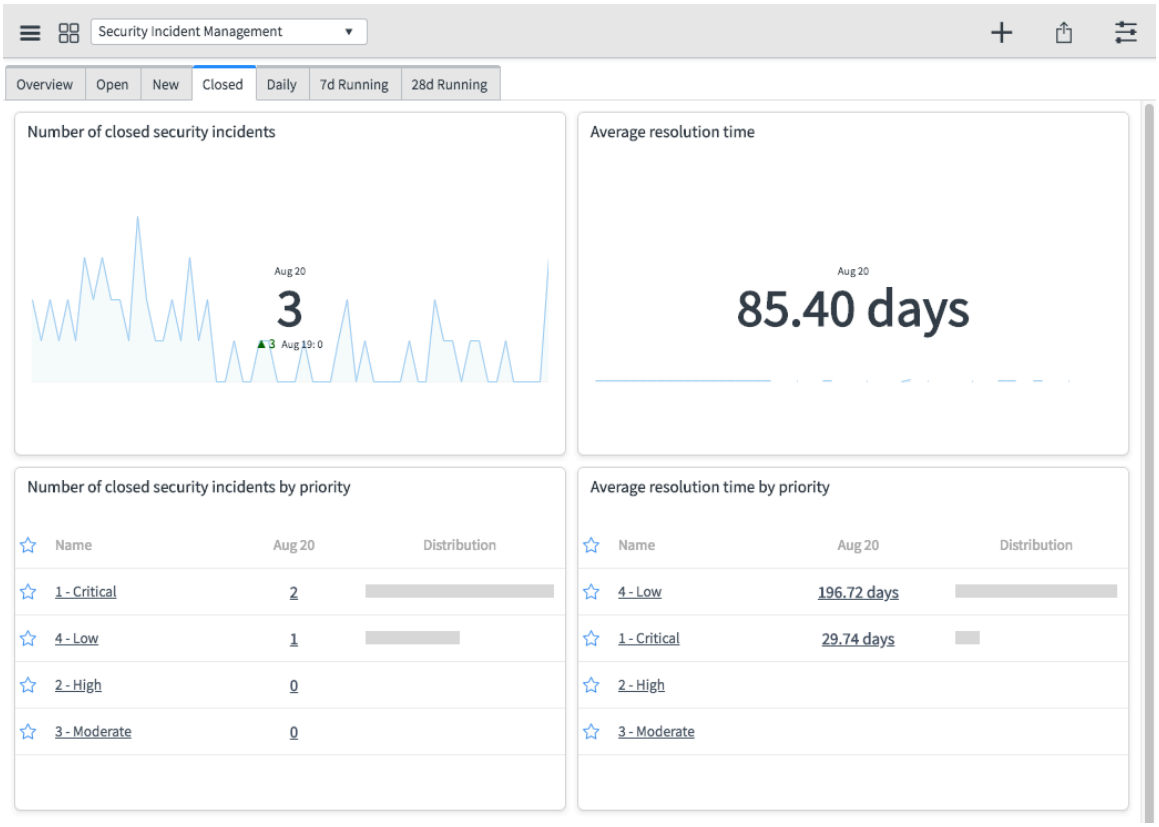
새 보안 인시던트 탭



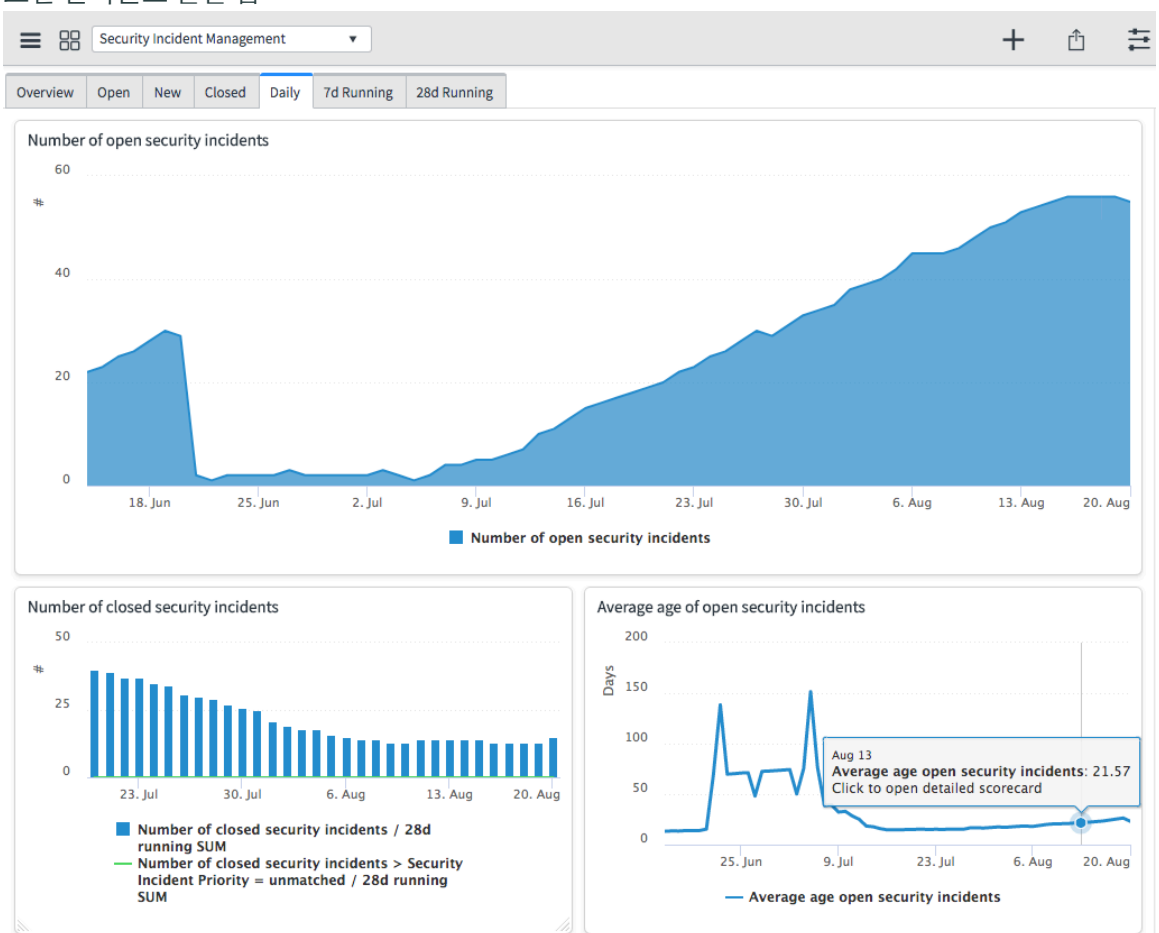
기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

종결된 보안 인시던트 탭



보안 인시던트 일일 탭



기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

7일 달리기 탭과 28일 달리기 탭은 일별 탭의 형식을 따릅니다.

최종 사용자 및 역할

최종 사용자 및 목표	필요한 역할	혜택
보안 응답 관리자: 애플리케이션 및 서비스와 관련된 보안 인시던트의 전체 상태와 볼륨에 대한 명확한 가시성이 필요합니다.	sn_si.manager	할당 그룹의 구성원을 조정할 수 있는 기능을 사용하여 전반적인 보안 태세를 검토할 수 있습니다.
보안 응답 관리자: 관심 영역을 신속하게 찾아내고 필요에 따라 영역과 기술을 관리하면서 모든 보안 인시던트 응답 데이터를 완전히 제어할 수 있어야 합니다.	sn_si.admin	위험 계산 매개변수를 조정하여 조직과 가장 관련된 취약한 항목을 먼저 처리할 수 있습니다.
보안 응답 분석가: 조직에 대한 중요도에 따라 집중할 취약성의 우선순위를 신속하게 결정해야 합니다.	sn_si.analyst	계층 1 및 2 보안 분석가가 보안 인시던트에 대해 작업합니다. 보안 인시던트, 요청 및 작업은 물론 인시던트와 관련된 문제, 변경 및 중단을 생성하고 업데이트할 수 있습니다.

보안 인시던트 관리 표시기

보안 인시던트 관리 대시보드에는 다음과 같은 핵심성과지표가 표시됩니다.

새 보안 인시던트

새 보안 인시던트 수를 나타내는 차트입니다.

열린 보안 인시던트

미해결 보안 인시던트 수, 지난 30일 동안 업데이트되지 않은 미해결 보안 인시던트 수, 지난 5일 동안 업데이트하지 않은 미해결 보안 인시던트 수를 비교할 수 있는 차트입니다.

기본 보안 표시기

지난 6일 동안 새 보안 인시던트 수, 종결된 보안 인시던트 수, 보안 인시던트 백로그 증가치 및 미해결 보안 인시던트 수 표시기 점수

우선순위별 새 보안 인시던트

우선순위별로 구분된 새 보안 인시던트 수입니다.

세부 항목

다음 세부 항목은 대시보드의 지표에 적용됩니다.

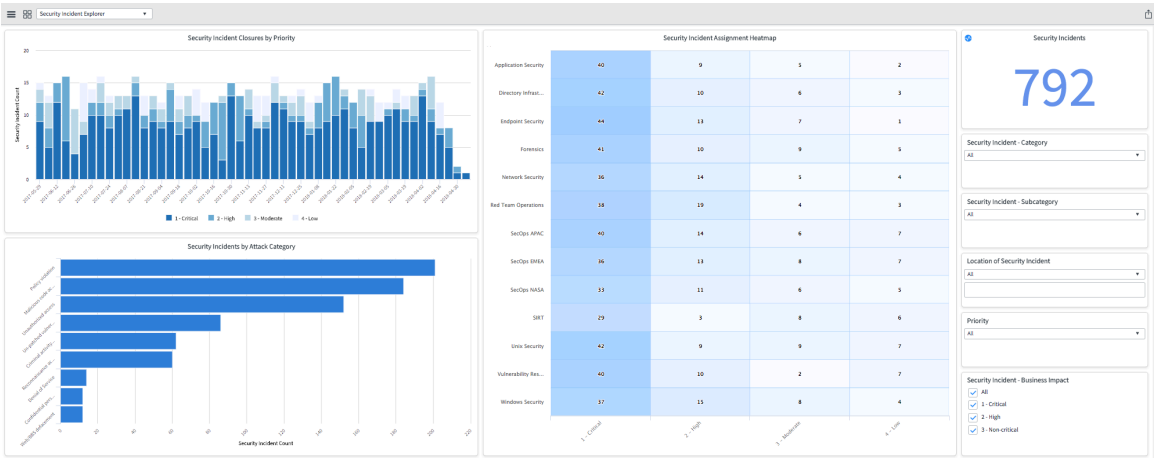
- 보안 그룹
- 보안 인시던트 기간
- 보안 인시던트 범주
- 보안 인시던트 우선순위
- 보안 인시던트 상태

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 인시던트 **Explorer** 대시보드

이 대시보드를 사용하여 보안 관리자는 범주, 하위 범주, 위치, 우선순위 및 비즈니스 영향별로 요약되고 그룹화된 보안 인시던트를 볼 수 있습니다. 이러한 보기를 통해 관리자는 공격이 발생하는 빈도와 영향을 받는 비즈니스 서비스에 대한 인사이트를 빠르게 얻을 수 있습니다.

보안 인시던트 탐색기 대시보드의 일부 뷰



최종 사용자 및 역할

최종 사용자 및 목표	필요한 역할	혜택
보안 응답 관리자: 애플리케이션 및 서비스와 관련된 보안 인시던트의 전체 상태와 볼륨에 대한 명확한 가시성이 필요합니다.	sn_si.manager	할당 그룹의 구성원을 조정할 수 있는 기능을 사용하여 전반적인 보안 태세를 검토할 수 있습니다.
보안 응답 관리자: 관심 영역을 신속하게 찾아내고 필요에 따라 영역과 기술을 관리하면서 모든 보안 인시던트 응답 데이터를 완전히 제어할 수 있어야 합니다.	sn_si.admin	위험 계산 매개변수를 조정하여 조직과 가장 관련된 취약한 항목을 먼저 처리할 수 있습니다.
보안 응답 분석가: 조직에 대한 중요도에 따라 집중해야 하는 취약성의 우선순위를 신속하게 결정해야 합니다.	sn_si.analyst	계층 1 및 2 보안 분석가가 보안 인시던트에 대해 작업합니다. 보안 인시던트, 요청 및 작업은 물론 인시던트와 관련된 문제, 변경 및 중단을 생성하고 업데이트할 수 있습니다.

보안 인시던트 탐색기 표시기

보안 인시던트 Explorer 대시보드에는 다음과 같은 핵심성과지표가 표시됩니다.

보안 인시던트

미해결 및 보류 중인 보안 인시던트의 총 볼륨입니다.

우선순위별 보안 인시던트 종결

우선순위별로 세분화한 종결된 보안 인시던트 수입니다.

공격 범주별 보안 인시던트

범주별로 세분화된 미해결된 보안 인시던트 수입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 인시던트 할당 히트맵

할당 그룹 및 우선순위별로 미해결된 보안 인시던트 수를 2수준으로 세분화한 결과입니다.

보안 인시던트 히트맵

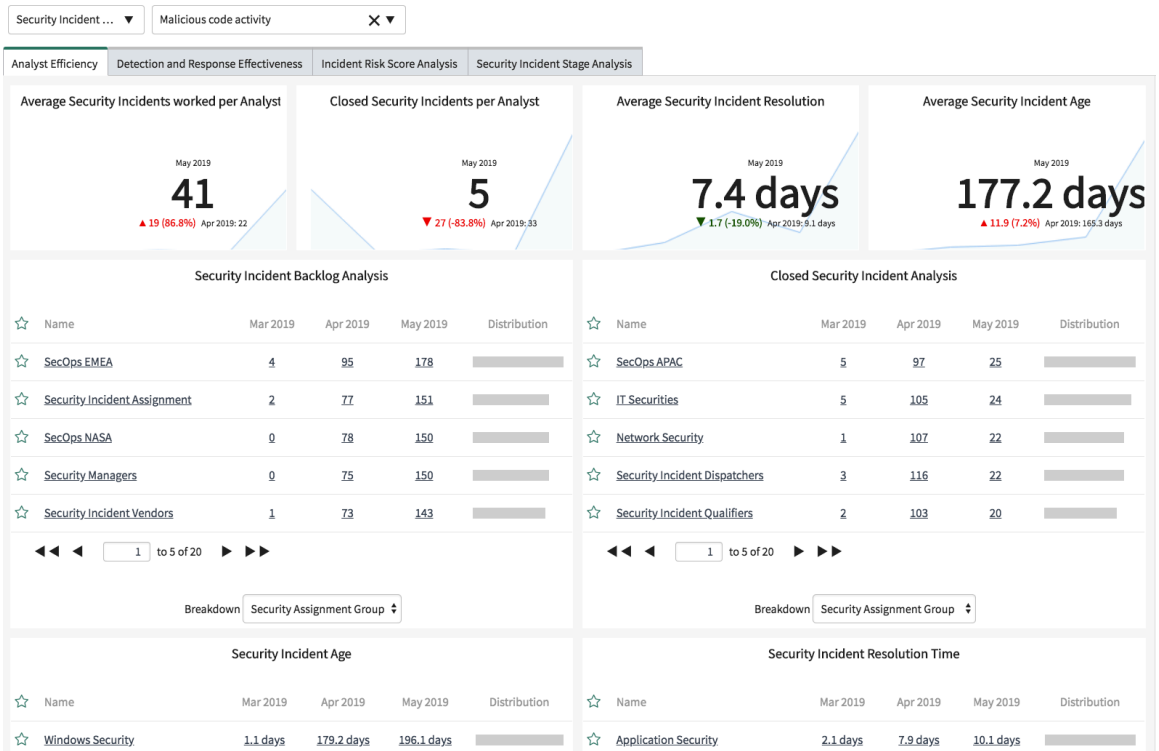
각 국가의 미해결 보안 인시던트 수를 보여주는 글로벌 맵입니다.

보안 운영 효율성 대시보드

SOC(보안 운영 센터) 관리자는 전체 효율성 메트릭을 보고 조직 내 SOC 팀 구성원의 개별 성과를 측정할 수 있습니다.

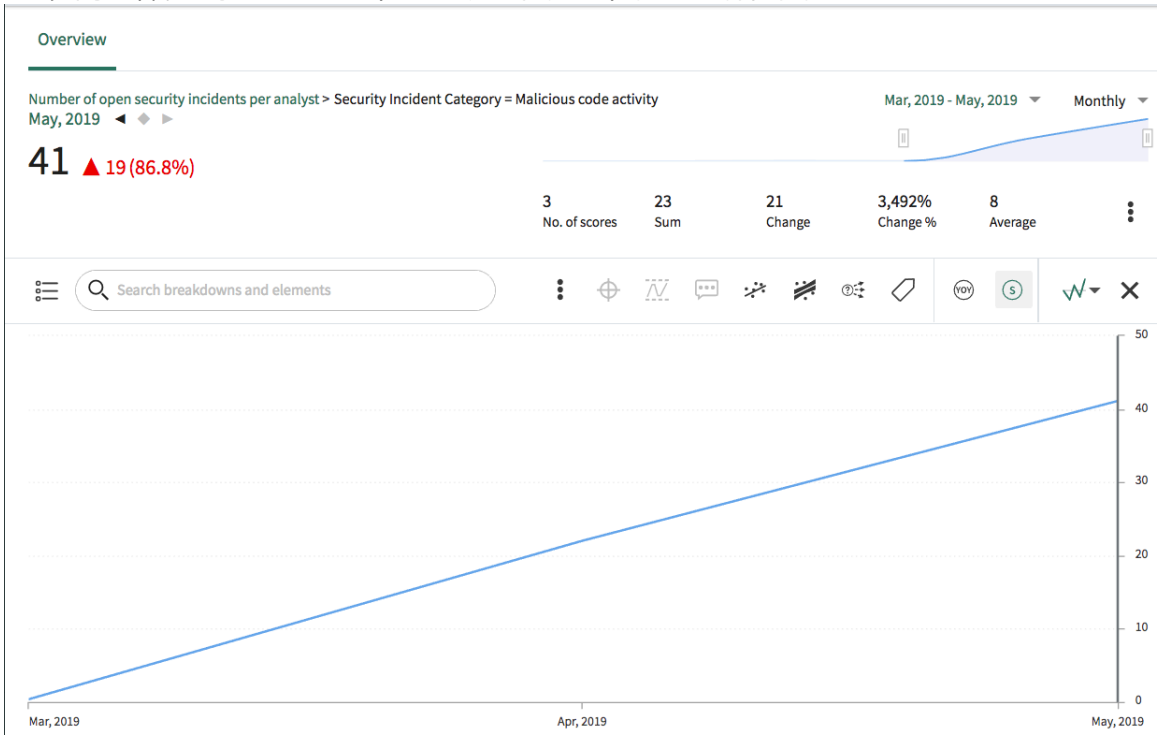
SOC 관리자는 퍼포먼스 분석 대시보드를 사용하여 효율성을 개선하고 시간이 지남에 따라 일반 및 특정 영역 모두에서 SOC의 성과에 대한 그림을 개발할 수 있습니다.

분석가 효율성 탭



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

표시기 중 하나를 클릭하여 상세 정보를 드릴다운합니다. 예를 들어 분석가당 작업한 평균 보안 인시던트 섹션에서 표시기를 클릭합니다.



그래프는 미해결 보안 인시던트 수가 3월 0건에서 5월 40건 이상으로 증가했음을 보여줍니다. 헤더에 데이터가 표시됩니다.

- 추세 표시기: 데이터가 수집된 최근 기간의 미해결 인시던트 수의 변화를 표시합니다. 이 차트는 2019년 3월부터 2019년 5월까지의 데이터를 보여주며 5월 한 달 동안 미해결 인시던트 수가 19건 증가했습니다. 일정 기간 동안 미해결 인시던트 수가 감소하면 분석가 효율성이 더 좋습니다.
- 아니요. 점수 수: 데이터 수집 기간(2019년 3월-5월)입니다.
- 합계: 3월과 5월 사이의 기간 동안 새로 오픈된 인시던트 수입니다.
- 변경: 3월과 4월 사이에 새로 오픈된 인시던트 수입니다.
- 평균: 선택한 기간 동안 분석가당 평균 미해결 인시던트 수입니다.

분석가 효율성 탭

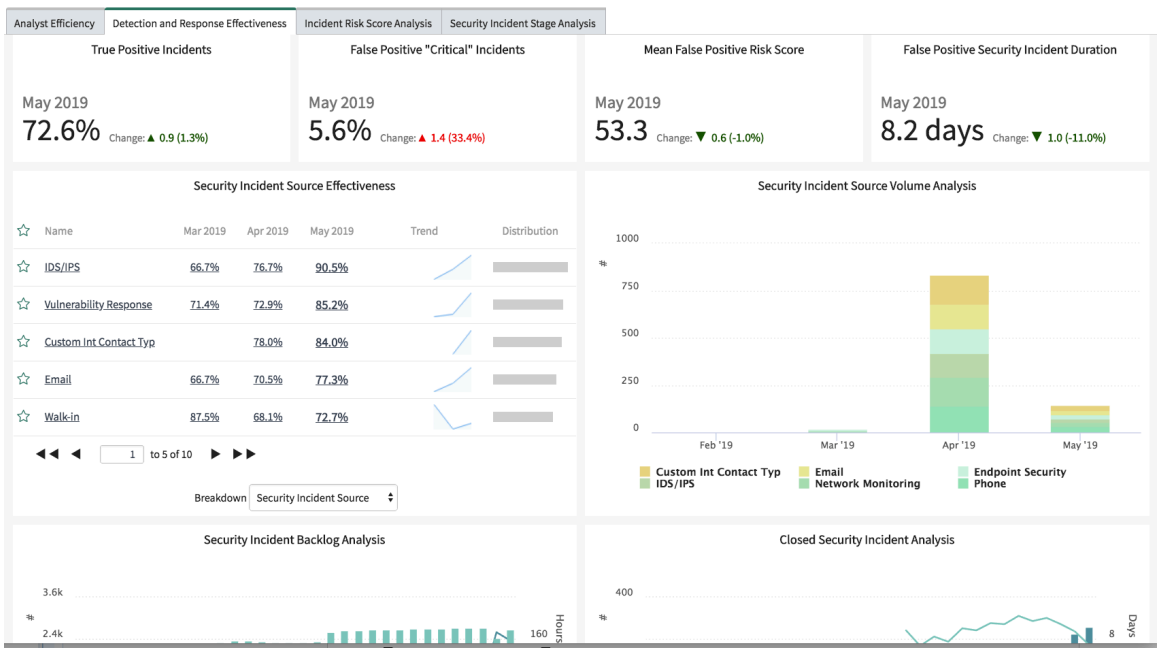
표시기	설명
분석가당 작업한 평균 보안 인시던트	지정된 기간 동안 분석가당 열린 보안 인시던트의 평균 수입니다. 사용되는 수식은 [[### ## #### #/## ## +]]/[[## #### #]]###.
분석가당 닫힌 보안 인시던트	지정된 기간 동안 선택한 범주에서 각 분석가가 종결한 총 인시던트 수입니다. 사용되는 수식은 [## #### ##> ### ## #### # = <category_name>/## ## +]]/[[## #### #/## ## +]]]###.
평균 보안 인시던트 해결	각 분석가가 지정된 기간에 보안 인시던트를 종결하는 데 걸린 평균 시간입니다. 결과를 일 단위로 표시하는 데 사용되는 수식은 ([[## #### ##> ### ## ##### ## ## = <category_name>/# ## +]] / [[## #### ##> ### ## #### # = <category_name>/# ## +]]) / 24###.
평균 보안 인시던트 연령	각 분석가에게 보안 인시던트가 미결 상태로 유지되는 평균 일수입니다. 결과를 일 단위로 표시하는 데 사용되는 수식은 ([[### ## ##### ## ##> ## #### ## = <category_name>/## ## +]]/ [[## #### ##> ### ## #### # = <category_name>/## ## +]]) / 24###.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

분석가 효율성 탭

표시기	설명
보안 인시던트 백로그 분석	지정된 기간에 발생한 총 미해결 보안 인시던트 수입니다. 세부 항목 목록에서 옵션을 선택하여 각 분석가, 보안 그룹, 우선순위 등에 대한 백로그를 봅니다. 선택한 두 달 간의 미해결 보안 인시던트 수를 비교할 수도 있습니다.
종결된 보안 인시던트 분석	지정된 기간에 종결된 총 보안 인시던트 수입니다. 세부 항목 목록에서 옵션을 선택하여 각 분석가, 보안 그룹, 우선순위 등에 대한 개수를 봅니다. 선택한 두 달 사이에 종결된 보안 인시던트 수를 비교할 수도 있습니다.
보안 인시던트 연령	지정된 기간 동안 보안 인시던트가 미결 상태로 유지되는 평균 일수입니다. 세부 항목 목록에서 옵션을 선택하여 각 분석가, 보안 그룹, 우선 순위 등에 대한 보안 인시던트 연령을 봅니다. 결과를 일 단위로 표시하는 데 사용되는 수식은 ([[### ## ##### ## ## > ## #### ## = <category_name> > ## ## ## = <group_name>/## ## +]]/ [[### ## #### # > ## #### ## = <category_name> > ## ## ## = <group_name>/## ## +]]) / 24###.
보안 인시던트 해결 시간	지정된 기간 동안 보안 인시던트를 해결하는 데 걸린 평균 일 수입니다. 세부 항목 목록에서 옵션을 선택하여 각 분석가, 보안 그룹, 우선 순위 등에 대한 보안 인시던트 해결 시간을 봅니다. 결과를 일 단위로 표시하는 데 사용되는 수식은 ([[### ## ##### ## ## > ## #### ## = ## ## ## > ## ### = John Ashby / ## ## +]] / [[### ## #### # > ## #### ## = ## ## ## > ## ### = John Ashby / ## ## +]]) / 24###.

탐지 및 응답 효과성 탭



탐지 및 응답 효과성 탭

표시기	설명
참 긍정 인시던트	지정된 기간 동안 선택한 범주에서 양성 보안 인시던트의 백분율입니다. 사용되는 수식은 (1-

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

탐지 및 응답 효과성 탭

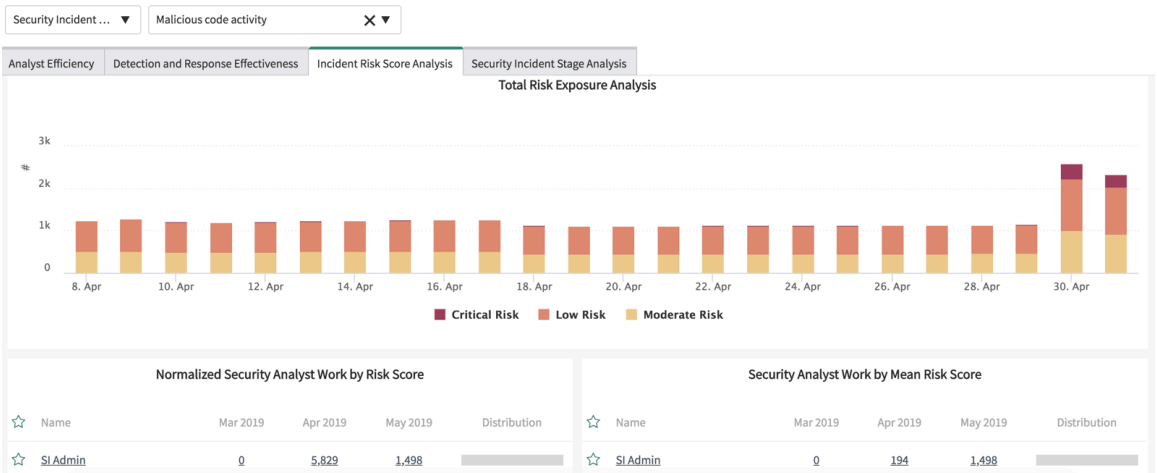
표시기	설명
	([[### ## #### # > ## #### ## = ## ## ## / ## ## +]] / [[## #### ##> ### ## #### # = ## ## ## / ## ## +]])) * 100###.
중요 인시던트 가양성	지정된 기간 동안 선택한 범주에서 중요 가양성 보안 인시던트의 백분율입니다. 사용되는 수식은 ([[### ## #### # > ## #### ## ## = ## ## > ## #### ## = ## ## ## / ## ## +]] / [[### ## #### # > ## #### ## = ## ## ## / ## ## +]]) * 100###. 주: ## ## = ### ### ## ###인 모든 보안 인시던트는 가양성 인시던트로 처리됩니다.
평균 가양성 위험 점수	가양성 인시던트로 식별된 종결된 보안 인시던트의 평균 월간 위험 점수입니다. 위험 점수가 낮을수록 보안 분석가가 가양성 인시던트를 분석하는 데 소요한 시간이 적다는 것을 나타냅니다. 사용되는 수식은 ([[### ## #### # > ## #### ## ## = ## ## > ## #### ## = ## ## ## / ## ## +]] / [[### ## #### # > ## #### ## = ## ## ## / ## ## +]]) * 100###.
가양성 보안 인시던트 기간	보안 분석가가 가양성 인시던트를 조사하는 데 소요한 평균 일수입니다. 사용되는 수식은 ([[### ## ##### ## ##]] / [[### ## #### #]]) / 24입니다.
보안 인시던트 소스 효과성	지정된 기간 동안 특정 소스에서 식별한 양성 보안 인시던트의 백분율입니다. 소스는 이메일, 네트워크 활동, 고객 지원 등일 수 있습니다. 이 데이터는 보안 인시던트 소스의 효과를 측정하는 데 도움이 됩니다. 사용되는 수식은 (1-([[### ## #### # > ## #### ## = ## ## ## > ## #### ## = IDS/IPS / ## ## +]] / [[### ## #### # > ## #### ## = ## ## ## > ## #### ## = IDS/IPS / ## ## +]])) * 100###.
보안 인시던트 소스 볼륨 분석	각 보안 인시던트 소스에서 이번 달에 종결된 보안 인시던트 수입니다. 선택한 두 달 간의 소스 유형별 보안 인시던트 수를 비교할 수도 있습니다.
보안 인시던트 백로그 분석	지정된 기간 동안 미해결된 보안 인시던트의 총 수와 인시던트가 미해결 상태로 유지되는 평균 일수입니다. 선택한 두 달 간의 미해결 보안 인시던트 수를 비교할 수도 있습니다. 평균 백로그 기간을 계산하는 데 사용되는 수식은 ([[### ## ##### ## ## > ## #### ## = ## ## ##]]/ [[### ## #### # > ## #### ## = ## ## ##]]) / 24###.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

탐지 및 응답 효과성 탭

표시기	설명
종결된 보안 인시던트 분석	지정된 기간 동안 종결된 총 보안 인시던트 수와 이러한 인시던트의 평균 해결 시간입니다. 평균 해결 시간을 계산하는 데 사용되는 수식은 ([[## #### ## > ### ## ##### ## ## = ## ## ##]] / [[## #### ## = ## ## ##]]> ### ## #### #]]) / 24###.

인시던트 위험 점수 분석 탭

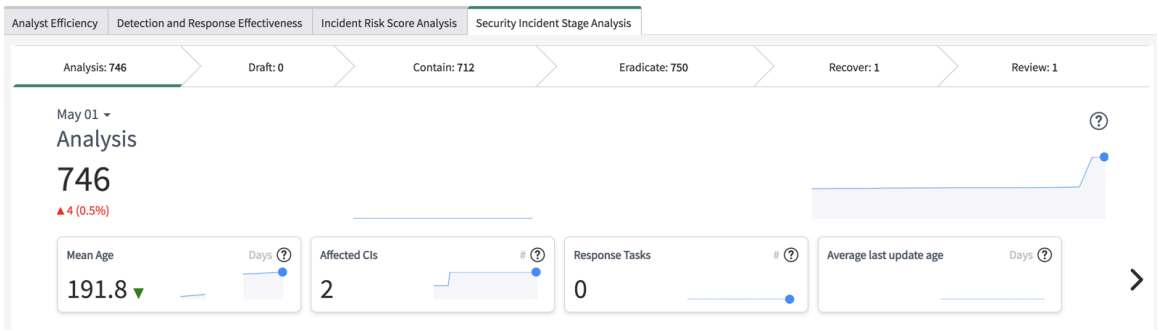


인시던트 위험 점수 분석 탭

표시기	설명
총 위험 노출 분석	지정된 기간 동안 각 위험 범주(낮음, 보통 및 중요)의 총 미해결 인시던트 수입니다. 두 달 사이에 서로 다른 위험 범주의 인시던트 수를 비교할 수도 있습니다.
위험 점수별 표준화된 보안 분석가 업무	지정된 기간 동안 각 보안 분석가의 총 위험 점수입니다. 보안 분석가가 종결한 양성 보안 인시던트 수를 기준으로 계산됩니다. 사용되는 수식은 다음과 같습니다. [[### ## ##### ## ## ## > ## #### ## = ## ## ## > ## ### = SI ### / ## ## +]] - [[### ## ##### ## ## ## > ## #### ## = ## ## ## > ## ### = SI ### / ## ## +]]
중위 위험 점수별 보안 분석가 업무	지정된 기간 동안 각 보안 분석가의 평균 위험 점수입니다. 사용된 수식은 다음과 같습니다. [[### ## ##### ## ## ## > ## #### ## = ## ## ## > ## ### = SI ### / ## ## +]] - [[### ## ##### ## ## ## > ## #### ## = ## ## ## > ## ### = SI ### / ## ## +]]

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 인시던트 스테이지 분석 탭



특정 날짜의 미해결 인시던트 수와 이러한 인시던트의 상태(분석, 초안, 포함, 근절, 복구 또는 검토)를 볼 수 있습니다. 각 단계에서 평균 연령, 영향을 받는 CI, 응답 작업 등을 볼 수 있습니다. 이러한 인시던트의 추가 세부 정보 또는 세부 항목을 보려면 링크를 클릭하십시오.

보안 인시던트 응답 작업 공간

이 ServiceNow# 보안 인시던트 응답 작업 공간 인터페이스는 보안 분석가와 SOC 관리자에게 차세대 사용자 환경을 제공하는 재구성된 인터페이스입니다. 보안 분석가는 이를 사용하여 초기 분석부터 방지, 근절, 복구에 이르는 보안 인시던트의 수명주기를 관리할 수 있습니다.

SIR Workspace 시작하기

시작하려면 타일을 선택합니다.

작업 공간 탐색

SIR 작업 공간 개념 및 기능에 대해 알아보기

작업 공간을 사용하는 관리자

SIR 작업 공간 및 기능 구성

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업 공간을 사용하는 분석가

분석가가 SIR Workspace를 사용하는 방법 알아보기

SIR 대시보드 보기

SIR 작업 공간 대시보드 보기

스토어에서 앱 요청

ServiceNow Store 웹 사이트를 방문하면 사용 가능한 모든 앱을 확인하고 스토어에 요청을 제출하는 방법에 대한 정보를 참조할 수 있습니다. 출시된 모든 앱의 누적 릴리스 정보는 ServiceNow Store 버전 기록 릴리스 정보 를 참조하십시오.

중요사항:

- 보안 인시던트 응답 에서 ServiceNow Store 13.4.5 버전 이상을 설치하면 기본적으로 (sn_si_aw) 1.5.1 버전 이상이 자동으로 설치됩니다 보안 인시던트 응답 작업 공간 . 종속 애플리케이션에 대한 자세한 내용은 이 SIR Workspace 플러그인 및 역할 섹션을 참조하십시오.
- 보안 인시던트 응답 작업 공간 버전 1.5.1 이상은 보안 인시던트 응답의 설치/업그레이드를 통해서만 설치/업그레이드할 수 있으며 독립적으로 설치할 수 없습니다.

기타 자원

보안 인시던트 응답 의 ServiceNow 커뮤니티포럼 을 방문하십시오.

SIR Workspace 탐색

보안 분석가 및 관리자가 향상된 사용자 경험을 통해 일상적인 운영을 수행하는 방법을 이해하고, 전체 인시던트 조사를 수행하고, 보안 분석가 및 팀에 할당된 보안 인시던트, 응답 작업 및 SLA의 개요를 확인하려면 탐색 보안 인시던트 응답 작업 공간 합니다.

이 섹션에서는 다음 사항에 대해 설명합니다.

- SIR Workspace 플러그인 및 필수 역할.
- 주요 SIR Workspace 기능.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

SIR Workspace 플러그인 및 역할

다음은 (sn_si_aw) 플러그인으로 보안 인시던트 응답 작업 공간 작업하는 데 필요한 애플리케이션입니다.

애플리케이션

보안 인시던트 응답 애플리케이션 버전 13.4.5 이상을 설치하면 및 다음 앱이 자동으로 설치됩니다보안 인시던트 응답 작업 공간.

- 엔터프라이즈 보안 케이스 관리 PAD 공통 [sn_escm_pad_cmn]
- 보안 운영 공통 작업 공간 [sn_escm_ws_cmn]
- 보안 인시던트 UI 카드 구성요소 [sn_sirw_evam]
- Security Operations 스포크 [sn_sec_spoke]

중요사항:

- 보안 인시던트 응답 에서 ServiceNow Store 13.4.5 버전 이상을 설치하면 기본적으로 (sn_si_aw) 1.5.1 버전 이상이 자동으로 설치됩니다 보안 인시던트 응답 작업 공간 . 종속 애플리케이션에 대한 자세한 내용은 이 SIR Workspace 플러그인 및 역할 섹션을 참조하십시오.
- 보안 인시던트 응답 작업 공간 버전 1.5.1 이상은 보안 인시던트 응답의 설치/업그레이드를 통해서만 설치/업그레이드할 수 있으며 독립적으로 설치할 수 없습니다.

엔터프라이즈 보안 케이스 관리 **PAD Commons** 에는 플레이북 경험 [playbook_experience] 플러그인이 필요합니다.

역할, 테이블, 속성 및 예약된 작업에 대한 보안 인시던트 응답 자세한 내용은 다음을 참조하십시오. 보안 인시던트 응답와 함께 설치되는 구성요소

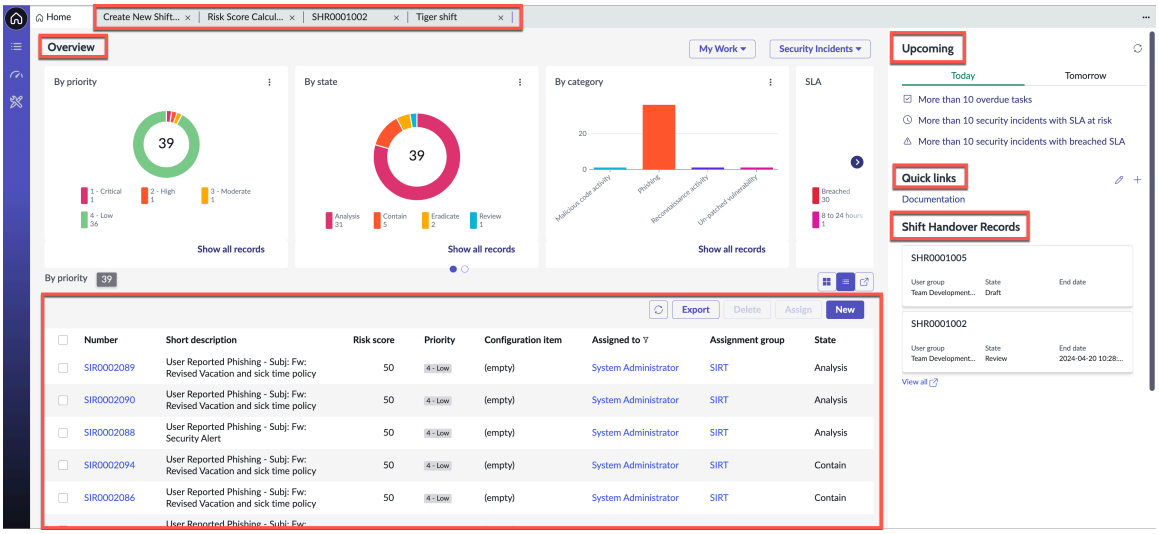
SIR 작업 공간 기능

다음과 보안 인시던트 응답 작업 공간 같은 주요 기능으로 구성됩니다.

- 개요 섹션
- 예정 섹션
- 빠른 링크 섹션
- 교대 인수인계 기록 섹션
- 목록 뷰
- 여러 보안 인시던트 열기를 지원하는 다중 탭 인터페이스

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

SIR 작업 공간 주요 기능



SIR Workspace 인터페이스 개요

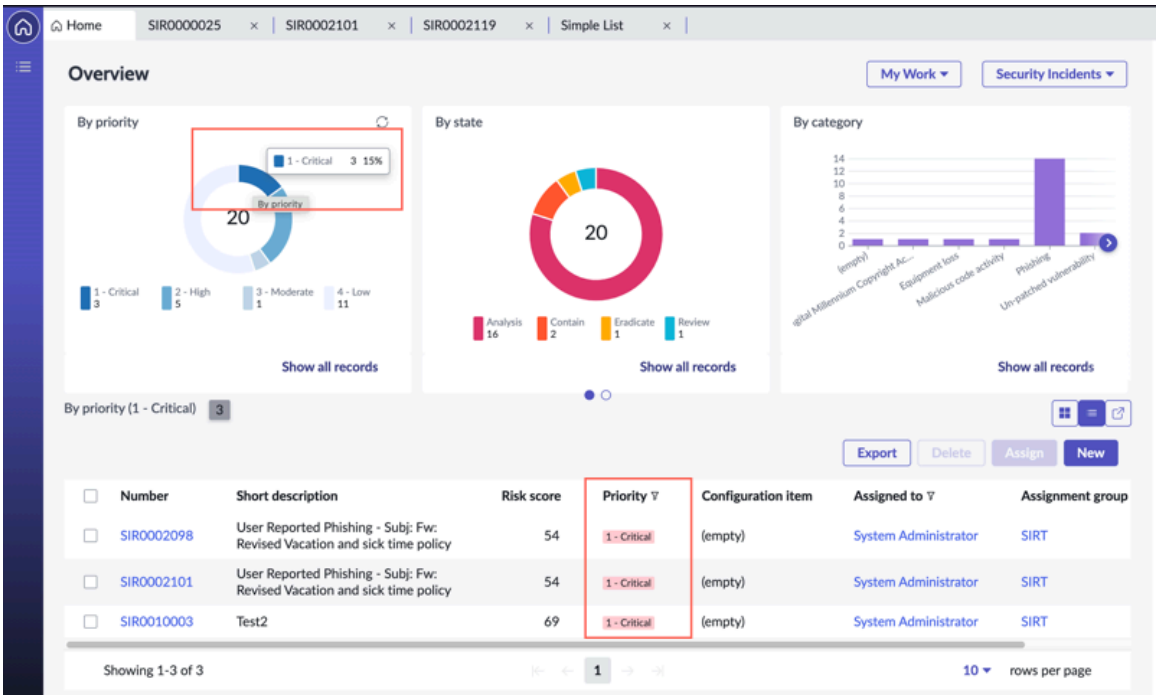
SIR Workspace 개요 페이지는 보안 분석가와 해당 팀의 보안 인시던트 및 응답 작업 상세 정보로 구성됩니다.

각 필터 아래에는 보안 분석가 큐와 보안 분석가 팀의 큐에 있는 우선 순위, 범주, 상태 및 SLA별로 그룹화된 다양한 위젯이 있습니다.

위젯에 필터를 적용하면 개요 페이지의 아래쪽 절반이 카드 또는 목록 항목으로 표시되는 해당 보안 인시던트 또는 응답 작업으로 채워집니다. 분석가는 원하는 대로 카드 뷰 또는 목록 뷰 간에 전환할 수 있습니다.

예를 들어 우선순위 위젯에서 모든 중요한 인시던트 또는 응답 작업을 선택하려면 위젯의 중요 세그먼트(아래 예시 스크린샷)를 클릭하면 중요한 인시던트 또는 응답 작업이 목록 또는 카드 뷰에 표시됩니다.

개요 섹션

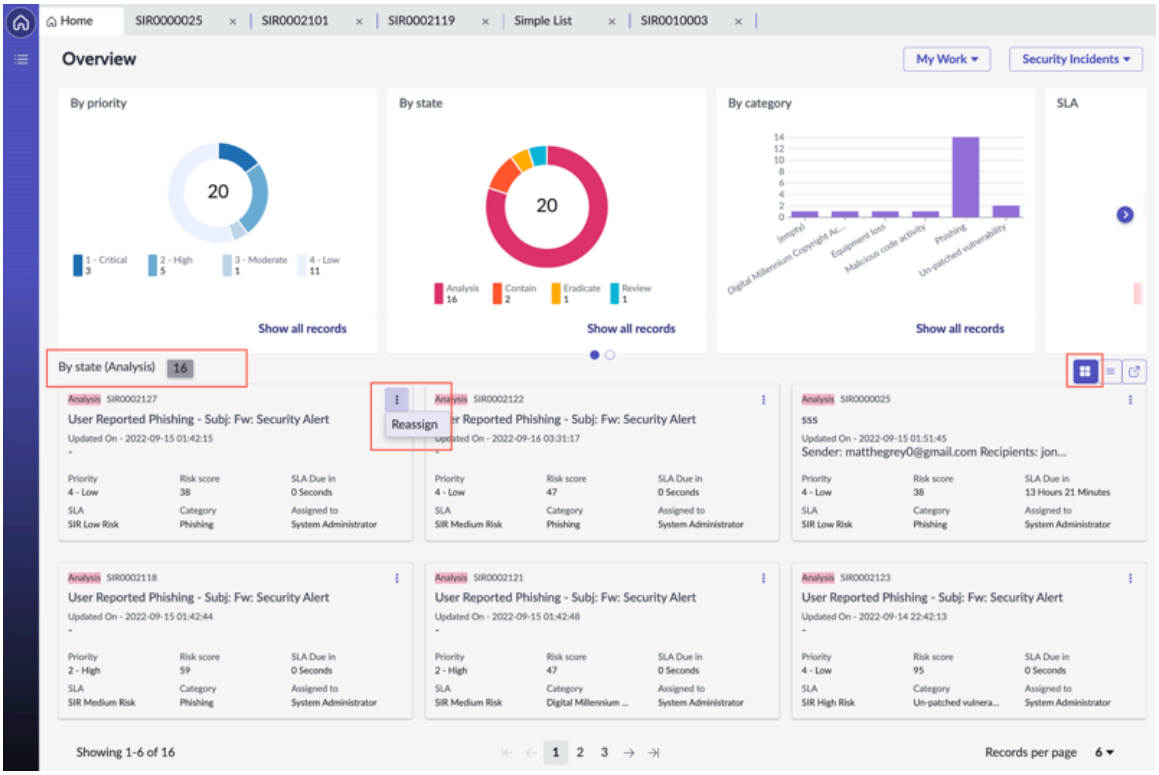


기계번역

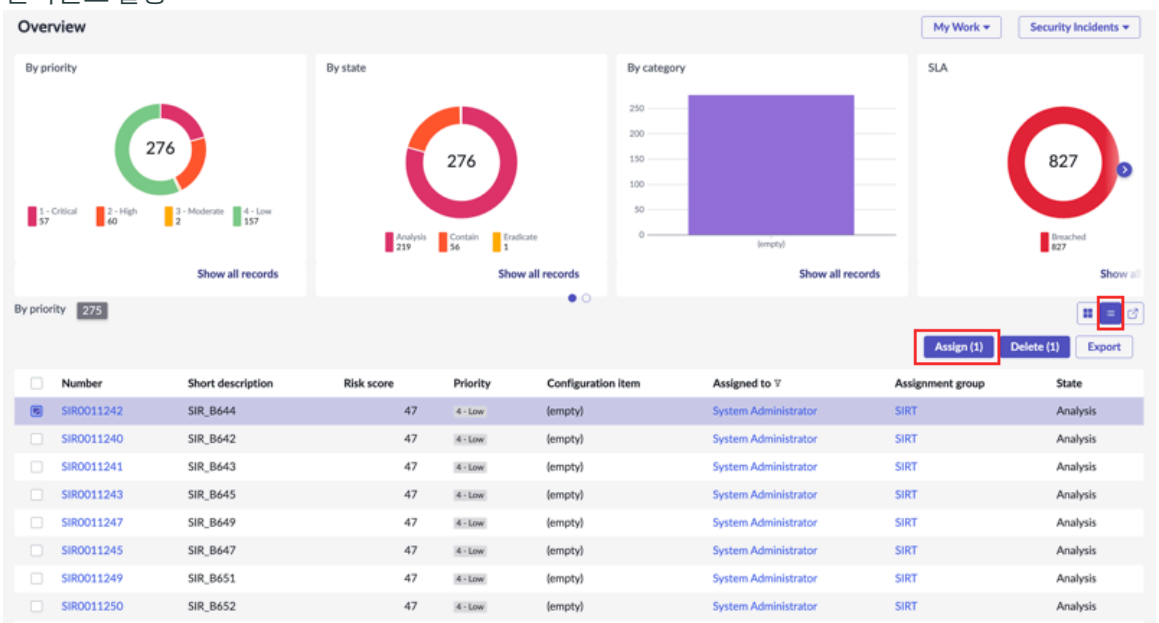
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

타원 아이콘을 클릭하고 할당 (카드 뷰의 옵션)을 선택하거나 할당 버튼(목록 뷰의 옵션)을 직접 눌러 인시던트를 할당하면 이 뷰에서 보안 인시던트 또는 응답 작업을 직접 할당하거나 재할당할 수 있습니다.

카드 뷰 및 재할당 예시



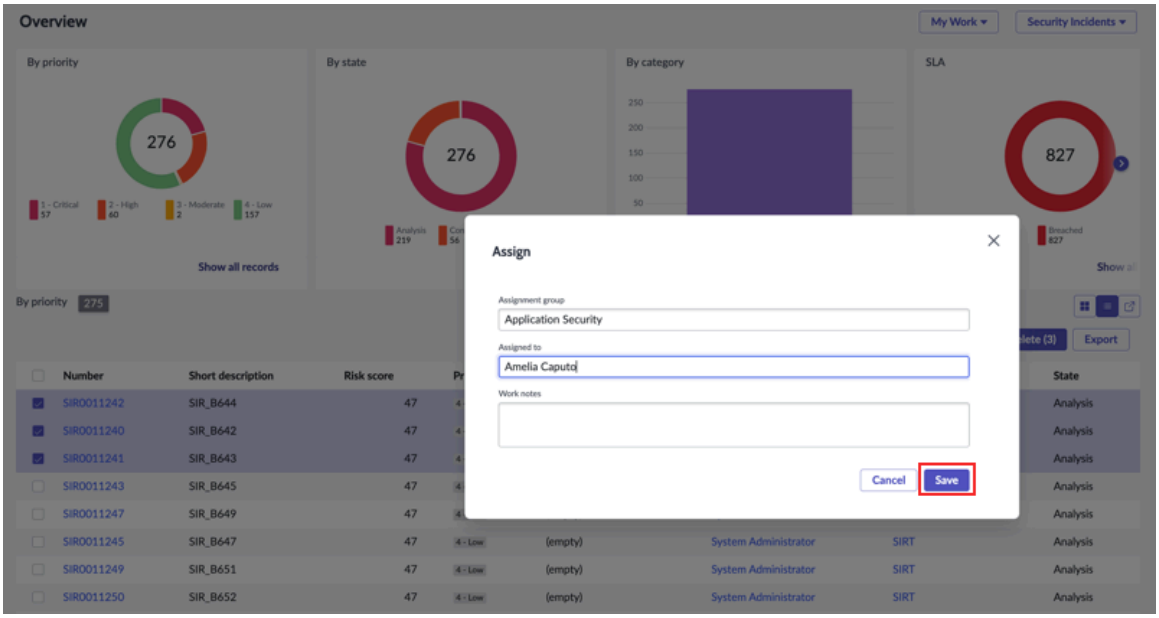
인시던트 할당



다음은 목록 뷰의 예입니다. 사용자는 목록 뷰에서도 인시던트를 할당할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

인시던트 할당



할당 그룹 및 할당 대상과 같은 담당자 상세 정보를 추가하거나 수정하고 필요한 경우 작업 주석을 추가합니다.

주:
하나 이상의 보안 인시던트 또는 응답 작업을 할당 그룹에 할당할 수 있습니다. 선택한 번호가 할당 버튼에 표시됩니다.

사용자는 이 뷰에서 보안 인시던트를 삭제할 수 있습니다. 삭제 버튼을 클릭하여 보안 인시던트를 삭제하면 목록 뷰에서 기록이 삭제됩니다.

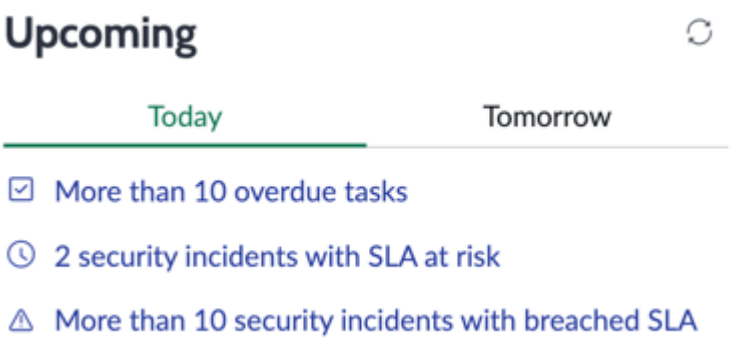
사용자는 목록 컨텐츠도 익스포트할 수 있습니다. 내보내기 버튼을 클릭하여 목록을 원하는 형식으로 내보냅니다.

예정 섹션

이 섹션에는 기한이 보안 인시던트 및 응답 작업과 같이 당일과 다음 날로 예정된 작업이 표시됩니다.

표시되는 보안 인시던트 및 응답 작업 목록은 해당 기록에 대해 정의된 기한 필드와 SLA 정의를 기반으로 합니다.

이 섹션에 둘 이상의 보안 인시던트 또는 응답 작업이 포함된 경우 인시던트나 기록은 새 탭에서 모든 기록을 엽니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

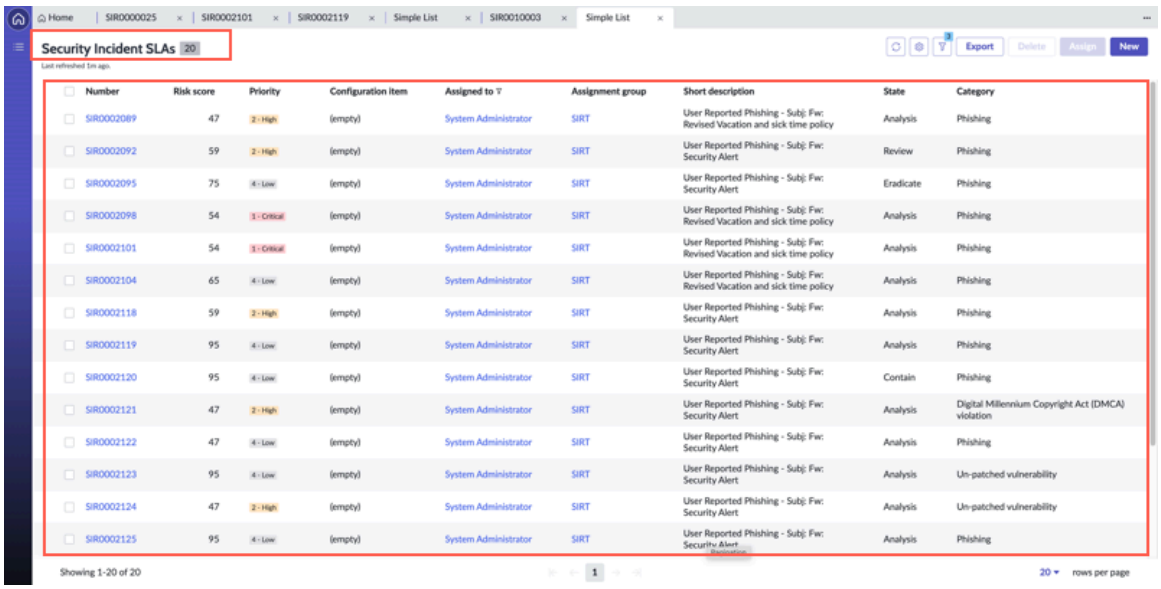
예정된 작업 보기

보안 분석가는 정의된 SLA의 기한, 지연 또는 위반된 보안 인시던트 및 응답 작업과 관련된 예정된 작업을 볼 수 있습니다.

시작하기 전에
필요한 역할: sn_si.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간 〉 예정.
2. 오늘 탭을 클릭하여 같은 날에 마감되는 작업을 봅니다.
3. 내일 탭을 선택하여 다음 날로 미뤄진 작업을 봅니다.
   다음 섹션에는 기한을 기준으로 기한이 지났고 SLA 정의를 위반한 보안 인시던트 또는 응답 작업이 나열됩니다.
4. 새로 고침 아이콘을 클릭하여 예정된 섹션 목록을 새로 고칩니다.
   예를 들어, **SLA** 위반이 있는 10개 이상의 보안 인시던트 링크를 클릭하면 작업 공간 내의 새 탭에 위반된 SLA 인시던트 목록이 표시됩니다.



> **주:**
> 모든 목록 뷰에서 새로 만들기, 할당, 익스포트 및 삭제 작업을 수행할 수 있습니다.

빠른 링크 섹션

빠른 링크는 책갈피 링크처럼 작동합니다. 외부 URL을 추가하고 작업 공간 내에서 빠르게 액세스할 수 있습니다.

빠른 링크 작업

쉽게 참조할 수 있도록 빠른 링크를 추가합니다.

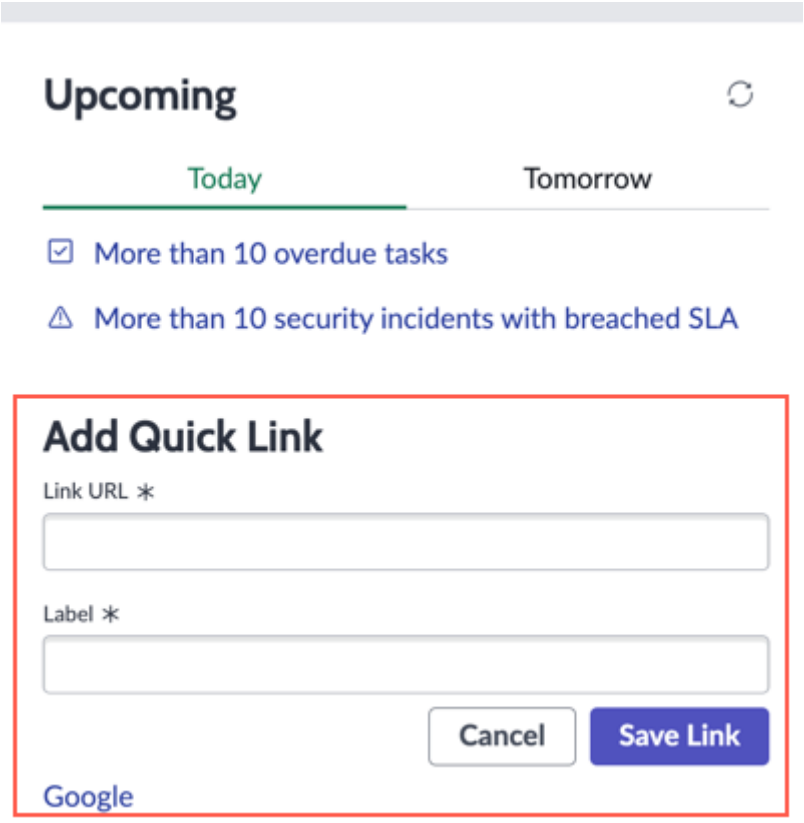
시작하기 전에
필요한 역할: sn_si.analyst

이 태스크 정보
유용한 빠른 링크를 추가 및 수정하고 인시던트 해결에 도움이 되는 링크를 책갈피로 지정할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간 〉 빠른 링크.
2. 빠른 링크 추가 아이콘을 클릭하여 링크를 추가합니다.
3. URL 및 레이블에 대한 링크를 입력합니다.
4. 링크 저장을 클릭합니다.



새 링크가 빠른 링크 섹션 아래에 추가됩니다.

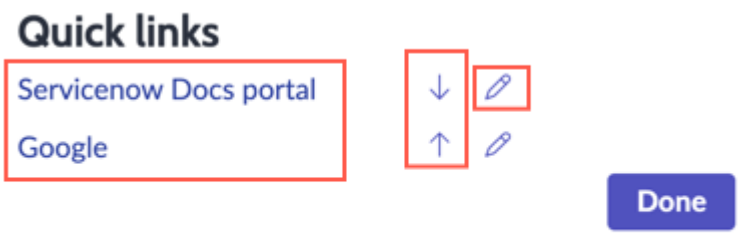
5. 링크를 수정하거나 삭제하려면:

   a. 링크 편집 아이콘을 클릭합니다.

   b. 원하는 링크를 수정하거나 URL의 레이블인 텍스트를 표시합니다.

   c. 저장을 클릭합니다.

   d. 완료를 클릭합니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

e. 위쪽 및 아래쪽 화살표를 사용하여 링크의 위치를 이동합니다.

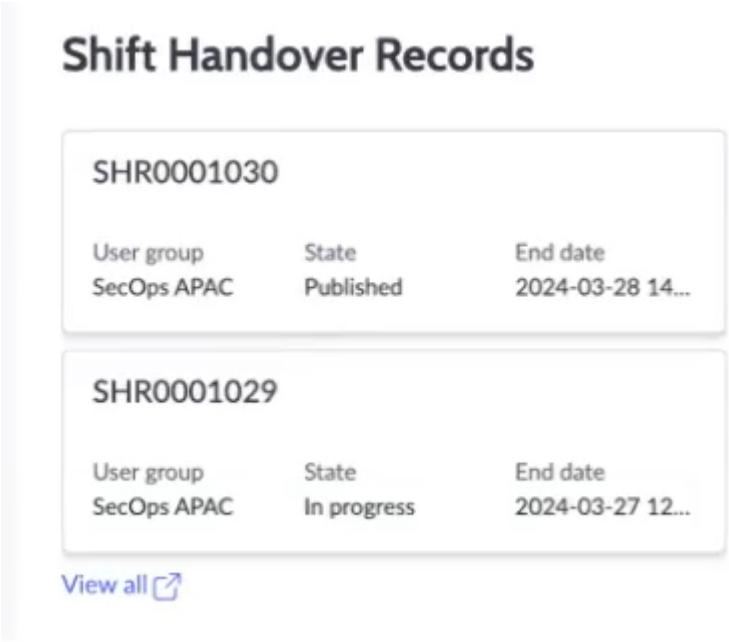
f. 편집을 하는 동안 책갈피가 지정된 링크를 삭제하려면 삭제를 클릭합니다.

교대 인수인계 기록 섹션

이 섹션에는 보안 인시던트 응답 작업 공간의 교대조 핸드오버 기록 목록이 표시됩니다.

보안 인시던트 응답 작업 공간의 교대조 핸드오버 기록 섹션에는 해당 기록에 대해 정의된 종료 날짜, 상태 및 사용자 그룹 필드를 기준으로 마지막 두 개의 교대조 핸드오버 기록이 표시됩니다. 모든 교대조 핸드오버 기록을 보려면 모두 보기를 선택합니다.

교대 인수인계 기록 섹션



의 목록 뷰 **SIR Workspace**

목록 뷰는 보안 인시던트, 응답 작업, 피싱 이메일 및 평가로 구성됩니다.

목록 뷰에는 나에게 할당됨, 팀에 할당됨, 미할당됨, 모두 오픈, 모두 등의 필터가 미리 적용되어 있습니다.

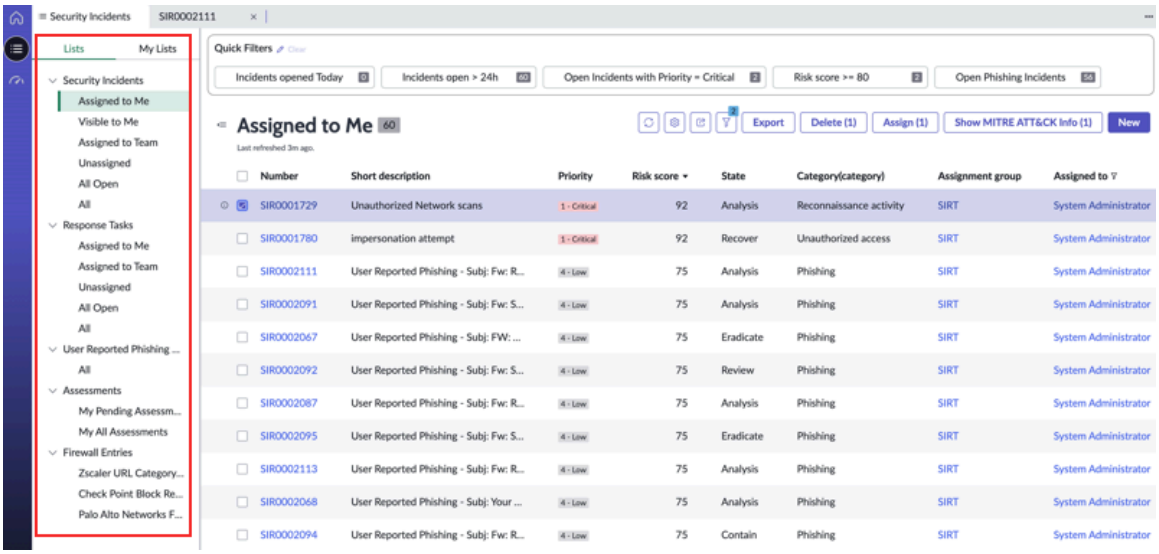
분석가는 이러한 목록 범주와 필터링된 목록을 사용하여 필요한 보안 인시던트 및 대응 작업 기록을 빠르게 찾을 수 있습니다.

목록 뷰에 액세스하려면 목록 아이콘( )을 클릭해야 합니다. 목록 뷰에서 기록을 클릭하면 기록이 새 탭에서 열립니다.

목록 유형

다음은 목록의 예제 보기입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



목록 창에는 다음 섹션이 포함되어 있습니다.

목록

목록 항목	설명	역량
보안 인시던트	보안 인시던트 목록을 보고 원하는 인시던트로 이동하여 작업을 시작합니다. 다음과 같은 목록을 사용할 수 있습니다. • 나에게 표시: 로그인한 사용자가 볼 수 있는 보안 인시던트입니다. • 나에게 할당: 분석가에게 할당된 보안 인시던트입니다. • 팀에 할당: 분석가가 속한 모든 팀에 할당된 보안 인시던트입니다. • 할당되지 않음: 할당되지 않은 보안 인시던트 목록입니다. • 모두 열기: 모든 미해결 보안 인시던트의 목록입니다. • **All**: 모든 보안 인시던트의 목록입니다.	• 목록 뷰에서 분석가는 인시던트 열 위에 있는 기어 아이콘을 클릭하여 열 목록을 구성할 수 있습니다. • 분석가는 하나 이상의 보안 인시던트를 선택하고 해당 인시던트를 다른 사용자에게 할당할 수 있습니다. • 분석가는 보안 인시던트를 삭제할 수 있습니다. • 분석가는 새 보안 인시던트를 만들 수 있습니다. • 분석가는 빠른 필터를 적용할 수 있습니다. 고급 필터 옵션을 사용하는 대신 빠른 필터 옵션을 클릭하여 필터를 적용합니다. 빠른 필터를 사용하면 즉각적인 주의가 필요한 보안 인시던트 목록을 신속하게 필터링할 수 있습니다. 자세한 내용은 빠른 필터 작업 문서를 참조하십시오. • 분석가는 인시던트 목록을 새로 고칠 수 있습니다. • 분석가는 목록 뷰를 Excel, CSV, JSON 및 PDF 형식으로 익스포트할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

목록

목록 항목	설명	역량
교대 인수인계 기록	교대조 핸드오버 기록 목록을 봅니다. 다음과 같은 목록을 사용할 수 있습니다. • 팀에 할당됨: 분석가가 속한 모든 팀/사용자 그룹에 할당된 교대조 핸드오버 기록입니다. • **All**: 모든 보안 인시던트의 목록입니다.	교대조 핸드오버는 다음과 같은 세 가지 역할을 지원합니다. • 관리자: 교대조 소유자 역할 • 보안 분석가: 교대조 분석가 역할 • 보안 관리자: 교대조 소유자 역할이지만 교대조 핸드오버 기록이 할당된 사용자 그룹에 대한 액세스 권한이 없습니다. • 활성 교대조의 사용자 그룹에 속하는 교대조 소유자/분석가 역할의 사용자는 초안 상태의 교대조 핸드오버 기록에서 컨텐츠를 추가하거나 수정할 수 있습니다. • 교대조 소유자/분석가 역할이 없거나 활성 교대조의 사용자 그룹에 속하지 않은 사용자는 교대조 핸드오버 기록의 컨텐츠만 볼 수 있습니다.
응답 작업	응답 작업 목록을 보고 원하는 응답 작업으로 이동하여 작업을 시작합니다. 목록 뷰에는 다음이 포함됩니다. • 나에게 할당됨: 분석가에게 할당된 응답 작업입니다. • 팀에 할당됨: 분석가가 속한 팀에 할당된 응답 작업입니다. • 할당되지 않음: 할당되지 않은 응답 작업 목록입니다. • 모두 열기: 모든 열린 응답 작업의 목록입니다. • 모두: 모든 응답 작업의 목록입니다.	• 목록 뷰에서 분석가는 인시던트 열 위에 있는 기어 아이콘을 클릭하여 열 목록을 구성할 수 있습니다. • 분석가는 하나 이상의 응답 작업을 선택하고 해당 작업을 다른 사용자에게 할당할 수 있습니다. • 분석가는 새 응답 작업을 만들 수 있습니다. • 분석가는 빠른 필터를 적용할 수 있습니다. 고급 필터 옵션을 사용하는 대신 빠른 필터 옵션을 클릭하여 필터를 적용합니다. 빠른 필터를 사용하면 즉각적인 주의가 필요한 응답 작업 목록을 빠르게 필터링할 수 있습니다. • 분석가는 응답 작업 목록을 새로 고칠 수 있습니다. • 분석가는 목록 뷰를 Excel, CSV, JSON 및 PDF 형식으로 익스포트할 수 있습니다. 자세한 내용은

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

목록

목록 항목	설명	역량
		보안 인시던트 또는 응답 작업 익스포트 문서를 참조하십시오.
피싱 이메일	모든 피싱 이메일 목록을 봅니다. 목록 뷰는 마지막 업데이트를 기준으로 정렬됩니다.	• 피싱 이메일을 보고합니다. 자세한 내용은 피싱 이메일을 보고하는 방법을 참조하세요 피싱 메일 보고 . • 피싱 이메일을 삭제합니다. • 피싱 이메일 목록 뷰를 Excel, CSV, JSON 및 PDF 형식으로 익스포트합니다.
평가	사후 인시던트 검토를 수행하는 데 필요한 평가 목록을 봅니다. • 내 보류 중인 평가: 보류 중인 평가 목록입니다. • 내 모든 평가: 모든 평가의 목록입니다.	평가를 수행합니다.

목록 개인화

보안 분석가 또는 관리자는 개별 기본 설정에 따라 보안 인시던트나 응답 작업 또는 피싱 이메일 사용자 지정 목록 뷰를 개인화할 수 있습니다.

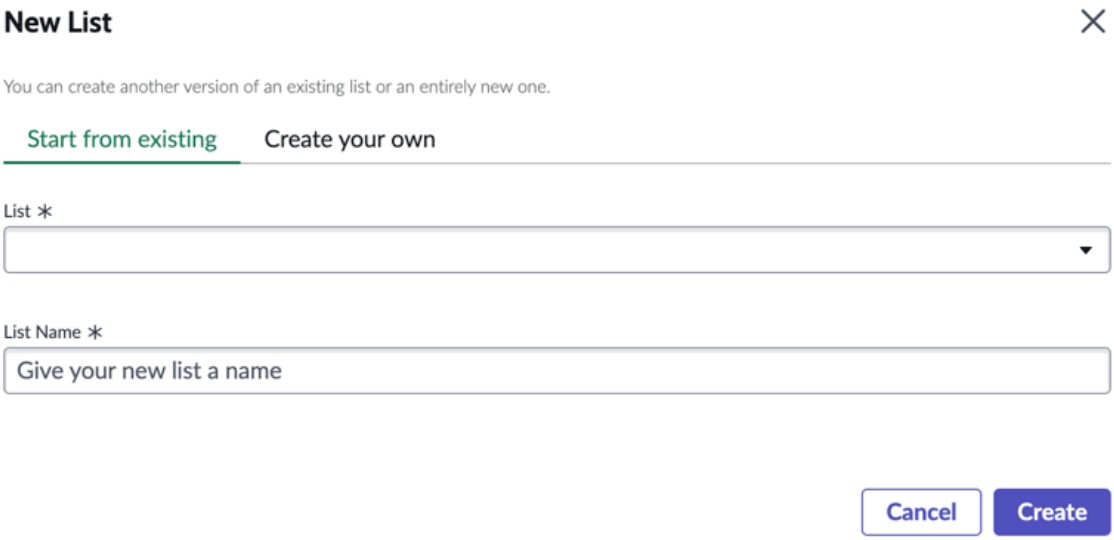
시작하기 전에

필요한 역할: sn_si.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간.
2. 목록 뷰를 클릭합니다.
3. 클릭 내 목록.
4. 내 목록 보기 하단에 있는 새 목록 추가를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



보안 분석가는 기존 목록의 다른 버전 또는 완전히 새로운 사용자 지정 목록을 만들 수 있습니다.

5. 기존 목록 뷰에서 생성하려면 다음을 수행합니다.

a. 기존 링크 에서 시작을 클릭합니다.

b. 드롭다운 목록에서 목록을 선택합니다.

> 주:
> 드롭다운 목록에서 어떤 목록을 선택하든 목록 이름은 기본 목록의 복사본이 됩니다. 예를 들어 보안 인시던트 섹션에서 나에게 할당을 선택하면 목록 이름이 나에게 할당 됨으로 표시됩니다. 보안 인시던트 섹션의 복사본입니다.

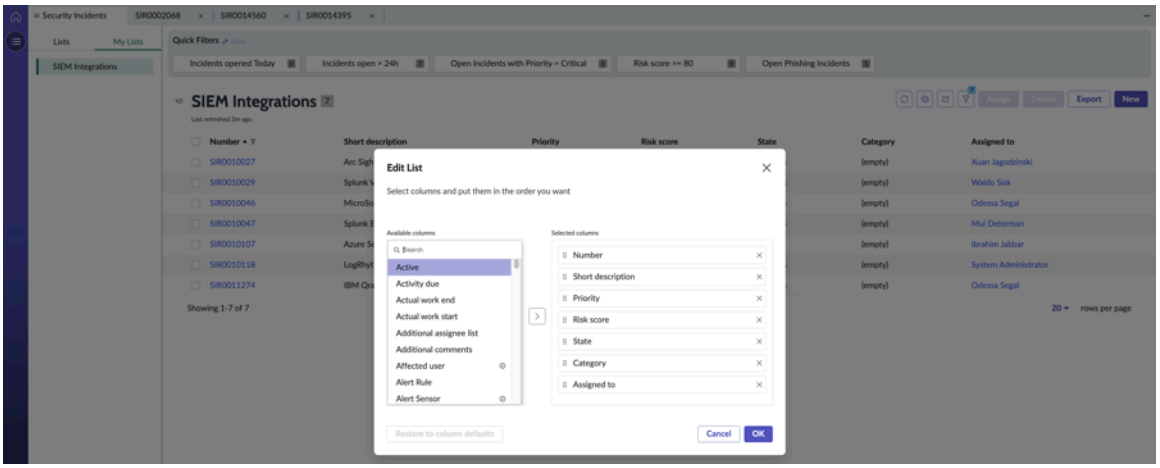
c. 개인화할 열을 선택하고 필터를 추가합니다.
필드, 연산자 및 값을 포함하는 조건을 추가하여 필터를 구성합니다.

d. 생성을 클릭합니다.

> 주:
> 사용자 지정 목록 뷰를 사용자 지정하려면 사용자 지정 열, 필터를 추가하고, 조건을 설정하고, 필요에 따라 순서별로 정렬할 수 있습니다.

e. 개인화된 목록 뷰를 만든 다음 기어 아이콘을 클릭하고 열 편집 옵션을 선택하여 목록 열을 사용자 지정하고 열을 편집하고 원하는 순서대로 정렬합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



또한 다음을 수행할 수 있습니다.

- 개인화된 목록 뷰의 이름을 바꿉니다.
- 개인화된 목록 뷰를 삭제합니다.
- 다른 이름으로 저장 옵션을 사용하여 원하는 대로 개인화된 목록 뷰를 저장합니다.
- 목록 뷰의 너비를 재설정합니다.

> **주:**
> 제공되는 할당, 삭제, 목록 뷰 익스포트와 같은 다른 목록 작업 버튼을 사용하여 이러한 작업을 직접 수행할 수도 있습니다.

6. 자신의 목록을 생성하려면 다음을 수행합니다.

a. 나만의 링크 만들기를 클릭합니다.

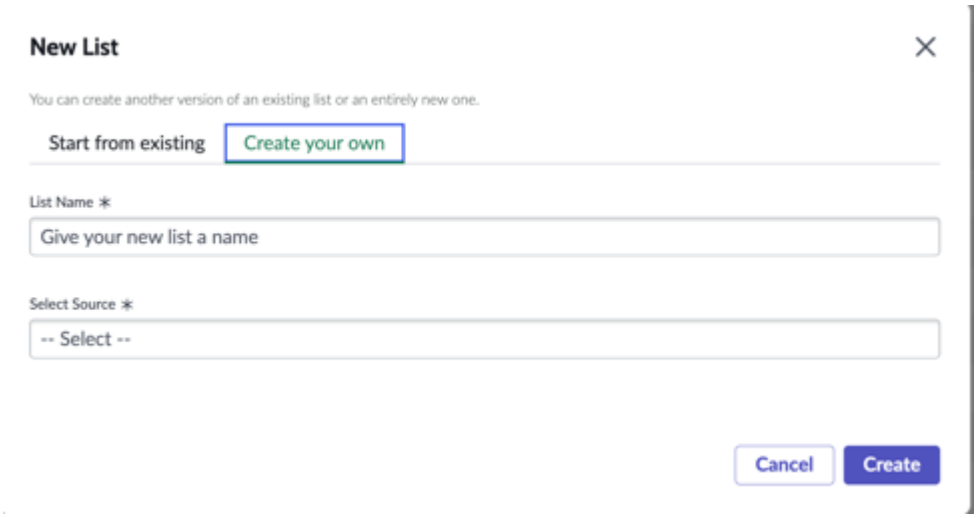
b. 목록 이름을 제공합니다.

c. 소스와 열을 선택합니다.

d. 필터를 추가합니다.
조건을 추가하여 필터를 구성하고 목록이 표시되는 순서를 제공합니다.

e. 생성을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



내 목록 섹션 아래에 사용자가 정의하고 사용자 지정한 대로 새 목록이 생성됩니다.

주:
위치를 이동하여 개인화된 뷰의 순서를 변경할 수 있습니다.

보안 인시던트 할당

보안 인시던트를 할당합니다.

시작하기 전에

필요한 역할: sn_si.basic

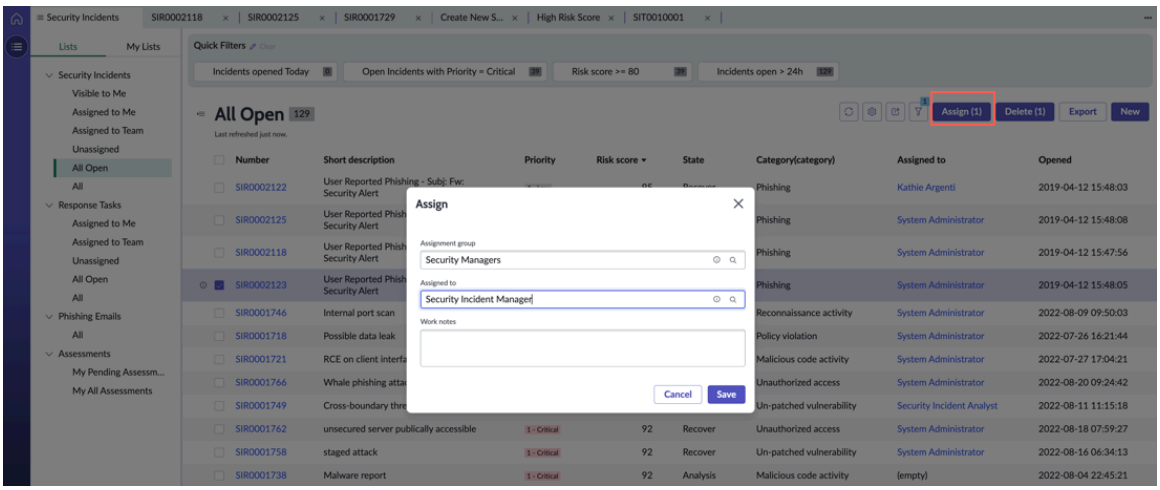
프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간.
2. 목록( ) 아이콘을 클릭합니다.
3. 목록을 클릭합니다.
4. 예를 들어, 보안 인시던트 〉 모든 오픈 항목.
5. 하나 이상의 보안 인시던트를 선택합니다.
6. 할당을 클릭합니다.
7. 할당 그룹, 할당 대상과 같은 상세 정보를 입력하고 필요한 경우 작업 메모를 추가합니다.
그러면 인시던트가 사용자에게 할당됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

8. 저장을 클릭합니다.

하나 이상의 보안 인시던트 할당



여러 보안 인시던트 종결

공통적인 근본 원인이나 오탐지 인시던트로 생성된 인시던트와 같이 관련 인시던트를 개별적으로 종결할 필요가 없도록 여러 보안 인시던트를 동시에 종결합니다.

시작하기 전에

필요한 역할: sn_si.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간.
2. List 아이콘()을 선택합니다.
3. 목록을 선택합니다.
4. 선택 보안 인시던트 〉 모든 오픈 항목.
5. 종결할 보안 인시던트를 하나 이상 선택하고 종결을 선택합니다.
   보안 인시던트 대량 종결 창 에는 종결하도록 선택한 보안 인시던트의 목록 액세스 링크가 표시됩니다 .
   - 선택한 보안 인시던트 하나 이상에 활성 작업, Playbook, 하위 SI, 평가 또는 활성 플로우와 같은 보류 중인 활동이 있는 경우 활성 작업, **Playbook,** 하위 **SI,** 평가 및 활성 플로우가 있는 보안 인시던트가 표시됩니다.
   - 종결을 위해 선택한 하나 이상의 보안 인시던트에 보류 중인 종결 활동이 없는 경우 종결 준비가 된 보안 인시던트가 표시됩니다.
6. 옵션: 보류 중인 활동이 있는 보안 인시던트를 검토합니다.

   주:
   보류 중인 활동을 수동으로 종결하지 않는 경우 대량 종결을 진행하면 보류 중인 활동이 자동으로 종결됩니다.

   a. 활성 작업, Playbook, 하위 SI, 평가 및 활성 플로우를 닫습니다.
   b. 다시 가져오기를 선택하여 보안 인시던트 대량 닫기 창으로 돌아갑니다.
7. 다음을 선택합니다.
8. 해당 종결 코드를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

9. 종결 메모를 입력합니다.
10. 대량 종결을 선택합니다.
    인시던트 종결 작업은 백그라운드에서 실행됩니다.

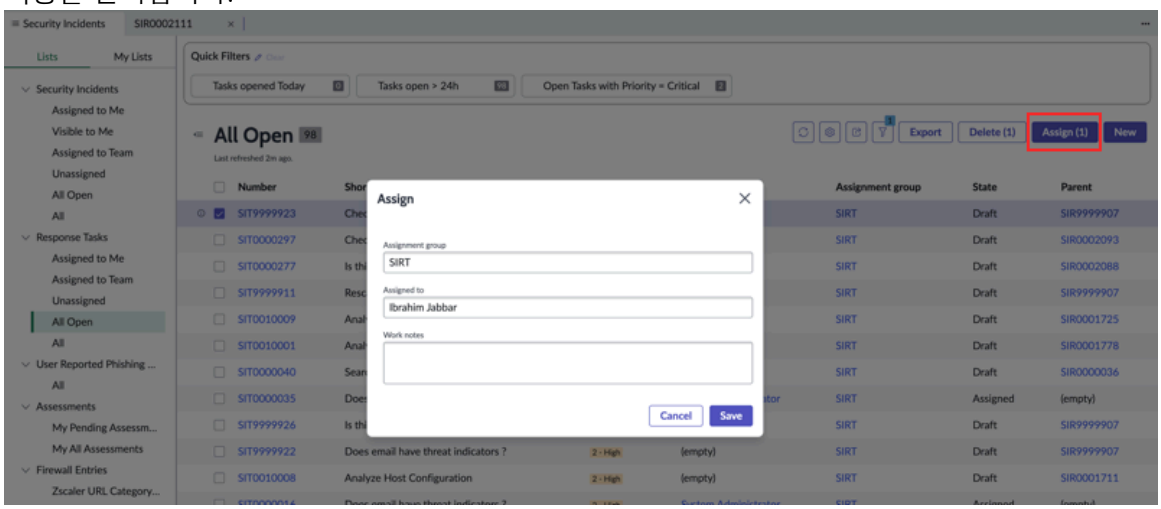
응답 작업 할당

보안 문제에 대한 응답 작업을 할당합니다.

시작하기 전에
필요한 역할: sn_si.basic

프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간.
2. 목록( ) 아이콘을 클릭합니다.
3. 목록을 클릭합니다.
   예를 들어, 응답 작업 〉 모든 오픈 항목.
4. 하나 이상의 응답 작업을 선택합니다.
5. 할당을 클릭합니다.
6. 할당 그룹, 할당 대상과 같은 상세 정보를 입력하고 필요한 경우 작업 메모를 추가합니다.
   그러면 인시던트가 사용자에게 할당됩니다.
7. 저장을 클릭합니다.



피싱 메일 보고

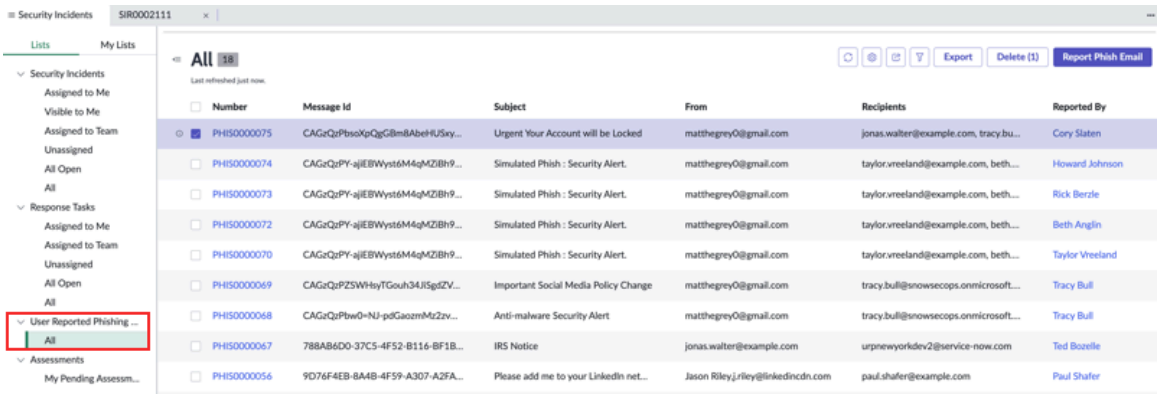
목록 뷰에서 피싱 이메일을 보고합니다.

시작하기 전에
필요한 역할: sn_si.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간.
2. 목록( ) 아이콘을 클릭합니다.
3. 이동 사용자가 보고한 피싱 이메일 〉 모두.
   사용자가 보고한 피싱 이메일 목록이 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 피싱 메일 보고 버튼을 클릭합니다.
   피싱 이메일을 업로드하여 보고합니다.
5. 파일 추가를 클릭하여 첨부 파일을 추가합니다.
6. 업로드를 클릭합니다.

   주:
   첨부 파일을 업로드하여 피싱 이메일을 보고합니다. 피싱 이메일은 한 번에 하나만 업로드할 수 있으며 .eml 형식이어야 합니다.

7. 제출을 클릭합니다.
   보안 인시던트를 로깅하는 피싱 이메일이 생성됩니다.

빠른 필터 작업

빠른 필터는 보안 인시던트 및 응답 작업 목록에서 사용할 수 있는 쉽게 액세스할 수 있는 필터입니다.

시작하기 전에
필요한 역할: sn_si.admin

SIR Workspace 보안 인시던트 또는 응답 작업 목록을 쉽게 필터링할 수 있는 빠른 필터 기능을 제공합니다.

빠른 필터를 사용하여 새 필터를 구성하거나 이러한 목록에 대해 표시되는 기존 필터를 수정할 수 있습니다. 기본 시스템은 각 보안 인시던트에 대해 다음과 같은 빠른 필터를 제공합니다.

- 오늘 개시된 인시던트
- 24시간 **>** 열린 인시던트
- 우선순위**=** 중요인 오픈 인시던트
- 위험 **>= 80**
- 미해결 피싱 인시던트

기본 시스템은 각 응답 작업에 대해 다음과 같은 빠른 필터를 제공합니다.

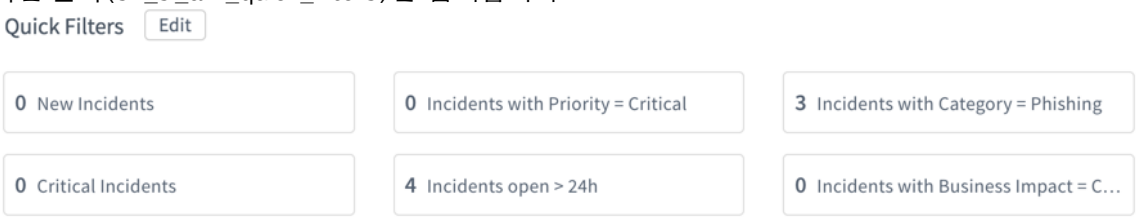
- 24시간 **>** 작업 오픈
- 우선순위 **=** 중요인 미해결 작업

주:
관리자는 조직의 필요에 따라 필요한 빠른 필터 목록을 구성할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 시스템 정의 〉 테이블.
2. 빠른 필터(sn_si_aw_quick_filters)를 검색합니다.

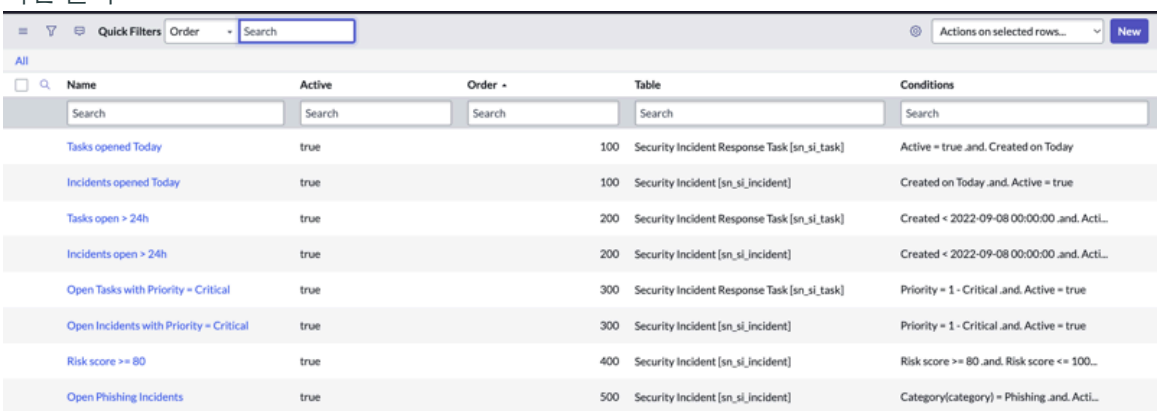


3. 이동 관련 링크 〉 목록 보기 절.
   빠른 필터 목록 페이지가 표시됩니다. OOTB. 다음은 애플리케이션과 함께 제공되는 빠른 필터 목록입니다.

이름	테이블	값
오늘 오픈된 작업	보안 인시던트 작업 (sn_si_task)	예
오늘 오픈된 인시던트	보안 인시던트(sn_si_incident)	예
24시간 〉 작업 오픈	보안 인시던트 응답 작업 (sn_si_task)	예
24시간 〉 오픈 인시던트	보안 인시던트(sn_si_incident)	예
우선순위 = 중요인 미해결 작업	보안 인시던트 응답 작업 (sn_si_incident)	예
우선순위 = 중요인 오픈 인시던트	보안 인시던트(sn_si_incident)	예
위험 점수 〉= 80	보안 인시던트(sn_si_incident)	예
미해결 피싱 인시던트	보안 인시던트(sn_si_incident)	예

주:
보안 관리자는 이러한 빠른 필터를 구성할 수 있습니다. 비즈니스 요구에 따라 관리자는 기존 값을 false로 수정하고 새 빠른 필터를 만들 수 있습니다.

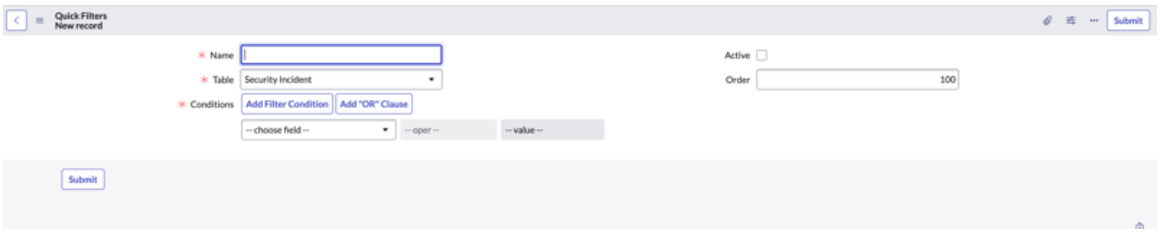
빠른 필터



4. 새 필터를 생성하려면 새로 만들기를 클릭합니다.
5. 필터 이름을 입력하고 테이블을 선택한 뒤 필터 조건을 지정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

6. 제출을 클릭하여 이전 목록 페이지로 돌아갑니다.
   페이지에 새로 추가된 필터가 표시됩니다.

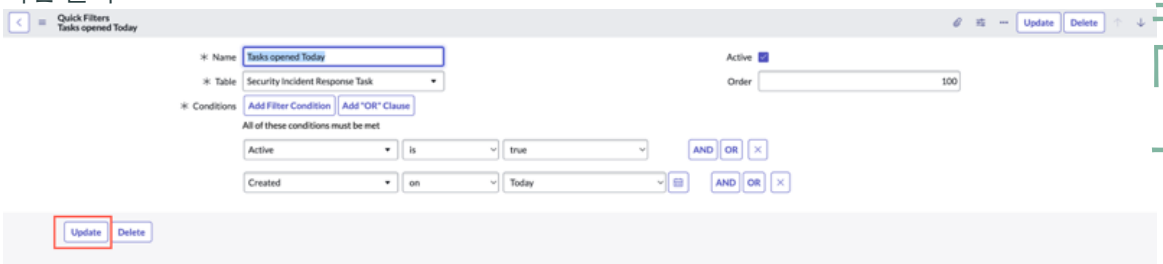


주:

- 빠른 필터는 활성 확인란이 선택된 경우에만 적용할 수 있습니다.
- 작업 공간 내에서 로그인한 사용자는 애플리케이션에서 사용할 수 있는 활성 빠른 필터를 개인화할 수 있습니다. 사용자는 새로 생성된 빠른 필터를 숨기거나 숨김 해제할 수 있습니다. 이 기능은 사용자 기본 설정을 기반으로 합니다.
- 사용자가 빠른 필터의 기본 설정을 수정한 후 새 빠른 필터를 만든 경우 빠른 필터가 활성으로 설정되어 있으면 사용자의 기본 설정에 적용되지 않습니다. 사용자는 개인화된 뷰에서 기본 설정을 수동으로 변경해야 합니다.

7. 기존 필터 기록을 선택하여 기존 빠른 필터를 수정합니다.
8. 이름 및 필터 조건을 수정합니다.
9. 업데이트를 클릭합니다.

빠른 필터



빠른 필터 추가 또는 수정

목록 뷰에서 보안 인시던트 또는 응답 작업에 대한 빠른 필터를 추가하거나 수정합니다.

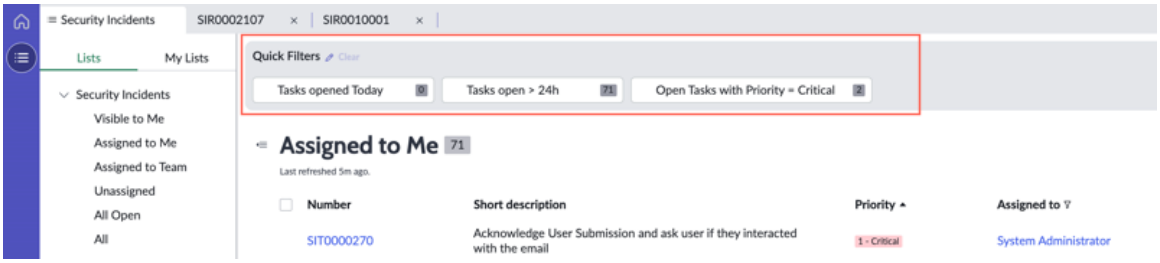
시작하기 전에

필요한 역할: sn_si.basic

프로시저

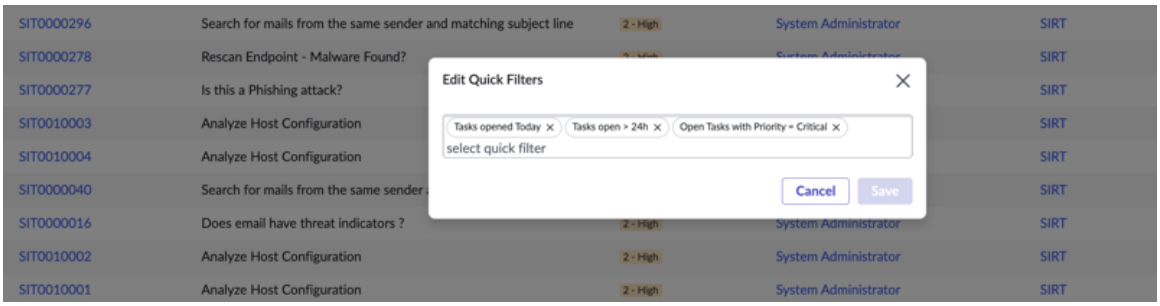
1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간.
2. 목록( ) 아이콘을 클릭합니다.
3. 예를 들어, 목록 〉 보안 인시던트 〉 빠른 필터 절.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 편집 아이콘을 클릭하여 변경합니다.

> **주:**
> 변경한 내용은 유지되며 다음에 사용자가 이 페이지로 다시 돌아오면 유지된 기본 설정이 표시됩니다.



5. 저장을 클릭합니다.

보안 인시던트 또는 응답 작업 익스포트

목록 뷰에서 보안 인시던트 또는 응답 작업을 익스포트합니다.

시작하기 전에

필요한 역할: sn_si.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간.

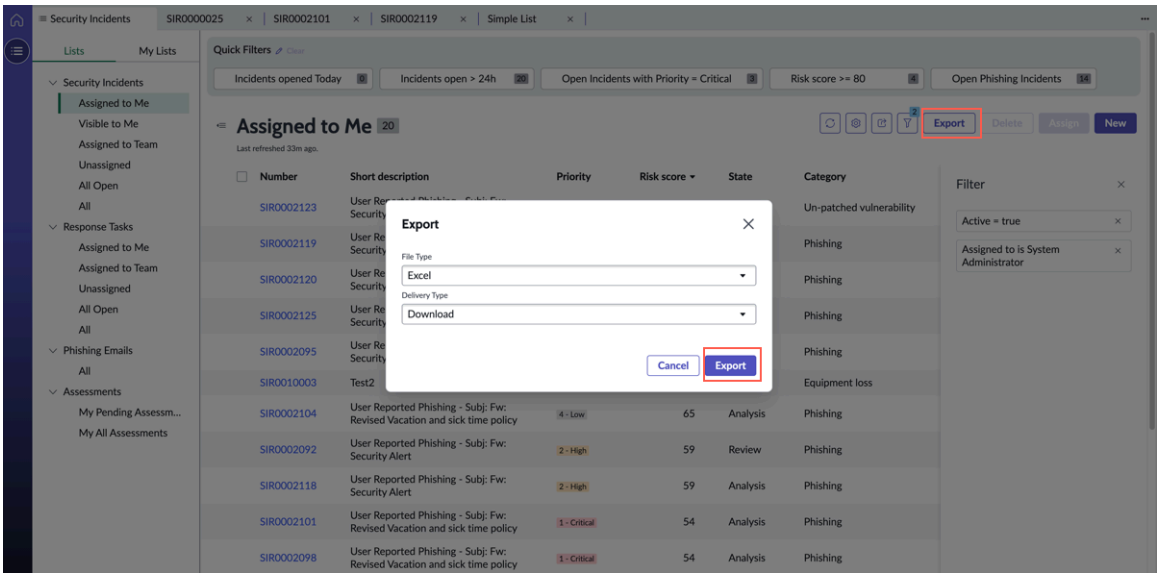
2. 목록 아이콘을 클릭합니다.

3. 목록을 클릭합니다.

4. 이동 보안 인시던트 또는 응답 작업 〉 모든 오픈 항목.

5. 목록을 보고 내보내기를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



6. 파일 유형 및 제공 유형을 선택합니다.
   예를 들어 **Excel** 을 선택하고 목록을 다운로드 하거나 이메일로 보낼 수 있습니다.
7. 익스포트를 클릭합니다.
   선택한 옵션에 따라 파일이 다운로드되거나 이메일로 전송됩니다.

교대조 핸드오버 기록 관리

교대조 핸드오버 기록 목록 뷰를 사용하여 교대조 핸드오버 기록을 생성, 편집, 복사 또는 삭제합니다. 각 교대조 핸드오버 기록은 교대조 핸드오버 보고서 템플릿과 연결됩니다.

시작하기 전에

필요한 역할:

- sn_escm_sh.shift_analyst: 교대조 핸드오버 기록에 액세스하기 위한 최소 요구 사항입니다.
- sn_escm_sh.shift_owner: 교대조 소유자가 속한 사용자 그룹에서 핸드오버 로그 기록을 작성, 편집 및 삭제합니다. 이 역할은 sn_escm_sh.shift_analyst 역할을 상속합니다.
- sn_escm_sh.shift_analyst: 모든 교대조 핸드오버 로그 기록을 보거나 교대조 분석가의 그룹에 할당된 진행 중인 교대조 핸드오버 기록에만 기여할 수 있습니다.
- sn_si.analyst - sn_escm_sh.shift_analyst 역할을 상속합니다.
- sn_si.admin - sn_escm_sh.shift_admin 역할을 상속합니다.
- sn_escm_sh.shift_admin - sn_escm_sh.shift_owner 역할을 상속합니다.

중요사항:
관리자로서 교대조 핸드오버 템플릿을 구성하는 방법에 대한 자세한 내용은 문서를 참조하십시오 교대조 핸드오버 템플릿 구성.

이 태스크 정보

교대조 소유자와 해당 팀 또는 사용자 그룹이 교대조 핸드오버 로그 기록을 생성합니다. 교대조 소유자는 교대조 핸드오버 보고서에서 작업할 교대조 핸드오버 템플릿과 사용자 그룹을 선택해야 합니다. 교대조 핸드오버 보고서가 완료되면 다음 활성 교대조 소유자 및 팀과 공유됩니다.

교대조 핸드오버 템플릿 핵심 사항:

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 활성 교대조 팀의 다른 분석가가 사용자보다 먼저 보고서를 업데이트한 경우 변경이 처리 중이면 보류 중인 컨텐츠 업데이트가 있다는 오류 메시지가 표시될 수 있습니다. 30초 동안 기다린 다음 "검토" 상태로 변경을 다시 선택해야 합니다. 오른쪽 창에서 통합 보고서를 볼 수 있으며 다른 분석가의 업데이트된 내용으로 업데이트됩니다.
- 교대조 소유자가 검토 상태의 섹션에서 컨텐츠를 수정한 경우 기록이 진행 중 상태로 다시 이동할 때 분석가에게 동일한 컨텐츠가 반영됩니다.
- 교대조 소유자는 검토 상태에서 컨텐츠를 편집하고 두 줄 병합, 두 섹션 병합, 섹션 제거와 같은 작업을 수행할 때 다른 분석가의 교대조 핸드오버 보고서에 영향을 미칠 수 있으므로 주의해야 합니다.
- 교대조 핸드오버 보고서를 게시한 후 교대조 소유자는 컨텐츠를 수정할 수 있지만 기록 상태를 변경할 수는 없습니다.
- 누군가가 컨텐츠를 수정하는 동안 해당 시간 동안 기록 상태가 진행 중에서 검토로 변경되면 저장되지 않은 컨텐츠 변경 내용이 삭제됩니다.
- 교대조 관리자는 사용자 그룹과 관계없이 모든 교대조 핸드오버 로그 기록에 대한 쓰기 권한을 갖습니다.

프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간.
2. 보안 인시던트 목록 아이콘을 선택합니다.
3. 목록 탭에서 교대조 핸드오버 기록을 선택합니다.
4. 모든 교대조 핸드오버 기록 목록을 보려면 모든 기록을 선택합니다.
5. 분석가가 속한 모든 팀/사용자 그룹에 할당된 교대조 핸드오버 기록 목록을 보려면 팀에 할당 됨을 선택합니다.
6. 새 교대조 핸드오버 기록을 생성하려면 새로 만들기를 선택합니다.
7. 양식에서 필드를 채웁니다.

교대조 핸드오버 기록

필드	설명
번호	교대조 핸드오버 기록에 대해 자동으로 생성되는 고유 번호입니다.
템플릿	사용할 교대조 핸드오버 템플릿입니다. 예를 들어, 샘플 교대조 템플릿입니다.
설명	교대조 핸드오버 기록에 대한 설명입니다.
사용자 그룹	할당할 교대조 핸드오버 기록의 사용자 그룹/팀입니다. 예를 들어 팀 개발 코드 검토자입니다.
상태	교대조 핸드오버 기록의 현재 상태입니다. 기본적으로 초기 상태는 초안입니다 **주:** 기록을 생성하는 동안에는 상태를 변경할 수 없습니다.

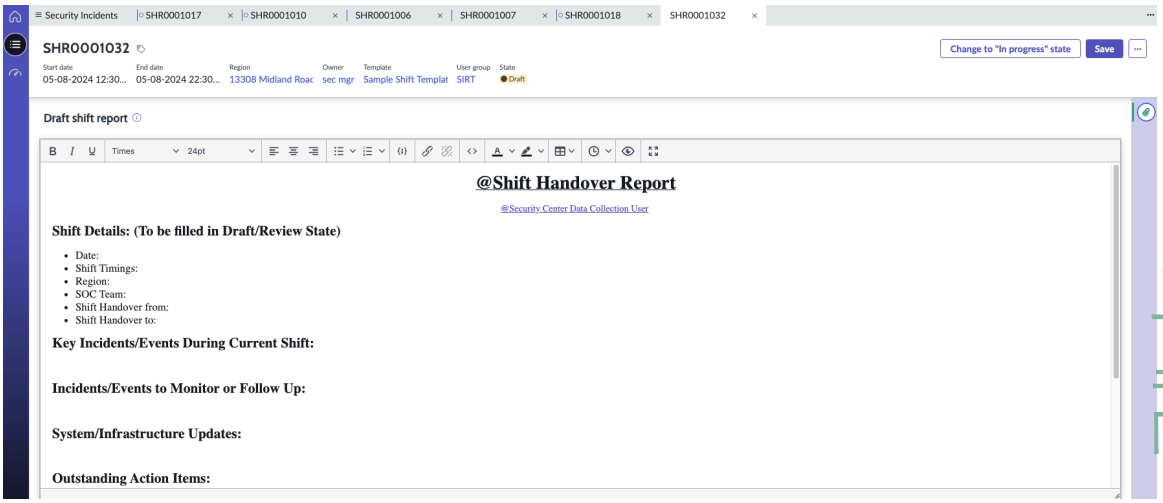
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
교대조 이름	교대조 시작 및 교대조 종료 상세 정보가 포함된 교대조 이름입니다. 예를 들어 미국 주간 교대조입니다.

8. 생성을 선택합니다.
   선택하고 목록 뷰에 추가한 템플릿을 기반으로 새 교대조 핸드오버 기록이 생성됩니다.
9. 새 교대조 핸드오버 기록을 열어 교대조 핸드오버 보고서에서 보안 인시던트의 상태와 상세 정보를 업데이트합니다.
   기본적으로 교대조 핸드오버 기록은 초안 상태입니다.

   주:
   교대조 소유자만 컨텐츠를 수정할 수 있습니다.

   교대조 핸드오버 보고서 컨텐츠



10. 초안 교대조 보고서 편집기에서 교대조 핸드오버 보고서 템플릿 섹션을 사용하여 보안 인시던트 및 사용자에 관한 상세 정보를 업데이트합니다.

    편집기의 모든 옵션(예: 글꼴, 색상, 글머리 기호, 링크, 첨부 파일)을 사용하여 보고서의 서식을 지정할 수 있습니다.

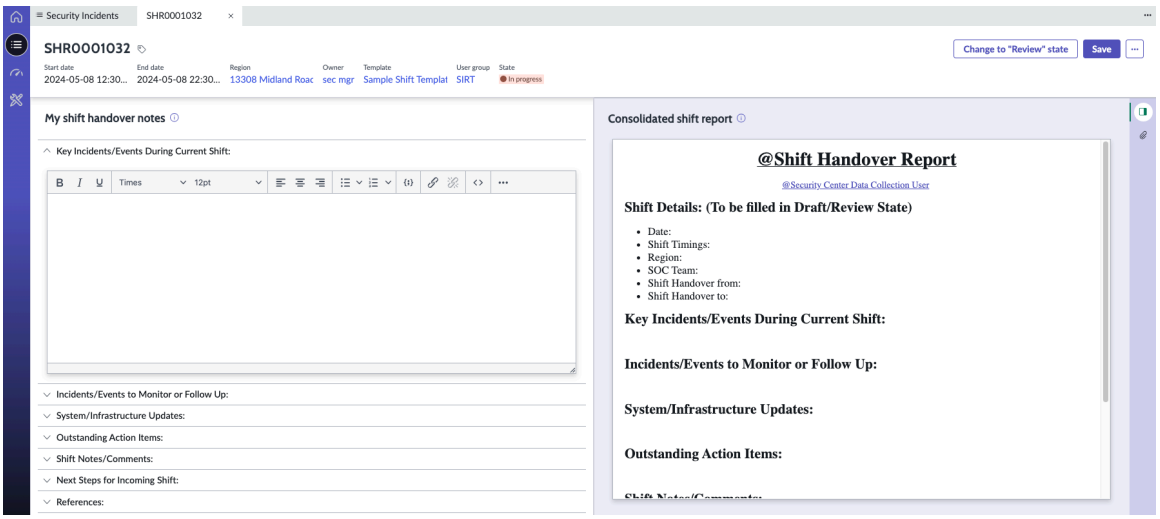
    주:
    교대조 소유자와 교대조 분석가는 모두 컨텐츠를 수정할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 교대조 핸드오버 보고서에 필요한 변경을 수행한 후 저장을 선택합니다.

b. 교대조 핸드오버 기록을 진행 중 상태로 전환하려면 "진행 중" 상태로 변경 작업을 선택합니다.

교대조 핸드오버 진행 중

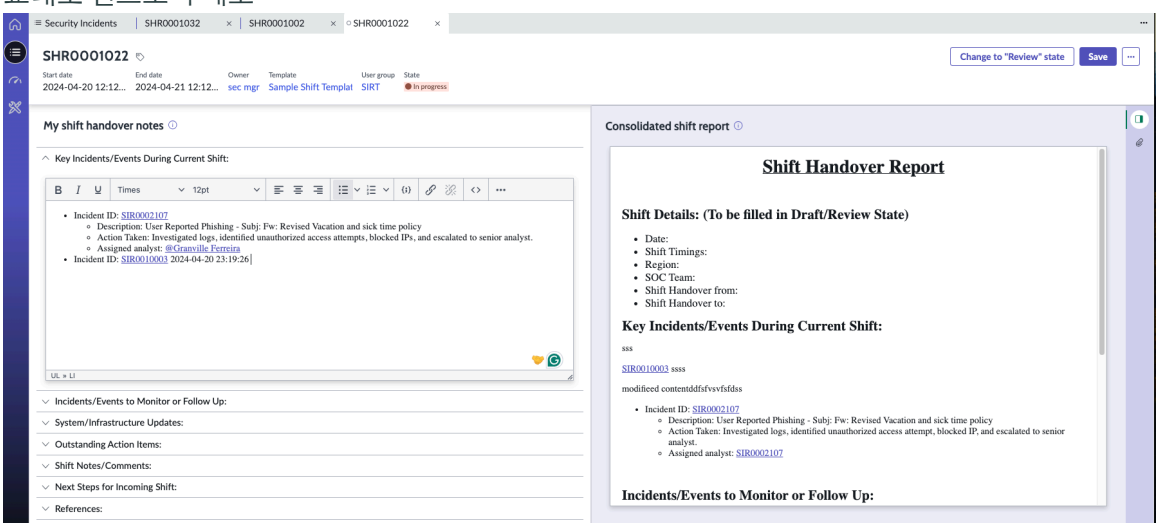


11. 내 교대조 핸드오버 메모 편집기에서 보안 인시던트 및 사용자 상세 정보와 같은 모든 섹션에 필요한 상세 정보를 업데이트합니다.

> **주:**
> 교대조 소유자와 교대조 분석가는 모두 컨텐츠를 수정할 수 있습니다.

a. 편집기에서 특정 기록을 언급하려면 /를 사용하고 기록 선택을 선택한 다음 팝업되는 테이블 목록에서 기록을 선택합니다.
예를 들어 보안 인시던트 기록을 선택하면 보안 인시던트 목록이 나타납니다. 목록에서 보안 인시던트(**SIR0010025**)를 선택하고 필요한 교대조 핸드오버 상세 정보를 업데이트합니다. 보안 인시던트 번호 뒤에 /를 사용하여 짧은 설명, 감시 list와 같은 보안 인시던트 관련 필드를 언급할 수도 있습니다.

교대조 핸드오버 메모



b. 편집기에서 특정 사용자를 언급하려면 /를 사용하고 사용자 선택을 선택한 다음, 팝업되는 목록에서 사용자를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

c. 편집기에서 레코드 수를 언급하려면 /를 사용하고 멘션 수를 선택한 다음 팝업 목록에서 레코드를 선택합니다.

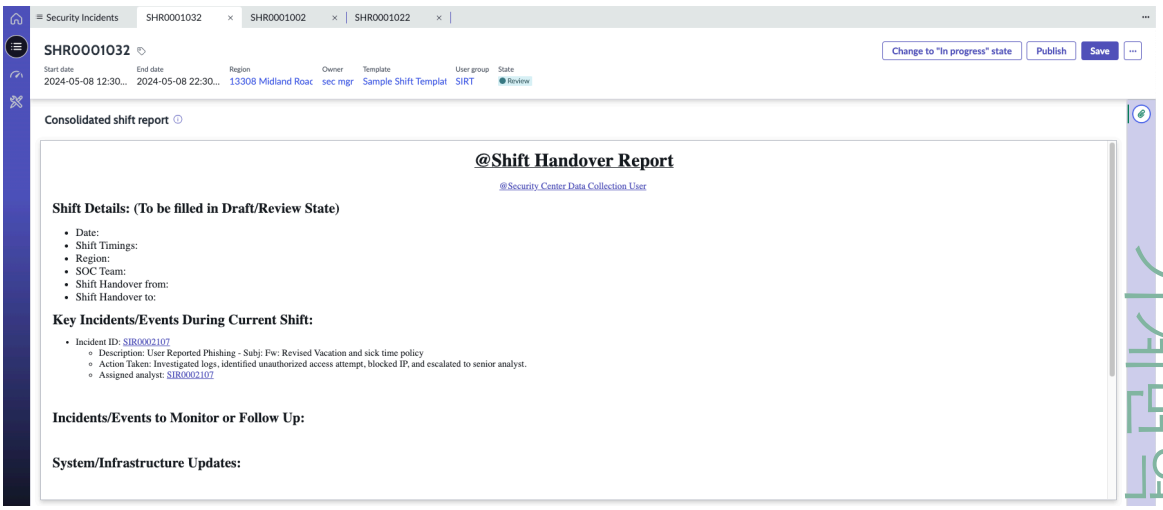
d. 편집기의 모든 옵션(예: 글꼴, 색상, 글머리 기호, 링크, 첨부 파일)을 사용하여 보고서의 서식을 지정할 수 있습니다.

e. 교대조 핸드오버 메모에 필요한 변경을 수행한 후 저장을 선택합니다.

f. 교대조 핸드오버 기록을 검토 상태로 이동하려면 "검토" 상태로 변경 작업을 선택합니다.

주:
활성 교대조 팀의 다른 분석가가 사용자보다 먼저 보고서를 업데이트한 경우 변경이 처리 중인 경우 오류 메시지가 표시될 수 있습니다. 몇 초간 기다린 다음 "검토" 상태로 변경을 다시 선택해야 합니다.

교대조 핸드오버 검토



12. 통합 교대조 보고서에서 교대조 핸드오버 보고서를 검토하고 필요한 사항을 변경합니다.

주:
교대조 소유자만 컨텐츠를 수정할 수 있습니다.

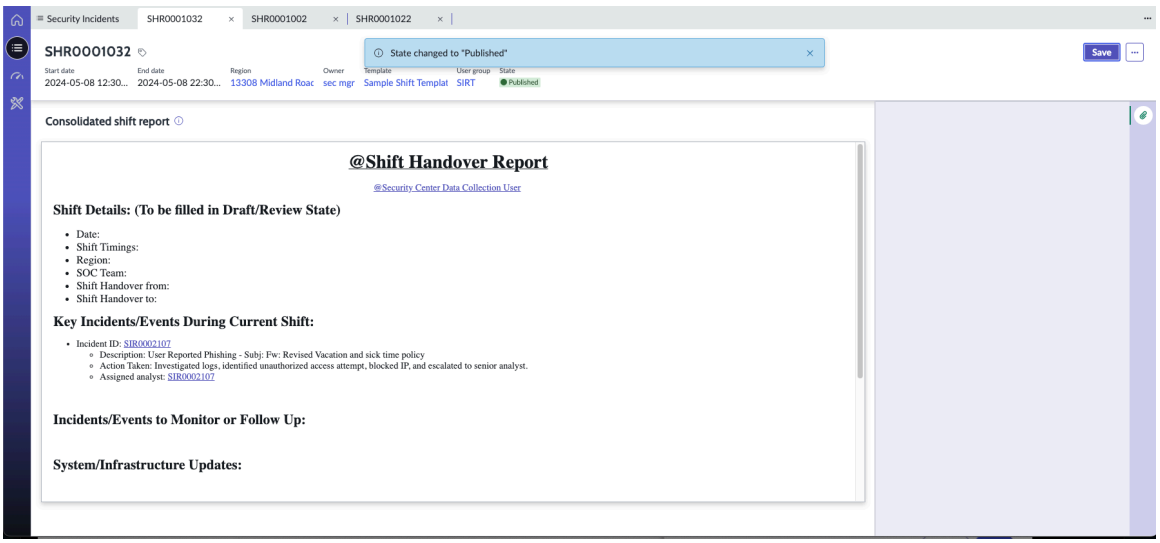
a. 교대조 핸드오버 메모에 필요한 변경을 수행한 후 저장을 선택합니다.

b. 교대조 핸드오버 보고서에 분석가의 추가 업데이트가 필요한 경우 "진행 중" 상태로 변경을 선택할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

c. 게시 작업을 선택하여 교대조 핸드오버 보고서를 게시합니다.

교대조 핸드오버 게시



13. 저장을 선택하여 교대조 핸드오버 보고서를 저장합니다.
저장한 후에는 미리 보기 창에서 최신 업데이트가 포함된 교대조 핸드오버 보고서의 미리 보기를 볼 수 있습니다.

> **주:**
> 교대조 핸드오버 보고서에서 업데이트된 내용을 즉시 미리 볼 수 있지만 다른 분석가가 변경 내용을 확인하는 데 몇 초 정도 걸릴 수 있습니다.

14. 교대조 소유자는 교대조 핸드오버 목록 뷰에서 다음 작업을 수행할 수도 있습니다.

a. 기존 교대조 핸드오버 기록을 편집하려면 기록을 선택하고 편집 작업을 선택합니다.
시작 시간, 종료 시간, 설명 및 지역만 수정할 수 있습니다.

b. 교대조 핸드오버 기록의 복사본을 생성하려면 기록을 선택하고 복사 작업 생성을 선택합니다.

c. 기존 교대조 핸드오버 기록을 삭제하려면 기록을 선택하고 삭제 작업을 선택합니다.

SIR Workspace 구성

이 단원에서는 를 보안 인시던트 응답 작업 공간사용하는 데 필요한 구성에 대해 설명합니다.

SIR 기록 뷰 설정

이 섹션에서는 쉽게 탐색할 수 있도록 관련 목록을 그룹화하고 SIR 관련 기록 탭에 표시하는 방법을 설명합니다.

작업 공간 사용자는 관련 목록을 이름으로도 검색할 수 있습니다. 관련 목록 구성에 대한 자세한 내용은 다음 문서를 참조하십시오 SIR Workspace 관련 기록.

SI 설계 시간 조사 구성

이 섹션을 사용하여 보안 인시던트 설계 시간 조사 페이지를 구성하여 여러 엔트리포인트 및 관련 기록을 보안 인시던트 응답 작업 공간.

필요한 역할: sn_si.admin.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음은 조사 보안 인시던트 응답 작업 공간페이지 구성과 관련된 단계를 자세히 설명합니다.

- 관련된 정보 테이블에 대한 뷰 생성
- 엔트리포인트 목록 추가
- 엔트리포인트 목록에 대한 연결 정보의 매핑 뷰
- 런타임 데이터 렌더링을 처리하도록 뷰에서 연결된 각 목록을 구성합니다.

관련 정보

조사 캔버스 탐색

관련된 정보 테이블에 대한 뷰 생성

조사 화면은 보안 인시던트에서 생성된 관련 목록 뷰를 활용하여 관련 목록을 구성합니다.

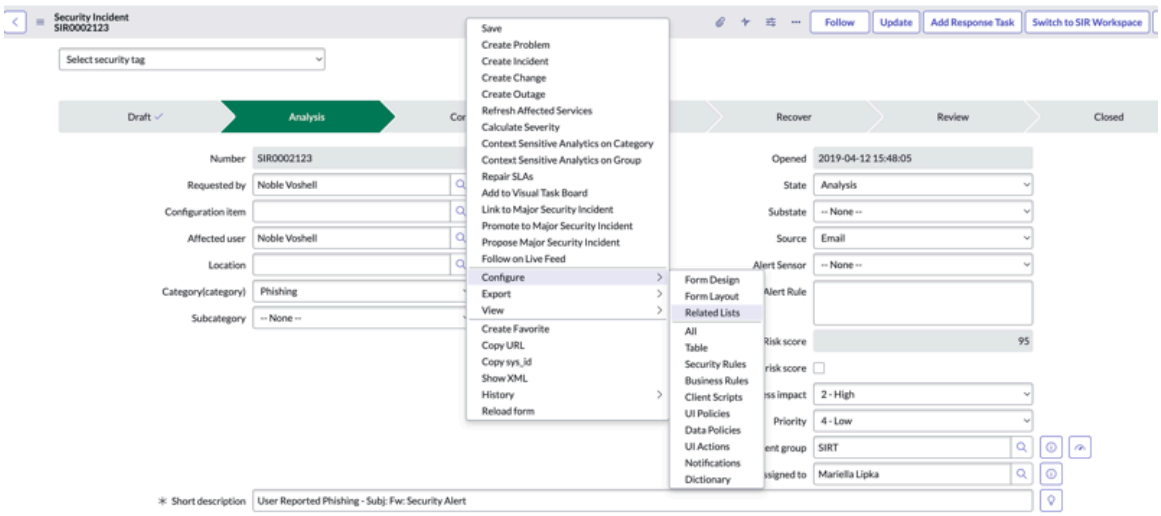
시작하기 전에

필요한 역할: sn_si.admin

다음은 뷰를 만들고 관련 목록을 추가하는 절차입니다.

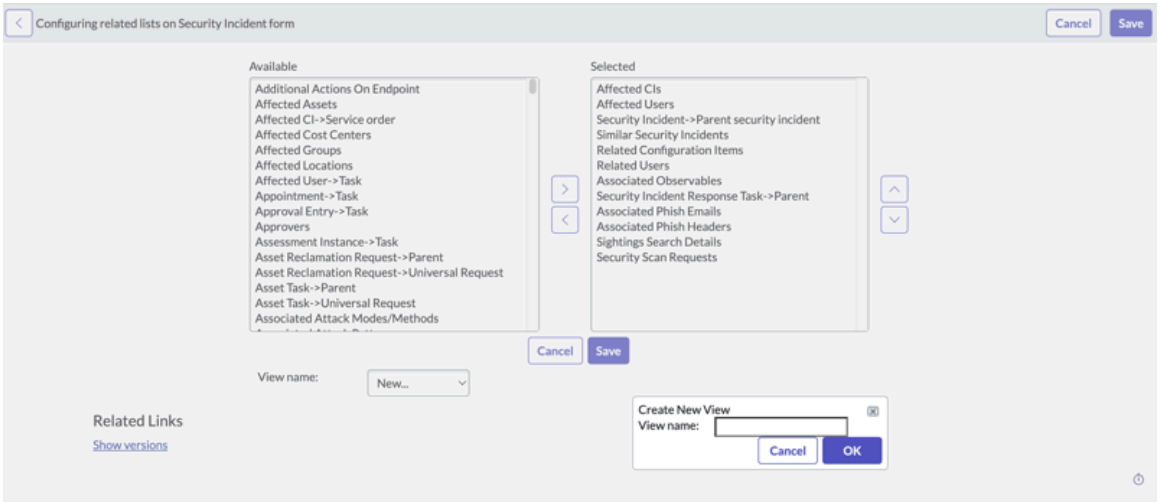
프로시저

1. 보안 인시던트 목록으로 이동합니다.
2. 클래식 UI에서 보안 인시던트를 엽니다.
3. 양식 컨텍스트 메뉴에서 다음으로 이동합니다. 구성 〉 관련 목록.
   슬러시 버킷 창이 표시됩니다.



4. 뷰 이름 드롭다운 목록으로 이동하고 새로 만들기를 클릭하여 새 뷰를 만듭니다.
   뷰에 이름을 추가해야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



5. 새로 생성된 뷰 아래의 오른쪽 버킷에 원하는 관련 목록을 추가하고 뷰를 저장합니다.
이 뷰는 조사 탭에서 관련 정보를 렌더링하는 데 사용됩니다.

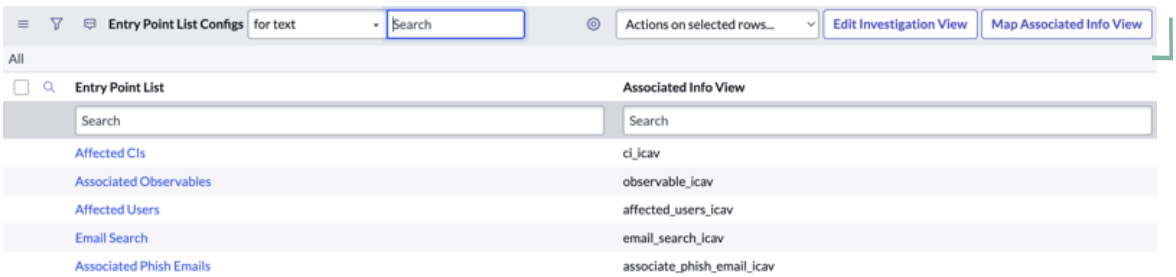
엔트리포인트 목록 추가

새 엔트리포인트 목록을 구성하여 조사 페이지에 추가합니다.

시작하기 전에
필요한 역할: 관리자

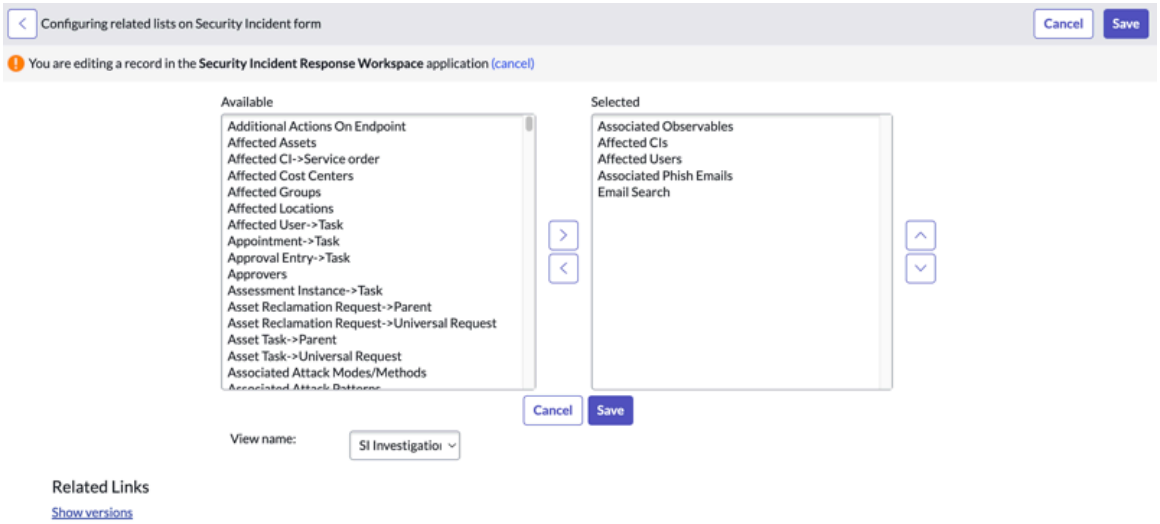
프로시저

1. 다음으로 이동 **sn_si_aw_entry_point_config.list**.
엔트리포인트 목록 구성 페이지가 표시됩니다.



2. 조사 화면에 엔트리포인트 목록을 추가하려면 조사 뷰 편집 버튼을 클릭합니다.
보안 인시던트 관련 목록 구성 양식이 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



3. 슬러시 버킷 뷰에서 엔트리포인트 목록을 추가하거나 제거합니다.

4. 저장을 클릭합니다.

> **주:**
> 엔트리포인트 목록이 있는 조사 화면에 해당하는 뷰를 **SI** 조사 뷰 라고 하며 조사 뷰 편집 페이지로 이동할 때 기본적으로 선택됩니다.
>
> 진입점 목록이 조사 캔버스에 표시되는 순서는 슬러시 버킷 선택됨 뷰의 순서에 따라 결정됩니다.

엔트리포인트 목록에 대한 연결 정보의 매핑 뷰

맵 관련 정보 뷰 작업을 사용하여 관련 정보 뷰를 새로 추가된 엔트리포인트 목록에 매핑합니다.

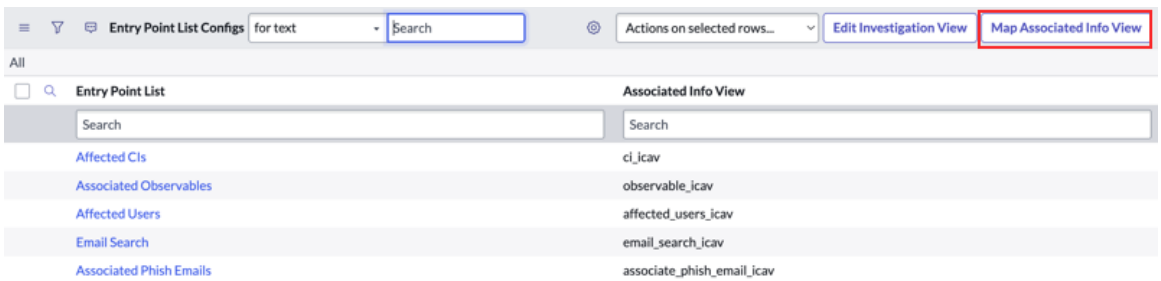
시작하기 전에

> **주:**
> 이 단계는 조사 페이지에 엔트리포인트 목록을 표시하는 데 필요합니다. 엔트리포인트 아래에 관련 정보 목록이 표시되지 않도록 하려면 더미 뷰를 생성하고 매핑해야 합니다.

필요한 역할: 관리자

프로시저

1. 엔트리포인트 구성 페이지에서 연결된 정보 뷰 매핑 버튼을 클릭합니다.

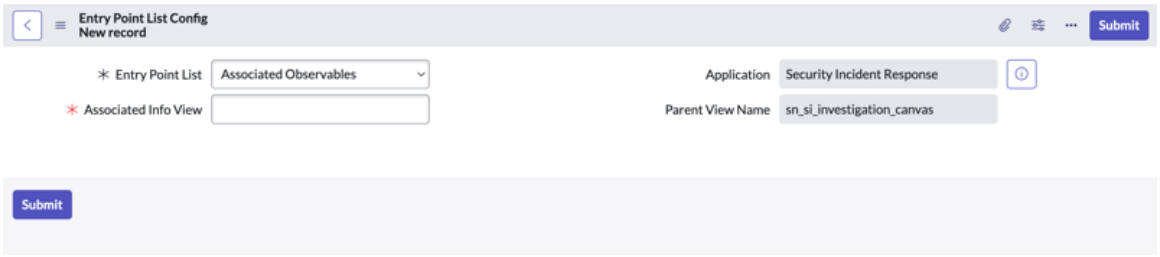


2. 엔트리포인트 목록 드롭다운 목록에서 새로 추가된 엔트리포인트 목록을 선택합니다.

3. 관련 정보 뷰 필드에 관련 정보 관련 목록이 포함된 뷰 이름을 입력합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관련 정보 관련 목록에 대한 뷰를 만드는 방법에 대한 자세한 내용은 문서를 참조하십시오 관련된 정보 테이블에 대한 뷰 생성.



4. 폼을 저장합니다.
5. 또한 필요한 경우 연결된 정보 뷰 편집을 사용하여 연결된 목록을 더 추가하거나 제거할 수 있습니다.
   엔트리포인트 목록 레이아웃 편집 작업을 사용하여 엔트리포인트 목록 레이아웃을 구성할 수도 있습니다. 원하는 경우 슬러시버킷에서 열을 추가하거나 제거하고 양식을 저장합니다.

런타임 데이터 렌더링을 처리하도록 뷰에서 연결된 각 목록을 구성합니다.

런타임 데이터 렌더링을 처리하도록 뷰에서 각 관련 목록을 구성합니다.

시작하기 전에

주:
이 단계는 관련 정보 뷰에 구성된 각 관련 목록에 대해 필수입니다. 그러지 않으면 조사 페이지에서 관련 목록을 사용할 수 없습니다.

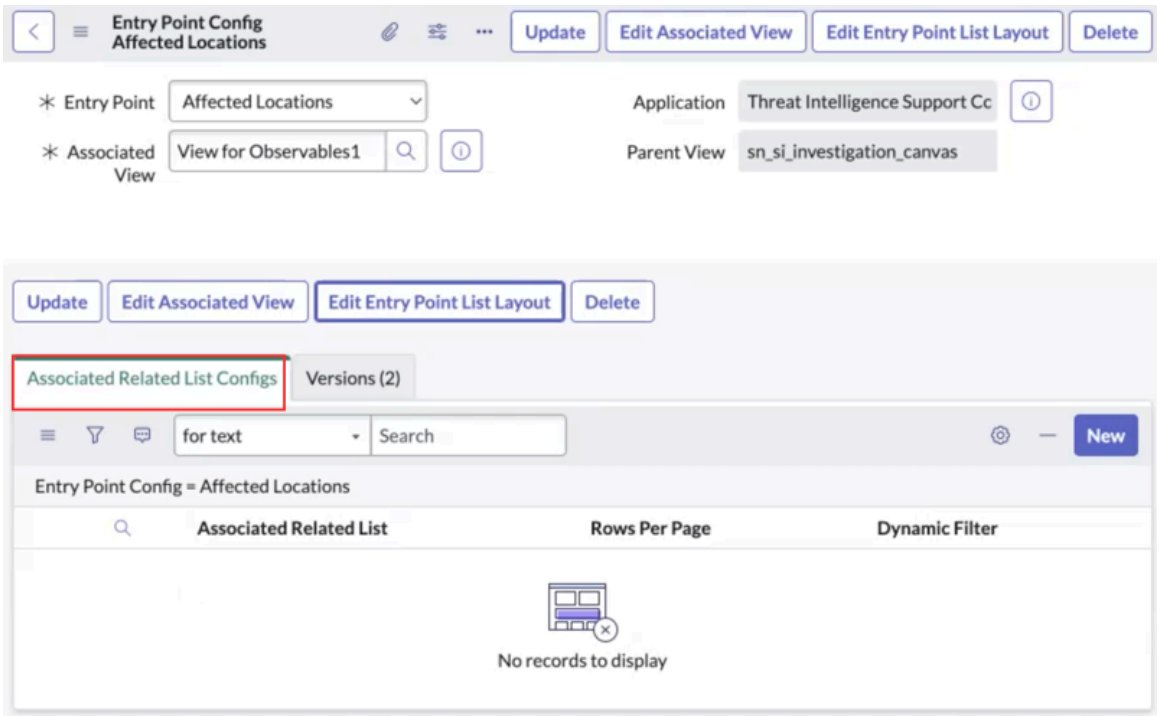
추가된 각 관련 목록(관련 정보 뷰를 엔트리포인트 목록에 매핑하는 동안)(엔트리포인트 목록에 대한 연결 정보의 매핑 뷰 또는 뷰에서 직접)에는 런타임 기록 선택 및 필터 선택과 관련하여 데이터를 필터링하기 위한 추가 구성이 필요합니다.

필요한 역할: 관리자

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

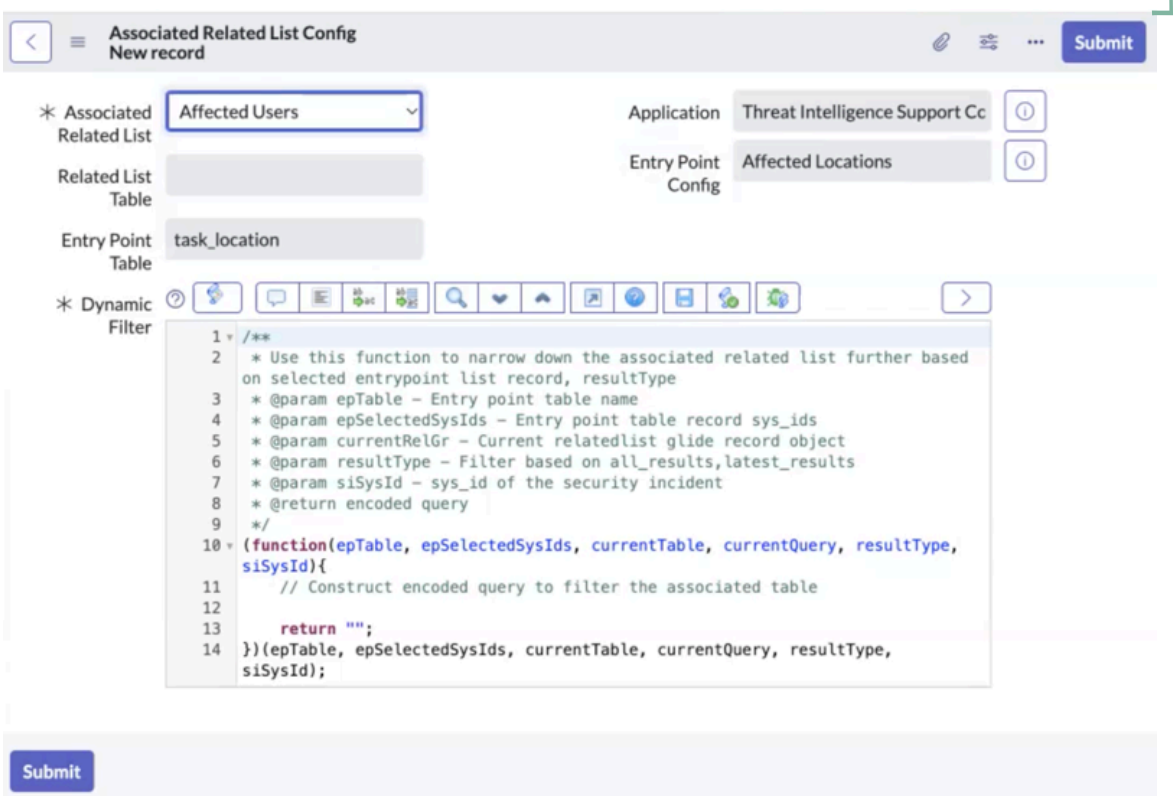
프로시저

1. 연결된 목록 구성에서 새로 만들기를 클릭합니다.



2. 연결된 목록 필드 값을 선택합니다.

3. 동적 필터 열을 사용하여 선택한 엔트리포인트 목록 기록 및 결과 유형(각 벤더 구현의 최신 결과, 모든 결과)을 기준으로 관련 목록을 추가로 필터링합니다.
제품 내에서 제공되는 기존 예시를 참조하십시오.



기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 또한 연결된 목록 레이아웃 편집 작업을 사용하여 연결된 목록 레이아웃을 구성할 수 있습니다. 슬러시 버킷 창에서 필요에 따라 열을 추가하거나 제거합니다.

SIR Workspace 관련 기록

이 섹션은 연결된 옵저버블 및 구성 항목과 같은 섹션으로 그룹화된 관련 목록 항목으로 구성됩니다.

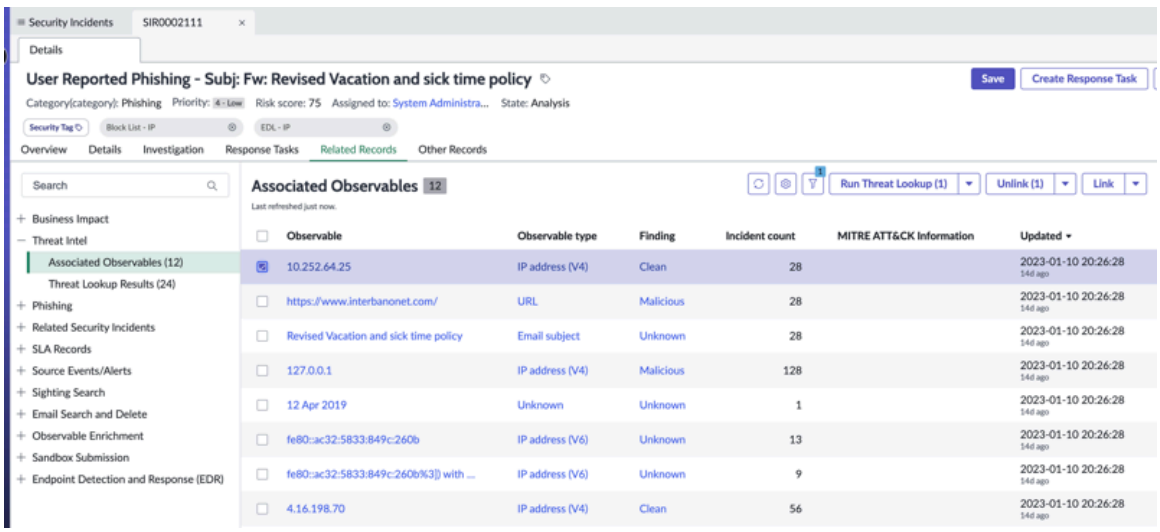
다음 관련 목록에는 기본 시스템의 일부로 사용할 수 있는 그룹이 나열되어 있습니다. 이러한 그룹을 수정하거나 애플리케이션 및 해당 작업 내에서 그룹을 생성할 수 있습니다.

이러한 그룹을 수정하거나 새 그룹을 생성할 수 있습니다. 자세한 내용은 보안 인시던트 및 응답 작업에 대한 관련 목록을 구성하고 그룹화하는 방법을 참조하십시오 보안 인시던트 관련 목록 구성 . 각 관련 목록은 .SIR Workspace

관련 목록	그룹화된 항목
비즈니스 영향	• 구성 항목 • 영향을 받는 사용자 • 관련 구성 항목 • 관련 사용자 • 영향을 받는 서비스
위협 인텔리전스	• 연결된 옵저버블 • 위협 조회 결과
피싱	• 연결된 피싱 메일 • 연결된 피싱 헤더
관련 보안 인시던트	• 상위 보안 인시던트 • 하위 보안 인시던트 • 유사한 보안 인시던트
SLA 기록	작업 SLA
소스 이벤트/경보	소스 이벤트 또는 경보는 소스 이메일, LogRhythm 드릴다운 로그, LogRhythm 이벤트, 집계된 IBM QRadar Offense 등의 SIEM 통합 지원 관련 목록입니다. **주:** 이 목록은 인스턴스에 있는 통합에 따라 완전히 달라집니다. 관련 SIEM 통합 관련 목록을 보려면 최신 버전을 설치해야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관련 목록	그룹화된 항목
검색 찾기	• 사이팅 검색 결과 • 사이팅 검색 정보 • 사이팅
관찰 대상 보강	• 옵저버블 보강 결과 • 연결된 MISP 이벤트 • MISP 보강 결과
엔드포인트 탐지 및 응답(EDR)	• 호스트 상세 정보 • 실행 중인 프로세스 • 운영 서비스 • 로그온한 사용자 • 네트워크 통계 • 파일 가져오기 • 호스트 항목 격리 • 엔드포인트에 대한 추가 작업 • Microsoft Defender for Endpoint-Related Machines 세부 정보



주:
일반적으로 해당되는 경우 관련 목록 그룹에 대해 새 기록을 만들거나 기존 기록 또는 새 기록을 연결하거나 연결 해제할 수 있습니다.

관련 정보

보안 인시던트 관련 목록 구성

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 인시던트 관련 목록 구성

새 관련 목록 또는 새 관련 목록 그룹을 추가하고 에 표시되는 기존 그룹 또는 관련 목록을 수정할 수 있습니다 SIR Workspace.

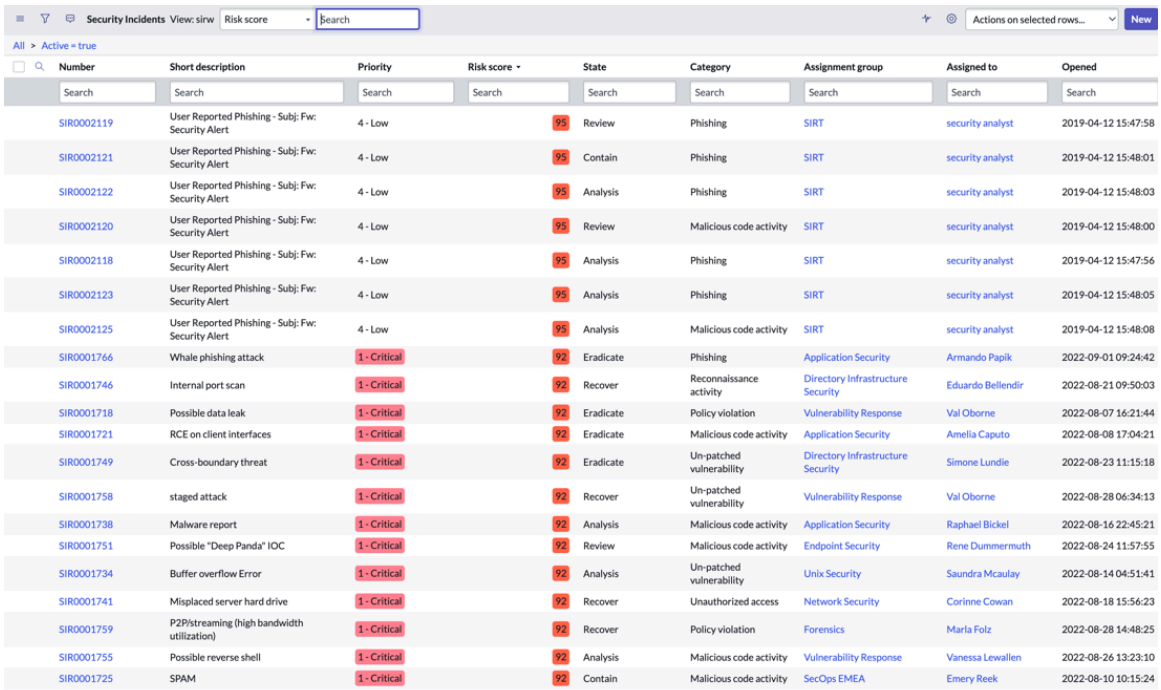
시작하기 전에

보안 인시던트 관련 목록이 그룹화되어 작업 공간의 관련 기록 탭에 그룹 관련 목록 항목으로 표시됩니다.

필요한 역할: sn_si.admin

프로시저

1. 클래식 UI에서 모두 〉 보안 인시던트 〉 열린 인시던트 표시.



Security Incidents View: sirw | Risk score | Search | Actions on selected rows... | New

All > Active = true

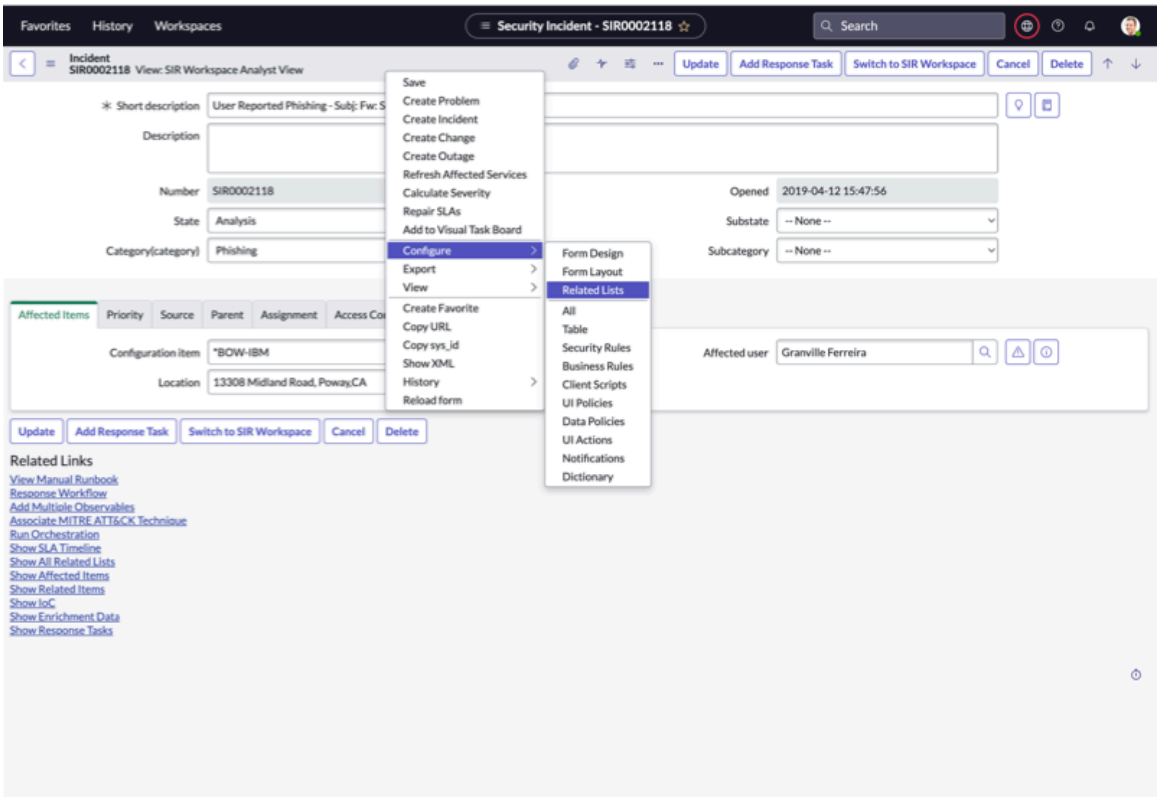
Number	Short description	Priority	Risk score	State	Category	Assignment group	Assigned to	Opened
SIR0002119	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Review	Phishing	SIRT	security analyst	2019-04-12 15:47:58
SIR0002121	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Contain	Phishing	SIRT	security analyst	2019-04-12 15:48:01
SIR0002122	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Analysis	Phishing	SIRT	security analyst	2019-04-12 15:48:03
SIR0002120	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Review	Malicious code activity	SIRT	security analyst	2019-04-12 15:48:00
SIR0002118	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Analysis	Phishing	SIRT	security analyst	2019-04-12 15:47:56
SIR0002123	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Analysis	Phishing	SIRT	security analyst	2019-04-12 15:48:05
SIR0002125	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Analysis	Malicious code activity	SIRT	security analyst	2019-04-12 15:48:08
SIR0001766	Whale phishing attack	1 - Critical	92	Eradicate	Phishing	Application Security	Armando Papik	2022-09-01 09:24:42
SIR0001746	Internal port scan	1 - Critical	92	Recover	Reconnaissance activity	Directory Infrastructure Security	Eduardo Bellendir	2022-08-21 09:50:03
SIR0001718	Possible data leak	1 - Critical	92	Eradicate	Policy violation	Vulnerability Response	Val Oborne	2022-08-07 16:21:44
SIR0001721	RCE on client interfaces	1 - Critical	92	Eradicate	Malicious code activity	Application Security	Amelia Caputo	2022-08-08 17:04:21
SIR0001749	Cross-boundary threat	1 - Critical	92	Eradicate	Un-patched vulnerability	Directory Infrastructure Security	Simone Lundie	2022-08-23 11:15:18
SIR0001758	staged attack	1 - Critical	92	Recover	Un-patched vulnerability	Vulnerability Response	Val Oborne	2022-08-28 06:34:13
SIR0001738	Malware report	1 - Critical	92	Analysis	Malicious code activity	Application Security	Raphael Bickel	2022-08-16 22:45:21
SIR0001751	Possible "Deep Panda" IOC	1 - Critical	92	Review	Malicious code activity	Endpoint Security	Rene Dummermuth	2022-08-24 11:57:55
SIR0001734	Buffer overflow Error	1 - Critical	92	Analysis	Un-patched vulnerability	Unix Security	Saundra Mcaulay	2022-08-14 04:51:41
SIR0001741	Misplaced server hard drive	1 - Critical	92	Recover	Unauthorized access	Network Security	Corinne Cowan	2022-08-18 15:56:23
SIR0001759	P2P/streaming (high bandwidth utilization)	1 - Critical	92	Recover	Policy violation	Forensics	Marla Folz	2022-08-28 14:48:25
SIR0001755	Possible reverse shell	1 - Critical	92	Analysis	Malicious code activity	Vulnerability Response	Vanessa Lewallen	2022-08-26 13:23:10
SIR0001725	SPAM	1 - Critical	92	Contain	Malicious code activity	SecOps EMEA	Emery Reek	2022-08-10 10:15:24

2. 인시던트 기록을 선택합니다.

3. 인시던트 컨텍스트 메뉴를 마우스 오른쪽 버튼으로 클릭합니다.

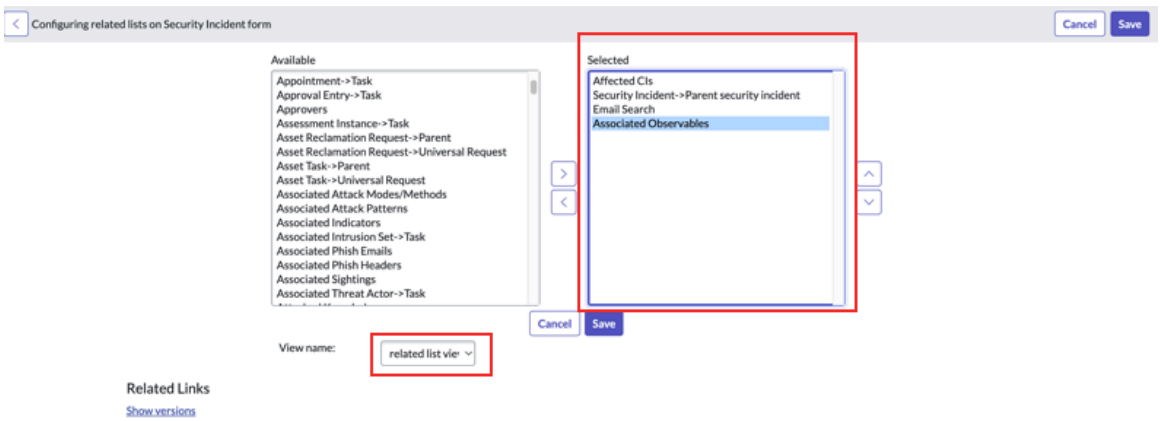
4. 이동 구성 〉 관련 목록.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



보안 인시던트 관련 목록 구성 양식이 표시됩니다.

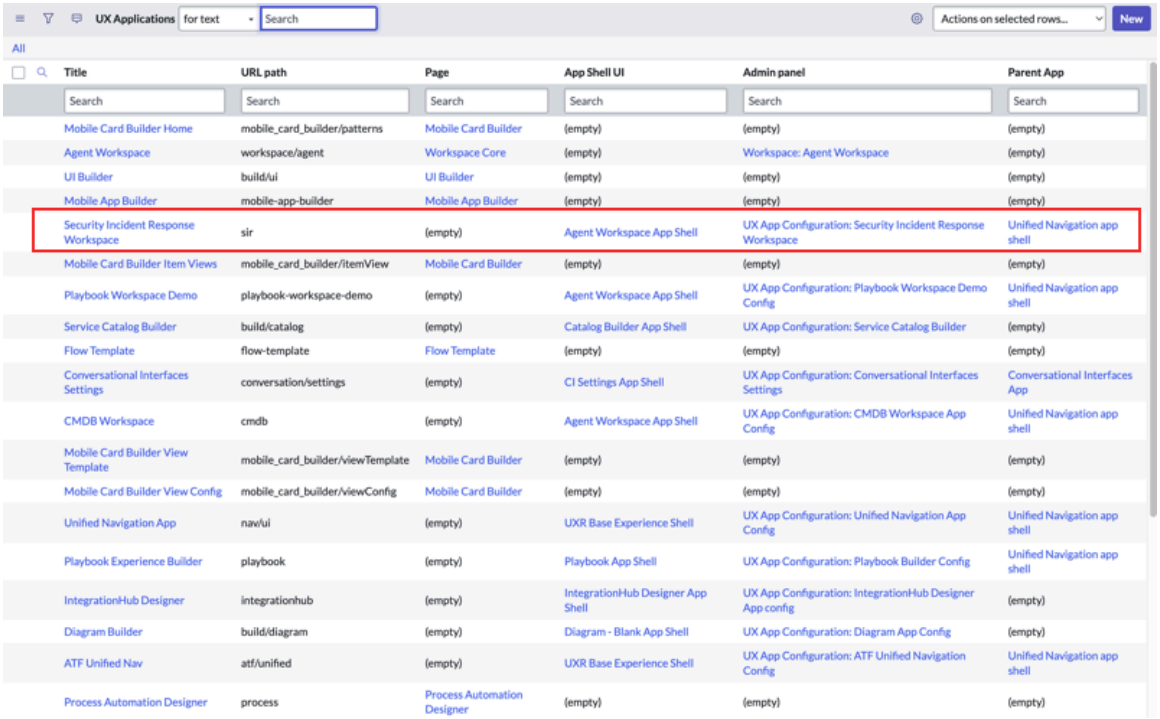
5. 이름 보기로 이동하고 새로 만들기를 선택합니다.
6. 뷰의 이름을 입력합니다.
7. 새로 만든 뷰를 선택합니다.
   뷰를 선택한 후 슬러시버킷에서 필요한 관련 목록 필드를 선택합니다.



> **주:**
> 수정하려면 뷰를 선택하고 항목을 제거하거나 추가합니다.

8. 저장을 클릭합니다.
9. 왼쪽 탐색에서 모두 〉 **Now Experience** 프레임워크 〉 경험.
10. 보안 인시던트 응답 작업 공간을 선택합니다.

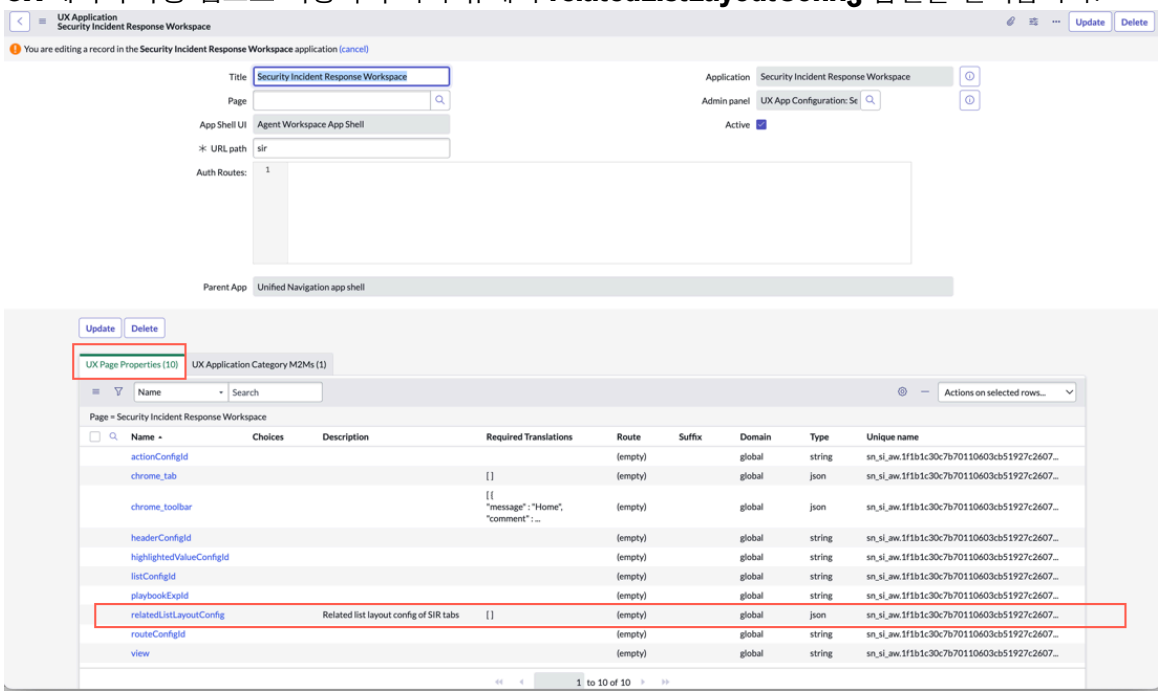
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



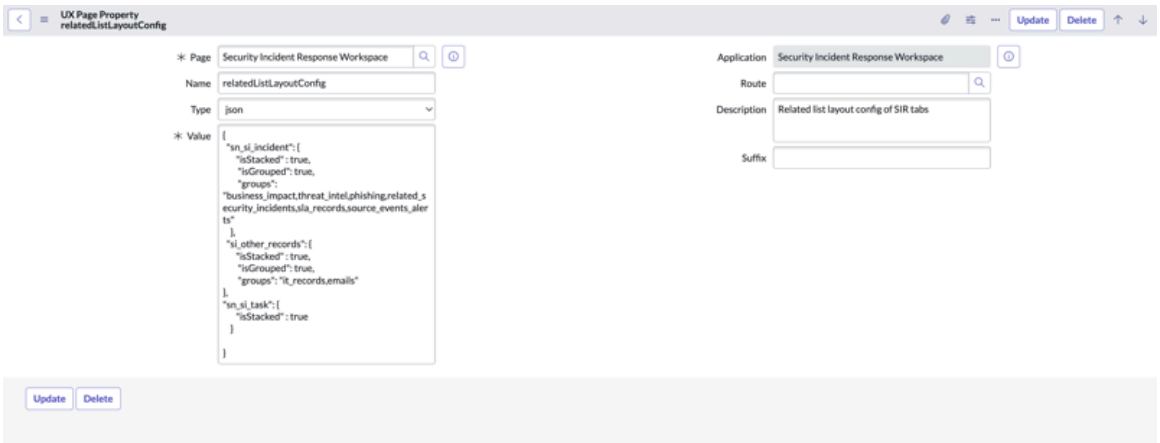
Title	URL path	Page	App Shell UI	Admin panel	Parent App
Search	Search	Search	Search	Search	Search
Mobile Card Builder Home	mobile_card_builder/patterns	Mobile Card Builder	(empty)	(empty)	(empty)
Agent Workspace	workspace/agent	Workspace Core	(empty)	Workspace: Agent Workspace	(empty)
UI Builder	build/ui	UI Builder	(empty)	(empty)	(empty)
Mobile App Builder	mobile-app-builder	Mobile App Builder	(empty)	(empty)	(empty)
Security Incident Response Workspace	sir	(empty)	Agent Workspace App Shell	UX App Configuration: Security Incident Response Workspace	Unified Navigation app shell
Mobile Card Builder Item Views	mobile_card_builder/itemView	Mobile Card Builder	(empty)	(empty)	(empty)
Playbook Workspace Demo	playbook-workspace-demo	(empty)	Agent Workspace App Shell	UX App Configuration: Playbook Workspace Demo Config	Unified Navigation app shell
Service Catalog Builder	build/catalog	(empty)	Catalog Builder App Shell	UX App Configuration: Service Catalog Builder	(empty)
Flow Template	flow-template	Flow Template	(empty)	(empty)	(empty)
Conversational Interfaces Settings	conversation/settings	(empty)	CI Settings App Shell	UX App Configuration: Conversational Interfaces Settings	Conversational Interfaces App
CMDB Workspace	cmdb	(empty)	Agent Workspace App Shell	UX App Configuration: CMDB Workspace App Config	Unified Navigation app shell
Mobile Card Builder View Template	mobile_card_builder/viewTemplate	Mobile Card Builder	(empty)	(empty)	(empty)
Mobile Card Builder View Config	mobile_card_builder/viewConfig	Mobile Card Builder	(empty)	(empty)	(empty)
Unified Navigation App	nav/ui	(empty)	UXR Base Experience Shell	UX App Configuration: Unified Navigation App Config	Unified Navigation app shell
Playbook Experience Builder	playbook	(empty)	Playbook App Shell	UX App Configuration: Playbook Builder Config	Unified Navigation app shell
IntegrationHub Designer	integrationhub	(empty)	IntegrationHub Designer App Shell	UX App Configuration: IntegrationHub Designer App config	(empty)
Diagram Builder	build/diagram	(empty)	Diagram - Blank App Shell	UX App Configuration: Diagram App Config	(empty)
ATF Unified Nav	atf/unified	(empty)	UXR Base Experience Shell	UX App Configuration: ATF Unified Navigation Config	Unified Navigation app shell
Process Automation Designer	process	Process Automation Designer	(empty)	(empty)	(empty)

UX 애플리케이션 보안 인시던트 응답 작업 공간 페이지가 표시됩니다.

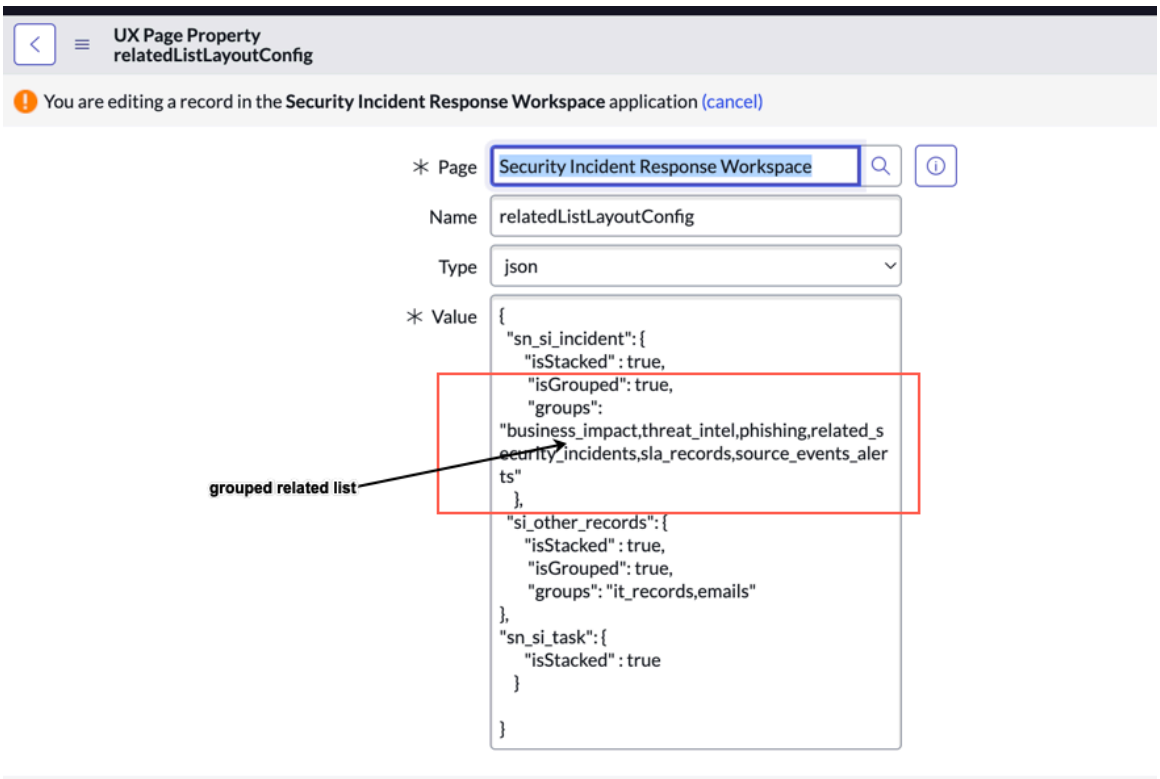
11. **UX** 페이지 속성 탭으로 이동하여 목록 뷰에서 **relatedListLayoutConfig** 옵션을 선택합니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



12. 새로 만든 뷰 이름을 **sn_si_incident.viewsUsedForGrouping** 필드 아래의 값 텍스트 상자에 있는 기존 값 목록에 쉼표로 구분하여 추가합니다.
예를 들어 비즈니스 영향 으로 새 뷰 이름을 생성한 경우 값 텍스트 상자에서 sn_si_incident:groups 필드 아래에 **business_impact** (뷰 이름 내에서 밑줄로 구분되고 기존 값 뒤에 쉼표로 구분됨)로 지정해야 합니다.

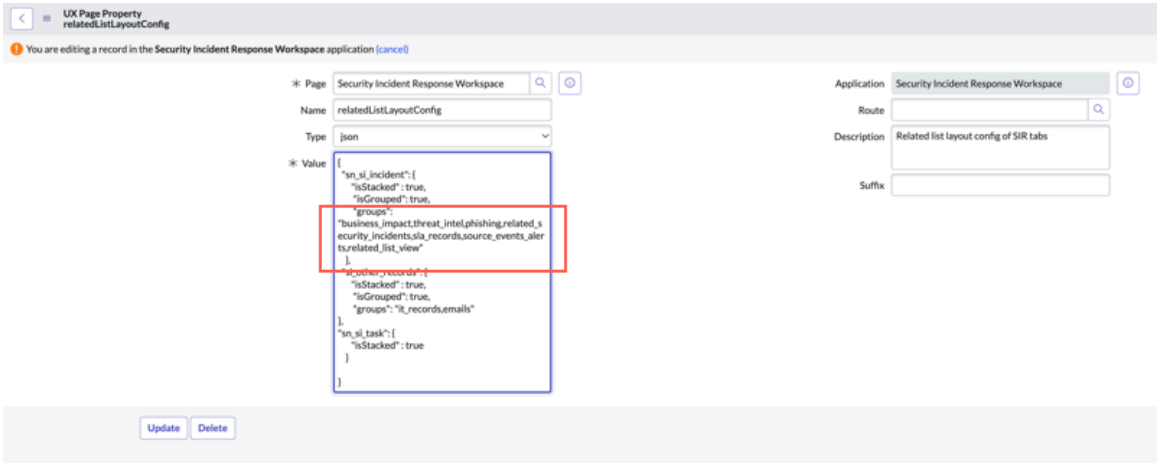


주:
sn_si_incident.viewsUsedForGrouping 필드 아래에 새 뷰 이름을 추가하면 작업 공간의 관련 기록 탭에 항목이 생성됩니다.

si_other_records.viewsUsedForGrouping에서 뷰 이름 항목을 업데이트하면 관련 목록 그룹이 작업 공간의 기타 기록 탭에 추가됩니다.

다음은 새로 생성된 뷰가 추가된 예시 뷰입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



주:
requiredRolesForGrouping 에는 쉼표로 구분된 sys_user_role 레코드 이름이 포함되어 있습니다. SIR 작업 공간 사용자에게 그룹화된 관련 목록을 사용하려면 이러한 역할 중 하나 이상의 역할이 있어야 합니다. 사용자에게 이러한 역할이 없는 경우 뷰 규칙 구성을 사용하여 현재 사용자 역할에 대해 구성된 관련 목록 뷰는 그룹화되지 않고 세로로 표시됩니다.
isGrouped 속성이 false로 설정되면 이 속성은 무시됩니다. 이 속성이 비어 있으면 모든 사용자가 그룹화된 관련 목록에 접근할 수 있습니다.

13. 저장을 클릭합니다.

14. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간.

15. 특정 보안 인시던트를 선택합니다.

16. 작업 공간의 관련 기록 탭으로 이동합니다.
그룹화된 관련 목록이 표시됩니다.

응답 작업 관련 목록 구성

이 섹션을 사용하여 보안 인시던트 응답 애플리케이션에 표시되는 새로운 관련 목록을 구성합니다.

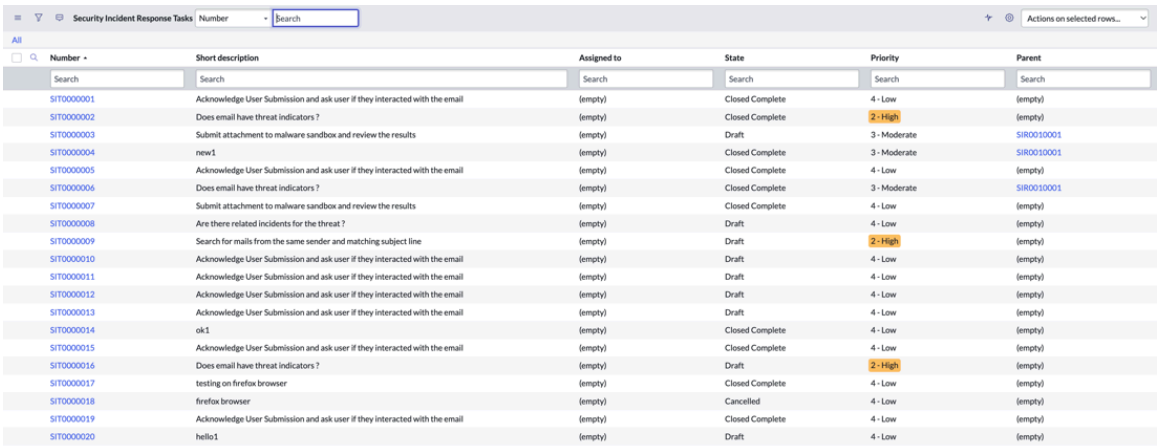
시작하기 전에
필요한 역할: sn_si.admin

이 태스크 정보
기본 목록이 거의 없기 때문에 응답 작업 관련 목록은 그룹화되지 않고 개별 관련 목록 항목으로 표시됩니다. 작업 공간에 있는 보안 인시던트 기록의 응답 작업 탭에서 응답 작업 관련 항목을 봅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 응답 작업 〉 모든 작업 표시.



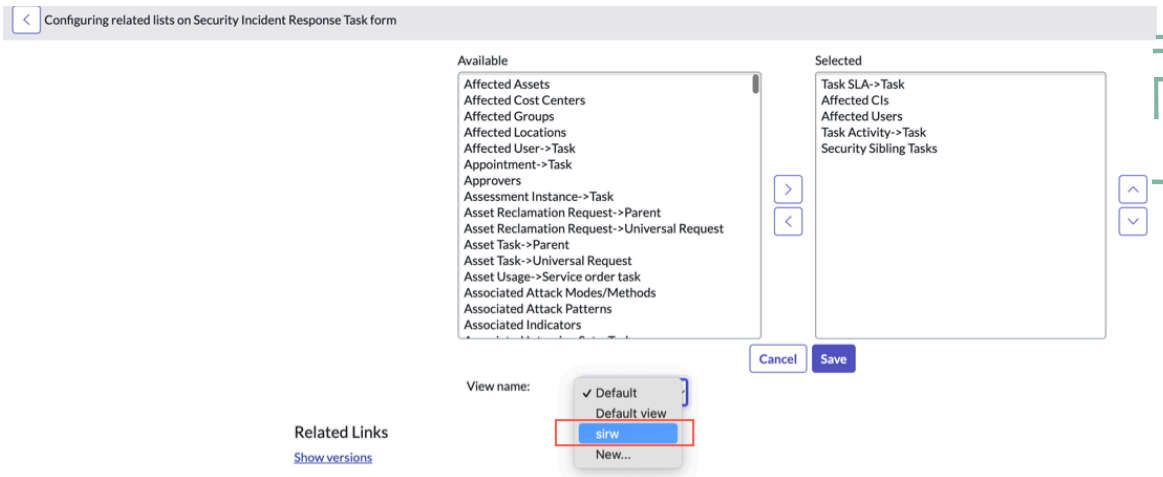
Number	Short description	Assigned to	State	Priority	Parent
SIT0000001	Acknowledge User Submission and ask user if they interacted with the email	(empty)	Closed Complete	4 - Low	(empty)
SIT0000002	Does email have threat indicators ?	(empty)	Closed Complete	2 - High	(empty)
SIT0000003	Submit attachment to malware sandbox and review the results	(empty)	Draft	3 - Moderate	SIR0010001
SIT0000004	new1	(empty)	Closed Complete	3 - Moderate	SIR0010001
SIT0000005	Acknowledge User Submission and ask user if they interacted with the email	(empty)	Closed Complete	4 - Low	(empty)
SIT0000006	Does email have threat indicators ?	(empty)	Closed Complete	3 - Moderate	SIR0010001
SIT0000007	Submit attachment to malware sandbox and review the results	(empty)	Closed Complete	4 - Low	(empty)
SIT0000008	Are there related incidents for the threat ?	(empty)	Draft	4 - Low	(empty)
SIT0000009	Search for mails from the same sender and matching subject line	(empty)	Draft	2 - High	(empty)
SIT0000010	Acknowledge User Submission and ask user if they interacted with the email	(empty)	Draft	4 - Low	(empty)
SIT0000011	Acknowledge User Submission and ask user if they interacted with the email	(empty)	Draft	4 - Low	(empty)
SIT0000012	Acknowledge User Submission and ask user if they interacted with the email	(empty)	Draft	4 - Low	(empty)
SIT0000013	Acknowledge User Submission and ask user if they interacted with the email	(empty)	Draft	4 - Low	(empty)
SIT0000014	ok1	(empty)	Closed Complete	4 - Low	(empty)
SIT0000015	Acknowledge User Submission and ask user if they interacted with the email	(empty)	Closed Complete	4 - Low	(empty)
SIT0000016	Does email have threat indicators ?	(empty)	Draft	2 - High	(empty)
SIT0000017	testing on firefox browser	(empty)	Closed Complete	4 - Low	(empty)
SIT0000018	firefox browser	(empty)	Cancelled	4 - Low	(empty)
SIT0000019	Acknowledge User Submission and ask user if they interacted with the email	(empty)	Closed Complete	4 - Low	(empty)
SIT0000020	hello1	(empty)	Draft	4 - Low	(empty)

2. 응답 작업 기록을 선택합니다.

3. 보안 인시던트 응답 작업 컨텍스트 메뉴를 마우스 오른쪽 버튼으로 클릭합니다.

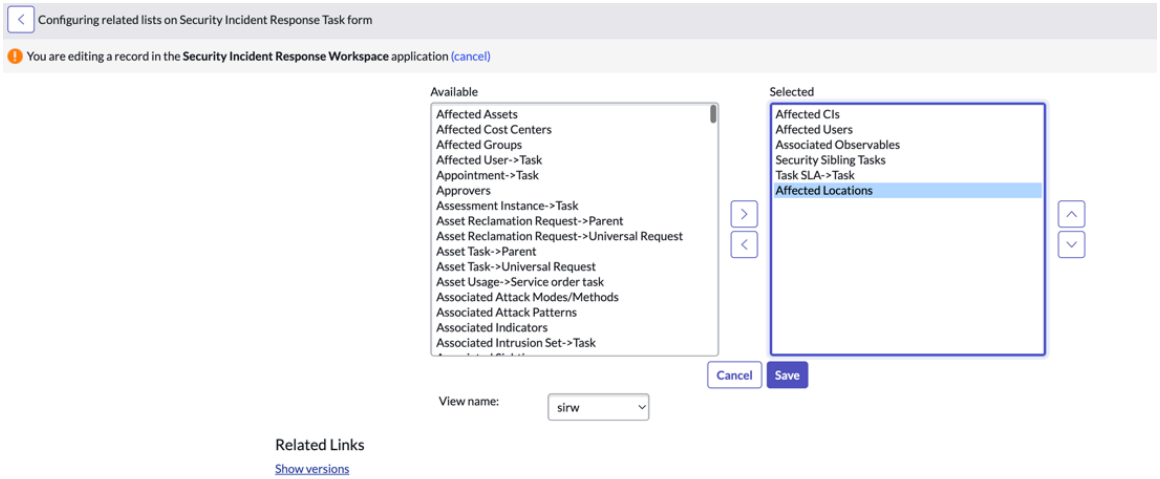
4. 다음으로 이동 구성 〉 관련 목록.
보안 응답 작업 관련 목록 구성 양식이 표시됩니다.

5. 뷰 이름으로 이동하여 **SIRW** 뷰를 선택합니다.

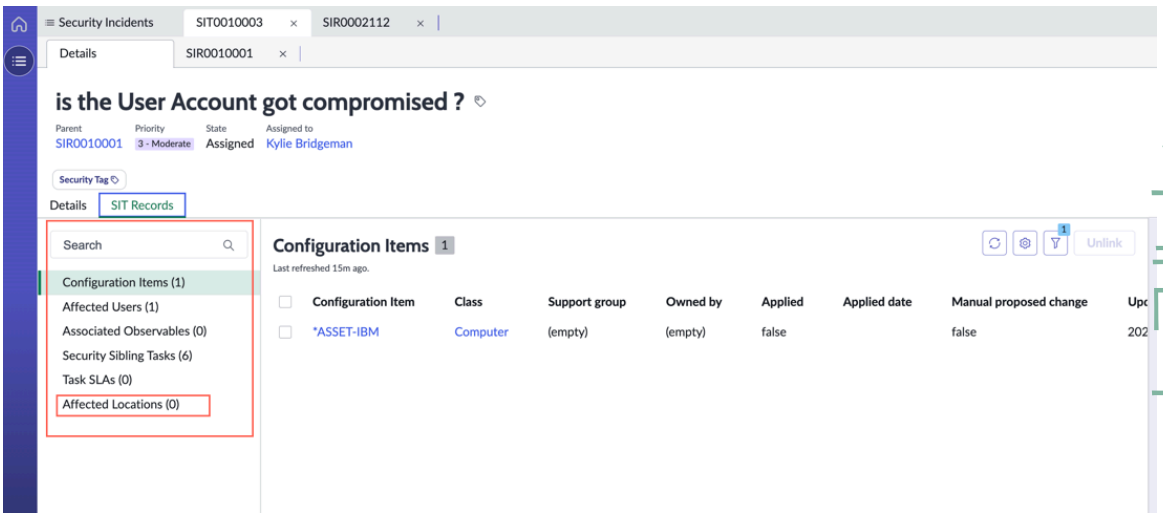


6. 슬러시버킷에서 원하는 관련 목록 필드를 선택합니다.
예: 영향을 받는 위치.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



7. 저장을 클릭합니다.
8. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간 〉 응답 작업 〉 **SIT** 기록.
   구성된 관련 목록(예: 선택한 영향을 받는 위치)이 SIT 기록 목록 내에 나열됩니다.



새 위험 점수 계산기 규칙 정의

새로운 위험 점수 계산기를 사용하여 보안 인시던트에 대한 투명한 인텔리전스 점수를 제공하는 사용자 정의 기준에 따라 보안 인시던트의 위험 점수를 정의하고 계산합니다. 보안 인시던트 기록의 위험 점수는 자동으로 계산됩니다.

시작하기 전에

필요한 역할: sn_si.admin.

sn_si_aw.activate_new_risk_score_calculator 시스템 속성을 true로 설정하여 새 위험 점수 계산기를 활성화합니다.

이 태스크 정보

사용자 정의 매개변수를 기반으로 생성된 보안 인시던트 기록에 대한 위험 점수를 정의합니다. 기본 시스템에는 하나의 위험 점수 규칙이 프로비저닝되며, 이에 따라 사용자 지정하고 활성화할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

- 기본적으로 새 위험 점수 계산기 규칙은 비활성 상태이며, 보안 인시던트의 위험 점수를 보려면 규칙을 활성화해야 합니다.
- 기본 시스템에서 사용할 수 있는 테이블 이외의 추가 관련 테이블에 대한 위험 점수를 계산하려면 다음 문서를 참조하십시오 추가 관련 테이블에 대한 위험 점수 계산기.

프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간 〉 관리.
2. 다음으로 이동 규칙 엔진 〉 위험 점수 계산기 규칙.
   위험 점수 계산기 규칙 페이지가 표시됩니다.

   주:

   - 기본 시스템의 일부로 위험 점수를 보거나 편집하거나 수정할 수 있는 미리 정의된 위험 점수 규칙 템플릿 하나가 제공됩니다. 그러나 미리 정의된 위험 점수 규칙 템플릿을 생성하거나 삭제할 수는 없습니다.
   - 변경한 내용은 새 보안 인시던트 또는 기존 보안 인시던트에 대한 업데이트에 적용됩니다. 과거 점수를 다시 작성하려면 점수 다시 계산 작업을 사용합니다.

3. 위험 점수 계산기 규칙을 선택합니다.
4. 양식에서 필드를 채웁니다.

필드	설명
이름	위험 점수 값의 이름입니다. 예를 들어, 위험 점수 계산기입니다.
전체 가중치(기준 작성기에서 적용 가능)	위험 규칙 내에서 이 필드의 가중치입니다. 이 필드는 편집할 수 없으며 활성화된 기준에 해당하는 가중치를 기준으로 시스템에서 계산한 전체 가중치를 표시합니다. 전체 가중치는 항상 100%여야 합니다.
설명	위험 점수 기록에 대한 설명입니다. 예를 들어, 미리 정의된 기준 점수의 가중치 합계를 기준으로 위험 점수를 계산합니다.
점수 산정 기준	보안 인시던트에 대한 점수 산정 기준을 나타냅니다. 다음 옵션을 사용하여 위험 점수 기준을 정의할 수 있습니다. ○ 기준 작성기: 이 옵션을 사용하여 위험 점수 계산에 기여하는 기준을 추가, 편집 또는 제거하고 사용 및 사용하지 않도록 설정하고 총 집계 가중치가 100%인지 확인합니다. ○ 스크립트 사용(고급): 스크립팅 기능은 위험 점수(0에서 100 사이의 정수 값)를 반환하는 사용자 지정 스크립트를 작성하는 고급 기능입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. 기준 작성기를 사용하여 점수 산정 기준을 정의하려면 다음 단계를 수행합니다.

> **주:**
> 기존 기준을 편집 또는 수정하거나 새 기준을 추가할 수 있습니다.

a. 새 기준을 추가하려면 +새 기준 작업을 선택합니다.

b. 기준을 설정할 테이블을 선택합니다.

> **주:**
> - 선택한 테이블이 보안 인시던트인 경우 위험 점수가 계산되는 보안 인시던트 기록에 조건이 적용됩니다. 선택한 테이블이 보안 인시던트가 아닌 경우 기록이 위험 점수가 계산되는 보안 인시던트와 관련된 경우에만 조건이 적용됩니다.
> - 보안 인시던트와 관련된 관계 수를 기준으로 점수를 정의하기 위해 추가 집계 유형이 추가됩니다.

c. 선택한 테이블의 유형 기준을 선택합니다.
유형 값은 선택한 테이블에 따라 필드 또는 집계 가 될 수 있습니다.

d. 선택한 테이블의 필드 기준을 선택합니다.
유형 값을 필드로 선택한 경우 필드 기준에 테이블과 관련된 필드 값이 표시됩니다. 유형 값을 집계로 선택한 경우 필드 기준에 테이블과 관련된 집계 값이 표시됩니다.

> **주:**
> 집계 형식은 카운트 값만 지원합니다.

예를 들어 테이블 기준을 보안 인시던트로 선택하면 유형 기준에 필드 옵션만 표시됩니다. 필드 기준에는 테이블과 관련된 모든 필드 값(심각도, 활성 등)이 표시됩니다. 마찬가지로 테이블 기준을 영향을 받는 사용자로 선택하면 유형 기준에 필드 및 집계 옵션이 모두 표시됩니다. 유형을 집계로 선택하면 필드 기준에 테이블과 관련된 집계 값(카운트)이 표시됩니다.

e. 0-100 사이의 기준 가중치 를 입력합니다.
모든 기준의 전체 가중치는 100%여야 합니다.

f. 기준의 이름과 간단한 설명을 입력합니다.

g. 점수 산정 기준을 사용하려면 점수 산정 기준 사용 확인란을 선택합니다.

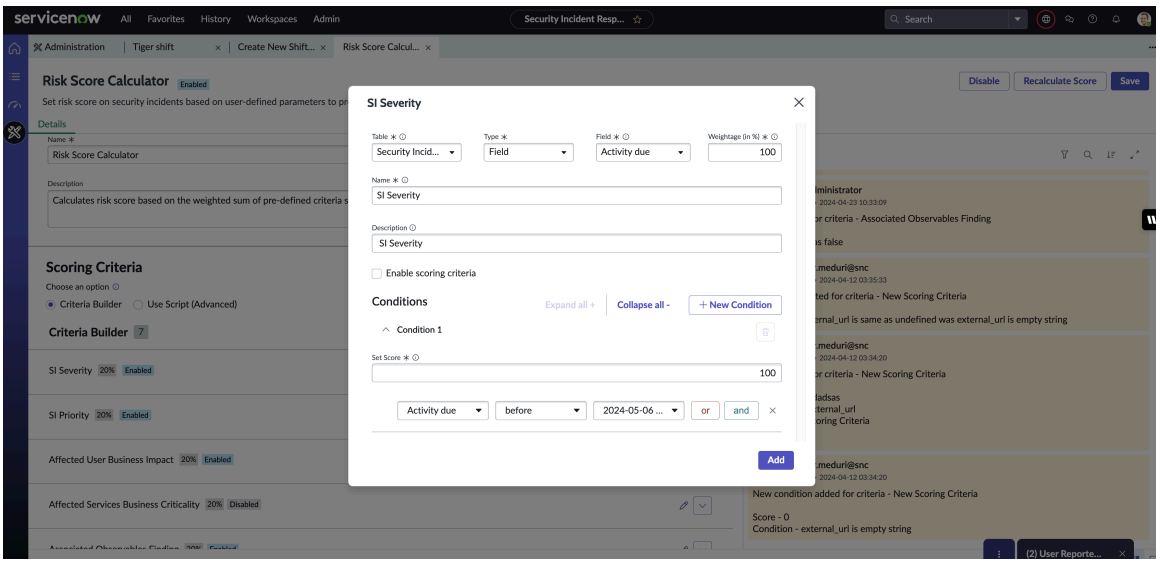
h. 조건을 정의하고 조건에 대한 점수를 설정합니다.

i. 새 조건 옵션을 사용하여 새 조건을 추가하고 기준 삭제 아이콘을 사용하여 기존 조건을 삭제할 수도 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

j. 추가를 선택하여 구성된 기준을 추가합니다.

기준 작성기를 사용한 점수 산정 기준



6. 위험 점수를 다시 계산하려면 점수 다시 계산 옵션을 선택합니다.

예를 들어 위험 점수 규칙이 변경된 경우입니다. 이 경우 과거에 위험 점수가 이미 계산된 보안 인시던트에 점수 산정 규칙을 다시 적용해야 합니다. 점수 다시 계산 작업을 사용하여 재계산 작업을 트리거합니다.

7. 확인을 선택합니다.

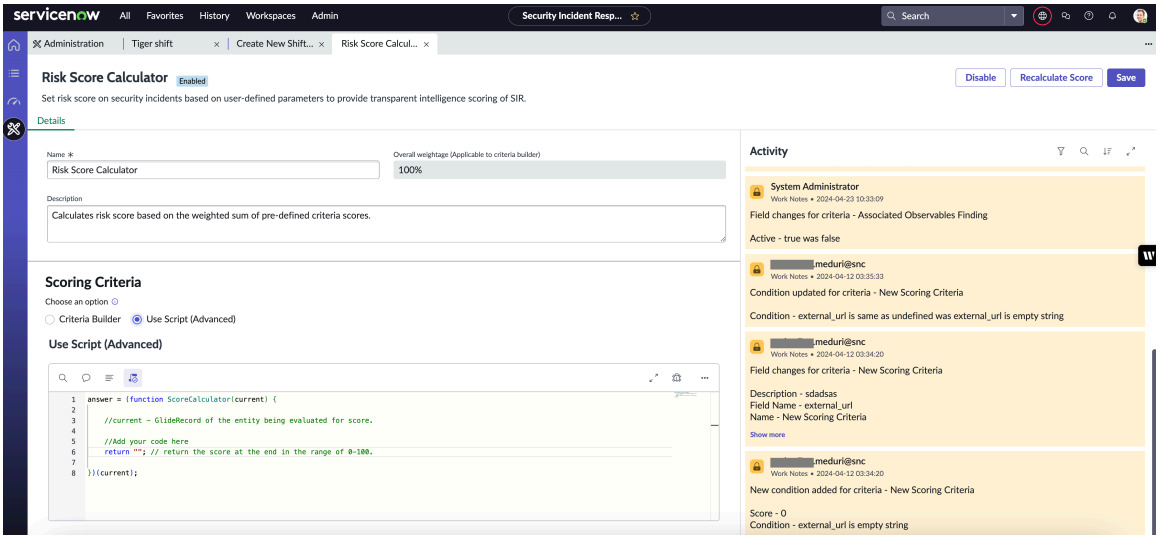
주:
이 작업을 트리거하면 프로세스가 백그라운드에서 실행되고 완료하는 데 몇 분 정도 걸립니다. 완료될 때까지 변경할 수 없습니다.

8. 스크립트 사용(고급) 옵션을 사용하여 점수 기준을 정의하려면 다음 단계를 수행합니다.

a. 이 미리 정의된 스크립트를 사용하여 위험 점수(0에서 100 사이의 정수 값)를 반환하는 사용자 지정 스크립트를 빌드합니다.
고급 스크립트 필드는 현재 매개변수를 사용하는 함수로 자동으로 채워지며 이 함수는 위험 점수(0에서 100 사이의 정수 값)를 반환해야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

스크립트를 사용한 점수 산정 기준(고급) 옵션



여기서 현재 매개변수는 위험 점수가 계산되는 엔터티(보안 인시던트)의 GlideRecord 객체입니다. 보안 인시던트의 경우 sn_si_incident 테이블의 GlideRecord에 해당합니다.

9. 위험 점수 계산기를 사용하지 않도록 설정하려면 사용 안 함을 선택합니다.
10. 저장을 선택합니다.

추가 관련 테이블에 대한 위험 점수 계산기

위험 점수 계산기는 사용자 정의 기준에 따라 보안 인시던트의 위험 점수를 계산하기 위해 기본 시스템의 일부로 하나의 위험 점수 규칙과 함께 프로비저닝됩니다. 그러나 추가 관련 테이블을 사용자 지정하고 포함하여 위험 점수를 계산할 수 있습니다.

시작하기 전에

필요한 역할: sn_si.admin.

프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 인시던트 〉 모든 인시던트 표시.
2. 보안 인시던트 기록을 선택합니다.
3. 보안 인시던트 번호 옆에 있는 추가 작업 옵션을 선택합니다.
4. 이동 구성 〉 관련 목록.
5. 뷰 이름으로 이동하여 위험 점수 계산기를 선택합니다.
   뷰를 선택한 후 슬러시버킷에서 추가하려는 필수 관련 목록을 선택합니다. 예를 들어, 연관된 사이팅입니다.
6. 저장을 선택합니다.
   위험 점수를 계산할 새 관련 목록 또는 테이블을 성공적으로 추가했습니다.

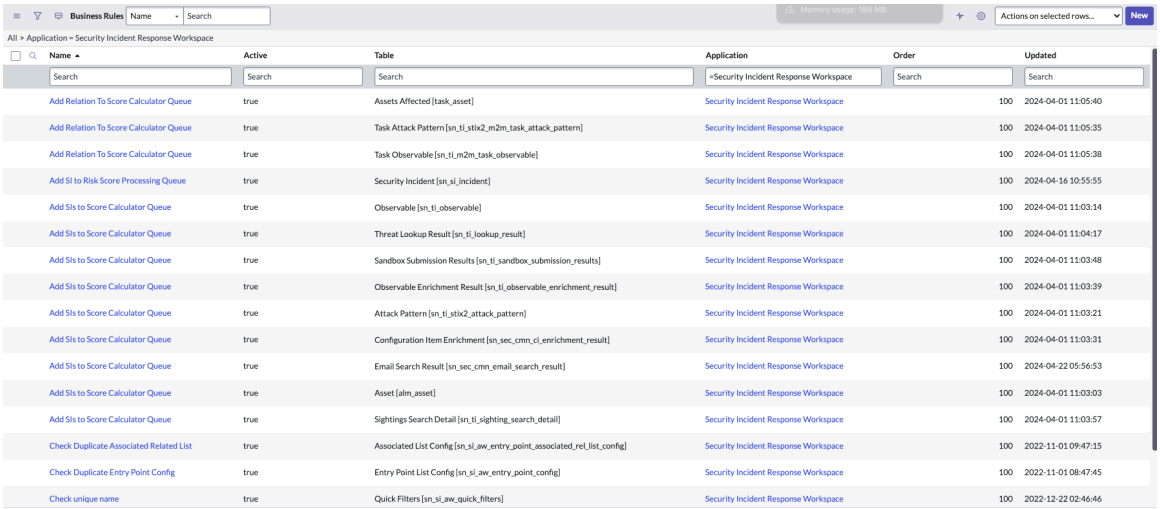
> **중요사항:**
> 새로 생성된 관련 목록으로 새 기준이 있는 보안 인시던트에 대한 위험 점수를 계산하려면 관련 목록의 기본 테이블에서 비즈니스 규칙을 정의해야 합니다.

7. 다음으로 이동 모두 〉 시스템 정의 〉 비즈니스 규칙.
   다음 두 비즈니스 규칙을 참조로 사용하여 고유한 비즈니스 규칙을 만들 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 점수 계산기 큐에 보안 인시던트(SI) 추가
- 점수 계산기 큐에 관계 추가(m2m 테이블에 적용 가능)

비즈니스 규칙



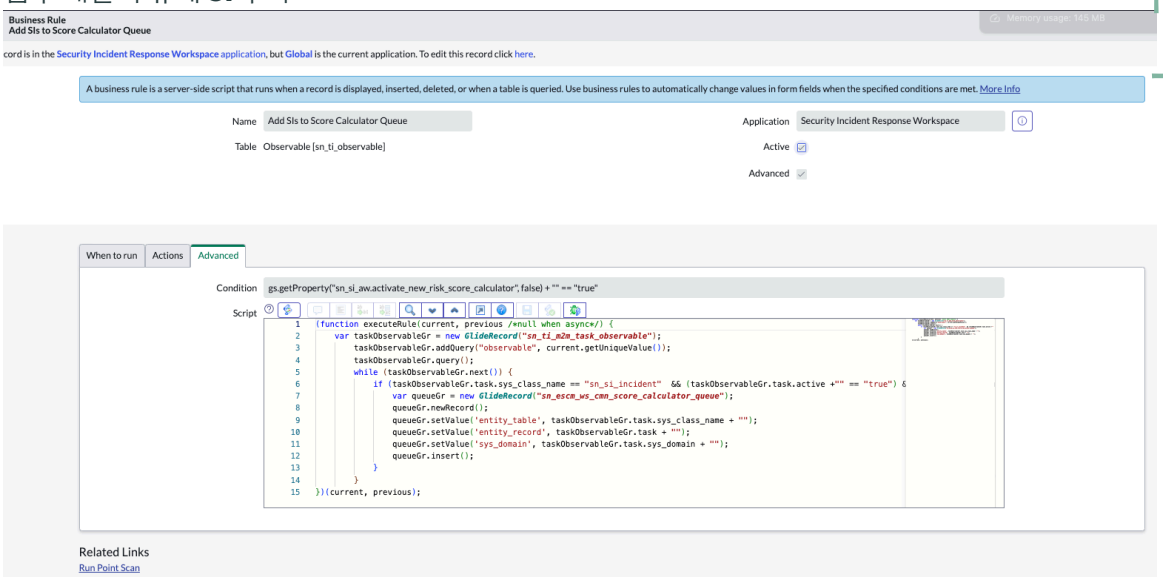
Name	Active	Table	Application	Order	Updated
Add Relation To Score Calculator Queue	true	Assets Affected [task_asset]	Security Incident Response Workspace	100	2024-04-01 11:05:40
Add Relation To Score Calculator Queue	true	Task Attack Pattern [sn_ti_stix2_m2m_task_attack_pattern]	Security Incident Response Workspace	100	2024-04-01 11:05:35
Add Relation To Score Calculator Queue	true	Task Observable [sn_ti_m2m_task_observable]	Security Incident Response Workspace	100	2024-04-01 11:05:38
Add SI to Risk Score Processing Queue	true	Security Incident [sn_si_incident]	Security Incident Response Workspace	100	2024-04-16 10:55:55
Add SIs to Score Calculator Queue	true	Observable [sn_ti_observable]	Security Incident Response Workspace	100	2024-04-01 11:03:14
Add SIs to Score Calculator Queue	true	Threat Lookup Result [sn_ti_lookup_result]	Security Incident Response Workspace	100	2024-04-01 11:04:17
Add SIs to Score Calculator Queue	true	Sandbox Submission Results [sn_ti_sandbox_submission_results]	Security Incident Response Workspace	100	2024-04-01 11:03:48
Add SIs to Score Calculator Queue	true	Observable Enrichment Result [sn_ti_observable_enrichment_result]	Security Incident Response Workspace	100	2024-04-01 11:03:39
Add SIs to Score Calculator Queue	true	Attack Pattern [sn_ti_stix2_attack_pattern]	Security Incident Response Workspace	100	2024-04-01 11:03:21
Add SIs to Score Calculator Queue	true	Configuration Item Enrichment [sn_sec_cmn_ci_enrichment_result]	Security Incident Response Workspace	100	2024-04-01 11:03:31
Add SIs to Score Calculator Queue	true	Email Search Result [sn_sec_cmn_email_search_result]	Security Incident Response Workspace	100	2024-04-22 05:56:53
Add SIs to Score Calculator Queue	true	Asset [alm_asset]	Security Incident Response Workspace	100	2024-04-01 11:03:03
Add SIs to Score Calculator Queue	true	Sightings Search Detail [sn_ti_sighting_search_detail]	Security Incident Response Workspace	100	2024-04-01 11:03:57
Check Duplicate Associated Related List	true	Associated List Config [sn_si_aw_entry_point_associated_rel_list_config]	Security Incident Response Workspace	100	2022-11-01 09:47:15
Check Duplicate Entry Point Config	true	Entry Point List Config [sn_si_aw_entry_point_config]	Security Incident Response Workspace	100	2022-11-01 08:47:45
Check unique name	true	Quick Filters [sn_si_aw_quick_filters]	Security Incident Response Workspace	100	2022-12-22 02:46:46

8. 예를 들어, 연결된 옵저버블 기준이 작동하도록 하기 위해 두 가지 비즈니스 규칙을 정의했습니다.

첫 번째는 점수 계산기 큐에 **SI** 추가 비즈니스 규칙입니다.

예를 들어 새 보안 인시던트가 생성되고 옵저버블(Observables[sn_ti_observable]) 테이블에 연결됩니다. 위협 조회 후 옵저버블이 악성으로 확인되었습니다. 그런 다음 이 악성 옵저버블과 연결된 모든 보안 인시던트를 큐에 추가하여 보안 인시던트의 위험 점수를 다시 계산해야 합니다.

점수 계산기 큐에 **SI** 추가



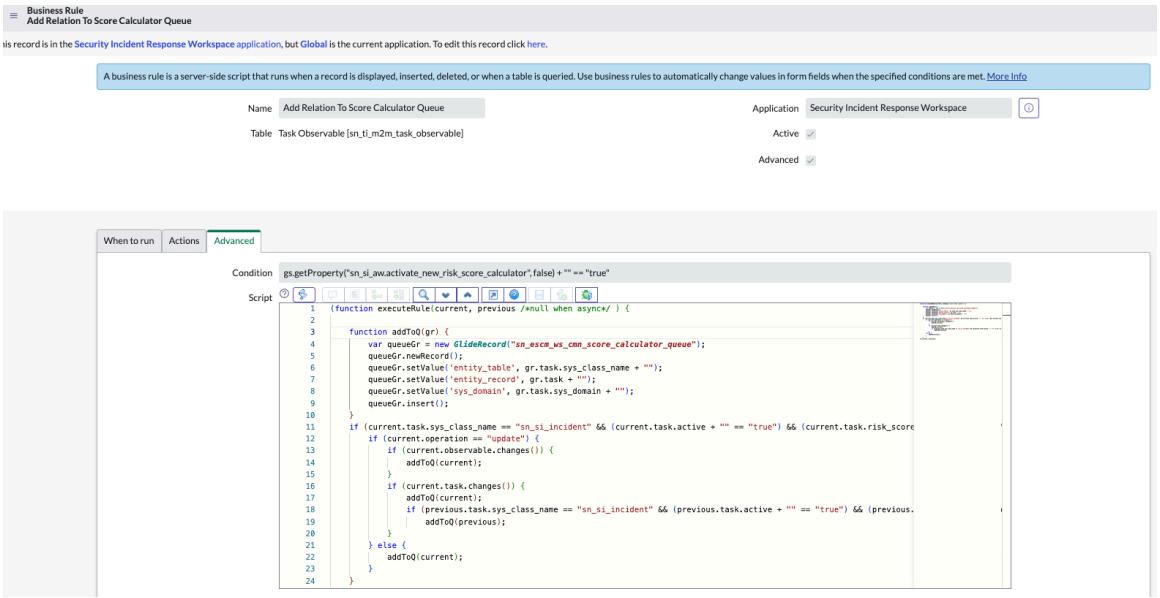
두 번째는 점수 계산기 큐에 관계 추가 비즈니스 규칙입니다.

예를 들어 새 보안 인시던트가 생성되거나 삭제되고 옵저버블(## #### [sn_ti_m2m_task_observable]) 테이블과 연결됩니다. 따라서 보안 인시던트의 연결에 변화가

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

있습니다. 그런 다음 해당 보안 인시던트를 큐에 추가하여 보안 인시던트의 위험 점수를 다시 계산해야 합니다.

점수 계산기 큐에 관계 추가



교대조 핸드오버 구성

다음 교대조 분석가에게 완전한 교대조 정보를 제공하도록 교대조 핸드오버 설정을 구성합니다.

교대조 핸드오버 템플릿 구성

관리자는 교대조 소유자가 교대조 핸드오버 기록을 생성하고 다음 교대조 팀에 전달할 수 있도록 다양한 교대조 핸드오버 템플릿을 정의하고 구성할 수 있습니다.

시작하기 전에
필요한 역할:

- sn_escm_sh.shift_admin
- sn_si.admin은 sn_escm_sh.shift_admin 역할을 상속합니다.

이 태스크 정보
교대조 핸드오버 템플릿을 구성하기 위해 관리자는 새 교대조 핸드오버 템플릿을 만들거나 기본 시스템에서 샘플 교대조 템플릿 이라는 이름으로 기존 템플릿을 열고 요구 사항에 따라 상세 정보와 섹션을 수정합니다.

교대조 소유자는 구성된 템플릿을 사용하여 교대조 핸드오버 로그 기록을 생성할 수 있으며, 그런 다음 교대조 핸드오버 보고서가 다음 활성 교대조 소유자 및 팀과 공유됩니다.

주:
교대조 소유자가 핸드오버 로그 기록을 생성하려면 활성 교대조 핸드오버 템플릿만 표시됩니다.

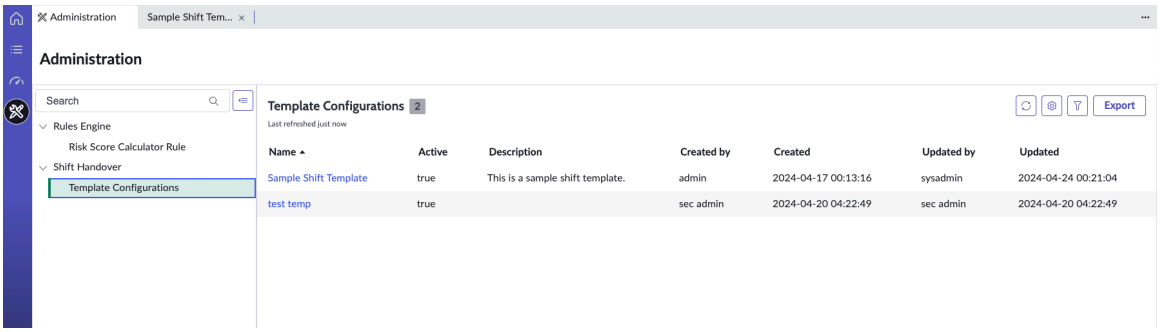
프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간 〉 관리.
2. 다음으로 이동 교대조 핸드오버 〉 템플릿 구성.
   템플릿 구성 페이지가 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
기본 시스템의 일부로, 교대조 핸드오버 템플릿을 보거나 편집하거나 수정할 수 있도록 미리 정의된 하나의 교대조 핸드오버 템플릿 구성이 제공됩니다. 그러나 미리 정의된 교대조 핸드오버 템플릿 구성을 만들거나 삭제할 수는 없습니다.

교대조 핸드오버 템플릿 구성



3. 새 교대조 핸드오버 템플릿을 생성하려면 새로 만들기를 선택합니다.

4. 상세 정보 양식의 필드에 내용을 입력합니다.

새 교대조 핸드오버 템플릿 생성

필드	설명
이름	교대조 핸드오버 템플릿의 이름입니다. 예를 들면 SIR 템플릿입니다.
애플리케이션	교대조 핸드오버 템플릿을 생성할 애플리케이션의 이름입니다. 예를 들어 보안 인시던트 응답 작업 공간입니다.
활성	교대조 핸드오버 템플릿이 활성 상태인지 여부를 나타내는 옵션입니다. 교대조 핸드오버 템플릿을 활성화하려면 이 옵션을 활성화합니다.
설명	교대조 핸드오버 템플릿에 대한 설명입니다.
기록 멘션 구성	이 필드를 사용하여 서식 있는 텍스트 편집기(RTE)의 기록 멘션 상세 정보를 구성합니다. 입력은 다음 필드가 있는 JSON 객체의 배열입니다. ○ *`sourceTable`*: 소스 테이블의 이름입니다. ○ *`label`*: 표시할 레이블의 이름입니다. ○ *`filterCondition`*: 필터링을 위한 인코딩된 쿼리입니다. 동일한 테이블에 대해 여러 쿼리를 추가하여 값을 동적으로 검색할 수 있습니다. 이러한 값은 교대조 핸드오버 기록이 게시될 때 또는 교대조의 시작 날짜 및/또는 종료 날짜를 기준으로 업데이트됩니다. 예를 들어 우선순위별 보안 인시던트 기록 수, 상태별 보안 인시던트 기록 수 등이 있습니다. 날짜 범위를 지정하기 위해 쿼리에서 {start_date} 및 {end_date} 인수를 사용할 수 있습니다. 예: `"filterCondition": "active=true^sys_created_on>=${start_date}^sys_created_on<=${end_date}"` ○ *##*: 패턴을 쿼리할 필드를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

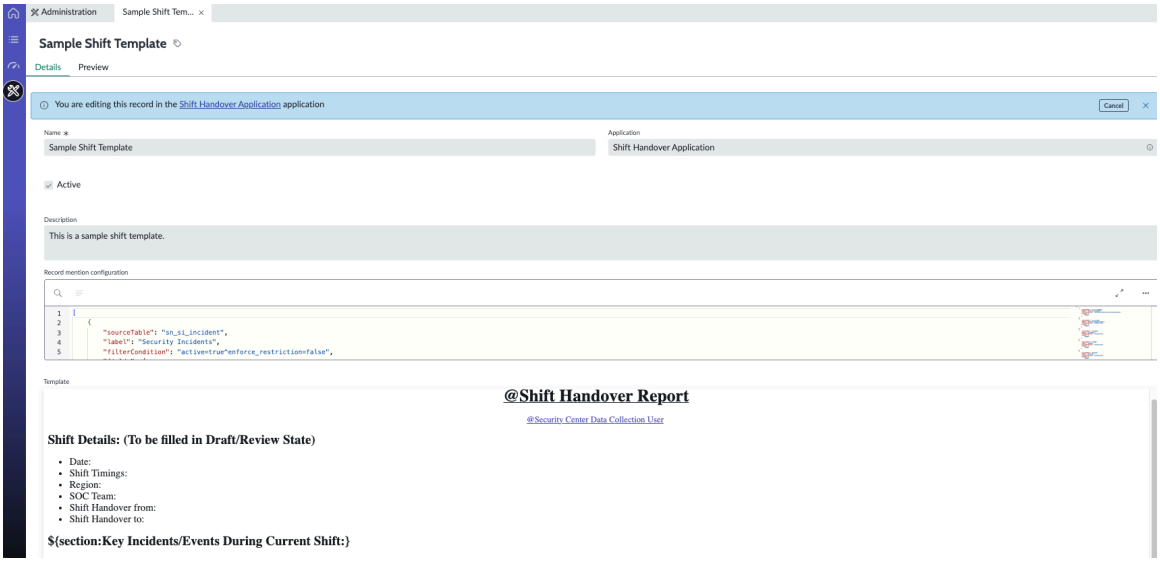
필드	설명
	기록 멘션 구성 필드에 복사하여 붙여넣을 수 있는 샘플 구성입니다. `[ { "sourceTable": "incident", "label": "Incidents active", "filterCondition": "active=true", "fields": [ "number" ] } { "sourceTable": "incident", "label": "Active incidents created after selected date", "filterCondition": "active=true^sys_created_on>=${start_date}", "fields": [ "number" ] } ]` 샘플 구성을 복사하려면 상황별 지원 창에서 클립보드에 복사 작업을 사용합니다. 그런 다음 요구 사항에 따라 추가 수정을 수행할 수 있습니다.

템플릿	섹션을 사용하여 교대조 핸드오버 템플릿을 생성합니다. 분석가가 템플릿을 기반으로 교대조 핸드오버 로그 기록에 기여하려면 섹션이 하나 이상 있어야 합니다.
	템플릿은 적절한 섹션에 정적 텍스트, 이미지 등을 포함할 수 있습니다. 이미지를 복사하여 템플릿 필드에 직접 붙여넣을 수 있습니다. 다음 코드를 사용하여 템플릿에 섹션을 만들 수 있습니다.
	`${section:Section Label}`
	예제:
	`${section:Key Incidents/Events During Current Shift}`
	`${section:Incidents/Events to Monitor or Follow Up}`
	`${section:System/Infrastructure Updates}`
	`${section:Next Steps for Incoming Shift}`
	`${section:References}`
	주:
	자세한 내용은 오른쪽 창의 상황별 지원을 참조하십시오.

5. 기존 교대조 핸드오버 템플릿을 사용하고 수정하려면 샘플 교대조 템플릿을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

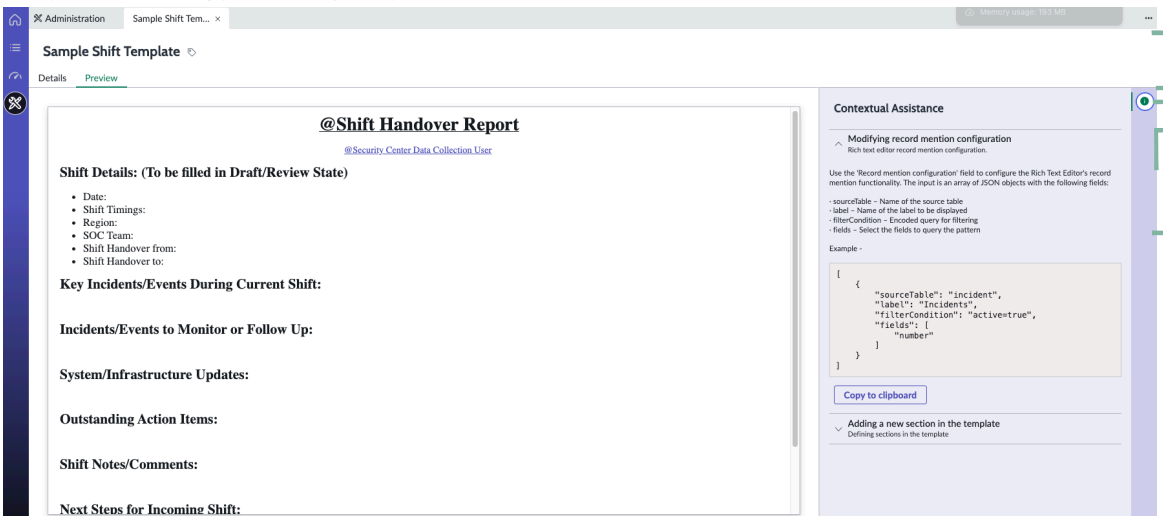
교대조 핸드오버 템플릿



6. 요구 사항에 따라 교대조 핸드오버 템플릿을 업데이트합니다.
7. 미리 보기를 선택하여 교대조 핸드오버 템플릿의 런타임 미리 보기를 확인합니다.

   보고서는 교대조 핸드오버 템플릿 구성을 기반으로 미리 보기를 생성합니다.

교대조 핸드오버 템플릿 미리 보기



8. 저장을 선택하여 교대조 핸드오버 템플릿을 저장합니다.

다음에 수행할 작업
목록 뷰에서 교대조 핸드오버 기록을 관리하고 교대조 핸드오버 기록 생성, 편집, 복사 또는 삭제와 같은 작업을 수행하는 방법에 대한 자세한 내용은 문서를 참조하십시오 교대조 핸드오버 기록 관리.

다음을 통해 **shifts** 생성 보안 인시던트 응답 작업 공간

S HIFT HAndover R코드를 구성할 때 사용할 교대조 보안 인시던트 응답 작업 공간 를 생성합니다.

시작하기 전에
필요한 역할:

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- sn_escm_sh.shift_admin
- sn_si.admin은 sn_escm_sh.shift_admin 역할을 상속합니다.

프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간 〉 관리.
2. 다음으로 이동 교대조 핸드오버 〉 교대조 시간 구성.
   교대조 시간 구성 페이지에 기존의 모든 교대조가 표시됩니다.
3. 새로 만들기를 선택합니다.
4. 교대조 필드에 이름을입력합니다.
5. 시작 시간 및 종료 시간 필드에 교대조의 시작 및 종료 시간을 입력합니다.

   주:
   시작 시간과 종료 시간은 현재 사용자가 구성한 시간대에 있습니다.

6. 저장을 선택합니다.

보안 인시던트 응답 **Conference** C모든 통합

보안 인시던트 응답 컨퍼런스 회의 통합을 사용하면 분석가, 관리자 및 영향을 받는 사용자에 대한 컨퍼런스 회의 및 채팅을 관리하고 시작할 수 있습니다.

전화 회의 기능을 사용하면 보안 인시던트 응답 고객 및 동료 에이전트와 공동 작업하여 통화 중에 보안 인시던트를 해결할 수 있습니다. 그룹 채팅을 사용하여 공동 작업할 수도 있습니다.

Microsoft Teams, Cisco Webex 또는 Zoom 회의와 같은 외부 공급업체 통신 채널을 사용하여 전화 회의를 시작할 수 있습니다. 채팅을 사용하여 공동 작업하려면 SIR 애플리케이션의 사이드바 채팅을 사용합니다.

주요 기능

보안 인시던트 응답 호출 공동 작업은 다음과 같은 주요 기능을 제공합니다.

- SIR 관리자/분석가는 보안 인시던트에서 직접 Microsoft Teams, Cisco Webex 또는 Zoom 전화 회의를 시작할 수 있습니다.
- SIR 관리자/분석가는 SIR 애플리케이션에서 직접 채팅을 시작할 수 있습니다.
- 전화 또는 채팅에 추가 참가자를 초대합니다.
- 통화 기록 및 채팅 상세 정보를 확인합니다.
- 이메일 및 Microsoft Teams 채팅을 통해 참가자에게 초대를 보냅니다.

컨퍼런스 회의 사용자 및 그룹 관리

관리자는 회의에 추가할 사용자 및 그룹의 미리 정의된 목록을 표시하도록 전화 회의 설정을 구성할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.admin

프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간 〉 관리.
2. 전화 회의를 선택한 다음 통화 구성을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. Call Configurations(통화 컨피그레이션) 페이지에서 **Conference Call** Config(컨퍼런스 회의 컨피그레이션)를 선택합니다.
   미리 정의된 사용자 및 그룹 목록을 구성할 수 있는 구성 페이지가 표시됩니다.
4. 상세 정보 양식의 필드에 내용을 입력합니다.

필드	설명
이름	전화 회의 구성의 이름입니다.
사용자 자동 채우기	전화 회의를 위해 구성된 사용자를 자동으로 채우는 옵션입니다. 이 옵션을 선택하면 구성된 사용자 및 그룹이 전화 회의에 추가됩니다. **주:** 통화를 시작할 때도 사용자/그룹을 추가하거나 제거할 수 있습니다.
영향을 받는 사용자 표시	통화에 추가할 영향을 받는 사용자를 표시하는 옵션입니다.
할당 그룹 사용자 표시	통화에 추가할 할당 그룹 사용자를 표시하는 옵션입니다.
기본 그룹	통화에 추가할 기본 그룹을 추가하는 옵션입니다.
기본 사용자	통화에 추가할 기본 사용자를 추가하는 옵션입니다.

5. 저장을 선택하여 컨퍼런스 회의 구성을 저장합니다.

SIR을 외부 공급업체 통신 채널과 통합

Microsoft Teams, Zoom 및 Cisco Webex 등의 외부 공급업체 통신 채널과 SIR 전화 회의를 통합하면 보안 인시던트에서 직접 통화를 관리하고 시작할 수 있습니다.

주요 기능

- 모든 보안 인시던트에서 직접 컨퍼런스 회의를 시작하고 종료합니다.
- 전화 회의에서 참가자를 추가 또는 제거합니다.
- 추가 분석을 위해 회의 기간 및 참석자와 같은 회의 상세 정보를 추적하고 보고합니다.

필수 구성요소

ServiceNow 인스턴스에 다음 통합 허브 플러그인을 설치했는지 확인하십시오.

- 알림 플러그인(com.snc.notify) 자세한 내용은 Configuring Notify 문서를 참조하십시오.
- 구성 가능한 작업 공간에 대한 알림 UI 구성요소
- Microsoft Teams를 통신 채널로 통합하려면 다음을 수행합니다.
  - Microsoft Teams Communications 스포크 플러그인(sn_msteams_com_spk).
  - Azure Active Directory sn_now_azure(사용자 매핑 플러그인).
- Zoom을 커뮤니케이션 채널로 통합하는 경우:

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- Zoom 스포크(sn_zoom_spoke)
- Zoom에 알림(sn_notify_zoom)

- Cisco Webex를 통신 채널로 통합하려면:
  - Cisco Webex 커넥터(sn_notify_webex) 알림
  - Cisco Webex Teams 스포크(sn_cisco_teams_spk)

자세한 내용은 Request Integration Hub 문서를 참조하십시오.

구성

사용하려는 통신 채널에 대해 다음 구성을 수행합니다.

- 알림 통신 채널을 사용하여 전화 회의 Cisco Webex 통합을 구성하려면 다음을 참조하십시오 Configure Notify Cisco Webex Connector.
- 알림 통신 채널을 사용하여 전화 회의 Zoom 통합을 구성하려면 문서를 참조하십시오 Configure Notify Zoom connector in Notify.
- 미리 구성된 앱을 사용하여 컨퍼런스 회의 Microsoft Teams 통합을 구성하려면 문서를 참조하십시오 Integrate Notify connector pre-published app with Microsoft Teams.
- 자체 구성된 앱을 사용하여 컨퍼런스 회의 Microsoft Teams 통합을 구성하려면 문서를 참조하십시오 Integrating Notify connector self-configured app with Microsoft Teams.

에서 보고서 템플릿 구성 보안 인시던트 응답

분석 및 공유를 위한 인시던트 요약 또는 실행 요약을 생성하는 데 사용할 수 있는 보고서 템플릿을 생성할 수 있습니다.

보고서 템플릿 기능을 사용하여 보안 인시던트 응답 인시던트의 분석가 수준 또는 임원 수준 요약을 제공하는 보고서를 생성하는 보고서 템플릿을 생성합니다. 다양한 인시던트 필드를 사용하여 요구 사항에 따라 보고서의 형식을 지정하고 구성할 수 있습니다.

다음 표에서는 기본 시스템 내에서 제공되는 보고서 템플릿에 대해 설명합니다.

보안 인시던트 응답의 보고서 템플릿

이름	설명
분석가 상태 보고	분석가를 위해 보안 인시던트에 대한 전체 정보를 제공합니다.
실무 요약	관리에 대한 보안 인시던트 상태에 대한 개요를 제공합니다.

주:
기본적으로 이러한 보고서는 초안 상태이며 읽기 전용 모드입니다. 이러한 기본 템플릿을 다시 사용하여 보고서 템플릿을 만들고 게시해야 합니다.

에서 보고서 템플릿 생성 보안 인시던트 응답

인시던트에 대한 분석가 요약 또는 실무 요약을 위한 새 보고서 템플릿을 생성합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_si.admin

프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간 〉 관리.
2. 보고서, 보고서 템플릿을 차례로 선택합니다.
   기본 시스템에서 사용할 수 있는 모든 템플릿이 포함된 보고서 템플릿 페이지가 나타납니다.
3. 새로 만들기를 선택합니다.
   템플릿의 상세 정보 페이지를 표시합니다.
4. 템플릿의 이름 및 설명을 입력합니다.
5. 저장을 선택합니다.
6. 콘텐츠 탭을 선택합니다.
   빈 보고서가 있는 템플릿의 콘텐츠 페이지를 표시합니다.
7. 확장을 선택하고 템플릿 본문에 원하는 필드를 삽입합니다.
   - 공통 **SIR** 필드: 인시던트에 가장 많이 사용되는 필드 목록입니다.
   - 모든 **SIR** 필드: 인시던트와 관련된 모든 필드입니다. 예를 들어, 인시던트 보고서를 생성하는 중에 간단한 설명이라는 필드를 추가하려면 모든 SIR 필드에서 해당 필드를 선택할 수 있습니다. 간단한 설명 필드가 보고서 템플릿에 변수로 추가됩니다. 분석가에 대한 보고서를 생성할 때 인시던트가 보고서에 표시되는 경우의 짧은 설명입니다.
   - 관련 기록: 특정 인시던트의 관련 기록입니다. 예를 들어 보고서에 연결된 옵저버블을 추가하려면 보고서 템플릿에 추가할 수 있습니다. 이러한 관련 기록은 테이블 형식으로 표시됩니다
   - 스크립트: 보고서의 날짜 및 시간을 추가하려면 보고서 템플릿에 현재 날짜 시간 스크립트를 추가할 수 있습니다. 이렇게 하면 보고서에 보고서 생성 날짜 및 시간이 추가됩니다.
   -
8. 내용 저장을 선택하여 보고서 템플릿의 내용을 저장합니다.
9. 미리 보기를 선택하여 보고서 형식을 미리 봅니다.

   보고서 템플릿에 필요한 모든 필드를 추가한 후 보고서 템플릿을 게시해야 합니다.

10. 게시를 선택하여 템플릿을 게시합니다.

    보고서 템플릿을 게시할 것인지 여부를 확인하는 메시지가 표시됩니다.

11. 옵션: 추가 작업 아이콘을 선택한 다음, 삭제를 선택하여 보고서 템플릿을 삭제합니다.

보고서의 시스템 속성

보고서의 시스템 속성은 보안 인시던트 응답 아래에 설명되어 있습니다.

보고서의 시스템 속성

속성	설명	값
sn_si.sn_si_incident.load_all_records	템플릿에서 생성한 보고서의 목록에 대한 모든 기록을 로드합니다. 예 - 모든 기록을 로드합니다. 아니오 - sn_si.sn_si_incident.reporting_list_records_count	아니오

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보고서의 시스템 속성

속성	설명	값
	속성으로 정의된 특정 수의 기록을 로드합니다.	
sn_si.sn_si_incident.max_list_columns_allowed	보고서 PDF에서 목록을 렌더링할 때 추가할 수 있는 열 수를 제한합니다. 이렇게 하면 뷰의 시작부터 허용된 제한까지의 열이 사용됩니다.	5
sn_si.sn_si_incident.report_default_style_object	이 속성을 사용하여 자유 양식 필드, 왼쪽 패널, 보고서 목록의 CSS를 제어합니다.	(JSON 객체)
sn_si.sn_si_incident.reporting_list_records_count	보고서 편집기에 특정 수의 기록을 로드합니다.	200
sn_si_reporting_email_template_sn_si_incident	공유 보고서에 사용할 SIR(sn_si_incident) 테이블에 대한 이메일 클라이언트 템플릿의 시스템 ID입니다.	9ce97ae6434612104168 96ed3ab8f258
sn_si.sn_si_incident.ctx_menu_field_header	필드 헤더	sn_si_incident_report_field_header,sn_si_incident_
sn_si.sn_si_incident.defang_record_list_urls	목록에서 URL을 제거할지 여부를 제어합니다.	아니오
sn_si.sn_si_incident.reporting_dot_walk_tables	보고서에서 닷워킹에 사용할 수 있는 테이블 목록입니다.	(JSON 객체)

에서 보고서 템플릿 복제 보안 인시던트 응답

보고서 템플릿을 복제하여 기존 템플릿을 편집하거나 재사용하여 새 템플릿을 생성합니다.

시작하기 전에

주:
실무 요약 및 분석가 상태 보고 템플릿의 사본을 만들어 재사용해야 합니다.

실무 요약 및 분석가 상태 보고를 재사용하려면 이러한 사본을 생성한 다음

필요한 역할: sn_si.admin

프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간 〉 관리.
2. 보고서, 보고서 템플릿을 차례로 선택합니다.
   기본 시스템에서 사용할 수 있는 모든 템플릿이 포함된 보고서 템플릿 페이지가 나타납니다.
3. 템플릿을 선택합니다.
4. 복제를 선택합니다.

결과
선택한 템플릿의 컨텐츠가 복제되고 선택한 템플릿의 복사본이 템플릿 목록에서 사용 가능합니다. 중복 템플릿이 초안 상태입니다. 컨텐츠를 사용자 지정한 다음 필요에 따라 템플릿 이름을 바꿀 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 수행할 작업
에서 보고서 템플릿 편집 보안 인시던트 응답

에서 보고서 템플릿 편집 보안 인시던트 응답

보고서 템플릿을 편집하여 기존 템플릿을 재사용하여 새 템플릿을 만듭니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간 〉 관리.
2. 보고서, 보고서 템플릿을 차례로 선택합니다.
   기본 시스템에서 사용할 수 있는 모든 템플릿이 포함된 보고서 템플릿 페이지가 나타납니다.
3. 템플릿을 선택합니다.
   편집 모드에서 템플릿의 상세 정보 탭을 표시합니다.
4. 템플릿의 이름과 설명을 업데이트합니다.
5. 저장을 선택합니다.
6. 콘텐츠 탭을 선택합니다.
   빈 보고서가 있는 템플릿의 콘텐츠 페이지를 표시합니다.
7. 확장을 선택하고 원하는 필드를 삽입/제거합니다.
   - 공통 **SIR** 필드: 인시던트에 가장 많이 사용되는 필드 목록입니다.
   - 모든 **SIR** 필드: 인시던트와 관련된 모든 필드입니다. 예를 들어, 인시던트 보고서를 생성하는 중에 간단한 설명이라는 필드를 추가하려면 모든 SIR 필드에서 해당 필드를 선택할 수 있습니다. 간단한 설명 필드가 보고서 템플릿에 변수로 추가됩니다. 분석가에 대한 보고서를 생성할 때 인시던트가 보고서에 표시되는 경우의 짧은 설명입니다.
   - 관련 기록: 특정 인시던트의 관련 기록입니다. 예를 들어 보고서에 연결된 옵저버블을 추가하려면 보고서 템플릿에 추가할 수 있습니다. 이러한 관련 기록은 테이블 형식으로 표시됩니다
   - 스크립트: 보고서의 날짜 및 시간을 추가하려면 보고서 템플릿에 현재 날짜 시간 스크립트를 추가할 수 있습니다. 이렇게 하면 보고서에 보고서 생성 날짜 및 시간이 추가됩니다.
8. 내용 저장을 선택하여 보고서 템플릿의 내용을 저장합니다.
9. 미리 보기를 선택하여 보고서 형식을 미리 봅니다.

   보고서 템플릿에 필요한 모든 필드를 추가한 후 보고서 템플릿을 게시해야 합니다.

10. 게시를 선택하여 템플릿을 게시합니다.

    보고서 템플릿을 게시할 것인지 여부를 확인하는 메시지가 표시됩니다.

의 당직 일정 관리 보안 인시던트 응답

의 보안 인시던트 응답 당직 일정 관리를 사용하여 분석가의 교대조를 보고 관리할 수 있습니다.

당직 일정 관리 기능을 사용하면 교대조를 확인 및 관리하고, 휴가 요청을 승인 또는 거부할 수 있습니다. 그룹에 대한 알림 기본 설정, 제공 채널, 에스컬레이션 트리거 규칙 및 정책을 관리할 수도 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

sn_si.manager/rota_manager의 주요 기능

- 간격, 휴가 요청 등을 포함하여 그룹의 당직 일정을 살펴봅니다.
- 휴가 요청을 승인 또는 거부합니다.
- 간격과 상충 유무를 검토하고 관리합니다.
- 적용 범위를 제공, 교체 또는 삭제하고 휴가 요청을 삭제합니다.
- 교대조를 생성하고 구성원을 교대조에 추가하거나 삭제합니다.
- 에스컬레이션, 그룹 및 성과 보고서를 봅니다.

sn_si.analyst/oc_read의 주요 기능

- 대기 일정과 기타 교대조 구성원을 봅니다.
- 휴가 요청을 제출하고 그룹의 다른 구성원에게 교대 근무를 위탁합니다.
- 가용성과 선호하는 연락 방법을 지정합니다.
- 교대조의 구성원 및 에스컬레이션 상세 정보를 봅니다.

On-Call Scheduling에 대한 설명서

당직 일정 관리 기능 구성 및 사용에 대한 자세한 내용은 설명서를 IT Service Management On-Call Scheduling 참조하십시오.

SIR Workspace 사용

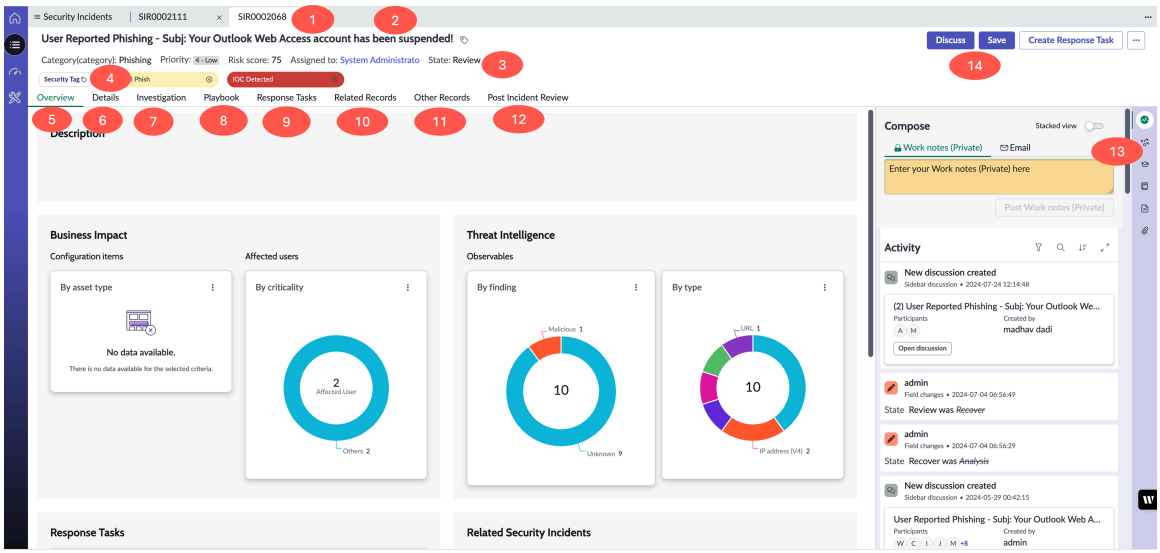
보안 분석가와 관리자는 향상된 사용자 경험으로 일상적인 운영을 수행하고, 인시던트 조사를 완료하고, 개요를 파악하는 데 사용합니다 SIR Workspace .

보안 인시던트 기록 작업

보안 인시던트 기록은 다음으로 구성됩니다.

보안 인시던트 기록에서 사용할 수 있는 주요 구성요소는 다음과 같습니다.

보안 인시던트의 주요 구성요소



기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

번호	이름	설명
1	보안 인시던트 번호	보안 인시던트 번호는 탭 이름에 대해 사용할 수 있습니다.
2	간단한 설명	양식 배너 위에 표시되는 보안 인시던트에 대한 짧은 설명입니다.
3	양식 배너	읽기 전용 섹션으로, 범주, 우선순위, 위험 점수, 상태 및 인시던트 할당 상세 정보와 같은 주요 필드가 포함되어 있습니다. 주: 일반 플랫폼 태그도 여기에 적용할 수 있습니다.
4	보안 태그	보안 인시던트와 관련된 보안 태그를 표시합니다.
5	개요	설명, 유형별 자산 상세 정보로 구성된 비즈니스 영향, 중요도별 영향 사용자, 찾기 및 유형별 옵저버블로 구성된 위협 인텔리전스 항목, 대응 작업, 하위 보안 인시던트로 구성된 관련 보안 인시던트 및 유사한 보안 인시던트와 같은 보안 인시던트에 대한 간략한 개요를 제공합니다.
6	상세 정보	상세 정보 탭에 보안 인시던트 양식이 표시됩니다.
7	조사	조사 탭에 인시던트 조사 환경이 표시됩니다.
8	플레이북	플레이북은 PAD(프로세스 자동화 디자이너)를 통해 트리거됩니다. 프로세스가 생성되고 트리거 조건이 보안 인시던트에 대한 Playbook을 트리거하도록 설정된 경우 그러면 플레이북이 나타납니다.
9	응답 작업	응답 작업은 보안 인시던트와 관련된 모든 응답 작업을 캡처합니다.
10	관련 기록	관련 기록 탭은 이 섹션 아래에 있는 클래식 UI의 모든 관련 목록으로 구성됩니다. 관련 목록은 쉽게 탐색할 수 있도록 비즈니스 영향, 위협 인텔리전스 등의 다양한 섹션 아래에 그룹화되어 있습니다.
11	기타 기록	기타 기록 탭은 이 섹션에 그룹화되고 표시되는 변경 요청, 인시던트 및 이메일과 같은 IT 기록으로 구성됩니다.
12	사후 인시던트 검토 탭	보안 인시던트가 검토 상태로 진행되면 사후 인시던트 검토 탭이 탭 내에 사후 인시던트 평가 및 보고서와 함께 표시됩니다.
13	상황별 메뉴	빠른 실행에 쉽게 액세스할 수 있으며 필요할 때마다 분석가가 액세스할 수 있도록 모든 탭에서 사용할 수 있습니다. 상황별 메뉴를 사용하면 다음과 같은 여러 자원을 쉽게 탐색할 수 있습니다. **1.** 활동 스트림 **2.** 플레이북 **3.** 분석가 지원

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

번호	이름	설명
		4. Runbook **5.** 템플릿 **6.** 첨부 파일
14	양식 UI 작업	다양한 보안 인시던트 양식 UI 작업이 인시던트 양식의 오른쪽 상단에 표시됩니다. 사용 가능한 양식 UI 작업은 다음과 같습니다. • 토론 • 저장 • 응답 작업 생성 • 이메일 작성 • 플레이북 추가 • 관련된 워크플로우 열기 • Crete 인시던트 • 문제 작성 • 변경 요청 작성 • 중단 작성 • 심각도 계산 • 중요 보안 인시던트에 연결 • (으)로 제안 중요 보안 인시던트 • 승격 대상 중요 보안 인시던트 • 엔드포인트에서 추가 작업 실행 • MITRE ATT&CK 기술 연결 • 클래식 UI로 전환 • 보안 케이스에 추가 • 삭제 자세한 내용은 양식 UI 작업 작업 문서를 참조하십시오.

보안 인시던트 개요 섹션

작업 공간의 개요 섹션에는 보안 인시던트와 관련된 주요 정보가 표시됩니다.

도넛형 차트는 드릴다운이 활성화되며, 분석가가 차트 항목을 선택하면 해당 탭 내에 있는 항목의 필터링된 목록 뷰를 사용하여 해당 기록으로 안내합니다. 예를 들어 악성 옵저버 블을 선택하면 관련 기록 탭에서 악성 옵저버블의 필터링된 목록 뷰가 있는 옵저버블로 이동합니다.

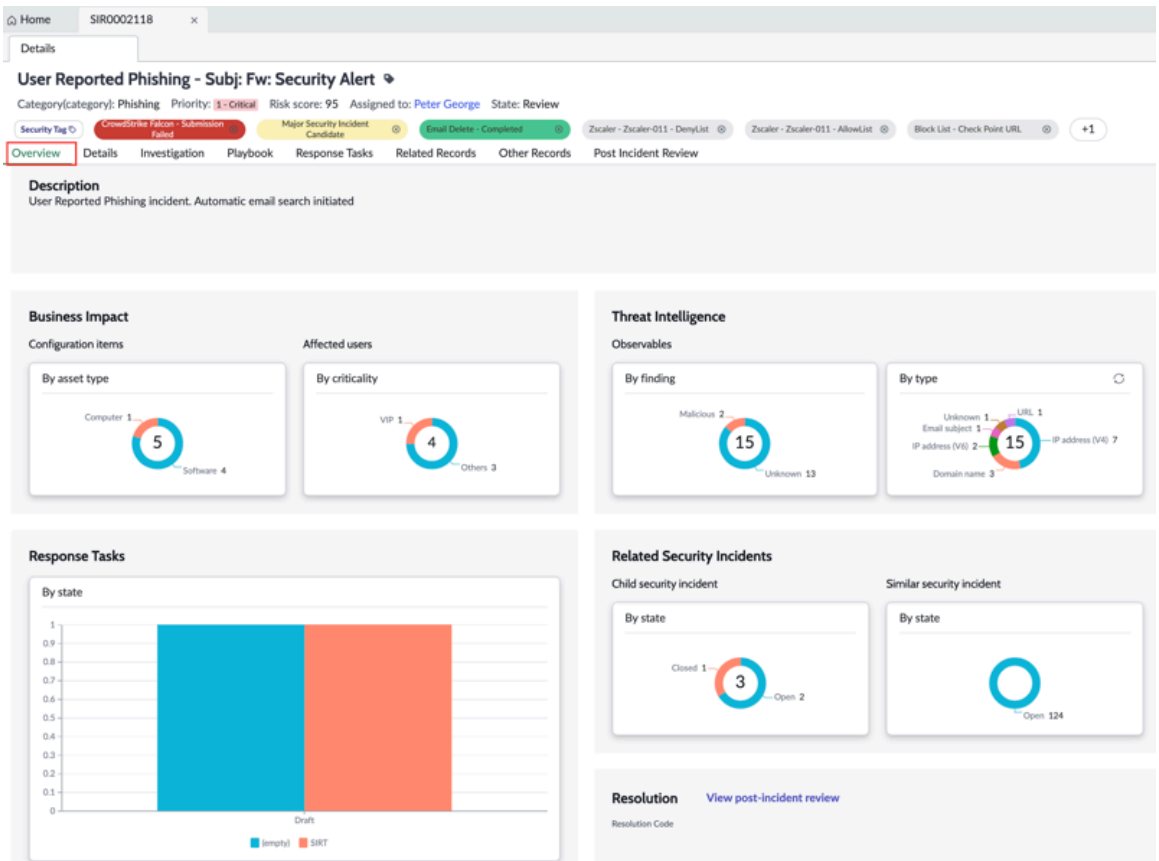
개요 섹션에는 다음이 표시됩니다.

- 보안 인시던트에 대한 설명입니다.
- 자산 유형별 구성 항목 및 중요도별 영향 사용자(VIP 사용자 또는 다른 사용자)와 같은 비즈니스 영향 상세 정보입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 옵저버블과 같은 위협 인텔리전스 항목은 옵저버블이 악성인지 알 수 없는지 여부와 유형별로 찾습니다.
- 상태 및 할당 그룹별 응답 작업입니다.
- 상태별(오픈 또는 종결) 하위 보안 인시던트와 오픈 또는 종결 여부에 관계없이 상태별 유사한 보안 인시던트로 구성된 관련 보안 인시던트입니다.
- 인시던트가 검토 상태로 이동하면 해결 섹션이 표시되며, 개요 섹션 내에 해결 섹션이 표시되어 사후 인시던트 검토를 볼 수 있습니다.
- 해결 - 사후 인시던트 검토 보기: 링크를 선택하여 사후 인시던트 검토 페이지로 이동합니다.
- 인시던트가 종결되면 해결 섹션에는 사후 인시던트 검토 상세 정보와 함께 해결 코드, 해결 메모 및 해결자(사용자)가 표시됩니다.
- 현재 같은 인시던트에 액세스하는 모든 사용자의 이니셜입니다.

개요 섹션



보안 인시던트 상세 정보 섹션

이 섹션에는 보안 인시던트 클래식 UI에서 렌더링되는 보안 인시던트 양식 필드가 표시됩니다.

클래식 UI에는 **SIRW** 뷰가 생성됨이라는 뷰가 있습니다. 이 뷰는 새 작업 공간의 상세 정보 탭에 매핑됩니다. 필요한 모든 사용자 지정 항목을 이 뷰에서 구현해야 합니다.

양식 필드는 다음 섹션으로 그룹화되어 상세 정보 탭의 양식 뷰에 표시되거나, 섹션을 클릭하거나 양식 내의 해당 섹션으로 이동하십시오.

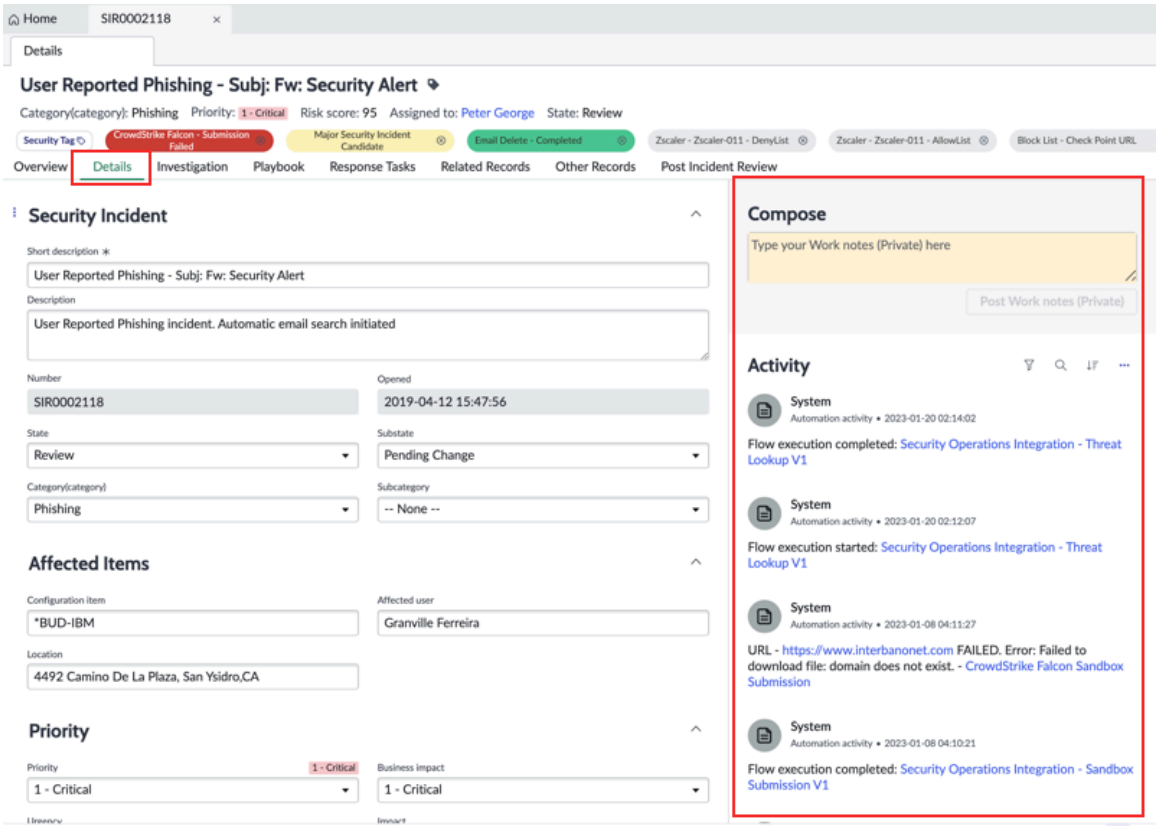
- 보안 인시던트
- 우선순위
- 소스

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 상위
- 지정
- 접근 통제
- 영향을 받는 항목
- 해결

상세 정보 탭의 상세 정보 양식 자체 내에 활동 스트림 섹션이 있으므로 보안 분석가가 빠르게 액세스하여 의견을 추가하고 게시할 수 있습니다.

상세 정보 탭 및 활동 스트림

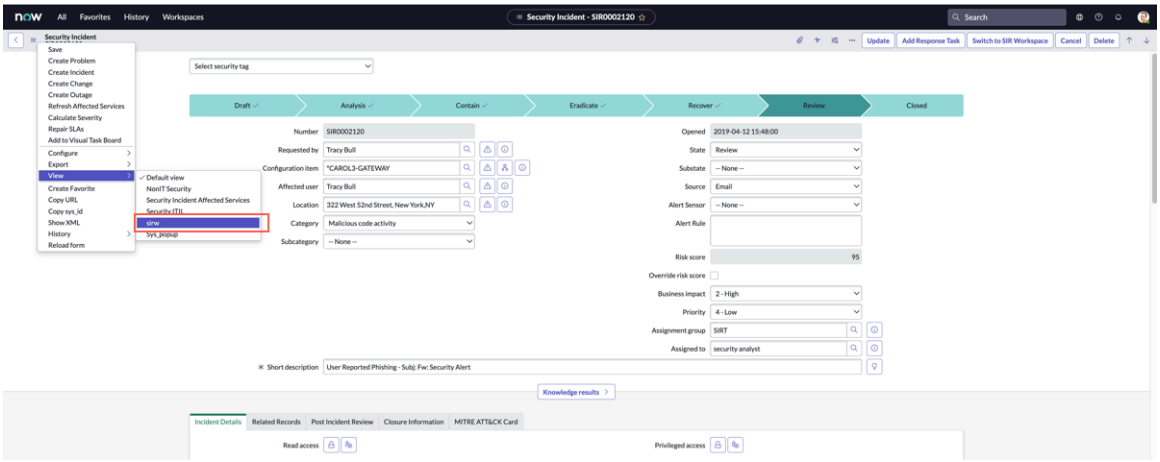


SIR 분석가 작업 공간 뷰를 봅니다.

1. 다음으로 이동 모두 〉 보안 인시던트 〉 미해결 인시던트 표시.
2. 보안 인시던트 기록을 선택합니다.
3. 상황에 맞는 메뉴를 클릭하고 뷰 〉 **SIRW**.

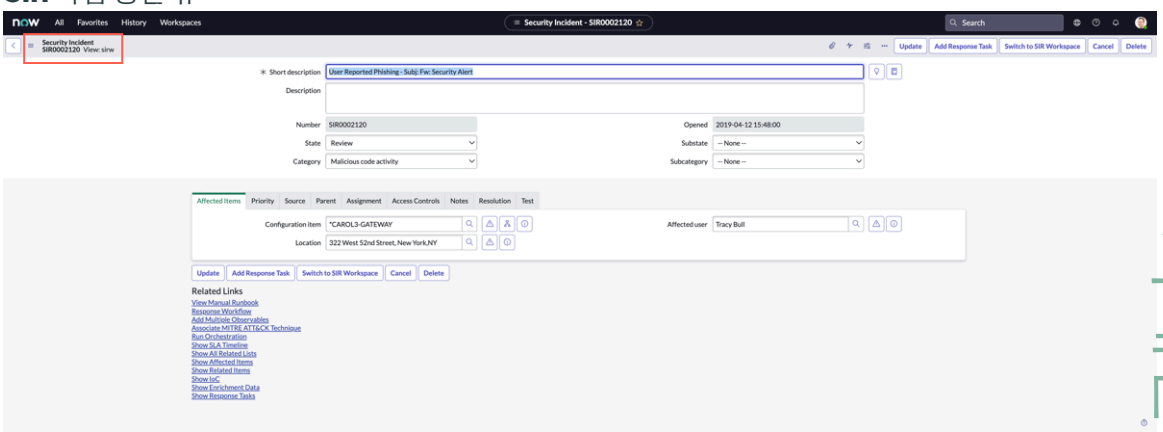
> 주:
> 클래식 UI 양식에서 **sirw** 작업 공간 뷰를 사용하여 사용자 지정할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



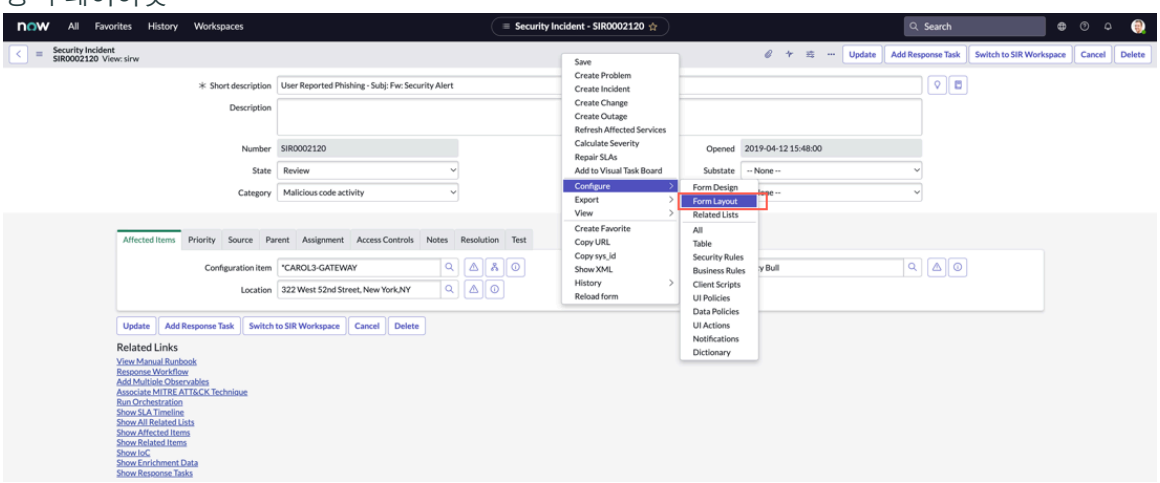
4. 보안 인시던트 작업 공간 뷰는 아래와 같이 렌더링됩니다.

SIR 작업 공간 뷰



5. 보안 인시던트 기록에서 마우스 오른쪽 버튼을 클릭하여 다음으로 이동합니다. 구성 〉 양식 레이아웃.

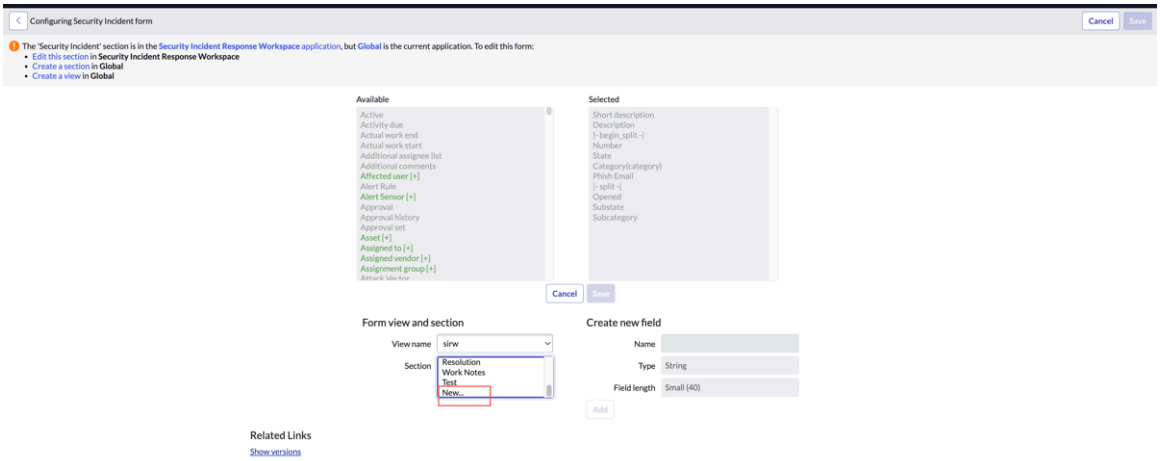
양식 레이아웃



6. 양식 뷰 및 섹션으로 드릴다운하고 섹션에서새로 만들기를 선택하여 새 섹션을 생성합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

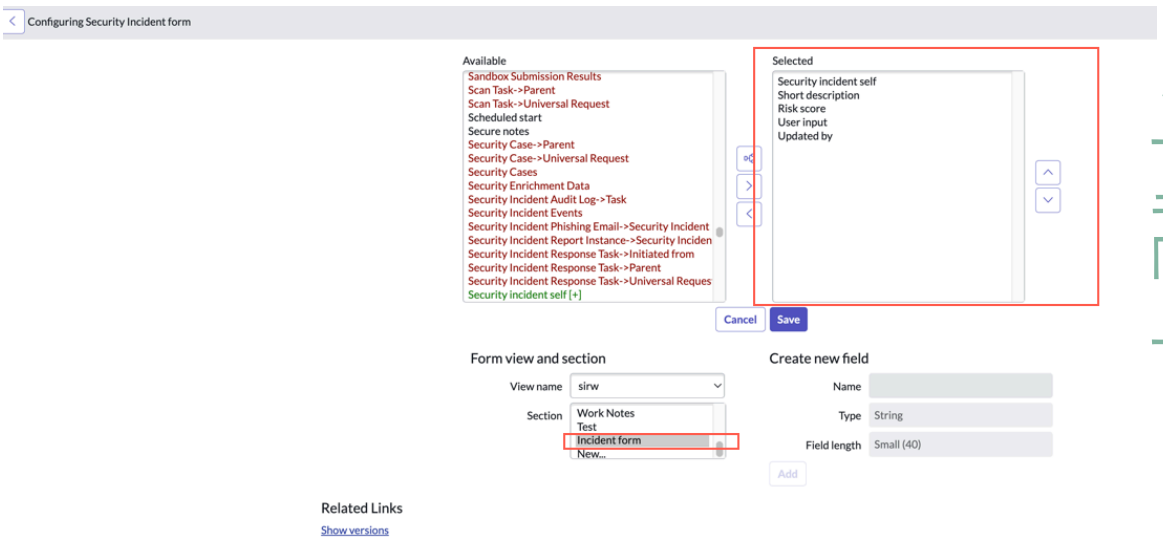
양식 레이아웃 - 단면 뷰



7. 새 섹션 이름을 입력하고 확인을 클릭합니다.

인시던트 양식을 예로 들 수 있습니다.

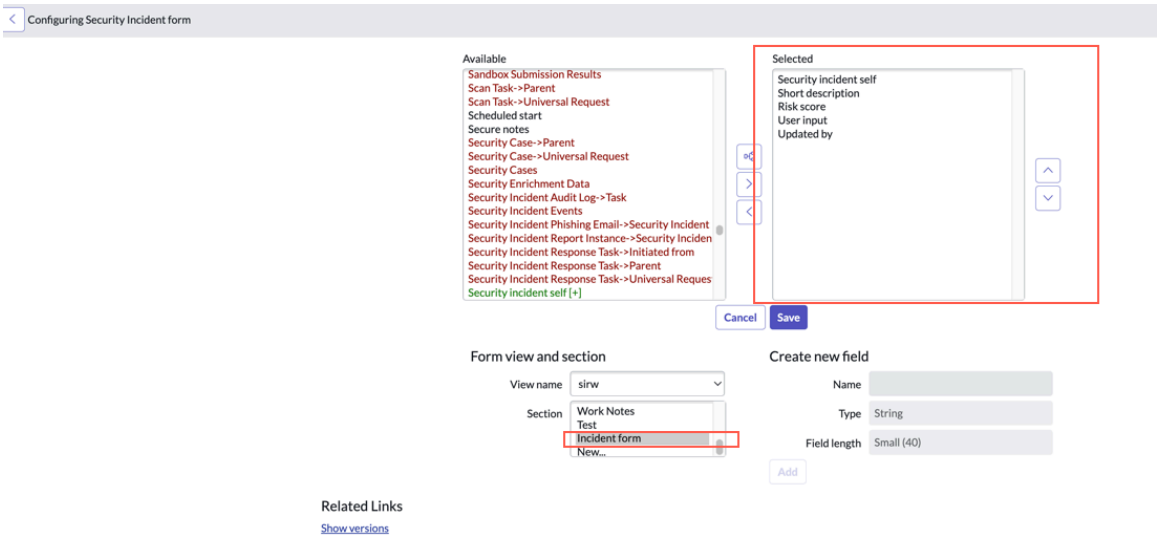
8. 새 섹션이 생성되어 섹션에 추가됩니다.



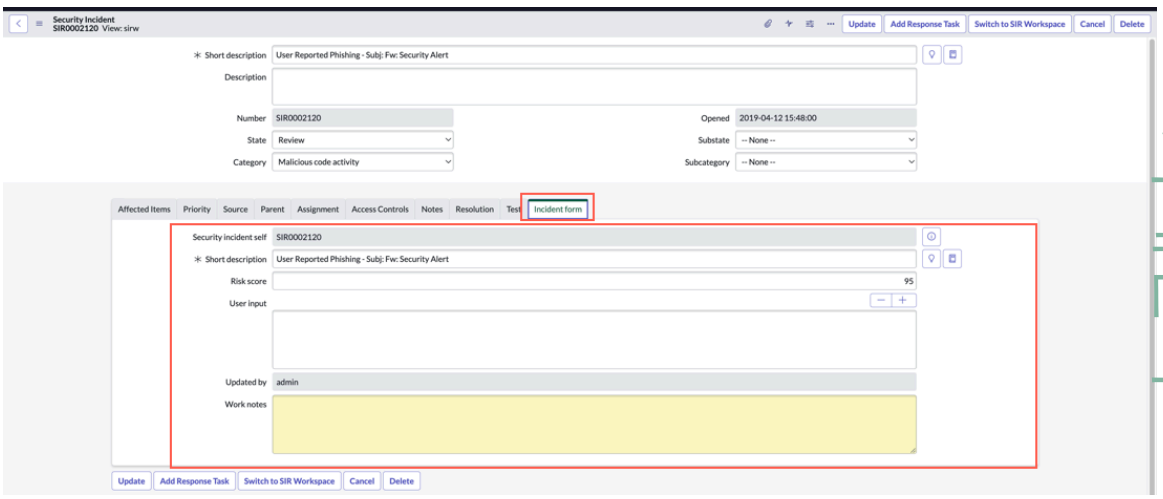
9. 새 섹션을 선택하고 슬러시 버킷에 필요한 섹션 필드를 추가한 다음 저장을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

섹션 필드



10. 새로 추가된 섹션은 보안 인시던트 양식 내에 기존 섹션 레이아웃과 함께 표시됩니다.



11. 이제 **SIR** 작업 공간으로 전환을 클릭하여 보안 인시던트 양식과 작업 공간의 상세 정보 탭에 있는 사용자 지정 섹션으로 이동합니다.

SIR Workspace 오케스트레이션

보안 인시던트 응답 작업 공간 오케스트레이션 활동은 보안 분석가가 조사 캔버스를 보고 적용 가능한 다양한 작업을 수행하는 데 도움이 됩니다.

SIR Workspace 조사 캔버스

보안 인시던트 응답 작업 공간 보안 분석가가 인시던트 정정 프로세스 중에 보안 인시던트와 관련된 핵심 정보를 볼 수 있도록 합니다. 주요 정보에는 옵저버블, 위협 조회 결과, 사이팅 검색, 옵저버블 보강 등의 관련 목록도 포함됩니다.

클래식 UI에서는 바로 사용 가능한 통합과 연결된 대부분의 오케스트레이션 작업을 관련 목록에 대해 사용할 수 있습니다. 예를 들어 위협 조회 실행, 옵저버블 보강 실행 등이 연관된 옵저버블 관련 목록에 대해 표시됩니다. 마찬가지로 호스트 세부 정보 가져오기, 네트워크 통계 가져오기 등은 구성 항목 관련 목록에 대해 사용할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 분석가가 이러한 작업을 수행하면 결과가 다른 관련 목록에 채워집니다. 예를 들어 사용자가 위협 조회 실행을 수행하면 위협 조회 결과 테이블에서 결과를 확인할 수 있습니다. 경우에 따라 결과를 여러 다른 테이블에서 사용할 수 있습니다. 이 과정에서 보안 분석가는 여러 위치의 정보를 상호 연관시키는 데 있어 단절되고 체계적이지 않은 사용자 경험을 하게 됩니다.

새롭게 구성된 조사SIR Workspace캔버스(탭)에서는 분석가가 조사를 수행하는 데 필요한 모든 정보를 논리적으로 한 곳에 그룹화하여 제공합니다.

조사 캔버스 탐색

조사 캔버스의 주요 목적은 필요한 보안 인시던트 데이터를 하나의 공통 위치에 표시하는 것입니다.

SIR Workspace내에서 보안 인시던트 조사는 주로 몇 가지 주요 엔트리포인트를 중심으로 이루어집니다.

다음은 기본 시스템 내의 보안 분석가를 위해 제공되는 몇 가지 주요 엔트리포인트입니다.

- 연결된 옵저버블
- 구성 항목
- 영향을 받는 사용자
- 연결된 피싱 메일
- 이메일 검색

엔트리포인트를 추가하거나, 수정하거나, 해당하는 경우 제거하여 위의 엔트리포인트를 구성할 수도 있습니다. 자세한 내용은 SI 설계 시간 조사 구성 문서를 참조하십시오.

조사 탭에서는 엔트리포인트 테이블이 상위 테이블 역할을 합니다. 상위 테이블에서 수행된 오케스트레이션 작업의 결과를 보유하는 모든 테이블은 엔트리포인트 내에 하위 테이블로 표시됩니다.

예를 들어 연결된 옵저버블 엔트리포인트의 경우 옵저버블 연결 테이블이 상위 테이블이고 위협 조회 결과, 샌드박스 제출 결과 등의 다른 테이블은 하위 테이블입니다.

보안 분석가는 연관된 옵저버블 테이블에서 모든 오케스트레이션 작업을 수행할 수 있으며, 여러 위치를 탐색할 필요 없이 동일한 페이지 내에서 모든 관련 정보를 볼 수 있습니다.

주:
사용자가 개요 페이지에서 상호작용 가능한 차트(예: 악성 옵저버블)를 클릭하면 조사 캔버스 내에서 악의적인 옵저버블의 필터링된 뷰로 이동합니다. 또는 사용자가 모든 데이터가 있는 조사 캔버스로 이동하여 조사를 직접 시작할 수 있습니다.

엔트리포인트 아래의 하위 테이블 목록도 구성할 수 있습니다. 자세한 내용은 SI 설계 시간 조사 구성 문서를 참조하십시오.

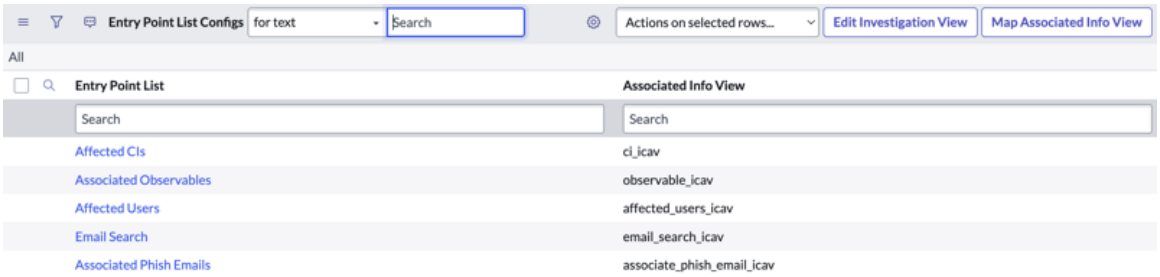
다음은 기본 시스템 내에서 구성되고 프로비저닝되는 엔트리포인트(연결된 옵저버블)의 자세한 예입니다.

1. 드롭다운 목록에서 연결된 옵저버블 엔트리포인트를 선택합니다.

   여기서 상위 테이블도 연결된 옵저버블입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

엔트리포인트 목록 구성



2. 상위 테이블에서 하나 이상의 옵저버블을 선택합니다.
3. 원하는 역량을 실행합니다.

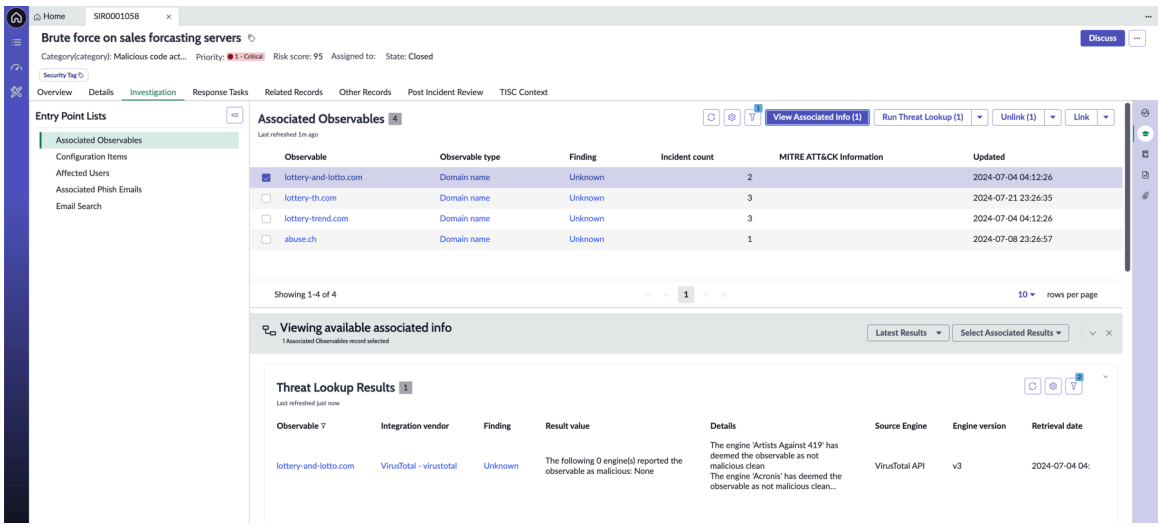
   예를 들어 위협 조회 실행을 선택하여 선택한 옵저버블에 대한 위협 조회 결과를 가져옵니다.

   주:
   해당 옵저버블 작업이 실행되면 백엔드에서 프로세스가 실행되고 결과가 옵저버블 목록 아래에 표시됩니다.

4. 옵저버블 결과를 보려면 관련 정보 보기를 클릭합니다. 결과는 같은 페이지에 표시됩니다.

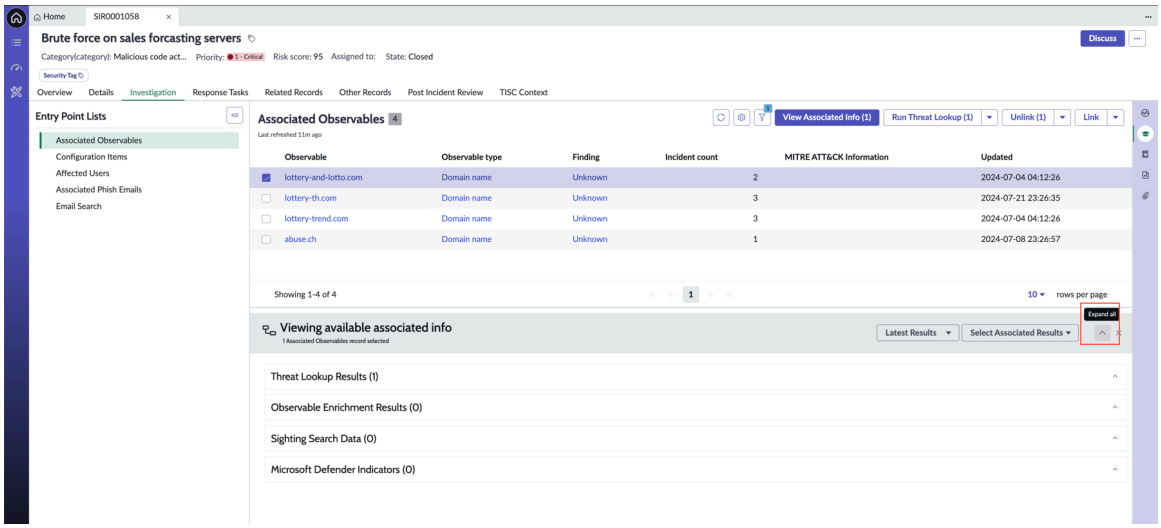
   주:
   결과별 필터를 사용하여 결과를 보고 모든 결과 또는 최신 결과 중 원하는 보기를 선택할 수 있습니다. 기본적으로 최신 결과가 표시됩니다. (통합의) 구현이 여러 개 있는 경우 구현당 최신 결과가 표시됩니다.

   또한 하위 테이블 결과인 연결된 관련 목록을 기준으로 결과를 필터링할 수 있습니다. 기본적으로 구성된 모든 하위 테이블 관련 목록이 표시됩니다. 자세한 내용은 SI 설계 시간 조사 구성 문서를 참조하십시오. 그러나 필요한 하위 테이블만 선택하도록 선택할 수 있습니다.



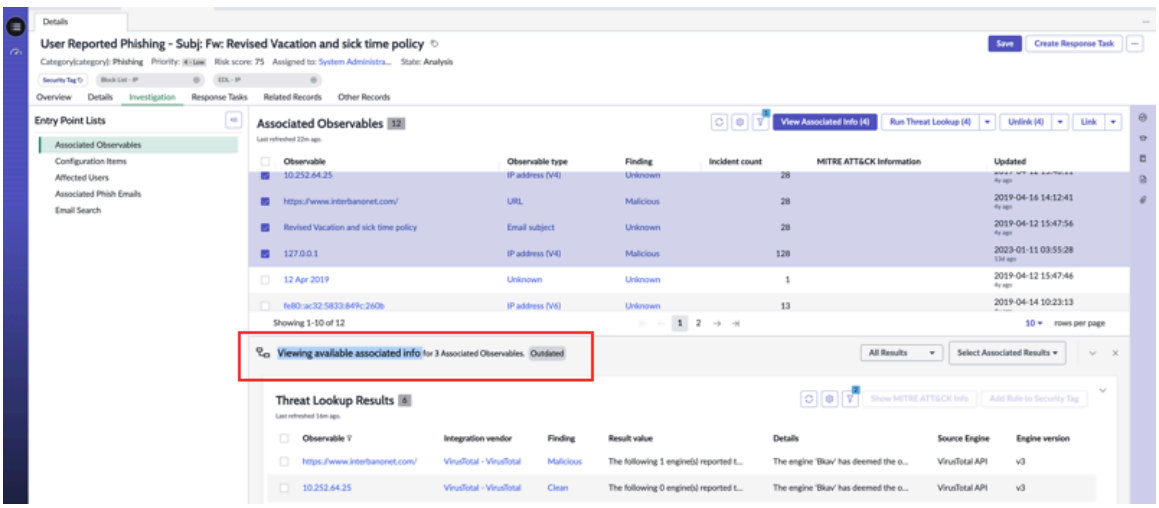
5. 연결된 정보 보기를 클릭하면 연결된 모든 하위 테이블 데이터를 한 곳에서 볼 수 있지만 보기 닫기 버튼을 선택하여 관련 목록 보기를 닫을 수 있습니다. 뷰를 닫으면 이전과 같이 옵저버블 상위 테이블만 볼 수 있습니다.
6. 사용 가능한 관련 정보 보기 결과 테이블 내에서 모든 위쪽 방향 확장 아이콘을 클릭하여 모든 관련 목록 하위 테이블 데이터를 확장합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



7. 모든 관련 목록 하위 테이블 데이터를 축소하려면 모든 아래쪽 방향 축소 아이콘을 클릭합니다.

주:
모든 하위 테이블 데이터가 포함된 관련 정보 섹션 상단의 배너는 사용자에게 제공되는 옵저버블 관련 정보의 수를 보여줍니다. 예를 들어 처음에 2개의 옵저버블을 선택하고 관련 정보 보기를 클릭하면 배너에 2개의 연결된 옵저버블에 대해 사용 가능한 관련 정보를 보는 중이라고 표시됩니다. 예를 들어 다른 옵저버블을 선택하면 정보가 오래되었다는 메시지가 배너에 표시됩니다(아래 스크린샷). 최신 데이터를 가져오려면 관련 정보 보기를 다시 클릭해야 합니다.



옵저버블 관련 정보에 대한 위의 포괄적인 뷰 외에도 상위 테이블의 기록에 대한 자세한 정보를 보려면 옵저버블을 클릭하면 선택한 기록에 대한 자세한 뷰가 있는 다른 탭에서 상위 테이블 기록 양식이 열립니다. 선택한 특정 기록의 모든 연결된 하위 테이블 데이터도 관련 정보 섹션 아래에 표시됩니다.

그러나 연결된 정보 섹션에는 조사 캔버스에 표시된 것처럼 하위 테이블의 최신 결과만 읽기 전용 모드로 표시됩니다. 이 뷰에서는 작업을 수행할 수 없습니다. 하위 테이블의 양식 페이지는 모든 작업(있는 경우)과 함께 전체 기능 페이지를 렌더링하는 새 탭에서 열 수 있습니다.

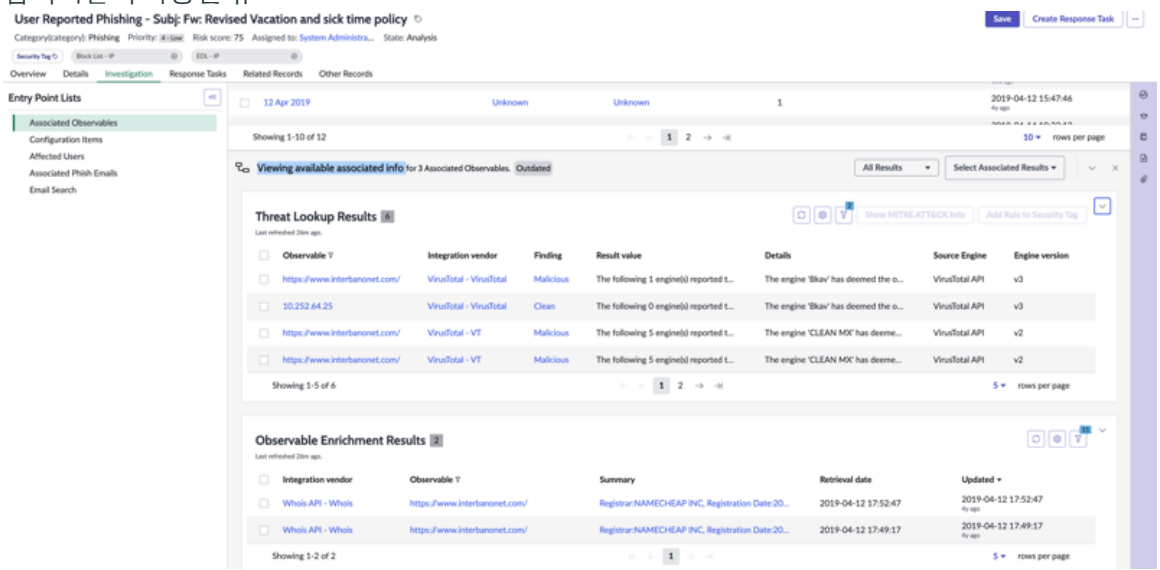
드롭다운 목록을 사용하여 여러 테이블 간에 전환할 수 있습니다. 관련 정보 섹션에서 각 양식을 확장하거나 축소할 수도 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵저버블 양식 페이지(상위 테이블 기록 양식 페이지) 내에서 사용 가능한 특정 작업을 수행할 수 있습니다. 작업을 수행할 때마다 연결된 정보 배너에서 새로 고침을 클릭하여 데이터를 새로 고칠 수 있습니다.

8. 모든 관련 목록 하위 테이블을 확장하려면 모두 확장을 클릭합니다. 기본적으로 모든 하위 항목이 확장됩니다.

옵저버블의 확장된 뷰



관련 정보

SI 설계 시간 조사 구성

역량 프레임워크 기반의 통합을 위한 통합 경험 프레임워크

클래식 UI에서는 위협 보기 실행, 사이팅 검색 수행 등과 같은 오케스트레이션 활동을 수행할 때 환경이 분리됩니다. 각 기능은 실행하는 동안 고유한 환경이 있습니다. 새 작업 공간에는 모든 기능에 걸쳐 통합된 경험이 있습니다.

통합 환경은 역량 프레임워크 내에 속하는 통합 및 오케스트레이션 활동에만 적용할 수 있습니다. 통합과 관련된 작업이 있을 수 있습니다(예: Microsoft Defender에서 표시기 만들기). 이러한 작업에는 사용 사례에 필요한 고유한 환경이 있습니다.

새 프레임워크는 아래에 설명된 대로 세 단계가 있는 모달 화면으로 구성됩니다.

1. 구현: 첫 번째 단계는 선택한 역량에 대해 존재하는 하나 이상의 구현을 선택하는 것입니다.

   예를 들어 분석가가 위협 조회 실행을 클릭하면 분석가는 위협 조회 실행 기능에 대해 존재하는 하나 이상의 구현을 선택할 수 있습니다.

   각 구현에는 통합 소스에 대한 세부 정보가 포함됩니다. 아래 표를 참조하십시오. 각 구현에 대한 추가 정보도 제공됩니다.

   추가 정보에는 필터에 대한 정보, 지원되는 옵저버블 유형 등이 포함될 수 있습니다. 추가 정보는 원하는 대로 구성할 수 있습니다. 자세한 내용은 UX 프레임워크 기술 구성 절차를 참조하십시오.

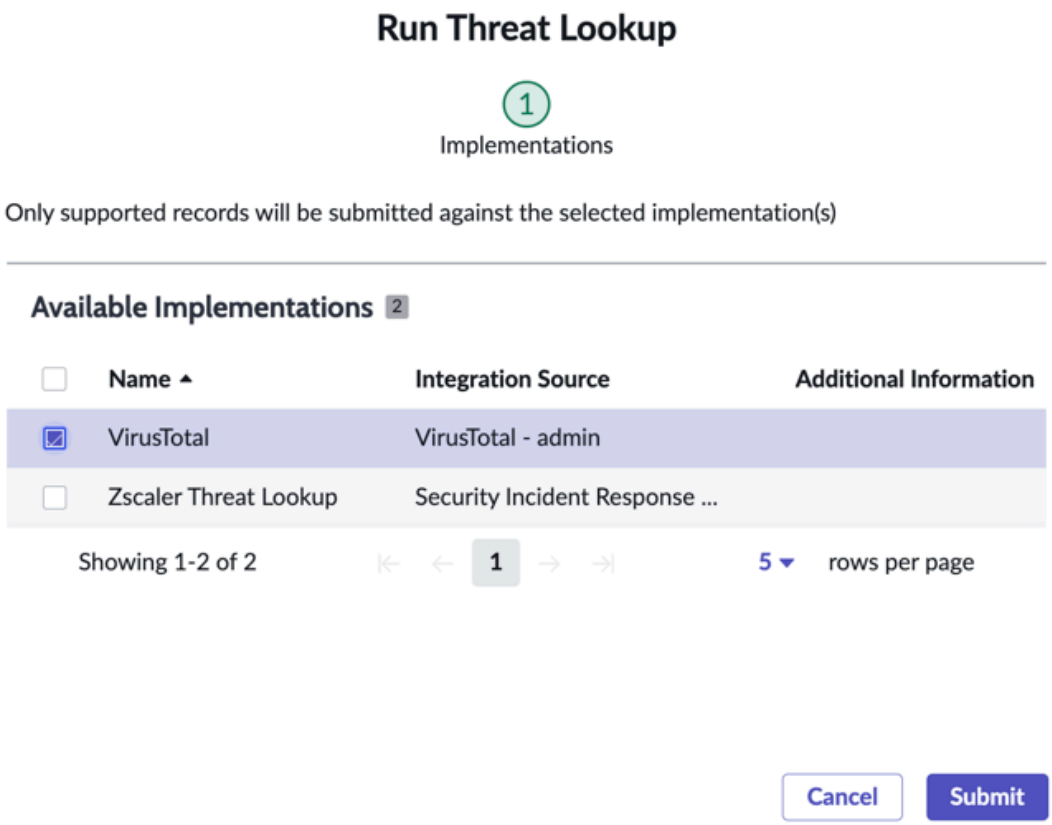
   통합 구현 프레임워크 모달

구현	설명
이름	구현의 이름입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

구현	설명
통합 소스	사용 중인 구성과 같은 구현의 소스입니다.
추가 정보	이 열은 작업을 진행하기 위해 선택한 구현에 대해 보안 분석가에게 더 많은 컨텍스트를 추가하는 정적 정보를 캡처합니다. 지원 가능성 또는 필터링된 정보를 예로 들 수 있습니다. 또한 구현에서 도메인 또는 URL과 같은 특정 유형의 옵저버블만 지원하는 경우 이 열에 해당 정보를 추가하여 사용자에게 컨텍스트를 제공할 수 있습니다. **주:** UI 프레임 워크는 기본적으로 모든 유형의 구현과 모든 유형의 옵저버블을 선택할 수 있습니다. 제출하는 동안 제공되는 기존 기본 시스템 통합은 백엔드에서 필터링을 처리하고 지원되는 유형의 옵저버블만 제출합니다. 지원 가능성과 일치하지 않는 나머지 레코드는 무시됩니다. 따라서 역량을 선택하는 동안 UI 정보 메시지가 표시됩니다. 선택한 구현에 대해 지원되는 기록만 제출됩니다.

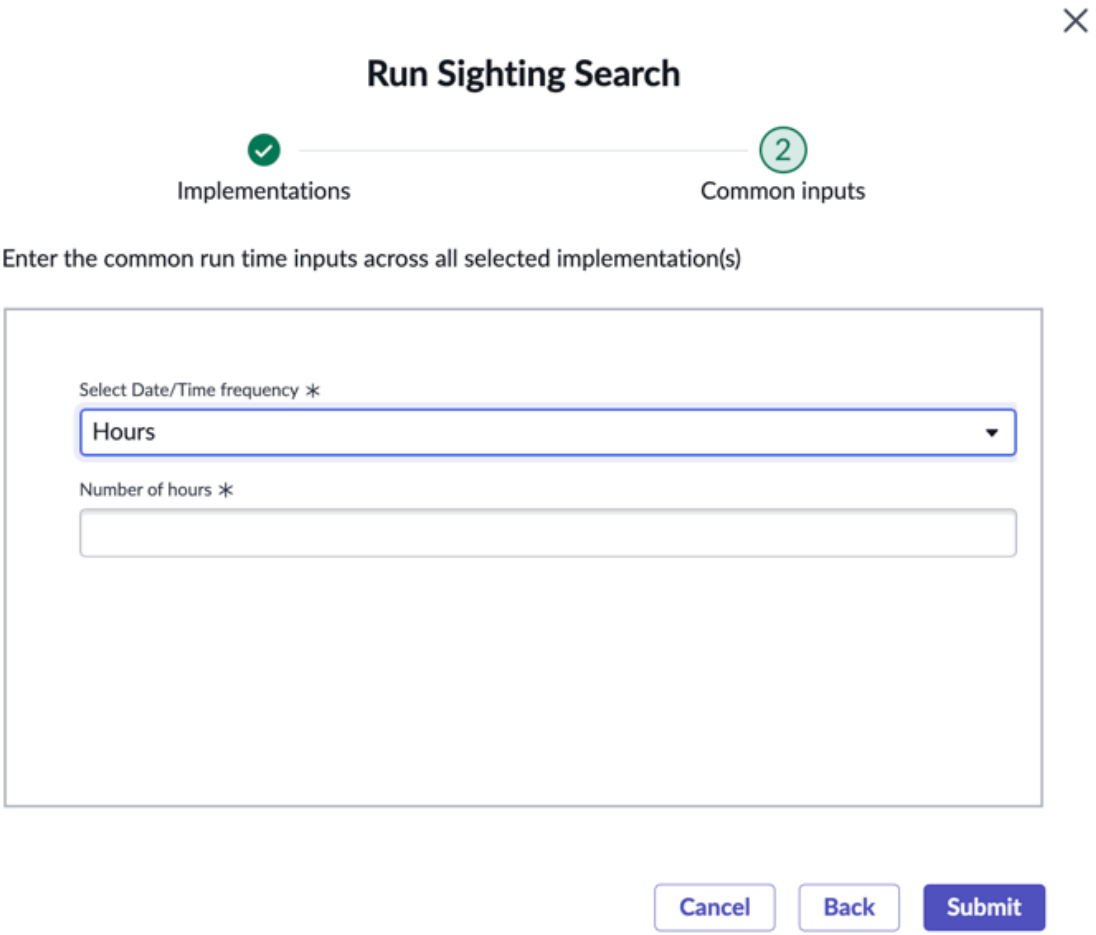
화면 **1:** 구현



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

2. 일반 입력: 선택한 구현 또는 선택한 모든 적용 가능한 구현에 대한 공통 입력을 추가합니다. 구현의 화면 2입니다. 예를 들어, 현재로서는 사이팅 검색 에만 공통 입력 화면이 있습니다. 이 구현은 화면 1(구현)과 화면 2(공통 입력)의 조합입니다.

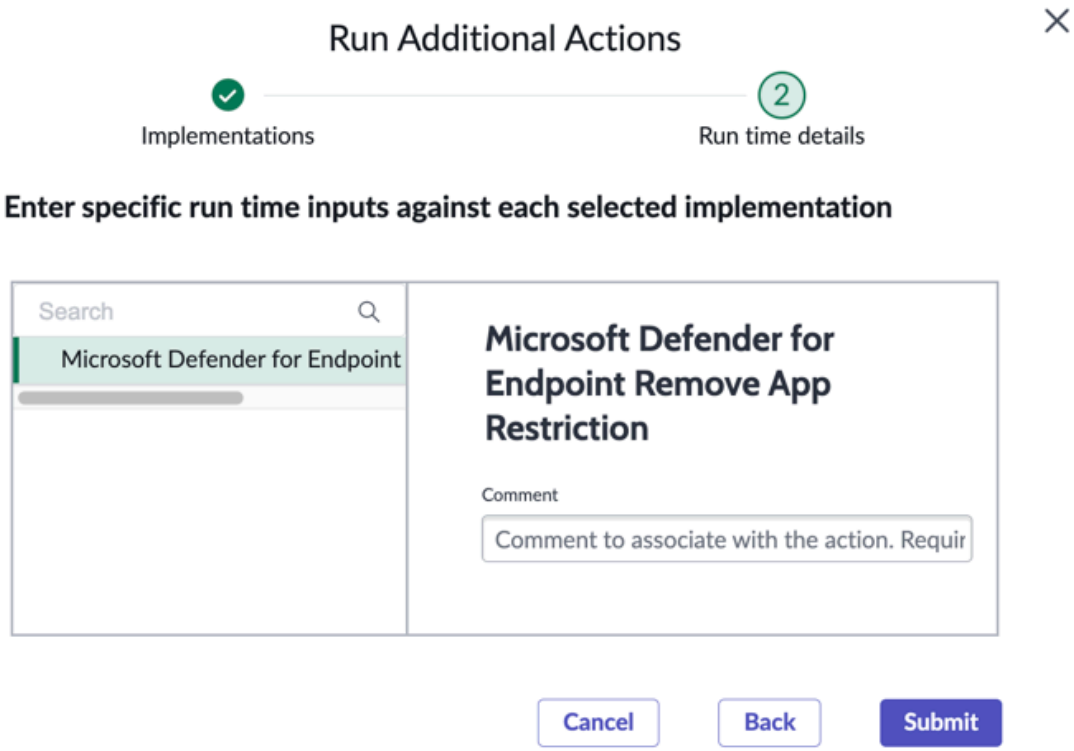
화면 **1** + 화면 **2**



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 실행 시간 상세 정보: 선택한 구현에 대해 서로 다른 특정 실행 시간 입력을 추가합니다. 구현의 화면 3입니다. 이 구현은 화면 1(구현)과 화면 3(특정 런타임 입력)의 조합입니다.

특정 입력



주:
세 단계가 모두 항상 필요한 것은 아닙니다. 필요한 입력 기능 및 유형에 따라 런타임 상세 정보 단계와 공통 입력 단계가 표시됩니다.

통합 경험 기능 및 모달 화면

아래 표에서는 기능 및 적용 가능한 화면에 대해 설명합니다.

역량 및 적용 가능한 화면 테이블

역량	UX 프레임워크 적용 가능한 화면	지원되는 통합
위협 조회 실행	화면 1 – 구현 선택만 적용할 수 있습니다. 위협 조회 실행에 적용할 수 있는 공통 입력 또는 구현 특정 입력이 없습니다. 따라서 하나 이상의 구현을 선택할 수 있도록 보안 분석가에게 화면 1만 표시됩니다. 구현을 선택한 후 보안 분석가가 작업을 제출할 수 있습니다.	• Virus Total • Hybrid Analysis • Zscaler와의 보안 인시던트 응답 통합 • 피스탱크 • 메타디펜더 • 위협군중 • 내가 전당포에 잡혔나? • Crowd Strike Falcon Intelligence

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

역량 및 적용 가능한 화면 테이블

역량	**UX** 프레임워크 적용 가능한 화면	지원되는 통합
옵저버블 보강 실행	화면 1 – 구현 선택만 적용할 수 있습니다. 옵저버블 보강 실행에 적용할 수 있는 공통 입력 또는 구현별 입력이 없습니다. 따라서 하나 이상의 구현을 선택할 수 있도록 보안 분석가에게 화면 1만 표시됩니다. 구현을 선택한 후 보안 분석가가 작업을 제출할 수 있습니다.	• MISP • Microsoft Defender 엔드포인트 • Shodan • RiskIQ • 후이즈 • 역방향 WHOIS
사이팅 검색 실행/웹 사이팅 검색 실행/이메일 사이팅 검색 실행	화면 1 – 구현 선택 및 화면 2 – 공통 입력을 적용할 수 있습니다. 사이팅 검색은 Splunk 및 기타 통합의 여러 구현에서 날짜 및 시간 빈도를 공통 입력으로 사용합니다. 이 화면은 날짜 및 시간 빈도를 캡처하기 위해 보안 분석가에게 표시됩니다. 이러한 입력이 필요하지 않은 통합(예: FireEye HX)의 경우 무시됩니다. 하나 이상의 구현을 선택하고 공통 입력을 제공하면 보안 분석가가 작업을 제출할 수 있습니다.	• splunk-incident 보강 • Carbon Black • 탄력적 검색 • FireEye HX • McaFee ESM • 엔드포인트용 MSFT Defender • Splunk 사이팅 • Qradar 사이팅 검색 • MISP
샌드박스에 제출	화면 1 – 구현 선택 및 화면 3 – 구현 특정 입력을 적용할 수 있습니다. Sandbox에 제출은 다른 구현에 대해 다른 입력을 사용합니다. 현재 이 역량에 대한 공통 입력이 없습니다. 예를 들어, 분석가가 Crowdstrike Falcon X 빠른 스캔, Crowdstrike Falcon X Windows 64, Crowdstrike Falcon X Linux 및 Zscaler를 선택하면 입력이 달라집니다. Crowdstrike Falcon X Quick scan 및 Zscaler는 추가 실행 시간 입력이 필요하지 않습니다. Crowdstrike Falcon X Windows 64는	• CrowdStrike Falcon X Sandbox 통합 • Zscaler와의 보안 인시던트 응답 통합

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

역량 및 적용 가능한 화면 테이블

역량	**UX** 프레임워크 적용 가능한 화면	지원되는 통합
	Crowdstrike Falcon X Linux와 다른 선택적 실행 시간 입력을 사용합니다. 따라서, 이들은 스크린 3에서 특히 적용 가능한 개별 선택된 구현에 대해 제공될 수 있다.	
감시 목록에 게시	화면 1 – 구현 선택만 적용할 수 있습니다. 감시 목록에 게시에 적용할 수 있는 공통 입력 또는 구현 특정 입력이 없습니다. 따라서 하나 이상의 구현을 선택할 수 있도록 보안 분석가에게 화면 1만 표시됩니다. 구현을 선택한 후 보안 분석가가 작업을 제출할 수 있습니다.	Crowdstrike Falcon 호스트
요청 허용/차단	화면 1 – 구현 선택만 적용할 수 있습니다. 허용 / 차단 요청에 적용할 수 있는 공통 입력 또는 구현 특정 입력이 없습니다. 따라서 하나 이상의 구현을 선택할 수 있도록 보안 분석가에게 화면 1만 표시됩니다. 구현을 선택한 후 보안 분석가가 작업을 제출할 수 있습니다.	• 팔로알토 네트워크 NGFW • 체크 포인트 NGFW • Zscaler와의 보안 인시던트 응답 통합
호스트 상세 정보 가져오기	화면 1 – 구현 선택만 적용할 수 있습니다. 호스트 상세 정보 가져오기에 적용할 수 있는 공통 입력 또는 구현 특정 입력이 없습니다. 따라서 하나 이상의 구현을 선택할 수 있도록 보안 분석가에게 화면 1만 표시됩니다. 구현을 선택한 후 보안 분석가가 작업을 제출할 수 있습니다.	• FireEye HX • 엔드포인트용 Microsoft Defender
파일 가져오기	화면 1 – 구현 선택 및 화면 2 – 공통 입력을 적용할 수 있습니다.	FireEye HX

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

역량 및 적용 가능한 화면 테이블

역량	**UX** 프레임워크 적용 가능한 화면	지원되는 통합
	파일 가져오기는 파일 이름, 경로를 일반 입력으로 사용합니다. 하나 이상의 구현을 선택하고 공통 입력을 제공하면 보안 분석가가 작업을 제출할 수 있습니다.	
네트워크 통계 가져오기	화면 1 – 구현 선택만 적용할 수 있습니다. 네트워크 통계 가져오기에 적용할 수 있는 공통 입력 또는 구현 특정 입력이 없습니다. 따라서 하나 이상의 구현을 선택할 수 있도록 보안 분석가에게 화면 1만 표시됩니다. 구현을 선택한 후 보안 분석가가 작업을 제출할 수 있습니다.	• FireEye HX • 넷스탯
실행 중인 프로세스 임포트	화면 1 – 구현 선택만 적용할 수 있습니다. 실행 중인 프로세스 가져오기에 적용할 수 있는 공통 입력 또는 구현별 입력이 없습니다. 따라서 하나 이상의 구현을 선택할 수 있도록 보안 분석가에게 화면 1만 표시됩니다. 구현을 선택한 후 보안 분석가가 작업을 제출할 수 있습니다.	• FireEye HX • Carbon Black • 시스템 명령
실행 중인 서비스 가져오기	화면 1 – 구현 선택만 적용할 수 있습니다. 실행 중인 서비스 가져오기에 적용할 수 있는 공통 입력 또는 구현 특정 입력이 없습니다. 따라서 하나 이상의 구현을 선택할 수 있는 화면 1만 분석가에게 표시됩니다. 구현을 선택한 후 분석가는 작업을 제출할 수 있습니다.	FireEye HX
호스트 격리/호스트 격리 해제	화면 1 – 구현 선택 및 화면 3 – 구현 특정 입력을 적용할 수 있습니다.	• FireEye HX • Microsoft Defender 엔드포인트 • Carbon Black

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

역량 및 적용 가능한 화면 테이블

역량	**UX** 프레임워크 적용 가능한 화면	지원되는 통합
	호스트 격리/호스트 격리 해제는 구현마다 다른 입력을 사용합니다. 현재 이 역량에 대한 공통 입력이 없습니다. 예를 들어 분석가가 FireEye HX 및 엔드포인트용 Microsoft Defender 선택하면 입력이 달라집니다. FireEye HX에는 실행 시간 입력이 필요하지 않습니다. 반면에 Microsoft Defender는 격리 유형 및 주석과 같은 입력을 사용합니다. 따라서, 이들은 스크린 3에서 특히 적용 가능한 개별 선택된 구현에 대해 제공될 수 있다.	
추가 작업 실행	화면 1 – 구현 선택 및 화면 3 – 구현 특정 입력을 적용할 수 있습니다. 추가 작업 실행 호스트는 다른 구현에 대해 다른 입력을 사용합니다. 현재 이 역량에 대한 공통 입력이 없습니다. 예를 들어, 분석가가 FireEye HX Standard Investigative Details Script, FireEye HX Triage Acquisition 및 Crowdstrike Falcon Insight reg unload를 선택하면 입력이 달라집니다. FireEye HX 표준 조사 상세 정보 스크립트 및 FireEye HX 환자 분류 획득은 둘 다에 대해 다를 수 있는 입력으로 의견을 사용합니다. Crowdstrike Falcon Insight reg 언로드는 하위 키를 입력으로 사용합니다. 따라서, 이들은 스크린 3에서 특히 적용 가능한 개별 선택된 구현에 대해 제공될 수 있다.	• FireEye HX • 엔드포인트용 Microsoft Defender • Crowdstrike Falcon Insight

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

역량 및 적용 가능한 화면 테이블

역량	UX 프레임워크 적용 가능한 화면	지원되는 통합
	주: 현재는 구현의 단일 선택만 지원합니다. 향후 릴리스에서는 다중 구현 선택이 지원될 예정입니다.	

통합 경험 예

이 예에서는 통합 경험 프레임워크 기능을 보여 줍니다.

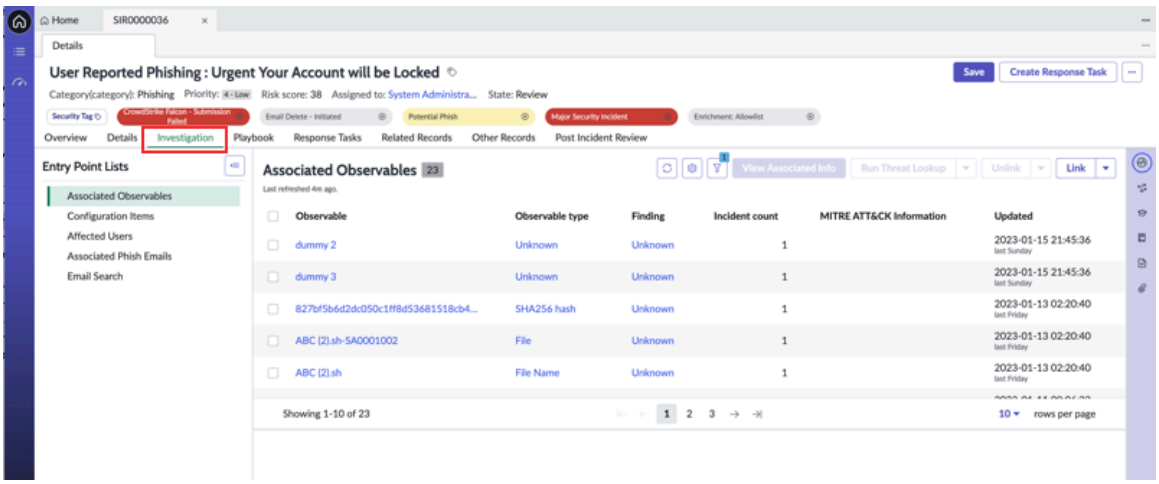
예시 **1:** 구현 선택: 위협 조회

아래 예제에서는 구현을 보여 줍니다.

예 **1:** 화면 1만 위협 조회

의 SIR Workspace조사 탭을 사용하여 위협 조회 실행 관련 통합 역량 작업을 수행할 수 있습니다.

1. 조사 탭에서 페이지 왼쪽에 표시되는 엔트리포인트 목록 섹션으로 이동합니다.
2. 엔트리포인트를 선택하고 통합 기능 작업을 실행합니다.



주:
작업 공간에서 관련 기록 탭으로 이동하여 통합 기능 작업을 수행할 수도 있습니다.

위협 조회 는 통합을 수행하는 방법에 대해 자세히 설명하는 예 중 하나입니다.

구현 선택

해당하는 구현을 하나 이상 선택합니다.

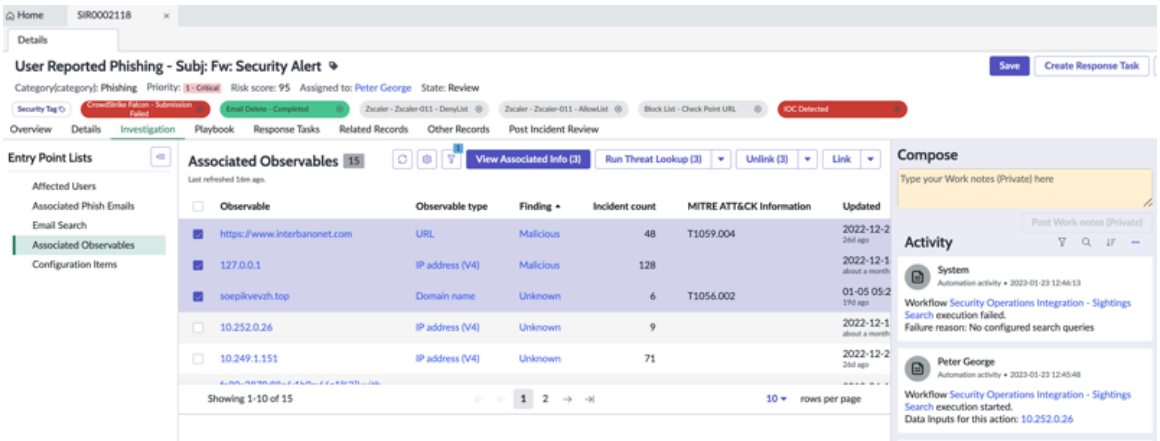
시작하기 전에
필요한 역할: sn_si.analyst

사용 가능한 구현이 나열됩니다. 구현을 선택합니다. 구현을 선택한 후에는 선택한 각 구현에 대해 지원되는 기록만 제출됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

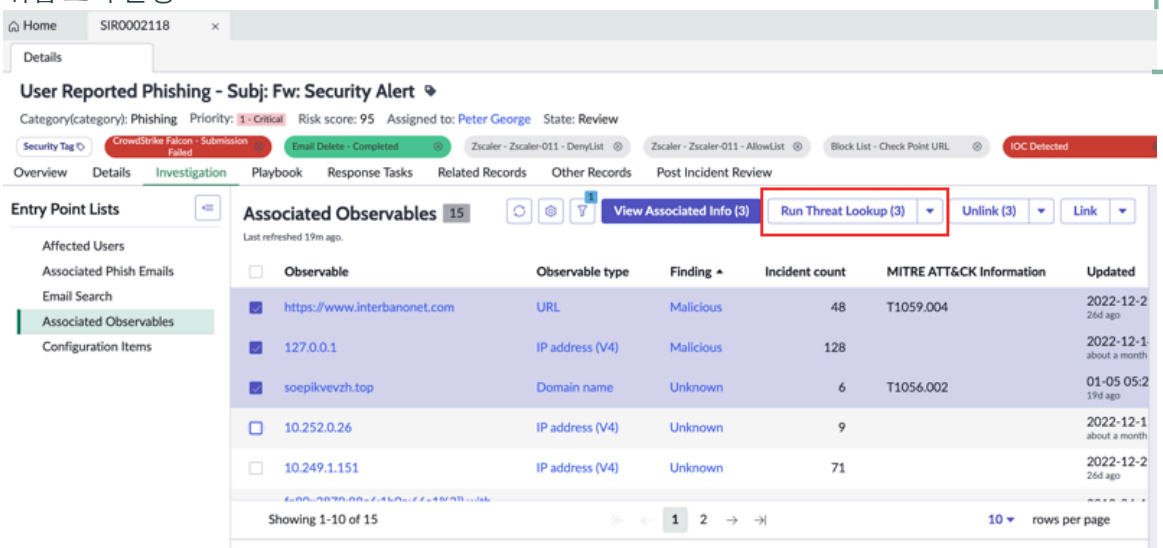
1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간.
2. 보안 인시던트를 엽니다.
3. 작업 공간의 조사 탭으로 이동합니다.
   엔트리포인트 목록이 있는 조사 탭이 표시됩니다.



4. 엔트리포인트 목록에서 연결된 옵저버블을 선택합니다.
   예를 들어 연결된 옵저버블 관련 목록. 해당 옵저버블 기록이 표시됩니다.

> **주:**
> 선택한 옵저버블에 대한 조회를 수행할 구현을 선택하거나 모든 구현을 선택하여 조회를 수행할 수 있습니다.

위협 조회 실행



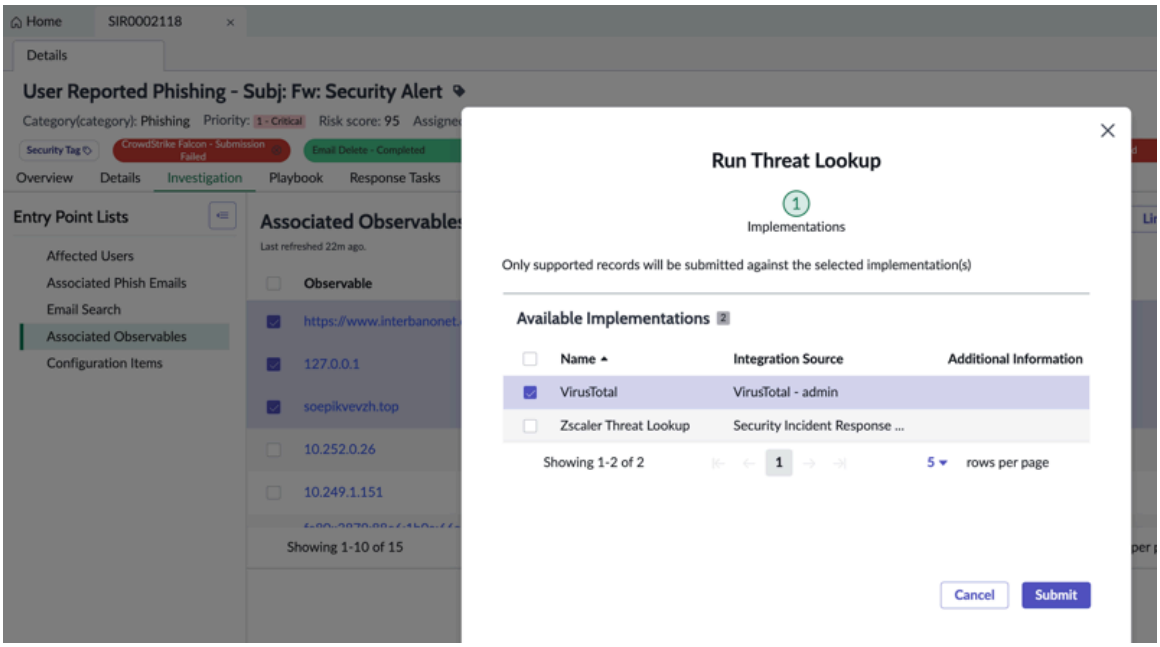
5. 위협 조회를 수행할 옵저버블 확인란을 선택합니다.
6. 관련 목록 페이지 상단에 표시되는 관련 목록 작업 드롭다운으로 이동합니다.
7. 위협 조회 실행을 선택하여 위협 인텔리전스 관련 통합 역량 작업을 수행합니다.

> **주:**
> 위협 조회 실행 기능은 위협 인텔리전스 조회를 수행하여 하나 이상의 옵저버블이 알려진 보안 위협과 연결되어 있는지 여부를 확인합니다.

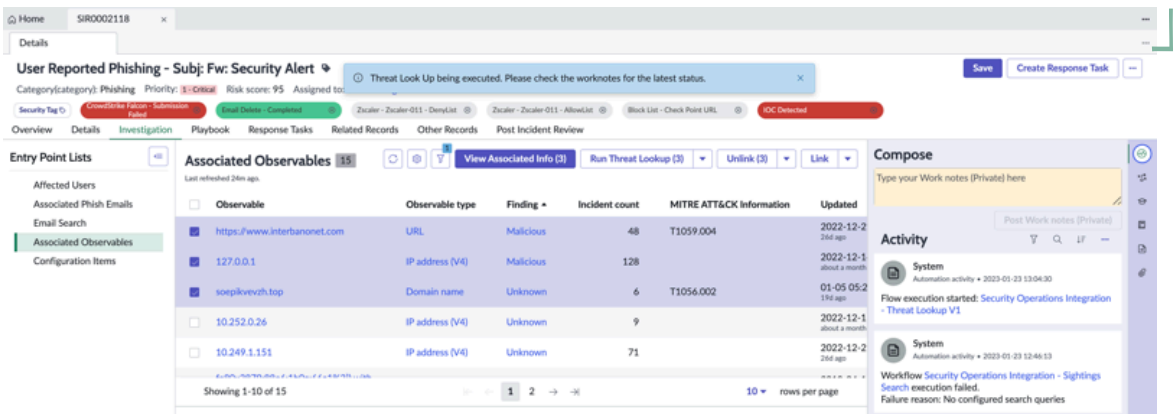
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

위협 조회 구현 실행 모달 화면이 표시됩니다.

위협 조회 구현 실행



8. 목록에서 하나 이상의 구현을 선택합니다.
9. 제출을 클릭합니다.
   선택한 기록이 제출되면 조회가 실행 중이라는 메시지가 표시됩니다. 구현이 백엔드에서 처리되면 위협 조회 결과 관련 목록 섹션에 결과가 표시됩니다. 또한 각 구현 활동이 활동 섹션에 표시됩니다. 두 가지 활동이 표시되는데, 하나는 구현 실행이 시작될 때이고 다른 하나는 실행이 완료될 때입니다.



> **주:**
> 연결된 옵저버블 관련 목록과 같은 위협 인텔리전스 관련 목록은 위협 조회 결과 섹션에 표시되고, 사이팅 검색 관련 목록은 관련 기록 아래의 사이팅 검색 결과 섹션에 표시됩니다.

예 **2:** 일반 입력: 사이팅 검색

아래 예제에서는 일반적인 입력 기능 작업을 보여 줍니다.

의 SIR Workspace조사 탭을 사용하여 사이팅 검색 관련 통합 역량 실행 작업을 수행할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

1. 조사 탭에서 페이지 왼쪽에 표시되는 엔트리포인트 목록 섹션으로 이동합니다.
2. 해당 엔트리포인트를 선택하고 통합 기능 작업을 실행합니다.

> **주:**
> 작업 공간에서 관련 기록 탭으로 이동하여 통합 기능 작업을 수행할 수도 있습니다.

구현에 일반 입력 추가

해당하는 경우 선택한 모든 구현에 적용되는 공통 실행 시간 입력을 추가합니다.

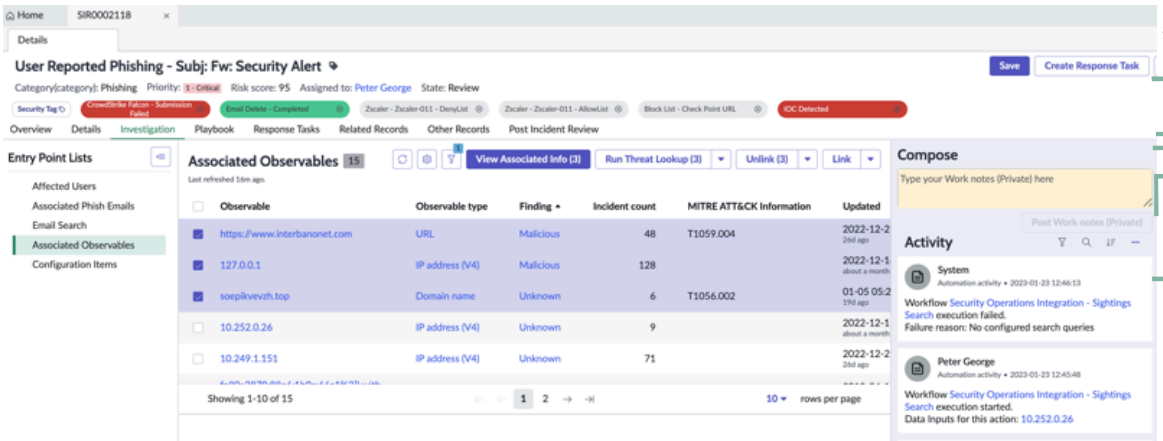
시작하기 전에

필요한 역할: sn_si.analyst

사용 가능한 구현이 나열됩니다. 구현을 선택합니다. 구현을 선택한 후에는 선택한 각 구현에 대해 지원되는 기록만 제출됩니다.

프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간.
2. 보안 인시던트를 엽니다.
3. 작업 공간의 조사 탭으로 이동합니다.
   엔트리포인트 목록이 있는 조사 탭이 표시됩니다.

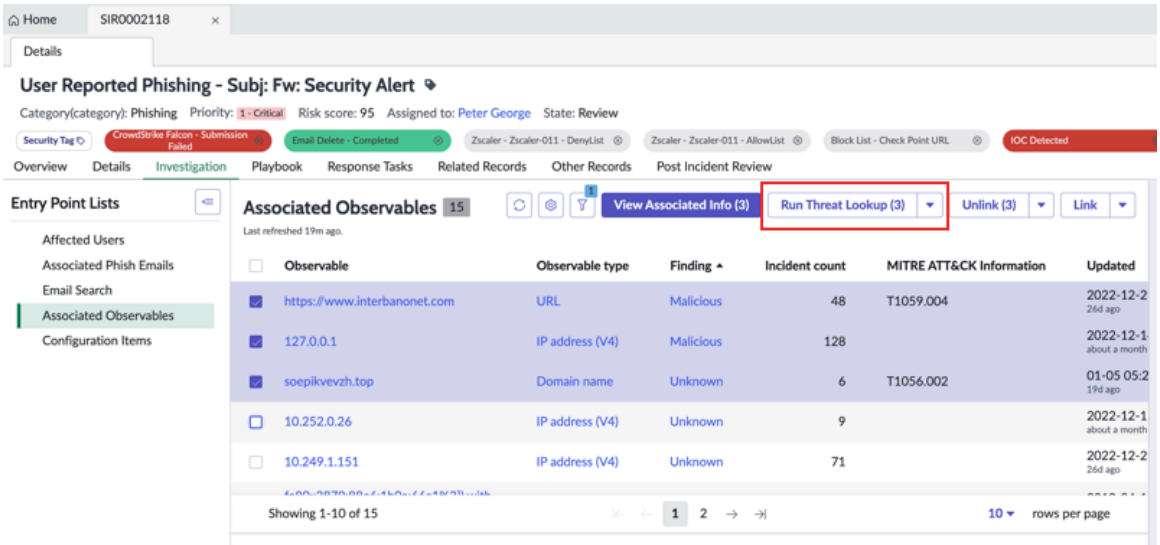


4. 엔트리포인트 목록에서 연결된 옵저버블을 선택합니다.
   예를 들어 연결된 옵저버블 관련 목록. 해당 옵저버블 기록이 표시됩니다.

> **주:**
> 선택한 옵저버블에 대한 사이팅 검색을 수행할 구현을 선택하거나 여러 구현을 선택하여 구현할 수 있습니다.

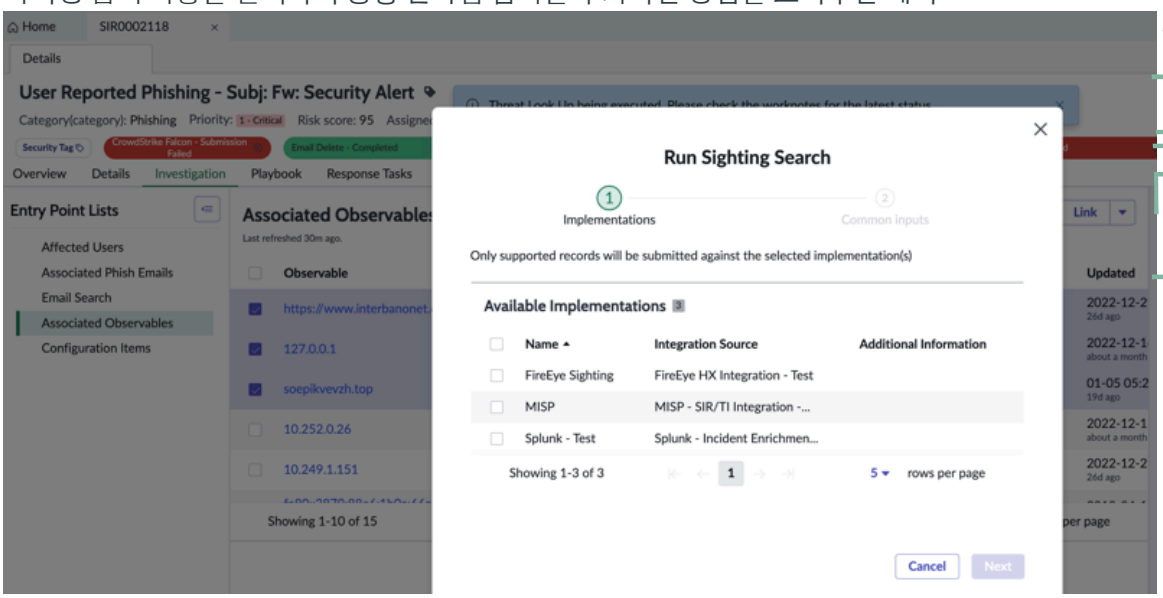
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

위협 조회 실행



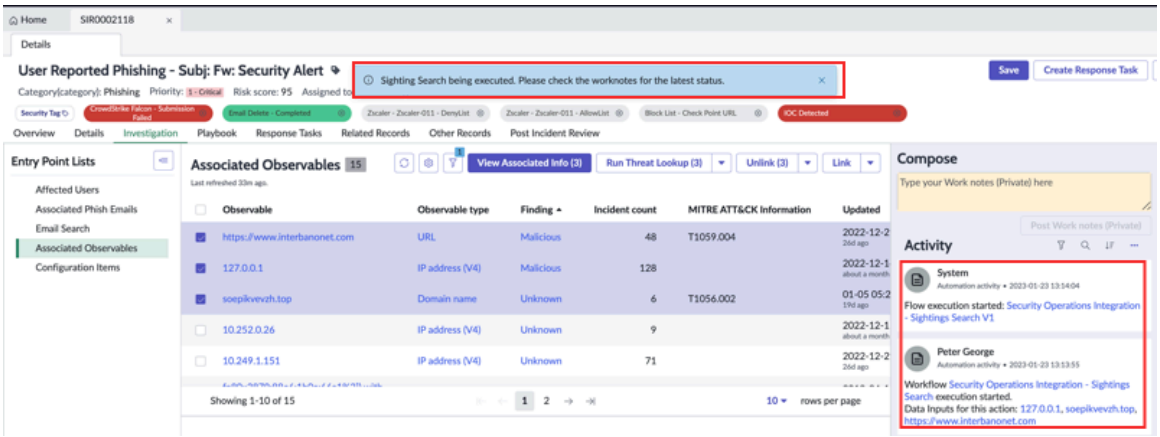
5. 위협 조회를 수행할 옵저버블 확인란을 선택합니다.
6. 이메일 검색을 수행하려면 사이팅 검색 실행을 선택합니다.
   사이팅 검색 구현 실행 모달 대화 상자가 표시됩니다.

사이팅 검색 역량을 선택하여 공통 런타임 입력을 추가하는 방법을 보여주는 예시



7. 목록에서 하나 이상의 구현을 선택합니다.
8. 다음을 클릭합니다.
   선택한 기록이 제출되면 사이팅 검색이 요청되고 있다는 메시지가 표시됩니다. 백엔드에서 구현이 처리되면 사이팅 검색 관련 목록 섹션에 결과가 표시됩니다. 또한 각 구현 활동이 활동 섹션에 표시됩니다. 두 가지 활동이 표시되는데, 하나는 구현 실행이 시작될 때이고 다른 하나는 실행이 완료될 때입니다.
9. 공통 실행 시간 입력 값을 선택합니다.
10. 제출을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



선택한 기록이 제출되면 사이팅 검색이 요청되고 있다는 메시지가 표시됩니다. 백엔드에서 구현이 처리되면 사이팅 검색 결과 관련 목록 섹션에 결과가 표시됩니다. 또한 해당 구현 활동 처리 상태가 활동 섹션에 표시됩니다.

예제 **3:** 구현에 특정 런타임 상세 정보 입력 추가: 추가 작업 실행

구현에 특정 런타임 상세 정보 입력을 추가하고 추가 작업을 실행합니다.

의 SIR Workspace조사 탭을 사용하여 추가 작업 실행 관련 통합 역량 작업을 수행할 수 있습니다.

1. 조사 탭에서 페이지 왼쪽에 표시되는 엔트리포인트 목록 섹션으로 이동합니다.
2. 해당 엔트리포인트를 선택하고 통합 기능 작업을 실행합니다.

> **주:**
> 작업 공간에서 관련 기록 탭으로 이동하여 통합 기능 작업을 수행할 수도 있습니다.

구현에 특정 입력 추가

해당하는 경우 선택한 각 구현에 대한 특정 실행 시간 입력을 추가합니다.

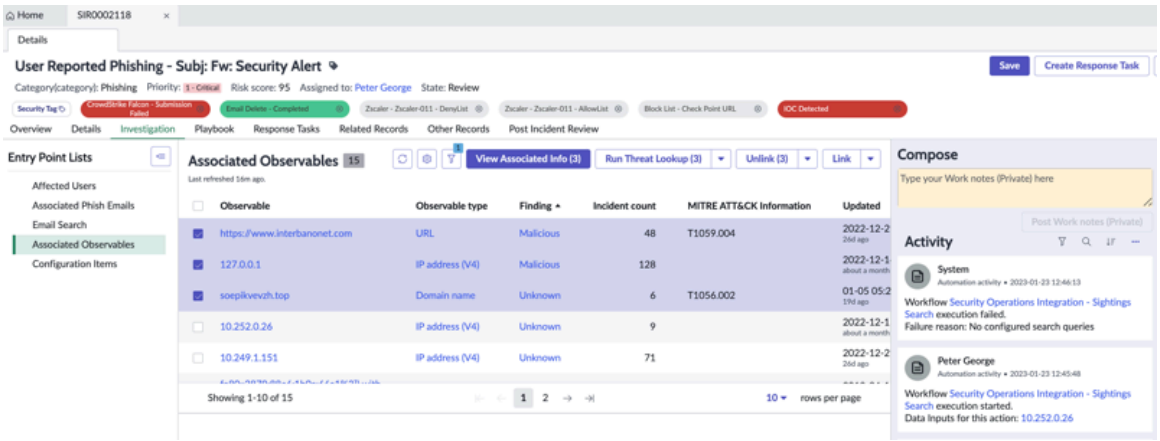
시작하기 전에
필요한 역할: sn_si.analyst

사용 가능한 구현이 나열됩니다. 구현을 선택합니다. 구현을 선택한 후에는 선택한 각 구현에 대해 지원되는 기록만 제출됩니다.

프로시저

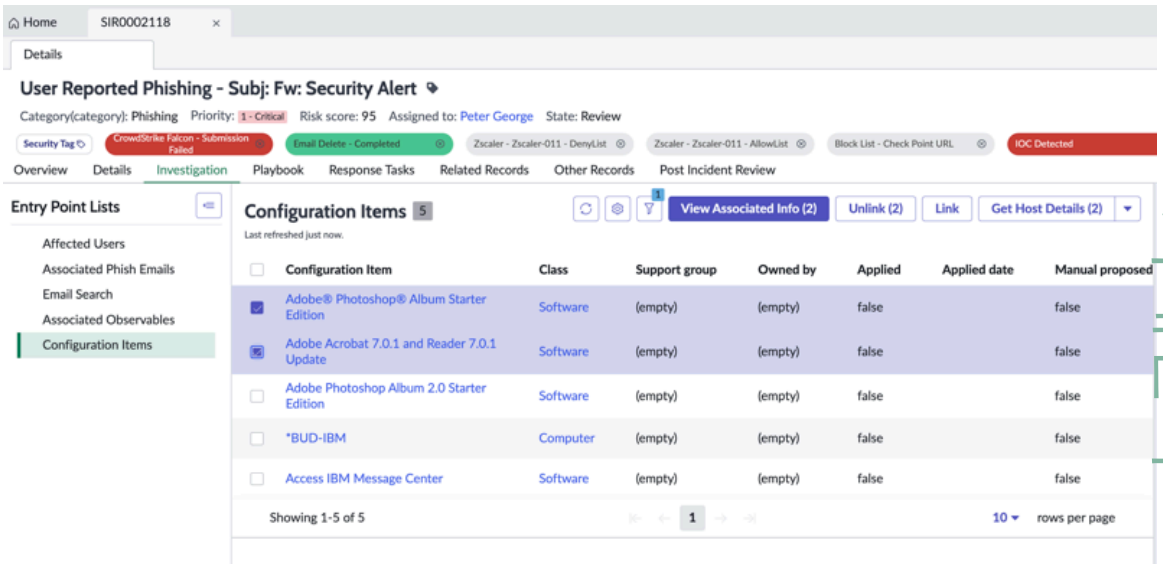
1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간.
2. 보안 인시던트를 엽니다.
3. 작업 공간의 조사 탭으로 이동합니다.
   엔트리포인트 목록이 있는 조사 탭이 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 엔트리포인트 목록에서 구성 항목을 선택합니다.
예를 들어 구성 항목 엔트리포인트 목록을 선택합니다. 해당 구성 항목 기록이 표시됩니다.

구성 항목 선택



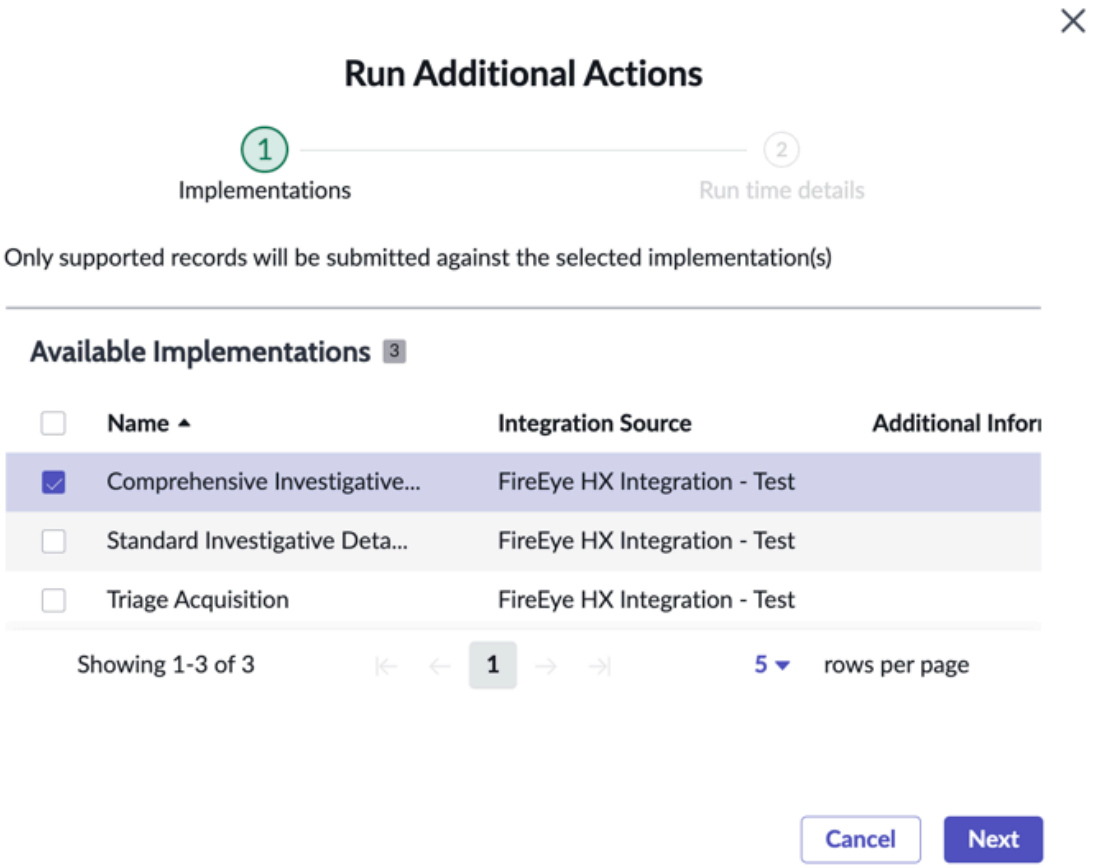
5. 구성 항목을 선택합니다.

6. 페이지 상단에 표시되는 관련 목록 드롭다운으로 이동합니다.
보안 인시던트 CI(구성 항목)의 경우 드롭다운 목록에는 다음과 같은 역량 작업 목록이 포함되어 있습니다. 나열된 CI 작업은 결과를 수집하여 보안 인시던트에 대한 보강 데이터로 저장합니다.

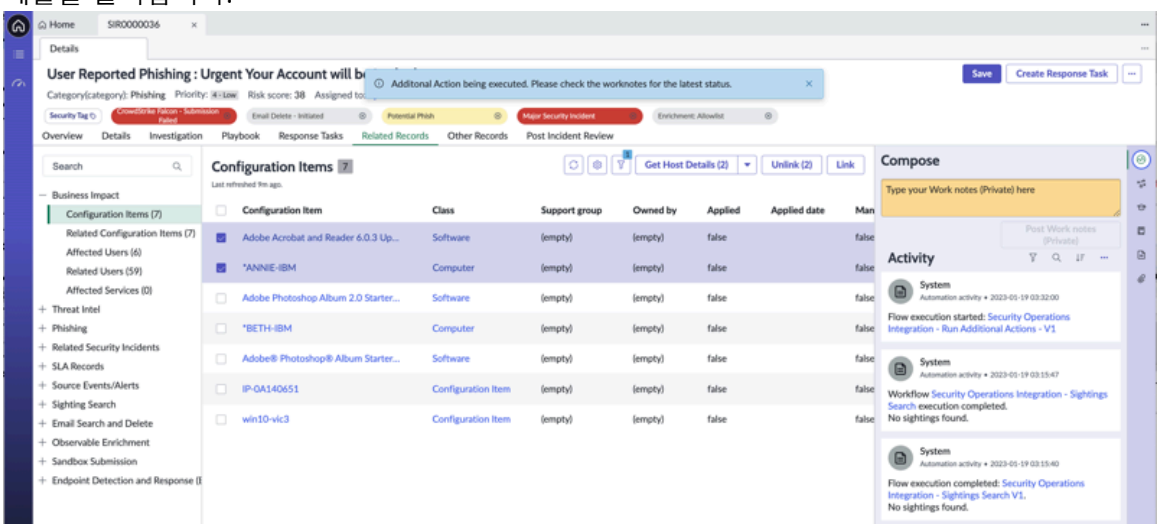
- 파일 가져오기: 이 기능은 특정 해시 값 또는 파일 이름을 가진 파일을 가져오는 작업을 수행합니다.
- 호스트 격리: 이 기능은 다른 장치에 대한 시스템 연결을 제한합니다.
- 호스트 상세 정보 가져오기: 이 기능은 호스트 상세 정보, 로그인한 사용자의 상세 정보 및 기타 보강 역량을 검색합니다.
- 추가 작업 실행: 이 기능은 표준 작업 이외의 추가 작업을 실행합니다.
- 네트워크 통계 가져오기: 이 기능은 영향을 받는 리소스에 대한 네트워크 통계를 검색합니다.
- 실행 중인 프로세스 가져오기: 이 기능은 호스트에서 CI(구성 항목)의 실행 중인 프로세스 목록을 검색합니다.
- 로그온한 사용자 가져오기: 이 기능은 로그온한 사용자의 데이터를 수집하고 보안 인시던트에 연결합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

7. 위협 인텔리전스 관련 통합 역량 작업을 수행하려면 추가 작업 실행을 선택합니다.
   추가 구현 실행 모달 대화 상자가 표시됩니다.
8. 목록에서 하나 이상의 구현을 선택합니다.



9. 다음을 클릭합니다.
   이제 실행 시간 세부 정보를 추가하기 위해 다음 단계로 이동됩니다.
10. 작업과 연결할 설명을 입력합니다.
11. 제출을 클릭합니다.



선택한 기록이 제출되면 추가 작업 요청이 실행 중이라는 메시지가 표시됩니다. 또한 각 구현 작업 진행률이 활동 섹션에 표시됩니다.

12. EDR 관련 목록 섹션에서 결과를 봅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

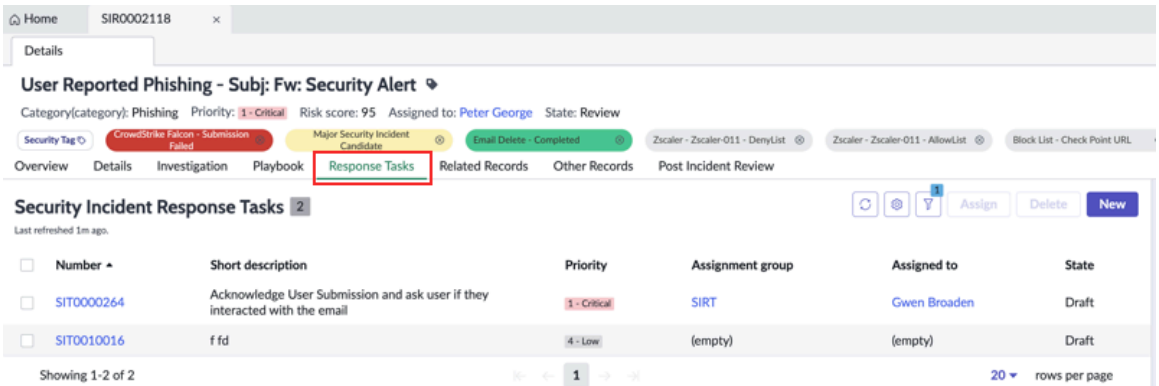
보안 인시던트 응답 작업

보안 인시던트와 연관된 모든 응답 작업이 응답 작업 섹션 내에 표시됩니다.

분석가는 다음을 수행할 수 있습니다.

- 새 응답 작업 생성
- 자신에게 또는 다른 사람에게 응답 작업 할당
- 응답 작업 삭제

작업 공간의 응답 작업



주:
응답 작업을 빠르게 편집합니다. 응답 작업을 선택하면 응답 작업 목록이 표시되면 기록을 선택하고 변경한 다음 응답 작업을 저장합니다.

응답 작업 생성

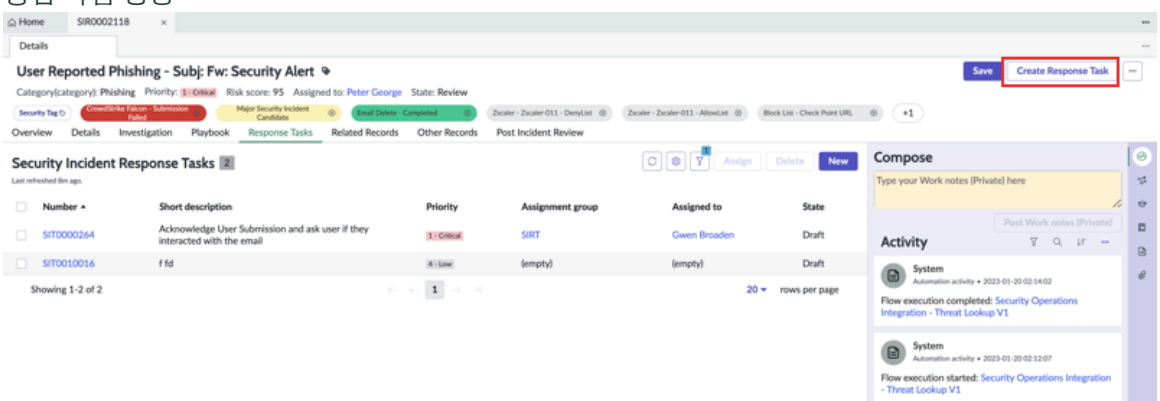
보안 문제에 대응하기 위해 수행할 별도의 작업을 추적하기 위한 응답 작업을 생성합니다.

시작하기 전에
필요한 역할: sn_si.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간.
2. UI 작업에서 응답 작업 생성을 클릭합니다.

응답 작업 생성

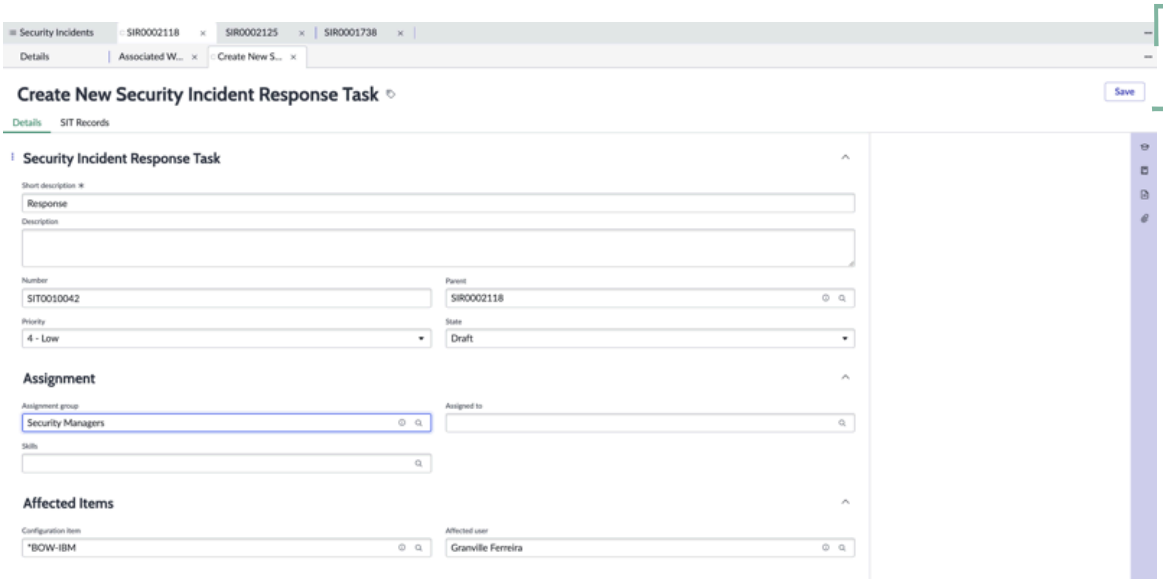


© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 양식의 필드에 적절히 입력합니다.

보안 인시던트

필드	설명
간단한 설명	작업에 대한 설명입니다 보안 인시던트 응답 .
설명	선택한 작업에 대한 설명입니다.
번호	보안 인시던트에 대해 자동으로 생성되는 고유 번호입니다.
상위	관련 보안 인시던트의 수입니다.
우선순위	이 작업이 수행되는 시기를 결정하는 데 사용되는 우선순위입니다.
상태	보안 응답 작업의 현재 상태입니다. 기본적으로 초기 상태는 초안입니다.
할당 그룹	할당된 작업자가 선택되는 할당 그룹입니다.
담당자	작업을 수행하도록 할당된 개인입니다.
기술	이 작업을 수행하는 데 필요한 기술입니다. 조회에서 검색하고 필요한 기술을 선택합니다.
영향을 받는 항목	보안 문제의 영향을 받는 항목입니다.
구성 항목	보안 문제의 영향을 받는 구성 항목입니다.
영향을 받는 사용자	보안 문제의 영향을 받는 사람입니다.



4. 저장을 클릭합니다.
새 응답 작업(SIT)이 생성됩니다.

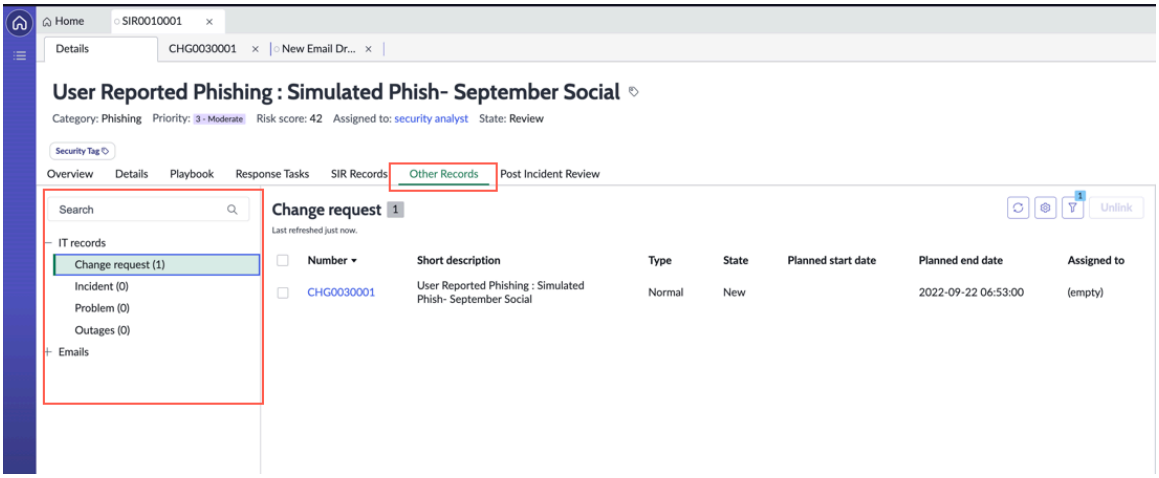
보안 인시던트 응답 기타 기록

이 섹션에는 IT 관련 기록 및 이메일 기록과 같은 기타 기록이 표시됩니다. IT 기록 아래에 인시던트, 변경 요청, 문제 및 중단이 표시됩니다.

아래에 이메일, 초안, 보낸 이메일 및 받은 이메일이 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

기타 기록



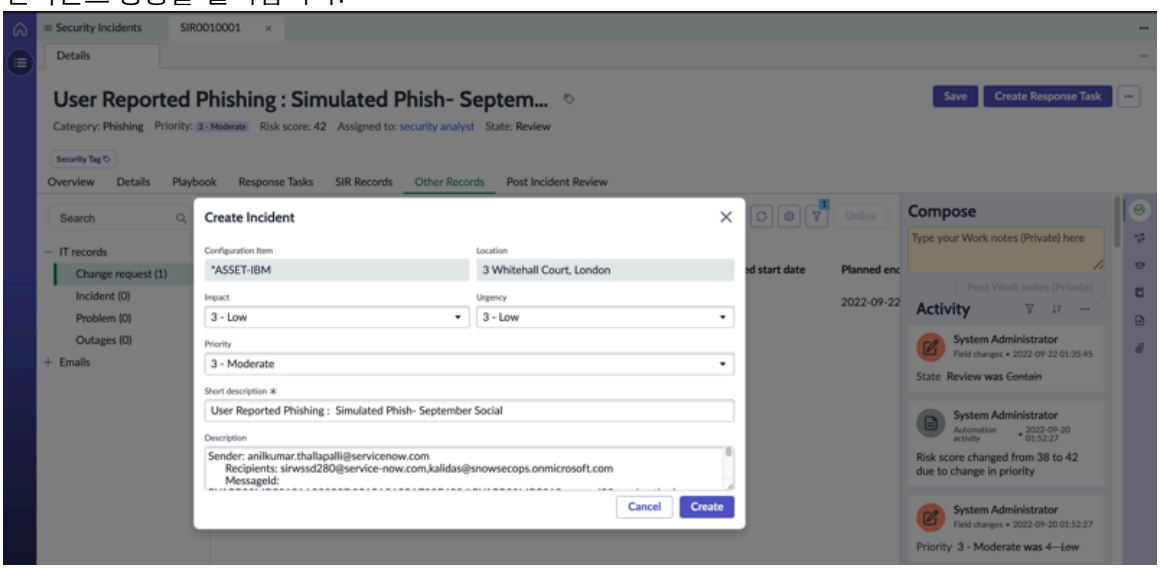
인시던트 생성

보안 인시던트 내에서 인시던트를 만듭니다.

시작하기 전에
필요한 역할: sn_si.analyst.

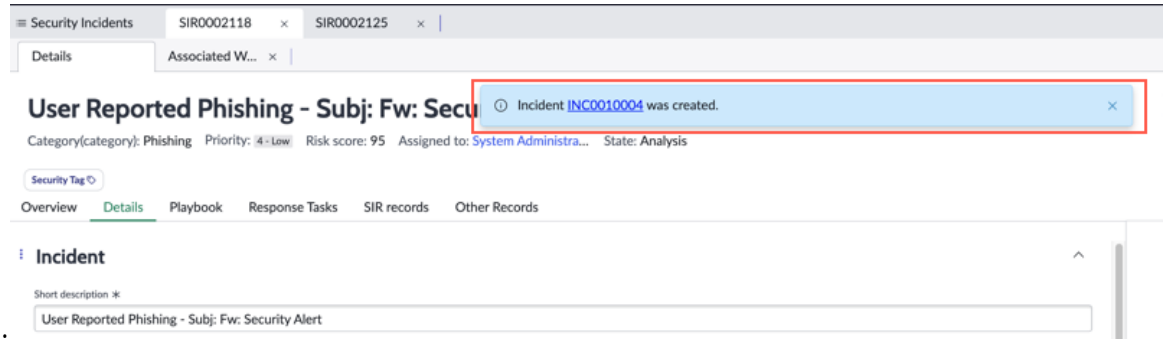
프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간.
2. 인시던트 기록을 엽니다.
3. 인시던트 생성을 클릭합니다.



4. 구성 항목, 영향도, 긴급도, 위치, 우선순위 및 간단한 설명과 같은 상세 정보를 입력합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. 생성을 

클릭합니다.

6. 인시던트가 생성됩니다.

여러 **ITSM** 인시던트 연결

보안 인시던트와 관련된 인시던트를 연결 IT Service Management (ITSM) 합니다.

시작하기 전에

주:
보안 인시던트에 연결할 인시던트를 생성할 ITSM 수도 있습니다. 자세한 내용은 인시던트 생성 문서를 참조하십시오.

필요한 역할: sn_si.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간.
2. 목록 아이콘 (아이콘.
3. 인시던트 기록을 엽니다.
4. 기타 기록 탭을 선택합니다.
5. **IT** 기록에서 인시던트를 선택합니다.

   주:
   클래식 UI로 전환하면 관련 기록 탭에서 인시던트 필드가 제거됩니다.

6. 링크를 선택합니다.
7. 선택한보안 인시던트에 연결할 인시던트를 선택합니다ITSM.
8. 링크를 선택합니다.

결과

선택한 ITSM 인시던트가 선택한 보안 인시던트 기록의 IT 기록 섹션에 나열됩니다 .

문제 작업 생성

문제 작업을 생성합니다.

시작하기 전에

필요한 역할: sn_si.analyst

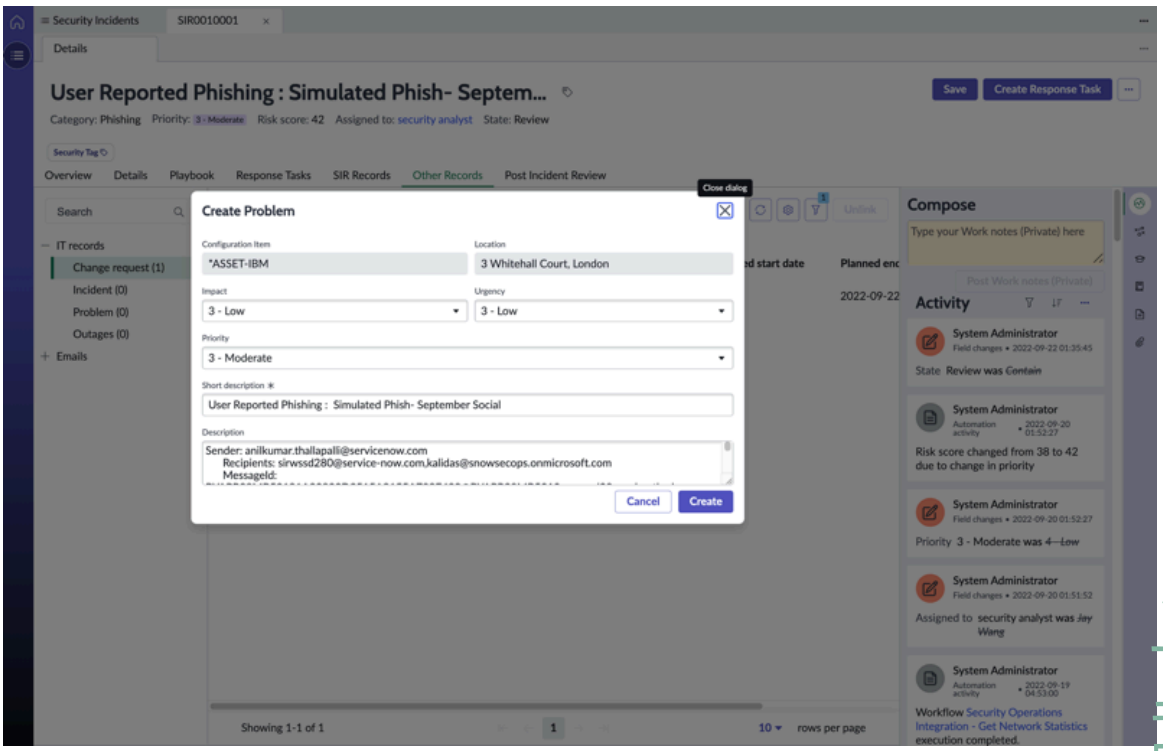
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간.

2. 인시던트 기록을 엽니다.

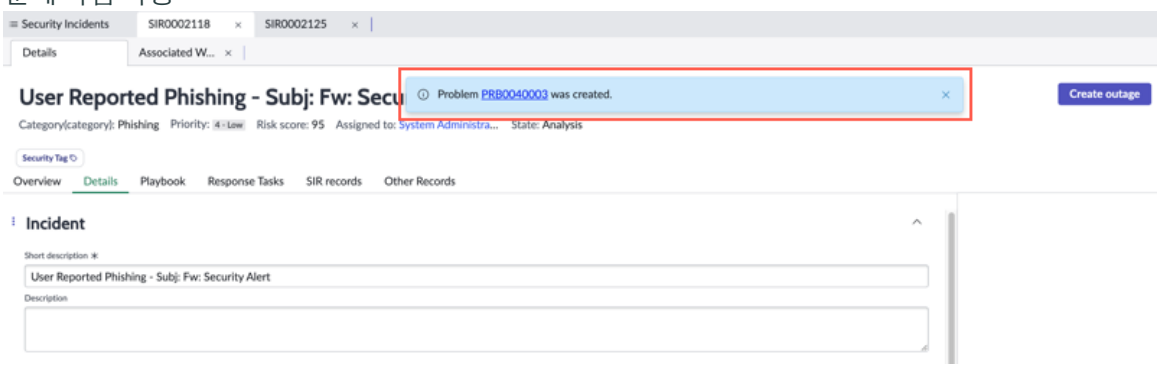
3. 문제 생성을 클릭합니다.



4. 구성 항목, 위치, 영향, 긴급도, 우선순위 및 짧은 설명과 같은 상세 정보를 입력합니다.

5. 생성을 클릭합니다.

문제 작업 작성



6. 문제 작업이 생성됩니다.

변경 요청 만들기

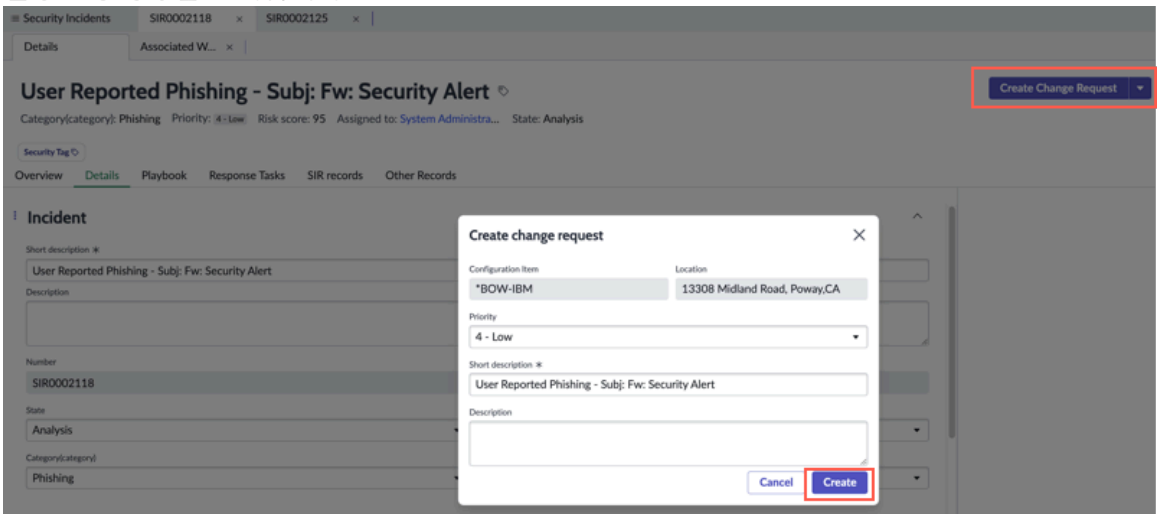
변경 요청을 생성합니다.

시작하기 전에
필요한 역할: sn_si.analyst.

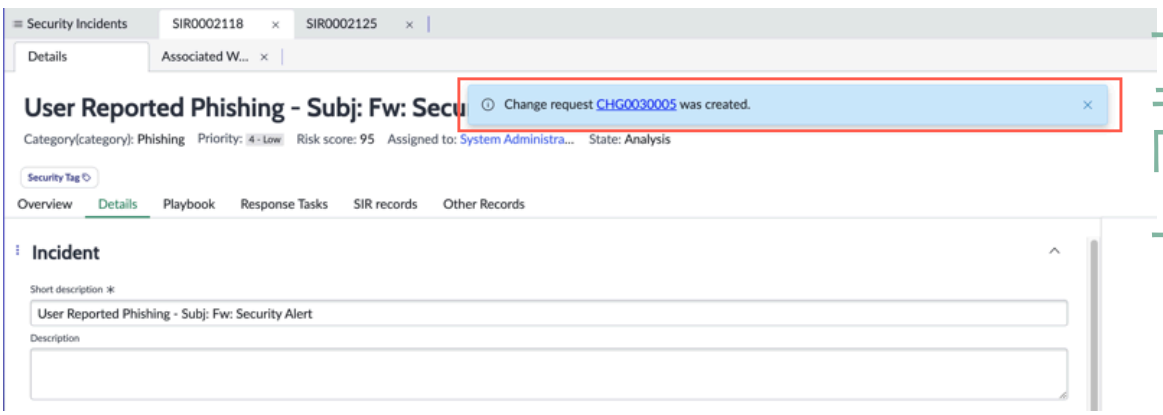
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간.
2. 인시던트 기록을 엽니다.
3. 변경 요청 생성을 클릭합니다.



4. 구성 항목, 위치, 우선순위 및 간단한 설명과 같은 상세 정보를 입력합니다.
5. 생성을 클릭합니다.



6. 변경 요청이 생성됩니다.

중단 생성

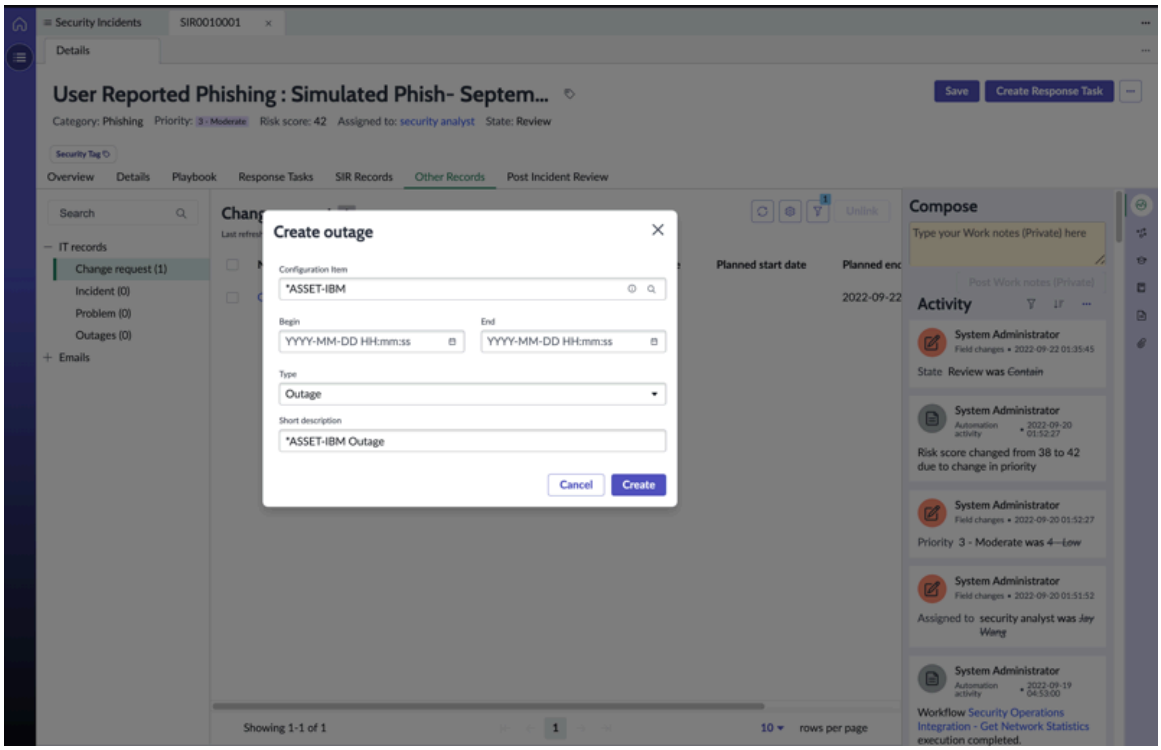
인시던트의 중단을 생성하여 구성 항목의 중단 시간을 추적합니다.

시작하기 전에
필요한 역할: sn_si.analyst

프로시저

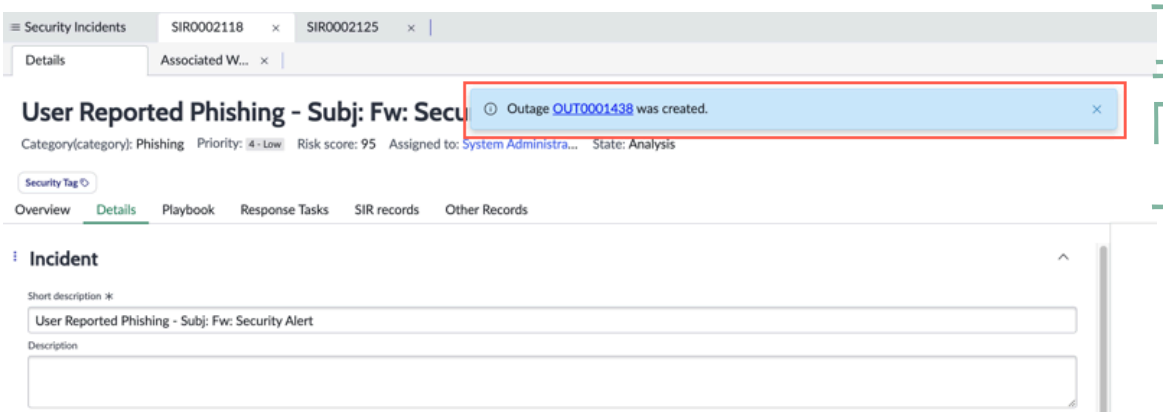
1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간.
2. 인시던트 기록을 엽니다.
3. 중단 생성을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 구성 항목, 시작 날짜, 종료 날짜, 유형 및 간단한 설명과 같은 상세 정보를 입력합니다.

5. 생성을 클릭합니다.



이메일 작성

분석가는 보안 인시던트에서 직접 이메일을 작성할 수 있습니다.

시작하기 전에

필요한 역할: sn_si.analyst

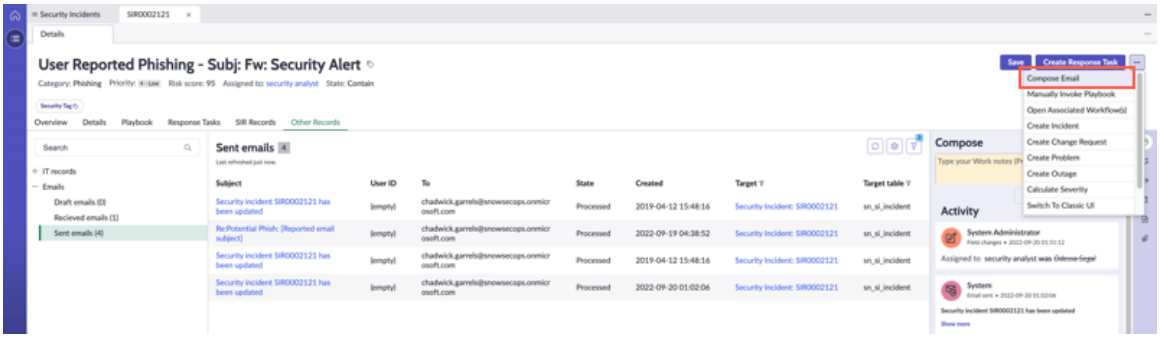
프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간.

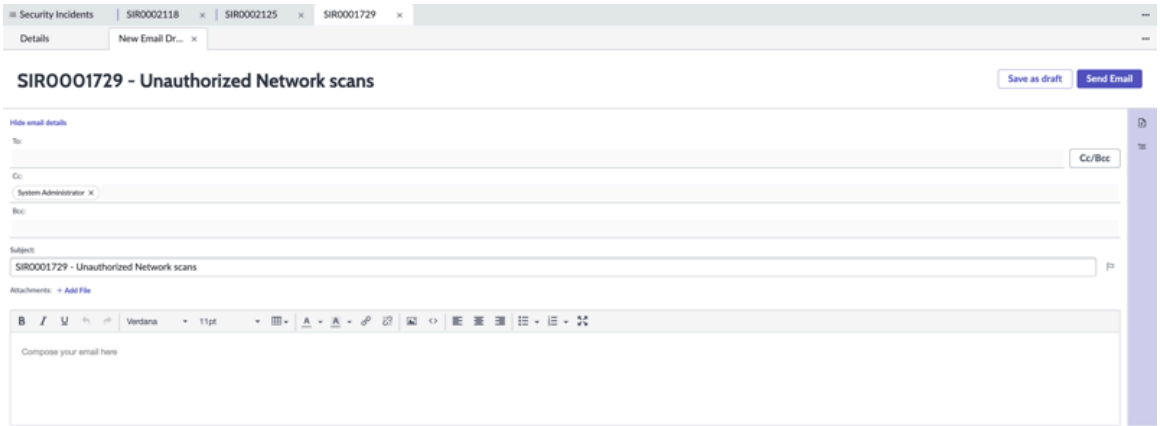
2. 이메일을 작성하려는 인시던트를 선택하여 엽니다.

3. 오버플로우를 클릭하고 이메일 작성을 선택합니다.

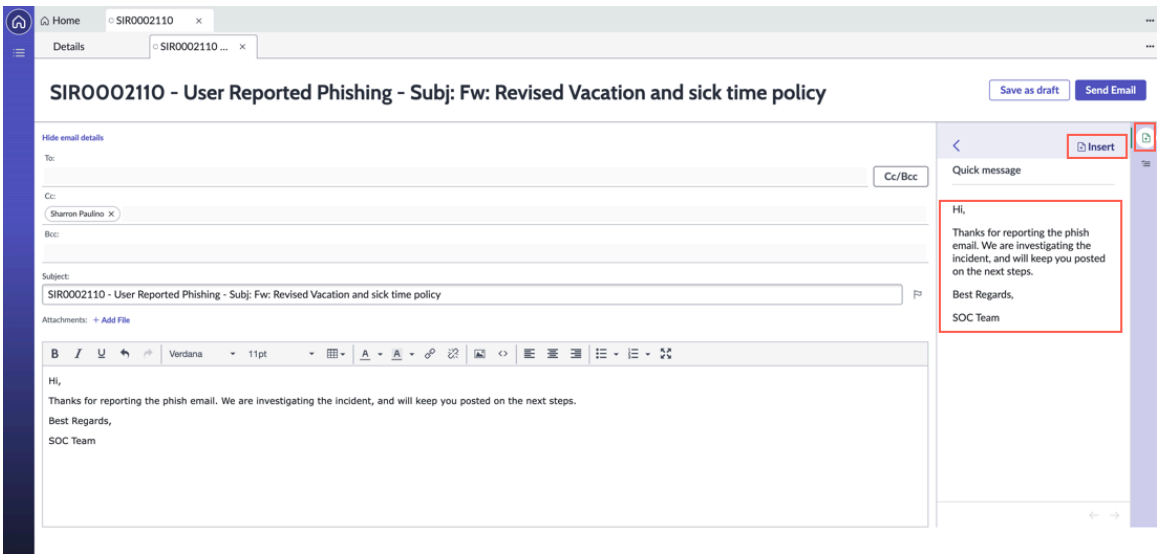
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 받는 사람 및 참조 필드를 입력합니다.



5. 첨부 파일을 추가합니다(있는 경우).
6. 이메일 양식에서 빠른 메시지를 클릭하여 이메일 작성 섹션의 오른쪽에 표시되는 빠른 메시지를 봅니다.
   사용 가능한 빠른 메시지가 표시됩니다. 메시지를 선택하고 삽입을 클릭합니다. 메시지가 이메일 본문에 삽입됩니다.



7. 이메일을 작성하고 이메일 보내기를 클릭합니다.

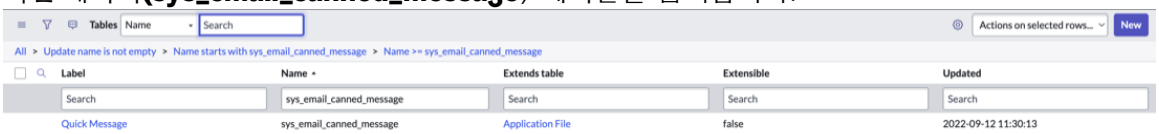
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
이메일을 초안으로 저장할 수 있습니다. 이러한 초안 이메일은 기타 기록 탭에서 사용할 수 있습니다.

빠른 메시지를 구성하는 방법:

a. 다음으로 이동 시스템 정의 〉 테이블.

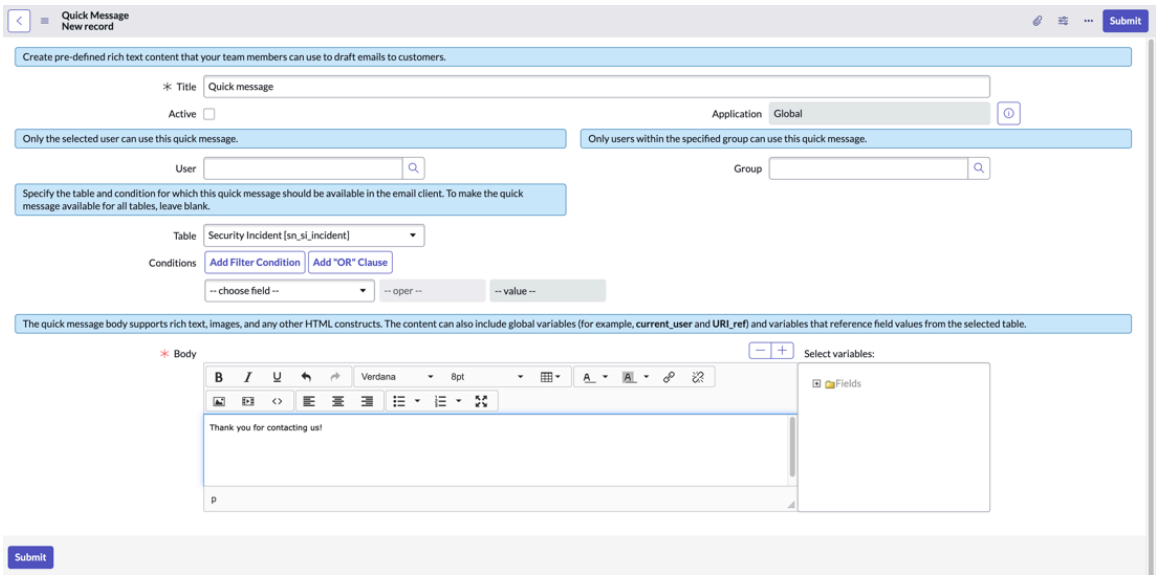
b. 빠른 메시지**(sys_email_canned_message**) 테이블을 검색합니다.



c. 이동 관련 링크 〉 목록 보기.

d. 새로 만듭니다.

e. 제목과 메시지 본문을 입력하고 테이블: 보안 인시던트**(sn_si_incident)** 및 활성 확인란을 선택합니다.

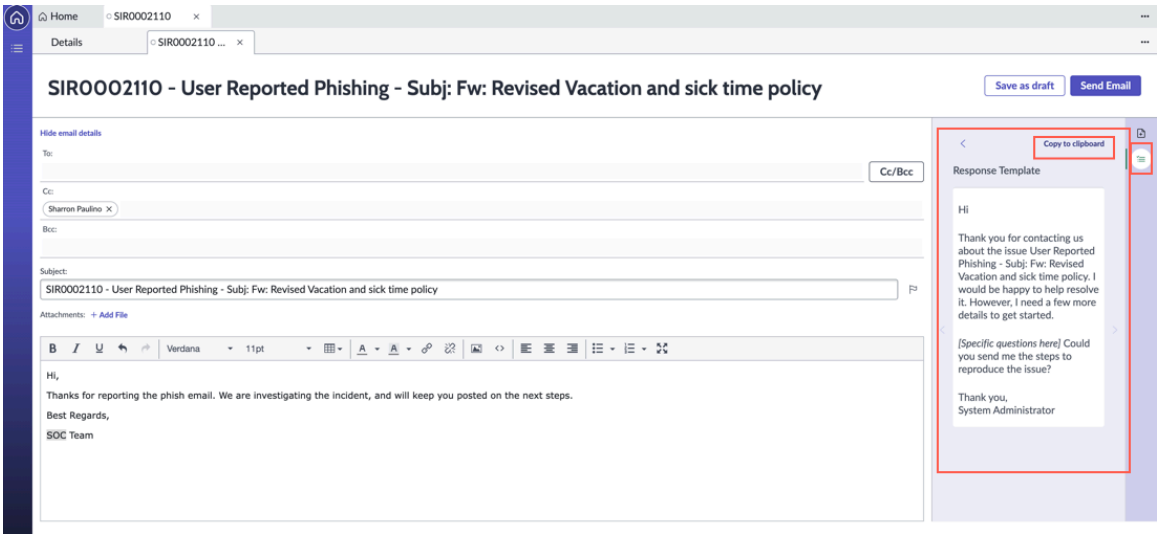


f. 제출을 클릭합니다.
테이블 내에 새 항목이 생성되면 상황별 메뉴에 빠른 메시지가 나타납니다.

8. 필요한 경우 템플릿을 클릭하여 템플릿을 추가합니다.

9. 응답 템플릿을 선택하고 클립보드에 복사를 클릭한 후 필요한 경우 템플릿을 적용합니다.

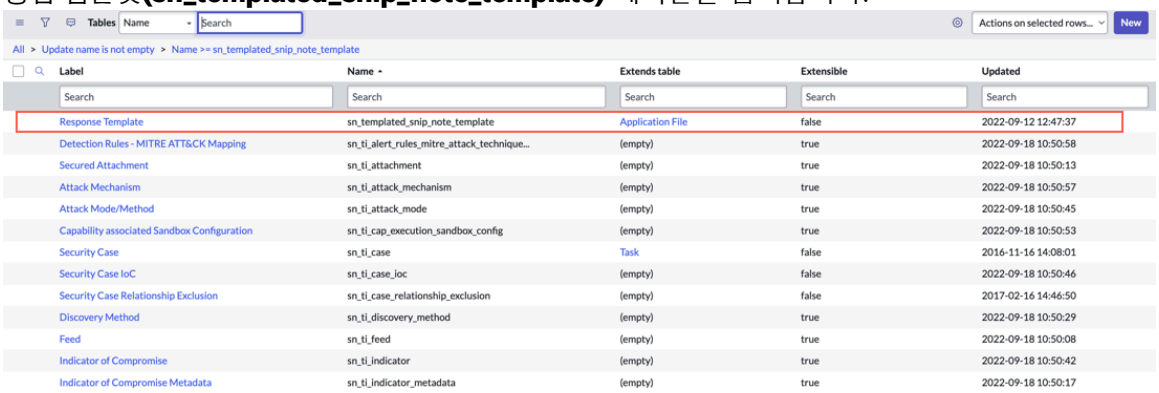
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



응답 템플릿을 구성하는 방법:

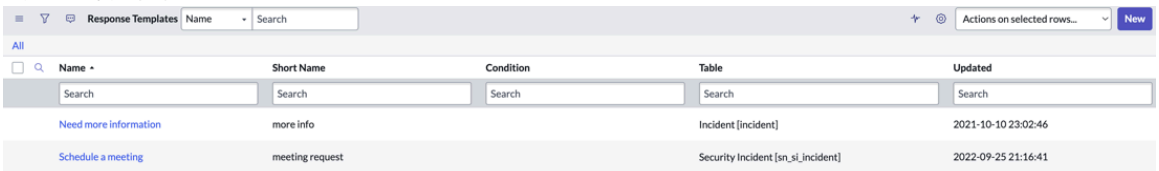
a. 다음으로 이동 시스템 정의 〉 테이블.

b. 응답 템플릿**(sn_templated_snip_note_template)** 테이블을 검색합니다.



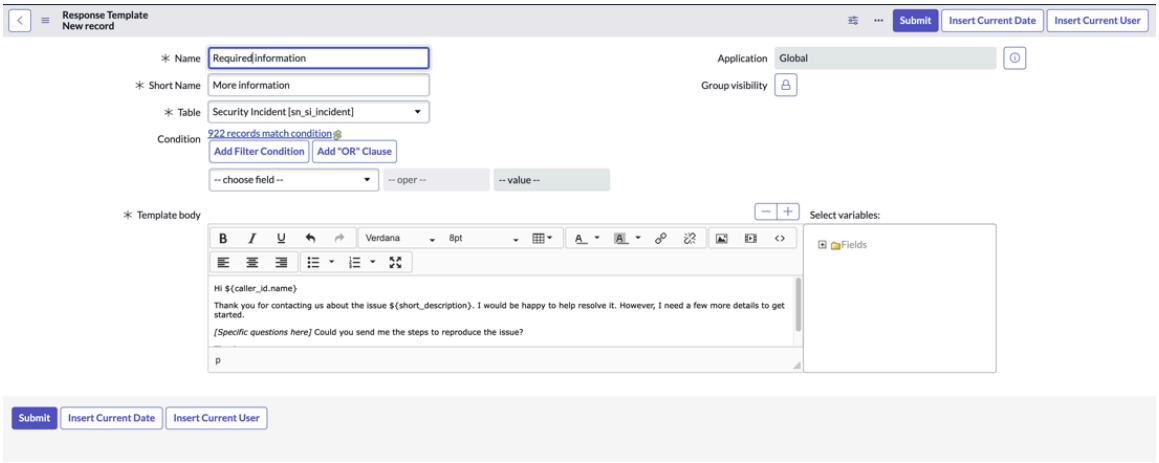
c. 이동 관련 링크 〉 목록 보기.

d. 새로 만듭니다.



e. 이름, 짧은 이름을 입력하고 테이블: 보안 인시던트**(sn_si_incident)** 및 템플릿 본문을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



f. 제출을 클릭합니다.
테이블 내에 새 항목이 생성되면 상황별 메뉴에 새 템플릿이 나타납니다.

보안 인시던트 응답 게시 인시던트 검토

인시던트가 검토 상태로 이동하면 사후 인시던트 검토가 표시됩니다.

사후 인시던트 활동 수행에 대한 자세한 내용은 다음을 참조하십시오. 사후 인시던트 검토 보고서

사후 인시던트 검토는 다음 섹션으로 구성됩니다.

1. 평가
2. 보고서

보안 인시던트 응답 작업 공간에서 이 새로운 두 가지 UI 작업을 사용하여 평가를 요청하고 수행할 수 있습니다.

이름	설명
평가	평가에는 보안 인시던트 기타 평가와 관련된 모든 평가가 표시됩니다. 분석가는 평가를 수행하고 평가를 요청할 수 있습니다. • 평가 수행: 평가 수행 을 클릭하여 평가를 수행하고(해당되는 경우) 평가를 완료합니다. 평가를 완료하기 전에 보안 인시던트 상태는 수행 준비이며 인시던트 기한은 빨간색으로 표시됩니다. • 평가 요청: 추가 평가를 위해 평가 요청을 클릭하고 요청하려는 새 사용자를 추가할 수 있습니다. 주: 이미 요청한 사용자는 이 섹션에 표시되지 않습니다. 이 인시던트에 대한 평가는 사후 인시던트 검토에 설정된 조건을 기반으로 구성되며, 필수 또는 선택 사항입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이름	설명
보고서	런타임 구성을 수정하고 보고서를 생성합니다. 보고서 인스턴스를 선택하고 필터를 수정한 다음 보고서를 저장합니다. 분석가는 PIR 보고서를 미리 보고 다운로드할 수 있습니다.

SIR 작업 공간 내에서 **TISC** 통합

다음 섹션에는 SIR 작업 공간 컨텍스트 내에서 Threat Intelligence Security Center 통합에 대한 정보가 포함되어 있습니다.

SIR 작업 공간에서 TISC로 데이터 보내기

다음 섹션에 설명된 절차에 따라 Threat Intelligence Security Center(TISC)와 Security Incident Response(SIR) 작업 공간 간에 데이터가 공동 작업되고 공유되는 방법을 알아봅니다.

데이터 전송을 위한 시스템 속성

SIRW와 결합할 TISC 통합에 대한 시스템 속성을 검토합니다. 이러한 속성을 구성하여 두 애플리케이션에서 통합을 관리하는 방법을 제어할 수 있습니다.

주요 고려 사항

TISC 통합을 위한 시스템 속성은 애플리케이션이 옵저버블 및 보강을 처리하는 방법에 대한 고급 구성 옵션을 제공합니다.

1. SIRW 내에서 TISC 통합 시스템 속성을 설정하려면 위협 인텔리전스에 대한 시스템 속성 으로 이동하여 [sys_properties] 테이블에 액세스합니다.
2. 시스템 속성은 각 개별 데이터 푸시 작업의 동작을 제어하고 처리합니다.
3. 이 속성을 활성화하면 SIR 작업 공간에서 옵저버블 또는 보강 데이터가 생성될 때 데이터가 자동으로 푸시됩니다.
4. 이 속성을 사용하지 않도록 설정하면 데이터가 수동으로 푸시되고 사용자가 SIR 작업 공간에서 UI 작업을 사용하여 데이터를 푸시할 수 있습니다.

다음 목록은 TISC - SIR 통합을 위한 시스템 속성을 보여줍니다.

- SIR에서 옵저버블 데이터를 자동 및 수동으로 푸시: 데이터를 자동 또는 수동으로 푸시하려면 sn_ti.allow_observable_and_enrichment_records_push 속성을 활성화합니다. 사용하지 않도록 설정하면 이 속성은 SIR의 모든 데이터 푸시에 대해 자동 모드와 수동 모드를 모두 사용하지 않도록 설정합니다.
- 위협 조회 결과 푸시: 위협 조회 데이터를 TISC에 자동으로 푸시하려면 이 sn_ti.automatic_push_threat_lookup_results 시스템 속성을 활성화합니다. 비활성화된 경우에도 보안 분석가는 위협 조회 데이터를 수동으로 푸시할 수 있습니다.
- 사이팅 검색 결과를 TISC로 푸시: sn_ti.automatic_push_sighting_results_to_tisc 이 시스템 속성을 활성화하여 사이팅 검색 데이터를 TISC에 자동으로 푸시합니다. 비활성화된 경우에도 보안 분석가는 사이팅 검색 데이터를 수동으로 푸시할 수 있습니다.
- 옵저버블 푸시: 옵저버블 데이터를 TISC에 자동으로 푸시하려면 이 시스템 속성인 sn_ti.automatic_push_observable_to_tisc를 활성화합니다. 사용하지 않도록 설정한 경우에도 보안 분석가는 옵저버블 데이터를 수동으로 푸시할 수 있습니다.
- 보강 결과 푸시: sn_ti.automatic_push_enichment_results 이 시스템 속성을 활성화하여 보강 결과 데이터를 TISC에 자동으로 푸시합니다. 비활성화된 경우에도 보안 분석가는 보강 결과 데이터를 수동으로 푸시할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

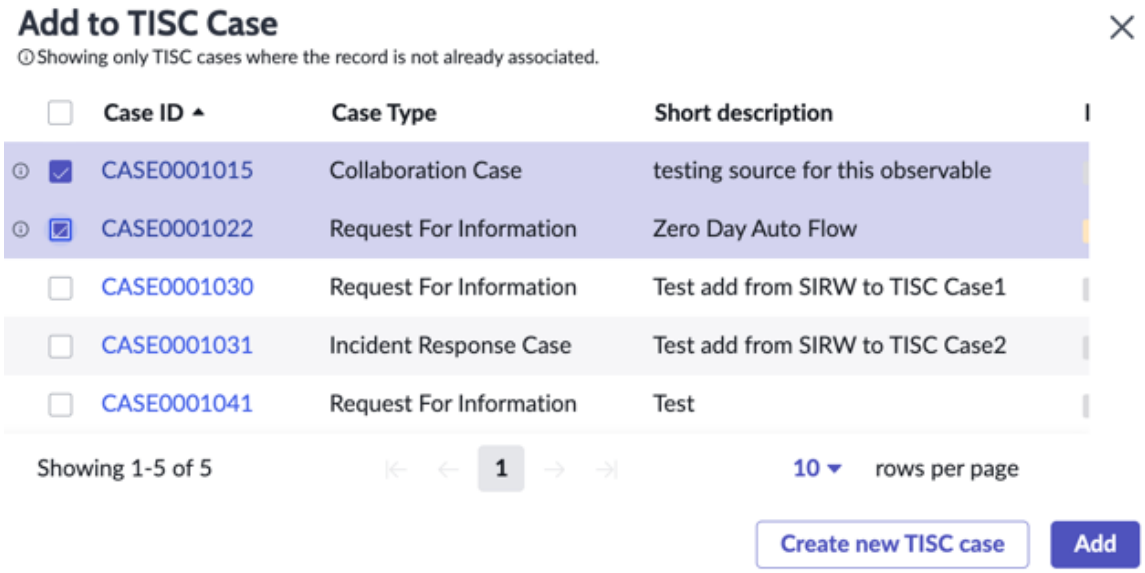
TISC 케이스에 보안 인시던트 추가

TISC 케이스 기록에 보안 인시던트를 추가합니다.

시작하기 전에
필요한 역할: sn_si.analyst, sn_sec_tisc.case_write

프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간 〉 보안 인시던트 〉 모두.
2. 조사 중인 특정 보안 인시던트를 찾아서 엽니다.
   인시던트 ID를 검색하거나, 빠른 필터 섹션에서 찾아보거나, 인시던트 상태를 통해 필터링하여 이 작업을 수행할 수도 있습니다.
3. 추가 작업 아이콘을 클릭합니다.
4. **TISC** 케이스에 추가 작업을 클릭합니다.
   TISC 케이스에 추가 대화 상자가 표시되고 여기에는 인시던트가 아직 연결되지 않은 TISC 케이스만 표시됩니다.
5. 케이스에 추가 대화 상자에서 케이스를 선택합니다.



> **주:**
> 케이스 기록이 없는 경우 새 TISC 케이스를 생성합니다. 케이스를 만드는 방법에 대한 자세한 내용은 을 참조하십시오 위협 분석가 워크벤치를 사용하여 케이스 생성.

6. 추가를 클릭합니다.
7. 케이스 기록을 클릭하여 표시된 정보 메시지나 활동 스트림에서 TISC의 케이스를 봅니다.

> **주:**
> 연결된 보안 인시던트를 보려면 보안 인시던트 활동 스트림에서 특정 케이스 기록을 클릭합니다. 이 버튼을 클릭하면 TISC 작업 공간의 케이스 기록으로 이동되고 케이스 관리 모듈의 아티팩트 탭에 보안 인시던트가 추가됩니다.

TISC 케이스에 옵저버블 추가

TISC 케이스 기록에 옵저버블을 추가합니다.

시작하기 전에
필요한 역할: sn_si.analyst, sn_sec_tisc.case_write

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

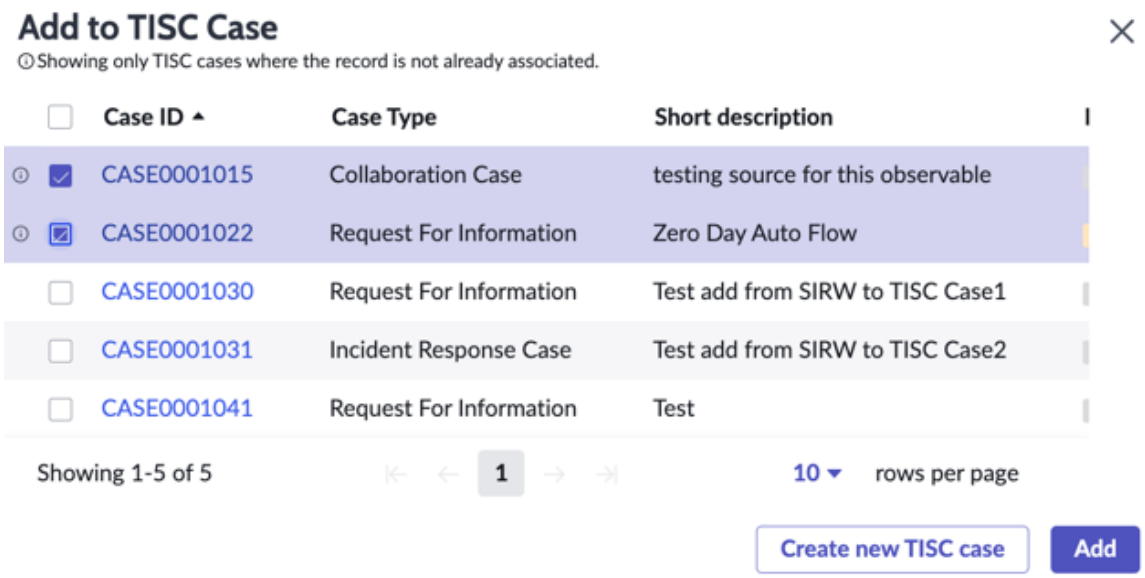
1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간 〉 보안 인시던트 〉 모두.
2. 조사 중인 특정 보안 인시던트를 찾아서 엽니다.
   인시던트 ID를 검색하거나, 빠른 필터 섹션에서 찾아보거나, 인시던트 상태를 통해 필터링하여 이 작업을 수행할 수도 있습니다.
3. 작업 공간에서 관련 기록 탭을 클릭합니다.
   보안 인시던트 응답 작업 공간의 다양한 탭을 사용하여 TISC 케이스에 옵저버블을 추가하는 작업을 수행할 수 있습니다.

   주:
   다음으로 이동합니다.
   - 관련 기록 탭의 옵저버블 상세 정보 페이지.
   - 조사 탭에서 페이지 왼쪽에 표시된 엔트리포인트 목록 섹션으로 이동하고 연결된 옵저버블을 선택하여 TISC 케이스에 옵저버블을 추가합니다.

4. 예를 들어 위협 인텔리전스 〉 연결된 옵저버블.
5. 선택한 옵저버블을 케이스 기록에 추가하려면 옵저버블을 하나 또는 여러 개 선택하십시오.

   주:
   옵저버블 기록을 클릭하면 다른 탭에 옵저버블 상세 페이지가 열리고, TISC 케이스에 추가를 클릭하여 여기에서 케이스 기록을 추가할 수 있습니다.

6. 역량 작업 분할 버튼을 클릭합니다.
7. **TISC** 케이스에 추가를 선택합니다.
8. 케이스에 추가 대화 상자에서 케이스를 선택합니다.



   주:
   케이스 기록이 없는 경우 새 TISC 케이스를 생성합니다. 케이스를 만드는 방법에 대한 자세한 내용은 을 참조하십시오 위협 분석가 워크벤치를 사용하여 케이스 생성.

9. 추가를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

10. 케이스 기록을 클릭하여 표시된 정보 메시지나 활동 스트림에서 TISC의 케이스를 봅니다.

> **주:**
> 옵저버블에 해당 TISC 옵저버블이 없는 경우 SIR 작업 공간에서 선택한 옵저버블이 자동으로 TISC로 전송되고 이후에 선택한 TISC 케이스 기록에 추가됩니다. 연결된 옵저버블을 보려면 활동 스트림에서 특정 케이스 기록을 클릭합니다. 이 버튼을 클릭하면 TISC 작업 공간의 케이스 기록으로 이동되고 케이스 관리 모듈의 아티팩트 탭에 옵저버블이 추가됩니다.

결과
옵저버블 데이터를 위협 인텔리전스 보안 센터 케이스 관리로 성공적으로 보냈습니다.

TISC에 옵저버블 보내기

이 기능을 사용하여 보안 분석가는 옵저버블 데이터를 SIR에서 TISC로 푸시할 수 있습니다. TISC 컨텍스트를 사용하면 옵저버블이 TISC에 있는지 확인할 수 있으며, 그렇지 않은 경우 보안 분석가가 필요할 때마다 데이터를 푸시할 수 있습니다.

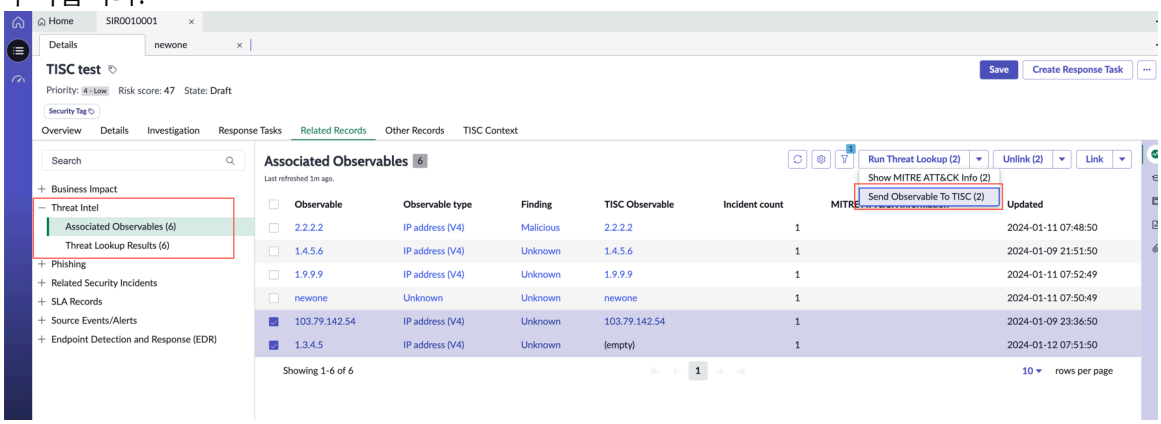
시작하기 전에
필요한 역할: sn_si.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간 〉 보안 인시던트 〉 모두.
2. 보안 인시던트를 엽니다.
3. 관련 기록 탭을 선택하여 TISC 통합 기능 작업을 수행합니다.

> **주:**
> - 조사 탭으로 이동하여 페이지 왼쪽에 표시된 엔트리포인트 목록 섹션으로 이동하고 연결된 옵저버블을 선택하여 푸시 작업을 수행할 수도 있습니다.
> - 조사 탭에서 관련 정보 보기를 선택하여 선택한 옵저버블에 대한 모든 관련 위협 조회, 사이팅 검색 및 보강 데이터를 봅니다. 자세한 내용은 조사 캔버스 탐색 문서를 참조하십시오.

4. 예를 들어 위협 인텔리전스 〉 연결된 옵저버블 밀어넣기 작업을 수행하고 데이터를 TISC에 수동으로 푸시합니다.
5. 수행할 옵저버블 기록을 하나 이상 선택하여 TISC에 옵저버블 전송 작업을 수행하여 데이터를 푸시합니다.



6. TISC에 옵저버블 보내기를 선택합니다.
7. TISC에 옵저버블 보내기 화면에서 다음을 제공합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

TISC 옵저버블에 정보 추가

필드	설명
신뢰도	옵저버블에 대한 신뢰도 점수입니다.
TLP	옵저버블에 대한 TLP(Traffic Light Protocol) 값입니다.
메모	옵저버블에 대한 메모입니다.
TISC 태그	전송할 옵저버블의 태그입니다. 옵저버블에 추가되는 사용자 지정 태그를 추가할 수 있습니다.

8. 보내기를 선택합니다.

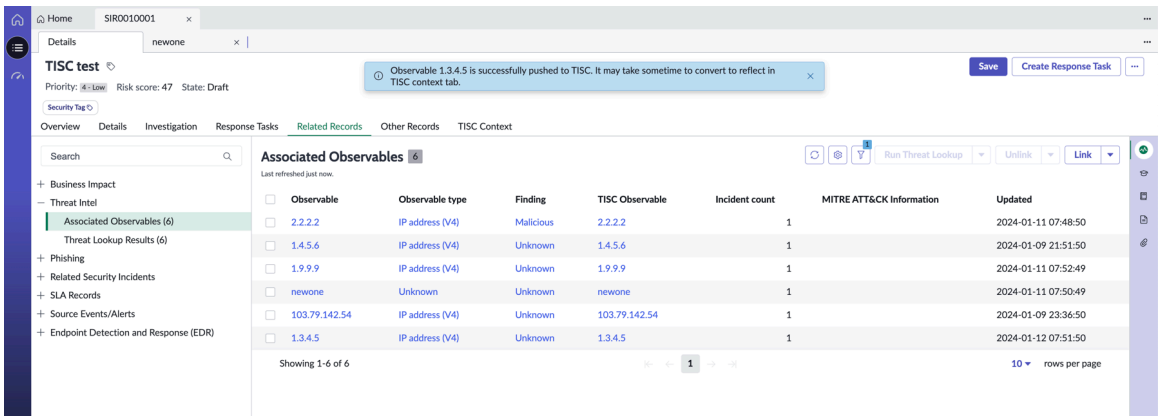
주:

- 선택한 옵저버블이 TISC에 없는 경우 먼저 옵저버블이 옵저버블 소스로 생성된 다음, 소스 옵저버블이 TISC 옵저버블 기록을 생성하면 옵저버블 기록이 새로 생성된 옵저버블과 자동으로 연결됩니다.
- 옵저버블 푸시 작업이 수행되면 정보 메시지가 표시됩니다.

  ## ☒☒☒☒☒ TISC☒ ☒☒☒☒☒ ☒☒☒☒☒☒☒. TISC ☒☒☒☒ ## ☒☒☒☒ # ### ## ## # ☒☒☒☒. 0.0.0.0

- 옵저버블이 이미 TISC인 경우 오류 메시지가 표시됩니다.

  ## ☒☒☒☒☒ TISC☒ ## ##: 0.0.0.0

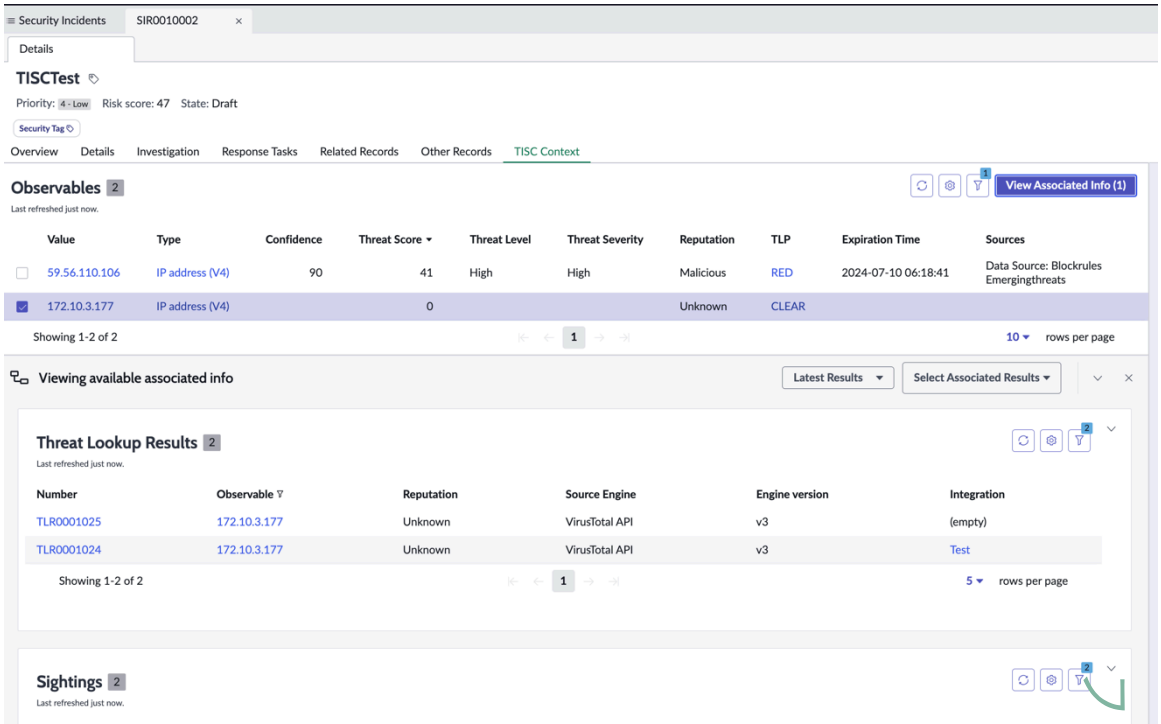


9. TISC 컨텍스트를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
:

- 이제 SIR 애플리케이션에서 TISC로 푸시된 옵저버블이 표시됩니다.



- 수동 푸시 작업에서: 옵저버블 데이터는 보안 인시던트에 연결된 경우에만 푸시할 수 있습니다. 옵저버블이 SIR에서 푸시되면 옵저버블에 연결된 보안 인시던트에 대한 참조가 있는 소스를 사용하여 해당 데이터를 식별할 수 있습니다.
- 자동 푸시 작업에서: 옵저버블 또는 보강 데이터는 보안 인시던트와 연결되면 자동으로 푸시됩니다.

  주:
  자동화된 플로우가 활성화되면 TISC에 옵저버블 보내기 옵션이 사라집니다.

- **TISC** 컨텍스트 는 TISC에도 있는 모든 SIR 연결 옵저버블을 보여줍니다.
- SIR 분석가는 TISC 컨텍스트를 사용하여 위협 조회, 사이팅 검색 및 옵저버블 보강 결과를 포함한 모든 TISC 보강 데이터를 볼 수 있습니다.
- 연결된 정보 보기 에는 선택한 옵저버블의 연결된 모든 옵저버블 보강 데이터가 표시됩니다.

10. 결과를 봅니다.

TISC에 위협 조회 보내기

이 기능을 사용하여 보안 분석가는 SIR에서 TISC로 위협 조회 데이터를 푸시할 수 있습니다. TISC 컨텍스트를 사용하면 위협 조회 결과가 TISC에 있는지 확인할 수 있습니다. 그렇지 않은 경우 보안 분석가가 필요할 때마다 데이터를 푸시할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.analyst

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

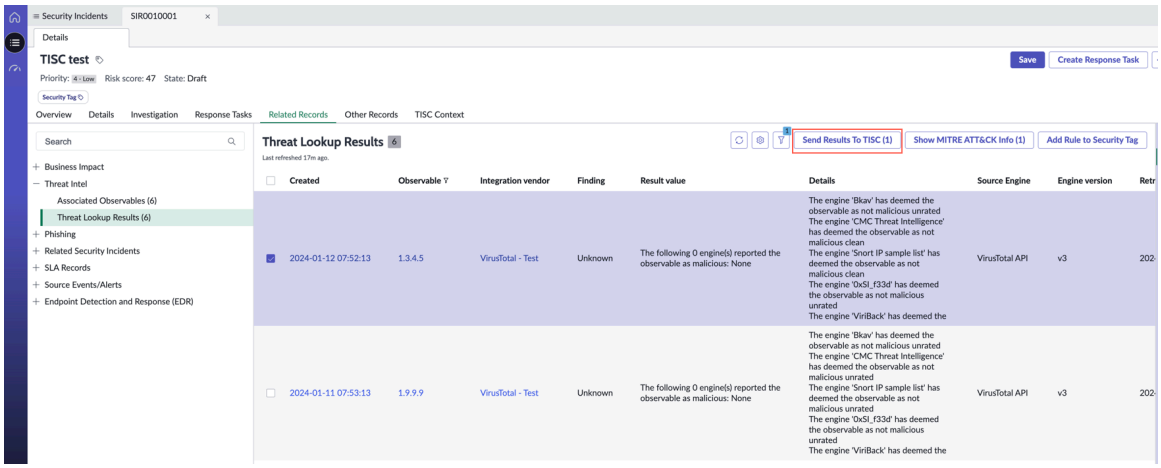
프로시저

1. SIR 작업 공간에서 관련 기록 탭으로 이동하여 TISC 통합 역량 작업을 수행합니다.

   주:

   - 조사 탭으로 이동하여 페이지 왼쪽에 표시된 엔트리포인트 목록 섹션으로 이동하고 연결된 옵저버블을 선택하여 푸시 작업을 수행할 수도 있습니다.
   - 조사 탭에서 관련 정보 보기를 클릭하여 선택한 옵저버블에 대한 모든 관련 위협 조회, 사이팅 검색 및 보강 데이터를 봅니다. 자세한 내용은 조사 캔버스 탐색 문서를 참조하십시오.

2. 선택 위협 인텔리전스 〉 위협 조회 결과 밀어넣기 작업을 수행하고 데이터를 TISC에 수동으로 푸시합니다.
3. 위협 조회 결과 기록을 하나 이상 선택합니다.
4. TISC에 결과 보내기를 클릭합니다.



   주:

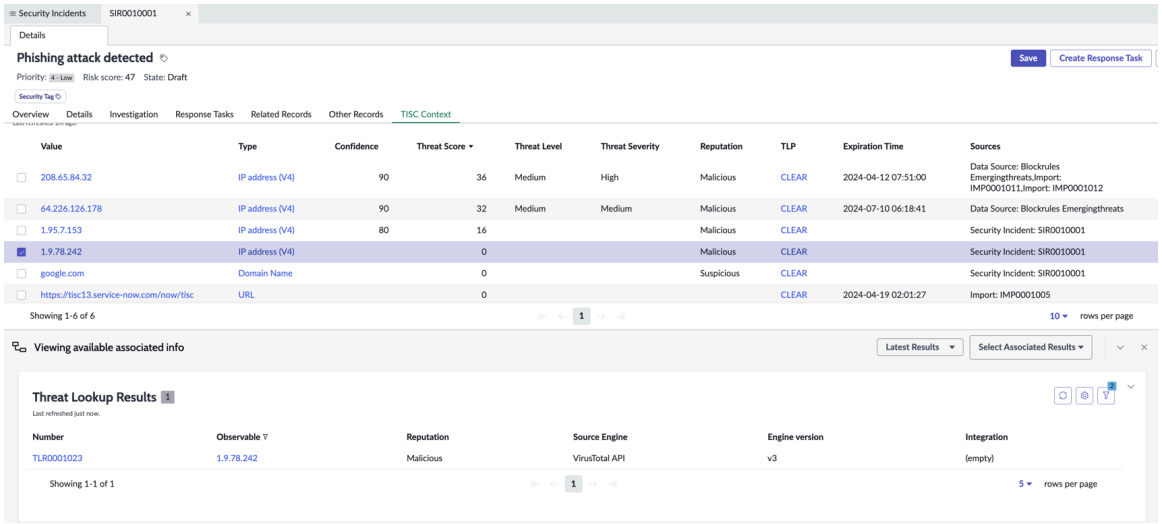
   - 선택한 위협 조회 옵저버블이 TISC에 없는 경우, 수동 모드에서 먼저 옵저버블이 옵저버블 소스로 생성된 다음, 소스 옵저버블이 TISC 옵저버블 기록을 생성하면 옵저버블 기록이 새로 생성된 옵저버블과 자동으로 연결됩니다. 또한 선택한 위협 조회는 수동 모드에서 새로 생성된 위협 조회 옵저버블에도 푸시됩니다.
   - 자동 모드에서는 옵저버블이 있으면 옵저버블이 푸시되지 않으며, 그러면 위협 조회가 자동으로 푸시됩니다. 옵저버블이 없으면 위협 조회가 푸시되지 않습니다.

5. 선택한 위협 조회 기록에 대한 옵저버블(1.9.78.242)이 TISC에 없다는 확인 메시지가 표시됩니다 . ##### #### TISC## #### ## ## ### #### #### # ## ### ####.
   이것이 처리되고 푸시되면 결과를 볼 수 있습니다.
6. **TISC** 컨텍스트를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
:

- 이제 SIR 애플리케이션에서 TISC로 푸시된 옵저버블이 표시됩니다.



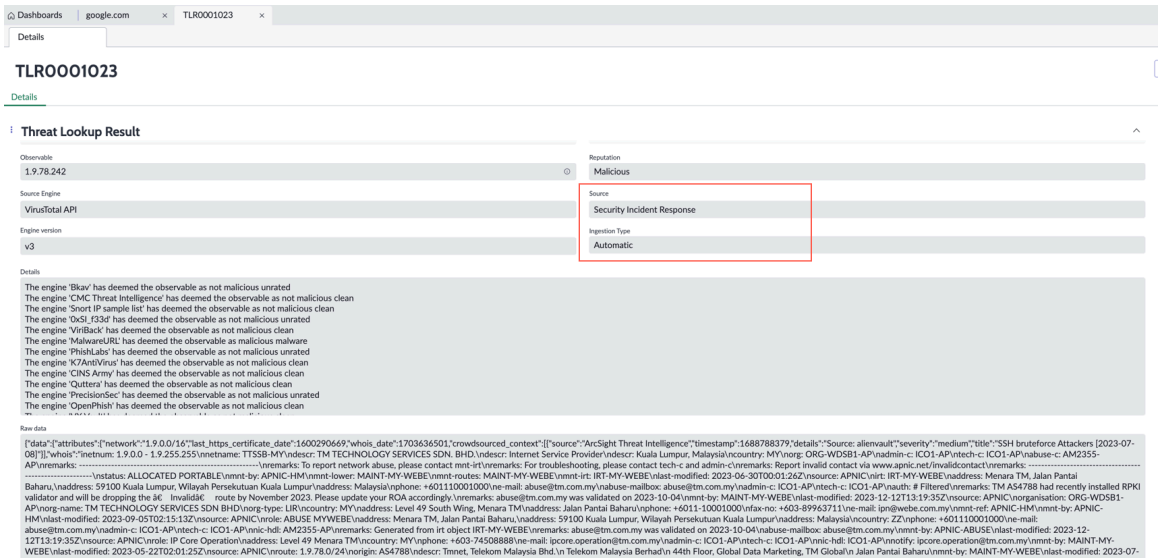
- 수동 푸시 작업에서: 옵저버블 데이터는 보안 인시던트에 연결된 경우에만 푸시할 수 있습니다. 옵저버블이 SIR에서 푸시되면 옵저버블에 연결된 보안 인시던트에 대한 참조가 있는 소스를 사용하여 해당 데이터를 식별할 수 있습니다.
- 자동 푸시 작업에서: 옵저버블 또는 보강 데이터는 보안 인시던트와 연결되면 자동으로 푸시됩니다.
- **TISC** 컨텍스트 는 TISC에도 있는 모든 SIR 연결 옵저버블을 보여줍니다.
- SIR 분석가는 TISC 컨텍스트를 사용하여 위협 조회, 사이팅 검색 및 옵저버블 보강 결과를 포함한 모든 TISC 보강 데이터를 볼 수 있습니다.
- 연결된 정보 보기 에는 선택한 옵저버블의 연결된 모든 옵저버블 보강 데이터가 표시됩니다.

7. 목록 보기에는 모든 위협 조회 결과가 표시되지만 기록을 선택하고 관련 정보 보기 버튼을 클릭합니다.

8. 위협 조회 결과를 봅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

9. 위협 조회 결과 기록을 클릭하여 푸시 또는 수집 유형 (자동 또는 수동)도 표시되는 양식 뷰의 기록을 보고 소스 는 보안 인시던트 응답이 됩니다.



TISC에 사이팅 검색 보내기

이 기능을 사용하여 보안 분석가는 사이팅 검색 데이터를 SIR에서 TISC로 푸시할 수 있습니다. 분석가는 TISC 컨텍스트를 사용하여 사이팅 검색 데이터가 TISC에 있는지 확인할 수 있으며, 그렇지 않은 경우 보안 분석가는 필요할 때마다 데이터를 푸시할 수 있습니다.

시작하기 전에

필요한 역할: sn_si.analyst

프로시저

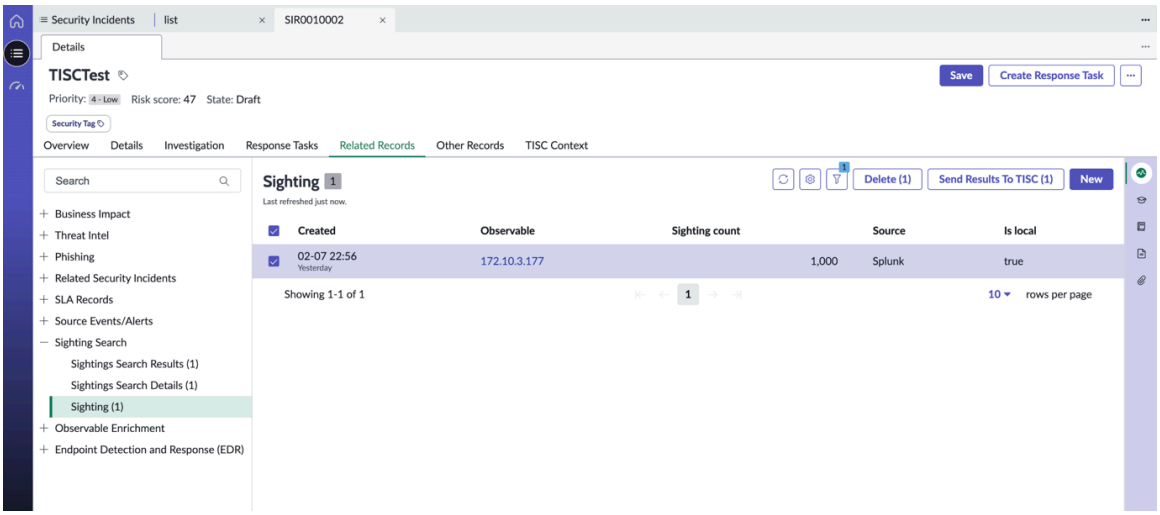
1. SIR 작업 공간에서 관련 기록 탭으로 이동하여 TISC 통합 역량 작업을 수행합니다.

   주:

   - 조사 탭으로 이동하여 페이지 왼쪽에 표시된 엔트리포인트 목록 섹션으로 이동하고 연결된 옵저버블을 선택하여 푸시 작업을 수행할 수도 있습니다.
   - 조사 탭에서 관련 정보 보기를 클릭하여 선택한 옵저버블에 대한 모든 관련 위협 조회, 사이팅 검색 및 보강 데이터를 봅니다. 자세한 내용은 조사 캔버스 탐색 문서를 참조하십시오.

2. 선택 검색 찾기 〉 사이팅 검색 결과 밀어넣기 작업을 수행하고 데이터를 TISC에 수동으로 푸시합니다.
3. 하나 이상의 사이팅 검색 결과 기록을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

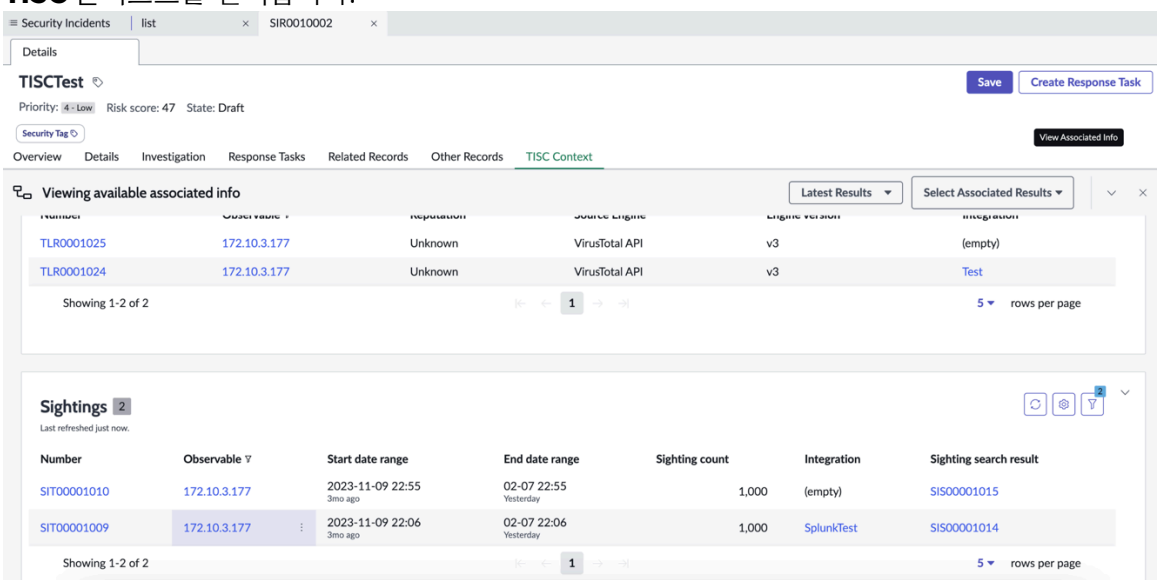


4. TISC에 결과 보내기를 클릭합니다.

주:

- 선택한 사이팅 검색 옵저버블이 TISC에 없는 경우, 수동 모드에서 먼저 옵저버블이 옵저버블 소스로 생성된 다음, 소스 옵저버블이 TISC 옵저버블 기록을 생성하면 옵저버블 기록이 새로 생성된 옵저버블과 자동으로 연결됩니다. 또한 선택한 사이팅 검색도 수동 모드에서 새로 생성된 위협 조회 옵저버블로 푸시됩니다.
- 자동 모드에서는 옵저버블이 있으면 옵저버블이 푸시되지 않으며, 그러면 위협 조회가 자동으로 푸시됩니다. 옵저버블이 없으면 위협 조회가 푸시되지 않습니다.

5. TISC 컨텍스트를 선택합니다.

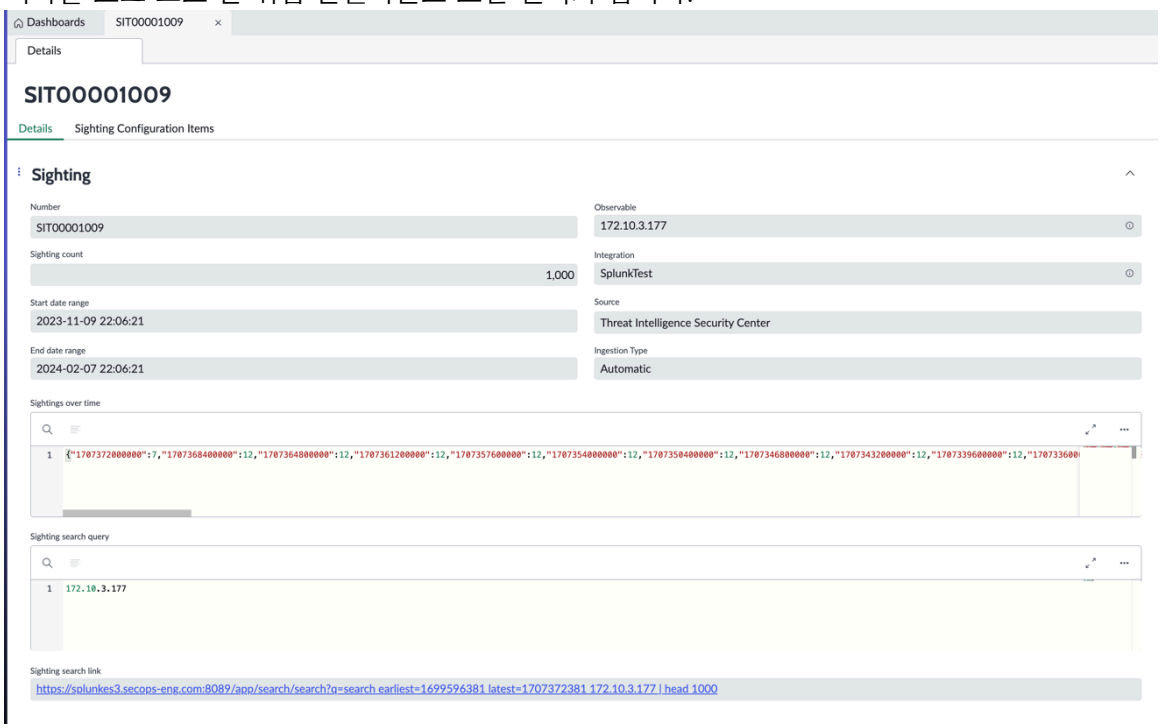


© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
:

- 이제 SIR 애플리케이션에서 TISC로 푸시된 옵저버블이 표시됩니다.
- 수동 푸시 작업에서: 옵저버블 데이터는 보안 인시던트에 연결된 경우에만 푸시할 수 있습니다. 옵저버블이 SIR에서 푸시되면 옵저버블에 연결된 보안 인시던트에 대한 참조가 있는 소스를 사용하여 해당 데이터를 식별할 수 있습니다.
- 자동 푸시 작업에서: 옵저버블 또는 보강 데이터는 보안 인시던트와 연결되면 자동으로 푸시됩니다.
- **TISC** 컨텍스트 는 TISC에도 있는 모든 SIR 연결 옵저버블을 보여줍니다.
- SIR 분석가는 TISC 컨텍스트를 사용하여 위협 조회, 사이팅 검색 및 옵저버블 보강 결과를 포함한 모든 TISC 보강 데이터를 볼 수 있습니다.
- 연결된 정보 보기 에는 선택한 옵저버블의 연결된 모든 옵저버블 보강 데이터가 표시됩니다.

6. 기록이 처리되면 기록을 선택하고 관련 정보 보기를 클릭합니다.
7. 결과를 봅니다.
8. 사이팅 검색 결과 기록을 클릭하여 푸시 또는 수집 유형 (자동 또는 수동)도 표시되는 양식 뷰에서 기록을 보고 소스 는 위협 인텔리전스 보안 센터가 됩니다.



옵저버블 보강을 TISC로 보내기

이 기능을 사용하여 보안 분석가는 사이팅 검색 데이터를 SIR에서 TISC로 푸시할 수 있습니다. 분석가는 TISC 컨텍스트를 사용하여 사이팅 검색 데이터가 TISC에 있는지 확인할 수 있으며, 그렇지 않은 경우 보안 분석가는 필요할 때마다 데이터를 푸시할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.analyst

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

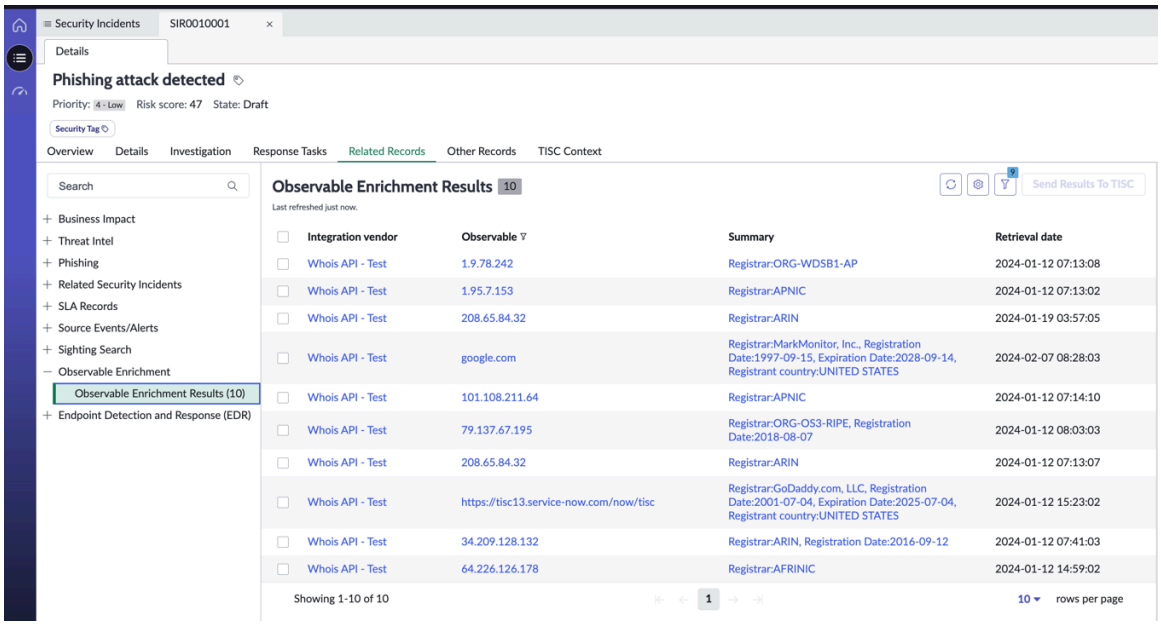
1. SIR 작업 공간에서 관련 기록 탭으로 이동하여 TISC 통합 역량 작업을 수행합니다.

주:

- 조사 탭으로 이동하여 페이지 왼쪽에 표시된 엔트리포인트 목록 섹션으로 이동하고 연결된 옵저버블을 선택하여 푸시 작업을 수행할 수도 있습니다.
- 조사 탭에서 관련 정보 보기를 클릭하여 선택한 옵저버블에 대한 모든 관련 위협 조회, 사이팅 검색 및 보강 데이터를 봅니다. 자세한 내용은 조사 캔버스 탐색 문서를 참조하십시오.

2. 선택 관찰 대상 보강 〉 옵저버블 보강 결과 밀어넣기 작업을 수행하고 데이터를 TISC에 수동으로 푸시합니다.

3. 수행할 옵저버블 기록을 하나 이상 선택하십시오. **TISC** 작업에 결과 전송 데이터를 푸시합니다.



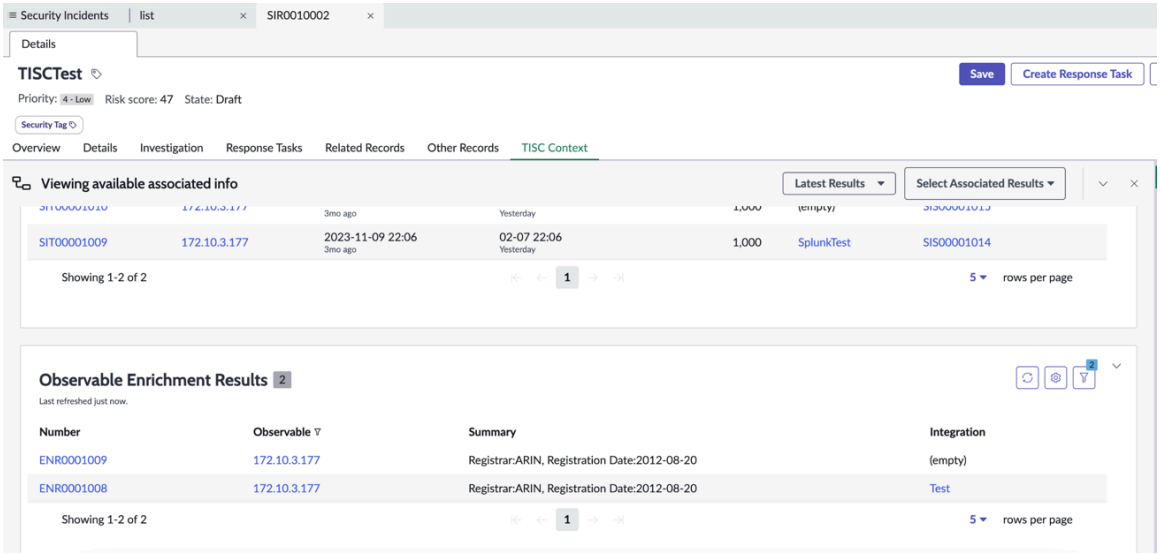
4. TISC에 결과 보내기를 클릭합니다.

주:

- 선택한 옵저버블이 TISC에 없는 경우 먼저 옵저버블이 옵저버블 소스로 생성된 다음, 소스 옵저버블이 TISC 옵저버블 기록을 생성하면 옵저버블 기록이 새로 생성된 옵저버블과 자동으로 연결됩니다.
- 옵저버블 푸시 작업이 수행되면 옵저버블 0.0.0.0이 TISC로 성공적으로 푸시되었다는 정보 메시지가 표시됩니다 . TISC #### ## ##### #### # ### ## # ####.

5. TISC 컨텍스트를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

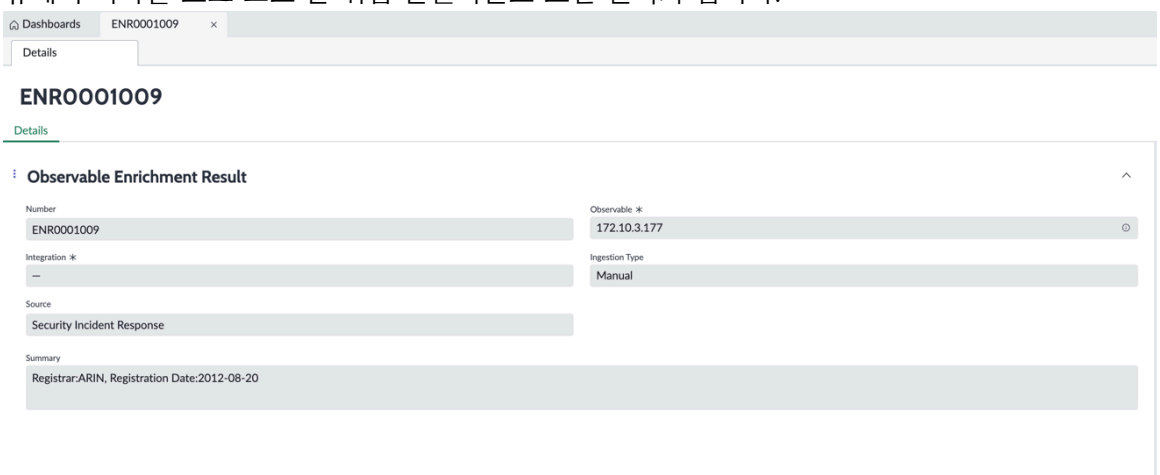


주:

:

- 이제 SIR 애플리케이션에서 TISC로 푸시된 옵저버블이 표시됩니다.
- 수동 푸시 작업에서: 옵저버블 데이터는 보안 인시던트에 연결된 경우에만 푸시할 수 있습니다. 옵저버블이 SIR에서 푸시되면 옵저버블에 연결된 보안 인시던트에 대한 참조가 있는 소스를 사용하여 해당 데이터를 식별할 수 있습니다.
- 자동 푸시 작업에서: 옵저버블 또는 보강 데이터는 보안 인시던트와 연결되면 자동으로 푸시됩니다.
- **TISC** 컨텍스트 는 TISC에도 있는 모든 SIR 연결 옵저버블을 보여줍니다.
- SIR 분석가는 TISC 컨텍스트를 사용하여 위협 조회, 사이팅 검색 및 옵저버블 보강 결과를 포함한 모든 TISC 보강 데이터를 볼 수 있습니다.
- 연결된 정보 보기 에는 선택한 옵저버블의 연결된 모든 옵저버블 보강 데이터가 표시됩니다.

6. 결과를 봅니다.
7. 옵저버블 보강 결과 기록을 클릭하여 푸시 또는 수집 유형 (자동 또는 수동)도 표시되는 양식 뷰에서 기록을 보고 소스 는 위협 인텔리전스 보안 센터가 됩니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

TISC 컨텍스트 작업

TISC 컨텍스트를 사용하면 보안 인시던트 대응 작업 공간 내에서 옵저버블과 같은 위협 인텔리전스 데이터를 쉽게 볼 수 있습니다.

이를 통해 보안 분석가는 작업 공간에서 보다 효과적으로 보안 인시던트를 탐지, 조사 및 대응할 수 있습니다.

보안 인시던트 응답 작업 공간의 TISC 컨텍스트를 사용하면 보안 분석가가 작업 공간에서 직접 보안 인시던트 또는 옵저버블을 TISC 케이스에 추가하고, 보강 결과를 보고, 옵저버블 관련 정보(관련 위협 행위자, 공격 패턴, 캠페인 등)를 볼 수 있습니다.

이 섹션을 사용하여 다음을 수행할 수 있습니다.

1. 옵저버블을 TISC 케이스에 연결합니다.
2. 연결된 옵저버블 정보를 봅니다.
3. 옵저버블 보강 결과를 봅니다.

자세한 내용 및 절차는 다음 섹션을 참조하고, TISC와 SIR 작업 공간 간의 통합 작동 방식에 대한 자세한 내용은 을 위협 인텔리전스 보안 센터참조하십시오SIR 작업 공간과 TISC 통합.

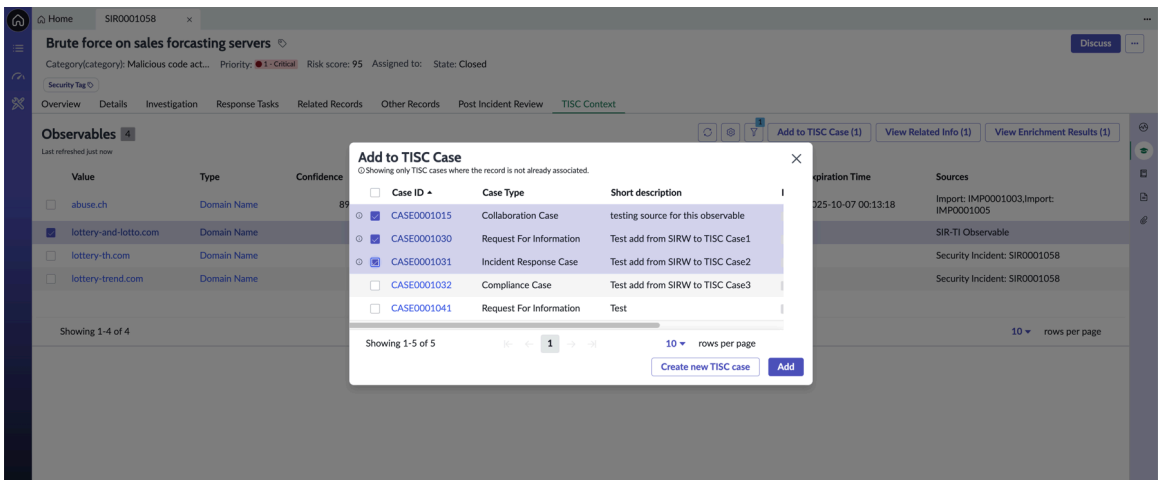
TISC 케이스에 옵저버블 추가

이 섹션을 사용하여 TISC 케이스에 보안 인시던트 또는 옵저버블을 추가합니다.

시작하기 전에
필요한 역할: sn_si.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간 〉 보안 인시던트 〉 모두.
2. 조사 중인 특정 보안 인시던트를 찾아서 엽니다.
   인시던트 ID를 검색하거나, 빠른 필터 섹션을 사용하여 필터링하거나, 인시던트 상태를 탐색하여 이 작업을 수행할 수도 있습니다.
3. TISC 컨텍스트 탭을 선택합니다.
4. TISC 케이스에 추가 버튼을 클릭합니다.
   TISC 케이스에 추가 대화 상자가 표시되고 기록이 아직 연결되지 않은 TISC 케이스만 표시됩니다.
5. 옵저버블을 선택합니다.
6. 케이스를 선택하고 추가를 클릭하여 옵저버블에 케이스를 추가하고 보안 인시던트에 연결합니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
기존 케이스가 없는 경우 새 **TISC** 케이스 생성을 클릭하여 새 케이스를 만들 수도 있습니다.

다음과 같은 확인 메시지가 표시됩니다.

- 다음 옵저버블이 아티팩트로 추가되었습니다.
- 다음 옵저버블이 TISC로 전송되고 이후에 선택한 TISC 케이스 기록에 추가됩니다.

주:
옵저버블 활동의 처리 및 연결은 연결이 완료될 때 활동 스트림에 게시됩니다.

7. 추가 단계를 위해 위협 인텔리전스 보안 센터 작업 공간에 로그인하여 관련 케이스 기록을 봅니다. 자세한 내용은 SIR 작업 공간과 TISC 통합 문서를 참조하십시오.

주:

보안 인시던트 응답 작업 공간에서 조사 및 관련 기록 탭의 케이스 기록에 옵저버블을 연결할 수도 있습니다.

주:
조사에서 옵저버블을 연결하려면 아래 절차를 따르고 여기에 설명된 관련 기록에서 연결하려면 다음을 TISC 케이스에 옵저버블 추가수행합니다. 조사 탭으로 이동하여 페이지 왼쪽에 표시된 엔트리포인트 목록 섹션으로 이동하고 연결된 옵저버블을 선택하여 TISC 케이스에 옵저버블을 추가할 수도 있습니다.

TISC에서 관련 정보 보기

이 섹션을 사용하여 SIR 작업 공간에서 관련 위협 액터, 공격 패턴, 캠페인 및 TISC의 케이스와 같은 관련 정보를 봅니다.

시작하기 전에
필요한 역할: sn_si.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간 〉 보안 인시던트 〉 모두.

2. 조사 중인 특정 보안 인시던트를 찾아서 엽니다.
인시던트 ID를 검색하거나, 빠른 필터 섹션에서 찾아보거나, 인시던트 상태를 통해 필터링하여 이 작업을 수행할 수도 있습니다.

3. 인시던트가 열리면 **TISC** 컨텍스트 탭으로 이동합니다.
뷰 관련 정보 보기:

인시던트 상세 정보 내의 여러 섹션에서 관련 정보를 볼 수 있습니다.

a. 하나 이상의 옵저버블을 선택합니다.

b. 관련 정보 보기 버튼을 클릭합니다.
이 섹션에는 선택한 옵저버블과 관련된 관련 정보가 표시됩니다.

이름	설명
위협 액터	선택한 옵저버블과 관련된 TISC for Threat Actors의 정보를 표시합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이름	설명
공격 패턴	선택한 옵저버블과 관련된 공격 패턴에 대한 TISC의 정보를 표시합니다.
캠페인	선택한 옵저버블과 관련된 TISC for Campaigns의 정보를 표시합니다.
케이스	선택한 옵저버블과 관련된 TISC 케이스에 대한 TISC의 정보를 표시합니다.

보강 결과 보기

이 섹션을 사용하여 SIR 작업 공간에서 TISC의 위협 조회 결과, 관찰 및 옵저버블 보강 결과와 같은 옵저버블 보강 결과를 봅니다.

시작하기 전에
필요한 역할: sn_si.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간 〉 보안 인시던트 〉 모두.
2. 조사 중인 특정 보안 인시던트를 찾아서 엽니다.
   인시던트 ID를 검색하거나, 빠른 필터 섹션에서 찾아보거나, 인시던트 상태를 통해 필터링하여 이 작업을 수행할 수도 있습니다.
3. 인시던트가 열리면 **TISC** 컨텍스트 탭으로 이동합니다.
   보강 결과 보기:

   인시던트 상세 정보 내의 여러 섹션에서 관련 정보를 볼 수 있습니다.

   a. 하나 이상의 옵저버블을 선택합니다.

   b. 보강 결과 보기 버튼을 클릭합니다.
   이 섹션에는 선택한 옵저버블과 관련된 상세 정보가 표시됩니다.

이름	설명
위협 조회 결과	선택한 TISC 옵저버블에 대한 모든 관련 위협 조회 결과를 나열합니다.
사이팅	선택한 TISC 옵저버블에 대한 모든 연관된 사이팅을 나열합니다.
옵저버블 보강 결과	선택한 TISC 옵저버블에 대해 연결된 모든 옵저버블 보강 결과를 나열합니다.

보안 인시던트 응답의 보고서

보안 인시던트와 관련된 모든 보고서는 보고서 섹션 내에서 분석 및 공유할 수 있습니다.

분석가는 다음을 수행할 수 있습니다.

- 보고서 작성
- 보고서 편집
- 보고서 삭제

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보고서 작성

분석가는 인시던트 보안 인시던트 응답 상태를 포함하는 보고서를 만들고 이메일을 통해 공유할 수 있습니다.

시작하기 전에

필요한 역할: sn_si.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간.
2. 보안 인시던트를 엽니다.
3. 보고서를 선택합니다.

   보고서 페이지에는 선택한 인시던트에 대해 생성된 모든 보고서 목록이 표시됩니다.

4. 새로 만들기를 선택합니다.
   게시된 모든 템플릿 목록과 함께 템플릿 선택 페이지가 나타납니다. 템플릿 목록은 관리자가 보고서 템플릿을 게시한 경우에만 사용할 수 있습니다. 자세한 내용은 에서 보고서 템플릿 생성 보안 인시던트 응답 문서를 참조하십시오.
5. 보고서 템플릿을 선택합니다.
   보고서는 템플릿에서 구성된 인시던트 데이터와 함께 편집 모드로 열립니다.
6. 확장을 선택하고 원하는 필드를 삽입/제거합니다.
   - 공통 **SIR** 필드: 인시던트에 가장 많이 사용되는 필드 목록입니다.
   - 모든 **SIR** 필드: 인시던트와 관련된 모든 필드입니다. 예를 들어, 인시던트 보고서를 생성하는 중에 간단한 설명이라는 필드를 추가하려면 모든 **SIR** 필드에서 해당 필드를 선택할 수 있습니다. 필드를 추가하면 인시던트가 보고서에 표시되는 경우의 짧은 설명입니다.
   - 관련 기록: 특정 인시던트의 관련 기록입니다. 예를 들어 보고서에 연결된 옵저버블을 추가하려면 보고서에 추가할 수 있습니다. 이러한 관련 기록은 테이블 형식으로 표시됩니다
   - 스크립트: 보고서의 날짜 및 시간을 추가하려면 보고서에 현재 날짜 시간 스크립트를 추가할 수 있습니다. 이렇게 하면 보고서에 보고서 생성 날짜 및 시간이 추가됩니다.
7. 보고서의 미리 보기를 보려면 미리 보기를 선택합니다.
8. **Save Content**를 선택하여 변경 내용을 저장합니다.
9. 옵션: 보고서 세부 정보 편집 아이콘을 선택하여 보고서 이름과 설명을 업데이트합니다.
10. 게시를 선택하여 보고서를 게시합니다.
11. 이메일에서 보고서 공유 아이콘을 선택합니다.
    a. 받는 사람 및 참조/숨은 참조 필드에 수신자의 이메일을 입력합니다.
    b. 이메일 제목과 이메일 본문을 업데이트합니다.
    c. 보내기를 선택하여 이메일을 통해 보고서를 공유합니다.

보고서 편집

분석가는 에서 보안 인시던트 응답 게시되지 않은 보고서를 수정하고 이메일을 통해 공유할 수 있습니다.

시작하기 전에

필요한 역할: sn_si.analyst

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간.
2. 보안 인시던트를 엽니다.
3. 보고서를 선택합니다.

   보고서 페이지에는 선택한 인시던트에 대해 생성된 모든 보고서 목록이 표시됩니다.

4. 업데이트할 보고서를 엽니다.
   보고서는 템플릿에서 구성된 인시던트 데이터와 함께 편집 모드로 열립니다.
5. 필요에 따라 보고서를 편집합니다.
6. 보고서의 미리 보기를 보려면 미리 보기를 선택합니다.
7. **Save Content**를 선택하여 변경 내용을 저장합니다.
8. 옵션: 보고서 세부 정보 편집 아이콘을 선택하여 보고서 이름과 설명을 업데이트합니다.
9. 게시를 선택하여 보고서를 게시합니다.
10. 이메일에서 보고서 공유 아이콘 을 선택합니다.
    a. 받는 사람 및 참조/숨은 참조 필드에 수신자의 이메일을 입력합니다.
    b. 이메일 제목과 이메일 본문을 업데이트합니다.
    c. 보내기를 선택하여 이메일을 통해 보고서를 공유합니다.

보고서 삭제

게시됨 또는 초안 상태인 보고서를 보안 인시던트 응답 삭제할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간.
2. 보안 인시던트를 엽니다.
3. 보고서를 선택합니다.

   보고서 페이지에는 선택한 인시던트에 대해 생성된 모든 보고서 목록이 표시됩니다.

4. 삭제할 보고서를 엽니다.
5. 삭제를 선택합니다.
   확인 메시지가 나타납니다.
6. 삭제를 선택하여 보고서를 삭제합니다.

에서 전화 회의 또는 채팅을 사용하여 공동 작업 보안 인시던트 응답

분석가 및 영향을 받는 사용자와 공동 작업하여 애플리케이션에서 인시던트를 해결하거나 논의할 수 있습니다 보안 인시던트 응답 .

관련 정보

Security Incident Response에서 전화 회의 시작

Security Incident Response에서 사이드바 채팅 시작

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Security Incident Response에서 전화 회의 시작

보안 분석가는 전화 회의를 사용하여 다른 분석가 및 영향을 받는 사용자와 실시간으로 협업할 수 있습니다. 이러한 호출은 인시던트 해결에 도움이 되는 정보 교환을 용이하게 합니다.

시작하기 전에

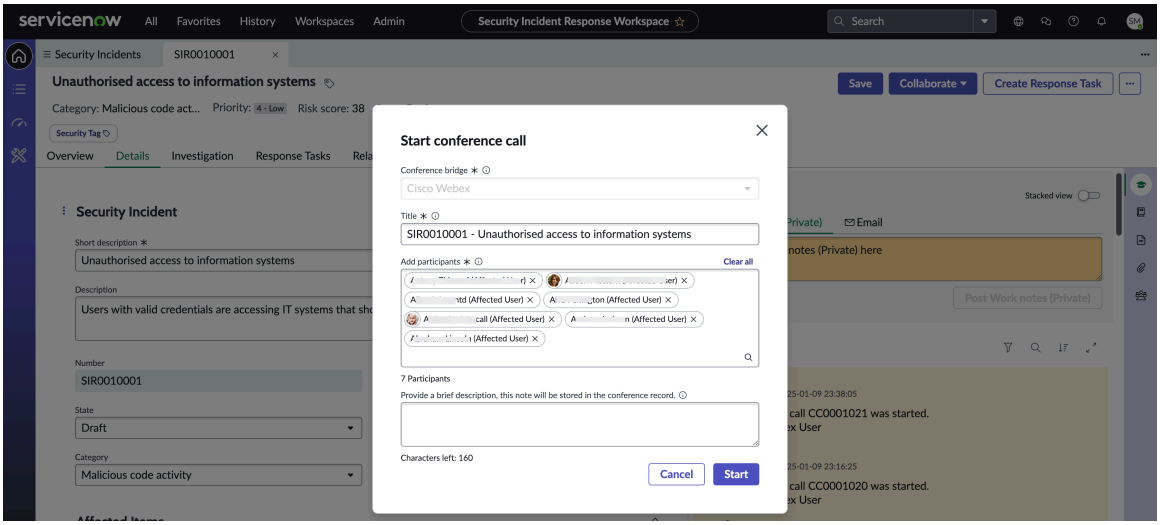
다음 앱과 플러그인의 설치를 완료하고 활성화했는지 확인하십시오.

- 알림 플러그인(com.snc.notify)
- 구성 가능한 작업 공간 앱에 대한 UI 구성요소를 알립니다.
- Visual Task Board 플러그인(com.devsnc.snb_vtb)

필요한 역할: sn_si.analyst 또는 sn_si.manager

프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간.
2. 전화 회의를 시작하려는 보안 인시던트를 엽니다.
3. 공동 작업을 선택한 다음 통화 시작을 선택하거나 선택한 다음 + 아이콘을 선택할 수 있습니다.



전화 회의 시작 팝업이 나타납니다.

4. **Conference** bridge(컨퍼런스 브리지) 필드에서 컨퍼런스 브리지를 선택합니다.
5. 제목에 전화 회의의 제목을 입력합니다.

> **주:**
> 기본적으로 인시던트 제목은 호출 제목으로 채워집니다. 기본 제목은 수정할 수 있습니다.

6. 에서 통화 참가자를 추가하거나 제거합니다. 참가자 추가.

> **주:**
> 전화 회의 설정의 구성에 따라 미리 채워진 참가자 목록이 참가자 추가 에 추가되거나 참가자 권장 목록을 사용할 수 있습니다. 자세한 내용은 컨퍼런스 회의 사용자 및 그룹 관리 문서를 참조하십시오.

7. 전화 회의 시작에 대한 간략한 설명을 제공합니다.
8. 시작을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

선택한 컨퍼런스 회의 브리지에서 전화 회의가 시작됩니다. 모든 참가자는 이메일과 회의 브리지를 통해 알림을 받습니다. 참가자는 링크 또는 알림을 사용하여 통화에 참여할 수 있습니다.

9. 애플리케이션에서 관련 인시던트 보안 인시던트 응답 를 열어 전화 회의 상세 정보를 봅니다.
10. 옵션: 활성 통화에 참가자를 추가하려면 초대 복사 를 선택합니다.
11. 통화 종료를 선택합니다.
    마지막 참가자가 전화 회의에서 나가면 통화가 종료됩니다
12. 옵션: 컨퍼런스 회의를 다시 시작하려면 완료됨 섹션으로 이동하여 필요한 컨퍼런스 회의의 다시 시작 옵션을 선택합니다.

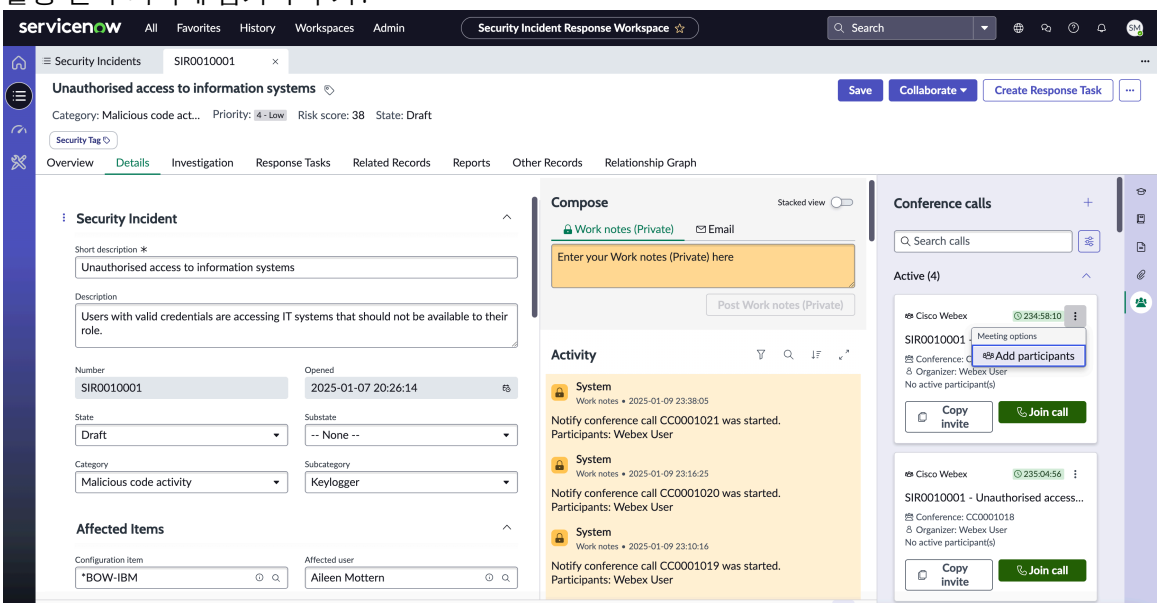
활성 전화 회의에 참가자 추가

전화 회의를 시작하기 전에 참가자를 추가하지 않은 경우 활성 전화 회의에 추가할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.analyst,sn_si.manager

프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간.
2. 전화 회의를 시작하려는 보안 인시던트를 엽니다.
3. 컨퍼런스 회의 아이콘을 선택하여 컨퍼런스 회의의 상세 정보를 봅니다.
4. 활성 전화 회의에 참가자 추가:



- 회의 옵션 아이콘을 선택합니다 ⋮ 활성 전화 회의에 대해 선택하고 참가자 추가를 선택합니다.
- 전화 회의 섹션에서 초대 복사를 선택하고 필요한 참가자와 초대를 공유합니다.

Security Incident Response에서 사이드바 채팅 시작

사이드바를 사용하면 보안 분석가가 작업 공간 작업 기반 또는 상호작용 기반 기록을 기반으로 다른 분석가와 실시간으로 공동 작업할 수 있습니다. 이러한 사이드바 토론은 정보와 지식의 교환을 용이하게 하여 고품질의 결과로 문제를 보다 빠르게 해결할 수 있도록 지원합니다.

시작하기 전에
필요한 역할: sn_si.read

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옴니 경험 표준 기능 세트 플러그인을 활성화했는지 확인합니다. 자세한 내용은 Installing Sidebar 문서를 참조하십시오.

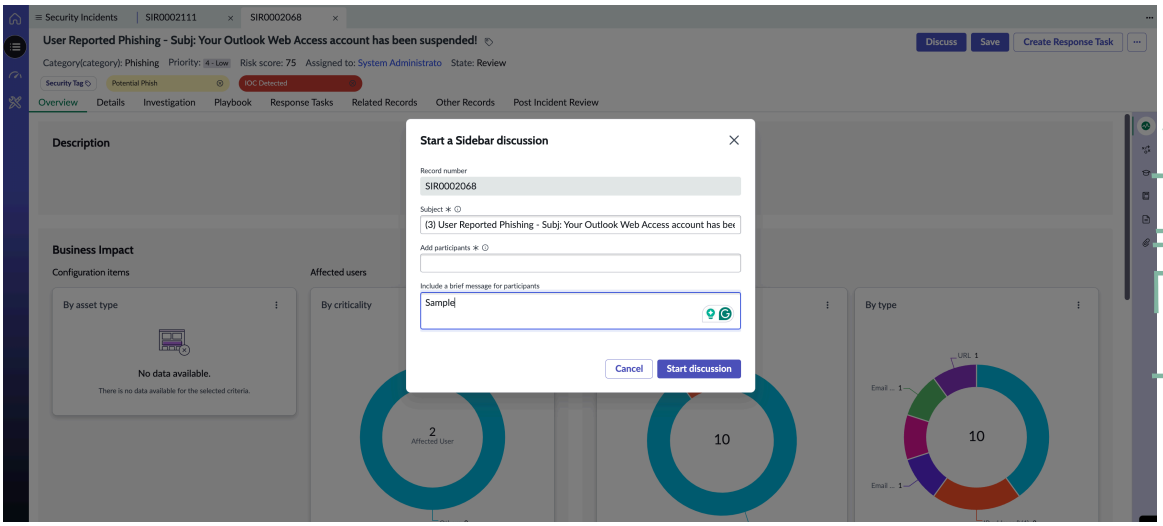
프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간.
2. 목록 뷰 아이콘을 선택합니다.
3. 사이드바 토론을 시작하려는 보안 인시던트를 엽니다.
4. 공동 작업을 선택한 다음 채팅 시작을 선택합니다.
   Sidebar 토론 시작 대화 상자가 나타납니다.

   주:
   Sidebar와 Microsoft Teams의 통합을 통해 Sidebar 사용자와 Microsoft Teams 사용자는 각자의 플랫폼에서 서로 통신할 수 있습니다. 자세한 내용은 Sidebar and Microsoft Teams 문서를 참조하십시오.

5. Sidebar 토론 시작 대화 상자에서 필드에 내용을 입력합니다.

보안 인시던트 응답에서 사이드바 채팅 시작



6. 토론 시작을 선택합니다.
7. 빠른 실행과 같은 추가 구성을 수행할 수 있습니다.
   작업 사용을 제한하려면 빠른 작업 페이지에서 그룹에 적용 필드를 사용할 수 있습니다. 자세한 내용은 Creating a quick action 문서를 참조하십시오.

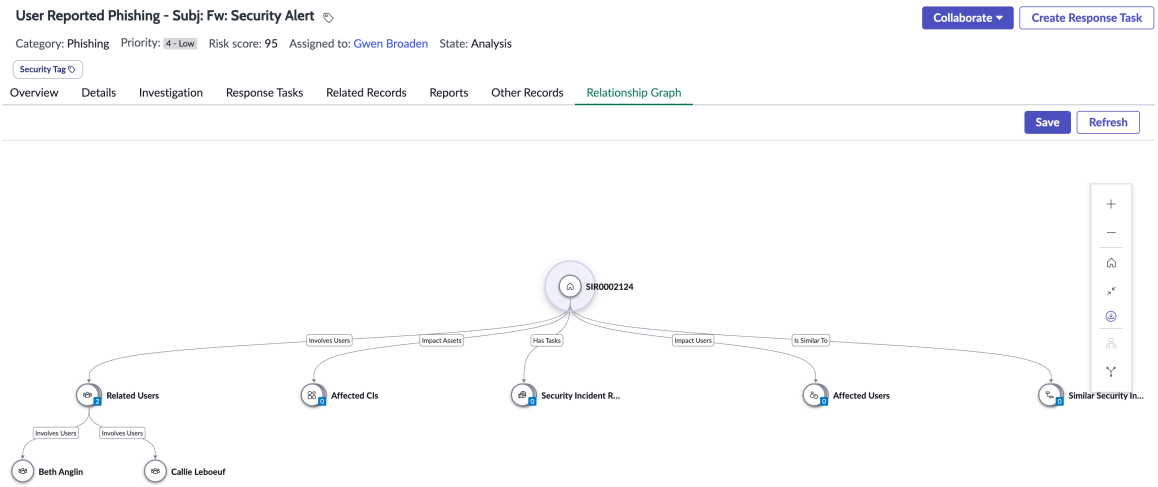
관계 그래프로 인시던트 상세 정보 보기

작업 공간의 관계 그래프에는 보안 인시던트 응답 보안 인시던트와 관련 항목 간의 연결이 시각적으로 표시되어 보안 인시던트의 전체 컨텍스트를 분석하는 데 도움이 됩니다.

보안 인시던트와 관련된 항목에는 관련 옵저버블, 구성 항목(CI), 유사한 보안 인시던트(SIR), 응답 작업 및 기타 관련 목록이 포함될 수 있습니다.

다음 관계 그래프 예는 보안 인시던트에 대한 상세 정보를 표시합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



보안 인시던트에 대한 관계 그래프를 열면 사용 가능한 구성이 기본적으로 표시됩니다. 다음과 같이 그래프와 상호 작용할 수 있습니다.

- 화면에 맞게 개체를 확대하고 노드를 드래그합니다.
- 사용 가능한 경우 각 노드에 대한 하위 노드를 추가하고 하위 노드의 상세 정보를 봅니다.
- 그래프에서 노드 또는 하위 노드를 숨깁니다.
- 하위 노드의 상세 정보를 봅니다.

관계 그래프 사용자 지정

관계 그래프에서 보안 인시던트 및 관련 데이터를 시각화하고 분석합니다.

시작하기 전에

필요한 역할: sn_si.admin

프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간 〉 관리.
2. 관계 그래프를 선택한 다음 관계 그래프 구성을 선택합니다.
3. 새로 만들기를 선택합니다.
4. 양식에서 필드를 채웁니다.

관계 그래프 구성

필드	설명
관련 테이블 이름	옵저버블 연결〔sn_ti_observable〕테이블 또는 보안 인시던트〔sn_si_incident〕테이블과 같이 보안 인시던트 옵저버블 데이터를 가져올 테이블입니다.
노드 레이블	관계 그래프에 나타나는 옵저버블의 노드 레이블입니다. 자동으로 제공되는 값은 선택한 관련 테이블에 따라 다릅니다.
활성	구성을 활성화하는 옵션입니다.
데이터 노드 레이블	선택한 관련 목록의 노드에 표시할 기본 레이블 및 보조 레이블입니다.
기본값 표시	데이터 노드 레이블을 표시하는 옵션입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
관계 레이블	관계 그래프에 표시할 노드와 링크 노드 간의 관계입니다.

5. 저장을 선택합니다.

인시던트에 대한 관계 그래프 만들기

에서 노드 관계 그래프 보안 인시던트 응답 를 생성하여 보안 인시던트를 악의적인 옵저버블, 구성 항목(CI), 유사한 보안 인시던트(SIR), 응답 작업 및 기타 관련 정보와 상호 연관시켜 보안 인시던트를 보다 효과적으로 분석할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.analyst

이 태스크 정보
미리 정의된 그래프를 사용하지 않고 사용자 지정 관계 그래프를 만드는 방법에 대한 자세한 내용은 을 참조하십시오 관계 그래프 사용자 지정.

> **주:**
> 관계 그래프에 대한 변경 내용은 자동으로 저장되지 않습니다.

프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간.
2. 보안 인시던트를 엽니다.
3. 관계 그래프 탭을 선택합니다.
4. 관계 그래프에서 상위 노드를 길게 선택하거나 마우스 오른쪽 버튼으로 클릭한 다음, 노드 추가를 선택합니다.
5. 관계 그래프에 표시할 관련 사용자, 영향을 받는 CI, 유사한 보안 인시던트(SIR) 또는 영향을 받는 사용자 등의 범주 노드를 하나 이상 선택합니다.

   > **주:**
   > 여러 범주 노드를 선택할 수 있습니다.

6. 범주 노드를 길게 선택하거나 마우스 오른쪽 버튼으로 클릭하고 링크 노드를 선택하여 범주 노드와 연결된 데이터를 추가합니다.

   > **주:**
   > 필터를 적용하여 목록의 항목 수를 줄일 수 있습니다.

   선택한 범주 노드의 모든 관련 기록 목록이 나타납니다. 예를 들어 노드 범주에서 영향을 받는 사용자를 선택하면 이 인시던트의 영향을 받는 모든 사용자 목록이 표시됩니다.
7. 목록에서 원하는 기록을 선택하고 추가를 선택합니다.
8. 추가를 선택합니다.
9. 옵션: 필요한 경우 새로 고침을 선택하여 변경 내용을 지웁니다.
10. 저장을 선택합니다.

    > **주:**
    > 관계 그래프를 저장할 때도 필터에 대한 변경 내용이 저장됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

11. 옵션: 하위 노드의 상세 정보를 표시합니다.
    a. 하위 노드를 선택합니다.
    b. 상세 정보 표시를 선택합니다.
12. 옵션: 맵을 시스템에 다운로드합니다.

    a. 맵의 일부만 화면에 표시되고 전체 화면을 PDF에 포함하려면 화면에 맞춤 아이콘(화면에)을 선택합니다.

    > 주:
    > 화면에 나타나는 맵 부분만 PDF 파일에 포함됩니다.

    b. 맵 내보내기 아이콘( )을 선택합니다.

Example: 관계 그래프를 편집하여 범주 노드와 하위 노드를 추가하는 방법을 보여주는 비디오
https://player.vimeo.com/video/1095955062?h=593c16e2b6&badge=0&autopause=0&player_id=0&app_id=58479

보안 인시던트 플레이북

보안 인시던트 플레이북 플로우를 자동 또는 수동으로 호출합니다.

플레이북은 하나 이상의 플레이북이 보안 인시던트와 연결된 경우에만 표시됩니다. 플레이북 구성요소는 Flow Designer 빌드 플로우가 아닌 PAD(프로세스 자동화 디자이너) 구축 프로세스에만 작동합니다. 플로우 디자이너가 활성화된 기존 플로우의 경우 계속 작동하며 활동은 응답 작업으로 계속 렌더링됩니다.

플레이북을 보안 인시던트와 연결하는 방법에는 두 가지가 있습니다.

- Playbook 자동 호출
- 수동으로 플레이북 추가

Playbook 자동 호출

플레이북을 자동으로 호출하려면 PAD(프로세스 자동화 디자이너)를 사용하여 프로세스를 정의해야 하며, 트리거 조건이 충족되면 플레이북 탭이 플레이북 활동과 함께 자동으로 렌더링됩니다.

수동으로 플레이북 추가

플레이북을 수동으로 호출하려면 양식 UI 작업 드롭다운으로 이동하여 플레이북 추가를 선택합니다. 자세한 내용은 플레이북 추가 문서를 참조하십시오.

> 주:
> 사용 가능한 플레이북이 이미 있는 경우 추가된 새 플레이북이 기존 플레이북과 동시에 실행됩니다.

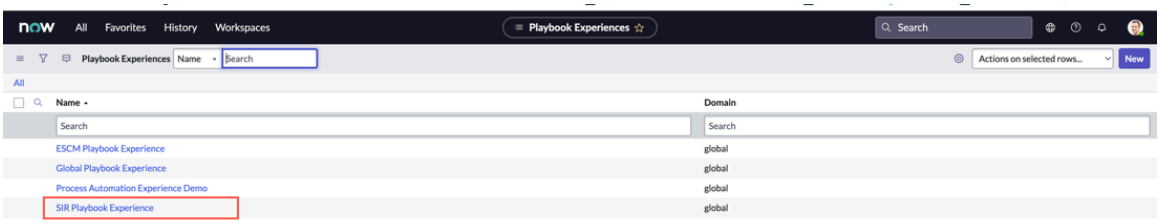
- 플레이북 내에서 분석가는 상태별로 플레이북 카드를 필터링할 수 있습니다.
- 분석가는 타원 아이콘에서 선택하여 플레이북을 취소할 수 있습니다.
- 각 활동 내에서 분석가는 활동 카드 내에 정의된 작업(예: 건너뛰기, 완료로 표시, 취소) 또는 오케스트레이션 작업(예: 샌드박스에 제출, 이메일 검색 등)을 수행할 수 있습니다.
- 이러한 각 작업은 활동 정의 내에 정의되며, 전체 카드 표시는 활동 정의 자체를 작성할 때 사용자 지정할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
앞으로 수행할 모든 활동 정의와 다음 단계는 잠금 아이콘과 함께 표시되며 사용자에게 읽기 전용 모드가 됩니다. 플레이북 표시 모드는 아래 설명된 대로 구성으로 제어됩니다.

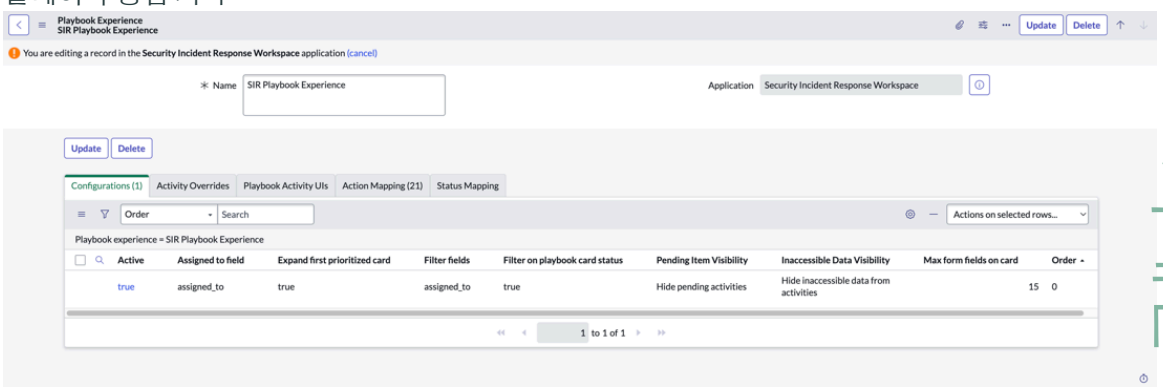
1. 다음으로 이동 모두 〉 플레이북 경험.
2. 플레이북 경험 페이지에서 **SIR** 플레이북 경험을 선택합니다.

플레이북 경험

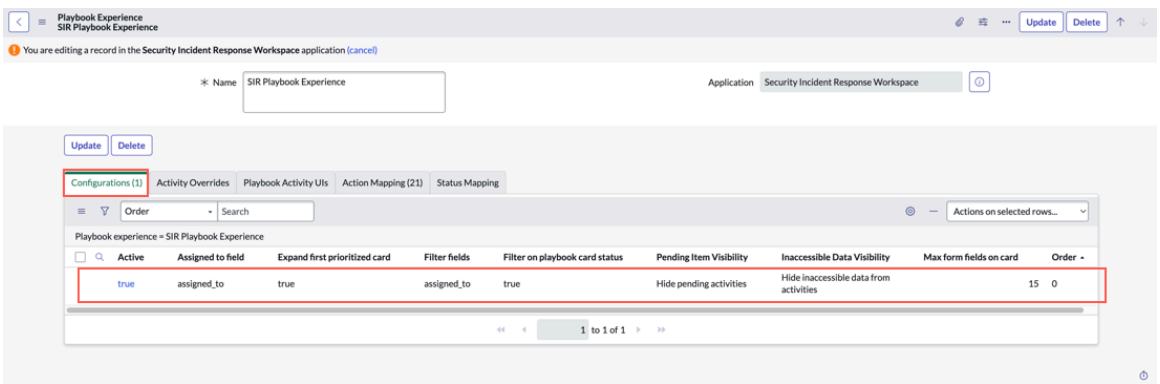


플레이북 경험 **SIR** 플레이북 경험 페이지가 표시됩니다.

플레이북 경험 기록



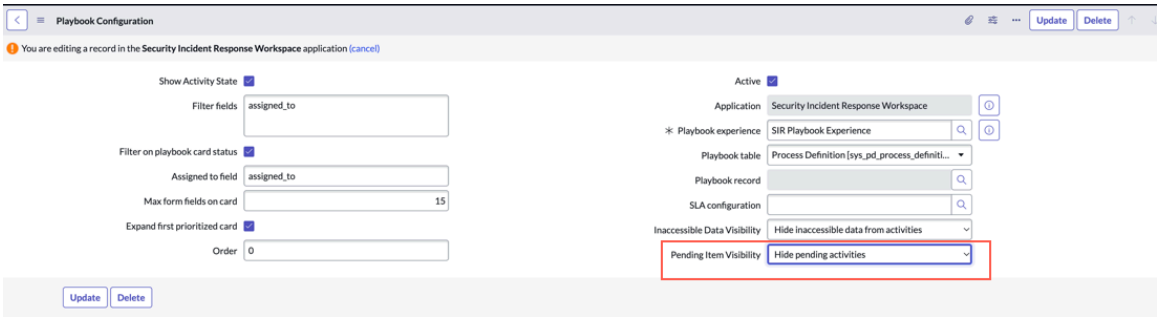
3. 구성 기록을 클릭합니다.



4. 구성 탭에서 SIR 플레이북 경험 구성을 클릭합니다.

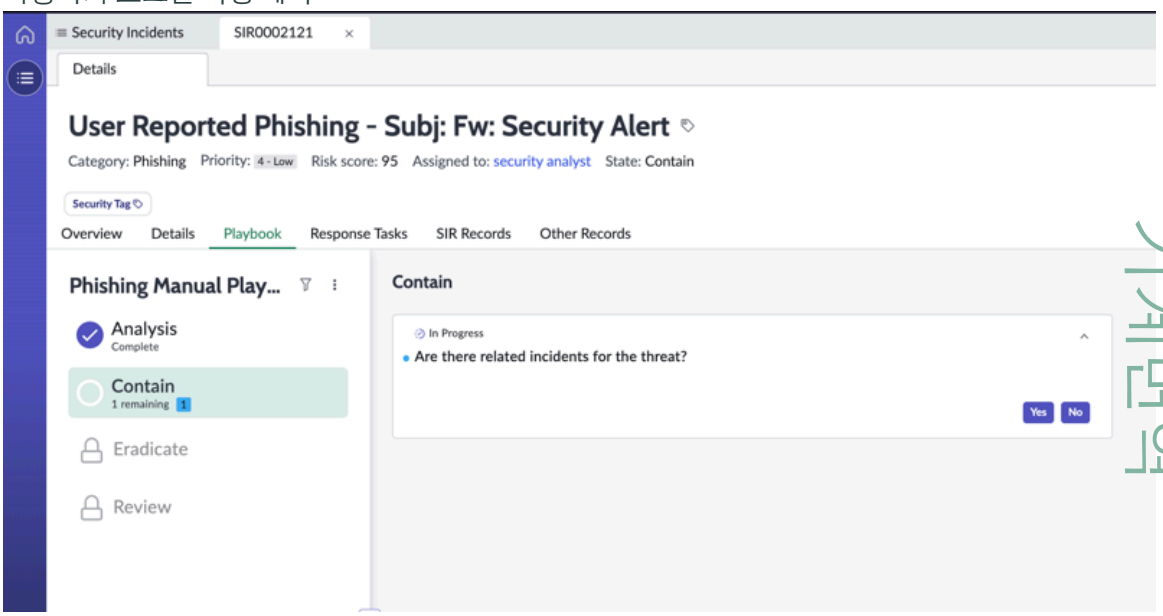
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

플레이북 구성



5. 보류 중인 항목 가시성 필드의 드롭다운 목록으로 이동하여 원하는 옵션을 선택하고 기록을 저장합니다. 다음 옵션 중에 선택합니다.
   - 보류 중인 활동 숨기기: 작업 공간의 플레이북 섹션에서 보려는 보류 중인 활동을 숨기려면 이 옵션을 선택합니다.

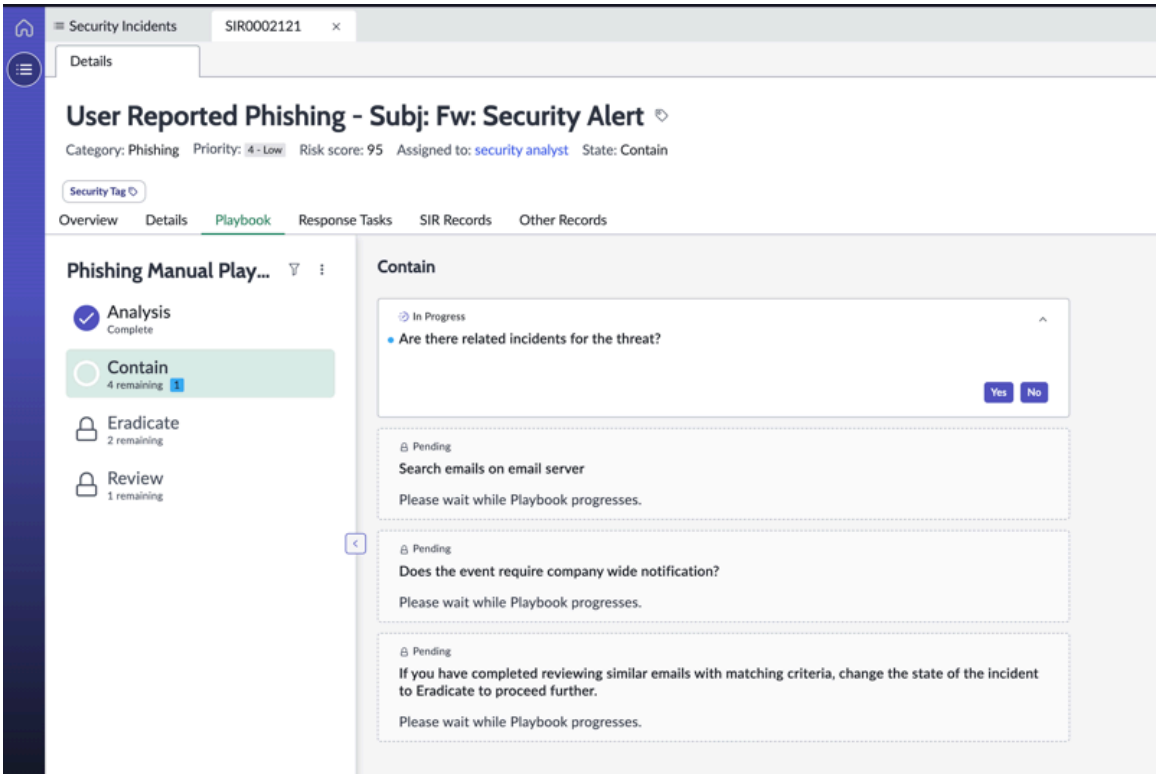
     사용자가 보고한 피싱 예시



   - 보류 중인 스테이지 및 활동 표시: 작업 공간의 플레이북 섹션에서 보려는 보류 중인 스테이지와 활동을 표시하려면 이 옵션을 선택합니다.

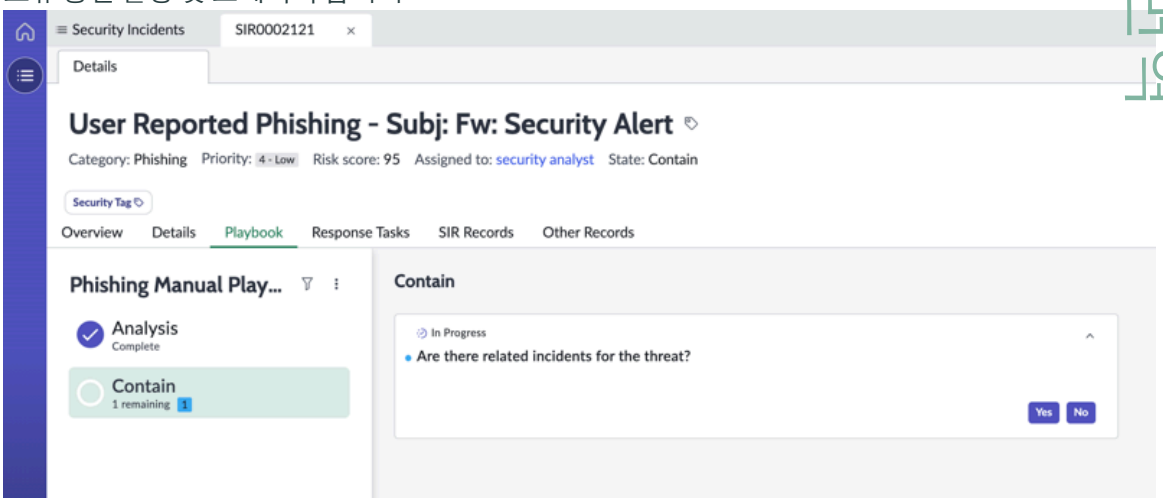
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보류 중인 스테이지 및 활동 표시



- 보류 중인 활동 및 스테이지 숨기기: 작업 공간의 플레이북 섹션에서 보려는 보류 중인 활동 및 스테이지를 숨기려면 이 옵션을 선택합니다.

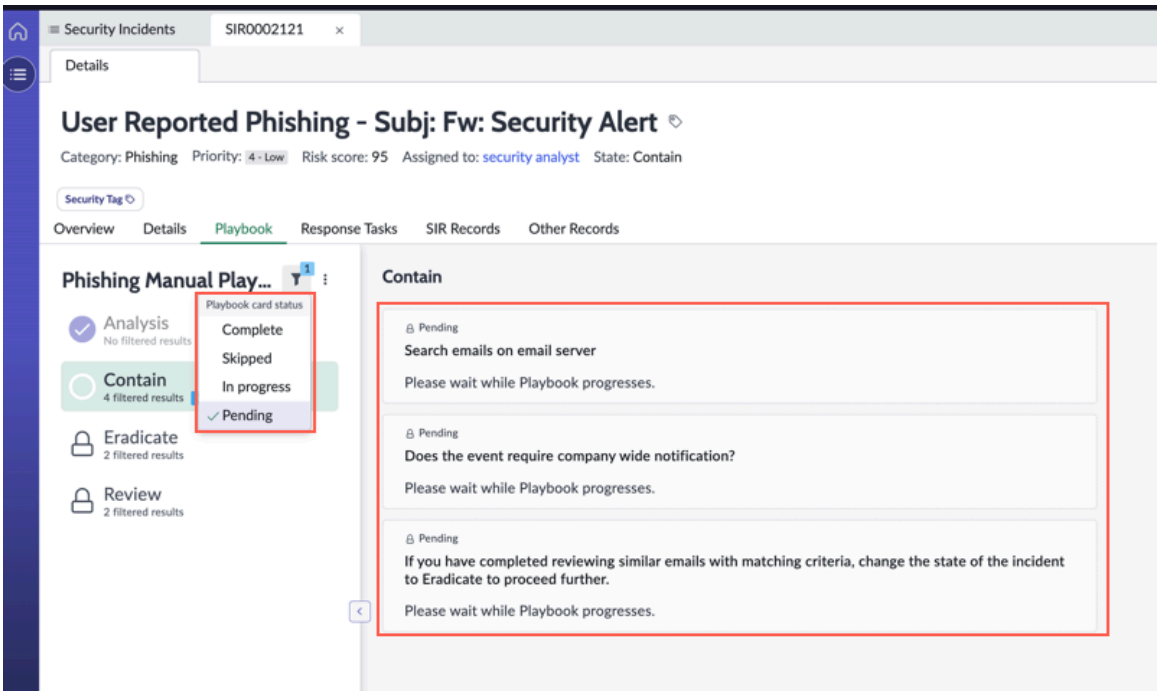
보류 중인 활동 및 스테이지 숨기기



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

6. 플레이북 섹션에서 필터 옵션을 사용하여 플레이북 카드 상태(활동 정의)를 기준으로 활동을 필터링합니다.

플레이북 카드 상태



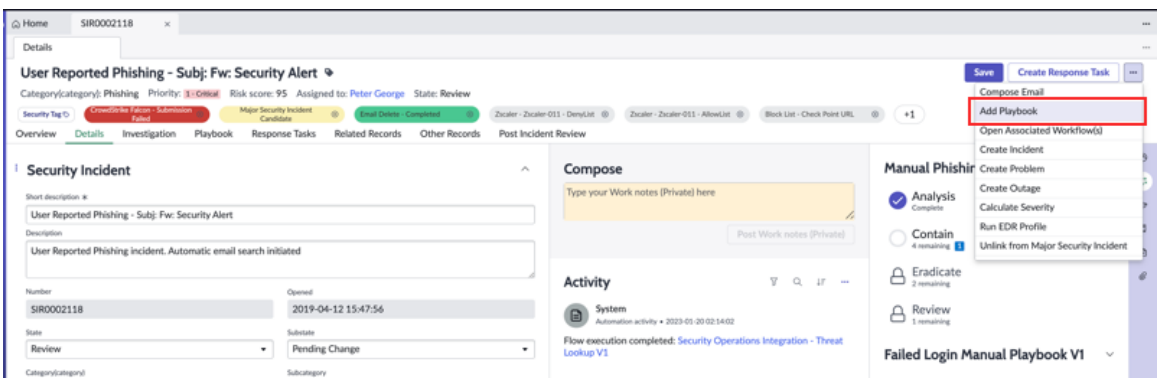
플레이북 추가

이 섹션을 사용하여 플레이북을 수동으로 추가합니다.

시작하기 전에
필요한 역할: sn_si.analyst

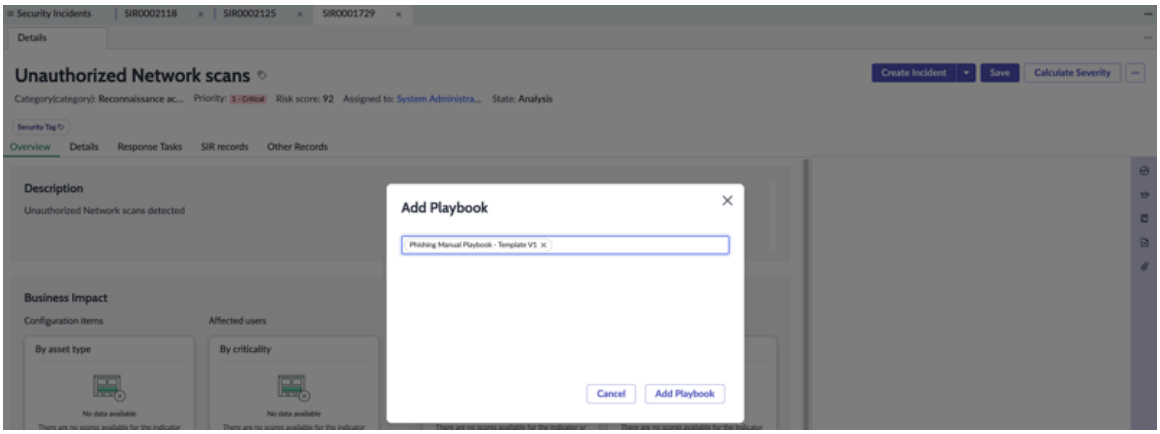
프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 보안 분석가 작업 공간.
2. 인시던트 기록을 엽니다.
3. 플레이북 추가를 클릭합니다.

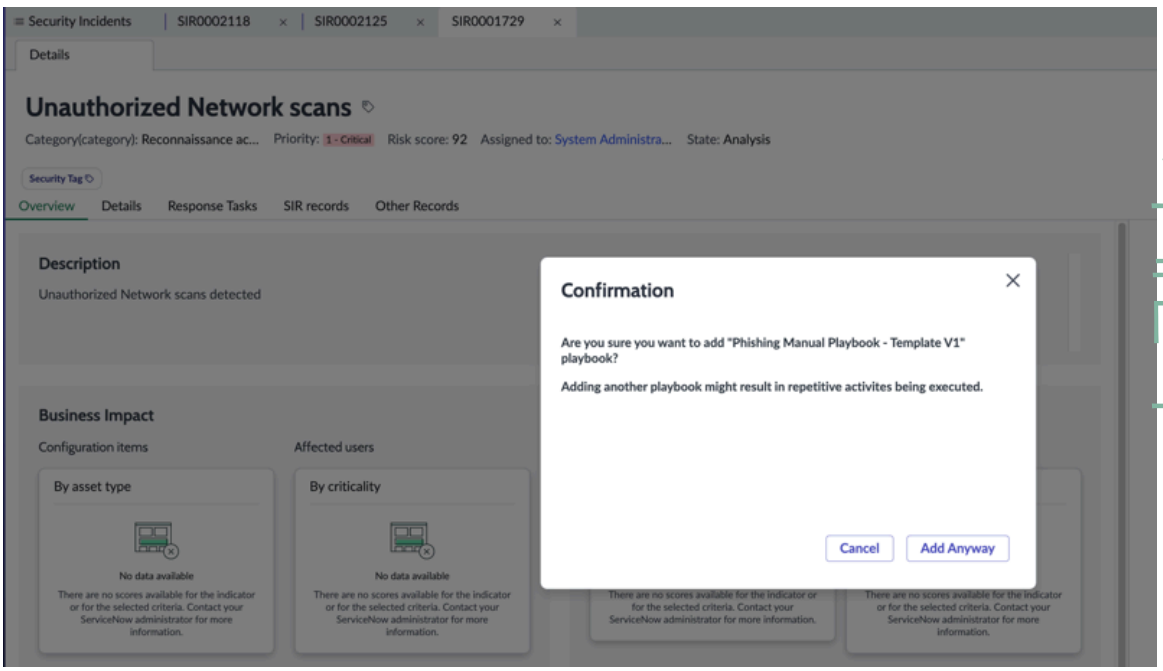


플레이북 추가 대화 상자가 표시됩니다.

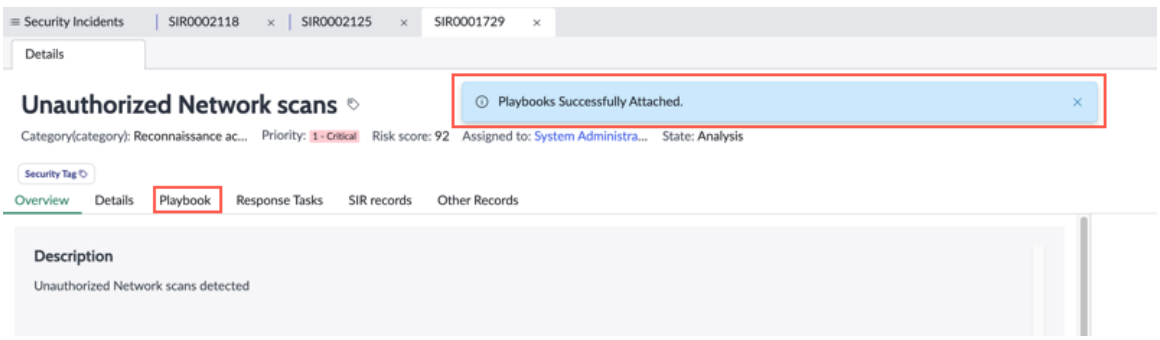
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 플레이북 템플릿을 선택합니다.
5. 플레이북 추가를 클릭합니다.
   확인할 수 있는 확인 메시지 대화 상자가 표시됩니다.
6. **Add** Anyway(계속 추가)를 클릭합니다.

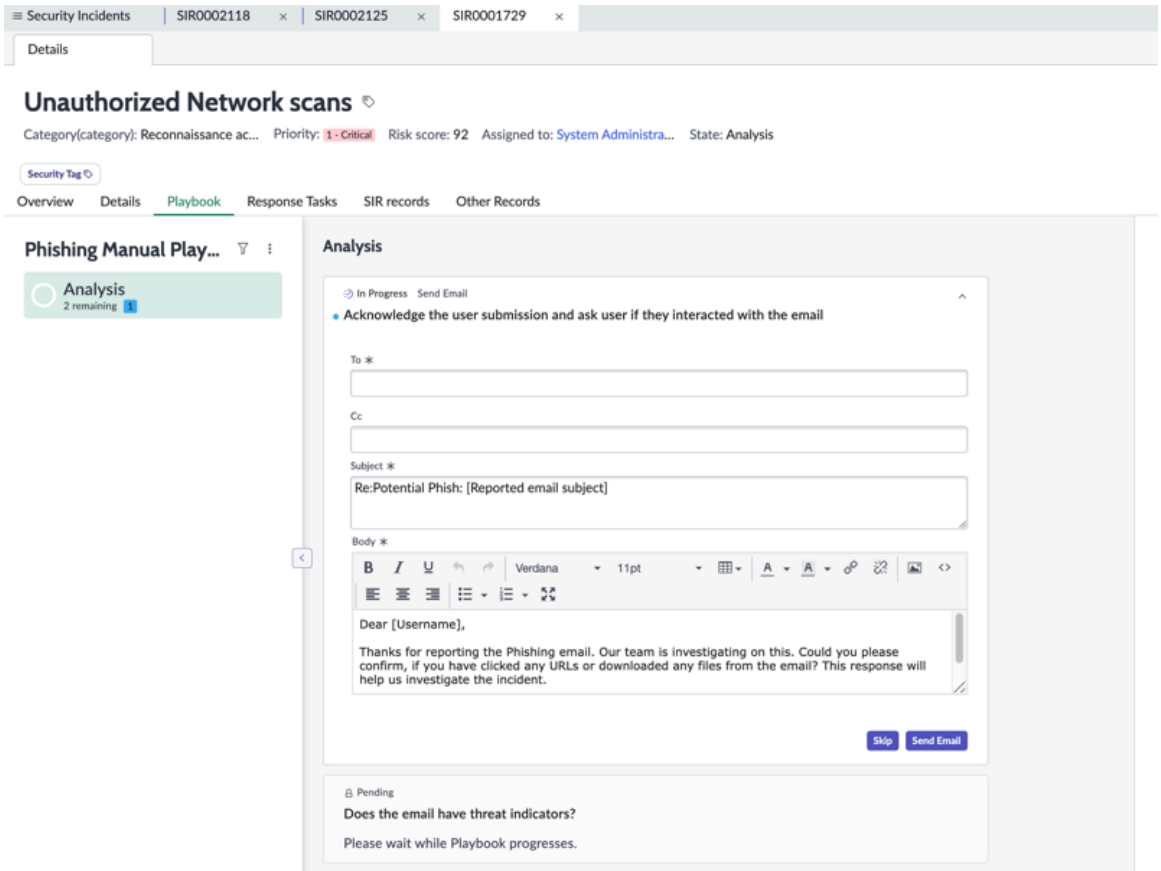


7. 플레이북이 상세 정보 탭 옆에 추가됩니다.



8. 플레이북 탭을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



9. 나열된 일련의 활동을 수행하여 다음 단계로 이동합니다.

> **주:**
> 보안 인시던트가 플레이북과 연결된 경우 연결된 플레이북이 종결되거나 취소될 때까지 사용자는 동일한 플레이북을 동일한 보안 인시던트에 다시 연결할 수 없습니다.

플레이북 사전 요구 사항

Playbook을 빌드하려면 다음 역할과 플러그인이 필요합니다.

필요한 역할: admin.

- PAD(프로세스 자동화 디자이너) [com.glide.pad.license] 플러그인을 활성화합니다.
- 플레이북 경험을 위해 다음 플러그인을 활성화합니다.
  - com.playbook_experience
  - now_playbook_exp
  - com.glide.playbook_experience.config
- 보안 운영 스포크를 활성화하여 플로우(com.snc.secops.spoke)에 액세스합니다.
- 엔터프라이즈 보안 케이스 관리 PAD Commons.

이 가이드를 시작하기 전에 Process Automation Designer 에 대한 Exploring playbooks 플랫폼 설명서를 읽었는지 확인하십시오.

에서 기존 플레이북 재빌드 워크플로우 스튜디오

기존 플로우를 에서 플레이북 워크플로우 스튜디오으로 직접 변환할 수 없습니다. 분석가를 안내하는 응답 작업을 생성하는 각 플로우 디자이너 단계는 별도의 동작 또는 하위 플로우로 세분화되어야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

기존 플로우를 의 플레이북 워크플로우 스튜디오으로 직접 변환할 수 없습니다. 분석가를 안내하는 응답 작업을 생성하는 각 플로우 디자이너 단계는 별도의 동작 또는 하위 플로우로 세분화되어야 합니다. 이러한 세분화된 하위 플로우 또는 작업을 사용하여 활동 정의를 생성해야 합니다. 이러한 활동 정의를 빌드하면 프로세스 정의의 스테이지 내에서 활동으로 추가됩니다. 여러 플레이북에서 활동 정의를 재사용할 수 있습니다.

각 활동을 사용자 지정하여 그 안에서 필요한 작업을 렌더링하고 활동 정의를 작성하는 동안 카드의 모양을 렌더링할 수 있습니다. 활동에는 이메일 클라이언트, 테이블, 작업, KB 문서, URL 등이 표시될 수 있습니다. 활동 정의 및 기본 작업 또는 하위 플로우가 생성되는 방법을 정의할 수 있습니다.

자세한 내용은 다음 섹션을 참조하십시오.

- 활동 정의
- Process Automation Designer

활동 정의

기본 ServiceNow AI Platform 시스템 내에서 몇 가지 활동 정의를 제공합니다. 또한 SIR 작업 공간 기본 시스템인 플레이북의 경우 엔터프라이즈 보안 케이스 관리 PAD 공통 애플리케이션의 기본 시스템에 정의된 몇 가지 활동 정의가 있습니다.

필요한 역할: sn_si.admin.

다음은 기본 시스템의 일부인 활동 정의 목록입니다.

활동 정의	테이블	설명	애플리케이션
환경이 없는 조건 대기	전역(global)	환경이 없는 조건 대기	엔터프라이즈 보안 케이스 관리 PAD 공통
CSF X Sandbox에 제출	보안 인시던트(sn_si_incident)	샌드박스에 제출	엔터프라이즈 보안 케이스 관리 PAD 공통
이메일 보내기	보안 인시던트(sn_si_incident)	SIR 플레이북에 대한 이메일 활동을 보냅니다.	엔터프라이즈 보안 케이스 관리 PAD 공통
이메일 검색	보안 인시던트(sn_si_incident)	이메일 서버에서 이메일 검색	엔터프라이즈 보안 케이스 관리 PAD 공통
작업 상태 업데이트	보안 인시던트(sn_si_incident)	작업 상태 업데이트	엔터프라이즈 보안 케이스 관리 PAD 공통
이메일 삭제	보안 인시던트(sn_si_incident)	이메일 삭제	엔터프라이즈 보안 케이스 관리 PAD 공통
예 아니요 결과	작업(task)	예상 결과	엔터프라이즈 보안 케이스 관리 PAD 공통

활동 정의 예시: 이메일 보내기

다음은 이메일 보내기 활동 정의의 예입니다.

기본

기본 상세 정보는 이름(레이블), 애플리케이션, 설명, 테이블 및 액세스 가능한 모든 애플리케이션을 캡처합니다.

자동화 계획, 활동 경험을 추가하고 제출합니다. 제출 후 문서를 편집하여 각 탭에 대한 상세 정보를 추가합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

자동화 계획

자동화 계획은 플로우 디자이너를 사용하여 빌드된 백엔드 작업 또는 하위 플로우를 연결합니다. 이 예에서는 다음을 사용합니다. 이메일 보내기 **- ESCM** 활동 하위 플로우.

이 하위 플로우를 사용하면 이메일 전송을 사용할 수 있습니다. 이메일을 보내는 핵심 논리가 있습니다. 모든 입력 필드와 출력 필드가 정의되어 있습니다.

모든 입력 필드는 자동화 계획 섹션 내에 표시됩니다. 각 입력 필드는 표준 모달, 표준 모달 및 구성 패널에서 관리자만 볼 수 있도록 설정할 수 있습니다.

- 관리자 가시성 전용: 관리자로 설정하면 관리자만 볼 수 있습니다.
- 표준 모델에 포함: 표준 모달에서 보기로 설정하면 속성 모달에만 나타납니다.
- 표준 모델 및 구성 패널에 포함: 표준 모달 및 구성 패널에서 보기로 설정하면 PAD 구성 패널과 속성 모달에 나타납니다. 자세한 내용은 활동 정의를 참조하십시오.

구성 시 이러한 값을 변경할 필요가 없는 경우 활동 정의 자체의 입력 필드를 정의할 수 있습니다. 이렇게 하면 비즈니스 프로세스 소유자가 프로세스 내에서 활동을 구성하는 동안 시간을 절약할 수 있습니다.

활동 경험

활동 경험 탭은 런타임에 활동 카드가 렌더링되는 방식을 정의합니다. 기본 시스템은 다음과 같은 환경 유형을 제공합니다.

- 승인
- 카탈로그 항목
- 기록 작성
- 교육용
- 지식
- 목록
- 알림
- 기록

선택한 경험 유형에 따라 추가 필드가 채워집니다. 자세한 내용은 설명서를 참조하십시오 ServiceNow AI Platform .

이 예에서는 기록 유형이 선택되었습니다.

주:
예를 들어 테이블을 렌더링하려면 목록을 경험 유형으로 선택할 수 있습니다.

관련된 기록

이 기록을 사용하여 현재 활동과 관련된 데이터를 저장합니다. 이렇게 하면 런타임 데이터와 경험 상태가 캡처됩니다.

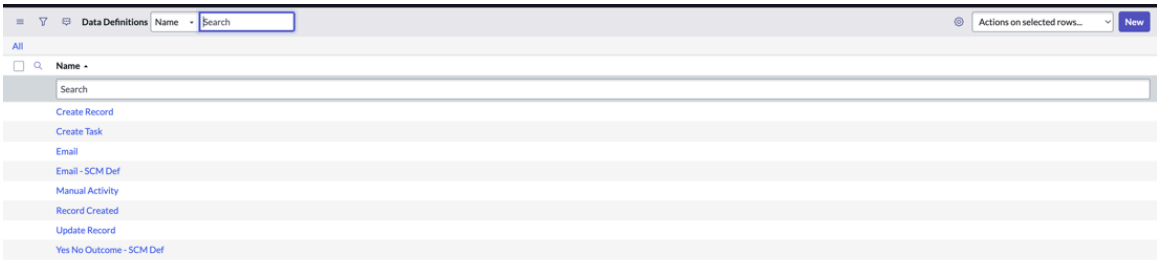
- 관련된 테이블: 플로우 데이터
- 관련된 기록: VL
- 경험 상태 테이블: 플로우 데이터
- 경험 상태 기록: VL

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 예시에서 플로우 데이터 테이블은 런타임 데이터를 캡처하는 데 사용됩니다. 실행 시간 데이터는 사용 사례에 따라 다를 수 있습니다. 이 예에서 실행 시간 데이터는 To, 참조, 주제 및 본문과 같은 필드입니다. 각 사용 사례마다 런타임 데이터의 유형을 정의하려면 플로우 데이터 정의를 생성해야 합니다.

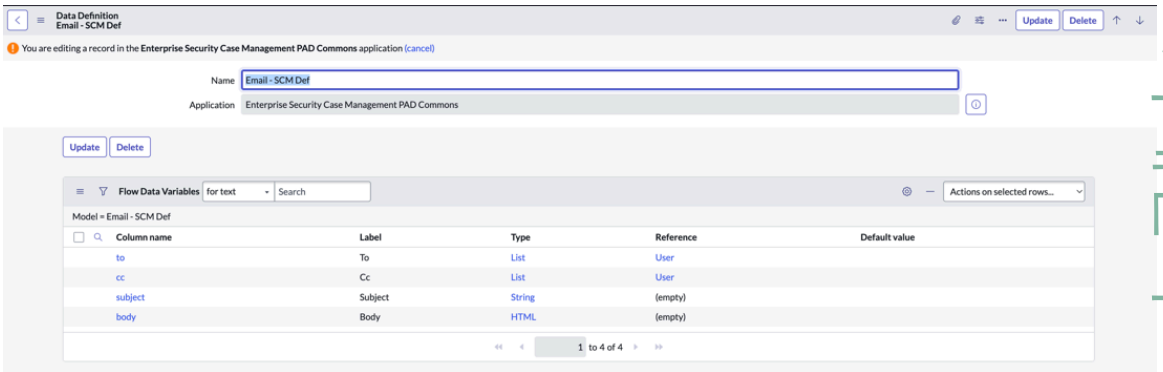
1. 왼쪽 창으로 이동하여 sys_flow_data_definition.list를 입력합니다. 플로우 데이터 테이블에 대해 생성된 정의 목록이 표시됩니다.

기록 연결



2. 이메일 열기 **- SCM** 정의 이 예제와 관련된 정의를 보려면 다음을 수행합니다.

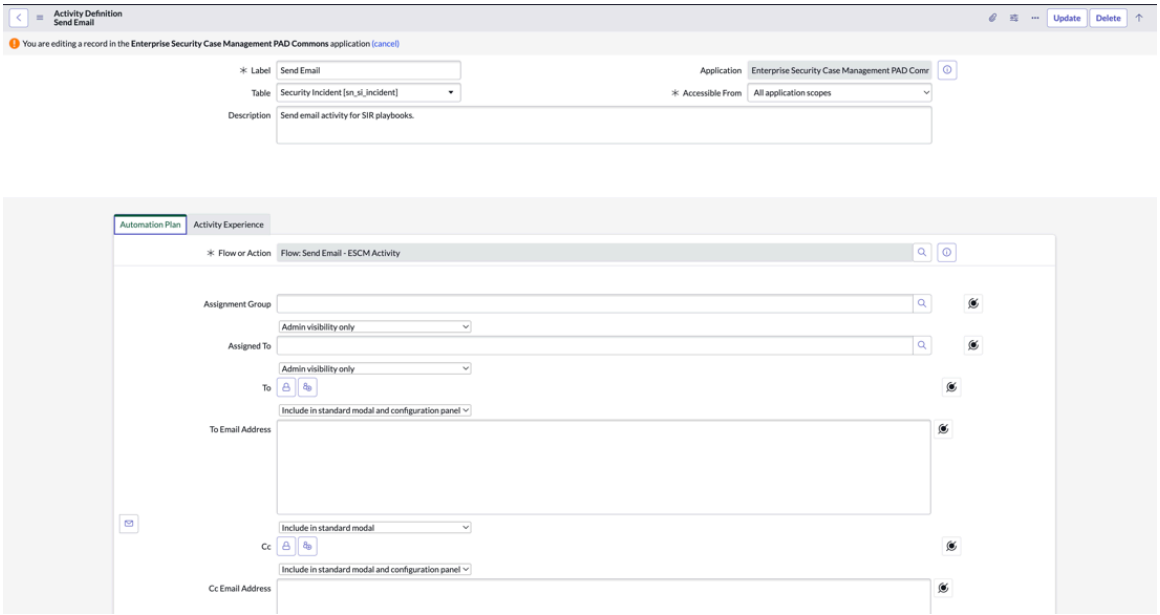
이메일 **- SCM def**



이 플로우 데이터 정의는 실행 시간 데이터를 캡처하기 위해 이 활동 정의(자동화 계획 참조)와 연결된 하위 플로우 또는 작업에서 사용해야 합니다.

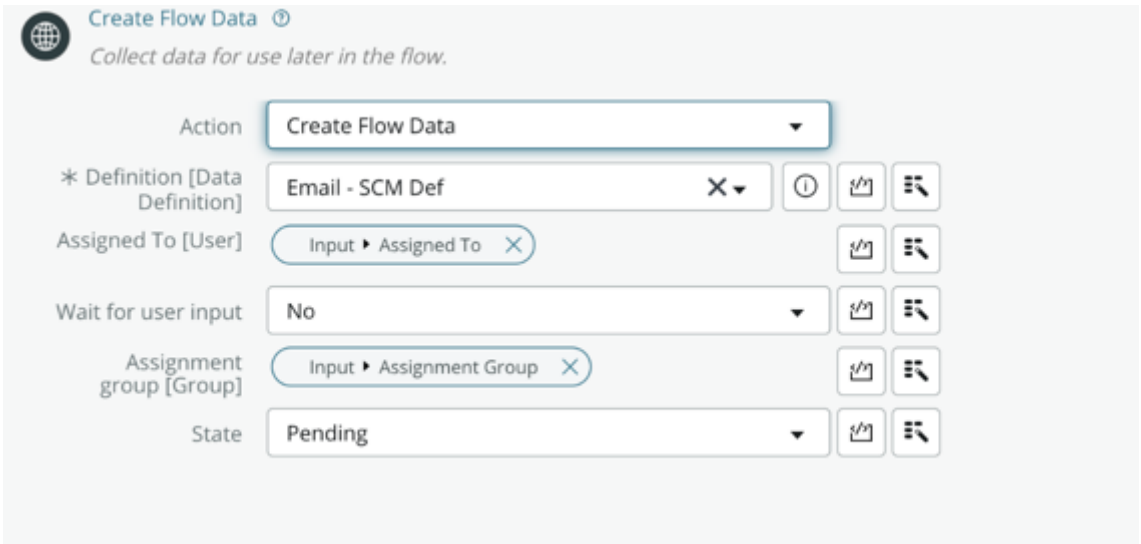
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

활동 정의



3. 이 예에서는 하위 플로우를 엽니다. 이메일 보내기 **- ESCM** 활동. 플로우 데이터 작성 단계에서 생성한 플로우 데이터 정의가 정의 필드에 매핑됩니다. 이 플로우 데이터 기록은 하위 플로우에서 사용됩니다. 이 예시에서는 활동 카드 상태(경험 상태)가 플로우 데이터 테이블에 캡처되어 있습니다.

이메일 보내기 **- ESCM** 활동



주:
예를 들어 응답 작업과 같이 플로우 데이터 테이블이 아닌 다른 테이블 기록에서 런타임 데이터를 캡처하려는 경우입니다. 연결된 테이블을 응답 작업 테이블로 선택할 수 있습니다. 연결된 기록은 하위 플로우에서 생성한 응답 작업 기록으로 설정되어야 합니다.

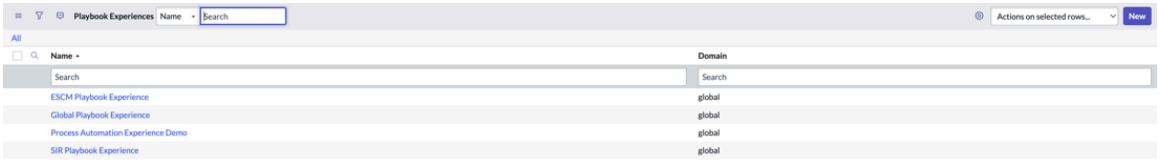
마찬가지로 경험 상태 테이블은 활동 카드의 상태를 캡처합니다. 기본 시스템에서 플로우 데이터 테이블의 상태 필드는 활동 카드 상태에 매핑됩니다. 따라서 플로우 데이터 테이블을 사용하여 경험 상태를 캡처하면 활동 카드 상태가 자동으로 업데이트됩니다. 플로우 데이터 테이블 이외의 다른 테이블을 사용하여 경험 상태를 캡처할 수도 있습니다.

예를 들어 응답 작업 상태를 활동 카드 상태에 매핑하려는 경우 가능합니다. 이렇게 하려면 다음을 수행하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

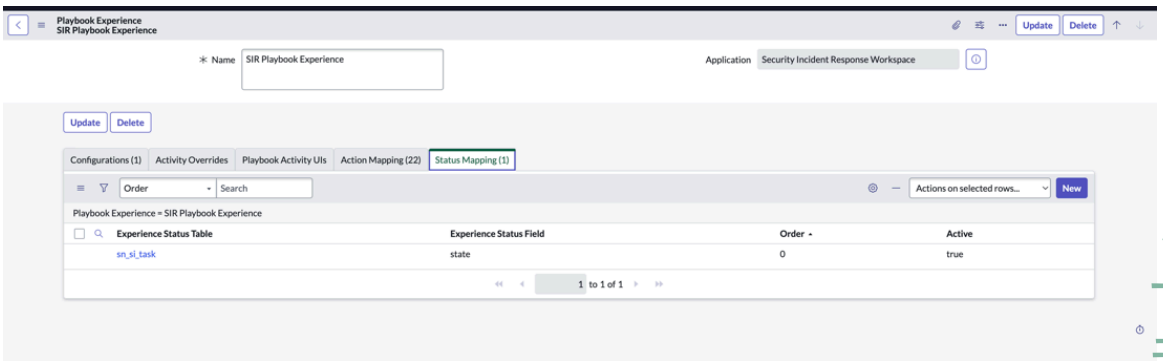
1. 다음으로 이동 모두 〉 플레이북 경험.

플레이북 경험



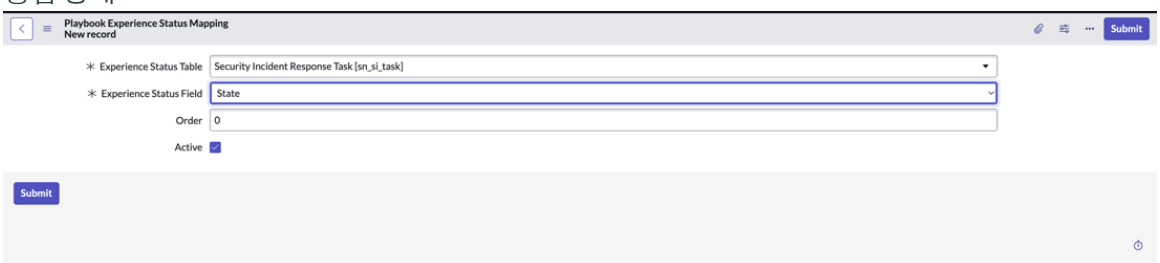
2. **SIR** 플레이북 경험을 엽니다.
3. 상태 매핑 관련 목록을 엽니다.

플레이북 경험



4. 경험 상태 테이블 필드에 대한 응답 작업을 입력합니다.
5. 경험 상태 필드에 대한 상태를 입력합니다.

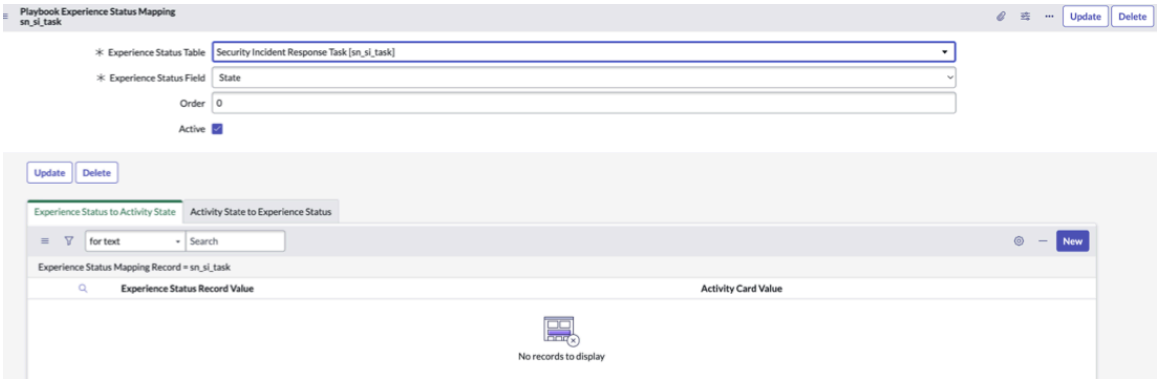
경험 상태



6. 제출을 클릭합니다. 레코드가 생성됩니다.

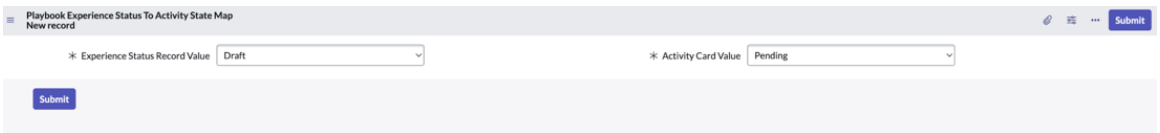
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

플레이북 경험 상태 매핑



7. 경험 상태 - 활동 상태에서 응답 작업의 상태를 활동 카드 상태에 매핑합니다.
8. 왼쪽에는 응답 작업의 상태가 표시되고 오른쪽에는 활동 카드 상태가 표시됩니다.

플레이북 경험 상태 매핑



9. 매핑은 양방향일 수 있습니다. 활동 상태와 경험 관련 목록에서도 상태를 올바르게 매핑합니다. 이 단계는 이전 단계의 반대입니다. 이 경우 왼쪽에는 활동 카드 상태가 표시되고 오른쪽에는 응답 작업 상태가 표시됩니다.

플레이북 경험 상태 매핑

상세 정보

- 태그 라인: 이메일 보내기
- 아이콘: 봉투 윤곽선(사용자 인터페이스에 표시되지 않음)
- 제목: 활동 〉 활동 인스턴스 〉 레이블. 여기에서 활동 인스턴스의 레이블을 선택했습니다. 이 닷워킹은 런타임에 레이블 값을 제목으로 동적으로 대체합니다.
- 설명: 활동 〉 활동 인스턴스 〉 설명. 여기에서 활동 인스턴스의 설명을 선택했습니다. 이 닷워킹은 런타임에 레이블 값을 제목으로 동적으로 대체합니다.
- 보류 중인 상태 제목: 이메일 알림을 보냅니다. 활동이 보류 중 상태일 때의 제목입니다.
- 보류 중인 상태 설명: 보내기 전에 이메일 제목과 본문을 확인하는 메시지를 표시합니다. 상태가 보류 중일 때 활동 카드에 대한 설명입니다. 기록 필드: 이 예에서는 선택된 기록 필드가 있습니다.

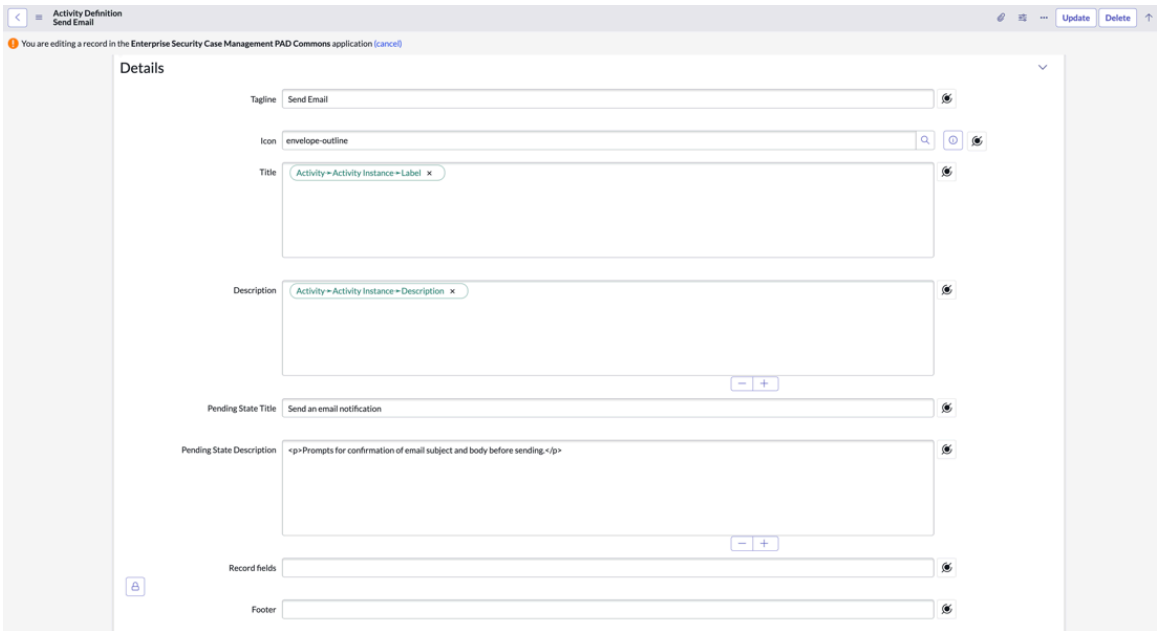
  기록 필드는 이름-값 쌍 목록에서 연결된 기록을 표시할 필드 이름의 목록으로, 쉼표로 구분됩니다. 데이터는 서버에서 미리 가져오고, 닷워킹이 지원되며, 각 필드에 대해 **canRead()** 권한이 평가됩니다.

- 바닥글: 이 예시에 대해 정의된 바닥글이 없습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

바닥글은 카드 바닥글의 회색 영역에 있는 텍스트입니다. 표시할 의미 있는 정보를 추가할 수 있습니다.

활동 정의 - 이메일 보내기

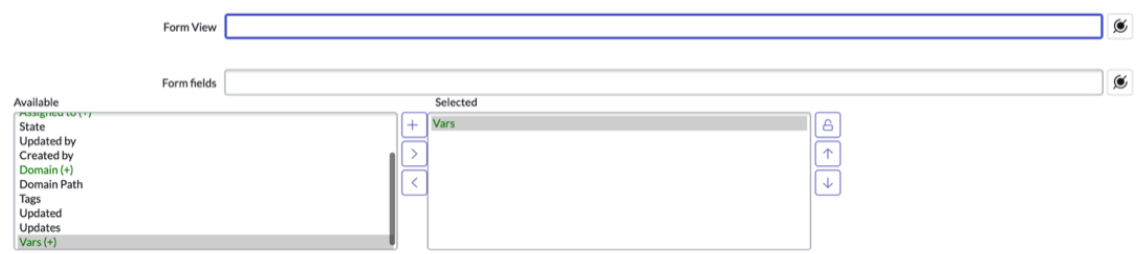


양식

- 양식 뷰: collect_data
- 양식 필드:

이 예시에서는 collect_data 뷰를 사용하여 입력을 입력하기 위해 사용자에게 제공해야 하는 필드를 표시합니다. Collect_data 뷰는 플로우 데이터 테이블에 해당하는 플랫폼 제공 뷰입니다. 또는 양식 뷰를 비워 두고 양식 필드에 대해 사용 가능한 값 목록에서 변수를 선택할 수 있습니다. (사용 가능한 값 목록을 열려면 자물쇠 아이콘을 클릭하십시오.)

양식 뷰



첨부 파일

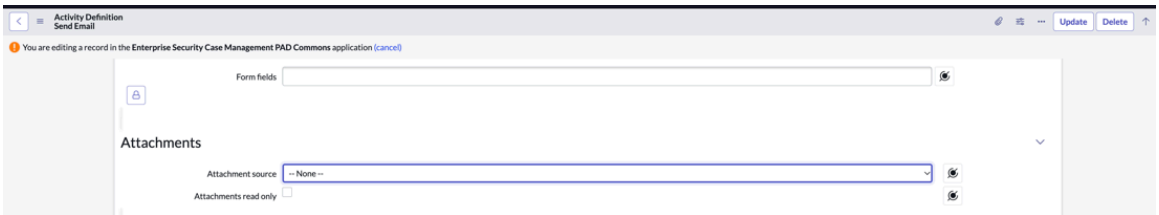
이 예는 다음과 같습니다.

- 첨부 파일 소스가 비어 있습니다.
- 첨부 파일 읽기 전용이 선택되지 않았습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

1. 첨부 파일 소스 - 드롭다운입니다. 카드에 표시할 첨부 파일: 상위 기록, 연결된 기록 또는 없음에 첨부된 첨부 파일입니다.
2. 첨부 파일 읽기 전용 - 예 또는 아니오입니다. 사용자가 기존 첨부 파일의 이름을 바꾸거나 삭제할 수 없도록 합니다.

활동 정의 - 이메일 보내기



기능

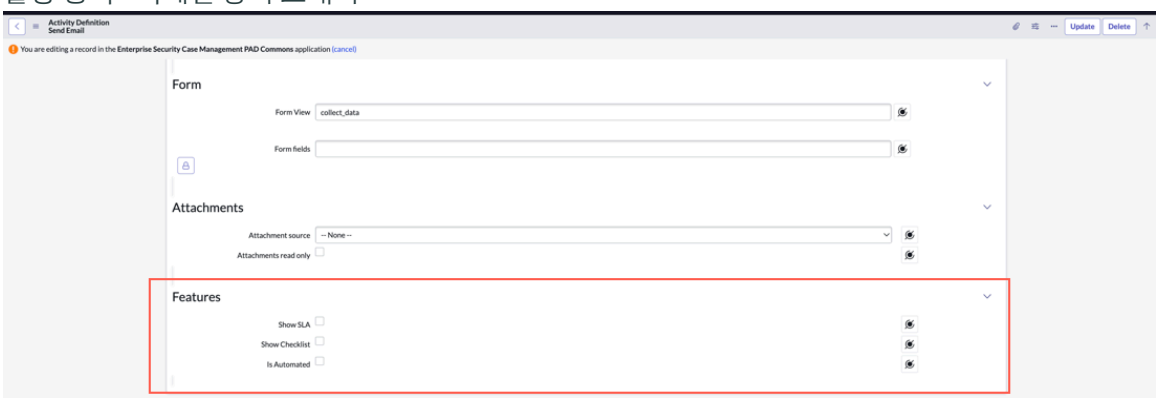
이 예에서는

- SLA 표시 - 지워짐
- 검사 목록 표시 - 지워짐
- 자동화됨 - 지워짐

SLA 표시: 예/아니오 관련된 기록에 대한 카드의 헤더에 SLA 타이머를 렌더링합니다. SLA는 플레이북 구성에 지정된 SLA 구성 기록에 따라 선택됩니다.

1. 검사 목록 표시 - 예 또는 아니오입니다. 연결된 기록에 첨부된 모든 검사 목록을 렌더링합니다. 검사 목록은 편집 가능하며 선언적 작업 없이도 변경 내용이 저장됩니다.
2. 자동화됨 - 예 또는 아니오입니다. 예일 경우 태그라인과 아이콘이텍스트 자동화 작업 및 자동화 아이콘으로 재정의됩니다.

활동 정의 - 이메일 양식 보내기



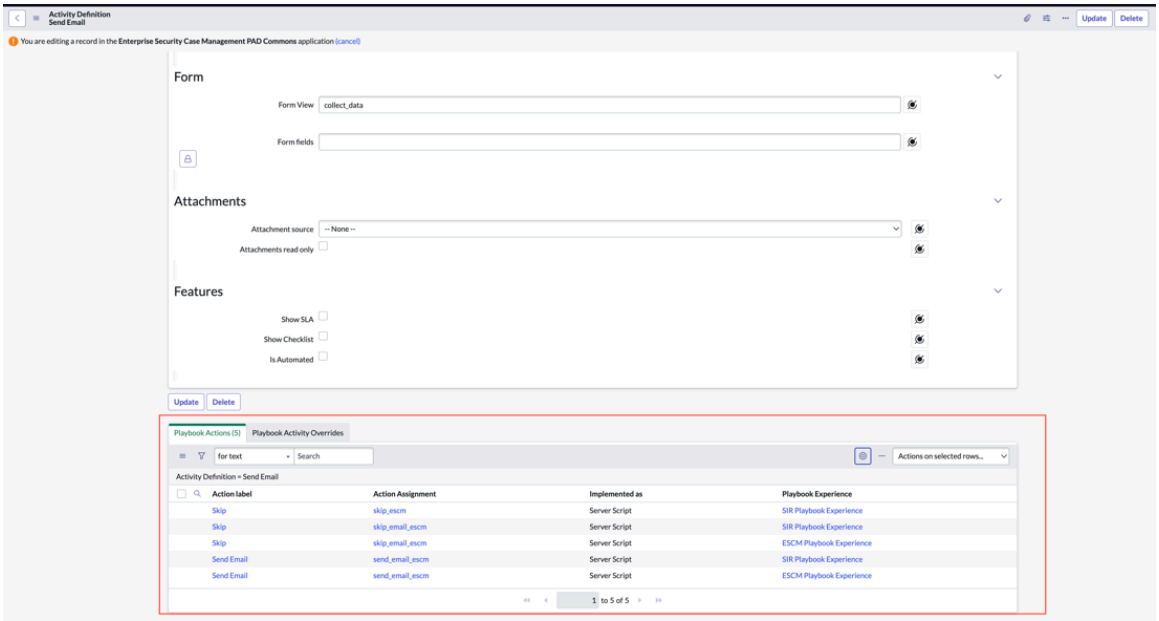
활동 정의의 플레이북 작업

이 섹션에는 활동 카드에서 렌더링될 작업이 있습니다. 이 예에는 건너뛰기 및 이메일 보내기 가동작으로 포함되어 있습니다.

활동 카드에 새 작업을 추가하려면 페이지 하단에 있는 플레이북 작업 관련 목록에서 기록을 생성해야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

플레이북 작업



1. 새로 만들기를 클릭합니다.
2. 작업 할당 필드에 대해 기존 활동 작업을 선택합니다.
3. 플레이북 경험 필드에 대해 **SIR** 플레이북 경험을 선택합니다.

활동 작업 생성

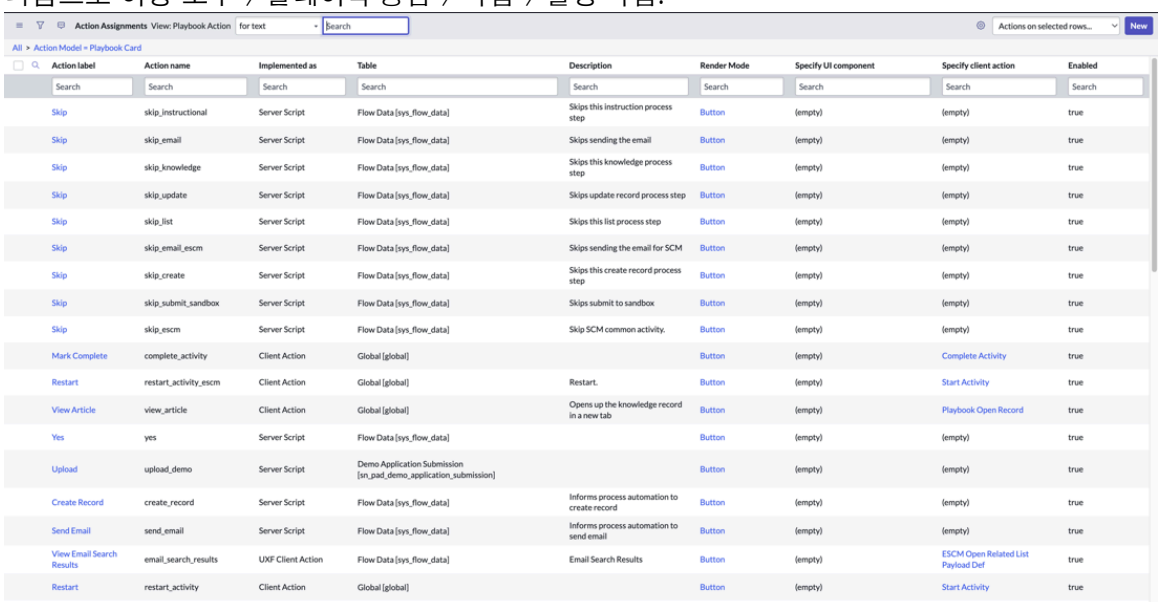
다음은 활동 작업을 생성하는 절차입니다.

시작하기 전에

필요한 역할: sn_si.admin

프로시저

1. 다음으로 이동 모두 〉 플레이북 경험 〉 작업 〉 활동 작업.



2. 새로 만들기를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이러한 작업을 생성하는 방법은 설명서를 참조하십시오 ServiceNow AI Platform . 이 예에서 건너뛰기는 서버 스크립트로 구현됩니다.

3. 플레이북 재정의:

   기존 활동 경험 유형을 재정의하려는 경우 가능합니다. 자세한 내용은 설명서를 참조하십시오 ServiceNow AI Platform . 이 예에 대한 플레이북 재정의가 없습니다.

CSF X Sandbox에 제출

CSF X Sandbox에 제출은 활동 정의 프로세스의 예입니다.

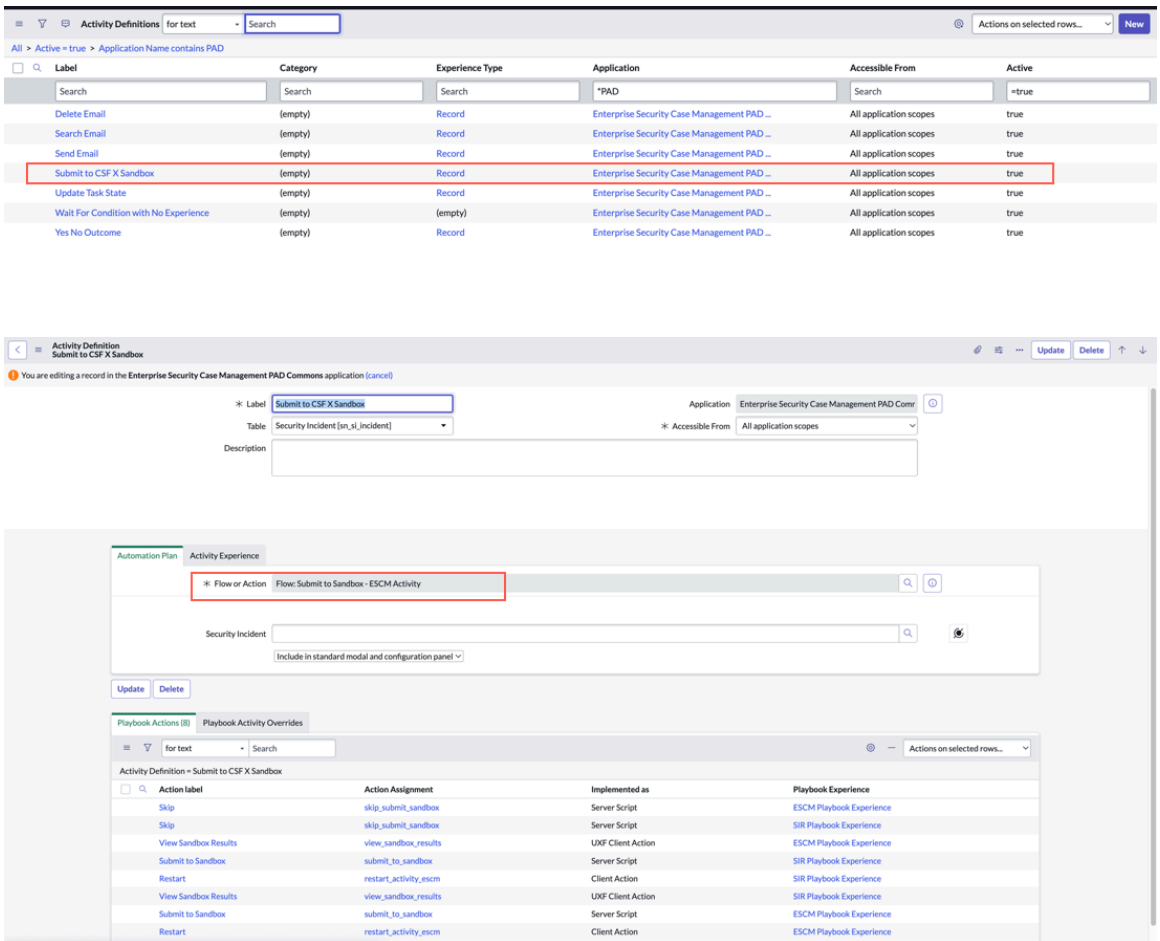
기본

기본 상세 정보는 이름(레이블), 애플리케이션, 설명, 테이블 및 액세스할 수 있는 모든 애플리케이션을 캡처합니다.

자동화 계획, 활동 경험을 추가하고 제출합니다. 제출이 완료되면 문서를 편집하여 각 탭에 대한 상세 정보를 추가합니다.

자동화 계획

자동화 계획은 플로우 디자이너를 사용하여 빌드된 백엔드 작업/하위 플로우를 연결합니다. 이 예에서는 Sandbox에 제출 **- ESCM** 활동하위 플로우를 사용합니다.



이 하위 플로우를 사용하면 악성 옵저버블을 샌드박스에 제출할 수 있습니다. 모든 입력 필드와 출력 필드가 정의되어 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 인시던트가 입력 필드입니다.

활동 경험

이 예에서는 기록 유형이 선택되었습니다.

관련된 기록

연결된 기록은 현재 활동과 관련된 데이터를 저장하는 것입니다. 이렇게 하면 런타임 데이터와 경험 상태가 캡처됩니다.

- 관련된 테이블: 플로우 데이터
- 관련된 기록: VL
- 경험 상태 테이블: 플로우 데이터
- 경험 상태 기록: VL

상세 정보

- 태그 라인: 이메일 보내기
- 아이콘: 봉투 윤곽선
- 제목: 활동 〉 활동 인스턴스 〉 레이블. 여기에서 활동 인스턴스의 레이블을 선택했습니다. 이 닷워킹은 런타임에 레이블 값을 제목으로 동적으로 대체합니다.
- 설명: VL(하위 플로우 출력이 매핑됨)
- 보류 중인 상태 제목: 비어 있음
- 보류 중인 상태 설명: 비어 있음
- 기록 필드
- 바닥글

양식

- 양식 뷰: 비어 있음
- 양식 필드: 비어 있음

첨부 파일

이 예는 다음과 같습니다.

- 첨부 파일 소스 - 없음
- 첨부 파일 읽기 전용 - 선택 안 됨

1. 첨부 파일 소스 - 드롭다운입니다. 카드에 표시할 첨부 파일: 상위 기록, 연결된 기록 또는 없음에 첨부된 첨부 파일입니다.
2. 첨부 파일 읽기 전용 - 예/아니오입니다. 사용자가 기존 첨부 파일의 이름을 바꾸거나 삭제할 수 없도록 합니다.

기능

이 예에서는

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- SLA 표시 - 선택 안 됨
- 검사 목록 표시 - 선택 안 됨
- 자동화됨 - 선택 안 됨

활동 정의의 플레이북 작업

이 섹션에는 활동 카드에서 렌더링될 작업이 있습니다.

이 예제에는 건너뛰기, 샌드박스 결과 보기, 샌드박스에 제출 및 다시 시작 작업이 있습니다.

활동 카드에 새 작업을 추가하려면 페이지 하단에 있는 플레이북 작업 관련 목록에서 새 기록을 생성해야 합니다.

플레이북 재정의

이 예에 대한 플레이북 재정의가 없습니다.

SIR 작업 공간용 샘플 플레이북

복잡한 코드를 작성하지 않고도 SIR Workspace용 Playbook을 빠르고 쉽게 생성하거나 구성할 수 있습니다. 이러한 Playbook을 사용하여 보안 위협을 단계별로 해결할 수 있습니다. 보안 인시던트 플레이북 플로우를 자동 또는 수동으로 호출할 수 있습니다.

보안 인시던트 응답은 기본 시스템과 함께 다음과 같은 플레이북을 제공합니다.

- 수동 피싱을 위한 플레이북
- 자동화된 피싱을 위한 플레이북
- 수동 맬웨어를 위한 플레이북
- 자동화된 맬웨어에 대한 플레이북
- 실패한 로그인에 대한 플레이북 수동

MSI 기록 작업

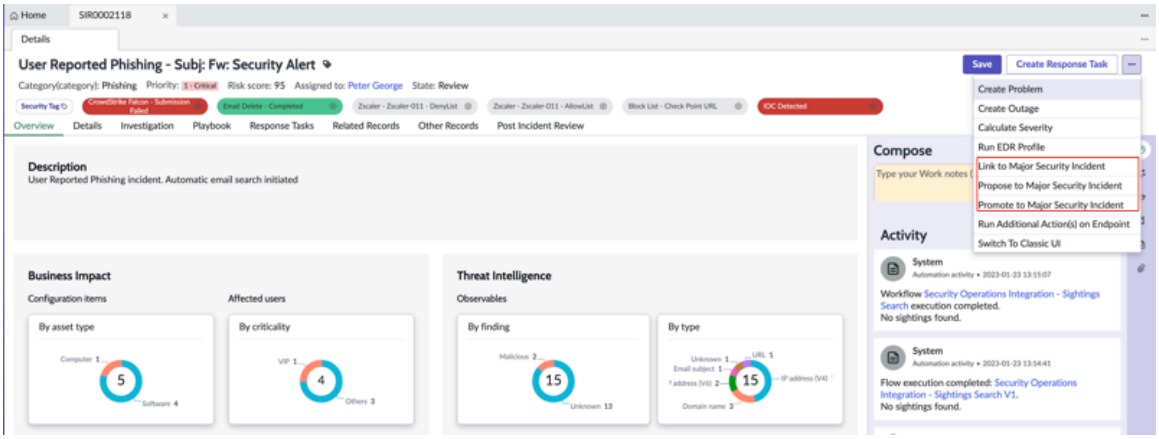
보안 인시던트 응답 작업 공간을 사용하면 인시던트가 조직에 중요한 위협으로 식별될 때 보안 인시던트를 중요 보안 인시던트로 제안, 승격 또는 연결할 수 있습니다.

인스턴스에 (MSIM)ServiceNow AI Platform을 설치한 중요 보안 인시던트 관리 후에는 보안 인시던트를 중요 인시던트로 전환하는 작업을 처리할 수 있습니다.

중요 보안 인시던트 관리 (MSIM) UI 작업은 SIR 작업 공간의 보안 인시던트 양식 배너 오른쪽 상단에 표시됩니다. 해당하는 경우 UI 작업을 선택합니다.

주:
일부 작업은 상황에 따라 다릅니다. 예를 들어 연결 해제 작업은 보안 인시던트가 이미 제안 또는 승격되었거나 중요 보안 인시던트에 연결된 경우에만 사용할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



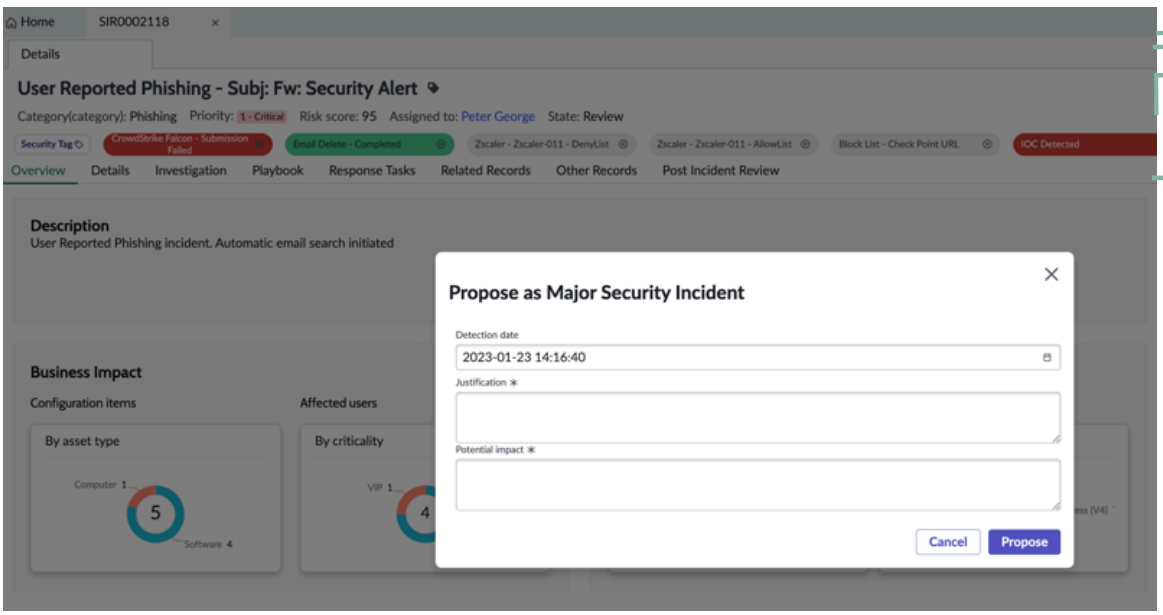
중요 보안 인시던트로 제안

보안 인시던트를 MSI(주요 보안 인시던트)로 제안합니다.

시작하기 전에
필요한 역할: sn_si.analyst.

프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간.
2. 보안 인시던트를 엽니다.
3. 중요 보안 인시던트에 제안을 클릭합니다.



4. 양식에서 탐지 날짜, 근거 및 잠재적 영향과 같은 필드에 내용을 입력합니다.
5. 제안을 클릭합니다.
   인시던트 기록은 중요 보안 인시던트 후보로 제안됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

인시던트 기록이 중요 보안 인시던트 후보로 제안되면 중요 보안 인시던트 후보 태그가 적용되고 보안 인시던트 양식 배너에 표시됩니다.

주:
제안하지 않거나 중요한 영향을 미치지 않는 경우 중요 보안 인시던트에서 연결 해제 를 클릭하여 인시던트의 연결을 해제합니다. 인시던트의 연결이 해제되고 목록 뷰 아래의 목록이 정정을 위해 보안 분석가에게 전달됩니다.

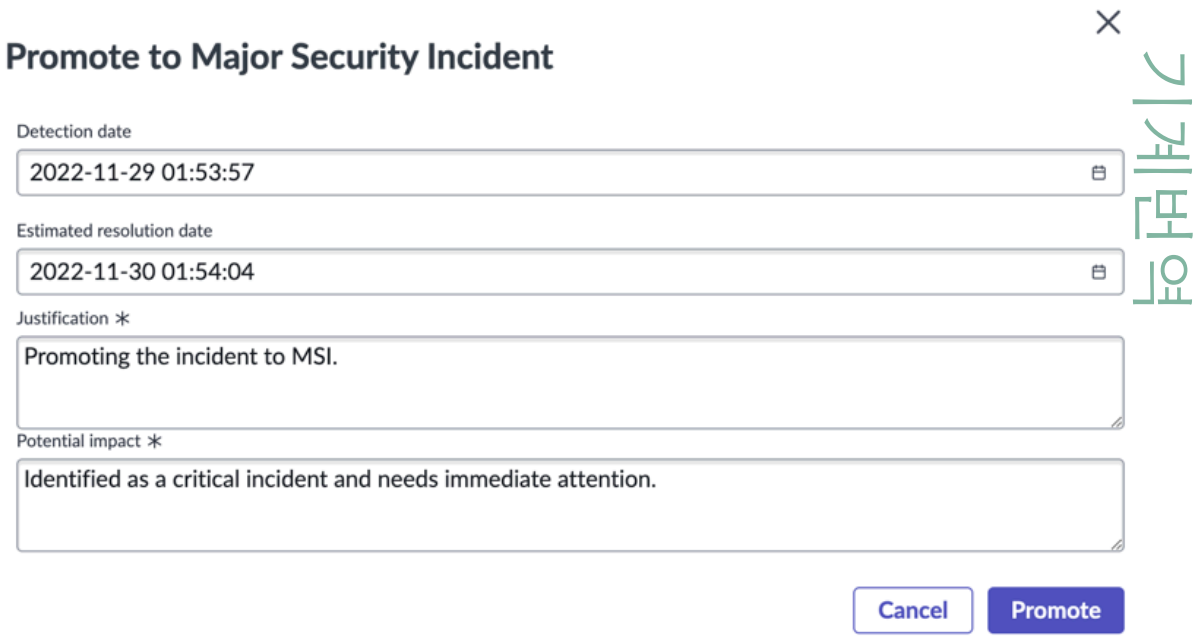
중요 보안 인시던트로 승격

보안 인시던트를 중요 보안 인시던트로 승격

시작하기 전에
필요한 역할: sn_si.analyst.

프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간.
2. 보안 인시던트를 엽니다.
3. 중요 보안 인시던트로 승격을 클릭합니다.
4. 양식에서 탐지 날짜, 예상 해결 날짜, 근거 및 잠재적 영향과 같은 필드에 내용을 입력합니다.



5. 승격을 클릭합니다.
   인시던트 기록은 중요 보안 인시던트로 승격됩니다.
   인시던트 기록이 중요 보안 인시던트로 승격되면 중요 보안 인시던트 태그가 적용되어 양식 배너에 표시됩니다.

주:
중요 보안 인시던트의 연결을 해제할 수도 있습니다. 인시던트가 중요하지 않은 경우 인시던트의 연결이 해제되고 보안 분석가의 정정을 위한 목록 뷰 아래에 나열됩니다.

중요 보안 인시던트에 연결

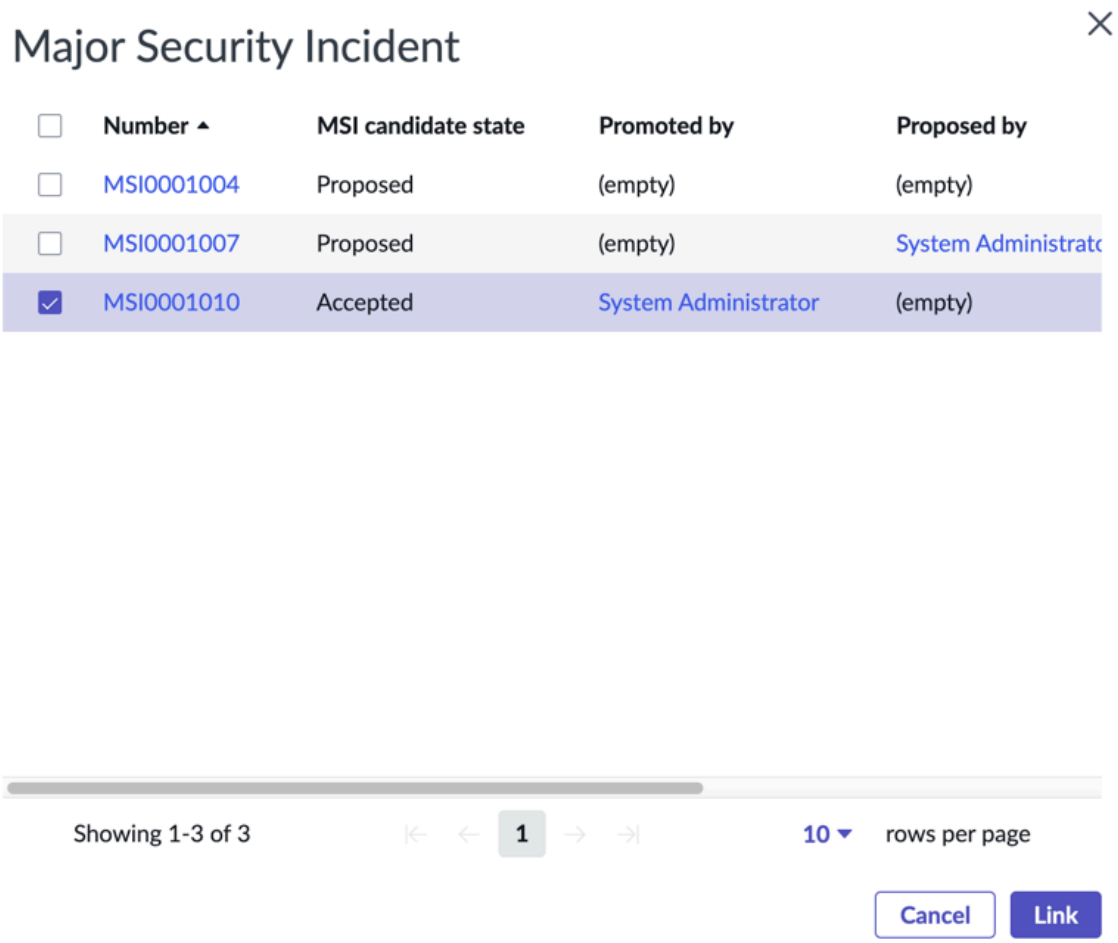
보안 인시던트를 주요 보안 인시던트에 하위 보안 인시던트로 연결합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_si.analyst.

프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간.
2. 보안 인시던트를 엽니다.
3. 중요 보안 인시던트에 연결을 클릭합니다.



4. 중요 보안 인시던트에 연결할 인시던트를 선택합니다.
5. 링크를 클릭합니다.
6. 인시던트 기록은 중요 보안 인시던트의 하위 인시던트로 연결됩니다.
   인시던트가 중요 보안 인시던트에 하위 인시던트로 연결되면 중요 보안 인시던트 태그가 적용되고 양식 배너에 표시됩니다.

양식 UI 작업 작업

다음은 보안 인시던트 양식에 표시되는 UI 작업입니다.

양식 UI 작업을 탐색하려면

1. 이동 작업 공간 〉 보안 인시던트 응답 작업 공간.
2. 목록 뷰에서 보안 인시던트를 선택합니다.
3. 모든 UI 작업은 보안 인시던트 양식의 오른쪽 상단 모서리에 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

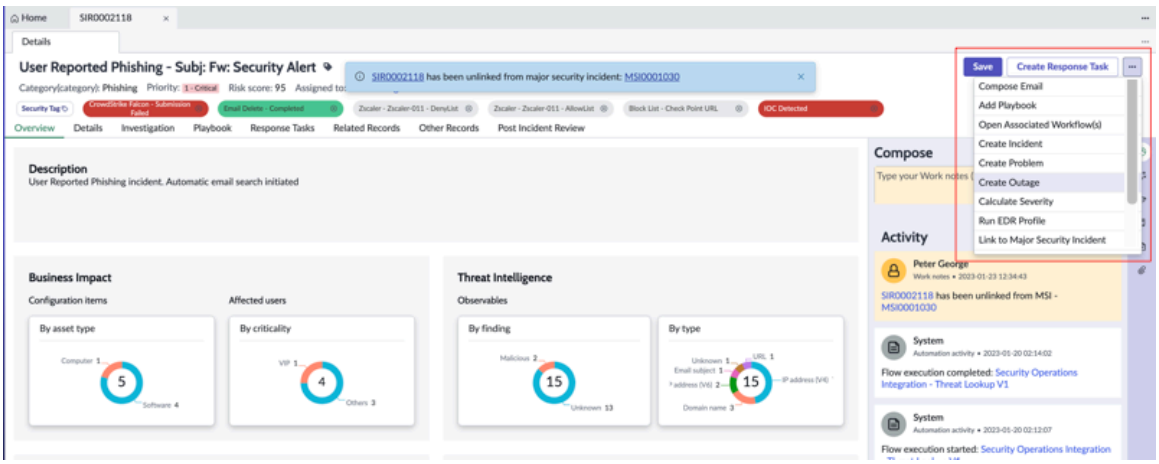
작업 공간 양식 **UI** 작업

필드 이름	설명
토론	보안 인시던트에 대한 사이드바 토론을 생성하거나 시작합니다.
저장	변경한 후 보안 인시던트 응답 기록을 저장하거나 업데이트합니다.
응답 작업 생성	보안 인시던트에 대한 응답 작업을 생성합니다.
이메일 작성	보안 인시던트에 대한 이메일을 작성합니다.
플레이북 추가	보안 인시던트에 대한 플레이북을 수동으로 추가합니다.
인시던트 생성	보안 인시던트 내에서 인시던트를 생성합니다.
고객 서비스 케이스 생성	고객 서비스 관리(CSM) 팀에서 추적할 보안 인시던트에 대한 고객 서비스 케이스를 만듭니다. 주: 이 옵션은 고객 서비스 관리(CSM)가 설치된 경우에만 사용할 수 있습니다.
연결된 **Wokflow** 열기	보안 인시던트와 관련된 워크플로우 컨텍스트를 엽니다. 이 옵션은 워크플로우가 있는 경우에만 표시됩니다.
변경 요청 생성	보안 인시던트 내에서 변경 요청을 생성합니다.
문제 생성	보안 인시던트 내에서 문제를 만듭니다.
중단 작성	보안 인시던트 내에 중단을 생성합니다.
심각도 계산	미리 정의된 계산기를 사용하여 보안 인시던트의 심각도를 계산합니다. 심각도는 계산기의 미리 정의된 규칙을 기반으로 계산됩니다. 인시던트 심각도는 위험 점수, 비즈니스 영향 및 우선순위를 기반으로 합니다.
EDR 프로파일 실행	필요한 통합에 대한 EDR 프로파일을 선택하고 실행합니다. 주: 이 옵션은 통합이 설치된 경우에만 사용할 수 있습니다.
중요 보안 인시던트에 연결	보안 인시던트를 중요 보안 인시던트와 연결합니다.
위험 이벤트 보고	이 보안 인시던트를 위험 관리 팀에 위험 이벤트로 보고하십시오. 위험 관리 팀은 이벤트를 분석하여 해당 이벤트 및 관련 손실이 재발하지 않도록 합니다. 주: 이 옵션은 위험 관리가 설치된 경우에만 사용할 수 있습니다.
중요 보안 인시던트에서 연결 해제	중요 보안 인시던트에서 연결을 해제합니다.
중요 보안 인시던트로 제안	보안 인시던트를 중요 보안 인시던트로 제안합니다.
중요 보안 인시던트로 승격	보안 인시던트를 중요 보안 인시던트로 승격합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드 이름	설명
엔드포인트에서 추가 작업 실행	엔드포인트에서 추가 작업을 실행합니다. 주: 이 옵션은 엔드포인트 통합이 설치된 경우에만 사용할 수 있습니다. 예: FireEye HX
MISP에서 새 이벤트 작성	MISP에서 이벤트를 자동 또는 수동으로 작성하고 수정합니다. 주: 이 옵션은 MISP 통합이 설치된 경우에만 사용할 수 있습니다.
MITRE ATT&K 기술 연결	MITRE ATT&K 기술을 보안 인시던트에 연결합니다. 주: 이 옵션은 MITRE ATT&K가 설치된 경우에 사용할 수 있습니다.
MITRE ATT&K 정보 표시	보안 인시던트와 관련된 MITRE ATT&K 정보를 표시합니다. 주: 이 옵션은 MITRE ATT&K가 설치된 경우에 사용할 수 있습니다.
보안 케이스에 추가	기존 또는 새 보안 케이스에 보안 인시던트를 추가합니다. 주: 이 옵션은 Threat Intel이 설치된 경우 사용할 수 있습니다.
클래식 UI로 전환	분석가가 새 작업 공간에서 아직 사용할 수 없는 기존 기능에 대한 작업도 수행할 수 있도록 분석가가 클래식 UI와 새 UI 간에 전환할 수 있도록 합니다.
취소	보안 인시던트를 취소합니다. 응답 작업과 같은 모든 관련 기록 취소 를 선택하면 하위 보안 인시던트도 취소됩니다.
삭제	보안 인시던트 기록을 삭제합니다.

4. 보안 인시던트 기록을 보려면 보안 인시던트 번호를 클릭하십시오. 페이지 상단에서 UI 작업을 볼 수 있습니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 인시던트 종결 워크플로우

인시던트 상태를 업데이트하여 보안 인시던트를 종결합니다.

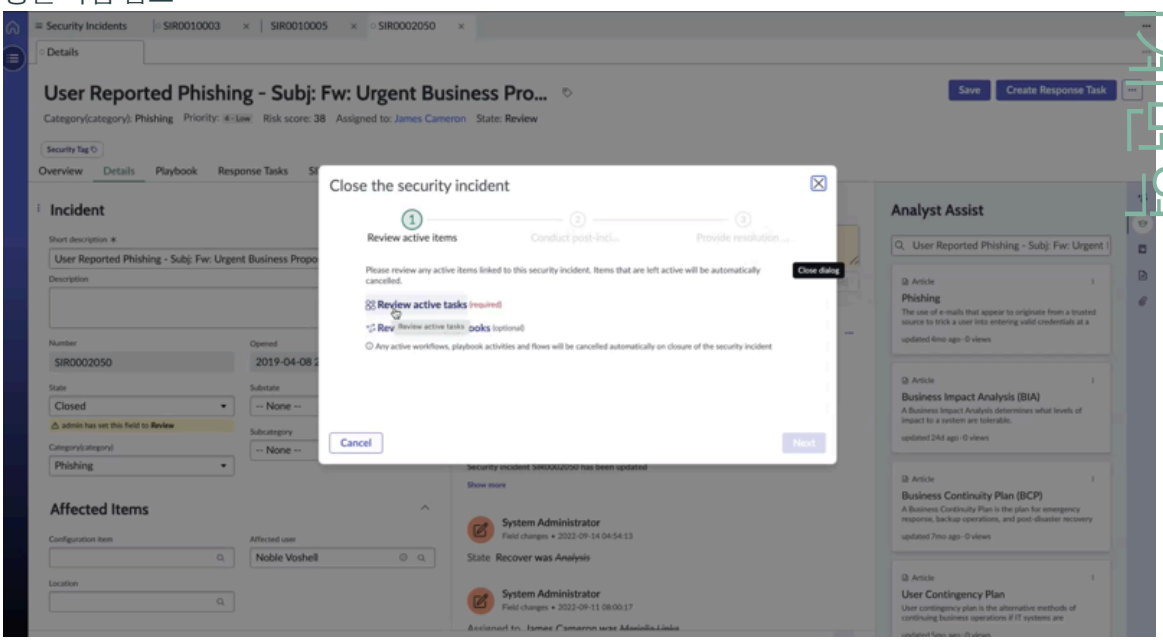
시작하기 전에
필요한 역할: sn_si.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간.
2. 예를 들어, 목록 〉 보안 인시던트 〉 오픈 인시던트.
3. 종료하려는 인시던트를 엽니다.
4. 세부 정보 탭으로 이동합니다.
5. 인시던트 상태로 드릴다운하고 종결을 선택합니다.
6. 종결 작업을 수행합니다.

   - 보안 인시던트를 종결하기 전에 모든 작업을 검토하기 위한 필수 단계입니다. 보안 인시던트로 종결하기 전에 분석가가 모든 응답 작업을 검토하고 종결하거나 취소해야 합니다. 분석가가 활성 작업 검토를 클릭하면 사용자가 응답 작업 탭으로 이동합니다. 보안 인시던트를 종결하는 중임을 알리는 세션 메시지가 표시됩니다. 계속을 클릭합니다.
   - 계속을 클릭합니다. 첫 번째 단계 – 보안 인시던트 종결의 활성 작업 검토가 완료되었습니다.

     종결 작업 검토

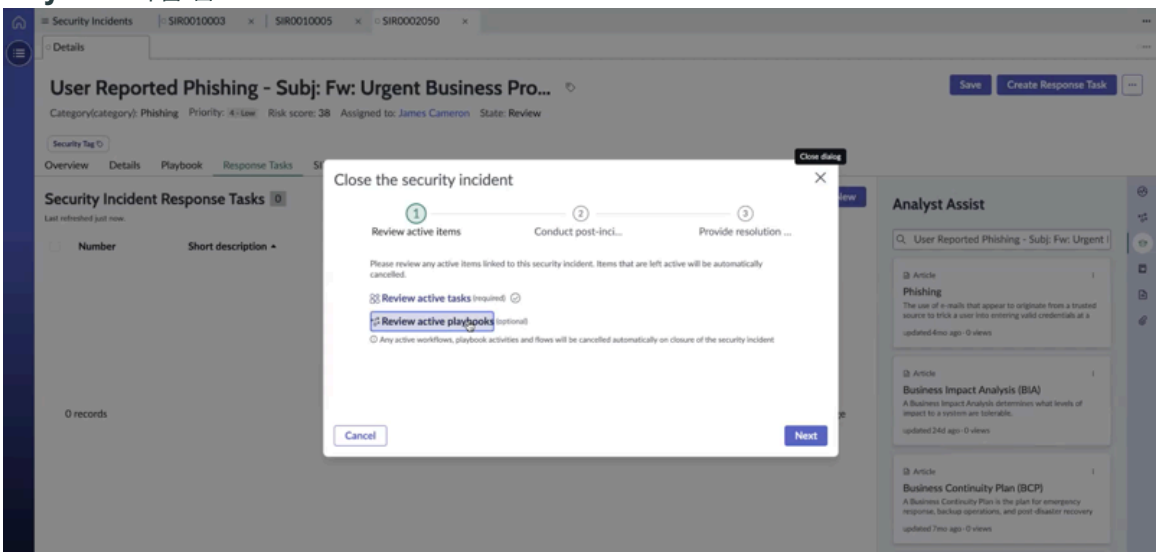
     

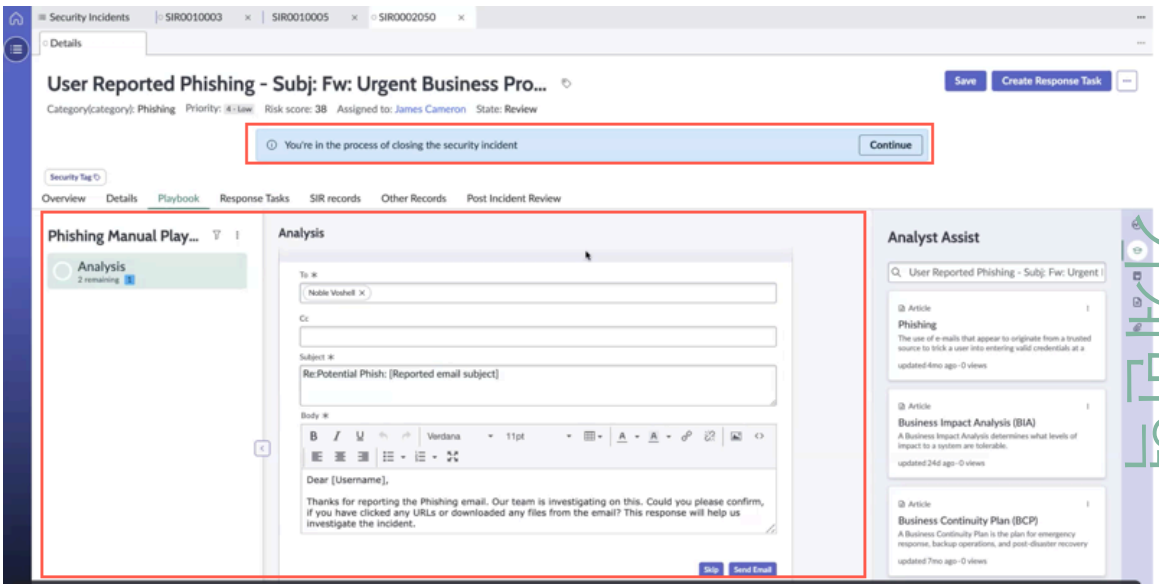
   - 다음 단계로 이동하여 분석가가 검토할 활성 플레이북을 검토합니다(선택 사항). 링크를 클릭하여 활성 플레이북 작업을 검토하고 필요한 경우 닫을 수 있습니다.

     주:
     보안 인시던트가 종결되면 활성 워크플로우, Playbook 활동 및 플로우가 자동으로 취소됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Playbook 작업 검토



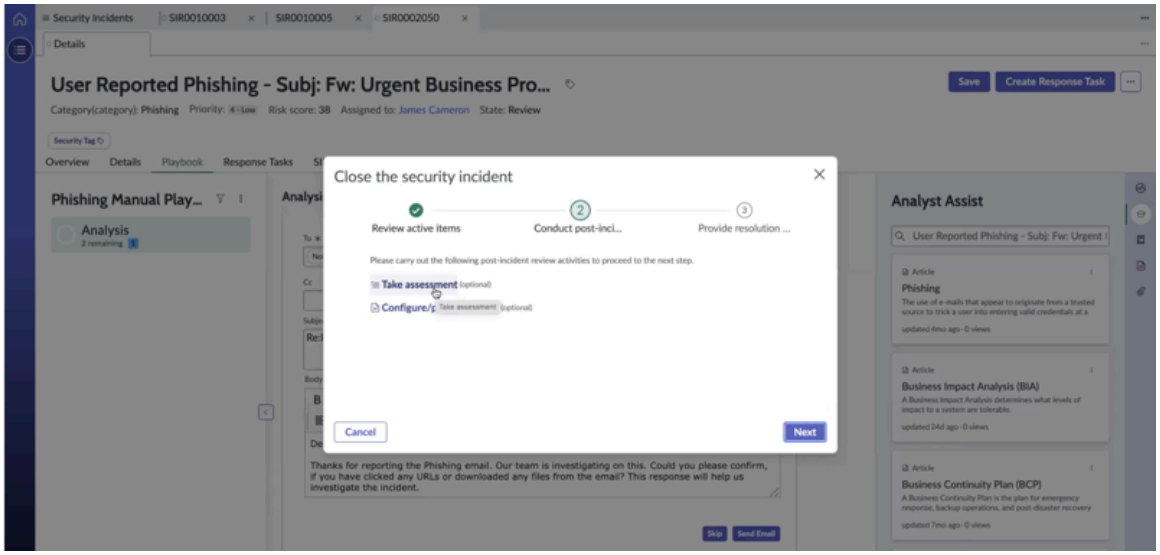


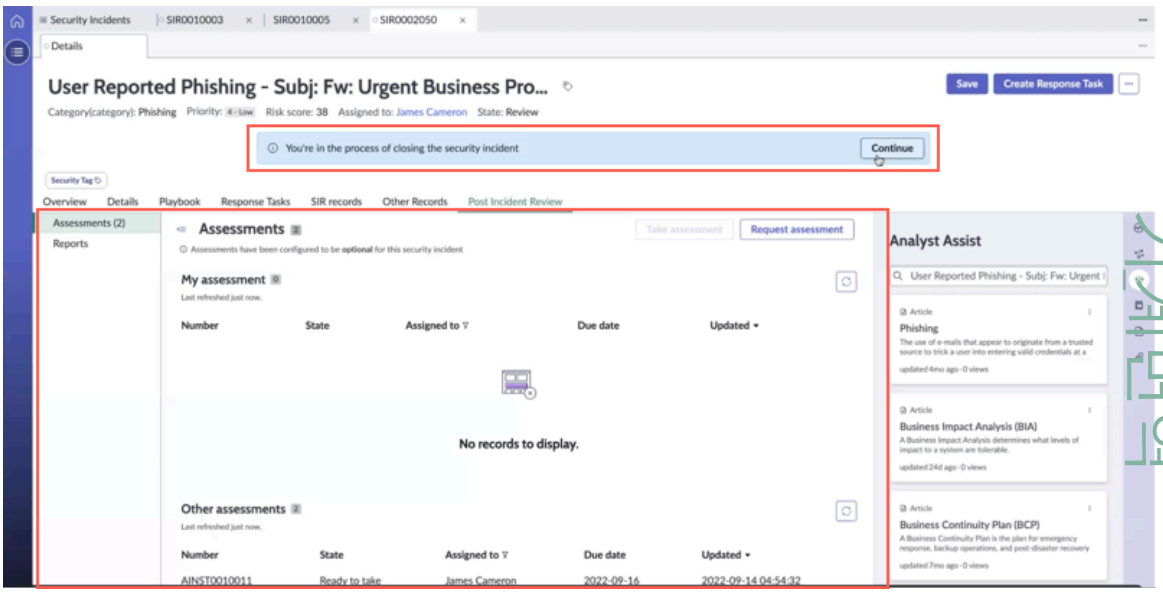
기계번역

- 사후 인시던트 검토 보고서: 이제 종결을 계속 진행하기 위해 사후 인시던트 활동을 검토하도록 이동됩니다. 평가가 선택 사항이면 단계를 건너뛰거나 평가가 필수인 경우 평가를 수행하고 완료합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

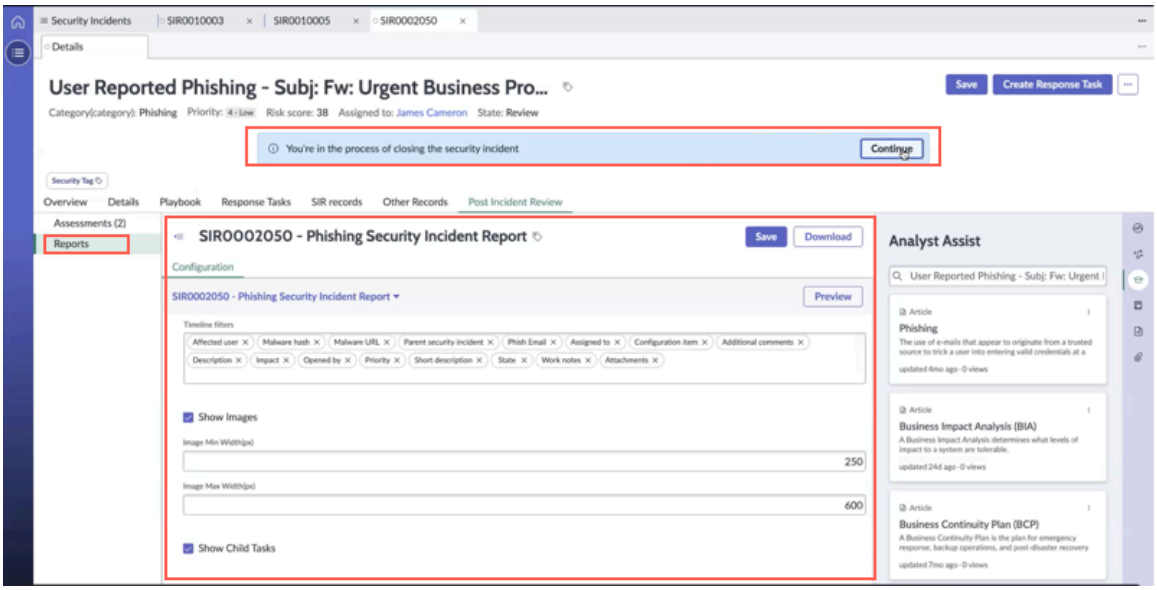
검토/평가 수행



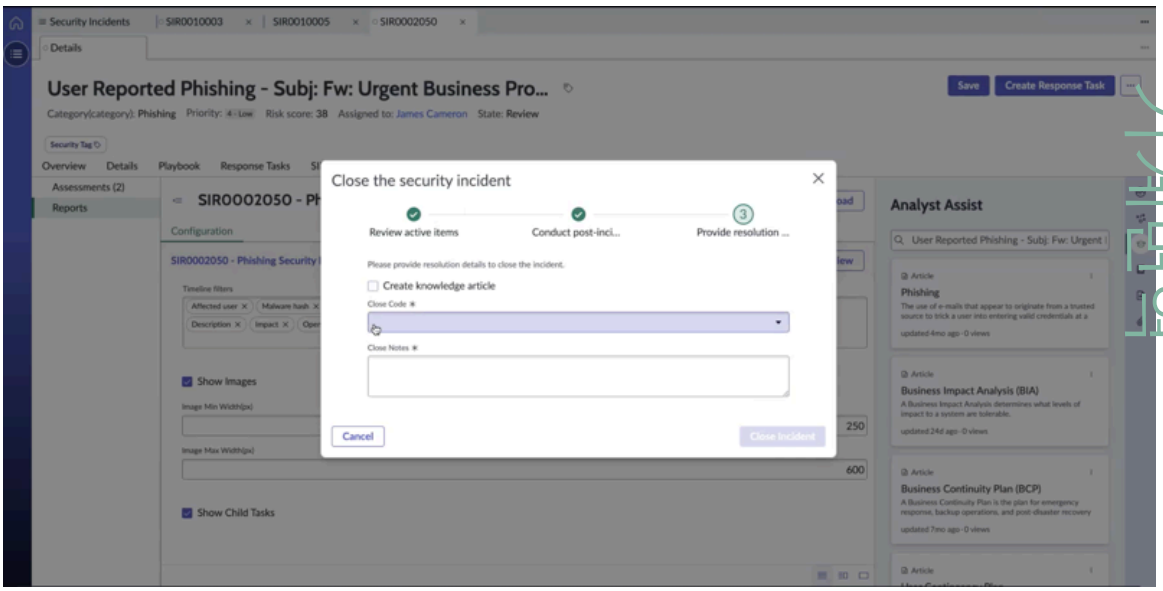


- 보고서 구성/미리 보기: 이 역시 선택적 단계이며, 링크를 클릭하여 보고서를 검토하고 다음 단계로 진행합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



- 해결 상세 정보 제공: 분석가는 확인란을 선택하여 지식 문서를 자동으로 생성할 수 있습니다.
- 종결 코드, 종결 메모를 입력하고 인시던트 종결을 클릭합니다.



주:
분석가가 보안 인시던트 닫기 대화 상자를 취소하면 분석가는 상세 정보 탭으로 이동하여 인시던트 상태를 종결 로 변경하여 종결을 계속할 수 있습니다.

SIR 작업 공간 대시보드 보기

이 섹션에는 새로운 보안 인시던트 또는 미해결 보안 인시던트의 평균 기간과 같은 프로세스를 분석하는 보안 인시던트 응답 중요한 메트릭이 나와 있습니다.

클래식 UI에는 플러그인 보안 인시던트 응답 이 설치될 때 퍼포먼스 분석 홈페이지 및 퍼포먼스 분석 대시보드에서 사용할 수 있는 표준 대시보드가 거의 없습니다. 이제 이러한 모든 기능을 **SIR** 대시보드 섹션의 새 작업 공간에서 사용할 수 있습니다.

홈페이지의 표준 대시보드:

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- Security Incident Response 개요
  - 분석가 개요
  - 관리자 개요(향후 릴리스에서 지원)
  - CISO 개요(향후 릴리스에서 지원)
- 용 플랫폼 분석## #### ##
  - 보안 인시던트 Explorer
  - CISO 대시보드(향후 릴리스)
  - 보안 인시던트 관리
  - 보안 인시던트 관리 프리미엄 KPI
  - 보안 운영 효율성
  - 상황별 분석 - SI 대시보드

주:
CISO 대시보드와 같은 보안 인시던트 응답 대시보드의 표준 및 플랫폼 분석에서 대시보드가 약간 반복될 수 있습니다. 플러그인이 설치되면 이러한 대시보드에 추가 컨텐츠가 있으며 중복으로 사용할 수 없습니다.

사용자는 작업 공간에 표시되도록 보안 인시던트 응답 대시보드용 플랫폼 분석 아래에 나열된 대시보드에 대한 플러그인을 설치해야 합니다. 그렇지 않으면 표준 대시보드만 사용할 수 있습니다.

현재 버전의 SIR Workspace경우 **SIR** 대시보드 섹션에서 다음 대시보드를 사용할 수 있습니다. 누락된 다른 대시보드는 이후 릴리스에서 사용할 수 있습니다.

Security Incident Response 대시보드

대시보드	설명
표준 대시보드	
보안 분석가 개요	이 대시보드를 사용하여 보안 분석가는 분석가의 중요 우선순위 작업, 높은 우선순위 작업, 분석가에게 할당된 보안 인시던트, 분석가에게 할당된 작업 및 인시던트 수를 기준으로 요약된 보안 인시던트를 볼 수 있습니다.
보안 인시던트 응답 대시보드용 Performance Analytics(PA)	
보안 인시던트 Explorer	이 대시보드를 사용하여 보안 관리자와 분석가는 범주, 하위 범주, 위치, 우선순위 및 비즈니스 영향별로 요약 및 그룹화된 보안 인시던트를 볼 수 있습니다. 이러한 보기를 통해 관리자와 분석가는 공격이 발생하는 빈도와 영향을 받는 비즈니스 서비스에 대한 인사이트를 빠르게 얻을 수 있습니다.
보안 인시던트 관리	이 대시보드를 사용하여 보안 관리자는 초기 분석/탐지에서 억제, 근절 및 복구에 이르기까지 보안 인시던트의 볼륨, 성능 및 진행 상황을 쉽게 추적할 수 있습니다.
CISO 대시보드	향후 릴리스에서 지원하도록 제안되었습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Security Incident Response 대시보드

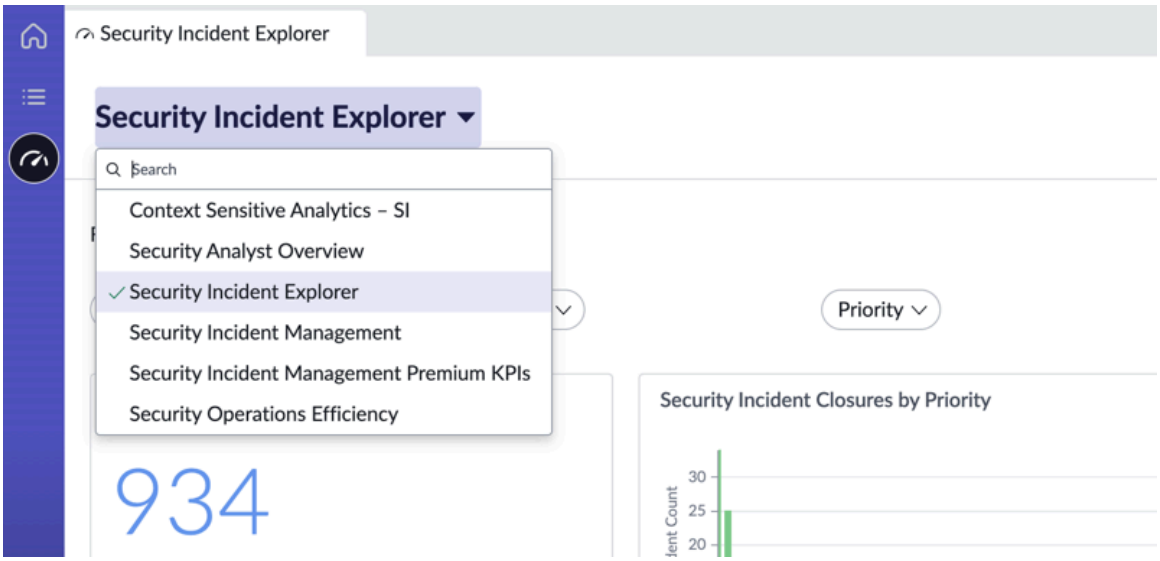
대시보드	설명
보안 운영 효율성	이 대시보드를 사용하여 관리자와 분석가는 전반적인 효율성 메트릭을 보고 SOC의 성과를 측정할 수 있습니다.
보안 인시던트 관리 프리미엄 KPI	이 대시보드를 사용하여 보안 관리자는 초기 분석/탐지부터 억제, 근절 및 복구에 이르기까지 보안 인시던트의 볼륨, 성능 및 진행 상황을 추적하고 볼 수 있습니다.
상황별 분석 - S	이 대시보드를 사용하여 관리자와 분석가는 미해결 보안 인시던트, 미해결 보안 인시던트의 평균 연령, 보안 인시던트의 평균 종결 시간, 당일 열리고 종결된 보안 인시던트의 백분율, 지난 5일 및 30일 동안 업데이트되지 않은 인시던트의 백분율을 볼 수 있습니다.

SIR 및 **PA** 대시보드 액세스

작업 공간 홈페이지 왼쪽에 표시되는 **SIR** 대시보드 아이콘입니다.

주:
sn_si.manager 또는 sn_si.admin 액세스 권한이 있는 사용자는 대시보드를 편집할 수 있습니다. 사용자는 사용자가 편집하려는 대시보드와 동일한 범위 내에 있어야 합니다. 예를 들어 SIR 작업 공간에서 보안 분석가 개요 대시보드를 사용할 수 있는 경우 대시보드를 편집하려면 사용자도 동일한 SIR 작업 공간 범위에 있어야 합니다.

1. 다음으로 이동 작업 공간 〉 보안 인시던트 관리 작업 공간.
2. **SIR** 대시보드 아이콘을 클릭합니다.
3. 드롭다운 목록에서 원하는 대시보드를 선택합니다.



대시보드를 편집하고, 대시보드에 새 요소를 추가하고, 대시보드를 직접 만들 수 있습니다. 대시보드 사용 방법에 대한 자세한 내용은 응답 대시보드 작업을 참조하세요.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 분석가 개요 대시보드 보기

이 대시보드를 사용하여 보안 분석가는 분석가의 중요 우선순위 작업, 높은 우선순위 작업, 분석가에게 할당된 보안 인시던트, 분석가에게 할당된 작업 및 인시던트 수를 기준으로 요약된 보안 인시던트를 볼 수 있습니다.

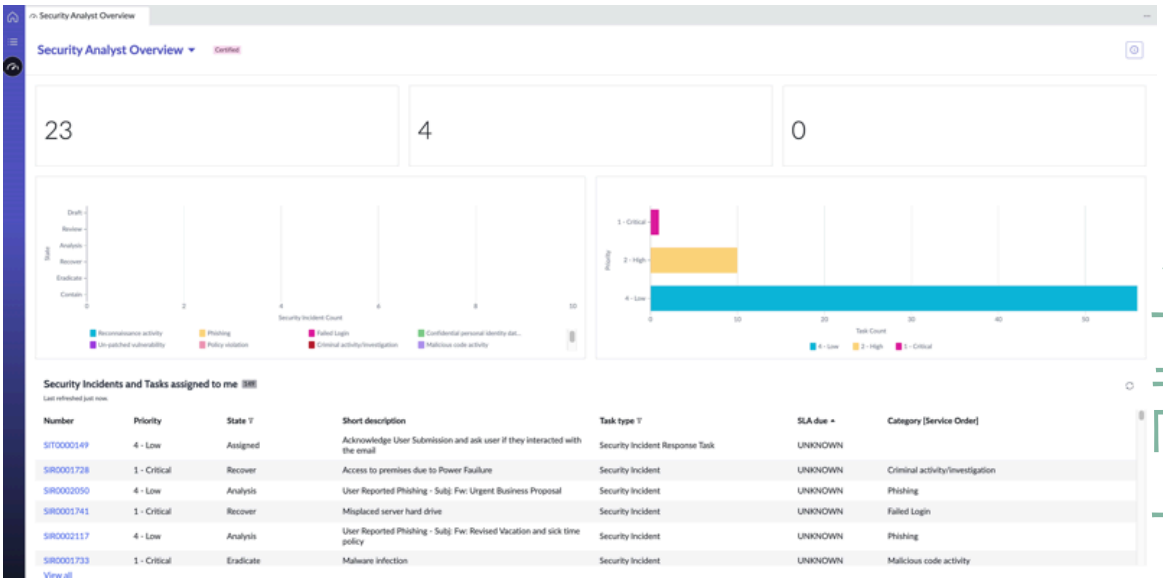
시작하기 전에

기본적으로 보안 분석가 개요 대시보드는 sn_si.analyst 액세스 권한이 있는 사용자에게 표시됩니다.

필요한 역할: sn_si.analyst(읽기), sn_si.manager 또는 sn_si.admin(쓰기)

프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답.
2. 작업 공간 홈페이지 왼쪽에 표시되는 **SIR** 대시보드 아이콘을 클릭합니다.
3. 드롭다운 목록에서 보안 분석가 개요를 선택합니다.



추가 작업은 보안 분석가 개요 대시보드를 참조하십시오. 보안 분석가 개요 대시보드에 대한 자세한 내용은 다음 문서를 참조하십시오 보안 인시던트 응답 플랫폼 분석 솔루션.

보안 인시던트 **Explorer** 대시보드 보기

이 대시보드를 사용하여 보안 관리자는 범주, 하위 범주, 위치, 우선순위 및 비즈니스 영향별로 요약되고 그룹화된 보안 인시던트를 볼 수 있습니다.

시작하기 전에

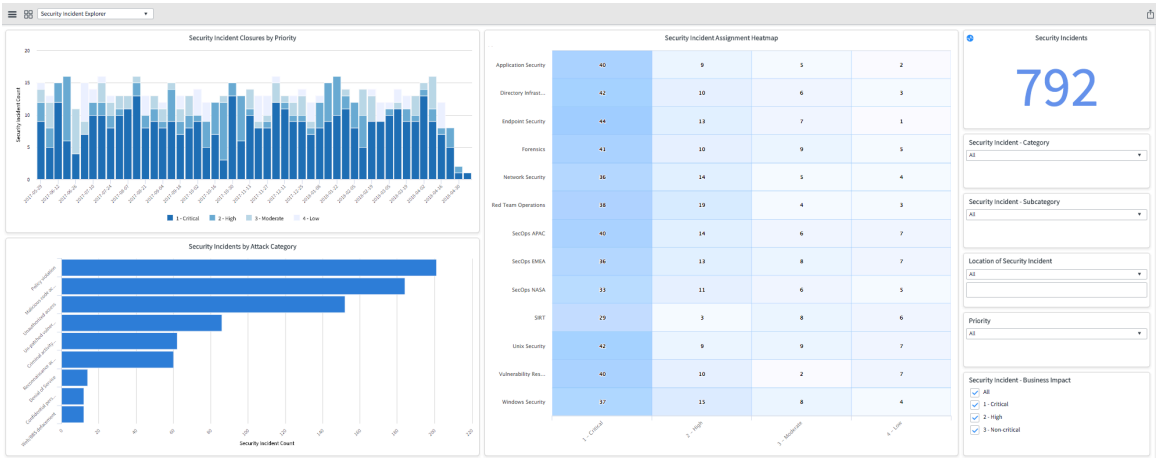
기본적으로 보안 인시던트 탐색기 대시보드는 sn_si.manager 액세스 권한이 있는 사용자에게 표시됩니다.

필요한 역할: sn_si.analyst(읽기), sn_si.manager 또는 sn_si.admin(쓰기)

프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답.
2. 작업 공간 홈페이지 왼쪽에 표시되는 **SIR** 대시보드 아이콘을 클릭합니다.
3. 드롭다운 목록에서 보안 인시던트 탐색기 를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



추가 작업은 보안 인시던트 Explorer 대시보드를 참조하십시오. 보안 인시던트 Explorer 대시보드에 대한 자세한 내용은 보안 인시던트 Explorer 대시보드를 참조하십시오.

현재 릴리스에서는 다음 보고서 목록이 보안 인시던트 탐색기 대시보드에서 지원되지 않습니다.

- 보안 인시던트 할당 히트맵 - 히트맵 시각화를 사용할 수 없습니다.
- 보안 인시던트 맵 - 맵 시각화를 사용할 수 없습니다.

Security Incident Management 대시보드 보기

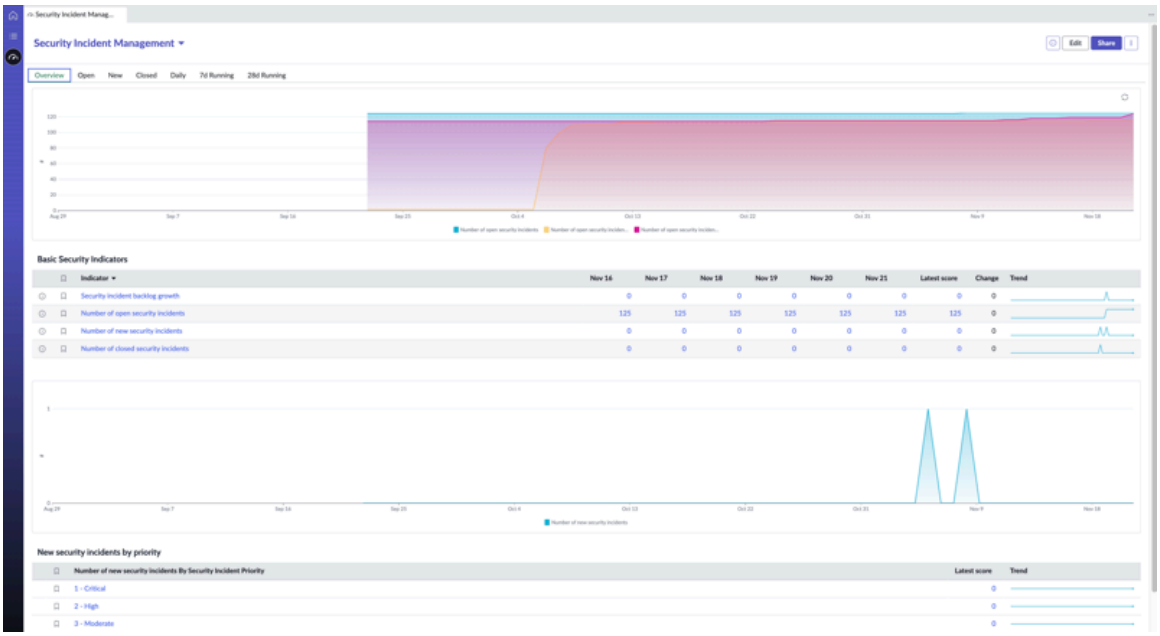
이 대시보드를 통해 보안 관리자는 초기 분석/탐지에서 억제, 근절 및 복구에 이르기까지 보안 인시던트의 볼륨, 성능 및 진행 상황을 쉽게 추적할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답.
2. 작업 공간 홈페이지 왼쪽에 표시되는 **SIR** 대시보드 아이콘을 클릭합니다.
3. 드롭다운 목록에서 **Security Incident Management** 를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



추가 작업은 보안 인시던트 관리 대시보드를 참조하십시오. 보안 인시던트 관리 대시보드에 대한 자세한 내용은 보안 인시던트 관리 대시보드를 참조하십시오.

보안 운영 효율성 대시보드 보기

SOC(보안 운영 센터) 관리자는 전체 효율성 메트릭을 보고 조직 내 SOC 팀 구성원의 개별 성과를 측정할 수 있습니다.

시작하기 전에

현재 릴리스에서는 보안 운영 효율성 대시보드에서 다음 보고서를 지원하지 않습니다.

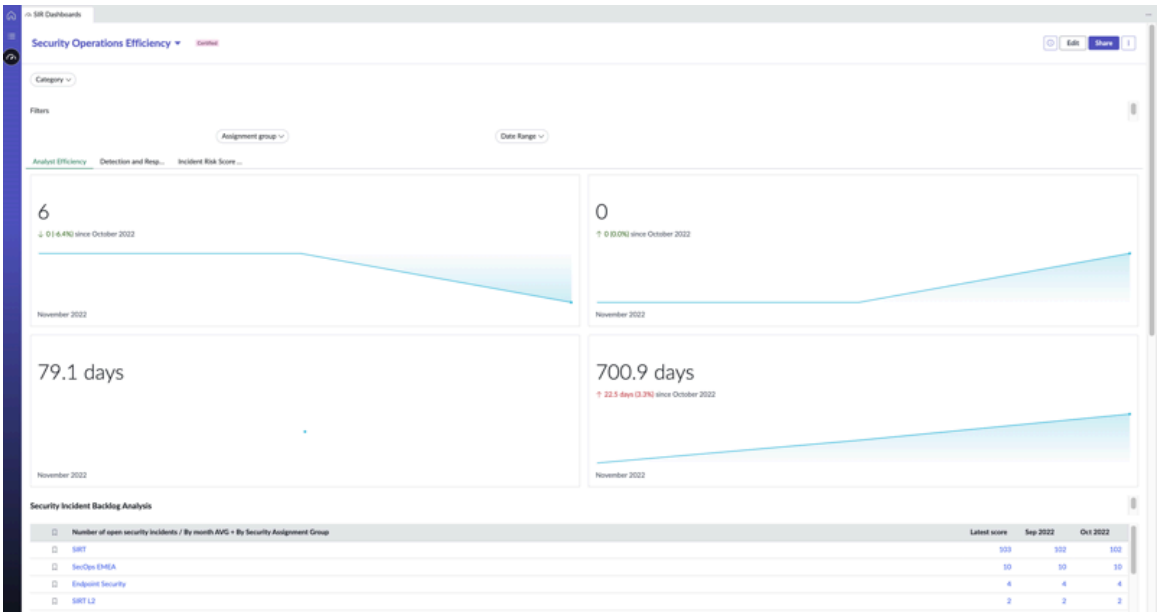
- 보안 인시던트 스테이지 분석 - 워크벤치를 사용할 수 없음

필요한 역할: sn_si.analyst(읽기), sn_si.manager 또는 sn_si.admin(쓰기)

프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답.
2. 작업 공간 홈페이지 왼쪽에 표시되는 **SIR** 대시보드 아이콘을 클릭합니다.
3. 드롭다운 목록에서 **Security Operations Efficiency** 를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



추가 작업은 보안 운영 효율성 대시보드를 참조하십시오. 보안 운영 효율성 대시보드에 대한 자세한 내용은 보안 운영 효율성 대시보드를 참조하십시오.

보안 인시던트 응답 프리미엄 **KPI** 대시보드 보기

이 대시보드를 사용하여 보안 관리자는 초기 분석/탐지부터 억제, 근절 및 복구에 이르기까지 보안 인시던트의 볼륨, 성능 및 진행 상황을 추적하고 볼 수 있습니다.

시작하기 전에

현재 릴리스에서는 다음 보고서 목록이 보안 인시던트 응답 프리미엄 KPI 대시보드에서 지원되지 않습니다.

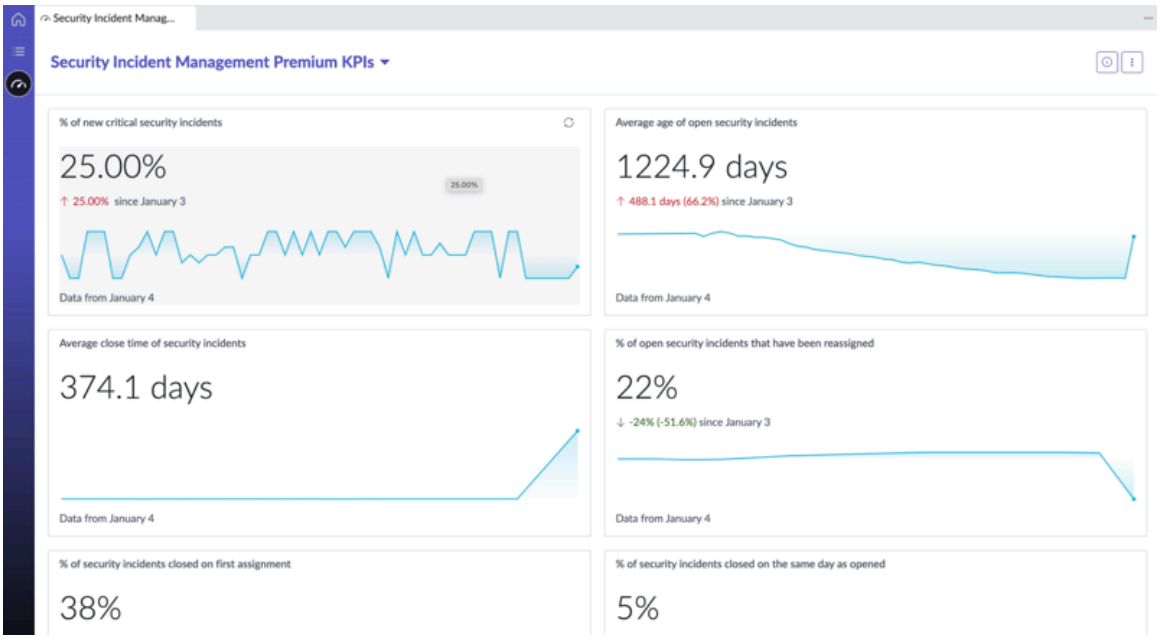
- 상태별 프로세스 - 워크벤치를 사용할 수 없음
- 연령별 프로세스 - 워크벤치를 사용할 수 없음
- 담당 그룹 및 상태별 30일 이상된 보안 인시던트 오픈 - 히트맵 시각화를 사용할 수 없습니다.
- 담당 그룹 및 상태별 30일 이상 업데이트되지 않은 보안 인시던트 - 히트맵 시각화를 사용할 수 없습니다.
- 활성 상태가 아닌 담당자가 있는 보안 인시던트 - 히트맵 시각화를 사용할 수 없습니다.

필요한 역할: sn_si.analyst(읽기), sn_si.manager 또는 sn_si.admin(쓰기)

프로시저

1. 다음으로 이동 모두 〉 작업 공간 〉 보안 인시던트 응답.
2. 작업 공간 홈페이지 왼쪽에 표시되는 **SIR** 대시보드 아이콘을 클릭합니다.
3. 드롭다운 목록에서 **Security Incident Response Premium KPI** 를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 추가 작업은 보안 인시던트 응답 프리미엄 KPI 대시보드를 참조하십시오.
   보안 인시던트 응답 프리미엄 KPI 대시보드에 대한 자세한 내용은 보안 인시던트 관리 프리미엄 대시보드를 참조하십시오.

상황별 분석 - SI 대시보드 보기

이 대시보드를 사용하여 관리자와 분석가는 미해결 보안 인시던트, 미해결 보안 인시던트의 평균 연령, 보안 인시던트의 평균 종결 시간, 당일 열리고 종결된 보안 인시던트의 백분율, 지난 5일 및 30일 동안 업데이트되지 않은 인시던트의 백분율을 볼 수 있습니다.

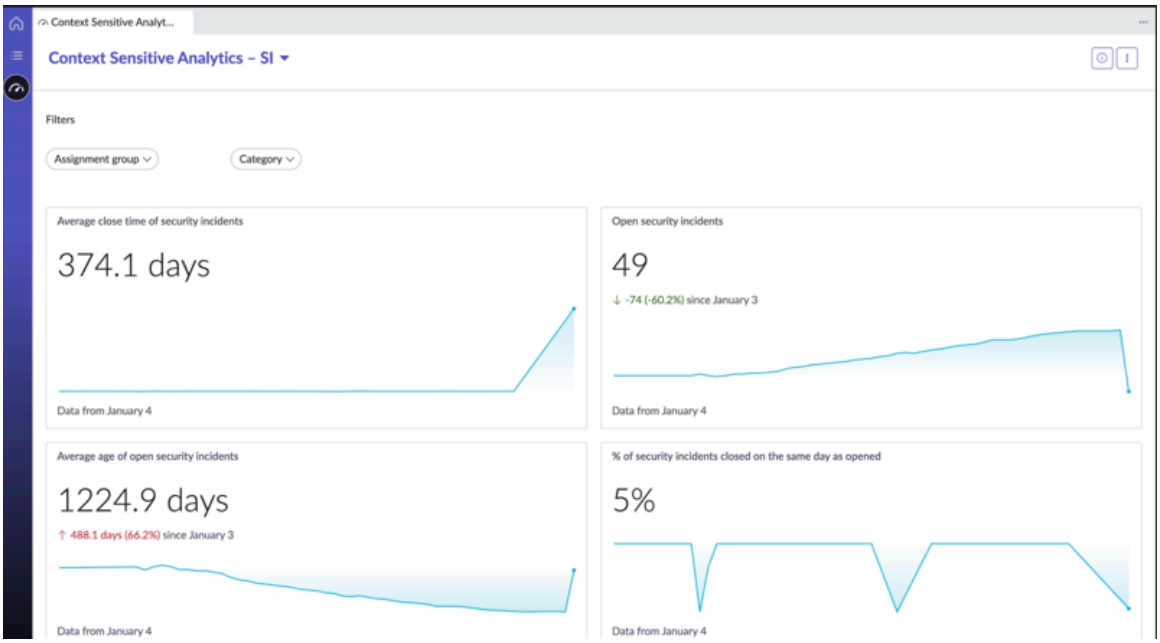
시작하기 전에

필요한 역할: sn_si.analyst(읽기), sn_si.manager 또는 sn_si.admin(쓰기)

프로시저

1. 다음으로 이동 모두 〉 작업 공간 〉 보안 인시던트 응답.
2. 작업 공간 홈페이지 왼쪽에 표시되는 **SIR** 대시보드 아이콘을 클릭합니다.
3. 드롭다운 목록에서 상황에 맞는 분석 - **SI** 를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 추가 작업은 상황별 분석 - SI 대시보드를 참조하십시오.

CISO 대시보드 보기

이 대시보드는 최고 정보 보안 책임자(CISO)에게 인스턴스의 보안 인시던트와 주간 인시던트 추세에 대한 개략적인 개요를 그래픽 차트 형식으로 제공합니다. 이러한 차트는 SOC(보안 운영 센터)의 수행 방식을 효과적으로 보고 분석하는 데 도움이 됩니다.

시작하기 전에

- 필요한 역할: sn_si.admin 및 sn_si.ciso - 인시던트를 편집하고 봅니다.
- 보안 인시던트 응답용 퍼포먼스 분석 앱이 설치되어 있는지 확인합니다.

이 태스크 정보

주:
CISO 대시보드와 CISO 개요 대시보드는 클래식 UI에서 서로 다른 두 가지였습니다. 그러나 이제 두 대시보드의 기능이 CISO 대시보드 아래에 병합되었습니다.

CISO 대시보드는 매주 보안 인시던트에 대한 주요 인사이트를 제공합니다. 표시기를 설정하고 표시기 속성의 조건과 일치하는 인시던트의 데이터 스냅샷을 수집할 수 있습니다. 수집된 데이터는 대시보드의 위젯을 사용하여 시각화됩니다.

CISO 대시보드의 위젯을 사용하여 주간 추세를 시각화할 수 있습니다. 보안 인시던트 추세에 대한 데이터 또는 통계는 조직에서 정의한 주간 인시던트 표시기 속성에서 수집됩니다. 다음 차트를 사용하여 주요 통찰력을 얻을 수 있습니다.

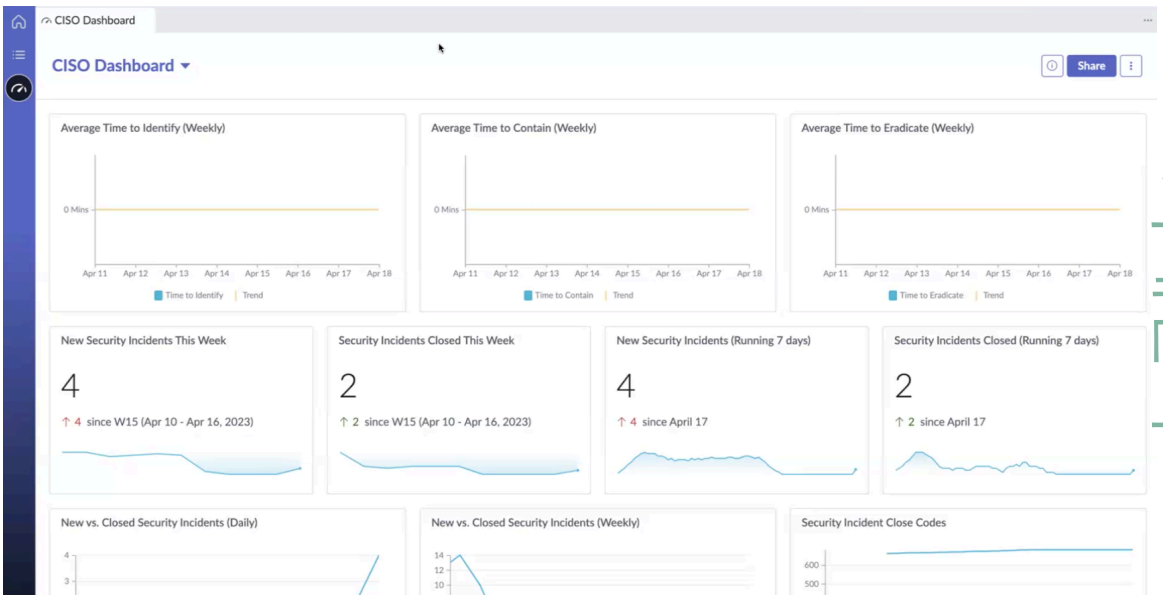
- 평균 식별 시간(주별): 이 차트는 보안 인시던트를 식별하는 데 걸리는 평균 주간 시간을 보여줍니다.
- 평균 포함 시간(주별): 이 차트는 보안 인시던트를 억제하는 데 걸린 평균 주간 시간을 보여줍니다.
- 평균 근절 시간(주별): 이 차트는 보안 인시던트를 근절하는 데 걸리는 평균 주간 시간을 보여줍니다.
- 이번 주 새로운 보안 인시던트: 이 차트는 이번 주에 발생한 새로운 보안 인시던트 수를 보여줍니다.
- 금주 종결된 보안 인시던트: 이 차트는 이번 주에 종결된 보안 인시던트 수를 보여줍니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 새 보안 인시던트(7일 이하): 이 차트는 일주일 동안 실행되는 새 보안 인시던트의 수를 보여줍니다.
- 종결된 보안 인시던트(7일 이하): 이 차트는 종결되었지만 일주일 동안 진행 중인 새 보안 인시던트의 수를 보여줍니다.
- 새로운 인시던트 대 종결된 인시던트(일간): 이 차트는 일일 새로운 보안 인시던트와 종결된 일일 보안 인시던트를 비교한 것입니다.
- 신규 인시던트 대 종결된 인시던트(주간): 이 차트에서는 주간 신규 보안 인시던트와 종결된 주간 보안 인시던트 간의 비교를 보여줍니다.
- 보안 인시던트 종결 코드: 이 차트는 보안 인시던트의 종결 코드를 보여줍니다.

프로시저

1. 다음으로 이동 모두 〉 작업 공간 〉 보안 인시던트 응답.
2. 작업 공간 홈페이지 왼쪽에 있는 **SIR** 대시보드 아이콘을 클릭합니다.
3. 드롭다운 목록에서 **CISO** 대시보드를 선택합니다.



4. 추가 작업을 위해 CISO 대시보드를 참조하십시오.

CISO 보고 개요 대시보드 보기

이 대시보드는 최고 정보 보안 책임자(CISO)에게 인스턴스의 보안 인시던트와 주간 인시던트 추세에 대한 개략적인 보고 개요를 그래픽 차트 형식으로 제공합니다. 이러한 차트는 SOC(보안 운영 센터)의 수행 방식을 효과적으로 보고 분석하는 데 도움이 됩니다.

시작하기 전에

필요한 역할: sn_si.admin 및 sn_si.ciso - 인시던트를 편집하고 봅니다.

이 태스크 정보

CISO 보고 개요 대시보드는 매주 보안 인시던트에 대한 주요 인사이트를 제공하며, 위젯을 사용하여 주간 추세를 시각화할 수 있습니다. 다음 차트를 사용하여 CISO 보고에 대한 주요 인사이트를 얻을 수 있습니다.

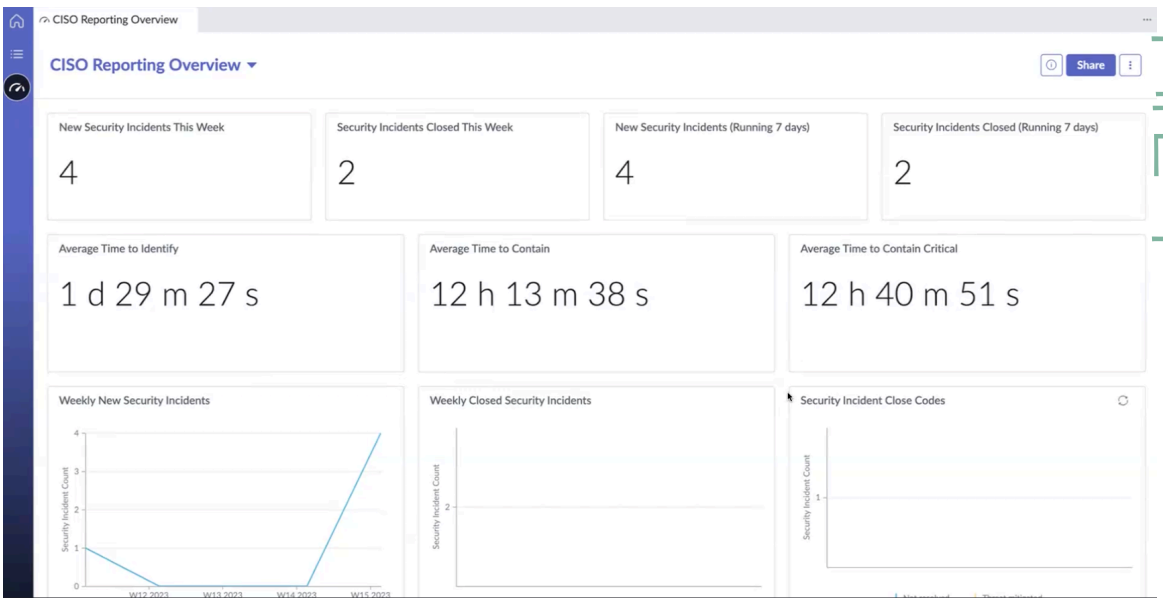
- 이번 주 새 보안 인시던트: 이 타일에는 이번 주 새 보안 인시던트 수에 대한 보고서가 표시됩니다.
- 이번 주 종결된 보안 인시던트: 이 타일에는 이번 주에 종결된 보안 인시던트 수에 대한 보고서가 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 새 보안 인시던트(7일 이하): 이 타일에는 일주일 동안 실행된 새 보안 인시던트 수에 대한 보고서가 표시됩니다.
- 종결된 보안 인시던트(7일 이하): 이 타일에는 종결되었지만 일주일 동안 실행 중인 새 보안 인시던트 수에 대한 보고서가 표시됩니다.
- 평균 식별 시간: 이 타일에는 보안 인시던트를 식별하는 데 걸린 평균 주간 시간 보고서가 표시됩니다.
- 평균 포함 시간: 이 타일에는 보안 인시던트를 억제하는 데 걸린 평균 주간 시간 보고서가 표시됩니다.
- 평균 중요 포함 시간: 이 타일에는 중요한 보안 인시던트를 포함하는 데 걸린 평균 주간 시간 보고서가 표시됩니다.
- 새로운 주간 보안 인시던트: 이 차트는 새로운 주간 보안 인시던트 보고서를 보여줍니다.
- 종결된 주간 보안 인시던트: 이 차트는 종결된 주간 보안 인시던트 보고서를 보여줍니다.
- 보안 인시던트 종결 코드: 이 차트는 보안 인시던트의 종결 코드 보고서를 보여줍니다.

프로시저

1. 다음으로 이동 모두 〉 작업 공간 〉 보안 인시던트 응답.
2. 작업 공간 홈페이지 왼쪽에 있는 **SIR** 대시보드 아이콘을 클릭합니다.
3. 드롭다운 목록에서 **CISO** 보고 개요를 선택합니다.



4. 추가 작업은 CISO 보고 대시보드를 참조하십시오.

보안 인시던트 관리자 개요 대시보드 보기

이 대시보드는 관리자에게 팀 수준에서 중요하거나 우선순위가 높은 보안 인시던트, 24시간 후에 만료되는 SLA, 인스턴스의 주간 인시던트 추세에 대한 개략적인 개요를 보고서 및 그래픽 차트 형식으로 제공합니다.

시작하기 전에
필요한 역할:

- sn_si.admin - 대시보드를 편집하고 봅니다.
- sn_si.manager - 대시보드를 봅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

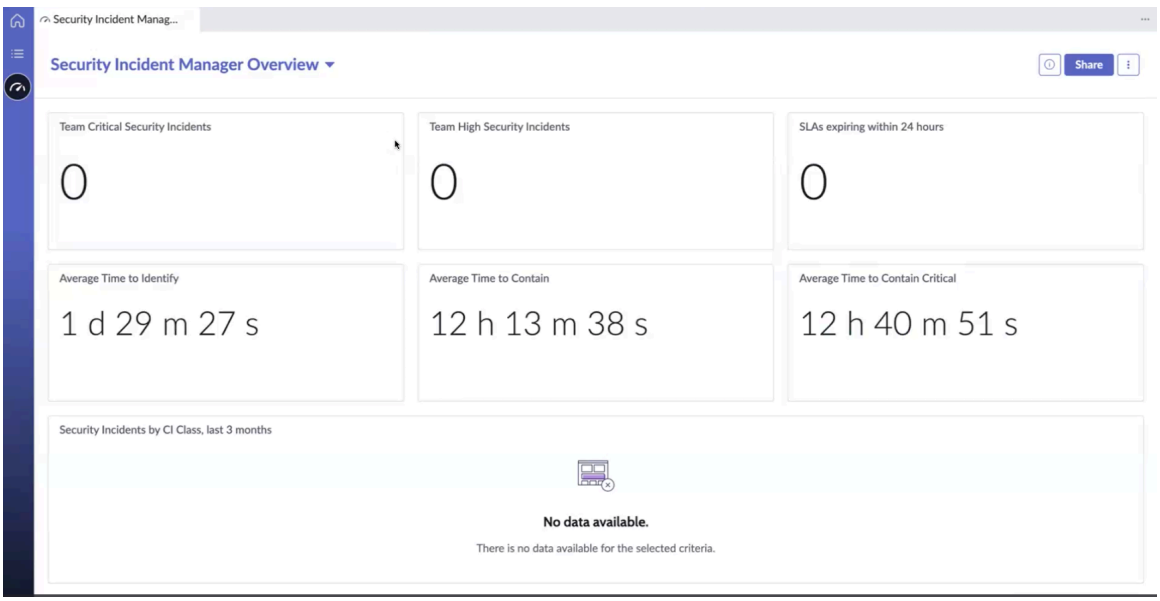
이 태스크 정보

즉각적인 주의가 필요한 중요하거나 우선순위가 높은 보안 인시던트 또는 SLA를 분석할 수 있습니다. 보안 인시던트 관리자 개요 대시보드의 위젯을 사용하여 주간 추세를 시각화할 수도 있습니다. 조직에서 정의한 인시던트 테이블에서 보안 인시던트의 주간 또는 월간 추세에 대한 데이터 또는 통계가 수집됩니다. 다음 차트를 사용하여 주요 통찰력을 얻을 수 있습니다.

- 팀 내 우선순위가 가장 높은 보안 인시던트: 이 타일에는 이번 주 팀의 중요 보안 인시던트 수가 표시됩니다.
- 팀 내 우선순위가 높은 보안 인시던트: 이 타일에는 이번 주 팀의 높은 보안 인시던트 수가 표시됩니다.
- 24시간 이내에 만료되는 **SLA**: 이 타일은 24시간 이내에 만료되는 SLA 수를 표시합니다.
- 평균 식별 시간: 이 타일에는 보안 인시던트를 식별하는 데 걸린 평균 주간 시간이 표시됩니다.
- 평균 포함 시간: 이 타일에는 보안 인시던트를 억제하는 데 걸린 평균 주간 시간이 표시됩니다.
- 평균 중요 포함 시간: 이 타일에는 중요한 보안 인시던트를 포함하는 데 걸린 평균 주간 시간이 표시됩니다.
- 지난 3개월 간의 **CI** 클래스별 보안 인시던트: 이 차트는 지난 3개월 동안의 CI 클래스를 기반으로 한 모든 보안 인시던트의 추세를 보여줍니다.
- 범주별 모든 보안 인시던트 추세: 이 차트는 범주를 기준으로 모든 보안 인시던트의 추세를 보여줍니다.
- 우선순위별 모든 보안 인시던트 추세: 이 차트는 우선순위에 따른 모든 보안 인시던트의 추세를 보여줍니다.

프로시저

1. 다음으로 이동 모두 〉 작업 공간 〉 보안 인시던트 응답.
2. 작업 공간 홈페이지 왼쪽에 있는 **SIR** 대시보드 아이콘을 클릭합니다.
3. 드롭다운 목록에서 보안 인시던트 관리자 개요를 선택합니다.



4. 추가 작업은 보안 인시던트 관리자 개요를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 인시던트 응답 상태 대시보드 보기

보안 인시던트 응답 상태 대시보드 기능은 인시던트 응답 프로세스 구현, 발생한 문제/오류 및 성과 메트릭과 관련된 중요한 측면에 대한 중앙 집중식 뷰를 제공합니다. 조직의 보안 인시던트 대응 역량의 효과를 모니터링하고 최적화하기 위한 중요한 도구 역할을 합니다.

시작하기 전에

필요한 역할: sn_si.admin, sn_si.analyst 또는 sn_si.analytics_read - 대시보드 보기.

이 태스크 정보

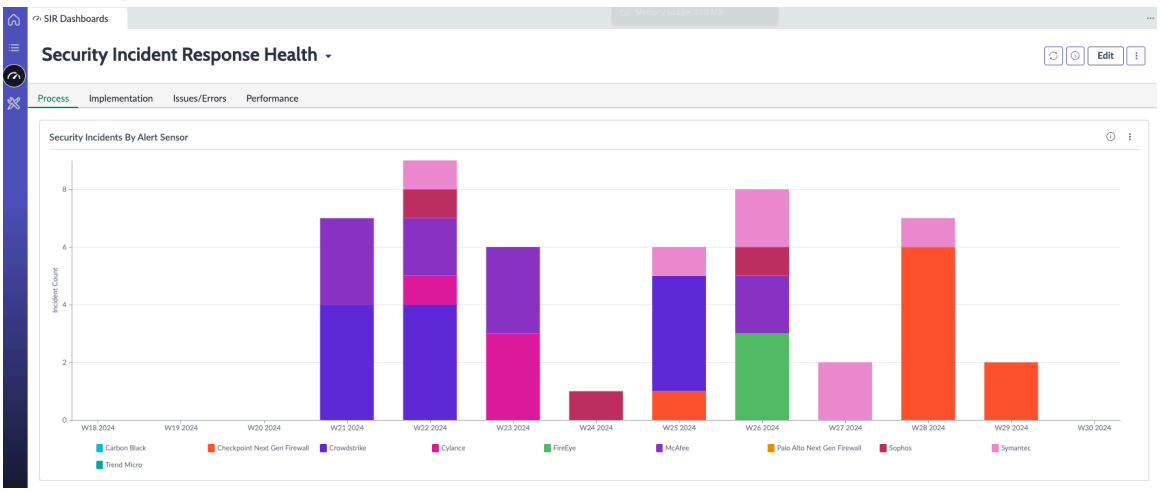
애플리케이션별로 위젯 및 추세 차트를 사용하여 보안 인시던트의 상태를 모니터링할 수 있습니다. 이러한 통계는 SIR 애플리케이션 내의 구성 상태와 정정 효과를 자세히 설명하는 포괄적인 상태 점수를 제공합니다. 보안 인시던트 응답 상태 대시보드는 다음 네 개의 탭을 지원합니다.

- 프로세스: 이 탭에는 매주 그룹화된 다양한 경보 센서의 모든 인시던트 요약이 표시됩니다.
- 구현: 이 탭에는 스크립트 포함, 비즈니스 규칙, 플로우 및 업그레이드를 포함하여 고객이 인스턴스에서 수행하는 사용자 지정이 표시됩니다.
- 문제/오류: 이 탭에는 통합 프로세스의 오류, 원시 인시던트 데이터 수집 중 불일치, SIR 애플리케이션의 아웃바운드 HTTP 오류 및 Playbook 실행 중에 발생하는 문제를 강조 표시하는 위젯이 표시됩니다.
- 성능: 이 탭에는 성능 쿼리, 비즈니스 규칙 및 스크립트의 속도 저하를 포함하여 SIR 애플리케이션의 성능 문제가 표시됩니다.

프로시저

1. 다음으로 이동 모두 〉 작업 공간 〉 보안 인시던트 응답 작업 공간.
2. SIR 작업 공간 홈페이지에서 **SIR** 대시보드 아이콘을 선택합니다.
3. 드롭다운 목록에서 보안 인시던트 응답 상태 대시보드를 선택합니다.
4. 프로세스 탭을 선택하여 차트의 각 경보 센서에 대해 매주 트리거된 보안 인시던트 수를 봅니다.

프로세스 탭



다음 작업을 수행할 수 있습니다.

a. 차트에서 경보 센서를 선택하여 일주일 동안 경보 센서에 의해 트리거된 보안 인시던트 수에 대한 KPI 세부 정보를 봅니다.

b. 특정 주의 KPI 세부 정보를 가져오려면 달력 옵션을 사용합니다.

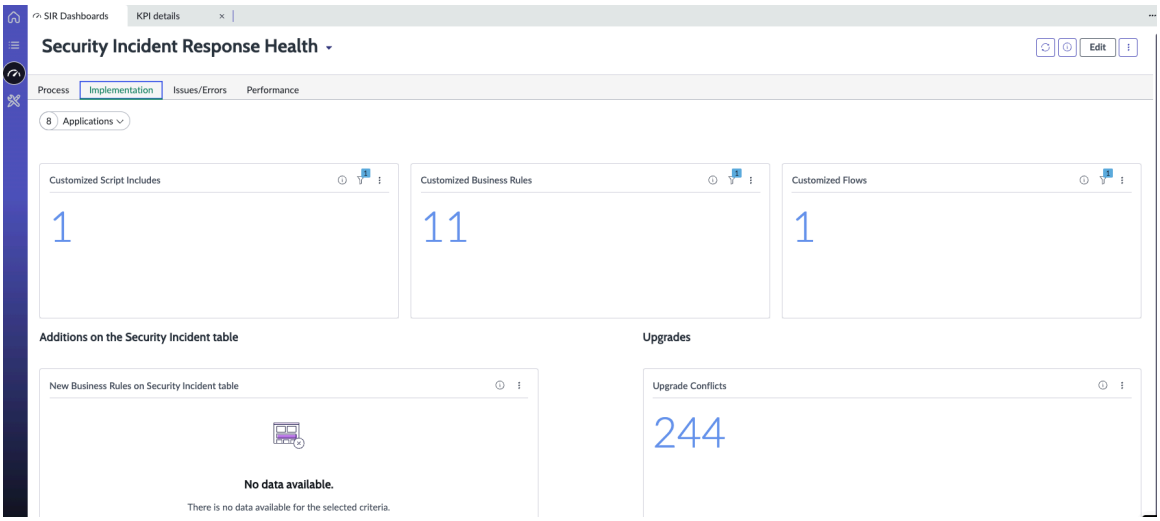
c. 경보 센서에서 트리거된 보안 인시던트를 비교하려면 기록 비교 옵션을 선택합니다.

d. 차트 유형, 시계열 또는 분석을 사용하려면 차트 옵션을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. 구현 탭을 선택하여 보안 인시던트 응답 애플리케이션에서 보안 인시던트에 대해 생성된 사용자 지정 수를 확인합니다.

구현 탭



구현 탭:

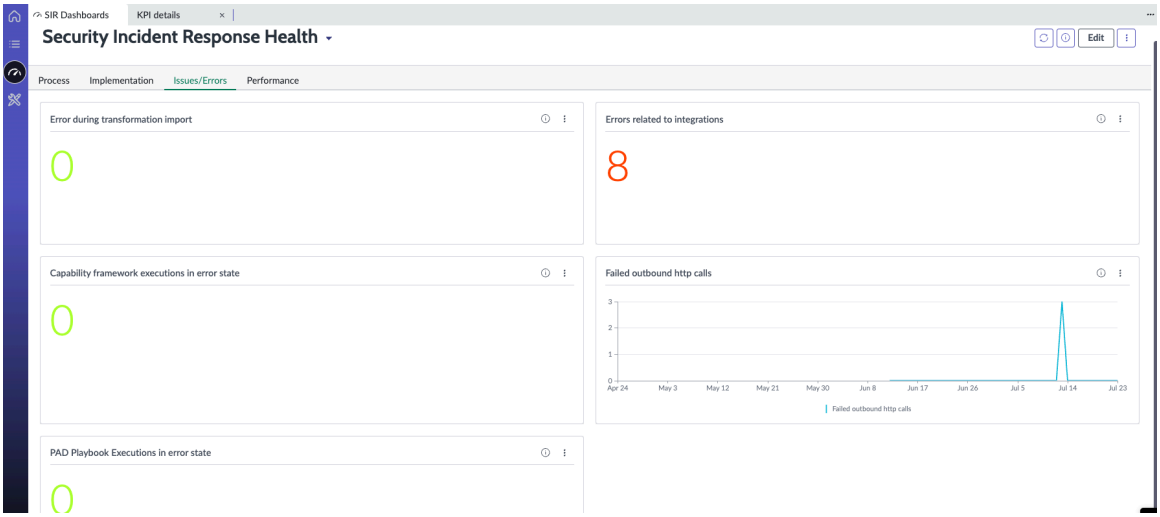
각 인시던트 응답 애플리케이션에 대해 만들어진 사용자 지정 수에 대해 집계된 대시보드를 볼 수 있습니다.

- 사용자 지정 스크립트 포함: 이 위젯은 SIR 애플리케이션의 요구 사항에 따라 추가된 사용자 지정 스크립트의 수를 표시합니다.
- 사용자 지정 비즈니스 규칙: 이 위젯에는 SIR 애플리케이션의 요구 사항에 따라 추가된 사용자 지정 비즈니스 규칙의 수가 표시됩니다.
- 사용자 지정 플로우: 이 위젯은 SIR 애플리케이션의 요구 사항에 따라 추가된 사용자 지정 플로우 수를 표시합니다.
- 보안 인시던트 테이블의 새 비즈니스 규칙: 이 위젯은 보안 인시던트 테이블에서 생성된 비즈니스 규칙의 수를 표시합니다.
- 업그레이드 상충: 이 위젯은 SIR 애플리케이션에서 업그레이드하는 동안 트리거된 상충 수를 표시합니다.

6. 문제/오류 탭을 선택하여 보안 인시던트 응답 애플리케이션에서 트리거된 문제 또는 오류의 수를 봅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

문제/오류 탭



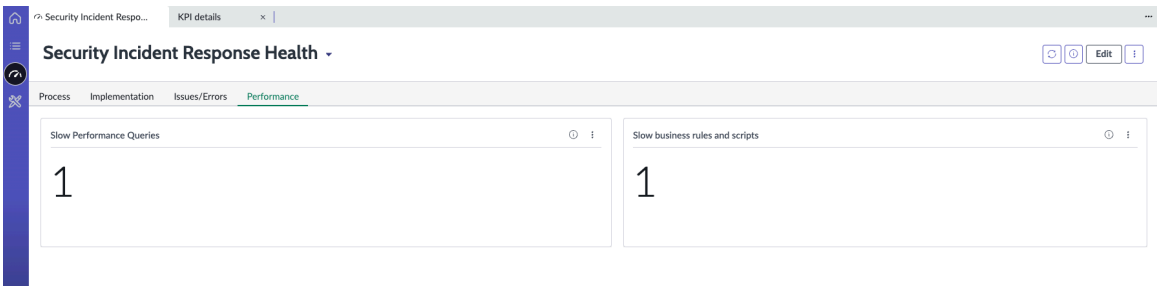
문제/오류 탭:

보안 인시던트 응답 애플리케이션에서 문제 또는 오류에 대한 집계된 대시보드를 볼 수 있습니다.

- 변환 임포트 중 오류: 이 위젯에는 SIR 애플리케이션에서 변환 임포트 중에 트리거된 오류 수가 표시됩니다.
- 통합과 관련된 오류: 이 위젯에는 SIR 통합 중에 트리거된 오류 수가 표시됩니다.
- 오류 상태의 역량 프레임워크 실행: 이 위젯은 SIR 애플리케이션에서 역량 프레임워크 실행 중에 트리거된 오류 수를 표시합니다.
- 실패한 아웃바운드 **HTTP** 호출: 이 위젯은 SIR 애플리케이션에서 트리거된 실패한 아웃바운드 HTTP 호출 수를 표시합니다.
- 오류 상태의 **PAD** 플레이북 실행: 이 위젯은 SIR 애플리케이션에서 트리거된 PAD 플레이북 실행 오류 수를 표시합니다.

7. 성과 탭을 선택하여 보안 인시던트 응답 애플리케이션에서 트리거된 성능 문제 수를 확인합니다.

성과 탭



성과 탭:

보안 인시던트 응답 애플리케이션에서 성과 문제에 대해 집계된 대시보드를 볼 수 있습니다.

- 느린 성능 쿼리: 이 위젯은 평균 실행 시간이 10ms보다 크고 1,000회 이상의 실행에서 평균인 SIR 애플리케이션의 성능 쿼리 수를 표시합니다.
- 느린 비즈니스 규칙 및 스크립트: 이 위젯은 평균 실행 시간이 10ms보다 크고 1,000회 이상의 실행 시 평균인 SIR 애플리케이션의 비즈니스 규칙 및 스크립트 수를 표시합니다.

8. 새로 고침 아이콘을 사용하여 보안 인시던트 응답 상태 대시보드의 데이터를 새로 고칠 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

9. 대시보드 세부 정보 보기 아이콘을 사용하여 보안 인시던트 응답 상태 대시보드의 세부 정보를 볼 수 있습니다.
10. 편집 옵션을 사용하여 보안 인시던트 응답 상태 대시보드의 상세 정보를 수정할 수 있습니다.
11. 더 보기 옵션을 사용하여 보안 인시던트 응답 상태 대시보드에서 추가 작업을 수행할 수 있습니다.

보안 인시던트 생성

보안 인시던트는 양식에서 수동으로 생성하거나 Splunk와 같은 통합된 외부 공급업체 경보 모니터링 도구에서 수신한 보안 이벤트를 통해 자동으로 생성할 수 있습니다.

중요사항:
의 보안 인시던트 응답 최신 기능은 에서만 사용할 수 있습니다 보안 인시던트 응답 작업 공간. 교대조 핸드오버, 위험 점수 계산기 등과 같은 기능에 액세스하고 활용하려면 최신 보안 인시던트 응답 버전을 보안 인시던트 응답 작업 공간 설치하거나 업그레이드하십시오.

보안 역할이 있는 경우 다음 방법 중 하나를 사용하여 보안 인시던트를 수동으로 만들 수 있습니다.

보안 인시던트를 수동으로 생성하는 방법

방법	설명
보안 인시던트 목록에서 수동으로 생성됨	보안 인시던트 목록에서 새로 만들기를 클릭하여 새 보안 인시던트를 만듭니다.
보안 인시던트 카탈로그에서 수동으로 생성	보안 인시던트 카탈로그에 정의된 보안 위협 범주에서 선택하여 보안 인시던트를 만들 수 있습니다.
인시던트 관리	인시던트 관리의 인시던트 양식에서 보안 인시던트 생성을 클릭하여 새 보안 인시던트를 만듭니다.
보안 요청에서 수동으로 변환됨	보안 요청 양식에서 보안 인시던트로 변환을 클릭하여 새 보안 인시던트를 만듭니다.
Event Management 경보에서 수동으로 작성됨	이벤트 관리 경보 양식에서 보안 인시던트 생성을 클릭하여 경보에서 새 보안 인시던트를 만듭니다.
경보에서 수동으로 생성됨	이벤트 관리 경보 양식에서 보안 인시던트 생성을 클릭하여 새 보안 인시던트를 만듭니다.
취약성 기록에서 수동으로 변환됨 (Vulnerability Response 플러그인이 활성화된 경우)	취약성 항목 양식에서 보안 인시던트 생성을 클릭하여 새 보안 인시던트를 만듭니다.

보안 인시던트 자동 생성

일반적으로 보안 관리자는 보안 인시던트를 자동으로 생성하는 데 사용되는 경보 규칙을 설정해야 합니다.

보안 인시던트를 생성하는 보안 관리자 방법

방법	설명
경보 규칙을 사용하여 자동으로 생성됨	보안 인시던트는 데이터 센터 애플리케이션의 이벤트 관리에 정의된 경보 규칙을 기반으로 생성할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 인시던트 수동 생성

보안 인시던트 양식이나 기타 여러 양식에서 보안 인시던트를 생성할 수 있습니다.

다음 양식의 기존 기록을 기반으로 보안 인시던트를 생성할 수 있습니다.

- 모든 보안 인시던트 목록에서
- 인시던트 양식
- 이벤트 관리 경보 양식
- 취약한 항목 양식
- 보안 요청 양식

보안 인시던트 목록에서 보안 인시던트 생성

보안 인시던트를 자동으로 생성하는 방법 외에도 필요에 따라 수동으로 보안 인시던트를 생성할 수 있습니다.

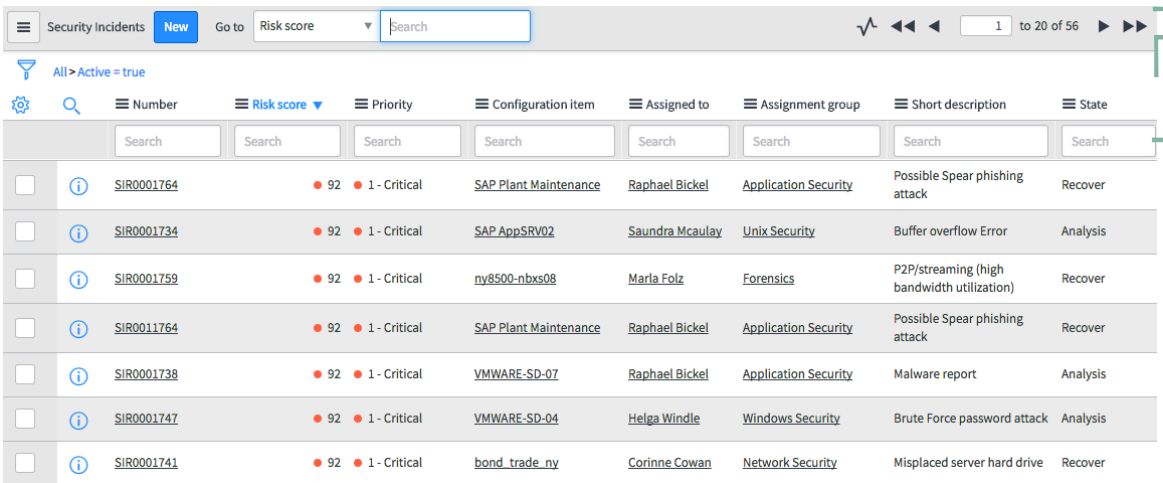
이 비디오에서는 보안 인시던트 목록에서 보안 인시던트를 생성하는 방법에 대한 시각적 개요를 보여줍니다.

보안 인시던트 목록에서 보안 인시던트 생성

시작하기 전에
필요한 역할: sn_si.basic

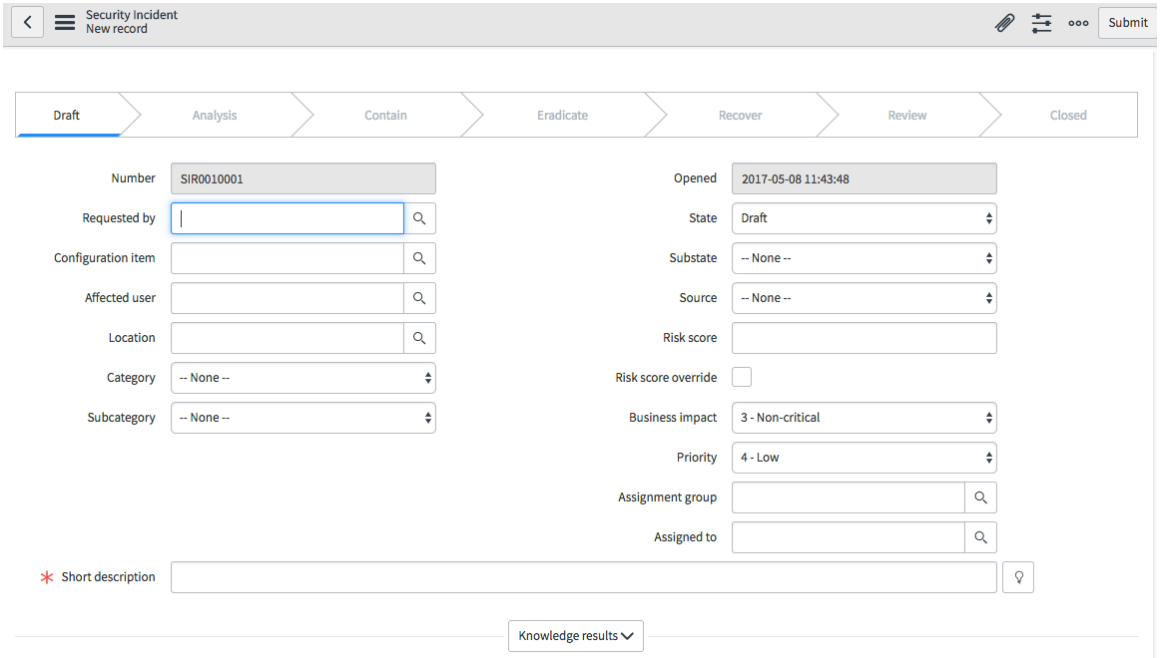
프로시저

1. 보안 인시던트 목록(예: 모두 〉 보안 인시던트 〉 인시던트 〉 모든 인시던트 표시).



2. 새로 만들기를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



3. 양식에서 필드를 채웁니다.

필드	설명
보안 태그 선택	필요한 경우 보안 태그를 선택하여 기록에 메타데이터를 추가하거나 이 보안 인시던트 기록에 접근할 수 있는 사용자를 식별합니다. 이 필드는 보안 인시던트가 저장된 후에만 나타납니다.
번호	〔읽기 전용〕 보안 인시던트 번호입니다.
요청한 사람	작업을 수행하도록 요청하는 사람입니다.
구성 항목	보안 문제의 영향을 받는 서버, 컴퓨터, 라우터 또는 기타 구성 항목입니다.
영향을 받는 사용자	보안 문제의 영향을 받는 사람입니다.
위치	요청자 또는 자원의 위치입니다. 구성 항목을 선택하지 않으면 이 필드는 요청자의 위치로 미리 채워집니다.
범주	보안 문제의 유형을 식별하는 범주입니다. 범주를 선택하면 기록이 저장될 때 이 문제를 분석하기 위한 워크플로우가 실행됩니다. 예를 들어 DoS(서비스 거부)를 선택하면 보안 인시던트 - DoS(서비스 거부) - 템플릿 워크플로우가 실행됩니다. 자세한 내용은 보안 인시던트 응답 워크플로우 템플릿 문서를 참조하십시오.
하위 범주	문제를 추가로 정의하는 하위 범주입니다.
개설 일시	〔읽기 전용〕 인시던트가 열린 날짜 및 시간을 표시합니다.

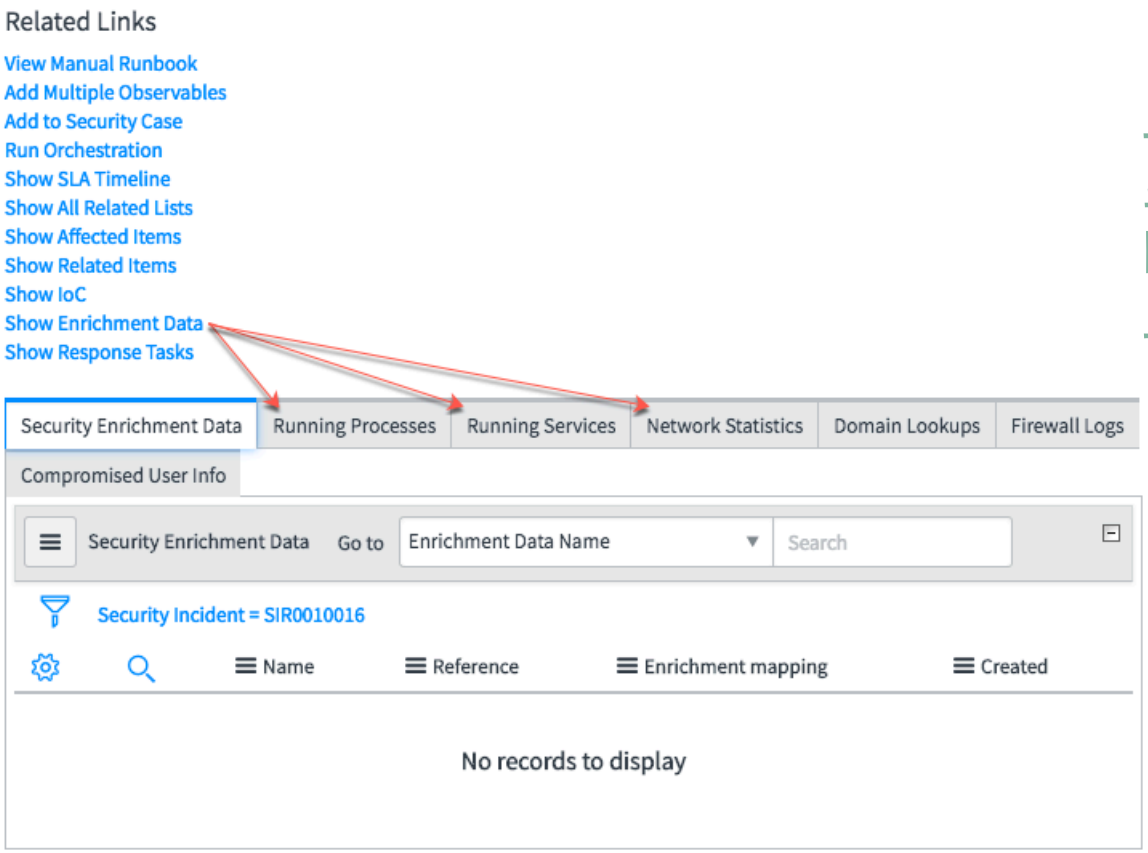
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
상태	보안 인시던트의 현재 상태입니다. 보안 인시던트 생성 시 이 필드는 기본적으로 초안으로 설정됩니다.
하위 상태	보안 인시던트에 보류 중인 문제 또는 변경 사항이 포함되어 있는지 여부를 식별합니다.
소스	이메일, 전화 통화 또는 네트워크 모니터링과 같은 보안 인시던트의 소스를 식별합니다.
경보 센서	경보 또는 이벤트 데이터(예: CarbonBlack, CrowdStrike, McAfee)를 수집하는 보안 통합입니다.
경보 규칙	이 보안 인시던트 생성을 트리거한 보안 제품의 규칙입니다.
위험 점수	이 보안 인시던트에 대해 계산된 위험 점수를 표시합니다. 이 값은 보안 인시던트의 우선순위, 보안 인시던트 유형(서비스 거부, 스피어 피싱 또는 악성 코드 활동) 및 표시기에서 실패한 평판 점수를 트리거한 소스 수를 기반으로 합니다. 위험 점수는 분석가의 보안 인시던트 작업 우선순위를 정하는 데 도움이 됩니다. 세 가지 보안 인시던트 속성을 사용하면 목록 뷰에서 위험 점수 옆에 색상으로 구분된 점을 표시하여 쉽게 식별할 수 있습니다. 보안 인시던트의 특정 필드(예: 비즈니스 영향 또는 우선순위)를 변경하고 기록을 저장하면 위험 점수 가 자동으로 다시 계산되어 표시됩니다. 변경 사항은 작업 메모와 위험 점수 감사 관련 목록에도 반영됩니다. **주:** 영향을 받는 사용자가 보안 인시던트, 영향을 받는 서비스 또는 취약한 항목과 연결되면 위험 점수도 다시 계산됩니다. 새 위험 점수를 수동으로 입력할 수도 있습니다. 이 기능은 분석 중인 보안 인시던트 목록의 맨 위에 특정 보안 인시던트를 유지하려는 경우에 유용할 수 있습니다. 새 위험 점수를 입력하면 위험 점수 무효화 확인란이 자동으로 선택됩니다. 보안 인시던트의 변경 사항에 관계없이 수동으로 입력한 위험 점수는 자동으로 다시 계산되지 않습니다. **주:** 이전 릴리스에서 인스턴스를 업그레이드한 경우 모든 미해결 보안 인시던트에 대한 위험 점수가 계산됩니다. 자세한 내용은 보안 인시던트 계산기 이해 문서를 참조하십시오.
위험 점수 재정의	위험 점수의 자동 업데이트를 무효화하려면 이 확인란을 선택합니다. 재정의는 작업 메모에 반영됩니다.
비즈니스 영향	비즈니스에 대한 이 보안 인시던트의 중요도를 선택합니다. 기본값은 중요하지 않음입니다. 보안 인시던트 기록을 저장한 후 우선순위 조건 또는 위험 필드의 값을 변경하면 비즈니스 영향 이 다시 계산됩니다.
우선순위	긴급도에 따라 이 보안 인시던트를 처리할 순서를 선택합니다. 기록이 저장된 후 이 값이 변경되면 비즈니스 영향 계산에 영향을 줄 수 있습니다.
할당 그룹	이 보안 인시던트가 할당된 그룹입니다.
담당자	이 보안 인시던트를 분석하도록 할당된 사람입니다. 할당은 수동 또는 자동으로 수행할 수 있습니다. 자세한 내용은 보안 분석가 할당 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
간단한 설명	보안 인시던트에 대한 간단한 설명입니다.
지식 결과	간단한 설명을 입력하면 지식베이스의 관련 문서 링크가 나타납니다. 정보를 스캔하면 문제가 해결될 수 있습니다.

4. 기록 헤더를 마우스 오른쪽 버튼으로 클릭하고 저장을 선택합니다.
보안 인시던트에 새 CI를 추가한 경우 다음 통합 워크플로우가 자동으로 실행됩니다.
   - 보안 운영 - 실행 중인 프로세스 가져오기 플로우. 이 워크플로우는 호스트나 엔드포인트에서 CI(구성 항목)의 실행 중인 프로세스 목록을 검색합니다.
   - 보안 인시던트 대응 - 실행 중인 서비스 가져오기 워크플로우. 이 워크플로우는 Windows 기반 CI에서 실행 중인 서비스 목록을 검색합니다.
   - 보안 운영 통합 - 네트워크 통계 플로우 가져오기. 이 워크플로우는 호스트나 엔드포인트에서 활성 네트워크 연결 목록을 검색합니다.
5. 이러한 워크플로우에서 가져온 정보를 보려면 향상된 데이터 표시 관련 링크를 클릭한 다음 표시된 탭 중 하나를 클릭합니다.



주:
추가 워크플로우는 다음과 같이 활성화한 외부 공급업체 통합을 기반으로 실행됩니다 보안 운영 Carbon Black 통합 - 실행 중인 프로세스 플로우 가져오기

관련 정보

보안 인시던트 응답 설정

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

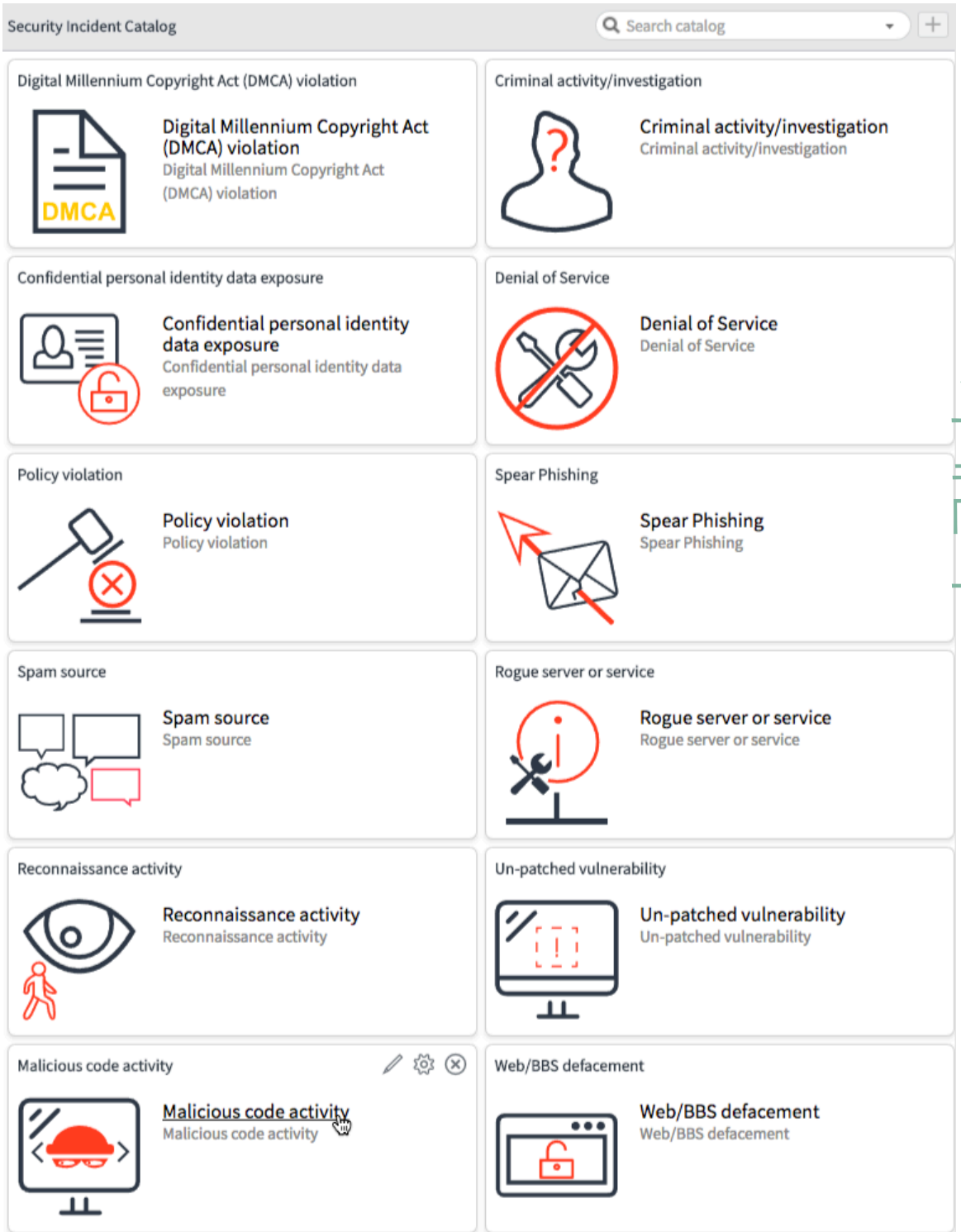
보안 인시던트 카탈로그에서 보안 인시던트 생성

회사의 사용자는 보안 인시던트 카탈로그를 사용하여 다양한 유형의 보안 관련 분석을 요청할 수 있습니다.

시작하기 전에
필요한 역할: 없음

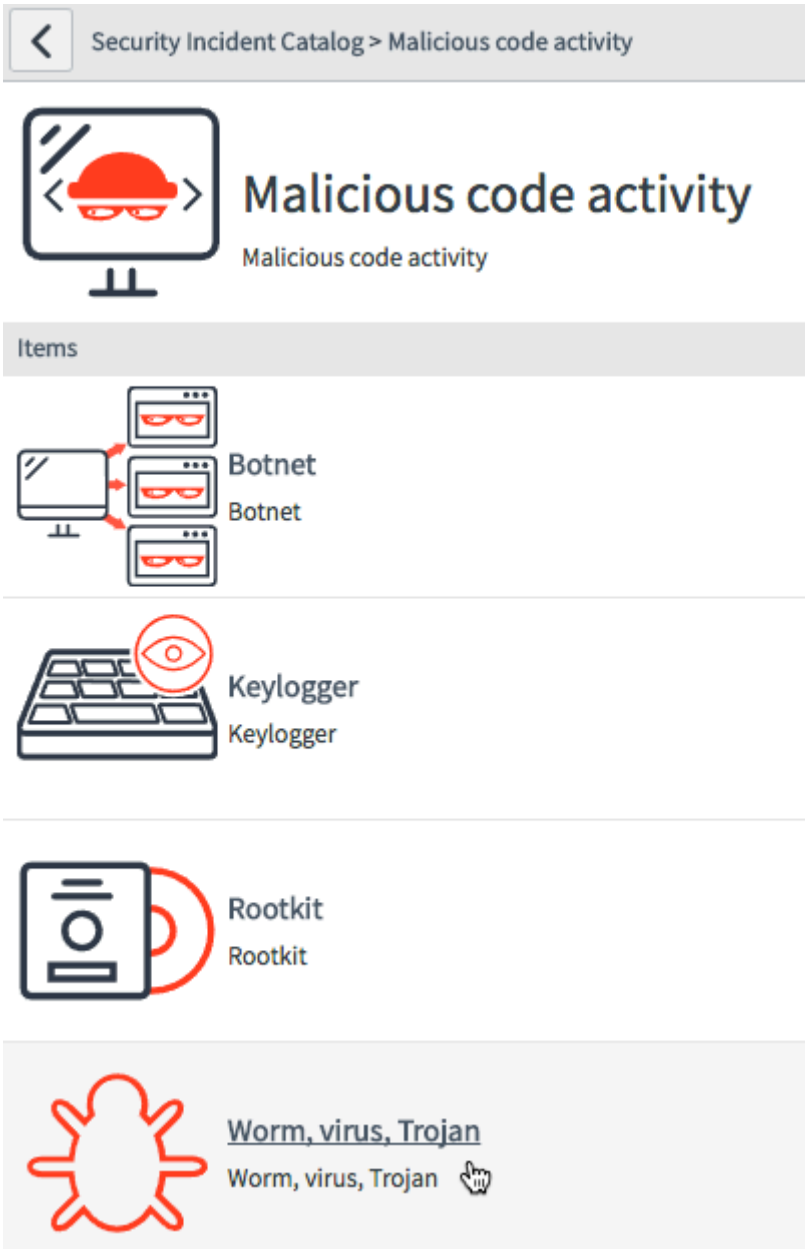
프로시저

1. 다음으로 이동 모두 〉 **Self-Service** 〉 보안 인시던트 카탈로그.



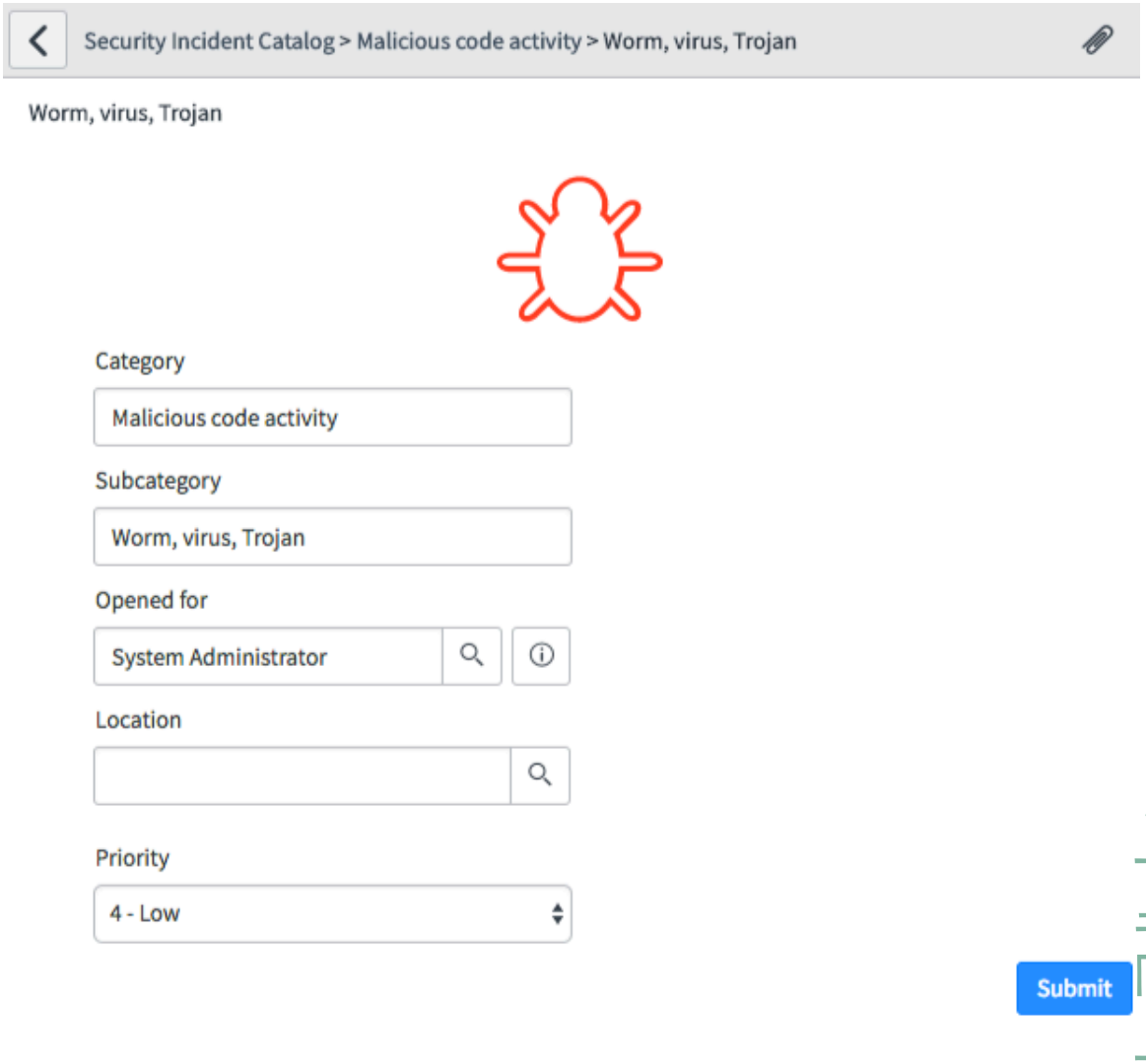
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

2. 요청하려는 카탈로그 항목을 클릭합니다.
   메인 카탈로그에서 선택한 항목에 하위 범주가 포함되어 있으면 목록이 표시됩니다. 다음 예제에서는 악성 코드 활동이 선택되었습니다.



3. 원하는 요청 유형과 가장 일치하는 하위 범주를 클릭합니다.
   이 예에서는 웜, 바이러스, 트로이 목마 하위 범주가 선택되었습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 요청에 대한 정보를 입력하고 제출을 클릭합니다.
   요청이 보안 인시던트 부서로 전송됩니다.
5. 요청을 제출한 후에는 다음으로 이동하여 진행 상황을 추적할 수 있습니다. **Self-Service** 〉 내 요청을 클릭하고 요청 번호를 입력합니다.

Event Management 경보에서 보안 인시던트 생성

이벤트 관리가 활성화되면 경보 양식에서 수동으로 보안 인시던트를 만들 수 있습니다.

시작하기 전에
Event Management 플러그인은 별도의 구독이 필요하며 ServiceNow 직원이 활성화해야 합니다. 이 플러그인은 데모 데이터를 포함하며 관련 플러그인이 아직 활성화되지 않은 경우 이를 활성화합니다. 이벤트 관리가 활성화되면 서비스 분석이 자동으로 활성화됩니다.
필요한 역할: evt_mgmt_admin, evt_mgmt_operator 또는 evt_mgmt_user

프로시저

1. 다음으로 이동 모두 〉 이벤트 관리 〉 모든 경보.
2. 경보 번호를 클릭합니다.
3. 보안 인시던트 생성을 클릭합니다.
4. 업데이트를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 인시던트 자동 생성

Splunk와 같은 타사 모니터링 도구를 통합하여 보안 인시던트 응답 해당 도구에서 가져온 보안 이벤트가 보안 인시던트를 자동으로 생성하도록 할 수 있습니다. 타사 도구에서 보안 경보로 데이터를 임포트할 수도 있습니다.

경보 모니터링 도구를 보안 인시던트 응답에 통합하려면 REST API 를 사용하여 보안 인시던트 임포트 [sn_si_incident_import] 테이블에 작성해야 합니다. 그런 다음 보안 인시던트 변환 변환 맵을 사용하여 임포트 세트 소스 테이블이 대상 보안 인시던트 [sn_si.incident] 테이블의 필드에 매핑됩니다.

변환 맵에서 인식되지 않는 CI 기록을 임포트하려고 시도하면 변환 맵 스크립트는 일치를 시도하면서 다음 순서에 대한 기록을 확인합니다.

- sys_id
- CI 이름
- 전체 주소 도메인 이름
- IP 주소

주:
보안 인시던트 변환 변환 맵이 사용 중인 외부 공급업체 경보 모니터링 도구에 적합하지 않은 것으로 확인되면 변환 맵을 복제하고 새로 만든 다음 필요한 경우 필드를 편집합니다.

이벤트 및 경보에서 생성되는 보안 인시던트

경보 모니터링 도구에서 이벤트를 가져오면 먼저 경보에서 Event Management 처리되고 경보로 그룹화됩니다. 이러한 경보를 사용하여 사용자 지정 가능한 경보 규칙에 따라 보안 인시던트를 만들거나 수동으로 검토하여 보안 인시던트로 조사할 경보를 선택할 수 있습니다.

애플리케이션 모듈 Event Management 에서 중요 경보로 보안 인시던트 생성이라는 경보 규칙 샘플 경보 규칙을 찾을 수 있습니다. 이 경보 규칙은 외부 공급업체 모니터링 애플리케이션 내부 ServiceNow 또는 외부 공급업체 모니터링 애플리케이션에서 중요한 보안 관련 이벤트가 수신될 때 자동으로 보안 인시던트를 생성합니다. 보안 인시던트가 생성된 후에는 새 이벤트가 수신되면 보안 인시던트가 업데이트됩니다. 경보 규칙의 작업 템플릿을 수정하여 이 경보 규칙에 의해 생성된 보안 인시던트의 초기 값을 변경할 수 있습니다. 생성하려는 각각의 고유한 다양한 보안 인시던트를 처리하기 위해 서로 다른 조건으로 다른 경보 규칙을 정의할 수 있습니다.

또는 보안 관리자 역할이 있는 사용자인 경우 의심스러운 경보에서 보안 인시던트 생성 버튼을 클릭하여 수동으로 보안 인시던트를 생성할 수 있습니다.

외부 도구에서 받은 이벤트에는 다음 정보가 포함되어야 합니다.

- 영향을 받는 자원이 되는 CI의 이름, IP 주소 또는 sys_id로 설정된 노드입니다.
- 이벤트 분류는 다른 IT 이벤트와 구분하기 위해 보안으로 설정됩니다.
- 보안 인시던트에 대한 설명을 채우는 이벤트 설명입니다.
- 추가 정보에는 범주, 공격 벡터, 반환 URL 또는 상관 관계 ID와 같이 이전에 나열된 필드 또는 기타 이벤트 필드에 맞지 않는 추가 정보가 포함될 수 있습니다. 형식은 다음 JSON 형식을 사용하여 필드 이름과 해당 값을 나열하는 문자열입니다.

```
{ "fieldName" : "fieldValue", "fieldName" : "fieldValue" }
```


© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
각 필드 및 값 쌍에 대해 열 이름이 fieldName과 일치하는 보안 인시던트의 필드가 비어 있으면 fieldValue로 설정됩니다. 보안 인시던트의 필드가 비어 있지 않으면 변경되지 않습니다. 두 경우 모두 이벤트와 추가 정보에 인코딩된 모든 필드 및 값은 이벤트를 설명하는 작업 메모 항목에 기록됩니다. 보안 인시던트에서 아무 것도 변경되지 않으면 작업 메모 항목이 생성되지 않습니다. 테이블에 추가하는 사용자 지정 필드를 포함하여 보안 인시던트의 모든 필드를 설정할 수 있습니다.

보안 경보로 임포트된 데이터

더 많은 JSON 인코딩 데이터로 이벤트가 생성되면 해당 데이터는 JSON 데이터에서 해당 값의 fieldName과 일치하는 이름을 가진 필드로 임포트됩니다.

타사 모니터링 소프트웨어(예: Splunk)에 기본 시스템에 공통되지 않는 데이터가 있는 경우, 경보 테이블에 새 필드를 추가하여 데이터 임포트를 수용할 수 있습니다. 경보로 데이터를 임포트하기 위한 JSON 형식은 이벤트 및 경보에서 보안 인시던트를 생성하는 데 사용되는 것과 동일한 형식입니다.

```
{ "fieldName" : "fieldValue", "fieldName" : "fieldValue" }
```

유일한 차이점은 필드의 데이터를 항상 fieldValue로 덮어쓴다는 것입니다.

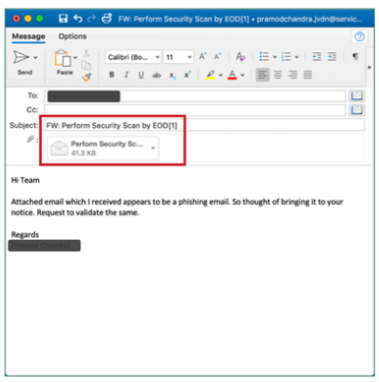
보안 이벤트 데이터를 임포트하면 경보 테이블의 필드가 일치하는 필드 이름으로 채워집니다. 경보가 나중에 보안 인시던트로 전환되면 동일한 추가 정보 데이터가 보안 인시던트의 일치하는 필드를 채웁니다.

사용자가 보고한 피싱 이메일에서 보안 인시던트 생성

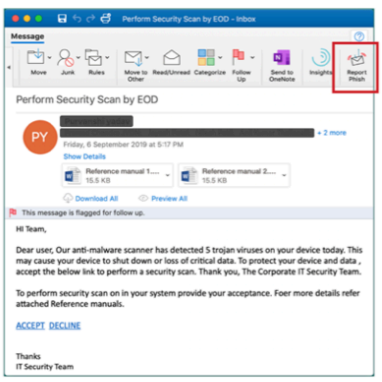
이 기능을 사용하여 사용자가 보고한 피싱 이메일에서 보안 인시던트를 생성합니다.

향상된 사용자 보고 피싱 기능에는 집계 기능, 이메일 헤더 추출 및 구성이 포함됩니다.

- 사용자는 여러 가지 방법으로 피싱 이메일을 보고할 수 있습니다.
  - 이메일을 첨부 파일로 전달할 수 있습니다.
  - **PhishAlarm** 플러그인(이전의 Wombat)이 Microsoft Outlook 클라이언트로 구성된 경우 사용자는 다음을 수행할 수 있습니다.
    - 피싱 보고 버튼을 클릭합니다.
    - 피싱 보고 옵션을 사용하여 모바일 장치에서 피싱 이메일을 전달합니다.



Desktop

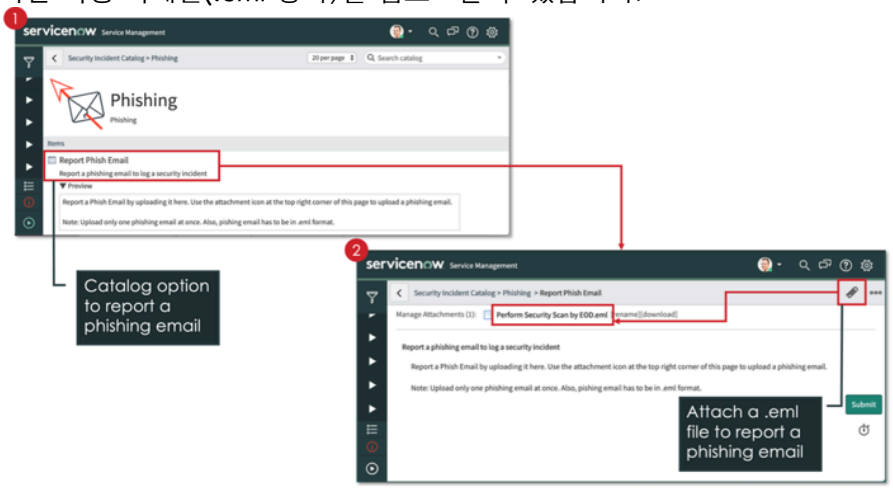


Desktop

Mobile

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 사용자는 피싱 이메일(.eml 형식)을 업로드할 수 있습니다.



- 사용자가 보고한 피싱에는 조직의 사용자가 보고한 중복 피싱 이메일을 식별하는 집계 비즈니스 논리 가 포함됩니다. 사용자는 이 기능을 사용하여 다음을 수행할 수 있습니다.
  - 중복 또는 유사한 사용자가 보고한 피싱 인시던트를 집계합니다(회사에서 시작한 피싱 캠페인).
  - 중복 사용자가 보고한 피싱 인시던트를 분류하지 않고 인시던트 통합과 관련된 수동 작업을 줄입니다.
  - 보안 분석가가 단일 사용자가 보고한 피싱 인시던트에 대해 작업할 수 있도록 합니다.
- 사용자가 보고한 피싱 인시던트 내에 피싱 이메일 헤더를 제공합니다.
  - 보안 분석가는 인시던트 내에서 주요 이메일 헤더 정보를 검색할 수 있습니다.
  - 다른 소스에서 헤더 정보를 수집하기 위한 수동 작업이 더 이상 필요하지 않습니다.
- 제출된 원래 피싱 이메일은 새 테이블에 피싱 이메일 기록 으로 저장됩니다.
- 보안 분석가는 피싱 이메일 콘텐츠, 헤더, 원본과 같은 원래 피싱 이메일의 상세 정보를 볼 수 있습니다.
- 보안 관리자는 다음을 포함하는 특정 개선 사항을 구성하고 적용할 수 있습니다.
  - 이메일 본문에서 이메일 헤더를 추출하는 구성입니다(피싱 제출 보고).
  - 선택한 헤더를 캡처하는 필터입니다.
  - 중복 피싱 이메일 기록이 식별될 때 상위-하위 인시던트 연결을 처리하기 위한 구성입니다.
  - 요구 사항에 따라 집계 비즈니스 논리를 수정하기 위한 플로우 디자이너 구성입니다.

사용자가 보고한 피싱에 대한 수집 규칙 설정

sn_si.admin 역할을 가진 사용자는 이메일 일치 규칙을 정의하여 특정 기준에 따라 사용자가 보고한 피싱 이메일을 필터링할 수 있습니다. 예를 들어 직접 또는 피싱 보고 버튼을 통해 *security@acme.com* 전송된 모든 이메일이 사용자가 보고한 피싱 이메일로 분류되는 규칙을 정의할 수 있습니다. 자세한 내용은 사용자가 보고한 피싱에 대한 수집 규칙 설정 문서를 참조하십시오.

사용자가 보고한 피싱 속성 정의

사용자가 보고한 피싱 이메일에서 캡처해야 하는 헤더 정보를 정의합니다. 자세한 내용은 사용자가 보고한 피싱 속성 정의 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용자가 보고한 피싱 이메일에서 생성된 피싱 이메일 기록

사용자가 보고한 피싱 이메일은 정의된 이메일 일치 규칙에 따라 보안 인시던트로 변환됩니다. 자세한 내용은 사용자가 보고한 피싱 이메일에서 생성된 피싱 이메일 기록 문서를 참조하십시오.

피싱 이메일을 보안 인시던트로 변환

피싱 이메일을 보안 인시던트로 변환 플로우는 피싱 이메일 기록을 보안 인시던트로 변환하거나 변환합니다. 자세한 내용은 사용자가 보고한 피싱 이메일을 보안 인시던트로 변환 문서를 참조하십시오.

피싱 이메일 기록에서 생성된 보안 인시던트 기록

관련 목록, 작업 메모 및 기타 중요 정보를 포함한 보안 인시던트 기록 상세 정보를 봅니다. 자세한 내용은 피싱 이메일 기록에서 생성된 보안 인시던트 기록 문서를 참조하십시오.

필수 구성요소 및 플러그인

이번 릴리스에서 사용할 수 있는 사용자 보고 피싱 기능은 London 릴리스에서 사용할 수 있는 기존 사용자 보고 피싱 기능의 향상된 버전입니다. 자세한 내용은 런던 문서에서 사용자가 보고한 피싱 공격을 확인하기 위한 규칙 만들기 항목을 참조하십시오.

중요한 설치 지침

이 개선 사항은 기존의 사용자 보고 피싱 설계를 대체합니다. 새 디자인에는 다음과 같은 업데이트가 포함됩니다.

- 기존 사용자가 보고한 피싱 이메일 인바운드 작업(유형 = 전달 및 유형 = 신규)이 비활성화되었습니다.
- 이제 새 피싱 이메일 생성 인바운드 작업을 사용할 수 있습니다.
- 사용자가 보고한 피싱 이메일을 보안 인시던트로 변환 새 플로우에는 새 설계에 대한 보안 인시던트 생성 및 집계 비즈니스 논리가 포함되어 있습니다. 새 설계를 적용하려면 이 플로우를 활성화해야 합니다.
- 기존 사용자 보고 피싱 규칙은 업그레이드 중에 보존되었습니다.

> **주:**
> 사용자가 보고한 피싱 제출에 대해 사용자 지정 이메일 인바운드 작업 및 사용자 지정 워크플로우를 사용하는 경우 이전 설계와 새 설계를 모두 검토하여 기능이 상충하거나 중복되는지 확인해야 합니다.

사용자가 보고한 피싱 개선 사항 상세 정보: 다음은 개선 사항에 대한 상세 정보입니다.

- 다양한 방법으로 피싱 이메일 보고: 자세한 내용은 을 참조하십시오 사용자가 보고한 피싱 이메일에서 보안 인시던트 생성 . 그러면 피싱 이메일이 *sn_si_phishing_email* 테이블로 이동됩니다.
- 피싱 이메일 기록 생성: 이메일 일치 규칙이 충족되면(참조 사용자가 보고한 피싱에 대한 수집 규칙 설정) 피싱 이메일 생성 인바운드 작업이 피싱 이메일 기록을 생성합니다. 구문 분석된 이메일 헤더는 cms*n_si_phishing_email_header* 테이블에 저장되고 피싱 이메일과 관련 목록으로 연결됩니다.
- 유사한 피싱 레코드를 단일 보안 인시던트로 집계: 플로우는 사용자가 보고한 피싱 이메일을 보안 인시던트로 변환 피싱 이메일 레코드에서 보안 인시던트를 생성하고 유사한 레코드를 단일 인시던트로 집계합니다. 집계 조건은 이 플로우에서 필요에 따라 수정할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

- Security **Incident** Response 9.0 릴리스 이전에 사용할 수 있었던 피싱 인바운드 작업을 사용자가 보고한 것은 이제 비활성화됩니다. 비활성화된 인바운드 작업을 통해 보안 인시던트가 더 이상 생성되지 않습니다.
- 새 설계를 적용하려면 Security Operations 스포크 애플리케이션을 설치해야 합니다. 여기에는 기본적으로 비활성 상태에서 사용할 수 있는 플로우가 사용자가 보고한 피싱 이메일을 보안 인시던트로 변환 포함됩니다. 이 플로우를 활성화하여 피싱 이메일 기록에서 보안 인시던트를 생성합니다.

다음 이미지는 이전 디자인과 새 디자인 간의 차이점을 보여 줍니다.

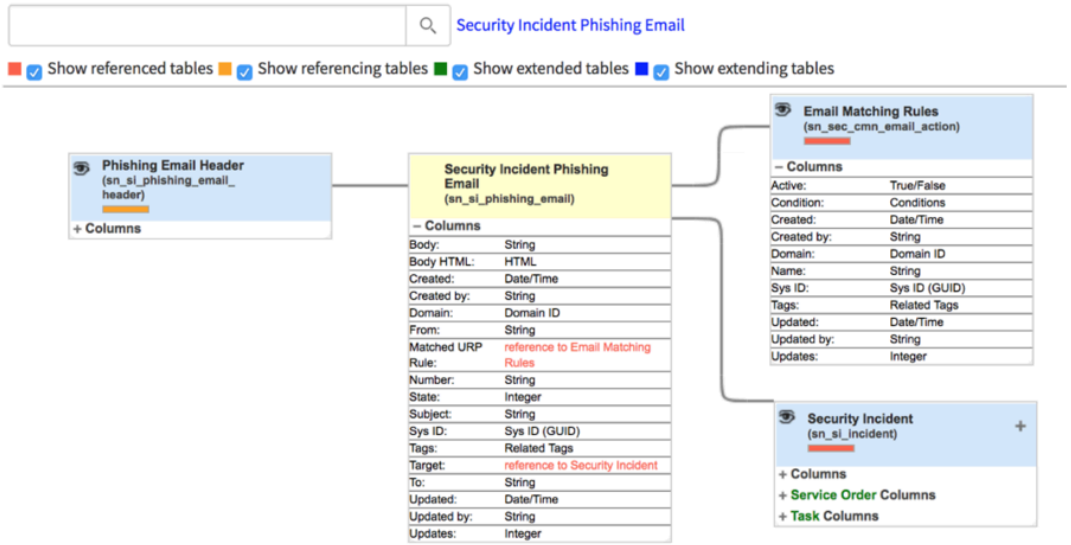
향상된 사용자 보고 피싱 기능을 사용하려면 다음 플러그인과 구성요소가 필요합니다.

- 보안 지원 공통(*sn_sec_cmn*): 포함 사항:
  - 인바운드 동작
  - 새 EmailUserReportedPhishing 스크립트
  - 수집 규칙 테이블
- Security Incident Response(sn_si): 포함 사항:
  - 보안 인시던트 테이블(sn_si_incident)
  - 보안 피싱 이메일 테이블(sn_si_phishing_email)
  - 보안 피싱 이메일 헤더 테이블(sn_si_phishing_email_header)
  - EML 업로드 기록 생성자
- Security Operations 스포크

  이메일을 집계하고 피싱 이메일을 보안 인시던트로 변환하는 플로우 및 하위 플로우입니다.

다음 그림은 일치하는 URP 규칙 및 대상 sn_si_incident(보안 인시던트 기록)에 대한 참조가 있는 새 피싱 이메일 테이블을 보여줍니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



사용자가 보고한 피싱에 대한 수집 규칙 설정

sn_si.admin 역할을 가진 사용자는 이메일 일치 규칙을 정의하여 특정 기준에 따라 사용자가 보고한 피싱 이메일을 필터링할 수 있습니다. 예를 들어 직접 또는 피싱 보고 버튼을 통해 *security@acme.com* 전송된 모든 이메일이 사용자가 보고한 피싱 이메일로 분류되는 규칙을 정의할 수 있습니다.

시작하기 전에

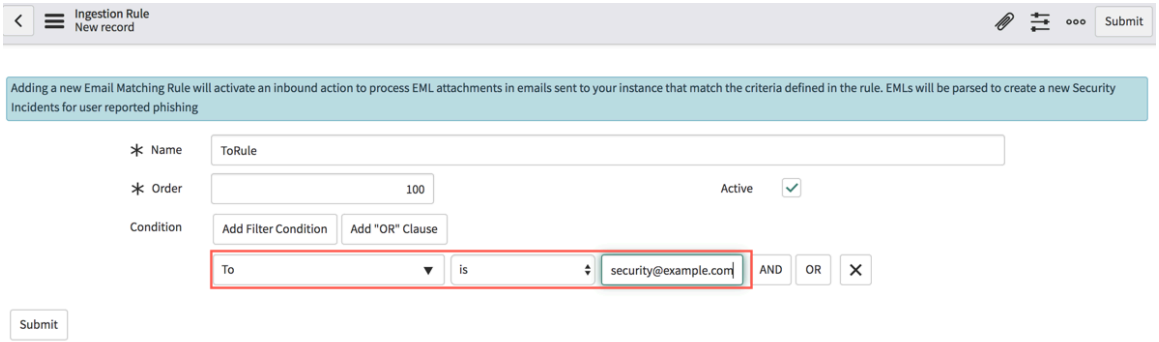
필요한 역할: sn_si.admin

프로시저

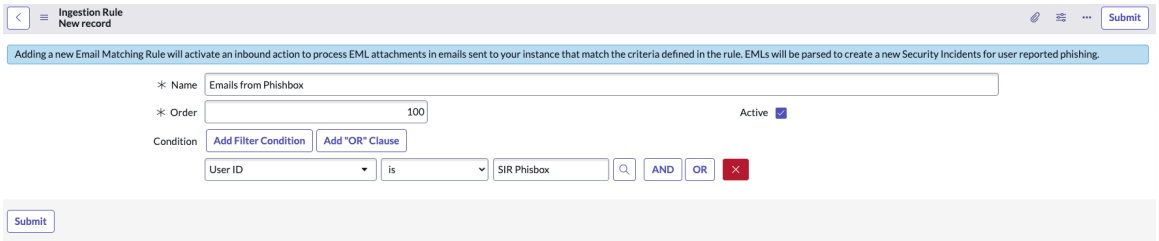
1. 다음으로 이동 모두 〉 보안 운영 〉 이메일 처리 〉 수집 규칙 - 사용자가 보고한 피싱.
2. 새로 만들기를 클릭하여 새 이메일 일치 규칙을 만듭니다.
3. 이름을 입력하고 규칙에 대한 하나 이상의 조건을 정의합니다.
4. 제출을 클릭하여 규칙을 저장합니다.
   다음은 몇 가지 샘플 규칙입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- **ToRule**: 직접 전송되었거나 *security@example.com* 이메일 ID로 전달된 이메일을 필터링합니다.



- 사용자 **ID** 규칙: 특정 이메일 ID에서 전송된 이메일을 필터링합니다.



사용자가 보고한 피싱 속성 정의

사용자가 보고한 피싱 이메일에서 캡처해야 하는 헤더 정보를 정의합니다.

시작하기 전에

필요한 역할: sn_si.admin

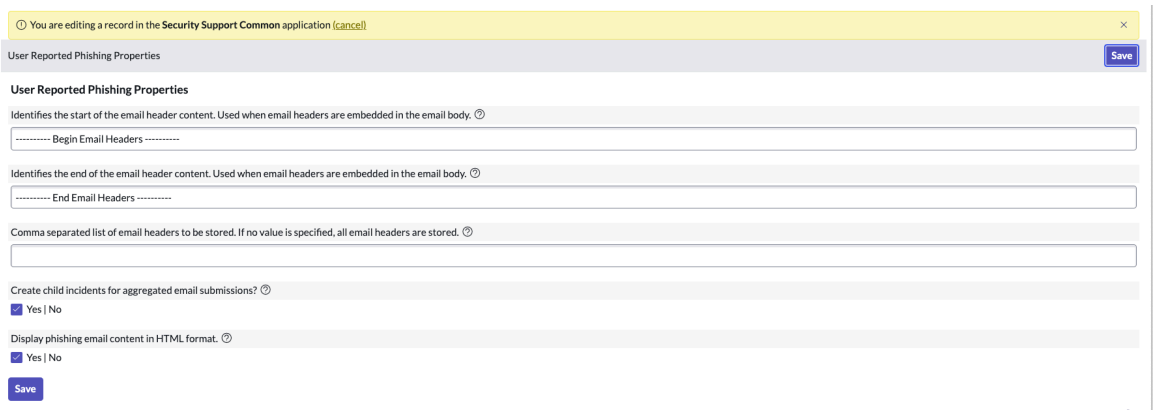
이 태스크 정보

이러한 옵션을 사용하여 다음과 같은 사용자가 보고한 피싱 설정을 구성합니다.

- 이메일 본문에서 이메일 헤더를 추출하는 구성입니다. (피싱 제출을 보고합니다.)
- 필터링하여 헤더를 선택합니다.
- 상위-하위 연결을 사용하거나 사용하지 않도록 설정합니다.

프로시저

1. 다음으로 이동 모두 〉 보안 운영 〉 이메일 처리 〉 사용자가 보고한 피싱 속성.



2. 이메일 본문에서 이메일 헤더를 추출하기 위한 구성을 지정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 이메일 헤더의 시작을 식별하는 문자열을 입력합니다.
- 이메일 헤더의 끝을 식별하는 문자열을 입력합니다.

> **주:**
> 이러한 설정은 피싱 이메일의 이메일 본문의 일부로 캡처된 헤더에만 적용됩니다. 예를 들어 **PhishAlarm** 플러그 인(이전의 Wombat)이 Microsoft Outlook 클라이언트로 구성된 경우 사용자가 피싱 보고 단추를 클릭하면 여기에 정의된 구성에 따라 전자 메일 헤더가 캡처됩니다. 피싱 이메일이 첨부 파일로 전달되면 헤더 정보가 캡처되지 않습니다.

3. 보안 인시던트를 조사하는 데 필요하지 않은 헤더를 제거하는 필터를 지정합니다.

   사용자가 보고한 피싱 이메일에서 캡처해야 하는 쉼표로 구분된 이메일 헤더 목록을 입력합니다. 여기에 값을 지정하지 않으면 모든 헤더 정보가 캡처됩니다.

4. 상위-하위 연결을 사용하거나 사용하지 않도록 설정합니다.
   기본적으로 예 옵션은 활성화되어 있습니다. 사용자가 보고한 피싱 이메일이 집계될 때 하위 보안 인시던트를 생성해야 함을 나타내려면 예를 선택합니다. 아니요를 선택하면 하위 보안 인시던트가 생성되지 않지만 사용자가 보고한 피싱 이메일이 보안 인시던트와 연결되고 보안 인시던트 기록이 업데이트됩니다. 하위 보안 인시던트가 생성되는 방식에 대한 자세한 내용은 을 참조하십시오 사용자가 보고한 피싱 이메일을 보안 인시던트로 변환 .

5. 피싱 이메일 컨텐츠를 HTML 형식으로 표시하는 옵션을 활성화하거나 비활성화합니다.
   기본적으로 예 옵션은 활성화되어 있습니다. 예를 선택하여 피싱 이메일 콘텐츠를 HTML 형식으로 표시합니다. 아니요를 선택하면 HTML 형식의 이메일 콘텐츠가 피싱 기록 내에 표시되지 않습니다.

사용자가 보고한 피싱 이메일에서 생성된 피싱 이메일 기록

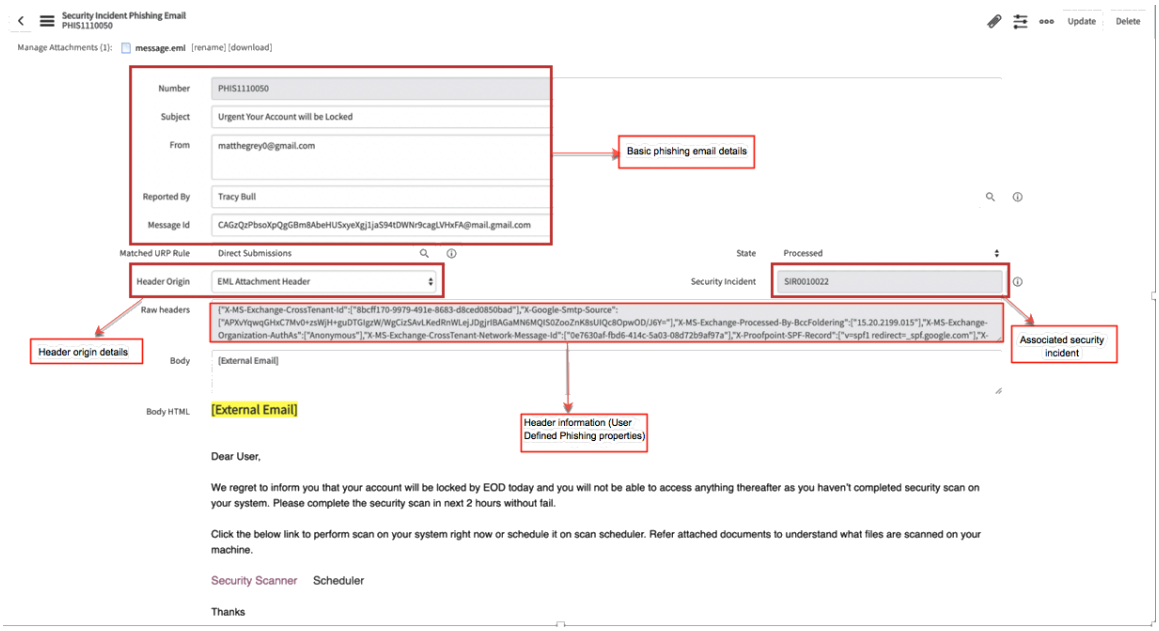
사용자가 보고한 피싱 이메일은 정의된 이메일 일치 규칙에 따라 보안 인시던트로 변환됩니다.

새 피싱 이메일이 보고되면 다음 작업이 수행됩니다.

- *sys_email* 테이블에 이메일 기록이 생성됩니다.
- 피싱 이메일 생성 인바운드 작업이 이메일 기록에서 실행되고 이메일 일치 규칙(참조사용자가 보고한 피싱에 대한 수집 규칙 설정)을 사용하여 피싱 이메일인지 확인합니다.
- 피싱 이메일로 식별되면 sn_si_phishing_email 테이블에 피싱 이메일 기록이 생성됩니다.
- 마지막으로 플로우가 사용자가 보고한 피싱 이메일을 보안 인시던트로 변환 적용되어 피싱 이메일 기록을 보안 인시던트로 전환합니다.

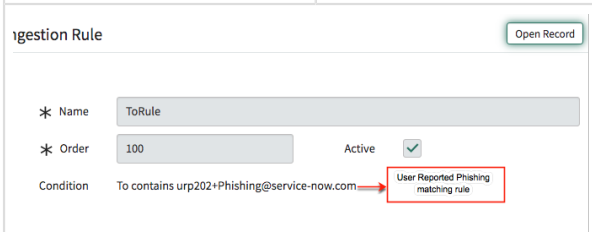
이메일 상세 정보를 보려면 다음으로 이동하십시오. 보안 인시던트 〉 모든 피싱 이메일 표시. 피싱 이메일 기록 목록이 표시됩니다. 생성됨 열에서 날짜 링크를 클릭하여 이메일 기록을 봅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



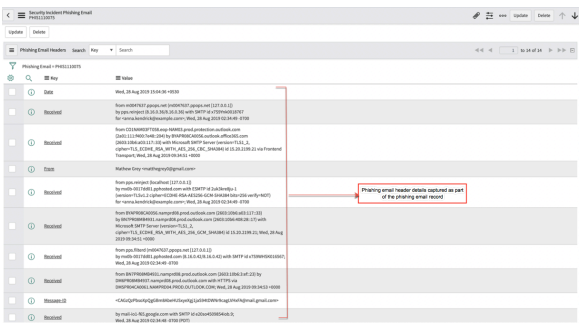
보안 인시던트 피싱 이메일 상세 정보

필드 이름	설명
번호	사용자가 보고한 피싱 이메일에 할당된 번호입니다.
제목	이메일의 제목입니다. 제목 규칙은 시뮬레이션된 피싱 캠페인 또는 테스트에 유용합니다. 이 경우 조직은 피싱 및 유사한 이메일 공격에 대한 대응을 테스트하기 위해 사기성 이메일을 직원에게 보냅니다. 시뮬레이션된 피싱 전자 메일 테스트에서 **PhishAlarm** 플러그 인(이전의 Wombat)이 있는 Microsoft Outlook 전자 메일 클라이언트를 사용하는 경우 사용자는 피싱 보고 단추를 클릭하여 피싱 전자 메일을 보고할 수 있습니다. 이메일의 제목에 시뮬레이션 된 피싱 이 추가된 이메일이 보안 운영 팀으로 전송됩니다. 이는 이메일을 시뮬레이션된 피싱 이메일로 식별하는 데 사용됩니다.
시작일	이 피싱 이메일이 시작된 이메일 주소입니다. 이 정보는 피싱 이메일이(으)로 전달될 경우 사용할 수 있습니다. EML 파일 첨부 파일 또는 원본 헤더가 이메일에 포함된 경우. 사용자가 피싱 이메일을 직접 전달한 경우 보낸 사람 주소를 사용하지 못할 수 있습니다.
보고자	이 피싱 이메일을 보고한 사용자의 이메일 ID입니다. 추가 상세 정보를 보려면 정보 아이콘을 클릭합니다.
메시지 ID	메시지에 할당된 ID입니다.
일치하는 URP 규칙	이 이메일에 적용할 사용자 보고 피싱 규칙입니다. 추가 상세 정보를 보려면 정보 아이콘을 클릭합니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 인시던트 피싱 이메일 상세 정보

필드 이름	설명
보시다시피 이 예에서 조건 필드는 이 이메일에 ToRule이 적용되고 보안 인시던트가 생성되었음을 보여줍니다. 이메일 일치 규칙 정의에 대한 자세한 내용은 을 참조하십시오 사용자가 보고한 피싱에 대한 수집 규칙 설정 .	
상태	sn_si_phishing_email 테이블에 새 피싱 이메일 기록이 생성되면 상태 필드가 신규로 설정됩니다. 이 이메일 기록이 보안 인시던트로 변환되면 (참조 사용자가 보고한 피싱 이메일을 보안 인시던트로 변환) 상태 필드가 처리됨으로 업데이트됩니다.
헤더 원본	이 필드는 이메일 헤더가 시작된 방법 또는 사용자가 피싱 이메일을 보고한 방법을 나타냅니다. • 이메일 헤더: 사용자가 피싱 이메일을 보안 운영 팀에 전달했습니다. • 이메일 텍스트 본문: ○ 사용자가 피싱 보고 옵션을 클릭했습니다(**PhishAlarm** 플러그 인(이전의 Wombat)가 전자 메일 클라이언트로 구성된 경우). ○ 정의된 사용자 보고 피싱 규칙에 따라 피싱 이메일이 보안 운영 팀으로 전달됩니다. • **EML** 첨부 파일 헤더: ○ 첨부 파일: 사용자가 이메일을 첨부 파일(. EML 파일). ○ Service Catalog 제출: 사용자가 이메일을 . EML 파일을 바탕 화면에 업로드한 다음 지정된 위치에 업로드했습니다. 그러면 이메일에서 보안 인시던트가 생성됩니다. • **EML** 첨부 파일 본문: ○ 사용자가 피싱 보고 옵션을 클릭했습니다(**PhishAlarm** 플러그 인(이전의 Wombat)가 전자 메일 클라이언트로 구성된 경우). ○ 정의된 사용자 보고 피싱 규칙에 따라 피싱 이메일은 보안 운영 팀에 첨부 파일로 전달됩니다.
보안 인시던트	사용자가 보고한 피싱 이메일이 처음 보고되면 이 필드는 비어 있습니다. 플로우가 사용자가 보고한 피싱 이메일을 보안 인시던트로 변환 실행되면 이 이메일이 보안 인시던트 기록으로 변환되고 이 기록 번호가 여기에 표시됩니다.
원시 헤더	이 필드에는 페이지에 정의된 사용자가 보고한 피싱 속성 정의 대로 이메일에서 추출한 전체 헤더 정보가 표시됩니다. 헤더는 키 값 쌍으로 구문 분석되고 피싱 이메일 헤더 목록에 표시됩니다.
	
본문	사용자가 보고한 피싱 이메일의 본문입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용자가 보고한 피싱 이메일을 보안 인시던트로 변환

피싱 이메일을 보안 인시던트로 변환 플로우는 피싱 이메일 기록을 보안 인시던트로 변환하거나 변환하는 새로운 플로우입니다.

시작하기 전에

주:
사용자가 보고한 피싱 기능을 사용하려면 플로우의 사본을 만들고 활성화해야 합니다. 사용자가 보고한 피싱 제출을 처리하기 위해 사용자 지정 인바운드 작업 및 사용자 지정 플로우를 생성한 경우 여기에 제안된 플로우 수정은 필요하지 않습니다.

- 필요한 역할: sn_si.admin
- Flow Designer 스포크가 설치되어 있어야 합니다.

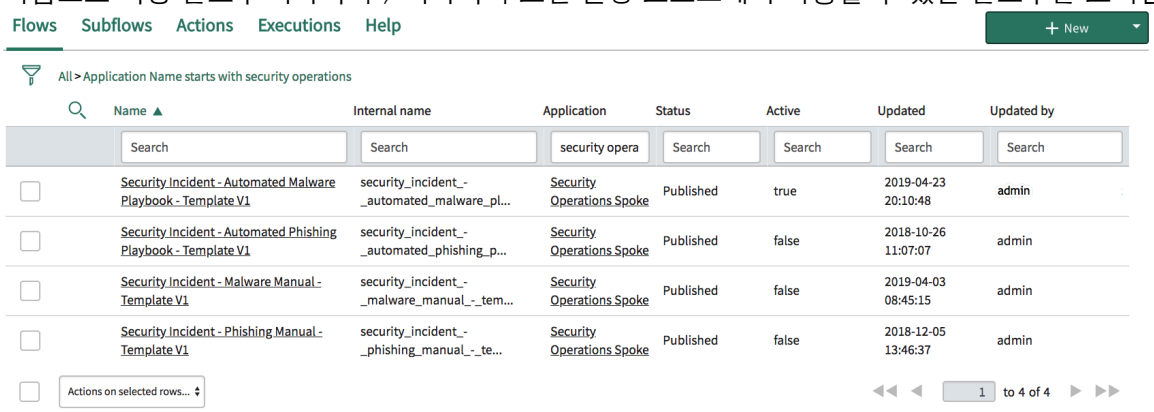
이 태스크 정보

이 플로우는 상태가 신규 로 설정된 사용자가 보고한 피싱 이메일 기록이 생성되면 자동으로 시작됩니다. 이 플로우에는 다음과 같은 논리가 포함되어 있습니다.

- 보안 인시던트를 집계합니다.
- 관련 메모로 보안 인시던트를 업데이트합니다.
- 헤더 데이터를 추가합니다.
- 필요에 따라 하위 인시던트를 생성합니다.

프로시저

- 다음으로 이동 플로우 디자이너 〉 디자이너 보안 운영 스포크에서 사용할 수 있는 플로우를 보려면

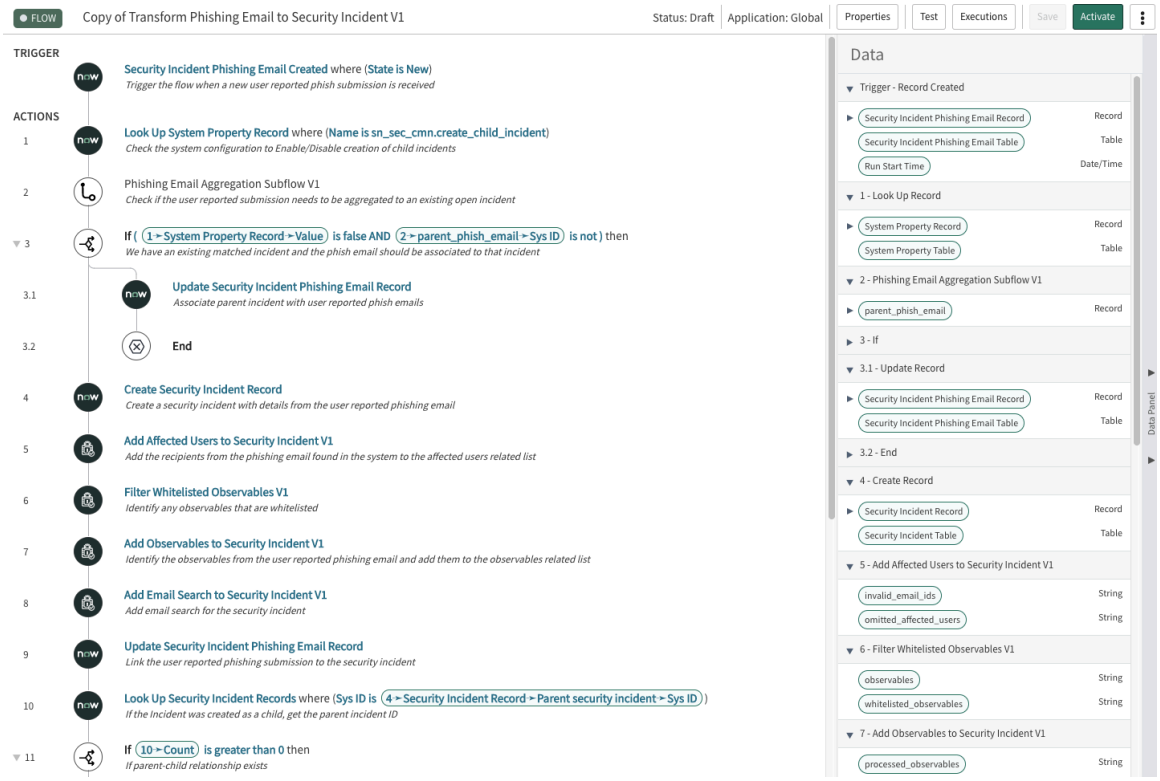


- 플로우를 보려면 피싱 이메일을 보안 인시던트로 변환 링크를 클릭합니다.
- 이 플로우는 기본 시스템과 함께 제공되며 읽기 전용 모드이므로 사용할 수 없습니다.

  더보기 아이콘 클릭하고 플로우의 사본을 만들어 사용할 수 있도록 엽니다. 이제 트리거 조건 또는 작업을 수정하거나 작업을 추가 및 제거하는 등 플로우를 변경할 수 있습니다. 필요한 변경을

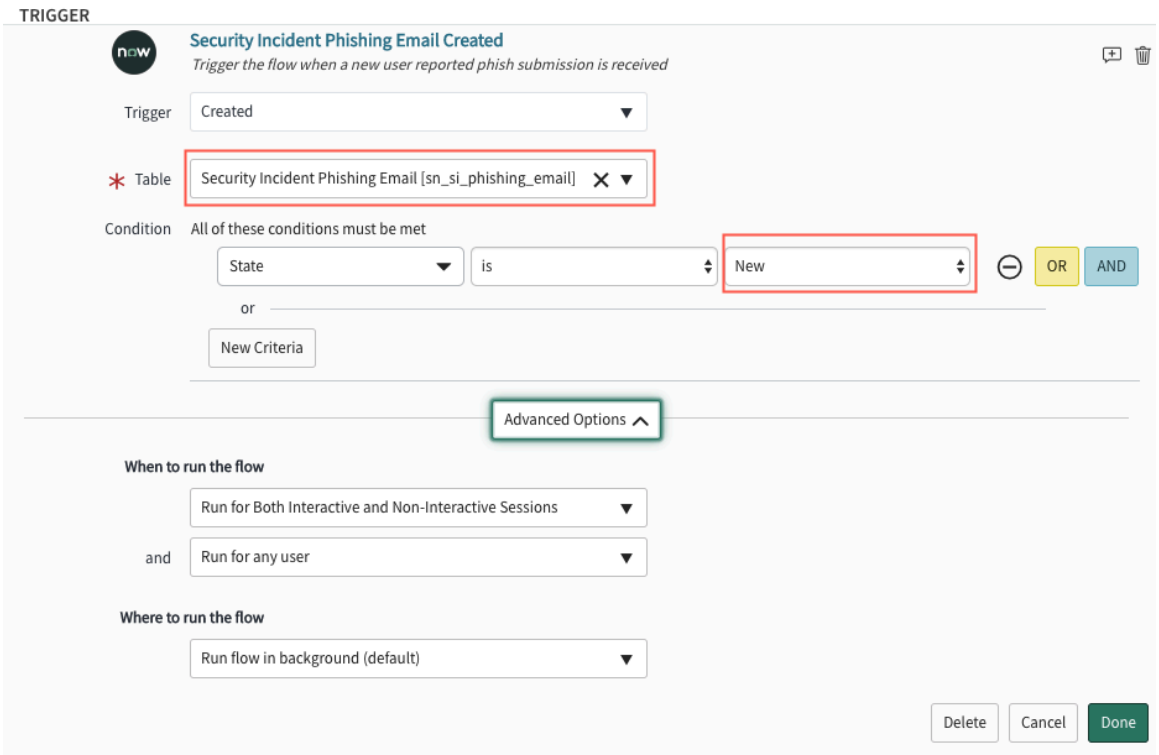
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

한 후에는 플로우를 활성화(참조 플로우 활성화 보안 인시던트 응답)하여 실행할 수 있도록 해야 합니다.



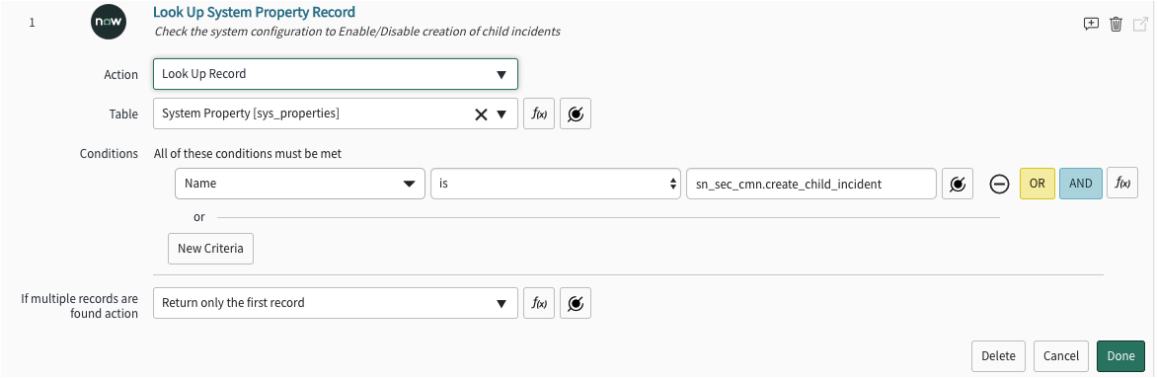
이 그림은 플로우와 함께 실행되는 트리거 및 단계를 보여줍니다. 오른쪽 패널은 데이터 흐름을 보여줍니다. 아이콘을 클릭하여 단계를 확장하고 세부 정보를 봅니다.

- 트리거 아이콘을 클릭합니다.
  첫 번째 단계에서는 플로우에 대한 트리거를 정의하거나 설정합니다. 조건이 충족될 때 수행할 트리거 및 작업의 조건을 지정합니다. 이 플로우는 새 기록이 sn_si_phishing_email 테이블에 업로드될 때 시작됩니다.

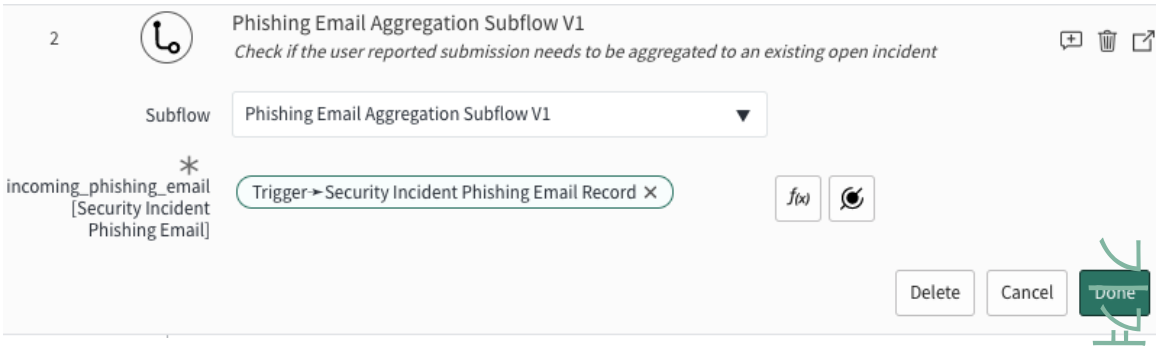


© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

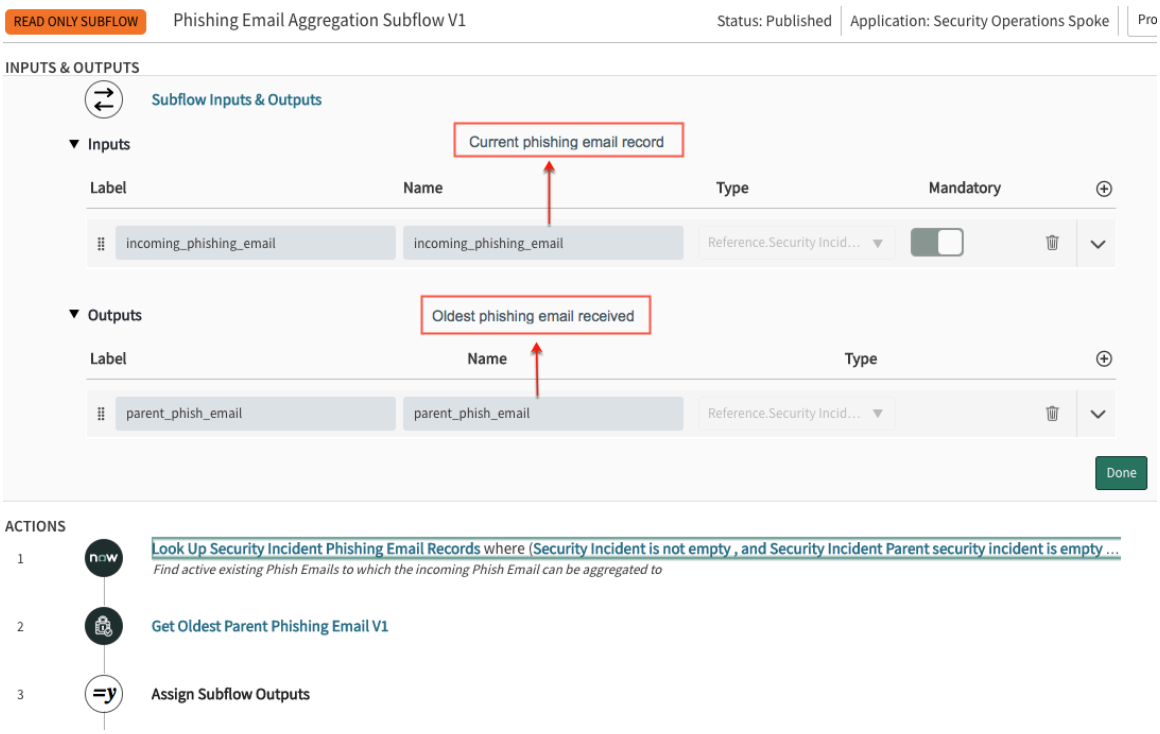
- 1단계에서 플로우는 집계된 이메일 제출에 대한 하위 인시던트 생성 플래그가 사용자가 보고한 피싱 이메일을 보안 인시던트로 변환 페이지에서 사용 또는 사용 안 함으로 설정되어 있는지 확인합니다.



- 2단계에서는 가장 오래된 상위 보안 인시던트가 식별됩니다.
  2단계에서 아이콘을 확인합니다. 이는 피싱 이메일 집계 하위 플로우가 이 단계의 일부로 실행됨을 나타냅니다.

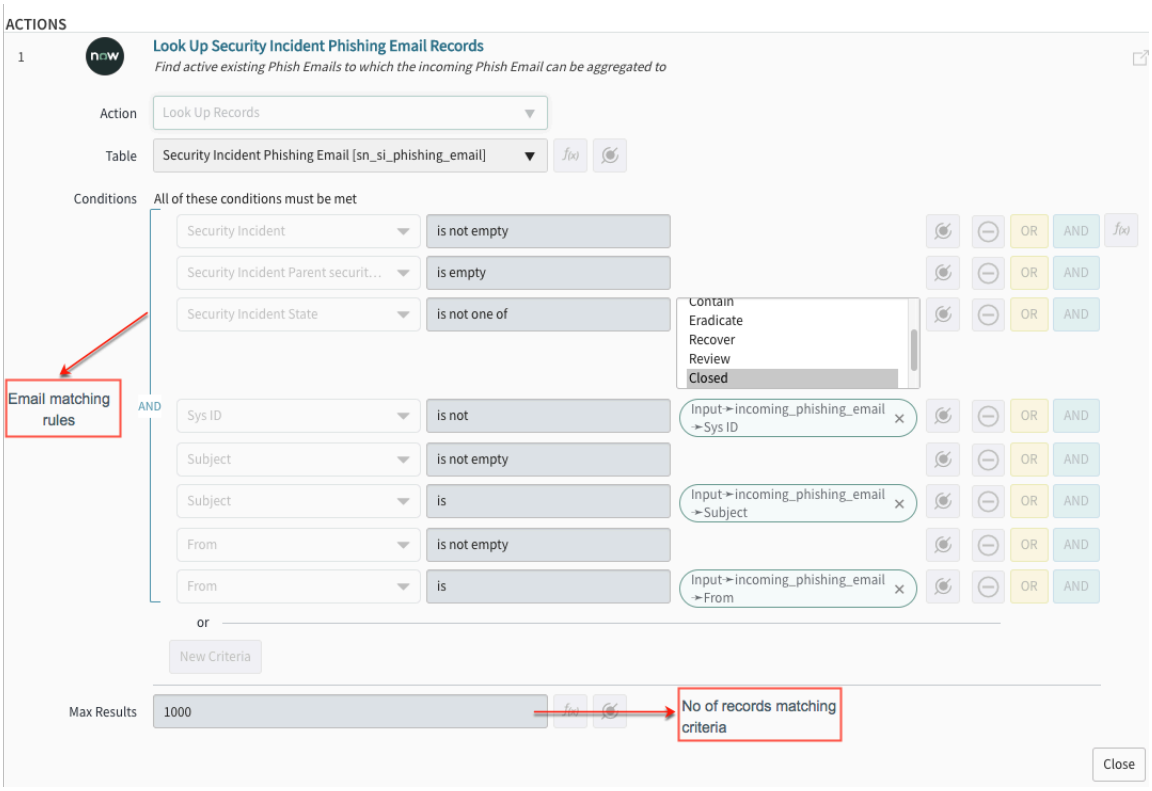


작업의 상세 뷰를 보려면 작업 디자이너 아이콘을 클릭하십시오. 이 하위 플로우는 피싱 이메일을 확인하고 지정된 기준에 따라 기존 보안 인시던트와 일치시킵니다.



이 두 작업은 이 하위 플로우가 실행될 때 수행됩니다. 추가 세부 정보를 보려면 첫 번째 작업의 링크를 클릭하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

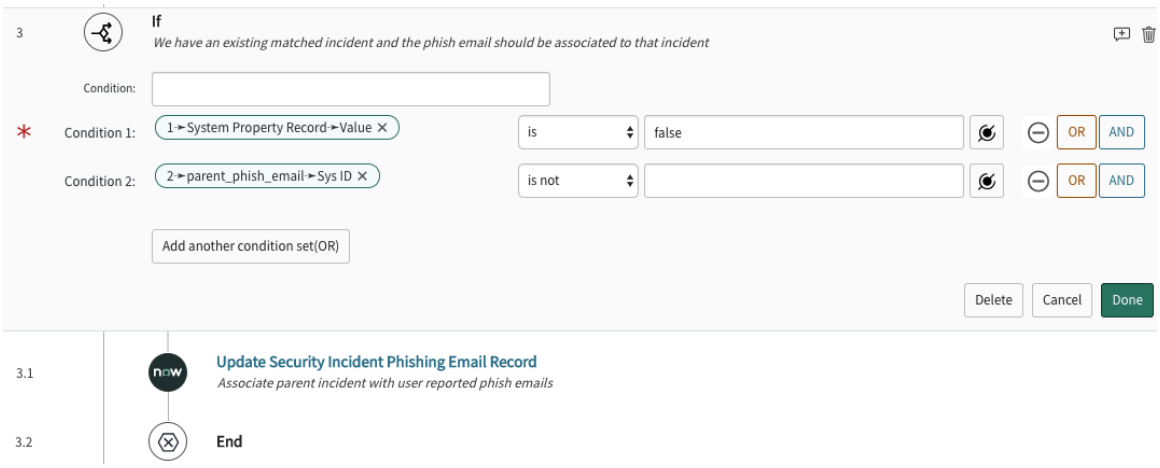


이 작업은 다음과 같은 조건에 따라 새 수신 이메일의 기준과 일치하는 이메일을 확인합니다.

- 보안 인시던트 상태가 종결되지 않은 경우.
- 제목 또는 보낸 사람 값이 정의된 이메일 일치 규칙 조건과 일치합니다(참조 사용자가 보고한 피싱에 대한 수집 규칙 설정).

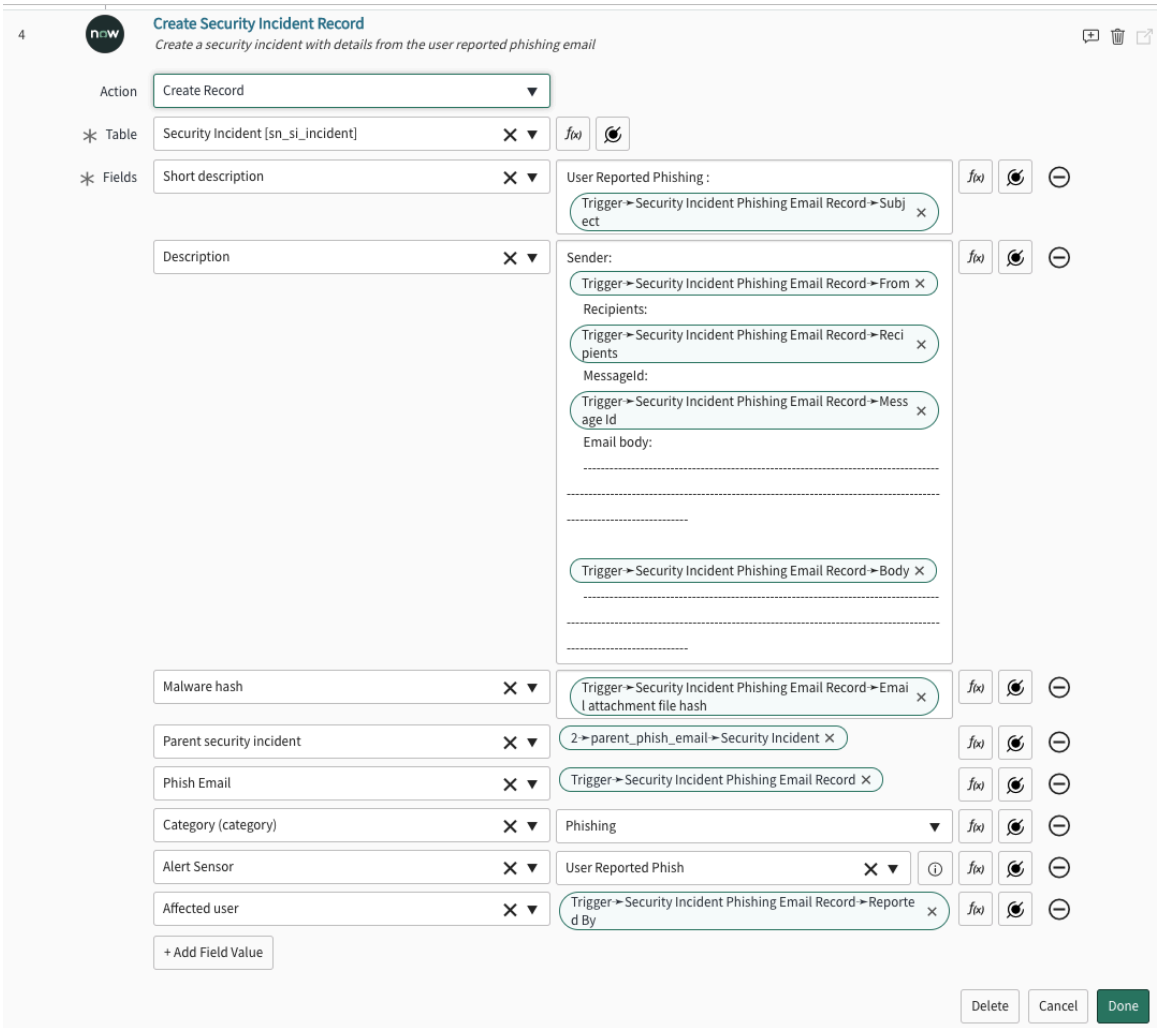
이러한 조건이 충족되면 최대 결과 필드의 기준과 일치하는 기록 수를 볼 수 있습니다. 목록에서 가장 오래된 기록 또는 첫 번째 기록이 보안 인시던트가 집계될 상위 기록으로 지정됩니다.

- 3단계는 집계된 이메일 전송에 대한 하위 인시던트를 생성하시겠습니까? 플래그가 페이지에서 아니요 로 설정된 경우에만 적용할 수 사용자가 보고한 피싱 이메일을 보안 인시던트로 변환 있습니다.
  이 경우 피싱 이메일이 보안 인시던트 기록과 연결되고 플로우가 종료됩니다.

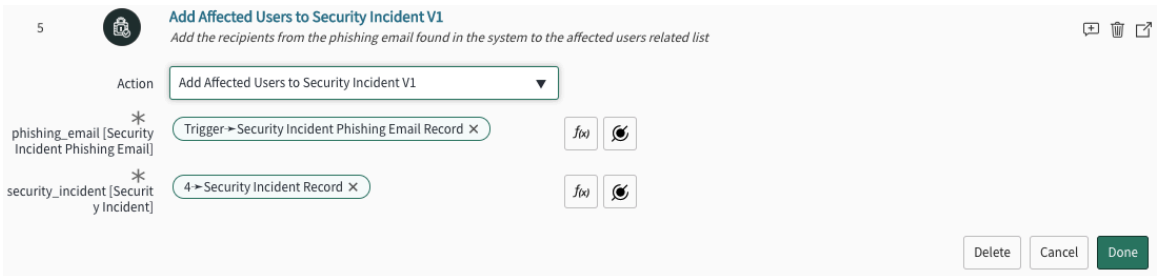


- 집계된 이메일 제출에 대한 하위 인시던트 생성이 예로 설정된 경우 플로우는 계속 실행되고 사용자가 보고한 피싱 이메일을 기반으로 새 보안 인시던트가 생성됩니다.

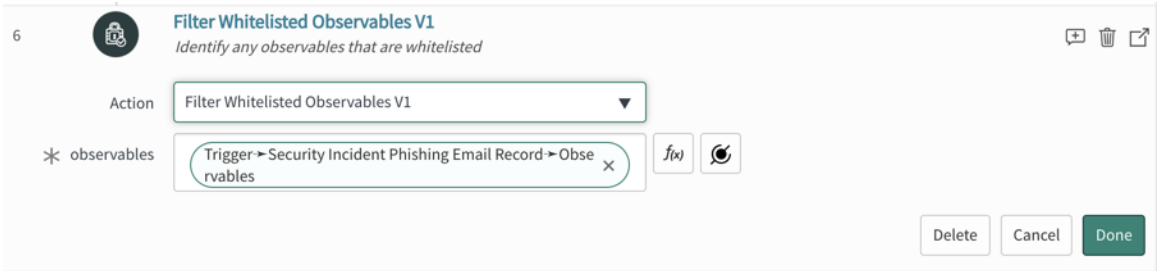
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



- 5단계에서 피싱 이메일을 받은 사용자(피싱 이메일의 받는 사람 및 참조 목록에 있는 직원)가 보안 인시던트 기록의 영향을 받는 사용자 관련 목록에 추가됩니다.

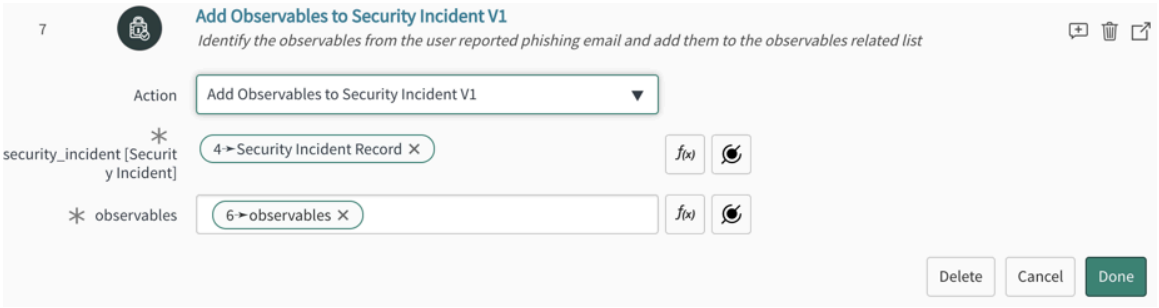


- 6단계에서는 허용 목록에 있는 옵저버블이 보안 인시던트의 옵저버블 목록에서 필터링됩니다. 이러한 허용 목록에 있는 옵저버블은 보안 인시던트에 추가되지 않습니다.

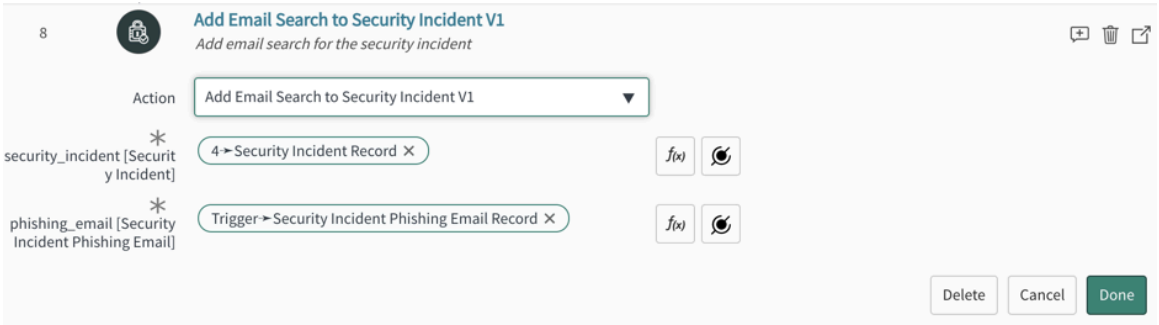


© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

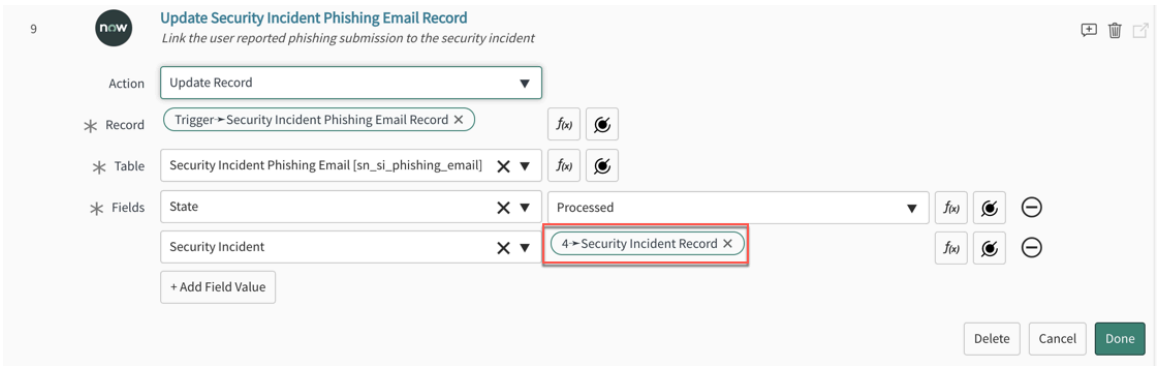
- 7단계에서는 사용자가 보고한 피싱 이메일에서 알 수 없는 옵저버블이 식별되어 옵저버블 관련 목록에 추가됩니다.



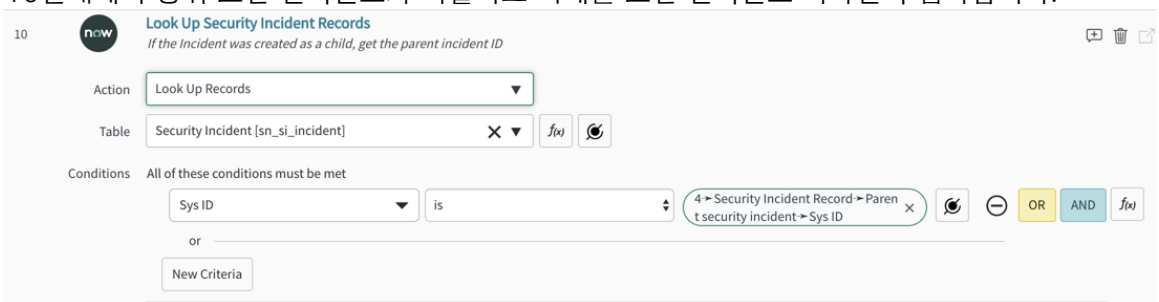
- 8단계에서는 이메일의 제목과 보낸 사람 주소를 조합한 이메일 검색 쿼리가 생성됩니다. 이 정보는 피싱을 당한 조직의 직원을 식별하는 데 유용합니다.



- 9단계에서 사용자가 보고한 피싱 이메일이 보안 인시던트와 연결되고 보안 인시던트 기록(4단계에서 생성됨)이 업데이트됩니다.

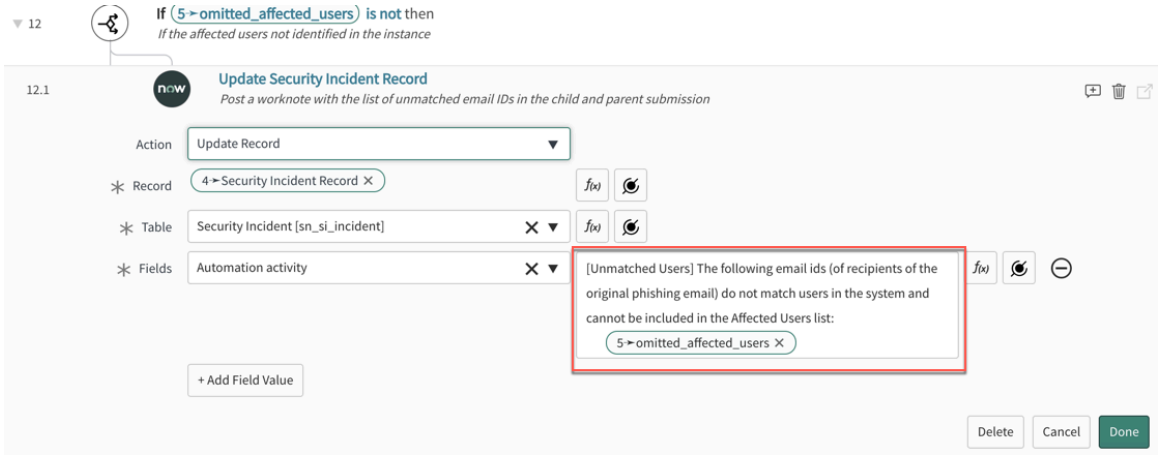


- 10단계에서 상위 보안 인시던트가 식별되고 미해결 보안 인시던트 기록인지 검사합니다.

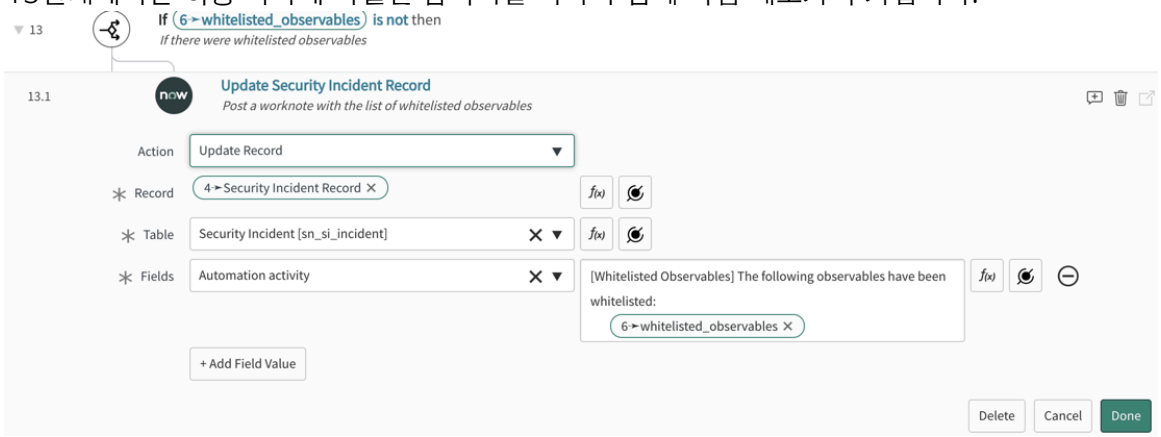


- 상위 보안이 활성 상태인 경우 하위 및 상위 보안 인시던트 기록에 이들이 서로 연결되는 방식을 나타내는 메모가 추가됩니다.
- 12단계에서 영향을 받는 사용자를 찾을 수 없으면(플로우의 5단계에서) 작업 메모가 추가되고 보안 인시던트 기록이 업데이트됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

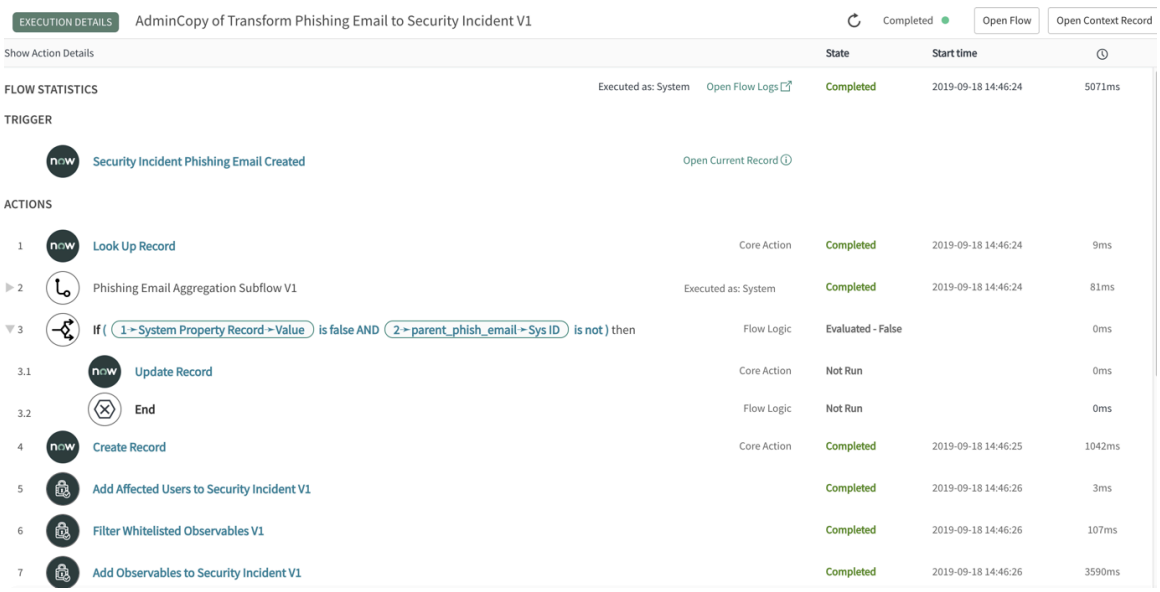


- 13단계에서는 허용 목록에 나열된 옵저버블 목록과 함께 작업 메모가 추가됩니다.



다음에 수행할 작업
테스트를 클릭하여 플로우의 작업을 게시하기 전에 시뮬레이션할 수 있습니다. 플로우를 테스트한 후 활성화 를 클릭하여 플로우를 활성화하면 실행됩니다.

실행을 클릭하여 플로우의 실행 세부 정보를 봅니다.



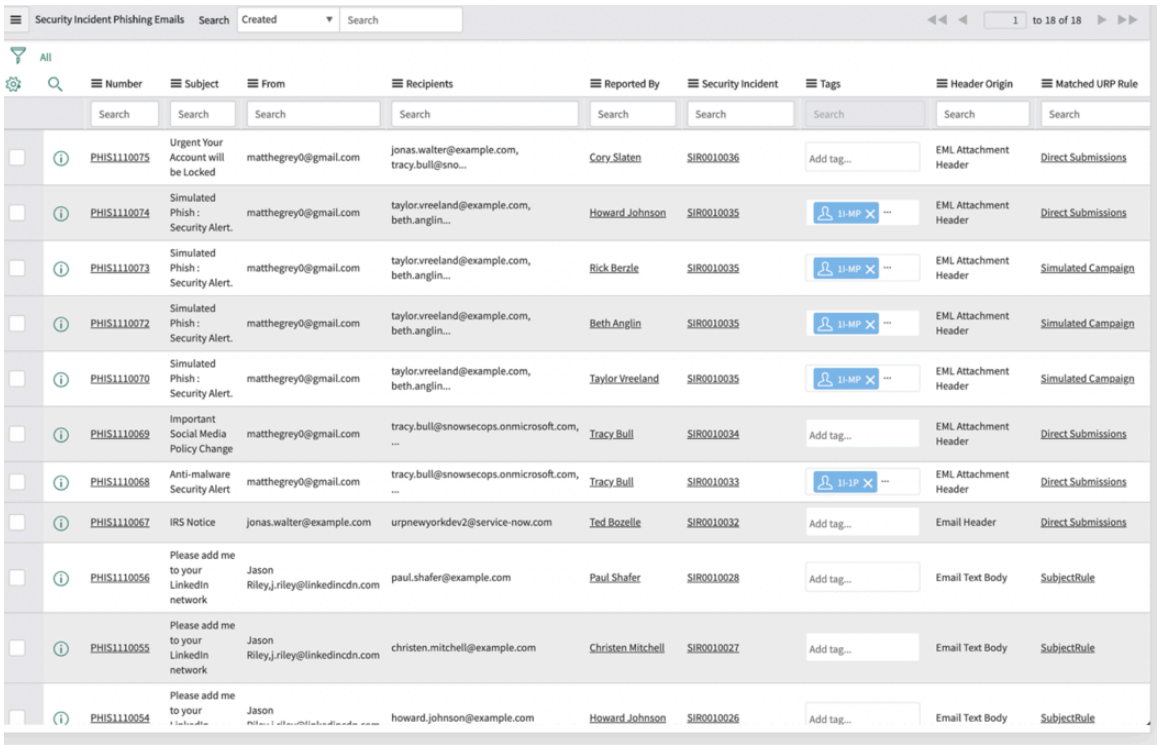
플로우가 실행되면 피싱 이메일 기록이 보안 인시던트로 변환됩니다. 피싱 이메일 기록에서 생성된 보안 인시던트 기록 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

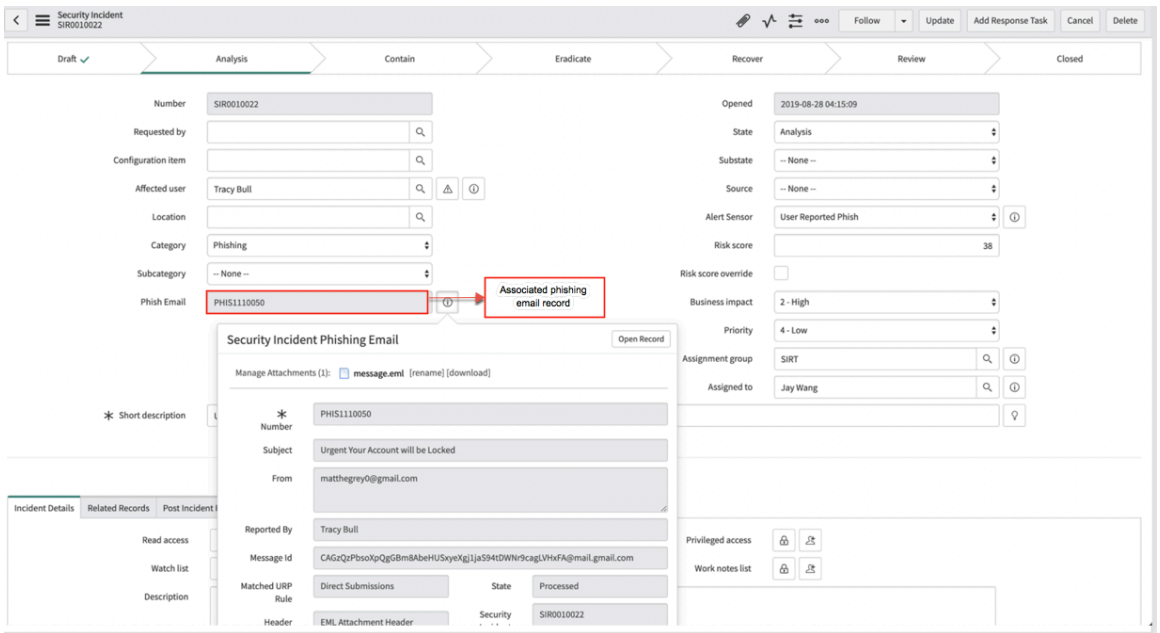
피싱 이메일 기록에서 생성된 보안 인시던트 기록

sn_si_phishing_email 테이블에 저장된 피싱 이메일 기록은 보안 인시던트 기록으로 변환됩니다.

피싱 이메일 기록과 연결된 보안 인시던트를 보려면 클릭하십시오. 보안 인시던트 〉 피싱 이메일 〉 모든 피싱 이메일 표시.



피싱 이메일 기록과 연결된 보안 인시던트 열에서 링크를 클릭합니다. 보안 인시던트 상세 정보가 표시됩니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

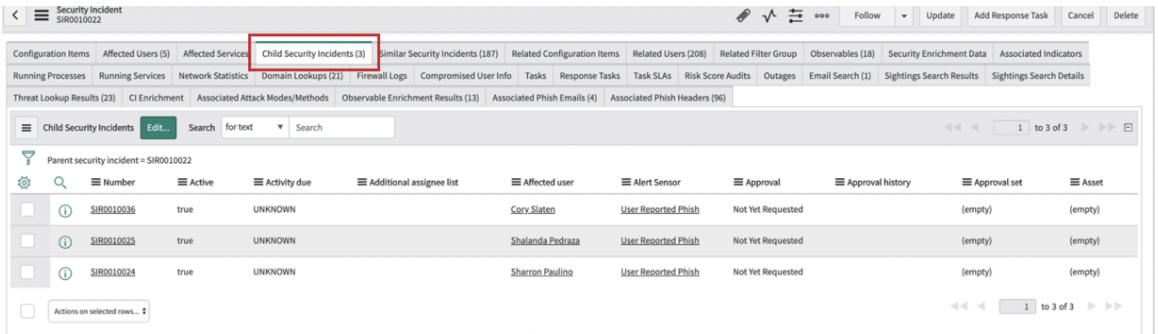
관련 목록

보안 인시던트의 관련 링크 섹션까지 아래로 스크롤하고 관련 목록 모두 표시를 클릭합니다. 하위 보안 인시던트, 영향을 받는 사용자, 관련 피싱 이메일과 같은 상세 정보를 봅니다.

하위 보안 인시던트

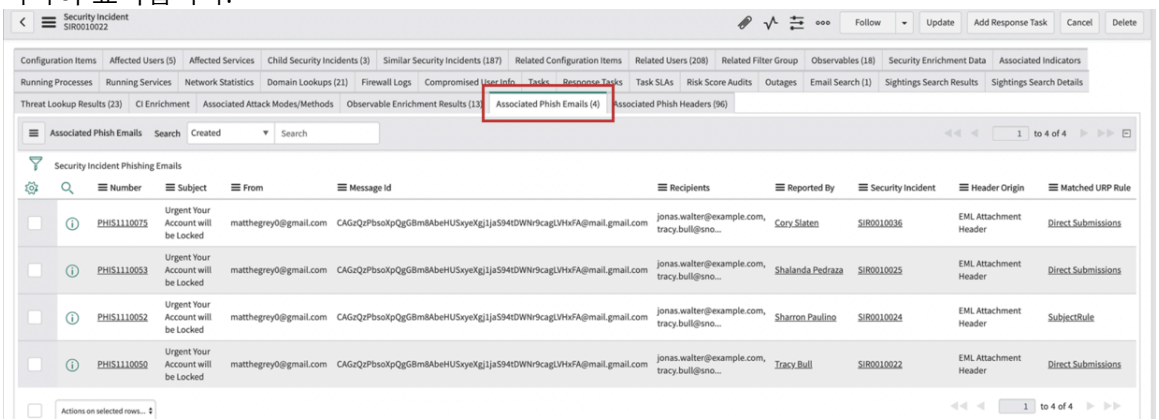
하위 보안 인시던트 탭을 클릭합니다. 적용된 집계 논리에 따라 상위 보안 인시던트와 연결된 하위 보안 인시던트 목록을 볼 수 있습니다. 추가된 모든 하위 기록에 대해 자동화된 시스템 활동이 상위 기록에 추가됩니다(작업 메모 섹션에서). 이렇게 하면 집계된 하위 기록에 대해 보안 분석가에게 알릴 수 있습니다.

주:
사용자가 보고한 피싱 속성 페이지에서 집계된 이메일 제출에 대한 하위 인시던트 생성 플래그가 예 로 설정된 경우에만 여기에서 하위 보안 인시던트를 볼 수 있습니다. 자세한 내용은 사용자가 보고한 피싱 속성 정의 문서를 참조하십시오.



관련된 피싱 이메일

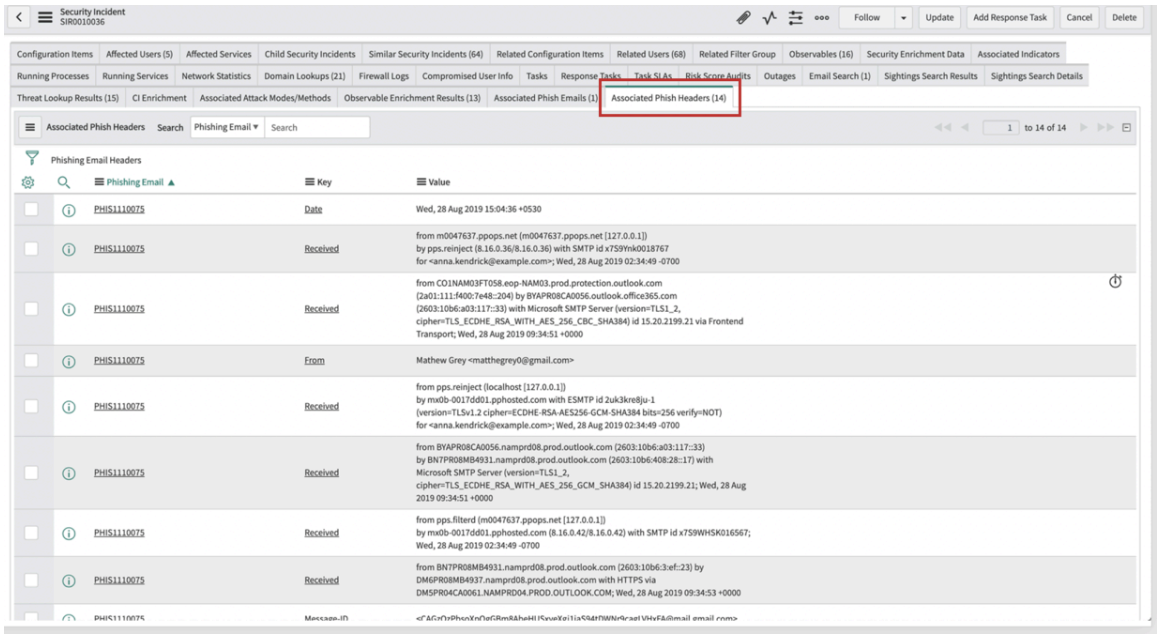
연결된 피싱 메일 탭을 클릭합니다. 상위 피싱 이메일 기록과 연결된 피싱 이메일 기록(중복 기록) 목록이 표시됩니다.



관련 피싱 이메일 헤더

연결된 피싱 메일 탭을 클릭합니다. 보안 인시던트의 일부로 캡처된 피싱 이메일 헤더 상세 정보가 표시됩니다. 상위 보안 인시던트로 집계된 모든 하위 기록 및 피싱 이메일 기록의 롤업된 헤더를 볼 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

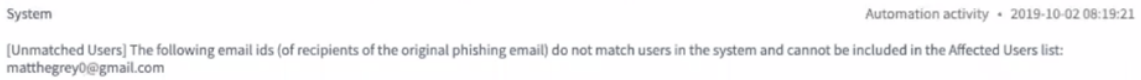


허용 목록 옵저버블

플로우가 사용자가 보고한 피싱 이메일을 보안 인시던트로 변환 실행되는 동안 보안 인시던트의 상태를 모니터링할 수 있습니다. 특정 옵저버블이 허용 목록 옵저버블로 표시되면 옵저버블 관련 목록에 추가되지 않습니다. 옵저버블을 허용 목록에 표시하여 중요한 상세 정보만 표시되도록 할 수 있습니다. 예를 들어 www.google.com 가 허용 목록으로 태그가 지정된 URL 중 하나이면 다음 시스템 메시지가 표시됩니다. 허용 목록 옵저버블을 사용하면 중요한 옵저버블만 모니터링됩니다.

일치하지 않는 사용자 캡처

피싱 이메일의 받는 사람 및 참조 목록에 있는 일부 이메일 ID는 조직의 사용자에게 속하지 않을 수 있습니다. 이러한 이메일 ID는 일치하지 않는 사용자로 분류되며 영향을 받는 사용자 관련 목록에 포함되지 않습니다. 일치하지 않는 사용자임을 나타내는 작업 메모가 표시됩니다.

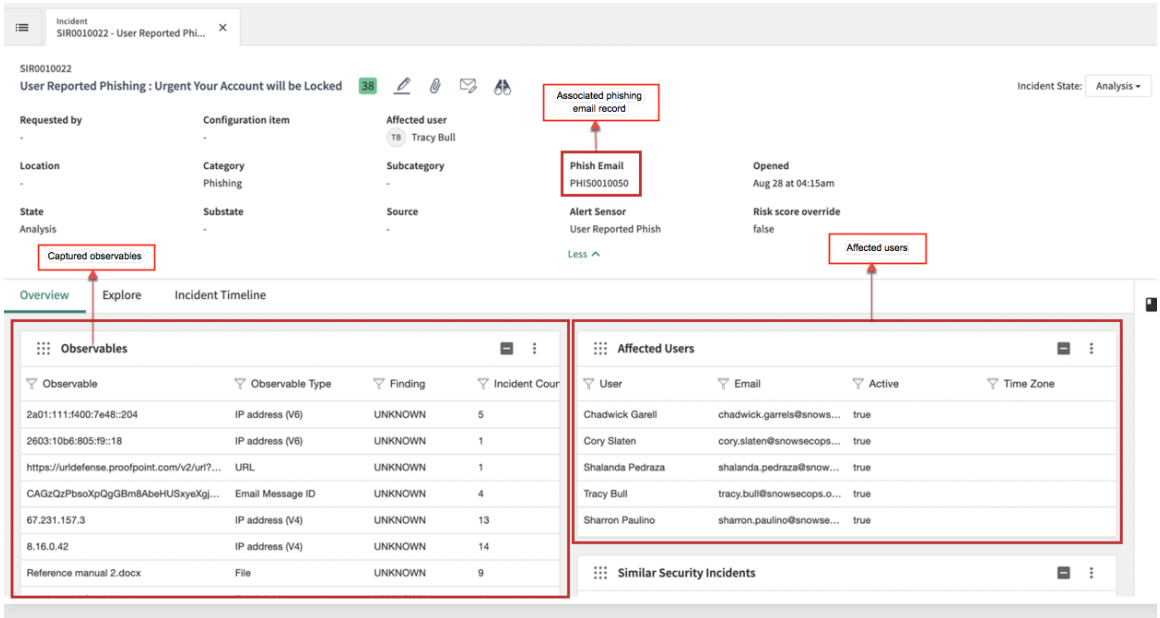


보안 분석가 작업 공간에서 사용자가 보고한 피싱

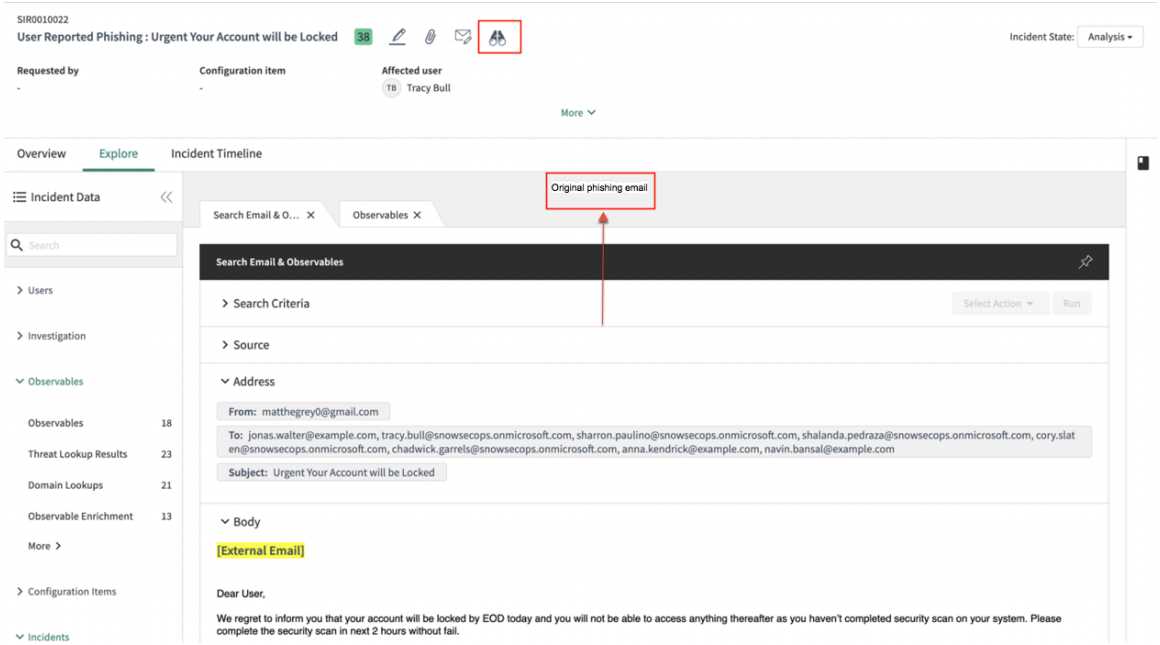
보안 분석가 작업 공간에서 피싱 이메일 기록과 연관된 보안 인시던트를 볼 수 있습니다.

다음으로 이동 보안 인시던트 〉 새 **UI**. 작업 공간이 별도의 브라우저 탭에서 열립니다. 피싱 이메일 기록과 연결된 보안 인시던트를 클릭하여 보안 인시던트를 확인합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

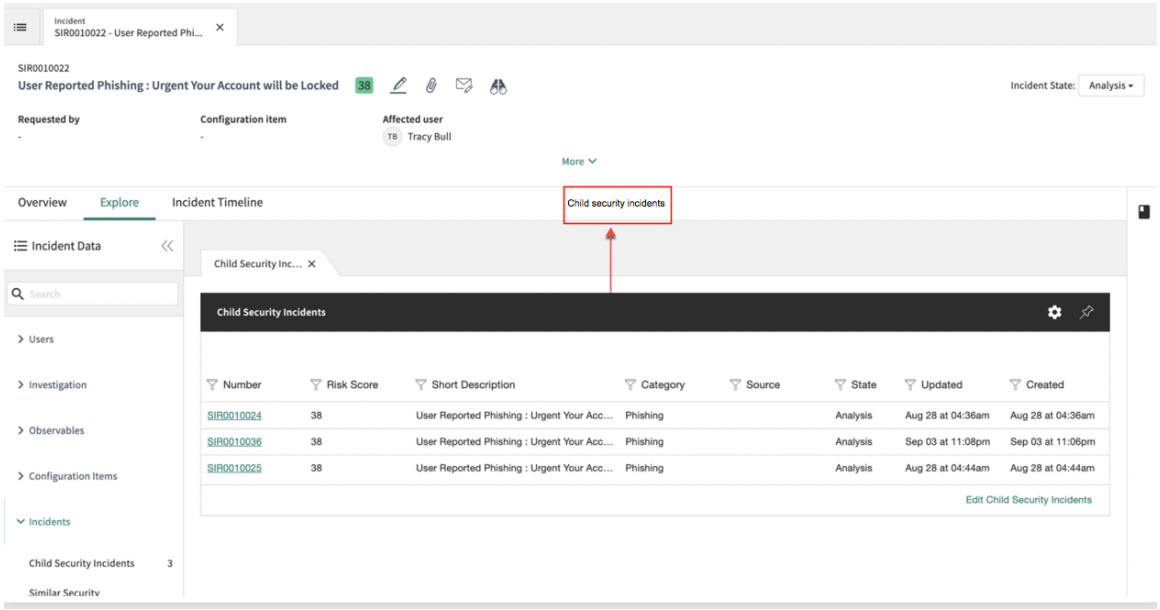


쌍안경 아이콘을 클릭합니다. 원래 피싱 이메일이 표시됩니다.

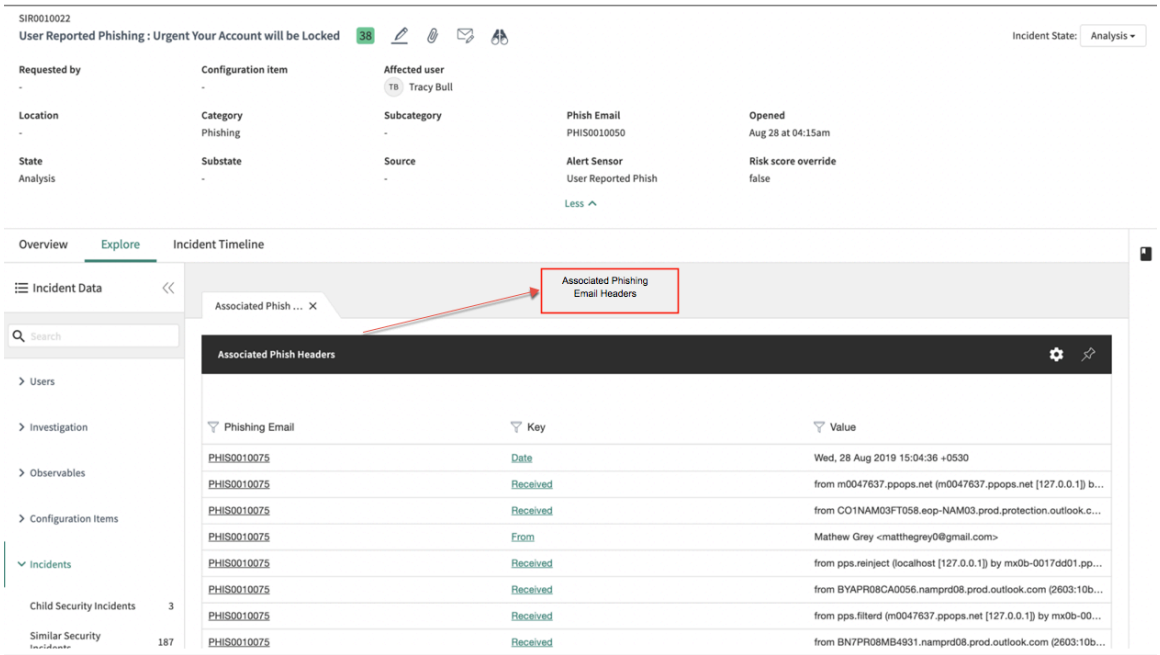


탐색 탭에서 인시던트 〉 하위 보안 인시던트.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

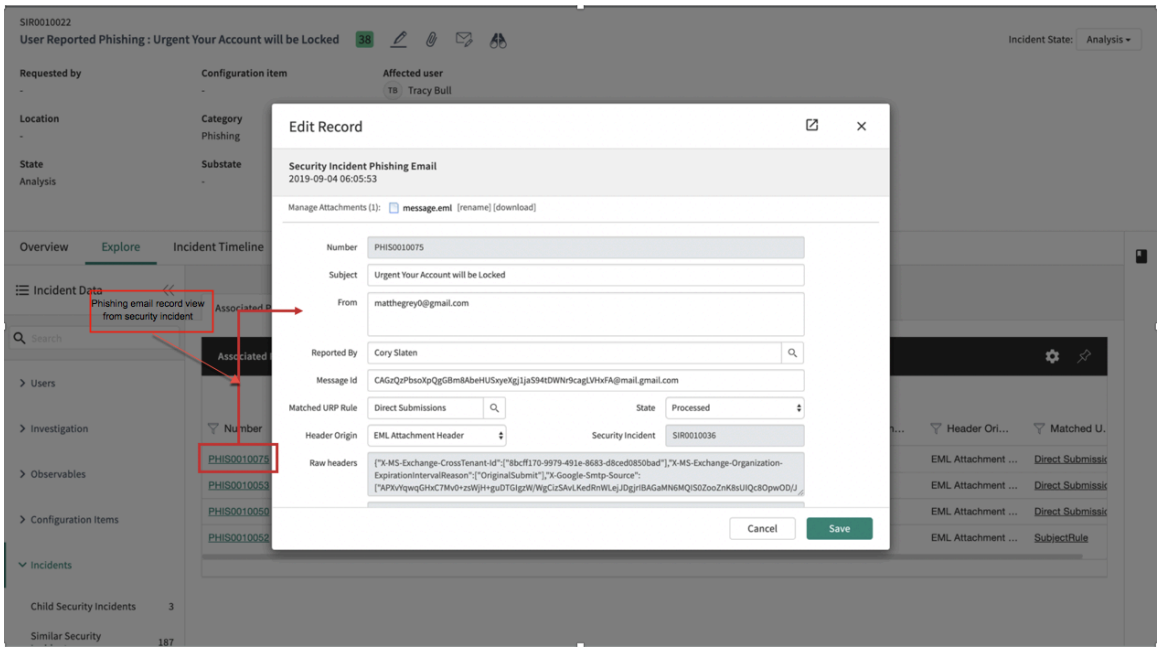


클릭 인시던트 〉 연결된 피싱 헤더 〉 . 상위 보안 인시던트로 집계된 모든 하위 기록 및 피싱 이메일 기록의 롤업된 헤더를 볼 수 있습니다.

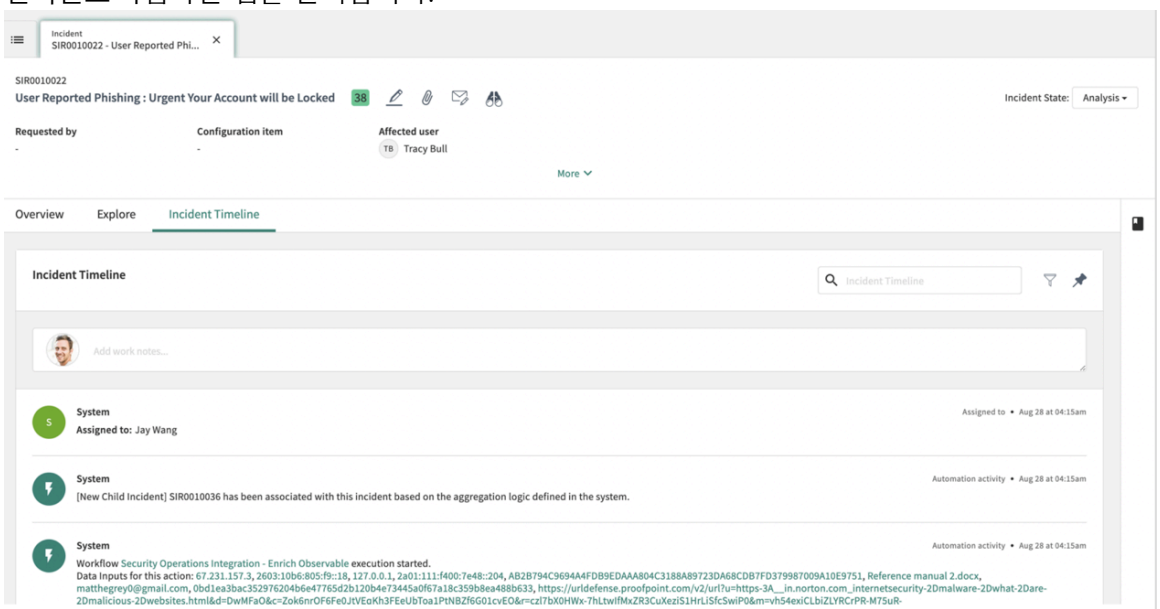


피싱 이메일 링크를 클릭하여 보안 인시던트와 관련된 피싱 이메일 기록을 봅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



인시던트 타임라인 탭을 클릭합니다.



강조 표시된 시스템 업데이트를 볼 수 있습니다.

- 중복 하위 기록이 식별되었습니다.
- 허용 목록 옵저버블입니다.
- 피싱 이메일을 받았지만 영향을 받는 사용자 목록에 속하지 않는 일치하지 않는 사용자입니다.

자주 묻는 질문

이 섹션에서는 향상된 사용자 보고 피싱 기능에 대한 몇 가지 질문과 대답을 다룹니다.

1. 새 Security Incident Response 스포크를 설치했지만 사용자가 보고한 피싱 인시던트를 볼 수 없습니다.

   사용자가 보고한 피싱 기능은 기본적으로 비활성화되어 있습니다.

   이 기능을 사용하려면 읽기 전용 사용자가 보고한 피싱 이메일을 보안 인시던트로 변환 플로우의 사본을 만들고 활성화한 후 사용해야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

2. 피싱 이메일을 수집하여 보안 인시던트로 전환하는 동안 피싱 이메일의 악성 링크와 첨부 파일을 처리하기 위해 어떤 예방 조치를 사용합니까?

   바이러스 백신 스캐너는 ServiceNow 이러한 악성 첨부 파일 및 링크를 검사합니다. 그러나 보안 분석가가 인시던트를 정확하게 보안 인시던트 응답 조사할 수 있도록 애플리케이션이 피싱 이메일의 일부인 모든 아티팩트를 캡처합니다. 그러나 사용자가 보고한 피싱 기능은 보안 분석가가 실수로 이러한 링크를 클릭하지 않도록 피싱 이메일의 악성 링크를 음소거합니다. 악성 첨부 파일과 관련하여 보안 분석가는 다운로드에 주의해야 합니다.

3. 보안 인시던트 보강을 위해 피싱 이메일에 포함된 악성 파일을 모두 캡처합니까?

   예, 피싱 이메일에서 모든 파일을 캡처합니다. 이러한 상세 정보는 파일 해시 형식으로 보안 인시던트 옵저버블의 일부로 사용할 수 있음을 볼 수 있습니다.

4. 조사를 위해 악성 파일과 피싱 이메일의 링크를 샌드박스 인스턴스로 전송합니까?

   현재 악성 파일 및 링크를 조사하기 위한 바로 사용 가능한 샌드박스 통합은 지원하지 않습니다.

5. 들어오는 중복 피싱 이메일 기록이 상위 보안 인시던트와 연결되는 기간을 정의하는 기간 또는 트리거가 있습니까?

   중복 피싱 이메일 기록은 활성 상위 보안 인시던트로만 집계됩니다. 상위 인시던트가 종결되거나 취소되면 들어오는 새로운 중복 피싱 이메일이 새 보안 인시던트로 생성됩니다. 그러나 이 시나리오에서는 새 보안 인시던트 내의 유사한 보안 인시던트 관련 목록에서 종결되거나 취소된 상위 보안 인시던트를 볼 수 있습니다.

   > **주:**
   > 이 동작은 플로우 디자이너를 사용하여 구성할 수 있습니다.

6. 사용자 피싱 신고 기능은 이메일 헤더 세부 정보를 캡처하기 위해 Microsoft Outlook **PhishAlarm** 플러그인(이전의 Wombat)만 사용할 수 있도록 지원합니까?

   사용자 보고 기능은 이메일 헤더를 구문 분석하도록 설계되었으며 RFC822 표준을 준수합니다. 따라서 **PhishAlarm** 플러그인(이전의 Wombat)과 마찬가지로 RFC822 표준을 기반으로 이메일 헤더를 캡처하는 다른 모든 Microsoft Outlook 플러그인이 지원됩니다.

보안 인시던트에서 기록 생성

보안 인시던트를 만들고 저장한 후에는 변경 요청(CHG), 인시던트(INC) 또는 문제(PRB) 기록을 만들 수 있습니다. 보안 인시던트에서 고객 서비스 케이스를 생성할 수도 있습니다.

보안 인시던트에서 변경, 인시던트 또는 문제 생성

보안 인시던트를 만들고 저장한 후에는 변경 요청(CHG), 인시던트(INC) 또는 문제(PRB) 기록을 만들 수 있습니다.

시작하기 전에
필요한 역할: sn.si_basic 이상

프로시저

1. 다음 방법 중 하나를 사용하여 보안 인시던트를 엽니다.
   - 다음으로 이동하여 기존 보안 인시던트를 엽니다. 보안 인시던트 > 미할당 > 인시던트을 클릭하고 보안 인시던트를 클릭합니다.
   - 다음으로 이동하여 보안 인시던트 생성 보안 인시던트 > 미할당 > 인시던트, 새로 만들기를 클릭하고 양식을 작성한 다음 기록을 저장합니다.
2. 보안 인시던트 헤더 막대를 마우스 오른쪽 버튼으로 클릭하고 다음 중 하나를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 변경 생성
- 인시던트 생성
- 문제 생성

주:
이 선택 항목은 팝업 속성(sn_vul.popup)이 활성화된 경우에만 적용됩니다. 이러한 버튼 중 하나를 클릭하면 변경, 인시던트 또는 문제를 생성하는 데 사용되는 보안 인시던트의 정보를 보여주는 미리 보기 창이 열립니다. 즉, 구성 항목, 해당 위치, 우선순위, 짧고 긴 설명이 여기에 해당합니다. 변경 요청을 생성하는 경우 우선순위, 간단한 설명 및 설명 필드를 편집할 수 있습니다. 인시던트를 생성하는 경우 영향, 긴급도, 간단한 설명 및 설명 필드를 편집할 수 있습니다. 관련 보안 인시던트 화면의 필드는 영향을 받지 않습니다.

3. 제출을 클릭하여 변경, 인시던트 또는 문제를 만듭니다.

보안 인시던트에서 고객 서비스 케이스 생성

보안 인시던트 응답 은 보안 인시던트를 (CS) 케이스에 고객 서비스 매핑하는 기본 필드 매핑과 함께 제공됩니다. 보안 인시던트에서 CS 케이스를 생성하고, 우선순위를 편집하고, 선택적 메모도 추가할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.basic 및 sn_customerservice_agent

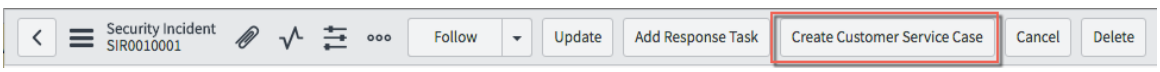
주:
고객 서비스 이 작업을 수행하려면 플러그인을 활성화해야 합니다.

프로시저

1. 보안 인시던트로 이동합니다.

2. CS 케이스를 추가할 보안 인시던트를 엽니다.

3. 상단 헤더에서 고객 서비스 케이스 생성을 클릭합니다.

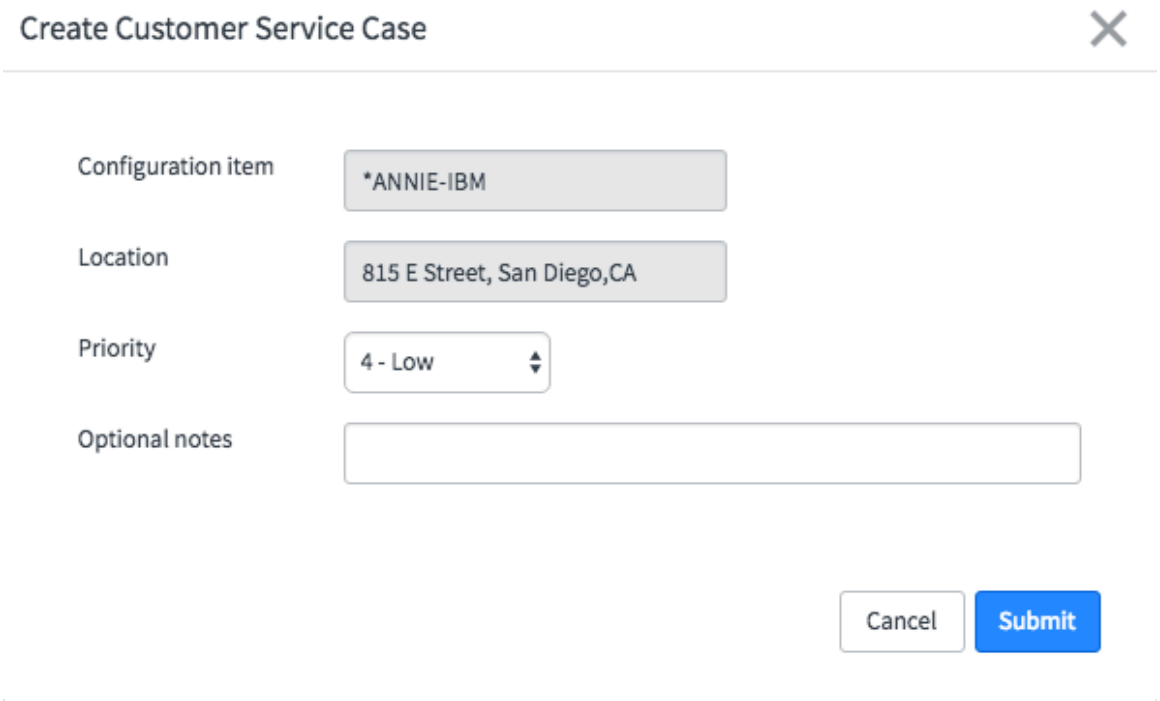


팝업 창은 필드 매핑을 기반으로 보안 인시던트의 정보로 미리 채워집니다.

4. 새 우선순위 를 선택하고 선택적 메모를 추가할 수 있습니다.

주:
우선순위 필드는 기본 설정을 덮어씁니다. 선택적 메모가 인시던트에 추가됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



5. 제출을 클릭합니다.
   CS 케이스가 생성되어 보안 인시던트의 고객 서비스 케이스 관련 목록에 표시됩니다.
6. CS 케이스 링크를 클릭하여 케이스에 대한 후속 조치를 취할 수 있습니다.

관련 정보

고객 서비스 케이스 관리

보안 케이스에 보안 인시던트 추가

보안 인시던트에 더 높은 수준의 분석이 필요하다고 판단되면 새 케이스 또는 기존 케이스에 추가합니다.

시작하기 전에

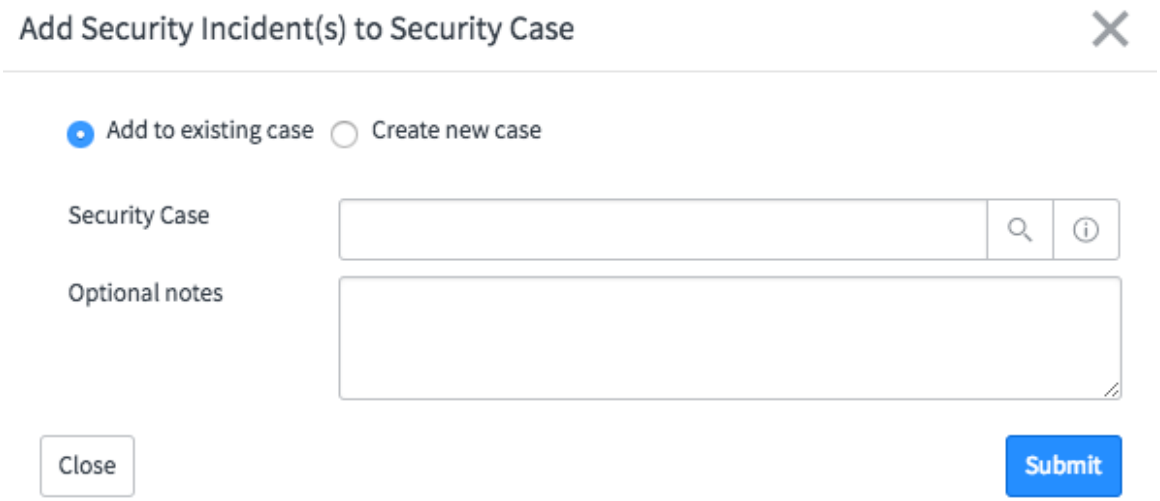
위협 인텔리전스 를 사용하려면 보안 케이스 관리플러그인을 활성화해야 합니다.

필요한 역할: sn_si.admin, sn_ti.case_user_write

프로시저

1. 을 클릭하여 에스컬레이션이 필요한 보안 인시던트로 이동합니다. 보안 인시던트 〉 인시던트 〉 나에게 할당됨을 클릭하고 보안 인시던트를 엽니다.
2. 보안 케이스에 추가 관련 링크를 클릭합니다.
   보안 케이스에 보안 인시던트 추가 대화 상자가 열립니다.

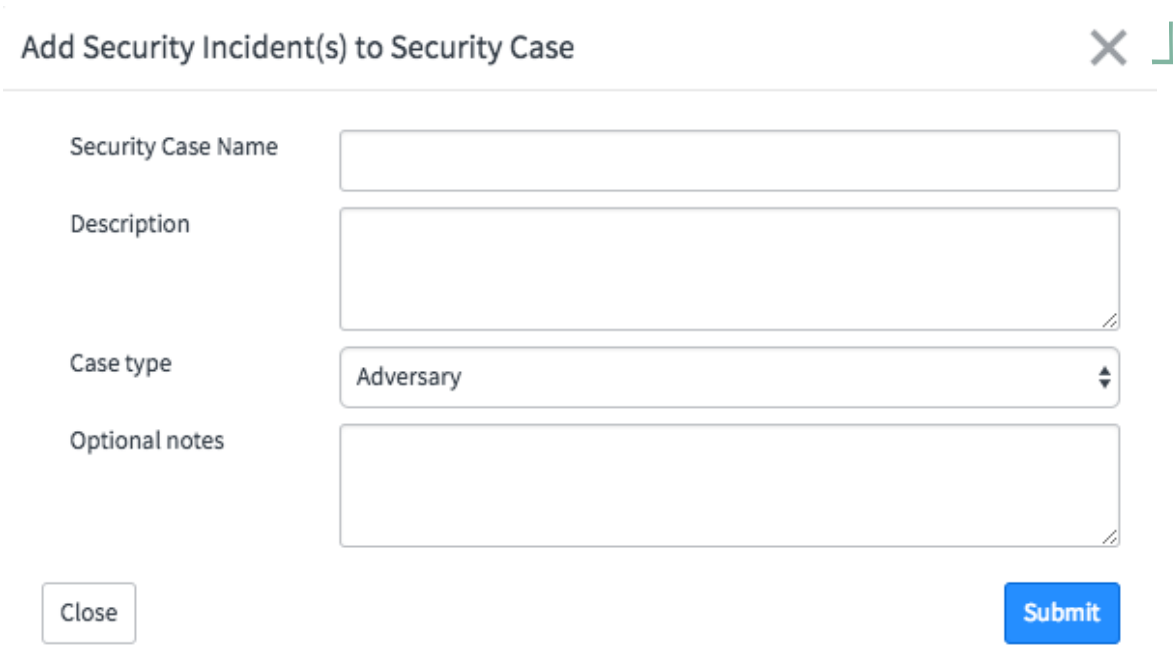
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



3. 이 보안 인시던트를 추가하려는 케이스가 할당되어 있는 경우 필드에 적절한 정보를 입력한 다음 제출을 클릭합니다.

필드	설명
보안 케이스	보안 케이스를 선택합니다.
선택적 메모	필요한 경우 케이스 분석가에게 도움이 될 만한 추가 메모를 입력합니다.

4. 하나 이상의 케이스가 할당되었지만 새 케이스를 만들고 보안 인시던트를 할당하려면 새 케이스 생성을 클릭하여 추가 필드를 표시합니다.



주:
할당된 케이스가 없는 경우 위의 화면이 먼저 열립니다.

5. 필드에 적절하게 입력합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
보안 케이스 이름	새 보안 케이스의 이름을 입력합니다.
설명	케이스에 대한 설명을 입력합니다.
케이스 유형	조사 중인 케이스의 유형을 선택합니다.
선택적 메모	필요한 경우 케이스 분석가에게 도움이 될 만한 추가 메모를 입력합니다.

6. 제출을 클릭합니다.
   보안 인시던트의 맨 위에 새 케이스에 대한 링크와 함께 메시지가 나타납니다.

관련 정보

Security Case Management

응답 작업 생성

보안 인시던트가 생성되면 대응 작업을 생성하여 보안 문제에 대응하기 위해 수행할 별도의 작업을 추적할 수 있습니다.

시작하기 전에

필요한 역할: sn_si.basic

프로시저

1. 적절한 위치로 이동하여 작업을 생성할 보안 인시던트를 엽니다.
   예:
   - 할당된 보안 인시던트를 기반으로 응답 작업을 생성하려면 다음을 선택합니다. 보안 인시던트 > 인시던트 > 나에게 할당됨.
   - 팀에 할당된 보안 인시던트를 기반으로 응답 작업을 생성하려면 다음을 선택합니다. 보안 인시던트 > 인시던트 > 팀에 할당됨 > 인시던트.
   - 할당되지 않은 보안 인시던트를 기반으로 응답 작업을 생성하려면 다음을 선택합니다. 보안 인시던트 > 인시던트 > 미할당 인시던트.
2. 응답 작업을 추가할 보안 인시던트를 엽니다.
3. 양식 헤더에서 대응 작업 추가 버튼을 클릭합니다.

   주:
   다른 작업을 생성하려면 인시던트 관련 목록에서 작업 탭을 클릭합니다.

4. 양식의 필드에 적절히 입력합니다.

   보안 인시던트

필드	설명
보안 태그 선택	보안 태그를 설정하고 활성화한 경우 하나 이상의 태그를 선택하여 기록에 메타데이터를 추가하거나 응답 작업의 민감도를 지정할 수 있습니다. 보안 태그를 설정하거나 활성화하지 않은 경우에는 이 드롭다운 목록이 표시되지 않습니다.
번호	[읽기 전용] 자동으로 생성된 보안 인시던트 응답 번호입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
상위	〔읽기 전용〕 관련 보안 인시던트의 수입니다.
구성 항목	보안 문제의 영향을 받는 구성 항목(자원)입니다.
영향을 받는 사용자	보안 문제의 영향을 받는 사람입니다.
우선순위	이 작업이 수행되는 시기를 결정하는 데 사용되는 우선순위입니다.
상태	보안 응답 작업의 현재 상태입니다. 작업 생성 시 이 필드는 기본적으로 초안으로 설정됩니다.
기술	이 작업을 수행하는 데 필요한 기술입니다. 잠금 아이콘을 클릭하고 필요한 기술을 선택합니다. 선택을 완료한 후 잠금 아이콘을 다시 클릭합니다.
할당 그룹	할당된 작업자가 선택되는 할당 그룹입니다.
담당자	작업을 수행하도록 할당된 개인입니다.
간단한 설명	작업에 대한 설명입니다 보안 인시던트 응답 .
설명	선택한 작업에 대한 설명입니다.
보안 메모	암호화되어 고객에게 표시되지 않는 작업 메모입니다.
작업 메모	고객에게 표시되지 않는 작업 메모입니다.
추가 의견	고객에게 표시하려는 코멘트입니다.

5. 입력을 완료했으면 제출을 클릭합니다.

   주:
   작업을 생성한 보안 인시던트 응답 후에는 응답 작업 모듈에서 다음 애플리케이션 중 하나를 사용하여 작업을 볼 수 있습니다.

   - 이(가) 나에게 할당되었습니다.
   - 팀에 할당됨.
   - 열린 작업 표시
   - 모든 작업 표시
   - 미할당 작업입니다.

사용자가 보고한 피싱에 대한 예측 인텔리전스 관리

사용자 보고 피싱에 대한 예측 인텔리전스 기능은 사용자가 보고한 피싱 이메일을 분류하고 우선순위를 지정하는 데 중요한 솔루션을 제공합니다.

이 섹션에서는 다음 사항에 대해 설명합니다.

- 사용자 신고 피싱에 대한 예측 인텔리전스
- 필수 구성요소 및 플러그인
- 사용자 보고 피싱에 대한 최종 평가 결과 생성
- 사용자 신고 피싱에 대한 예측 인텔리전스 문제 해결

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용자 신고 피싱에 대한 예측 인텔리전스

이 기능은 보안 분석가가 사용자가 보고한 피싱 이메일을 분류하고 우선순위를 지정하는 데 도움이 됩니다.

예측 인텔리전스 프레임워크는 데이터 결과를 예측, 추천 및 구성하도록 시스템을 교육하는 솔루션을 제공합니다. 예측 인텔리전스에 대한 자세한 내용은 다음 문서를 참조하십시오 Predictive Intelligence. 이 프레임워크를 사용하면 사용자가 보고한 피싱 이메일이 의심스러운지 또는 합법적인지 여부를 자동으로 예측하는 모델을 빌드할 수 있습니다.

보안 분석가는 사용자가 보고한 과거 피싱 보안 인시던트 데이터(보안 인시던트 종결 코드를 통해 캡처된 이메일 헤더, 이메일 본문 및 분류 결과)를 사용하여 들어오는 사용자가 보고한 피싱 제출을 추가 분류가 필요한 제출(의심스러울 수 있음)과 합법적인 제출로 분류하도록 시스템을 교육할 수 있습니다.

보안 분석가는 수신 이메일을 자동으로 분류하여 인시던트 큐의 우선 순위를 쉽게 지정하고 무엇보다도 조직에 위험을 초래할 가능성이 있는 인시던트에 집중할 수 있으며 가양성일 가능성이 매우 높은 이메일에 대한 노력을 줄일 수 있습니다. 또한 예측 결과는 분류에 대한 신뢰도 점수를 제공하여 세분화된 우선순위 지정을 가능하게 합니다.

필수 구성요소 및 플러그인

사용자가 보고한 피싱에 예측 인텔리전스를 사용하려면 다음 애플리케이션을 설치해야 합니다

플러그인 이름	최소 버전
보안 인시던트 응답	9.0.1 또는 10.0.2
예측 인텔리전스	Orlando 버전
사용자 신고 피싱에 대한 예측 인텔리전스	10.0.2

주:
Security Incident Response 10.4에서 사용할 수 있는 새로운 개선 사항은 다음과 같습니다.

- 모델 교육을 위해 사용자 지정 필드에서 종결 코드를 선택하는 기능.
- 모델 빌드 후 예측을 명시적으로 활성화하는 기능입니다.
- 결정 테이블을 사용하여 사용자가 보고한 피싱 제출에 대한 최종 판정을 생성하는 기능입니다. (보안 운영 스포크 10.3.0 필요)

새로운 개선 사항을 사용하려면 다음 애플리케이션을 업그레이드해야 합니다.

플러그인 이름	로 업그레이드
보안 인시던트 응답	10.0.4
사용자 신고 피싱에 대한 예측 인텔리전스	10.3.1

신규 및 업데이트된 테이블

- sn_sir_ml_urp_config(신규): URP ML 애플리케이션에 대한 구성을 포함합니다.
- sn_sir_ml_urp_feature(신규): sn_si_phishing 이메일 테이블에서 추출한 레코드입니다.
- sn_sir_ml_urp_feature_import(신규): 과거 피싱 이메일 데이터를 업로드하는 데 사용됩니다.
- sn_si_incident(업데이트됨): 다음과 같은 새 필드가 추가되었습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 예측 수락됨
- 예측 결과
- 신뢰 점수

- **Script Includes**
  - URPMLUtil: 구성을 검색하고, 예측 작업을 실행하고, 예측 프로세스를 추적합니다.
  - URPMLProcessor: sn_si_phishing_email 테이블에서 데이터를 추출하고 처리합니다.
  - URPMLAction: 예측 결과를 수락하기 위해 플로우를 실행합니다.

사용자 보고 피싱에 대한 최종 평가 결과 생성

이제 보안 인시던트 대응 팀은 예측 인텔리전스 및 위협 보강 통합의 결과를 기반으로 사용자가 보고한 피싱 기록에 대한 최종 판정을 내릴 수 있습니다.

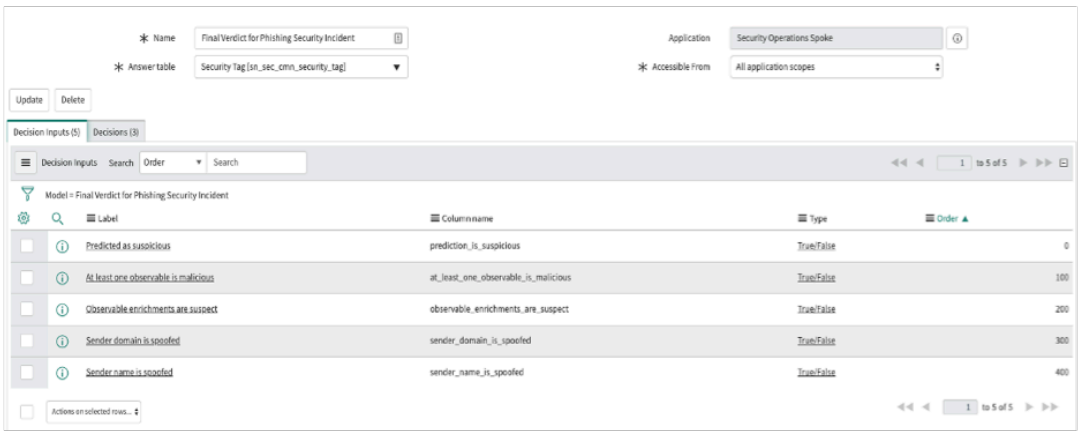
이 최종 판정 생성은 결정 테이블 구성을 통해 활성화되고 플로우 내에서 활용됩니다.

필수 조건

나열된 필수 구성요소 및 플러그인 모든 플러그인이 설치되었는지 확인합니다.

다음으로 이동 피싱용 예측 인텔리전스 〉 최종 평가 결과 〉 피싱 보안 인시던트에 대한 최종 평가 결과.

결정 입력 탭에는 최종 판정에 도달하기 위해 평가된 다양한 조건이 표시됩니다.

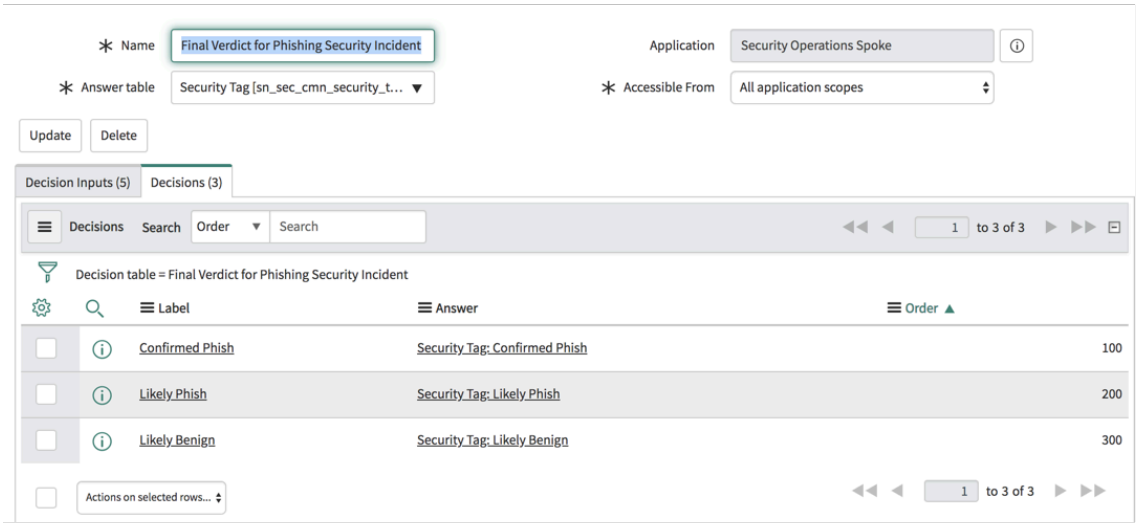


기본 시스템에서 사용할 수 있는 조건은 다음과 같습니다.

- 의심스러운 것으로 예측: 예측 인텔리전스가 피싱 이메일을 의심스러운 것으로 분류한 경우.
- 하나 이상의 옵저버블은 악성입니다. 보안 인시던트에 관련된 옵저버블(예: URL, 도메인, IP, 해시)이 위협 인텔리전스 소스에 의해 악성 으로 분류된 경우입니다.
- 옵저버블 보강이 의심스럽다: 옵저버블에 대한 보강(예: 피싱 도메인 등록의 최신성, 피싱 도메인 등록의 국가)이 의심스러운 것으로 간주되는 경우.
- 발신자 도메인이 스푸핑된 경우: 피싱 클라이언트의 이메일 도메인이 신뢰할 수 있는 도메인을 스푸핑한 것으로 의심되는 경우.
- 보낸 사람 이름이 스푸핑됨: 피싱 사용자의 이메일 주소가 조직의 신뢰할 수 있는 직원을 스푸핑하는 것으로 의심되는 경우.

결정 탭에는 지정된 보안 인시던트에 대해 도달할 수 있는 최종 판정 옵션이 표시됩니다.

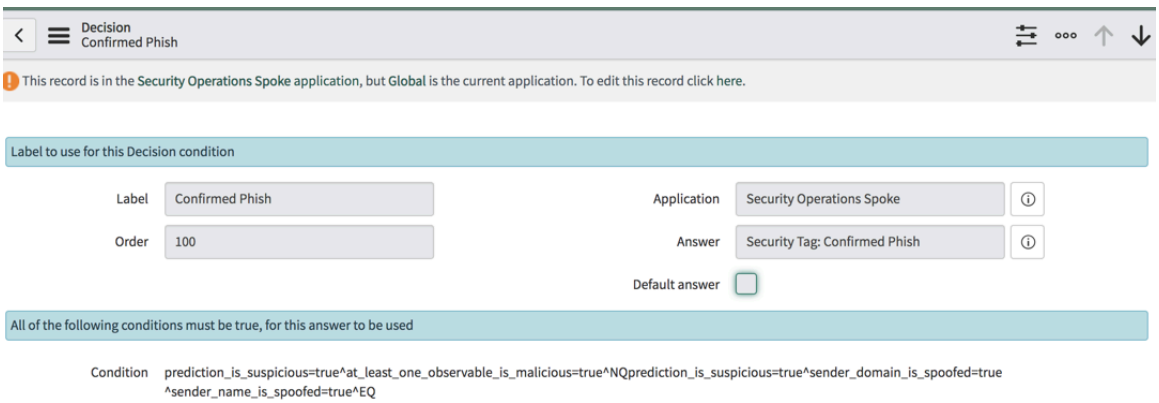
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



기본 시스템에서 다음 결정을 사용할 수 있습니다.

- 확인된 피싱: 조건으로 인해 확인된 피싱 이메일이라는 최종 평결이 나온 경우입니다.
- 피시 가능성: 조건으로 인해 잠재적인 피싱 시도로 최종 판정이 내려진 경우입니다.
- 양성 가능성: 조건이 양성 제출로 최종 평결로 이어졌을 때.

각 최종 판정 옵션에 대해 평가된 조건을 볼 수 있습니다. 조건을 보려면 레이블 링크를 클릭합니다.



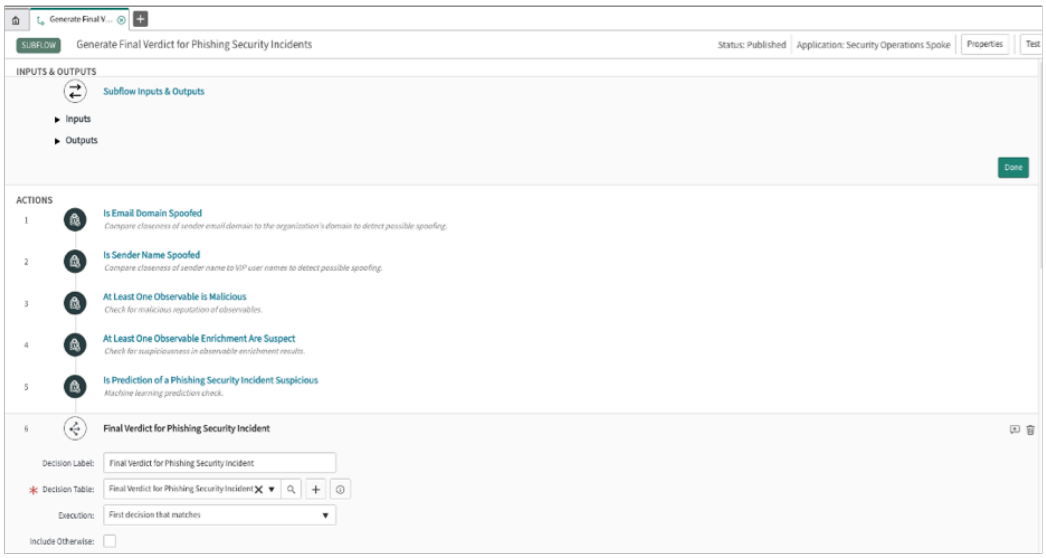
기본 시스템과 함께 제공되는 결정 테이블을 사용자 지정하거나 고유한 결정 테이블을 생성할 수 있습니다. 이 결정 테이블은 보안 인시던트 응답 플레이북에서 활용할 수 있습니다. 피싱 보안 인시던트에 대한 최종 평가 결과 생성 하위 플로우는 기본 시스템에서 사용할 수 있습니다. 이 하위 플로우는 피싱 보안 인시던트에 대한 최종 평가 결과를 자동으로 생성하고 해당 결정에 따라 보안 태그를 적용합니다. 이 하위 플로우를 자동화된 피싱 플레이북의 일부로 포함할 수 있습니다.

이 하위 플로우에 대한 입력은 다음과 같습니다.

- incident_id: 피싱 보안 인시던트의 시스템 ID입니다.
- c_level_names: 피싱 공격에서 스푸핑되었을 가능성이 있는 쉼표로 구분된 이름 목록(예: 조직의 임원 이름)입니다.
- trusted_domains: 신뢰할 수 있는 전자 메일 도메인의 쉼표로 구분된 목록입니다.
- enrichment_keywords: 보강 결과에서 옵저버블의 악성도를 나타내는 쉼표로 구분된 키워드 목록입니다.
- sender_email(선택 사항): 피싱 이메일 발신자의 이메일 주소입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 플로우의 출력은 피싱으로 확인됨, 피싱일 가능성이 높음 또는 양성일 가능성이 있음일 수 있습니다.



사용자 신고 피싱에 대한 예측 인텔리전스 문제 해결

이 섹션에서는 몇 가지 일반적인 문제 시나리오에 대해 설명합니다.

- 문제: Predictive Intelligence 구성을 수정할 수 없습니다.

  해결 방법: 그렇게 할 수 있는 권한이 있는지 확인합니다. 임계치를 수정하려면 ml_admin 역할을 가진 사용자로 로그인해야 합니다. 일부 시나리오에는 더 높은 권한이 필요할 수 있습니다(예: 학습 데이터 제한을 수정해야 하는 경우). 이러한 시나리오의 경우 고객 지원에 도움을 요청해야 합니다.

- 문제: 모델 교육에 실패했습니다.

  해결 방법: ML 스케줄러의 URL이 설정되었는지 확인합니다. 다음으로 이동 시스템 속성 〉 모든 속성 `glide.shared_service_scheduler.url` 속성이 구성되었는지 확인합니다.

- 문제: 보안 인시던트에 대한 예측 결과를 사용할 수 없습니다.

  용액:

  - 예측 URL이 `glide.prediction_service.url` 시스템 속성에 설정되어 있는지 확인하고 데이터 센터가 URL과 일치하는지 확인합니다.
  - 사용자가 보고한 피싱 이메일 예측 예약된 작업이 활성 상태인지 확인합니다.

사용자가 보고한 피싱에 대한 예측 인텔리전스 구성

사용자가 보고한 피싱 이메일을 식별하도록 모델을 구성하고 준비합니다.

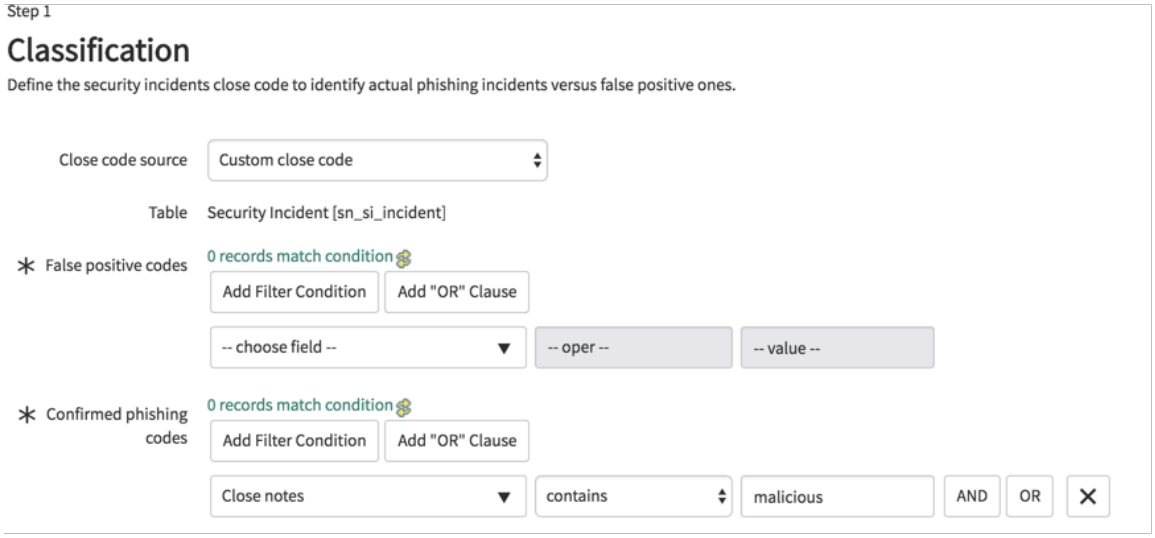
시작하기 전에
필요한 역할: ml_admin

프로시저

1. 다음으로 이동 모두 〉 피싱용 예측 인텔리전스 〉 구성.
2. 구성의 1단계에 있는 종결 코드 소스 목록에서 다음 옵션 중 하나를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 기본 종결 코드: 교육 모델에서 악성 이메일과 합법적인 이메일을 식별하는 데 사용해야 하는 기본 보안 인시던트 종결 코드를 지정하려면 이 옵션을 선택합니다. 잠금 아이콘을 클릭하고 하나 이상의 긍정 오류 코드 또는 확인된 피싱 코드를 선택합니다.
- 사용자 지정 종결 코드: 기존 인시던트 응답 절차의 일부로 사용될 수 있는 사용자 지정 필드에서 종결 코드를 정의하려면 사용자 지정 종결 코드 옵션을 선택합니다. 종결 코드를 정의하려면 보안 인시던트 테이블에서 필드를 선택하고 하나 이상의 필터 조건을 지정합니다.



3. 2단계에서는 모델을 학습시키는 데 사용할 수 있는 기록 데이터를 임포트합니다.
이력 데이터를 임포트할 데이터 소스를 선택합니다. 다음과 같을 수 있습니다.

- 사용자가 보고한 피싱 이메일 테이블: 기록 데이터로 임포트할 수 있는 기록 수를 볼 수 있습니다. 이 옵션을 선택하고 임포트를 클릭합니다.
- 사용자 지정 데이터 소스: 기록 데이터 기록이 포함된 단일 형식의 CSV 파일을 첨부할 수 있습니다. 파일을 선택하고 〔가져오기〕를 클릭합니다.

> **주:**
> 임포트하는 CSV 파일에는 다음 헤더가 포함되어야 합니다.
>
> - 레이블
> - 머리글
> - 본문 텍스트
>
> 각 레코드는 CSV 파일의 레이블 열에 악의적이거나 합법적인 태그를 포함해야 합니다.

데이터 가져오기를 중지하려면 **Cancel** Import(임포트 취소)를 클릭합니다. 임포트 프로세스가 취소되고 지금까지 임포트한 모든 기록이 삭제됩니다.

4. 기록 데이터를 임포트한 후 링크를 클릭하여 페이지를 새로 고칩니다.
그런 다음, 더 많은 교육 데이터를 임포트하거나 다음 단계를 계속할 수 있습니다.

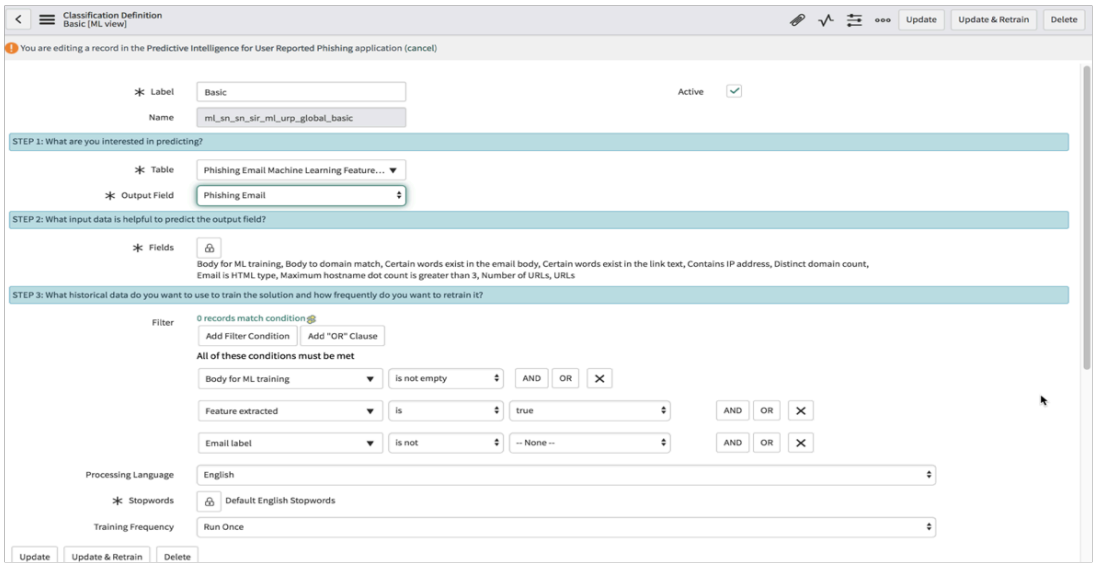
5. 3단계에서는 교육에 사용할 수 있는 레코드 수가 최소 임계치 요구 사항을 충족하는지 확인합니다.

> **주:**
> 최대 및 최소 교육 기록 수에 대한 기본값이 표시됩니다. 이러한 임계치는 플랫폼 머신 러닝 속성 페이지에서 수정할 수 있습니다. 도움이 필요하면 고객 지원에 문의하십시오.

6. 학습 데이터가 충분하면 모델 학습을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

아래 화면에서 교육에 대한 입력을 업데이트할 수 있습니다.



7. 수정할 수 있는 예측 입력은 다음과 같습니다.

- 무엇을 예측하고 싶습니까?
- 출력 필드 예측에 유용한 입력 데이터는 무엇입니까?
- 솔루션 교육에 사용하려는 이전 데이터는 무엇이며, 원하는 재교육 빈도는 무엇입니까?

이러한 입력의 기본값이 표시됩니다. 이러한 항목을 수정하고 다음 중 하나를 클릭할 수 있습니다.

- 업데이트: 교육 모델 정의를 업데이트합니다.
- 업데이트 및 재교육: 교육 모델 정의를 업데이트하고 모델을 다시 교육합니다(모델 교육 기능 트리거).

8. 마지막으로 모델 교육을 완료했으면 예측 활성화 확인란을 클릭합니다.
이제 해당 모델을 사용하여 보고된 모든 사용자 피싱 기록에 대한 예측이 제공됩니다. 사용자가 보고한 피싱 기록에 대한 예측 제공을 중지하려면 예측 활성화 확인란의 선택을 취소하고 비활성화를 클릭합니다.

보안 분석가 할당

관리 구성 화면의 SIR 설정에 따라 보안 분석가를 보안 인시던트에 수동으로 할당하거나, 워크플로우를 사용하여 자동으로 할당하거나, 자동 할당을 사용하여 자동으로 할당할 수 있습니다.

수동 분석가 할당

사용자 또는 SIR 애플리케이션에서 보안 인시던트를 생성하거나 보안 응답 작업을 생성할 때마다 보안 분석가를 수동으로 할당하도록 관리 구성 화면을 구성할 보안 인시던트 응답 수 있습니다.

보안 인시던트 또는 응답 작업을 자동으로 할당할 수 없는 경우 관리 구성 화면을 설정하여 SIR 보안 분석가를 수동으로 할당할 수 있습니다. 요청을 완료하는 데 필요한 보안 분석가 수가 제한되어 있거나 자동으로 할당하고 싶지 않은 경우에 적합합니다.

워크플로우 기반 보안 분석가 할당

사용자 또는 SIR 애플리케이션이 보안 인시던트 또는 보안 응답 작업을 생성할 때마다 선택한 워크플로우를 사용하여 보안 분석가를 할당하도록 관리 구성 화면을 구성할 보안 인시던트 응답 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 인시던트 관리 구성 화면에서 워크플로우를 사용하여 각 보안 인시던트 또는 보안 응답 작업에 분석가를 할당하도록 선택할 수 있습니다. 이 옵션은 보안 문제를 해결하기 위해 사용자 지정 프로세스를 사용하거나 자동화할 수 있는 프로세스가 있는 조직에 적합합니다.

자동 보안 분석가 할당

사용자 또는 SIR 애플리케이션이 보안 인시던트 또는 보안 응답 작업을 생성할 때마다 보안 분석가를 자동으로 할당하도록 관리 구성 화면을 구성할 보안 인시던트 응답 수 있습니다. 자동 할당을 사용하면 조직의 필요에 따라 분석가가 보안 인시던트에 자동으로 할당되는 기준을 정의할 수 있습니다.

에이전트 평가에 따라 에이전트 자동 할당

자동 할당이 활성화되고 보안 인시던트 또는 응답 작업이 생성되면 다음 동작이 발생합니다.

- 사용 가능한 보안 분석가는 구성에 정의된 기준에 따라 평가됩니다.
- 적절한 보안 분석가가 작업에 자동으로 할당됩니다.
- 작업이 할당됨 상태로 이동됩니다.

기술, 위치, 시간대 또는 그룹 적용 범위와 같은 조건 집합을 두 개 이상 고려하도록 구성이 설정된 경우 보안 분석가는 가중치 속성 설정 및 기타 기준에 따라 평가됩니다. 이러한 구성 설정은 선택적 속성에 따라 에이전트를 자동 할당하는 데 도움이 됩니다. 계산된 등급은 보안 인시던트 또는 응답 작업에 가장 적합한 에이전트를 결정하는 데 사용됩니다. 등급 기반 방법의 조합은 애플리케이션 구성 화면에서 사용할 수 있습니다.

작업을 생성하면 사용 설정된 각 선택 기준 유형의 등급이 사용 가능한 각 에이전트에 대해 계산됩니다. 총 등급이 가장 높은 에이전트는 자동 할당 대상으로 간주됩니다.

자동 할당 가중치 속성에 대한 설정은 보안 인시던트 〉 관리 〉 속성, 등급 계산에 포함됩니다.

이 값을 통해 조직에 더 중요한 자동 할당 선택 기준의 우선순위를 정할 수 있습니다. 1(덜 중요)과 10(중요) 사이의 우선순위 값을 설정합니다.

가중치 지정 속성이 에이전트 등급에 어떤 영향을 미치는지에 관한 예는 여러 선택 기준을 사용하는 에이전트 자동 할당를 참조하십시오.

On-Call Scheduling

당직 일정 관리 애플리케이션을 사용하면 문제가 발생할 때 이를 해결할 전담 지원 팀 구성원들을 활용할 수 있습니다. 당직 일정, 명단 교대 및 에스컬레이션 정책을 설정하고 그룹에 대한 알림을 에스컬레이션하고 에스컬레이션의 현재 연락처를 설정할 수 있습니다. 애플리케이션은 할당되고 사용할 수 있는 지원 그룹 구성원을 식별합니다(예: 인시던트 할당 시). 자세한 내용은 On-Call Scheduling 문서를 참조하십시오. Security Incident Response의 당직 일정 관리도 동일한 방식으로 작동합니다.

위치를 사용한 에이전트 자동 할당

에이전트는 사용자 기록의 홈 위치와 작업 위치를 기반으로 자동으로 할당될 수 있습니다.

위치별 자동 할당은 에이전트의 자동 선택이 에이전트의 위치를 고려하는 구성 옵션이 활성화된 경우에 수행됩니다.

작업(보안 인시던트 또는 응답 작업)이 생성되면 작업 위치에 가장 가까운 에이전트가 작업에 고려됩니다. 위치만 고려하도록 애플리케이션을 구성하면 가장 가까운 에이전트에게 작업이 자동으로 할당됩니다.

작업이 생성되면 에이전트 위치가 다음 범위와 비교하여 각 에이전트 위치 등급을 결정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

위치 등급 계산

에이전트에서 작업까지의 거리(마일)	평가 등급
0에서 0.1	1
0.11에서 0.5	0.9
0.51에서 5	0.7
5.1에서 10	0.5
10.1에서 20	0.4
20.1에서 30	0.3
30.1에서 40	0.2
40.1에서 100	0.1
〉100	0

애플리케이션이 기술, 시간대 또는 일정과 같은 다른 선택 기준을 사용하도록 구성된 경우 모든 선택 기준의 등급에 가중치가 적용되고 요약됩니다. 전체 등급이 가장 높은 에이전트가 작업에 자동으로 할당됩니다. 자세한 내용은 여러 선택 기준을 사용하는 에이전트 자동 할당 문서를 참조하십시오.

기술을 사용한 에이전트 자동 할당

에이전트는 기술과 작업 수행에 필요한 기술에 따라 자동으로 할당될 수 있습니다. 을 사용하여 사용자 기록에 기술 할당 기술 〉 사용자.

작업에 대한 에이전트의 자동 선택에서 에이전트에게 기술 구성 옵션이 모두 또는 일부여야 하는 경우 기술별 자동 할당을 수행할 수 있습니다.

기술이 포함된 작업이 자동으로 할당되면 에이전트의 기술은 작업을 수행하는 데 필요한 기술과 비교됩니다. 등급은 기술 구성 옵션을 기준으로 계산됩니다. 이 옵션을 일부로 설정하면 가장 유사한 기술을 보유한 에이전트가 자동으로 작업에 할당됩니다. 이 옵션이 모두로 설정된 경우에는 필요한 모든 기술을 보유한 에이전트만 고려됩니다. 작업을 수행하는 데 필요한 모든 기술을 보유한 에이전트가 없으면 아무도 자동으로 할당되지 않습니다.

기술 등급은 다음과 같이 계산됩니다.

Skills_agent/Skills_task

위치:

- Skills_agent는 작업에 필요한 기술과 일치하는 에이전트가 보유한 기술의 수입니다.
- Skills_task는 작업에 필요한 기술의 총수입니다.

예를 들어 다음과 같이 작업에 네 가지 기술이 필요한데 에이전트 A가 이 중에서 세 가지를 보유하고 있고 에이전트 B는 두 가지를 보유하고 있다고 합시다.

- 에이전트 A 스킬 등급 = 3/4 또는 0.75
- 에이전트 B 스킬 등급 = 2/4 또는 0.5

애플리케이션이 위치 또는 시간대와 같은 다른 선택 기준을 사용하도록 구성된 경우 모든 선택 기준의 등급에 가중치가 적용되고 요약됩니다. 전체 등급이 가장 높은 에이전트가 작업에 선택됩니다. 자세한 내용은 여러 선택 기준을 사용하는 에이전트 자동 할당 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시간대를 사용한 에이전트 자동 할당

사용자 기록에 정의된 시간대와 작업의 시간대에 따라 에이전트를 자동으로 할당할 수 있습니다.

에이전트의 자동 선택이 작업 구성 옵션의 시간대를 고려하는 경우 시간대별 자동 할당을 수행할 수 있습니다.

작업이 생성되면 작업 시간대와 가장 가까운 시간대의 에이전트가 작업에 고려됩니다. 시간대만 고려하도록 애플리케이션을 구성한 경우 시간대가 같은 에이전트만 작업을 자동으로 할당할 수 있습니다.

주:
에이전트와 작업의 시간대가 올바르게 설정되어야 합니다.

작업이 생성되면 에이전트는 다음 수식을 사용하여 작업의 시간대 및 에이전트의 시간대를 기준으로 등급이 매겨집니다.

1 - 〔abs(Task_tz – Agent_tz) ÷ 12〕

위치:

- abs는 절대값을 계산하는 수학적 함수입니다.
- Task_tz는 작업 및 GMT의 시간대 간 오프셋입니다.
- Agent_tz는 에이전트와 GMT의 시간대 간 오프셋입니다.

예를 들어 뉴욕 시(GMT-4)에서 작업을 생성하였는데 이 작업을 수행할 수 있는 에이전트가 로스앤젤레스(GMT-7)와 프랑스 파리(GMT+1)에 각각 한 명이라고 합시다.

로스앤젤레스에 있는 에이전트의 등급은 다음과 같이 계산됩니다.

1 - abs((-4) - (-7)) ÷ 12 or 0.75

파리에 있는 에이전트의 등급은 다음과 같이 계산됩니다.

1 - abs((-4) - (+1)) ÷ 12 or 0.58

따라서 작업의 자동 할당이 시간대만을 기준으로 하는 경우 로스앤젤레스에 있는 에이전트에게 할당됩니다.

애플리케이션이 기술 또는 위치와 같은 다른 선택 기준을 사용하도록 구성된 경우 모든 선택 기준의 등급에 가중치가 적용되고 합산됩니다. 전체 등급이 가장 높은 에이전트가 작업에 선택됩니다. 자세한 내용은 여러 선택 기준을 사용하는 에이전트 자동 할당 문서를 참조하십시오.

그룹 범위 영역을 사용한 에이전트 자동 할당

사용자 기록에 정의된 그룹 범위 영역에 따라 에이전트를 자동으로 할당할 수 있습니다.

여러 선택 기준을 사용하는 에이전트 자동 할당

작업이 생성되면 에이전트 등급이 계산됩니다. 자세한 내용은 다음을 참조하십시오.

- 위치를 사용한 에이전트 자동 할당
- 기술을 사용한 에이전트 자동 할당
- 시간대를 사용한 에이전트 자동 할당

자동 할당은 다음 계산을 기반으로 합니다.

(Criteria_1 등급 x Criteria_1 가중치) + (Criteria_2 등급 x Criteria_2 가중치) + (Criteria_3 등급 x Criteria_3 가중치) / 사용되는 기준 유형의 수:

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용된 기준 유형의 수 = 사용된 위치, 기술 및 시간대 설정에 따라 1, 2 또는 3으로 결정됩니다.

다음 예에서는 위치 및 기술에 근거하여 에이전트 자동 할당을 계산합니다. 이 예는 다음과 같은 가정에 기반을 둔 것입니다.

- 애플리케이션에 대해 에이전트의 자동 선택은 에이전트의 위치를 고려함 구성 옵션이 설정되어 있습니다.
- 애플리케이션에 대해 작업에 대한 에이전트의 자동 선택을 사용하려면 에이전트가 기술을 보유해야 함 구성 옵션이 설정되어 있습니다.
- 애플리케이션에 대해 기술 가중치 속성이 10으로 설정되어 있습니다.
- 애플리케이션에 대해 위치 가중치 속성이 5로 설정되어 있습니다.
- 에이전트 A와 B가 작업을 수행할 수 있으며 이 작업에는 네 가지 특정 기술이 필요합니다.
- 에이전트 A 위치는 작업 현장에서 5마일 떨어져 있으며 필요한 4가지 기술 중 3가지를 보유하고 있습니다.
- 에이전트 B의 위치는 현장에서 1/4 마일 떨어져 있으며 필요한 두 가지 기술을 보유하고 있습니다.

에이전트에 대한 자동 할당은 다음 계산을 사용합니다. `[(## ## x ## ###) + (## ## x ## ###)]/ 2`

- 에이전트 A에 대한 자동 할당 계산은 `[(0.7 x 0.5) + (0.75 x 1)]/ 2 = 0.55`입니다.
- 에이전트 B에 대한 자동 할당 계산은 `[(0.9 x 0.5) + (0.5 x 1)]/ 2 = 0.475`입니다.

이 예에서 에이전트 A는 작업에 자동으로 할당됩니다.

용 프로세스 마이닝 작업 공간 보안 인시던트 응답

프로세스 마이닝은 보안 인시던트 감사 로그를 스캔하고 여러 번의 재할당, 장기간의 보류 시간, 보안 인시던트의 비활성 기간 등 비효율성에 기여하는 요인을 식별합니다. 조직은 이 정보를 사용하여 비효율성을 해결할 수 있습니다.

프로세스 마이닝을 사용하면 다음과 같은 보안 인시던트 개선 기회를 파악할 수 있습니다.

프로세스 마이닝을 통한 기회

기회	설명
두 개 이상의 할당 그룹 변경이 있는 인시던트	할당 그룹이 두 번 이상 변경된 인시던트
SIRT(최대 반복 횟수는 2)	
인시던트가 높은 우선순위로 에스컬레이션되는 데 5시간 이상 걸렸습니다.	5시간 후에 우선순위가 높은 우선순위로 에스컬레이션된 인시던트입니다.
분석하는 데 5시간 이상 걸린 인시던트	5시간 이상 분석 상태였던 인시던트
30분 이내에 분석되는 인시던트	30분 미만 동안 분석 상태에 있었던 인시던트.
검토(최대 반복 횟수는 2)	두 번 동안 검토 상태로 이동된 인시던트.
근절(최대 반복 횟수는 2임)	두 번 근절 상태로 이동한 인시던트입니다.

프로세스 마이닝 콘텐츠 팩은 보안 인시던트 응답 보안 인시던트에 대해 미리 정의된 프로세스 모델 정의를 포함하는 사전 구축된 프로젝트를 추가합니다. 프로젝트를 생성하려면 을 참조하십시오 보안 인시던트에 대한 프로세스 마이닝 프로젝트 생성.

주:
에서 보안 인시던트 응답프로세스 마이닝을 사용하려면 컨텐츠 팩을 다운로드하여 설치합니다. 자세한 내용은 Content pack for Security Incident Response 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 인시던트에 대한 프로세스 마이닝 프로젝트 생성

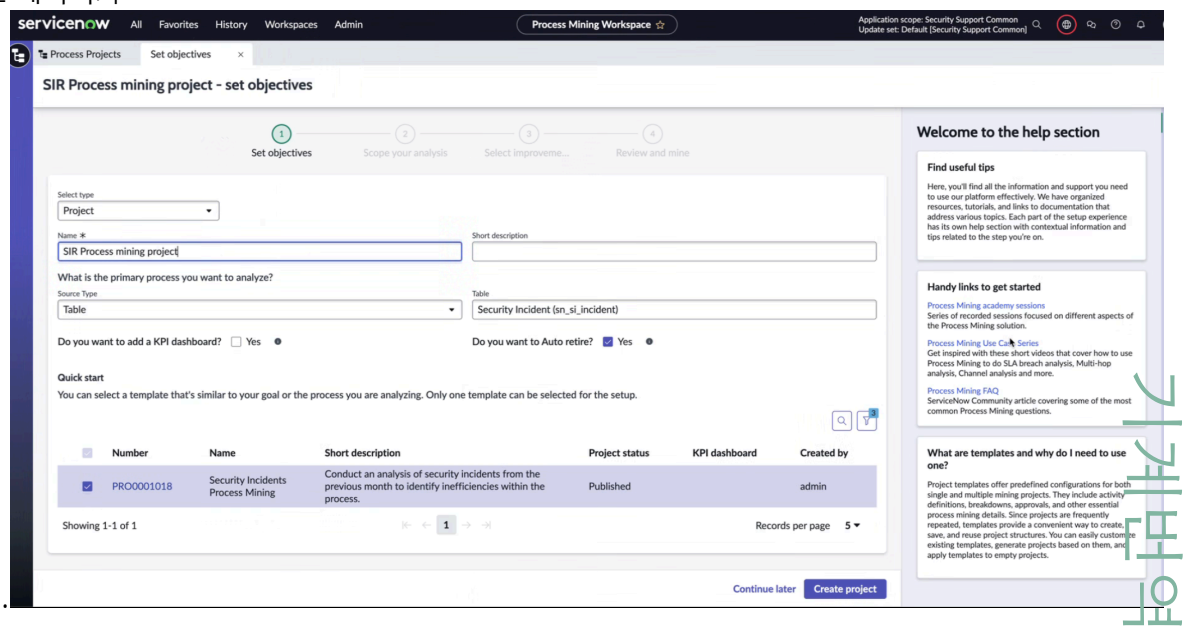
콘텐츠 팩의 사전 구축 프로세스 모델 정의를 사용하여 프로세스 마이닝 작업 공간에서 프로젝트를 생성하여 보안 인시던트 기록의 감사 로그를 살펴보고 보안 인시던트 수명주기의 비효율성을 식별합니다.

시작하기 전에

필요한 역할: sn_process_optimization_analyst 및 sn_si_read

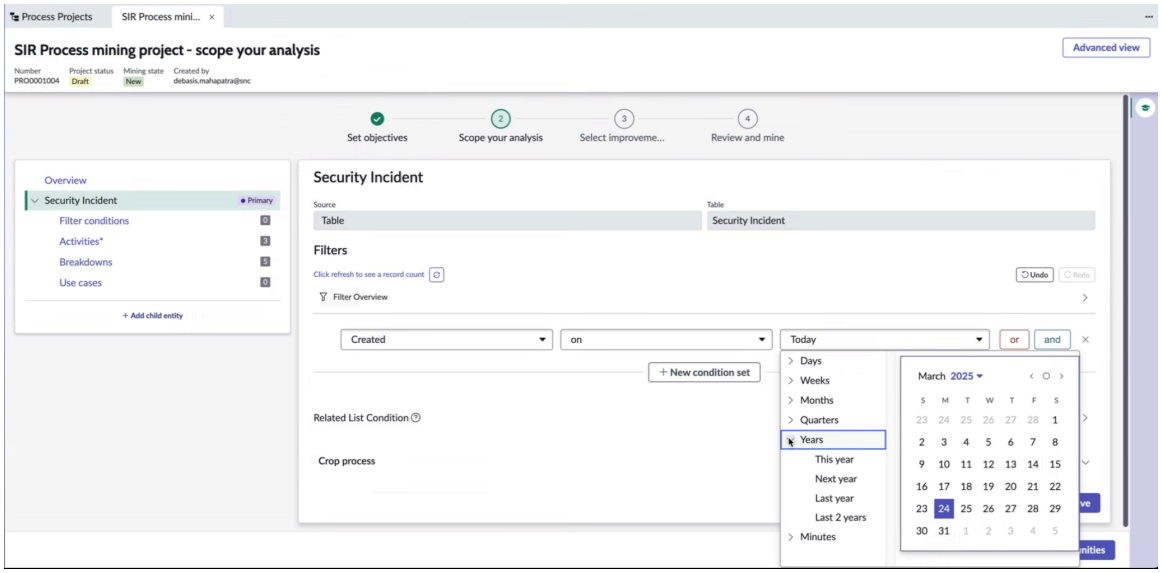
프로시저

1. 다음으로 이동 모두 〉 작업 공간 〉 프로세스 마이닝 작업 공간.
2. 새 프로젝트 만들기를 선택합니다.
   단계 목표 페이지가 열립니다.



3. 이름에 프로세스 마이닝 프로젝트 이름을 입력합니다.
4. 옵션: 짧은 설명에 프로젝트에 대한 짧은 설명을 추가합니다.
5. 소스 유형을 테이블로 선택합니다.
6. 테이블에서## ####(sn_si_incident)를 선택합니다.
7. 기본 템플릿을 선택한 다음, 프로젝트 만들기를 선택합니다.
   구성된 모든 설정이 포함된 프로젝트 대시보드가 나타납니다.
8. 분석 범위에 해당하는 편집( ) 아이콘을 선택하고 필터를 구성하여 마이닝할 기록 수를 설정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



9. 개선 기회 선택을 선택하고 보안 인시던트에 대한 개선 사항을 구성합니다.
   개선 기회 목록이 표시됩니다. 개선 기회 구성에 대한 자세한 내용은 다음 문서를 참조하십시오 Working with improvement opportunities .
10. 검토 및 마이닝을 선택한 다음, 프로젝트 마이닝을 선택합니다.
11. 샘플 마이닝 또는 전체 마이닝을 선택합니다.
12. 확인 및 마이닝을 선택하여 마이닝을 시작합니다.
    마이닝이 시작되고 마이닝 상태가 표시됩니다.

보안 인시던트에 대한 프로세스 마이닝 사용 사례

다음 프로세스 마이닝 사용 사례는 보안 인시던트를 해결하는 동안 비효율성을 식별하는 데 사용할 수 있는 다양한 분석 방법을 제공합니다.

멀티홉 분석

보안 인시던트가 다른 팀에 여러 번 재할당되면 해결이 지연될 수 있습니다. 이러한 보안 인시던트에 대한 재할당 이유와 인시던트가 장기간 지연되는 위치를 분석하여 전반적인 효율성을 개선할 수 있습니다.

다음은 더 긴 경로를 사용한 보안 인시던트 목록을 가져오는 예시 단계입니다.

1. 다음으로 이동 작업 공간 〉 프로세스 마이닝 작업 공간.
2. 할당 그룹을 선택합니다.
3. 프로젝트를 열고 분석가 워크벤치로 이동합니다.

   마이닝된 프로세스 최적화 프로젝트를 열면 기본적으로 분석가 워크벤치가 열립니다.
4. 변형 분석을 선택합니다.
5. 필터( ) 아이콘을 선택하고 다음과 유사한 필터를 설정합니다.
   - 평균 단계 수보다 큰 단계입니다.
   - 최소 기록 수보다 크고 더 긴 경로를 사용한 기록입니다.

   주:
   요구 사항에 따라 값을 구성할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

6. 적용을 선택합니다.

   필터 조건과 일치하는 모든 기록이 나타납니다. 기록을 선택하여 기록의 종결 경로를 봅니다.

7. 기록을 선택한 다음 경로 표시를 선택합니다.

   기록에 의해 통과된 경로가 나타납니다. 이 경로를 사용하여 인시던트가 예상보다 오래 지연된 단계를 식별할 수 있습니다.

SLA 위반 분석

프로세스 마이닝을 사용하여 특정 SLA(서비스 수준 계약)를 위반한 보안 인시던트를 분석할 수 있습니다.

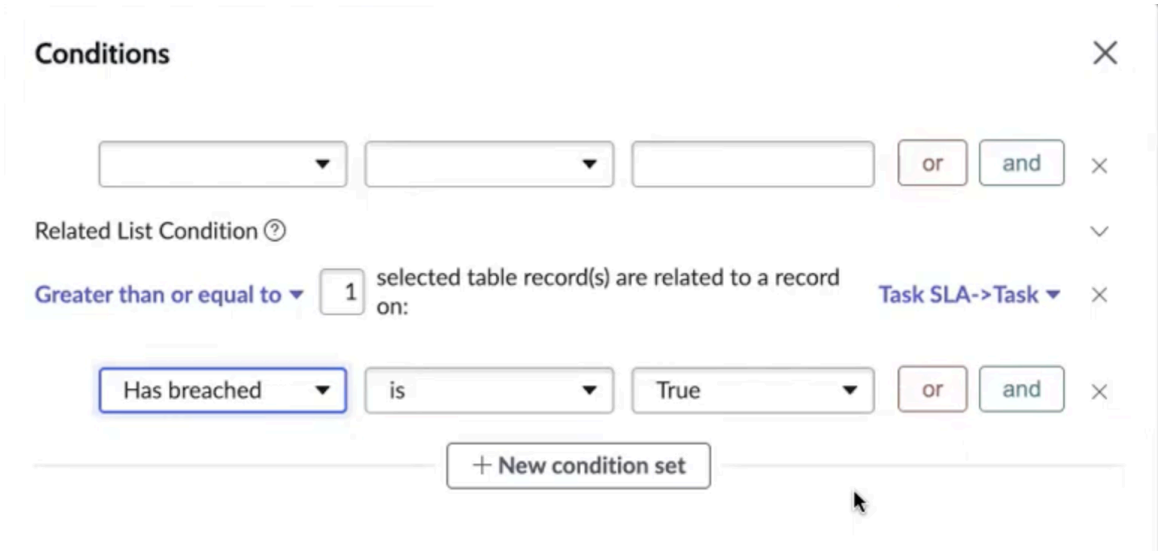
다음은 SLA를 위반한 보안 인시던트 목록을 가져오는 단계 예시입니다.

1. 다음으로 이동 작업 공간 〉 프로세스 마이닝 작업 공간.
2. 프로젝트를 열고 분석가 워크벤치로 이동합니다.

   마이닝된 프로세스 최적화 프로젝트를 열면 기본적으로 분석가 워크벤치가 열립니다.

3. 고급 필터에서 조건을 선택합니다.
4. 관련 목록 상태에 해당하는 화살표를 선택합니다.
5. 다음과 유사한 조건을 설정합니다.
   - 선택 목록을 사용하여 ## SLA 테이블을 선택합니다.
   - 크거나 같음 필드의 값을 1로 설정합니다.
   - 위반됨 값을 **True**로 설정합니다.
   - 특정 SLA를 위반한 보안 인시던트를 식별하려면 **SLA** 정의 필터를 설정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



6. 적용을 선택합니다.

   조건과 일치하는 모든 기록이 나타납니다. 분석할 기록의 경로를 보려면 기록을 선택합니다.

우선순위 분석

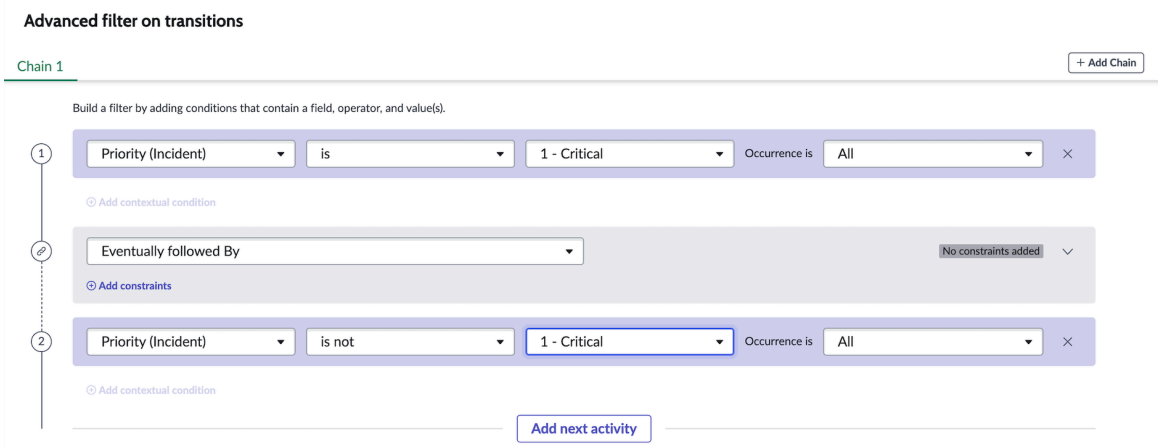
프로세스 마이닝을 사용하여 보안 인시던트에 대한 기존 우선순위 할당 프로세스를 검토하고 개선할 수 있습니다.

다음은 우선순위가 수정된 보안 인시던트 목록을 가져오는 단계 예시입니다.

1. 다음으로 이동 작업 공간 〉 프로세스 마이닝 작업 공간.
2. 프로젝트를 열고 분석가 워크벤치로 이동합니다.

   마이닝된 프로세스 최적화 프로젝트를 열면 기본적으로 분석가 워크벤치가 열립니다.

3. 우선순위를 선택합니다.
4. Advanced filters(고급 필터)에서 Transitions(전환)를 선택합니다.
5. 전환 시 고급 필터에서 다음을 구성합니다.
   a. 우선 순위 설정은 1 - 중요입니다.
   b. 궁극적으로 다음으로 이어짐 선택
   c. 우선순위가 1 - 중요가 아닙니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

6. 모든 체인 적용을 선택합니다.

맵에는 우선순위 1이 할당되고 나중에 우선순위가 낮아진 모든 보안 인시던트가 표시됩니다.

병목현상 분석

프로세스 마이닝을 사용하여 보안 인시던트의 상태 전환을 검토할 수 있습니다. 이 분석은 일반적이지 않은 전환과 그로 인해 발생하는 시간 지연을 식별합니다.

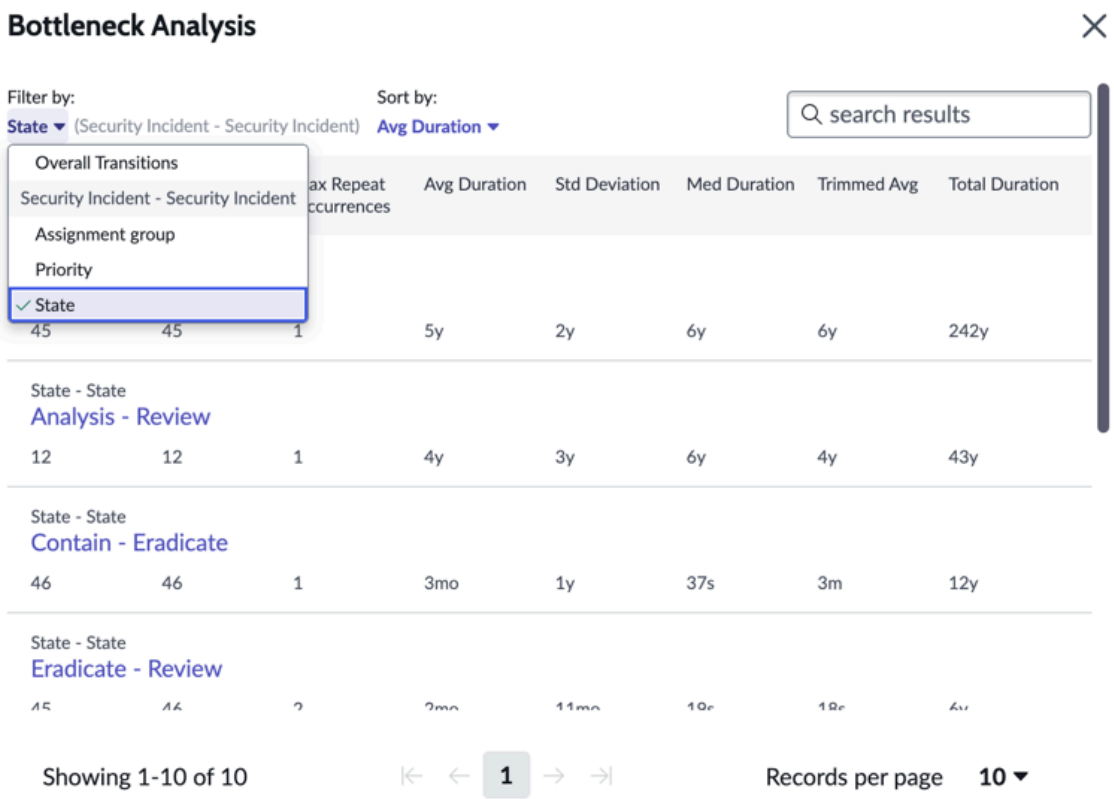
다음은 병목현상 분석을 수행하는 단계 예시입니다.

1. 다음으로 이동 작업 공간 〉 프로세스 마이닝 작업 공간.
2. 프로젝트를 열고 분석가 워크벤치로 이동합니다.

마이닝된 프로세스 최적화 프로젝트를 열면 기본적으로 분석가 워크벤치가 열립니다.

3. 모델 옵션**(Model Options)**에서 병목 분석**(Bottleneck Analysis)**을 선택합니다.

화면에 보안 인시던트에 대한 상태 전환이 표시됩니다.



4. 병목 현상 전환을 식별하려면 필터 기준을 선택합니다. 또는 검색 창을 사용하여 병목 현상 전환을 검색합니다. 예를 들어, 종결 상태에서 다른 상태로 이동된 인시던트를 식별하려면 "종결 " 또는 "종결 -"을 사용합니다.

해결보다 시작하는 데 오랜 시간이 걸림

프로세스 마이닝을 사용하여 초안 상태에 도달하는 데 시간이 오래 걸리지만 비교적 짧은 시간 내에 종결된 인시던트를 검토할 수 있습니다.

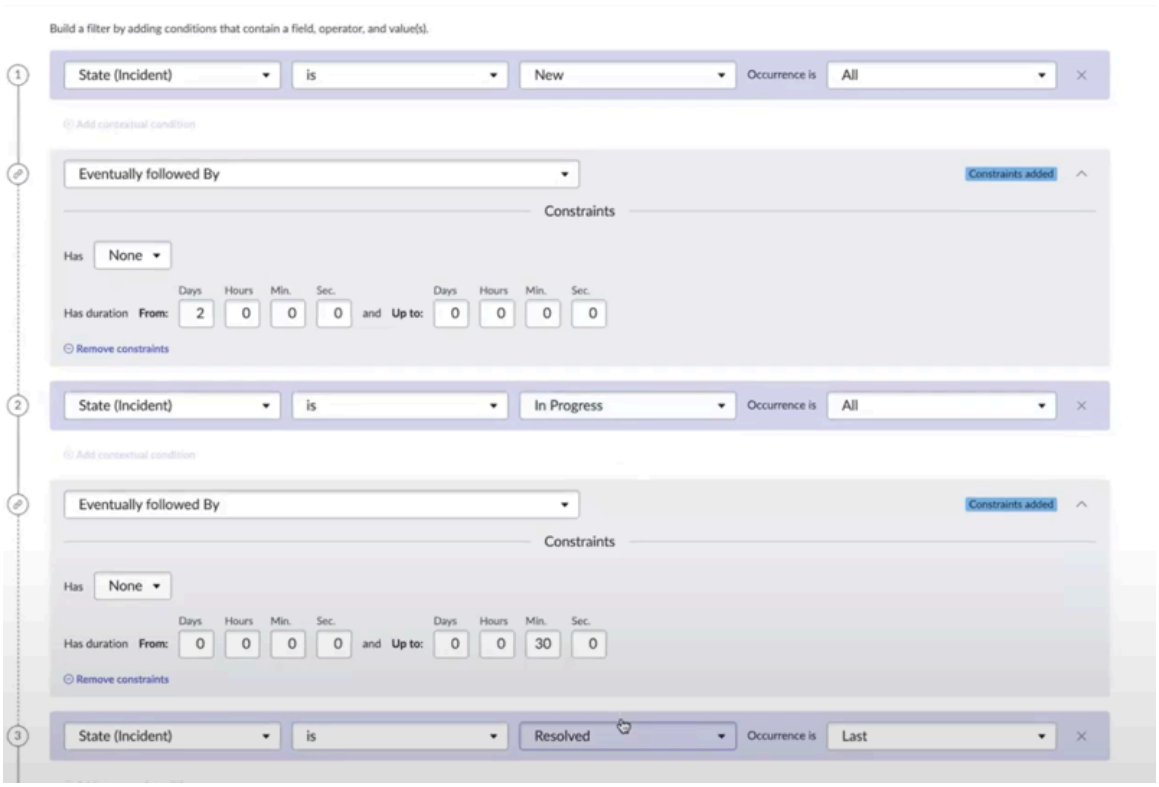
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음은 2일 이상 초안 상태였다가 분석 상태로 전환한 후 30분 이내에 종결된 보안 인시던트를 식별하는 단계의 예입니다.

1. 다음으로 이동 작업 공간 〉 프로세스 마이닝 작업 공간.
2. 프로젝트를 열고 분석가 워크벤치로 이동합니다.

   마이닝된 프로세스 최적화 프로젝트를 열면 기본적으로 분석가 워크벤치가 열립니다.

3. Advanced filters(고급 필터)에서 Transitions(전환)를 선택합니다.
4. 전환 시 고급 필터에서 다음을 구성합니다.
   a. ## ##(####)이 #####.
   b. 궁극적으로 다음으로 이어짐 선택
   c. 제약 조건 추가를 선택하고 시작일을2일로 설정합니다.
   d. 다음 활동 추가를 선택합니다.
   e. ## ##(####)이 ## 중입니다.
   f. 궁극적으로 다음으로 이어짐 선택
   g. 제약 조건 추가를 선택하고 최대 30분으로 설정합니다.
   h. 다음 활동 추가를 선택합니다.
   i. 궁극적으로 다음으로 이어짐 선택
   j. 제약 조건 추가를 선택하고 최대 30분으로 설정합니다.
   k. ## ##(####)이 ##됨입니다.



5. 모든 체인 적용을 선택합니다.
6. 세부 항목 필터를 선택하고 가장 긴 평균 기간을 기준으로 정렬합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 인시던트 및 인바운드 요청 관리

보안 인시던트가 생성된 후 문제 분석이 해결로 진행됨에 따라 다양한 유형의 정보를 추가하고 볼 수 있습니다.

중요사항:
의 보안 인시던트 응답 최신 기능은 에서만 사용할 수 있습니다 보안 인시던트 응답 작업 공간. 교대조 핸드오버, 위험 점수 계산기 등과 같은 기능에 액세스하고 활용하려면 최신 보안 인시던트 응답 버전을 보안 인시던트 응답 작업 공간 설치하거나 업그레이드하십시오.

이 섹션에서는 다음 사항에 대해 설명합니다.

- 인바운드 요청 생성
- 옵저버블 관리
- 조회 및 스캔 관리
- 보안 인시던트 심각도 계산
- 사후 인시던트 활동 관리
- 보안 인시던트 종결

인바운드 요청 생성

보안 인시던트와 달리 인바운드 요청은 일반적으로 우선순위가 낮습니다. 조회, 스캔 또는 새 배지에 대한 요청은 인바운드 요청의 예입니다.

시작하기 전에
필요한 역할: sn_si.basic 이상의 역할

프로시저

1. 요청 양식 중 하나로 이동합니다.
   예: 모두 〉 보안 인시던트 〉 인바운드 요청 〉 나에게 할당됨.
2. 새로 만들기를 클릭합니다.
3. 양식의 필드에 적절히 입력합니다.

보안 요청

필드	설명
번호	〔읽기 전용〕 자동으로 생성된 보안 요청 번호입니다.
회사	요청자 회사입니다.
위치	CI 위치입니다(해당하는 경우). 이 필드는 CI가 선택될 때 미리 채워집니다.
구성 항목	요청의 영향을 받는 구성 항목입니다.
우선순위	요청의 우선순위입니다.
개설 일시	〔읽기 전용〕 요청이 열린 날짜 및 시간입니다.
상태	보안 요청의 현재 상태입니다. 보안 요청 생성 시 이 필드는 기본적으로 초안으로 설정됩니다.
할당 그룹	할당된 작업자가 선택되는 할당 그룹입니다.
담당자	작업을 수행하도록 할당된 개인입니다.
간단한 설명	요청자에게 표시되는 보안 요청에 대한 간략한 설명입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
설명	요청자에게 표시되는 요청에 대한 전체 설명입니다.
작업 메모	요청자가 볼 수 있는 작업 메모입니다.

4. 입력을 완료했으면 제출을 클릭합니다.
5. 요청을 보안 인시던트로 에스컬레이션해야 하는 경우 보안 인시던트로 변환을 클릭합니다.

옵저버블 관리

옵저버블은 네트워크 또는 운영 체제에서 발견되는 아티팩트로, 침입을 나타낼 가능성이 높습니다. 일반적인 옵저버블은 IP 주소, 멀웨어 파일 또는 URL의 MD5 해시 또는 도메인 이름입니다. 위협 인텔리전스 옵저버블 테이블 데이터는 보안 인시던트 내에서 사용할 수 있습니다.

옵저버블 정보에는 값, 유형, 컨텍스트 및 타임스탬프가 포함됩니다.

조회 요청을 통해 수동 또는 자동으로 옵저버블을 생성하거나 삭제할 수 있습니다.

위협 조회 결과 탭에 새 찾기 열이 추가되었습니다. 가능한 값은 악성 및 알 수 없음입니다.

IoC 조회 요청에서 보안 인시던트 옵저버블을 찾지 못하면 알 수 없음으로 레이블이 지정됩니다.

IoC 조회 요청에서 보안 인시던트 옵저버블을 찾으면 악성으로 표시됩니다.

업그레이드하는 동안 기존 항목에는 찾기 열이 악성으로 설정되어 있습니다.

주:
위협 인텔리전스 옵저버블 테이블 데이터는 보안 인시던트의 일부이지만 모듈과의 다른 상호작용은 위협 인텔리전스 포함되지 않습니다. 모든 위협 기능을 위협 인텔리전스 사용하려면 구독을 통해 플러그인을 사용할 수 있습니다.

관련 정보

보안 인시던트 옵저버블 생성

보안 인시던트에 대한 **IoC** 정보 표시

보안 인시던트와 관련된 옵저버블 및 사이팅 검색 결과와 같은 IoC 정보를 볼 수 있습니다.

시작하기 전에
필요한 역할: sn_si.basic

프로시저

1. 아직 열려 있지 않으면 IoC 관련 정보를 보려는 보안 인시던트를 엽니다.
2. **IoC** 표시 관련 링크를 클릭합니다.
3. 관련 목록을 클릭하여 보안 인시던트에 대한 정보를 보거나 추가합니다.

탭	설명
옵저버블	보안 인시던트와 관련된 옵저버블을 보거나 수동으로 추가하거나 편집합니다. 자세한 내용은 옵저버블 관리 문서를 참조하십시오.
연동된 표시기	위협 인텔리전스 가 활성화되면 동일한 위협 레코드와 연결된 다른 표시기를 볼 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

탭	설명
사이팅 검색 결과	사이팅 검색 결과를 포함합니다.
사이팅 검색 정보	사이팅 검색 기록 상세 정보를 포함합니다.
위협 조회	맬웨어 탐지 시스템의 보강 데이터를 저장합니다. 이 탭은 플러그인이 위협 인텔리전스 설치된 경우에만 나타납니다.
연결된 공격 모드/방식	위협 인텔리전스 가 활성화되면 동일한 위협 레코드와 관련된 다른 공격 유형을 볼 수 있습니다.
보안 검사 요청	위협 인텔리전스 가 활성화되면 보안 인시던트에 첨부된 스캔 및 조회 요청을 볼 수 있습니다.
유사한 IoC가 포함된 자원	위협 인텔리전스 가 활성화되면 비슷한 표시기가 있는 다른 자원을 볼 수 있습니다.
유사한 IoC를 가진 사용자	위협 인텔리전스 가 활성화되면 비슷한 표시기를 가진 다른 사용자를 볼 수 있습니다.

4. 보안 인시던트를 추가로 업데이트하려면 다음 관련 링크 중 하나를 클릭하십시오.
   - 영향을 받는 항목 표시
   - 관련 항목 표시
   - 보강 데이터 표시
   - 응답 작업 표시
5. 입력을 완료했으면 제출을 클릭합니다.

보안 인시던트 옵저버블 생성

보안 인시던트 내에서 옵저버블을 생성 및 확인하고 적절한 조치를 취할 수 있습니다. 보안 인시던트에 옵저버블을 사용할 수 있도록 하면 확장 가능하고 응답시간이 단축됩니다.

시작하기 전에

필요한 역할:

- sn_ti_observable.write (쓰기)
- sn_ti_observable.read (읽기)
- sn_ti_observable.admin(삭제)

프로시저

1. 보안 인시던트로 이동합니다.
2. 인시던트를 선택합니다.
3. 보안 인시던트 옵저버블 관련 목록 탭을 클릭합니다.
4. 새로 만들기를 클릭합니다.
5. 양식의 필드에 적절히 입력합니다.

필드	설명
분류 태그 선택	보안 태그를 설정하고 활성화하여 기록에 메타데이터를 추가하는 경우 하나 이상의 태그를 선택하여 옵저버블의 민감도를 지정할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	보안 태그를 설정하거나 활성화하지 않은 경우에는 이 드롭다운 목록이 표시되지 않습니다.
값	옵저버블과 연결된 값(예: IP 주소 또는 해시)입니다. 주: IP 주소 또는 해시에 대한 위협 검사 , 반환된 맬웨어 또는 기타 오류가 발생하면 IP 주소 또는 해시 값이 옵저버블 [sn_ti_observable] 테이블에 자동으로 추가됩니다. 따라서 옵저버블 양식에서 검색할 수 있습니다.
옵저버블 유형	IP 주소 또는 파일 해시와 같은 옵저버블 분류를 선택합니다. 이러한 옵저버블 유형은 **Observable Types** 모듈에 정의되어 있습니다.
인시던트 수	옵저버블 값이 발생한 횟수입니다.
컴퍼지션임	이 필드는 옵저버블 기록이 저장된 후에만 표시됩니다. 옵저버블 유형이옵저버블 컴포지션 이외의 항목으로 설정되어 있고 이 새 옵저버블이 컴포지션인 경우 이 확인란을 선택합니다. 옵저버블 유형이 이미 옵저버블 컴포지션으로 설정된 경우 확인란이 선택되고 읽기 전용입니다. 옵저버블 컴포지션은 자식 옵저버블을 포함하는 옵저버블입니다.
찾기	다음 중 하나를 선택합니다. ○ 악성: 옵저버블이 조직에 해롭다는 것을 나타냅니다. ○ 의심스러움: 옵저버블이 조직에 해로울 수 있음을 나타냅니다. ○ **Clean**: 옵저버블이 조직에 해롭지 않음을 나타냅니다. ○ 알 수 없음: 옵저버블의 발견 사항이 아직 결정되지 않았음을 나타냅니다. ○ 기본값: 알 수 없음. 자세한 내용은 위협 조회 찾기 계산기 문서를 참조하십시오. 주: 업그레이드 후 기존 옵저버블은 악성으로 표시됩니다.
운영자	이 필드는 컴포지션 확인란이 선택된 경우에만 나타납니다. 이 필드의 설정에 따라 연결된 표시기가 있는지 여부를 결정할 때 옵저버블과 해당 하위 항목이 고려됩니다. 연결된 표시기가 존재하는 것으로 간주되기 위해 모든 하위 옵저버블이 있어야 하는 경우 이 필드를 **AND** 로 설정합니다. 연결된 표시기가 존재하는 것으로 간주하기 위해 하위 옵저버블이 있는 경우 **OR** 로 설정합니다.
존재하지 않아야 함	이 필드는 옵저버블 기록이 저장된 후에만 표시됩니다. 선택하는 경우 이 필드는 옵저버블의 부재가 잠재적인 문제(예: 레지스트리 키 누락)임을 나타냅니다.
위치	두 속성의 설정과 스크립트 포함 정의를 사용하면 이 필드에 로드할 더 많은 IoC 데이터 로드 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

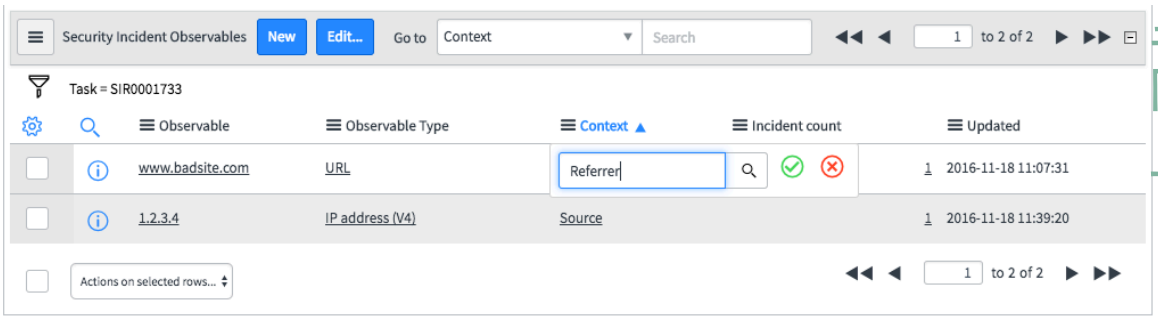
필드	설명
메모	옵저버블에 대한 추가 메모를 입력합니다.

6. 양식 헤더를 마우스 오른쪽 버튼으로 클릭하고 저장을 클릭합니다.
이제 다음 관련 목록 중 하나를 클릭하여 추가 정보를 볼 수 있습니다.

관련 목록	설명
관련 표시기	위협 소스에서 식별한 표시기를 나열합니다.
관련된 작업	옵저버블과 연결된 변경 내용을 나열합니다.
하위 옵저버블	위협 소스에서 식별한 관련 옵저버블을 나열합니다.
IP에 대해 일치하는 자원	옵저버블이 IP 주소인 경우 이 목록에는 일치하는 IP 주소가 있는 모든 리소스(구성 항목)가 표시됩니다.
옵저버블 소스	소스의 신뢰도와 함께 이 옵저버블의 소스를 나열합니다.
보안 주석	이 옵저버블에 추가된 보안 주석을 나열합니다.

7. 보안 인시던트로 돌아가면 다음 정보를 사용할 수 있습니다.

주:
보안 인시던트에 옵저버블을 추가하면 시스템은 이와 관련된 다른 구성 항목이나 사용자가 있는지 확인합니다. 관련 구성 항목 및 관련 사용자 관련 목록 탭이 업데이트됩니다.



열	정의
옵저버블	옵저버블과 연결된 값(예: IP 주소 또는 해시)입니다.
관찰 대상 유형	특정 유형의 옵저버블입니다.
컨텍스트	사용자가 선택합니다. 선택 항목은 다음과 같습니다. ○ IP - 소스 또는 대상 주: 및이 활성화된 경우 위협 인텔리전스 이 필드에 값을 변경하거나 추가하면 로그 데이터 플로우 가져오기 Security Operations Palo Alto Networks - 로그 데이터 가져오기 워크플로우가 실행됩니다.Palo Alto Networks - Firewall 워크플로우는 방화벽에서 보강된 위협 로그 데이터를 검색하여 보안 인시던트에 연결합니다. 또한 이 정보는 구문 분석되어 보강 데이터 탭 아래의 방화벽 로그 섹션에 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

열	정의
	○ URL - 참조자 주: 사용자가 피싱 이메일의 링크를 클릭할 때 리퍼러는 맬웨어 URL에 액세스하기 전 마지막 점프의 URL입니다.
인시던트 수	이 옵저버블이 나타나는 인시던트 수입니다. 이 값은 옵저버블이 수동으로 또는 워크플로우를 통해 다른 인시던트에 추가될 때 자동으로 업데이트됩니다.
업데이트됨	목록이 마지막으로 업데이트된 데이터 및 시간입니다.

주:
플러그인이 위협 인텔리전스 설치된 경우 **IoC** 리포지토리의 옵저버블 목록에서 옵저버블을 볼 수도 있습니다.

관련 정보

보안 인시던트 옵저버블 목록 편집

여러 보안 인시던트 옵저버블추가

파일 옵저버블 관리

파일 옵저버블 관리는 의심스러운 파일을 저장하기 위한 엄격한 보안 조치를 제공하고 샌드박스 통합을 위해 파일 유형 옵저버블을 활성화합니다.

시작하기 전에

필요한 역할: sn_ti_malicious_attachment_access(업로드)

옵저버블 파일 유형 업로드:

- 자동: 피싱 이메일에 대한 보안 인시던트가 생성되면 피싱 이메일의 첨부 파일이 옵저버블 파일 형식으로 생성됩니다.
- 수동으로: 보안 분석가는 의심스러운 파일을 업로드하여 옵저버블 파일 유형을 생성할 수도 있습니다.

이 태스크 정보

보안 인시던트에 대한 옵저버블 파일 유형을 생성하고 볼 수 있습니다. 옵저버블의 일부인 의심스러운 파일은 특정 위치에 저장되며, 보안 분석가가 특정 역할로만 파일을 다운로드하기 위해 액세스할 수 있습니다.

프로시저

1. 보안 인시던트로 이동합니다.
2. 모든 관련 목록 표시 탭에서 옵저버블을 선택합니다.

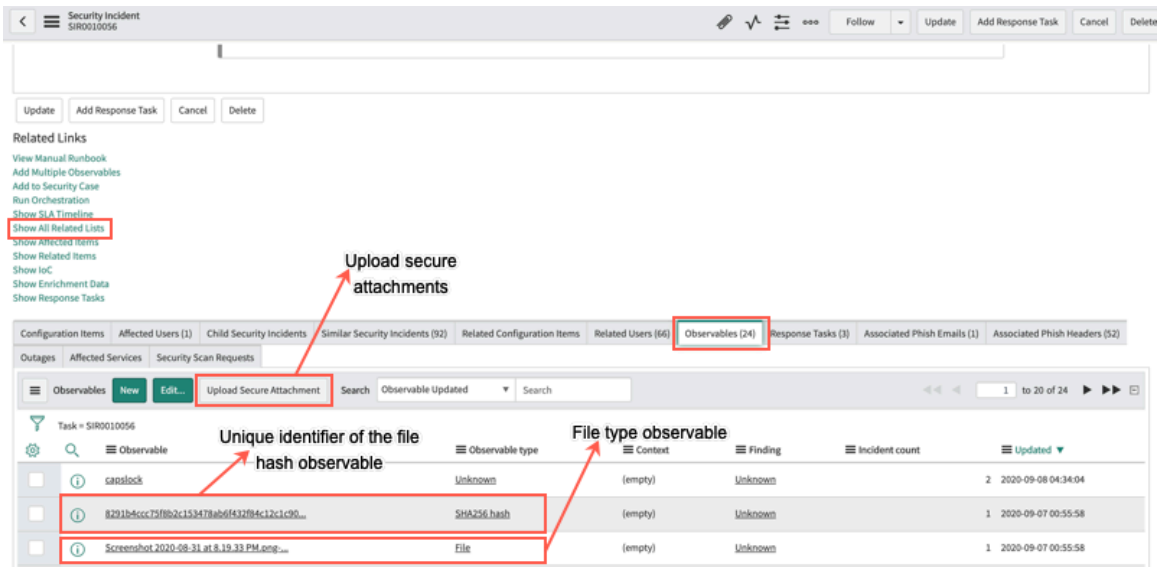
   피싱 이메일에 첨부 파일이 있는 경우 기본적으로 이러한 첨부 파일은 해당 보안 인시던트에서 파일 유형 옵저버블로 생성됩니다. 각 첨부 파일은 파일 유형 및 파일 해시 옵저버블과 같은 두 개의 옵저버블로 생성됩니다.

3. 보안 첨부 파일을 수동으로 업로드하려면 다음과 같이 하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 보안 첨부 파일 업로드를 클릭합니다.
- 보안 첨부 파일 업로드에서 파일 선택을 클릭하여 하나 이상의 파일을 업로드합니다. 각 파일은 단일 옵저버블 기록으로 간주됩니다.
- 파일 옵저버블 생성을 클릭하여 옵저버블 파일 유형을 생성합니다. 예를 들어 하나는 파일 유형이고 다른 하나는 고유 식별자인 파일 해시입니다.

옵저버블 파일 형식



샌드박스, 위협 조회와 같은 추가 통합을 위해 처리할 옵저버블 파일 유형을 선택합니다. 또한 옵저버블 파일 형식에서 첨부 파일을 다운로드할 수도 있습니다.

주:

위협 조회(VirusTotal)는 새 파일 유형 옵저버블에 대해 보안 첨부 파일에서 파일을 검색하며, 아래 시스템 속성은 새 파일 유형 옵저버블에 적용할 수 없습니다.

- sn_ti.scan.delete_attachment_after_hash
- sn_ti.scan.use_file_hash

빠른 참조를 위해 파일 유형 observable은 해시 옵저버블에 하위로 매핑되고 해시 옵저버블은 파일 옵저버블에 하위로 매핑됩니다.

피싱 이메일 첨부 파일이 정의된 크기보다 큰 경우 옵저버블이 생성되지 않습니다. 더 큰 크기의 파일을 지원하려면 시스템 속성을 수정해야 합니다.

파일 크기 시스템 속성

시스템 속성	설명
glide.email.inbound.max_total_attachment_size_bytes	피싱 이메일을 직접 전달하는 경우 이 시스템 속성 값을 사용하여 파일 크기를 18MB에서 원하는 파일 크기로 늘립니다.
com.glide.attachment.max_get_크기	피싱 이메일을 첨부 파일로 전달하는 경우 이 시스템 속성 값을 사용하여 전역 범위에서 아래 시스템 속성을 생성하여 파일 크기를 5MB에서 원하는 크기로 늘립니다.

다음과 같이 새 파일 유형 옵저버블을 생성할 수도 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 새로 만들기를 클릭합니다.

b. 옵저버블 유형 범주: 파일 선택

c. 업로드를 클릭하여 파일을 첨부합니다.

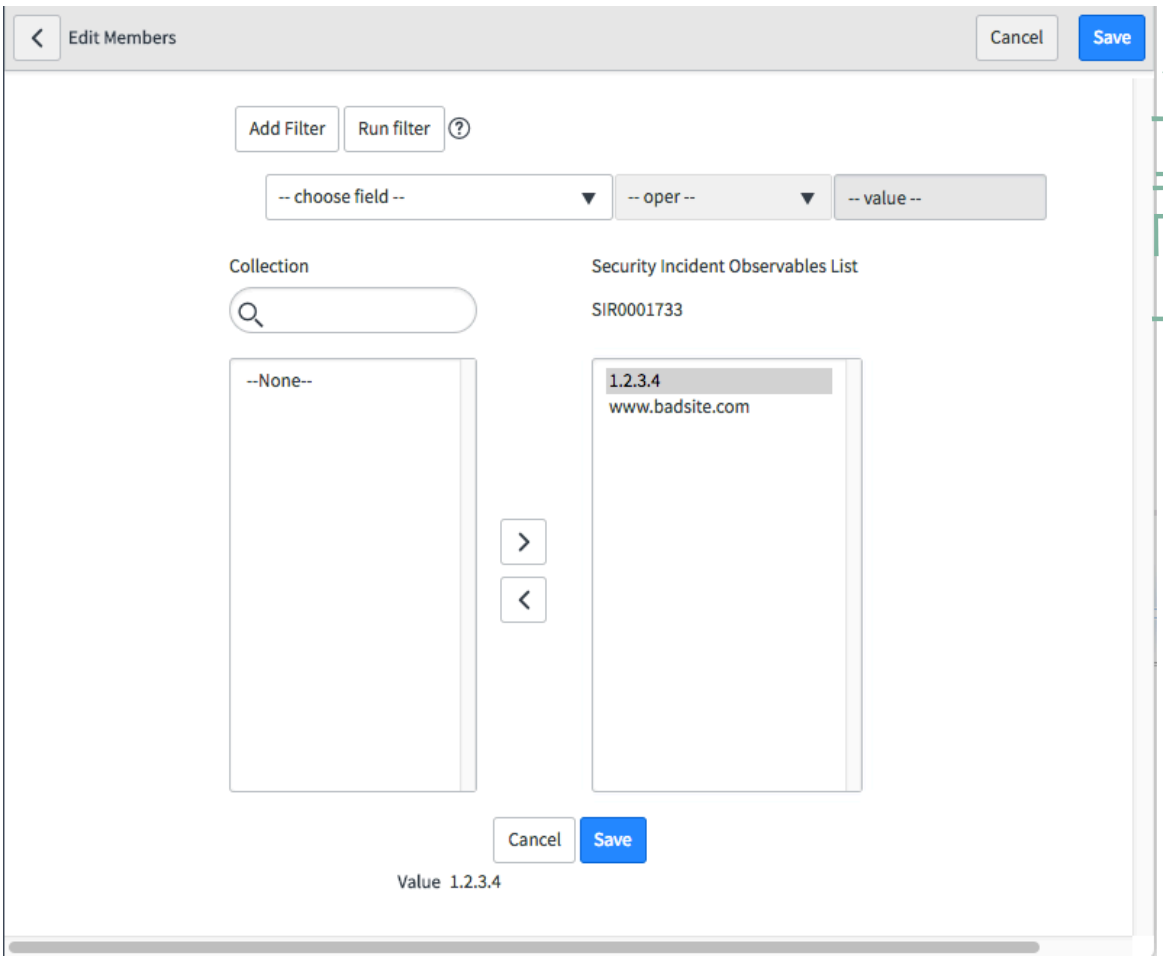
보안 인시던트 옵저버블 목록 편집

목록에서 표시할 보안 인시던트와 관련된 옵저버블을 편집할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.basic

프로시저

1. 보안 인시던트로 이동합니다.
2. 인시던트를 선택합니다.
3. 보안 인시던트 옵저버블 관련 목록 탭을 클릭합니다.
4. 편집을 클릭합니다.
5. 목록에서 옵저버블을 추가하거나 제거합니다.
   긴 목록에 대한 필터를 생성합니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

6. 저장을 클릭합니다.

> 주:
> 보안 인시던트에 옵저버블을 추가하면 시스템은 이와 관련된 다른 구성 항목이나 사용자가 있는지 확인합니다. 관련 구성 항목 및 관련 사용자 관련 목록 탭이 업데이트됩니다. 또한 플러그인이 위협 인텔리전스 활성화되어 있고 하나 이상의보안 인시던트 응답 통합 통합 구현이 활성화되어 있는 경우 에서 보안 운영 통합 - 위협 조회 기능 하나 이상의 워크플로우를 실행하고, 추가한 옵저버블에서 위협 보안 조회가 수행됩니다. 결과는 위협 조회 결과 탭에 나타납니다.

관련 정보

여러 보안 인시던트 옵저버블추가

보안 인시던트 옵저버블 생성

여러 보안 인시던트 옵저버블추가

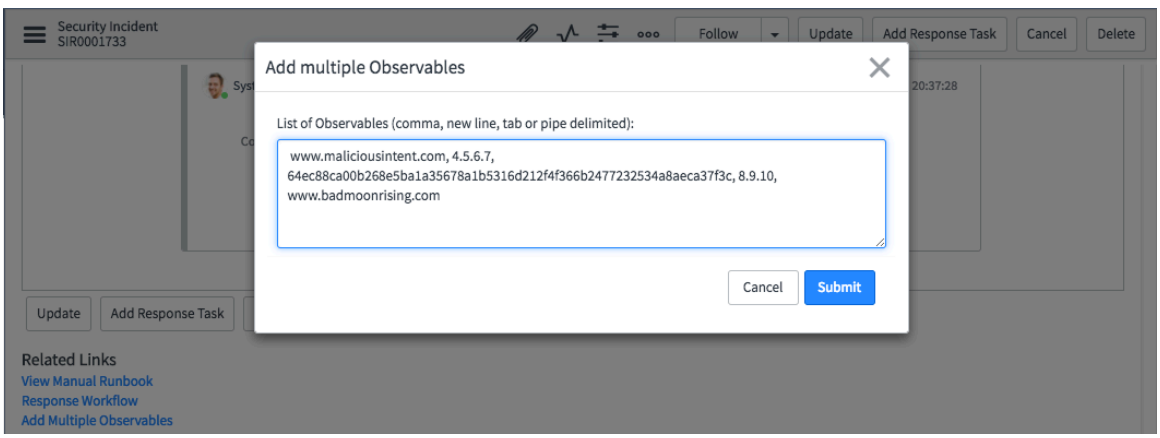
시간을 절약하기 위해 보안 인시던트 옵저버블 목록에 여러 보안 인시던트 옵저버블을 추가할 수 있습니다.

시작하기 전에
필요한 역할: sn_ti_write

> 주:
> 여러 보안 인시던트 옵저버블을 추가할 때 처리 중에 중복 항목은 무시됩니다.

프로시저

1. 보안 인시던트로 이동합니다.
2. 인시던트를 선택합니다.
3. 복수 옵저버블 추가 관련 링크를 클릭합니다.
4. 여러 옵저버블을 입력하거나 붙여넣습니다.
   항목은 모든 옵저버블 유형일 수 있습니다. 허용되는 형식은 쉼표, 줄 바꿈, 탭 또는 파이프 구분 기호입니다.



> 주:
> 보안 인시던트에 옵저버블을 추가하면 시스템은 이와 관련된 다른 구성 항목이나 사용자가 있는지 확인합니다. 관련 구성 항목 및 관련 사용자 관련 목록 탭이 업데이트됩니다.

참고: 자동 탐지되지 않은 옵저버블 값은 알 수 없음 유형에 할당됩니다.

5. 제출을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

자동 보안 인시던트 옵저버블 로그 데이터 보강

통합을 Palo Alto Networks - Firewall 비롯한 위협 인텔리전스 특정 애플리케이션 및 통합이 설정되면 옵저버블의 소스 IP가 수정될 때마다 보안 인시던트의 옵저버블 정보를 위협 로그 데이터로 자동으로 보강할 수 있습니다.

수정이 발생하면 비즈니스 규칙이 방화벽의 위협 로그에서 데이터를 검색하고 보안 인시던트의 옵저버블 정보를 보강하는 워크플로우를 시작합니다.

옵저버블을 보강하려면 먼저 다음 단계를 수행해야 합니다.

- Threat Intelligence 를 활성화해야 합니다.
- Palo Alto Networks 방화벽 통합을 활성화하고 구성해야 합니다. 여기에는 도 포함될 MID 서버에 대한 SSH 자격 증명 설정수 있습니다.

설정이 완료된 후 보안 인시던트와 연결된 옵저버블의 소스 IP를 변경하면 비즈니스 규칙이 보안 운영 **Palo Alto Networks -** 로그 데이터 가져오기 워크플로우를 실행합니다. 워크플로우 활동은 방화벽에서 검색 쿼리를 대기열에 추가하고 방화벽에서 위협 로그 데이터를 검색하고 보안 인시던트에 XML 파일로 첨부하는 데 사용되는 작업 ID를 반환합니다.

관련 정보

자동 포커스 세션 정보 가져오기 보강 플로우

Palo Alto Networks 방화벽 시작 관리자 워크플로우

Security Operations Palo Alto Networks - 값 워크플로우 확인 및 차단

로그 데이터 플로우 가져오기

WildFire 데이터 보강 플로우 가져오기

외부 공급업체 감시 목록에 옵저버블 게시

하나 이상의 옵저버블 또는 관련 표시기를 외부 공급업체 주시 목록에 게시할 수 있습니다. 현재 이 기능을 지원하는 유일한 구현은 CrowdStrike Falcon Host입니다.

시작하기 전에

필요한 역할: sn_si.analyst

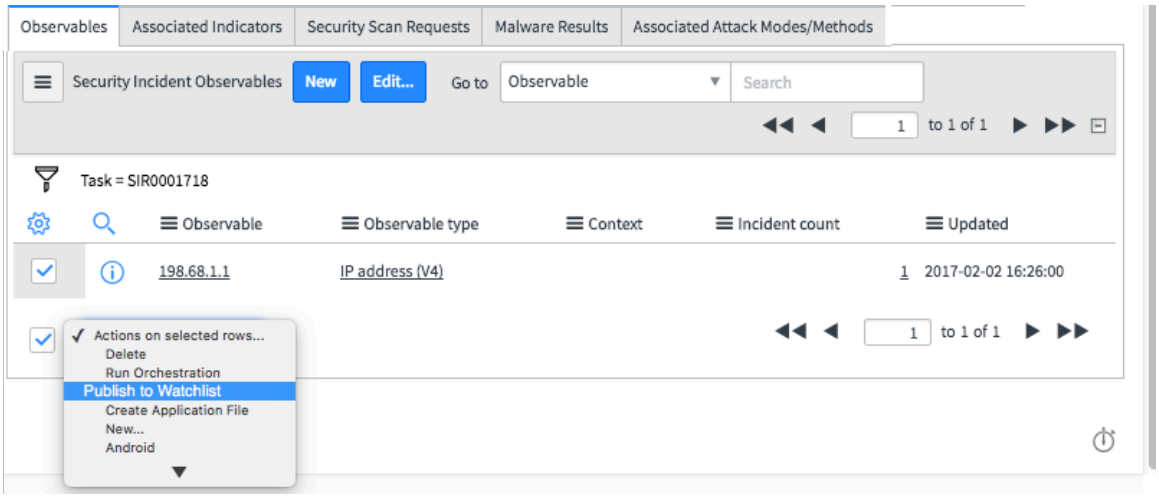
이 태스크 정보

주:
사용 가능한 구현이 없으면 역량 작업이 제품 메뉴에 표시되지 않습니다.

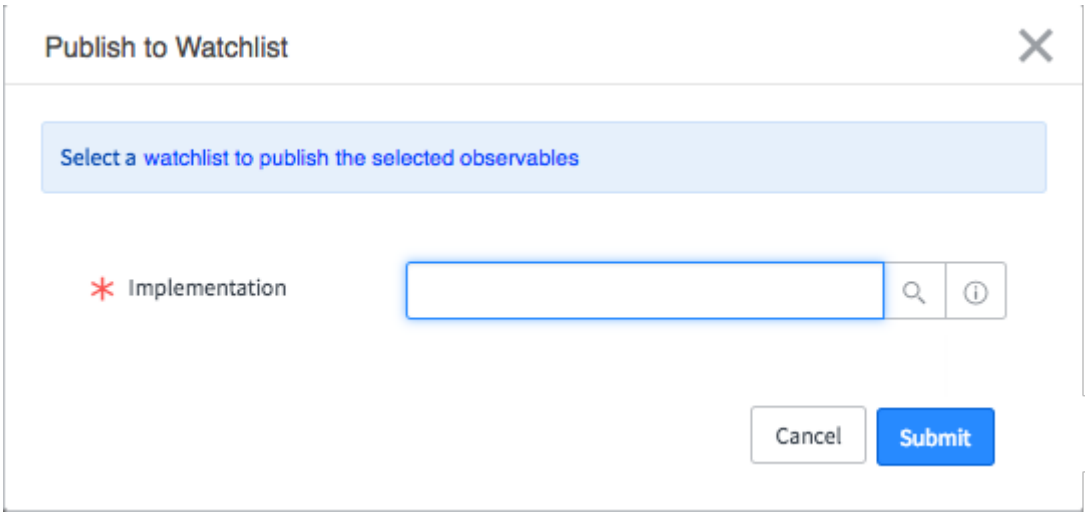
프로시저

1. 보안 인시던트로 이동합니다.
2. 관련 목록 탭에서 옵저버블을 선택합니다.
3. **Actions on selected rows...**(선택한 행에 대한 작업) 드롭다운 메뉴에서 **Publish to** Watchlist(감시 목록에 게시)를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



대화 상자가 나타납니다.



4. 구현을 입력하거나 선택합니다.

> **주:**
> 워크플로우는 CrowdStrike Falcon Host 구현을 선택할 때 보안 운영 통합 - 감시 목록에 게시 기능 트리거됩니다.

5. 제출을 클릭합니다.

조회 및 스캔 관리

보안 인시던트 및 보안 인시던트 카탈로그에서 조회 및 취약성 검사를 수행하여 잠재적인 위협과 취약성을 식별할 수 있습니다.

보안 인시던트에서 **IoC** 조회 요청 제출

옵저버블이 보안 인시던트에 추가될 때마다 IoC 조회가 자동으로 실행됩니다. 또한 보안 인시던트에 첨부 파일이 있는 경우 버튼을 눌러 쉽게 찾을 수 있습니다.

시작하기 전에
자동 IoC 조회의 위협 인텔리전스 경우 플러그인을 활성화해야 합니다.

필요한 역할: sn_si.basic

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

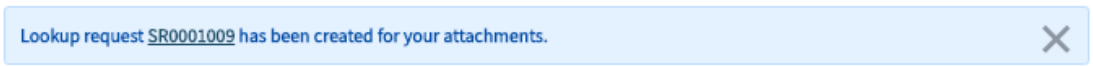
주:
기본적으로 파일에 대한 조회 유형은 비활성 상태입니다.

프로시저

1. 새 보안 인시던트를 생성하거나 새 파일을 첨부하려는 경우 기존 보안 인시던트를 엽니다.
2. 양식 헤더에서 종이 클립 아이콘을 클릭하고 하나 이상의 파일을 첨부합니다.
3. 양식에 대한 입력을 완료했으면 양식 헤더를 마우스 오른쪽 버튼으로 클릭하고 저장을 클릭합니다.
   기록이 저장되면 첨부 파일 조회 버튼이 나타납니다.
4. 첨부 파일 조회를 클릭합니다.

   주:
   인시던트 상세 정보 아래의 작업 메모는 조회 프로세스의 진행률을 보고합니다.

5. 메시지 끝에 있는 조회 번호를 클릭하면 조회 기록을 볼 수 있습니다.
   참조 조회 링크를 클릭하면 자세한 결과를 볼 수 있습니다.



에서 **IoC** 조회 요청 제출 보안 인시던트 카탈로그

플러그인이 보안 인시던트 응답 활성화되면 보안 인시던트 카탈로그에서 파일, 해시 값, URL 및 IP 주소에 대한 위협 조회를 제출할 수 있습니다. 요청이 제출되고 내 요청 모듈에서 결과를 볼 수 있습니다.

시작하기 전에
필요한 역할: 없음

이 태스크 정보
조회 기록에 나열된 각 조회 소스의 기본 조회 유형에 대해 조회가 자동으로 수행됩니다. 조회 요청의 결과는 내 요청 모듈에서 확인할 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 **Self-Service** 〉 보안 인시던트 카탈로그.
2. **IoC** 조회를 클릭합니다.
3. 파일, 해시 값, **URL** 또는 **IP** 주소 조회를 클릭합니다.
4. 다음 중 하나 이상을 입력합니다.

IoC 조회 요청

조회할 항목	설명
파일	종이 클립 아이콘을 클릭한 다음 조회하려는 파일을 찾아 첨부합니다. 주: 기본적으로 파일에대한 조회 유형은 비활성 상태입니다. 파일은 변환되어 해시 값으로 제출됩니다.
URL	**URL** 필드에 조회하려는 URL을 쉼표로 구분하여 입력합니다. 예: www.abc.com,www.xyz.net.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

조회할 항목	설명
IP 주소	**IP** 주소 필드에 조회하려는 IP 주소를 쉼표로 구분하여 입력합니다.
해시 값	해시 값 필드에 조회하려는 해시 값을 쉼표로 구분하여 입력합니다. 주: 파일에 대한 조회 유형이 비활성 상태인 경우 이 값은 파일 및 해시 값 모두에 대한 기본 작업입니다.

5. 선택을 마쳤으면 제출을 클릭합니다.
6. 조회의 상태 및/또는 결과를 보려면 다음으로 이동하십시오. **Self-Service** 〉 내 요청.
7. 요청의 SR 번호를 클릭합니다.
   활동 아래의 작업 메모에는 각 파일, 해시 값, URL 또는 IP 주소, 조회 결과에 대한 개별 조회 생성을 포함하여 조회 중에 수행된 작업이 나열됩니다.

보안 인시던트에서 취약성 스캔 요청 제출

보안 인시던트에 구성 항목(서버, 컴퓨터 등)이 하나 이상 있는 경우 양식에서 보안 인시던트 응답 취약성을 검사할 수 있습니다.

시작하기 전에

취약성 대응 플러그인을 활성화해야 합니다.

필요한 역할: sn_si.write

프로시저

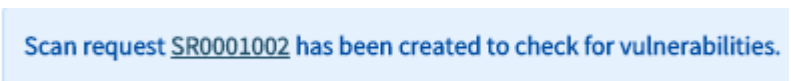
1. 보안 인시던트를 생성하고 하나 이상의 자원을 포함합니다.
   구성 항목이 있는 기존 인시던트를 열 수도 있습니다.
2. 양식에 대한 입력을 완료했으면 양식 헤더를 마우스 오른쪽 버튼으로 클릭하고 저장을 클릭합니다.
   기록이 저장되면 취약성 검사 관련 링크가 나타납니다.

   주:
   취약성 검사 관련 목록이 표시되지 않으면 다음으로 이동해야 합니다. 취약성 〉 스캐너, 하나 이상의 스캐너를 설정하고, 기본값을 **true**로 설정합니다.

3. 취약성 검사를 클릭합니다.

   주:

   보안 인시던트 양식 상단에 스캔 기록에 대한 링크와 함께 메시지가 표시됩니다.

4. 스캔 요청 번호를 클릭하면 스캔 기록을 볼 수 있습니다.
   인시던트 상세 정보에는 보안 스캔 요청 기록의 검사 결과가 표시됩니다.

보안 인시던트 응답 카탈로그에서 취약성 검사 요청 제출

카탈로그에서 CI 및 IP 주소에 대한 취약성 스캔을 제출할 수 있습니다 보안 인시던트 응답 . 요청이 제출되고 내 요청 모듈에서 결과를 볼 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: 없음

프로시저

1. 다음으로 이동 모두 〉 **Self-Service** 〉 보안 인시던트 카탈로그.
2. 취약성 스캔을 클릭합니다.
3. 구성 항목 및 **IP** 주소 검색을 클릭합니다.
4. 검사할 다음 항목을 하나 이상 입력합니다.

취약성 스캐너

스캔할 항목	설명
구성 항목	스캔할 구성 항목 필드에서 스캔할 CI를 선택합니다.
IP 주소	검사할 **IP** 주소 필드에 IP 주소를 쉼표로 구분하여 입력합니다.

5. 선택을 마쳤으면 제출을 클릭합니다.
   옵저버블이 발견되면 STIXX 표준에 따라 표시기가 생성됩니다.
6. 스캔의 상태 및/또는 결과를 보려면 다음으로 이동하십시오. **Self-Service** 〉 내 요청.
7. 요청의 SR 번호를 클릭합니다.
   활동 아래의 작업 메모에는 각 CI 또는 IP 주소에 대한 개별 스캔 생성과 스캔 결과를 비롯하여 스캔 중에 수행된 작업이 나열됩니다.

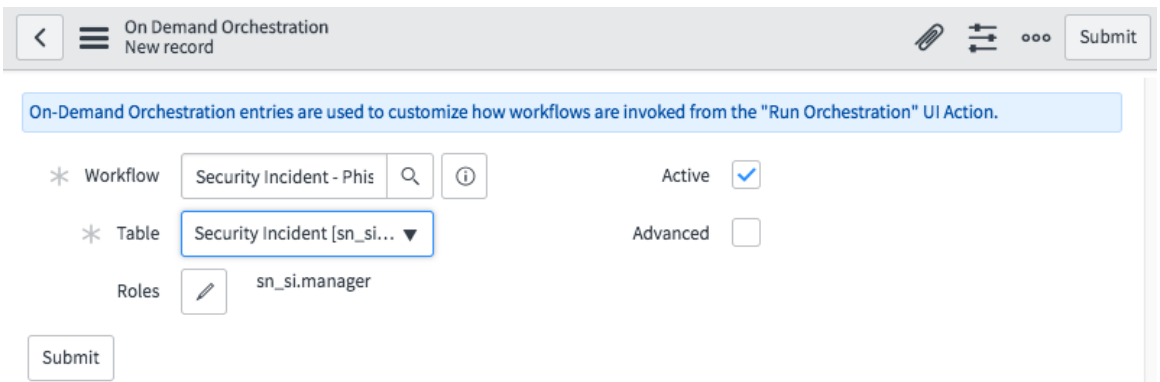
새 요청 시 오케스트레이션 정의

기본 시스템에서는 미리 정의된 워크플로우를 실행하는 요청 시 오케스트레이션을 선택할 수 있습니다. 새로운 요청 시 오케스트레이션을 정의하여 오케스트레이션 실행 선택 목록에서 워크플로우를 호출하는 방법을 사용자 지정할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.write

프로시저

1. 다음으로 이동 모두 〉 보안 운영 〉 유틸리티 〉 요청 시 오케스트레이션
2. 새로 만들기를 클릭합니다.



3. 필드에 적절한 정보를 입력합니다.

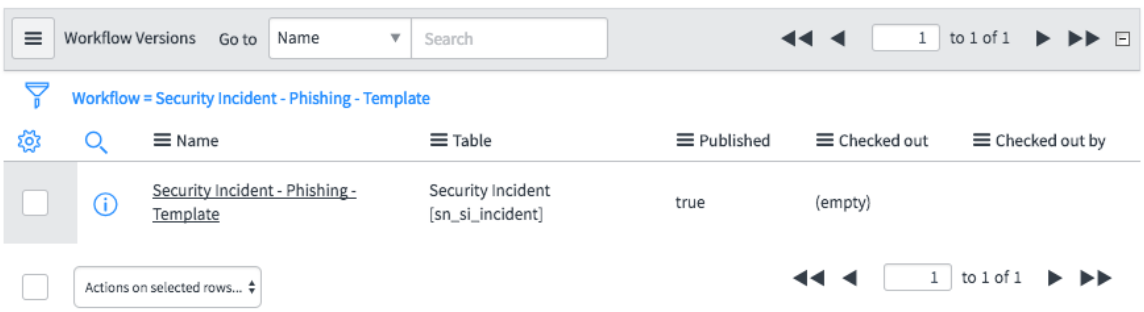
기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

요청 시 오케스트레이션

필드	설명
워크플로우	오케스트레이션 실행 선택 목록에 포함할 워크플로우를 선택합니다.
테이블	선택한 워크플로우가 실행되는 테이블을 선택합니다. 테이블이 선택한 워크플로우에 대해 구성된 테이블과 일치하지 않으면 고급 확인란을 선택하고 실행 스크립트를 수정하여 실행 시 워크플로우에 올바른 기록을 전달해야 합니다.
역할	필요에 따라 추가 역할을 선택하여 오케스트레이션 실행 선택 목록에서 이 워크플로우를 볼 수 있는 사람을 제한합니다.
활성	이 요청 시 오케스트레이션 기록을 활성화하려면 이 확인란을 선택합니다.
고급	이 확인란을 선택하여 이 워크플로우에 대해 선택한 테이블에 올바른 기록을 전달할 수 있도록 실행 스크립트를 수정합니다.
실행 스크립트	이 워크플로우에 대해 선택한 테이블에 올바른 기록을 전달할 수 있도록 실행 스크립트를 수정합니다. 이 필드는 고급 확인란이 선택된 경우에만 나타납니다.

4. 기록 헤더를 마우스 오른쪽 버튼으로 클릭하고 저장을 선택합니다.
워크플로우 버전 관련 목록이 나타납니다.



5. 워크플로우를 추가로 수정해야 하는 경우 체크 아웃해야 합니다.

관련 정보

워크플로우 버전 작업

요청 시 오케스트레이션을 위한 새 보안 운영 애플리케이션 등록

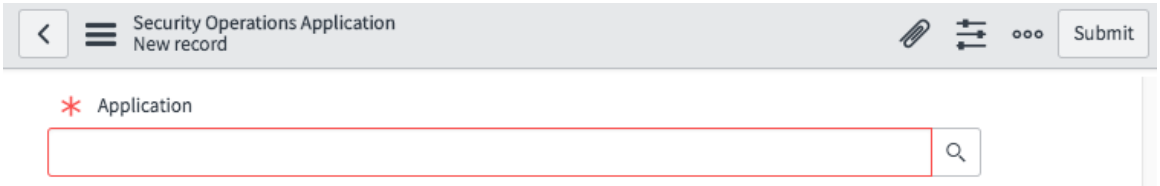
기본 시스템에서 Security Operations 애플리케이션은 활성화될 때 자동으로 등록됩니다. 등록을 통해 애플리케이션과 연결된 워크플로우를 요청 시 오케스트레이션 요청에 사용할 수 있습니다. 필요한 경우 새 애플리케이션을 정의하고 요청 시 오케스트레이션을 위해 워크플로우를 연결할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

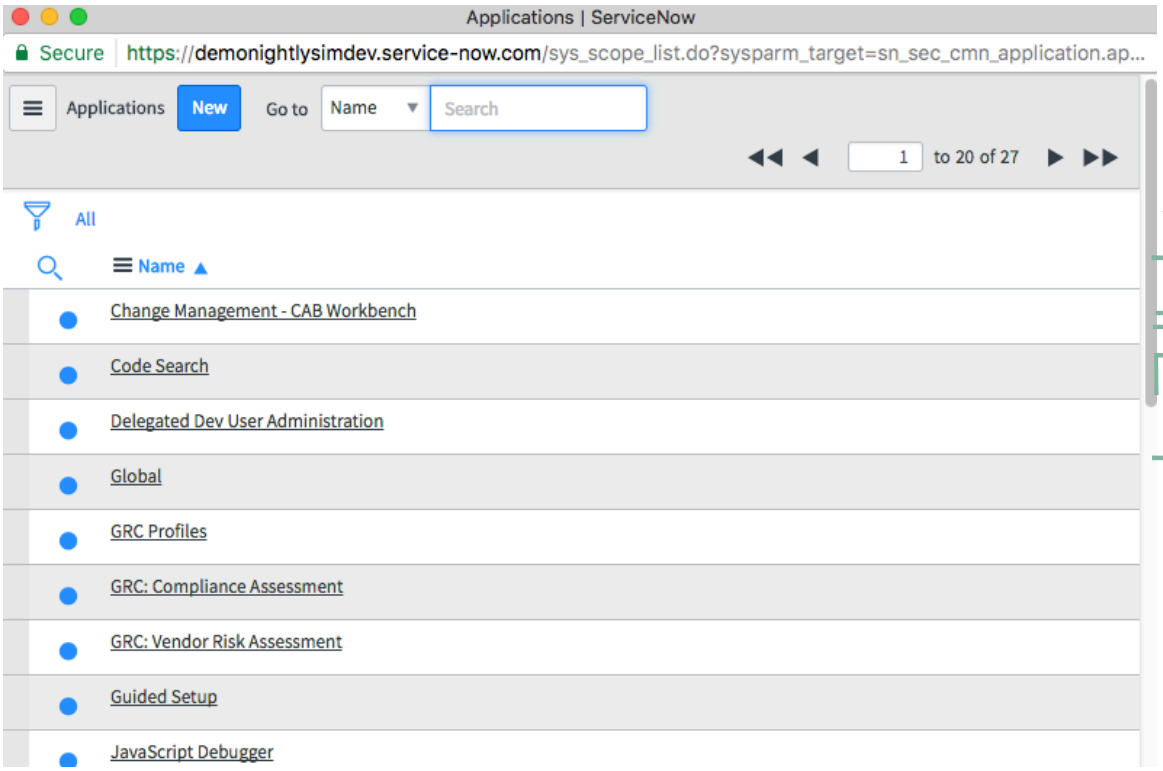
시작하기 전에
필요한 역할: sn_si.write

프로시저

1. 다음으로 이동 모두 〉 보안 운영 〉 유틸리티 〉 **SecOps** 애플리케이션 레지스트리을 클릭하고 애플리케이션 등록을 클릭합니다.
   Security Operations Application 화면이 나타납니다.

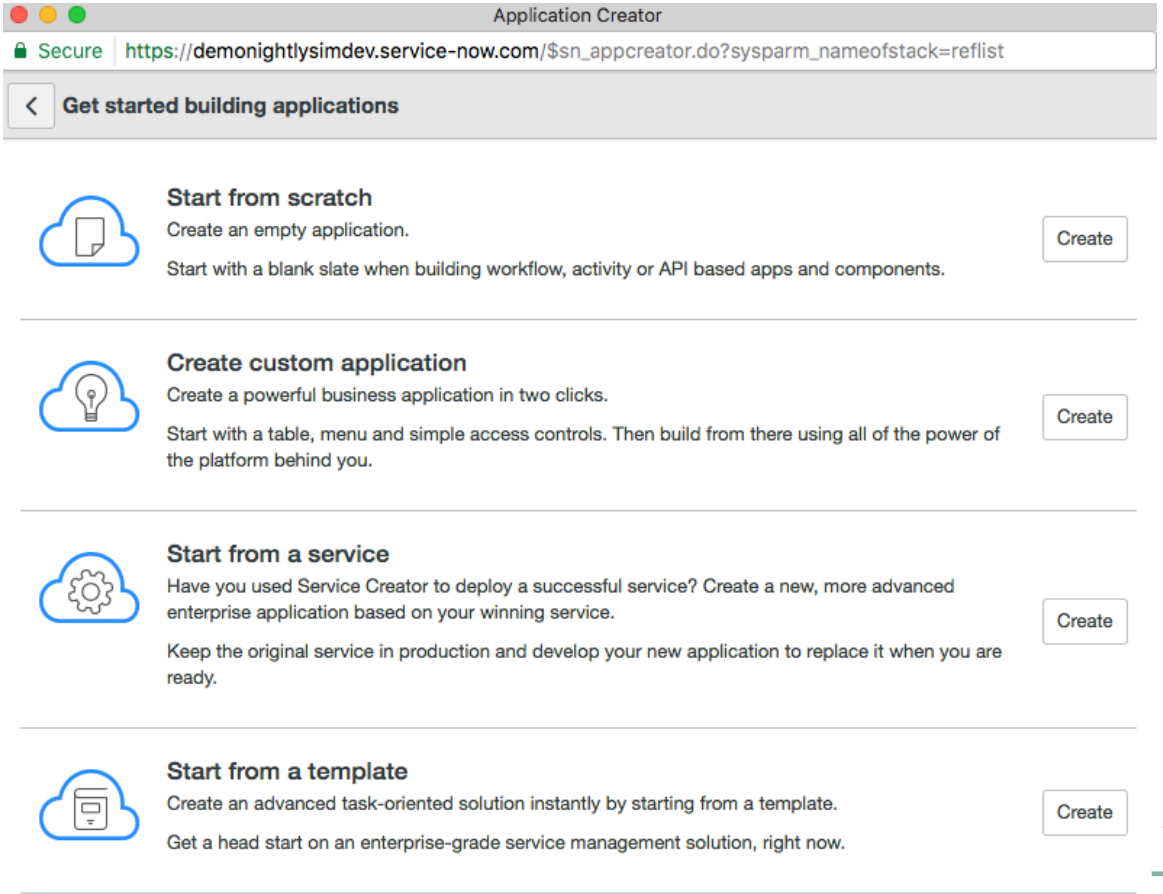


2. 애플리케이션 필드에서 조회(돋보기) 아이콘을 클릭합니다.
   애플리케이션 화면이 나타납니다.



3. 새로 만들기를 클릭합니다.
   애플리케이션 작성자 화면이 나타납니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



주:
표시되는 옵션은 활성화한 애플리케이션에 따라 다릅니다. 새 애플리케이션 생성에 대한 자세한 내용은 다음을 참조하십시오. Building applications .

4. 애플리케이션이 생성된 후 요청 시 오케스트레이션을 설정하기 위한 스크립트를 만들 수 있습니다.

주:
새 애플리케이션에 대한 요청 시 오케스트레이션을 설정하려면 스크립트(비즈니스 규칙, UI 작업, 워크플로우 등)에 대한 트리거 스크립팅 및 생성에 대한 고급 기술 지식이 필요합니다. 자세한 내용은 전문 서비스에 문의하십시오 ServiceNow .

보안 인시던트에 정보 추가

보안 인시던트가 생성되면 액세스 역할 및 다양한 종류의 메모와 같은 상세 정보를 추가하여 분석에 도움이 되도록 할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.basic

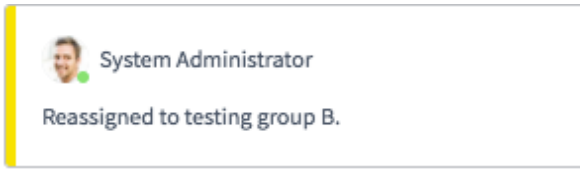
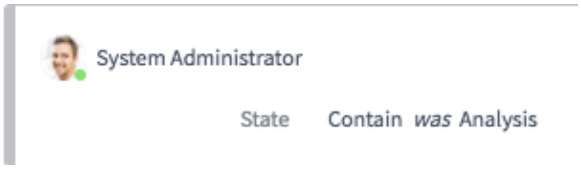
프로시저

1. 아직 열려 있지 않으면 업데이트할 보안 인시던트를 엽니다.
2. 인시던트 상세 정보 탭을 클릭합니다.
3. 필요에 따라, 필드를 채웁니다.

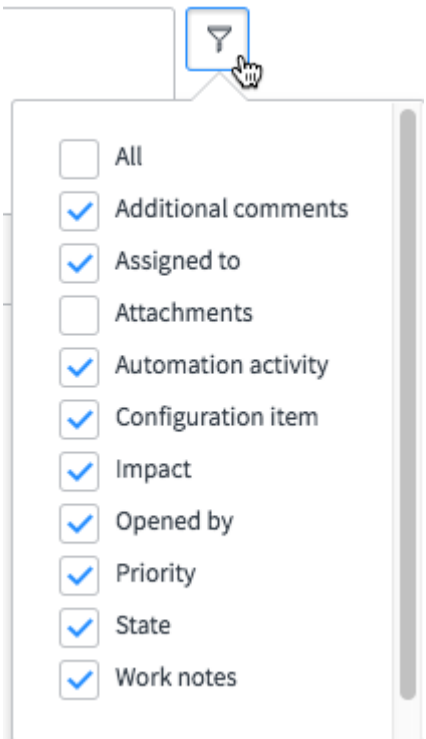
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
읽기 액세스	특수 액세스 역할을 가진 사용자에게 보안 인시던트에 대한 읽기 권한을 부여합니다. 사용자는 작업 메모를 읽고 쓸 수 있습니다. 주: ○ 사용자가 읽기 액세스 및 권한 있는 액세스 목록에 모두 추가되면 권한 있는 액세스 권한만 유지됩니다. ○ sn_si.admin 역할을 가진 사용자는 읽기 액세스와 권한 있는 액세스만 수정할 수 있습니다.
관찰 목록	보안 인시던트에 변경이 발생할 때 알림을 받을 사용자를 추가하려면 자물쇠 아이콘을 클릭합니다. 필드가 잠금 해제된 후에는 여러 사용자를 추가 또는 제거하거나 사용자 이메일 주소를 입력하는 옵션을 사용할 수 있습니다. 입력을 완료했으면 잠금 아이콘을 클릭하여 필드를 잠급니다.
권한 있는 액세스	특수 액세스 역할을 가진 사용자에게 할당 대상을 제외한 보안 인시던트의 모든 필드에 대한 읽기 및 쓰기 권한을 부여합니다. 특수 액세스 역할이 있는 사용자에게는 할당된 모든 보안 인시던트가 포함된 자체 모듈이 있습니다. 다른 모듈은 사용할 수 없습니다. 다른 사람은 나에게 표시 모듈을 볼 수 없습니다. 주: 할당된 사용자 또는 보안 역할(예: sn_si_analyst 또는 sn_si.admin)이 있는 사람만 할당 대상 필드를 변경할 수 있습니다. 사용자가 읽기 액세스 및 권한 있는 액세스 목록에 모두 추가되면 권한 있는 액세스 권한만 유지됩니다.
작업 메모 공유자	 잠금 아이콘( )을 클릭하여 새 작업 메모가 추가될 때 알림을 받는 사용자를 추가합니다. 필드가 잠금 해제된 후에는 여러 사용자를 추가 또는 제거하거나 사용자 이메일 주소를 입력하는 옵션을 사용할 수 있습니다. 입력을 완료했으면 잠금 아이콘을 클릭하여 필드를 잠급니다.
설명	보안 인시던트에 대한 전체 설명과 함께 원인을 찾거나 문제를 해결하는 데 도움이 될 수 있는 정보를 입력합니다.
보안 메모	sn_si.admin 및 sn_si.analyst 역할을 가진 사용자 역할만 보안 메모를 보거나 편집할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
작업 메모	고객에게 표시되지 않는 작업 메모를 입력합니다. 작업 메모가 활동 영역에 나타납니다.
활동	이 보안 인시던트의 관련 기록에 작업 메모에 수동으로 입력한 정보와 동적으로 업데이트되는 모든 작업 활동(작업, 코멘트, 작업 메모 등)을 표시합니다. 작업 메모는 노란색 밴드로 표시됩니다.  자동으로 생성된 메모는 회색 밴드로 표시됩니다. 

4. 필터( ) 아이콘을 클릭하여 활동 필드에 표시되는 정보의 유형을 제한할 수 있습니다.



주:
자동화 활동 확인란을 사용하면 워크플로우 활동, 위험 점수 업데이트 등을 포함하여 이 보안 인시던트에서 수행하는 보강을 포함할 수 있습니다.

5. 다음 탭 중 하나를 클릭하여 보안 인시던트를 추가로 업데이트합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 관련 기록
- 게시 인시던트 검토
- 종결 처리 정보

6. 입력을 완료했으면 제출을 클릭합니다.

보안 인시던트에 관련 문제, 변경 및 인시던트 추가

기존 보안 인시던트에 문제, 변경 사항 및 인시던트와 같은 관련 기록을 추가할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.basic

프로시저

1. 아직 열려 있지 않으면 업데이트할 보안 인시던트를 엽니다.
2. 관련 기록 탭을 클릭합니다.
3. 필요에 따라, 필드를 채웁니다.

필드	설명
문제	이 보안 인시던트가 생성되도록 유발한 근본적인 문제를 해결하는 문제(PRB) 기록을 선택하십시오. 이 인시던트에 대한 PRB는 일반적으로 보안 인시던트 양식 헤더를 마우스 오른쪽 버튼으로 클릭하고 문제 생성을 선택하여 생성됩니다.
상위	이 보안 인시던트를 생성하게 된 근본적인 문제와 관련된 작업 기록을 선택합니다.
상위 보안 인시던트	이 보안 인시던트를 생성하게 된 근본적인 문제와 관련된 보안 인시던트 기록을 선택합니다. 상위 및 하위 보안 인시던트 관계 문서를 참조하십시오.
인시던트	이 보안 인시던트를 생성하게 한 근본적인 문제를 해결하는 인시던트(INC) 기록을 선택합니다. 일반적으로 보안 인시던트 양식 헤더를 마우스 오른쪽 버튼으로 클릭하고 인시던트 생성을 선택하면 인시던트가 생성됩니다.
변경 요청	이 보안 인시던트를 생성하게 된 근본적인 문제를 해결하는 변경 요청(CHG) 기록을 선택합니다. 변경 요청은 일반적으로 보안 인시던트 폼 헤더를 마우스 오른쪽 버튼으로 클릭하고 변경 생성을 선택하여 생성됩니다.

4. 다음 탭 중 하나를 클릭하여 보안 인시던트를 추가로 업데이트합니다.
   - 인시던트 상세 정보
   - 게시 인시던트 검토
   - 종결 처리 정보
5. 입력을 완료했으면 제출을 클릭합니다.

Windows에서 보강된 프로세스에 대한 프로세스 덤프 호출

보안 분석가는 특정 프로세스에서 프로세스 덤프를 실행하고 파일로 덤프한 다음 내부 네트워크의 공유 사이트에 게시할 수 있습니다. 그런 다음 분석가는 보안 인시던트에서 빨간색으로 강조 표시된 거부 목록에 나열된 프로세스를 보고 추가 분석을 수행할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
다음이 필요합니다.

- Windows Vista 이상을 실행하는 클라이언트 또는 Windows Server 2008 이상을 실행하는 서버.
- procdump 실행 파일 경로를 가리키는 시스템 환경 변수와 함께 ProcDump 명령줄 유틸리티가 설치됩니다. 변수의 이름은 PROCDUMP여야 합니다. 이 이름은 powershell 스크립트에 사용됩니다.

필요한 역할: sn_si.analyst

프로시저

1. 를 클릭하여 procdump를 호출할 보강된 프로세스가 있는 보안 인시던트로 이동합니다. 모두 〉 보안 인시던트 〉 열린 인시던트 표시, 보안 인시던트를 엽니다.
2. **Enrichment Data** 탭을 클릭합니다.
3. 실행 중인 프로세스 보강 검색 기록을 클릭합니다.
4. procdump를 수행하려는 실행 중인 프로세스의 확인란을 선택하고 목록 맨 아래에 있는 선택한 행에 대한 작업 드롭다운 목록을 클릭한 다음 **Run Procdump**를 클릭합니다.
   선택한 프로세스에 대해 시작된 **prodump** 워크플로우 메시지가 목록 맨 위에 나타나고 보안 인시던트 응답 **- procdump** 실행 워크플로우가 실행됩니다.

보안 인시던트의 정보 보기

관련 링크를 사용하여 기존 보안 인시던트에 대해 여러 가지 다른 작업을 수행할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.basic

프로시저

1. 아직 열려 있지 않으면 업데이트할 보안 인시던트를 엽니다.
2. 관련 링크 내에서 다음 작업을 수행할 수 있습니다.

옵션	설명
수동 Runbook 보기	이 보안 인시던트에 사용할 수 있는 Runbook 목록을 봅니다.
응답 워크플로우	이 인시던트와 관련된 모든 워크플로우를 봅니다.
복수 옵저버블 추가	옵저버블 목록을 쉼표, 줄 바꿈, 탭 또는 파이프 구분 형식으로 추가합니다.
보안 케이스에 추가	하나 이상의 보안 케이스에 보안 인시던트를 추가합니다. 새 보안 케이스를 생성하고 이 보안 인시던트를 추가할 수도 있습니다.
QRadar IP 요약 가져오기	QRadar 통합을 사용할 수 있고 올바른 CI, 소스 및 대상 IP 주소를 포함하는 경우 QRadar 워크플로우를 트리거하고 결과를 작업 메모에 표시합니다.
오케스트레이션 실행	보안 운영 워크플로우를 선택하고 실행합니다.
View SLA timeline	작업 SLA 기록 또는 SLA 정의에서 SLA 타임라인을 볼 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵션	설명
모든 관련 목록 표시	모든 표준 관련 목록과 수동으로 추가된 모든 목록을 표시합니다. 주: 수동으로 추가한 항목은 이 뷰에서만 사용할 수 있습니다.
영향을 받는 항목 표시	이 인시던트의 직접적인 영향을 받는 CI, 사용자 및 서비스 목록을 표시합니다.
관련 항목 표시	이 인시던트의 영향을 받는 관련 인시던트, CI, 사용자 및 그룹의 목록을 표시합니다.
IoC 표시	이 인시던트와 관련된 옵저버블, 표시기, 맬웨어, 모드 및 방법, 보안 검사 요청 목록을 표시합니다.
보강 데이터 표시	이 인시던트와 관련된 보강 데이터, 프로세스, 서비스, 통계, 조회, 방화벽 로그 및 손상된 사용자 정보 목록을 표시합니다.
응답 작업 표시	이 인시던트와 관련된 작업, SLA, 위험 점수 감사, 중단 및 Exchange 검색 목록을 표시합니다.
외부 시스템에서 상세 정보 보기	이 보안 인시던트가 외부 애플리케이션에서 직접 또는 이벤트에 의해 생성되고 원래 데이터에 대한 링크가 제공된 경우 외부 시스템에서 상세 정보 보기 작업이 URL을 엽니다. 이 인시던트를 생성한 로그를 보고 검색할 수 있습니다.
취약성 스캔	취약성 대응 가 활성화되고 보안 인시던트에 대해 영향을 받는 CI를 하나 이상 선택한 경우 검사 요청을 제출하여 CI에 존재하는 취약성을 확인할 수 있습니다.

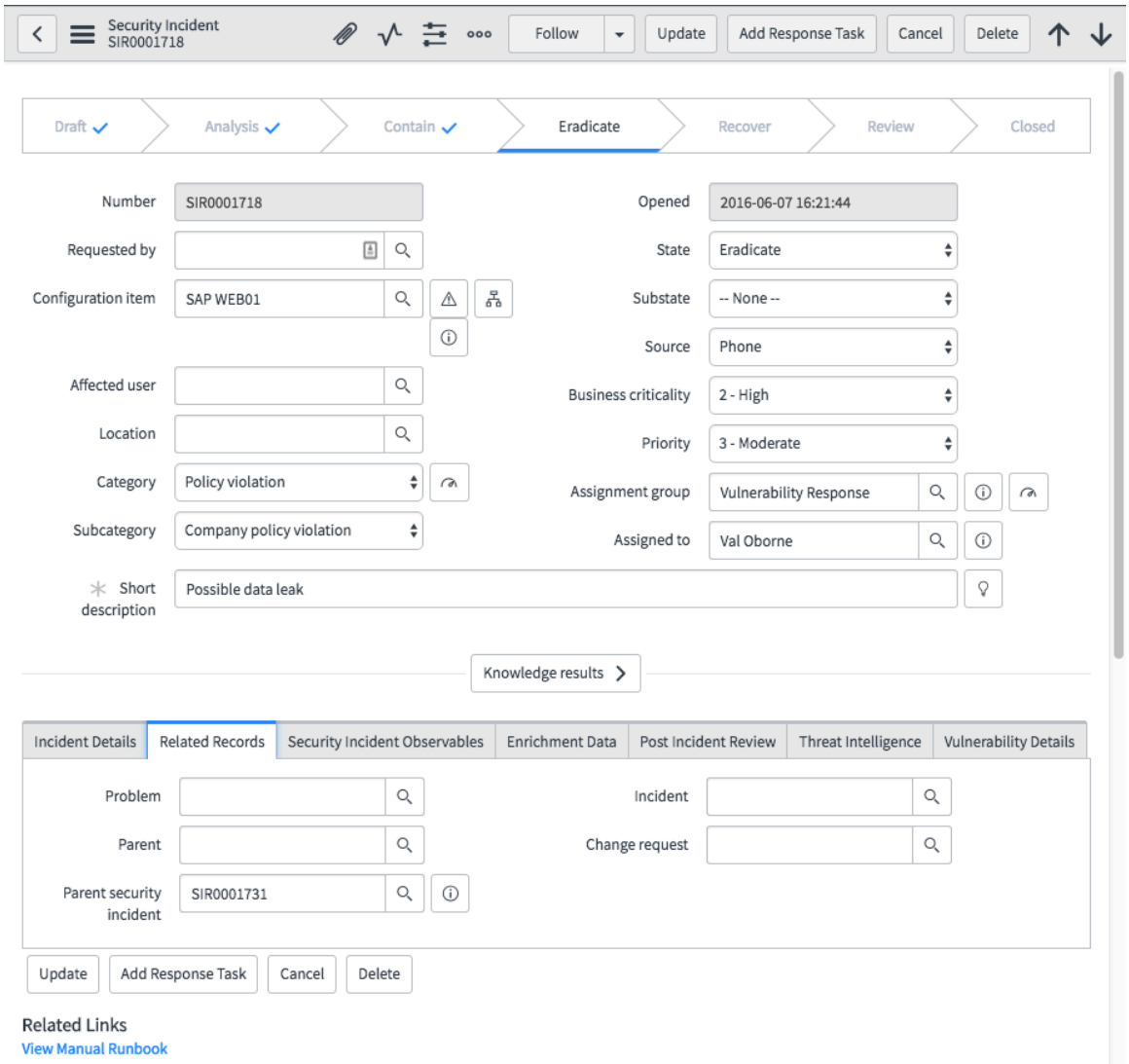
상위 및 하위 보안 인시던트 관계

에서 상위 및 하위 보안 인시던트 관계를 사용하여 지정된 문제의 영향을 연결하고 추적할 수 있습니다 보안 인시던트 응답.

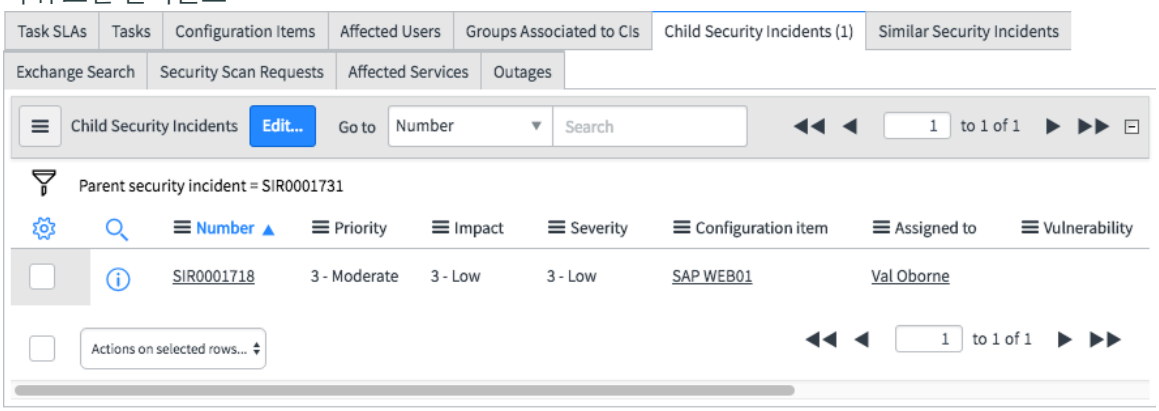
관련 기록 탭을 사용하여 양식에 상위 보안 인시던트 문제를 추가할 수 있습니다보안 인시던트 응답. 이 기능을 사용하면 인시던트가 상위 문제의 관련 목록 - 하위 보안 인시던트 탭에 자동으로 하위 인시던트로 설정됩니다.

주:
두 인시던트에 동일한 번호를 사용하여 기존의 상위 보안 인시던트를 고유한 하위 인시던트로 만들 수 없습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



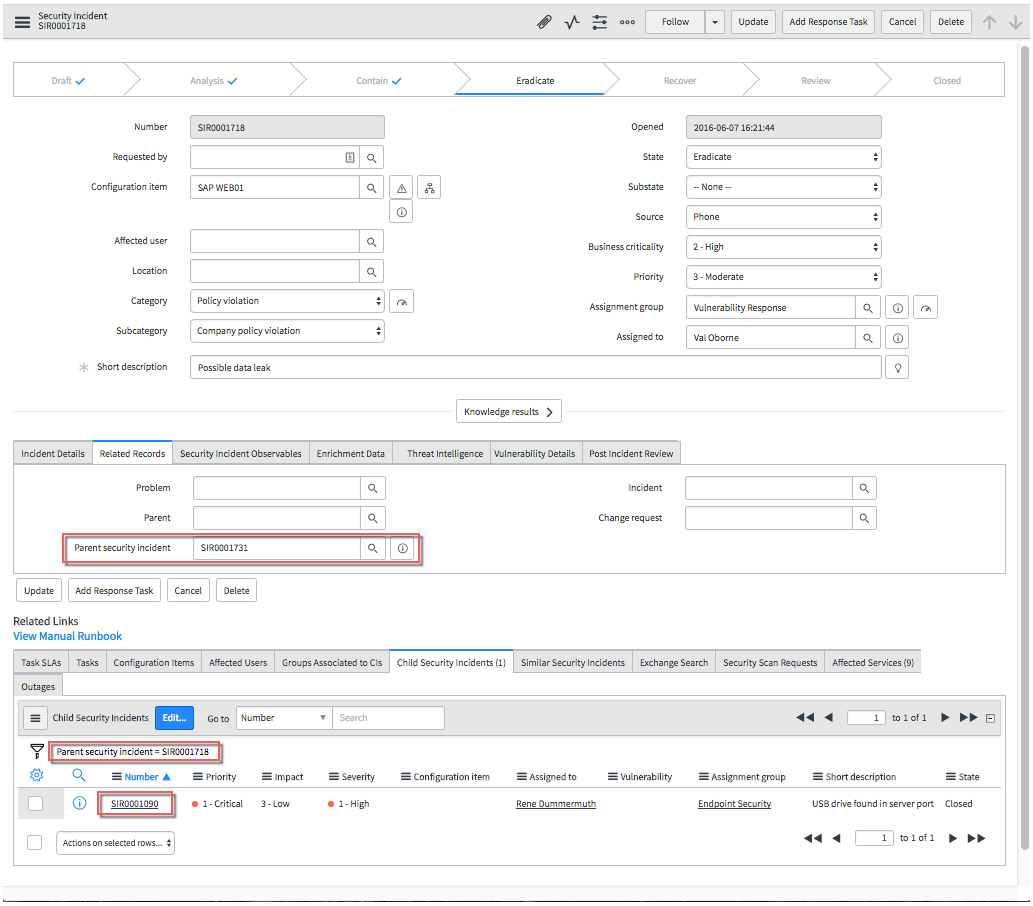
하위 보안 인시던트



하위 보안 인시던트 탭의 편집 버튼을 사용하여 하나 이상의 하위 보안 인시던트를 보안 인시던트 기록에 추가할 수도 있습니다. 다음 예시에서는 세 개의 기록이 모두 연결되어 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

조부모, 부모 및 하위 보안 인시던트



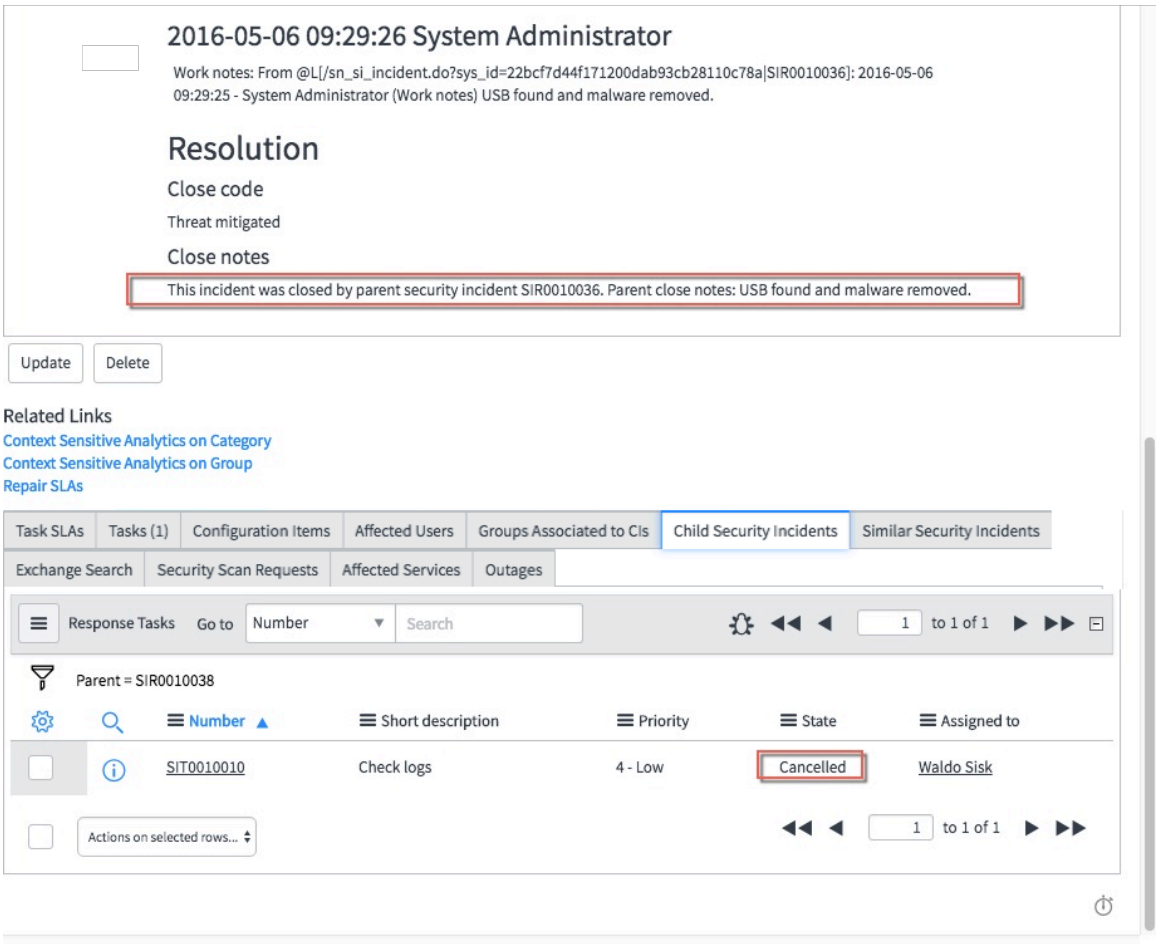
참고:

- 상위에 기록된 모든 작업 메모는 인시던트 상세 정보 탭 아래 활동의 활성 하위 항목으로 전파됩니다.
- 상위 필드는 보안 인시던트를 보안 인시던트 모듈 외부에 있는 중요 인시던트, 문제 또는 변경 요청과 같은 상위 기록과 연결하는 데 사용됩니다. 여러 보안 인시던트를 메인 보안 인시던트로 그룹화하려면 상위 보안 인시던트 필드가 사용됩니다.

상위가 종결되거나 취소되면 활성 하위 항목도 종결되거나 취소됩니다. 하위 인시던트의 활성 응답 작업이 모두 취소됩니다. 열려 있는 다른 작업이 없으면 하위 인시던트가 종결됩니다. 종결되면 사후 인시던트 인터뷰 에서 종결을 기록하고 종결 처리 정보 탭에 있는 정보가 상위에서 하위로 전파됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

하위 응답 작업 닫기



보안 인시던트의 영향을 받는 항목 보기

보안 인시던트와 관련된 CI, 영향을 받는 사용자 및 영향을 받는 서비스 등 영향을 받는 항목을 볼 수 있습니다.

시작하기 전에

필요한 역할: sn_si.basic

프로시저

1. 아직 열려 있지 않으면 영향을 받는 항목을 보려는 보안 인시던트를 엽니다.
2. 영향을 받는 항목 표시 관련 링크를 클릭합니다.
3. 관련 목록을 클릭하여 보안 인시던트에 대한 정보를 보거나 추가합니다.

탭	설명
구성 항목	영향을 받는 CI(구성 항목) 영향을 받는 CI를 식별한 후 이 관련 목록에서 영향을 받는 자원을 수동으로 추가할 수 있습니다.
영향을 받는 사용자	영향을 받는 사용자를 식별한 후 이 관련 목록에서 영향을 받는 사용자를 수동으로 추가할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

탭	설명
영향을 받는 서비스	보안 인시던트와 관련된 비즈니스 서비스를 보거나 추가합니다. 주: 보안 인시던트가 열린 후에 영향을 받는 CI가 추가되면 양식 헤더를 마우스 오른쪽 버튼으로 클릭하고 영향을 받는 서비스 새로 고침을 선택하는 것이 좋습니다.

주:
보안 운영 통합 - 실행 중인 프로세스 가져오기 통합 기능이 활성 상태이고 보안 인시던트에 CI를 추가하면 실행 중인 프로세스 가져오기 워크플로우가 실행되고 CI에서 실행 중인 프로세스 목록을 조회합니다.

보안 운영 통합 - 호스트 격리 통합 기능이 활성 상태인 경우 하나 이상의 CI를 선택하고 시스템 연결을 다른 장치로 제한할 수 있습니다. 이렇게 하려면 CI의 확인란을 선택하고 선택한 행의 작업 선택 목록에서 호스트 격리를 클릭합니다.

4. 보안 인시던트를 추가로 업데이트하려면 다음 관련 링크 중 하나를 클릭하십시오.
   - 관련 항목 표시
   - IoC 표시
   - 보강 데이터 표시
   - 응답 작업 표시
5. 입력을 완료했으면 제출을 클릭합니다.

보안 인시던트에 대한 관련 항목 보기

보안 인시던트와 관련된 유사한 보안 인시던트 및 하위 보안 인시던트, 관련 사용자, 취약성 그룹 및 취약한 항목과 같은 관련 항목을 볼 수 있습니다.

시작하기 전에
필요한 역할: sn_si.basic

프로시저

1. 아직 열려 있지 않으면 관련 항목을 보려는 보안 인시던트를 엽니다.
2. 관련 항목 표시 관련 링크를 클릭합니다.
3. 관련 목록을 클릭하여 보안 인시던트에 대한 정보를 보거나 추가합니다.

탭	설명
하위 보안 인시던트	이 보안 인시던트를 생성하게 한 문제와 관련된 작업 기록을 선택합니다.
유사한 보안 인시던트	동일한 옵저버블 기록과 연결된 다른 보안 인시던트를 봅니다.
관련 구성 항목	이 보안 인시던트와 옵저버블이 동일한 구성 항목이 포함된 보안 인시던트 목록을 표시합니다. 이 목록은 **CI** 제외 필터 그룹을 사용하여 필터링할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

탭	설명
	옵저버블이 보안 인시던트에 추가되면 이 목록이 자동으로 업데이트됩니다. 기본적으로 컨텍스트 유형이 대상인 옵저버블은 제외됩니다.
관련 사용자	이 보안 인시던트와 동일한 옵저버블을 가진 사용자가 포함된 보안 인시던트 목록을 표시합니다. 이 목록은 사용자 제외 필터 그룹을 사용하여 필터링할 수 있습니다. 옵저버블이 보안 인시던트에 추가되면 이 목록이 자동으로 업데이트됩니다. 기본적으로 컨텍스트 유형이 대상인 옵저버블은 제외됩니다.
관련 필터 그룹	구성 항목이 확인되면 일치하는 CI 또는 필터 그룹이 자동으로 추가됩니다.
취약성 그룹	취약성 대응 가 활성화되면 이 보안 인시던트와 관련된 취약성 그룹을 볼 수 있습니다.
취약 항목	취약성 대응 가 활성화되면 이 보안 인시던트와 관련된 취약성 항목을 볼 수 있습니다.
위험	핵심 위험 관리 플러그인(정책 및 준수 관리, 감사, 관리 또는 위험 관리)이 활성화되면 보안 인시던트와 관련된 위험을 보거나 추가할 수 있습니다. 아래의 양식 헤더 컨텍스트 메뉴에서 이 관련 목록을 추가할 수 있습니다. 구성 〉 관련 목록.
구성 항목 이벤트	이벤트 관리 가 활성화되면 이벤트를 볼 수 있습니다.
구성 항목 경보	이벤트 관리 가 활성화되면 경보를 볼 수 있습니다.
고객 서비스 케이스	고객 서비스 가 활성화되면 케이스 정보를 볼 고객 서비스 수 있습니다.

4. 보안 인시던트를 추가로 업데이트하려면 다음 관련 링크 중 하나를 클릭하십시오.
   - 영향을 받는 항목 표시
   - IoC 표시
   - 보강 데이터 표시
   - 응답 작업 표시
5. 입력을 완료했으면 제출을 클릭합니다.

보안 인시던트에 대한 보강 데이터 보기

실행 중인 프로세스, 실행 중인 서비스 및 보안 인시던트와 관련된 네트워크 통계와 같은 보강 데이터를 볼 수 있습니다.

시작하기 전에
필요한 역할: sn_si.basic

프로시저

1. 아직 열려 있지 않으면 보강 데이터를 보려는 보안 인시던트를 엽니다.
2. 보강 데이터 표시 관련 링크를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 관련 목록을 클릭하여 보안 인시던트에 대한 정보를 보거나 추가합니다.

   주:
   원시 데이터 상세 정보는 보강 데이터 기록의 첨부 파일에 저장됩니다. 필드 한도를 초과하면 표시된 상세 정보가 잘립니다.

탭	설명
실행 중인 프로세스	보안 인시던트 응답 실행 중인 프로세스 가져오기 워크플로우에서 만든 기록을 저장합니다.
운영 서비스	보안 인시던트 응답 실행 중인 서비스 가져오기 워크플로우로 생성된 기록을 저장합니다.
네트워크 통계	보안 인시던트 응답 네트워크 통계 가져오기 워크플로에서 만든 레코드를 저장합니다.
도메인 조회	플러그인이 WhoisXML API Integration 활성화되면 Whois 조회로 작성된 기록이 저장됩니다.
방화벽 로그	Palo Alto Network 방화벽 로그와 같은 방화벽 로그의 보강 데이터를 저장합니다.
손상된 사용자 정보	Have I Been Pwned?를 통해 손상된 것으로 확인된 계정을 저장합니다. 조회.

   참고: **Security Enrichment** Data(보안 보강 데이터) 탭에는 네트워크 통계 검색 또는 실행 중인 프로세스와 같은 워크플로우의 보안 인시던트 응답 원시 보강 데이터가 표시됩니다. 이 탭은 모든 관련 목록 표시 관련 링크를 클릭하여 볼 수 있습니다.

4. 보안 인시던트를 추가로 업데이트하려면 다음 관련 링크 중 하나를 클릭하십시오.
   - 영향을 받는 항목 표시
   - 관련 항목 표시
   - IoC 표시
   - 응답 작업 표시
5. 입력을 완료했으면 제출을 클릭합니다.

보안 인시던트에 대한 응답 작업 정보 보기

보안 인시던트와 연관된 작업 SLA, 위험 점수 감사 및 중단과 같은 응답 작업 정보를 볼 수 있습니다.

시작하기 전에
필요한 역할: sn_si.basic

프로시저

1. 아직 열려 있지 않으면 응답 작업을 보려는 보안 인시던트를 엽니다.
2. 응답 작업 표시 관련 링크를 클릭합니다.
3. 관련 목록을 클릭하여 보안 인시던트에 대한 정보를 보거나 추가합니다.

탭	설명
작업	보안 인시던트에 대해 이미 정의된 작업을 표시합니다. 응답 작업을 수동으로 생성할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

탭	설명
응답 작업	보안 인시던트에 대응하여 수행할 작업을 표시합니다.
작업 SLA	보안 인시던트에 대해 정의된 활성 작업 SLA를 보거나 추가합니다.
위험 점수 감사	변경되는 위험 점수의 각 인스턴스에 대한 감사 기록입니다.
중단	보안 인시던트와 관련된 새 중단 기록을 보거나 수동으로 추가합니다.
이메일 검색	설치된 구현에 따라 Microsoft# Exchange Server와 같은 이메일 서버에서 쿼리를 실행하기 위한 검색 기준을 포함하고 받은 결과를 저장하는 기록 목록입니다. 주: 이(가 보안 운영 통합 - 이메일 검색 및 삭제 기능) 활성 상태가 아니면 이메일 검색 관련 링크가 표시되지 않습니다.

4. 보안 인시던트를 추가로 업데이트하려면 다음 관련 링크 중 하나를 클릭하십시오.
   - 영향을 받는 항목 표시
   - 관련 항목 표시
   - IoC 표시
   - 보강 데이터 표시
5. 입력을 완료했으면 제출을 클릭합니다.

보안 인시던트의 관련 이벤트 및 경보 보기

보안 인시던트를 처리하는 동안 이벤트의 상세 정보를 볼 수 있습니다. 경보의 경우 이러한 경보를 확인 및 확인하고, 필요한 경우 경보에서 인시던트 또는 보안 인시던트를 만들 수 있습니다.

시작하기 전에

보안 인시던트 응답 이벤트 관리 지원 플러그인이 활성화되어 있어야 합니다.

필요한 역할: si.sn_agent

프로시저

1. 보안 인시던트 목록(예: 모두 〉 보안 인시던트 〉 인시던트 〉 미할당 인시던트).
2. 보고 있는 보안 인시던트의 영향을 받는 자원이 지난 24시간 내에 경보 또는 이벤트를 수신한 경우 다음 관련 목록 중 하나 또는 둘 모두가 나타납니다.
   - 보안 인시던트 CI 경보
   - 보안 인시던트 CI 이벤트
3. 보려는 관련 목록을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관련 목록	설명
보안 인시던트 CI 경보	지난 24시간 내에 받은 경보에 대한 상세 정보를 볼 수 있습니다. 확인을 클릭하여 경보를 인지하고 있으며 경보가 처리 중임을 나타낼 수 있습니다. 닫기를 사용하여 경보가 중요하지 않음을 나타냅니다.
보안 인시던트 CI 이벤트	지난 24시간 내에 받은 이벤트에 대한 상세 정보를 볼 수 있습니다.

고객 서비스 케이스 매핑에 대한 보안 인시던트 보기

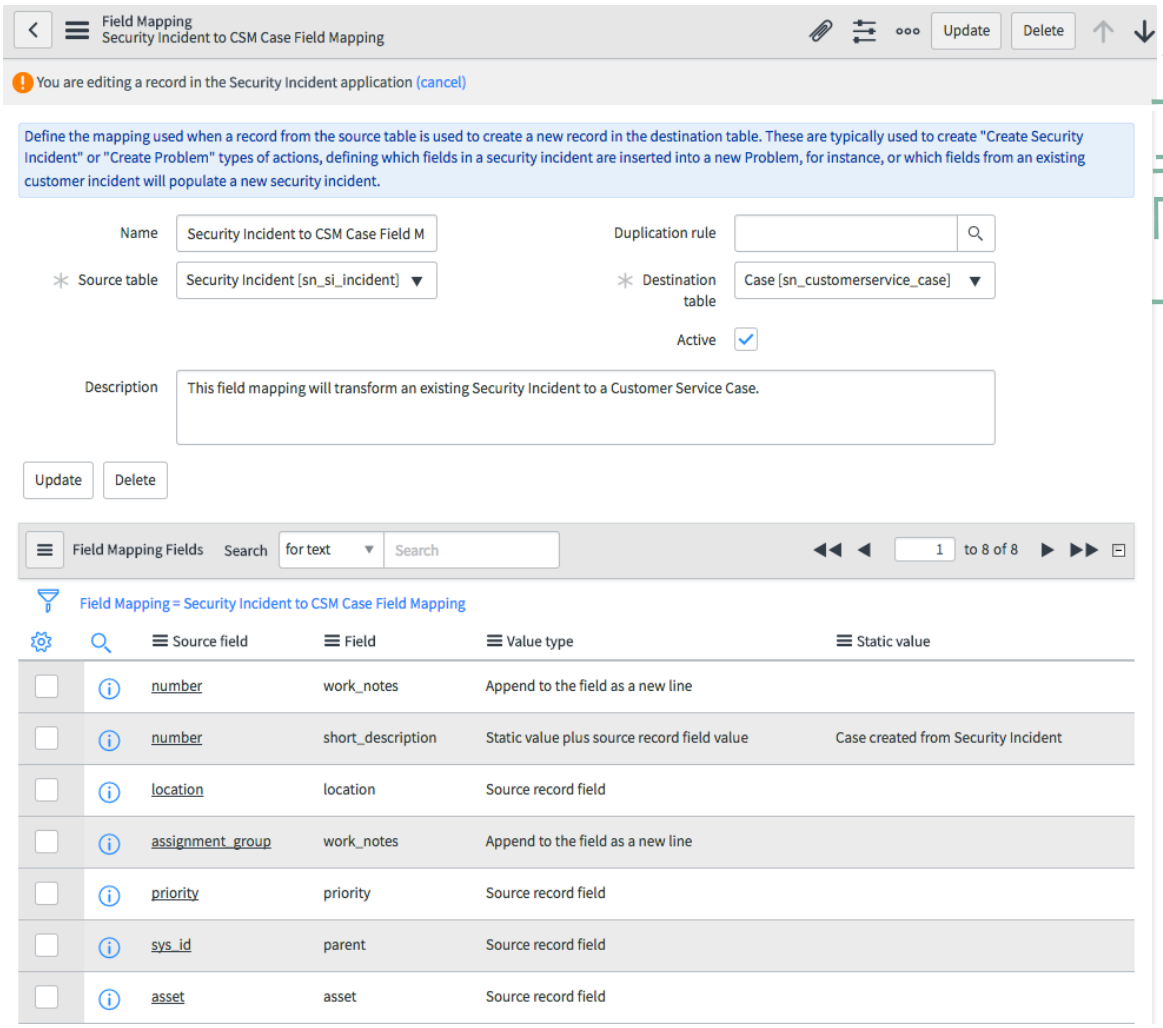
보안 인시던트 응답 은 보안 인시던트를 케이스에 고객 서비스 매핑하는 기본 필드 매핑과 함께 제공됩니다. CS 케이스 기본 맵에 대한 보안 인시던트를 볼 수 있습니다.

시작하기 전에

필요한 역할: sec_cmn.read

프로시저

1. 다음으로 이동 모두 〉 보안 운영 〉 유틸리티 〉 필드 매핑.
2. 기본 맵을 보려면 보안 인시던트와 **CSM** 케이스 필드 매핑 을 클릭하십시오.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 필요한 경우 매핑을 편집할 수 있습니다.
4. 변경을 완료했으면 업데이트를 클릭합니다.

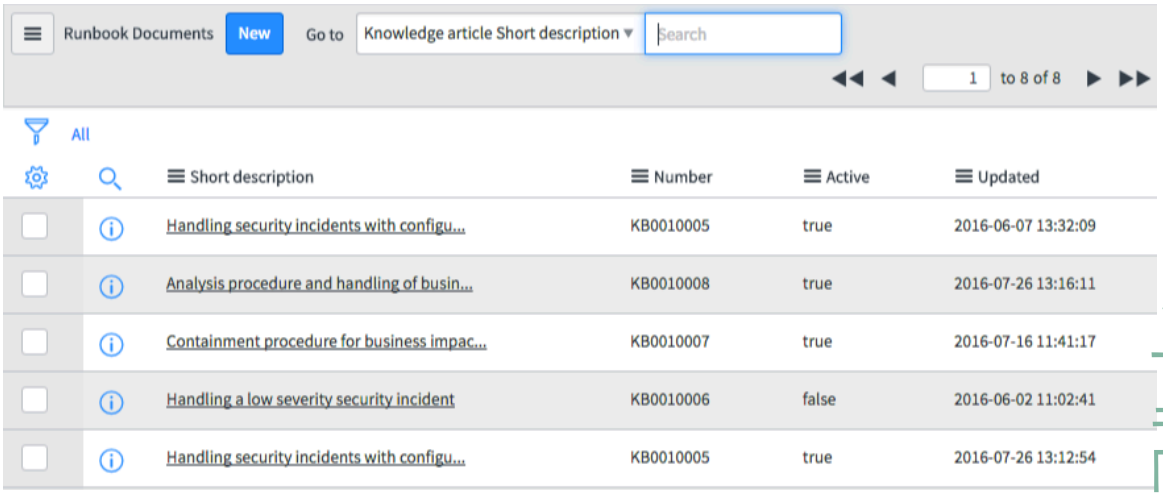
보안 인시던트 응답 Runbook 보기

Runbook을 사용하면 작업 중인 작업과 관련된 절차에 액세스할 수 있습니다.

시작하기 전에
필요한 역할: sn.si.knowledge_admin

프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 수동 **Runbook** 〉 **Runbook** 문서 보기.
2. 목록에서 Runbook을 선택합니다.



3. Runbook을 만들려면 새로 만들기를 클릭합니다.
   자세한 내용은 Runbook 만들기를 참조하세요.

보안 인시던트의 영향을 받는 모든 구성 항목 식별

보안 인시던트의 원인이 되는 자원(서버, 데스크톱 또는 기타 구성 항목)을 알고 있고 영향을 받을 수 있는 관련 자원 및 비즈니스 서비스를 식별하려는 경우 비즈니스 서비스 관리(BSM) 맵을 사용할 수 있습니다.

시작하기 전에
필요한 역할: admin 또는 sn_si.admin

이 태스크 정보
BSM 맵은 선택한 루트 CI의 업스트림과 다운스트림 의존성을 표시합니다.

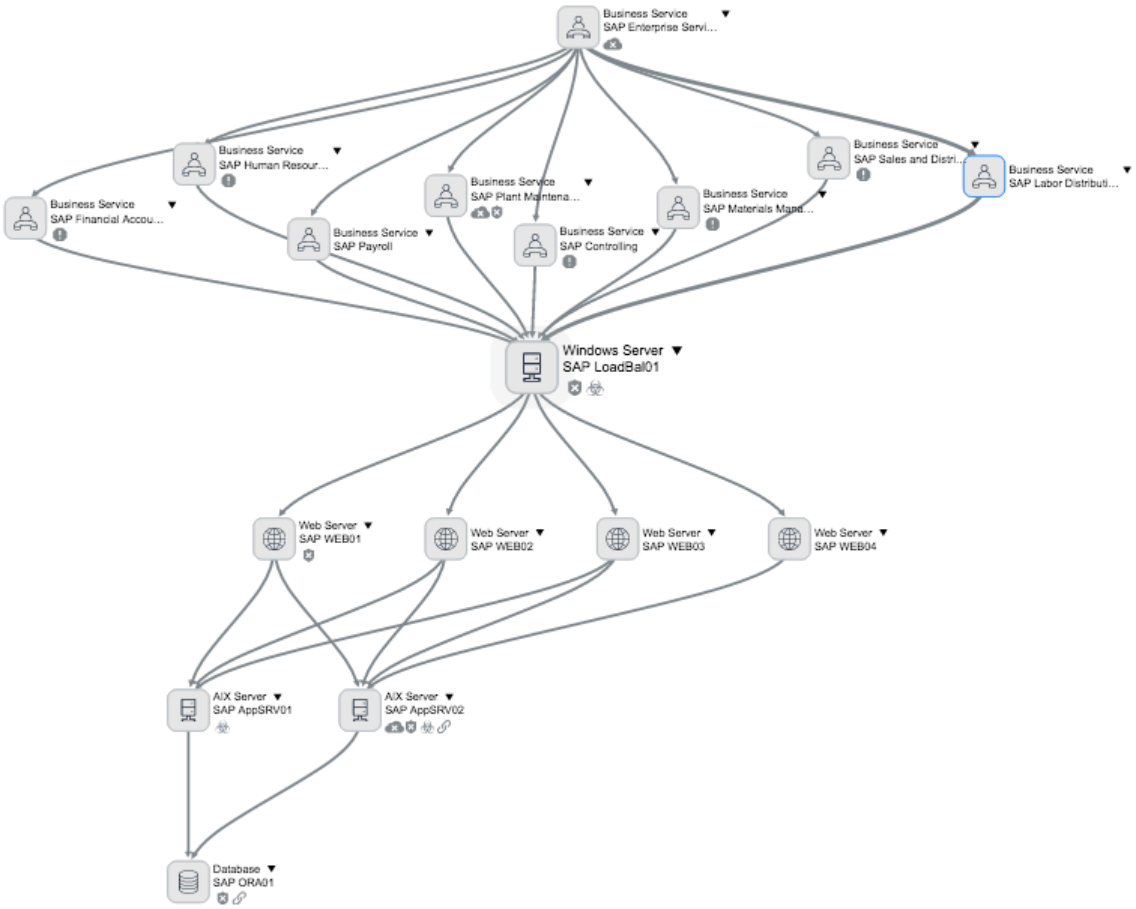
CI에 대한 BSM 맵을 보는 데 사용할 수 있는 두 가지 방법이 있습니다.

- 작업의 컨텍스트에서 CI를 보려면 보안 인시던트 양식에서 봅니다.
- 작업 관점에서 CI를 않으려면 탐색 모음에서 봅니다.

프로시저

1. 보안 인시던트 양식에서 구성 항목 필드를 채우고 BSM 맵 아이콘( )을 클릭합니다.
   BSM 맵 화면에는 인시던트 관리에서 액세스한 마지막 인시던트 또는 보안 인시던트 관리에서 액세스한 마지막 보안 인시던트에 대한 맵이 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



2. 자원(서버, 데스크톱 또는 기타 CI)에 대한 여러 종류의 상세 정보를 보려면 구성 항목 옆에 있는 아이콘을 클릭합니다.
   예를 들어 (⚠)을 클릭하여 CI와 연결된 경보를 봅니다.

   주:
   사용 가능한 모든 아이콘의 목록을 보려면 BSM 맵 위의 필터를 클릭하고 필터 작업 유형을 펼치십시오.

3. 맵을 다양한 구성으로 정렬하려면 맵 위에 나열된 형식(세로, 가로, 방사형)을 선택하거나 필터를 클릭하여 쉽게 볼 수 있도록 맵을 필터링합니다.
4. 보안 인시던트 양식에서 BSM 맵을 연 경우 CI를 마우스 오른쪽 버튼으로 클릭하고 영향을 받는 **CI** 추가를 선택하여 종속 CI를 보안 인시던트에 추가할 수 있습니다.
   한 번에 여러 CI를 추가할 수도 있습니다. 추가할 CI 주위의 상자를 끌고 마우스 오른쪽 상자를 클릭한 다음 영향을 받는 **CI** 추가를 선택합니다.
   CI가 보안 인시던트의 영향을 받는 CI 관련 목록에 추가됩니다.

보안 인시던트 심각도 계산

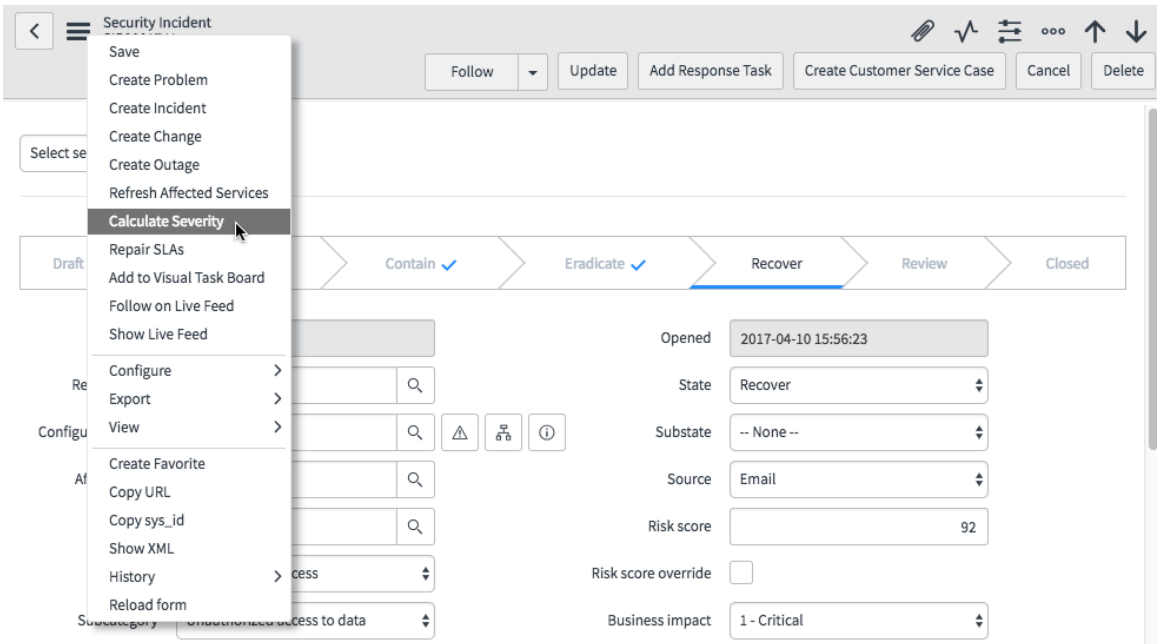
미리 정의된 계산기를 사용하여 보안 인시던트의 심각도를 계산할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.basic

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 아직 열려 있지 않으면 심각도를 계산할 보안 인시던트를 엽니다.
2. 양식 헤더 컨텍스트 메뉴를 클릭하고 심각도 계산을 선택합니다.



심각도는 기본 계산기에 대해 미리 정의된 규칙에 따라 계산됩니다. 자세한 내용은 보안 인시던트 계산기 이해 문서를 참조하십시오.

피싱 이메일 검색 및 삭제

피싱 이메일을 삭제하면 조직 전체에서 특정 공격에 대한 노출을 줄이는 데 도움이 될 수 있습니다. 이메일 서버에서 피싱 이메일을 검색, 승인 및 삭제하여 관리할 수 있습니다.

시작하기 전에

필요한 역할: sn_sec_cmn.cap_email_read

보안 인시던트와 연결된 이메일 기록을 쿼리하여 피싱 공격의 대상이 된 사용자 수를 확인할 수 있습니다.

지원되는 소프트웨어:

- 마이크로소프트# 익스체인지 서버 2010

제한: 이메일 본문을 검색할 때 최대 1,500개의 사서함을 검색할 수 있습니다.

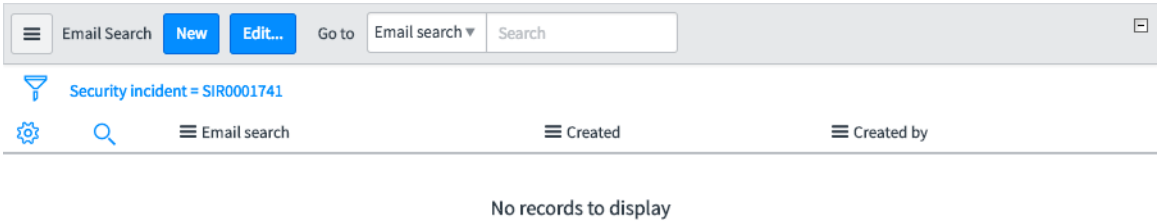
이 태스크 정보

이 기능은 이메일 Security Operations Integration - 이메일 검색 및 삭제 플로우 서버에 대해 쿼리를 실행하는 데 사용됩니다. 선택한 검색 기준에 따라 검색은 피싱 공격 내의 모든 이메일을 식별하고 영향을 받는 총 이메일 수 또는 영향을 받는 이메일의 상세 정보를 반환합니다.

프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 열린 인시던트 표시.
2. 보안 인시던트를 선택합니다.
3. 이메일 검색 관련 목록이 표시되지 않으면 모든 관련 링크 표시 관련 링크를 클릭합니다.
4. 이메일 검색 관련 목록을 클릭합니다.

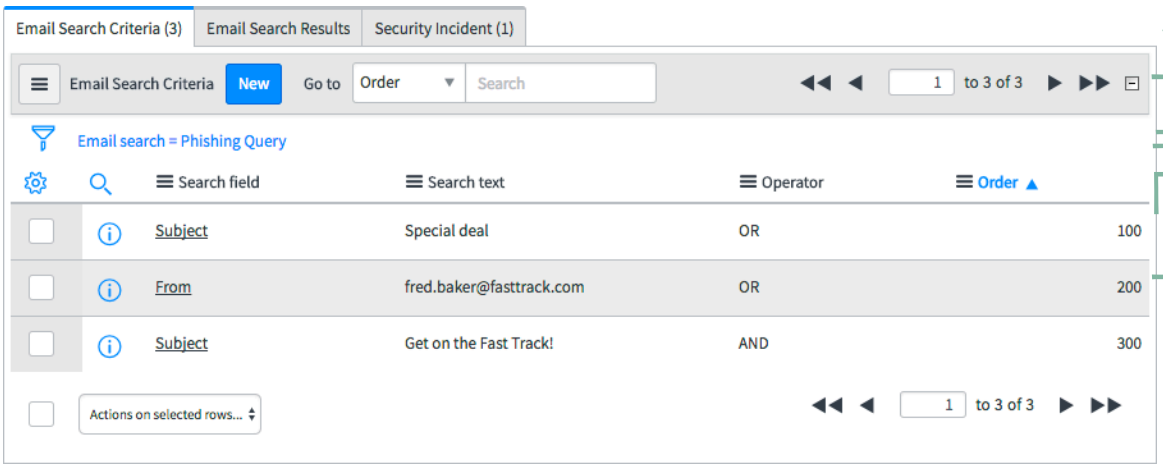
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



5. 새로 만들기를 클릭합니다.
6. 필드에 적절하게 입력합니다.

필드	설명
이름	검색 쿼리의 이름
기준 쿼리	이메일 서버에서 실행되는 쿼리의 미리 보기입니다. 연결된 모든 활성 검색 기준 기록에서 생성됩니다.
설명	검색 쿼리가 무엇을 찾고 있는지 설명합니다.

7. 양식 헤더를 마우스 오른쪽 버튼으로 클릭하고 저장을 선택합니다.



8. 이메일 검색 기준 탭을 클릭하고 신규를 클릭합니다.
9. 필요에 따라 필드를 입력하거나 편집합니다.

필드	설명
이메일 검색	이메일 검색의 이름을 표시합니다. 필요한 경우 변경할 수 있습니다.
검색 필드	이메일 서버에서 검색할 필드입니다. 검색 필드에는 다음 선택 사항이 있습니다. 제목 이 기준은 검색 텍스트 필드에 지정된 제목 라인 텍스트를 포함하는 이메일을 검색합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

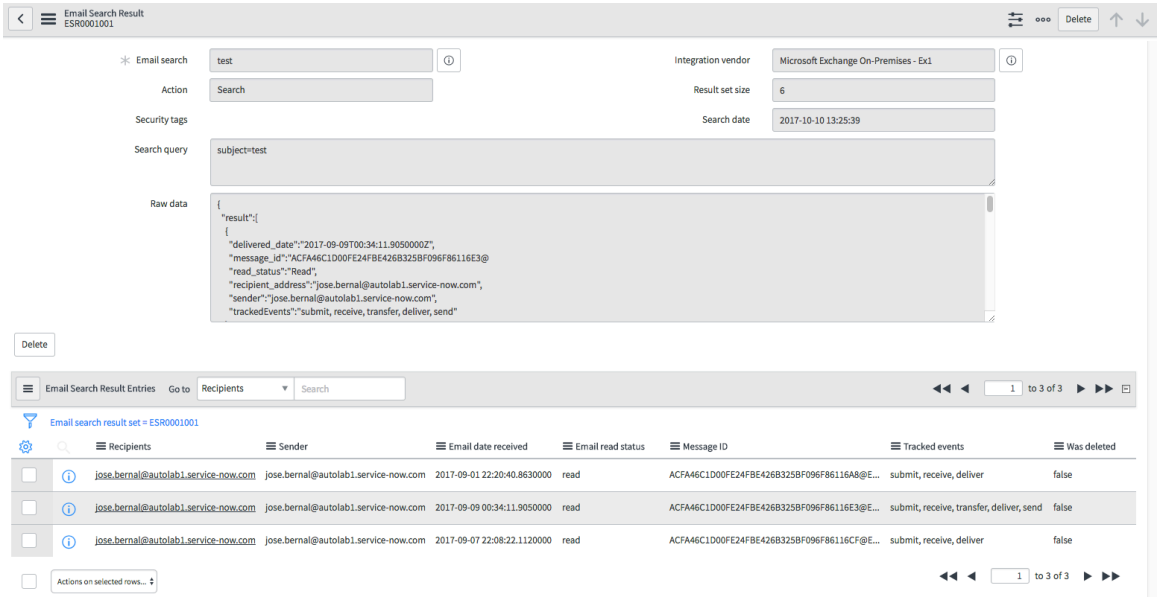
필드	설명
	이 검색 기준을 충족하는 이메일의 경우 총 피싱 이메일 수와 받은 이메일 날짜, 이메일 읽음 상태, 수신자 및 메시지 ID를 포함한 각 이메일의 상세 정보가 반환됩니다. 시작일 이 기준은 검색 텍스트 필드에 지정된 보낸 사람의 전체 이메일 주소(예: jane.doe@abc.com)가 포함된 이메일을 검색합니다. 이 검색 기준을 충족하는 이메일의 경우 총 피싱 이메일 수와 받은 이메일 날짜, 이메일 읽음 상태, 수신자 및 메시지 ID를 포함한 각 이메일의 상세 정보가 반환됩니다. 주: 같은 쿼리에서 보낸 사람 및 수신자 필드를 사용할 수 없습니다. 수신자 이 기준은 검색 텍스트 필드에 지정된 수신자의 전체 이메일 주소(예: john.doe@abc.com)가 포함된 이메일을 검색합니다. 또한 받는 사람, 참조 및 숨은 참조 필드에서 이메일을 검색합니다. 이 검색 기준을 충족하는 이메일의 경우 총 피싱 이메일 수와 받은 이메일 날짜, 이메일 읽음 상태, 수신자 및 메시지 ID를 포함한 각 이메일의 상세 정보가 반환됩니다. 주: 같은 쿼리에서 보낸 사람 및 수신자 필드를 사용할 수 없습니다. 본문 이 기준은 검색 텍스트 필드에 지정된 본문 텍스트가 포함된 이메일을 검색합니다. 이 검색 기준을 충족하는 이메일의 경우 총 피싱 이메일 수가 반환됩니다. 주: 이메일 본문을 검색할 때 최대 1,500개의 사서함을 검색할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	참조: 이 기준은 검색 텍스트 필드에 지정된 참조 전체 이메일 주소(예: jane.doe@abc.com)가 포함된 이메일을 검색합니다. 이 검색 기준을 충족하는 이메일의 경우 총 피싱 이메일 수가 반환됩니다. 숨은 참조: 이 기준은 검색 텍스트 필드에 지정된 숨은 참조 전체 이메일 주소(예: jane.doe@abc.com)를 포함하는 이메일을 검색합니다. 이 검색 기준을 충족하는 이메일의 경우 총 피싱 이메일 수가 반환됩니다. 첨부 파일 이 기준은 검색 텍스트 필드에 지정된 첨부 파일 이름 또는 첨부 파일 내용이 포함된 이메일을 검색합니다. 이 검색 기준을 충족하는 이메일의 경우 총 피싱 이메일 수가 반환됩니다. 주: 첨부 파일 내용을 검색할 때는 일반 텍스트 첨부 파일만 지원됩니다. 유지 보험 이 기준은 검색 텍스트 필드에 지정된 보존 정책 번호가 포함된 이메일을 검색합니다. 이 검색 기준을 충족하는 이메일의 경우 총 피싱 이메일 수가 반환됩니다.
활성	이 이메일 검색 쿼리를 활성화하려면 이 확인란을 선택합니다.
운영자	가능한 값은 AND 및 OR입니다. 검색 조건을 결합하여 이메일 서버에서 실행하는 방법을 정의할 수 있습니다.
순서	검색 기준에서 검색 쿼리가 작성되는 순서입니다.
검색 텍스트	검색할 텍스트입니다. 작은따옴표, 큰따옴표 및 콜론은 지원되지 않습니다.

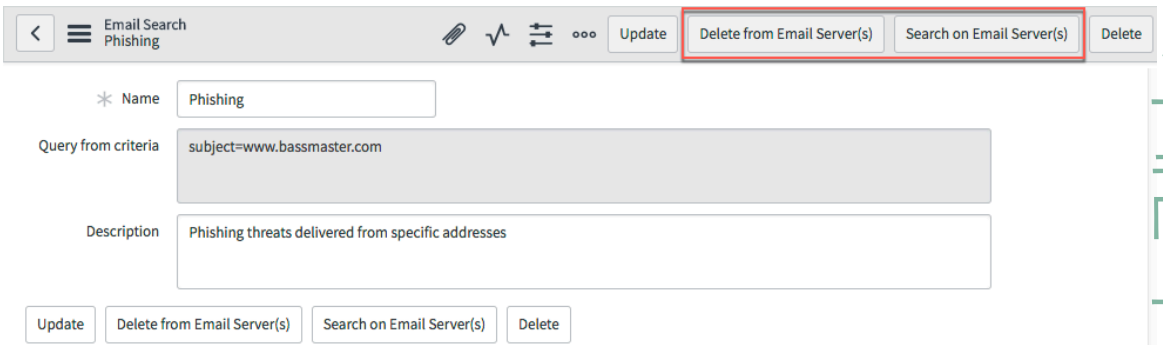
10. 제출을 클릭합니다.
11. 추가 검색 기준을 정의하려면 필요한 만큼 반복합니다.
12. 이메일 검색 결과 탭을 클릭하여 검색 결과를 볼 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



이메일 검색 결과 항목 양식의 각 줄은 개별 이메일을 나타냅니다.

13. 검색 기준 기록을 생성하면 이메일 검색 양식에 두 개의 버튼, 즉 이메일 서버에서 삭제 와 이메일 서버에서 검색이 표시됩니다.



14. 선택한 서버에서 정의한 검색 기준을 충족하는 이메일을 검색하려면 이메일 서버에서 검색을 클릭합니다.

보안 인시던트 지식 문서 생성

보안 인시던트 및 응답 작업을 수행할 때 수행 중인 작업에 대한 관련 정보를 제공하는 지식 문서가 자동으로 표시됩니다. 조직은 보안 인시던트 지식베이스에서 문서를 만들고 유지관리할 수 있습니다.

시작하기 전에

필요한 역할: sn_si.knowledge_admin

이 태스크 정보

지식 문서는 보안 정보를 공유하고, 조직이 직면한 사이버 위협의 유형을 문서화하며, 이러한 위협에 대한 답변과 대응을 제공합니다.
필요한 경우 지식 문서를 Runbook으로 구성하여 문서와 특정 작업 간의 연결을 생성할 수 있습니다. 예를 들어 피싱 공격에 대한 보안 인시던트를 생성할 때 피싱에 대한 지식베이스 문서가 표시되도록 하는 조건으로 Runbook을 구성할 수 있습니다. 자세한 내용은 보안 인시던트 응답 Runbook 생성 문서를 참조하십시오.

Runbook의 지식 문서는 Playbook의 특정 작업과도 연결할 수 있습니다. 자세한 내용은 지식 문서를 플레이북 작업과 연결 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

지식 문서의 이점은 다음과 같습니다.

- 직원은 검색하기 쉬운 정보 소스를 보유합니다.
- 지식 문서는 작성, 검토 및 업데이트, 게시, 폐기에 이르는 수명주기가 정의되어 있으므로 정보를 최신 상태로 유지할 수 있습니다.
- 보안 요청, 인시던트 또는 응답 작업을 수동으로 생성하는 경우 짧은 설명을 입력하면 관련 문서 목록이 표시됩니다.

주:
각 보안 인시던트 지식베이스에 지식 관리자를 할당하는 것이 중요합니다.

프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 카탈로그 및 지식베이스 〉 지식.
2. 문서 생성 아이콘( )을 클릭합니다.
3. 양식의 필드에 적절히 입력합니다.

Knowledge 양식

필드	설명
번호	자동으로 생성된 KB 번호입니다.
지식베이스	이 문서에 대해 선택된 지식베이스입니다.
범주	이 문서의 범주입니다.
게시 날짜:	이 지식 문서가 게시된 시기입니다. 이 값은 문서 생성 시 설정되며 문서가 게시될 때 업데이트됩니다.
유효 기간(종료)	이 지식 문서가 만료되는 시기입니다. 이 문서는 이 날짜 이후 또는 날짜를 선택하지 않은 경우 검색 결과에 표시되지 않습니다.
이미지	레거시 지식 포털에서 검색할 때 문서 옆에 나타나는 이미지입니다.
워크플로우	〔읽기 전용〕 초안 또는 게시됨 등의 문서 게시 상태입니다. 시기 기존 문서에서 새 문서를 삽입하면 새 문서의 상태가 초안으로 재설정됩니다.
소스	이 지식 문서가 응답하여 생성된 작업입니다(있는 경우). 이 필드는 작업 기록에서 지식 문서를 생성할 때 자동으로 설정됩니다.
첨부 파일 링크	사용자가 문서에 액세스할 때 문서 보기를 열지 않고 첨부 파일을 자동으로 다운로드하는 확인란입니다. 이 옵션을 사용하려면 문서에 첨부 파일을 추가합니다.
첨부 파일 표시	이 지식 문서를 보는 사용자에게 첨부 파일을 표시하는 확인란입니다. 첨부 파일은 문서 텍스트 아래에 표시됩니다. 이 옵션을 사용하려면 문서에 하나 이상의 첨부 파일을 추가합니다.
간단한 설명	문서의 제목입니다. 이 제목은 지식을 탐색하고 검색할 때, 그리고 문서 상단에 표시됩니다.
텍스트	문서의 내용입니다. 컨텐츠를 작성하려면 WYSIWYG HTML 편집기를 사용하십시오. 지식을 탐색하고 검색할 때 컨텐츠의 미리 보기가 나타납니다.

주:
플레이북 작업에 연결할 지식 문서를 생성하는 경우 지식베이스 필드를 보안 인시던트 응답 **Runbook**으로 설정합니다.

4. 제출을 클릭하여 문서를 생성합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 수행할 작업
승인과 같이 문서를 게시하는 데 필요한 추가 단계는 지식베이스에 대한 게시 워크플로우 입니다.

관련 정보

보안 인시던트 응답 Runbook 생성

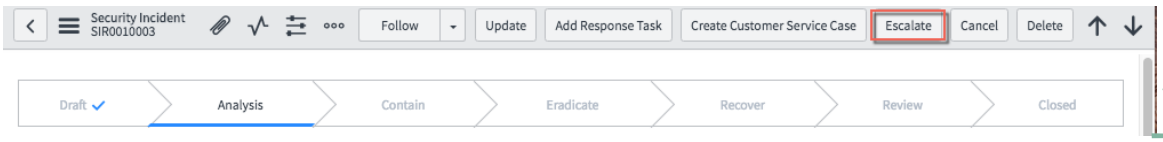
보안 인시던트 에스컬레이션

보안 인시던트에 대한 에스컬레이션 경로가 존재하는 경우 보안 인시던트 헤더에서 에스컬레이션 버튼을 사용할 수 있습니다.

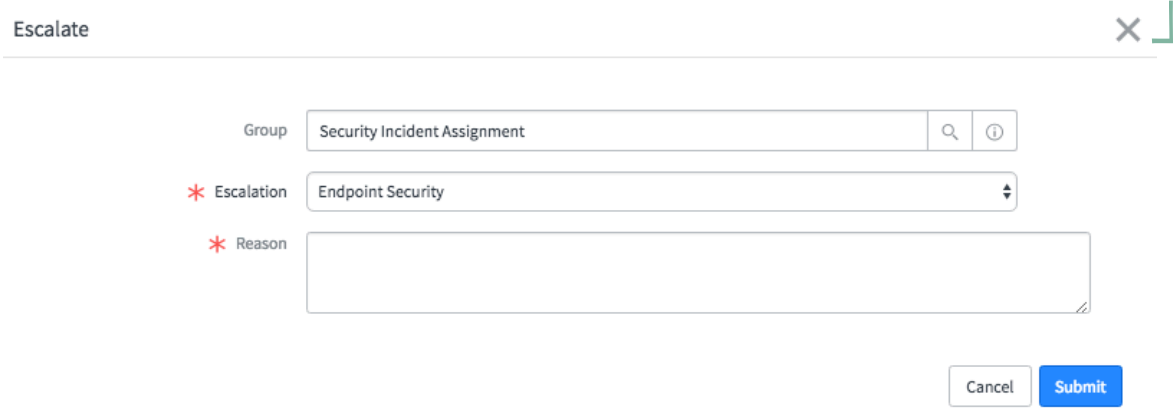
시작하기 전에
필요한 역할: sn_si.admin
이 버튼을 보려면 생성된 에스컬레이션 그룹이 있어야 합니다. 자세한 내용은 보안 운영 사용자 정의 에스컬레이션 그룹 생성 문서를 참조하십시오.

프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 열린 인시던트 표시.
2. 에스컬레이션할 인시던트를 엽니다.
3. 에스컬레이션 버튼을 클릭합니다.



4. 에스컬레이션 그룹을 선택합니다.
5. 에스컬레이션 사유를 입력합니다.



6. 제출을 클릭합니다.
   보안 인시던트에서 할당 그룹 및 할당 대상을 업데이트합니다.

사후 인시던트 활동 관리

비즈니스 요구 사항에 따라 원본 검토와 보안 인시던트 처리가 주로 필요합니다.

게시 인시던트 검토 의 ServiceNow 기능은 이 프로세스를 자동화, 추적, 감사 및 간소화하기 위한 다양한 도구를 제공합니다.

이 섹션에서는 다음 사항에 대해 설명합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 사후 인시던트 검토 역할 할당
- 평가 트리거 조건 구성
- 질문서 기반 사후 인시던트 검토 수행
- PIR 담당 규칙 생성
- 사후 인시던트 검토 보고서

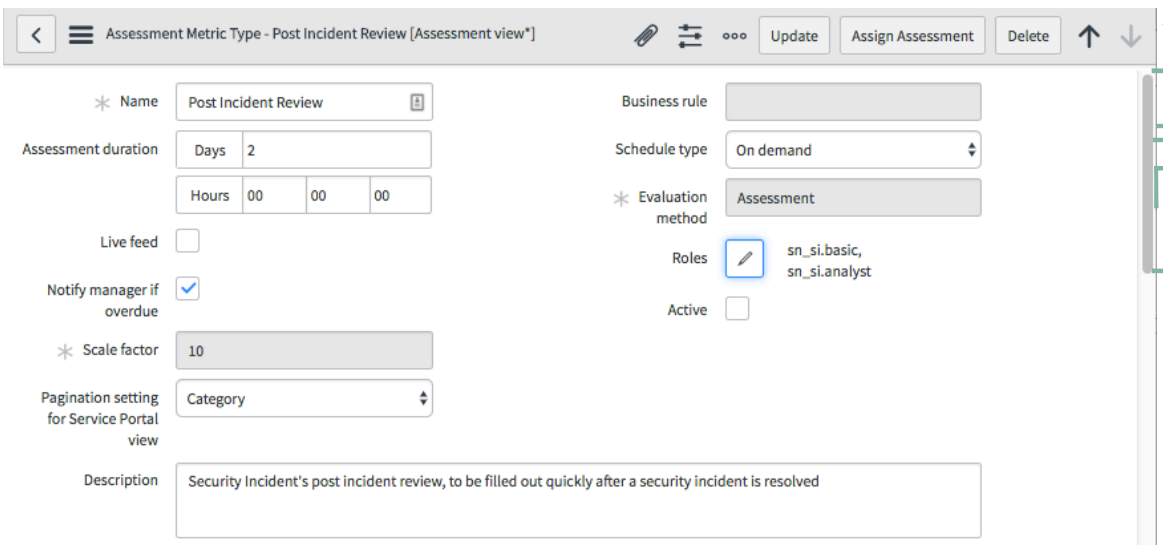
사후 인시던트 검토 역할 할당

PIR(사후 인시던트 검토) 범주에 역할을 할당하여 사전 정의된 특정 그룹에 질문을 대상으로 지정할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 〉 평가 〉 메트릭 정의 〉 유형.
2. 유형 열에서 사후 인시던트 검토 기록을 검색합니다.
3. 기록을 엽니다.
4. 이 질문 범주에 하나 이상의 역할을 할당합니다.



5. 업데이트를 클릭합니다.
6. 다음으로 이동 사용자 관리 〉 사용자.
7. 사용자 선택
8. 사용자 기록에 하나 이상의 메트릭 유형 역할을 추가합니다.

> **주:**
> 역할은 사후 인시던트 검토 범주에 할당된 역할에 해당해야 합니다.

사후 인시던트 검토 보고서

PIR(사후 인시던트 검토) 보고서 기능을 사용하면 사후 인시던트 검토 탭을 사용하여 사후 인시던트 검토 보고서를 설정하고 다운로드할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 관리자는 보고서 템플릿을 생성 및 구성한 후 보고서 구성을 사용하여 해당 템플릿을 보안 인시던트에 매핑할 수 있습니다. 그러면 보안 분석가는 보안 인시던트가 해결되고 상태가 검토 상태로 업데이트된 후 보고서를 보거나 다운로드할 수 있습니다.

구성에 성공한 후 인시던트가 종결 상태로 이동하면 PDF 보고서가 생성되어 보안 인시던트에 첨부됩니다.

주:
보고서 기능은 Orlando 패치 9에서 적용 및 지원됩니다.

사후 인시던트 검토 보고서를 사용자 지정하려면 다음 구성을 수행해야 합니다.

1. 보고서 템플릿: 다음 보고서 템플릿 기능을 사용자 지정하고 구성하여 보고서에 정보를 추가합니다.
   a. 타임라인
   b. 브랜딩
   c. 템플릿 스크립트
2. 보고서 구성

이 섹션에서는 구성 절차에 대해 설명합니다.

보고서 템플릿

보고서 템플릿 섹션을 사용하여 사후 인시던트 검토 보고서를 생성하기 위해 보안 인시던트에 적용되는 기본 및 추가 보고서 템플릿을 생성합니다. 요구 사항에 따라 보고서의 형식을 지정하고 구성할 수 있습니다. 또한 템플릿을 통해 템플릿에 평가 세부 정보를 포함할 수 있습니다.

다음은 템플릿을 빌드하는 동안 수행할 수 있는 몇 가지 선택적 단계입니다.

1. 브랜딩 정보 구성
2. 페이지 크기 및 페이지 여백을 설정합니다.
3. 보안 인시던트 관련 필드 추가(사용자 지정 및 표준 모두)
4. 다음과 같이 미리 정의된 사용자 지정 토큰을 사용합니다.
   a. *$sessionUser*: 로그인한 사용자 이름을 반환합니다.
   b. *$date*: 현재 날짜를 반환합니다.
   c. *$if_not_null_start#&#$if_not_null_end*이러한 태그가 필드에 대해 사용되는 경우 값이 존재하는 경우에만 태그가 표시됩니다. 예:
      - *${if_not_null_start:problem}*
      - *Problem Category: ${problem.category}*
      - *${if_not_null_end:problem}*
5. 템플릿 스크립트를 사용하여 관련 목록 데이터를 포함합니다. 자세한 내용은 아래 템플릿 스크립트 섹션을 참조하십시오.
6. 타임라인 필터를 사용하여 타임라인 정보를 포함합니다. 자세한 내용은 아래 타임라인 섹션을 참조하십시오.
7. 첨부 파일, 테이블 및 이미지와 같은 템플릿 콘텐츠를 관리하고 서식을 지정합니다.

주:
향상된 보고서 템플릿 도구 모음 기능은 Paris 릴리스 버전에서만 사용할 수 있습니다.

보고서 템플릿 핵심 사항:

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

1. 보고서 템플릿에 첨부된 이미지는 sys_attachment 테이블에 포함된 경우에만 사후 인시던트 검토 보고서에 표시됩니다.

   주:
   db_image 테이블에서 선택한 이미지는 사후 인시던트 검토 보고서에 표시되지 않습니다.

2. 비디오는 사후 인시던트 검토 보고서에서 지원되지 않습니다.
3. PDF의 URL을 클릭할 수 없습니다. 클릭할 수 없는(.) URL을 사용하려면 (점)으로 표시됩니다.
4. 보고서 템플릿의 크기가 50MB를 초과하면 보고서가 생성되지 않습니다.
5. 보고서 템플릿 컨텐츠에 대해 선택한 글꼴 제품군은 PDF 작성기에서 지원되지 않는 경우 PDF에 적용되지 않습니다.

   주:
   해당 글꼴이 없는 경우 PDF 생성기는 가장 가까운 대체 글꼴을 식별한 다음 PDF를 생성합니다.

6. 더 높은 페이지 여백 값을 제공하면 사후 인시던트 검토 보고서를 생성하지 못합니다. 예를 들어 위쪽 및 아래쪽 여백은 450>, 왼쪽 및 오른쪽 여백은 450〉입니다.
7. 보고서 템플릿에 공백 없이 큰 텍스트가 포함되면 텍스트가 잘릴 수 있습니다. 텍스트를 미리 보고 그에 따라 수정합니다.

보안 관리자는 보고서 템플릿 페이지에서 사용할 수 있는 보고서 미리 보기 버튼을 사용하여 보고서를 미리 볼 수 있습니다.

주:

보안 인시던트를 선택하여 이 템플릿으로 보고서를 미리 보고보고서 미리 보기를 클릭합니다.

브랜딩

브랜딩 템플릿 이름, 머리글 및 바닥글 이미지, 머리글 및 바닥글 텍스트를 추가하고, 페이지 번호를 생성하고, 브랜딩 기록을 만든 후 보고서 템플릿에 포함할 수 있습니다.

다음은 샘플 브랜딩 보고서 형식입니다.

보고서 템플릿 브랜딩 핵심 포인트:

1. 머리글 및 바닥글 이미지에 허용되는 최대 크기는 5MB입니다. 크기가 지정된 한도를 초과하면 보안 인시던트에 '이미지 형식을 인식할 수 없습니다'라는 오류 메시지가 표시됩니다.
2. 바닥글 텍스트 길이는 100자로 제한됩니다.
   a. 미리 보는 동안 바닥글 이미지 텍스트와 보고서 콘텐츠가 겹치는 경우 브랜딩 기록을 변경해야 합니다.
   b. 바닥글 텍스트에 URL 링크가 포함되어 있으면 바닥글 이미지와 겹칠 수 있습니다. 필요에 따라 미리 보고 수정합니다.

타임라인

타임라인 구성을 사용하면 필요에 따라 타임라인 필터를 만들고 수정할 수 있습니다. 보고서에 포함해야 하는 활동 유형을 필터링하고, 보고서에 하위 작업을 포함할지 또는 제외할지를 구성하고, 이미지를 보고서에 포함할지 또는 제외할지를 구성할 수 있습니다.

타임라인 구성을 활용하고 채우려면 아래에 *${timeline:timeline name}*언급된 대로 태그를 추가해야 합니다. 예를 들어 피싱 보고서 템플릿과 기본 보고서 템플릿에 사용되는 설정에는 두 가지 샘플 타임라인 구성이 제공됩니다. 구성을 수정하고 재사용할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

템플릿 스크립트

템플릿 스크립트를 사용하여 관련 목록 데이터, 날짜 및 타임스탬프, 그리고 직접적인 닷워킹이 불가능한 모든 기타 데이터를 포함합니다. 예를 들면 다음과 같습니다.

보고서 템플릿에 관련 목록을 표시하는 템플릿 스크립트를 구성합니다.

1. 관련 목록 데이터를 준비하려면 PostIncidentReportUtils.fetchRelatedListDataForReport 메서드를 호출합니다.
2. 1단계 데이터를 표 형식 및 스타일로 나타내려면 ReportTemplateUtil.constructTablefunction 메서드를 호출합니다.

템플릿 스크립트를 활용하고 채우려면 태그 템플릿 스크립트 태그를 로 *`${template_script:script name}`*추가해야 합니다.

다음은 사후 인시던트 보고서를 구성하고 수정할 수 있도록 제공되는 몇 가지 샘플 템플릿 스크립트입니다.

스크립트 이름	설명
formatted_current_date	현재 현지 날짜 및 시간을 DDMMYYYY 00.00 AM 또는 PM 형식으로 반환합니다. 예: 2021년 1월 21일 오후 3:51 PST.
si_affected_users	관련 목록에서 영향을 받는 사용자를 표 형식으로 반환합니다.
si_assessments	사후 인시던트 평가 결과를 표 형식으로 반환합니다.
si_associated_phish_emails	관련 목록에서 연결된 피싱 이메일을 표 형식으로 반환합니다.
si_associated_phish_headers	관련 목록에서 연결된 피싱 헤더를 테이블 형식으로 반환합니다.
si_business_criticality	색상으로 구분된 비즈니스 중요도 값을 반환합니다.
si_malicious_observables	관련 목록에서 악성 옵저버블을 표 형식으로 반환합니다.
si_observables	관련 목록에서 옵저버블을 표 형식으로 반환합니다.
si_priority	색상으로 구분된 우선순위 값을 반환합니다.
si_response_tasks	관련 목록에서 응답 작업을 표 형식으로 반환합니다.
si_time_to_identify	초안 및 분석 상태에서 소요된 기간을 반환합니다.
si_time_to_resolve	인시던트 해결 시간을 반환합니다.

보고서 템플릿 스크립트 핵심 포인트:

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

1. 관련 목록에 5개 이상의 열이 추가되면 PDF 생성 중에 테이블 데이터가 잘립니다. 각 열의 최소 너비는 124px로 설정됩니다.
2. 템플릿 스크립트가 기술적인 문제로 인해 보고서 템플릿의 컨텐츠를 로드할 수 없는 경우 보고서에 '템플릿 스크립트를 평가하는 동안 오류가 발생했습니다'라는 오류 메시지가 표시되며 보안 관리자는 스크립트의 정확성을 평가하여 문제를 해결해야 합니다.
3. si_assessments: 기본적으로 모든 평가 범주가 보고서에 추가됩니다. 보안 관리자는 필요에 따라 템플릿 스크립트를 수정하여 데이터를 필터링할 수 있습니다. *`categories: sys_id1, # sys_id2;`* 매개변수를 추가하여 데이터를 필터링합니다.
4. 스크립트 해결 시간 및 식별 시간: 메트릭 관련 목록에 포함된 정의 기록을 사용합니다. 보안 인시던트에 대해 정의 기록을 사용할 수 없는 경우 해당 정의 기록을 생성하거나 추가하여 두 필드의 값을 채웁니다.

주:

기본적으로 보안 관리자에게는 테이블의 버전 기록을 볼 수 있는 액세스 권한이 없습니다. 버전 기록에 액세스하고 이전 버전으로 되돌리려면 관리자 역할을 추가해야 합니다.

보고서 구성

보고서 구성 섹션을 사용하여 조건을 설정하고 보고서 템플릿을 보안 인시던트에 적용합니다. 동일한 조건에 기본 보고서 하나와 추가 보고서 템플릿을 하나 이상 추가할 수 있습니다.

다음은 피싱 보고서 템플릿을 피싱 범주 인시던트에 적용하기 위해 제공되는 조건과 모든 보안 인시던트에 기본 보고서 템플릿을 적용하기 위해 제공되는 다른 조건의 예입니다. 조건이 충족되지 않으면 기본 보고서 템플릿이 보안 인시던트에 적용됩니다.

새 구현을 끄는 절차

1. 다음 비즈니스 규칙을 비활성화합니다.
   a. PIR PDF 생성
   b. 종결 처리 시 지식 생성 신규
2. 다음 비즈니스 규칙을 활성화합니다.
   a. 검토 및 종결 시 PIR 생성
   b. 종결 처리에 대한 지식 작성
   c. [종결/취소/삭제 시 PIR 다시 작성]
3. UI 규칙 *`Hide PIR field when empty`*을 활성화합니다.
4. 보안 인시던트 양식의 양식 레이아웃으로 이동합니다. 사후 인시던트 검토 섹션에서 다음을 수행합니다.
   a. PIR 섹션에서 PIR 보고서 선택기 제거
   b. PIR 섹션에 사후 인시던트 보고서 필드 추가

하위 보안 인시던트에 대한 PIR(사후 인시던트 검토) 보고서 속성 구성

하위 보안 인시던트에 대해 다음 두 가지 PIR 보고서 속성을 구성하는 옵션이 있습니다.

- **sn_si.generate_pir_report_for_child_si**
- **sn_si.include_child_si_timeline_in_pir**

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
시스템 관리자 (admin) 역할을 가진 사용자는 속성을 볼 수 있습니다. 보안 관리자 (sn_si.admin) 역할이 있는 사용자는 이를 수정할 수 있습니다.

하위 보안 인시던트에 대한 **PIR** 보고서 속성 구성

속성	사용량
sn_si.generate_pir_report_for_child_si	하위 보안 인시던트에 대한 PIR(사후 인시던트 검토) 보고서 생성을 활성화하는 옵션입니다. • 유형: true | false • 기본값: false • 위치: 모든 > 시스템 속성 > 모든 속성으로 이동합니다.
sn_si.include_child_si_timeline_in_pir	상위 보안 인시던트의 PIR 보고서에 하위 보안 인시던트의 타임라인을 포함하는 옵션입니다. • 유형: true | false • 기본값: false • 위치: 모든 > 시스템 속성 > 모든 속성으로 이동합니다.

사후 인시던트 검토 보고서 관리

사후 인시던트 검토 관리 보고서에는 보안 관리자가 구성 및 적용한 정보가 포함되며, 보안 분석가는 런타임에 타임라인 필터를 수정하고 다운로드할 수 있습니다.

시작하기 전에
필요한 역할: sn.si_analyst

이 태스크 정보
보안 분석가는 사용 가능한 기본 또는 추가 보고서 템플릿 중 하나를 선택하고 타임라인 필터를 구성하고 보고서를 미리 보고 다운로드할 수 있습니다. 보안 분석가는 마지막으로 적용된 타임라인 구성을 사용하여 보고서를 직접 다운로드할 수도 있습니다.

보안 분석가는 사후 인시던트 검토 탭을 사용하여 보고서에 액세스할 수 있습니다.

프로시저

1. 검토 상태의 보안 인시던트로 이동합니다.
2. 사후 인시던트 검토 탭을 클릭합니다.
3. 보안 인시던트가 검토 상태인 경우:
   보고서 템플릿:
   - 기본적으로 설정 페이지에서 구성된 기본 보고서 템플릿이 보안 인시던트에 적용되고 다운로드할 수 있습니다.
   - 분석가는 드롭다운 목록에서 다른 보고서를 선택하여 보고서를 구성하고 다운로드할 수 있습니다.
4. 구성/미리 보기:

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 분석가는 보고서 템플릿 구성을 미리 보고 수정할 수 있습니다. 현재 구성에서 보안 분석가는 타임라인 필터만 수정할 수 있습니다.

보안 인시던트가 종결되기 전에 기본 보고서에 대한 구성이 수정된 경우 보안 인시던트에 첨부된 사후 인시던트 검토 보고서는 보안 분석가가 수행한 수정 사항에 따라 업데이트됩니다. 종결 후 분석가는 구성을 수정하고 이동 중에 보고서를 다운로드할 수 있습니다. 그러나 첨부된 보고서는 종결되기 전의 마지막 구성을 따릅니다.

보고서를 구성/미리 보려면 다음 단계를 수행하십시오.

a. 사후 인시던트 검토 탭의 보고서 템플릿 드롭다운 목록에서 원하는 보고서 템플릿을 선택합니다.

b. 구성/미리 보기 탭을 클릭합니다.

c. 필요에 따라 타임라인 필터를 업데이트하거나 구성합니다.

d. 이미지 표시 확인란을 사용하여 타임라인에서 이미지를 포함하거나 제외합니다. 이 옵션을 선택하지 않으면 이미지 이름만 타임라인 섹션에 포함됩니다.

e. 하위 작업 표시 확인란을 사용하여 보안 인시던트와 연결된 모든 하위 작업을 나열합니다.

5. 구성을 저장하고미리 보기 탭을 클릭하여 보고서를 미리 보고 다운로드합니다.

6. 다운로드를 클릭하여 보고서를 직접 다운로드합니다.

평가 트리거 조건 구성

규칙 조건을 정의하고 특정 보안 인시던트에 대한 필수 및 선택적 평가를 생성합니다.

시작하기 전에
필요한 역할: sn_si.admin

주:
사후 인시던트 검토 평가 트리거 조건 기능을 사용하려면 11.0으로 보안 인시던트 응답 업그레이드해야 합니다. 업그레이드하기 전에 사후 인시던트 검토 메트릭 유형 및 트리거 조건에 대한 사용자 지정을 되돌려야 합니다. 또한 사후 인시던트 검토와 관련된 비즈니스 규칙으로 수행한 사용자 지정을 되돌려야 할 수도 있습니다.

- 평가를 완료해야 함
- 스토어 담당자

프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 관리 〉 사후 인시던트 검토 - 평가 설정.

2. 평가 트리거 조건 구성 섹션에서 구성을 클릭합니다.

주:
평가 구성 양식의 평가 구성 섹션에서 평가 생성 확인란이 기본적으로 선택되어 있습니다.

- 이 확인란을 선택하면 모든 보안 인시던트에 대해 선택적 평가가 생성됩니다.
- 확인란의 선택을 취소하면 평가가 생성되지 않습니다. 평가 규칙은 표시되지 않으며 보안 인시던트에 대한 조건을 구성할 수 없습니다.

3. 평가 구성 양식의 조건 섹션에서 필요한 정보를 지정합니다.

a. 이름 필드에 규칙 이름을 지정합니다.

b. 이행 필드에서 이행 유형을 지정합니다.

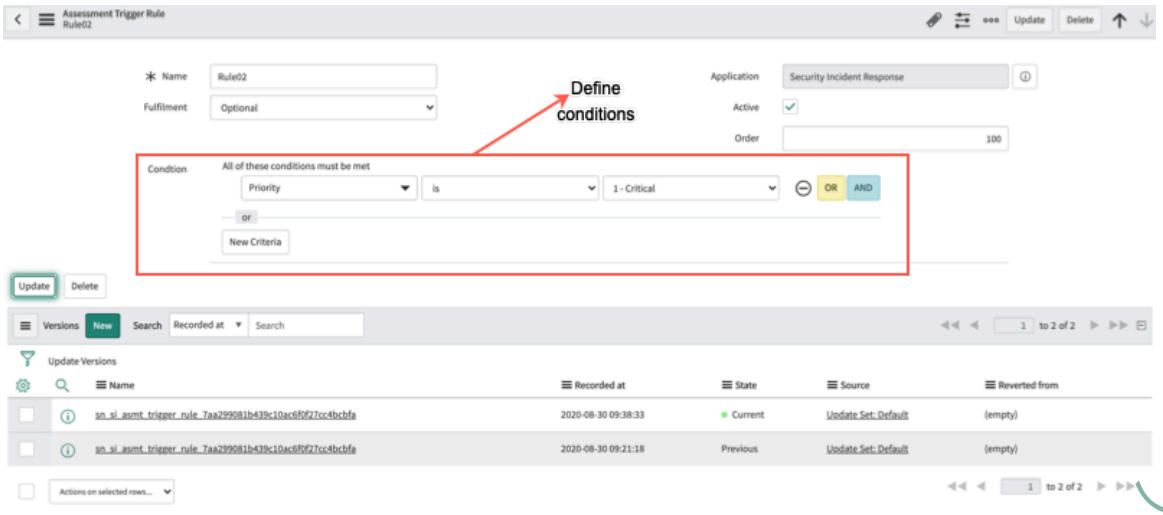
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

c. 조건을 구성하려면 규칙 기록을 클릭하고 조건 필드에서 조건을 정의합니다.

주:

- 조건 필드에 조건을 정의하지 않고 규칙을 생성하면 조건이 true로 평가되고 모든 보안 인시던트에 규칙이 적용 가능합니다.
- 특정 규칙을 정의하여 평가를 필수 또는 선택 사항으로 만들 수 있으며, 정의된 규칙과 일치하지 않는 나머지 보안 인시던트에 대해서는 평가가 생성되지 않습니다.

트리거 조건



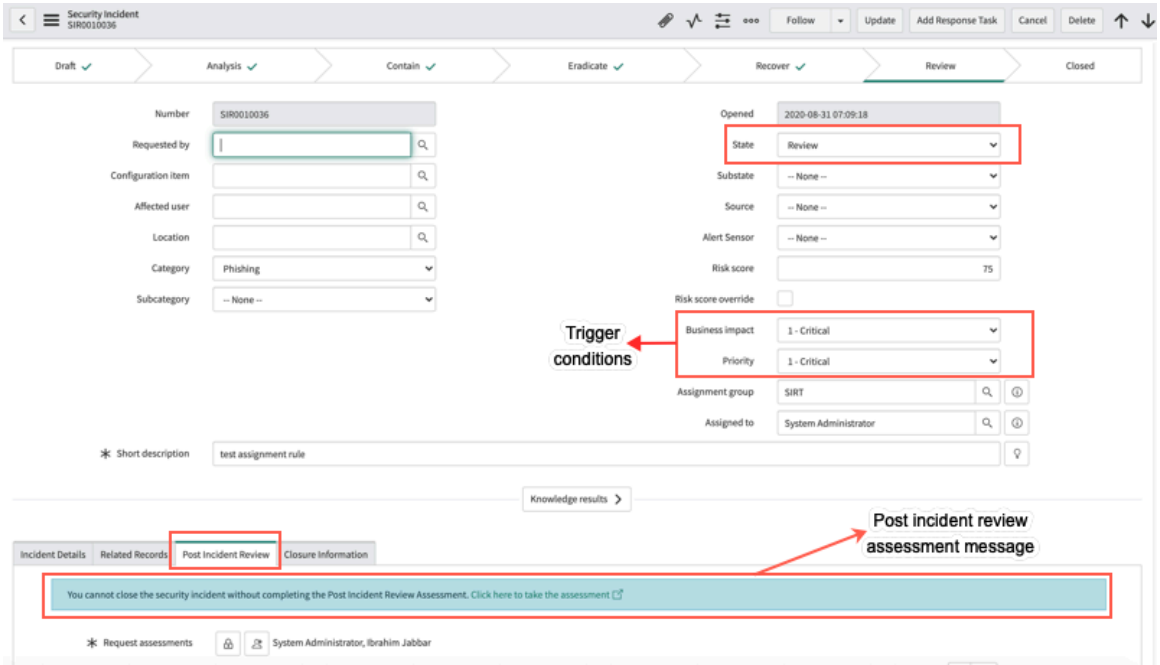
평가 트리거 조건 예시

다음 예시에서는 필수 및 선택적 평가 트리거 조건이 생성되는 방법에 대한 다양한 시나리오를 제공합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 평가 트리거 조건 양식의 평가 트리거 규칙 페이지에서 보안 인시던트에 대한 우선순위 및 비즈니스 영향이 중요로 설정된 경우 필수 평가를 생성합니다. 이러한 시나리오에서 보안 분석가는 필수 평가가 완료될 때까지 인시던트를 종결할 수 없습니다.

필수 평가 예시



- 보시다시피 이 예에서는 보안 인시던트가 검토 상태인 경우 보안 분석가가 사후 인시던트 검토 평가를 완료하지 않으면 보안 인시던트를 종결할 수 없습니다. 인시던트에 할당되거나 평가를 요청한 보안 분석가에게 평가를 전달하는 데 평가 링크를 사용할 수 있습니다.
- 평가 트리거 조건 양식에서 보안 인시던트에 대한 우선순위 및 비즈니스 영향 이 높음으로 설정된 경우 선택적 평가를 생성합니다. 이 예에서 보안 분석가가 평가를 완료하고 보안 인시던트를 종결하지 않으면 평가가 자동으로 취소됩니다.
- 필수 또는 선택적 평가가 보안 인시던트와 일치하지 않는 경우 해당 보안 인시던트에 대한 평가가 생성되지 않습니다. 보안 분석가가 사후 인시던트 검토 평가를 완료하지 않고도 보안 인시던트를 종결할 수 있습니다.

질문서 기반 사후 인시던트 검토 수행

보안 인시던트에 대한 사후 인시던트 검토가 필요하다고 결정할 수 있습니다. 사후 인시던트 검토에서는 발생한 상황을 설명하고 인시던트가 발생한 이유를 확인하는 데 도움을 주며 향후 인시던트를 방지하거나 처리할 수 있는 방법을 식별합니다.

시작하기 전에

필요한 역할: sn_si.admin, sn_si.manager, sn_si.analyst

주:
역할에 관계 없이 모든 사용자가 사후 인시던트 검토 질문서에 참여할 수 있습니다. 역할은 검토에 할당될 수 있습니다.

이 태스크 정보

이 ServiceNow 보안 인시던트 응답 애플리케이션은 질문서를 사용하여 보안 인시던트와 관련된 모든 사람으로부터 사후 인시던트 검토 정보 수집을 자동화할 수 있습니다. 사후 인시던트 검토의 일환으로 질문서를 사용하기로 결정하면 보안 인시던트와 관련된 질문 목록이 사용자 정의 참가자 목록으로 전송됩니다. 각 사용자가 질문서를 작성하면 인시던트 사후 보고서가 자동으로

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

생성됩니다. 보고서에는 보안 인시던트와 관련된 모든 정보와 사후 인시던트 검토에 대한 모든 응답이 수집됩니다.

초기 질문 목록이 기본 시스템과 함께 제공되지만 사용자 지정이 가능합니다. 범주를 만들고 새 질문을 추가하거나 기존 범주 내에서 개별 질문을 변경할 수 있습니다. 역할에 따라 질문을 할 수 있습니다. 특정 질문을 하는 시기를 정의할 수 있습니다. 예를 들어, UNIX 서버에 대해서만 질문하거나 범죄 행위가 있는 경우에만 질문이 있을 수 있습니다. 다른 질문에 대한 답변이나 양식의 필드 값에 따라 묻는 질문을 정의할 수 있습니다. 데이터베이스를 쿼리하여 완전히 채워지는 질문도 있을 수 있습니다.

보안 인시던트가 해결되고 검토 상태로 이동하면 할당된 모든 사용자와 평가 요청 목록에서 직접 추가된 사용자에 대한 평가가 생성됩니다.

질문서는 다양한 소스에서 보안 인시던트 처리에 대한 정보를 수집하는 데 유용한 도구일 수 있습니다.

검토하는 동안 질문서 작성을 시작한 사용자가 아닌 경우 목록에 사용자를 더 추가하거나 기존 사용자를 목록에서 제거할 수 있습니다. 목록에 새 사용자를 추가하면 기록이 저장될 때 해당 사용자가 질문을 받게 됩니다. 모든 질문서를 완료할 때까지 보안 인시던트를 종결할 수 없습니다. 각 사용자가 질문서를 작성하면 사후 인시던트 보고서가 자동으로 생성(및 재생성)되어 사후 인시던트 검토 탭에 표시됩니다.

사후 인시던트 검토를 시작하려면 다음을 수행합니다.

프로시저

1. 보안 인시던트를 생성하거나 다음으로 이동하여 기존 보안 인시던트를 엽니다. 보안 인시던트 〉 인시던트 〉 나에게 할당됨(또는 팀에 할당됨 또는 미할당 인시던트).
2. 사후 인시던트 검토 탭을 클릭합니다.
3. 평가 요청 필드는 기본적으로 할당 대상 필드의 개인으로 설정됩니다.
   검토 목록에 다른 사용자를 추가하려면 자물쇠 아이콘을 클릭합니다. 필드가 잠금 해제된 후에는 여러 사용자, 역할을 추가 또는 제거하거나 사용자 이메일 주소를 입력하는 옵션을 사용할 수 있습니다.
4. 입력을 완료했으면 잠금 아이콘을 클릭하여 필드를 잠급니다.

   주:
   또한 보안 인시던트에서 충족될 경우 특정 사용자가 해당 보안 인시던트에 대한 평가 요청 필드에 자동으로 추가되도록 하는 조건을 정의할 수 있습니다. 예를 들어 보안 인시던트 범주가 피싱으로 변경되면 피싱 위협에 대한 전문 지식을 가진 특정 개인을 사후 인시던트 검토 목록에 추가할 수 있습니다. 자세한 내용은 PIR 담당 규칙 생성 문서를 참조하십시오.

5. 업데이트를 클릭합니다.
   인시던트가 검토 상태로 전환되면(또는 이미 검토 상태에 있는 경우 즉시) 검토 목록에 있는 각 사용자는 초기 이메일 알림을 받습니다. 기한이 가까워지면 미리 알림이 전송됩니다. 각 사용자가 이메일 링크를 통해 또는 다음으로 이동하여 질문서에 액세스할 때 게시 인시던트 검토 〉 보류 중인 사용자 검토, 표시된 질문은 이 보안 인시던트에 맞는 모든 범주에서 가져온 것입니다. 기한에 도달하기 전에 새 사용자가 검토 목록에 추가되면 보안 인시던트가 저장될 때 알림이 전송됩니다.

   사용자가 질문서를 작성하면 사후 인시던트 보고서가 데이터를 컴파일하여 사후 인시던트 검토 탭에 보고서를 표시합니다. 질문서 데이터는 발견 사항 탭에 표시됩니다.

사후 인시던트 검토 질문서 범주 생성

기본 시스템과 함께 제공되는 질문서 범주를 사용하거나 자신만의 범주를 생성할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn.si_admin

이 태스크 정보
질문의 새 범주를 만들려면 다음과 같이 하십시오.

프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 게시 인시던트 검토.
2. 질문 검토를 클릭합니다.
   질문이 제기되는 조건을 정의하는 필터 및 순서 및 필터와 함께 범주 목록이 표시됩니다(예: 보안 인시던트 범주가 ## ##인 경우에만). 각 범주는 사후 인시던트 검토 질문서의 섹션이며 각 범주의 질문은 보안 인시던트가 조건 필터와 일치하는 경우에만 포함됩니다. 예를 들어 Linux 서버에만 적용되는 질문 범주의 경우 영향을 받는 자원 유형이 Linux 서버인 보안 인시던트를 선택하는 필터를 설정할 수 있습니다. 그런 다음 이 범주에서 보안 인시던트가 Linux 서버에 있을 때 필요한 모든 질문을 생성합니다. 기본 시스템에 제공된 범주 중 하나를 사용하거나 새 범주를 생성합니다. 이 절차에서는 질문을 정의하기 전에 새 범주를 생성한다고 가정합니다.
3. 범주 목록에서 새로 만들기를 클릭합니다.
4. 양식의 필드에 적절히 입력합니다.

보안 인시던트

필드	설명
이름	보안 인시던트 질문서에 표시되는 범주의 이름입니다.
유형	사후 인시던트 검토가 기본값입니다.
이해 관계자 작성	에 의해 보안 인시던트 응답사용되지 않음 .
테이블	이 필드는 양식이 제출되면 자동으로 할당됩니다.
필터	이 범주의 질문이 사용되는 시기를 결정하는 조건을 입력합니다. 보안 인시던트 기록이 이 필터와 일치하면 해당 보안 인시던트에 대한 사후 인시던트 검토에 질문이 포함됩니다. 필터는 기록 또는 이 기록에 연결된 다른 기록의 모든 데이터를 사용할 수 있습니다. 예를 들어 요청하는 사용자의 관리자 부서입니다.
애플리케이션	인시던트에 대한 범위 애플리케이션입니다.
가중치	동일한 범주의 다른 메트릭과 비교했을 때 이 메트릭의 중요도를 나타내는 숫자 값입니다. 기본적으로 가중치는 10입니다.
총 메트릭	범주에서 사용하는 메트릭 수입니다.
설명	질문서에 대한 설명입니다.

5. 제출을 클릭하여 범주를 저장합니다.

사후 인시던트 검토 질문 작성

기본 시스템과 함께 제공되는 질문을 사용하거나 직접 질문을 생성할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보

사후 인시던트 검토 정보를 수집하는 방법은 질문 형태이거나 스크립트를 사용하여 자동으로 수집된 데이터일 수 있습니다.

질문은 다른 질문에 대한 답변에 따라 달라질 수 있습니다. 예를 들어 필요한 모든 로그를 사용할 수 있는지 물어볼 수 있습니다. 대답이 아니요인 경우 후속 질문을 하여 필요한 로그 중 사용하도록 설정되지 않은 로그를 확인합니다.

스크립트 메트릭이라고도 하는 스크립팅된 데이터 수집은 사용자가 작성하는 스크립트를 통해 보안 인시던트와 관련된 데이터를 수집합니다. 이 작업은 보안 인시던트 기록 자체의 데이터를 훨씬 넘어설 수 있습니다. 예를 들어 스크립트 메트릭은 이 보안 인시던트의 영향을 받는 서버에 대한 최근 중단 시간을 수집할 수 있습니다.

마지막으로 두 가지 유형을 혼합할 수 있습니다. 질문에는 스크립트에서 가져온 기본값이나 보안 인시던트 기록의 필드에서 가져온 기본값이 있을 수 있습니다. #### ## ### 사용할 때... 유형의 질문에서 사용자가 항상 질문에 대답하도록 할지(기본값이 초기 값을 제공함) 또는 스크립트 또는 필드가 비어 있는 경우에만 사용자에게 질문하도록 할지 선택할 수 있습니다.

새 질문을 만들려면:

프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 게시 인시던트 검토.
2. 새 질문을 생성할 범주를 클릭합니다.
3. 평가 메트릭 탭을 클릭합니다.
4. 새로 만들기를 클릭합니다.
   기존 질문을 클릭하여 수정할 수도 있습니다.
5. 양식의 필드에 적절히 입력합니다.

메트릭 양식

필드	설명
이름	메트릭(질문 또는 스크립트)의 이름입니다. 메트릭이 스크립팅된 데이터 수집인 경우 이 이름은 사후 인시던트 보고서에 나타납니다.
범주	메트릭이 속한 범주입니다. 메트릭 범주 양식에서 새 메트릭을 만들면 시스템이 이 범주를 자동으로 채웁니다. 주: 종속 대상 필드가 설정되거나 다른 메트릭이 이 메트릭에 종속된 경우에는 범주를 변경할 수 없습니다.
방법	다음과 같이 메트릭 유형을 나타냅니다. ○ *Assessment*: 기본값이 없는 질문입니다. 필드 유형 탭의 데이터 유형 필드에는 확인란, 선택 목록, 텍스트 입력 등 여러 데이터 유형을 정의할 수 있습니다. ○ *Script*: 스크립팅된 메트릭입니다. 사용자 지정 스크립트를 작성하여 값을 가져옵니다. 이 *Script* 메서드는 **Duration**, **Number** 및 **Percentage** 데이터 형식과 호환됩니다. ○ *Default answer from field*: 보안 인시던트에서 선택한 필드에서 기본 응답이 제공되는 질문입니다. 이 옵션을 선택하면 일반 탭에 두 개의 필드가 추가됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	▪ *Default answer*: 질문에 대한 기본 답변이 포함된 보안 인시던트에서 필드를 선택합니다. 예를 들어 "이 인시던트를 처음 보고한 사람은 누구입니까?"라는 질문의 경우 요청자 필드를 선택할 수 있습니다. ▪ *Ask question*: 질문 시기(항상 또는 기본 답변 필드가 비어 있는 경우에만)를 지정합니다. 위의 예시를 사용하면 요청한 사람 필드가 비어 있는지 묻는 질문이 표시될 것입니다. ○ *Default answer from script*: 스크립트에서 기본 대답을 가져오는 질문입니다. 정답은 숫자, 문자열 또는 백분율일 수 있습니다. 일반 탭은 다음 필드를 추가합니다. *Ask question*: 질문 시기를 지정합니다. 항상 또는 스크립트가 기본 대답을 제공하지 않는 경우에만. 스크립트는 필드 유형 탭에서 정의됩니다. **주:** 선택한 방법과 호환되지 않는 데이터 유형을 선택하면 시스템이 자동으로 방법을 호환되는 값으로 변경합니다.
가중치	〔필수〕 동일한 범주의 다른 메트릭과 비교했을 때 이 메트릭의 중요도를 나타내는 숫자 값입니다. 기본적으로 가중치는 10입니다. 이 필드는 데이터 유형이날짜,날짜/시간 또는 문자열이 아닌 한 표시되고 필수입니다. 이러한 데이터 유형은 결과 계산에 포함되지 않습니다.
순서	〔필수〕 같은 범주의 다른 메트릭 질문을 기준으로 평가 질문서에 대한 메트릭 질문의 순서를 결정하는 숫자 값입니다. 순서 값이 가장 작은 메트릭이 범주 섹션에서 첫 번째 질문으로 나타납니다. 기본적으로 순서는 100입니다. **주:** 질문서에 나타나지 않으므로 스크립트 방법을 사용하는 메트릭에 어떤 순서 값을 사용하는지는 중요하지 않습니다.
활성	이 메트릭이 사용되는지 여부를 결정하는 확인란입니다. 확인란을 선택하지 않으면 메트릭 기록이 없는 것과 같습니다.
필수	평가 질문서에서 메트릭 질문을 필수(선택) 또는 선택(선택 취소)으로 만드는 확인란입니다. 사용자는 빨간색 필드 상태 표시기로 표시된 모든 필수 질문에 유효한 응답을 제공할 때까지 질문서를 제출할 수 없습니다. 이 필드는 종속 대상 필드가 비어 있고 데이터 유형이 확인란이 아닌 경우에만 표시됩니다.

6. 일반 탭을 클릭하고 필드에 적절한 정보를 입력합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

일반 탭

필드	설명
질문	보안 인시던트 검토 질문서에 대한 질문으로 사용할 텍스트입니다. 다음과 같이 쉽게 대답할 수 있는 명확하고 직관적인 질문을 입력합니다. 예를 들어 인시던트를 어떻게 억제했습니까?
설명	메트릭 및 메트릭 평가 대상에 대한 정보입니다. 평가*Method*인 경우 사용자가 질문에 대답하는 방법을 이해하는 데 도움이 되는 상세 정보를 포함합니다. 이 텍스트는 사용자가 질문서의 질문 텍스트를 가리키면 힌트로 나타납니다.
종속 대상 및 표시되는 경우	현재 질문이 종속 된 종속 대상 필드에서 질문을 선택합니다. 예를 들어 "어떤 추가 로그가 필요했습니까?"라는 질문은 "필요한 모든 로그를 사용할 수 있습니까?"라는 질문에 따라 달라집니다. 다음으로, 표시되는 경우 필드를 사용하여 종속 질문을 질문서에 표시할 시기를 식별합니다. 예를 들어 사용자가 "필요한 모든 로그를 사용할 수 있습니까?" 질문에 아니요라고 대답한 경우에만 종속 질문을 묻도록 하려면 표시되는 경우 필드에서 아니요를 선택합니다. **주:** 시스템은 메트릭 간에 재귀 의존성이 생성되지 않도록 방지합니다. 예를 들어 메트릭 A가 메트릭 B에 종속된 경우 메트릭 B는 메트릭 A에 종속될 수 없습니다.

7. 필드 유형 탭을 클릭하고 필드에 적절한 정보를 입력합니다.

필드 유형 탭

필드	설명
데이터 유형	예상 응답의 데이터 유형으로, 사용 가능한 유형 목록은 선택한 방법에 따라 달라집니다. 메서드가 평가인 경우 데이터 유형에 따라 사용자가 질문서의 해당 질문에 답변하는 방법이 결정됩니다. 메서드가 스크립트인 경우 데이터 유형에 따라 시스템이 평가 결과를 계산하는 방법이 결정됩니다. **주:** 다른 메트릭이 이 메트릭에 종속되는 경우 데이터 유형을 변경할 수 없습니다.
대답 임의대로	사용자가 질문이 포함된 평가 질문서를 열 때마다 이 메트릭 질문에 대한 답변 옵션을 임의의 순서로 표시할지 여부를 결정하는 확인란입니다. 답변 기본 설정은 답변 옵션이 나타나는 순서에 따라 달라질 수 있습니다. 이로 인해 편향된 결과가 발생할 수 있습니다. 답변 옵션을 무작위로 지정하면 이러한 편향을 방지하는 데 도움이 될 수 있습니다. 이 필드는 데이터 유형 필드에서 **Likert** 척도 또는 선택을 선택한 경우에만 표시됩니다.
종속 플러그인	(스크립트인 경우 *Method* 필수입니다.)

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	스크립트에서 쿼리된 테이블을 포함하는 플러그인입니다. 플러그인이 활성 상태인 경우에만 시스템이 메트릭 스크립트를 실행합니다. 사용 가능한 기본 값은 자산 관리, **CMDB,Core**, 비용 관리, 구매 및 소프트웨어 자산 관리입니다. 이 필드는 스크립트인 경우에만 *Method* 표시됩니다. 주: ○ Core 기본값을 사용하면 스크립트가 항상 실행됩니다. ○ 관리자인 경우 필드에 더 많은 플러그인 선택 항목을 추가할 수 있습니다.
기준 정의	평가 결과 계산에서 더 작거나 큰 숫자 값이 좋은 점수와 같은지 여부를 결정하는 설정입니다. 벤더의 결함 수를 측정하는 메트릭과 같이 숫자 값이 낮을수록 좋을 경우 낮음을 선택합니다. 1에서 5까지의 척도로 사용자 만족도를 측정하는 메트릭과 같이 숫자 값이 클수록 더 나은 경우 높음 을 선택합니다. 기본값은 높음입니다. 이 필드는 날짜, 날짜/시간 또는 문자열이 아닌 한 표시되며 필수입니다*Data type*. 이러한 데이터 유형의 결과는 결과 계산에 포함되지 않습니다.
최소	평가에 대한 답변 옵션 또는 스크립팅된 메트릭에서 확장된 값으로 사용할 가장 낮은 숫자 값입니다. 이 필드는 특정 데이터 유형을 선택한 경우에만 표시되고 필요합니다. 데이터 유형이 선택 또는 **Likert** 척도인 경우 이 필드는 읽기 전용이며 가장 작은 메트릭 정의 *Value*에 따라 자동으로 설정됩니다.
최대	응답 옵션 또는 배율 값으로 사용할 가장 높은 숫자 값입니다. 이 필드는 특정 데이터 유형을 선택한 경우에만 표시되고 필요합니다. 데이터 유형이 선택 또는 **Likert** 척도인 경우 이 필드는 읽기 전용이며 가장 큰 메트릭 정의 *Value*에 따라 자동으로 설정됩니다.
스크립트	원하는 시스템 정보를 가져오는 스크립트입니다. 스크립트에는 보안 인시던트(기본)의 ID로 설정된 입력 변수 1개와 스크립트에서 설정할 수 있는 출력 변수 세 가지, string_result, scaled_result, actual_result가 있습니다. 데이터 형식이 문자열이면 string_result만 필요합니다. 이 필드는 스크립트이거나 스크립트에서 기본값을 가져올 때 *Method* 표시되고 필수입니다.
템플릿	질문에 사용할 미리 정의된 일반적인 답변 세트입니다. 예를 들어 빈도 템플릿은 "절대 안 함" 값으로 시작하여 "항상"이라는 최상위 값까지 올라갈 수 있습니다. 이 필드는 템플릿인 경우에만 *Data type* 표시되고 필요합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	주: 다른 메트릭이 이 메트릭에 종속되는 경우 템플릿을 변경할 수 없습니다.

8. 옵션: 입력을 완료했으면 업데이트를 클릭합니다.

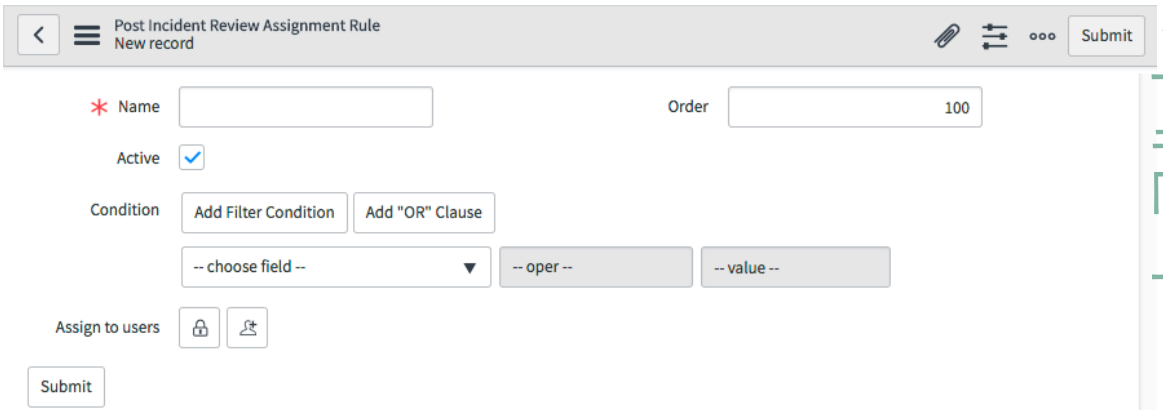
PIR 담당 규칙 생성

보안 인시던트에 대한 사후 인시던트 검토 평가 목록을 수동으로 추가하는 것 외에도 사용자를 목록에 자동으로 추가하는 담당 규칙을 정의할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.admin, sn_si.manager, sn_si.analyst

프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 관리 〉 사후 인시던트 검토 - 평가 설정.
2. 사용자 할당 규칙 섹션으로 드릴다운합니다.
3. 구성을 클릭합니다.
4. 새로 만들기를 클릭합니다.



5. 필요에 따라, 필드를 채웁니다.

필드	설명
이름	이 할당 규칙의 이름입니다.
활성	규칙을 활성화하려면 이 확인란을 선택합니다.
순서	숫자 값을 입력하여 담당 규칙 목록에서 이 규칙이 나타날 위치를 지정합니다. 낮은 숫자가 목록 맨 위에 나타납니다. 주: 일치하는 첫 번째 할당 규칙만 실행되고 해당 규칙에 정의된 사용자만 평가 목록에 추가됩니다.
조건	다음 사용 이 규칙을 실행하려면 보안 인시던트에서 충족해야 하는 조건을 정의하는 조건 작성기 입니다. 자세한 내용은 아래 예를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

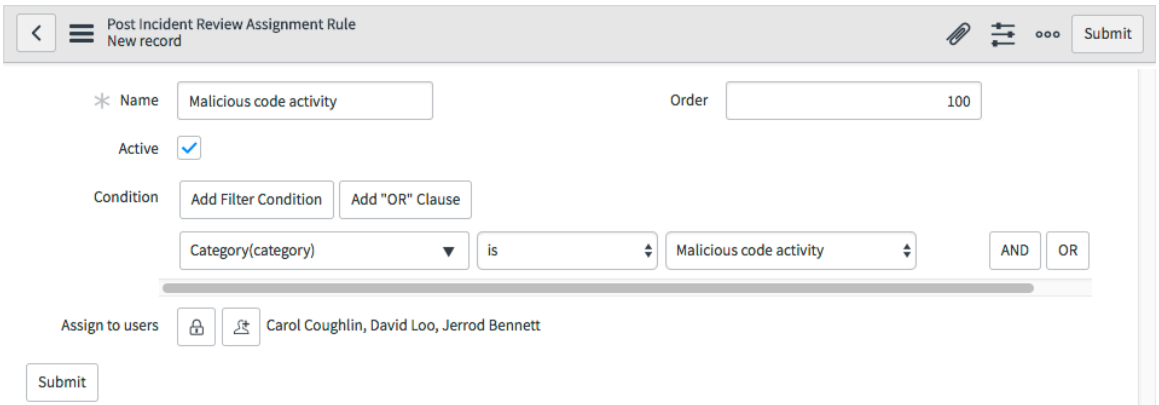
필드	설명
사용자에게 할당	검토 목록에 사용자를 추가하려면 자물쇠 아이콘을 클릭합니다. 필드가 잠금 해제된 후에는 여러 사용자, 역할을 추가 또는 제거하거나 사용자 이메일 주소를 입력하는 옵션을 사용할 수 있습니다.

6. 제출을 클릭합니다.

Example: 악성 코드 활동

여기에 표시된 사후 인시던트 검토 할당 규칙에서 범주 필드가 악성 코드 활동 으로 설정된 보안 인시던트가 검토 상태로 전환되면 식별된 사용자 3명(악성 코드 활동을 처리하는 전문가)이 이 보안 인시던트에 대한 사후 인시던트 검토 질문서를 받을 사용자 목록에 추가됩니다.

악성 코드 활동



보안 인시던트 종결

보안 인시던트가 검토 상태로 전환되면 인시던트를 종결하고 적절한 종결 코드를 입력할 수 있습니다. 폐쇄 코드는 나중에 쉽게 찾을 수 있도록 검색할 수 있습니다.

시작하기 전에

필요한 역할: sn_si.write

이 태스크 정보

주:
이전 버전의 보안 인시던트 응답에서는 사용자가 보안 인시던트 또는 요청을 스팸으로 종결할 수 있었습니다. Istanbul 릴리스에서는 스팸 옵션을 더 이상 사용할 수 없습니다. 스팸 보안 인시던트 또는 요청은 적절하게 취소하거나 삭제할 수 있습니다.

프로시저

1. 종료하려는 보안 인시던트가 아직 열려 있지 않은 경우 보안 인시던트 > 인시던트 > 모든 인시던트 표시을 클릭하고 종결할 보안 인시던트를 찾습니다.

   주:
   이 보안 인시던트에 대해 완료되지 않은 사후 인시던트 검토 평가 가 있는 경우 보안 인시던트를 종결할 수 없습니다. 반환 대상 보안 인시던트 > 게시 인시던트 검토 > 모든 완료되지 않은 검토, 불완전한 검토를 찾은 다음 검토자에게 검토를 완료하도록 요청하거나 나머지 평가를 취소합니다.

2. 종결 처리 정보 탭을 클릭하고 필드에 적절한 정보를 입력합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 인시던트

필드	설명
지식 문서 생성	이 필드를 선택하면 사후 인시던트 검토 내용이 포함된 지식베이스 문서 초안이 자동으로 생성됩니다.
종결 코드	이 보안 인시던트를 종결하는 이유를 가장 잘 설명하는 종결 코드를 선택합니다. ○ 조사 완료됨 ○ 위협 완화됨 ○ 패치된 취약성 ○ 잘못된 취약성 ○ 해결 안 됨 ○ 긍정 오류
종결한 사람	기록이 업데이트된 후 보안 인시던트를 종결한 사용자를 표시합니다.
종결됨	기록이 업데이트된 후 종결 날짜 및 시간을 표시합니다.
종결 메모	이 보안 인시던트 종결 결과를 설명하는 추가 메모를 입력합니다.

3. 업데이트를 클릭합니다.
4. 할당된 사용자는 수동으로 상태를종결로 변경할 수 있습니다.
   상위 인시던트가 종결되면 하위 인시던트에 속하는 모든 응답 작업이 취소됩니다. 다른 유형의 작업이 없으면 하위 인시던트도 종결됩니다.

보안 인시던트에 종결 처리 정보 추가

보안 인시던트가 검토 또는 종결 상태인 경우 종결 처리 정보를 입력할 수 있습니다.

시작하기 전에

필요한 역할: sn_si.basic

프로시저

1. 아직 열려 있지 않으면 업데이트할 보안 인시던트를 엽니다.
2. 관련 기록 탭을 클릭합니다.
3. 필요에 따라, 필드를 채웁니다.

필드	설명
지식 문서 생성	사후 인시던트 보고서의 내용을 사용하여 지식 문서를 생성하려면 이 확인란을 선택합니다.
종결 코드	보안 인시던트를 종결하는 이유를 가장 잘 설명하는 종결 코드를 선택합니다.
종결한 사람	〔읽기 전용〕 보안 인시던트를 종결한 사용자를 표시합니다.
종결됨	〔읽기 전용〕 보안 인시던트가 종결된 날짜 및 시간을 표시합니다.
종결 메모	학습한 교훈, 해결 방법 등 보안 인시던트를 종결한 방법입니다.

4. 다음 탭 중 하나를 클릭하여 보안 인시던트를 추가로 업데이트합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 인시던트 상세 정보
- 게시 인시던트 검토

5. 입력을 완료했으면 제출을 클릭합니다.

보안 인시던트에 대한 접근 제한

중요한 정보가 포함된 보안 인시던트에 대한 액세스를 관리합니다. 보안 인시던트 제한을 적용하여 특정 인시던트에 액세스할 수 있는 사용자를 결정하고 특정 사용자 또는 그룹으로만 액세스를 제한할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.admin

이 태스크 정보
보안 인시던트 제한을 사용하면 특정 조직의 다른 사용자가 중요한 보안 인시던트에 액세스하지 못하도록 숨길 수 있습니다. 이러한 제한을 통해 사용자가 액세스할 수 있는 보안 인시던트를 보다 세부적으로 제어할 수 있습니다. 제한 적용 확인란을 선택한 다음 특정 보안 인시던트에 액세스할 수 있는 사용자 또는 그룹을 선택하여 보안 인시던트 제한을 적용할 수 있습니다.

특정 보안 인시던트에 제한을 적용하고 특정 사용자 또는 그룹에 대한 액세스를 제한하면 조직의 나머지 모든 사용자는 특정 제한된 보안 인시던트를 검색하더라도 이러한 보안 인시던트에 액세스할 수 없습니다.

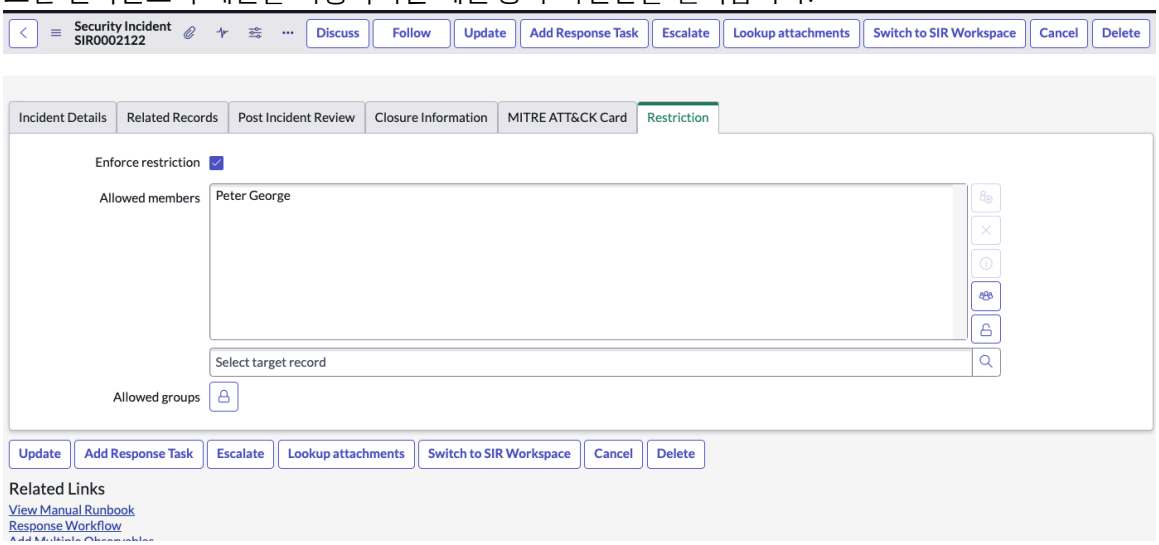
프로시저

1. 제한하려는 보안 인시던트를 엽니다.

2. 클래식 UI를 사용하는 경우 다음을 수행합니다.

a. 제한 탭을 클릭합니다.

b. 보안 인시던트의 제한을 사용하려면 제한 강화 확인란을 선택합니다.



c. 허용된 구성원 필드에서 아이콘을 클릭하여 보안 인시던트에 액세스할 수 있는 사용자를 선택합니다.

d. 아이콘을 선택하여 자신을 허용된 사용자로 추가합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

e. 사용자를 추가하거나 제거하려면 아이콘을 선택합니다.

f. 허용된 그룹 필드에서 아이콘을 클릭하여 보안 인시던트에 액세스할 수 있는 그룹을 선택합니다.

g. 그룹을 추가하거나 제거하려면 아이콘을 선택합니다.

> **주:**
> 보안 인시던트에 제한 적용 확인란이 활성화되면 sn_si.admin 및 허용된 구성원 또는 그룹만 보안 인시던트에 액세스할 수 있습니다.

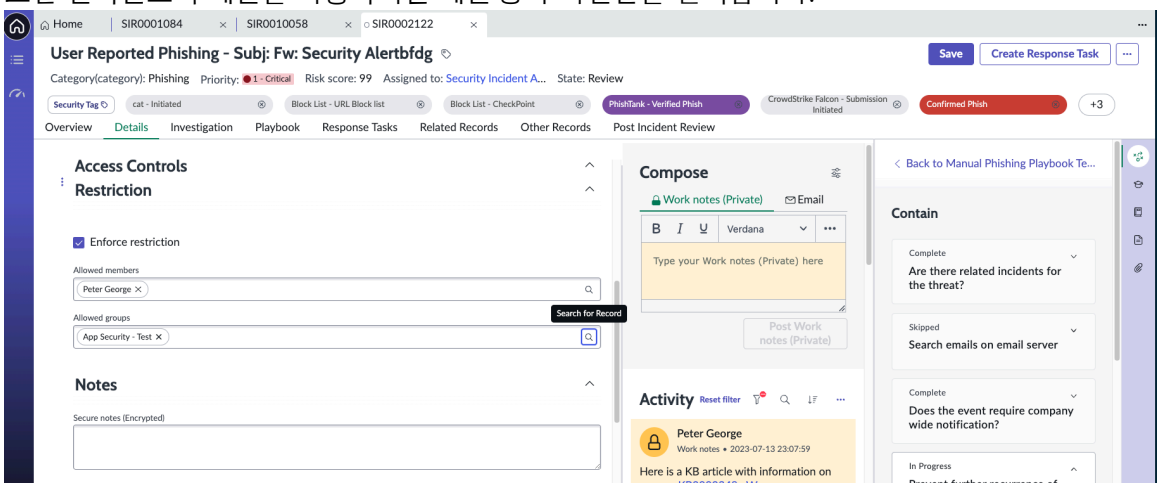
h. 업데이트를 클릭합니다.

3. SIR 작업 공간을 사용하는 경우 다음을 수행합니다.

a. 보안 인시던트에서 상세 정보 탭을 클릭합니다.

b. 아래로 스크롤하여 제한 섹션을 클릭합니다.

c. 보안 인시던트의 제한을 사용하려면 제한 강화 확인란을 선택합니다.



d. 허용된 구성원 필드에서 검색 옵션을 사용하여 보안 인시던트에 접근할 수 있는 사용자를 선택합니다.

e. 허용된 그룹 필드에서 검색 옵션을 사용하여 보안 인시던트에 액세스할 수 있는 그룹을 선택합니다.

> **주:**
> 보안 인시던트에 제한 적용 확인란이 활성화되면 sn_si.admin 및 허용된 구성원 또는 그룹만 보안 인시던트에 액세스할 수 있습니다.

f. 저장을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

를 사용하여 보안 위협 관리 보안 분석가 작업 공간

보안 인시던트 응답 에는 플레이북, 엿보기 뷰 및 여러 보안 인시던트를 처리하기 위한 탭을 포함하여 분석을 지원하는 강력한 도구를 제공하는 새로운 사용자 인터페이스가 보안 분석가 작업 공간 포함되어 있습니다.

보안 분석가를 위해 특별히 설계된 강력한 도구를 보안 분석가 작업 공간 사용하면 보안 인시던트와 관련하여 계속 증가하는 데이터 볼륨을 분석할 수 있습니다. 또한 자동화된 작업은 보안 인시던트 조사 시간을 크게 단축하며, 이는 공격을 중지하는 것과 침해를 겪는 것의 차이가 될 수 있습니다.

사용하기 전에 보안 분석가 작업 공간

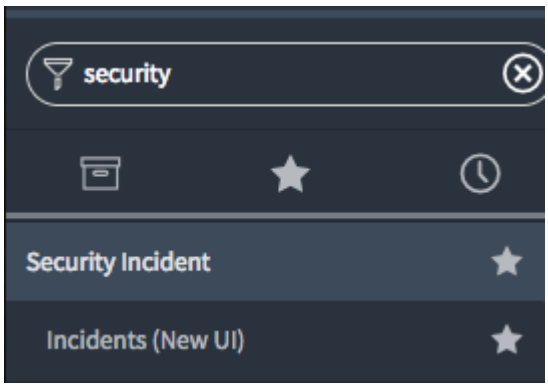
를 보안 분석가 작업 공간사용하려면 먼저 인스턴스에 London 패치 3 이상이 설치되어 있는지, 올바른 역할이 정의되어 있는지, 다음이 있는지 확인해야 합니다. 에서 보안 인시던트 응답 UI 애플리케이션을 다운로드함 ServiceNow Store.

주:
인스턴스에서 London 패치 3 이전 버전을 실행 중인 경우, HI 고객 서비스 시스템을 통해 보안 인시던트 응답 UI 플러그인을 요청해야 합니다.

보안 분석가 작업 공간 액세스

이 새 작업 공간에 액세스하려면 다음으로 이동합니다. 보안 인시던트 〉 인시던트(신규 **UI)**.

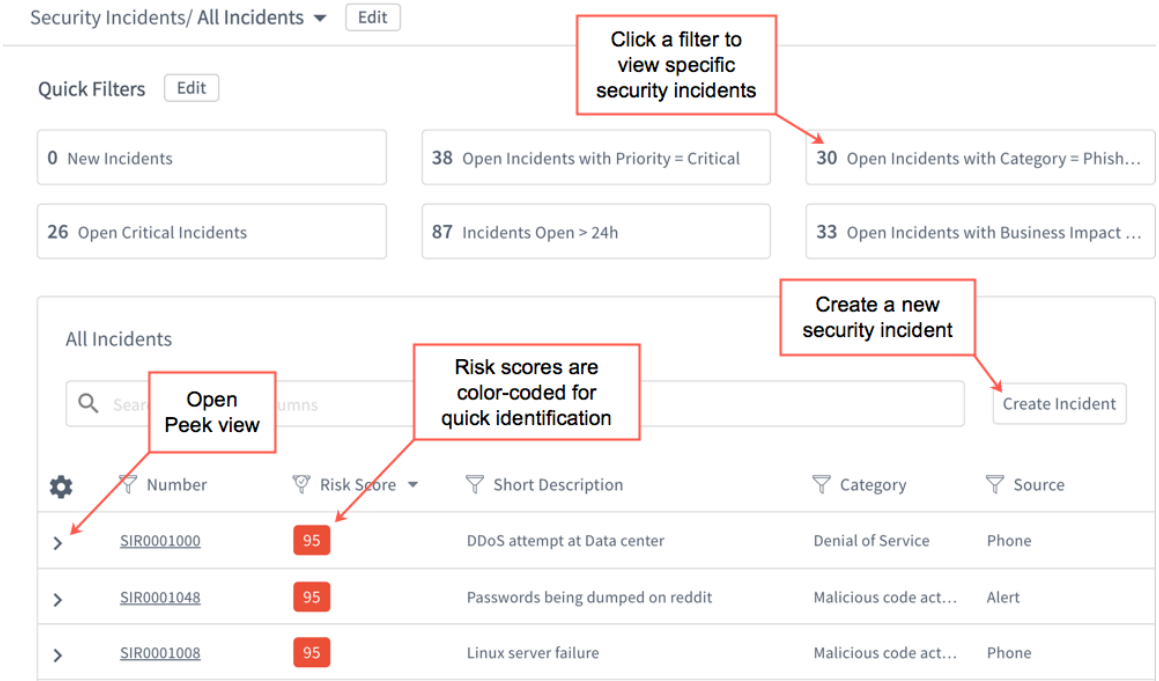
보안 인시던트



작업 공간이 별도의 브라우저 탭에서 열립니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

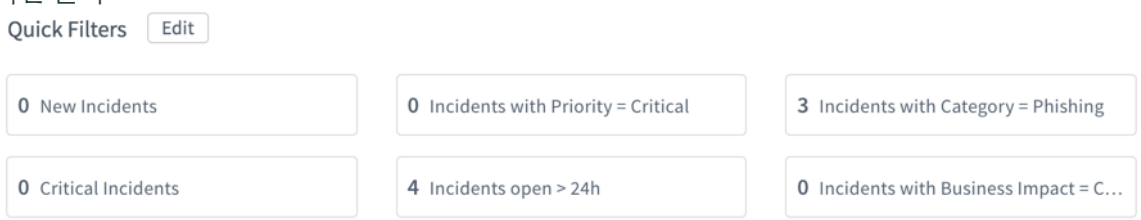
보안 인시던트



빠른 필터로 분석하려는 보안 인시던트를 찾습니다.

분석 보안 분석가 작업 공간 하려는 보안 인시던트를 빠르게 찾을 수 있도록 보안 인시던트 목록을 필터링하는 몇 가지 도구를 제공합니다. 빠른 필터를 사용하면 필터의 기준에 따라 보안 인시던트의 하위 집합을 선택할 수 있습니다.

빠른 필터



사용하려는 빠른 필터를 클릭하기만 하면 됩니다.

> **주:**
> 편집 버튼을 클릭하여 목록 화면에 표시할 빠른 필터를 지정할 수 있습니다. 최소 1개(최대 6개)의 필터를 선택해야 합니다.

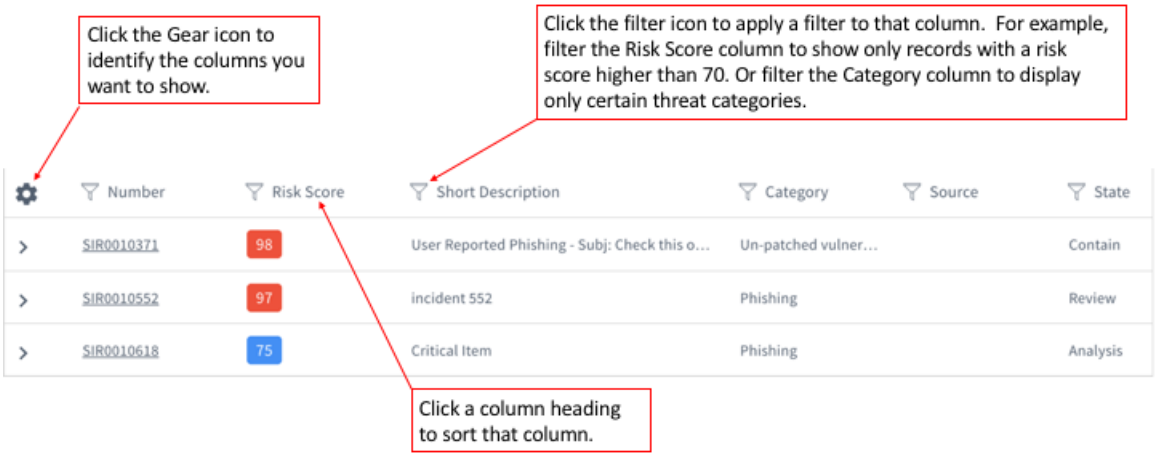
클래식 환경을 사용하여 에 대한 보안 분석가 작업 공간기본 필터뿐만 아니라 추가 빠른 필터도 정의할 수 있습니다. 자세한 내용은 에 대한 기본 및 보조 필터 설정 보안 분석가 작업 공간 문서를 참조하십시오.

보안 인시던트 목록 개인화

인스턴스의 모든 목록과 마찬가지로, 이 보안 분석가 작업 공간 앱은 분석 요구 사항에 맞게 목록을 개인화하고 표시된 정보를 정렬하는 도구를 제공합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

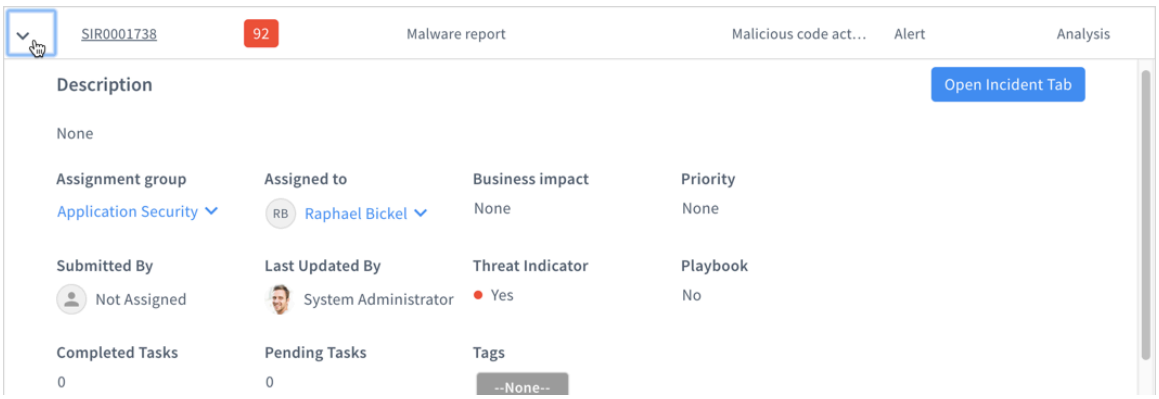
보안 인시던트 목록 개인화



엿보기 보기로 시간 절약

보안 인시던트 기록을 열기 전에 미리 보기 보기를 사용하면 시간을 절약할 수 있습니다. 이 기능을 사용하면 전체 페이지를 다시 로드하지 않고도 중요한 보안 아티팩트를 빠르게 찾을 수 있습니다. 보안 인시던트 번호 왼쪽에 있는 **>** 아이콘을 클릭하기만 하면 미리 볼 수 있습니다.

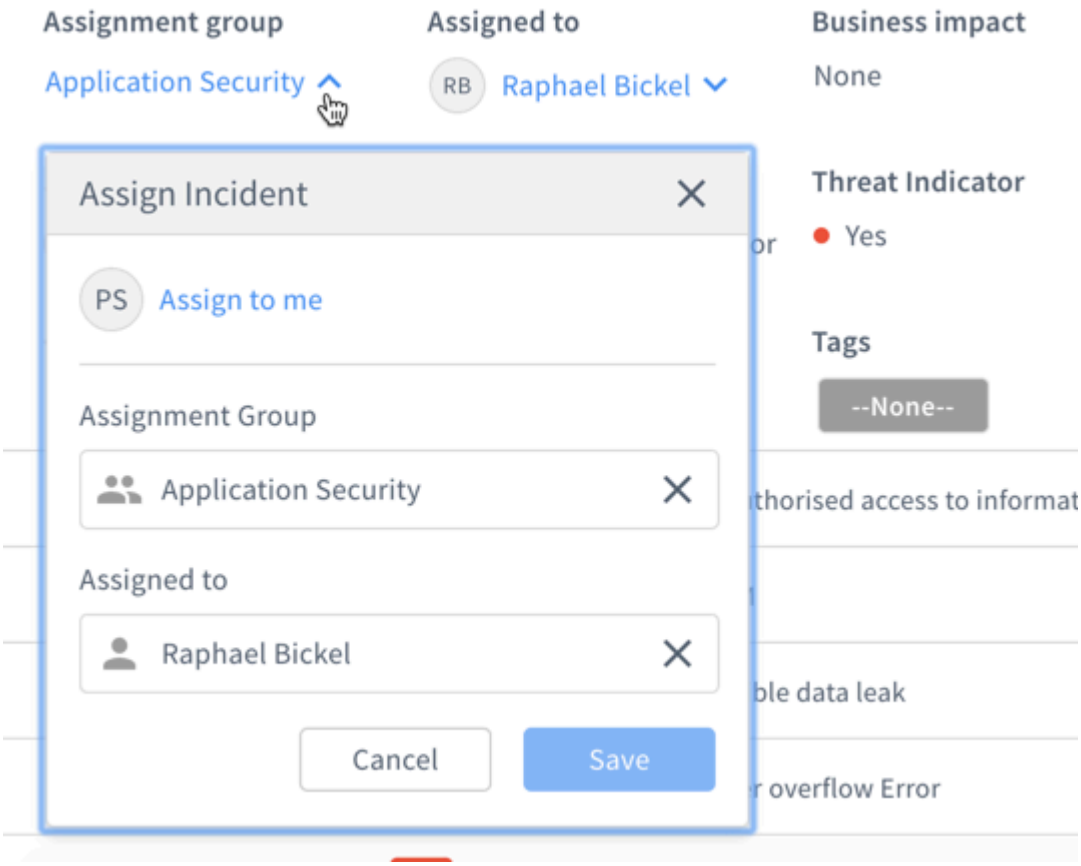
미리 보기



엿보기 보기는 단일 보기에서 중요한 정보의 스냅샷을 제공합니다. 이 뷰는 여러 인시던트로 작업할 때 귀중한 시간을 절약할 수 있습니다. 특정 필드에서 아래쪽 화살표를 클릭하여 할당 그룹 또는 특정 분석가 할당과 같은 즉석에서 업데이트를 수행할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

세부 정보 보기 보기



보안 인시던트에 대한 빠른 작업 수행

특정 보안 인시던트를 선택하고 연 후에는 해당 기록에서 시간을 절약해 주는 작업을 수행할 수 있습니다.

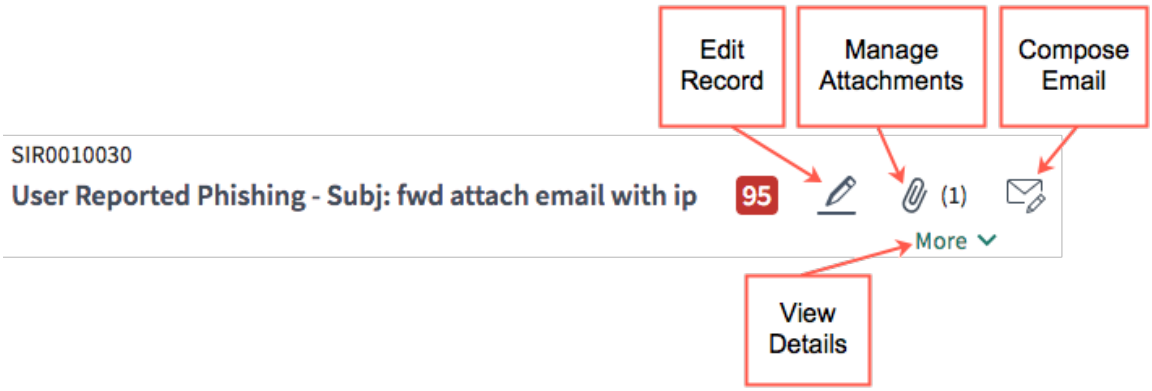
- 보안 인시던트가 열려 있는 경우 기록 편집 아이콘을 클릭하여 필드를 빠르게 변경합니다. 기록이 종결된 경우에는 해당 태그만 변경할 수 있습니다.
- 첨부 파일 관리를 클릭하여 보안 인시던트에 파일을 첨부합니다. 첨부 파일을 다운로드하거나 제거하고 첨부 파일에 적용된 암호화를 편집할 수도 있습니다.
- 이메일 작성을 클릭하여 동료에게 빠른 이메일을 보냅니다. 이메일은 자유 형식이거나 템플릿 목록에서 선택한 미리 준비된 이메일을 보낼 수 있습니다. 보낸 이메일과 받은 회신은 인시던트 타임라인에 캡처됩니다.

  주:
  이메일 및 이메일 알림에 재사용 가능한 콘텐츠가 포함된 사용자 지정 템플릿을 생성할 수 있습니다. 변수는 제목, 우선순위 또는 위협 범주와 같은 보안 인시던트 또는 경보와 관련된 정보를 삽입하는 데 사용할 수 있습니다. 와 관련된 보안 인시던트 응답이메일 및 이메일 알림에 보안 인시던트 〔sn_si_incident〕 테이블을 사용합니다. 자세한 내용은 이메일 템플릿을 참조하십시오.

- 자세히를 클릭하면 설명, 비즈니스 영향 및 우선순위와 같은 보안 인시던트의 간략한 스냅샷을 볼 수 있습니다. 할당 그룹 및 할당 대상 필드에서 아래쪽 화살표를 클릭하여 해당 필드를 즉석에서 변경할 수도 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

할당 그룹



여러 보안 인시던트 처리

탭 인터페이스를 사용하면 여러 보안 인시던트를 동시에 열어 둘 수 있으므로 클릭 한 번으로 전환 할 수 있습니다. 이를 통해 시간을 절약하고 여러 소스의 위협이 식별될 때 큰 그림을 볼 수 있습니다.

여러 보안 인시던트 처리

보안 인시던트 탭에서 분석 정보 보기

보안 인시던트 기록을 열면 다음 세 개의 탭이 표시됩니다.

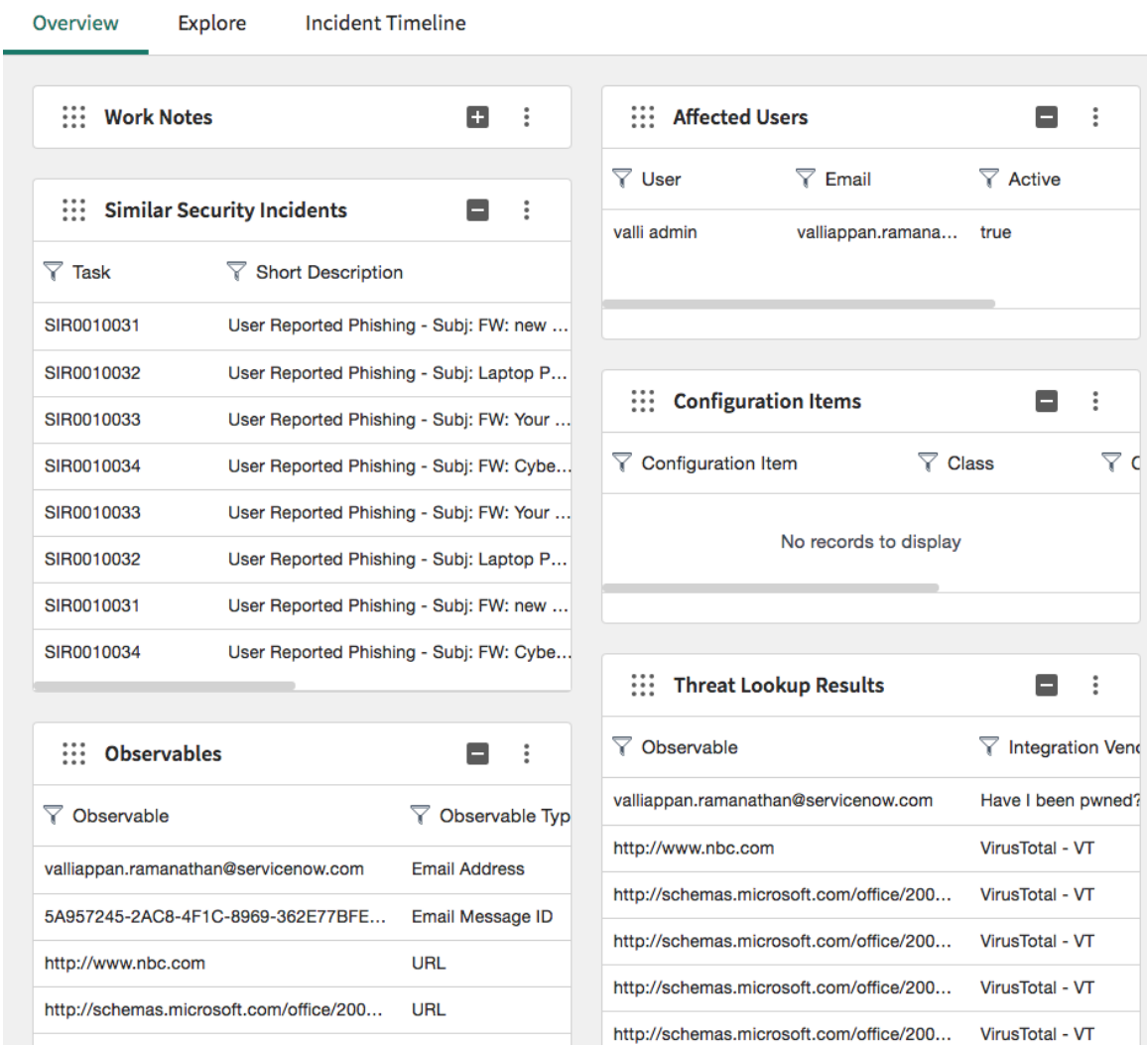
- 개요
- 탐색
- 인시던트 타임라인

개요 탭

개요 탭을 사용하여 단일 위치에서 보안 인시던트의 정보를 볼 수 있습니다. 다른 애플리케이션이나 콘솔을 열 필요가 없습니다.

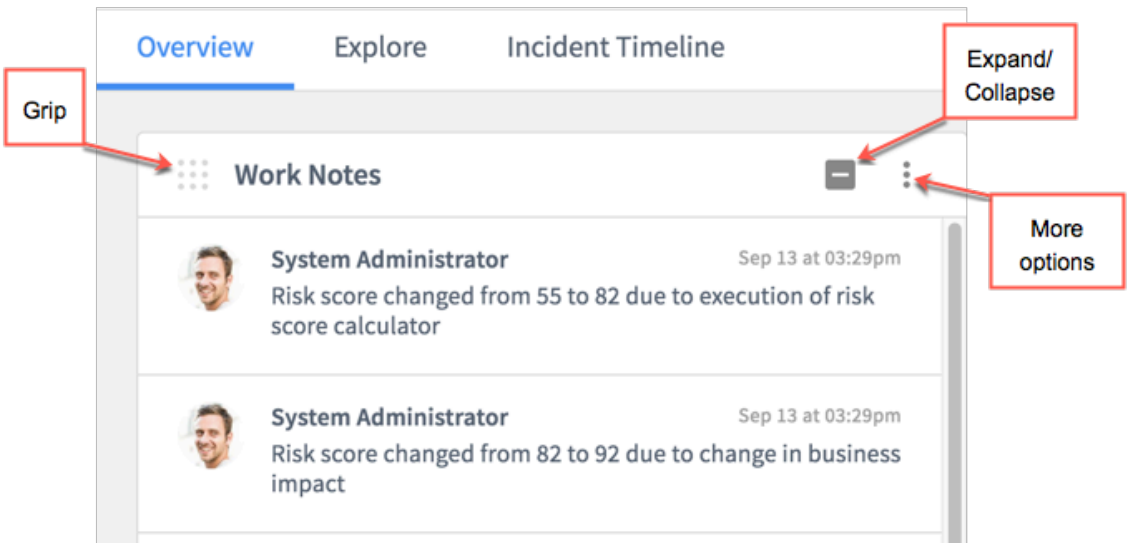
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

개요



개요 탭에 표시되는 타일은 사용자 지정할 수 있습니다. 필요에 따라 축소 및 확장할 수 있으며 그립 아이콘을 끌어 이동할 수 있습니다. 추가 옵션 아이콘을 클릭하여 타일을 삭제하거나 제목 텍스트를 변경합니다.

개요 탭

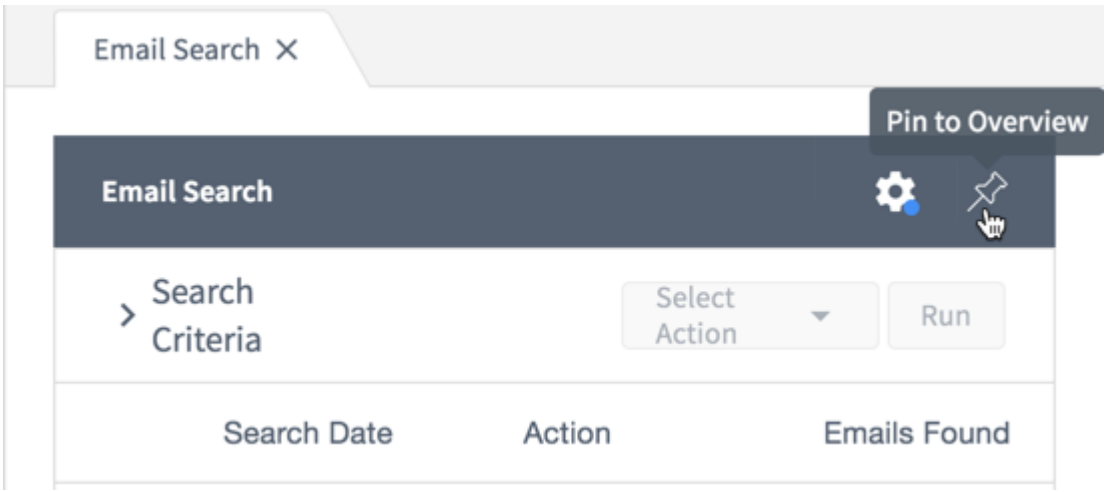


© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

탐색 탭

탐색 탭을 사용하여 개요 탭에 표시되는 타일을 구성합니다. 왼쪽 창에서 보려는 타일을 선택하고 핀 아이콘을 클릭하기만 하면 됩니다. 고정된 타일이 개요 탭에 자동으로 나타납니다.

노출 탭



탐색 탭의 왼쪽 창에는 개요 탭에 표시할 수 있는 다양한 정보가 포함되어 있습니다. 예를 들어 옵저버블을 확장하여 이러한 관련 목록을 표시합니다.

- 옵저버블
- 위협 조회 결과
- 보안 스캔 결과
- 도메인 조회
- 관찰 대상 보강

추가 관련 목록은 사용자, 구성 항목 및 인시던트에서 사용할 수 있습니다.

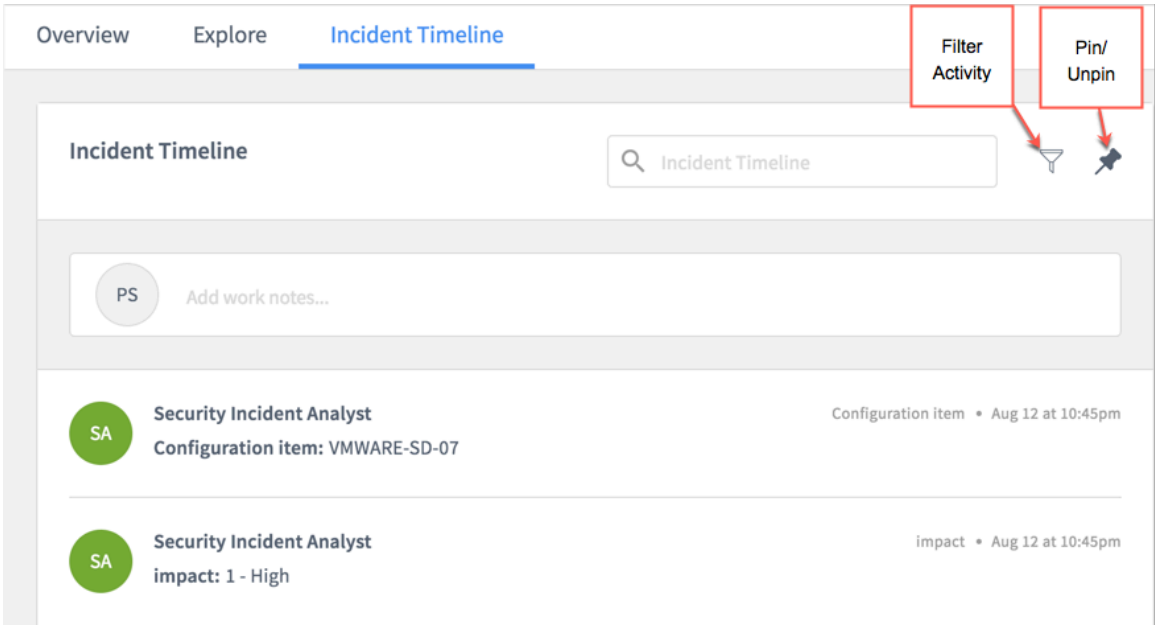
인시던트 타임라인 탭

추적 목적으로 조사 중에 인시던트 타임라인 탭을 사용합니다. 보안 인시던트에 대한 작업이 수행될 때마다 시스템은 이를 인시던트 타임라인에 기록합니다.

- 작업 메모 추가 상자에 작업 메모를 입력하고 게시를 클릭하여 타임라인에 작업 메모를 수동으로 추가할 수도 있습니다.
- 검색 상자를 사용하여 특정 타임라인 활동을 검색할 수 있습니다.
- 활동 필터링 아이콘을 사용하면 보려는 타임라인 활동 유형만 표시할 수 있습니다(예: 특정 분석가가 만든 인시던트만).
- 고정/고정 해제 아이콘을 사용하여 개요 탭에서 인시던트 타임라인을 추가하거나 제거할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

인시던트 타임라인 탭



Playbook을 사용하여 보안 인시던트 처리

내장된 보안 분석가 플레이북을 사용하여 특정 유형의 보안 위협을 단계별로 해결합니다. 예를 들어 분석가는 Playbook을 사용하여 악성 코드 활동으로 인한 피싱 공격 및 위협을 해결할 수 있습니다. 자세한 내용은 플레이북으로 보안 위협 해결 문서를 참조하십시오.

플레이북으로 보안 위협 해결

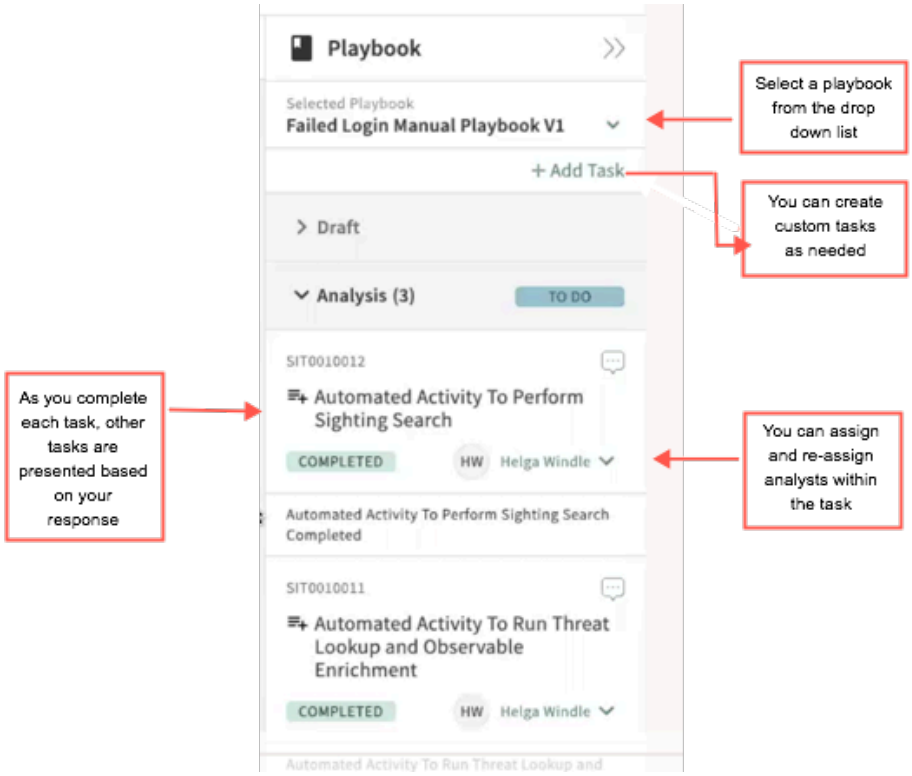
Playbook을 사용하여 특정 유형의 보안 위협을 단계별로 해결합니다. 예를 들어 Playbook을 사용하여 악성 코드 활동으로 인한 피싱 공격 및 위협을 해결할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.admin 또는 admin

이 태스크 정보
각 작업 그룹(분석, 포함 등)은 위협을 해결하기 위한 일련의 질문과 기타 활동으로 안내합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

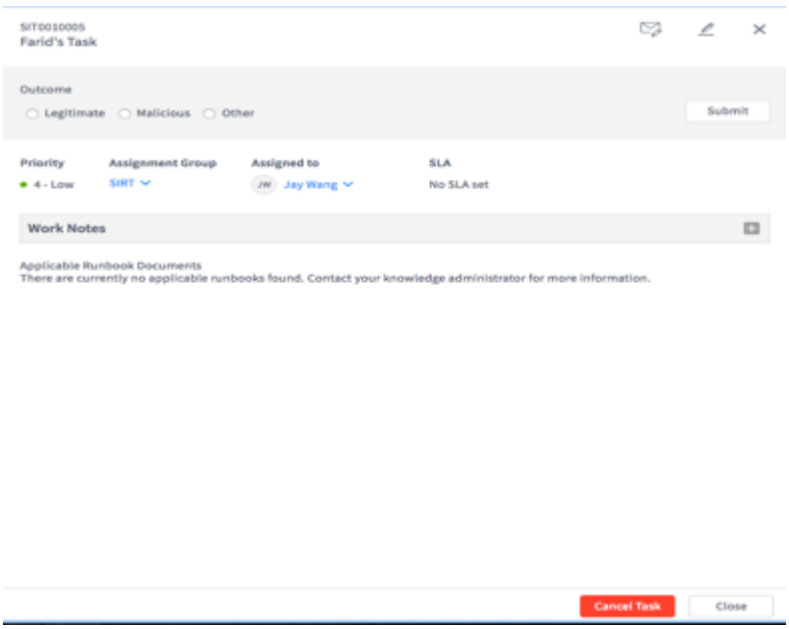
플레이북



각 작업을 수행할 때 나중에 유사한 공격을 분석하는 데 도움이 되는 작업 메모를 입력합니다. 위협이 식별되면 Playbook의 정보를 사용하여 위협을 격리하고, 영향을 유사하게 받는 자산을 격리하고, 맬웨어를 제거할 수도 있습니다.

각 작업에 포함된 지식 문서는 필요한 단계를 수행하는 데 도움이 되는 팁과 기타 정보를 제공합니다.

지식 문서



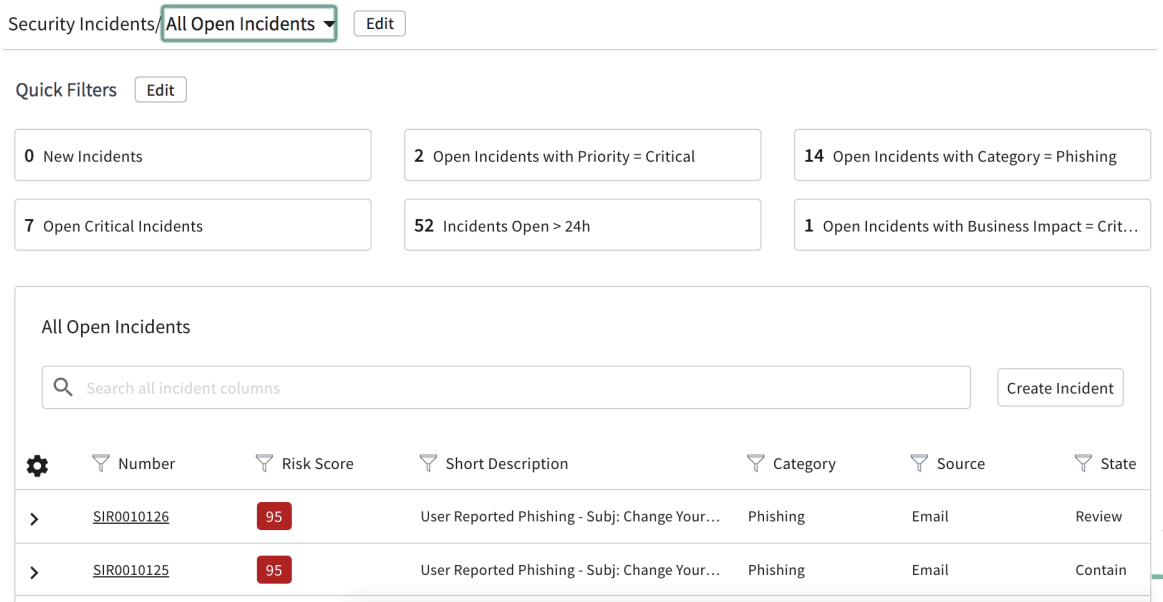
기본 시스템에는 각 플레이북 작업에 대한 지식 문서가 포함되어 있습니다. 그러나 자체 지식 문서를 작성 하여 플레이북 작업에 연결할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
플레이북을 사용하여 특정 위협을 분석하고 해결하는 방법의 예는 다음 문서를 플레이북으로 사용자가 보고한 피싱 공격 해결참조하십시오.

프로시저

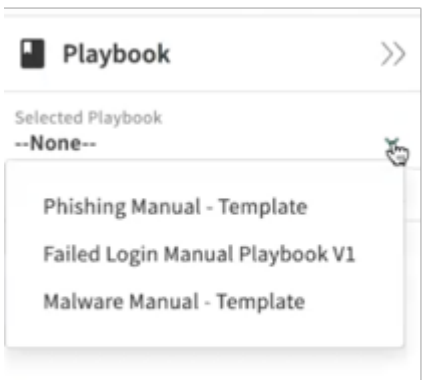
1. 다음으로 이동 모두 〉 보안 인시던트 〉 인시던트(신규 **UI**).
   보안 인시던트 화면에는 할당된 보안 인시던트가 표시됩니다.



2. 나에게 할당됨 선택 목록을 클릭하여 모든 열린 인시던트 또는 모든 미할당 인시던트와 같은 다른 필터를 선택할 수 있습니다.
   또는 빠른 필터 중 하나를 클릭하여 중요 인시던트와 같은 특정 유형의 보안 인시던트를 볼 수 있습니다.
3. 분석할 보안 인시던트를 클릭합니다.

   위험 점수가 높은 보안 인시던트의 우선순위를 정하는 것이 좋습니다.

4. 화면 오른쪽 가장자리에 있는 플레이북 창이 닫히면 플레이북 아이콘(플레이)을 눌러 엽니다.
   보안 인시던트에 플레이북이 할당되지 않은 경우 아래와 같이 선택한 플레이북 선택 목록에서 플레이북을 선택할 수 있습니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 인시던트에 다른 플레이북을 할당할 수도 있습니다. 선택한 플레이북 선택 목록에 플레이북을 포함하거나 보안 인시던트에 대한 플레이북을 변경하려면 에서 분석가 선택을 위해 플레이북 사용 확인할 수 있습니다.

보안 위협 유형에 맞는 플레이북이 열립니다. 이는 유사한 작업의 범주로 구분됩니다. 예를 들어 분석 그룹의 작업을 사용하여 위협의 유효성과 범위를 결정합니다. 포함 그룹에는 특정 사용자 또는 자산에 대한 위협을 격리하기 위한 작업이 포함됩니다. 근절 그룹의 작업은 맬웨어를 제거하거나 호스트를 이미지로 다시 설치하는 프로세스를 안내합니다.

5. 첫 번째 그룹(분석)을 클릭한 다음 플레이북에서 첫 번째 작업을 클릭합니다.
6. 작업의 프롬프트를 따릅니다.
   - 일부 작업은 "이메일이 캠페인의 일부입니까?"와 같은 질문을 합니다. 질문에 대답하는 데 필요한 분석을 수행하고 예 또는 아니요를 선택합니다.
   - 지식 문서를 정의하고 플레이북 작업과 연결한 경우 작업을 시작할 때 문서가 나타납니다.
   - 일부 작업은 과도기적입니다. 단순히 보안 인시던트에 옵저버블을 추가하는 등의 작업을 수행하도록 지시할 뿐입니다. 작업을 완료한 후 완료로 표시를 클릭합니다.

   작업을 완료하면 선택한 항목에 따라 후속 작업이 표시됩니다. 회색으로 표시된 그룹(예: 복구, 검토 등)은 선택에 따라 활성화될 수 있습니다.
7. 위협을 해결하고 보안 인시던트를 종결하기 위한 모든 작업을 완료할 때까지 제시된 각 작업을 계속 수행합니다.

관련 정보

플레이북에 사용자 지정 작업 추가

플레이북으로 사용자가 보고한 피싱 공격 해결

피싱 플레이북은 회사 직원 중 한 명이 보고한 피싱 공격을 분석하고 해결하는 데 필요한 작업을 안내합니다.

사용자가 보고한 피싱 공격에서 보안 인시던트를 생성하는 방법

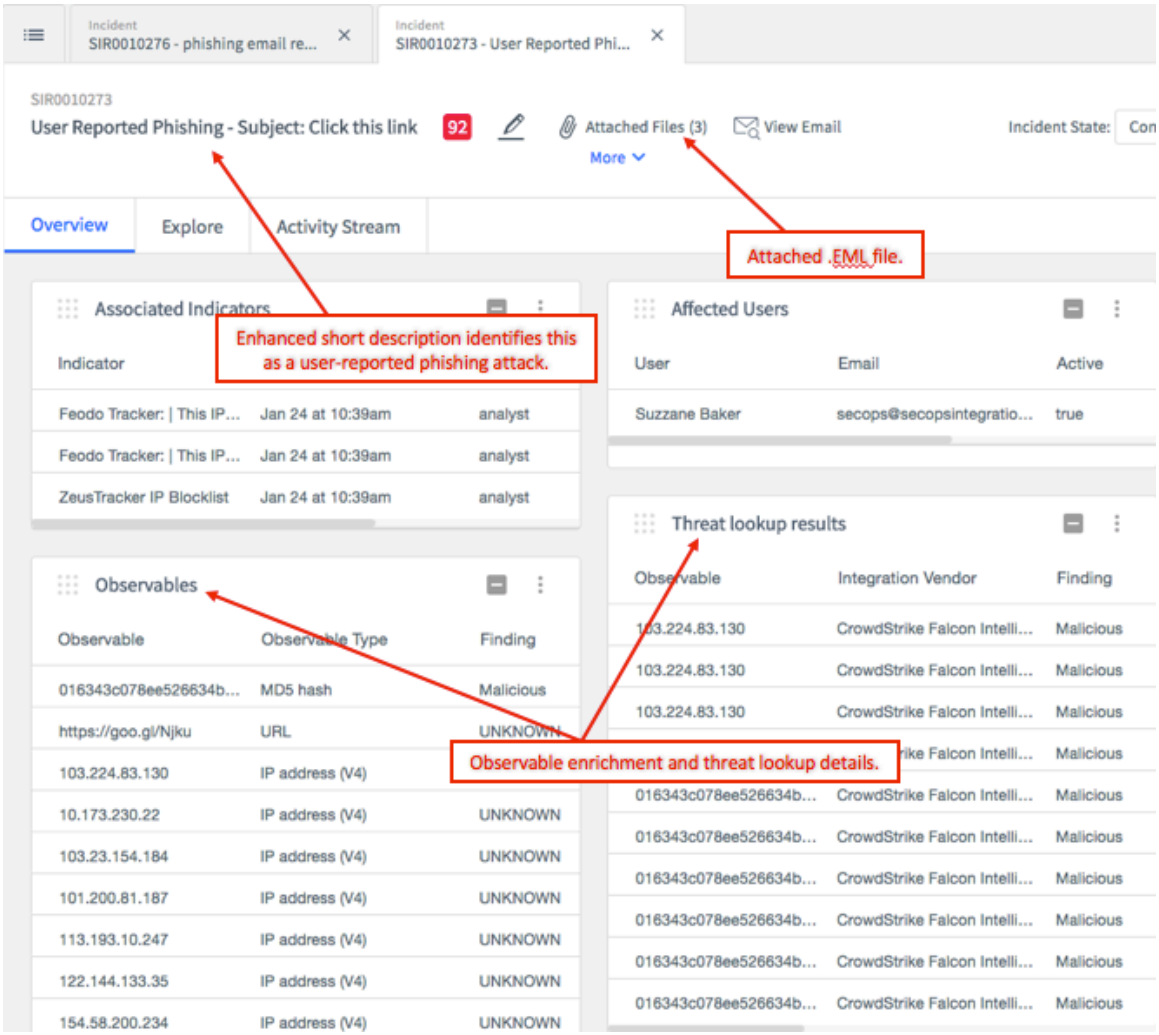
보안 인시던트 응답을 설정하는 동안 시스템 관리자는 피싱 공격의 징후가 포함된 이메일을 식별할 수 있는 일련의 이메일 일치 규칙을 만듭니다. 직원이 피싱 공격의 일반적인 징후가 포함된 의심스러운 이메일을 수신하면(보안 정책에서 정의한대로) 해당 이메일을 . 조직에서 정의한 피싱 이메일 주소에 대한 EML 첨부 파일입니다.

피싱 이메일 주소로 이메일이 수신되면 . EML 첨부 파일이 구문 분석되고 해당 정보가 이메일 일치 규칙과 비교됩니다. 일치하는 항목이 발견되면 다음 정보를 포함하는 보안 인시던트가 생성됩니다.

- 짧은 설명에는 사용자가 보고한 피싱과 발신 이메일의 실제 제목이 포함됩니다.
- 이 . EML 파일이 보안 인시던트에 첨부되어 있습니다.
- 만약 . EML에는 모든 옵저버블이 포함되어 있으며 구문 분석되고 보강 및 위협 조회가 자동으로 수행됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

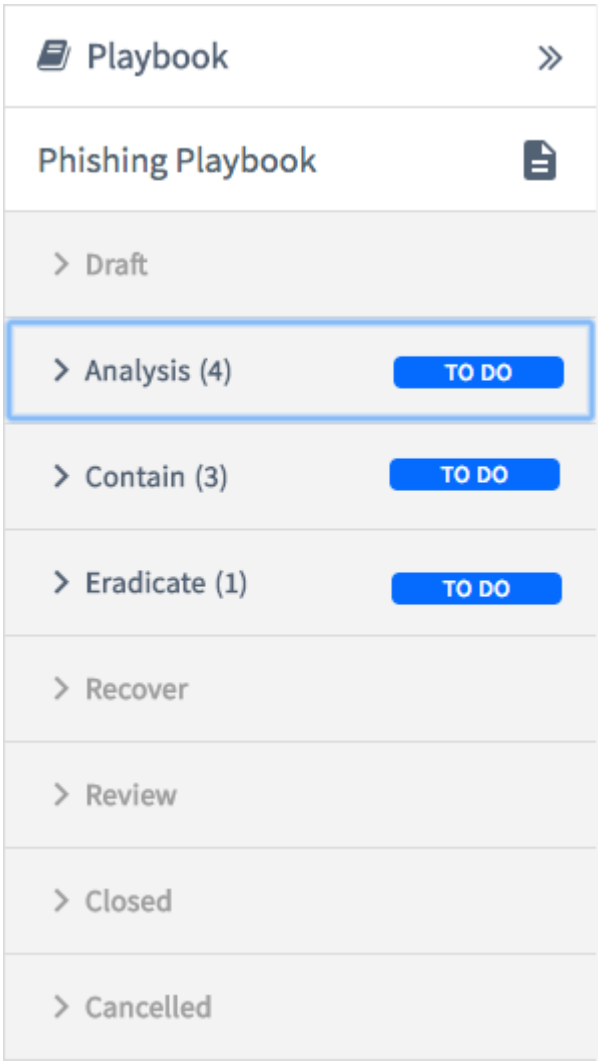
사용자가 보고한 피싱



피싱 범주 보안 인시던트가 열리면 피싱 플레이북을 자동으로 사용할 수 있습니다. 플레이북 아이콘( )을 클릭하여 플레이북을 열기만 하면 됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

피싱 플레이북



피싱 플레이북에는 피싱 위협을 분석, 억제 및 근절하는 데 도움이 되는 작업이 포함되어 있습니다. 작업은 상태(예: 분석, 포함 등)로 구성됩니다. 상태에 대한 모든 작업이 완료되면 플레이북이 다음 상태로 안내합니다.

보안 인시던트 상세 정보 분석

보안 인시던트가 분석 상태인 경우 다음을 포함하여 인시던트에 대한 기본 조사를 수행하는 작업이 제공됩니다.

- 인시던트의 유효성을 확인하는 중입니다.
- 잠재적 위협의 영향을 연구합니다.
- 인시던트에 대한 효과적인 대응을 조정합니다.

작업을 진행하면서 다음을 수행합니다.

- 지식 문서를 숙지합니다.
- 이메일 첨부 파일을 열고 일반적인 피싱 요소의 징후가 있는지 검사합니다.
- 위협 조회 결과를 검토합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 인시던트 포함

보안 인시던트가 포함 상태인 경우 이메일의 상세 정보를 검토하는 작업이 제공됩니다. 위협이 조직에 침투할 수 없도록 하려면 침입 방어 시스템(IDS) 및 침입 방지 시스템(IPS) 서명 및 규칙의 형태로 네트워크 방어를 업데이트합니다.

작업을 진행하면서 다음을 수행합니다.

- 영향을 받는 장치를 격리하는 등 위협 영향을 제한하기 위한 조치를 취합니다.
- 이메일에 첨부된 옵저버블을 검토합니다.
- 다음을 포함하여 알려진 위협과 이메일 컨텐츠가 연관되어 있는지 확인합니다.
  - URL
  - 이메일 발신자
  - 피싱 URL
  - 보낸 사람 SMTP 서버의 IP 주소

맬웨어 근절

업데이트된 서명 및 규칙을 바이러스 백신 솔루션에 배포한 후 **Eradicate** 상태의 작업을 사용하여 맬웨어가 있는지 확인하고 그에 따라 처리합니다.

작업을 진행하면서 다음을 수행합니다.

- 영향을 받는 장치의 엔드포인트에서 맬웨어가 있는지 검사합니다.
- 발견된 맬웨어를 제거합니다.
- 최후의 수단으로 호스트 장치를 지우고 이미지로 다시 설치합니다.

보안 인시던트 검토

분석 작업을 수행할 때 피싱 공격이 허위 경보인 것으로 확인되면 보안 인시던트가 검토 상태로 이동하므로 이메일 첨부 파일을 열어도 안전하다는 것을 사용자에게 알려야 합니다.

보안 인시던트 종결

Playbook의 모든 작업이 완료되면 보안 인시던트가 종결 상태로 전환됩니다. 인시던트를 종결하려면 종결 코멘트를 입력해야 합니다.

보안 인시던트 취소

보안 인시던트가 검토 상태이고 사용자에게 이메일이 위협이 아니라는 것을 성공적으로 알린 경우 취소 됨 상태가 활성화되고 보안 인시던트를 취소할 수 있습니다.

주:
복구 작업은 피싱 플레이북에서 사용되지 않습니다.

지식 문서를 플레이북 작업과 연결

플레이북을 보안 인시던트 응답 사용하여 보안 위협을 분석할 때 조직에서 정의한 각 작업에 대한 지식 문서를 볼 수 있습니다. 지식 문서가 없는 경우 문서를 생성하고 플레이북 작업에 연결할 수 있습니다.

시작하기 전에
의 보안 인시던트 응답플레이북을 사용할 때 각 작업과 연결된 텍스트를 기록해 둡니다. 예를 들어 피싱 범주의 첫 번째 작업은 **Was Alert Employee-Submitted?**(경보가 직원에 의해

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

제출되었습니까?)입니다. 이것은 작업에 대한 간단한 설명이며, 지식 문서를 작업과 연결하려면 이 텍스트(플레이북에 표시된 것과 일치)가 필요합니다.

필요한 역할: sn_sir.knowledge_admin, sn_si.admin 또는 admin

프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 카탈로그 및 지식베이스 〉 지식.
2. 특정 플레이북 작업에 대한 지식 문서를 생성하고 게시합니다.
3. 다음으로 이동 보안 인시던트 〉 수동 **Runbook** 〉 새 **Runbook** 생성.
4. 다음 정보를 입력하여 Runbook을 생성합니다.

필드	설명
지식 문서	플레이북 작업과 연결할 게시된 지식 문서를 선택합니다.
테이블	작업 〔sn_si_task〕을 선택합니다 보안 인시던트 응답 .
조건	조건 작성기를 다음과 같이 설정합니다. ○ 선택:간단한 설명을 선택합니다. ○ 연산자:을(를) 선택합니다. ○ 입력 값: Playbook에 표시된 대로 작업에 대한 간단한 설명을 정확하게 입력합니다.

5. 제출을 클릭합니다.
   다음에 플레이북을 실행하고 이 작업을 선택하면 연결된 지식 문서가 표시됩니다.

관련 정보

보안 인시던트 지식 문서 생성

보안 인시던트 응답 Runbook 생성

플레이북에 사용자 지정 작업 추가

기본 시스템에는 보안 분석가 작업 공간 각 위협 범주에 대한 일련의 작업이 포함되어 있습니다. 시스템 또는 고객의 고유한 요구를 충족하는 사용자 지정 작업을 생성할 수 있습니다.

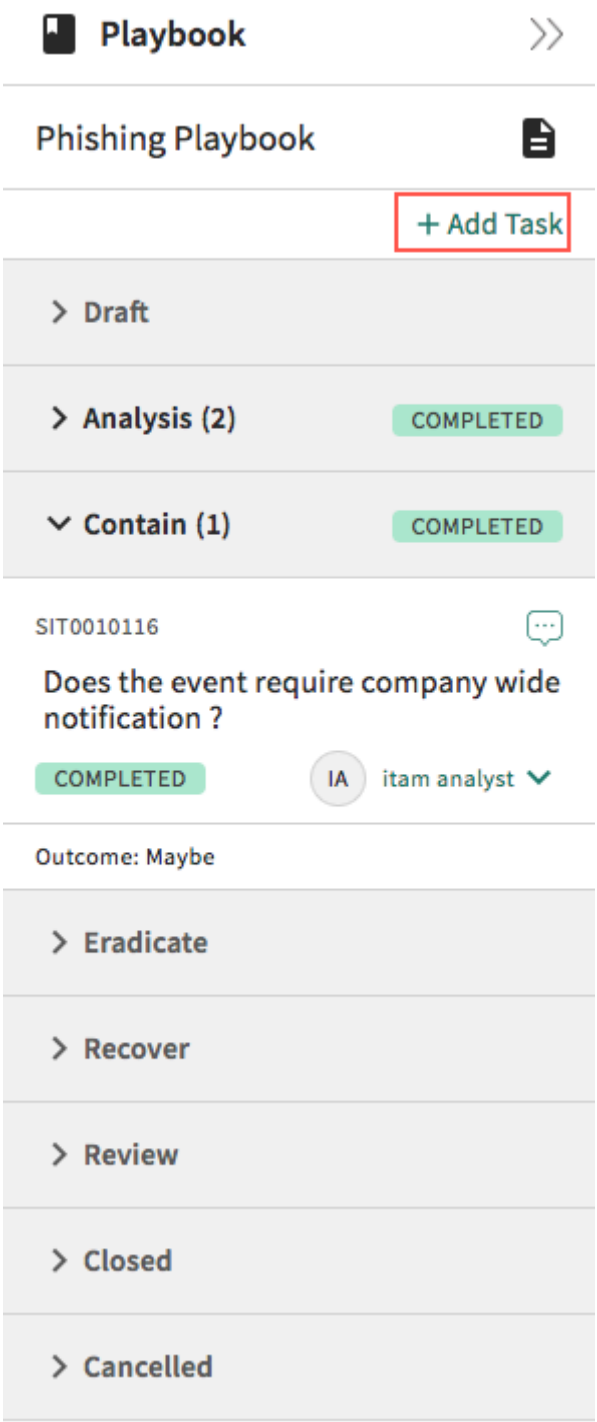
시작하기 전에

필요한 역할: sn_si.basic 또는 security_admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

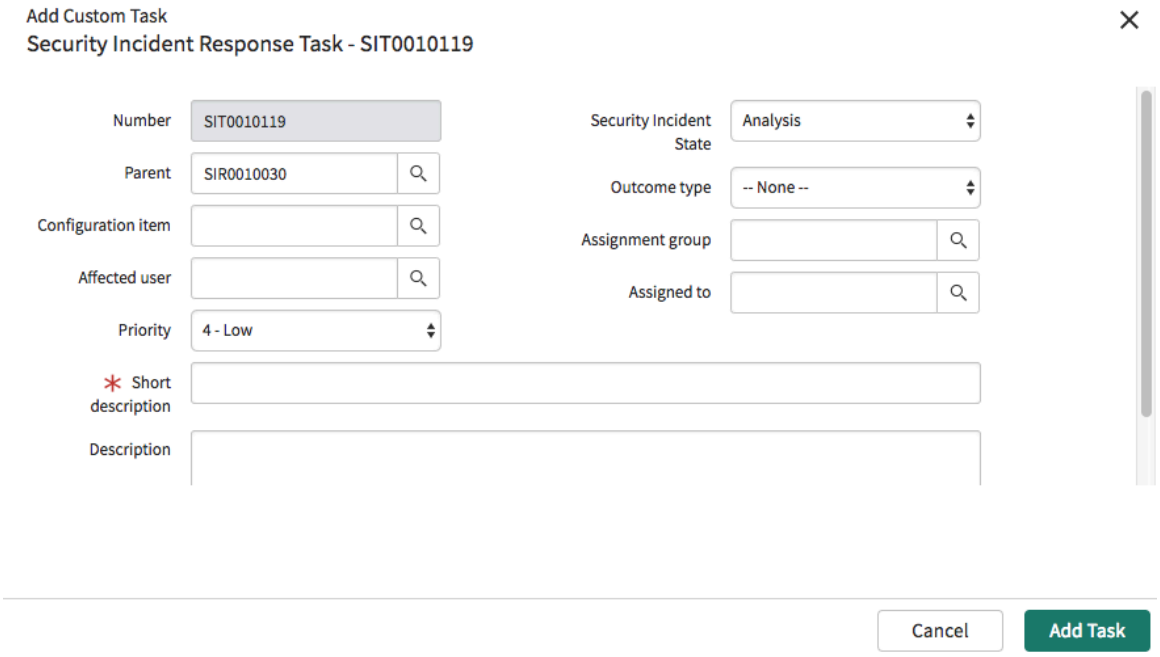
프로시저

1. 플레이북이 열리면 작업 추가를 클릭합니다.



사용자 지정 작업 추가 화면이 열립니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



2. 필요에 따라, 필드를 채웁니다.

필드	설명
번호	〔읽기 전용〕 자동으로 생성된 보안 인시던트 작업 번호입니다.
상위	관련 보안 인시던트의 수입니다.
구성 항목	보안 문제의 영향을 받는 구성 항목입니다(있는 경우).
영향을 받는 사용자	보안 문제의 영향을 받는 사용자입니다(있는 경우).
우선순위	이 작업을 수행해야 하는 시기를 결정하는 데 사용되는 우선순위를 선택합니다.
보안 인시던트 상태	보안 응답 작업의 현재 상태입니다. 필요한 경우 미래 상태를 선택할 수 있습니다.
결과 유형	sn_si.basic 역할이 있는 경우 결과 유형으로 예/아니요 를 선택합니다. security_admin 역할이 있는 경우 여러 사용자 지정 출력 값을 사용하여 사용자 지정 결과 형식을 만들 수 있습니다. 예를 들어 위협 범주에 따라 종속 값으로 작업을 정의할 수 있습니다. 자세한 내용은 선택 목록을 참조하십시오.
할당 그룹	할당된 작업자가 선택될 할당 그룹입니다.
담당자	작업을 수행하도록 할당된 개인입니다.
간단한 설명	보안 인시던트 플레이북 작업에 대한 설명입니다.
설명	선택한 작업에 대한 설명을 입력합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 입력을 마쳤으면 작업 추가를 클릭합니다.
   작업은 현재 작업 다음에 플레이북에 삽입됩니다.

사용자가 보고한 피싱 및 맬웨어 공격에 대한 사이팅 검색

이메일 또는 옵저버블에 대한 사이팅 검색을 수행하여 네트워크에서 피싱 공격 또는 악성 IP 또는 URL을 사용한 통신과 같은 특정 유형의 공격이 발생하는 빈도를 확인합니다. 각 발생은 사이팅으로 간주됩니다. 옵저버블에 대한 사이팅 검색은 로그 저장소 또는 SIEM(보안 정보 및 이벤트 관리)에 대해 구성해야 합니다.

사이팅 검색 기능을 사용하여 피싱된 사용자를 찾고 네트워크의 로그 저장소 내에서 피싱 및 맬웨어 옵저버블을 추적하는 방법입니다.

사이팅 검색 기능을 사용하여 피싱된 사용자를 찾고 네트워크의 로그 저장소 내에서 피싱 및 맬웨어 옵저버블을 추적하는 방법을 알아보려면 이 3분짜리 비디오를 시청하십시오.

다음 용어는 사용자가 보고한 피싱 공격을 설명하는 데 사용됩니다.

- 피싱 사용자: 피싱 이메일을 받은 사용자입니다.
- 피해자 사용자: 일반적으로 피싱 이메일의 링크를 클릭하여 피싱 URL과 상호 작용한 사용자입니다. 이 작업은 잠재적으로 공격자에게 자격 증명을 노출합니다.

피싱 인시던트 분석을 시작할 때 이메일 사이팅 검색 수행 또는 옵저버블 사이팅 검색 수행 을 수행하여 동일한 피싱 공격의 영향을 받는 조직의 다른 사용자를 식별할 수 있습니다. 로그 저장소를 검색하여 피싱 및 피해자 사용자를 식별합니다. 영향을 받는 사용자 목록을 식별한 후에는 에서 사용할 수 보안 인시던트 응답있는 도구를 사용하여 포괄적인 인시던트 응답 절차를 수행하는 하위 보안 인시던트를 생성합니다.

주:
다음 방법을 사용하여 사이팅 검색을 수행할 수도 있습니다.

- 다음으로 이동 보안 인시던트 〉 모든 인시던트 표시 을 클릭하고 보안 인시던트를 클릭합니다.
- 관련 링크에서 **IoC** 표시를 클릭합니다. 옵저버블 목록이 표시됩니다.
- 목록에서 옵저버블을 선택하고 작업 목록에서 다음 옵션 중 하나를 선택합니다.
  - 웹 트래픽 사이팅 검색 실행
  - 이메일 트래픽 사이팅 검색 실행
- 시간 범위를 지정하고 검색을 클릭하여 사이팅 검색을 수행합니다.

저장된 사이팅 검색 구성

사이팅 검색을 구성하고 SIEM에 대해 저장된 구성 또는 옵저버블 인스턴스에 대한 기타 로그 저장소를 생성하여 사용자 환경에 악의적인 옵저버블이 있는지 확인합니다.

주:
저장된 검색 및 즉석 쿼리는 Splunk 통합에 대해서만 지원됩니다.

관련 정보

사이팅 검색 구성 기록 생성

사용자가 보고한 피싱 공격에 대한 이메일 사이팅 검색을 수행합니다.

이메일 제목, 보낸 사람 이름 또는 메시지 ID와 같은 옵저버블을 기반으로 피싱 이메일을 받은 사용자를 검색합니다. 그런 다음 조직에서 이러한 피싱 이메일을 포함하고 근절할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_si.analyst

이 태스크 정보
Splunk 이메일 트래픽 로그를 검색하여 의심스러운 이메일의 수신자 목록을 수집합니다. 이메일 발신자, 이메일 메시지 ID 또는 보안 인시던트와 연관된 이메일 제목을 기준으로 사용하여 검색을 수행할 수 있습니다.

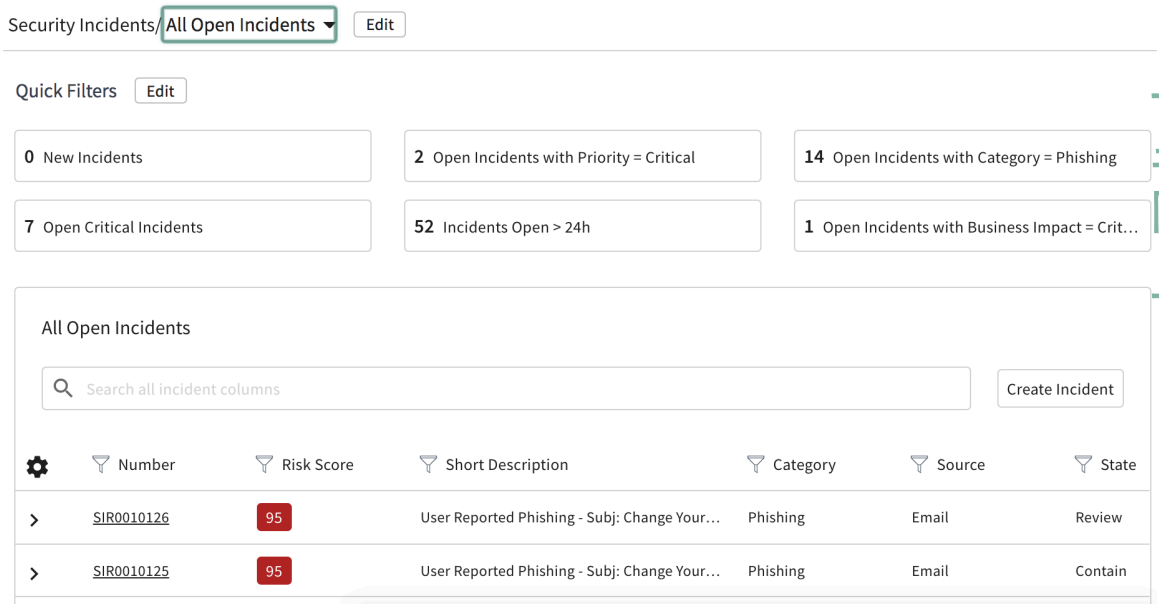
주:

- 이메일 기반 옵저버블에 대한 이러한 사이팅 검색 구현은 Splunk Enterprise 로그 스토어에서만 테스트되었습니다.
- Splunk 로그 이벤트는 사이팅 검색 쿼리가 정확한 결과를 반환할 수 있도록 CIM(공통 정보 모델)과 호환되어야 합니다.

프로시저

1. 팀에 할당된 보안 인시던트를 보려면 보안 인시던트 〉 인시던트(신규 **UI**).
2. 보안 인시던트 목록에서 모든 미해결 인시던트, 사용자에게 할당된 모든 인시던트 또는 모든 인시던트 등의 필터 중 하나를 선택합니다.

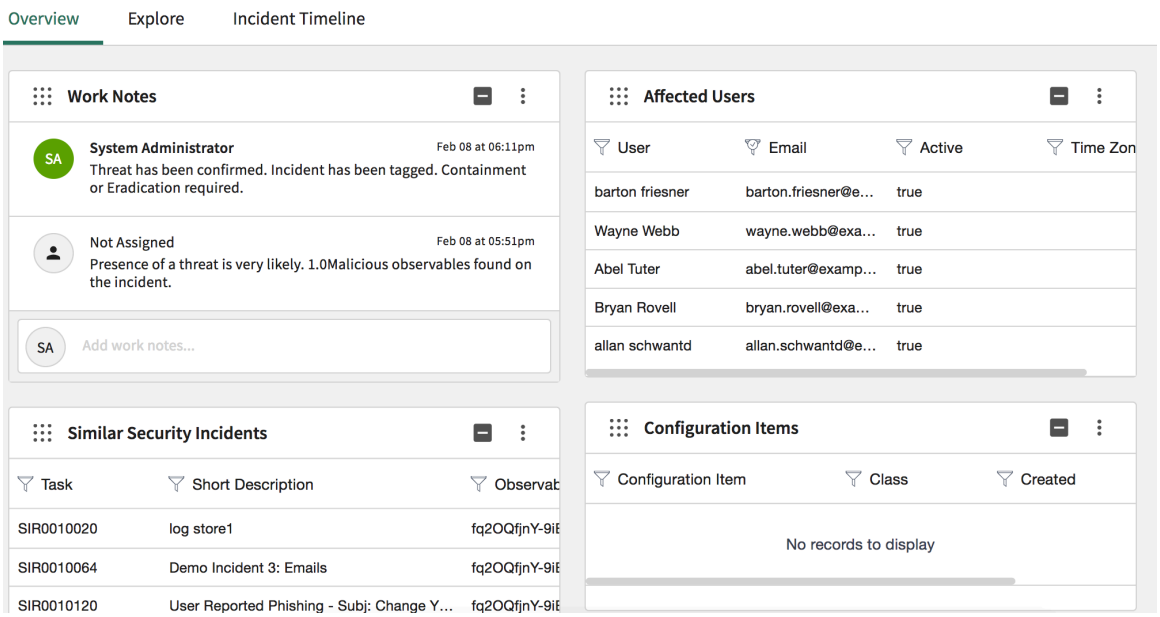
   중요 인시던트 또는 피싱 이메일과 같은 특정 유형의 보안 인시던트 를 보려면 빠른 필터 중 하나를 클릭합니다.



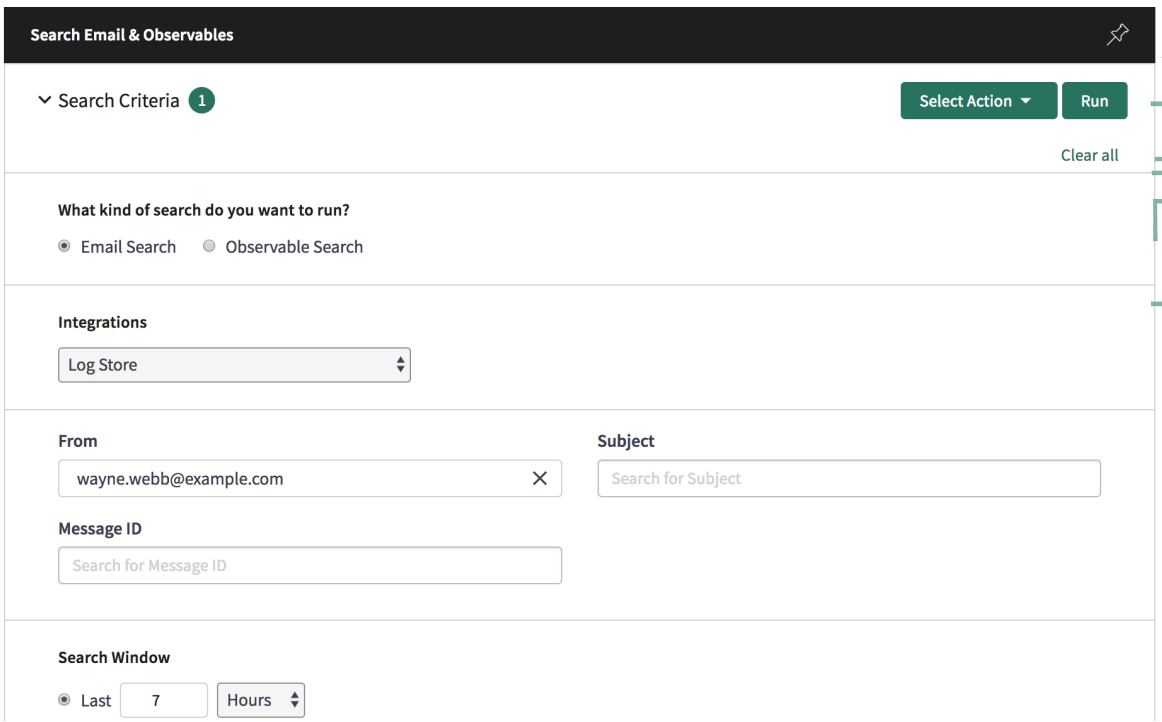
3. 분석할 보안 인시던트를 클릭합니다.

   개요 탭은 옵저버블, 영향을 받는 사용자 및 유사한 보안 인시던트 목록을 포함하여 보안 인시던트에 대한 개요를 제공합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 탐색 탭을 클릭합니다.
5. 인시던트 데이터에서 조사 〉 이메일 및 옵저버블 검색.



6. 검색 기준 섹션을 확장합니다.
7. 실행할 검색 유형으로 이메일 검색을 선택하고 나머지 검색 기준을 지정합니다.

검색 기준 양식

필드	설명
통합	통합 유형입니다. 목록에서 로그 저장소를 선택합니다.

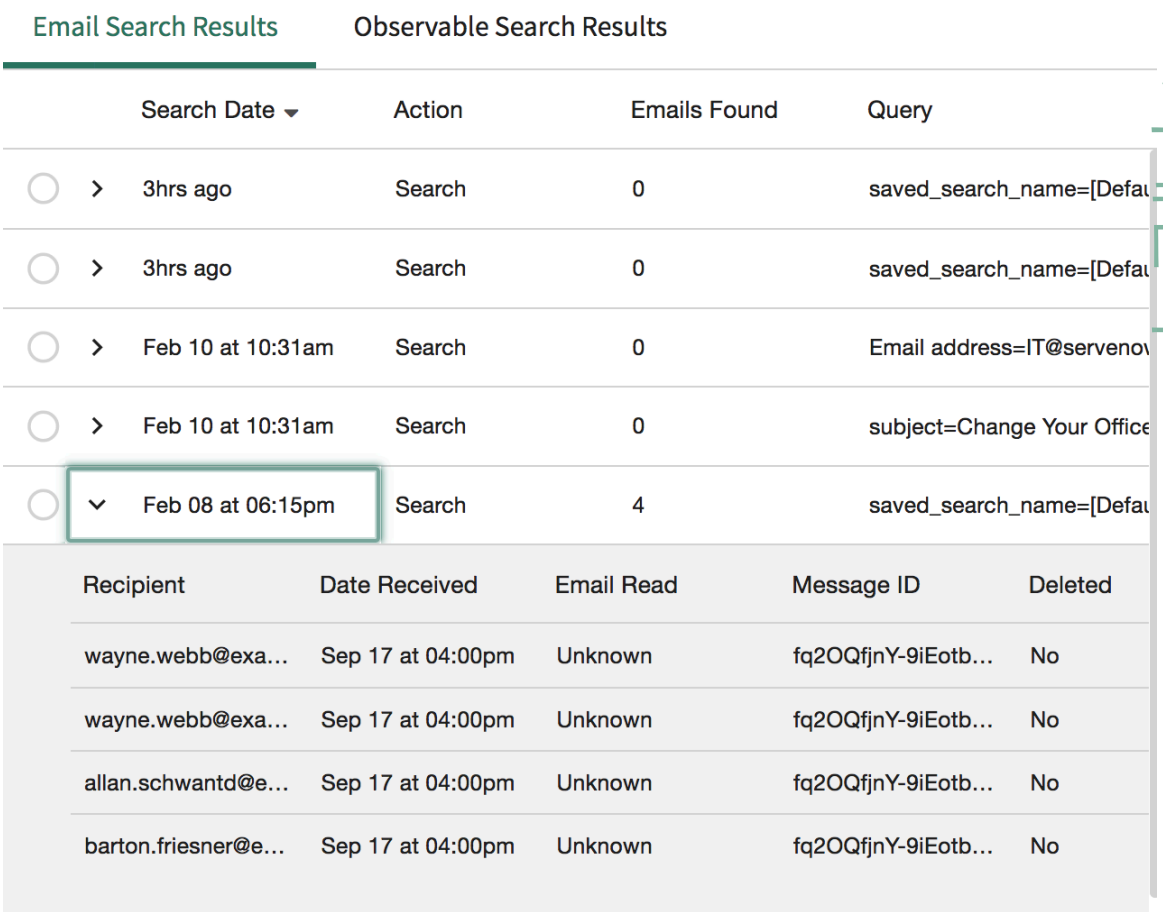
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	주: 이 기능은 Splunk 로그 스토어에서만 지원됩니다.
시작일	보낸 사람의 전체 이메일 주소(예: jane.doe@example.com)입니다.
메시지 ID	로그 저장소의 이메일 메시지 ID입니다.
제목	피싱 이메일의 제목입니다.
검색 기간	검색할 시간 창(예: 지난 24시간)입니다.

8. 작업 선택 목록에서 검색을 선택하고 실행을 클릭합니다.

   입력한 조건을 사용하여 Splunk 로그 저장소가 검색되고 피싱 공격의 대상이 되는 사용자가 이메일 검색 결과 탭에 표시됩니다. 피싱 이메일의 총 수와 각 이메일의 상세 정보(이메일 수신 날짜, 수신자 및 메시지 ID 포함)가 표시됩니다.

9. 피싱 이메일을 받은 사용자 목록을 보려면 검색 날짜 열에서 **>** 기호를 클릭합니다.



10. 이메일을 받은 사용자 목록을 보려면 사용자 〉 영향을 받는 사용자.

    피싱 사용자 열은 이메일 받는 사람을 식별합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
영향을 받는 사용자 페이지에는 ServiceNow 인스턴스에 있는 사용자 기록만 표시됩니다.

11. 피싱 공격의 대상인 사용자를 추가로 조사하려면 다음 단계를 수행합니다.
    a. 사용자 이름 옆에 있는 확인란을 선택합니다.
    b. 목록에서 **Create Child Security** Incident(하위 보안 인시던트 생성)를 선택하고 Run(실행)을 클릭합니다.

하위 보안 인시던트가 생성되었음을 보여주는 메시지가 표시됩니다. 상위 인시던트와 연결된 하위 보안 인시던트를 보려면 탐색 탭을 클릭하고 인시던트 〉 하위 보안 인시던트.

결과
피싱 처리된 사용자 목록이 표시됩니다.

사용자가 보고한 피싱 및 맬웨어 공격에 대한 옵저버블 사이팅 검색을 수행합니다.

옵저버블에 대한 사이팅 검색을 수행하여 특정 기간 내에 악의적이거나 의심스러운 웹 사이트를 방문한 사용자 수를 확인합니다.

시작하기 전에
필요한 역할: sn_si.analyst

이 태스크 정보
보안 인시던트와 관련된 URL, 대상 호스트 또는 대상 IP 주소와 같은 옵저버블에 대해 네트워크 트래픽 검색을 수행할 수 있습니다.

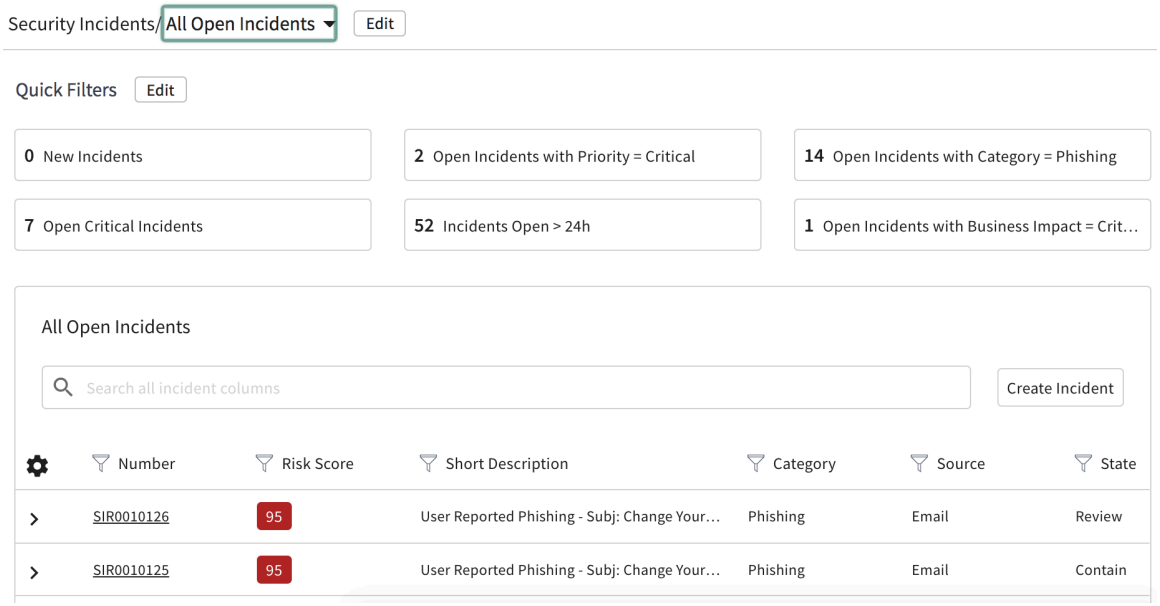
주:
- 옵저버블에 대한 이러한 사이팅 검색 구현은 Splunk Enterprise 로그 저장소에서만 테스트되었습니다.
- Splunk 로그 이벤트는 사이팅 검색 쿼리가 정확한 결과를 반환할 수 있도록 CIM(공통 정보 모델)과 호환되어야 합니다.

프로시저

1. 팀에 할당된 보안 인시던트를 보려면 다음으로 이동합니다. 보안 인시던트 〉 인시던트(신규 **UI**).
2. 보안 인시던트 목록에서 나에게 할당된 모든 인시던트, 모든 오픈 인시던트 또는 모든 인시던트와 같은 다른 필터를 선택합니다.

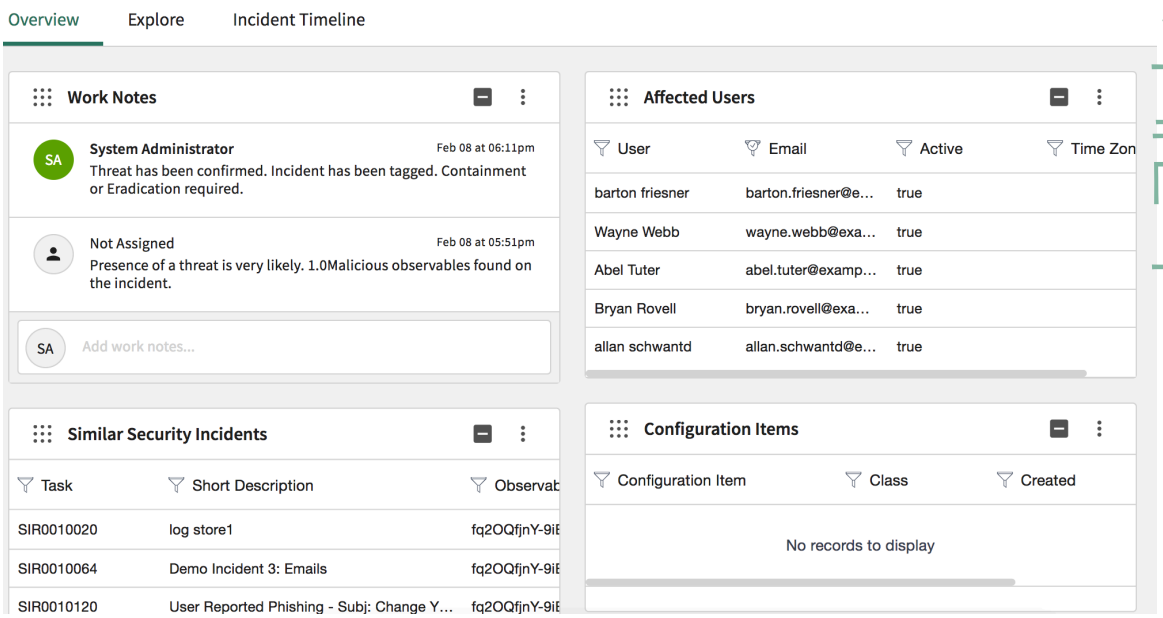
   중요 인시던트 또는 피싱 이메일과 같은 특정 유형의 보안 인시던트 를 보려면 빠른 필터 중 하나를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



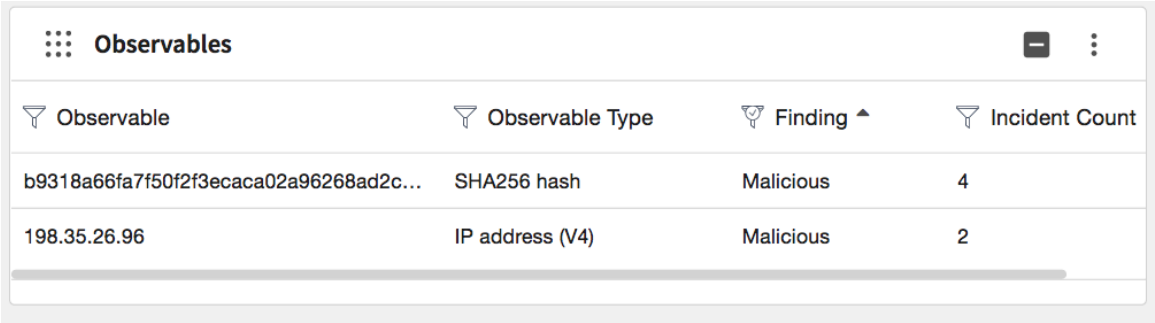
3. 분석할 보안 인시던트를 클릭합니다.

옵저버블, 영향을 받는 사용자 및 유사한 보안 인시던트 목록을 포함하여 보안 인시던트에 대한 개요를 볼 수 있습니다.

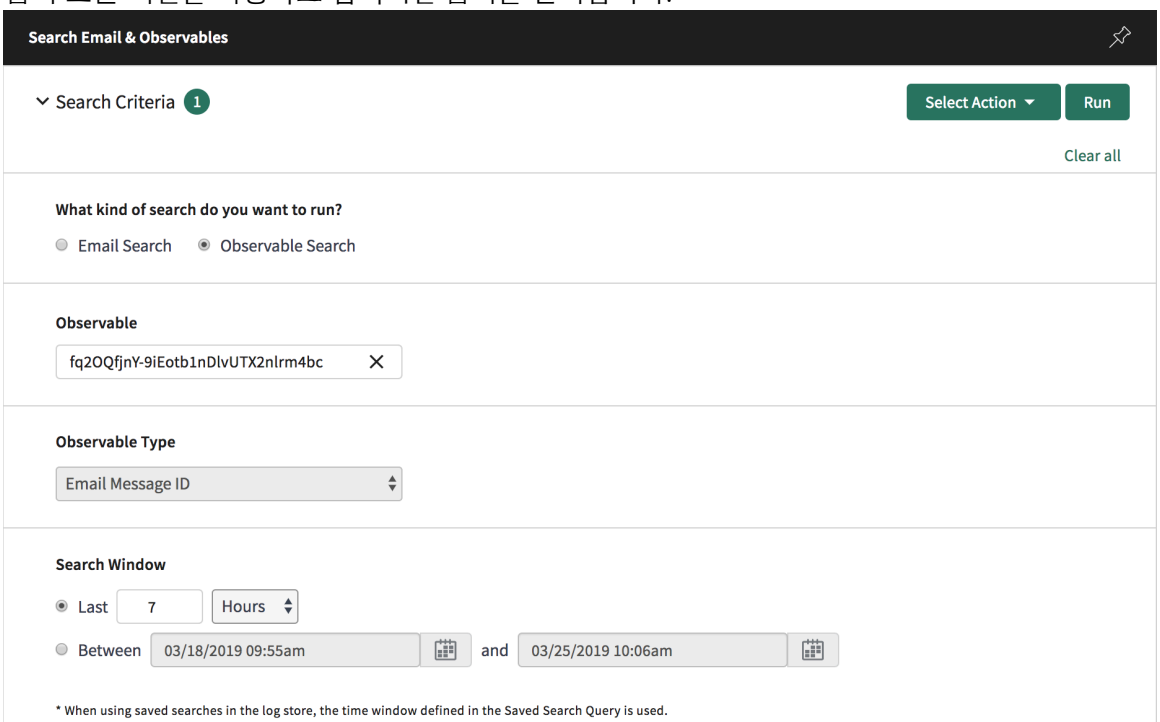


옵저버블 섹션에서 옵저버블 열에 이메일 주소, 제목 및 URL이 표시됩니다. 또한 발견 사항 열에는 피싱 이메일이 제출되고 알려진 악성 URL로 확인되었을 때 URL이 자동으로 검사되었다고 표시됩니다. 인시던트 수 열에는 동일한 옵저버블을 공유하는 다른 인시던트가 표시됩니다. 이러한 아티팩트는 조직에서 영향을 받은 사용자 수를 확인하는 것을 포함하여 이 피싱 공격에 대한 방지 절차로 이동할 준비가 되었음을 나타냅니다.

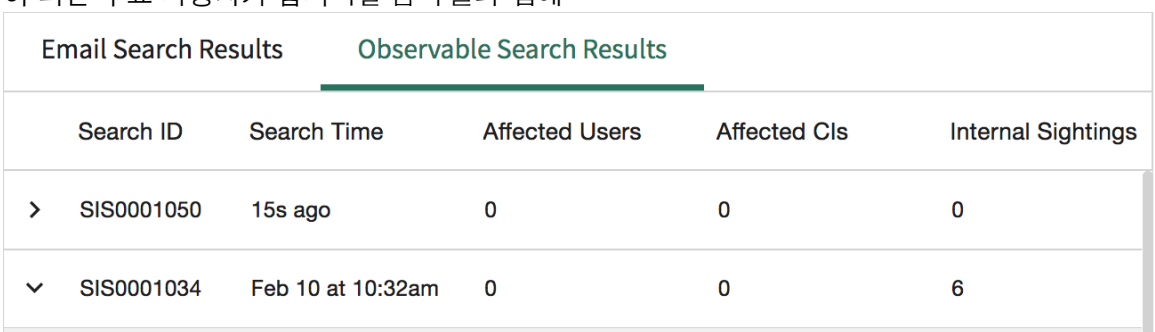
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 다음으로 이동 탐색 〉 조사 〉 이메일 및 옵저버블 검색.
5. 검색 조건 섹션을 확장하고 옵저버블 검색을 클릭합니다.



6. 검색 중인 옵저버블과 검색할 기간(예: 지난 24시간)을 입력합니다.
7. 작업 선택 목록에서 검색을 선택합니다.
   Splunk 로그 저장소는 입력한 조건을 사용하여 검색되고 악의적인 공격의 대상이 되는 주요 사용자가 옵저버블 검색 결과 탭에



   표시됩니다.
8. 이메일을 받은 사용자를 보려면 다음으로 이동하십시오. 사용자 〉 영향을 받는 사용자.

   피싱 사용자 열은 피싱 이메일의 받는 사람을 식별하고 사용자 상호 작용 열은 피싱 URL을 클릭하거나 의심스러운 이메일 주소와 상호 작용한 사용자를 식별합니다. 사용자 상호작용 열은 사용자가 악성 링크 또는 IP를 클릭했는지 여부에 따라 true 또는 false로 설정됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
영향을 받는 사용자 페이지에는 ServiceNow 인스턴스에 있는 사용자 기록만 표시됩니다.

9. 피싱 이메일을 클릭하여 자격 증명이 손상되었을 가능성이 있는 사용자를 자세히 조사하려면 다음을 수행합니다.

   a. 피싱 사용자 및 사용자 상호작용 열에서 **true**로 표시되는 사용자 이름 옆에 있는 확인란을 선택합니다.

   b. **Create Child Security** Incident(하위 보안 인시던트 생성)를 클릭한 다음 Run(실행)을 클릭합니다.
   하위 보안 인시던트가 생성되었음을 보여주는 메시지가 표시됩니다. 상위 인시던트와 연결된 하위 보안 인시던트를 보려면 탐색 탭을 클릭하고 인시던트 〉 하위 보안 인시던트.

결과
피싱 처리된 사용자 목록이 표시됩니다.

사이팅 검색 구성 기록 생성

여러 사이팅 검색 구성 기록을 생성하여 여러 로그 저장소를 쿼리하거나 검색 매개변수를 변경하는 동안 사용합니다.

시작하기 전에
필요한 역할: sn_si.admin

- Splunk 인스턴스에 CIM 추가 기능을 설치해야 합니다.
- 저장된 검색 및 즉석 쿼리는 Splunk 통합에 대해서만 지원됩니다.

이 태스크 정보
사이팅 검색 구성 레코드를 생성하여 Splunk 엔터프라이즈 로그 저장소에 저장된 검색을 호출할 수도 있습니다.

주:
검색 구성 쿼리는 Splunk CIM(공통 정보 모델)을 준수하기 위해 Splunk 로그 데이터를 사용합니다.

저장된 검색 구성을 사용하여 다음을 수행할 수 있습니다.

- 여러 이벤트 기록을 결합하는 사용자 지정 검색을 생성합니다.
- 설계 효율적이고 효과적인 검색.
- Splunk 저장된 검색에서 매개변수화된 입력을 사용합니다.

기본 시스템에는 다음 이미지에 표시된 샘플 컨피그레이션이 포함되어 있습니다.

저장된 검색 구성

	Name	Observable type	Search	Is saved search
	Search	Search	Search	Search
	Default Proofpoint Inplace Search-Emails	Email	tag=email [| search tag="email" AND (sub...	false
	Default Saved Search - Emails	Email	args.email.subject=${email.subject}&args...	true
	Default PAN Inplace Search - URLs	URL	tag=network url=${observable} | table us...	false

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

저장된 검색 및 Inplace 구성 쿼리는 예제 쿼리이며 사용자 환경에 적합한 매개 변수로 대체할 수 있습니다. 필요에 따라 저장된 검색 구성을 추가로 생성합니다. 저장된 검색 구성을 정의할 때 검색 쿼리의 이름과 매개변수는 Splunk 인스턴스에 정의된 저장된 구성과 일치해야 합니다. 이름과 매개변수가 동일하지 않으면 사이팅 검색을 수행할 때 정확한 결과를 볼 수 없습니다.

주:
Splunk 인스턴스에서 검색, 보고서 및 경보 페이지로 이동하여 저장된 검색 쿼리를 찾습니다. 권한 링크를 눌러 권한 페이지로 이동합니다. 모든 앱 라디오 버튼을 선택하고 모든 사용자에 대해 읽기 권한 옵션을 활성화합니다. 이렇게 하면 저장된 검색 쿼리의 공유 열 값이 비공개에서 앱으로 변경됩니다. 이 항목이 설정되어 있지 않으면 저장된 검색 쿼리가 결과를 반환하지 않을 수 있습니다.

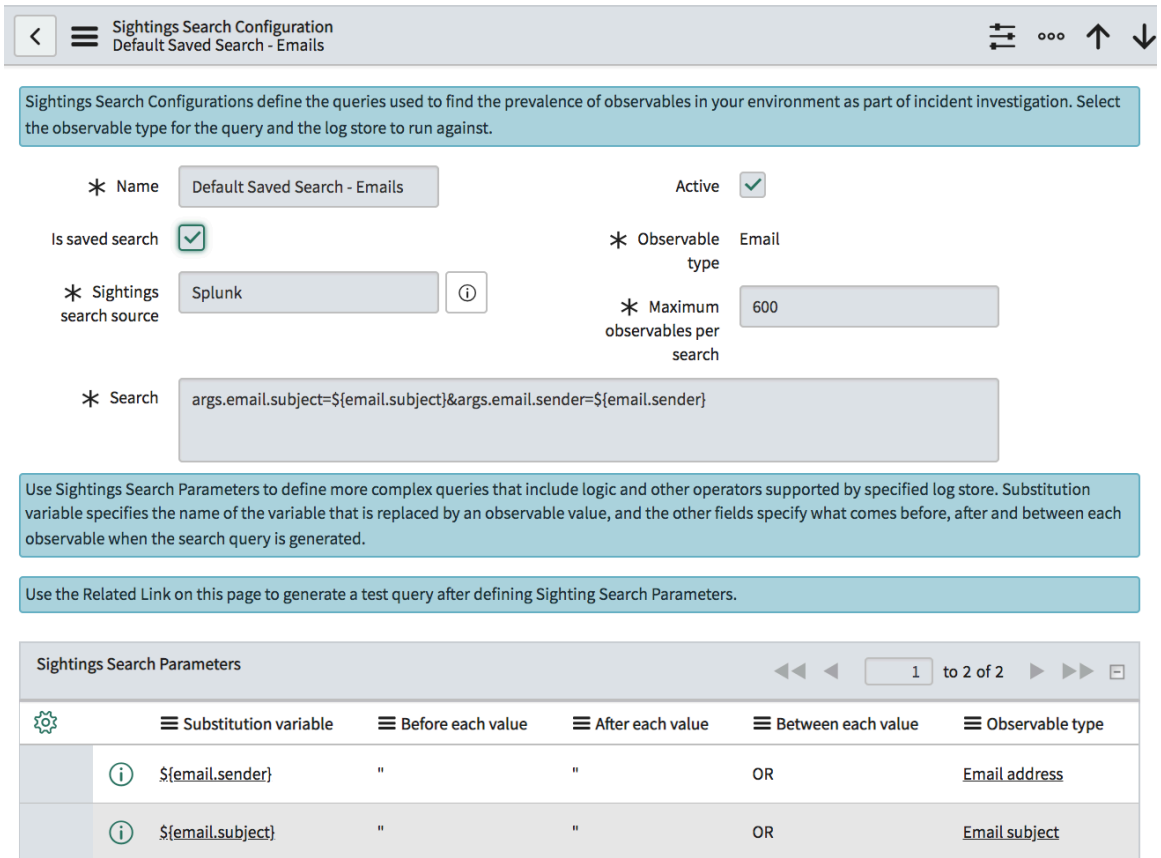
저장된 검색 구성이 Splunk 인스턴스에 정의된 구성과 일치하는지 확인하려면 다음을 수행합니다.

1. 다음으로 이동 설정 〉 검색, 보고서 및 경보.
2. 앱 컨텍스트를 모두로 변경합니다.

   검색 보고서 목록이 표시됩니다.
3. 저장된 검색 쿼리가 목록에 있는지 확인합니다.

예를 들어, 사이팅 검색 구성 양식에는 이메일 주소와 이메일 발신자가 검색 매개변수로 포함되어 있습니다.

사이팅 검색 구성 양식



Splunk 인스턴스에서 동일한 이름, 기본 저장된 검색 - 이메일, 이메일 주소 및 이메일 제목에 대한 동일한 검색 매개변수를 사용하여 저장된 검색을 정의합니다. 이름과 검색 매개변수가 동일하지 않으면 사이팅 검색이 정확한 결과를 생성하지 않습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 보안 운영 〉 통합 〉 사이팅 검색 구성 그런 다음 새 기록을 생성합니다(필드 설명은 표 참조).

사이팅 검색 구성 양식

필드	설명
이름	구성의 이름입니다.
저장된 검색 여부	이 옵션을 선택하면 저장된 검색 구성이 생성됩니다.
관찰 검색 소스	사이팅 검색의 소스입니다. Splunk 로그 저장소를 소스로 선택합니다.
활성	저장된 검색 상태에 대한 옵션입니다. 사이팅 검색을 수행하는 데는 활성 검색 구성만 사용할 수 있습니다.
옵저버블 유형	옵저버블 유형은 IP, 해시 값, URL, 도메인 이름 등과 같은 모든 옵저버블 유형일 수 있습니다.
검색당 최대 옵저버블	검색에서 반환될 최대 옵저버블 수입니다.
검색	기본 검색 문자열은 $(observable)이지만 Splunk 로그 저장소에서 지원하는 매개변수를 지정하여 사용자 고유의 검색 쿼리를 정의할 수 있습니다.

2. 제출을 클릭합니다.

결과
사이팅 검색 구성 기록을 생성했습니다.

다음에 수행할 작업
검색 쿼리를 정의한 후 사이팅 검색 테스트 쿼리 생성을 클릭하고 옵저버블 값 목록을 지정하여 이 저장된 검색 구성을 기반으로 테스트 쿼리를 생성합니다.

플레이북 자원

Security Incident Response는 포괄적인 Playbook, 하위 플로우 및 작업 라이브러리를 포함하는 풍부한 플레이북 자원 세트를 제공합니다. 복잡한 코드를 작성하지 않고도 플레이북을 빠르고 쉽게 생성하거나 구성할 수 있습니다. 이러한 Playbook을 사용하여 보안 위협을 단계별로 해결할 수 있습니다.

플레이북 자원에는 다음이 포함됩니다.

보안 인시던트 응답 플레이북	보안 인시던트 응답 플레이북 작업
기본 시스템과 함께 제공되는 플레이북은 복잡하고 일상적인 작업을 자동화하여 보안 인시던트 조사 프로세스를 가속화하도록 설계되었습니다. 플레이북은 구성 가능성이 높고 ServiceNow의 Flow Designer 기술을 사용하여 빌드됩니다. 구성하려면 기본 시스템과 함께 제공된 플레이북을 복사하고 간단한 끌어서 놓기 그래픽 인터페이스를 사용하여 수정합니다. 보안 인시던트 응답 플레이북 문서를 참조하십시오.	플레이북을 빌드하는 데 중요한 복잡한 작업을 작업 라이브러리로 사용할 수 있습니다. 보안 관리자는 이러한 작업 라이브러리를 사용하여 복잡한 코드를 작성하지 않고도 플레이북을 생성할 수 있습니다. 보안 인시던트 응답 플레이북 작업 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

플로우 활성화 보안 인시던트 응답

보안 관리자와 플로우 설계자는 보안 인시던트 응답 플로우를 사용하여 조직의 보안 인시던트 해결 프로세스를 자동화할 수 있습니다.

시작하기 전에

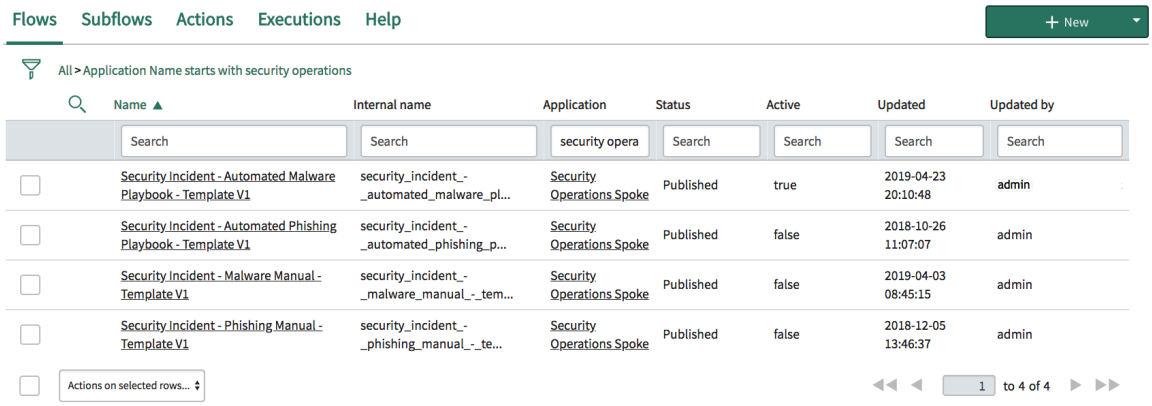
필요한 역할: sn_si.admin, action_designer, flow_designer

이 태스크 정보

기본 시스템과 함께 제공되는 플로우가 비활성 상태입니다. 이러한 플로우를 사용하기 전에 활성화합니다.

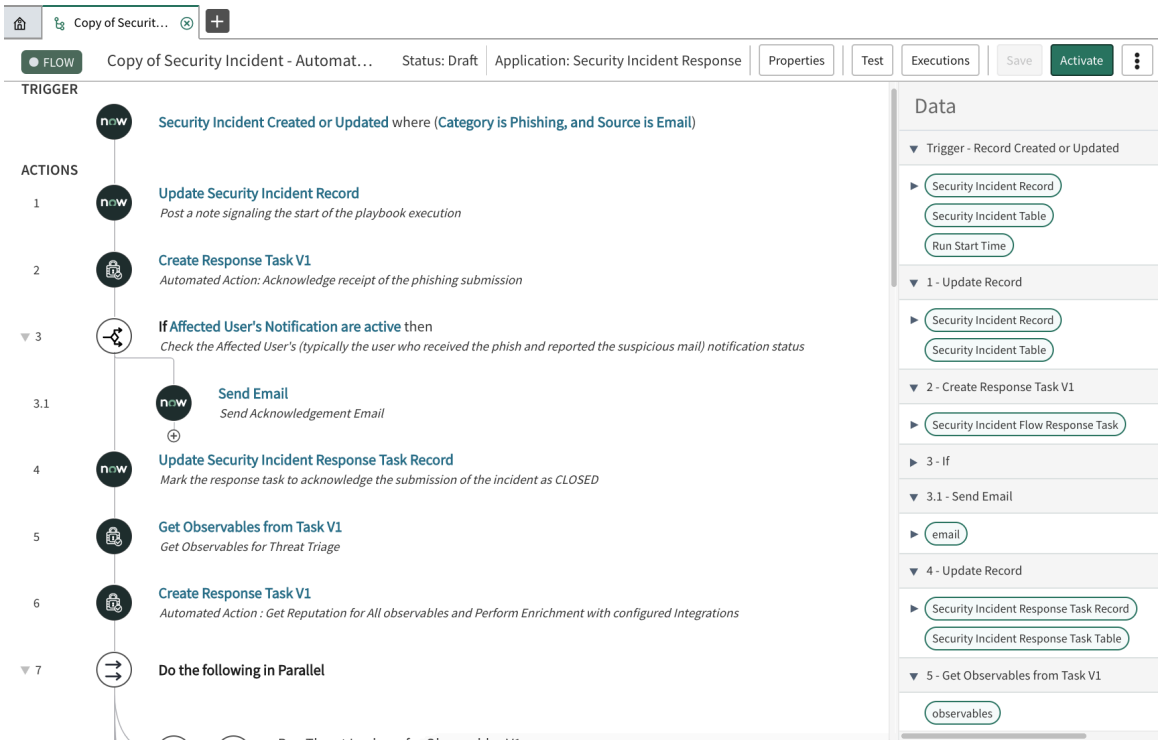
프로시저

1. 스포크 애플리케이션을 다운로드하여 설치합니다보안 운영.
   이 스포크 애플리케이션은 플로우를 정의하는 보안 인시던트 응답 동안 사용할 수 있는 보안 운영 작업을 제공합니다.
2. 다음으로 이동 플로우 디자이너 〉 디자이너 을 클릭하고 스포크 애플리케이션을 검색하여 보안 운영 보안 인시던트 관련 플로우를 봅니다.



플로우가 게시 상태로 비활성 상태입니다.

3. 예를 들어 자동화된 맬웨어 플레이북 플로우를 활성화하려면 보안 인시던트 - 자동화된 피싱 플레이북 - 템플릿 **V1** 링크를 클릭하여 플로우를 봅니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
기본 시스템에 제공된 플로우는 읽기 전용 플로우이므로 편집할 수 없습니다. 이러한 플로우를 그대로 사용하거나 필요에 따라 사본을 만들고 수정할 수 있습니다.

4. 활성화를 클릭하여 플로우를 활성화합니다.

결과
자동화된 피싱 플레이북 플로우가 활성 상태이며 사용할 준비가 되었습니다.

보안 인시던트 응답 플레이북

보안 인시던트 플레이북 플로우를 자동 또는 수동으로 호출할 수 있습니다.

플레이북은 하나 이상의 플레이북이 보안 인시던트와 연결된 경우에만 표시됩니다. 플레이북 구성요소는 Flow Designer 빌드 플로우가 아닌 PAD(프로세스 자동화 디자이너) 구축 프로세스에만 작동합니다. 플로우 디자이너가 활성화된 기존 플로우의 경우 계속 작동하며 활동은 응답 작업으로 계속 렌더링됩니다.

보안 인시던트 응답 는 다음 두 가지 유형의 Playbook을 지원합니다.

- 프로세스 기반 플레이북
- 플로우 기반 플레이북

나열된 플레이북 외에도 플로우 플레이북에서 호출할 수 있는 보안 운영 스포크 내의 하위 플로우도 있습니다. 랜섬웨어는 그러한 하위 플로우 중 하나입니다.

이러한 플로우를 사용하기 전에 활성화합니다. 자세한 내용은 보안 인시던트 응답 플로우 활성화를 참조하십시오.

프로세스 기반 플레이북

플레이북 구성요소는 플로우가 아닌 내장된 워크플로우 스튜디오 플레이북에만 작동합니다. 그러나 기존 플로우 기반 Playbook은 계속 작동하며 활동은 계속해서 응답 작업으로 렌더링됩니다.

보안 인시던트 응답 에서는 기본 시스템과 함께 다음과 같은 플레이북을 제공합니다.

수동 피싱을 위한 플레이북

수동 피싱 플레이북은 분석가가 피싱 활동에서 특정 유형의 보안 위협을 수동으로 해결할 수 있는 방법에 대한 단계별 지침을 제공합니다.

개요

수동 피싱 플레이북 템플릿은 피싱 응답 작업을 수동으로 수행하도록 설계되었으며 트리거 조건을 포함하는 일련의 작업을 포함합니다. PAD 템플릿을 사용하여 피싱 응답 플레이북의 단계를 수행하고 이러한 인시던트를 효율적으로 해결할 수 있습니다.

이 Playbook은 보안 인시던트가 생성되거나 업데이트되는 경우에 사용할 수 있습니다. PAD(프로세스 자동화 디자이너)에서 수동 피싱 플레이북을 활성화한 다음 분석, 포함, 근절 및 검토와 같은 모든 작업을 수행해야 합니다.

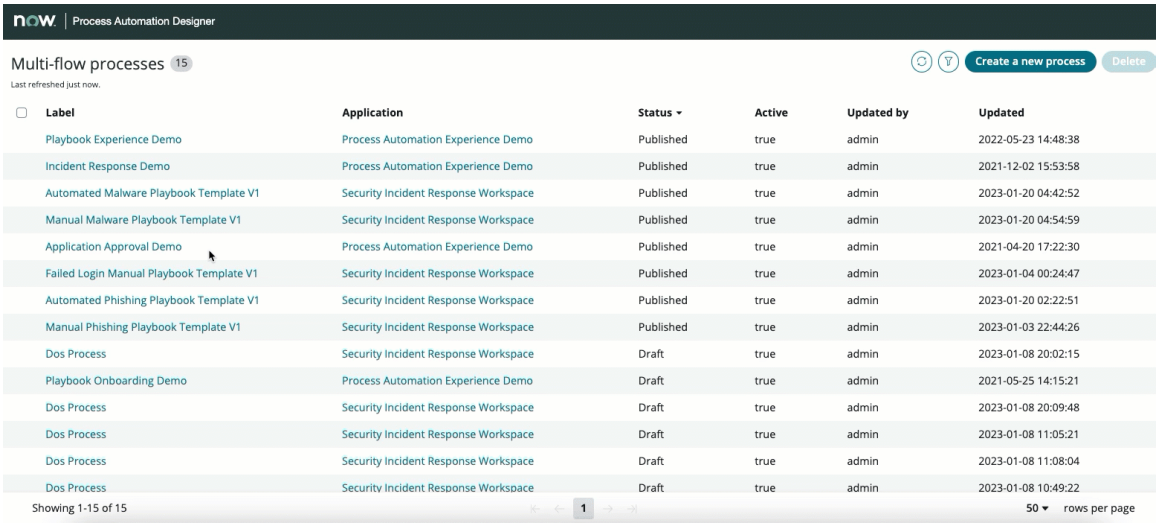
다음은 프로세스 정의의 스테이지이며 보안 인시던트 상태에 해당합니다.

- 분석
- 포함
- 근절
- 검토

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

각 스테이지에는 활동이 있습니다.

수동 피싱 플레이북



스테이지에서 작업을 완료로 표시하면 다음 작업으로 이동할 수 있습니다. 언제든지 작업을 저장하고 나중에 날짜 및 시간에 플레이북으로 돌아갈 수 있습니다. 스테이지의 모든 작업을 완료한 후 다음 스테이지로 이동할 수 있습니다. 작업과 스테이지를 계속 완료하면 왼쪽 패널에 상태가 반영됩니다. 플레이북 오른쪽에 있는 활동 로그에는 각 작업에 대해 입력한 모든 데이터가 표시됩니다.

모든 작업을 완료한 후에는 모든 스테이지에서 입력한 세부 정보를 검토하라는 메시지가 표시됩니다. 필드를 편집하거나 마침을 클릭하여 권리를 생성하는 프로세스를 완료할 수 있습니다.

에서 수동 피싱을 위한 플레이북 생성 워크플로우 스튜디오

다음 단계를 사용하여 에서 수동 피싱에 대한 플레이북을 워크플로우 스튜디오생성합니다.

시작하기 전에
필요한 역할: sn_si.admin 또는 sn_si.manager

프로시저

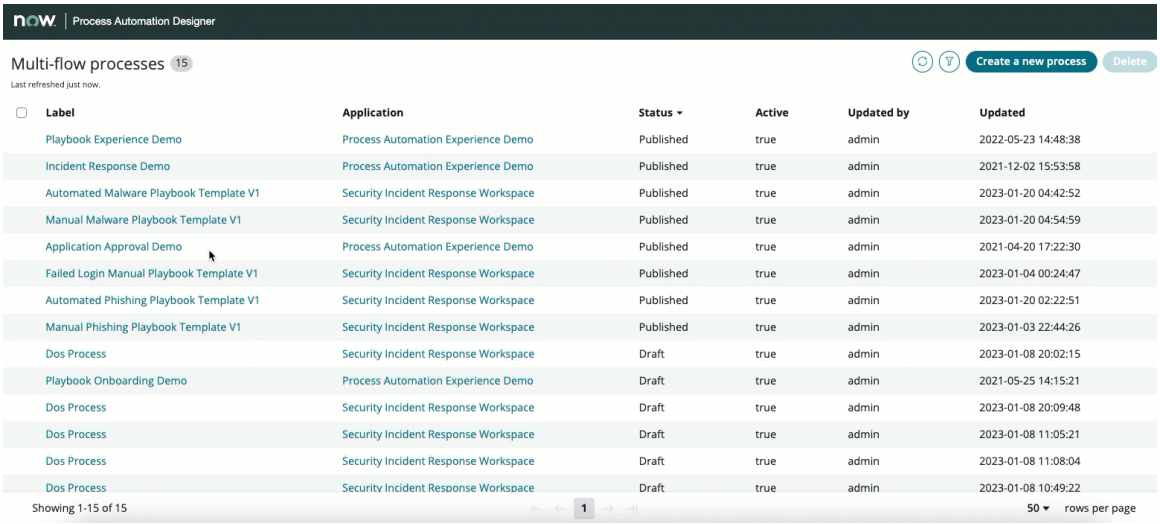
1. 클릭 모두 〉 프로세스 자동화 디자이너 〉 〉 신규 을 클릭하고 플레이북을 선택합니다.

   예: 수동 피싱 플레이북 템플릿 V1.

2. 플레이북의 이름, 설명, 플레이북이 생성될 애플리케이션을 입력합니다.
3. 트리거 선택을 클릭합니다.
4. 프로세스가 실행되는 시기에 대한 고유한 조건 정의를 선택하고 Playbook을 실행해야 하는 시기에 대한 트리거 조건을 선택합니다.
5. 트리거 조건 설정을 클릭합니다.
6. 테이블을 선택하고 조건을 입력하여 플레이북을 실행해야 하는 시기를 정의하는 조건을 선택합니다.
   예를 들어 트리거 조건은 피싱 범주의 보안 인시던트가 생성될 때입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

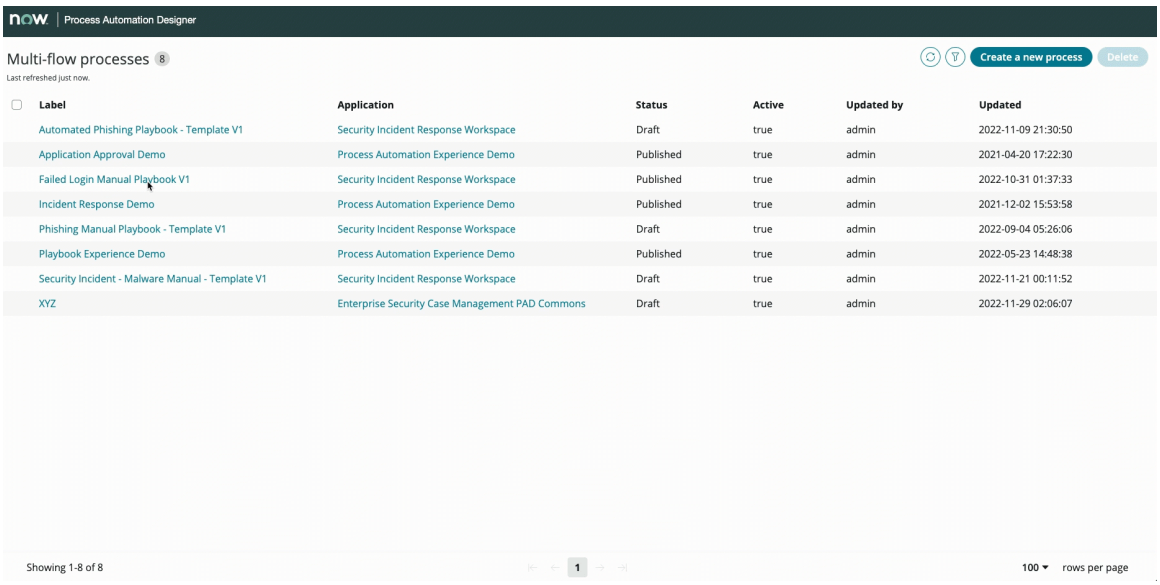
수동 피싱



7. 디자이너로 이동을 클릭합니다.
8. 자동화된 프로세스 설계를 시작하려면 새 스테이지 추가를 클릭합니다.
   UI 오른쪽에 스테이지 속성 창이 열립니다.
9. 스테이지 속성 창에 이름, 설명, 실행 조건, 시작 시기 표시와 같은 세부 정보를 입력합니다.
   실행 조건 및 시작 시기 표시 필드는 스테이지가 실행되는 시기를 의미합니다.
10. 저장 후 닫기를 클릭합니다.
11. 다른 스테이지를 추가하려면 **Add another** stage(다른 스테이지 추가)를 클릭합니다.
    마찬가지로 원하는 만큼 스테이지를 만들 수 있습니다. 이 예에서는 각각 분석, 포함, 근절 및 검토에 대한 스테이지를 만들 수 있습니다. 다음 예시에서는 분석 단계가 즉시 시작되며 실행 조건이 없습니다. 이전 스테이지가 완료된 후 스테이지 시작을 포함하며 이전 스테이지의 활동 결과를 기반으로 하는 실행 조건이 있습니다.
    스테이지를 추가한 후에는 각 스테이지에 대한 프로세스 활동을 추가해야 합니다.
12. 특정 스테이지(예: 분석 스테이지)에서 다른 활동 추가를 클릭합니다.
    활동 추가 팝업이 열립니다.
    a. 활동 추가 팝업에서 필요한 활동 정의를 선택합니다.
13. 새 활동 만들기를 클릭합니다.
    활동 정의를 추가한 후 스테이지와 유사하게 추가로 구성할 수 있습니다. 마찬가지로 각 스테이지 아래에 다른 프로세스 활동을 생성할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

수동 피싱 활동



14. 활동 속성 창에서 실행 조건을 추가하고 활동 시작 시기를 나타냅니다.
15. 실행 조건을 추가하고 시작 시기를 나타냅니다.
    이 활동에 필요한 모든 입력(구성된 자동화 계획의 입력 포함)이 표시됩니다. 값을 재정의하거나 미리 구성된 값을 사용할 수 있습니다.
16. 모든 속성 보기를 클릭하고 고급 속성 토글을 활성화하여 활동 정의의 모든 활동 경험 필드를 표시합니다.

병렬 활동 추가

시작 시기 필드가 이전과 함께 설정되어 있으면 병렬 활동을 시작할 수 있습니다.

한 스테이지에서 다음 스테이지로 이동

실행 조건이 정의되지 않은 경우 스테이지와 활동이 순차적으로 실행됩니다.

실행 조건을 사용하여 활동 또는 스테이지를 건너뛸 수 있습니다. 이 예에서 포함 단계는 '이메일에 위협 표시기가 있습니까?'의 결과가 예일 때 시작됩니다.

한 스테이지에서 다른 스테이지로 이동하려면 플랫폼에서 제공하는 활동 정의인 기록 업데이트를 사용할 수 있습니다. 이렇게 하면 보안 인시던트의 상태 필드가 업데이트되고 Playbook 실행이 다음 단계로 재개됩니다.

그러나 이 활동 정의의 문제는 플레이북이 분석 단계에 있고 사용자가 검토라고 하기 위해 상태를 수동으로 업데이트한 경우 기록 업데이트 활동이 플레이북 실행을 계속하기 위해 상태를 다시 포함으로 변경한다는 것입니다. 이렇게 하면 수행된 수동 변경이 재정의됩니다.

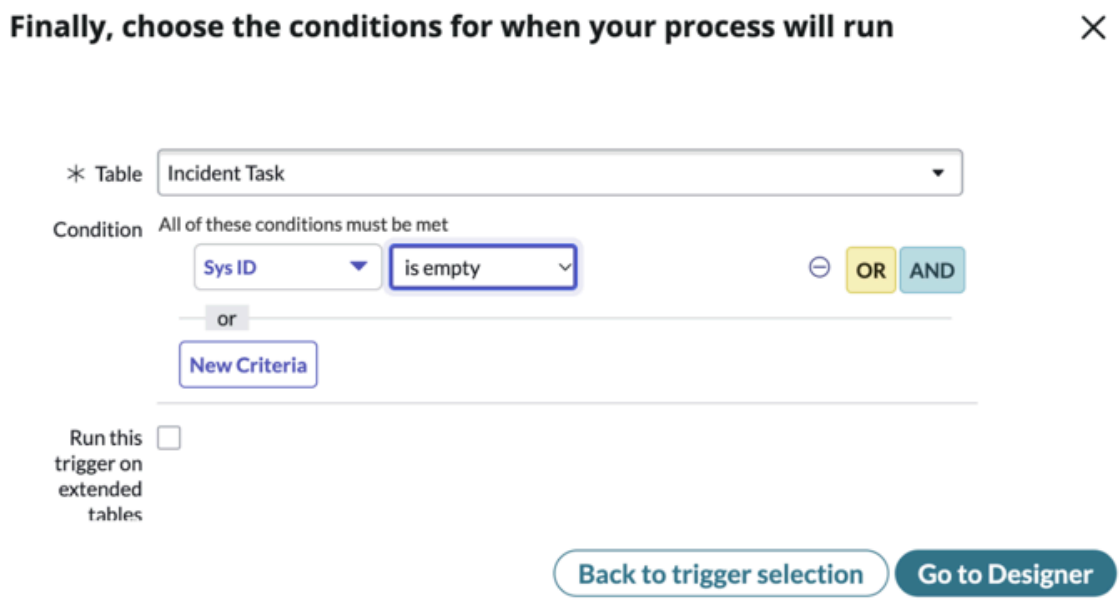
이를 극복하기 위해 기본 시스템에서는 작업 상태 업데이트 라는 활동 정의가 제공됩니다. 보안 상태의 현재 상태가 플레이북의 스테이지보다 앞서는 경우 이 활동은 보안 인시던트 상태를 재정의하지 않습니다.

더미 트리거 조건을 사용하여 프로세스 정의 생성

프로세스 정의에는 항상 트리거 조건이 필요합니다. 그러나 프로세스를 트리거해야 하는 시기를 잘 모르는 경우에도 더미 트리거 조건을 사용하여 프로세스 정의를 생성할 수 있습니다. 트리거 조건을 **sys_id** 비어 있도록 설정합니다. 이 조건은 결코 충족되지 않을 것입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로세스 조건



수동 피싱 플레이북 사용

다음 단계를 사용하여 SIR 분석가 작업 공간에서 수동 피싱 플레이북을 사용하는 방법과 해당 기능을 알아봅니다.

시작하기 전에
필요한 역할: sn_si.admin 또는 sn_si.manager 또는 sn_si.analyst

프로시저

1. SIR 작업 공간에서 보안 인시던트를 엽니다.
2. 플레이북 탭을 클릭합니다.

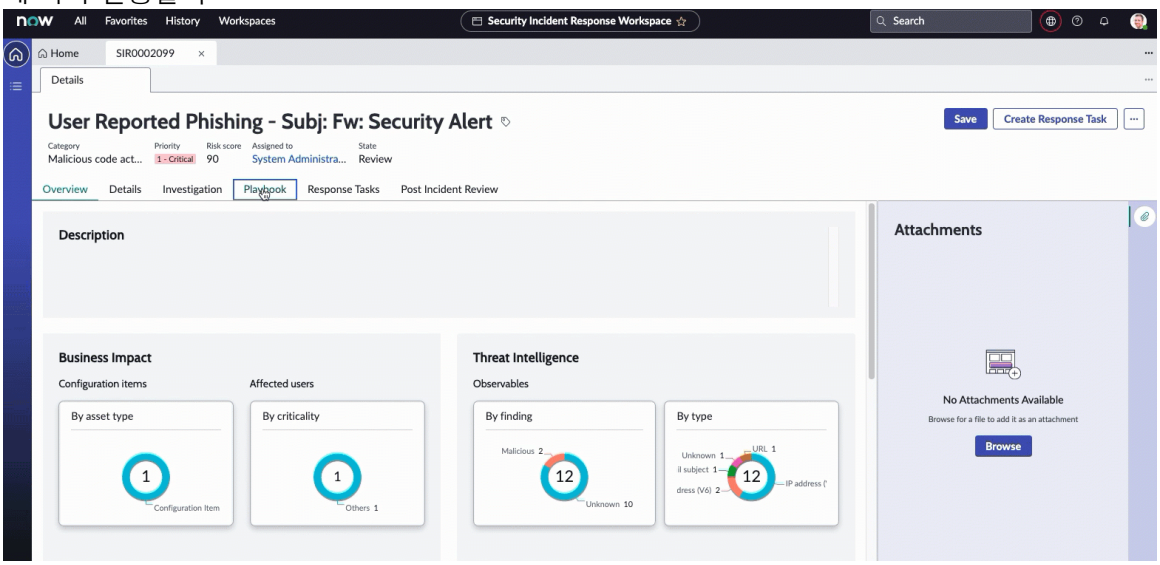
   보안 인시던트에 대해 활성화된 플레이북을 볼 수 있습니다. 보안 인시던트의 범주, 위험 점수와 같은 상세 정보도 볼 수 있습니다.

   주:
   나열된 플레이북이 표시되지 않으면 PAD로 이동하여 플레이북 탭에서 볼 수 있도록 해야 합니다.

3. 수동 피싱 플레이북을 클릭합니다.
4. 각 스테이지를 클릭하여 이 플레이북에서 어떤 작업이 수행되었는지 확인합니다.
5. 분석을 클릭하여 분석 단계에서 수행된 활동 목록을 봅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

요구 사항에 따라 변경할 수 있습니다.



6. 마찬가지로 포함, 근절 및 검토를 클릭하여 각 단계에서 수행된 활동 목록을 볼 수 있습니다. 요구 사항에 따라 변경할 수 있습니다. 수행해야 하는 나머지 활동 또는 사용자 작업이 있는 경우 해당 단계에 표시됩니다.
7. 단계에 필요한 나머지 활동 또는 사용자 작업이 있는 경우 해당 단계를 클릭하고 작업을 수행하여 활동을 완료합니다.

작업 공간 플레이북 요약

다음은 프로세스 요약에 대한 설명입니다.

- 레거시 플로우 기반 플레이북을 이해합니다.
- 플로우를 분석한 후 가능한 활동과 스테이지를 나열합니다. 실제 오케스트레이션을 만들 수 있는 단계를 찾습니다.
- 각 활동을 수행하고 기본 시스템 제공 활동 정의가 사용 케이스를 이행할 수 있는지 여부를 확인합니다.
- 새 활동 정의를 구현해야 하는 활동 사용 사례를 나열합니다. 대화형, 비대화형, 자동화형으로 분류합니다. 활동 정의를 생성하려면 다음을 수행합니다.
  - 사용 사례에 대한 하위 플로우 또는 작업을 생성합니다.
  - 연결된 데이터를 플로우 데이터 테이블이나 사용자 지정 테이블에서 캡처해야 하는지 결정합니다.
  - 플로우 데이터 테이블을 사용하는 경우 **sys_flow_data_definition**에서 플로우 데이터 정의를 생성합니다. 하위 플로우에서 플로우 데이터 기록을 생성하는 동안 생성된 플로우 데이터 정의를 선택합니다.
  - 활동 정의를 생성합니다.
  - 자동화 계획을 매핑합니다.
  - 활동 경험 속성을 입력합니다.
  - 플레이북 작업에서 작업을 생성합니다. 활동 정의에 할당할 기존 활동 작업이 있어야 합니다.
  - 선택한 경험 유형에 따라 기본 카드 환경을 재정의하려면 활동 UI 개념을 사용하여 Playbook 재정의를 추가합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 일부 활동은 하위 플로우에서 사용자 입력 대기 플래그를 사용하여 자동 및 대화형을 모두 처리하도록 만들 수 있습니다. 프로세스 정의에서 활동을 구성하는 동안 이 입력을 전달할 수 있습니다.
- 프로세스에 필요한 모든 활동 정의가 있으면 를 사용하여 워크플로우 스튜디오프로세스 정의 작성을 시작합니다.

자동화된 피싱을 위한 플레이북

자동화된 피싱 플레이북은 분석가에게 자동화된 피싱 활동에서 특정 유형의 보안 위협을 해결할 수 있는 방법에 대한 단계별 지침을 제공합니다.

개요

자동화된 피싱 플레이북 템플릿은 피싱 응답 작업을 자동화하도록 설계되었으며 트리거 조건을 포함하는 일련의 작업을 포함합니다. 의 워크플로우 스튜디오 플레이북 템플릿을 사용하여 피싱 응답 플레이북의 단계를 자동화하고 이러한 인시던트를 효율적으로 해결할 수 있습니다. 이 플레이북 템플릿에는 피싱 공격에 대응하도록 설계된 재사용 가능한 작업 시퀀스가 포함되어 있습니다. 각 플로우에는 트리거(조건), 작업 시퀀스 및 주석을 달 수 있는 하위 플로우가 있습니다.

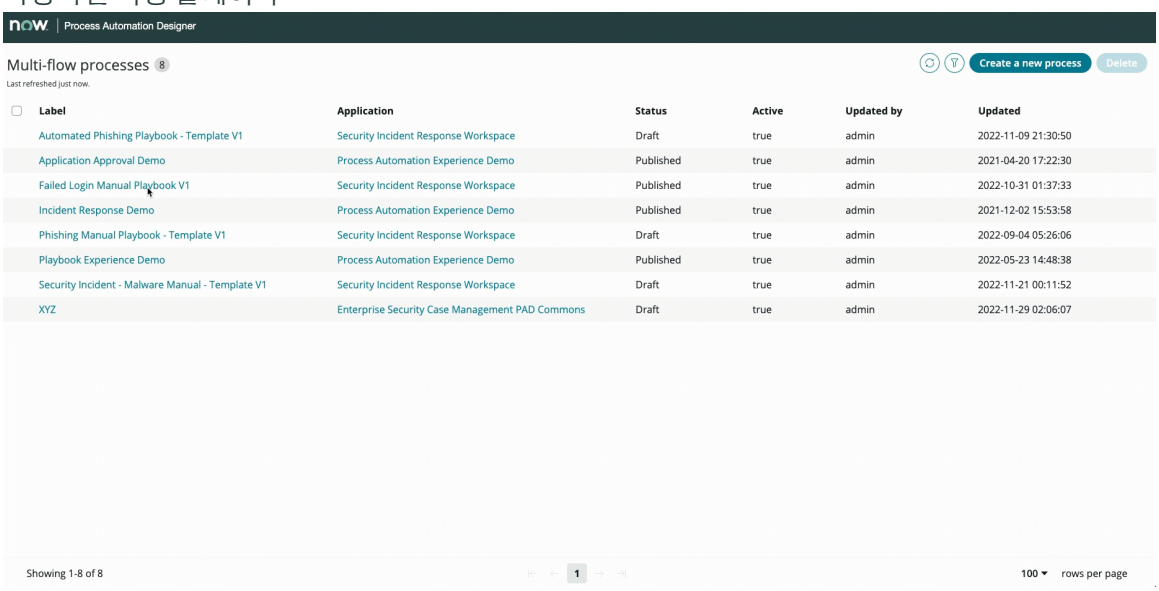
이 Playbook에서는 보안 인시던트의 범주가 피싱으로 설정된 경우 사용자 상호작용이 없습니다. 이 Playbook은 보안 인시던트가 생성되거나 업데이트되는 경우에 사용할 수 있습니다. 에서 워크플로우 스튜디오자동화된 피싱 플레이북을 활성화해야 하며, 이 플레이북은 분석, 포함, 근절 및 검토와 같은 모든 작업을 자동으로 수행합니다.

다음은 프로세스 정의의 스테이지이며 보안 인시던트 상태에 해당합니다.

- 분석
- 포함
- 근절
- 검토

각 스테이지에는 활동이 있습니다.

자동화된 피싱 플레이북



스테이지에서 작업을 완료로 표시하면 다음 작업으로 이동할 수 있습니다. 언제든지 작업을 저장하고 나중에 날짜 및 시간에 플레이북으로 돌아갈 수 있습니다. 스테이지의 모든 작업을 완료한 후 다음

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

스테이지로 이동할 수 있습니다. 작업과 스테이지를 계속 완료하면 왼쪽 패널에 상태가 반영됩니다. 플레이북 오른쪽에 있는 활동 로그에는 각 작업에 대해 입력한 모든 데이터가 표시됩니다.

모든 작업을 완료한 후에는 모든 스테이지에서 입력한 세부 정보를 검토하라는 메시지가 표시됩니다. 필드를 편집하거나 마침을 클릭하여 권리를 생성하는 프로세스를 완료할 수 있습니다.

PAD에서 자동화된 피싱을 위한 프로세스 생성

다음 단계를 사용하여 PAD(프로세스 자동화 디자이너)에서 자동화된 피싱에 대한 프로세스를 생성합니다.

시작하기 전에
필요한 역할: sn_si.admin 또는 sn_si.manager

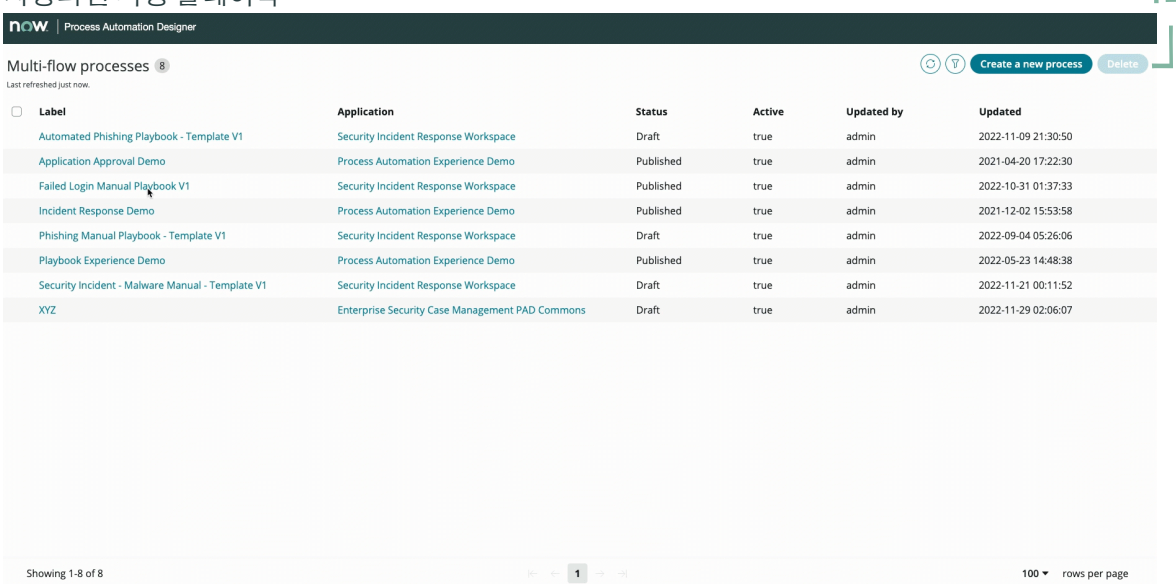
프로시저

1. 클릭 **ALL** 〉 프로세스 자동화 디자이너 〉 〉 새 프로세스 작성.

   예를 들어 자동화된 피싱 플레이북 템플릿 V1입니다.

2. 프로세스의 이름, 설명 및 프로세스를 생성할 애플리케이션을 입력합니다.
3. 트리거 선택을 클릭합니다.
4. 프로세스가 실행되는 시기에 대한 고유한 조건 정의를 선택하고 프로세스를 실행해야 하는 시기에 대한 트리거 조건을 선택합니다.
5. 트리거 조건 설정을 클릭합니다.
6. 테이블을 선택하고 조건을 입력하여 프로세스를 실행해야 하는 시기를 정의하는 조건을 선택합니다.
   예를 들어 트리거 조건은 피싱 범주의 보안 인시던트가 생성될 때입니다.

자동화된 피싱 플레이북

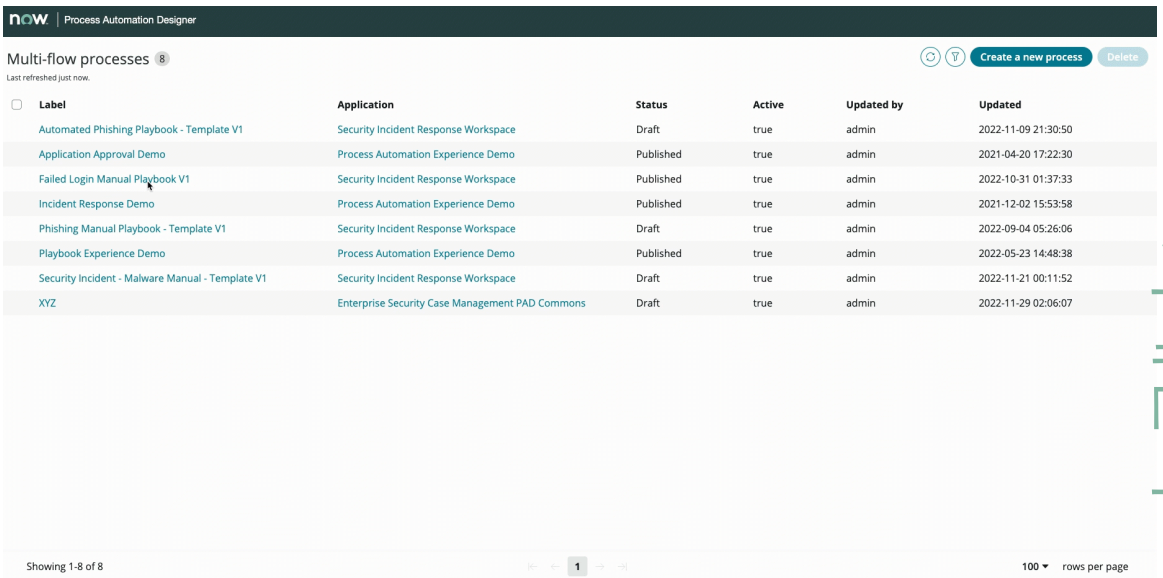


7. 디자이너로 이동을 클릭합니다.
   Process Automation Designer 페이지가 열립니다.
8. 자동화된 프로세스 설계를 시작하려면 새 스테이지 추가를 클릭합니다.
   UI 오른쪽에 스테이지 속성 창이 열립니다.
9. 스테이지 속성 창에 이름, 설명, 실행 조건, 시작 시기 표시와 같은 세부 정보를 입력합니다.
   실행 조건 및 시작 시기 표시 필드는 스테이지가 실행되는 시기를 의미합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

10. 저장 후 닫기를 클릭합니다.
11. 다른 스테이지를 추가하려면 **Add another** stage(다른 스테이지 추가)를 클릭합니다.
    마찬가지로 원하는 만큼 스테이지를 만들 수 있습니다. 이 예에서는 각각 분석, 포함, 근절 및 검토에 대한 스테이지를 만들 수 있습니다. 다음 예시에서는 분석 단계가 즉시 시작되며 실행 조건이 없습니다. 이전 스테이지가 완료된 후 스테이지 시작을 포함하며 이전 스테이지의 활동 결과를 기반으로 하는 실행 조건이 있습니다.
    스테이지를 추가한 후에는 각 스테이지에 대한 프로세스 활동을 추가해야 합니다.
12. 특정 스테이지(예: 분석 스테이지)에서 다른 프로세스 활동 추가를 클릭합니다.
    활동 추가 팝업이 열립니다.
    a. 활동 추가 팝업에서 필요한 활동 정의를 선택합니다.
13. 새 활동 만들기를 클릭합니다.
    활동 정의를 추가한 후 스테이지와 유사하게 추가로 구성할 수 있습니다. 마찬가지로 각 스테이지 아래에 다른 프로세스 활동을 생성할 수 있습니다.

자동화된 피싱 활동



14. 활동 속성 창에서 실행 조건을 추가하고 프로세스 활동을 시작할 시기를 나타냅니다.
15. 실행 조건을 추가하고 시작 시기를 나타냅니다.
    이 활동에 필요한 모든 입력(구성된 자동화 계획의 입력 포함)이 표시됩니다. 값을 재정의하거나 미리 구성된 값을 사용할 수 있습니다.
16. 모든 속성 보기를 클릭하고 고급 속성 토글을 활성화하여 활동 정의의 모든 활동 경험 필드를 표시합니다.

자동화된 피싱 플레이북 사용

다음 단계를 사용하여 SIR 분석가 작업 공간에서 자동화된 피싱 플레이북을 사용하는 방법과 해당 기능을 알아봅니다.

시작하기 전에

필요한 역할: sn_si.admin 또는 sn_si.manager 또는 sn_si.analyst

프로시저

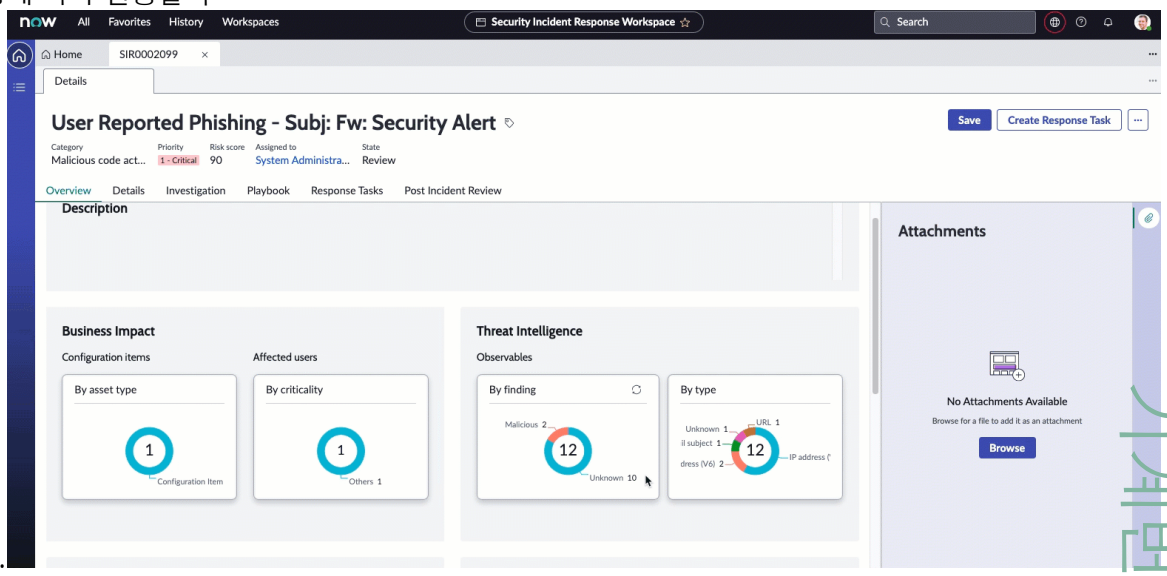
1. SIR 작업 공간에서 보안 인시던트를 엽니다.
2. 플레이북 탭을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 인시던트에 대해 활성화된 플레이북을 볼 수 있습니다. 보안 인시던트의 범주, 위험 점수와 같은 상세 정보도 볼 수 있습니다.

> **주:**
> 나열된 플레이북이 표시되지 않으면 PAD로 이동하여 플레이북 탭에서 볼 수 있도록 해야 합니다.

3. 자동화된 피싱 플레이북을 클릭합니다.
   자동화된 피싱의 경우 보안 인시던트에 대한 작업이 자동으로 수행됩니다.
4. 각 스테이지를 클릭하여 이 플레이북에서 어떤 작업이 수행되었는지 확인합니다.
5. 분석을 클릭하여 분석 단계에서 수행된 활동 목록을 봅니다.
   요구 사항에 따라 변경할 수



있습니다.

6. 마찬가지로 포함, 근절 및 검토를 클릭하여 각 단계에서 수행된 활동 목록을 볼 수 있습니다.
   요구 사항에 따라 변경할 수 있습니다. 수행해야 하는 나머지 활동 또는 사용자 작업이 있는 경우 해당 단계에 표시됩니다.
7. 단계에 필요한 나머지 활동 또는 사용자 작업이 있는 경우 해당 단계를 클릭하고 작업을 수행하여 활동을 완료합니다.

수동 맬웨어를 위한 플레이북

수동 맬웨어 플레이북은 분석가가 맬웨어 경고를 보다 효율적으로 수동으로 해결할 수 있는 방법에 대한 단계별 지침을 제공합니다.

수동 맬웨어 플레이북 템플릿은 엔드포인트 또는 네트워크에서 맬웨어 경고를 처리하는 것과 관련된 단계를 수동으로 수행하도록 설계되었습니다. 의 워크플로우 스튜디오 플레이북 템플릿을 사용하여 수동 맬웨어 플레이북의 단계를 수행하고 이러한 경보를 효율적으로 해결할 수 있습니다. 이 플레이북에는 트리거 조건, 작업 시퀀스 및 주석을 달 수 있는 하위 플로우가 포함되어 있습니다. 이 플레이북에는 맬웨어 공격에 대응하도록 설계된 재사용 가능한 작업 시퀀스가 포함되어 있습니다. 각 플로우에는 트리거(조건), 작업 시퀀스 및 주석에 대한 하위 플로우가 있습니다.

맬웨어가 생성되거나 업데이트되면 이 플레이북을 사용할 수 있습니다. 에서 워크플로우 스튜디오 수동 맬웨어 플레이북을 활성화하고 분석, 포함, 근절 및 검토와 같은 모든 작업을 생성해야 합니다.

다음은 프로세스 정의의 스테이지이며 맬웨어 경보 상태에 해당합니다.

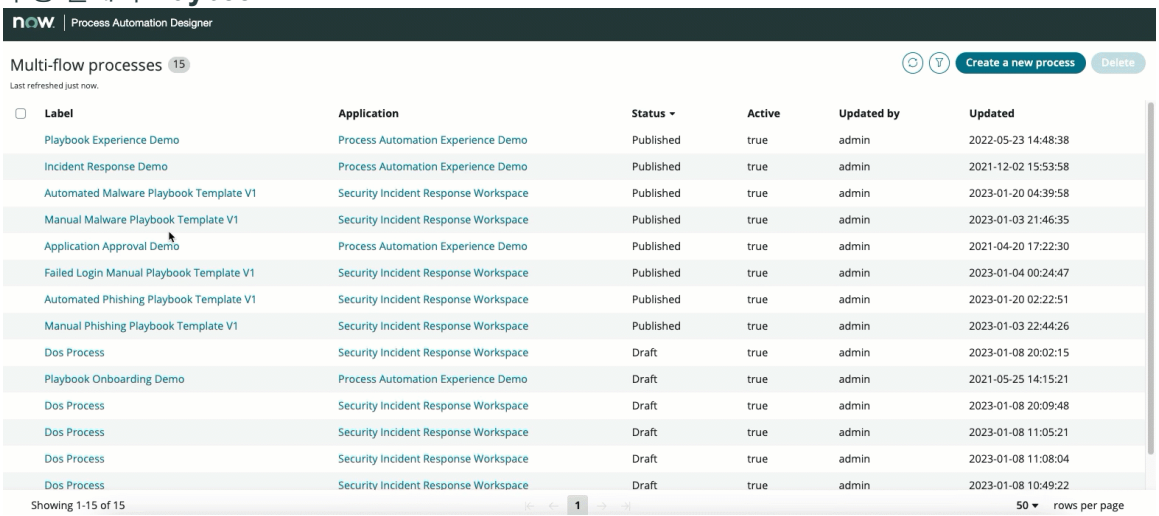
- 분석
- 포함

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 근절
- 검토

각 스테이지에는 활동이 있습니다.

수동 맬웨어 **Playbook**



스테이지에서 작업을 완료로 표시한 후 다음 작업으로 이동할 수 있습니다. 언제든지 작업을 저장하고 나중에 날짜 및 시간에 플레이북으로 돌아갈 수 있습니다. 스테이지의 모든 작업을 완료한 후 다음 스테이지로 이동할 수 있습니다. 작업과 스테이지를 계속 완료하면 왼쪽 패널에 상태가 반영됩니다. 플레이북 오른쪽에 있는 활동 로그에는 각 작업에 대해 입력한 모든 데이터가 표시됩니다.

모든 작업을 완료한 후에는 모든 스테이지에서 입력한 세부 정보를 검토하라는 메시지가 표시됩니다. 필드를 편집하거나 마침을 클릭하여 권리를 생성하는 프로세스를 완료할 수 있습니다.

PAD에서 수동 맬웨어에 대한 프로세스 생성

다음 단계를 사용하여 PAD(프로세스 자동화 디자이너)에서 수동 맬웨어에 대한 프로세스를 생성합니다.

시작하기 전에
필요한 역할: sn_si.admin 또는 sn_si.manager

프로시저

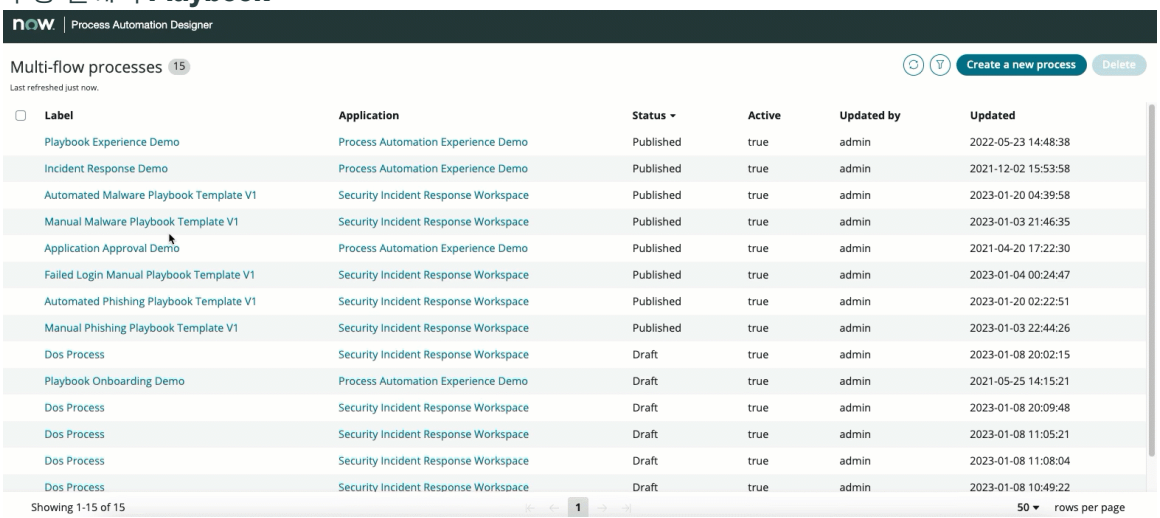
1. 클릭 **ALL** 〉 프로세스 자동화 디자이너 〉 〉 새 프로세스 작성.

   예를 들어 수동 맬웨어 플레이북 템플릿 V1입니다.

2. 프로세스의 이름, 설명 및 프로세스를 생성할 애플리케이션을 입력합니다.
3. 트리거 선택을 클릭합니다.
4. 프로세스가 실행되는 시기에 대한 고유한 조건 정의를 선택하고 프로세스를 실행해야 하는 시기에 대한 트리거 조건을 선택합니다.
5. 트리거 조건 설정을 클릭합니다.
6. 테이블을 선택하고 조건을 입력하여 프로세스를 실행해야 하는 시기를 정의하는 조건을 선택합니다.
   예를 들어 트리거 조건은 피싱 범주의 보안 인시던트가 생성될 때입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

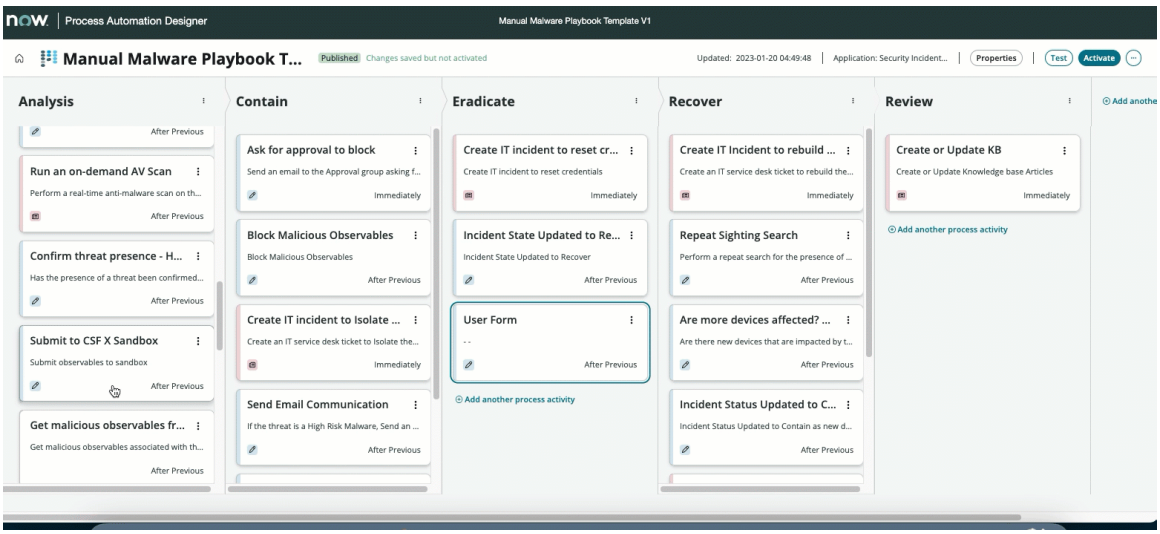
수동 맬웨어 **Playbook**



7. 디자이너로 이동을 클릭합니다.
   Process Automation Designer 페이지가 열립니다.
8. 자동화된 프로세스 설계를 시작하려면 새 스테이지 추가를 클릭합니다.
   UI 오른쪽에 스테이지 속성 창이 열립니다.
9. 스테이지 속성 창에 이름, 설명, 실행 조건, 시작 시기 표시와 같은 세부 정보를 입력합니다.
   실행 조건 및 시작 시기 표시 필드는 스테이지가 실행되는 시기를 의미합니다.
10. 저장 후 닫기를 클릭합니다.
11. 다른 스테이지를 추가하려면 **Add another** stage(다른 스테이지 추가)를 클릭합니다.
    마찬가지로 원하는 만큼 스테이지를 만들 수 있습니다. 이 예에서는 각각 분석, 포함, 근절 및 검토에 대한 스테이지를 만들 수 있습니다. 다음 예시에서는 분석 단계가 즉시 시작되며 실행 조건이 없습니다. 이전 스테이지가 완료된 후 스테이지 시작을 포함하며 이전 스테이지의 활동 결과를 기반으로 하는 실행 조건이 있습니다.
    스테이지를 추가한 후에는 각 스테이지에 대한 프로세스 활동을 추가해야 합니다.
12. 특정 스테이지(예: 분석 스테이지)에서 다른 프로세스 활동 추가를 클릭합니다.
    활동 추가 팝업이 열립니다.
    a. 활동 추가 팝업에서 필요한 활동 정의를 선택합니다.
13. 새 활동 만들기를 클릭합니다.
    활동 정의를 추가한 후 스테이지와 유사하게 추가로 구성할 수 있습니다. 마찬가지로 각 스테이지 아래에 다른 프로세스 활동을 생성할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

수동 맬웨어 활동



14. 활동 속성 창에서 실행 조건을 추가하고 프로세스 활동을 시작할 시기를 나타냅니다.
15. 실행 조건을 추가하고 시작 시기를 나타냅니다.
    이 활동에 필요한 모든 입력(구성된 자동화 계획의 입력 포함)이 표시됩니다. 값을 재정의하거나 미리 구성된 값을 사용할 수 있습니다.
16. 모든 속성 보기를 클릭하고 고급 속성 토글을 활성화하여 활동 정의의 모든 활동 경험 필드를 표시합니다.

수동 맬웨어 플레이북 사용

다음 단계를 사용하여 SIR 분석가 작업 공간에서 수동 맬웨어 플레이북을 사용하는 방법과 해당 기능을 알아봅니다.

시작하기 전에

필요한 역할: sn_si.admin 또는 sn_si.manager 또는 sn_si.analyst

프로시저

1. SIR 작업 공간에서 보안 인시던트를 엽니다.
2. 플레이북 탭을 클릭합니다.

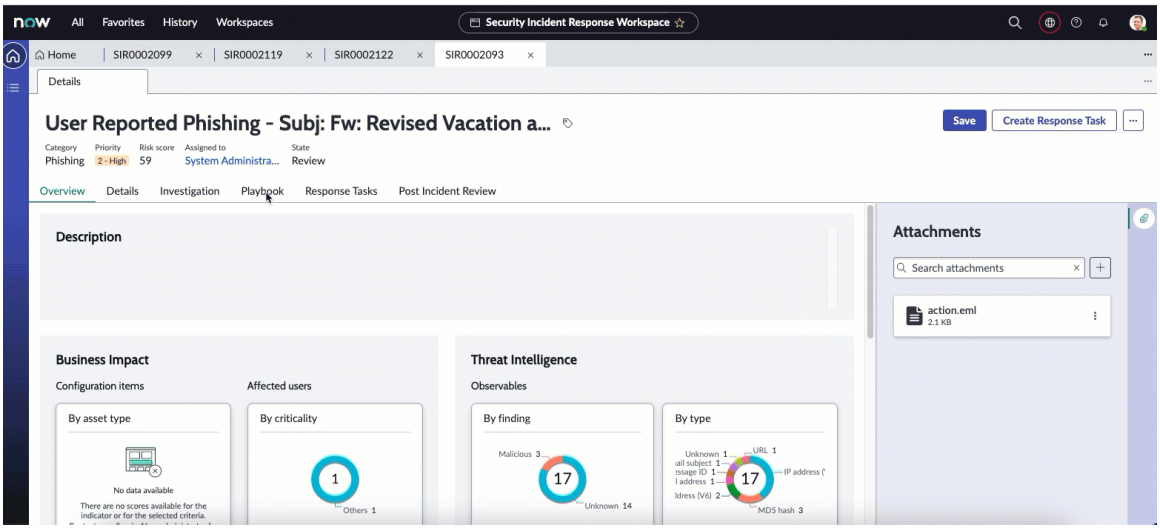
   보안 인시던트에 대해 활성화된 플레이북을 볼 수 있습니다. 보안 인시던트의 범주, 위험 점수와 같은 상세 정보도 볼 수 있습니다.

   > **주:**
   > 나열된 플레이북이 표시되지 않으면 PAD로 이동하여 플레이북 탭에서 볼 수 있도록 해야 합니다.

3. 수동 맬웨어 플레이북을 클릭합니다.
   수동 맬웨어의 경우 보안 인시던트에 대한 작업이 자동으로 수행됩니다.
4. 각 스테이지를 클릭하여 이 플레이북에서 어떤 작업이 수행되었는지 확인합니다.
5. 분석을 클릭하여 분석 단계에서 수행된 활동 목록을 봅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

요구 사항에 따라 변경할 수 있습니다.



6. 마찬가지로 포함, 근절 및 검토를 클릭하여 각 단계에서 수행된 활동 목록을 볼 수 있습니다. 요구 사항에 따라 변경할 수 있습니다. 수행해야 하는 나머지 활동 또는 사용자 작업이 있는 경우 해당 단계에 표시됩니다.
7. 단계에 필요한 나머지 활동 또는 사용자 작업이 있는 경우 해당 단계를 클릭하고 작업을 수행하여 활동을 완료합니다.

자동화된 맬웨어에 대한 플레이북

자동화된 맬웨어 플레이북은 분석가가 맬웨어 경고를 보다 효율적으로 해결하는 데 도움이 되는 일련의 자동화된 단계를 제공합니다.

자동화된 맬웨어 플레이북 템플릿은 엔드포인트 또는 네트워크에서 맬웨어 경고를 처리하는 데 관련된 단계를 자동화하도록 설계되었습니다. 의 워크플로우 스튜디오 플레이북 템플릿을 사용하여 자동화된 맬웨어 플레이북의 단계를 자동화하고 이러한 경보를 효율적으로 해결할 수 있습니다. 이 플레이북에는 트리거 조건, 작업 시퀀스 및 주석을 달 수 있는 하위 플로우가 포함되어 있습니다. 이 플레이북에는 맬웨어 공격에 대응하도록 설계된 재사용 가능한 작업 시퀀스가 포함되어 있습니다. 각 플로우에는 트리거(조건), 작업 시퀀스 및 주석에 대한 하위 플로우가 있습니다.

이 Playbook은 보안 인시던트가 생성되거나 업데이트되는 경우에 사용할 수 있습니다. 에서 워크플로우 스튜디오자동화된 맬웨어 플레이북을 활성화해야 하며, 이 플레이북은 분석, 포함, 근절 및 검토와 같은 모든 작업을 자동으로 수행합니다.

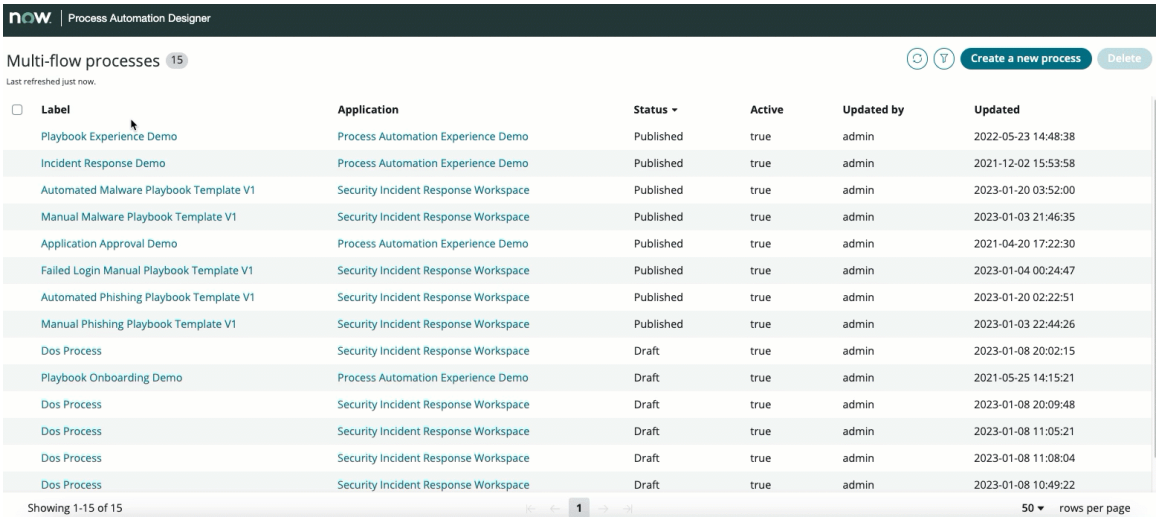
다음은 프로세스 정의의 스테이지이며 보안 인시던트 상태에 해당합니다.

- 분석
- 포함
- 근절
- 검토

각 스테이지에는 활동이 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

자동화된 맬웨어 플레이북



스테이지에서 작업을 완료로 표시하면 다음 작업으로 이동할 수 있습니다. 언제든지 작업을 저장하고 나중에 날짜 및 시간에 플레이북으로 돌아갈 수 있습니다. 스테이지의 모든 작업을 완료한 후 다음 스테이지로 이동할 수 있습니다. 작업과 스테이지를 계속 완료하면 왼쪽 패널에 상태가 반영됩니다. 플레이북 오른쪽에 있는 활동 로그에는 각 작업에 대해 입력한 모든 데이터가 표시됩니다.

모든 작업을 완료한 후에는 모든 스테이지에서 입력한 세부 정보를 검토하라는 메시지가 표시됩니다. 필드를 편집하거나 마침을 클릭하여 권리를 생성하는 프로세스를 완료할 수 있습니다.

프로세스 생성 PAD의 자동화된 맬웨어

다음 단계를 사용하여 PAD(프로세스 자동화 디자이너)에서 자동화된 맬웨어에 대한 프로세스를 생성합니다.

시작하기 전에
필요한 역할: sn_si.admin 또는 sn_si.manager

프로시저

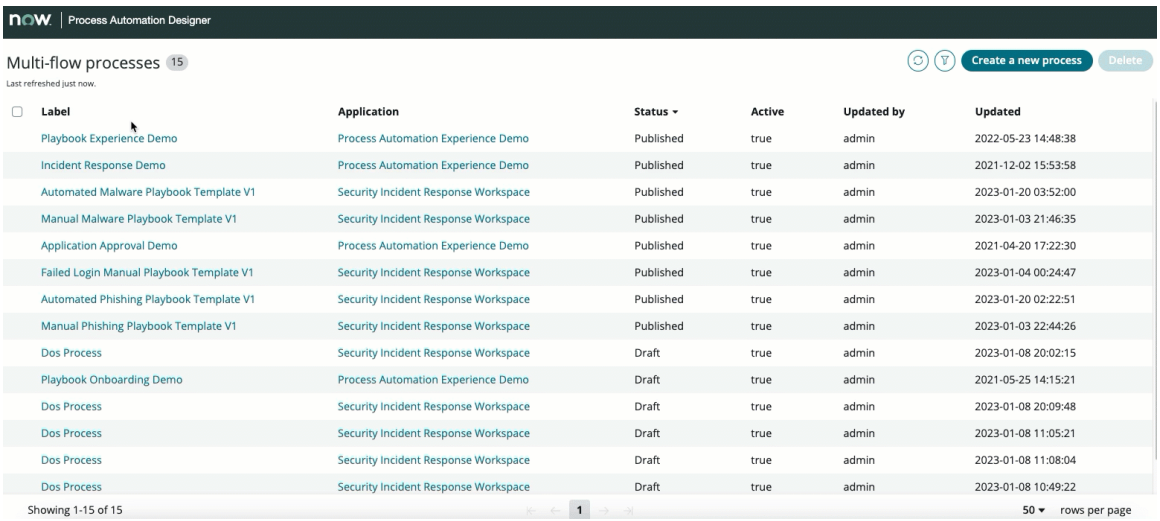
1. 클릭 **ALL** 〉 프로세스 자동화 디자이너 〉 〉 새 프로세스 작성.

   예를 들어 자동화된 맬웨어 플레이북 템플릿 V1입니다.

2. 프로세스의 이름, 설명 및 프로세스를 생성할 애플리케이션을 입력합니다.
3. 트리거 선택을 클릭합니다.
4. 프로세스가 실행되는 시기에 대한 고유한 조건 정의를 선택하고 프로세스를 실행해야 하는 시기에 대한 트리거 조건을 선택합니다.
5. 트리거 조건 설정을 클릭합니다.
6. 테이블을 선택하고 조건을 입력하여 프로세스를 실행해야 하는 시기를 정의하는 조건을 선택합니다.
   예를 들어 트리거 조건은 피싱 범주의 보안 인시던트가 생성될 때입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

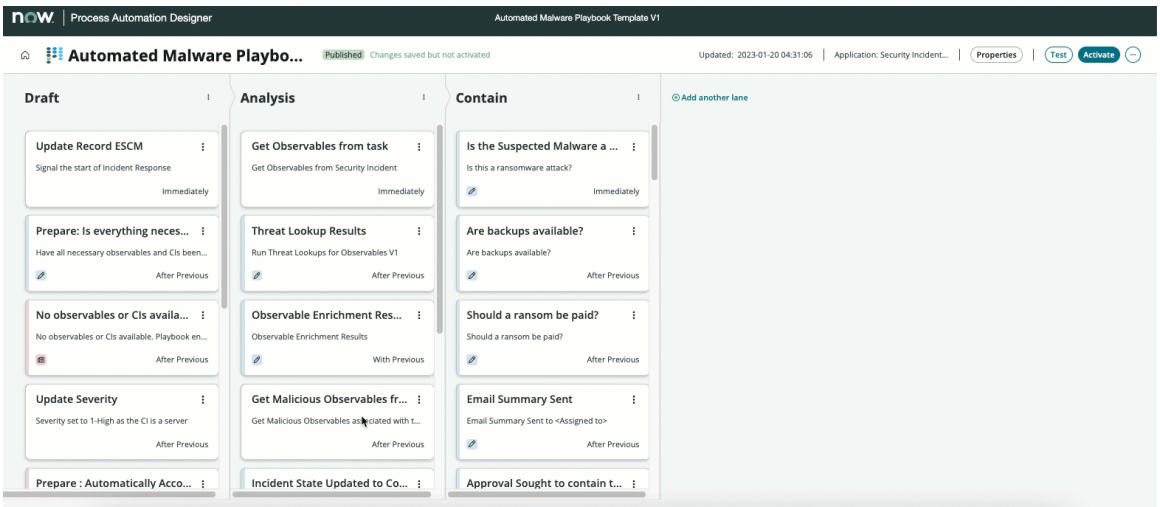
자동화된 맬웨어 플레이북



7. 디자이너로 이동을 클릭합니다.
   Process Automation Designer 페이지가 열립니다.
8. 자동화된 프로세스 설계를 시작하려면 새 스테이지 추가를 클릭합니다.
   UI 오른쪽에 스테이지 속성 창이 열립니다.
9. 스테이지 속성 창에 이름, 설명, 실행 조건, 시작 시기 표시와 같은 세부 정보를 입력합니다.
   실행 조건 및 시작 시기 표시 필드는 스테이지가 실행되는 시기를 의미합니다.
10. 저장 후 닫기를 클릭합니다.
11. 다른 스테이지를 추가하려면 **Add another** stage(다른 스테이지 추가)를 클릭합니다.
    마찬가지로 원하는 만큼 스테이지를 만들 수 있습니다. 이 예에서는 각각 분석, 포함, 근절 및 검토에 대한 스테이지를 만들 수 있습니다. 다음 예시에서는 분석 단계가 즉시 시작되며 실행 조건이 없습니다. 이전 스테이지가 완료된 후 스테이지 시작을 포함하며 이전 스테이지의 활동 결과를 기반으로 하는 실행 조건이 있습니다.
    스테이지를 추가한 후에는 각 스테이지에 대한 프로세스 활동을 추가해야 합니다.
12. 특정 스테이지(예: 분석 스테이지)에서 다른 프로세스 활동 추가를 클릭합니다.
    활동 추가 팝업이 열립니다.
    a. 활동 추가 팝업에서 필요한 활동 정의를 선택합니다.
13. 새 활동 만들기를 클릭합니다.
    활동 정의를 추가한 후 스테이지와 유사하게 추가로 구성할 수 있습니다. 마찬가지로 각 스테이지 아래에 다른 프로세스 활동을 생성할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

자동화된 맬웨어 활동



14. 활동 속성 창에서 실행 조건을 추가하고 프로세스 활동을 시작할 시기를 나타냅니다.
15. 실행 조건을 추가하고 시작 시기를 나타냅니다.
    이 활동에 필요한 모든 입력(구성된 자동화 계획의 입력 포함)이 표시됩니다. 값을 재정의하거나 미리 구성된 값을 사용할 수 있습니다.
16. 모든 속성 보기를 클릭하고 고급 속성 토글을 활성화하여 활동 정의의 모든 활동 경험 필드를 표시합니다.

자동화된 맬웨어 플레이북 사용

다음 단계를 사용하여 SIR 분석가 작업 공간에서 자동화된 맬웨어 플레이북을 사용하는 방법과 해당 기능을 알아봅니다.

시작하기 전에

필요한 역할: sn_si.admin 또는 sn_si.manager 또는 sn_si.analyst

프로시저

1. SIR 작업 공간에서 보안 인시던트를 엽니다.
2. 플레이북 탭을 클릭합니다.

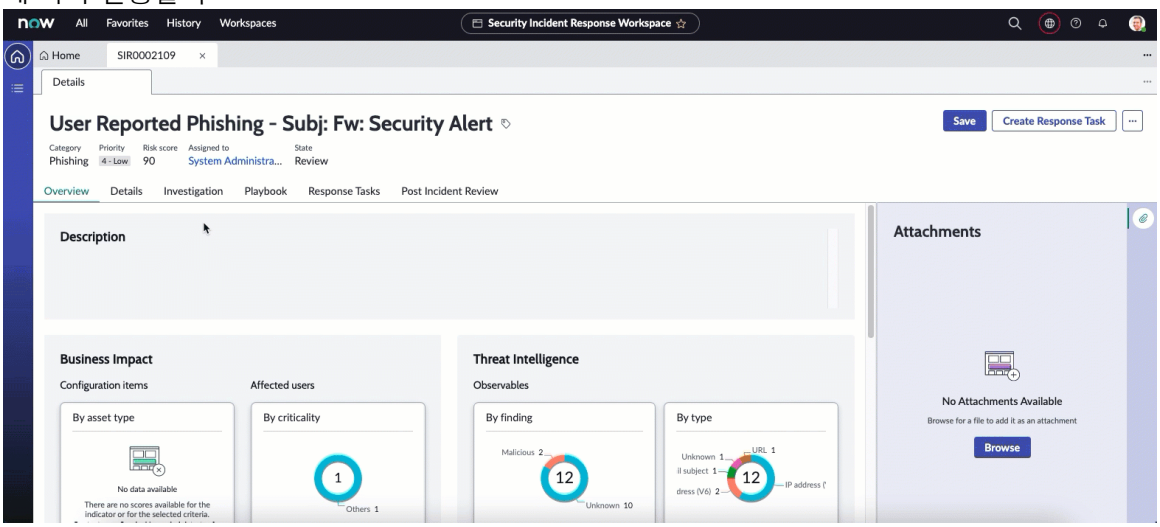
   보안 인시던트에 대해 활성화된 플레이북을 볼 수 있습니다. 보안 인시던트의 범주, 위험 점수와 같은 상세 정보도 볼 수 있습니다.

   > **주:**
   > 나열된 플레이북이 표시되지 않으면 PAD로 이동하여 플레이북 탭에서 볼 수 있도록 해야 합니다.

3. 자동화된 맬웨어 플레이북을 클릭합니다.
   자동화된 맬웨어의 경우 보안 인시던트에 대한 작업이 자동으로 수행됩니다.
4. 각 스테이지를 클릭하여 이 플레이북에서 어떤 작업이 수행되었는지 확인합니다.
5. 분석을 클릭하여 분석 단계에서 수행된 활동 목록을 봅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

요구 사항에 따라 변경할 수 있습니다.



6. 마찬가지로 포함, 근절 및 검토를 클릭하여 각 단계에서 수행된 활동 목록을 볼 수 있습니다. 요구 사항에 따라 수정할 수 있습니다. 수행해야 하는 나머지 활동 또는 사용자 작업이 있는 경우 해당 단계에 표시됩니다.
7. 단계에 필요한 나머지 활동 또는 사용자 작업이 있는 경우 해당 단계를 클릭하고 작업을 수행하여 활동을 완료합니다.

실패한 로그인에 대한 플레이북 수동

실패한 로그인 수동 플레이북은 지침을 제공하고 실패한 로그인 보안 인시던트의 조사를 최적화하는 데 도움을 줍니다.

사용자가 SIM 구성에 따라 특정 로그인 시도를 실패하면 보안 인시던트가 생성됩니다. 이러한 실패한 로그인 시도는 가양성이거나 공격자가 사용자 이메일 계정에 대한 액세스 권한을 얻으려는 시도일 수 있습니다.

의 워크플로우 스튜디오 플레이북 템플릿을 사용하여 실패한 로그인 플레이북의 단계를 수행하고 실패한 로그인 보안 인시던트를 효율적으로 해결할 수 있습니다. 이 플레이북에는 트리거 조건, 작업 시퀀스 및 주석을 달 수 있는 하위 플로우가 포함되어 있습니다. 이 플레이북에는 실패한 로그인 보안 인시던트에 대응하도록 설계된 재사용 가능한 작업 시퀀스가 포함되어 있습니다. 각 플로우에는 트리거(조건), 작업 시퀀스 및 주석에 대한 하위 플로우가 있습니다.

실패한 로그인 보안 인시던트가 생성되거나 업데이트되면 이 플레이북을 사용할 수 있습니다. 에서 워크플로우 스튜디오 실패한 로그인 수동 플레이북을 활성화하고 분석, 포함, 근절, 검토와 같은 모든 작업을 생성해야 합니다.

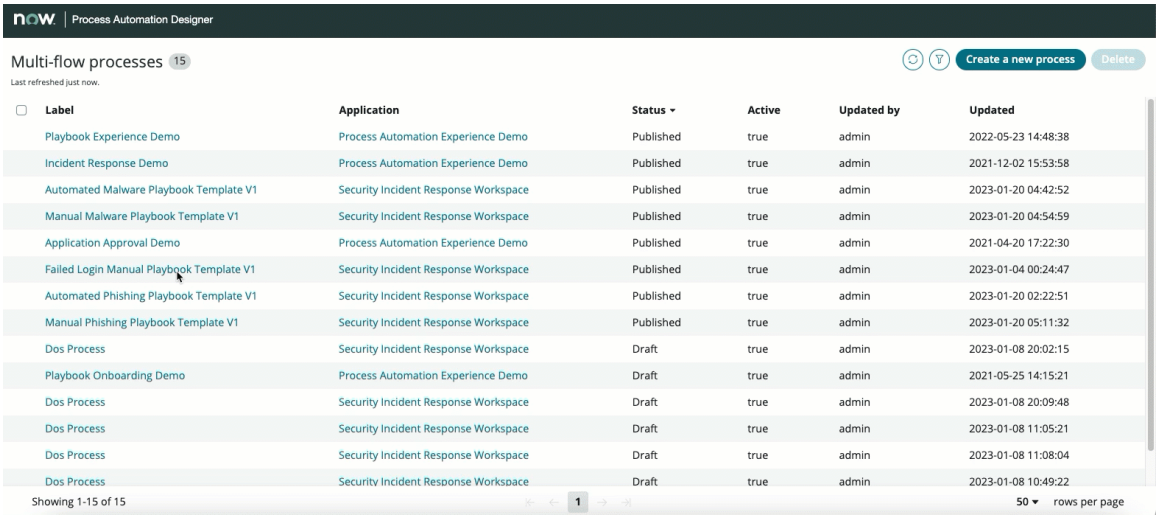
다음은 프로세스 정의의 스테이지이며 보안 인시던트 상태에 해당합니다.

- 분석
- 포함
- 근절
- 검토

각 스테이지에는 활동이 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

실패한 로그인 수동 플레이북



스테이지에서 작업을 완료로 표시하면 다음 작업으로 이동할 수 있습니다. 언제든지 작업을 저장하고 나중에 날짜 및 시간에 플레이북으로 돌아갈 수 있습니다. 스테이지의 모든 작업을 완료한 후 다음 스테이지로 이동할 수 있습니다. 작업과 스테이지를 계속 완료하면 왼쪽 패널에 상태가 반영됩니다. 플레이북 오른쪽에 있는 활동 로그에는 각 작업에 대해 입력한 모든 데이터가 표시됩니다.

모든 작업을 완료한 후에는 모든 스테이지에서 입력한 세부 정보를 검토하라는 메시지가 표시됩니다. 필드를 편집하거나 마침을 클릭하여 권리를 생성하는 프로세스를 완료할 수 있습니다.

PAD에서 실패한 로그인 설명서에 대한 프로세스 생성

다음 단계를 사용하여 PAD(프로세스 자동화 디자이너)에서 실패한 로그인 수동에 대한 프로세스를 생성합니다.

시작하기 전에

필요한 역할: sn_si.admin 또는 sn_si.manager

프로시저

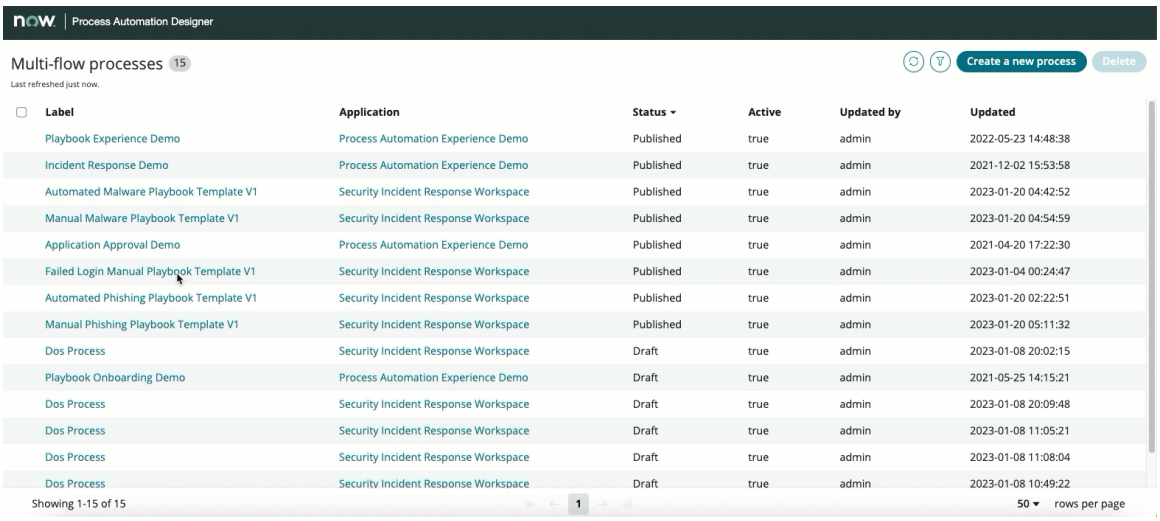
1. 클릭 **ALL** 〉 프로세스 자동화 디자이너 〉 〉 새 프로세스 작성.

   예를 들어 실패한 로그인 수동 플레이북 템플릿 V1입니다.

2. 프로세스의 이름, 설명 및 프로세스를 생성할 애플리케이션을 입력합니다.
3. 트리거 선택을 클릭합니다.
4. 프로세스가 실행되는 시기에 대한 고유한 조건 정의를 선택하고 프로세스를 실행해야 하는 시기에 대한 트리거 조건을 선택합니다.
5. 트리거 조건 설정을 클릭합니다.
6. 테이블을 선택하고 조건을 입력하여 프로세스를 실행해야 하는 시기를 정의하는 조건을 선택합니다.
   예를 들어 트리거 조건은 피싱 범주의 보안 인시던트가 생성될 때입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

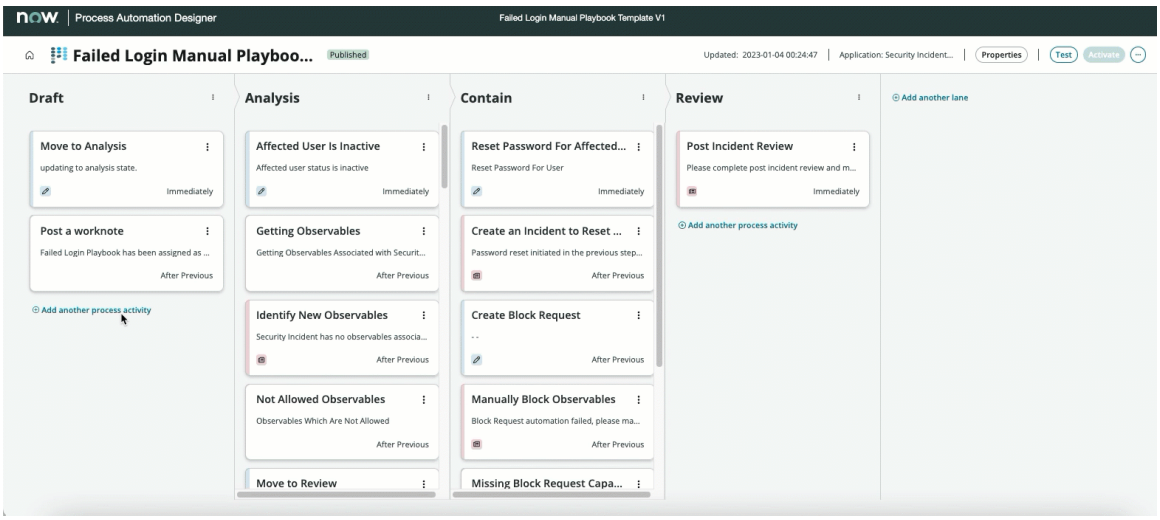
실패한 로그인 수동 플레이북



7. 디자이너로 이동을 클릭합니다.
   Process Automation Designer 페이지가 열립니다.
8. 자동화된 프로세스 설계를 시작하려면 새 스테이지 추가를 클릭합니다.
   UI 오른쪽에 스테이지 속성 창이 열립니다.
9. 스테이지 속성 창에 이름, 설명, 실행 조건, 시작 시기 표시와 같은 세부 정보를 입력합니다.
   실행 조건 및 시작 시기 표시 필드는 스테이지가 실행되는 시기를 의미합니다.
10. 저장 후 닫기를 클릭합니다.
11. 다른 스테이지를 추가하려면 **Add another** stage(다른 스테이지 추가)를 클릭합니다.
    마찬가지로 원하는 만큼 스테이지를 만들 수 있습니다. 이 예에서는 각각 분석, 포함, 근절 및 검토에 대한 스테이지를 만들 수 있습니다. 다음 예시에서는 분석 단계가 즉시 시작되며 실행 조건이 없습니다. 이전 스테이지가 완료된 후 스테이지 시작을 포함하며 이전 스테이지의 활동 결과를 기반으로 하는 실행 조건이 있습니다.
    스테이지를 추가한 후에는 각 스테이지에 대한 프로세스 활동을 추가해야 합니다.
12. 특정 스테이지(예: 분석 스테이지)에서 다른 프로세스 활동 추가를 클릭합니다.
    활동 추가 팝업이 열립니다.
    a. 활동 추가 팝업에서 필요한 활동 정의를 선택합니다.
13. 새 활동 만들기를 클릭합니다.
    활동 정의를 추가한 후 스테이지와 유사하게 추가로 구성할 수 있습니다. 마찬가지로 각 스테이지 아래에 다른 프로세스 활동을 생성할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

실패한 로그인 수동 활동



14. 활동 속성 창에서 실행 조건을 추가하고 프로세스 활동을 시작할 시기를 나타냅니다.
15. 실행 조건을 추가하고 시작 시기를 나타냅니다.
    이 활동에 필요한 모든 입력(구성된 자동화 계획의 입력 포함)이 표시됩니다. 값을 재정의하거나 미리 구성된 값을 사용할 수 있습니다.
16. 모든 속성 보기를 클릭하고 고급 속성 토글을 활성화하여 활동 정의의 모든 활동 경험 필드를 표시합니다.

실패한 로그인 수동 플레이북 사용

다음 단계를 사용하여 SIR 분석가 작업 공간에서 실패한 로그인 수동 플레이북을 사용하는 방법과 해당 기능을 알아봅니다.

시작하기 전에

필요한 역할: sn_si.admin 또는 sn_si.manager 또는 sn_si.analyst

프로시저

1. SIR 작업 공간에서 보안 인시던트를 엽니다.
2. 플레이북 탭을 클릭합니다.

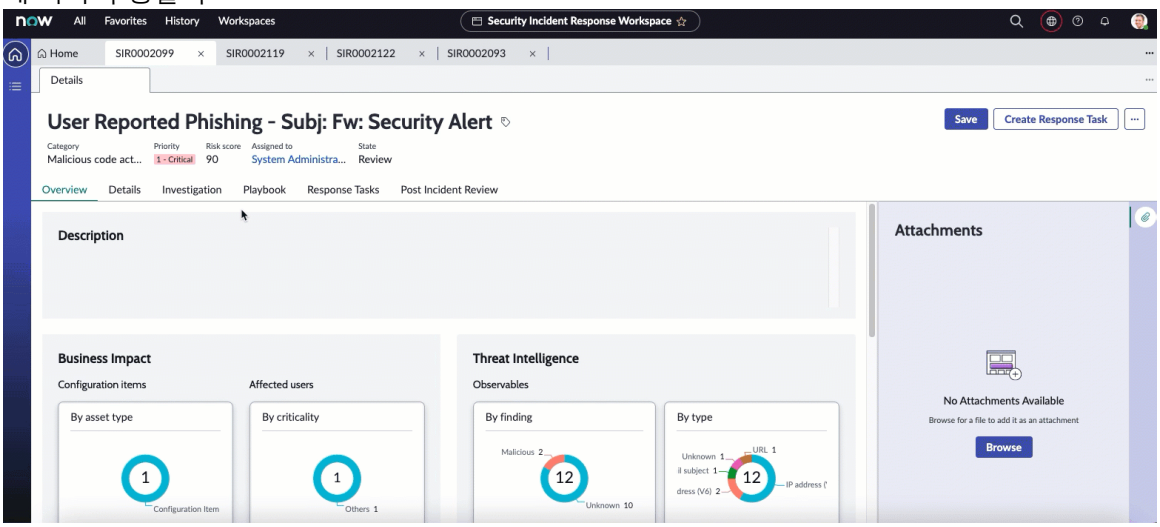
   보안 인시던트에 대해 활성화된 플레이북을 볼 수 있습니다. 보안 인시던트의 범주, 위험 점수와 같은 상세 정보도 볼 수 있습니다.

   > **주:**
   > 나열된 플레이북이 표시되지 않으면 PAD로 이동하여 플레이북 탭에서 볼 수 있도록 해야 합니다.

3. 실패한 로그인 수동 플레이북을 클릭합니다.
   실패한 로그인 설명서의 경우 보안 인시던트에 대한 작업이 자동으로 수행됩니다.
4. 각 스테이지를 클릭하여 이 플레이북에서 어떤 작업이 수행되었는지 확인합니다.
5. 분석을 클릭하여 분석 단계에서 수행된 활동 목록을 봅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

요구 사항에 따라 수정할 수 있습니다.



6. 마찬가지로 포함, 근절 및 검토를 클릭하여 각 단계에서 수행된 활동 목록을 볼 수 있습니다. 요구 사항에 따라 변경할 수 있습니다. 수행해야 하는 나머지 활동 또는 사용자 작업이 있는 경우 해당 단계에 표시됩니다.
7. 단계에 필요한 나머지 활동 또는 사용자 작업이 있는 경우 해당 단계를 클릭하고 작업을 수행하여 활동을 완료합니다.

플로우 기반 플레이북

Flow Designer를 사용하면 보안 관리자와 Flow Design 작성자가 수동 또는 문서화되지 않은 플레이북에서 자동화되고 반복 가능한 플레이북으로 더 쉽게 전환할 수 있습니다. 끌어서 놓기 기능은 객체 이동, 조건 검사, 병렬 분기, 결정 테이블 등에 유연성을 제공합니다.

보안 인시던트 응답 에서는 기본 시스템과 함께 다음과 같은 플레이북을 제공합니다.

나열된 플레이북 외에도 플로우 플레이북에서 호출할 수 있는 보안 운영 스포크 내의 하위 플로우도 있습니다. 랜섬웨어는 그러한 하위 플로우 중 하나입니다.

이러한 플로우를 사용하기 전에 활성화합니다. 자세한 내용은 보안 인시던트 응답 플로우 활성화를 참조하십시오.

자동화된 피싱을 위한 플레이북

자동화된 피싱 플레이북은 특정 유형의 보안 위협을 단계별로 해결하는 데 도움이 됩니다. 플로우 디자이너 템플릿을 사용하면 피싱 응답 플레이북의 단계를 자동화하고 인시던트를 빠르고 효율적으로 해결할 수 있습니다.

플로우 디자이너로 작성된 템플릿을 사용하여 피싱 응답 플레이북 의 작업을 자동화함으로써 조직의 피싱 공격을 분석하고 해결할 수 있습니다.

피싱 응답 플레이북에는 다음과 같은 플로우와 하위 플로우가 포함됩니다.

- 보안 인시던트 - 자동화된 피싱 응답 템플릿: 이 템플릿은 피싱 응답 작업을 자동화하도록 설계되었으며 트리거를 비롯한 일련의 작업을 포함합니다.
- 보안 인시던트 - 피싱 수동 템플릿: 이 템플릿은 기존 수동 피싱 응답 워크플로우입니다. 범주를 피싱으로 설정하여 플로우를 활성화합니다.

이러한 템플릿에는 피싱 공격에 대응하도록 설계된 재사용 가능한 작업 시퀀스가 포함되어 있습니다. 각 플로우에는 트리거(조건), 작업 시퀀스 및 하위 플로우가 있으며 가독성을 위해 주석을 달 수 있습니다. 이러한 플로우에 액세스하려면보안 운영 스포크 를 설치해야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
이러한 템플릿을 사용하려면 먼저 활성화해야 합니다. 자세한 내용은 보안 인시던트 응답 플로우 활성화 를 참조하십시오.

- 옵저버블에 대한 위협 조회 실행: 선택한 옵저버블의 위협 조회를 수행합니다.
- 옵저버블 보강: 다양한 소스의 추가 정보로 옵저버블을 보강할 수 있습니다.
- 피싱 이메일 영향 평가: 피싱 이메일의 영향을 평가할 수 있습니다. 피싱 이메일 주소로 이메일을 받으면 이 하위 플로우는 . EML 첨부 파일을 만들고 정보를 이메일 일치 규칙과 비교합니다.
- 피싱 이메일 근절: 피싱 이메일을 삭제하거나 근절하여 특정 공격에 대한 노출을 줄일 수 있습니다.
- 옵저버블에 대해 사이팅 검색 실행: 시간 경과에 따른 위협의 확산을 확인하거나 정정 또는 근절 노력을 테스트합니다.
- 차단 요청 생성: 인시던트와 관련된 옵저버블과의 통신을 차단합니다.

이러한 하위 플로우는 여러 플레이북에서 사용할 수 있는 재사용 가능한 작업 세트를 나타냅니다. 이러한 하위 플로우를 사용하여 요구 사항에 따라 사용자 지정 템플릿(플로우)을 정의할 수 있습니다.

사용자 지정 템플릿(플로우)을 생성하려면 플로우의 지침을 따릅니다.

자동화된 피싱 응답 플레이북 플로우 실행

플로우 디자이너를 사용하면 플레이북에서 작업을 정의하고 자동화하여 조직에 대한 피싱 공격을 분석하고 해결할 수 있습니다.

시작하기 전에

- 필요한 역할: sn_si.admin, flow_designer, action_designer
- 올바른 자격 증명을 사용하여 다음 통합을 설치하고 구성합니다.
  - 블록 요청(보안 운영 Palo Alto Networks NGFW 통합)
  - 관찰 대상 보강
  - 사이팅 검색
  - 위협 조회
  - Microsoft Office Exchange

이 태스크 정보

직원이 피싱 공격의 일반적인 징후가 포함된 의심스러운 이메일을 수신하면(보안 정책에서 정의한대로) 해당 이메일을 . 조직에서 정의한 피싱 이메일 주소에 대한 EML 첨부 파일입니다. 자동화된 피싱 플레이북 플로우에 정의된 작업을 사용하여 피싱 위협을 분류, 분석, 억제 및 근절할 수 있습니다. 이러한 작업은 여러 인시던트 상태(예: 분석, 포함 등)의 일부로 호출될 수 있습니다. 피싱 보안 인시던트가 생성되면 자동화된 피싱 플로우가 자동으로 트리거될 수 있습니다. 플로우 디자이너를 사용하면 호출되는 다양한 인시던트 응답 작업의 상세 정보를 볼 수 있습니다.

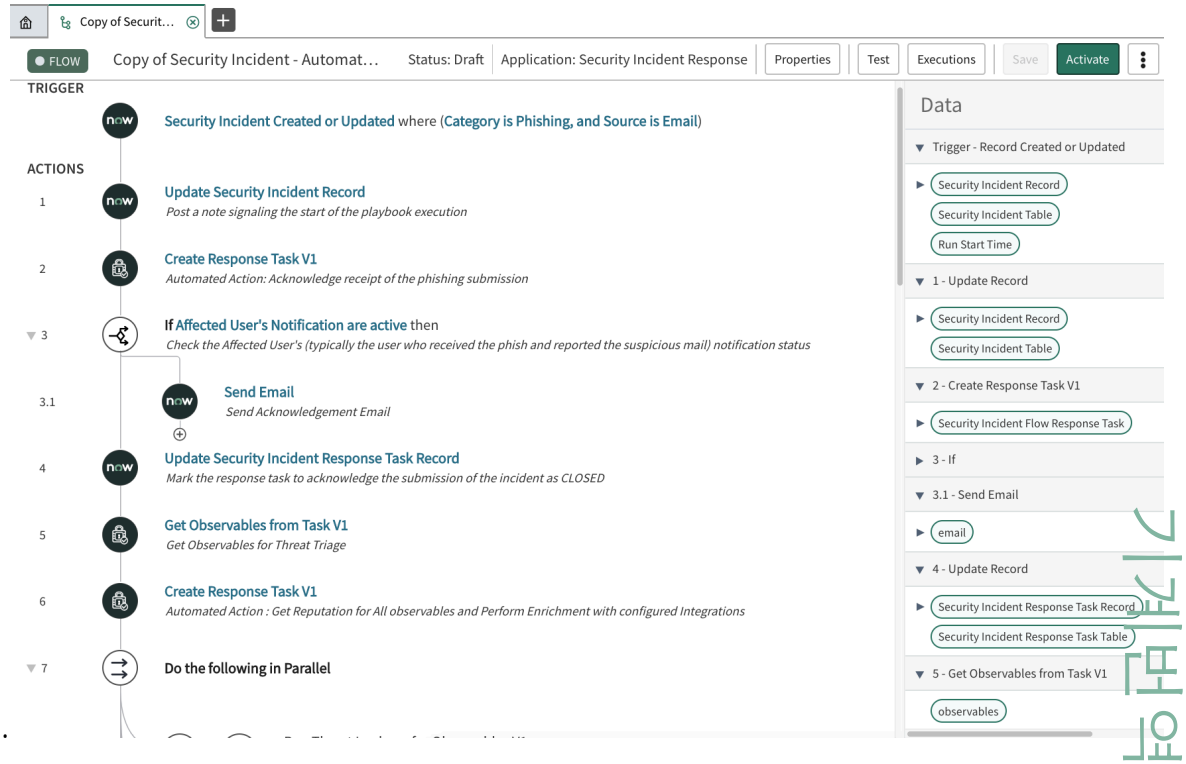
주:
보안 인시던트 - 자동화된 피싱 응답 템플릿 V1 플레이북 플로우는 읽기 전용입니다. 플로우의 사본을 만들고 필요에 따라 변경할 수 있습니다.

다음 단계에서는 피싱 플레이북 템플릿의 사본을 만드는 방법을 설명하고 플로우의 일부 작업을 안내합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

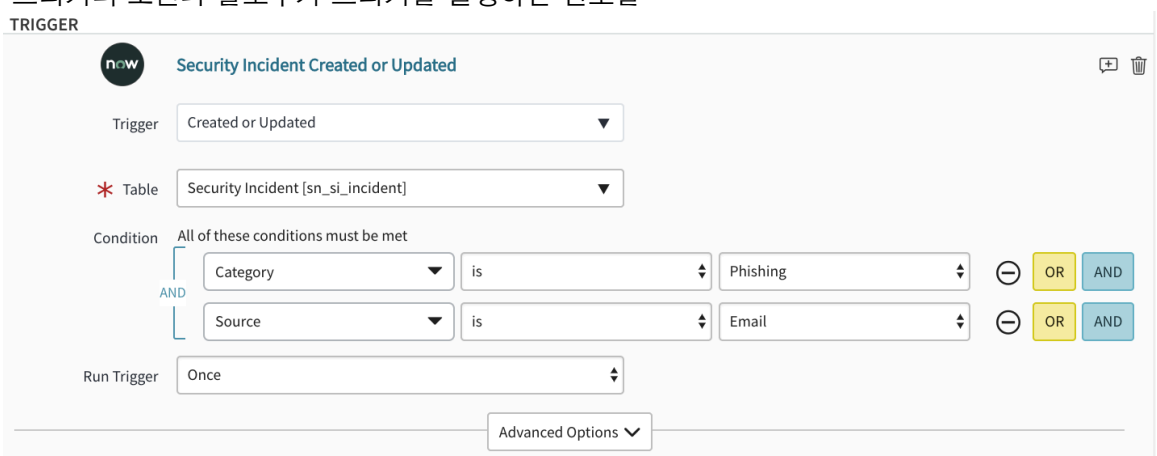
프로시저

1. 다음으로 이동 모두 〉 플로우 디자이너 〉 디자이너 을 클릭하여 스포크에서 사용할 수 있는 플로우를 보안 운영 봅니다.
2. 보안 인시던트 - 자동화된 피싱 응답 템플릿 **VI** 링크를 클릭합니다.
3. 플로우 페이지에서 더 보기 아이콘 ⋮ 을 클릭하고 플로우의 사본을 만들고 사용할 수 있도록 엽니다.
   트리거 조건을 수정하고, 작업을 추가 또는 제거하고, 플로우에 기타 변경 사항을 적용할 수 있습니다.



이 이미지는 트리거 조건과 플로우가 실행되는 단계를 보여줍니다. 오른쪽 패널에는 데이터 흐름이 표시됩니다. 아이콘을 클릭하여 단계를 확장하고 상세 정보를 봅니다.

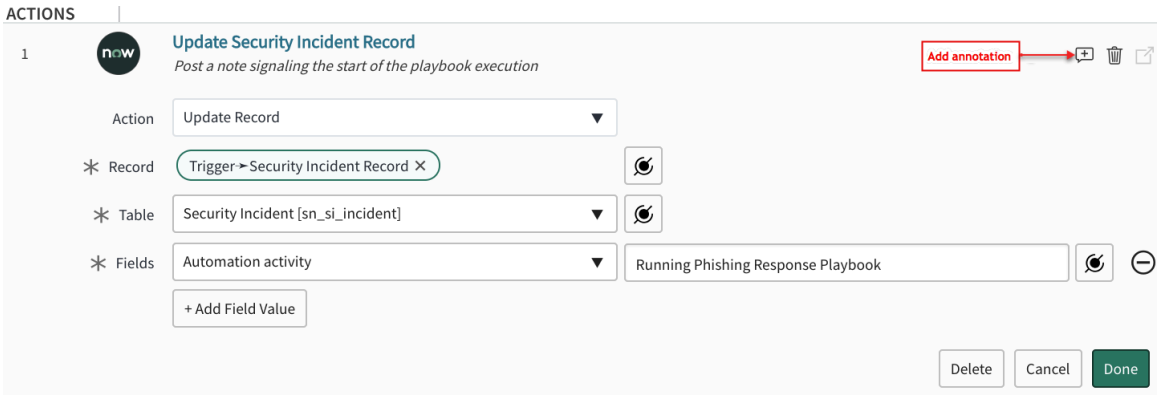
4. 트리거 아이콘을 클릭합니다.
   첫 번째 단계에서는 플로우에 대한 트리거를 정의하거나 설정합니다. 트리거의 조건과 플로우가 트리거를 실행하는 빈도를 지정합니다.



플로우에 정의된 조건(범주는 피싱, 소스는 이메일)이 인시던트 기록에서 충족되면 자동화된 피싱 플로우의 작업이 순차적으로 실행되기 시작합니다. 트리거를 수정하고, 주석을 추가하고, 조건을 추가 또는 삭제하는 등의 작업을 수행할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

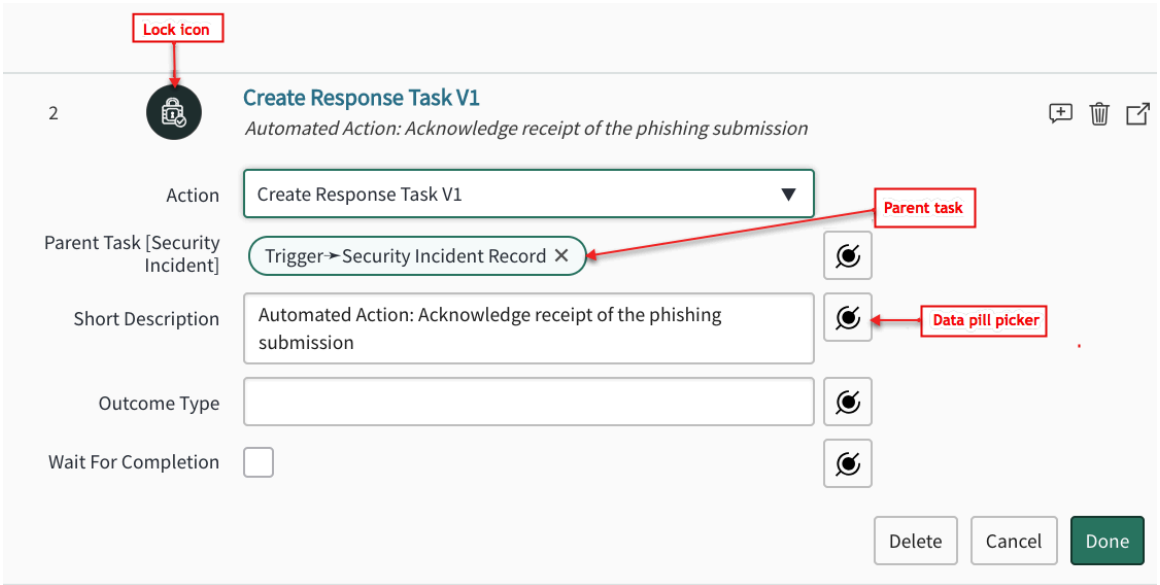
5. 보안 인시던트 기록 업데이트 링크를 클릭합니다.



보안 인시던트 기록 업데이트는 플로우의 첫 번째 단계입니다. 주석 아이콘 클릭하여 피싱 인시던트가 발생했으며 자동화된 피싱 플레이북 플로우가 실행되기 시작했음을 나타내는 메모를 보안 분석가에게 추가합니다.

6. 플로우의 2단계를 계속 진행하고 응답 작업 생성 링크를 클릭합니다.

이 단계에서 플로우는 자동화된 응답 작업을 생성하여 인시던트 제출자 또는 영향을 받는 사용자에게 수신을 확인합니다.

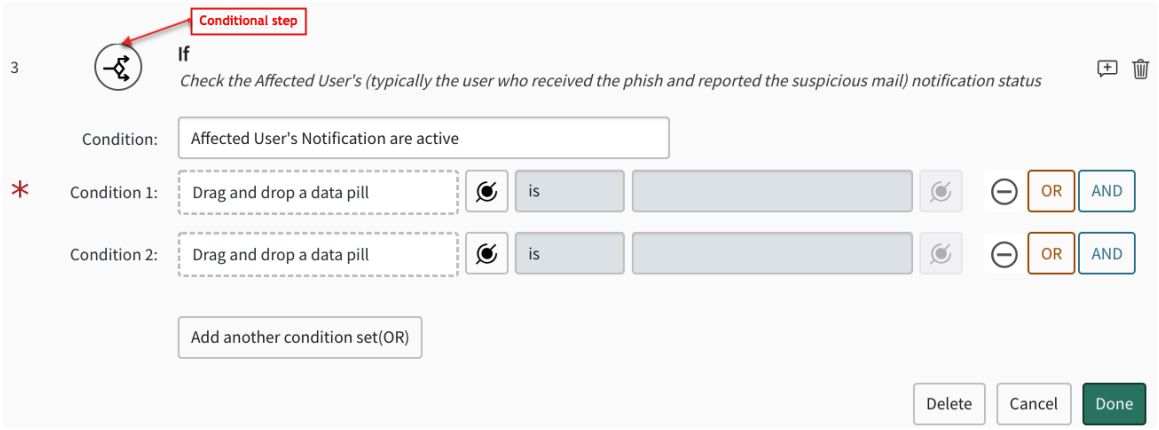


상위 작업〔보안 인시던트〕필드는 이 단계와 연결된 상위 기록을 참조합니다. 데이터 정제 선택기 아이콘, 사용하여 참조 기록을 선택하거나 오른쪽 패널에서 관련 참조 항목을 끌어서 참조 기록을 선택할 수 있습니다. 잠금 아이콘 을 확인합니다. 잠금 아이콘은 단계에 사용자 개입이 필요하지 않음을 나타냅니다.

7. 3단계에서 플로우는 영향을 받는 사용자(일반적으로 인시던트를 제출한 사용자)에 대한 추가 상세 정보를 수집하여 알림을 성공적으로 보낼 수 있도록 합니다.

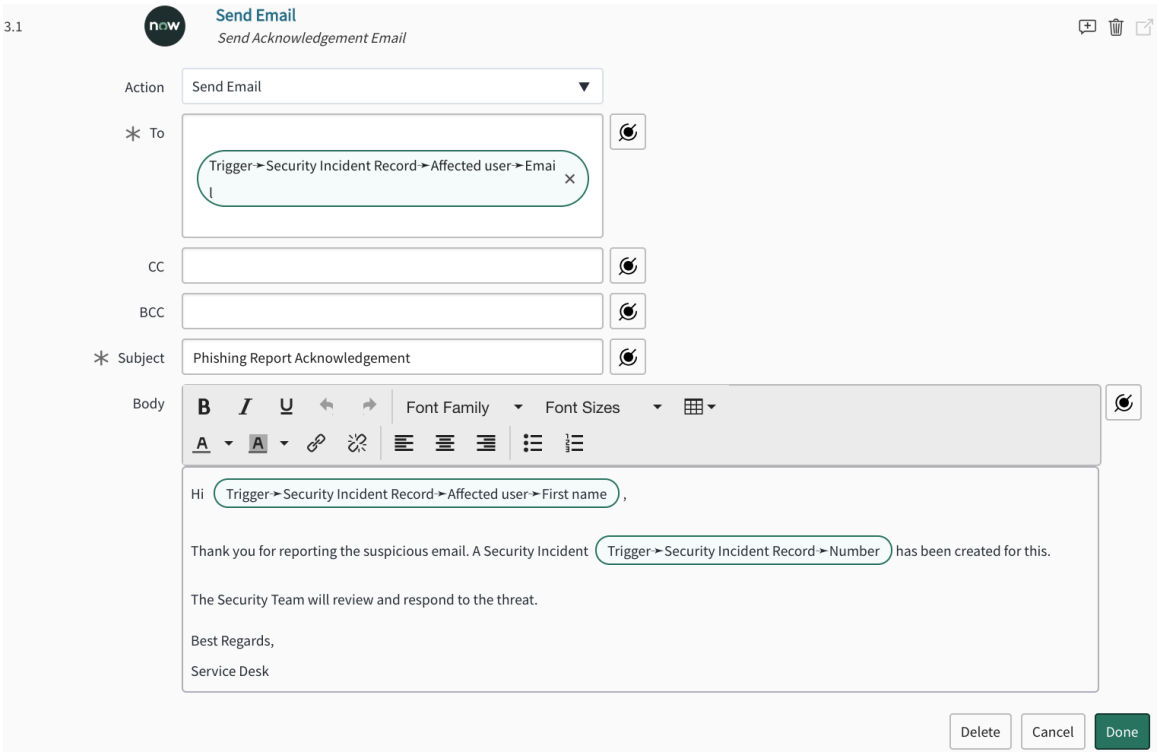
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

영향을 받는 사용자의 상태가 활성이고 사용자가 알림을 받을 수 있는지 확인하는 조건을 지정할 수



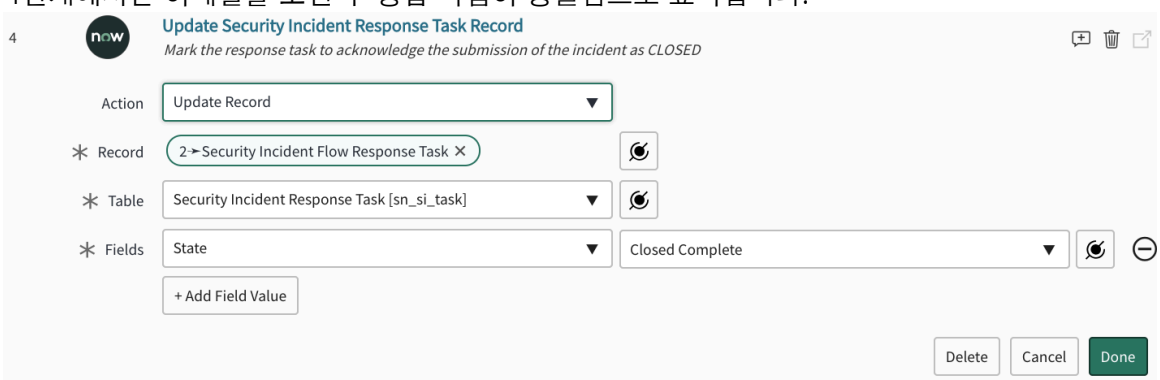
있습니다.

3단계의 조건부 확인합니다. 지정된 조건이 충족되는 경우에만 플로우가 다음 단계(3.1)를 실행합니다.



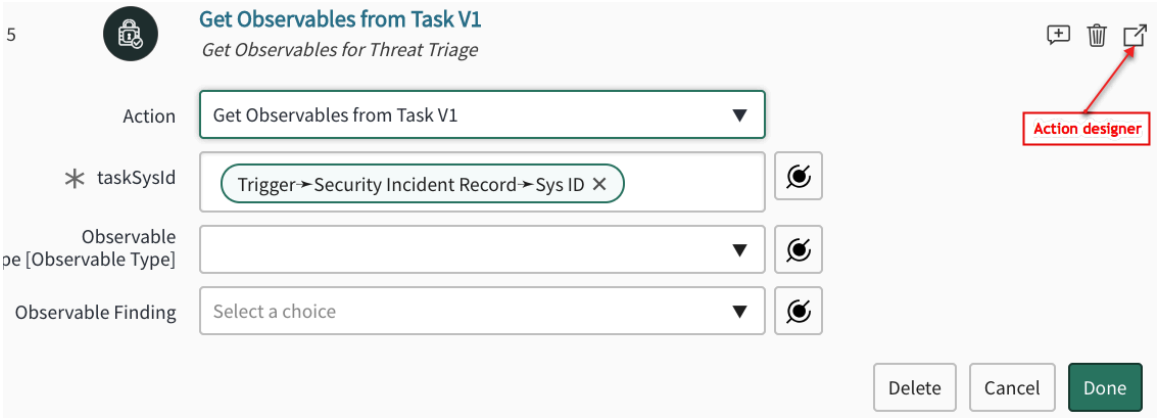
3단계에서 정의된 조건이 성공적으로 충족되면 이메일이 전송됩니다.

8. 4단계에서는 이메일을 보낸 후 응답 작업이 종결됨으로 표시됩니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

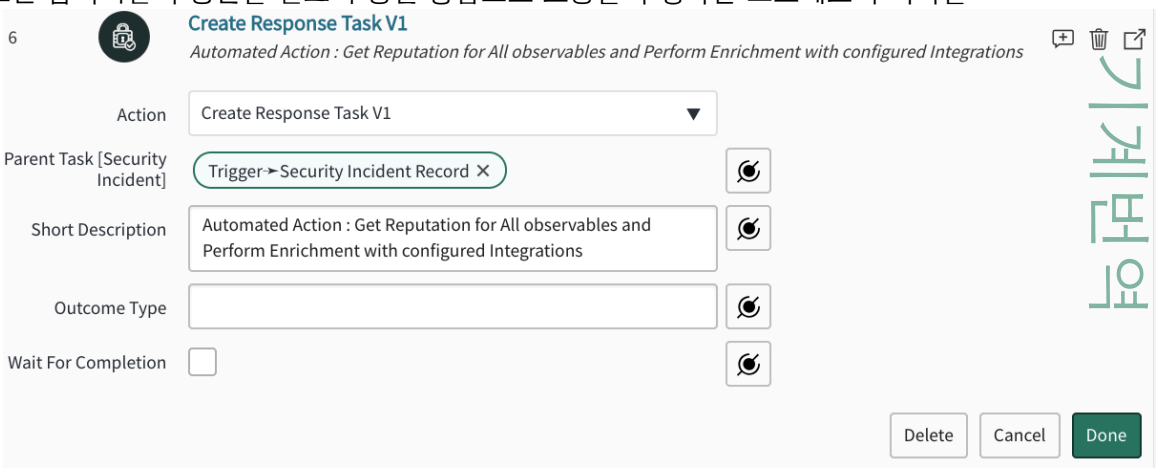
9. 5단계에서는 인시던트에 관련된 모든 옵저버블(예: 이메일 제목, 피싱 이메일이 전송된 이메일 주소, 피싱 URL) 또는 선택한 범주(해시, 파일 또는 도메인)에 속하는 옵저버블을 수집하여 후속 플레이북 단계에서 추가 자동화 작업을 수행합니다.



작업의 상세 뷰를 보려면 작업 디자이너 아이콘 클릭합니다.

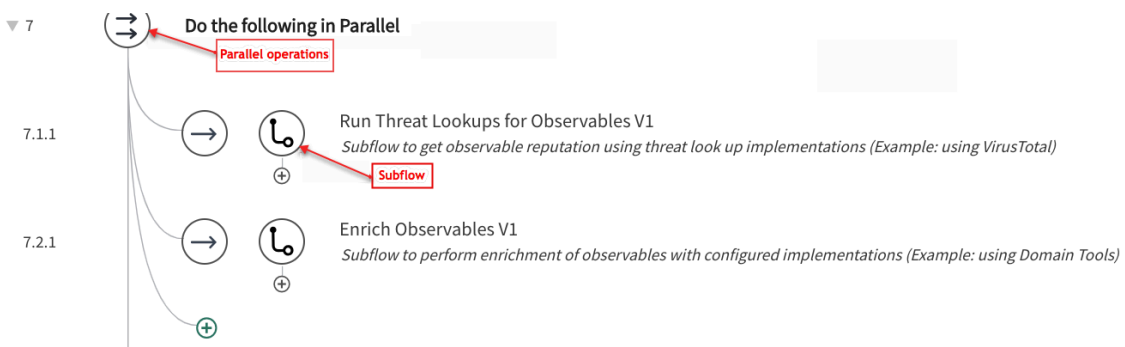
작업 디자이너 페이지를 보려면 플로우에서 단계를 확장하고 작업 디자이너 아이콘을 클릭합니다.

10. 6단계에서는 자동 응답 작업이 생성됩니다.
이 작업은 모든 옵저버블의 평판을 얻고 구성된 통합으로 보강을 수행하는 프로세스의 시작을



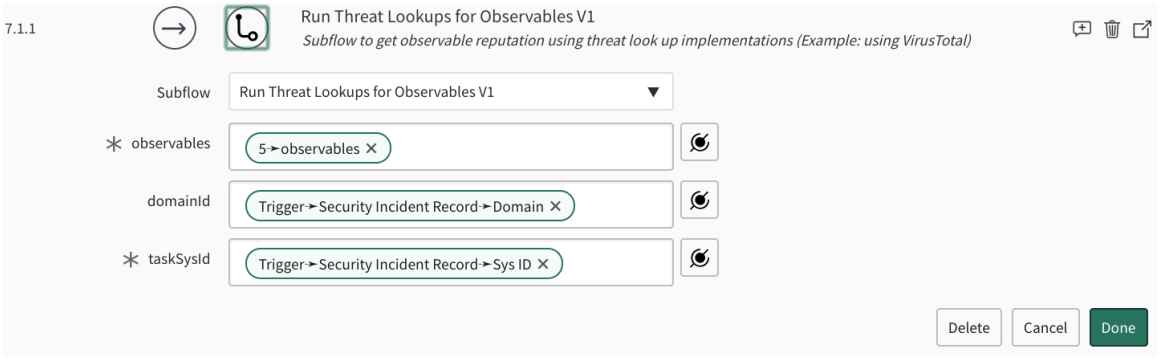
캡처합니다.

11. 7단계에서는 두 개의 하위 플로우가 호출됩니다.
    - 옵저버블에 대한 위협 조회 실행: 이 하위 플로우는 위협 조회 구현을 사용하여 모든 옵저버블의 평판을 가져오는 데 사용됩니다.
    - 옵저버블 보강: 이 하위 플로우는 구성된 구현으로 옵저버블을 보강하는 데 사용됩니다.



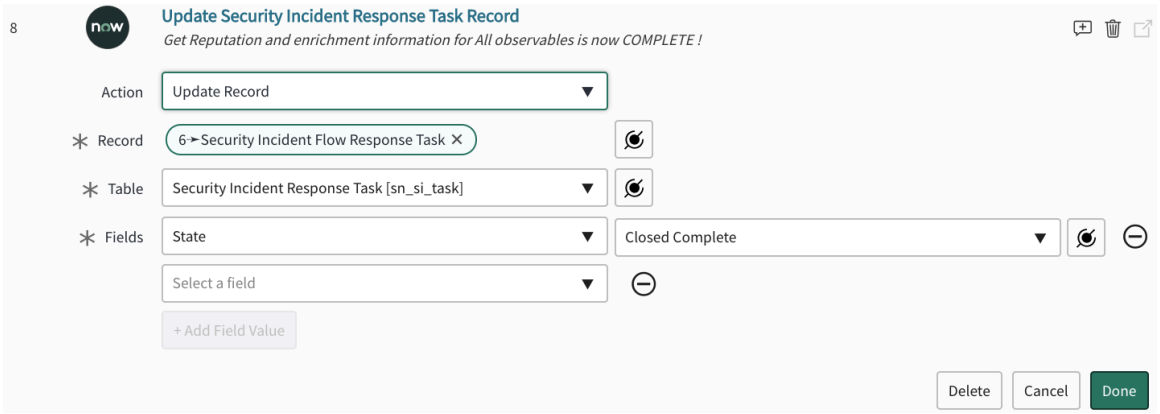
이 작업의 아이콘을 확인하십시오. 병렬 은 두 작업이 동시에 수행됨을 나타내고 하위 수행 중인 작업이 아래와 같이 하위 플로우임을 나타냅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

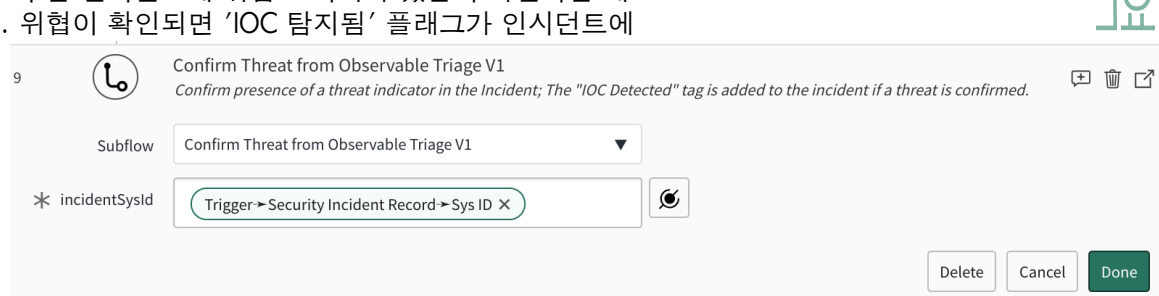


옵저버블 필드에 숫자 5가 표시됩니다. 이는 위협 조회가 5단계에서 검색된 옵저버블에서 실행됨을 나타냅니다. 그런 다음 이 하위 플로우는 하위 플로우 디자이너에 표시된 대로 기존 워크플로우와 작업을 호출합니다.

12. 8단계에서는 하위 플로우가 완료된 후 응답 작업이 종결됨으로 표시됩니다.

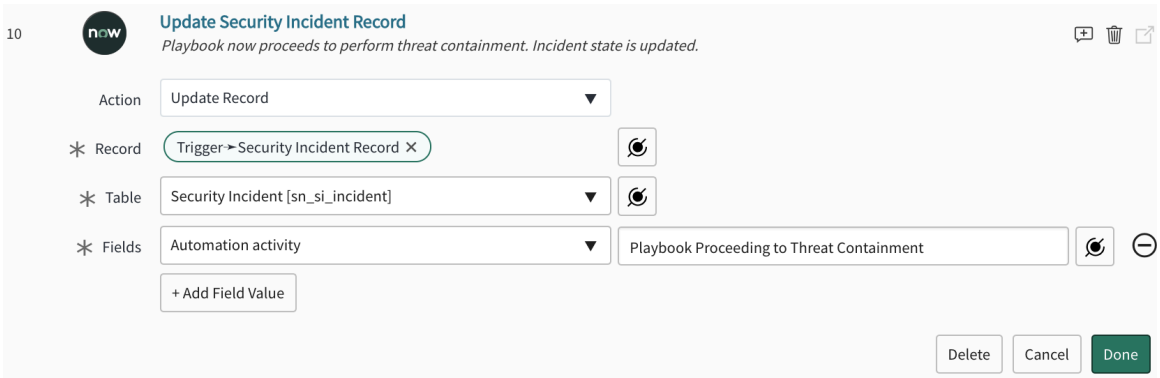


13. 9단계에서는 옵저버블 환자 분류 하위 플로우에서 위협 확인이 호출됩니다. 이 하위 플로우는 인시던트에 위협 표시기가 있는지 확인하는 데 사용됩니다. 위협이 확인되면 'IOC 탐지됨' 플래그가 인시던트에



추가됩니다.

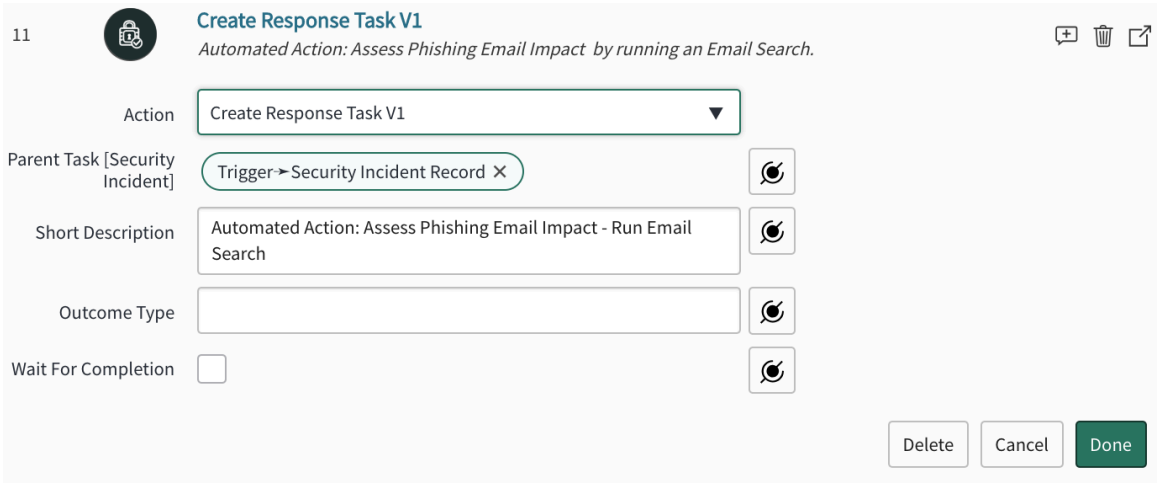
14. 위협이 확인되면 10단계에서 보안 인시던트를 업데이트하고 위협 억제 작업이 시작됨을 나타내는 메모를 추가합니다.



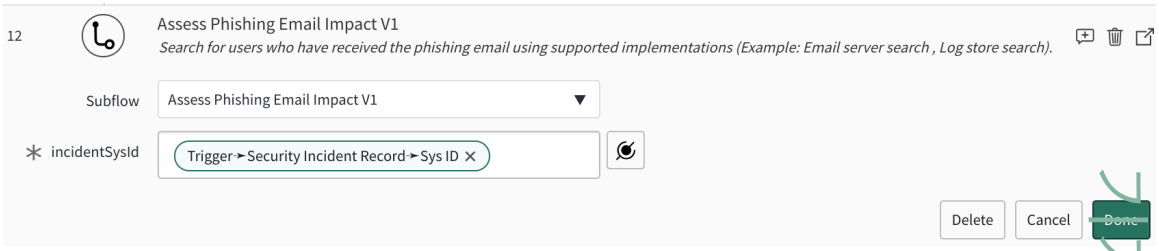
기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

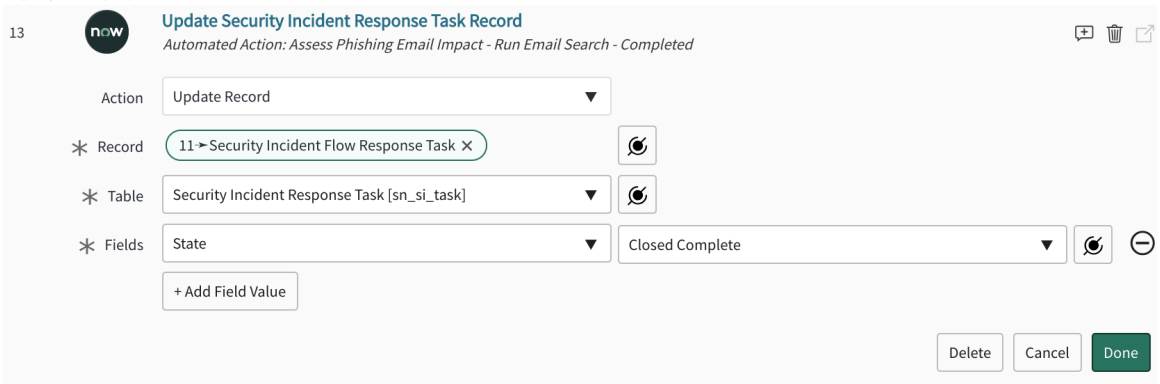
15. 11단계는 피싱 이메일의 영향을 평가하는 데 사용되는 작업의 시작 및 완료를 캡처하는 자동화된 응답 작업입니다.



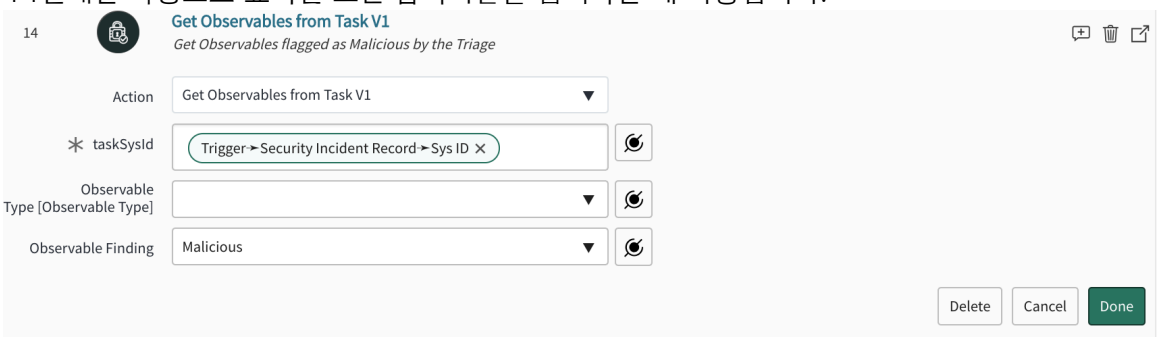
16. 12단계에서는 피싱 이메일 영향 평가 하위 플로우가 호출됩니다.
이 하위 플로우는 지원되는 구현을 사용하여 피싱 이메일을 받은 사용자를 검색하는 데 사용됩니다.



17. 13단계에서는 작업이 종결됨으로 표시되어 피싱 이메일 영향 평가 하위 플로우가 실행되었음을 나타냅니다.

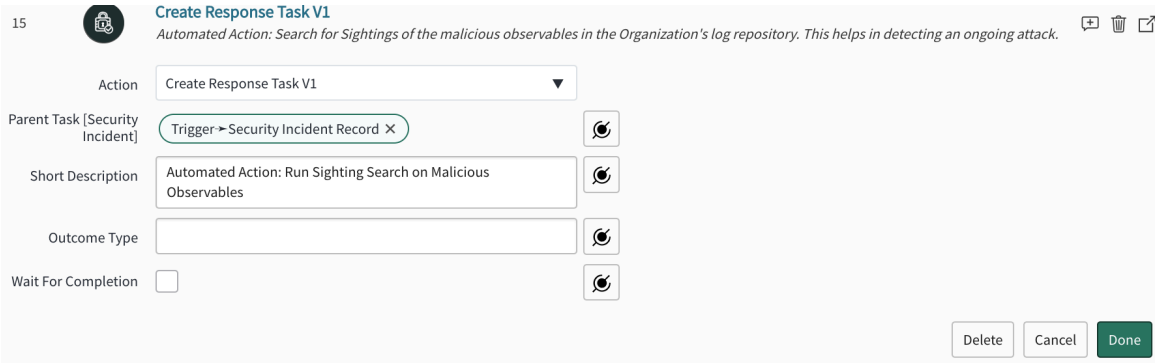


18. 14단계는 악성으로 표시된 모든 옵저버블을 검색하는 데 사용됩니다.

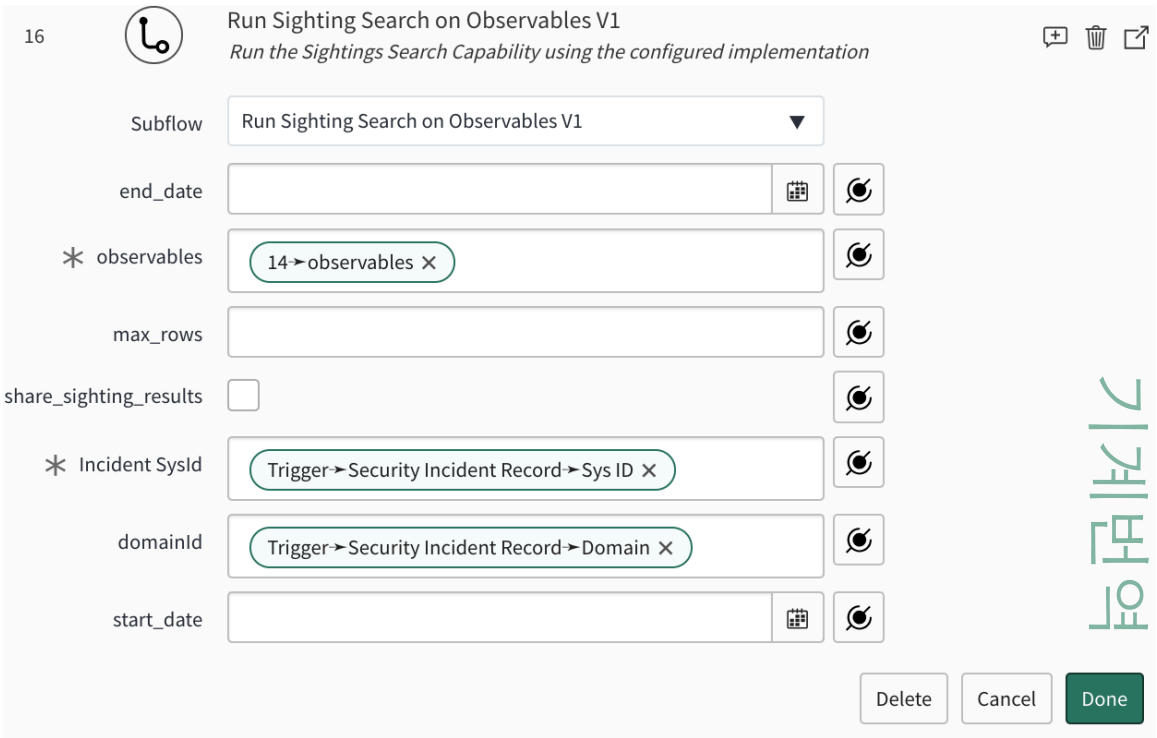


19. 15단계는 옵저버블 사이팅 검색 작업의 시작 및 완료를 캡처하는 자동화된 응답 작업입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

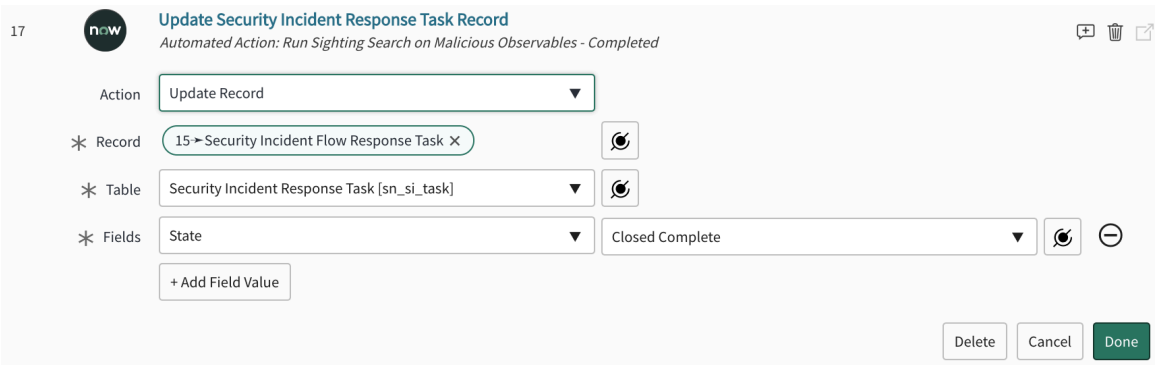


20. 16단계에서는 옵저버블에 대한 사이팅 검색 실행 하위 플로우가 호출됩니다. 이 하위 플로우는 구성된 구현을 사용하여 사이팅 검색을



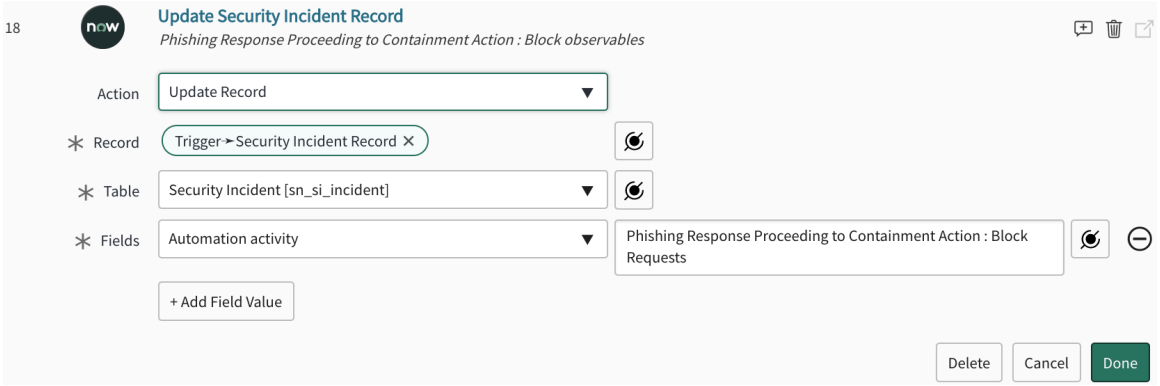
수행합니다.

21. 17단계에서는 옵저버블에 대한 사이팅 검색 실행 하위 플로우가 완료되었음을 나타내기 위해 작업이 종결됨으로 표시됩니다.

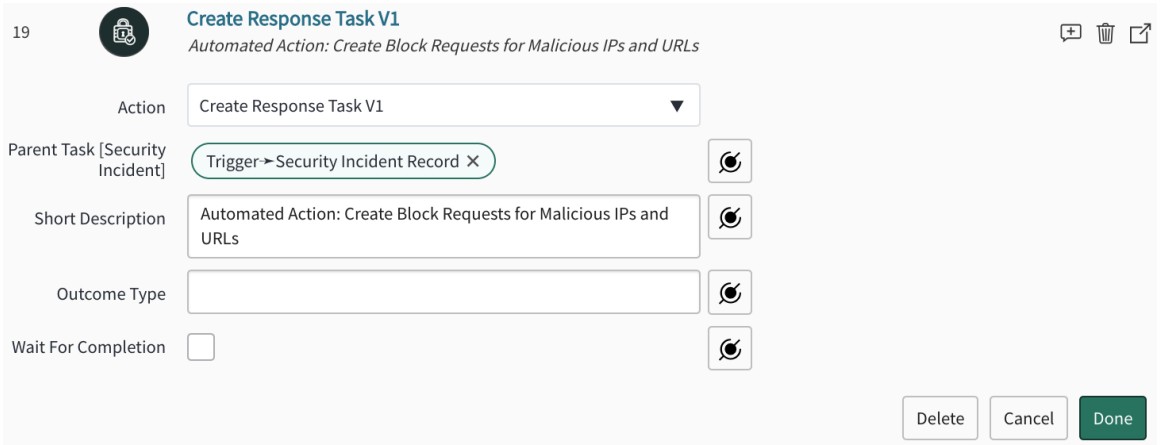


22. 악의적인 옵저버블을 식별한 후 18단계에서 보안 인시던트 기록을 업데이트하여 방지 작업이 이제 시작됨을 나타냅니다.

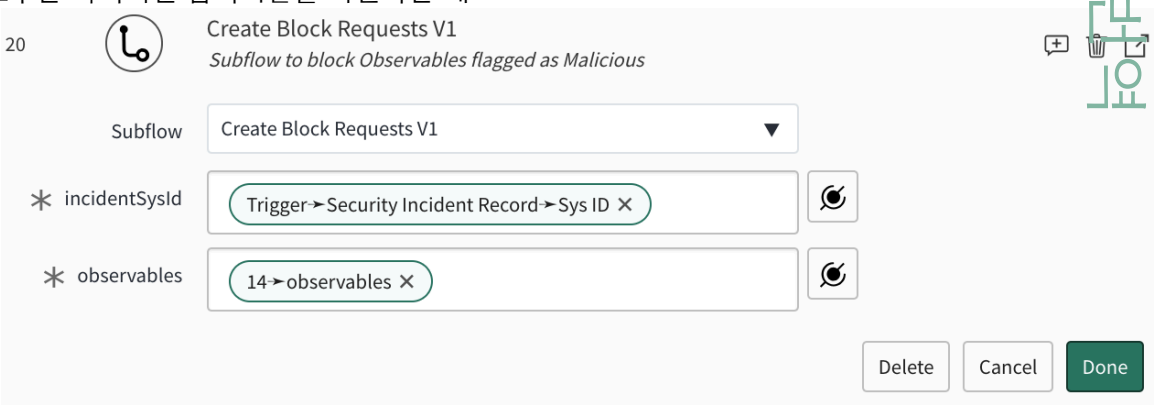
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



23. 19단계는 차단 요청 작업의 시작 및 완료를 캡처하는 자동화된 응답 작업입니다.

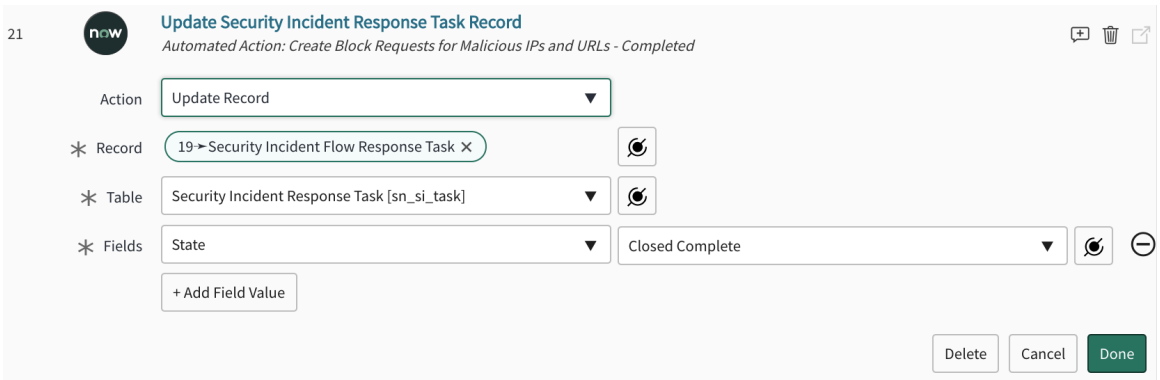


24. 20단계에서는 블록 요청 생성 하위 플로우가 호출됩니다.
이 하위 플로우는 악의적인 옵저버블을 차단하는 데



사용됩니다.

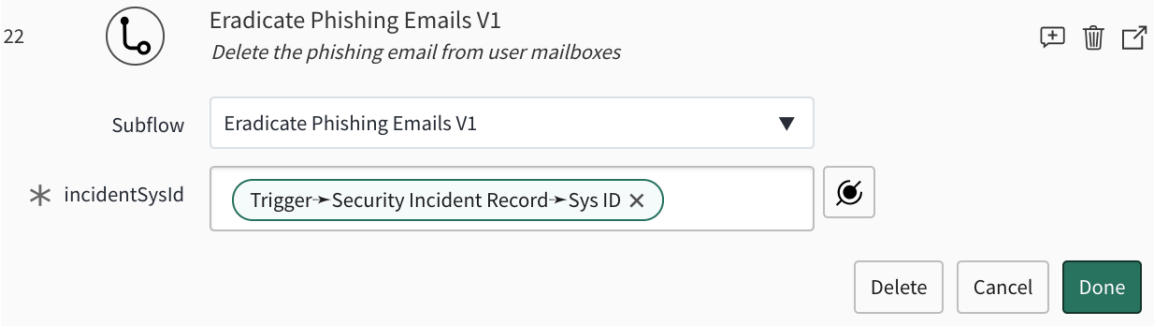
25. 21단계에서는 작업이 종결됨으로 표시되어 블록 요청 하위 플로우 생성이 완료되었음을 나타냅니다.



26. 22단계에서는 피싱 이메일 근절 하위 플로우가 호출됩니다.

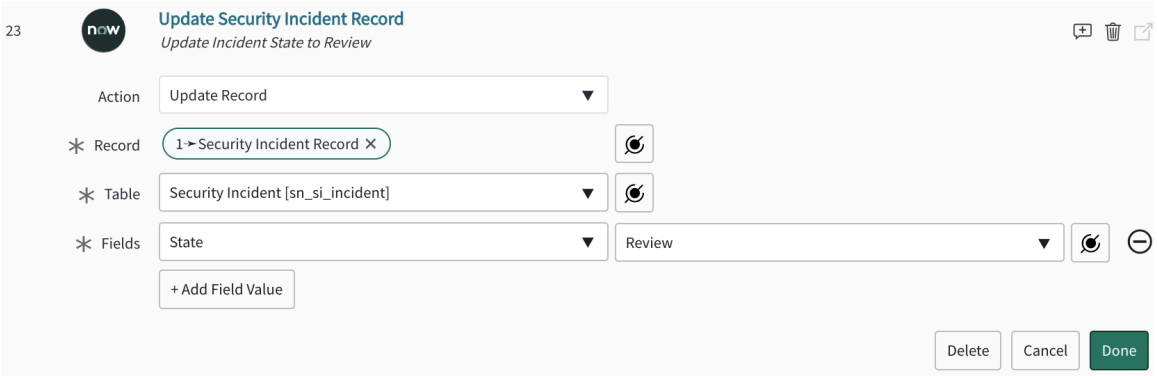
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 하위 플로우는 사용자 사서함에서 피싱 이메일을 삭제하는 데

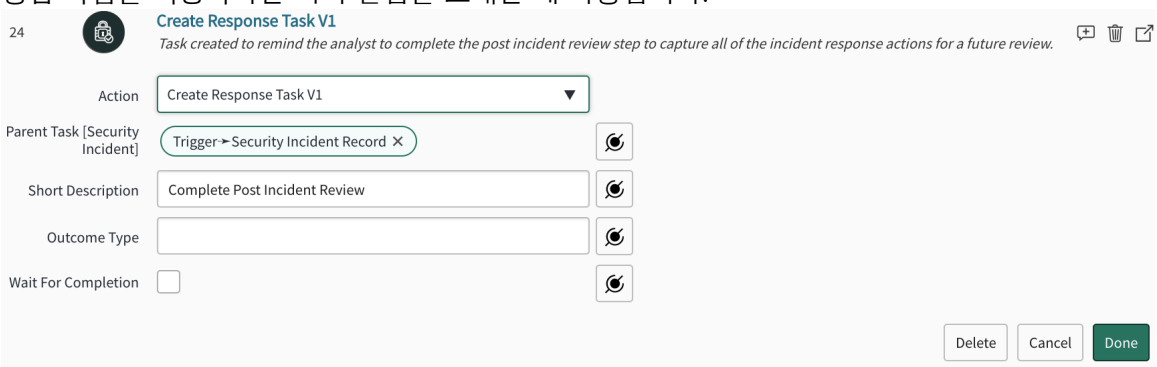


사용됩니다.

27. 피싱 이메일이 삭제된 후 23단계에서 보안 인시던트 기록을 업데이트하여 인시던트 상태를 검토해야 함을 나타냅니다.



28. 마지막 단계에서 플로우는 자동화된 응답 작업을 생성합니다. 이 작업은 보안 분석가에게 향후 검토를 위해 모든 인시던트 응답 작업을 저장하라는 미리 알림을 보내는 데 사용됩니다.

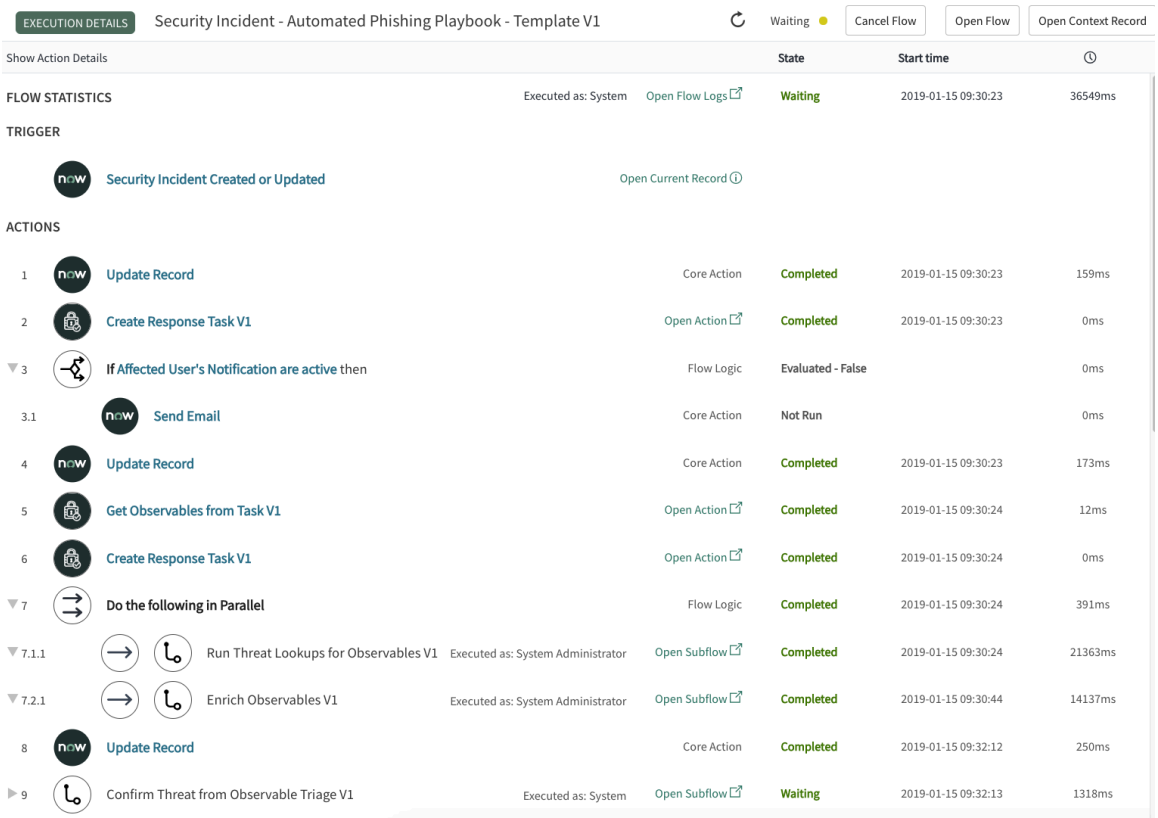


다음에 수행할 작업

게시하기 전에 테스트를 클릭하여 플로우의 작업을 시뮬레이션할 수 있습니다. 플로우를 테스트한 후 활성화 를 클릭하여 플로우를 활성화하고 실행합니다.

실행을 클릭하여 플로우의 실행 세부 정보를 봅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



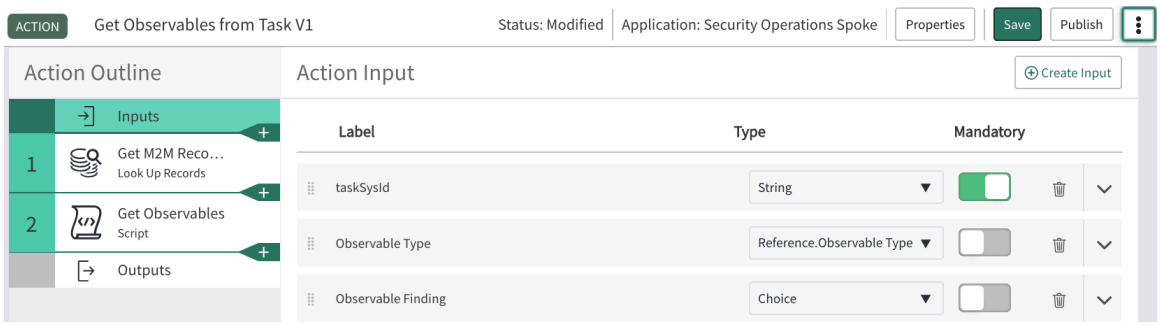
자동화된 피싱 응답 플레이북 플로우 작업 디자이너 보기

작업 디자이너로 드릴다운하여 자동화된 피싱 응답 플레이북 플로우의 특정 단계에 대해 수행 중인 작업에 대한 자세한 정보를 볼 수 있습니다.

이 페이지에서는 작업에서 옵저버블 가져오기 단계의 작업 디자이너 페이지에 대해 설명합니다. 상세 정보를 보려면 작업 개요 패널에서 작업을 선택합니다.

작업 입력

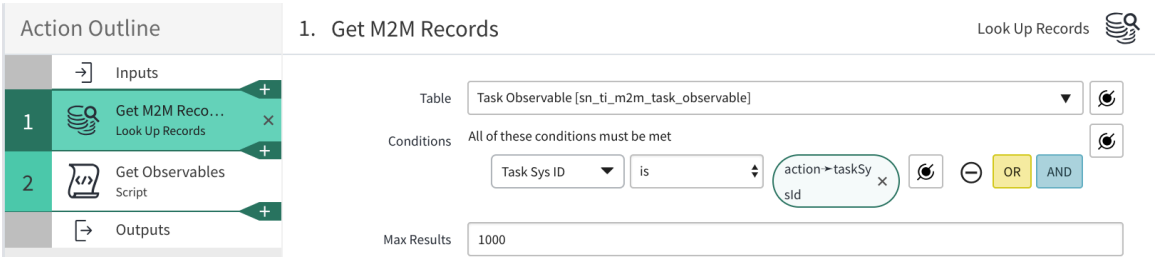
이 섹션에는 인시던트 ID, 옵저버블 유형(해시 또는 IP) 및 옵저버블 찾기(악성 이메일만 해당)를 포함하여 작업이 생성된 방법에 대한 상세 정보가 표시됩니다.



M2M 기록 가져오기

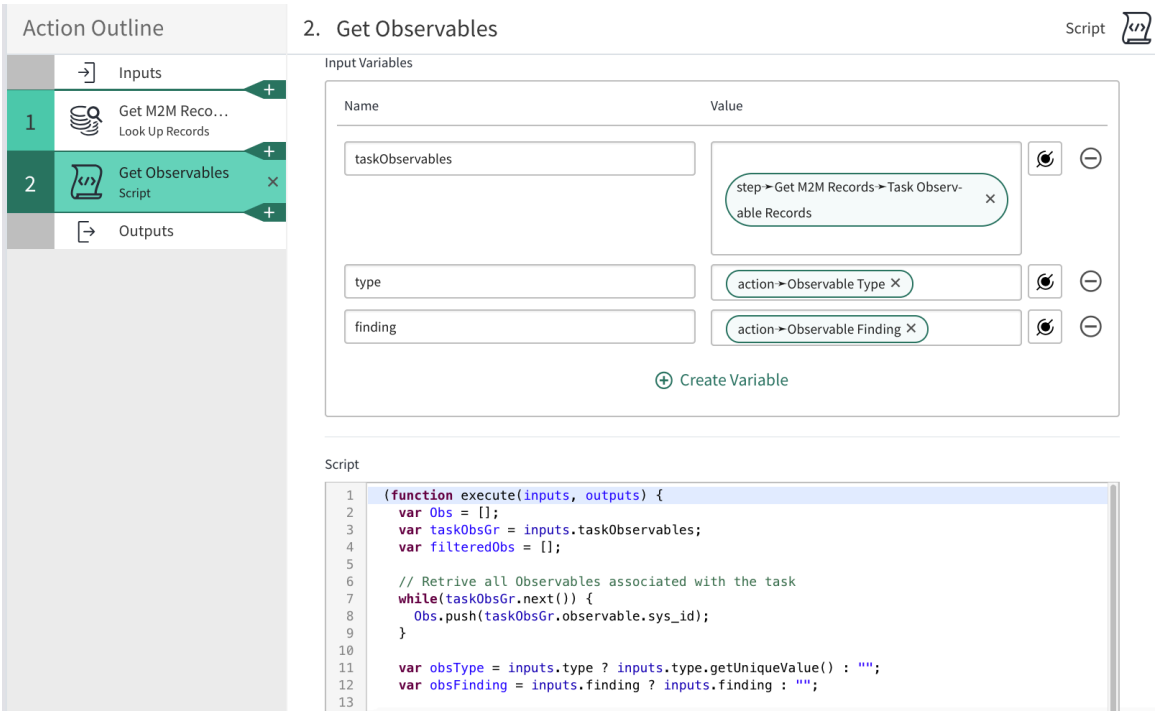
이 섹션에서는 지정된 테이블에서 옵저버블을 검색하기 위해 정의된 조건을 보여줍니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



옵저버블 가져오기

이 섹션에서는 지정된 필터 조건에 따라 옵저버블을 검색하는 데 사용되는 스크립트를 보여줍니다. 마지막으로 이 기준을 충족하는 옵저버블과 개수가 표시됩니다.



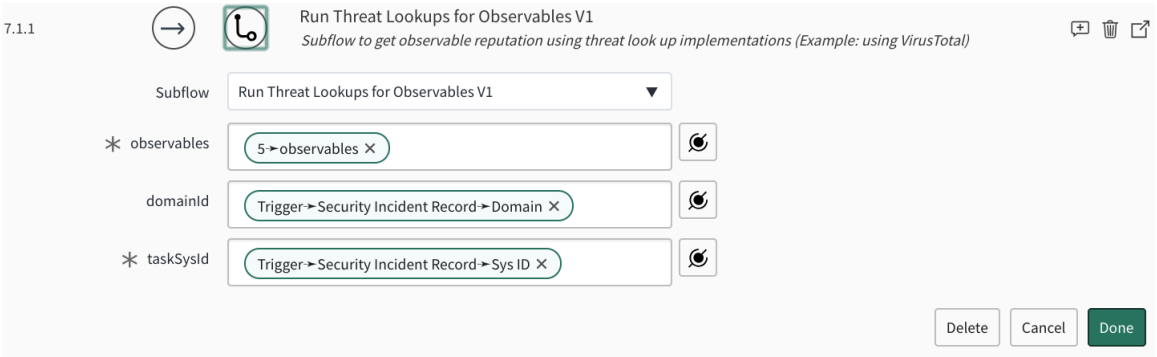
주:
이 플로우에 정의된 모든 작업은 다시 사용할 수 있으며 요구 사항에 따라 수정할 수 있습니다.

자동화된 피싱 응답 플레이북 보기 하위 플로우 디자이너

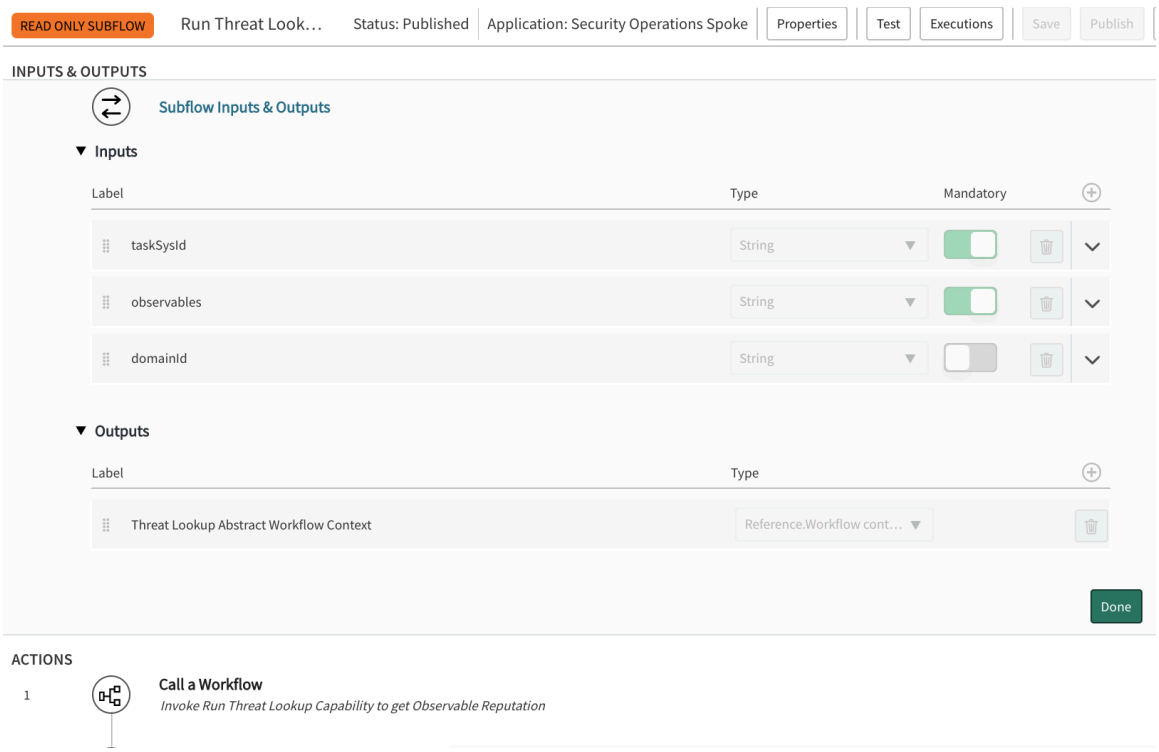
하위 플로우 디자이너로 드릴다운하면 자동화된 피싱 응답 플레이북 플로우의 일부로 실행되고 있는 하위 플로우에 대한 자세한 정보를 볼 수 있습니다.

하위 플로우 디자이너를 시작하여 하위 플로우의 추가 상세 정보를 볼 수 있습니다. 옵저버블에 대한 위협 조회 실행 하위 플로우에 대한 하위 플로우 디자이너 페이지가 여기에 표시됩니다. 하위 플로우 디자이너를 보려면 아래 이미지에서 아이콘을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



하위 플로우 디자이너 페이지에서 이 하위 플로우에 대한 입력과 출력 및 실행 중인 기본 워크플로우 작업을 볼 수 있습니다.



주:
이 하위 플로우는 읽기 전용이며 편집할 수 없습니다. 단계에 하위 플로우를 추가하거나 삭제할 수 있지만 하위 플로우를 수정할 수는 없습니다.

자동화된 맬웨어에 대한 플레이북

자동화된 맬웨어 플레이북은 맬웨어 경고를 빠르고 효율적으로 해결하는 데 도움이 되는 일련의 자동화된 단계를 제공합니다.

맬웨어 플레이북 플로우를 사용하여 엔드포인트 또는 네트워크에서 맬웨어 경고를 처리하는 단계를 자동화합니다. 플로우 템플릿에는 트리거 조건, 작업 시퀀스 및 가독성을 위해 주석이 달린 하위 플로우가 포함되어 있습니다.

이러한 템플릿에는 피싱 공격에 대응하도록 설계된 재사용 가능한 작업 시퀀스가 포함되어 있습니다. 각 플로우에는 트리거(조건), 작업 시퀀스 및 가독성을 위해 주석이 달린 하위 플로우가 있습니다. 이러한 플로우에 액세스하려면 에서 ServiceNow StoreSecurity Operations 스포크 및 Security Operations Palo Alto Networks - WildFire 앱을 설치해야 합니다.

주:
이러한 템플릿을 사용하려면 먼저 활성화해야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음 플로우 및 하위 플로우가 포함됩니다.

- 보안 인시던트 - 자동화된 맬웨어 플레이북 템플릿: 이 템플릿은 맬웨어 경고에 대한 응답을 자동화하도록 설계되었으며 트리거를 포함한 일련의 작업을 포함합니다.
- 보안 인시던트 - 맬웨어 수동 템플릿: 이 템플릿은 범주가 악성 코드 활동으로 설정될 때 활성화되는 기존 수동 맬웨어 응답 워크플로우입니다.

하위 플로우

- 옵저버블에서 위협 확인: 옵저버블이 악성이고 해결해야 하는지 확인합니다.
- 인시던트 심각도 설정: 인시던트의 심각도 상태를 설정합니다.
- 랜섬웨어 플레이북: 랜섬웨어 공격인지 여부를 결정합니다.

이러한 하위 플로우는 여러 플레이북에서 사용할 수 있는 재사용 가능한 작업 세트를 나타냅니다. 이러한 하위 플로우를 사용하여 요구 사항에 따라 사용자 지정 템플릿(플로우)을 정의할 수 있습니다.

사용자 지정 템플릿(플로우)을 생성하려면 플로우의 지침을 따릅니다.

자동화된 맬웨어 플레이북 플로우 실행

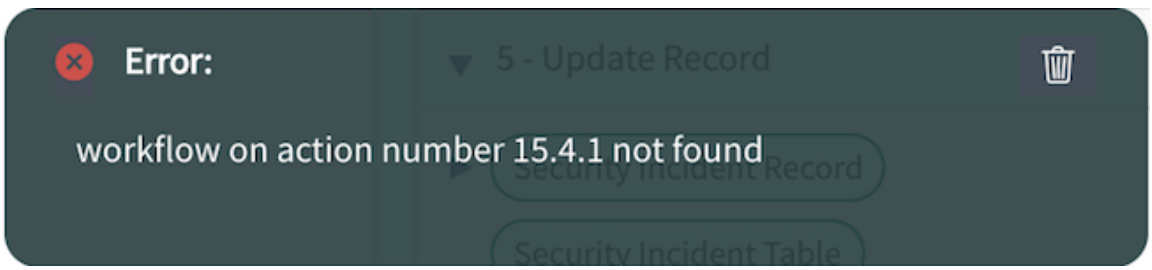
이 플로우를 사용하여 Playbook의 작업을 자동화하여 조직에 대한 맬웨어 공격을 분석하고 해결합니다.

시작하기 전에

- 필요한 역할: sn_si.admin, flow_designer, action_designer
- 올바른 자격 증명을 사용하여 다음 통합을 설치하고 구성합니다.
  - Security Operations를 위한 Palo Alto Networks WildFire
  - 사이팅 검색(Splunk)
  - 요청 차단
  - 위협 조회
  - 옵저버블 보강

  보안 인시던트 - 자동화된 맬웨어 플레이북 템플릿을 활성화 하기 전에 이러한 통합이 제대로 작동하는지 확인합니다.

- Security Operations Palo Alto Networks Wildfire 앱: 자동화된 맬웨어 플레이북 플로우에 액세스하려면 에서 ServiceNow StoreSecurity Operations Spoke 및 Security Operations Palo Alto Networks - WildFire 앱을 설치해야 합니다. Security Operations Palo Alto Networks Wildfire App이 설치되어 있지 않으면 아래와 같이 "작업 번호 15.4.1의 워크플로우를 찾을 수 없습니다"라는 오류가 표시됩니다.



  이 앱을 설치하지 않으려면 자동화된 맬웨어 플레이북 플로우에서 **15.2, 15.3** 및 **15.4** 단계를 삭제합니다.

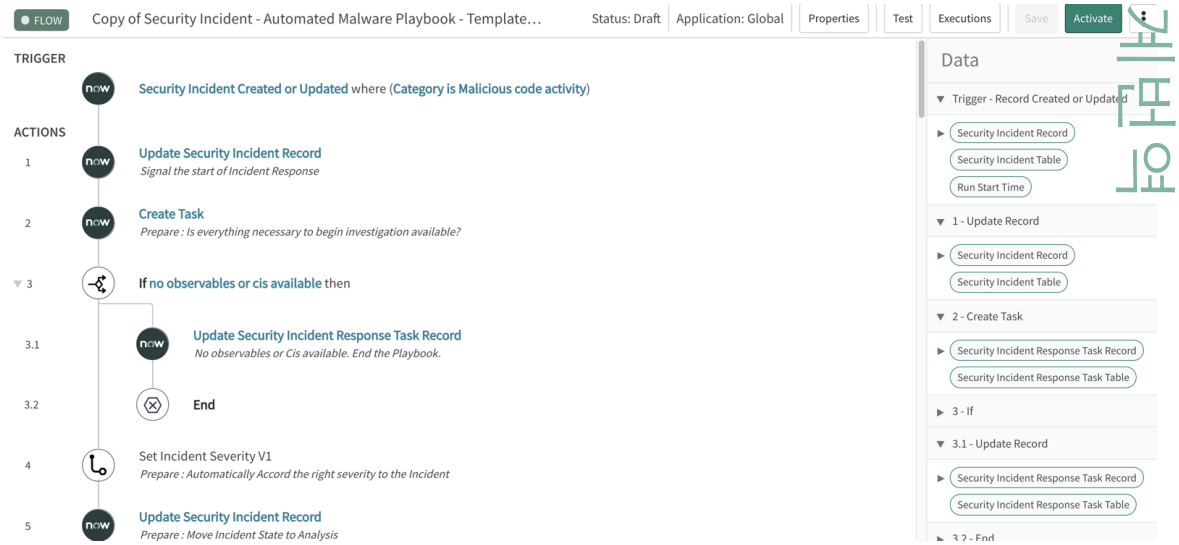
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 다음 조건이 충족되었는지 확인합니다.
  - 보안 인시던트가 적절한 승인 그룹에 속한 보안 분석가에게 할당되었습니다.
  - 인시던트를 처리하는 보안 분석가에게는 유효한 이메일 주소가 있어야 합니다.
  - 필요한 구성 항목과 옵저버블이 보안 인시던트에 추가되었습니다.
- 21단계(승인 요청)에서는 그룹을 보안 인시던트 할당에서 기본 그룹으로 변경합니다.
- 플로우의 21단계는 승인 요청이 관리자에게 전송되는 필수 작업 승인 단계입니다. 요청을 승인하려면 관리자가 작업 승인 페이지로 이동하여 상태 필드를 승인됨으로 설정해야 합니다. 작업이 승인되지 않으면 Flow Designer가 더 이상 진행할 수 없으며 프로세스가 종료됩니다.

이 태스크 정보
네트워크에서 악성 코드 활동이 탐지되면 보안 인시던트가 생성되고 자동화된 멀웨어 플레이북 플로우가 시작됩니다. 자동화된 맬웨어 플레이북 플로우에 정의된 작업을 사용하여 위협을 분류, 분석, 억제 및 근절할 수 있습니다.

프로시저

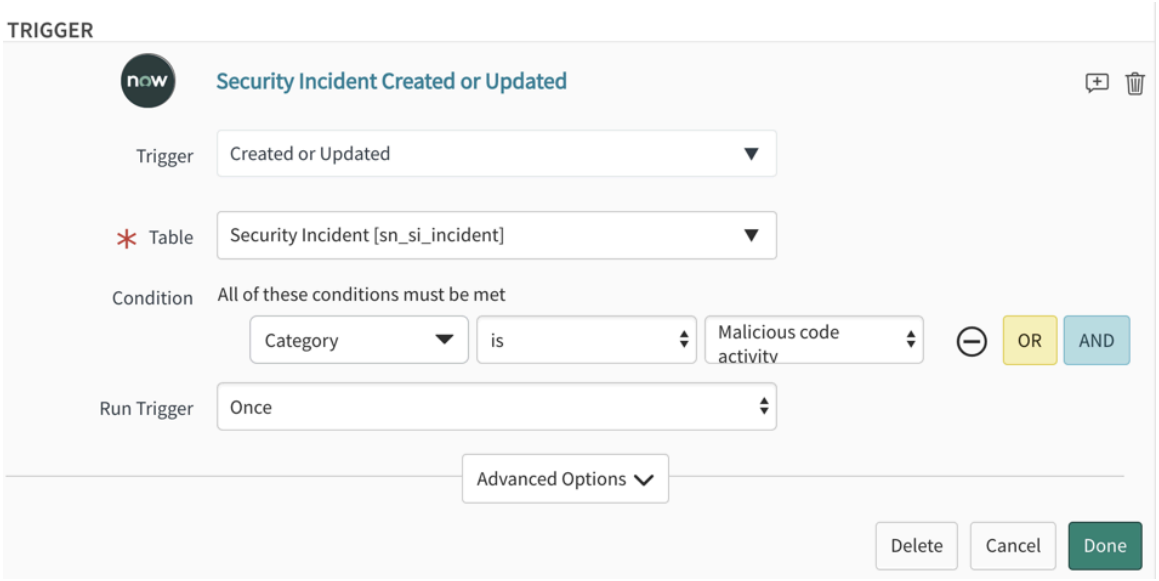
1. 다음으로 이동 모두 〉 플로우 디자이너 〉 디자이너 보안 운영 스포크에서 사용할 수 있는 플로우를 보려면
2. 보안 인시던트 - 자동화된 맬웨어 플레이북 템플릿 **VI** 링크를 클릭합니다.
3. 플로우 페이지에서 더 보기 아이콘 ⋮ 을 클릭하고 플로우의 사본을 만들고 사용할 수 있도록 엽니다.
   이제 트리거 조건 또는 작업을 수정하거나 작업을 추가 및 제거하는 등 플로우를 변경할 수 있습니다.



   이는 트리거와 플로우로 실행될 단계를 보여줍니다. 오른쪽 패널은 데이터 흐름을 보여줍니다. 아이콘을 클릭하여 단계를 확장하고 세부 정보를 봅니다.
4. 트리거 아이콘을 클릭합니다.

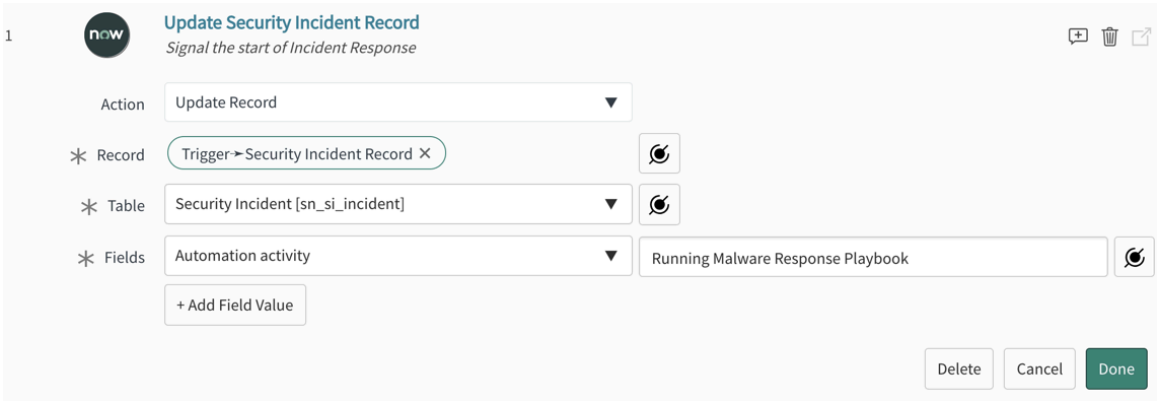
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

첫 번째 단계에서는 플로우에 대한 트리거를 정의하거나 설정합니다. 조건이 충족될 때 수행할 트리거 및 작업의 조건을 지정합니다.



플로우에 정의된 조건(범주는 악성 코드 활동)이 인시던트 기록에서 충족되면 자동화된 피싱 플로우의 작업이 순차적으로 실행되기 시작합니다. 트리거를 수정하고, 주석을 추가하고, 조건을 추가 또는 삭제하는 등의 작업을 수행할 수 있습니다.

5. 플로우의 첫 번째 단계는 보안 인시던트 기록 업데이트입니다.

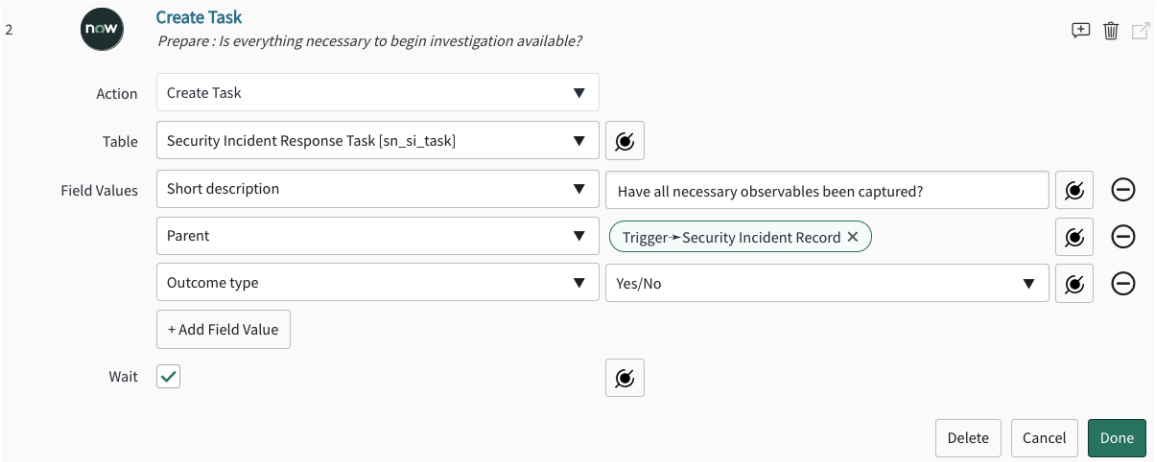


링크를 클릭하고 주석 아이콘 클릭하여 보안 분석가에게 악성 코드 활동이 있었고 자동화된 맬웨어 대응 Playbook 플로우가 실행되기 시작했음을 나타내는 메모를 추가합니다.

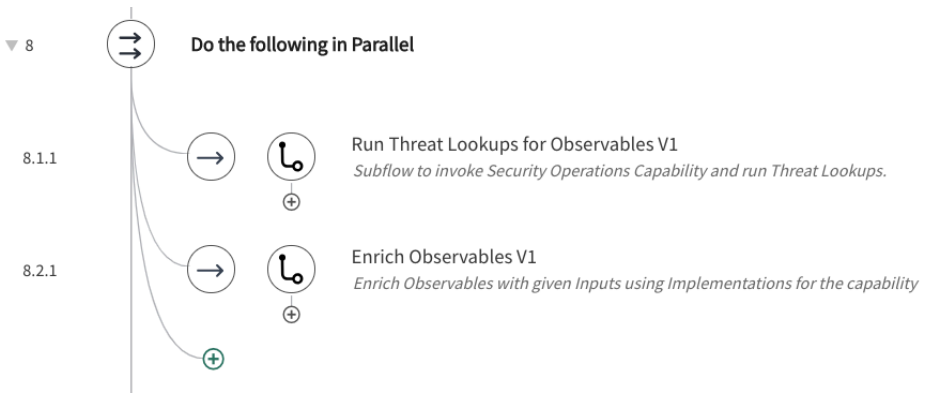
6. 플로우의 2단계를 계속 진행하고 작업 생성 링크를 클릭합니다.

이 단계에서는 필요한 모든 옵저버블이 캡처되었는지, 조사를 시작할 수 있는지 확인하기 위해 자동 응답 작업이 생성됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

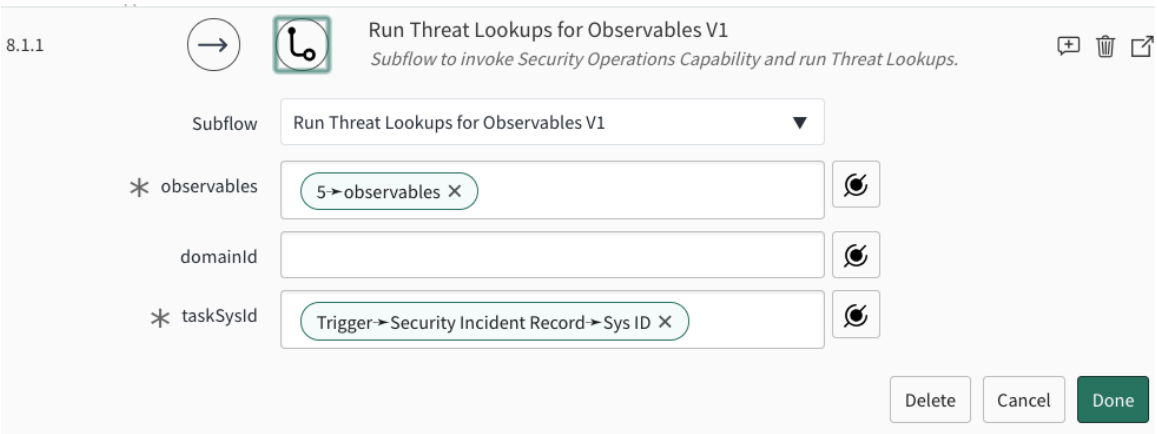


7. 결과 유형이 아니요이면 조사를 시작하는 데 사용할 수 있는 옵저버블과 CI가 없음을 나타냅니다. Playbook을 더 이상 진행할 수 없음을 나타내도록 보안 인시던트 기록을 업데이트합니다.
8. 결과 유형이 예인 경우 인시던트 심각도 설정 하위 플로우가 보안 인시던트에 올바른 심각도를 자동으로 할당합니다.
9. 다음 단계에서는 보안 인시던트 기록이 업데이트됩니다.
10. 다음 단계에서는 인시던트 또는 선택한 범주와 관련된 모든 옵저버블을 수집하여 후속 플레이북 단계에서 추가 자동화 작업을 수행합니다.
11. 다음 단계에서는 자동 응답 작업이 생성됩니다.
    이 작업은 모든 옵저버블의 평판을 얻고 구성된 통합으로 보강을 수행하는 프로세스의 시작을 캡처합니다.
12. 8단계에서는 두 개의 하위 플로우가 호출됩니다.
    - 옵저버블에 대한 위협 조회 실행: 이 하위 플로우는 위협 조회 구현을 사용하여 모든 옵저버블의 평판을 가져오는 데 사용됩니다.
    - 옵저버블 보강: 이 하위 플로우는 구성된 구현으로 옵저버블을 보강하는 데 사용됩니다.



이 작업의 아이콘을 확인하십시오. 병렬 은 두 작업이 동시에 수행됨을 나타내고 하위 수행 중인 작업이 아래와 같이 하위 플로우임을 나타냅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



옵저버블 필드에 숫자 5가 표시됩니다. 이는 위협 조회가 5단계에서 검색된 옵저버블에서 실행됨을 나타냅니다. 이 하위 플로우는 기존 워크플로우와 작업을 호출합니다.

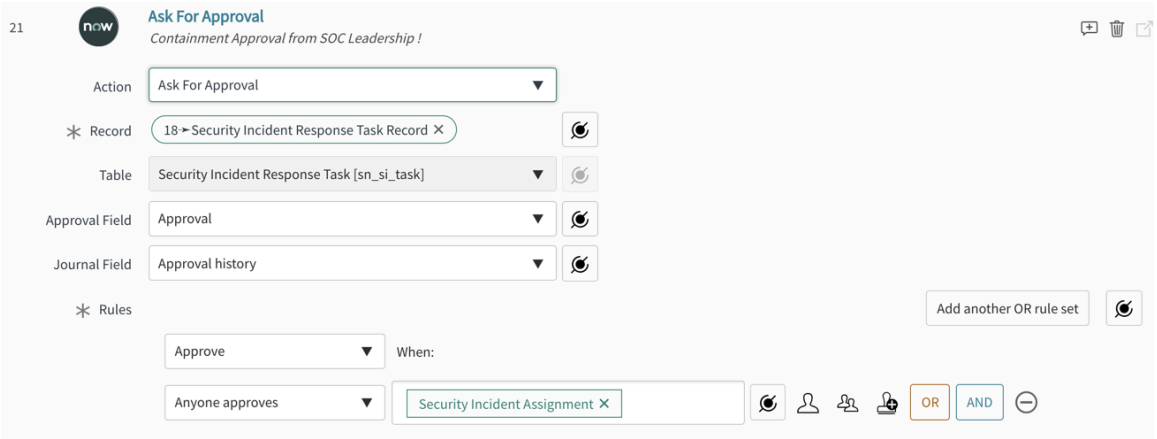
13. 다음 단계에서는 기록 조회 실행 작업이 실행됩니다.
이 작업은 상위 워크플로우가 다음 중 하나일 수 있는 워크플로우 컨텍스트 기록을 조회하는 데 사용됩니다.
    - 위협 조회 추상 워크플로우 컨텍스트
    - 옵저버블 보강 추상 워크플로우 컨텍스트
14. 다음 단계에서는 기록 8개마다 평판 및 보강 결과를 검토합니다.
15. 다음 단계를 계속 검토합니다.
    a. 보안 인시던트 기록 업데이트: 평판 조회 및 보강 활동이 완료되었음을 나타내도록 보안 인시던트 기록을 업데이트합니다.
    b. 작업에서 옵저버블 가져오기: 보안 인시던트와 관련된 모든 악성 옵저버블을 검색합니다.
    c. 작업 생성: 자동화된 분류 실행이 성공했는지 확인하고 확인합니다.
16. 악성으로 플래그가 지정된 옵저버블이 있는 경우:
    a. 보안 인시던트 기록 업데이트: 위협이 탐지되었음을 나타내는 작업 메모를 게시합니다.
    b. 옵저버블에서 입력 쿼리 작성: 10개 이상의 옵저버블에 악성으로 플래그가 지정된 경우 옵저버블에 대한 사이팅 검색 하위 플로우(Splunk 또는 Carbon Black)가 실행됩니다.
17. 옵저버블에 악성으로 플래그가 지정되지 않은 경우 플로우는 다음 단계로 계속됩니다.
    a. 보안 인시던트 기록 업데이트: 위협이 탐지되지 않았음을 나타내는 작업 메모를 게시합니다.
    b. 작업에서 옵저버블 가져오기: 인시던트에서 모든 SHA256 해시 ID를 식별합니다.
    c. 옵저버블 기록 조회: 이 기준을 충족하는 기록을 조회합니다.
18. 다음 단계를 계속 검토합니다.
    a. 각 악성 옵저버블에 대해 **Security Operations Palo Alto Networks - Get Wildfire Data Enrichment** 워크플로우가 실행됩니다.
    b. 조사 결과를 검토하여 만족스러운지 확인합니다.
의심되는 맬웨어가 랜섬웨어 공격인지 확인하기 위한 응답 작업이 생성됩니다. 그렇다면 랜섬웨어 플레이북 하위 플로우가 실행됩니다.
    c. 다음 단계에서는 분석 요약이 포함된 이메일을 전송하고 격리 절차를 시작하기 위한 승인을 요청합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

d. 요청된 승인의 상세 정보를 캡처하기 위한 작업이 생성됩니다.

e. 다음 단계는 보안 인시던트 기록을 업데이트하는 것입니다.
보안 분석가에게 승인 요청이 완료되었음을 알리는 작업 메모를 게시합니다.

f. SOC 관리자의 맬웨어 공격을 포함하기 위한 승인을 요청합니다.



주:
플로우에서 승인 요청이 생성되면 작업 메모가 다음 메시지로 업데이트됩니다.

##<## ID)>## ## ## ### #######. 이 작업을 승인하려면 SOC 관리자로서 다음 단계를 수동으로 수행합니다.

- 작업 승인 페이지로 이동합니다.
- 승인 목록이 표시됩니다. 승인할 〈작업 ID〉를 클릭합니다.
- 상태를 승인 으로 변경하고 업데이트된 〈작업 ID〉를 저장합니다.

g. 다음 단계에서는 승인 상태를 추적하기 위해 보안 인시던트 기록이 업데이트됩니다.

h. 다음으로 격리 절차를 시작하는 작업이 생성됩니다.

i. 악의적인 옵저버블에 대한 블록 요청 생성 실행 하위 플로우가 실행되고, 감염된 장치와 해당 자산을 다시 빌드하라는 요청이 포함된 인시던트 기록이 생성됩니다.

j. 다음으로 사이팅 검색을 실행하여 환경이 안전한지 확인하는 작업이 생성됩니다.
목격 검색은 목격을 찾을 수 없을 때까지 반복됩니다.

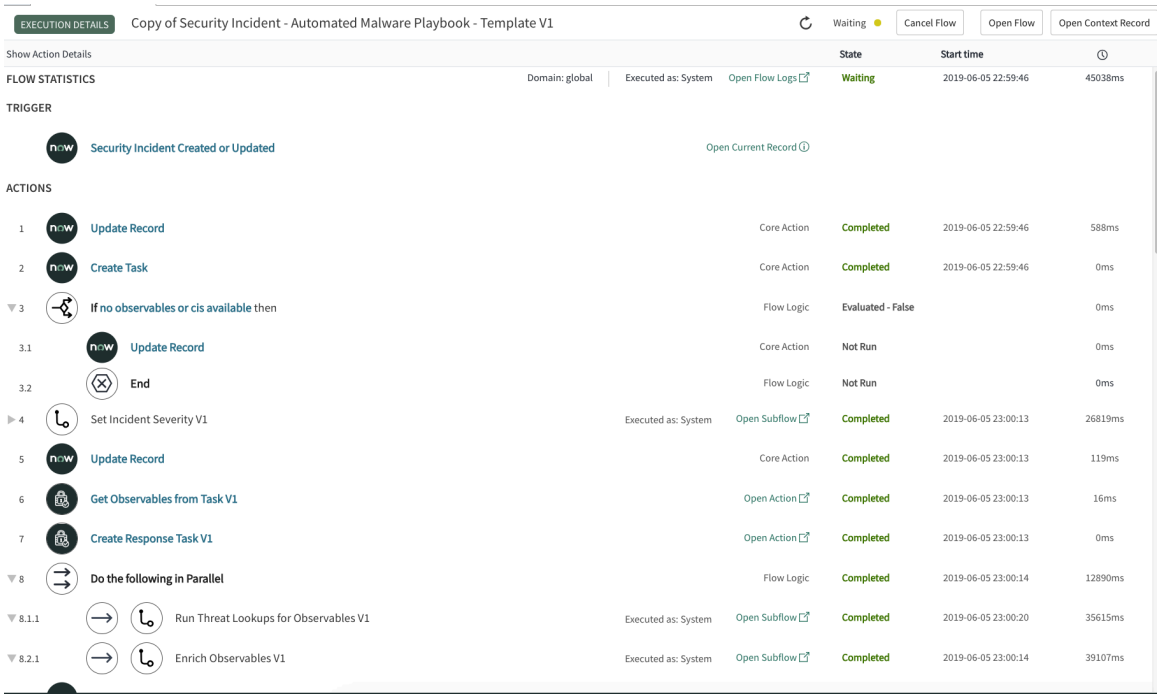
k. 다음으로 보안 인시던트 기록을 검토할 준비가 되었음을 나타내는 작업이 생성됩니다.

l. 마지막으로 기록이 업데이트되고 검토 단계로 이동됩니다.

다음에 수행할 작업
테스트를 클릭하여 플로우의 작업을 게시하기 전에 시뮬레이션할 수 있습니다. 플로우를 테스트한 후 활성화 를 클릭하여 플로우를 활성화하면 실행됩니다.

실행을 클릭하여 플로우의 실행 세부 정보를 봅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



실패한 로그인에 대한 플레이북 수동

사용자가 SIM 구성에 따라 특정 로그인 시도를 실패하면 보안 인시던트가 생성됩니다.

이러한 실패한 로그인 시도는 가양성이거나 공격자가 사용자 이메일 계정에 대한 액세스 권한을 얻으려는 시도일 수 있습니다. 이러한 시나리오에서 실패한 로그인 수동 플레이북은 지침을 제공하고 실패한 로그인 보안 인시던트의 조사를 최적화하는 데 도움이 될 수 있습니다.

필수 구성요소

필요한 역할:

- sn_si.admin
- flow_designer

스포크: Security Operations 스포크 설치(sn_sec_spoke)

핵심 기능

실패한 로그인 플레이북은 보안 인시던트를 조사하기 위한 다음 역량을 다룹니다.

1. 영향을 받는 사용자가 활성/비활성 사용자인지 확인
2. 필터 허용 목록 옵저버블
3. 옵저버블 보강
4. 자동화된 위협 조회를 수행합니다.
5. 실패한 로그인 시도를 확인하기 위해 사용자에게 자동화된 이메일을 보냅니다.
6. 사용자 액세스를 조사하기 위해 분석가에게 작업을 할당합니다.
7. 악의적인 옵저버블을 식별하고 IP 및 URL을 차단합니다.
8. 사용자 암호를 재설정합니다.
9. 보안 인시던트 상태 업데이트
10. 사후 인시던트 검토를 처리할 보안 분석가에게 작업을 할당합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필요한 역량

- 위협 조회(바이러스 합계, 하이브리드 분석)
- 옵저버블 보강(Whois, ReverseWhois)
- 사이팅 검색(Splunk, QRadar)
- 옵저버블 차단(CheckPoint, Palo Alto)

자세한 내용은 ServiceNow Store 를 참조하십시오.

보안 분석가 경험

보안 위협을 단계별로 해결하는 방법을 이해하려면 을 참조하십시오 플레이북으로 보안 위협 해결.

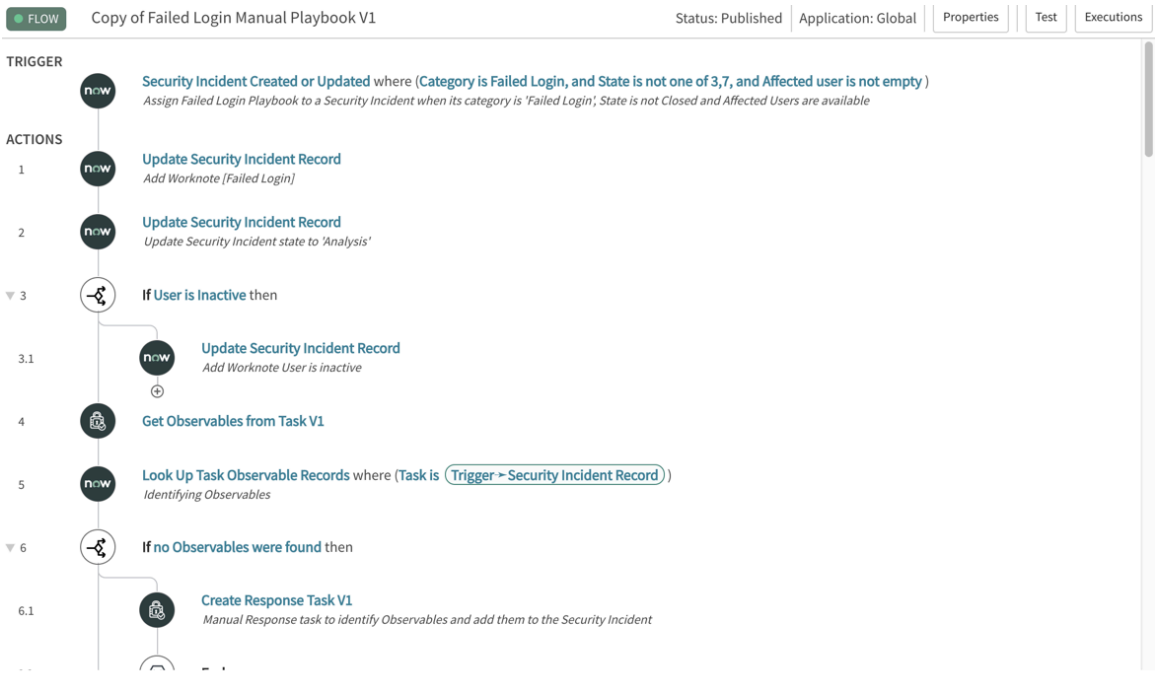
Flow Designer 기능과 함께 실패한 로그인 플레이북 사용

시작

1. sn_si.user 및 flow_designer 역할을 가진 사용자로 로그인합니다.
2. 다음으로 이동 플로우 디자이너 〉 디자이너 을 클릭하고 로그인 실패 플레이북을 클릭합니다.
3. 다음 플로우의 사본을 만들어 실패한 로그인 플레이북을 복사하고 필요에 따라 수정합니다. 이 단계는 선택 사항입니다. 플로우를 사용자 지정하거나 특정 변경을 수행하려는 경우에만 이 단계를 수행합니다.)
   - 실패한 로그인 수동 플레이북 V1
   - 로그인 실패 - 사용자의 회신 구문 분석 및 응답 업데이트 작업 V1
4. 요구 사항에 따라 필요한 수정을 수행합니다. 이 단계는 선택 사항입니다. 플로우를 사용자 지정하거나 특정 변경을 수행하려는 경우에만 이 단계를 수행합니다.)
5. 플레이북을 활성화합니다.
   - 기본 시스템에서 사용할 수 있는 플레이북을 사용하려면 메인 플로우를 활성화합니다.
   - 요구 사항에 따라 수정한 후 복사된 플로우를 활성화합니다.

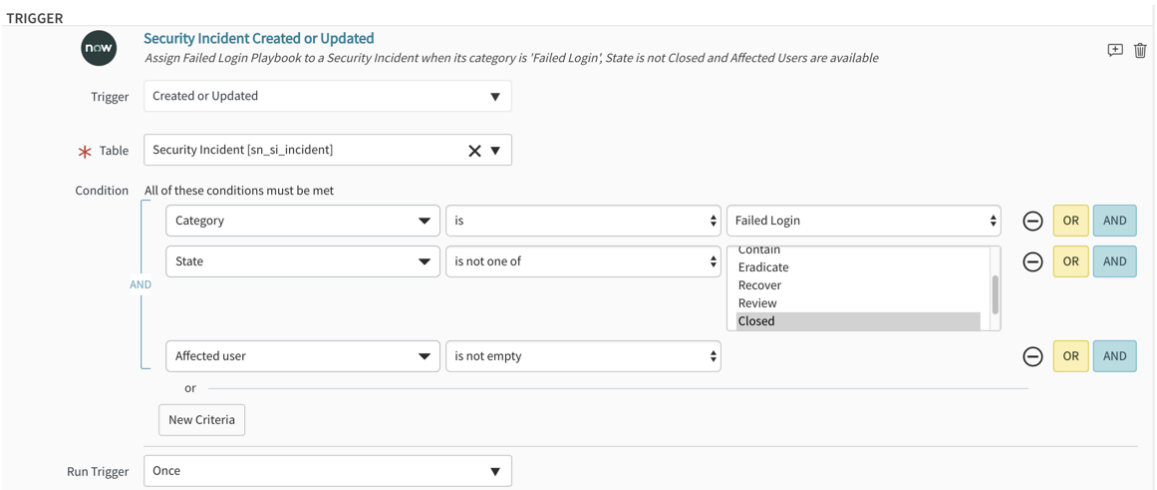
다음 이미지는 실패한 로그인 수동 플레이북의 복사본을 보여줍니다. 아래 단계를 검토하여 플레이북의 다양한 작업을 파악합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



다음 조건이 충족되면 이 플레이북이 트리거되고 보안 인시던트와 연결됩니다.

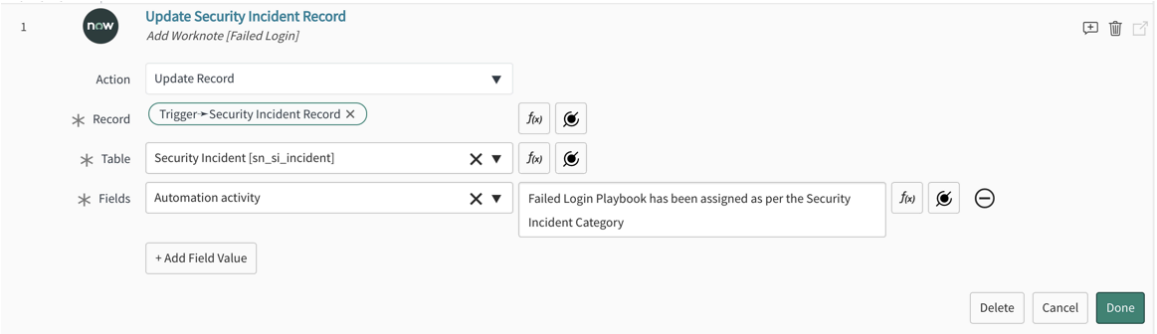
- 범주가 실패한 로그인임
- 영향을 받는 사용자가 한 명 이상 있음
- 보안 인시던트가 종결되거나 취소되지 않음



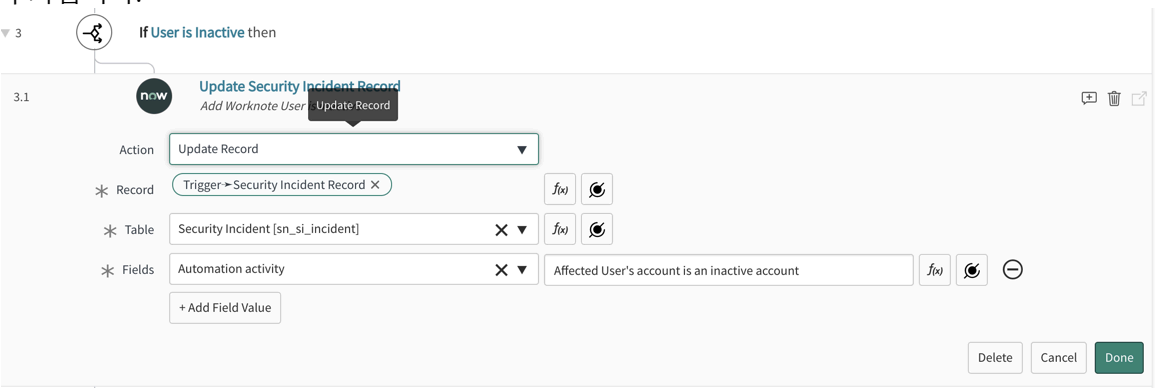
다음 단계에서는 실패한 로그인 수동 플레이북에서 사용할 수 있는 작업, 작업 및 하위 플로우를 안내합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

1. 플레이북 실행이 시작되면 1단계에서 실패한 로그인 범주가 할당된 보안 인시던트를 보여주는 작업 메모로 플레이북이 자동으로 업데이트됩니다.



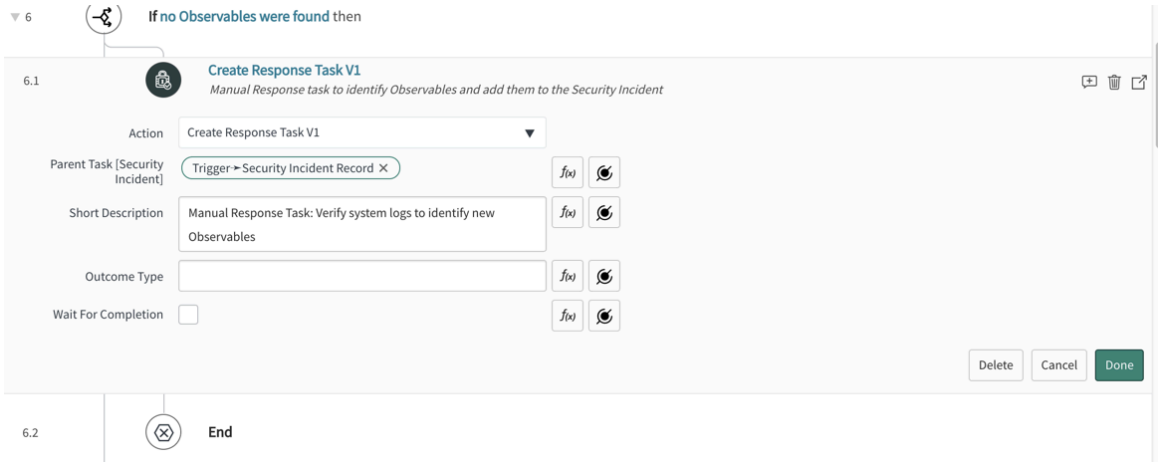
2. 2단계에서는 플레이북이 업데이트되고 분석 상태로 이동됩니다.
3. 3단계에서 플레이북은 영향을 받는 사용자가 활성 사용자인지 비활성 사용자인지 확인합니다. 사용자가 비활성 상태인 경우 사용자 계정이 비활성 상태인 보안 인시던트에 작업 메모가 추가됩니다.



> **주:**
> 플로우의 3단계에서 플로우는 에서 ServiceNow사용할 수 있는 *sn_si_incident* 테이블에서 비활성 사용자를 확인합니다. 이 단계는 지침으로 제공되며 특정 환경에 맞게 수정해야 합니다. 이 기능을 사용하려면 환경에 Active Directory 통합을 설정하는 것이 좋습니다. Active Directory 통합을 확인하여 사용자 상태를 찾고 응답에 따라 플레이북의 다음 단계를 설계할 수 있습니다.
>
> Active Directory 통합이 없는 경우 보안 분석가가 IT 팀과 협력하여 사용자를 차단하고 플레이북의 나머지 단계를 진행할 수 있도록 이 단계를 수동 작업으로 대체합니다.

4. 4단계에서는 보안 인시던트에 대한 옵저버블이 검색됩니다.
5. 5단계에서는 옵저버블이 식별됩니다.
6. 옵저버블을 찾을 수 없는 경우 6단계에서 수동 응답 작업이 생성되고 플로우가 종료됩니다.

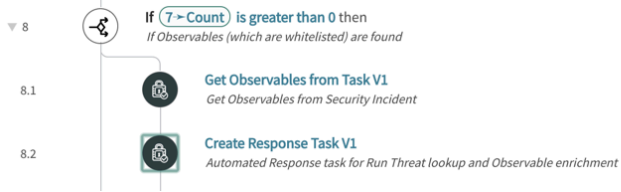
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



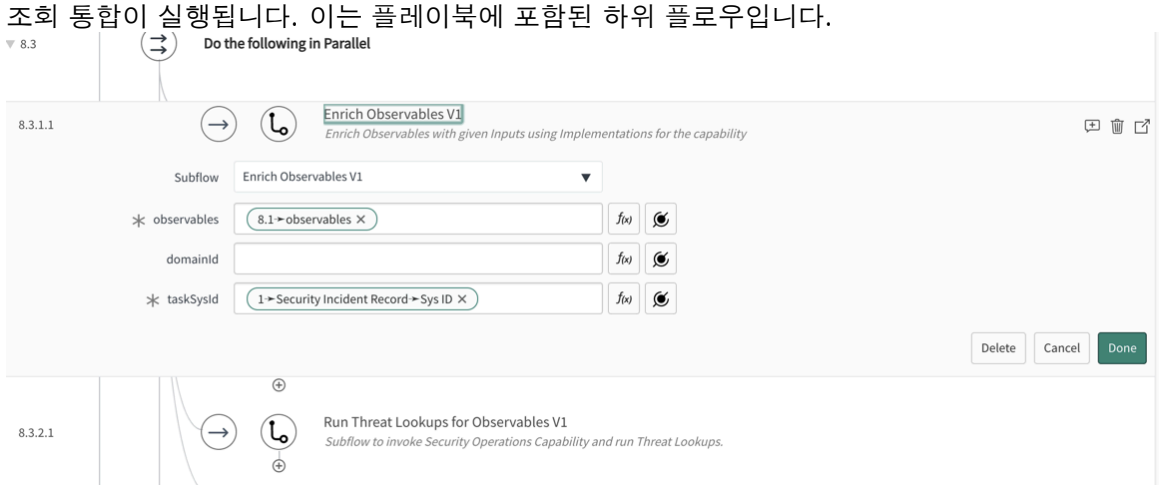
7. 7단계에서 옵저버블이 발견되면 허용되지 않는 옵저버블이 식별됩니다.

8. 하나 이상의 옵저버블이 허용 목록에 없는 경우 다음 단계가 수행됩니다.

a. 8.1단계와 8.2단계가 실행됩니다. 옵저버블이 검색되고 자동 응답 작업이 시작됩니다.



b. 자동화된 작업이 생성되면 8.3단계(8.3.1.1 및 8.3.2.1)가 실행되고 옵저버블 보강 및 위협 조회 통합이 실행됩니다. 이는 플레이북에 포함된 하위 플로우입니다.



c. 8.4단계에서는 통합이 완료된 후 보안 인시던트 기록이 업데이트됩니다.

d. 8.5단계에서는 수행될 다음 자동화 작업을 나타내기 위해 새 응답 작업이 생성됩니다.

e. 8.6단계에서는 옵저버블에서 사이팅 검색 통합이 실행됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

f. 사이팅 검색 하위 플로우가 완료된 후 8.7단계에서 보안 인시던트가 업데이트됩니다.

g. 8.8단계에서는 옵저버블을 검사하여 옵저버블이 악성인지 확인합니다.

h. 옵저버블이 악성이 아니고 사용자 계정이 활성 상태인 경우 실패한 로그인 시도를 다시 확인하기 위해 자동화된 이메일이 사용자에게 전송됩니다. 옵저버블을 식별하고 보안 인시던트에 추가하기 위한 수동 응답 작업이 생성됩니다. 플레이북은 이 단계에서 종료됩니다.

i. 옵저버블이 악성인 경우 3개의 응답 작업이 생성됩니다.

i. 실패한 로그인 시도를 확인 (예 또는 아니요) 하기 위해 자동화된 이메일이 사용자에게 전송됩니다. 사용자가 예라고 응답하는 경우:

1. 보안 인시던트 상태가 포함으로 업데이트됩니다.

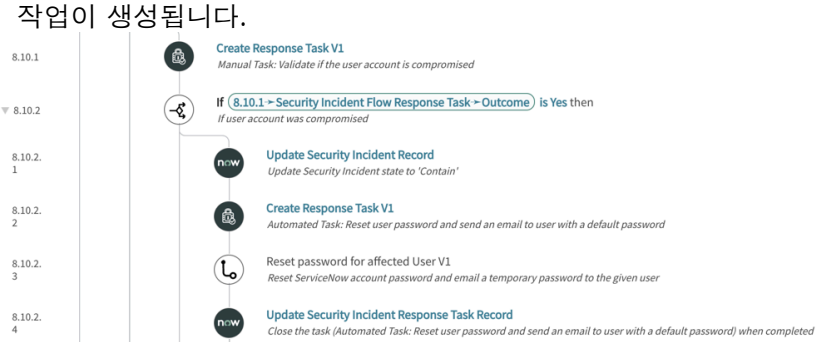
2. 암호를 재설정하기 위해 자동화된 이메일이 사용자에게 전송됩니다.

3. 암호 재설정 하위 플로우가 시작되고 작업이 완료되면 사용자에게 이메일이 전송됩니다.

> **주:**
> 암호 재설정 단계는 지침으로 제공됩니다. 플로우의 단계는 ServiceNow 시스템에서 사용자 계정의 암호를 재설정합니다. 그러나 암호를 재설정하는 프로세스는 환경에 따라 다를 수 있습니다. Active Directory 통합을 확인하여 사용자의 암호를 자동으로 재설정할 수 있습니다. Active Directory 통합이 없는 경우 보안 분석가가 해당 IT 팀과 협력하여 사용자 암호를 재설정하고 해당 작업을 완료한 후 플레이북의 나머지 단계를 진행할 수 있도록 이 단계를 수동 작업으로 대체합니다.

ii. 사용자가 아니요라고 응답하면 응답을 다시 확인하기 위해 자동화된 전자 메일이 사용자에게 전송됩니다. 보안 분석가는 적절한 작업을 수동으로 수행해야 합니다.

iii. 사용자가 자동화된 이메일에 응답하지 않으면 보안 분석가가 보안 인시던트를 수동으로 업데이트하고 응답을 제공해야 합니다. 사용자 계정이 손상되었는지 확인하기 위한 수동 작업이 생성됩니다.



9. 8.10.3단계에서 보안 인시던트 상태가 업데이트됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

10. 8.10.4단계에서는 악의적인 IP 및 URL에 대한 블록 요청 생성 기능 구현을 사용할 수 있는지 확인하기 위해 자동화된 작업이 생성됩니다. 역량 구현을 사용할 수 있는 경우 블록 요청 생성 하위 플로우가 실행됩니다. 이를 사용할 수 없는 경우 보안 인시던트가 업데이트되고 기능 구현을 사용할 수 없음을 나타내는 작업 메모가 게시됩니다.
11. 9단계에서는 보안 인시던트가 업데이트되고 상태가 검토로 설정됩니다.
12. 10단계에서는 사용자가 작업을 닫기 전에 사후 인시던트 검토를 완료할 수 있도록 응답 작업이 생성됩니다.

하위 보안 인시던트 자동화를 위한 플레이북

중복 보안 인시던트는 하위 보안 인시던트로 분류되어 상위 보안 인시던트로 롤업됩니다.

하위 보안 인시던트 자동화 플레이북은 중복 보안 인시던트를 조사하고 종결하는 데 필요한 시간을 단축하는 데 도움이 됩니다. 이 플레이북은 하위 보안 인시던트의 특정한 고유 아티팩트(옵저버블, 영향을 받는 사용자, CI)를 상위 보안 인시던트에 자동으로 롤업합니다.

필수 구성요소

필요한 역할:

- sn_si.admin
- flow_designer

스포크: Security Operations 스포크 설치(sn_sec_spoke)

핵심 기능

하위 자동화 플레이북에서는 다음과 같은 기능을 다룹니다.

1. 보안 인시던트를 분석 단계로 이동합니다.
2. 중복을 제거하고 영향을 받는 사용자 및 CI를 상위 보안 인시던트에 추가(롤업)합니다.
3. 하위 인시던트의 옵저버블을 상위 보안 인시던트에 추가합니다.
4. 상위 보안 인시던트가 종결되면 하위 보안 인시던트를 종결하거나 취소합니다.

필요한 역량

자세한 내용은 ServiceNow Store 를 참조하십시오.

보안 분석가 경험

보안 위협을 단계별로 해결하는 방법을 이해하려면 을 참조하십시오 플레이북으로 보안 위협 해결.

Flow Designer 기능을 갖춘 하위 보안 인시던트 자동화 플레이북에 대한 심층 이해

시작

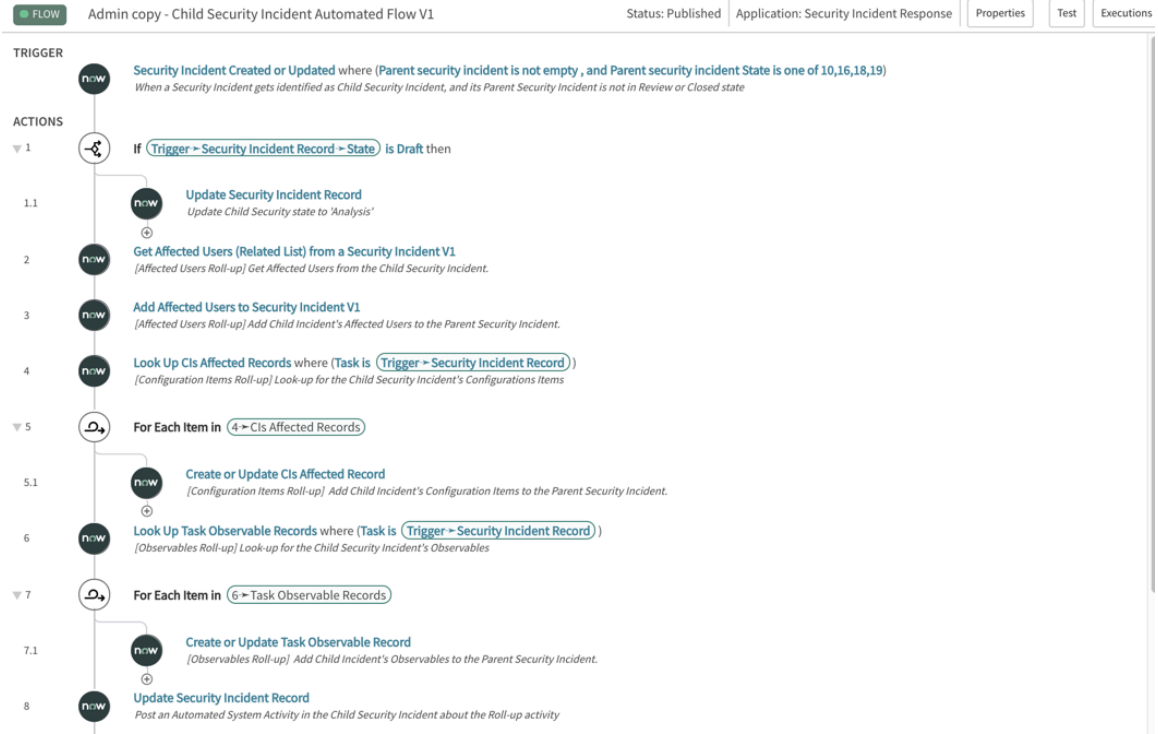
1. sn_si.user 및 flow_designer 역할을 가진 사용자로 로그인합니다.
2. 다음으로 이동 플로우 디자이너 〉 디자이너 을 클릭하고 로그인 실패 플레이북을 클릭합니다.
3. 하위 보안 인시던트 자동화 플레이북의 사본을 만들고 필요에 따라 수정합니다. 이 단계는 선택 사항입니다. 플로우를 사용자 지정하거나 특정 변경을 수행하려는 경우에만 이 단계를 수행합니다.)
4. 요구 사항에 따라 필요한 수정을 수행합니다. 이 단계는 선택 사항입니다. 플로우를 사용자 지정하거나 특정 변경을 수행하려는 경우에만 이 단계를 수행합니다.)

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. 플레이북을 활성화합니다.

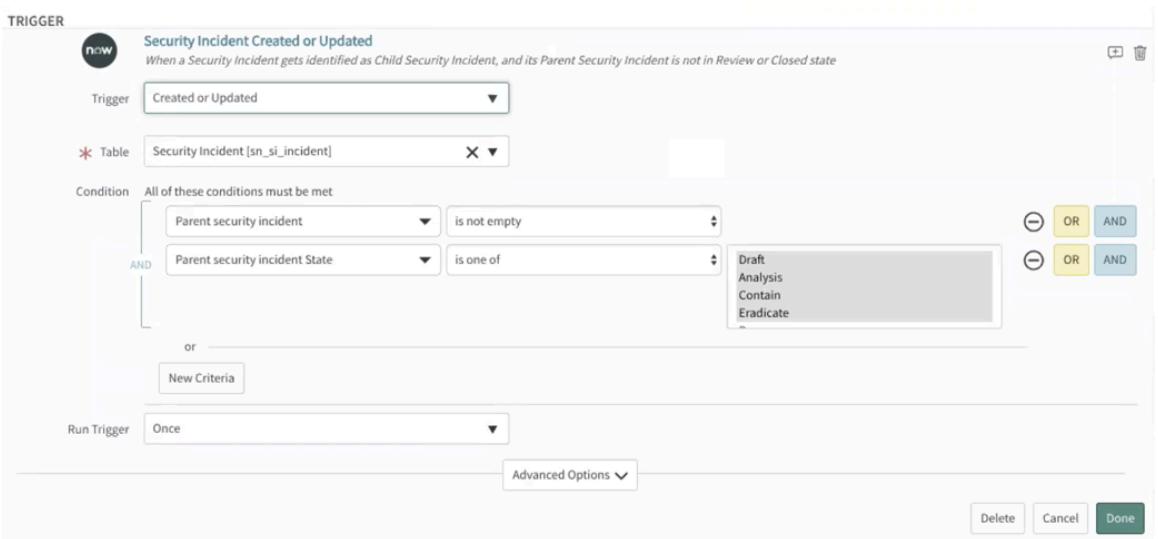
- 기본 시스템에서 사용할 수 있는 플레이북을 사용하려면 메인 플로우를 활성화합니다.
- 요구 사항에 따라 수정한 후 복사된 플로우를 활성화합니다.

다음 이미지는 하위 보안 인시던트 자동화 플레이북의 복사본을 보여줍니다. 아래 단계를 검토하여 플레이북의 다양한 작업을 파악합니다.



이 Playbook은 다음과 같은 경우에 트리거됩니다.

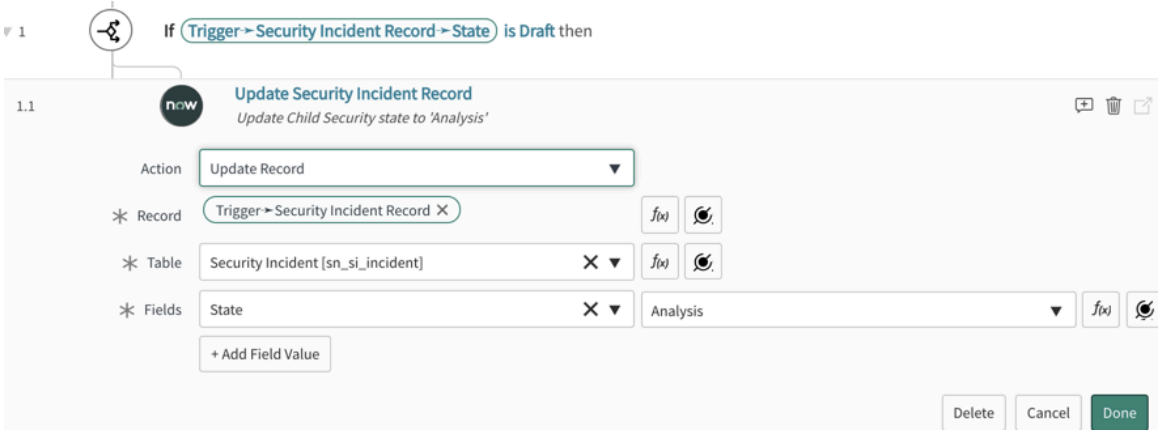
- 상위 보안 인시던트 필드가 비어 있지 않습니다.
- 상위 보안 인시던트가 초안, 분석, 포함 또는 근절 상태입니다.



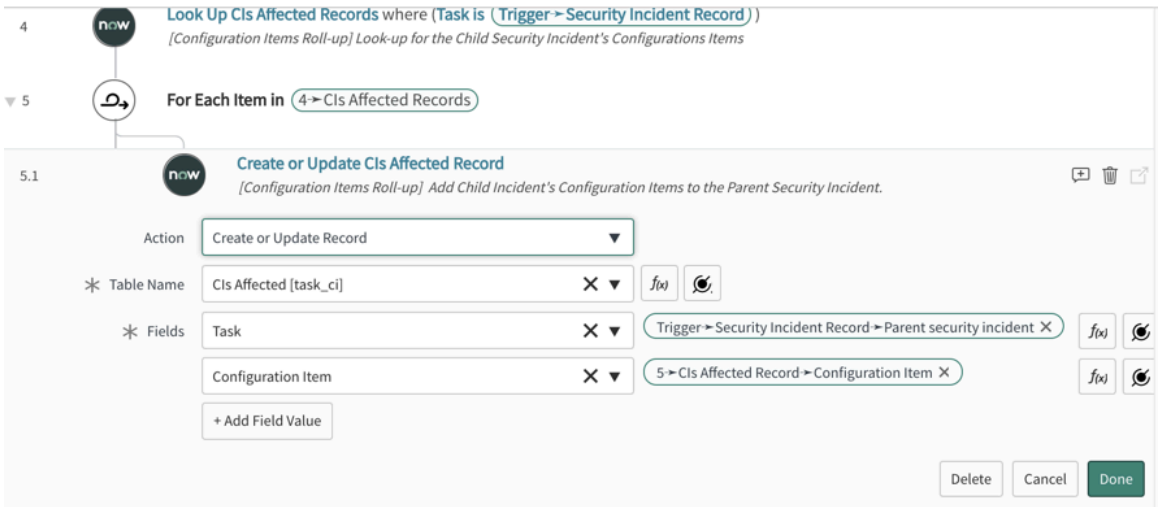
다음 단계에서는 하위 보안 인시던트 자동화 플레이북에서 사용할 수 있는 작업과 작업을 안내합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

1. 플레이북 실행이 시작될 때 1단계에서 보안 인시던트가 초안 상태인 경우 업데이트되고 분석 상태로 설정됩니다.

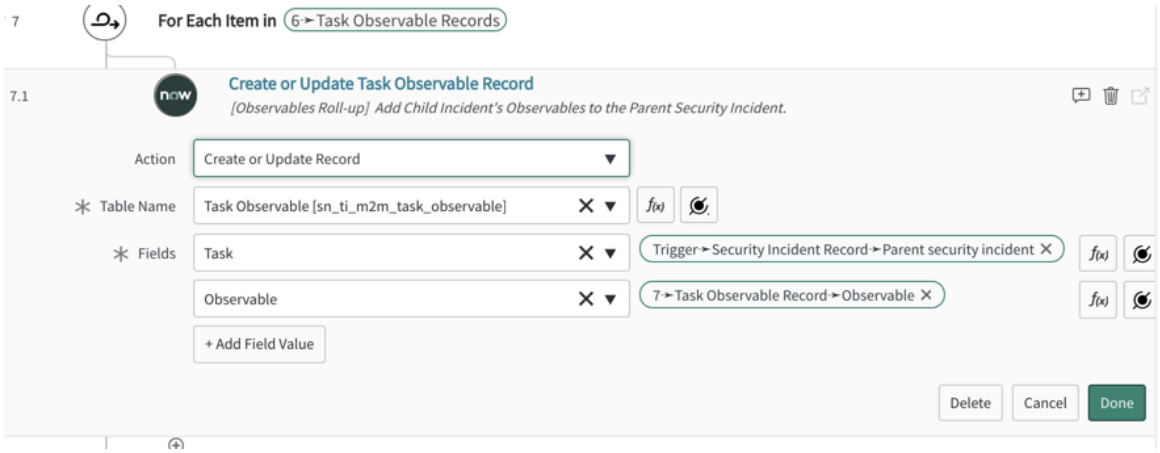


2. 2단계와 3단계에서는 보안 인시던트의 영향을 받는 사용자가 검색되어 상위 보안 인시던트로 롤업됩니다. 중복 사용자는 제거됩니다.
3. 4단계와 5단계에서는 하위 보안 인시던트와 연결된 구성 항목이 검색되고 고유 CI가 상위 보안 인시던트로 롤업됩니다.



4. 6단계와 7단계에서는 하위 보안 인시던트와 연결된 옵저버블이 검색되고 고유 옵저버블이 상위 보안 인시던트로 롤업됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



5. 8단계와 9단계에서는 영향을 받는 사용자, 구성 항목 및 옵저버블이 하위에서 상위 보안 인시던트로 롤업되었음을 나타내는 자동화된 작업 메모가 상위 및 하위 보안 인시던트에 게시됩니다.

Office 365용 플레이북 **-** 악성 파일 탐지됨

이 플레이북은 Office 365에서 검색된 악성 파일을 조사하기 위한 체계적인 수정 단계를 제공합니다.

Office 365에서 악성 파일이 검색되면 Flow Designer의 365 - 악성 파일 탐지 플레이북을 지침으로 사용하고 이러한 악성 파일의 조사를 최적화할 수 있습니다.

Office Malicous 파일 탐지 플레이북 설정

다음 단계를 사용하여 Office Malicous 파일 검색 플레이북을 설정합니다.

시작하기 전에
필요한 역할:

- sn_si.admin
- flow_designer

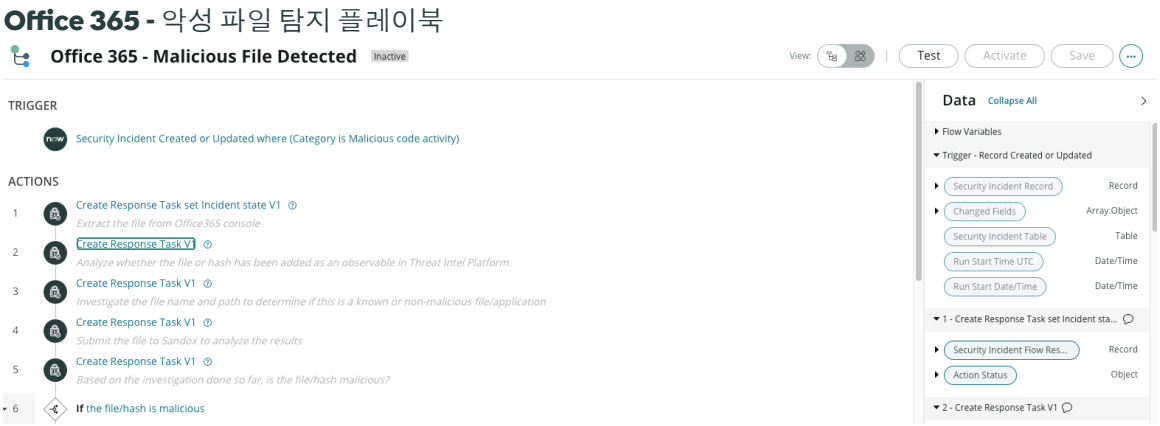
Security Operations 스포크(*sn_sec_spoke*)를 설치했는지 확인하십시오.

프로시저

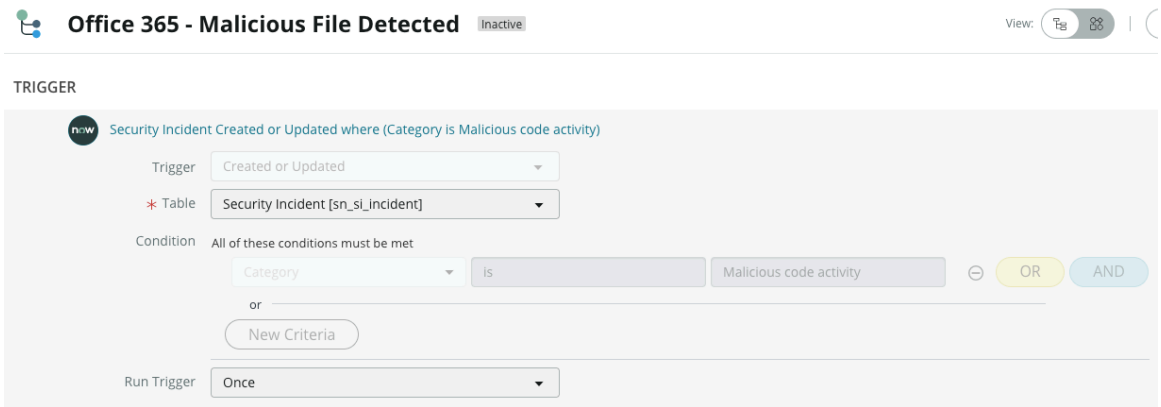
1. sn_si.user 및 flow_designer 역할을 가진 사용자로 로그인합니다.
2. 다음으로 이동 모두 〉 플로우 디자이너 을 클릭하고 **Office 365 -** 악성 파일 검색 플레이북을 선택합니다.
3. 옵션: Office 365 - 악성 파일 탐지 플레이북 플로우의 복사본을 만들고 필요에 따라 수정할 수 있습니다.

   플레이북 플로우의 사본을 생성하려면 아이콘을 클릭하고 플로우 복사를 선택합니다. 플로우를 사용자 지정하거나 특정 변경을 수행하려는 경우에만 이 단계를 수행합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 플레이북을 활성화합니다.
   - 기본 시스템에서 사용할 수 있는 플레이북을 사용하려면 메인 플로우를 활성화합니다.
   - 필요한 사항을 변경한 후 복사된 플로우를 활성화합니다.
5. 플레이북에 대한 트리거 조건을 설정합니다.
   이 Playbook은 범주 가 악성 코드 활동일 때 트리거되고 보안 인시던트와 연결됩니다.



Office 365 악성 파일 탐지 플레이북 사용

이 플레이북을 사용하여 Office 365에서 검색된 악성 파일을 조사합니다. 다음 단계에서는 Office 365 악성 파일 검색 플레이북에서 사용할 수 있는 작업, 작업 및 하위 흐름에 대한 연습을 제공합니다.

시작하기 전에

필요한 역할:

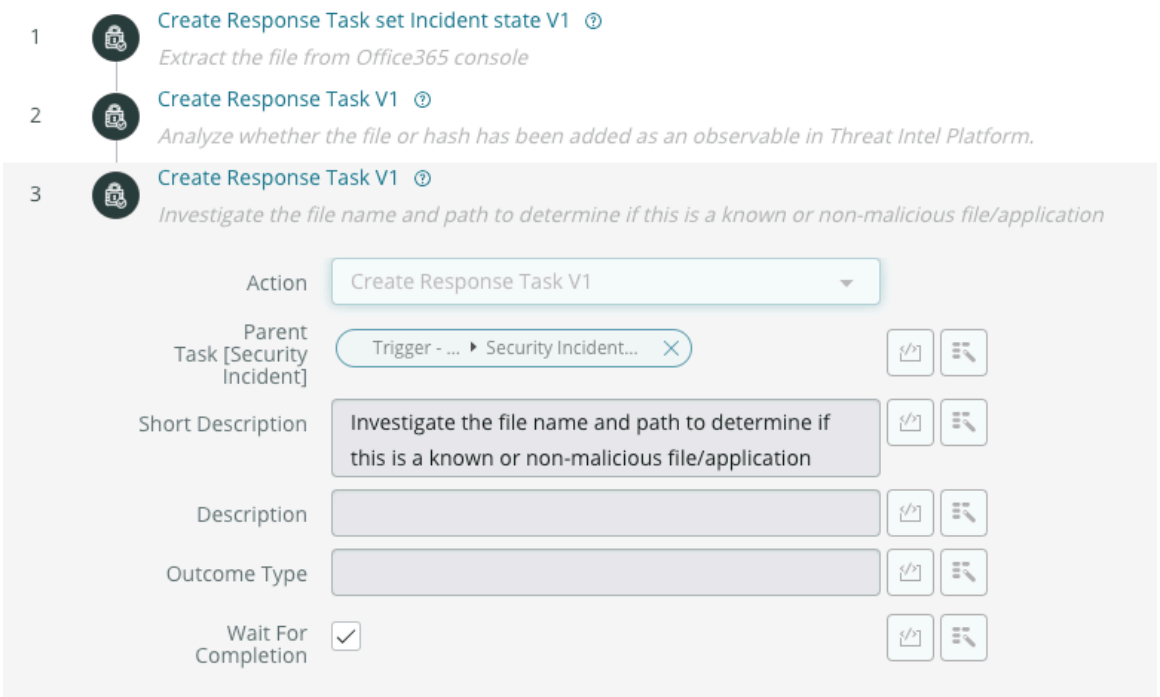
- sn_si.admin
- flow_designer

프로시저

1. 플레이북이 트리거되고 실행이 시작되면 작업 1에서 Office 365 콘솔에서 악성 파일을 추출해야 합니다.
2. 작업 2에서는 파일 또는 해시가 위협 인텔리전스 플랫폼에서 옵저버블로 추가되었는지 여부를 분석해야 합니다.
3. 작업 3에서는 파일 이름과 경로를 조사하여 알려진 파일/애플리케이션인지 또는 악성이 아닌지 확인해야 합니다.

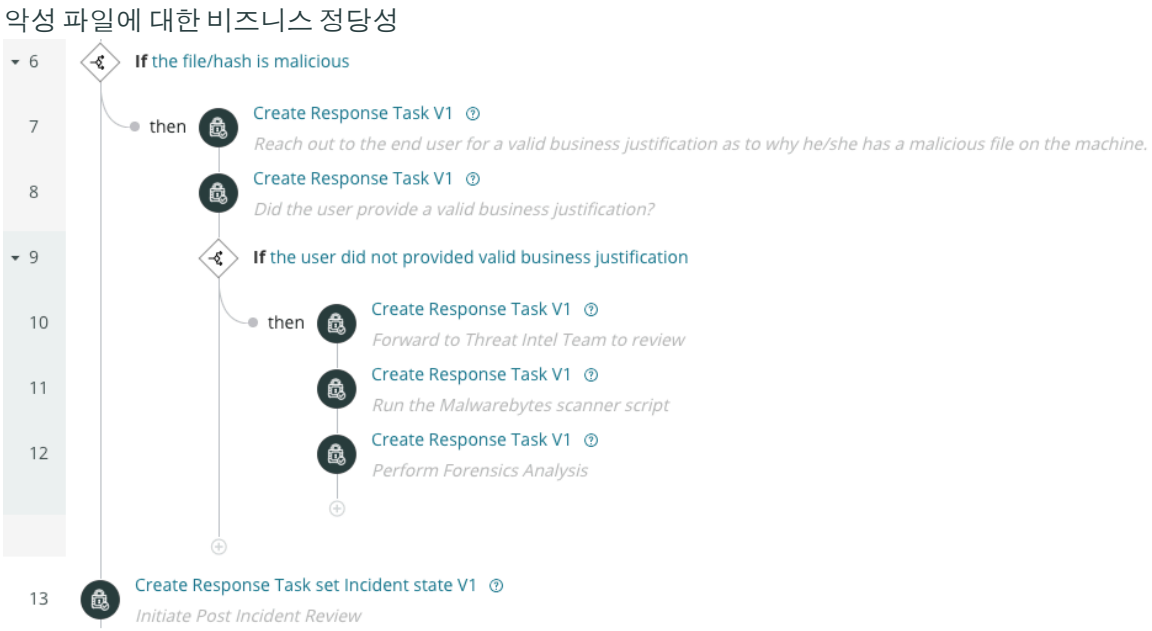
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Office 365 악성 파일 탐지 플레이북



4. 작업 4에서는 결과 분석을 위해 파일을 Sandbox에 제출해야 합니다.
5. Action 5에서는 지금까지 수행된 조사를 기반으로 파일 또는 해시가 악성인지 여부를 확인해야 합니다.
   파일 또는 해시가 악성이 아닌 경우 작업 5에서 수동 응답 작업이 생성되고 흐름이 종료됩니다.
6. 작업 6에서 파일 또는 해시가 악성인 경우 작업 7과 8이 실행됩니다.
7. 작업 7에서는 최종 사용자에게 연락하여 디바이스에 악성 파일이 있는 이유에 대한 유효한 비즈니스 정당성을 확인해야 합니다.
   파일 또는 해시가 악의적인 경우 Playbook의 기존 이메일 템플릿을 사용하여 최종 사용자에게 이메일을 보내 설명을 요청할 수 있습니다.
8. 작업 8에서는 최종 사용자가 유효한 비즈니스 정당성을 제공했는지 여부를 확인해야 합니다.
   최종 사용자가 유효한 비즈니스 정당성을 제공한 경우 작업 5에서 수동 응답 작업이 생성되고 플로우가 종료됩니다.
9. 작업 9에서 사용자가 유효한 비즈니스 정당성을 제공하지 않은 경우 작업 10, 11 및 12가 실행됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



10. Action 10에서는 유효한 비즈니스 정당성이 없었으므로 악성 파일 또는 해시를 위협 인텔리전스 팀에 전달하여 검토할 수 있습니다.
11. 작업 11에서는 Malware bytes 스캐너 스크립트를 실행하여 파일 또는 해시가 악성인지 확인해야 합니다.
12. Action 12에서는 포렌식 분석을 수행하여 파일 또는 해시가 악성인지 확인해야 합니다.
13. 작업 13에서는 사용자가 작업을 닫기 전에 사후 인시던트 검토를 완료할 수 있도록 응답 작업이 생성됩니다.

반복 탐지를 위한 플레이북

이 Playbook은 인시던트 응답이 과거에 정확히 또는 유사한 피싱 보고서에 제공되었는지 확인하고 새 보고서에서도 유사하게 자동으로 작동하는지 확인하는 데 도움이 됩니다.

반복 탐지 플레이북은 새로 보고된 피싱 인시던트가 과거 인시던트와 유사한지 확인합니다. 반복 탐지가 식별되면 일치하는 보안 인시던트 및 해결 상세 정보가 분석가에게 제공되고, 분석가는 새로 보고된 인시던트에 사용할 수 있으므로 보안 인시던트를 신속하게 정정할 수 있습니다.

반복 탐지 플레이북 설정

다음 단계를 사용하여 반복 탐지 플레이북을 설정합니다.

시작하기 전에
필요한 역할:

- sn_si.admin
- flow_designer

Security Operations 스포크(*sn_sec_spoke*)를 설치했는지 확인하십시오. 다음 시스템 속성을 수정할 수 있는 옵션이 있습니다.

- *sn_sec_spoke.SimilarPhish.earlyTermination ##*
- *sn_sec_spoke.similarphish.lookbackdays*
- *sn_sec_spoke.similarphish.maxcomparisonsize*
- *sn_sec_spoke.similarphish.minmatchscore*

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

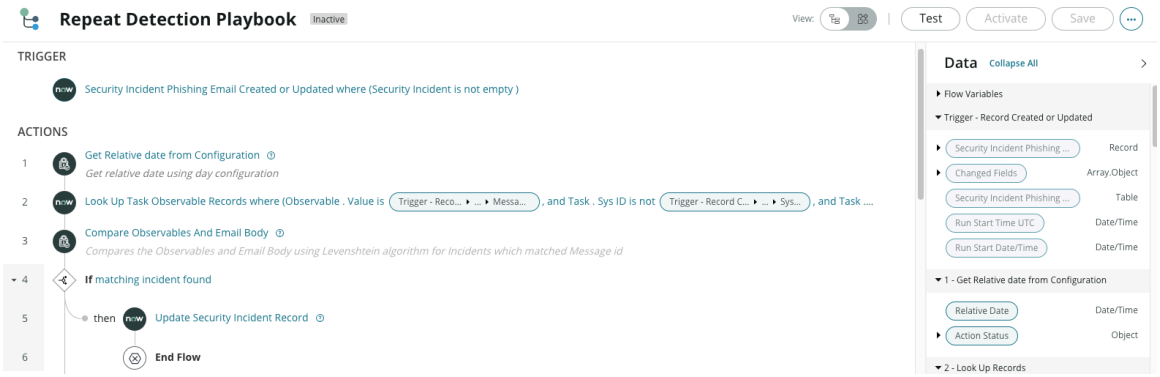
1. sn_si.user 및 flow_designer 역할을 가진 사용자로 로그인합니다.

2. 다음으로 이동 모두 〉 플로우 디자이너 을 클릭하고 반복 탐지 플레이북을 선택합니다.

3. 옵션: 반복 탐지 플레이북 플로우의 사본을 생성하고 필요에 따라 수정할 수 있습니다.

플레이북 플로우의 사본을 생성하려면 아이콘을 클릭하고 플로우 복사를 선택합니다. 플로우를 사용자 지정하거나 특정 변경을 수행하려는 경우에만 이 단계를 수행합니다.

반복 탐지 플레이북

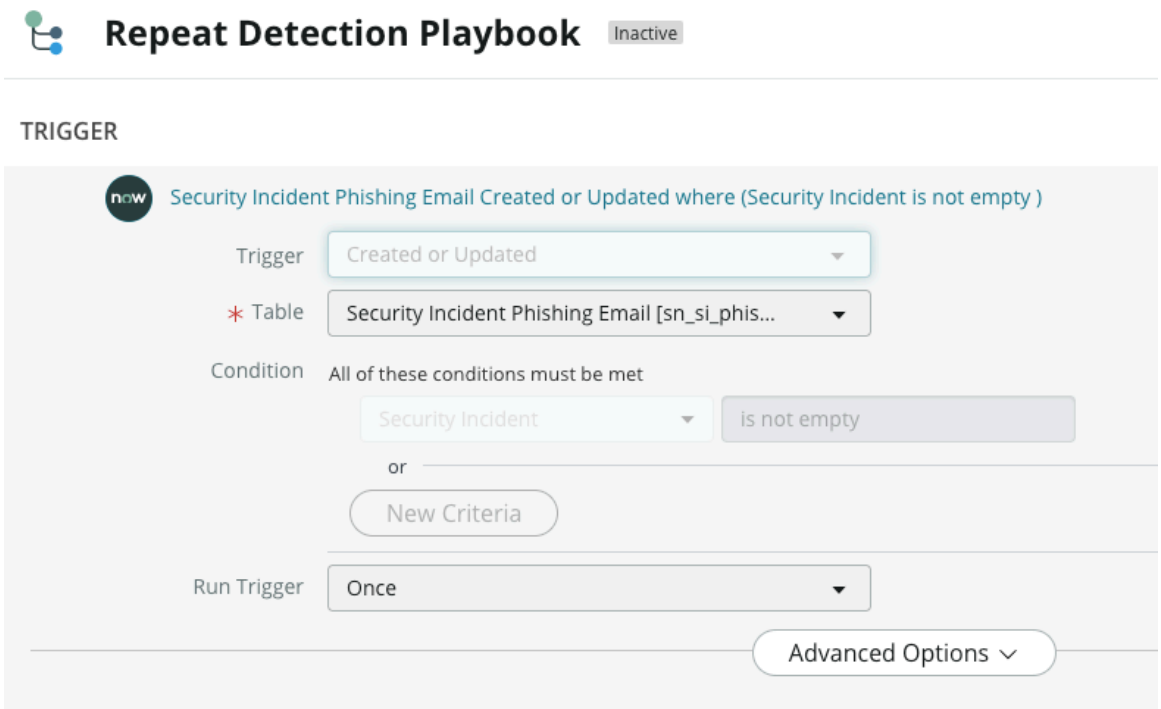


4. 플레이북을 활성화합니다.

- 기본 시스템에서 사용할 수 있는 플레이북을 사용하려면 메인 플로우를 활성화합니다.
- 필요한 사항을 변경한 후 복사된 플로우를 활성화합니다.

5. 플레이북에 대한 트리거 조건을 설정합니다.

이 Playbook은 보안 인시던트 가 비어 있지 않을 때 트리거됩니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

반복 탐지 플레이북 사용

이 Playbook을 사용하여 인시던트 응답이 과거에 정확히 일치하거나 유사한 피싱 보고서에 제공되었고 새 보고서에서도 유사하게 자동으로 작동하는지 조사할 수 있습니다. 다음 단계에서는 반복 탐지 플레이북에서 사용할 수 있는 작업, 작업 및 하위 플로우에 대한 둘러보기를 제공합니다.

시작하기 전에

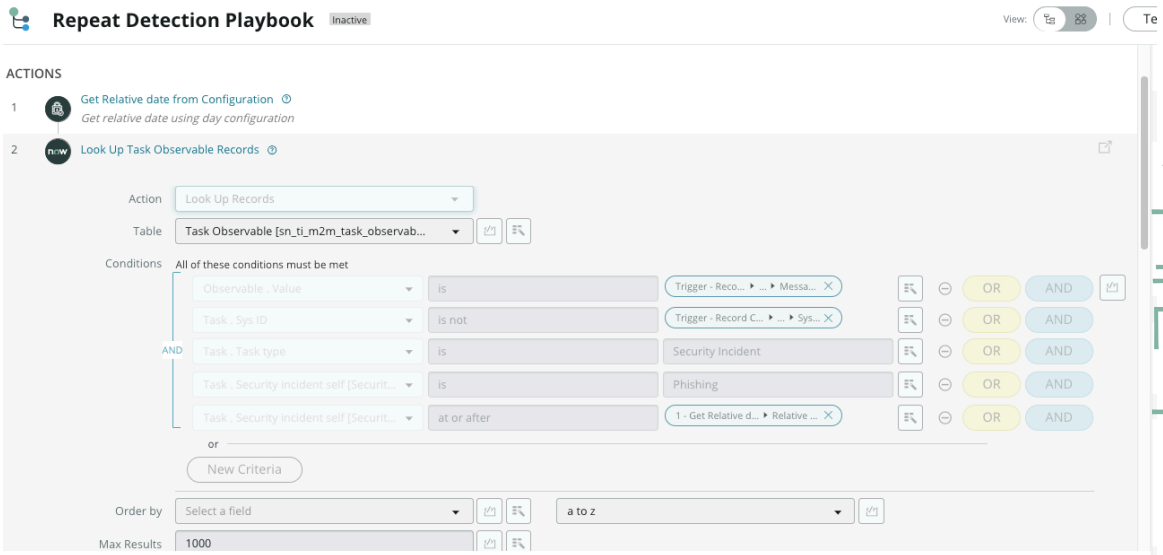
필요한 역할:

- sn_si.admin
- flow_designer

프로시저

1. 플레이북이 트리거되고 실행이 시작되면 작업 1에서 플레이북은 일 구성을 사용하여 보안 인시던트의 상대 날짜를 검색합니다.
2. 작업 2에서 플레이북은 메시지 ID를 기반으로 인시던트와 일치하는 테이블 *sn_ti_m2m_task_observable* 에서 작업 옵저버블 기록을 찾습니다.

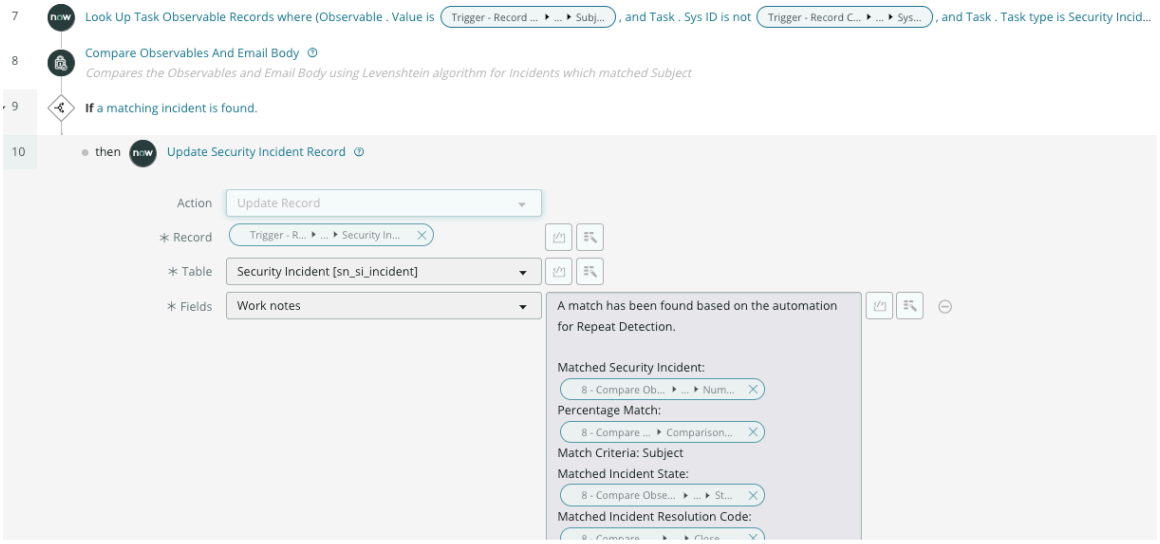
반복 탐지 플레이북



3. 작업 3에서 플레이북은 메시지 ID와 일치하는 인시던트에 대해 Levenshtein 알고리즘을 사용하여 작업 옵저버블과 이메일 본문을 비교합니다.
4. 작업 4에서는 지금까지 수행된 조사를 기반으로 플레이북이 메시지 ID를 기반으로 일치하는 인시던트를 찾았는지 여부를 확인합니다.
   작업 5에서 일치하는 인시던트가 발견되면 Playbook은 반복 탐지에 대한 자동화를 기반으로 일치하는 항목이 발견되었음을 작업 메모에 자동으로 업데이트합니다. 작업 6에서 플로우가 종료됩니다.
5. 일치하는 인시던트를 찾을 수 없는 경우, 작업 7에서 플레이북은 제목을 기준으로 인시던트와 일치하는 테이블 *sn_ti_m2m_task_observable* 에서 작업 옵저버블 기록을 찾습니다.
6. 작업 8에서 플레이북은 제목과 일치하는 인시던트에 대해 Levenshtein 알고리즘을 사용하여 작업 옵저버블과 이메일 본문을 비교합니다.
7. 작업 9에서 플레이북은 일치하는 인시던트가 있는지 여부를 확인합니다.
   작업 10에서 일치하는 인시던트가 발견되면 Playbook은 반복 탐지에 대한 자동화를 기반으로 일치하는 항목이 발견되었음을 작업 노트에 자동으로 업데이트합니다. 작업 11에서 흐름이 종료됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

일치하는 인시던트



8. 작업 12에서 플레이북은 주소를 기준으로 인시던트와 일치하는 테이블 *sn_ti_m2m_task_observable* 에서 작업 옵저버블 기록을 찾습니다.
9. 작업 13에서 플레이북은 주소와 일치하는 인시던트에 대해 Levenshtein 알고리즘을 사용하여 작업 옵저버블과 이메일 본문을 비교합니다.
10. 작업 14에서 Playbook은 주소를 기반으로 일치하는 인시던트를 찾았는지 여부를 확인합니다. 작업 15에서 일치하는 인시던트가 발견되면 Playbook은 반복 탐지에 대한 자동화를 기반으로 일치하는 항목이 발견되었음을 작업 메모에 자동으로 업데이트합니다. 작업 16에서 흐름이 종료됩니다.

스푸핑된 이메일에 대한 플레이북(동일한 표시 이름 사용)

이 플레이북은 스푸핑된 이메일 이름이 조직의 직원에게 전송될 때 트리거되는 스푸핑된 이메일을 조사하기 위한 체계적인 정정 단계를 제공합니다.

스푸핑된 이메일 플레이북 설정

다음 단계를 사용하여 스푸핑된 이메일 플레이북을 설정합니다.

시작하기 전에

필요한 역할:

- sn_si.admin
- flow_designer

Security Operations 스포크(*sn_sec_spoke*)를 설치했는지 확인하십시오.

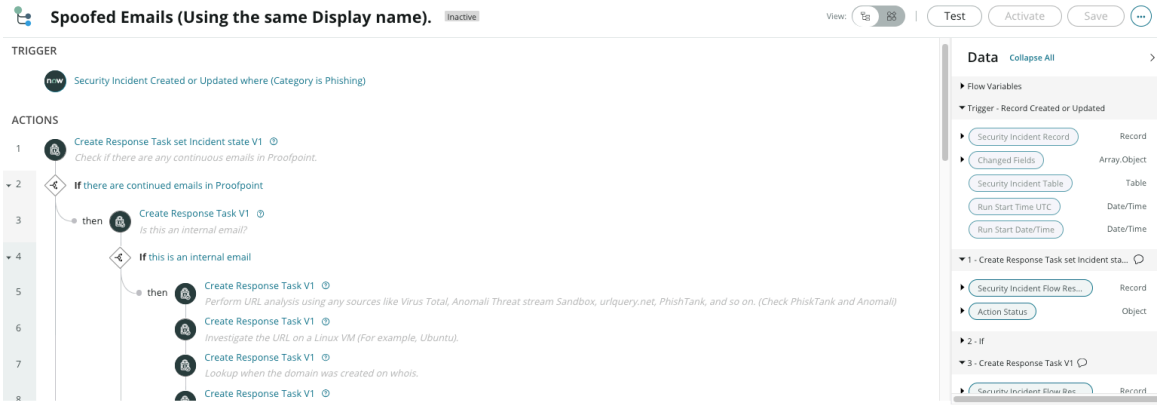
프로시저

1. sn_si.user 및 flow_designer 역할을 가진 사용자로 로그인합니다.
2. 다음으로 이동 모두 〉 플로우 디자이너 을 클릭하고 스푸핑된 이메일(동일한 표시 이름 사용) 플레이북을 선택합니다.
3. 옵션: 반복 탐지 플레이북 플로우의 사본을 생성하고 필요에 따라 수정할 수 있습니다.

   플레이북 플로우의 사본을 생성하려면 아이콘을 클릭하고 플로우 복사를 선택합니다. 플로우를 사용자 지정하거나 특정 변경을 수행하려는 경우에만 이 단계를 수행합니다.

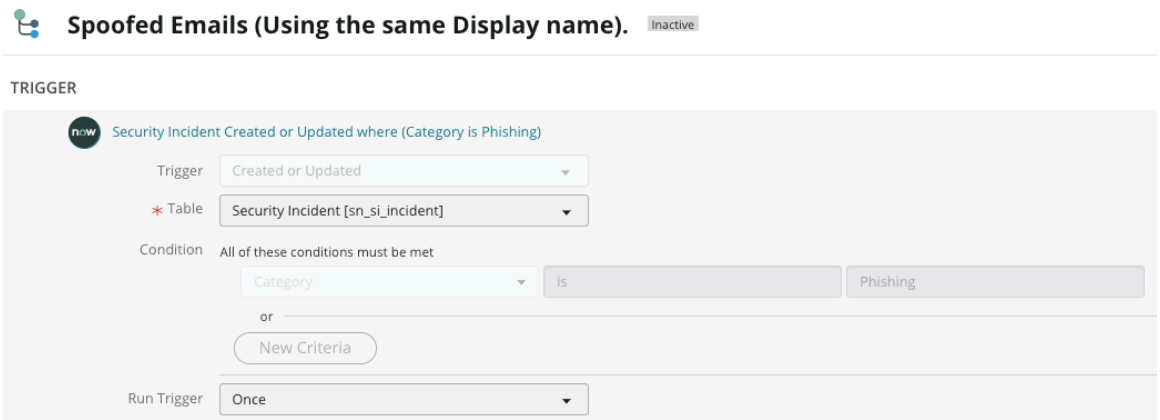
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

스푸핑된 이메일 플레이북



4. 플레이북을 활성화합니다.
   - 기본 시스템에서 사용할 수 있는 플레이북을 사용하려면 메인 플로우를 활성화합니다.
   - 필요한 사항을 변경한 후 복사된 플로우를 활성화합니다.
5. 플레이북에 대한 트리거 조건을 설정합니다.

   범주가 피싱일 때 이 Playbook이 트리거되고 보안 인시던트와 연결됩니다.



스푸핑된 이메일(동일한 표시 이름 사용) 플레이북 사용

이 플레이북을 사용하여 스푸핑된 이메일 이름이 조직의 직원에게 전송될 때 트리거되는 스푸핑된 이메일을 조사합니다. 다음 단계에서는 스푸핑된 이메일(동일한 표시 이름 사용) 플레이북에서 사용할 수 있는 작업, 작업 및 하위 플로우에 대한 안내를 제공합니다.

시작하기 전에
필요한 역할:

- sn_si.admin
- flow_designer

프로시저

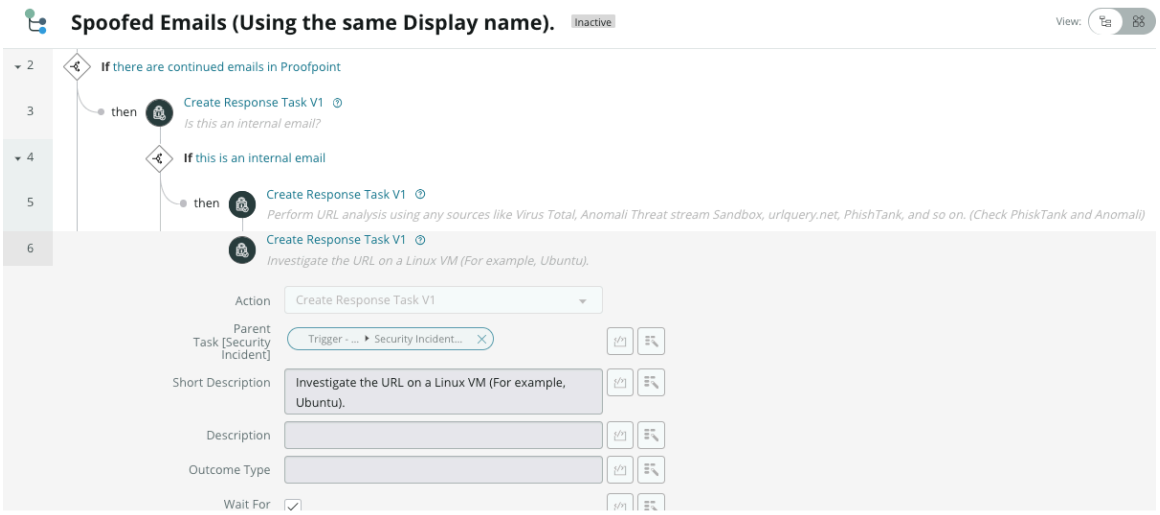
1. 플레이북이 트리거되고 실행이 시작되면 작업 1에서 Proofpoint에 지속적으로 스푸핑된 이메일이 있는지 확인해야 합니다.
2. 작업 2에서 Proofpoint에 연속 이메일이 있는 경우 내부 스푸핑된 이메일인지 확인합니다.
3. 작업 3에서 내부 스푸핑된 이메일인 경우 다음 작업을 수행합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 작업 5에서는 Virus Total, Anomali, Threat stream, Sandbox, urlquery.net, PhishTank(예: PhiskTank 및 Anomali 확인)와 같은 소스를 사용하여 URL 분석을 수행해야 합니다.

b. 작업 6에서는 Linux VM(예: Ubuntu)에서 URL을 조사해야 합니다.

스푸핑된 이메일(동일한 표시 이름 사용) 플레이북



c. 작업 7에서 도메인이 WHOIS에서 생성된 시기를 조회해야 합니다.
최근에 등록된 도메인 중 의심스럽고 피싱 공격 가능성이 높은 도메인(지난주 이내)을 찾습니다.

d. 작업 8에서는 지금까지 수행된 조사에 따라 이 이메일에 악성 첨부 파일이나 링크가 포함되어 있는지 확인해야 합니다.
이 이메일에 악의적인 첨부 파일이나 링크가 포함되어 있지 않으면 플로우가 종료됩니다.

스푸핑된 이메일에 악성 첨부 파일 또는 링크가 포함되어 있습니다.

e. 작업 9에서 이메일에 악성 첨부 파일이나 링크가 포함되어 있는 경우 다음 작업을 수행합니다.

i. 작업 10에서는 영향을 받는 사용자에게 연락하여 자격 증명이 손상되었는지 확인해야 합니다. 제공된 이메일 템플릿을 사용하여 영향을 받는 사용자에게 연락할 수 있습니다.

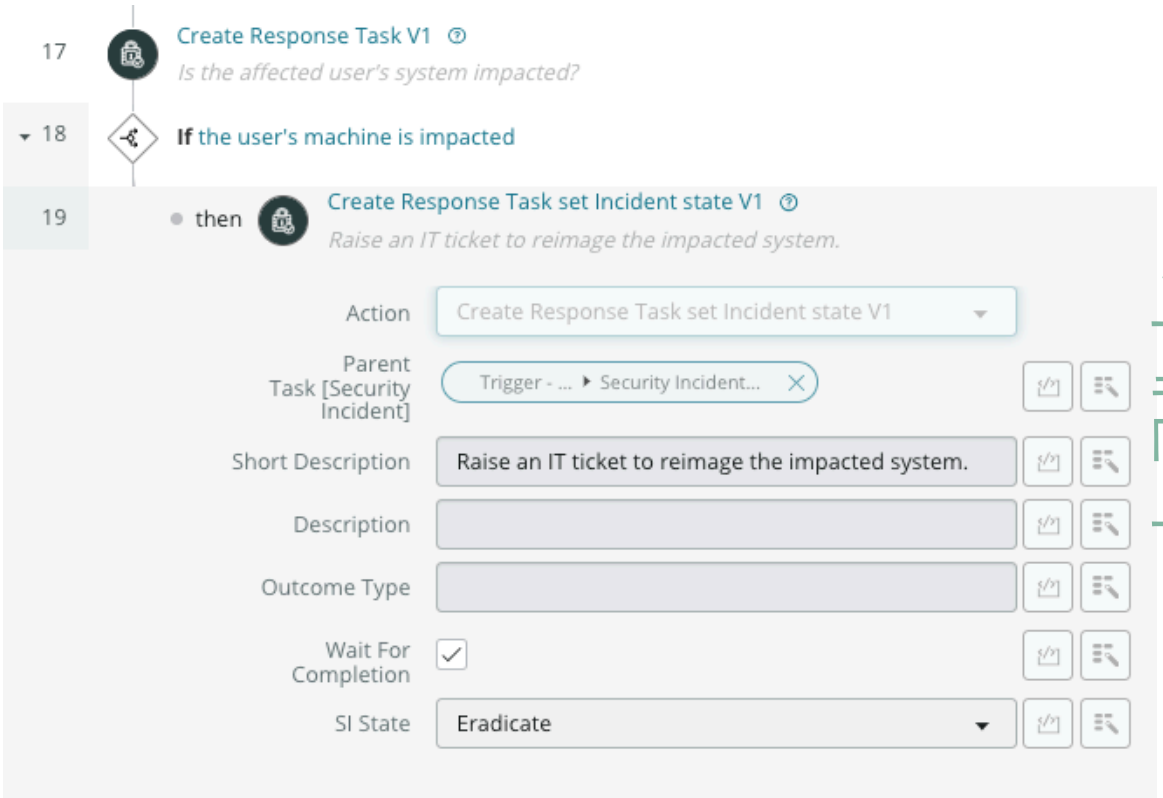
ii. 작업 11에서는 이메일 응답에 따라 자격 증명이 손상되었는지 여부를 확인해야 합니다. 자격 증명이 손상되지 않은 경우 플로우가 종료됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

1. 작업 12에서 자격 증명이 손상된 경우 작업 13에서 추가 사용자가 영향을 받는지 확인해야 합니다. 추가 사용자가 영향을 받지 않으면 플로우가 종료됩니다.
2. 작업 14에서 추가 사용자가 영향을 받는 경우 다음 작업을 수행합니다.
   a. 작업 15에서는 Microsoft Exchange Online을 사용하여 이메일을 검색하고 삭제해야 합니다.
   b. 작업 16에서는 Office 365 및 Proofpoint에서 보낸 사람과 악성 파일 또는 첨부 파일을 차단해야 합니다.

4. 작업 17에서 내부 스푸핑된 이메일이 아닌 경우 영향을 받는 사용자의 시스템이 영향을 받는지 확인해야 합니다.
5. 작업 18에서 사용자의 시스템이 영향을 받는 경우 작업 19에서 IT 티켓을 제기하여 영향을 받는 시스템의 이미지를 다시 설치합니다.

영향을 받는 사용자의 시스템이 영향을 받는지 확인



6. 작업 20에서는 작업을 종결하기 전에 사후 인시던트 검토를 완료하기 위한 응답 작업이 생성됩니다.

엔드포인트 탐지를 위한 플레이북

이 플레이북은 호스트 또는 엔드포인트에서 트리거된 맬웨어 경보(예: 악성 파일 탐지)를 조사하기 위한 체계적인 정정 단계를 제공합니다.

호스트나 엔드포인트에서 CrowdStrike 경보가 트리거되면 플로우 디자이너의 엔드포인트 탐지 플레이북을 사용하여 이러한 악성 파일의 조사를 안내하고 최적화할 수 있습니다.

엔드포인트 탐지 **Playbook** 설정

다음 단계를 사용하여 엔드포인트 검색 플레이북을 설정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할:

- sn_si.admin
- flow_designer

Security Operations 스포크(*sn_sec_spoke*)를 설치했는지 확인하십시오.

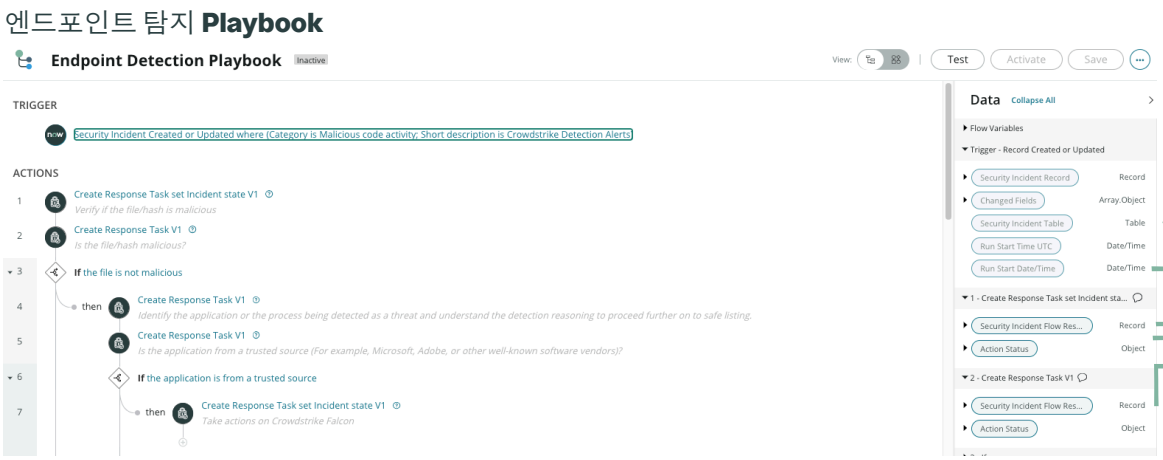
프로시저

1. sn_si.user 및 flow_designer 역할을 가진 사용자로 로그인합니다.

2. 다음으로 이동 모두 〉 플로우 디자이너 을 클릭하고 엔드포인트 감지 플레이북을 선택합니다.

3. 옵션: 엔드포인트 탐지 플레이북 플로우의 사본을 생성하고 필요에 따라 수정할 수 있습니다.

플레이북 플로우의 사본을 생성하려면 ••• 아이콘을 클릭하고 플로우 복사를 선택합니다.
플로우를 사용자 지정하거나 특정 변경을 수행하려는 경우에만 이 단계를 수행합니다.

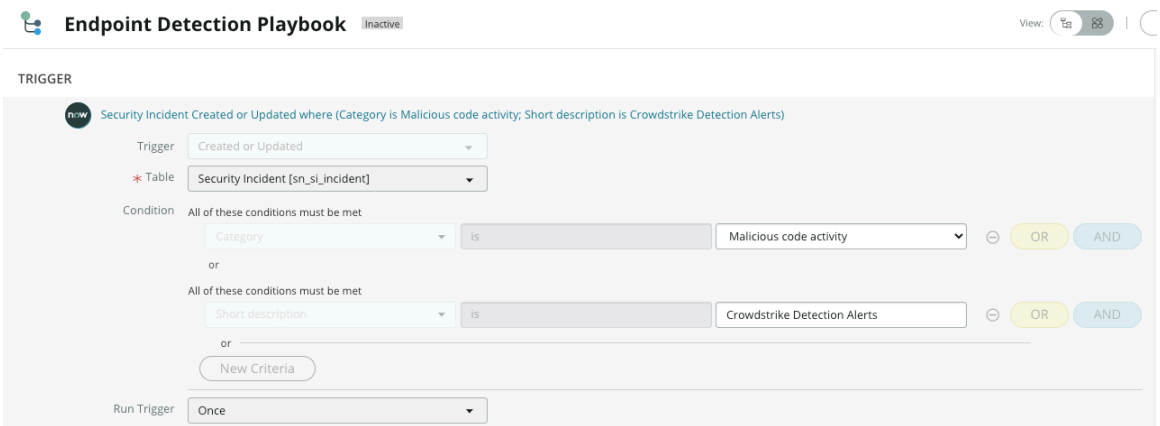


4. 플레이북을 활성화합니다.

- 기본 시스템에서 사용할 수 있는 플레이북을 사용하려면 메인 플로우를 활성화합니다.
- 필요한 사항을 변경한 후 복사된 플로우를 활성화합니다.

5. 플레이북에 대한 트리거 조건을 설정합니다.
다음 조건이 충족되면 이 플레이북이 트리거되고 보안 인시던트와 연결됩니다.

- 범주 는 악성 코드 활동입니다.
- 짧은 설명은**CrowdStrike** 탐지 경보입니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

엔드포인트 탐지 플레이북 사용

이 Playbook을 사용하여 호스트 또는 엔드포인트에서 트리거된 맬웨어 경보를 조사합니다. 다음 단계에서는 엔드포인트 감지 플레이북에서 사용할 수 있는 작업, 작업 및 하위 플로우에 대한 둘러보기를 제공합니다.

시작하기 전에

필요한 역할:

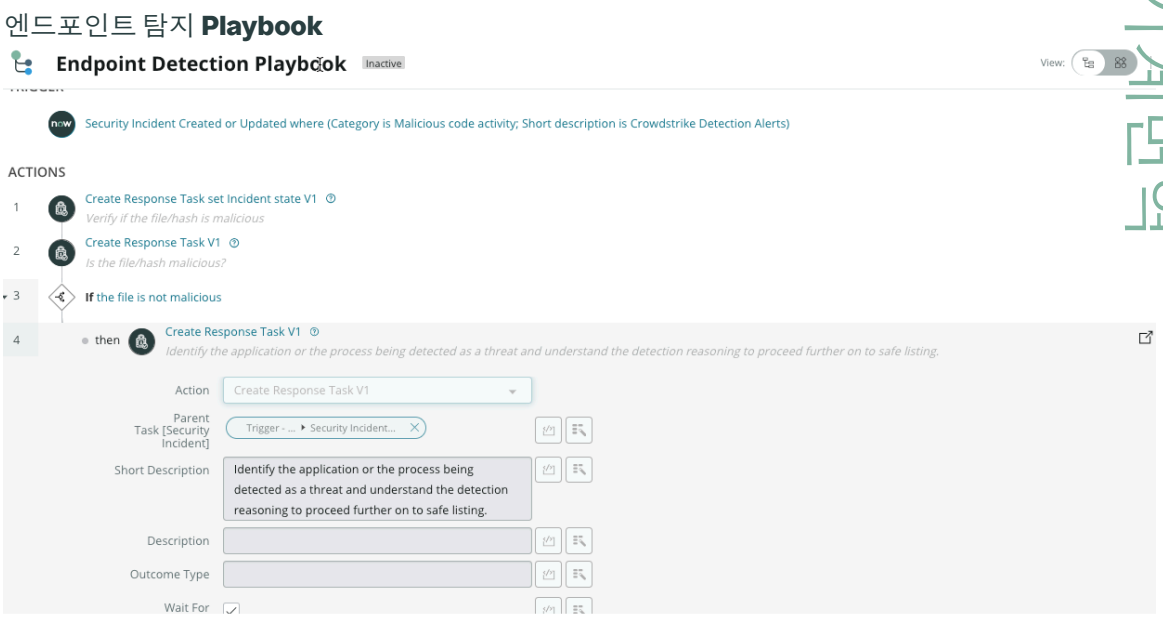
- sn_si.admin
- flow_designer

Security Operations 스포크(*sn_sec_spoke*)를 설치했는지 확인하십시오.

프로시저

1. 플레이북이 트리거되고 실행이 시작되면 작업 1에서 SIR에서 위협 조회 결과를 분석하고 VirusTotal, WildFire, ThreatCrowd 등에서 정보를 수집하여 파일 또는 해시가 악성인지 확인해야 합니다.
2. Action 2에서는 파일 또는 해시가 악성인지 여부를 확인해야 합니다.
3. 작업 3에서 파일 또는 해시가 악의적인 경우 다음 작업을 수행합니다.

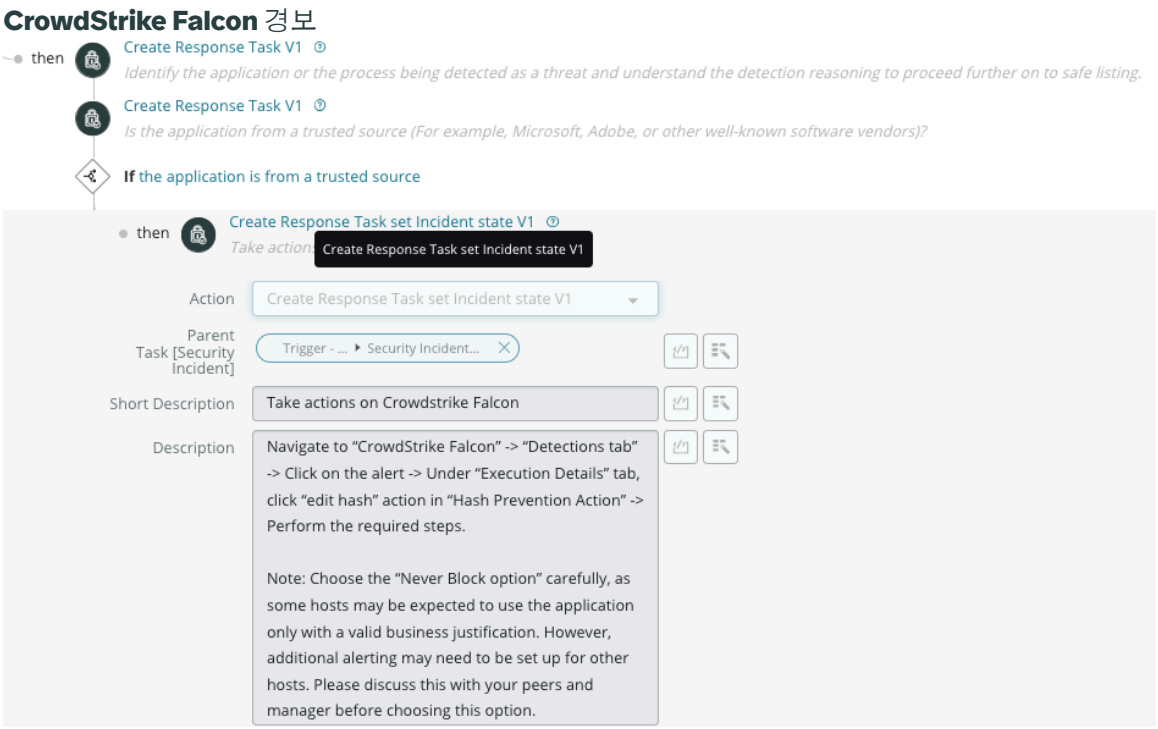
   a. 작업 4에서는 애플리케이션 또는 검색 중인 프로세스를 위협으로 식별하고 검색 이유에 대한 정보를 수집하여 허용 목록에 추가로 적용해야 합니다.



   b. 작업 5에서는 애플리케이션이 신뢰할 수 있는 소스(예: Microsoft, Adobe 또는 기타 잘 알려진 소프트웨어 벤더)에서 온 것인지 확인해야 합니다.

   c. 작업 6에서 애플리케이션이 신뢰할 수 있는 출처에서 제공된 경우 CrowdStrike Falcon 경보에 대해 조치를 취해야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



d. 작업 7에서 다음 작업을 수행합니다.

i. 다음으로 이동 크라우드스트라이크 팔콘 〉 탐지 탭.

ii. CrowdStrike Falcon 경보를 클릭합니다.

iii. Execution Details(실행 세부 정보) 탭의 Hash Prevention Action(해시 방지 작업)에서 **Edit Hash** action(해시 편집 작업)을 클릭합니다.

iv. 필요한 단계를 수행합니다.

> 주:
> 특정 호스트만 유효한 비즈니스 정당성이 있는 응용 프로그램을 사용할 수 있으므로 차단 안 함 옵션을 신중하게 선택합니다. 그러나 다른 호스트에 대해 추가 경보를 설정해야 할 수 있습니다.

e. 작업 8에서 응용 프로그램이 신뢰할 수 있는 원본이 아닌 경우 장치에서 로컬로 파일 또는 응용 프로그램을 포기할지 여부를 선택해야 합니다.
작업 10에서 로컬로 장치에서 파일 또는 애플리케이션을 포기하려면 다음 작업을 수행하십시오.

i. 작업 11에서 격리된 파일 탭으로 이동하고 장치 이름을 검색하여 끝점을 필터링합니다.

ii. 로컬에서 면제해야 하는 파일을 선택하고 릴리스를 클릭합니다.

> 주:
>
> - 파일은 이 특정 엔드포인트에서 계속 실행됩니다. 그러나 탐지 및 격리는 다른 모든 호스트에서 계속 발생합니다.
> - 여러 호스트에서 격리 파일을 대량으로 릴리스하려면 적절한 파일 이름과 상태를 선택합니다. Select(선택)를 클릭하고 Release(릴리스)를 선택합니다.

작업 12에서 디바이스에서 로컬로 파일 또는 애플리케이션을 포기하지 않으려면 사용자를 IT 지원으로 리디렉션하여 승인된 애플리케이션의 설치를 요청할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 작업 14에서 파일 또는 해시가 악성이 아닌 경우 다음 작업을 수행합니다.

a. 작업 15에서는 사용자의 역할(중요한 정보를 처리하는 부서 또는 직위), 애플리케이션 유형(랜섬웨어, 루트킷 등) 및 애플리케이션의 영향(영향을 받은 사용자 수)에 따라 파일/해시가 위험도가 높은지 낮은 위험인지 확인해야 합니다.

b. 작업 16에서 파일이 고위험 파일인 경우 다음 작업을 수행하십시오.

i. 작업 17에서 위협 인텔리전스 팀과 함께 결과를 검토합니다.

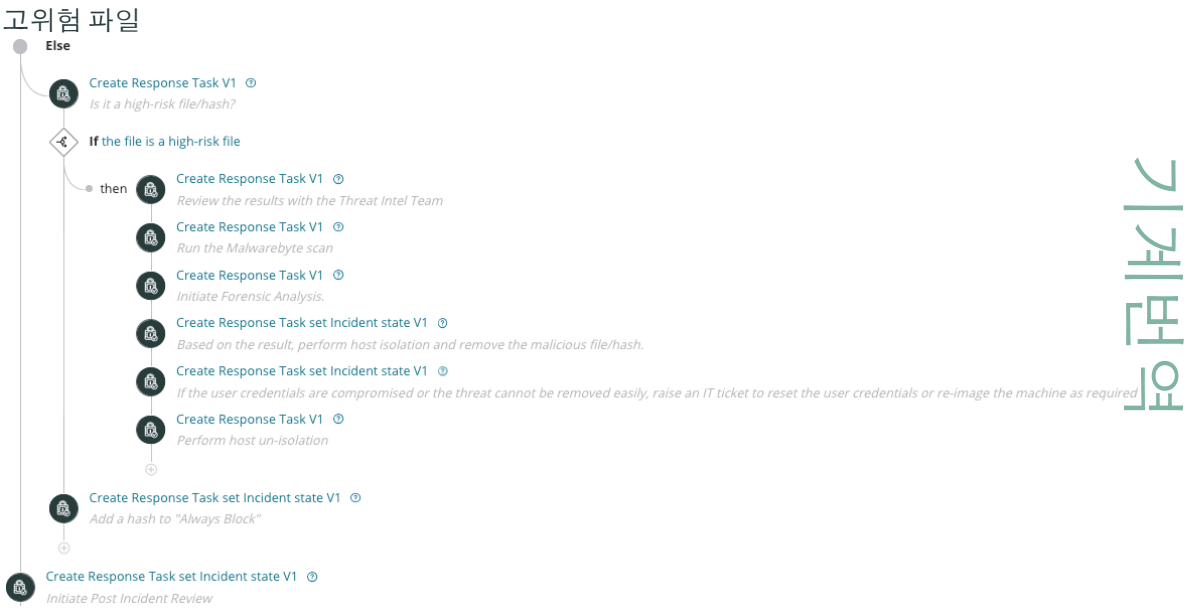
ii. 동작 18에서 파일에 대해 맬웨어 바이트 스캔을 실행합니다.

iii. 조치 19에서 포렌식 분석을 시작합니다.

iv. 작업 20에서는 포렌식 분석 결과에 따라 호스트 격리를 수행하고 악성 파일/해시를 제거합니다.

v. Action 21에서 사용자 자격 증명이 손상되거나 위협을 쉽게 제거할 수 없는 경우 IT 티켓을 제기하여 사용자 자격 증명을 재설정하거나 필요에 따라 컴퓨터를 이미지로 다시 설치합니다.

vi. 작업 22에서 호스트 격리 해제를 수행합니다.



c. 작업 23에서 파일이 고위험 파일이 아닌 경우 다음 작업을 수행합니다.

i. 다음으로 이동 크라우드스트라이크 팔콘 〉 구성 탭.

ii. 구성 탭에서 예방 해시 〉 〉 해시 업로드 〉 해시 추가.

iii. 필요한 OS를 선택하고 항상 차단을 선택합니다.

5. 작업 24에서는 사용자가 작업을 닫기 전에 사후 인시던트 검토를 완료할 수 있도록 응답 작업이 생성됩니다.

암호 스프레이 가능성에 대한 플레이북

이 플레이북은 여러 번의 로그인 실패로 인해 트리거되는 암호 스프레이 경보를 조사하기 위한 체계적인 정정 단계를 제공합니다(동일한 사용자에 대해 둘 이상의 IP 주소에서 너무 많은 인증 실패).

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

가능한 암호 스프레이 플레이북 설정

다음 단계를 사용하여 가능한 암호 스프레이 플레이북을 설정합니다.

시작하기 전에

필요한 역할:

- sn_si.admin
- flow_designer

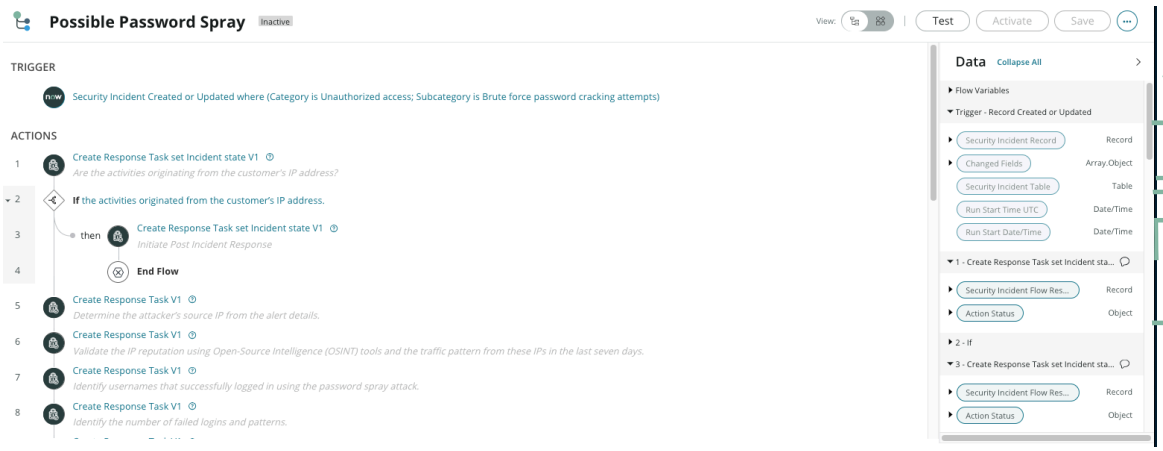
Security Operations 스포크(*sn_sec_spoke*)를 설치했는지 확인하십시오.

프로시저

1. sn_si.user 및 flow_designer 역할을 가진 사용자로 로그인합니다.
2. 다음으로 이동 모두 〉 플로우 디자이너 을 클릭하고 가능한 암호 스프레이 플레이북을 선택합니다.
3. 옵션: 가능한 암호 스프레이 플레이북 플로우의 사본을 생성하고 필요에 따라 수정할 수 있습니다.

   플레이북 플로우의 사본을 생성하려면 아이콘을 클릭하고 플로우 복사를 선택합니다.
   플로우를 사용자 지정하거나 특정 변경을 수행하려는 경우에만 이 단계를 수행합니다.

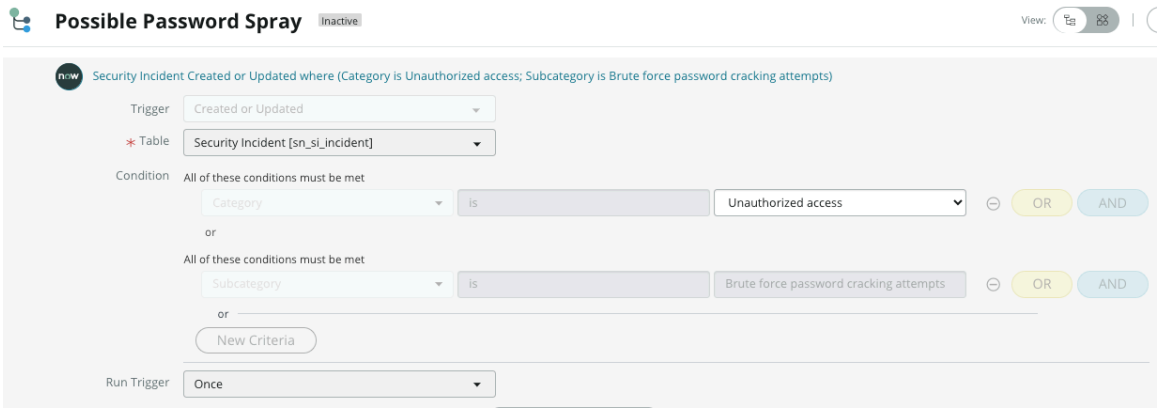
   가능한 암호 스프레이 플레이북



4. 플레이북을 활성화합니다.
   - 기본 시스템에서 사용할 수 있는 플레이북을 사용하려면 메인 플로우를 활성화합니다.
   - 필요한 사항을 변경한 후 복사된 플로우를 활성화합니다.
5. 플레이북에 대한 트리거 조건을 설정합니다.
   다음 조건이 충족되면 이 플레이북이 트리거되고 보안 인시던트와 연결됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 범주 는 무단 접근입니다.
- 하위 범주 는 무차별 암호 대입 공격 시도입니다.



가능한 암호 스프레이 플레이북 사용

이 플레이북을 사용하여 여러 번의 로그인 실패로 인해 트리거되는 암호 스프레이 경보를 조사합니다(동일한 사용자에 대해 둘 이상의 IP 주소에서 너무 많은 인증 실패). 다음 단계에서는 가능한 암호 스프레이 플레이북에서 사용할 수 있는 작업, 작업 및 하위 플로우에 대한 안내를 제공합니다.

시작하기 전에
필요한 역할:

- sn_si.admin
- flow_designer

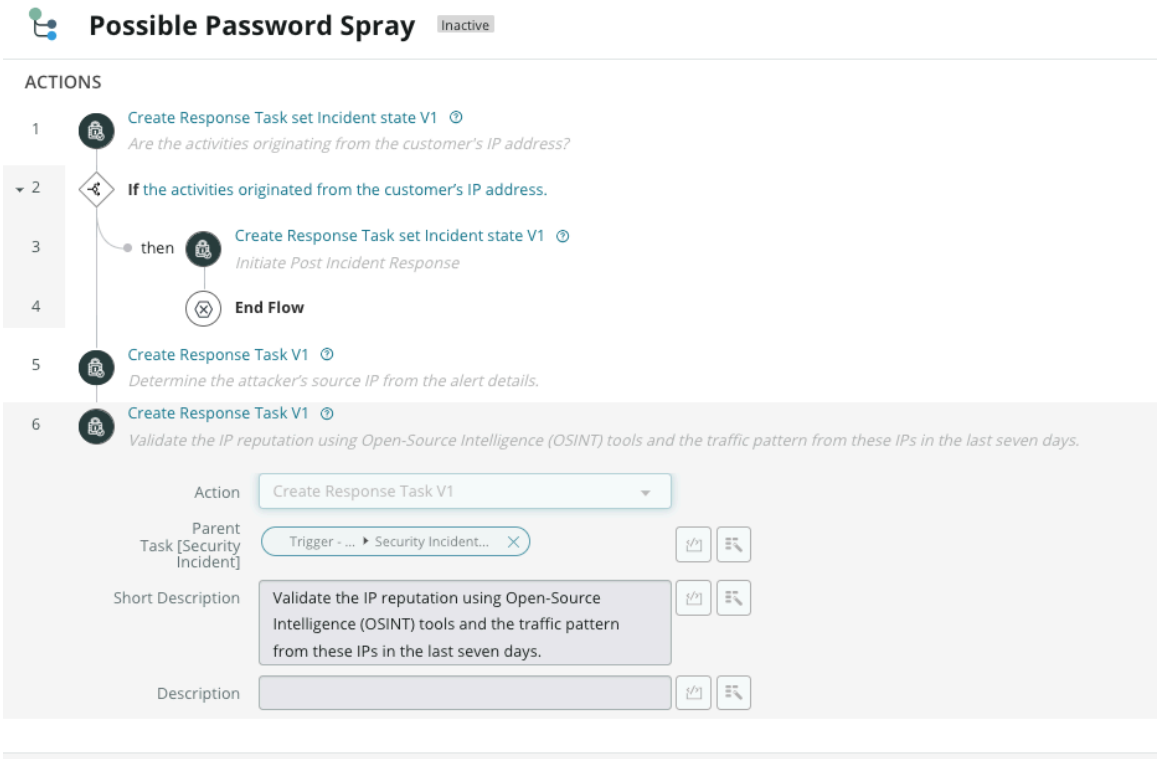
Security Operations 스포크(*sn_sec_spoke*)를 설치했는지 확인하십시오.

프로시저

1. 플레이북이 트리거되고 실행이 시작되면 작업 1에서 활동이 고객의 IP 주소에서 시작되었는지 확인해야 합니다.
   암호 스프레이 공격을 수행하는 IP 주소를 식별합니다. 예를 들어 경보의 TXID(트랜잭션 ID)를 사용하고 F5 로그와 비교하여 조회합니다.
2. 작업 2에서 활동이 고객의 IP 주소에서 시작된 경우 다음 작업을 수행합니다.
   a. 작업 3에서는 가능한 암호 스프레이 공격에 대한 사후 인시던트 검토를 시작해야 합니다.
   b. 작업 4에서 흐름이 종료됩니다.
3. 작업 5에서 활동이 고객의 IP 주소에서 시작되지 않은 경우 경고 세부 정보에서 공격자의 원본 IP를 확인합니다.
4. 작업 6에서는 OSINT(Open-Source Intelligence) 툴을 사용하여 IP 평판과 지난 7일 동안 이러한 IP의 트래픽 패턴을 검증해야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

가능한 암호 스프레이 플레이북

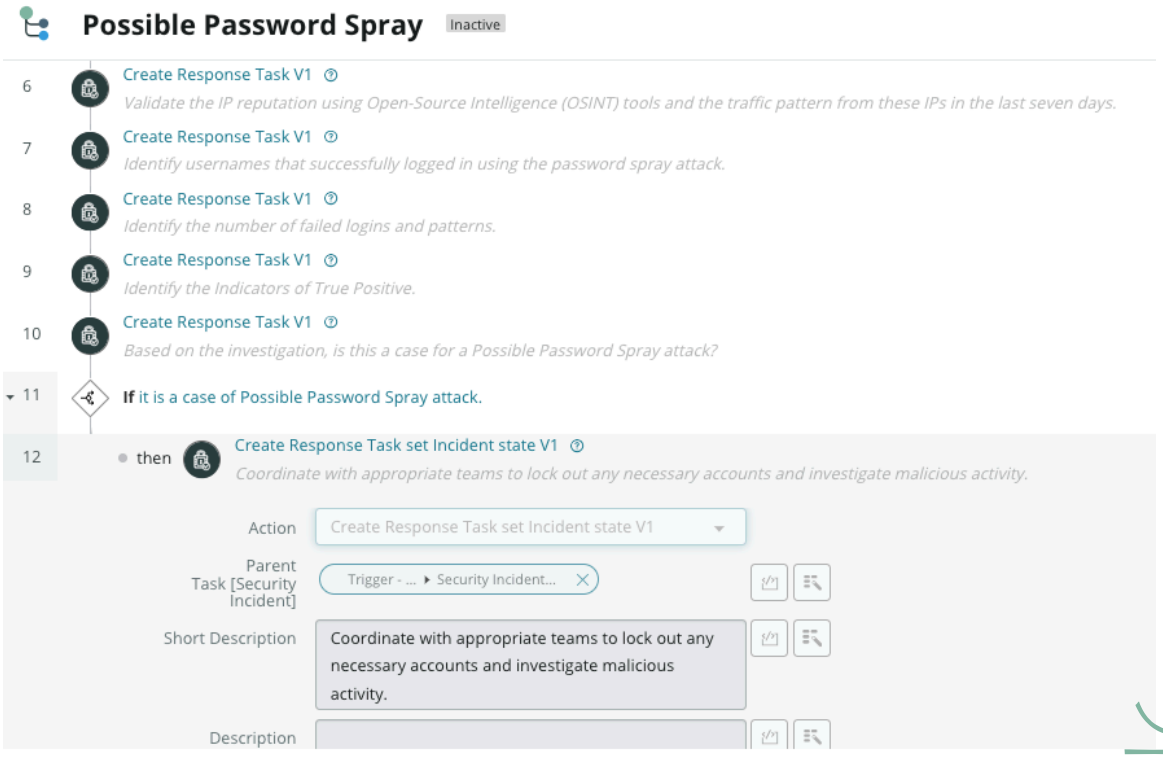


5. 작업 7에서는 암호 스프레이 공격을 사용하여 성공적으로 로그인한 사용자 이름을 식별해야 합니다.
6. 작업 8에서는 실패한 로그인 및 패턴 수를 식별해야 합니다.
7. 작업 9에서는 진양성 표시기를 식별해야 합니다.
   - 지난 60일 동안 소스 IP의 트래픽을 확인합니다. 어떤 과거 트래픽도 진정한 긍정의 표시가 될 수 없습니다.
   - 인증 실패가 있는 사용자 이름 패턴과 개수를 확인합니다. 개수가 높을수록 진양성일 확률이 높습니다.
   - 사용자 이름은 딕셔너리 기반(A부터 Z까지)처럼 보이며 admin, sysadmin, root 등과 같은 일반적인 관리자 이름을 가질 수 있습니다
   - john.doe, johnd, jdoe, john_doe, jdoe7 등에 대해 동일한 경보에 오류가 있을 수 있는 것처럼 동일한 사용자 이름이 스프레이 공격에서 다른 패턴을 가질 수 있으며, 이는 공격자가 일반적인 사용 사례를 기반으로 사용자 이름 패턴을 추측함을 나타냅니다.
   - 위 단계의 F5 로그에서 사용자 에이전트와 URI를 확인하고 IOC가 Red Condor 경고와 관련이 있는지 확인합니다. 일치하면 진정한 긍정 이벤트입니다.
8. Action 10에서는 지금까지 수행된 조사를 기반으로 이것이 Possible Password Spray 공격의 경우인지 여부를 확인해야 합니다.
9. 작업 11에서 암호 스프레이 공격이 가능한 경우 다음 작업을 수행하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 작업 12에서는 적절한 팀과 협력하여 필요한 계정을 잠그고 악의적인 활동을 조사해야 합니다.

가능한 암호 스프레이 플레이북



b. 작업 13에서는 가능한 암호 스프레이 공격에 대한 사후 인시던트 검토를 시작해야 합니다.

c. 액션 14에서는 플로우가 끝납니다.

10. 작업 15에서 이것이 암호 스프레이 공격의 경우가 아닌지 확인해야 합니다.

11. 작업 16에서 가능한 암호 스프레이 공격의 경우가 아닌 경우 다음 작업을 수행합니다.

a. Action 17에서는 지금까지의 결과를 문서화해야 합니다.

b. 작업 18에서는 가능한 암호 스프레이 공격에 대한 사후 인시던트 검토를 시작해야 합니다.

c. 동작 19에서 흐름이 끝납니다.

12. 작업 20에서는 동료 및 GIR 관리자와 지침을 참조해야 합니다.

13. 작업 21에서는 작업을 종결하기 전에 사후 인시던트 검토를 완료하기 위한 응답 작업이 생성됩니다.

T1003용 플레이북 - 자격 증명 덤핑 도구 탐지

이 플레이북은 자격 증명 덤핑 활동과 관련된 인시던트를 조사하기 위한 체계적인 정정 단계를 제공합니다.

T1003 - 자격 증명 덤핑 도구 검색 플레이북 설정

다음 단계를 사용하여 T1003 - 자격 증명 덤핑 도구 검색 플레이북을 설정합니다.

시작하기 전에
필요한 역할:

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- sn_si.admin
- flow_designer

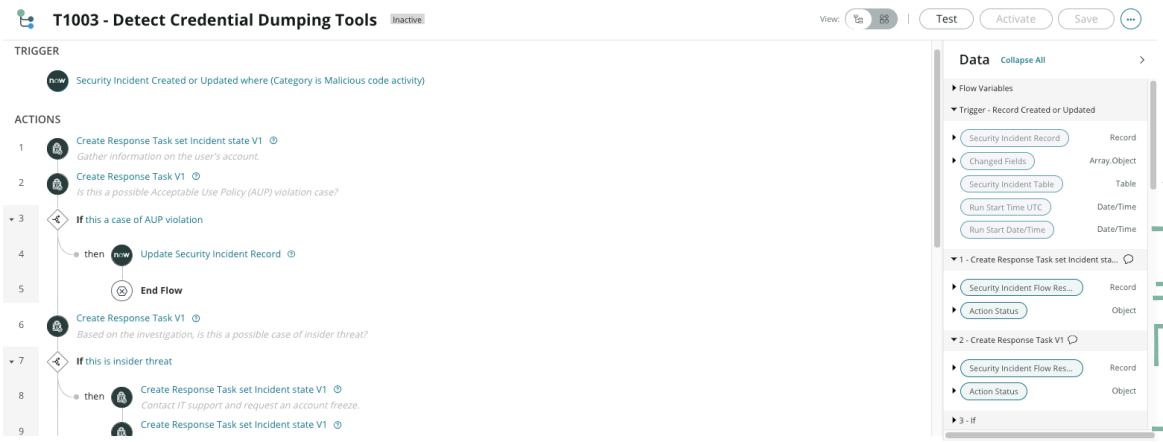
Security Operations 스포크(*sn_sec_spoke*)를 설치했는지 확인하십시오.

프로시저

1. sn_si.user 및 flow_designer 역할을 가진 사용자로 로그인합니다.
2. 다음으로 이동 모두 〉 플로우 디자이너 을 클릭하고 **T1003 -** 자격 증명 덤핑 도구 검색 플레이북을 선택합니다.
3. 옵션: T1003 - 자격 증명 덤핑 도구 탐지 플레이북 플로우의 복사본을 생성하고 필요에 따라 수정할 수 있습니다.

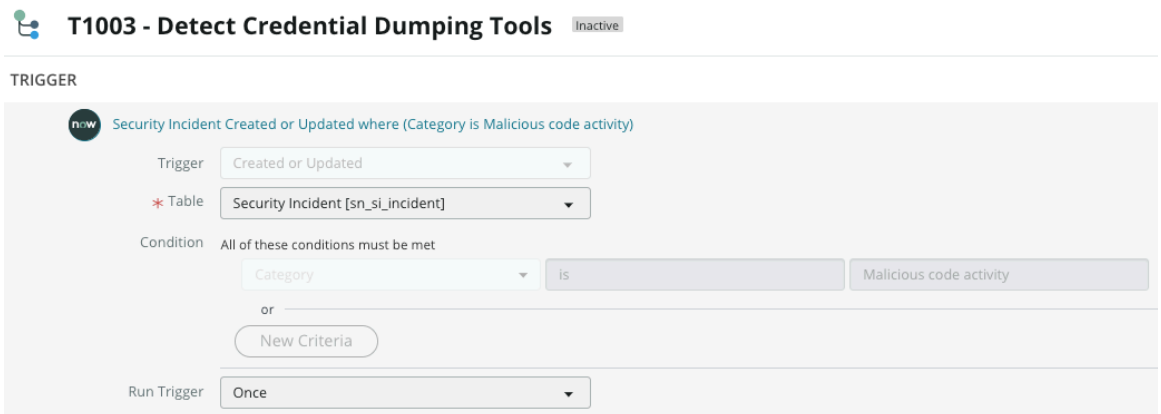
   플레이북 플로우의 사본을 생성하려면 ••• 아이콘을 클릭하고 플로우 복사를 선택합니다. 플로우를 사용자 지정하거나 특정 변경을 수행하려는 경우에만 이 단계를 수행합니다.

   T1003 - 자격 증명 덤핑 도구 검색 플레이북



4. 플레이북을 활성화합니다.
   - 기본 시스템에서 사용할 수 있는 플레이북을 사용하려면 메인 플로우를 활성화합니다.
   - 필요한 사항을 변경한 후 복사된 플로우를 활성화합니다.
5. 플레이북에 대한 트리거 조건을 설정합니다.

   이 Playbook은 범주 가 악성 코드 활동일 때 트리거되고 보안 인시던트와 연결됩니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

T1003 - 자격 증명 덤핑 도구 검색 플레이북 사용

이 플레이북을 사용하여 자격 증명 덤핑 활동과 관련된 인시던트를 조사합니다. 다음 단계에서는 T1003 - 자격 증명 덤핑 도구 탐지 플레이북에서 사용할 수 있는 작업, 작업 및 하위 플로우에 대한 안내를 제공합니다.

시작하기 전에

필요한 역할:

- sn_si.admin
- flow_designer

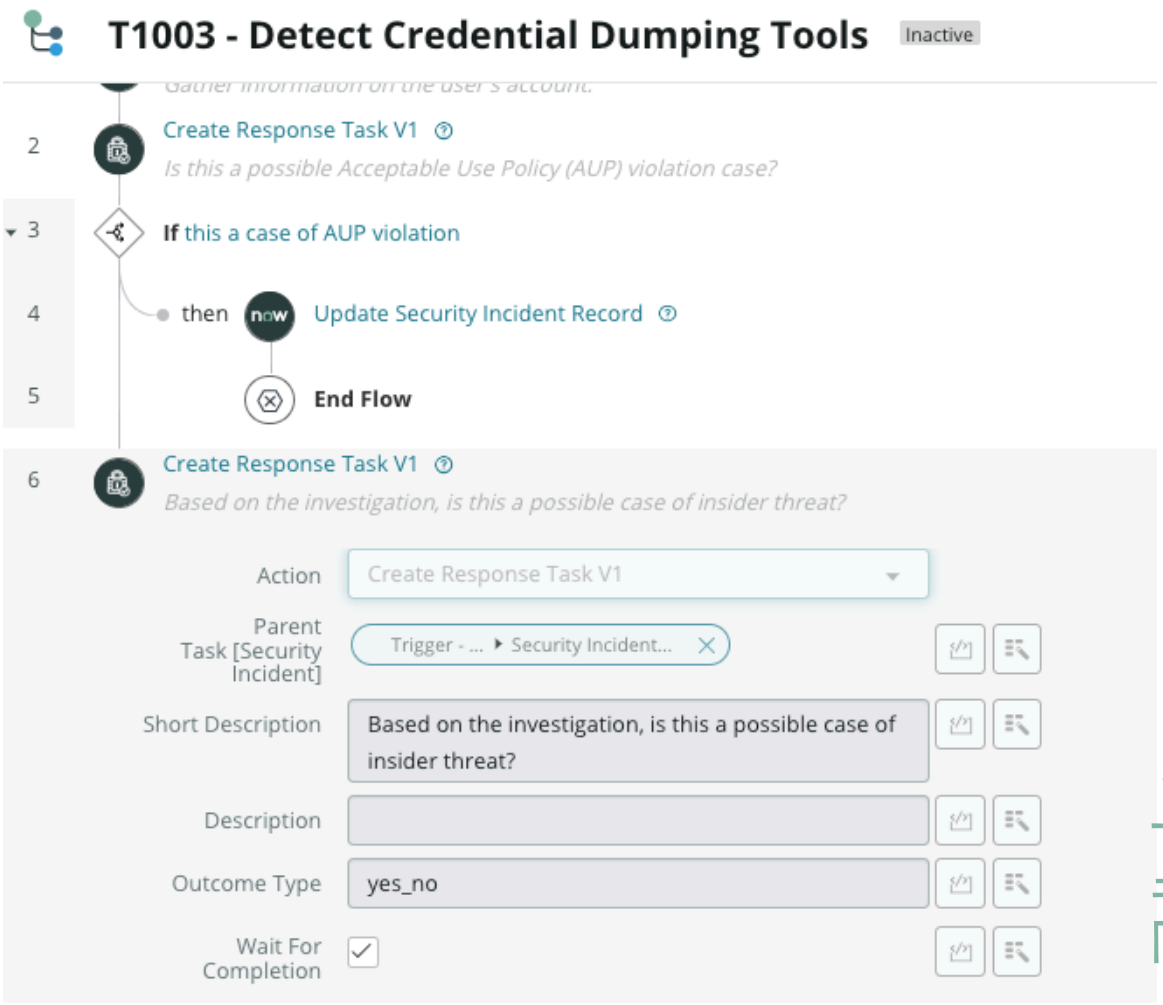
Security Operations 스포크(*sn_sec_spoke*)를 설치했는지 확인하십시오.

프로시저

1. 플레이북이 트리거되고 실행이 시작되면 작업 1에서 사용자 계정에 대한 정보를 수집해야 합니다.
   - 의심스러운 활동을 찾으려면 호스트 활동을 확인해야 합니다.
   - 서버/엔드포인트/VM의 소유자를 식별하고 도구와 상관 관계가 있는 데이터를 캡처해야 합니다.
   - 사용자의 다른 계정에 대한 정보를 수집해야 합니다.
2. 작업 2에서는 이것이 가능한 AUP(제한적 사용 정책) 위반 사례인지 확인해야 합니다. 수집한 증거를 가지고 동료 검토를 수행하고 해당 사용자에게 연락할지 여부를 지역 인시던트 관리자와 상의할 수 있습니다.
3. 작업 3에서 이것이 제한적 사용 정책(AUP) 위반인 경우 다음 작업을 수행합니다.
   a. 작업 4에서는 AUP 위반 사례라는 보안 인시던트를 업데이트해야 합니다.
   b. 작업 5에서 플로우가 종료됩니다.
4. 작업 6에서는 지금까지 수행된 조사에 따라 이것이 내부자 위협의 가능한 사례인지 여부를 확인해야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

T1003 - 자격 증명 덤핑 도구 검색 플레이북



기계번역

5. 작업 7에서 내부자 위협인 경우 다음 작업을 수행합니다.

a. 작업 8에서는 IT 지원에 문의하여 계정 동결을 요청해야 합니다.

b. 작업 9에서는 악성 IP를 차단해야 합니다.

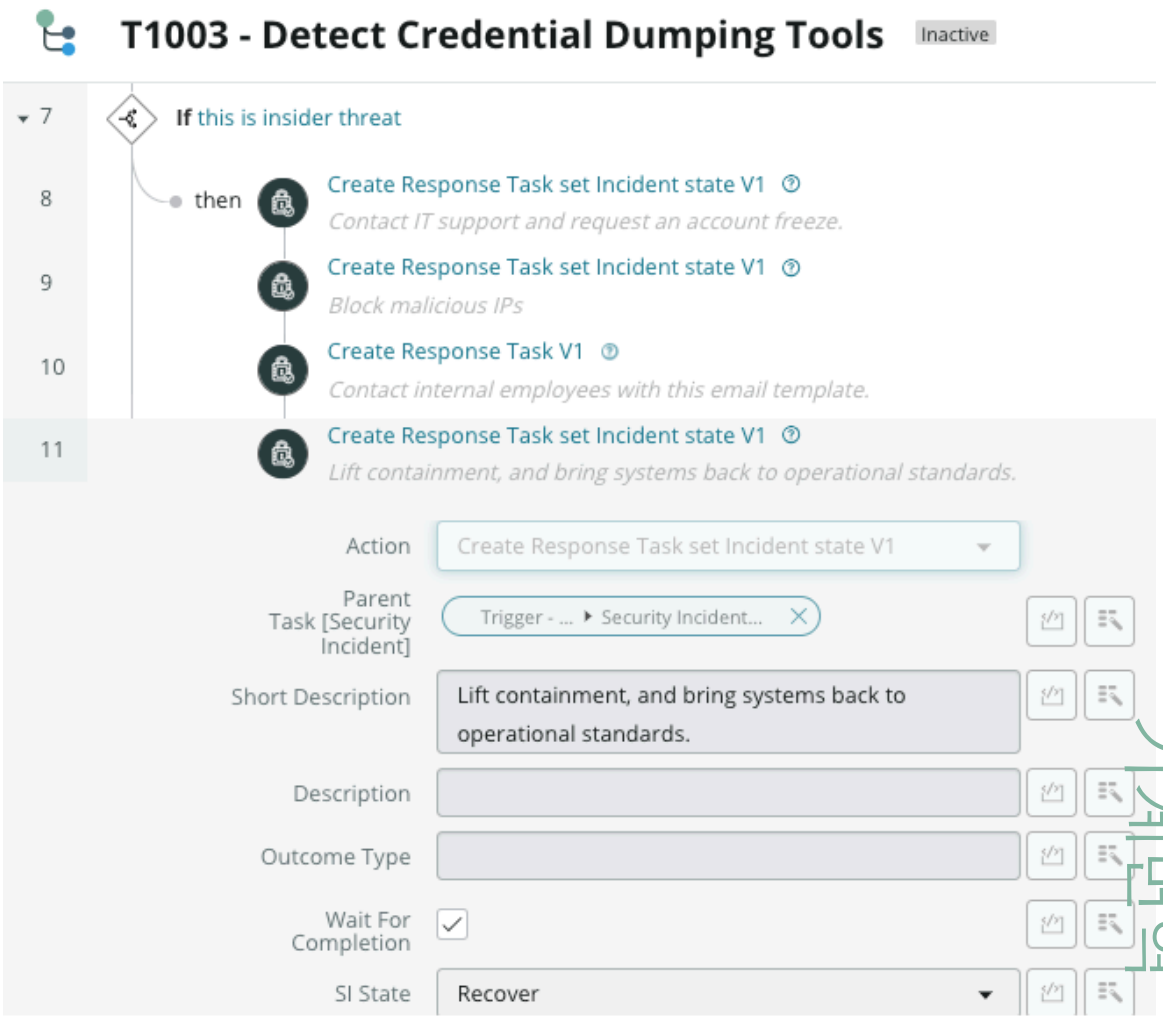
c. 작업 10에서는 이메일을 통해 내부 직원에게 연락해야 합니다.
제공된 이메일 템플릿을 사용하여 내부 직원에게 연락할 수 있습니다.

d. Action 11에서는 봉쇄를 해제하고 시스템을 작동 표준으로 되돌려야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

플로우가 종료됩니다.

봉쇄를 해제하기 위한 대응 작업



6. 작업 12에서 내부자 위협의 경우가 아닌 경우 작업 13에서 동료 검토를 수행하여 제외 목록에 추가해야 하는지 여부를 결정해야 합니다.
   플로우가 종료됩니다.
7. 작업 14에서는 작업을 종결하기 전에 사후 인시던트 검토를 완료하기 위한 응답 작업이 생성됩니다.

이메일 도메인 스푸핑 탐지를 위한 플레이북

이 플레이북은 분석가에게 피셔의 이메일 주소에 유사한 도메인이 있을 가능성을 경고하여 사용자가 보고한 피싱 제출을 초기 스테이지에서 분류하는 데 도움이 됩니다.

이메일 도메인 스푸핑 탐지 플레이북은 옵저버블 리포지토리에 신뢰할 수 있는 도메인 이름이 있는 피셔의 보낸 사람 이메일 도메인 간의 유사성 일치를 찾습니다. 플레이북에서 스푸핑된 발신자 이메일 도메인 일치가 식별되면 분석가에게 태그가 포함된 알림이 전송됩니다.

워크플로우는 인시던트 조사를 위한 일관되고 효율적인 접근 방식을 제공하는 기존 플레이북을 기반으로 생성됩니다. 플레이북의 각 결정 지점은 결과 기반 작업으로 변환되었으며 이러한 작업의 결과에 따라 플로우의 방향이 변경됩니다.

이메일 스푸핑 탐지 플레이북 설정

다음 단계를 사용하여 이메일 스푸핑 탐지 플레이북을 설정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할:

- sn_si.admin
- flow_designer

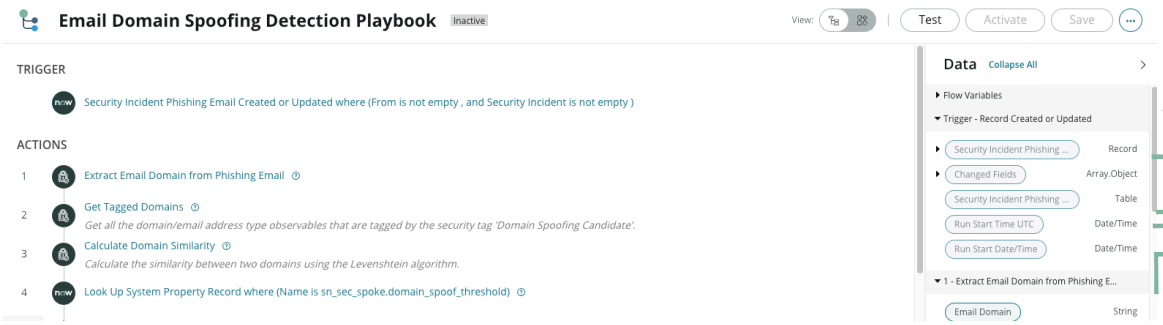
Security Operations 스포크(*sn_sec_spoke*)를 설치했는지 확인하십시오.

프로시저

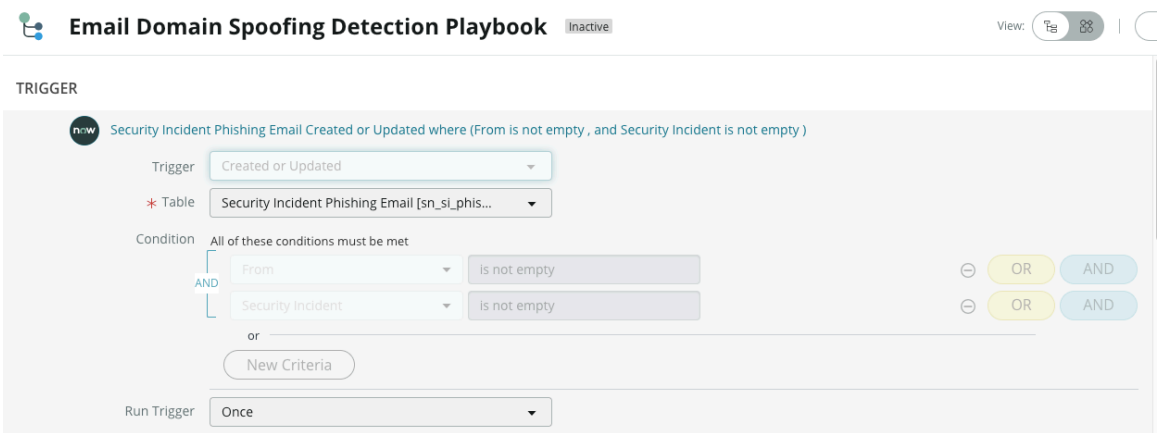
1. sn_si.user 및 flow_designer 역할을 가진 사용자로 로그인합니다.
2. 다음으로 이동 모두 〉 플로우 디자이너 을 클릭하고 이메일 도메인 스푸핑 탐지 플레이북 플레이북을 선택합니다.
3. 옵션: 이메일 도메인 스푸핑 탐지 플레이북 플로우의 사본을 생성하고 필요에 따라 수정할 수 있습니다.

   플레이북 플로우의 사본을 생성하려면 ••• 아이콘을 클릭하고 플로우 복사를 선택합니다. 플로우를 사용자 지정하거나 특정 변경을 수행하려는 경우에만 이 단계를 수행합니다.

   이메일 도메인 스푸핑 탐지 **Playbook**



4. 플레이북을 활성화합니다.
   - 기본 시스템에서 사용할 수 있는 플레이북을 사용하려면 메인 플로우를 활성화합니다.
   - 필요한 사항을 변경한 후 복사된 플로우를 활성화합니다.
5. 플레이북에 대한 트리거 조건을 설정합니다.
   다음 조건이 충족되면 이 플레이북이 트리거되고 보안 인시던트와 연결됩니다.
   - 보낸 사람이 비어 있지 않습니다.
   - 보안 인시던트 는 비어 있지 않습니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이메일 도메인 스푸핑 탐지 플레이북 사용

이 플레이북을 사용하여 신뢰할 수 있는 도메인 이름을 가진 피셔의 보낸 사람 이메일 도메인이 옵저버블 리포지토리에 있는 유사성 일치를 찾습니다. 다음 단계에서는 이메일 도메인 스푸핑 탐지 플레이북에서 사용할 수 있는 작업, 작업 및 하위 플로우에 대한 안내를 제공합니다.

시작하기 전에
필요한 역할:

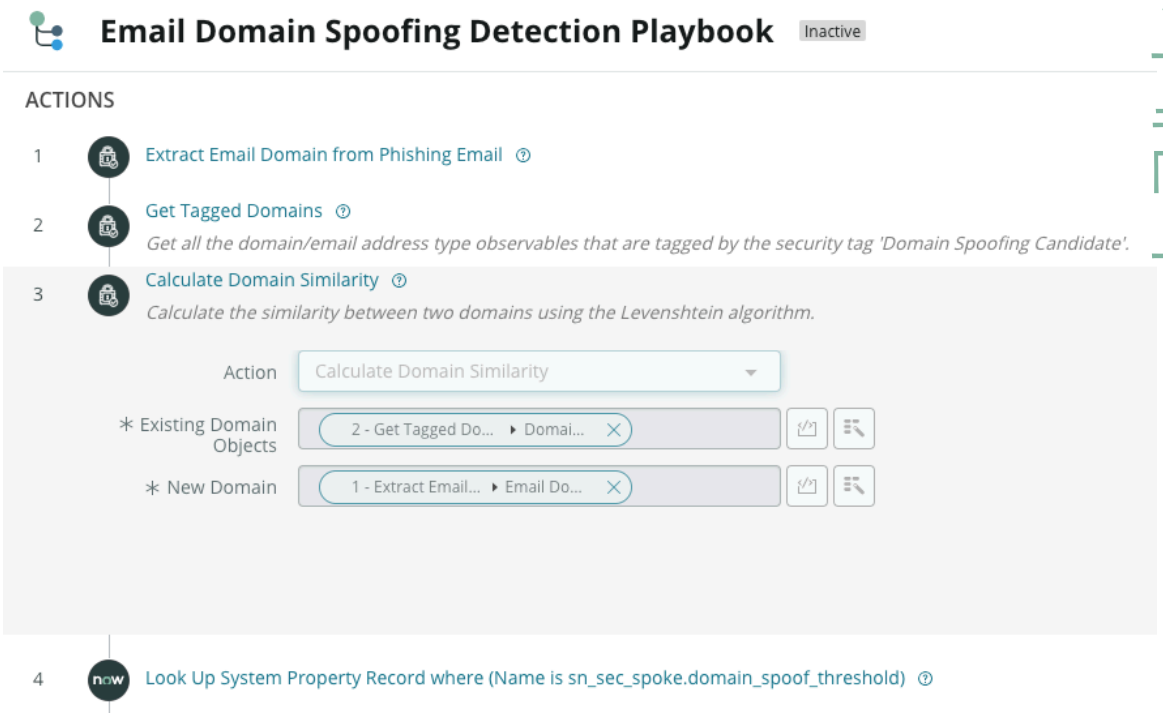
- sn_si.admin
- flow_designer

Security Operations 스포크(*sn_sec_spoke*)를 설치했는지 확인하십시오.

프로시저

1. 플레이북이 트리거되고 실행이 시작되면 작업 1에서 플레이북이 피싱 이메일에서 이메일 도메인을 추출합니다.
2. 작업 2에서 Playbook은 보안 태그 "도메인 스푸핑 후보"로 태그가 지정된 모든 도메인/이메일 주소 유형 옵저버블을 검색합니다.
3. 작업 3에서 플레이북은 Levenshtein 알고리즘을 사용하여 Get Tagged 도메인과 이메일 도메인 간의 유사성을 계산합니다.

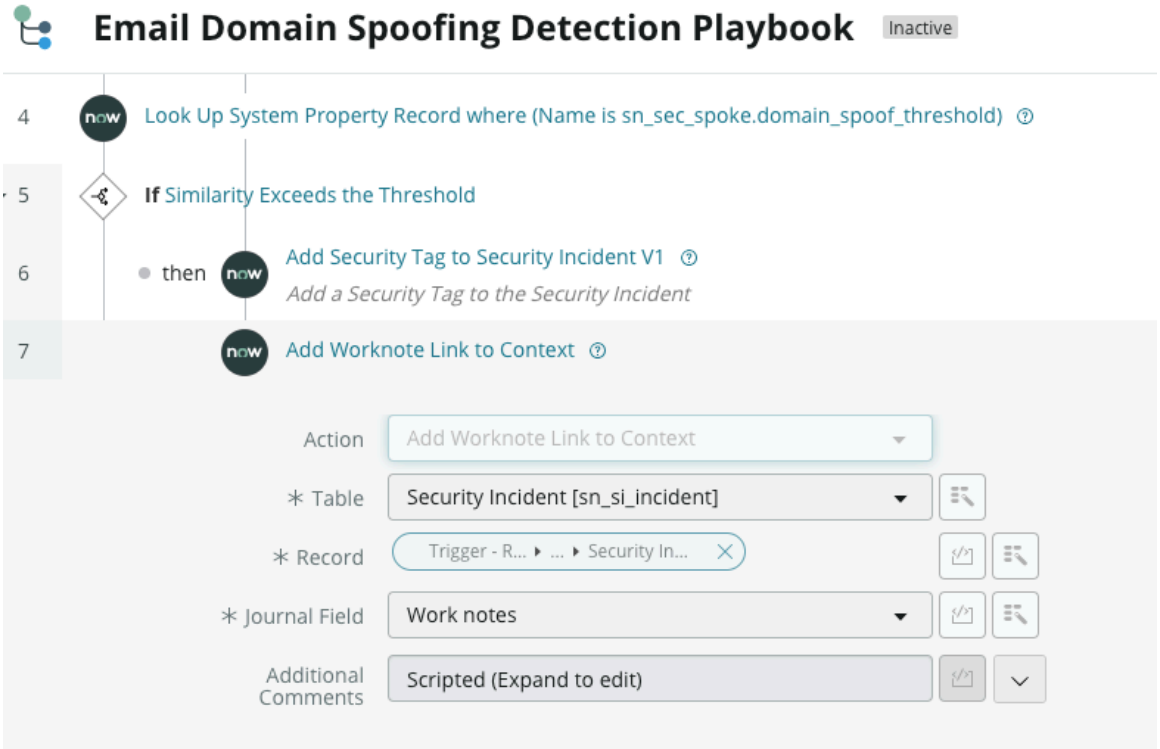
이메일 도메인 스푸핑 탐지 **Playbook**



4. 작업 4에서 플레이북은 다음 조건에 따라 시스템 속성 기록을 찾습니다.
   - 이름은 sn_sec_spoke.domain_spoof_threshold,(또는)
   - 이름은 a부터 z까지이며, 기록이 여러 개 발견되면 첫 번째 기록만 반환합니다.
5. 작업 5에서는 지금까지 수행된 조사를 기반으로 플레이북이 두 도메인의 유사성이 임계치를 초과하는지 여부를 확인합니다.
   두 도메인의 유사성이 임계치를 초과하지 않으면 작업 5에서 수동 응답 작업이 생성되고 플로우가 종료됩니다. 두 도메인의 유사성이 임계치를 초과하면 작업 6과 7이 실행됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

유사성이 임계치를 초과함



6. 작업 6에서 플레이북은 보안 인시던트에 이메일 도메인 스푸핑 보안 태그를 추가합니다.
7. 작업 7에서 플레이북은 스크립트 옵션을 사용하여 컨텍스트에 작업 메모 링크를 추가합니다.
8. 작업 8에서 플로우가 종료됩니다.

오타에 대한 플레이북 스쿼트 도메인

이 플레이북은 철자가 잘못된 도메인을 조사하고 조직의 법무 부서와 공동 작업하여 중단을 방지하기 위한 체계적인 절차를 제공합니다. 오타가 있는 도메인은 합법적인 도메인 이름과 매우 유사한 의도적으로 철자가 틀린 도메인 이름입니다. 공격자는 철자 오류를 이용하여 재정적 착취 또는 기타 악의적인 활동을 위해 악의적인 웹 사이트로 유도합니다.

오타 스쿼트 도메인은 디지털 위험 보호 솔루션(Digital Shadows) 및 위협 인텔리전스 플랫폼(Anomali Threatstream)과 같은 다양한 소스에서 보안 운영 팀에 보고됩니다. 보안 인시던트가 생성되면 이 솔루션은 도메인이 실제로 오타 스쿼트 도메인인지 식별하는 데 도움이 됩니다. 오타가 있는 도메인인 경우 분석가는 추가 조치를 취할 수 있도록 법무팀에 보고할 수 있습니다.

워크플로우는 인시던트 조사를 위한 일관되고 효율적인 접근 방식을 제공하는 기존 플레이북을 기반으로 생성됩니다. 플레이북의 각 결정 지점은 결과 기반 작업으로 변환되었으며 이러한 작업의 결과에 따라 흐름의 방향이 변경됩니다.

오타 무단 점유 도메인 플레이북 설정

다음 단계를 사용하여 오타 무단 점유 도메인 플레이북을 설정합니다.

시작하기 전에
필요한 역할:

- sn_si.admin
- flow_designer

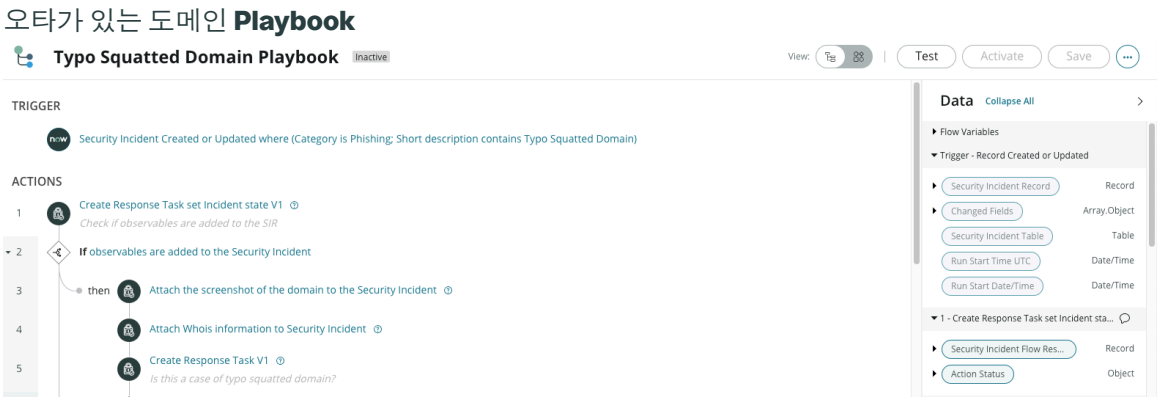
Security Operations 스포크(*sn_sec_spoke*)를 설치했는지 확인하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

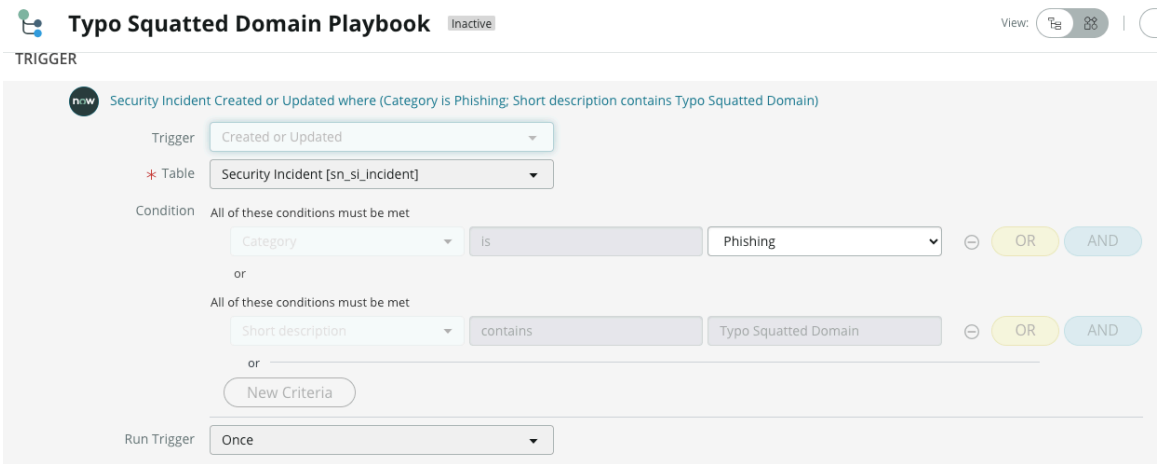
1. sn_si.user 및 flow_designer 역할을 가진 사용자로 로그인합니다.
2. 다음으로 이동 모두 〉 플로우 디자이너 을 클릭하고 **Typo Squatted Domain** 플레이북을 선택합니다.
3. 옵션: 오타 무단 점유 도메인 플레이북 플로우의 사본을 생성하고 필요에 따라 수정할 수 있습니다.

   (Optional) 플레이북 플로우의 사본을 생성하려면 ••• 아이콘을 클릭하고 플로우 복사를 선택합니다. 플로우를 사용자 지정하거나 특정 변경을 수행하려는 경우에만 이 단계를 수행합니다.



4. 플레이북을 활성화합니다.
   - 기본 시스템에서 사용할 수 있는 플레이북을 사용하려면 메인 플로우를 활성화합니다.
   - 필요한 사항을 변경한 후 복사된 플로우를 활성화합니다.
5. 플레이북에 대한 트리거 조건을 설정합니다.

   다음 조건이 충족되면 이 플레이북이 트리거되고 보안 인시던트와 연결됩니다.
   - 범주 는 피싱입니다.
   - 간단한 설명에 오타가 있습니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

오타 무단 점유 도메인 플레이북 사용

이 Playbook을 사용하여 철자가 잘못된 도메인을 조사하고 조직의 법무 부서와 협력하여 게시 중단을 방지합니다. 다음 단계에서는 Typo Squatted Domain 플레이북에서 사용할 수 있는 작업, 작업 및 하위 플로우에 대한 둘러보기를 제공합니다.

시작하기 전에

필요한 역할:

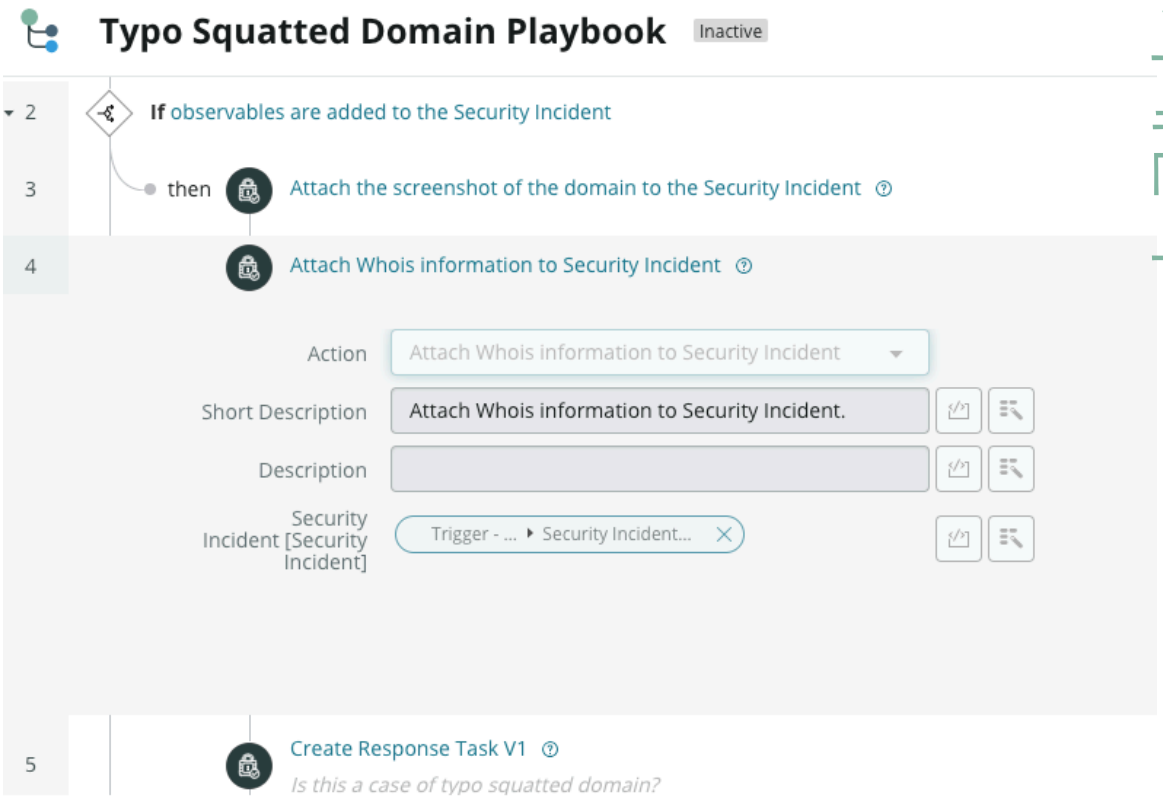
- sn_si.admin
- flow_designer

Security Operations 스포크(*sn_sec_spoke*)를 설치했는지 확인하십시오.

프로시저

1. 플레이북이 트리거되고 실행이 시작되면 작업 1에서 옵저버블이 SIR(보안 인시던트 응답)에 추가되었는지 확인해야 합니다.
   옵저버블이 SIR에 추가되지 않은 경우 계속하기 전에 옵저버블을 추가하십시오. 옵저버블을 사용할 수 없는 경우 작업 10이 실행되고 보안 인시던트가 종결됩니다.
2. 작업 2에서 옵저버블이 보안 인시던트에 추가되면 다음 작업이 실행됩니다.
3. 작업 3에서는 오타 무단 커밋 도메인의 스크린샷을 보안 인시던트에 첨부해야 합니다.

오타가 있는 도메인 **Playbook**



4. 작업 4에서 Whois 정보를 보안 인시던트에 첨부해야 합니다.
5. 작업 5에서 지금까지 수행된 조사를 기반으로 플레이북은 이것이 오타 스쿼트 도메인의 경우인지 여부를 확인합니다.
   오타가 있는 도메인의 경우가 아닌 경우 작업 5에서 수동 응답 작업이 생성되고 플로우가 종료됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

6. 작업 6에서 오타가 있는 도메인의 경우이면 작업 7이 실행됩니다.
7. 작업 7에서는 법무 및 기타 필요한 팀에 이것이 오타 무단 점유 도메인의 경우임을 알리고 이를 근절하는 데 필요한 조치를 취해야 합니다.
   오타가 있는 도메인의 경우가 아닌 경우 작업 5에서 수동 응답 작업이 생성되고 플로우가 종료됩니다.

오타가 있는 경우 스쿼트된 도메인

8. 작업 9에서는 작업을 종결하기 전에 사후 인시던트 검토를 완료하기 위한 응답 작업이 생성됩니다.

자격 증명 스니핑을 위한 플레이북

이 플레이북은 ServiceNow 인스턴스의 테이블을 통해 *sys_installation_exit* 수행된 자격 증명 스니핑 활동과 관련된 인시던트를 조사하기 위한 시스템 정정 단계를 제공합니다.

자격 증명 스니핑 플레이북은 테이블의 기록을 *sys_installation_exit* 사용하여 데이터베이스(DB) 로그인, 1회 사용자 인증(SSO) 및 LDAP(Lightweight Directory Access Protocol)를 처리하는 스크립트 필드를 제공합니다. 이러한 권한 있는 스크립팅 필드를 사용하면 로그인 중에 사용자 이름 및 암호와 같은 사용자 자격 증명을 포함하여 인스턴스에 대한 사용자 요청 및 매개변수를 수신할 수 있습니다.

악의적인 사용자가 스크립트를 만들어 사용자 요청을 수신하고 이러한 요청을 인스턴스에 기록할 수 있습니다. *sys_installation_exit* 인스턴스의 테이블은 해당 인스턴스에서 모든 사용자의 로그인 및 로그아웃 활동을 처리하는 규칙을 정의합니다.

자격 증명 스니핑 플레이북 설정

다음 단계를 사용하여 자격 증명 스니핑 플레이북을 설정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할:

- sn_si.admin
- flow_designer

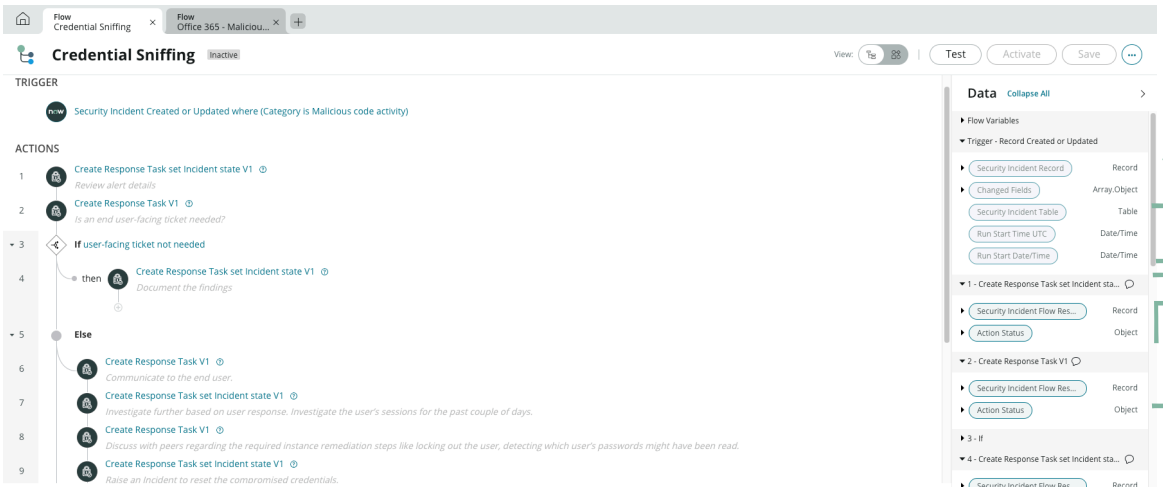
Security Operations 스포크(*sn_sec_spoke*)를 설치했는지 확인하십시오.

프로시저

1. sn_si.user 및 flow_designer 역할을 가진 사용자로 로그인합니다.
2. 다음으로 이동 모두 〉 플로우 디자이너 을 클릭하고 자격 증명 스니핑 플레이북을 선택합니다.
3. 옵션: 자격 증명 스니핑 플레이북 플로우의 복사본을 생성하고 필요에 따라 수정합니다.

   (Optional) 플레이북 플로우의 복사본을 생성하려면 아이콘을 선택하고 플로우 복사를 선택합니다. 플로우를 사용자 지정하거나 특정 변경을 수행하려는 경우에만 이 단계를 수행합니다.

   자격 증명 스니핑 플레이북

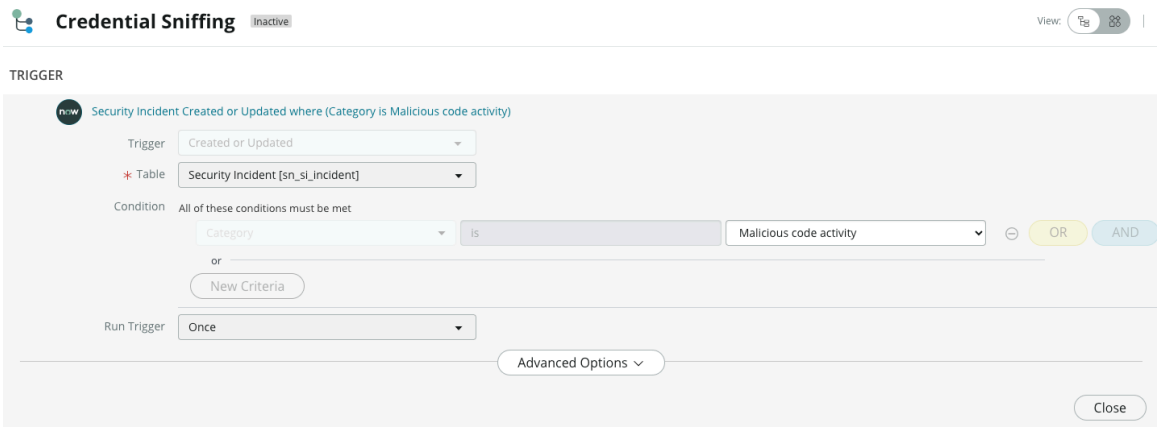


4. 플레이북을 활성화합니다.
   a. 기본 시스템에서 사용할 수 있는 플레이북을 사용하려면 메인 플로우를 활성화합니다.
   b. 필요한 사항을 변경한 후 복사된 플로우를 활성화합니다.
5. 플레이북에 대한 트리거 조건을 설정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 Playbook은 범주 가 악성 코드 활동일 때 트리거되고 보안 인시던트와 연결됩니다.

자격 증명 스니핑 플레이북 트리거 조건



자격 증명 스니핑 플레이북 사용

이 Playbook을 사용하여 ServiceNow 인스턴스의 테이블을 통해 수행된 자격 증명 스니핑 활동과 *sys_installation_exit* 관련된 인시던트를 조사합니다. 다음 단계에서는 자격 증명 스니핑 플레이북에서 사용할 수 있는 작업, 작업 및 하위 플로우에 대한 안내를 제공합니다.

시작하기 전에

필요한 역할:

- sn_si.admin
- flow_designer

프로시저

1. 플레이북이 트리거되고 실행이 시작되면 작업 1에서 다음 경보 상세 정보를 검토합니다.
   - 인스턴스
   - 세션 ID
   - 트랜잭션 ID
   - _raw: 전체 스크립트를 제공합니다.

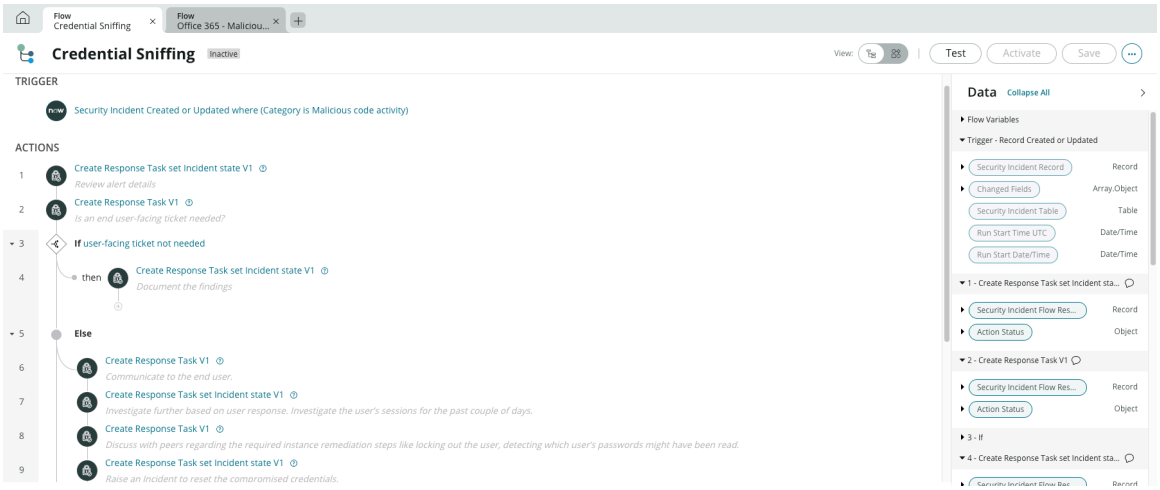
     예시 스크립트:

     ```
     Var pass= request.getParameter(“user_password”);
     Gs.log(pass);
     ```

2. 작업 2에서는 지금까지 수집된 데이터를 기반으로 이 경보에 최종 사용자 티켓이 필요한지 여부를 확인합니다.
3. 작업 3에서 경보에 최종 사용자 티켓이 필요하지 않은 경우 작업 4에서 지금까지의 결과를 문서화합니다.
   플로우가 종료됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

자격 증명 스니핑 플레이북



4. 작업 5에서 경보에 최종 사용자 티켓이 필요한 경우 다음 단계를 수행합니다.

a. 작업 6에서 경보에는 최종 사용자 티켓이 필요하다는 것을 최종 사용자에게 알립니다.

b. 작업 7에서는 지난 며칠 동안 사용자의 응답과 사용자의 세션을 기반으로 추가로 조사합니다.

c. 작업 8에서는 사용자 잠금 및 읽혔을 수 있는 사용자의 암호 탐지와 같은 인스턴스의 정정 단계에 대해 동료들과 논의합니다.

d. 작업 9에서 인시던트 또는 티켓을 제기하여 손상된 사용자 자격 증명을 재설정합니다.

e. Action 10에서는 격납고를 해제하고 시스템을 작동 표준으로 되돌립니다.
플로우가 종료됩니다.

5. 작업 11에서 작업을 종결하기 전에 사후 인시던트 검토를 완료합니다.

T1070용 플레이북 - **Windows** 이벤트 로그 지워짐

이 플레이북은 사용자가 보안 로그를 제거하는 이벤트 유형을 추적하는 인시던트를 조사하기 위한 정정 단계를 제공합니다. 보안 로그가 지워질 때마다 감사 시스템 이벤트 정책 상태에 관계없이 이벤트 517 및 1102가 기록됩니다.

이 경보는 다음과 같은 유형의 이벤트를 추적할 수 있습니다.

- 이벤트 **517**: 기본 사용자 이름 및 클라이언트 사용자 이름 필드는 로그를 지운 사용자를 식별합니다. 기본 사용자 이름은 시스템에 해당하며 클라이언트 사용자 이름은 로그를 지운 사용자를 나타냅니다.
- 이벤트 **1102**: 계정 이름 및 도메인 이름 필드는 로그를 지운 사용자를 식별합니다. 로그온 ID를 사용하면 로그온 이벤트 및 동일한 로그온 세션 동안 기록된 다른 이벤트와 역방향 상관 관계를 지정할 수 있습니다.

T1070 설정 - **Windows** 이벤트 로그 지워짐 플레이북

다음 단계를 사용하여 T1070 - Windows 이벤트 로그 지워짐 플레이북을 설정합니다.

시작하기 전에
필요한 역할:

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- sn_si.admin
- flow_designer

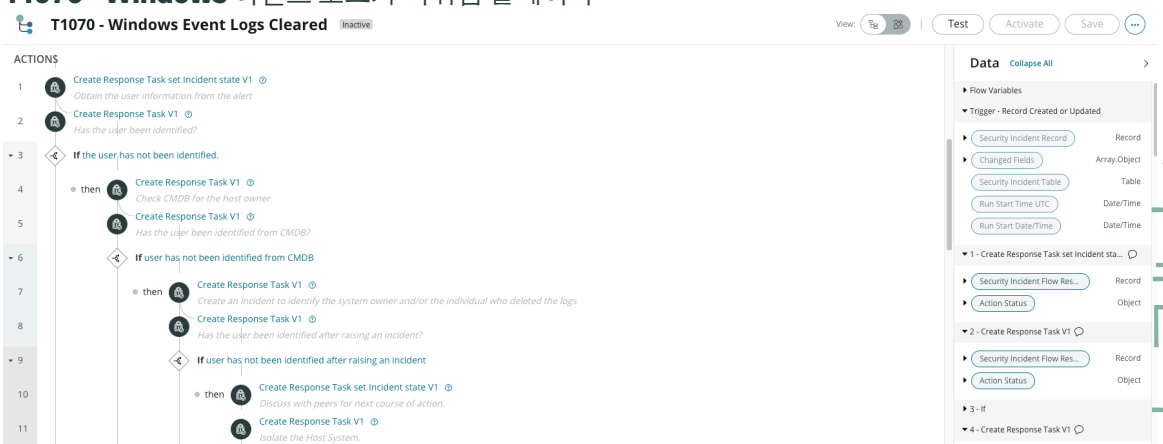
Security Operations 스포크(*sn_sec_spoke*)를 설치했는지 확인하십시오.

프로시저

1. sn_si.user 및 flow_designer 역할을 가진 사용자로 로그인합니다.
2. 다음으로 이동 모두 〉 플로우 디자이너 을 클릭하고 **T1070 - Windows** 이벤트 로그 지워짐 플레이북을 선택합니다.
3. 옵션: T1070 - Windows 이벤트 로그 지워진 플레이북 플로우의 사본을 만들고 필요에 따라 수정합니다.

   (Optional) 플레이북 플로우의 복사본을 생성하려면 아이콘을 선택하고 플로우 복사를 선택합니다. 플로우를 사용자 지정하거나 특정 변경을 수행하려는 경우에만 이 단계를 수행합니다.

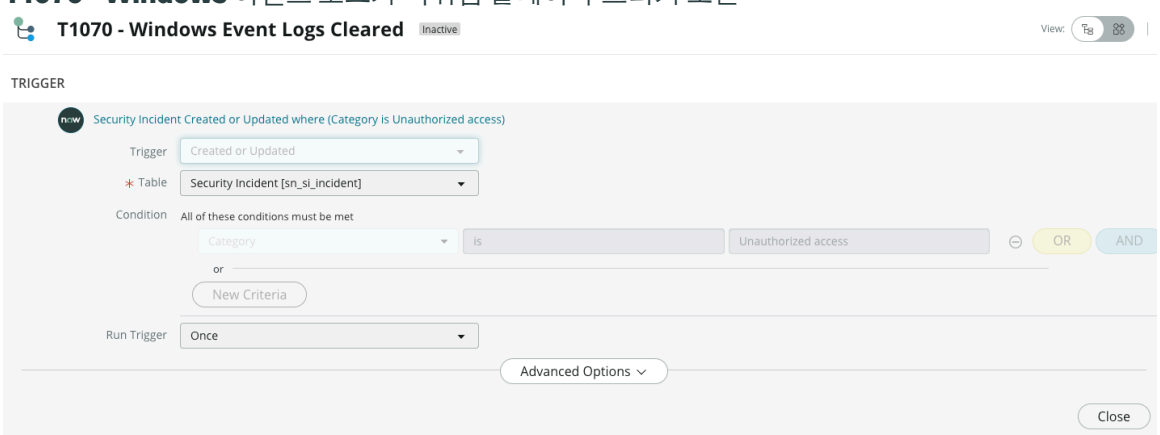
T1070 - Windows 이벤트 로그가 지워짐 플레이북



4. 플레이북을 활성화합니다.
   a. 기본 시스템에서 사용할 수 있는 플레이북을 사용하려면 메인 플로우를 활성화합니다.
   b. 필요한 사항을 변경한 후 복사된 플로우를 활성화합니다.
5. 플레이북에 대한 트리거 조건을 설정합니다.

   이 플레이북은 범주 가 무단 액세스일 때 트리거되고 보안 인시던트와 연결됩니다.

T1070 - Windows 이벤트 로그가 지워짐 플레이북 트리거 조건



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

T1070 - Windows 이벤트 로그 지워짐 플레이북 사용

이 플레이북을 사용하여 사용자가 보안 로그를 제거하는 이벤트 유형을 추적하는 인시던트를 조사합니다. 다음 단계에서는 T1070 - Windows 이벤트 로그 지워짐 플레이북에서 사용할 수 있는 작업, 작업 및 하위 흐름에 대한 연습을 제공합니다.

시작하기 전에
필요한 역할:

- sn_si.admin
- flow_designer

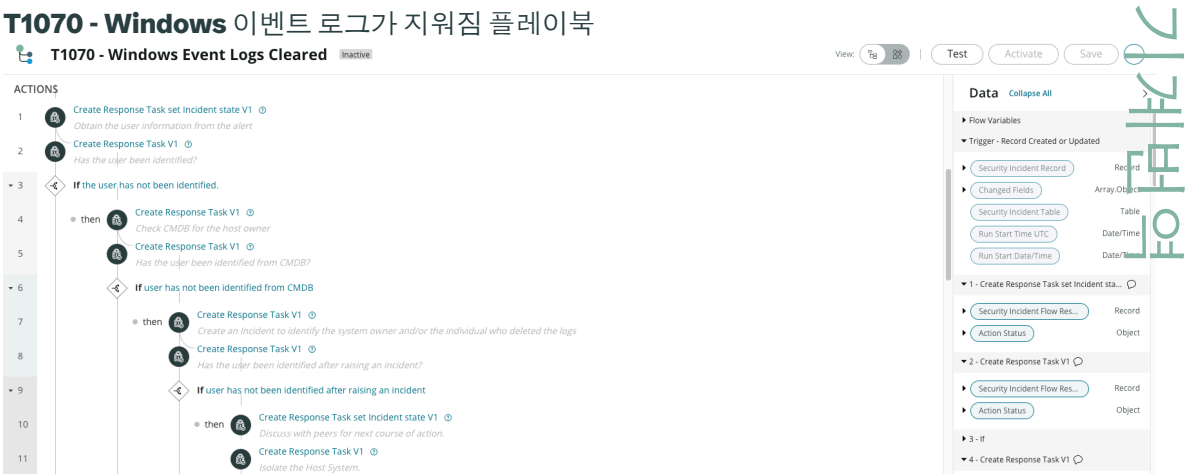
프로시저

1. 플레이북이 트리거되고 실행이 시작되면 작업 1의 경보에서 사용자 상세 정보를 가져옵니다.
2. 작업 2에서 사용자가 식별되었는지 여부를 확인합니다.
3. 작업 3에서 사용자를 식별하지 않은 경우 다음 단계를 수행합니다.

   a. 작업 4에서 CMDB(구성 관리 데이터베이스)에서 호스트 소유자 상세 정보를 확인합니다.

   b. 작업 5에서 사용자가 CMDB에서 식별되었는지 여부를 확인합니다.

      사용자가 CMDB에서 식별된 경우 작업 5에서 수동 응답 작업이 생성되고 플로우가 종료됩니다.



   c. 작업 6에서 사용자가 CMDB에서 식별되지 않은 경우 다음 단계를 수행합니다.

      i. 작업 7에서 인시던트를 생성하여 시스템 소유자와 로그를 삭제한 개인을 식별합니다.

      ii. 작업 8에서는 인시던트를 제기한 후 사용자를 식별했는지 여부를 확인합니다.

         인시던트를 제기한 후 사용자가 식별되면 작업 8에서 수동 응답 작업이 생성되고 플로우가 종료됩니다.

      iii. 작업 9에서 인시던트를 제기한 후 사용자를 식별하지 못한 경우 다음 단계를 수행합니다.

         1. 동작 10에서는 동료들과 다음 행동 방침에 대해 논의합니다.
         2. 작업 11에서 호스트 시스템을 격리합니다.
         3. 작업 12에서 생성되었을 수 있는 원치 않는 파일을 제거하고 불량 계정을 삭제합니다.
         4. 행동 13에서는 격납고를 해제하고 시스템을 작동 표준으로 되돌립니다.

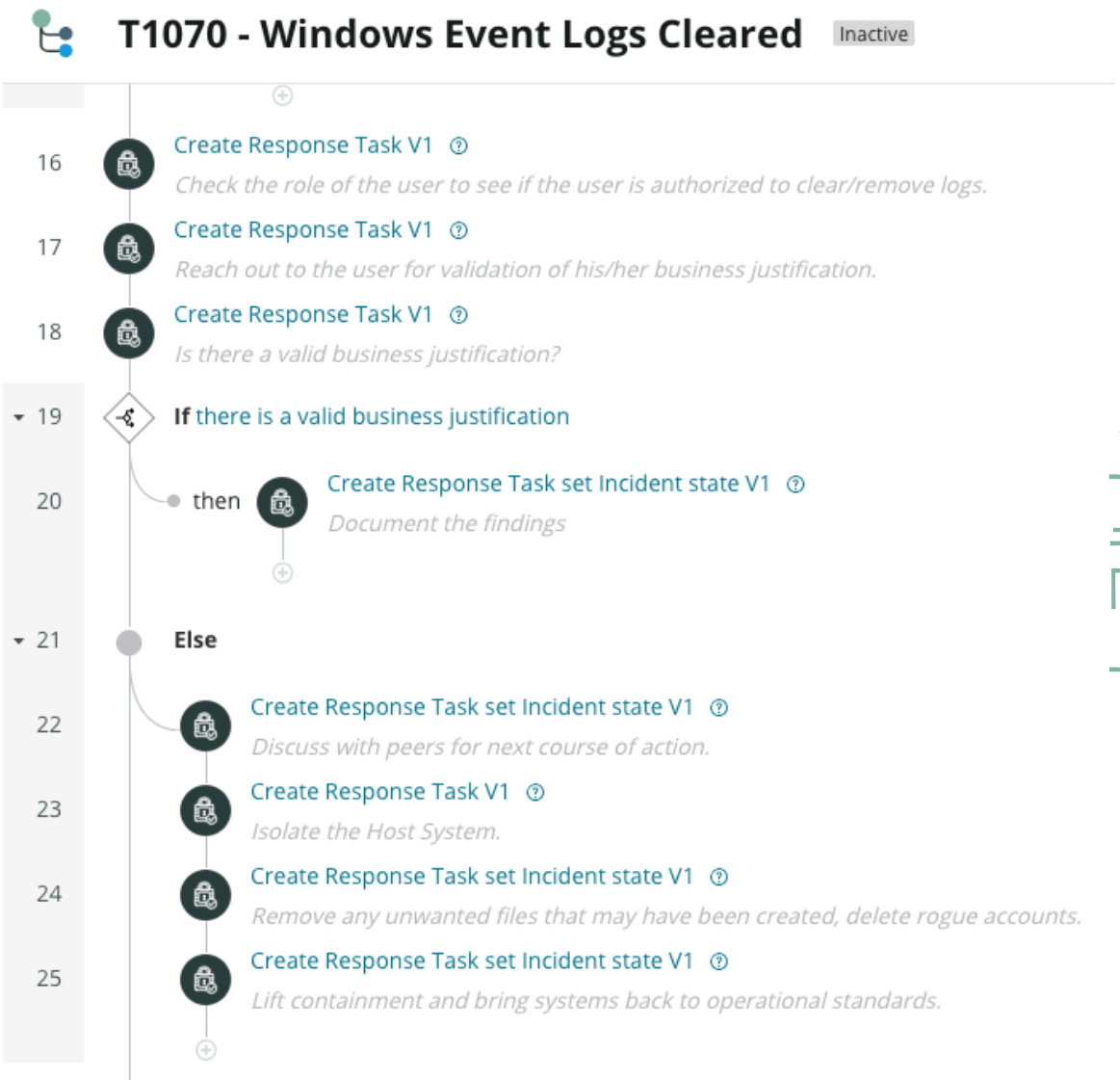
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. 작업 14에서 작업을 종결하기 전에 사후 인시던트 검토를 완료합니다.

   작업 15에서 흐름이 종료됩니다.

4. 작업 16에서 사용자가 식별된 경우 사용자의 역할을 확인하여 사용자에게 로그를 지우거나 제거할 수 있는 권한이 있는지 확인합니다.
5. 작업 17에서 사용자에게 연락하여 비즈니스 정당성의 유효성을 확인합니다.
   제공된 이메일 템플릿을 사용하여 사용자에게 연락할 수 있습니다.

T1070 사용 **- Windows** 이벤트 로그 지워짐 플레이북



6. 작업 18에서 유효한 비즈니스 정당성이 제공되었는지 여부를 확인합니다.
7. 조치 19에서 유효한 비즈니스 정당성이 제공된 경우 조치 20에서 지금까지의 결과를 문서화합니다.
   플로우가 종료됩니다.
8. 작업 21에서 유효한 비즈니스 정당성이 제공되지 않은 경우 다음 단계를 수행합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 행동 22에서 동료들과 다음 행동 방침에 대해 논의합니다.

b. 작업 23에서 호스트 시스템을 격리합니다.

c. Action 24에서 생성되었을 수 있는 원치 않는 파일을 제거하고 불량 계정을 삭제합니다.

d. 액션 25에서는 격납고를 해제하고 시스템을 작동 표준으로 되돌립니다.
플로우가 종료됩니다.

9. 작업 26에서 작업을 종결하기 전에 사후 인시던트 검토를 완료합니다.

플레이북 **/etc/hosts** 파일의 외부 주소 쿼리

이 플레이북은 내부 호스트 이름 또는 도메인이 Linux 서버의 로컬 DNS(/etc/hosts)에 있는 외부 IP 주소에 할당되었음을 나타내는 인시던트를 조사하기 위한 체계적인 정정 단계를 제공합니다.

/etc/hosts 파일 플레이북에서 외부 주소의 **OSquery** 설정

다음 단계를 사용하여 /etc/hosts 파일 플레이북에서 외부 주소의 OSquery를 설정합니다.

시작하기 전에
필요한 역할:

- sn_si.admin
- flow_designer

Security Operations 스포크(*sn_sec_spoke*)를 설치했는지 확인하십시오.

프로시저

1. sn_si.user 및 flow_designer 역할을 가진 사용자로 로그인합니다.

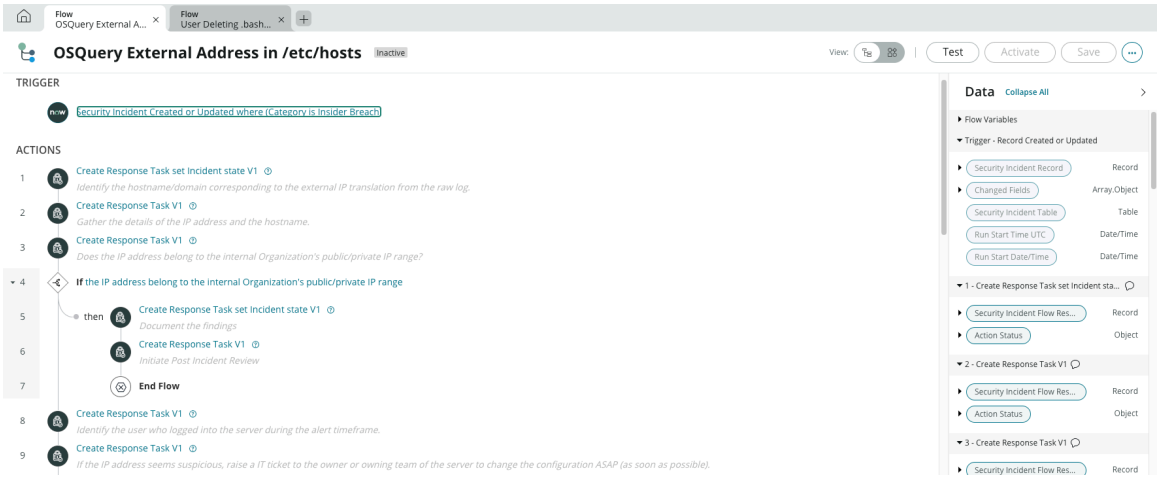
2. 다음으로 이동 모두 〉 플로우 디자이너 을 클릭하고 **/etc/hosts** 플레이북에서 **OSquery** 외부 주소를 선택합니다.

3. 옵션: /etc/hosts 플레이북 플로우에서 OSquery 외부 주소의 사본을 생성하고 필요에 따라 수정합니다.

(Optional) 플레이북 플로우의 복사본을 생성하려면 아이콘을 선택하고 플로우 복사를 선택합니다. 플로우를 사용자 지정하거나 특정 변경을 수행하려는 경우에만 이 단계를 수행합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

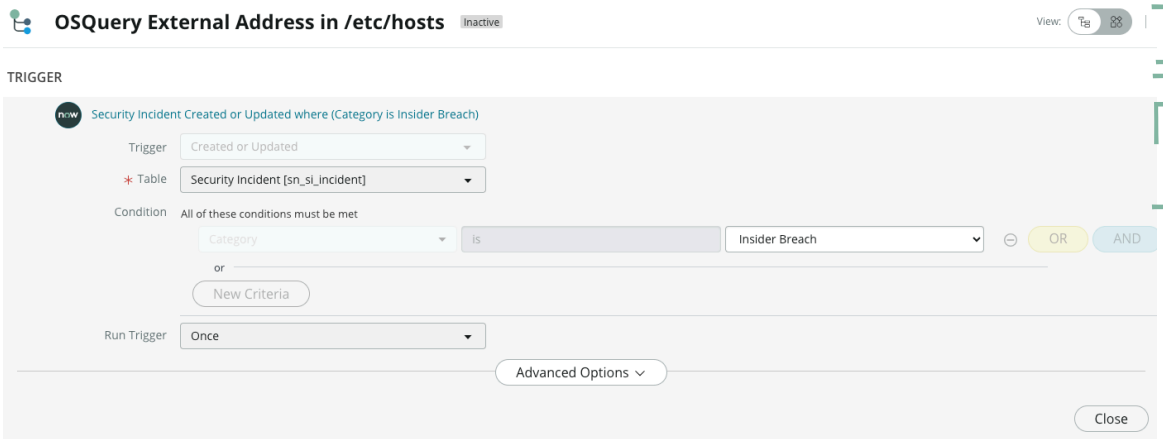
OS/etc/hosts 플레이북의 외부 주소 쿼리



4. 플레이북을 활성화합니다.
   a. 기본 시스템에서 사용할 수 있는 플레이북을 사용하려면 메인 플로우를 활성화합니다.
   b. 필요한 사항을 변경한 후 복사된 플로우를 활성화합니다.
5. 플레이북에 대한 트리거 조건을 설정합니다.

   이 플레이북은 범주 가 내부자 위반일 때 트리거되고 보안 인시던트와 연결됩니다.

OS/etc/hosts 플레이북 트리거 조건의 외부 주소 쿼리



/etc/hosts 파일 플레이북에서 외부 주소의 **OSquery** 사용

이 플레이북을 사용하여 내부 호스트 이름 또는 도메인이 Linux 서버의 로컬 DNS(/etc/hosts)에 있는 외부 IP 주소에 할당되었음을 나타내는 인시던트를 조사합니다. 다음 단계에서는 /etc/hosts 파일 플레이북의 외부 주소 OSquery에서 사용할 수 있는 조치, 작업 및 하위 플로우에 대한 검토 과정을 제공합니다.

시작하기 전에
필요한 역할:

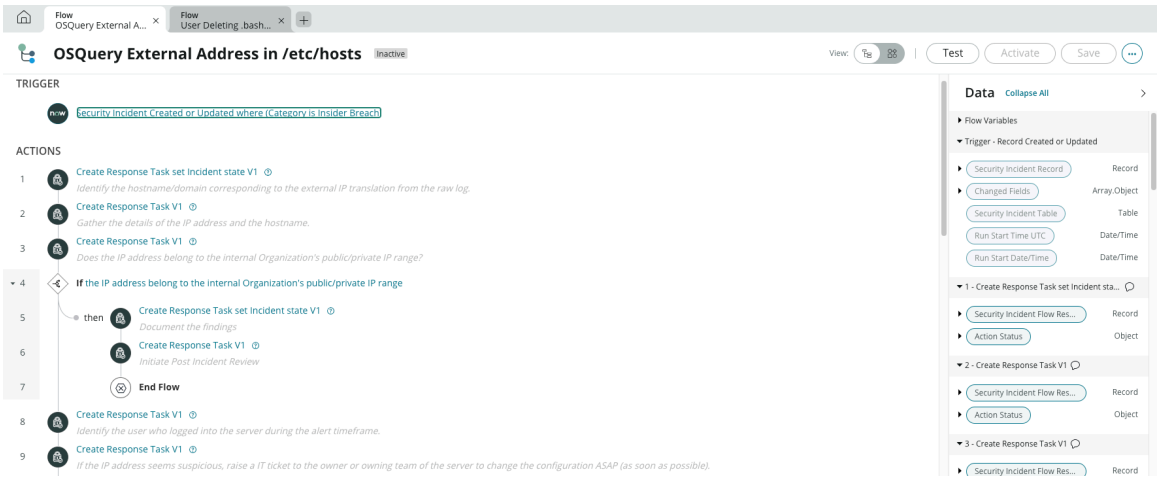
- sn_si.admin
- flow_designer

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 플레이북이 트리거되고 실행이 시작되면 작업 1에서 원시 로그의 외부 IP 변환에 해당하는 호스트 이름 또는 도메인 이름을 식별합니다.
2. 작업 2에서 IP 주소 및 호스트 이름에 대한 세부 정보를 수집합니다.
3. 작업 3에서 이 IP 주소가 내부 조직의 퍼블릭/프라이빗 IP 범위에 속하는지 여부를 확인합니다.

OS/etc/hosts 파일 플레이북의 외부 주소 쿼리



4. 작업 4에서 IP 주소가 내부 조직의 공용/개인 IP 범위에 속하는 경우 다음 단계를 수행합니다.

   a. 작업 5에서는 지금까지의 결과를 문서화합니다.

   b. 작업 6에서 사후 인시던트 검토를 시작합니다.
   작업 7에서는 사후 인시던트 검토 후 플로우가 종료됩니다.

5. IP 주소가 내부 조직의 퍼블릭/프라이빗 IP 범위에 속하지 않는 경우 작업 8에서 경보 기간 동안 서버에 로그인한 사용자를 식별합니다.
6. 작업 9에서 IP 주소가 의심스러운 경우 소유자 또는 서버 팀에 IT 티켓을 제기하여 가능한 한 빨리 구성을 변경합니다.
7. 작업 10에서 DNS 항목을 추가하기 전과 후에 서버에 악의적인 활동이 있었는지 확인합니다.
8. 작업 11에서 서버에서 외부 IP 주소에 대한 연결을 확인합니다.
9. Action 12에서는 지금까지의 결과를 문서화합니다.
10. 작업 13에서 소유자 또는 팀 정보를 사용할 수 있는지 여부를 확인합니다.
11. 작업 14에서 소유자 또는 팀 정보를 사용할 수 있는 경우 다음 단계를 수행합니다.

    a. 작업 15에서 소유자 또는 서버 팀에 연락하여 활동을 인식하는지 확인합니다.
    제공된 이메일 템플릿을 사용하여 소유자 또는 서버 팀에 문의할 수 있습니다.

    b. 작업 16에서 소유자 또는 팀이 유효한 비즈니스 정당성을 제공했는지 여부를 확인합니다.

    c. 작업 17에서 제공된 소유자 또는 팀이 유효한 비즈니스 정당성을 제공하지 않으면 플로우가 종료됩니다.
    그러나 소유자 또는 팀이 유효한 비즈니스 정당성을 제공한 경우 다음 단계를 수행합니다.

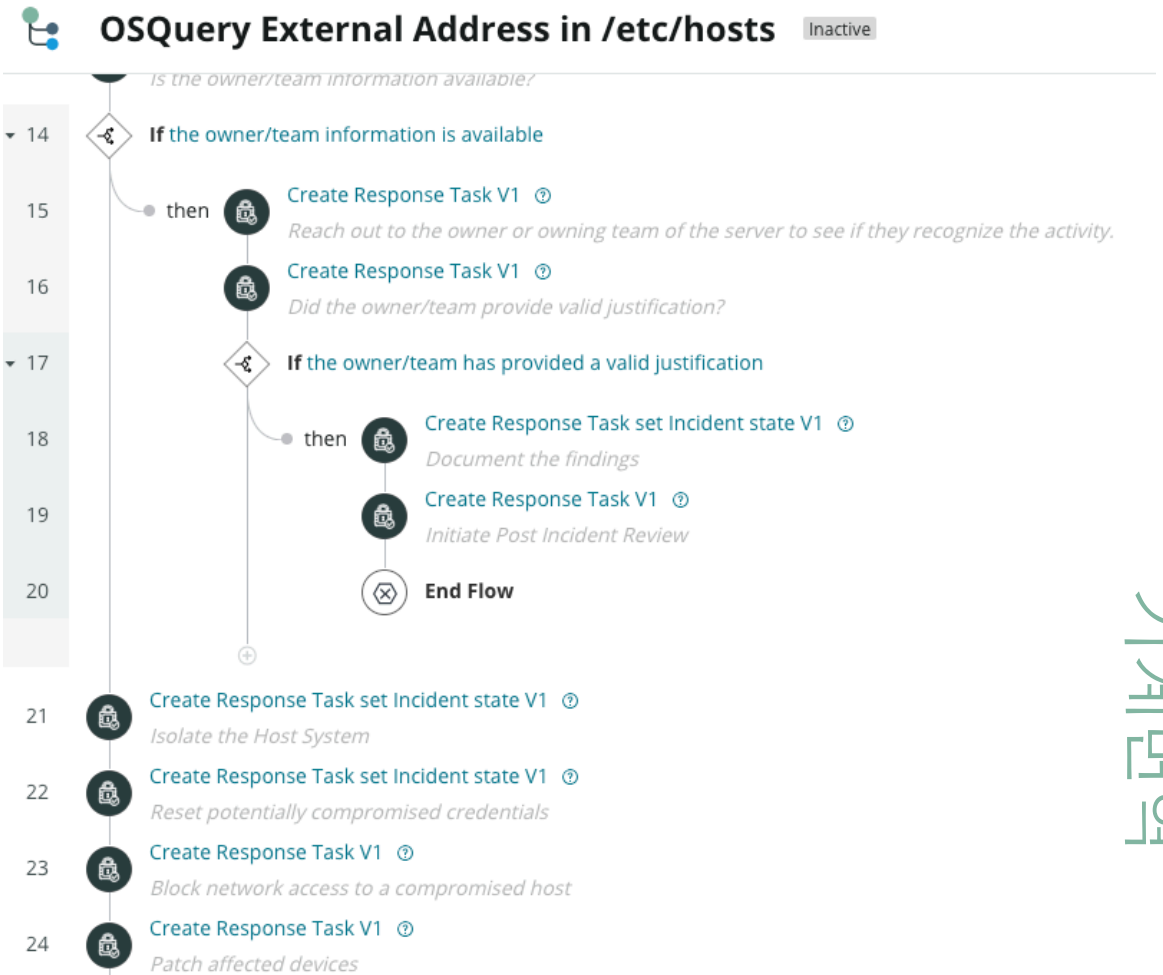
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

i. Action 18에서는 지금까지의 결과를 문서화합니다.

ii. 작업 19에서 사후 인시던트 검토를 시작합니다.

작업 20에서는 사후 인시던트 검토 후 플로우가 종료됩니다.

/etc/hosts 파일 플레이북에서 외부 주소의 **OSquery** 사용



12. 작업 21에서 소유자 또는 팀 정보를 사용할 수 없는 경우 호스트 시스템을 격리합니다.

13. 작업 22에서 잠재적으로 손상된 자격 증명을 재설정합니다.

14. 작업 23에서 손상된 호스트에 대한 네트워크 액세스를 차단합니다.

15. Action 24에서 영향을 받는 장치를 패치합니다.

16. 액션 25에서는 봉쇄를 해제하고 시스템을 운영 표준으로 되돌립니다.

17. 작업 26에서 작업을 종결하기 전에 사후 인시던트 검토를 완료합니다.

사용자를 위한 플레이북 **Bash** 이력 삭제 **-** 클라우드

이 플레이북은 누군가가 Linux 서버에서 *.bash_history*(bash 기록) 파일을 제거하려고 했는지 여부를 나타내는 인시던트를 조사하기 위한 체계적인 정정 단계를 제공합니다.

주:
이 경고는 거의 트리거되지 않고 내부자 위협을 나타낼 수 있으므로 이 경고를 완화할 때는 주의해야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용자 설정 **Bash** 이력 삭제 플레이북

다음 단계를 사용하여 사용자 삭제 Bash 기록 플레이북을 설정합니다.

시작하기 전에

필요한 역할:

- sn_si.admin
- flow_designer

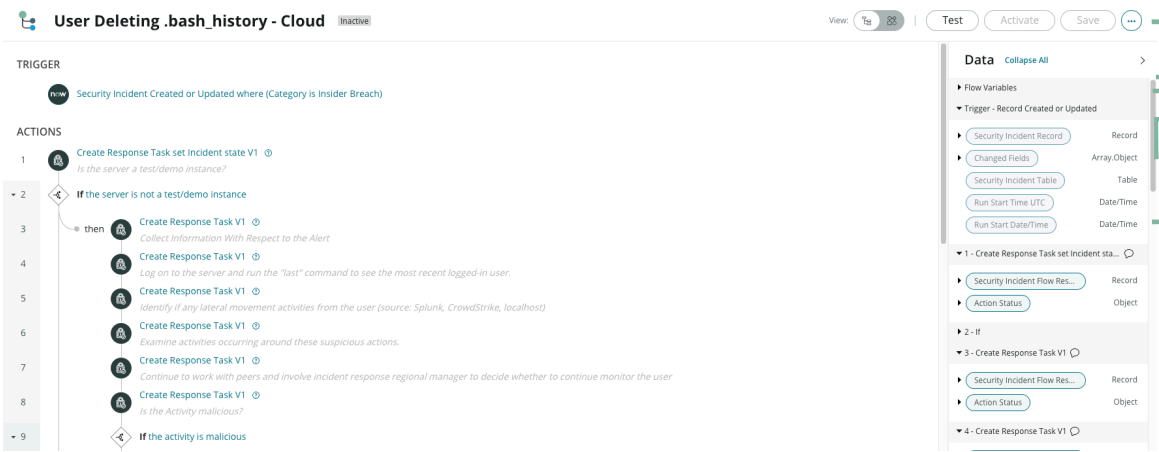
Security Operations 스포크(*sn_sec_spoke*)를 설치했는지 확인하십시오.

프로시저

1. sn_si.user 및 flow_designer 역할을 가진 사용자로 로그인합니다.
2. 다음으로 이동 모두 〉 플로우 디자이너 을 클릭하고 사용자 삭제 **.bash_history - 클라우드** 플레이북을 선택합니다.
3. 옵션: 사용자 .bash_history 삭제 - 클라우드 플레이북 플로우의 사본을 생성하고 필요에 따라 수정합니다.

   (Optional) 플레이북 플로우의 복사본을 생성하려면 아이콘을 선택하고 플로우 복사를 선택합니다. 플로우를 사용자 지정하거나 특정 변경을 수행하려는 경우에만 이 단계를 수행합니다.

   사용자가 **Bash** 이력을 삭제하는 중 **-** 클라우드 플레이북

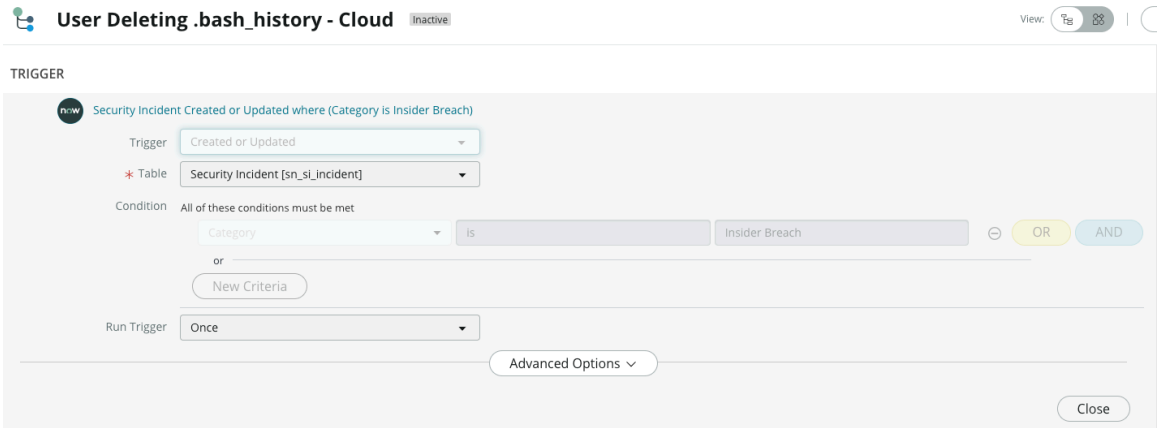


4. 플레이북을 활성화합니다.
   a. 기본 시스템에서 사용할 수 있는 플레이북을 사용하려면 메인 플로우를 활성화합니다.
   b. 필요한 사항을 변경한 후 복사된 플로우를 활성화합니다.
5. 플레이북에 대한 트리거 조건을 설정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 플레이북은 범주 가 내부자 위반일 때 트리거되고 보안 인시던트와 연결됩니다.

사용자가 **Bash** 이력을 삭제하는 중 **-** 클라우드 플레이북 트리거 조건



사용자 삭제 **Bash** 기록 플레이북 사용

이 플레이북을 사용하여 누군가가 Linux 서버에서 bash 기록 파일을 제거하려고 시도했는지 여부를 나타내는 인시던트를 조사합니다. 다음 단계에서는 사용자 Bash 기록 삭제(*.bash_history*) 플레이북에서 사용할 수 있는 작업, 작업 및 하위 플로우에 대한 안내를 제공합니다.

시작하기 전에
필요한 역할:

- sn_si.admin
- flow_designer

프로시저

1. 플레이북이 트리거되고 실행이 시작되면 작업 1에서 서버가 테스트 인스턴스인지 데모 인스턴스인지 확인합니다.
2. 작업 2에서 서버가 테스트 또는 데모 인스턴스가 아닌 경우 다음 단계를 수행합니다.

   a. 작업 3에서 경보에 대한 다음 정보를 수집합니다.
      - 사용자 이름
      - IP 주소
      - bash 기록을 삭제하려는 악의적인 명령
      - 사용자가 실행하는 모든 명령(CrowdStrike 로그에서 사용 가능한 경우)

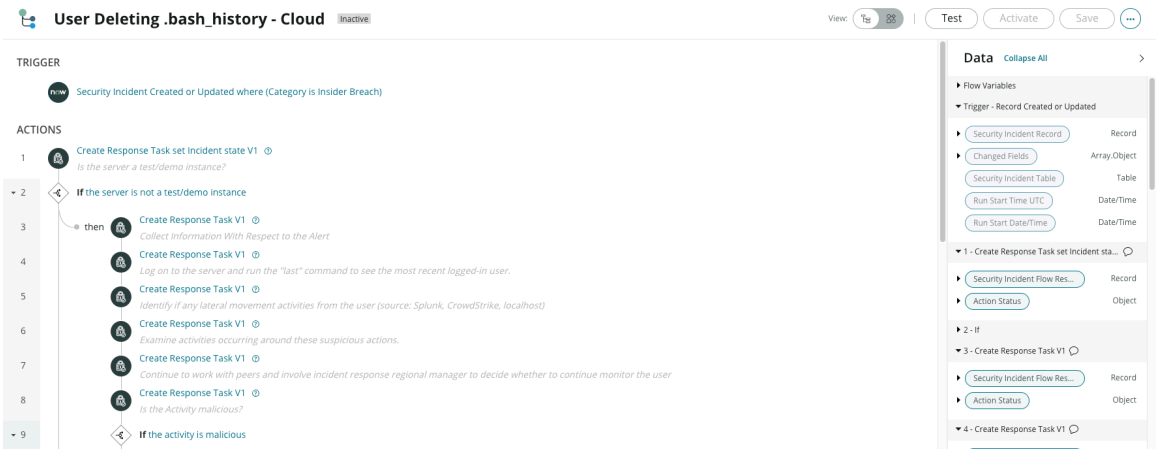
   b. 작업 4에서 서버에 로그인하고 ### 명령을 실행하여 가장 최근에 로그인한 사용자를 봅니다.

   c. 작업 5에서 사용자의 횡적 이동 활동이 있었는지 확인합니다(출처: Splunk, CrowdStrike, localhost).

   d. 작업 6에서 이러한 의심스러운 행동과 관련하여 발생하는 활동을 조사합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용자가 **Bash** 이력 Playbook을 삭제하는 중



e. 작업 7에서는 동료와 계속 협력하고 사용자를 계속 모니터링할지 여부를 결정하는 데 인시던트 응답 지역 관리자를 참여시킵니다.

f. 작업 8에서 활동이 악성인지 여부를 확인합니다.

g. 작업 9에서 활동이 악의적인 경우 다음 단계를 수행합니다.

i. 작업 10에서 조사하는 동안 IT 지원에 연락하여 계정 동결을 요청합니다.

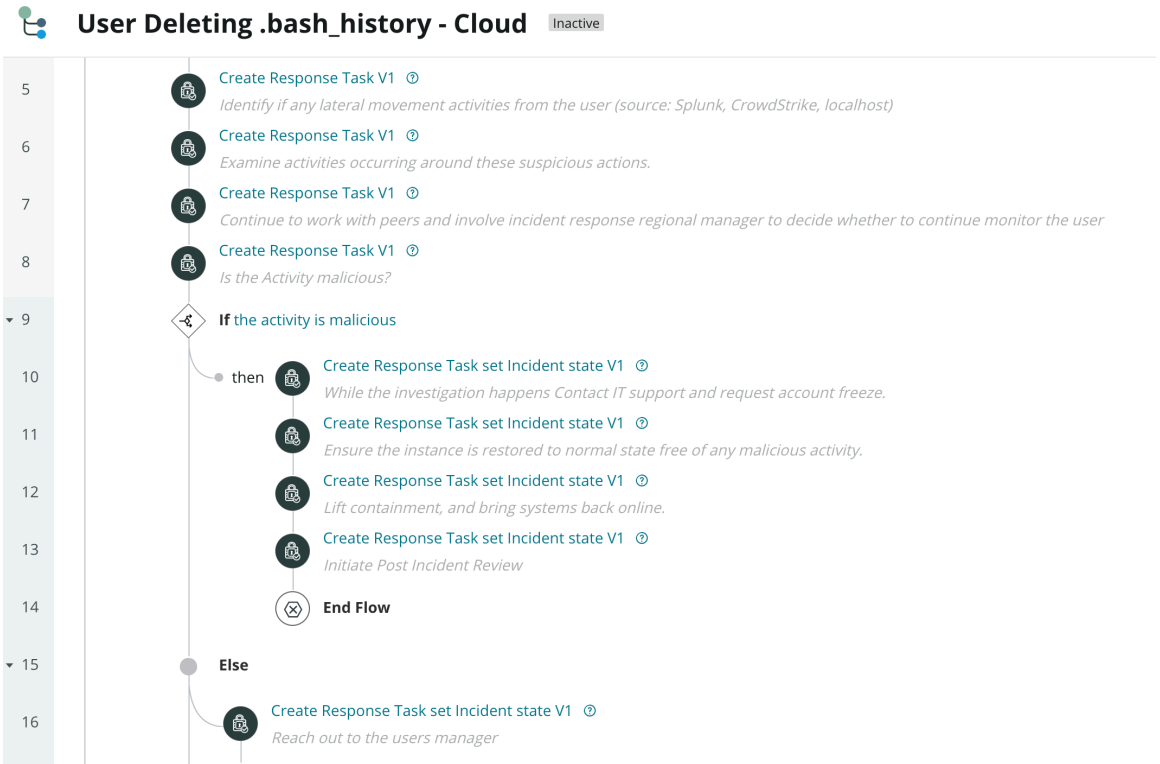
ii. 작업 11에서는 인스턴스가 악의적인 활동이 없는 정상 상태로 복원되었는지 확인합니다.

iii. Action 12에서는 봉쇄를 해제하고 시스템을 운영 표준으로 되돌립니다.

iv. 작업 13에서 사후 인시던트 검토를 시작합니다.

작업 14에서는 사후 인시던트 검토 후 플로우가 종료됩니다.

사용자 삭제 **Bash** 기록 플레이북 사용



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

h. 작업 15에서 활동이 악의적이지 않은 경우 작업 16에서 사용자의 관리자에게 연락합니다. 제공된 이메일 템플릿을 사용하여 사용자의 관리자에게 문의하고 권장 접근 방식에 대해 알릴 수 있습니다.

3. Action 17에서는 지금까지의 결과를 문서화합니다.

4. 작업 18에서 작업을 종결하기 전에 사후 인시던트 검토를 완료합니다.

서비스 계정에서 성공적인 **VPN** 시도를 위한 플레이북 - 회사/클라우드

이 플레이북은 VPN을 통해 서비스 계정에서 성공적인 로그인 시도를 추적하는 인시던트를 조사하기 위한 체계적인 정정 단계를 제공합니다. 서비스 계정에는 VPN의 로그인 이벤트가 없어야 하며 이러한 이벤트는 무차별 암호 대입 또는 계정 자격 증명 노출 가능성의 지표일 수 있습니다.

서비스 계정 플레이북에서 성공한 **VPN** 시도 설정

다음 단계를 사용하여 서비스 계정 플레이북에서 성공한 VPN 시도를 설정합니다.

시작하기 전에
필요한 역할:

- sn_si.admin
- flow_designer

Security Operations 스포크(*sn_sec_spoke*)를 설치했는지 확인하십시오.

프로시저

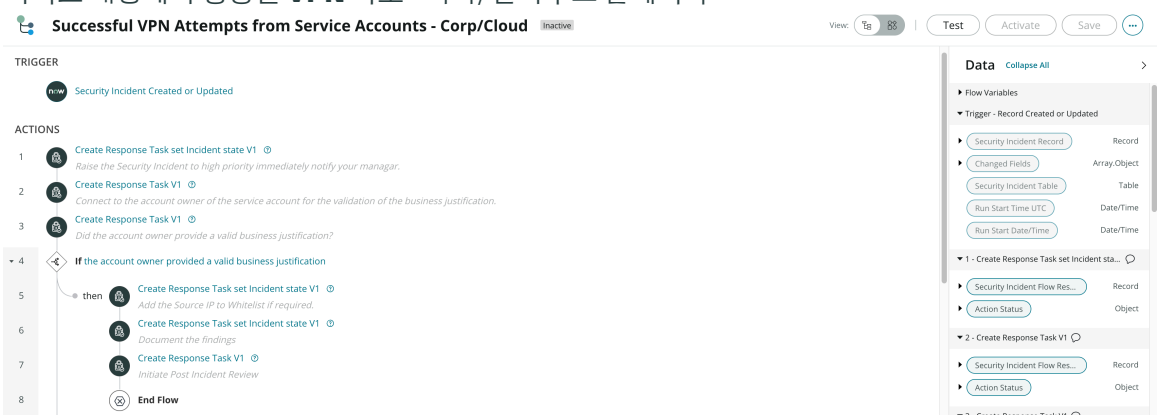
1. sn_si.user 및 flow_designer 역할을 가진 사용자로 로그인합니다.

2. 다음으로 이동 모두 〉 플로우 디자이너 을 클릭하고 **Service** Accounts(서비스 계정) 플레이북에서 **Successful VPN** Attempts(성공한 **VPN** 시도)를 선택합니다.

3. 옵션: 서비스 계정 플레이북 플로우에서 성공한 VPN 시도의 사본을 생성하고 필요에 따라 수정합니다.

(Optional) 플레이북 플로우의 복사본을 생성하려면 아이콘을 선택하고 플로우 복사를 선택합니다. 플로우를 사용자 지정하거나 특정 변경을 수행하려는 경우에만 이 단계를 수행합니다.

서비스 계정에서 성공한 **VPN** 시도 - 회사/클라우드 플레이북



4. 플레이북을 활성화합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

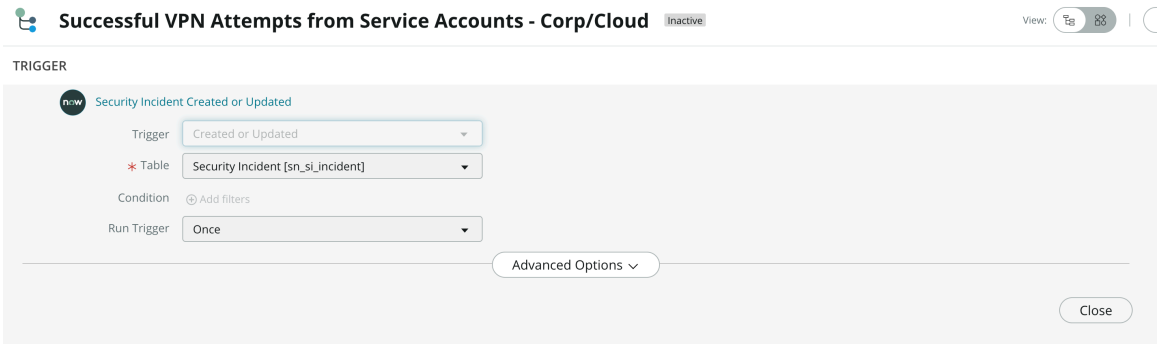
a. 기본 시스템에서 사용할 수 있는 플레이북을 사용하려면 메인 플로우를 활성화합니다.

b. 필요한 사항을 변경한 후 복사된 플로우를 활성화합니다.

5. 플레이북에 대한 트리거 조건을 설정합니다.

이 Playbook은 필수 조건에 따라 보안 인시던트가 생성되거나 업데이트될 때 트리거되고 보안 인시던트와 연결됩니다. 예를 들어 범주 가 내부자 위반인 경우입니다.

서비스 계정에서 성공한 **VPN** 시도 **-** 회사/클라우드 플레이북 트리거 조건



서비스 계정 플레이북에서 성공한 **VPN** 시도 사용

이 플레이북을 사용하여 VPN을 통해 서비스 계정에서 성공적인 로그인 시도를 추적하는 인시던트를 조사합니다. 다음 단계에서는 서비스 계정 플레이북의 성공적인 VPN 시도에서 사용할 수 있는 작업, 작업 및 하위 플로우에 대한 검토 과정을 제공합니다.

시작하기 전에
필요한 역할:

- sn_si.admin
- flow_designer

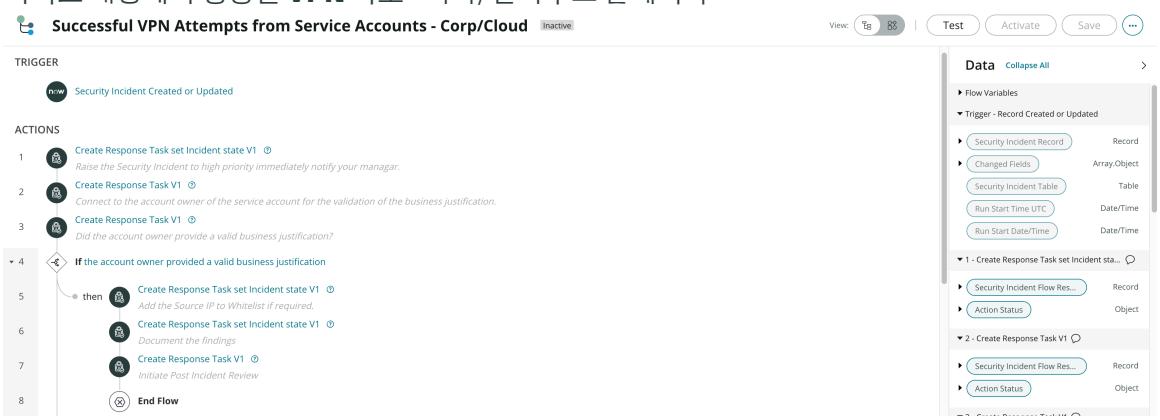
프로시저

1. Playbook이 트리거되고 실행이 시작되면 작업 1에서 보안 인시던트를 높은 우선순위로 올리고 관리자에게 즉시 알립니다.

2. 작업 2에서는 서비스 계정의 소유자에게 연락하여 비즈니스 정당성을 확인합니다.
제공된 이메일 템플릿을 사용하여 서비스 계정 소유자에게 연락하여 비즈니스 정당성을 확인할 수 있습니다.

3. 작업 3에서 서비스 계정 소유자가 유효한 비즈니스 정당성을 제공했는지 확인합니다.

서비스 계정에서 성공한 **VPN** 시도 **-** 회사/클라우드 플레이북



기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

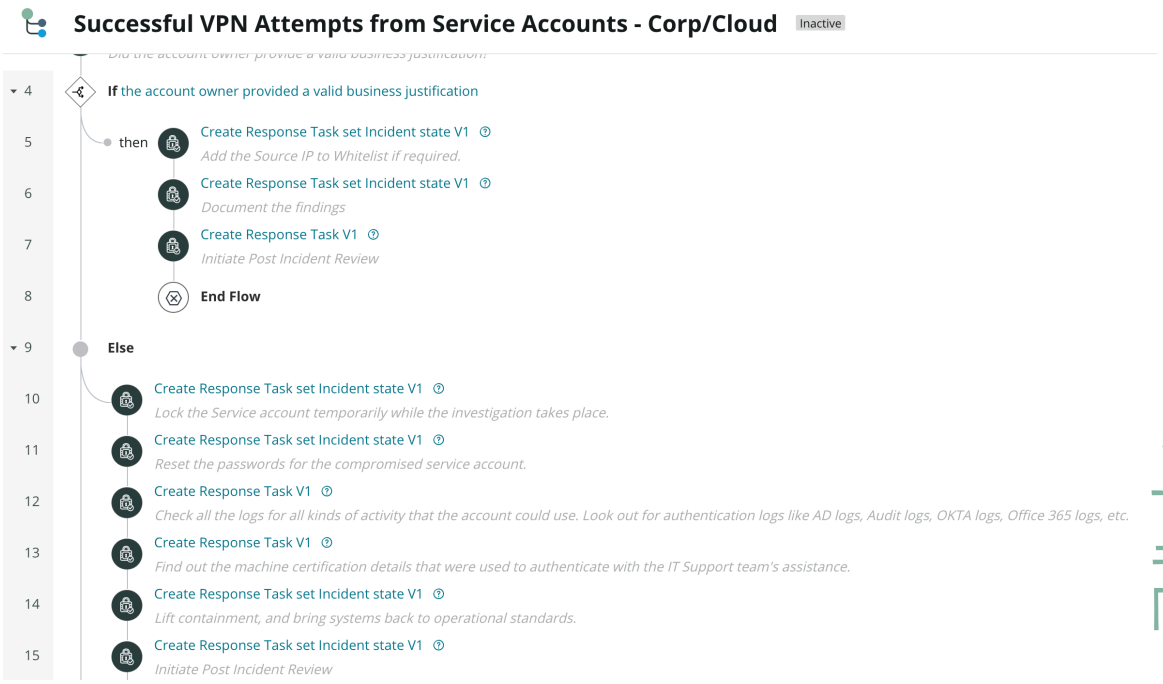
4. 작업 4에서 서비스 계정 소유자가 유효한 비즈니스 정당성을 제공한 경우 다음 단계를 수행합니다.

a. 작업 5에서 필요한 경우 소스 IP를 허용 목록에 추가합니다.

b. 작업 6에서는 지금까지의 결과를 문서화합니다.

c. 작업 7에서 사후 인시던트 검토를 시작합니다.
작업 8에서는 사후 인시던트 검토 후 플로우가 종료됩니다.

서비스 계정에서 성공한 **VPN** 시도 사용 **-** 회사/클라우드 플레이북



5. 작업 9에서 서비스 계정 소유자가 유효한 비즈니스 정당성을 제공하지 않은 경우 다음 단계를 수행합니다.

a. 작업 10에서 조사가 진행되는 동안 서비스 계정을 일시적으로 잠급니다.

b. 작업 11에서 손상된 서비스 계정의 암호를 재설정합니다.

c. 작업 12에서 계정에서 사용할 수 있는 모든 종류의 활동에 대한 로그를 확인합니다.
Active Directory 로그, 감사 로그, Okta 로그, Office 365 로그 등과 같은 인증 로그를 찾습니다.

d. 작업 13에서 IT 지원 팀의 지원을 받아 인증하는 데 사용되는 컴퓨터 인증 상세 정보를 찾습니다.

e. 행동 14에서는 봉쇄를 해제하고 시스템을 운영 표준으로 되돌립니다.

f. 작업 15에서 작업을 닫기 전에 사후 인시던트 검토를 완료합니다.

비활성화된 계정에 대한 액세스 시도를 위한 플레이북

이 플레이북은 계정이 종료, 비활성화 또는 분리된 직원이 자격 증명으로 로그인을 시도할 때 트리거됩니다. Sail 포인트의 사용자 ID 상태는 일반적으로 종료 날짜에 비활성화됨으로 업데이트됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

종료 날짜로부터 30일은 분리된 상태로 업데이트하기에 이상적인 시간입니다. Sail point의 비즈니스 논리를 사용하여 30일 후에 RSA 계정을 삭제하고 Active Directory(AD) 그룹 구성원 자격을 제거할 수 있습니다.

시도된 액세스 비활성화된 계정 플레이북 설정

다음 단계를 사용하여 액세스 시도 비활성화된 계정 플레이북을 설정합니다.

시작하기 전에

필요한 역할:

- sn_si.admin
- flow_designer

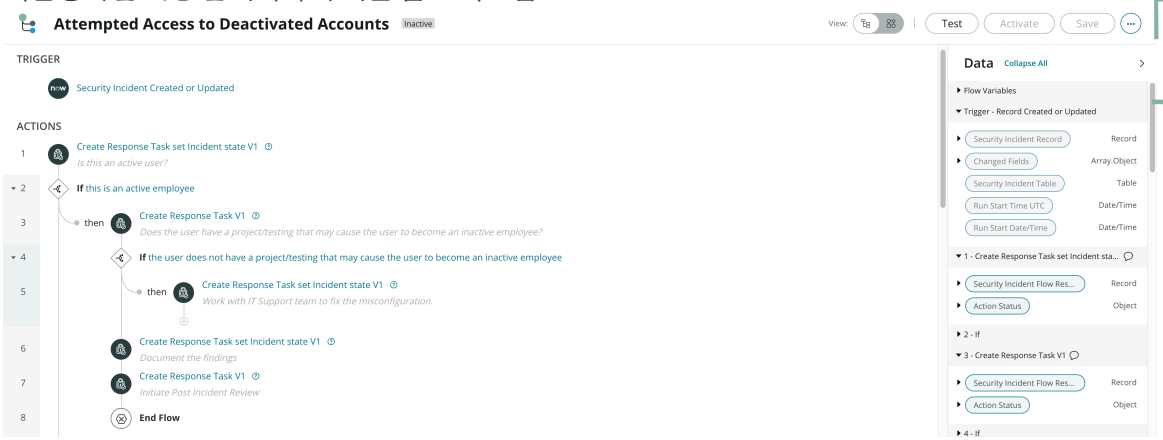
Security Operations 스포크(*sn_sec_spoke*)를 설치했는지 확인하십시오.

프로시저

1. sn_si.user 및 flow_designer 역할을 가진 사용자로 로그인합니다.
2. 다음으로 이동 모두 〉 플로우 디자이너 을 클릭하고 **Attempted Access Deactivated Account** 플레이북을 선택합니다.
3. 옵션: 시도된 액세스 비활성화된 계정 플레이북 플로우의 사본을 생성하고 필요에 따라 수정합니다.

   (Optional) 플레이북 플로우의 복사본을 생성하려면 아이콘을 선택하고 플로우 복사를 선택합니다. 플로우를 사용자 지정하거나 특정 변경을 수행하려는 경우에만 이 단계를 수행합니다.

   비활성화된 계정 플레이북에 대한 접근 시도됨

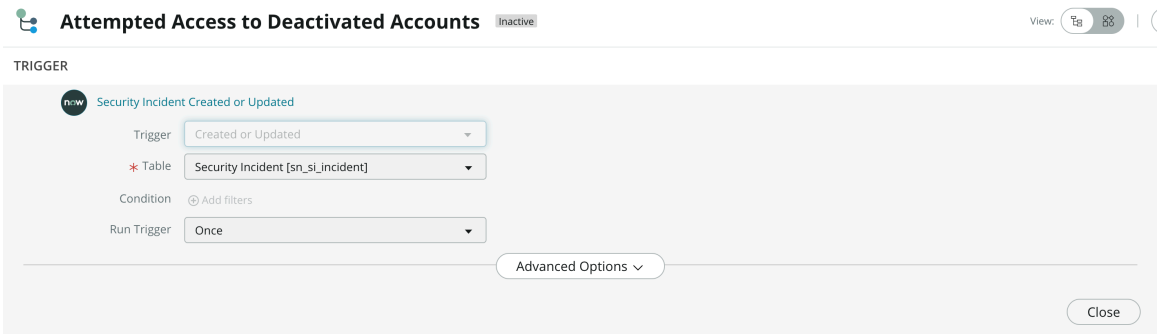


4. 플레이북을 활성화합니다.
   a. 기본 시스템에서 사용할 수 있는 플레이북을 사용하려면 메인 플로우를 활성화합니다.
   b. 필요한 사항을 변경한 후 복사된 플로우를 활성화합니다.
5. 플레이북에 대한 트리거 조건을 설정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 Playbook은 필수 조건에 따라 보안 인시던트가 생성되거나 업데이트될 때 트리거됩니다. 예를 들어 범주가 내부자 위반인 경우입니다.

비활성화된 계정에 대한 접근 시도됨 플레이북 트리거 조건



비활성화된 계정에 대한 시도된 액세스 플레이북 사용

계정이 종료, 비활성화 또는 분리된 직원이 자격 증명으로 로그인을 시도할 때 이 플레이북을 사용합니다. 다음 단계에서는 비활성화된 계정에 대한 액세스 시도 플레이북에서 사용할 수 있는 작업, 작업 및 하위 플로우에 대한 안내를 제공합니다.

시작하기 전에

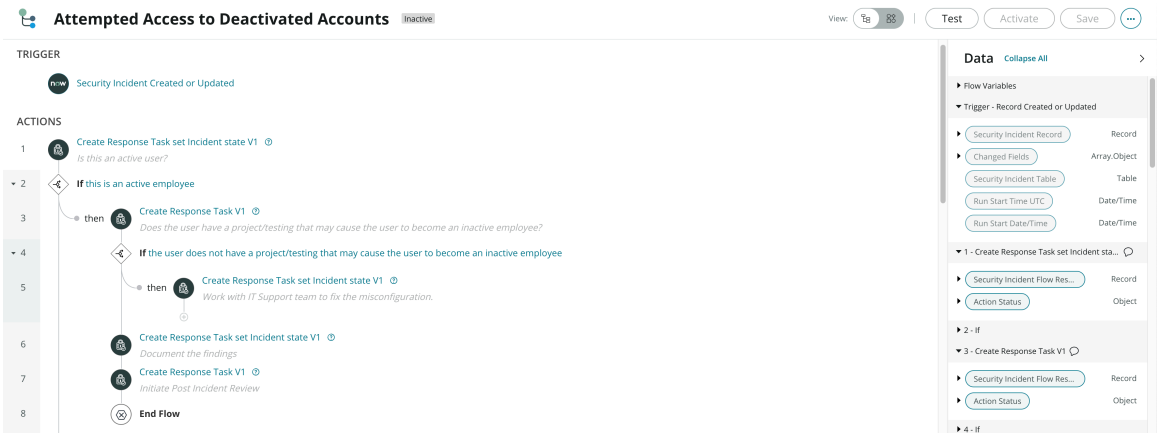
필요한 역할:

- sn_si.admin
- flow_designer

프로시저

1. 플레이북이 트리거되고 실행이 시작되면 작업 1에서 비활성화된 계정에 대해 활성 사용자가 액세스하려고 시도했는지 확인합니다.
2. 작업 2에서 비활성화된 계정에 대해 활성 직원이 액세스하려고 시도했는지 확인합니다.

비활성화된 계정 플레이북에 대한 접근 시도됨



3. 활성 직원이 비활성화된 계정에 액세스하려고 시도한 경우 다음 단계를 수행합니다.

   a. 작업 3에서 사용자를 비활성 직원이 되게 하는 프로젝트 또는 테스트 케이스가 있는지 확인합니다.

   b. 작업 4에서 사용자가 비활성 직원이 되는 프로젝트 또는 테스트 케이스가 사용자에게 없는 경우 IT 지원 팀과 협력하여 잘못된 구성을 수정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

플로우가 종료됩니다.

c. 작업 5에서 사용자에게 비활성 직원이 되는 프로젝트 또는 테스트 케이스가 있는 경우 다음 단계를 수행합니다.

i. 작업 6에서는 지금까지의 결과를 문서화합니다.

ii. 작업 7에서 사후 인시던트 검토를 시작합니다.

작업 8에서는 사후 인시던트 검토 후 플로우가 종료됩니다.

4. 작업 9에서 활성 직원이 비활성화된 계정에 액세스하려고 시도한 것이 아닌 경우 다음 단계를 수행합니다.

a. 작업 10에서 사용자의 로그인에 성공했는지 확인합니다.

b. 작업 11에서 직원이 언제 오프보딩되었는지 확인합니다.

c. 작업 12에서 Splunk에 대한 이벤트를 조사하여 해당 기간 동안의 사용자 활동을 조사합니다.

d. 지금까지의 조사를 기반으로 작업 13에서 사용자가 데이터를 유출했는지 여부를 확인합니다.

e. 작업 14에서 사용자가 데이터를 유출하지 않은 경우 다음 단계를 수행합니다.

i. 작업 15에서는 IT 지원 팀과 협력하여 활성 세션을 종료하고 계정을 비활성화합니다.

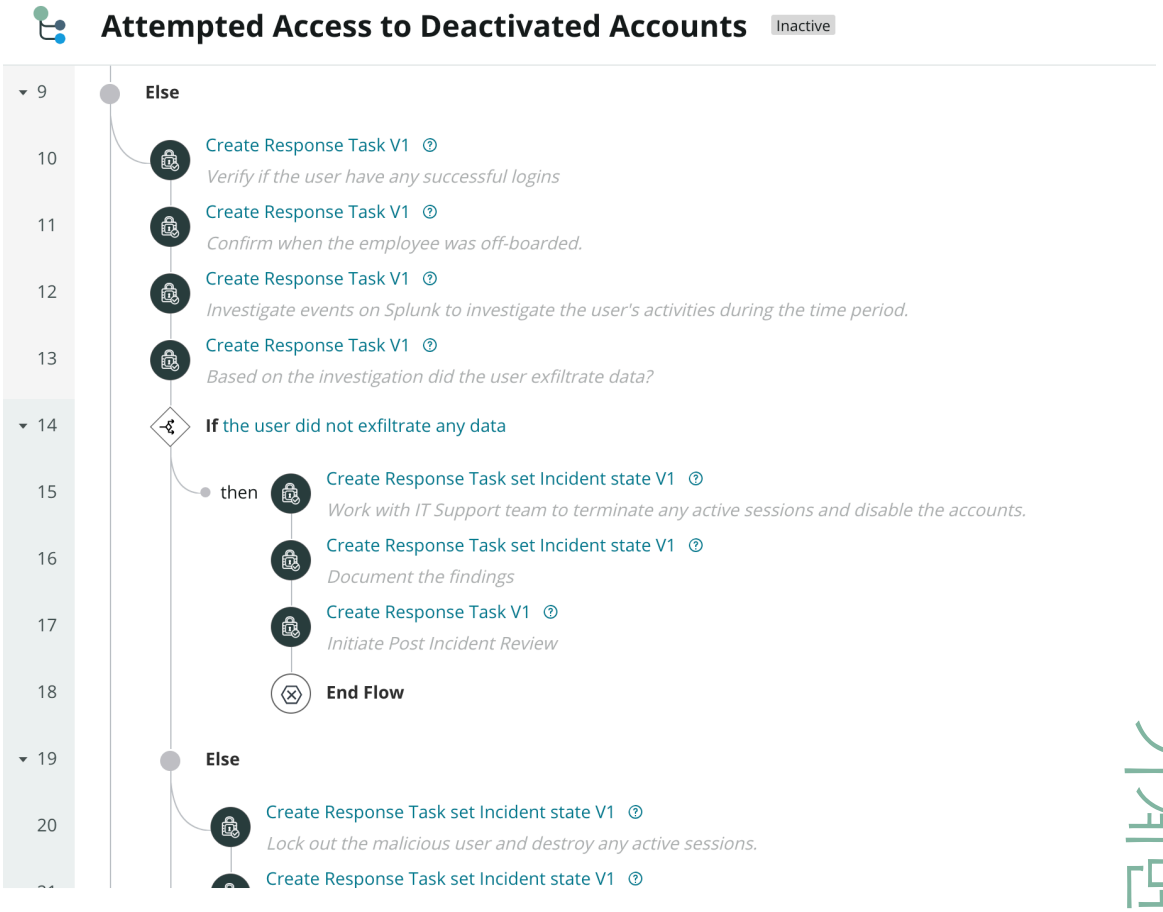
ii. Action 16에서는 지금까지의 결과를 문서화합니다.

iii. 작업 17에서 사후 인시던트 검토를 시작합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업 18에서는 사후 인시던트 검토 후 플로우가 종료됩니다.

비활성화된 계정에 대한 액세스 시도 플레이북 사용



5. 작업 19에서 사용자가 데이터를 반출한 경우 다음 단계를 수행합니다.

a. 작업 20에서 악의적인 사용자를 잠그고 활성 세션을 삭제합니다.

b. 작업 21에서는 IT 지원 팀과 협력하여 모든 계정을 비활성화합니다.

c. 작업 22에서는 리소스가 정상 상태로 복원되고 악의적인 활동이 없는지 확인합니다. 필요한 경우 자원을 이미지로 다시 설치할 수 있습니다.

d. 액션 23에서는 봉쇄를 해제하고 시스템을 운영 표준으로 되돌립니다.

e. 작업 24에서 작업을 종결하기 전에 사후 인시던트 검토를 완료합니다.

T1003용 플레이북 - 방어 회피 - **Mimikatz DCShadow**

이 플레이북은 Mimikatz DCShadow로 인해 발생한 것으로 의심되는 인시던트를 조사하기 위한 체계적인 정정 단계를 제공합니다. DCShadow는 도메인 컨트롤러(Active Directory를 제어하는 서버)의 동작을 시뮬레이션하여 대부분의 표준 보안 제어(SIEM 포함)를 우회하여 자체 데이터를 삽입하는 Mimikatz의 기능입니다.

Mimikatz DCShadow는 공격자가 AD(Active Directory)의 일부가 되는 Rogue DC(도메인 컨트롤러)를 설정하는 데 도움이 됩니다. 일단 등록되면 합법적인 DC로 작동하여 손상을 일으킬 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

T1003 설정 **-** 방어 회피 **- Mimikatz DCShadow** 플레이북

다음 단계를 사용하여 T1003 - Defense Evasion - Mimikatz DCShadow 플레이북을 설정합니다.

시작하기 전에
필요한 역할:

- sn_si.admin
- flow_designer

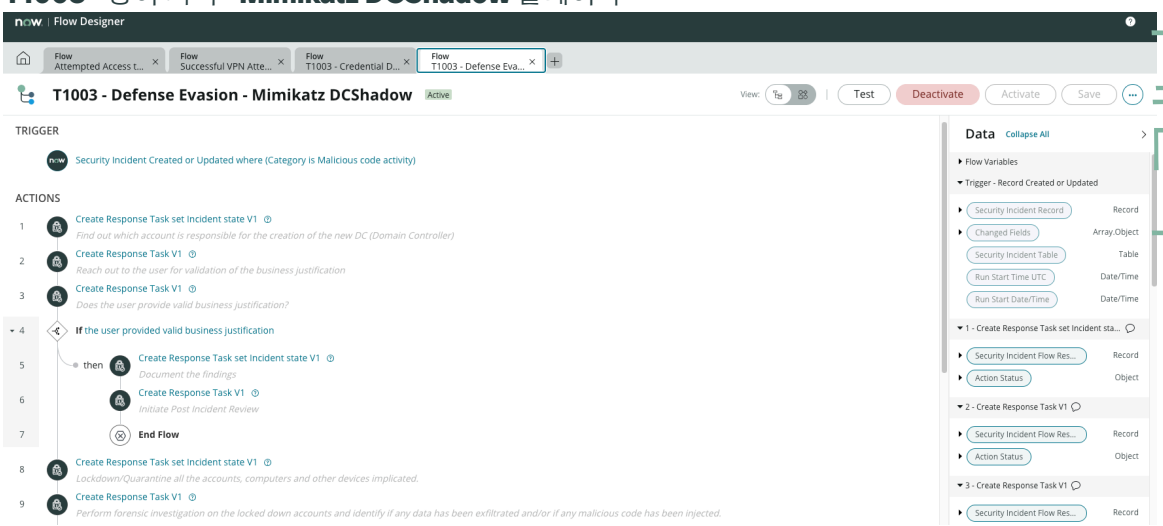
Security Operations 스포크(*sn_sec_spoke*)를 설치했는지 확인하십시오.

프로시저

1. sn_si.user 및 flow_designer 역할을 가진 사용자로 로그인합니다.
2. 다음으로 이동 모두 〉 플로우 디자이너 **T1003 - Defense Evasion - Mimikatz DCShadow** 플레이북을 선택합니다.
3. 옵션: T1003 - Defense Evasion - Mimikatz DCShadow 플레이북 플로우의 복사본을 만들고 필요한 수정을 수행합니다.

   (Optional) 플레이북 플로우의 복사본을 생성하려면 아이콘을 선택하고 플로우 복사를 선택합니다. 플로우를 사용자 지정하거나 특정 변경을 수행하려는 경우에만 이 단계를 수행합니다.

T1003 - 방어 회피 **- Mimikatz DCShadow** 플레이북

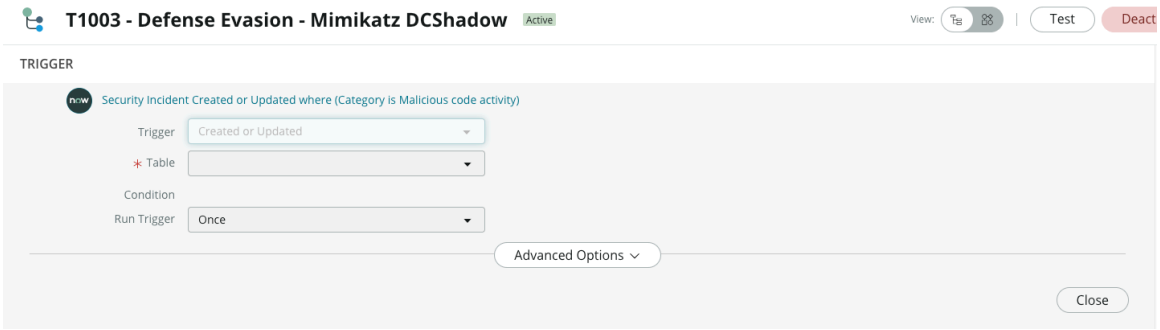


4. 플레이북을 활성화합니다.
   a. 기본 시스템에서 사용할 수 있는 플레이북을 사용하려면 메인 플로우를 활성화합니다.
   b. 필요한 사항을 변경한 후 복사된 플로우를 활성화합니다.
5. 플레이북에 대한 트리거 조건을 설정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 Playbook은 범주 가 악성 코드 활동일 때 트리거되고 보안 인시던트와 연결됩니다.

T1003 - 방어 회피 **- Mimikatz DCShadow** 플레이북 트리거 조건



T1003 - 방어 회피 **- Mimikatz DCShadow** 플레이북 사용

이 Playbook을 사용하여 Mimikatz DCShadow로 인해 발생한 것으로 의심되는 보안 인시던트를 조사합니다. 다음 단계에서는 T1003 - Defense Evasion - Mimikatz DCShadow 플레이북에서 사용할 수 있는 작업, 작업 및 하위 플로우에 대한 안내를 제공합니다.

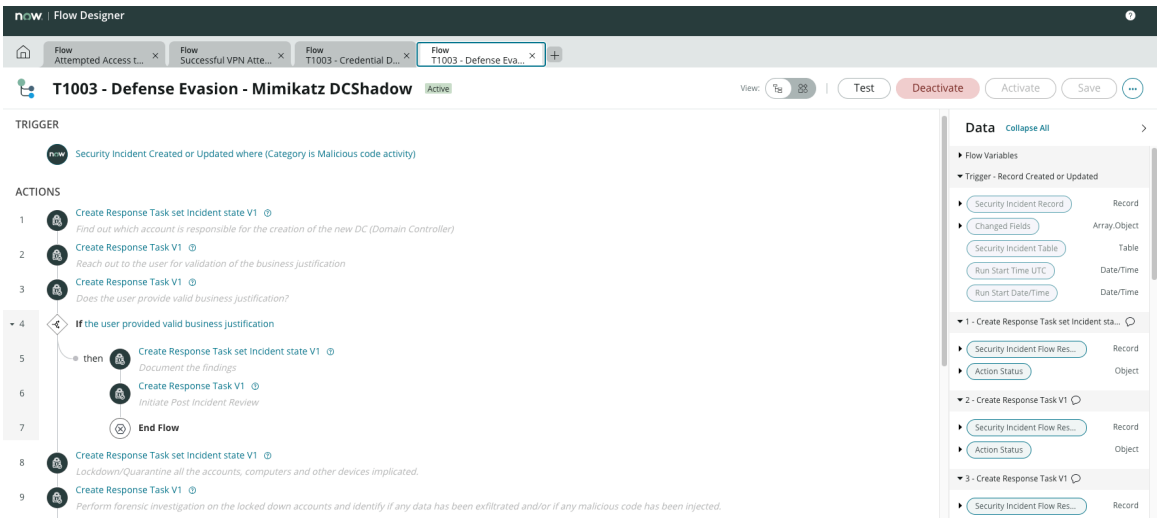
시작하기 전에
필요한 역할:

- sn_si.admin
- flow_designer

프로시저

1. 플레이북이 트리거되고 실행이 시작되면 작업 1에서 새 DC(도메인 컨트롤러)의 생성을 담당하는 계정을 찾습니다.
2. 작업 2에서 사용자에게 연락하여 비즈니스 정당성을 확인합니다.
   제공된 이메일 템플릿을 사용하여 사용자에게 연락할 수 있습니다.
3. 작업 3에서 사용자가 유효한 비즈니스 정당성을 제공했는지 확인합니다.
4. 작업 4에서 사용자가 유효한 비즈니스 정당성을 제공한 경우 다음 단계를 수행합니다.

T1003 - 방어 회피 **- Mimikatz DCShadow** 플레이북



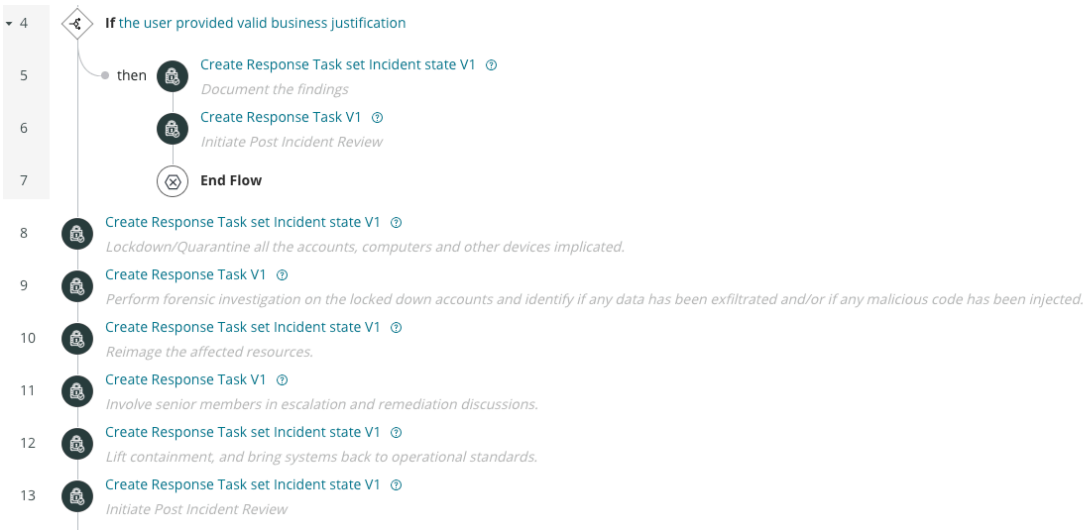
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 작업 5에서는 지금까지의 결과를 문서화합니다.

b. 작업 6에서 사후 인시던트 검토를 시작합니다.
작업 7에서는 사후 인시던트 검토 후 플로우가 종료됩니다.

5. 작업 8에서 사용자가 유효한 비즈니스 정당성을 제공하지 않은 경우 다음 단계를 수행합니다.

T1003 - 방어 회피 **- Mimikatz DCShadow** 플레이북 사용



a. 작업 9에서는 관련된 모든 계정, 컴퓨터 및 기타 장치를 잠그거나 격리합니다.

b. 작업 10에서 잠긴 계정에 대해 포렌식 조사를 수행하고 데이터가 유출되었거나 악성 코드가 삽입되었는지 확인합니다.

c. 작업 11에서 영향을 받는 자원의 이미지를 다시 설치합니다.

d. Action 12에서는 봉쇄를 해제하고 시스템을 운영 표준으로 되돌립니다.

e. 작업 13에서 작업을 종결하기 전에 사후 인시던트 검토를 완료합니다.

T1003용 플레이북 **-** 자격 증명 덤핑 **- Mimikatz DCSync**

이 플레이북은 Mimikatz DCSync에 의해 발생한 것으로 의심되는 인시던트를 조사하기 위한 체계적인 정정 단계를 제공합니다. 이 플레이북은 Mimikatz 함수 (`lsadump::d csync`) 중 하나가 사용될 때 트리거됩니다. 이 함수는 일반적으로 공격받는 DC(도메인 컨트롤러)에서 사용됩니다.

Mimikatz는 사용자가 공격받은 시스템에서 기밀 데이터를 검색하는 데 도움이 되는 명령을 내릴 수 있도록 하는 인기 있는 해킹 도구입니다. 기밀 데이터에는 암호, 해시 등이 포함됩니다.

주:
이 경보는 충실도가 높은 경보로, 거의 트리거되지 않는 것으로 간주됩니다. 트리거되면 즉시 선임 팀 구성원이나 관리자에게 알려야 합니다.

T1003 설정 **-** 자격 증명 덤핑 **- Mimikatz DCsync** 플레이북

다음 단계를 사용하여 T1003 - 자격 증명 덤핑 - Mimikatz DCsync 플레이북을 설정합니다.

시작하기 전에
필요한 역할:

- sn_si.admin
- flow_designer

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

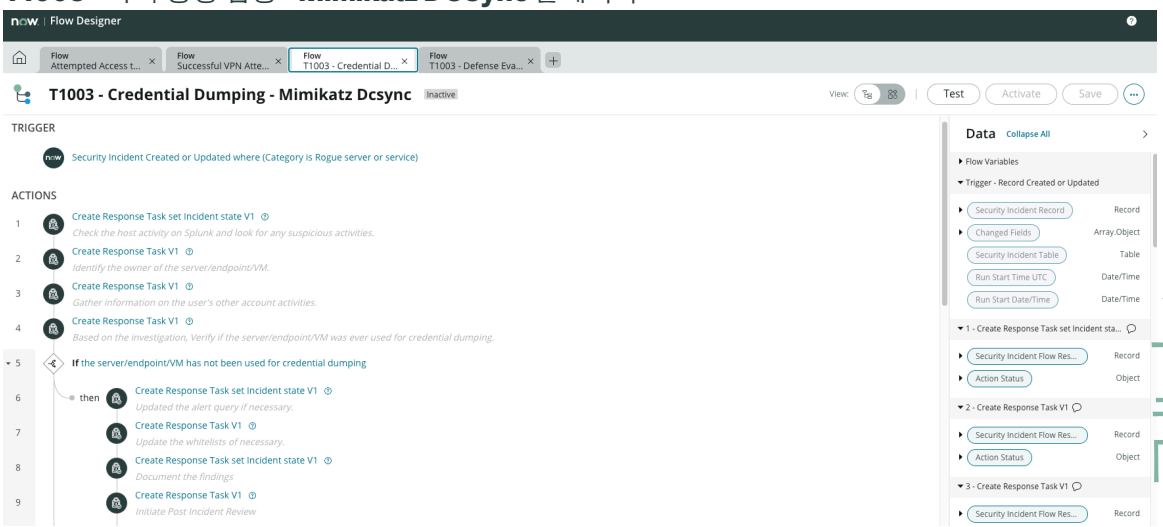
Security Operations 스포크(*sn_sec_spoke*)를 설치했는지 확인하십시오.

프로시저

1. sn_si.user 및 flow_designer 역할을 가진 사용자로 로그인합니다.
2. 다음으로 이동 모두 〉 플로우 디자이너 을 클릭하고 **T1003 -** 자격 증명 덤핑 **- Mimikatz DCsync** 플레이북을 선택합니다.
3. 옵션: T1003 - 자격 증명 덤핑 - Mimikatz DCsync 플레이북 흐름의 복사본을 만들고 필요한 수정을 수행합니다.

   (Optional) 플레이북 플로우의 복사본을 생성하려면 아이콘을 선택하고 플로우 복사를 선택합니다. 플로우를 사용자 지정하거나 특정 변경을 수행하려는 경우에만 이 단계를 수행합니다.

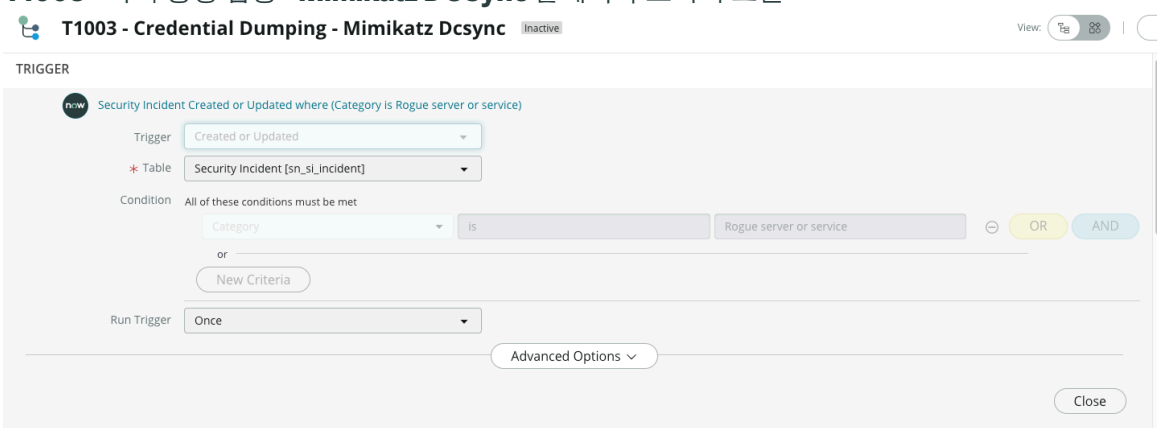
T1003 - 자격 증명 덤핑 **- Mimikatz DCSync** 플레이북



4. 플레이북을 활성화합니다.
   a. 기본 시스템에서 사용할 수 있는 플레이북을 사용하려면 메인 플로우를 활성화합니다.
   b. 필요한 사항을 변경한 후 복사된 플로우를 활성화합니다.
5. 플레이북에 대한 트리거 조건을 설정합니다.

   범주가 **Rogue** 서버 또는 서비스일 때 이 Playbook이 트리거되고 보안 인시던트와 연결됩니다.

T1003 - 자격 증명 덤핑 **- Mimikatz DCSync** 플레이북 트리거 조건



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

T1003 - 자격 증명 덤핑 - Mimikatz DCsync 플레이북 사용

이 플레이북을 사용하여 Mimikatz DCSync로 인해 발생한 것으로 의심되는 인시던트를 조사합니다. 다음 단계에서는 T1003 - 자격 증명 덤핑 - Mimikatz DCsync 플레이북에서 사용할 수 있는 작업, 작업 및 하위 흐름에 대한 연습을 제공합니다.

시작하기 전에

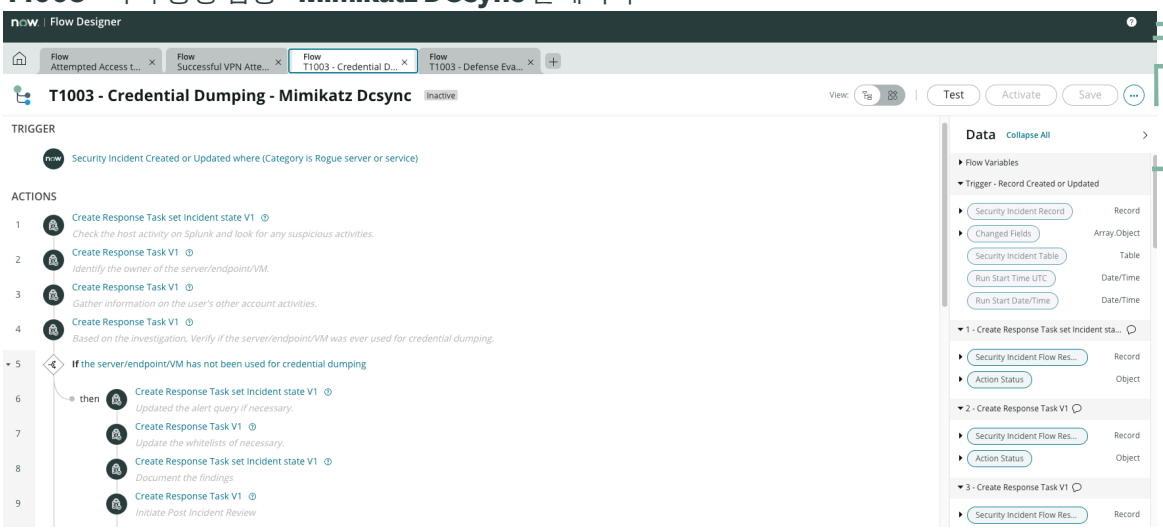
필요한 역할:

- sn_si.admin
- flow_designer

프로시저

1. 플레이북이 트리거되고 실행이 시작되면 작업 1에서 Splunk의 호스트 활동을 확인하고 의심스러운 활동이 있는지 찾습니다.
2. 작업 2에서 서버/엔드포인트/VM의 소유자를 식별합니다.
   사용자가 온라인 상태인 경우 CrowdStrike EDR을 실행하여 시스템 활동의 범위를 더 잘 수집합니다.
3. 작업 3에서 사용자의 다른 계정 활동에 대한 정보를 수집합니다.
4. 작업 4에서 조사에 따라 서버/엔드포인트/VM이 자격 증명 덤핑에 사용된 적이 있는지 확인합니다.
5. 작업 5에서 서버/엔드포인트/VM이 자격 증명 덤핑에 사용되지 않은 경우 다음 작업을 수행합니다.

T1003 - 자격 증명 덤핑 - Mimikatz DCsync 플레이북



   a. 작업 6에서 필요한 경우 경보 쿼리를 업데이트합니다.

   b. 작업 7에서 필요한 경우 허용 목록을 업데이트합니다.

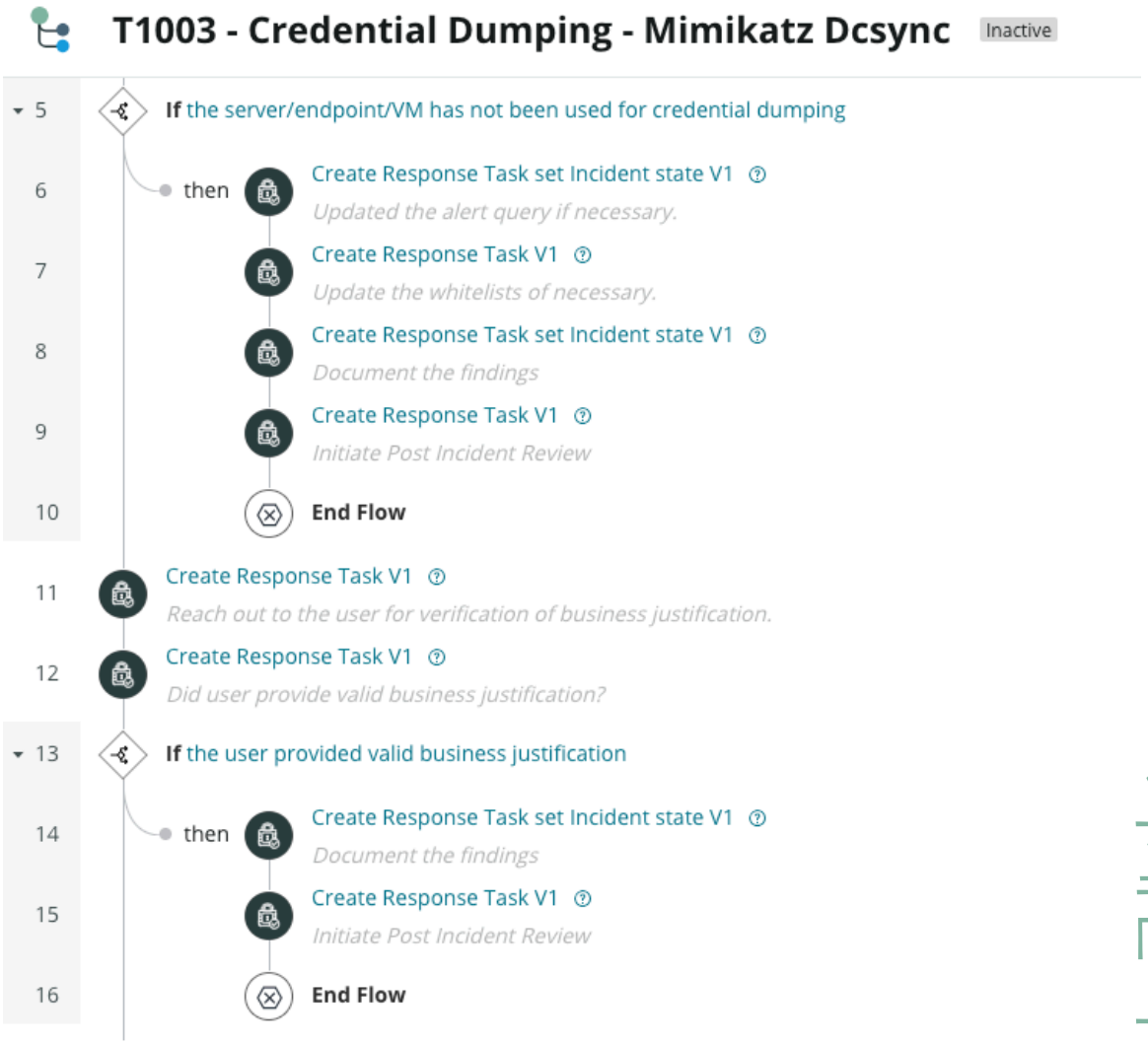
   c. 작업 8에서는 지금까지의 결과를 문서화합니다.

   d. 작업 9에서 사후 인시던트 검토를 시작합니다.
   동작 10에서 흐름이 종료됩니다.

6. 자격 증명 덤핑에 서버/엔드포인트/VM을 사용한 경우 작업 11에서 사용자에게 연락합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

T1003 - 자격 증명 덤핑 **- Mimikatz DCsync** 플레이북 사용



7. 작업 12에서 사용자에게 연락하여 비즈니스 정당성을 확인합니다.

8. 작업 13에서 사용자가 유효한 비즈니스 정당성을 제공한 경우 다음 작업을 수행합니다.

a. Action 14에서는 지금까지의 결과를 문서화합니다.

b. 작업 15에서 사후 인시던트 검토를 시작합니다.
작업 16에서 흐름이 종료됩니다.

9. 사용자가 유효한 비즈니스 정당성을 제공하지 않은 경우 작업 17에서 시스템을 격리합니다.

10. Action 18에서 불량 계정에 의해 생성되거나 삭제되었을 수 있는 원치 않는 파일을 제거합니다.

11. 액션 19에서는 봉쇄를 해제하고 시스템을 운영 표준으로 되돌립니다.

12. 작업 20에서 작업을 닫기 전에 사후 인시던트 검토를 완료합니다.

여러 IP에서 **Okta** 사용자 로그인 실패를 위한 플레이북

이 플레이북은 Okta에서 사용자 로그인 실패 인시던트를 조사하기 위한 체계적인 정정 단계를 제공합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

여러 IP에서 Okta 사용자 로그인 실패 플레이북에서는 여러 비 ServiceNow IP의 Okta에서 ServiceNow 계정 실패가 관찰될 때 경보를 분석하는 방법에 대한 지침을 제공합니다. 이 플레이북과 관련된 경보가 Okta 로그를 확인합니다. 1시간 동안 3개를 초과하는 비 ServiceNow IP 범위에서 ServiceNow 사용자 ID에 대해 로그인 실패가 발생하면 경보를 트리거합니다.

다중 IP에서 **Okta** 사용자 로그인 실패 플레이북 설정

다음 단계를 사용하여 다중 IP에서 Okta 사용자 로그인 실패 플레이북을 설정합니다.

시작하기 전에

필요한 역할:

- sn_si.admin
- flow_designer

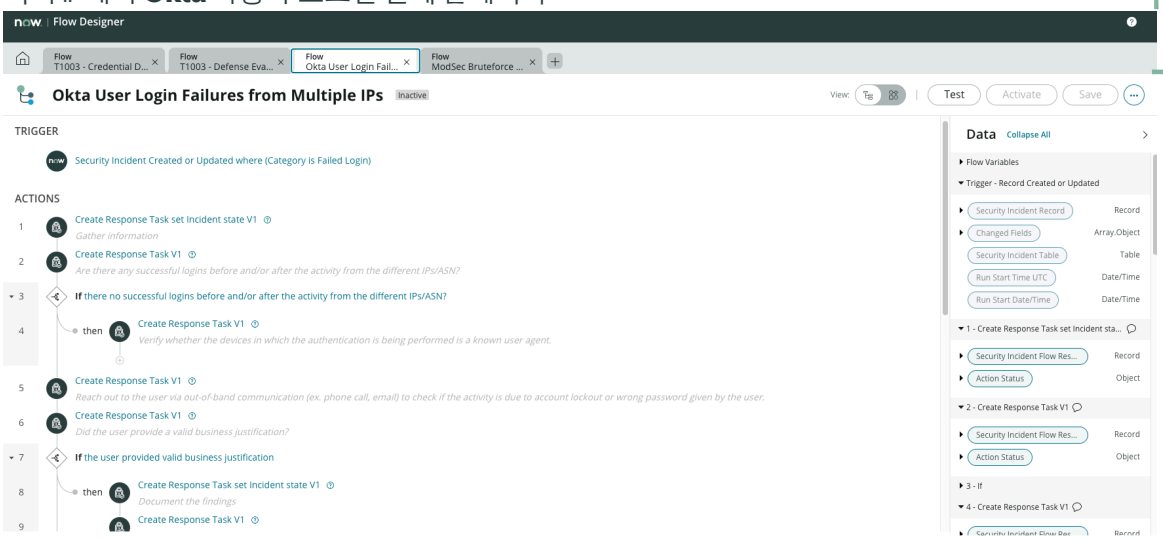
Security Operations 스포크(*sn_sec_spoke*)를 설치했는지 확인하십시오.

프로시저

1. sn_si.user 및 flow_designer 역할을 가진 사용자로 로그인합니다.
2. 다음으로 이동 모두 〉 플로우 디자이너 을 클릭하고 여러 IP에서 **Okta** 사용자 로그인 실패 플레이북을 선택합니다.
3. 옵션: 다중 IP에서 Okta 사용자 로그인 실패 플레이북 플로우의 사본을 생성하고 필요에 따라 수정합니다.

   (Optional) 플레이북 플로우의 복사본을 생성하려면 아이콘을 선택하고 플로우 복사를 선택합니다. 플로우를 사용자 지정하거나 특정 변경을 수행하려는 경우에만 이 단계를 수행합니다.

   여러 IP에서 **Okta** 사용자 로그인 실패 플레이북

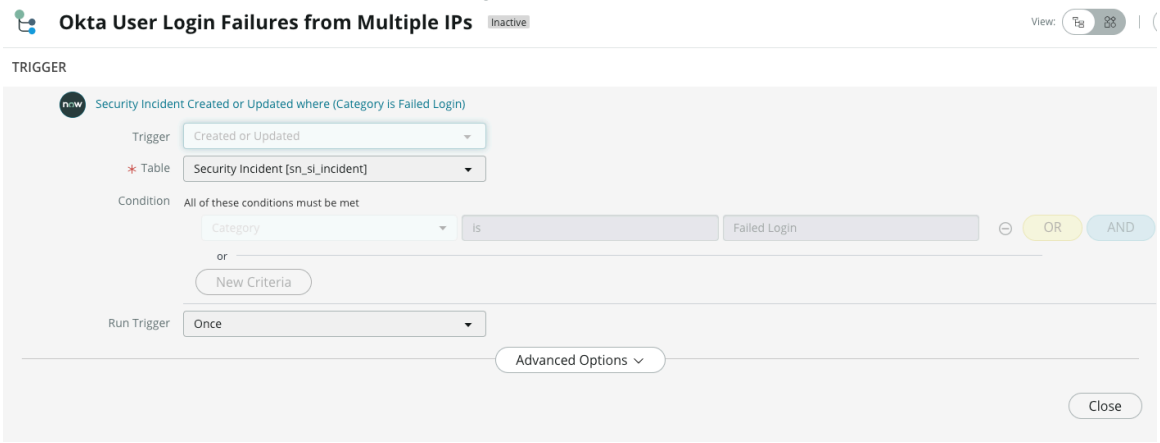


4. 플레이북을 활성화합니다.
   a. 기본 시스템에서 사용할 수 있는 플레이북을 사용하려면 메인 플로우를 활성화합니다.
   b. 필요한 사항을 변경한 후 복사된 플로우를 활성화합니다.
5. 플레이북에 대한 트리거 조건을 설정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 플레이북은 범주 가 로그인에 실패할 때 트리거되고 보안 인시던트와 연결됩니다.

여러 IP에서 **Okta** 사용자 로그인 실패 **Playbook** 트리거 조건



다중 IP에서 **Okta** 사용자 로그인 실패 플레이북 사용

이 플레이북을 사용하여 Okta의 사용자 로그인 실패에 대한 보안 인시던트를 조사합니다. 다음 단계에서는 다중 IP에서 Okta 사용자 로그인 실패 플레이북에서 사용할 수 있는 작업, 작업 및 하위 플로우에 대한 안내를 제공합니다.

시작하기 전에
필요한 역할:

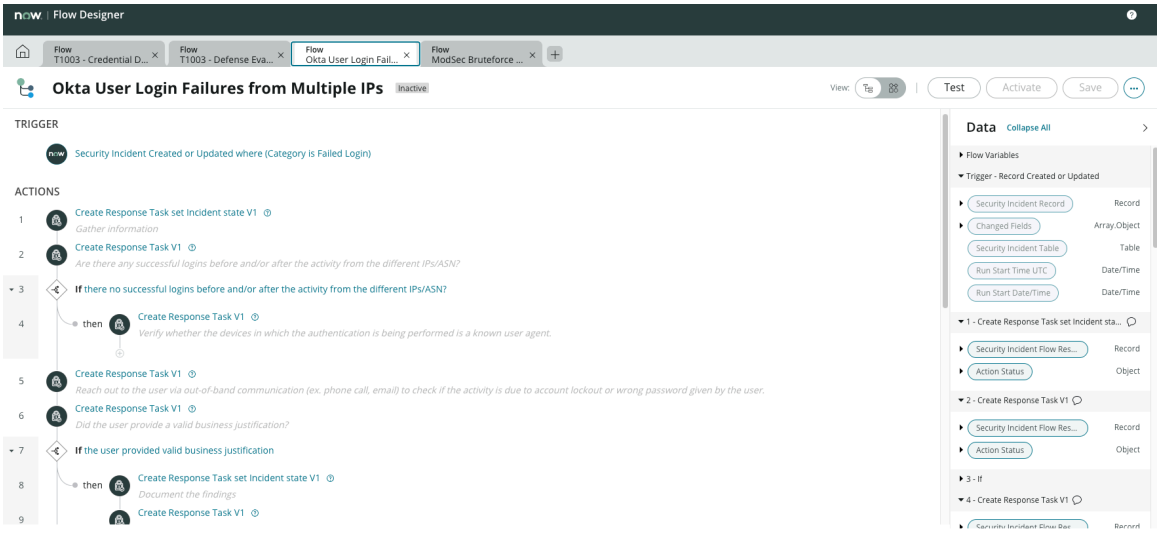
- sn_si.admin
- flow_designer

프로시저

1. 플레이북이 트리거되고 실행이 시작되면 작업 1에서 다음 작업을 수행합니다.
   - 대상이 되는 사용자 계정을 식별합니다.
   - IP 서브넷을 확인하고 모두 동일한 ASN(Autonomous System Number) 소유자에 속하는지 확인합니다.
2. 작업 2에서 다른 IP/ASN의 활동 이전 또는 이후에 성공적인 로그인이 있었는지 확인합니다.
3. 작업 3에서 다른 IP/ASN의 활동 전후에 로그인에 성공하지 못한 경우 작업 4에서 인증이 수행되는 디바이스가 알려진 사용자 에이전트인지 확인합니다.
   알려진 사용자 에이전트가 장치를 인증하면 플로우가 종료됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

여러 IP에서 **Okta** 사용자 로그인 실패 플레이북



4. 작업 5에서는 조사에 따라 대역 외 통신(예: 전화 통화 또는 이메일)을 통해 사용자에게 연락하여 활동이 계정 잠금 또는 사용자가 제공한 잘못된 암호로 인한 것인지 확인합니다.
5. 작업 6에서 사용자가 유효한 비즈니스 정당성을 제공했는지 확인합니다.
6. 작업 7에서 사용자가 유효한 비즈니스 정당성을 제공한 경우 다음 작업을 수행합니다.

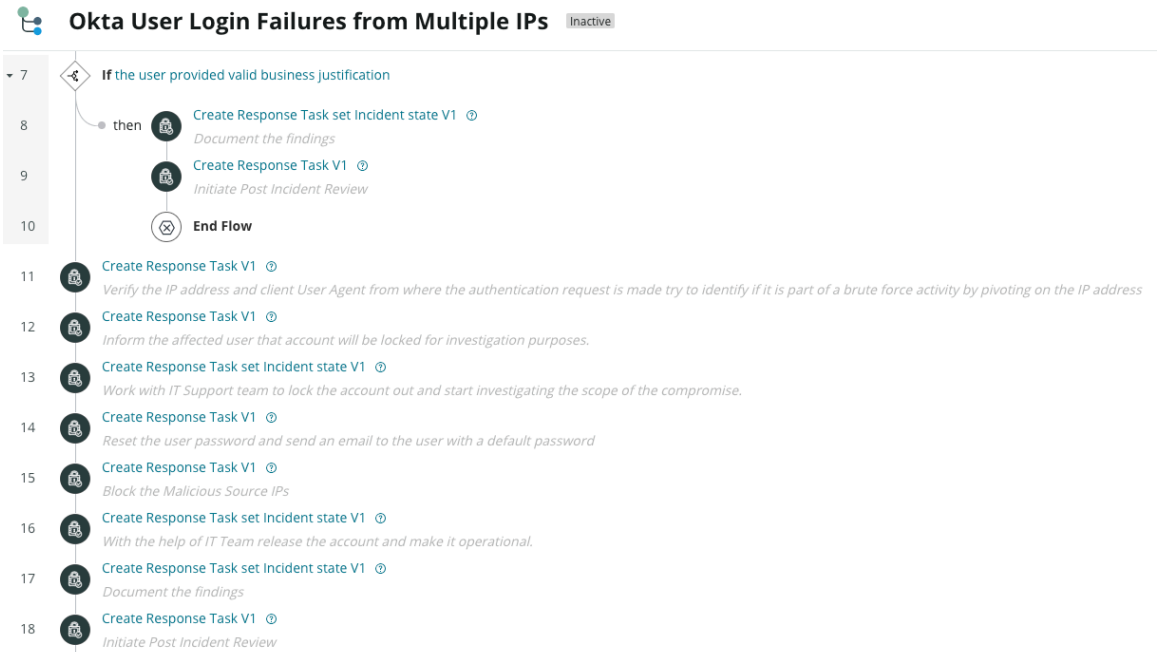
   a. 작업 8에서 지금까지의 결과를 문서화하는 응답 작업을 생성합니다.

   b. 작업 9에서 사후 인시던트 검토를 시작하는 응답을 생성합니다.
   동작 10에서 흐름이 종료됩니다.

7. 작업 11에서 인증 요청이 수행된 IP 주소 및 클라이언트 사용자 에이전트를 확인하고 IP 주소를 피벗하여 무차별 암호 대입 활동의 일부인지 확인합니다.
8. 작업 12에서 영향을 받는 사용자에게 조사 목적으로 계정이 잠길 것임을 알립니다.
   제공된 이메일 템플릿을 사용하여 영향을 받는 사용자에게 알릴 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다중 IP에서 **Okta** 사용자 로그인 실패 플레이북 사용



9. 작업 13에서 IT 지원 팀과 협력하여 계정을 잠그고 손상 범위를 조사하기 시작합니다.
10. 작업 14에서 사용자 암호를 재설정하고 기본 암호를 사용하여 사용자에게 이메일을 보냅니다.
11. 작업 15에서 악성 소스 IP를 차단합니다.
12. 작업 16에서 IT 지원 팀의 도움을 받아 계정을 해제하고 운영 표준으로 되돌립니다.
13. Action 17에서는 지금까지의 결과를 문서화합니다.
14. 작업 18에서 작업을 종결하기 전에 사후 인시던트 검토를 완료합니다.

ModSec 플레이북 **IP** 버스트별 무차별 암호 대입 공격

이 플레이북은 ModSec에서 탐지한 여러 IP의 로그인 페이지에 대한 무차별 암호 대입 공격 인시던트를 조사하기 위한 체계적인 해결 단계를 제공합니다. 이벤트 조건은 ModSec 정책 자체에서 설정할 수 있으며 ModSec에서 이벤트가 생성될 때 Splunk에서 경보를 발생시킵니다.

이 플레이북은 로그인 페이지에서 비정상적인 트래픽 수를 탐지하는 데 도움이 됩니다. 이 예에서는 IP에서 로그인 페이지로 50회 이상의 연속 버스트가 두 번 연속으로 발생해야 하며, 이는 무차별 암호 대입 로그인 시도를 나타냅니다.

IP 버스트별 모드보안 무차별 암호 대입 플레이북 설정

다음 단계를 사용하여 IP 버스트별 ModSec 무차별 암호 대입 플레이북을 설정합니다.

시작하기 전에
필요한 역할:

- sn_si.admin
- flow_designer

Security Operations 스포크(*sn_sec_spoke*)를 설치했는지 확인하십시오.

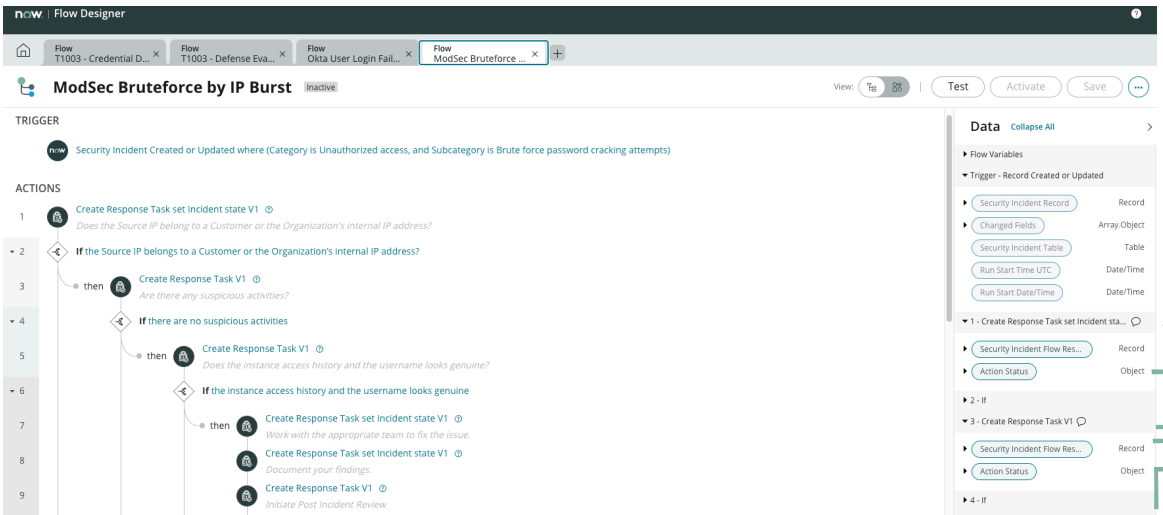
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. sn_si.user 및 flow_designer 역할을 가진 사용자로 로그인합니다.
2. 다음으로 이동 모두 〉 플로우 디자이너 을 클릭하고 **ModSec Bruteforce by IP Burst** 플레이북을 선택합니다.
3. 옵션: IP 버스트별 모드보안 무차별 암호 대입 플레이북 플로우의 사본을 생성하고 필요에 따라 수정합니다.

   (Optional) 플레이북 플로우의 복사본을 생성하려면 추가 작업 메뉴 아이콘( )을 선택하고 플로우 복사를 선택합니다. 플로우를 사용자 지정하거나 특정 변경을 수행하려는 경우에만 이 단계를 수행합니다.

ModSec IP 버스트별 무차별 암호 대입 공격 플레이북

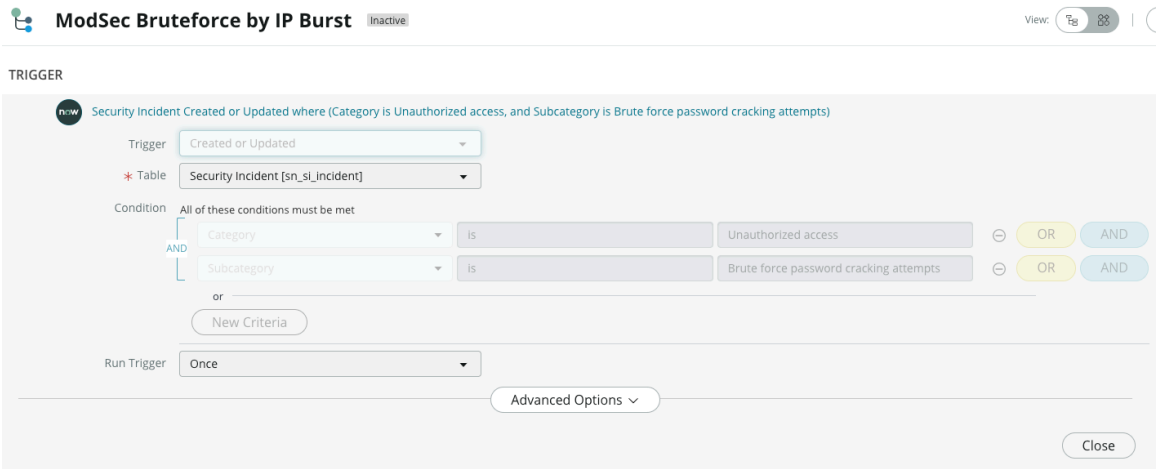


4. 플레이북을 활성화합니다.
   a. 기본 시스템에서 사용할 수 있는 플레이북을 사용하려면 메인 플로우를 활성화합니다.
   b. 필요한 사항을 변경한 후 복사된 플로우를 활성화합니다.
5. 플레이북에 대한 트리거 조건을 설정합니다.
   다음 조건이 충족되면 이 플레이북이 트리거되고 보안 인시던트와 연결됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 범주 는 무단 접근입니다.
- 하위 범주 는 무차별 암호 대입 공격 시도입니다.

ModSec IP별 무차별 암호 대입 공격 버스트 플레이북 트리거 조건



IP 버스트별 모드 보안 무차별 암호 대입 공격 플레이북 사용

이 플레이북을 사용하여 ModSec에서 탐지한 여러 IP의 로그인 페이지에 대한 무차별 암호 대입 공격 인시던트를 조사합니다. 다음 단계에서는 IP 버스트별 ModSec 무차별 암호 대입 플레이북에서 사용할 수 있는 작업, 작업 및 하위 플로우에 대한 안내를 제공합니다.

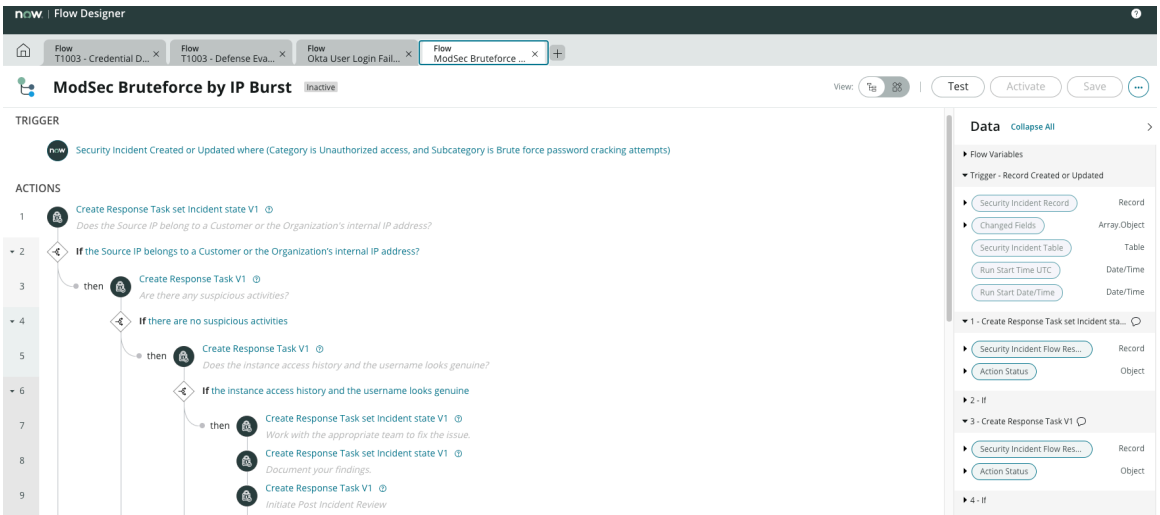
시작하기 전에
필요한 역할:

- sn_si.admin
- flow_designer

프로시저

1. 플레이북이 트리거되고 실행이 시작되면 작업 1에서 소스 IP가 고객 또는 조직의 내부 IP 주소에 속하는지 확인합니다.
2. 작업 2에서 소스 IP가 고객 또는 조직의 내부 IP 주소에 속하는 경우 다음 단계를 수행합니다.

ModSec IP 버스트별 무차별 암호 대입 공격 플레이북



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 작업 3에서 의심스러운 활동이 있었는지 확인합니다.

- 지난 며칠 동안 소스 IP에서 활동을 확인합니다. IP에 무시할 수 있는 트래픽이 있는 경우 실제 공격을 나타냅니다.
- 스프레이 사용자 이름을 확인하십시오. 예를 들어 사용자 이름이 알파벳 순서로 정렬되어 있는지 확인합니다.
- 관련된 일반 계정 이름을 찾으십시오. 예를 들어 관리자, sysadmin, 루트, 관리자 및 기타 애플리케이션 계정 이름입니다.

의심스러운 활동이 없으면 플로우가 종료됩니다.

b. 작업 4에서 의심스러운 활동이 있는 경우 작업 5에서 인스턴스 액세스 기록과 사용자 이름이 진짜인지 확인합니다.

로그에서 *Appnode* 실패 징후를 확인합니다. 운영 문제로 인해 SAML, SSO 또는 LDAP 실패 이벤트가 발생할 수 있습니다.

인스턴스 액세스 이력과 사용자 이름이 진짜로 보이지 않으면 플로우가 종료됩니다.

c. 작업 6에서 인스턴스 액세스 기록과 사용자 이름이 정품인 것 같으면 다음 단계를 수행합니다.

i. 작업 7에서 적절한 팀과 협력하여 문제를 해결합니다.

ii. 작업 8에서는 지금까지의 결과를 문서화합니다.

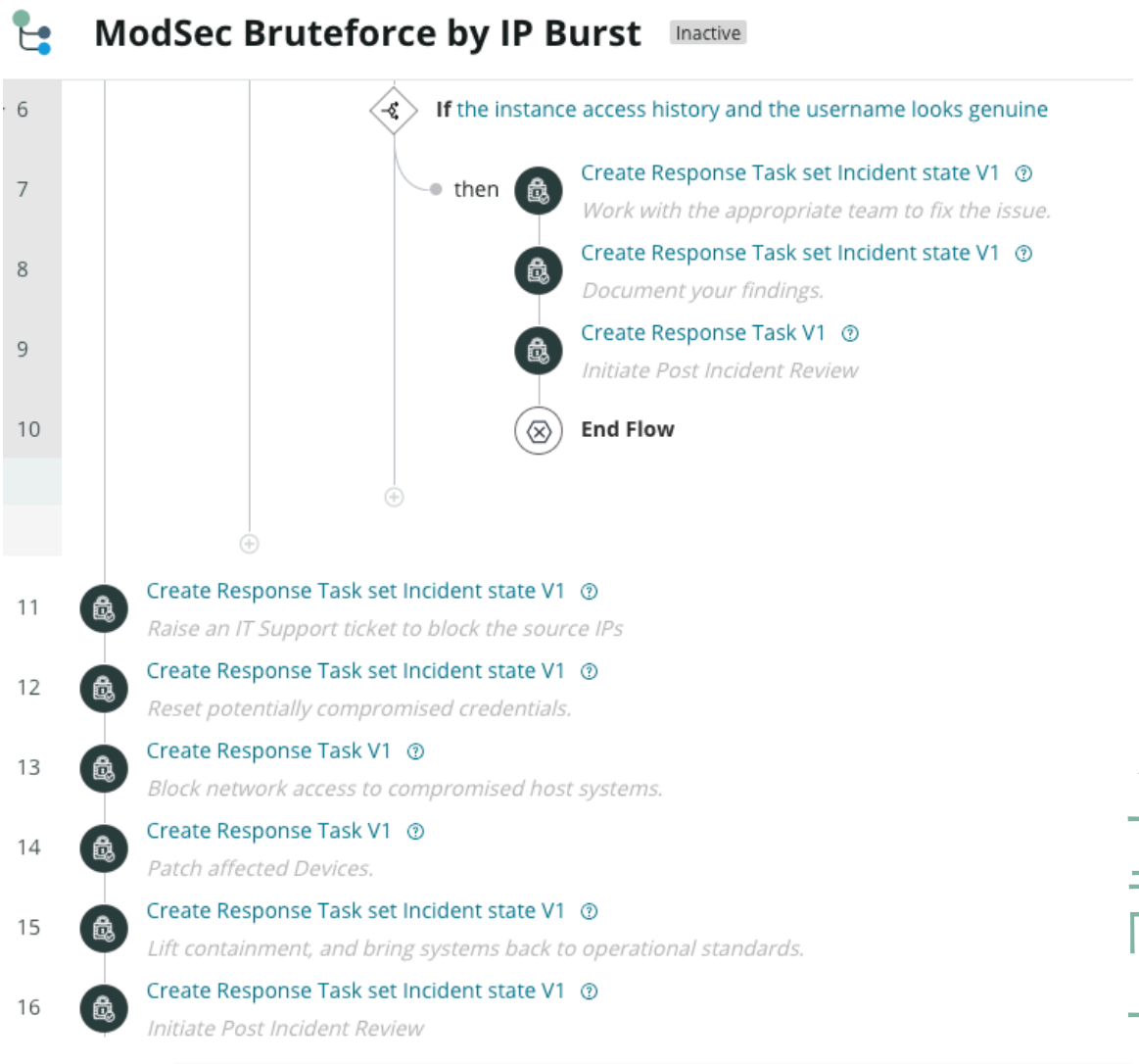
iii. 작업 9에서 작업을 닫기 전에 사후 인시던트 검토를 완료합니다.

동작 10에서 흐름이 종료됩니다.

3. 원본 IP가 고객 또는 조직의 내부 IP 주소에 속하지 않는 경우 작업 11에서 IT 지원 티켓을 제기하여 원본 IP를 차단합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

ModSec 무차별 암호 대입 공격 **IP** 버스트 플레이북 사용



4. 작업 12에서 잠재적으로 손상된 자격 증명을 재설정합니다.
5. 작업 13에서 손상된 호스트 시스템에 대한 네트워크 액세스를 차단합니다.
6. 작업 14에서 영향을 받는 디바이스에 패치를 적용합니다.
7. 작전 15에서는 격납고를 해제하고 시스템을 작동 표준으로 되돌립니다.
8. 작업 16에서 작업을 종결하기 전 사후 인시던트 검토를 완료합니다.

보안 인시던트 응답 플레이북 작업

이 단원에서는 Flow Designer 작업 라이브러리에서 제공되는 동작에 대해 설명합니다.

작업 이름	설명	예시 시나리오	
보안 인시던트에 보안 태그 추가	이 작업을 사용하면 플로우 디자이너 논리를 사용하여 보안 태그를 자동으로 추가할 수 있습니다.	플로우에서 IOC를 탐지하면 이 작업을 사용하여 **IOC** 탐지됨 태그를 자동으로 추가할 수 있습니다.	• 입력: 보안 인시던트, 보안 태그 • 출력: 해당 사항 없음

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업 이름	설명	예시 시나리오	
		흐름:	
보안 인시던트에 옵저버블 추가	이 작업을 사용하여 선택한 보안 인시던트에 옵저버블을 추가합니다. • 기본적으로 옵저버블 목록은 쉼표(,) 구분 기호로 구분되지만 수정할 수 있습니다. 다른 단일 특수 문자를 구분 기호로 지정할 수 있습니다. 옵저버블을 추가하는 동안 유형(URL, IP 주소, 해시)이 자동으로 설정됩니다. • 옵저버블이 보안 인시던트에 추가되면 유형(URL, IP 주소, 해시)이 자동으로 설정됩니다. • 옵저버블이 추가될 때 허용 목록 옵저버블 필터링 옵션은 허용 목록 옵저버블을 식별하지만 보안 인시던트의 옵저버블 관련 목록에 추가하지 않습니다. 이러한 옵저버블이 제거되었음을 나타내기 위해 자동화된 시스템 활동(응답)이 추가됩니다.		• 입력: ○ 보안 인시던트 ○ 옵저버블 ○ 구분 기호 ○ 허용 목록 옵저버블 및 사후 활동 메모 필터링 • 출력: 해당 사항 없음
여러 보안 인시던트 V1에서 영향을 받는 사용자(관련 목록) 가져오기	지정된 보안 인시던트의 영향을 받는 사용자 관련 목록에 나열된 영향을 받는 모든 사용자를 검색합니다.	여러 하위 보안 인시던트와 함께 상위 보안 인시던트가 있을 수 있습니다. 이 작업을 사용하여 영향을 받는 사용자를 모든 하위 보안 인시던트에서 해당 상위 보안 인시던트로 롤업합니다. 영향을 받는 고유 사용자만 롤업되고 모든 중복 항목은 제거됩니다.	• 입력: 보안 인시던트 • 출력: ○ 영향을 받는 사용자 ○ 카운트

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업 이름	설명	예시 시나리오	
여러 보안 인시던트에서 영향을 받는 사용자 가져오기	지정된 보안 인시던트에 대해 영향을 받는 기본 사용자를 검색합니다. 영향을 받는 사용자 관련 목록의 영향을 받는 사용자는 포함되지 않습니다.	• 피싱 보안 인시던트를 조사하는 동안 영향을 받는 기본 사용자(피싱 인시던트를 보고한 사용자)에게 이메일을 보내 피싱 이메일의 악성 링크를 클릭한 사용자가 있는지 확인합니다. • 영향을 받는 기본 사용자 수를 기준으로 상위 보안 인시던트 심각도 또는 위험 점수를 업데이트합니다.	• 입력: 보안 인시던트 • 출력: ○ 영향을 받는 사용자 ○ 카운트
보안 인시던트에서 영향을 받는 사용자(관련 목록) 가져오기	지정된 보안 인시던트의 영향을 받는 사용자 관련 목록에 나열된 영향을 받는 모든 사용자를 검색합니다.		• 입력: 보안 인시던트 • 출력: ○ 영향을 받는 사용자 ○ 카운트
영향을 받는 사용자를 보안 인시던트에 추가	영향을 받는 모든 사용자를 보안 인시던트에 추가합니다.	여러 하위 보안 인시던트가 있는 상위 보안 인시던트가 있다고 가정해 보겠습니다. 이 작업을 사용하여 영향을 받는 사용자를 모든 하위 보안 인시던트에서 해당 상위 보안 인시던트로 롤업할 수 있습니다. 영향을 받는 고유 사용자만 롤업되고 모든 중복 항목은 제거됩니다.	• 입력: ○ 보안 인시던트 ○ 사용자 • 출력: 해당 사항 없음
영향을 받는 사용자의 구성 항목 가져오기	영향을 받는 모든 사용자의 구성 항목(CI)을 검색합니다.	피싱 또는 맬웨어 시나리오에서는 이 작업을 사용하여 영향을 받는 CI(구성 항목) 관련 목록을 업데이트하고 CI를 조사할 수 있습니다. 그런 다음 식별된 CI 수를 기반으로 보안 인시던트의 심각도 또는 위험 점수를	• 입력: 사용자 • 출력: ○ 구성 항목 ○ 카운트

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업 이름	설명	예시 시나리오	
		업데이트할 수 있습니다.	
보안 인시던트에 대한 모든 하위 보안 인시던트 가져오기	특정 상위 보안 인시던트와 관련된 모든 하위 보안 인시던트를 검색합니다.	예제 시나리오: 이 작업을 사용하여 다음을 수행합니다. • 해당 상위 보안 인시던트 상태가 업데이트되면 하위 보안 인시던트의 상태를 업데이트합니다. • 하위 보안 인시던트 수에 따라 보안 인시던트의 심각도 또는 위험 점수를 자동으로 업데이트합니다.	• 입력: ○ 보안 인시던트 ○ 인시던트 상태 • 출력: ○ 하위 보안 인시던트 ○ 카운트
옵저버블에 대한 구성 항목 가져오기(유형 IP 주소)	유형 IP 주소의 옵저버블에 대한 모든 CI(구성 항목)를 검색합니다.	IP 주소 옵저버블을 구성 항목과 연결할 수 있습니다. 예를 들어 서버의 IP 주소입니다. 이 작업을 사용하면 서버에 대한 정보를 검색할 수 있습니다.	• 입력: 옵저버블 IP 주소 • 출력: ○ 구성 항목 ○ 카운트
옵저버블 악성 여부	옵저버블 집합에 하나 이상의 악의적인 옵저버블이 있는지 확인합니다.	위협 조회가 완료되고 악의적인 옵저버블의 존재를 식별한 후에는 보안 인시던트의 심각도 또는 위험 점수를 높일 수 있습니다.	• 입력: 보안 인시던트 • 출력: 악의적(예/아니오)
사용자 상호작용을 확인하기 위해 이메일 보내기	사용자 응답에 대한 응답으로 이메일을 보냅니다.	사용자가 애플리케이션에 로그인을 여러 번 시도했지만 실패하면 로그인 시나리오가 실패합니다. 이 경우 사용자가 로그인을 시도했는지 여부를 확인하기 위해 사용자에게 이메일이 전송됩니다. 사용자 응답(예 또는 아니요)에 따라 다른 작업을 수행할 수 있습니다. 플로우: 실패한 로그인 수동 플레이북	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업 이름	설명	예시 시나리오	
허용 목록 옵저버블 필터링	이 작업을 사용하여 지정된 옵저버블 집합에서 옵저버블 목록을 허용합니다.	옵저버블 집합에서 무시할 수 있는 특정 옵저버블을 식별할 수 있습니다. 이러한 옵저버블은 보안 인시던트를 해결하는 동안 고려되지 않습니다.	• 입력: 보안 인시던트 • 출력: ○ 허용 목록 옵저버블 ○ 카운트
영향을 받는 사용자의 암호 재설정	이 작업을 사용하여 영향을 받는 사용자의 암호를 재설정합니다.	사용자 계정이 해킹되었거나 사용자가 암호 재설정을 요청하는 경우 암호를 재설정하라는 이메일이 사용자에게 전송됩니다. 플로우: 실패한 로그인 수동 플레이북.	
영향을 받는 사용자에 대한 사용자 그룹 가져오기	영향을 받는 사용자의 사용자 그룹 상세 정보를 조회합니다.	조직에서 두 명 이상의 사용자가 피싱 이메일을 보고하는 경우 사용자가 속한 그룹을 확인하고 더 많은 사용자가 영향을 받았는지 확인할 수 있습니다	• 입력: user • 출력: ○ 사용자 그룹 ○ 카운트

Security Incident Response 보고의 시각적 표현

보안 관리자는 맵, 트리맵과 같은 고급 그래픽 인터페이스를 사용하여 관심 영역을 정확히 찾아낼 수 있습니다.

탐색기 대시보드를 자세히 보려면 보안 인시던트 응답 문서를 참조하십시오SIR 작업 공간 대시보드 보기.보안 인시던트 응답 작업 공간

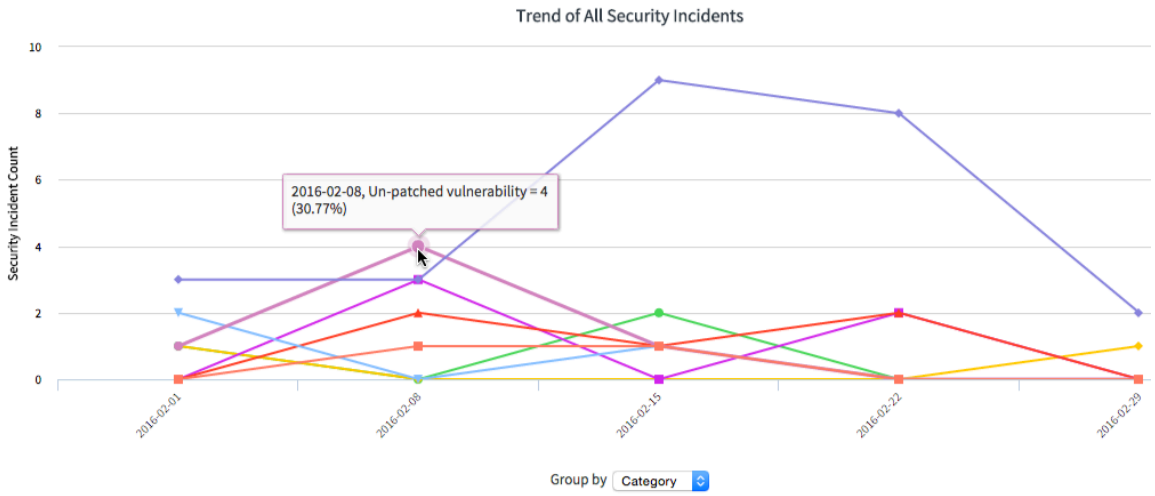
보안 인시던트 응답 개요 대시보드

개요 대시보드는 보안 인시던트 응답 보안 인시던트 활동에 대한 경영적 뷰를 제공하고, 추세와 보고서, 특정 데이터에 대한 드릴다운을 제공합니다.

개요 모듈에는 사용자 역할에 맞게 조정된 보안 인시던트 정보가 표시됩니다. 차트의 원하는 부분(막대형, 원형, 데이터 요소, 열 지도 등)을 가리키면 해당 부분과 관련된 일반 데이터를 볼 수 있습니다. 다음 이미지를 참조하십시오. 보고서의 일부를 클릭하면 자세한 정보를 제공하는 목록이 열립니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모든 보안 인시던트 추세



보안 인시던트 관리자 개요

보안 인시던트 관리자 및 보안 인시던트 관리자 역할의 사용자는 보안 인시던트 관리자 개요를 봅니다. 기본 시스템에는 다음과 같은 보고서가 포함되어 있습니다.

보안 인시던트 관리자 개요 보고서

이름	Visual	설명
팀 내 우선순위가 가장 높은 보안 인시던트	단일 점수	팀에 할당된 중요 보안 인시던트 수입니다.
팀 내 우선순위가 높은 보안 인시던트	단일 점수	팀에 할당된 높은 보안 인시던트의 수입니다.
24시간 이내에 만료되는 SLA	단일 점수	다음 24시간 이내에 만료되는 SLA 수입니다.
위험 대 심각도	열 지도	위험 및 심각도별로 팀에 할당된 보안 인시던트의 분포입니다.
지난 3개월 간의 CI 클래스별 보안 인시던트	가로 막대형 차트	구성 항목 클래스별로 팀에 할당된 보안 인시던트 수입니다.
모든 보안 인시던트 추세	추세	범주 또는 우선순위별로 수신된 보안 인시던트 수를 표시합니다.
무단 접근 보안 인시던트	가로 막대형 차트	시간 경과에 따라 수신된 보안 인시던트 범주의 유형을 표시합니다.
평균 포함 시간	단일 점수	모든 보안 인시던트를 억제하는 데 걸리는 평균 시간입니다.
평균 중요도 포함 시간	단일 점수	중요한 보안 인시던트를 모두 포함하는 데 걸리는 평균 시간입니다.
평균 신원 확인 시간	단일 점수	모든 보안 인시던트를 식별하는 데 걸리는 평균 시간입니다.

보안 분석가 개요

보안 인시던트 분석가 역할의 사용자는 보안 분석가 개요를 볼 수 있습니다. 기본 시스템에는 다음과 같은 보고서가 포함되어 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 분석가 개요 보고서

이름	Visual	설명
내 중요 우선순위 작업	단일 점수	나에게 할당된 중요 보안 인시던트 수입니다.
내 높은 우선순위 작업	단일 점수	나에게 할당된 높은 보안 인시던트 수
24시간 이내에 만료되는 내 SLA	단일 점수	나에게 할당되었으며 다음 24시간 이내에 만료되는 SLA의 수입니다.
나에게 할당된 보안 인시던트	가로 막대형 차트	인시던트 상태 또는 범주별로 나에게 할당된 보안 인시던트입니다.
유형별로 나에게 할당된 작업	가로 막대형 차트	유형 또는 우선순위별로 나에게 할당된 보안 작업(인시던트, 작업 또는 요청)입니다.
나에게 할당된 보안 인시던트, 요청, 작업	목록	나에게 할당된 모든 보안 인시던트, 보안 요청 및 작업의 목록입니다.
보안 인시던트 위치	맵	보안 인시던트의 지역별 위치입니다.
카운트	맵	지역당 보안 인시던트 수입니다.
최소/최대 카운트	색상 스펙트럼 막대	영역당 최소 및 최대 보안 인시던트 수로, 색상 스펙트럼 막대로 표시됩니다.
카운트의 백분율	맵	지역당 총 인시던트 수의 백분율입니다.

보안 인시던트 분석이 활성화된 보안 인시던트 **CISO** 개요

플러그인이 보안 인시던트 분석 활성화되면 보안 인시던트 CISO 및 시스템 관리자 역할을 가진 사용자는 보안 인시던트 CISO 개요를 볼 수 있습니다. 기본 시스템에는 다음과 같은 CISO 보고서가 제공됩니다.

보안 인시던트 **CISO** 개요 보고서(보안 인시던트 분석이 활성화된 상태)

이름	Visual	설명
새 보안 인시던트 금주	단일 점수	이번 주에 수신된 새 보안 인시던트 수입니다.
금주 종결된 보안 인시던트	단일 점수	이번 주에 종결된 보안 인시던트 수입니다.
새 보안 인시던트(7일 이하)	단일 점수	지난 7일 동안 열린 보안 인시던트 수입니다.
종결된 보안 인시던트(7일 이하)	단일 점수	지난 7일 내에 종결된 보안 인시던트 수입니다.
일일 신규 보안 인시던트와 종결된 보안 인시던트 비교	추세	시간 경과에 따른 신규 및 종결된 보안 인시던트 수는 일별로 계산됩니다.
새로운 주간 보안 인시던트와 종결된 보안 인시던트의 비교	추세	시간 경과에 따른 주별 신규 및 종결된 보안 인시던트입니다.
보안 인시던트 종결 코드	추세	시간 경과에 따른 종결 코드의 전체 수입니다.
보안 인시던트 비즈니스 영향	트리맵	비즈니스 중요도별로 사용 가능한 그룹화가 있는 보안 인시던트가 있는 비즈니스 서비스입니다.
평균 포함 시간(주별)	추세	시간 경과에 따라 보안 인시던트를 억제하는 데 걸리는 평균 7일 시간입니다.
평균 근절 시간(주별)	추세	시간 경과에 따라 보안 인시던트를 근절하는 데 걸리는 평균 7일 시간입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 인시던트 **CISO** 개요 보고서(보안 인시던트 분석이 활성화된 상태)

이름	Visual	설명
평균 식별 시간(주별)	추세	시간 경과에 따라 보안 인시던트를 식별하는 데 걸리는 평균 7일 시간입니다.
보안 인시던트 위치	맵	보안 인시던트의 지역별 위치입니다.
카운트	맵	지역당 보안 인시던트 수입니다.
최소/최대 카운트	색상 스펙트럼 막대	영역당 최소 및 최대 보안 인시던트 수로, 색상 스펙트럼 막대로 표시됩니다.
카운트의 백분율	맵	지역당 총 인시던트 수의 백분율입니다.

보안 인시던트 **CISO** 개요 보안 인시던트 분석이 활성화되지 않은 경우

플러그인이 보안 인시던트 분석 활성화되지 않은 경우 보안 인시던트 CISO 및 시스템 관리자 역할을 가진 사용자는 보안 인시던트 CISO 보고 개요를 볼 수 있습니다. 기본 시스템에는 다음과 같은 CISO 보고서가 제공됩니다.

보안 인시던트 **CISO** 개요 보고서(보안 인시던트 분석이 활성화되지 않음)

이름	Visual	설명
새 보안 인시던트 금주	단일 점수	이번 주에 오픈된 새 보안 인시던트 수입니다.
금주 종결된 보안 인시던트	단일 점수	이번 주에 종결된 보안 인시던트 수입니다.
새 보안 인시던트(7일 이하)	단일 점수	지난 7일 동안 열린 보안 인시던트 수입니다.
종결된 보안 인시던트(7일 이하)	단일 점수	지난 7일 내에 종결된 보안 인시던트 수입니다.
새로운 주간 보안 인시던트	추세	새로운 보안 인시던트는 매주 열렸습니다.
종결된 주간 보안 인시던트	추세	보안 인시던트는 주 단위로 종결되었습니다.
보안 인시던트 종결 코드	추세	시간 경과에 따른 보안 인시던트 종결 코드입니다.
보안 인시던트가 있는 비즈니스 서비스 - 비즈니스 영향	트리맵	비즈니스 중요도별로 사용 가능한 그룹화가 있는 보안 인시던트가 있는 비즈니스 서비스입니다.
평균 포함 시간	단일 점수	모든 보안 인시던트를 억제하는 데 걸리는 평균 시간입니다.
평균 중요도 포함 시간	단일 점수	중요한 보안 인시던트를 모두 포함하는 데 걸리는 평균 시간입니다.
평균 신원 확인 시간	단일 점수	모든 보안 인시던트를 식별하는 데 걸리는 평균 시간입니다.

주:
기본 시스템에는 보안 인시던트 응답 사전 구성된 베스트 프랙티스 대시보드를 표시하기 위한 퍼포먼스 분석 솔루션이 포함되어 있습니다. 대시보드는 새 보안 인시던트 또는 미해결 보안 인시던트의 평균 기간과 같은 보안 인시던트 응답 프로세스 분석에 중요한 메트릭을 제공합니다. 자세한 정보 및 설치 지침은 다음을 참조하십시오. 보안 인시던트 응답 플랫폼 분석 솔루션.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 인시던트 응답 탐색기에 액세스

Explorer 대시보드에 보안 인시던트 응답 액세스하여 보안 인시던트 활동을 확인하여 관심 영역을 즉시 찾아내고 문제를 신속하게 해결할 수 있습니다.

시작하기 전에
필요한 역할:

- sn_si.admin(쓰기 위해)
- sn_si_basic(읽기 위해)

프로시저

1. 다음으로 이동 모두 〉 **Self-Service** 〉 홈페이지 또는 다음으로 이동 **Self-Service** 〉 대시보드.
2. 보고서 목록에서 보안 인시던트 탐색기를 선택합니다.

결과
탐색기 대시보드가 보안 인시던트 응답 나타납니다.

다음에 수행할 작업
탐색기 대시보드를 자세히 보려면 보안 인시던트 응답 문서를 참조하십시오SIR 작업 공간 대시보드 보기.보안 인시던트 응답 작업 공간

보안 인시던트 맵

보안 인시던트 맵은 지리적 위치별로 데이터를 제공합니다. 월드 맵은 인시던트가 발생하는 모든 영역에서 강조 표시됩니다. 플러그인이 보안 인시던트 분석 활성화되면 개요에 보안 인시던트 맵을 추가할 수 있습니다 보안 인시던트 응답 . 맵을 추가한 후에는 맵 필터를 수정하여 맵을 구성할 수 있습니다.

개요에 보안 인시던트 응답 맵 추가

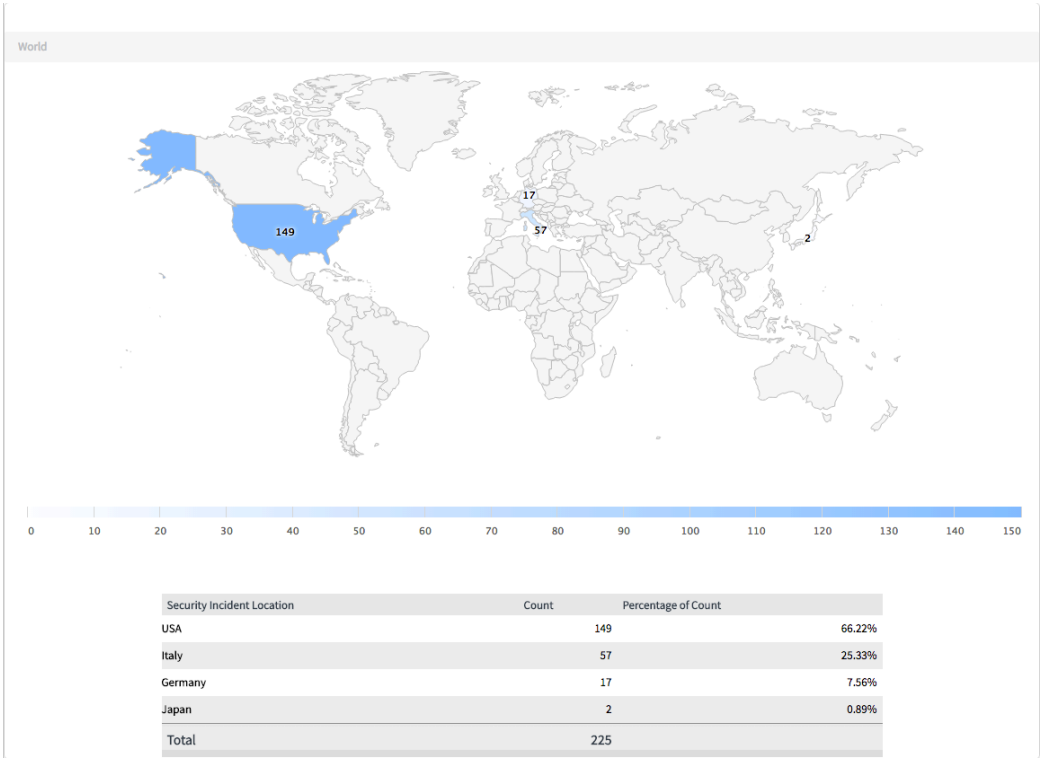
맵에 맵을 보안 인시던트 응답 추가하여 지리적 위치별로 보안 인시던트 데이터를 볼 수 있습니다. 맵을 사용하면 위치별로 보안 인시던트 정보를 드릴다운할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.admin

프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 개요.
2. 페이지의 왼쪽 위 모서리에 있는 콘텐츠 추가를 클릭하여 위젯 선택 컨트롤을 엽니다.
3. 첫 번째 선택 상자에서 보고서를 클릭합니다.
4. 두 번째 선택 상자에서 보안 인시던트를 클릭합니다.
5. 세 번째 선택 상자에서 보안 인시던트 맵을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



Security Incident Location	Count	Percentage of Count
USA	149	66.22%
Italy	57	25.33%
Germany	17	7.56%
Japan	2	0.89%
Total	225	

6. 화면 하단에서 보고서에 추가할 화면의 위치를 클릭합니다.

7. 콘텐츠 추가 상자를 닫습니다.

보안 인시던트 맵 수정

전역 도메인의 관리자는 보안 인시던트 맵에서 필터를 사용하여 보안 인시던트를 처리하는 방법을 수정할 수 있습니다.

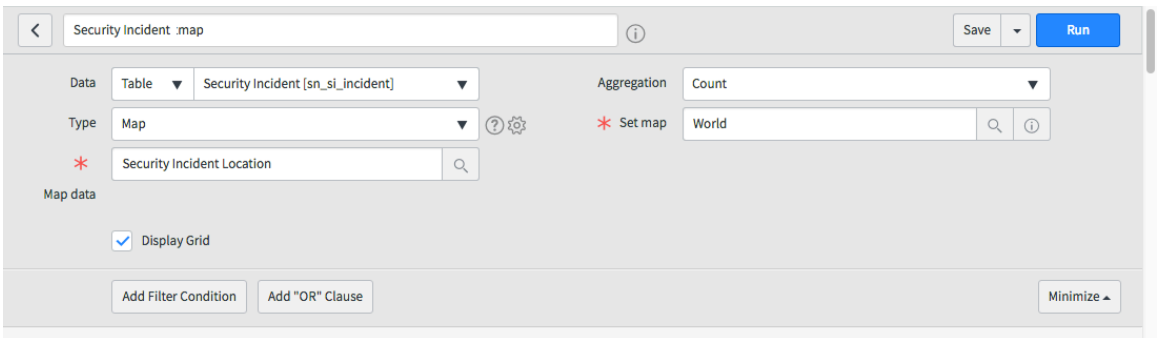
시작하기 전에
필요한 역할: sn_si.admin

프로시저

1. 다음으로 이동 보고서 〉 관리 〉 모두.

2. 보안 인시던트 맵을 검색합니다.

3. 보고서 편집을 클릭합니다.



4. 필터를 추가하거나 편집하려면 필터 조건 추가를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. 실행을 클릭하여 적용된 변경 내용을 확인합니다.
6. 저장을 클릭합니다.

보안 인시던트 트리맵

플러그인이 보안 인시던트 분석 활성화되면 보안 인시던트 - 서비스 영향도 및 보안 인시던트 - 실시간 트리맵을 개요에 추가할 수 있습니다 보안 인시던트 응답 . 트리맵을 추가한 후에는 트리맵 범주와 표시기를 수정하여 트리맵을 구성할 수 있습니다.

보안 인시던트 응답 개요에 트리맵 추가

트리맵은 계층적(트리 구조화) 데이터를 중첩된 사각형 집합으로 표시합니다. 트리의 각 가지에는 사각형이 주어지며, 이 사각형은 하위 분기를 나타내는 더 작은 사각형으로 바둑판식으로 배열됩니다. 트리맵을 사용하면 보안 인시던트 정보를 동적이고 관련성 높은 방식으로 표시할 수 있습니다.

시작하기 전에

필요한 역할: sn_si.admin

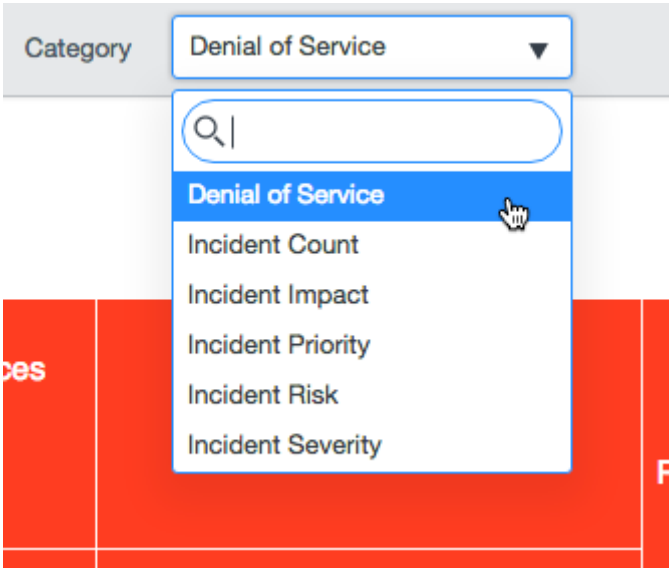
프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 개요.
2. 페이지의 왼쪽 위 모서리에 있는 콘텐츠 추가를 클릭하여 위젯 선택 컨트롤을 엽니다.
3. 첫 번째 선택 상자에서 트리맵을 클릭합니다.
4. 두 번째 선택 상자의 다음 목록에서 삽입할 트리맵을 선택합니다.
   - 보안 인시던트 - 서비스 영향도
   - 보안 인시던트 - 실시간
   - 보안 인시던트 - 비즈니스 영향
   - 취약성 유의성

   주:
   비즈니스 영향 트리맵은 기본적으로 홈페이지에 보안 인시던트 응답 표시됩니다. 서비스 영향 및 실시간 트리맵을 사용하려면 보안 인시던트 분석 플러그인을 활성화해야 합니다.
5. 세 번째 선택 상자에서 선택한 트리맵에 대해 검색할 정보의 세분성 수준을 선택합니다.

   주:
   보안 인시던트 - 서비스 영향 트리맵의 세 번째 선택 상자에서 보안 인시던트 를 선택합니다. 이 선택 항목은 여러 데이터 범주가 포함된 드롭다운 목록을 제공합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



6. 화면 아래쪽에서 게이지를 추가할 화면의 위치를 클릭합니다.
7. 콘텐츠 추가 상자를 닫습니다.

트리맵 범주 생성 또는 업데이트

보안 인시던트 트리맵에 대해 미리 정의된 범주를 수정하거나 필요에 따라 범주를 생성할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.admin

트리맵은 퍼포먼스 분석을 데이터 소스로 사용합니다. Performance Analytics 모듈에는 별도의 플러그인이 필요합니다.

이 태스크 정보
기본 시스템에는 인시던트 위험, DoS(서비스 거부) 및 인시던트 심각도와 같은 트리맵 범주가 포함됩니다. 이러한 범주를 수정하거나 필요에 따라 더 많은 범주를 정의할 수 있습니다.

프로시저
1. 다음으로 이동 모두 〉 보안 인시던트 〉 관리을 클릭하고 범주를 구성할 트리맵 정의를 엽니다.
   - 서비스 중요도 보고 정의
   - 실시간 정의
2. 옵션: 트리맵 정의 이름을 변경합니다.
   기본 시스템에서 서비스 영향 트리맵 정의의 기본 이름은 보안 인시던트입니다. 실시간 트리맵 정의의 기본 이름은 보안 인시던트 - 실시간입니다.
3. 사용자 지정 작성 트리맵을 사용하지 않는 경우에는 **PA** 표시기 그룹 값을 변경하지 마십시오.
4. 트리맵 정의를 비활성화하려면 활성 확인란의 선택을 취소합니다.
   예를 들어 시스템 영향 대시보드에서 서비스 거부 범주를 비활성화하면 해당 트리맵 범주를 사용할 수 없습니다.
5. 트리맵 범주 관련 목록에서 수정할 범주를 선택하거나 신규를 클릭하여 새 범주를 생성합니다.
6. 필드에 내용을 입력합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

트리맵 범주 양식

필드	설명
이름	트리맵 위의 범주 목록에서 범주에 대해 표시되는 이름입니다.
순서	범주가 트리맵 위의 범주 목록에 표시되는 순서입니다.
트리맵	이 범주를 사용하는 트리맵의 이름입니다.
색상	트리맵에서 이 범주에 대해 표시되는 색상입니다.
활성	이 범주를 활성화하려면 선택하십시오.
설명	범주에 대한 설명입니다.
모든 역할에 의해 표시	역할에 관계없이 모든 사용자가 이 범주를 볼 수 있도록 하려면 선택합니다.
역할	모든 역할에 의해 표시 확인란을 선택하지 않은 경우 이 범주를 볼 수 있는 역할을 선택합니다.

7. 제출 또는 업데이트를 클릭합니다.

트리맵 표시기 생성 또는 업데이트

트리맵 범주에 대해 미리 정의된 표시기를 수정하거나 새 표시기를 만들 수 있습니다. 각 표시기에 대해 데이터 소스를 구성하고 표시기와 함께 표시되는 트리맵에서 보안 인시던트 목록을 여는 방법을 지정할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.admin

트리맵은 퍼포먼스 분석을 데이터 소스로 사용합니다. Performance Analytics 모듈에는 별도의 플러그인이 필요합니다.

프로시저

1. 표시기를 구성하려는 트리맵 정의를 엽니다.

2. 트리맵 범주 관련 목록에서 표시기를 구성할 범주를 선택합니다.

3. 트리맵 표시기 관련 목록에서 수정할 표시기를 선택하거나 신규를 클릭하여 새 표시기를 생성합니다.

4. 필드에 내용을 입력합니다.

트리맵 표시기 양식

필드	설명
이름	서비스 영향 대시보드의 표시기 목록에서 표시기에 대해 표시되는 이름입니다.
간단한 설명	트리맵 위의 표시기 목록에서 표시기에 대해 표시되는 설명입니다.
결과 제한	허용되는 최대 결과 수입니다. 상한은 100입니다.
결과 정밀도	소수점 뒤에 표시할 자릿수입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	이 필드는 실시간 트리맵 정의에 대해서만 표시됩니다.
활성	이 표시기를 활성화하는 확인란입니다.
범주	이전 화면에서 입력한 범주 이름입니다.
방향	트리맵의 타일이 최소화되는지 최대화되는지를 나타냅니다. 이 필드는 실시간 트리맵 정의에 대해서만 표시됩니다.
단위	메트릭에 사용할 측정 단위입니다. 이 필드는 실시간 정의에 대해서만 표시됩니다.
자동 새로 고침 간격	트리맵을 새로 고치는 빈도입니다.
순서	트리맵 위의 표시기 목록에 표시기가 표시되는 순서입니다.

5. 데이터 소스 구성 탭을 클릭하고 표시기에 대해 다음 데이터 소스 옵션 중 하나를 구성합니다.

6. 클릭스루 탭을 클릭하고 트리맵에서 보안 인시던트 목록을 여는 방법을 지정합니다.
   a. 클릭스루 **URL** 탐색 유형 필드에서 보안 인시던트 목록을 새 창에서 열지, 같은 창에서 열지, 대화 상자에서 열지 여부를 선택합니다.
   b. 옵션: 필요한 경우 클릭스루 **URL** 스크립트 필드에서 샘플 스크립트를 수정합니다.
7. 제출 또는 업데이트를 클릭합니다.

개요에 취약성 유의성 차트 추가

플러그인이 취약성 대응 활성화되면 취약성 유의성 정의 차트와 기타 시각화를 개요에 추가할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.admin

프로시저

1. 취약성 유의성 게이지를 추가할 개요 페이지로 이동합니다.
2. 페이지의 왼쪽 위 모서리에 있는 콘텐츠 추가를 클릭하여 위젯 선택 컨트롤을 엽니다.
3. 세 개의 선택 상자에서 추가할 게이지(트리 맵 또는 점수 보고서)에 따라 선택합니다.
   - 취약성 심각도 트리 맵을 추가하려면 다음을 선택합니다.
     - 트리맵
     - 취약성 유의성
     - 취약성 유의성
   - 취약성 유의성 점수 보고서를 추가하려면 다음을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 퍼포먼스 분석
- 포인트
- 취약성 유의성이 있는 서비스

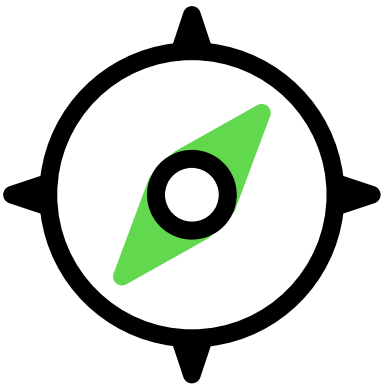
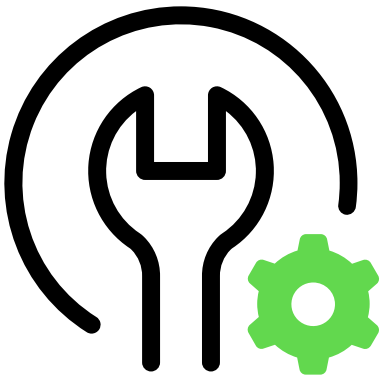
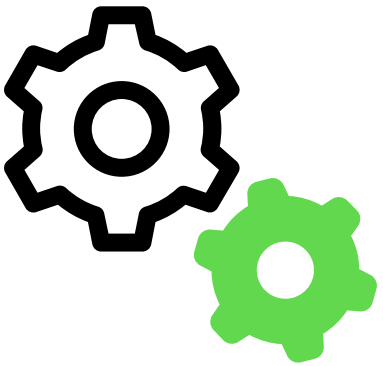
4. 화면에서 게이지를 추가할 위치를 클릭합니다.

5. 콘텐츠 추가 상자를 닫습니다.

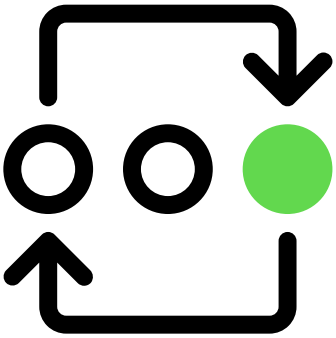
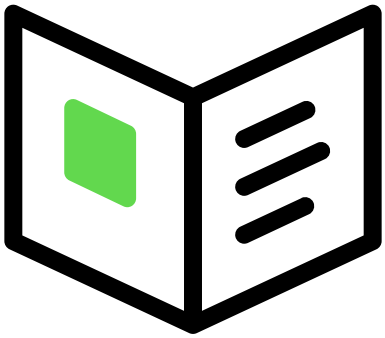
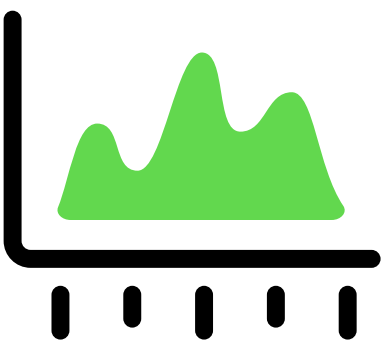
중요 보안 인시던트 관리

이 ServiceNow# 중요 보안 인시던트 관리 애플리케이션은 검색부터 보안 인시던트 제안, 승격 및 연결, 종결에 이르기까지 (MSI)의 중요 보안 인시던트 진행 상황을 추적합니다.

중요 보안 인시던트 관리

탐색	구성	통합
		
분석가, 관리자 및 관리자가 주요 보안 인시던트 관리 (MSIM)를 사용하는 방법에 대해 알아봅니다.	구현 계획 및 구성	다른 Microsoft 애플리케이션과 통합하여 MSIM 기능 확장

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관리자	사용	상태 보고서
		
인시던트 기록에 태그를 지정하고 레이블을 구성하는 방법에 대한 관리 작업	작업 공간 관리를 통해 중요 보안 인시던트 기록 제안, 승격, 연결 및 거부	메트릭, 추세 차트 및 보고서를 통해 인시던트 관련 작업을 모니터링하고 프로세스를 개선합니다
추가 기능		
기록을 롤업할 정보 구성		

스토어에서 앱 요청

ServiceNow Store 웹 사이트를 방문하면 사용 가능한 모든 앱을 확인하고 스토어에 요청을 제출하는 방법에 대한 정보를 참조할 수 있습니다. 출시된 모든 앱의 누적 릴리스 정보는 ServiceNow Store 버전 기록 릴리스 정보를 참조하십시오.

스토어에서 보안 운영 앱 요청

해당 날짜 Rome 이후의 신규 보안 운영 고객인 경우 ServiceNow Store 웹 사이트에서 사용 가능한 앱과 스토어에 요청을 제출하는 방법에 대한 정보를 볼 수 있습니다.

문제 해결 및 도움 받기

- 중요 보안 인시던트 관리 포럼 - ServiceNow 커뮤니티.
- Security Operations 리소스 라이브러리

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- Security Operations 커뮤니티
- 알려진 오류 포털에서 알려진 오류 문서 검색
- 연락처 고객 서비스 및 지원

Major Security Incident Management 탐색

조직에 위협으로 식별된 우선순위가 높은 중요 보안 인시던트를 추적하는 측면에서 애플리케이션의 작동 방식을 이해합니다 중요 보안 인시던트 관리 .

이 섹션을 사용하여 주요 보안 인시던트 기록 작업과 관련된 주요 기능과 다양한 역할에 대해 알아봅니다. 또한 이 섹션은 애플리케이션을 사용하는 데 필요한 애플리케이션, 필수 조건 및 플러그인을 시작하는 방법을 이해하는 데 도움이 됩니다.

중요 보안 인시던트 관리

를 통해 중요 보안 인시던트 관리일반적으로 중요 보안 인시던트 해결의 일부인 다양한 활동을 추적하고 관리합니다. 직관적인 작업 공간을 통해 인시던트 관리자와 인시던트 담당 담당자는 중요 인시던트를 제안 및 승격하고, 중요 보안 인시던트 활동을 추적하고, 동료와 쉽게 협업할 수 있습니다.

개요

중요 보안 인시던트 관리 기능은 기존 보안 인시던트 응답 제품 기능과 함께 작동합니다. 여기에는 보안 분석가가 표준 보안 인시던트를 중요 보안 인시던트로 에스컬레이션하여 새로운 제품 기능을 사용하여 정정 프로세스를 지원할 수 있는 기능이 포함됩니다.

인스턴스에 설치한 ServiceNow 후 보안 인시던트 분석가는 다음을 수행할 수 있습니다.

- 주요 보안 인시던트 후보에 대한 보안 인시던트를 제안하여 주요 보안 인시던트 생성이 필요한 경우 검토 프로세스를 시작합니다.
- 추가 검토 프로세스 없이 보안 인시던트를 중요 보안 인시던트로 바로 승격
- MSI(주요 보안 인시던트)로 제안된 보안 인시던트를 거부합니다.
- 모든 보안 인시던트를 처리할 수 있도록 보안 인시던트를 하위 인시던트로 MSI(주요 보안 인시던트)와 연결합니다.

주요 기능

MSIM(Major Security Incident Management)은 다음 기능을 통해 중요 보안 인시던트 정정 프로세스를 개선합니다.

- 주요 보안 인시던트 관리자 사용자 역할용으로 설계된 주요 보안 인시던트를 관리하기 위한 전용 작업 공간입니다.
- 여러 '하위' 보안 인시던트의 응답 작업을 구성합니다.
- 주요 보안 인시던트가 생성된 후 공동 작업 폴더와 채팅 커뮤니케이션 채널을 자동으로 생성하고 인시던트 종결의 일부로 보관합니다.
- 통합을 통해 주요 보안 인시던트와 관련된 아티팩트(파일) 컬렉션을 구성하고 추적하는 파일 탐색기 구성요소입니다 Microsoft SharePoint .
- 통합을 통해 여러 보안, IT 및 기능 그룹 간의 커뮤니케이션을 관리할 수 있는 채팅 채널 관리자 및 활동 스트림 구성요소입니다 Microsoft Teams .

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업 공간 구성요소

제품에는 중요 보안 인시던트 관리 다음과 같은 주요 기능 기능을 제공하는 몇 가지 새로운 작업 공간 구성요소와 사용자 인터페이스 페이지가 포함되어 있습니다.

- 주요 보안 인시던트 관리자 사용자 역할을 위해 특별히 설계된 주요 보안 인시던트를 관리하기 위한 전용 작업 공간입니다.
- 여러 하위 보안 인시던트의 응답 작업을 구성합니다.
- 주요 보안 인시던트가 생성된 후 공동 작업 폴더와 채팅 커뮤니케이션 채널을 자동으로 생성하고 인시던트 종결의 일부로 보관합니다.
- 통합을 통해 주요 보안 인시던트와 관련된 아티팩트(파일) 컬렉션을 구성하고 추적하는 파일 탐색기 구성요소입니다 Microsoft SharePoint .
- 통합을 통해 여러 보안, IT 및 기능 그룹 간의 커뮤니케이션을 관리할 수 있는 채팅 채널 관리자 및 활동 스트림 구성요소입니다 Microsoft Teams .

지원되는 **Major Security Incident Management** 버전

중요 보안 인시던트 관리 (MSIM)에는 다음이 필요합니다. ServiceNow AI Platform# 로마 버전.

이 기능은 제품군의 Microsoft Office 365 채팅 중심 작업 공간인 을 지원합니다Microsoft Teams. 이전에는 Microsoft Teams 응용 프로그램과 별도의 설치 Microsoft Office 365 가있었습니다.

지원되는 **ServiceNow AI Platform** 버전

이 기능은 이후 릴리스에서 Rome 지원됩니다.

다음 보안 운영 애플리케이션은 이미 보안 인시던트 응답 (SIR)를 사용중인 경우 대부분의 사용자에 대해 설치될 가능성이 높은 표준 보안 인시던트 응답 플러그인입니다. 설치되어 있지 않은 경우 에서 설치하고 활성화해야 ServiceNow Store합니다. 원활한 설치를 위해 언급된 순서대로 한 번에 하나의 애플리케이션을 설치한 다음 활성화합니다.

1. 보안 인시던트 응답: com.snc.si_dep 종속 플러그인입니다. 이 플러그인을 설치하면 다른 보안 운영 애플리케이션이 활성화됩니다.
2. 보안 통합 프레임워크
3. Security Support Common
4. Security Support Common 오케스트레이션

MSIM 시작하기

작업을 중요 보안 인시던트 관리시작하기 전에 다음 정보를 검토합니다.

필요한 역할: sn_msi.workspace_admin.

애플리케이션을 쉽게 설치하고 구성 중요 보안 인시던트 관리 하려면 다음 플러그인이 활성화되어 있는지 확인해야 할 수 있습니다.

중요사항:
업데이트 세트(KB1289784)는 Major Security Incident Management 빠른 시작 가이드에 있습니다. 사용자가 쉽게 구성을 설정할 수 있도록 하려면 애플리케이션 설치를 완료한 후 업데이트 세트를 가져와야 합니다. ServiceNow Store에 있는 MSIM 애플리케이션의 지원 문서 섹션에 있는 빠른 시작 가이드(2단계)에 설명된 절차를 따르십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필수 구성요소

작업	설명
애플리케이션을 시작하기 전에 필요한 종속 플러그인이 있는지 확인하십시오.	첫 번째 단계로 다음을 설치합니다. • ServiceNow 통합 허브 설치 관리자 (com.glide.hub.integrations) • ServiceNow# 통합 허브 런타임 (com.glide.hub.integration.runtime). • ServiceNow# 통합 허브 Action Step - REST(com.glide.hub.action_step.rest) • ServiceNow# 통합 허브 작업 템플릿 - 데이터 스트림 (com.glide.hub.action_type.datastream) • ServiceNow# 통합 허브 Flow Designer - 동적 입력(com.glide.hub.dynamic_inputs) 주: 나열된 ServiceNow# 통합 허브 플러그인에 필요한 권한이 없는 경우 지원 티켓을 제기하여 해당 필수 애플리케이션을 설치합니다.
스포크 및 Microsoft Teams Graph 스포크를 설치하기 Microsoft SharePoint 위해 필요한 액세스 권한이 있는지 확인합니다. 주: 위에 나열된 것은 시작할 중요 보안 인시던트 관리기본 종속 애플리케이션입니다.	스포크 및 Microsoft Teams Graph 스포크를 설치하기 Microsoft SharePoint 전에 애플리케이션에 필요한 액세스 권한이 ServiceNow 통합 허브 있는지 확인하십시오. 주: Microsoft SharePoint 스포크와 Microsoft Teams Graph 스포크는 애플리케이션에 종속된 애플리케이션입니다 ServiceNow# 통합 허브 .

설정 검사 **MSIM** 목록

(MSIM) 애플리케이션을 사용하기 ServiceNow# 중요 보안 인시던트 관리 전에 에서 ServiceNow# Store애플리케이션을 다운로드합니다.

다음 표의 설정, 설치 및 구성에 대한 진행률을 추적합니다.

주:
애플리케이션에 할당된 중요 보안 인시던트 관리 역할은 다음 섹션에 나열되어 있습니다. 자세한 내용은 문서를 참조하십시오 중요 보안 인시던트 관리 역할.

다음 검사 목록을 사용하여 애플리케이션을 설치하고 구성하는 중요 보안 인시던트 관리 엔드 투 엔드 단계를 안내합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

검사 목록

설정 작업	설명
중요 보안 인시던트 관리 애플리케이션에서 애플리케이션이 설치되고 활성화ServiceNow# Store되었는지 확인합니다.	중요 보안 인시던트 관리 v1.1.1은 에서 사용할 수 있습니다 ServiceNow# Store. 다음 지침을 따릅니다. 에서 애플리케이션 다운로드 ServiceNow Store.
다음 애플리케이션이 지정된 순서대로 설치되었는지 확인합니다.	현재 애플리케이션 릴리스 버전에 애플리케이션을 설치한 중요 보안 인시던트 관리 후 기본적으로 다음 애플리케이션이 설치됩니다. • File Explorer 보안 운영용 코어 v1.1.1 • Microsoft SharePoint File Explorer v1.1.1용 보안 운영 커넥터 • File Explorer v1.0.0용 보안 운영 구성요소 • Microsoft Teams 보안 운영용 채팅 커넥터 v1.0.0 • v1.0.0용 보안 운영 채팅 코어 • 중요 보안 인시던트 응답 v1.1.1 • 작업 공간용 MSIM 공동 채팅 EVAM 카드 v1.0.0(이 애플리케이션은 작업 공간의 애플리케이션 백그라운드에서 중요 보안 인시던트 관리 UI 시각화에 대해서만 설정됨) • 작업 공간 1.0.0용 중요 보안 인시던트 관리 작업 관리자 UI 구성요소 • 보안 인시던트 응답 v12.8.1
사용자 역할이 적절하게 할당 중요 보안 인시던트 되었는지 확인합니다.	다음은 정정 프로세스의 인시던트 수명주기 중요 보안 인시던트 전반에 걸쳐 관여되는 역할입니다. • MSI 관리자 [sn_msi.workspace_admin] • MSI 관리자 [sn_msi.workspace_manager] • MSI 응답자 [sn_msi.workspace_responder 각 역할에 대한 자세한 내용은 다음 문서를 참조하십시오 중요 보안 인시던트 관리 역할.
v1.0.0 구성을 성공적으로 설정 Microsoft SharePoint 했는지 확인합니다.	Microsoft SharePoint 의 사이트, 폴더, 파일, 그룹 및 사용자를 Microsoft SharePoint관리합니다. 인스턴스에 데이터를 ServiceNow# 추가합니다Microsoft SharePoint. 이렇게 하려면 Graph 및 Rest 연결을 설정해야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

검사 목록

설정 작업	설명
	자세한 내용은 REST 및 그래프 연결 구성을 설정하는 방법에 대한Microsoft SharePoint 스포크 v1.1.2 설명서를 참조하십시오. 에서 인스턴스에 Microsoft SharePoint연결하려면 ServiceNow# 그래프 및 REST 연결을 설정합니다.
문서 라이브러리를 만들 사이트를 만들었 Microsoft SharePoint 는지 확인합니다.	Microsoft SharePoint 필요한 경우 사이트를 만들거나 기존 사이트를 사용하여 문서 라이브러리를 만들 수 있습니다.
사이트 아래에 Microsoft SharePoint 문서 라이브러리를 만들었는지 확인합니다.	새 사이트 또는 기존 Microsoft SharePoint 사이트 아래에 전용 문서 라이브러리를 만듭니다.
필요한 권한이 사용자에게 제공되고 의 필수 사용자 그룹에 Microsoft SharePoint할당되었는지 확인합니다.	사이트에서 다른 사용자 및 사용자 그룹에 대한 액세스를 Microsoft SharePoint 관리합니다.
드라이브 및 필요한 구성 설정을 만들고 구성 Microsoft SharePoint 했는지 확인합니다.	드라이브 구성을 확인하려면 파일 탐색기 커넥터, 폴더 및 파일 동작, 폴더 템플릿을 설정합니다 Microsoft SharePoint . • 파일 탐색기 리포지토리 드라이브 구성: 에서 인스턴스로 Microsoft SharePointServiceNow# 연결을 생성합니다. • 폴더 및 파일 작업 설정 구성: 파일 탐색기 구성요소에 표시되는 개별 폴더 및 파일 작업을 구성하고 제어합니다. • 폴더 템플릿 작성: 다양한 중요 보안 인시던트 유형에 대해 고유한 폴더를 생성하도록 구성합니다.
Microsoft Teams 채팅 커넥터 애플리케이션에 대한 연결을 성공적으로 설정했는지 확인합니다.	인스턴스와 ServiceNow# Microsoft Teams 채팅 커넥터 애플리케이션 연결을 설정하려면 여기에 에서 MS Teams 그래프 연결 설정 ServiceNow AI Platform설명된 절차를 따르십시오.
인스턴스로 ServiceNow AI Platform# Microsoft Teams를 구성하고 연결 및 자격 증명 구성을 생성했는지 확인합니다.	인스턴스를 사용하여 ServiceNow# 구성을 확인하려면 Microsoft Teams 여기에 설명된 절차를 따르십시오. • 에서 MS Teams 그래프 연결 설정 ServiceNow AI Platform • 채팅 채널 템플릿 생성

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

검사 목록

설정 작업	설명
Major Security 인시던트 관리 - 구성 설정이 성공했는지 확인합니다.	MSI 관리자는 다음을 수행할 수 있어야 합니다. • 보안 분석가가 인시던트를 제안 및 승격하고 다른 보안 인시던트를 연결할 수 있는지 여부를 결정합니다. • 인시던트가 제안되거나 승격될 때 알림을 활성화하거나 비활성화합니다. 기본 템플릿 메시지를 편집하는 기능입니다. • 보안 분석가 인터페이스에 표시되는 보안 태그를 구성하여 중요 보안 인시던트 후보로 제안되었거나 중요 보안 인시던트로 승격된 인시던트를 구분합니다.
Major Security 인시던트 관리 - 알림 설정이 성공했는지 확인합니다.	MSI 관리자는 보안 인시던트가 제안되고 알림 목록에 구성된 모든 사용자와 그룹에 전송될 때 이메일 알림을 트리거합니다. 자세한 내용은 다음에 대한 알림 기본 설정 지정 MSIM 문서를 참조하십시오.

중요 보안 인시던트 관리 역할

사용자가 MSIM 애플리케이션 내에서 필요한 모든 작업을 수행할 수 있도록 역할을 할당합니다.

중요 인시던트 관리에 대한 역할

역할 유형	역할	설명
MSI 관리자	sn_msi.workspace_admin	(FE), Microsoft Teams 및 채팅 채널 구성, 작업 공간 설정, MSI 관리: 구성 및 알림 설정과 같은 File Explorer 종속 애플리케이션을 설치하고 구성하고 중요 인시던트 관리 설정할 수 있습니까? 설정 방법: • FE(파일 탐색기) 구성요소: ○ 파일 리포지토리를 구성합니다. ○ Major Security Incident Management 작업 공간에서 공동 작업 탭의 파일 탐색기 구성요소에 제공되는 파일 및 폴더 작업을 구성합니다. ○ 루트 폴더와 하위 폴더를 만들고 하위 폴더에 대한 액세스를 제공합니다. • 채팅 채널 관리

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

중요 인시던트 관리에 대한 역할

역할 유형	역할	설명
		◦ 연결을 확인하여 Microsoft Teams 활성화하고 구성합니다Microsoft Teams. ◦ 채팅 팀 및 채팅 채널을 생성하고 사용자를 추가하고 다양한 사용자 그룹에 사용자를 할당합니다. • MSI 관리: ◦ 구성: 보안 분석가의 작업, 인시던트가 제안되고 승격될 때 전송되는 알림을 구성하고 보안 인시던트에 대한 태그를 표시합니다. ◦ 알림: 보안 인시던트가 제안되거나 중요 보안 인시던트로 승격될 때 이메일 알림 프로세스 및 사용자 알림을 자동화합니다.
MSI 관리자	sn_msi.workspace_manager	• Major Security Incident Management 구성 설정 페이지에 대한 액세스 권한을 봅니다. 구성 설정을 수정할 수 없습니다. • 작업 공간의 상세 정보, 공동 작업, 작업 관리자 탭에서 중요 인시던트 관리 인시던트 기록 데이터를 보고 편집합니다. • 보안 인시던트를 중요 보안 인시던트로 승격합니다. • 작업 공간의 공동 작업 탭에 중요 인시던트 관리 있는 파일 탐색기 구성요소에서 사용할 수 있는 파일 및 폴더 작업을 구성합니다. • 작업 공간에서 중요 보안 인시던트에 추가 기록을 연결 및 연결 해제
MSI 응답자	sn_msi.workspace_responder	• 에서 중요 보안 인시던트를 보고, 편집하고, 대응하기 위한 선택적 역할 상세 정보

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

중요 인시던트 관리에 대한 역할

역할 유형	역할	설명
		및 작업 중요 인시던트 관리 작업 공간의 탭. • 작업 공간에서 중요 보안 인시던트에 추가 기록을 연결 및 연결 해제

통합 중요 보안 인시던트 관리

애플리케이션과 통합하여 인스턴스의 중요 보안 인시던트 관리 기능을 확장하고 인스턴스와 ServiceNow AI PlatformMicrosoft 연결합니다.

중요사항:
업데이트 세트(KB1289784)는 Major Security Incident Management 빠른 시작 가이드에 있습니다. 사용자가 쉽게 구성을 설정할 수 있도록 하려면 애플리케이션 설치를 완료한 후 업데이트 세트를 가져와야 합니다. ServiceNow Store에 있는 MSIM 애플리케이션의 지원 문서 섹션에 있는 빠른 시작 가이드(2단계)에 설명된 절차를 따르십시오.

중요 보안 인시던트 관리와 **Microsoft SharePoint** 통합

와 중요 보안 인시던트 관리통합하십시오Microsoft SharePoint.

SharePoint 연결을 위해 **Azure** Portal에 새 애플리케이션 등록

통합을 위해 Azure Portal에 새 애플리케이션을 등록합니다 Microsoft SharePoint .

시작하기 전에
필요한 역할: admin, Azure admin

프로시저

1. 에 로그인 Microsoft Azure 포털은 Microsoft 계정을 Azure 관리자로 사용합니다.
2. 다음으로 이동 **Azure** 서비스 〉 애플리케이션 등록 〉 신규 등록.

   주:
   찾을 수 없는 경우 **Azure** 서비스로 이동하여 앱 등록을 검색합니다.

3. 애플리케이션의 이름을 입력합니다.
   예를 들어 그래프입니다 Microsoft SharePoint .
4. 지원되는 계정 유형 선택: 이 조직 디렉터리의 계정만**(Service Now** 전용 **-** 단일 테넌트).
5. 리디렉션 URI(옵션) 필드 아래의 드롭다운 목록에서 웹 유형을 선택합니다.
6. 허용된 리디렉션 URL 필드에 인스턴스 리디렉션 URL을 입력합니다 ServiceNow AI Platform# .
   예: https://<InstanceName>.service-now.com/oauth_redirect.do.
7. 등록을 클릭하고 페이지가 개요 섹션과 함께 표시되는지 확인합니다.
8. 개요 페이지의 **Essentials** 섹션에서 클라이언트 ID 및 테넌트 ID를 기록해 둡니다.
9. **API** 권한에서 Microsoft Graph 권한을 추가합니다.
   a. 권한 추가를 클릭합니다.
   b. **Microsoft Graph**를 선택합니다.
   c. 애플리케이션 권한을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

d. 사이트 목록에서 **Sites.Selected** 권한을 선택합니다.

e. 권한 추가를 클릭합니다.

10. API 권한에서 SharePoint 권한을 추가합니다.

a. 권한 추가를 클릭합니다.

b. SharePoint를 선택합니다.

c. 애플리케이션 권한을 선택합니다.

d. 사이트 목록에서 **Sites.Selected** 사용 권한을 선택합니다.

e. 권한 추가를 클릭합니다.

11. 권한을 추가한 후 관리자 동의 부여를 클릭합니다.
이제 모든 권한이 관리자에게 동의되었습니다.

인증에 인증서 사용

인증서 자격 증명을 사용하여 액세스 토큰을 요청합니다.

시작하기 전에

1. 자체 서명된 인증서 또는 CA 발급 인증서를 사용할 수 있습니다. 앱 전용 액세스를 위한 Azure AD 앱 설정에 설명된 대로 PowerShell 스크립트를 실행하여 자체 서명된 인증서를 만들 수 있습니다. 스크립트는 다음 두 개의 파일을 생성합니다. PFX 파일 및 . CER 파일.

> **주:**
> 를 생성하기 위해 개인 키를 암호화하는 데 사용되는 암호를 알고 있어야 합니다. PFX 파일 및 . CER 파일.

2. 를 사용하십시오. JKS(Java 키 저장소) 파일을 만드는 PFX 파일입니다.

> **주:**
> 에서 JKS 파일을 생성하는 데 사용되는 암호를 알고 있어야 합니다. PFX 파일.

필요한 역할: 관리자

프로시저

1. Azure AD 포털에서 앱 등록 으로 이동합니다.

2. 관리 섹션에서 인증서 및 암호를 클릭합니다.

3. Certificates(인증서) 탭에서 **Upload** Certificate(인증서 업로드)를 클릭합니다.

4. 양식에서 다음 값을 입력합니다.

필드	설명
.cer, .pem, .crt 파일 형식 중 하나를 사용하여 인증서(공개 키)를 업로드합니다.	. PowerShell 스크립트를 사용하여 생성한 CER 파일입니다.
설명	인증서에 대한 설명입니다.

5. 추가를 클릭합니다.
인증서가 업로드되고 해당 상세 정보가 인증서 탭 아래에 표시됩니다.

6. 업로드된 인증서의 지문 값을 복사합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
지문 값은 16진수 값입니다.

7. 지문 값을 Base64 값으로 인코딩하고 나중에 사용할 수 있도록 값을 기록합니다.

주:
16진수에서 Base64로(Hex to Base64) 변환기 도구를 사용하여 지문 값을 Base64 값으로 인코딩할 수 있습니다.

로 구성 **Microsoft SharePoint**중요 보안 인시던트 관리

중요 보안 인시던트 관리 연결을 사용하여 Microsoft SharePoint 설정합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 작업 공간 〉 중요 보안 인시던트 관리 〉 관리.

2. 문서 공동 작업을 선택한 다음 **Microsoft SharePoint** 설치를 선택합니다.

3. 상황에 맞는 메뉴에서 **Azure** 앱에 **SharePoint** 사이트에 대한 액세스 권한 부여 를 선택합니다.

4. Curl 명령, Azure CLI 또는 PowerShell 방법 중 하나를 사용하여 등록된 애플리케이션에 대한 액세스 권한을 부여합니다.

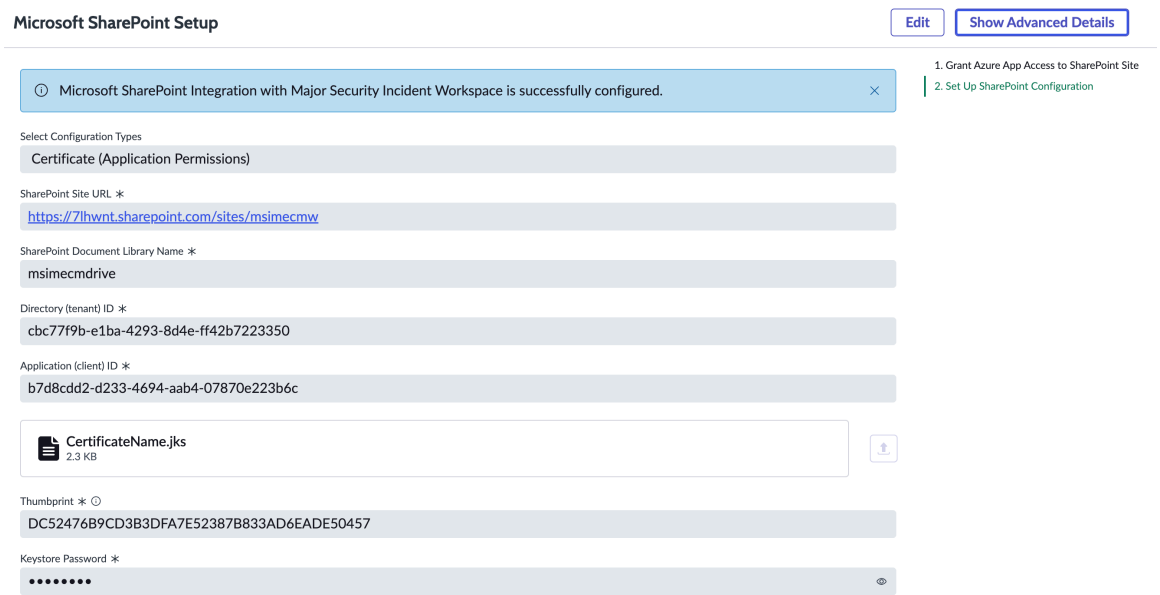
주:

- Azure 관리자가 액세스 구성을 제공해야 합니다.
- 등록된 애플리케이션에 대한 Sites.FullControl.All 권한을 부여합니다.
- 액세스 권한이 성공적으로 부여되면 Sites.FullControl.All 권한을 제거합니다.

5. 상황에 맞는 메뉴에서 **SharePoint** 구성 설정을 선택합니다.

6. 구성 유형 선택에서 구성 유형을 선택하고 다음을 구성합니다.

- 인증서(애플리케이션 권한)



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

인증서에 대한 **SharePoint** 설정

필드	설명
SharePoint 사이트 URL	사이트 URL입니다 Microsoft SharePoint .
SharePoint 문서 라이브러리 이름	문서 라이브러리의 Microsoft SharePoint 이름입니다.
디렉터리(테넌트) ID	Azure Active Directory 인스턴스의 고유 식별자입니다.
애플리케이션(클라이언트) ID	Azure에 등록된 애플리케이션의 고유 식별자입니다.
인증서 업로드	인증을 위한 인증서 파일입니다.
지문	인증서의 지문입니다.
키 스토어 암호	인증서의 지문에 접근하기 위한 키 저장소 암호입니다.

○ 클라이언트 비밀(애플리케이션 권한)

클라이언트 암호에 대한 **SharePoint** 설정

필드	설명
SharePoint 사이트 URL	사이트 URL입니다 Microsoft SharePoint .
SharePoint 문서 라이브러리 이름	문서 라이브러리의 Microsoft SharePoint 이름입니다.
디렉터리(테넌트) ID	Azure Active Directory 인스턴스의 고유 식별자입니다.
애플리케이션(클라이언트) ID	Azure에 등록된 애플리케이션의 고유 식별자입니다.
클라이언트 비밀	토큰을 요청하는 데 사용되는 애플리케이션의 비밀 문자열입니다.

7. 구성 및 **OAuth** 토큰 가져오기를 선택합니다.
Microsoft 계정 세부 정보를 제공하는 로그인 프롬프트가 나타납니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

8. Microsoft 계정 세부 정보 및 로그인을 제공합니다.
   성공 메시지가 나타나고 연결이 설정됩니다.

중요 보안 인시던트 관리와 **Microsoft Teams** 통합

와 중요 보안 인시던트 관리통합하십시오Microsoft Teams.

- 연결을 위해 Microsoft Teams Azure Portal에서 새 애플리케이션 등록
- 다음과의 연결 구성 Microsoft Teams중요 보안 인시던트 관리

연결을 위해 **Microsoft Teams Azure** Portal에서 새 애플리케이션 등록

통합을 위해 Microsoft Teams Azure Portal에 새 애플리케이션을 등록하고 Azure 앱에 대한 액세스 권한을 부여합니다.

시작하기 전에

> **주:**
> 원하는 경우 SharePoint용으로 만든 것과 동일한 애플리케이션을 사용하여 Microsoft Teams Graph 연결을 설정할 수 있습니다.

필요한 역할: admin, Azure admin

프로시저

1. Microsoft 계정을 사용하여 Azure Portal에 로그인합니다.
2. 다음으로 이동 **Azure** 서비스 〉 애플리케이션 등록 〉 신규 등록.
3. 애플리케이션의 이름을 입력합니다.
   예를 들어 Microsoft Teams Graph입니다.
4. 지원되는 계정 유형: 이 조직 디렉터리의 계정 전용**(Service Now** 전용 **-** 단일 테넌트)을 선택합니다.
5. 리디렉션 URL 아래의 드롭다운 목록에서 웹 유형을 선택합니다.
6. 허용된 리디렉션 URL 필드에 인스턴스 리디렉션 URL을 입력합니다 ServiceNow AI Platform# .
   예: https://<<InstanceName>>.service-now.com/oauth_redirect.do
7. 등록을 클릭하고 페이지가 개요 섹션과 함께 표시되는지 확인합니다.
8. 개요 페이지의 **Essentials** 섹션에서 클라이언트 ID와 테넌트 ID를 기록해 둡니다.
9. 6.1단계 또는 6.2단계에 따라 인스턴스에서 연결을 설정하는 절차를 완료할 수 있습니다 ServiceNow .

다음과의 연결 구성 **Microsoft Teams**중요 보안 인시던트 관리

중요 보안 인시던트 관리 연결을 사용하여 Microsoft Teams 설정합니다.

시작하기 전에

필수 구성 요소: 필요한 대리인 권한을 사용하여 Azure Active Directory에 응용 프로그램을 등록했는지 확인합니다.

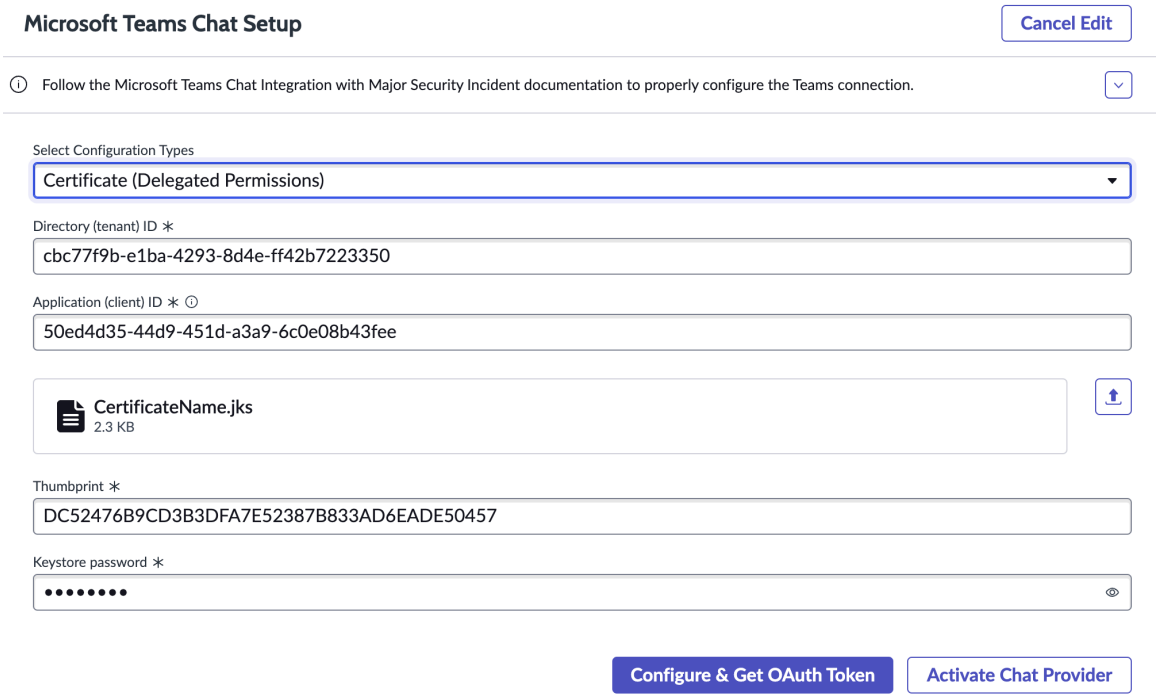
필요한 역할: 관리자

프로시저

1. 다음으로 이동 작업 공간 〉 중요 보안 인시던트 관리 〉 관리.
2. 채팅 공동 작업을 선택한 다음 **Microsoft Teams** 설정을 선택합니다.
3. 구성 유형 선택 필드에서 구성 유형을 선택하고 다음을 구성합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

○ 인증서(위임된 권한)

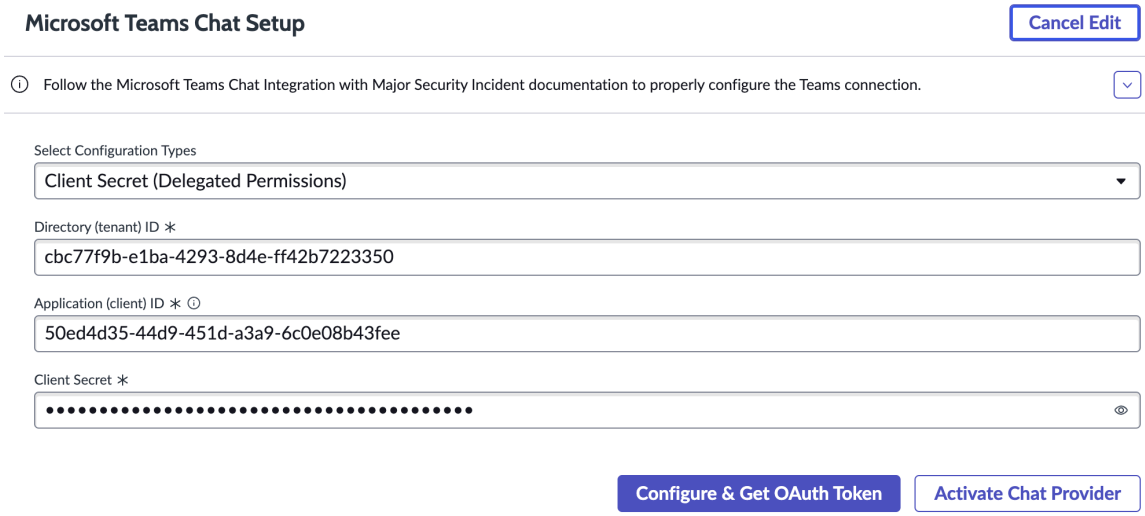


인증서에 대한 **Microsoft Teams** 설정

필드	설명
디렉터리(테넌트) ID	Azure Active Directory 인스턴스의 고유 식별자입니다.
애플리케이션(클라이언트) ID	Azure에 등록된 애플리케이션의 고유 식별자입니다.
인증서 업로드	인증을 위한 인증서 파일입니다.
지문	인증서의 지문입니다.
키 스토어 암호	인증서의 지문에 접근하기 위한 키 저장소 암호입니다.

○ 클라이언트 비밀(위임된 권한)

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



클라이언트 비밀에 대한 **Microsoft Teams** 설정

필드	설명
디렉터리(테넌트) ID	Azure Active Directory 인스턴스의 고유 식별자입니다.
애플리케이션(클라이언트) ID	Azure에 등록된 애플리케이션의 고유 식별자입니다.
클라이언트 비밀	토큰을 요청하는 데 사용되는 애플리케이션의 비밀 문자열입니다.

4. 구성 및 **OAuth** 토큰 가져오기를 선택합니다.
   Microsoft 계정 세부 정보를 제공하는 로그인 프롬프트가 나타납니다.
5. Microsoft 계정 세부 정보 및 로그인을 제공합니다.
   성공 메시지가 나타나고 연결이 설정됩니다.
6. 채팅 공급자 활성화를 선택하여 연결을 활성화합니다Microsoft Teams.
7. 옵션: 구성 세부 정보를 보려면 고급 세부 정보 표시를 선택합니다.

에서 **MS Teams** 그래프 연결 설정 **ServiceNow AI Platform**

연결을 설정하여 Microsoft Teams Graph 인스턴스와 Microsoft Teams 계정을 통합합니다ServiceNow AI Platform.

시작하기 전에

원하는 경우 SharePoint용으로 만든 것과 동일한 애플리케이션을 사용하여 Microsoft Teams Graph 연결을 설정할 수 있습니다.

필요한 역할: admin, Azure admin

Microsoft Teams 그래프 연결을 위해 Azure에 새 애플리케이션 등록

프로시저

1. 계정을 사용하여 Azure Portal에 Microsoft 로그인합니다.
2. 다음으로 이동 **Azure** 서비스 〉 애플리케이션 등록 〉 신규 등록.
3. 애플리케이션의 이름을 입력합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예를 들어 Microsoft Teams Graph입니다.

4. 조직에 적용할 수 있는 지원되는 각 계정 유형 옵션을 선택합니다.
예를 들어 이 조직 디렉터리 계정 전용**(Service Now** 전용 **-** 단일 테넌트) 옵션을 선택합니다.

> 주:
> 지원되는 계정 유형에 대한 자세한 내용은 Microsoft ID 플랫폼에 애플리케이션 등록을 참조하세요.

5. 리디렉션 URL 아래의 드롭다운 목록에서 웹 유형을 선택합니다.
6. 허용된 리디렉션 URL 필드에 인스턴스 리디렉션 URL을 입력합니다 ServiceNow AI Platform .
예: https://〈〈InstanceName〉〉.service-now.com/oauth_redirect.do
7. 등록을 클릭하여 새 애플리케이션을 등록하고 페이지가 개요 섹션과 함께 표시되는지 확인합니다.

인증을 위해 인증서 사용

인증서 자격 증명을 사용하여 액세스 토큰을 요청합니다.

시작하기 전에

1. 자체 서명된 인증서 또는 CA 발급 인증서를 사용할 수 있습니다. 앱 전용 액세스를 위한 Azure AD 앱 설정에 설명된 대로 PowerShell 스크립트를 실행하여 자체 서명된 인증서를 만들 수 있습니다. 스크립트는 다음 두 개의 파일을 생성합니다. PFX 파일 및 . CER 파일.

> 주:
> 를 생성하기 위해 개인 키를 암호화하는 데 사용되는 암호를 알고 있어야 합니다. PFX 파일 및 . CER 파일.

2. 를 사용하십시오. JKS(Java 키 저장소) 파일을 만드는 PFX 파일입니다.

> 주:
> 에서 JKS 파일을 생성하는 데 사용되는 암호를 알고 있어야 합니다. PFX 파일.

필요한 역할: 관리자

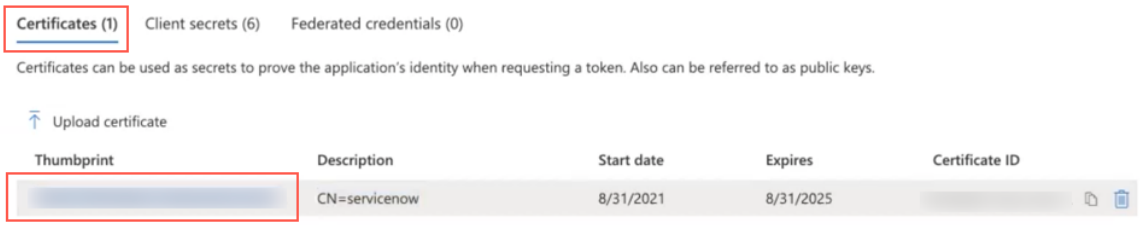
프로시저

1. Azure AD 포털에서 앱 등록 으로 이동합니다.
2. 관리 섹션에서 인증서 및 암호를 클릭합니다.
3. Certificates(인증서) 탭에서 **Upload** Certificate(인증서 업로드)를 클릭합니다.
4. 양식에서 다음 값을 입력합니다.

필드	설명
.cer, .pem, .crt 파일 형식 중 하나를 사용하여 인증서(공개 키)를 업로드합니다.	. PowerShell 스크립트를 사용하여 생성한 CER 파일입니다.
설명	인증서에 대한 설명입니다.

5. 추가를 클릭합니다.
인증서가 업로드되고 해당 상세 정보가 인증서 탭 아래에 표시됩니다.
6. 업로드된 인증서의 지문 값을 복사합니다.
지문 값은 16진수 값입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



7. 지문 값을 Base64 값으로 인코딩하고 나중에 사용할 수 있도록 값을 기록합니다.

> 주:
> 16진수에서 Base64로(Hex to Base64) 변환기 도구를 사용하여 지문 값을 Base64 값으로 인코딩할 수 있습니다.

MS Teams에 대한 **Java** 키 스토어 인증서 첨부

유효한 JKS(Java 키 스토어) 인증서를 첨부하여 JWT 전달자 부여 토큰 인증을 사용하도록 설정합니다.

시작하기 전에
ServiceNow 인스턴스에 로그인하여 다음 절차를 수행합니다.

- 유효한 Java 키 스토어 인증서
- 필요한 역할: 관리자

프로시저

1. 다음으로 이동 시스템 정의 〉 인증서.

2. **Microsoft Teams** 커넥터 인증서 기록을 엽니다.
기본 기록인 **Microsoft Teams** 커넥터 인증서 만 사용해야 합니다.

3. 키 스토어 암호에 JKS 파일과 연결된 암호를 입력합니다.

4. 첨부 파일 아이콘( )을 클릭하고 생성한 JKS 인증서를 첨부합니다.
자세한 내용은 문서를 참조하십시오.

5. **Validate Stores/**Certificates(저장소/인증서 확인)를 클릭합니다.

6. 업데이트를 클릭합니다.

MS Teams에 대한 **JWT** 서명 키 구성

Java 키 스토어 인증서에 할당할 JWT(JSON Web Token) 서명 키를 생성합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 시스템 **OAuth** 〉 **JWT** 키.

2. **Microsoft Teams Connector JWT** 기록을 엽니다.

3. 를 생성하기 위해 개인 키를 암호화하는 데 사용되는 암호를 입력합니다. PFX 파일 및 . 서명 키 암호의 CER 파일입니다.

4. 업데이트를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

MS Teams에 대한 JWT 제공자 구성

ServiceNow 인스턴스에 JSON 웹 토큰(JWT) 제공자를 추가합니다.

시작하기 전에

- Azure 포털에 등록한 애플리케이션의 애플리케이션(클라이언트) **ID** 및 디렉터리(테넌트) **ID** 값을 복사하여 기록합니다.

- 필요한 역할: 관리자

프로시저

1. 다음으로 이동 시스템 **OAuth** 〉 **JWT** 제공자.
2. MS **Teams** 커넥터 **JWT** 제공자 기록을 엽니다.
3. 표준 클레임 관련 목록에서 **iss**, **sub** 및 **aud** 에 대한 값을 입력합니다.

필드	값
aud	https://login.microsoftonline.com/<### ID>/oauth2/token 형식의 Microsoft Online URL. <tenant-id>를 Azure Portal에 등록된 애플리케이션의 디렉터리(테넌트) **ID** 값으로 바꿉니다.
ISS는	Azure 포털에 등록한 애플리케이션의 애플리케이션(클라이언트) **ID**입니다.
하위	Azure 포털에 등록한 애플리케이션의 애플리케이션(클라이언트) **ID**입니다.

4. 업데이트를 클릭합니다.

인증서를 사용하여 연결 설정

인증서를 사용하여 새로 만든 Microsoft Teams Graph 애플리케이션 간에 연결을 설정합니다.

시작하기 전에

필요한 역할: 관리자

프로시저

1. 다음으로 이동 연결 및 자격 증명 〉 연결 및 자격 증명 별칭.
2. **Microsoft Teams** 스포크를 엽니다.
3. 필드 값 구성 템플릿: **MSIM Microsoft Teams** 커넥터 인증 코드 템플릿을 수정하고 양식을 저장합니다.

> **주:**
> 이 템플릿에는 MSTeams 통합에 필요한 위임된 API 권한이 포함되어 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 관련 링크 섹션에서 새 연결 및 자격 증명 작성을 클릭하십시오.

5. **OAuth** 토큰 작성 및 가져오기를 클릭합니다.
   401- unauthorizeised라는 오류 메시지가 표시됩니다.
6. 양식을 다시 로드하고 연결 관련 목록에서 기록을 엽니다.
7. 특성 섹션의 인코딩된 인증서 지문 특성에 Base64로 인코딩된 지문 값을 입력합니다.

   주:
   지문 값은 16진수 값입니다. 16진수 toBase64(Hex to Base64) 변환기 도구를 사용하여 지문 값을 Base64 값으로 인코딩할 수 있습니다.

8. 다음으로 이동 시스템 **OAuth** 〉 애플리케이션 레지스트리
9. **MSIM Microsoft Teams** 커넥터 인증 코드 기록을 엽니다.
10. OAuth API 스크립트 수정: **OAuthUtilJWTMSTeamsConnector**.
11. 다음으로 이동 연결 및 자격 증명 〉 자격 증명.
12. **MSIM Microsoft Teams** 커넥터 자격 증명 기록을 엽니다.
13. 관련 링크에서 **OAuth** 토큰 가져오기를 클릭합니다.
    성공 시 다음 API 권한이 Azure 애플리케이션에 추가됩니다.

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (13)				
Channel.Create	Delegated	Create channels	Yes	Granted for Service Now
Channel.Delete.All	Delegated	Delete channels	Yes	Granted for Service Now
Channel.ReadBasic.All	Delegated	Read the names and descriptions of channels	No	Granted for Service Now
ChannelMember.ReadWrite.All	Delegated	Add and remove members from channels	Yes	Granted for Service Now
ChannelMessage.Read.All	Delegated	Read user channel messages	Yes	Granted for Service Now
ChannelSettings.ReadWrite.All	Delegated	Read and write the names, descriptions, and settings of ch...	Yes	Granted for Service Now
offline_access	Delegated	Maintain access to data you have given it access to	No	Granted for Service Now
openid	Delegated	Sign users in	No	Granted for Service Now
Team.Create	Delegated	Create teams	No	Granted for Service Now
TeamMember.ReadWrite.All	Delegated	Add and remove members from teams	Yes	Granted for Service Now
TeamSettings.ReadWrite.All	Delegated	Read and change teams' settings	Yes	Granted for Service Now
User.Read	Delegated	Sign in and read user profile	No	Granted for Service Now
User.Read.All	Delegated	Read all users' full profiles	Yes	Granted for Service Now

클라이언트 비밀 값 사용

클라이언트 비밀 값을 사용하여 Graph 애플리케이션 레지스트리 기록을 구성합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. Azure AD 포털에서 앱 등록 으로 이동합니다.
2. 관리 섹션에서 인증서 및 암호를 클릭합니다.
3. 새 클라이언트 비밀 을 클릭합니다.
4. 값 필드에서 생성된 클라이언트 비밀을 복사하고 기록해 둡니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

클라이언트 비밀을 사용하여 연결 설정

새로 만든 Microsoft Teams Graph 애플리케이션과 ServiceNow AI Platform 인스턴스 간의 연결을 설정합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 연결 및 자격 증명 〉 연결 및 자격 증명 별칭.
2. **Microsoft Teams** 스포크를 엽니다.
3. 필드 값 구성 템플릿: **MSIM Microsoft Teams** 커넥터 인증 코드 템플릿을 수정하고 양식을 저장합니다.

   주:
   이 템플릿에는 MSTeams 통합에 필요한 위임된 API 권한이 포함되어 있습니다.

4. 관련 링크 섹션에서 새 연결 및 자격 증명 작성을 클릭하십시오.

5. **OAuth** 토큰 작성 및 가져오기를 클릭합니다.
   성공 시 다음 API 권한이 Azure 애플리케이션에 추가됩니다.

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (13)				
Channel.Create	Delegated	Create channels	Yes	Granted for Service Now
Channel.Delete.All	Delegated	Delete channels	Yes	Granted for Service Now
Channel.ReadBasic.All	Delegated	Read the names and descriptions of channels	No	Granted for Service Now
ChannelMember.ReadWrite.All	Delegated	Add and remove members from channels	Yes	Granted for Service Now
ChannelMessage.Read.All	Delegated	Read user channel messages	Yes	Granted for Service Now
ChannelSettings.ReadWrite.All	Delegated	Read and write the names, descriptions, and settings of ch...	Yes	Granted for Service Now
offline_access	Delegated	Maintain access to data you have given it access to	No	Granted for Service Now
openid	Delegated	Sign users in	No	Granted for Service Now
Team.Create	Delegated	Create teams	No	Granted for Service Now
TeamMember.ReadWrite.All	Delegated	Add and remove members from teams	Yes	Granted for Service Now
TeamSettings.ReadWrite.All	Delegated	Read and change teams' settings	Yes	Granted for Service Now
User.Read	Delegated	Sign in and read user profile	No	Granted for Service Now
User.Read.All	Delegated	Read all users' full profiles	Yes	Granted for Service Now

MS Teams Graph 스포크 사용자용 **MS Teams** 채팅 커넥터 활성화

기존 사용자인 경우 이 섹션의 절차에 따라 MS Teams Graph 스포크 사용자용 Microsoft Teams 채팅 커넥터를 활성화합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

기존 **Microsoft Teams Graph** 스포크 사용자인 경우 다음 단계를 따르십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- Microsoft Teams Graph 스포크에서 사용하는 Azure Portal에 등록된 애플리케이션으로 이동합니다.
- **API** 권한 섹션으로 이동하여 필요한 API 권한을 구성합니다.
- 권한 추가를 클릭합니다.
- **Microsoft Graph**를 선택합니다.
- Microsoft Teams 커넥터 애플리케이션을 사용하려면 Azure Portal에서 애플리케이션에 "ChannelMember.ReadWrite.All" 및 "TeamMember.ReadWrite.All"이라는 두 개의 위임된 권한을 추가해야 합니다.
- 위의 필수 권한을 추가한 후 관리자 동의 부여를 클릭합니다.

기존 사용자의 인스턴스에 **MS Teams** *ServiceNow AI Platform* 구성:

- 연결 및 자격 증명 별칭으로 이동합니다.
- **Microsoft Teams** 스포크 기록을 선택합니다.
- Microsoft Teams 스포크와 연결된 자격 증명 기록을 선택합니다.
- **OAuth** 토큰 가져오기를 클릭합니다. OAuth 새로 고침 토큰을 사용할 수 있다는 확인 메시지가 표시됩니다.

기존 사용자로서 이제 Microsoft Teams 채팅 커넥터 애플리케이션과 Microsoft Teams 그래프 API 통합을 완료했습니다.

중요 보안 인시던트 관리 컨퍼런스 회의 통합

전화 회의 통합을 사용하면 중요 보안 인시던트 관리 고객 및 동료 에이전트와 공동 작업하여 , Cisco WebexMSIM Zoom 애플리케이션의 비디오 및 화면 공유 옵션을 Microsoft Teams사용하여 고객 문제를 해결할 수 있습니다.

컨퍼런스 중요 보안 인시던트 관리 회의 통합을 사용하면 , , 또는 Zoom 애플리케이션에서 직접 회의를 관리하고 시작하여 Microsoft TeamsCisco Webex컨퍼런스 커뮤니케이션 채널을 커뮤니케이션 채널과 알림 통합할 수 있습니다중요 보안 인시던트 관리.

MSI 관리자는 MSIM 전화 회의 통합을 사용하여 , Cisco Webex 또는 Zoom 회의를 시작할 Microsoft Teams수 있습니다. 외부 공급업체 서비스 제공자와의 전화 회의를 통신 채널로 통합하여 중요 보안 인시던트 관리 이해 관계자와 만나 주요 보안 인시던트를 해결합니다.

주요 기능

관리 전화 회의 통합은 다음과 같은 중요 보안 인시던트 주요 기능을 제공합니다.

- MSI 관리자는 중요 보안 인시던트에서 직접 , Cisco Webex, 또는 Zoom 전화 회의를 시작할 Microsoft Teams수 있습니다.
- 통화에 추가 참가자를 초대합니다.
- 통화 기록 및 채팅 상세 정보를 확인합니다.
- 이메일 및 Microsoft Teams 채팅을 통해 참가자에게 초대를 보냅니다.

전화 회의 시작

한 명 이상의 사용자를 전화 회의에 초대하여 작업 또는 중요 보안에서 전화 회의를 시작합니다. 두 명 이상의 참가자가 참가한 경우에만 전화 회의가 시작됩니다.

시작하기 전에
필요한 역할: sn_msi.workspace_manager

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

인스턴스에서 다음 ServiceNow# 작업을 수행했는지 확인합니다.

- 플러그인(com.snc.notify)을 설치하고 활성화했습니다 알림 .
- 구성 가능한 알림 작업 공간 앱을 위한 UI 구성 요소를 설치했습니다.
- 시각적 작업 보드 플러그인(com.devsnc.snb_vtb)을 설치하고 활성화했습니다.

자세한 내용은 통합 허브 요청을 참조하십시오.

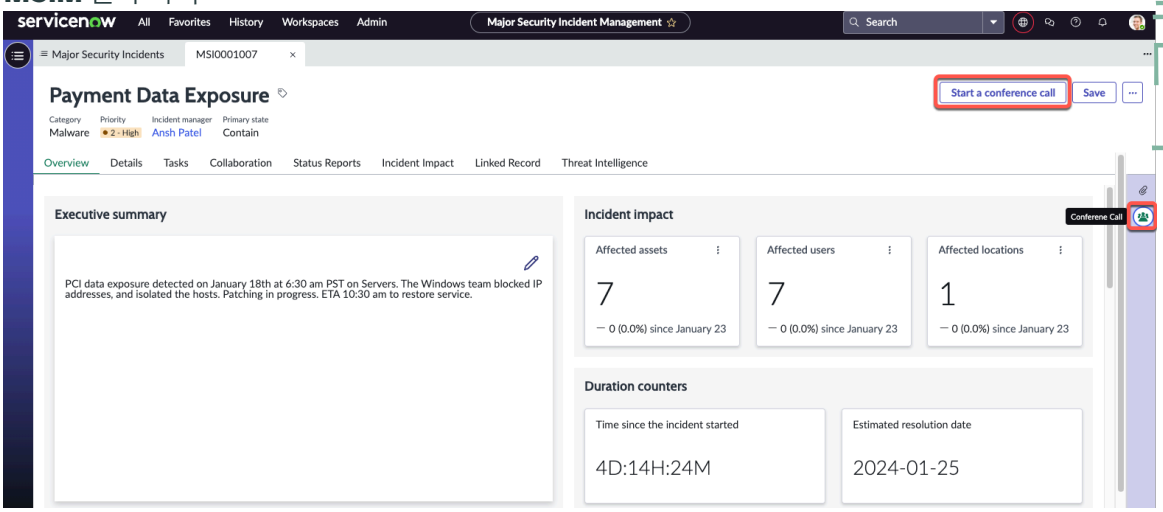
이 태스크 정보
통화 참가자에는 다음이 포함될 수 있습니다.

- 특정 책임이 할당된 사용자입니다.
- 임시 또는 요청 시 연락처
- 기타 외부 공급업체 연락처

프로시저

1. 다음으로 이동 작업 공간 〉 중요 보안 인시던트 관리.
2. 중요 보안 인시던트 목록에서 중요 보안 인시던트를 선택합니다.
3. 전화 회의 작업 시작을 선택합니다.
4. 오른쪽 컨텍스트 메뉴에서 회의 아이콘을 선택하고 + 아이콘을 선택하여 컨퍼런스 회의를 시작할 수도 있습니다.
   전화 회의 시작 팝업이 나타납니다.

MSIM 전화 회의



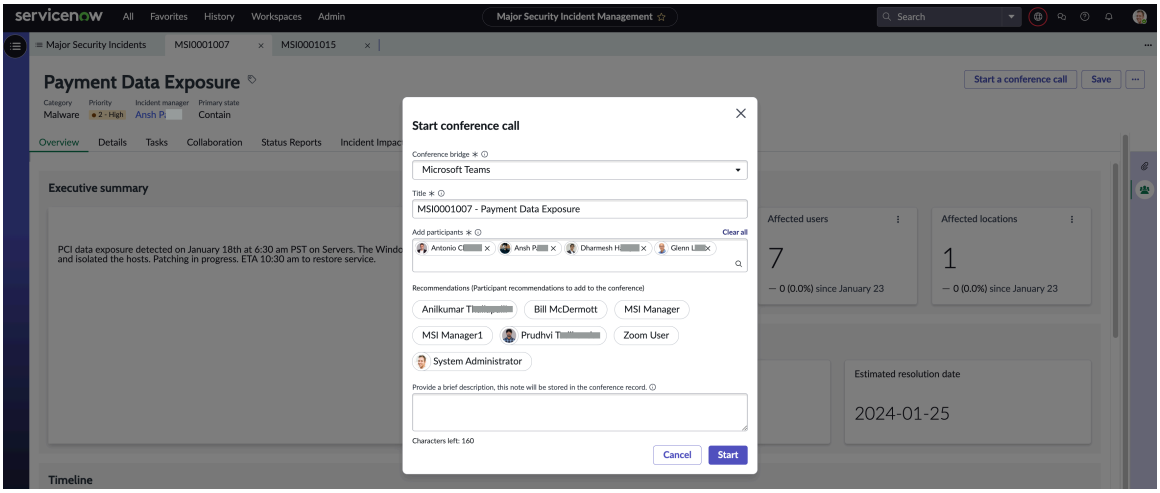
5. Conference bridge(컨퍼런스 브리지) 필드에서 연결할 **Conference** 브리지 를 선택합니다.
   예를 들어 Microsoft Team, Zoom 또는 Cisco Webex와 같습니다.
6. 제목 필드에 전화 회의의 이유를 설명하는 제목을 입력합니다.
7. 참가자 추가 필드에서 전화 회의 참가자를 선택합니다.
   검색 옵션을 사용하여 필요한 참가자를 찾아 추가하거나, 전화 회의에 추가할 참가자 권장 사항을 제공하는 권장 사항 목록에서 참가자를 선택할 수 있습니다.

   전화 회의를 시작하는 사용자(호스트)가 선택한 참가자 목록에 자동으로 추가됩니다. 중요 보안 인시던트와 관련된 모든 사용자는 기본적으로 권장 사항 목록에서 사용할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
선택한 참가자의 이메일 주소가 유효한지 확인합니다.

전화 회의 시작



8. 참가자를 선택한 후 설명 필드에 전화 회의를 시작하는 이유에 대한 간략한 설명을 입력합니다.
   입력한 설명이 회의 기록에 추가됩니다.
9. 참가자 목록이 완료되면 시작을 선택합니다.
   선택한 컨퍼런스 회의 브리지에서 전화 회의가 시작됩니다. 모든 참가자는 이메일을 통해 알림을 받으며, 선택한 각 회의 브리지를 통해서도 알림을 받습니다.
10. 중요 보안 인시던트 위에 있는 여기를 클릭 옵션을 선택하여 전화 회의에 참가합니다.
    참가자는 이메일 알림의 링크 또는 선택한 회의 브리지의 알림을 사용하여 통화에 참가할 수 있습니다.
11. 연관된 중요 보안 인시던트를 열어 전화 회의 세부 정보를 봅니다.
    최종 참가자가 회의에서 나가면 전화 회의가 종료되거나 통화 종료 를 선택하여 전화 회의를 종료합니다.

전화 회의에 참가자 추가

전화 회의 시작 팝업의 검색 옵션을 사용하여 전화 회의에 참가자를 추가하고 필요한 참가자를 찾아 추가합니다. 컨퍼런스 회의에 추가할 참가자 권장 사항을 제공하는 권장 사항 목록에서 참가자를 선택하여 참가자를 추가할 수도 있습니다.

시작하기 전에
필요한 역할: sn_msi.workspace_manager

이 태스크 정보
전화 회의를 시작하는 사용자(호스트)가 선택한 참가자 목록에 자동으로 추가됩니다. 중요 보안 인시던트와 관련된 모든 사용자는 기본적으로 권장 사항 목록에서 사용할 수 있습니다.

통화 참가자에는 다음이 포함될 수 있습니다.

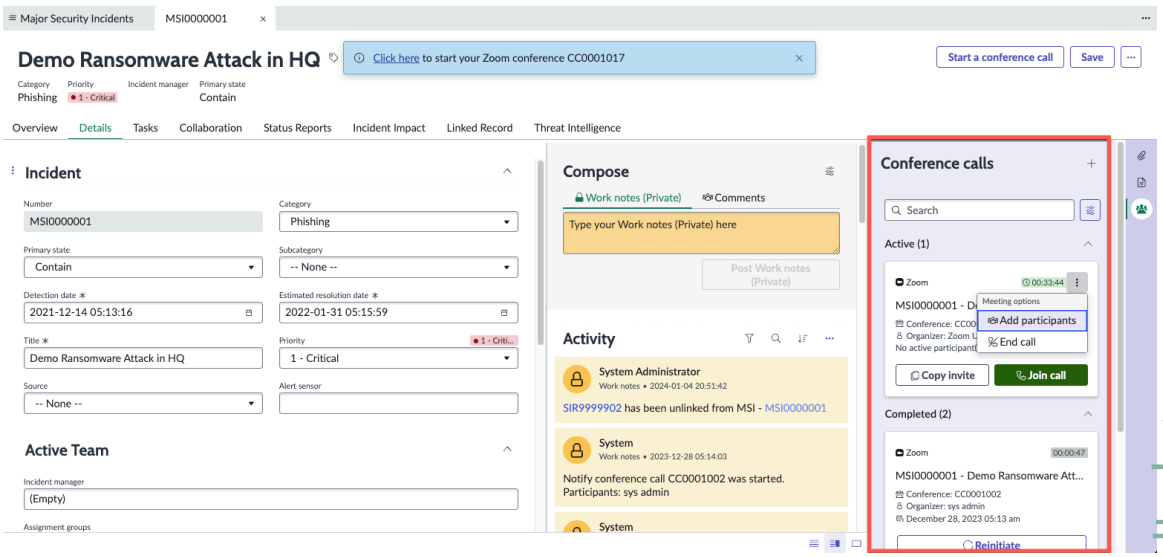
- 특정 책임이 할당된 사용자입니다.
- 임시 또는 요청 시 연락처
- 기타 외부 공급업체 연락처

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 작업 공간 〉 중요 보안 인시던트 관리.
2. 중요 보안 인시던트 목록에서 전화 회의에서 해결하려는 중요 보안 인시던트를 선택합니다.
3. 오른쪽 컨텍스트 메뉴에서 아이콘을 선택하여 컨퍼런스 회의의 세부 정보를 봅니다. 여기에는 회의 브리지 이름, 주최자 이름, 날짜, 시간, 통화 시간, 활성 및 비활성 참가자와 같은 세부 정보가 포함됩니다.
4. 활성 전화 회의 옆에 있는 ⋮ 선택하고 참가자 추가 옵션을 선택합니다.

전화 회의에 참가자 추가



5. 검색 옵션을 사용하여 필요한 참가자를 찾아 추가하거나, 전화 회의에 추가할 참가자 권장 사항을 제공하는 권장 사항 목록에서 참가자를 선택할 수 있습니다.
6. 참가자를 선택한 후 설명 필드에 전화 회의를 시작하는 이유에 대한 간략한 설명을 입력합니다. 모든 참가자는 이메일을 통해 알림을 받으며, 선택한 각 회의 브리지를 통해서도 알림을 받습니다. 참가자는 이메일 알림의 링크 또는 선택한 회의 브리지의 알림을 사용하여 통화에 참가할 수 있습니다.
7. 또는 오른쪽 컨텍스트 메뉴의 컨퍼런스 회의 섹션에서 초대 복사 옵션을 선택하여 참가자를 추가하고 필요한 참가자와 공유할 수 있습니다.

전화 회의에서 참가자 음소거

MSI 관리자 또는 전화 회의 호스트는 전화 회의의 특정 참가자 또는 모든 참가자를 음소거할 수 있습니다.

시작하기 전에

필요한 역할: sn_msi.workspace_manager

이 절차를 시작하기 전에 한 명 이상의 참가자가 있는 활성 전화 회의가 있는지 확인합니다.

프로시저

1. 다음으로 이동 작업 공간 〉 중요 보안 인시던트 관리.
2. 중요 보안 인시던트 목록에서 전화 회의에서 해결하려는 중요 보안 인시던트를 선택합니다.
3. 오른쪽 컨텍스트 메뉴에서 아이콘을 선택하여 컨퍼런스 회의의 세부 정보를 봅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 활성 회의 브리지에서 통화 참가 를 선택합니다.
5. 전화 회의에 참가한 후 음소거할 참가자를 선택하고 회의 브리지에서 음소거를 선택합니다.
6. 전화 회의의 모든 참가자를 음소거하려면 회의 컨트롤에서 참가자를 선택하고 모두 음소거를 선택합니다.

컨퍼런스 회의 상세 정보 보기

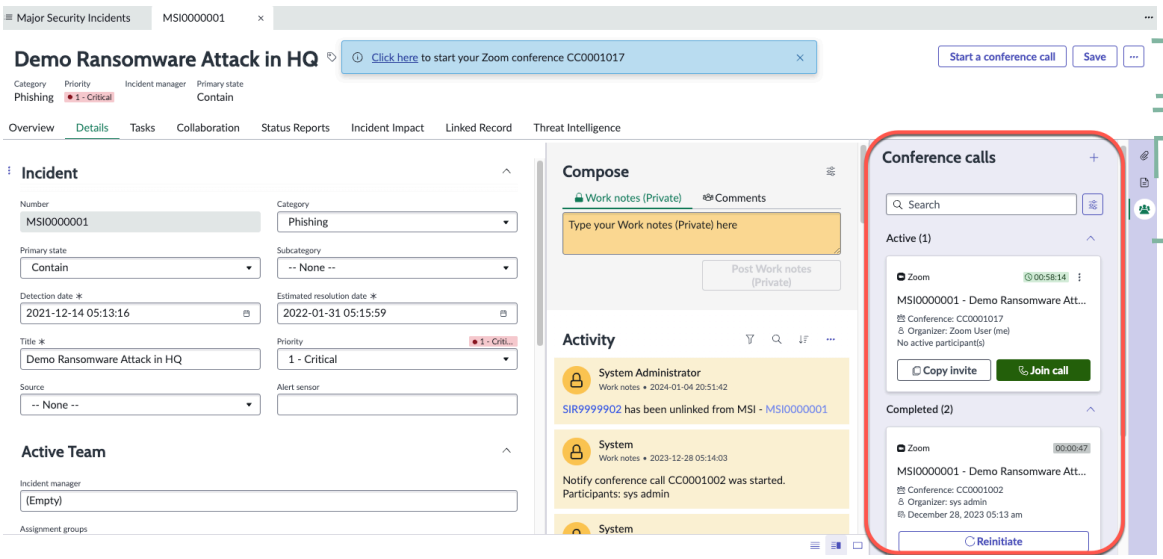
컨퍼런스 회의는 중요 보안 인시던트의 활동 섹션에 시스템 활동으로 나열되며 컨퍼런스 회의 관련 목록에도 나열됩니다. 회의 브리지 이름, 주최자 이름, 날짜, 시간, 통화 시간, 활성 및 비활성 참가자와 같은 상세 정보를 볼 수 있습니다.

시작하기 전에
필요한 역할: sn_msi.workspace_manager

프로시저

1. 다음으로 이동 작업 공간 〉 중요 보안 인시던트 관리.
2. 중요 보안 인시던트 목록에서 전화 회의에서 해결하려는 중요 보안 인시던트를 선택합니다.
3. 오른쪽 컨텍스트 메뉴에서 아이콘을 선택하여 컨퍼런스 회의의 세부 정보를 봅니다.
   여기에는 회의 브리지 이름, 주최자 이름, 날짜, 시간, 통화 시간, 활성 및 비활성 참가자와 같은 세부 정보가 포함됩니다.

컨퍼런스 회의 상세 정보 보기



4. 검색 옵션을 사용하여 특정 전화 회의를 찾을 수 있습니다.
   동일한 중요 보안 인시던트에 대한 호출이 여러 개 있을 수 있습니다.
5. 전화 회의에 참가자를 추가하려면 활성 통화 전화 회의 옆에 있는 ⋮ 선택하고 참가자 추가 옵션을 선택합니다.
6. 초대 복사 옵션을 사용하고 필요한 참가자와 링크를 공유하여 참가자를 추가할 수도 있습니다.
7. 전화 회의에 참가하려면 활성 섹션으로 이동하여 필요한 전화 회의의 통화 참가 옵션을 선택합니다.
8. 전화 회의를 종료하려면 활성 전화 회의 옆에 있는 ⋮ 선택하고 통화 종료 옵션을 선택합니다.
9. 컨퍼런스 회의를 다시 시작하려면 완료됨 섹션으로 이동하여 필요한 컨퍼런스 회의의 다시 시작 옵션을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

와 **MSIM** 컨퍼런스 회의 통합 **Microsoft Teams**

컨퍼런스 회의 Microsoft Teams 통합을 사용하면 주요 보안 인시던트에서 직접 컨퍼런스 회의를 관리하고 시작할 Microsoft Teams 수 있습니다.

주요 기능

- 중요 보안 인시던트 또는 주요 보안 워크벤치에서 직접 컨퍼런스 회의를 시작하고 종료합니다 Microsoft Teams .
- 참가자를 Microsoft Teams 추가하거나 제거하여 전화 회의를 관리합니다.

필수 구성요소

인스턴스에 다음 통합 허브 플러그인을 ServiceNow 설치했는지 확인합니다.

- 알림 플러그인(com.snc.notify)
- Microsoft Teams 커뮤니케이션 스포크 플러그인(sn_msteams_com_spk).
- Azure Active Directory sn_now_azure(사용자 매핑 플러그인).
- 알림 구성 가능한 작업 공간의 UI 구성요소

자세한 내용은 통합 허브 요청을 참조하십시오.

구성

- 미리 구성된 앱을 사용하여 MSIM 전화 회의 Microsoft Teams 통합을 구성하려면 문서를 참조하십시오 Integrate Notify connector pre-published app with Microsoft Teams .
- 자체 구성된 앱을 사용하여 MSIM 전화 회의 Microsoft Teams 통합을 구성하려면 문서를 참조하십시오 Integrating Notify connector self-configured app with Microsoft Teams .

MSIM 전화 회의 **Microsoft Teams** 통합 사용

다음 단계에서는 중요 보안 인시던트에서 직접 전화 회의를 관리하고 시작할 Microsoft Teams 수 있는 방법에 대한 둘러보기를 제공합니다.

시작하기 전에

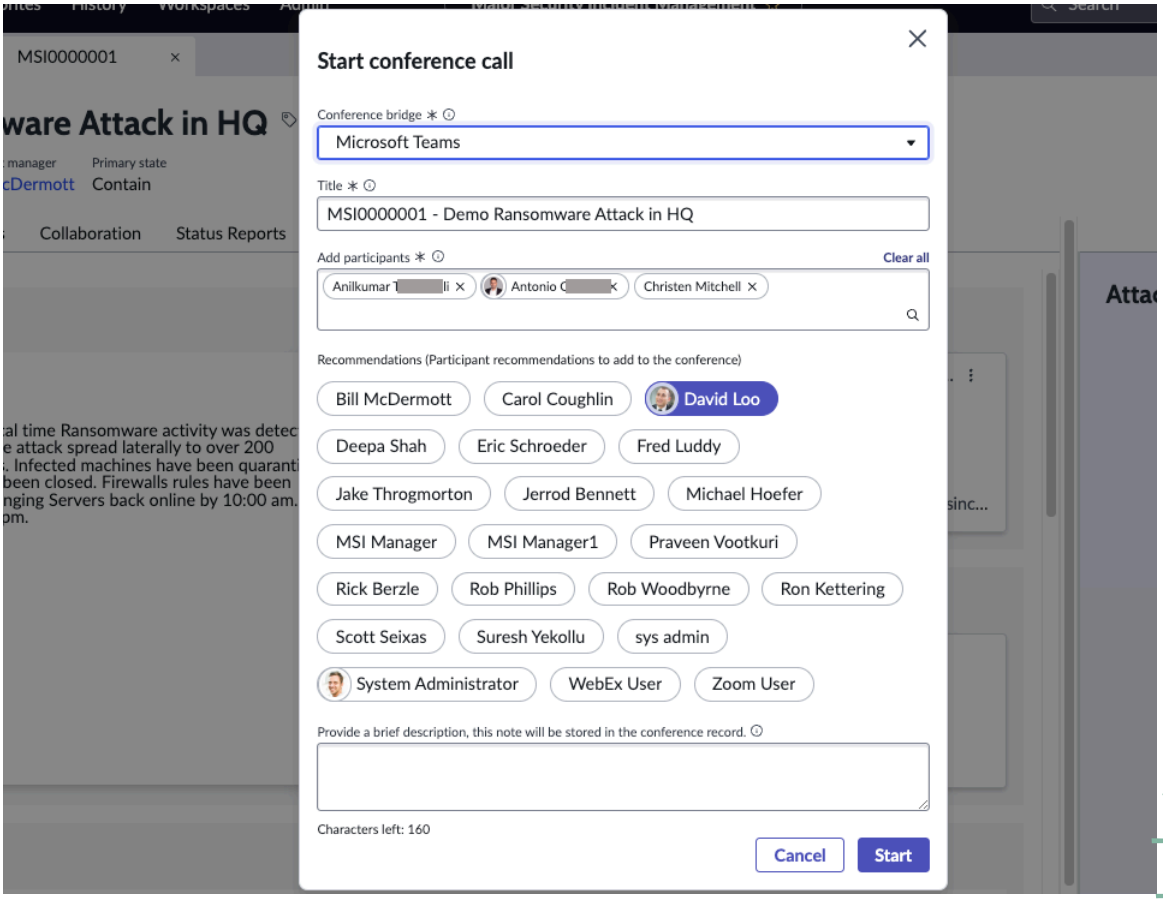
필요한 역할: sn_msi.workspace_manager

프로시저

1. 다음으로 이동 작업 공간 〉 중요 보안 인시던트 관리.
2. 중요 보안 인시던트 목록에서 중요 보안 인시던트를 선택합니다.
3. 전화 회의 작업 시작을 선택합니다.
4. 오른쪽 컨텍스트 메뉴에서 회의 아이콘을 선택하고 + 아이콘을 선택하여 컨퍼런스 회의를 시작할 수도 있습니다.
   전화 회의 시작 팝업이 나타납니다.
5. 연결하려는 회의 브리지로 **Microsoft Teams** 를 선택합니다.
6. 제목 필드에 Microsoft Teams 전화 회의의 이유를 설명하는 제목을 입력합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

전화 회의 **Microsoft Teams** 통합 사용



7. 참가자 추가 필드에서 Microsoft Teams 전화 회의 참가자를 선택합니다.
검색 옵션을 사용하여 필요한 참가자를 찾아 추가하거나, Microsoft Teams 전화 회의에 추가할 참가자 권장 사항을 제공하는 권장 사항 목록에서 참가자를 선택할 수 있습니다.

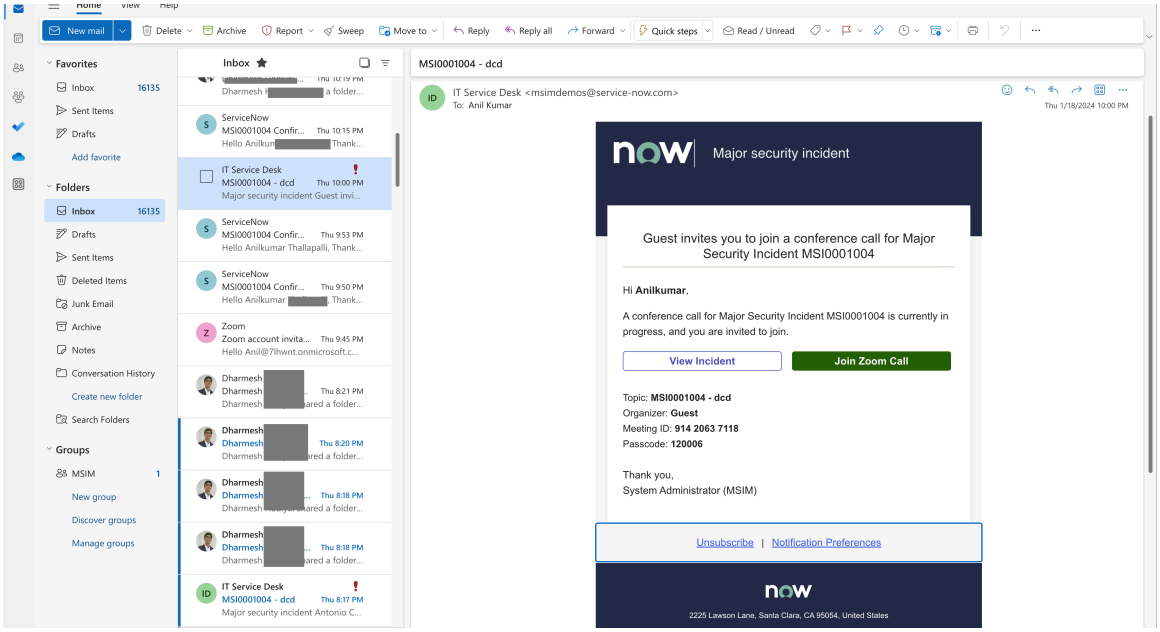
   Microsoft Teams 전화 회의를 시작하는 사용자(호스트)가 선택한 참가자 목록에 자동으로 추가됩니다. 중요 보안 인시던트와 관련된 모든 사용자는 기본적으로 권장 사항 목록에서 사용할 수 있습니다.

   주:
   선택한 참가자의 이메일 주소가 유효한지 확인합니다.

8. 참가자를 선택한 후 설명 필드에 전화 회의를 시작하는 이유에 대한 간략한 설명을 입력합니다.
입력한 설명이 회의 기록에 추가됩니다.
9. 참가자 목록이 완료되면 시작을 선택합니다.
Microsoft Teams 앱에서 전화 회의가 시작됩니다. 모든 참가자는 MSIM 앱의 이메일을 통해 알림을 받고 다른 알림은 Microsoft Teams 앱의 봇을 통해 전송됩니다.
10. 중요 보안 인시던트 위에 있는 여기를 클릭 옵션을 선택하여 Microsoft Teams 앱에서 전화 회의에 참가합니다.
참가자는 MSIM 이메일 알림의 링크 또는 Microsoft Teams 앱의 알림을 사용하여 통화에 참가할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이메일 알림



11. MSIM 작업 공간에서 연결된 중요 보안 인시던트를 열어 전화 회의 세부 정보를 봅니다.

최종 참가자가 통화에서 나가면 전화 회의가 종료되거나 전화 회의 섹션에서 통화 종료 를 선택하여 전화 회의를 종료합니다.

와 **MSIM** 컨퍼런스 회의 통합 **Zoom**

컨퍼런스 회의 Zoom 통합을 사용하면 주요 보안 인시던트에서 직접 컨퍼런스 회의를 관리하고 시작할 Zoom 수 있습니다.

주요 기능

- 중요 보안 인시던트나 변경 또는 중요 인시던트 워크벤치와 같은 작업 기록에서 직접 회의를 시작하고 종료합니다 Zoom .
- 참가자를 추가하거나 제거하여 회의를 관리합니다 Zoom .
- 추가 분석을 위해 회의 기간 및 참석자와 같은 회의 상세 정보를 추적하고 보고합니다.

필수 구성요소

인스턴스에 다음 통합 허브 플러그인을 ServiceNow 설치했는지 확인합니다.

- 알림 플러그인(com.snc.notify)
- Zoom 스포크(sn_zoom_spoke)
- 알림 확대/축소(sn_notify_zoom)
- 알림 구성 가능한 작업 공간의 UI 구성요소

자세한 내용은 통합 허브 요청을 참조하십시오.

구성

통신 채널을 사용하여 알림 MSIM 전화 회의 Zoom 통합을 구성하려면 문서를 Configure Notify Zoom connector in Notify 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

MSIM 전화 회의 **Zoom** 통합 사용

다음 단계에서는 중요 보안 인시던트에서 직접 전화 회의를 관리하고 시작할 Zoom 수 있는 방법에 대한 둘러보기를 제공합니다.

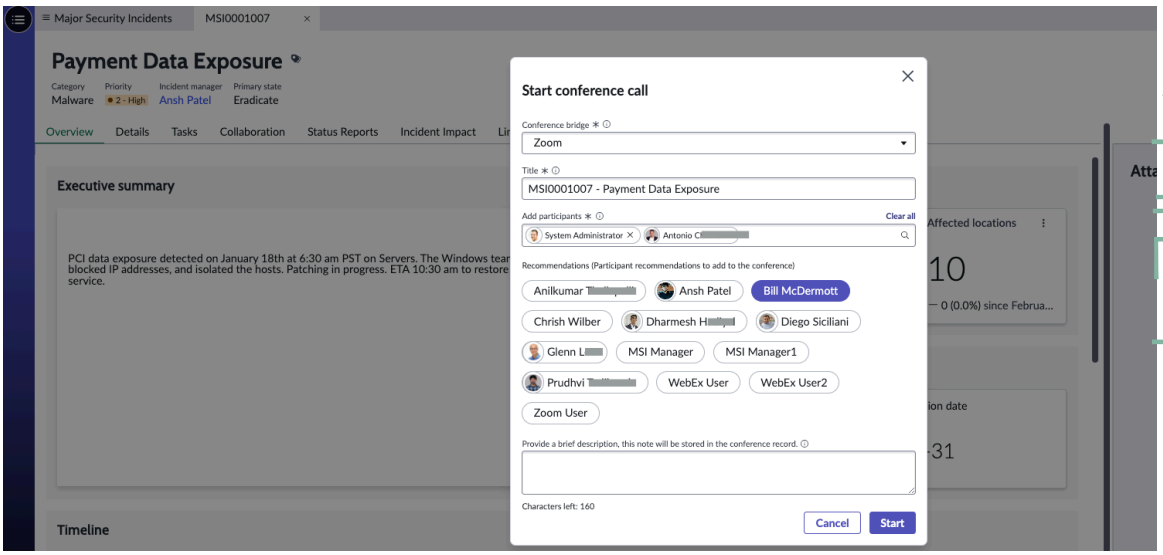
시작하기 전에

필요한 역할: sn_msi.workspace_manager

프로시저

1. 다음으로 이동 작업 공간 〉 중요 보안 인시던트 관리.
2. 중요 보안 인시던트 목록에서 중요 보안 인시던트를 선택합니다.
3. 전화 회의 작업 시작을 클릭합니다.
4. 오른쪽 컨텍스트 메뉴에서 아이콘을 클릭하고 + 아이콘을 선택하여 컨퍼런스 회의를 시작할 수도 있습니다.
   전화 회의 시작 팝업이 나타납니다.
5. 연결하려는 회의 브리지로 **Zoom** 을 선택합니다.
6. 제목 필드에 Zoom 전화 회의의 이유를 설명하는 제목을 입력합니다.

전화 회의 **Zoom** 통합 사용



7. 참가자 추가 필드에서 Zoom 전화 회의 참가자를 선택합니다.
   검색 옵션을 사용하여 필요한 참가자를 찾아 추가하거나, Zoom 전화 회의에 추가할 참가자 권장 사항을 제공하는 권장 사항 목록에서 참가자를 선택할 수 있습니다.

   Zoom 전화 회의를 시작하는 사용자(호스트)가 선택한 참가자 목록에 자동으로 추가됩니다. 중요 보안 인시던트와 관련된 모든 사용자는 기본적으로 권장 사항 목록에서 사용할 수 있습니다.

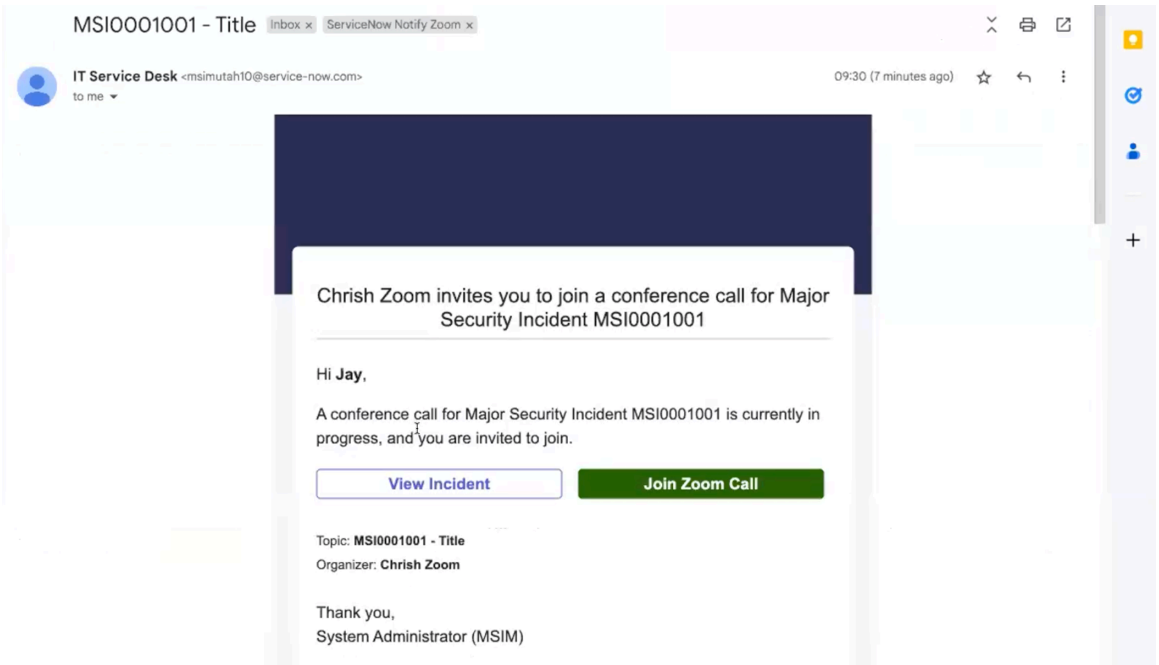
   주:
   선택한 참가자의 이메일 주소가 유효한지 확인합니다.

8. 참가자를 선택한 후 설명 필드에 전화 회의를 시작하는 이유에 대한 간략한 설명을 입력합니다.
   입력한 설명이 회의 기록에 추가됩니다.
9. 참가자 목록이 완료되면 시작을 클릭합니다.
   전화 회의가 Zoom 앱에서 시작됩니다. 모든 참가자는 두 개의 이메일을 통해 알림을 받으며, 한 이메일은 MSIM 앱에서 참가자에게 전송되고 다른 이메일은 Zoom 회의 브리지에서 전송됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

10. 중요 보안 인시던트 위에 있는 여기를 클릭 옵션을 선택하여 Zoom 앱에서 전화 회의에 참가합니다. 참가자는 MSIM 이메일 알림의 링크 또는 Zoom 앱의 알림을 사용하여 통화에 참여할 수 있습니다.

이메일 알림



11. MSIM 작업 공간에서 연결된 중요 보안 인시던트를 열어 전화 회의 세부 정보를 봅니다.

최종 참가자가 통화에서 나가면 전화 회의가 종료되거나 전화 회의 섹션에서 통화 종료 를 선택하여 전화 회의를 종료합니다.

컨퍼런스 회의가 녹화된 경우 잠시 후 관련된 중요 보안 인시던트의 컨퍼런스 회의 섹션에서 기록을 사용할 수 있습니다.

와 **MSIM** 컨퍼런스 회의 통합 **Cisco Webex**

MSIM 컨퍼런스 회의 Cisco Webex 통합을 사용하면 주요 보안 인시던트에서 직접 컨퍼런스 회의를 관리하고 시작할 Cisco Webex 수 있습니다.

주요 기능

- 중요 보안 인시던트에서 직접 회의를 시작하고 종료합니다 Cisco Webex .
- 참가자를 Cisco Webex 추가하거나 제거하여 회의를 관리합니다.

필수 구성요소

인스턴스에 다음 통합 허브 플러그인을 ServiceNow 설치했는지 확인합니다.

- 알림 플러그인(com.snc.notify)
- 알림 Cisco Webex 커넥터(sn_notify_webex)
- Cisco Webex Teams 스포크(sn_cisco_teams_spk)
- 알림 구성 가능한 작업 공간의 UI 구성요소

자세한 내용은 통합 허브 요청을 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

구성

통신 채널을 사용하여 알림 MSIM 전화 회의 Cisco Webex 통합을 구성하려면 문서를 Configure Notify Cisco Webex Connector 참조하십시오.

컨퍼런스 회의 **Cisco Webex** 통합 사용

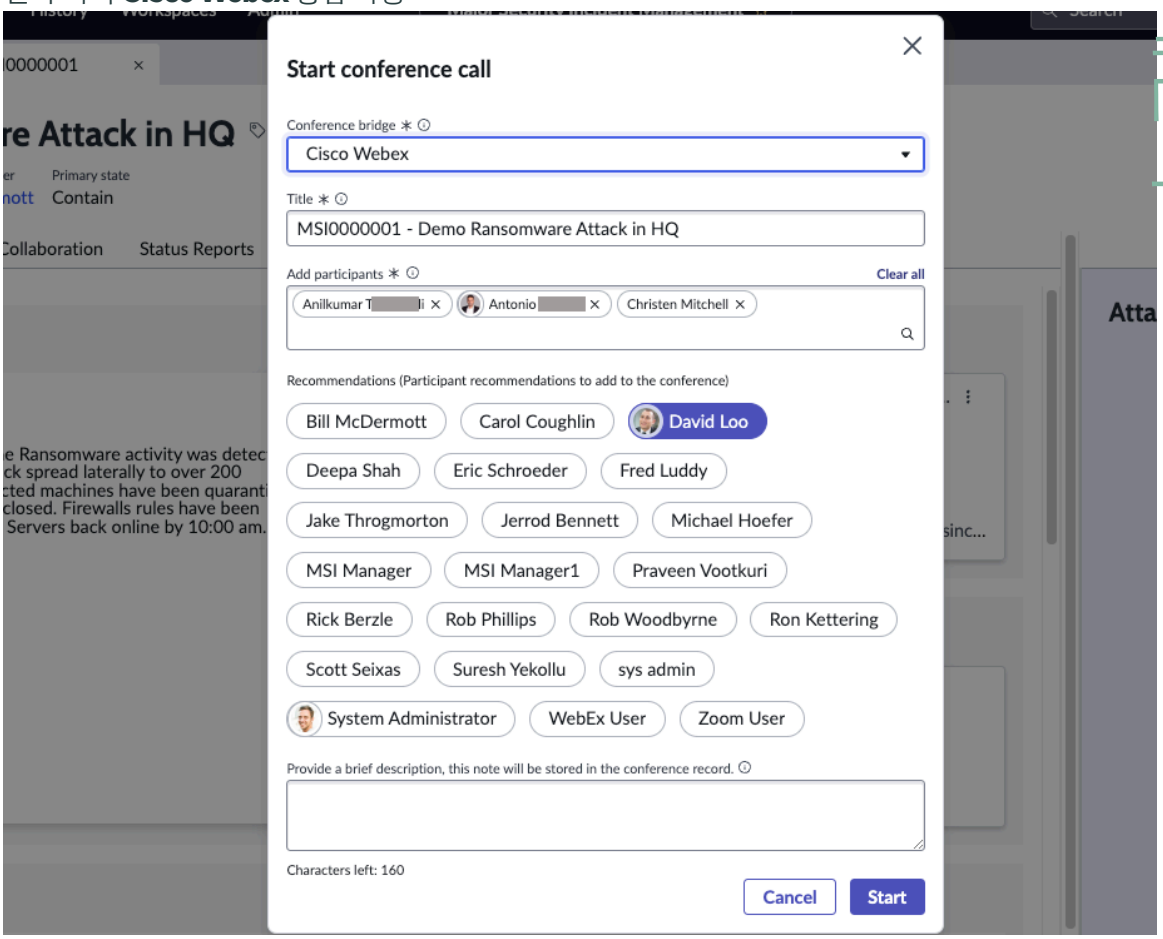
다음 단계에서는 중요 보안 인시던트에서 직접 전화 회의를 관리하고 시작할 Cisco Webex 수 있는 방법에 대한 둘러보기를 제공합니다.

시작하기 전에
필요한 역할: sn_msi.workspace_manager

프로시저

1. 다음으로 이동 작업 공간 〉 중요 보안 인시던트 관리.
2. 중요 보안 인시던트 목록에서 중요 보안 인시던트를 선택합니다.
3. 전화 회의 작업 시작을 선택합니다.
4. 오른쪽 컨텍스트 메뉴에서 회의 아이콘을 선택하고 + 아이콘을 선택하여 컨퍼런스 회의를 시작할 수도 있습니다.
   전화 회의 시작 팝업이 나타납니다.
5. 연결하려는 전화회의 브리지로 **Cisco Webex** 를 선택합니다.
6. 제목 필드에 Cisco Webex 전화 회의에 대한 이유를 설명하는 제목을 입력합니다.

전화 회의 **Cisco Webex** 통합 사용



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

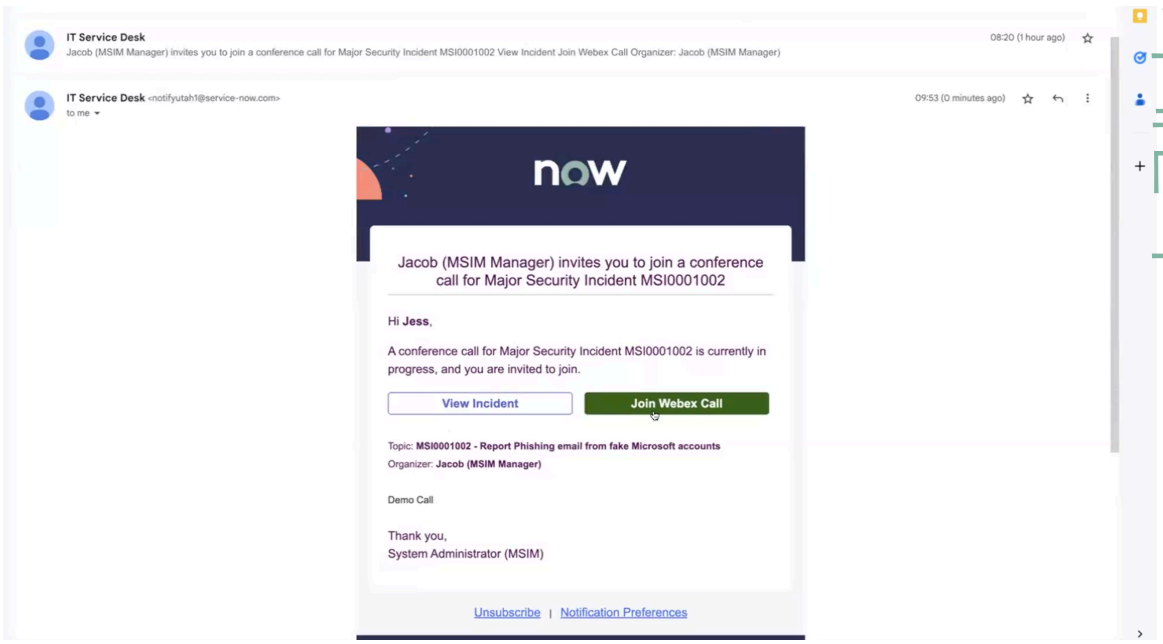
7. 참가자 추가 필드에서 Cisco Webex 전화 회의 참가자를 선택합니다.
검색 옵션을 사용하여 필요한 참가자를 찾아 추가하거나, Cisco Webex 전화 회의에 추가할 참가자 권장 사항을 제공하는 권장 사항 목록에서 참가자를 선택할 수 있습니다.

   Cisco Webex 전화 회의를 시작하는 사용자(호스트)는 선택한 참가자 목록에 자동으로 추가됩니다. 중요 보안 인시던트와 관련된 모든 사용자는 기본적으로 권장 사항 목록에서 사용할 수 있습니다.

   주:
   선택한 참가자의 이메일 주소가 유효한지 확인합니다.

8. 참가자를 선택한 후 설명 필드에 전화 회의를 시작하는 이유에 대한 간략한 설명을 입력합니다.
입력한 설명이 회의 기록에 추가됩니다.
9. 참가자 목록이 완료되면 시작을 선택합니다.
전화회의가 Cisco Webex 앱에서 시작됩니다. 모든 참가자는 두 개의 이메일을 통해 알림을 받습니다. 한 이메일은 MSIM 앱에서 참가자에게 전송되고 다른 이메일은 Cisco Webex 컨퍼런스 브리지에서 전송됩니다.
10. 주요 보안 인시던트 위에 있는 여기 클릭 옵션을 선택하여 Cisco Webex 앱에서 전화 회의에 참가합니다.
참가자는 MSIM 이메일 알림의 링크 또는 Cisco Webex 앱의 알림을 사용하여 통화에 참여할 수 있습니다.

이메일 알림



11. MSIM 작업 공간에서 연결된 중요 보안 인시던트를 열어 전화 회의 세부 정보를 봅니다.

    최종 참가자가 통화에서 나가면 전화 회의가 종료되거나 전화 회의 섹션에서 통화 종료 를 선택하여 전화 회의를 종료합니다.

    컨퍼런스 회의가 녹화된 경우 잠시 후 관련된 중요 보안 인시던트의 컨퍼런스 회의 섹션에서 기록을 사용할 수 있습니다.

중요 보안 인시던트 관리 구성

애플리케이션을 설치하고 구성합니다 중요 보안 인시던트 관리 .

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

중요사항:

- 구성을 빠르게 시작하려면 중요 보안 인시던트 관리 ServiceNow Store에서 Major Security Incident Management(MSIM) 빠른 시작 가이드를 참조하십시오.
- 앱을 설치한 중요 보안 인시던트 관리 후에는 KB1289784 에서 업데이트 세트를 임포트하여 부분적으로 사전 구성된 파일을 로드해야 합니다.

이 섹션에서는 인스턴스와의 ServiceNow 연결을 설정하기 위해 다른 외부 Microsoft 애플리케이션과 통합하여 기록 작업에 중요 보안 인시던트 필요한 필수 구성을 설정하는 방법을 알아봅니다.

파일 탐색기 구성요소 구성

파일 탐색기 작업 공간 구성요소는 중요 보안 인시던트와 관련된 아티팩트(파일) 컬렉션을 구성하고 추적합니다. 작업 공간과 같은 Microsoft SharePoint중요 보안 인시던트 관리 외부 공급업체 파일 호스팅 제공자와의 통합을 지원하도록 설계되었습니다.

- File Explorer 구성 요소: 파일 시스템을 표시하는 그래픽 사용자 인터페이스를 제공하고 사용자가 파일 작업을 수행할 수 있도록 합니다.
- File Explorer Core: 파일 탐색기 구성 요소가 외부 리포지토리와 통신하는 데 사용되는 기본 커넥터에 대해 알지 못해도 파일 시스템을 표시하고 다양한 파일 작업을 수행할 수 있도록 하는 추상화 계층을 제공합니다.
- File Explorer Microsoft SharePoint 커넥터 애플리케이션: 문서 라이브러리에서 Microsoft SharePoint 파일/폴더 메타데이터를 추적 및 가져오고 파일 작업을 수행하는 데 필요한 구현 모듈을 제공합니다.

코어 구성요소는 File Explorer 다양한 파일 공유 커넥터 애플리케이션이 연결 속성을 정의하는 데 필요한 기본 인프라를 제공합니다.

파일 호스팅 공급자 위치에서 파일 메타데이터를 끌어오려면 연결 속성을 추가하여 파일 리포지토리 드라이브 및 파일 리포지토리 공급자를 설치하고 구성해야 합니다.

현재 버전의 File Explorer경우 이러한 지침에는 파일 및 폴더 업데이트, 파일 작업 및 파일 활동 로깅과 같은 Microsoft SharePoint 파일 메타데이터 검색의 구성 및 구독이 포함됩니다. 중요 보안 인시던트와 관련된 개별 폴더를 만들려면 지정된 Microsoft SharePoint 문서 라이브러리 및 관련 드라이브 구성이 필요합니다.

File Explorer 와 같은 Microsoft SharePoint커넥터 애플리케이션도 허용합니다. 이 예제를 사용하여 다음과 같은 파일 작업 구현을 구성할 수 있습니다 다운로드 또는 이름 바꾸기 폴더 및 파일 작업은 파일 탐색기 작업 영역 구성 요소에서 활성화됩니다. 이러한 작업은 통합된 플로우 디자이너 하위 플로우를 사용하여 활성화되고 실행됩니다. 자세한 내용은 폴더 및 파일 작업 설정을 참조하십시오.

File Explorer 구성 에는 다음 설정이 포함됩니다.

- 파일 탐색기 리포지토리 드라이브 구성
- 폴더 및 파일 작업 설정 구성
- 폴더 템플릿 작성

파일 탐색기 시작하기

구성요소 작업을 File Explorer 시작하기 전에 다음 정보를 검토하십시오.

와의 Microsoft SharePoint연결 설정을 시작하기 전에 다음 정보를 검토하고, 폴더 및 파일 작업을 생성하고, 파일 탐색기 구성 요소에 대한 폴더 템플릿을 생성합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필수 구성요소

이름	설명
Microsoft SharePoint 스포크, 통합 허브용 ServiceNow# 버전 2.0.2.	**sn_sp_spoke** 플러그인 ID를 사용하여 스포크를 검색하고 설치합니다Microsoft SharePoint. 이 플러그인을 설치하면 에서 Microsoft SharePoint공동 작업, 문서 관리 및 사용자 액세스 권한을 자동화하는 플로우와 작업이 제공됩니다.
파일 탐색기 구성 요소 v1.1.0	**sn_file_explorer** 플러그인 ID를 사용하여 파일 탐색기 구성요소 v1.1.0 검색 및 설치 이 플러그인을 설치하면 파일 탐색기 코어에서 사용할 수 있는 파일 시스템을 찾아볼 수 있는 그래픽 사용자 인터페이스가 제공됩니다.
보안 운영용 파일 탐색기 코어 v1.1.1	**sn_fe** 플러그인 ID를 사용하여 파일 탐색기 코어를 검색하고 설치합니다. 이 플러그인을 설치하면 타사 파일 호스팅 제공자와 통합할 수 있는 기본 인프라가 제공됩니다.
Microsoft SharePoint 보안 운영용 파일 탐색기 커넥터 v1.1.1	**sn_fe_sharepoint** 플러그인 ID를 사용하여 파일 탐색기 커넥터를 검색하고 설치합니다Microsoft SharePoint. 이 플러그인을 설치하면 파일 탐색기를 Microsoft SharePoint 사용하여 파일/폴더가 관리됩니다.

파일 탐색기 리포지토리 드라이브 구성

커넥터는 Microsoft SharePoint 파일 메타데이터를 관리하고 추적하여 파일 탐색기 기능에서 Microsoft SharePoint 구현할 수 있는 다양한 기능을 제공합니다.

시작하기 전에
필요한 역할: sn_msi.workspace_admin

프로시저

1. 다음으로 이동 모두 〉 중요 보안 인시던트 〉 파일 탐색기 〉 파일 리포지토리 구성.
2. 다음 테이블에 설명된 대로 다음 필드를 채웁니다.

필드 이름	필드 설명
이름	사용량을 식별하는 파일 리포지토리 기록의 이름입니다. 예를 들어 MSIM입니다.
제공자	외부 공급업체 파일 호스팅 리포지토리 공급자인 공급자의 이름입니다. 예를 들어,Microsoft SharePoint.
속성	

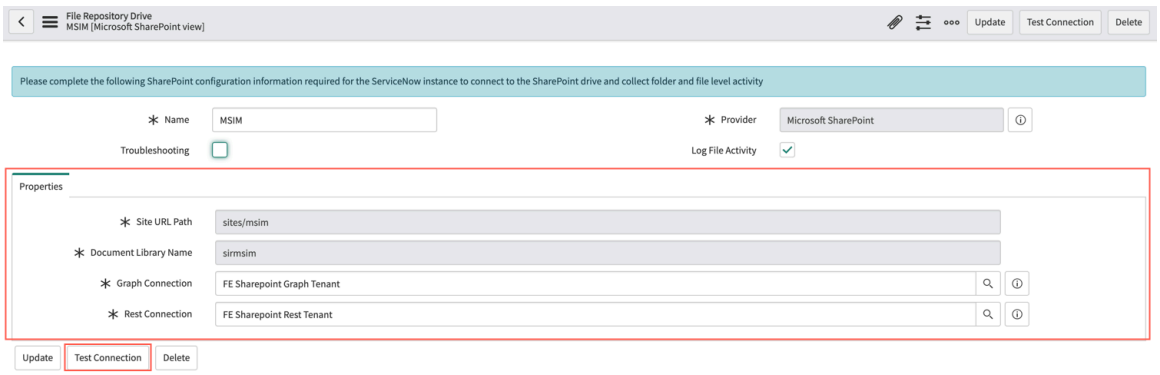
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드 이름	필드 설명
사이트 URL 경로	특정 사이트 경로가 있는 URL을 Microsoft SharePoint 입력합니다. 사이트에 대한 상대 경로만 제공합니다. 전체 사이트 URL은 필요하지 않을 수 있습니다. 예: Sites/MSIM.
문서 라이브러리 이름	사이트 아래에 Microsoft SharePoint 문서 라이브러리를 만들고 여기에 동일한 문서 라이브러리 이름을 제공합니다. 이는 커넥터 드라이브 설정에서 만든 것과 동일한 문서 라이브러리입니다 Microsoft SharePoint .
그래프 연결	파일 탐색기 Graph 테넌트 기록을 선택합니다. 테넌트 연결 구성에 대한 자세한 내용은 Microsoft SharePoint 스포크를 참조하세요.
REST 연결	파일 탐색기 REST 테넌트 기록을 선택합니다. 테넌트 연결 구성에 대한 자세한 내용은 Microsoft SharePoint 스포크를 참조하세요.

3. 저장을 선택합니다.
4. 클릭 연결 테스트 탭을 눌러 연결을 테스트하고 파일 리포지토리 드라이브 구성 속성의 유효성을 확인합니다.

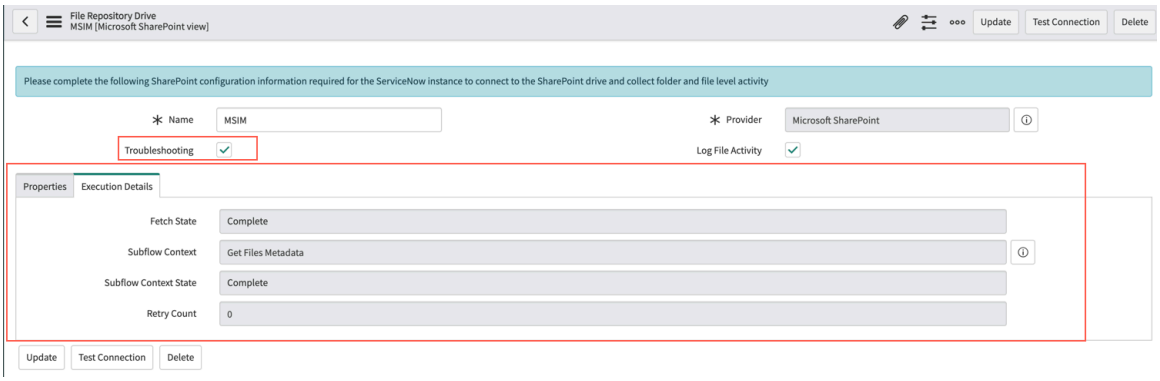
   주:
   파일 리포지토리를 활성화 하기 전에 의 Microsoft SharePoint 해당 문서 라이브러리에 폴더 또는 파일 데이터가 없는지 확인합니다.

5. 활성화를 클릭하여 파일 리포지토리를 활성화합니다.



6. 문제 해결 확인란을 선택하여 파일 리포지토리 실행 세부 정보를 확인하고 상태 가져오기 이(가) 완료되었으며 드라이브 구독이 Microsoft SharePoint 생성되고 상태가 완료인지 확인합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



주:
연결 테스트 단추를 사용하면 MSI 관리자 또는 MSI 관리자가 파일 리포지토리 구성의 유효성을 검사할 수만 있습니다.

폴더 및 파일 작업 설정 구성

폴더 및 파일 작업 설정 설정 페이지를 사용하여 Major Security Incident Management 작업 공간의 파일 탐색기 구성요소에서 활성화하려는 폴더 및 파일 작업을 파악 합니다. MSI 관리자는 파일 탐색기 구성 요소에 표시되는 개별 폴더 및 파일 작업을 제어할 수 있습니다.

시작하기 전에
다음은 플로우 디자이너를 사용하여 파일 탐색기 구성요소에 구현된 파일 작업 기능입니다.ServiceNow#

파일 운영 기능

파일 작업	설명
에서 열기 Microsoft SharePoint	새 브라우저 탭을 열어 문서 라이브러리 파일 뷰를 표시합니다 Microsoft SharePoint .
폴더 작성	중요 보안 인시던트가 생성된 후 추가 임시 폴더를 생성하는 기능
폴더 이름 변경	생성된 폴더의 이름을 바꿀 수 있습니다.
파일 이동	작업 공간의 파일 탐색기 구성 요소에있는 폴더간에 파일을 이동할 수 있으므로 파일을 이동할 수 있습니다. Microsoft SharePoint
파일 찾기	사용 시 폴더 위치를 표시합니다. 최근 항목 파일 탐색기 뷰.
파일 삭제	파일을 삭제합니다.
폴더 삭제	폴더를 삭제합니다.
파일 다운로드	빠른 보기를 위해 기존 MSIM 작업 공간 브라우저 탭 내에 파일을 다운로드합니다.
파일 이름 변경	파일 이름을 바꿉니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

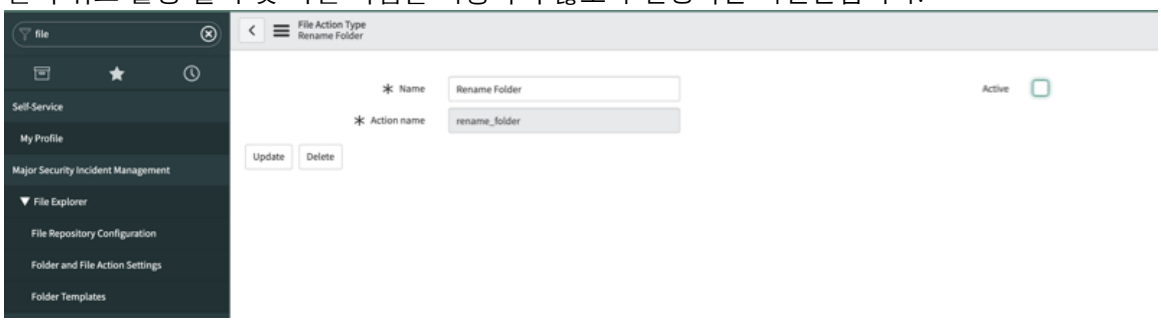
1. 나열된 모든 작업은 현재 기본적으로 활성화되어 있습니다. 다음을 편집해야 합니다. 파일 작업 설정 특정 작업이 표시되지 않도록 하려는 경우. 모든 설정은 현재 모든 사용자에 대해 전역이므로 특정 역할을 가진 사용자의 하위 집합에 대해 작업을 사용하도록 설정할 수 없습니다.
2. 사용자 접근 취소 및 권한 추가 작업은 시스템과 관련된 작업입니다. 이러한 파일 동작은 수정하지 않는 것이 좋습니다.

다음 샘플 절차 에서는 파일 탐색기 리포지토리를 구성하는 동안 특정 폴더 및 파일 작업을 사용하지 않도록 설정하는 파일 작업 기능 중 하나에 대해 설명합니다. 이 절차는 편집해야 할 수 있는 다른 모든 작업에 적용할 수 있습니다.

필요한 역할: sn_msi.workspace_admin

프로시저

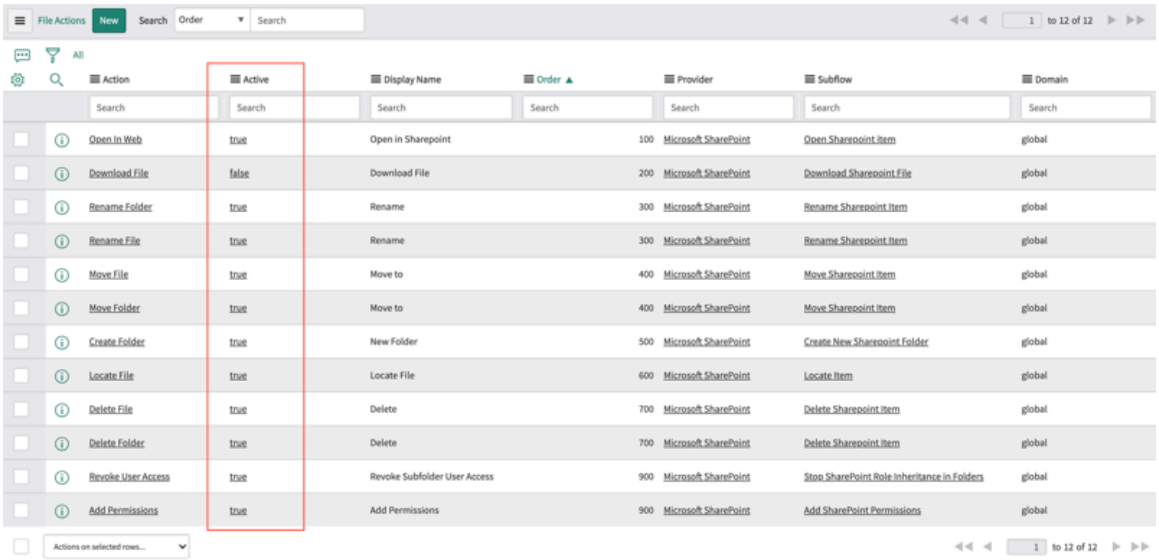
1. 다음으로 이동 중요 보안 인시던트 관리 〉 파일 탐색기 〉 폴더 및 파일 작업 설정.
2. 원하는 기록을 선택하여 폴더 또는 파일 작업을 각각 사용하거나 사용하지 않도록 설정합니다.
3. 선택 취소 활성 폴더 및 파일 작업을 사용하지 않도록 설정하는 확인란입니다.



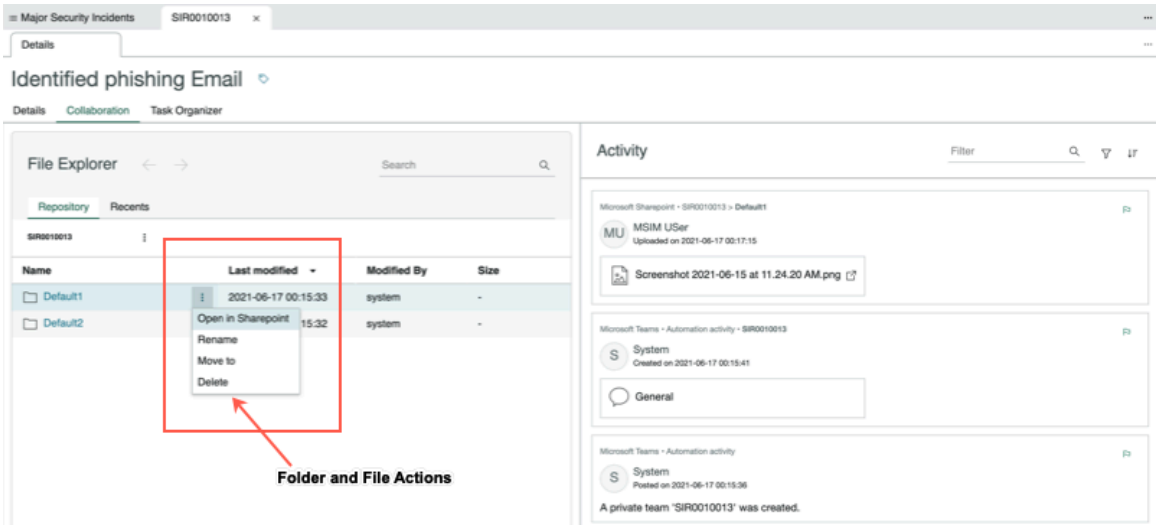
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 드라이브 기록을 업데이트합니다 .

주:
를 선택하여 표시된 파일 작업 목록에서 직접 파일 작업을 수행할 수도 있습니다. 활성 열 값을 True 또는 False로 설정합니다.



수행된 파일 작업이 비활성화된 경우 작업이 다음에 표시되지 않습니다. 공동 작업 탭의 중요 보안 인시던트 관리 작업.



폴더 템플릿 작성

폴더 템플릿을 사용하여 다양한 중요 보안 인시던트 유형에 대한 고유 폴더를 자동으로 생성합니다. 파일 탐색기 구성요소 내의 폴더 템플릿은 의 Microsoft SharePoint보안 인시던트에 대한 기본 폴더 구조를 만드는 데 사용됩니다.

시작하기 전에

MSI 관리자는 여러 인시던트 대응자 그룹 간에 공동 작업을 허용하는 데 필요한 초기 폴더 구조를 정의하고 하위 폴더 수준에서 적절한 액세스 권한을 할당합니다. 특정 중요 보안 인시던트 필드 값에 대한 조건 작성기를 사용하여 다양한 중요 보안 인시던트 유형에 대해 여러 구성을 생성할 수 있으며, 여기에는 각 하위 폴더 수준에서 서로 다른 사용자 및 사용자 그룹에 대한 액세스 허용이 포함됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
이러한 폴더 템플릿은 조건 작성기에 지정된 조건을 충족하는 모든 중요 보안 인시던트에서 사용됩니다. 인시던트 번호 또는 범주와 같은 인시던트 필드 변수를 사용하여 하나의 주요 보안 인시던트에 대한 공통 폴더 이름을 가진 하위 폴더 집합을 다른 주요 보안 인시던트의 일부인 이러한 이름의 유사한 폴더와 구분하는 고유한 루트 폴더 이름을 만드는 것이 좋습니다.

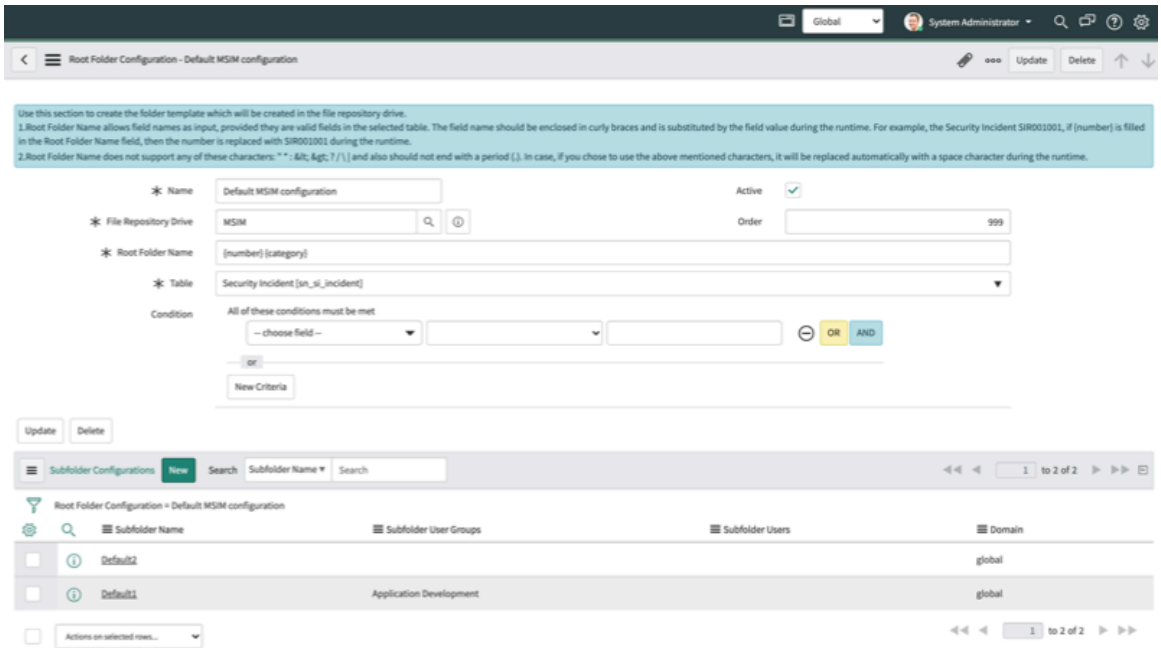
정의된 폴더 템플릿 구성은 조건이 일치하는 경우에만 중요 보안 인시던트에 적용됩니다.

주:
기본 시스템 구성(하위 폴더 없음)이 모든 보안 인시던트에 적용됩니다. 특정 하위 폴더를 포함하도록 이 기본 구성을 편집하거나 지정된 중요 보안 인시던트 필드 값 집합을 기반으로 새 구성을 만들 수 있습니다. 예를 들어 category = 악성 코드 활동입니다.

필요한 역할: sn_msi.workspace_admin

프로시저

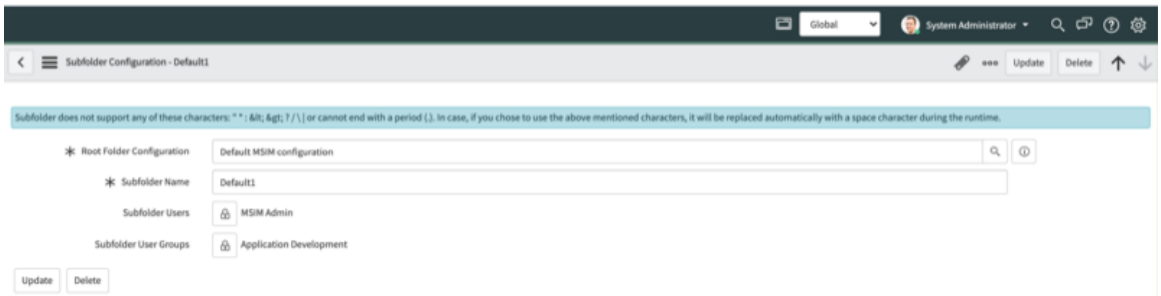
1. 다음으로 이동 모두 〉 중요 보안 인시던트 관리 〉 파일 탐색기 〉 폴더 템플릿.
2. 클릭 신규 루트 폴더 구성의 경우.
3. 양식에서 필드를 채웁니다.
4. 보안 인시던트 정의 조건 값.



5. 업데이트 기록.
   정의된 값으로 하위 폴더가 만들어집니다.
6. 원하는 하위 폴더를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

적절한 이름의 하위 폴더를 생성하지 않으면 하위 폴더 이름이 기본값 안에 하위 폴더 구성 절.

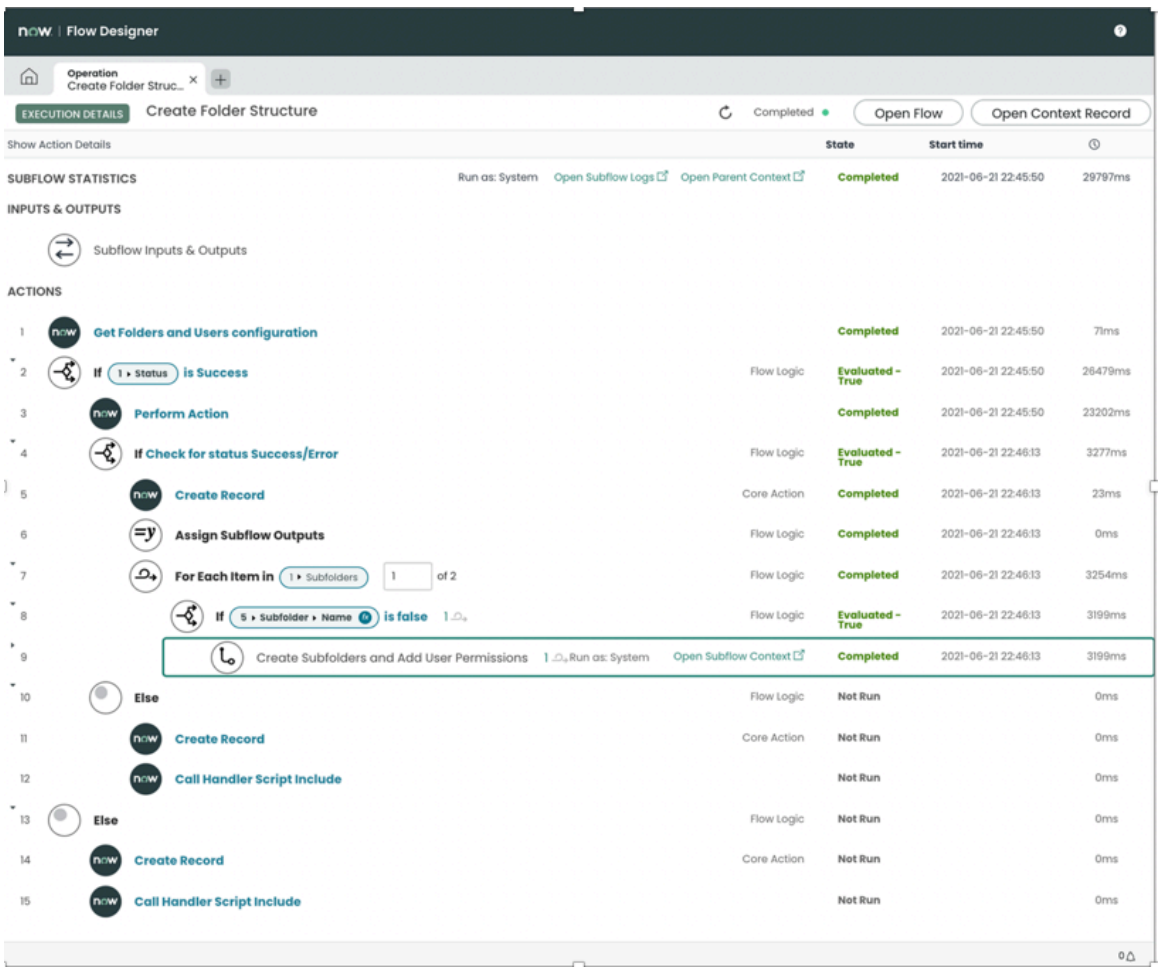


에서 구성된 것과 동일한 액세스 권한을 사용하여 동일한 폴더 구조가 자동으로 Microsoft SharePoint 생성됩니다. 폴더 템플릿 페이지.

주:

- 루트 폴더 이름은 선택한 테이블에서 유효한 필드인 경우 필드 변수 이름을 입력으로 허용합니다. 필드 이름은 중괄호로 묶어야 하며 플로우 실행 런타임 동안 필드 값으로 대체됩니다. 예를 들어, 보안 인시던트 SIR001001의 경우 루트 폴더 이름 필드에 {number} 변수가 구성된 경우 런타임 동안 숫자가 SIR001001로 대체됩니다.
- 루트 폴더 이름 은(는) 다음 문자를 지원하지 않습니다: " * : < > ? / \ | 또한 마침표(.)로 끝나지 않아야 합니다. 위에서 언급한 문자를 사용하면 런타임 중에 공백 문자로 자동 대체됩니다.
- 루트 폴더 및 하위 폴더 이름이 정의된 제한(256자)을 초과하면 폴더 이름이 잘립니다.

다음은 폴더 구조 작성 하위 플로우의 실행 시간입니다.



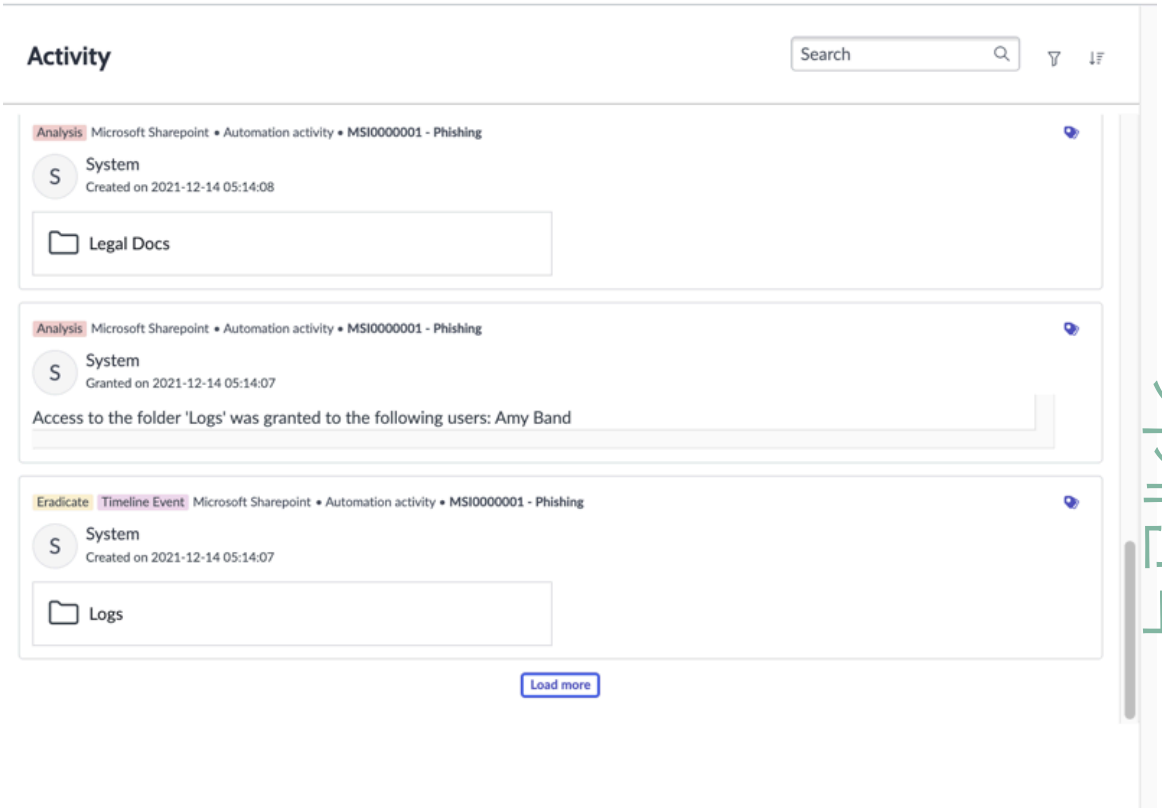
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

File Explorer 작업 공간의 활동 스트림

작업 공간의 파일 탐색기 섹션을 중요 보안 인시던트 관리 사용하여 문서 라이브러리에서 Microsoft SharePoint 생성된 폴더와 파일의 순서를 표시합니다.

활동 스트림에는 해결 중에 중요 보안 인시던트 발생하는 폴더와 파일 활동 또는 로그가 있을 때마다 모든 자동화 활동 게시물이 나열됩니다. 활동 스트림 구조는 생성된 폴더와 해당 폴더에 할당된 사용자 또는 사용자 그룹을 보여 주는 라이브러리와 Microsoft SharePoint 동일한 형식으로 정렬됩니다.

활동 스트림을 사용하면 작업 공간 관리자와 다른 사용자 또는 사용자 그룹이 효과적으로 통신 및 협업하고, 폴더 및 파일에서 수행된 Microsoft SharePoint 활동을 나열하고, 인시던트 상태를 모니터링하고, 메모를 게시하고, 인시던트 기록에 대한 추가 코멘트를 추가할 수 있습니다. 작업 공간 관리자는 마지막으로 업데이트된 활동을 선택하여 작업할 수



있습니다.

File Explorer 문제 해결

문제 해결 섹션은 구성요소를 설정할 File Explorer 때 발생할 수 있는 몇 가지 기술적 문제를 해결하는 데 도움이 될 수 있습니다.

예약된 작업, 시스템 속성 및 File Explorer Flow Designer 하위 플로우에 대한 자세한 내용은 다음 섹션을 참조하십시오.

다음에 대해 예약된 작업 **File Explorer**

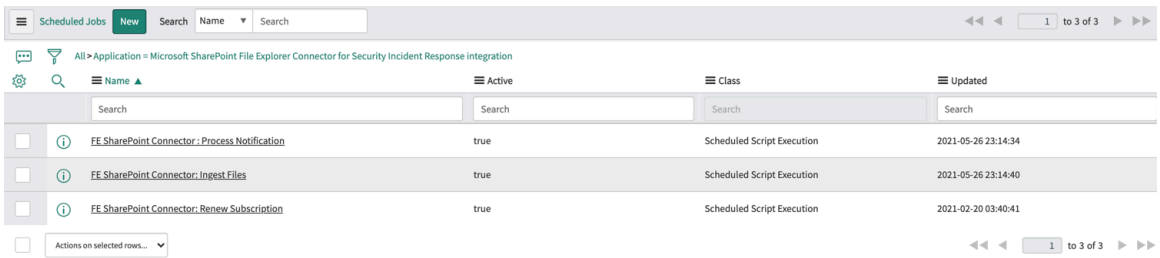
예약된 작업은 에서 Microsoft SharePoint알림을 처리하고, 파일 메타데이터를 인스턴스로 ServiceNow 수집하고, 반복 일정에 따라 파일 리포지토리 구독을 갱신하기 위해 실행되는 자동화된 작업입니다.

예약된 작업은 다음을 수행하기 위해 백그라운드에서 실행되는 자동화된 작업입니다.

- Microsoft Microsoft SharePoint의 알림을 처리합니다.
- 파일 메타데이터를 인스턴스로 ServiceNow AI Platform 수집합니다.
- 알림을 받으려면 문서 라이브러리로 Microsoft SharePoint 구독을 갱신하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업	설명
Microsoft SharePoint File Explorer 커넥터: 프로세스 알림	30초마다 실행되며 알림 읽기를 담당하여 구독한 문서 라이브러리에 변경 사항이 발생했음을 나타내고 드라이브 상태(sn_fe_file_repo_drive)를 보류 중으로 표시합니다.
Microsoft SharePoint File Explorer 커넥터: 파일 수집	30초마다 실행되며 보류 중인 상태인 드라이브(sn_fe_file_repo_drive)의 처리를 주로 담당하며 마지막 끌어오기 이후 구성된 Microsoft SharePoint 문서 라이브러리에서 델타 파일 변경 내용을 가져옵니다.
Microsoft SharePoint File Explorer: 구독 갱신	10분마다 실행되며 만료 날짜 하루 전에 문서 라이브러리 구독을 갱신 Microsoft SharePoint 합니다. 일반적으로 이러한 구독은 30일 후에 만료됩니다.



사용 가능한 파일 탐색기 시스템 속성

다음은 사용 가능한 Microsoft SharePoint 파일 탐색기 커넥터 시스템 속성입니다.

시스템 속성

속성 이름	설명
sn_fe_sharepoint.max_retry_count	커넥터 응용 프로그램이 실패한 드라이브를 끌어오거나 실패한 구독을 갱신하려고 시도하는 Microsoft SharePoint 빈도를 제어합니다. 기본 빈도 값은 50으로 설정됩니다.
sn_fe_sharepoint.retry_after_seconds	실패한 드라이브를 끌어오거나 구독을 갱신하려는 각 시도 사이의 시간 간격입니다. 기본값은 900초 또는 15분으로 설정됩니다.
sn_fe_sharepoint.max_subscription_expiration_time	의 Microsoft SharePoint최대 구독 만료 기간(일 수)입니다. 기본 만료 기간은 30일로 설정됩니다.

File Explorer Flow Designer 하위 플로우

다음은 커넥터와 함께 Microsoft SharePoint File Explorer 설치되는 플로우 디자이너 하위 플로우입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

하위 플로우

이름	설명
권한 추가 Microsoft SharePoint	특정 사용자에게 특정 폴더에 대한 편집 권한을 부여합니다.
드라이브 구독 작성	문서 라이브러리에서 발생하는 업데이트에 대한 알림을 받기 위해 구성된 Microsoft SharePoint 문서 라이브러리를 구독합니다.
새 Microsoft SharePoint 폴더 작성	지정된 상위 폴더 아래에 새 Microsoft SharePoint 폴더를 작성합니다.
항목 삭제 Microsoft SharePoint	파일 및 폴더를 삭제합니다 Microsoft SharePoint .
파일 다운로드 Microsoft SharePoint	파일의 다운로드 URL을 Microsoft SharePoint 반환합니다.
파일 메타데이터 가져오기	문서 라이브러리를 구독하고 변경 사항을 Microsoft SharePoint 가져옵니다.
항목 이동 Microsoft SharePoint	파일/폴더를 대상 폴더로 이동합니다 Microsoft SharePoint .
오픈 Microsoft SharePoint 항목	브라우저에서 열 파일/폴더의 웹 URL Microsoft SharePoint 을 반환합니다.
드라이브 구독 갱신	문서 라이브러리로 Microsoft SharePoint 구독을 갱신합니다.
폴더 구조 작성	폴더 템플릿 구성을 따르고 문서 라이브러리에 폴더 구조를 Microsoft SharePoint 작성합니다.

Microsoft Teams 구성

채팅을 통한 통신을 해결하는 데 도움이 되는 것을 구성합니다 중요 보안 인시던트 관리중요 보안 인시던트.Microsoft Teams

채팅 환경을 구성 및 구독 Microsoft Teams 하고, 지정된 채널에서 채팅 대화를 검색하고, 팀 및 관련 채널을 보관하는 것은 인시던트 종결 프로세스의 일부로 포함됩니다. 에 특정한 중요 보안 인시던트개별 채널을 만들려면 지정된 Microsoft Teams 환경 및 관련 Microsoft Teams Graph API 구성이 필요합니다.

Microsoft Teams를 구성하려면 Teams를 채팅 공급자로 활성화합니다. 그런 다음 활동에 대해 통신하는 다양한 이해 관계자 및 그룹을 위한 채팅 채널을 생성하고 채팅 대화를 추적하여 문제를 해결할 수 있습니다 중요 보안 인시던트. Microsoft Teams 및 Microsoft Graph API 구성에는 다음이 포함됩니다.

- 에서 MS Teams 그래프 연결 설정 ServiceNow AI Platform
- MS Teams를 채팅 공급자로 활성화
- 채팅 채널 템플릿 생성
- 채팅 메시지 활동 보기

Microsoft Teams 시작하기

커넥터 애플리케이션으로 작업을 Microsoft Teams 시작하기 전에 다음 정보를 검토합니다.

연결 설정, 활성화 및 검증 Microsoft Teams 을 시작하기 전에 다음 플러그인이 설치되어 있는지 확인하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필요 플러그인

이름	설명
보안 인시던트 관리와 채팅 통합	**sn_chat_collab_core** 플러그인 ID를 사용하여 Chat을 검색하고 설치합니다Microsoft Teams. 이 플러그인을 설치하면 Microsoft Teams(또는 Slack 및 기타 외부 공급업체 채팅 애플리케이션)와 같은 외부 공급업체 애플리케이션에 대한 채팅 활동을 추적할 수 있습니다.
보안 인시던트 관리용 Microsoft Teams 채팅 커넥터	**sn_ms_teams_connector** 플러그인 ID를 사용하여 Major Security 인시던트 관리용 Microsoft Teams 채팅 커넥터를 검색하고 설치합니다. 이 플러그인을 설치하면 에 특정한 공동 작업 구성 요소를 사용하여 채팅 활동을 추적할 수 있습니다 Microsoft Teams.
Microsoft Teams 그래프 스포크	이 플러그인을 설치하면 그래프 스포크 연결이 Microsoft Teams설정됩니다. 자세한 내용은 Microsoft Teams Graph 스포크를 참조하십시오.

MS Teams를 채팅 공급자로 활성화

연결을 확인하여 Microsoft Teams 활성화합니다Microsoft Teams.

시작하기 전에
필요한 역할: sn_msi.workspace_admin

연결이 활성화되고 유효성이 검사되면 제공자 연결의 유효성이 성공적으로 확인되었다는 정보 메시지가 표시됩니다. 사용자를 추가 및 제거하고 채널을 더 추가하거나 기존 채널의 이름을 변경하여 채널 구성을 수정할 수 있습니다.

프로시저

1. 다음으로 이동 중요 보안 인시던트 관리 〉 채팅 공급자 구성.
2. **Microsoft Teams** 기록을 선택합니다.
3. 연결 확인을 클릭합니다.
   제공자 연결의 유효성이 성공적으로 확인되었다는 확인 메시지가 표시됩니다.
4. 제공자 기록을 활성화하려면 활성 확인란을 선택합니다.
   제공자 연결의 유효성이 성공적으로 확인되었다는 확인 메시지가 표시됩니다.
5. 채팅 제공자 구성을 활성화한 후 양식을 저장합니다.
   이 연결을 통해 Microsoft Teams와 ServiceNow AI Platform 인스턴스 간의 연결이 성공적으로 설정되었습니다.

채팅 채널 템플릿 생성

채팅 팀 및 채널 템플릿을 구성하여 공동 작업할 채팅 팀 및 채널을 만들고, 채팅 대화를 추적하고, 해당 채팅 채널에 사용자 및 사용자 그룹을 추가합니다. 이러한 채널 템플릿은 중요 보안 인시던트가 승격될 때 Microsoft Teams에 만들어집니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_msi.workspace_admin

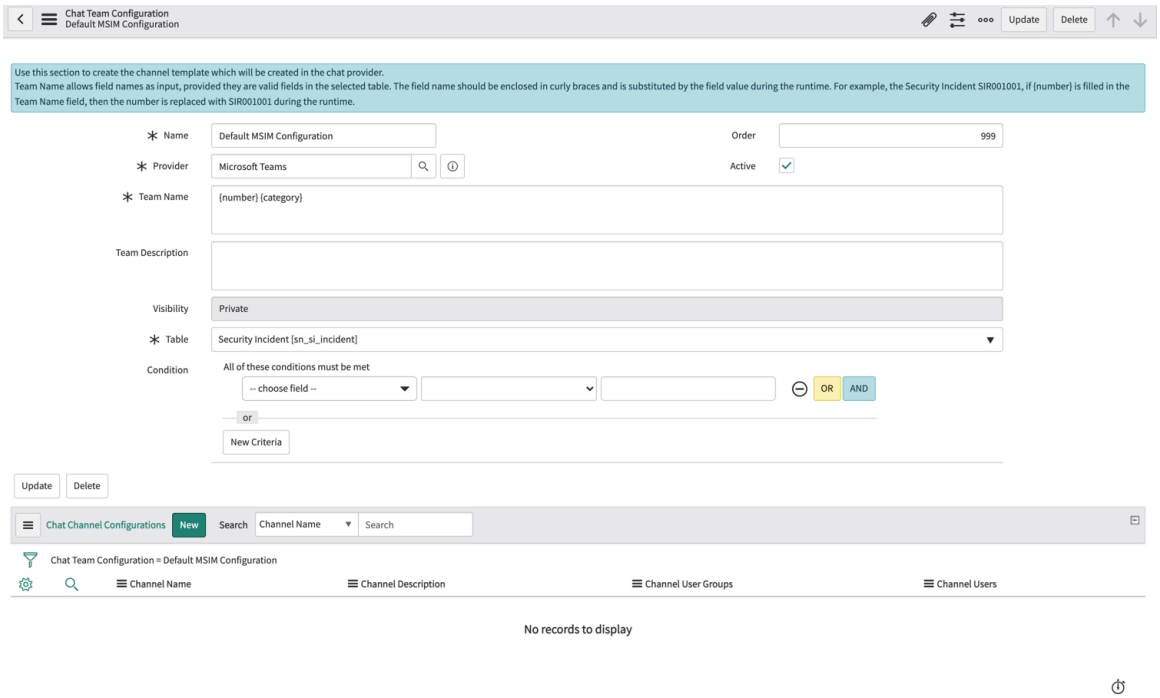
프로시저

1. 다음으로 이동 중요 보안 인시던트 관리 〉 채팅 채널 〉 채널 템플릿.
2. 채팅 채널 구성 양식의 양식 헤더에서 신규 를 클릭합니다.
3. 양식에서 필드를 채웁니다.

채팅 팀 구성 양식

필드	설명
이름	폴더의 이름입니다.
제공자	Microsoft 팀즈.
팀 이름	팀의 이름입니다(예: {number}-{category} 형식). 주: 여기에 제공된 팀 이름은 모든 중요 보안 인시던트 기록에 사용됩니다. 실제 Microsoft 팀 이름이 MS Teams 애플리케이션에 표시되고 여러 중요 보안 인시던트에 대한 고유한 이름 값을 가지도록 하려면 인시던트 번호 - {number}와 같은 고유한 인시던트 필드 값을 사용하는 것이 좋습니다. 스크린샷 예와 같이 {number} 다음에 구분 기호 '-'와 {category} 필드 변수가 오면 Microsoft Teams가 생성되는 중요 보안 인시던트에 대한 고유 번호와 설명이 제공됩니다(예: {number} - {category}).
팀 설명	팀에 대한 선택적 설명입니다.
테이블	sn_msi_incident(중요 보안 인시던트)

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



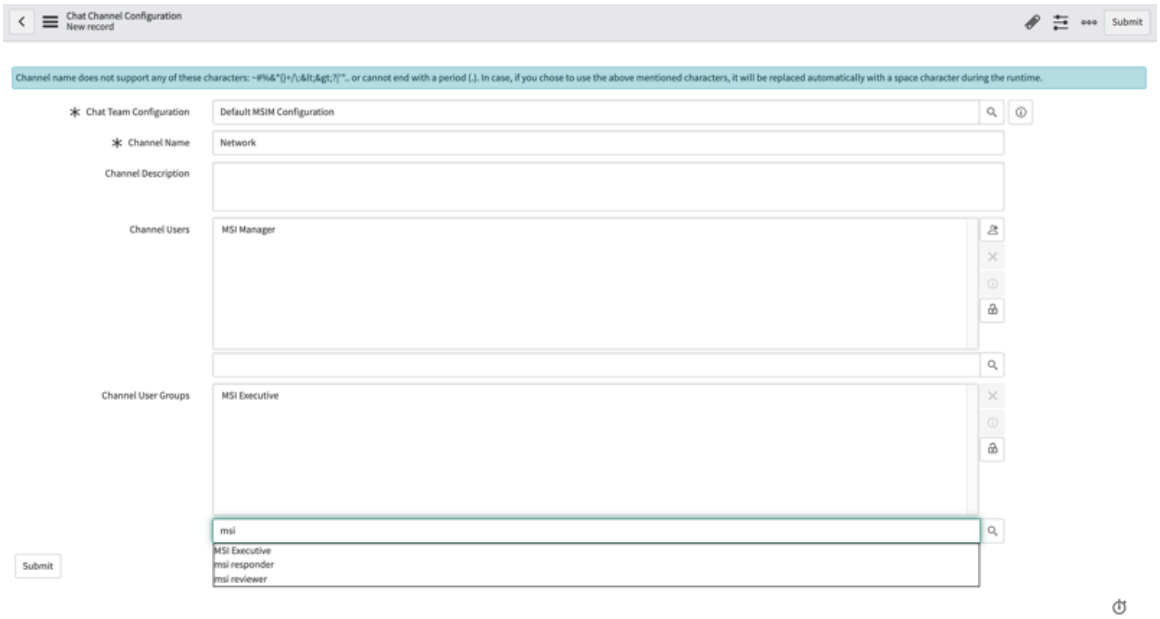
4. 제출을 클릭합니다.
5. 채팅 채널 구성 섹션으로 이동합니다.
6. 클릭 신규 새 채팅 채널 구성을 생성합니다.
7. 다음을 입력하십시오. 채팅 팀 구성 및 채널 이름.

   주:
   여기에서 만든 새 채널은 Microsoft Teams에서도 채널 이름이 됩니다. 동일한 채널을 검색하고 대화를 추가할 수 있습니다.

8. 추가 채널 사용자 및 채널 사용자 그룹 목록 조회에서.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

9. 제출 새 채팅 채널 구성 기록입니다.



결과
이제 채팅 채널이 생성되고 사용자가 해당 채팅 채널 그룹에 할당됩니다. 채팅 채널 제공자 구성에 구성된 대로 구성된 채팅 채널 계층 구조를 사용하여 MSIM 작업 공간의 공동 작업 활동 스트림과 Microsoft Teams 공동 작업 활동 스트림 모두에서 공동 작업 채팅 활동을 볼 수 있습니다.

채팅 메시지 활동 보기

채팅 메시지 활동이 기록되고 Major Security Incident Management 작업 공간의 공동 작업 탭에 표시됩니다.

채팅 메시지 활동에는 참가자와 다른 사용자 그룹 간에 발생한 모든 채팅 대화가 포함됩니다.

MSIM에 대한 **MS Teams** 채팅 커넥터 문제 해결

예약된 작업, 시스템 속성, Microsoft Teams 플로우 디자이너 하위 플로우에 대한 내용은 Microsoft Teams 채팅 커넥터 문제 해결 섹션을 참조하십시오.

공동 작업 채팅 메시지가 Microsoft 팀 및 MSIM 작업 영역의 외부 공동 작업 활동 스트림에 게시되지 않는 경우 어떤 경우에도 채팅 커넥터 프로세스 예약된 작업을 확인합니다.

에 대한 예약된 작업 **Microsoft Teams**

예약된 작업은 채팅 커넥터의 Microsoft Teams 알림을 처리하고 되풀이 일정에 따라 Microsoft Teams 구독을 갱신하기 위해 실행되는 자동화된 작업입니다.

필요한 역할: admin.

- **MS Teams** 채팅 커넥터: 프로세스 알림

  각 채팅 메시지 이벤트에 대해 리소스 ID와 테이블에 저장된 알림이 있는 알림이 수신됩니다. 처리되지 않은 알림을 선택하고 Microsoft Teams API를 쿼리하여 다른 테이블에 추가로 저장되는 실제 메시지 내용을 가져오기 위해 예약 작업이 30초마다 실행됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- **MS Teams** 채팅 커넥터: 구독 갱신

  팀 내의 각 채널에 대해 생성, 업데이트 및 삭제된 이벤트에 대한 알림을 받기 위한 구독이 생성됩니다. 이 구독은 60분 동안만 활성화됩니다. 구독은 Microsoft Teams 커넥터: 알림 갱신 일정 작업을 통해 25분마다 갱신됩니다.

Microsoft Teams 채팅 커넥터 기능 플로우

이 섹션을 보고 주요 보안 인시던트에서 Microsoft Teams 채팅 채널 생성 및 사용자 액세스를 관리하는 데 사용되는 관련 Flow Designer 하위 플로우를 이해합니다.

시작하기 전에

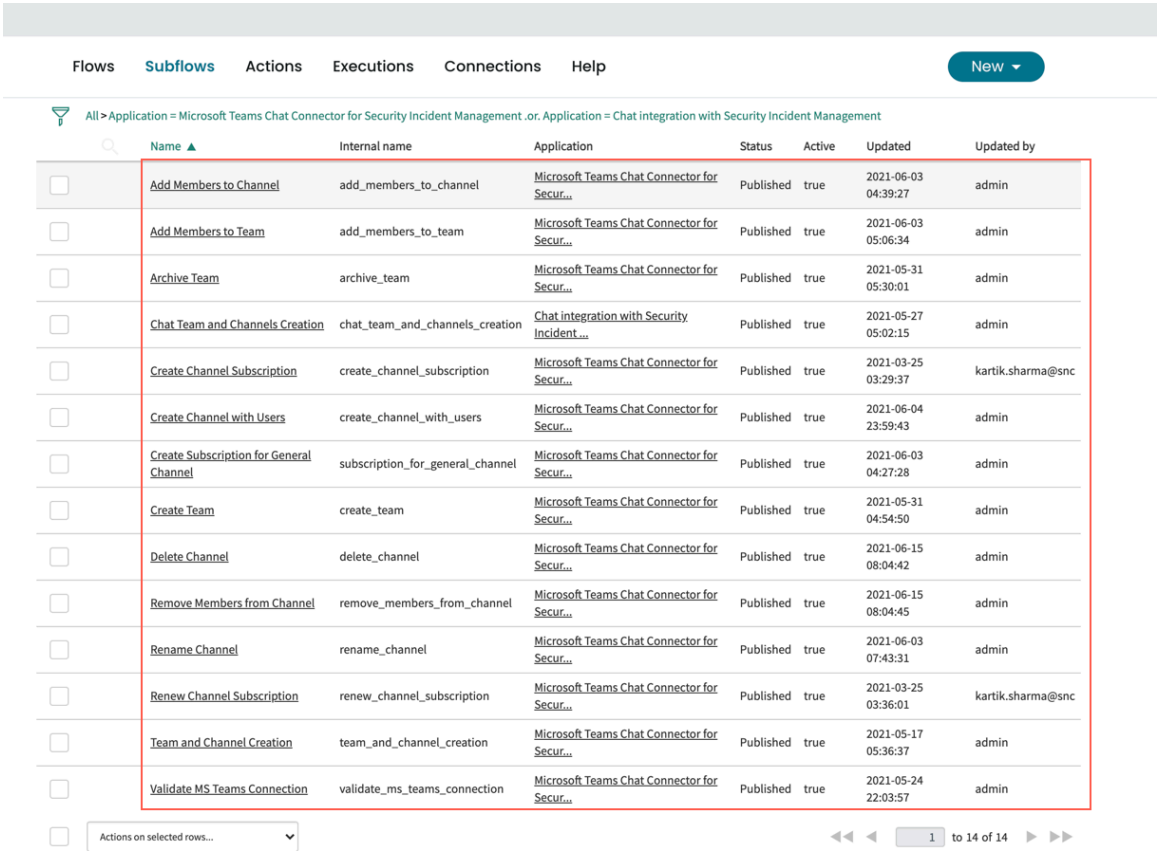
필요한 역할: sn_msi.workspace_admin

프로시저

1. 다음으로 이동 모두 〉 플로우 디자이너.
2. 채널에 구성원 추가
3. 팀에 구성원 추가
4. 팀 보관
5. 채팅 팀 및 채널 작성
6. 채널 구독 작성
7. 사용자와 채널 생성
8. 일반 채널에 대한 구독 작성
9. 팀 작성
10. 채널 삭제
11. 채널에서 구성원 제거
12. 채널 이름 변경
13. 채널 구독 갱신
14. 팀 및 채널 작성

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

15. MS Teams 연결 확인



중요 보안 인시던트에 대한 **Slack** 채팅 커넥터 구성

와 Slack 통합하고 협업하여 중요 보안 인시던트를 해결함으로써 공동 작업 채팅 활동을 확인하고 필터링합니다.

채팅 환경을 구성 및 구독 Slack 하고, 지정된 채널 내에서 채팅 대화를 검색하고, Slack 및 관련 채널을 보관하는 것은 인시던트 종결 프로세스의 일부로 포함됩니다. 에 특정한 중요 보안 인시던트개별 채널을 만들려면 지정된 Slack 환경 및 관련 Slack API 구성이 필요합니다.

Slack을 구성하려면 Slack을 채팅 공급자로 활성화합니다. 그런 다음 활동에 대해 통신하는 다양한 이해 관계자 및 그룹을 위한 채팅 채널을 생성하고 채팅 대화를 추적하여 문제를 해결할 수 있습니다 중요 보안 인시던트. 및 Slack API 구성에는 Slack 다음이 포함됩니다.

- Slack 채팅 커넥터 구성 시작하기
- Slack을 채널 공급자로 활성화
- Slack용 채팅 채널 템플릿 생성
- Slack에서 채팅 메시지 활동 보기

Slack 채팅 커넥터 구성 시작하기

커넥터 애플리케이션으로 작업을 Slack 시작하기 전에 다음 정보를 검토합니다.

연결 설정, 활성화 및 검증 Slack 을 시작하기 전에 다음 플러그인이 설치되어 있는지 확인하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필요 플러그인

이름	설명
Slack 보안 인시던트 관리용 채팅 커넥터	**sn_slack_connector** 플러그인 ID를 사용하여 Major Security Incident Management용 커넥터를 검색하고 설치합니다Slack. 이 플러그인을 설치하면 에 특정한 공동 작업 구성 요소를 사용하여 채팅 활동을 추적할 수 있습니다 Slack.
Slack 스포크	이 플러그인을 설치하면 .Slack 자세한 내용은 Slack Spoke 문서를 참조하십시오.

Slack용 채팅 채널 템플릿 생성

채팅 팀 및 채널 템플릿을 구성하여 공동 작업할 채팅 팀 및 채널을 만들고, 채팅 대화를 추적하고, 해당 채팅 채널에 사용자 및 사용자 그룹을 추가합니다. 이러한 채널 템플릿은 중요 보안 인시던트가 승격될 때 생성됩니다 Slack .

시작하기 전에

필요한 역할: sn_msi.workspace_admin

이 태스크 정보

새로 만든 채널도 채널 이름이 Slack 됩니다. 동일한 채널을 검색하고 대화를 추가할 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 중요 보안 인시던트 관리 〉 채팅 채널 〉 채널 템플릿.
2. Slack 구성 상세 정보를 보려면 **Slack** 채널 구성을 선택합니다.
3. Slack 채팅 채널 구성을 활성화하려면 활성 확인란을 선택합니다.
4. 팀 이름 필드에 MSI 번호와 코드 이름을 입력합니다.

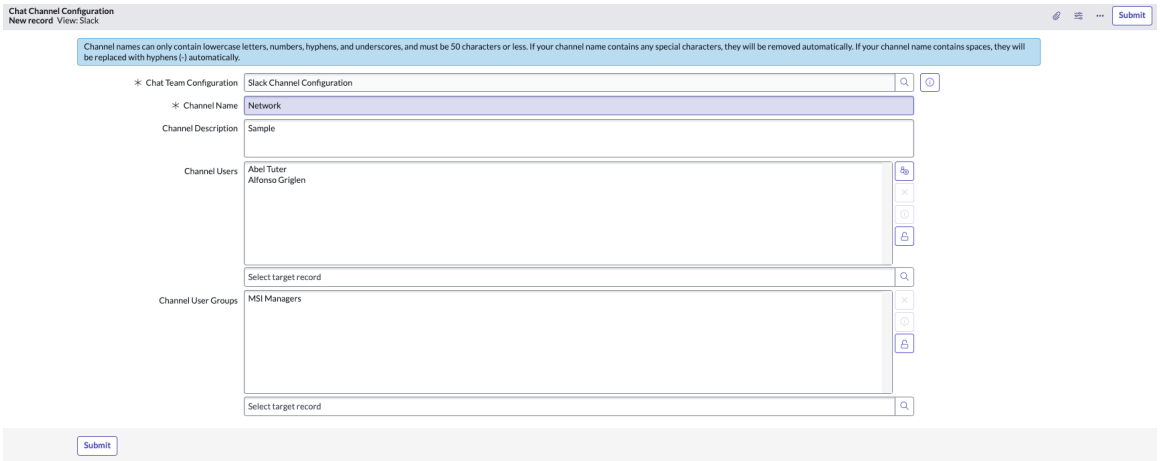
   기본적으로 모든 Slack 채널에는 인시던트 번호가 프리픽스로 표시됩니다. 예: `MSI000000 - {## ##}`. 프리픽스를 {field_name} 형식으로 원하는 필드로 변경할 수 있습니다.

   > **주:**
   > 여기에 제공된 팀 이름은 모든 중요 보안 인시던트 기록에 사용됩니다. 실제 Slack 값이 애플리케이션에 표시되고 Slack 다른 중요 보안 인시던트에 대한 고유한 이름 값을 갖는지 확인하려면 `MSI000000 - {## ##}`과 같은 고유한 인시던트 필드 값을 사용하는 것이 좋습니다.

5. 구성을 마우스 오른쪽 버튼으로 클릭하고 저장을 선택합니다.
6. 채팅 채널 구성 섹션으로 이동합니다.
7. 선택 신규 새 채팅 채널 구성을 생성합니다.
8. 양식에서 필드를 채웁니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Slack 채팅 채널 구성



9. 제출을 선택합니다.

결과
이제 채팅 채널이 생성되고 사용자가 해당 채팅 채널 그룹에 할당됩니다. 채팅 채널 제공자 구성에 구성된 대로 구성된 채팅 채널 계층 구조를 사용하여 MSIM 작업 공간의 공동 작업 활동 스트림과 Slack 공동 작업 활동 스트림 모두에서 공동 작업 채팅 활동을 볼 수 있습니다.

Slack을 채널 공급자로 활성화

연결을 확인하여 Slack 활성화합니다Slack.

시작하기 전에
필요한 역할:

- sn_msi.workspace_admin - 쓰기
- sn_msi.chat_collab_provider - 읽기

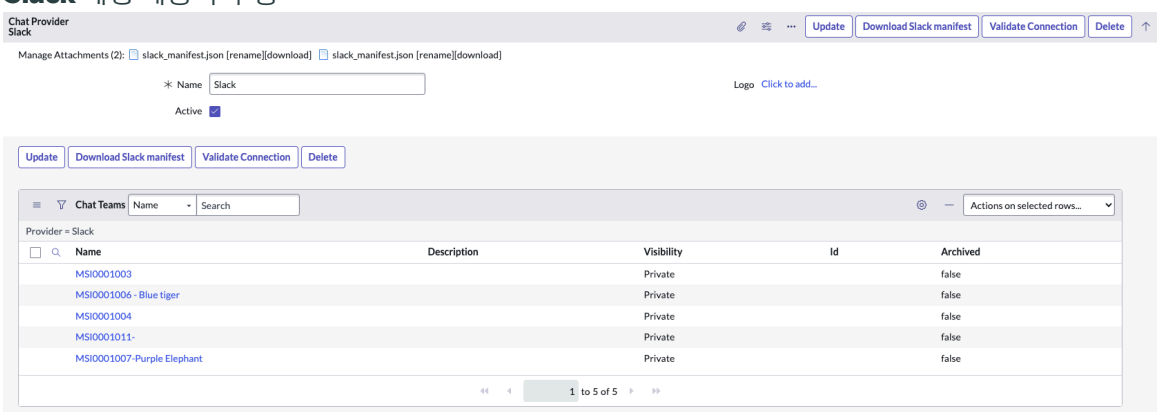
연결이 활성화되고 유효성이 검사되면 제공자 연결의 유효성이 성공적으로 확인되었다는 정보 메시지가 표시됩니다. 사용자를 추가 및 제거하고 채널을 더 추가하거나 기존 채널의 이름을 변경하여 채널 구성을 수정할 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 중요 보안 인시던트 관리 〉 채팅 채널 〉 채팅 공급자 구성.

2. Slack을 선택하여 Slack 채팅 제공자 구성을 엽니다.

Slack 채팅 제공자 구성



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. **Slack** 매니페스트 다운로드를 선택하여 slack_manifest.json 파일을 다운로드합니다.
   slack_manifest.json 파일에는 Slack 설정에 대한 전체 구성이 포함되어 있으며 Slack을 자동으로 구성할 수 있습니다. 이 JSON 파일을 Slack 구성에 업로드해야 합니다.
4. slack_manifest.json 파일을 열고 다음 단계를 수행합니다.

   a. 웹 브라우저에서 api.slack.com/apps URL로 이동합니다.

   b. 새 앱 작업 만들기를 선택합니다.

   c. 앱 만들기 팝업에서 앱 매니페스트에서**(From an app manifest**) 옵션을 선택합니다.

   d. 앱을 개발할 작업 영역 선택 팝업의 목록에서 작업 영역을 선택하고 다음을 선택합니다.
   예: MSIM Slack 작업 공간.

   e. 아래에 앱 매니페스트 입력 팝업에서 **JSON** 탭을 선택하고 slack_manifest.json 파일의 코드를 복사하여 붙여넣습니다.

   f. 다음을 선택합니다.

   g. 요약 검토 및 앱 만들기 팝업에서 만들기를 선택합니다.
   이제 앱이 생성되었습니다.

   h. 기본 정보 페이지에서 작업 영역에 설치를 선택합니다.
   Slack 통합 봇이 MSIM Slack 작업 공간에 액세스할 수 있는 권한을 요청합니다.

   i. 허용을 선택합니다.

   j. 앱 자격 증명 섹션에서 ServiceNow 인스턴스로 다시 이동하여 상세 정보를 입력합니다.

   k. 선택 모두 〉 **Slack** 구성.
   이 작업에는 sn_msi.workspace_admin 역할이 필요합니다.

   l. 서명 암호 속성을 선택합니다.

   m. 서명 비밀을 복사하여 Slack의 앱 자격 증명 섹션에 붙여넣습니다.

   n. ServiceNow 인스턴스에서 모두 〉 플로우 디자이너.

   o. 다음으로 이동 연결 〉 **Slack** 〉 상세 정보 보기 〉 구성.

   p. 양식에서 필드를 채웁니다.

필드	설명
연결 이름	이 연결의 이름입니다. 예: Slack.
연결 URL	이 연결의 URL입니다. 예: https://slack.com
자격 증명 이름	자격 증명의 이름입니다. 예를 들어 Slack 자격 증명입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
OAuth 이름	OAuth의 이름입니다. 예: Slack OAuth.
OAuth 클라이언트 ID	Slack에서 생성한 계정에 대해 생성된 클라이언트 ID입니다.
OAuth 클라이언트 비밀	Slack에서 생성한 계정의 클라이언트 암호입니다.
OAuth 리디렉션 URL	OAuth 리디렉션 인스턴스 이름입니다. 예: msimslack.service-now.com/oauth_redirect.do

q. **OAuth** 토큰 구성 및 가져오기를 선택합니다.
Slack 통합 봇이 MSIM Slack 작업 공간에 액세스할 수 있는 권한을 요청합니다.

r. 허용을 선택합니다.
OAuth 액세스 토큰을 사용할 수 있으며 〈YYYY-MM-DD〉〈HH:MM:SS〉에 만료됩니다.

5. 다음으로 이동 모두 〉 중요 보안 인시던트 관리 〉 채팅 채널 〉 채팅 공급자 구성.

6. 채팅 제공자 기록을 활성화하려면 활성 확인란을 선택합니다.

7. 연결 확인을 선택하여 연결을 테스트합니다.
제공자 연결의 유효성이 성공적으로 확인되었다는 확인 메시지가 표시됩니다.

8. 기록을 마우스 오른쪽 버튼으로 클릭하고 저장을 선택합니다.
이후 Slack과 ServiceNow AI Platform 인스턴스 간의 연결이 성공적으로 설정됩니다.

9. 다음으로 이동 **api.slack.com/apps** 〉 기능 〉 **OAuth** 및 권한.

a. 모든 범위가 올바른지 확인합니다.

b. 다음으로 이동 기능 〉 이벤트 구독.

c. 요청 URL 필드에서 재시도를 선택합니다.
확인된 메시지를 볼 수 있습니다.

d. 저장을 선택합니다.

Slack에서 채팅 메시지 활동 보기

채팅 메시지 활동이 기록되고 Major Security Incident Management 작업 공간의 공동 작업 탭에 표시됩니다.

시작하기 전에
필요한 역할: sn_msi.workspace_admin

이 태스크 정보
채팅 메시지 활동에는 참가자와 다른 사용자 그룹 간에 발생한 모든 채팅 대화가 포함됩니다. 자세한 내용은 Slack을 사용하여 채팅 채널 커뮤니케이션 관리 문서를 참조하십시오.

중요 보안 인시던트 관리 관리

중요 보안 인시던트 관리 구현을 계획하고 구성합니다.

다음과 같은 중요 보안 인시던트 관리 관리 측면을 구성할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

중요 보안 인시던트의 제안, 프로모션 및 연결 지원

사용자가 인시던트를 중요 보안 인시던트로 제안하거나 승격할지 결정할 수 있도록 합니다. 보안 인시던트를 상위 또는 하위 인시던트에 연결할 수 있도록 하여 중요 보안 인시던트와 관련된 모든 인시던트를 쉽게 추적합니다.

시작하기 전에
필요한 역할: sn_msi.workspace_admin

프로시저

1. 다음으로 이동 모두 〉 중요 보안 인시던트 관리 〉 **MSI** 관리 〉 구성.
2. SIR/VR 작업 공간 작업 섹션에서 중요 보안 인시던트 제안 확인란을 선택하여 사용자가 중요 보안 인시던트에 보안 인시던트를 제안할 수 있도록 합니다.
3. 사용자가 중요 보안 인시던트로 승격 확인란을 선택하여 보안 인시던트를 중요 보안 인시던트로 승격할 수 있도록 합니다.
4. 중요 보안 인시던트에 연결 확인란을 선택하여 보안 인시던트를 중요 보안 인시던트와 연결하여 함께 추적할 수 있도록 합니다.
5. 업데이트를 선택합니다.

보안 인시던트를 중요 보안 인시던트로 태그 지정

인시던트가 제안되거나 승격될 때 보안 인시던트 또는 취약한 기록에 태그를 지정하거나 중요 보안 인시던트에 레이블을 지정합니다. 보안 인시던트가 제안되면 인시던트 기록을 중요 보안 인시던트 후보라고 합니다. 보안이 승격되면 인시던트 기록이 중요 보안 인시던트라고 하며 상태가 수용됨이라고 합니다.

시작하기 전에
필요한 역할: sn_msi.workspace_admin

프로시저

1. 다음으로 이동 모두 〉 중요 보안 인시던트 관리 〉 **MSI** 관리 〉 구성.
2. 레이블 표시 확인란을 활성화하여 제안된 인시던트 후보를 레이블 이름 **-** 후보로 제안 조회 필드를 선택하고 **SIR/VR** 작업 공간 레이블 섹션에서 중요 보안 인시던트 후보를 선택합니다.
3. 레이블 표시 확인란을 활성화하여 승격된 인시던트 후보를 중요 보안 인시던트로 레이블을 지정하려면 레이블 이름 **-** 중요 보안 인시던트로 승격 조회 필드를 선택하고 **SIR/VR** 작업 공간 레이블 섹션에서 중요 보안 인시던트를 선택합니다.
4. 업데이트를 선택합니다.

중요 보안 인시던트에 대한 레이블 구성

사용자 지정 레이블을 생성하고 활동 스트림에서 외부 공동 작업 활동 및 작업을 필터링하도록 Major Security Incident Management에서 레이블을 구성합니다. 구현된 레이블의 다양한 유형은 상태 레이블과 타임라인 레이블입니다.

시작하기 전에
필요한 역할: sn_msi.workspace_admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 중요 보안 인시던트 관리 〉 **MSI** 관리 〉 구성.
2. 레이블 표시 확인란을 활성화하여 **MSIM** 작업 공간 레이블(공동 작업 활동 및 작업에 표시) 섹션에서 분석, 포함, 근절, 복구, 검토, 타임라인 이벤트 등 다양한 인시던트 상태에 레이블을 지정할 수 있습니다.
3. 업데이트를 선택합니다.

중요 보안 인시던트에 대한 레이블 구성

인시던트 상태를 더 잘 필터링하고 표시할 수 있도록 다양한 유형의 레이블을 구성합니다. 중요 보안 인시던트 레이블은 인시던트 기록의 공동 작업 활동 및 작업에 레이블을 지정할 수 있는 유연성을 제공합니다.

시작하기 전에
필요한 역할: sn_msi.workspace_admin

MSIM 작업 공간의 공동 작업 및 작업 관리자 섹션에 있는 활동 스트림 섹션에서 사용할 수 있는 레이블 아이콘을 사용하여 레이블을 선택하거나 선택 취소할 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 중요 보안 인시던트 관리 〉 **MSI** 관리 〉 **MSI** 레이블.
2. 새로 만들기를 클릭하여 새 레이블을 만듭니다.
3. 레이블 이름 및 레이블 색으로 폼을 채웁니다.
4. 레이블 만들기를 클릭합니다.
5. 다음은 기본 시스템의 일부로 각 인시던트 상태에 대해 구성된 레이블이며 레이블 이름이나 색상은 수정할 수 없습니다.
   - 분석
   - 포함
   - 근절
   - 검토
   - 복구
   - 타임라인 이벤트

   주:
   사용자 지정 레이블과 해당 속성을 수정할 수 있습니다.

중요 보안 인시던트에 대한 타임라인 범주 구성

개요 탭의 타임라인 섹션을 사용하여 주요 보안 인시던트에 위협, 응답 또는 사용자 지정과 같은 타임라인 범주를 구성하고 할당합니다.

시작하기 전에
필요한 역할: sn_msi.workspace_admin

프로시저

1. 다음으로 이동 모두 〉 중요 보안 인시던트 관리 〉 **MSI** 관리 〉 타임라인 범주.
   기본 시스템의 일부로 제공되는 타임라인 범주는 다음과 같습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 사용자 지정.
- 응답.
- 위협.

2. 기존 타임라인 이벤트 범주를 수정하려면 다음 단계를 수행합니다.
   a. 목록에서 타임라인 이벤트 범주를 선택합니다.
   b. 타임라인 이벤트 범주의 이름을 수정할 수 있습니다.
   c. 이벤트 색상을 수정하고 타임라인 이벤트 범주에 대해 다른 색상을 선택할 수 있습니다.
   d. 업데이트를 선택합니다.
3. 새 타임라인 이벤트 범주를 만들려면 다음 단계를 수행합니다.
   a. 새로 만들기를 선택합니다.
   b. 이름 필드에 타임라인 이벤트 범주의 이름을 입력합니다.
   c. 이벤트 색상 필드에서 드롭다운 목록을 사용하여 이벤트 타임라인 범주의 색상을 선택합니다.
   d. 제출을 선택합니다.

다음에 대한 알림 기본 설정 지정 **MSIM**

이메일 알림 프로세스를 자동화하고 보안 인시던트가 제안되거나 중요 보안 인시던트 후보로 승격될 때 사용자에게 알립니다.

필요한 역할: sn_msi.workspace_admin.

알림은 보안 인시던트가 제안되고 알림 목록에 구성된 모든 사용자와 그룹에 전송되는 경우에만 트리거됩니다. 기본적으로 이메일 알림은 보안 인시던트를 중요 보안 인시던트 후보로 제안한 사용자가 수신합니다.

알림: 보안 인시던트 제안됨(SI)을 MSI(중요 보안 인시던트)로

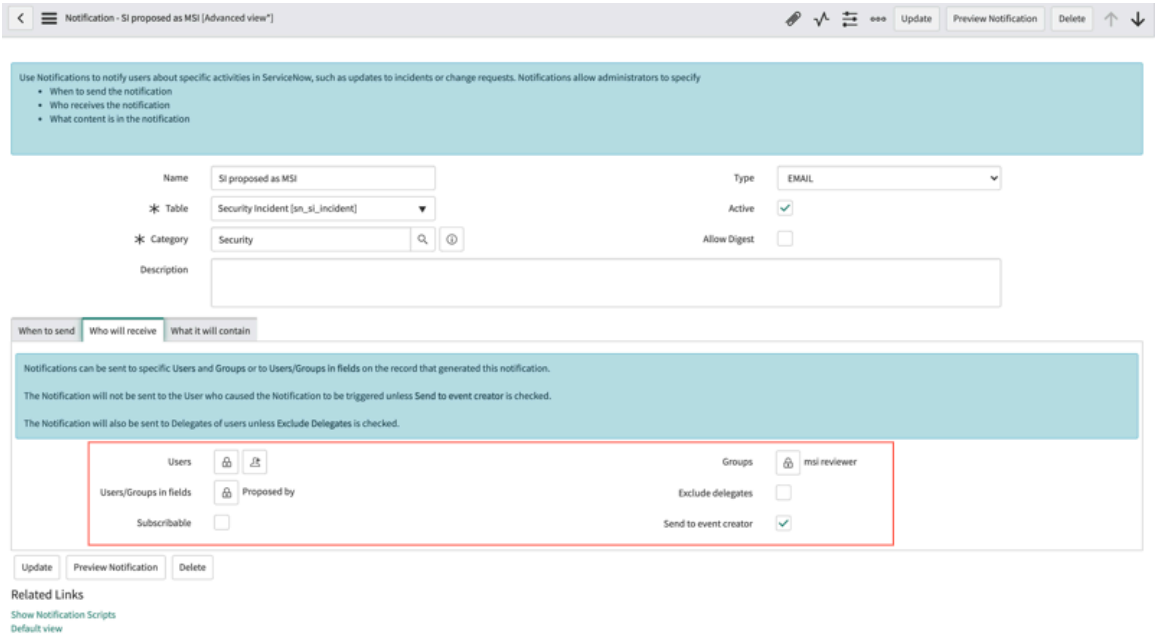
수신인:

- 기본적으로 **MSI** 검토자 그룹 이름이 생성되고 이 그룹에 추가된 모든 사용자에게 다음과 같은 권한이 부여됩니다. **MSIM** 관리자 그리고 해당 그룹에 속한 사용자는 알림 이메일을 받게 됩니다.
- 에 추가된 모든 특정 사용자 사용자 목록에서 알림 이메일도 받게 됩니다.

여기에는 다음이 포함됩니다.

제목 또는 메시지 HTML이 포함된 이메일 본문과 같은 이메일 내용을 수정하려면 시스템 관리자 역할 액세스 권한이 있거나 MSI 관리자가 아닌 시스템 관리자로 할당되어야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



알림: 보안 인시던트가 SI(중요 보안 인시던트)로 승격됨**(MSI)**

이 알림은 보안 인시던트가 승격되고 파일 탐색기 및 Microsoft Teams 기본 구조가 생성될 때 트리거됩니다. 기본적으로 이 알림은 보안 인시던트를 중요 보안 인시던트로 승격한 사용자가 받습니다.

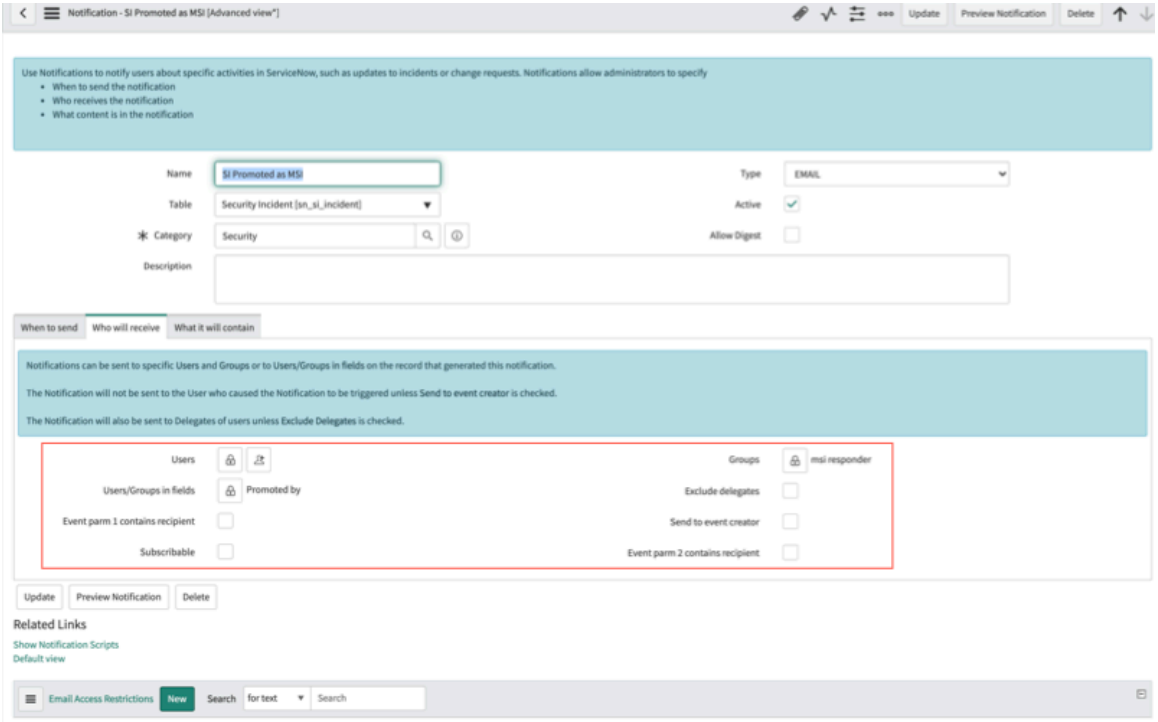
수신인

- 기본적으로 그룹 이름별 **MSI** 응답자 이(가) 작성되었으며 이 그룹에 추가된 모든 사용자에게 다음과 같은 권한이 부여됩니다. **MSIM** 응답자 역할과 해당 그룹에 속한 모든 사용자가 알림 이메일을 받게 됩니다.
- 에 추가된 모든 특정 사용자 사용자 목록에서 알림 이메일도 받게 됩니다.

여기에는 무엇이 포함될 것인가

제목 또는 메시지 HTML을 포함하는 이메일 본문과 같은 이메일 내용을 수정하려면 시스템 관리자 역할 액세스 권한이 있거나 MSI 관리자가 아닌 시스템 관리자로 할당되어야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



MSI 종결 활동 구성

중요 보안 인시던트가 종결될 때 자동으로 발생하는 작업을 설정합니다. 해결 정보가 포함된 폴더에 대한 접근 권한을 자동으로 보관하고 제거하여 보안을 강화합니다.

시작하기 전에
필요한 역할: sn_msi.workspace_admin

프로시저

1. 다음으로 이동 모두 〉 중요 보안 인시던트 관리 〉 **MSI** 관리 〉 구성.
2. 자동화된 종결 작업 섹션에서 공동 작업 채널 보관 확인란을 선택하여 인시던트 해결과 관련된 채팅 통신을 보관합니다.
3. 공동 작업 폴더 제거 확인란을 선택하여 인시던트 해결과 관련된 자료가 포함된 폴더를 제거합니다.
4. 업데이트를 선택합니다.

중요 보안 인시던트 관리 **Workspace**

중요 보안 인시던트 관리 은 관리자를 위해 중요 보안 인시던트 특별히 설계된 주요 보안 인시던트를 관리하기 위한 전용 작업 공간을 제공합니다.

파일 및 폴더를 공유 및 보고, 인시던트 작업을 보고 업데이트하여 주요 보안 인시던트를 해결하는 데 도움이 되는 활동에 대해 쉽게 공동 작업하고, 전용 채팅 채널을 통해 인시던트 작업 담당자와 통신할 수 있습니다.

MSIM(Major Security Incident Management)은 주요 보안 인시던트를 추적하고 해결하기 위한 메커니즘을 제공합니다. MSIM은 기존 보안 인시던트 및 취약성 대응 제품 기능과 함께 작동하며 다음 기능으로 주요 보안 인시던트 정정 프로세스를 개선합니다.

- 주요 보안 인시던트 관리자 사용자 역할을 위해 특별히 설계된 주요 보안 인시던트를 관리하기 위한 전용 작업 공간입니다.
- 연결된 보안 인시던트 및 취약성 그룹에서 추적되는 작업을 포함하여 주요 보안 인시던트 응답 작업을 구성합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 주요 보안 인시던트가 생성되면 협업 폴더와 채팅 커뮤니케이션 채널을 자동으로 생성하고 인시던트 종결의 일부로 보관합니다.
- 통합을 통해 주요 보안 인시던트와 관련된 아티팩트(파일) 컬렉션을 구성하고 추적할 수 있는 파일 탐색기 구성요소입니다 Microsoft SharePoint .
- 통합을 통해 여러 보안, IT 및 기능 그룹 간의 커뮤니케이션을 관리할 수 있는 채팅 채널 관리자 및 활동 스트림 구성요소입니다 Microsoft Teams .
- 영향을 받는 자산, 사용자, 위치 및 팀 자원의 롤업과 중요한 인시던트 마일스톤의 타임라인을 포함하여 주요 보안 인시던트 영향 및 진행률 메트릭에 대한 요약 보고입니다.

MSIM 작업 공간을 사용하여 주요 보안 인시던트를 추적하고 해결합니다.

1. 중요 보안 인시던트의 추세 차트와 진행 상황을 봅니다.
2. MSIM 작업 공간을 통해 Microsoft SharePoint 파일 활동을 추적하고 구성합니다.
3. MSIM 작업 공간을 통해 Microsoft Teams 채팅 활동을 추적하고 구성합니다.
4. MSIM 작업 공간을 통해 인시던트 상세 정보를 보고 업데이트합니다.
5. MSIM 작업 공간 활동 스트림에서 공동 작업 활동을 필터링합니다.

중요 보안 인시던트 관리 사용

관리자는 작업 공간을 사용하여 중요 보안 인시던트 관리 제안, 승격, 연결, 거부된 인시던트 기록을 보고 관련 활동을 추적할 수 있습니다.

인시던트 기록 제안, 승격 및 연결

인시던트가 조직에 대한 중요한 위협으로 식별되면 보안 인시던트를 중요 보안 인시던트로 제안하거나 승격합니다.

인스턴스에 Major Security Incident Management가 설치 ServiceNow 되면 다음과 같이 보안 인시던트를 중요 인시던트로 전환하는 작업을 처리할 수 있습니다.

- 검토 프로세스를 시작할 중요 보안 인시던트 후보에 대한 보안 인시던트를 제안합니다.
- 검토 프로세스 없이 보안 인시던트를 중요 보안 인시던트로 바로 승격
- 중요 보안 인시던트로 제안된 보안 인시던트를 거절합니다.

보안 인시던트를 중요 보안 인시던트에 하위 인시던트로 연결하여 관련된 모든 보안 인시던트를 함께 추적할 수도 있습니다.

다음으로 제안 중요 보안 인시던트

보안 인시던트를 중요 보안 인시던트로 제안합니다.

시작하기 전에
필요한 역할: sn_si.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간 〉 보안 인시던트 〉 목록.
2. 중요 보안 인시던트로 제안하려는 관련 범주의 보안 인시던트를 선택합니다.
3. 추가 작업 아이콘을 선택하고 중요 보안 인시던트로 제안을 선택합니다.
4. 중요 보안 인시던트로 제안 대화 상자의 필드에 내용을 입력합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 탐지 날짜: 중요 보안 인시던트가 처음 생성되거나 제안된 날짜입니다.

b. 근거: 인시던트를 제안한 근거를 제공합니다.

c. 잠재적 영향: 인시던트의 영향을 나타냅니다.

5. 제안을 선택합니다.

결과
인시던트가 제안되고 다음 동작이 발생합니다.

- 보안 인시던트 기록에 검증 배너 메시지가 표시되고 정의된 중요 보안 인시던트 태그가 나타납니다.
- 기록은 인시던트 기록의 중요 보안 인시던트 관련 목록에 나타나고 상태는 제안됨으로 나열되며 MSIM 작업 공간 후보 목록에 표시됩니다.
- MSIM 작업 공간의 활동 섹션에는 보안 인시던트가 중요 보안 인시던트로 승격되도록 제안되었다고 표시됩니다.
- 인시던트의 상세 정보 탭과 인시던트 기록에 대한 링크가 포함된 정의된 알림 목록에 있는 사람들에게 메시지가 전송됩니다.

로 승격 중요 보안 인시던트

보안 인시던트를 중요 보안 인시던트로 승격하거나 (MSIM) 작업 공간을 통해 승격된 제안을 거부합니다 중요 보안 인시던트 관리 .

시작하기 전에
필요한 역할: sn_msi.workspace_admin

프로시저

1. 다음으로 이동 작업 공간 〉 보안 인시던트 응답 작업 공간 〉 보안 인시던트 〉 목록.

2. 중요 보안 인시던트로 승격하려는 관련 범주의 보안 인시던트를 선택합니다.
상세 정보 섹션에서 보안 인시던트의 상세 정보를 검토하거나 추가 상세 정보 보기를 클릭하여 별도의 탭에서 인시던트 기록의 확장된 상세 정보를 봅니다.

3. 추가 작업 아이콘을 선택하고 중요 보안 인시던트로 승격을 선택합니다.

4. 중요 보안 인시던트 승격 대화 상자에서 필드를 채웁니다.

a. 탐지 날짜: 중요 보안 인시던트가 처음 생성되거나 제안된 날짜입니다.

b. 예상 해결 날짜: 중요 보안 인시던트가 해결될 것으로 예상되는 예상 해결 날짜입니다.

c. 코드 이름: 중요 보안 인시던트의 코드 이름을 선택합니다.
예를 들어 Blue Tiger입니다.

d. 범주: 중요 보안 인시던트에 대한 범주를 선택합니다.
예를 들어, 잘못된 구성입니다.

e. 근거: 인시던트를 제안한 근거를 제공합니다.

f. 잠재적 영향: 인시던트의 영향을 나타냅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. 제안을 선택합니다.
6. 보안 인시던트를 승격하거나 승격 제안을 거부합니다.
   - 인시던트를 승격하려면 중요 보안 인시던트로 승격을 클릭합니다.
   - 승격 제안을 거부하려면 중요 보안 인시던트로 거부를 클릭하십시오.
7. 저장을 선택합니다.

결과

- 승격 제안을 거부한 경우 인시던트가 승격되지 않고 인시던트 항목이 거부됨 탭으로 이동합니다.
- 인시던트를 승격한 경우 인시던트 항목이 오픈 탭으로 이동하고 보안 기록에 중요 보안 인시던트임을 나타내는 태그가 표시됩니다.
- 결정은 MSIM 작업 영역의 활동 섹션에 나열됩니다.

인시던트가 승격되면 기본 구성이 적용됩니다.

- 폴더 템플릿 구성을 기반으로 폴더 구조가 생성됩니다.
- 채팅 채널은 채널 구성에 따라 생성됩니다.
- 지정된 사용자에게 이메일 메시지가 전송됩니다. 기본 알림에는 중요 보안 인시던트에 대한 링크와 인시던트 상세 정보가 포함됩니다. 이제 지정된 사용자는 공동 작업 자원에도 액세스할 수 있으므로 알림에는 Microsoft 팀 이름과 인시던트와 관련된 Microsoft SharePoint 폴더에 대한 링크도 포함됩니다.

중요 보안 인시던트에 연결

보안 인시던트를 중요 보안 인시던트와 연결합니다.

시작하기 전에
필요한 역할: sn_msi.workspace_admin

프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 인시던트 〉 모든 인시던트 표시.
2. 중요 보안 인시던트에 연결할 관련 범주의 보안 인시던트를 선택합니다.
3. 추가 작업 아이콘을 선택하고 중요 보안 인시던트에 연결을 선택합니다.
4. 연결하려는 중요 보안 인시던트를 선택합니다.
   a. 대화 상자에서 목록을 사용하여 조회 아이콘을 선택합니다.
   b. 연결하려는 중요 보안 인시던트를 선택합니다.
   c. 확인을 선택합니다.
5. 제안을 선택합니다.

결과
제안서가 제출되고 다음 작업이 발생합니다.

- 보안 인시던트 기록에 검증 배너 메시지가 표시되고 정의된 중요 보안 인시던트 태그가 보안 태그 선택 필드 옆에 표시됩니다.
- 의 중요 보안 인시던트 관리중요 보안 인시던트에 대한 상세 정보 탭의 기록 번호 드롭다운 목록에는 두 인시던트가 모두 포함됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 기록이 인시던트 기록의 중요 보안 인시던트 관련 목록에 나타나고 상태는 제안됨으로 나열됩니다.
- 인시던트의 상세 정보 탭과 인시던트 기록에 대한 링크가 포함된 정의된 알림 목록에 있는 사람들에게 메시지가 전송됩니다.
- MSIM 작업 공간의 활동 섹션에는 보안 인시던트가 링크와 함께 주요 보안 인시던트에 하위 보안 인시던트로 추가되었다고 표시됩니다.

MSIM 작업 공간에서 **MSI** 목록 뷰 사용

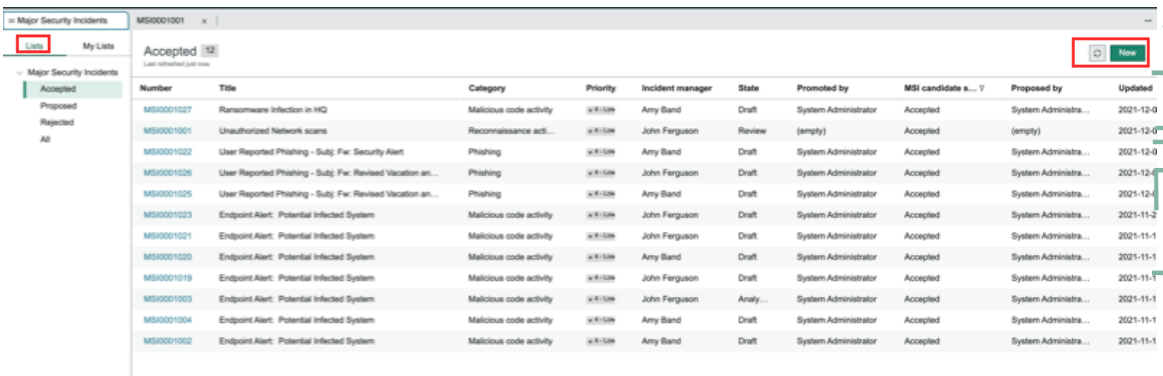
MSIM 작업 공간의 목록 뷰를 사용하여 제안, 승격 및 거부된 중요 보안 인시던트를 볼 수 있습니다.

시작하기 전에
필요한 역할: sn_msi.workspace_manager

작업 공간의 오른쪽 상단에 있는 새로 만들기 버튼을 사용하여 새 인시던트를 만들 수도 있습니다.

프로시저

1. 다음으로 이동 중요 보안 인시던트 관리 〉 **MSIM** 작업 공간.
2. 목록 탭을 선택하여 목록 뷰를 표시합니다.



3. 내 목록을 선택하여 중요 보안 인시던트의 고유한 목록을 생성합니다.
4. 목록 뷰에서 수행할 수 있는 작업은 다음 테이블을 참조하십시오.

작업	설명
내 목록	새 MSI 기록 목록을 만들고 만든 목록을 봅니다.
목록의 열에 대한 필터 설정	열을 선택하고 세로 점 메뉴를 확장하여 열의 데이터를 추가로 필터링하는 옵션을 봅니다.
열의 행에서 항목 또는 일치 항목을 필터링합니다.	열에서 셀을 선택하고 다음 중 하나를 선택하여 표시된 데이터를 구체화합니다. ○ 일치 표시 - 열에서 선택한 항목과 일치하는 항목만 표시합니다. ○ 필터링 - 해당 열에서 선택한 항목과 일치하는 항목을 열에서 필터링합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업	설명
목록 새로 고침	목록을 새로 고치고 업데이트된 전체 목록을 봅니다.
신규	새 MSI 기록을 생성합니다.

영향 메트릭 보기 중요 보안 인시던트

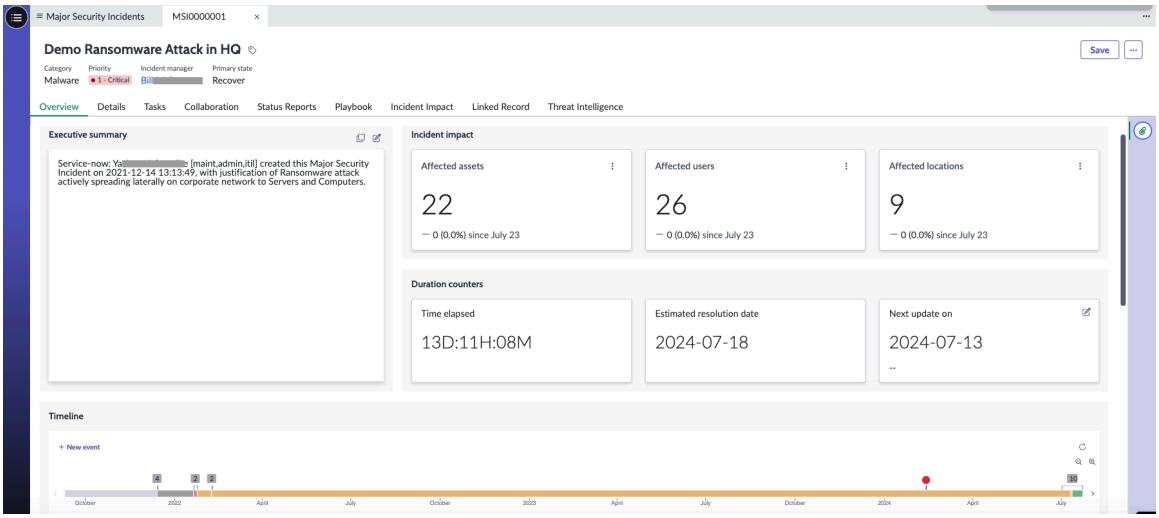
새 작업 공간을 사용하여 주요 보안 인시던트를 관리하는 데 있어 중요한 측면인 중요 보안 인시던트의 영향과 진행 상황에 대한 최신 요약 보고를 제공합니다.

개요 탭은 영향을 받는 자산, 사용자, 위치 및 팀 자원의 롤업과 중요한 인시던트 마일스톤의 타임라인을 포함하여 인시던트의 범위와 진행률을 관리하는 관련 메트릭을 제공합니다.

타임라인은 특정 중요 보안 인시던트 해결의 일부로 발생한 주요 이벤트 및 마일스톤에 대한 수평 뷰를 제공합니다. 타임라인 구성요소는 모든 Major Security Incident Management 작업 공간 탭 상단에 표시되며 필요에 따라 축소 및 확장하여 볼 수 있습니다. 표시된 이벤트 데이터는 지정된 마일스톤 이벤트 또는 마일스톤이 추가되거나 업데이트될 때마다 업데이트되고 새로 고쳐집니다.

각 이벤트 또는 마일스톤은 이벤트 또는 마일스톤의 수와 유형을 식별할 수 있는 다른 타임라인 이벤트 유형 옵션과 함께 표시됩니다. NOW 기록 업데이트, 공동 작업 활동을 예로 들 수 있습니다. 또한 다양한 중요 보안 인시던트 상태의 시간 범위 기간이 자동으로 추적되고 각 인시던트 상태의 기간과 함께 표시되는 색 구분 범위를 사용하여 표시됩니다.

MSIM 개요 탭



실행 요약 및 인시던트 영향

작업	설명
실무 요약	사용자 이름, 사용자 역할 및 타임스탬프 상세 정보와 함께 중요 보안 인시던트에 대한 간략한 요약입니다. • 편집 아이콘을 선택하여 실무 요약을 수정할 수 있습니다. 필요한 변경을 수행한 후 업데이트 옵션을 선택합니다. • 실무 요약을 복사하여 중요 보안 인시던트에 붙여 넣으려면 복사 아이콘을 선택하고 요약을 필요한 중요 보안 인시던트에 붙여넣습니다.

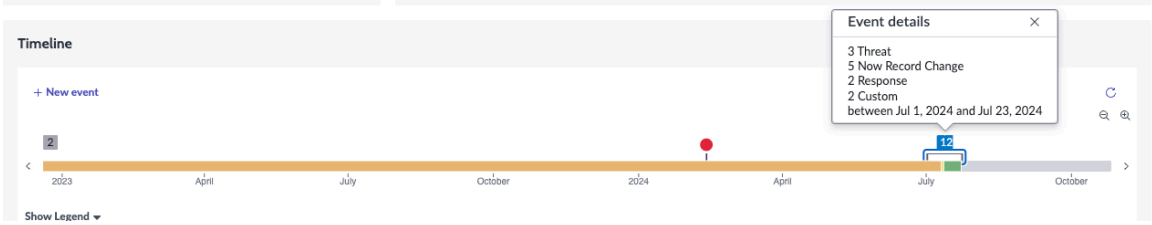
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

실행 요약 및 인시던트 영향

작업	설명
인시던트 영향	이러한 구성요소는 식별된 자산, 사용자, 위치 및 할당된 팀 구성원과 함께 모든 활성 작업 및 연결된 인시던트의 롤업을 기반으로 영향을 받는 자원을 표시합니다. 영향을 받는 자원은 다음과 같습니다. • 영향을 받는 자산 • 영향을 받는 사용자 • 영향을 받는 위치 숫자 값을 선택하면 영향을 받는 자산, 사용자 및 위치 상세 정보로 드릴다운하고 탐색할 수 있으며 작업 공간의 인시던트 영향 탭에 관련 작업이 표시됩니다. 선택한 인시던트 영향 유형 링크에 따라 작업 유형 및 설명, 할당 그룹 및 인시던트 상태와 같은 관련 인시던트 상세 정보가 인시던트 영향 탭. MSIM 작업 공간의
기간 카운터	이러한 구성요소는 중요 보안 인시던트의 기간을 표시합니다. 영향을 받는 자원은 다음과 같습니다. • 경과 시간: 중요 보안 인시던트가 탐지된 후 경과한 시간을 표시합니다. • 예상 해결 날짜: 중요 보안 인시던트가 해결될 것으로 예상되는 시기의 예상 해결 날짜를 표시합니다. • 다음 업데이트 날짜: 중요 보안 인시던트를 해결하기 위한 다음 업데이트의 날짜 및 시간입니다. 예를 들어 2024년 3월 25일 오후 5:00 EST입니다. 편집 아이콘을 선택하여 다음 업데이트를 수정할 수 있습니다. 새 날짜 및 시간을 선택하고 업데이트를 선택합니다.

필터 토글 버튼을 사용하여 타임라인 표시기와 타임라인 범위 모두에 대해 특정 이벤트 유형 보기를 활성화하거나 비활성화할 수 있습니다.

타임라인



타임라인 구성요소에서 사용할 수 있는 추가 기능은 다음 테이블을 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

타임라인 구성요소 추가 기능

작업	설명
새 이벤트	새 사용자 지정 이벤트를 생성하고 이러한 이벤트를 MSI 기록에 연결합니다. 이렇게 하면 타임라인에 기본적으로 표시되는 레이블이 지정된 작업, 기록 상태 변경 또는 레이블이 지정된 공동 작업 활동을 통해 캡처되지 않을 수 있는 과거 및 미래 날짜에 대한 이벤트를 생성하는 데 도움이 됩니다.
새로 고침	타임라인 이벤트를 새로 고침하여 최신 업데이트를 표시합니다.
타임라인 표시기	Now 기록 필드 변경, 레이블이 지정된 공동 작업 활동 및 기타(사용자 지정) 등 다양한 이벤트 유형과 아이콘 및 각 이벤트 유형 표시기와 관련하여 발생한 총 이벤트 수를 나열합니다. 슬라이드 표시기를 사용하면 특정 이벤트 유형에 대한 모든 이벤트를 사용하거나 사용하지 않도록 설정할 수 있습니다.
범례 표시	다양한 유형의 타임라인 표시기가 포함된 드롭다운 범례를 표시하려면 선택합니다.
타임라인 진행률 표시줄	표시된 여러 타임라인 범위 내에서 발생한 지정된 타임라인, 이벤트 또는 마일스톤을 통해 인시던트의 전체 진행률을 표시합니다. 이벤트 유형을 이벤트 범주에 연결할 수도 있습니다. 이벤트 상세 정보를 연결하면 타임라인의 두 위치에서 모두 이벤트 상세 정보가 업데이트됩니다.
타임라인 범위	전체 중요 보안 인시던트 수명주기 동안 인시던트 진행에 따른 다양한 인시던트, 상태 유형 및 기간을 표시합니다. 인시던트 상태에 따라 특정 이벤트를 활성화하거나 비활성화합니다.

타임라인 이벤트 생성

새 타임라인 이벤트를 만들려면 다음 단계를 수행합니다.

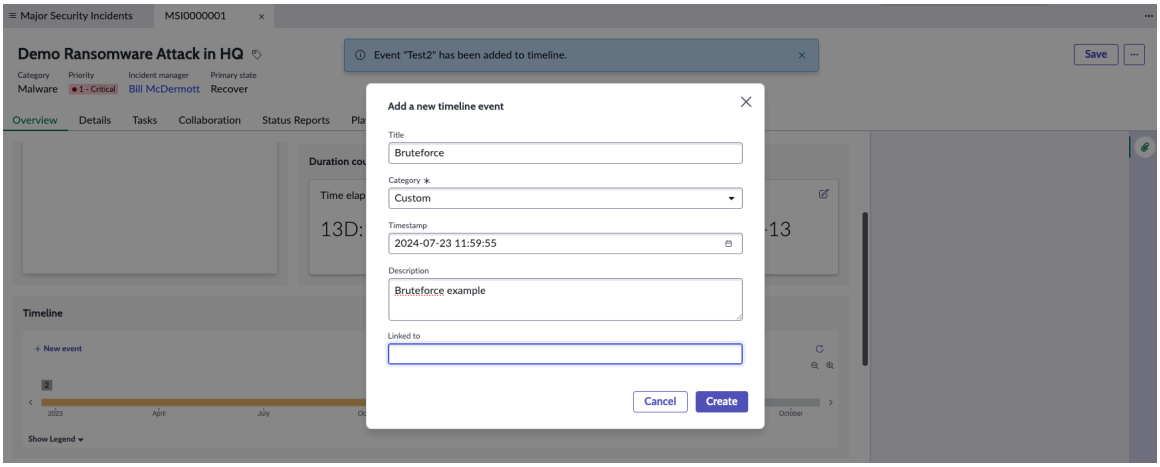
1. 개요 탭에서 타임라인 섹션으로 이동합니다.

2. 선택 **+** 새 이벤트.

3. 새 타임라인 이벤트 추가 팝업의 필드에 내용을 입력합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

새 타임라인 이벤트



작업	설명
직위	타임라인 이벤트의 제목을 입력합니다.
범주	타임라인 이벤트의 범주를 선택합니다. 기본 시스템의 일부로 다음 범주가 제공되며 요구 사항에 따라 선택할 수 있습니다. ○ 사용자 지정. ○ 응답. ○ 위협. 타임라인 이벤트 범주를 추가하거나 구성하려면 다음 문서를 참조하십시오 중요 보안 인시던트에 대한 타임라인 범주 구성.
타임스탬프	타임스탬프 달력을 사용하여 타임라인 이벤트의 날짜 및 시간을 선택합니다. 시작 날짜 전후에 타임라인에 이벤트를 추가할 수 있습니다.
설명	타임라인 이벤트에 대한 간략한 설명을 제공합니다.
링크 대상	타임라인 이벤트를 중요 보안 인시던트 기록에 연결하는 옵션입니다.

4. 선택 작성.
5. 확대 및 축소 아이콘을 사용하여 타임라인 진행률 표시줄을 확대하거나 축소할 수 있습니다. 여기에는 가까운 시간에 근접한 여러 이벤트를 나타내기 위해 숫자가 표시될 때 개별 이벤트 표시가 포함됩니다.

   기본 확대/축소 수준을 추가하여 모든 이벤트를 표시할 수도 있습니다.
6. 새로 고침 아이콘을 선택하여 최신 타임라인 이벤트를 표시합니다.

추세 차트 보기 중요 보안 인시던트

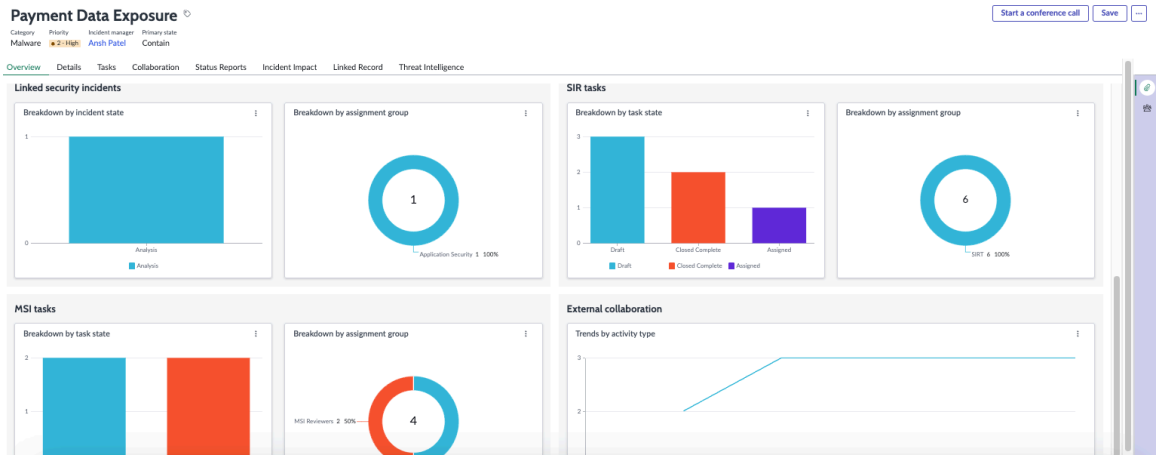
막대 그래프 및 차트로 시각화된 중요 보안 인시던트 영향 진행률 메트릭을 봅니다.

인시던트 타임라인 및 진행률 추세 차트 시각화 외에도 개요 탭은 영향을 받는 자산, 사용자, 위치 및 팀 자원의 롤업을 포함하여 인시던트의 변경 범위를 관리하는 관련 영향 메트릭을 제공합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시각화 구성요소에 표시되는 개수는 연결된 SIR(보안 인시던트 응답) 인시던트의 활성 작업을 기반으로 합니다. 작업이 열리고 닫히면 이러한 개수는 추세 차트 시각화 구성요소에 표시된 추세를 나타내기 위해 중요 보안 인시던트에 대해 계획된 나머지 활동의 특성과 양 측면에서 변경됩니다.

MSIM 개요 탭 영향 메트릭



에서 수행할 수 있는 UI 작업에 대해서는 다음 테이블을 참조하십시오. 개요 절:

개요 **UI** 섹션

직위	설명
시간	중요 보안 인시던트가 활성화된 시점부터 총 기간(일)을 표시합니다. 시간은 다음을 기준으로 계산됩니다. 탐지 날짜에 입력됨 상세 정보 작업 공간의 탭입니다. 탐지 날짜는 종종 중요 보안 인시던트가 처음 생성되거나 제안되었을 때 처음에 캡처됩니다. 이 날짜가 수정될 때마다 시간이 자동으로 계산되고 새로 고쳐지며 일: 시간: 분 형식으로 표시됩니다(예: 20D: 13H: 58M). 예상 해결 날짜: 인시던트 해결 예상 날짜가 해결될 것으로 예상되는 날짜입니다. 이 날짜는 종종 중요 보안 인시던트가 처음 생성되거나 승격되었을 때 처음에 캡처됩니다. 날짜는 다음에 제공된 예상 날짜를 기준으로 업데이트되고 새로 고쳐집니다. 상세 정보 작업 공간의 탭입니다. 상세 정보 섹션에 예상 날짜가 제공되지 않은 경우 이 섹션에는 날짜 값 없이 "하이픈"이 표시됩니다.
활성 팀	주요 보안 인시던트와 관련 작업에 대해 적극적으로 작업 중인 각 팀의 다양한 응답 팀과 팀 구성원을 표시합니다. 활성 팀 추세: 주기적으로 중요 보안 인시던트 및 관련 작업을 적극적으로 수행 중인 각 팀 및 팀 구성원의 추세 차트를 표시합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

개요 **UI** 섹션

직위	설명
	주: 에서 할당된 활성 그룹 보기 상세 정보 작업 공간의 탭입니다.
연결된 **SIR** 인시던트	인시던트 상태별: 분석, 포함, 근절, 복구 또는 검토 등의 인시던트 상태를 기준으로 연결된 보안 인시던트의 분포를 봅니다. 인시던트 상태별 추세: 인시던트 상태를 기준으로 연결된 인시던트 수가 어떻게 진행되고 있는지에 대한 추세 뷰를 추가로 나타냅니다. 각 인시던트 상태 링크를 선택하면 연결된 보안 인시던트 상세 정보를 탐색하여 연결된 **SI/VI** 작업 공간의 탭입니다. 이 섹션은 기본 인시던트에 변경이 발생할 때마다 자동으로 업데이트되고 새로 고쳐집니다.
SIR 작업	SIR 인시던트를 통해 MSI 기록에 연결된 활성 작업 합계를 표시합니다. • 작업 상태별: 초안, 할당됨, 진행 중, 완료 종결 등의 인시던트 상태를 기반으로 인시던트 응답 작업을 봅니다. 이 분포 차트를 사용하면 할당 그룹별로 추가로 분포 세부 항목을 수행할 수 있습니다. 각 작업 상태를 선택하면 에서 인시던트 작업 상태별로 필터링된 목록을 볼 수 있습니다. 작업 작업 공간의 탭입니다. 필터링된 보기를 통해 개별 작업 상세 정보를 보고 업데이트할 수 있습니다. • 인시던트 상태 레이블별 진행 중인 작업: 작업 관리자 구성요소에서 적용해야 하는 인시던트 상태 레이블을 기반으로 활성 작업 및 그룹을 표시합니다. 이러한 기본 레이블에는 분석, 포함, 근절, 복구 또는 검토와 같은 값이 포함되어 관련 작업의 특성을 나타냅니다. • 지연: 활성 상태이며 기한을 초과한 보안 인시던트 응답 작업을 표시합니다. 총 지연 개수를 선택하고 작업 탭으로 자동 탐색하도록 하여 모든 지연된 작업의 상세 정보를 볼 수 있습니다. • 작업 상태별 추세: 인시던트 기간 동안 진행 중인 작업과 종결된 응답 작업의 진행 추세를 봅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

개요 **UI** 섹션

직위	설명
	주: 추세 차트 그래프는 예약된 작업을 기준으로 최신 데이터를 검색합니다. 필요에 따라 데이터 검색 시간 간격을 구성하거나 수정할 수 있습니다.
MSI 작업	MSI 기록에 직접 생성된(연결된 응답 작업이 아닌) 총 활성 작업을 표시합니다. 작업 상태별: 생성된 중요 보안 인시던트 작업, 할당된 작업 및 관련 정보를 봅니다. 각 작업 상태를 선택하면 에서 인시던트 작업 상태별로 필터링된 목록을 볼 수 있습니다. 작업 작업 공간의 탭입니다. 필터링된 뷰를 통해 개별 작업 상세 정보를 보고 업데이트할 수 있습니다.
외부 공동 작업	공동 작업 활동 스트림에서 레이블이 지정된 모든 공동 작업 활동에 대한 총 공동 작업 활동이 표시됩니다. • 인시던트 상태 레이블별:작업 공간의 공동 작업 탭에서 분석, 포함, 근절 또는 복구와 같은 인시던트 상태 레이블을 사용하여 레이블이 지정된 인시던트 공동 작업 활동 데이터와 Microsoft TeamsMicrosoft SharePoint 파일 및 폴더를 봅니다. • 활동 유형별 추세: 인시던트 기간 동안의 파일 및 폴더 활동 수에 Microsoft TeamsMicrosoft SharePoint 대한 추세 차트를 봅니다.

세부 정보 업데이트 중요 보안 인시던트

인시던트 기록 상세 정보, 활성 팀 참가자 및 해당 활동 로그와 같은 중요 보안 인시던트와 관련된 특정 상세 정보를 보고 업데이트합니다.

중요 보안 인시던트의 모든 관련 상세 정보가 작업 공간의 상세 정보 탭에 다양한 양식 섹션과 함께 표시됩니다. 인시던트 기록 상세 정보, 활성 팀 참가자 및 해당 활동 로그와 같은 상세 정보를 표시합니다. 연결된 SIR 인시던트, 취약성 그룹 레코드 상세 정보 및 연결된 모든 인시던트 레코드에 활동 게시를 브로드캐스트하는 기능도 볼 수 있습니다.

기본적으로 상세 정보 탭에는 다음이 포함됩니다.

1. 중요 보안 인시던트 양식 필드 및 인시던트 관련 UI 섹션
2. 활동 스트림

다음 테이블에서는 중요 보안 인시던트 양식 필드의 상세 정보를 제공합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

중요 보안 인시던트 양식 섹션

필드	설명
인시던트	
번호	중요 보안 인시던트 기록 번호입니다.
기본 상태	중요 보안 인시던트 기록의 기본 상태입니다.
탐지 날짜	중요 보안 인시던트가 처음 생성되거나 제안된 날짜입니다. 상세 정보 탭에서 탐지 날짜를 수정할 때마다 MSI의 날짜 및 시간이 자동으로 계산되고 새로 고쳐지며 시간 〉 인시던트가 시작된 이후의 시간 섹션에 있습니다.
직위	중요 보안 인시던트의 제목입니다.
코드 이름	중요 보안 인시던트의 코드 이름입니다. 예를 들어 Blue Tiger입니다.
다음 업데이트	중요 보안 인시던트를 해결하기 위한 다음 업데이트의 날짜 및 시간입니다. 예를 들어 2024년 3월 25일 오후 5:00 EST입니다.
범주	중요 보안 인시던트의 범주입니다.
하위 범주	중요 보안 인시던트의 하위 범주 유형입니다.
예상 해결 날짜	인시던트가 해결될 것으로 예상되는 예상 날짜입니다. 기본값은 중요 보안 인시던트 생성 시점으로부터 7일입니다.
우선순위	중요 보안 인시던트의 우선순위입니다.
경보 센서	중요 보안 인시던트의 경보 센서입니다. 예를 들어 사용자가 보고한 피싱입니다.
소스	중요 보안 인시던트의 소스입니다.
활성 팀	
인시던트 관리자	인시던트 관리자의 이름입니다.
담당 그룹	주요 보안 인시던트에 대해 적극적으로 작업 중인 각 팀의 다양한 응답 팀 및 팀 구성원을 나타냅니다.
지원자	
MSI 후보 상태	제안됨 또는 승격됨과 같은 중요 보안 인시던트 후보 상태를 나타냅니다. 인시던트가 승격되면 상태가 수락됨으로 표시됩니다.
승격한 사람	중요 보안 인시던트를 승격한 사용자입니다.
승격됨	중요 보안 인시던트가 승격된 날짜입니다.
근거	중요 보안 인시던트의 근거입니다. 근거에는 MSI 번호와 코드 이름이 포함되어야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

중요 보안 인시던트 양식 섹션

필드	설명
잠재적 영향	중요 보안 인시던트의 잠재적 영향과 심각도입니다. 잠재적 영향에는 MSI 번호와 코드 이름이 포함되어야 합니다.
제한	
제한 강화	특정 중요 보안 인시던트 제한에 제한을 적용하려면 이 옵션을 선택합니다. 특정 사용자 또는 그룹으로만 보기 또는 수정 액세스를 제한하는 제한을 적용할 수 있습니다. 자세한 내용은 특정 중요 보안 인시던트에 대한 접근 제한 문서를 참조하십시오.
허용된 구성원	중요 보안 인시던트에 액세스할 수 있는 사용자 목록입니다.
허용된 그룹	중요 보안 인시던트에 액세스할 수 있는 그룹 목록입니다.
기타 작업	
첨부 파일	중요 보안 인시던트와 관련된 모든 첨부 파일입니다. 인시던트에 첨부 파일을 추가하려면 옵션 선택을 선택합니다.
컨퍼런스 회의	외부 공급업체 서비스 제공자와의 전화 회의를 통신 채널로 사용하여 이해 관계자와 만나 중요 보안 인시던트를 해결합니다. 자세한 내용은 중요 보안 인시던트 관리 컨퍼런스 회의 통합 문서를 참조하십시오.

활동:

활동 섹션을 사용하여 작업 메모와 코멘트를 추가하고, 활동을 비공개로 게시하고, 작성 섹션을 사용하여 필요에 따라 코멘트를 추가합니다. 작업 메모와 설명을 게시한 후 활동을 저장하여 활동 섹션에서 추가된 활동 또는 작업 메모를 확인합니다.

주:
상세 정보 표시 링크를 선택하여 해당 중요 보안 인시던트와 연결된 특정 보안 인시던트 기록의 상세 정보를 봅니다.

기본 설정을 구성하여 다음과 같은 관련 활동을 봅니다.

1. 필터: 필터 세트 아이콘을 선택하여 필터를 설정합니다.

   작업 메모, 이메일, 타임라인 및 추가 코멘트에 추가된 활동과 같은 활동 대화를 보려면 필터를 설정합니다.

2. 플래그 지정됨: 플래그 지정됨 아이콘을 선택하여 활동에 플래그를 지정합니다.

   중요한 활동 대화에 플래그를 지정하여 편리하게 사용할 수 있도록 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

특정 중요 보안 인시던트에 대한 접근 제한

중요한 정보가 포함된 중요 보안 인시던트를 보거나 수정할 수 있는 사람을 관리합니다. 중요 보안 인시던트 제한을 적용하여 특정 중요 보안 인시던트 기록 및 관련 목록을 보거나 수정할 수 있는 액세스 권한을 가진 사람을 결정하고 특정 사용자 또는 그룹으로만 읽기 또는 쓰기 액세스를 제한할 수 있습니다.

시작하기 전에

필요한 역할: sn_msi.workspace_manager

이 태스크 정보

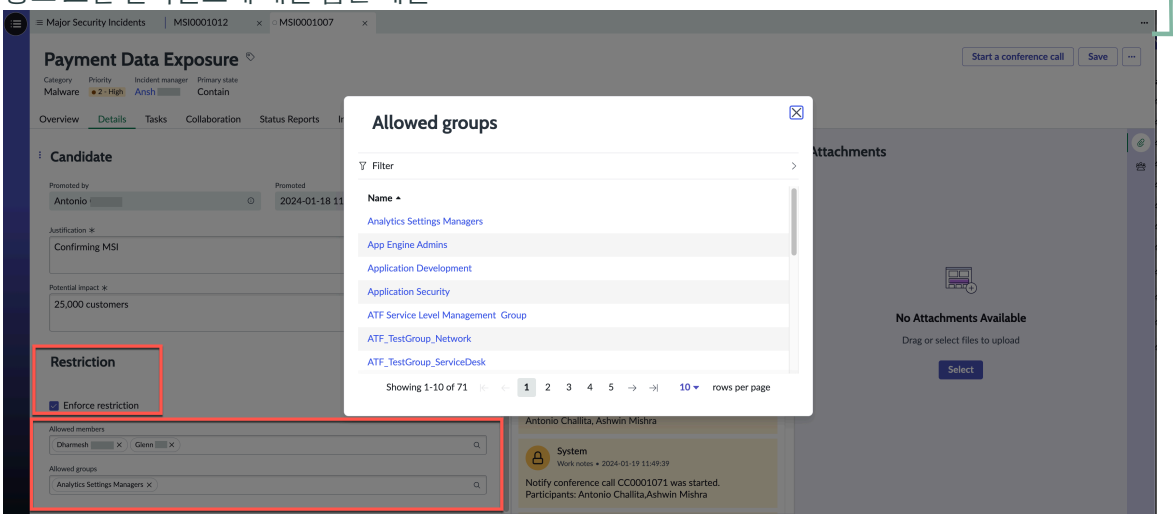
중요 보안 인시던트 제한을 사용하면 특정 조직의 모든 사용자나 그룹이 중요한 중요 보안 인시던트에 액세스하거나 수정하지 못하도록 숨길 수 있습니다. 이러한 제한 사항을 사용하면 사용자나 그룹이 보거나 수정할 수 있는 중요 보안 인시던트를 보다 세부적으로 제어할 수 있습니다. 제한 적용 확인란을 선택하고 특정 중요 보안 인시던트를 보거나 수정할 수 있는 사용자 또는 그룹을 선택하여 주요 보안 인시던트 제한을 적용할 수 있습니다.

주요 보안 인시던트 또는 관련 목록에 대한 제한을 특정 사용자 또는 그룹에 적용하면 조직의 나머지 모든 사용자 또는 그룹이 이러한 주요 보안 인시던트 또는 관련 목록을 보거나 수정할 수 없습니다.

프로시저

1. 다음으로 이동 작업 공간 〉 중요 보안 인시던트 관리 〉 중요 보안 인시던트.
2. 목록 뷰를 선택합니다.
3. 필요한 중요 보안 인시던트 기록을 선택합니다.
4. 상세정보 탭을 선택합니다.
5. 아래로 스크롤하여 제한 섹션을 선택합니다.
6. 제한 강화 확인란을 선택하여 중요 보안 인시던트의 제한을 활성화합니다.

중요 보안 인시던트에 대한 접근 제한



7. 허용된 구성원 필드에서 검색 옵션을 사용하여 중요 보안 인시던트를 보거나 수정할 수 있는 사용자를 선택합니다.
8. 허용된 그룹 필드에서 검색 옵션을 사용하여 중요 보안 인시던트를 보거나 수정할 수 있는 그룹을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

> **주:**
> 중요 보안 인시던트에 대해 제한 적용 확인란을 사용하도록 설정하면 sn_msi.workspace_manager 및 허용된 구성원 또는 그룹만 중요 보안 인시던트를 보거나 수정할 수 있습니다.

9. 저장을 선택합니다.

추가 기록 연결 중요 보안 인시던트

작업 공간에서 기록 연결 기능을 사용하여 관련 보안 인시던트 기록과 하위 보안 인시던트, 취약성 대응의 정정 작업, 위협 인텔리전스의 보안 케이스를 (MSI) 기록에 중요 보안 인시던트 연결합니다.

시작하기 전에
필요한 역할: sn_msi.workspace_manager 및 sn_msi.workspace_responder

프로시저

1. 다음으로 이동 중요 보안 인시던트 응답 〉 **MSIM** 작업 공간.
2. 작업 공간의 왼쪽 창에 표시되는 목록 뷰로 이동합니다.
3. 수락을 클릭하여 승격된 중요 보안 인시던트 기록을 선택합니다.
4. 승격된 기록 목록에서 종결 상태가 아닌 연결해야 하는 인시던트 기록을 선택합니다.
5. 연결된 기록 탭을 클릭합니다.
   다른 연결된 기록 테이블을 선택할 수 있는 드롭다운 목록이 제공됩니다.
   연결된 기록 섹션에는 중요 보안 인시던트에 연결된 연결된 기록 및 관련 기록이 표시됩니다.
6. 목록에서 보안 인시던트, 정정 작업(취약한 항목) 또는 보안 케이스와 같은 원하는 테이블 뷰를 선택합니다.
   선택 유형 기록 테이블 뷰에 따라 중요 보안 인시던트 기록에 연결된 연결된 기록이 표시됩니다.
7. MSI 기록에 연결되지 않고 열림 상태인 기록을 선택하고 페이지 오른쪽 상단에 있는 기록 연결을 클릭하여 기록을 연결합니다.

   > **주:**
   > 종결 상태인 경우 인시던트 기록을 MSI 기록에 연결할 수 없습니다.

8. 연결할 기록을 선택하고 연결을 클릭합니다.
   기록이 성공적으로 연결되었고 관련 기록의 롤업이 백그라운드에서 처리된다는 확인 메시지가 표시됩니다.

   > **주:**
   > 기록이 연결되면 목록 뷰가 자동으로 새로 고쳐지고 인시던트 기록의 업데이트된 목록이 나열됩니다.

관련 정보

다음에서 기록 연결 해제 중요 보안 인시던트

다음에서 기록 연결 해제 중요 보안 인시던트

Major Security Incident Management 작업 공간을 사용하여 연결된 기록 섹션에서 Major Security 인시던트 기록의 연결을 해제합니다.

시작하기 전에
필요한 역할: sn_msi.workspace_manager 및 sn_msi.workspace_responder

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

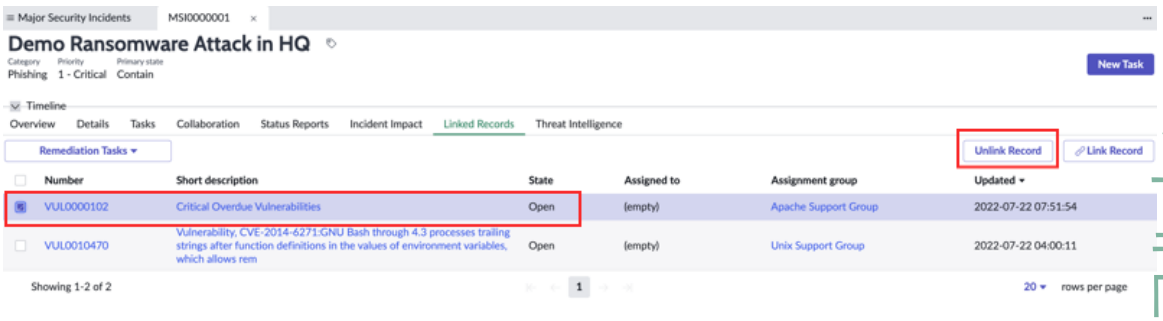
주:
한 번에 하나의 기록만 연결 해제할 수 있습니다. 기록 연결을 해제하면 관련 롤업된 정보가 작업 공간의 인시던트 영향 및 위협 인텔리전스 섹션에서 제거되고 작업을 취소할 수 없습니다.

롤업 기록에 대한 자세한 내용은 다음 문서를 참조하십시오 용 롤업 프레임워크 MSIM.

프로시저

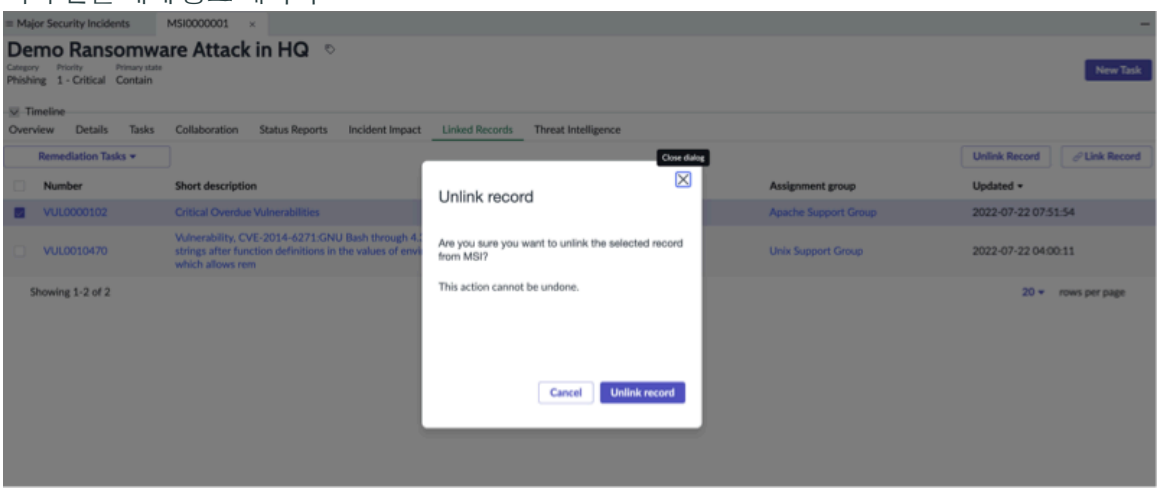
1. 다음으로 이동 중요 보안 인시던트 응답 〉 **MSIM** 작업 공간.
2. 작업 공간의 왼쪽 창에 표시되는 목록 뷰로 이동합니다.
3. 수락을 클릭하여 승격된 중요 보안 인시던트 기록을 선택합니다.
4. 연결된 기록 탭을 클릭합니다.
   이 섹션에는 연결된 기록과 중요 보안 인시던트에 연결된 관련 기록이 표시됩니다.
5. 보안 인시던트, 정정 작업(취약한 항목) 또는 보안 케이스와 같은 원하는 테이블 뷰를 선택합니다.
6. 기록의 목록 뷰에서 연결을 해제할 기록을 선택합니다.
7. 기록 연결 해제를 클릭합니다.

기록 연결 해제



8. 선택한 레코드를 MSI에서 연결 해제할 것인지 묻는 경고 메시지가 표시됩니다.

기록 연결 해제 경고 메시지



9. 기록 연결 해제를 클릭합니다.
   기록의 연결이 해제되고 연결이 해제되면 변경 내용을 되돌릴 수 없습니다. 연결을 해제하면 연결된 기록의 목록 뷰가 새로 고침됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관련 정보

에서 연결된 기록 구성 중요 보안 인시던트 관리

에서 롤업 기록 구성 중요 보안 인시던트 관리

에서 작업 관리 중요 보안 인시던트

작업 탭을 사용하면 MSIM 작업 공간에서 주요 보안 인시던트와 관련된 모든 작업을 추적하고 관리할 수 있습니다. 기본 시각적 작업 보드(칸반 뷰) 또는 목록 뷰를 사용하여 다양한 작업을 볼 수 있습니다.

sn_msi.workspace_manager는 작업 탭에서 다음을 수행할 수 있습니다.

- 작업 작성
- 수정 작업
- 작업을 보고 자신에게 또는 다른 사람에게 할당
- 작업 삭제

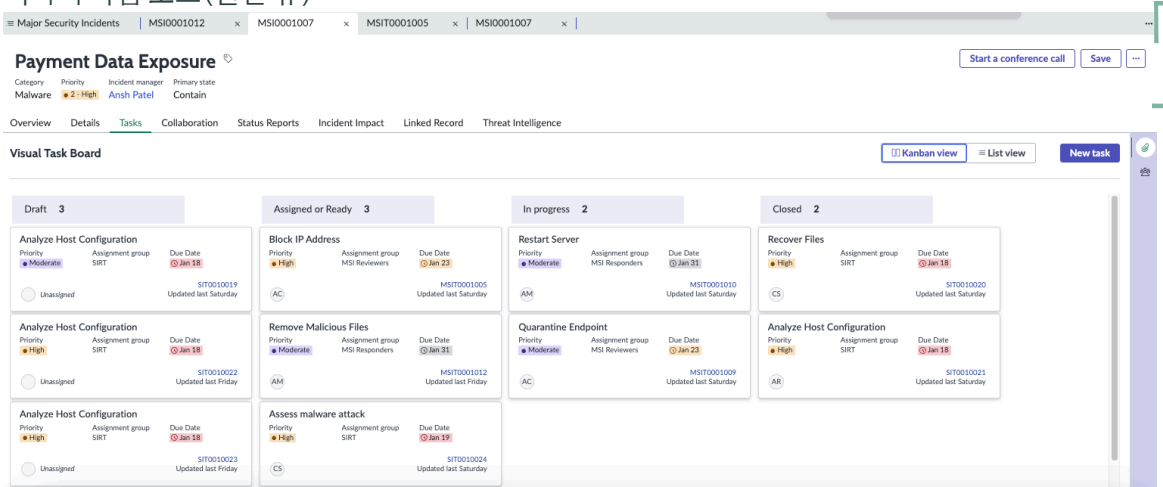
주:
MSIM 앱을 설치한 후 **MSIM VTB** 작업 카드: **1.0.1v** 앱을 별도로 설치했는지 확인하십시오.

작업 탭에는 중요 보안 인시던트와 관련된 모든 작업의 상세 정보가 표시됩니다. 작업 탭은 다음 두 가지 뷰를 지원합니다.

- 시각적 작업 보드(칸반 뷰):

  시각적 작업 보드에 카드로 나타나는 여러 작업 기록을 보고 업데이트하고 주요 보안 인시던트의 작업 상태에 따라 레인 간에 이동할 수 있습니다.

  시각적 작업 보드(칸반 뷰)

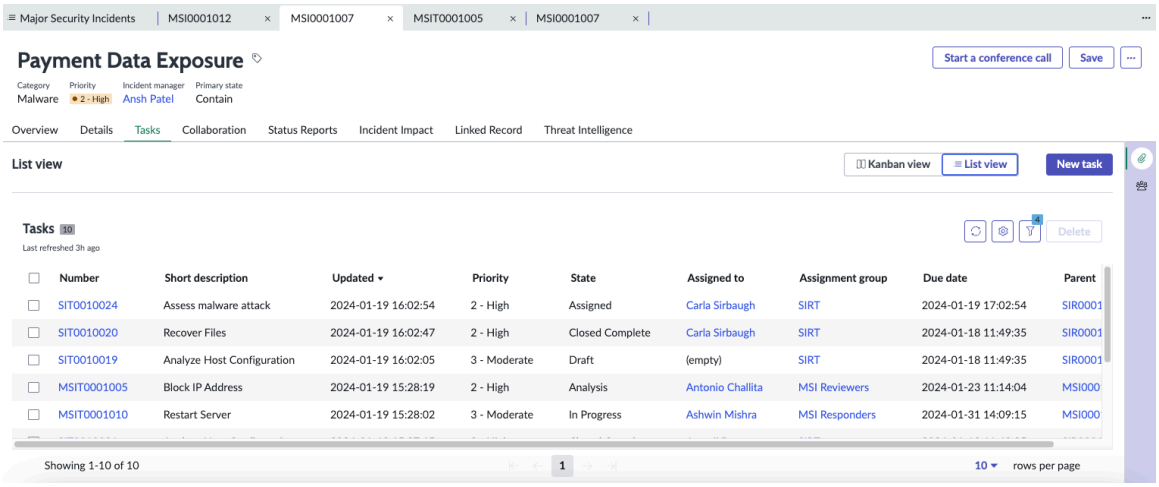


- 목록 뷰:

  목록 형식을 사용하여 여러 작업 기록을 보고 업데이트합니다. 이러한 목록 범주와 필터를 사용하면 주요 보안 인시던트에서 처리해야 하는 작업을 빠르게 찾고 추적할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

목록 뷰



레이블이 지정된 활동이 요약되어 중요 보안 인시던트의 개요 섹션에 표시됩니다. 개요 섹션에서 추세 차트 그래프를 사용하여 통합된 작업 활동 상태를 볼 수 있습니다.

시각적 작업 보드를 사용하여 작업 관리

시각적 작업 보드(칸반 뷰)를 사용하여 중요 보안 인시던트와 연관된 모든 작업을 추적하고 관리합니다.

시각적 작업 보드를 사용하여 작업 상태에 따라 초안, 할당됨 또는 준비됨, 진행 중, 종결됨과 같은 레인 간에 카드를 단계별로 이동할 수 있습니다. 보드의 활동 스트림에 최근 활동이 표시되어 작업 변경 사항을 쉽게 추적할 수 있습니다. 작업을 확장하는 모든 테이블에서 작업 카드를 추가하여 업데이트를 빠르게 추적하고 보드에서 직접 주요 보안 인시던트를 편집할 수 있습니다.

시각적 작업 보드를 사용하여 작업 생성

필요한 역할: sn_msi.workspace_manager.

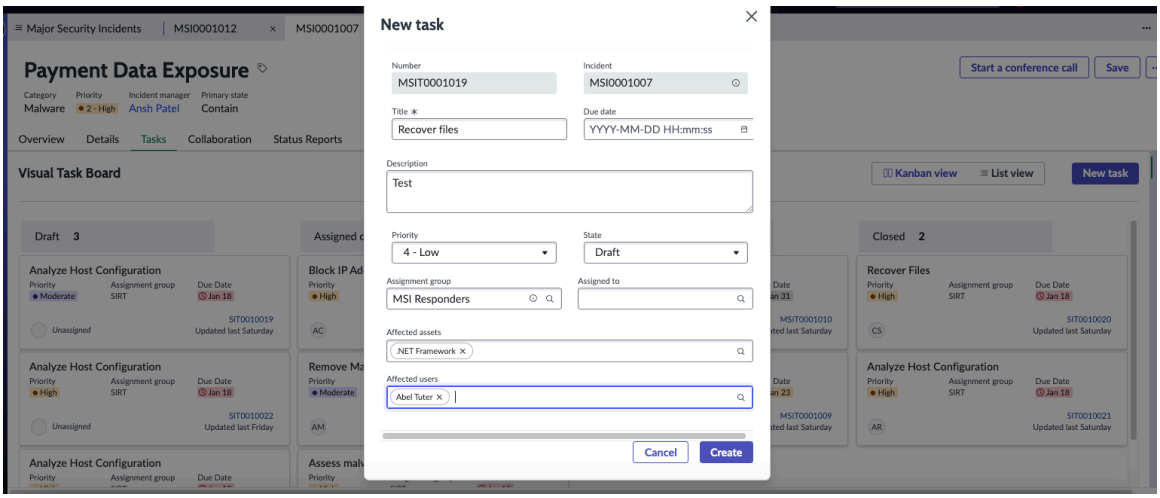
주:
MSIM 앱을 설치한 후 **MSIM VTB** 작업 카드: **1.0.1v** 앱을 별도로 설치했는지 확인하십시오.

MSI 관리자는 다음 단계를 사용하여 시각적 작업 보드에서 작업을 만들 수 있습니다.

1. 다음으로 이동 작업 공간 〉 중요 보안 인시던트 관리 〉 중요 보안 인시던트.
2. 목록 뷰를 선택합니다.
3. 필요한 중요 보안 인시던트 기록을 선택합니다.
4. 작업 탭을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시각적 작업 보드를 사용하여 작업 생성



5. Kanban 보기를 선택하고 새 작업을 선택합니다.

6. 양식에서 필드를 채웁니다.

필드	설명
번호	선택한 작업에 대해 자동으로 생성되는 고유 번호입니다. 이 필드는 편집할 수 없습니다.
인시던트	중요 보안 인시던트 번호입니다. 이 필드는 편집할 수 없습니다.
직위	작업 이름을 입력합니다.
기한	작업을 완료할 기한 및 시간을 선택합니다. 달력 옵션을 사용하여 날짜를 선택하고 시간 선택 섹션에서 시간을 지정합니다.
설명	작업에 대한 고유한 설명을 입력합니다.
우선순위	작업의 우선순위를 선택하여 작업 수행 시기를 결정합니다. 우선순위는 다음 값 중 하나일 수 있습니다. ○ 없음 ○ 1-중요 ○ **2 -** 높음 ○ **3 -** 보통 ○ **4 -** 낮음 ○ **5-** 계획
상태	작업의 현재 상태를 선택합니다. 상태는 다음 중 하나일 수 있습니다. ○ 초안 ○ 분석 ○ 진행 중 ○ 종결

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	기본 상태는 초안입니다.
할당 그룹	검색 옵션을 사용하여 작업을 할당할 사용자의 할당 그룹을 선택합니다.
담당자	검색 옵션을 사용하여 작업을 할당할 사용자를 선택합니다.
영향을 받는 자산	검색 옵션을 사용하여 작업에 의해 영향을 받는 자산을 선택합니다.
영향을 받는 사용자	검색 옵션을 사용하여 작업에 의해 영향을 받는 사용자를 선택합니다.

7. 만들기를 선택하여 작업을 만듭니다.

시각적 작업 보드를 사용하여 작업 보기 및 수정

필요한 역할: sn_msi.workspace_manager.

주:
MSIM 앱을 설치한 후 **MSIM VTB** 작업 카드: **1.0.1v** 앱을 별도로 설치했는지 확인하십시오.

MSI 관리자는 MSI 응답자로부터 작업의 상세 정보와 활동 정보를 볼 수 있으며, 다음 단계를 사용하여 시각적 작업 보드에서 작업을 수정할 수 있습니다.

1. 다음으로 이동 작업 공간 〉 중요 보안 인시던트 관리 〉 중요 보안 인시던트.

2. 목록 뷰를 선택합니다.

3. 필요한 중요 보안 인시던트 기록을 선택합니다.

4. 작업 탭을 선택하고 칸반 보기를 선택합니다.

5. 레인 중 하나에서 원하는 작업 카드를 선택하여 작업의 상세 정보를 봅니다.

작업 카드는 초안, 할당됨 또는 준비됨, 진행 중 또는 종결 레인 중 하나에 있을 수 있습니다.

6. 작업 정보 섹션에서 다음 상세 정보를 수정할 수 있습니다.

필드	설명
번호	선택한 작업에 대해 자동으로 생성되는 고유 번호입니다. 이 필드는 편집할 수 없습니다.
인시던트	중요 보안 인시던트 번호입니다. 이 필드는 편집할 수 없습니다.
직위	작업 이름을 입력합니다.
기한	작업을 완료할 기한 및 시간을 선택합니다. 달력 옵션을 사용하여 날짜를 선택하고 시간 선택 섹션에서 시간을 지정합니다.
설명	작업에 대한 고유한 설명을 입력합니다.
우선순위	작업의 우선순위를 선택하여 작업 수행 시기를 결정합니다. 우선순위는 다음 값 중 하나일 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

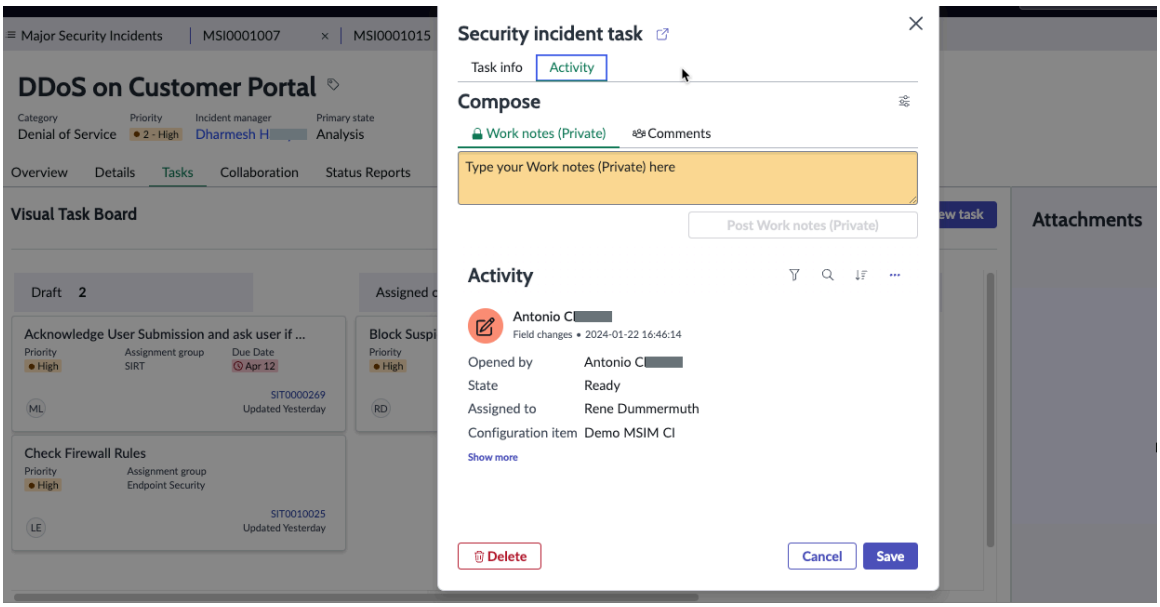
필드	설명
	○ 없음 ○ 1 - 중요 ○ **2 -** 높음 ○ **3 -** 보통 ○ **4 -** 낮음 ○ **5-** 계획
상태	작업의 현재 상태를 선택합니다. 상태는 다음 중 하나일 수 있습니다. ○ 초안 ○ 분석 ○ 진행 중 ○ 종결 기본 상태는 초안입니다.
할당 그룹	검색 옵션을 사용하여 작업을 할당할 사용자의 할당 그룹을 선택합니다.
담당자	검색 옵션을 사용하여 작업을 할당할 사용자를 선택합니다.
영향을 받는 자산	검색 옵션을 사용하여 작업에 의해 영향을 받는 자산을 선택합니다.
영향을 받는 사용자	검색 옵션을 사용하여 작업에 의해 영향을 받는 사용자를 선택합니다.

7. 활동 섹션을 선택하여 MSI 응답자의 활동 세부 정보를 봅니다.

활동 섹션을 사용하여 작업 메모와 코멘트를 추가하고, 활동을 비공개로 게시하고, 작성 섹션을 사용하여 필요에 따라 코멘트를 추가합니다. 작업 메모와 코멘트를 게시한 후 활동을 저장하여 활동 섹션에서 추가된 활동 또는 작업 메모를 봅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시각적 작업 보드의 활동 섹션



주:
해당 중요 보안 인시던트와 연결된 특정 보안 인시던트 기록의 상세 정보를 보려면 상세 정보 표시 링크를 선택합니다.

8. 저장을 선택하여 작업 정보를 업데이트합니다.

   작업 정보가 즉시 업데이트됩니다.

시각적 작업 보드를 사용하여 작업 삭제

필요한 역할: sn_msi.workspace_manager.

주:
MSIM 앱을 설치한 후 **MSIM VTB** 작업 카드: **1.0.1v** 앱을 별도로 설치했는지 확인하십시오.

MSI 관리자는 다음 단계를 통해 시각적 작업 보드에서 작업을 삭제할 수 있습니다.

1. 다음으로 이동 작업 공간 〉 중요 보안 인시던트 관리 〉 중요 보안 인시던트.
2. 목록 뷰를 선택합니다.
3. 필요한 중요 보안 인시던트 기록을 선택합니다.
4. 작업 탭을 선택하고 칸반 보기를 선택합니다.
5. 삭제할 작업 카드를 선택합니다.
6. 중요 보안 인시던트 작업 팝업에서 삭제 옵션을 선택합니다.

   작업 삭제 확인을 요청하는 작업 삭제 팝업이 나타납니다.

7. 삭제를 선택합니다.

목록 뷰를 사용하여 작업 관리

목록 뷰를 사용하여 중요 보안 인시던트와 관련된 모든 작업을 추적하고 관리합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

목록 뷰에는 작업 번호, 우선순위, 현재 상태, 할당 대상, 할당된 그룹 등 중요 보안 인시던트와 관련된 모든 작업의 상세 정보가 표시됩니다. 이러한 목록 범주와 필터를 사용하면 주요 보안 인시던트에서 수행해야 할 필수 작업을 빠르게 찾고 추적할 수 있습니다.

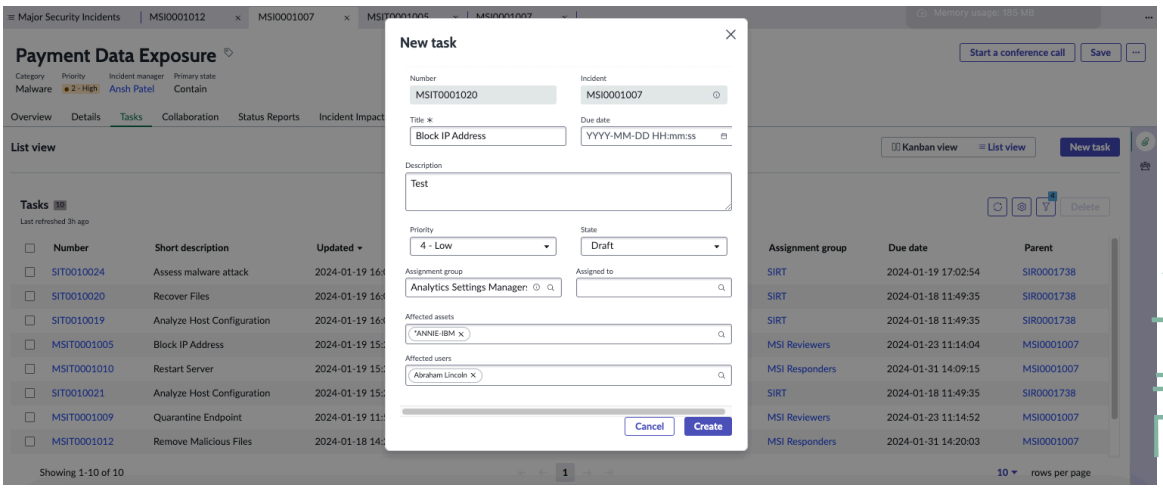
목록 뷰를 사용하여 작업 생성

필요한 역할: sn_msi.workspace_manager.

MSI 관리자는 다음 단계를 사용하여 목록 뷰에서 작업을 만들 수 있습니다.

1. 다음으로 이동 작업 공간 〉 중요 보안 인시던트 관리 〉 중요 보안 인시던트.
2. 목록 뷰를 선택합니다.
3. 필요한 중요 보안 인시던트 기록을 선택합니다.
4. 작업 탭을 선택합니다.

목록 뷰를 사용하여 작업 생성



5. 목록 보기를 선택하고 새 작업을 선택합니다.
6. 양식에서 필드를 채웁니다.

필드	설명
번호	선택한 작업에 대해 자동으로 생성되는 고유 번호입니다. 이 필드는 편집할 수 없습니다.
인시던트	중요 보안 인시던트 번호입니다. 이 필드는 편집할 수 없습니다.
직위	작업 이름을 입력합니다.
기한	작업을 완료할 기한 및 시간을 선택합니다. 달력 옵션을 사용하여 날짜를 선택하고 시간 선택 섹션에서 시간을 지정합니다.
설명	작업에 대한 고유한 설명을 입력합니다.
우선순위	작업의 우선순위를 선택하여 작업 수행 시기를 결정합니다. 우선순위는 다음 값 중 하나일 수 있습니다. ○ 없음 ○ 1 - 중요 ○ **2 -** 높음

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	○ **3 -** 보통 ○ **4 -** 낮음 ○ **5-** 계획
상태	작업의 현재 상태를 선택합니다. 상태는 다음 중 하나일 수 있습니다. ○ 초안 ○ 분석 ○ 진행 중 ○ 종결 기본 상태는 초안입니다.
할당 그룹	검색 옵션을 사용하여 작업을 할당할 사용자의 할당 그룹을 선택합니다.
담당자	검색 옵션을 사용하여 작업을 할당할 사용자를 선택합니다.
영향을 받는 자산	검색 옵션을 사용하여 작업에 의해 영향을 받는 자산을 선택합니다.
영향을 받는 사용자	검색 옵션을 사용하여 작업에 의해 영향을 받는 사용자를 선택합니다.

7. 만들기를 선택하여 작업을 만듭니다.

목록 뷰를 사용하여 작업 보기 및 수정

필요한 역할: sn_msi.workspace_manager.

MSI 관리자는 MSI 응답자로부터 작업의 상세 정보와 활동 정보를 볼 수 있으며, 다음 단계를 사용하여 목록 뷰에서 작업을 수정할 수 있습니다

1. 다음으로 이동 작업 공간 〉 중요 보안 인시던트 관리 〉 중요 보안 인시던트.

2. 목록 뷰를 선택합니다.

3. 필요한 중요 보안 인시던트 기록을 선택합니다.

4. 작업(**Tasks**) 탭을 선택하고 목록 보기**(List view**)를 선택합니다.

5. 목록 뷰에서 원하는 작업을 선택하여 작업의 상세 정보를 봅니다.

6. 작업 정보 섹션에서 다음 상세 정보를 수정할 수 있습니다.

필드	설명
번호	선택한 작업에 대해 자동으로 생성되는 고유 번호입니다. 이 필드는 편집할 수 없습니다.
인시던트	중요 보안 인시던트 번호입니다. 이 필드는 편집할 수 없습니다.
직위	작업 이름을 입력합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

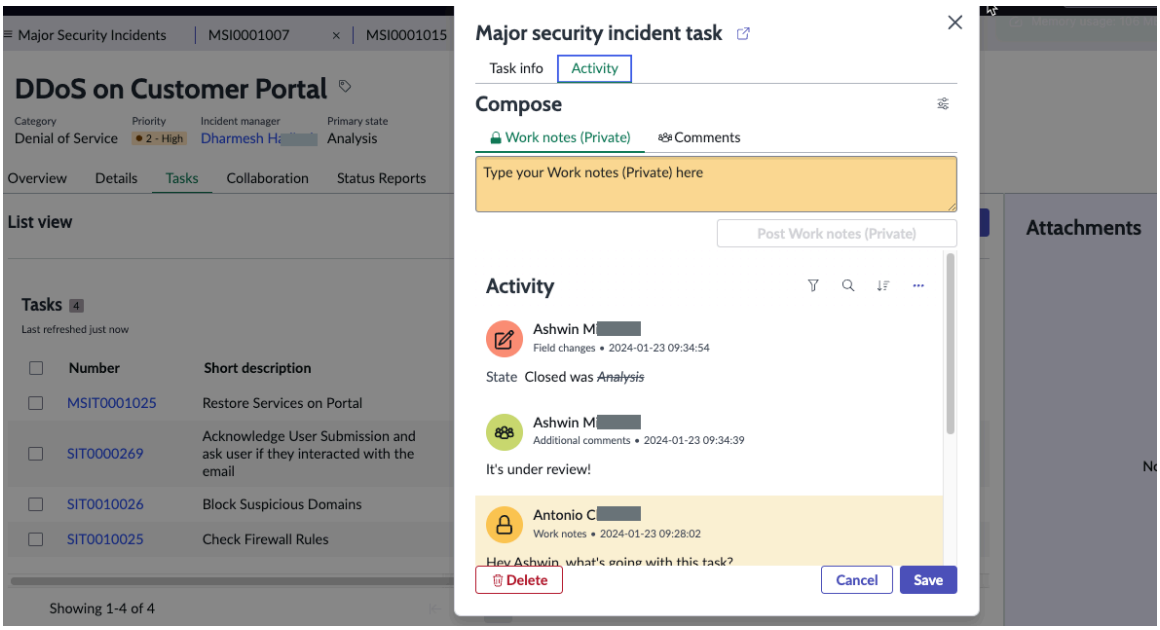
필드	설명
기한	작업을 완료할 기한 및 시간을 선택합니다. 달력 옵션을 사용하여 날짜를 선택하고 시간 선택 섹션에서 시간을 지정합니다.
설명	작업에 대한 고유한 설명을 입력합니다.
우선순위	작업의 우선순위를 선택하여 작업 수행 시기를 결정합니다. 우선순위는 다음 값 중 하나일 수 있습니다. ○ 없음 ○ 1-중요 ○ **2 -** 높음 ○ **3 -** 보통 ○ **4 -** 낮음 ○ **5-** 계획
상태	작업의 현재 상태를 선택합니다. 상태는 다음 중 하나일 수 있습니다. ○ 초안 ○ 분석 ○ 진행 중 ○ 종결 기본 상태는 초안입니다.
할당 그룹	검색 옵션을 사용하여 작업을 할당할 사용자의 할당 그룹을 선택합니다.
담당자	검색 옵션을 사용하여 작업을 할당할 사용자를 선택합니다.
영향을 받는 자산	검색 옵션을 사용하여 작업에 의해 영향을 받는 자산을 선택합니다.
영향을 받는 사용자	검색 옵션을 사용하여 작업에 의해 영향을 받는 사용자를 선택합니다.

7. 활동 섹션을 선택하여 MSI 응답자의 활동 세부 정보를 봅니다.

   활동 섹션을 사용하여 작업 메모와 코멘트를 추가하고, 활동을 비공개로 게시하고, 작성 섹션을 사용하여 필요에 따라 코멘트를 추가합니다. 작업 메모와 코멘트를 게시한 후 활동을 저장하여 활동 섹션에서 추가된 활동 또는 작업 메모를 봅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

목록 뷰의 활동 섹션



주:
해당 중요 보안 인시던트와 연결된 특정 보안 인시던트 기록의 상세 정보를 보려면 상세 정보 표시 링크를 선택합니다.

8. 저장을 선택하여 작업 정보를 업데이트합니다.

   작업 정보가 즉시 업데이트됩니다.

9. 목록 뷰에서 다음 작업을 수행할 수도 있습니다.
   a. 목록 뷰에서 작업 목록을 새로 고치려면 새로 고침 아이콘을 선택합니다.
   b. 설정 아이콘을 선택하고 열 편집 옵션을 사용하여 목록 뷰에 표시되는 열 목록을 수정합니다. 너비 재설정 옵션을 사용하여 열의 너비를 재설정합니다.

목록 뷰를 사용하여 작업 삭제

필요한 역할: sn_msi.workspace_manager.

MSI 관리자는 다음 단계에 따라 목록 뷰에서 작업을 삭제할 수 있습니다.

1. 다음으로 이동 작업 공간 〉 중요 보안 인시던트 관리 〉 중요 보안 인시던트.
2. 목록 뷰를 선택합니다.
3. 필요한 중요 보안 인시던트 기록을 선택합니다.
4. 작업 탭을 선택합니다.
5. 목록 뷰를 선택합니다.
6. 목록에서 삭제할 작업을 선택합니다.
7. 중요 보안 인시던트 작업 팝업에서 삭제 옵션을 선택합니다.

   작업 삭제 확인을 요청하는 작업 삭제 팝업이 나타납니다.

8. 삭제를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업 공간을 통한 **MSIM** 공동 작업 활동 추적

MSIM 작업 공간을 통해 중요 보안 인시던트 해결과 관련된 채팅 및 파일 활동을 추적합니다.

활동은 채팅, Microsoft SharePoint 파일 및 폴더를 사용하여 Microsoft Teams 조정된 다음 통합을 통해 다시 중요 보안 인시던트 게시됩니다.

와 Microsoft SharePoint가 통합중요 보안 인시던트 관리되면 Microsoft Teams 작업 공간을 사용하여 MSIM 인시던트 응답 사용자와 주요 보안 인시던트 해결에 기여하는 다른 그룹 간의 공동 작업을 추적할 수 있습니다. 내 Microsoft SharePoint 공동 작업 폴더 및 파일에 대한 모든 업데이트는 작업 공간과 File Explorer 동기화 MSIM 되고 활동 스트림 구성요소에도 반영됩니다.

보안 인시던트가 중요 보안 인시던트로 승격되는 경우:

1. 폴더 템플릿 구성에 따라 폴더 구조가 생성됩니다 Microsoft SharePoint . 동일한 폴더 구조가 작업 공간의 구성요소에 File Explorer 반영됩니다.
2. 애플리케이션에서 여러 채널이 있는 팀이 생성 Microsoft Teams 되고 작업 공간의 채팅 관리 구성요소에 동일한 내용이 반영됩니다.

필요한 역할: sn_msi.workspace_manager.

파일 및 폴더와 상호작용

파일 탐색기에 파일 시스템이 표시되므로 인시던트 해결과 관련된 파일 및 폴더를 보고 상호 작용할 수 있습니다.

특정 보안 인시던트에 대해 Microsoft SharePoint에서 캡처한 파일 및 폴더를 표시합니다. 이러한 폴더는 해당 중요 보안 인시던트에 대해 Microsoft SharePoint에 자동으로 생성됩니다. 필요한 경우 이 기본 생성 폴더를 사용하여 지원 파일을 업로드할 수 있습니다. 필요에 따라 이러한 파일 및 폴더의 이름을 바꾸거나 이동하거나 삭제할 수 있습니다.

또한 폴더에 파일을 업로드할 때마다 해당 폴더에 해당하는 활동이 공동 작업 탭의 파일 탐색기 폴더에 자동으로 연결되고 활동이 기록되어 Major Security Incident Management 작업 공간의 활동 섹션에 표시됩니다.

> **주:**
> 공동 작업 탭에서 인시던트 기록이 고유한 인시던트 번호와 인시던트 범주로 SharePoint의 상위 파일에 추가됩니다.

1. 리포지토리 뷰: 특정 보안 인시던트에 대해 Microsoft SharePoint에 나열된 파일 및 폴더를 나열합니다. 각 파일 또는 폴더에 대해 저장소 보기에 이름, 수정한 사람, 마지막으로 수정한 날짜 및 크기가 표시됩니다.

   리포지토리 뷰

필드	설명
SharePoint에서 열기	중요 보안 인시던트 옆에 있는 이 옵션을 선택합니다. 링크를 클릭하여 Microsoft SharePoint에서 폴더 구조를 선택하고 봅니다.
새 폴더	필요에 따라 새 폴더를 생성하려면 이 옵션을 선택합니다. 새 폴더를 만들면 기본적으로 동일한 새 폴더가 만들어지고 Microsoft SharePoint에 연결됩니다.

2. 최근 항목: 모든 최근 활동 로그를 표시합니다. 이러한 로그에는 SharePoint 및 파일 탐색기 활동이 모두 포함됩니다. 최근 활동은 일반적으로 상위 폴더를 포함하는 지원 파일입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음은 로그 파일을 찾는 절차입니다.

a. 해당 파일을 선택하여 상세 정보를 봅니다.

b. 파일 찾기를 클릭합니다.

> **주:**
> 상위 파일 및 상위 폴더의 탐색과 상세 정보가 최근 목록 뷰 섹션 아래에 표시됩니다. SharePoint에서 동일한 파일을 열 수 있습니다. 관련 로그 파일 또는 활동을 업로드할 때마다 해당 모든 파일 및 활동이 SharePoint 및 파일 탐색기 모두 표시됩니다.

Microsoft Teams를 사용하여 채팅 채널 커뮤니케이션 관리

채팅 채널 관리자는 구성 템플릿 설정을 기반으로 Microsoft Teams 애플리케이션에서 생성된 여러 채널과 함께 Microsoft Teams를 표시합니다.

이렇게 구성된 채널은 할당된 사용자 및 사용자 그룹과 함께 채팅 관리 구성요소에 반영됩니다. 채팅 채널 관리자를 사용하면 다음을 수행할 수 있습니다.

- 채팅 채널 관리
- 팀 이름 변경
- 팀 구성원 관리

팀과 채널은 Microsoft Teams의 채팅 채널 구성을 기반으로 생성됩니다.

채팅 채널 관리

채팅 채널 관리자를 사용하여 채팅 채널을 생성, 편집 또는 삭제할 수 있습니다. Microsoft Teams에서 채팅 채널을 관리하려면 다음 단계를 수행하십시오.

1. 공동 작업 탭을 선택합니다.

2. 다음으로 이동 채팅 채널 관리자 〉 새 채널 생성.

3. 새 채널 이름, 설명을 추가하고 채널의 구성원 을 선택합니다.

4. 생성을 선택합니다.

> **주:**
> 새 채널 기록은 Microsoft Teams 애플리케이션의 Microsoft Teams 채널 섹션에 생성되고 동일한 기록이 MSIM에 반영됩니다.

5. 채팅 채널을 편집하려면 채팅 채널 관리자 목록에서 채팅 채널을 선택하십시오.

6. 요구 사항에 따라 채널 이름, 구성원 목록, 그룹 구성원 목록을 수정할 수 있습니다.

7. 저장을 선택합니다.

8. 채팅 채널을 삭제하려면 채팅 채널 관리자 목록에서 채팅 채널을 선택하십시오.

9. 채널 삭제를 선택합니다.

팀 이름 변경

Microsoft Teams에서 팀 이름을 바꾸려면 다음 단계를 수행합니다.

1. 공동 작업 탭을 선택합니다.

2. 다음으로 이동 채팅 채널 관리자 〉 팀 이름 변경.

3. 팀 이름 필드에서 요구 사항에 따라 팀 이름을 바꿉니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 저장을 선택합니다.

> 주:
> 팀 이름을 변경하면 Microsoft Teams의 팀 이름도 변경됩니다.

팀 구성원 관리

채팅 채널 관리자를 사용하면 Microsoft Teams에서 팀 구성원을 추가하거나 제거할 수 있습니다. 그룹을 통해서도 구성원을 추가할 수 있습니다. Microsoft Teams에서 팀 구성원을 관리하려면 다음 단계를 수행합니다.

1. 공동 작업 탭을 선택합니다.
2. 다음으로 이동 채팅 채널 관리자 〉 팀 구성원 관리.
3. 구성원 필드에서 요구 사항에 따라 팀 구성원을 추가하거나 제거합니다.
4. 그룹을 통해 구성원 추가 필드에서 Microsoft Teams에 추가할 그룹을 선택합니다.

> 주:
> 그룹 구성원이 이미 팀에 있는 경우 해당 구성원은 추가되지 않습니다.

5. 저장을 선택합니다.

채팅 채널 관리자에는 전체 팀 구성원의 세부 정보와 추가될 새 구성원 수가 표시됩니다.

Slack을 사용하여 채팅 채널 커뮤니케이션 관리

채팅 채널 관리자는 구성 템플릿 설정을 기반으로 Slack 애플리케이션에서 생성된 여러 채널과 함께 Slack을 표시합니다.

이렇게 구성된 채널은 할당된 사용자 및 사용자 그룹과 함께 채팅 관리 구성요소에 반영됩니다. 채팅 채널 관리자를 사용하면 채팅 채널을 관리할 수 있습니다. 팀과 채널은 Slack의 채팅 채널 구성을 기반으로 생성됩니다.

채팅 채널 관리

채팅 채널 관리자를 사용하면 Slack에서 채팅 채널을 생성, 편집 또는 삭제할 수 있습니다. 채팅 채널을 관리하려면 다음 단계를 수행하십시오.

1. 공동 작업 탭을 선택합니다.
2. 다음으로 이동 채팅 채널 관리자 〉 새 채널 생성.
3. 새 채널 이름, 설명을 추가하고 채널의 구성원 을 선택합니다.
4. 생성을 선택합니다.

> 주:
> Slack 애플리케이션의 Slack 채널 섹션에 새 채널 기록이 만들어지고 동일한 기록이 MSIM에 반영됩니다.

5. 채팅 채널을 편집하려면 채팅 채널 관리자 목록에서 채팅 채널을 선택하십시오.
6. 요구 사항에 따라 채널 이름, 구성원 목록, 그룹 구성원 목록을 수정할 수 있습니다.
7. 저장을 선택합니다.
8. 채팅 채널을 삭제하려면 채팅 채널 관리자 목록에서 채팅 채널을 선택하십시오.
9. 채널 삭제를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

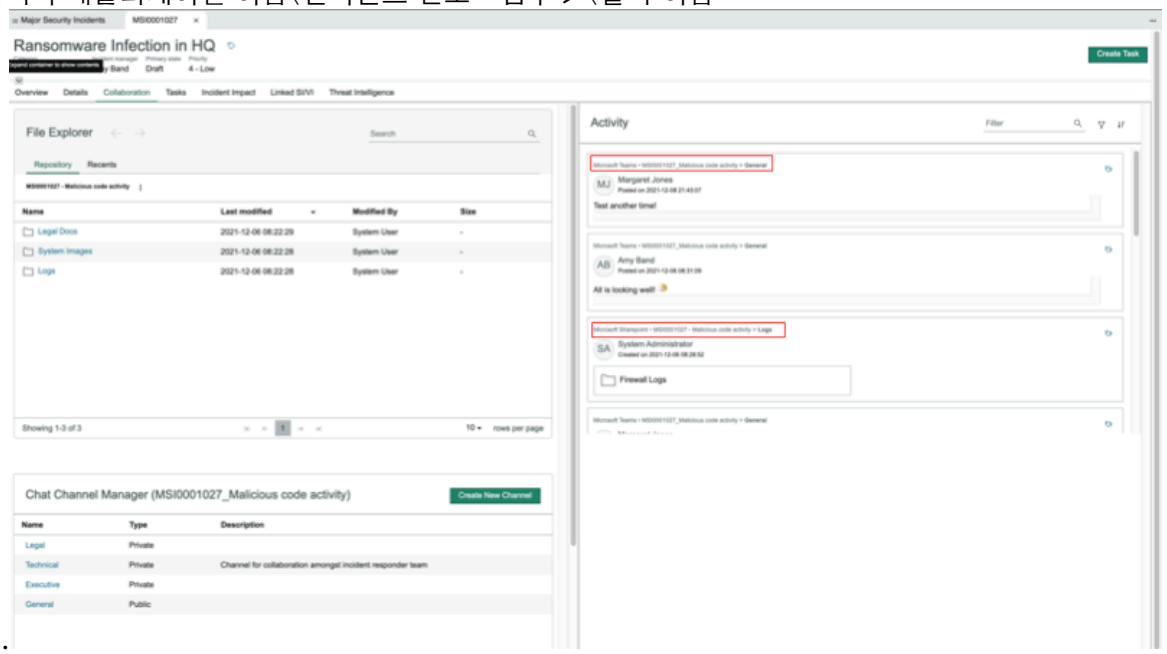
활동 스트림 대화 관리

, 파일 탐색기 및 Microsoft Teams에서 수행된 Microsoft SharePoint모든 활동, 로그, 상태를 표시합니다.

특정 활동을 보거나 다양한 파일 및 폴더와 Microsoft Teams 간에 상호 작용한 공동 작업 활동 세부 정보를 검색하려면 활동 스트림 섹션의 오른쪽 상단에 표시되는 필터 기능을 사용하여 원하는 활동 상세 정보를 찾을 수 있습니다.

Major Security Incident Management와 공유되는 폴더 및 채팅 대화는 다음 구조와 함께 이동 경로로 반영됩니다.

커넥터 애플리케이션 이름〈인시던트 번호 - 범주 > 〈폴더 이름



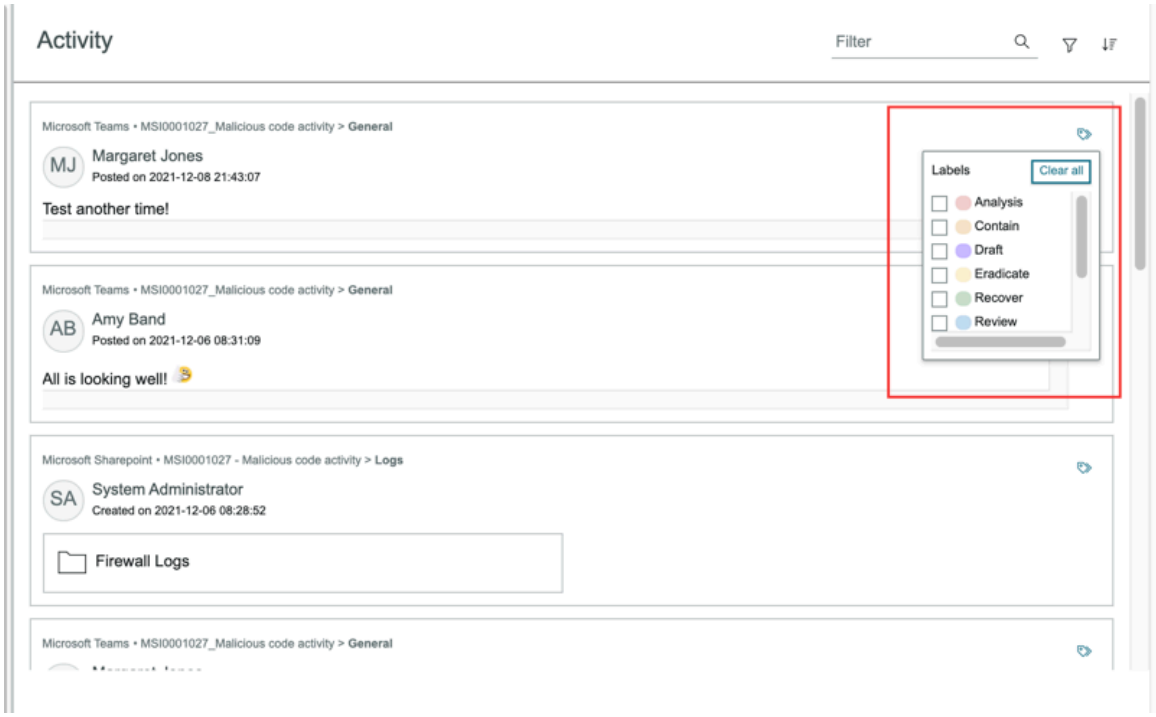
>).

활동에 레이블을 지정합니다.

1. 레이블 아이콘을 클릭합니다.

2. 아래 스크린샷에 표시된 대로 해당 인시던트 활동 레이블 확인란을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



3. 레이블이 지정된 활동은 색상으로 구분되며 작업 공간의 외부 공동 작업 섹션에 진행률 추세 그래프로 표시됩니다.

상태 보고서 생성 및 배포 **MSIM**

중요 보안 인시던트 관리자는 중요 보안 인시던트 해결 과정에서 구성된 보고서 템플릿 또는 이전 상태 보고서를 기반으로 다양한 간격으로 다양한 상태 보고서를 생성하여 여러 이해 관계자에게 배포할 수 있습니다.

시작하기 전에

필요한 역할: sn_msi.workspace_manager

다른 이해 관계자에게 배포하기 전에 이전에 구성된 요약 보고서 데이터 요소를 미리 보고, 추가 텍스트 또는 요약을 추가하고, 필요에 따라 개별 보고서 구성요소를 제거하고, 보고서의 정확성과 완전성을 확인할 수 있습니다.

MSI 보고서 템플릿 설정 페이지에서 처음에 구성된 원하는 보고서 템플릿을 선택하여 상태 보고서를 만듭니다.

프로시저

1. 다음으로 이동 작업 공간 〉 중요 보안 인시던트 관리 〉 중요 보안 인시던트.
2. 목록 뷰를 선택합니다.
3. 승격된 각 MSI 기록을 선택합니다.
4. 상태 보고서 탭을 선택합니다.
   상태 보고서 탭에는 아래와 같은 세 가지 유형의 하위 섹션이 포함되어 있습니다.

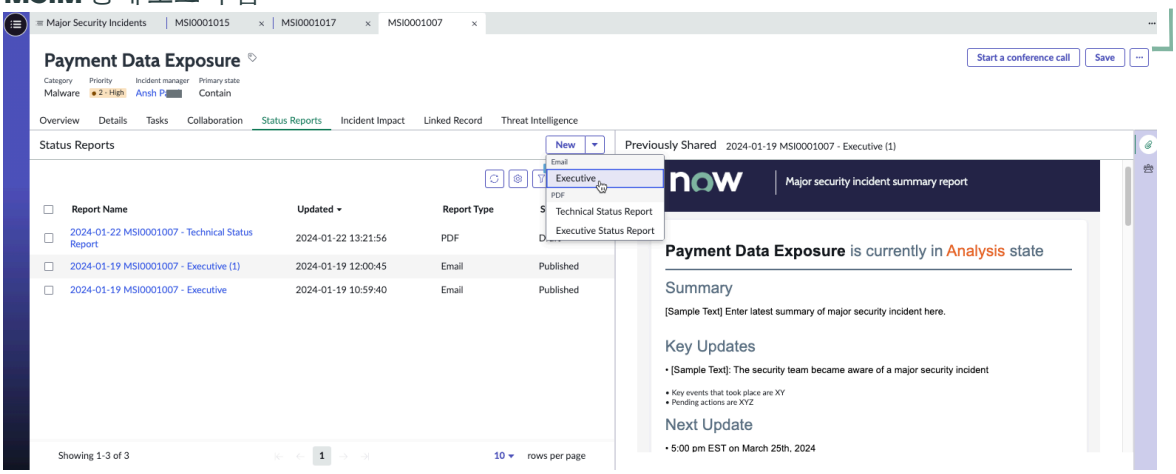
필드	설명
보고서 이름	상태 보고서 템플릿의 이름입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	주: 상태 보고서 뷰에는 관련 가상 사용자에 대한 기본 시스템의 일부로 사용할 수 있는 미리 정의된 기존 보고서 템플릿이 나열됩니다. 예를 들어, 이메일을 통한 경영 상태 보고서(모바일 친화적), 기술 상태 보고서, PDF로 된 경영 상태 보고서를 작성할 수 있습니다.
업데이트됨	보고서 템플릿이 마지막으로 업데이트된 날짜입니다.
보고서 유형	상태 보고서의 유형입니다. 상태 보고서는 다음 유형 중 하나일 수 있습니다. ○ PDF ○ 이메일
상태	상태 보고서의 상태입니다. 상태 보고서는 다음 상태 중 하나일 수 있습니다. ○ 초안 ○ 큐에 대기 중 ○ 게시 날짜:

5. 보려는 상태 보고서의 유형을 선택하거나 새로 만들기를 선택하여 상태 보고서를 만듭니다.

MSIM 상태 보고서 탭



6. 목록에서 다음 상태 보고서 유형 중 하나를 선택합니다.

- 경영자 모바일 친화적인 이메일 상태 보고서.
- 기술 상태 보고서 PDF (영어)
- 경영진 상태 보고서 PDF (영어)

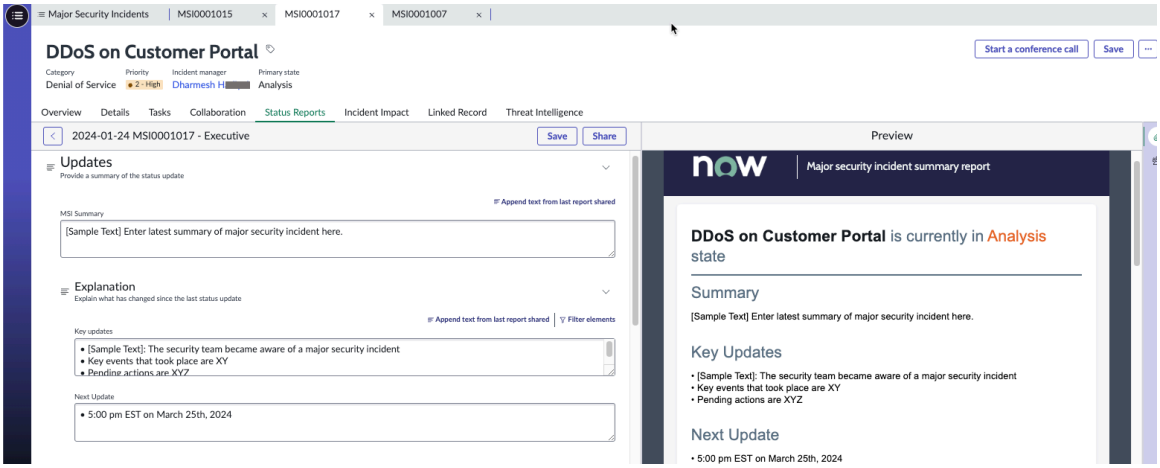
주:
원하는 보고서 템플릿을 선택하면 선택한 보고서의 미리 보기가 오른쪽 창에 즉시 생성됩니다. MSI의 선택한 상태 보고서를 볼 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

7. 임원 이메일 상태 보고서 템플릿에서 상태 보고서의 세부 정보로 섹션을 채웁니다.

> **주:**
> 상태 보고서 섹션에서 선택한 옵션은 미리 보기 보고서에서 렌더링되는 옵션과 동일합니다.

상태 보고서 템플릿



8. 저장을 선택하여 상태 보고서에 대한 업데이트를 저장합니다.

9. 공유를 선택하여 내부 및 외부 이해 관계자와 상태 보고서를 공유합니다.
공유 대화 상자가 나타납니다.

a. 제목 필드에 이메일 보고서의 제목을 입력합니다.

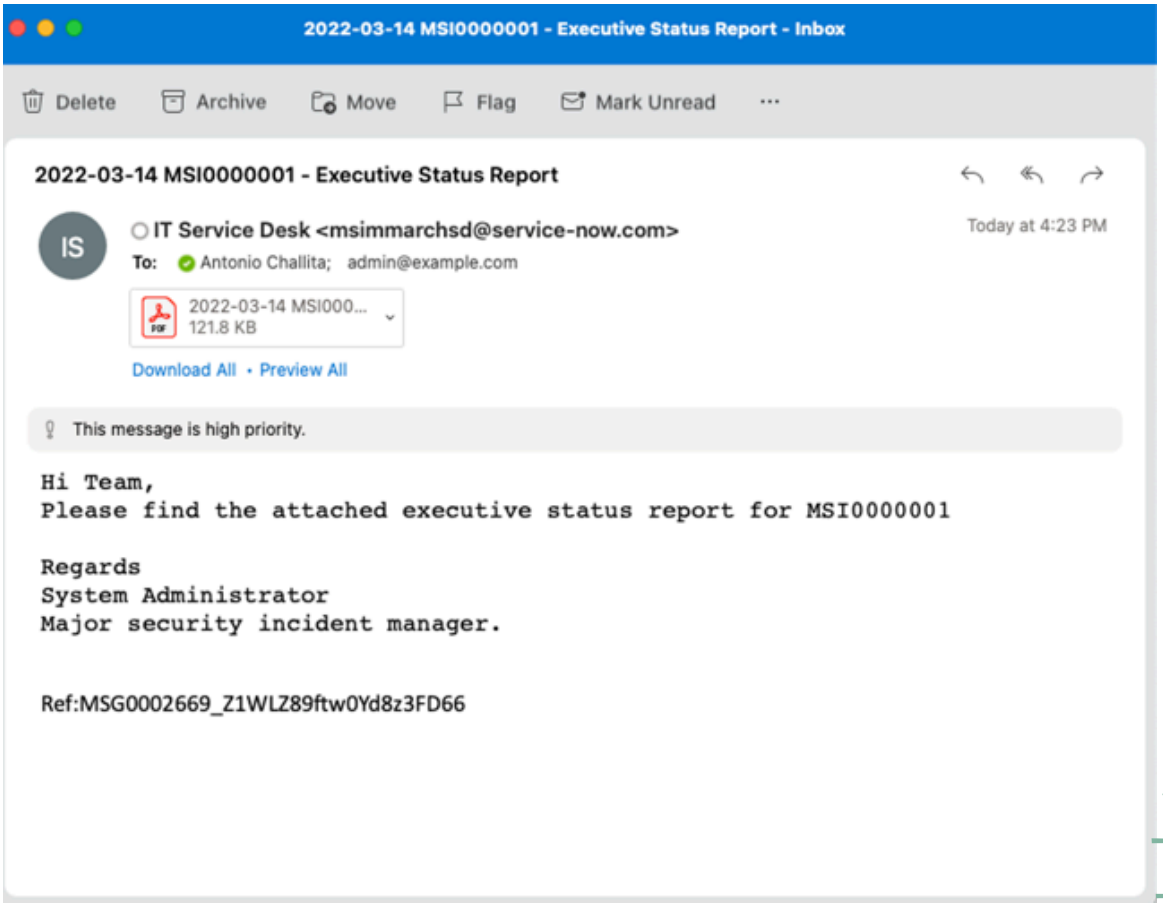
b. 내부 수신자 추가 필드에 이메일 보고서의 수신자를 입력하고 선택합니다.

c. Add external recipients(외부 수신자 추가) 필드에 수신자의 이메일 또는 이메일 보고서에 대한 DL을 입력합니다.
쉼표나 세미콜론을 사용하여 여러 이메일 ID를 추가할 수 있습니다.

10. 이메일 보고서를 선택합니다.
PDF 상태 보고서가 첨부된 이메일이 관련 수신자가 확인할 수 있도록 성공적으로 전송됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

상태 보고서 - 이메일



11. 상태 보고서 탭에서 다음 작업을 수행할 수도 있습니다.

a. 상태 보고서 뷰에서 새로 고침 작업을 사용하여 상태 보고서 목록을 새로 고칩니다.

b. 상태 보고서 뷰의 목록 작업 작업을 사용하여 열을 편집하거나 상태 보고서 목록의 너비를 재설정할 수 있습니다.

c. 상태 보고서 뷰에서 필터 동작을 사용하여 특정 조건을 기준으로 상태 보고서를 필터링합니다.

관련 정보

상태 보고서 구성 중요 보안 인시던트

상태 보고서 관리 **MSIM**

상태 보고서는 실행 가능한 데이터 시각화와 함께 사전 구성된 추세 차트를 제공하여 보안 운영 프로세스를 개선하고 할당된 각 작업의 해결 타임라인, 지연 횟수 및 상태를 측정 및 분석합니다.

상태 보고서 구성 중요 보안 인시던트

중요 보안 인시던트 기록 정정 프로세스의 수명주기 동안 비즈니스 요구에 따라 보고서를 설정하고 다운로드하도록 중요 보안 인시던트 보고서를 구성합니다.

특정 형식 및 레이아웃으로 보고서 템플릿을 빌드하고 작업 영역의 상태 보고서 기능을 사용하여 특정 요구 사항에 따라 이러한 보고서를 사용자 지정할 수 있습니다 중요 보안 인시던트 관리 .

sn_msi.workspace_manager 역할을 가진 사용자는 임원급 이해 관계자, 법무 부서와 같은 특정 사용자와 공유하고 이러한 템플릿을 주요 보안 인시던트 기록에 매핑할 수 있는 모든 상태 보고서를 생성하는 데 사용할 수 있는 보고서 정보 유형을 개략적으로 설명하는 보고서 템플릿을 만들고 구성할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

MSI 상태 보고서를 사용자 지정하려면 먼저 보고서 템플릿을 사용하여 보고서 템플릿을 설정해야 합니다. 보고서 템플릿을 사용하여 보고서 템플릿 유형을 빌드하고, 해당 보고서 템플릿에 대한 보고서 구성요소를 정의하고, 추가 정보를 추가하고, 범위 및 진행률 메트릭을 추적하기 위해 시각화된 데이터를 만들고, 관련 목록 데이터를 추가하고, 상태 보고서를 생성할 수 있습니다.

다음은 모든 보고서 템플릿 유형에 제공되는 기본 필드에 대한 설명입니다. 섹션, 하위 섹션 및 해당 요소를 사용하여 요구 사항에 따라 보고서 템플릿을 구성하고 형식을 지정할 수 있습니다.

상태 보고서 구성요소

구성요소 유형	설명
보고서 제목	보고서 유형의 제목입니다. 예를 들어 보고서 유형의 기본 형식은 다음과 같습니다. {MSI 번호} - {임원 이해 관계자 보고서}는 MSI0001001: 임원 이해 관계자 보고서로 표시됩니다.
이름	Major Security Incident Management 작업 공간의 상태 보고서 섹션을 사용하여 보고서를 생성한 사용자의 이름을 표시합니다.
요약	보고서의 간략한 요약을 표시합니다.
날짜	보고서가 관련 수신자와 공유된 날짜를 표시합니다.
진행률	연결된 SIR 인시던트, 응답 작업, 보조 작업, 외부 공동 작업, 타임라인 구성요소 및 최근 타임라인 이벤트와 같은 범위 및 진행률 메트릭을 표시합니다.
과제	이 섹션에서는 주요 보안 인시던트 정정 프로세스 전체에서 발생하는 문제에 대해 간략하게 설명합니다.
다음 단계	이 섹션에는 주요 보안 인시던트 해결과 관련된 다음 단계에 대한 간략한 설명이 표시됩니다. 예를 들어 임원 이해 관계자 보고서의 활성 팀 하위 섹션은 중요 보안 인시던트 기록의 추가 분석에 관여하는 팀 할당의 다음 단계에 대한 정보를 제공합니다.
기타 커스터마이제이션	보고서 템플릿은 로고를 업로드하고 보고서의 머리글과 바닥글을 사용자 지정하는 기능도 제공합니다.

다음은 설정하고 볼 수 있는 보고서 범주 유형입니다.

- 경영자 메일 주소
- 기술 상태 보고서 PDF (영어)
- 경영진 상태 보고서 PDF (영어)

위의 보고서는 구성되어 사용자가 Major Security Incident Management 작업 공간에서 보고서를 선택하고, 보고, 생성할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

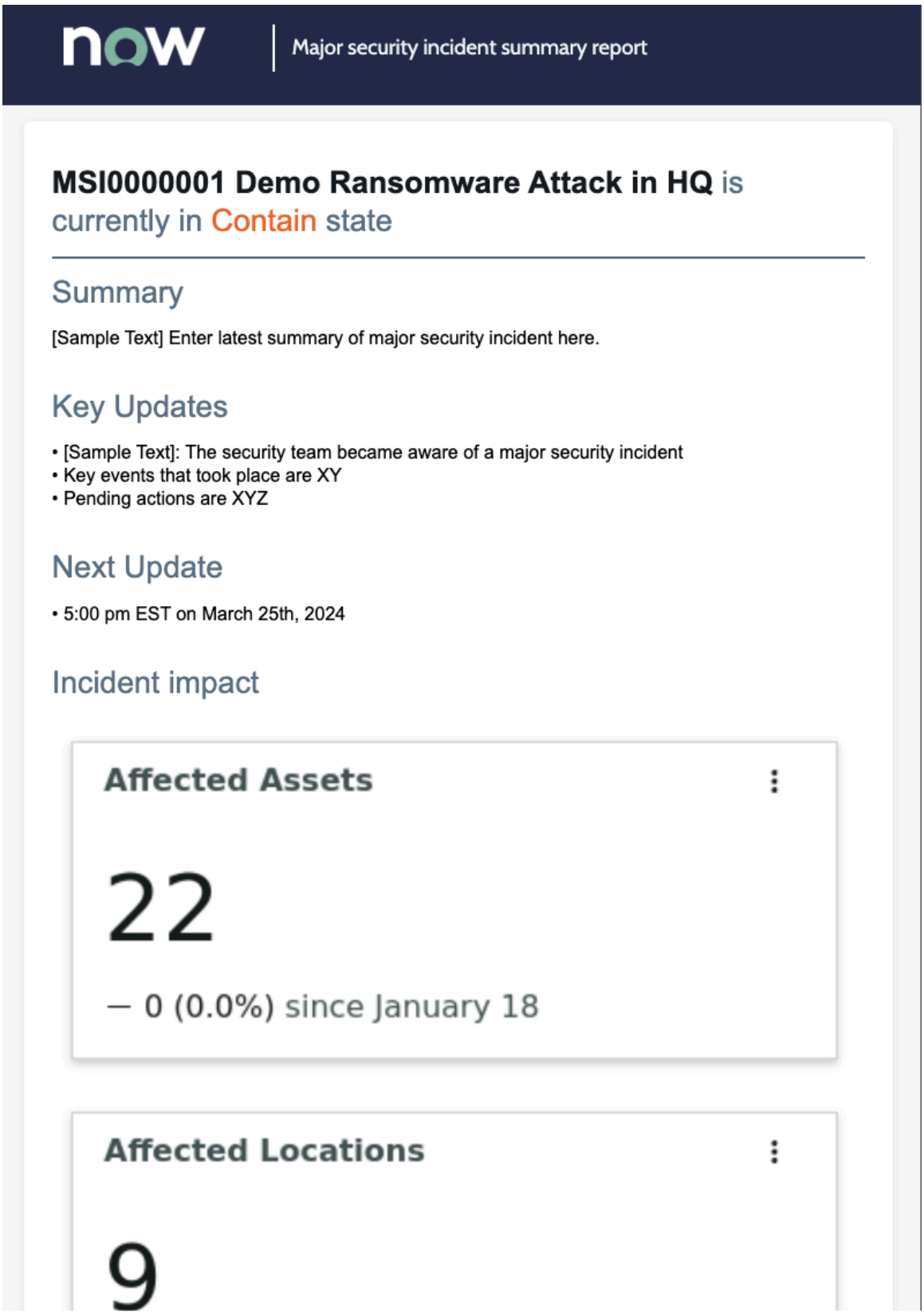
모바일 친화적인 경영진 상태 보고서 - 이메일

경영진 상태 보고서 - 이메일은 이메일 형식으로 생성되는 모바일 친화적인 상태 보고서입니다. 보고서 섹션에는 보고서 요약, MSI 기간 열, 인시던트 범위/영향, 활성 팀 메트릭, 진행률 메트릭 및 타임라인 구성요소(예: 해당 특정 중요 보안 인시던트 기록에 대한 최근 타임라인 이벤트)가 포함됩니다.

다음 보고서 템플릿 기능을 사용자 지정하고 구성하여 보고서에 정보를 추가합니다. 샘플 임원 이메일 상태 보고서는 참조를 위해 아래에 나와 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

경영진 상태 보고서 이메일



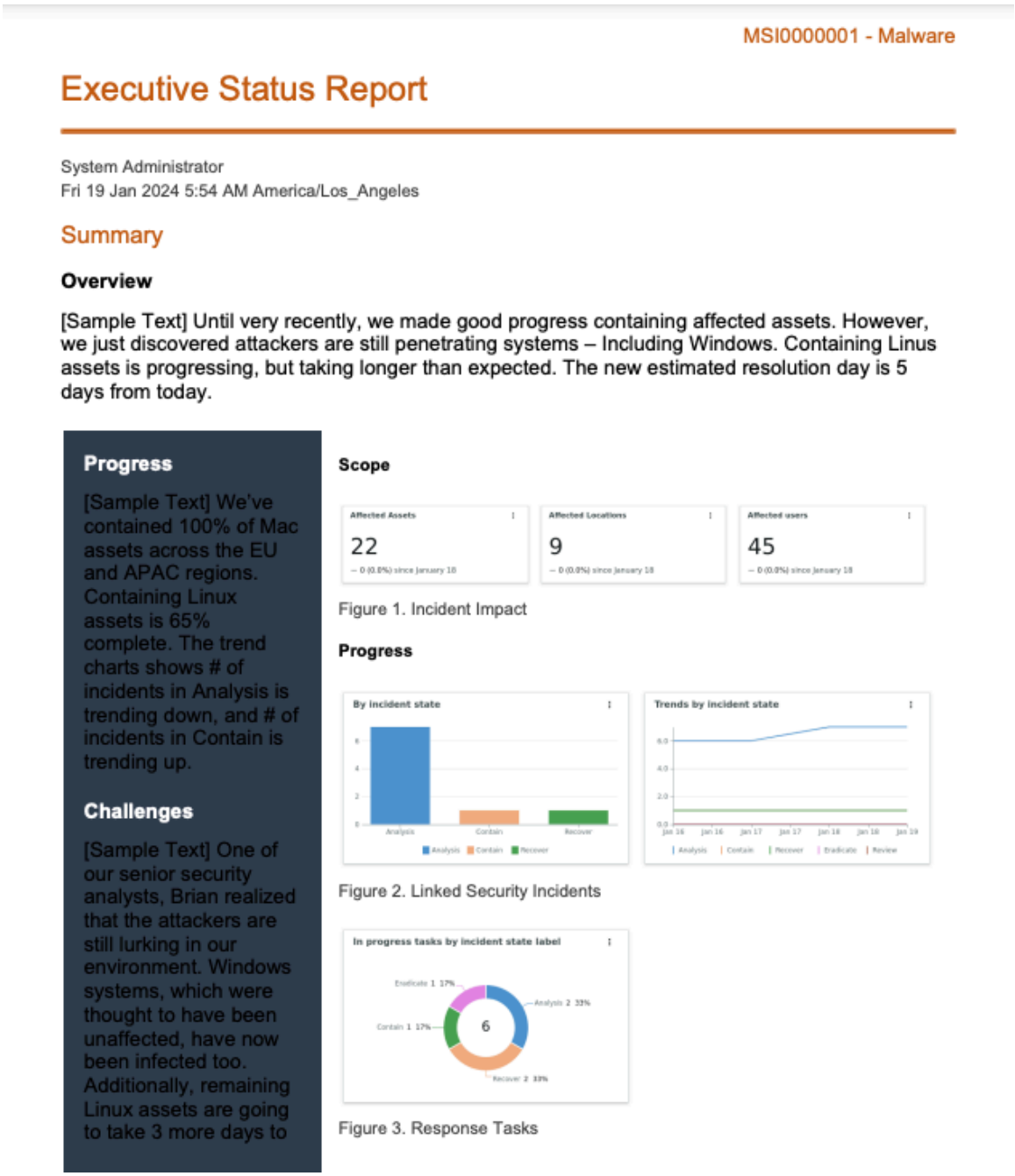
경영진 상태 보고서 **- PDF**

경영진 상태 보고서 - PDF는 PDF 형식으로 생성된 상태 보고서입니다. 보고서 섹션에는 보고서 요약, MSI 기간 열, 인시던트 범위/영향, 활성 팀 메트릭, 진행률 메트릭 및 타임라인 구성요소(예: 해당 특정 중요 보안 인시던트 기록에 대한 최근 타임라인 이벤트)가 포함됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음 보고서 템플릿 기능을 사용자 지정하고 구성하여 보고서에 정보를 추가합니다. 샘플 임원 보고서는 참조를 위해 아래에 나와 있습니다.

경영진 상태 보고서 **PDF**



MSI0000001 - Malware

Executive Status Report

System Administrator
Fri 19 Jan 2024 5:54 AM America/Los_Angeles

Summary

Overview

[Sample Text] Until very recently, we made good progress containing affected assets. However, we just discovered attackers are still penetrating systems – Including Windows. Containing Linus assets is progressing, but taking longer than expected. The new estimated resolution day is 5 days from today.

Progress

[Sample Text] We've contained 100% of Mac assets across the EU and APAC regions. Containing Linux assets is 65% complete. The trend charts shows # of incidents in Analysis is trending down, and # of incidents in Contain is trending up.

Challenges

[Sample Text] One of our senior security analysts, Brian realized that the attackers are still lurking in our environment. Windows systems, which were thought to have been unaffected, have now been infected too. Additionally, remaining Linux assets are going to take 3 more days to

Scope

Affected Assets 22
Affected Locations 9
Affected users 45

Figure 1. Incident Impact

Progress

By incident state
Trends by incident state

Figure 2. Linked Security Incidents

In progress tasks by incident state label
6

Figure 3. Response Tasks

기술 상태 보고서 - **PDF**

기술 상태 보고서 - PDF는 PDF 형식으로 생성된 상태 보고서입니다. 보고서 섹션에는 보고서 요약, MSI 기간 열, 인시던트 범위/영향도, 활성 팀 메트릭, 진행률 메트릭 및 타임라인 구성요소(예: 할당 그룹 및 선택한 태그 레이블을 기준으로 특정 중요 보안 인시던트 기록에 대한 최근 타임라인 이벤트), 레이블이 지정된 작업 업데이트 및 레이블이 지정된 활동이 포함되어 있습니다. 마지막 상태 보고서가 생성된 이후, 인시던트 영향 및 연결된 인시던트와 같은 추가 정보.

보고서 템플릿을 사용자 지정하고 구성하여 보고서에 정보를 추가합니다. 인시던트 영향과 같은 추가 정보를 보여주는 샘플 기술 보고서는 참조를 위해 아래에 설명되어 있으며, 보고서 정보의 나머지 부분은 임원 보고서와 유사합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

MSI0000001 - Malware

System Admins Status Report

System Administrator
Fri 19 Jan 2024 6:00 AM America/Los_Angeles

Summary

Overview

[Sample Text] Until very recently, we made good progress containing affected assets. However, we just discovered attackers are still penetrating systems – Including Windows. Containing Linus assets is progressing, but taking longer than expected. The new estimated resolution day is 5 days from today.

Progress

[Sample Text] We've contained 100% of Mac assets across the EU and APAC regions. Containing Linux assets is 65% complete. The trend charts shows # of incidents in Analysis is trending down, and # of incidents in Contain is trending up.

Challenges

[Sample Text] One of our senior security analysts, Brian realized that the attackers are still lurking in our environment. Windows systems, which were thought to have been unaffected, have now been infected too. Additionally, remaining Linux assets are going to take 3 more days to

Scope

Affected Assets 22
Affected Locations 9
Affected users 45

Figure 1. Incident Impact

Progress

By incident state
Trends by incident state

Figure 2. Linked Security Incidents

Response Tasks by State
In progress tasks by incident state label

보고서 템플릿 섹션에는 다음과 같은 보고서 하위 섹션과 해당 요소를 구성하는 방법을 설명하는 다양한 하위 섹션이 포함되어 있습니다.

1. 브랜딩: 보고서 템플릿에 브랜딩 추가
2. 템플릿 스크립트: 보고서 템플릿에 템플릿 스크립트 사용
3. 보고서 템플릿에서 시각화 사용
4. 보고서 템플릿에서 보고서 목록 사용

보고서 템플릿 생성

중요 보안 인시던트에 적용할 수 있는 다양한 보고서 템플릿을 생성하고 상태 보고서를 생성합니다. 표준 및 사용자 지정 Major Security Incident Response 양식 필드를 닷워킹이 가능한 보고서 템플릿에 추가할 수 있습니다. 또한 섹션, 하위 섹션 및 해당 요소를 사용하여 요구 사항에 따라 보고서의 형식을 지정하고 구성할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

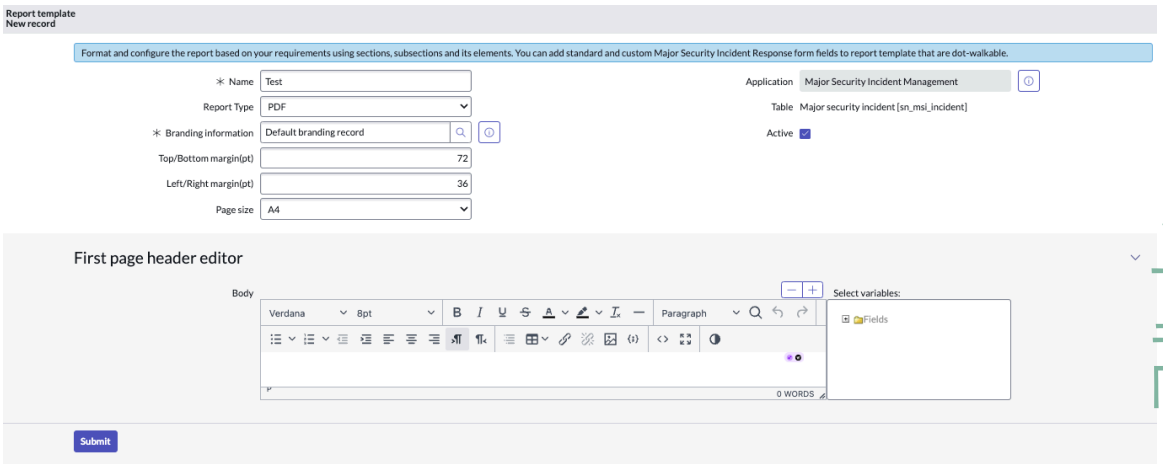
시작하기 전에
필요한 역할: sn_msi.workspace_manager

이 태스크 정보
보고서 템플릿을 위해 보고서 구성요소를 정의하고 추가 정보를 제공할 수 있습니다. 시각화된 데이터를 생성하여 범위 및 진행률 메트릭을 추적하고, 관련 목록 데이터를 추가하고, 상태 보고서를 미리 보고 생성하거나 공유합니다.

프로시저

1. 다음으로 이동 모두 〉 중요 보안 인시던트 관리 〉 **MSI** 관리 〉 상태 보고서 설정.
   MSI 상태 보고서 설정 페이지가 표시됩니다.
2. 보고서 템플릿 섹션에서 구성을 선택합니다.
3. 새로 만들기를 선택하여 보고서 템플릿을 만듭니다.
4. 보고서 템플릿 양식의 필드에 내용을 입력합니다.

보고서 템플릿 생성



5. 새 보고서 템플릿 기록을 제출합니다.
   보고서 템플릿 페이지 아래에 새 보고서 템플릿이 만들어집니다.

관련 정보

상태 보고서 생성 및 배포 MSIM

보고서 템플릿에 브랜딩 추가

보고서에 브랜딩을 추가합니다. 머리글 및 바닥글 이미지, 머리글 및 바닥글 텍스트를 추가할 수 있습니다. 미리 정의된 두 보고서 외에 만들려는 보고서 템플릿 유형에 이 브랜딩 정보를 포함할 수 있습니다.

시작하기 전에
필요한 역할: sn_msi.workspace_manager

이 태스크 정보
보고서 서식 파일에 브랜딩을 추가할 때 고려해야 할 주요 사항은 다음과 같습니다.

- 머리글 및 바닥글 이미지를 업로드하고 이미지 위치를 정렬합니다.
- 머리글 및 바닥글 이미지의 최대 크기 제한은 5MB입니다. 크기가 지정된 한도를 초과하면 '이미지 형식을 인식할 수 없습니다'라는 오류 메시지가 중요 보안 인시던트에 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 머리글 및 바닥글 이미지 높이를 조정합니다.
- 바닥글 텍스트 길이는 100자로 제한됩니다.

프로시저

1. 다음으로 이동 모두 〉 중요 보안 인시던트 관리 〉 **MSI** 관리 〉 상태 보고서 설정.
2. 까지 드릴다운 보고서 템플릿 〉 브랜딩.
3. 구성을 선택합니다.
4. 새로 만들기를 선택하여 보고서 템플릿에 브랜딩을 추가합니다.
5. 브랜딩 템플릿 양식의 필드에 내용을 입력합니다.
6. 제출을 선택합니다.
   브랜딩 템플릿 페이지 아래에 새 브랜딩 템플릿이 만들어집니다.

보고서 템플릿에서 시각화 사용

보고서 위젯을 사용하여 MSIM 상태 보고서에 데이터 시각화와 같은 UIB(User Interface Builder) 요소를 정의하고 포함합니다.

시작하기 전에
필요한 역할: sn_msi.workspace_manager

프로시저

1. 다음으로 이동 모두 〉 중요 보안 인시던트 관리 〉 **MSI** 관리 〉 상태 보고서 설정.
   MSI 상태 보고서 설정 페이지가 표시됩니다.
2. 까지 드릴다운 보고서 템플릿 〉 **Visualizations**.
3. 구성을 선택합니다.
   다음은 기본 시스템의 일부로 미리 정의된 UIB 시각화로, 상태 보고서를 구성하고 수정하는 데 사용할 수 있습니다.

관련 정보

시각화 유형 요소 생성

보고서 템플릿에서 보고서 목록 사용

보고서 목록을 사용하여 관련 목록 아티팩트를 정의하고 포함함으로써 구성된 MSI 목록 기록을 기반으로 PDF에 목록을 생성합니다.

시작하기 전에
필요한 역할: sn_msi.workspace_manager

프로시저

1. 다음으로 이동 중요 보안 인시던트 관리 〉 **MSI** 관리 〉 상태 보고서 설정.
   MSI 상태 보고서 설정 페이지가 표시됩니다.
2. 까지 드릴다운 보고서 템플릿 〉 목록.
3. 구성을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

MSI 상태 보고서 목록 섹션에서는 인시던트가 생성된 이후 각각의 특정 관련 목록이 어떤 영향을 받는지 설명합니다. 다음은 기본 시스템의 일부로 미리 정의된 MSI 보고서 목록으로, 상태 보고서를 구성하고 수정하는 데 사용할 수 있습니다.

관련 정보

목록 유형 요소 생성

보고서 템플릿에 템플릿 스크립트 사용

관련 목록 데이터, 날짜 작업, 그리고 직접적인 닷워킹이 불가능한 모든 기타 데이터를 포함하도록 스크립트를 생성합니다.

시작하기 전에

필요한 역할: sn_msi.workspace_manager

이 태스크 정보

보고서 템플릿에서 이 미리 정의된 템플릿 스크립트를 사용하여 보고서 템플릿을 구성하고 사용자 지정한 후 관련 데이터를 포함할 수 있습니다.

보고서 템플릿에 관련 목록 데이터를 표시하는 템플릿 스크립트를 구성합니다. 템플릿 스크립트를 활용하고 채우려면 태그 템플릿 스크립트 태그를 ${template_script:script name}으로 추가해야 합니다.

예: ${template_script:msi_collab_cards}

주:
미리 정의된 템플릿 스크립트는 삭제할 수 없습니다. 관리자 역할을 가진 사용자가 보고서 템플릿과 매핑된 템플릿 스크립트 기록을 삭제하려고 하면 오류 메시지가 표시됩니다.

프로시저

1. 다음으로 이동 중요 보안 인시던트 관리 > **MSI** 관리 > 상태 보고서 설정.
   MSI 상태 보고서 설정 페이지가 표시됩니다.
2. 까지 드릴다운 보고서 템플릿 > 템플릿 스크립트.
3. 구성을 선택합니다.
   다음은 기본 시스템의 일부로 제공되는 미리 정의된 템플릿 스크립트로, 상태 보고서를 구성하고 수정하는 데 사용할 수 있습니다.

   주:
   나열된 템플릿 스크립트 외에 관련 목록 데이터, 날짜 작업 및 직접적인 닷워킹이 불가능한 기타 데이터를 포함하도록 고유한 템플릿 스크립트를 만들 수도 있습니다.

보고서 템플릿 미리 보기

미리 보기 기능을 사용하여 디자인 타임 보고서 템플릿을 미리 보고 작업 공간에서 런타임 중요 보안 인시던트 관리 중에 보고서를 생성하고 다른 이해 관계자와 공유할 수 있습니다.

시작하기 전에

필요한 역할: sn_msi.workspace_manager

프로시저

1. 다음으로 이동 중요 보안 인시던트 관리 > **MSI** 관리 > 상태 보고서 설정.
   MSI 상태 보고서 설정 페이지가 표시됩니다.
2. 보고서 템플릿 섹션에서 구성을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 원하는 보고서 템플릿을 선택합니다.
4. 요구 사항에 따라 보고서 유형을 이메일 또는 **PDF** 로 선택합니다.
5. 보고서 저장 및 미리 보기 작업을 선택합니다.

   보고서 미리 보기 대화 상자가 표시됩니다.

6. 선택한 템플릿으로 보고서를 미리 보려면 검색 옵션을 사용하여 중요 보안 인시던트를 선택합니다.
7. 보고서 미리 보기를 선택합니다.
   보고서는 선택한 템플릿 구성에 따라 미리 보기를 생성합니다. 보고서 유형을 이메일로 선택한 경우 미리 보기는 이메일 템플릿 형식입니다. 이메일 형식의 상태 보고서는 모바일에 적합합니다.

보고서 섹션 템플릿 생성

보고서는 다양한 섹션으로 더 나눌 수 있습니다. 보고서 섹션을 사용하여 보고서를 여러 섹션으로 나누고 순서대로 재구성합니다.

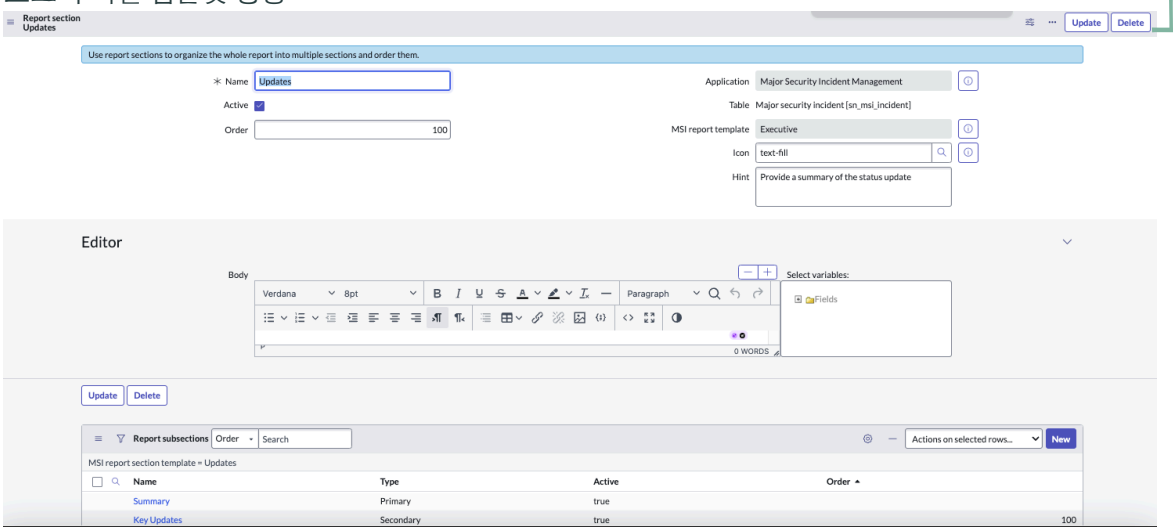
시작하기 전에

필요한 역할: sn_msi.workspace_manager

프로시저

1. 다음으로 이동 중요 보안 인시던트 관리 〉 **MSI** 관리 〉 상태 보고서 설정.
   MSI 상태 보고서 설정 페이지가 표시됩니다.
2. 보고서 템플릿 섹션에서 구성을 선택합니다.
3. 기존 보고서 템플릿을 엽니다.
4. 다음으로 이동 보고서 섹션 〉 신규.
   새 보고서 섹션 페이지가 표시됩니다.

보고서 섹션 템플릿 생성



5. 보고서 섹션 템플릿 양식의 필드에 내용을 입력합니다.
6. 새 보고서 템플릿 섹션을 저장하고 제출 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보고서 하위 섹션 템플릿 생성

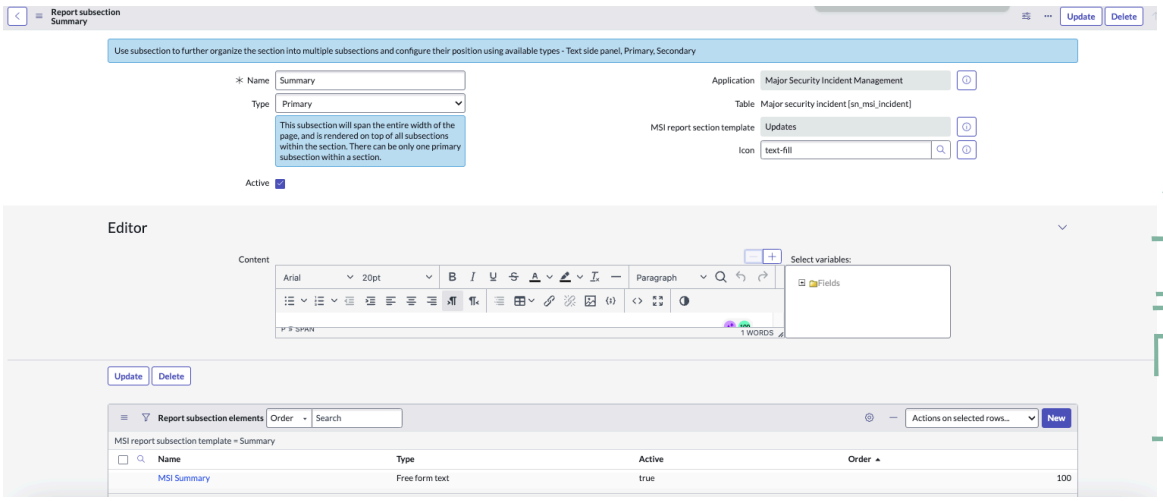
보고서 하위 섹션을 사용하여 섹션을 여러 하위 섹션으로 추가로 구성하고 텍스트 측면 패널, 기본 및 보조와 같은 사용 가능한 유형을 사용하여 정렬 및 위치를 구성합니다.

시작하기 전에
필요한 역할: sn_msi.workspace_manager

프로시저

1. 다음으로 이동 중요 보안 인시던트 관리 〉 **MSI** 관리 〉 상태 보고서 설정.
   MSI 상태 보고서 설정 페이지가 표시됩니다.
2. 보고서 템플릿 섹션에서 구성을 선택합니다.
3. 기존 보고서 템플릿을 열고 해당 보고서 섹션 목록으로 이동합니다.
4. 보고서 섹션 목록에서 기존 보고서 섹션 템플릿을 엽니다.
5. 다음으로 이동 보고서 하위 섹션 〉 신규.

보고서 하위 섹션 템플릿 생성



6. 보고서 하위 섹션 양식의 필드에 내용을 입력합니다.
7. 새 보고서 템플릿 섹션을 저장하고 제출 합니다.

보고서 하위 섹션 생성 요소 템플릿

하위 섹션 요소를 사용하여 하위 섹션을 여러 요소로 추가로 구성합니다. 하위 섹션 요소는 할당 그룹 및 레이블과 같은 필터 옵션을 사용하여 시각화, 목록, 자유 형식 텍스트를 보다 선언적으로 정의하는 데 도움이 됩니다.

시작하기 전에
필요한 역할: sn_msi.workspace_manager

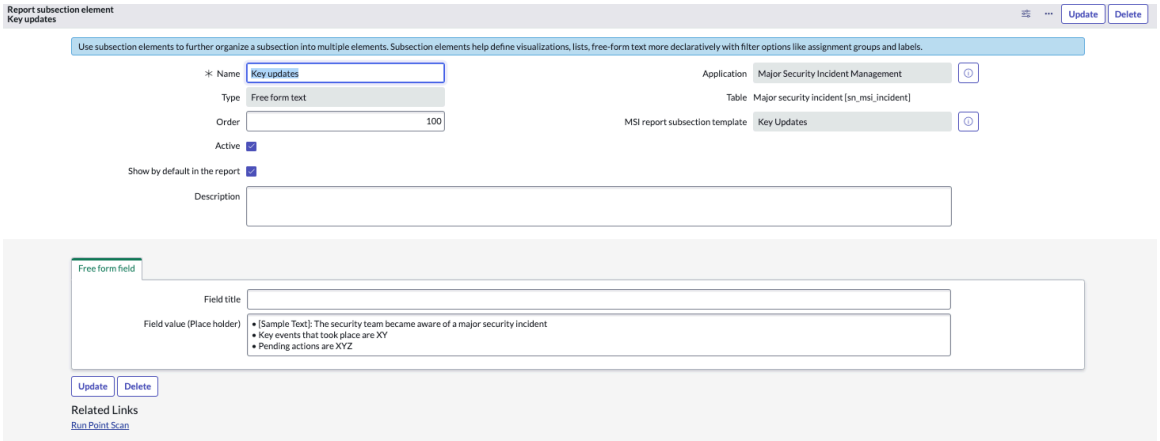
프로시저

1. 다음으로 이동 중요 보안 인시던트 관리 〉 **MSI** 관리 〉 상태 보고서 설정.
   MSI 상태 보고서 설정 페이지가 표시됩니다.
2. 보고서 템플릿 섹션에서 구성을 선택합니다.
3. 기존 보고서 템플릿을 열고 해당 보고서 섹션 목록으로 이동합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 보고서 섹션 목록에서 기존 보고서 섹션 템플릿을 엽니다.
5. 보고서 섹션 템플릿 목록에서 기존 보고서 하위 섹션 템플릿을 엽니다.
6. 다음으로 이동 보고서 하위 섹션 요소 〉 신규.

보고서 하위 섹션 요소 템플릿 생성



7. 보고서 하위 섹션 요소 양식의 필드에 내용을 입력합니다.
8. 새 보고서 템플릿 섹션을 저장하고 업데이트합니다 .

자유 양식 유형 요소 작성

자유 양식 요소 유형을 생성하여 담당 그룹 및 레이블과 같은 필터 옵션을 사용하여 자유 양식 텍스트를 보다 선언적으로 정의합니다.

시작하기 전에
필요한 역할: sn_msi.workspace_manager

프로시저

1. 다음으로 이동 중요 보안 인시던트 관리 〉 **MSI** 관리 〉 상태 보고서 설정.
   MSI 상태 보고서 설정 페이지가 표시됩니다.
2. 보고서 템플릿 섹션에서 구성을 선택합니다.
3. 기존 보고서 템플릿을 열고 해당 보고서 섹션 목록으로 이동합니다.
4. 보고서 섹션 목록에서 기존 보고서 섹션 템플릿을 엽니다.
5. 보고서 섹션 템플릿 목록에서 기존 보고서 하위 섹션 템플릿을 엽니다.
6. 다음으로 이동 보고서 하위 섹션 요소 〉 신규.
7. 에 설명된 보고서 하위 섹션 생성 요소 템플릿대로 필요한 세부 정보로 보고서 하위 섹션 요소 양식을 채웁니다.
8. 보고서 하위 섹션 요소 유형 필드로 이동하여 자유 양식 필드 옵션을 선택합니다.
   그러면 자유 양식 필드 섹션이 표시됩니다.
9. 자유 양식 탭의 필드에 내용을 입력합니다.

시각화 유형 요소 생성

시각화 요소 유형을 생성하여 할당 그룹 및 레이블과 같은 필터 옵션을 사용하여 시각화 요소를 보다 선언적으로 정의합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

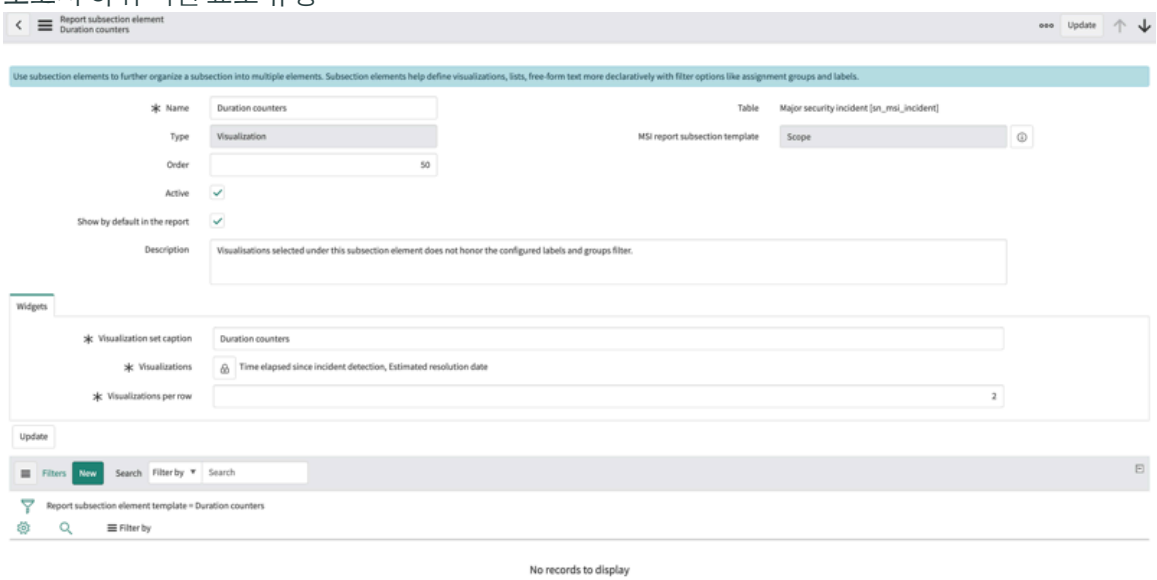
시작하기 전에
필요한 역할: sn_msi.workspace_manager

프로시저

1. 다음으로 이동 중요 보안 인시던트 관리 〉 **MSI** 관리 〉 상태 보고서 설정.
   MSI 상태 보고서 설정 페이지가 표시됩니다.
2. 보고서 템플릿 섹션에서 구성을 선택합니다.
3. 기존 보고서 템플릿을 열고 해당 보고서 섹션 목록으로 이동합니다.
4. 보고서 섹션 목록에서 기존 보고서 섹션 템플릿을 엽니다.
5. 보고서 섹션 템플릿 목록에서 기존 보고서 하위 섹션 템플릿을 엽니다.
6. 다음으로 이동 보고서 하위 섹션 요소 〉 신규.
7. 에 설명된 보고서 하위 섹션 생성 요소 템플릿대로 필요한 세부 정보로 보고서 하위 섹션 요소 양식을 채웁니다.
8. 보고서 하위 섹션 요소 유형 필드로 이동하여 시각화 옵션을 선택합니다.
   시각화 섹션이 표시됩니다.
9. 시각화 양식의 필드에 내용을 입력합니다.
10. 제출을 선택합니다.

Example: 보고서 템플릿 기술 상태 보고서에 대한 하위 섹션 요소 유형

보고서 하위 섹션 요소 유형



목록 유형 요소 생성

할당 그룹 및 레이블과 같은 필터 옵션을 사용하여 관련 목록 요소를 선언적으로 정의하는 목록 유형 요소를 생성합니다.

시작하기 전에
필요한 역할: sn_msi.workspace_manager

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 중요 보안 인시던트 관리 〉 **MSI** 관리 〉 상태 보고서 설정.
   MSI 상태 보고서 설정 페이지가 표시됩니다.
2. 보고서 템플릿 섹션에서 구성을 선택합니다.
3. 기존 보고서 템플릿을 열고 해당 보고서 섹션 목록으로 이동합니다.
4. 보고서 섹션 목록에서 기존 보고서 섹션 템플릿을 엽니다.
5. 보고서 섹션 템플릿 목록에서 기존 보고서 하위 섹션 템플릿을 엽니다.
6. 다음으로 이동 보고서 하위 섹션 요소 〉 신규.
7. 에 설명된 보고서 하위 섹션 생성 요소 템플릿대로 필요한 세부 정보로 보고서 하위 섹션 요소 양식을 채웁니다.
8. 보고서 하위 섹션 요소 유형 필드로 이동하여 목록 옵션을 선택합니다.
   목록 섹션이 표시됩니다.
9. 목록 양식의 필드에 내용을 입력합니다.

사용자 지정 유형 요소 만들기

할당 그룹 및 레이블과 같은 필터 옵션을 사용하여 관련 목록 요소를 선언적으로 정의하는 목록 유형 요소를 생성합니다.

시작하기 전에
필요한 역할: sn_msi.workspace_manager

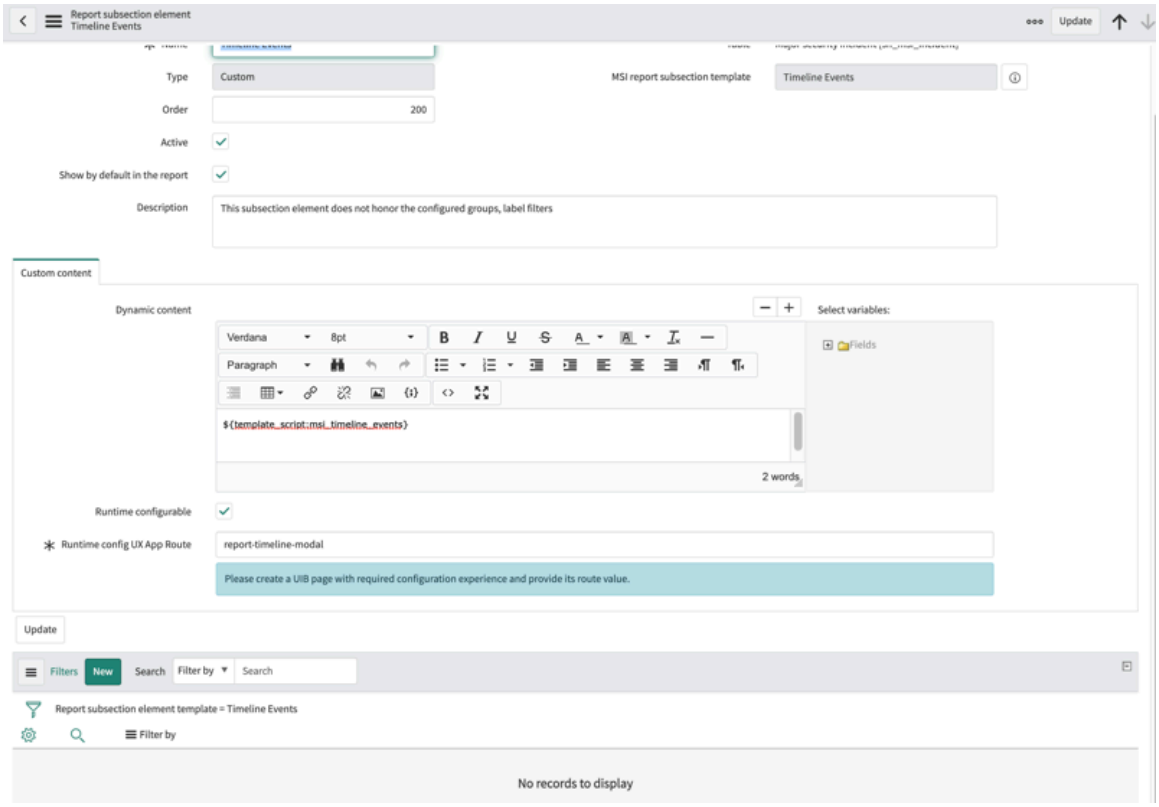
프로시저

1. 다음으로 이동 중요 보안 인시던트 관리 〉 **MSI** 관리 〉 상태 보고서 설정.
   MSI 상태 보고서 설정 페이지가 표시됩니다.
2. 보고서 템플릿 섹션에서 구성을 선택합니다.
3. 기존 보고서 템플릿을 열고 해당 보고서 섹션 목록으로 이동합니다.
4. 보고서 섹션 목록에서 기존 보고서 섹션 템플릿을 엽니다.
5. 보고서 섹션 템플릿 목록에서 기존 보고서 하위 섹션 템플릿을 엽니다.
6. 다음으로 이동 보고서 하위 섹션 요소 〉 신규.
7. 에 설명된 보고서 하위 섹션 생성 요소 템플릿대로 필요한 세부 정보로 보고서 하위 섹션 요소 양식을 채웁니다.
8. 보고서 하위 섹션 요소 유형 필드로 이동하여 사용자 지정 옵션을 선택합니다.
   그러면 사용자 지정 콘텐츠 섹션이 표시됩니다.
9. 사용자 지정 컨텐츠 양식의 필드에 내용을 입력합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Example: 다음은 기술 상태 보고서에 대한 보고서 템플릿 하위 섹션 요소 유형의 예입니다

보고서 하위 섹션 요소 유형



시스템 속성 추가

MSIM 응용 프로그램 동작을 제어하는 시스템 속성을 추가합니다. 다음은 상태 보고서의 일부로 중요 보안 인시던트 관리 도입되는 기본 시스템 속성입니다.

시스템 속성

속성 이름	설명
sn_msi.export_img	이 속성을 사용하여 이미지 익스포트를 제어합니다. 기본값은 ON으로 설정됩니다.
sn_msi.export_img_log	이 속성을 사용하여 브라우저 콘솔에 로그인할 수 있습니다. 기본값은 OFF로 설정되어 있습니다.
sn_msi.export_img_parallel_threshold	이 속성을 사용하여 보고서 위젯 구성에서 이미지를 생성하기 위한 최대 병렬 요청 수를 제어합니다. 기본값은 14로 설정됩니다.
sn_msi.img_export_log	이 속성을 사용하여 브라우저에서 콘솔 로그를 활성화합니다.
sn_msi.img_export_poll_interval	이 속성을 사용하여 이미지가 생성되는지 여부를 확인하는 폴링 간 시간 간격을 제어합니다. 기본 폴링 간격 시간은 3000밀리초로 설정됩니다.
sn_msi.export_poll_request_timeout	이 속성을 사용하여 시스템에서 익스포트한 이미지를 폴링할 수 있는 최대 시간을 제어합니다. 기본값은 120000밀리초입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시스템 속성

속성 이름	설명
sn_msi.msi_report_uib_element_js_path	이 속성을 사용하여 UIB 페이지 부분에서 이미지를 캡처할 일반 경로를 제어합니다.
sn_msi.report_default_style_objects	이 속성을 사용하여 글꼴 크기, 글꼴 색상 또는 필드 값과 같은 생성된 PDF의 CSS를 변경합니다. 예를 들어, sn_msi.workspace_manager가 생성된 PDF 상태 보고서의 왼쪽 패널 글꼴 색상을 변경하려는 경우 작업 공간 관리자는 시스템 속성 글꼴 색상을 수정하고 원하는 뷰에서 PDF를 렌더링할 수 있습니다.

중요 보안 인시던트 관리 플레이북

Major Security Incident Management 플레이북 플로우를 자동 또는 수동으로 호출할 수 있습니다.

플레이북은 하나 이상의 플레이북이 보안 인시던트와 연결된 경우에만 표시됩니다. 플레이북 구성요소는 빌드된 PAD(프로세스 자동화 디자이너)에 대해서만 지원됩니다. Major Security Incident Management는 법무 요청 플레이북에 기본 시스템을 제공합니다.

법무 요청을 위한 플레이북

법무 요청 플레이북은 중대한 위반에 필요한 4일 이내에 SEC에 알릴 수 있도록 MSI의 최신 요약에 대해 법무팀에 알릴 수 있는 방법에 대한 단계별 지침을 제공합니다.

개요

인시던트 관리자는 법무 요청 플레이북을 사용하여 MSI의 최신 요약을 법무 팀에 알릴 수 있으므로 법무 팀이 중대한 위반에 대해 SEC에 알릴 수 있습니다. PAD(프로세스 자동화 디자이너) 템플릿을 사용하여 법무 요청 플레이북의 단계를 수행하고 그에 따라 법무 팀에 알릴 수 있습니다.

이 플레이북은 중요 보안 인시던트가 생성되거나 업데이트되는 경우에 사용할 수 있습니다. PAD에서 법무 요청 플레이북을 활성화한 다음 분석, 포함, 근절 및 검토와 같은 모든 작업을 수행해야 합니다.

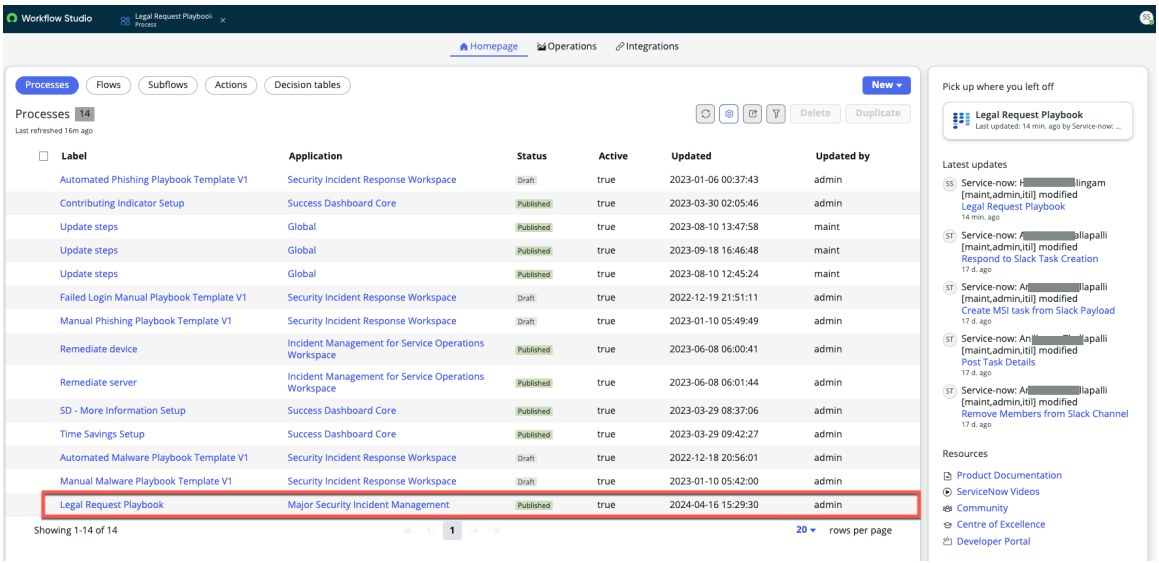
다음은 프로세스 정의의 레인이며 중요 보안 인시던트 상태에 해당합니다.

- 분석
- 포함
- 근절
- 검토

각 레인에는 특정 활동이 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

법무 요청을 위한 플레이북



레인에서 작업을 완료로 표시하면 다음 작업으로 이동할 수 있습니다. 언제든지 작업을 저장하고 나중에 날짜 및 시간에 플레이북으로 돌아갈 수 있습니다. 레인의 모든 작업을 완료한 후 다음 레인으로 이동할 수 있습니다. 작업과 레인을 계속 완료하면 상태가 왼쪽 패널에 반영됩니다. 플레이북 오른쪽에 있는 활동 로그에는 각 작업에 대해 입력한 모든 데이터가 표시됩니다.

모든 작업을 완료한 후에는 모든 레인에 입력한 상세 정보를 검토하라는 메시지가 표시됩니다. 필드를 편집하거나 마침 을 선택하여 권리를 생성하는 프로세스를 완료할 수 있습니다.

법무 요청 Playbook에 대한 프로세스 생성

다음 단계를 사용하여 PAD(프로세스 자동화 디자이너)에서 법무 요청 플레이북에 대한 프로세스를 생성합니다.

시작하기 전에
필요한 역할: sn_msi.workspace_manager.

프로시저

1. 클릭 **ALL** 〉 프로세스 자동화 디자이너 〉 〉 새 프로세스 작성.

   (예: 법무 요청 플레이북)

2. 프로세스의 이름, 설명 및 프로세스를 생성할 애플리케이션을 입력합니다.
3. 트리거 선택을 클릭합니다.
4. 프로세스가 실행되는 시기에 대한 고유한 조건 정의를 선택하고 프로세스를 실행해야 하는 시기에 대한 트리거 조건을 선택합니다.
5. 트리거 조건 설정을 클릭합니다.
6. 테이블을 선택하고 조건을 입력하여 프로세스를 실행해야 하는 시기를 정의하는 조건을 선택합니다.
7. 디자이너로 이동을 클릭합니다.
   Process Automation Designer 페이지가 열립니다.
8. 자동화된 프로세스 설계를 시작하려면 새 레인 추가를 클릭합니다.
   UI 오른쪽에 레인 속성 창이 열립니다.
9. 레인 속성 창에서 이름, 설명, 실행 조건, 시작 시기 표시에 대한 상세 정보를 입력합니다.
   실행 조건 및 시작 시기 표시 필드는 차선이 실행되는 시기를 의미합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

10. 저장 후 닫기를 클릭합니다.
11. 다른 레인을 추가하려면 다른 레인 추가를 클릭합니다.
    마찬가지로 원하는 만큼 레인을 만들 수 있습니다. 이 예에서는 각각 분석, 포함, 근절 및 검토에 대한 레인을 만들 수 있습니다. 다음 예시에서는 분석 레인이 즉시 시작되며 실행 조건이 없습니다. 이전 레인이 완료된 후 레인 시작을 포함하며 이전 레인의 활동 결과를 기반으로 하는 실행 조건이 있습니다.
    레인을 추가한 후에는 각 레인에 대한 프로세스 활동을 추가해야 합니다.
12. 특정 레인(예: 분석 레인)에서 다른 프로세스 활동 추가를 클릭합니다.
    활동 추가 팝업이 열립니다.
    a. 활동 추가 팝업에서 필요한 활동 정의를 선택합니다.
13. 새 활동 만들기를 클릭합니다.
    활동 정의가 추가된 후 레인과 유사하게 추가로 구성할 수 있습니다. 마찬가지로 각 레인 아래에 다른 프로세스 활동을 생성할 수 있습니다.
14. 활동 속성 창에서 실행 조건을 추가하고 프로세스 활동을 시작할 시기를 나타냅니다.
15. 실행 조건을 추가하고 시작 시기를 나타냅니다.
    이 활동에 필요한 모든 입력(구성된 자동화 계획의 입력 포함)이 표시됩니다. 값을 재정의하거나 미리 구성된 값을 사용할 수 있습니다.
16. 모든 속성 보기를 클릭하고 고급 속성 토글을 활성화하여 활동 정의의 모든 활동 경험 필드를 표시합니다.

법무 요청 플레이북 사용

다음 단계를 사용하여 MSIM 작업 공간에서 법무 요청 플레이북을 사용하는 방법과 그 역량을 알아봅니다.

시작하기 전에

필요한 역할: sn_msi.workspace_manager.

프로시저

1. MSIM 작업 공간에서 중요 보안 인시던트를 엽니다.
2. 플레이북 탭을 선택합니다.

   중요 보안 인시던트에 대해 활성화된 플레이북을 볼 수 있습니다.

   > **주:**
   > 나열된 플레이북이 표시되지 않으면 PAD로 이동하여 플레이북 탭에서 볼 수 있도록 해야 합니다.

3. 법무 요청 플레이북을 선택합니다.
4. 각 레인을 클릭하여 이 플레이북에서 어떤 작업을 수행했는지 확인합니다.
5. 분석을 클릭하여 분석 단계에서 수행된 활동 목록을 봅니다.
   요구 사항에 따라 변경할 수 있습니다.
6. 마찬가지로 포함, 근절 및 검토를 클릭하여 각 단계에서 수행된 활동 목록을 볼 수 있습니다.
   요구 사항에 따라 변경할 수 있습니다. 수행해야 하는 나머지 활동 또는 사용자 작업이 있는 경우 해당 단계에 표시됩니다.
7. 단계에 필요한 나머지 활동 또는 사용자 작업이 있는 경우 해당 단계를 클릭하고 작업을 수행하여 활동을 완료합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

용 롤업 프레임워크 **MSIM**

작업 공간에서 소스 기록을 중요 보안 인시던트 관리 연결하는 기능을 확장합니다.

개요

롤업 프레임워크를 사용하면 롤업 플로우를 구성 및 확장할 수 있습니다. 이 프레임워크 모델을 사용하여 중요 보안 인시던트로 롤업할 수 있는 정보를 구성합니다.

이전에 sn_msi.workspace_manager는 로 제안되거나 승격 MSI된 보안 인시던트와 취약한 항목을 연결할 수 있었습니다. 보안 인시던트 또는 취약한 항목을 연결한 후 정보가 중요 보안 인시던트로 롤업되었습니다. 롤업해야 하는 정보 유형은 스크립트에 하드 코딩되어 있습니다.

프레임워크 모델을 사용하여 롤업 플로우를 구성할 수 있으며, 롤업 플로우는 다음 기능을 지원하고 애플리케이션의 기존 문제를 해결합니다.

롤업 프레임워크 모델을 사용하면 sn_msi.workspace_manager를 사용할 수 있으며 다음과 같은 이점이 있습니다.

- 테이블에서 연결 기록 기능을 추가하거나 제거하거나, 제안 또는 승격 MSI 하여 작업 테이블을 확장합니다.
- 인시던트 기록에 대한 링크/제안/승격 등의 작업을 수행하는 동안 롤업 MSI 할 정보의 유형을 제어합니다.
- 클래식 환경 및 중요 보안 인시던트 관리 작업 공간 모두에서 보안 인시던트, 정정 작업 및 보안 케이스(OOTB)에 대한 연결, 제안 또는 승격을 지원합니다.

롤업 프레임워크는 다음 테이블에 설명된 대로 구성을 표시합니다.

롤업 프레임워크 구성

이름	설명
연결된 기록 구성	에 연결/승격/제안 중요 보안 인시던트하는 데 사용할 수 있는 작업 테이블 정보를 저장합니다.
롤업 기록 구성	연결/승격/제안 작업이 수행될 때 작업 테이블에서 롤업할 수 있는 정보를 캡처합니다.
목록 레이아웃 구성	작업 공간 탭에 표시된 것처럼 다양한 테이블의 레이블과 목록 레이아웃(중요 보안 인시던트 관리 예: 인시던트 영향, 연결된 기록 및 위협 인텔리전스.

에서 연결된 기록 구성 중요 보안 인시던트 관리

연결된 기록 구성을 사용하여 . 연결/승격/제안 중요 보안 인시던트하는 데 사용할 수 있는 작업 테이블 정보를 저장합니다.

필요한 역할: admin 및 sn_msi.workspace_admin

주:
관리자는 기록을 생성할 수 있으며 MSIM 작업 공간 관리자는 기록을 업데이트할 수 있습니다.

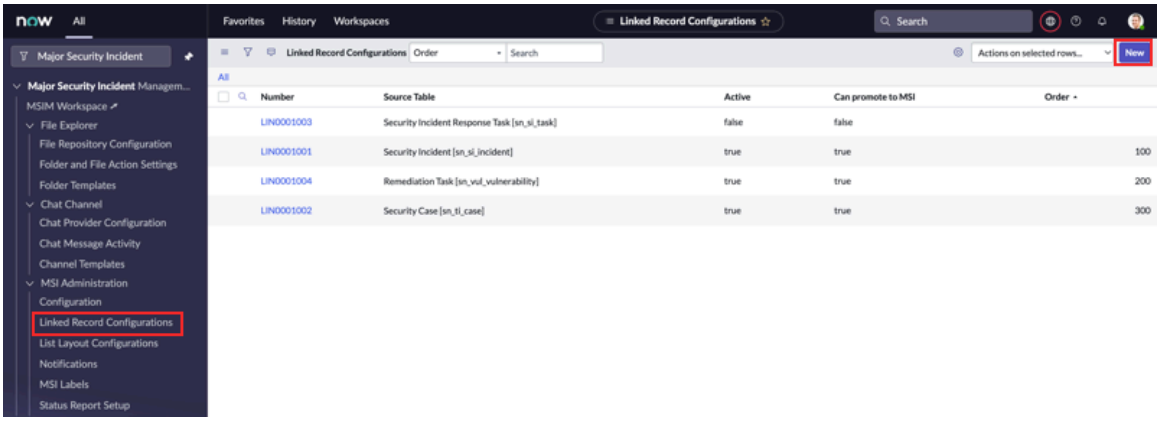
절차

1. 다음으로 이동 중요 보안 인시던트 관리 〉 연결된 기록 구성.

   연결된 기록 구성 페이지가 표시됩니다.

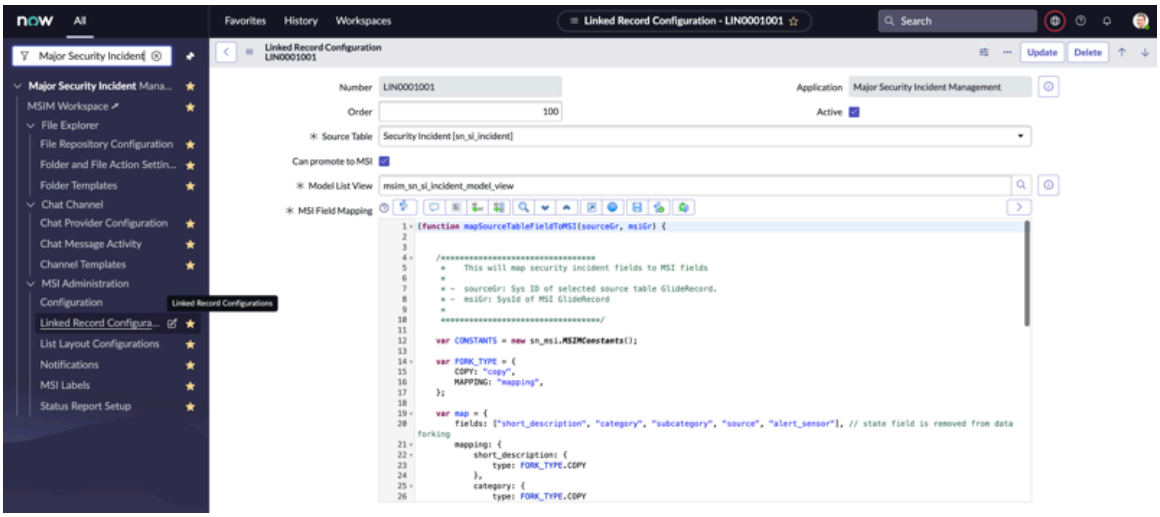
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

연결된 기록 구성



2. 연결된 기록 구성 페이지에서 새로 만들기를 클릭합니다

주:
애플리케이션이 범위 내에 중요 보안 인시던트 관리 있는지 확인합니다.



3. 기록 구성 양식의 필드에 내용을 입력합니다.

연결된 기록 필드 설명

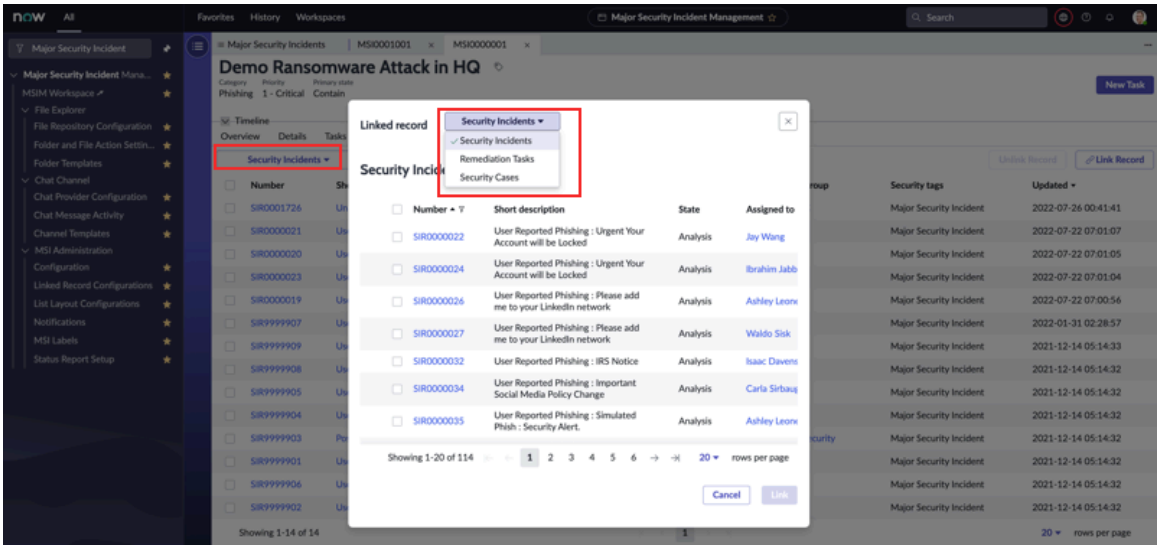
필드	설명
소스 테이블	연결되고 롤업 중요 보안 인시던트되어야 하는 작업 테이블을 나타냅니다.
순서	MSIM 작업 공간 드롭다운에서 현재 소스 테이블의 순서를 제어할 수 있습니다. 다음은 주문의 예입니다. 이 표 다음에 제공되는 아래 이미지 1을 참조하십시오.
모델 ListView	연결된 기록 모달 목록에 표시되는 목록 레이아웃을 제어할 수 있는 뷰를 선택하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

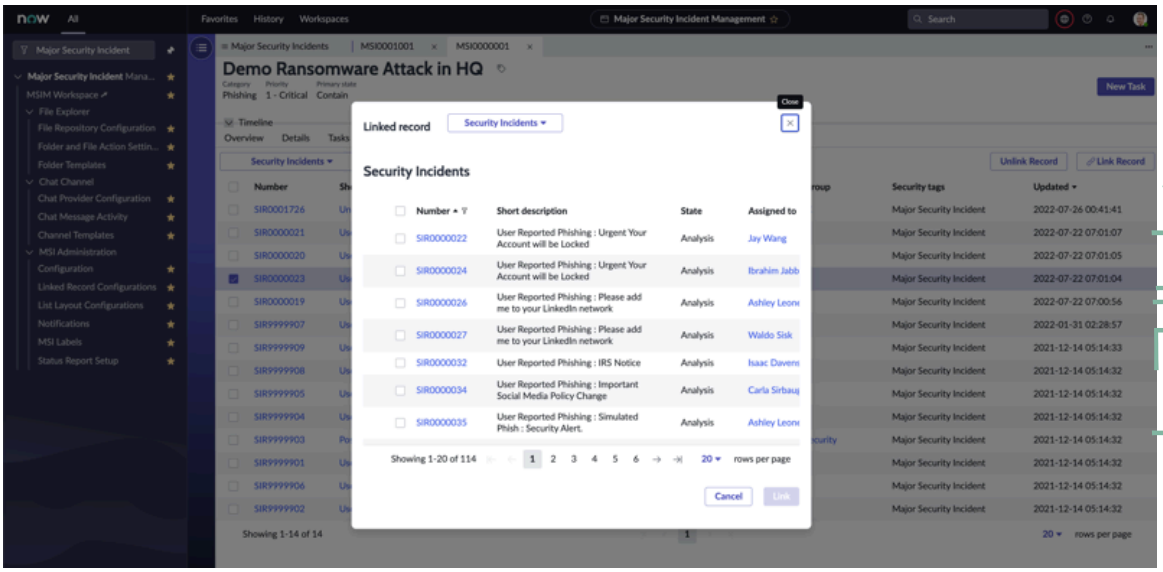
필드	설명
다음으로 승격할 수 있음 MSI	이 확인란을 선택하여 기록이 기본 기록인지 확인합니다. 다음은 MSI로 승격할 수 있음 옵션 선택의 예입니다. 이 표 다음에 나오는 다음 이미지 2를 참조하십시오. 이 확인란이 선택되어 있고 값이 true일 경우: ○ 추가 구성과 함께 클래식 환경 작업을 사용하도록 소스 기록을 중요 보안 인시던트 직접 제안하고 승격할 수 있습니다. ○ 클래식 환경과 MSIM 작업 공간 모두에서 소스 기록을 중요 보안 인시던트에 연결할 수 있습니다. ○ 중요 보안 인시던트 관리 작업 공간 연결된 기록 페이지에 연결된 소스 테이블 기록이 표시됩니다. **주:** 기록을 로 직접 제안/승격할 중요 보안 인시던트수 있는 경우 해당 기록이 기본 기록입니다. 예를 들어 보안 응답 작업 테이블 구성에서 보안 응답 작업을 중요 보안 인시던트에 직접 승격할 수 없으므로 MSI로 승격할 수 있음의 값은 false입니다. 따라서 작업 공간 연결된 기록 탭 드롭다운 목록에 표시되지 MSIM 않습니다.
MSI 필드 매핑	소스 테이블 기록이 제안 또는 승격되는 중일 때 소스 기록 필드를 새로 생성된 중요 보안 인시던트에 매핑하는 스크립트를 작성합니다. 이 스크립트는 MSI로 승격할 수 있음 값이 예인 경우에만 실행됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이미지 **1:** 연결된 기록 목록 보기 순서



이미지 **2:** MSI로 승격 가능



에서 롤업 기록 구성 중요 보안 인시던트 관리

정보를 제어하도록 롤업 기록을 중요 보안 인시던트 관리 구성하면 소스 기록이 중요 보안 인시던트로 연결/제안/승격될 때 롤업됩니다.

필요한 역할: admin 및 sn_msi.workspace_admin

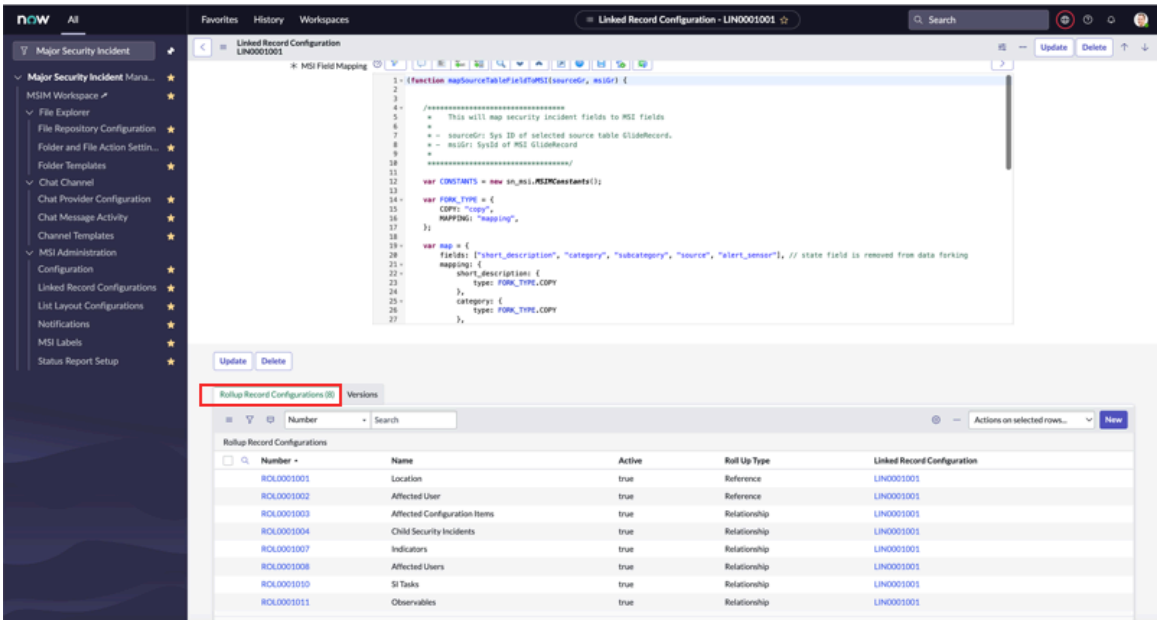
주:
시스템 관리자는 기록을 생성할 수 있으며 MSI 작업 공간 관리자는 업데이트할 수 있습니다.

절차

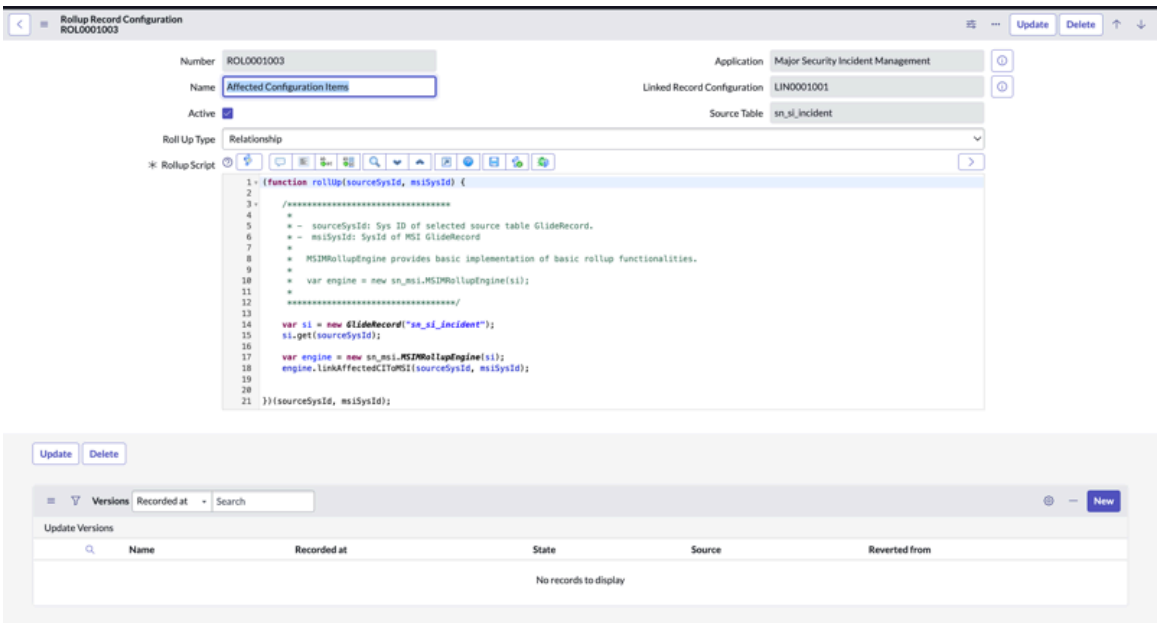
1. 다음으로 이동 중요 보안 인시던트 응답 〉 연결된 기록 구성. 연결된 기록 구성 페이지가 표시됩니다.
2. 새 연결된 기록을 선택하거나 생성하고 같은 페이지에서 기록 구성 롤업 섹션으로 이동합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

롤업 기록 구성 섹션



3. 새로 만들기를 클릭합니다.



4. 구성 페이지에서 상세 정보를 입력합니다.

롤업 기록 구성

필드 이름	필드 설명
이름	롤업 기록의 이름을 나타냅니다.
활성	소스 기록의 롤업이 발생할 때 현재 구성을 구현하려면 이 확인란을 선택합니다.
연결된 기록 구성	상위 연결된 기록 구성을 나타내며 읽기 전용인 고유 번호를 나타냅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드 이름	필드 설명
소스 테이블	연결된 기록 구성에 사용되는 소스 테이블 이름으로, 읽기 전용입니다.
롤업 유형	롤업해야 하는 정보의 유형을 설명합니다. ○ 관계: 데이터를 관련 목록으로 표시해야 하는 경우 이 옵션을 선택합니다. ○ 참조: 데이터가 소스 테이블 양식에 참조 필드로 존재하는 경우 이 옵션을 선택합니다.
롤업 스크립트	롤업 유형이 관계인 경우 롤업 스크립트 필드가 활성화되어 스크립트를 작성하고 정보를 롤업하는 데 사용할 수 있습니다. 여기서 스크립트는 소스 기록과 중요 보안 인시던트에 대한 정보가 포함된 입력을 수신합니다. 스크립트는 관계 테이블에서 정보를 찾고 sn_msi_m2m_child(연결된 기록) 테이블로 롤업할 수 있어야 합니다.
소스 필드	롤업 유형이 참조인 경우 소스 필드를 사용할 수 있습니다. 이렇게 하면 롤업해야 하는 정보가 포함된 소스 테이블 참조 필드를 선택할 수 있습니다.
대상 필드	롤업 유형이 참조인 경우 대상 필드를 사용할 수 있습니다. 이렇게 하면 연결된 기록(sn_msi_m2m_child) 테이블의 필드를 참조할 수 있으며 선택한 소스 필드와 소스 테이블 기록에 있는 데이터를 저장할 수 있습니다.

롤업을 위한 스크립트 작성

이름	설명
입력	• sourceSysId: 연결/제안/승격되는 소스 테이블 기록의 시스템 ID입니다. • msiSysId: 소스 기록이 연결/제안/승격되는 중요 보안 인시던트의 시스템 ID입니다.
출력	출력 반환 값이 없습니다.
책임	스크립트는 연결된 기록(sn_msi_m2m_child) 테이블에 정보를 롤업해야 합니다. • sourceSysID를 사용하여 관계 테이블에서 ServiceNow 데이터를 쿼리합니다. • 데이터를 가져온 후 MSIRollupEngine 유틸리티를 사용하여 데이터를 sn_msi_m2m_child(연결된 기록)에 롤업하여 데이터를 롤업합니다.

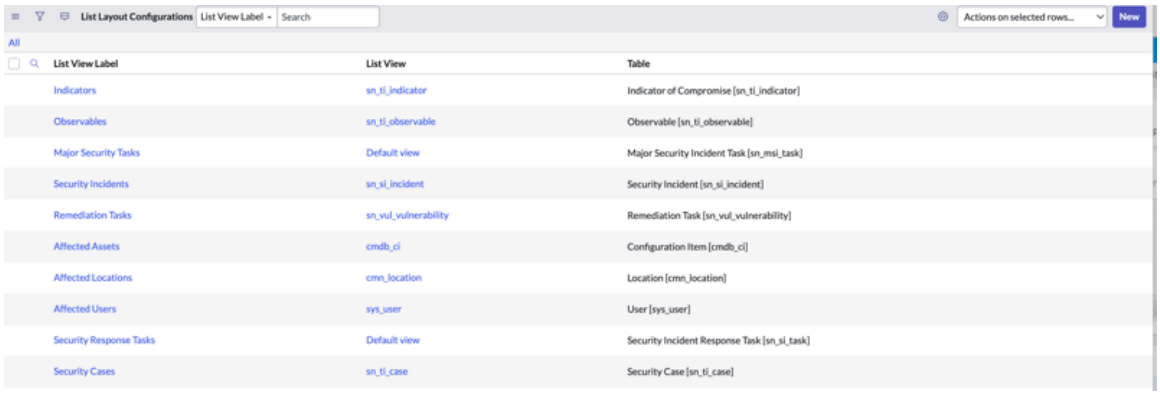
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

에서 목록 레이아웃 구성 중요 보안 인시던트 관리

인시던트 영향, 연결된 기록 및 위협 인텔리전스 탭과 같은 작업 공간에 사용되는 중요 보안 인시던트 관리 레이아웃과 레이블을 사용자 지정하도록 목록 레이아웃을 구성합니다.

필요한 역할: admin 및 sn_msi.workspace_admin

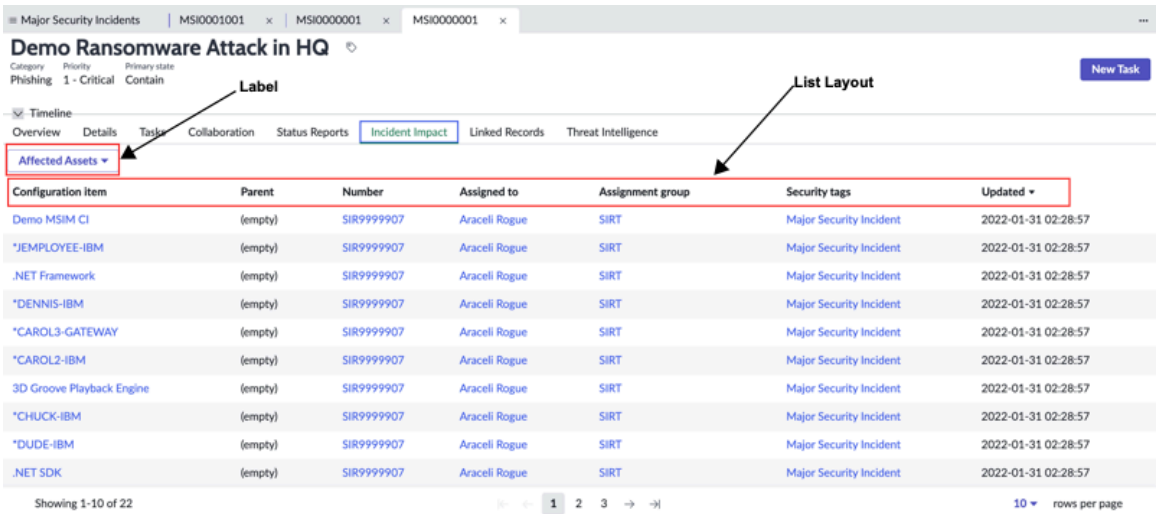
주:
시스템 관리자는 기록을 생성할 수 있으며 MSI 작업 공간 관리자는 업데이트할 수 있습니다.



작업 공간에 표시된 중요 보안 인시던트 관리 기존 알려진 테이블에 대해 목록 레이아웃 구성이 이미 제공되었습니다.

주:

- 기존 테이블에 대한 사용자 지정 뷰를 렌더링하려면 사용자 지정 목록 뷰를 사용하여 목록 레이아웃 구성에서 해당 테이블 기록을 업데이트할 수 있습니다.
- 새 작업 테이블의 경우 새 목록 레이아웃 구성을 생성하여 사용자 지정 목록 뷰와 레이블을 렌더링할 수 있습니다. 자세한 절차는 다음 방법을 참조하십시오. 4 단계. 보안 케이스에 대한 새 연결된 기록 탭에 대한 뷰 생성



보안 케이스에 대한 사용 사례 구현 롤업 예시

다음 단계에서는 보안 케이스 테이블에 대한 중요 보안 인시던트를 연결/제안/승격하기 위한 지원을 추가하는 방법에 대한 사용 사례 예를 설명합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 1 단계. 보안 케이스에 대한 연결 기록 구성 만들기
- 2 단계. 보안 케이스에 대한 모달 창 뷰 생성
- 3 단계. 보안 케이스의 소스 테이블에 대한 UI 작업 생성
- 4 단계. 보안 케이스에 대한 새 연결된 기록 탭에 대한 뷰 생성
- 5 단계. 작업 공간 사용자에 대한 중요 보안 인시던트 관리 접근 제어 목록(ACL) 추가
- 6 단계. 보안 케이스에 대한 비즈니스 규칙 생성
- 7 단계. 롤업 기록 구성 작성

1 단계. 보안 케이스에 대한 연결 기록 구성 만들기

보안 케이스에 대한 연결된 기록 구성을 만듭니다.

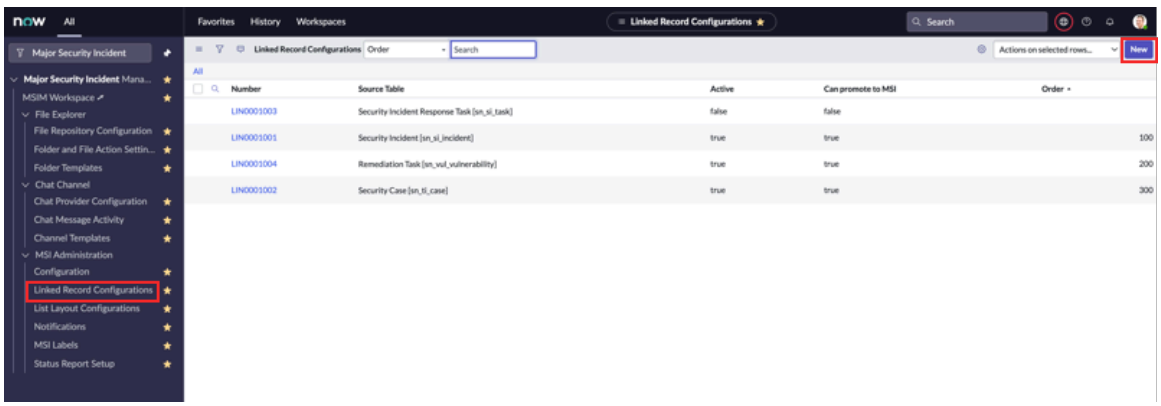
시작하기 전에
필요한 역할: admin 및 sn_msi.workspace_admin

> **주:**
> 시스템 관리자는 기록을 생성할 수 있으며 MSI 작업 공간 관리자는 업데이트할 수 있습니다.

프로시저

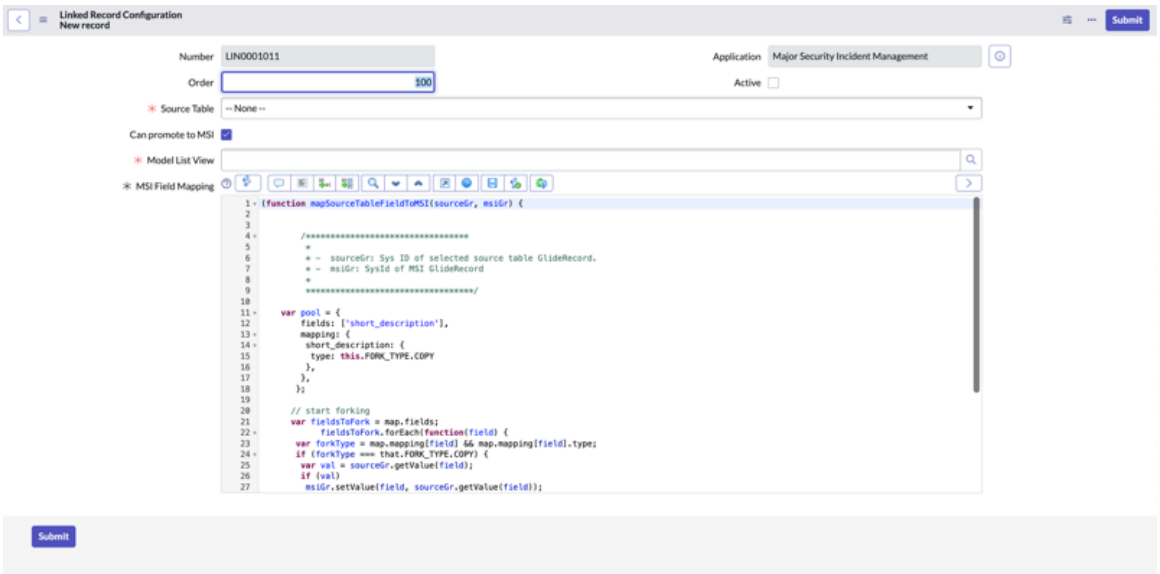
1. 왼쪽 탐색에서 연결된 기록 구성을 검색합니다.

2. 새로 만들기를 클릭합니다.

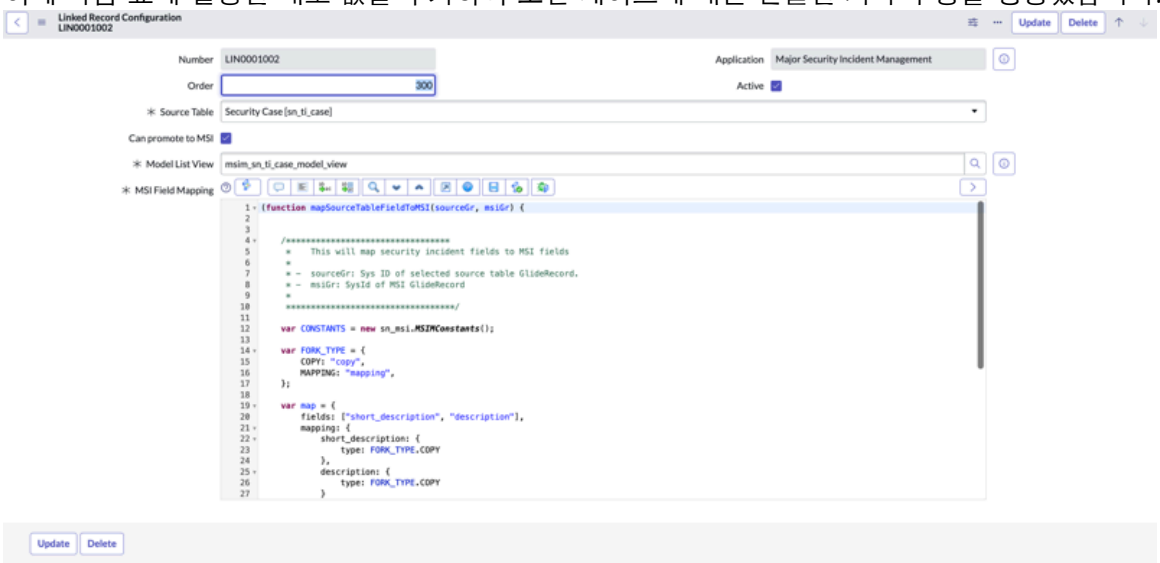


3. 필요한 열로 양식을 채우고 필드 매핑 스크립트를 작성합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 이제 다음 표에 설명된 대로 값을 추가하여 보안 케이스에 대한 연결된 기록 구성을 생성했습니다.



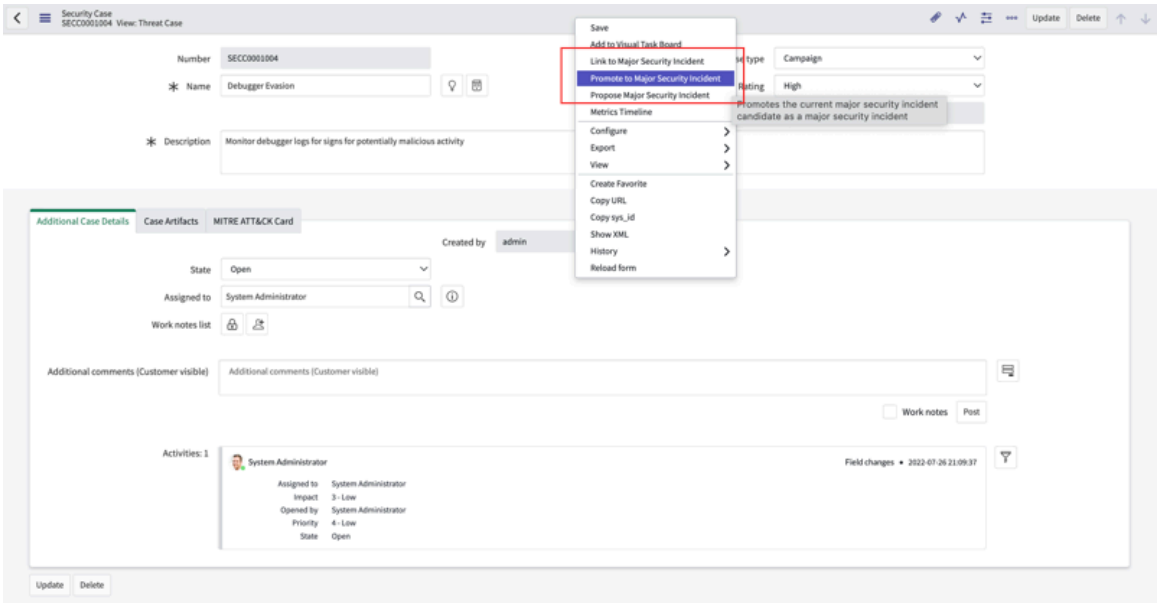
이름	설명
소스 테이블	sn_ti_case(보안 사례). 이 예에서는 보안 케이스를 MSI로 연결/승격/제안합니다.
순서	입력 값: 300 주: 낮은 순서가 높은 순서보다 우선합니다. 보안 케이스는 보안 인시던트 및 정정 작업보다 순서가 높으므로 마지막 시퀀스에 나타납니다.
MSI로 승격 가능	예, 보안 케이스를 MSI로 승격하려면 이 확인란을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

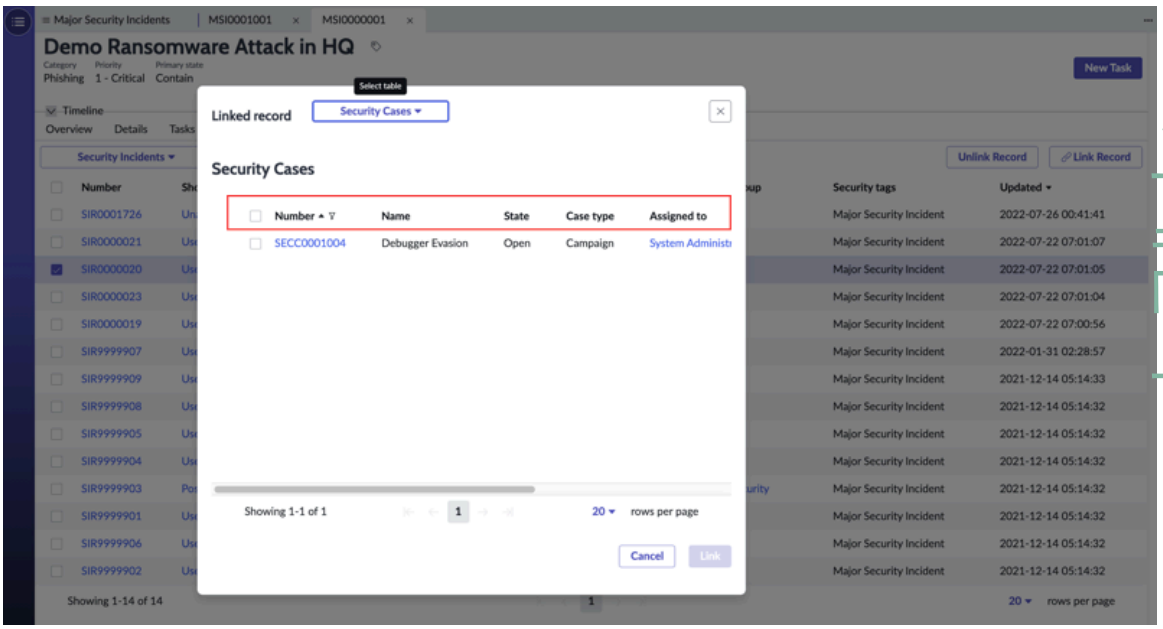
이름	설명
	주: ○ 작업 공간에서 보안 케이스 기록을 중요 보안 인시던트 중요 보안 인시던트 관리에 연결 및 연결 해제 또한 기록 연결 해제 기능은 연결된 기록에 대해서만 표시됩니다. ▪ 이렇게 하면 클래식 환경 작업을 사용하여 중요 보안 인시던트에 대한 연결, 승격 및 제안이 활성화되지만 이러한 UI 작업은 즉시 사용할 수 없습니다. 각 UI 작업은 수동으로 만들어야 합니다. 자세한 내용은 3 단계. 보안 케이스의 소스 테이블에 대한 UI 작업 생성 문서를 참조하십시오. ▪ 링크/승격/제안 UI 작업은 보안 인시던트, 정정 작업 및 보안 케이스에 즉시 사용할 수 있습니다. ○ MSIM 작업 공간 연결된 기록 페이지에 연결된 보안 케이스 기록이 표시됩니다. 이 확인란을 선택한 후 사용할 수 있는 옵션을 보려면 아래 이미지 1을 참조하십시오.
모달 목록 뷰	msim_sn_ti_case_model_view 주: 이 뷰에는 MSIM 작업 공간의 링크 기록 모달에서 목록 뷰에 표시된 필드와 필드 순서가 포함되어 있습니다. 자세한 내용은 2 단계. 보안 케이스에 대한 모달 창 뷰 생성 문서를 참조하십시오. 연결된 기록 페이지에서 보려면 아래 이미지 2를 참조하십시오.
필드 매핑 스크립트	이 스크립트는 소스 테이블 기록이 제안되거나 승격될 때 새로 생성된 중요 보안 인시던트에 매핑되는 소스 테이블 기록의 필드를 설명합니다. 입력을 수신합니다: ○ sourceGr: 보안 케이스 Glide 기록 객체 ○ msiGr: 중요 보안 인시던트 Glide 기록 객체 스크립트는 보안 케이스의 짧은 설명에서 읽고 중요 보안 인시던트의 제목으로 복사합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이미지 **1:** MSI로 승격 가능



이미지 **2.** 모달 뷰



2 단계. 보안 케이스에 대한 모달 창 뷰 생성

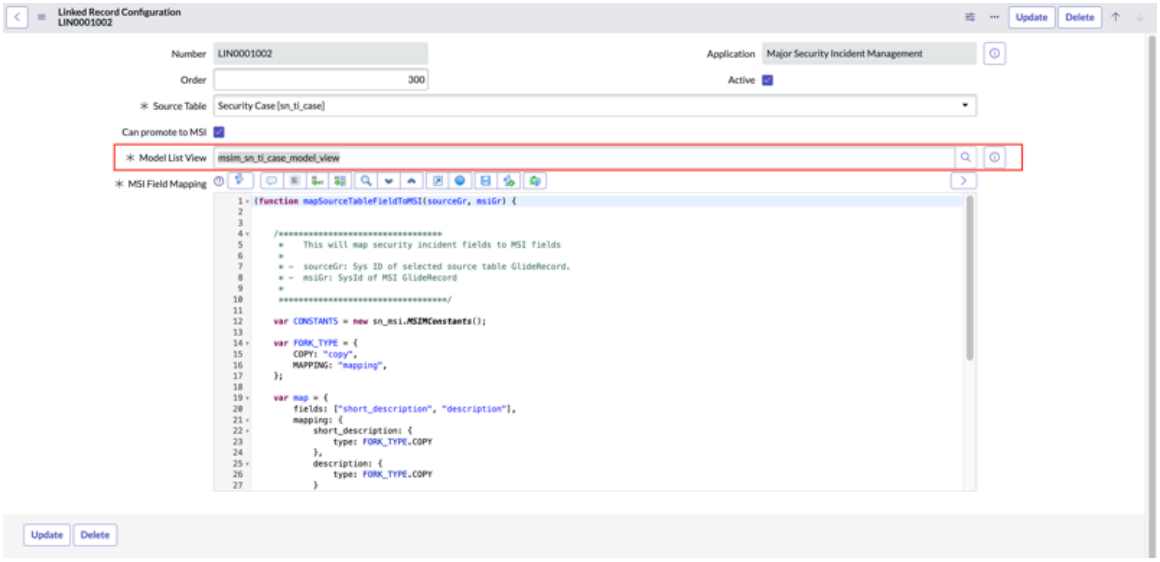
보안 케이스에 대한 모달 창에 대한 뷰를 만듭니다.

시작하기 전에
주요 고려 사항:

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 기본적으로 연결된 기록 모달 목록에는 기본 목록 레이아웃만 표시됩니다. 목록 레이아웃을 사용자 지정하려면 소스 테이블의 사용자 지정 뷰를 사용하면 됩니다.
- 사용자 지정 뷰를 렌더링하려면 소스 테이블에 대한 연결된 기록 구성에서도 사용자 지정 뷰를 선택해야 합니다.

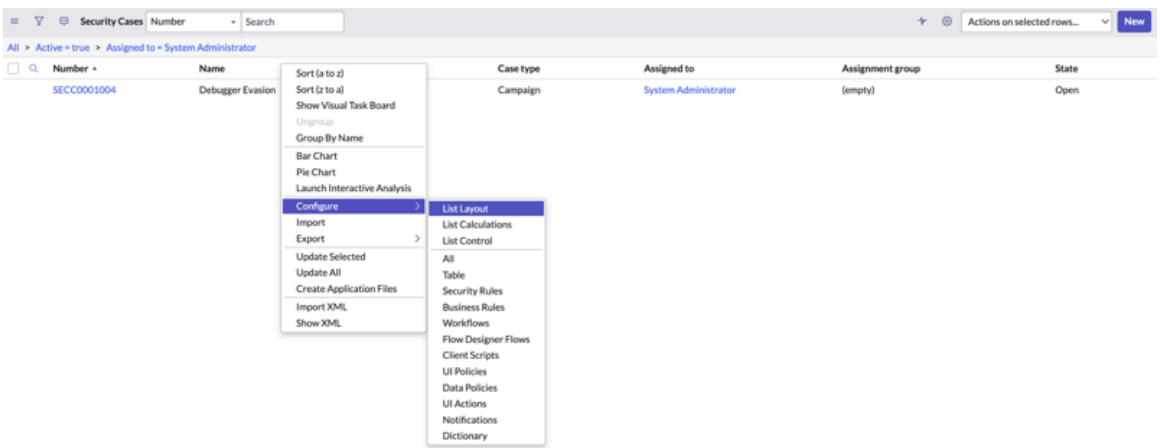
소스 테이블에 대한 모달 뷰 연결된 기록 구성



필요한 역할: 관리자

프로시저

1. 소스 테이블로 이동하여 구성 〉 목록 레이아웃.



2. 이동 목록 뷰 〉 뷰 이름.
3. 뷰 이름 드롭다운 목록에서 새로 만들기를 클릭하고 새 뷰(예: msim_sn_ti_case_modal_view)를 생성합니다.
4. 새로 만든 뷰를 선택합니다.
   선택한 후에는 사용 가능 목록에서 필수 필드를 선택할 수 있습니다.
5. 저장을 클릭합니다.
6. 다음으로 이동 메뉴 〉 뷰 뷰를 제대로 렌더링했는지 확인합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

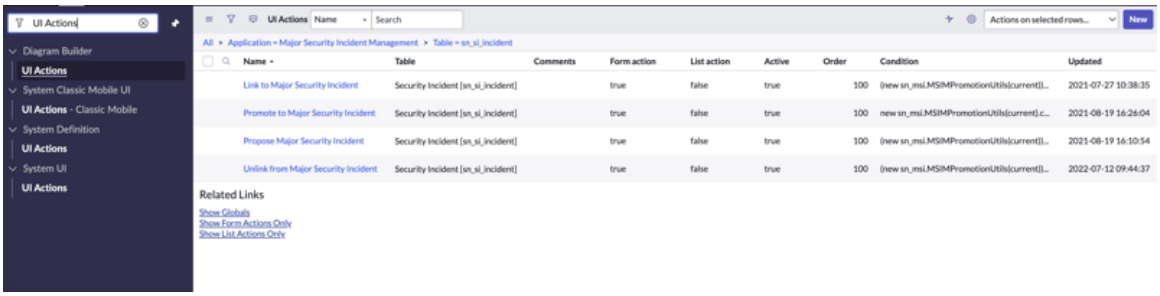
3 단계. 보안 케이스의 소스 테이블에 대한 UI 작업 생성

보안 케이스의 소스 테이블에 대한 UI 작업을 만듭니다.

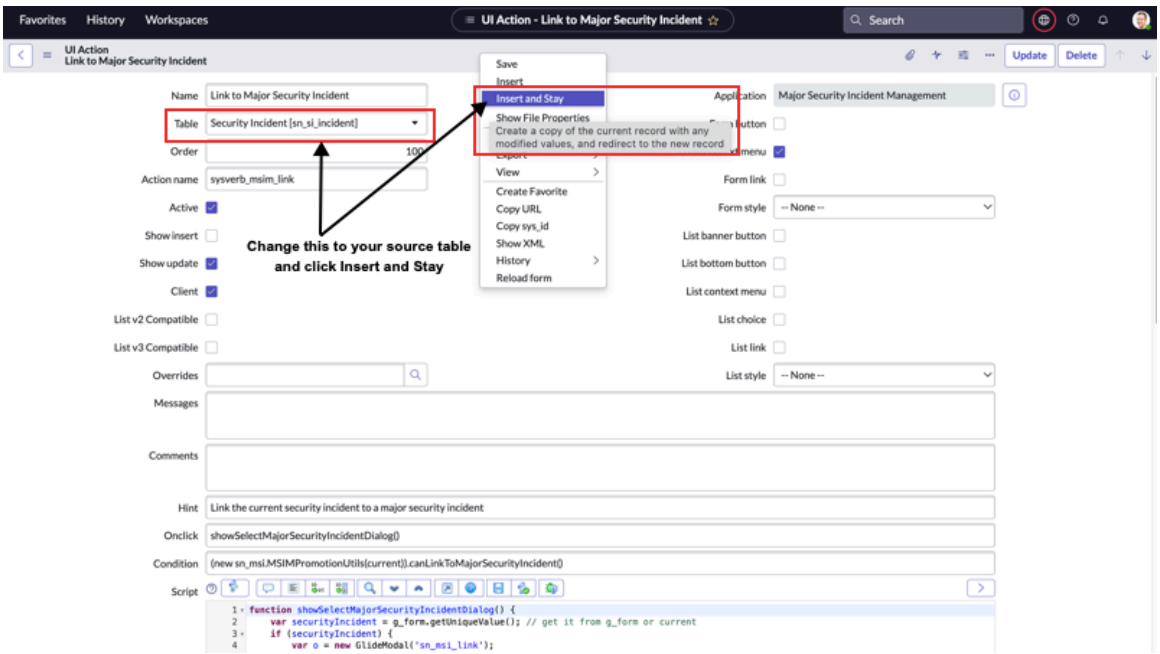
시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 시스템 정의 〉 **UI** 작업.
2. 필터 옵션을 실행하여 애플리케이션: Major Security Incident Management 및 테이블: sn_si_incident별로 목록을 필터링합니다.



3. 각 UI 작업을 하나씩 선택하고 소스 테이블의 상세 정보를 저장합니다.



4. 다음 UI 작업에 대해 위와 동일한 단계를 반복합니다.
   - 중요 보안 인시던트에 연결
   - 제안된 중요 보안 인시던트
   - 중요 보안 인시던트에서 연결 해제
   - 중요 보안 인시던트로 승격

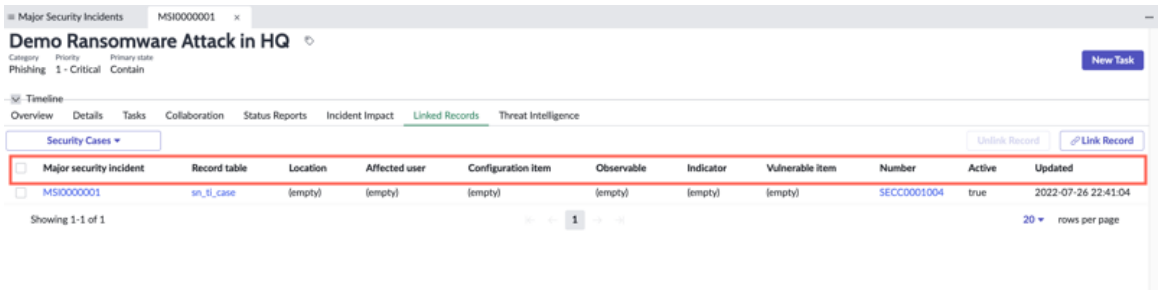
4 단계. 보안 케이스에 대한 새 연결된 기록 탭에 대한 뷰 생성

보안 케이스 테이블이 작업 공간과 함께 중요 보안 인시던트 관리 기록 연결 페이지에 표시될 때 이 테이블의 목록 레이아웃을 사용자 지정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필수 구성 요소:

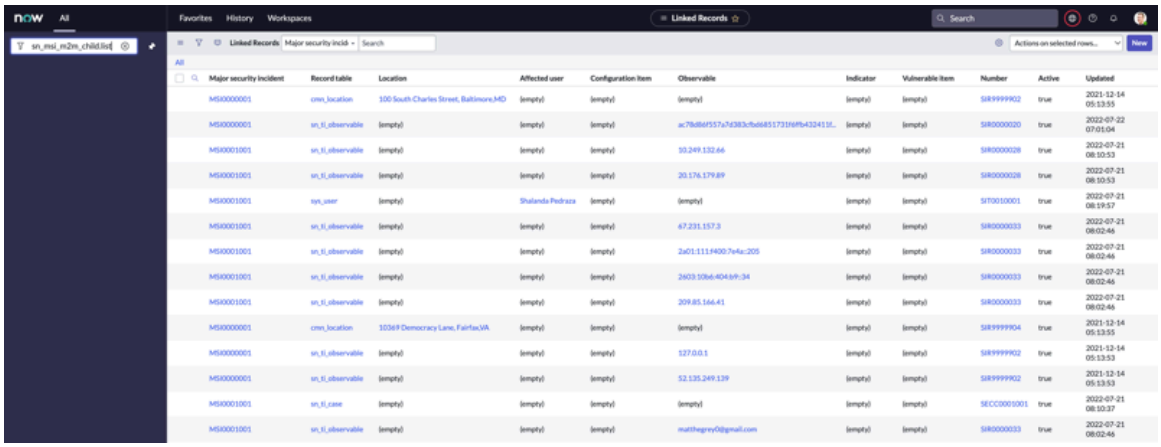
- 보안 케이스 테이블에 대해 목록을 렌더링할 때 표시할 열을 선택하십시오.
- 드롭다운 목록에 표시할 필드의 순서를 선택합니다.



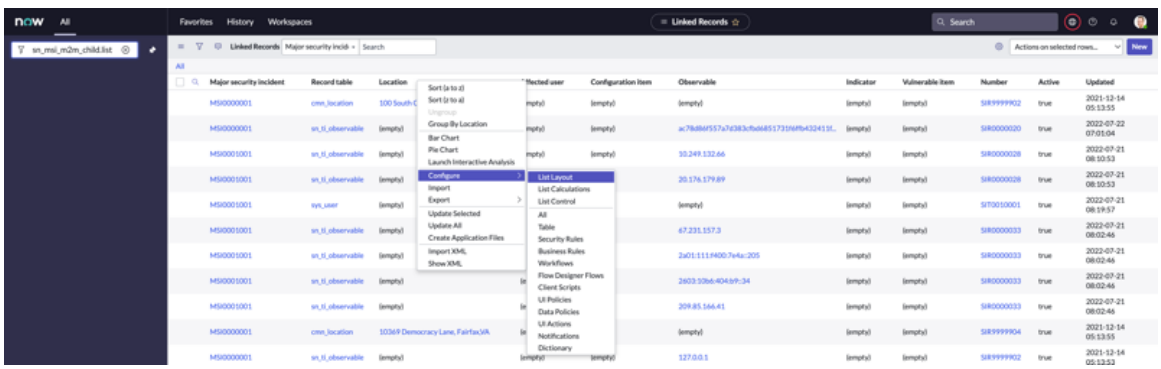
필요한 역할: 관리자

프로시저

1. 왼쪽 탐색을 사용하여 **sn_msi_m2m_child.list** 를 검색합니다.
   연결된 기록 테이블이 표시됩니다.

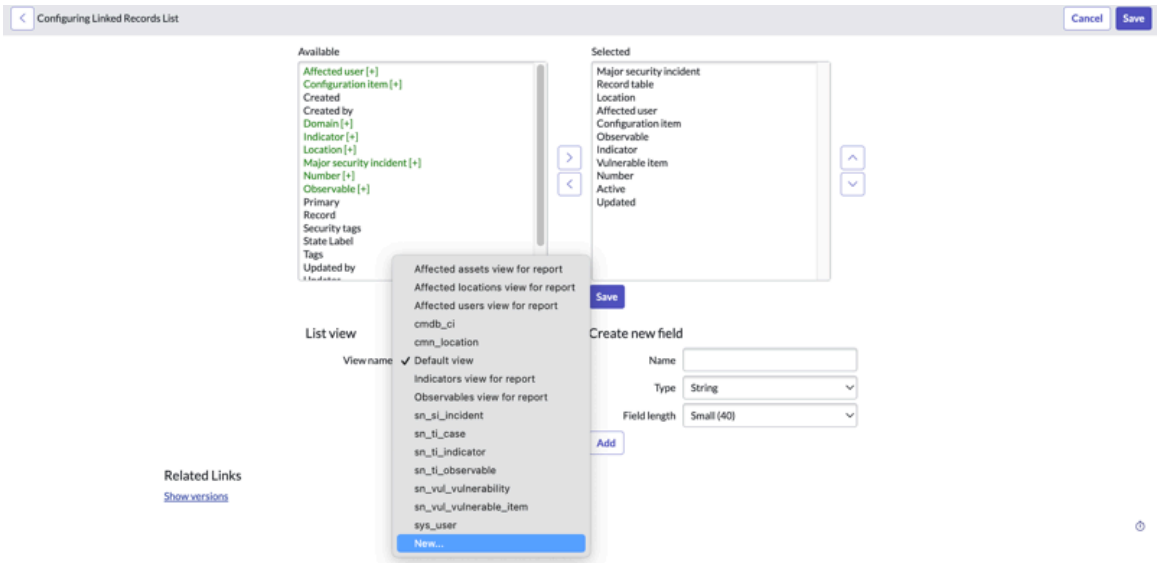


2. 헤더를 마우스 오른쪽 버튼으로 클릭하고 구성 〉 목록 레이아웃.
   연결된 기록 목록 구성 페이지가 표시됩니다.

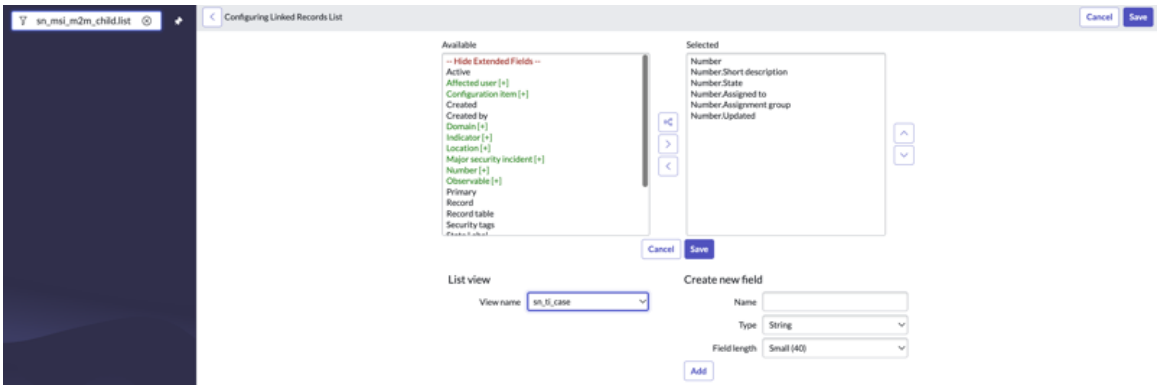


3. 이동 목록 뷰 〉 뷰 이름.
4. 뷰 이름 드롭다운 목록에서 새로 만들기를 선택합니다.

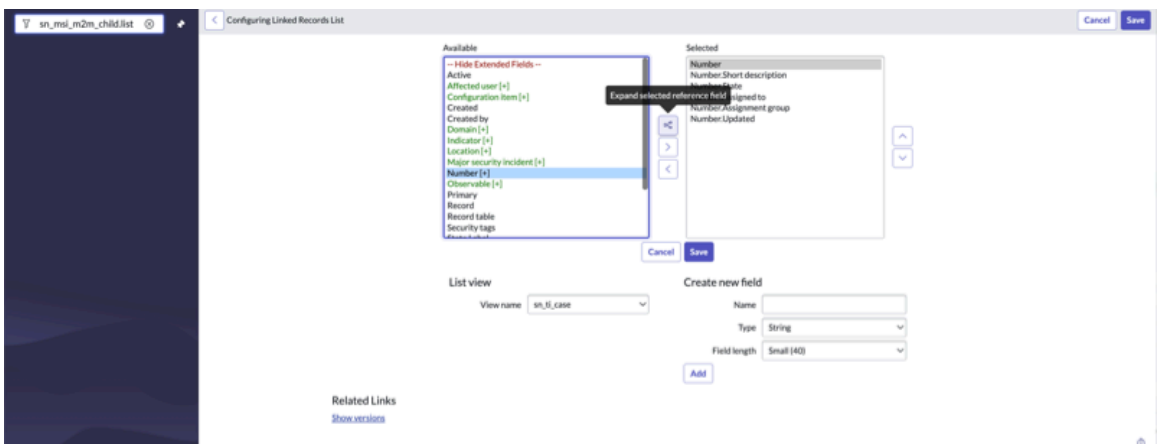
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



5. 작업 공간 목록 뷰에서 렌더링할 열을 선택합니다.
보안 케이스 기록은 번호 열에 저장됩니다. 보안 케이스에서 정보를 렌더링하려면 번호 열에서 닷워킹을 수행해야 합니다.

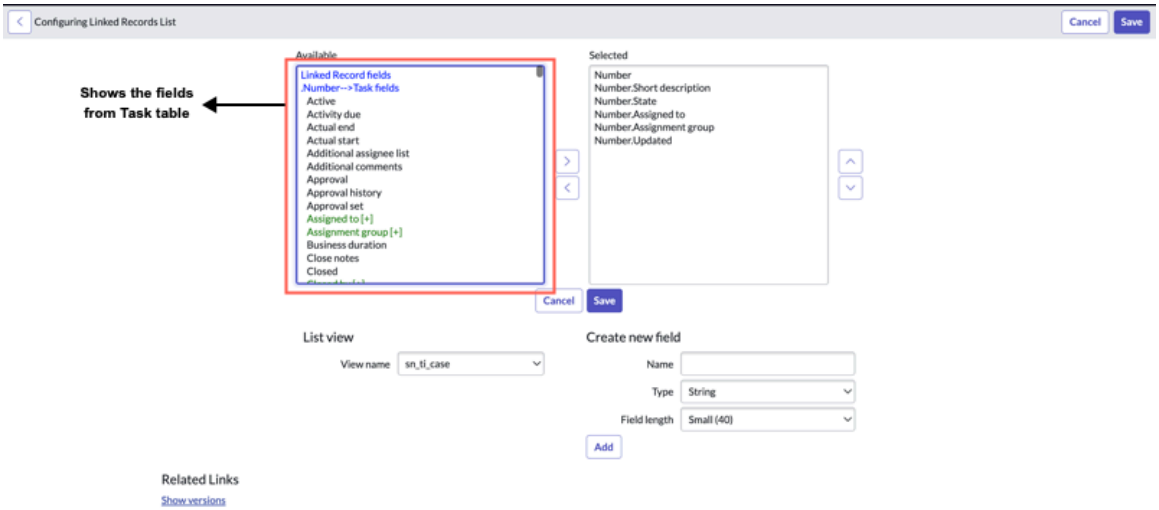


a. 닷워킹을 하려면 먼저 사용 가능 목록에서 번호 열을 선택한 다음 선택한 참조 필드 확장을 클릭합니다.



b. 번호에서 열을 확장하여 선택하고 선택됨 목록으로 이동합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



c. Save(저장)를 클릭하여 뷰를 저장하고 생성합니다.

6. 다음 단계는 작업 공간 내에서 중요 보안 인시던트 관리 생성된 뷰를 렌더링하는 것입니다. 목록 레이아웃 구성을 생성해야 합니다.

a. 왼쪽 탐색을 사용하여 목록 레이아웃 구성을 검색합니다.

b. 클릭 **MSI** 관리 〉 목록 레이아웃 구성.

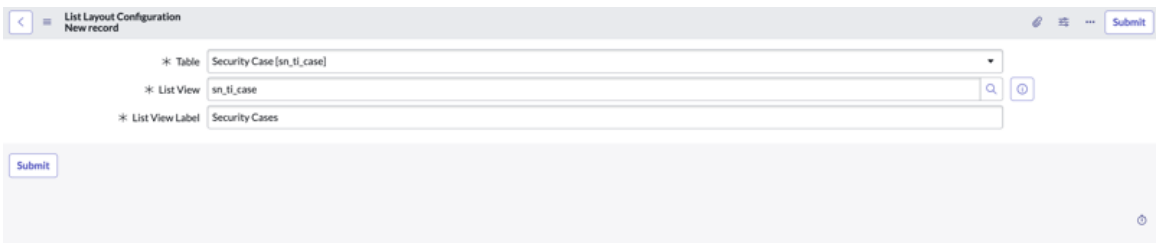
c. 새로 만들기를 클릭하여 새 구성을 만듭니다.

d. 테이블 열에서 소스 테이블을 선택하고 목록 뷰 필드에서 새로 생성한 뷰를 선택합니다.

e. 목록 뷰 레이블을 사용하면 동일한 소스 테이블이 작업 공간에서 렌더링 중요 보안 인시던트 관리 될 때 레이블을 제어할 수 있습니다.

f. 기록을 저장합니다.

> 주:
> 기록이 저장되면 작업 공간으로 중요 보안 인시던트 관리 이동하여 작업 공간 내에서 렌더링된 목록 뷰와 레이블을 봅니다.



5 단계. 작업 공간 사용자에 대한 중요 보안 인시던트 관리 접근 제어 목록**(ACL)** 추가

작업 공간 사용자에 대한 ACL(접근 제어 목록)을 중요 보안 인시던트 관리 추가합니다.

시작하기 전에
필요한 역할: 관리자

> 주:
> 연결 및 연결 해제 기능에 필요한 권한은 sn_msi.linkedsivi_read 역할로 제어합니다.

중요 보안 인시던트 관리 가상 사용자에는 sn_msi.linkedsivi_read 역할이 포함되어 있습니다.

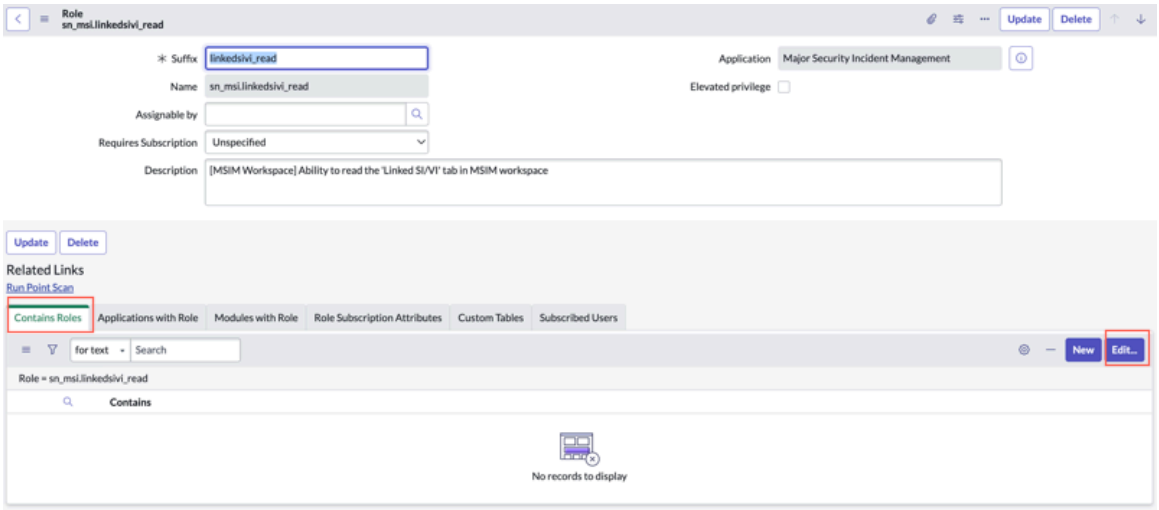
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

1. sn_msi.workspace_admin(MSIM 작업 공간 관리자)
2. sn_msi.workspace_manager(MSIM 작업 공간 관리자)
3. sn_msi.workspace_responder(MSIM 작업 공간 응답자)

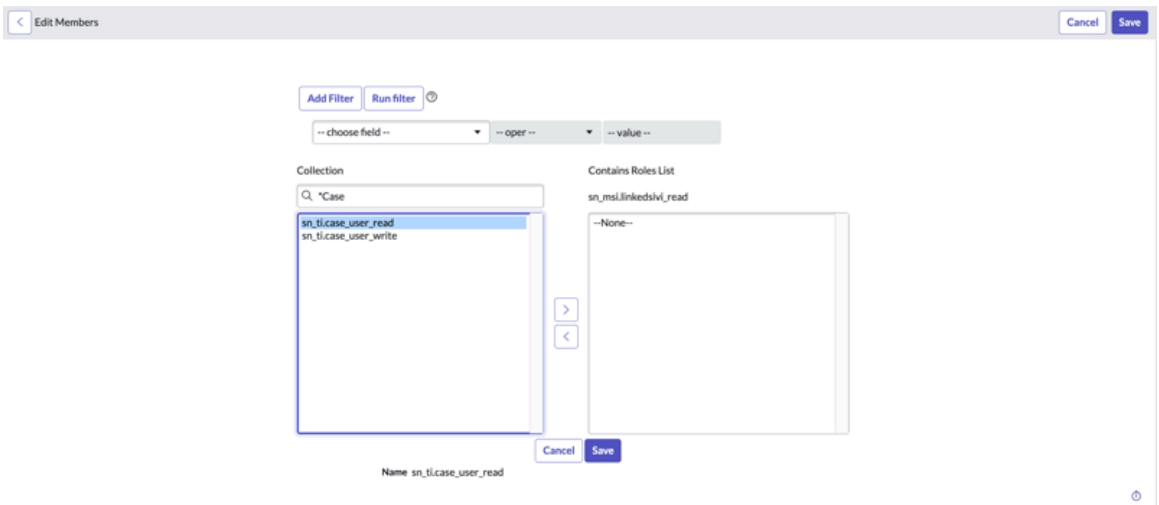
주:
모든 소스 테이블의 경우 필요한 역할이 sn_msi.linkedsivi_read 역할에 추가되었는지 확인해야 합니다.

프로시저

1. 다음으로 이동 사용자 관리 〉 역할 을 클릭하고 **sn_msi.linkedsivi_read** 역할을 검색합니다.
2. 역할 포함 관련 목록 섹션에서 편집을 클릭합니다.



3. 소스 테이블 역할이 역할 포함 섹션 아래에 추가되었는지 확인합니다.
보안 케이스에 필요한 역할을 구성할 수 있도록 구성원 편집 페이지가 표시됩니다.



4. 컬렉션 섹션에서 소스 테이블 역할을 검색합니다.
보안 케이스의 소스 테이블에서 읽기 및 쓰기 액세스를 허용하는 데 필요한 역할을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

- 보안 케이스의 경우 읽기와 쓰기를 위한 두 개의 별도 역할이 필요합니다.
- 작업 공간 연결된 기록 모달에서 중요 보안 인시던트 관리 소스 기록을 선택할 수 있는 테이블에 대한 쓰기 권한입니다.

5. 저장을 클릭하여 역할을 추가합니다.
6. 역할이 역할 포함 관련 목록 섹션에 성공적으로 추가되었는지 확인합니다.

6 단계. 보안 케이스에 대한 비즈니스 규칙 생성

보안 케이스에 필요한 비즈니스 규칙을 생성합니다.

시작하기 전에
필요한 역할: 관리자

새 소스 테이블 보안 케이스(sn_ti_case)에 대해 다음 세 가지 비즈니스 규칙을 생성합니다. 이러한 비즈니스 규칙은 보안 인시던트(sn_si_incident)와 같이 바로 사용 가능한 소스 테이블을 통해 동작의 일관성을 유지하는 데 필요합니다.

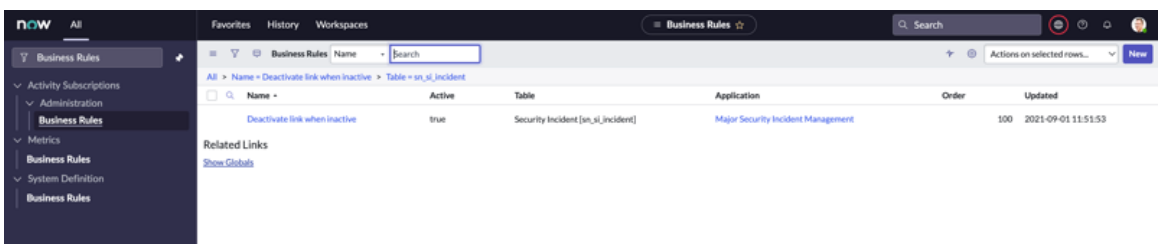
새 소스 테이블에 대한 비즈니스 규칙:

1. 비활성 시 링크 비활성화: 보안 케이스가 종결되면 관련 정보가 작업 공간 페이지에 더 이상 표시되지 중요 보안 인시던트 관리 않습니다.
2. 업데이트 시 팀 정보 동기화: 중요 보안 인시던트 상세 정보 탭에는 서로 다른 작업을 진행 중인 모든 활성 팀 및 사용자에 대한 정보가 표시됩니다. 보안 케이스에서 사용자에게 할당되거나 할당 그룹이 변경되면 중요 보안 인시던트 활성 팀 섹션에서 보안 케이스 팀 정보를 업데이트해야 합니다. 이러한 비즈니스 규칙은 활성 팀 섹션에서 새로 할당된 사용자 및 할당 그룹을 업데이트합니다.
3. 삭제 시 팀 정보 동기화: 중요 보안 인시던트 상세 정보 탭에는 다른 작업을 수행하는 모든 활성 팀 및 사용자에 대한 정보가 표시됩니다. 보안 케이스를 종결한 후에는 더 이상 중요 보안 인시던트 활성 팀 섹션에 보안 케이스 팀 정보를 표시할 필요가 없습니다. 이러한 비즈니스 규칙은 활성 팀에서 할당 대상 사용자 및 할당 그룹을 제거합니다.

새 소스 테이블에 대한 비즈니스 규칙 작성:

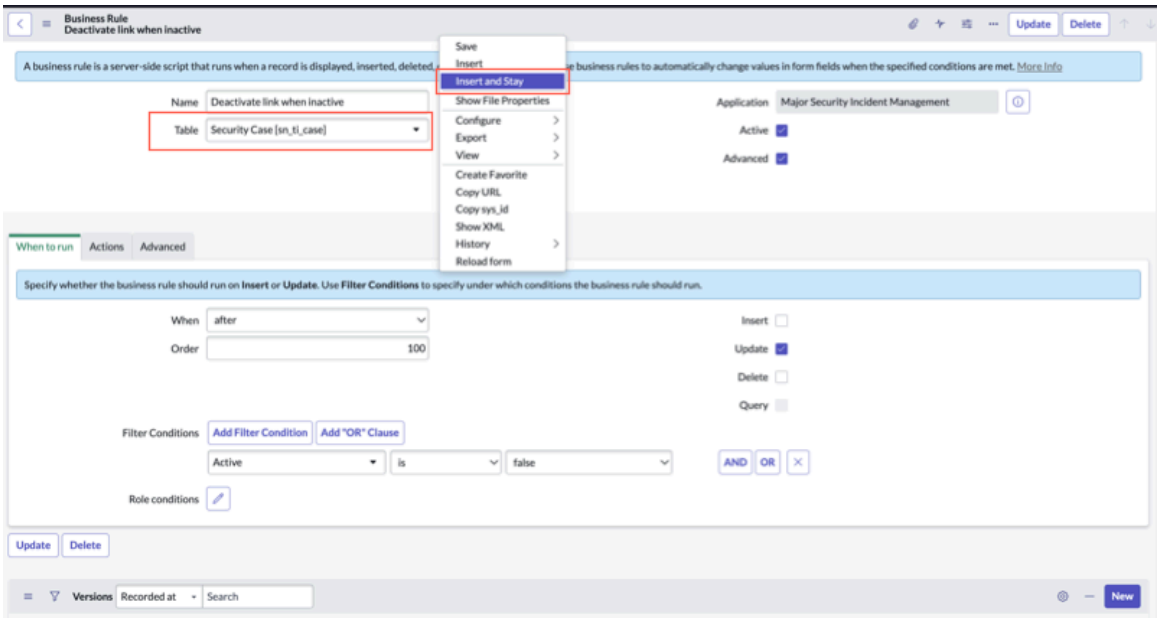
프로시저

1. 다음으로 이동 시스템 정의 〉 비즈니스 규칙.
2. 필터 옵션을 실행하여 아래 정보로 비즈니스 규칙 기준을 필터링합니다.
   - 이름: 비활성 시 링크 비활성화
   - 테이블: sn_si_incident



3. 기록을 열고 테이블 이름을 새 소스 테이블인 sn_ti_case로 변경합니다.
4. 페이지에서 메뉴를 마우스 오른쪽 버튼으로 클릭하고 삽입 및 유지 를 클릭하여 기록을 생성합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



5. 다른 두 비즈니스 규칙에 대해서도 이 절차를 반복합니다.
   - 삭제 시 팀 정보 동기화
   - 업데이트 시 팀 정보 동기화

7 단계. 롤업 기록 구성 작성

롤업 기록 구성을 생성하여 추가 기록을 MSI에 연결 및 연결 해제합니다.

시작하기 전에
필요한 역할: admin 및 sn_msi.workspace_admin

주:
시스템 관리자는 기록을 생성할 수 있으며 MSI 작업 공간 관리자는 업데이트할 수 있습니다.

보안 케이스와 관련된 구성 항목, 옵저버블 및 손상 표시기와 같은 정보를 롤업하려면 롤업 기록 구성을 생성합니다.

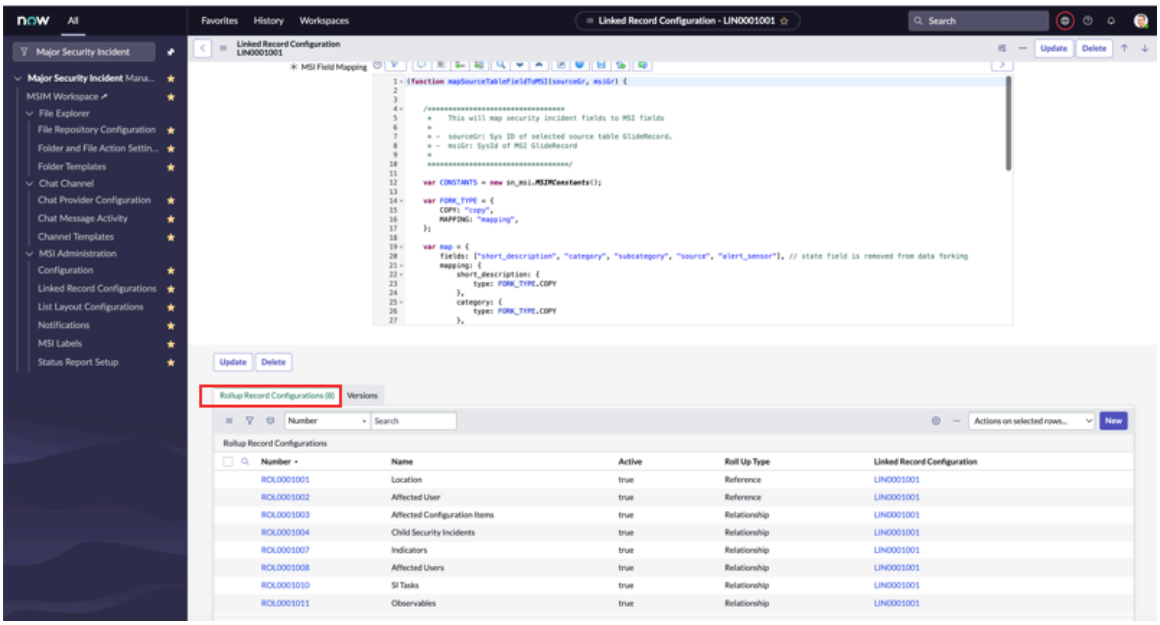
프로시저

1. 다음으로 이동 중요 보안 인시던트 응답 〉 연결된 기록 구성.
   연결된 기록 구성 페이지가 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

2. 새 연결된 기록을 선택하거나 만들고 같은 페이지에서 롤업 기록 구성 섹션으로 이동합니다.

롤업 기록 구성 섹션



다음에 수행할 작업

- 자세한 내용은 다음을 참조하십시오. 에서 롤업 기록 구성 중요 보안 인시던트 관리
- 보안 케이스 예제 정보는 다음을 참조하십시오.보안 케이스에 대한 스크립트 작성

보안 케이스에 대한 스크립트 작성

기록 구성을 롤업하는 보안 케이스에 대한 스크립트 작성

시작하기 전에

필요한 역할: admin 및 sn_msi.workspace_admin

주:
시스템 관리자는 기록을 생성할 수 있으며 MSI 작업 공간 관리자는 업데이트할 수 있습니다.

프로시저

1. 왼쪽 탐색을 사용하여 연결된 기록 구성을 검색합니다.

2. 다음으로 이동 **MSI** 관리 〉 연결된 기록 구성.

3. 보안 케이스에 대해 생성된 구성 기록을 엽니다.

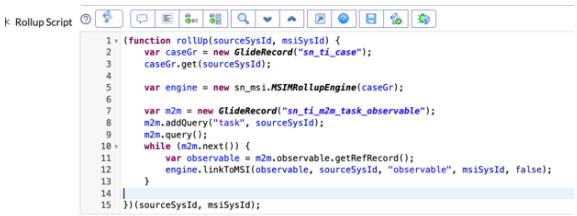
4. 롤업 기록 구성이 관련 목록 섹션에 표시됩니다.

5. 새로 만들기를 클릭하여 새 롤업 기록 구성을 만듭니다.

다음은 필드 값을 다음과 같이 롤업하려고 하는 보안 케이스와 관련된 옵저버블 데이터를 롤업하기 위해 생성된 예제 기록입니다.

이름	설명
롤업 유형	관계

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이름	설명
	주: 옵저버블 정보는 관련 목록 형식으로 제공됩니다.
롤업 스크립트	입력 sourceSysId에는 보안 케이스 시스템 ID가 포함되어 있고 msiSysId에는 중요 보안 인시던트 시스템 ID가 포함되어 있습니다.  ○ Line 2: As a first step, query for Glide Record for sourceSysId from **Security Case(sn_ti_case)** table. ○ Line 7: Next, query **sn_ti_m2m_task_observable** table using security case sys ID to figure out all the linked observables to a security case. ○ Line 10: Next, iterate over all the linked observables and link them to a Major Security Incident using the method: `MSIMRollupEngine.linkToMSI("entityGr", "sourceSysId", "fieldNameInLinkedRecordTable", "msiSysId", "isPrimaryRecord")`

요청 시 원자 롤업 수행

롤업 프레임워크는 기존 연결된 기록에 대한 업데이트를 처리할 수 없습니다. 이러한 경우 연결된 기록에 대해 요청 시 원자성 롤업이 발생해야 하며, 이는 비즈니스 규칙을 통해 달성할 수 있습니다.

연결된 기록에 대한 업데이트를 캡처하려면 소스 테이블에서 비즈니스 규칙을 생성해야 합니다.

이러한 비즈니스 규칙은 삽입, 업데이트 및 삭제 작업에 작동합니다. 삽입 또는 업데이트를 수행할 때 롤업된 정보를 에 추가하거나 업데이트해야 합니다 MSI. 삭제하면 롤업된 정보가 에서 제거됩니다 MSI.

예를 들어 보안 인시던트가 에 연결되면 MSI관련 정보가 자동으로 MSI롤업됩니다. 그러나 나중에 새 옵저버블 MSI을 에 추가하면 새로 추가된 옵저버블도 로 롤업 MSI됩니다. 여기서 롤업된 옵저버블 비즈니스 규칙 동기화 는 업데이트를 캡처하고 업데이트된 기록을 에 롤업합니다 MSI. 마찬가지로 동일한 비즈니스 규칙이 기존의 롤업된 옵저버블이 보안 인시던트에서 제거되는 경우 해당 옵저버블의 제거도 처리합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

미리 정의된 비즈니스 규칙

다음은 원자 롤업을 처리하는 방법을 이해하는 데 도움이 되는 미리 정의된 몇 가지 비즈니스 규칙입니다

규칙	설명
롤업 표시기 동기화(sn_ti_m2m_task_indicator)	이 비즈니스 규칙을 사용하여 보안 인시던트, 보안 케이스 및 정정 작업에서 손상 표시기의 롤업 및 제거를 처리합니다.
롤업된 옵저버블(sn_ti_m2m_task_observable) 동기화	이 비즈니스 규칙을 사용하면 보안 인시던트, 보안 케이스 및 정정 작업에서 연결된 옵저버블의 롤업 및 제거를 처리할 수 있습니다.
롤업된 영향을 받는 사용자 (sn_si_m2m_task_affected_user) 동기화	이 비즈니스 규칙을 사용하면 보안 인시던트, 보안 케이스 및 정정 작업에서 영향을 받는 연결 사용자를 롤업하고 제거할 수 있습니다.
롤업된 영향을 받는 CI(task_ci) 동기화	이 비즈니스 규칙을 사용하면 보안 인시던트, 보안 케이스 및 정정 작업에서 연관된 구성 항목의 롤업 및 제거를 처리할 수 있습니다.

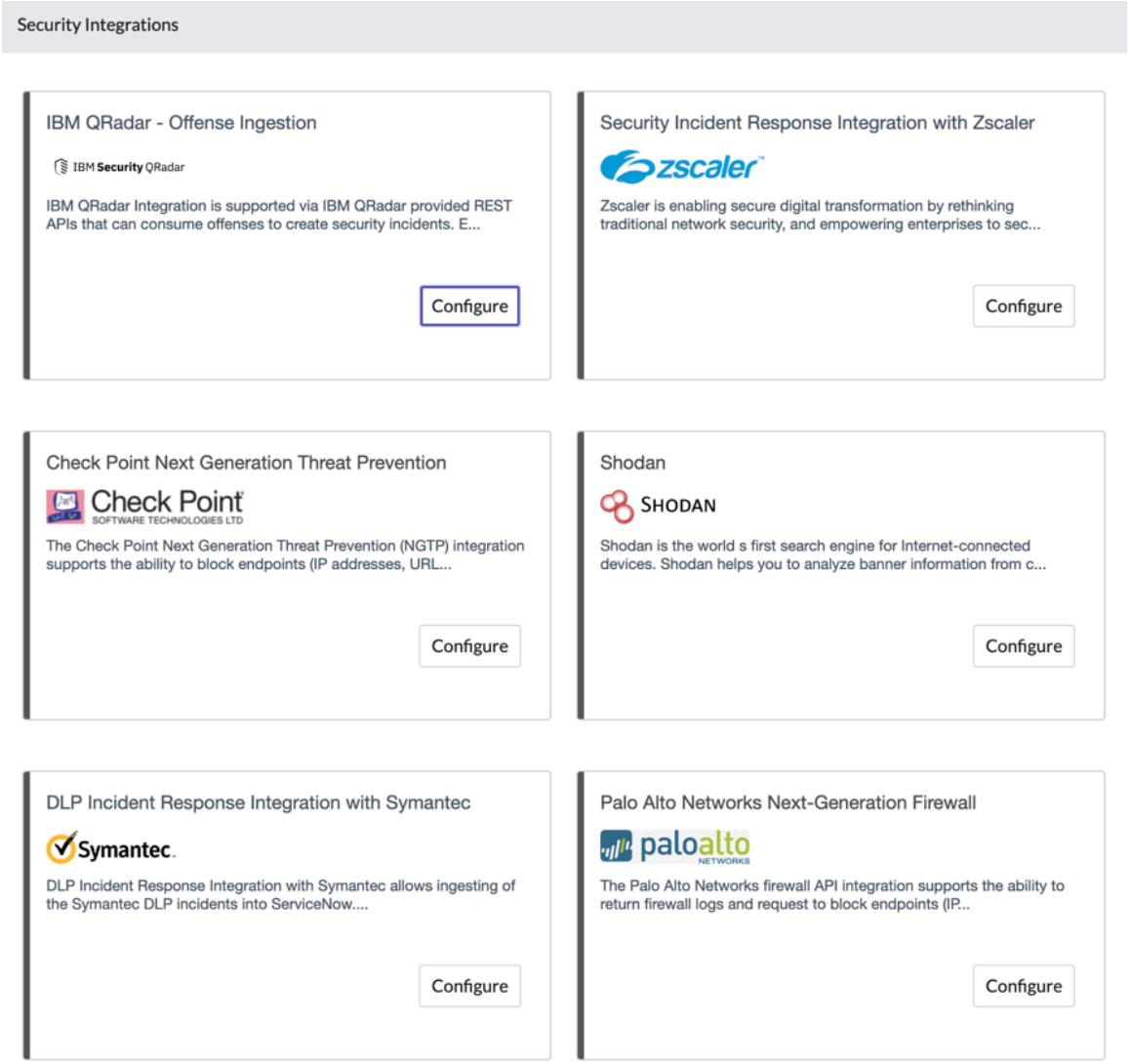
보안 인시던트 응답 통합

보안 운영 모든 핵심 애플리케이션과 비핵심 타사 통합은 에서 ServiceNow Store사용할 수 있습니다. 이 섹션에서는 통합을 활성화하고 타사 통합을 모두 ServiceNow 구성하기 위한 지침을 제공합니다. 또한 자체 통합을 개발하기 위한 몇 가지 기본 지침과 기본 시스템에 포함된 특정 통합에 대한 세부 정보가 포함되어 있습니다.

통합 구성

기본 시스템에는 활성화하고 사용할 수 있는 각 통합 구현에 대한 일련의 "카드"가 포함되어 있습니다. 또한 플러그인에 종속되어 보안 운영 있는 ServiceNow Store에 게시된 모든 통합에 대한 카드가 표시됩니다. 통합 카드는 선택하여 볼 수 있습니다. 보안 운영 〉 통합 구성.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



범주 드롭다운 메뉴를 사용하여 표시되는 통합을 필터링할 수 있습니다. **Show Configurations** 드롭다운 메뉴를 사용하면 생성을 허용하는 구현의 여러 인스턴스를 볼 수 있습니다.

통합 카드의 버튼

통합 카드는 통합의 현재 상태와 카드의 소스에 따라 서로 다른 버튼을 표시합니다.

단추	설명
플러그인 설치	통합을 활성화하려면 해당 플러그인을 설치하려면 이 버튼을 클릭하십시오. 플러그인이 설치되면 버튼이 구성으로 변경됩니다.
구성	통합 구성을 위한 정보를 입력하려면 이 버튼을 클릭합니다. 일부 통합의 경우 타사 통합 웹 사이트에서 가져온 API 키 또는 URL을 입력해야 할 수 있습니다.
신규	Carbon Black 및 IBM QRadar와 같은 특정 통합을 사용하면 동일한 통합의 여러 구현을 정의할 수 있습니다. 이러한 통합의 경우 플러그인이 활성화된 후 새로 만들기를 클릭합니다. 카드를 사용하면 플러그인을 설치하고(해당되는 경우) 사용할 구현을 구성할 수 있습니다.
페이지 열기	기본 시스템에서 인스턴스는 플러그인에 종속 보안 운영 된 애플리케이션에 대해 ServiceNow Store에 대한 쿼리를 수행합니다. 이러한 애플리케이션이 발견되고 연결된 애플리케이션 플러그인이 활성화되면 해당 애플리케이션에 대한 통합 카드가 다른 보안

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

단추	설명
	통합 카드와 함께 표시됩니다. 페이지 열기를 클릭하여 통합을 구성할 외부 공급업체 애플리케이션의 웹 사이트에 액세스합니다. 구성을 완료하면 페이지 열기 버튼이 구성으로 변경됩니다.

ArcSight ESM 이벤트 수집 통합

ArcSight ESM 제품과 이벤트 수집 통합을 보안 인시던트 응답 통해 보안 인시던트 분석가는 상관 관계가 있는 이벤트를 수집하고 플랫폼으로 보안 인시던트 생성을 자동화할 수 있습니다ServiceNow. 데이터는 구성된 폴링 일정에 따라 지속적으로 수집되며 분석가가 잠재적인 사이버 보안 위협을 식별하고 대응하는 데 사용됩니다.

이 통합을 사용하면 보안 인시던트의 후보인 상관 관계 이벤트를 주기적으로 수집할 수 있습니다. 상관 관계가 있는 이벤트의 필드를 보안 인시던트 필드에 매핑하고, 이벤트 설정을 보안 인시던트로 미리 보고, 예약된 이벤트 수집을 설정하여 지속적으로 보안 인시던트를 자동으로 생성할 수 있습니다.

ArcSight ESM 이벤트 수집 통합 개요

이 통합은 보안 운영 센터(SOC) 분석가에게 의 ArcSight ESM상관관계 이벤트에 대한 가시성을 제공합니다. 이 데이터는 추가 조사 및 정정을 위해 SIR(보안 인시던트 응답) 보안 인시던트에 통합 ServiceNow AI Platform 될 수 있습니다. 프로파일은 의 ArcSight ESM상관관계 쿼리 뷰어를 통해 생성되고 제공되는 다양한 상관관계 이벤트 유형을 처리하기 위해 인스턴스에 생성됩니다ServiceNow AI Platform. 이러한 프로파일은 SIR 보안 인시던트에 상관 관계가 있는 다양한 ArcSight ESM 이벤트 필드가 표시되는 방식을 사용자 지정합니다.

주요 기능

이 통합에는 다음과 같은 주요 기능이 포함됩니다.

- 여러 이벤트 수집 프로필을 생성하여 맬웨어 및 무단 액세스 시도와 같은 특정 유형의 위협에 대한 보안 인시던트를 생성합니다 SIR .
- 상관관계 이벤트 필드 값을 연결된 SIR 보안 인시던트 필드에 끌어서 놓기로 매핑 ArcSight ESM 합니다.
- 이벤트 매핑 상세 정보를 확인하기 위한 샘플 상관관계 이벤트를 기반으로 하는 보안 인시던트 레이아웃의 SIR 미리 보기입니다.
- 구성 가능한 간격으로 과거 상관관계 이벤트뿐만 아니라 새로운 주목할 만한 이벤트를 수집합니다.
- 인시던트 작성 기준에 맞지 않는 SIR 상관관계 이벤트(예: 우선순위가 낮은 이벤트)를 필터링합니다.
- 중복 보안 인시던트를 방지하기 위해 일치하는 필드 값을 기준으로 이벤트를 기존 SIR 보안 인시던트에 집계합니다.
- 양방향 인터페이스를 통해 인시던트 생성 및/또는 종결 조건을 기반으로 SIR 상관관계 이벤트를 업데이트합니다.

지원되는 **ServiceNow AI Platform** 버전

이 통합은 New York 패치 6 및 Orlando ServiceNow AI Platform 릴리스를 지원합니다.

다음 Security Operations 애플리케이션은 .ServiceNow Store 원활한 설치를 위해 아래 나열된 순서대로 한 번에 하나의 애플리케이션을 설치하고 활성화합니다.

1. 보안 통합 프레임워크
2. Security Support Common

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 보안 인시던트 응답
4. Security Operations에 대한 이벤트 및 경보 수집
5. 통합 허브 플러그인
   a. ServiceNow 통합 허브 런타임
   b. ServiceNow 통합 허브 작업 단계 - REST

핵심 애플리케이션 설치에 보안 운영 대한 자세한 내용은 해당 애플리케이션 활성화 ServiceNow Store문서를 참조하십시오제품 또는 애플리케이션에 대한 보안 운영 권리 가져오기.

ArcSight ESM 지원되는 버전

이 통합은 Manager의 ArcSight ESM 버전 7.0.0.2436에서 테스트되었습니다. 통합은 온-프레미스 및 클라우드/호스팅된 서비스 환경을 모두 ArcSight ESM 지원합니다.

MID 서버

이 통합을 위해서는 서버가 회사 네트워크 내에 배포될 때 ArcSight ESM 서비스에 연결하기 ArcSight ESM 위해 인스턴스에 MID 서버가 ServiceNow AI Platform# 설치 및 구성되어 있어야 합니다. 클라우드 서비스를 사용하는 ArcSight ESM 경우에는 MID 서버가 필요하지 않습니다. MID Server에 대한 자세한 내용은 ServiceNow 제품 설명서 웹 사이트를 참조하십시오.

참조

참조	문서 식별자	문서 제목
1	ArcSight ESM 제품 설명서	ArcSight 제품 설명서.
2	ServiceNow 제품 설명서 웹 사이트	ServiceNow 제품 설명서 웹 사이트

ServiceNow AI Platform® 이벤트 수집 통합을 위한 ArcSight ESM 인스턴스 설정

다음 섹션에서는 에서 애플리케이션을 ServiceNow Store설치하기 전에 인스턴스에서 완료해야 ServiceNow AI Platform# 하는 설정 작업을 나열합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
원활한 설치 및 구성을 위해 애플리케이션을 다운로드하고 설치하기 전에 다음 테이블을 참조하고 나열된 작업을 모두 완료했는지 확인하십시오.

설정 작업	설명
필수 ServiceNow AI Platform# 역할과 보안 인시던트 응답(SIR) 역할을 할당했는지 확인합니다.	인스턴스에서 통합을 ServiceNow AI Platform# 설치, 설정 및 사용하려면 다음 역할이 필요합니다. • 관리자 역할(admin)의 ServiceNow AI Platform# 사용자는 보안 인시던트 관리자(sn_si.admin) 역할을 사용하여 ServiceNow Store 애플리케이션을 설치하고 할당합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설정 작업	설명
	• sn_si.admin 역할을 가진 사용자는 다음 ServiceNow AI Platform#에서 다음 작업을 감독합니다. ◦ 이벤트 프로파일의 이름을 지정하고, 생성하고, 편집합니다. ◦ 상관관계 이벤트에서 보안 인시던트로 ArcSight ESM 값을 선택하고 매핑합니다. ◦ 구성을 완료하기 전에 보안 인시던트 상세 정보가 정확한지 미리 봅니다. ◦ 진행 중인 상관 관계 이벤트 수집을 예약합니다. ◦ SIR 인시던트가 생성되고 종결되면 상관 관계 이벤트 업데이트를 활성화합니다. ◦ 보안 인시던트 분석가(sn_si.analyst) 역할을 할당합니다. ◦ sn_si.analyst 사용자는 보안 인시던트에 대한 작업을 수행합니다. 역할 및 사용자에게 역할을 할당하는 방법에 대한 자세한 내용은 ServiceNow 제품 설명서 웹 사이트의 역할을 참조하십시오.
Manager 버전 7.0.0.2436 이상을 ArcSight ESM 사용하고 있는지 확인합니다. 이전 버전은 지원되지 않습니다.	쿼리 뷰어에 ArcSight ESM 대한 액세스 권한이 있는 경우 이 통합에 필요한 API에 액세스할 수 있습니다. API에 필요한 다른 특수 설정은 없습니다.
에서 쿼리 뷰어를 ArcSight ESM설정합니다.	상관관계 이벤트를 수집하려면 먼저 콘솔에서 쿼리 뷰어를 ArcSight ESM 구성해야 합니다. 자세한 내용은 쿼리 뷰어 설정Set up the ArcSight ESM Query Viewer 문서를 참조하십시오.
옵션 에서 ArcSight ESM 상관관계 이벤트 업데이트에 대한 사용자 지정 스테이지를 생성합니다.	상관관계 이벤트는 종결되기 전에 수명주기에서 여러 스테이지를 거칩니다. ArcSight ESM 초기, 모니터링, 큐에 대기 중 및 종결됨과 같은 기본 스테이지를 제공합니다. 이 스테이지 중 일부는 사용자 입력이 필요하지만, 다른 스테이지는 사용자 개입 없이 이벤트에 자동으로 적용됩니다(콘솔에서 사용자 필수 필드가 선택 ArcSight ESM 취소되어 있음). 사용자 개입이 필요하지 않은 사용자 지정 스테이지를 생성하여 인스턴스에서 사용할 수 있습니다 ServiceNow AI Platform# . 자세한 내용은 추가 옵션: 인시던트 상태에 따라 SIR 상호 관련된 이벤트 업데이트 및 종결을 자동화 문서를 참조하십시오.
MID 서버 애플리케이션을 설치하고 구성했는지 확인하십시오.	구성된 MID 서버 애플리케이션 서버가 회사 네트워크 내에 배포된 경우 ArcSight ESM 서비스의 MID Server ServiceNow AI Platform# 가 서비스에 연결 ArcSight ESM 되어야 합니다. MID 서버 애플리케이션 구성 방법에 대한 지침은 을 참조하십시오 이벤트 수집 통합을 위한 ArcSight ESM ServiceNow 애플리케이션 설치 및 구성 .

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설정 작업	설명
	MID 서버에 대한 자세한 내용은 MID 서버를 참조하십시오. 인터넷에 액세스할 수 있는 호스팅 서비스 또는 클라우드 서비스를 사용하는 경우에는 MID 서버가 필요하지 않습니다.
ServiceNow 통합을 위해 애플리케이션을 설치하기 전에 통합을 지원하는 데 필요한 핵심 애플리케이션이 설치되고 활성화되었는지 확인합니다.	에서 ServiceNow Store다음 보안 운영 애플리케이션이 설치되고 활성화되는지 확인합니다. 설치되지 않은 경우 원활한 설치를 위해 다음 순서로 한 번에 하나의 애플리케이션을 설치하고 활성화합니다. **1.** 보안 인시던트 응답 **2.** 보안 통합 프레임워크 **3.** Security Support Common **4.** 보안 운영용 이벤트 및 경보 수집: 이 애플리케이션에는 다음이 필요합니다. ○ com.glide.hub.integration.runtime => ServiceNow 통합 허브 런타임 ○ com.glide.hub.action_step.rest => ServiceNow 통합 허브 작업 단계 - REST **5.** Threat Core 핵심 애플리케이션 설치에 보안 운영 대한 자세한 내용은 해당 애플리케이션 활성화 ServiceNow Store문서를 참조하십시오제품 또는 애플리케이션에 대한 보안 운영 권리 가져오기.

다음에 수행할 작업
통합을 위한 인스턴스를 성공적으로 설정 ServiceNow AI Platform# 했습니다. 다음 단계는 통합을 위해 보안 운영용 보안 이벤트 수집 애플리케이션을 ServiceNow Store 설치하는 ArcSight ESM 것입니다.

쿼리 뷰어 설정**Set up the ArcSight ESM Query Viewer**

쿼리 뷰어를 만들고 수집할 ServiceNow최근에 만든 상관 관계 이벤트를 포함할 필터를 정의합니다.

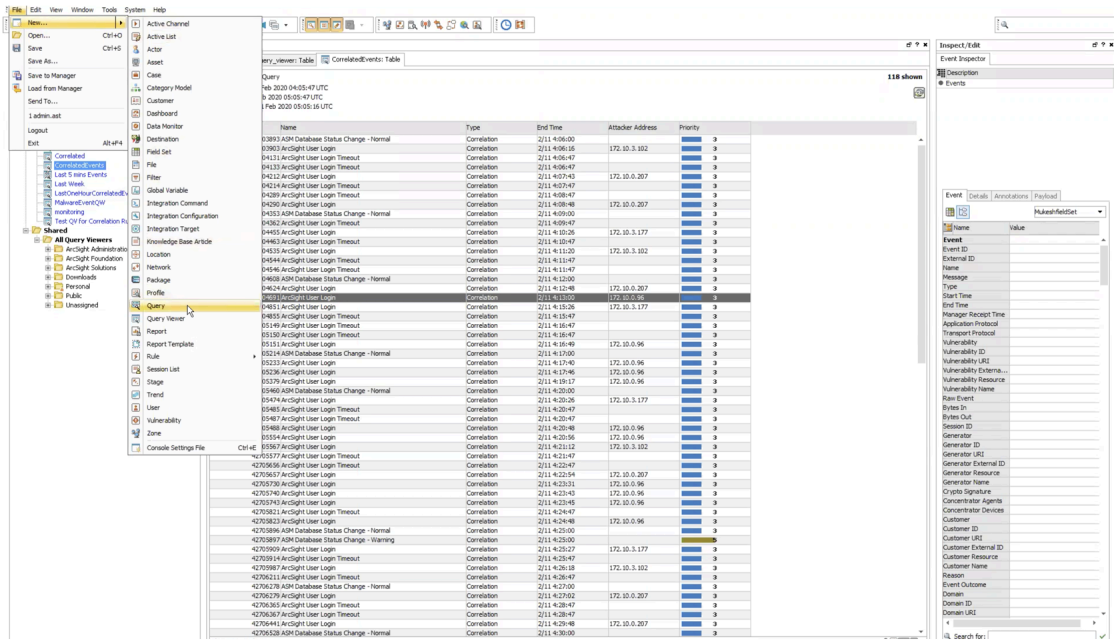
시작하기 전에
필요한 역할: ArcSight 관리자

프로시저

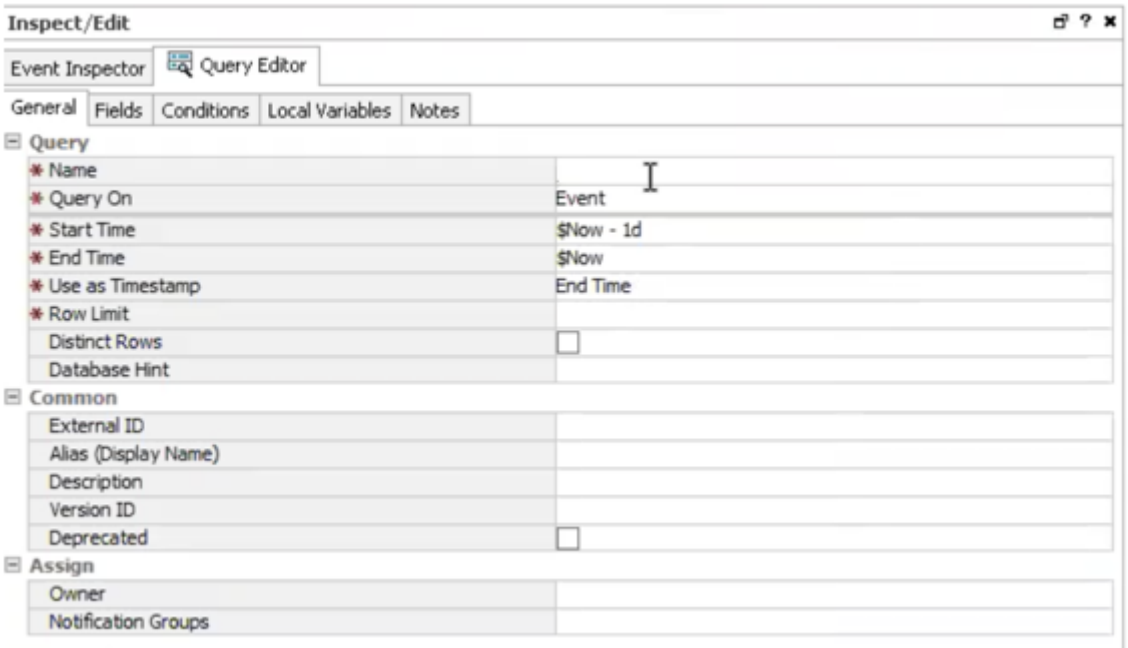
1. ArcSight ESM 콘솔에 로그인하여 쿼리 뷰어를 만듭니다.

2. 새 쿼리를 만들려면 다음으로 이동합니다. 파일 〉 신규 〉 쿼리.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

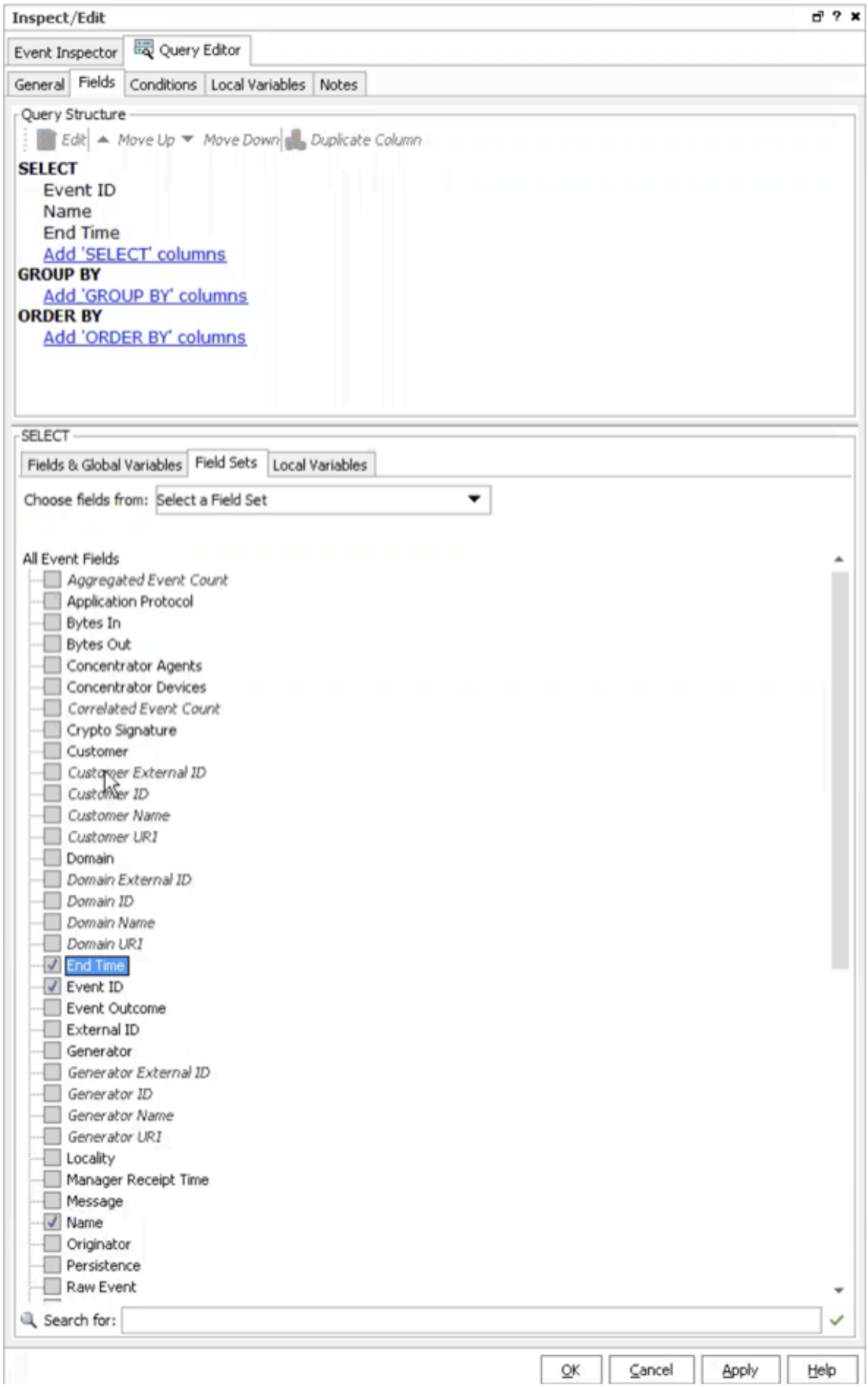


3. 검사/편집 패널에서 쿼리 뷰어에 대한 조건을 정의합니다.



4. 필드 탭을 클릭합니다.

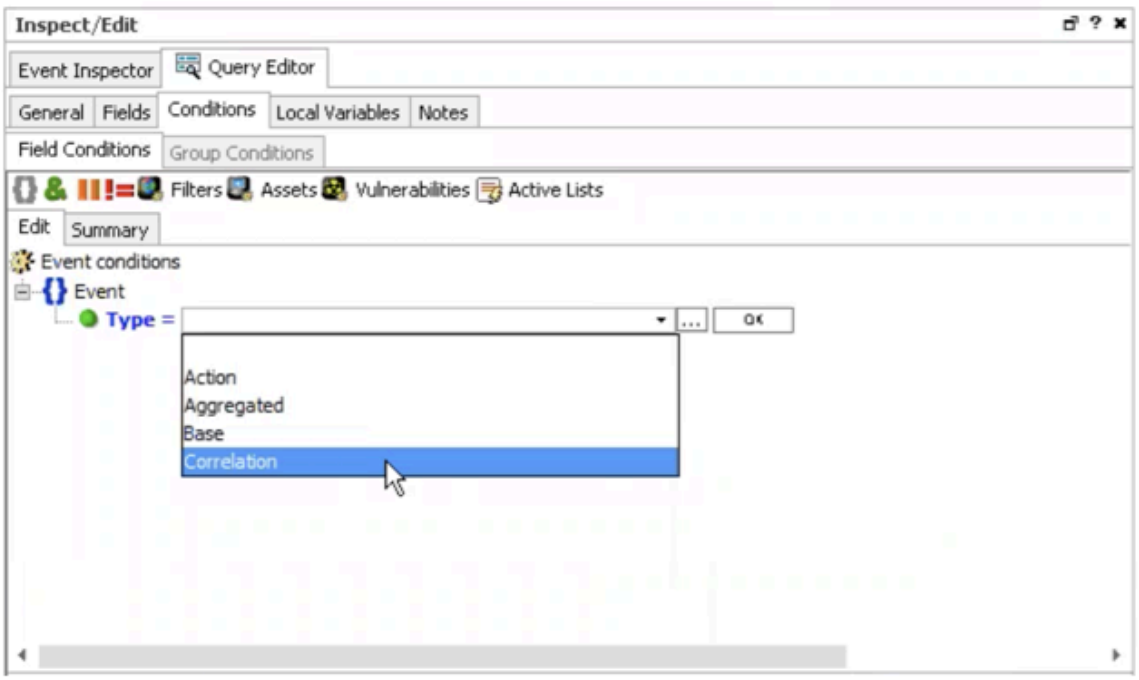
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

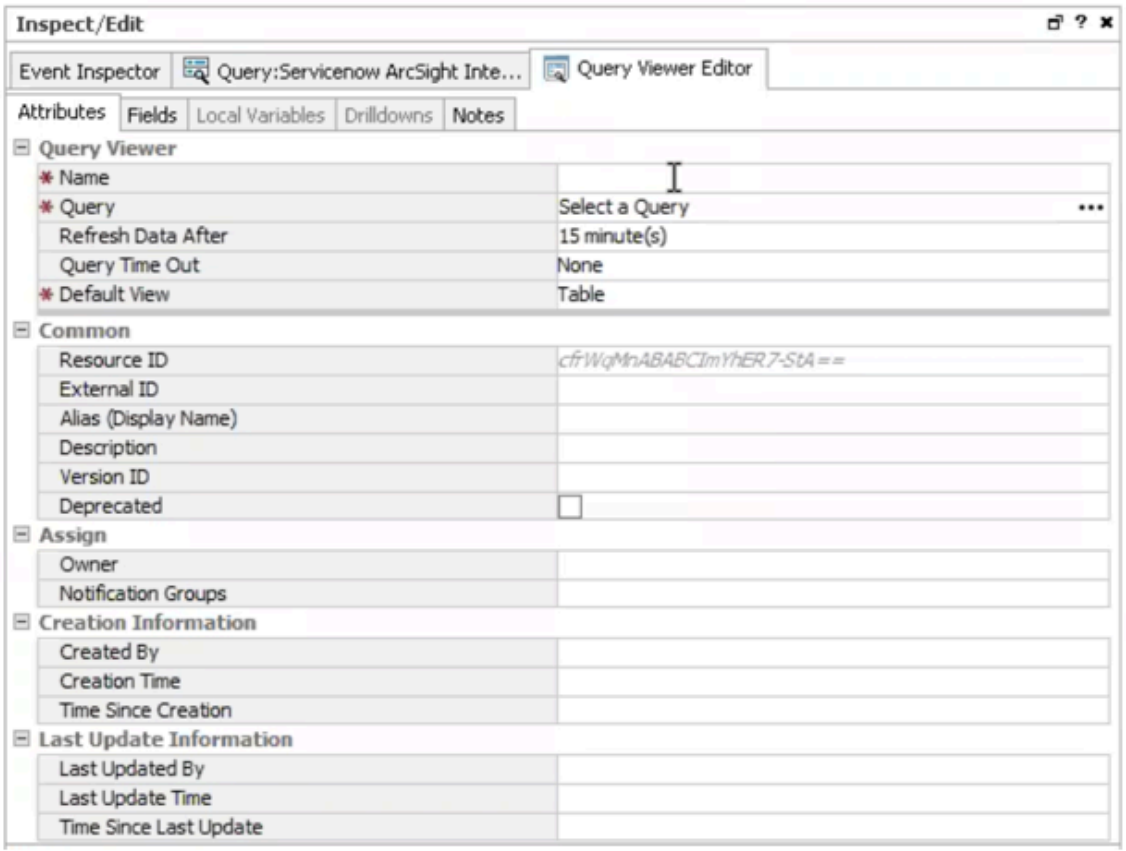
5. 수집 중에 포함해야 하는 필드를 선택합니다.
   수집이 성공하려면 *### ID*, *##* 및 *## ##* 필드를 선택해야 합니다.
6. "정렬 기준" 열 추가 링크를 클릭하고 이벤트 **ID** 필드를 선택한 후 정렬 순서를 내림차순으로 지정하여 최신 이벤트가 수집되도록 합니다.
7. 조건 탭을 클릭합니다.
8. 요약 섹션의 이벤트 조건에서이벤트를 마우스 오른쪽 버튼으로 클릭합니다.
9. 클릭 새 조건 〉 근본 〉 유형 을 클릭하고 이벤트 유형을 상관 관계로 선택합니다.

> **중요사항:**
> 상관관계 이벤트만 검색됩니다. 상관 관계에 대한 기본 이벤트는 검색되지 않습니다.

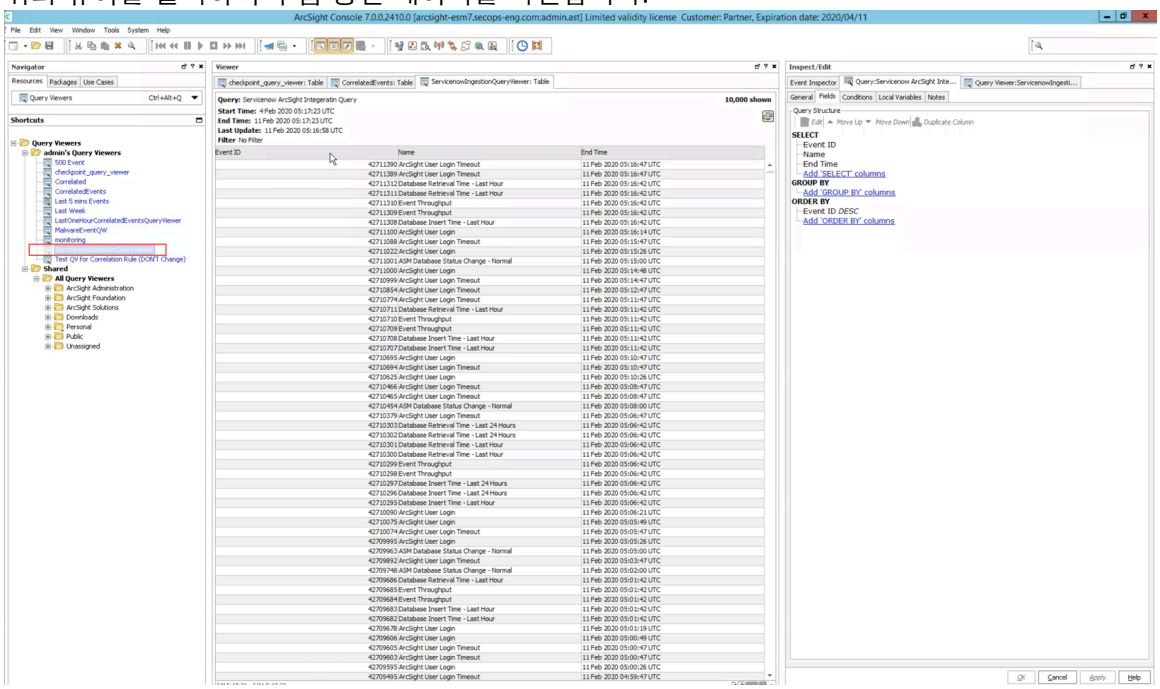


10. 확인을 클릭하여 쿼리를 저장합니다.
    다음 단계는 이 쿼리에 대한 쿼리 뷰어를 만드는 것입니다.
11. 다음으로 이동 파일 〉 신규 〉 쿼리 뷰어.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



12. 필드 탭을 클릭하고 쿼리에 지정한 필수 필드(*### ID, ##, ## ##*)가 선택되어 있는지 확인합니다.
13. 적용을 클릭하여 쿼리 뷰어를 저장합니다.
    만든 새 쿼리 뷰어가 쿼리 뷰어 섹션에 나열됩니다.
14. 쿼리 뷰어를 클릭하여 수집 중인 데이터를 확인합니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

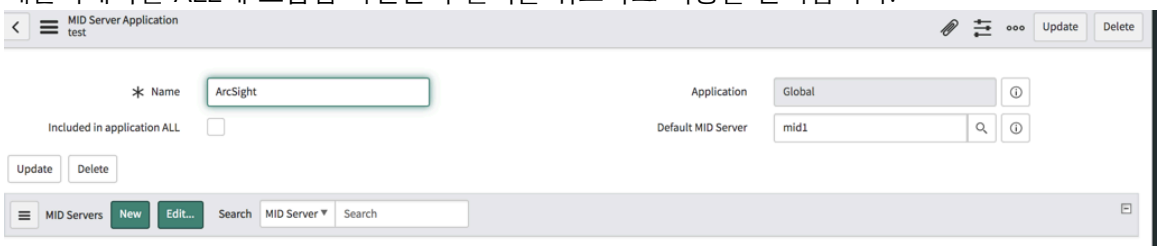
이벤트 수집 통합을 위한 **ArcSight ESM ServiceNow** 애플리케이션 설치 및 구성

인스턴스에서 통합을 ServiceNow AI Platform# 실행하기 전에 다음 설치 및 구성 단계를 완료하여 애플리케이션이 인스턴스의 및 보안 운영 제품과 ServiceNow AI Platform 제대로 통합 보안 인시던트 응답 되도록 합니다.

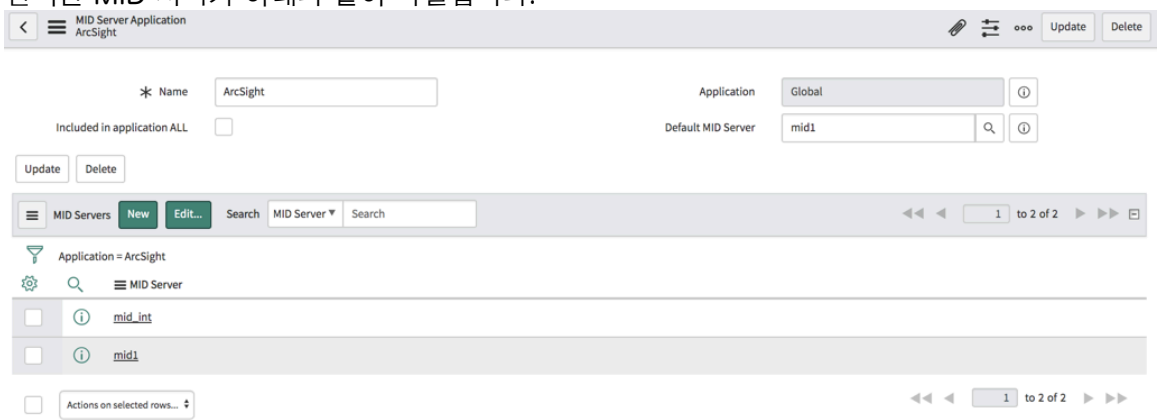
시작하기 전에
필요한 역할: sn_si.admin

프로시저

1. 통합을 위해 애플리케이션을 ServiceNow Store 설치하지 ArcSight ESM 않은 경우 를 참조 보안 운영 통합 설치 하고 단계에 따라 설치합니다.
2. 애플리케이션을 성공적으로 설치한 후 통합 〉 통합 구성 타일을 ArcSight ESM 찾습니다.
3. 애플리케이션을 구성하려면 새로 만들기를 클릭합니다.
4. 또는 구성 단추가 타일에 표시되면 클릭하여 기존 구성을 편집합니다.
5. 양식에서 필드를 채웁니다.
   새 MID 서버 애플리케이션을 작성하려면 다음 단계를 따르십시오.
   a. 다음으로 이동 **Mid Server** 〉 애플리케이션 을 클릭하고 신규를 클릭합니다.
   b. MID 서버 애플리케이션의 이름을 입력하고 기본값으로 사용할 MID 서버를 선택합니다.
   c. 애플리케이션 ALL에 포함됨 확인란의 선택을 취소하고 저장을 클릭합니다.

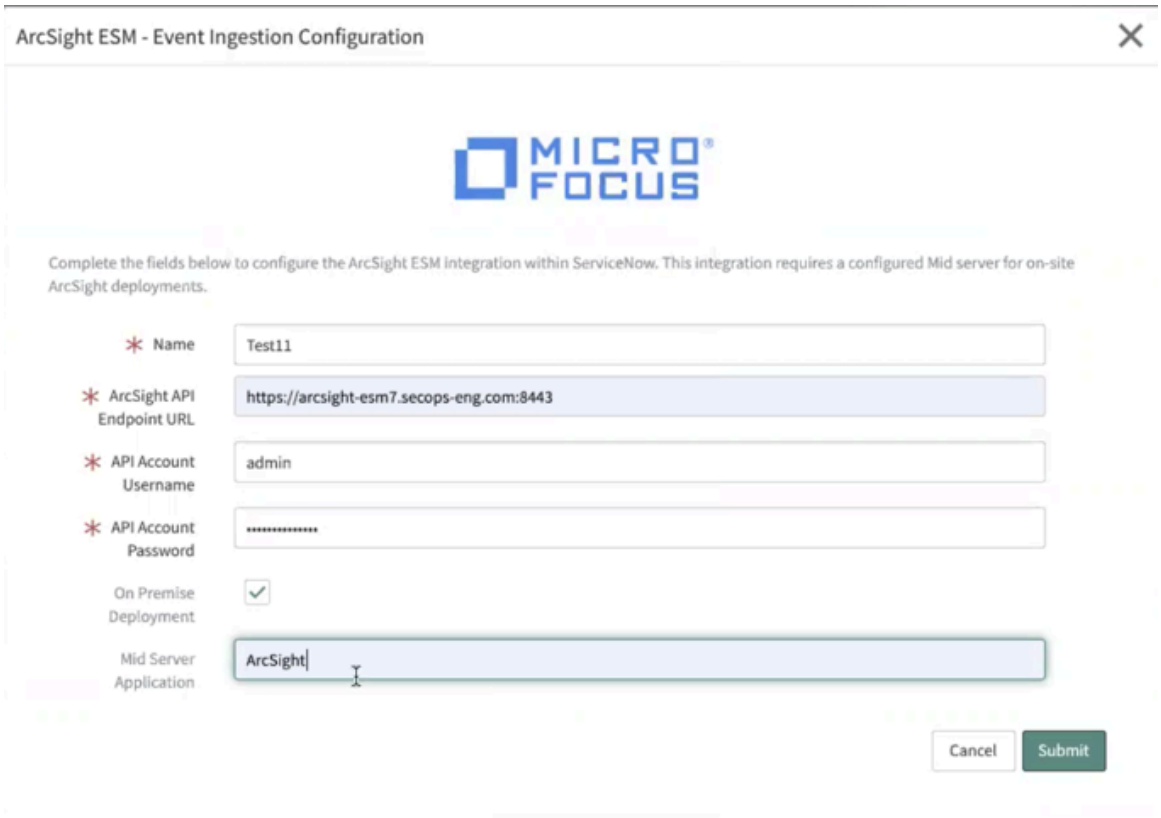


   d. 편집을 클릭합니다. 구성원 편집 페이지에서 사용 가능한 모든 MID Server를 선택하고 MID 서버 목록으로 이동한 다음 저장을 클릭합니다.
   e. 선택한 MID 서버가 아래와 같이 나열됩니다.



   가용성에 따라 MID Server 애플리케이션으로 구성된 MID Server 중 하나가 사용됩니다.
6. 구성 상세 정보를 입력하고 생성한 MID 서버 애플리케이션을 지정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



관리자 콘솔에서 수집하는 ArcSight ESM 각 상관관계 이벤트에는 인스턴스에 고유한 이벤트 프로파일이 필요합니다. 그러나 이벤트 수집 구성 양식에서 구성하는 소스는 각 프로필이 ArcSight ESM 고유한 상관관계 이벤트 유형을 수집하는 한 여러 프로필에 다시 사용할 수 있습니다.

7. 제출을 클릭합니다.
   성공적으로 확인 및 제출된 각 ArcSight ESM 서버 구성은 보안 통합 페이지에 타일로 저장됩니다. 저장된 구성 타일이 보안 통합 페이지에 표시되지 않으면 페이지 오른쪽 상단 모서리에 있는 구성 선택 목록 표시에서 예를 클릭합니다.

다음에 수행할 작업

애플리케이션을 성공적으로 설치하고 구성했습니다. 다음 단계는 이벤트 프로파일을 만드는 것입니다.

프로파일 생성

sn_si.admin 역할을 가진 사용자는 인스턴스에 프로파일을 ServiceNow AI Platform 생성하고 어떤 상관관계 이벤트가 보안 인시던트를 생성하는지 결정합니다. SIR상관관계 이벤트에서 보안 인시던트가 생성되기 전 ServiceNow AI Platform 보안 인시던트 응답 ()에는 이벤트의 필드 값이 보안 인시던트의 ServiceNow AI Platform 레이아웃에 표시되므로 실제 보안 인시던트가 생성되는 방식을 미리 볼 수 있습니다.

시작하기 전에

필요한 역할: sn_si.admin

이 태스크 정보

상관관계 이벤트는 정의된 프로파일 유형에 따라 인스턴스의 환경 ServiceNow AI Platform 으로 보안 운영 자동 수집됩니다. 프로파일은 무단 액세스 시도 또는 맬웨어와 같은 한 가지 유형의 상관관계 이벤트를 캡슐화한 것입니다.

상관관계 이벤트를 수집한 후에는 개별 상관관계 이벤트 필드를 보안 인시던트의 해당 필드에 매핑할 수 있습니다. 상관관계 이벤트를 필터링하여 보안 인시던트를 생성하는 이벤트를 지정할 수 있습니다. 예를 들어 고위험으로 식별된 상관관계 이벤트에 대해서만 보안 인시던트를 생성하는

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필터를 선호할 수 있습니다. 들어오는 중복 상관관계 이벤트가 미해결 보안 인시던트로 집계되도록 추가 이벤트 집계 기준을 정의할 수도 있습니다. 마지막으로 수집 일정을 정의하고 프로파일을 활성화할 수 있습니다.

인스턴스의 이벤트 프로파일 ServiceNow AI Platform 이름은 고유해야 하며 특정 시점에 하나의 활성 이벤트 프로파일에만 매핑할 수 있습니다.

이벤트 수집 통합을 위한 **ArcSight ESM** 프로파일 생성 및 이름 지정

상관관계 이벤트를 수집하도록 프로파일을 설정할 수 있습니다.

시작하기 전에

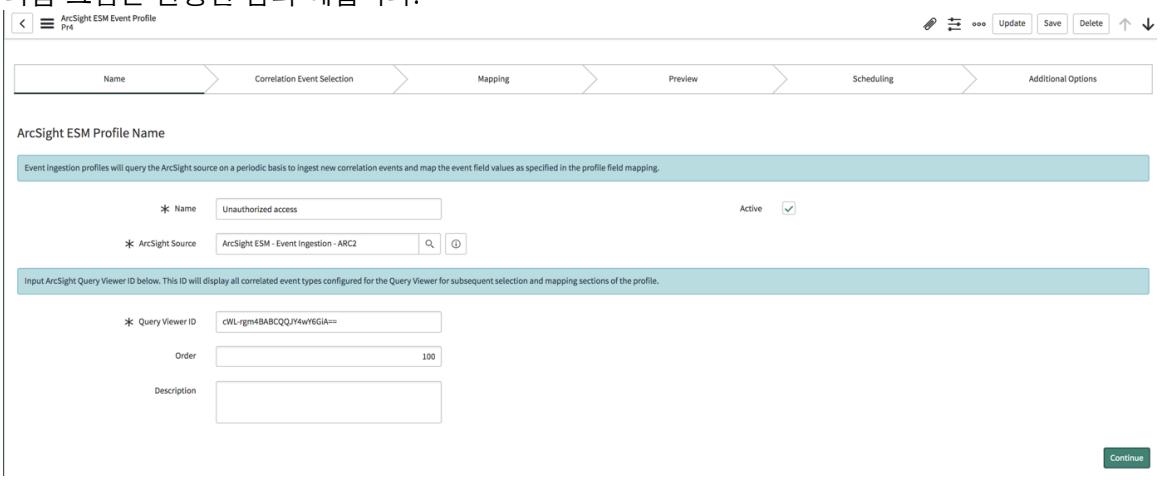
필요한 역할: sn_si.admin

프로시저

1. 인스턴스에서 상관관계 이벤트에 ServiceNow AI Platform 대한 이벤트 프로파일을 생성하려면 다음으로 이동하십시오. **ArcSight ESM** 통합 〉 **ArcSight ESM** 이벤트 프로파일.
2. 새로 만들기를 클릭합니다.
3. 필드에 내용을 입력합니다.

   완료된 양식의 예가 테이블 다음에 나옵니다.

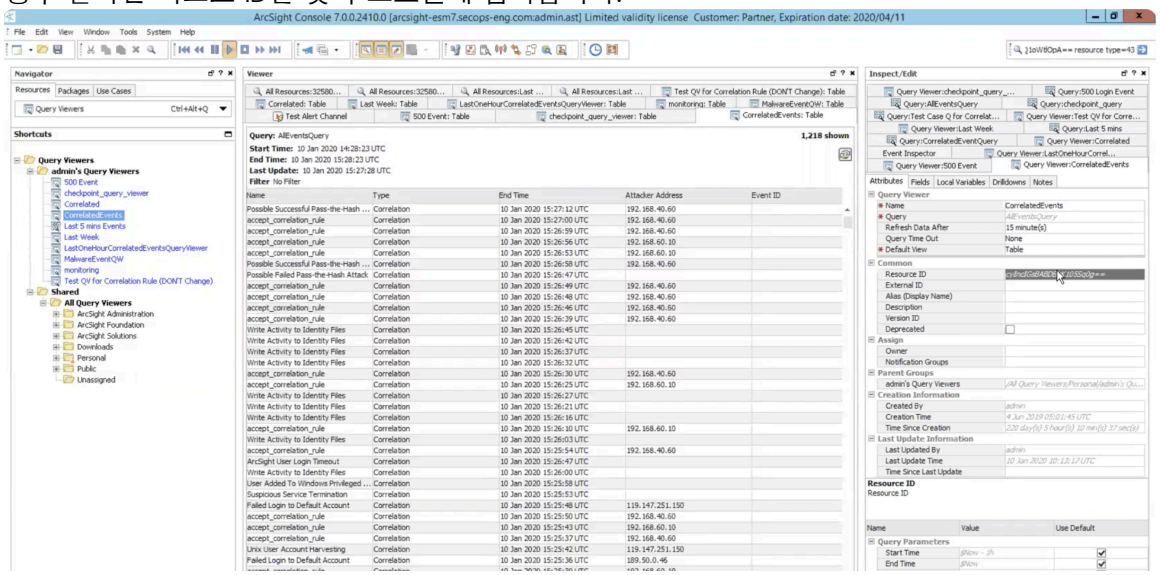
   다음 그림은 완성된 폼의 예입니다.



   프로필 세부 정보를 입력한 후 계속을 클릭합니다. 쿼리 뷰어 ID의 유효성이 검사되고 해당 리소스 ID가 쿼리 뷰어에 ArcSight ESM 있는 경우 아래와 같이 쿼리 뷰어의 이름이 반환됩니다. 유효성

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

검사에 실패하면 콘솔에 리소스 ID가 있는지 ArcSight ESM 확인합니다. 리소스 ID를 찾을 수 없는 경우 올바른 리소스 ID를 찾아 프로필에 입력합니다.



다음에 수행할 작업
다음 단계는 이전 단계에서 선택한 쿼리 뷰어에서 수집할 상관 관계 이벤트 유형을 선택하는 것입니다.

이벤트 수집 통합을 위한 **ArcSight ESM** 상관 관계 이벤트 선택

원본 및 구성된 쿼리 뷰어에 따라 ArcSight ESM 프로필에 대한 상관관계 이벤트 규칙을 선택합니다.

시작하기 전에
필요한 역할: sn_si.admin

이 태스크 정보
인스턴스의 상관관계 이벤트 선택 ServiceNow AI Platform 에 나열된 사용 가능한 상관관계 이벤트를 확인하여 수집할 상관관계 이벤트를 결정하고 보안 인시던트를 생성합니다. 각 프로파일의 목록에서 하나의 상관관계 규칙 유형만 선택할 수 있습니다.

쿼리 뷰어 양식에 지정된 쿼리 뷰어 ID 및 쿼리 뷰어 이름이 표시됩니다. 수집된 상관 관계 이벤트에 대한 구성 매핑을 만드는 데 사용할 수 있는 목록에서 상관관계 이벤트를 선택합니다.

상관관계 이벤트 목록 필드에서 드롭다운 목록을 클릭합니다. 쿼리 뷰어 콘솔에 있는 ArcSight ESM 상관 관계 이벤트 목록이 표시됩니다.

계속을 클릭하여 마법사의 다음 단계로 진행합니다.

이벤트 수집 통합을 위한 **ArcSight ESM** 상관 관계 이벤트 필드 매핑

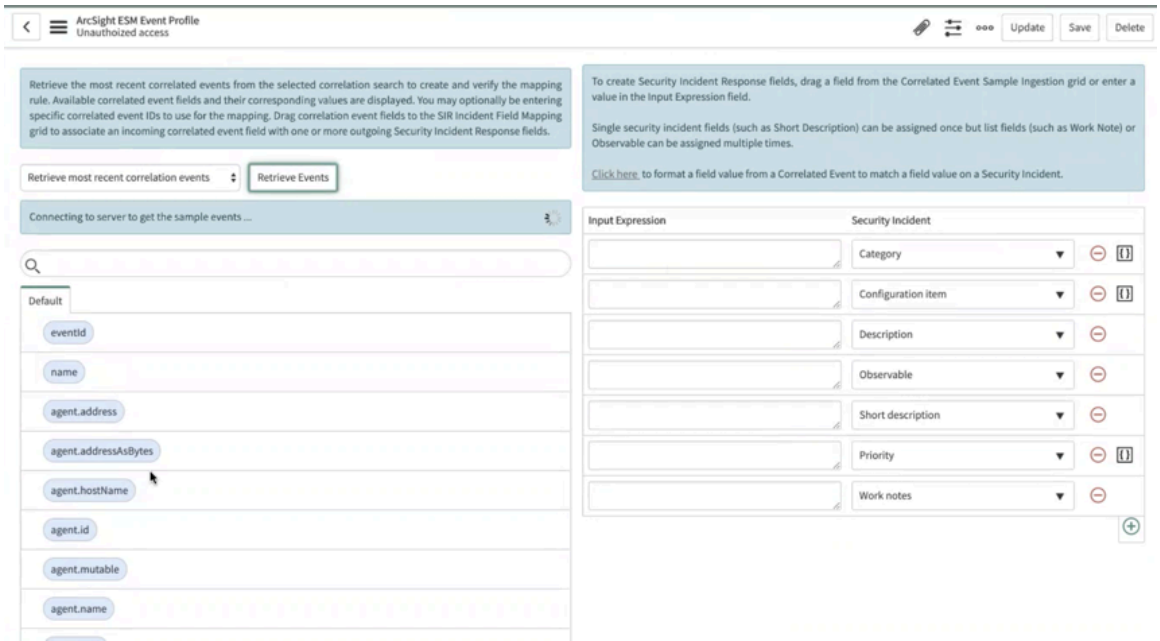
목록에서 특정 상관관계 이벤트 규칙을 식별한 후 다음 단계는 상관관계 이벤트 필드를 보안 인시던트 양식의 필드에 매핑하는 것입니다.

상관 관계 이벤트 필드 매핑 개요

매핑 단계에서는 선택한 상관관계 규칙에 대한 샘플 상관관계 이벤트를 수집할 수 있습니다. 이 매핑 단계에서는 모든 관련 상관관계 이벤트 필드 데이터가 인시던트 양식의 적절한 위치에 SIR 매핑되었는지 확인한 다음 미리 보기 섹션에서 인시던트를 시각화 SIR 할 수 있습니다.

다음 그림은 상관관계 이벤트 프로파일을 만들기 위해 제공되는 기본 매핑 구성을 보여줍니다. 보안 인시던트를 채우는 필드를 사용자 지정할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



이벤트 검색을 클릭하면 상관관계 이벤트 필드 이름과 해당 값이 양식 왼쪽에 채워집니다. ArcSight ESM 보안 인시던트 필드에 매핑할 수 있는 상관관계 이벤트 필드입니다.

콘솔에서 필드 매핑 구성 단계를 위해 수집할 몇 가지 샘플 상관관계 이벤트를 검토하는 것을 선호할 수 있습니다. 이 단계는 진행률 표시줄에 매핑이라는 레이블이 지정됩니다. 이 페이지가 표시되지 않으면 진행률 표시줄에서 매핑 을 클릭합니다. 선택한 상관관계 규칙에 대해 관리자에서 ArcSight ESM 최대 5개의 샘플 상관관계 이벤트를 수집하여 필드 매핑 프로세스를 지원할 수 있습니다. 선택한 상관 관계 이벤트에 대해 가장 최근의 상관 관계 이벤트 5개를 수집하거나 이벤트 ID를 기반으로 최대 5개의 특정 상관관계 이벤트를 수집하는 옵션이 있습니다.

다음은 상관관계 이벤트를 매핑하는 데 필요한 단계를 요약한 것입니다.

- 필드 매핑: 상관관계 이벤트 필드를 왼쪽에서 끌어서 오른쪽의 인시던트 매핑 섹션에 놓아 SIR 매핑 구성을 편집합니다. 오른쪽의 매핑은 수신 상관관계 이벤트 필드를 발신 보안 인시던트 필드와 연결합니다.
- 매핑 환경: SIR 인시던트 필드 매핑 섹션 하단에 있는 + 아이콘을 사용하여 필드를 추가하거나 제거하여 매핑 그리드를 사용자 지정합니다. 제공된 색상 코딩으로 간과되었거나 이전에 매핑된 필드를 추적합니다(매핑된 필드는 회색으로 표시되고 파란색 필드는 매핑되지 않음).
- 인시던트 생성 조건: 매핑 섹션이 완료되면 필터 조건을 정의하여 보안 인시던트를 생성해야 하는 상관관계 이벤트와 필터링해야 하는 상관관계 이벤트(예: 우선순위가 낮은 상관관계 이벤트)를 필터링할 수 있습니다. 이 작업은 상관관계 이벤트 샘플 수집 섹션 아래에 있는 인시던트 생성 조건 섹션에서 수행됩니다.
- 이벤트 집계 기준: 중복될 가능성이 있는 유사한 인시던트를 생성하는 대신 수신 상관관계 이벤트를 기존 SIR 보안 인시던트로 집계하는 추가 이벤트 집계 기준을 정의합니다. 이 추가 집계 기능은 각 프로파일에 대해 필드 일치 값 기준을 사용하여 모든 관련 보안 중요 이벤트 데이터를 단일 보안 인시던트에 배치함으로써 활성 상태의 중복 보안 인시던트 수를 줄일 수 있습니다.
- 필드 형식 변환: 경우에 따라 상관관계 이벤트의 이벤트 필드 값이 ArcSight ESM 보안 인시던트의 필드 SIR 로 직접 변환되지 않을 수 있습니다. 이러한 값의 경우 스크립트 편집기를 사용하여 매핑 단계 중에 보안 인시던트의 필드 값에 대한 형식을 지정할 수 있습니다. 비슷하지만 동일하지는 않은 값의 형식을 지정하려면 스크립트 편집기를 사용하십시오.

  예를 들어 스크립트 편집기를 사용하면 맬웨어 경보 및 바이러스 감염의 범주 값이 소스 범주에 대해 다를 수 있지만 두 값 모두 필드 번역 서식 지정 기능을 사용하여 보안 인시던트의 SIR 범주 필드에서 공통 악성 코드 활동으로 변환할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음 단계는 샘플 상관관계 이벤트를 수집하고 값을 보안 인시던트 필드에 매핑하는 SIR 것입니다.

이벤트 수집 통합을 위한 **ArcSight ESM** 매핑 생성

이 단계에서는 샘플 상관관계 이벤트를 수집하고 값을 SIR 보안 인시던트 필드에 매핑합니다.

시작하기 전에
필요한 역할: admin, sn_si.admin

이 태스크 정보
sn_si.admin 역할이 있는 사용자는 양식 왼쪽에 있는 상관 관계 이벤트 샘플 수집 열에서 최대 5개의 샘플 상관관계 이벤트를 검토하여 이벤트 필드 값을 오른쪽에 있는 SIR 인시던트 필드 매핑 열의 보안 인시던트 필드로 매핑하고 변환할 수 있습니다.
양식의 오른쪽에 있는 매핑 그리드에서 필드를 추가하거나 제거하여 사용자 지정 매핑을 생성합니다. 기본적으로 표시되는 필드는 일반적으로 보안 인시던트 응답 양식에 채워야 하는 중요한 필드입니다. 그러나 이러한 필드를 제거할 수 있으며 + 및 - 버튼을 사용하여 추가 필드를 표시할 수 있습니다.
양식 오른쪽의 매핑 그리드에서 필드를 추가하거나 제거하여 사용자 지정 맵을 생성합니다. 필드를 사용자 지정하면 보안 인시던트의 기본 매핑 그리드에 표시되지 않는 필드를 매핑 ArcSight ESM 할 수 있습니다.

프로시저

1. 매핑 양식이 표시되지 않으면 진행률 표시줄에서 매핑 을 클릭합니다.
2. 선택한 상관관계 규칙에 대한 가장 최근의 샘플 상관관계 이벤트를 끌어오거나 상관관계 이벤트 매핑 환경에 사용하려는 특정 상관관계 이벤트에 대한 고유한 상관관계 이벤트 ID를 제공할 수 있습니다.
3. 드롭다운 목록에서 다음 중 하나를 선택합니다.
   - 가장 최근의 상관관계 이벤트 검색
   - 이벤트 ID를 기준으로 상관관계 이벤트 선택

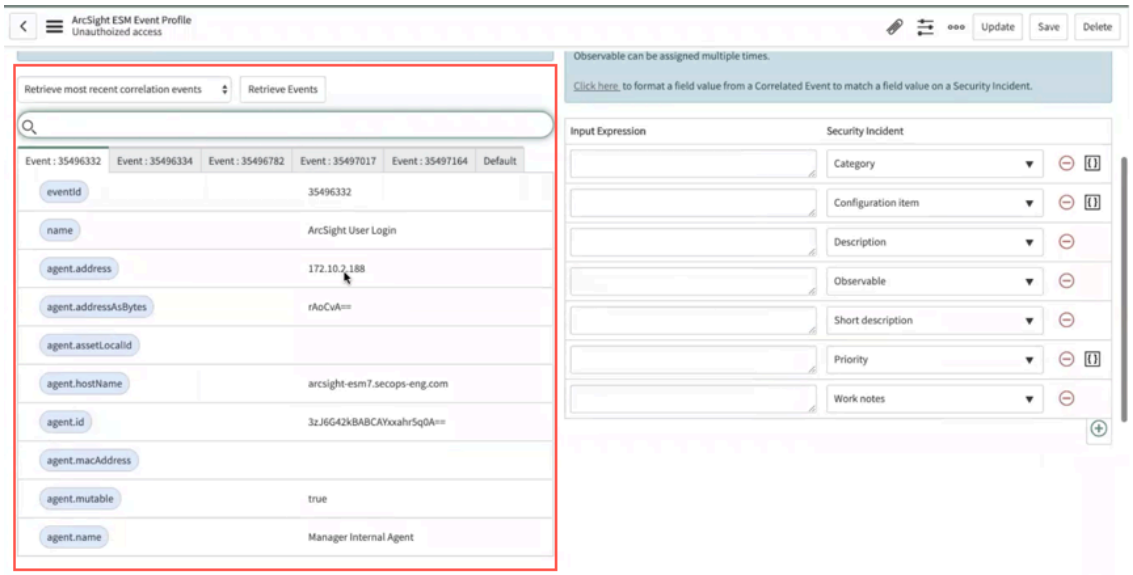
   선택한 상관관계 검색 규칙에 대한 최신 샘플 상관관계 이벤트를 ArcSight ESM 콘솔에서 가져오려면 이벤트 검색을 클릭합니다.

   상관관계 이벤트 필드와 값 결과는 개별 탭으로 표시됩니다.

   샘플 상관관계 이벤트를 끌어오기에는 몇 분 정도 걸릴 수 있습니다. 트랜잭션이 작동 중임을 나타내는 메시지가 화면 맨 위에 표시됩니다.

   다음 그림에서는 수집된 상관 관계 이벤트 또는 임포트된 샘플 이벤트에 대한 필드 이름 값 쌍이 수집 끌어오기가 완료된 후 이 양식의 왼쪽에 표시됩니다. 이러한 값은 양식의 SIR 인시던트 필드 매핑 측면에 있는 보안 인시던트 필드에 매핑하는 값입니다.

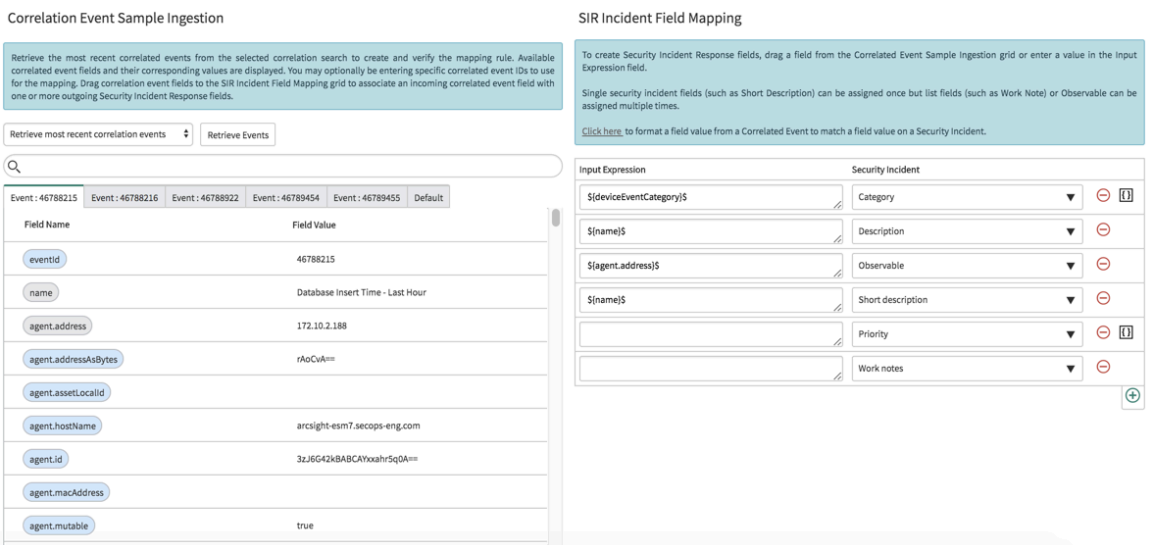
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 양식 왼쪽의 필드 값을 양식 오른쪽에 있는 보안 인시던트의 필드에 매핑하려면 양식 왼쪽에 있는 파란색 필드 이름을 길게 클릭합니다.
5. 필드 이름(예: agent.hostname)을 끌어서 보안 인시던트 열의 필드 이름 옆에 있는 입력 식 열의 필드에 놓습니다.

   매핑 프로세스에서 이벤트 필드가 간과되거나 중복되지 않도록 하기 위해 필드는 색으로 구분됩니다. 왼쪽의 연한 파란색 필드는 상관관계 이벤트 필드가 아직 선택되지 않았으며 보안 인시던트에 매핑되지 않았음을 나타냅니다. 수신 상관관계 필드를 보안 인시던트의 둘 이상의 필드와 연결하는 것을 선호할 수 있습니다.

   회색 필드는 필드가 선택되었고 보안 인시던트의 필드에 매핑되었음을 나타냅니다. 이 색상 코딩은 향후 보안 인시던트 필드 매핑에 이미 사용된 이벤트 필드를 추적하는 데 도움이 됩니다.



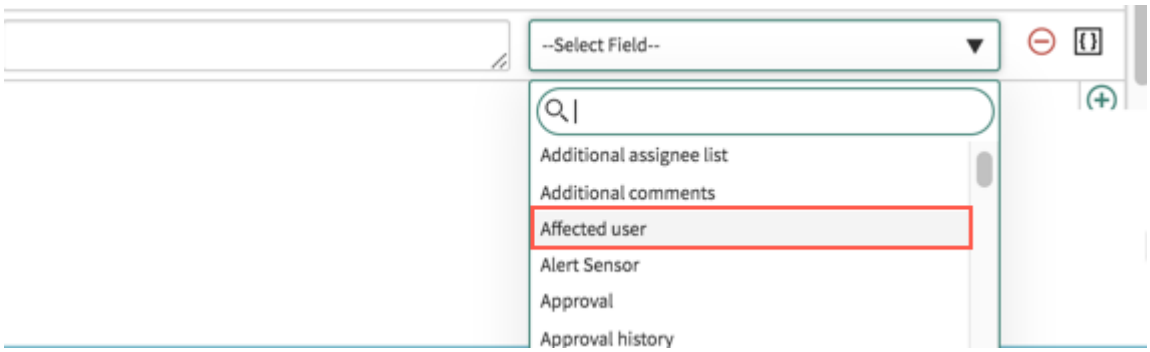
6. 양식 오른쪽의 보안 인시던트에 표시되는 기본 필드에 필드를 추가하려면 다음 단계를 따르십시오.

   a. 양식 오른쪽의 SIR 인시던트 필드 매핑 섹션 그리드 하단에서 더하기 아이콘을 클릭합니다. 새 필드가 표시됩니다.

   b. 보안 인시던트 열에서 표시되는 선택 목록을 확장하고 필드를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

새 필드의 확장된 선택 목록에서 일부 필드는 음영 처리됩니다. 다음 그림에서 ### ## #### 보안 인시던트에 매핑되었기 때문에 회색 배경입니다. 양식 왼쪽에 있는 상관관계 이벤트 필드에 대한 색상 코딩과 유사하게 오른쪽에 있는 보안 인시던트 필드에 대한 이 색상 코딩은 이미 매핑된 SIR 인시던트 필드를 추적하는 데 도움이 됩니다.



주:
동일한 보안 인시던트에 여러 옵저버블을 표시할 수 있도록 옵저버블 필드를 서로 다른 값으로 여러 번 매핑할 수 있습니다. 마찬가지로 구성 항목 및 작업 메모 필드는 여러 값을 지원합니다. 여러 값을 지원할 수 없는 필드에 두 값을 매핑하려고 하면 인시던트를 미리 볼 때 필드에 값이 없다는 오류 메시지가 표시됩니다. 마찬가지로 보안 인시던트의 필드에 여러 옵션을 선택할 수 있는 선택 목록이 있고 선택 목록에 표시되지 않는 해당 필드에 옵션을 매핑하려고 하면 보안 인시던트에 필드가 채워지지 않습니다.

c. 또는 새 행의 검색 필드에 값을 입력합니다.

d. 폼의 왼쪽에서 마우스 왼쪽 버튼을 클릭하여 입력 식 필드에서 원하는 이벤트 **ID**를 선택합니다. 끌어서 놓기 기능을 사용하여 새 필드 옆에 매핑합니다.

7. 옵션: 스크립트 편집기를 열고 계속 편집합니다.

(Optional) 스크립트 편집기에 대한 자세한 내용은 문서를 참조하십시오 스크립트 편집기를 사용하여 상관관계 이벤트 값의 형식 지정.인시던트 생성 필터링 조건

8. 옵션: 앞의 필드 매핑 단계를 완료한 후에는 인시던트 생성 조건 작성기에서 동일한 필드 값을 사용하여 들어오는 상관관계 이벤트가 충족해야 보안 인시던트를 만들기 위해 충족해야 하는 추가 기준을 정의할 수 있습니다 SIR .
인시던트 생성 조건을 설정하려면 다음 단계를 수행합니다.

a. 양식에서 인시던트 생성 조건 섹션으로 스크롤하고 조건을 기준으로 필터링 확인란을 선택하여 옵션을 활성화합니다.

(Optional) 필터 조건 작성기가 표시됩니다. 이러한 필터를 사용하여 필드에 설명된 특정 조건과 일치하는 보안 인시던트를 생성합니다.

필터 조건 작성기의 첫 번째 필드에 대한 선택 목록의 옵션은 수집한 이벤트의 상관 관계 이벤트 샘플 수집 섹션에 표시되는 필드와 일치합니다. 이러한 필드는 동적이며 수집하는 상관관계 이벤트에 따라 변경됩니다. 입력하는 기준은 대/소문자를 구분하며 상관관계 이벤트의 값과 ArcSight ESM 정확히 일치해야 합니다.

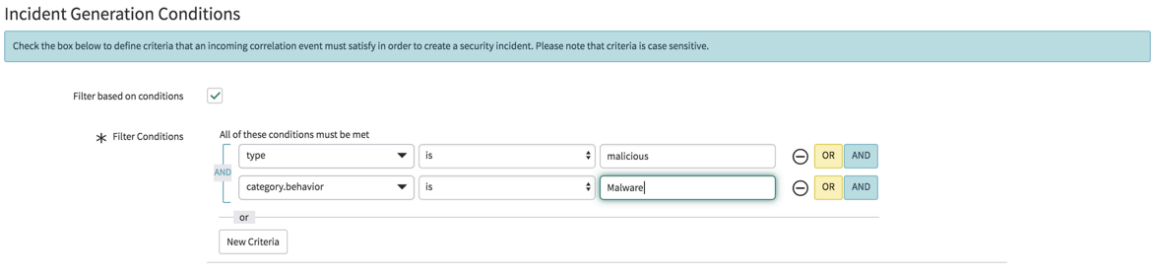
조건 작성기의 선택 목록과 필드를 사용하여 첫 번째 행에 대한 필터를 설정합니다.

b. 조건을 더 추가하려면 필드 오른쪽에서 AND 또는 **OR**을 클릭합니다.
AND를 선택하면 모든 조건이 일치해야 합니다. **OR**을 선택하면 두 조건을 일치시킬 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

c. 옵션: 두 번째 행에서 두 번째 필터 조건을 설정합니다.

(Optional) 다음 이미지는 보안 인시던트가 생성되기 전에 일치해야 하는 두 가지 조건이 있는 예입니다.



(Optional) 입력한 두 필터링 조건이 모두 일치하는 경우에만 보안 인시던트가 생성되도록 인시던트 생성 조건을 설정했습니다.

이러한 유형의 인시던트 생성 조건 필터링을 사용하면 보안 이벤트 범위를 좁히고, 기본 상관관계 검색을 수정하거나 에서 이벤트를 필터링하지 않고도 사용자가 생성하는 불필요한 보안 인시던트 수를 제한할 수 있습니다 ArcSight ESM. 추가 필터링 기준이 설정되면 모든 기준과 일치하는 상관관계 이벤트만 인시던트에 매핑됩니다.

> **주:**
> 이벤트 필드 이름에 따옴표(″), 하이픈(′), 밑줄(-) 또는 앰퍼샌드(@)와 같은 특수 문자가 있는 경우, 매핑 번역을 위해 이러한 문자를 바꿔야 할 수 있으며 중복된 이벤트 이름을 작성할 수도 있습니다. 매핑을 적절히 수행할 수 있지만 중복된 이벤트 이름이 있는 필드를 구분하기 위해 숫자 접미사가 추가됩니다. 예를 들어 첫 번째 이벤트 필드가 events.event 이고 두 번째 이벤트 필드가 events.event인 경우 나머지 표준 텍스트 문자가 동일하므로 이러한 필드를 고유하게 식별할 수 없습니다. 이 경우 두 번째 이벤트 필드에 접미사가 추가되고 필드 이름이 events@event(1)로 변경됩니다.

유사한 상관관계 이벤트를 처리하고 중복 인시던트를 방지하기 위한 이벤트 집계 기준

9. 옵션: 중복 보안 인시던트 생성을 방지하려면 수신 상관관계 이벤트가 미해결 보안 인시던트로 집계되도록 추가 이벤트 집계 기준을 정의합니다.
기준을 설정하려면 다음 단계를 수행합니다.

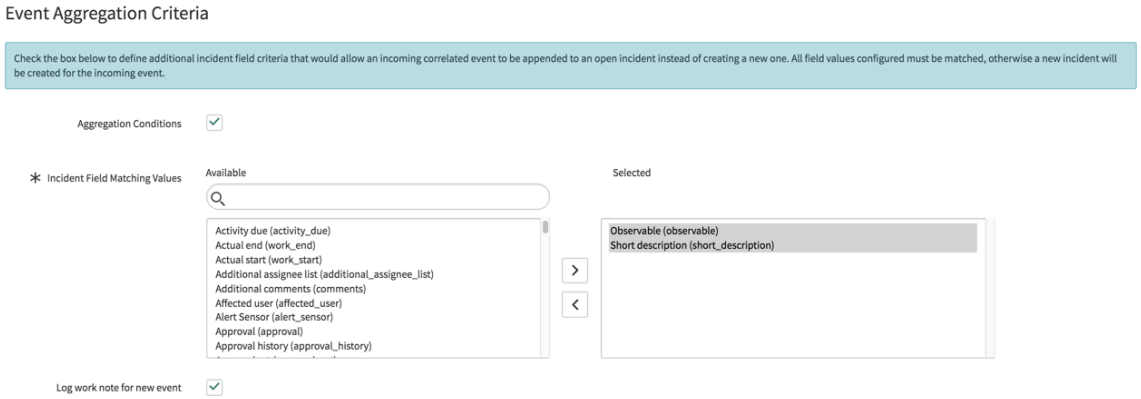
a. 양식의 이벤트 집계 기준 섹션으로 스크롤한 후 집계 조건 확인란을 선택하여 이 옵션을 활성화합니다.

(Optional) 인시던트 필드 일치 값 열이 표시됩니다. 이러한 필드 이름은 보안 인시던트에 구성된 SIR 사용자 지정 필드를 포함하는 보안 인시던트의 필드입니다.

b. 사용 가능 목록에서 기존 보안 인시던트 ServiceNow AI Platform 와 일치시킬 필드 값을 선택하고 선택됨 목록으로 이동합니다.

(Optional) 이 수신 상관관계 이벤트를 기존 보안 인시던트에 추가하려면 선택하는 모든 필드 값이 일치해야 합니다. 여기에는 옵저버블 및 구성 항목과 같이 여러 상관관계 이벤트 필드 값이 매핑될 수 있는 필드가 포함됩니다. 모든 값이 일치해야 합니다. 값의 하위 집합만 일치하면 이벤트 집계 조건이 충족되지 않고 새 보안 인시던트가 생성됩니다. 다중 값 필드 매핑에 대한 아래 스크린샷을 참조하십시오.

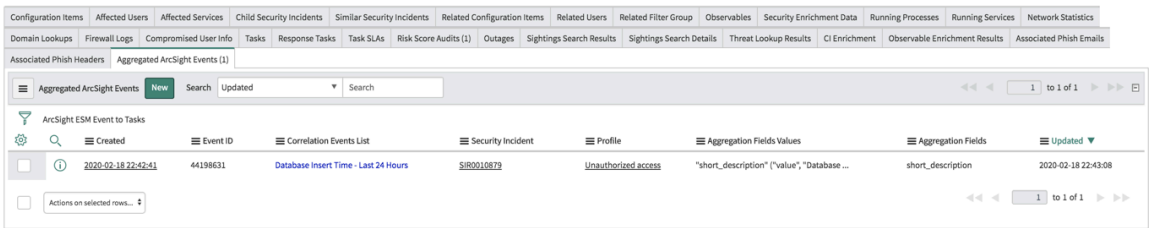
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



새 상관관계 이벤트가 매핑 단계의 집계 필드 조건에서 선택된 모든 값과 일치하면 새 상관관계 이벤트가 동일한 필드 값으로 가장 최근에 열린 보안 인시던트에 자동으로 추가됩니다. 보안 인시던트를 담당하는 SOC 분석가는 보안 인시던트의 관련 목록에서 추가된 모든 집계된 상관관계 이벤트를 볼 수 있습니다. 보안 인시던트에 대한 모든 집계된 상관관계 이벤트가 집계된 **ArcSight** 이벤트 관련 목록에 표시됩니다. 이 목록에는 관련 타임 스탬프 및 집계된 필드 값이 자세히 설명되어 있습니다. 이 정보는 이러한 상관관계 이벤트가 기존 보안 인시던트로 집계되는 이유를 이해하는 데 도움이 됩니다. 이 탭이 표시되지 않으면 관련 링크 아래에 있는 기록의 왼쪽으로 스크롤하여 모든 관련 목록 표시 링크를 클릭합니다.

주:
이 관련 목록이 표시되지 않으면 다음 단계를 수행합니다.

- 보안 인시던트 양식 헤더를 마우스 오른쪽 버튼으로 클릭하고 구성 〉 관련 목록.
- 사용 가능 목록에서 집계된 **ArcSight** 이벤트를 선택하고 선택됨 목록으로 이동한 다음 저장을 클릭합니다.
- 관련 목록 표시를 클릭합니다. 이제 관련 목록 섹션에 집계된 **ArcSight** 이벤트 탭이 표시됩니다.



c. 옵션: 보안 인시던트에 대해 이벤트가 집계될 때마다 작업 메모를 기록하려면 이 옵션을 활성화하는 확인란을 선택합니다.
작업 메모는 상관 관계가 있는 이벤트 상세 정보에 대한 링크와 함께 새로운 상관 관계가 있는 이벤트가 추가되었음을 기록합니다.

상관관계 이벤트의 값을 보안 인시던트의 SIR 필드에 매핑했습니다. 또한 인시던트 생성 필터링 기준을 사용하여 보안 인시던트 생성을 제한하는 추가 조건을 구성했습니다. 또한 이벤트 필드 값이 구성된 집계 기준과 일치하는 경우 상관관계 이벤트를 기존 SIR 보안 인시던트로 집계했습니다.

10. 하나를 선택하여 프로파일 구성을 계속합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이벤트 수집 통합에 대한 **ArcSight ESM** 보안 인시던트 미리 보기

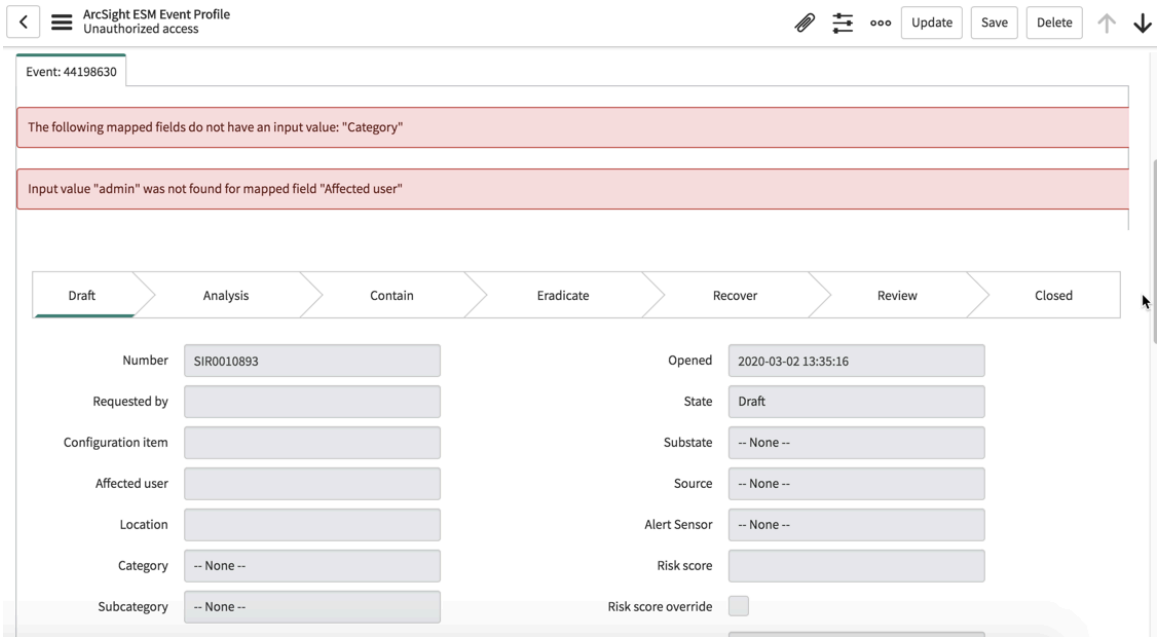
매핑 단계를 완료한 후 (SIR) 보안 인시던트에서 ServiceNow AI Platform 보안 인시던트 응답 매핑한 값을 미리 봅니다. 이 미리 보기 단계를 사용하면 보안 인시던트에 표시할 모든 상관관계 필드를 매핑했는지 확인할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.admin.

이 태스크 정보
sn_si.admin 역할을 가진 사용자는 보안 인시던트를 미리 보고 필요에 따라 매핑을 다시 편집하여 오류가 있는 필드를 수정하거나 누락된 데이터를 채웁니다. 미리 보기가 성공적으로 완료되지 않으면 예약 단계로 진행할 수 없습니다. 보안 인시던트 미리 보기는 제품에 실제 인시던트 보안 인시던트 응답 로 저장되지 않습니다.

프로시저

1. 보안 인시던트 미리 보기가 표시되지 않으면 진행률 표시줄에서 미리 보기를 클릭합니다.
2. 샘플 이벤트 ID 선택 목록에서 항목을 선택합니다.
   보안 인시던트가 표시됩니다. 필드의 정보를 변경하지 마십시오. 이 뷰는 읽기 전용 뷰이며 이 보안 인시던트의 기록은 저장되지 않습니다.
3. 보안 인시던트에서 상관관계 이벤트 값의 필드 매핑을 검토합니다.

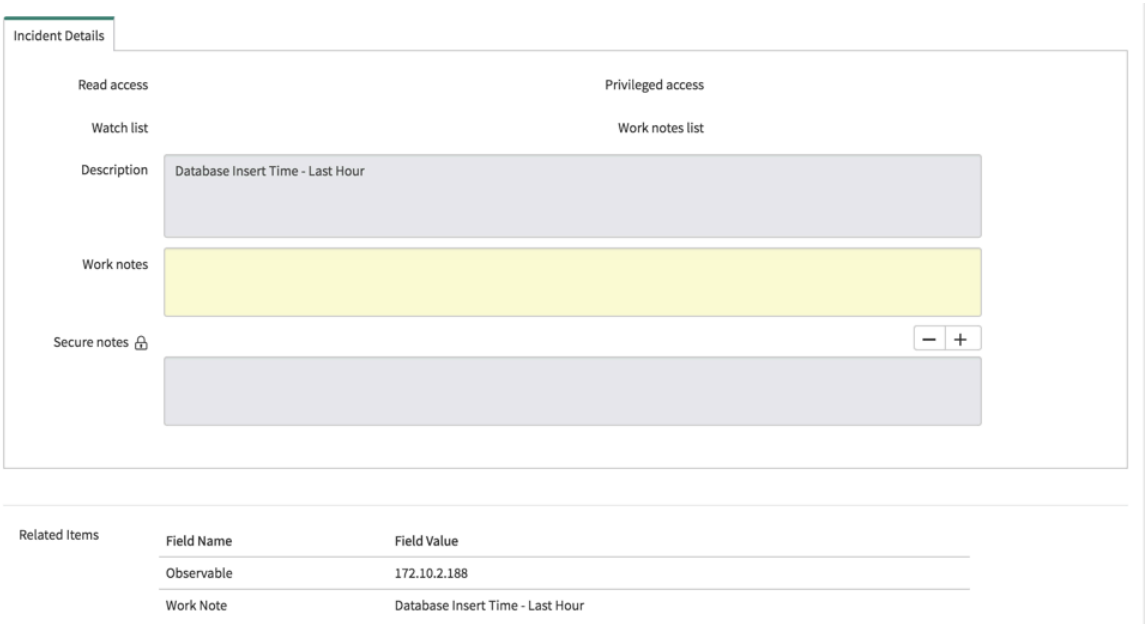


   앞의 이미지는 매핑 오류가 있는 미리 보기의 예입니다. 이 예시에서는 상관관계 이벤트의 필드 값이 SIR 인시던트 양식의 참조 필드에 허용되는 값을 갖지 않습니다. 특정 값 집합이 있는 참조 필드인 ## 필드에 대한 입력 값을 찾을 수 없음을 나타내는 오류 메시지가 표시됩니다. 따라서 이 매핑된 필드 값은 추가 수정 없이 보안 인시던트 양식에 SIR 표시되지 않습니다.

4. 이 오류를 해결하려면 진행률 표시줄에서 매핑 을 클릭합니다.
5. 매핑을 편집하여 잘못된 값을 수정하거나 누락된 데이터를 채웁니다.
6. 매핑을 다시 미리 보고 오류 메시지에 설명된 오류를 계속 수정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음 그림은 모든 오류 메시지가 해결된 후 보안 인시던트 하단 절반에 있는 인시던트 상세 정보 탭의 예입니다. 이 예에서는 설명 및 작업 메모 필드가 매핑되었으며, 이러한 필드는 상관관계 이벤트 샘플에서 ArcSight ESM 가져온 값 쌍의 값으로 채워집니다.



다음에 수행할 작업

오류 메시지가 표시되지 않고 보안 인시던트의 필드 매핑에 만족하는 경우 다음 단계는 일정을 정의하는 것입니다.

이벤트 수집 수집 일정 **ArcSight ESM** 생성

새로운 상관 관계 이벤트에 대한 폴링 또는 풀 일정을 정의할 수 있습니다. 이 단계에서 상관관계 이벤트 검색에 대한 기존 설정을 확인하거나 필요에 따라 일정을 수정할 수 있습니다. 또한 이 단계에서는 날짜 범위를 사용하여 과거 상관관계 이벤트를 검색할 수 있습니다.

시작하기 전에

필요한 역할: sn_si.admin.

이 태스크 정보

스케줄링 단계 중에 과거 상관관계 이벤트를 수집할지 여부를 선택할 수 있습니다. 또한 프로파일 구성과 일치하는 향후 새 상관관계 이벤트를 폴링할 빈도를 선택합니다.

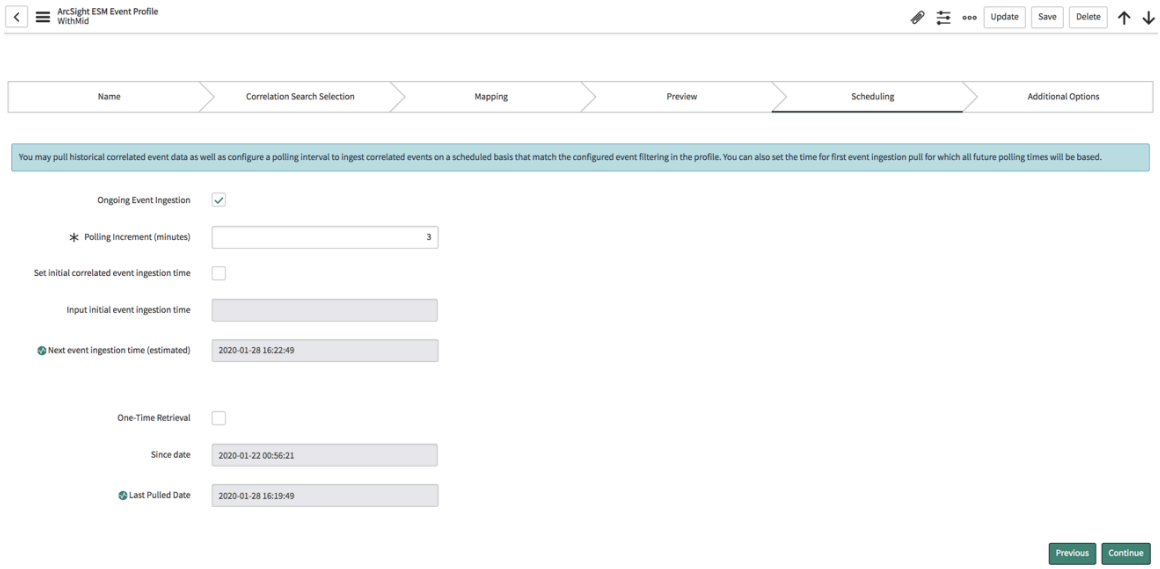
sn_si.admin 역할을 가진 사용자는 프로파일별로 이러한 폴링 간격을 구성합니다. 상관관계 이벤트 수집 통합의 ArcSight ESM 성능은 다른 폴링 간격의 영향을 받을 수 있습니다. 일정을 세울 때, 서버의 폴링 오버헤드를 ArcSight ESM 줄이는 것과 이벤트가 생성되거나 업데이트될 때 가능한 한 빨리 알림을 받으려는 욕구 사이에서 균형을 맞추는 것이 좋습니다. 모든 프로파일에 대해 5분 기본값이 설정되어 있지만 필요한 경우 이 설정을 1분 정도로 수정하는 것을 선호할 수 있습니다.

신규 및 업데이트된 상관관계 이벤트 끌어오기

프로시저

1. 진행률 표시줄에 스케줄링 페이지가 표시되지 않으면 스케줄링을 선택합니다.
2. 〈ArcSight〉 콘솔에서 상관관계 이벤트를 끌어오는 방법과 시기를 예약하려면 하나를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



초기 상관관계 이벤트 수집 시간을 예약하는 예로, 현지 시간으로 하루에 한 번 실행되는 일일 ArcSight ESM 보안 검사가 있는 경우, 현지 시간으로 오전 4시 5분에 실행되도록 인스턴스에서 해당 상관관계 이벤트 프로파일을 ServiceNow AI Platform 설정하여 보안 장애 이벤트를 즉시 캡처하고 보안 인시던트를 만들 수 있습니다. 초기 이벤트 수집 필드에 04 05 00 을 입력합니다. 증분(분) 필드에 1440 (24시간)을 입력하여 초기 이벤트 수집으로부터 24시간 동안 다음 이벤트 수집을 예약합니다. 초기 이벤트 수집 시간과 다음 이벤트 수집 시간이 모두 필드에 표시됩니다.

3. 이 예제의 설정을 구성하려면 다음 단계를 수행합니다.

a. 예약 페이지가 표시되면 진행 중인 이벤트 수집 확인란을 선택하여 이 옵션을 활성화합니다.

b. 증분(분) 필드에 1440 (24시간)을 입력합니다.

c. 초기 상관 관계 이벤트 수집 시간 설정 확인란을 클릭하여 초기 이벤트 수집 및 다음 이벤트 수집 필드를 편집할 수 있습니다.

d. 초기 이벤트 수집 시간 필드에 04 05 00을 입력합니다.
다음 이벤트 수집 시간(예상) 필드에 다음 이벤트 수집 시간이 표시됩니다.

4. 계속을 클릭하여 추가 옵션 페이지로 이동합니다.

> **주:**
> 하루에 생성하고 집계할 수 있는 기본 보안 인시던트 수와 플로우 기간은 통합 설정에서 정의됩니다 ArcSight ESM . 필요한 경우 이러한 설정을 수정할 수 있습니다. 자세한 내용은 ArcSight ESM 이벤트 수집 통합을 위한 통합 설정 문서를 참조하십시오.

추가 옵션: 인시던트 상태에 따라 **SIR** 상호 관련된 이벤트 업데이트 및 종결을 자동화

통합 ArcSight ESM 에는 양방향 인터페이스가 있어 상관관계 이벤트를 통해 보안 인시던트를 생성하고, 보안 인시던트가 생성되거나 종결되면 보안 인시던트 번호, 할당 그룹, SIR 인시던트 URL 등의 관련 인시던트 상세 정보로 상관관계 이벤트를 업데이트할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

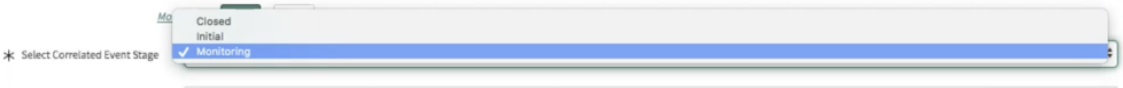
프로시저

1. 진행률 표시줄에 추가 옵션 페이지가 표시되지 않으면 추가 옵션을 선택합니다.
2. 아래 지침에 따라 보안 인시던트가 생성될 때 상관 관계가 있는 이벤트를 업데이트하기 위한 구성을 완료합니다.

   상관 관계가 있는 이벤트 스테이지가 구성되지 않음: 인스턴스에 상관 관계가 있는 이벤트 스테이지 ServiceNow AI Platform 를 구성하지 않은 경우 상관 관계가 있는 이벤트 스테이지 업데이트 선택 목록에 스테이지 할당 - 초기 설정 만 표시됩니다. 스테이지를 구성하려면 다음 단계를 수행합니다.

   - Enter Stage Resource ID 필드에 리소스 ID를 입력하고 **Submit**을 클릭합니다. 콘솔에서 자원 ID가 확인 ArcSight ESM 되고 다음 화면이 표시됩니다.

   - 저장을 클릭하여 새 단계(모니터링)를 저장합니다.
   - Select Correlated Event Stage 드롭다운 목록을 누릅니다.



   - 목록에서 새로 생성된 스테이지를 선택할 수 있습니다.

   상관 관계가 있는 이벤트 단계가 이미 구성됨: 상관 관계가 있는 이벤트 단계를 이미 구성한 경우 다음 단계를 수행합니다.

   - 상관 관계가 있는 이벤트 스테이지 업데이트 선택 목록에서 이전에 할당된 스테이지 사용을 선택합니다.
   - 아래와 같이 상관 관계 이벤트 스테이지 선택 목록에서 기존 스테이지를 선택합니다.

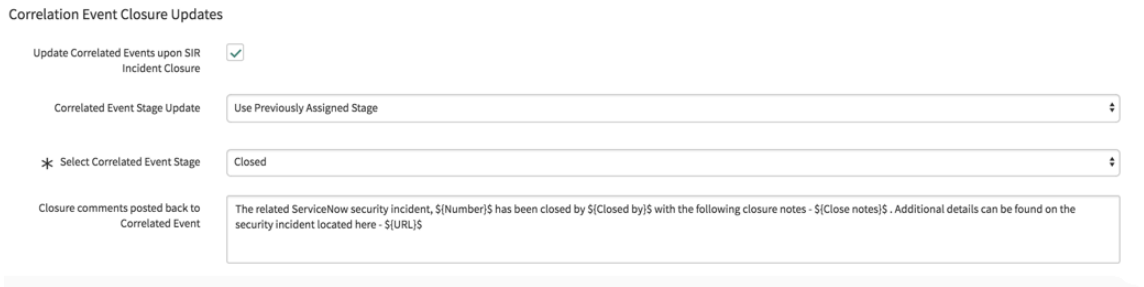
   - 상관 관계 이벤트에 다시 게시된 초기 의견: 상관 관계 이벤트 단계 값을 업데이트하는 것 외에도 상관 관계 단계 주석에 의견을 게시할 수도 있습니다. 지침에 나와 있는 것처럼 Security Incident Response 인시던트 양식의 필드에 $$ 형식을 사용하여 대체 변수를 추가하거나 수정하는 등 댓글 섹션에 표시된 기본 텍스트를 편집할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
콘솔에 정의된 ArcSight ESM 기본 단계를 사용하거나 사용자 지정 단계를 생성할 수 있습니다. 새 스테이지를 만들려면 다음 단계를 수행합니다.

- ArcSight ESM 콘솔에서 파일 〉 신규 〉 스테이지. 검사/편집 탭이 표시됩니다.
- 새 스테이지를 정의하고 사용자 필요 확인란은 선택하지 않습니다. 스테이지가 올바르게 정의되었고 이벤트 수명주기에서 올바른 위치에 있는지 확인합니다.

3. 상관 관계가 있는 이벤트 종결 자동화 섹션에서 보안 인시던트가 종결되었을 때 업데이트하는 방법을 정의할 수 있습니다.
4. 양식에서 필드를 채웁니다.



5. Finish(마침)를 클릭하여 구성을 완료합니다.
확인 대화 상자가 표시됩니다. 통합에 대한 설정 및 구성을 성공적으로 완료했습니다. 이 프로파일을 활성화하여 일정에 따라 콘솔에서 상관관계 이벤트를 ArcSight ESM 끌어옵니다.

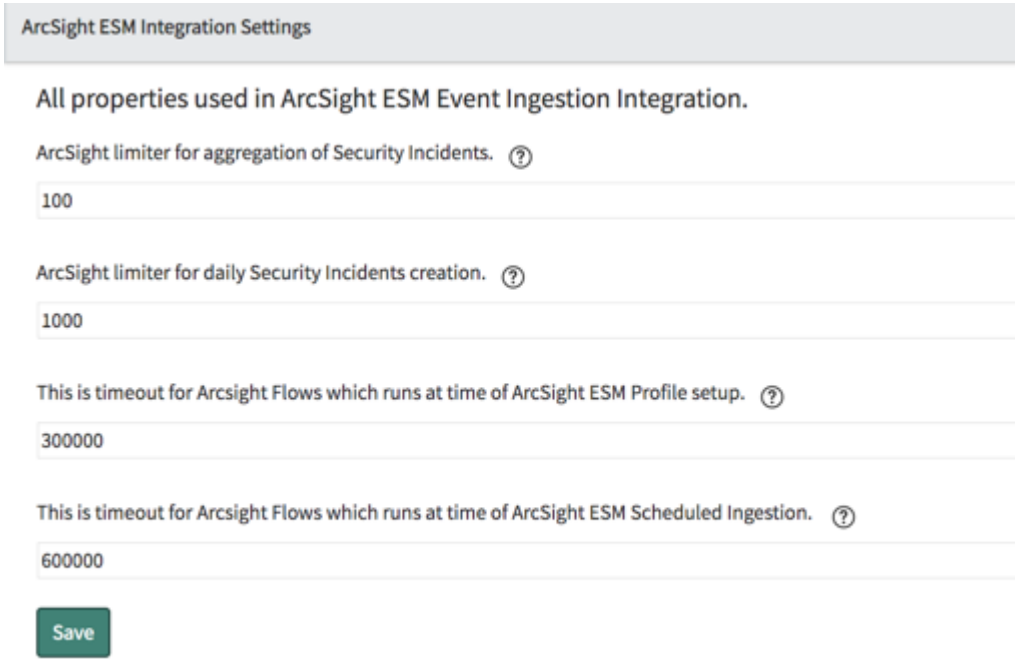
ArcSight ESM 이벤트 수집 통합을 위한 통합 설정

이 옵션을 사용하여 기본 수집 설정을 수정합니다 ArcSight ESM .

시스템 속성을 수정하려면 *sn_si.admin* 역할의 사용자로 로그인하고 **ArcSight ESM** 통합 〉 **ArcSight ESM** 통합 설정.

기본 구성 설정이 표시됩니다. 필요한 경우 이러한 설정을 수정할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

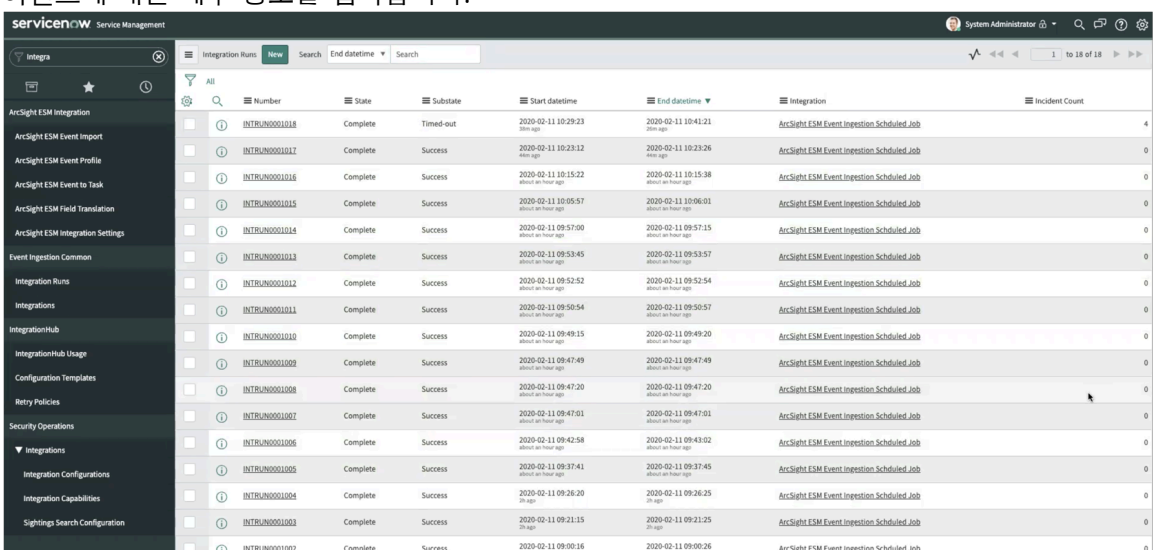


이벤트 수집 통합 문제 해결 **ArcSight ESM**

이 섹션에서는 이벤트 수집 중에 발생할 수 있는 오류를 해결하는 방법에 대한 정보를 제공합니다.

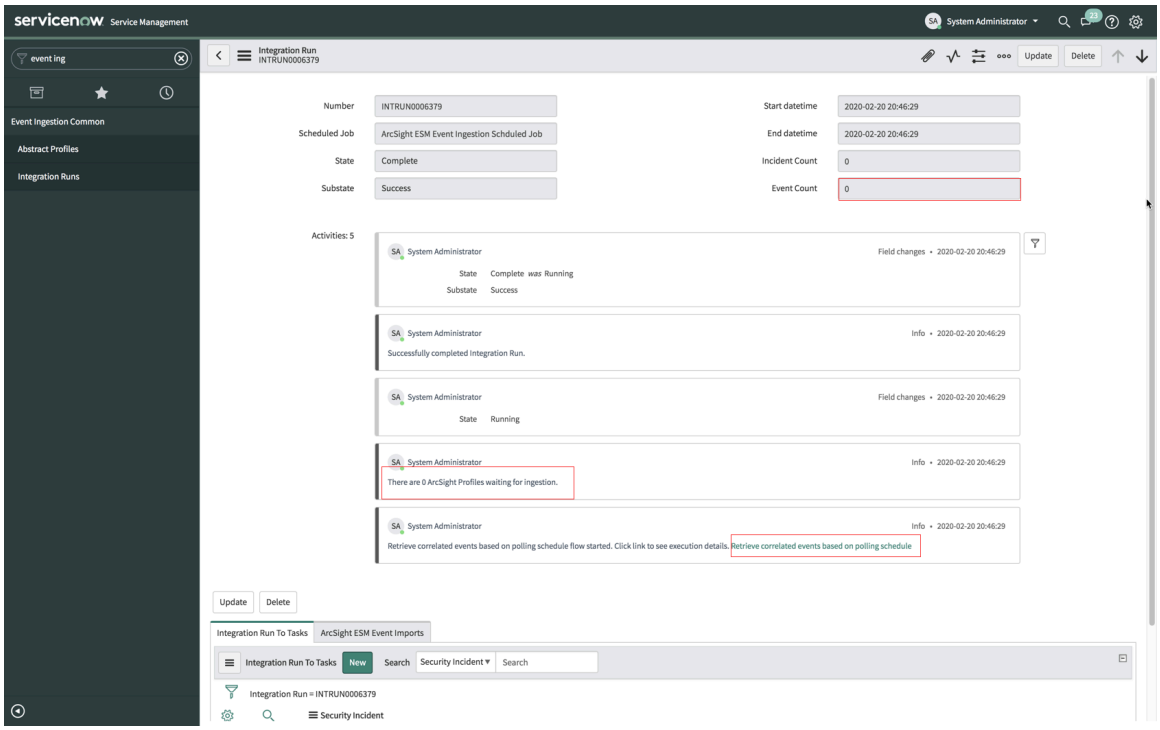
통합 실행

다음으로 이동 이벤트 수집 공통 〉 통합 실행. 통합 실행은 1분마다 수행되며 예약된 작업 중에 수집된 이벤트에 대한 세부 정보를 캡처합니다.



통합 실행 목록과 각 실행의 상태(성공, 시간 초과, 대기 중) 및 생성된 보안 인시던트 수를 볼 수 있습니다. 번호 링크를 클릭하여 자세한 통합 실행 페이지로 드릴다운합니다.

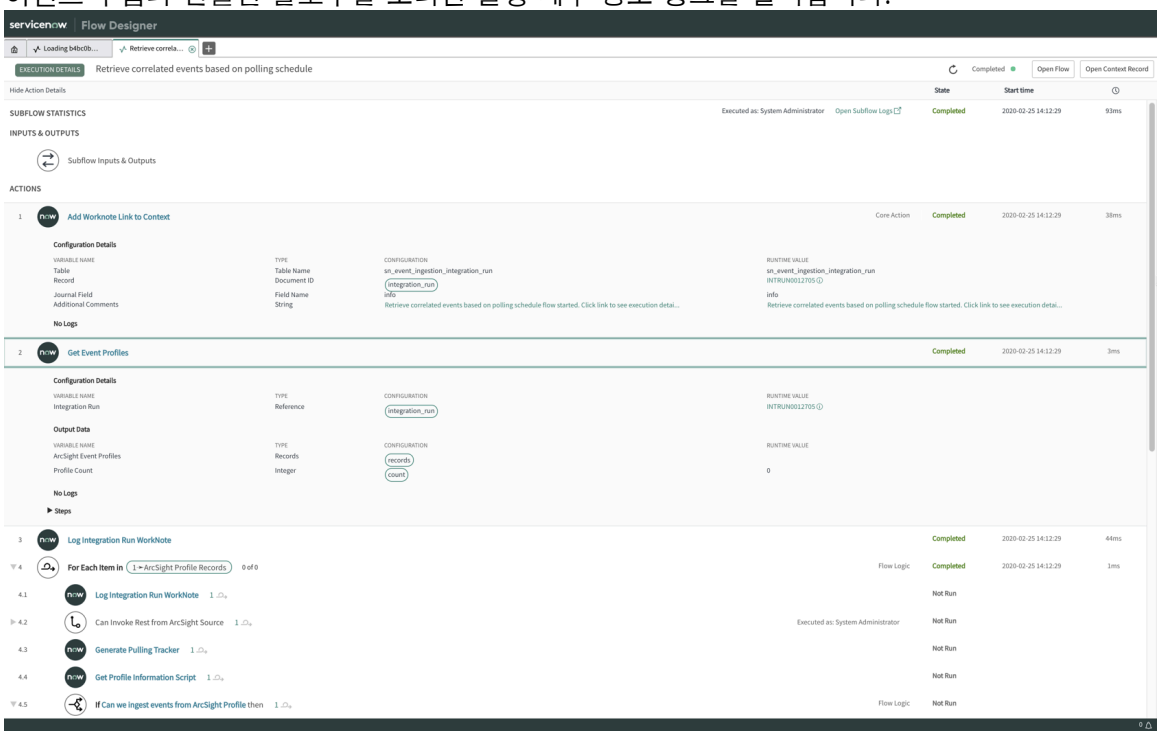
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



수집된 이벤트 수, 상태, 보안 인시던트로 변환된 이벤트, 수집 중에 수행된 다양한 작업과 같은 상세 정보를 볼 수 있습니다. 또한 링크를 클릭하여 플로우 실행 상세 정보를 볼 수 있습니다.

플로우 실행 상세 정보

이벤트 수집과 연결된 플로우를 보려면 실행 세부 정보 링크를 클릭합니다.



플로우의 일부로 실행된 다양한 작업과 하위 플로우를 자세히 설명하는 플로우의 단계별 실행을 볼 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이벤트 수집 통합을 위한 프로파일 복사 **ArcSight ESM**

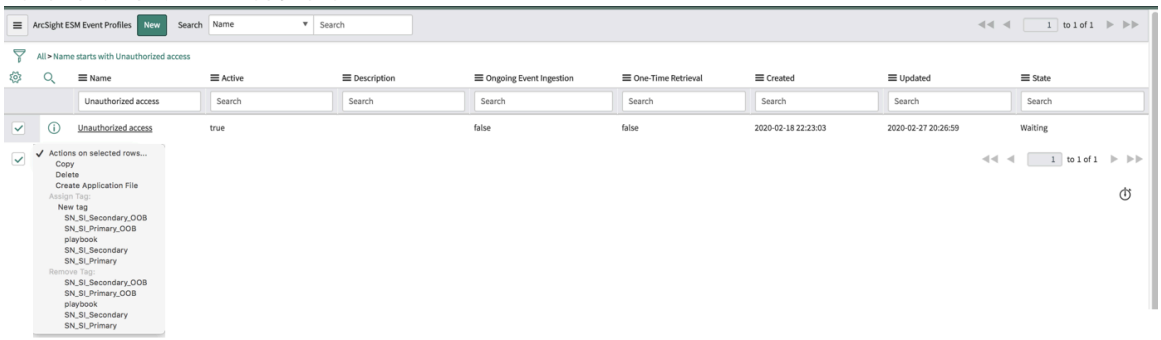
새 프로파일을 생성하는 대신 기존 프로파일 및 관련 설정을 복사합니다. 여러 프로필을 만드는 경우 기존 프로필의 설정을 다시 사용하려면 프로필을 복사하여 시간을 절약할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.admin

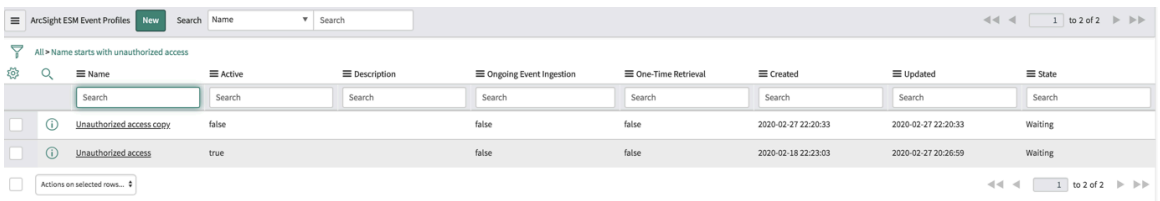
이 태스크 정보
sn_si.admin 역할을 가진 사용자가 프로파일을 복사하는 경우 프로파일 중복을 방지하기 위해 프로파일 이름이 처음에 수정됩니다. 또한 복사된 프로파일이 비활성화(false)되므로 컨피그레이션을 완료하기 전에 실수로 활성화되지 않습니다. 이미 미리 보고 확인한 보안 인시던트에 대해 프로파일을 복사하고 기존 맵을 사용합니다.

프로시저

1. 다음으로 이동 모두 〉 **ArcSight ESM** 통합 〉 **ArcSight ESM** 이벤트 프로파일.
2. 표시되는 ArcSight 프로파일 목록에서 복사할 프로파일을 선택하고 선택한 행에 대한 작업 선택 목록에서 복사를 클릭합니다.



프로파일이 복사되어 목록에 표시됩니다. 복사본에는 매핑 및 일정 구성을 포함하여 원래 프로필의 모든 설정이 포함됩니다. 프로파일의 이름에는 사본이 포함되어 있습니다. 원본 프로파일이 활성화되었지만(true) 이 시점에서는 복사본이 비활성화됩니다(false). 복사된 프로파일의 값을 편집하고 필요에 따라 구성 설정이 새 프로파일에 적용되도록 이름을 바꿀 수 있습니다.



기존 프로파일에서 새 프로파일로 설정을 복사했습니다. 프로파일을 활성화해야 하므로 활성 열 상태가 false로 설정됩니다.

스크립트 편집기를 사용하여 상관관계 이벤트 값의 형식 지정

수집된 상관관계 이벤트 값에서 직접 매핑된 필드 외에도 스크립트 편집기를 사용하여 매핑 단계 중에 보안 인시던트의 필드 값에 대한 서식을 지정합니다.

시작하기 전에
필요한 역할: sn_si.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보

스크립트 편집기는 보안 인시던트에서 지원하는 ServiceNow AI Platform SIR 값이 범주, CI(구성 항목), 옵저버블 및 기타 보안 인시던트 필드에 매핑되도록 상관관계 이벤트 필드의 값을 ArcSight ESM 변경합니다.

경우에 따라 ArcSight ESM 상관관계 이벤트 값이 보안 인시던트의 범주, CI(구성 항목) 및 옵저버블 필드와 같은 참조 필드에 매핑됩니다. sn_si.admin 역할을 가진 사용자는 매핑된 이벤트 필드 값을 편집하여 인시던트 필드 형식 및 예상되는 값에 맞게 형식 또는 데이터 값을 변환하는 것을 선호할 수 있습니다. 상관관계 이벤트의 값을 ArcSight ESM 보안 인시던트의 이러한 필드에서 SIR 지원하는 값으로 변환하려면 스크립트 편집기를 사용합니다.

프로시저

1. 매핑 양식이 표시되면 링크를 클릭하여 스크립트 편집기를 엽니다.
2. 선택 목록에서 편집할 값의 대상 필드를 선택합니다.
3. 또는 SIR 인시던트 필드 매핑 섹션에서 필드 옆에 있는 대괄호 아이콘 [{}] 을 클릭하여 해당 필드의 스크립트 편집기를 엽니다.

   경우에 따라 스크립트 포함이 구성 항목 필드에 적합할 수 있습니다. 예를 들어, 상관 관계 이벤트의 경우 구성 항목의 값이 일치하지 않을 수 있습니다.

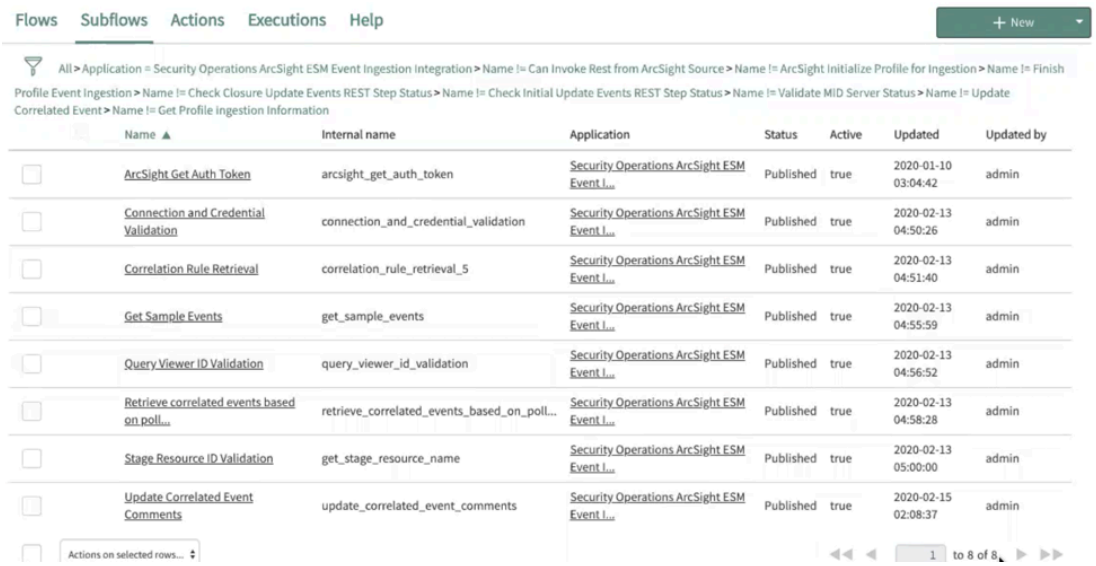
   다음 그림과 같이 구성 항목 필드의 CMDB에서 ServiceNow AI Platform 호스트 이름과 일치하는 항목을 찾을 수 없는 경우 IP 주소가 발견되면 구성 항목 필드를 채우도록 규칙을 편집할 수 있습니다.

   대상 필드에 필드가 표시된 상태로 편집기가 열립니다.
4. 스크립트에 대한 변경 내용을 입력하고 업데이트를 클릭하여 변경 내용을 저장합니다. ArcSight ESM 필드 번역 테이블이 표시됩니다.
5. 테이블을 닫고 매핑 양식으로 돌아갑니다.

이벤트 수집 통합을 통한 **ArcSight ESM** 플로우 디자이너 사용량

Integration Hub 및 Flow Designer를 사용하면 통합에 여러 플로우, 하위 플로우 및 작업을 사용할 수 있습니다 ArcSight ESM .

이러한 하위 플로우를 보려면 다음으로 이동합니다. 플로우 디자이너 〉 디자이너 을 클릭하고 하위 플로우 탭을 클릭합니다. 아래 그림은 프로필 만들기 및 예약된 수집 작업 중에 사용되는 중요한 하위 플로우를 보여줍니다.

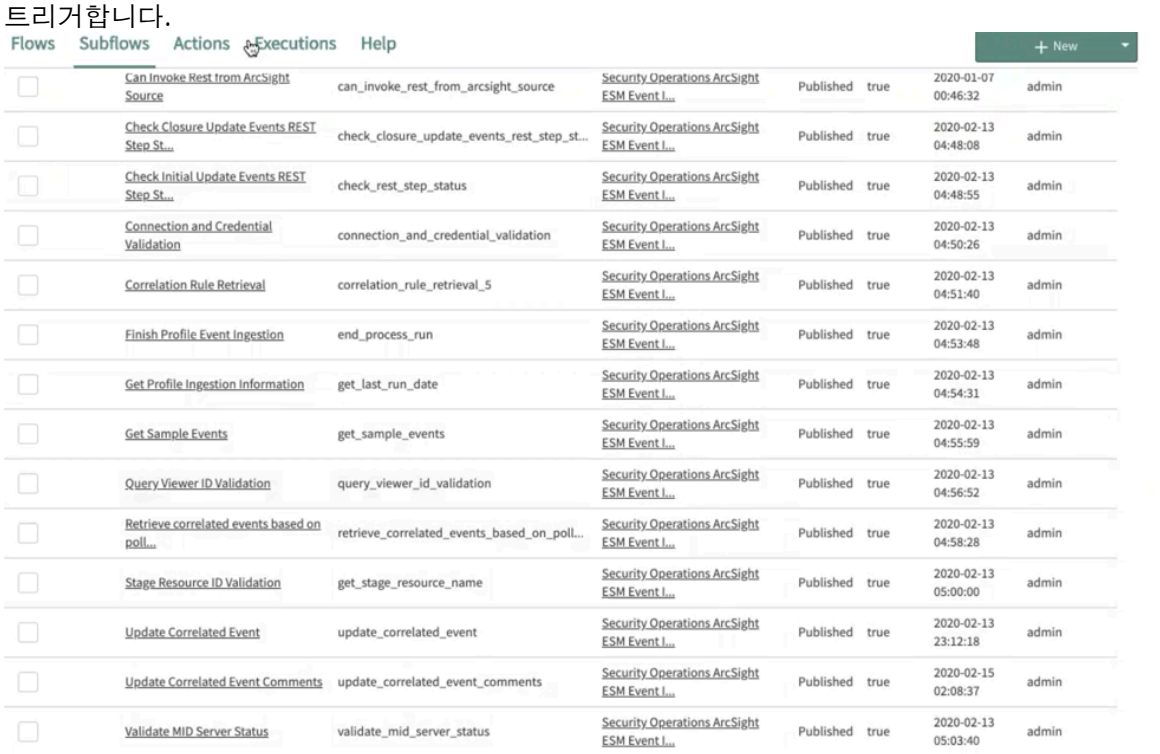


© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이러한 하위 플로우는 실행 순서에 따라 아래에 나열되어 있습니다.

- 연결 및 자격 증명 확인: 이 하위 플로우는 ServiceNow 서버 및 지정된 자격 증명과의 ArcSight ESM 연결을 확인합니다. 이 하위 플로우는 **ArcSight ESM -** 이벤트 수집타일의 구성 버튼을 클릭할 때 사용됩니다. 보안 운영 〉 통합 〉 통합 구성 페이지.
- **ArcSight** 인증 토큰 가져오기: 이 하위 플로우는 ArcSight ESM 로그인 서비스를 사용하여 ArcSight ESM 사용자 이름 및 암호에서 인증 토큰을 작성합니다. 로그인 서비스는 다른 ArcSight ESM 엔드포인트를 호출하는 데 사용할 수 있는 인증 토큰을 제공합니다. 이 하위 플로우는 다른 모든 하위 플로우에 사용됩니다.
- 쿼리 뷰어 **ID** 유효성 검사: 이 하위 플로우는 ArcSight ESM 프로필 생성 중에 지정된 쿼리 뷰어 ID가 서버에 있는지 확인합니다.
- 상관 관계 규칙 검색: 이 하위 플로우는 쿼리 뷰어 ID를 기반으로 상관관계 규칙을 검색합니다.
- 샘플 이벤트 가져오기: 이 하위 플로우는 서버에서 샘플 상관관계 이벤트를 ArcSight ESM 가져옵니다. 그런 다음 이러한 샘플 이벤트는 프로파일의 매핑 섹션에 있는 보안 인시던트 필드에 매핑됩니다.
- 스테이지 리소스 **ID** 확인: 이 하위 플로우는 콘솔에서 지정된 스테이지 리소스 ID를 ArcSight ESM 확인하고 리소스 이름을 가져옵니다.
- 상관 이벤트 설명 업데이트: 이 하위 플로우는 프로파일의 추가 옵션 페이지에 있는 인시던트 초기 및 종결 섹션에서 상관 이벤트 설명을 업데이트합니다.
- 폴링 일정에 따라 상관 이벤트 검색: 이 하위 플로우는 폴링 간격에 따라 상관 관계가 있는 이벤트를 가져오는 예약된 작업을 실행합니다.

실행 중에 위의 하위 플로우는 아래와 같이 직접 또는 간접적으로 여러 다른 하위 플로우와 작업을 트리거합니다.



Can Invoke Rest from ArcSight Source	can_invoke_rest_from_arcsight_source	Security Operations ArcSight ESM Event I...	Published	true	2020-01-07 00:46:32	admin
Check Closure Update Events REST Step St...	check_closure_update_events_rest_step_st...	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:48:08	admin
Check Initial Update Events REST Step St...	check_rest_step_status	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:48:55	admin
Connection and Credential Validation	connection_and_credential_validation	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:50:26	admin
Correlation Rule Retrieval	correlation_rule_retrieval_5	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:51:40	admin
Finish Profile Event Ingestion	end_process_run	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:53:48	admin
Get Profile Ingestion Information	get_last_run_date	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:54:31	admin
Get Sample Events	get_sample_events	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:55:59	admin
Query Viewer ID Validation	query_viewer_id_validation	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:56:52	admin
Retrieve correlated events based on poll...	retrieve_correlated_events_based_on_poll...	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:58:28	admin
Stage Resource ID Validation	get_stage_resource_name	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 05:00:00	admin
Update Correlated Event	update_correlated_event	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 23:12:18	admin
Update Correlated Event Comments	update_correlated_event_comments	Security Operations ArcSight ESM Event I...	Published	true	2020-02-15 02:08:37	admin
Validate MID Server Status	validate_mid_server_status	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 05:03:40	admin

Amazon Web Services (AWS) 보안 허브 통합

AWS Security Hub 는 AWS 자원에 대한 자동화되고 지속적인 보안 검사 및 베스트 프랙티스 검사를 제공하는 클라우드 보안 태세 관리(CSPM) 서비스입니다.

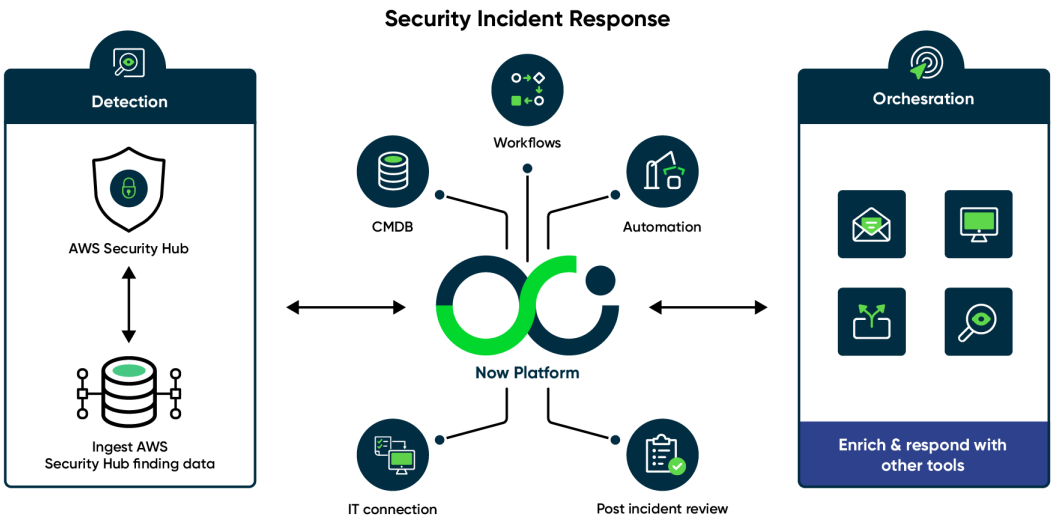
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

AWS Security Hub 통합 개요

AWS Security Hub 을 사용하면 구성의 문제를 식별할 수 있습니다. Security Hub는 검색 결과라고 하는 보안 경고를 집계합니다. AWS Security Hub 는 이러한 결과를 표준화된 형식으로 생성하고 결과를 보다 쉽게 보강, 조사 및 정정할 수 있도록 우선순위를 지정합니다. 통합을 사용하여 AWS Security Hub Security Hub 찾기를 수집하고 에서 보안 인시던트를 자동으로 생성할 수 있습니다 보안 인시던트 응답.

AWS Security Hub 의 SIR 통합은 양방향 아키텍처를 따릅니다. SIR 는 보안 허브 찾기 데이터를 수집하여 보안 인시던트를 생성하는 동시에 해당 보안 인시던트의 모든 업데이트로 결과를 업데이트합니다 보안 허브 .

AWS Security Hub가 애플리케이션과 통합되는 방법을 알아보려면 다음 다이어그램을 ServiceNow AI Platform 보안 운영 참조하세요.



스토어에서 앱 요청

ServiceNow Store 웹 사이트를 방문하면 사용 가능한 모든 앱을 확인하고 스토어에 요청을 제출하는 방법에 대한 정보를 참조할 수 있습니다. 출시된 모든 앱의 누적 릴리스 정보는 ServiceNow Store 버전 기록 릴리스 정보 를 참조하십시오.

주요 기능

이 통합의 주요 기능을 사용하여 다음 작업을 수행합니다.

- 보안 인시던트의 후보인 AWS Security Hub 찾기를 검색하고 이러한 보안 인시던트 생성을 자동화합니다.
- AWS Security Hub 찾기 및 엔터티 필드를 보안 인시던트 필드에 매핑합니다 SIR .
- AWS Security Hub 찾기를 필터링합니다.
- 중복 보안 인시던트를 생성할 필요가 없도록 결과를 기존 미해결 보안 인시던트로 집계합니다.
- 보안 인시던트를 생성하고 종결할 수 있도록 보안 인시던트 응답에 대한 AWS Security Hub 찾기 상태 업데이트를 자동화합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
ServiceNow 또한 보안 인시던트의 생성, 진행 또는 종결에 따라 AWS Security Hub 찾기의 상태를 업데이트합니다. 이 업데이트에는 집계된 결과와 새로운 결과에 대한 의견도 포함되어 있습니다.

- 찾기 수집을 예약하여 보안 인시던트를 주기적으로 생성합니다.
- AWS Security Hub 찾기를 작업 메모와 동기화합니다 SIR .

이 통합에 대해 알아보기

문서 식별자	문서 제목
AWS Security Hub 제품 설명서 웹 사이트	AWS Security Hub 설명서 웹 사이트
ServiceNow 제품 설명서 웹 사이트	ServiceNow 제품 설명서 웹 사이트

통합 시작하기 **AWS Security Hub**

보안 운영 플러그인에 대한 결과 통합을 활성화하고 설정하여 AWS Security Hub 인스턴스 및 보안 인시던트 응답 제품과 인터페이스합니다ServiceNow#.

시작하기 전에
필요한 역할: sn_si.admin

통합을 사용하려면 AWS Security Hub 먼저 다음 ServiceNow Store에서 다운로드해야 합니다.

이 태스크 정보
다음 설정 검사 목록을 검토하고 원활한 통합을 위한 모든 작업을 완료했는지 확인합니다.

검사 목록

필요한 ServiceNow# 플랫폼과 보안 인시던트 응답 역할을 할당하고 확인합니다.	예상 결과를 구성하고 검증하려면 다음 역할이 필요합니다. • 관리자 역할은 에서 ServiceNow Store 통합을 설치하고 sn_si.admin 역할을 할당합니다. • sn_si.admin 역할은 다음 작업을 수행합니다. ○ 통합을 구성합니다. ○ 인시던트 프로파일을 생성합니다. ○ AWS Security Hub 찾기 데이터 필드를 보안 인시던트 필드에 매핑합니다. ○ 진행 중인 인시던트 수집을 예약합니다. ○ 인시던트가 생성되거나 종결되면 인시던트 업데이트를 보안 인시던트 응답 활성화합니다.
필요한 역할을 할당합니다 AWS Security Hub .	애플리케이션을 등록하고 구성하려면 다음 역할이 필요합니다 AWS Security Hub .

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

검사 목록

	• SecurityHubReadOnlyAccess • SecurityHubFullAccess
AWS Security Hub 통합 설정 검토	다음으로 이동 모두 〉 **AWS Security Hub** 찾기 통합 〉 **AWS Security Hub** 찾기 통합 설정. 요구 사항에 따라 속성 설정을 검토하거나 수정합니다.
포털에서 애플리케이션을 AWS 구성합니다.	포털에 애플리케이션을 AWS 등록하고 사용자에게 애플리케이션에 대한 읽기 및 쓰기 권한을 부여합니다. 자세한 내용은 다음 항목을 참조하십시오. • 콘솔을 사용하여 AWS Config 설정 • 보안 허브 통합.

포털 등록 및 구성 **AWS Security Hub**

포털에 애플리케이션을 AWS Security Hub 등록하고 사용자에게 애플리케이션에 대한 읽기 및 쓰기 권한을 부여합니다.

포털에 사용자 프로파일 **AWS** 등록 **ServiceNow®**

시작하기 전에
필요한 역할: AWSSecurityHubFullAccess

프로시저

1. AWS 포털에 로그인합니다.
2. 다음으로 이동 **IAM(ID** 및 액세스 관리) 〉 사용자 〉 새 사용자 생성.
3. 다음 표에서는 사용자 프로필을 만들기 위해 구성해야 하는 필드에 대해 설명합니다.

사용자 프로파일 생성

필드	설명
사용자 상세 정보 지정 〉 사용자 이름	사용자 프로파일의 이름입니다.
권한 설정 〉 그룹에 사용자 추가	미리 정의된 권한 정책이 있는 그룹에 사용자 프로파일을 추가합니다. 기본 설정에 따라 그룹을 생성하고 그룹에 권한 정책을 할당할 수 있습니다. 나중에 그룹에 사용자 프로필을 추가할 수 있으며 그룹에 할당된 권한 정책은 사용자 프로필에 자동으로 할당됩니다.
권한 복사	사용자 프로파일에서 권한을 복사하고 새 사용자 프로파일에 동일한 권한을 할당합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
정책을 직접 연결	AWSSecurityHubFullAccess를 사용자 프로파일에 대한 권한 정책으로 추가합니다. 기본 설정에 따라 사용자 프로파일에 새 권한 정책을 할당합니다.
검토 및 생성	사용자 프로파일에 추가한 모든 상세 정보를 검토합니다.

4. 사용자 만들기를 선택합니다.
5. 표시된 팝업 창에서 사용자 보기를 선택합니다.
6. 사용자 프로파일에 대한 접근 키와 비밀 접근 키를 생성합니다.
   인스턴스에서 통합 ServiceNow# 에 AWS Security Hub 액세스하려면 이러한 키가 필요합니다.
7. 다음으로 이동 **AWS** 서비스 〉 검색 〉 **AWS** 보안 허브 〉 **.**
8. 로 이동 ## ##을 선택합니다.
9. Enable(활성화 AWS Security Hub) 페이지에서 Download(다운로드)를 선택하여 Config(구성)를 활성화합니다 AWS .
   파일을 다운로드하여 계정에서 실행합니다. 이렇게 하면 다양한 AWS 보고 서비스에서 AWS Security Hub모든 정보를 수집하고 .
10. 페이지 아래쪽에서 사용을 *AWS Security Hub*선택합니다.
    대시보드에 모든 상세 정보가 표시되는 데 *AWS Security Hub* 는 약간의 시간이 걸립니다.
11. 전역에서 미국 동부(오하이오)로 지역을 변경합니다.
    미국 동부(오하이오)의 코드는 **us-east-2**입니다. 모든 ServiceNow# 자원이 이 지역 코드에 할당됩니다.

통합 설치 및 구성 **AWS Security Hub**

인스턴스에서 통합을 ServiceNow StoreServiceNow AI Platform 설치하고 구성하여 AWS Security Hub 결과 수집 AWS Security Hub 을 시작합니다.

시작하기 전에
필요한 역할: sn_si.admin

프로시저

1. AWS Security Hub 에서 ServiceNow Store 통합을 다운로드하여 설치합니다.
2. 다음으로 이동 보안 운영 〉 통합 〉 통합 구성.
3. 타일을 AWS Security Hub 검색하고 구성을 클릭합니다.
4. 양식에서 필드를 채웁니다.

AWS Security Hub 구성 양식

필드	설명
이름	AWS Security Hub 인스턴스 구성의 이름입니다.
지역 이름	포털의 AWS Security Hub 사용자 프로파일에서 할당한 지역입니다ServiceNow#.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
비밀 키	포털에서 사용자 프로파일 AWS Security Hub 에 대해 생성한 비밀 키입니다ServiceNow#.
접근 키	포털에서 사용자 프로파일에 대해 생성한 접근 키입니다 ServiceNow#AWS Security Hub .

5. 제출을 클릭합니다.

결과
구성을 성공적으로 확인하고 제출하면 각 보안 허브 찾기 수집 서버 구성이 보안 통합 페이지에 타일로 저장됩니다.

찾기 통합을 위한 **AWS Security Hub** 프로파일 생성

AWS Security Hub 데이터를 AWS Security Hub 수집하고 에서 해당 보안 인시던트보안 인시던트 응답 작업 공간를 생성하는 데 사용할 프로파일을 ServiceNow AI Platform 인스턴스에 생성합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
통합을 통해 플랫폼에서 무단 액세스 시도 및 맬웨어와 같은 다양한 유형의 결과에 대한 보안 인시던트를 AWS Security Hub 생성할 수 있습니다. 이러한 인시던트는 인스턴스에서 구성한 ServiceNow AI Platform 프로파일을 기반으로 생성됩니다. 모든 인시던트는 처음에 프로파일에 구성된 찾기 유형에 대해 생성됩니다. 생성한 결과를 추가로 필터링하여 보안 인시던트를 생성하는 결과를 지정할 수 있습니다.

테넌트의 AWS Security Hub 선택 기준을 충족하고 API를 AWS Security Hub 통해 사용할 수 있는 모든 결과는 처음에 인스턴스에 수집 ServiceNow AI Platform 됩니다.

프로시저

1. 다음으로 이동 모두 〉 **AWS Security Hub** 찾기 통합 〉 **AWS Security Hub** 찾기 프로파일.

2. 새로 만들기를 클릭합니다.

3. 양식에서 필드를 채웁니다.

AWS Security Hub - 결과 수집 구성 양식

필드	설명
이름	프로파일의 이름입니다. 이 이름은 프로파일 유형을 식별하는 데 도움이 되며 이 프로파일과 연결된 보안 태그의 기본 이름이기도 합니다.
활성	프로파일을 활성화하려면 선택합니다. 프로파일이 활성 상태이면 필터링 조건이 일치할 때 찾기 데이터를 적극적으로 수집하고 AWS Security Hub 해당 보안 인시던트가 생성 SIR 됨을 ServiceNow AI Platform 의미합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
소스	찾기를 AWS Security Hub 수집하도록 구성한 통합 테넌트입니다. 여러 테넌트가 구성된 경우 프로파일에 대해 수집하려는 찾기 유형에 적합한 테넌트를 선택합니다.
순서	둘 이상의 프로파일이 트리거 조건을 공유할 때 플로우가 실행되는 순서를 나타내는 이 필드에 값을 입력합니다. 숫자가 가장 낮은 플로우의 우선순위가 가장 높습니다. 작업 순서를 설정하려면 값을 입력합니다. 예를 들어 100, 200, 300, 400입니다. 기본값은 100입니다.
설명	이 프로파일을 다른 프로파일과 구별하는 데 도움이 되는 추가 텍스트입니다.

AWS Security Hub 찾기 필드 매핑

매핑된 데이터로 인시던트를 생성할 수 있도록 개별 AWS Security Hub 찾기 필드를 보안 인시던트의 SIR 필드에 매핑합니다.

시작하기 전에
필요한 역할: sn_si.admin

프로시저

1. 매핑 페이지의 AWS Security Hub 매핑 섹션에서 샘플 수집 방법 중 하나를 선택합니다.

샘플 수집 방법

필드	설명
모든 기본 찾기 필드	이 수집 방법을 사용하여 모든 찾기 필드의 정적 목록을 봅니다. 이 메서드에는 값 없이 기본 필드 이름만 포함됩니다. 이 정보를 사용하여 필드와 매핑할 수 있습니다 SIR .
최근 AWS Security Hub 결과 검색	이 수집 방법을 사용하여 가장 최근의 결과 데이터를 임포트합니다. 기본적으로 5개의 샘플 찾기와 최대 20개의 샘플 찾기를 수집할 수 있습니다. 샘플 찾기 필드 값은 프로파일이 샘플 찾기를 수집할 때 채워집니다. 이러한 결과를 **SIR** 인시던트 대상 필드에 매핑할 수 있습니다. 찾기 필드와 값은 개별 탭으로 나타납니다.
샘플 데이터 임포트	샘플 데이터 임포트를 선택하여 샘플 찾기를 AWS Security Hub임포트합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	이 버튼은 최근 AWS Security Hub 찾기 수집 방법 검색을 선택할 때 나타납니다. 서버에서 샘플 찾기 AWS Security Hub 를 검색하는 데 몇 분 정도 걸립니다. 이러한 결과를 **SIR** 인시던트 대상 필드에 매핑합니다. 찾기 필드와 값은 개별 탭으로 나타납니다.

2. 보안 인시던트에 표시되는 기본 필드에 필드를 추가하려면 다음 작업을 수행합니다.

SIR 인시던트 대상 필드 섹션에서 ⊕ Map another field 버튼을 클릭합니다. 새 필드를 표시하도록 선택할 수 있는 필드 목록이 SIR 표시됩니다.

a. 보안 인시던트 열에서 표시되는 목록을 확장한 다음 필드를 선택합니다.

ⓘ 주:
동일한 보안 인시던트에 여러 옵저버블을 표시할 수 있습니다. 예를 들어 옵저버블 필드는 서로 다른 값으로 여러 번 매핑될 수 있습니다. 마찬가지로 구성 항목 및 작업 메모 필드는 여러 값을 지원합니다. 여러 값을 지원할 수 없는 필드에 두 값을 매핑하려고 하면 이 필드가 여러 값을 지원하지 않는다는 오류 메시지가 표시됩니다. 마찬가지로 보안 인시던트의 필드에 여러 옵션을 선택할 수 있는 목록이 있고 목록에 표시되지 않은 필드에 옵션을 매핑하려고 하면 필드가 보안 인시던트에 채워지지 않습니다.

b. AWS Security Hub 소스 필드 섹션에서 필드를 끌어 새 필드에 매핑합니다.

c. 필드에 해당하는 확인란을 선택하면 새 변경 사항이나 업데이트된 변경 AWS Security Hub 사항이 해당 SIR에서 새 인시던트 데이터로 자동 업데이트됩니다.

ⓘ 주:
기본 시스템에서 SIR에 연결된 새 경보와 관련된 업데이트를 받으려면 AWS Security Hub 시스템 속성 sn_sec_security.finding_updates가 기본적으로 True로 설정됩니다.

- 기본적으로 영향을 받는 사용자, 구성 항목 및 옵저버블 필드가 선택되어 있습니다. 즉, 새로운 옵저버블이나 관련 구성 항목이 있거나 영향을 받는 사용자가 인시던트에 추가될 때마다 해당 폴링 간격 동안 해당 정보가 자동으로 추출되어 보안 인시던트 응답(SIR)의 관련 목록에 채워집니다.
- 다른 필드의 경우 의 찾기 AWS Security Hub에서 수행된 새 변경 내용이나 업데이트된 변경 내용에 해당하는 확인란을 선택해야 합니다. 이렇게 하면 해당 SIR 인시던트 데이터가 새 인시던트 데이터로 자동 업데이트됩니다.

ⓘ 중요사항:
기존 데이터를 재정의하면 분석가가 작업할 데이터가 불안정해질 수 있으며 보안 인시던트의 필드 값으로 설정된 다른 자동화도 영향을 받을 수 있으므로 이 기능을 선택하기 전에 실사를 수행해야 합니다. 따라서 재정의 기능을 선택하기 전에 실사를 수행하는 것이 중요합니다.

3. 필드를 제거하려면 SIR 인시던트 대상 필드 섹션의 입력 식 필드 옆에 있는 ⊖, (항목 제거) 단추를 사용합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 소스 필드 섹션의 AWS Security Hub 필드 값을 SIR 인시던트 대상 필드 섹션의 필드에 매핑하려면 다음 작업 중 하나를 사용합니다.

   a. 필드 이름(예: id)을 끌어서 SIR 인시던트 대상 필드 열의 필드 이름 옆에 놓습니다.

      소스 필드 섹션의 AWS Security Hub 값을 SIR 인시던트 대상 필드 섹션의 필드와 일치시킬 수 있습니다. 필드는 색상으로 구분되므로 매핑 프로세스에서 찾기 필드를 간과하거나 중복하지 않습니다. 연한 파란색 필드는 찾기 필드가 아직 선택되지 않았으며 보안 인시던트에 매핑되지 않았음을 나타냅니다. 수신 찾기 필드를 보안 인시던트의 둘 이상의 필드와 연결하는 것을 선호할 수 있습니다. 회색 필드는 찾기 필드가 선택되었고 보안 인시던트의 필드에 매핑되었음을 나타냅니다. 이러한 방식으로 보안 인시던트에 추가된 필드 값과 나머지 중요한 찾기 정보가 매핑되지 않은 상태로 남아 있는지 시각화할 수 있습니다. 그러나 소스 필드 섹션에는 AWS Security Hub SIR 인시던트 대상 필드 섹션의 필드와 호환되지 않는 필드가 있습니다. 이러한 값을 매핑하면 SIR이 생성될 때 표시되지 않습니다.

   b. 텍스트와 필드의 조합을 추가할 수 있습니다.
   예를 들어 Finding name# ${name}$###. 여기서는 소스 필드 섹션에서 ${name}$이 매핑 AWS Security Hub 되는 동안 ## ### 수동으로 입력할 수 있습니다.

   c. 소스 찾기 필드를 수동으로 입력하고 대상 필드에 매핑할 수 있습니다.
   ${field name}$ 형식을 사용하여 소스 찾기 필드를 수동으로 매핑합니다. 예를 들어, 찾기 필드 심각도를 매핑하려면 ### ${properties(severity)}$입니다.

   이 통합은 특정 옵저버블 하위 유형을 분류합니다. 찾기 필드를 SIR 옵저버블 필드와 매핑 AWS Security Hub 하면 옵저버블이 자동 분류됩니다 ServiceNow AI Platform . 수신 AWS Security Hub 옵저버블을 의 옵저버블 유형에 SIR일반적으로 매핑하려면 옵저버블 필드에 필드를 끌어서 놓습니다 AWS Security Hub . 그러나 에서 SIR들어오는 AWS Security Hub 옵저버블에 대한 옵저버블 유형을 알고 있는 경우 옵저버블 유형 필드에 구체적으로 매핑합니다SIR. 에서 SIR 특정 옵저버블 유형의 예로는 Observable(도메인 이름), Observable(이메일 주소), Observable(IP 주소(V4)) 및 Observable(호스트 이름)이 있습니다.

   경우에 따라 에서 AWS Security Hub 필드 값을 찾는 것이 SIR 보안 인시던트의 필드로 직접 변환되지 않을 수 있습니다. 이러한 값의 경우 스크립트 편집기를 사용하여 매핑 단계 중에 보안 인시던트의 필드 값에 대한 형식을 지정할 수 있습니다. 비슷하지만 동일하지는 않은 값의 형식을 지정하려면 스크립트 편집기를 사용하십시오.

5. 찾은 결과의 AWS Security Hub 새 필드에 대한 필드 번역의 형식을 보안 인시던트의 필드 값과 일치하도록 지정하려면 **SIR** 인시던트 대상 필드 헤더에서 여기를 클릭 링크를 클릭하십시오.

6. 필드 번역을 지원하는 필드를 수정하려면 스크립트 형식 필드 번역 아이콘을 클릭하십시오.

   필드 번역을 지원하는 필드는 범주, 구성 항목 및 우선순위입니다. 예를 들어 범주 옆에 있는 아이콘을 클릭합니다. 결과 필드 번역 스크립트 편집기가 AWS Security Hub 열립니다.

7. 스크립트에 대한 변경 내용을 입력하고 업데이트를 클릭하여 변경 내용을 저장하고 매핑 페이지로 돌아갑니다.
   예를 들어 범주의 경우 스크립트 편집기에서 다음을 정의합니다.

   ```
   "<Incoming Security Hub finding Field Value>" : "<Category to assign to the Security Incident>".
   ```

   이 매핑을 통해 프로파일은 구성된 범주만 사용합니다.

8. 필드 값을 추가하거나 제거하여 매핑을 계속합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

인시던트 생성 조건 작성기에서 동일한 필드 값을 사용하여 들어오는 찾기가 보안 인시던트를 생성하기 위해 충족해야 하는 추가 기준을 정의할 수 있습니다.

9. 필터링 및 집계 섹션으로 이동하려면 계속을 클릭합니다.

다음에 수행할 작업

보안 인시던트를 생성하는 결과를 지정할 수 있도록 필터 조건을 정의하고 설정합니다. 인시던트 생성 조건 빌더(필터링 및 집계 섹션)에서 동일한 필드 값(매핑 섹션에 정의됨)을 사용하여 수신 찾기가 보안 인시던트를 생성하기 위해 충족해야 하는 추가 기준을 정의할 수 있습니다.

찾기 수집을 위한 **AWS Security Hub** 필터 및 집계 기준 정의

필터 조건을 정의하고 설정하여 보안 인시던트를 생성해야 하는 수신 찾기를 지정할 수 있습니다. 또한 동일한 찾기에 대해 다른 보안 인시던트를 생성하는 대신 수신 찾기를 미해결 보안 인시던트에 추가할 수 있는 추가 인시던트 필드 기준을 정의할 수도 있습니다.

찾은 결과에 대한 **AWS Security Hub** 필터링 조건을 설정하여 보안 인시던트 생성

필터링 조건이 일치하는 경우에만 보안 인시던트가 생성되도록 필터링 조건을 설정합니다.

시작하기 전에

필요한 역할: sn_si.admin

이 태스크 정보

이러한 유형의 필터링은 보안 인시던트를 격리하고 생성하는 보안 인시던트 수를 제한하는 데 도움이 됩니다. 추가 필터링 기준을 설정하면 쿼리 또는 트리거된 인시던트 구성을 변경할 필요 없이 필요한 결과만 수집됩니다.

다음 단계를 수행하여 보안 인시던트가 생성되도록 수신 AWS Security Hub 찾기가 충족해야 하는 기준을 정의합니다.

프로시저

1. Pre-Filtering(사전 필터링) 섹션에서 **Apply Pre-**Filter(사전 필터 적용)를 선택합니다.

이 옵션을 사용하여 특정 찾기를 필터링하고 찾기 수집 로드를 줄일 수 있습니다.

API 필터 필드에 요구 사항에 따라 조건을 기반으로 특정 결과를 필터링하는 JSON 조건을 입력합니다. 예를 들어 다음 값을 입력하여 Workflow Status(워크플로우 상태)가 Security Hub에서 해결됨인 결과를 필터링합니다.

```
{"Filters"{
  "WorkflowStatus":[{
  "Comparison":"NOT_EQUALS",
  "Value": "RESOLVED"}]
 }
}
```

제공된 조건에 AWS Security Hub 따라 찾기가 수집되어 찾기 원시 테이블에 AWS Security Hub 표시됩니다.

다음으로 이동 모두 〉 **AWS Security Hub** 찾기 통합 〉 **AWS Security Hub** 찾기 원시 을 클릭하여 원시 결과 데이터를 봅니다.

2. 필터 조건에 대한 찾기 필드 선택 섹션에서 사용 가능한 찾기 필드 표시를 선택하여 찾은 결과에서 AWS Security Hub 사용 가능한 모든 필드 목록을 표시합니다.
모든 찾기 필드 목록에서 보안 인시던트 생성 조건 섹션에 표시할 찾기 필드를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
AWS Security Hub 검색 결과에는 여러 필드와 값이 포함되어 있습니다. 모든 찾기 필드 목록에서 요구 사항에 따라 찾기 필드를 검색하고 선택할 수 있습니다.

3. 보안 인시던트 생성 조건 섹션에서 조건을 기준으로 필터링 을 선택하여 들어오는 AWS Security Hub 검색 결과가 보안 인시던트를 생성하기 위해 충족해야 하는 기준을 정의합니다.

   필터 조건의 첫 번째 필드에는 찾기에서 AWS Security Hub 사용할 수 있는 200개의 필드로 구성된 기본 목록과 필터 조건에 대한 찾기 필드 선택 섹션에서 선택한 찾기 필드가 포함되어 있습니다.

   필터 조건의 두 번째 필드에는 조건 연산자가 포함되어 있습니다. 선택한 옵션에 따라 찾기를 수집하기 위해 충족해야 하는 조건이 결정됩니다.

   필터 조건의 세 번째 필드에는 사용 가능한 찾기 필드에서 지원하는 값이 포함됩니다. 입력한 찾기 필드가 결과 값과 일치하는지 확인합니다.

   예를 들어, 여러 값이 있는 다음 필드에 *## ## ##* 필터를 사용합니다.

   - Workflow(Status)
   - WorkflowState

4. 조건 작성기의 목록과 필드를 사용하여 첫 번째 행의 필터를 설정합니다.
5. 조건을 더 추가하려면 **AND** 또는 **OR**을 클릭합니다.
   - **AND**를 선택하면 모든 조건이 일치해야 합니다.
   - **OR**을 선택하면 두 조건을 일치시킬 수 있습니다.
6. 두 번째 필터 조건을 설정하려면 새 기준을 클릭합니다.

결과
필터링 조건에 AWS Security Hub 따라 찾기가 로 임포트 SIR됩니다. 다음으로 이동 모두 〉 **AWS Security Hub** 찾기 통합 〉 **AWS Security Hub** 찾기 임포트 임포트한 결과를 보려면 다음을 수행합니다.

결과를 보안 인시던트로 집계 **AWS Security Hub** 하는 조건 정의

중복될 가능성이 있는 유사한 인시던트를 생성하는 대신 수신 AWS Security Hub 발견 사항을 기존 SIR 보안 인시던트로 집계하는 추가 인시던트 집계 기준을 정의합니다. 각 프로파일에 대해 필드 일치 값 기준을 사용하는 경우 이 추가 집계는 모든 관련 인시던트 데이터를 단일 보안 인시던트에 배치하여 활성 상태의 중복 보안 인시던트 수를 줄일 수 있습니다.

시작하기 전에
필요한 역할: sn_si.admin

이 태스크 정보
새 인시던트가 매핑 단계의 집계 필드 조건에서 선택한 모든 값과 일치하는 경우, 인시던트는 동일한 필드 값을 사용하여 가장 최근에 열린 보안 인시던트에 자동으로 추가됩니다. 보안 인시던트를 담당하는 sn_si.analyst 역할을 가진 사용자는 보안 인시던트의 관련 목록에서 추가된 모든 집계 인시던트를 볼 수 있습니다.
보안 인시던트에 대한 모든 집계 AWS Security Hub 된 결과가 관련 목록에 표시됩니다 AWS Security Hub . 이 목록은 관련 타임스탬프 및 집계된 필드 값에 대해 자세히 설명합니다. 이 정보는 기존 보안 인시던트에 결과가 추가되는 이유를 AWS Security Hub 이해하는 데 도움이 됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 새 인시던트를 생성하는 대신 수신 AWS Security Hub 찾기를 미해결 보안 인시던트에 추가할 수 있는 추가 인시던트 필드 기준을 정의하려면 집계 조건 옵션을 선택합니다.
2. 일치하는 값이 있는 인시던트 필드 필드에 인스턴스의 기존 보안 인시던트 ServiceNow AI Platform와 일치시키려는 필드 값을 입력합니다.
   집계 기준이 충족되고 이 수신 인시던트를 기존 보안 인시던트에 추가할 수 있도록 다중 선택 입력 필드에서 선택한 모든 필드 값이 일치해야 합니다. 이 선택은 여러 필드 값을 가질 수 있는 옵저버블 및 구성 항목과 같은 필드가 매핑되는 *AND* 조건을 의미합니다. 값의 하위 집합만 일치 AWS Security Hub 하면 결과 집계 조건이 충족되지 않고 새 보안 인시던트가 생성됩니다.
3. 여러 필드 일치 조건을 추가하려면 새 기준 추가를 클릭합니다.
   사용자가 정의하는 다중 선택 필드 조건 중 하나가 충족되면 집계가 발생합니다. 이 선택은 *OR* 조건을 의미합니다.
4. 새 찾기가 보안 인시던트에 추가될 때 새 찾기에 대한 작업 메모를 업데이트하려면 새 찾기에 대한 작업 메모 로깅을 선택합니다.

   작업 메모는 새 찾기가 추가되었음을 기록하고 결과 상세 정보에 대한 링크를 포함합니다. 로그 작업 메모는 매핑 섹션의 작업 메모 필드에 추가하는 상세 정보도 업데이트합니다.

5. 일정을 구성하려면 계속을 클릭합니다.

결과
집계 조건에 AWS Security Hub 따라 결과를 집계하여 인시던트를 생성합니다 SIR . 다음으로 이동 모두 〉 **AWS Security Hub** 찾기 통합 〉 **AWS Security Hub** 찾기에서 작업 생성된 보안 인시던트 목록을 볼 수 있습니다.

다음에 수행할 작업
찾기 데이터를 검색하고 프로파일의 기준과 일치하는 인시던트를 찾도록 일정을 설정합니다.

AWS Security Hub 찾기 검색 예약

찾기 데이터를 검색하고 프로파일의 기준과 일치하는 결과를 수집 AWS Security Hub 하도록 일정을 설정합니다.

시작하기 전에
필요한 역할: sn_sni.admin

이 태스크 정보
찾기 프로파일 구성과 일치하는 향후 AWS Security Hub 찾기를 폴링할 빈도를 계획할 AWS Security Hub 수 있습니다.

폴링 간격은 각 프로파일에 대해 개별적으로 구성됩니다. 다른 폴링 간격은 찾기 통합의 AWS Security Hub 성능에 영향을 줄 수 있습니다. 일정을 예약할 때 인시던트의 긴급도에 따라 시스템 부하의 균형을 맞추도록 계획합니다. 모든 프로필에 대해 1분 기본값이 설정됩니다. 인시던트의 긴급도와 시스템의 예상 로드에 따라 이 설정을 수정할 수 있습니다.

특정 폴링 간격으로 인시던트에 추가되는 모든 경보는 처리된 후 경보 관련 목록 및 설명에 AWS Security Hub 추가됩니다.

프로시저

1. 예약 양식의 필드에 내용을 입력합니다.

   테넌트에서 결과를 끌어오는 방법과 시기를 정의하도록 AWS Security Hub 일정을 구성합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

일정 양식

필드	설명
진행 중인 찾기 수집	새 인시던트에 ServiceNow AI Platform 대해 인스턴스가 테넌트에서 끌어오는 지속적 찾기 수집입니다 AWS Security Hub . 트리거된 결과가 발견되고 보안 인시던트 생성 필터링 기준이 일치하면 보안 인시던트가 생성됩니다.
폴링 종결된 찾기	해결된 여론 조사 결과입니다. 이러한 결과는 진행 중인 인시던트 수집 중에 수집됩니다.
폴링 증분(분)	분 단위로 정의된 폴링 빈도입니다.
초기 찾기 수집 시간 설정	구성된 날짜 및 시간을 기준으로 하는 찾기 수집입니다. 이 옵션을 사용하여 초기 수집에 대한 특정 날짜 및 시간을 정의할 수 있습니다. 후속 수집은 폴링 간격 기간을 기반으로 합니다.
초기 찾기 수집 시간 입력	인시던트 수집을 위해 지정하는 날짜 및 시간입니다.
일회성 검색	기록 AWS Security Hub 결과를 한 번 검색한 다음 데이터를 조정하려면 이 확인란을 선택합니다. 이 확인란을 선택하면 애플리케이션이 약 최대 90일 동안의 모든 오픈 결과와 종결 AWS Security Hub 된 결과를 끌어옵니다. 데이터를 처리할 때 진행 중인 결과와 기록 데이터를 모두 끌어오지만 진행 중인 결과의 처리가 기록 끌어오기보다 우선합니다. 그렇지 않으면 기간과 수집된 결과 수에 따라 기록 끌어오기에 다소 시간이 걸릴 수 있습니다. **주:** 검색된 이력 AWS Security Hub 결과는 애플리케이션 내의 보안 인시던트 응답 중복을 방지하기 위해 중복 제거 검사를 거칩니다.
날짜 이후	기록 결과가 수집된 AWS Security Hub이후 날짜입니다. **주:** 결과 데이터는 대략 지난 90일 동안 가져온 것입니다.

예약 페이지를 사용하면 테넌트에서 찾기를 끌어오는 방법과 시기를 정의할 수 있습니다 AWS Security Hub .

2. 추가 옵션 페이지로 이동하려면 계속을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

인시던트 상태별로 **SIR** 찾기, **AWS Security Hub** 업데이트 및 종결을 자동화

인시던트 상태에 따라 찾기 AWS Security Hub 의 업데이트 및 종결을 자동화합니다 SIR . 통합 AWS Security Hub 에는 찾기 수집을 사용하여 보안 인시던트를 생성하고 인시던트의 SIR 변경 내용에 따라 결과의 상태를 업데이트할 수 있는 양방향 인터페이스가 있습니다.

시작하기 전에
필요한 역할: sn_si.admin

프로시저

1. 양식에 상세 정보를 입력합니다.
에서 SIR보안 인시던트를 생성하거나 종결할 때 지침에 따라 결과를 업데이트 AWS Security Hub 하기 위한 구성을 완료합니다.

인시던트 업데이트 자동화 양식

범주	필드	설명
상태 업데이트	SIR 인시던트 상태	인시던트 상태 목록을 SIR 표시합니다. 이 목록에서 옵션을 선택하여 찾기 상태에 매핑합니다 보안 허브 .
	보안 허브 상태 찾기	워크플로우 상태 목록을 보안 허브 표시합니다. 찾은 결과의 워크플로우 상태는 해당 SIR 상태 인시던트 상태가 변경될 때 AWS Security Hub 업데이트됩니다.
우선순위 업데이트	SIR 인시던트 우선순위	인시던트 우선순위 수준 목록을 SIR 표시합니다. 이 목록에서 옵션을 선택하여 찾기 우선순위 수준에 매핑합니다 보안 허브 .
	보안 허브 우선순위 찾기	심각도 수준 목록에서 보안 허브 옵션을 선택합니다. 발견 사항의 심각도는 해당 보안 인시던트 우선순위가 변경되면 업데이트됩니다 AWS Security Hub .
작업 메모 업데이트	해당SIR 인시던트에 대한 작업 메모가 업데이트될 때 메모 섹션을보안 허브 업데이트하려면 이 옵션을 선택합니다. 의 SIR 작업 메모 섹션은 512자로 제한되며 결과의 보안 허브 메모 섹션도 동일하게 지원됩니다.	
추가 설명 업데이트	인시던트에 SIR 제공한 추가 코멘트로 AWS Security Hub 찾기 코멘트 섹션을 업데이트하려면 선택합니다.	
해결 참고 사항 업데이트	인시던트가 해결될 때 SIR 제공한 해결 메모로 종결 설명 섹션을 업데이트 AWS Security Hub 하려면 선택합니다.	

주:
작업 메모의 각 업데이트는 결과의 보안 허브 메모 섹션에 있는 마지막 업데이트를 재정의합니다. 인시던트에 SIR 관련 작업 메모를 추가하는 것이 좋습니다.

2. 마침을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 수행할 작업
프로파일이 대기 중 상태로 전환됩니다. 설정 및 구성이 완료되었다는 확인 메시지가 표시되면 프로파일을 활성화할 수 있습니다.

SIR 찾기 수집 후 **AWS Security Hub** 양식

ServiceNow AI Platform 찾은 정보를 수집 AWS Security Hub 하면 보안 인시던트가 생성되고 해당 보안 인시던트 기록이 업데이트됩니다.

작업 메모

작업 메모는 인시던트가 집계될 때 및 에서 찾기 수집을 위한 AWS Security Hub 필터 및 집계 기준 정의새 찾기에 대한 작업 메모 기록 옵션을 구성한 경우 게시됩니다.

원시 인시던트 데이터가 포함된 내부 찾기 임포트 기록을 볼 수도 있습니다.

여기를 클릭 링크를 클릭하면 환경에서 기록을 AWS Security Hub 볼 수 있습니다. 다음 예는 환경의 기록을 AWS Security Hub 보여줍니다.

집계된 **AWS Security Hub** 결과

집계된 AWS Security Hub 결과 보기: 보안 인시던트에 대해 집계된 인시던트를 봅니다. 다음으로 이동 모든 관련 목록 표시 〉 집계된 **AWS Security Hub** 찾기.

보안 인시던트 생성: 목록에서 인시던트를 선택하고 작업 메뉴를 클릭한 다음 보안 인시던트 만들기를 클릭합니다. 이 옵션은 인시던트에 대한 새 보안 인시던트를 생성하고 이 인시던트는 상위 보안 인시던트에서 집계 해제됩니다.

Carbon Black - 인시던트 보강 통합

Carbon Black 통합을 통해 보안 인시던트와 연관된 엔드포인트를 쿼리하고 상호작용하는 API를 통해 보안 인시던트를 조사하고 그에 대응합니다.

Carbon Black - 인시던트 보강 통합 자원 찾기

- Carbon Black - 인시던트 보강 통합 시작하기
- 보안 운영 Carbon Black 통합 - 실행 중인 프로세스 플로우 가져오기
- Security Operations Carbon Black 통합 - 호스트 분리 플로우
- 보안 운영 Carbon Black 통합 - 호스트 격리 플로우 제거

통합 개념 이해

- 제공되는 통합의 ServiceNow 유형
- 보안 운영 워크플로우 트리거

ServiceNow 자원에서 도움받기

- 보안 운영 커뮤니티에서 질문 또는 답변하기
- 알려진 오류 포털에서 알려진 오류 문서 검색
- 연락처 고객 서비스 및 지원
- 마드리드로 업그레이드

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

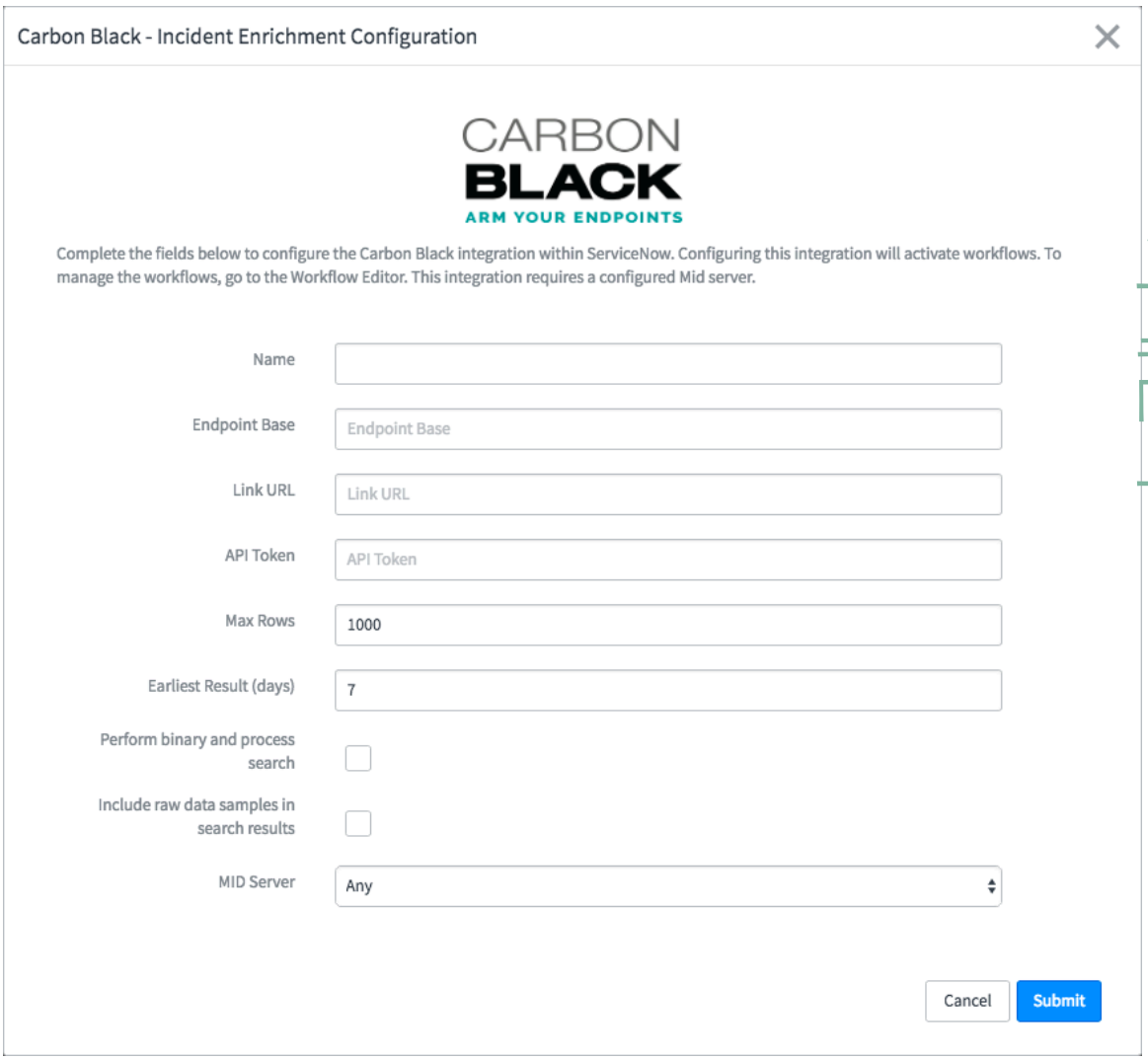
Carbon Black - 인시던트 보강 통합 시작하기

Carbon Black 인시던트 보강을 사용하면 로그에서 잠재적으로 악의적인 표시기를 쿼리하여 보안 인시던트를 쉽게 조사할 수 있습니다. Carbon Black - 인시던트 보강 통합을 사용하려면 먼저 에서 ServiceNow Store 다운로드하여 적절한 엔드포인트 기본 URL 및 MID 서버를 추가해야 합니다.

시작하기 전에
필요한 역할: sn_si_admin

프로시저

1. 에서 통합을 다운로드합니다. ServiceNow Store.
2. 다운로드가 완료되면 웹 사이트에 액세스하고 Carbon Black 프로파일에서 엔드포인트 기본 URL과 API 토큰을 가져옵니다.
3. 인스턴스에서 다음으로 이동합니다. 보안 운영 〉 통합 〉 통합 구성.
4. Carbon Black - 인시던트 보강 카드에서 구성을 클릭합니다.



5. 필요에 따라, 필드를 채웁니다.

필드	설명
이름	이 구성의 이름입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
엔드포인트 기본	Carbon Black 사이트에서 가져온 엔드포인트 URL입니다.
링크 URL	사용 가능한 경우 Carbon Black 인스턴스로 연결되는 링크 URL입니다.
API 토큰	Carbon Black 사이트에서 획득한 API 토큰입니다.
최대 행 수	검색할 행의 최대 수입니다. 기본값은 1,000행입니다.
가장 빠른 결과(일)	일수 단위로 보려는 가장 빠른 결과입니다.
이진 및 프로세스 검색 수행	파일 해시와 같은 이진 파일을 찾기 위해 이진 검색을 수행하고 실행되었을 수 있는 .exe 프로세스를 검색하려면 이 옵션을 선택합니다.
검색 결과에 원시 데이터 샘플 포함	사이팅 검색 결과에 원시 데이터 샘플을 포함하려면 이 옵션을 선택합니다. 반환되는 데이터의 양은 보안 인시던트 응답 속성의원시 데이터 속성 행 수의 설정에 따라 달라집니다.
MID 서버	활성 MID 서버를 사용하려면 임의 를 선택하고, 특정 MID 서버 이름을 선택합니다.

주:
이 통합을 구성하면 워크플로우가 활성화됩니다. 워크플로우를 관리하려면 워크플로우 편집기로 이동합니다.

6. 제출을 클릭합니다.
   통합 구성 카드가 표시됩니다.
7. 통합 구성 카드의 원래 목록으로 돌아가려면 구성 표시 드롭다운 목록에서 아니요를 선택합니다.

Carbon Black 통합

Carbon Black 통합을 사용하면 API를 사용하여 보안 인시던트와 연관된 엔드포인트를 쿼리하고 상호작용함으로써 보안 인시던트를 조사하고 그에 대응할 수 있습니다.

탐색

- 보안 인시던트 응답 통합
- Carbon Black - 인시던트 보강 통합

설정

Carbon Black 통합 시작하기

사용

- 보안 운영 워크플로우 트리거
- 보안 인시던트의 영향을 받는 항목 보기
- 보안 운영 - 실행 중인 프로세스 가져오기 플로우
- 보안 운영 Carbon Black 통합 - 실행 중인 프로세스 플로우 가져오기
- 보안 인시던트의 영향을 받는 항목 보기

개발

- ServiceNow 보안 운영 통합 개발 가이드라인
- 통합 작성을 위한 팁
- 개발자 교육
- 개발자 설명서
- 애플리케이션과 함께 설치되는 구성요소 찾기

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 차단 요청 실행
- Security Operations Integration - 요청 플로우 차단
- 호스트 격리 실행
- Security Operations Carbon Black 통합 - 호스트 분리 플로우
- 보안 운영 Carbon Black 통합 - 호스트 격리 플로우 제거

문제 해결 및 도움받기

- 통합 문제 해결
- 보안 운영 커뮤니티에서 질문 또는 답변하기
- 알려진 오류 포털에서 알려진 오류 문서 검색

- 연락처 고객 서비스 및 지원

Carbon Black 통합 시작하기

카본 블랙은 쉽게 통합되는 보안 운영고급 보안 시스템입니다. Carbon Black 통합을 사용하려면 먼저 에서 ServiceNow Store 통합을 다운로드하고 적절한 엔드포인트 기본 및 API 토큰을 추가해야 합니다.

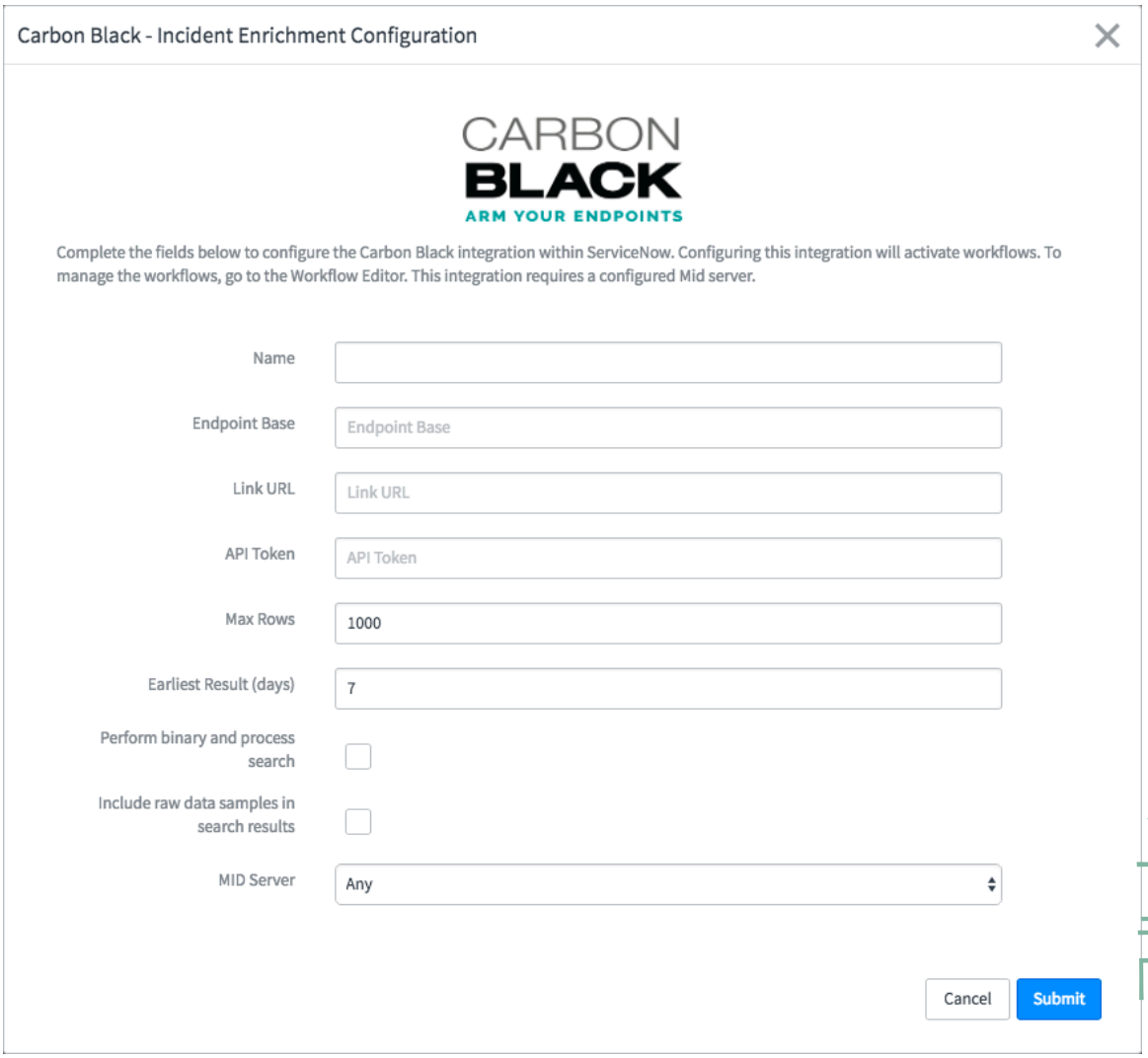
시작하기 전에

필요한 역할: sn_si_admin

프로시저

1. 에서 통합을 다운로드합니다. ServiceNow Store.
2. 설치가 완료되면 웹 사이트에 액세스하고 Carbon Black 프로파일에서 엔드포인트 기본 URL 및 API 토큰을 가져옵니다.
3. 인스턴스에서 다음으로 이동합니다. 보안 운영 〉 통합 〉 통합 구성.
   사용 가능한 보안 통합은 일련의 카드로 표시됩니다.
4. 카드에서 Carbon Black새로 만들기를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



5. 필요에 따라, 필드를 채웁니다.

필드	설명
이름	이 구성의 이름입니다.
엔드포인트 기본	Carbon Black 사이트에서 가져온 끝점 기반입니다.
API 토큰	Carbon Black 사이트에서 획득한 API 토큰입니다.
MID 서버 사용	아직 선택되어 있지 않으면 이 확인란을 선택합니다.
MID 서버	활성 MID 서버를 사용하려면 임의 를 선택하고, 특정 MID 서버 이름을 선택합니다.
호스트 격리 사용	선택한 구성 항목을 보안 인시던트의 구성 항목 관련 목록 탭에서 격리할 수 있도록 하려면 이 확인란을 선택합니다.

주:
이 통합을 구성하면 워크플로우가 활성화됩니다. 워크플로우를 관리하려면 워크플로우 편집기로 이동합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

6. 제출을 클릭합니다.
   통합 구성 카드가 표시됩니다.
7. 통합 구성 카드의 원래 목록으로 돌아가려면 구성 표시 드롭다운 목록에서 아니요를 선택합니다.

Check Point Anti-bot - Email Parser 통합

Check Point 안티 봇 - 이메일 파서 통합은 Check Point 안티 봇의 이메일 알림을 사용하여 보안 인시던트를 생성하고 보강 및 응답 워크플로우를 구동하는 이메일 파서를 사용하여 지원됩니다.

Check Point 안티봇 **-** 이메일 파서 통합 구성

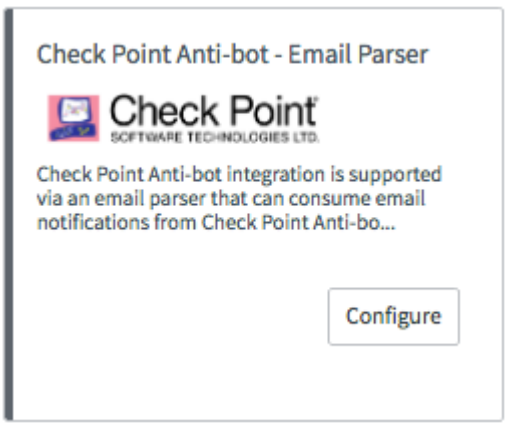
Check Point 안티봇 - 이메일 파서 통합은 이메일 알림을 사용하여 보강 및 응답 워크플로우를 구동합니다.

시작하기 전에
필요한 역할: sn_si_admin

이 태스크 정보
통합에 사용할 Check Point 안티 봇 이메일 파서 템플릿이 제공됩니다. 통합이 발생하기 전에 구성하고 활성화해야 합니다. 파서를 업데이트하면 활성화됩니다.

프로시저

1. 다음으로 이동 모두 〉 보안 운영 〉 통합 〉 통합 구성.
   사용 가능한 보안 통합은 일련의 카드로 표시됩니다.



2. Check Point 안티 봇 - 이메일 파서 카드에서 구성을 클릭합니다.
3. **Check Point** 안티봇 **-** 이메일 파서 구성 대화 상자에서 이메일 파서 구성 링크를 클릭합니다.
4. **Check Point** 안티 봇 링크를 클릭하여 제공된 템플릿 이메일 파서의 설정을 편집합니다.
   최소한 '### ###' 필드를 채우십시오. 이메일 파서를 생성하려면 다음 문서를 참조하십시오 보안 운영에서 이메일 파서 생성.
5. 활성 상자를 선택합니다.
6. 이메일 파서 양식에서 업데이트를 클릭합니다.
   이메일 파서가 활성 상태입니다. 통합 구성으로 돌아갈 필요가 없습니다.

Check Point Next Generation Threat Prevention 통합

이 문서에서는 애플리케이션이 제대로 작동하도록 NGTP(Check Point Next Generation Threat Prevention) 기능을 SIR(SIR)과 ServiceNow# 보안 인시던트 응답 통합하는 데 필요한 단계에 대해 설명합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설치 및 구성이 완료되면 보안 인시던트 분석가는 이 통합을 통해 (SIR) 제품의 차단 요청 목록 기능을 사용하여 악성 IP 주소, URL 및 도메인을 차단합니다 ServiceNow 보안 인시던트 응답 . 이 차단 요청 목록은 Check Point 게이트웨이에서 사용자 지정 인텔리전스 피드로 구성됩니다. 사용자 지정 인텔리전스 피드 기능은 사용자 지정 사이버 인텔리전스 피드를 차세대 위협 방지 엔진에 추가하는 기능을 제공합니다. 이를 통해 타사 서버(이 경우 ServiceNow 보안 인시던트 응답 애플리케이션)에서 안티바이러스 및 안티봇 블레이드에 의해 적용될 Check Point Next Generation Gateway로 직접 피드를 가져올 수 있습니다. 보안 인시던트 응답 분석가는 SIR 보안 인시던트에서 악성 ServiceNow 으로 확인된 옵저버블에서 Check Point 차단 목록에 대한 항목을 생성합니다.

대부분의 구현에서 차단 요청 목록은 외부 웹 서버에서 호스팅되는 csv 파일입니다. 이 통합의 경우 이 웹 서버는 ServiceNow AI Platform Check Point 차세대 위협 예방 엔진이 차단할 IP 주소, URL 및 도메인 목록을 가져오도록 허용하는 인스턴스입니다.

Check Point 게이트웨이에서 차단 옵저버블을 적용하려면 위협 방지 정책이 안티봇 및 안티바이러스 블레이드가 활성화된 상태로 구성되어 있는지 확인합니다. 차단 목록 항목이 수정되면 Threat Prevention Engine은 구성된 간격으로 목록을 동적으로 임포트하고 방화벽에서 구성 변경이나 커밋 없이 정책을 적용합니다. 이 통합을 ServiceNow AI Platform 위해 이(가) 구성된 검색 간격으로 인증된 Check Point 차세대 게이트웨이에서 검색한 차단 목록 항목이 포함된 테이블을 생성했습니다.

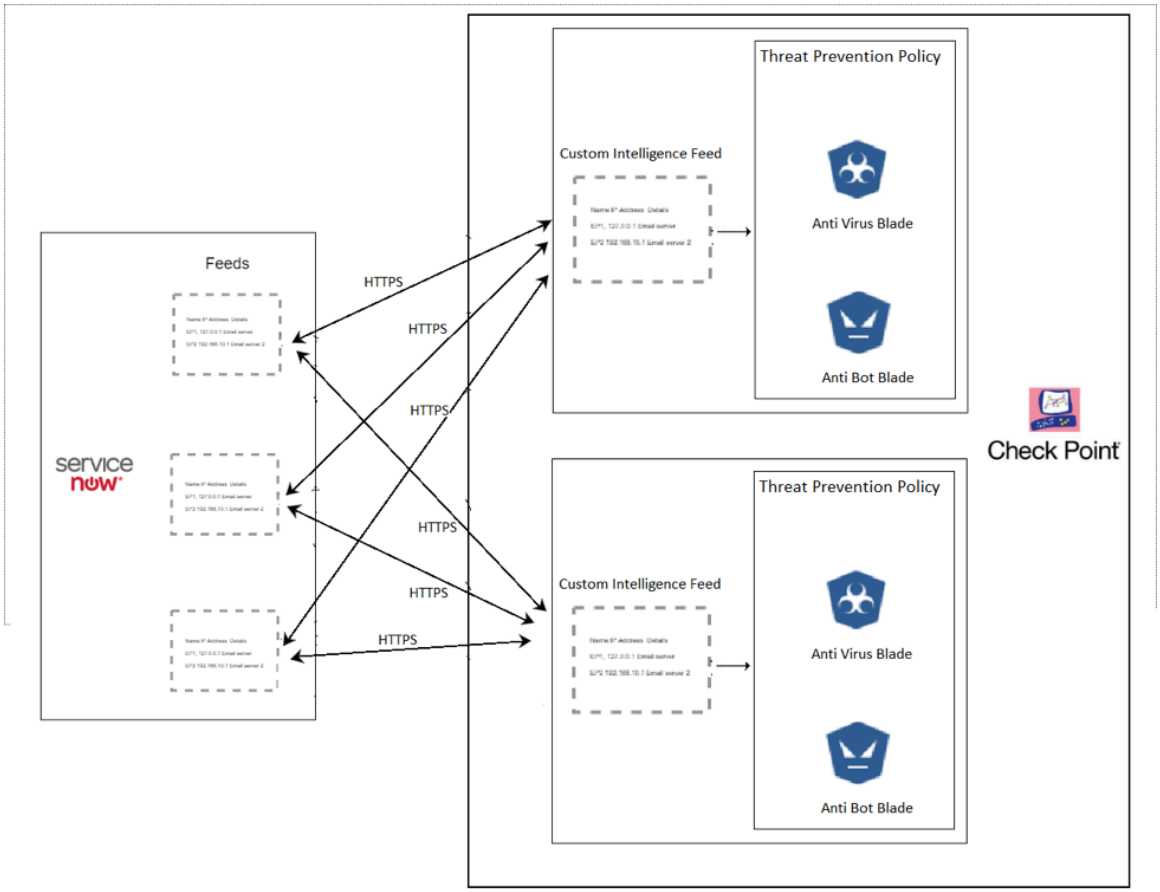
통합에는 다음과 같은 기능이 포함됩니다.

- 여러 체크 포인트 게이트웨이에 적용되는 여러 블록 목록을 생성할 수 있는 유연성.
- 차단되는 사이트 유형(피싱, 맬웨어 및 허용 목록에 지정된 사이트)에 대한 자세한 보고입니다.
- 차단 목록 항목을 옵저버블 유형(URL, 도메인, IP 주소)별로 보안 인시던트에 ServiceNow AI Platform 태그를 지정합니다.
- 이전 항목을 자동으로 만료 또는 제거하여 차단 목록 크기를 유지하도록 차단 목록 만료 기간을 구성합니다.
- 서로 다른 차단 목록 간의 차단 목록 항목 검색
- 차단 목록 항목을 위협 인텔리전스 결과와 항목이 차단된 이유에 대한 세부 정보가 포함된 옵저버블 기록 및 보안 인시던트에 연결합니다.

통합 아키텍처 다이어그램

다음은 관련 구성요소와 NOW Platform과 Check Point Systems 간의 통합 지점을 보여주는 개략적인 아키텍처 다이어그램입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



주:
Check Point Systems 로고, 안티바이러스 블레이드 이미지 및 안티 봇 블레이드 이미지는 Check Point Systems ©에서 가져온 것입니다. Check Point Systems의 속성입니다.

플러그인

통합하려면 (com.snc.security_incident) 플러그인을 활성화해야 합니다 보안 인시던트 응답 .

플러그인을 설치 보안 인시던트 응답 하려면:

1. HI 자격 증명을 사용하여 인스턴스에 로그인합니다.
2. 관리자(admin) 역할이 있는지 확인합니다.
3. 인스턴스에서 시스템 정의〉플러그인으로 이동합니다.
4. 보안 인시던트 응답을 선택하고 클릭합니다.

이러한 플러그인이 설치되면 ServiceNow Store에서 새 Check Point 통합 플러그인을 업로드하고 다음 구성 지침을 따를 수 있습니다.

지원되는 체크 포인트 OS 버전

이러한 통합에는 Check Point와 안티봇 및 안티바이러스 블레이드의 사용자 지정 인텔리전스 피드가 필요합니다. R80.20 이상에서 지원됩니다. Check Point R80.10 Jumbo HF take 121 이상으로 알려진 Custom Intelligence 기능의 핫픽스를 설치합니다. 제품 호환성 매트릭스에 대한 자세한 내용은 Check Point 사용자 지정 인텔리전스 피드 설명서의 설치 섹션을 참조하십시오.

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

핫픽스를 설치한 후 Check Point 게이트웨이에서 아래 명령에 액세스할 수 있는지 확인합니다. 게이트웨이에 SSH를 연결하고 전문가 모드로 로그인합니다.

```
[gw-93440b> expert
[Enter expert password:


Warning! All configurations should be done through clish
You are in expert mode now.

[[Expert@gw-93440b:0]# ioc_feeds --help
External indicators configuration

positional arguments:
  show, add, delete, modify
                        Select an action for the external indicators configurations

optional arguments:
  -h, --help            show this help message and exit
  --feed_name           Set feed name
  --transport           Set feed transport protocol: http, https, local_file, local_directory
  --resource            Set feed resource URL
  --state               Set feed enforcement Active / Inactive
  --feed_action         Set feed action: Prevent, Detect, Ask
  --proxy               Set feed proxy
  --proxy_user_name     Set feed proxy user name
  --user_name           Set user name for remote feed
  --test                Set test as true if feed is for testing purposes only
  --format [ [ ...]]    Enter format in order to fetch custom csv file
  --delimiter           Enter delimiter in order to fetch custom csv file
  --comment [ [ ...]]   Enter comment char in order to fetch custom csv file
Missing a few arguments.
[Expert@gw-93440b:0]#
```

지원되는 **ServiceNow** 버전

San Diego 릴리스 버전 이상이 지원됩니다.

참조

다음은 필수 구성요소를 설정하는 데 유용한 몇 가지 Check Point 참조입니다.

1. 사용자 지정 인텔리전스 피드 기능 - https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193
2. 안티 봇 및 안티 바이러스 블레이드를 설정하려면 Check Point 사용자 가이드를 참조하십시오. http://downloads.checkpoint.com/dc/download.htm?ID=46534
3. Check Point에서 HTTPS 검사를 설정하려면 아래 링크를 따르십시오. https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk108202

권한 및 역할

다음 ServiceNow 역할이 필요합니다.

- 통합 애플리케이션 플러그인 설치를 위한 관리자(admin)
- ServiceNow에서 차단 목록을 생성하고 차단 목록 항목 추가 및 비활성화 요청을 승인해 주는 보안 인시던트 관리자(sn_si.admin)
- 차단 목록 항목 기록을 생성하고 유지 관리하기 위한 보안 분석가(여기서는 SOC 분석가, sn_si.analyst라고도 함)입니다.

보안 분석가 역할 할당에 대한 자세한 내용은 ServiceNow 설명서 웹 사이트에서 보안 운영〉보안 인시던트 응답> 보안 분석가 할당을 참조하십시오.

Check Point NGTP 설정

통합을 사용하려면 Check Point NGTP 먼저 API 계정을 만들고, 정책을 설정하고, 통합을 활성화해야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

통합을 위한 **Check Point NGTP API** 계정 생성

이 통합을 위해서는 인스턴스에 ServiceNow AI Platform API 계정 역할이 필요합니다. 이 계정과 연결된 사용자 이름 및 암호는 체크 포인트에 ServiceNow AI Platform 작성되어 입력되므로 체크 포인트는 차단 목록 항목을 검색할 때 체크 포인트로 ServiceNow AI Platform 인증됩니다.

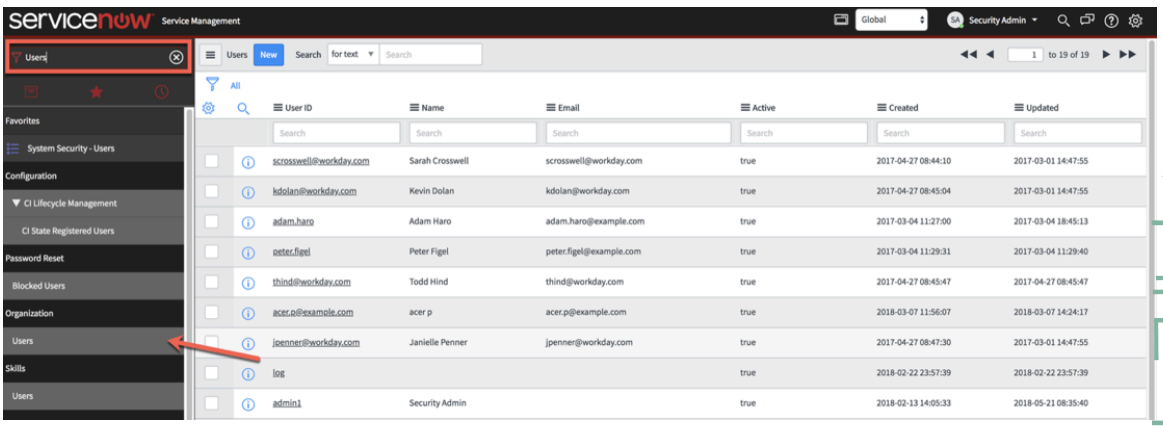
시작하기 전에
필요한 역할: 관리자

이 태스크 정보
ServiceNow AI Platform 관리자는 API 계정 역할(sn_sec_checkpoint.api_account_access)을 생성합니다. 이 계정은 Check Point에서 인증에 필요한 자격 증명을 입력하는 데만 사용되므로 게이트웨이 ServiceNow AI Platform는 . 이 계정은 인스턴스에서 별도의 고유한 API 사용자 계정 ServiceNow AI Platform 이며 Check Point 관리자에게 할당됩니다.

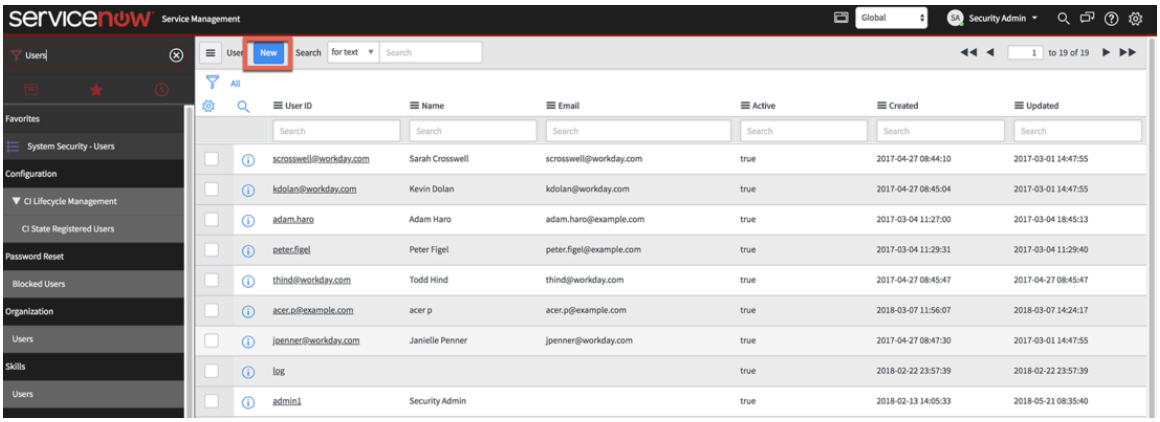
프로시저

1. 다음으로 이동 모두 〉 조직 〉 사용자.

2. 사용자 모듈을 클릭합니다.

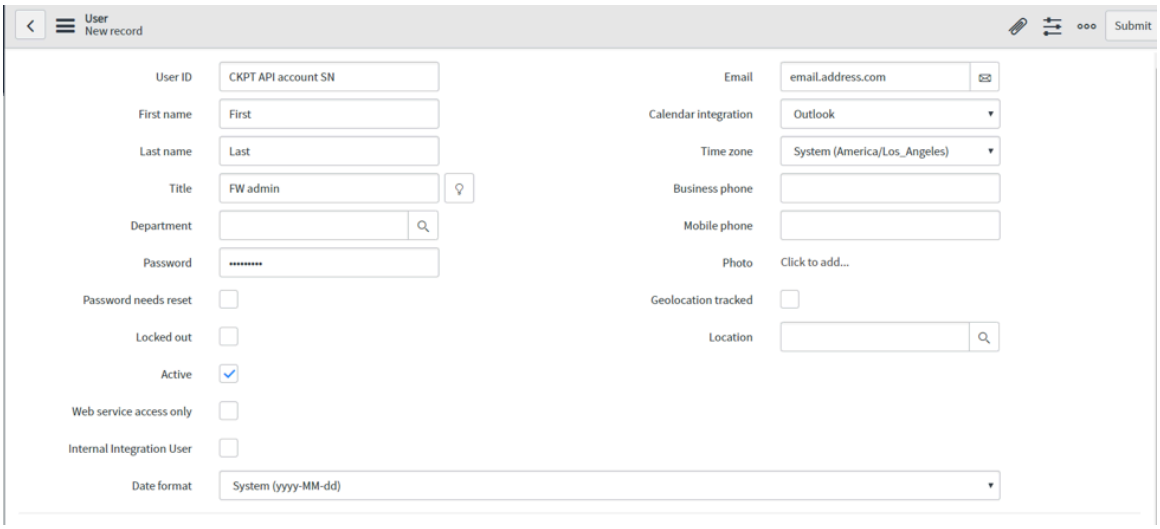


3. 표시되는 사용자 목록에서 새로 만들기를 클릭합니다.



새 양식이 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



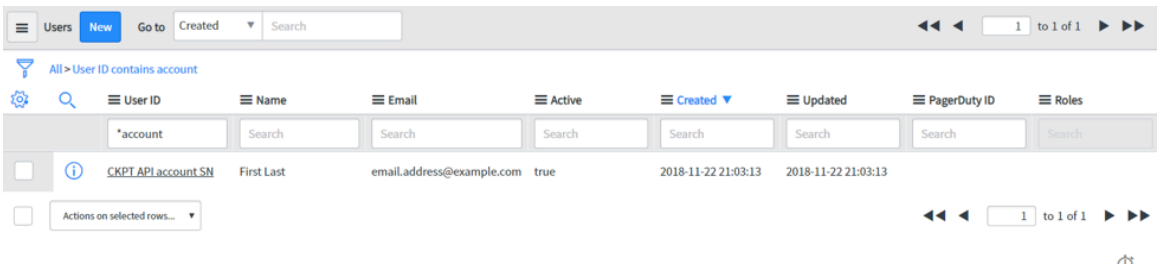
4. 필요에 따라 양식을 작성합니다.

주:
다음 표와 그림에 표시된 사용자 ID, 제목 및 전자 메일 주소의 값은 예제 값입니다.

필드	설명
사용자 ID	인스턴스의 역할에 대한 고유 사용자 ID입니다 ServiceNow AI Platform . 이 사용자 ID는 차단 목록 구성 체크 포인트 게이트웨이의 클라이언트 인증 섹션에 있는 사용자 이름 필드에 입력됩니다. 예를 들어 CKPT API 계정 SN이 있습니다.
이름	할당하려는 사람
성	할당하려는 사람
직위	직함(예: FW 관리자).
암호	이 역할에 대해 생성된 고유한 암호입니다. 이 암호는 Check Point 게이트웨이의 차단 목록 구성의 클라이언트 인증 섹션에 있는 암호 필드에 입력됩니다.
이메일	고유 이메일 주소

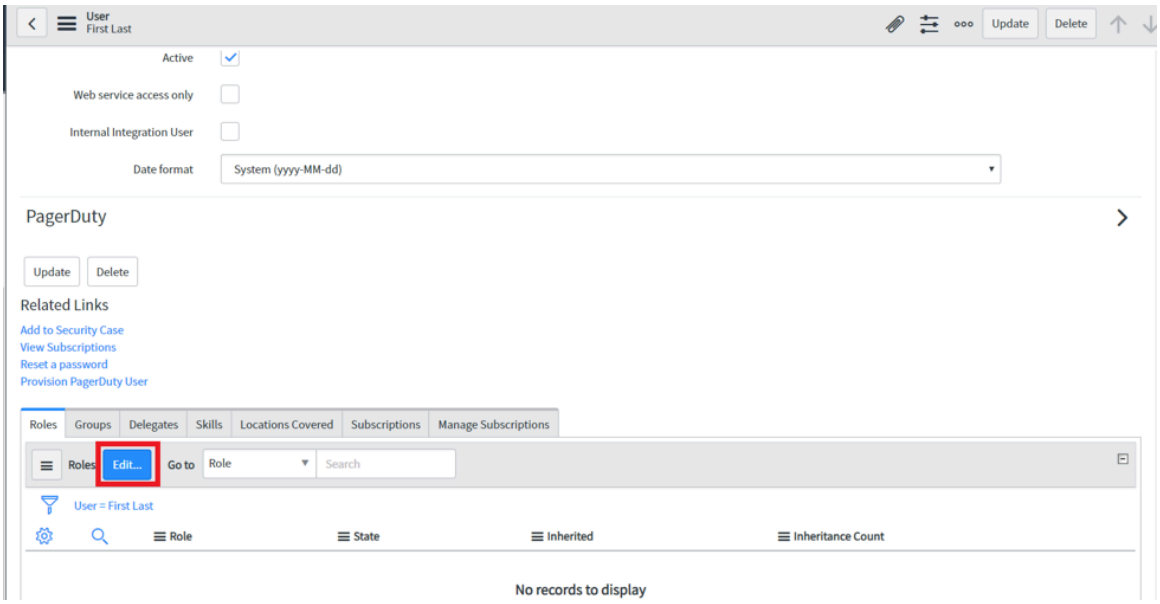
5. 제출을 클릭합니다.
제출한 후에는 역할을 할당할 수 있습니다.

6. 사용자 목록의 사용자 ID 열에서 입력한 사용자 ID의 이름(예: CKPTAPI 계정 SN)을 클릭합니다.

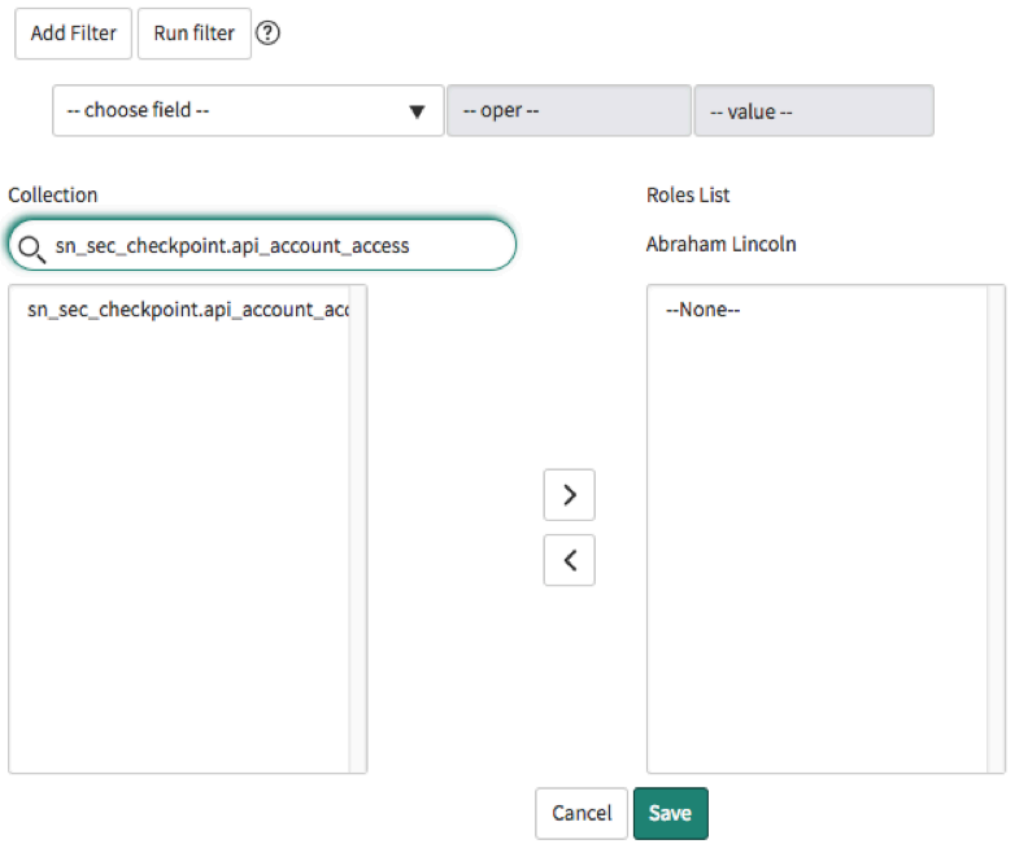


7. 역할 섹션의 열린 기록에서 편집을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

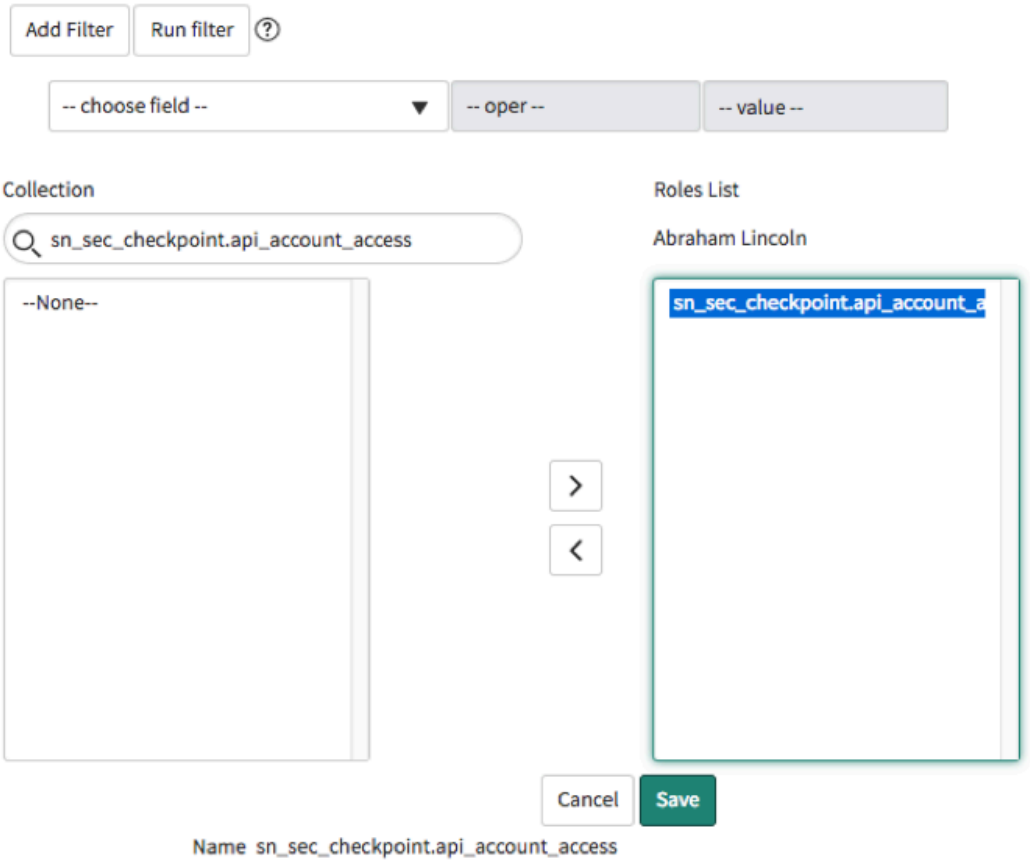


8. 표시되는 구성원 편집 양식의 컬렉션 필드에 sn_sec_checkpoint.api_account_access를 입력합니다.



9. 컬렉션 열에서 sn_sec_checkpoint.api_account_access를 선택한 후 역할 목록으로 이동합니다.
10. 저장을 클릭합니다.
11. 사용자로 이동하고 목록의 사용자 열에서 역할에 대해 생성한 ID 이름(CKPT API 계정 SN)을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



12. 사용자 기록이 표시됩니다. 이 기록은 사용자 계정이 할당되었음을 확인합니다.

Check Point NGTP 통합 설정

통합을 설정하려면 Check Point Next Generation Threat Prevention 다음 단계를 완료하십시오. 이렇게 하면 통합이 작동하기 위한 전제 조건이 마련됩니다.

시작하기 전에
필요한 역할: 관리자

프로시저

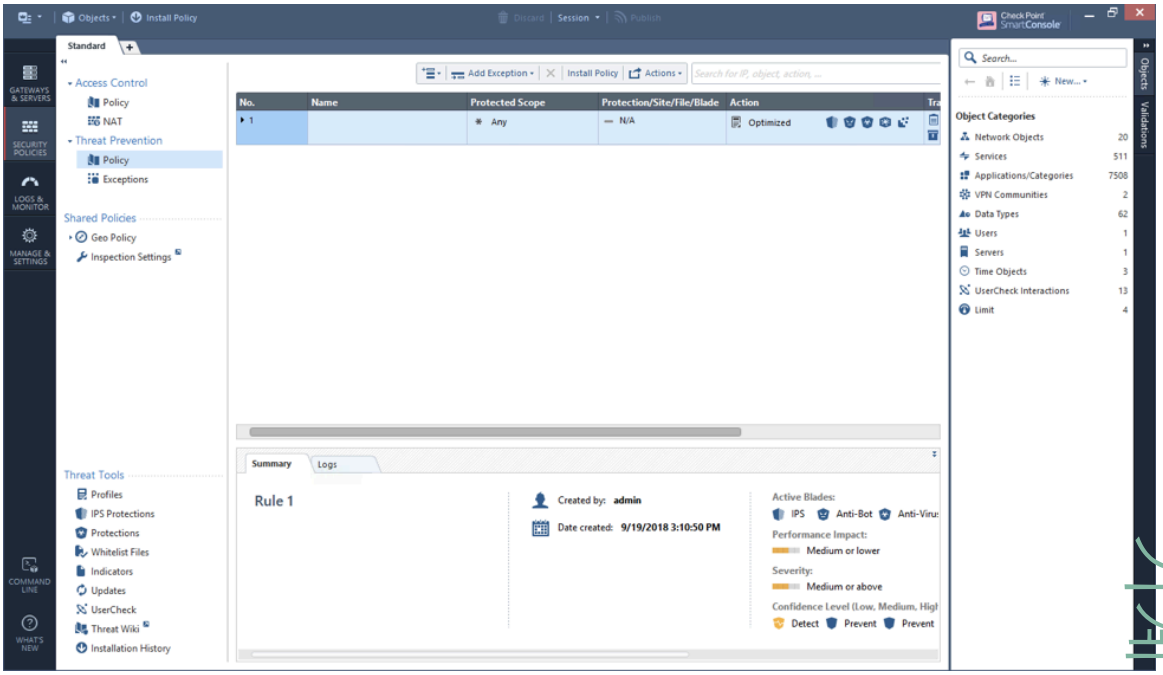
1. 위협 방지 정책이 안티봇 및 안티바이러스 블레이드가 활성화된 상태로 구성되어 있는지 확인합니다.
   안티 봇 및 안티 바이러스 블레이드 설정에 대한 자세한 내용은 참조 섹션에 언급된 Check Point 사용자 가이드를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

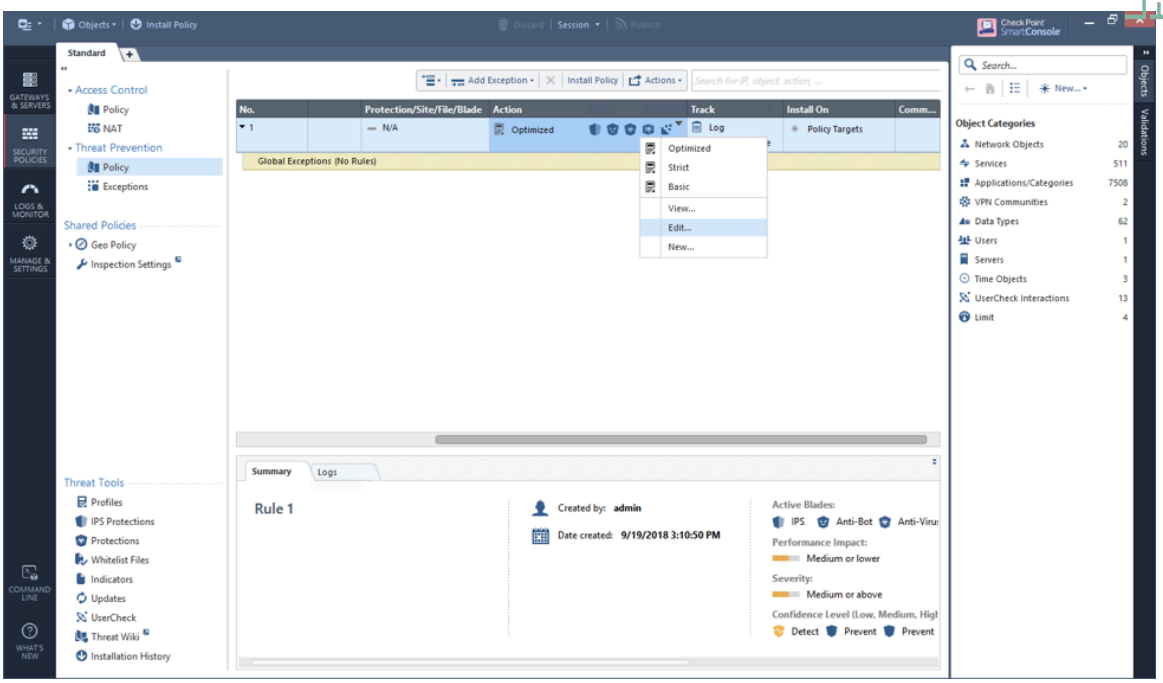
주:
이 항목의 이미지는 권한이 있고 독점적이며 Check Point Software Technologies, Ltd.의 허가를 받아 사용됩니다.

a. Smart Console에 로그인합니다.

b. 다음으로 이동 보안 정책 〉 위협 예방 〉 정책.



c. 편집 모드에서 Threat Prevention 정책을 엽니다.

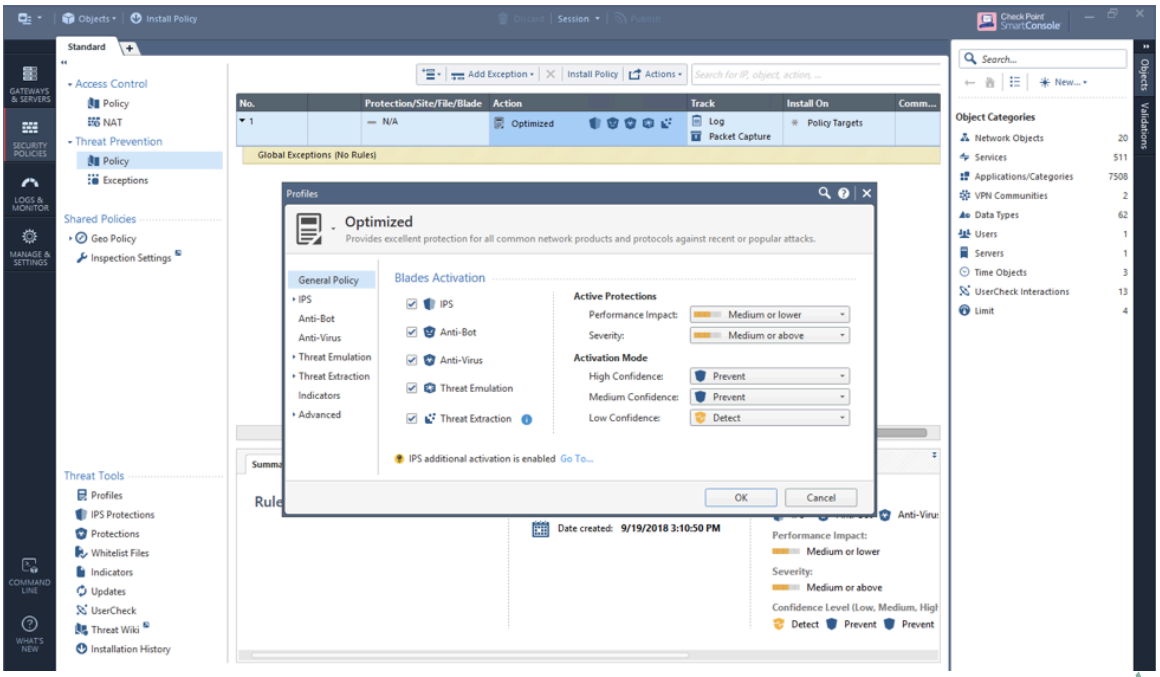


d. 활성 보호 → 심각도는 "중간 이상"이어야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

e. 높은 신뢰도→ 활성화 모드는 "방지"여야 합니다.

f. Blades Activation # Anti-Virus 및 Anti-Bot을 선택해야 합니다.



g. 변경 내용(있는 경우)을 게시하고 정책을 설치합니다.

2. 아직 구성되지 않은 경우 안티봇 및 안티바이러스 블레이드를 활성화한 후 사용자 지정 인텔리전스 피드를 추가해야 합니다.
Check Point 사용자 지정 인텔리전스 피드 기능 설명서의 설치 섹션을 참조하십시오. https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193

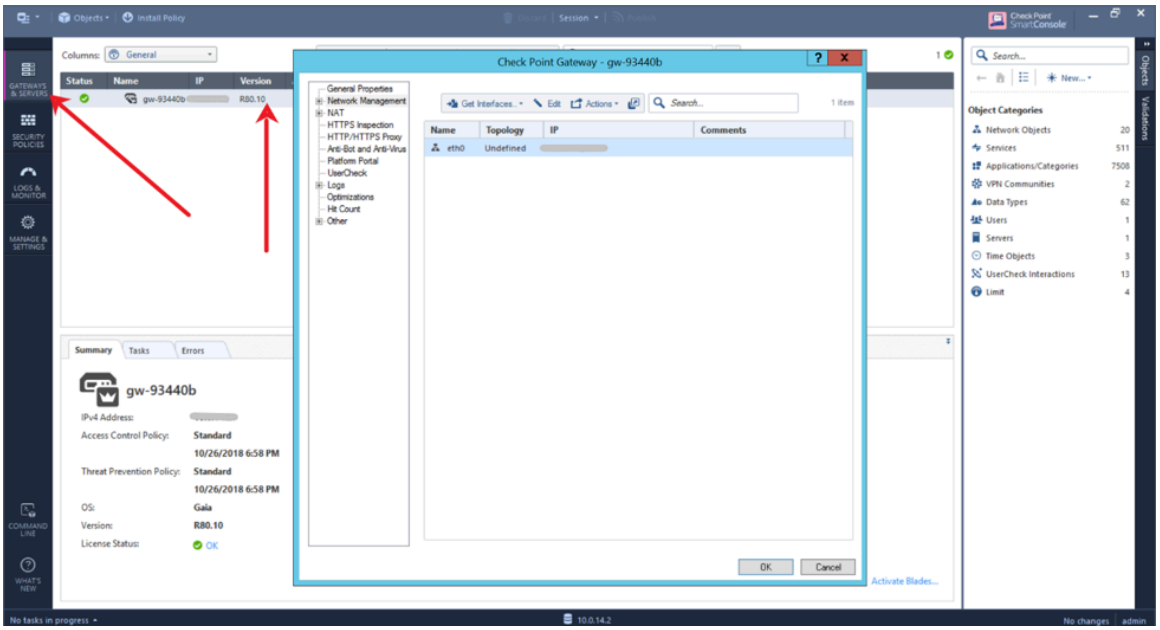
3. 아직 구성하지 않은 경우 HTTP 프록시를 통해 모든 인터넷 트래픽을 라우팅하도록 Check Point 게이트웨이를 설정합니다(HTTPS 검사를 구성하는 경우).

> **주:**
> Check Point NGTP에서 URL 차단의 경우 확인해야 하는 특정 설정이 있습니다. HTTPS 인터넷 트래픽은 SSL(Secure Sockets Layer) 프로토콜을 사용하며 암호화되어 데이터 프라이버시를 제공합니다. 그러나 HTTPS는 차단되었어야 하는 악성 트래픽을 숨길 수 있습니다. Check Point 게이트웨이가 HTTPS 트래픽에 대한 가시성을 확보하려면 HTTP 프록시를 통해 트래픽을 라우팅하거나 HTTPS 검사 (권장)를 설정하십시오. 이 섹션에서는 Check Point 게이트웨이에서 HTTP 프록시를 설정하기 위해 따라야 할 단계에 대해 자세히 설명합니다.

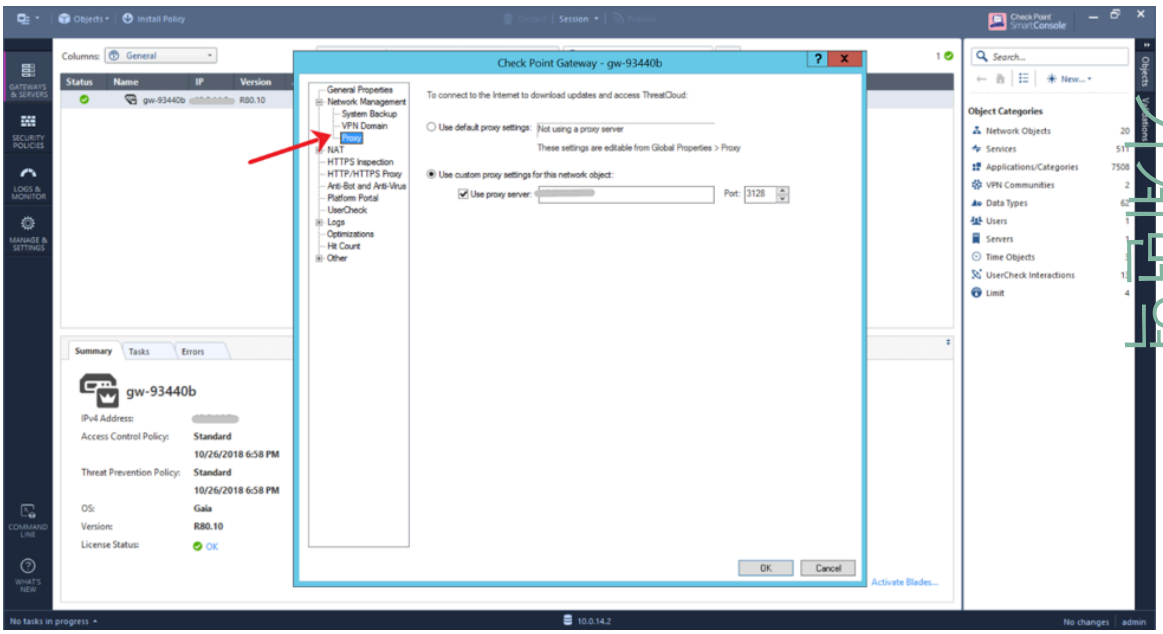
a. Smart Console에 로그인합니다.

b. 서버 및 게이트웨이로 이동하고 해당 서버를 두 번 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



c. 다음으로 이동 네트워크 관리 〉 프록시.



d. HTTP 트래픽을 라우팅하는 데 사용할 프록시 상세 정보를 제공합니다.

e. 클라이언트 엔드포인트의 HTTP 요청이 HTTP 프록시를 통해 이루어지는지 확인합니다.

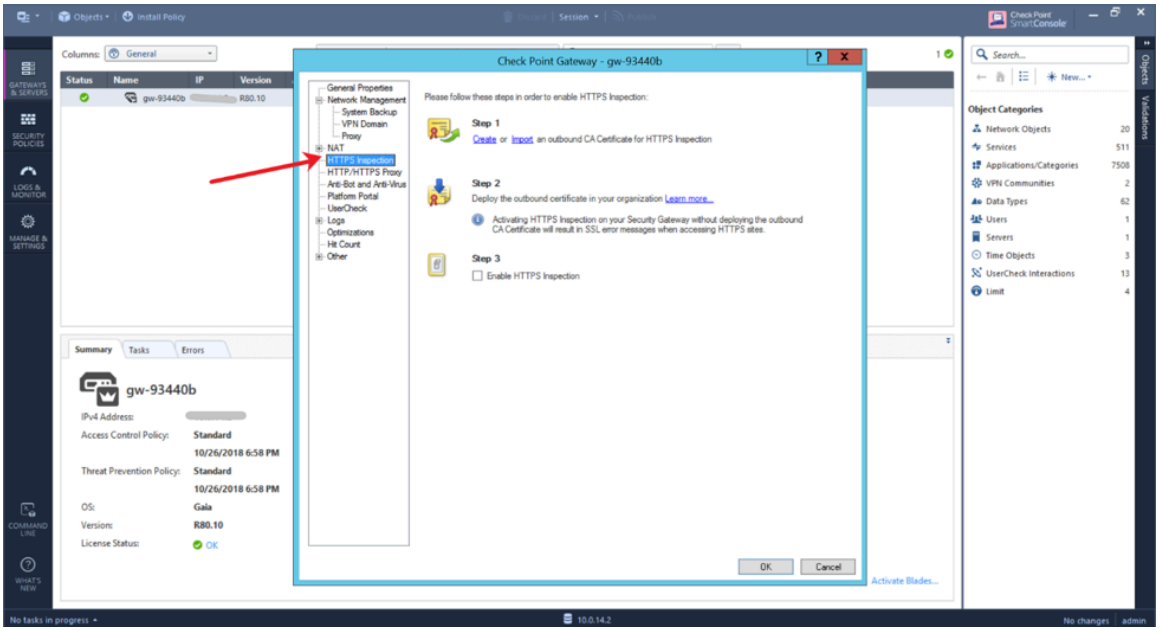
4. 아직 구성되지 않은 경우 HTTPS 검사를 활성화합니다(HTTP 프록시가 구성된 경우).
대부분의 트래픽이 SSL을 통해 이루어지는 경우 HTTPS 검사 블레이드를 사용하는 것이 좋습니다. 이렇게 하면 트래픽이 GW에 투명해집니다. 다음과 같이 Check Point 게이트웨이에서 HTTPS 검사를 사용하도록 설정합니다.

a. Smart Console에 로그인합니다.

b. 서버 및 게이트웨이로 이동하고 해당 서버를 두 번 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

c. HTTPS 검사로 이동합니다.



d. Check Point 사용자 가이드에서 HTTPS 검사를 구성하는 단계를 따르십시오.

통합 활성화 **Check Point NGTP**

애플리케이션을 설치하지 않은 경우 지침에 따라 설치합니다.

시작하기 전에

필요한 역할: 관리자

프로시저

1. 애플리케이션을 설치할 인스턴스에 로그인합니다.
2. 다음으로 이동 시스템 애플리케이션 〉 애플리케이션.
3. 다운로드 탭을 클릭합니다.
   설치할 수 있는 애플리케이션 목록이 표시됩니다.
4. 응용 프로그램을 찾아서 Check Point Next Generation Threat Prevention 선택하고 설치를 클릭합니다.
   애플리케이션이 인스턴스에 자동으로 설치됩니다.

차단 목록 작업

통합은 ServiceNow Check Point Next Generation Threat Prevention IP, URL 및 도메인 옵저버블을 허용하는 차단 목록을 지원합니다.

ServiceNow 구성된 차단 목록은 외부 웹 서버에서 호스팅되는 CSV 파일이며, 이 통합에서는 인스턴스가 해당 ServiceNow AI Platform 됩니다. 사용자 지정 인텔리전스 피드는 미리 구성된 간격으로 IP 주소, URL 및 도메인을 ServiceNow AI Platform 끌어오는 체크 포인트 게이트웨이에 구성됩니다.

이 통합은 다음 세 가지 유형의 차단 목록을 지원합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- IP 주소(여기에는 차단 목록에 대한 개별 IP 주소(IPv4에만 해당)와 허용 목록에 대한 CIDR 블록(주소 범위)이 포함됨)
- URL
- 도메인

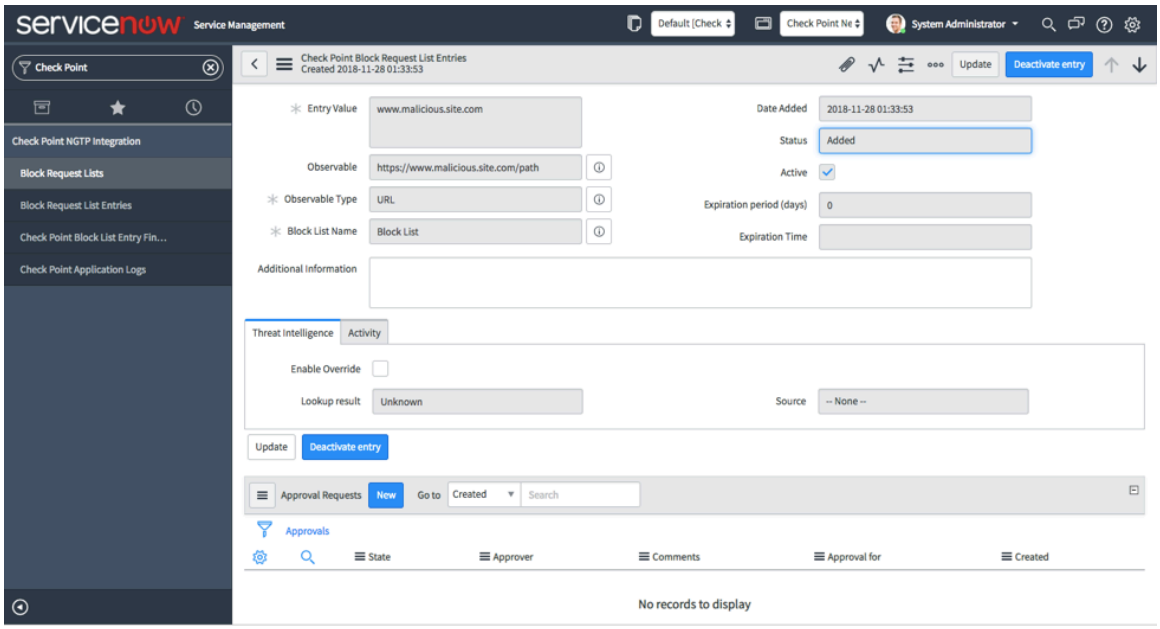
통합에서 **Check Point NGTP** 지원되는 옵저버블

이 섹션에는 이 통합에서 지원되는 옵저버블에 대한 설명과 각 유형에 대한 예제 형식이 나열되어 있습니다.

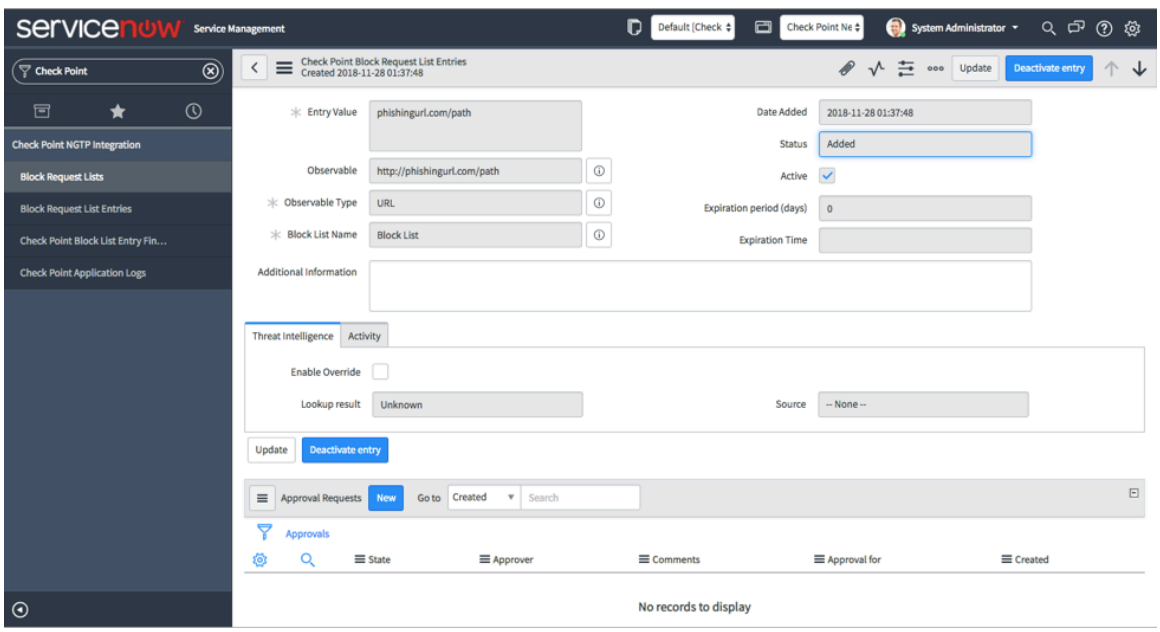
관찰 대상 유형	예제	설명
도메인	• example.com • mail.example.com	와일드카드는 지원되지 않습니다.
IP 주소	95.153.103.54(IPv4)	고유한 단일 인터페이스 주소를 나타냅니다. 통합은 IPv4 및 CIDR 형식만 지원합니다(CIDR 형식은 허용 목록 목적으로만 지원됨). 허용 목록을 위해 통합에는 CIDR(Classless Inter-Domain Routing) 범위(예: 95.153.100.0/22)가 포함된 IP 주소 옵저버블이 지원됩니다. **주:** CIDR 범위의 일부로 이미 나열된 차단 목록에 단일 IP 주소를 연결하려고 하면 오류 메시지가 표시됩니다. 예를 들어 단일 주소 95.153.103.54는 95.153.100.0/22(95.153.100.0-95.153.103.255)로 표현되는 CIDR 범위의 일부입니다.
URL	• https://www.example.com • http://www.example.com	설명 - HTTPS URL은 URL에서 경로를 자르고 도메인 이름만 유지하도록 애플리케이션에 의해 형식이 지정됩니다. Check Point NGTP는 HTTP CONNECT 요청을 사용하여 웹 트래픽을 평가하고 차단을 적용합니다. HTTPS CONNECT 요청의 경우 전체 URL이 요청에 표시되지 않고 도메인 이름만 표시됩니다. 사용자가 특정 경로(예:

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관찰 대상 유형	예제	설명
		https://www.example.com/path)가 있는 HTTPS URL을 차단하면 애플리케이션이 경로를 자동으로 트리밍합니다(www.example.com). 애플리케이션은 원래 옵저버블과 서식이 지정된 URL 간의 관계를 유지합니다. 다음은 형식이 지정된 URL과 원래 옵저버블을 보여주는 차단 목록 항목의 스크린샷입니다.



특정 경로(예: http://www.example.com/path)가 있는 HTTP URL의 경우 전체 URL이 CONNECT 요청에 표시되므로 Check Point에서 지정된 URL을 차단합니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

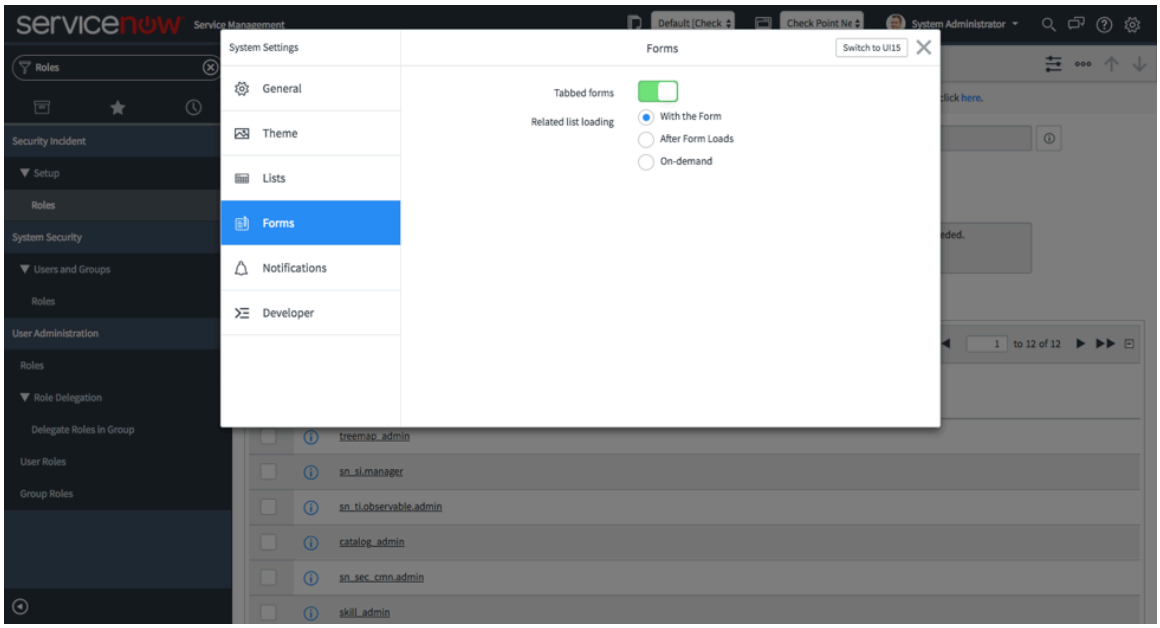
통합에 **Check Point NGTP** 대한 차단 목록 생성

인스턴스에 차단 목록을 ServiceNow AI Platform 생성합니다. 승인 및 활성화되면 Now Platform SIR(Security Incident Response) 인시던트에서 악성으로 확인된 옵저버블에서 이러한 차단 목록에 대한 항목을 생성하고 차단 승인을 요청할 수 있습니다.

시작하기 전에
필요한 역할: 보안 인시던트 관리자(sn_si.admin)

이 태스크 정보
Check Point에서 목록에 포함된 객체(IP 주소, URL, 도메인)를 임포트할 수 있도록 인스턴스에 차단 목록을 ServiceNow AI Platform 생성합니다. 사용자 지정 인텔리전스 피드는 사전 구성된 간격으로 Now Platform에서 IP 주소, URL, 도메인을 끌어오는 Check Point Gateway에 구성됩니다. 옵저버블을 차단하려면 안티봇 및 안티바이러스 블레이드가 활성화된 위협 예방 정책을 구성해야 합니다.

주:
이 항목의 그림은 시스템 설정에서 선택 취소된 탭 양식 으로 표시됩니다.



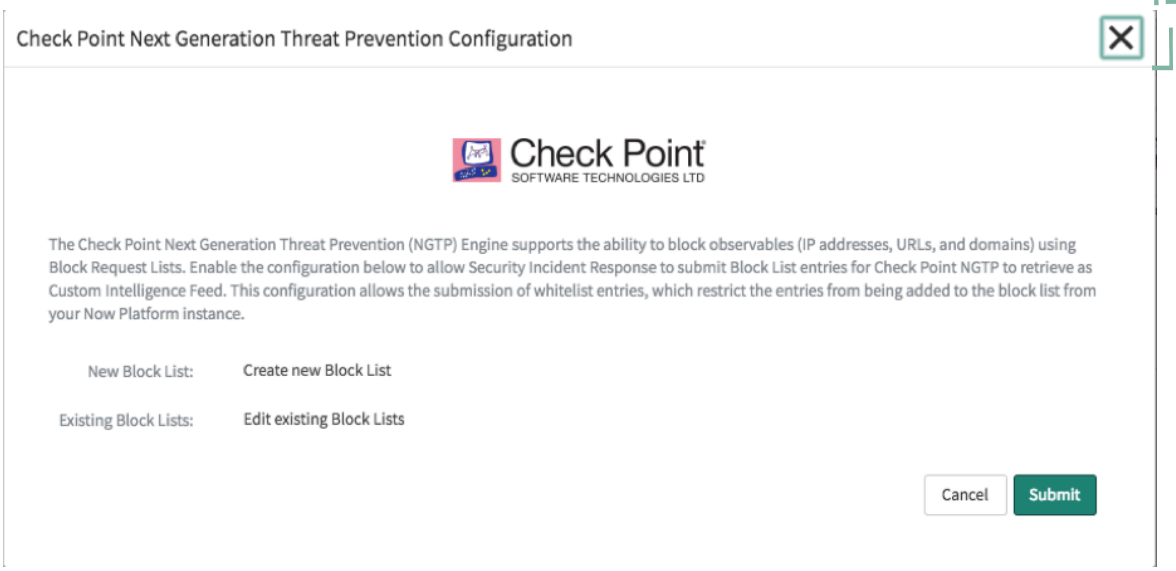
프로시저

1. 애플리케이션 설치가 완료되면 통합 〉 통합 구성.
2. **Check Point Next Generation Threat Prevention** 카드를 찾아 Configure(구성)를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
Check Point Software Technologies, Ltd.의 허가를 받아 사용되는 특권 및 독점 콘텐츠

3. 새 차단 목록 만들기를 클릭합니다.



4. 양식에서 필드를 채웁니다.

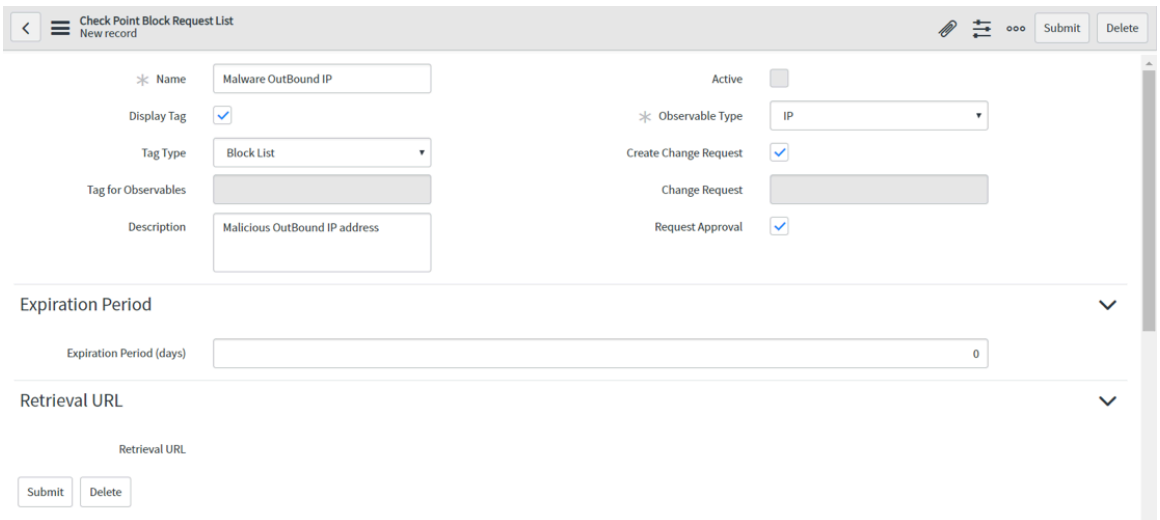
필드	설명
이름	체크 포인트 차단 요청 목록 이름입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	보안 분석가가 차단 목록의 의도를 이름으로 쉽게 인식할 수 있도록 이 필드에 옵저버블 유형(URL, IP, 도메인)을 포함합니다. 또한 이름은 이러한 차단 목록 개체가 매핑되는 방화벽 정책을 명확하게 나타내야 합니다. 차단 목록 이름의 예로는 아웃바운드 맬웨어 IP 또는 아웃바운드 피싱 URL이 있습니다.
활성	이 확인란은 차단 목록이 비활성 상태임을 나타내기 위해 기본적으로 선택이 취소되어 있습니다. 비활성화되면 차단 목록에서 추가 항목을 받을 수 없습니다. 이 확인란을 선택하면(변경 요청이 종결되거나 변경 요청이 생성되지 않은 경우) 차단 목록이 활성화되고 차단 목록 항목에 사용할 수 있습니다.
태그 표시	옵저버블이 차단 목록에서 차단된 경우 옵저버블 및 관련 보안 인시던트 기록에 자동으로 태그를 지정하려면 확인란이 기본적으로 선택되어 있습니다. 선택하면 양식에서 "옵저버블에 대한 태그" 필드를 사용할 수 있습니다. 주: 태그 이름은 기본적으로 Check Point-Prefix (예: Check Point-Malware OutBound IP)를 사용하여 Name 필드에 입력한 값에서 생성됩니다. 태그 이름과 색상을 변경할 수 있습니다. 차단 목록이 저장되면 태그 이름이 "옵저버블에 대한 태그" 필드에 표시됩니다. 확인란의 선택을 취소하면 태그가 생성되지 않으며 양식에서 "옵저버블에 대한 태그" 필드를 사용할 수 없습니다.
관찰 대상 유형	이 차단 목록이 목록에서 허용하는 옵저버블 유형(IP 주소(허용 목록의 CIDR 포함), URL 또는 도메인)을 선택합니다.
태그 유형	목록에서 사용할 수 있는 태그입니다. 차단 목록은 Check Point Next Generation Threat Prevention에서 차단하려는 옵저버블 목록입니다. 허용 목록은 어떤 경우에도 Check Point 차세대 위협 방지에서 차단하지 않으려는 옵저버블 목록입니다. 기본적으로 차단 목록 태그 색은 검은색이고 허용 목록 태그 색은 회색입니다. 색상을 변경할 수 있습니다.
변경 요청 작성	이 확인란은 기본적으로 선택되어 있으며, 인스턴스에서 차단 목록 기록에 연결된 변경 요청 및 변경 작업을 ServiceNow AI Platform 자동으로 생성합니다. 변경 요청은 Check Point 차세대 방화벽 게이트웨이에서 차단 목록 검색 URL을 구성하는 데 사용됩니다. 방화벽 관리자가 방화벽 정책 또는 규칙 변경에도 사용하는 ServiceNow AI Platform 경우 이 옵션을 사용하는 것이 좋습니다. 요청을 생성한 경우 요청이 종결되면 차단 목록이 자동으로 활성화됩니다. 방화벽 관리자로부터 사용자 지정 인텔리전스 피드가 모든 체크 포인트 게이트웨이에 구성되었다는 전자 메일을 통해 알림을 받은 후 차단 목록을 수동으로 활성화하려면 확인란의 선택을 취소합니다. 변경 요청 생성 확인란의 선택을 취소하면 변경 요청 필드를 사용할 수 없습니다.

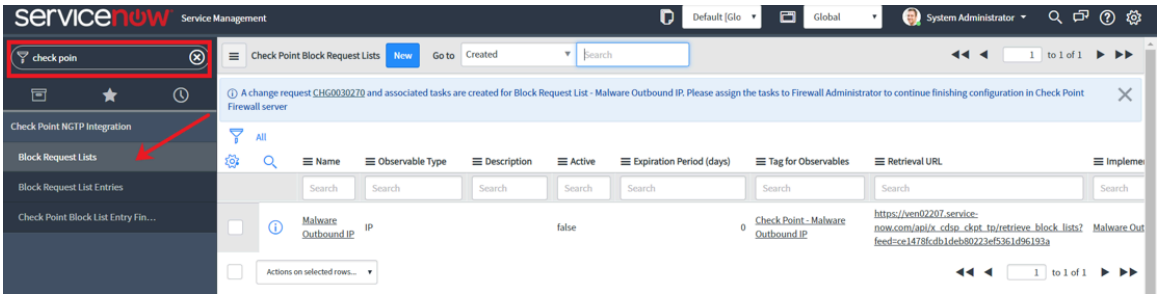
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
승인 요청	이 확인란은 차단 목록에서 차단 목록 항목을 활성화/제거하기 위한 승인을 요청하기 위해 기본적으로 선택됩니다. 보안 인시던트 관리자(sn_si.admin) 역할을 가진 사용자가 승인을 요청합니다. 승인 요청은 이메일을 통해 승인자에게 전송됩니다. 승인이 수락되면 해당 차단 목록에서 항목이 활성화됩니다. 이 확인란을 선택하지 않으면 해당 차단 목록에 대한 항목이 승인 워크플로우를 따르지 않고 차단 목록에서 직접 활성화됩니다.
옵저버블 태그	이 필드는 태그 표시 확인란이 선택된 경우에만 표시됩니다. 이름 필드의 기본값으로 차단 목록을 저장하면 필드가 자동으로 채워집니다. "맬웨어 URL"이라는 이름으로 차단 목록이 생성된 경우 파생된 태그 이름은 "차단 목록 – 맬웨어 URL"입니다.
변경 요청	변경 요청 생성 확인란을 선택하면 차단 목록이 저장되면 Now Platform 인스턴스에 변경 요청 번호가 표시됩니다. 변경 요청 생성 확인란의 선택을 취소하면 이 필드가 표시되지 않습니다.
설명	체크 포인트 차단 목록에 대한 설명입니다. 이름에는 일반적으로 이 차단 목록에 포함될 것으로 예상되는 사이트 및 옵저버블 유형이 포함되며 이 필드를 사용하여 자세한 내용을 확인할 수 있습니다.
만료 기간(일)	차단 목록의 만료 기간입니다. 0(기본값)은 차단 목록 항목이 만료되지 않음을 나타냅니다. 이 값을 변경하면 입력한 일수 동안 이 항목이 활성화됩니다. 최솟값 1, 즉 24시간을 입력할 수 있으며 최댓값은 없습니다.
검색 URL	차단 목록이 저장되면 검색 URL이 자동으로 생성됩니다. Check Point 게이트웨이에서 이 차단 목록을 구성하려면 이 URL을 사용해야 합니다. 이 URL이 구성되면 Check Point는 차단할 옵저버블을 csv 형식으로 가져옵니다.

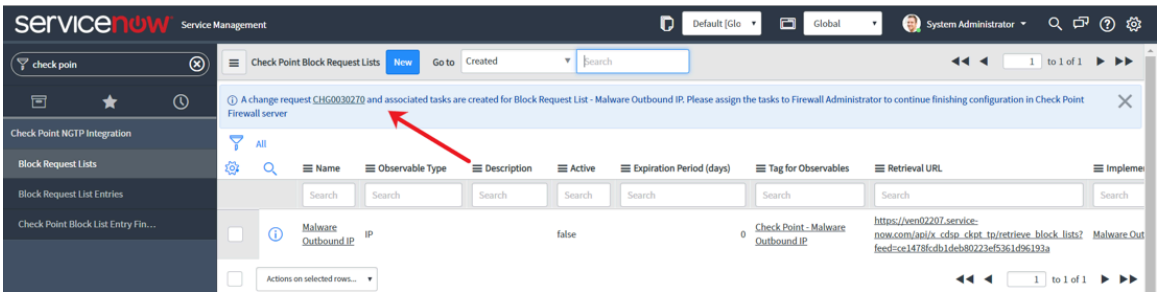


5. 제출을 클릭합니다.
6. 체크 포인트 차단 요청 목록이 표시되지 않으면 체크 포인트 **NGTP** 통합 〉 요청 목록 차단.

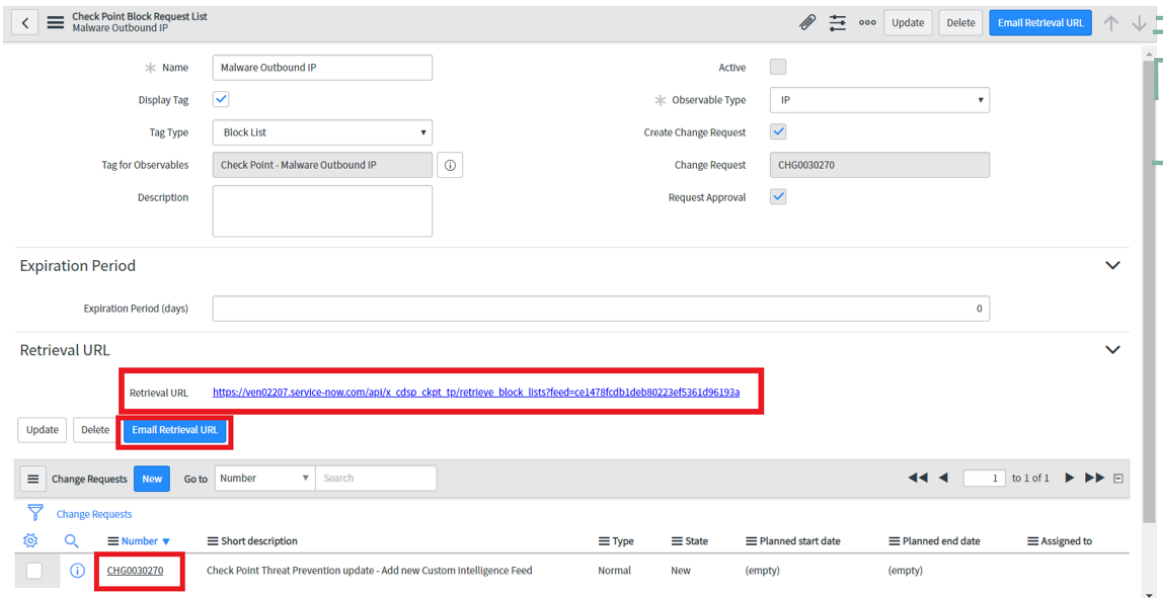
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



새 차단 목록이 표시됩니다. 차단 목록 상태가 여전히 비활성(false)이며, 이는 차단 목록에 항목을 수락할 수 없음을 의미합니다. 변경 요청 생성이 구성된 경우 변경 요청과 인스턴스에 작업이 생성 ServiceNow AI Platform 되었음을 나타내는 메시지가 표시됩니다.



7. 이름 열에서 항목을 클릭하여 기록을 엽니다.
차단 목록 기록이 표시됩니다. 이 예에서는 맬웨어 아웃바운드 IP 차단 목록을 보여 줍니다. 다음 필드, 옵션 및 링크는 제출 후 새 기록에 표시되고 다음 테이블에 설명되어 있습니다.



필드	설명
이메일 검색 URL	Check Point 방화벽 관리자에게 차단 링크를 구성에 사용할 수 있다는 알림을 이메일로 전송합니다.
검색 URL	이 URL은 Check Point 게이트웨이에서 사용자 지정 인텔리전스 피드를 구성하는 데 사용됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	주: 시스템 설정이 탭 유형 양식으로 설정되어 있는 경우 이 링크는 기록 하단의 차단 목록 검색 정보 탭에 표시됩니다.
ServiceNow AI Platform 변경 요청	구성되면 변경 요청 기록에 대한 링크가 변경 요청 섹션에 표시되고, 요청 번호는 변경 요청 필드에 표시됩니다.
업데이트	데이터를 수정하고 편집 가능한 필드를 업데이트합니다.
삭제	기록을 삭제합니다.

8. 필요에 따라 차단 목록을 더 만들고 추가합니다.
   차단 목록은 체크 포인트 차단 요청 목록 페이지에 표시됩니다.

다음에 수행할 작업

차단 요청 목록을 수동으로 또는 변경 요청과 ServiceNow AI Platform 함께 활성화합니다.

통합에 대한 **Check Point NGTP** 차단 목록 활성화

차단 ServiceNow AI Platform 목록이 만들어지고 URL을 사용할 수 있게 되면 Check Point 관리자는 모든 Check Point Next Generation Gateway에서 차단 목록을 사용자 지정 인텔리전스 피드로 구성합니다. 차단 목록 항목을 수락하려면 먼저 Check Point ServiceNow AI Platform에서 차단 목록을 구성하고 .

시작하기 전에

필요한 역할: 보안 인시던트 관리자(sn_si.admin)

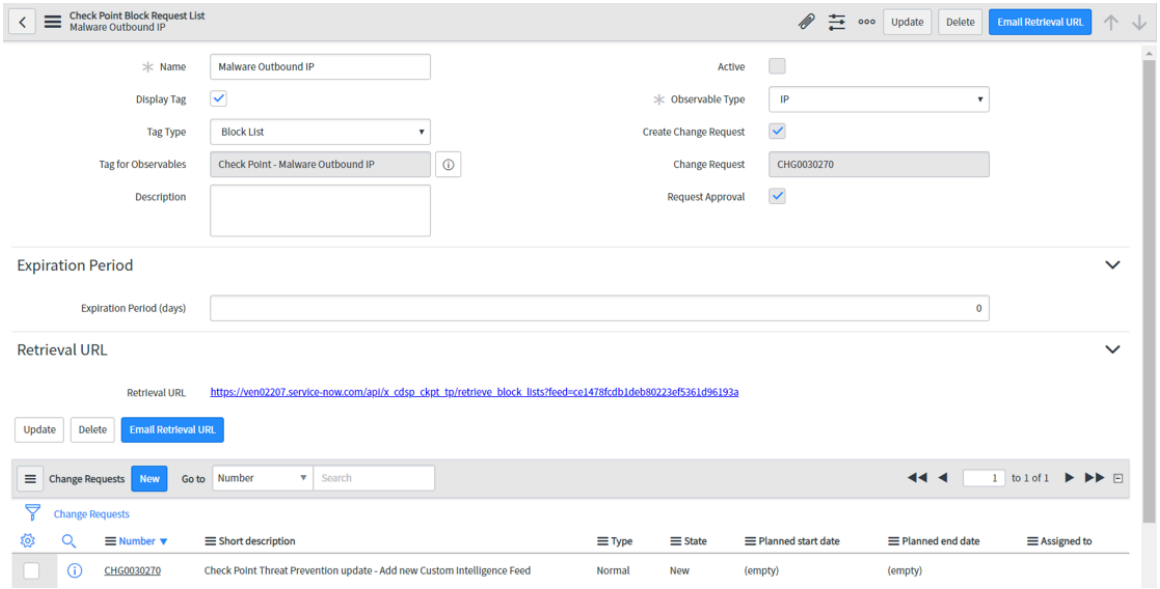
이 태스크 정보

차단 목록을 구성한 후 보안 인시던트 관리자는 차단 목록을 수동으로 활성화할 수 있으며, 변경 요청 완료 ServiceNow AI Platform 시 차단 목록이 자동으로 활성화됩니다. 변경 요청이 승인 후 비활성 상태에서 활성 상태로 전환되어야 차단 목록 항목을 수락할 수 있습니다.

프로시저

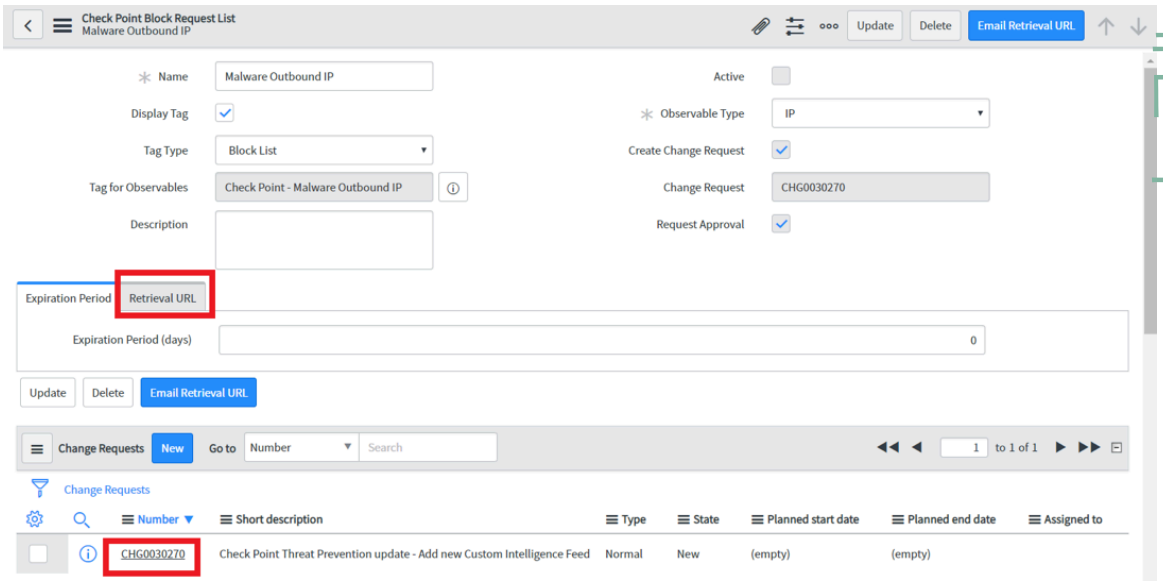
1. 다음으로 이동 모두 〉 체크 포인트 **NGTP** 통합 〉 요청 목록 차단을 클릭하고 차단 요청 목록 모듈을 선택합니다.
2. 표시되는 체크 포인트 차단 요청 목록 목록의 이름 열에서 새 차단 목록을 선택합니다.
3. 표시되는 기록에서 이메일 검색 **URL** 버튼, 활성 차단 목록 검색 URL 링크, 변경 요청(구성된 경우) ServiceNow AI Platform 섹션의 변경 요청을 적어둡니다.
   또한 활성 확인란의 선택이 취소되어 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



주:
시스템 설정에서 탭 구분 양식을 선택 취소하면 차단 목록 검색 URL이 검색 URL 섹션에 나타납니다.

4. 차단 목록 검색 **URL** 탭을 클릭하여 검색 URL을 표시합니다.
다음 그림에서는 시스템 설정에서 탭 구분 양식이 선택된 탭으로 표시되는 차단 목록 검색 URL을 보여 줍니다. 변경 요청(CH0030270)에 대한 링크도 표시됩니다.



5. 구성을 완료하고 차단 목록을 비활성에서 활성으로 이동하려면 다음 옵션 중 하나를 선택하여 방화벽 관리자에게 검색 URL을 사용할 수 있음을 알려야 합니다.

옵션	설명
이메일 검색 URL을 클릭합니다.	이메일 차단 목록 검색 URL을 방화벽 관리자에게 직접 보냅니다. 이 옵션을 사용하면 방화벽 관리자가 Check Point 플랫폼에서 구성을 완료할 수 있습니다. 방화벽 관리자가 를 ServiceNow AI Platform사용하지 않는 경우 이 옵션을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵션	설명
ServiceNow AI Platform 변경 요청을 완료하고 방화벽 관리자에게 구성 작업을 할당합니다.	이 옵션은 Check Point의 방화벽 관리자도 Now Platform을 사용하고 변경 ServiceNow AI Platform 관리 및 승인 프로세스가 구성된 경우에만 사용할 수 있습니다. **주:** 보안 인시던트 관리자(sn_si.admin) 역할이 있는 사용자는 변경 요청을 승인할 ServiceNow AI Platform 수 있습니다. 구성 작업이 완료되고 변경 요청이 종결되면 차단 목록이 자동으로 활성화됩니다.

다음에 수행할 작업

검색 URL을 사용할 수 있음을 방화벽 관리자에게 알리고 Check Point에서 차단 목록이 구성되었는지 확인한 후 보안 인시던트 관리자는 차단 목록을 활성화해야 합니다. 차단 목록을 수동으로 활성화하거나, 구성된 경우 변경 요청 양식을 사용하여 ServiceNow AI Platform 차단 목록을 활성화합니다. 차단 목록은 변경 요청이 종결될 때 자동으로 활성화됩니다.

통합에서 **Check Point NGTP** 차단 목록을 사용자 지정 인텔리전스 피드로 구성

방화벽 관리자는 NOW 플랫폼에서 생성된 차단 목록에 해당하는 사용자 지정 인텔리전스 피드를 구성해야 합니다.

시작하기 전에

필요한 역할: 관리자

이 태스크 정보

이 작업은 각 Check Point NGTP 게이트웨이에서 수행해야 합니다. 방화벽 관리자는 게이트웨이 서버의 SSH 액세스 권한이 필요합니다. 조직에 ServiceNow AI Platform 변경 관리 및 승인 프로세스가 있는 경우 이메일 보내기/받기 기능이 활성화되어 있는지 확인합니다.

방화벽 관리자는 차단 목록의 검색 URL과 체크 포인트 API 계정 접근 역할 (sn_sec_checkpoint.api_account_access) 역할이 있는 ServiceNow 사용자 자격 증명이 필요합니다.

방화벽 관리자가 NOW 플랫폼을 사용하지 않는 경우 NOW Security 인시던트 관리자가 이메일을 통해 필요한 정보를 제공할 수 있습니다. 또는 방화벽 관리자가 NOW Platform을 사용하는 경우 차단 목록과 연결된 변경 요청을 방화벽 관리자에게 할당할 수 있습니다. 이 변경 요청에는 사용자 지정 인텔리전스 피드를 구성하는 데 필요한 정보가 있습니다.

Check Point 게이트웨이에서 사용자 지정 인텔리전스 피드를 설정하는 방법에 대한 자세한 내용은 다음을 참조하십시오. https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193

프로시저

1. 다음으로 이동하여 인스턴스에서 이메일 보내기/받기 기능이 활성화되어 ServiceNow AI Platform 있는지 확인합니다. 이메일 속성 〉 관리 〉 이메일 속성.
2. 아웃바운드 이메일 구성에서 이메일 전송 및 이메일 수신 이 선택되어 있는지 확인합니다.
3. 전문가 모드를 사용하여 SSH를 Check Point Gateway로 수정합니다.
4. 명령을 실행하여 사용자 지정 인텔리전스 피드를 추가합니다.
   명령 실행은 대화형이며 피드 형식과 암호를 묻는 메시지를 표시합니다.
   - 피드 형식을 묻는 메시지가 표시되면 'cp_csv'을 입력합니다.
   - API 접근 권한이 있는 NOW Platform 사용자 암호를 입력하라는 메시지가 표시되면

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

명령 실행은 컴퓨터에서 서버 인증서(NOW Platform)를 신뢰하지 않는 것에 대해 경고하고 컴퓨터의 신뢰할 수 있는 저장소에 서버 보안 인증서를 추가하라는 메시지를 표시합니다. **Y**를 입력합니다.

피드가 성공적으로 추가되었음을 확인하는 "Status:Succeed" 메시지가 나타납니다.

```
[Expert@gw-93440b:0]# ioc_feeds add --feed_name phishing_url --transport https --resource https://<NOW-INSTANCE>.service-now.com/api/x_cdsp_ckpt_tp/
retrieve_block_lists?feed=<feed_id> --user_name <now_ckpt_api_user> --feed_action Prevent
Enter feed format. Should be cp_csv/stix_1.x: cp_csv
Only Check Point's csv format files will be loaded
Enter Password
Password: <now_ckpt_api_password>

Default value for active is: true

Feed Name: phishing_url
Feed is Active
File will be fetched via HTTPS
Resource: https://<NOW-INSTANCE>.service-now.com/api/x_cdsp_ckpt_tp/retrieve_block_lists?feed=<feed_id>
Action: Prevent
User Name: admin

[============================================================] 100.0% ...Getting file from the server
The server security certificate is not trusted by your machine.
SHA256 Fingerprint=SHA256 fingerprint of the NOW instance.

Do you want to trust it for this specific feed?  [y/n]: y
Fetching active feeds

Update summary
##############
feed: phishing_url. Status: Succeed
##############
Activating Scheduler

[Expert@gw-93440b:0]#
```

통합을 위해 **Check Point NGTP** 보안 인시던트의 차단 목록 항목 제출

보안 인시던트 기록에 첨부된 옵저버블은 승인을 위해 다른 차단 목록에 차단 목록 항목으로 제출됩니다. 차단 목록 항목에 대한 선택적 승인 프로세스는 미리 구성된 워크플로우의 일부입니다. 게이트웨이는 차단 목록에 포함된 차단 목록 항목(IP 주소, URL, 도메인)을 가져옵니다.

시작하기 전에
필요한 역할:

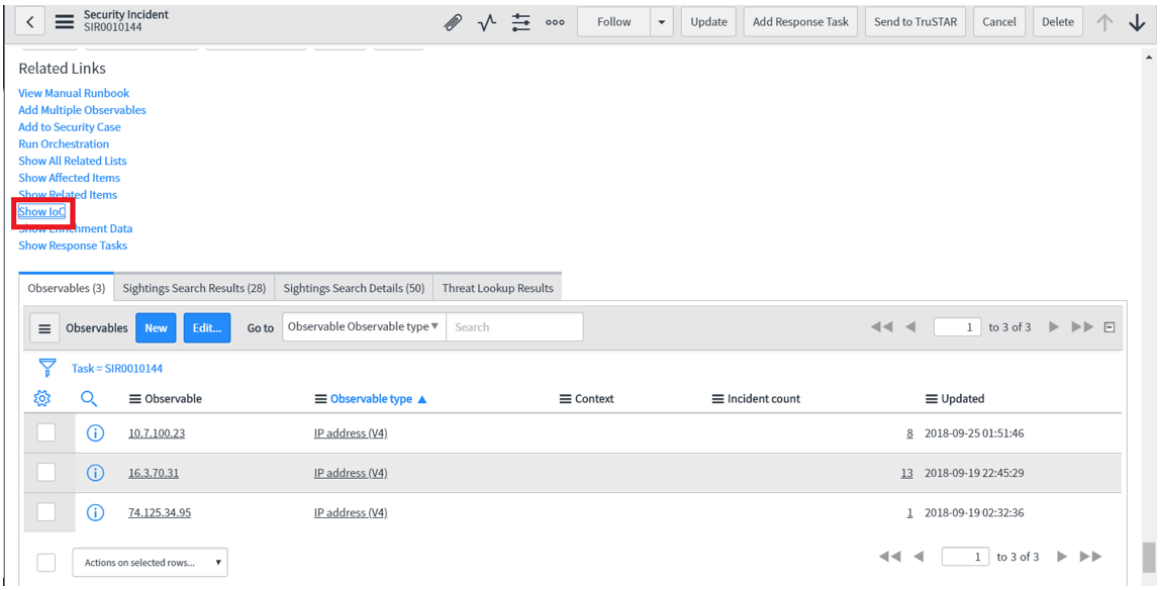
- 차단 목록 항목을 제출하는 보안 인시던트 분석가(sn_si.analyst)
- 차단 목록 항목을 승인하는 보안 인시던트 관리자(sn_si.admin) 이 권한은 조직에서 필요에 따라 할당할 수 있습니다.

이 태스크 정보
sn_si.analyst 역할을 가진 사용자는 보안 인시던트 기록에 첨부된 옵저버블에 대한 차단을 요청하여 블록 항목을 제출합니다. 제출되면 보류 중 상태의 차단 목록 항목이 생성되고 승인을 위해 전송됩니다. 다음 예는 URL 옵저버블에 대한 차단 요청을 보여줍니다.

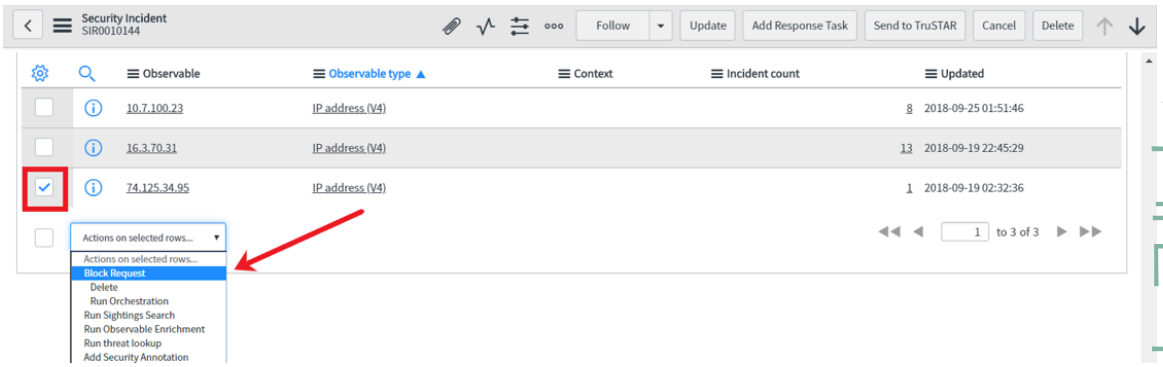
프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 모든 인시던트 표시을 클릭하고 보안 인시던트 기록을 클릭하여 엽니다.
2. **IoC** 표시 관련 링크를 클릭합니다.

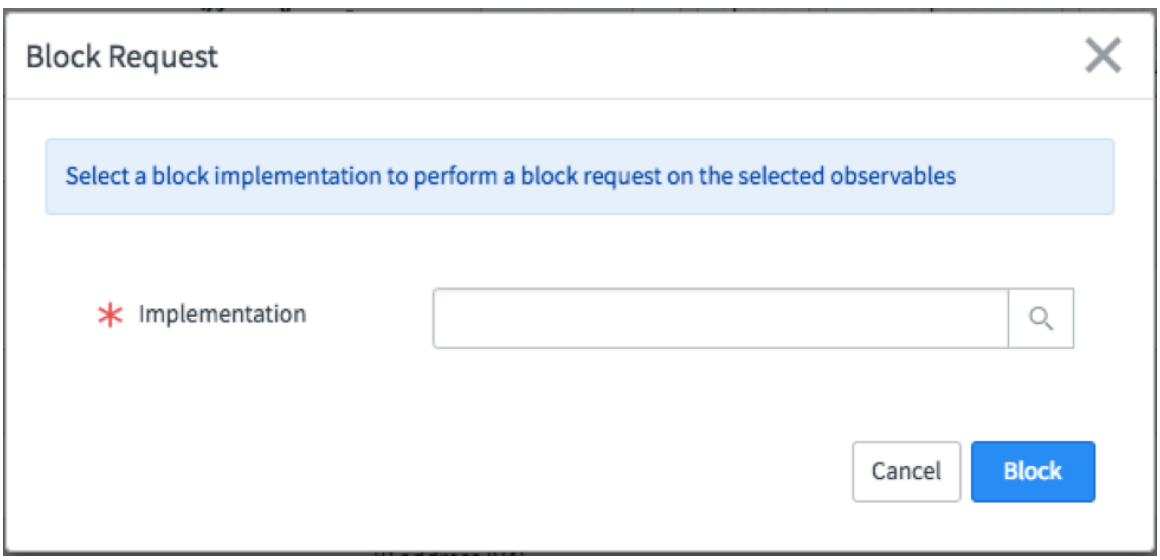
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



3. 옵저버블 관련 목록에서 차단할 옵저버블을 선택하고 선택한 행의 작업 목록에서 차단 요청을 선택합니다.



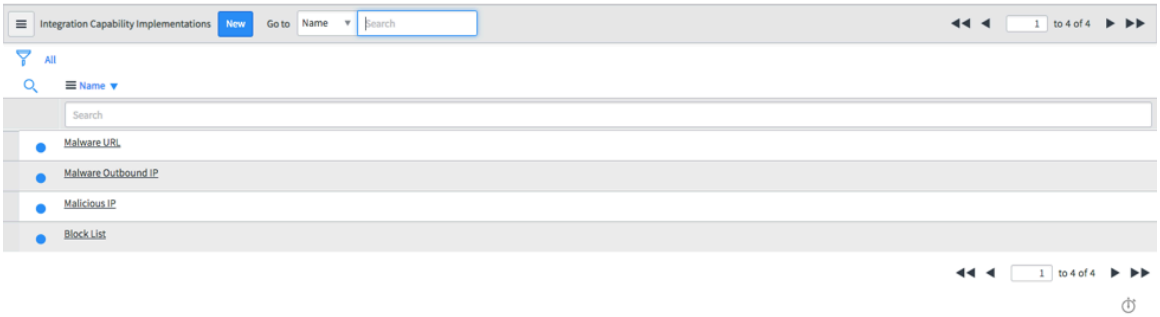
4. 표시되는 대화 상자에서 검색 아이콘(돋)을 클릭합니다



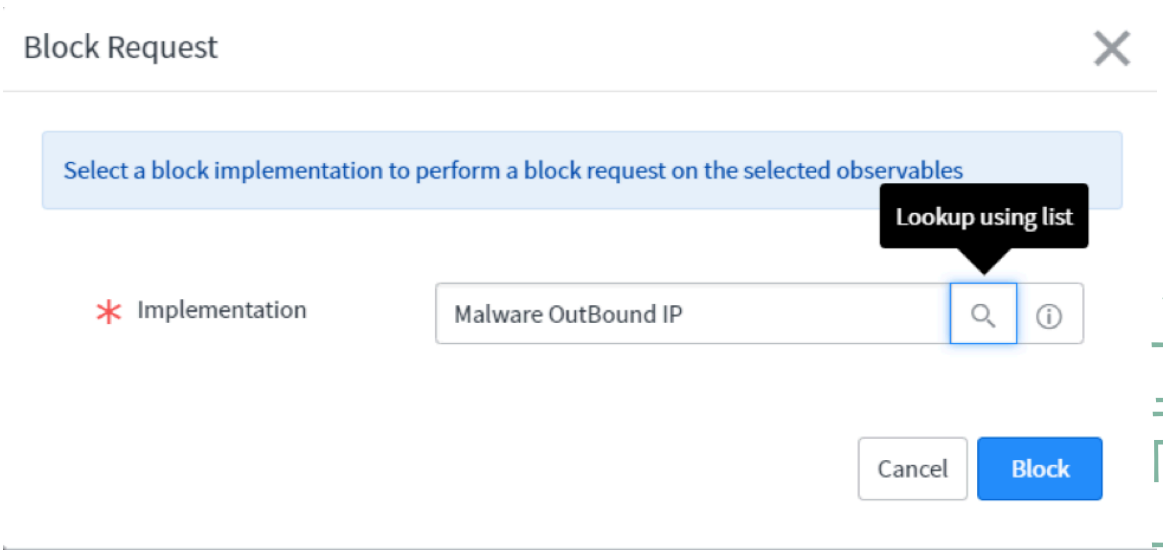
5. 목록에서 이 항목을 연결할 차단 목록을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
이 예에서는 항목 옵저버블 유형(IP)이 차단 목록 옵저버블 유형(IP)과 일치해야 합니다.

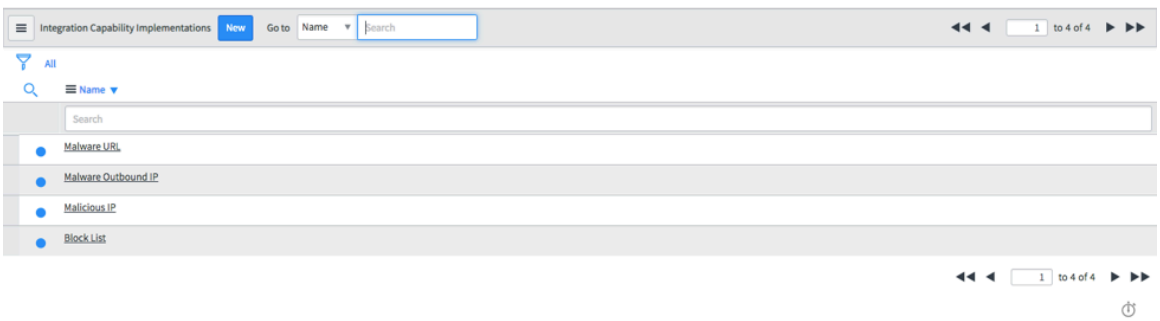


6. 구현 필드에 차단 목록 이름이 표시된 차단 요청 대화 상자에서 차단을 클릭합니다.



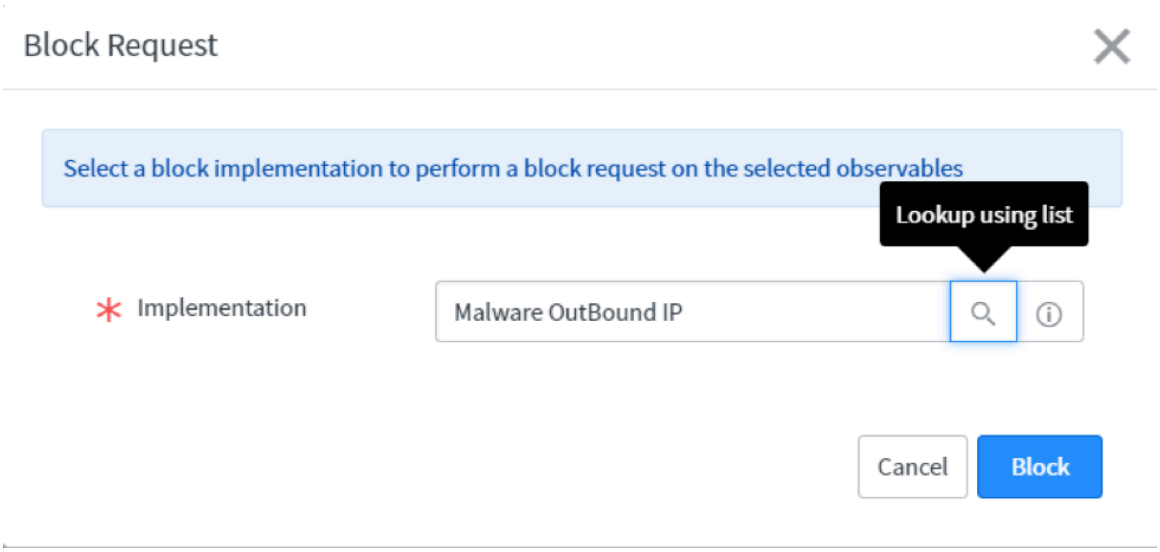
7. 표시되는 목록에서 이 항목을 연결할 차단 목록을 선택합니다.

주:
이 예에서는 항목 옵저버블 유형(IP)이 차단 목록 옵저버블 유형(IP)과 일치해야 합니다.

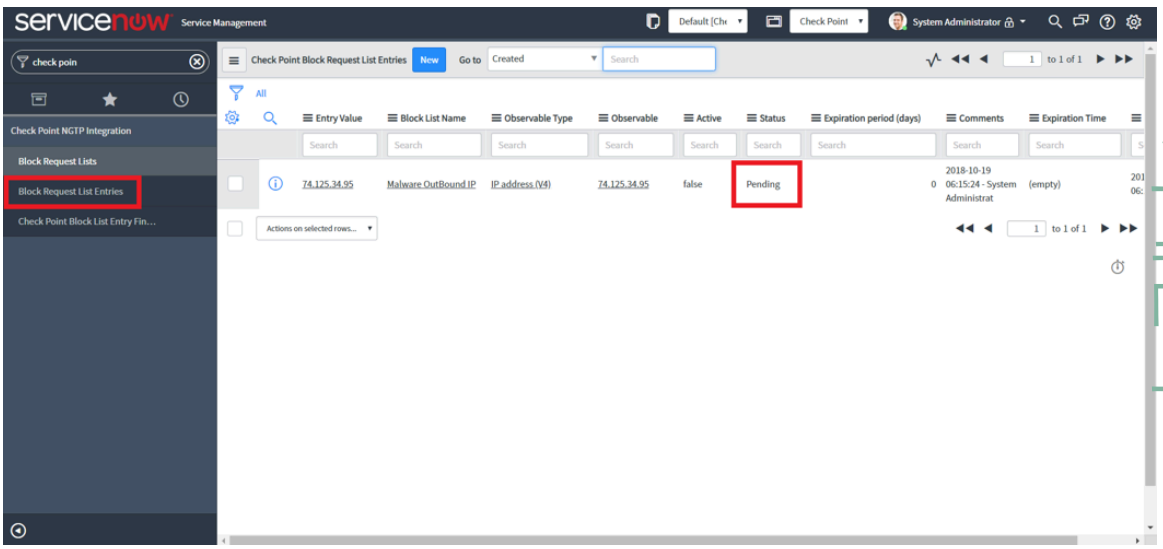


8. 구현 필드에 차단 목록 이름이 표시된 차단 요청 대화 상자에서 차단을 클릭합니다.

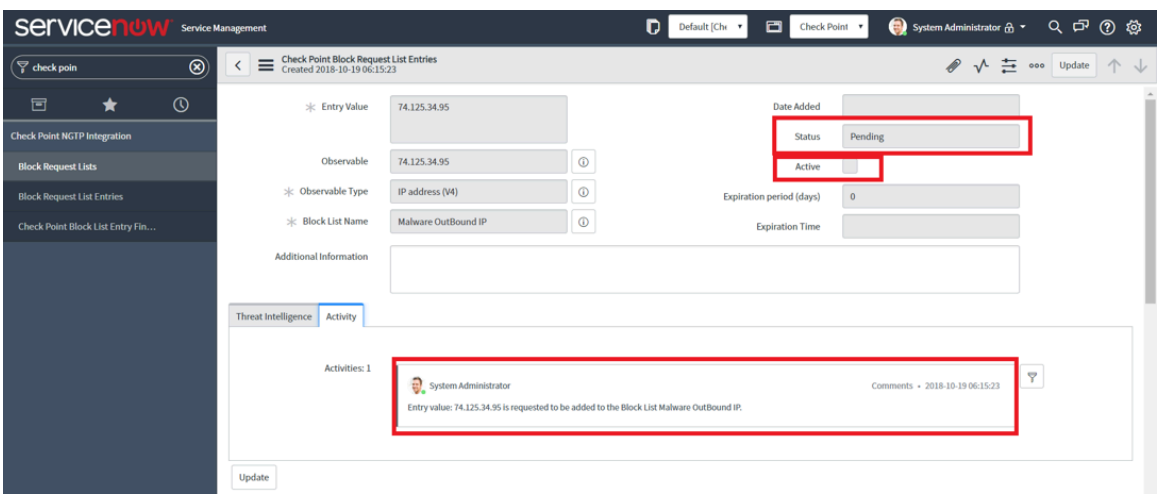
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



9. 다음으로 이동 체크 포인트 **NGTP** 통합 〉 요청 목록 항목 차단을 클릭하고 요청 목록 항목 차단을 클릭합니다.



10. 체크 포인트 차단 요청 목록 항목 목록의 항목 값 열에서 옵저버블을 클릭하여 기록을 엽니다. 이 예에서는 **74.125.34.95** 에 대한 기록이 표시됩니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

상태가 보류 중이고, 활성 확인란의 선택이 취소되어 있으며, 옵저버블 추가 요청이 작업 메모에 표시됩니다. 이 차단 목록 항목 요청이 승인될 준비가 되었습니다.

옵저버블 필드 옆의 아이콘은 옵저버블 테이블에 대한 링크입니다 ServiceNow AI Platform .

옵저버블 필드(74.125.34.95)의 값은 옵저버블 테이블에 연결되며 보안 인시던트 응답 인시던트 트리거 이벤트에서 가져온 형식과 일치합니다.

차단 목록 항목 테이블에서 직접 차단 목록 항목 제출

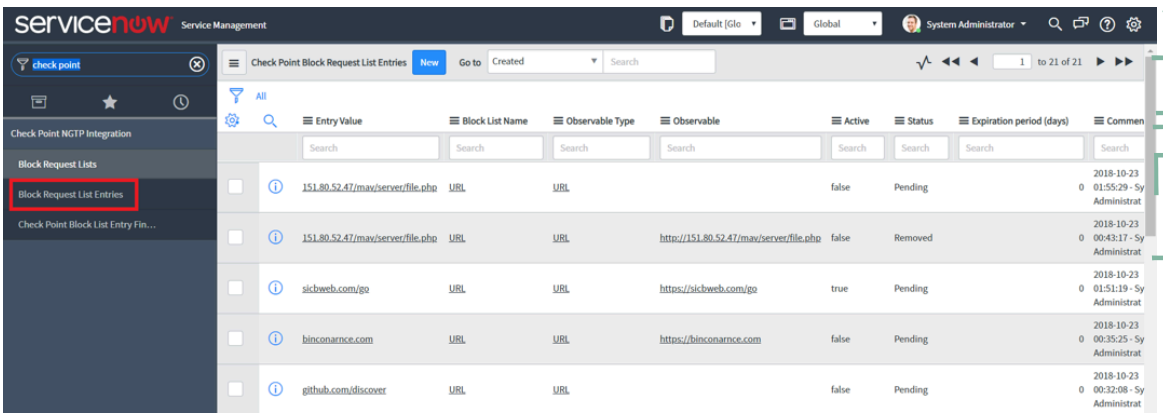
악성으로 판단되고 특정 Now Platform 보안 인시던트와 연결되지 않은 옵저버블의 경우 차단 목록에서 차단 목록 항목을 제출합니다.

시작하기 전에
필요한 역할: 보안 인시던트 관리자(sn_si.analyst)

이 태스크 정보
악성으로 확인된 옵저버블을 차단하거나, 악성이 아닌 옵저버블을 허용하고 옵저버블이 특정 ServiceNow AI Platform 보안 인시던트 기록과 연결되지 않은 경우 차단 목록에서 직접 차단 목록 항목을 제출합니다. 이러한 유형의 차단 목록 항목의 예로는 특정 사이트의 URL 또는 도메인이 있을 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 체크 포인트 **NGTP** 통합 〉 요청 항목 차단.



2. 요청 목록 차단 모듈을 클릭합니다.

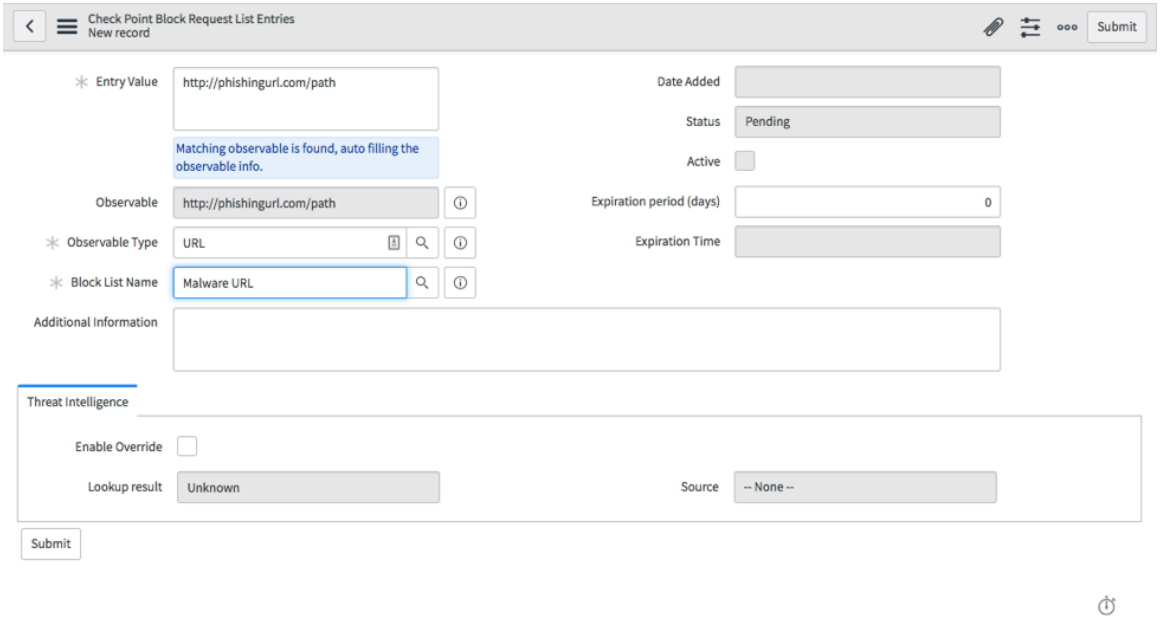
3. 체크 포인트 차단 요청 목록 항목 목록에서 새로 만들기를 클릭합니다.

4. 항목 값 필드에 옵저버블 값을 입력합니다.
이 항목의 두 가지 가능한 결과:

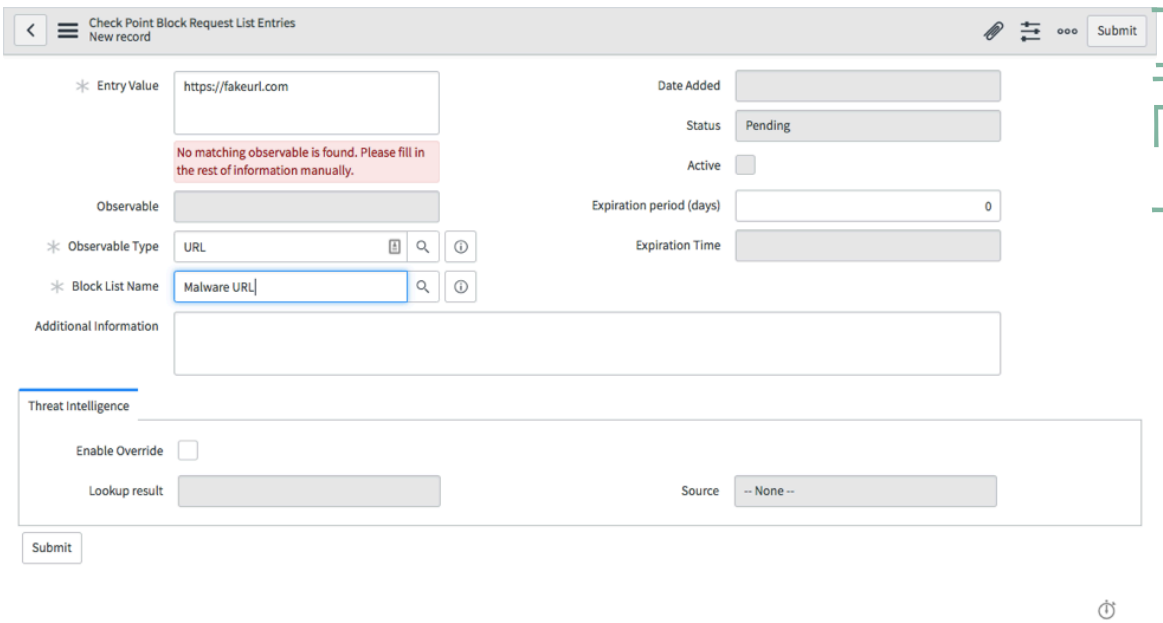
- 양식의 나머지 필드는 자동으로 완성됩니다.
- 일치하는 옵저버블이 발견되고 일치하는 옵저버블이 존재한다는 메시지가 표시됩니다. 이 항목을 첨부할 차단 목록을 선택하고 제출을 클릭합니다. 만료 기간을 설정하기 전에 이 항목을 연결할 차단 목록을 선택합니다.

양식을 작성하라는 메시지가 표시됩니다. 일치하는 옵저버블을 찾을 수 없습니다. 양식을 작성해야 합니다. 완료한 후 옵저버블을 첨부할 차단 목록을 선택하고 제출을 클릭합니다. 옵저버블 기록이 생성됩니다. 다음 그림은 기존 도메인 옵저버블의 예와 필드가 자동으로 완성되는 방법을 보여줍니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



5. 검색 아이콘을 클릭하여 항목을 첨부할 차단 목록을 선택합니다.
6. 제출을 클릭합니다.
7. 워크플로우에 이메일 승인이 구성되어 있으면 승인 이메일 요청이 전송됩니다.
   나머지 정보를 수동으로 입력하도록 요청하는 메시지가 표시되면 필드에 내용을 입력합니다.

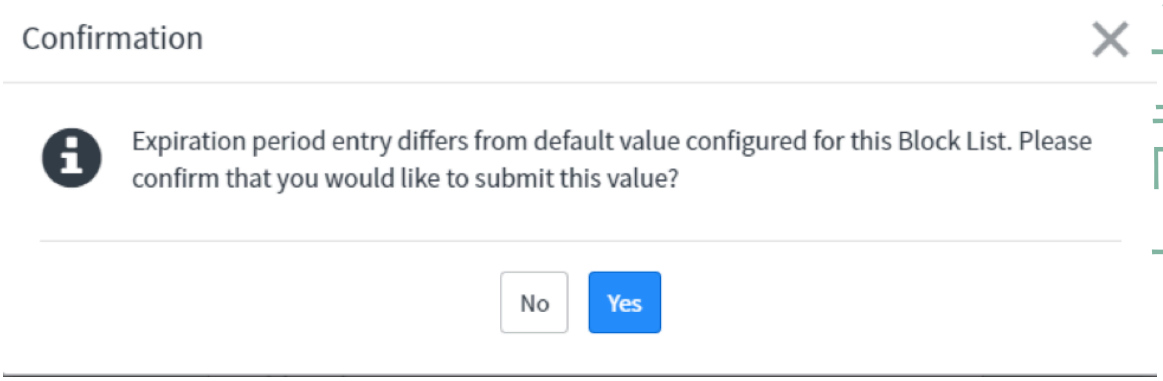


필드	설명
옵저버블 유형	대화 상자에서 지원되는 옵저버블 유형입니다.
차단 목록 이름	항목에 추가할 차단 목록입니다. 주: 만료 기간을 설정하기 전에 항목을 연결할 차단 목록을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
무효화 사용 (기본값이 선택됨)	조회 결과 또는 소스입니다. 구성되면 조회 결과와 결과를 찾는 데 사용되는 소스를 입력할 수 있습니다. 이러한 필드는 일반적으로 보안 인시던트 기록이 생성될 때 채워집니다. 이 경우 조회 결과나 소스가 없으며 이러한 필드를 수동으로 입력합니다.
조회 결과	알 수 없음 또는 악성을 선택합니다.
소스	차단 목록 항목(예: ThreatCrowd 등)에서 위협 조회를 수행하는 소스
만료 기간	기본적으로 차단 목록에서 상속된 만료 기간입니다. 이 값은 재정의할 수 있지만 항목을 생성하는 동안에만 가능합니다. 0은 차단 목록 항목이 만료되지 않음을 나타냅니다. 이 값을 변경하면 입력한 일수 동안 이 항목이 활성화됩니다. 최솟값은 1로 입력할 수 있으며 최댓값은 없습니다. 예를 들어 5월 1일 오후 2:01에 30일을 입력하면 차단 목록 항목은 5월 31일 오후 2:01에 만료됩니다. 그러나 스케줄러는 매일 00:00에 만료된 항목을 확인하고 항목의 상태를 6월 1일 00:00에 '만료됨'으로 변경합니다.

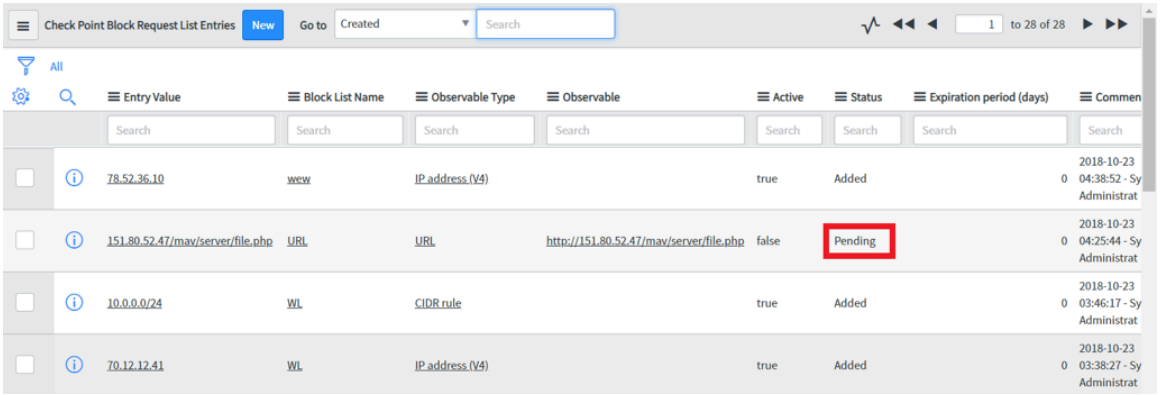
8. 제출을 클릭합니다.
차단 목록 항목의 기본 만료 기간을 변경한 경우 해당 기간이 선택한 차단 목록과 다르다는 경고 확인 대화 상자가 표시됩니다.



옵션	설명
예	만료 재정의를 확인하고 기록을 저장한 후 체크 포인트 차단 목록 항목으로 돌아갑니다. 워크플로우에 이메일 승인이 구성되어 있으면 승인 이메일 요청이 전송됩니다.
아니요	재정의를 취소합니다. 이때 만료 기간의 값을 변경할 수 있습니다. 값을 변경한 후 제출을 클릭하여 체크 포인트 블록 항목 리스트로 돌아갑니다.

9. 표시되지 않으면 체크 포인트 차단 요청 목록 항목으로 이동하여 항목의 상태가 보류 중임을 확인합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



이제 항목을 승인할 준비가 되었습니다.

통합에 **Check Point NGTP** 대한 차단 목록 항목 승인

차단 목록 항목에 대한 승인 프로세스는 미리 구성된 워크플로우의 일부입니다. 차단 목록에서 항목이 활성화되기 전에 차단 목록 항목을 승인합니다. 차단 목록 항목을 승인하면 게이트웨이가 항목을 검색하고 옵저버블은 해당 시점부터 차단됩니다.

시작하기 전에

- 차단 목록 항목에 대한 승인은 기본적으로 보안 인시던트 관리자(sn_si.admin)에게 할당되지만 조직에서 요구하는 경우 이 권한을 할당할 수 있습니다. 다음 예시 ServiceNow AI Platform 에서는 관리자에게 승인 권한이 있습니다.

필요한 역할: sn.si.admin

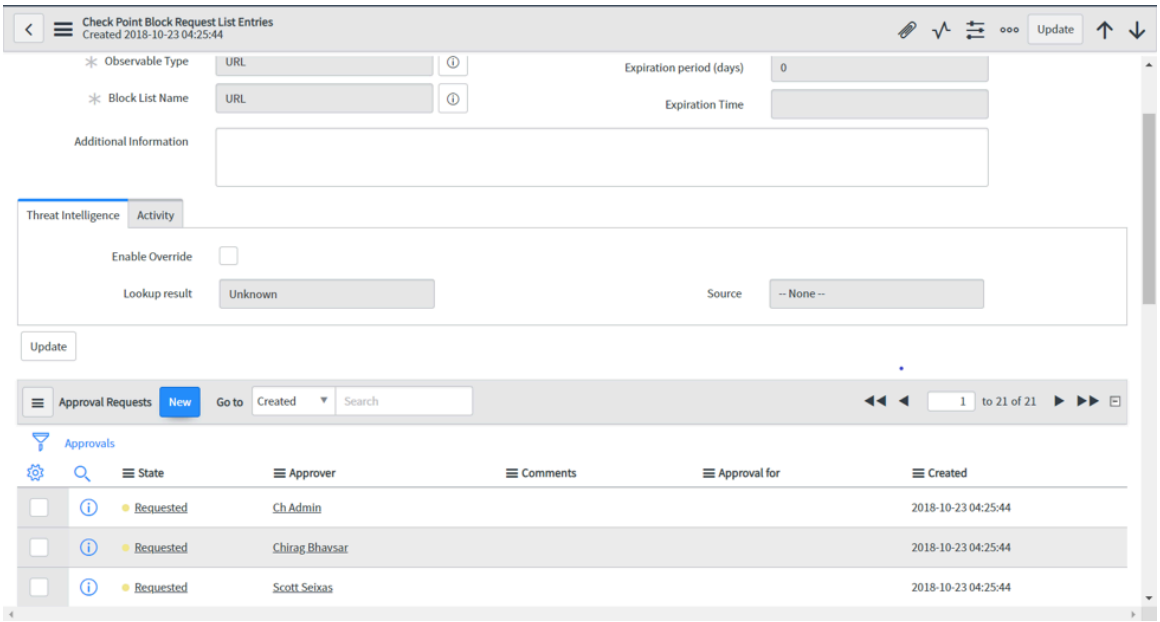
이 태스크 정보

승인 프로세스를 사용하면 승인될 때까지 차단 목록에서 차단 목록 항목이 활성화되거나 비활성화되지 않습니다.

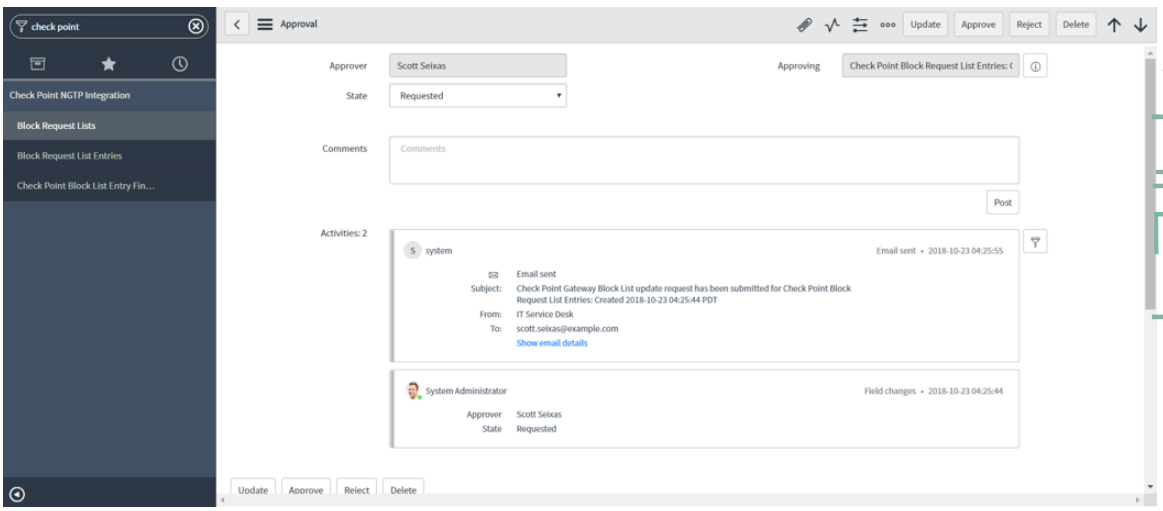
프로시저

1. 다음으로 이동 모두 〉 체크 포인트 **NGTP** 통합 〉 요청 목록 항목 차단을 클릭하고 차단 목록 항목 기록을 엽니다.
2. 차단 목록 항목 기록에서 승인 요청 섹션으로 스크롤합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



3. 승인 요청의 상태 열에서 항목을 클릭하여 엽니다.
승인 기록이 표시됩니다.

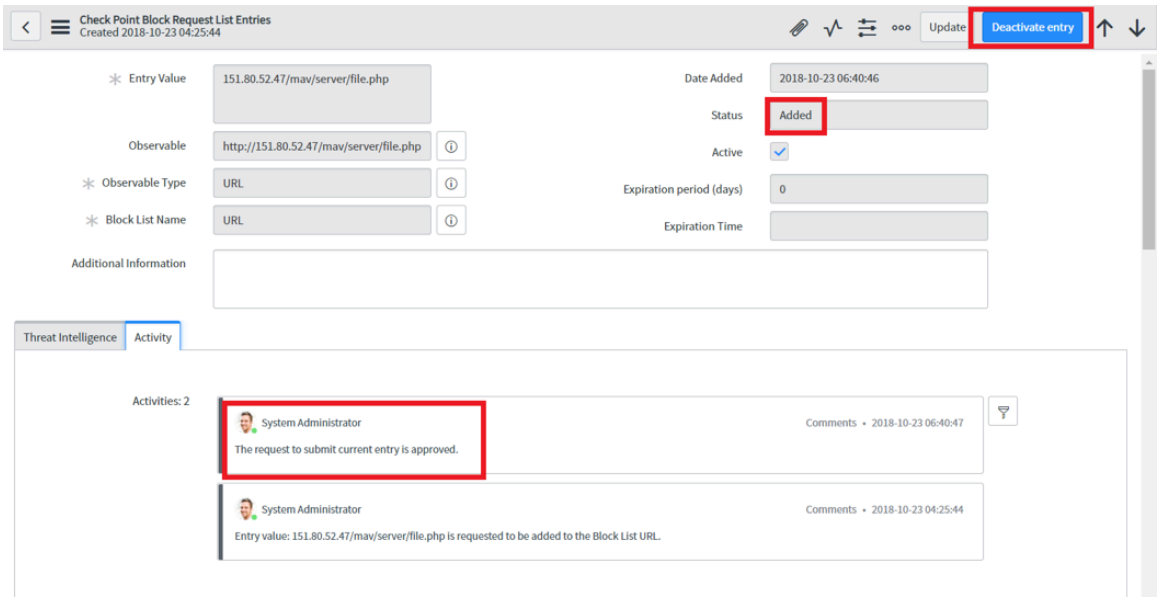


4. 차단 목록 항목을 승인하기 위한 하나의 옵션을 선택합니다.

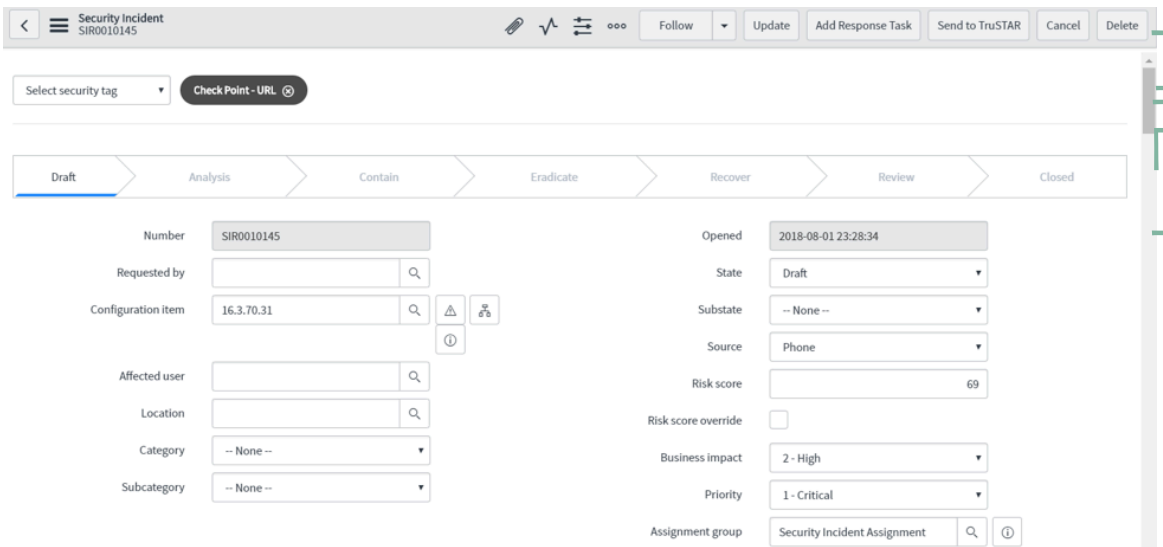
옵션	설명
승인	항목 기록에서 상태 필드가 추가됨으로 변경되고 활성 확인란이 선택됩니다. 비활성화 버튼이 표시되고 활성화됩니다. 작업 메모에 차단 목록 항목에 대한 요청이 승인되었음을 보여 줍니다.
거부	항목 기록에서 상태 필드가 거부됨으로 변경되고 활성 확인란의 선택이 취소되어 게이트웨이에서 항목이 차단되지 않았음을 나타냅니다. 작업 메모에 차단 목록 항목에 대한 요청이 거부되었다고 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

차단 목록 항목을 승인하고 활성화되면 Check Point 차세대 방화벽은 다음 검색 간격 후에 차단 목록 항목을 검색합니다. 항목이 검색되면 해당 시점부터 옵저버블이 차단됩니다. 다음 그림에서는 활성 확인란이 선택되어 있고 상태가 추가됨이며 작업 메모에 요청이 승인되었음을 나타냅니다.

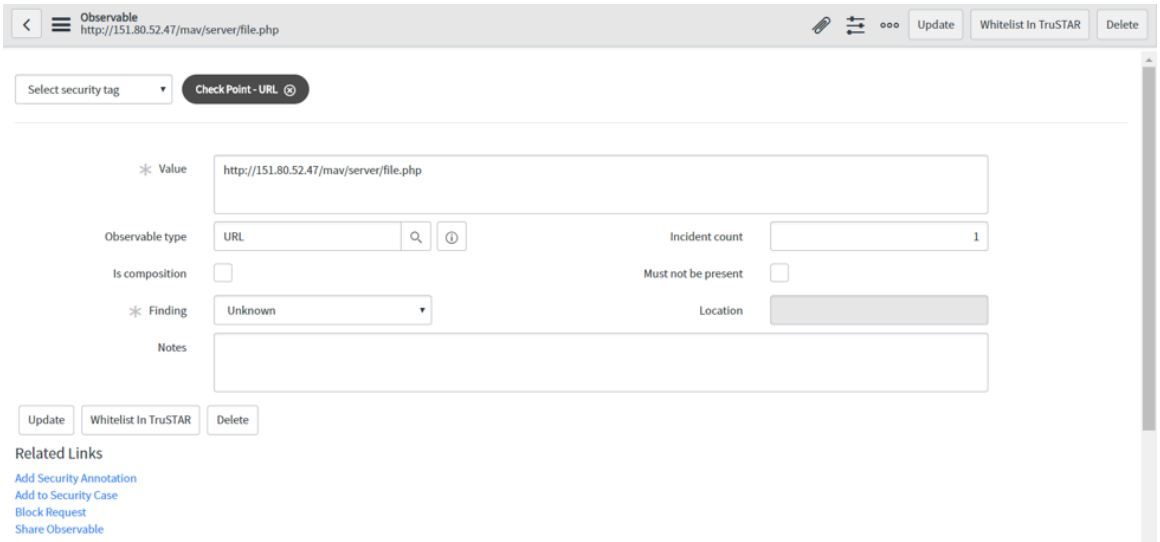


차단 목록 항목이 승인되고 활성화되면 보안 인시던트 기록에 보안 태그가 표시됩니다. 태그가 기록 상단에 표시됩니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 태그는 옵저버블 기록에도 표시됩니다.



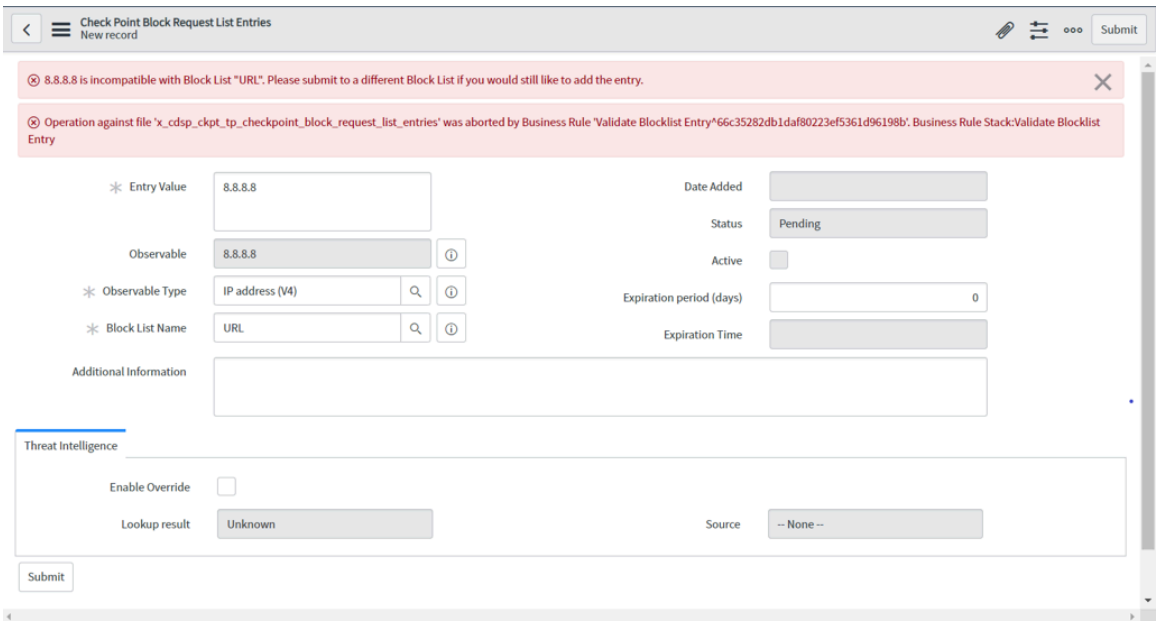
통합에 **Check Point NGTP** 대한 차단 목록 항목 예외

차단 목록 항목을 차단 목록에 추가하는 데는 제한이 있습니다. 차단 목록에 차단 목록 항목을 추가하려고 할 때 중복, 호환성 또는 CIDR(Classless Inter-Domain Routing) 충돌이 발생하는 경우 이러한 오류를 해결하는 데 도움이 되는 오류 메시지가 표시됩니다.

호환성 예외

각 차단 목록은 옵저버블 유형과 호환되는 항목만 허용합니다. 도메인 차단 목록을 생성한 후 옵저버블 IP 주소를 첨부하려고 하면 호환되지 않는 오류 메시지가 표시됩니다. 예를 들어 다음 그림과 같이 도메인 차단 목록은 도메인 옵저버블만 허용할 수 있습니다.

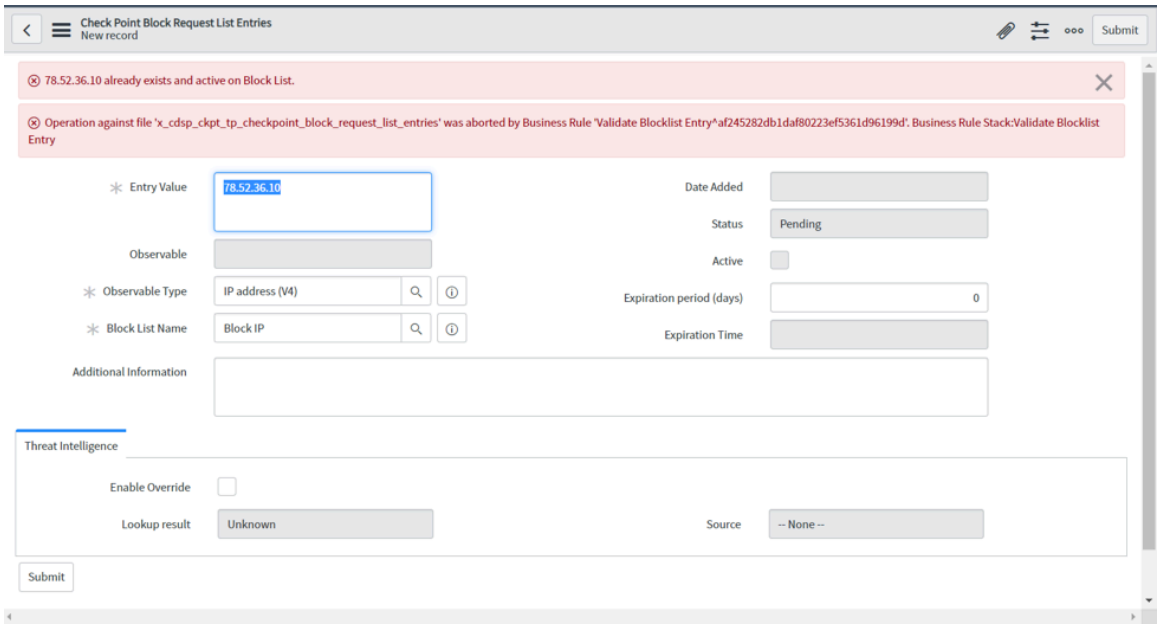
호환성 오류가 있는 차단 목록 양식



중복 예외

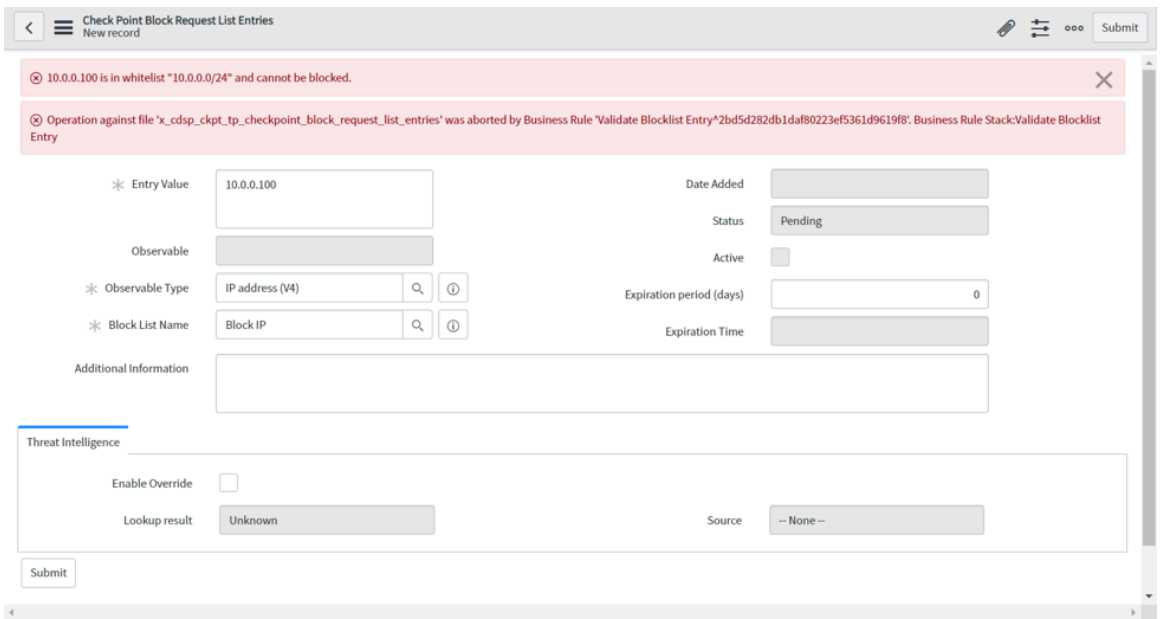
옵저버블 유형은 동일한 옵저버블 유형의 여러 차단 목록에서 옵저버블을 활성화할 수 없습니다. URL 차단 목록에서 URL 옵저버블이 이미 활성화되어 있는 경우 피싱 URL 차단 목록에서 동일한 옵저버블을 활성화하려고 하면 중복 오류 메시지가 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



CIDR(Classless Inter-Domain Routing) 예외

단일 IP 주소를 허용 목록에 연결하려고 할 때 이 IP 주소가 이미 차단 목록/허용 목록에 있는 CIDR 옵저버블의 일부인 경우 CIDR 상충 오류가 표시됩니다. 이 오류는 단일 IP 주소가 CIDR 옵저버블의 일부로 차단 목록 또는 허용 목록에 이미 포함되어 있음을 나타냅니다. 예를 들어, 192.168.24.25은 CIDR 블록 192.168.0.0/22의 일부입니다.



통합에 대한 **Check Point NGTP** 보안 태그 이름 편집

차단 목록 레코드를 만들 때 태그 표시 확인란을 선택하면 보안 태그의 태그 이름과 색상을 편집할 수 있습니다. 보안 태그는 이미 차단된 옵저버블을 추적하는 데 도움이 됩니다.

시작하기 전에
필요한 역할: sn.si.admin

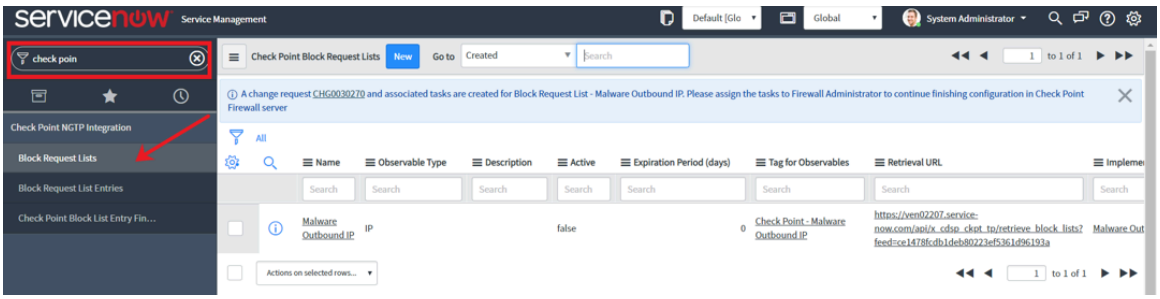
이 태스크 정보
보안 태그를 사용하면 차단 목록에 옵저버블이 있는 보안 인시던트를 빠르게 식별할 수 있습니다. 또한 태그는 옵저버블이 이미 차단되었는지 또는 차단 목록에서 제거되었는지 식별하는 데 도움이

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

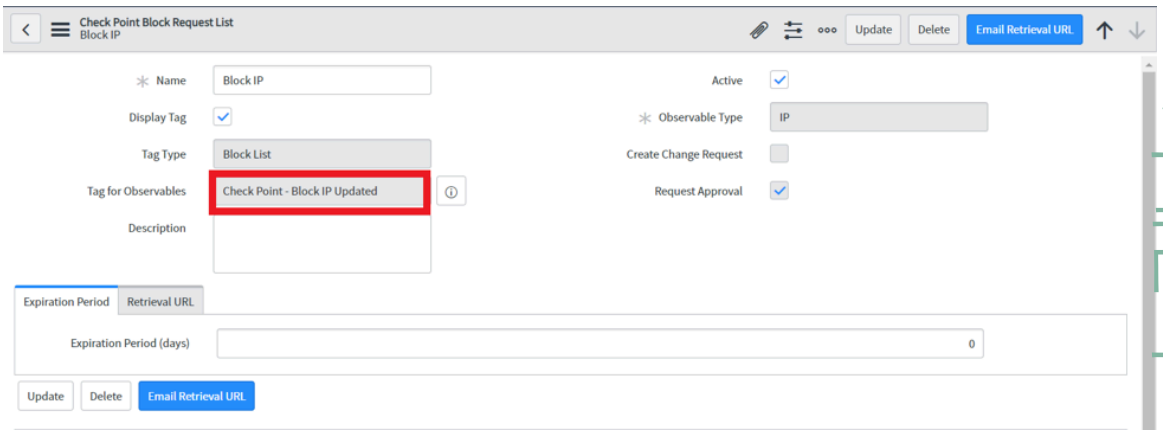
됩니다. 기본적으로 보안 태그의 색은 차단 목록 항목의 경우 검은색이고 허용 목록 항목의 경우 회색입니다. 특정 태그를 더 쉽게 인식할 수 있도록 태그의 이름과 색상을 변경할 수 있습니다.

프로시저

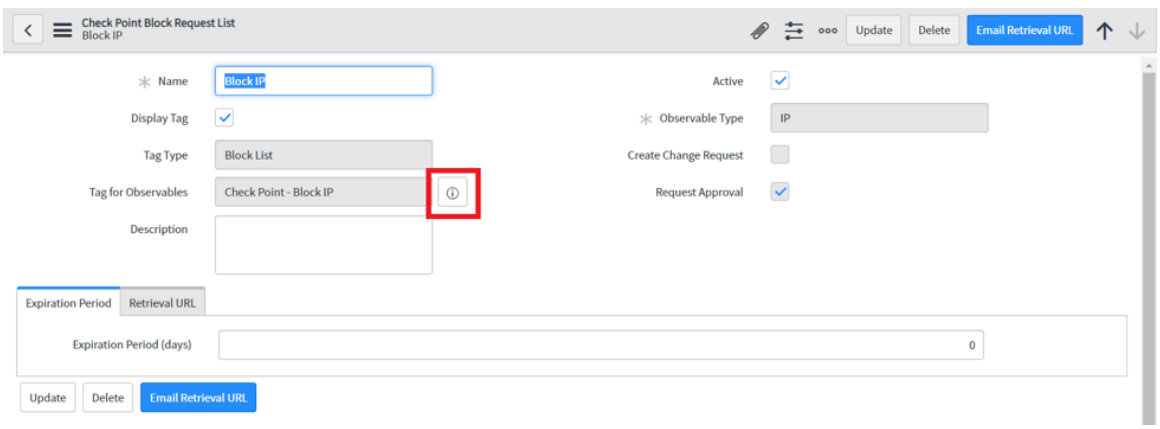
1. 다음으로 이동 모두 〉 체크 포인트 **NGTP** 통합 〉 차단 요청 목록 구성.



2. 이름 열에서 항목을 클릭하여 엽니다.
차단 목록 기록이 표시됩니다. 기본적으로 보안 태그 이름은 차단 목록을 만들 때 이름 필드에 입력한 값과 같습니다. 기본적으로 이름에는 차단 목록 접두사(예: 차단 목록 – 맬웨어 악성 URL)도 포함됩니다.

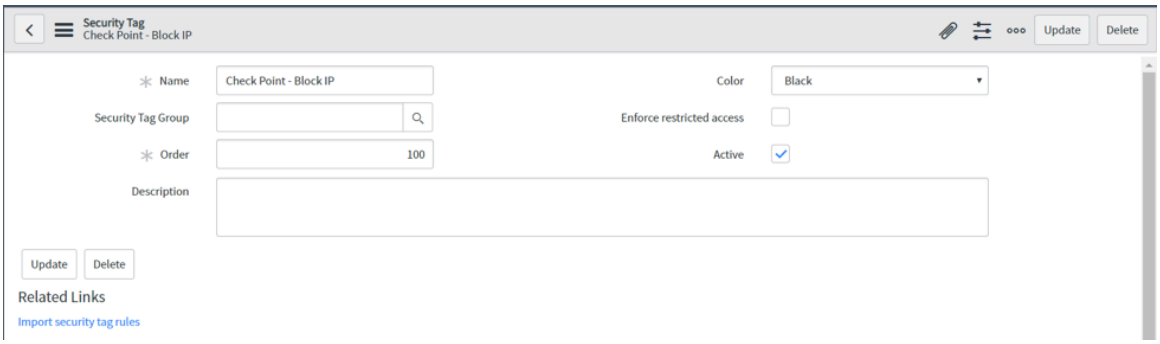


3. 옵저버블 태그 옆에 있는 정보 아이콘을 클릭한 다음 기록 열기를 클릭합니다.



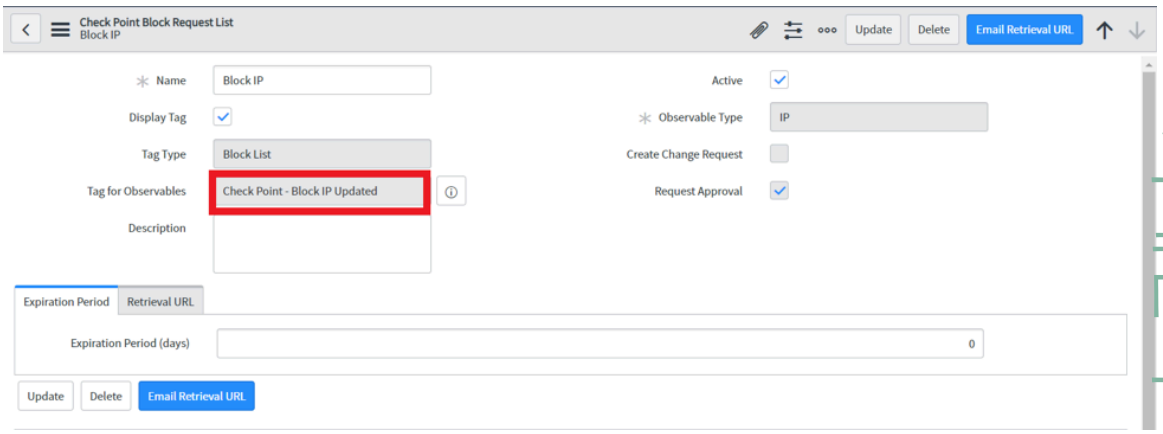
보안 태그 양식이 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 이름 필드에서 보안 태그 이름을 수정합니다.
5. 업데이트를 클릭합니다.
   업데이트된 차단 목록 기록이 수정된 태그 이름으로 표시됩니다.

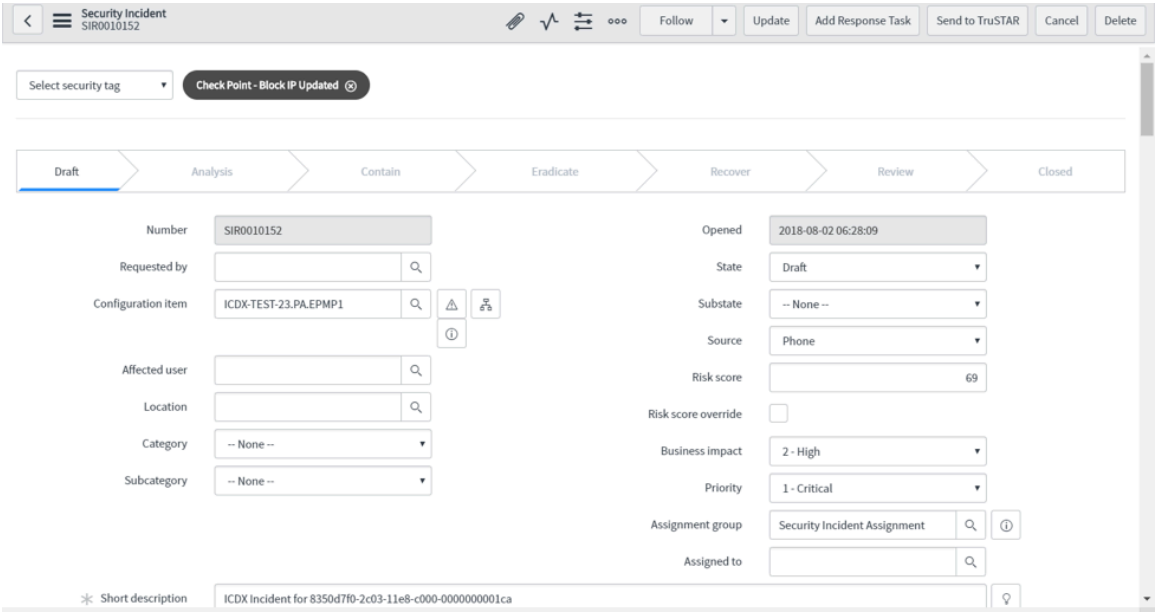
   주:
   다음 예시에서는 아웃바운드가 태그 이름에 추가되었습니다. 새 태그 이름에 Check Point 프리픽스를 유지하면 태그가 Check Point 차세대 방화벽 통합과 연결되어 있는지 식별하는 데 도움이 됩니다.



보안 태그는 옵저버블이 차단 목록에 추가될 때마다 보안 인시던트 기록 및 옵저버블 기록의 각 옵저버블 유형(IP, URL, 도메인)에 대해 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

결과



옵저버블이 차단 목록에 이미 추가되었고 이 옵저버블에 대한 보안 인시던트에 보안 태그가 표시되는 경우 차단 목록 보안 태그도 생성되는 후속 보안 인시던트 기록에 자동으로 표시됩니다. 이 중복은 옵저버블이 이미 차단 목록에 있음을 알려줍니다. 이 옵저버블을 추가하고 다시 차단할 필요가 없습니다.

옵저버블이 더 이상 차단되지 않으면 보안 인시던트 기록 또는 옵저버블 기록에 보안 태그가 표시되지 않습니다. 이 경우 보안 태그가 없으면 옵저버블의 만료 날짜가 지났거나 옵저버블이 차단 목록에서 비활성화되었을 수 있습니다.

통합 제거 **Check Point NGTP**

인스턴스에서 통합을 ServiceNow AI Platform 제거하고 Check Point NGTP 통합에서 나머지 항목을 모두 제거하려면 ServiceNow 설명서 사이트에서 애플리케이션 제거 지침을 참조하십시오.

필요한 역할: admin

CrowdStrike Falcon Host 통합

통합을 CrowdStrike Falcon 호스트 통해 보안 인시던트의 옵저버블을 감시 목록으로 푸시하여 추가 경보를 생성할 수 있습니다. 이 통합은 CrowdStrike Falcon Host - 감시 목록에 게시 워크플로우의 구현입니다.

탐색

보안 인시던트 응답 통합

설정

통합 시작하기 CrowdStrike Falcon 호스트

사용

옵저버블에 대한 조회 수행

개발

- ServiceNow 보안 운영 통합 개발 가이드라인
- 통합 작성을 위한 팁
- 개발자 교육

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 개발자 설명서
- 애플리케이션과 함께 설치되는 구성요소 찾기

문제 해결 및 도움받기

- 통합 문제 해결
- 보안 운영 커뮤니티에서 질문 또는 답변하기
- 알려진 오류 포털에서 알려진 오류 문서 검색

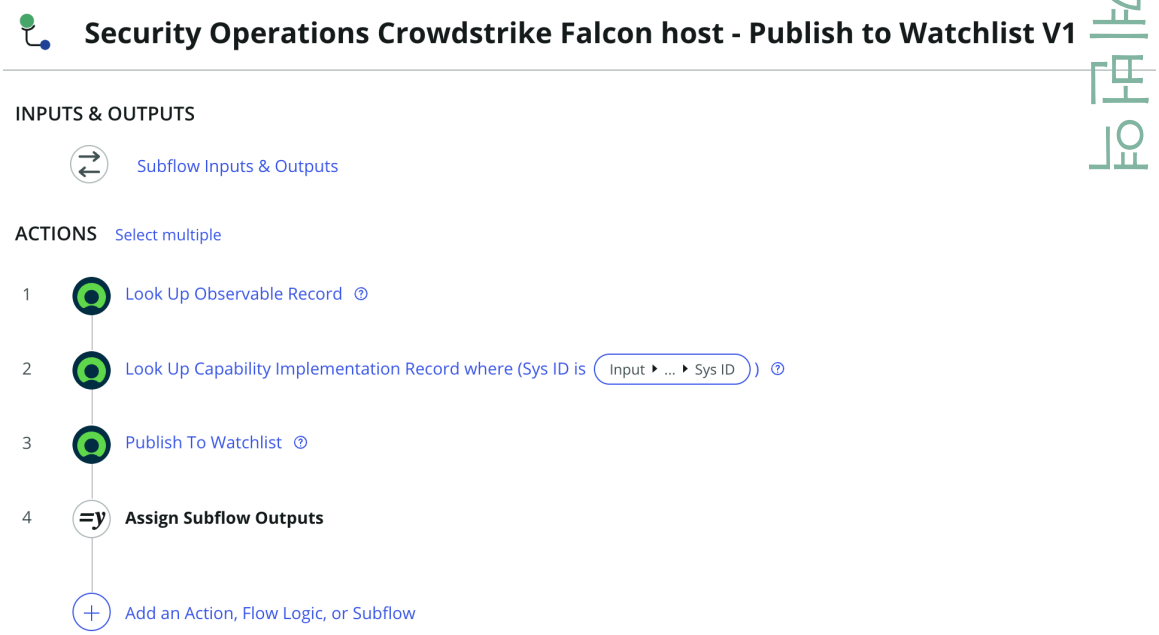
- 연락처 고객 서비스 및 지원

보안 운영 **CrowdStrike Falcon Host -** 감시 목록에 게시 플로우

보안 운영 **CrowdStrike Falcon** 호스트 **-** 감시 목록에 게시 플로우 디자이너는 경보 또는 이벤트 생성을 위한 감시 목록을 지정하는 데 사용됩니다. 경보 및 이벤트는 구성된 방식에 따라 CrowdStrike Falcon Host 시스템에 표시됩니다.

감시 목록에 게시 플로우

이 플로우 디자이너는 보안 인시던트와 연결된 하나 이상의 옵저버블을 선택하고 감시 목록에 게시 UI 작업을 사용하여 옵저버블을 감시 목록으로 푸시할 때 트리거 보안 운영 통합 - 감시 목록에 게시 기능 됩니다. 그런 다음 옵저버블을 사용하여 추가 경보를 생성할 수 있습니다. 자세한 내용은 외부 공급업체 감시 목록에 옵저버블 게시 문서를



참조하십시오.

통합 시작하기 **CrowdStrike Falcon** 호스트

통합 구성 기능을 사용하면 통합을 포함하여 외부 공급업체 보안 통합을 빠르게 활성화하고 설정할 수 있습니다 CrowdStrike Falcon 호스트 . 통합을 사용하려면 CrowdStrike Falcon 호스트 먼저 다음 ServiceNow Store 에서 다운로드한 다음 사용자 이름과 암호를 추가해야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에

- 이전 버전에서 통합을 업그레이드하는 CrowdStrike Falcon 호스트 경우 기존 구성을 삭제하고 새 구성을 설정해야 합니다. 새 통합은 OAUTH2 인증을 지원합니다. 이 업데이트를 수행하려면 **API** 클라이언트 **ID** 와 **API** 클라이언트 암호를 입력하여 인증하고 구성을 완료해야 합니다.
- CrowdStrike Falcon 호스트 포털 **API** 범위에서IOC(침해 표시기)에 대한 읽기 및 쓰기 설정을 활성화합니다.

필요한 역할: sn_si_admin

프로시저

1. 에서 통합을 다운로드합니다. ServiceNow Store.
2. 설치가 완료되면 보안 운영 〉 통합 〉 통합 구성.
   사용 가능한 보안 통합은 일련의 카드로 표시됩니다.
3. CrowdStrike Falcon Host 카드에서 구성을 누릅니다.
4. 양식의 필드에 내용을 입력하여 구성을 완료합니다.

CrowdStrike Falcon 호스트 구성

필드	설명
이름	통합의 이름입니다(예: `demo-1`).
API 클라이언트 **ID**	포털에서 계정 프로파일의 설정 섹션에서 얻은 클라이언트 ID입니다 CrowdStrike Falcon 호스트 .
API 클라이언트 비밀	포털에서 계정 프로파일 CrowdStrike Falcon 호스트 의 설정 섹션에서 가져온 클라이언트 비밀 키입니다.

5. 제출을 클릭합니다.

결과
구성이 완료되면 CrowdStrike Falcon 호스트 의 감시 목록에 보안 인시던트 응답옵저버블을 게시하기 위해 통합을 선택할 수 있습니다.

CrowdStrike Falcon 인사이트 통합

CrowdStrike Falcon 인사이트 for 보안 운영 통합을 사용하면 엔드포인트에서 실시간으로 정정 작업을 수행하고, 프로파일을 사용하여 호스트에 대한 세부 정보를 수집하고, 제품을 사용하여 엔드포인트에서 특정 쿼리 또는 작업을 수행할 수 있습니다ServiceNow AI Platform 보안 인시던트 응답.

스토어에서 앱 요청

ServiceNow Store 웹 사이트를 방문하면 사용 가능한 모든 앱을 확인하고 스토어에 요청을 제출하는 방법에 대한 정보를 참조할 수 있습니다. 출시된 모든 앱의 누적 릴리스 정보는 ServiceNow Store 버전 기록 릴리스 정보 를 참조하십시오.

for 보안 운영 통합은 CrowdStrike Falcon 인사이트 인시던트 범위에 대한 추가 인사이트를 얻을 수 있도록 와 ServiceNow AI Platform 함께 작동합니다. 는 CrowdStrike Falcon 인사이트 모든 관련

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

엔드포인트 이벤트 활동을 캡처하므로 조사 및 정정 작업에 집중할 수 ServiceNow AI Platform 있습니다.

이 통합에 대해 알아보기

문서 식별자	문서 제목
ServiceNow 제품 설명서 웹 사이트	ServiceNow 제품 설명서 웹 사이트
보안 운영에 대한 CrowdStrike Falcon 인사이트	통합 시작하기 CrowdStrike Falcon 인사이트

통합 시작하기 **CrowdStrike Falcon** 인사이트

인스턴스 CrowdStrike Falcon 인사이트 및 보안 인시던트 응답 제품과 인터페이스하도록 활성화하고 설정할 수 있습니다ServiceNow AI Platform.

필요한 역할: 관리자

통합에 보안 운영 사용하려면 CrowdStrike Falcon 인사이트 먼저 에서 ServiceNow Store다운로드해야 합니다.

검사 목록

설정 작업	설명
필수 ServiceNow AI Platform 및 보안 인시던트 응답 역할을 할당하고 확인합니다.	다음 역할은 예상 결과를 구성하고 검증하는 데 필요합니다. • 관리자 역할은 에서 ServiceNow Store 통합을 설치하고 sn_si.admin 역할을 할당합니다. • sn_si.admin 역할은 통합을 구성하고 프로파일을 생성 및 활성화한 다음 sn_si.analyst 역할을 할당합니다. • sn_si.analyst 역할은 보안 인시던트에 대응하고, 프로파일을 수동으로 실행하며, 승인된 그룹에 대한 호스트 격리 및 호스트 격리 제거와 같은 작업에 대한 요청을 제출할 수 있습니다.
ServiceNow 이 통합을 구성하기 전에 통합을 지원하는 데 필요한 핵심 애플리케이션이 설치되고 활성화되었는지 확인합니다.	ServiceNow 통합 허브 엔터프라이즈 팩 설치 관리자 [com.glide.hub.integrations.enterprise] 플러그인이 필요합니다. 이 플러그인을 사용하면 통합 허브 작업 및 플로우를 실행할 수 있습니다. 플러그인(com.snc.security_incident)이 보안 인시던트 응답 필요합니다. 이 플러그인은 제품을 지원하는 데 필요한 모든 종속성을 보안 인시던트 응답 자동으로 설치합니다. 통합에 필요한 다른 보안 운영 애플리케이션을 설치하고 활성화하기 전에 이 플러그인을 설치하고 활성화합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

검사 목록

설정 작업	설명
	에서 ServiceNow Store다음 보안 운영 애플리케이션이 설치되고 활성화되는지 확인합니다. 이러한 애플리케이션이 아직 설치되어 있지 않은 경우 원활한 설치를 위해 다음 순서대로 각 애플리케이션을 한 번에 하나씩 설치하고 활성화해야 합니다. **1.** 보안 인시던트 응답 의존성(com.snc.si_dep) **2.** 보안 통합 프레임워크 **3.** Security Support Common **4.** 보안 지원 오케스트레이션 **5.** 위협 인텔리전스 공통 지원 **6.** Trusted Security Circles **7.** 보안 운영 설정 도우미 **8.** 보안 인시던트 응답
승인 그룹을 설정합니다.	선택적 승인 기능은 호스트 시스템을 격리하고, 네트워크에 복원하고, 사이팅 검색을 시작하는 데 사용할 수 있습니다. 이 옵션을 사용하려면 호스트 컴퓨터를 격리하고 네트워크에 복원하기 전에 또는 사이팅 검색을 수행할 때 sn_si.admin 역할의 사전 승인이 필요합니다. 이러한 작업에 대한 추가 제어 수준이 필요한 경우 프로파일을 구성할 때 승인 필요 옵션을 활성화합니다. 승인 권한은 sn_si.admin 역할을 가진 사용자에게 할당됩니다. 이 승인 권한을 승인 그룹에 재할당할 수도 있습니다.
CrowdStrike Falcon Platform 역할을 할당하고 확인합니다.	통합 구성을 위해 CrowdStrike Falcon 플랫폼에서 필요한 역할은 다음과 같습니다. • API 클라이언트 또는 키를 보거나 생성하거나 수정하려면 Falcon 관리자 역할이 필요합니다. • 사용자 지정 스크립트를 만들고 실행하려면 실시간 응답자 - 관리자 역할이 필요합니다. • 사용자 지정 스크립트를 작성하고 실행하려면 실시간 응답자 - 능동 응답자 역할이 필요합니다.
사용자 지정 스크립트, 역할 및 권한이 CrowdStrike Falcon 플랫폼에서 활성화되어 있는지 확인합니다.	이 통합은 몇 가지 보강 기능에 대해 CrowdStrike의 사용자 지정 스크립트를 사용합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

검사 목록

설정 작업	설명
	• 실시간 응답자 - 관리자 및 실시간 응답자 - 능동 응답자 역할을 사용할 수 있는지 확인합니다. • CrowdStrike Falcon UI의 구성 > 응답 정책에서 기본**(Windows)** 정책 옵션이 활성화되어 있는지 확인합니다. • 실시간 기능 아래의 실시간 응답 및 사용자 지정 스크립트가 CrowdStrike Falcon UI에서 활성화되어 있는지 확인합니다.
CrowdStrike Falcon 플랫폼에서 API 클라이언트 및 키를 생성합니다.	통합 구성에 사용할 ServiceNow AI Platform CrowdStrike Falcon 플랫폼에서 CrowdStrike API 클라이언트 또는 키를 생성합니다.

CrowdStrike API 클라이언트 생성 및 키 생성

CrowdStrike API 클라이언트를 만들고 통합을 구성하는 CrowdStrike Falcon 인사이트 데 사용하는 클라이언트 ID 및 키를 생성합니다.

시작하기 전에
필요한 역할: CrowdStrike Falcon 관리자

프로시저

1. CrowdStrike Falcon 플랫폼에서 **API** 클라이언트 및 키로 이동합니다.
2. OAuth2 API 클라이언트 테이블에서 새 **API** 클라이언트 추가를 클릭하십시오.
3. 다음 상세 정보를 입력하여 API 클라이언트를 정의합니다.

필드	설명
클라이언트 이름	클라이언트 이름을 입력합니다. 이 필드는 필수입니다.
설명	클라이언트 이름에 대한 설명을 입력합니다.
API 범위	범위를 정의해야 합니다. **중요사항:** API 계정을 활성화하고 API 계정에 대해 다음 범위가 활성화되어 있는지 확인합니다. ○ 호스트 API에 대한 읽기 및 쓰기 범위 사용 ○ 표시기 API에 대한 읽기 범위 사용

4. 추가를 클릭하여 API 클라이언트를 저장하고 클라이언트 ID 및 비밀 키를 생성합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

CrowdStrike Falcon 인사이트 설치 및 구성

인스턴스에서 용 보안 운영 애플리케이션을 ServiceNow StoreServiceNow AI Platform 설치하고 구성합니다CrowdStrike Falcon 인사이트.

시작하기 전에

필요한 역할: 관리자

> **주:**
> 역량은 하나의 프로파일에만 연결할 수 있습니다. 역량을 여러 프로파일과 연결할 수 없습니다. CrowdStrike 서버를 구성할 때 CrowdStrike 서버를 공유하는 여러 프로파일에서 CrowdStrike 기능을 재사용할 수 없습니다. 프로파일은 동일한 CrowdStrike 기능을 가질 수 있으며, 각 프로파일은 자체 CrowdStrike 서버를 사용해야 합니다.

프로시저

1. CrowdStrike Falcon 인사이트 에서 ServiceNow Store for Security Operations 통합을 다운로드하고 설치합니다.
2. 다음으로 이동 보안 운영 〉 통합 〉 통합 구성.
3. 통합 타일을 CrowdStrike Falcon 인사이트 검색하고 구성을 클릭합니다.보안 운영
4. 양식의 필드에 내용을 입력하여 구성을 완료합니다.

CrowdStrike Falcon Insight 구성

필드	설명
이름	통합의 이름입니다(예: `demo-1`).
CrowdStrike Falcon Insight API URL	CrowdStrike API를 호스팅하는 기본 URL입니다. HTTPS 프로토콜로 URL을 입력합니다. 예를 들어 https://api.crowdstrike.com.
클라이언트 ID	포털에 있는 계정 프로파일의 설정 섹션에서 얻은 클라이언트 ID입니다 CrowdStrike Falcon 인사이트 .
클라이언트 비밀	포털에 있는 계정 프로파일의 설정 섹션에서 가져온 클라이언트 비밀 키입니다 CrowdStrike Falcon 인사이트 .

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. 제출을 클릭합니다.

결과
통합이 성공적으로 확인되고 제출되면 보안 통합 페이지에 타일로 저장됩니다. 애플리케이션 네비게이터에서 모듈을 볼 CrowdStrike Falcon 인사이트 수 있습니다.

승인 그룹 생성

호스트 컴퓨터를 격리하고 네트워크로 복원하며 사이팅 검색을 시작하기 위한 요청을 승인할 수 있는 통합용 보안 운영 승인 그룹을 CrowdStrike Falcon 인사이트 생성합니다.

시작하기 전에
인스턴스에서 승인 그룹을 사용할 수 없는 경우 그룹에 승인 권한을 재할당할 수 없습니다.

> **주:**
> 프로파일 구성의 승인 옵션은 호스트 격리 및 호스트 격리 제거 기능에만 표시됩니다.

필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 〉 사용자 관리 〉 그룹.

2. 그룹 목록에서 새로 만들기를 클릭합니다.

3. 양식에서 필드를 채웁니다.

승인 그룹 양식

필드	설명
이름	승인 요청을 제출할 때 표시되는 그룹의 이름입니다.
그룹 이메일	그룹 관리자와 같은 접촉 창구의 이메일 주소 또는 그룹 이메일 배포 목록입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
관리자	그룹 관리자의 이름입니다. 검색 아이콘을 클릭하여 목록을 봅니다.
상위	상위와 연결된 경우 상위 그룹의 이름입니다.
유형	그룹의 범주입니다.
벤더	조직의 벤더 관리 프로세스에서 사용자에게 할당하는 vendor_manager 역할입니다.
설명	그룹에 대한 추가 정보입니다.

4. 제출을 클릭합니다.
   새 그룹이 그룹 목록에 표시됩니다.

   이 그룹은 이 프로파일을 구성하는 동안 승인 필요 옵션을 활성화하면 요청을 처리할 수 있습니다.

   sn_si.analyst 역할을 가진 사용자가 제출한 요청을 모니터링하고 처리하기 위해 승인 그룹의 각 구성원은 의 ServiceNow AI Platform내 승인 탭으로 이동합니다.

다음에 수행할 작업
다음 단계는 ServiceNow Store에서 CrowdStrike Falcon 인사이트 애플리케이션을 설치하고 구성하는 것입니다.

통합에 **CrowdStrike Falcon** 인사이트 대한 역량 프로파일 생성

프로파일을 생성하고 프로파일을 실행할 기능을 선택합니다 CrowdStrike Falcon 인사이트 .

시작하기 전에
필요한 역할: sn_si.admin

이 태스크 정보
프로파일에 역량을 추가하기 CrowdStrike Falcon 인사이트 전에 프로파일을 생성하려는 이유를 고려하십시오. 다음 표에는 프로필에서 특정 쿼리 또는 작업을 수행하려는 경우 프로필에 추가해야 하는 기능이 나와 있습니다.

시스템 상세 정보에 대한 쿼리를 실행하고, 로그인한 사용자를 나열하고, 실행 중인 서비스를 가져오고, 실행 중인 프로세스를 가져오고, 네트워크 통계를 가져오고, 호스트를 격리하고, 격리된 호스트를 제거하는 단일 프로파일을 만들 수 있습니다. 또는 각각 고유한 단일 기능을 가진 여러 프로필을 만들 수 있습니다.

주:
호스트 격리, 격리 제거 및 파일 가져오기 역량은 프로파일을 생성하는 동안 다른 역량과 병합할 수 없습니다.

프로파일 유형 및 필수 **CrowdStrike Falcon Insight** 역량

프로파일 목적	**CrowdStrike** 역량
호스트 상세 정보 및 로그인한 사용자 수집	• 호스트 상세 정보 가져오기 • 로그온한 사용자 가져오기

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로파일 유형 및 필수 **CrowdStrike Falcon Insight** 역량

프로파일 목적	**CrowdStrike** 역량
호스트에 대해 실행 중인 네트워크 통계, 프로세스 및 서비스 가져오기	• 네트워크 통계 임포트 • 실행 중인 프로세스 임포트 • 실행 중인 서비스 가져오기
호스트 격리	호스트 분리
호스트에 대한 격리 제거	격리 제거
호스트 엔드포인트에서 파일 가져오기	파일 가져오기

프로시저

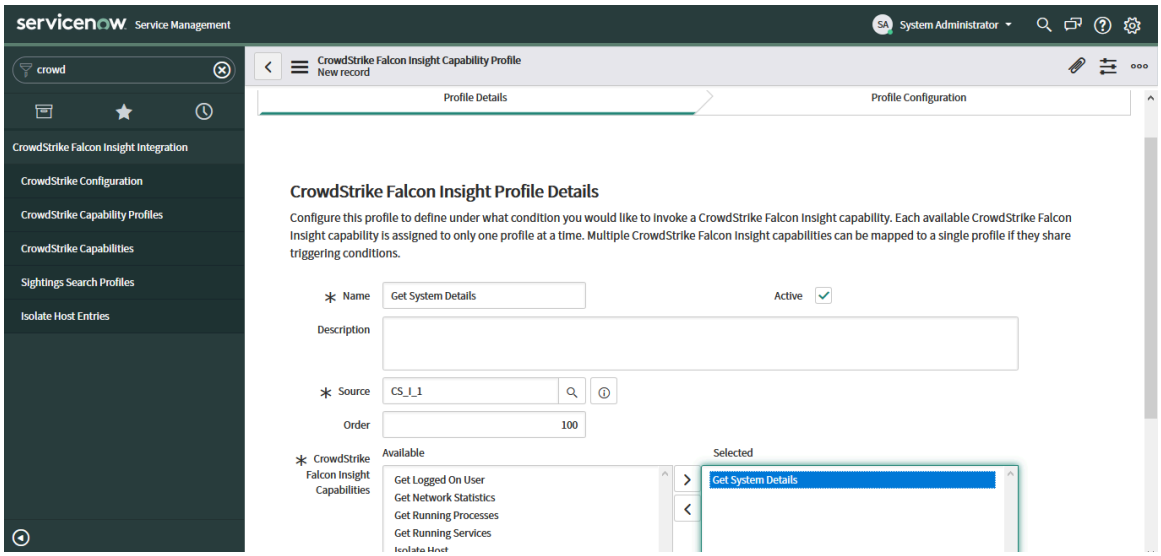
1. 다음으로 이동 모두 〉 **CrowdStrike Falcon Insight** 통합 〉 **CrowdStrike** 역량 프로파일.
2. 새로 만들기를 클릭합니다.
3. 양식의 필드에 내용을 입력합니다.

필드	설명
이름	새 역량 프로파일의 이름입니다. 이 이름은 프로파일 유형을 식별하는 데 도움이 되며 이 프로파일과 연결된 보안 태그의 기본 이름이기도 합니다.
활성	프로파일이 활성 상태인지 여부를 나타냅니다. 프로파일이 활성 상태이면 구성에 지정한 필터링 조건과 일치하는 보안 인시던트가 생성되면 프로파일이 자동으로 트리거됩니다.
설명	역량 프로파일에 대한 고유 설명입니다.
소스	서버 이름입니다. 목록에서 이전에 구성된 서버만 볼 수 있습니다.
순서	플로우 우선순위입니다. 이 필드의 값은 둘 이상의 프로파일이 트리거 조건을 공유할 때 플로우가 실행되는 순서를 나타냅니다. 숫자가 가장 낮은 플로우의 우선순위가 가장 높습니다. 작업 순서를 설정하려면 값을 입력합니다. 예를 들어 100, 200, 300, 400입니다. 기본값: 100
CrowdStrike Falcon Insight 역량	CrowdStrike Falcon Insight 프로파일의 기능입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	사용 가능 열에서 선택됨열에 이 프로파일에 대해 원하는 기능을 선택합니다.

다음 예제에서는 시스템 세부 정보 가져오기 기능이 있는 프로필에 대한 전체 양식을 보여 줍니다.



4. 다음을 클릭합니다.

다음에 수행할 작업

이제프로필을 구성할 수 있습니다. 프로파일을 구성하기 전에 프로파일 및 트리거 조건 구성에 대한 개념을 검토 해야 합니다.

통합에 **CrowdStrike Falcon** 인사이트 대한 프로파일 및 보안 인시던트 구성

설정한 조건에서만 프로파일이 트리거되도록 프로파일 설정을 구성합니다.

시작하기 전에

필요한 역할: sn_si.admin

이 태스크 정보

프로파일에 대해 선택한 기능을 자동으로 트리거 CrowdStrike Falcon 인사이트 하는 조건을 정의합니다. CI(구성 항목) 필드에 대해 대체 입력 필드를 선택할 수도 있습니다. 이 대체 필드에서는 트리거 이벤트와 관련된 보안 인시던트만 프로파일을 자동으로 트리거하도록 필터링 조건을 설정할 수 있습니다.

주:
프로파일 세부 정보를 입력한 후에만 프로파일 구성 페이지로 이동합니다. 자세한 내용은 CrowdStrike Falcon Insight 통합을 위한 역량 프로파일 생성을 참조하십시오.

프로시저

1. 프로필 구성 페이지에서 다음 섹션을 검토하고 구성합니다.

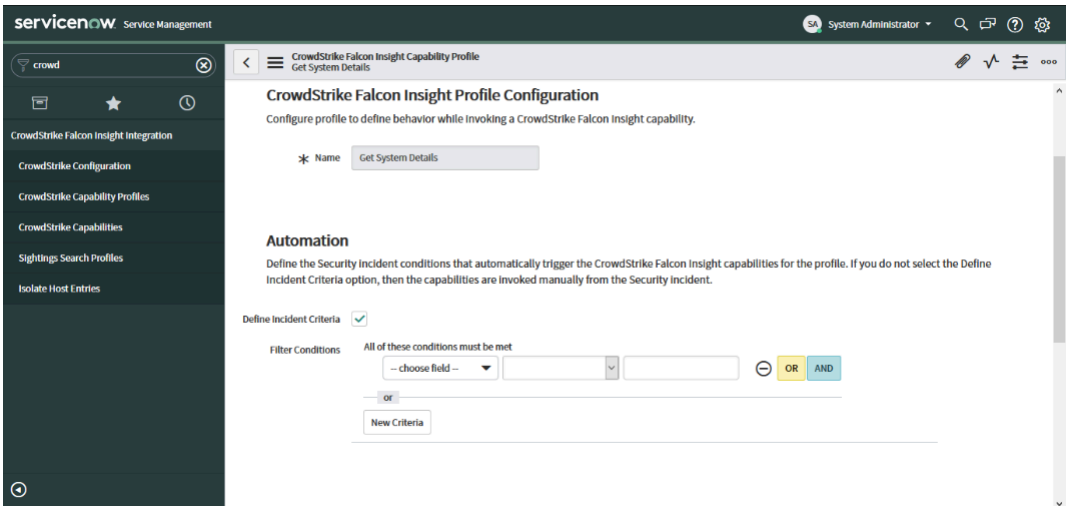
   인시던트 기준 정의(자동화)

   프로파일의 역량을 자동으로 트리거 CrowdStrike Falcon 인사이트 하는 보안 인시던트 조건을 정의합니다. 인시던트 기준 정의 옵션을 선택하지 않으면 보안 인시던트에서 기능이 수동으로 호출됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

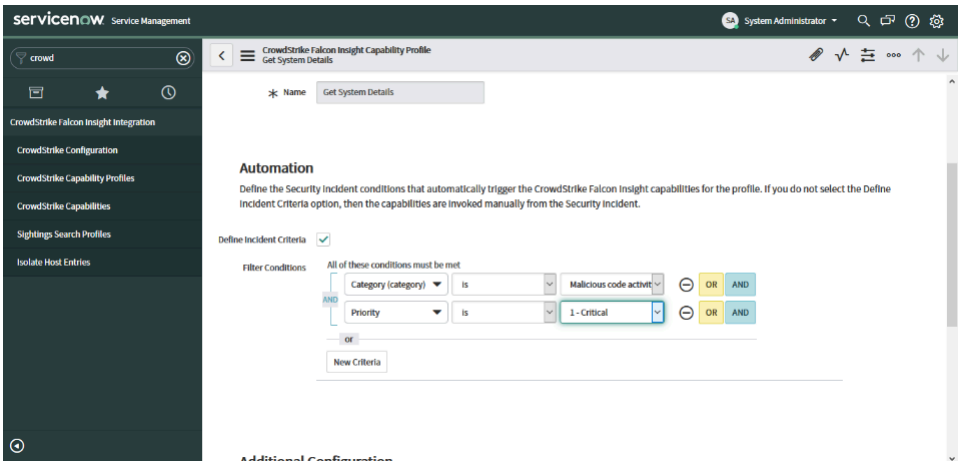
a. 인시던트 기준 정의 옵션을 선택합니다.

b. 조건을 정의하려면 필터 조건 섹션에서 필드와 해당 요구 사항을 선택합니다.



선택합니다.

c. 새 기준 필드에 새 기준을 입력한 다음 **OR** 또는 **AND** 조건을 정의합니다.

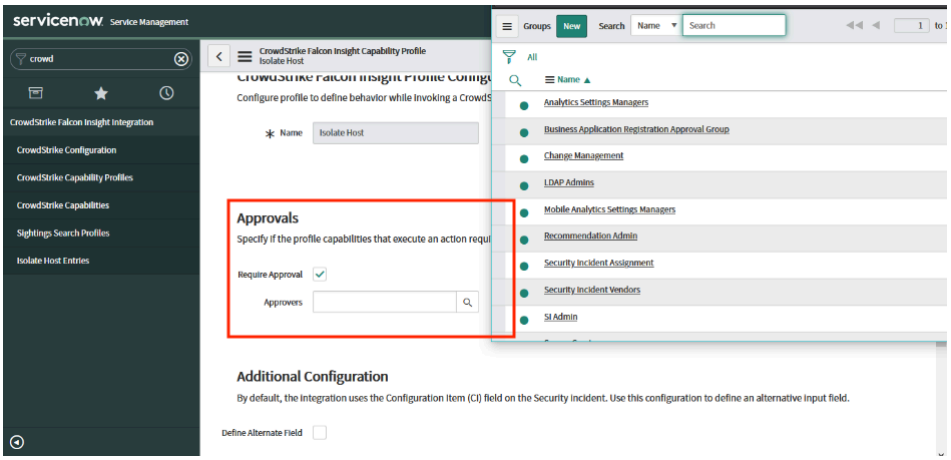


승인

CrowdStrike Falcon Insight 기능을 사용할 때 추가 제어 수준을 제공하려면 승인 필요 옵션을 선택합니다. 프로파일 구성의 승인 옵션은 호스트 격리 및 호스트 격리 제거 기능에 대해서만 나타납니다.

> **주:**
> 승인 권한은 sn_si.admin 역할을 가진 사용자에게 할당됩니다. 이 승인 권한을 승인 그룹에 재할당할 수도 있습니다. 자세한 내용은 승인 그룹 설정을 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



추가 구성

보안 인시던트에서 대체 필드를 선택하여 자산을 스캔하는 동안 찾은 일치하는 CI 데이터를 표시합니다. 기본적으로 통합은 보안 인시던트의 CI(구성 항목) 필드를 사용합니다.

a. 대체 필드 정의 옵션을 선택합니다.

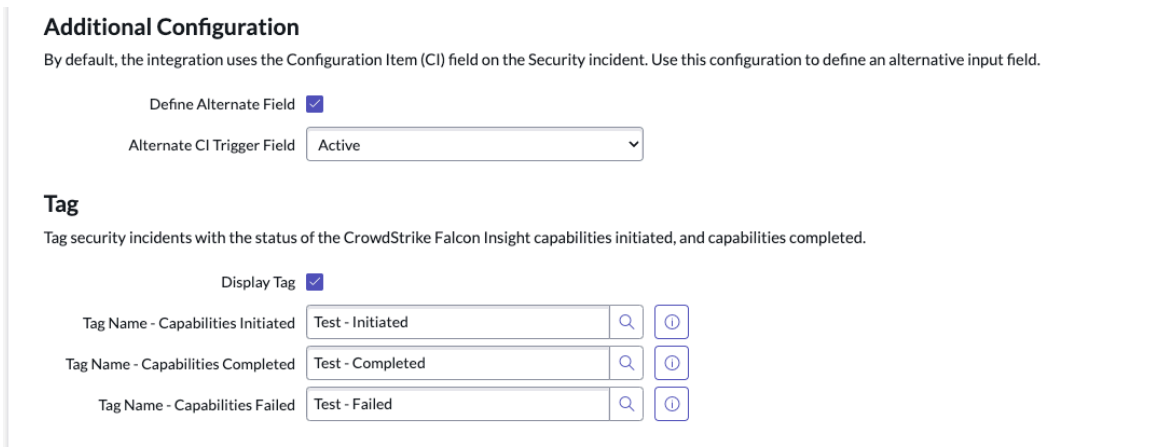
b. 대체 **CI** 트리거 필드에서 입력 필드를 선택합니다.

> **주:**
> 자세한 내용은 프로필의 구성 항목에서 트리거 조건이 작동하는 방식 이해를 참조하세요.

태그

보안 인시던트에 Capabilities-Initiated CrowdStrike Falcon 인사이트 , Capabilities-Completed 및 Capabilities-Failed 태그를 지정하려면 태그 표시 옵션을 선택합니다. 기본적으로 이 옵션은 모든 프로필에 대해 비활성화되어 있습니다.

> **주:**
> 이러한 태그는 기본 시스템과 함께 제공됩니다. 필요한 경우 태그를 직접 생성할 수 있습니다.



2. 완료를 클릭합니다.

트리거 조건이 프로파일의 구성 항목에서 작동하는 방식

특정 조건 세트가 충족되는 경우에만 프로파일이 실행되도록 프로파일 설정을 구성하거나 보안 인시던트에서 특정 필드 값을 검색하도록 프로파일을 설정할 수 있습니다.

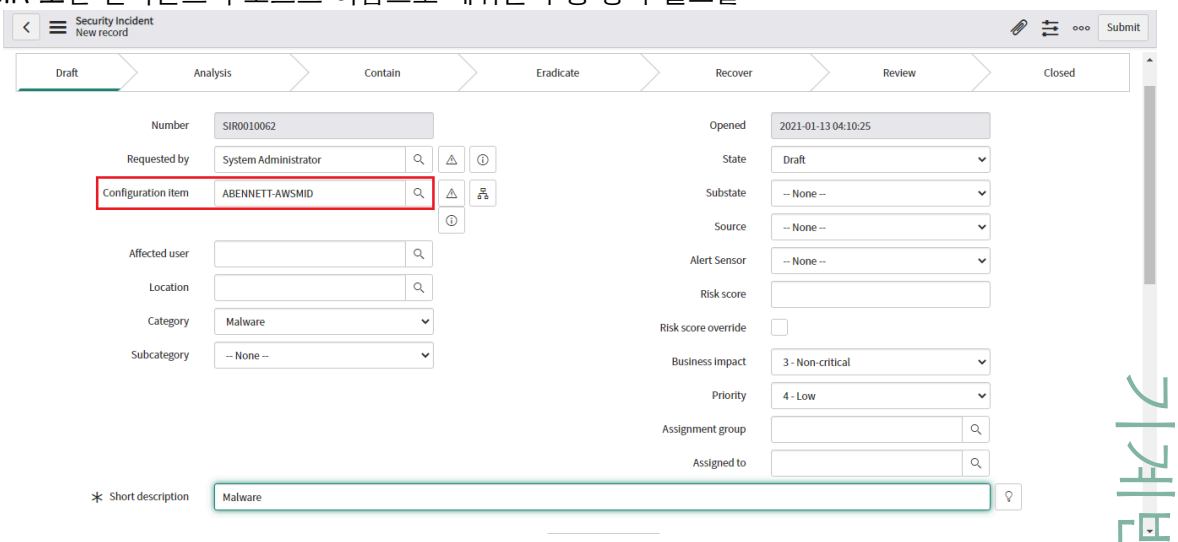
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로파일을 생성하고 프로파일을 실행할 기능을 선택한 CrowdStrike Falcon 인사이트 후에는 기본 필드 값이 보안 인시던트와 일치할 때 프로파일이 자동으로 실행되도록 트리거 조건을 설정할 수 있습니다 ServiceNow AI Platform .

기본적으로 통합은 보안 인시던트의 CI(구성 항목) 필드를 사용합니다. 이 필드는 자산 ID를 데이터베이스에 저장된 ServiceNow AI Platform 정보와 일치시키는 데 사용됩니다. SIR 보안 인시던트가 보안 이벤트에 의해 생성되고 프로파일이 활성화되면 호스트 이름 또는 IP 주소에서 일치하는 값을 찾기 위해 자산을 스캔합니다.

데이터베이스에서 일치하는 값이 발견되면 콘솔에서 해당 데이터가 수집 CrowdStrike Falcon 인사이트 되어 인스턴스로 ServiceNow AI Platform 가져와서 보안 인시던트의 관련 목록에 표시됩니다.

다음 예는 SIR 보안 인시던트의 호스트 이름으로 채워진 구성 항목 필드를



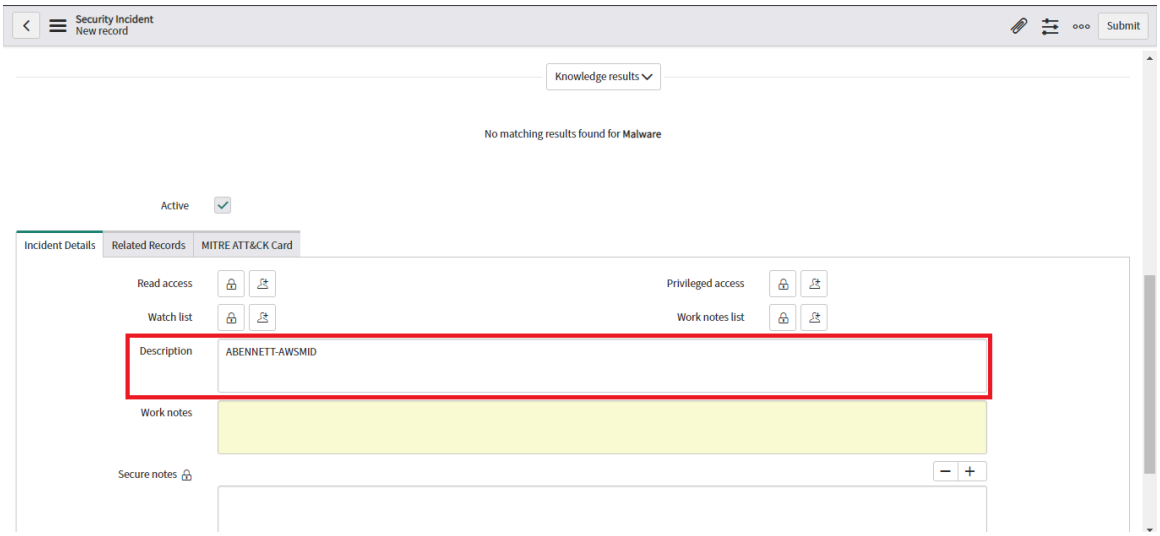
보여줍니다.

CI(구성 항목) 필드가 데이터베이스와 일치하는 호스트 이름 또는 IP 주소로 채워지지 않은 경우, 보안 인시던트의 다른 필드를 선택하여 자산을 스캔하는 동안 찾은 일치하는 CI 데이터를 표시할 수 있습니다.

프로파일 설정을 구성할 때 엔드포인트 식별을 위한 대체 **CI** 트리거 필드를 선택하여 조회의 CrowdStrike Falcon 인사이트 CI 데이터가 연결된 보안 인시던트에 채워지도록 할 수 있습니다. 생성한 사용자 지정 필드를 포함하여 보안 인시던트의 모든 필드를 대체 CI 트리거 필드로 선택할 수 있습니다. 인시던트 생성 시 연관된 보안 인시던트에 CI 필드가 채워지지 않은 경우 대체 CI 필드를 선택하여 프로파일이 트리거되도록 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음 예는 SIR 보안 인시던트에서 호스트 이름으로 채워진 대체 필드를 보여줍니다. 대체 필드는 설명



필드입니다.

프로파일 트리거 조건 확인 **CrowdStrike Falcon** 인사이트

프로파일을 테스트하고 구성한 트리거 조건 필터가 예상대로 작동하는지 확인합니다.

시작하기 전에

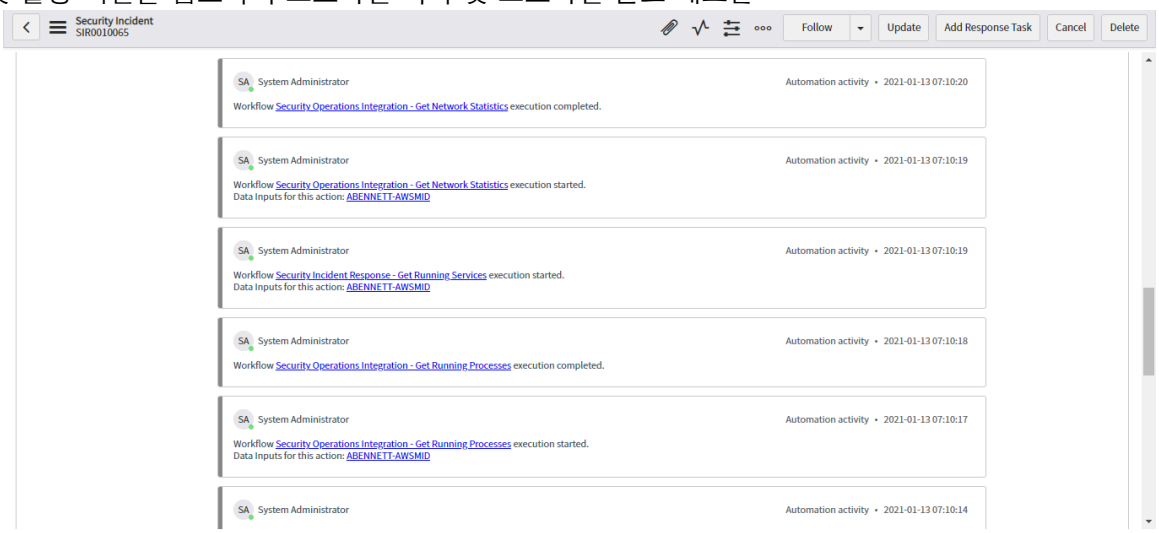
필요한 역할: sn_si.admin

이 태스크 정보

보안 인시던트에서 ServiceNow AI Platform 쿼리 결과를 볼 수 있도록 지정한 구성된 트리거 조건을 기반으로 하는 프로파일을 활성화합니다.

프로시저

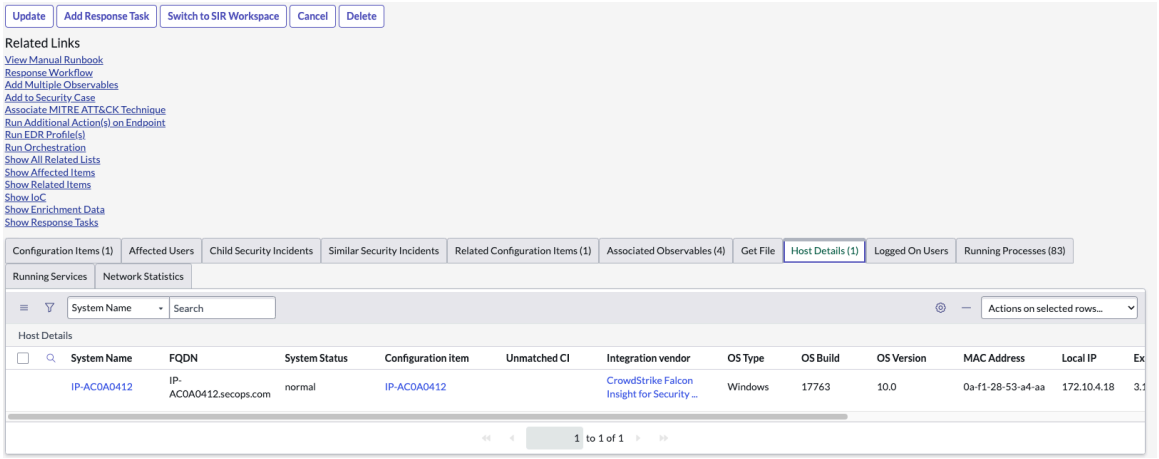
1. 다음으로 이동 모두 〉 보안 인시던트 〉 모든 인시던트 표시.
2. 새로 만들기를 선택하여 보안 인시던트를 만듭니다.
3. 보안 인시던트를 만들려면 필요한 정보를 입력하고 저장을 클릭합니다.
4. 작업 메모 및 활동 섹션을 검토하여 프로파일 시작 및 프로파일 완료 태그를



확인합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. 파일 가져오기, 호스트 상세 정보, 로그온한 사용자, 실행 중인 프로세스, 실행 중인 서비스, 네트워크 통계 등과 같은 상세 정보 관련 목록에서 상세 정보를 CrowdStrike Falcon 인사이트 검토합니다.



보안 인시던트에서 수동으로 프로파일 트리거 **CrowdStrike Falcon** 인사이트

보안 인시던트를 검토한 후 프로파일을 수동으로 트리거합니다.

시작하기 전에

필요한 역할: 관리자

이 태스크 정보

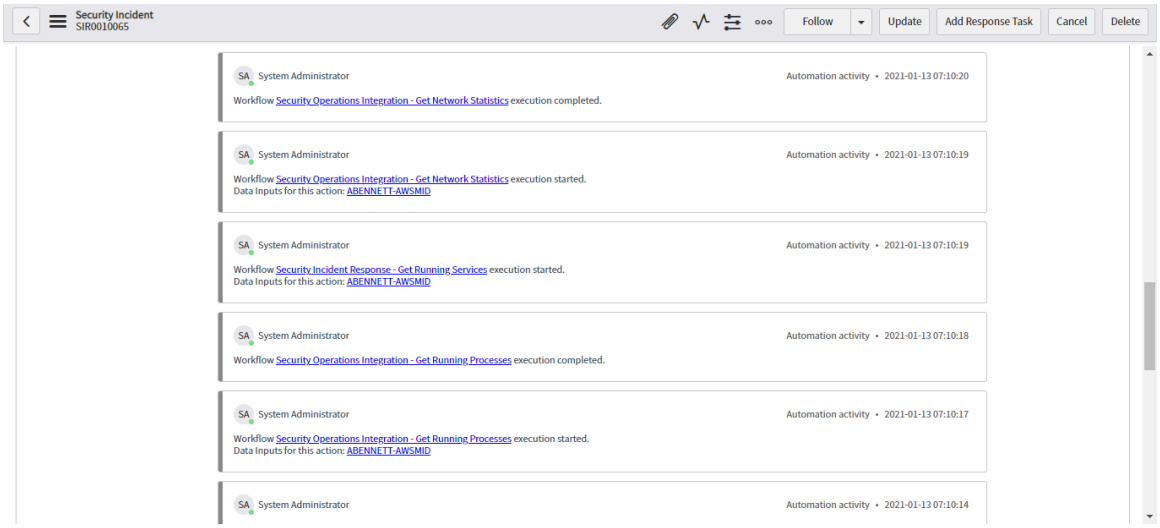
프로파일을 활성화하면 구성된 트리거 조건에 따라 보안 인시던트에서 ServiceNow AI Platform 쿼리 결과를 볼 수 있습니다. CrowdStrike Falcon 인사이트 또한 프로파일을 사용하지 않고 CI(구성 항목)에서 개별 역량을 실행할 수 있습니다.

프로시저

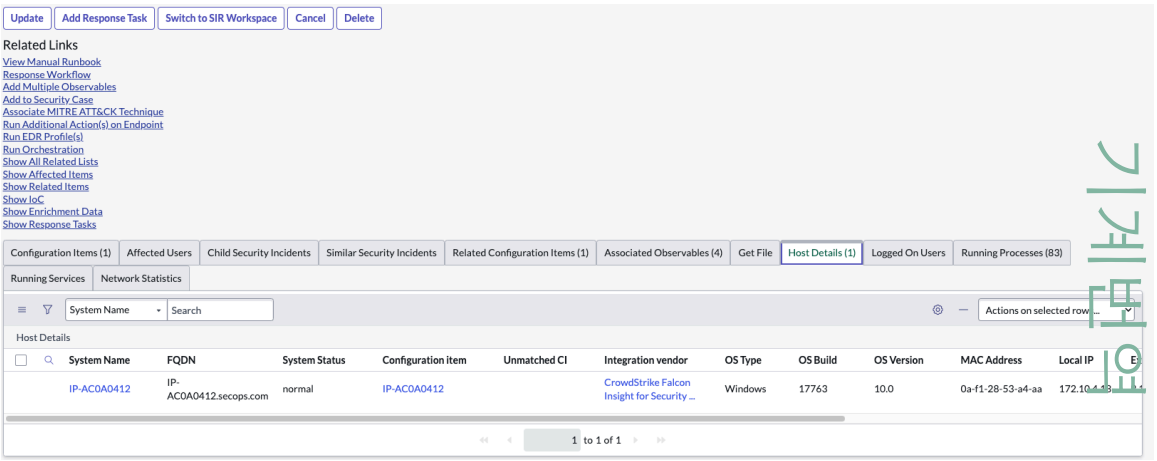
1. 다음으로 이동 모두 〉 보안 인시던트 〉 모든 인시던트 표시.
2. 정보로 검토하려는 보안 인시던트를 CrowdStrike Falcon 인사이트 선택합니다.
3. 관련 목록 섹션에서 **EDR** 프로파일 실행을 선택합니다.
4. 사용 가능한 프로파일 목록에서 프로파일을 찾아 선택합니다.
5. 프로파일의 모든 관련 CI에서 이 프로파일을 실행하려면 관련 **CI** 포함 을 선택합니다.
   예를 들어 보안 인시던트와 연결된 CI가 5개 있는 경우 선택한 프로파일이 5개의 CI 모두에서 실행됩니다.
6. 제출을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

선택한 프로파일이 수동으로 트리거됩니다. 작업 메모 섹션에서 작업 메모 및 활동 섹션과 프로파일 시작 및 프로파일 완료 태그를 검토할 수 있습니다.



7. 결과는 파일 가져오기, 호스트 상세 정보, 로그온한 사용자, 실행 중인 프로세스, 실행 중인 서비스, 네트워크 통계 등과 같은 관련 목록의 형태로 나타납니다.



8. CI에서 개별 기능을 실행하려면 다음 단계를 수행합니다.

a. 구성 항목 관련 목록에서 필요한 CI를 선택합니다.

b. 선택한 행에 대해 수행할 작업... 드롭다운 목록을 클릭하고 선택한 CI에 대해 실행할 필수 기능을 선택합니다.
예: 호스트 격리.

c. 검색 옵션을 사용하여 CI에 필요한 기능 구현을 조회하고 **CrowdStrike Falcon Insight** 호스트 격리를 선택합니다.

d. 호스트 격리를 클릭하여 선택한 CI에서 실행합니다.

사이팅 검색을 위한 프로파일 생성 및 구성

사이팅 검색을 CrowdStrike Falcon 인사이트 사용하여 조직의 네트워크 전체에서 감염된 컴퓨터를 찾고 보안 인시던트 응답 케이스를 해결합니다.

시작하기 전에
필요한 역할: sn_si.analyst

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보
개별 또는 여러 옵저버블을 선택하고 수동 사이팅 검색을 CrowdStrike Falcon 인사이트 수행하여 시간 경과에 따른 위협의 확산을 확인합니다.

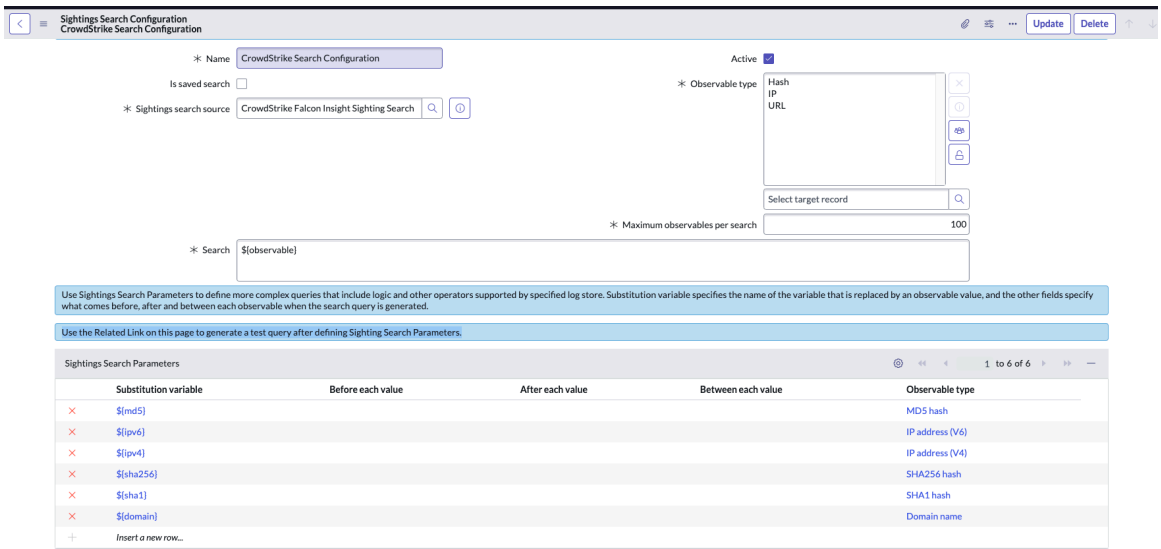
프로시저

1. 다음으로 이동 모두 〉 **CrowdStrike Falcon Insight** 통합 〉 사이팅 검색 프로파일.
2. 새로 만들기를 클릭합니다.
3. 특정 CrowdStrike Falcon Insight 검색 기능을 검색할 서버를 결정하려면 이 프로파일을 구성합니다.
4. 양식에서 필드에 다음을 입력합니다.

필드	설명
이름	사이팅 검색 프로파일의 이름입니다.
저장된 검색 여부	이 옵션을 선택하면 저장된 검색 구성이 생성됩니다.
관찰 검색 소스	사이팅 검색의 소스입니다. **CrowdStrike Falcon Insight** 관찰 검색을 소스로 선택합니다.
활성	추가가 활성 상태인지 여부를 나타내는 옵션입니다.
옵저버블 유형	CrowdStrike Falcon Insight 통합은 다음 옵저버블 유형을 지원합니다. ○ 해시 ○ IP ○ URL 사이팅 검색은 다음 옵저버블 유형에 대해 지원됩니다. ○ 도메인 이름 ○ IP 주소(V4) ○ IP 주소(V6) ○ MD5 해시 ○ SHA1 해시 ○ SHA256 해시
검색당 최대 옵저버블	검색 쿼리에서 볼 수 있는 최대 옵저버블 수입니다.
검색	기본 검색 문자열은 $(observable)이지만 통합에서 CrowdStrike Falcon 인사이트 지원하는 매개변수를 지정하여 고유한 검색 쿼리를 정의할 수 있습니다.
사이팅 검색 매개변수	지정된 로그 저장소에서 지원하는 논리 및 기타 연산자를 포함하는 보다 복잡한 쿼리를 정의하는 매개변수

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	페이지 하단의 관련 링크를 사용하여 사이팅 검색 매개변수를 정의한 후 테스트 쿼리를 생성할 수 있습니다.



5. 제출을 클릭합니다.
   구성이 완료되었으며 보안 인시던트에서 사이팅 검색을 호출할 수 있습니다 ServiceNow AI Platform .
6. 구성을 확인하고 사이팅 검색을 실행하려면 다음 단계를 수행하십시오.

   a. 보안 인시던트를 열고 보안 인시던트의 맨 아래로 스크롤한 다음 모든 관련 목록 표시를 클릭합니다.

   b. 실행 중인 프로세스 관련 목록에서 하나 이상의 CI(구성 항목)를 선택하는 경우

   > **주:**
   > 실행 중인 프로세스 관련 목록에서 CI에 대한 사이팅 검색을 실행하면 프로세스 해시 사이팅 검색만 수행됩니다.

   c. 선택한 행에 대해 수행할 작업... 드롭다운 목록을 누르고 **CrowdStrike** 사이팅 검색 실행을 선택합니다.

   d. 검색 옵션을 사용하여 필요한 사이팅 검색 프로파일을 조회합니다.

   e. 필요한 사이팅 검색 프로파일을 선택하고 제출을 클릭합니다.

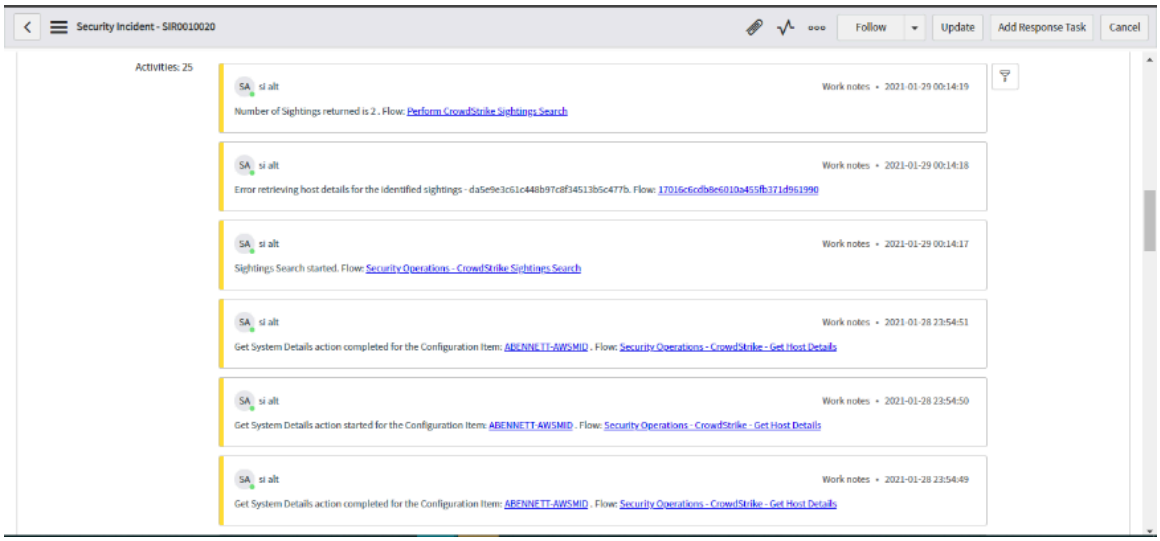
   f. 연결된 옵저버블 관련 목록에서 하나 이상의 옵저버블을 선택하는 경우

   g. 선택한 행에 대해 수행할 작업... 드롭다운 목록을 클릭하고 사이팅 검색 실행을 선택합니다.

   h. 시간 범위 팝업에서 임의의 값을 선택하고 검색을 클릭합니다.

   i. 검색이 완료되면 작업 메모 및 관련 목록에서 결과와 상세 정보를 확인합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



j. 사이팅 세부 정보를 보려면 사이팅 탭을 선택합니다.

k. CrowdStrike 사이팅 세부 정보에 대한 자세한 내용을 보려면 CI 옆에 있는 미리보기 아이콘을 클릭하십시오.

l. 사이팅 검색 상세 정보를 보려면 사이팅 검색 상세 정보를 클릭하고 검색 결과에 대해 사이팅 검색 결과 탭을 클릭합니다.

에서 추가 작업 구성 및 트리거 **CrowdStrike Falcon** 인사이트

통합은 CrowdStrike Falcon 인사이트 정규 표현식(regex)과 같은 추가 작업 실행을 지원합니다. 통합은 CrowdStrike Falcon 인사이트 기본 시스템에 40개의 추가 작업을 제공합니다.

시작하기 전에
필요한 역할: sn_si.analyst

프로시저

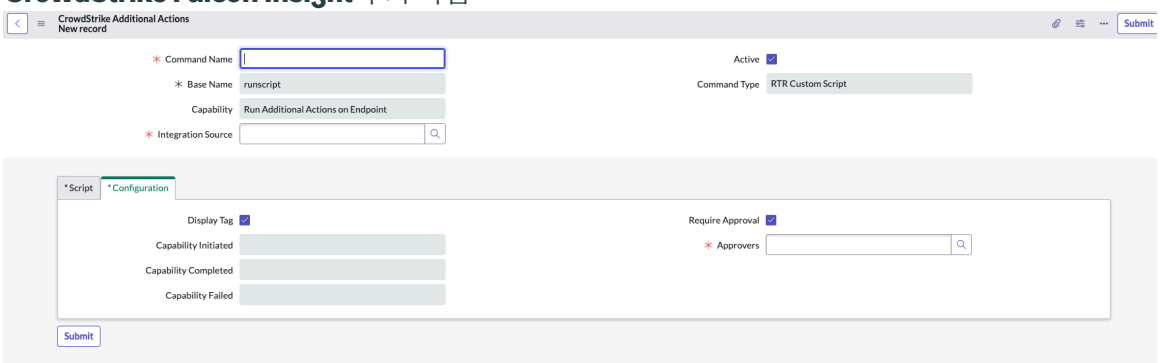
1. 다음으로 이동 모두 〉 **CrowdStrike Falcon Insight** 통합 〉 **CrowdStrike** 추가 작업.
2. 새로 만들기를 클릭하여 추가 작업을 직접 만들거나 기본 시스템과 함께 제공되는 기존 작업을 선택합니다.
   예를 들어 새 추가 작업을 생성해 보겠습니다.
3. 양식에서 필드를 채웁니다.

필드	설명
명령 이름	추가 작업에 대한 명령 이름입니다. 예를 들어 reg set입니다.
기본 이름	추가 작업의 기본 이름입니다. 이 필드는 기본적으로 설정됩니다. 예: reg.
역량	추가 작업에 대한 역량 이름입니다. 이 필드는 기본적으로 설정됩니다. 예를 들어 엔드포인트에서 추가 작업을 실행합니다.
통합 소스	추가 작업의 소스입니다. 예를 들어 CrowdStrike Falcon Insight 통합입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
활성	추가가 활성 상태인지 여부를 나타내는 옵션입니다.
명령 유형	추가 작업에 대한 명령 유형입니다. 이 필드는 기본적으로 설정됩니다. 예: RTR 사용자 지정 스크립트.
스크립트	○ **OS** 유형: 스크립트의 OS 유형을 선택하는 옵션입니다. 다음 중 하나를 선택합니다. ▪ **Windows** ▪ **MAC OS X** ▪ **Linux** ▪ 없음 ○ 스크립트: 없음 옵션을 제외하고 다음 OS 중 하나를 선택한 경우 스크립트를 입력하는 옵션입니다.
구성	○ 태그 표시: 구성에 대한 태그를 표시하는 옵션입니다. 다음 필드에 대한 태그를 선택할 수 있습니다. ▪ 역량 - 시작됨. 예: reg set - Initiated. ▪ 역량 - 완료됨. 예: reg set - Completed. ▪ 역량 - 실패함. 예: reg set - Failed. ○ 승인 필요: 구성을 승인해야 하는 승인자 또는 그룹을 선택하는 옵션입니다.

CrowdStrike Falcon Insight 추가 작업

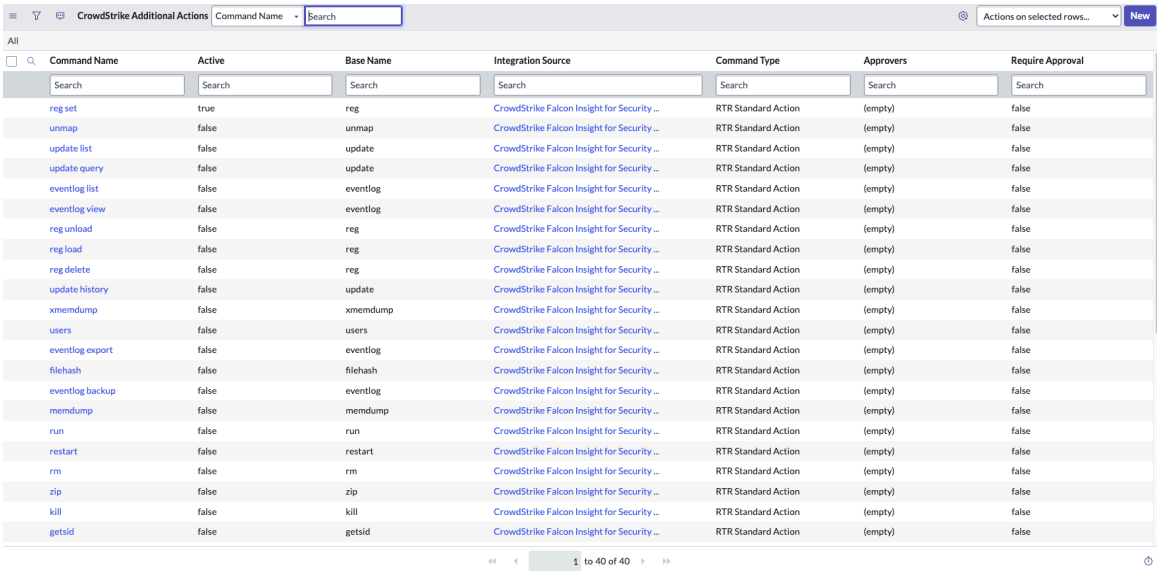


4. 제출을 클릭합니다.
5. 다음과 같은 기존 추가 작업 중에서 선택할 수도 있습니다.
   기본 시스템과 함께 제공되는 40개의 추가 작업이 있으며, 추가 구성을 수행하는 데 사용할 수 있습니다.

   주:
   CrowdStrike 추가 작업 목록을 열고 필요한 추가 작업을 **true**로 설정해야 합니다. 그렇지 않으면 작업 공간에서 추가 작업을 사용할 수 없습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

기본 시스템과 함께 제공되는 추가 작업 목록



Command Name	Active	Base Name	Integration Source	Command Type	Approvers	Require Approval
reg set	true	reg	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
unmap	false	unmap	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
update list	false	update	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
update query	false	update	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
eventlog list	false	eventlog	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
eventlog view	false	eventlog	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
reg unload	false	reg	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
reg load	false	reg	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
reg delete	false	reg	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
update history	false	update	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
xmemdump	false	xmemdump	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
users	false	users	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
eventlog export	false	eventlog	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
filehash	false	filehash	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
eventlog backup	false	eventlog	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
memdump	false	memdump	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
run	false	run	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
restart	false	restart	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
rm	false	rm	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
zip	false	zip	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
kill	false	kill	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
getsid	false	getsid	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false

1 to 40 of 40

6. 다음으로 이동 보안 인시던트 〉 모든 인시던트 표시.
7. 엔드포인트에서 추가 작업 실행으로 검토하려는 보안 인시던트를 선택합니다.
   a. 관련 링크 섹션에서 이 버튼을 클릭합니다. 엔드포인트에서 추가 작업 실행.
   b. 필요한 역량을 찾아 선택합니다.
   예를 들어, **reg set** 기능을 클릭합니다.
   c. 엔드포인트의 모든 관련 CI에 대해 추가 작업을 실행하려면 관련 **CI** 포함 을 선택합니다.
   d. 엔드포인트에서 추가 작업을 실행하기 위한 하위 키를 정의할 수 있습니다.
   이 하위 키는 HKLM/Software/new 키일 수 있습니다.
8. 엔드포인트에서 추가 작업 실행을 시작하려면 추가 작업 실행을 클릭합니다.
9. 실행의 자동화 활동을 보고 검증합니다.
10. 엔드포인트에 대한 추가 작업 관련 목록에서 작업의 상태를 확인합니다.

분석가 작업 공간에서 통합 사용 **CrowdStrike Falcon** 인사이트

CrowdStrike Falcon 인사이트 통합을 사용하여 SIR 분석가 작업 공간의 기능을 활용합니다CrowdStrike Falcon 인사이트.

시작하기 전에

필요한 역할: sn_si.admin

보안 인시던트 응답 작업 공간에서 통합을 사용하려면 CrowdStrike Falcon 인사이트 먼저 에서 ServiceNow Store 다운로드하여 구성해야 합니다. 자세한 내용은 통합 시작하기 CrowdStrike Falcon 인사이트 문서를 참조하십시오.

이 태스크 정보

통합을 사용하여 CrowdStrike Falcon 인사이트 엔드포인트에서 실시간으로 정정 작업을 수행하고, 프로필을 사용하여 호스트에 대한 상세 정보를 수집하고, 작업 공간을 사용하여 엔드포인트에서 특정 쿼리 또는 작업을 수행할 수 있습니다 보안 인시던트 응답 .

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

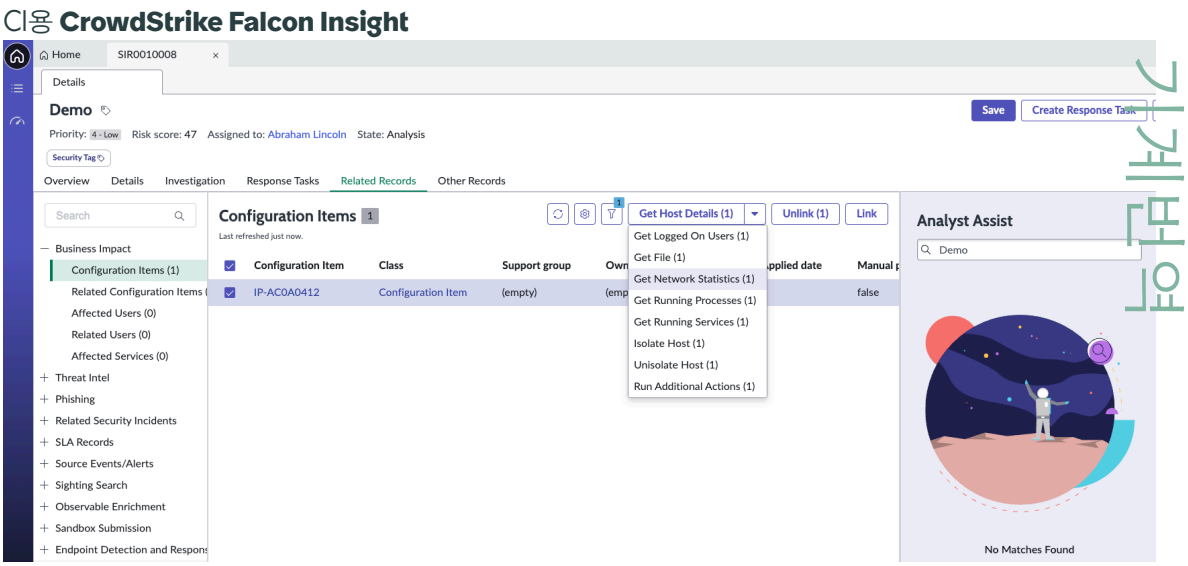
통합을 통해 CrowdStrike Falcon 인사이트 분석가는 분석가 작업 공간에서 보안 인시던트 응답 다음 CrowdStrike Falcon 인사이트 기능을 사용할 수 있습니다.

- 호스트 상세 정보 가져오기
- 로그온한 사용자 가져오기
- 네트워크 통계 임포트
- 실행 중인 프로세스 임포트
- 실행 중인 서비스 가져오기
- 호스트 분리
- 격리 제거
- 파일 가져오기

프로시저

1. SIR 작업 공간에서 필요한 보안 인시던트를 열고 관련 기록 탭을 선택합니다.
2. 비즈니스 영향 관련 목록에서 CrowdStrike Falcon Insight 기능을 분석을 위해 사용할 수 있습니다.

   a. 구성 항목을 선택하고 드롭다운 목록에서 기능을 선택합니다.



   b. **CrowdStrike Falcon Insight** 구현을 선택하고 제출을 클릭하십시오.
   네트워크 통계 가져오기 기능은 CI에서 호출됩니다. 결과 및 결과에 대한 작업 주석을 볼 수 있습니다.

3. 분석을 위해 엔드포인트 탐지 및 응답**(EDR)** 관련 목록에서 CrowdStrike Falcon Insight 기능을 사용할 수 있습니다.

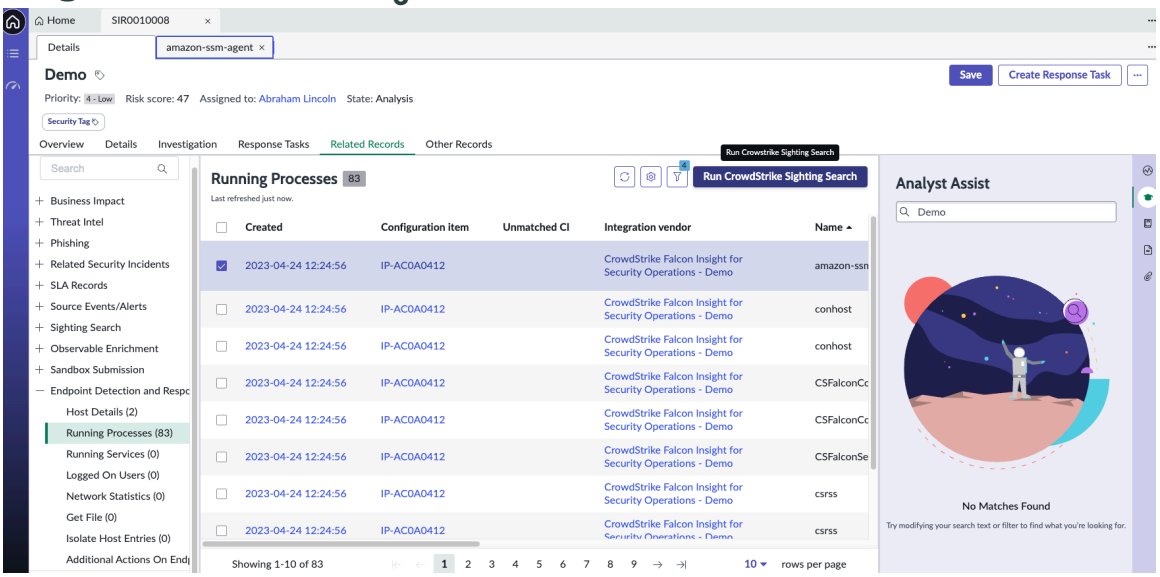
   a. EDR(엔드포인트 탐지 및 응답) 관련 목록의 목록에서 EDR을 선택합니다.

   b. CrowdStrike Falcon Insight 실행 중인 프로세스 상세 정보를 보려면 특정 실행 중인 프로세스를 클릭합니다.

   c. 실행 중인 특정 프로세스에서 CrowdStrike Falcon 관찰 검색을 실행하려면 실행 중인 프로세스를 선택하고 **CrowdStrike** 관찰 실행을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

EDR용 **CrowdStrike Falcon Insight**



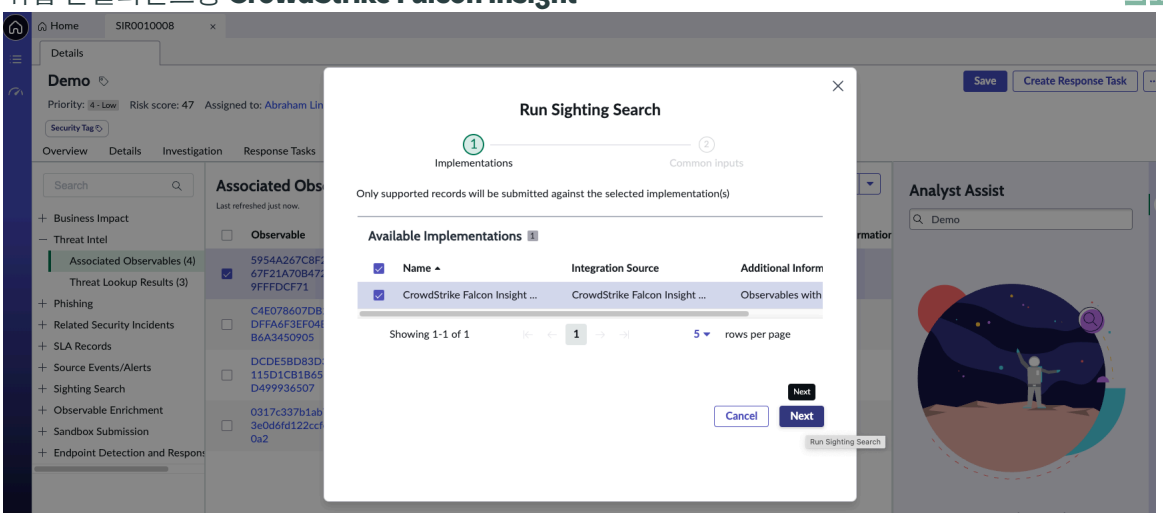
d. CrowdStrike Falcon Insight 구현을 선택하고 검색 실행을 클릭합니다.
그런 다음 선택한 실행 중인 프로세스에서 해시 사이팅 검색이 실행됩니다. 결과 및 결과에 대한 작업 주석을 볼 수 있습니다.

4. 위협 인텔리전스에서 CrowdStrike Falcon Insight 기능을 사용하여 분석할 수 있습니다.

a. 위협 인텔리전스 그룹에서 옵저버블을 선택하고 드롭다운 목록에서 기능을 선택합니다 CrowdStrike Falcon 인사이트 .

b. CrowdStrike Falcon Insight 구현을 선택하고 다음을 클릭합니다.

위협 인텔리전스용 **CrowdStrike Falcon Insight**



c. 날짜/시간 선택 팝업에서 임의의 값을 선택하고 제출을 클릭합니다.
그런 다음, 선택한 옵저버블에 대해 사이팅 검색이 실행됩니다. 결과 및 결과에 대한 작업 주석을 볼 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

CrowdStrike Next-Gen SIEM 통합

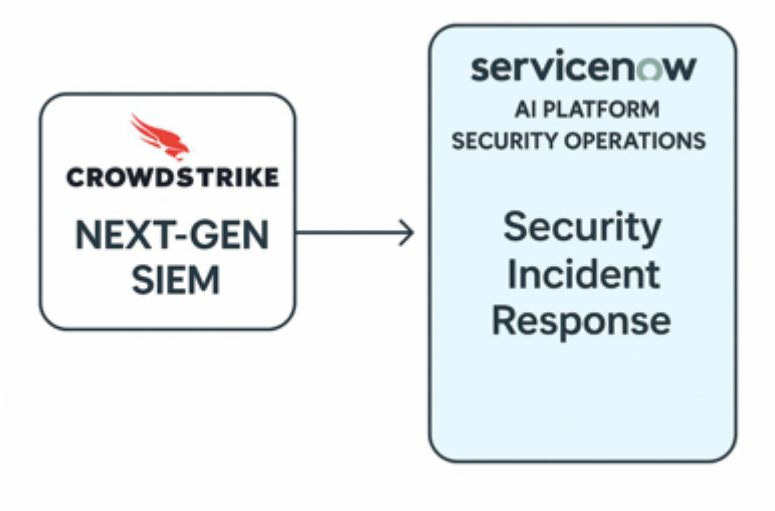
통합은 CrowdStrike Next-Gen SIEM 잠재적인 보안 인시던트를 나타낼 수 있는 탐지 데이터를 자동으로 수집하고 SIR(보안 인시던트 응답)에서 ServiceNow# 보안 인시던트 생성을 간소화하여 시기 적절하고 효과적인 응답을 보장합니다.

스토어에서 앱 요청

ServiceNow Store 웹 사이트를 방문하면 사용 가능한 모든 앱을 확인하고 스토어에 요청을 제출하는 방법에 대한 정보를 참조할 수 있습니다. 출시된 모든 앱의 누적 릴리스 정보는 ServiceNow Store 버전 기록 릴리스 정보를 참조하십시오.

CrowdStrike Next-Gen SIEM 통합 개요

다음 그래픽을 참조하여 애플리케이션과 통합하는 ServiceNow AI Platform 보안 운영 방법을 CrowdStrike Next-Gen SIEM 알아보십시오.



주요 기능

이 통합의 주요 기능을 사용하여 다음 작업을 수행합니다.

- 보안 인시던트 후보인 탐지를 검색하고 CrowdStrike Next-Gen SIEM 이러한 보안 인시던트 생성을 자동화합니다.
- 결함 및 엔터티 필드를 보안 인시던트 필드에 매핑 CrowdStrike Next-Gen SIEM 합니다 SIR .
- 필터 CrowdStrike Next-Gen SIEM 결함.
- 중복 보안 인시던트를 생성할 필요가 없도록 인시던트를 기존 미해결 보안 인시던트에 집계합니다.
- 보안 인시던트를 만들고 종결할 수 있도록 보안 인시던트 응답에 대한 탐지 상태 업데이트를 자동화 CrowdStrike Next-Gen SIEM 합니다.

  주:
  ServiceNow 보안 인시던트 생성 또는 종결에 따라 탐지 상태를 CrowdStrike Next-Gen SIEM 업데이트합니다. 이 업데이트에는 집계된 탐지 및 새로운 탐지에 대한 설명도 포함됩니다.

- 주기적으로 보안 인시던트를 생성하도록 탐지 수집을 예약합니다.
- 탐지 코멘트를 작업 메모와 SIR 동기화합니다CrowdStrike Next-Gen SIEM.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

통합 시작하기 **CrowdStrike Next-Gen SIEM**

인스턴스 및 보안 인시던트 응답 제품과 인터페이스 ServiceNow AI Platform 할 보안 운영 플러그인에 대한 통합을 활성화하고 설정합니다CrowdStrike Next-Gen SIEM.

통합을 사용하려면 CrowdStrike Next-Gen SIEM 먼저 다음 ServiceNow Store에서 다운로드해야 합니다.

다음 설정 검사 목록을 검토하고 원활한 통합을 위한 모든 작업을 완료했는지 확인합니다.

검사 목록

설정 작업	설명
필수 ServiceNow AI Platform 및 보안 인시던트 응답 역할을 할당하고 확인합니다.	예상 결과를 구성하고 검증하려면 다음 역할이 필요합니다. • 관리자 역할은 에서 ServiceNow Store 통합을 설치하고 sn_si.ingestion_profile_admin 및 sn_si.analyst 역할을 할당합니다. • sn_si.ingestion_profile_admin 역할은 다음 작업을 수행합니다. ○ 통합을 구성합니다. ○ 탐지 프로파일을 생성합니다. ○ CrowdStrike Next-Gen SIEM 탐지 데이터 필드를 보안 인시던트 필드에 매핑합니다. ○ 진행 중인 탐지 수집을 예약합니다. ○ 탐지가 생성되거나 종결될 보안 인시던트 응답 때 탐지 업데이트를 활성화합니다.
CrowdStrike에 필요한 역할을 할당합니다.	CrowdStrike에서 애플리케이션을 등록하고 구성하려면 다음 역할이 필요합니다. • 애플리케이션을 등록할 애플리케이션 개발자입니다. • 테넌트 관리자가 관리자 동의 엔드포인트를 호출하여 애플리케이션에 권한을 부여합니다.
ServiceNow 이 통합을 구성하기 전에 통합을 지원하는 데 필요한 핵심 애플리케이션이 설치되고 활성화되었는지 확인합니다.	플러그인(com.snc.security_incident)이 보안 인시던트 응답 필요합니다. 이 플러그인은 제품을 지원하는 데 필요한 모든 종속성을 보안 인시던트 응답 자동으로 설치합니다. 통합에 필요한 다른 보안 운영 애플리케이션을 설치하고 활성화하기 전에 이 플러그인을 설치하고 활성화합니다.
설치 및 구성	ServiceNow AI Platform 인스턴스에서 애플리케이션에 ServiceNow Store 대한 보안 운영 통합을 설치하고 구성합니다CrowdStrike Next-Gen SIEM.

설치 및 구성

ServiceNow AI Platform 인스턴스에서 애플리케이션에 ServiceNow Store 대한 보안 운영 통합을 설치하고 구성합니다CrowdStrike Next-Gen SIEM.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_si.ingestion_profile_admin

주:
sn_si.admin 역할을 가진 사용자는 기본적으로 필요한 권한을 상속하기 때문에 프로파일 관리자가 사용할 수 있는 모든 작업을 수행할 수 있습니다.

프로시저

1. CrowdStrike Next-Gen SIEM 에서 ServiceNow Store 통합을 다운로드하여 설치합니다.
   자세한 내용은 에서 처음으로 애플리케이션 ServiceNow Store 다운로드 문서를 참조하십시오.
2. 다음으로 이동 보안 운영 〉 통합 〉 통합 구성.
3. 통합 타일을 CrowdStrike Next-Gen SIEM 검색하고 구성을 선택합니다.
4. 양식에서 필드를 채웁니다.

CrowdStrike 차세대 **SIEM** 통합 양식

필드	설명
이름	통합의 CrowdStrike Next-Gen SIEM 이름입니다.
클라이언트 ID	CrowdStrike 포털에 있는 계정 프로파일의 설정 섹션에서 얻은 클라이언트 ID입니다.
클라이언트 비밀	CrowdStrike 포털에 있는 계정 프로파일의 설정 섹션에서 얻은 클라이언트 비밀 키입니다.
지역	데이터를 끌어올 데이터 센터입니다. 리전 지정: US-1, US-2, EU-1, US-GOV-1, US-GOV-2 기본적으로 이 필드는 US-1로 설정됩니다

5. 제출을 선택합니다.
   구성된 통합 타일이 표시됩니다.

다음에 수행할 작업
탐지 프로파일 생성

탐지 프로파일 생성

CrowdStrike Next-Gen SIEM 인스턴스에 탐지 프로파일을 ServiceNow AI Platform 생성하여 보안 인시던트를 생성하는 데 적합한 탐지를 결정합니다.

시작하기 전에
필요한 역할: sn_si.ingestion_profile_admin

주:
sn_si.admin 역할은 기본적으로 필수 권한을 상속하므로 sn_si.admin 역할을 가진 사용자는 프로파일 관리자가 사용할 수 있는 모든 작업을 수행할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 *CrowdStrike Next-Gen SIEM* 〉 탐지 프로파일.
2. 새로 만들기를 선택합니다.
3. 양식에서 필드를 채웁니다.

CrowdStrike Next-Gen SIEM - 탐지 수집 구성 양식

필드	설명
이름	프로필의 이름입니다. 이 이름은 이 프로파일과 연결된 보안 태그의 기본 이름이기도 합니다.
활성	프로파일을 활성 상태로 만드는 옵션입니다. 프로파일이 활성 ServiceNow AI Platform 상태이면 필터링 조건이 일치할 때 능동적으로 CrowdStrike Next-Gen SIEM 탐지 및 해당 보안 탐지가 생성됩니다 보안 인시던트 응답 .
소스	CrowdStrike 탐지를 수집하도록 구성한 테넌트입니다. 여러 테넌트가 구성된 경우 프로필에 대해 수집하려는 탐지 유형에 적합한 테넌트를 선택합니다.
순서	둘 이상의 프로파일이 트리거 조건을 공유할 때 프로파일이 실행되는 우선순위입니다. 우선순위 값은 일반적으로 100(기본값), 200, 300 등으로 제공됩니다. 가장 낮은 번호의 프로파일이 가장 높은 우선순위를 갖습니다.
설명	프로파일에 대한 설명(선택 사항)입니다.

4. 업데이트 를 선택합니다.

   초기 탐지 프로파일은 기본 정보를 사용하여 생성됩니다. 이때 프로파일을 저장하면 중단된 경우 프로파일을 계속 정의할 수 있습니다.

5. 옵션: 프로파일 정의 프로세스를 즉시 계속하십시오.
   a. CrowdStrike-Nextgen 탐지 프로파일 페이지에서 방금 생성한 프로파일을 선택합니다.
   b. 진행률 표시줄에서 상관관계 규칙을 선택합니다.

다음에 수행할 작업
상관 관계 규칙 설정

상관 관계 규칙 설정

탐지 프로파일을 생성한 CrowdStrike Next-Gen SIEM 후 상관관계 규칙을 선택하여 해당 탐지를 보안 인시던트에 매핑합니다. 상관관계 규칙은 프로파일이 열릴 때마다 새로 고쳐지며 새 규칙을 선택할 수 있습니다. 통합은 CrowdStrike Next-Gen SIEM 여러 프로파일을 지원합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_si.ingestion_profile_admin

> **주:**
> sn_si.admin 역할은 기본적으로 필수 권한을 상속하므로 sn_si.admin 역할을 가진 사용자는 프로파일 관리자가 사용할 수 있는 모든 작업을 수행할 수 있습니다.

프로시저

1. 탐지 프로파일 정의 프로세스의 이전 섹션에서 계속하지 않는 경우 정의하는 프로파일에 액세스합니다.
   a. 다음으로 이동 모두 〉 *CrowdStrike Next-Gen SIEM* 〉 탐지 프로파일.
   b. 계속 정의할 프로파일을 선택합니다.
   c. 진행률 표시줄에서 상관관계 규칙을 선택합니다.
2. 모든 상관관계 규칙이 선택됨 확인란의 선택을 취소합니다.
3. 상관관계 규칙 목록 검색 필드에 포털에서 생성된 CrowdStrike 상관관계 규칙 이름을 입력합니다.
4. 상관관계 규칙을 선택합니다.
5. 오른쪽 화살표를 사용하여 규칙을 사용 가능 에서 선택됨 열로 이동합니다.
6. 계속을 선택하여 탐지 프로파일 정의 프로세스의 이 섹션을 완료합니다.

다음에 수행할 작업
개별 CrowdStrike Next-Gen SIEM 탐지 필드를 보안 인시던트의 필드에 매핑합니다 ServiceNow AI Platform 보안 인시던트 응답 . 자세한 내용은 맵 탐지 필드 문서를 참조하십시오.

맵 탐지 필드

매핑된 데이터로 탐지를 생성할 수 있도록 개별 CrowdStrike 차세대 탐지 필드를 보안 인시던트의 SIR 필드에 매핑합니다.

시작하기 전에
필요한 역할: sn_si.ingestion_profile_admin

> **주:**
> sn_si.admin 역할은 기본적으로 필수 권한을 상속하므로 sn_si.admin 역할을 가진 사용자는 프로필 관리자가 사용할 수 있는 모든 작업을 수행할 수 있습니다.

프로시저

1. 매핑 페이지의 CrowdStrike 차세대 필드 매핑 섹션에서 샘플 수집 방법 중 하나를 선택합니다.

샘플 수집 방법

필드	설명
모든 기본 탐지 및 이벤트 필드	이 수집 방법을 사용하여 모든 탐지 및 이벤트 필드의 정적 목록을 봅니다. 이 메서드에는 값 없이 기본 필드 이름만 포함됩니다. 이 정보를 사용하여 필드와 매핑할 수 있습니다 SIR .
최근 탐지 검색	이 수집 방법을 사용하여 가장 최근의 탐지 및 엔터티 데이터를 임포트합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	CrowdStrike 차세대 탐지에 여러 경보가 포함되어 있는 경우 탐지의 일부인 가장 빠른 경보가 매핑 섹션에 표시됩니다. 수집 중에도 가장 빠른 보안 경보 필드 값이 사용됩니다. 5개의 샘플 탐지를 수집할 수 있습니다. 샘플 탐지 필드 값은 프로파일이 샘플 탐지를 수집할 때 채워집니다. 이러한 탐지를 **SIR** 인시던트 대상 필드에 매핑할 수 있습니다. 탐지 필드와 값은 개별 탭으로 나타납니다.

2. 보안 인시던트에 표시되는 기본 필드에 필드를 추가하려면 다음 작업을 수행합니다.

a. SIR 인시던트 대상 필드 섹션에서 ⊕ Map another field 다른 필드 매핑 버튼.
표시할 새 필드에 대한 필드를 선택할 수 있는 필드 목록이 SIR 표시됩니다.

b. 보안 인시던트 열에서 표시되는 목록을 확장한 다음 필드를 선택합니다.

ⓘ 주:
동일한 보안 인시던트에 여러 옵저버블을 표시할 수 있습니다. 예를 들어 옵저버블 필드는 서로 다른 값으로 여러 번 매핑될 수 있습니다. 마찬가지로 구성 항목 및 작업 메모 필드는 여러 값을 지원합니다. 여러 값을 지원할 수 없는 필드에 두 값을 매핑하려고 하면 이 필드가 여러 값을 지원하지 않는다는 오류 메시지가 표시됩니다. 마찬가지로 보안 인시던트의 필드에 여러 옵션을 선택할 수 있는 목록이 있고 목록에 표시되지 않은 해당 필드에 옵션을 매핑하려고 하면 필드가 보안 인시던트에 채워지지 않습니다.

c. 탐지 및 이벤트 필드 섹션에서 필드를 끌어서 놓아 새 필드에 매핑합니다.

d. 필드에 해당하는 확인란을 선택하면 CrowdStrike에서 새로 변경되거나 업데이트된 변경 사항이 자동으로 해당 SIR 인시던트 데이터를 새 인시던트 데이터로 업데이트합니다.

ⓘ 주:
기본 시스템에서 시스템 속성 sn_sec_cs_ngsiem.detection_updates는 기본적으로 False로 설정되어 있으므로 SIR에 연결된 새 경보와 관련된 CrowdStrike 차세대 업데이트를 받을 수 있습니다.

- 기본적으로 영향을 받는 사용자, 구성 항목 및 옵저버블 필드가 선택되어 있습니다. 즉, 새로운 옵저버블이나 관련 구성 항목이 있거나 영향을 받는 사용자가 인시던트에 추가될 때마다 해당 폴링 간격 동안 해당 정보가 자동으로 추출되어 보안 인시던트 응답(SIR)의 관련 목록에 채워집니다.
- 다른 필드의 경우 CrowdStrike 내 CrowdStrike 탐지 기록의 새 변경 사항 또는 업데이트된 변경 내용에 대한 필드에 해당하는 확인란을 선택해야 합니다. 이렇게 하면 해당 SIR 인시던트 데이터가 새 탐지 데이터로 자동 업데이트됩니다.

ⓘ 중요사항:
기존 데이터를 재정의하면 분석가가 작업할 데이터가 불안정해질 수 있으며 보안 인시던트의 필드 값으로 설정된 다른 자동화도 영향을 받을 수 있으므로 이 기능을 선택하기 전에 실사를 수행해야 합니다. 따라서 재정의 기능을 선택하기 전에 실사를 수행하는 것이 매우 중요합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 필드를 제거하려면 SIR 인시던트 대상 필드 섹션의 입력 식 필드 옆에 있는 ⊖ 항목 제거 버튼을 사용합니다.
4. 탐지 및 이벤트 필드 섹션의 필드 값을 SIR 인시던트 대상 필드 섹션의 필드에 매핑하려면 다음 작업 중 하나를 사용합니다.

   a. 탐지 필드 이름(예: id)을 끌어서 SIR 인시던트 대상 필드 열의 필드 이름 옆에 놓습니다.

      탐지 및 이벤트 필드 섹션의 값을 SIR 인시던트 대상 필드 섹션의 필드와 일치시킬 수 있습니다. 필드는 색상으로 구분되므로 매핑 프로세스에서 탐지 필드를 간과하거나 중복하지 않습니다. 연한 파란색 필드는 탐지 필드가 아직 선택되지 않았으며 보안 인시던트에 매핑되지 않았음을 나타냅니다. 수신 탐지 필드를 보안 인시던트의 둘 이상의 필드와 연결하는 것을 선호할 수 있습니다. 회색 필드는 필드가 선택되었고 보안 인시던트의 필드에 매핑되었음을 나타냅니다. 이렇게 하면 보안 인시던트에 추가된 필드 값과 나머지 중요한 인시던트 정보가 매핑되지 않은 상태로 남아 있는지 시각화할 수 있습니다.

   b. 텍스트와 필드의 조합을 추가할 수 있습니다.
   예를 들어 ## ### ${Detections: name}$###. 여기서 ## ### 수동으로 입력할 수 있으며 ${Detections: name}$ 은 탐지 및 이벤트 필드 섹션에서 매핑됩니다.

   c. 소스 탐지 또는 이벤트 필드를 직접 수동으로 입력하고 대상 필드에 매핑할 수 있습니다.
      - 소스 탐지 필드를 수동으로 매핑하려면 ${field name}$ 형식을 사용합니다. 예를 들어 탐지 필드 심각도를 매핑하려면 형식은 ${Detections: severity}$입니다.
      - 소스 이벤트 필드를 수동으로 추가하려면 ${events names: events fields}$ 형식을 사용합니다. 예를 들어 이벤트 필드 설명 이벤트 보안 경보를 매핑하려면 형식은 ${Events: description}$입니다.

   이 통합은 특정 옵저버블 하위 유형을 분류합니다. CrowdStrike Next-Gen 필드를 SIR 옵저버블 필드와 매핑하면 옵저버블이 자동 분류됩니다 ServiceNow AI Platform . 수신 CrowdStrike 차세대 옵저버블을 의 옵저버블 유형에 SIR일반적으로 매핑하려면 옵저버블 필드에 탐지 및 이벤트 필드를 끌어다 놓습니다. 그러나 에서 수신 CrowdStrike 차세대 옵저버블 SIR에 대한 옵저버블 유형을 알고 있는 경우에는 옵저버블 유형 필드에 구체적으로 매핑합니다 SIR . 에서 SIR 특정 옵저버블 유형의 예로는 Observable(도메인 이름), Observable(이메일 주소), Observable(IP 주소(V4)) 및 Observable(호스트 이름)이 있습니다.

   수신 CrowdStrike Next-Gen 필드에 정보가 포함되어 MITRE-ATT&CK 있는 경우 이를 기술 필드에 매핑합니다 MITRE-ATT&CK . 수신 CrowdStrike Next-Gen 필드에 기술 ID 또는 기술 이름이 포함되어 MITRE-ATT&CK 있는지 확인합니다.

   CrowdStrike Next-Gen의 탐지 필드 값이 SIR 보안 인시던트의 필드로 직접 변환되지 않는 경우가 있습니다. 이러한 값의 경우 스크립트 편집기를 사용하여 매핑 단계 중에 보안 인시던트의 필드 값에 대한 형식을 지정할 수 있습니다. 비슷하지만 동일하지는 않은 값의 형식을 지정하려면 스크립트 편집기를 사용하십시오.

5. CrowdStrike 차세대 탐지에서 얻은 새 필드의 필드 번역을 보안 인시던트의 필드 값과 일치하도록 형식을 지정하려면 **SIR** 인시던트 대상 필드 헤더에서 여기를 클릭 링크를 선택합니다.
6. 필드 번역을 지원하는 필드를 수정하려면 스크립트 형식 필드 번역 아이콘을 선택합니다. 필드 번역을 지원하는 필드에는 영향 받는 사용자, 구성 항목 및 우선순위가 있습니다. 예를 들어 범주 옆에 있는 아이콘을 클릭합니다. CrowdStrike 차세대 현장 번역 스크립트 편집기가 열립니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

7. 스크립트에 대한 변경 내용을 입력하고 업데이트를 선택하여 변경 내용을 저장하고 매핑 페이지로 돌아갑니다.
   예를 들어 범주의 경우 스크립트 편집기에서 다음을 정의합니다.

   ```
   "<Incoming CrowdStrike Detection Field Value>" : "<Category to assign to the Security Incident>".
   ```

   이 매핑을 통해 프로파일은 구성된 범주만 사용합니다.
8. 필드 값을 추가하거나 제거하여 매핑을 계속합니다.
   탐지 생성 조건 작성기에서 동일한 필드 값을 사용하여 들어오는 탐지가 보안 인시던트를 생성하기 위해 충족해야 하는 추가 기준을 정의할 수 있습니다.
9. 필터링 및 집계 섹션으로 이동하려면 계속을 선택합니다.

다음에 수행할 작업

보안 인시던트를 생성할 탐지를 지정할 수 있도록 필터 조건을 정의하고 설정합니다. 탐지 생성 조건 빌더(필터링 및 집계 섹션)에서 동일한 필드 값(매핑 섹션에 정의됨)을 사용하여 수신 탐지가 보안 인시던트를 생성하기 위해 충족해야 하는 추가 기준을 정의할 수 있습니다.

필터 및 집계 기준 정의

필터 조건을 정의하고 설정하여 들어오는 CrowdStrike Next-Gen SIEM 탐지에서 보안 인시던트를 생성할지 지정합니다. 인시던트를 생성하는 대신 수신 탐지를 미해결 보안 인시던트에 추가할 수 있는 추가 탐지 필드 기준을 정의할 수도 있습니다.

필터링 조건 설정

필터링 조건이 일치하는 경우에만 보안 인시던트가 생성되도록 필터링 조건을 설정합니다.

시작하기 전에

필요한 역할: sn_si.ingestion_profile_admin

> **주:**
> sn_si.admin 역할은 기본적으로 필수 권한을 상속하므로 sn_si.admin 역할을 가진 사용자는 프로필 관리자가 사용할 수 있는 모든 작업을 수행할 수 있습니다.

이 태스크 정보

이러한 유형의 필터링은 보안 인시던트를 격리하고 생성하는 보안 인시던트 수를 제한하는 데 도움이 됩니다. 추가 필터링 기준을 설정하면 쿼리 또는 트리거된 탐지 구성을 변경할 필요 없이 필요한 탐지만 수집됩니다.

프로시저

1. 보안 인시던트가 생성되도록 들어오는 CrowdStrike Next-Gen 탐지가 충족해야 하는 기준을 정의하려면 조건을 기준으로 필터링을 선택합니다.

   필터 조건의 첫 번째 필드에 있는 옵션은 수집한 탐지에 대한 CrowdStrike 차세대 샘플 탐지 수집 섹션에 표시되는 필드와 일치합니다. 이러한 필드는 동적이며 수집하는 탐지에 따라 변경됩니다. 입력하는 기준은 대/소문자를 구분합니다. 정의하는 기준이 탐지 값과 일치하는지 확인합니다.

   값이 여러 개인 다음 필드에 *## ## ## detection_id* 사용합니다.

   - composite_id
   - host_names
   - seconds_to_resolved
   - seconds_to_triaged

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필터 조건은 문자열만 검색할 수 있으므로 데이터가 올바르게 필터링되도록 위 필드에 `detection_id` 필터 조건을 사용해야 합니다.

2. 조건 작성기의 목록과 필드를 사용하여 첫 번째 행의 필터를 설정합니다.
3. 조건을 더 추가하려면 **AND** 또는 **OR**을 클릭합니다.
   - **AND**를 선택하면 모든 조건이 일치해야 합니다.
   - **OR**을 선택하면 두 조건을 일치시킬 수 있습니다.
4. 두 번째 필터 조건을 설정하려면 새 기준을 클릭합니다.

집계 조건 정의

중복될 가능성이 있는 유사 탐지를 생성하는 대신 수신 탐지를 기존 SIR 보안 인시던트로 집계하는 추가 인시던트 집계 기준을 정의합니다. 각 프로파일에 대해 필드 일치 값 기준을 사용하는 경우 이 추가 집계는 모든 관련 탐지 데이터를 단일 보안 인시던트에 배치하여 활성 상태의 중복 보안 인시던트 수를 줄일 수 있습니다.

시작하기 전에

필요한 역할: sn_si.ingestion_profile_admin

> **주:**
> sn_si.admin 역할은 기본적으로 필수 권한을 상속하므로 sn_si.admin 역할을 가진 사용자는 프로필 관리자가 사용할 수 있는 모든 작업을 수행할 수 있습니다.

이 태스크 정보

새 인시던트가 매핑 단계의 집계 필드 조건에서 선택한 모든 값과 일치하는 경우, 인시던트는 동일한 필드 값을 사용하여 가장 최근에 열린 보안 인시던트에 자동으로 추가됩니다. 보안 인시던트를 담당하는 sn_si.ingestion_profile_admin 역할을 가진 사용자는 보안 인시던트의 관련 목록에서 추가된 모든 집계 인시던트를 볼 수 있습니다.
보안 인시던트에 대한 모든 집계 인시던트가 집계된 인시던트 관련 목록에 표시됩니다 CrowdStrike Next-Gen SIEM . 이 목록은 관련 타임스탬프 및 집계된 필드 값에 대해 자세히 설명합니다. 이 정보는 기존 보안 인시던트에 인시던트가 추가되는 이유를 이해하는 데 도움이 됩니다.

프로시저

1. 새 인시던트를 생성하는 대신 수신 CrowdStrike Next-Gen SIEM 탐지를 미해결 보안 인시던트에 추가할 수 있는 추가 인시던트 필드 기준을 정의하려면 다음 그림과 같이 집계 조건 옵션을 선택합니다.
2. 일치하는 값이 있는 인시던트 필드 필드에 인스턴스의 기존 보안 인시던트 ServiceNow AI Platform와 일치시키려는 필드 값을 입력합니다.
   집계 기준이 충족되고 이 수신 인시던트를 기존 보안 인시던트에 추가할 수 있도록 다중 선택 입력 필드에서 선택한 모든 필드 값이 일치해야 합니다. 이 선택은 여러 필드 값을 가질 수 있는 옵저버블 및 구성 항목과 같은 필드가 매핑되는 *AND* 조건을 의미합니다. 값의 하위 집합만 일치 CrowdStrike Next-Gen SIEM 하면 인시던트 집계 조건이 충족되지 않고 새 보안 인시던트가 생성됩니다.
3. 여러 필드 일치 조건을 추가하려면 새 기준 추가를 클릭합니다.
   사용자가 정의하는 다중 선택 필드 조건 중 하나가 충족되면 집계가 발생합니다. 이 선택은 *OR* 조건을 의미합니다.
4. 새 인시던트가 보안 인시던트에 추가될 때 해당 인시던트에 대한 작업 메모를 업데이트하려면 새 인시던트에 대한 작업 메모 기록을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업 메모는 새 인시던트가 추가되었음을 기록하고 인시던트 상세 정보에 대한 링크를 포함합니다. 로그 작업 메모는 매핑 섹션의 작업 메모 필드에 추가하는 상세 정보도 업데이트합니다.

5. 일정을 구성하려면 계속을 클릭합니다.

다음에 수행할 작업

프로파일의 기준과 일치하는 인시던트 데이터 및 수집된 인시던트를 검색하도록 일정을 설정합니다.

탐지 검색 예약

테넌트에서 탐지를 CrowdStrike Next-Gen SIEM 끌어오는 방법과 시기를 정의하는 일정을 구성합니다.

시작하기 전에

필요한 역할: sn_si.ingestion_profile_admin

주:
sn_si.admin 역할은 기본적으로 필수 권한을 상속하므로 sn_si.admin 역할을 가진 사용자는 프로파일 관리자가 사용할 수 있는 모든 작업을 수행할 수 있습니다.

프로시저

1. 필터링 및 집계 기준의 이전 섹션에서 계속하지 않는 경우 정의하고 있는 프로파일에 액세스합니다.
   a. 다음으로 이동 모두 〉 *CrowdStrike Next-Gen SIEM* 〉 탐지 프로파일.
   b. 계속 정의할 프로파일을 선택합니다.
   c. 진행률 표시줄에서 스케줄링을 선택합니다.
2. 예약 양식의 필드에 내용을 입력합니다.

CrowdStrike Next-Gen SIEM 일정 양식

필드	설명
진행 중인 탐지 수집	인스턴스가 새 탐지를 위해 테넌트에서 끌어오는 지속적 탐지 수집 ServiceNow AI Platform 을 CrowdStrike Next-Gen SIEM 설정하는 옵션입니다. 트리거된 탐지가 발견되고 탐지 생성 필터링 기준이 일치하면 보안 인시던트가 생성됩니다.
폴링 증분(분)	분 단위로 정의된 폴링 빈도입니다.
탐지 수집 시간 설정	초기 수집에 대한 날짜 및 시간을 추가하는 옵션입니다.
초기 탐지 수집 시간	탐지 수집을 위해 지정하는 날짜 및 시간입니다.
일회성 검색	탐지 기록을 CrowdStrike Next-Gen SIEM 1회 검색한 후 데이터를 조정하는 옵션입니다. 데이터를 처리할 때 진행 중인 탐지 데이터와 기록 데이터를 모두 끌어옵니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	주: 검색된 이력 CrowdStrike Next-Gen SIEM 탐지는 애플리케이션 내에서 보안 인시던트 응답 중복을 방지하기 위해 중복 제거 검사를 거칩니다.
날짜 이후	에서 CrowdStrike Next-Gen SIEM탐지 이력을 수집한 이후의 날짜입니다.

3. 계속을 선택하여 프로필의 이 섹션을 완료합니다.

다음에 수행할 작업
탐지 업데이트 및 종결 자동화

탐지 업데이트 및 종결 자동화

인시던트 상태에 따라 탐지 업데이트 및 종결을 자동화합니다 보안 인시던트 응답 . 통합을 CrowdStrike Next-Gen SIEM 통해 탐지에서 보안 인시던트를 생성하고 인시던트가 생성되거나 종결된 후에 업데이트할 수도 있습니다.

시작하기 전에
필요한 역할: sn_si.ingestion_profile_admin

주:
sn_si.admin 역할은 기본적으로 필수 권한을 상속하므로 sn_si.admin 역할을 가진 사용자는 프로파일 관리자가 사용할 수 있는 모든 작업을 수행할 수 있습니다.

프로시저

1. 예약 프로세스의 이전 섹션에 이어 계속하지 않는 경우 정의하는 프로파일에 액세스합니다.
   a. 다음으로 이동 모두 〉 *CrowdStrike Next-Gen SIEM* 〉 탐지 프로파일.
   b. 계속 정의할 프로파일을 선택합니다.
   c. 진행률 표시줄에서 추가 옵션을 선택합니다.
2. 양식에서 필드를 채웁니다.

탐지 업데이트 자동화 양식

범주	필드	설명
보안 인시던트 작성 업데이트	SIR 인시던트 생성 시 CrowdStrike 차세대 탐지 상태 업데이트	자동 탐지 업데이트 기능을 사용하는 옵션입니다. CrowdStrike Next-Gen SIEM 탐지 상태는 에서 ServiceNow AI Platform인시던트가 생성된 후 SIR 설명으로 탐지에서 CrowdStrike Next-Gen SIEM 업데이트됩니다.
	초기 탐지 상태 업데이트	환경에서 업데이트된 CrowdStrike Next-Gen SIEM 초기 탐지 상태(신규 또는 진행 중)입니다.
	탐지에 다시 게시된 초기 설명	환경에서 탐지 CrowdStrike Next-Gen SIEM 에 게시되는 초기 코멘트입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

범주	필드	설명
탐지 종결 업데이트	SIR 인시던트 종결 시 CrowdStrike 차세대 탐지 종결	자동 탐지 상태 업데이트 기능을 사용하는 옵션입니다. CrowdStrike Next-Gen SIEM 탐지는 에서 인시던트가 종결된 후 SIR 제공된 설명과 함께 포털에서 종결 CrowdStrike Next-Gen SIEMServiceNow AI Platform됩니다.
	종결 탐지 상태 업데이트	에서 보안 인시던트가 종결SIR된 경우 탐지의 CrowdStrike Next-Gen SIEM 상태 업데이트 .
	종결 설명 탐지에 다시 게시됨	에서 보안 인시던트가 종결SIR될 때 탐지에서 탐지에 CrowdStrike Next-Gen SIEM 게시된 코멘트입니다.
종결된 탐지 끌어오기	종결된 탐지 끌어오기	진행 중인 수집 및 일회성 검색 중에 종결된 탐지를 가져오는 옵션입니다. 종결 SIR 된 인시던트는 다음의 새 데이터로 업데이트되지 않습니다. CrowdStrike Next-Gen SIEM
탐지 설명 및 SIR 작업 메모 동기화	CrowdStrike 차세대 탐지 의견으로 SIR 자동화 활동 업데이트	자동화 활동에서 SIR 코멘트를 업데이트하는 CrowdStrike Next-Gen SIEM 옵션입니다. 자동화 활동의 코멘트 SIR 는 `CrowdStrike# ###` 프리픽스와 함께 나타납니다.
	SIR 작업 메모로 탐지 설명 업데이트 CrowdStrike Next-Gen SIEM	탐지 코멘트에서 CrowdStrike Next-Gen SIEM 작업 메모를 업데이트하는 SIR 옵션입니다. 의 주석은 CrowdStrike Next-Gen SIEM`ServiceNow# ##` 프리픽스와 함께 나타납니다.

3. 마침을 선택합니다.
4. 프로파일을 활성화합니다.
   a. 진행률 표시줄의 이름 섹션을 선택합니다.
   b. 활성 확인란을 선택합니다.
   c. 계속을 선택합니다.

CrowdStrike Falcon X Sandbox for Security Operations 통합

CrowdStrike Falcon X 샌드박스 통합을 보안 운영 위해 보안 인시던트 응답 프로세스의 일부로 파일과 URL을 제출하여 상세한 멀웨어 및 위협 분석을 수행할 수 CrowdStrike Falcon X 샌드박스 있습니다.

통합은 CrowdStrike Falcon X 샌드박스 맬웨어 분석을 수행하고 통합을 통해 보안 인시던트에 ServiceNow 결과를 제공할 수 있는 온디맨드 격리된 가상 환경을 제공합니다.

맬웨어 인시던트를 제출하면 보안 인시던트 기록의 일부로 유지됩니다. 이러한 기록을 사용하거나 향후 인시던트 해결에 사용하고파일 및 URL의 제출을 자동화할 수 있습니다.

통합은 피싱 및 맬웨어 응답 플레이북 의 자동화를 지원하여 센터 직원이 보안 인시던트에 보다 생산적이고 효율적으로 대응할 수 보안 운영 있도록 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주요 이점

그의 통합을 통해 다음을 수행할 수 있습니다.

- 사용자가 보고한 피싱(URP), 이메일 메시지, 첨부 파일 및 기타 보안 인시던트의 파일 및 URL 제출을 자동화합니다.
- 업데이트된 분석을 위해 이전에 분석한 파일 및 URL을 수동으로 제출하거나 다시 제출합니다.
- 운영 체제, 검사 유형 및 런타임 옵션과 같은 제출 매개변수를 자동으로 적용하는 CrowdStrike Falcon X 샌드박스 여러 제출 구성을 만듭니다.
- 인시던트 내에서 맬웨어 및 위협 결과를 HTML 형식의 보고서로 분석합니다 SIR . 여러 번 분석된 파일 및 URL에 대한 조회 결과와 표시기 이력을 볼 수 있습니다.
- 제출 처리 상태와 위협 찾기 결과로 인시던트에 태그를 지정합니다 ServiceNow .

참고 항목

문서 식별자	문서 제목
CrowdStrike Falcon X 샌드박스	CrowdStrike Falcon Sandbox FAQ
ServiceNow 제품 설명서 웹 사이트	ServiceNow 제품 설명서 웹 사이트

통합 시작하기 **CrowdStrike Falcon X** 샌드박스

인스턴스 및 보안 인시던트 응답 제품과 인터페이스 ServiceNow 하도록 활성화하고 설정합니다CrowdStrike Falcon X 샌드박스.

시작하기 전에

- 보안 운영 통합을 사용하려면 CrowdStrike Falcon X 샌드박스먼저 ServiceNow Store에서 다운로드해야 합니다.
- 다음 설정 검사 목록을 검토하고 원활한 CrowdStrike Falcon X 샌드박스 통합을 위한 모든 작업을 완료했는지 확인합니다.

필요한 역할: admin, sn_si.admin

검사 목록

설정 작업	설명
필수 ServiceNow AI Platform 및 보안 인시던트 응답 역할을 할당했는지 확인합니다.	예상 결과를 구성하고 검증하려면 다음 역할이 필요합니다. • 관리자(admin)는 ServiceNow 앱 스토어에서 sandbox 통합을 설치하고 보안 인시던트 관리자(sn_si.admin) 역할을 할당합니다. • sn_si.admin은 구성 및 전역 설정을 생성하고 편집한 다음 보안 인시던트 분석가(sn_si.analyst) 역할을 할당합니다. • 보안 인시던트 분석가(sn_si.analyst)는 파일 및 URL을 앤드박스에 제출하고 제출 결과를 분석하는 등 보안 인시던트 에 대응합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

검사 목록

설정 작업	설명
ServiceNow 이 통합을 구성하기 전에 통합을 지원하는 데 필요한 핵심 애플리케이션이 설치되고 활성화되었는지 확인합니다.	이 통합은 및 Orlando 릴리스에서 Paris 지원됩니다. 이러한 종속 플러그인이 설치되어 있는지 확인합니다. 이러한 플러그인을 사용하면 작업 및 플로우를 통합 허브 실행할 수 있습니다. • ServiceNow 통합 허브 작업 단계 - REST(com.glide.hub.action_step.rest) • ServiceNow 통합 허브 런타임 (com.glide.hub.integration.runtime) 주: 플러그인을 찾을 수 없으면 담당자에게 요청 ServiceNow 해야 할 수 있습니다. 플러그인을 요청하려면 플러그인 요청 의 단계를 따르십시오. 플러그인(com.snc.security_incident)이 보안 인시던트 응답 필요합니다. 이 플러그인은 제품을 지원하는 데 필요한 모든 종속성을 보안 인시던트 응답 자동으로 설치합니다. 통합에 필요한 다른 보안 운영 애플리케이션을 설치하고 활성화하기 전에 이 플러그인을 설치하고 활성화합니다. 에서 ServiceNow Store다음 보안 운영 애플리케이션이 설치되고 활성화되는지 확인합니다. 설치되지 않은 경우 원활한 설치를 위해 다음 순서로 한 번에 하나의 애플리케이션을 설치하고 활성화합니다. **1.** 보안 인시던트 응답 의존성(com.snc.si_dep) **2.** 보안 통합 프레임워크 **3.** Security Support Common **4.** 보안 지원 오케스트레이션 **5.** 위협 인텔리전스공통 지원(샌드박스 통합 기능에 필요) **6.** Trusted Security Circles **7.** 보안 운영 설정 도우미 **8.** 보안 인시던트 응답 통합을 위한 인스턴스 설정에 ServiceNow AI Platform 대한 자세한 내용은 보안 운영 제품 또는 애플리케이션에 대한 권리 얻기 및

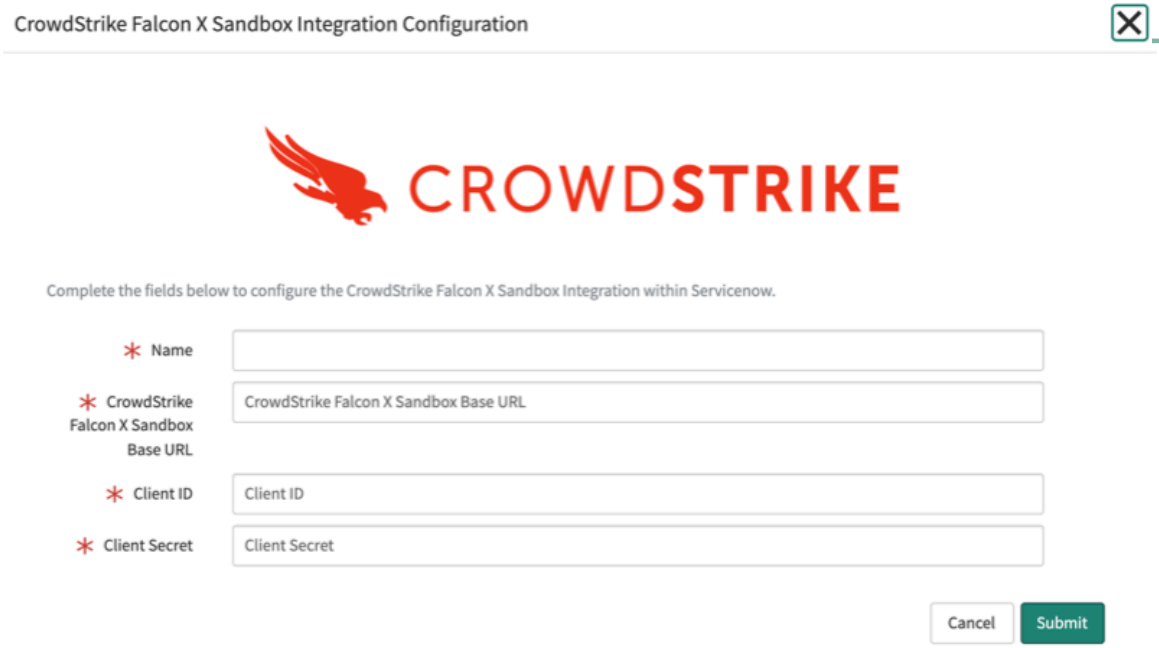
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

검사 목록

설정 작업	설명
	ServiceNow Store 애플리케이션 활성화를 참조하십시오.
Falcon Sandbox 프라이빗 API 키에 대한 라이선스가 있는지 확인하고 전체 API 키를 가져옵니다CrowdStrike Falcon X 샌드박스.	이 통합은 Falcon Sandbox 프라이빗 클라우드만 지원합니다. 주: 이 릴리스는 Falcon X 통합을 지원하지 않습니다. CrowdStrike Falcon X 샌드박스 는 자체 서명된 제한된 API 키와 업그레이드된 전체 API 키를 제공합니다. 자동화된 제출에 대한 무제한 액세스를 활성화하므로 이 통합에 전체 API 키를 사용합니다. 자세한 내용은 CrowdStrike Falcon Sandbox 지식베이스 를 참조하십시오.

프로시저

1. ServiceNow Store에서 보안 운영용 CrowdStrike Falcon Sandbox 통합을 다운로드합니다.
2. 설치가 완료되면 보안 운영 〉 통합 〉 통합 구성으로 이동합니다.
3. 통합 타일을 CrowdStrike Falcon X 샌드박스 검색하고 구성을 클릭합니다.

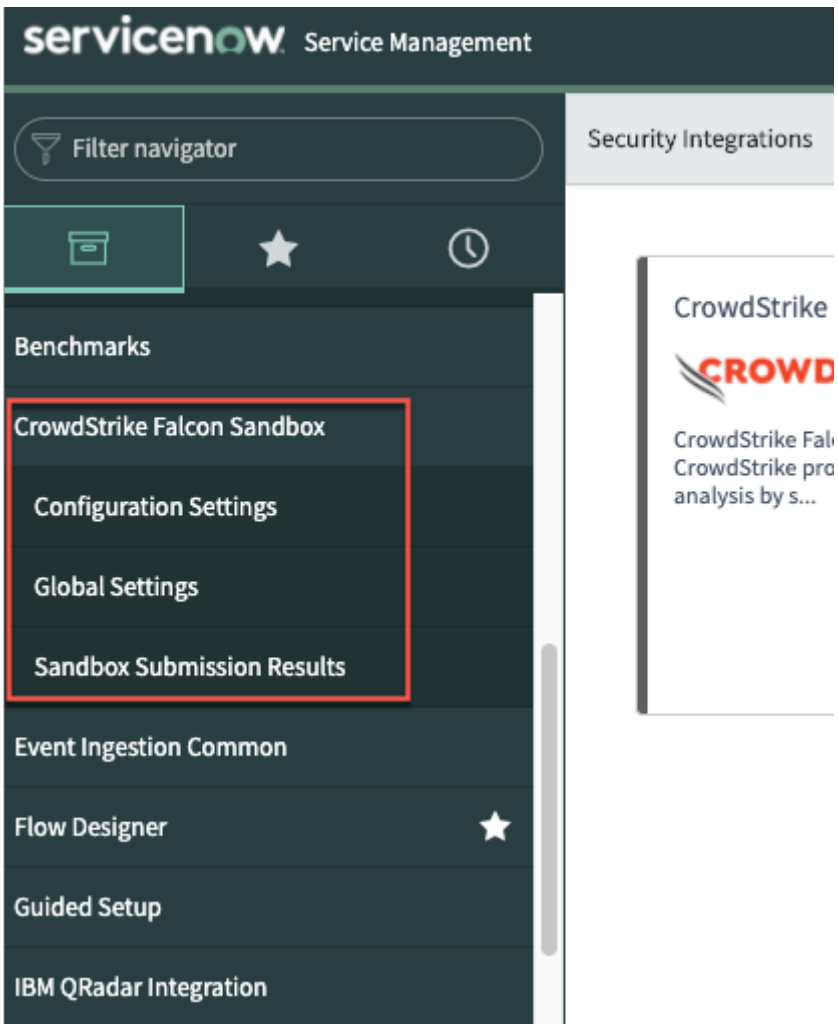


4. 구성을 완료하려면 다음 상세 정보를 입력하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
이름	이 통합의 이름입니다(예: demo-1). Sandbox 구성을 식별하는 고유한 이름이지만 ServiceNow 인스턴스당 하나의 통합만 구성할 수 있습니다.
CrowdStrike Falcon Sandbox 기본 **URL**	Sandbox 기본 URL입니다. 이 URL은 sandbox를 구성한 후에 사용할 수 있습니다.예를 들어 https://servicenow.falcon-sandbox.com 은 기본 URL입니다.
클라이언트 **ID**	OAuth2 API 클라이언트 ID입니다. 자세한 내용은 API 클라이언트 및 키를 참조하세요.
클라이언트 비밀	OAuth2 API 클라이언트 비밀 키입니다. 자세한 내용은 API 클라이언트 및 키를 참조하세요.

5. 제출을 클릭합니다.
샌드박스가 성공적으로 확인되고 제출되면 보안 통합 페이지에 타일로 저장됩니다. 이제 애플리케이션 내비게이터에서 샌드박스 모듈을 볼 수 있습니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 수행할 작업
통합을 성공적으로 완료한 후 다음 단계는 샌드박스 제출 구성을 설정하는 것입니다.

샌드박스 제출 구성 설정

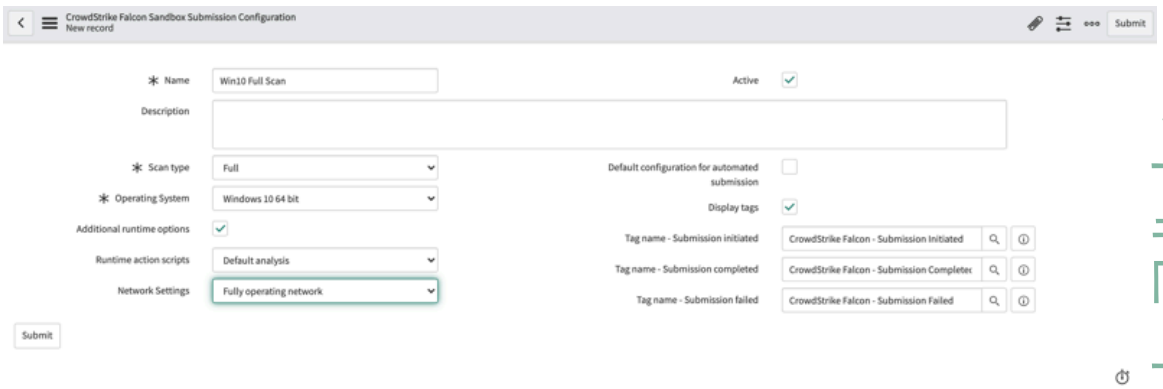
샌드박스 구성을 설정하여 맬웨어 분석을 위한 보안 인시던트 기록 제출에 대한 분석 환경 및 런타임 옵션을 정의합니다.

시작하기 전에
필요한 역할: sn_si.admin

이 태스크 정보
통합을 사용하여 파일 또는 URL CrowdStrike Falcon X 샌드박스 을 제출하려면 먼저 하나 이상의 제출 구성을 구성해야 합니다. 제출 구성은 샌드박스 운영 체제, 검사 유형, 실행 시간 옵션 및 기타 인시던트 처리 특성을 정의합니다. 환경에서 사용할 수 CrowdStrike Falcon X 샌드박스 있는 다양한 옵션을 사용하기 위해 여러 구성을 생성할 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 **CrowdStrike Falcon X** 샌드박스 〉 구성 설정.
2. 새로 만들기를 클릭합니다.



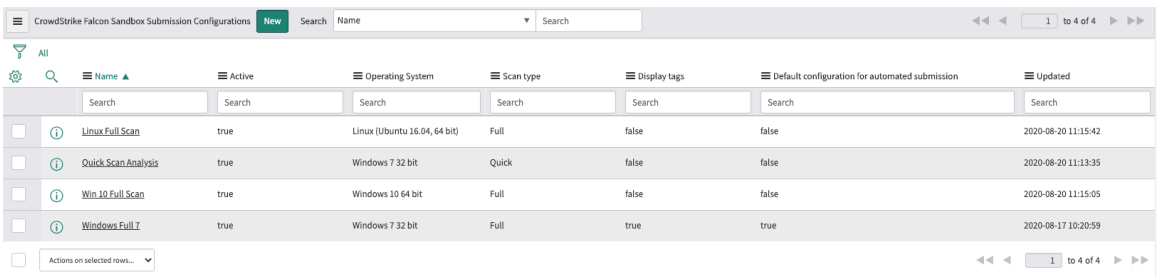
3. 전체 스캔 유형에 대한 구성을 작성하려면 다음 필드를 완료하십시오.

필드	설명
이름	제출 구성의 고유한 이름입니다. 이 이름은 분석가가 파일을 제출할 때 나타납니다. 이름이 설명적이고 다른 구성과 쉽게 구분할 수 있는지 확인하는 것이 중요합니다(예: Win 10 전체 스캔). 이름이 고유하지 않으면 오류가 나타나고 중복된 구성 기록 이름은 저장되지 않습니다.
스캔 유형	S는 전체로 입력할 수 있습니다. 빠른 검사 유형은 제한된 위협 분석을 제공합니다.
운영 체제	sandbox가 파일 또는 URL을 검사하는 nalysis VM 환경입니다.
활성	파일 또는 URL을 수동으로 제출할 때 선택하는 항목입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
자동화된 제출에 대한 기본 구성	기본적으로 지워지는 Option입니다. 이 옵션을 선택하면 맬웨어 분석 제출을 자동화하는 데 이 구성을 사용할 수 있습니다. 주: 자동화된 제출의 기본 구성으로 활성 제출 구성을 하나만 사용할 수 있습니다.
태그 표시	기본적으로 지워지는 Option입니다. 이 옵션을 선택하면 파일 또는 URL 제출 상태를 제공하는 태그가 표시됩니다. 분석을 처리하는 데 몇 분 정도 걸릴 수 있습니다. 표시 태그는 제출 시작됨, 제출 완료됨 또는 제출 실패입니다.
추가 런타임 옵션	기본적으로 지워지는 Option입니다. 이 옵션을 선택하면 샌드박스가 지원하는 추가 런타임 파라미터를 사용할 수 있습니다.
런타임 동작 스크립트	분석 중에 인간의 행동을 시뮬레이션하고 파일 또는 URL과 상호 작용하는 ction 스크립트를 사용할 수 있도록 하는 옵션입니다. https://www.crowdstrike.com/endpoint-security-products/falcon-sandbox-malware-analysis/ 자세한 내용은 설명서를 참조하십시오 CrowdStrike Falcon X 샌드박스 .
네트워크 설정	Sandbox에 URL 또는 파일을 제출하는 동안 사용되는 네트워크 설정 유형을 선택할 수 있는 옵션입니다.

4. 제출을 클릭합니다.
구성을 제출하면 구성 설정 페이지에 기록으로 저장됩니다. andbox 제출에 사용하려면 구성이 활성 상태여야 합니다.



다음에 수행할 작업
s andbox 제출을 구성한 후 다음 단계는 파일 또는 ULR을 Sandbox에 수동으로 제출하는 것입니다

.

Sandbox에 수동으로 파일 또는 **URL** 제출

범주가 피싱임과 같은 특정 인시던트 기준이 충족되면 파일 또는 URL을 샌드박스에 수동으로 제출할 수 있습니다.

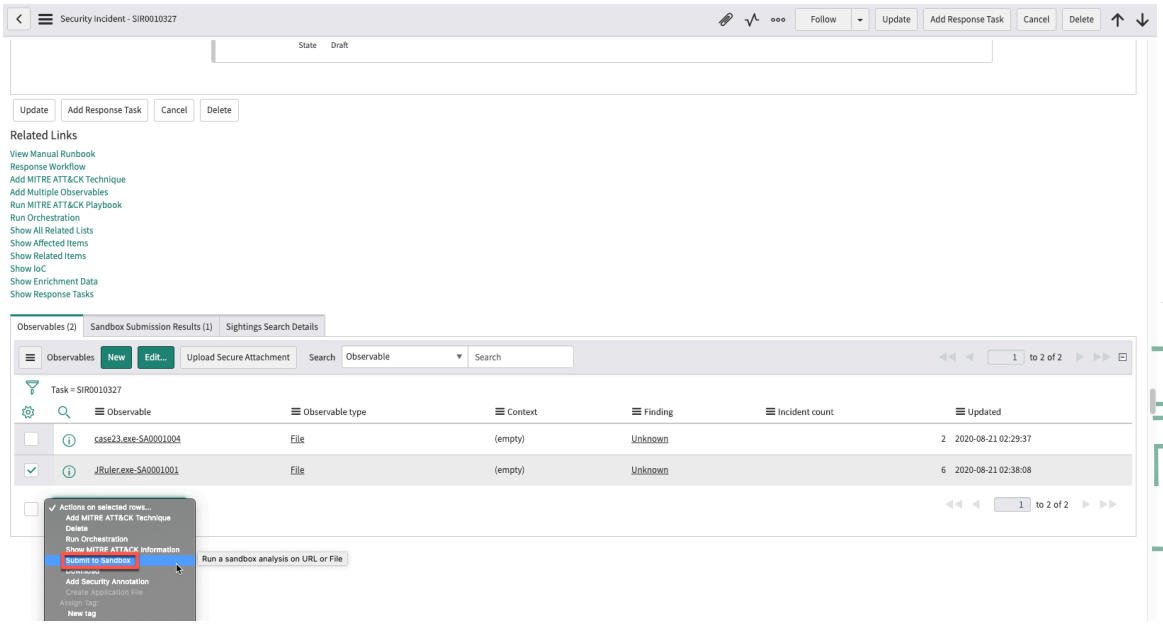
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_si.analyst

이 태스크 정보
보안 인시던트 및 파일 또는 URL을 검토한 후 Sandbox에 제출 옵션을 선택하여 맬웨어 분석을 수행할 수 있습니다.

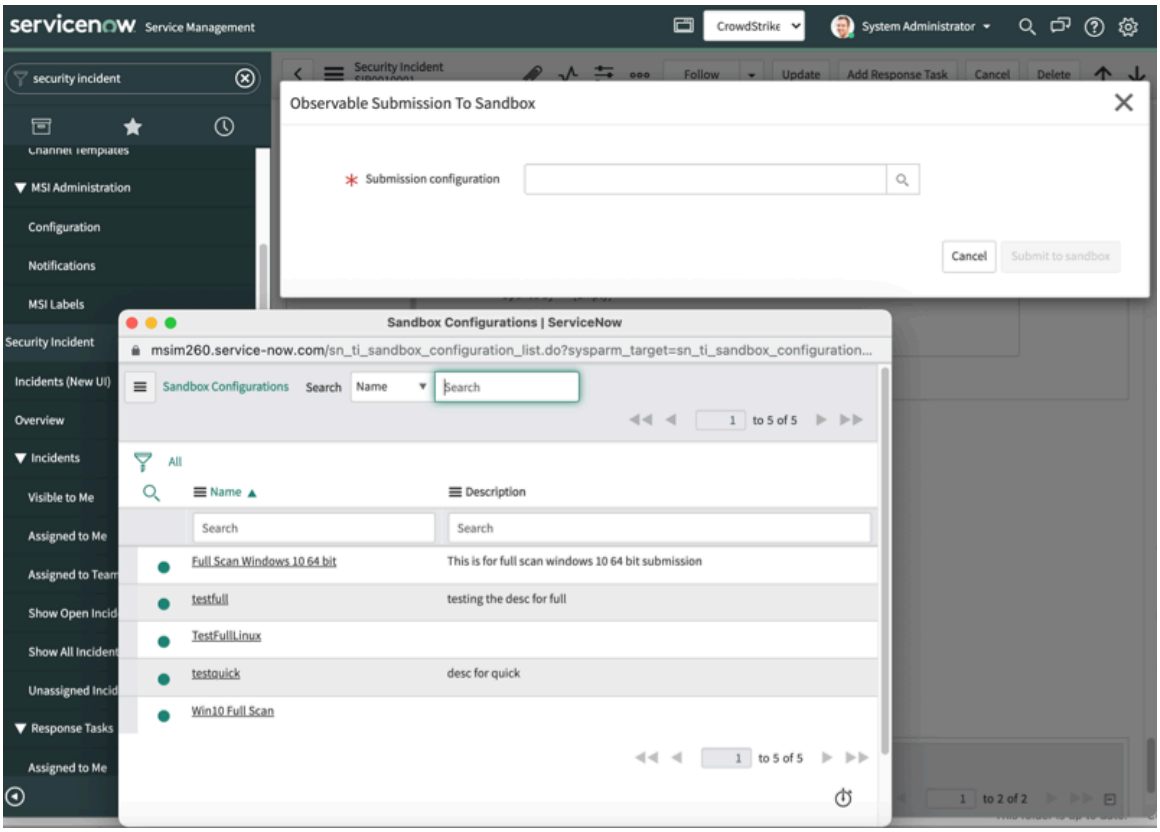
프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 인시던트 〉 모든 인시던트 표시 및 파일 또는 URL 옵저버블 유형 기록을 제출할 보안 인시던트를 엽니다.
2. **IoC** 표시 관련 링크를 클릭합니다.
3. 옵저버블 탭에서 멀웨어 또는 위협 분석을 수행할 기록을 하나 또는 여러 개 선택하고 Sandbox에 제출을 클릭합니다.

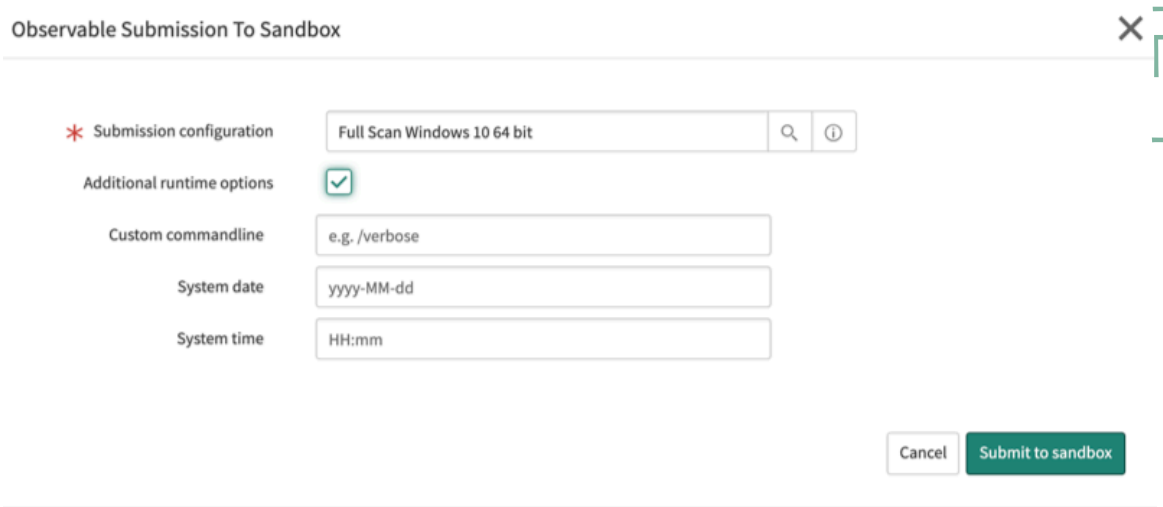


4. 파일 제출 필터가 나타나면 제출 구성에서 원하는 샌드박스 구성을 선택하고 샌드박스에 제출을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



5. 옵션: 추가 사용자 지정 옵션을 제공하려면 추가 런타임 옵션을 선택합니다.



필드	설명
사용자 지정 커맨드 라인	일반 애플리케이션 명령줄 또는 특수 작업입니다.
시스템 날짜	yyyy-MM-dd 형식의 시스템 날짜입니다.
시스템 시간	HH:mm 형식의 시스템 시간입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

제출을 시작한 후에는 작업 메모를 보고 제출 상태를 확인할 수 있습니다. 제출 상태에 대한 자세한 내용이나 결과 분석은 샌드박스 제출 결과를 참조하십시오.

> **주:**
> CrowdStrike Falcon X Sandbox에서는 URL에 대해 빠른 스캔이 지원되지 않습니다.
> 작업 메모에 너무 많은 정보가 있는 경우 필터 옵션을 사용하여 관련된 필수 작업 메모로 드릴다운할 수 있습니다.

다음에 수행할 작업

맬웨어 분석을 위해 옵저버블을 샌드박스에 제출하면 샌드박스 제출 결과를 확인하여 잠재적인 위협에 대한 다음 단계를 수행합니다.

Flow Designer를 사용하여 **Falcon Sandbox** 제출 자동화 **CrowdStrike**

통합에는 CrowdStrike Falcon X 샌드박스 보안 인시던트 기록과 함께 작동하는 를 워크플로우 스튜디오 사용하여 생성된 플로우 템플릿이 포함됩니다.

시작하기 전에

- 샌드박스 제출 구성을 생성했고 한 구성을 자동 제출의 기본 구성으로 활성화했는지 확인합니다. 플로우가 트리거되면 기본 구성에서 샌드박스 제출이 발생합니다.

필요한 역할: sn_si.admin

이 태스크 정보

이러한 플로우는 주로 인시던트 응답 워크플로우의 일부로 파일 또는 URL 제출을 자동화하려는 경우에 시작할 수 있도록 설계되었습니다.
샘플 플로우를 활성화할 때 샘플 플로우에서 보안 인시던트를 피싱으로 정의하면 피싱 파일 첨부 파일이 자동으로 제출됩니다. 또는 이 파일 형식이 옵저버블 기록에 첨부된 경우 모든 .exe 파일을 제출할 수 있습니다.

이러한 샘플 플로우를 수정하여 다양한 조건, 범주, 복합 조건 등에서 자동화된 제출을 트리거할 수 있습니다.

샌드박스 통합은 기본적으로 비활성화되어 있는 두 개의 기본 시스템 플로우로 구성됩니다.

- 범주가 피싱일 때 파일 제출: 이 플로우는 보안 인시던트 범주가 피싱으로 정의되면 맬웨어 분석을 위해 파일을 샌드박스에 제출합니다. 보안 인시던트의 옵저버블 기록에 파일을 첨부해야 합니다. URP(User Reported Phishing) 기능을 사용하는 경우 이메일 첨부 파일이 자동으로 구문 분석되어 SIR 인시던트 기록에 옵저버블 레코드로 추가됩니다. 제출을 자동화하기 위한 추가 조치는 필요하지 않습니다.
- 옵저버블에 대한 파일 형식이 exe인 경우 제출: 이 플로우는 보안 인시던트 옵저버블이 exe인 경우 맬웨어 분석을 위해 샌드박스에 파일을 제출합니다. 피싱 범주 플로우와 마찬가지로 보안 인시던트의 옵저버블 기록에 파일을 첨부해야 합니다. 파일을 업로드하여 수동으로 이 작업을 수행하거나 피싱 이메일 첨부 파일 또는 인시던트를 생성하는 기타 메커니즘이 옵저버블 기록과 연결된 경우 자동으로 이 작업을 수행할 수 있습니다.

플로우가 구성되고 인시던트 조건이 매개변수를 충족하면 보안 인시던트를 검토할 때 샌드박스 제출이 자동으로 트리거됩니다. 제출이 시작되었고, 구성에서 활성화된 경우 태그가 표시되며, 보류 중인 제출 결과 기록을 나타내는 작업 메모를 검토합니다.

샌드박스 통합에는 여러 하위 플로우도 포함되어 있습니다. 하위 플로우는 전체 통합 제출 기능의 내부 구성요소입니다. 보안 기준에 맞게 하위 플로우를 사용자 지정하고 편집할 수 있습니다.

하위 플로우를 참조하여 샌드박스 제출 관련 문제를 해결할 수 있습니다. 하위 플로우를 호출할 때마다 실행 기록이 생성됩니다. 이 기록은 플로우에서 특정 오류가 발생한 위치를 나타내며 문제를 해결할 수 있도록 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

샌드박스 통합 - 다중 워크플로우

Flows Subflows Executions Help + New

All > Application Name contains Sandbox

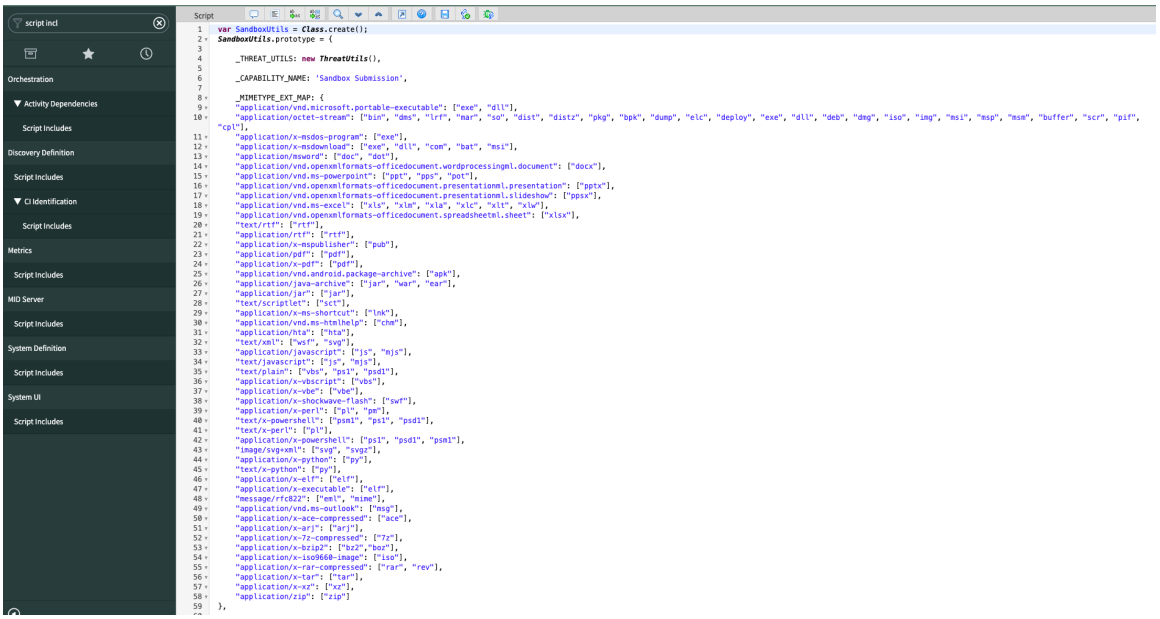
Name ▲	Internal name	Application	Status	Active	Updated	Updated by
Search	Search	*Sandbox	Search	Search	Search	Search
Add submission status tag on SIR	add_submission_status_tag_on_sir	Security Operations CrowdStrike Falcon S...	Published	true	2020-07-16 12:33:57	admin
Aggregate Additional Runtime Options	aggregate_additional_runtime_options	Security Operations CrowdStrike Falcon S...	Published	true	2020-07-16 08:47:54	admin
Connection and Credential Validation	connection_and_credential_validation	Security Operations CrowdStrike Falcon S...	Published	true	2020-05-18 02:52:33	admin
CrowdStrike Falcon Sandbox Poll Submission	crowdstrike_falcon_sandbox_polling	Security Operations CrowdStrike Falcon S...	Published	true	2020-08-02 05:11:53	admin
CrowdStrike Falcon Sandbox Submission	submit_file_to_sandbox	Security Operations CrowdStrike Falcon S...	Published	true	2020-08-13 06:17:57	admin
CrowdStrike Falcon Submission Results	crowdstrike_falcon_submission_results	Security Operations CrowdStrike Falcon S...	Published	true	2020-08-13 06:30:16	admin
CrowdStrike Polling Quick/Full Scan	crowdstrike_polling_quickfull_scan	Security Operations CrowdStrike Falcon S...	Published	true	2020-07-20 20:23:07	admin
Fetch Environment Ids from Sandbox	fetch_environment_ids_from_sandbox	Security Operations CrowdStrike Falcon S...	Published	true	2020-05-25 07:45:54	admin
Submit File or URL to CrowdStrike Quick ...	submit_fileurl_to_crowdstrike	Security Operations CrowdStrike Falcon S...	Published	true	2020-07-20 19:04:42	admin
Submit File/URL to Sandbox	submit_fileurl_to_sandbox	Security Operations CrowdStrike Falcon S...	Draft	true	2020-05-25 07:50:18	admin
Submit Observable for Automated submission	submit_observable_for_automated_submission	Security Operations CrowdStrike Falcon S...	Published	true	2020-08-06 06:15:35	admin

Actions on selected rows... 1 to 11 of 11

주:

- 기본 플로우를 사용자 지정하도록 선택하는 경우 자동 제출을 트리거하기 위해 자동화된 제출에 대한 옵저버블 제출 하위 플로우가 플로우에 포함되어 있는지 확인해야 합니다.
- exe에 대한 파일 확장명을 사용자 지정하고 정의할 수 있습니다. 플로우의 사본 생성 옵저버블의 파일 형식이 exe일 때 제출하고 복사본을 변경합니다. 컨텐츠 유형과 파일 확장자는 SandboxUtils 스크립트에 매핑됩니다. 스크립트 포함에 액세스하려면 시스템 정의 > 스크립트 포함 으로 이동하여 SandboxUtils를 검색하십시오.

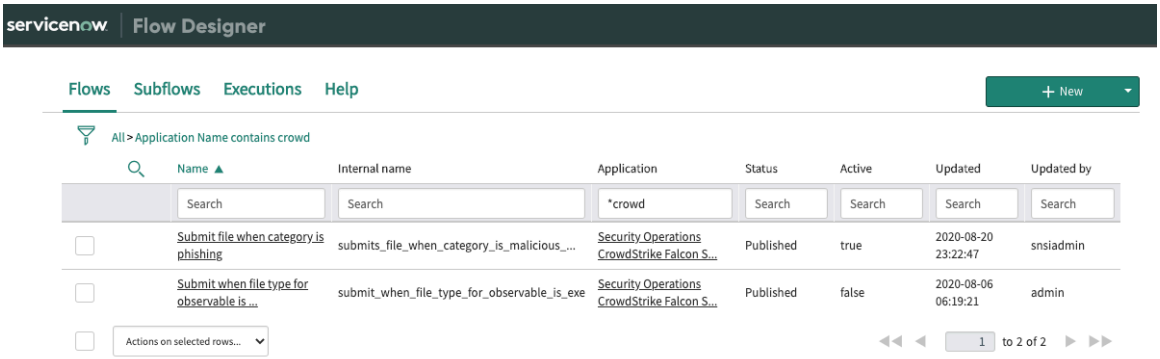
SandboxUtils 스크립트



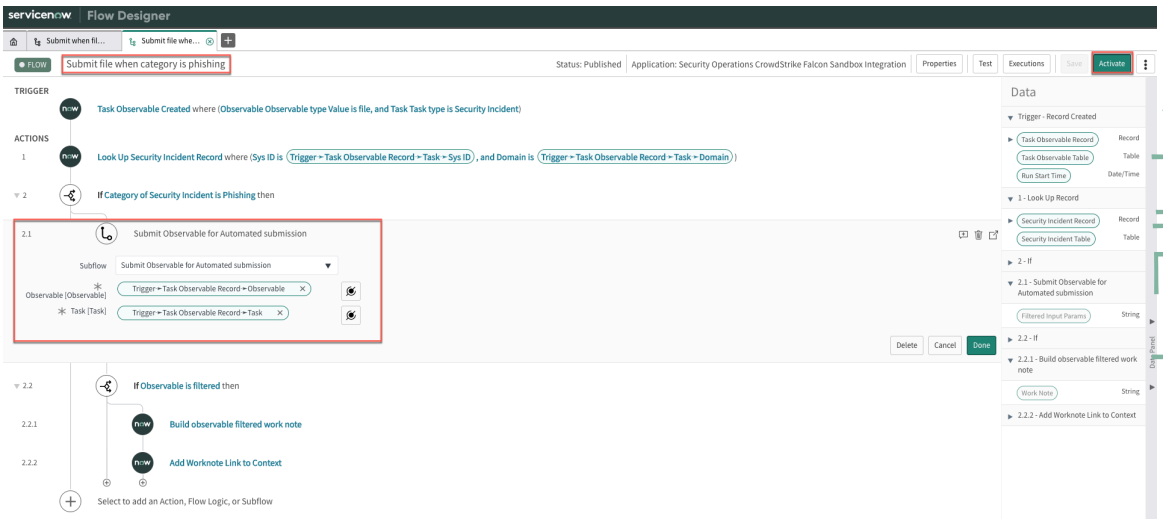
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 플로우 디자이너 〉 디자이너 〉 플로우.
2. 애플리케이션 유형별로 플로우를 필터링합니다.
   예를 들어, *crowd는 두 CrowdStrike Falcon X 샌드박스 플로우를 필터링합니다.



3. 세부 정보를 보려면 플로우를 선택합니다.
   아래 예는 범주가 피싱일 때 파일 제출 플로우를 보여줍니다.



4. 활성화**(Activate)**를 클릭한 후 확인 메시지가 나타나면 확인**(OK)**을 클릭합니다.

다음에 수행할 작업

자동화된 제출 플로우를 구성한 후 샌드박스 제출 결과를 확인하여 위협을 분석할 수 있습니다.

샌드박스에서 제출 결과 모니터링

모든 샌드박스 제출에 대한 결과는 모든 보안 인시던트에 대한 샌드박스 제출 결과 탭에 표시됩니다.

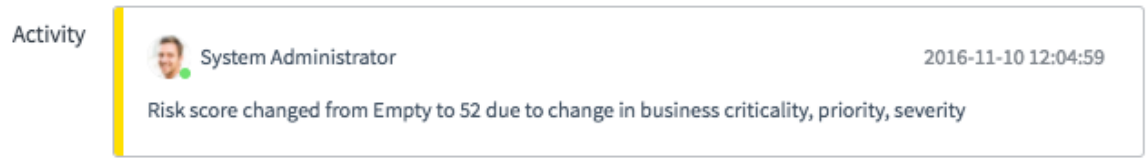
시작하기 전에

필요한 역할: sn_si.analyst

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

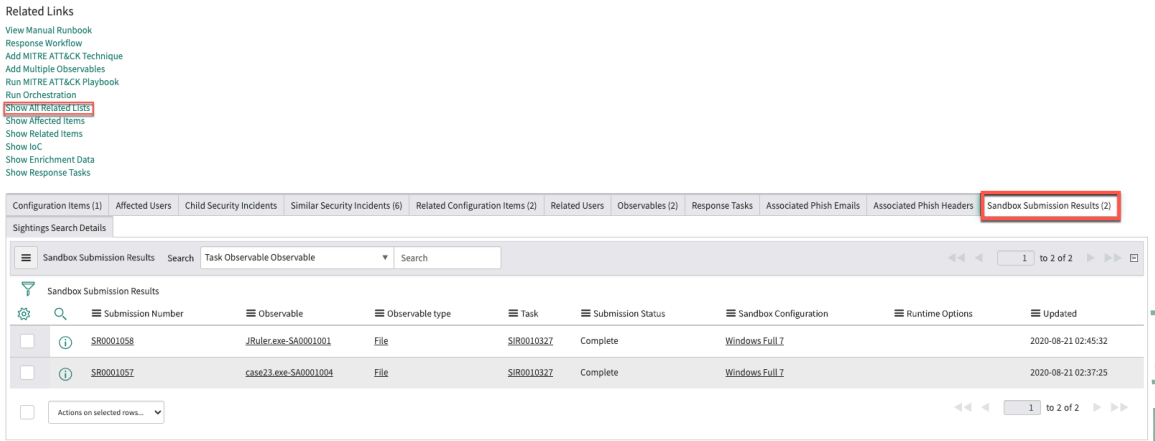
프로시저

1. 작업 중인 보안 인시던트를 열고 SAndbox 제출이 성공적으로 완료되었는지 확인합니다.

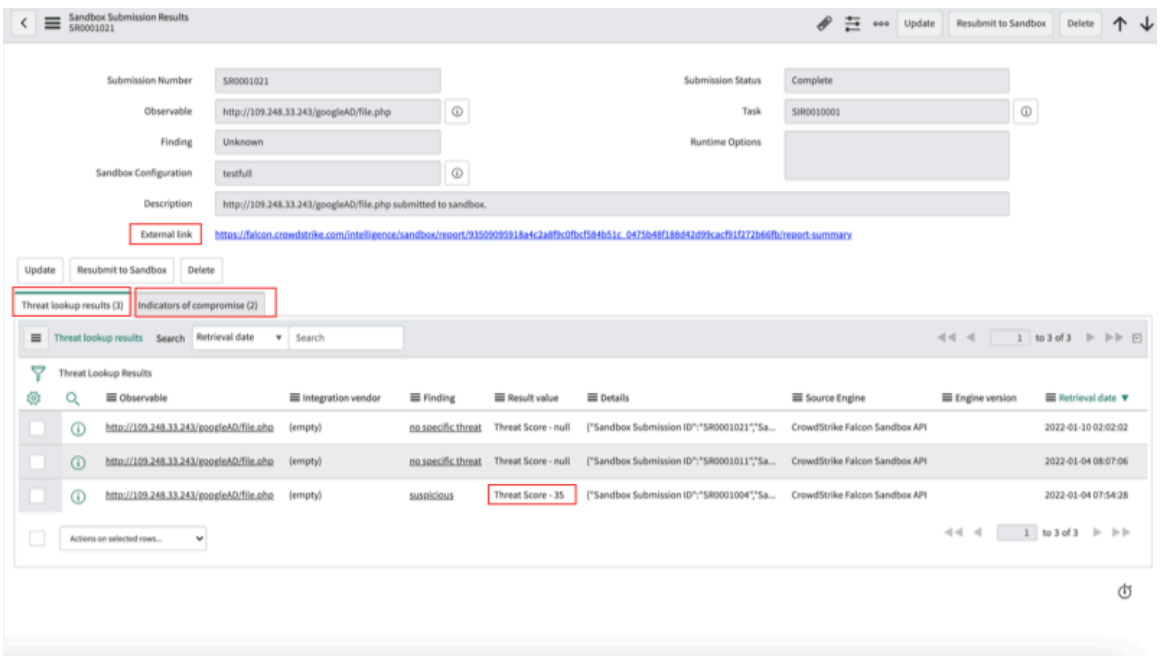


2. 자세한 내용은 Work 메모를 검토하고 검사가 성공했는지 확인할 수 없는 경우 진행 방법을 알아봅니다.

3. 작업메모에서 전체 결과 링크를 클릭하거나 보안 인시던트 하단에서 모든 관련 목록 표시〉 샌드박스 제출 결과로 이동합니다.
결과는 샌드박스 제출 결과 탭에 표시됩니다.



4. 전체 Sandbox 분석을 보려면 기록을 클릭하십시오.



5. 옵션: 샌드박스에 다시 제출을 클릭하여 옵저버블을 다시 처리합니다.

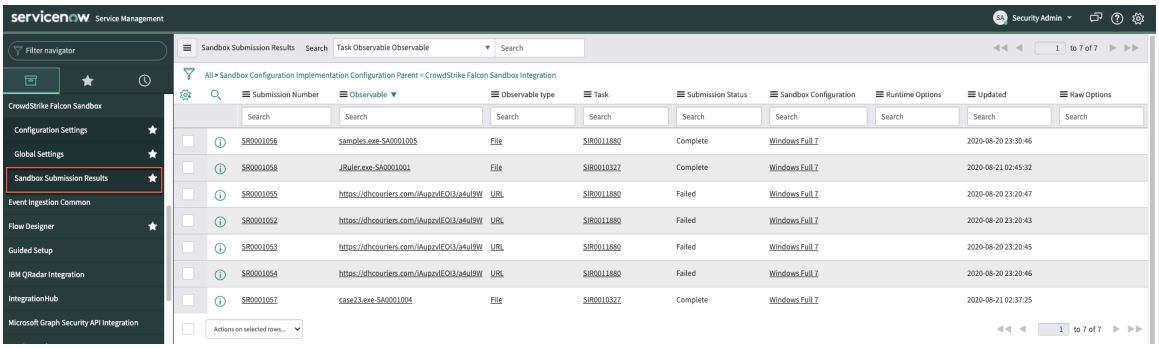
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

결과

- 위협 조회 결과 탭은 악의적인 결과, 위협 점수 및 추가 세부 정보를 포함한 위협 평가를 제공합니다. 이러한세부 정보는 모든 ServiceNow 위협 조회 통합에 대한 표준 위협 조회 형식 구조로 제공됩니다.
- 침해 표시기 탭은 신뢰도 점수와 함께 악성 또는 의심스러운 앤드박스 결과를 제공합니다 . 신뢰 점수는 플랫폼에 저장된 ServiceNow 다른 표시기 정보와 유사합니다. 정보 제공용으로 분류된 표시기는 이 탭에 포함되지 않습니다.
- 외부 링크를 클릭하여 포털에서 샌드박스 결과를CrowdStrike Falcon X 샌드박스 봅니다.

> **주:**
> 이 옵션을 사용하려면 결과를 볼 수 있는 역할이 있어야 CrowdStrike Falcon X 샌드박스 합니다.

다음으로 이동하여 모든 보안 인시던트에 대한 Sandbox 제출 결과를 모니터링할 수도 있습니다. **CrowdStrike Falcon** 샌드박스 〉 샌드박스 제출 결과.



샌드박스 제출 상태로 보안 인시던트에 태그 지정

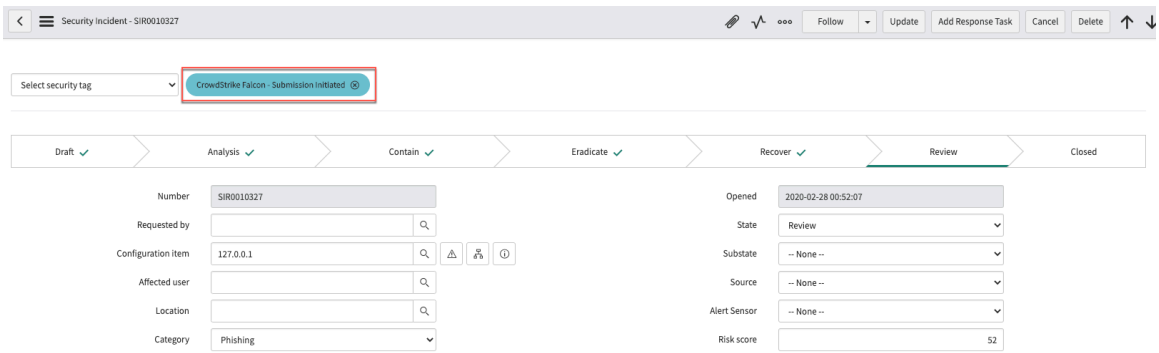
필요에 따라 보안 인시던트에 Submission Initiated 및 Submission Complete 태그를 지정할 수 있습니다.

샌드박스 제출 구성에서 태그 표시 옵션을 선택하면 파일 또는 URL 제출의 상태를 제공하는 태그가 표시됩니다. 이 방법으로 상태를 확인하는 것은 s andbox 분석을 처리하는 데 몇 분 정도 걸릴 수 있으므로유용합니다.

표시 태그는 제출 시작됨, 제출 완료됨 및 제출 실패로 지칭됩니다.

다음 예는 제출이 시작된 보안 인시던트를 보여줍니다.

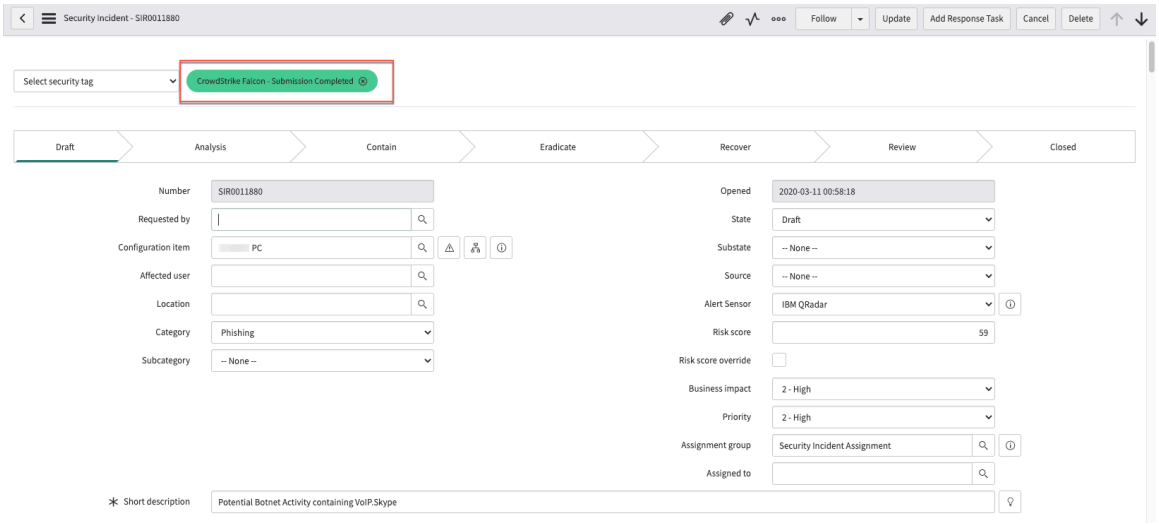
제출 시작됨 - 보안 인시던트



다음 예는 제출이 완료된 보안 인시던트를 보여줍니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

제출 완료됨 - 보안 인시던트



샌드박스 전역 설정 검토

파일 또는 URL 제출 결과에 문제가 있는 경우 전역 샌드박스 설정을 검토하고 수정합니다.

시작하기 전에
필요한 역할: sn_si.admin

프로시저

1. 다음으로 이동 모두 〉 **CrowdStrike Falcon Sandbox** 〉 전역 설정.
2. 양식에서 필드를 채웁니다.

필드	설명
파일 크기 제한(MB)	샌드박스 업로드 파일 크기 제한(MB)입니다. **주:** 기본적으로 256MB의 파일 크기 제한이 구성됩니다. 값을 256MB 이상으로 늘리지 마십시오. 그러나 큰 파일을 전송하지 않도록 최대 파일 크기 제한을 줄일 수 있습니다.
제출 결과의 최대 시간 제한(분)	샌드박스에서 제출 결과의 최대 시간 제한입니다. **주:** 기본 제한 시간은 30분입니다. 결과가 30분 이상 걸리는 경우 시간을 늘릴 수 있습니다. 또한 샌드박스 포털에서 결과를 볼 수 있습니다.

3. 저장을 클릭합니다.

Elasticsearch 인시던트 보강 통합

인시던트 보강 통합은 Elasticsearch 로그를 검색하고 관련 사이팅 정보를 보안 인시던트에 추가합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

탐색	설정
보안 인시던트 응답 통합	• 인시던트 보강 통합 시작하기 Elasticsearch • 사이팅 검색 구성 기록 생성

사용	개발
• 사이팅 검색 실행 • Security Operations Integration - 사이팅 검색 플로우 • 보안 운영 - Elasticsearch 사이팅 검색 플로우	• ServiceNow 보안 운영 통합 개발 가이드라인 • 통합 작성을 위한 팁 • 개발자 교육 • 개발자 설명서 • 애플리케이션과 함께 설치되는 구성요소 찾기

문제 해결 및 도움받기

- 통합 문제 해결
- 보안 운영 커뮤니티에서 질문 또는 답변하기
- 알려진 오류 포털에서 알려진 오류 문서 검색
- 연락처 고객 서비스 및 지원

인시던트 보강 통합 시작하기 **Elasticsearch**

Elasticsearch 는 와 쉽게 통합 보안 운영되는 분산형 RESTful 검색 및 분석 엔진입니다. 인시던트 보강 통합을 사용하려면 Elasticsearch 먼저 다음 ServiceNow Store 에서 다운로드하고 적절한 API 기준 URL 및 로그인 자격 증명을 추가해야 합니다.

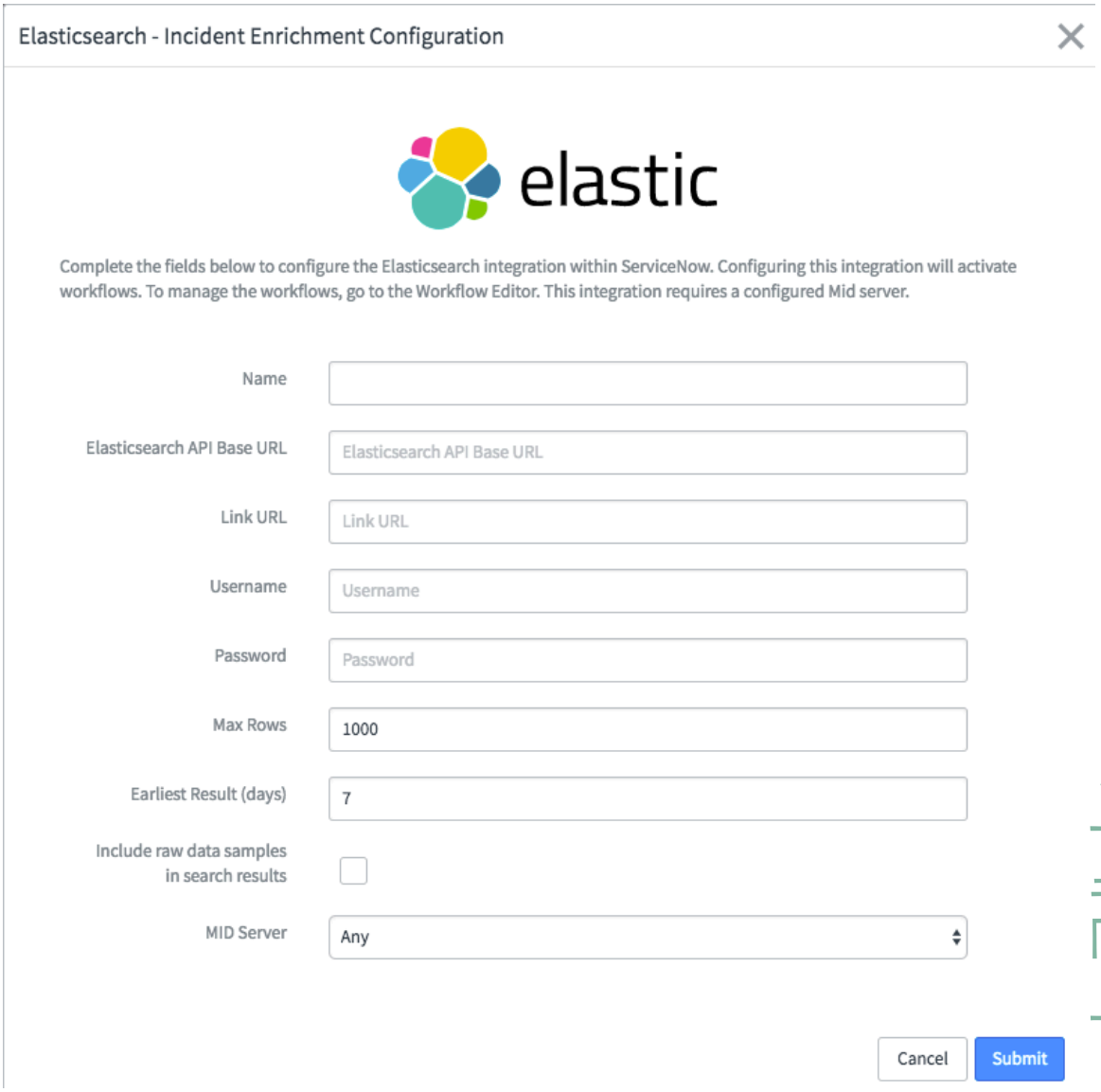
시작하기 전에

필요한 역할: sn_si.admin

프로시저

1. 에서 통합을 다운로드합니다. ServiceNow Store.
2. 설치가 완료되면 Elasticsearch 프로파일에서 API 기준 URL에 액세스하고 Elasticsearch 가져옵니다.
3. 인스턴스에서 다음으로 이동합니다. 보안 운영 〉 통합 〉 통합 구성.
   사용 가능한 보안 통합은 일련의 카드로 표시됩니다.
4. - 인시던트 보강 카드에서 Elasticsearch새로 만들기를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



5. 필요에 따라, 필드를 채웁니다.

필드	설명
이름	이 구성의 이름입니다.
Elasticsearch API 기준 URL	사이트에서 가져온 기본 URL입니다 Elasticsearch .
링크 URL	〔선택사항〕 사용 가능한 경우, Kibana 인스턴스에 대한 링크
사용자 이름	인텔 Elasticsearch 사용자 이름입니다.
암호	인텔 Elasticsearch 암호입니다.
최대 행 수	검색할 행의 최대 수입니다.
가장 빠른 결과(일)	일수 단위로 보려는 가장 빠른 결과입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
검색 결과에 원시 데이터 샘플 포함	사이팅 검색 결과에 원시 데이터 샘플을 포함하려면 이 옵션을 선택합니다. 반환되는 데이터의 양은 보안 인시던트 응답 속성의원시 데이터 속성 행 수의 설정에 따라 달라집니다.
MID 서버	활성 MID 서버를 사용하려면 임의 를 선택하고, 특정 MID 서버 이름을 선택합니다.

주:
이 통합을 구성하면 워크플로우가 활성화됩니다. 워크플로우를 관리하려면 워크플로우 편집기로 이동합니다.

6. 제출을 클릭합니다.
   통합 구성 카드가 표시됩니다.
7. 새 구성 카드를 볼 때 구성 또는 삭제를 클릭하여 구성을 변경하거나 삭제할 수 있습니다.
8. 통합 구성 카드의 원래 목록으로 돌아가려면 구성 표시 드롭다운 목록에서 아니요를 선택합니다.

결과
구성된 후에는 보안 인시던트 응답의 Elasticsearch 감시 목록에 옵저버블을 게시하기 위해 인시던트 보강 통합을 선택할 수 있습니다.

FireEye 엔드포인트 보안 통합

FireEye Endpoint Security(HX 시리즈)는 조직이 모든 엔드포인트에서 알려진 위협과 알려지지 않은 위협을 포함하는 위협을 검사하고 분석할 수 있도록 지원합니다.

오늘날 숙련된 공격자는 대부분의 보안 팀이 엔드포인트를 보호하기 위해 수년 동안 의존해 온 기존 방어를 우회합니다. 전통적인 방어가 알려진 위협을 막을 때조차도 그 위협이 무엇을 하려고 했는지 판단할 수 없습니다. FireEye HX Endpoint Security는 보안 팀이 엔드포인트에 대해 알려지거나 알려지지 않은 지능형 위협을 추적하고 차단하는 데 도움이 됩니다.

와 Gold Standard Security Incident Response 통합을 FireEye HX사용하면 보안 분석가가 도구 사이를 이동할 필요 없이 쉽고 효율적으로 보안 인시던트를 즉시 조사하고 정정할 수 있습니다. 네트워크 포함을 사용하여 엔드포인트에서 업데이트 적용 작업을 수행하고, 호스트에 대한 특정 세부 정보를 수집하는 프로파일을 구현하고, 엔드포인트에서 특정 쿼리 또는 작업을 수행할 수 있습니다.

주요 기능

- 호스트 세부 정보, 네트워크 통계, 사용자 세부 정보, 파일 세부 정보, 프로세스 세부 정보 및 서비스 세부 정보와 같은 엔드포인트에 대한 자세한 정보를 수집하기 위해 호스트 강화 작업을 수행하는 능력.
- 엔터프라이즈 보안 검색을 수행하여 엔드포인트 전반의 잠재적인 악성 옵저버블을 확인하고 정정 작업을 수행하는 기능입니다.
- 심층적인 엔드포인트 검사 및 분석을 위해 분류 및 데이터 수집을 수집하는 능력.

제한

이 통합의 알려진 제한 사항은 다음과 같습니다.

1. MID 애플리케이션 필드 값은 수동으로 입력해야 합니다.
2. Linux 에이전트에서는 호스트 격리 및 실행 중인 서비스 가져오기를 수행할 수 없습니다.
3. 격리 제거는 Linux 에이전트를 지원하지 않습니다.
4. 환자 분류 취득은 Linux 에이전트를 지원하지 않습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. 사용자는 보강 데이터 표시 관련 링크를 구성해야 합니다. 바로 사용할 수 없습니다.
6. 사이팅 검색의 경우 한 번에 5개의 활성 검색만 존재할 수 있습니다. 나머지는 큐에 대기 중이며 진행 중인 목격 중 하나가 완료된 후 시작됩니다.
7. 사이팅은 바로 사용할 수 있으며 기본적으로 활성화되고 false입니다.
8. 실행 중인 프로세스 가져오기에는 해시가 지원되지 않습니다.

FireEye 통합을 위한 NowPlatform 인스턴스 설정

다음 구성 절차를 확인하고 검토하여 Fireeye 통합을 위한 NowPlatform 인스턴스를 설정합니다.

시작하기 전에
필요한 역할: ServiceNow AI Platform 관리자(sn_si.admin)

다음 섹션에는 FireEye 통합을 위한 애플리케이션을 설치하기 전에 NowPlatform 인스턴스에서 완료해야 하는 설정 작업이 나열되어 있습니다.

ServiceNow Store에서 애플리케이션을 설치하기 전에 다음 작업을 완료했는지 확인하십시오.

작업	설명
필요한 NowPlatform 및 보안 인시던트 응답(SIR) 역할을 할당했는지 확인합니다.	다음과 같은 역할이 필요합니다. 1. 통합을 위해 애플리케이션을 설치하려면 시스템 관리자(관리자) 역할을 가진 사용자가 필요합니다. 2. 통합을 구성하고 프로파일을 생성, 활성화 및 제거하려면 보안 인시던트 관리자(sn_si.admin) 역할을 가진 사용자가 필요합니다. 3. 보안 인시던트를 사용하려면 보안 인시던트 분석가(sn_si.analyst) 역할을 가진 사용자가 필요합니다. 이 역할을 가진 사용자는 통합에서 사용할 수 있는 모든 기능을 시작할 수 있습니다.
MID Server를 설치하고 구성했는지 확인하십시오.	MID Server 구성: 파일을 관리하고 조직 네트워크 내에 배포된 FireEye 서비스에 연결하려면 NowPlatform 인스턴스의 MID Server가 필요합니다. MID 서버에 대한 자세한 내용은 다음을 참조하십시오. https://servicenow.com/docs
애플리케이션을 설치하기 전에 통합을 지원하는 데 필요한 ServiceNow Core 애플리케이션이 설치되고 활성화되었는지 확인합니다.	이 애플리케이션을 설치하기 전에 ServiceNow Store에서 다음 애플리케이션을 설치하고 활성화해야 합니다. 원활한 설치를 위해 아래 나열된 순서대로 한 번에 하나의 애플리케이션을 설치하고 활성화합니다. 1. Security Incident Response 지원 2. 보안 지원 코어 3. Security Support Common 4. 보안 인시던트 응답

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업	설명
	5. Threat Intelligence 지원 공통 **6.** ServiceNow Integration Hub 엔터프라이즈 팩 설치 관리자
프로파일에 대한 승인 옵션을 활성화하기 전에 승인 그룹을 생성했는지 확인하십시오.	선택적 승인 워크플로우를 사용하여 호스트 시스템을 격리하고, 다시 네트워크로 복원하고, 파일을 가져오고, 엔드포인트에서 추가 작업을 실행할 수 있습니다. 조직에서 이러한 작업에 대한 추가 제어 수준을 원하는 경우 프로파일을 구성하는 동안 승인 필요 옵션을 활성화합니다. 프로파일이 없는 경우, 관련 목록에서 직접 역량을 호출하면 FireEye 기본 설정 모듈에서 승인을 처리할 수 있습니다. 보안 관리자는 프로파일과 기본 설정을 구성하면서 승인을 설정할 수 있습니다. 인스턴스의 그룹 목록에서 승인 그룹을 사용할 수 있어야 합니다.

프로시저

1. 다음으로 이동 사용자 관리 〉 그룹.

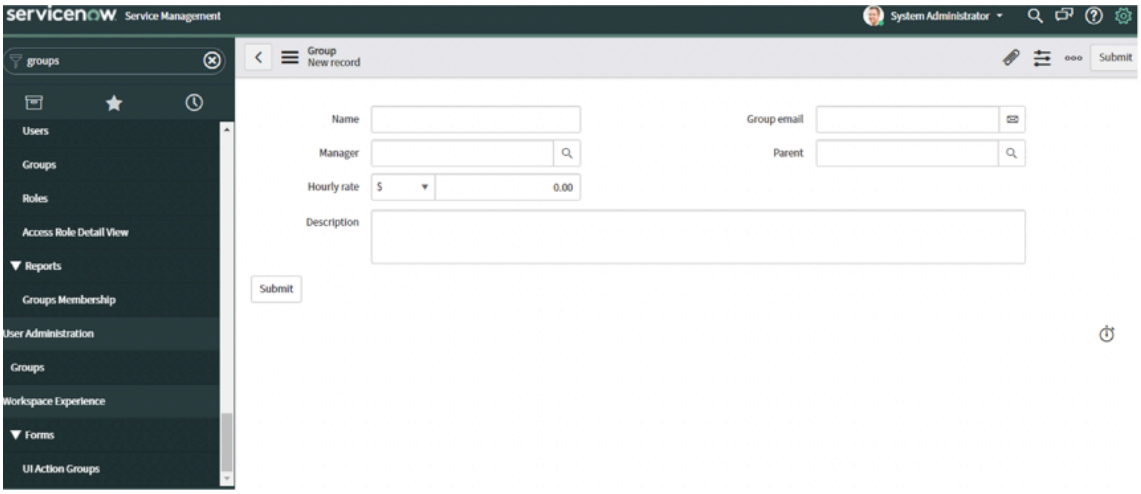
2. 클릭 신규 을 선택합니다.

3. 다음 정보로 폼을 채웁니다.

필드	설명
이름	승인 요청이 제출될 때 표시되는 그룹의 이름입니다.
그룹 이메일	(선택 사항) 그룹 관리자 같은 접촉 창구의 이메일 주소 또는 그룹 이메일 배포 목록입니다.
관리자	(선택 사항) 그룹 관리자의 이름입니다. 검색 아이콘을 클릭하여 목록을 봅니다.
상위	(선택 사항) 상위와 연결된 경우 상위 그룹의 이름입니다.
시간별 요금	(선택 사항) 일한 시간당 지불된 금액.
설명	(선택 사항) 그룹에 대한 추가 정보입니다.

4. 클릭 제출.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



새 그룹이 그룹 목록에 표시됩니다. 승인 그룹을 성공적으로 생성했습니다. 필요에 따라 보안 분석가가 제출한 요청을 승인할 수 있는 사용자를 새 그룹에 추가합니다. 사용자는 사용자가 속한 모든 그룹에서 역할을 상속합니다. 사용자에게 직접 역할을 할당할 수도 있습니다.

sn_si.analyst 역할을 가진 사용자가 제출한 요청을 모니터링하고 처리하려면 승인 그룹의 각 구성원이 에서 내 승인 ServiceNow AI Platform으로 이동해야 합니다. 또는 승인자는 FireEye 승인에서 FireEye 통합을 위해 특별히 제출된 요청을 찾을 수 있습니다.

다음에 수행할 작업
다음 단계는 ServiceNow Store에서 애플리케이션을 설치하고 구성하는 것입니다.

환자 분류 수집을 위한 타임스탬프 설정 구성

설치 절차 전에 타임스탬프 설정을 구성하고 확인합니다.

시작하기 전에
필요한 역할: NowPlatform Security 인시던트 관리자(sn_si.admin)

FireEye 애플리케이션을 설치하기 전에 FireEye에서 수행해야 하는 몇 가지 전제 조건이 있습니다.

"Around Timestamp" 필드 또는 "Standard" 필드를 입력하여 환자 분류 수집을 요청할 수 있습니다. 타임스탬프 전후의 지정된 시간까지 타임스탬프 이전의 지정된 시간 동안 수집된 정보를 요청합니다. 타임스탬프는 경보를 생성한 이벤트가 발생한 시간입니다. 표준을 선택하면 Endpoint Security 장치가 이벤트와 관련된 모든 데이터에 대해 호스트에서 정보를 요청합니다.

Endpoint Security 사용자가 특정 날짜 및 시간을 기준으로 분류 수집을 요청하면 에이전트는 경보 전후의 특정 기간에 대한 정보를 반환합니다. 타임스탬프 설정은 분류 수집의 창 길이를 제어합니다. 타임스탬프 설정은 에이전트 URL 이벤트(URL 모니터 이벤트) 및 레지스트리 키 이벤트(레지스트리 키 이벤트)에만 적용됩니다.

타임스탬프 설정 탭을 사용하여 정보가 수집되는 타임스탬프 전후의 기간을 지정할 수 있습니다. 타임스탬프 설정 범위는 0-86,400초입니다. 두 설정의 기본값은 600초입니다.

자동 분류 설정 페이지의 타임스탬프 설정 탭을 사용하여 정보가 수집되는 타임스탬프 전후의 기간을 지정할 수 있습니다. 타임스탬프는 경보를 트리거한 이벤트가 발생한 시간입니다.

프로시저

1. 다음으로 이동 엔드포인트 보안 웹 **UI**.
2. 선택 관리자 〉 분류 설정.
3. 클릭 타임스탬프 설정 탭의 자동 환자 분류 설정 페이지.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 정보가 필요한 타임스탬프 전후의 시간 길이를 지정합니다.
5. 정보가 필요한 지정된 타임스탬프 이전의 시간(초)을 입력합니다.
6. 정보가 필요한 타임스탬프 이후의 시간(초)을 입력합니다.
7. 클릭 저장.

> **주:**
> 클릭하여 페이지의 모든 값을 기본 설정으로 되돌릴 수 있습니다. 기본값으로 재설정을 클릭하고 저장을 클릭합니다.

- 취득 공간 영역: 취득 페이지에는 취득을 위해 남아 있는 디스크 공간이 표시됩니다.
- 취득에 대한 디스크 사용률 제한 설정:
  - 환자 분류, 파일 획득 및 데이터 수집은 시간이 지남에 따라 누적될 수 있으며 점점 더 많은 디스크 공간을 사용할 수 있습니다. 이를 제어하기 위해 설정된 양의 디스크 공간을 할당할 수 있습니다. 지정한 디스크 공간의 10%는 자동 분류 획득을 위해 예약됩니다. 할당된 총 취득 공간을 초과하면 가장 오래된 자동 분류가 삭제됩니다.
  - 완료된 수집의 총 디스크 크기가 지정된 제한을 초과하면 Endpoint Security 장치는 충분한 디스크 공간이 확보되어 총계가 지정된 제한 미만이 될 때까지 가장 오래된 완료된 수집을 삭제합니다. 아직 완료되지 않은 취득은 영향을 받지 않습니다.
  - 관리자, 분석가 또는 조사자가 Endpoint Security 웹 UI를 사용하여 연결된 에이전트를 수동으로 삭제하는 경우 Endpoint Security 어플라이언스는 자동으로 취득을 삭제합니다.

웹 UI를 사용하여 전체 수집에 대한 디스크 사용률 제한을 설정하려면:

- 엔드포인트 보안 웹 **UI**로 이동합니다.
- 선택 디스크 사용률 제한 에서 관리자 메뉴.
- 안에 취득 공간 제한 area에서 환자 분류, 파일 및 데이터 수집을 저장하는 데 사용할 수 있는 최대 디스크 공간(GB)을 지정합니다. 유효한 값과 기본값은 Endpoint Security 장치 모델에 따라 다릅니다. 모델에 적합한 값이 디스크 사용률 제한 페이지에 표시됩니다.
- 클릭 저장.

> **주:**
> 언급된 모든 설정이 적용되며 오류나 오류가 ServiceNow AI Platform 발생한 경우 해당 오류만 반환합니다.

애플리케이션을 설치하고 통합을 위한 소스 구성

인스턴스의 ServiceNow Store ServiceNow AI Platform 에서 애플리케이션을 설치하고 구성합니다.

시작하기 전에
필요한 역할: NowPlatform 관리자(admin)

> **주:**
> 소스를 구성하려면 활성 MID 서버가 필수입니다.

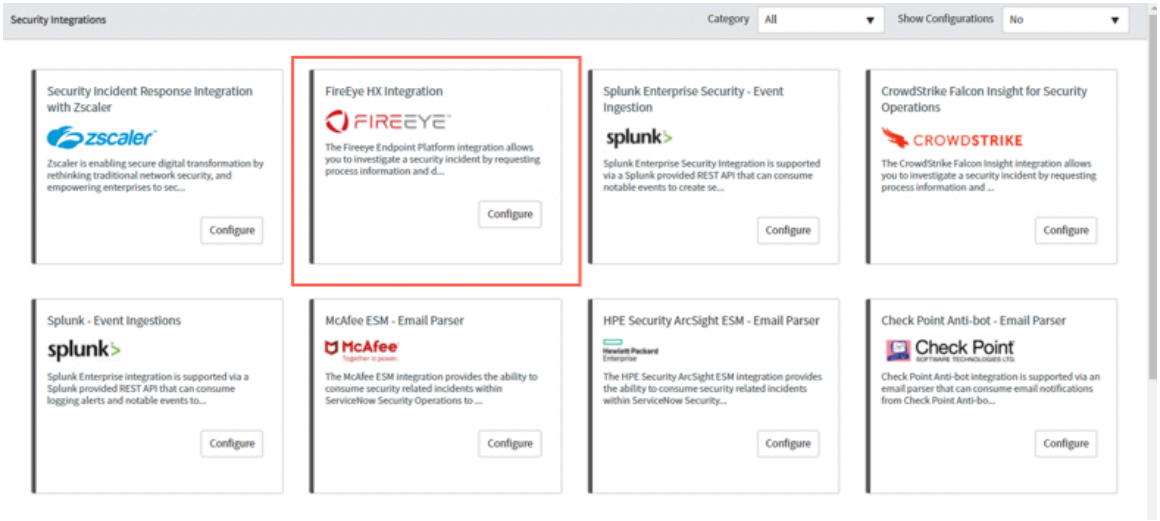
ServiceNow Store에서 애플리케이션과의 FireEye HX 보안 인시던트 응답 통합을 다운로드하여 설치합니다.

애플리케이션을 성공적으로 설치한 후 아래 단계에 따라 구성하십시오.

프로시저

1. 다음으로 이동 통합 〉 통합 구성.
2. 선택합니다. 통합 구성 모듈을 사용하여 사용 가능한 통합을 표시하고 파이어아이 타일.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

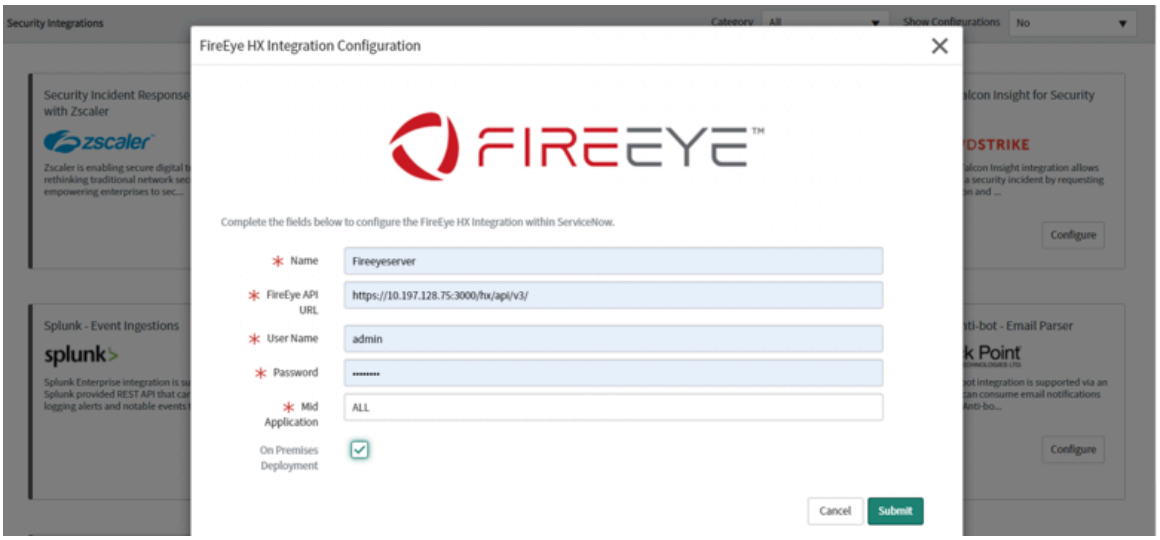


3. 클릭 구성 FireEye 타일에 있습니다.

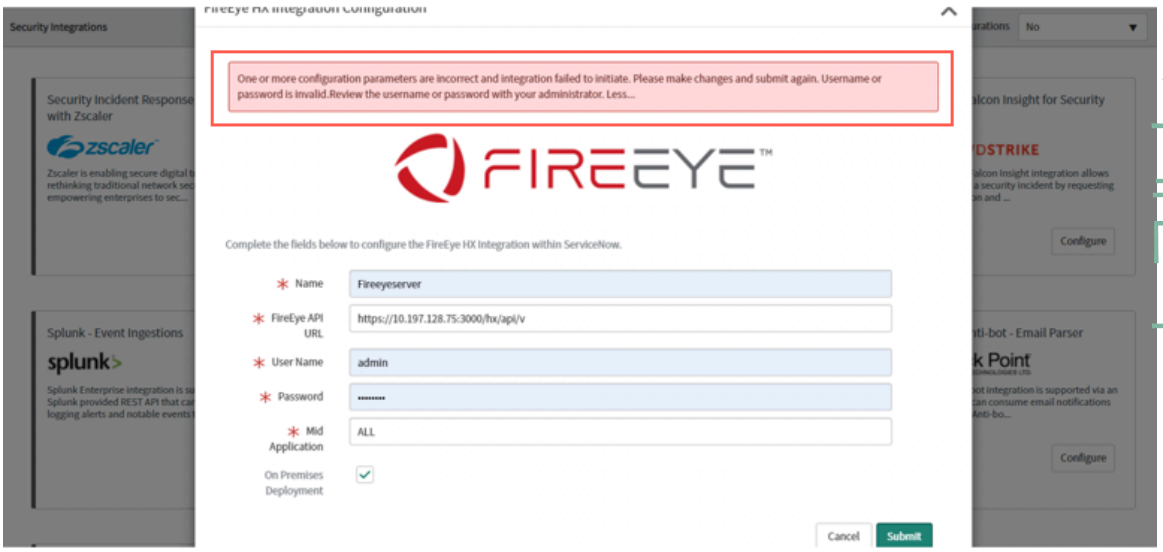
4. FireEye 통합을 설정하려면 다음 상세 정보를 제공하십시오.

필드	설명
이름	FireEye 구성의 이름입니다. 이 이름은 소스 및 관련 자격 증명과 구성을 식별하는 데 사용됩니다. 이 이름은 자격 증명과 계정을 구별하고 각 소스를 식별하여 프로파일과의 충돌을 방지하는 데 도움이 됩니다.
API URL	FireEye API를 호스팅하는 기본 URL입니다.
사용자 이름	FireEye 계정의 사용자 이름을 입력합니다.
암호	FireEye 계정의 암호를 입력합니다.
MID 애플리케이션	사용자 환경에 설정된 MID 애플리케이션입니다. 일부 보강 기능을 위해 zip 파일을 처리하려면 MID 서버가 필요합니다. 기본적으로 모두입니다. 사용자는 올바른 애플리케이션 이름을 수동으로 제공해야 합니다.
직접 배포	기본값은 사용 안 함입니다. 클라우드 기반 버전의 FireEye를 사용하는 경우 확인란의 선택이 취소되어 있는지 확인합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



5. 클릭 제출.
   FireEye 구성 목록이 새 구성 기록과 함께 표시됩니다. FireEye 서버에 대한 컨피그레이션을 완료했습니다. FireEye에 연결할 수 없거나 자격 증명이 잘못된 경우 다음 그림과 같이 유효성 검사 오류 메시지가 표시됩니다. 자격 증명이 올바른지 확인하고 다시 시도하십시오.



FireEye 기본 설정

다음은 설치를 완료한 후의 추가 구성 설정입니다.

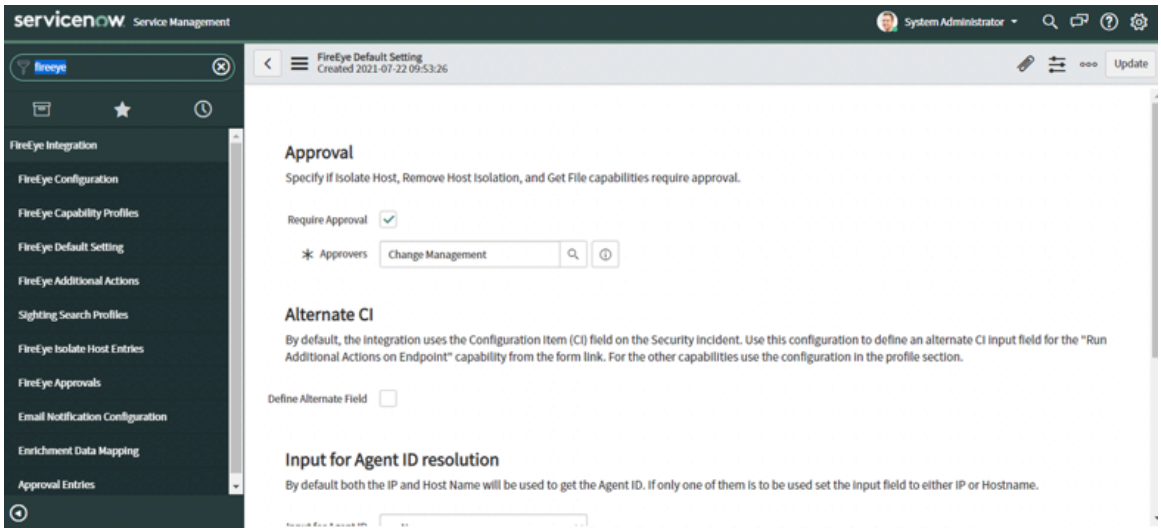
설치가 완료되면 왼쪽 탐색 메뉴에서 FireEye 기본 설정 모듈을 찾을 수 있습니다. 여기에는 다양한 FireEye 기능에 대한 기본 설정이 포함되어 있습니다.

추가 구성

추가 구성 설정은 다음과 같습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

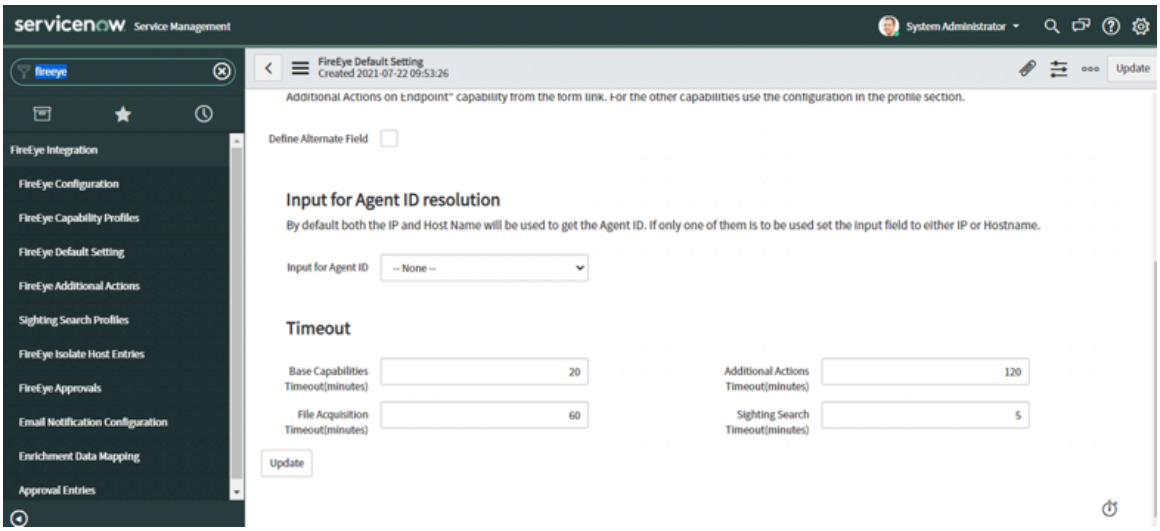
1. 승인: 이 승인은 호스트 격리, 호스트 격리 제거 및 파일 가져오기 역량이 관련 목록에서 직접 트리거되고 해당 프로파일이 없는 경우에 해당됩니다. 이러한 역량에 대한 기존 프로파일이 있는 경우 프로파일의 승인 구성이 적용됩니다.
   - 승인 필요: 승인 필요를 활성화하면 양식에서 승인자 필드를 사용할 수 있습니다.
   - 승인자: 승인자 그룹의 목록입니다. 요청을 제출한 후 요청을 완료하려면 그룹의 승인이 필요합니다.
2. 대체 **CI**: 이 확인란을 활성화하면 대체 CI를 역량에 전달하는 데 사용할 수 있는 필드 목록이 제공됩니다. 기본적으로 통합은 보안 인시던트의 CI(구성 항목) 필드를 사용합니다. 이 구성은 "엔드포인트에서 추가 작업 실행" 기능에만 적용할 수 있습니다. 따라서 이 구성을 사용하여 "엔드포인트에서 추가 작업 실행" 기능만을 위한 대체 CI 입력 필드를 정의합니다. 다른 기능의 경우 프로파일 섹션의 구성을 사용합니다. 프로파일이 대체 CI를 정의하지 않는 경우 역량은 보안 인시던트 양식에서 CI 필드를 선택합니다.
3. 에이전트 **ID** 해결을 위한 입력: 기본적으로 에이전트 ID를 가져오는 데 IP 및 호스트 이름을 사용합니다. 그 중 하나만 사용할 경우 입력 필드를 IP 또는 호스트 이름으로 설정합니다.



4. 시간 제한:
   - 기본 역량 시간 제한(분): 설정된 시간에 응답이 렌더링되지 않으면 호스트 보강, 호스트 격리 및 호스트 격리 제거 기능이 실패합니다.
   - 추가 작업 시간 제한(분): 설정된 시간에 아무런 응답도 렌더링되지 않으면 엔드포인트에서 추가 작업 실행 역량이 실패합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 파일 취득 시간 제한(분): 설정된 시간에 응답이 렌더링되지 않으면 파일 가져오기 기능이 실패합니다.
- 목격 검색 시간 제한(분): 설정된 시간이 지나면 검색이 중지됩니다.



FireEye 엔드포인트 통합을 위한 역량 프로파일 생성

프로파일을 생성하고 프로파일을 실행할 기능을 선택합니다 FireEye HX .

시작하기 전에
필요한 역할: NowPlatform Security 인시던트 관리자(sn_si.admin)

이 태스크 정보
프로파일은 기능을 조합하기 위해 생성되며 분석가가 조사/수정을 쉽게 수행하는 데 도움이 됩니다.

프로파일에 추가할 수 있는 역량 목록은 다음과 같습니다.

1. 호스트 상세 정보 가져오기
2. 로그온한 사용자 가져오기
3. 네트워크 통계 가져오기
4. 실행 중인 프로세스 임포트
5. 실행 중인 서비스 가져오기
6. 파일 가져오기
7. 호스트 격리
8. 격리 제거

프로파일을 생성하는 동안에는 파일 가져오기, 호스트 격리 및 호스트 격리 제거 역량을 다른 기능과 함께 묶을 수 없습니다. 이에 대한 프로필은 개별적으로 만들어야 합니다. 반면에 시스템 세부 정보 가져오기, 로그온한 사용자 가져오기, 네트워크 통계 가져오기, 실행 중인 프로세스 가져오기 및 실행 중인 서비스 가져오기를 함께 구성할 수 있습니다. 프로필을 개별적으로 만들거나 필요에 따라 전체 또는 부분적으로 묶을 수 있습니다. 프로파일에 역량이 포함되면 다른 프로파일에 포함할 수 없습니다.

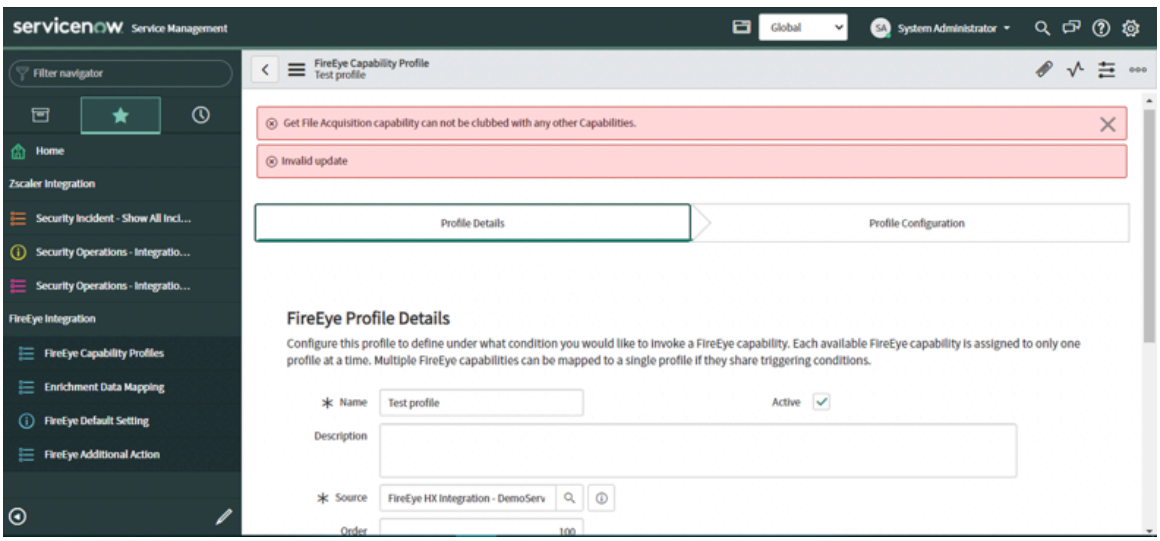
새 역량 프로파일을 생성하려면 다음 단계를 따르십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 **FireEye** 통합 〉 **FireEye** 역량 프로파일.
   역량 프로파일 목록이 표시됩니다.
2. 클릭 신규.
3. 양식에서 필드를 채웁니다.

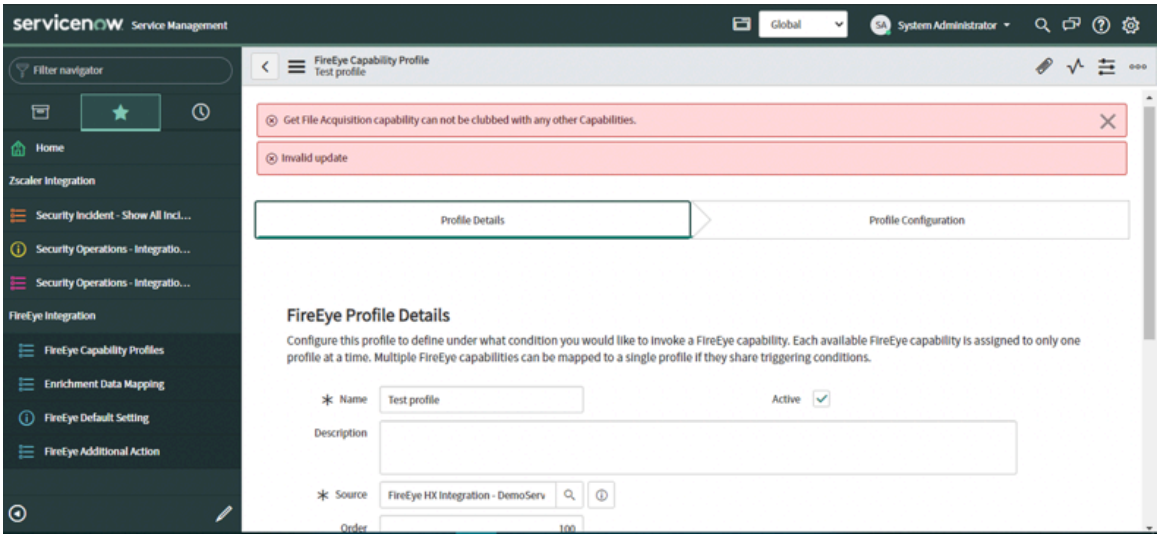
이름	역량 프로파일의 FireEye HX 이름입니다. 이 이름은 프로파일 유형을 식별하고 설명하는 데 도움이 됩니다.
설명	프로파일에 대한 추가 정보로, 프로파일에 대한 자세한 설명을 제공합니다.
소스	소스의 FireEye HX 이름입니다. 구성된 소스만 선택 목록에서 사용할 수 있습니다.
FireEye HX 기능	프로파일의 FireEye HX 기능입니다. 사용 가능 열에서 이 프로파일에 대해 원하는 역량을 선택하고 선택됨 열로 이동합니다.
순서	플로우 우선순위입니다. 기본값은 100입니다. 이 필드의 값은 둘 이상의 프로파일이 트리거 조건을 공유할 때 플로우가 실행되는 순서를 나타냅니다. 숫자가 가장 낮은 플로우의 우선순위가 가장 높습니다. 작업 순서를 설정하려면 값을 입력합니다. 예를 들어 100, 200, 300, 400입니다.
활성	이는 프로파일이 활성 상태임을 나타냅니다. 프로파일이 활성 상태이면 구성에 지정한 필터링 조건과 일치하는 보안 인시던트가 생성되면 프로파일이 자동으로 트리거됩니다.



다음 그림은 호스트 상세 정보 가져오기 기능을 사용하여 프로파일 상세 정보에 대해 작성된 양식의 예입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 클릭 다음 을 클릭하여 프로파일 구성을 계속합니다.



주:
호스트 격리, 호스트 격리 제거 및 파일 가져오기 기능은 다른 기능과 결합할 수 없습니다.

다음에 수행할 작업

다음 단계는 프로필을 구성하는 것입니다. 프로필에 대한 설정을 구성하기 전에 프로필 구성 및 트리거 조건에 대한 개념을 검토하는 것이 좋습니다. 자세한 내용은 프로필의 구성 항목에서 트리거 조건이 작동하는 방식 이해를 참조하세요.

구성 항목에서 트리거 조건이 작동하는 방식 이해

프로필을 만들고 프로필을 실행할 FireEye 기능을 선택한 후 특정 조건 집합이 충족되는 경우에만 실행되도록 프로필 설정을 구성합니다.

트리거 조건과 일치하는 보안 인시던트가 생성될 때마다 프로파일이 자동으로 실행되도록 트리거 조건을 설정할 수 있습니다. 트리거 조건이 설정되지 않은 경우 보안 인시던트에서 "EDR 프로파일 실행" 양식을 클릭하고 프로파일을 선택하여 이러한 프로파일을 수동으로 실행할 수 있습니다.

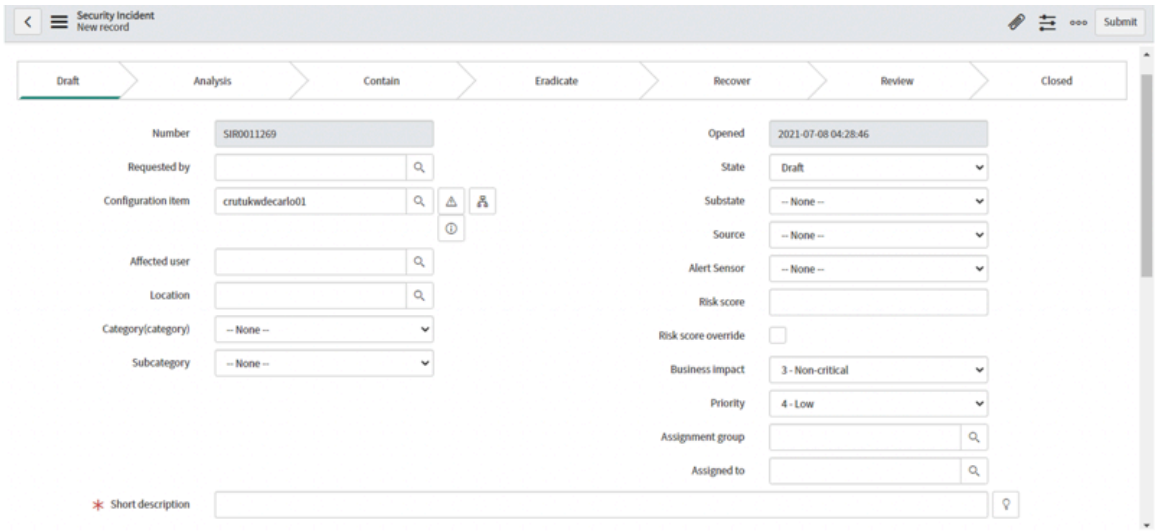
기본적으로 통합은 보안 인시던트의 CI(구성 항목) 필드를 사용합니다. 이 값은 자산의 ID를 Now Platform CMDB에 저장된 정보와 일치시키는 데 사용됩니다. 보안 인시던트가 생성되고 프로파일이 자동 또는 수동으로 실행되면 CMDB가 검색되어 CI 필드의 값을 기반으로 호스트 이름 및/또는 IP 주소를 검색합니다. 호스트 이름 및/또는 IP는 엔드포인트 식별을 위해 에이전트 ID FireEye HX 를 확인하는 데 사용됩니다.

이상적인 경우, 데이터베이스에서 일치하는 값을 찾을 수 있으며, 일치하는 자산에 대한 데이터가 콘솔에서 수집 FireEye HX 됩니다. 다양한 역량에 대한 데이터를 인스턴스로 ServiceNow AI Platform 가져와 보안 인시던트의 관련 목록에 표시합니다. 보안 인시던트의 CI(구성 항목) 필드가 호스트 이름 또는 데이터베이스와 일치하는 IP 주소로 채워지지 않은 경우 호스트 이름 또는 IP가 포함된 보안 인시던트의 대체 필드를 선택하여 에이전트 ID 확인을 수행할 수 있습니다.

프로파일 설정의 구성 단계에서 엔드포인트 식별을 위한 대체 CI 필드를 선택하여 에서 엔드포인트를 FireEye HX식별할 수 있도록 할 수 있습니다. 생성한 사용자 지정 필드를 비롯한 대체 CI 트리거 필드로 보안 인시던트의 모든 필드를 선택할 수 있습니다. 이 대체 CI 필드를 백업으로 선택하면 인시던트 생성 시 연관된 보안 인시던트에 CI 필드가 채워지지 않아도 프로파일이 실행되도록 할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
대체 CI 필드는 프로파일에 추가할 수 있는 기능에 대해서만 고려됩니다. 모든 추가 작업에 대해 기본 설정 페이지에서 대체 CI가 선택됩니다.



통합에 **FireEye HX** 대한 프로파일 및 보안 인시던트 구성

프로필을 만들고 프로필을 실행할 기능을 선택한 FireEye HX 후 정의된 조건에서만 프로필을 호출할 수 있도록 설정을 구성합니다.

시작하기 전에
필요한 역할: sn_si.admin

지정한 조건이 충족되는 경우에만 실행되도록 프로파일을 구성합니다. 필요한 경우 CI(구성 항목) 필드에 대한 대체 입력 필드를 선택하고, 트리거 조건을 충족하는 보안 인시던트가 생성될 때 프로파일이 자동으로 트리거될 수 있도록 필터링 조건을 설정합니다.

주:
다음으로 이동합니다. 프로파일 구성 페이지를 입력한 후에만 프로파일 상세 정보.

프로시저

1. 다음으로 이동 **FireEye** 통합 〉 **FireEye** 역량 프로파일.
2. 클릭 다음 에 프로파일 상세 정보 페이지 프로필 상세 정보 섹션을 완료한 후
3. 다음 섹션을 검토하고 구성합니다.
   - 인시던트 기준 정의(자동화): 프로파일에 대한 역량을 FireEye HX 자동으로 트리거하는 보안 인시던트 조건을 정의합니다. 를 선택하지 않으면 인시던트 기준 정의 옵션을 선택하면 보안 인시던트에서 프로파일과 기본 기능을 수동으로 호출할 수 있습니다.
     - 선택 인시던트 기준 정의 프로파일에서 역량을 자동으로 트리거 FireEye HX 하는 옵션입니다.
     - 안에 필터 조건에서 필수 필드를 선택합니다.
     - 다음을 추가할 수 있습니다. 새 기준 OR 또는 AND 조건도 정의합니다.

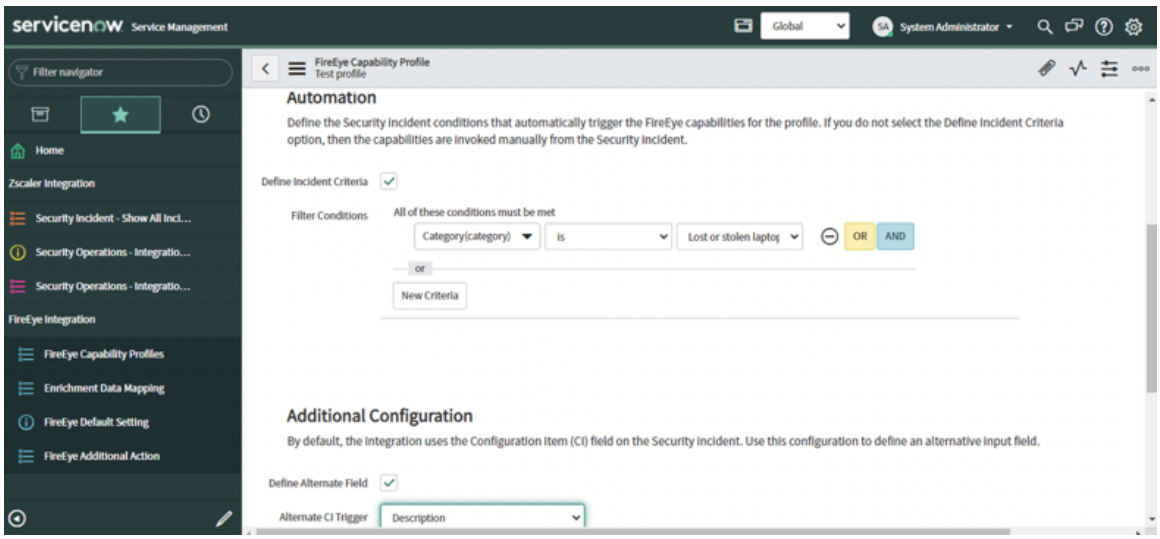
       주:
       호스트 격리, 호스트 격리 제거, 파일 가져오기를 자동으로 트리거할 수 없습니다.

   - 추가 구성: 보안 인시던트의 CI(구성 항목) 필드가 호스트 이름 또는 데이터베이스와 일치하는 IP 주소로 채워지지 않은 경우 보안 인시던트에서 대체 필드를 선택하여 API를 쿼리할 FireEye HX 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

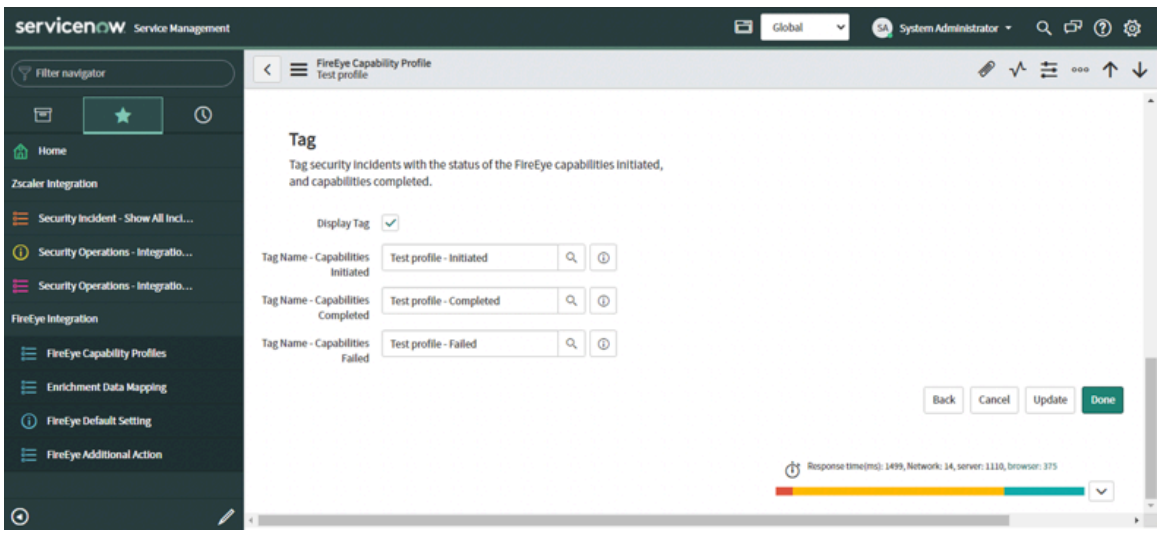
- 선택합니다. 대체 필드 정의 대체 입력 필드를 정의하는 옵션입니다.
- 다음에서 입력 필드를 선택합니다. 대체 **CI** 트리거 필드.

> **주:**
> 자세한 내용은 구성 항목에서 트리거 조건이 작동하는 방식 이해 문서를 참조하십시오.



- 태그: 프로파일 시작됨, 프로파일 완료 및 프로파일 실패 태그를 사용하여 보안 인시던트에 FireEye HX 선택적으로 태그를 지정할 수 있습니다.

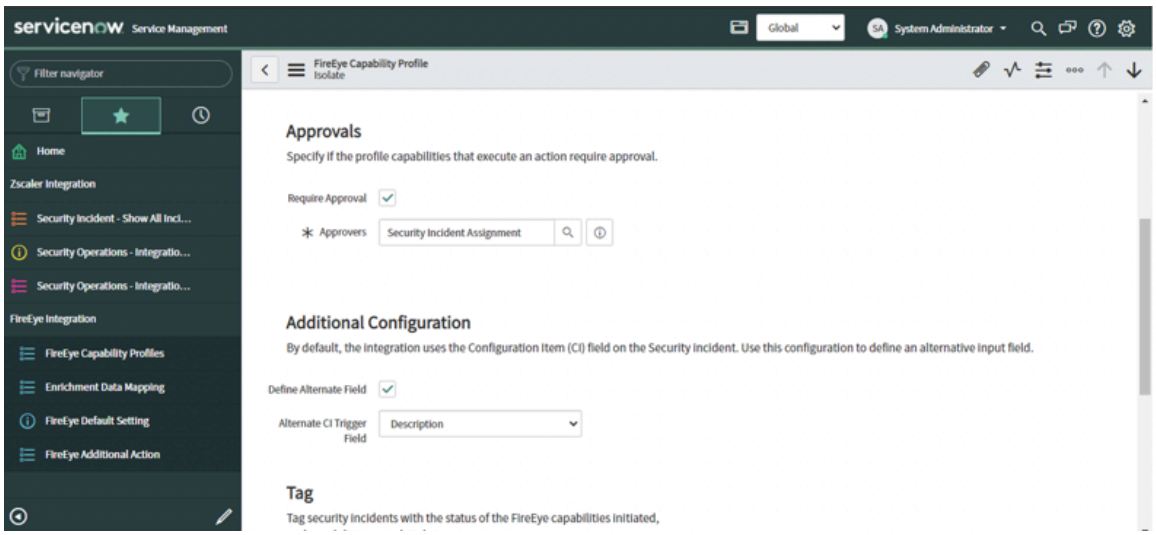
  선택합니다. 태그 표시 보안 인시던트 태그 지정을 활성화하는 확인란으로, 태그 사용 시 프로파일 이름이 프리픽스로 표시됩니다. 기본적으로 이 옵션은 모든 프로필에 대해 비활성화되어 있습니다.



- 승인: 선택 승인 필요 호스트 컴퓨터를 격리하고, 네트워크에 복원하고, 파일을 가져오는 기능을 사용할 FireEye HX 때 추가 제어 수준을 제공하는 확인란입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로파일 구성의 승인 옵션은 호스트 격리, 호스트 격리 제거 및 파일 가져오기 기능에만 표시됩니다.



4. 완료를 클릭합니다.
5. 트리거 조건을 확인합니다 FireEye HX .

트리거 조건 필터 확인

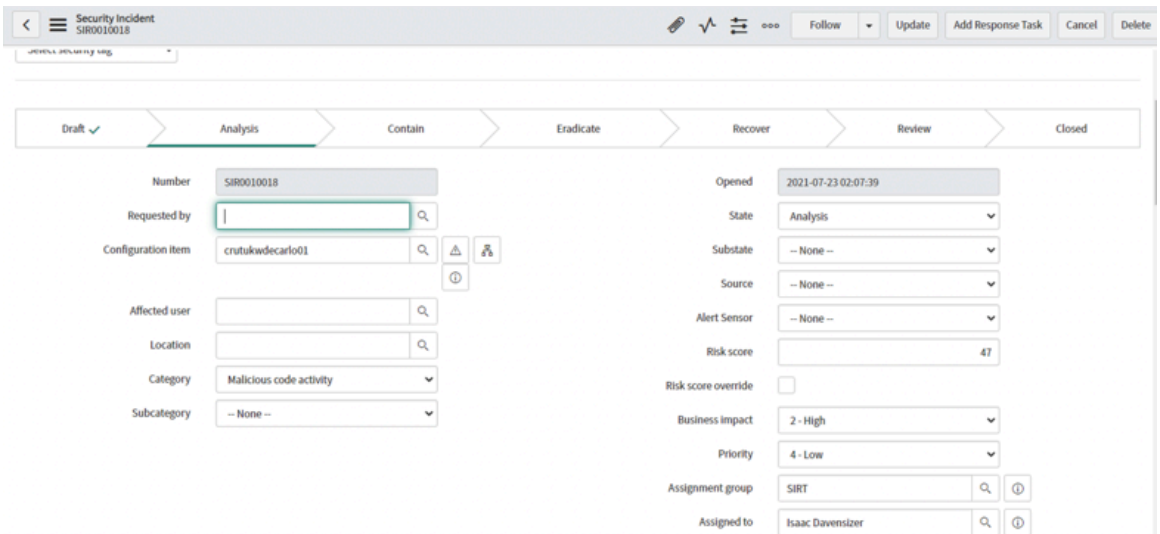
프로파일을 테스트하고 구성한 트리거 조건 필터가 예상대로 작동하는지 확인합니다.

시작하기 전에
필요한 역할: sn_si.admin 또는 sn_si.analyst

프로파일을 활성화하면 구성된 트리거 조건에 따라 보안 인시던트의 쿼리 결과를 볼 수 있습니다 ServiceNow AI Platform .

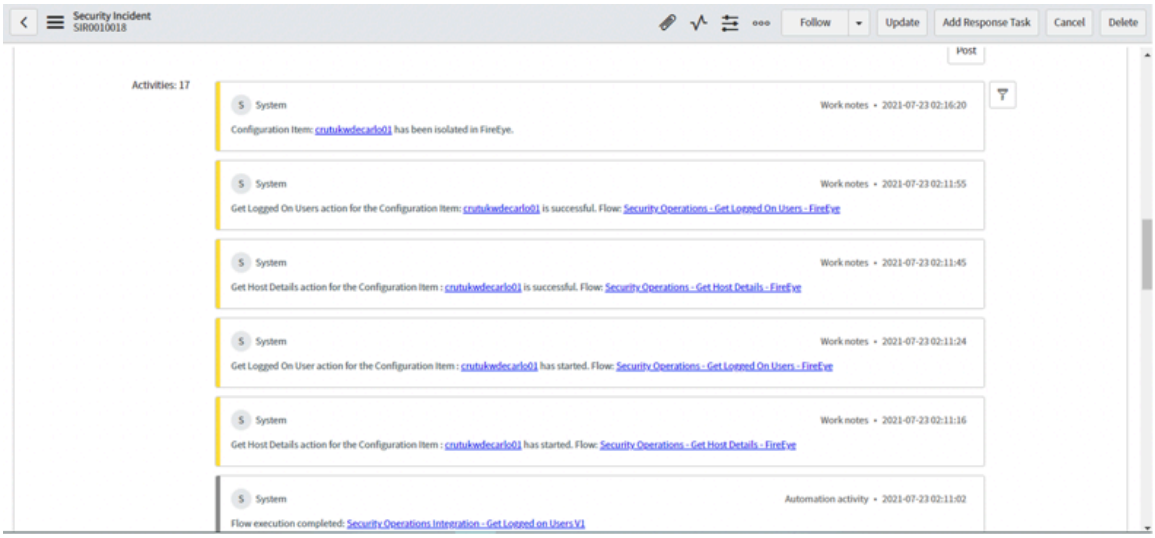
프로시저

1. 다음으로 이동 보안 인시던트 〉 모든 인시던트 표시.
2. 선택 신규 새 보안 인시던트를 생성합니다.
3. 역량 프로파일에 지정된 대로 필터 조건을 제공하여 해당 프로파일을 트리거합니다.

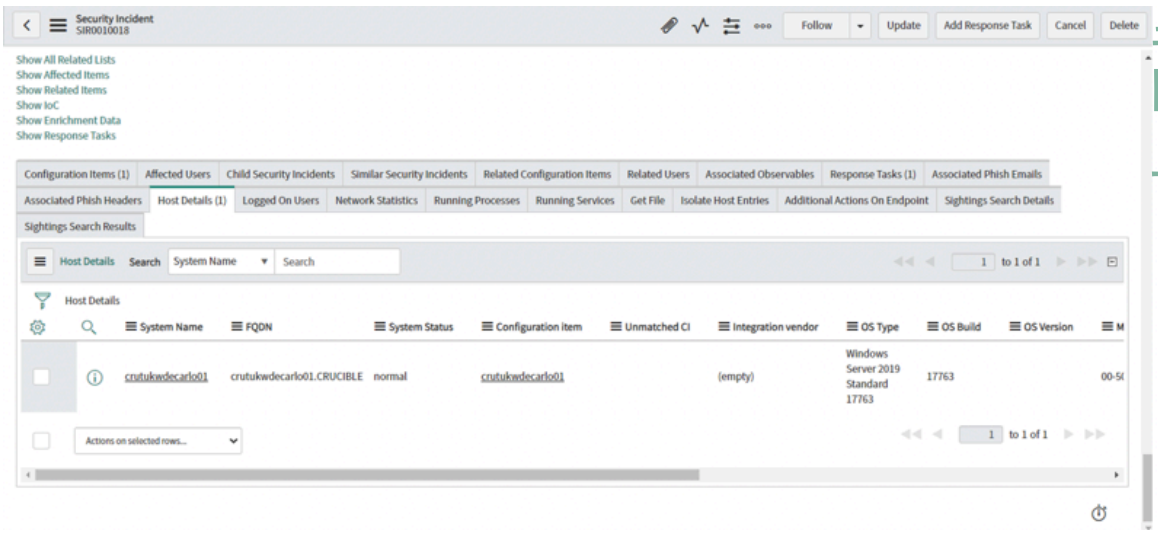


© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 클릭 저장.



5. 작업 메모 및 활동 섹션을 검토합니다.
6. 시작된 프로파일, 완료된 프로파일 또는 실패한 프로파일 태그를 봅니다.
7. 클릭 모든 관련 목록 표시.
8. 관련 목록(탭)을 클릭합니다.
   예: 호스트 상세 정보.



관련 링크에서 **FireEye** 역량 프로파일 트리거

관련 링크에서 보안 인시던트를 검토한 후 역량 프로파일을 수동으로 트리거합니다.

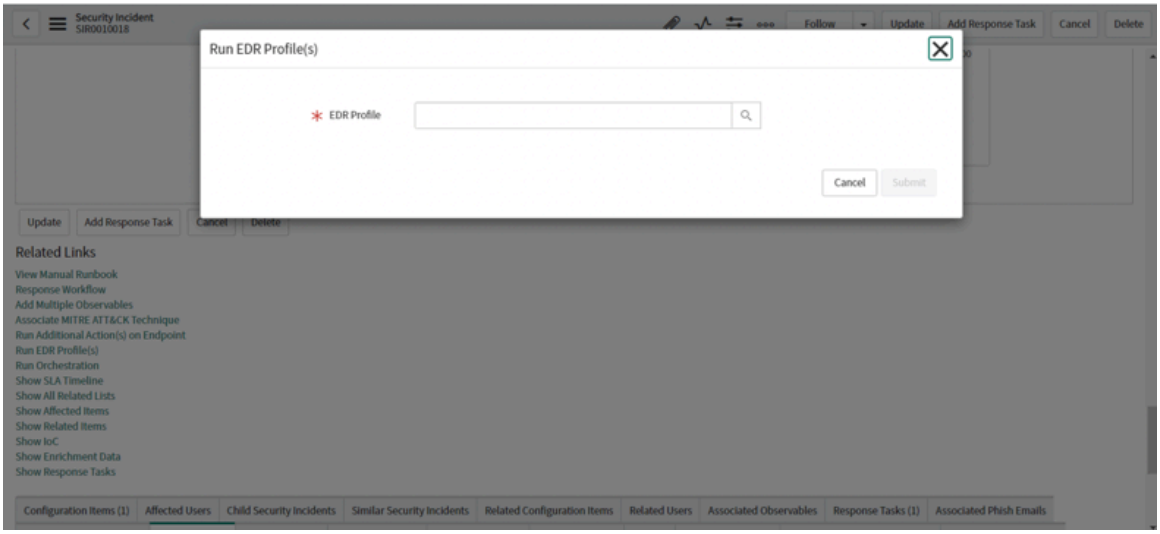
시작하기 전에

필요한 역할: sn_si.admin 또는 sn_si.analyst

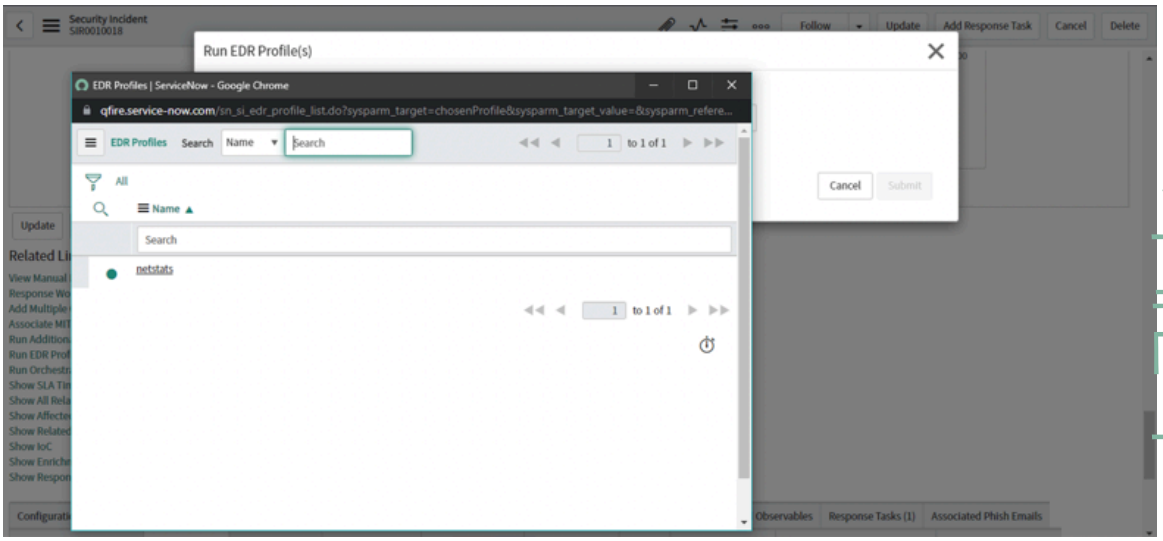
프로시저

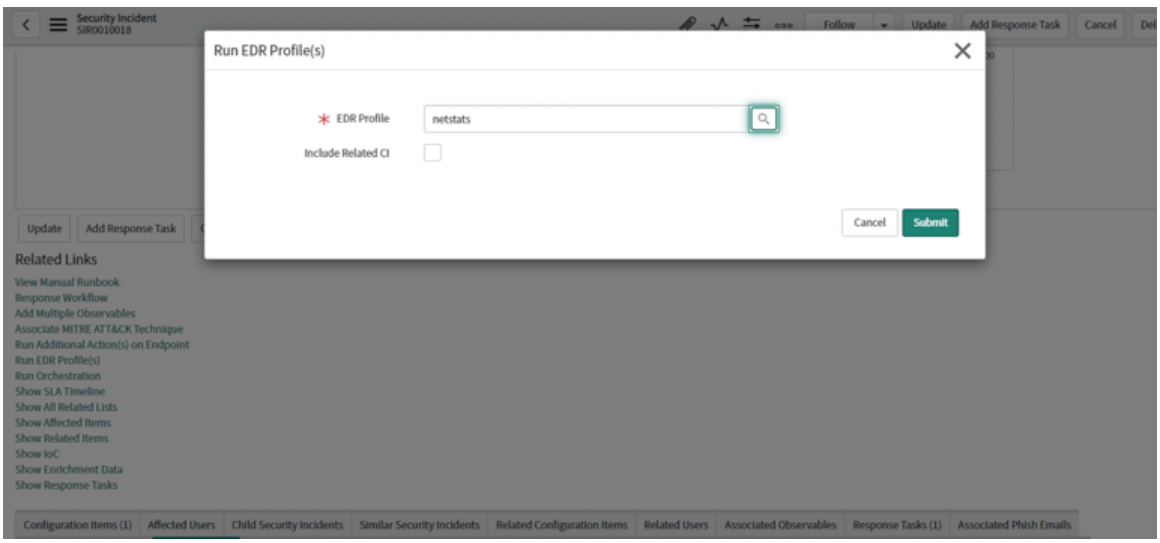
1. 다음으로 이동 보안 인시던트 〉 모든 인시던트 표시.
2. 검토하려는 보안 인시던트를 선택합니다.
3. 클릭 **EDR** 프로파일 실행관련 링크 섹션

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 사용 가능한 프로파일 목록에서 프로파일을 찾아 선택하고 제출.





5. 선택한 프로파일이 수동으로 트리거됩니다.

6. 작업 메모 및 활동 섹션을 검토합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

7. 태그를 보고 관련 목록에서 데이터를 확인합니다.

> 주:
> CI 또는 보안 인시던트의 대체 CI에 대한 프로파일을 실행하는 것 외에도, 대화 상자에서 관련 CI 포함을 선택하여 구성 항목 관련 목록에 있는 CI 값에 대한 프로파일을 실행할 수도 있습니다. 이렇게 하면 관련 목록에 있는 CI 값에 대한 데이터도 가져옵니다. 또는 관련 목록에 있는 CI 값에 대해서만 프로파일을 실행할 수 있습니다.

구성 항목 관련 목록에서 **FireEye** 역량 프로파일 트리거

구성 항목 관련 목록에서 역량 프로파일을 수동으로 트리거합니다.

시작하기 전에

필요한 역할: sn_si.admin, sn_si.analyst

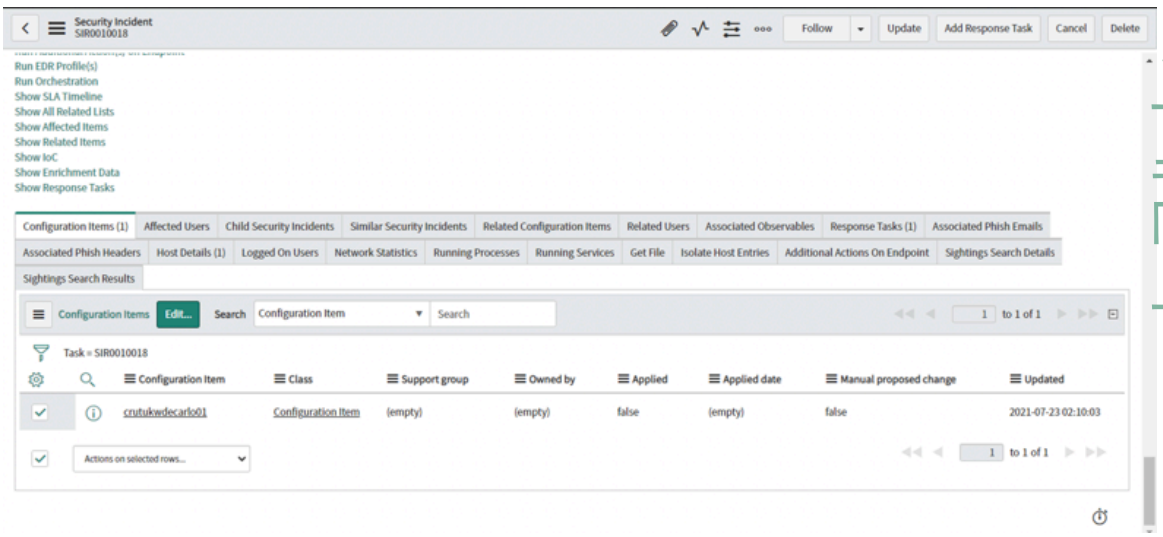
프로시저

1. 다음으로 이동 보안 인시던트 〉 모든 인시던트 표시.

2. 정보로 검토하려는 보안 인시던트를 FireEye HX 선택합니다.

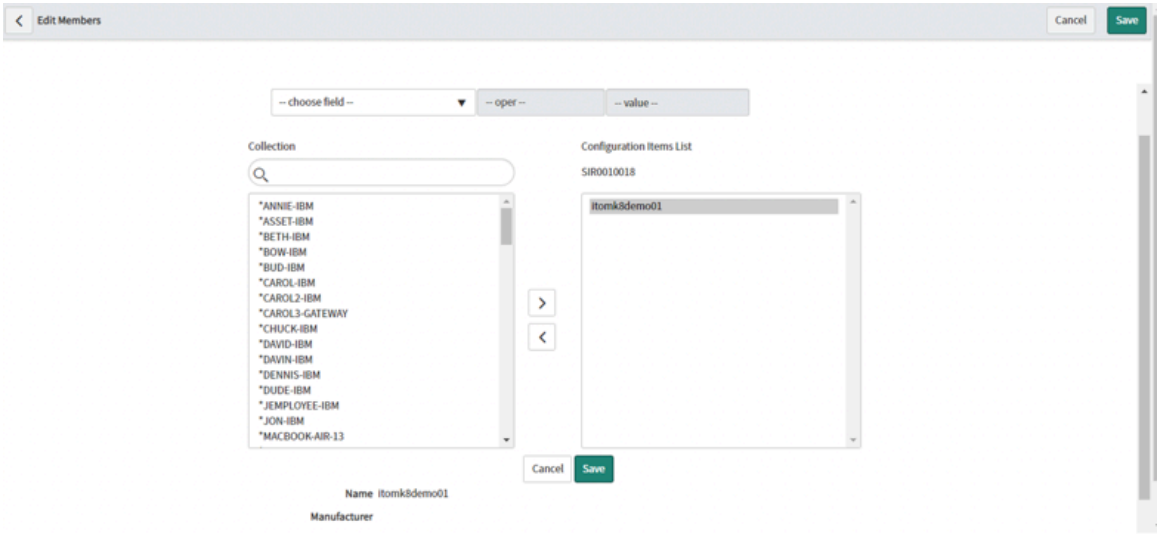
3. 클릭 모든 관련 목록 표시 관련 목록 섹션에 있습니다.

4. 다음을 클릭 구성 항목 관련 목록.

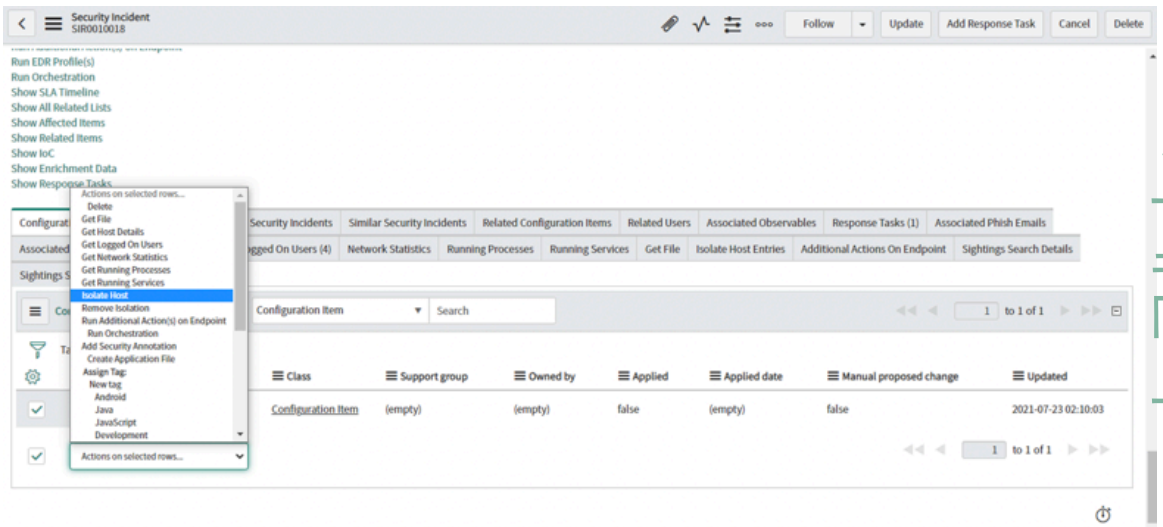


5. 클릭 편집 사용 가능한 구성 항목을 추가하려면 값이 아직 없는 경우 저장.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



6. 추가된 구성 항목을 선택하고 선택한 행에 대한 작업에서 역량을 선택합니다.



7. 선택한 역량이 수동으로 트리거됩니다.

8. 작업 메모 및 활동 섹션을 검토합니다.

9. 태그를 보고 관련 목록에서 데이터를 확인합니다.

FireEye 파일 가져오기 역량

파일 취득 요청은 Endpoint Security Agent에 호스트 엔드포인트에서 파일을 가져오도록 지시합니다. 파일 획득은 잠재적 또는 검증된 손상의 정적 또는 동적 분석뿐만 아니라 내부자 위협 조사 중 증거 보존에도 사용됩니다. 파일 가져오기 기능은 별도의 프로파일로 만들어야 합니다.

시작하기 전에
필요한 역할: 관리자

파일 프로파일 가져오기 트리거 및 역량 프로파일 생성 FireEye HX 파일 가져오기 능력.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

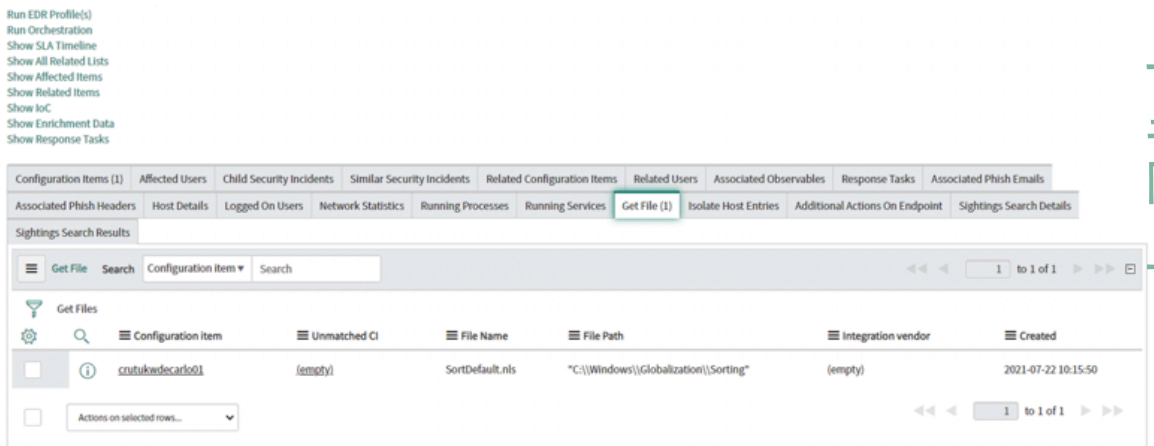
프로시저

1. 다음으로 이동 보안 인시던트 〉 모든 인시던트 표시.
2. 검토하려는 보안 인시던트를 선택합니다.
3. 클릭 **EDR** 프로파일 실행관련 링크 섹션
4. 사용 가능한 프로파일 목록에서 파일 프로파일 가져오기를 찾아 선택합니다.
5. 제공 파일 이름 및 파일 경로.

   주:
   획득하려는 파일의 이름을 입력합니다. 정확한 경로 이름이나 다른 적절한 경로 기반 Windows 환경 변수를 지정합니다. 드라이브 문자 또는 경로 이름을 지정해야 합니다. 엔드포인트마다 드라이브 매핑이 다를 수 있습니다. 폴더 이름을 명시적으로 지정하는 경우 경로를 백슬래시로 끝낼 수 있습니다. 그러나 마지막 백슬래시는 필수가 아닙니다.

6. 클릭 제출.
7. 작업 메모 및 활동 섹션을 검토합니다.
8. 다음에서 태그를 보고 결과를 확인합니다. 파일 가져오기 관련 목록.

   주:
   이제 파일 가져오기 프로필이 수동으로 트리거됩니다.



다운로드된 파일 취득을 검토하는 방법:

- 파일 취득 .zip 파일을 엽니다.
- 파일을 여는 데 필요한 암호를 입력합니다. 비밀번호는 콘솔의 FireEye HX 다운로드 링크 위로 마우스를 가져가면 볼 수 있습니다. 암호를 보려면 아래 단계를 따르십시오.
  - FireEye HX 콘솔에 로그인합니다.
  - 다음으로 이동 취득 취득 유형 – 파일별로 필터링합니다.
  - 원하는 기록을 선택합니다.

    주:
    오른쪽 탭에서 획득한 파일의 세부 정보를 볼 수 있습니다.

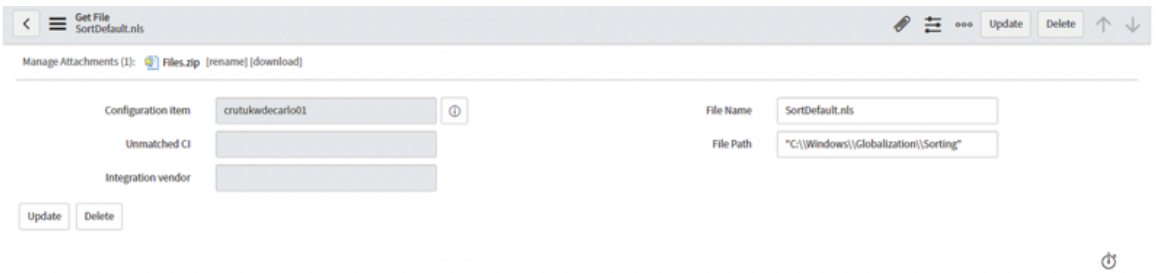
  - 마우스로 가리키기 다운로드 비밀번호를 얻기 위해 상단에서 링크를 사용할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

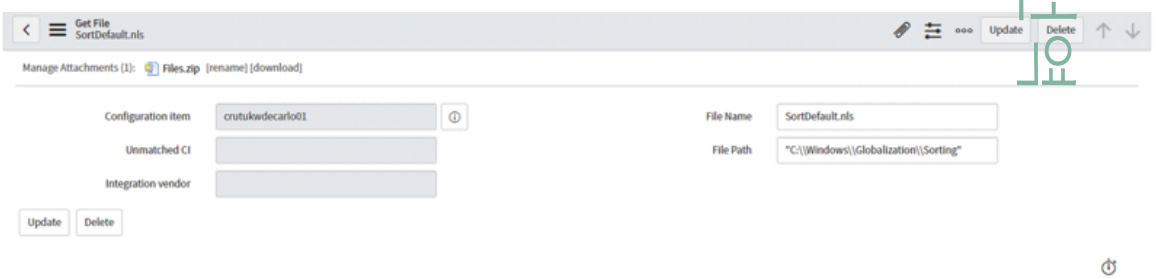
- 텍스트 또는 XML 편집기를 사용하여 .zip 파일 내의 파일을 열고 검토합니다.

  주:

  - 검색된 파일을 수동으로 옵저버블로 추가하여 보안 인시던트에 대한 증거로 추적할 수 있도록 하는 것이 좋습니다. 이렇게하면 나중에 암호를 잊어 버리거나 변경할 때 파일을 볼 수 있습니다.
  - 파일 가져오기 작업에 지원되는 최대 파일 크기는 1024MB이며 이 값은 다음을 변경하여 구성할 수 있습니다. com.glide.attachment.max_크기및 기본 시간 제한은 기본 설정 페이지에서 구성할 FireEye HX 수 있는 60분입니다.



  - 파일 가져오기는 구성 항목 관련 목록에서도 트리거할 수 있습니다.



엔드포인트에 대한 **FireEye** 추가 작업

FireEye 통합은 표준 작업 이상의 추가 작업 실행을 지원합니다.

이러한 작업은 환자 분류 수집 및 데이터 수집으로 구성됩니다. 기본적으로 두 가지 데이터 수집이 지원됩니다.

- 포괄적인 조사 상세 정보 스크립트
- 표준 조사 상세 정보 스크립트

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

또한 환자 분류 획득도 즉시 지원됩니다. 이 세 가지는 모두 기본적으로 소스와 함께 생성됩니다. 고객은 FireEye 추가 작업 모듈에서 데이터 수집과 같은 자체 작업을 생성할 수도 있습니다. [1] FireEye 추가 작업에 지원되는 최대 파일 크기는 1024이며, 이 값은 com.glide.attachment.max_크기, 기본 시간 제한은 FireEye 기본 설정 페이지에서 구성할 수 있는 120분입니다.

포괄적인 조사 상세 정보 스크립트

엔드포인트에서 모든 포렌식 및 조사 아티팩트를 수집할 수 있지만 가장 비용이 많이 드는 옵션입니다. 이 구성은 해당 엔드포인트에서 데이터를 수집하기 위한 창이 하나뿐이고 나중에 더 많은 데이터를 수집하는 기능을 보장할 수 없는 상황에 이상적입니다. 따라서 이 작업은 주의해서 사용해야 합니다.

표준 조사 상세 정보 스크립트

엔드포인트에서 포렌식 및 조사 아티팩트를 수집하는 가장 일반적인 옵션을 활성화합니다. 엔드포인트가 손상되었을 수 있다고 의심되어 해당 엔드포인트에 대한 심층 분석을 수행해야 할 때 기본 응답 도구입니다. 가장 관련성이 높고 가치 있는 데이터를 수집하는 동시에 추가 조사를 통해 필요한 것으로 판명되면 나중에 수집할 수 있는 비용이 많이 드는 옵션을 피하는 것 사이의 균형을 유지하는 것을 목표로 합니다.

환자 분류 취득

분류 모음에는 조회 캐시 내의 정보와 URL 다운로드 기록, 파일 다운로드 기록, 프로세스 및 포트 목록, 표준 시스템 정보와 같은 추가 포렌식 감사 정보가 포함됩니다. 비정상적인 네트워크 트래픽이 탐지될 때 이러한 정보를 검사하고 엔드포인트 작업에 대한 가시성을 높이고자 할 수 있습니다.

FireEye에서 데이터 수집 스크립트 유지 관리

데이터 수집 요청(Live Response 요청이라고도 함)을 사용하면 실행 중인 단일 엔드포인트에서 필요한 모든 데이터를 수집할 수 있습니다. FireEye의 데이터 수집 스크립트 페이지를 사용하여 데이터 수집 요청에 사용되는 데이터 수집 스크립트를 생성, 편집, 복사 및 삭제할 수 있습니다.

FireEye의 데이터 수집 스크립트 페이지에 액세스

데이터 취득 스크립트 페이지에 액세스하려면

1. 엔드포인트 보안 웹 사용자 인터페이스로 이동합니다.
2. Admin 메뉴에서 Data Acquisition Scripts를 선택합니다.

FireEye에서 스크립트 생성

데이터 수집 스크립트를 생성하려면:

1. 선택 데이터 취득 스크립트 〉 관리자 Endpoint Security 웹 사용자 인터페이스의 메뉴입니다.
2. 클릭 스크립트 작성.
3. 에 새 스크립트의 이름을 입력합니다. 스크립트 이름 필드
4. 선택적으로 스크립트의 설명을 입력합니다.
5. 스크립트가 적용되는 운영 체제를 선택합니다. 스크립트 생성 대화상자에서 단일 운영 체제만 선택할 수 있습니다.
6. 클릭 작성 스크립트 정의를 시작합니다.
7. 다음에서 취득 데이터 유형 선택 취득 유형 추가드롭다운 상자를 클릭하고 추가. 요청한 취득 유형에 대한 옵션이 스크립트 목록의 오른쪽에 나타납니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

8. 취득 유형 옵션에 대한 값을 제공하거나 이미 선택된 기본값을 사용합니다. 웹 UI는 사용자에게 경고하거나 사양에서 탭, 공백 또는 원치 않는 문자(예: \n)를 제거하지 않습니다.
9. 이전 2단계를 반복하여 데이터 수집 스크립트에 대한 추가 데이터를 요청합니다. 일부 취득 데이터 형식은 스크립트에 대해 한 번만 사용할 수 있는 반면 다른 데이터 형식은 두 번 이상 지정할 수 있습니다. 스크립트에 취득 유형을 추가하면 취득 유형 추가드롭다운 상자가 적절하게 조정됩니다.
10. 스크립트에서 취득 데이터 유형을 제거하려면 페이지 왼쪽의 취득 탭에서 x 아이콘( )을 클릭합니다.

주:
이 통합은 다음을 지원하지 않습니다. 획득하기 전에 편집 허용 옵션을 선택합니다. 따라서 확인란이 선택 취소되어 있는지 확인하십시오.

FireEye에서 스크립트 내보내기

데이터 취득 스크립트를 JSON 파일로 내보낼 수 있습니다. 데이터 수집 스크립트를 내보내는 방법:

1. 선택 데이터 취득 스크립트 〉 관리자 엔드포인트 보안 웹 사용자 인터페이스의
2. Admin 메뉴에서 Data Acquisition Scripts를 선택합니다.
3. 페이지 왼쪽에서 익스포트할 스크립트를 선택합니다.
4. 선택 작업 〉 스크립트 익스포트.
5. JSON 파일이 컴퓨터에 다운로드됩니다. JSON 파일 이름에는 운영 체제가 포함되어 있으므로 어떤 운영 체제에 대한 스크립트인지 쉽게 확인할 수 있습니다.

에서 새 데이터 취득 동작 생성 **ServiceNow AI Platform**

새 작업을 만들려면 다음 단계를 수행합니다.

1. 다음으로 이동 **FireEye** 통합 〉 **FireEye** 추가 작업. FireEye 추가 작업 목록이 표시됩니다.
2. 클릭 신규. 새 작업의 양식이 표시됩니다.
3. 양식을 작성합니다.

작업 이름	수행되는 FireEye 작업의 이름입니다. 이 이름은 작업 유형을 식별하고 설명하는 데 도움이 됩니다.
취득	취득을 통해 분석할 데이터를 가져옵니다. 이 필드는 읽기 전용이며 기본값은 데이터 수집입니다.
소스	FireEye 소스의 이름입니다. 구성된 소스만 선택 목록에서 사용할 수 있습니다.
역량	읽기 전용 필드로, 추가 작업 실행 기능으로 채워집니다.
취득 유형	획득 및 분석해야 하는 취득 작업의 유형입니다.
활성	이는 작업이 활성 상태임을 나타냅니다.
승인 필요	승인 필요 옵션을 활성화하면 양식에서 승인자 필드를 사용할 수 있습니다. 요청을 제출한 후 요청을 완료하려면 그룹의 승인이 필요합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

태그 표시	스크립트 추가를 위한 Windows, Mac, Linux와 같은 운영 체제의 유형입니다. 주: 현재는 한 가지 유형의 OS만 지원됩니다. 운영 체제당 하나의 작업을 생성할 수 있습니다. 다른 운영 체제의 경우 필요에 따라 새 작업을 생성합니다.
스크립트	선택한 OS 유형에 대해 FireEye에서 가져온 스크립트를 제공해야 합니다. 각 OS 유형에 하나의 스크립트만 추가할 수 있습니다.

4. 클릭 제출.

보안 인시던트에서 데이터 수집 트리거

생성된 추가 작업은 호출된 관련 링크를 통해 실행할 수 있습니다. 엔드포인트에서 추가 작업 실행 보안 인시던트에서.

주:
획득하기 전에 편집 허용 FireEye 기능은 엔드포인트의 추가 작업에 대해 지원되지 않습니다.

FireEye 통합으로 사이팅 검색을 위한 프로파일 구성

다음 절차를 사용하여 사이팅 검색 프로파일을 구성합니다.

시작하기 전에
필요한 역할: NowPlatform Security 인시던트 관리자(sn_si.admin)

소스가 생성될 때마다 5가지 유형(파일, IP(v4), MD5, SHA1 및 SHA256)에 대한 개별 사이팅 검색 구성이 생성되고 기본적으로 비활성화됩니다. 사이팅 검색을 사용하기 전에 활성화해야 합니다. 각 옵저버블 유형에는 사이팅을 검색하기 위한 다른 검색 쿼리가 있습니다. 각 옵저버블 유형에 대해 다른 검색을 시작합니다. 사이팅 검색을 위한 다중 옵저버블 검색은 옵저버블에 대해 AND 연산을 수행하고 결과가 부정확할 수 있으므로 FireEye에서 불가능합니다.

주:
사이팅 검색의 경우 한 번에 5개의 활성 검색만 존재할 수 있습니다. 나머지는 큐에 대기 중이며 진행 중인 목격 중 하나가 완료된 후 시작됩니다.

새 사이팅 검색 프로파일을 만들려면 아래 단계에 따라 프로파일을 만듭니다.

프로시저

1. 다음으로 이동 통합 〉 사이팅 검색 구성.
2. 클릭 신규.
3. 양식에서 필드를 채웁니다.

필드	설명
이름	역량 프로파일의 이름입니다.
저장된 검색 여부	이렇게 하면 저장된 검색이 실행됩니다. 예를 들어 이름 필드는 저장된 검색의 이름과 일치해야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
관찰 검색 소스	통합을 위해 구성된 소스를 정의합니다.
검색	네이티브 검색 문자열을 추가하여 쿼리를 만듭니다.
활성	쿼리는 활성 상태인 경우에만 실행됩니다.
옵저버블 유형	옵저버블 범주의 유형을 정의합니다.
검색당 최대 옵저버블	검색 쿼리가 여러 쿼리로 분할되기 전의 옵저버블 수입니다. 이 통합에 대해 이 값을 1로 설정합니다.
사이팅 검색 매개변수	사이팅 검색 매개변수를 사용하여 지정된 로그 저장소에서 지원하는 논리 및 기타 연산자를 포함하는 보다 복잡한 쿼리를 정의합니다.

4. 클릭 제출 구성을 완료합니다.

보안 인시던트에서 사이팅 검색 호출

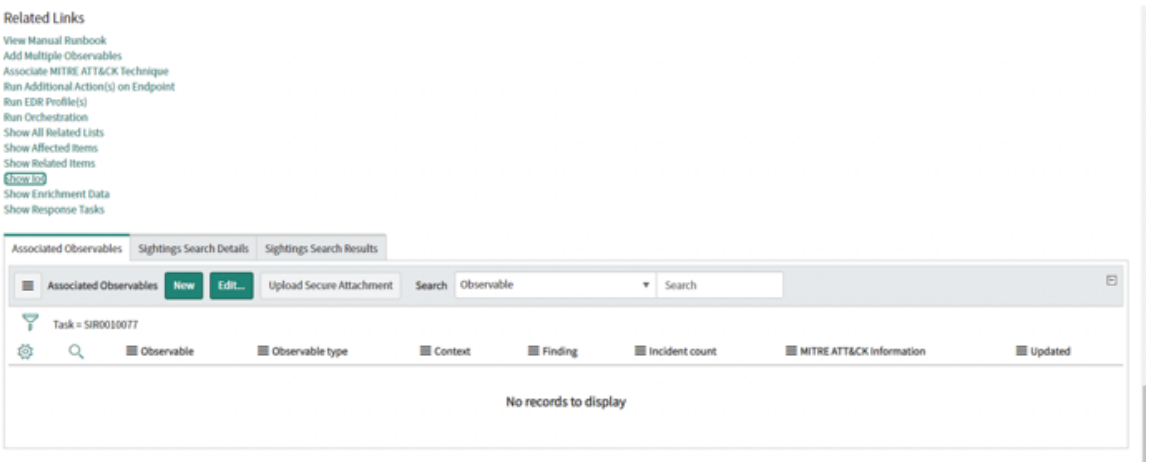
아래 절차에 따라 SIR 보안 인시던트에서 사이팅 검색을 호출합니다.

시작하기 전에

필요한 역할: ServiceNow AI Platform 관리자(sn_si.admin)

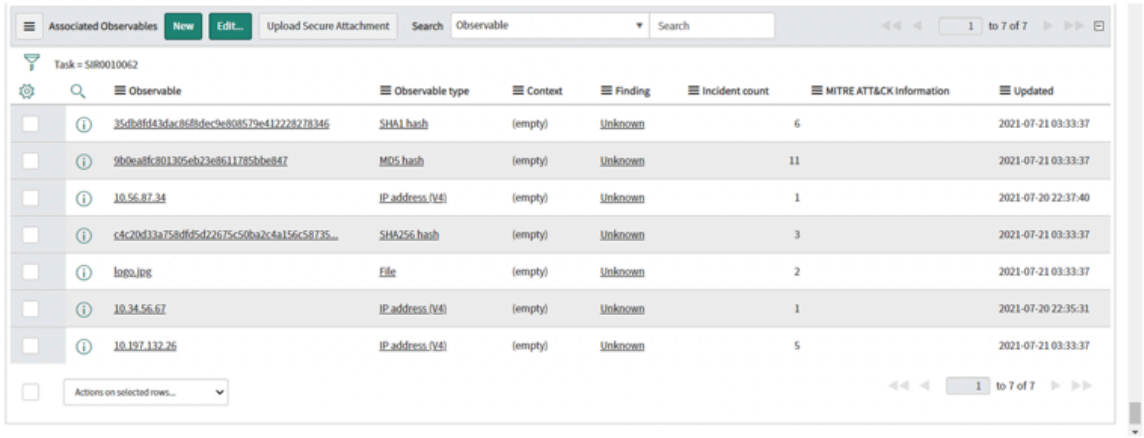
프로시저

1. 보안 인시던트로 이동합니다.
2. 기존 SIR을 열거나 새 SIR을 생성합니다.
3. 관련 링크에 IoC 표시를 클릭합니다.
4. 클릭 연결된 옵저버블 관련 목록.

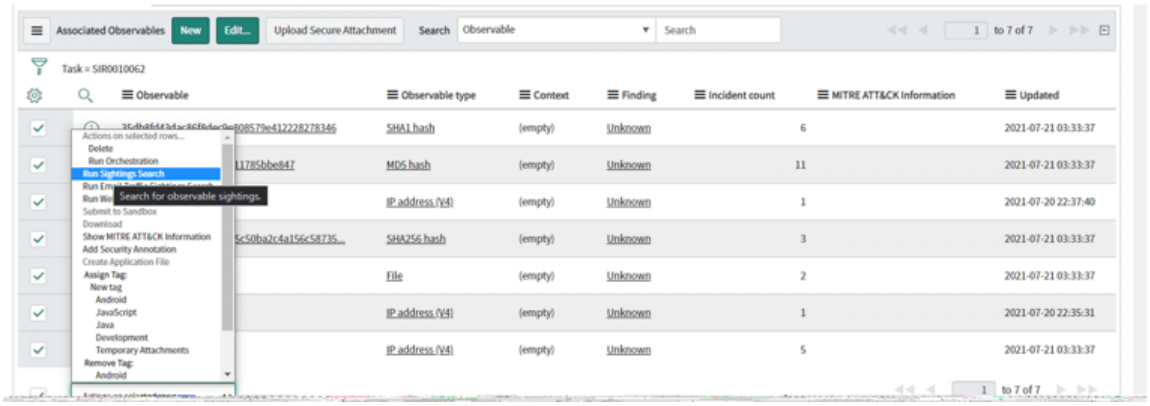


5. 기존 옵저버블을 추가하거나 새 옵저버블을 생성합니다.

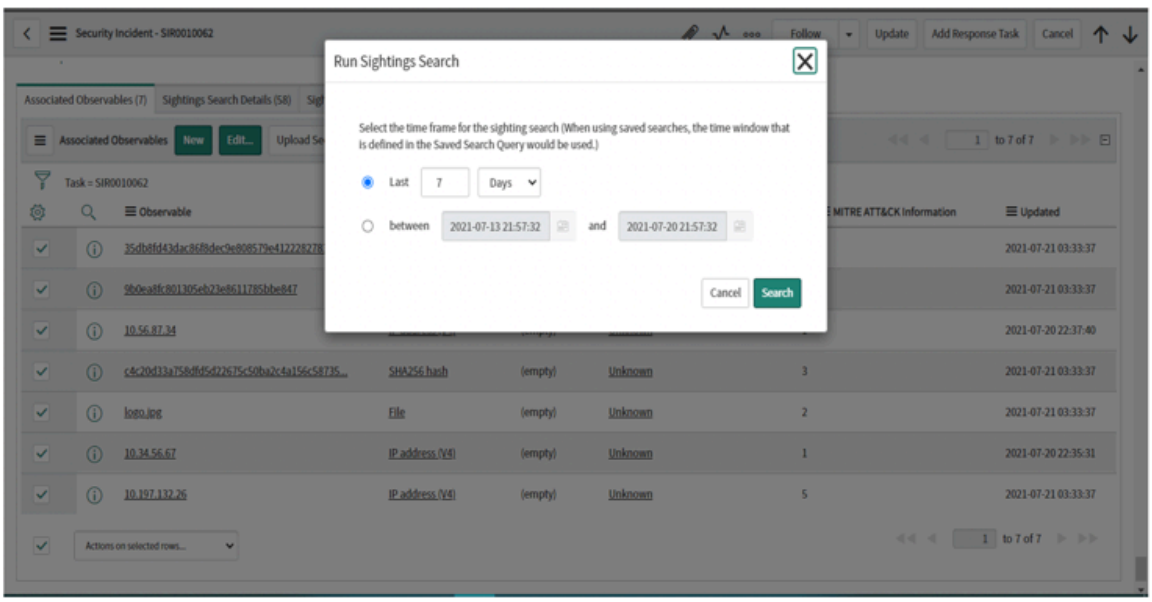
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



6. 옵저버블을 선택하고 선택한 행에 대해 수행할 작업에서 사이팅 검색 실행.

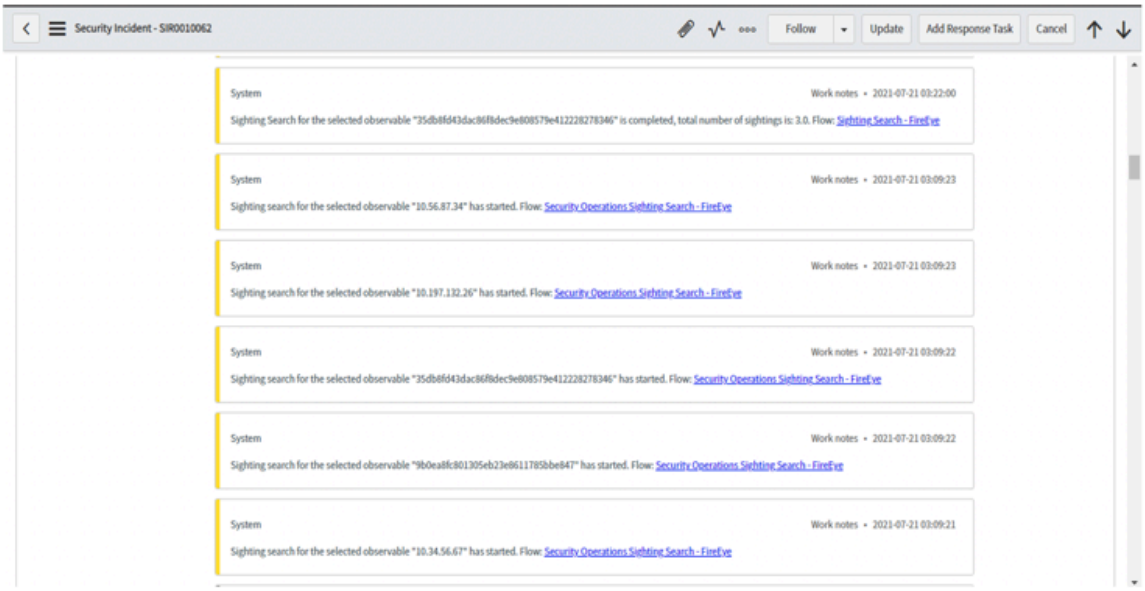


7. 다음 대화 상자에서 시간 데이터를 요청하는 입력은 무시합니다.
채워진 기본값이 있습니다. 그러나 검색은 실시간으로 수행되며 이 통합에 대한 시간 값은 무시됩니다.



8. 상태에 대한 작업 주석을 확인합니다.

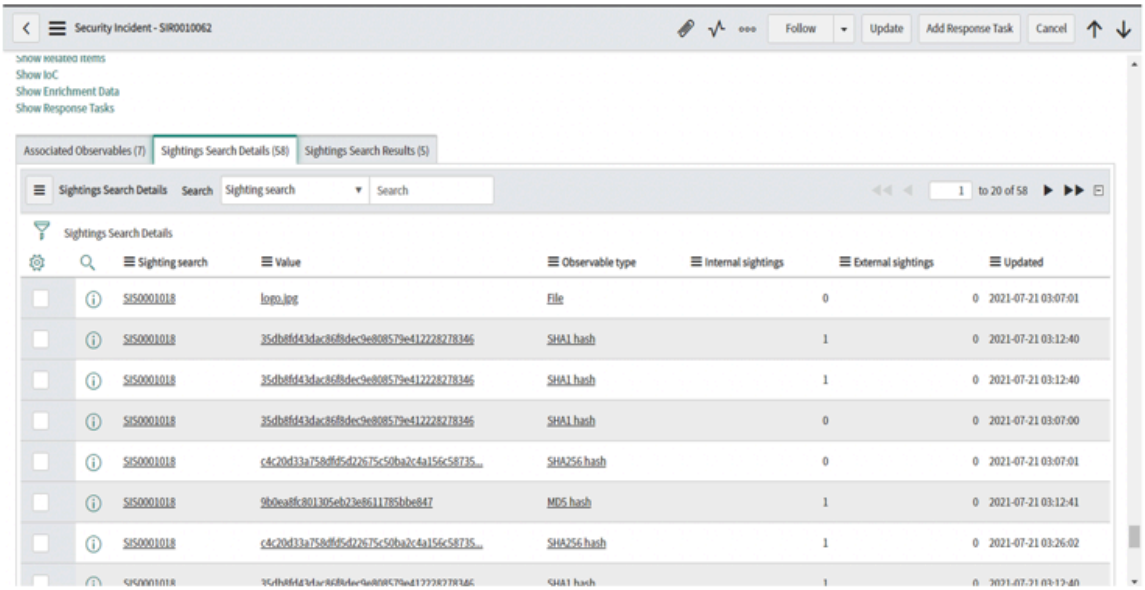
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

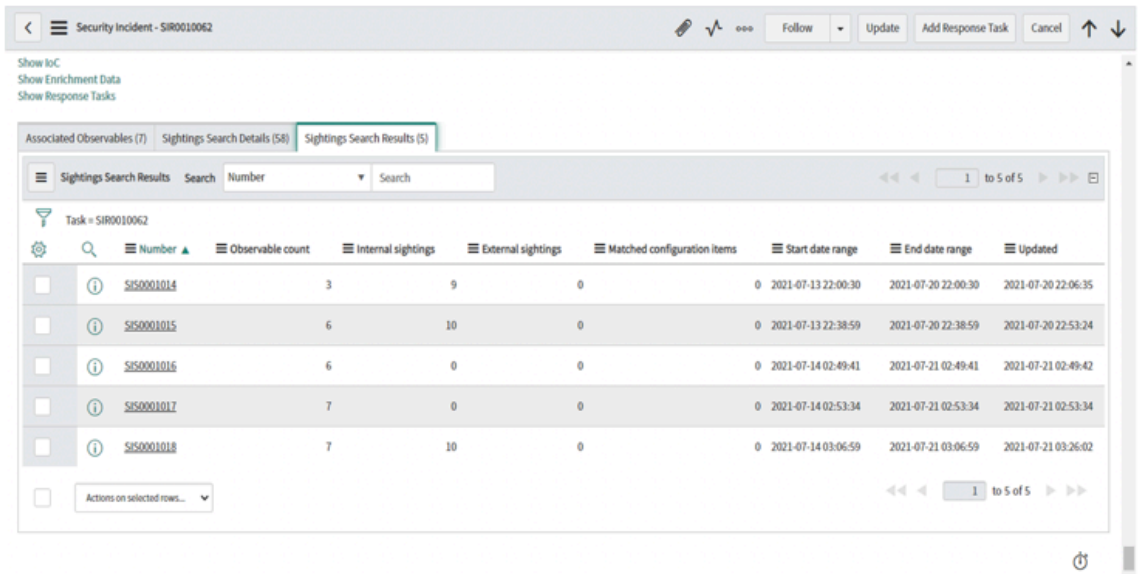


9. 검색이 완료되면 관련 목록에서 결과와 상세 정보를 확인합니다.

10. 클릭 사이팅 검색 정보 탭 - 상세 정보 및 사이팅 검색 결과 검색 결과 탭.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.





Have I been pwned? 통합

통합을 보안 운영 Have I been pwned? 통해 도메인 이름 및 이메일 주소에 대한 조회를 제출하여 데이터 위반으로 인해 사용자 개인 데이터가 손상되었는지 여부를 확인할 수 있습니다.

탐색

보안 인시던트 응답 통합

설정

- Have I been pwned? 통합 설정
- 활성화

사용

옵저버블에 대한 조회 수행 위협 조회 - Have I been pwned? 플로우

개발

- ServiceNow 보안 운영 통합 개발 가이드라인
- 통합 작성을 위한 팁

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 개발자 교육
- 개발자 설명서
- 애플리케이션과 함께 설치되는 구성요소 찾기

문제 해결 및 도움받기

- 통합 문제 해결
- 보안 운영 커뮤니티에서 질문 또는 답변하기
- 알려진 오류 포털에서 알려진 오류 문서 검색

- 연락처 고객 서비스 및 지원

Have I been pwned? 통합 설정

Have I been pwned? 는 데이터 침해로 인해 온라인 계정이 손상되거나 "pwned"되어 누군가가 위험에 처했을 수 있는지 평가하는 데 사용되는 무료 리소스입니다. 와 쉽게 통합됩니다 보안 운영.

통합을 사용하려면 Have I been pwned? 먼저 플러그인을 활성화해야 합니다. 필요한 경우 X509 SSL 인증을 업데이트할 수도 있습니다.

통합을 보안 인시던트 응답구현하려면 , 위협 인텔리전스및 보안 운영 Have I been pwned? 플러그인이 보안 운영 Have I been pwned? 필요합니다.

위협 조회 **- Have I been pwned?** 플로우

위협 조회 - Have I been pwned? 플로우는 선택한 옵저버블에 대해 조회를 수행합니다. 옵저버블이에서 인식 Have I been pwned?하는 유형인 경우 옵저버블에 맬웨어가 있는지 검사되고 결과가 반환됩니다.

필요한 역할: sn_si_admin

이 플로우는 하나 이상의 옵저버블에 대해 위협 조회를 수행하고 구현이 선택될 때 트리거 보안 운영 통합 - 위협 조회 기능 됩니다 Have I been pwned? . 자세한 내용은 옵저버블에 대한 조회 수행 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

내가 **pwned** 흐름이었습니까?

이 플로우에서 사용하는 활동에 대한 자세한 내용은 다음 문서를 일반 Security Operations 통합 플로우 및 오케스트레이션 활동참조하십시오.

활성화

통합 구성 기능을 사용하면 통합을 포함하여 외부 공급업체 보안 통합을 빠르게 활성화하고 설정할 수 있습니다 보안 운영 Have I been pwned? . 통합을 사용하려면 Have I been pwned? 먼저 다음 ServiceNow Store에서 다운로드해야 합니다.

시작하기 전에

- 위협 인텔리전스 통합을 사용하려면 보안 운영 Have I been pwned? 플러그인을 설치하고 활성화해야 합니다.

필요한 역할: sn_si_admin

프로시저

에서 통합을 다운로드합니다. ServiceNow Store.
이 통합은 개방형 API를 지원하며 추가 구성이 필요하지 않습니다. Have I been pwned? 이제 보안 인시던트의 옵저버블 위협 인텔리전스 과 옵저버블에 대한 조회를 수행하기 위해 선택할 수 있습니다.

관련 정보

옵저버블에 대한 조회 수행

X.509 인증서 업데이트

통합에 SSL 연결이 필요한 경우 외부 공급업체 벤더가 제공한 인증서를 아직 신뢰 ServiceNow 하지 않거나 만료된 경우가 있습니다. 이 작업은 선택 사항입니다.

시작하기 전에
필요한 역할: admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 외부 공급업체 벤더로부터 SSL 인증서를 받습니다.
   예를 들어, 다음과 같이 Firefox 브라우저의 SSL 엔드포인트에서 X.509 인증서(PEM)를 임포트할 수 있습니다.

   a. 브라우저 주소 표시줄에 엔드포인트 URL을 입력합니다.
      예: https://<3rdparty>/.

   b. 주소란에서 자물쇠 아이콘을 클릭합니다.

   c. 추가 정보를 클릭하고 보안 탭을 클릭합니다.

   d. **View** Certificate(인증서 보기)를 클릭하고 Detail(세부 정보) 탭을 클릭합니다.

   e. 내보내기를 클릭하여 PEM을 로컬 파일 시스템에 저장합니다.

   f. 저장된 파일을 텍스트 편집기 도구에서 열고 내용을 클립보드에 복사합니다.
      -----BEGIN CERTIFICATE-----로 시작하고 -----END CERTIFICATE-----로 끝나야 합니다.

2. 다음으로 이동 시스템 정의 〉 인증서.
3. 새로 만들기를 클릭하고 통합에 대한 새 기록을 생성합니다.
4. **PEM** 인증서에서 이전에 다운로드하여 클립보드에 복사한 인증서를 붙여넣습니다.
5. ID 제공자 기록에 인증서를 추가합니다.
   a. 다음으로 이동 복수 제공자 **SSO** 〉 **ID** 제공자.
   b. 새 인증서를 만들 활성 기본 ID 제공자를 선택합니다.
   c. 아래로 스크롤하여 **X.509** 인증서 관련 목록을 클릭하고 편집을 클릭합니다.
   d. 새로 만든 인증서를 선택됨 열로 이동합니다.
6. 저장을 클릭합니다.
   기록의 다른 필드는 자동으로 생성됩니다.

   주:
   만료된 인증서가 있는 경우 인증서를 제거해야 합니다. 만료된 인증서를 제거하는 방법에 대한 자세한 내용은 KB0691439 만료되는 SAML 인증서 교체를 참조하십시오.

HPE Security ArcSight ESM - 이메일 파서 통합

HPE Security ArcSight ESM - 이메일 파서 통합은 ESM의 이메일 알림을 사용하여 보안 인시던트를 생성하는 이메일 파서를 사용하여 지원됩니다.

HPE Security ArcSight ESM - 이메일 파서 통합 구성

HPE Security ArcSight ESM - 이메일 파서 통합은 ESM의 이메일 알림을 사용하여 보강 및 응답 워크플로우를 구동합니다.

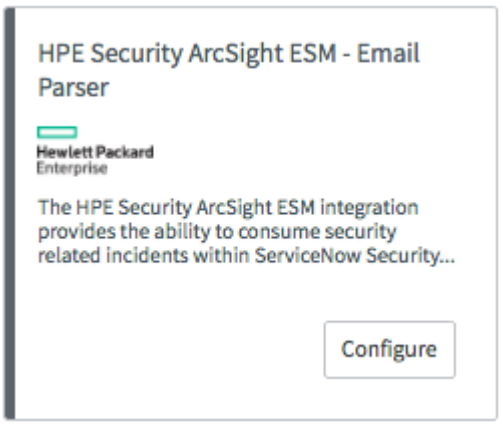
시작하기 전에
필요한 역할: sn_si_admin

이 태스크 정보
통합에 사용할 HPE Security ArcSight ESM - 이메일 파서 템플릿이 제공됩니다. 통합이 발생하기 전에 구성하고 활성화해야 합니다. 파서를 업데이트하면 활성화됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 보안 운영 〉 통합 〉 통합 구성.
   사용 가능한 보안 통합은 일련의 카드로 표시됩니다.



2. HPE Security ArcSight ESM - Email Parser 카드에서 구성을 클릭합니다.
3. **HPE Security ArcSight ESM -** 이메일 파서 구성 대화 상자에서 이메일 파서 구성 링크를 클릭합니다.
4. **ArcSight ESM** 링크를 클릭하여 제공된 템플릿 이메일 파서의 설정을 편집합니다.
   최소한 '### ###' 필드를 채우십시오. 고유한 이메일 파서를 생성하려면 문서를 참조하십시오 보안 운영에서 이메일 파서 생성.
5. 활성 상자를 선택합니다.
6. 이메일 파서 양식에서 업데이트를 클릭합니다.
   이메일 파서가 활성 상태입니다. 통합 구성으로 돌아갈 필요가 없습니다.

HPE ArcSight Logger - 인시던트 보강 통합

인시던트 보강 통합은 HPE ArcSight Logger 로그를 검색하고 관련 사이팅 정보를 보안 인시던트에 추가합니다.

탐색	설정
보안 인시던트 응답 통합	• 시작하기 HPE ArcSight Logger • 사이팅 검색 구성 기록 생성
사용	**개발**
• 사이팅 검색 실행 • Security Operations Integration - 사이팅 검색 플로우 • 보안 운영 - Arcsight 로거 사이팅 검색 플로우 • 사이팅 검색 상세 정보 보기 • 사이팅 검색 결과 보기	• ServiceNow 보안 운영 통합 개발 가이드라인 • 통합 작성을 위한 팁 • 개발자 교육 • 개발자 설명서 • 애플리케이션과 함께 설치되는 구성요소 찾기

문제 해결 및 도움받기

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 통합 문제 해결
- 보안 운영 커뮤니티에서 질문 또는 답변하기
- 알려진 오류 포털에서 알려진 오류 문서 검색

- 연락처 고객 서비스 및 지원

시작하기 **HPE ArcSight Logger**

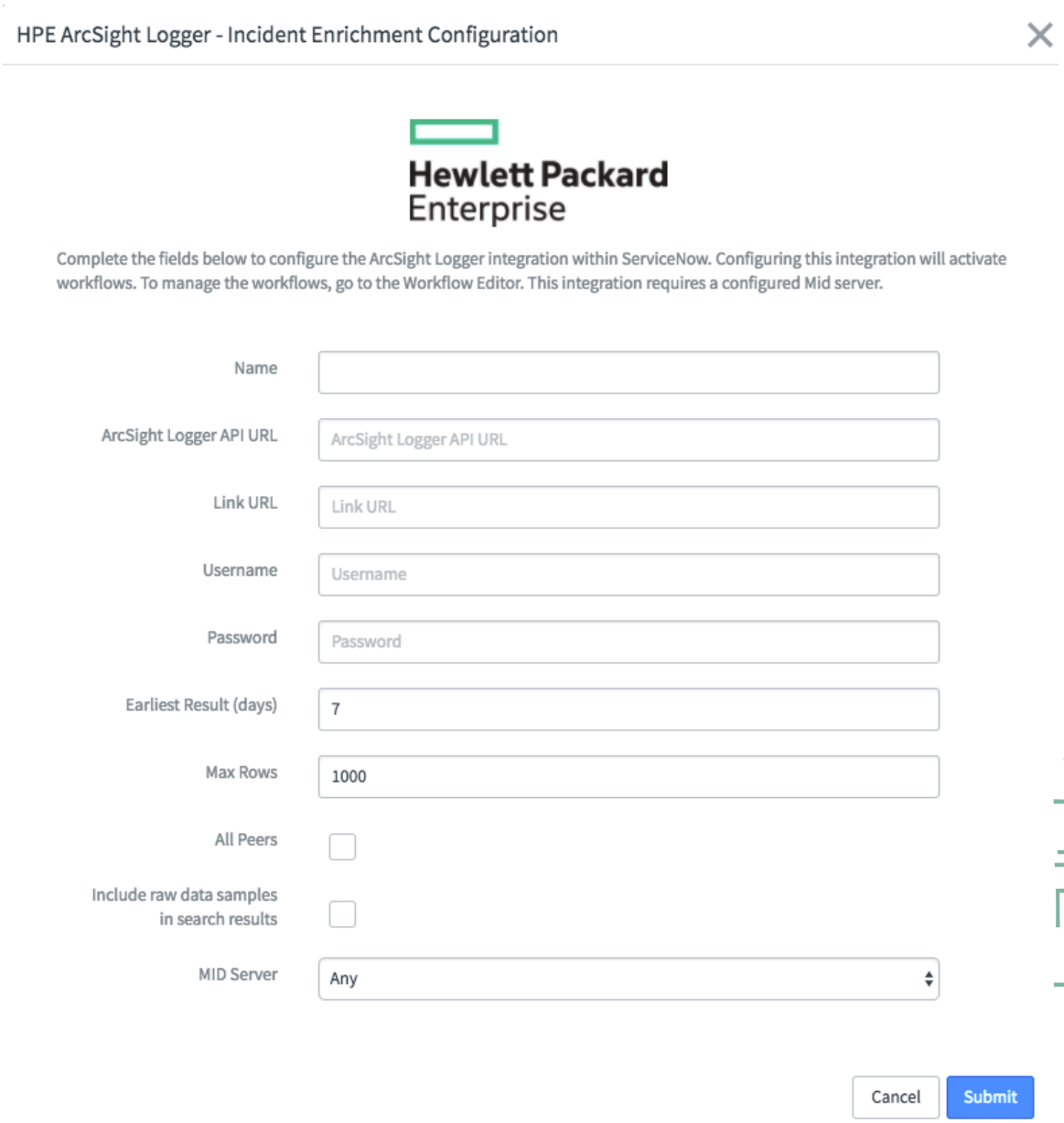
HPE ArcSight Logger 실시간 데이터를 스트리밍하여 특정 로그로 분류하고 보안 운영. 인시던트 보강 통합을 사용하려면 HPE ArcSight Logger 먼저 다음 ServiceNow Store 에서 다운로드하여 API URL과 로그인 자격 증명을 추가해야 합니다.

시작하기 전에
필요한 역할: sn_si_admin

프로시저

1. 에서 통합을 다운로드합니다. ServiceNow Store.
2. 설치가 완료되면 보안 운영 〉 통합 〉 통합 구성.
   사용 가능한 보안 통합은 일련의 카드로 표시됩니다.
3. - 인시던트 보강 카드에서 HPE ArcSight Logger새로 만들기를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 필요에 따라, 필드를 채웁니다.

필드	설명
이름	이 구성의 이름입니다.
ArcSight 로거 API 기준 URL	HPE Security ArcSight Logger 사이트에서 가져온 기본 URL입니다.
링크 URL	〔선택사항〕 사용 가능한 경우 HPE Security ArcSight Logger 인스턴스에 연결되는 링크 URL입니다.
사용자 이름	인텔 HPE ArcSight Logger 사용자 이름입니다.
암호	인텔 HPE ArcSight Logger 암호입니다.
가장 빠른 결과(일)	일수 단위로 보려는 가장 빠른 결과입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
최대 행 수	검색할 행의 최대 수입니다.
모든 피어	기본값은 선택 취소되어 있으며 연결된 로컬 로거만 검색합니다. 선택하면 서로 연결된 모든 로거를 검색합니다.
검색 결과에 원시 데이터 샘플 포함	사이팅 검색 결과에 원시 데이터 샘플을 포함하려면 이 옵션을 선택합니다. 반환되는 데이터의 양은 보안 인시던트 응답 속성의원시 데이터 속성 행 수의 설정에 따라 달라집니다.
MID 서버	활성 MID 서버를 사용하려면 임의 를 선택하고, 특정 MID 서버 이름을 선택합니다.

주:
이 통합을 구성하면 워크플로우가 활성화됩니다. 워크플로우를 관리하려면 워크플로우 편집기로 이동합니다.

5. 제출을 클릭합니다.
   통합 구성 카드가 표시됩니다.
6. 새 구성 카드를 볼 때 구성 또는 삭제를 클릭하여 구성을 변경하거나 삭제할 수 있습니다.
7. 통합 구성 카드의 원래 목록으로 돌아가려면 구성 표시 드롭다운 목록에서 아니요를 선택합니다.

하이브리드 분석 통합

이 하이브리드 분석 응용 프로그램은 사용자가 위협에 대한 파일과 URL을 분석하는 개방형 온라인 커뮤니티의 일부입니다. 결과를 공유하고 커뮤니티의 조사를 활용하여 보다 효과적인 인시던트 응답을 수행합니다. 제품과 통합 ServiceNow AI Platform 보안 운영 되면 공유 위협 인텔리전스가 특정 옵저버블의 심각도에 대한 추가 인사이트를 제공합니다.

통합은 하이브리드 분석 다음 옵저버블에 대해 위협 조회를 수행합니다.

- 파일 해시
- IP 주소
- URL

플로우는 새 옵저버블이 보안 인시던트에 도착하면 이를 확인합니다. 옵저버블이 API 통합에서 인식되는 유형인 경우 옵저버블이 평가됩니다. 악성으로 확인된 옵저버블에 태그가 지정됩니다.

설치 및 구성

인스턴스에서 통합을 실행하기 전에 설치 및 구성 단계를 하이브리드 분석 완료하여 애플리케이션이 .ServiceNow AI Platform 보안 운영

시작하기 전에

설치하기 전에 다음 설정 검사 목록을 완료합니다. 이러한 설정 작업은 원활한 설치 및 구성을 위해 필요합니다.

설정 작업	설명
필수 ServiceNow AI Platform 및 보안 인시던트 응답 역할을 할당했는지 확인합니다.	예상 결과의 설치, 구성 및 검증에 필요한 역할은 다음과 같습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설정 작업	설명
	• 관리자(admin)가 앱을 설치하고 보안 인시던트 관리자(sn_si.admin) 역할을 할당합니다. • 보안 인시던트 관리자(sn_si.admin)는 구성을 감독하고 예상 결과를 검증합니다. 또한 이 역할은 모듈에 액세스할 보안 운영 수 있으며 sn_si.analyst 역할을 할당합니다.
API 키를 가져옵니다.	API 키에 대한 정보를 확인하고 계정을 작성하려면 하이브리드 분석웹 사이트를 방문하십시오. 구성하려면 API 키를 입력해야 합니다.
ServiceNow 통합을 위해 애플리케이션을 설치하기 전에 통합을 지원하는 데 필요한 핵심 애플리케이션이 설치되고 활성화되었는지 확인합니다.	Madrid 릴리스 및 이후 제품군 릴리스의 경우 com.snc.si_dep 플러그인이 필요합니다. 이 플러그인은 제품을 지원하는 데 필요한 모든 종속성을 보안 인시던트 응답 자동으로 설치합니다. 다른 보안 운영 애플리케이션을 설치 및 활성화하기 전에 이 플러그인을 설치하고 활성화하십시오. 에서 ServiceNow Store다음 보안 운영 애플리케이션을 설치하고 활성화해야 합니다. 원활한 설치를 위해 아래 나열된 순서대로 한 번에 하나의 애플리케이션을 설치하고 활성화합니다. **1.** 보안 통합 프레임워크 **2.** Security Support Common **3.** 보안 지원 오케스트레이션 **4.** 보안 인시던트 응답 통합을 위한 인스턴스 설정에 ServiceNow AI Platform 대한 자세한 내용은 해당 문서를 애플리케이션 활성화 ServiceNow Store참조하십시오제품 또는 애플리케이션에 대한 보안 운영 권리 가져오기.

필요한 역할: 관리자

이 태스크 정보

다음 단계를 수행하여 시스템 속성을 업데이트하고 통합을 설치 및 구성합니다.

프로시저

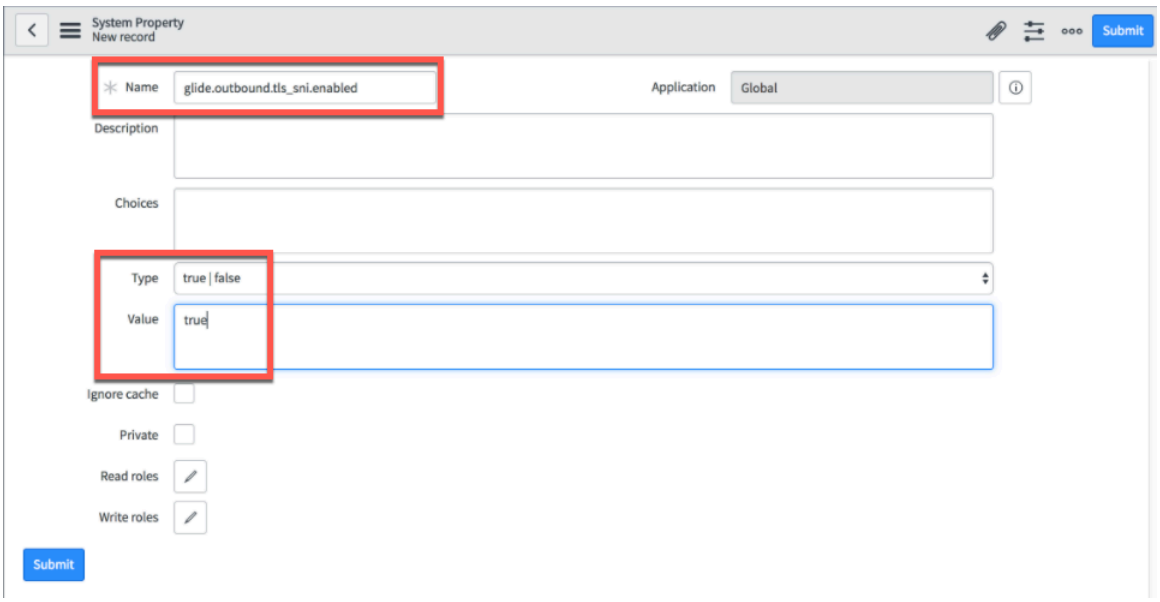
1. 탐색 필터에서 sys_properties.list를 입력하고 **Enter** 키를 누릅니다.
시스템 속성 목록이 표시됩니다.

2. 새로 만들기를 클릭합니다.
새 기록이 표시됩니다.

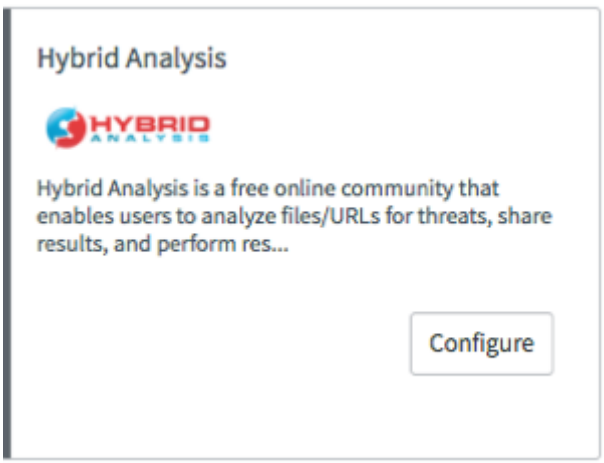
3. 필드를 입력하거나 다음 테이블에 나열된 값을 선택하고 제출을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드 이름	값
이름	glide.outbound.tls_sni.####
유형	**true I false** 선택
값	true

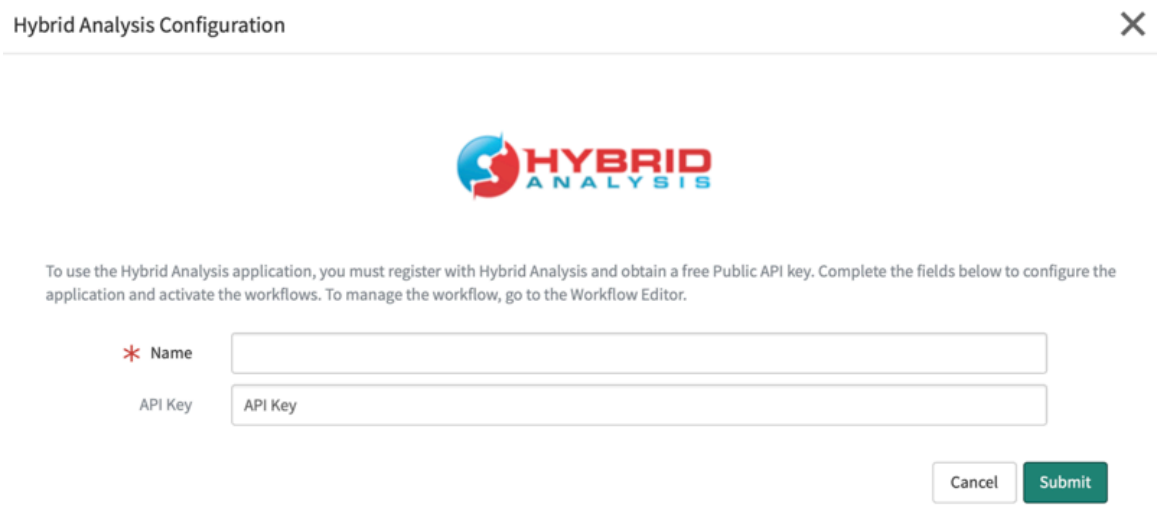


4. 통합을 위해 애플리케이션을 설치하지 않은 경우 이를 확인하고 보안 운영 통합 설치 단계에 따라 설치합니다.
5. 설치가 완료되면 통합 〉 통합 구성 타일을 하이브리드 분석 찾습니다.
6. 구성을 클릭합니다.



7. 하이브리드 분석 구성 대화 상자에서 웹 사이트에서 가져온 하이브리드 분석 API 키를 입력하고 제출을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



8. 구성이 성공했는지 확인합니다.
   오류 메시지가 표시되지 않는 한 구성이 성공적으로 완료된 것입니다.

   Trouble?

   구성 하이브리드 분석 중에 오류 메시지가 표시되면 API 키가 잘못되었을 수 있습니다.

예상 결과 확인

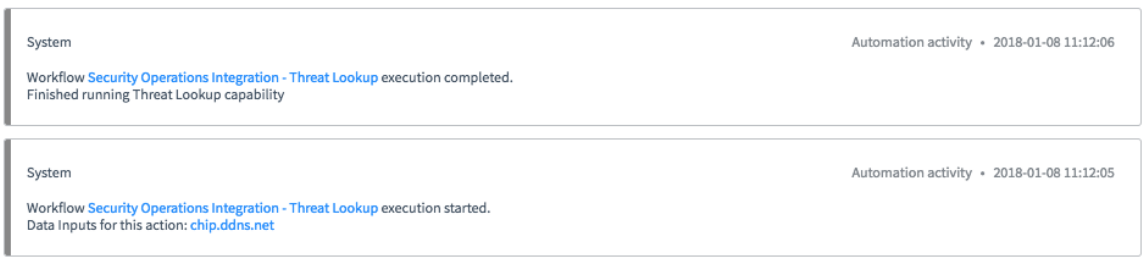
옵저버블은 보안 인시던트에 의해 자동으로 생성되고 애플리케이션에서 검사됩니다. 보안 인시던트에서 조회 결과를 찾아 위협 조회가 성공적으로 실행되었는지 확인합니다. 또한 원시 데이터를 보고 하위 옵저버블에 대한 위협 조회를 실행합니다.

시작하기 전에

필요한 역할: sn_si.analyst

프로시저

1. 작업 중인 보안 인시던트 기록을 열고 조회가 성공적으로 실행되었는지 확인합니다.

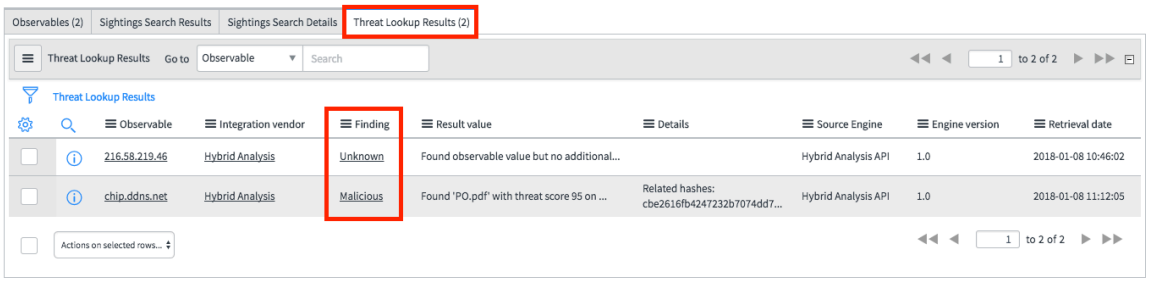


   애플리케이션이 구성되면 인시던트 생성 시 플로우가 자동으로 시작됩니다. 조회의 실행 및 완료 상태가 보안 인시던트의 작업 메모에 표시됩니다.

2. 조회가 성공적으로 실행되었는지 확인할 수 없는 경우 진행 방법에 대한 자세한 내용은 작업 메모를 검토하십시오.
3. 보안 인시던트 기록의 하단으로 이동하고 모든 관련 목록 표시 관련 링크를 클릭하여 결과를 봅니다.

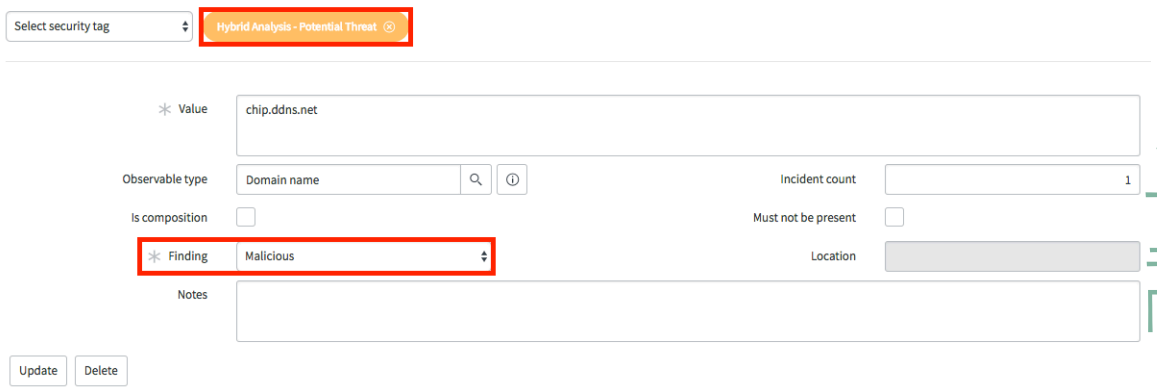
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
다음 단계의 그림은 시스템 설정에서 탭 양식 설정이 활성화된 상태로 표시됩니다. 배너 프레임의 오른쪽 위 모서리에서 설정 기어 아이콘을 클릭합니다. 표시되는 시스템 설정 대화 상자에서 폼을 클릭하고 탭 폼 및 폼 사용이 선택되어 있는지 확인합니다.



위협 조회 결과 탭은 보안 인시던트 기록 하단에 조회 결과를 표시합니다. 악성으로 확인되지 않은 기록에 대해서는 결과 열에 # # ## 이 표시됩니다. 악성과 일치하는 결과의 경우 결과 열에 ### 표시됩니다.

4. 옵저버블 열에서 옵저버블을 클릭하여 기록을 엽니다.



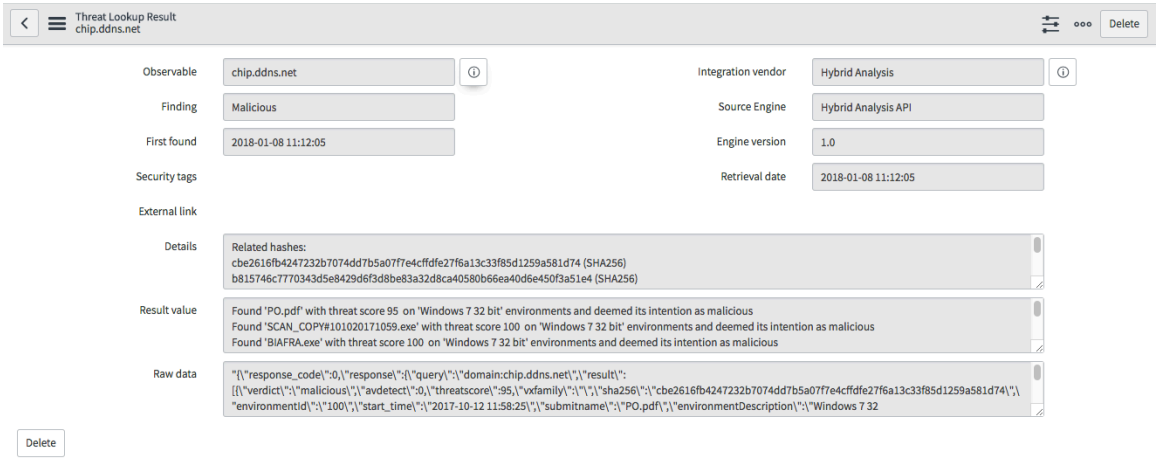
악성과 일치하는 조회의 경우 찾기 필드에 ### 표시되고, 옵저버블에는 악성으로 확인된 소스(이 경우 통합)하이브리드 분석가 태그됩니다위협 인텔리전스.

5. 옵션: 단계에 따라 원시 데이터를 보고, 하위 옵저버블 목록을 보고, 선택한 하위 옵저버블에 대한 위협 조회를 실행합니다.

a. 보안 인시던트로 다시 이동하여 위협 조회 결과 탭에서 옵저버블 옆에 있는 파란색 정보 아이콘을 클릭합니다.

b. 표시되는 창에서 기록 열기 를 클릭하여 데이터를 봅니다.
또한 조회를 통해 표시되는 원시 데이터에서 볼 수 있는 모든 옵저버블에서 통합은 하이브리드 분석 하위 옵저버블 또는 관련 옵저버블을 생성합니다.

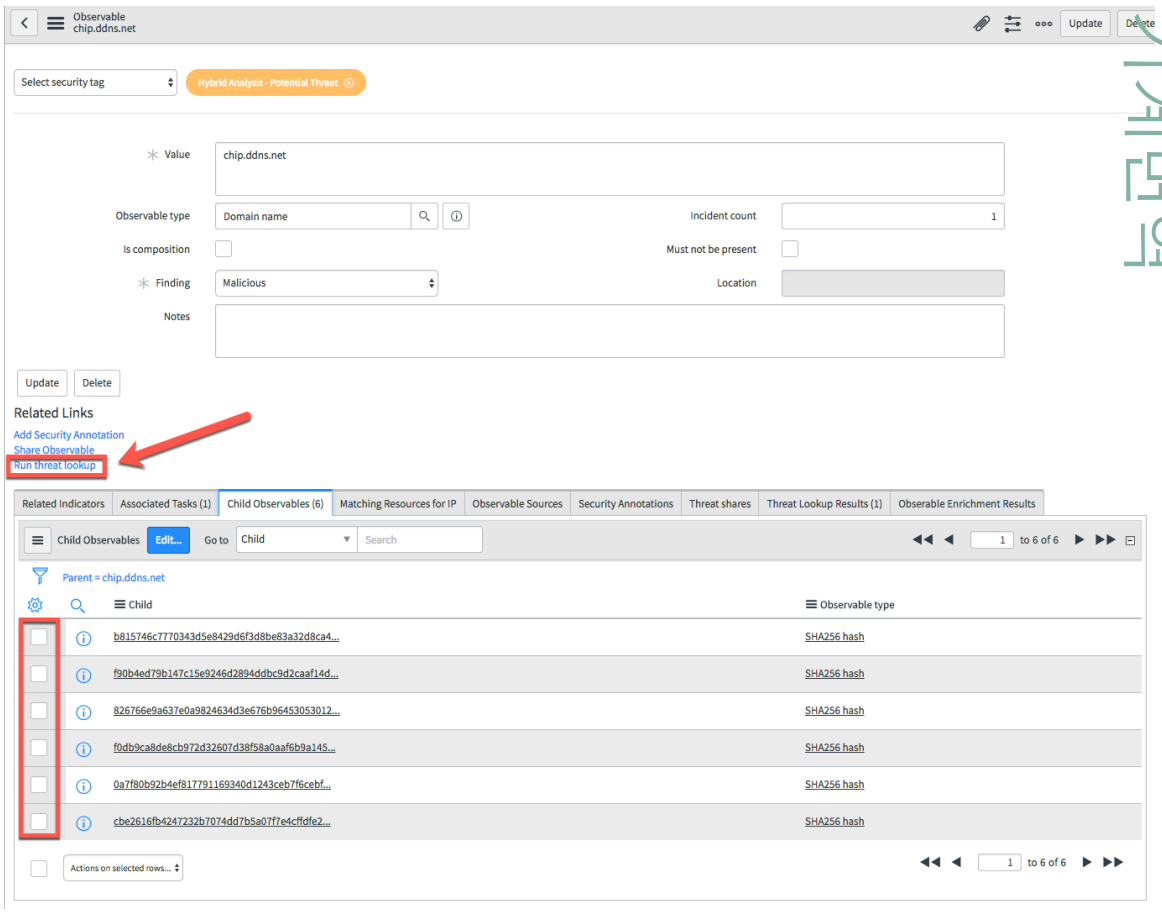
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



API에서 생성한 링크, 원시 데이터 및 기타 정보가 표시됩니다.

c. 보안 인시던트로 다시 이동하여 **IoC** 표시 관련 링크를 클릭합니다.
하위 옵저버블은 보안 인시던트의 하위 옵저버블 탭에 표시됩니다. 이는 조회에서 이러한 관련 옵저버블과 처음에 제출된 옵저버블 간의 기존 연결을 발견했기 때문입니다.

d. 하위 열에서 옵저버블 옆에 있는 필드를 클릭하여 선택한 다음 위협 조회 실행 관련 링크를 클릭하여 조회를 수행합니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

e. 표시되는 대화 상자에서 통합이 하이브리드 분석 선택되었는지 확인하고 제출을 클릭합니다.

f. 작업 메모에서 조회가 성공적으로 실행되었는지 확인하고 보안 인시던트의 위협 조회 결과 탭에서 하위 옵저버블에 대한 조회 결과를 찾습니다.

Trouble?
위협 조회 결과 탭에 결과가 표시되지 않으면 옵저버블이 통합에서 조회를 위해 지원하는 유형인지 확인합니다.

(선택 사항) 다음에 대한 옵저버블을 수동으로 첨부 하이브리드 분석

초기 이벤트 트리거에서 보안 인시던트에 첨부되지 않은 옵저버블에 대해 위협 조회를 수행하려는 경우 옵저버블을 수동으로 첨부할 수 있습니다. 또한 관련 옵저버블에 대한 자세한 정보가 필요한 경우에도 이 작업을 수행할 수 있습니다.

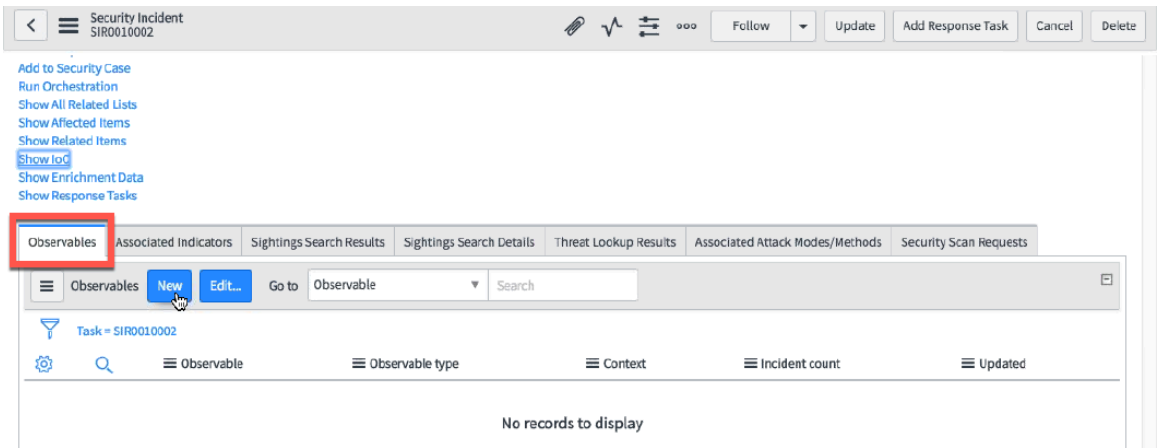
시작하기 전에
옵저버블이 통합에서 지원되는 유형인지 확인합니다. 통합은 다음 유형의 옵저버블에 대한 조회를 수행합니다.

- 파일 해시
- IP 주소
- URL

필요한 역할: sn_si.analyst

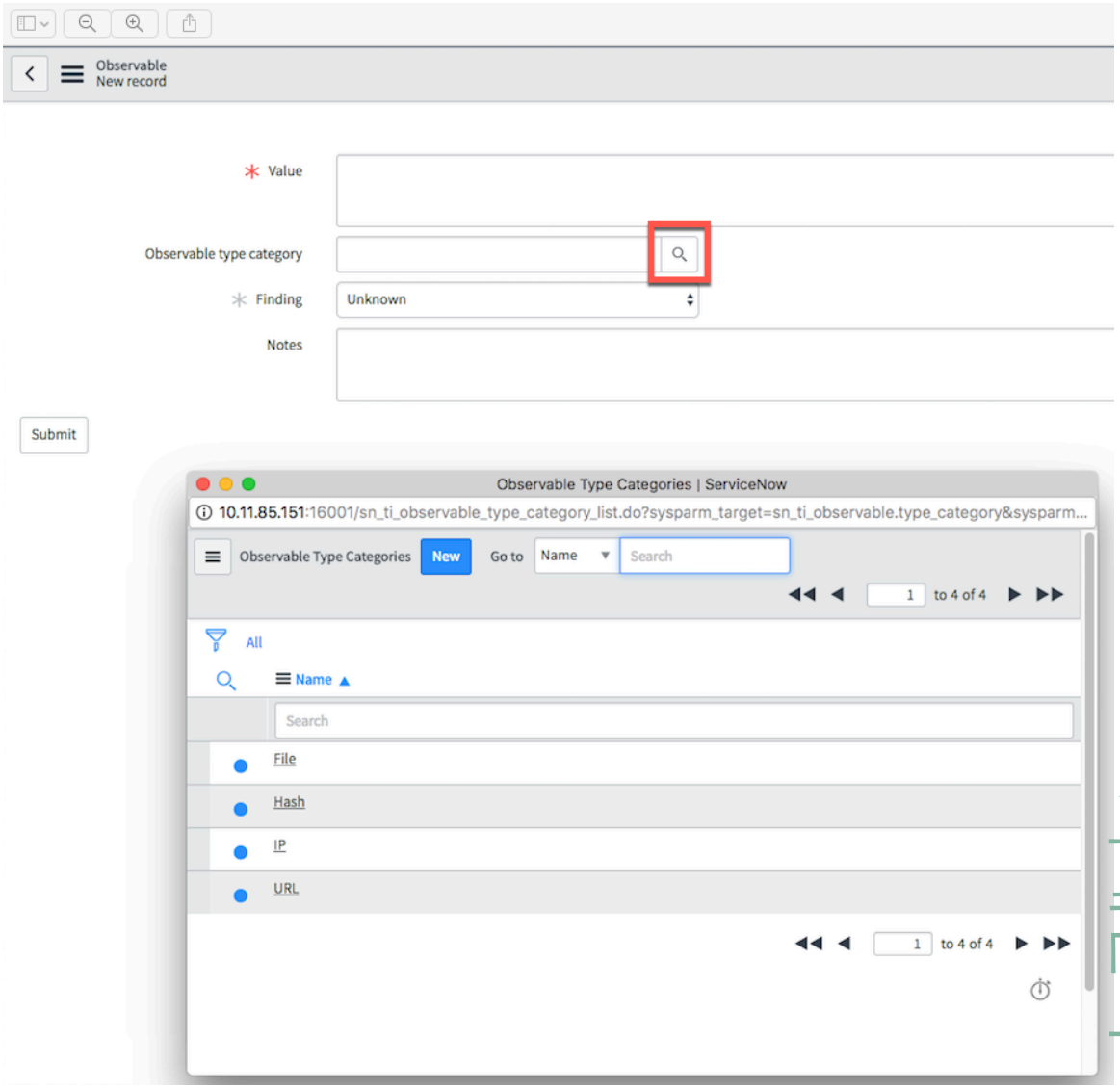
프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 인시던트 〉 모든 인시던트 표시 및 옵저버블을 연결할 보안 인시던트를 엽니다.
2. 오픈 보안 인시던트에서 관련 링크의 **IoC** 표시링크를 클릭합니다.



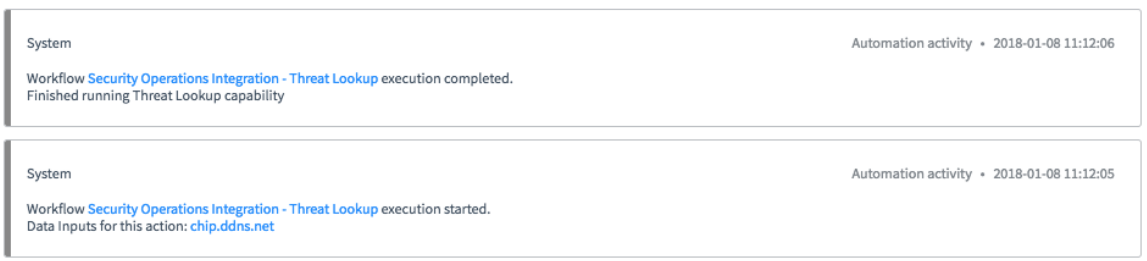
3. 옵저버블 탭에서 새로 만들기를 클릭합니다.
옵저버블 양식이 표시됩니다.
4. 값 필드에 옵저버블(파일 해시, IP 주소 또는 URL)을 입력합니다.
5. 검색 아이콘을 클릭하고 옵저버블 유형 범주 대화 상자의 목록에서 원하는 옵저버블 유형을 클릭하여 필드를 채웁니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



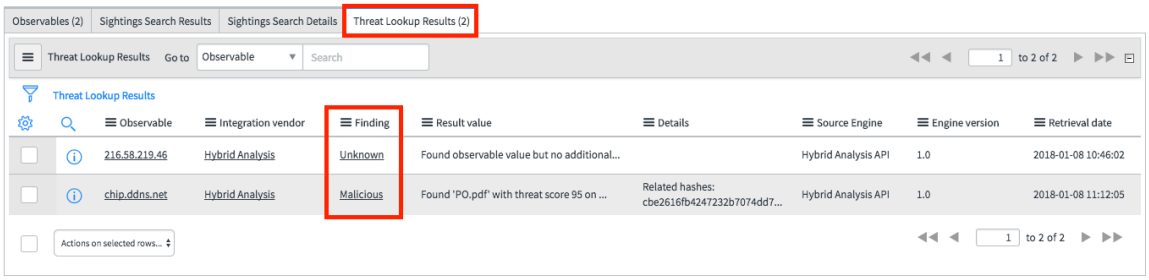
기계번역

6. 제출을 클릭합니다.
   플로우가 시작되고 새 옵저버블이 있는지 확인합니다. 실행 및 완료 상태는 보안 인시던트 기록의 작업 메모 섹션에 표시됩니다.
7. 보안 인시던트로 이동하여 작업 메모를 검토합니다.

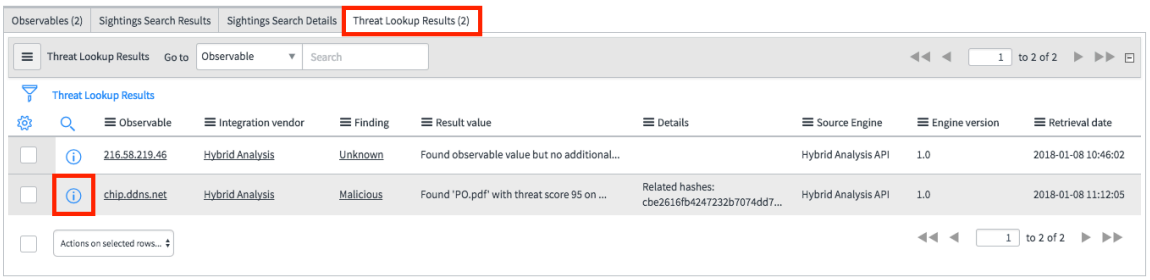


8. 기록 하단에서 모든 관련 목록 표시 관련 링크를 클릭합니다.
9. 위협 조회 결과 탭을 클릭하여 결과를 확인합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



10. 옵저버블 열에서 지정된 옵저버블 옆에 있는 파란색 정보 아이콘을 클릭하면 자세한 정보와 원시 데이터를 볼 수 있습니다.



11. 표시되는 대화 상자에서 기록 열기 를 클릭하여 원시 데이터 및 자세한 내용을 봅니다.
또는 기존 옵저버블을 보안 인시던트 기록에 첨부할 수도 있습니다.

12. 옵션: 옵저버블 탭을 선택한 상태에서 편집을 클릭합니다.

13. 옵션: 표시되는 구성원 편집 양식에서 기존 옵저버블을 컬렉션 에서 옵저버블 목록으로 이동하고 저장을 클릭합니다.
보안 인시던트로 돌아갑니다.

14. 맨 왼쪽 열에서 조회를 실행할 옵저버블을 선택하고 선택한 행에 대해 수행할 작업... 선택 목록에서 위협 조회 실행을 선택합니다.
기록 상단에 요청이 처리 중이라는 메시지가 표시됩니다. 조회가 성공적으로 실행되었는지 확인합니다.

Trouble?
자세한 내용은 작업 메모를 검토하고, 조회가 성공적으로 실행되었는지 확인할 수 없는 경우 진행 방법을 확인하십시오.

IBM QRadar Offense Ingestion 통합

통합을 IBM QRadar Offense Ingestion 통해 위반을 자동으로 가져와서 IBM QRadar 보안 인시던트로 변환하고 자동화된 응답 작업을 활성화할 수 있습니다.

이 통합은 다음을 지원합니다.

- 보안 인시던트의 후보인 위반을 IBM QRadar 검색합니다.
- 위반과 관련된 최근 이벤트 또는 플로우 가져오기
- 위반에 대한 주요 업데이트를 주기적으로 추적합니다.
- 위반, 이벤트 및 플로우 필드를 보안 인시던트 필드에 매핑합니다.
- 매핑된 필드의 예비 뷰입니다.
- 보안 인시던트를 주기적으로 생성하기 위해 예약된 위반 수집을 설정합니다.
- 보안 인시던트가 종결되면 위반을 종결합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

공격 수집 통합을 위한 **IBM QRadar** 애플리케이션 설치 및 구성 **ServiceNow**

인스턴스에서 통합을 ServiceNow AI Platform# 실행하기 전에 다음 설치 및 구성 단계를 완료하여 애플리케이션이 인스턴스의 및 보안 운영 제품과 ServiceNow AI Platform 제대로 통합 보안 인시던트 응답 되도록 합니다.

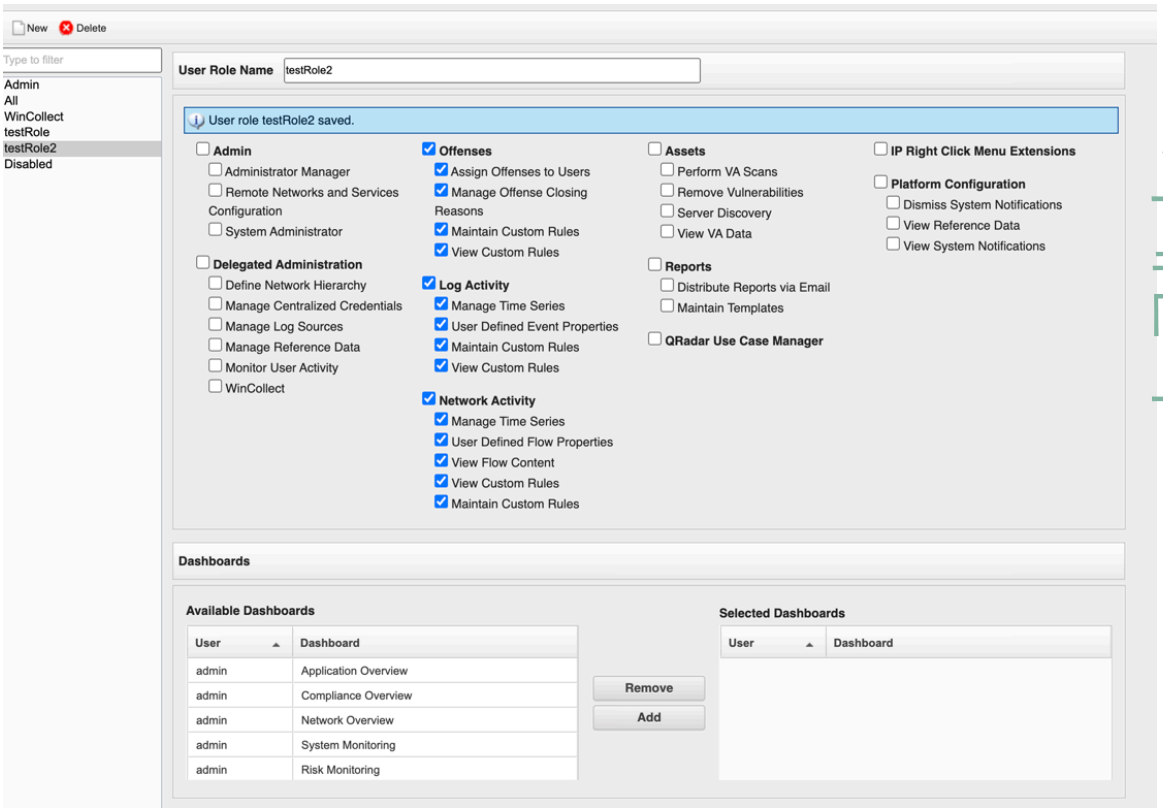
시작하기 전에

필요한 역할: sn_si.admin

프로시저

1. 통합을 위해 애플리케이션을 ServiceNow Store 설치하지 IBM QRadar 않은 경우 를 참조 보안 운영 통합 설치 하고 단계에 따라 설치합니다.
2. 애플리케이션을 성공적으로 설치한 후 통합 〉 통합 구성 타일을 IBM QRadar 찾습니다.
3. 애플리케이션을 구성하려면 새로 만들기를 클릭합니다.
4. 또는 구성 단추가 타일에 표시되면 클릭하여 기존 구성을 편집합니다.
5. 표시되는 위반 수집 구성 대화 상자에서 필드를 채웁니다.

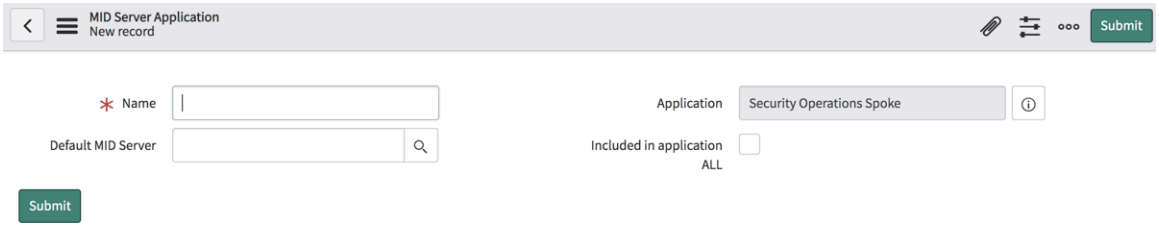
최소 사용자 역할



새 MID 서버 애플리케이션을 작성하려면 다음 단계를 따르십시오.

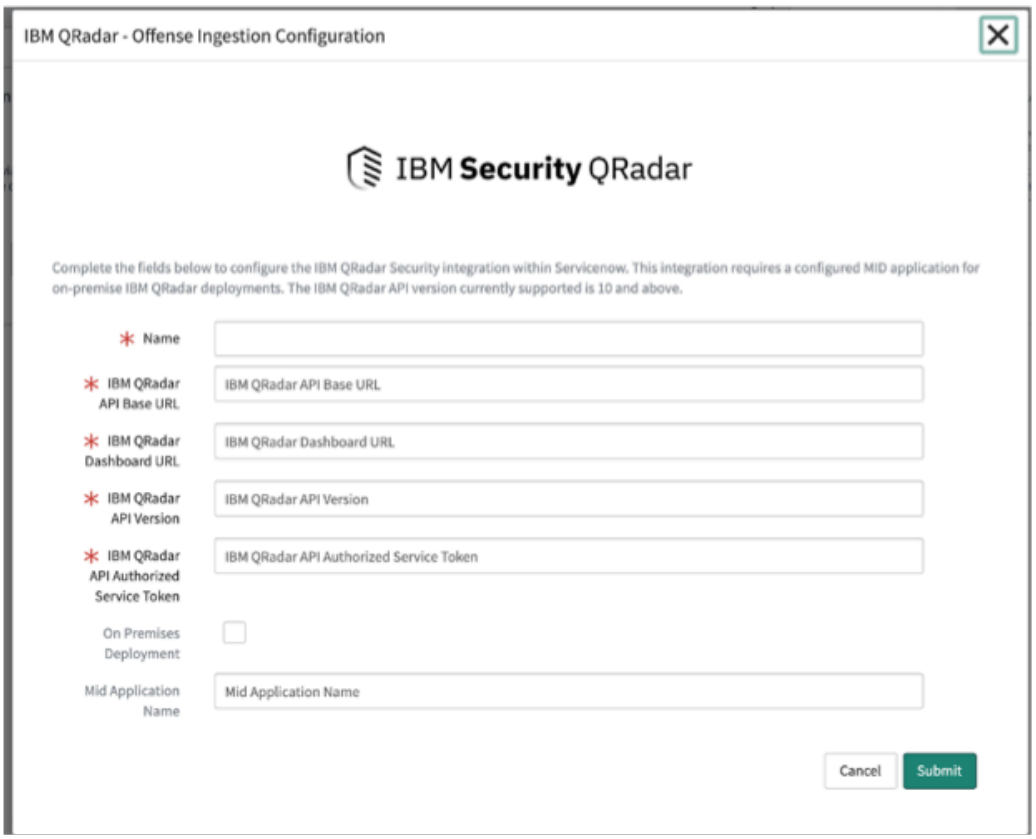
- 다음으로 이동 **MID** 서버 〉 애플리케이션 을 클릭하고 신규를 클릭합니다.
- MID 서버 애플리케이션의 이름을 입력하고 기본값으로 사용할 MID 서버를 선택합니다.
- 애플리케이션 ALL에 포함됨 확인란의 선택을 취소하고 저장을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



- 편집을 클릭합니다. 구성원 편집 페이지에서 사용 가능한 모든 MID Server를 선택하고 MID 서버 목록으로 이동한 다음 저장을 클릭합니다. 가용성에 따라 MID Server 애플리케이션으로 구성된 MID Server 중 하나가 사용됩니다.

6. 구성 상세 정보를 입력하고 생성한 MID 서버 애플리케이션을 지정합니다.



IBM QRadar Offense Ingestion Configuration 양식에서 구성하는 소스는 각 프로파일이 위반을 수집하는 한 여러 ServiceNow AI Platform 프로파일에 재사용할 수 있습니다.

7. 제출을 클릭합니다.
성공적으로 확인 및 제출된 각 IBM QRadar 서버 구성은 보안 통합 페이지에 타일로 저장됩니다. 저장된 구성 타일이 보안 통합 페이지에 표시되지 않으면 페이지 오른쪽 상단 모서리에 있는 구성 선택 목록 표시에서 예를 클릭합니다.

> **주:**
> 도메인 세분화 기능에 문제가 IBM QRadar 발생하면 고객 지원에 문의하여 IBM QRadar 도움을 받으십시오.

다음에 수행할 작업
애플리케이션을 성공적으로 설치하고 구성했습니다. 다음 단계는 프로필을 만드는 것입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

ServiceNow AI Platform® 공격 수집 통합을 위한 IBM QRadar 인스턴스 설정

다음 섹션에서는 에서 애플리케이션을 ServiceNow Store설치하기 전에 인스턴스에서 완료해야 ServiceNow AI Platform# 하는 설정 작업을 나열합니다.

시작하기 전에

필요한 역할: sn_si.admin

이 태스크 정보

원활한 설치 및 구성을 위해 애플리케이션을 다운로드하고 설치하기 전에 다음 테이블을 참조하고 나열된 작업을 모두 완료했는지 확인하십시오.

설정 작업	설명
필수 ServiceNow AI Platform# 역할과 보안 인시던트 응답(SIR) 역할을 할당했는지 확인합니다.	인스턴스에서 통합을 ServiceNow AI Platform# 설치, 설정 및 사용하려면 다음 역할이 필요합니다. • 관리자 역할(admin)의 ServiceNow AI Platform# 사용자는 보안 인시던트 관리자(sn_si.admin) 역할을 사용하여 ServiceNow Store 애플리케이션을 설치하고 할당합니다. • sn_si.admin 역할을 가진 사용자는 다음 ServiceNow AI Platform#에서 다음 작업을 감독합니다. ○ 위반 프로파일의 이름을 지정하고, 생성하고, 편집합니다. ○ 위반 데이터 필드를 선택하고 보안 인시던트 필드에 매핑 IBM QRadar 합니다. ○ 구성을 완료하기 전에 보안 인시던트 상세 정보가 정확한지 미리 봅니다. ○ 진행 중인 공격 수집을 예약합니다. ○ SIR 인시던트가 생성되고 종결되면 위반 업데이트를 활성화합니다. ○ 보안 인시던트 분석가(sn_si.analyst) 역할을 할당합니다. ○ sn_si.analyst 사용자는 보안 인시던트에 대한 작업을 수행합니다. 역할 및 사용자에게 역할을 할당하는 방법에 대한 자세한 내용은 ServiceNow 제품 설명서 웹 사이트의 역할을 참조하십시오.
다음 버전을 사용하고 있는지 확인합니다. • IBM QRadar 버전 7.3.2 이상. • IBM QRadar API 버전 10 이상. 이전 버전은 지원되지 않습니다.	콘솔에 액세스할 IBM QRadar 수 있는 경우 이 통합에 필요한 API에 액세스할 수 있습니다. API에 필요한 다른 특수 설정은 없습니다.
MID 서버 애플리케이션을 설치하고 구성했는지 확인하십시오.	구성된 MID 서버 애플리케이션. 서버가 회사 네트워크 내에 배포된 경우 IBM QRadar 서비스의 MID Server ServiceNow AI Platform# 가

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설정 작업	설명
	서비스에 연결 IBM QRadar 되어야 합니다. MID Server에 대한 내용은 ServiceNow 제품 설명서 웹 사이트를 참조하십시오. 클라우드 서비스를 사용하는 IBM QRadar 경우에는 MID 서버가 필요하지 않습니다.
ServiceNow 통합을 위해 애플리케이션을 설치하기 전에 통합을 지원하는 데 필요한 핵심 애플리케이션이 설치되고 활성화되었는지 확인합니다.	에서 ServiceNow Store다음 보안 운영 애플리케이션이 설치되고 활성화되는지 확인합니다. 설치되지 않은 경우 원활한 설치를 위해 다음 순서로 한 번에 하나의 애플리케이션을 설치하고 활성화합니다. **1.** 보안 인시던트 응답 **2.** 보안 운영용 이벤트 및 경보 수집: 이 애플리케이션에는 다음이 필요합니다. ○ com.glide.hub.integration.runtime => ServiceNow 통합 허브 런타임 ○ com.glide.hub.action_step.rest => ServiceNow 통합 허브 작업 단계 - REST 주: 통합 허브 구성요소는 이벤트 및 경보 수집 플러그인과 함께 설치됩니다. 설치되지 않은 경우 고객 지원에 문의하여 도움을 받으십시오. 핵심 애플리케이션 설치에 보안 운영 대한 자세한 내용은 해당 애플리케이션 활성화 ServiceNow Store문서를 참조하십시오제품 또는 애플리케이션에 대한 보안 운영 권리 가져오기.

다음에 수행할 작업

통합을 위한 인스턴스를 성공적으로 설정 ServiceNow AI Platform# 했습니다. 다음 단계는 통합을 위해 애플리케이션을 ServiceNow Store 설치하는 IBM QRadar 것입니다.

공격 수집 통합을 위한 **IBM QRadar** 프로파일 생성

sn_si.admin 역할을 가진 사용자는 인스턴스에 공격 프로필을 ServiceNow AI Platform 만들고 보안 인시던트를 생성하는 위반을 결정합니다. 위반SIR에서 보안 인시던트가 생성되기 전 ServiceNow AI Platform 보안 인시던트 응답 ()에는 실제 보안 인시던트가 생성되는 방식을 미리 볼 수 있도록 위반의 필드 값이 보안 인시던트의 ServiceNow AI Platform 레이아웃에 표시됩니다.

시작하기 전에

필요한 역할: sn_si.admin

이 태스크 정보

사용 가능한 API IBM QRadar 를 사용하는 통합 관점에서 정의된 프로파일 유형에 따라 위반이 인스턴스 환경 ServiceNow AI Platform 으로 보안 운영 자동 수집됩니다. 통합 워크플로우는 무단 접근 시도, 멀웨어 등 다양한 유형의 위반을 수집합니다. 이러한 위반은 인스턴스 환경에서 구성하는 보안 운영 프로파일을 기반으로 수집됩니다. 모든 위반은 처음에 프로파일에 구성된 위반 유형에 대해 수집됩니다. 수집된 위반을 추가로 필터링하여 보안 인시던트를 생성하는 위반을 지정할 수 있습니다. 예를 들어 고위험으로 식별된 위반에 대해서만 보안 인시던트를 생성하는 필터를 선호할 수 있습니다. 프로파일이 활성화되고 수집된 위반에서 보안 인시던트를 생성하기 전에 위반의 개별 필드 값이 미리 보기를 위해 보안 인시던트 레이아웃의 해당 필드에 매핑됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

인스턴스에 있는 ServiceNow AI Platform 위반 프로필의 이름은 고유해야 합니다. 여러 소스에 대한 여러 구성을 생성할 수 있으며 단일 소스에 대한 여러 프로파일을 생성할 수도 있습니다.

위반 수집 **IBM QRadar** 을 위한 프로파일 생성

위반을 수집하도록 프로파일을 설정할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.admin

프로시저

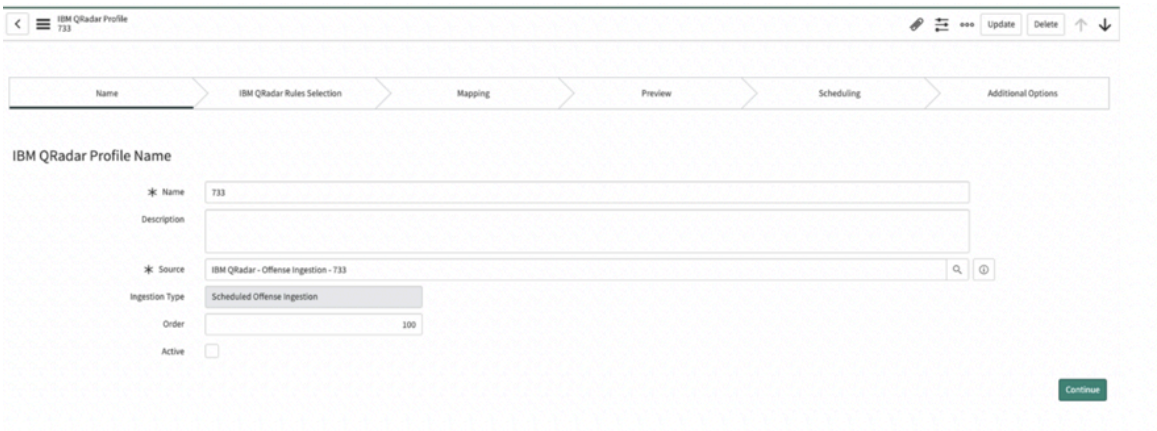
1. 인스턴스에서 범죄 ServiceNow AI Platform 에 대한 프로파일을 생성하려면 다음으로 이동하십시오. **IBM QRadar** 통합 〉 **IBM QRadar** 프로파일.
2. 새로 만들기를 클릭합니다.
3. 필드에 내용을 입력합니다.

   완료된 양식의 예가 테이블 다음에 나옵니다.

필드	설명
이름	프로파일의 고유한 이름입니다. 이름이 고유하지 않으면 오류가 표시되고 중복된 프로파일 이름은 저장되지 않습니다. 인스턴스의 프로파일 이름은 ServiceNow AI Platform 고유해야 합니다.
활성	확인란은 기본적으로 선택이 취소되어 있습니다. 이 옵션을 비활성화하면 프로필이 활성화되지 않고 수집이 수행되지 않습니다. 주: 프로파일을 활성화하기 전에 프로파일의 모든 섹션을 완료해야 합니다.
소스	IBM QRadar 위반을 수집하도록 구성한 서버입니다. 여러 IBM QRadar 서버가 구성된 경우 프로파일에 대해 수집할 공격 유형에 적합한 서버를 선택하십시오. 값을 입력해야 합니다.
순서	기본값은 100입니다. 여러 프로필을 만든 경우 둘 이상의 프로필이 동일한 트리거 조건을 공유할 때 이 값은 런타임 실행 우선 순위를 제공합니다. 숫자가 가장 낮은 프로파일의 워크플로우가 가장 높은 우선순위를 갖습니다.
(선택 사항) 묘사	이 프로파일을 다른 프로파일과 구별하는 데 도움이 되는 추가 텍스트입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음 그림은 완성된 폼의 예입니다.



다음에 수행할 작업
다음 단계는 수집할 범죄를 선택하는 것입니다.

규칙 선택 **IBM QRadar**

소스에 IBM QRadar 따라 프로파일에 대한 규칙을 하나 이상 IBM QRadar 선택합니다.

시작하기 전에
필요한 역할: sn_si.admin

이 태스크 정보
인스턴스에서 사용 가능한 IBM QRadar 규칙을 ServiceNow AI Platform 확인하여 보안 인시던트를 수집하고 생성하려는 활성 IBM QRadar 규칙을 알 수 있습니다.

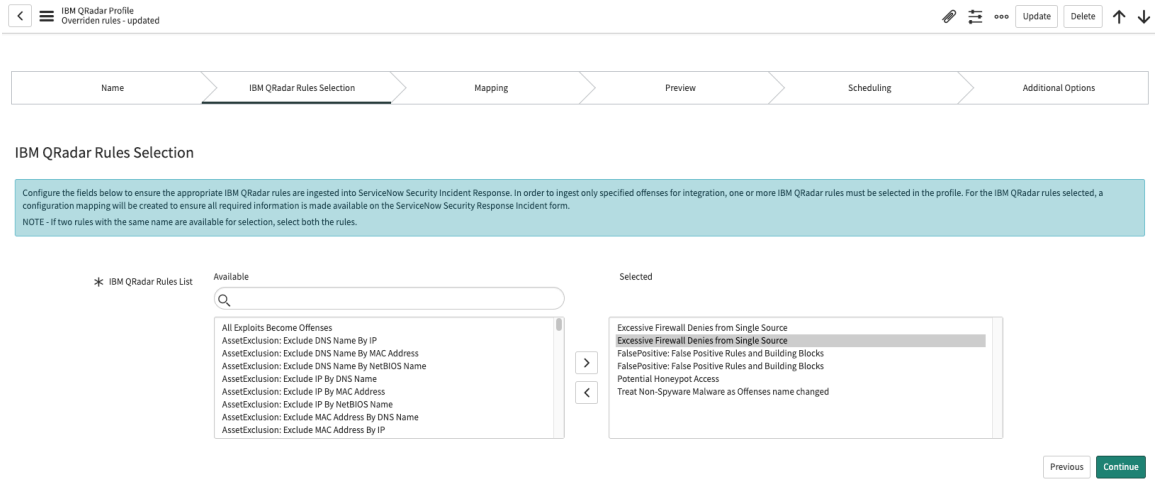
에서 IBM QRadar규칙을 System, Override, User 규칙의 기원으로 식별할 수 있습니다. 기본적으로 규칙의 출처는 시스템 규칙에 연결됩니다. 에서 IBM QRadar시스템 규칙을 수정하면 해당 원점이 재정의로 설정됩니다.

규칙 목록 필드에서 목록을 IBM QRadar 클릭합니다. 콘솔에 있는 IBM QRadar 활성 IBM QRadar 규칙 목록이 표시됩니다. 목록에서 하나 이상의 규칙을 선택하고 선택됨 열로 이동합니다. 선택한 규칙 중 하나 이상에 의해 트리거되는 IBM QRadar 위반이 이 프로파일에서 수집됩니다.

이름이 같은 규칙: ServiceNow AI Platform 인스턴스에 활성 또는 활성화된 규칙의 목록이 표시됩니다. 에서 IBM QRadar활성 또는 활성화된 시스템 규칙을 수정하면 새 무효화 규칙이 생성됩니다. 그러면 두 개의 규칙이 .ServiceNow AI Platform 이 시나리오가 발생하면 수집할 두 규칙을 모두 선택하고 보안 인시던트를 생성합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음 그림은 완료된 양식의 예제입니다.



계속을 클릭하여 마법사의 다음 단계로 진행합니다.

통합을 위한 **IBM QRadar** 위반 필드 매핑

규칙을 선택한 후 다음 단계는 위반, 이벤트 또는 플로우 필드를 보안 인시던트 양식의 필드에 매핑하는 것입니다.

개요

매핑 단계의 경우 먼저 하나 이상의 선택한 IBM QRadar 규칙에 대한 샘플 위반을 수집해야 합니다. 그런 다음 모든 관련 위반 필드 데이터가 인시던트 양식의 적절한 위치에 SIR 매핑되었는지 확인한 다음 미리 보기 섹션에서 인시던트를 시각화 SIR 해야 합니다.

샘플 위반 필드의 매핑에는 다음이 포함됩니다.

- 샘플 데이터 가져오기 및 채우기: 을 참조하십시오 샘플 IBM QRadar 위반 수집.
- 보안 인시던트에 위반 필드 매핑: 을 참조하십시오 보안 인시던트 응답 필드에 위반 필드 매핑 IBM QRadar.

샘플 **IBM QRadar** 위반 수집

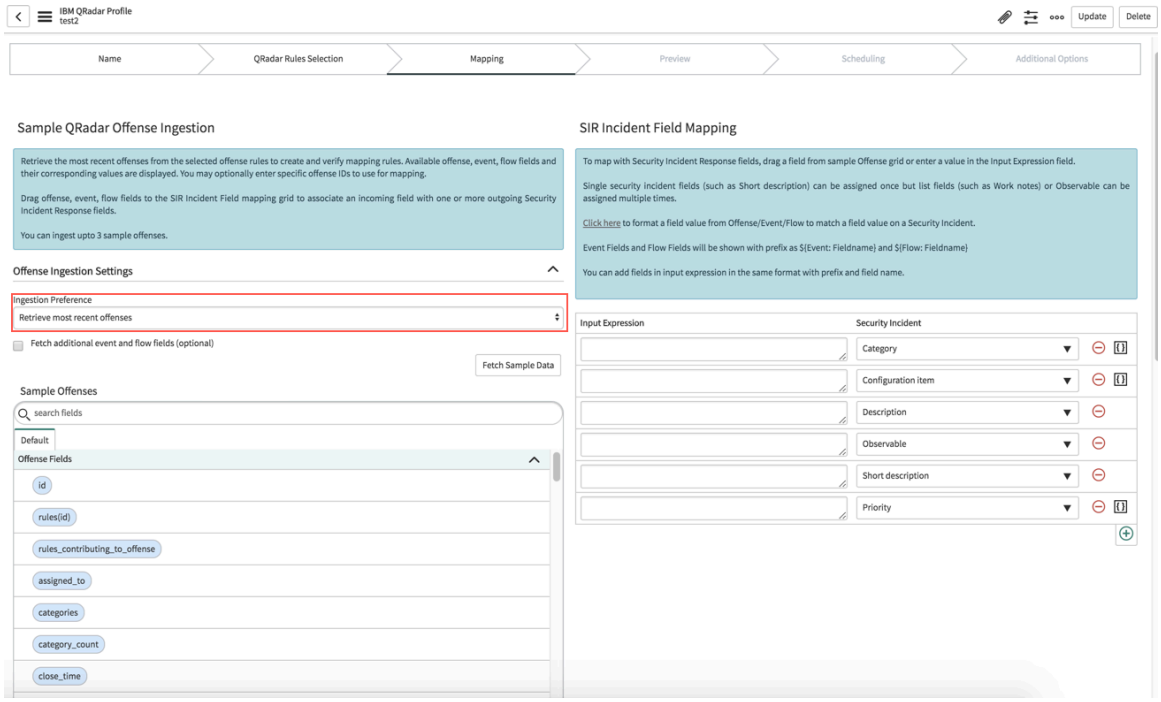
하나 이상의 선택한 IBM QRadar 규칙에 대해 샘플 위반을 수집할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.admin

프로시저

1. 매핑 양식이 표시되지 않으면 진행률 표시줄에서 매핑 을 클릭합니다.
2. 가장 최근의 샘플 위반 3개를 끌어오거나 매핑 경험에 사용할 특정 위반에 대한 고유한 위반 ID를 제공할 수 있습니다.
   수집 기본 설정 선택 목록에서 다음 중 하나를 선택합니다.
   - 가장 최근 위반 검색: 선택한 규칙의 가장 최근 위반 3개가 검색됩니다.
   - 위반 ID를 기준으로 위반 선택: 검색할 위반에 대한 위반 ID를 지정합니다. 쉼표로 구분된 최대 3개의 위반 ID를 지정할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



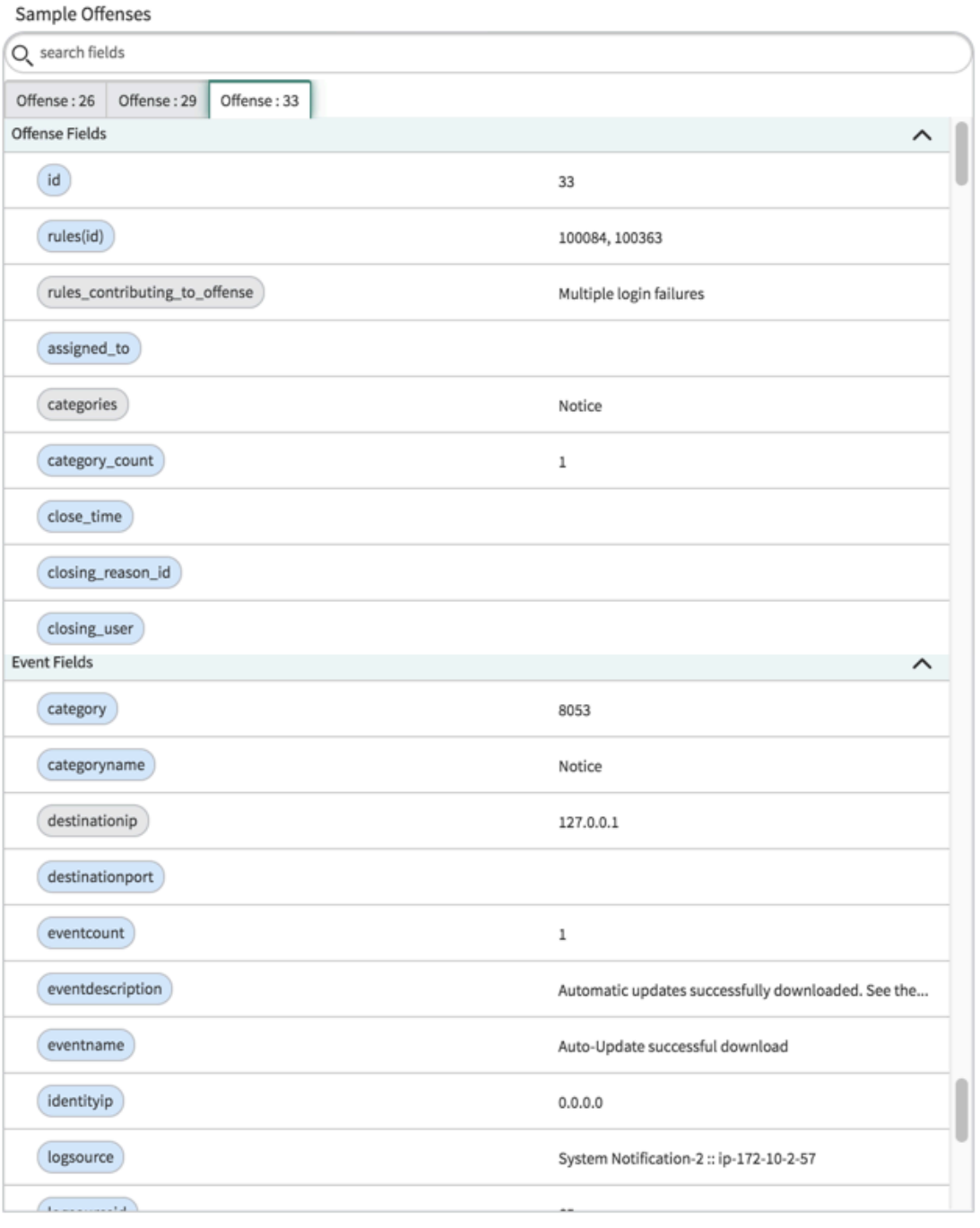
3. 샘플 데이터 가져오기를 클릭하여 선택한 위반 규칙에 대한 콘솔에서 최신 샘플 위반 데이터를 IBM QRadar 가져옵니다.

   위반 필드와 값 결과는 개별 탭으로 표시됩니다. 공격은 다음 세 가지 유형의 규칙에 의해 트리거될 수 있습니다.

   - 이벤트: 이 규칙에서는 이벤트 로그를 확인하고 지정된 기준이 충족되면 위반이 생성됩니다.
   - 흐름: 네트워크 데이터 및 트래픽을 확인하고 특정 조건이 충족되면 공격이 생성됩니다.
   - 공통: 이 경우 이벤트 또는 플로우에 대한 조건을 지정할 수 있으며 조건 중 하나 또는 둘 다 충족되면 위반이 생성됩니다.

   샘플 공격에 대한 풀링은 몇 분 정도 걸릴 수 있습니다. 트랜잭션이 작동 중임을 나타내는 메시지가 화면 맨 위에 표시됩니다. 아래 그림에 표시된 대로 위반 필드와 함께 위반을 트리거한 규칙에 따라 이벤트 또는 플로우 필드가 채워집니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



주:
표시된 이벤트 또는 플로우 필드는 해당 이벤트 또는 플로우 규칙에 따라 공격을 트리거한 첫 번째 이벤트 또는 플로우 필드에 속합니다.

4. 다음은 이 통합에 대해 작성된 사용자 지정 공격 필드입니다.
이러한 사용자 지정 필드 외에 표준 위반 필드를 매핑에 사용할 수 있습니다.
   - rules_contributing_to_offense: IBM QRadar 규칙 ID에 따라 공격에 기여한 규칙입니다.
   - users: 위반의 사용자 이름
   - remote_destination_ip: 공격의 원격 대상 IP입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

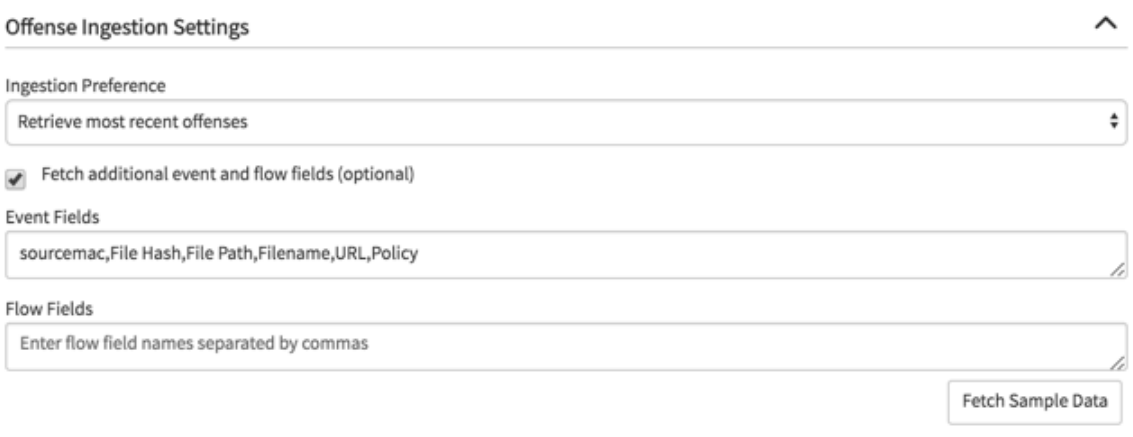
위반에 대한 로컬 대상 ID를 기반으로 다음 사용자 지정 로컬 대상 주소 필드를 사용할 수 있습니다.

- local_destination_address(domain_id)
- local_destination_address(event_flow_count)
- local_destination_address(first_event_flow_seen)
- local_destination_address(id)
- local_destination_address(last_event_flow_seen)
- local_destination_address(local_destination_address_ids)
- local_destination_address(크기)
- local_destination_address(네트워크)
- local_destination_address(offense_ids)
- local_destination_address(local_destination_ip)

○ 공격의 소스 ID를 기반으로 다음 소스 주소를 사용할 수 있습니다.

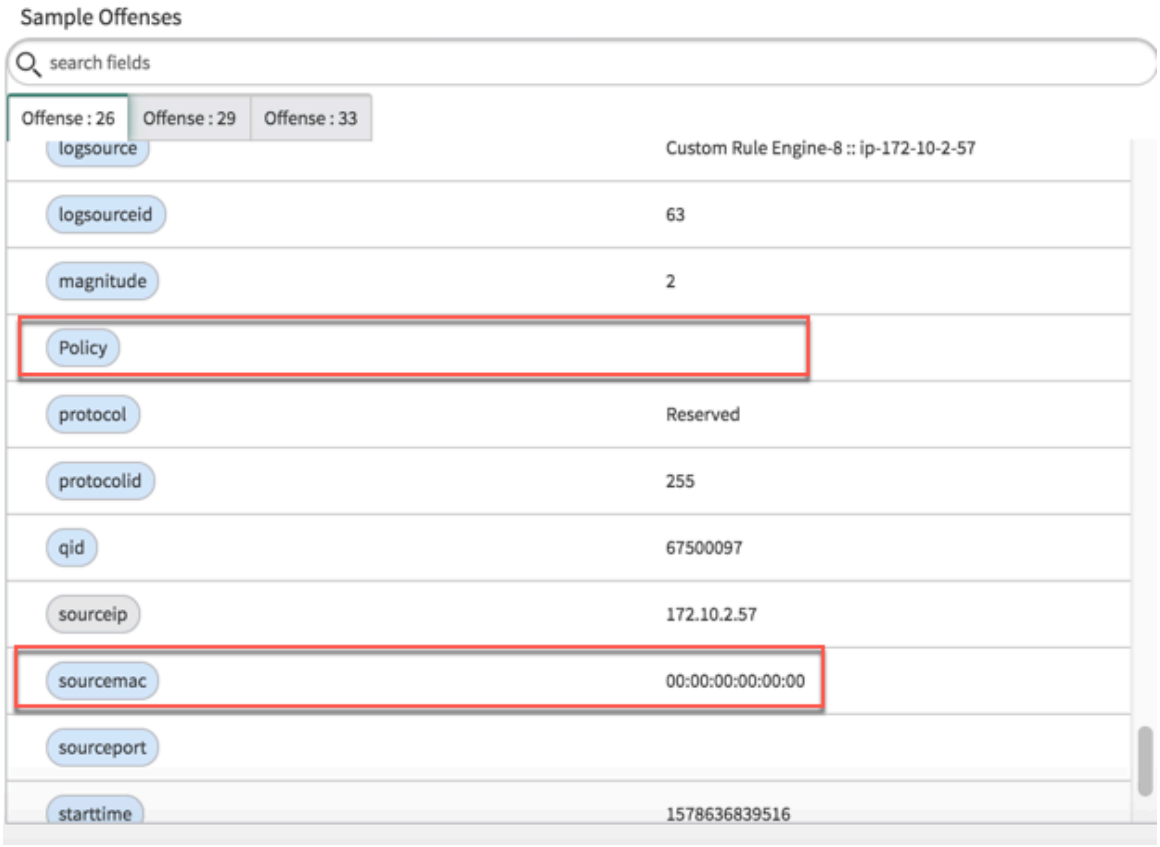
- source_addresses(domain_id)
- source_addresses(event_flow_count)
- source_addresses(first_event_flow_seen)
- source_addresses(id)
- source_addresses(last_event_flow_seen)
- source_addresses(source_address_ids)
- source_addresses(크기)
- source_addresses(네트워크)
- source_addresses(offense_ids)
- source_addresses(source_ip)

추가 이벤트 및 플로우 필드 가져오기(선택 사항) 확인란을 선택합니다. 활성의 유효한 사용자 지정 이벤트 및 플로우 필드에서 샘플 이벤트 및 플로우 데이터를 가져올 수 있습니다. 아래와 같이 쉼표로 구분된 사용자 지정 필드를 지정합니다.

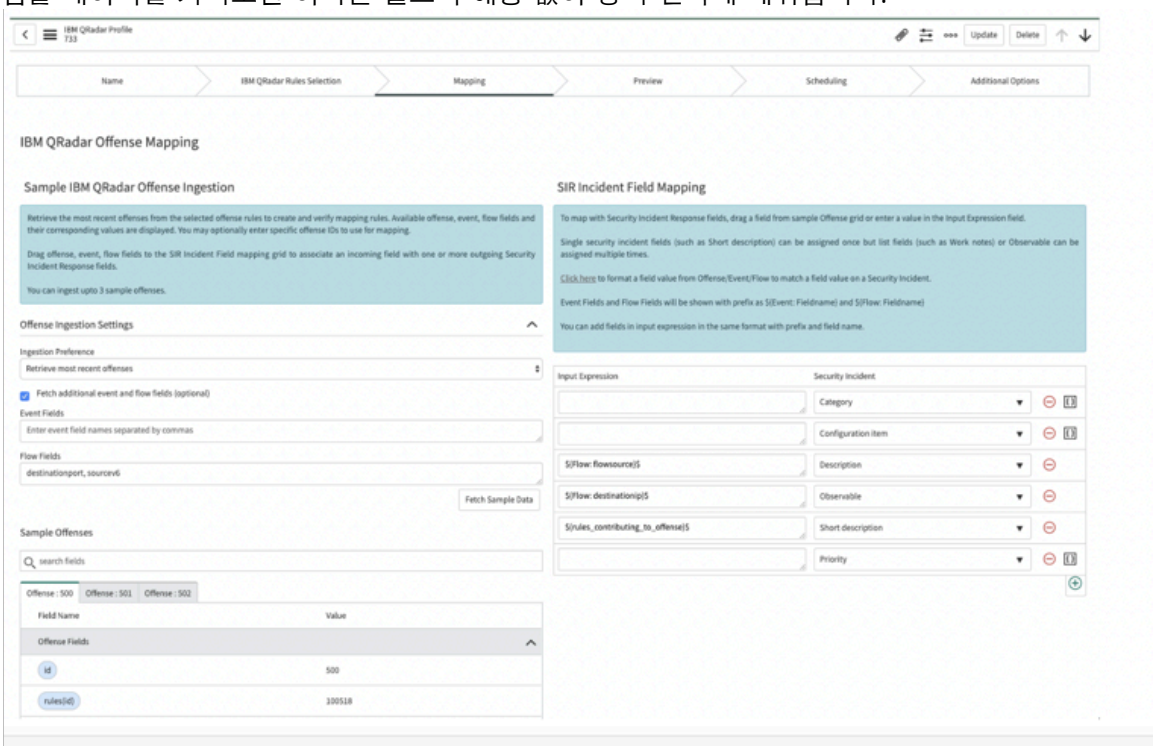


샘플 데이터 가져오기를 클릭합니다. 아래와 같이 지정된 이벤트 또는 플로우 필드가 해당 값(사용 가능한 경우)과 함께 이벤트 또는 플로우 섹션에 추가됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



샘플 데이터를 가져오면 이러한 필드의 해당 값이 양식 왼쪽에 채워집니다.



다음에 수행할 작업

샘플 데이터를 가져온 후 다음 단계는 위반 필드를 보안 인시던트에 매핑하는 것입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 인시던트 응답 필드에 위반 필드 매핑 **IBM QRadar**

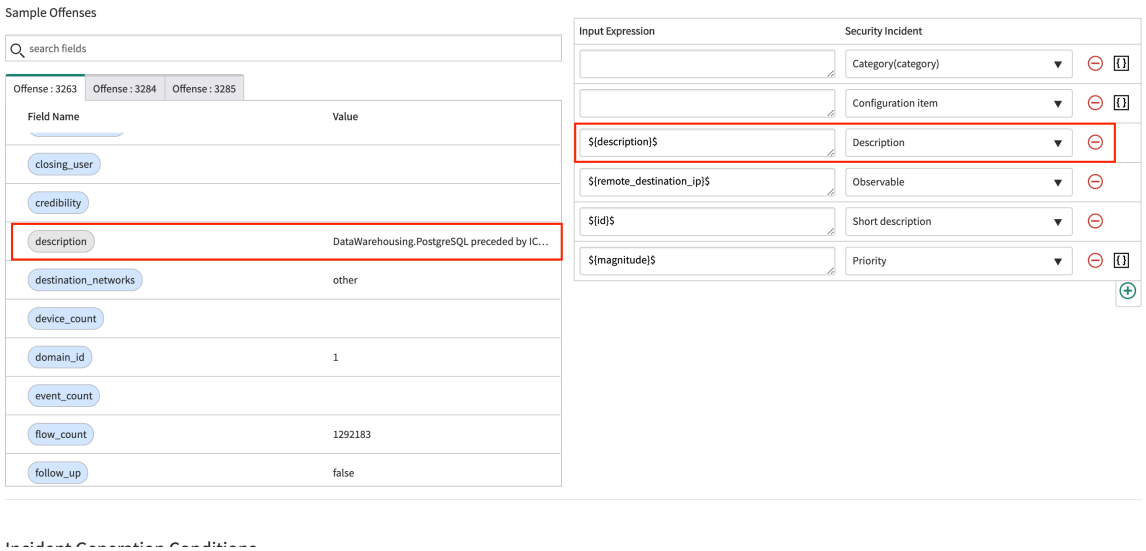
개별 공격, 이벤트 및 플로우 필드를 보안 인시던트의 필드에 매핑합니다 ServiceNow AI Platform SIR .

공격 필드 매핑

sn_si.admin 역할이 있는 사용자는 왼쪽에 있는 샘플 위반 섹션의 필드를 사용하여 SIR 인시던트 필드 매핑 열의 보안 인시던트 필드에 매핑합니다. 왼쪽에서 위반, 이벤트 또는 플로우 필드를 오른쪽의 인시던트 매핑 섹션에 끌어다 놓 ServiceNow SIR 아 매핑 구성을 편집합니다. 오른쪽의 매핑은 수신 공격 필드를 발신 보안 인시던트 필드와 연결합니다.

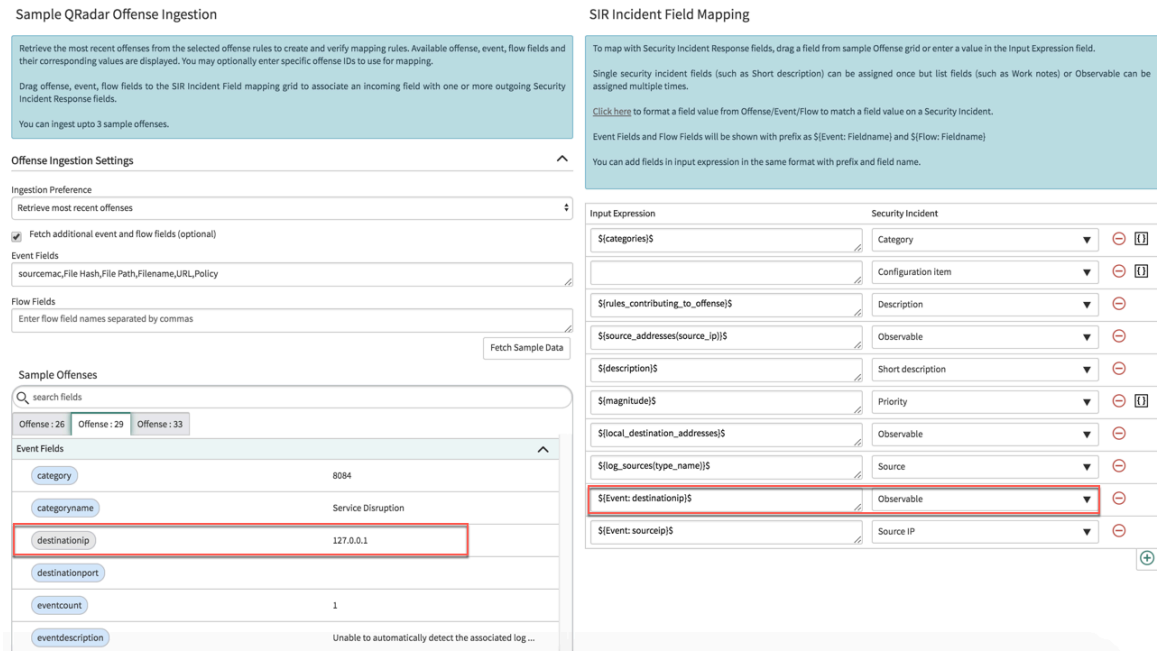
1. 샘플 데이터를 가져온 후 다음 단계는 위반, 이벤트 또는 플로우 필드를 보안 인시던트에 매핑하는 것입니다. 양식 왼쪽의 필드 값을 양식 오른쪽에 있는 보안 인시던트의 필드에 매핑하려면 양식 왼쪽에 있는 파란색 필드 이름을 길게 클릭합니다.
2. 필드 이름(예: ##)을 끌어서 보안 인시던트 열의 필드 이름 옆에 있는 입력 식 열의 필드에 놓습니다.

   필드 값이 입력 식 열에 표시됩니다. 다음 이미지에서 ### 보안 인시던트의 ## 필드에 매핑되어 있습니다.



주:
입력 식 섹션에 이벤트 또는 플로우 필드 이름을 수동으로 입력하는 경우, 매핑되는 필드 이름 앞에 프리픽스를 *${Event:eventfield}$* 또는 *${Flow:flowfield}$* 로 추가해야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



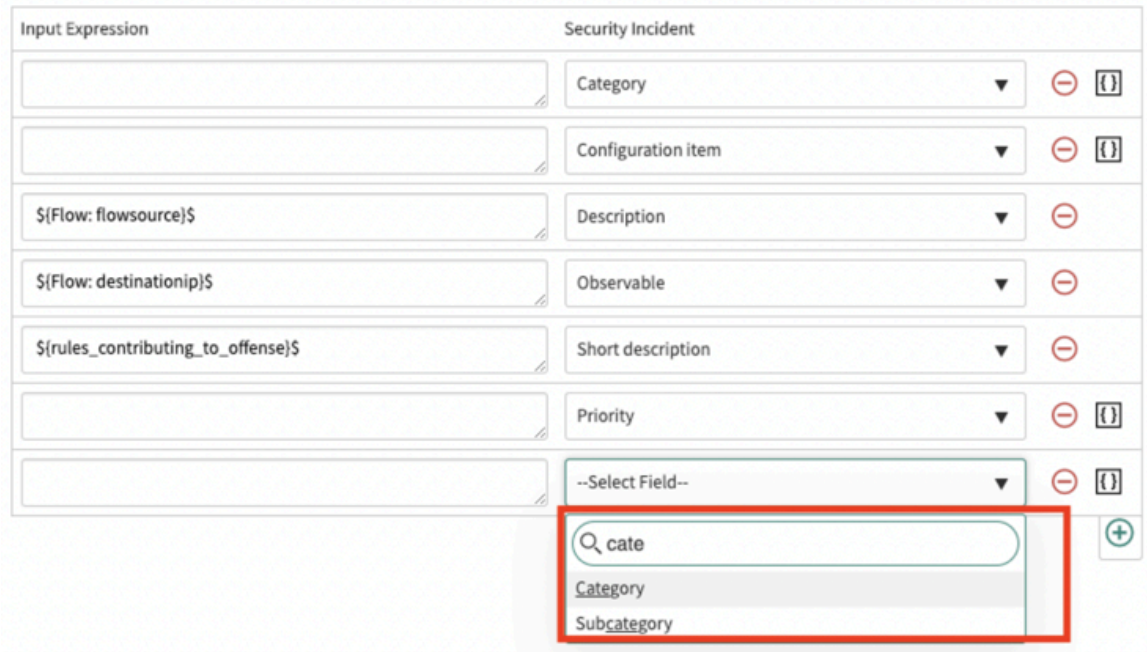
매핑 프로세스에서 위반, 이벤트 또는 플로우 필드가 간과되거나 중복되지 않도록 하기 위해 필드는 색상으로 구분됩니다. 위반 필드의 색상 코딩은 이미 매핑한 위반 값이 회색으로 표시되고 나머지 매핑되지 않은 필드는 모두 파란색으로 나타날 때 이를 추적하는 데 도움이 됩니다. 이렇게 하면 보안 인시던트에 추가된 필드 값과 나머지 중요한 범죄 정보가 매핑되지 않은 상태로 남아 있는지 시각화하는 데 도움이 됩니다.

왼쪽의 연한 파란색 필드는 공격 필드가 아직 선택되지 않았으며 보안 인시던트에 매핑되지 않았음을 나타냅니다. 수신 위반, 이벤트 또는 플로우 필드를 보안 인시던트의 둘 이상의 필드와 연결하는 것을 선호할 수 있습니다. 회색 필드는 필드가 선택되었고 보안 인시던트의 필드에 매핑되었음을 나타냅니다. 이 색상 코딩은 매핑을 추적하는 데 도움이 됩니다.

3. 양식 오른쪽의 보안 인시던트에 표시되는 기본 필드에 필드를 추가하려면 다음 단계를 따르십시오.
   a. 양식 오른쪽의 SIR 인시던트 필드 매핑 섹션 그리드 하단에서 더하기(+) 아이콘을 클릭합니다. 새 필드가 표시됩니다.
   b. 보안 인시던트 열에서 표시되는 선택 목록을 확장하고 필드를 선택합니다.

      새 필드의 확장된 선택 목록에서 일부 필드는 음영 처리됩니다. 다음 그림에서 범주는 보안 인시던트에 매핑되었기 때문에 회색 배경입니다. 양식 왼쪽에 있는 위반 필드의 색상 코딩과 유사하게 오른쪽에 있는 보안 인시던트 필드에 대한 이 색상 코딩은 이미 매핑된 SIR 인시던트 필드를 추적하는 데 도움이 됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



주:
동일한 보안 인시던트에 여러 옵저버블을 표시할 수 있으므로 옵저버블 필드를 서로 다른 값으로 여러 번 매핑할 수 있습니다. 마찬가지로 구성 항목 및 작업 메모 필드는 여러 값을 지원합니다. 여러 값을 지원할 수 없는 필드에 두 값을 매핑하려고 하면 인시던트를 미리 볼 때 필드에 값이 없다는 오류 메시지가 표시됩니다. 마찬가지로 보안 인시던트의 필드에 여러 옵션을 선택할 수 있는 선택 목록이 있고 선택 목록에 표시되지 않는 해당 필드에 옵션을 매핑하려고 하면 보안 인시던트에 필드가 채워지지 않습니다.

c. 또는 새 행의 검색 필드에 값을 입력합니다.

d. 양식 왼쪽에서 위반 필드를 선택하고 오른쪽에 있는 적절한 보안 인시던트 필드로 끌어서 놓습니다.

4. SIR 인시던트 필드 매핑 섹션의 필드 이름 옆에 있는 - 아이콘을 사용하여 필드를 제거합니다.

5. 매핑에 필드 값을 추가하거나 제거하여 매핑을 계속합니다.

여러 값이 있는 위반 필드

- 기본 제품에서 사용할 수 있는 범주 및 사용자 필드(예: 영향을 받는 사용자, 할당 대상)와 같은 보안 인시던트 필드는 여러 값을 지원하지 않습니다.
- 다음 IBM QRadar 필드는 여러 값을 지원합니다.
  - *####*
  - *destination_networks*
  - *source_address_ids*
  - *local_destination_address_ids*
  - *remote_destination_ips*
  - *rules_contributing_to_offense*
  - *###*

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

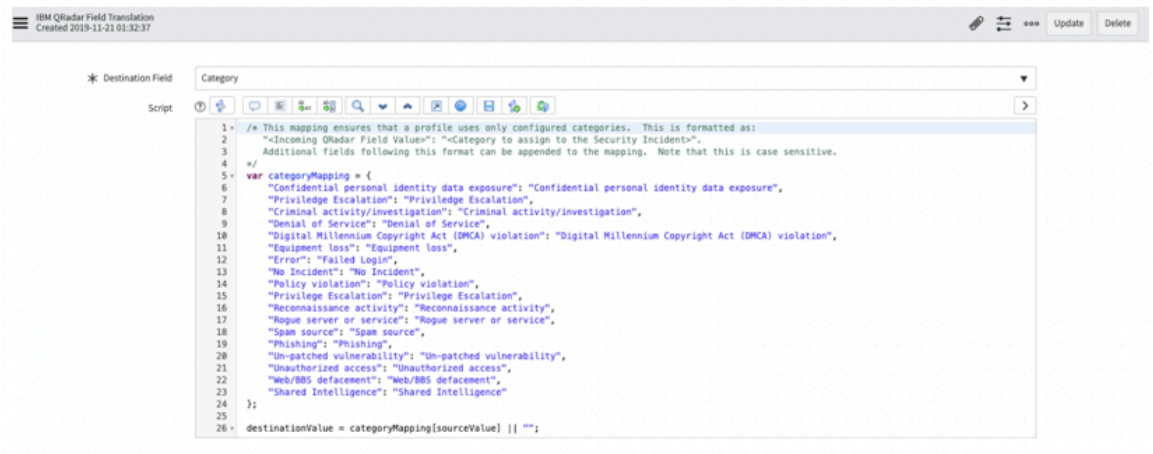
위의 필드를 CI 및 옵저버블 유형 필드를 제외한 모든 보안 인시던트 응답 필드에 매핑해야 하는 경우 목록 유형의 새 보안 인시던트 응답 필드를 생성하여 매핑에 사용해야 합니다.

주:
기본적으로 비참조 목록 유형 필드만 지원됩니다.

필드 형식 변환

경우에 따라 의 IBM QRadar 위반 필드 값이 SIR 보안 인시던트의 필드로 직접 변환되지 않을 수 있습니다. 이러한 값의 경우 스크립트 편집기를 사용하여 매핑 단계 중에 보안 인시던트의 필드 값에 대한 형식을 지정할 수 있습니다. 비슷하지만 동일하지는 않은 값의 형식을 지정하려면 스크립트 편집기를 사용하십시오. 예를 들어 스크립트 편집기를 사용하면 맬웨어 경보 및 바이러스 감염의 범주 값이 소스 범주에 대해 서로 다를 수 있지만 형식 필드 번역 기능을 사용하면 두 값 모두 SIR 보안 인시던트의 범주 필드에서 공통 악성 코드 활동으로 변환할 수 있습니다.

스크립트 편집기를 사용하려면 {} 클릭하십시오. 스크립트 편집기가 표시됩니다.



스크립트에 대한 변경 내용을 입력하고 업데이트를 클릭하여 변경 내용을 저장하고 매핑 페이지로 돌아갑니다.

인시던트 생성 조건

매핑 섹션이 완료되면 필터 조건을 설정하여 보안 인시던트를 생성할 범죄와 필터링할 범죄(예: 우선순위가 낮은 범죄)를 지정할 수 있습니다. 인시던트 생성 조건 작성기에서 동일한 필드 값을 사용하여 들어오는 위반이 보안 인시던트를 생성하기 위해 충족해야 하는 추가 기준을 정의할 수 있습니다. 인시던트 생성 조건을 설정하려면 다음 단계를 수행합니다.

1. 양식에서 인시던트 생성 조건 섹션으로 스크롤하고 조건을 기준으로 필터링 확인란을 선택하여 옵션을 활성화합니다.

   필터 조건 작성기가 표시됩니다. 이러한 필터를 사용하여 필드에 설명된 특정 조건과 일치하는 보안 인시던트를 생성합니다.

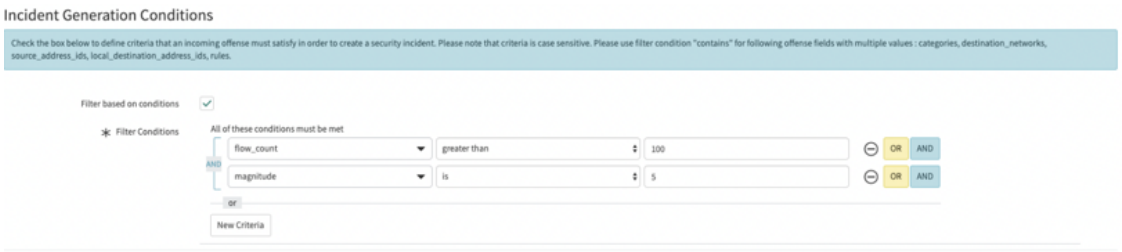
   필터 조건 빌더의 첫 번째 필드에 대한 선택 목록의 옵션은 수집한 위반에 대한 샘플 QRadar 위반 수집 섹션에 표시되는 필드와 일치합니다. 이러한 필드는 동적이며 수집하는 위반에 따라 변경됩니다. 입력하는 기준은 대소문자를 구분하며 위반 값과 IBM QRadar 정확히 일치해야 합니다. 필터 필드에 입력할 값을 잘 모르는 경우, 콘솔로 돌아가서 IBM QRadar 해당 키워드에 대한 위반 사항을 검토하는 것이 좋습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

> 주:
> *##*, *destination_networks*, *source_address_ids*, *local_destination_address_ids*, *remote_destination_ips*, *rules_contributing_to_offense* 및 *###* 공격 필드에는 여러 값이 있을 수 있습니다(값이 배열에 저장되므로). 필터 조건은 문자열만 검색할 수 있으므로 데이터가 올바르게 필터링되도록 이러한 필드에 *## Contains* 필터 조건을 사용해야 합니다.

2. 조건 작성기의 선택 목록과 필드를 사용하여 첫 번째 행에 대한 필터를 설정합니다.
3. 조건을 더 추가하려면 필드 오른쪽에서 AND 또는 **OR**을 클릭합니다.
   - **AND**를 선택하면 모든 조건이 일치해야 합니다.
   - **OR**을 선택하면 두 조건을 일치시킬 수 있습니다.
4. (선택 사항) 두 번째 행에서 두 번째 필터 조건을 설정합니다.

   다음 이미지는 보안 인시던트가 생성되기 전에 일치해야 하는 두 가지 조건이 있는 예입니다.



   입력한 두 필터링 조건이 모두 일치하는 경우에만 보안 인시던트가 생성되도록 인시던트 생성 조건을 설정했습니다.

   이러한 유형의 인시던트 생성 조건 필터링을 사용하면 의 기본 규칙이나 필터를 IBM QRadar수정하지 않고도 위반 범위를 좁히고 사용자가 생성하는 불필요한 보안 인시던트 수를 제한할 수 있습니다. 추가 필터링 기준이 설정되면 모든 기준과 일치하는 위반만 인시던트에 매핑됩니다.

> 주:
> 위반 필드 이름에 따옴표(″), 하이픈(′), 밑줄(-) 또는 앰퍼샌드(@)와 같은 특수 문자가 있는 경우, 필터링을 위해 이러한 문자를 대체해야 할 수 있지만 중복된 위반 이름이 있는 필드를 구별하기 위해 숫자 접미사가 추가됩니다. 예를 들어 첫 번째 위반 필드가 alerts.alert 이고 두 번째 위반 필드가 alerts@alerts인 경우 나머지 표준 텍스트 문자가 동일하므로 이러한 필드를 고유하게 식별할 수 없습니다. 이 경우 두 번째 위반 필드에 접미사가 추가되고 필터 조건 목록에 표시될 때 필드 이름이 alerts@alert(1) 로 변경됩니다.

유사한 범죄를 처리하고 중복 인시던트를 방지하기 위한 위반 집계 기준

중복될 가능성이 있는 유사한 인시던트를 생성하는 대신 들어오는 위반을 기존 SIR 보안 인시던트로 집계하는 추가 위반 집계 기준을 정의합니다. 각 프로파일에 대해 필드 일치 값 기준을 사용하는 이 추가 집계 기능은 모든 관련 위반 데이터를 단일 보안 인시던트에 배치함으로써 중복되는 활성 보안 인시던트의 수를 줄일 수 있습니다. 기준을 설정하려면 다음 단계를 수행합니다.

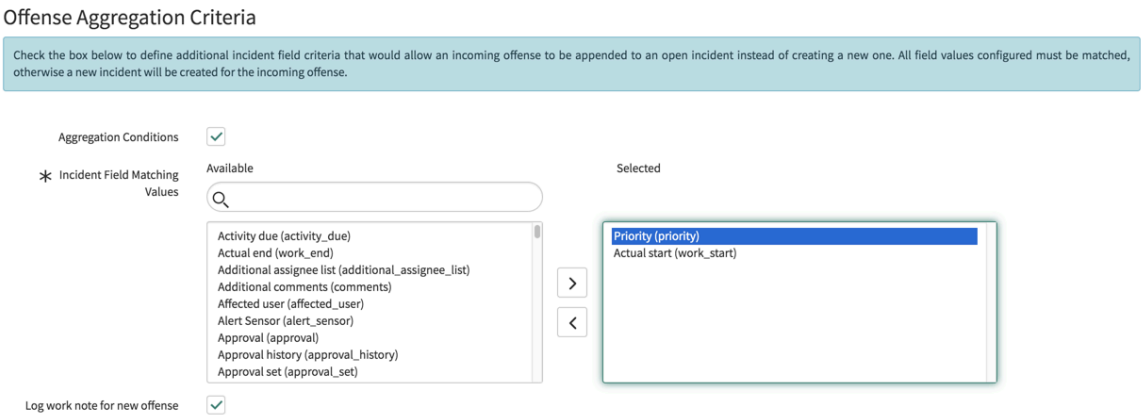
1. 양식의 위반 집계 기준 섹션으로 스크롤하고 집계 조건 선택란을 선택하여 이 옵션을 사용하십시오.

   인시던트 필드 일치 값 열이 표시됩니다. 이러한 필드 이름은 보안 인시던트에 구성된 SIR 사용자 지정 필드를 포함하는 보안 인시던트의 필드입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

2. 사용 가능 목록에서 기존 보안 인시던트 ServiceNow AI Platform 와 일치시킬 필드 값을 선택하고 선택됨 목록으로 이동합니다.

   이 수신 경보를 기존 보안 인시던트에 추가하려면 선택하는 모든 필드 값이 일치해야 합니다. 여기에는 옵저버블 및 구성 항목과 같이 여러 위반 필드 값이 매핑될 수 있는 필드가 포함됩니다. 모든 값이 일치해야 합니다. 값의 하위 세트만 일치하면 위반 집계 조건이 충족되지 않고 새 보안 인시던트가 생성됩니다. 다중 값 필드 매핑에 대한 아래 스크린샷을 참조하십시오.



   새 위반이 맵핑 단계의 집계 필드 조건에서 선택된 모든 값과 일치하는 경우, 새 위반은 동일한 필드 값을 사용하여 가장 최근에 열린 보안 인시던트에 자동으로 추가됩니다. 보안 인시던트를 담당하는 sn_si.analyst 역할을 가진 사용자는 보안 인시던트의 관련 목록에서 추가된 모든 집계 위반을 볼 수 있습니다. 이 목록에는 관련 타임 스탬프 및 집계된 필드 값이 자세히 설명되어 있습니다. 이 정보는 이러한 위반이 기존 보안 인시던트에 집계되는 이유를 이해하는 데 도움이 됩니다. 이 탭이 표시되지 않으면 관련 링크 아래에 있는 기록의 왼쪽으로 스크롤하여 모든 관련 목록 표시 링크를 클릭합니다.

3. (선택 사항) 보안 인시던트에 최근에 추가된 새 위반에 대한 작업 메모를 기록하려면 이 옵션을 사용하는 확인란을 선택합니다. 작업 메모는 위반 상세 정보 및 매핑 섹션의 작업 메모 필드에 추가되었을 수 있는 기타 상세 정보에 대한 링크와 함께 새 위반이 추가되었음을 기록합니다.

   위반의 IBM QRadar 값을 보안 인시던트의 필드로 매핑했습니다. 또한 인시던트 생성 필터링 기준을 사용하여 보안 인시던트 생성을 제한하는 추가 조건을 구성했습니다. 또한 위반 필드 값이 구성된 집계 기준과 일치할 때 기존 보안 인시던트에 위반을 추가했습니다.

4. 계속을 클릭하여 프로파일 구성을 계속합니다. 다음 단계는 보안 인시던트에서 SIR 매핑한 필드를 미리 보는 것입니다

보안 인시던트 미리 보기

매핑 단계를 완료한 후 보안 인시던트에서 SIR 매핑한 값을 미리 봅니다. 이 미리보기 단계를 사용하면 보안 인시던트에 표시할 모든 위반 필드를 매핑했는지 확인할 수 있습니다.

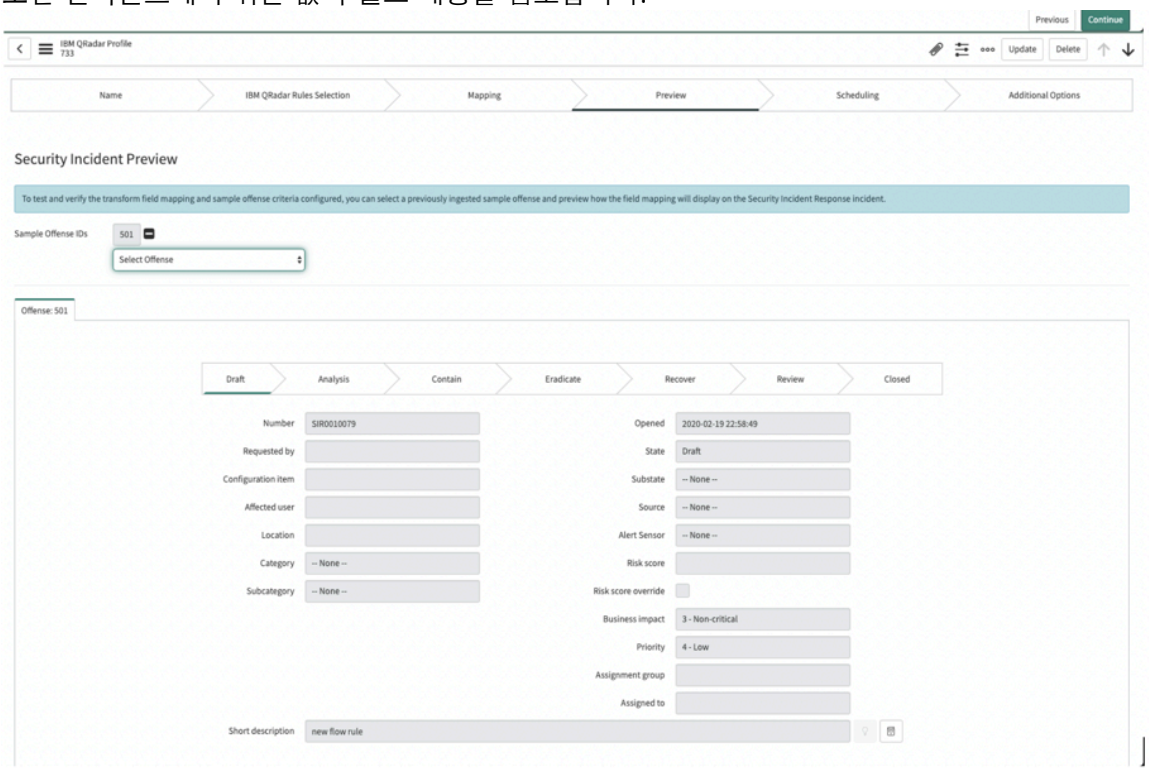
시작하기 전에
필요한 역할: sn_si.admin

이 태스크 정보
sn_si.admin 역할을 가진 사용자는 보안 인시던트를 미리 보고 필요에 따라 매핑을 다시 편집하여 오류가 있는 필드를 수정하거나 누락된 데이터를 채웁니다. 미리 보기가 성공적으로 완료되지 않으면 예약 단계로 진행할 수 없습니다. SIR 보안 인시던트 미리 보기는 제품에 실제 인시던트 보안 인시던트 응답 로 저장되지 않습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 보안 인시던트 미리 보기가 표시되지 않으면 진행률 표시줄에서 미리 보기를 클릭합니다.
2. 샘플 위반 ID 선택 목록에서 항목을 선택하십시오.
   보안 인시던트가 표시됩니다. 이 뷰는 읽기 전용 뷰이며 이 보안 인시던트의 기록은 저장되지 않습니다.
3. 보안 인시던트에서 위반 값의 필드 매핑을 검토합니다.



앞의 이미지는 수집된 샘플의 매핑 오류가 있는 미리 보기의 예입니다.

4. 이 오류를 해결하려면 진행률 표시줄에서 매핑 을 클릭합니다.
5. 매핑을 편집하여 잘못된 값을 수정하거나 누락된 데이터를 채웁니다.
6. 매핑을 다시 미리 보고 오류 메시지에 설명된 오류를 계속 수정합니다.

다음에 수행할 작업
오류 메시지가 표시되지 않고 보안 인시던트의 필드 매핑에 만족하는 경우 다음 단계는 일정을 정의하는 것입니다.

일정 정의

위반 수집 일정을 정의할 수 있습니다. 이 단계에서 위반 검색에 대한 기본 설정을 확인하거나 필요에 따라 스케줄링을 수정할 수 있습니다. 또한 이 단계에서는 날짜 범위를 사용하여 과거 위반을 검색할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.admin

이 태스크 정보
스케줄링 단계에서 과거 위반을 수집할지 여부를 선택할 수 있습니다. 프로파일 구성과 일치하는 향후 새로운 위반 및 업데이트된 위반에 대해 폴링할 빈도를 선택합니다.

sn_si.admin 역할을 가진 사용자는 프로파일별로 이러한 폴링 간격을 구성합니다. 공격 수집 통합의 IBM QRadar 성능은 다른 폴링 간격의 영향을 받을 수 있습니다. 스케줄링할 때 서버의

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

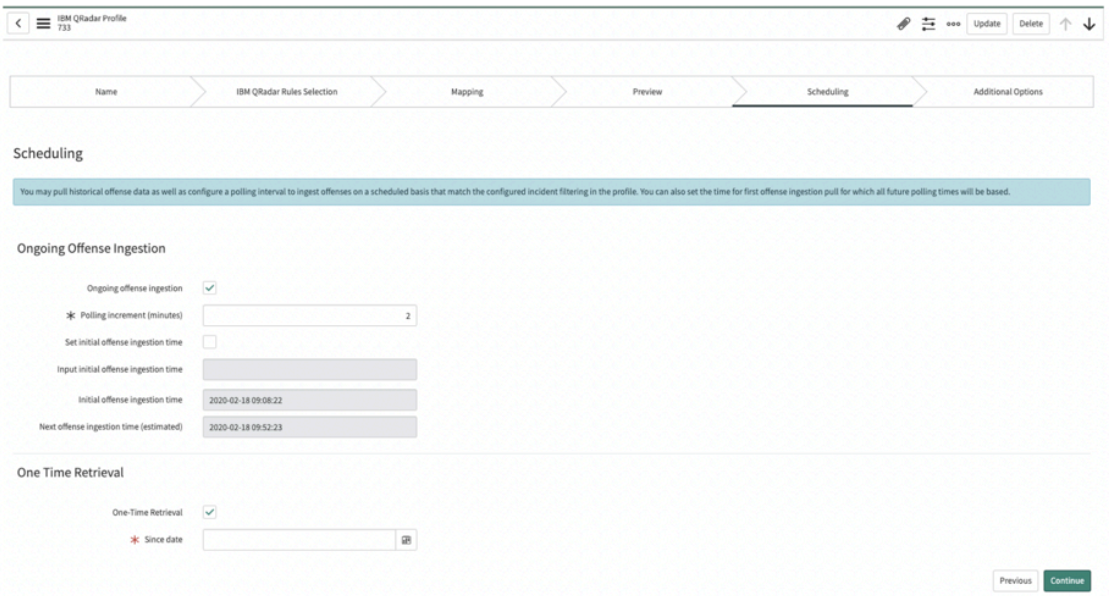
폴링 오버헤드를 IBM QRadar 줄이는 것과 위반이 작성되거나 업데이트될 때 가능한 한 빨리 알림을 받으려는 욕구 사이에서 균형을 맞추는 것을 선호할 수 있습니다. 모든 프로파일에 대해 5분 기본값이 설정되어 있지만 필요한 경우 이 설정을 1분 정도로 수정하는 것을 선호할 수 있습니다.

신규 및 업데이트된 위반 끌어오기

폴링 일정이 설정되면 예약된 작업은 이전에 끌어왔지만 인시던트 필터링 기준을 충족하지 않은 신규 및 업데이트된 위반을 모두 가져옵니다. 따라서 위반이 처음 생성될 때는 존재하지 않을 수 있지만 업데이트가 발생한 후(예: 조사 단계) 사용할 수 있는 기준에 따라 인시던트를 유연하게 생성할 수 있습니다. 특정 위반에 대한 인시던트가 생성되면 해당 위반이 활성 ServiceNow 보안 인시던트로 처리될 것으로 예상되므로 후속 업데이트는 무시됩니다. 그러나 이전에 수집되었지만 인시던트 생성 기준을 충족하지 못한 다른 모든 위반은 활성 인시던트의 일부가 될 때까지 계속해서 인시던트 생성 기준에 대해 끌어오고 확인됩니다.

프로시저

1. 진행률 표시줄에 스케줄링 페이지가 표시되지 않으면 스케줄링을 선택합니다.
2. 콘솔에서 위반을 끌어오는 IBM QRadar 방법과 시기를 예약하려면 하나를 선택합니다.



3. 계속을 클릭하여 추가 옵션 페이지로 이동합니다.

SIR 인시던트 상태에 따라 공격 업데이트 및 종결을 자동화

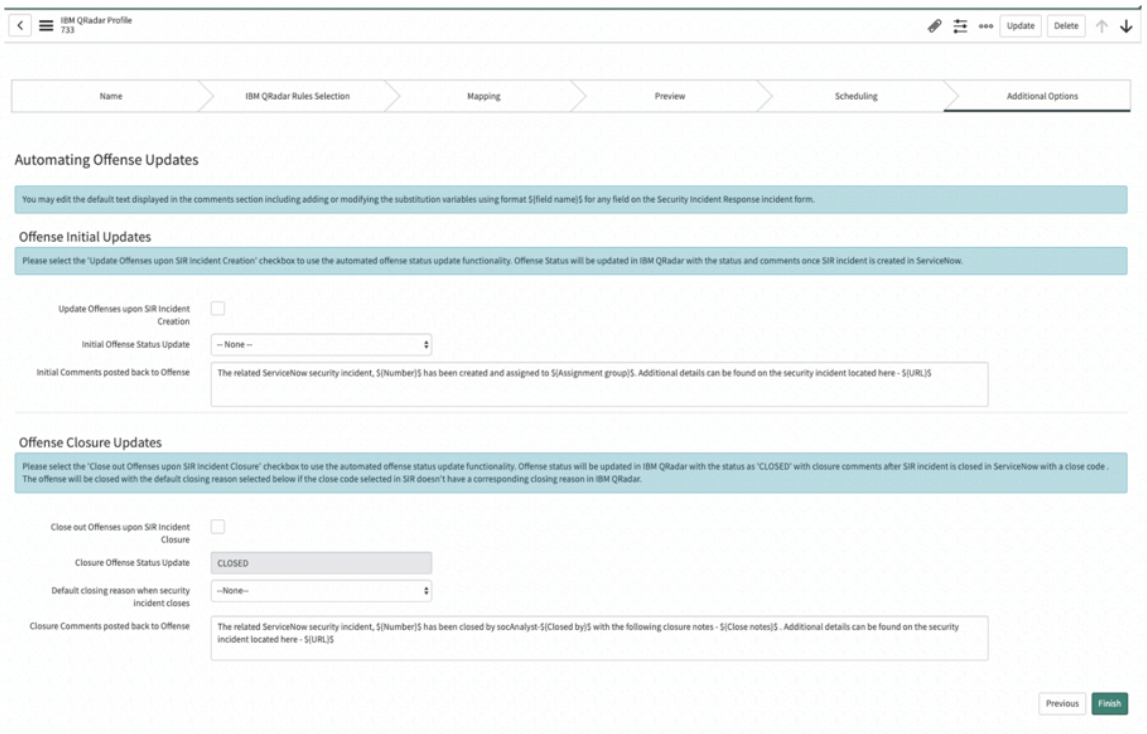
통합 IBM QRadar 에는 양방향 인터페이스가 있어 두 위반 모두 보안 인시던트를 생성할 수 있으며, 보안 인시던트가 생성 및/또는 종결되면 보안 인시던트 번호, 할당 그룹, 보안 인시던트 URL 등의 관련 인시던트 상세 정보로 위반을 업데이트할 수 있는 양방향 인터페이스가 있습니다.

시작하기 전에
필요한 역할: sn_si.admin

프로시저

1. 진행률 표시줄에 추가 옵션 페이지가 표시되지 않으면 추가 옵션을 선택합니다.
2. 아래 지침에 따라 보안 인시던트 생성 시 위반을 업데이트하기 위한 구성을 완료하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



3. Finish(마침)를 클릭하여 구성을 완료하고 프로파일을 **Waiting** 상태로 이동합니다. 확인 대화 상자가 표시됩니다. 통합에 대한 설정 및 구성을 성공적으로 완료했습니다. 이 프로파일을 활성화하여 일정에 따라 콘솔에서 범죄를 IBM QRadar 가져옵니다.

구성 설정

이 옵션을 사용하여 수집 통합 기본 시스템 속성을 수정합니다 IBM QRadar .

시스템 속성을 수정하려면 *sn_si.admin* 역할의 사용자로 로그인하고 **IBM QRadar** 통합 〉 **IBM QRadar** 통합 설정.

IBM QRadar 통합 설정

속성 이름	설명
24시간 동안 만들 수 있는 보안 인시던트 수를 제한하십시오. sn_sec_qradar.max_si_per_day	24시간 내에 만들 수 있는 최대 보안 인시던트 수를 지정합니다. • 유형: 정수 • 기본값: 1000
단일 인시던트로 집계할 수 있는 위반 수를 제한하십시오. sn_sec_qradar.max_aggregation_per_si	보안 인시던트에 대한 위반 집계 제한입니다. 예를 들어, 102개의 위반이 있는 경우 처음 100개의 위반은 보안 incident_1 에 집계되고 나머지 2개는 보안 incident_2에 집계됩니다. • 유형: 정수 • 기본값: 100
이 속성은 특정 위반에 대한 최근 이벤트/플로우를 가져오기 위해 AQL의 기간을 설정합니다.	특정 위반에 대한 최근 이벤트 또는 플로우를 가져올 일 수를 지정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

IBM QRadar 통합 설정

속성 이름	설명
sn_sec_qradar.on_demand_recent_days_limit	• 유형: 정수 • 기본값: 7
이 속성은 특정 범죄에 대해 가져온 최근 이벤트 수를 제한합니다. sn_sec_qradar.on_demand_event_limit	위반에 대해 검색되는 이벤트 수를 지정합니다. 이벤트 타임스탬프를 기준으로 가장 최근 이벤트가 먼저 검색됩니다. • 유형: 정수 • 기본값: 100
이 속성은 특정 위반에 대해 가져온 최근 플로우 수를 제한합니다. sn_sec_qradar.on_demand_flow_limit	위반에 대해 검색되는 플로우 수를 지정합니다. 플로우 타임스탬프를 기준으로 최근 플로우가 먼저 검색됩니다. • 유형: 정수 • 기본값: 100
이 특성은 특정 위반에 대한 최근 플로우/이벤트를 가져오는 AQL의 제한시간 값(초)을 설정합니다. sn_sec_qradar.on_demand_timeout	• 유형: 정수 • 기본값: 300
위반의 AQL을 폴링하기 위해 큐에 있는 레코드의 검색 ID 시간 제한(초)입니다. sn_sec_qradar.sid_ttl	보안 인시던트를 작성하기 전에 큐의 위반에 대한 AQL의 시간 초과입니다. 예를 들어, 90개의 위반이 있는 경우, 첫 번째 50개의 위반은 첫 번째 배치에서 AQL 데이터에 대해 처리되고 나머지 40개의 위반은 동일한 폴링 간격의 후속 배치에서 처리됩니다. • 유형: 정수 • 기본값: 300
예약된 통합에 의해 트리거되는 한 번에 실행할 IBM QRadar 수 있는 검색 수를 제어하는 임계치 job.sn_sec_qradar.records_threshold_in_que_for_aql	폴링 간격에서 단일 배치로 가져오는 위반 수를 지정합니다. • 유형: 정수 • 기본값: 50
통합 테이블 정리 일 수입니다. sn_sec_qradar.queue_item_expire	다음은 통합 테이블입니다. • sn_sec_qradar_events - IBM QRadar 이벤트 • sn_sec_qradar_flows - IBM QRadar 플로우 • sn_sec_qradar_offense_updates - IBM QRadar Offense 업데이트 • sn_sec_qradar_offense_to_task - 작업에 대한 IBM QRadar 위반

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

IBM QRadar 통합 설정

속성 이름	설명
	• 유형: 정수 • 기본값: 30
일회성 검색 또는 진행 중인 수집에서 프로파일당 실행된 예약된 작업당 위반 제한입니다. sn_sec_qradar.max_offense_limit_per_run	한 번의 검색에서 가져오는 ServiceNow AI Platform 위반 수를 지정합니다. • 유형: 정수 • 기본값: 1000
위반 업데이트 기능을 활성화하려면 이 속성을 설정하십시오. sn_sec_qradar.get_offense_updates	주: 이 설정을 활성화하면 보안 인시던트 생성이 지연될 수 있습니다. • 유형: true| 거짓 • 기본값: false

수정된 통합 설정은 프로파일에 정의된 다음 폴링 간격 동안 적용됩니다.

옵션: 프로파일 복사 **IBM QRadar**

새 프로파일을 생성하는 대신 기존 프로파일 및 관련 설정을 복사합니다. 여러 프로필을 만드는 경우 기존 프로필의 설정을 다시 사용하려면 프로필을 복사하여 시간을 절약할 수 있습니다.

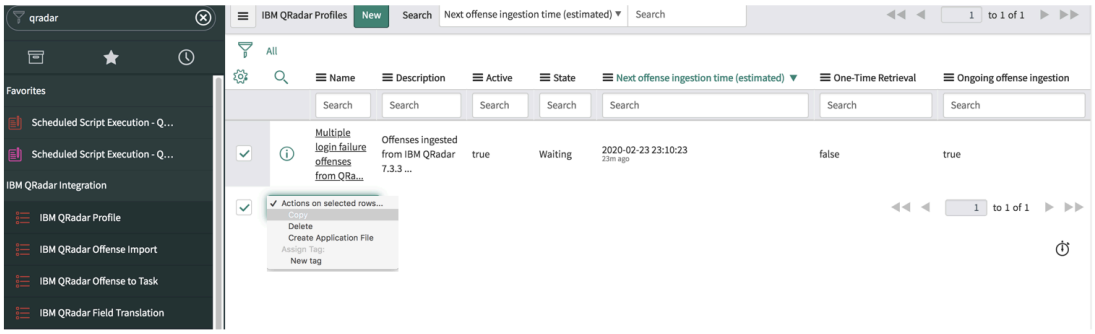
시작하기 전에
필요한 역할: sn_si.admin

이 태스크 정보
sn_si.admin 역할을 가진 사용자가 프로파일을 복사하는 경우 프로파일 중복을 방지하기 위해 프로파일 이름이 처음에 수정됩니다. 또한 복사된 프로파일이 비활성화(false)되므로 컨피그레이션을 완료하기 전에 실수로 활성화되지 않습니다. 이미 미리 보고 확인한 보안 인시던트에 대해 프로파일을 복사하고 기존 맵을 사용합니다.

프로시저

1. 다음으로 이동 모두 〉 **IBM QRadar** 통합 〉 **IBM QRadar** 프로파일.
2. 표시되는 IBM QRadar 프로파일 목록에서 복사할 프로파일을 선택하고 선택한 행 선택 목록에 대한 조치 목록에서 복사를 클릭하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



프로파일이 복사되어 목록에 표시됩니다. 복사본에는 매핑 및 일정 구성을 포함하여 원래 프로필의 모든 설정이 포함됩니다. 프로파일의 이름에는 사본이 포함되어 있습니다. 원본 프로파일이 활성화되었지만(true) 이 시점에서는 복사본이 비활성화됩니다(false). 복사된 프로파일의 값을 편집하고 필요에 따라 구성 설정이 새 프로파일에 적용되도록 이름을 바꿀 수 있습니다.

주:
프로파일에 대해 다른 소스를 선택하는 경우 프로파일에 대해 새 규칙(규칙 선택 IBM QRadar)을 선택해야 합니다. 그러나 동일한 소스를 사용하고 새 규칙을 선택하면 샘플 위반이 지워집니다.

기존 프로파일에서 새 프로파일로 설정을 복사했습니다. 프로파일을 활성화해야 하므로 활성 열 상태가 false로 설정됩니다.

다음에 수행할 작업
구성 단계를 완료한 후 새 프로파일을 활성화(활성화)하라는 메시지가 표시됩니다.

도메인 분리 및 **IBM QRadar** 위반 수집

도메인 분리 는 공격 수집에서 IBM QRadar 지원됩니다. 도메인 분리를 사용하여 데이터, 프로세스 및 관리 작업을 도메인이라는 논리적 그룹으로 분할할 수 있습니다. 어떤 사용자가 데이터를 보고 액세스할 수 있는지를 포함하여 이러한 분리의 여러 측면을 제어할 수 있습니다.

지원 수준: 기본

- 비즈니스 논리: 데이터가 애플리케이션의 서비스 제공자 사용 사례에 적합한 도메인으로 들어가도록 보장합니다.
- 애플리케이션은 런타임에서 도메인 분리를 지원합니다. 도메인 분리에는 사용자 인터페이스, 캐시키, 보고서, 롤업, 집계 등에서의 분리가 포함됩니다.
- 인스턴스 소유자는 여러 테넌트에서 작동하도록 애플리케이션을 설정해야 합니다.

샘플 사용 사례: 서비스 제공자(SP)가 채팅을 사용하여 테넌트 고객의 메시지에 응답할 때 고객이 SP의 응답을 볼 수 있어야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

지원 수준에 대한 자세한 내용은 도메인 분리를 위한 애플리케이션 지원 을 참조하십시오.

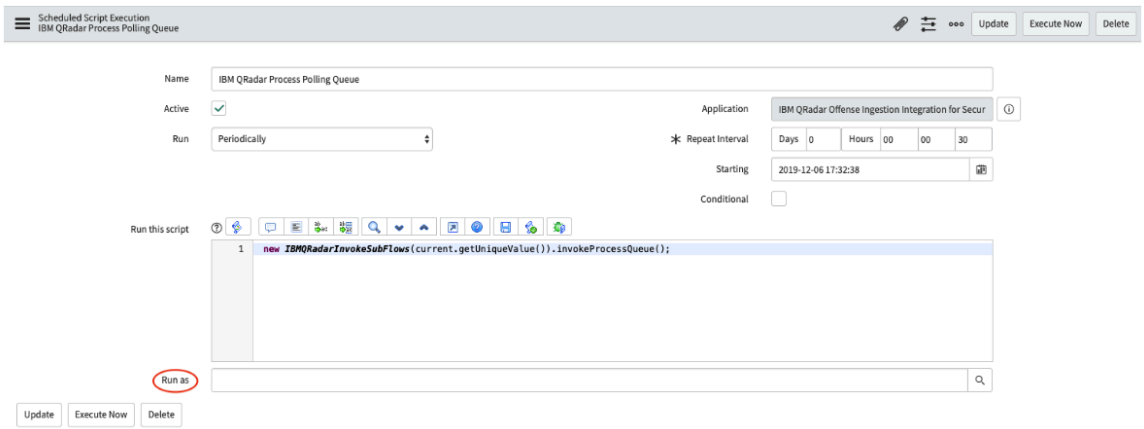
공격 수집에서 도메인 분리가 **IBM QRadar** 작동하는 방식

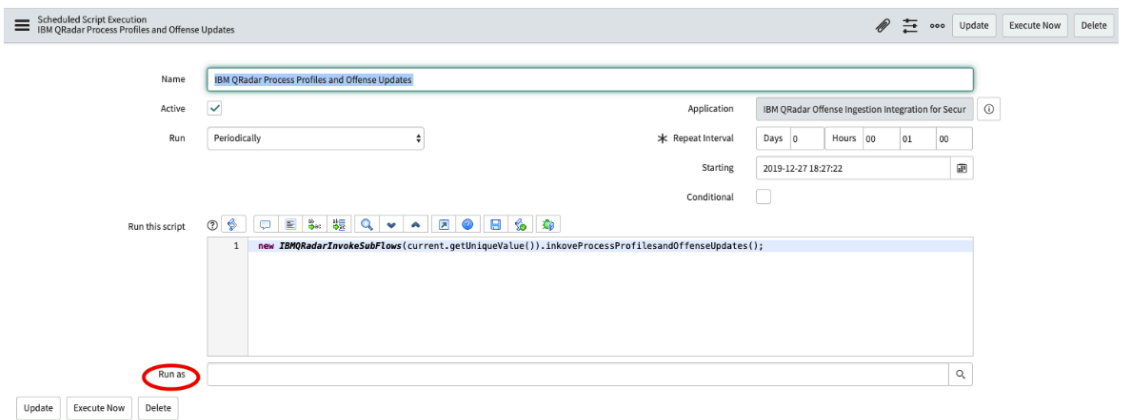
도메인 분리를 수행하려면 다음 단계를 따르십시오.

- 해당 도메인에서 *sn_si.admin* 역할을 가진 사용자를 생성합니다.

  주:
  프로필을 만들 때 도메인 선택기를 사용하여 특정 도메인을 선택합니다. 상위 도메인에서 사용자를 만든 후 나중에 프로필의 도메인을 변경하지 마십시오. 프로파일의 각 도메인마다 *sn_si.admin* 역할을 가진 특정 사용자가 있어야 합니다. 이 사용자를 사용하여 프로파일에서 설정을 만들거나 수정합니다.

- 기존 예약된 작업을 사용하지 않도록 설정합니다.
- 모든 도메인에 대해 프로세스 폴링 큐, IBM QRadar 프로세스 프로파일 및 공격 업데이트 스케줄된 작업을 복제 IBM QRadar 하십시오.
- 시스템 사용자에서 해당 도메인의 *sn_si.admin* 역할이 있는 사용자로 다른 사용자 이름으로 실행을 변경하고 예약된 작업을 실행합니다.





관련 정보

서비스 제공자용 도메인 분리

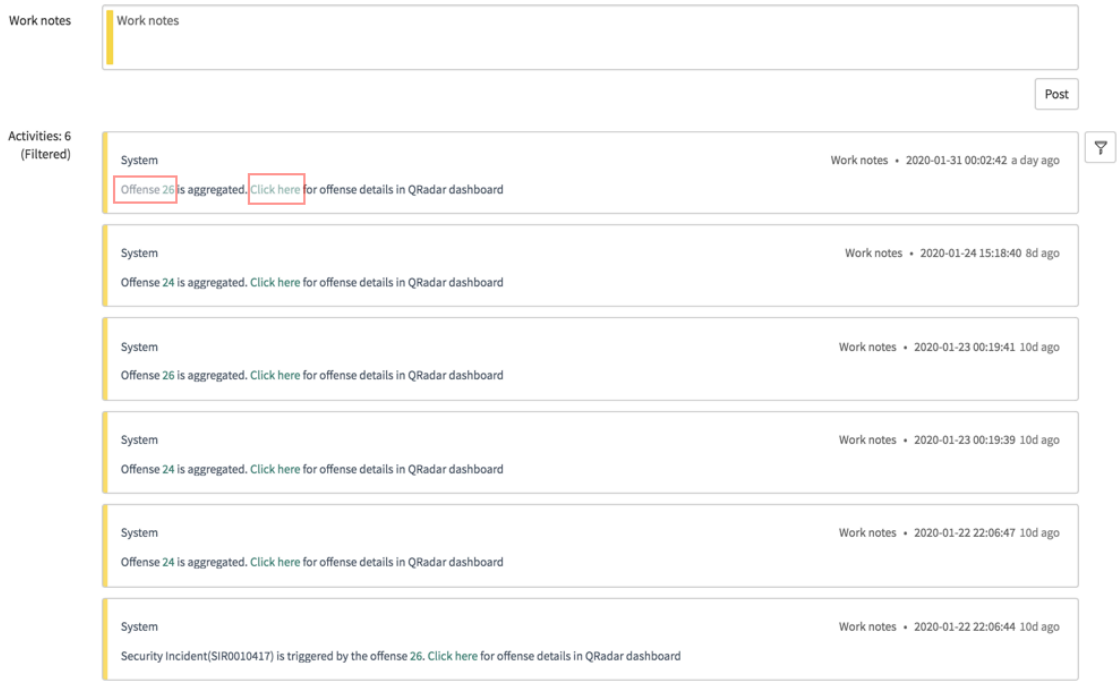
위반 수집 후 보안 인시던트 응답 양식

위반이 IBM QRadar 수집되면 보안 인시던트가 생성되고 해당 업데이트가 보안 인시던트 기록에 적용됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

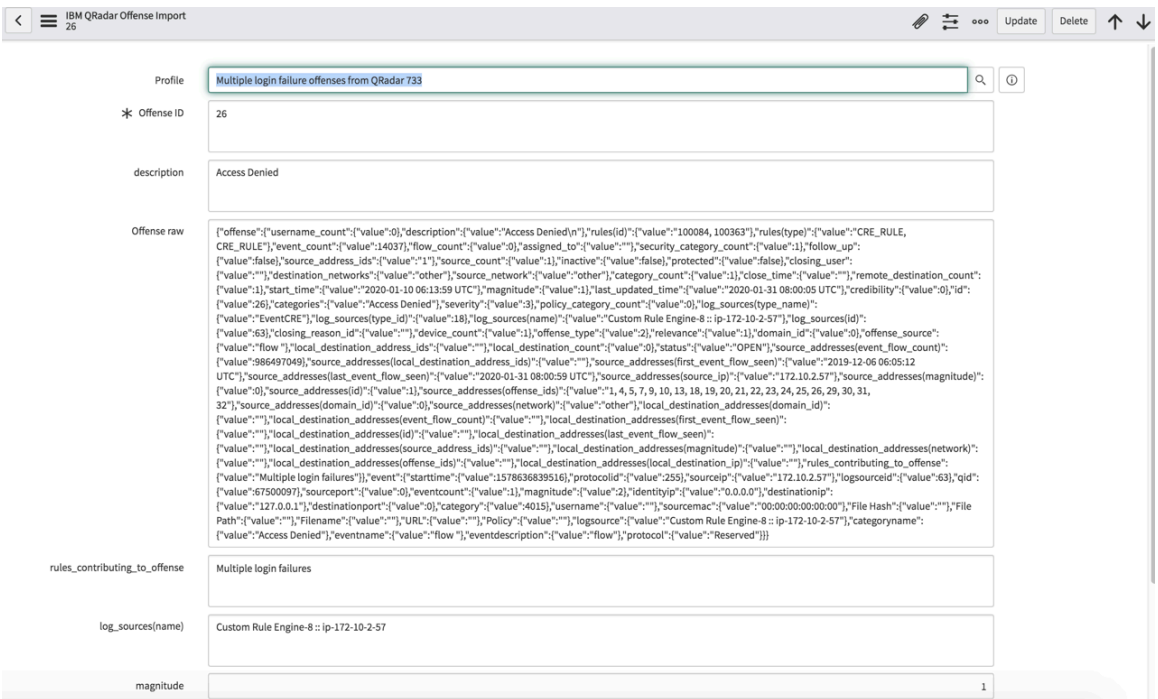
작업 메모

보안 인시던트를 트리거한 위반에 대한 상세 정보가 포함된 작업 메모가 게시됩니다.



내부 보안 인시던트 기록으로 이동하려면 위반 링크를 클릭하십시오. 여기를 클릭 하이퍼링크는 위반 세부 정보를 볼 수 있는 대시보드로 IBM QRadar 이동합니다.

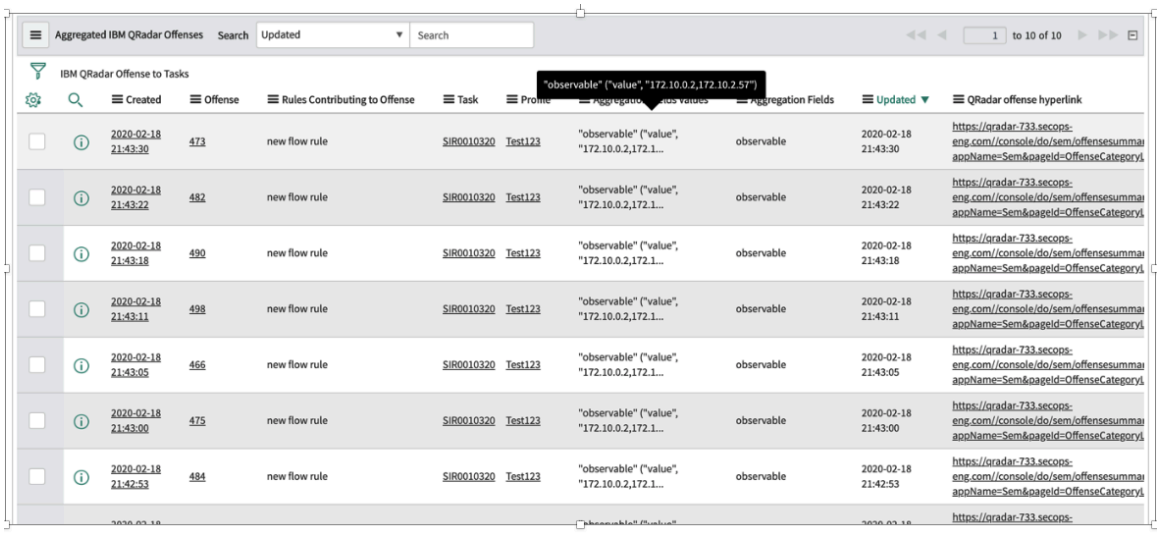
에 보안 인시던트 응답 필드에 위반 필드 매핑 IBM QRadar설명된 대로 위반 집계 기준에서 새 위반에 대한 작업 메모 기록 옵션을 선택한 경우 위반이 집계될 때 작업 메모가 게시됩니다.



집계된 위반

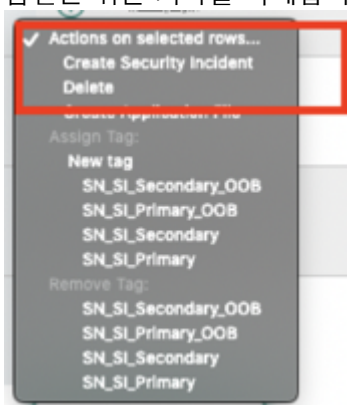
클릭 관련 목록 〉 집계된 **IBM QRadar** 위반 보안 인시던트에 집계된 위반을 보려면 QRadar 위반 하이퍼링크를 클릭하여 대시보드에서 IBM QRadar 위반을 보십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



보안 인시던트 생성: 목록에서 위반을 선택하고 작업 메뉴를 클릭한 다음 보안 인시던트 생성을 클릭합니다. 이 옵션은 위반에 대한 보안 인시던트를 생성하고 이 위반은 상위 보안 인시던트에서 세분화됩니다.

위반 레코드 삭제: 목록에서 위반을 선택하고 조치 메뉴를 클릭한 후 삭제를 클릭하십시오. 이 옵션은 위반 기록을 삭제합니다.

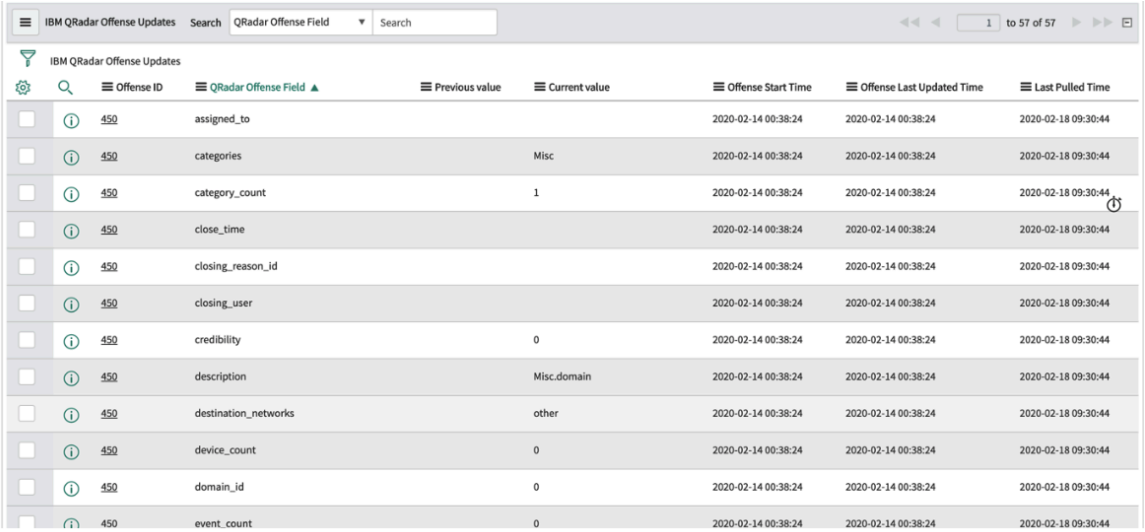


IBM QRadar 위반 업데이트

이것은 표준 및 사용자 지정 공격 필드를 표시하고 모든 폴링 간격 동안 공격에 대한 변경 사항을 추적합니다. 대시보드로 IBM QRadar 이동하지 않고 바로 위반 업데이트를 볼 수 있으므로 유용합니다. 값에 대한 모든 변경 사항은 이전 값 및 현재 값 필드에 표시됩니다.

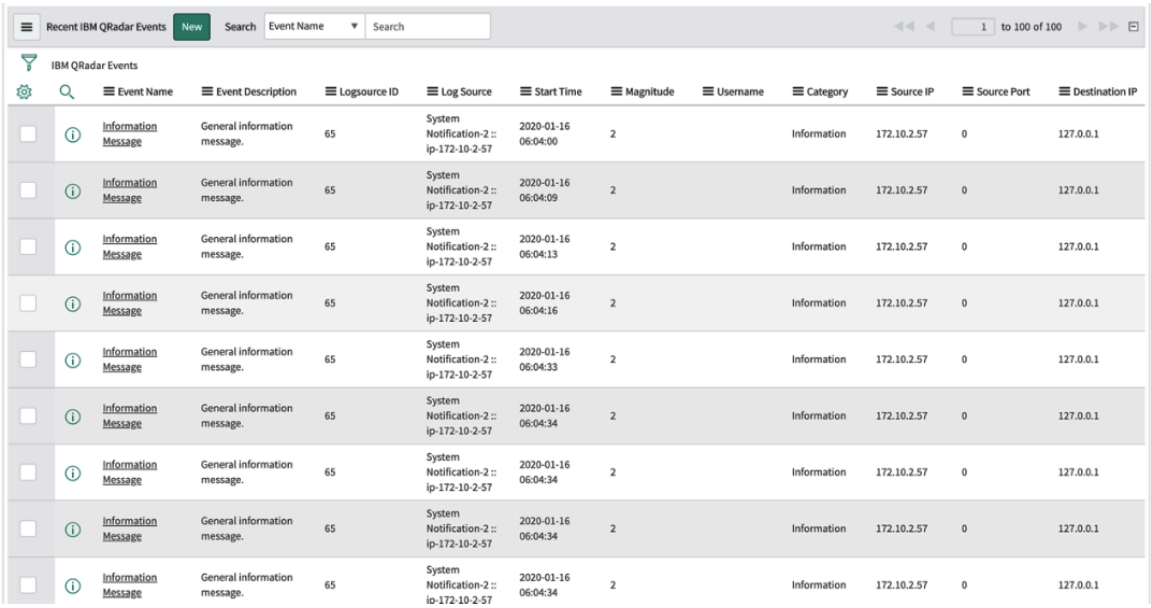
위반 업데이트 기능을 사용하려면 다음으로 이동하십시오. **IBM QRadar** 통합 〉 **IBM QRadar** 통합 설정 을 클릭하고 이 속성 설정을 사용하여 **Offense Updates** 기능을 활성화하십시오. 기본적으로 이 설정은 사용되지 않습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



최근 **IBM QRadar** 이벤트

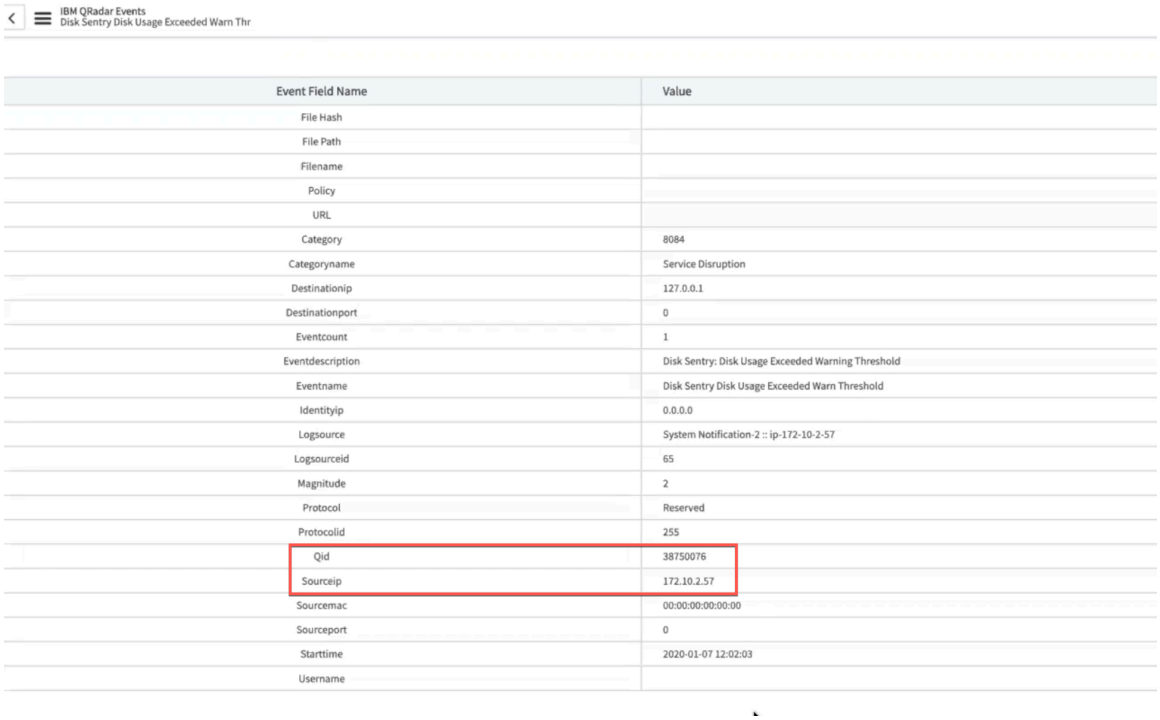
관련 링크 아래에서 최근 **IBM QRadar** 이벤트 가져오기 옵션을 클릭하여 최신 IBM QRadar 이벤트를 보십시오.



기본적으로 최대 100개의 이벤트가 표시됩니다. 에서 이 기본 설정을 수정할 수 있습니다 구성 설정.

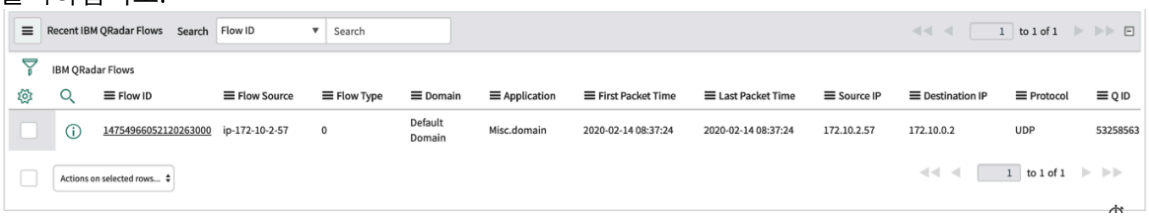
주:
위의 이미지는 위반과 관련된 표준 이벤트 필드를 보여줍니다. 사용자 지정 이벤트 필드를 구성하고 매핑한 경우(See 보안 인시던트 응답 필드에 위반 필드 매핑 IBM QRadar) 이벤트 이름 링크를 클릭하여 목록 뷰에서 볼 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



최근 **IBM QRadar** 플로우

Integration Hub 및 Flow Designer를 사용하면 통합과 함께 여러 플로우, 하위 플로우, 작업을 사용할 수 있습니다 IBM QRadar . 관련 링크 아래에서 최근 **IBM QRadar** 플로우 가져오기 옵션을 클릭하면 가장 최근 플로우가 검색됩니다. 이러한 플로우를 보려면 최근 **IBM QRadar** 플로우를 클릭하십시오.



기본적으로 최대 100개의 플로우가 표시됩니다. 에서 이 기본 설정을 수정할 수 있습니다 구성 설정.

주:
위의 이미지는 위반과 관련된 표준 플로우 필드를 보여줍니다. 사용자 지정 플로우 필드를 구성하고 매핑한 경우(참조 보안 인시던트 응답 필드에 위반 필드 매핑 IBM QRadar) 플로우 ID 링크를 클릭하여 목록 뷰에서 볼 수 있습니다.

IBM QRadar 공격 수집 통합에서 **Flow Designer** 및 **Integration Hub** 사용

플로우 디자이너 및 통합 허브 기능을 사용하여 여러 하위 플로우와 작업이 공격 수집 통합의 IBM QRadar 일부로 빌드되었습니다.

다음과 같은 IBM QRadar 하위 플로우를 사용할 수 있습니다.

- 연결 및 자격 증명 확인: 초기 설정에서 호스트 및 자격 증명을 확인하기 위한 구성 타일에 사용됩니다.
- IBM QRadar 규칙 검색: 프로파일 설정의 규칙 섹션에서 의 모든 활성 규칙을 IBM QRadar검색하는 데 사용됩니다. 이 하위 플로우는 비동기식으로 트리거됩니다.
- IBM QRadar에서 샘플 위반 데이터 가져오기: 이는 샘플 데이터를 가져오기 위해 프로파일 설정의 맵핑 섹션에서 사용됩니다. 이 하위 플로우는 비동기식으로 트리거됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- IBM QRadar Offense 상태 업데이트: 이는 1분마다 스케줄된 작업에 의해 트리거되며 보안 인시던트가 IBM QRadar 작성되거나 종결될 때 공격을 업데이트합니다.
- 예약된 작업 및 큐 위반에서 프로파일 처리: 폴링 간격에 따라 프로파일당 위반을 가져오기 위해 1분마다 예약된 작업에 의해 트리거됩니다. 이렇게 하면 위반을 가져와서 추가 처리를 위해 폴링 테이블로 큐에 넣습니다.
- 일괄 처리 폴링 큐 및 폴링: 폴링 테이블 큐를 처리하기 위해 30초마다 예약된 작업에 의해 트리거됩니다.
- 최근 IBM QRadar 플로우 가져오기: 보안 인시던트 양식 링크에서 트리거되어 최신 공격 플로우를 가져옵니다.
- 최근 IBM QRadar 이벤트 가져오기: 보안 인시던트 양식 링크에서 트리거되어 최신 공격 이벤트를 가져옵니다.

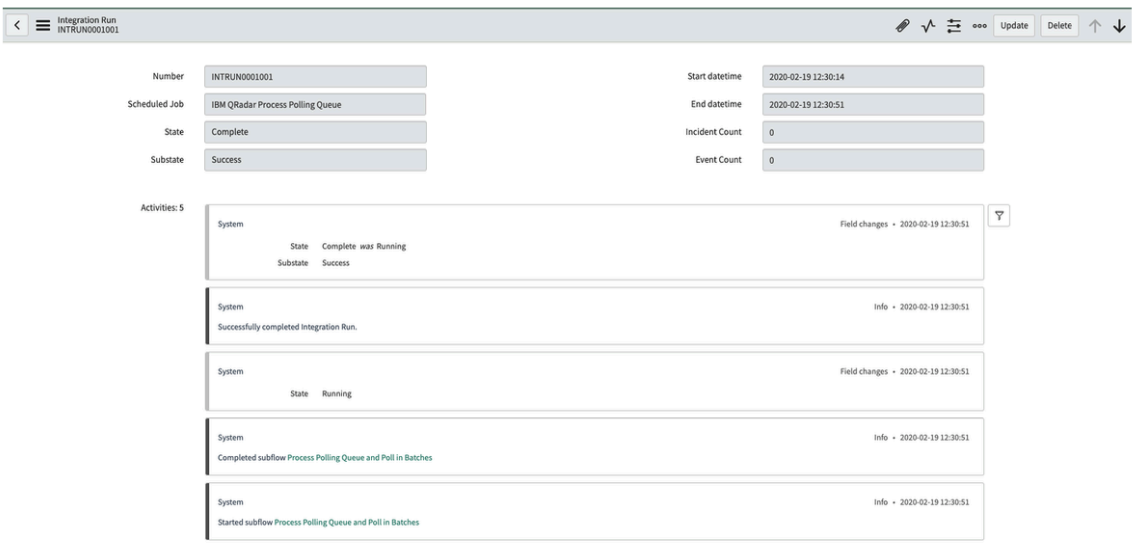
이러한 하위 플로우를 보려면 *sn_si.admin* 역할을 가진 사용자로 로그인하고 플로우 디자이너 〉 디자이너. 하위 플로우를 자세히 보려면 위에 나열된 하위 플로우 중 하나의 이름 링크를 클릭합니다.

공격 수집 통합 문제 해결 **IBM QRadar**

이 섹션에서는 공격 수집과 IBM QRadar 관련된 중요한 문제 해결 팁과 자주 묻는 질문에 대해 설명합니다.

- 통합 실행: 예약된 작업이 실행을 시작하면 로그, 오류 및 경고가 포함된 통합 실행 기록이 표시됩니다. 끌어온 위반 수와 예약된 작업 실행에서 생성된 인시던트 수도 표시됩니다. sn_si.analyst 역할을 가진 사용자는 통합 실행 중에 오류/프로파일 끌어오기에 실패한 경우 확인할 수 있습니다.

  통합 실행의 작업 메모는 실행된 하위 플로우에 대한 링크를 제공합니다. sn_si.analyst 역할을 가진 사용자는 발생한 오류에 대해 sn_event_ingestion_integration_run 테이블을 확인할 수 있습니다. 통합 문제를 해결하려면 먼저 통합 실행을 확인해야 합니다. 오류는 예약된 작업 실행 every every scheduled job에 대한 통합 실행 기록에 작업 메모로 기록됩니다.



- SSL 문제: 클라우드 인스턴스에 연결할 IBM QRadar 때 인스턴스에 만료되지 않은 유효한 CA 인증서가 있는지 확인합니다. RSA 또는 자체 인증서를 플랫폼으로 임포트하고 인증서의 일반 이름이 호스트 이름과 일치하는지 확인할 수 있습니다. 자세한 내용은 https://support.servicenow.com/nav_to.do?uri=%2Fkb_view.do%3Fsys_kb_id%3D55ecefd61bf3774cada243f6fe4bcb44 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 불완전한 프로필: 프로필을 구성하는 동안 추가 옵션()SIR 인시던트 상태에 따라 공격 업데이트 및 종결을 자동화 섹션에서 마침 단추를 클릭하여 프로필이 수집 대기 중임을 나타내는 대기 상태로 이동되도록 해야 합니다.
- 프로파일 확인: 통합이 올바르게 작동하는지 확인하려면 프로파일 상태, 프로파일의 마지막 가져온 날짜, 위반 임포트 테이블, 작업 테이블 기록에 대한 위반을 확인합니다.
- MID 서버 구성: 애플리케이션을 온 프레미스에 IBM QRadar 설치하는 경우 MID 서버를 구성한 후 MID 서버 애플리케이션을 생성해야 합니다. 통합 구성 타일에서는 MID 서버 이름 대신 MID 서버 애플리케이션 이름을 사용해야 합니다.

  주:
  기본 MID 서브 시간 제한은 30초입니다. 시간 초과 기간 비활성화에 대한 지침을 보려면 문서를 참조하십시오 〈link〉. 이는 시스템 전체의 변경 사항이며 다른 통합에 영향을 미칠 수 있습니다.

- 위반 업데이트: *sn_sec_qradar.get_offense_updates* 속성을 활성화했으며 보안 인시던트 작성이 지연된 경우 해당 특성을 사용 안함으로 설정하십시오. 폴링 간격이 낮고 QRadar 의 위반 로드가 높을 때 큐 로드가 증가하므로 이 특성을 사용하지 마십시오.
- 보안 인시던트에서 이벤트, 플로우 데이터, remote_ip 또는 사용자 데이터 누락: 보안 인시던트에서 이벤트, 플로우 데이터, remote_ip 또는 사용자 데이터가 누락된 것을 관찰하는 경우 *sn_sec_qradar.sid_ttl* 매개변수의 시간 제한(초)을 늘립니다. 지속 시간을 늘리면 AQL이 각 위반 구문 분석을 완료할 때까지 보안 인시던트 작성이 지연됩니다.
- 시간 초과: 애플리케이션 로그에서 시간 제한 오류를 확인할 경우, 다음 플로우 디자이너 작업을 검토하고 수정합니다.

Flow Designer 작업

매개변수	작업
샘플 위반 가져오기 `var flow_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.fire_rest_for_offenses', flow_inputs, 60000);`	기간을 밀리초 단위로 검토하고 업데이트합니다.
샘플 위반 가져오기 `var flow_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.fire_rest_for_offenses', flow_inputs);`	*executeAction*에 대한 매개변수를 추가하고 기간을 밀리초 단위로 입력합니다.
폴링 테이블의 프로파일 및 큐 기록에 대한 위반 가져오기 `var flow_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.fire_rest_for_offenses', flow_inputs, 180000);`	기간을 밀리초 단위로 검토하고 업데이트합니다.
연결 **REST** 테스트용 래퍼 `var rest_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.test_connection_rest', rest_inputs);`	*executeAction*에 대한 매개변수를 추가하고 기간을 밀리초 단위로 입력합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

매개변수	작업
API 자격 증명 REST를 확인하기 위한 래퍼 `var rest_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.validate_credentials_rest', rest_inputs);`	*executeAction*에 대한 매개변수를 추가하고 기간을 밀리초 단위로 입력합니다.
IBM QRadar Offense 업데이트에 대한 **REST** 단계 `var ## = sn_fd.FlowAPI.executeAction('sn_sec_qradar.' +restStep, ##, 60000);`	기간을 밀리초 단위로 검토하고 업데이트합니다.

IBM QRadar - 인시던트 보강 통합

인시던트 보강 통합은 IBM QRadar 로그를 검색하고 관련 사이팅 정보를 보안 인시던트에 추가합니다.

탐색

보안 인시던트 응답 통합

설정

- 인시던트 보강 통합 시작하기 IBM QRadar
- 사이팅 검색 구성 기록 생성

사용

- 사이팅 검색 실행
- Security Operations Integration - 사이팅 검색 플로우
- 보안 운영 - QRadar 사이팅 검색 플로우
- 사이팅 검색 상세 정보 보기
- 사이팅 검색 결과 보기

개발

- ServiceNow 보안 운영 통합 개발 가이드라인
- 통합 작성을 위한 팁
- 개발자 교육
- 개발자 설명서

문제 해결 및 도움받기

- 통합 문제 해결
- 보안 운영 커뮤니티에서 질문 또는 답변하기
- 알려진 오류 포털에서 알려진 오류 문서 검색

- 연락처 고객 서비스 및 지원

인시던트 보강 통합 시작하기 **IBM QRadar**

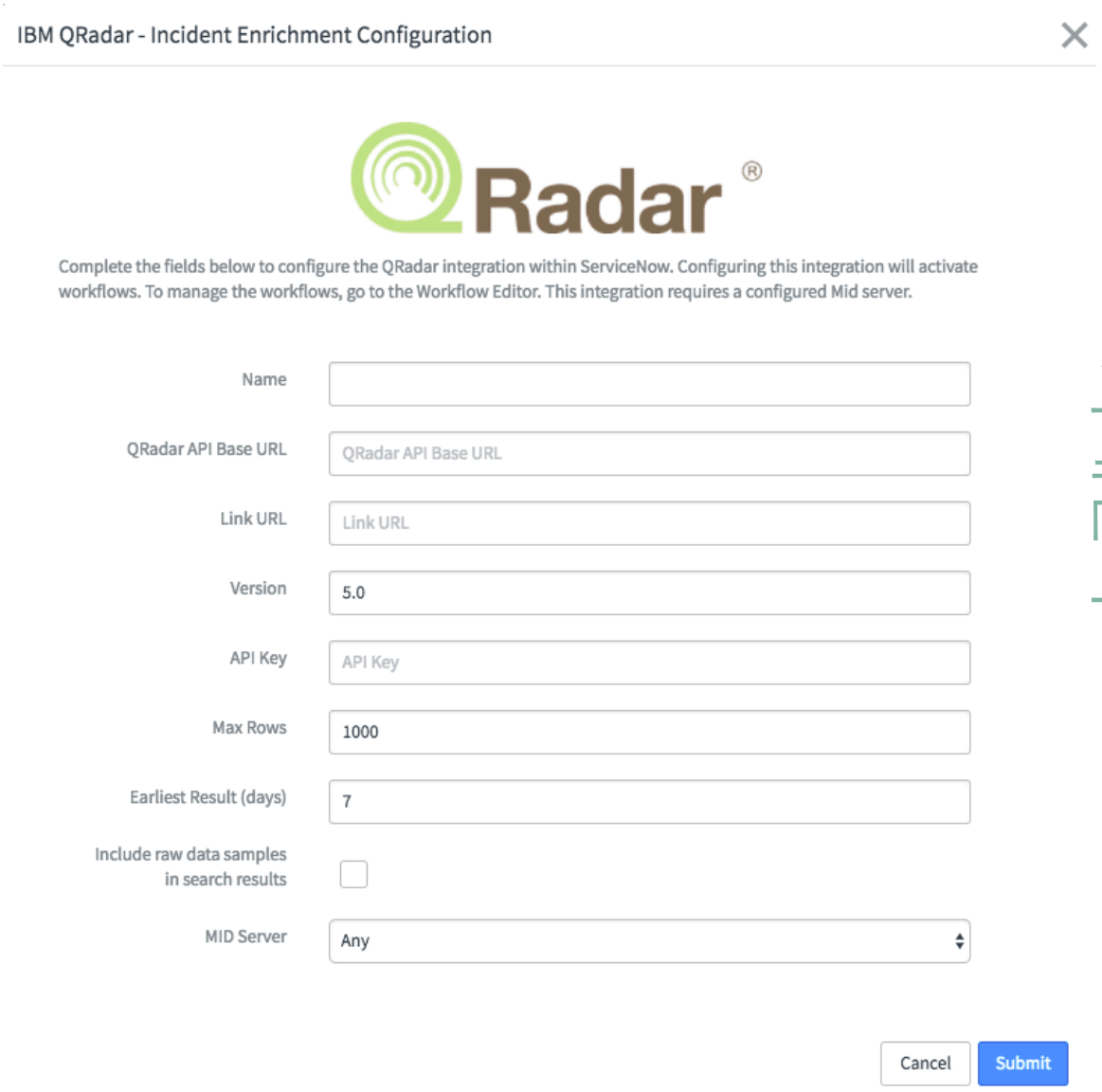
IBM QRadar 는 와 쉽게 보안 운영통합되는 엔터프라이즈 SIEM(보안 정보 및 이벤트 관리) 제품입니다. 인시던트 보강 통합을 사용하려면 IBM QRadar 먼저 에서 ServiceNow Store 다운로드하여 적절한 API 기준 URL 및 API 키를 추가해야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_si_admin

프로시저

1. 에서 통합을 다운로드합니다. ServiceNow Store.
2. 설치가 완료되면 프로파일에서 IBM QRadar API 기준 URL 및 API 키에 액세스하고 IBM QRadar 가져옵니다.
3. 인스턴스에서 다음으로 이동합니다. 보안 운영 〉 통합 〉 통합 구성.
   사용 가능한 보안 통합은 일련의 카드로 표시됩니다.
4. - 인시던트 보강 카드에서 IBM QRadar새로 만들기를 클릭합니다.



5. 필요에 따라, 필드를 채웁니다.

필드	설명
이름	이 구성의 이름입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
QRadar API 기준 URL	사이트에서 가져온 기본 URL입니다 IBM QRadar .
링크 URL	〔선택사항〕 사용 가능한 경우 인스턴스에 링크되는 링크 URL입니다 IBM QRadar .
버전	IBM QRadar 버전은 5.0이 기본값입니다.
API 키	사이트에서 가져온 API 키입니다 IBM QRadar .
최대 행 수	검색할 행의 최대 수입니다.
가장 빠른 결과 (일)	일수 단위로 보려는 가장 빠른 결과입니다.
검색 결과에 원시 데이터 샘플 포함	사이팅 검색 결과에 원시 데이터 샘플을 포함하려면 이 옵션을 선택합니다. 반환되는 데이터의 양은 보안 인시던트 응답 속성의원시 데이터 속성 행 수의 설정에 따라 달라집니다.
MID 서버	활성 MID 서버를 사용하려면 임의 를 선택하고, 특정 MID 서버 이름을 선택합니다.

주:
이 통합을 구성하면 워크플로우가 활성화됩니다. 워크플로우를 관리하려면 워크플로우 편집기로 이동합니다.

6. 제출을 클릭합니다.
   통합 구성 카드가 표시됩니다.
7. 새 구성 카드를 볼 때 구성 또는 삭제를 클릭하여 구성을 변경하거나 삭제할 수 있습니다.
8. 통합 구성 카드의 원래 목록으로 돌아가려면 구성 표시 드롭다운 목록에서 아니요를 선택합니다.

LogRhythm 개요

이 통합의 매핑 유연성은 분석가에게 추가 조사 및 정정을 위해 보안 인시던트에 ServiceNow AI Platform 통합할 수 있는 이벤트 및 관련 경보 데이터에 대한 가시성을 제공합니다.

경보 프로파일은 보안 인시던트에 ServiceNow AI Platform 다양한 LogRhythm 경보 필드가 표시되는 방식을 사용자 지정하기 위해 인스턴스에 생성됩니다ServiceNow AI Platform. 알람 필드의 기본 매핑이 제공되며, 고객별 요구 사항에 맞게 편집할 수 있습니다.

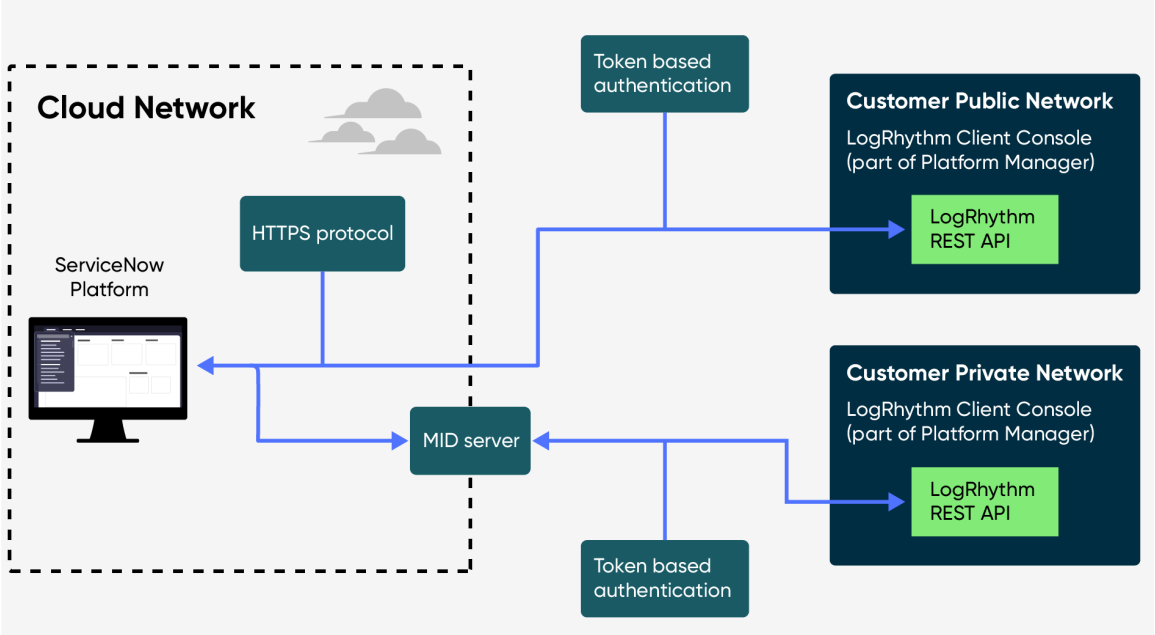
다음 그림은 고객 환경의 예입니다. 이벤트가 인스턴스에서 보안 인시던트 ServiceNow AI Platform# 생성을 트리거하면 MID 서버를 통해 또는 MID 서버가 없는 경우에도 클라이언트 콘솔에서 경보를 LogRhythm 가져오도록 인스턴스에서 요청이 전송됩니다ServiceNow AI Platform#.

REST API 키는 클라이언트 ServiceNow AI Platform# 콘솔에서 인증 LogRhythm 하는 데 사용됩니다. 이 연결을 사용하면 ServiceNow AI Platform 인스턴스가 구성된 프로파일을 기반으로 개별 LogRhythm 경보를 가져올 수 있습니다.

REST API는 REST API에서 액세스하지 않는 메시지 상세 정보를 수집하는 데 사용됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

LogRhythm 통합



주요 기능

이 통합에는 다음과 같은 주요 기능이 포함됩니다.

- 다양한 경보 유형(예: 피싱,맬웨어)에 대해 여러 경보 프로필을 생성할 수 있는 유연성.
- 경보 필드 값을 연관된 SIR 보안 인시던트 필드에 끌어서 놓기로 매핑 LogRhythm 합니다.
- 샘플 경보를 SIR 기반으로 LogRhythm 한 보안 인시던트 레이아웃의 미리 보기입니다.
- 구성 가능한 간격으로 과거 경보뿐만 아니라 진행 중인 향후 경보도 수집합니다.
- 인시던트 종결 시 SIR 자동 LogRhythm 경보 종결. 쉽게 참조할 수 SIR 있도록 인시던트에 대한 URL과 인시던트 ID가 제공됩니다.

지원되는 릴리스 **ServiceNow AI Platform**

이 통합은 Quebec 또는 이후 릴리스와 ServiceNow AI Platform#호환됩니다.

지원되는 버전 **LogRhythm**

이 통합은 7.8 이상과 LogRhythm 호환됩니다. 이전 버전은 API 제한으로 인해 지원되지 않습니다.

주:
다음 항목에 번호가 매겨져 있습니다. 원활한 설치를 위해 예상 결과를 확인하는 데 도움이 되도록 제시된 순서대로 주제를 따르십시오.

에 대한 **REST API** 설정 **LogRhythm**

REST API 키를 사용하여 LogRhythm 개별 경보 필드에 대한 추가 이벤트 상세 정보를 수집합니다. API 키는 REST API를 LogRhythm 사용하여 사용할 수 없는 상세 정보를 제공합니다.

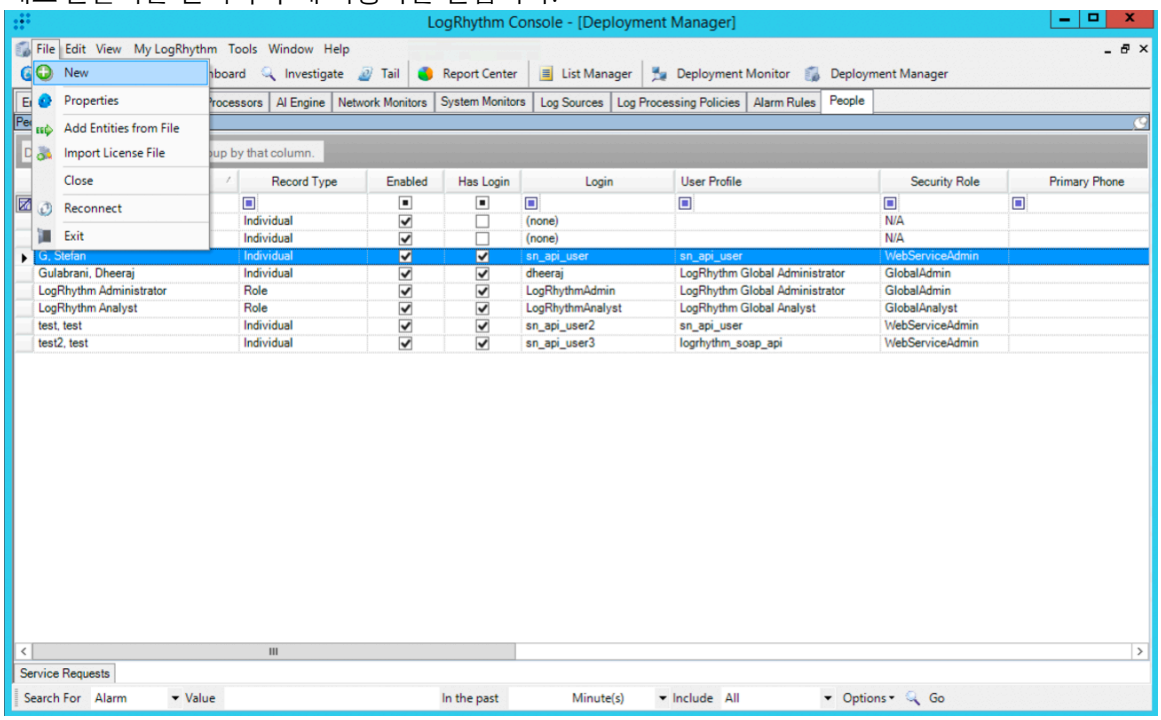
시작하기 전에
필요한 역할: LogRhythm 클라이언트 콘솔/플랫폼 관리자 관리자

이 태스크 정보
이 작업은 클라이언트 콘솔에서 수행됩니다 LogRhythm . 에서 ServiceNow Store플러그인을 설치하기 전에 REST API를 LogRhythm 설정합니다.

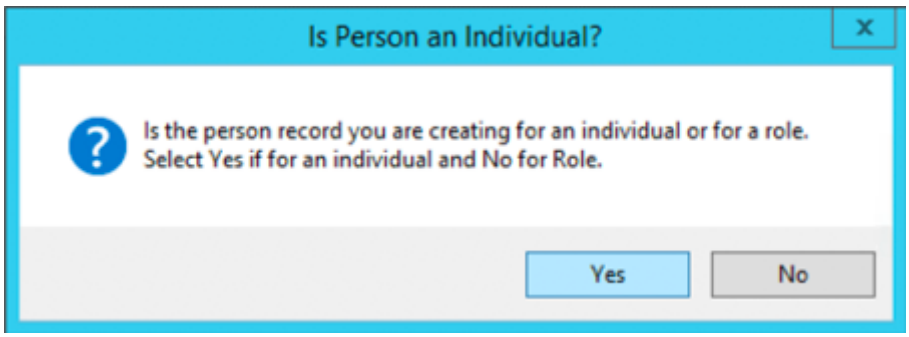
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 클라이언트 콘솔로 LogRhythm 이동하여 파일 메뉴를 선택합니다.
2. 새로 만들기를 클릭하여 새 사용자를 만듭니다.



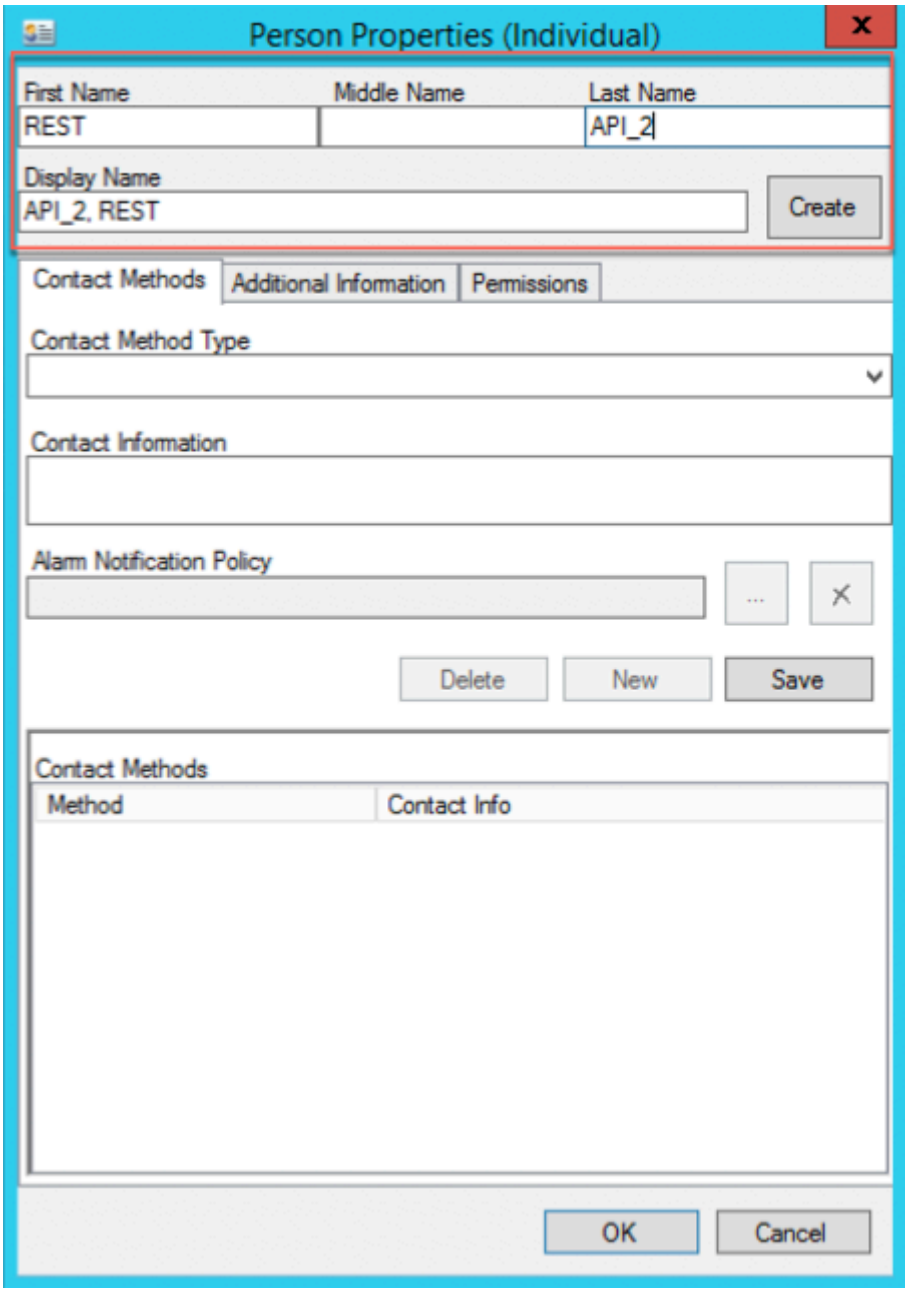
3. 개인이 개인입니까? 대화 상자가 표시되면 예를 클릭합니다.



4. 표시되는 Person Properties 대화 상자에서 Name 필드를 입력합니다.

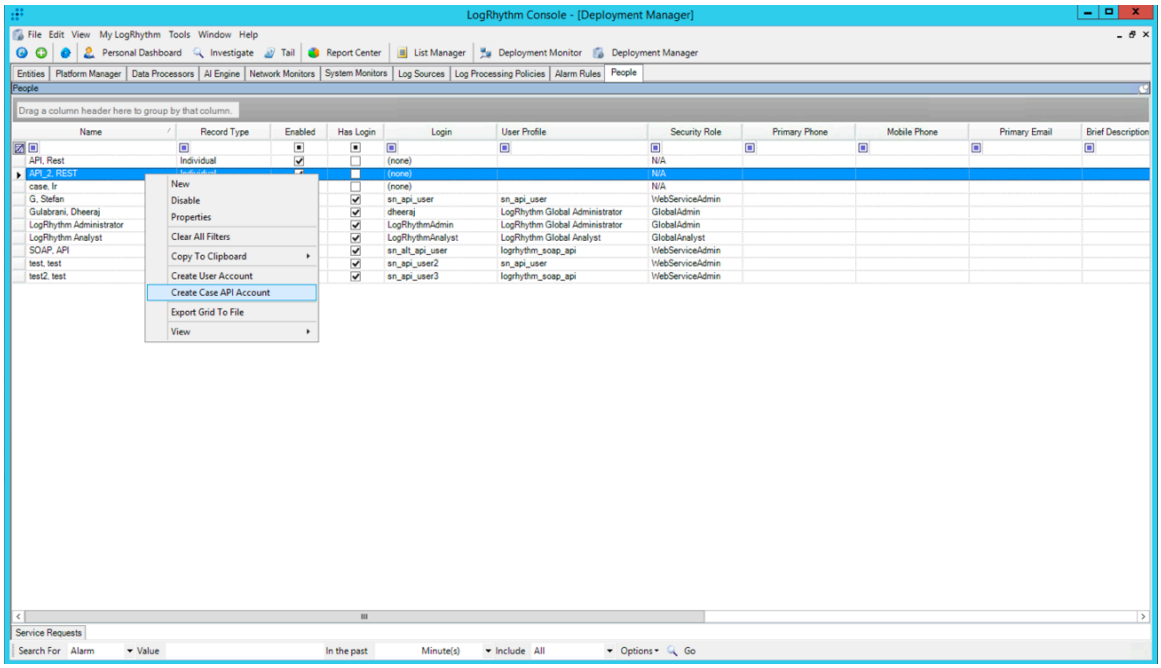
   REST API를 LogRhythm 생성하는 데 사용한 것과 다른 REST API 이름(예: REST API_2)을 사용합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



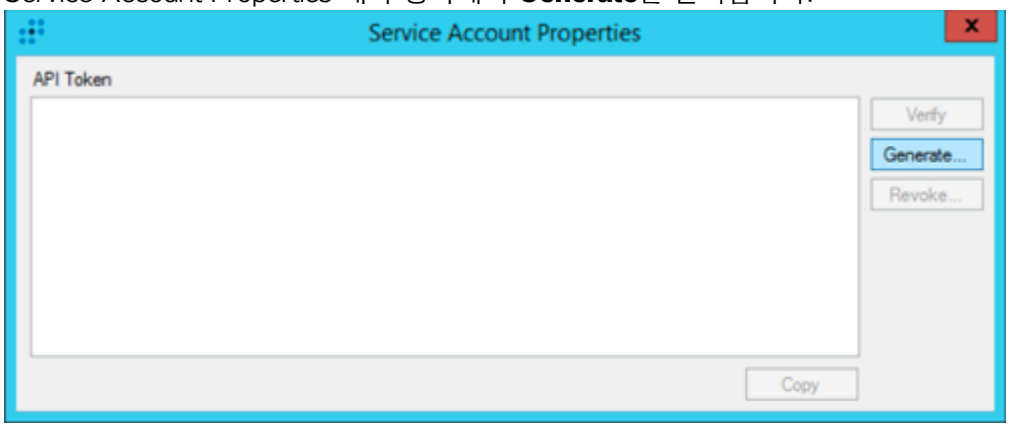
5. 확인을 클릭합니다.
6. 이름 열(**API_2_REST**)에서 새 목록을 마우스 오른쪽 버튼으로 클릭하고 선택 목록에서 케이스 **API** 계정 생성을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

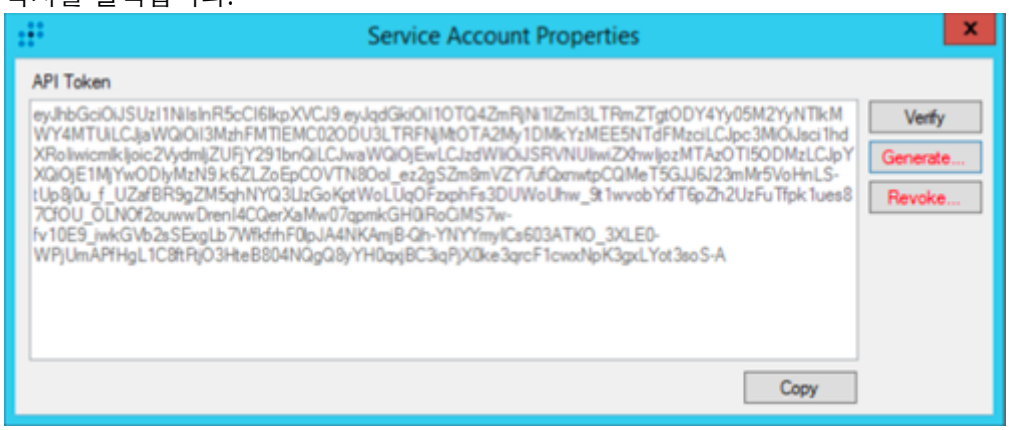


주:
케이스 API는 사용되지 않지만 케이스 API 계정과 REST API의 LogRhythm 자격 증명은 동일합니다.

7. Service Account Properties 대화 상자에서 **Generate**를 클릭합니다.



8. 복사를 클릭합니다.



이제 REST API를 LogRhythm 설정했습니다. 에 나열된 플러그인 설치 및 구성 LogRhythm구성 단계를 수행하는 동안 이전 단계에서 ServiceNow AI Platform 복사한 문자열을 REST API 토큰 필드의 인스턴스에 LogRhythm 붙여 넣습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 수행할 작업
이제 할 준비가 플러그인 설치 및 구성 LogRhythm되었습니다.

플러그인 설치 및 구성 **LogRhythm**

인스턴스에서 통합을 실행하기 전에 설치 및 구성 단계를 완료하여 애플리케이션이 보안 운영ServiceNow AI Platform#.

시작하기 전에

필요한 역할: 관리자

설치하기 전에 다음 설정 검사 목록을 완료합니다. 이러한 설정 작업은 원활한 설치 및 구성을 위해 필요합니다. 최신 LogRhythm 버전은 7.8 이상입니다.

주:
기존 경보 프로파일은 최신 LogRhythm 버전에서 더 이상 지원되지 않으므로 새 알람 프로파일을 만들고 필요한 구성을 수행해야 합니다.

설정 작업	설명
필수 ServiceNow AI Platform# 역할과 보안 인시던트 응답(SIR) 역할을 할당했는지 확인합니다.	예상 결과의 설치, 구성 및 검증에 필요한 역할은 다음과 같습니다. • 시스템 관리자(admin)가 애플리케이션 플러그인을 설치하고 보안 인시던트 관리자(sn_si.admin) 역할을 할당합니다. • (sn_si.admin)은 다음 작업을 감독합니다. ○ 경보 프로파일의 이름을 지정하고, 생성하고, 편집합니다. ○ 경보 매핑 및 필터링 – 보안 인시던트를 생성하는 특정 LogRhythm 경보를 식별하고 이러한 경보 필드가 보안 인시던트에 ServiceNow AI Platform# 매핑되는 방법을 구성합니다. ○ 구성을 완료하기 전에 보안 인시던트 상세 정보가 정확한지 미리 봅니다. ○ 과거 경보를 수집하고 끌어온 경보를 예약합니다. ○ 보안 인시던트 분석가(sn_si.analyst) 역할을 할당합니다. ○ 이 역할은 모듈에 대한 보안 운영 액세스 권한도 갖습니다. • 보안 인시던트 분석가(sn_si.analyst)는 경보 프로파일 설정을 기반으로 생성된 보안 인시던트에 응답합니다.
API 사용자 이름 및 비밀번호를 확보 LogRhythm 하고 버전 LogRhythm 7.8 이상을 사용 중인지 확인하십시오.	API 키에 대한 자세한 내용을 확인하고 계정을 생성하려면 제품 웹 사이트(LogRhythm Enterprise 웹 사이트)를 방문하십시오. 애플리케이션을 설치하기 전에 사용자 계정, 자격 증명 및 인증서를 올바르게 구성해야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

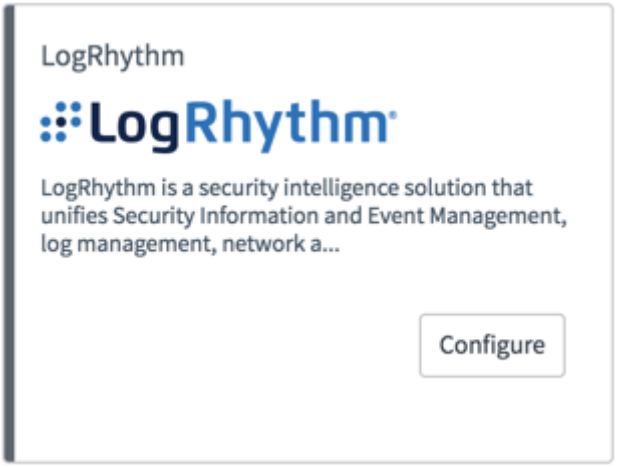
설정 작업	설명
	통합하려면 버전 7.8 이상과 REST API가 LogRhythm 필요합니다LogRhythm. 에 대한 REST API 설정 LogRhythm 문서를 참조하십시오.
MID Server를 설치하고 구성했는지 확인하십시오.	사용자 ServiceNow AI Platform 환경에는 MID 서버가 필요합니다. MID Server를 설정하고 구성하는 방법에 대한 정보는 ServiceNow 제품 설명서 웹 사이트를 참조하십시오.
ServiceNow 통합을 위해 애플리케이션을 설치하기 전에 통합을 지원하는 데 필요한 핵심 애플리케이션이 설치되고 활성화되었는지 확인합니다.	Rome 릴리스 및 이후 제품군 릴리스의 경우 종속성 플러그인(com.snc.si_dep)이 보안 인시던트 응답 필요합니다. 이 플러그인은 제품을 지원하는 데 필요한 모든 종속성을 보안 인시던트 응답 자동으로 설치합니다. 통합에 필요한 다른 보안 운영 애플리케이션을 설치하고 활성화하기 전에 이 플러그인을 설치하고 활성화합니다. 에서 ServiceNow Store다음 보안 운영 애플리케이션이 설치되고 활성화되는지 확인합니다. 설치되지 않은 경우 원활한 설치를 위해 다음 순서로 한 번에 하나의 애플리케이션을 설치하고 활성화합니다. **1.** 보안 인시던트 응답 **2.** 보안 통합 프레임워크 **3.** Security Support Common **4.** 보안 지원 오케스트레이션 통합을 위한 인스턴스 설정에 ServiceNow AI Platform 대한 자세한 내용은 해당 문서를 애플리케이션 활성화 ServiceNow Store참조하십시오제품 또는 애플리케이션에 대한 보안 운영 권리 가져오기.

중요사항:
클라이언트 콘솔에 대한 연결 문제가 LogRhythm 있는 경우 를 참조하십시오 에 대한 연결 확인 LogRhythm.

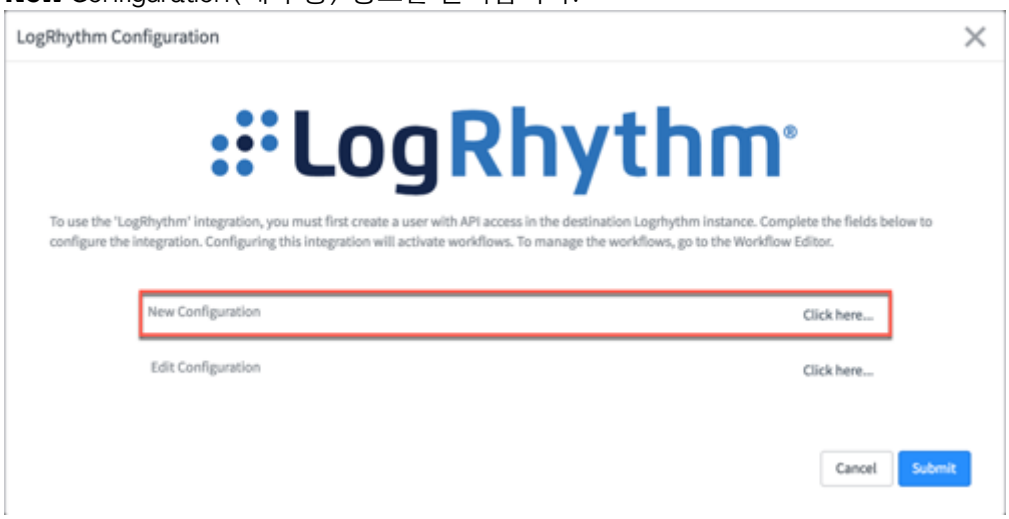
프로시저

1. 통합을 위해 애플리케이션을 설치하지 않은 경우 이를 확인하고 보안 운영 통합 설치 단계에 따라 설치합니다.
2. 설치가 완료되면 다음으로 이동합니다. 통합 〉 통합 구성 타일을 LogRhythm 찾습니다.
3. 구성을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. **New** Configuration(새 구성) 링크를 클릭합니다.



5. 양식의 필드에 내용을 입력합니다.

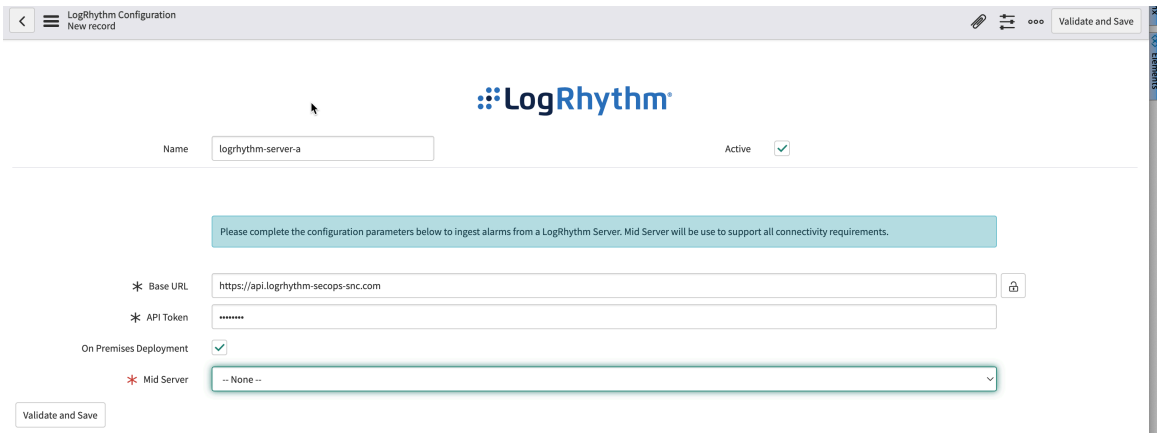
LogRhythm 구성

필드	설명
이름	LogRhythm 서버 이름(예: logrhythm-server-a)
기본 URL	REST API를 호스팅하는 기본 URL입니다 LogRhythm . MID Server는 LogRhythm 클라이언트 콘솔이 호스팅되는 네트워크에 대한 액세스를 허용합니다. 이 URL은 해당 네트워크 내에서 서버가 호스트되는 LogRhythm 위치입니다. 오른쪽 끝에 있는 자물쇠 아이콘을 클릭하여 필드를 편집하고 URL 텍스트(예: https://logrhythm.secops-eng.com:8501/)를 입력합니다.
API 토큰	클라이언트 콘솔에서 생성한 LogRhythm REST API와 연결된 토큰을 입력합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
온 프레미스 배포	온 프레미스 배포인지 LogRhythm 선택하는 옵션입니다.
MID 서버	사용자 환경에 설치된 특정 MID 서버. 활성 상태이고 유효성이 확인된 MID Server만 이 선택 목록에서 사용할 수 있습니다.

다음 그림은 완성된 폼의 예입니다.



6. 확인 및 저장을 클릭합니다.
   확인이 성공적으로 완료되면 메시지가 표시되고 구성 페이지가 다시 로드됩니다 LogRhythm . 다음 단계는 경보 프로필을 만드는 것입니다.

다음에 수행할 작업

유효성 검사가 성공적으로 완료된 후 다음 단계는 입니다 에 대한 경보 프로파일 생성 LogRhythm.

에 대한 경보 프로파일 생성 **LogRhythm**

생성하고 이름을 지정하는 경보 프로파일에서 클라이언트 콘솔에서 끌어올 경보를 LogRhythm 지정합니다. 또한 보안 인시던트의 ServiceNow AI Platform 필드에 매핑되는 방식도 정의합니다.

시작하기 전에

필요한 역할: sn_si.admin

이 태스크 정보

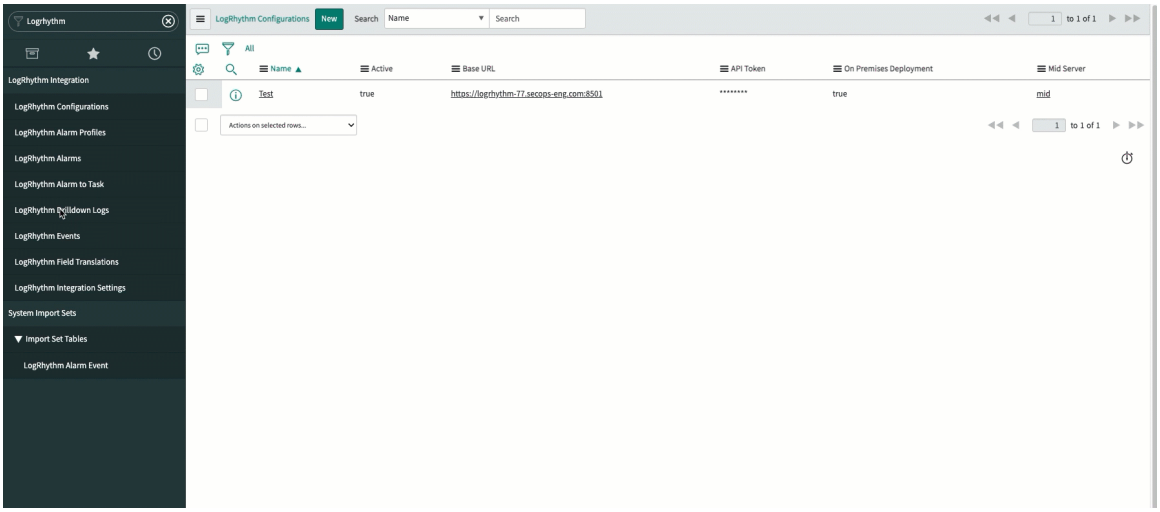
구성된 알람 프로파일에 따라 하나의 알람 프로파일이 모든 유형의 알람을 즉시 수집할 수 있지만 필터 기준을 사용하여 특정 유형의 알람을 수집할 수 있습니다. 이 ServiceNow AI Platform 통합을 사용하면 구성된 모든 경보 규칙 또는 생성된 프로파일을 기반으로 하는 특정 경보 규칙이 수집됩니다. 그런 다음 고위험 수준의 경보와 같은 경보 규칙을 필터링하여 보안 인시던트를 생성해야 하는 경보를 지정할 수 있습니다. 보안 인시던트가 생성되기 전에 필터링된 경보의 개별 필드 값이 보안 인시던트의 ServiceNow AI Platform 해당 필드에 매핑됩니다. 이 구성은 인스턴스 내의 ServiceNow AI Platform 경보 프로필을 통해 수행됩니다.

프로시저

1. 다음으로 이동 모두 〉 **LogRhythm** 통합.
2. **LogRhythm Alarm Profiles** 모듈을 선택하여 **Alarm Profiles** 목록을 표시합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

경보 프로파일



3. 새 경보 프로필을 만들려면 새로 만들기를 클릭합니다.
   새 경보 프로파일 양식이 표시됩니다. 진행률 표시줄의 페이지 상단에서 이름이 선택됩니다. 이 막대는 구성 중 진행 상황을 추적합니다.
4. 양식에서 필드를 채웁니다.

경보 프로파일

필드	설명
이름	경보 프로파일의 이름입니다. 이 이름은 무단 액세스 (*VPN*), 맬웨어 또는 피싱과 같은 경보 유형을 식별하는 데 도움이 됩니다.
간단한 설명	경보 유형 또는 경보 범주를 포함할 수 있는 경보 프로파일에 대한 추가 정보를 위한 짧은 텍스트입니다. 예 설명: 무단 Powershell 및 Sudo 액세스 시도와 관련된 모든 경보입니다.
소스	선택 목록의 소스 서버. 목록은 이미 설정한 구성으로 구성됩니다 LogRhythm (예: `logrhythm-server-a`). 플러그인 설치 및 구성 LogRhythm 문서를 참조하십시오.
순서	경보 프로파일 우선 순위입니다. 이 필드는 두 개 이상의 경보 프로파일이 트리거 조건을 공유할 때 알람 프로파일이 실행되는 순서를 나타냅니다.
활성	기본적으로 이 옵션은 선택되어 있지 않습니다. 모든 알람 프로파일 설정 단계를 완료하고 마침을 클릭하면 이 확인란을 선택하여 알람 프로파일을 활성화하라는 메시지가 표시됩니다. 경보 프로파일이 활성 상태이면 클라이언트 콘솔에서 자동으로 경보를 LogRhythm 가져옵니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. 계속을 클릭하여 데이터를 저장하고 매핑 양식으로 이동합니다.

   확인에 성공하면 페이지가 다시 로드되고 매핑 양식이 표시됩니다. 연결 및 자격 증명을 성공적으로 확인하기 전까지는 구성을 진행할 수 없습니다.

관련 정보

매핑

매핑

수집할 소스를 선택한 LogRhythm 후에는 개별 LogRhythm 경보 필드를 ServiceNow AI Platform 보안 인시던트 필드에 매핑해야 합니다.

경보 매핑에는 다음 작업이 포함됩니다.

- 경보를 매핑 LogRhythm 합니다. 이 작업에서는 클라이언트 콘솔에서 경보 ID 또는 최신 경보를 사용하여 샘플 경보를 나열하고 수집(끌어오기)합니다 LogRhythm .
- 샘플 알람 필드는 다음 세 그룹으로 분류됩니다.
  - 경보 필드: 사용 가능한 경보 필드와 해당 값이 표시됩니다.
  - 이벤트 필드: 사용할 수 있는 이벤트 필드와 해당 값이 표시됩니다.
  - DrillDownLog 필드: 사용 가능한 드릴다운 로그 필드와 해당 값이 표시됩니다.
- 끌어온 각 경보 ID는 탭으로 표시됩니다. 경보 ID 탭에서 양식 왼쪽에 있는 경보 샘플 수집 섹션의 모든 중요 경보 필드가 양식 오른쪽에 있는 SIR 인시던트 필드 매핑 섹션에 매핑되는지 확인합니다.
- 경보를 SIR 인시던트 필드 매핑 필드에 매핑하면 입력 식 필드에도 경보 범주가 표시되는 것을 볼 수 있습니다. 예: ${Alarm: alarmid}$.
- 보안 인시던트에서 필드를 추가하거나 제거하여 구성을 수정할 수 있습니다. 제공된 색상 코딩으로 간과되거나 중복된 필드를 추적합니다.
- 경보를 필터링하여 SIR 애플리케이션에 수집되는 경보를 지정할 수 있습니다. 경보를 직접 필터링하거나 경보 범주를 사용하여 경보, 이벤트 또는 드릴다운 로그를 기반으로 검색을 드릴다운할 수 있습니다.
- 보안 인시던트의 우선순위 및 범주 필드 값의 형식을 지정하려면 스크립트 편집기를 사용하십시오.

다음 단계는 .경보 필드를 보안 인시던트 필드에 매핑 LogRhythm

관련 정보

경보 필드를 보안 인시던트 필드에 매핑 LogRhythm

스크립트 편집기를 사용하여 값 서식 지정 LogRhythm

다음에 대한 경보 필터링 LogRhythm

경보 필드를 보안 인시던트 필드에 매핑 **LogRhythm**

개별 경보 필드를 보안 인시던트 필드에 매핑합니다. 미리 구성된 매핑을 편집할 수 있으며 필드에 색상 코딩이 제공되어 이미 매핑된 경보를 모니터링하는 데 도움이 됩니다. 이 단계는 편집 내용이 보안 인시던트의 필드에 미치는 영향을 시각화하는 데 도움이 됩니다.

시작하기 전에
필요한 역할: sn_si.admin
경보에 LogRhythm 익숙하지 않은 경우 클라이언트 콘솔로 LogRhythm 이동하여 몇 가지 샘플 경보 ID를 검토합니다. 다음 예에서는 LogRhythm 경보 9468 및 9474 를 사용하여 경보를 보안 인시던트에 매핑했습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

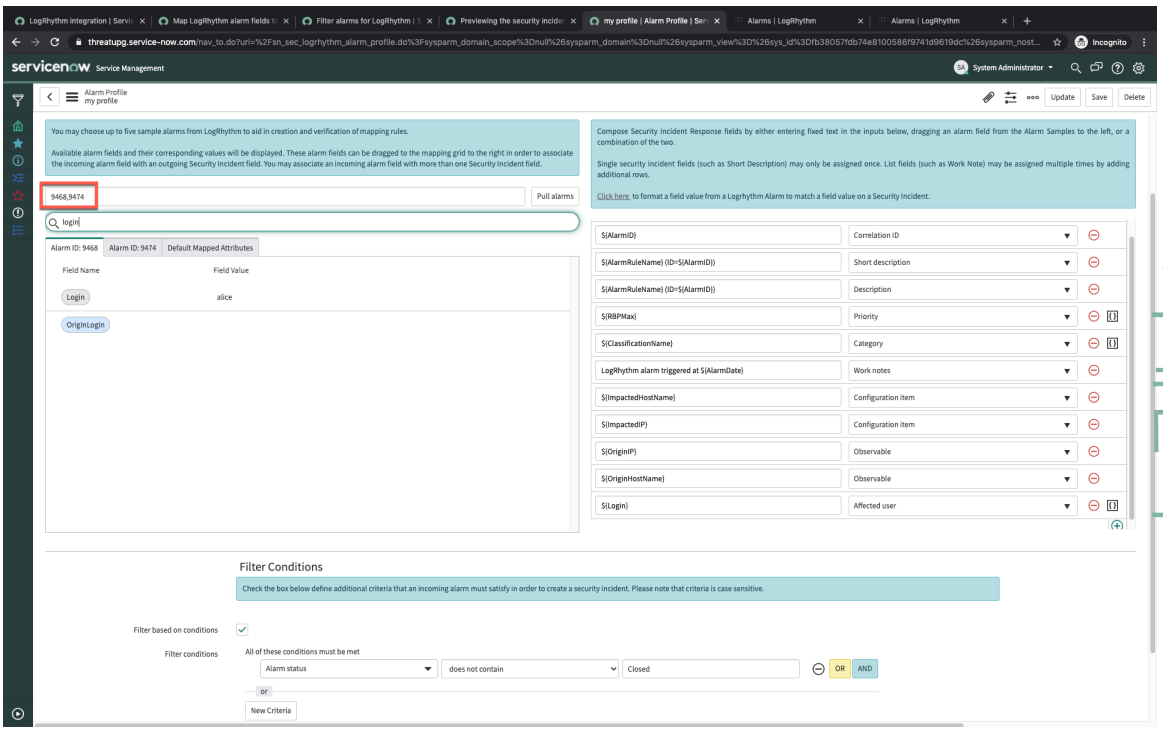
이 태스크 정보
이 양식을 사용하여 왼쪽의 경보 규칙을 오른쪽의 보안 인시던트 필드에 매핑 LogRhythm 합니다.

다음 그림은 각 경보 프로파일에 대해 미리 구성된 경보의 기본 매핑을 보여줍니다. 이 기본 매핑은 편집할 수 있으며, 이 양식을 사용하여 보안 인시던트를 채우는 필드를 사용자 지정합니다. 이 매핑을 완료하면 경보 필드를 추가하거나 제거하면 보안 인시던트의 필드 값에 어떤 영향을 줄 수 있는지 확인할 수 있습니다.

다음 그림 LogRhythm 에서 이 양식의 왼쪽에는 경보 규칙이 요약되어 있습니다. 이러한 경보 규칙의 값은 양식 오른쪽에 있는 보안 인시던트 필드에 매핑됩니다.

프로시저

1. LogRhythm에 대한 경보 프로필을 만든 후 진행률 표시줄에서 매핑 을 클릭합니다.
2. 알람 샘플 수집 필드에 최대 5개의 샘플 LogRhythm 알람 ID를 쉼표로 구분하여 입력합니다 (9468,9474).



3. 경보 필드 옆에 있는 **Pull** Alarms를 클릭합니다.

   샘플 알람을 끌어오는 데 몇 분 정도 걸릴 수 있습니다. 트랜잭션이 작동 중임을 나타내는 메시지가 화면 맨 위에 표시됩니다.

   샘플 경보 ID가 제출되고 서버에서 성공적으로 끌어오 LogRhythm 면 경보 필드와 해당 값이 탭에 표시됩니다.

   주:
   경보 ID를 성공적으로 끌어온 후 다음 ServiceNow AI Platform 메시지를 반환할 수 있습니다. ## # ### # #### # ####. ### ### #### ##### ## ## # # ## # ##### ## ######. itemspacketsin, itemspacketsout.

   이 메시지는 끌어온 단일 경보에 이전에 에서 ServiceNow AI Platform처리하지 않은 필드 이름이 포함될 때 발생합니다. 이러한 필드는 매핑에 사용할 수 있지만 이 메시지가 표시되면 필터링 조건을 설정할 준비가 되면 이러한 필드가 조건 작성기의 필터 선택 목록에 표시되고 사용할 수 있도록 양식을 다시 로드하십시오.

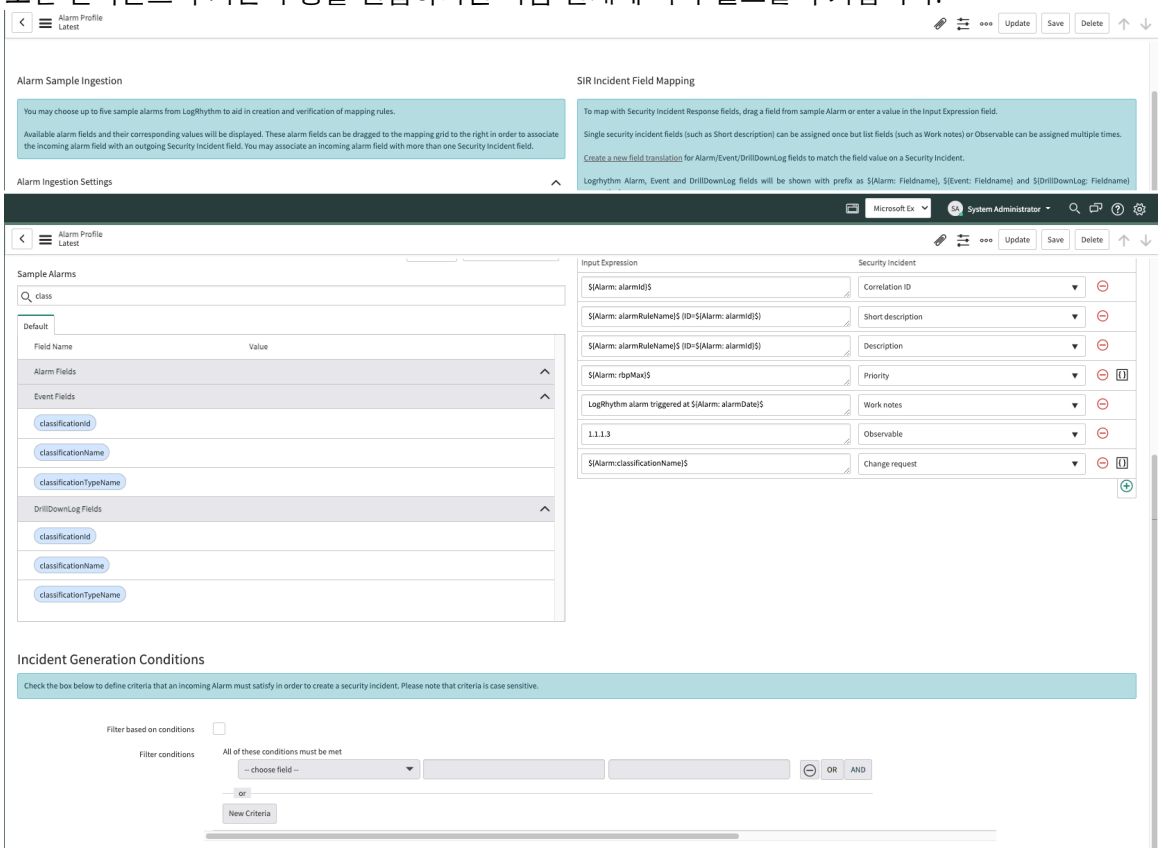
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

경보 프로파일 구성에서 이러한 샘플 경보를 수집하면 값이 없는 보안 인시던트에 경보 필드를 매핑하는 것을 방지할 수 있습니다. 또한 경보 필드를 보안 인시던트의 적절한 필드에 값과 맞춥니다. 이 단계에서는 모든 중요 경보 필드가 매핑되고 보안 인시던트에 필드 값이 누락되지 않도록 합니다.

매핑 프로세스에서 경보가 간과되거나 중복되지 않도록 경보 필드는 색상으로 구분됩니다. 연한 파란색 경보 필드(Account, AlarmRuleID, AlarmStatus 등)는 보안 인시던트에 매핑할 필드가 아직 선택되지 않았음을 나타냅니다.

회색 필드(AlarmDate, AlarmID # AlarmRuleName)는 필드가 이미 선택되었고 보안 인시던트의 필드에 매핑되었음을 나타냅니다. 경우에 따라 경보 필드가 보안 인시던트의 두 개 이상의 필드에 매핑될 수 있으므로 이 색상 코딩은 매핑을 추적하는 데 도움이 됩니다. 예를 들어 #### 및 ## ## 필드에는 둘 이상의 값이 있을 수 있습니다.

4. 샘플 알람 데이터를 지우려면 **Clear Sample Alarm Data**를 클릭합니다.
5. 보안 인시던트의 기본 구성을 편집하려면 다음 단계에 따라 필드를 추가합니다.



   a. 양식의 오른쪽 아래에 있는 더하기 아이콘을 클릭합니다.
   새 필드가 표시됩니다.

   b. 보안 인시던트 열의 선택 목록에서 사용 가능한 필드를 선택합니다.

   확장된 선택 목록에서 일부 필드는 음영 처리됩니다. 예를 들어 ## 의 회색 배경은 보안 인시던트에 매핑되었음을 나타냅니다. 경보 필드의 색상 코딩 LogRhythm 과 마찬가지로 보안 인시던트 필드에 대한 이 색상 코딩은 경보 필드의 값이 실수로 동일한 보안 인시던트 필드에 매핑되지 않도록 합니다.

   위 그림에서 경보 규칙 ${Alarm:classificationName}$ 은 이 프로파일의 보안 인시던트에 있는 ## 필드에 이미 매핑되어 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
옵저버블 필드는 여러 옵저버블을 표시할 수 있도록 동일한 보안 인시던트의 보다 큼 필드에 매핑될 수 있습니다. 마찬가지로 ## ## 및 ## ## 필드를 매핑하여 여러 값을 표시할 수 있습니다.

양식의 경보 샘플 수집 쪽에서 파란색은 경보 규칙 필드가 매핑되지 않았음을 나타냅니다. 회색은 매핑되었음을 나타냅니다. 양식의 SIR 인시던트 필드 매핑 쪽에 있는 선택 목록에서 흰색은 필드가 매핑되지 않았음을 나타냅니다. 회색은 필드가 매핑되었음을 나타냅니다. 이 색상 코딩을 사용하면 필드 매핑을 추적하는 데 도움이 됩니다.

위 그림에서는 ### ## #### 선택 목록에서 보안 인시던트의 새 필드로 선택되었습니다.

c. 양식 왼쪽에 있는 경보 샘플 수집 섹션에서 입력 식 필드에서 원하는 경보 ID를 마우스 왼쪽 버튼으로 클릭하여 선택합니다.

위 그림에서는 ### 이 선택되었습니다.

d. 지워진 필드로 끌어다 놓습니다.
SIR 인시던트 필드 매핑 섹션의 왼쪽 열에 ### ## ### 필드의 새 값이 표시됩니다. 이 경우 경보의 LogRhythm### 값이 보안 인시던트의 ### ## ### 필드에 표시됩니다.

6. 또는 입력 표현식(Input Expression) 열의 필드 값을 수동으로 입력하려면 입력 표현식(Input Expression) 필드에 커서를 놓고 원하는 경보 값을 입력합니다.

예를 들어 위 그림에서는 다른 필드(## ##)가 보안 인시던트 양식에 추가되어 있고 이 필드에는 ## #### ## 이 수동으로 입력되어 있습니다.

7. 필요에 따라 미리 구성된 매핑을 계속 편집합니다.
경보 필드의 LogRhythm 값을 보안 인시던트의 필드에서 지원하는 값으로 변환해야 하는 경우 스크립트 편집기를 사용할 수 있습니다. 스크립트 편집기를 사용하여 값 서식 지정 LogRhythm 문서를 참조하십시오.

다음에 수행할 작업
필드 매핑을 완료한 후 다음 단계는 입니다 다음에 대한 경보 필터링 LogRhythm.

다음에 대한 경보 필터링 **LogRhythm**

필드를 매핑한 후 경보에 대한 필터링 기준을 설정하면 SIR 애플리케이션에 수집할 경보를 결정하는 데 도움이 됩니다. 경보를 필터링하면 경보 프로파일이 활성화될 때 수집하는 경보 수를 크게 줄일 수 있습니다.

시작하기 전에
필요한 역할: sn_si.admin

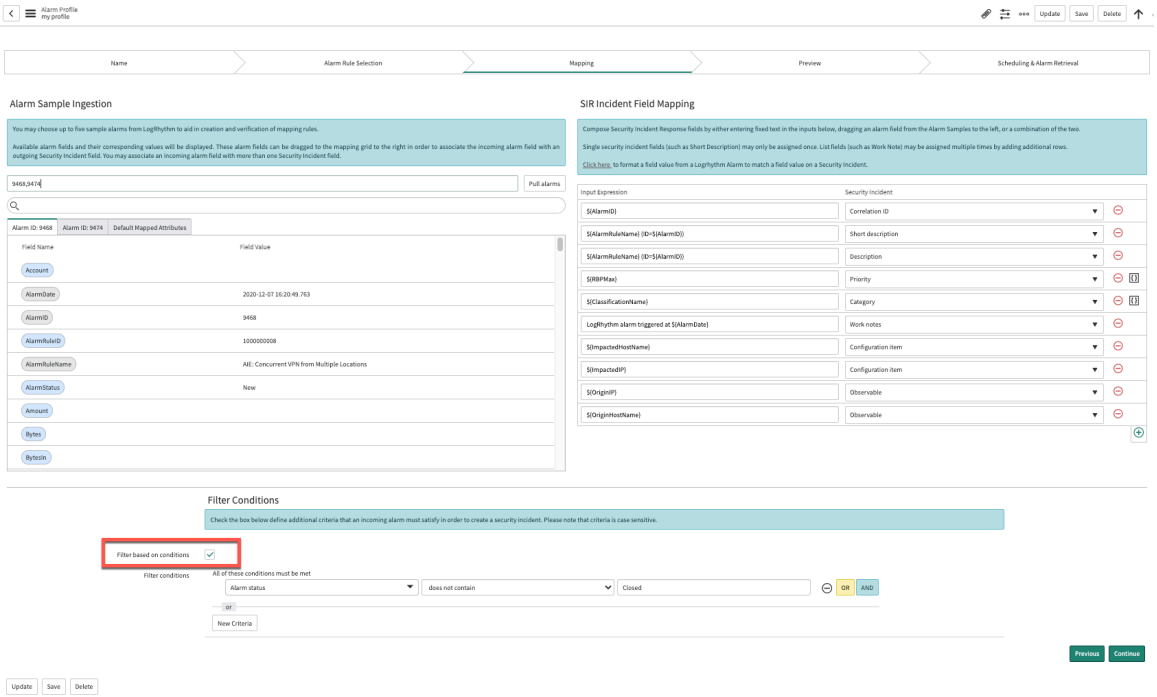
이 태스크 정보
매핑 양식 하단의 필터링 조건을 사용하여 특정 경보를 필터링하거나 특정 필드 수준 기준을 충족하는 경보로만 수집을 제한합니다. 필터링하면 경보 프로파일이 활성화된 후 수집하는 경보 수가 크게 줄어듭니다. 필터링을 사용하여 보안 운영 센터(SOC) 직원이 지원할 수 있는 관리 가능한 양의 경보를 수집합니다.

주:
다음 예는 Alarm status-does-not-contain-Closed 가 기본 설정인 기본 필터 설정을 보여줍니다. 이 필터는 활성 경보만 가져오며 이 설정은 끌어온 경보 수를 줄입니다. 다음 단계는 심각도 또는 우선 순위 값이 가장 높은 경보만 포함하는 또 다른 유용한 필터를 추가하는 방법을 보여줍니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 필터링 기준을 편집하려면 조건에 따라 필터링 확인란을 선택합니다.

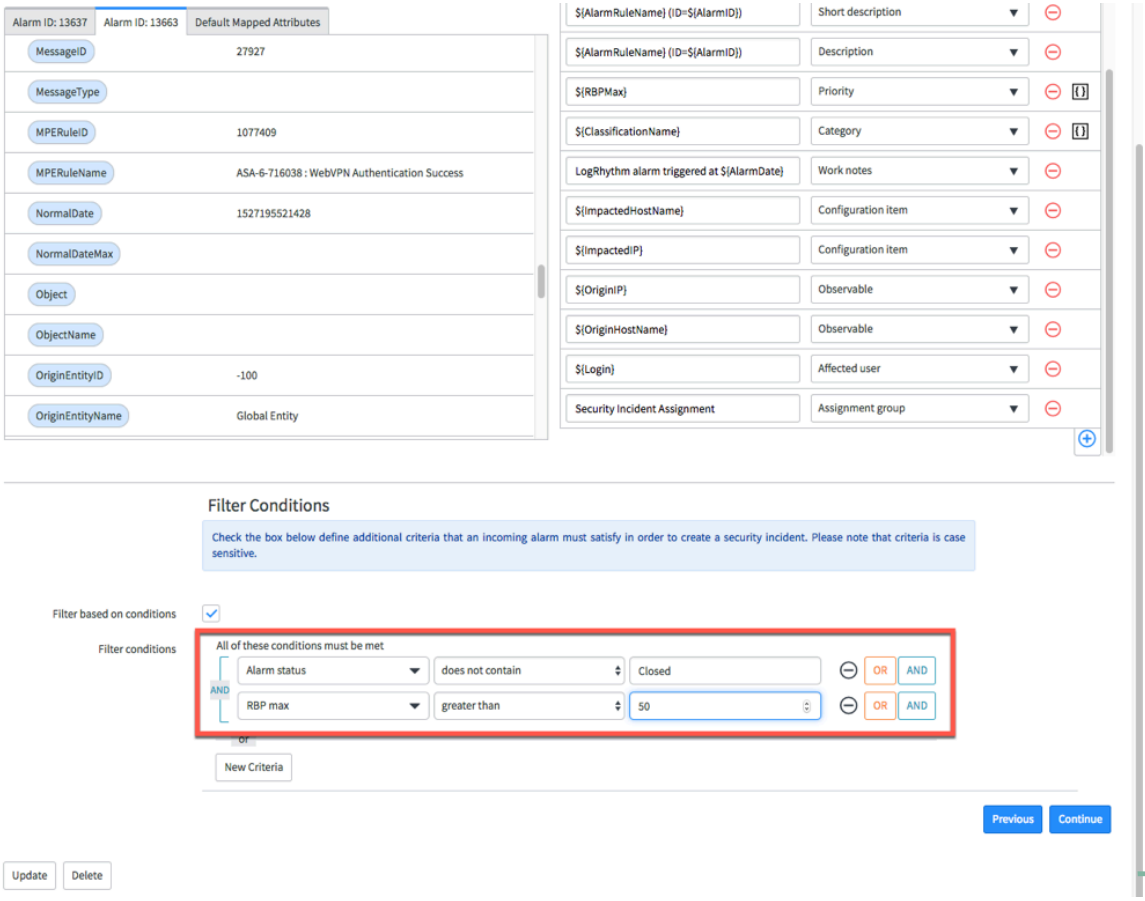


2. 필터 조건 필드 오른쪽에서 OR 또는 **AND**를 클릭합니다.

3. 표시되는 새 줄의 선택 목록에서 필터링 조건을 선택합니다.

다음 이미지는 위험 기반 우선 순위(RBP max)가 50보다 큰 조건에 추가된 추가 필터를 보여줍니다. 이 필터 설정을 사용하면 위험 기반 우선순위 값이 50보다 큰 경보만 LogRhythm 끌어옵니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 모든 중요 LogRhythm 경보 필드가 보안 인시던트에 ServiceNow AI Platform 매핑되었는지 확인하고 경보 수집을 제한하는 필터링 기준을 설정한 후에는 하나를 선택하여 구성을 계속합니다.

다음에 수행할 작업

다음 단계는 보안 인시던트에서 매핑된 필드를 미리 보는 것입니다. 매핑 LogRhythm 된 경보 값으로 보안 인시던트 미리 보기 문서를 참조하십시오.

매핑 **LogRhythm** 된 경보 값으로 보안 인시던트 미리 보기

매핑 단계를 완료한 후 보안 인시던트의 필드에 매핑한 값을 미리 봅니다. 이 미리 보기 단계를 사용하면 보안 인시던트에 표시할 중요 LogRhythm 경보 필드를 모두 매핑했는지 확인할 수 있습니다.

필요한 역할: sn_si.admin.

보안 인시던트

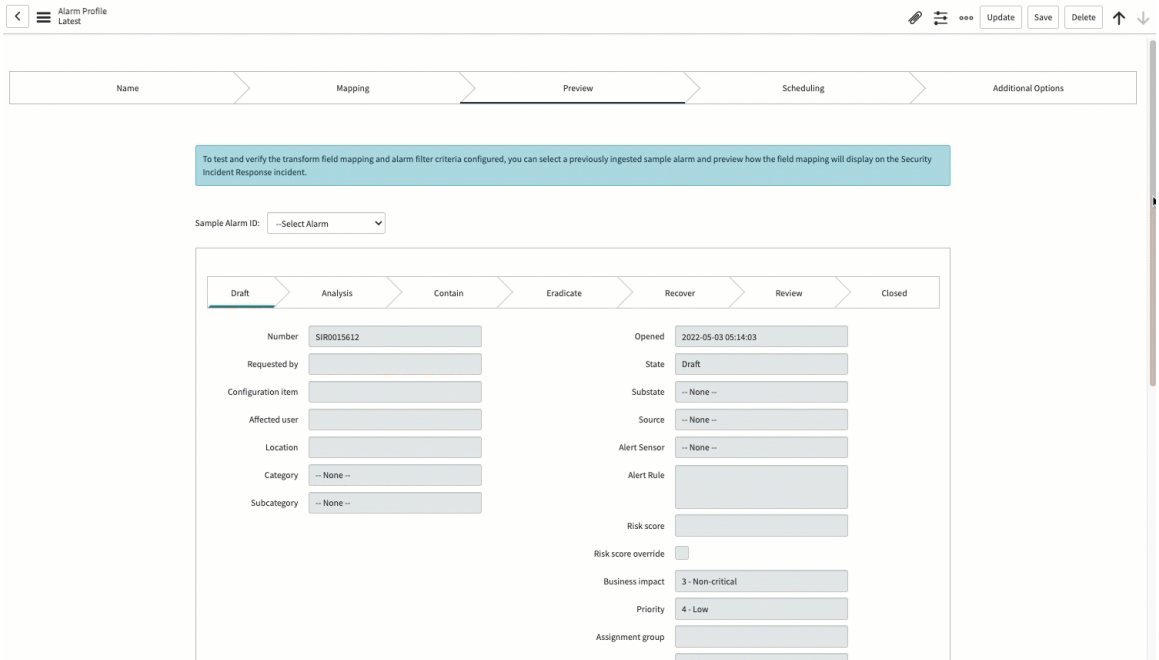
보안 인시던트 미리 보기가 표시되지 않으면 진행률 표시줄에서 미리 보기를 클릭합니다.

전체 ServiceNow AI Platform 보안 인시던트에 대한 미리 보기의 예가 다음 두 그림에 표시되어 있습니다. 보안 인시던트 미리 보기의 이 예는 샘플 경보 13663에서 매핑된 경보 필드로 LogRhythm 채워져 있습니다.

다음 그림에는 보안 인시던트의 ## ##, ### ## ###, ####, ## ## 및 ### ## 필드가 채워져 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 인시던트의 상위 절반



보안 인시던트 양식의 아래쪽에는 ## 필드가 채워져 있습니다. 관련 항목 섹션에서 ## ##, #### 및 ## ## 필드가 값으로 채워집니다. 이러한 필드의 여러 값이 매핑된 경우 각 필드가 둘 이상의 값을 허용할 수 있으므로 각 값이 보안 인시던트에 표시됩니다.

미리 보기의 오류 조건

보안 인시던트를 미리 볼 때 다음 경고 메시지가 표시될 수 있습니다. 샘플 경보가 필터링 기준을 통과하지 못하면 전체 보안 인시던트가 채워지지 않습니다.

입력 값을 찾을 수 없음

경보 ID가 필터링 조건 내에 포함된 경우 특정 매핑된 필드에 대한 특정 입력 값을 찾을 수 없으면 경고 메시지가 계속 표시될 수 있습니다. 다음 예에서는 기록 미리 보기에서 매핑 된 경우에도 ## ## 필드에 값이 없다고 가정합니다.

이러한 유형의 메시지의 경우 매핑 기록에서 입력 값이 올바른지 확인합니다. 이 경우 보안 인시던트의 ## ## 필드에 있는 사람이 인스턴스에서 잘못되었습니다 ServiceNow AI Platform . 이 경보가 수집되고 이 조건으로 보안 인시던트를 생성하면 이 입력 값(Abel Tuter)이 있는 필드는 보안 인시던트에서 비어 있습니다.

파란색으로 표시된 나머지 메시지는 정보 제공용이며 이러한 필드에 미리 보기에 표시할 값이 없음을 나타냅니다. 이 미리 보기를 사용하면 보안 인시던트 관리자가 경보 프로파일을 구성하여 초기 생성 단계에서 이러한 필드에 값이 없는지 확인할 수 있습니다. 경우에 따라 보안 인시던트 필드가 나중에 자동으로 채워질 수 있기 때문입니다. 다른 매핑 오류도 표시됩니다.

매핑 및 보안 인시던트 미리 보기가 만족스러우면 하나를 선택하여 구성을 계속합니다.

옵션	설명
진행률 표시줄에서 계속 또는 예약을 클릭합니다.	스케줄링 및 경보 검색 양식으로 이동합니다. 예약 및 경보 검색 이 진행률 표시줄에서 선택됩니다. 다음 단계는 경보 검색을 예약하는 것입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵션	설명
이전을 클릭합니다.	알람 프로파일로 돌아가 매핑을 계속합니다.
미리 보기 양식 상단에 있는 샘플 알람 **ID** 선택 목록에 다른 알람 ID를 입력합니다.	입력한 모든 경보 ID에 대해 샘플 경보 **ID** 선택 목록이 표시됩니다. 최대 5개의 알람을 선택할 수 있습니다. 이 옵션을 사용하면 보안 인시던트의 다른 LogRhythm 경보 ID를 미리 볼 수 있습니다.

보안 인시던트를 미리 보고 결과에 만족하면 다음 단계는 입니다 경보 예약 및 검색 LogRhythm.

경보 예약 및 검색 **LogRhythm**

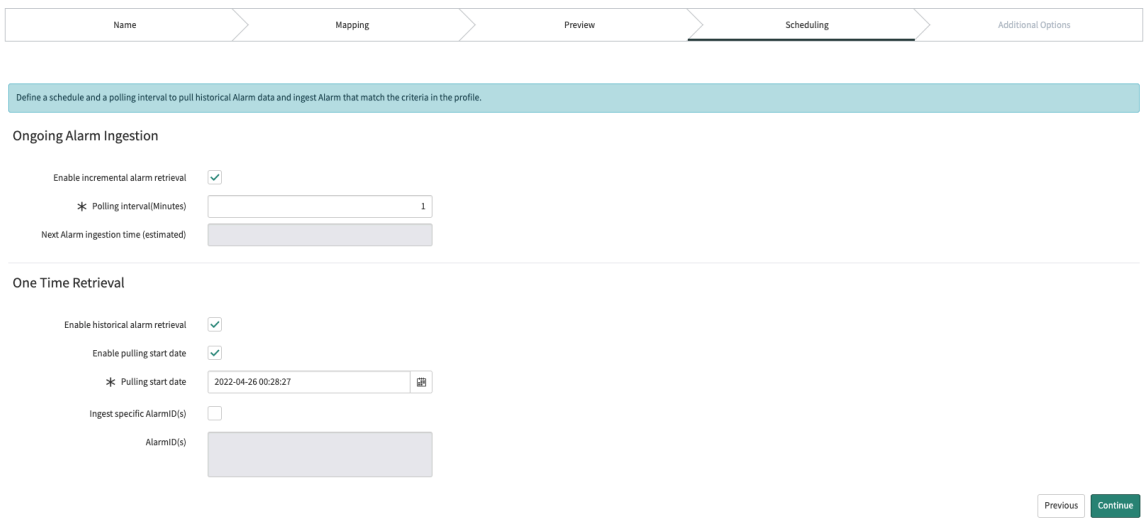
선택하고 매핑한 경보로 LogRhythm 보안 인시던트를 미리 보고 나면 경보 검색을 예약할 준비가 된 것입니다. 이 단계를 완료하면 알람 프로파일을 활성화할 준비가 된 것입니다.

시작하기 전에
필요한 역할: sn_si.admin

이 태스크 정보
스케줄링을 사용하면 검색을 위해 선택한 알람 유형과 스케줄링을 수정할 수 있습니다. 날짜 범위 또는 특정 경보 ID를 기반으로 수집한 경보를 필터링합니다. 이 단계에서는 과거 경보를 수집할지 여부와 경보 프로파일 구성과 일치하는 향후 경보를 폴링하는 빈도를 결정합니다.

프로시저

1. 진행률 표시줄에서 예약 단계를 클릭합니다.



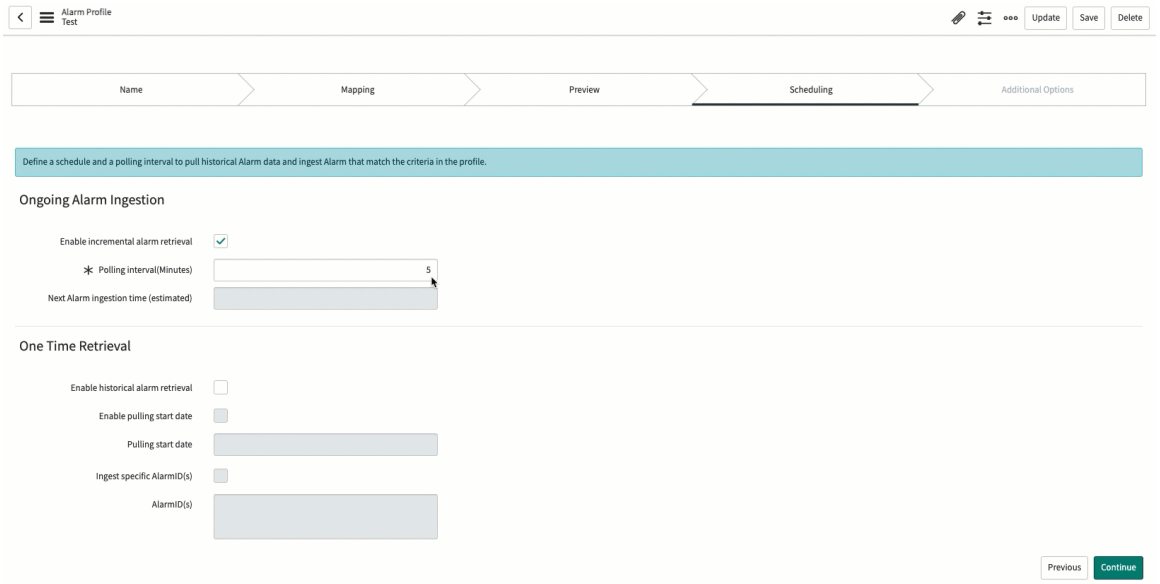
2. 다음 옵션 중에서 선택하여 경보 검색을 구성합니다.

3. 알람 이력 검색을 편집하려면 다음 단계에 따라 알람 검색 날짜 또는 특정 알람 ID를 입력합니다.

   a. **Enable pulling start** date(끌어오기 시작 날짜 사용)를 선택한 다음 **Pulling start** date(끌어오기 시작 날짜)를 선택합니다.

   b. 시작 날짜 가져오기 필드에서 표시되는 달력을 클릭하고 날짜를 선택한 다음 녹색 확인 표시를 선택하여 항목을 저장합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



날짜가 표시됩니다.

c. 또는 **Ingest specific Alarm ID(s)** 옵션을 선택하고 **AlarmID** 필드에 기록 데이터에 대한 특정 Alarm ID를 입력하여 특정 Alarm ID를 검색합니다.

쉼표로 구분된 경보를 최대 5개까지 입력할 수 있습니다.

d. 업데이트를 클릭합니다.

4. 편집을 계속하거나 구성을 완료하려면 다음 옵션 중 하나를 선택합니다.

다음에 수행할 작업

진행 중인 경보 수집 및 일회성 검색 상세 정보를 구성한 후 다음 단계는 입니다 경보에 대한 LogRhythm 추가 옵션.

경보에 대한 **LogRhythm** 추가 옵션

LogRhythm 엔터프라이즈 통합을 사용하면 보안 인시던트에 따라 경보를 LogRhythm 자동으로 업데이트하거나 종결할 수 있습니다.

시작하기 전에

필요한 역할: sn_si.analyst

이 태스크 정보

경보 초기 업데이트 옵션을 활성화하면 경보가 LogRhythm 주석에서 초기 경보 업데이트와 함께 자동으로 업데이트됩니다. 마찬가지로 경보 종결 업데이트 옵션을 활성화하면 경보가 SIR 종결 코드 및 종결 주석과 함께 LogRhythm에서 자동으로 종결됩니다.

LogRhythm 경보 ID는 인시던트의 수명주기 동안 보안 인시던트 ID에 ServiceNow AI Platform 연결됩니다. 이 상관관계를 통해 동시에 자동화된 보안 인시던트/경보 종결이 발생할 수 있습니다. (SIR) 보안 인시던트 기록이 보안 인시던트 응답 종결되면 웹 콘솔의 경보에 설명이 게시됩니다LogRhythm. 이 설명은 보안 인시던트의 종결 ServiceNow AI Platform 에 따라 경보가 종결되었음을 나타냅니다. 인시던트 번호와 참조를 위해 보안 인시던트로 다시 연결되는 URL도 경보의 LogRhythm 설명 섹션에 포함됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 진행률 표시줄에서 추가 옵션 단계를 클릭합니다.
2. SIR 인시던트 생성에 자동화된 경보 업데이트를 사용하려면 다음 옵션 중에서 선택하여 경보 검색을 구성합니다.
3. SIR 인시던트 종결에 자동화된 경보 업데이트를 사용하려면 다음 옵션 중에서 선택하여 경보 검색을 구성합니다.
4. 마침을 클릭하여 경보 프로파일을 저장합니다.

Trouble?
보안 인시던트에서 경보가 성공적으로 종결되었음을 나타내는 메모가 표시되지 않으면 작업 메모에서 문제 해결 방법에 대한 자세한 내용을 검토하십시오. 또한 서버 연결을 확인하십시오. 보안 인시던트가 ServiceNow AI Platform 종결되었고 서버 시간이 초과되지 않은 것을 확인하면 웹 콘솔에서 수동으로 경보를 닫아야 할 수도 있습니다 LogRhythm .

통합을 위한 **LogRhythm** 추가 구성

LogRhythm 통합 설정을 사용하여 사전 설정 시스템 및 문제 해결 속성을 요구 사항에 따라 수정합니다.

시작하기 전에
필요한 역할: sn_si.admin

프로시저

1. 다음으로 이동 모두 〉 **LogRhythm** 통합 〉 **LogRhythm** 통합 설정.
2. 요구 사항에 따라 시스템 속성을 구성합니다.
3. 양식에서 필드를 채웁니다.

LogRhythm 통합 시스템 속성

필드	설명
데이터가 ServiceNow 테이블에 저장되기 전에 필터가 적용됩니다.	데이터가 ServiceNow 테이블에 저장되기 전에 필터를 적용할지 여부를 결정하는 옵션입니다. 기본적으로 값은 예로 설정됩니다.
하루에 최대 보안 인시던트를 작성할 수 있습니다.	하루에 만들 수 있는 최대 보안 인시던트 수를 정의하는 옵션입니다. 기본적으로 이 값은 2000으로 설정됩니다.
LogRhythm 주기적 수집은 1000+ 경보일 수 있으므로 페이지 매김은 경보를 수집하는 데 사용됩니다. 페이지당 경보의 수를 가져올 수 있는 페이지당 제한입니다.	단일 페이지에서 검색할 최대 경보 수를 정의하는 옵션입니다. 기본적으로 이 값은 100으로 설정됩니다.
지정된 일수보다 오래된 "작업에 대한 소스" 테이블 기록을 삭제합니다.	지정된 일수가 위반되었을 때 작업 테이블 기록에 대한 소스를 삭제하는 옵션입니다. 기본적으로 이 값은 30으로 설정됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 요구 사항에 따라 문제 해결 속성을 구성합니다.
5. 양식에서 필드를 채웁니다.

LogRhythm 통합 문제 해결 속성

필드	설명
예약된 수집 디버그: 예약된 작업에 의해 수행되는 수집에 대한 디버그 수준 시스템 로그를 사용할 수 있습니다. 에서 경보/드릴다운 로그/이벤트를 LogRhythm끌어오는 동안 예약된 수집에 의해 작성된 모든 메시지/예외를 기록합니다.	예약된 작업에서 수행하는 수집에 대해 디버그 수준 시스템 로그를 활성화하는 옵션입니다. 기본적으로 값은 아니요로 설정됩니다.
변환 맵 디버그: 변환 맵에 대한 디버그 수준 시스템 로그를 활성화합니다. 경보 임포트에서 보안 인시던트를 생성하는 동안 변환 맵에서 생성된 모든 메시지를 기록합니다. 또한 경보 임포트 테이블에서 UI 작업을 활성화하여 변환 맵을 다시 실행했습니다.	변환 맵에 대해 디버그 수준 시스템 로그를 활성화하는 옵션입니다. 기본적으로 값은 아니요로 설정됩니다.
경보 프로파일에서 샘플 수집 디버그: 샘플 수집을 위한 디버그 수준 시스템 로그를 활성화합니다. 이는 샘플이 수집되는 동안 생성된 모든 메시지를 기록합니다.	샘플 수집에 디버그 수준 시스템 로그를 활성화하는 옵션입니다. 기본적으로 값은 아니요로 설정됩니다.
Debug Preview In Alarm Profile(경보 프로파일의 디버그 미리 보기): 알람 프로파일 미리 보기에 대한 디버그 레벨 시스템 로그를 활성화합니다. 샘플 경보에 대해 미리 보기가 렌더링되는 동안 생성된 모든 메시지가 로깅됩니다.	경보 프로파일 미리 보기에 대한 디버그 수준 시스템 로그를 활성화하는 옵션입니다. 기본적으로 값은 아니요로 설정됩니다.
아웃바운드 REST 호출 디버그: 이 속성을 활성화하면 에서 MID Server LogRhythm와 함께 또는 사용하지 않는 모든 REST 호출(요청 및 응답)에 대해 시스템 로그 테이블에 디버그 수준 로깅이 허용됩니다.	에서 MID 서버를 LogRhythm사용하거나 사용하지 않는 모든 REST 호출에 대해 시스템 로그 테이블에서 디버그 수준 로깅을 활성화하는 옵션입니다. 기본적으로 값은 아니요로 설정됩니다.

6. 저장을 클릭합니다.

스크립트 편집기를 사용하여 값 서식 지정 **LogRhythm**

끌어온 경보 값에서 직접 매핑된 필드와 수동으로 입력하는 경보 값 외에도 스크립트 편집기를 사용하여 매핑 단계(선택 사항) 중에 보안 인시던트의 필드 값에 대한 서식을 지정할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.admin

스크립트 편집기는 보안 인시던트의 #### 및 ## 필드에 매핑된 값이 지원되도록 경보 값을 LogRhythm 변경합니다.

이 태스크 정보
경우에 따라 경보 값이 보안 인시던트의 #### 및 ## 필드에 매핑된 경우 LogRhythm 매핑된 값을 편집할 수 있습니다. 경보 값을 LogRhythm 보안 인시던트의 #### 또는 ## 필드에서 지원하는 값으로 변환하려면 스크립트 편집기를 사용합니다.

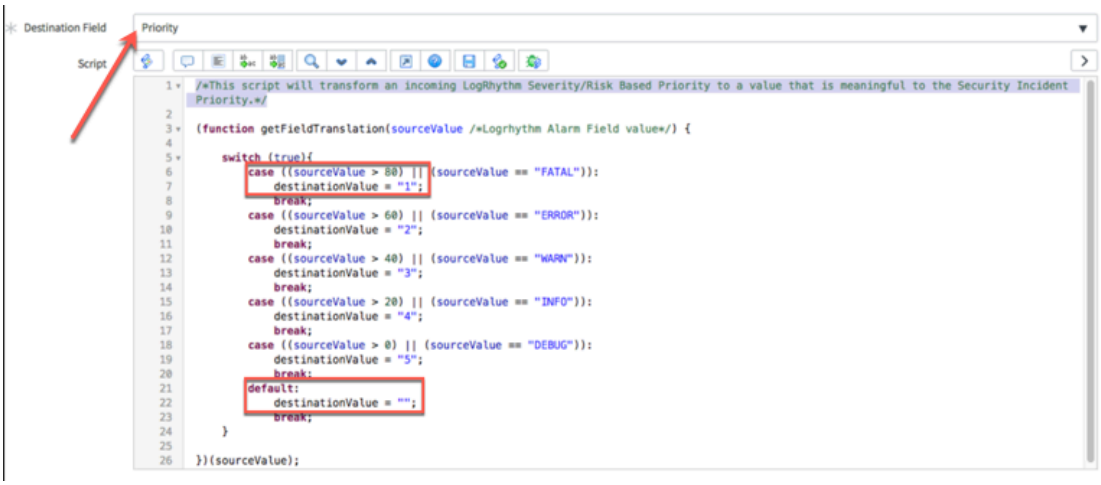
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 매핑 양식이 표시되면 SIR 인시던트 필드 매핑 섹션에서 대괄호 아이콘 [{}] 을 클릭하여 스크립트 편집기를 엽니다.

기본값은 보안 인시던트의 #### 및 ## 필드에 포함됩니다. 이러한 값을 편집할 수 있습니다.

이 예에서는 다음 그림과 같이 열려 있는 편집기에서 대상 필드 선택 목록에 우선 순위가 표시되는지 확인합니다. 이 필드는 위험 기반 우선순위가 아니라 보안 인시던트 우선순위입니다LogRhythm.



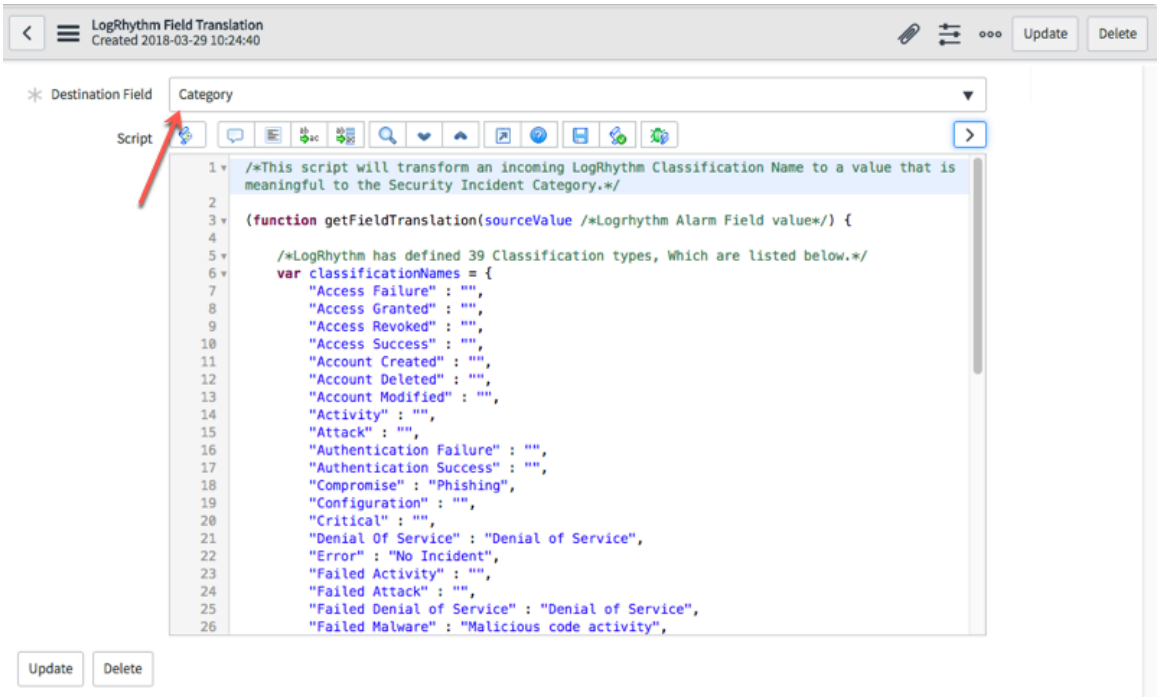
경우에 따라 스크립트 포함이 #### 필드에 적합할 수 있습니다. LogRhythm 예를 들어 경보의 경우 위험 기반 우선순위 점수에는 0-100 사이의 값이 할당됩니다. 그러나 에서 ServiceNow AI Platform보안 인시던트의 우선순위 필드는 1-5 사이의 값을 지원합니다. 앞의 그림에 설명된 것처럼 스크립트 포함은 경보 필드 값을 의 보안 인시던트 ServiceNow AI Platform필드에서 지원하는 적절한 값으로 변환합니다LogRhythm.

필드의 LogRhythm 경우 경보 값이 80 이상이면 보안 인시던트 필드(####)에 1이 표시됩니다. 이 값은 보안 인시던트에서 ## 우선순위로 변환됩니다. 경보에 대한 값이 없으면 보안 인시던트의 필드가 null로 설정됩니다.

2. 변경 내용을 입력하고 업데이트를 클릭하여 변경 내용을 저장합니다.
LogRhythm 필드 번역 테이블이 표시됩니다.
3. 테이블을 닫고 매핑 양식으로 돌아갑니다.

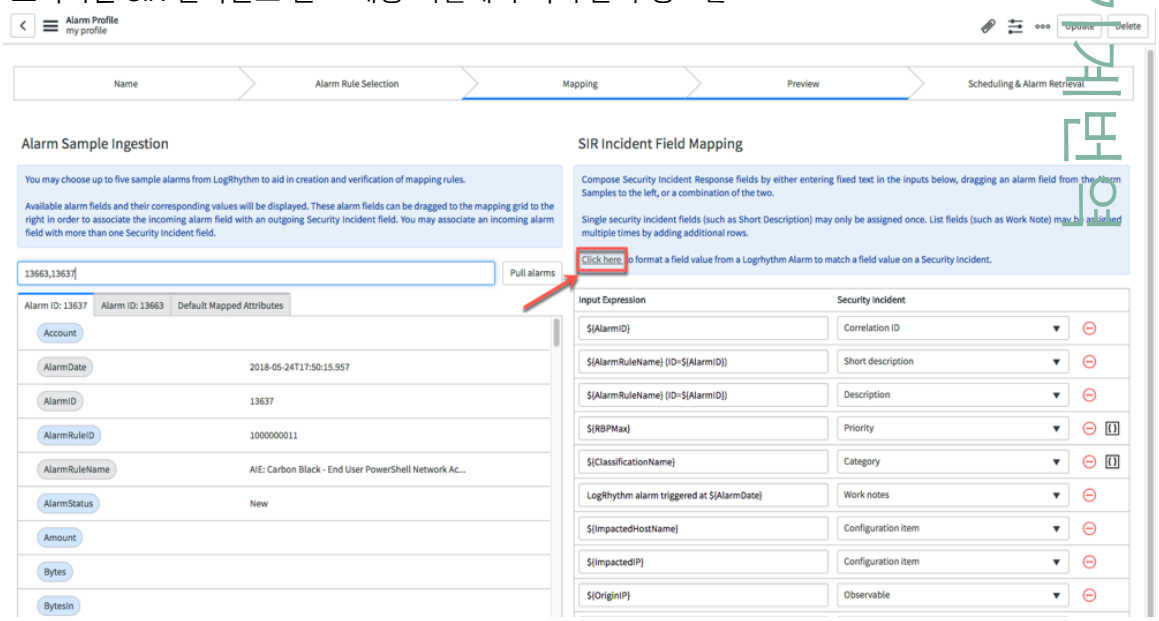
다음 그림은 대상 필드 선택 목록에서 ## 가 선택된 스크립트 편집기를 보여줍니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 필드 번역 목록에 새 필드를 추가하려면 다음 단계에 따라 새 기록을 추가합니다.

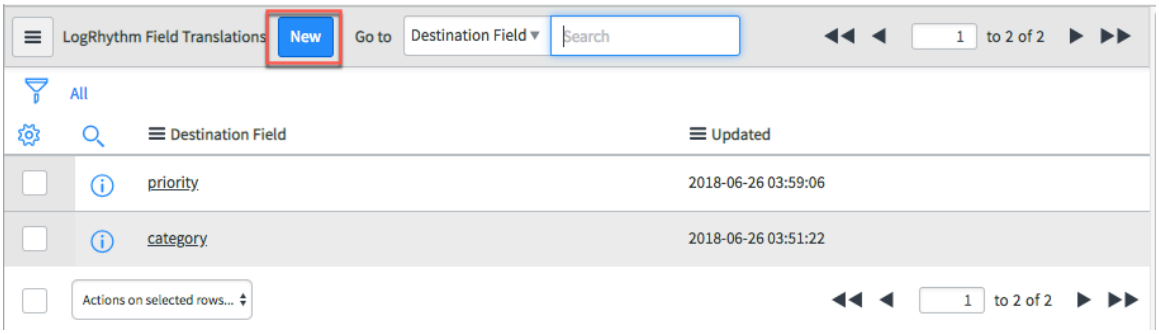
a. 매핑 양식이 표시되면 SIR 인시던트 필드 매핑 섹션에서 여기 클릭 링크를 클릭합니다.



LogRhythm#### 및 ## 대상 필드가 있는 필드 번역 목록이 표시됩니다.

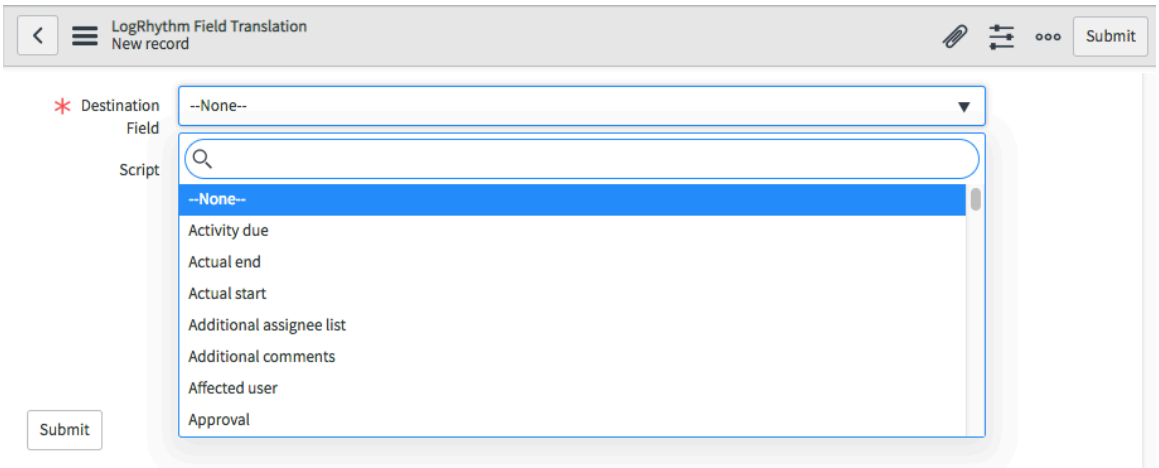
b. 신규를 클릭하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



새 기록이 표시됩니다.

c. 대상 필드 선택 목록에서 스크립팅된 값을 표시할 보안 인시던트의 대상 필드를 선택합니다.



d. 제출을 클릭합니다.
스크립트 편집기가 표시됩니다.

e. 편집기에 변경 내용을 입력하고 제출 을 클릭하여 변경 내용을 저장합니다.
새 기록이 LogRhythm 있는 필드 번역 테이블이 표시됩니다.

5. 테이블을 닫고 매핑 양식으로 돌아갑니다.

에 대한 경보 프로파일 복사 **LogRhythm**

새 경보 프로파일을 생성하는 대신 기존 프로파일 및 관련 설정을 복사합니다. 서로 다른 유형의 알람에 대해 여러 경보 프로필을 만들고 기존 프로필의 설정을 다시 사용하려는 경우 경고 프로필을 복사하여 시간을 절약할 수 있습니다. 이 프로세스는 선택 사항입니다.

시작하기 전에
필요한 역할: sn_si.admin

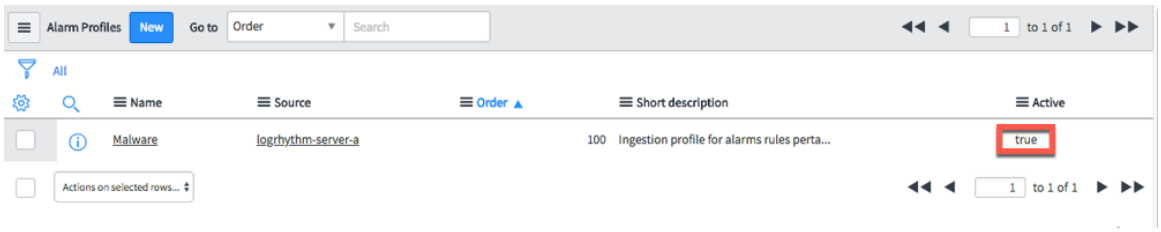
이 태스크 정보
프로파일을 복사하는 경우 프로파일 중복을 방지하기 위해 처음에 프로파일 이름이 수정됩니다. 또한 복사된 프로파일은 비활성으로 설정되므로 구성을 완료하기 전에 실수로 활성화되지 않습니다.

프로시저

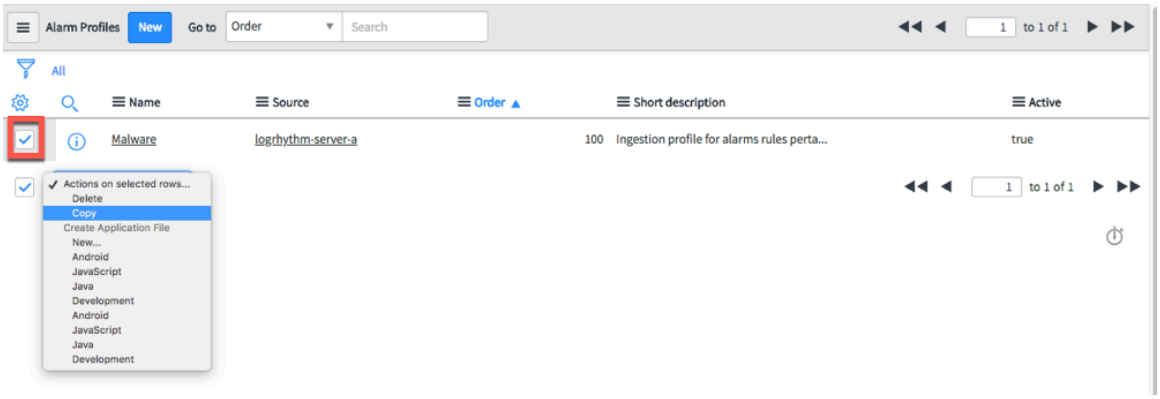
1. 다음으로 이동 모두 〉 **LogRhythm** 통합 〉 **LogRhythm** 경보 프로파일.

표시되는 목록에서 ## 열은 프로파일이 활성 상태(true)인지 여부를 나타냅니다.

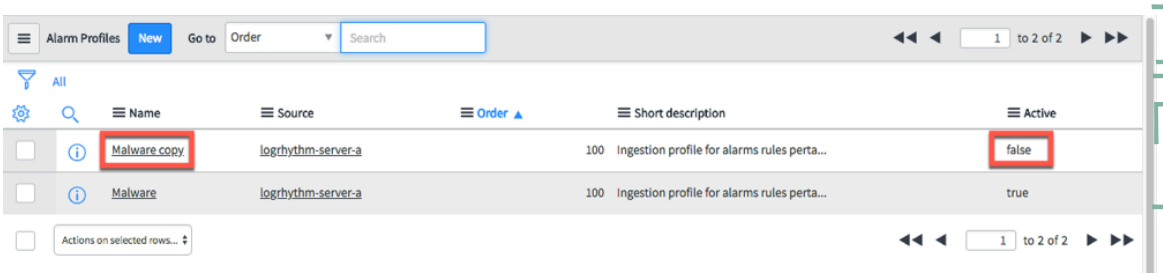
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



2. 이름 열 왼쪽에 있는 필드에서 기록의 이름을 선택합니다.
3. 선택한 행 선택 목록에 대한 작업 목록에서 복사를 선택합니다.



경보 프로파일 목록에 복사본과 원본 프로파일이 모두 표시됩니다. 원본 레코드는 활성 상태이지만 이 시점에서 복사본은 비활성 상태입니다(false). 구성한 후 이 복사된 프로파일을 활성화합니다.



복사된 프로파일의 값을 편집하고 이름을 변경하여 끌어온 경보 규칙이 새 프로파일에 적용되도록 할 수 있습니다. 구성 단계가 완료되면 새 프로파일을 활성화하라는 메시지가 표시됩니다.

에 대한 자동 경보 종결 비활성화 **LogRhythm**

웹 콘솔에서 보안 인시던트 종결 정보를 더 이상 확인하지 않으려면 자동 경보 종결 기능을 비활성화합니다 LogRhythm . 비활성화되면 더 ServiceNow AI Platform 이상 웹 콘솔 내에서 경보를 LogRhythm 닫지 않습니다. 이 프로세스는 선택 사항입니다.

시작하기 전에

필요한 역할: sn_si.admin

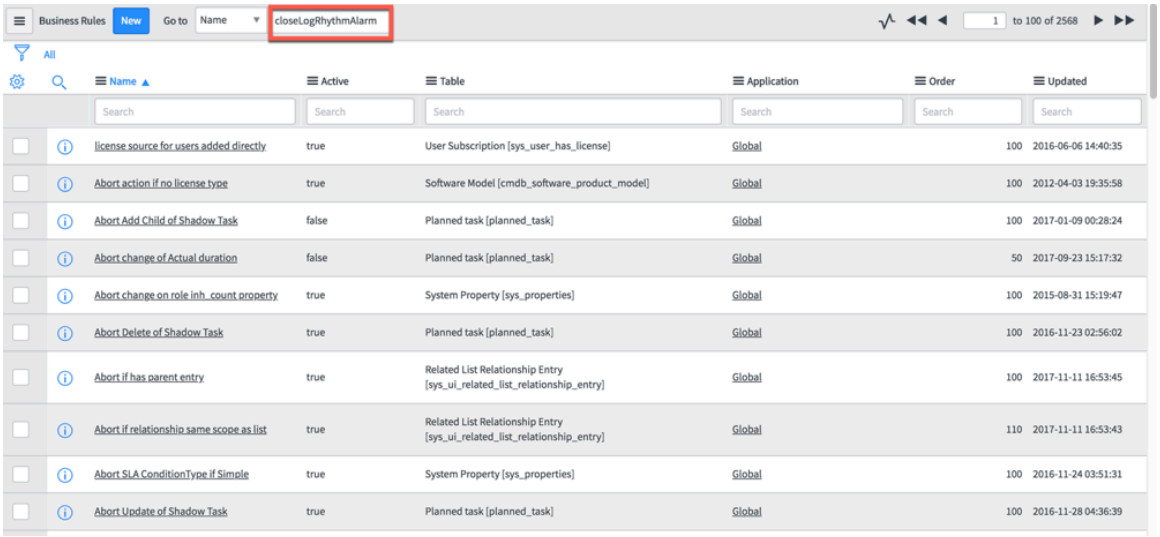
이 태스크 정보

비활성화되면 보안 인시던트에 대한 상태 메모 및 기타 종결 정보가 더 이상 웹 콘솔에 표시되지 LogRhythm 않습니다.

프로시저

1. 다음으로 이동 모두 〉 시스템 정의 〉 비즈니스 규칙 을 클릭하고 비즈니스 규칙 모듈을 선택합니다.
2. 비즈니스 규칙 목록에 표시되지 않으면 검색 필드에 **LogRhythm Close Alarm On SI Closure**를 입력하고 **Enter** 키를 누릅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



3. 이름 열에서 **LogRhythm Close Alarm On SI Closure** 링크를 클릭하여 레코드를 엽니다.
4. 표시되는 기록에서 활성 확인란의 선택을 취소합니다.
5. 업데이트를 클릭합니다.
   이제 자동 경보 종결 기능이 비활성화되었습니다.

드릴다운 이벤트 보기 **LogRhythm**

보안 인시던트의 경보에 대한 LogRhythm 관련 원시 또는 기본 이벤트를 봅니다.

시작하기 전에

필요한 역할: sn_si.admin

이 태스크 정보

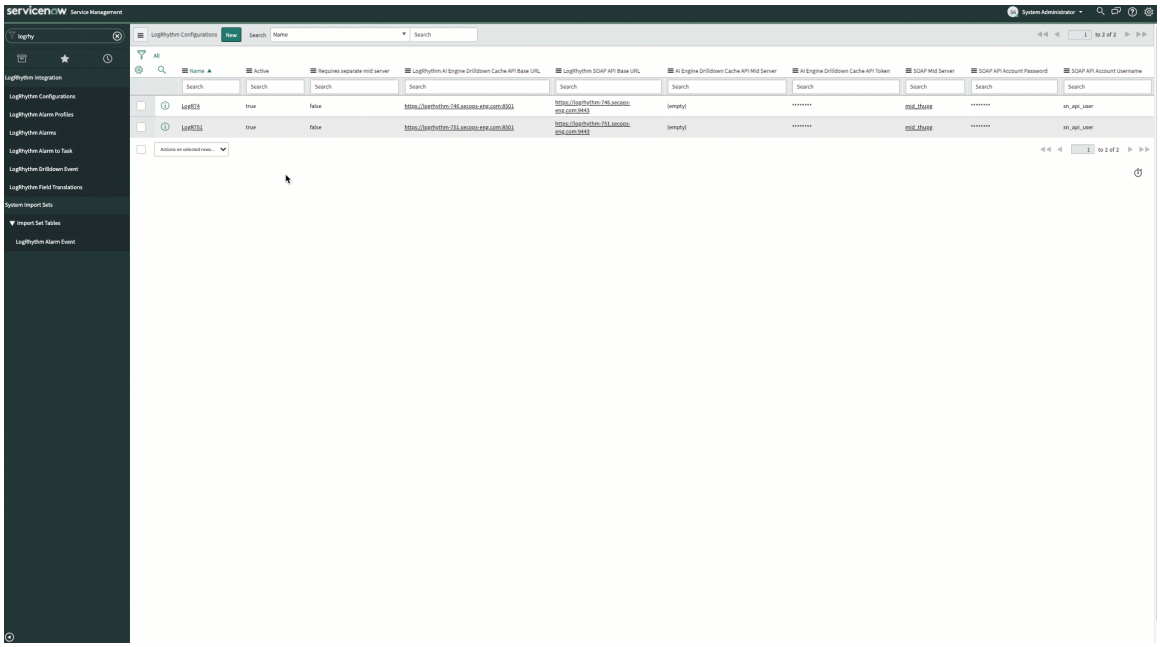
보안 분석가는 콘솔로 돌아가지 않고도 경보에 대한 LogRhythm 관련 원시 또는 기본 이벤트를 볼 수 있습니다 LogRhythm . 인시던트에 대한 SIR 모든 드릴다운 이벤트가 포함된 관련 목록으로 이동하여 이 작업을 수행할 수 있습니다.

프로시저

다음으로 이동 모두 〉 **LogRhythm** 통합 〉 **LogRhythm** 드릴다운 이벤트.

다음 그림에서는 **LogRhythm** 드릴다운 이벤트 모듈로 이동하여 이벤트 목록을 경보 ID별로 그룹화별로 정렬하고 연결된 보안 인시던트를 클릭하는 방법을 보여줍니다. 보안 인시던트의 관련 링크에서 **LogRhythm** 드릴다운 이벤트 탭을 찾을 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



LogRhythm 통합 문제 해결

연결 및 경보 수집 문제를 해결합니다.

문제 해결을 위해 다음 항목을 참조하십시오.

- 에 대한 연결 확인 LogRhythm
- 에 대한 스크립트 실행 및 시스템 로그 LogRhythm

에 대한 연결 확인 **LogRhythm**

REST API를 LogRhythm 테스트 LogRhythm 하기 위해 curl 요청을 전송하여 클라이언트 콘솔에 대한 연결을 확인합니다. 확인 프로세스는 선택 사항입니다.

시작하기 전에
필요한 역할: sn_si.admin

이 태스크 정보
REST API를 설정한 LogRhythm 후 클라이언트 콘솔에 대한 연결이 LogRhythm 제대로 작동하는지 확인하려면 에서 플러그인 설치 및 구성 LogRhythm구성한 MID 서버를 호스팅하는 컴퓨터에서 두 개의 curl 요청을 보냅니다.

REST API는 LogRhythm 인증에 WSSE를 사용하므로 Curl 및 Postman과 함께 작동하려면 일부 외부 스크립팅이 필요합니다.

REST API는 LogRhythm 인증을 위해 토큰을 사용하므로 통합에서 사용하는 실제 확인 호출을 수행할 수 있습니다. URL 끝에 있는 "0"은 알람 ID입니다 LogRhythm . LogRhythm 기본 구성의 REST API에는 포트 8501이 필요합니다. 이 포트 번호는 테스트에 사용하려는 URL에 포함되어야 합니다.

프로시저

다음 curl 요청에서 URL **<LogRhythm REST url>** 및 토큰 **<api** 토큰**>** 을 업데이트하고 REST API의 LogRhythm 유효성을 검사하도록 보냅니다. curl -k -i -v --trace-time -o /dev/null -H "Content-Type: text/json" -H "Authorization: Bearer <api token>" "https://<cache drilldown url>/lr-drilldown-cache-api/drilldown/0"

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

REST API에 LogRhythm 성공적으로 연결하려면 HTTP 404를 수신해야 하지만 응답 본문에는 Alarm ID: 0 not found가 포함됩니다.

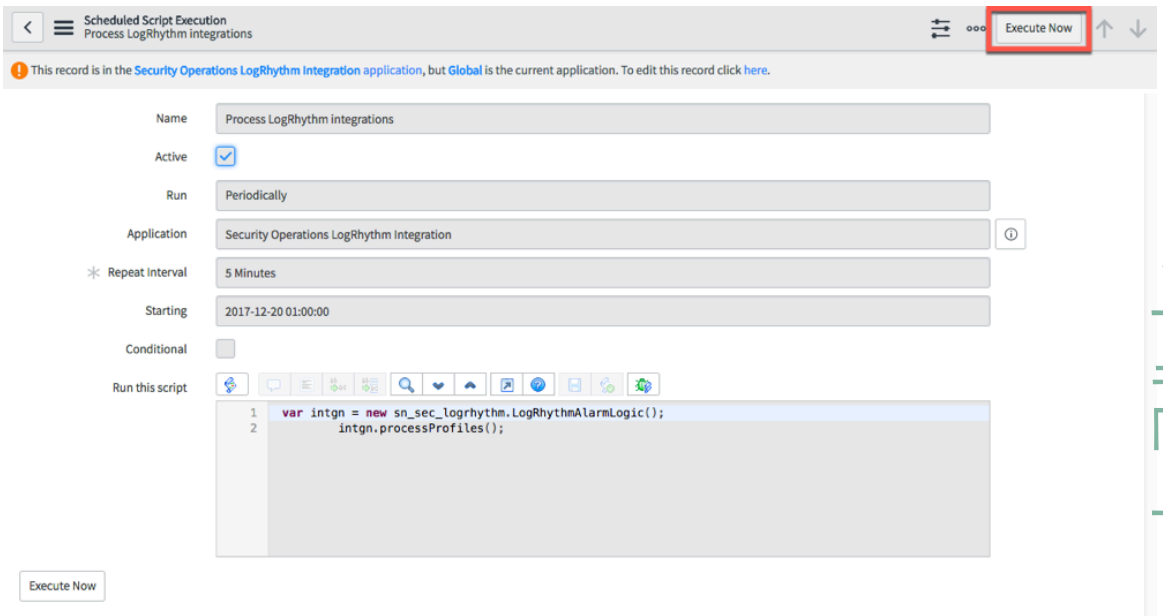
스크립트 실행 및 시스템 로그

경보 수집 문제를 해결하는 경우 기본 5분 폴링 간격을 재정의하여 결과를 즉시 볼 수 있습니다. 이 시나리오에서는 스크립트 실행을 수동으로 호출하여 폴링을 실행합니다. 이 실행은 선택 사항입니다.

시작하기 전에
필요한 역할: sn_si.admin

프로시저

1. 다음으로 이동 모두 〉 예약된 작업 〉 예약된 작업 을 클릭하고 예약된 작업 모듈을 선택합니다.
2. 프로세스 LogRhythm 통합 작업 기록을 클릭합니다.
3. 표시되는 예약된 스크립트 실행 기록에서 지금 실행을 클릭합니다.



더 많은 문제 해결 도움이 필요한 경우 시스템 로그에서 쿼리를 확인할 수 있습니다 LogRhythm .

4. 다른 일반적인 문제 해결 문제의 경우 다음 단계에 따라 시스템 로그에 액세스합니다.

   a. 다음으로 이동 시스템 로그 〉 모두 을 클릭하고 모두를 선택합니다.

   b. 필터(##)를 소스 로 설정하고 sn_sec_logrhythm 입력합니다.

   c. **Enter** 키를 누릅니다.
   통합에 의해 생성된 모든 메시지가 이 테이블에 표시됩니다. 나열된 메시지는 통합의 실행 프로세스에 대한 인사이트를 제공할 수 있으며 추가 문제 해결에 도움이 될 수 있습니다.

McAfee ePO 통합

SOC(보안 운영 센터) 분석가가 McAfee ePO 사이버 위협을 식별하고 악성 파일로 인한 피해를 복구하는 데 도움이 되는 통합 엔드포인트 탐지 및 대응(EDR) 기능입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

개요

이 통합에 사용되는 두 가지 McAfee ePO 기능 집합, 즉 호스트 격리 및 맬웨어 검사 시작과 같은 작업을 호출하는 기능과 쿼리를 실행하여 시스템 상세 정보 및 위협 이벤트를 수집하는 기능이 있습니다. 작업 및 쿼리와 같은 기능 유형은 모두 인스턴스에서 호출 ServiceNow AI Platform# 됩니다. 특정 유형의 보안 이벤트가 발생할 때 자동으로 실행하도록 이러한 기능을 그룹화하거나 보안 인시던트에서 ServiceNow AI Platform# 수동으로 호출할 수 있습니다.

이 통합에 사용할 수 있는 기능은 다음과 같습니다 McAfee ePO .

시스템 상세 정보 가져오기
: 운영 체제 상세 정보를 포함하여 시스템 상세 정보를 수집합니다.

맬웨어 검사 시작
: 스캔 구성 및 일정에 따라 영향을 받는 엔드포인트의 스캔을 시작합니다.

호스트 격리/격리 해제
: 조사를 위해 네트워크 액세스에서 시스템을 제거하고 네트워크 액세스를 복원합니다.

위협 이벤트 나열
: 규정 준수 상태 및 최신 위협 이벤트를 수집합니다.

주요 기능

이 통합에는 다음과 같은 주요 기능이 포함됩니다.

- 인시던트 조건에 따라 쿼리가 McAfee ePO 자동으로 트리거되는 것을 지원합니다.
- 요청 시 작업을 수행하는 (SIR) 보안 인시던트에서 ServiceNow AI Platform# 보안 인시던트 응답 수동으로 기능을 시작할 McAfee ePO 수 있습니다.
- 다양한 유형과 역량을 McAfee ePOServiceNow AI Platform# 보안 운영 트리거하기 위해 여러 프로필을 생성할 수 있는 유연성. 이러한 프로파일은 위협 이벤트 정보를 수집하거나 멀웨어와 같은 특정 인시던트 범주의 조건에 따라 작업을 수행합니다.
- 보안 인시던트 결과 SIR 의 McAfee ePO 미리 보기를 사용하여 프로파일 구성의 유효성을 검사합니다.
- 태그 지정을 사용하는 경우 보안 태그는 워크플로우에서 처음 시작하는 기능과 쿼리 또는 작업이 성공적으로 완료된 시기를 식별합니다 McAfee ePO .
- 쿼리 및 작업에 대한 McAfee ePO 전체 감사 추적이 보안 인시던트에 대한 SIR 작업 메모에 게시되고 의 ServiceNow AI Platform# 명령이 콘솔에 기록됩니다 McAfee ePO .
- 여러 McAfee ePO 콘솔을 지원합니다.

ServiceNow 플러그인

com.snc.si_dep 플러그인이 필요합니다. 이 플러그인은 제품을 지원하는 데 필요한 모든 종속성을 보안 인시던트 응답 자동으로 설치합니다. 다른 보안 운영 애플리케이션을 설치 및 활성화하기 전에 이 플러그인을 설치하고 활성화하십시오.

에서 ServiceNow Store다음 보안 운영 애플리케이션을 설치하고 활성화해야 합니다. 원활한 설치를 위해 아래 나열된 순서대로 한 번에 하나의 애플리케이션을 설치하고 활성화합니다.

1. 보안 통합 프레임워크
2. Security Support Common
3. 보안 지원 오케스트레이션

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 보안 인시던트 응답
5. 보안 인시던트 응답 작업 공간

통합을 위한 인스턴스 설정에 ServiceNow AI Platform 대한 자세한 내용은 다음 문서를 ServiceNow AI Platform 통합을 위한 McAfee ePO 인스턴스 설정참조하십시오.

확장 **ServiceNow** 플러그인

이 통합에는 McAfee ePO용 ServiceNow 보안 운영 확장# 플러그인이 필요합니다. 콘솔에 이 ServiceNow 플러그인을 McAfee ePO 설치합니다. 자세한 내용은 ServiceNow AI Platform 통합을 위한 McAfee ePO 인스턴스 설정 문서를 참조하십시오.

MID 서버

이 통합을 수행하려면 인스턴스에 MID 서버가 설치 및 구성되어 있어야 서버(콘솔)에 McAfee ePO 연결할 수 ServiceNow AI Platform# 있습니다. MID Server에 대한 자세한 내용은 ServiceNow 제품 설명서 웹 사이트를 참조하십시오.

지원되는 **McAfee** 버전

통합은 의 버전 5.9.1 및 5.10 McAfee ePO을 지원합니다. McAfee Agent: MA 5.5.1.388을 지원합니다. McAfee 제품 및 ePolicy Orchestrator에 대한 자세한 내용은 McAfee 제품 웹 사이트를 참조하십시오.

통합은 McAfee Endpoint Security Threat Prevention 제품의 버전 10.5를 지원합니다. 버전 10.5를 실행 중이 아니라면 관리자에게 문의하여 McAfee ePO 사용 중인 버전이 태그 작업을 통한 요청 시 스캔을 지원할 수 있는지 확인하십시오.

McAfee ePO 보안 태그가 이 통합에 사용됩니다. 콘솔에서 이러한 태그를 생성해야 합니다 McAfee ePO . 이러한 태그에 대한 자세한 내용은 다음 문서를 참조하십시오 McAfee ePO(SIR)과 보안 인시던트 응답 통합하도록 콘솔 설정.

참조

참조	문서 식별자	문서 제목
1	McAfee 제품 웹 사이트	McAfee 제품 웹 사이트
2	ePolicy Orchestrator Cloud용 McAfee 비즈니스 제품 설명서	McAfee 제품 설명서
3	ServiceNow 제품 설명서 웹 사이트	ServiceNow 제품 설명서 웹 사이트

통합 결과 설정, 설치 및 확인 진행률을 추적하는 검사 목록은 문서를 참조하십시오 통합을 위한 McAfee ePO 검사 목록.

애플리케이션을 원활하게 설치하고 예상 결과를 확인하려면 항목을 제시된 순서대로 따르십시오.

관련 정보

용 통합 아키텍처 McAfee ePO

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

용 통합 아키텍처 **McAfee ePO**

다음 항목은 시스템 아키텍처에 대한 개요이며 통합의 주요 기능을 나열합니다. 또한 이 섹션에서는 에서 응용프로그램ServiceNow Store을 설치하기 전에 인스턴스 ServiceNow AI Platform 및 McAfee ePolicy Orchestrator()McAfee ePO 콘솔에서 완료해야 하는 설정 단계에 대한 정보도 제공합니다.

통합의 **McAfee ePO** 주요 용어

다음 용어는 통합을 위한 설치 및 구성 설명서 전체에서 사용됩니다.

ServiceNow AI Platform

엔터프라이즈 ServiceNow 제품입니다. ServiceNow AI Platform 는 (),SIR ITSM(IT Service Management) 및 기타 제품과 같은 보안 인시던트 응답 개별 구성요소가 빌드되는 기반입니다.

보안 인시던트 응답(SIR)

ServiceNow AI Platform 검색 및 초기 분석부터 방지, 근절 및 복구를 거쳐 최종 사후 인시던트 검토 및 종결에 이르는 보안 인시던트의 진행 상황을 추적하는 애플리케이션입니다.

플러그인

플러그인은 인스턴스 내에서 특정 기능 및 기능성을 제공하는 소프트웨어 구성요소입니다 ServiceNow AI Platform . 통합 플러그인의 설치 및 구성에 대한 자세한 내용은 문서를 참조하십시오 애플리케이션 설치 및 통합을 위한 McAfee ePO 서버 구성.

ePolicy Orchestrator(McAfee ePO)

McAfee 서비스, 제품 및 설정을 관리하는 사용자 콘솔입니다.

McAfee 확장 플러그인

이 통합에는 이 ServiceNow 확장 플러그인이 필요합니다. 이 플러그인은 콘솔에 있으며 McAfee ePO 콘솔을 McAfee ePOServiceNow AI Platform 인스턴스에 연결합니다.

역량

인스턴스에서 시작되는 ServiceNow AI Platform 자동 활동으로, 강화 쿼리를 수행하고 자산에 대한 작업을 수행하기 위해 콘솔에서 실행됩니다 McAfee ePO .

프로필

역량이 강화 쿼리를 수행하고 자산에 대한 작업을 수행하는 시기와 조건을 지정하기 위해 구성하는 역량에 대한 McAfee ePO 설정입니다.

MID 서버

외부 애플리케이션, 데이터 소스 및 서비스 간의 ServiceNow AI Platform 데이터 이동과 통신을 용이하게 하는 애플리케이션입니다.

ServiceNow 관리자(admin)

이 역할이 있는 사용자가 AND McAfee ePO 플러그인을 ServiceNow AI Platform 다운로드하여 인스턴스에 설치합니다SIR. 또한 이 역할을 가진 사용자는 필요에 따라 보안 인시던트 관리자 역할도 할당합니다.

ServiceNow 보안 인시던트 관리자(sn_si.admin)

이 역할을 가진 사용자는 필요에 따라 인스턴스의 (SIR) 제품 ServiceNow AI Platform 과의 보안 인시던트 응답 통합 구성을 McAfee ePO 수행합니다. 이 역할을 가진 사용자는 필요에 따라 보안 인시던트 분석가 역할도 할당합니다.

ServiceNow 보안 인시던트 분석가(sn_si.analyst)

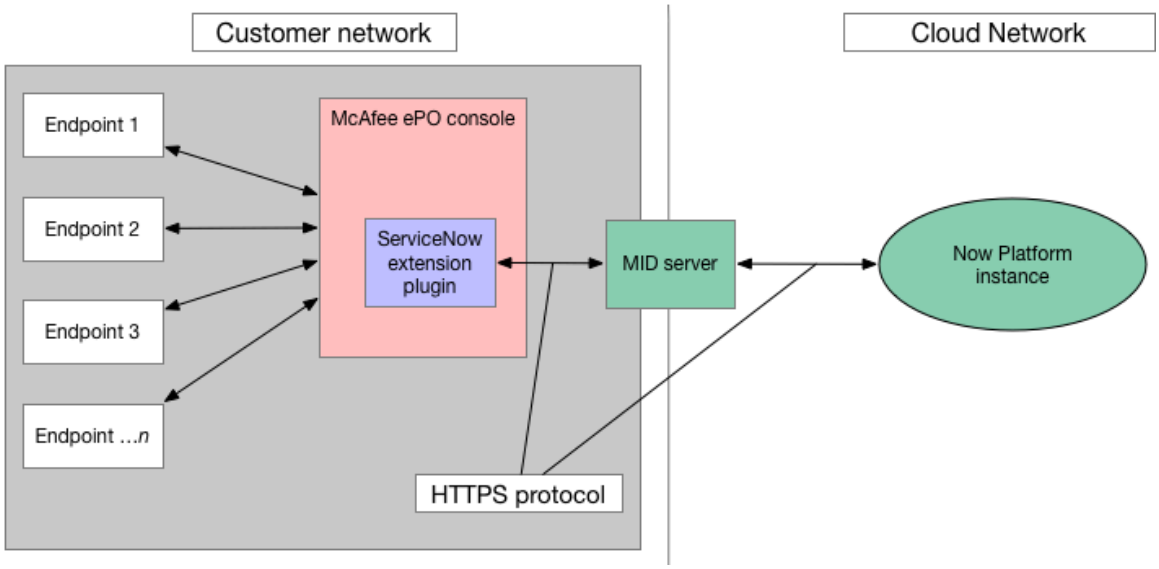
이 역할을 가진 사용자는 SIR 제품의 보안 인시던트와 상호작용하고 이를 분석합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시스템 연결 및 데이터 흐름

다음 그림은 고객 환경의 예입니다. ServiceNow AI Platform 인스턴스가 확장 플러그인을 통해 ServiceNow 서버(콘솔)에 McAfee ePO 연결할 수 있도록 MID ServiceNow AI Platform 서버가 필요합니다. 연결되면 사용자의 ServiceNow AI Platform 기능을 호출하여 멀웨어 스캔을 시작하고, 호스트 시스템을 격리 및 네트워크로 복원하고, 마지막 스캔 결과를 검색하고, 자산에 대한 시스템 상세 정보를 수집할 수 있습니다. 이러한 역량이 검색 기준과 일치하는 자산에서 결과를 반환하면 MID Server를 통해 데이터를 인스턴스로 ServiceNow AI Platform 끌어옵니다. 데이터는 (SIR) 보안 인시던트의 ServiceNow AI Platform 보안 인시던트 응답 관련 목록에 표시됩니다. 다음 그림에서는 하나의 McAfee ePO 콘솔에서 관리되는 한 엔드포인트 그룹에 대한 데이터 흐름을 보여 줍니다.

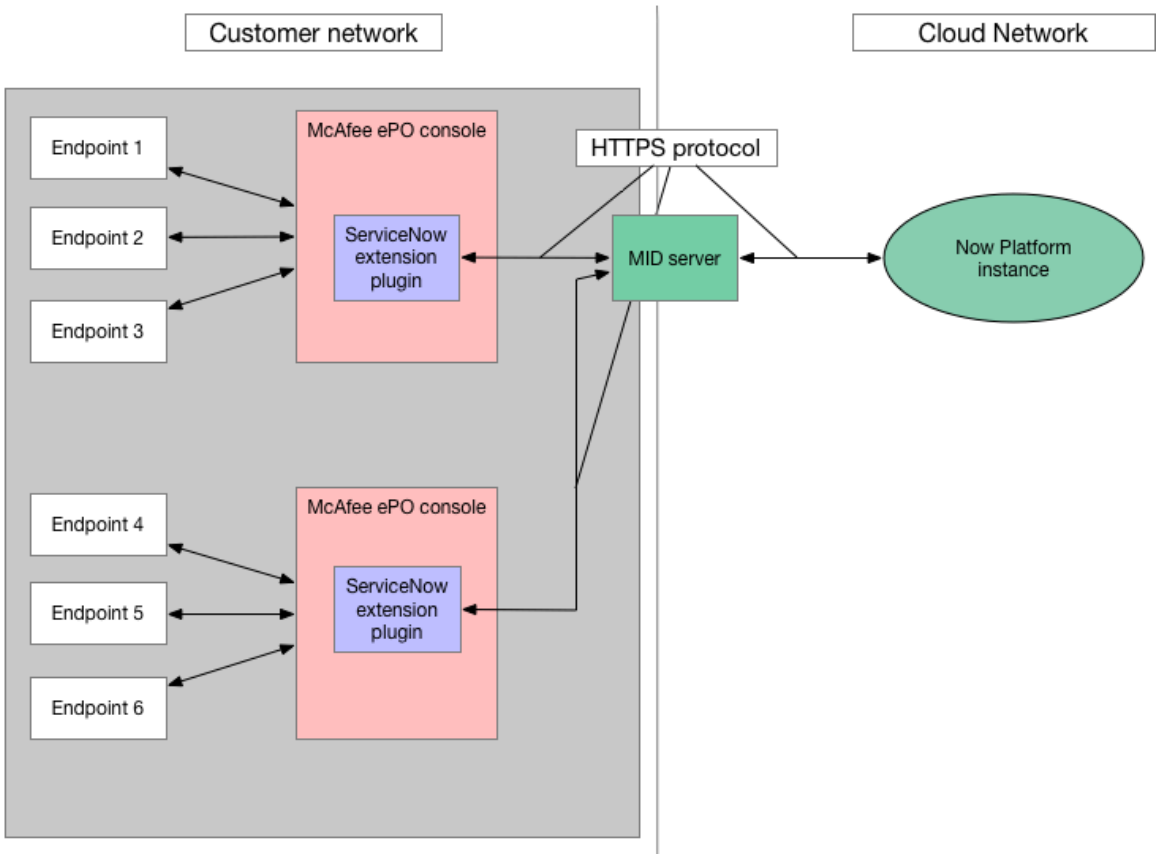
단일 엔드포인트 구성



다음 그림과 같이 이 통합은 둘 McAfee ePO 이상의 콘솔을 지원할 수 있습니다. 한 McAfee ePO 콘솔에서 관리하는 엔드포인트 그룹과 다른 McAfee ePO 콘솔에서 관리하는 다른 엔드포인트 그룹을 가질 수 있습니다. 여러 McAfee ePO 콘솔의 데이터가 단일 MID Server를 통해 끌어와집니다. 그러나 조직에서 필요로 할 경우 여러 MID Server를 구성하는 것을 선호할 수도 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

MID 서버 구성



통합을 위한 **McAfee ePO** 워크플로우

이 통합에는 다음 워크플로우가 포함됩니다. 이러한 워크플로우는 사전 구성되어 있으며 이 통합을 위해 특별히 설계되었습니다. 필요에 따라 이러한 워크플로우를 조직의 필요에 맞게 편집할 수 있습니다. 워크플로 및 워크플로 편집기 사용에 대한 자세한 내용은 워크플로 시작을 참조하세요.

- 보안 운영 McAfee EPO 통합 - 호스트 상세 정보 가져오기
- 보안 운영 McAfee EPO 통합 - 맬웨어 검색 시작
- 보안 운영 McAfee EPO 통합 - 호스트 격리
- 보안 운영 McAfee EPO 통합 - 위협 이벤트 나열
- 보안 운영 McAfee EPO 통합 - 격리 제거

외부 시스템 연결

통합하려면 MID 서버가 HTTPS 프로토콜 연결을 통해 콘솔과 McAfee ePO 통신해야 합니다.

통합을 위한 **McAfee ePO** 검사 목록

이 검사 목록을 사용하여 통합의 모든 작업을 안내합니다. 다음 검사 목록에는 설정 및 설치 작업과 통합에 대한 예상 결과를 포함하는 사용 사례의 예가 포함되어 있습니다.

시작하기 전에

필요한 역할: 각 단계에 대한 역할이 나열됩니다.

이 태스크 정보

다음 표를 사용하여 통합의 설정, 설치 및 구성으로 진행 상황을 추적합니다. 다음 단계로 이동하기 전에 단계에 대한 모든 작업을 완료합니다. 테이블의 각 행은 작업을 나열하고 작업을 수행하는 데 필요한 역할을 식별합니다. 설치 및 구성 안내서의 번호가 매겨진 주제도 참조됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

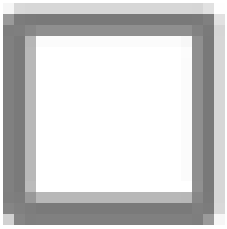
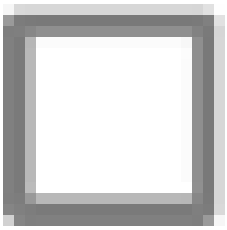
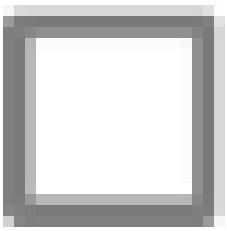
프로시저

표의 단계를 제시된 순서대로 따릅니다.

검사 목록

항목	설명
☐	관리자 역할이 있는 ServiceNow AI Platform# 사용자가 인스턴스를 설정합니다 ServiceNow AI Platform# . **a.** 및 보안 인시던트 응답 역할을 할당합니다ServiceNow AI Platform#. **b.** 통합을 지원하는 모든 ServiceNow 보안 인시던트 응답 플러그인과 해당 릴리스 ServiceNow AI Platform에 대해 활성화되어 있는지 확인합니다. **c.** 인스턴스에 MID Server ServiceNow AI Platform# 를 설치하고 구성합니다. **d.** 호스트 격리 및 맬웨어 검사 작업 시작을 위해 보안 인시던트 분석가가 제출한 요청을 처리하려면 승인 그룹을 생성합니다. 자세한 내용은 ServiceNow AI Platform 통합을 위한 McAfee ePO 인스턴스 설정 문서를 참조하십시오.
☐	관리자 자격으로 McAfee ePO 콘솔을 설정합니다 McAfee ePO . **a.** 의 버전 5.9 McAfee ePO를 사용하고 있는지 확인합니다. **b.** ServiceNow 콘솔에 확장 플러그인을 McAfee ePO 설치합니다. **c.** 호스트 격리 및 맬웨어 검사 작업 시작에 대한 콘솔에 보안 태그를 McAfee ePO 생성했는지 확인합니다. 자세한 내용은 McAfee ePO(SIR)과 보안 인시던트 응답 통합하도록 콘솔 설정 문서를 참조하십시오. 자세한 내용을 확인하고 확장 플러그인 파일을 ServiceNow AI Platform 가져오려면 인스턴스에서 지식 〉 문서 〉 모두 그리고 검색 필드에 ServiceNow Security Operations Extension for McAfee ePO# 입력합니다.
☐	관리자 역할이 있는 ServiceNow AI Platform 사용자는 에서 ServiceNow Store애플리케이션을 설치하고 McAfee ePO 서버를 구성한 다음 콘솔에 연결합니다McAfee ePO. 자세한 내용은 애플리케이션 설치 및 통합을 위한 McAfee ePO 서버 구성 문서를 참조하십시오.
☐	보안 인시던트 관리자 역할이 있는 ServiceNow AI Platform 사용자는 인스턴스에서 보안 태그 이름을 ServiceNow AI Platform# 편집하여 콘솔에서 생성한 McAfee ePO 태그 이름과 일치하도록 합니다. 자세한 내용은 통합을 위해 McAfee ePO 에서 ServiceNow AI Platform 보안 태그 편집 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

항목	설명
	보안 인시던트 관리자 역할의 사용자가 역량에 대한 McAfee ePO 프로파일을 생성합니다. 프로파일에 대한 자세한 내용은 을 참조하십시오 McAfee ePO 통합 역량 프로파일. 프로파일을 만드는 데 필요한 단계는 문서를 참조하십시오 역량 프로파일 생성.
	보안 인시던트 관리자 역할의 사용자가 프로파일을 구성하고 보안 인시던트를 테스트합니다. **a.** 트리거 조건 및 설정에 대한 정보를 검토합니다. **b.** 프로파일을 구성합니다. **c.** 보안 인시던트를 테스트하고 미리 봅니다. **d.** 보안 인시던트의 관련 목록에서 검색 결과 및 기타 상세 정보를 찾습니다. **e.** 다양한 유형의 프로파일을 생성 및 구성하고 각 유형에 대한 보안 인시던트를 테스트합니다. 트리거 조건 및 대체 CI 필드에 대한 자세한 내용은 다음 문서를 참조하십시오 CI(구성 항목) 필드로 트리거 조건 정의. 프로파일을 구성하고, 보안 인시던트를 테스트하고, 미리 보는 데 필요한 단계와 프로파일 유형의 예는 다음 설정 구성예를 참조하십시오.
	보안 인시던트 분석가 역할의 ServiceNow AI Platform 사용자는 맬웨어 검사 및 위협 이벤트 나열에 대한 추가 요청을 제출합니다. 자세한 내용은 보안 인시던트에서 수동으로 프로파일 트리거 McAfee ePO 문서를 참조하십시오. ServiceNow AI Platform에서 승인 역할이 있는 사용자 또는 승인 그룹의 구성원은 호스트 격리 및 격리 제거 요청을 승인합니다. 승인 요청 처리에 대한 자세한 내용은 다음 문서를 참조하십시오 승인 그룹 생성.

설정 단계를 완료하고, 애플리케이션을 설치 및 구성하고, 통합에 대한 예상 결과를 확인했습니다.

ServiceNow AI Platform® 통합을 위한 **McAfee ePO** 인스턴스 설정

다음 섹션에는 통합을 위한 애플리케이션을 설치하기 전에 인스턴스에서 완료해야 ServiceNow AI Platform# 하는 설정 작업이 나열되어 있습니다 McAfee ePO .

요구 사항 설정

필요한 역할: ServiceNow AI Platform 관리자(admin). 통합을 위해 McAfee ePO 인스턴스를 생성하기 ServiceNow AI Platform# 전에 다음 정보를 검토합니다.

다음 표는 애플리케이션에 대한 설치 요구 사항 목록입니다. 에서 ServiceNow Store통합을 위한 애플리케이션을 설치하기 전에 이러한 작업을 완료했는지 확인합니다.

작업 설정	설명
필수 ServiceNow AI Platform# 및 보안 인시던트 응답 (SIR) 역할을 할당했는지 확인합니다.	다음과 같은 역할이 필요합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업 설정	설명
	• 애플리케이션을 설치하기 위한 시스템 관리자(admin) 역할을 가진 사용자입니다. • 보안 인시던트 관리자(sn_si.admin) 역할의 사용자가 애플리케이션을 구성하고 프로파일을 생성, 활성화 및 제거합니다. • 보안 인시던트 분석가(sn_si.analyst) 역할을 가진 사용자는 보안 인시던트를 다룹니다. 작업에는 보안 인시던트에서 프로파일을 수동으로 시작하는 작업이 포함됩니다. 구성 단계 중에 프로파일에서 승인 옵션을 선택한 경우 이 역할을 가진 사용자는 호스트를 격리하고 네트워크에 반환하기 위한 요청도 제출합니다.
의 버전 5.9 McAfee ePO를 사용하고 있는지 확인합니다.	통합은 McAfee ePolicy Orchestrator의 버전 10.4.3을 지원합니다.
콘솔에 확장 플러그인을 McAfee ePO 설치 ServiceNow 했는지 확인합니다.	ServiceNow 콘솔에 플러그인을 McAfee ePO 설치합니다. 자세한 내용을 확인하고 플러그인 파일을 ServiceNow AI Platform 가져오려면 인스턴스에서 지식 〉 문서 〉 모두 그리고 검색 필드에 ServiceNow Security Operations Extension for McAfee ePO를 입력합니다.
ServiceNow 통합을 위해 애플리케이션을 설치하기 전에 통합을 지원하는 데 필요한 핵심 애플리케이션이 설치되고 활성화되었는지 확인합니다.	보안 인시던트 응답 의존성 플러그인(com.snc.si_dep)이 필요합니다. 이 플러그인은 제품을 지원하는 데 필요한 모든 종속성을 보안 인시던트 응답 자동으로 설치합니다. 통합에 필요한 다른 보안 운영 애플리케이션을 설치하고 활성화하기 전에 이 플러그인을 설치하고 활성화합니다. 에서 ServiceNow Store다음 보안 운영 애플리케이션이 설치되고 활성화되는지 확인합니다. 설치되지 않은 경우 원활한 설치를 위해 다음 순서로 한 번에 하나의 애플리케이션을 설치하고 활성화합니다. **1.** 보안 인시던트 응답 **2.** 보안 인시던트 응답 작업 공간 **3.** 보안 통합 프레임워크 **4.** Security Support Common **5.** 보안 지원 오케스트레이션 Security Operations Core 애플리케이션 설치에 대한 자세한 내용은 해당 애플리케이션 활성화 ServiceNow Store문서를

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업 설정	설명
	참조하십시오제품 또는 애플리케이션에 대한 보안 운영 권리 가져오기.
MID Server를 설치하고 구성했는지 확인하십시오.	인스턴스에 설치 및 구성된 MID 서버가 필요합니다 ServiceNow AI Platform# . MID Server에 대한 자세한 내용은 ServiceNow 제품 설명서 웹 사이트를 참조하십시오.
프로파일에 대한 승인 프로세스를 활성화하려면 요청을 처리할 승인 그룹을 생성했는지 확인합니다.	호스트 시스템을 격리하고 네트워크에 복원하는 데 사용할 수 있는 선택적 승인 프로세스가 있습니다. 이 옵션을 사용하는 경우 호스트 컴퓨터를 격리하고 네트워크에 복원하기 전에 사전 승인이 필요합니다. 조직에서 이러한 작업에 대한 추가 제어 수준을 원하는 경우 프로파일에 대한 구성 단계 중에 승인 필요 옵션을 활성화합니다. 기본적으로 승인 권한은 보안 인시던트 관리자 (sn_si.admin)에게 ServiceNow AI Platform# 할당됩니다. 이 권한은 승인 그룹에 재할당할 수 있습니다. 그룹 내에서 모든 구성원은 요청을 승인하거나 거부할 수 있는 권한이 있습니다. 프로파일 설정의 구성 단계에서 활성 승인 그룹을 선택합니다. 자세한 내용은 승인 그룹 생성 문서를 참조하십시오.

McAfee ePO(SIR)과 보안 인시던트 응답 통합하도록 콘솔 설정

다음 섹션에는 통합을 위해 애플리케이션을 ServiceNow Store 설치하기 전에 콘솔에서 완료해야 McAfee ePO 하는 설정 단계가 나열되어 있습니다.

시작하기 전에
필요한 역할: McAfee ePO 관리자

관리자 권한이 있는 McAfee ePO 사용자는 콘솔에 Servicenow.zip 확장 플러그인을 McAfee ePO 설치했는지 확인합니다. 통합에 이 확장 플러그인이 필요합니다. 자세한 내용을 확인하고 플러그인을 ServiceNow AI Platform 얻으려면 인스턴스에서 지식 〉 문서 〉 모두. 검색 필드에 ServiceNow Security Operations Extension for McAfee ePO를 입력합니다.

이 태스크 정보
확장 플러그인은 ServiceNow 인스턴스를 McAfee ePO 콘솔에 연결합니다ServiceNow AI Platform. 이 연결을 통해 격리 호스트에 대해 콘솔에서 생성한 McAfee ePO 보안 태그를 참조하고 인스턴스의 역량 프로파일에 대한 맬웨어 스캔 작업을 시작할 수 있습니다 ServiceNow AI Platform .

콘솔의 McAfee ePO 보안 태그가 인스턴스의 ServiceNow AI Platform 기능 레코드에 있는 보안 태그와 일치해야 합니다.

다음 단계에서는 확장 플러그인을 설치하고, 콘솔에 보안 태그를 McAfee ePO 만들고, 태그에 작업을 할당하는 방법을 보여줍니다. 콘솔의 McAfee ePO 보안 태그에 대한 자세한 내용은 McAfee 제품 설명서 웹 사이트를 참조하십시오.

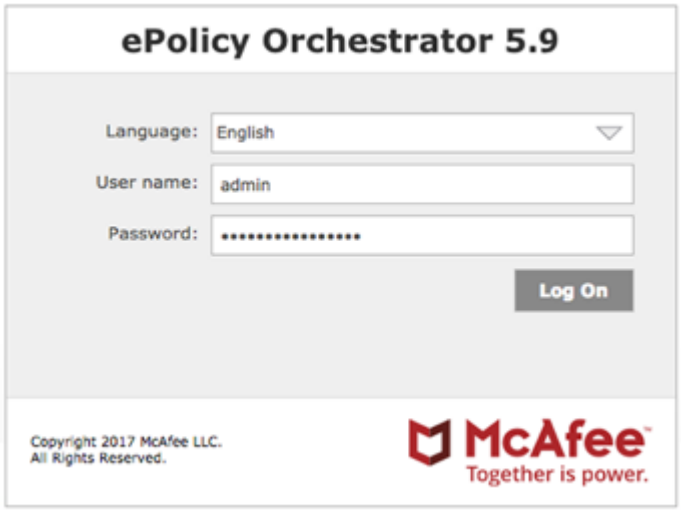
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
다음 섹션의 그림은 콘솔에서 가져온 McAfee ePO 것입니다.

프로시저

1. 콘솔에 확장 플러그인을 McAfee ePO 설치하지 ServiceNow 않은 경우 다음 단계에 따라 설치합니다.

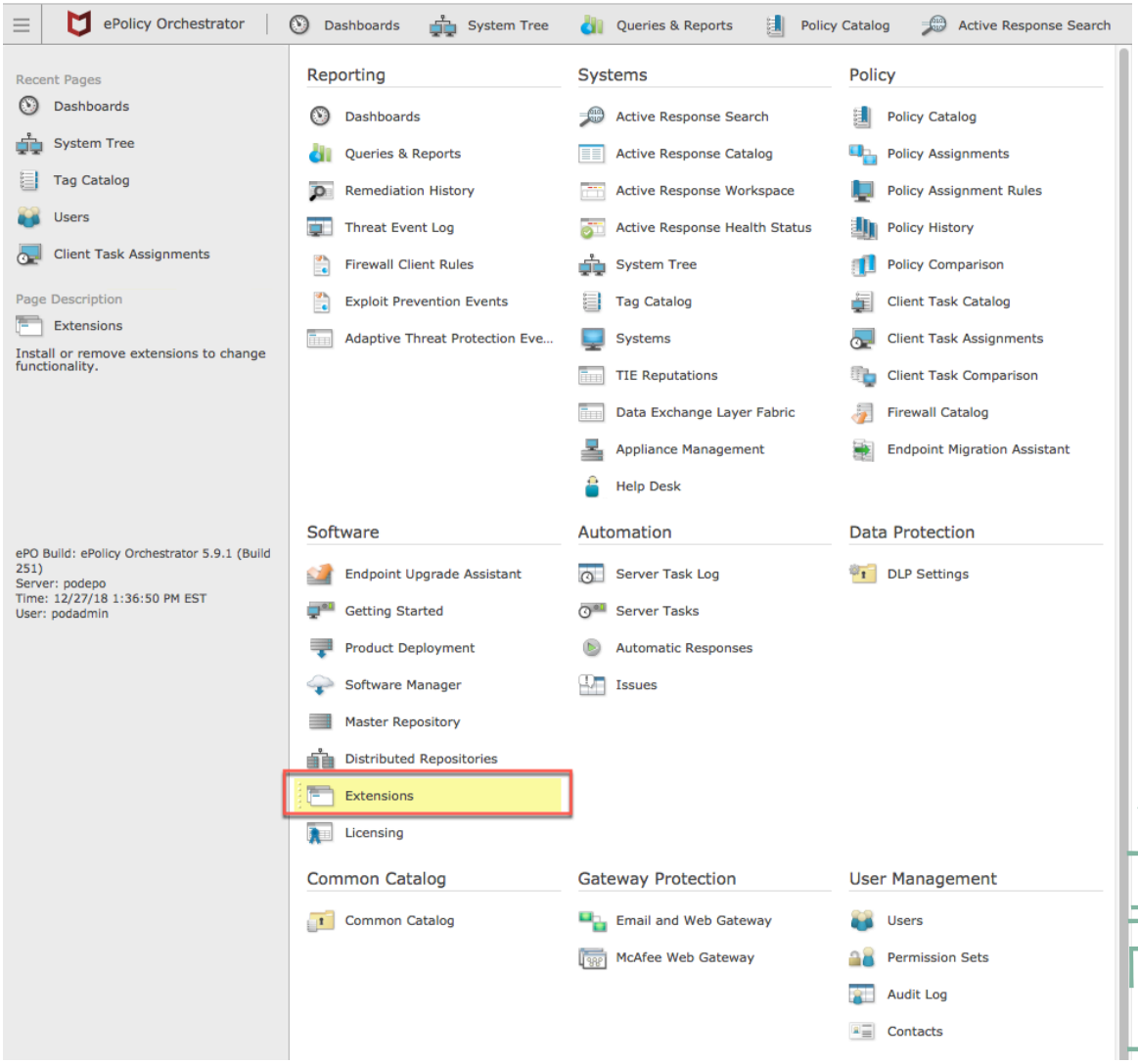
   a. McAfee ePO McAfee 사용자 이름과 암호를 사용하여 콘솔에 로그인합니다.



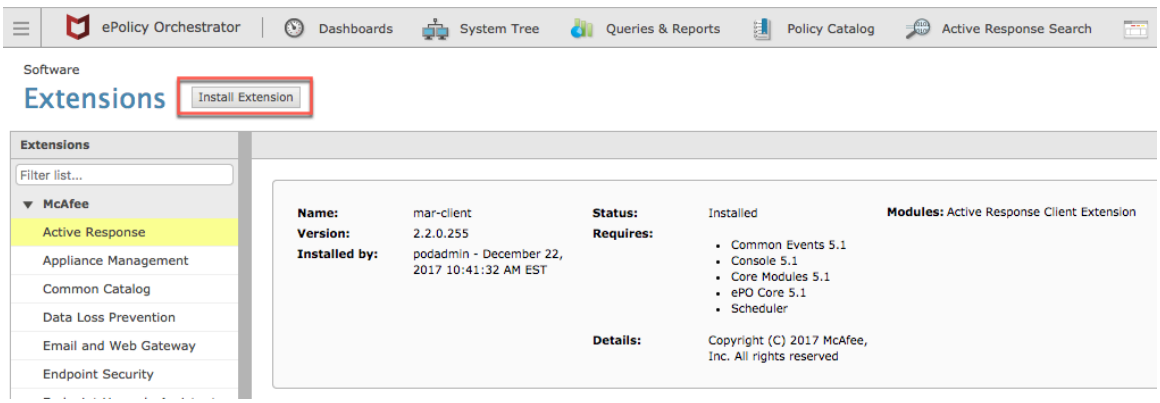
2. 다음 그림에 표시된 페이지가 표시되지 않으면 홈페이지의 배너 왼쪽 상단에서 메뉴 아이콘을 클릭하여 표시합니다.

3. 소프트웨어 섹션에서 확장 프로그램 링크를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

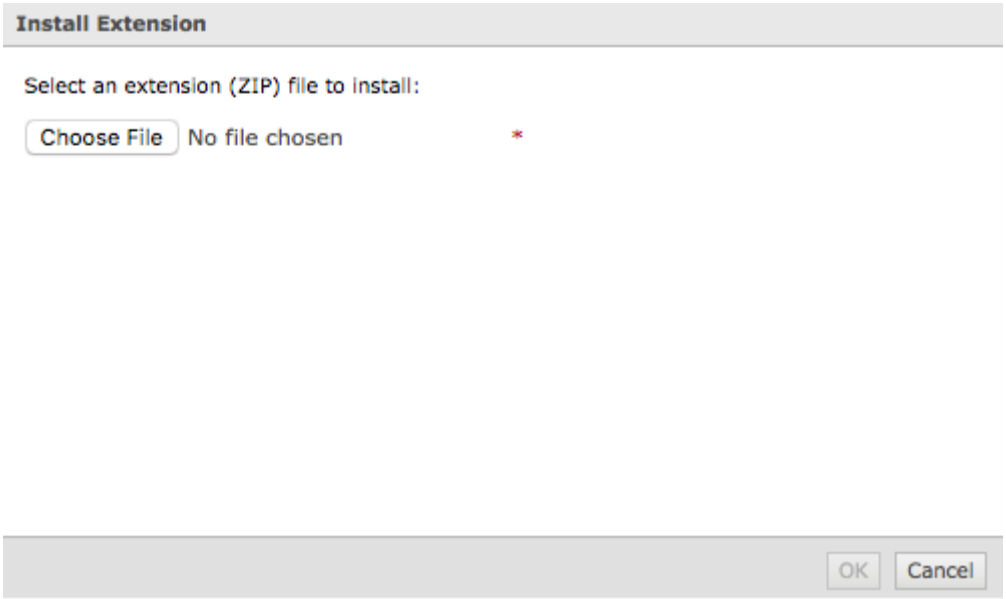


4. 표시되는 확장 페이지에서 확장 설치를 클릭합니다.

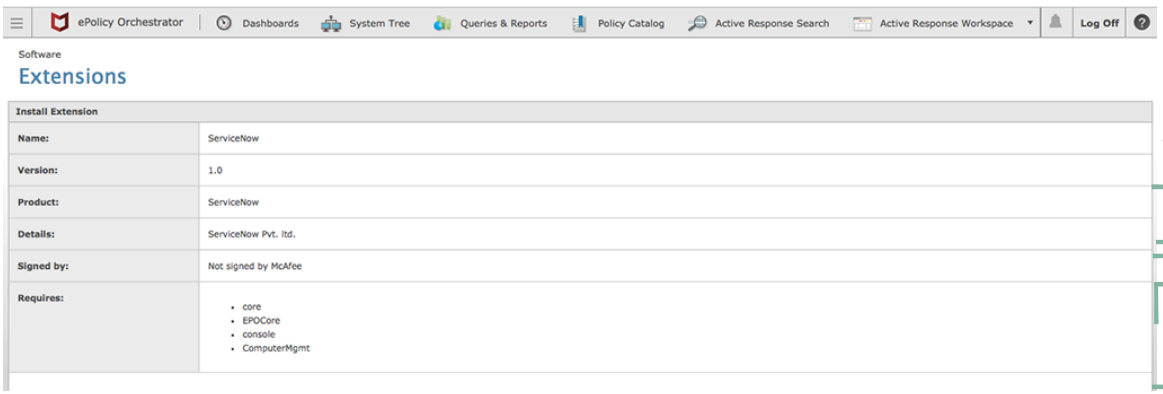


5. 설치 확장 대화 상자에서 파일 선택을 클릭하고 시스템의 Servicenow.zip 파일로 이동한 다음 확인을 클릭하여 다운로드합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



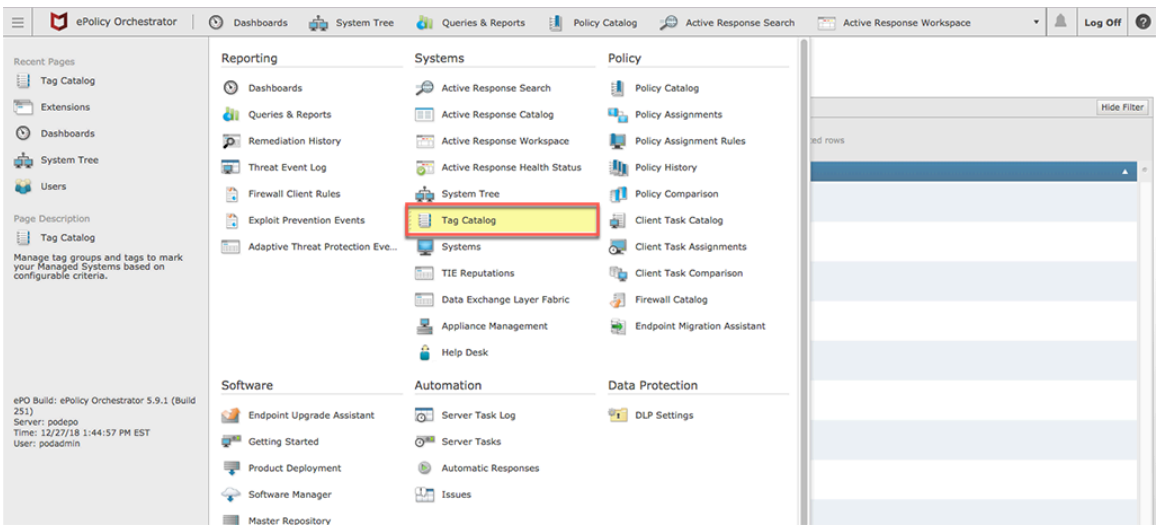
다운로드가 완료되면 확장 플러그인이 ServiceNow 나열된 소프트웨어 확장 페이지가 표시됩니다.



콘솔에 플러그인 확장을 성공적으로 설치 ServiceNow 했습니다 McAfee ePO .

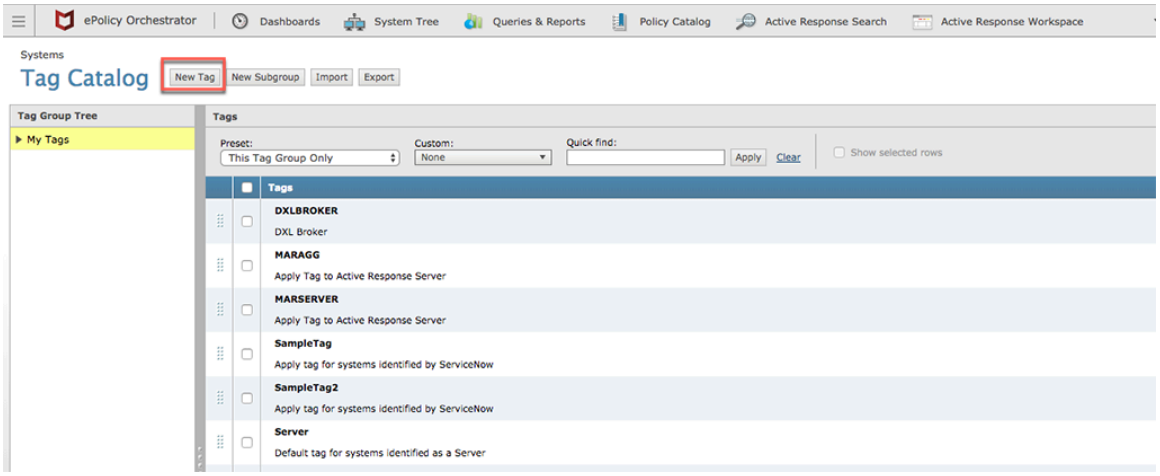
6. 콘솔에서 맬웨어 검사 시작 및 호스트 격리 작업에 대한 보안 태그를 McAfee ePO 생성하지 않은 경우 다음 단계를 수행합니다.

a. 홈페이지로 이동하여 태그 카탈로그 링크를 클릭합니다.



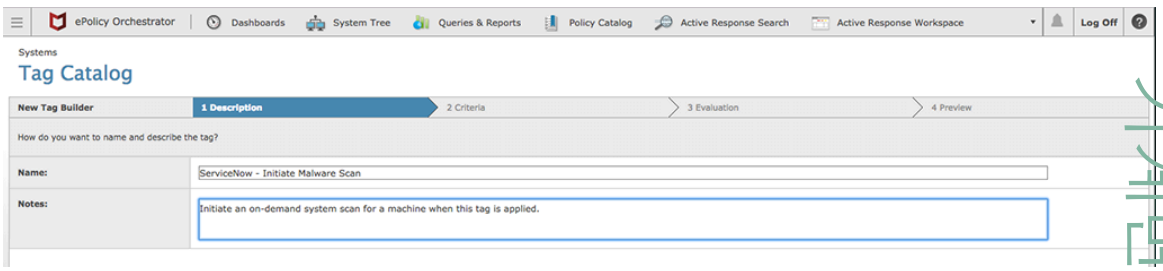
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

b. 표시되는 태그 카탈로그 페이지에서 새 태그를 클릭합니다.

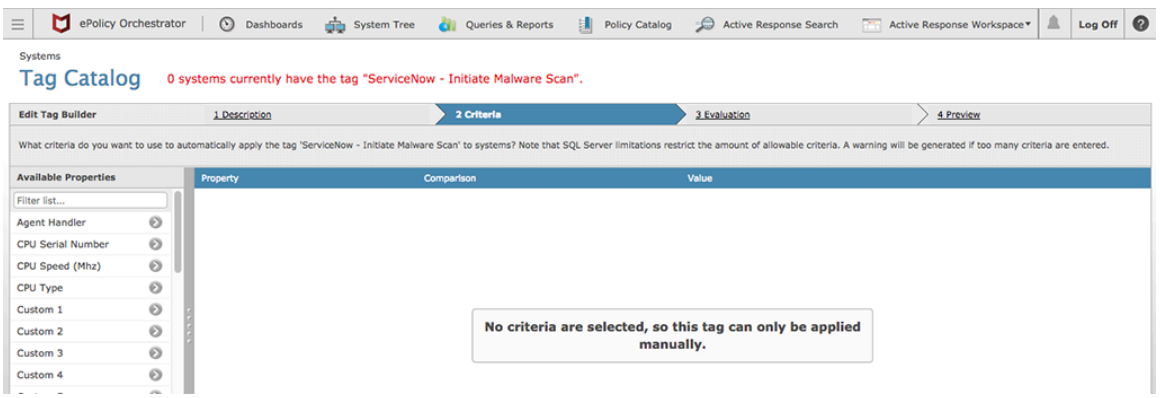


c. 표시되는 진행률 표시줄에서 설명 단계를 선택하고 태그의 이름과 설명을 입력합니다.

이 예에서는 맬웨어 스캔 시작 기능에 대한 이름과 설명이 포함된 태그가 표시됩니다. 이 태그 이름은 인스턴스에서 일치하고 참조 ServiceNow AI Platform 되는 이름입니다.

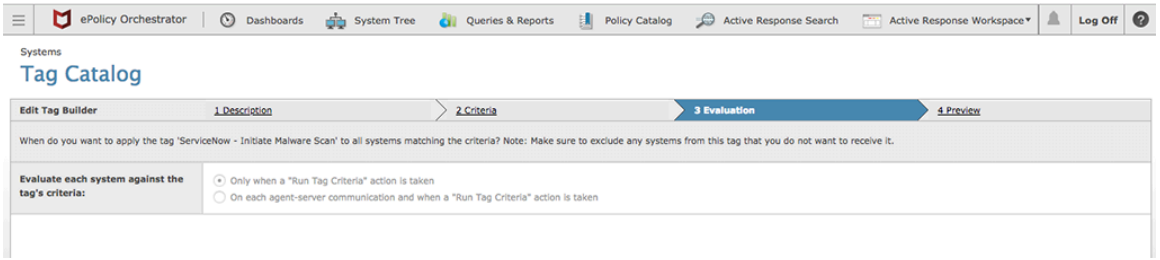


d. 기준 단계로 이동하려면 진행률 표시줄에서 기준을 클릭합니다.
표시되는 메시지는 현재 이 태그에 할당된 작업이 없고 태그를 수동으로만 적용할 수 있음을 나타냅니다.

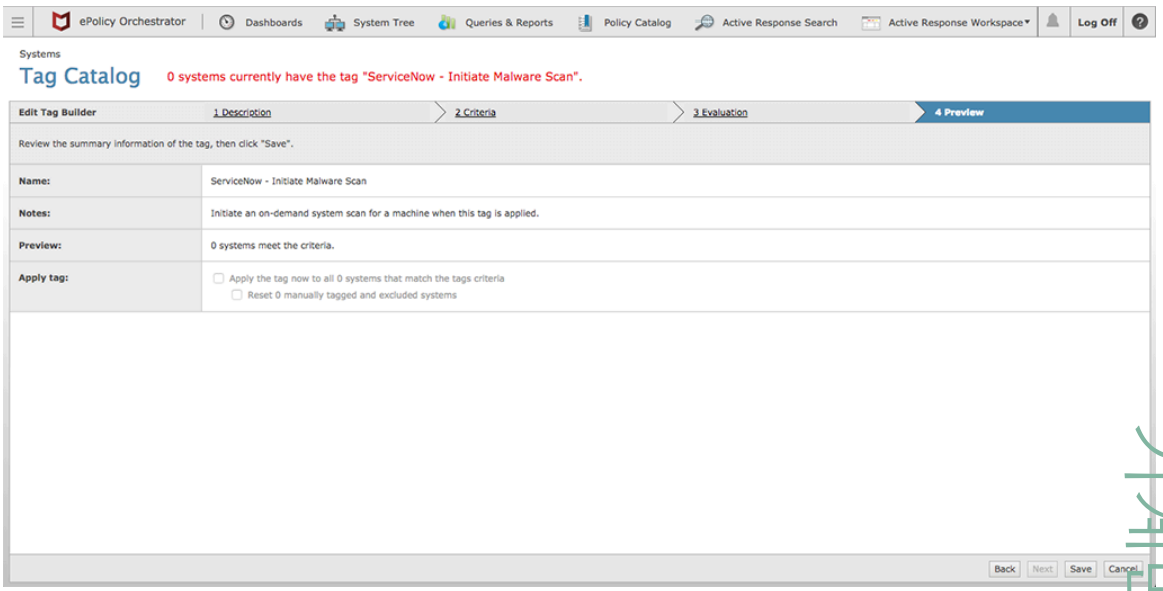


e. 진행률 표시줄에서 평가를 클릭하여 계속합니다.

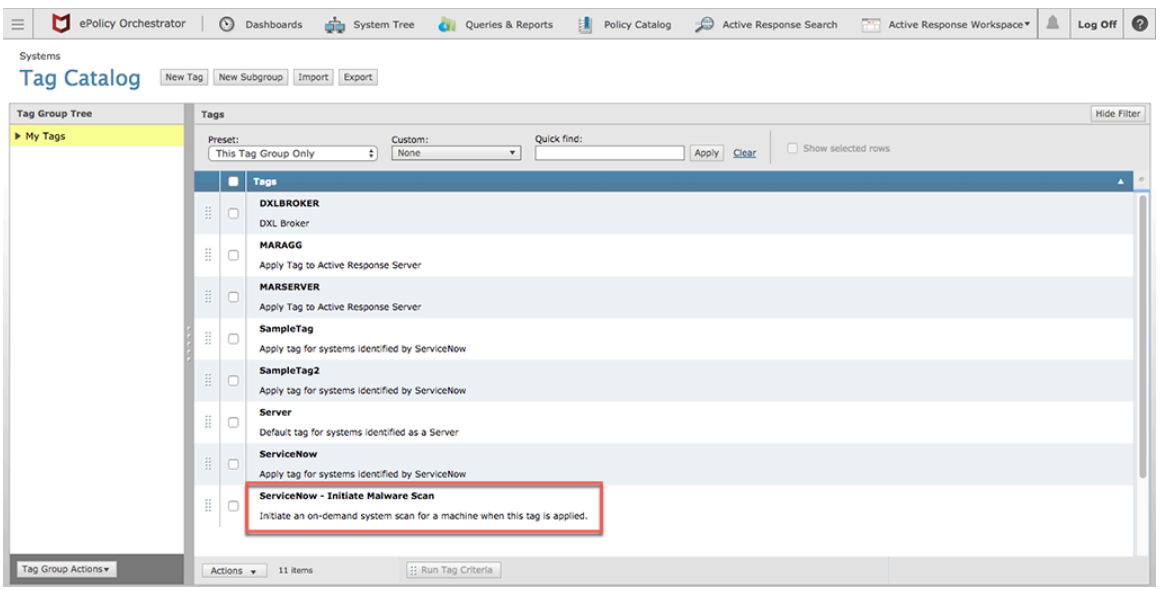
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



f. 평가 단계의 태그 카탈로그 페이지가 표시되면 이 페이지의 설정을 기본값으로 두고 진행률 표시줄에서 미리 보기를 클릭합니다.



g. 미리 보기 페이지가 표시되면 페이지 오른쪽 아래에 있는 저장을 클릭하여 기록을 저장합니다. 새 태그는 다음 그림과 같이 태그 카탈로그에 표시됩니다.

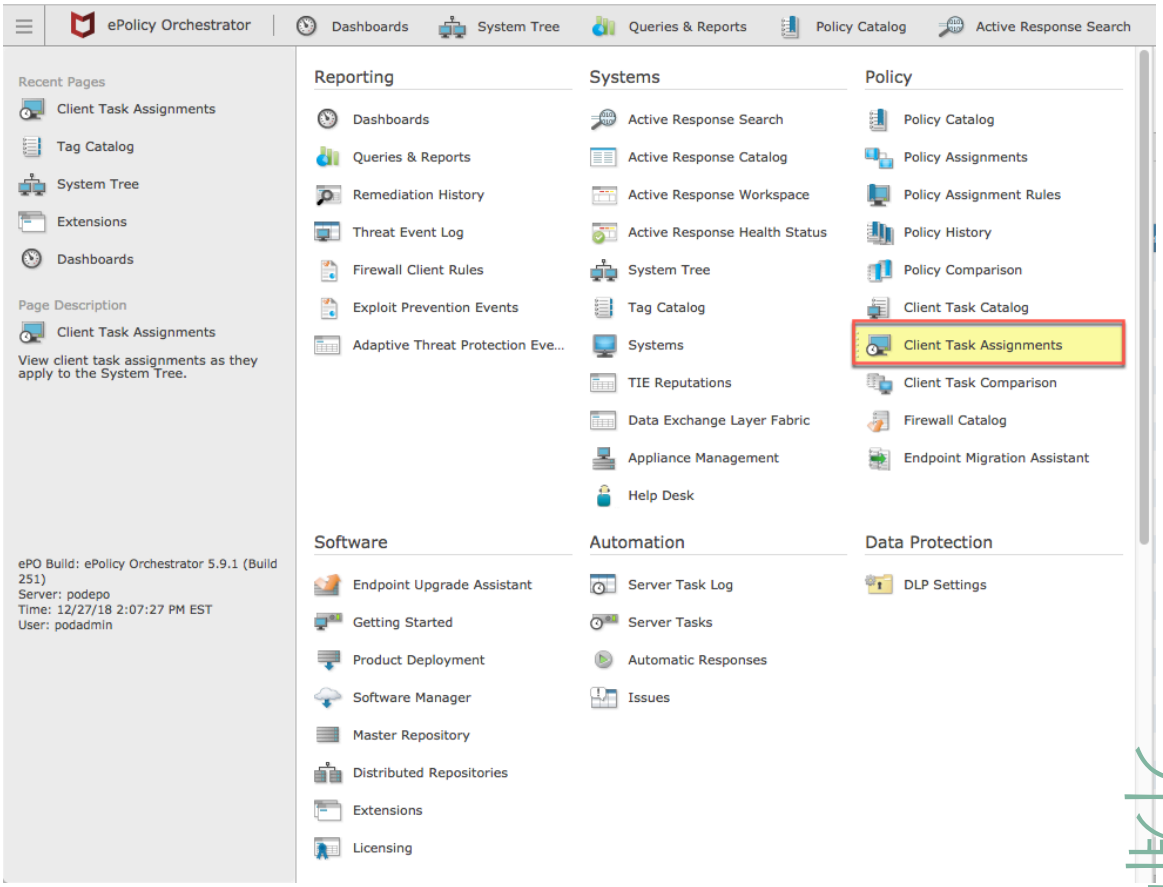


7. 이전 단계를 반복하여 호스트 분리 작업에 대한 보안 태그를 생성합니다. 두 태그를 모두 생성했으면 새 태그에 작업을 할당할 준비가 된 것입니다.

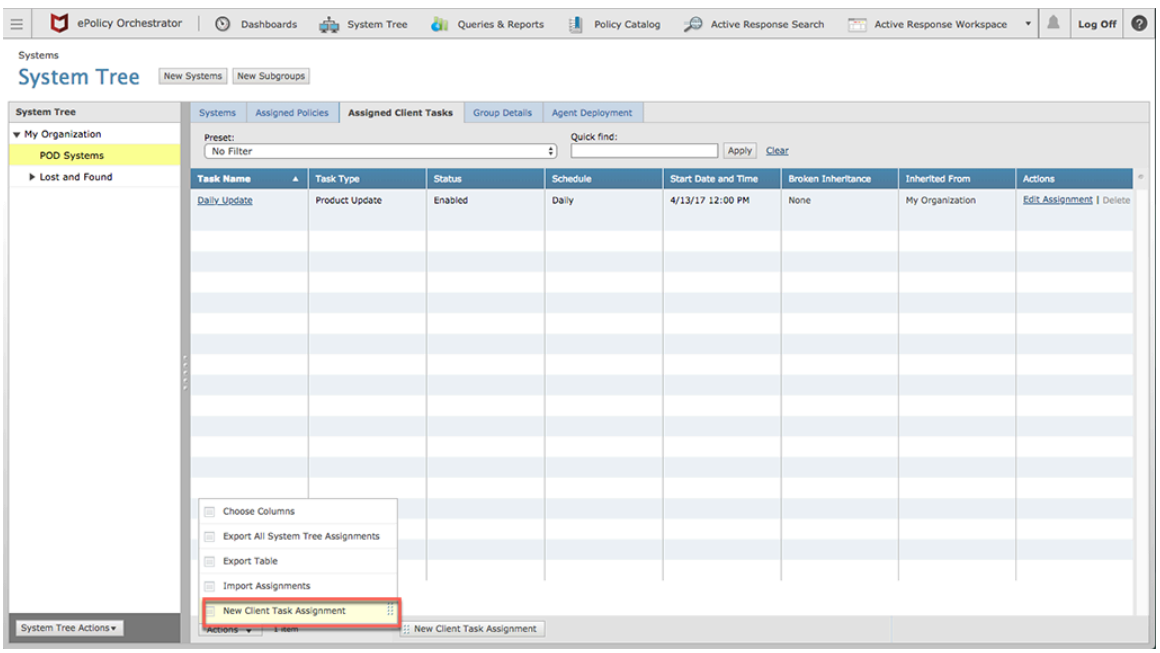
8. 새 태그에 작업을 추가하려면 다음 단계를 따르세요.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 홈페이지로 이동하여 정책 섹션에서 클라이언트 작업 할당 링크를 클릭합니다.

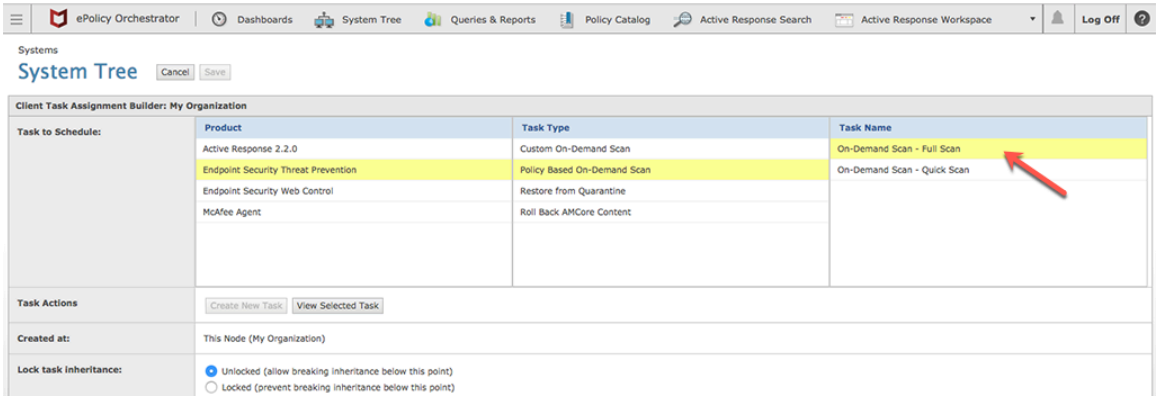


b. 표시되는 시스템 트리 페이지에서 페이지 아래쪽에서 작업 메뉴를 확장하고 새 클라이언트 작업 할당을 선택합니다.

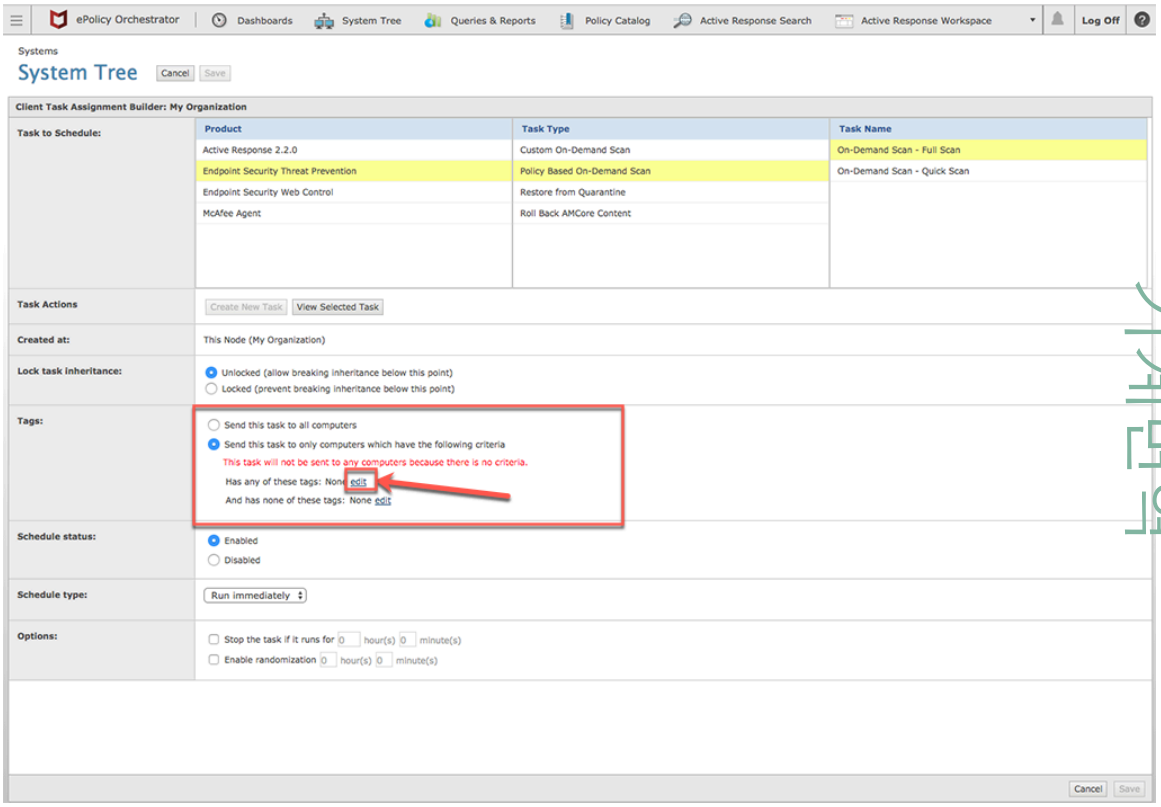


c. 표시되는 페이지에서 엔드포인트 보안 위협 방지 〉 온디맨드 검사에 기반한 정책 〉 요청 시 스캔 - 전체 스캔 다음 그림과 같이 경로를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

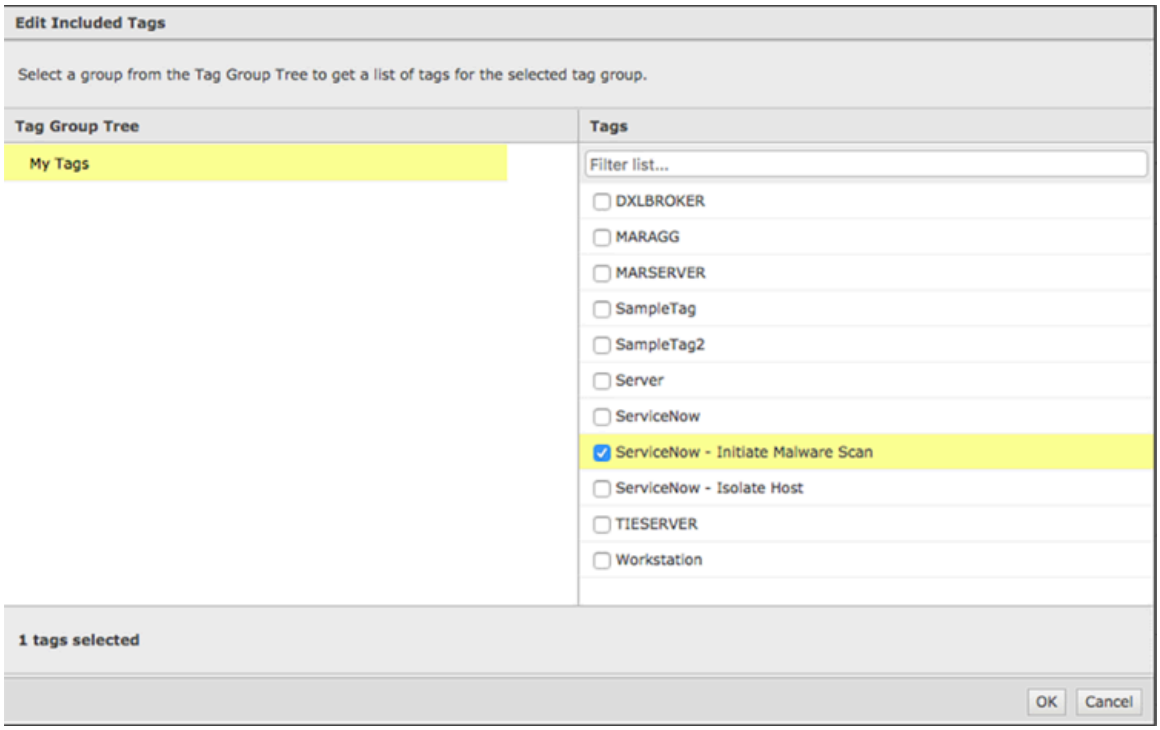


d. 태그 섹션의 라디오 버튼 아래 다음 ## ##: 옆에 있는 편집 링크를 클릭하여 태그의 기준을 편집합니다.



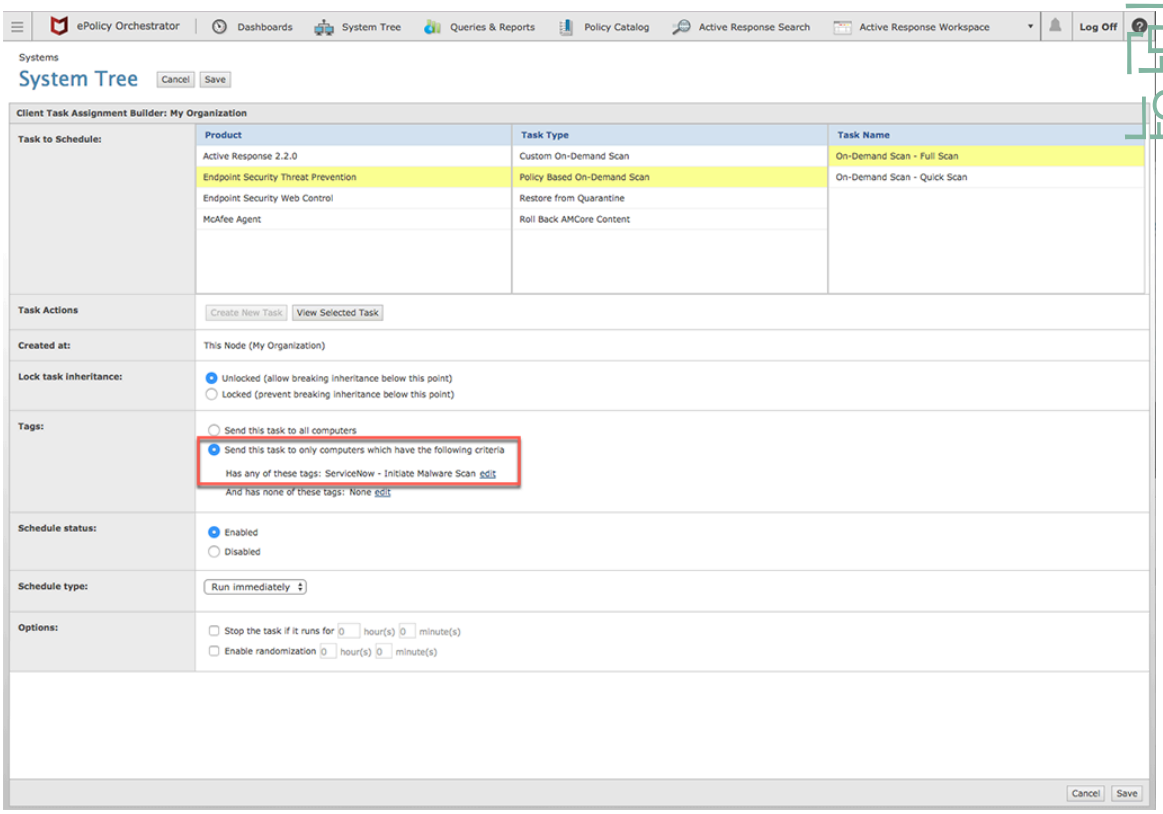
e. 표시되는 대화 상자에서 이전 단계에서 만든 맬웨어 검사 ServiceNow 시작 태그를 선택하고 확인을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



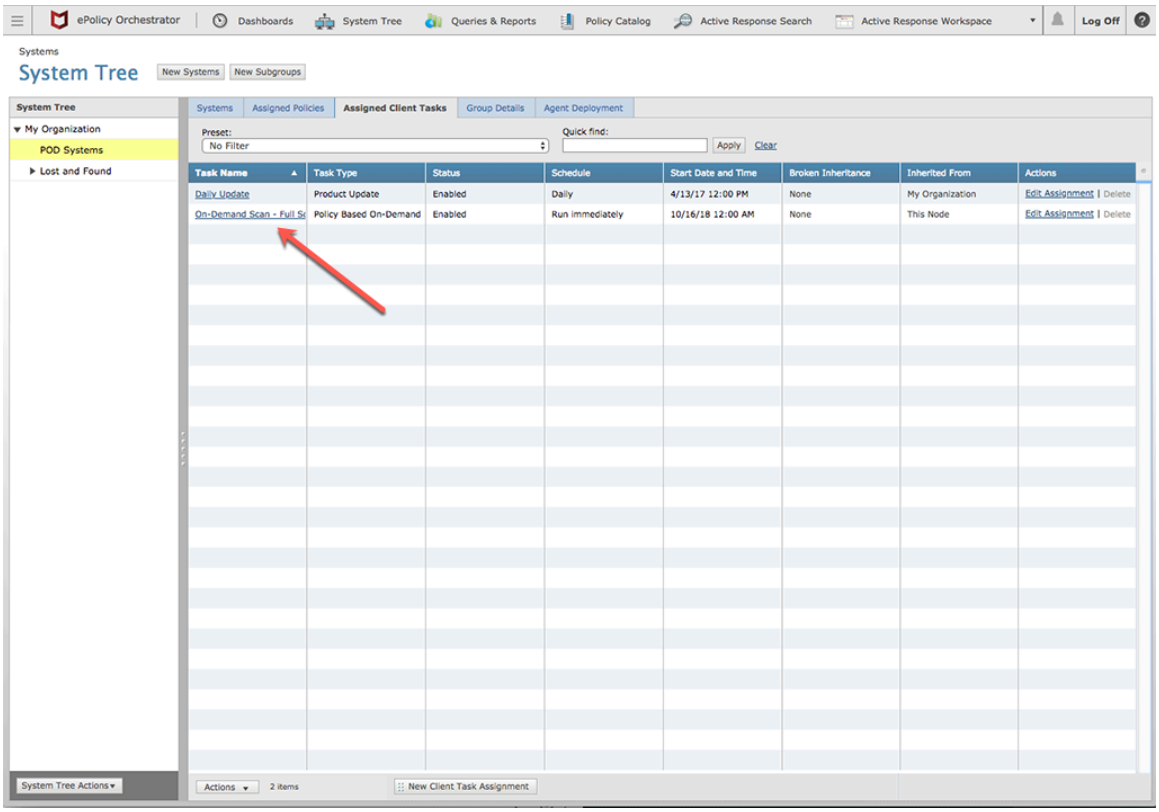
생성한 ServiceNow 맬웨어 검사 시작 태그가 요청 시 검사 작업에 할당됩니다.

f. 확인을 클릭합니다.
Tags(태그) 섹션의 라디오 버튼 아래 Has any of these tags(## ## ##): 옆에 Initiate Malware Scan(맬웨어 검사 시작) 태그가 표시됩니다.



g. 저장을 클릭합니다.
시스템 트리 페이지의 할당된 클라이언트 작업 목록(탭)에 작업이 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



h. 호스트 분리 작업에 작업을 할당하지 않은 경우 이전 단계를 반복하여 할당합니다.

확장 플러그인을 성공적으로 설치하고, 보안 태그를 만들고, 태그에 작업을 할당했습니다. 콘솔에서 통합 설정을 완료했습니다 McAfee ePO . 다음 단계는 인스턴스에서 서버를 ServiceNow AI Platform 구성하는 것입니다.

애플리케이션 설치 및 통합을 위한 **McAfee ePO** 서버 구성

통합을 위한 워크플로우를 호출하기 전에 인스턴스에서 애플리케이션을 ServiceNow StoreServiceNow AI Platform 설치하고 구성합니다McAfee ePO. 콘솔에 연결하려면 McAfee ePO 구성이 필요합니다.

시작하기 전에

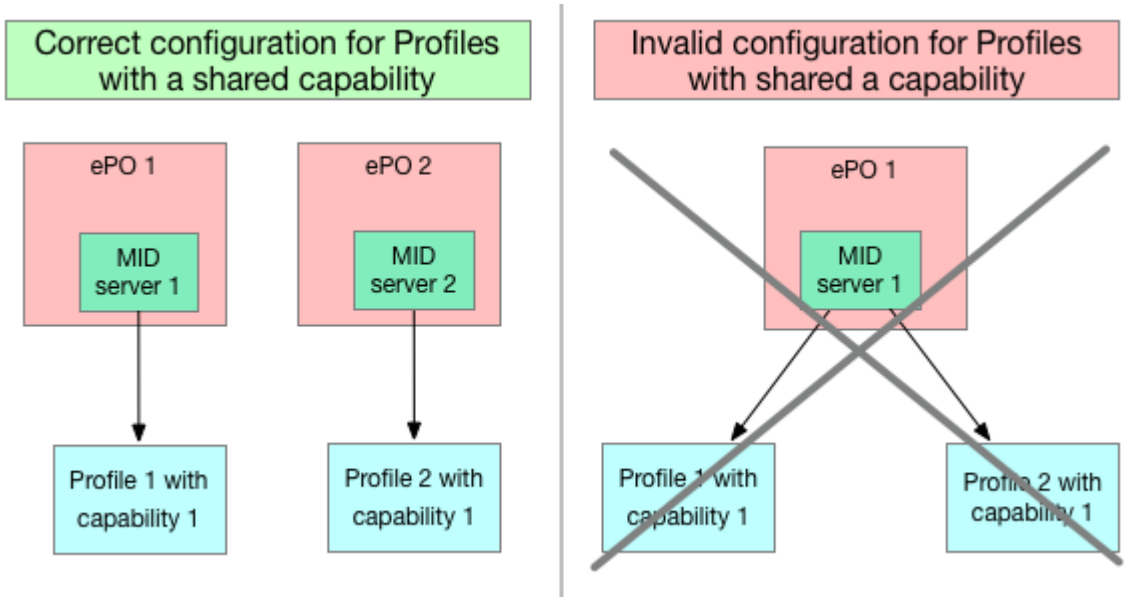
필요한 역할: ServiceNow AI Platform 관리자(admin)

이 태스크 정보

통합은 여러 서버를 지원하지만 동일한 트리거 조건을 공유하는 프로파일의 충돌을 방지하기 위해 동일한 McAfee ePO 서버를 사용하는 여러 프로파일과 기능을 공유할 McAfee ePO 수 없습니다. 예를 들어 다음 그림과 같이 각 McAfee ePO 서버가 기능 1이 있는 고유한 프로필에 매핑되는 한 둘 이상의 프로필에 기능 1을 사용할 수 있습니다.

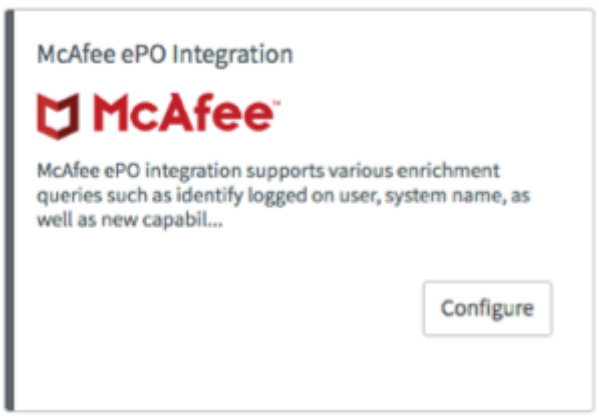
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

McAfee 공유 프로파일 제한 사항



프로시저

1. 에서 for 보안 운영ServiceNow Store 를 McAfee ePO 다운로드하여 설치합니다.
2. 다음으로 이동 보안 운영 〉 통합 〉 통합 구성.
3. 통합 타일을 McAfee ePO 검색하고 구성을 클릭합니다.보안 운영



4. 양식에서 필드를 채웁니다.

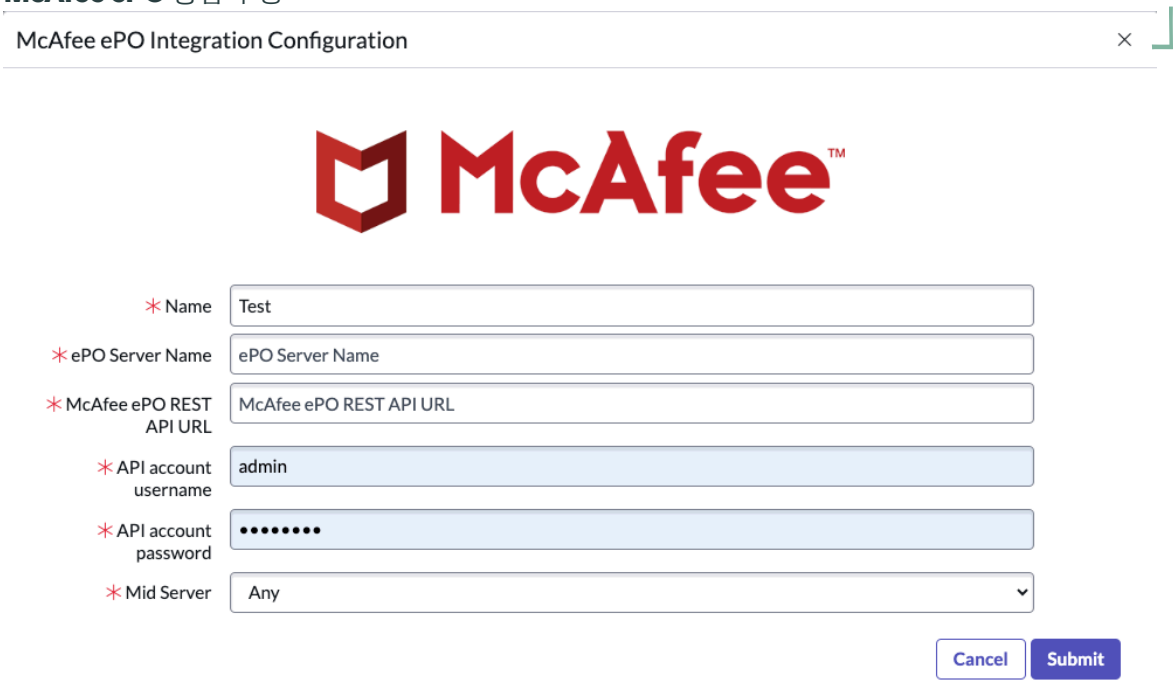
McAfee ePO 통합 구성

필드	설명
이름	통합의 이름입니다(예: `demo-1`).
ePO 서버 이름	McAfee ePO 서버 이름입니다. 하나의 서버를 사용하는 경우 #: McAfee HQ (McAfee Head Quarters). 이 이름은 서버 및 관련 자격 증명이 인식되는 방법입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	조직에서 여러 서버에 대한 지원이 필요한 경우 각 서버의 이름을 입력하고 프로세스를 반복합니다.
McAfee ePO REST API URL	REST API를 호스팅하는 기본 URL입니다 McAfee ePO . https:// 프로토콜을 사용하여 URL을 입력합니다(예: `https://corp.epo_server:8443`).
API 계정 사용자 이름	고유 계정 사용자 이름(예: ServiceNow API)
API 계정 암호	API 계정의 고유한 암호입니다.
MID 서버	인스턴스를 설정하는 ServiceNow AI Platform 동안 구성한 MID 서버의 이름을 선택합니다. 목록에서 특정 MID 서버를 선택하거나 임의 를 선택하여 이 통합에 대해 유효한 MID 서버를 목록에서 자동으로 선택할 수 있습니다. 주: ○ 이 구성 시간 동안 선택한 MID 서버는 이 통합 전체에 적용됩니다. ○ 활성 상태이고 유효성이 검사된 MID Server만 이 목록에 표시됩니다. 기본적으로 이 값은 임의로 설정됩니다. 예시 이름은 secops_local_midserver입니다.

McAfee ePO 통합 구성



5. 제출을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

McAfee ePO 구성 목록이 새 구성 기록과 함께 표시됩니다. 서버에 대한 구성을 성공적으로 완료했습니다 McAfee ePO .

주:
조직에서 여러 서버에 대한 지원이 필요한 경우 단계를 반복합니다.

통합을 위해 **McAfee ePO** 에서 **ServiceNow AI Platform** 보안 태그 편집

통합 설정의 일부로, 인스턴스의 콘솔에서 ServiceNow AI Platform 생성한 McAfee ePO 보안 태그 이름을 편집합니다. 콘솔의 ServiceNow AI Platform 태그 McAfee ePO 이름과 일치하도록 인스턴스의 태그 이름을 편집합니다.

시작하기 전에
필요한 역할: ServiceNow AI Platform 보안 인시던트 관리자(sn_si.admin)

이 태스크 정보
맬웨어 검사 시작 및 호스트 격리 작업에 대한 콘솔의 McAfee ePO 보안 태그 이름은 인스턴스의 이러한 기능에 ServiceNow AI Platform 대한 기록의 보안 태그 이름과 일치해야 합니다.

역량 프로파일을 생성하여 역량을 실행하기 전에 사용 가능한 McAfee ePO 역량 목록을 보고 콘솔의 McAfee ePO 보안 태그 이름과 일치하도록 인스턴스의 보안 태그를 ServiceNow AI Platform 편집합니다.

콘솔에서 보안 태그 이름을 McAfee ePO 생성하는 방법에 대한 자세한 내용은 문서를 참조하십시오 McAfee ePO(SIR)과 보안 인시던트 응답 통합하도록 콘솔 설정.

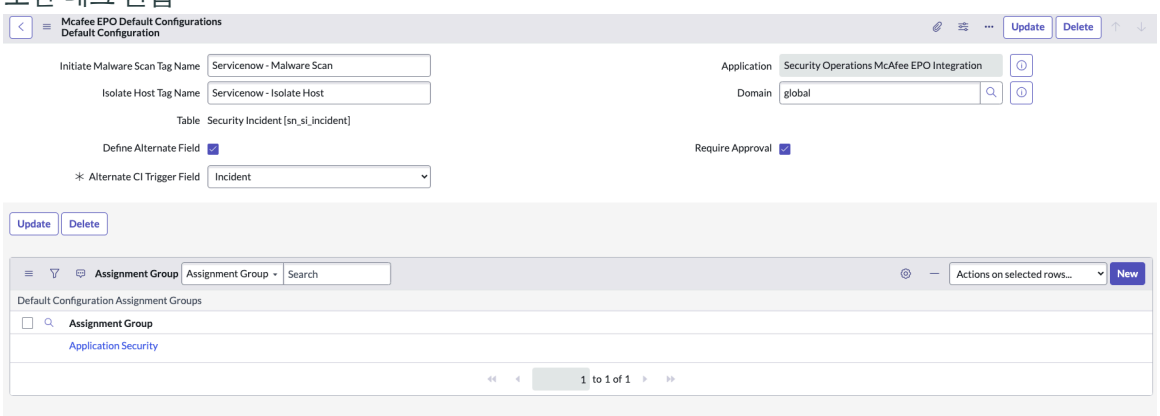
프로시저

1. 다음으로 이동 모두 〉 **McAfee ePO** 통합 〉 기본값 설정.
2. 통합의 McAfee ePO 보안 태그 이름을 편집하려면 기본 구성을 클릭합니다.

   주:
   통합을 설치한 McAfee ePO 후 이 구성을 수행해야 합니다.

3. 맬웨어 검사 태그 이름 시작 필드에 검사 시작 작업에 대해 콘솔에서 생성한 McAfee ePO 보안 태그의 이름을 입력합니다.
   예: ServiceNow - 맬웨어 검사
4. 호스트 태그 이름 격리 필드에 호스트 격리 작업에 대해 콘솔에서 생성한 McAfee ePO 보안 태그의 이름을 입력합니다.
   예: ServiceNow - 호스트 격리
5. 인시던트 생성 시 CI 트리거 필드를 사용하지 않으려면 대체 필드 정의 확인란을 선택합니다.
   이 옵션을 사용하면 대체 CI 트리거 필드 선택 목록이 표시됩니다.

보안 태그 편집



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

6. 선택 목록에서 대체 필드를 선택하여 CI 검색 기준을 확인합니다.
   이 예에서는 sn_si.admin 역할을 가진 사용자는 인시던트 생성 시 보안 인시던트의 CI 필드가 채워지지 않을 것으로 예상합니다. 또는 FQDN, 호스트 이름 또는 IP 주소에 대한 CI 정보가 보안 인시던트의 ### CI 필드에 채워질 것으로 생각하고 식별된 CI 필드를 대안으로 선택합니다. 이 예에서는 식별된 CI가 선택되었지만 대체 CI에 대한 보안 인시던트의 모든 필드를 사용할 수 있습니다.
7. 도메인 필드에서 검색 옵션을 사용하여 이 구성에 대한 도메인 또는 그룹을 선택합니다.
   예를 들어 전역입니다.
8. 호스트 격리 및 격리 제거 역량을 사용하는 경우 승인 필요 필드에서 승인 필요 확인란을 선택합니다.

   주:
   맬웨어 검사 시작, 위협 이벤트 나열 및 시스템 세부 정보 가져오기 기능은 승인이 필요하지 않습니다.

9. 업데이트를 클릭합니다.
   EPO 태그 이름이 업데이트되고 McAfee ePO 기본 구성 목록에 표시됩니다. 인스턴스의 맬웨어 검사 작업에 ServiceNow AI Platform 대한 보안 태그 이름이 콘솔의 McAfee ePO 검사 이름과 일치합니다.

   인스턴스에서 멀웨어 검사 및 호스트 격리 역량에 대한 EPO 태그 이름을 성공적으로 편집했습니다 ServiceNow AI Platform . 다음 단계는 역량에 대한 프로필을 만드는 것입니다.

관련 정보

McAfee 제품 설명서

승인 그룹 생성

호스트 시스템을 격리하고 네트워크로 복원하기 위한 요청을 승인할 수 있는 통합용 보안 운영 승인 그룹을 McAfee ePO 생성합니다.

시작하기 전에
인스턴스에서 승인 그룹을 사용할 수 없는 경우 그룹에 승인 권한을 재할당할 수 없습니다.

주:
의 설정 구성 승인 옵션은 호스트 격리 및 호스트 격리 제거 기능에만 표시됩니다.

필요한 역할: ServiceNow AI Platform# 보안 인시던트 관리자(sn_si.admin)

이 태스크 정보
호스트 컴퓨터를 격리하고 격리를 제거하기 위해 보안 인시던트 분석가가 제출한 승인 요청은 기본적으로 sn_si.admin 역할이 있는 사용자에게 할당됩니다. 이 역할을 가진 사용자는 프로파일의 구성 단계에서 이 승인 기관을 재할당할 수 있습니다. 승인 그룹에 권한을 재할당하려면 먼저 인스턴스의 ## 목록에서 ServiceNow AI Platform 승인 그룹을 사용할 수 있어야 합니다.

프로시저

1. 다음으로 이동 모두 〉 사용자 관리 〉 그룹.
2. 그룹 목록에서 새로 만들기를 클릭합니다.
3. 양식에서 필드를 채웁니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

승인 그룹 양식

필드	설명
이름	승인 요청이 제출될 때 표시되는 그룹의 이름(예: ### McAfee ### ##)입니다.
그룹 이메일	그룹 관리자 McAfeeapproval@servicenow 같은 접촉 창구의 이메일 주소 또는 그룹 이메일 배포 목록입니다.com
관리자	그룹 관리자의 이름입니다. 검색 아이콘을 클릭하여 목록을 봅니다.
상위	(선택 사항) 이 그룹에 상위 항목이 있을 경우 이 그룹이 구성원으로 속해 있는 다른 그룹입니다.
설명	이 그룹에 대한 추가 정보입니다.
구성원 포함	이 그룹에 구성원을 포함하는 옵션입니다.
기본 담당자	사용자를 이 그룹의 기본 담당자로 선택하는 옵션입니다. 검색 옵션을 사용하여 사용자 목록을 엽니다.
역할	이 그룹의 역할을 선택하는 옵션입니다. 추가 및 제거 옵션을 사용하여 역할을 추가하고 제거합니다.
유형	이 그룹의 범주를 선택하는 옵션입니다. 검색 옵션을 사용하여 그룹 유형 목록을 엽니다.
벤더	이 그룹에 대한 벤더를 선택하는 옵션입니다. 검색 옵션을 사용하여 벤더 목록을 엽니다.

4. 제출을 클릭합니다.
   새 그룹이 그룹 목록에 표시됩니다.

   이 그룹은 이 프로파일을 구성하는 동안 승인 필요 옵션을 활성화하면 요청을 처리할 수 있습니다.

   sn_si.analyst 역할을 가진 사용자가 제출한 요청을 모니터링하고 처리하기 위해 승인 그룹의 각 구성원은 의 ServiceNow AI Platform내 승인 탭으로 이동합니다.

McAfee ePO 통합 역량 프로파일

보안 인시던트 관리자(sn_si.admin) 역할을 가진 사용자는 인스턴스의 역량 ServiceNow AI Platform# 에 McAfee ePO 대한 프로필을 생성합니다. 프로파일의 쿼리 또는 작업을 그룹화하고 새 보안 인시던트가 생성될 때 실행할 역량을 결정합니다 McAfee ePO .

역량 프로파일

역량™을 그룹화 McAfee ePO 하고 인스턴스에서 이러한 역량 ServiceNow AI Platform# 에 대한 설정을 구성할 수 있도록 프로파일을 생성합니다. 이러한 기능에는 여러 프로필을 유연하게 생성할 수 있으며, 이를 통해 (SIR) 인시던트가 생성될 때 호출되는 작업이나 쿼리를 결정할 수 있습니다 보안 인시던트 응답 . 예를 들어, 조직의 요구 사항에 맞게 시스템 세부 정보에 대한 쿼리를 실행하고, 맬웨어 검사를 시작하고, 호스트 컴퓨터를 격리하는 단일 프로필을 만들거나, 각각 고유한 단일 McAfee ePO 기능을 가진 여러 프로필을 만들 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로파일 유형 및 필수 **McAfee ePO** 역량

프로파일의 기본 목적	요구 사항 설정	이 프로파일 유형에 필요한 **McAfee ePO** 기능
시스템 상세 정보 수집	안 함	호스트 상세 정보 가져오기
호스트 격리	McAfee ePO 콘솔에서 호스트 격리 작업에 McAfee ePO 대한 보안 태그를 생성했는지 관리자에게 확인하십시오. 자세한 내용은 McAfee ePO(SIR)과 보안 인시던트 응답 통합하도록 콘솔 설정 문서를 참조하십시오.	호스트 분리
호스트에서 위협 스캔 및 검색	McAfee ePO 콘솔에서 맬웨어 검사 시작 작업에 McAfee ePO 대한 보안 태그를 생성했는지 관리자에게 확인하십시오. 자세한 내용은 McAfee ePO(SIR)과 보안 인시던트 응답 통합하도록 콘솔 설정 문서를 참조하십시오.	맬웨어 스캔 시작 **주:** 맬웨어 검사의 McAfee ePO 일부로 위협 이벤트 나열 기능이 자동으로 호출됩니다. 그러나 맬웨어 검사 기능을 사용하여 프로필에 위협 이벤트 나열 기능을 추가할 필요는 없습니다. 맬웨어 검사 결과는 보안 인시던트의 위협 이벤트 상세 정보 탭에 표시됩니다.
호스트에 대한 격리 제거	McAfee ePO 콘솔에서 호스트 격리 작업에 McAfee ePO 대한 보안 태그를 생성했는지 관리자에게 확인하십시오. 자세한 내용은 McAfee ePO(SIR)과 보안 인시던트 응답 통합하도록 콘솔 설정 문서를 참조하십시오.	격리 제거
위협 보강 데이터를 수집합니다.	안 함	위협 이벤트 나열

역량 프로파일 생성

프로파일을 생성하고 프로파일을 실행할 기능을 선택합니다 McAfee ePO .

시작하기 전에

필요한 역할: ServiceNow AI Platform# 보안 인시던트 관리자(sn_si.admin)

이 태스크 정보

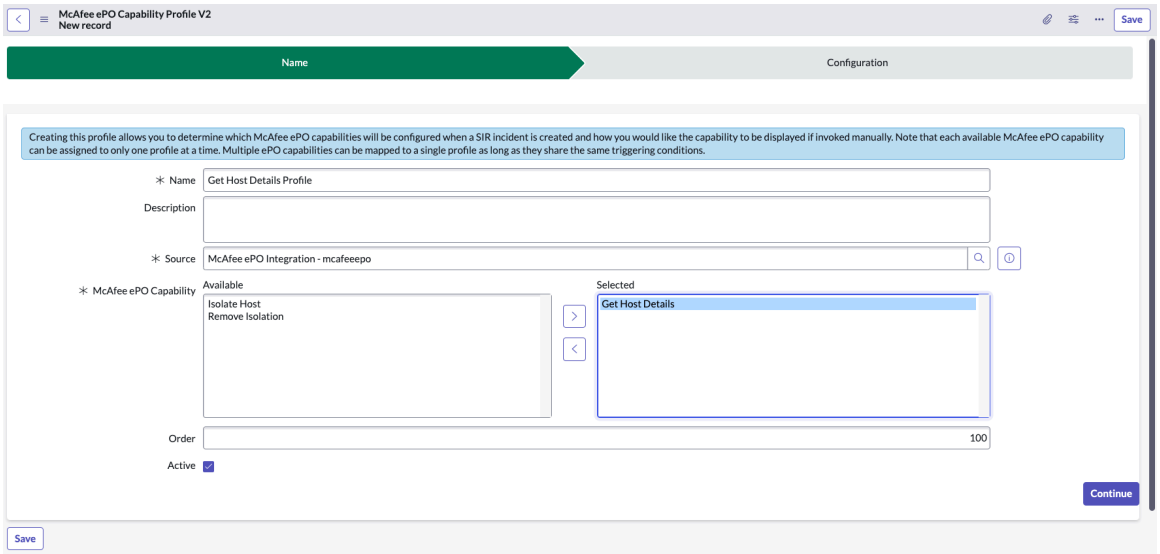
구성의 이 단계에서는 기능에 대한 McAfee ePO 프로필을 생성합니다. 프로파일을 만들 때는 프로파일에 역량을 추가하기 McAfee ePO 전에 프로파일의 의도를 고려하십시오. 프로파일을 생성할 때 다음 테이블을 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음 표에서는 프로필에서 특정 쿼리 또는 작업을 수행하려는 경우 프로필에 추가해야 하는 기능을 보여 줍니다. 호스트 상세 정보에 대한 쿼리를 실행하고, 맬웨어 검사를 시작하고, 격리를 제거하고, 호스트 시스템을 격리하는 단일 프로파일을 생성하거나, 각각 고유한 단일 기능을 가진 여러 프로파일을 생성합니다.

프로시저

1. 다음으로 이동 **McAfee ePO** 통합 〉 **McAfee ePO** 기능 프로파일.
   McAfee ePO 역량 프로파일 목록이 표시됩니다.
2. 새로 만들기를 클릭합니다.
3. 양식에서 필드에 입력합니다.



4. 프로파일을 저장하고 유효성을 검사하려면 계속을 클릭합니다.
   확인에 성공하면 페이지가 다시 로드되고 구성 양식이 표시됩니다.

다음에 수행할 작업

다음 단계는 프로필을 구성하는 것입니다. 프로필에 대한 설정을 구성하기 전에 프로필 구성 및 트리거 조건에 대한 개념을 검토하는 것이 좋습니다. 자세한 내용은 AND CI(구성 항목) 필드로 트리거 조건 정의 문서를 참조하십시오McAfee ePO(SIR)과 보안 인시던트 응답 통합하도록 콘솔 설정.

CI(구성 항목) 필드로 트리거 조건 정의

프로필을 만들고 프로필에서 실행할 기능을 선택한 McAfee ePO 후 특정 조건 집합이 충족되는 경우에만 실행되도록 프로필의 설정을 구성합니다.

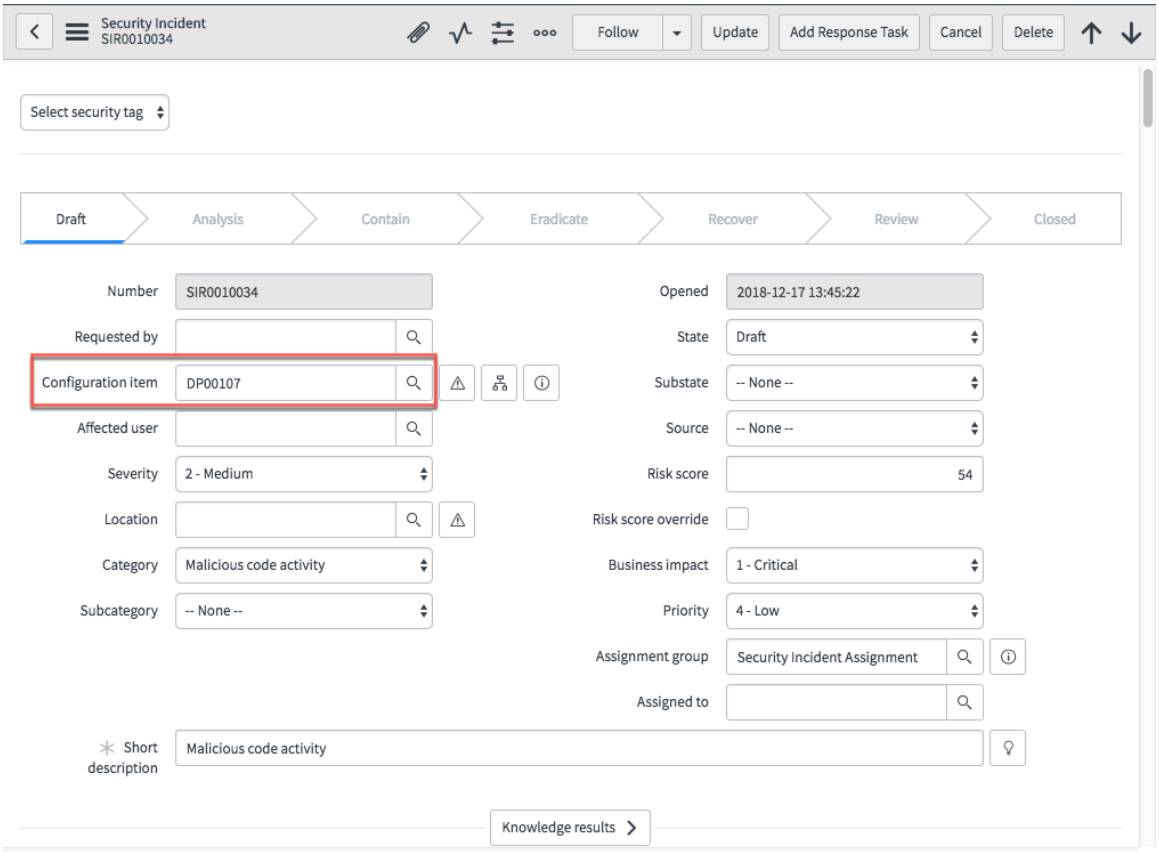
보안 인시던트와 ServiceNow AI Platform# 보안 인시던트 응답 일치하는 기본 필드 값에 따라 프로파일이 자동으로 실행되도록 이러한 트리거 조건을 유연하게 설정할 수 있습니다. 또는 보안 인시던트에서 구체적으로 식별한 필드 값의 일치 항목을 검색하도록 프로파일을 설정할 수 있습니다.

통합 기능과 프로파일 작동 방식에 대한 핵심 중 하나는 (SIR) 보안 인시던트의 ServiceNow AI Platform# 보안 인시던트 응답 CI(구성 항목) 필드입니다. 이 필드의 값은 보안 인시던트의 원칙 값입니다. 이 값은 자산 ID를 데이터베이스에 저장된 ServiceNow AI Platform# 정보와 일치시키는 데 사용됩니다. SIR 보안 이벤트에 의해 보안 인시던트가 생성되고 프로파일이 활성화되면 구성 항목 필드의 값을 기준으로 FQDN(정규화된 도메인 이름), 호스트 이름 또는 IP 주소와 일치하는 값을 찾기 위해 자산을 검색합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이상적인 케이스는 데이터베이스에서 일치하는 값을 찾은 다음, 일치하는 자산에 대한 데이터를 콘솔에서 수집 McAfee ePO 하여 인스턴스로 ServiceNow AI Platform# 가져와서 보안 인시던트의 관련 목록에 표시하는 것입니다. 다음 그림은 보안 인시던트에서 SIR 호스트 이름으로 채워진 구성 항목 필드의 예를 보여줍니다.

보안 인시던트 - 구성 항목



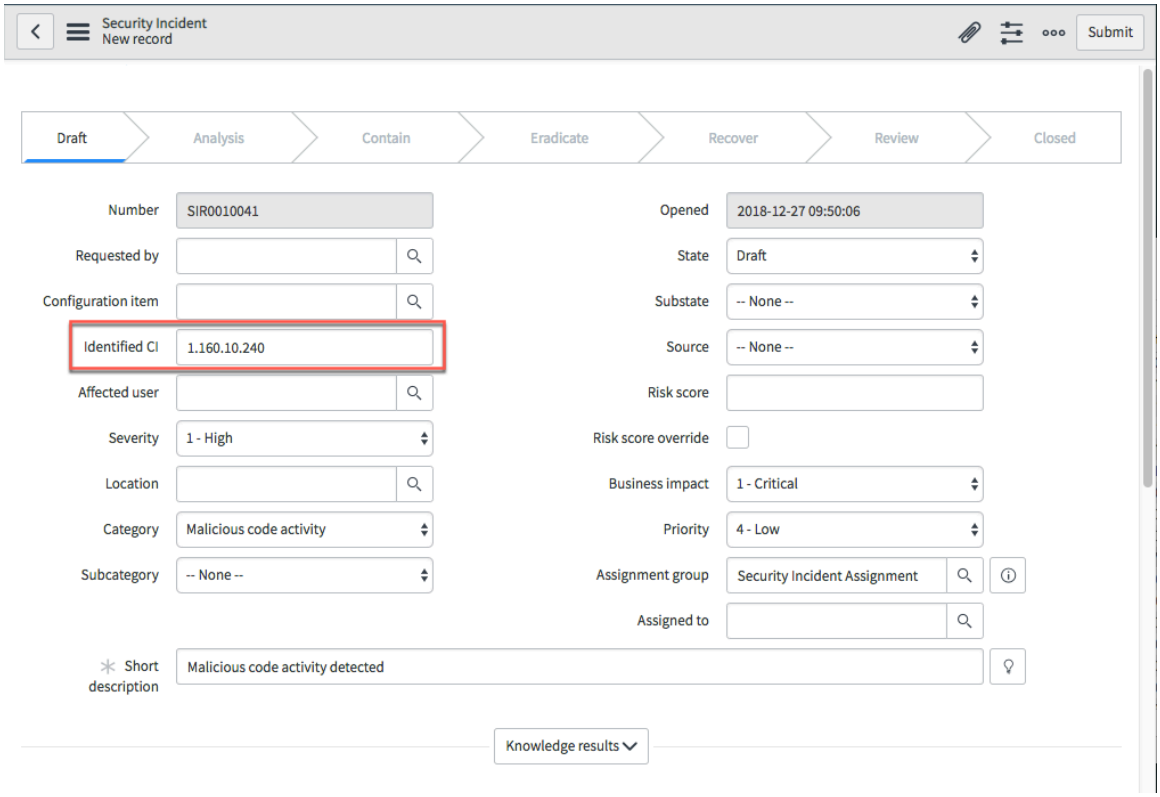
보안 인시던트에서 CI(구성 항목) 필드가 채워지지 않았거나 데이터베이스와 일치하는 FQDN, 호스트 이름 또는 IP 주소와 일치하는 항목을 찾을 수 없는 경우 보안 인시던트에서 대체 필드를 선택하여 자산 스캔 중에 발견된 일치하는 CI 보강 데이터를 표시할 수 있습니다.

프로파일 설정의 구성 단계에서 엔드포인트 식별을 위한 대체 CI 트리거 필드를 선택하여 조회의 McAfee ePO CI 보강 데이터가 연결된 보안 인시던트에 채워지도록 할 수 있습니다. 생성한 사용자 지정 필드를 비롯한 대체 CI 트리거 필드로 보안 인시던트의 모든 필드를 선택할 수 있습니다. 이 대체 CI 필드를 백업으로 선택하면 인시던트 생성 시 연관된 보안 인시던트에 CI 필드가 채워지지 않아도 프로파일이 실행되도록 할 수 있습니다.

예를 들어, 보안 운영 센터(SOC) 분석가가 내 보안 인시던트의 IP 주소라는 보안 인시던트에 대한 사용자 지정 필드를 생성합니다. 인시던트 생성 시 이 사용자 지정 필드의 값이 보안 인시던트의 구성 항목 필드에 표시되지 않을 것으로 생각되면 이 IP 주소를 스캔하도록 프로파일을 설정할 수 있습니다. 일치하는 경우 선택한 필드의 보안 인시던트에 IP 주소가 표시됩니다. 다음 그림에서 ### CI 필드가 이 예시의 IP 주소에 대한 대체 필드로 선택됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

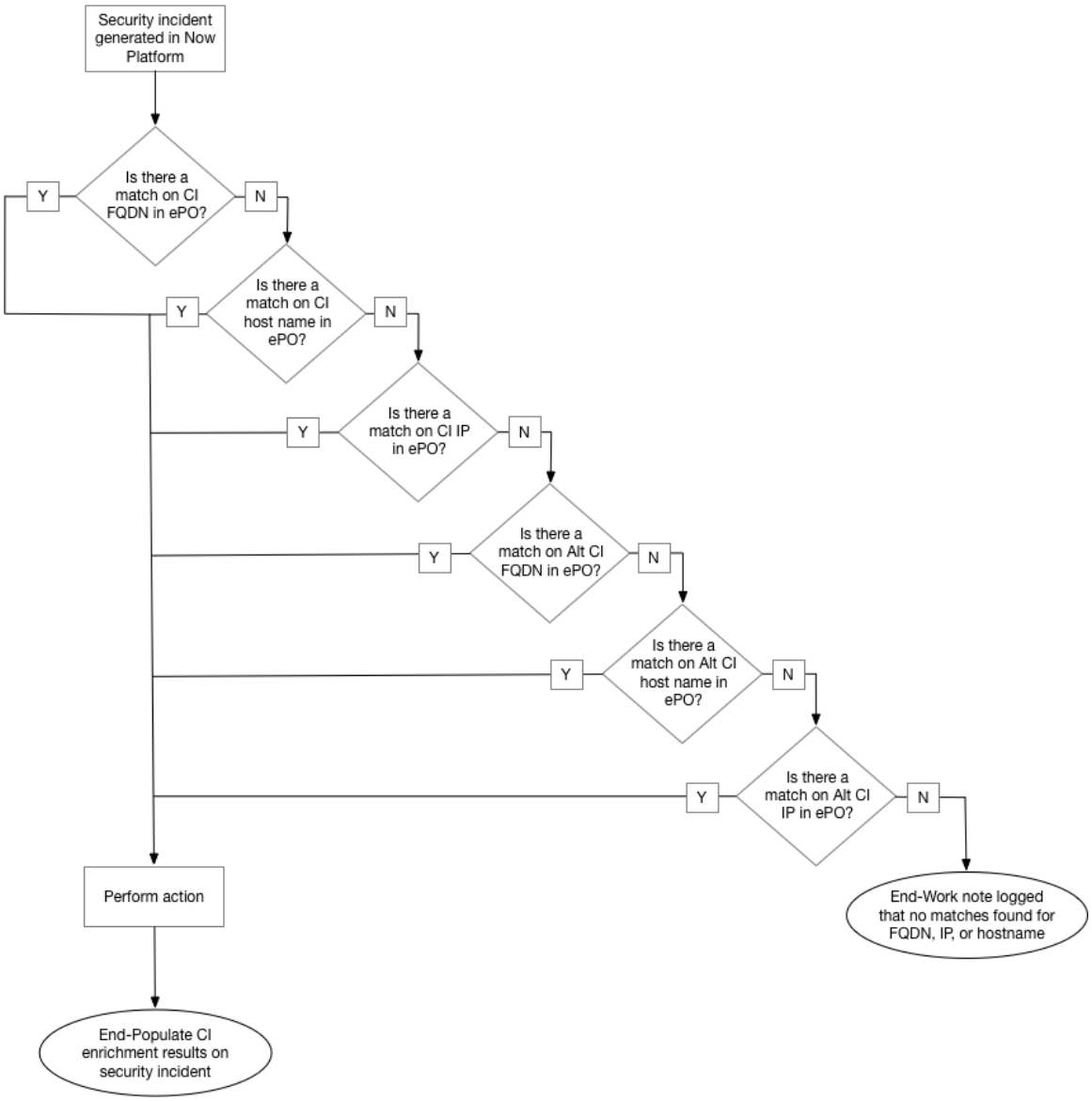
보안 인시던트 - 식별된 CI



다음 그림에서는 워크플로의 첫 번째 검색에서 구성 항목의 일치 항목을 검색하는 방법을 보여 줍니다. 대체 CI 트리거 필드가 활성화된 경우 두 번째 검색에서 대체 값의 일치 항목을 검색합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

구성 항목 워크플로우



CI 필드 또는 대체 CI 필드에 대해 일치하는 ID를 찾을 수 없는 경우 작업 메모가 기록되고 보안 인시던트에 메시지가 표시됩니다. 일치하는 항목이 없으면 이벤트와 관련된 보안 인시던트에 대한 보강 데이터가 채워지지 않습니다.

대체 CI 트리거 필드를 활성화하고 프로파일의 구성 단계에서 일치하는 ID를 표시할 필드를 선택합니다. 대체 CI 필드를 활성화하는 이 단계는 다른 프로파일 구성 요구 사항과 함께 에 설명되어 있습니다 설정 구성.

설정 구성

프로필을 만들고 프로필을 실행할 기능을 선택한 McAfee ePO 후 정의한 특정 조건에서만 프로필이 호출되도록 설정을 구성합니다.

프로파일 구성

이 단계에서는 지정한 조건이 충족되는 경우에만 실행되도록 역량 프로파일을 구성합니다. 프로파일에 대해 선택한 기능을 자동으로 트리거 McAfee ePO 하는 보안 인시던트의 조건을 정의합니다. 또한 CI(구성 항목) 필드에 대한 대체 입력 필드를 선택하고 필터링 조건을 설정하여 트리거 이벤트와 관련된 보안 인시던트만 프로파일을 자동으로 시작하도록 할 수 있습니다. 구성 단계에서는 프로파일의 구성 양식에 다음 설정을 포함합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

대체 구성 항목(CI) 트리거 필드

(SIR) 보안 인시던트의 ServiceNow AI Platform# 보안 인시던트 응답 CI(구성 항목) 필드가 값으로 채워지지 않았거나 데이터베이스에서 일치하는 항목을 찾을 수 없는 경우 보안 인시던트에서 대체 필드를 선택하여 자산 스캔 중에 발견된 일치하는 CI 보강 데이터를 표시할 수 있습니다. 보안 인시던트의 구성 항목 및 대체 구성 항목 필드에 대한 자세한 내용은 다음 문서를 참조하십시오 CI(구성 항목) 필드로 트리거 조건 정의.

보안 태그

격리된 호스트 시스템의 상태와 맬웨어 검사가 시작되는 시기를 추적하는 데 도움이 되도록 선택적 태그 지정 기능을 사용할 수 있습니다. 기본적으로 이 옵션은 프로파일의 구성 양식에서 사용할 수 없습니다. 구성 단계에서 이 옵션을 사용하도록 설정하면 구성 양식에 보안 태그 이름이 표시됩니다. 관련 보안 인시던트에 표시되는 태그의 이름입니다. 이러한 태그는 호스트 분리 작업이 성공적으로 시작되고 승인되는 시기를 알려줍니다. 호스트가 네트워크에 성공적으로 반환되면 보안 태그가 보안 인시던트에서 자동으로 제거됩니다. 맬웨어 검사의 경우 검사가 예약되면 관련 보안 인시던트에 태그가 표시됩니다. 스캔이 완료되면 예약된 태그는 스캔이 성공적으로 완료되었음을 나타내는 태그로 자동 대체됩니다.

인시던트를 기반으로 자동 트리거

인시던트를 기반으로 자동 트리거 옵션을 사용하는 경우 필터 조건 작성기를 사용할 수 있으며 프로파일이 자동으로 실행되는 시기를 지정하는 필터링 조건을 설정해야 합니다. 일반적인 필터는 범주는 악성 코드 활동이고™비즈니스 영향은 1 - 중요입니다™. 이러한 필터를 사용하면 악성 코드와 관련이 있으며 비즈니스에 중대한 영향을 미치는 보안 인시던트만 프로파일을 시작합니다. 자동 트리거 옵션을 사용하면 프로파일을 자동으로 호출하는 보안 인시던트 수를 줄일 수 있습니다.

승인

조직에서 호스트 컴퓨터 격리 및 맬웨어 검사 시작과 같은 작업에 대한 추가 제어 수준을 원하는 경우 프로파일의 구성 단계에서 승인 필요 옵션을 활성화할 수 있습니다.

예를 들어 프로파일에 승인 및 태그 지정 기능이 모두 활성화된 경우 호스트 시스템을 격리하거나 승인을 위해 네트워크로 반환하는 요청이 제출되면 작업이 시작되었음을 알리는 태그가 연결된 보안 인시던트에 자동으로 지정됩니다. 요청은 기본적으로 sn_si.admin 역할을 가진 사용자에게 승인을 위해 전송되지만 이 승인은 조직의 필요에 맞게 다른 개인 또는 승인 그룹에 재할당할 수 있습니다. 승인자는 인스턴스의 ServiceNow AI Platform#내 승인에서 요청을 처리합니다. 관련 보안 인시던트에 보안 태그가 표시됩니다. 감사 추적을 생성하기 위해 모든 워크플로우 활동도 작업 메모에 기록됩니다.

ServiceNow 콘솔의 McAfee ePO 감사 로그

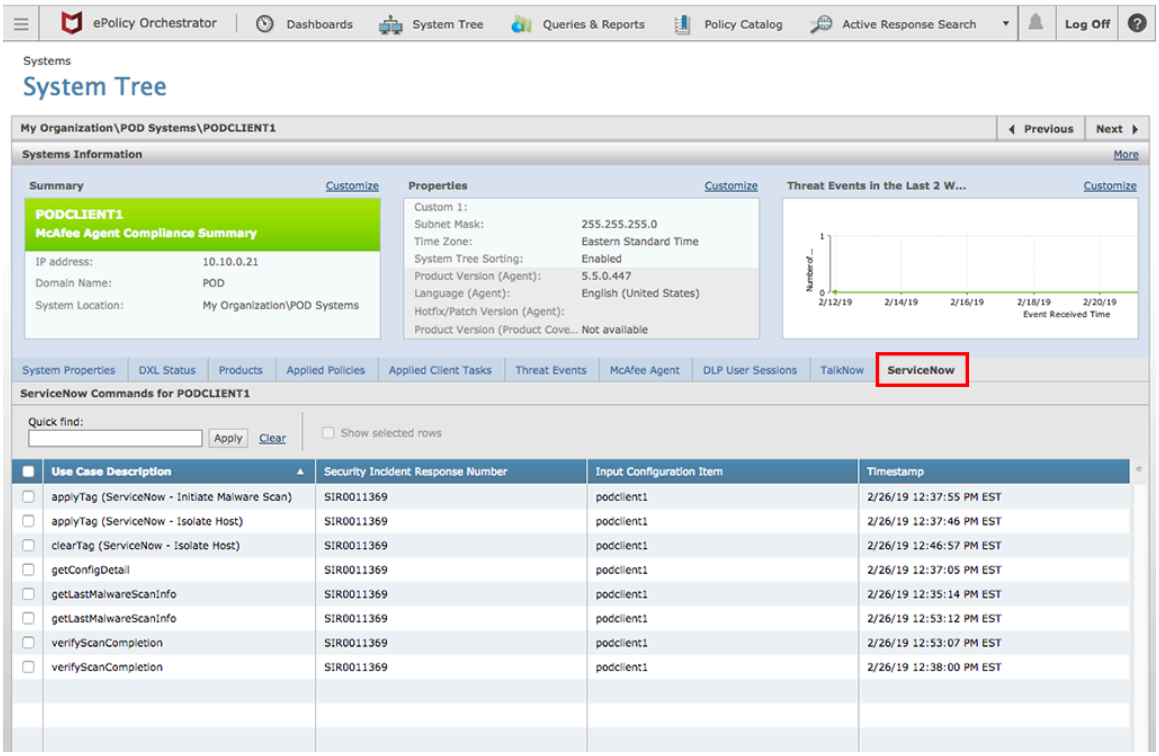
버전 5.10.0 McAfee ePOServiceNow 에서는 인스턴스에서 시작된 ServiceNow AI Platform# 명령 로그가 포함된 탭이 표시됩니다. 콘솔의 호스트 머신(엔드포인트)McAfee ePO에 있는 인스턴스의 프로파일 ServiceNow AI Platform# 에서 작업 또는 쿼리를 호출한 후 콘솔에 명령의 감사 로그 ServiceNow 가 생성됩니다McAfee ePO. 이 로그는 콘솔의 McAfee ePO 시스템 트리에 표시되며 특정 엔드포인트로 전송된 명령의 시간을 감사하는 데 도움이 됩니다. 콘솔의 McAfee ePO 특정 머신에 기록된 ServiceNow 이벤트를 보려면 다음 단계를 수행합니다.

1. 콘솔에서 시스템 트리 McAfee ePO 로 이동하여 탭을 찾습니다 ServiceNow .
2. 탭을 클릭하여 호스트 시스템 목록을 엽니다.
3. 이름 열에서 호스트 이름을 클릭하여 감사 로그를 엽니다.

다음 이미지에는 호스트(PODCLIENT1)에 대한 로그의 예가 표시되어 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

포드클리언트



인스턴스의 프로파일 ServiceNow AI Platform# 에서 시작된 이벤트가 기록되고 로그에 표시됩니다. 호스트 시스템의 상태를 확인하여 로그에 나열된 이벤트가 호스트에서 성공적으로 완료되었는지 확인합니다.

예시 프로파일

다음 주제에는 프로파일을 구성하고 보안 인시던트를 테스트하는 방법에 대한 예가 포함되어 있습니다. 이러한 예에는 이 통합에 사용할 수 있는 모든 McAfee ePO 역량에 대한 프로파일이 포함되어 있습니다.

시스템 보강 쿼리에 대한 프로파일 및 보안 인시던트 구성

설정한 조건에서만 프로파일이 트리거되도록 프로파일 설정을 구성합니다.

시작하기 전에

필요한 역할: ServiceNow AI Platform# 보안 인시던트 관리자(sn_si.admin)

이 태스크 정보

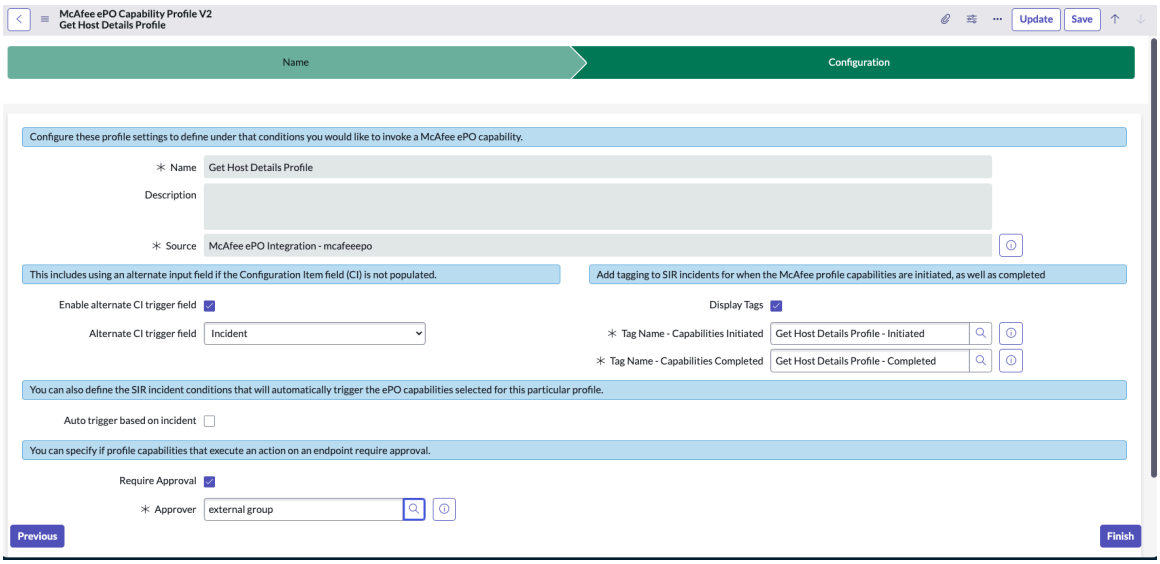
프로파일에 대해 선택한 기능을 자동으로 트리거 McAfee ePO 하는 조건을 정의합니다. CI(구성 항목) 필드에 대해 대체 입력 필드를 선택할 수도 있습니다. 이 대체 필드에서는 트리거 이벤트와 관련된 보안 인시던트만 프로파일을 자동으로 트리거하도록 필터링 조건을 설정할 수 있습니다.

프로시저

1. 구성 페이지가 표시되지 않으면 진행률 표시줄에서 구성을 클릭합니다.

2. 양식에서 필드를 채웁니다

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



3. 대체 CI 필드 옵션을 활성화하고 이 프로파일을 자동으로 호출하는 필터링 조건을 설정하려면 다음 단계를 수행합니다.

   a. 대체 **CI** 트리거 필드 사용 확인란을 선택합니다.
   대체 CI 트리거 필드가 표시됩니다. 이 예에서는 sn_si.admin 역할을 가진 사용자는 인시던트 생성 시 보안 인시던트의 CI 필드가 채워지지 않을 것으로 예상합니다. 또는 FQDN, 호스트 이름 또는 IP 주소에 대한 CI 정보가 보안 인시던트의 ### CI 필드에 채워질 것으로 생각하고 식별된 CI 필드를 대안으로 선택합니다. 이 예에서는 식별된 CI가 선택되었지만 대체 CI에 대한 보안 인시던트의 모든 필드를 사용할 수 있습니다.

   b. 표시되는 대체 **CI** 트리거 필드 선택 목록에서 식별된 **CI** 필드를 선택합니다.

   보안 인시던트에서 사용 가능한 모든 필드가 사용자 지정 필드를 포함하여 목록에 표시됩니다. 대체 CI 트리거 필드에 ### CI 가 표시됩니다.

   이 프로파일이 호출되고 초기 이벤트 트리거 시 연관된 보안 인시던트에 CI 필드가 채워지지 않으면 프로파일은 검색에서 식별된 CI 필드의 값을 사용합니다.

   c. 인시던트를 기반으로 자동 트리거 확인란을 선택합니다.
   필터 조건 작성기가 표시됩니다. 이 옵션을 사용하여 필터링 조건을 설정하고 보안 인시던트 생성 시 프로파일이 자동으로 호출되는 시기를 지정합니다.

   d. 이 특정 프로파일에 대해 선택된 ePO 기능을 자동으로 트리거하는 SIR 인시던트 조건을 정의합니다.

   e. 엔드포인트에서 작업을 실행하는 프로파일 기능에 승인이 필요한 경우 승인 필요 확인란을 선택합니다.

   f. 검색 아이콘을 사용하여 승인을 선택합니다.

4. 마침을 클릭합니다.
   인시던트 작성 시 프로파일이 자동으로 트리거되고 대체 필드를 사용하여 일치하는 CI 결과를 채우도록 프로파일을 성공적으로 구성했습니다.

맬웨어 검사를 시작하도록 프로파일 구성

맬웨어 검사 시작 기능 및 프로필을 실행하려는 다른 McAfee ePO 기능을 사용하여 프로필을 만든 후 정의한 특정 조건에서 호출되도록 프로필의 설정을 구성합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

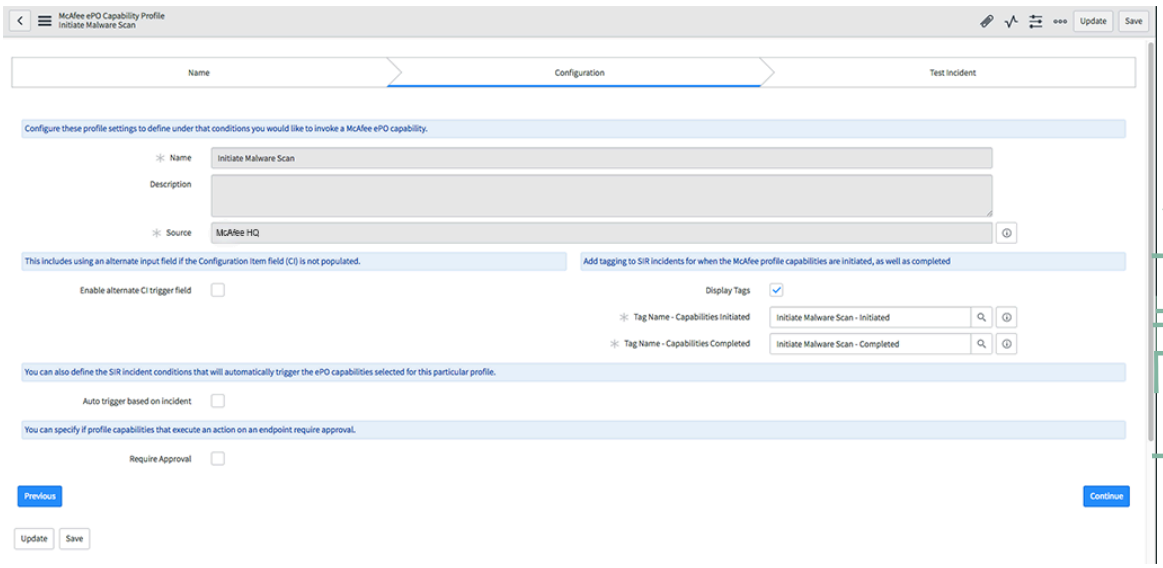
시작하기 전에
필요한 역할: sn_si.admin

이 태스크 정보
sn_si.admin 역할을 가진 사용자는 (SIR) 보안 인시던트에서 ServiceNow AI Platform 보안 인시던트 응답 지정한 조건이 충족될 때만 검사를 예약하도록 프로파일을 구성합니다. 스캔을 트리거하는 보안 인시던트의 조건을 정의합니다. 프로파일에 대해 선택하는 다른 McAfee ePO 모든 기능은 트리거 조건을 공유합니다. CI(구성 항목) 필드에 대한 대체 입력 필드를 선택하고 필터링 조건을 설정하는 옵션을 사용할 수 있습니다. 트리거 이벤트와 관련된 보안 인시던트만 SIR 자동으로 프로파일을 호출하도록 필터링을 설정할 수 있습니다.

호스트 격리 작업과 마찬가지로 보안 인시던트에서 SIR 직접 요청 시 검사를 시작할 수 있습니다. 수동으로 검사를 시작하는 방법에 대한 자세한 내용은 문서를 참조하십시오 보안 인시던트에서 수동으로 프로파일 트리거 McAfee ePO.

프로시저

1. 구성 페이지가 표시되지 않으면 진행률 표시줄에서 구성을 클릭합니다.



구성 양식이 표시됩니다.

2. 양식을 작성합니다.

이 예에서는 프로파일에 대해 승인 및 태그 지정 옵션을 사용할 수 있습니다. 대체 CI 트리거 사용 필드 및 인시던트 옵션에 따라 자동 트리거를 구성하는 방법에 대한 자세한 내용은 다음 문서를 시스템 보강 쿼리에 대한 프로파일 및 보안 인시던트 구성참조하십시오.

3. 계속하려면 하나의 옵션을 선택하십시오.
인시던트 작성 시 맬웨어 스캔이 자동으로 트리거되도록 프로파일을 성공적으로 구성했습니다. 대체 CI 필드는 스캔에서 일치하는 CI 결과를 채우는 데 사용됩니다. 다음 단계는 이 프로파일에 대한 보안 인시던트를 미리 보고 테스트하는 것입니다.

보안 인시던트에서 수동으로 프로파일 트리거 **McAfee ePO**

(SIR) 보안 인시던트에서 역량 프로파일을 수동으로 트리거합니다 ServiceNow AI Platform 보안 인시던트 응답 .

시작하기 전에
필요한 역할: sn_si.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
의 설정 구성 승인 옵션은 호스트 격리 및 호스트 격리 제거 기능에만 표시됩니다.

이 태스크 정보

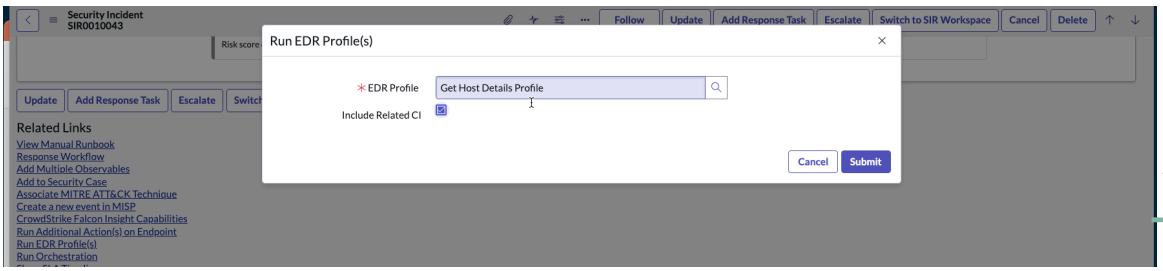
프로파일에 지정한 트리거 조건이 보안 인시던트의 조건과 일치하는 경우 호스트 상세 정보 가져오기, 호스트 컴퓨터 격리 또는 컴퓨터 격리 제거 요청을 자동으로 호출할 수 있습니다. 또는 수동으로 요청을 제출하려면 보안 인시던트에서 직접 요청을 제출합니다.

프로파일을 활성화하면 구성된 트리거 조건에 따라 보안 인시던트에서 ServiceNow AI Platform 쿼리 결과를 볼 수 있습니다. McAfee ePO 또한 통합을 사용하면 프로파일을 사용하지 않고 CI(구성 항목)에서 개별 역량을 실행할 수 있습니다.

프로시저

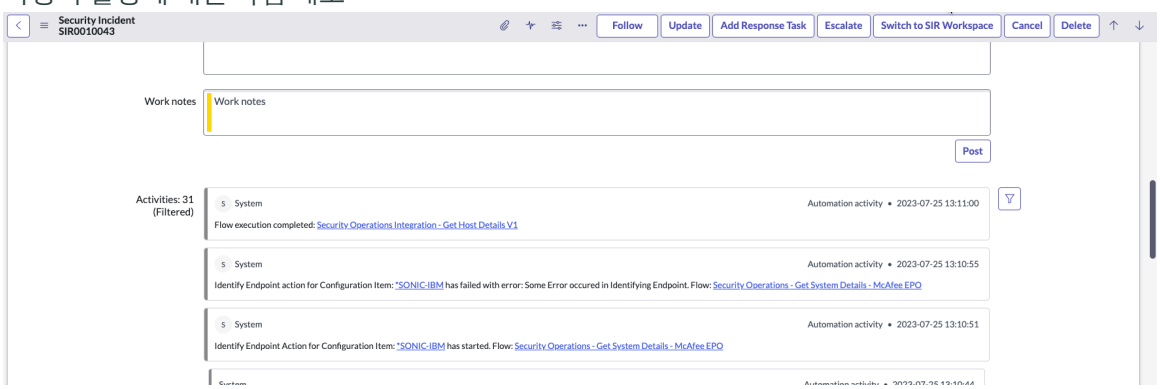
1. 다음으로 이동 모두 〉 보안 인시던트 〉 모든 인시던트 표시.
2. 정보로 검토하려는 보안 인시던트를 McAfee ePO 선택합니다.
3. 관련 목록 섹션에서 **EDR** 프로파일 실행을 선택합니다.

McAfee 실행 **EDR** 프로파일



4. 사용 가능한 프로파일 목록에서 프로파일을 찾아 선택합니다.
   사용 가능한 프로파일 목록에는 호스트 상세 정보 가져오기, 호스트 컴퓨터 격리 및 격리 제거가 있습니다. 예를 들어 호스트 상세 정보 가져오기를 선택해 보겠습니다.
5. 프로파일의 모든 관련 CI에서 이 프로파일을 실행하려면 관련 **CI** 포함 을 선택합니다.
   예를 들어 보안 인시던트와 연결된 CI가 5개 있는 경우 선택한 프로파일이 5개의 CI 모두에서 실행됩니다.
6. 제출을 클릭합니다.
   선택한 프로파일이 수동으로 트리거됩니다. 작업 메모 섹션에서 작업 메모 및 활동 섹션과 프로파일 시작 및 프로파일 완료 태그를 검토할 수 있습니다.

자동화 활동에 대한 작업 메모

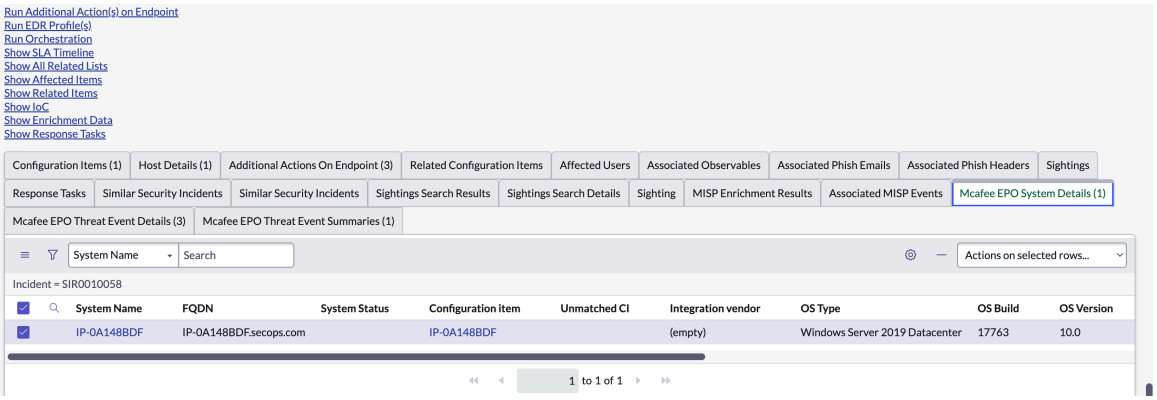


결과는 호스트 상세 정보 가져오기, 호스트 컴퓨터 격리 또는 격리 제거와 같은 관련 목록의 형태로 나타납니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
모든 관련 목록 테이블은 기본 테이블을 확장합니다. 이 예에서 McAfee EPO 시스템 상세 정보는 호스트 상세 정보 기본 테이블의 확장된 테이블입니다.

McAfee 관련 목록



7. CI(구성 항목)에서 개별 기능을 실행하려면 다음 단계를 수행합니다.

a. 구성 항목 관련 목록에서 필요한 CI를 선택합니다.

b. 선택한 행에 대해 수행할 작업... 드롭다운 목록을 클릭하고 선택한 CI에 대해 실행할 필수 기능을 선택합니다.
예: 호스트 격리.

c. 호스트 격리를 클릭하여 선택한 CI에서 실행합니다.
선택한 CI가 네트워크에서 격리됩니다.

통합에서 **McAfee ePO** 추가 작업 트리거

위협 이벤트 나열 및 맬웨어 검사 시작 기능은 추가 작업 실행에서 트리거할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.admin

이 태스크 정보
위협 이벤트 나열 및 McAfee ePO 맬웨어 스캔 시작 기능을 포함하는 McAfee ePO엔드포인트에서 추가 작업 실행을 사용하여 통합 활성화에서 McAfee ePO 추가 작업을 구성하고 트리거할 수 있습니다.

프로시저

1. 다음으로 이동 보안 인시던트 〉 모든 인시던트 표시.

2. 추가 작업을 실행할 보안 인시던트를 선택합니다.

3. 관련 링크 섹션에서 엔드포인트에서 추가 작업 실행을 클릭합니다.

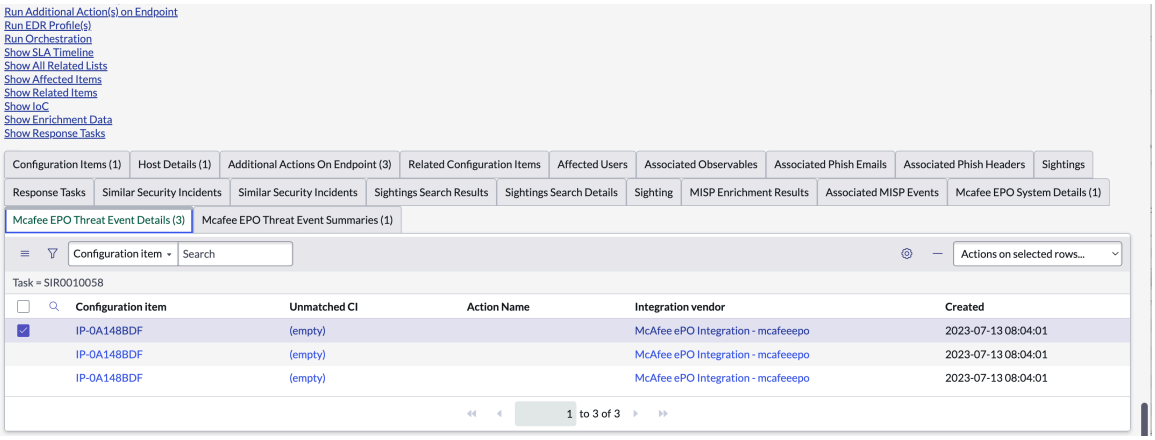
4. 추가 작업 목록에서 트리거할 역량 구현을 찾아 선택합니다.
위협 이벤트 나열을 예로 들 수 있습니다 McAfee ePO .

5. 프로파일의 모든 관련 CI에 대해 이 추가 작업을 실행하려면 관련 **CI** 포함 을 선택합니다.
예를 들어 보안 인시던트와 연결된 CI가 5개 있는 경우 선택한 프로파일이 5개의 CI 모두에서 실행됩니다.

6. Run Additional Actions(추가 작업 실행)를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

McAfee ePO 위협 이벤트 상세 정보



주:
모든 관련 목록 테이블은 기본 테이블을 확장합니다. 이 예에서 McAfee EPO 위협 이벤트 상세 정보 테이블은 엔드포인트에 대한 추가 작업 기본 테이블의 확장된 테이블입니다.

7. 관련 목록에서 McAfee ePO 위협 이벤트 상세 정보를 보고 확인합니다.

분석가 작업 공간에서 통합 사용 **McAfee ePO**

McAfee ePO 통합을 사용하여 SIR 분석가 작업 공간의 기능을 활용합니다McAfee ePO.

시작하기 전에
필요한 역할: sn_si.admin

보안 인시던트 응답 작업 공간에서 통합을 사용하려면 McAfee ePO 먼저 에서 ServiceNow Store 다운로드하여 구성해야 합니다. 자세한 내용은 ServiceNow AI Platform 통합을 위한 McAfee ePO 인스턴스 설정 문서를 참조하십시오.

이 태스크 정보
통합을 사용하여 McAfee ePO 엔드포인트에서 실시간으로 정정 작업을 수행하고, 프로필을 사용하여 호스트에 대한 상세 정보를 수집하고, 작업 공간을 사용하여 엔드포인트에서 특정 쿼리 또는 작업을 수행할 수 있습니다 보안 인시던트 응답 .

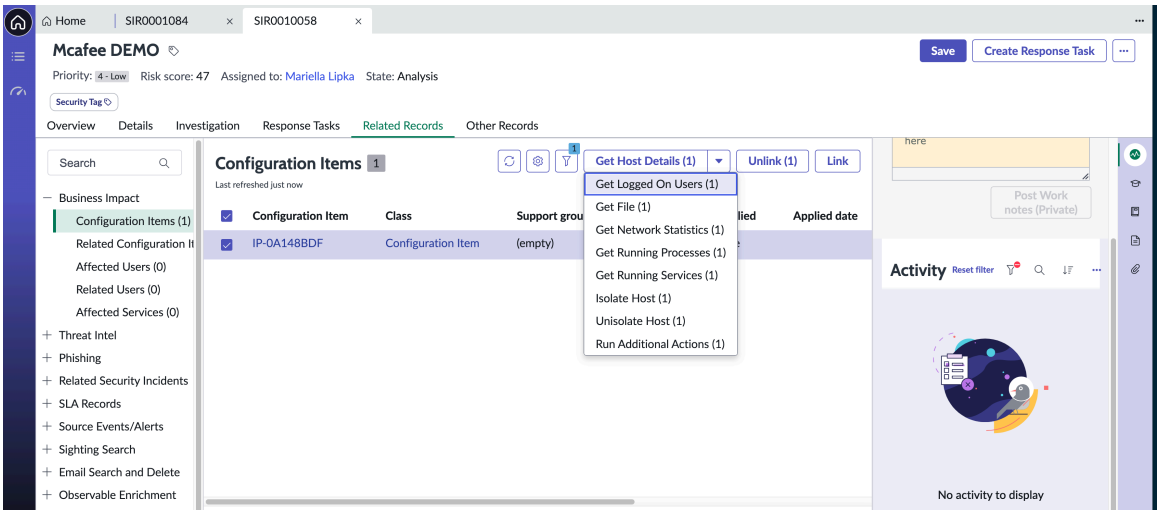
통합을 통해 McAfee ePO 분석가는 분석가 작업 공간에서 보안 인시던트 응답 다음 McAfee ePO 기능을 사용할 수 있습니다.

- 호스트 상세 정보 가져오기
- 호스트 분리
- 격리 제거
- 엔드포인트에서 추가 작업 실행

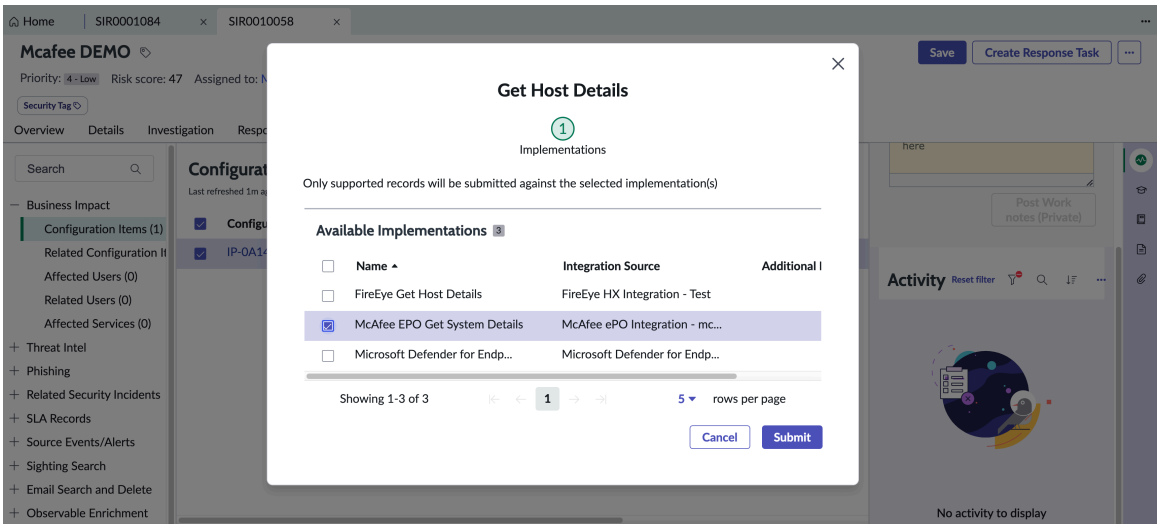
프로시저

1. SIR 작업 공간에서 보안 인시던트를 열려면 보안 인시던트에서 **SIR** 작업 공간으로 전환을 클릭하십시오.
2. SIR 작업 공간에서 관련 기록 탭을 선택합니다.
3. 구성 항목을 선택하고 관련 목록 드롭다운 작업에서 트리거할 McAfee ePO 기능을 선택합니다. 예를 들어 호스트 상세 정보 가져오기가 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 호스트 상세 정보 가져오기 팝업에서 **McAfee ePO** 구현을 선택합니다.



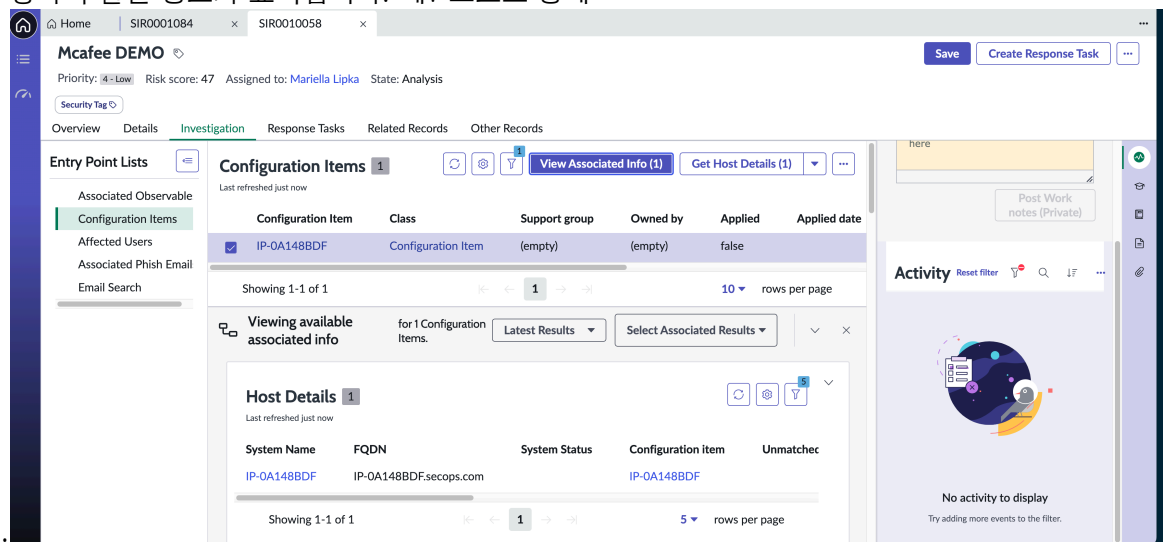
5. 제출을 클릭합니다.
호스트 상세 정보 가져오기 기능은 CI에서 호출됩니다. 결과 및 결과에 대한 작업 주석을 볼 수 있습니다.

6. 트리거된 역량에 대한 데이터를 보려면 조사 탭을 선택합니다.

7. 구성 항목을 선택하고 관련 정보 보기 작업을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

구성 항목의 관련 정보가 표시됩니다. 예: 호스트 상세 정보.



8. 구성 항목을 클릭하여 호스트 세부 정보를 봅니다.
   마찬가지로 SIR 분석가 작업 공간에서 보안 인시던트에 다른 McAfee ePO 기능을 사용해 볼 수 있습니다.
9. 분석을 위해 엔드포인트 탐지 및 응답**(EDR)** 관련 목록에서 McAfee ePO 기능을 사용할 수 있습니다.
10. 사용 가능한 프로파일 목록에서 프로파일을 찾아 선택합니다.
    사용 가능한 프로파일 목록에는 호스트 상세 정보 가져오기, 호스트 컴퓨터 격리 및 격리 제거가 있습니다. 예를 들어 호스트 상세 정보 가져오기를 선택해 보겠습니다.
11. **McAfee ePO** 구현을 선택하고 제출을 클릭합니다.

보안 인시던트를 테스트하여 맬웨어 스캔 시작

맬웨어 검사에 대한 프로필을 구성한 후 프로필을 테스트하고 프로필의 설정과 일치하는 보안 인시던트를 확인합니다. (SIR) 보안 인시던트의 ServiceNow AI Platform 보안 인시던트 응답 관련 목록에서 검사 결과를 미리 봅니다.

시작하기 전에

필요한 역할: sn_si.admin

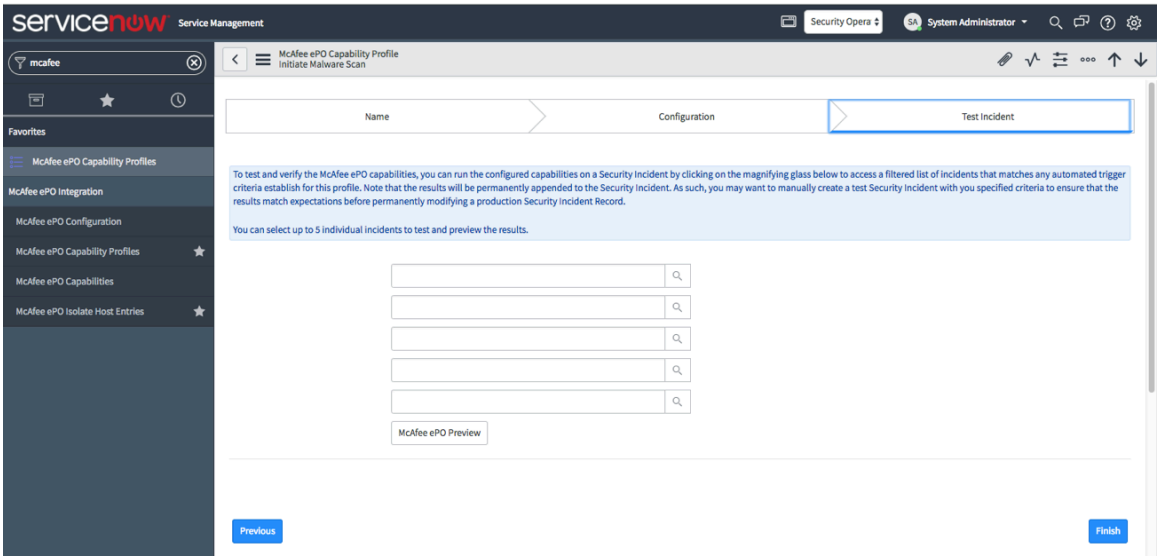
이 태스크 정보

sn_si.admin 역할을 가진 사용자는 맬웨어 검사 기능이 있는 프로파일이 호출되고 검사 검색 결과가 ()SIR 보안 인시던트의 ServiceNow AI Platform 보안 인시던트 응답 관련 목록 미리 보기와 예상되는 것과 일치하는지 확인합니다. 미리 보기를 사용하면 프로파일에 대해 스캔 결과가 예상대로 반환되는지 확인할 수 있습니다.

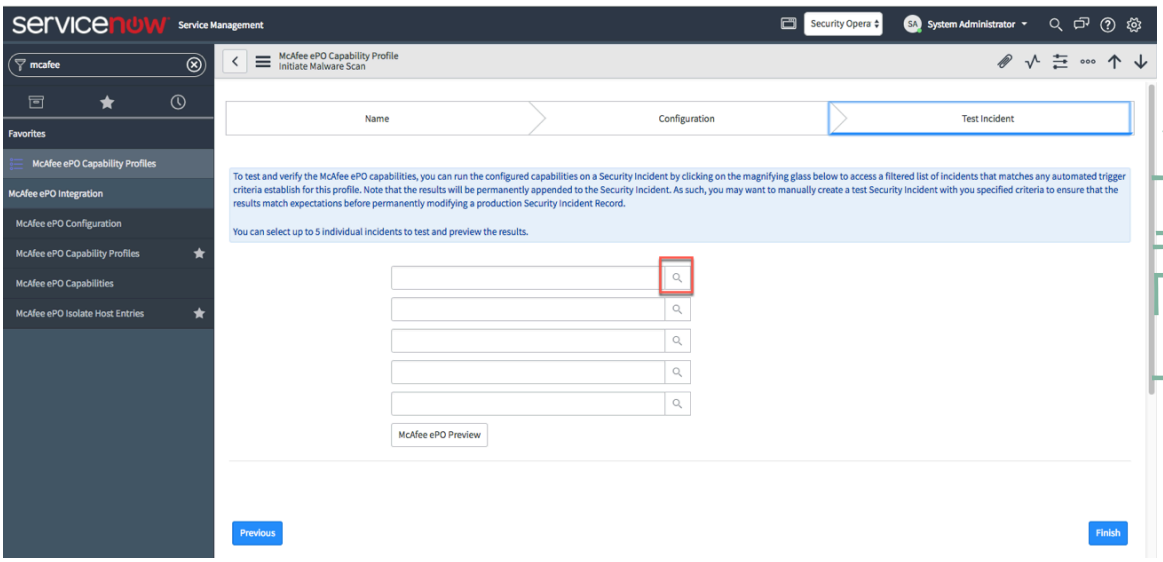
프로시저

1. 인시던트 테스트 페이지가 표시되지 않으면 진행률 표시줄에서 인시던트 테스트를 클릭합니다.
   프로파일에 대한 테스트 인시던트 페이지가 표시됩니다. 이 예에서는 이전 섹션에서 생성하고 구성한 맬웨어 검사 시작 프로파일이 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



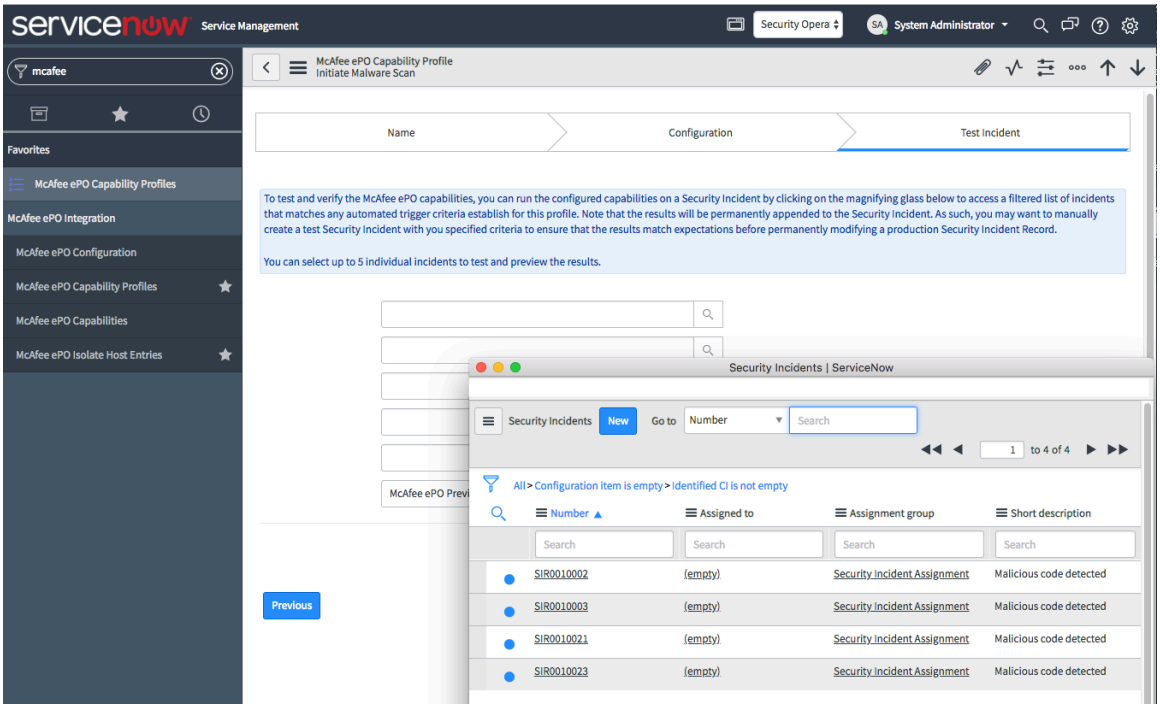
2. 상단 필드 오른쪽에 있는 검색 아이콘을 클릭하여 미리 보기에 표시할 보안 인시던트를 선택합니다.



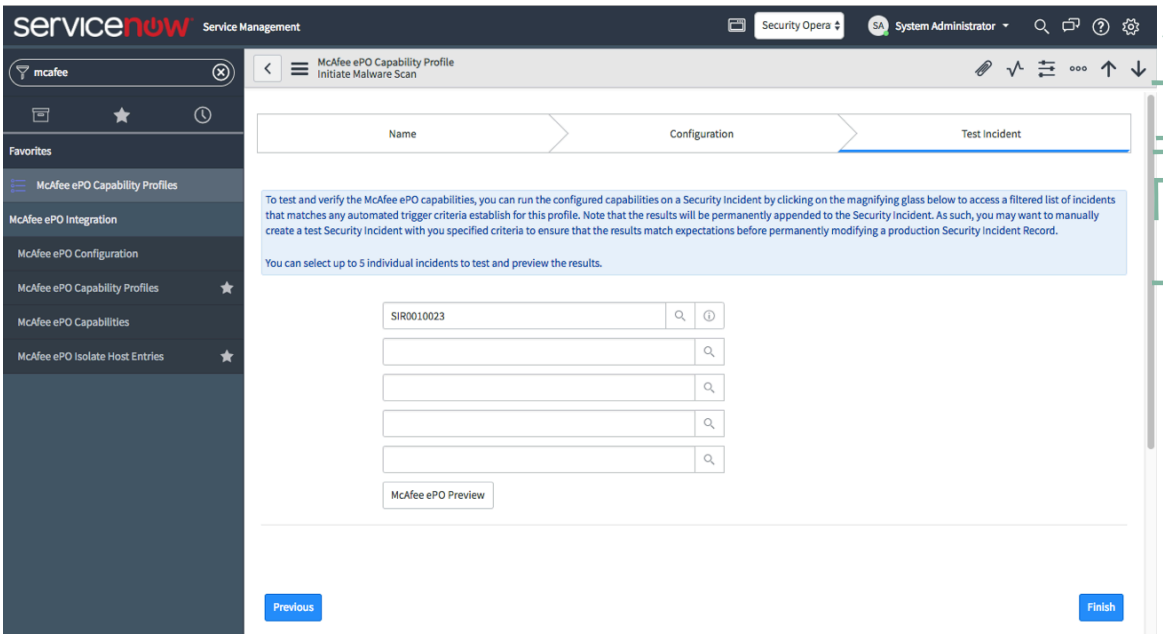
프로파일 기준과 일치하는 보안 인시던트만 표시됩니다.

3. 표시되는 목록의 번호 열에서 미리 보기에 표시할 항목을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

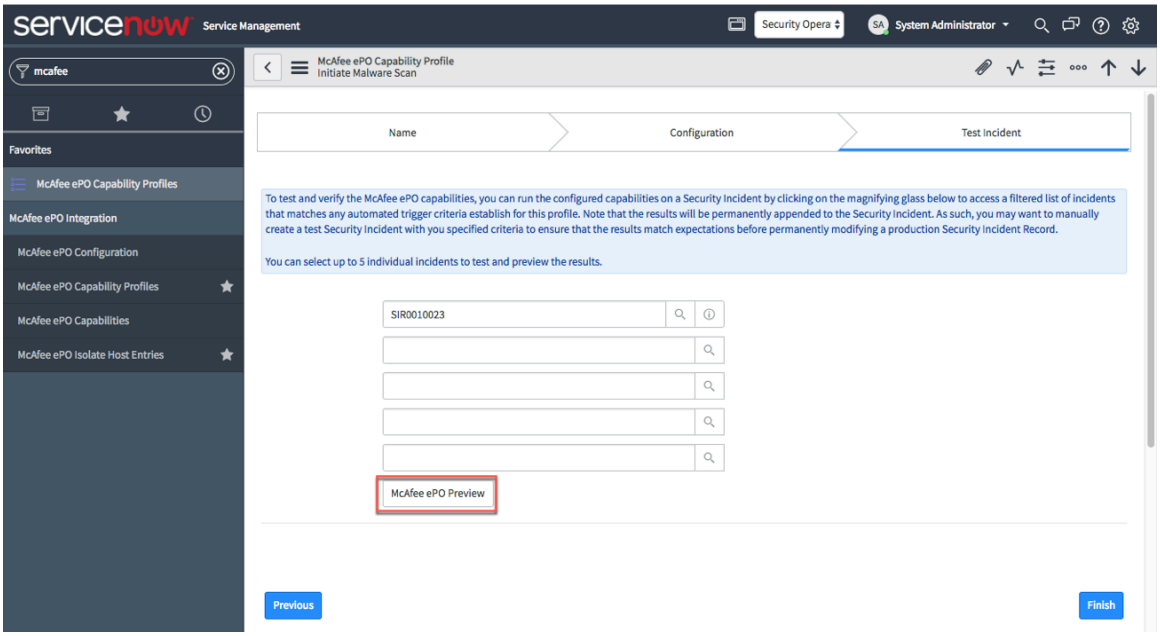


보안 인시던트 번호가 필드에 표시됩니다.

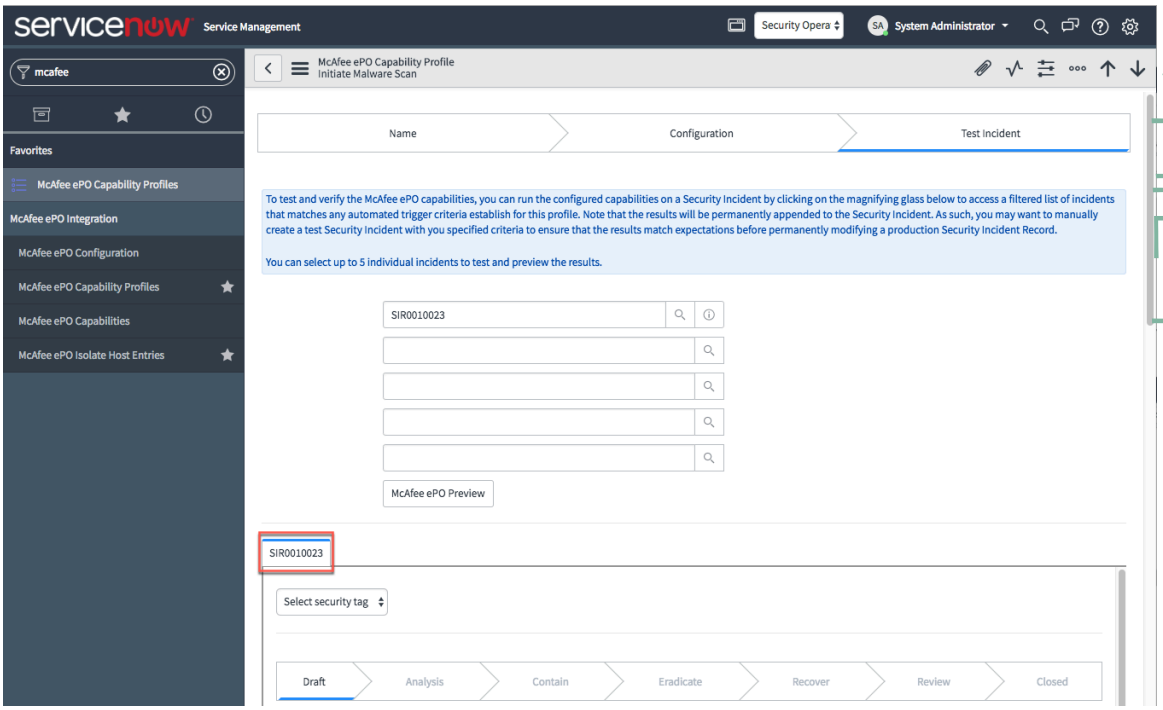


4. 미리 보려는 모든 인시던트가 필드에 표시될 때까지 2단계와 3단계를 반복합니다.
   미리 보기에 보안 인시던트를 최대 5개까지 선택합니다.
5. **McAfee ePO** 미리 보기를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



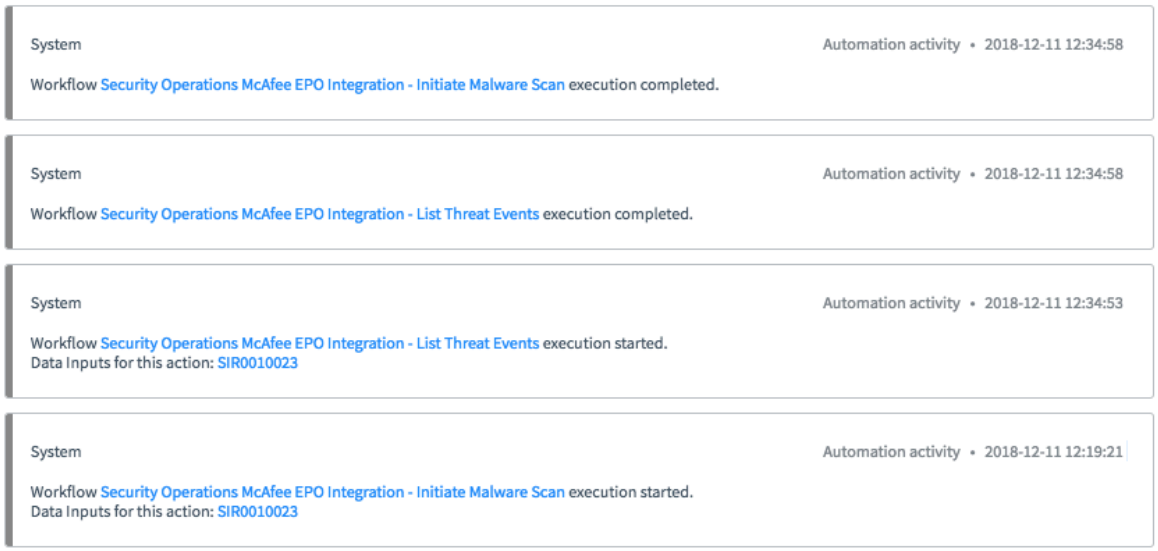
프로파일의 이벤트 조건과 일치하는 보안 인시던트가 표시됩니다. 페이지가 로드되면 페이지 하단에 각 보안 인시던트에 대한 탭이 표시됩니다.



6. 스크롤하여 작업 메모를 봅니다.

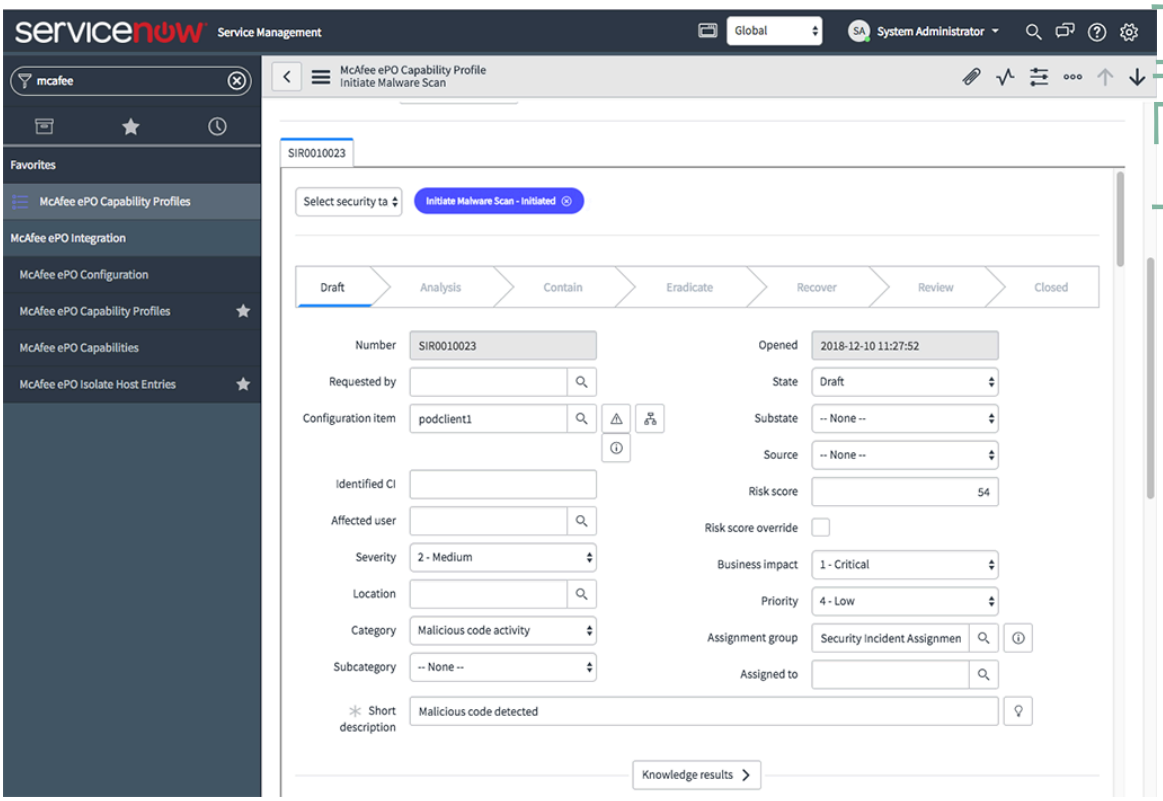
주:
위협 이벤트 나열 워크플로우는 검사의 일부입니다. 맬웨어 검사 기능을 사용하여 프로필을 만드는 방법에 대한 자세한 내용은 을 참조하십시오 역량 프로파일 생성.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



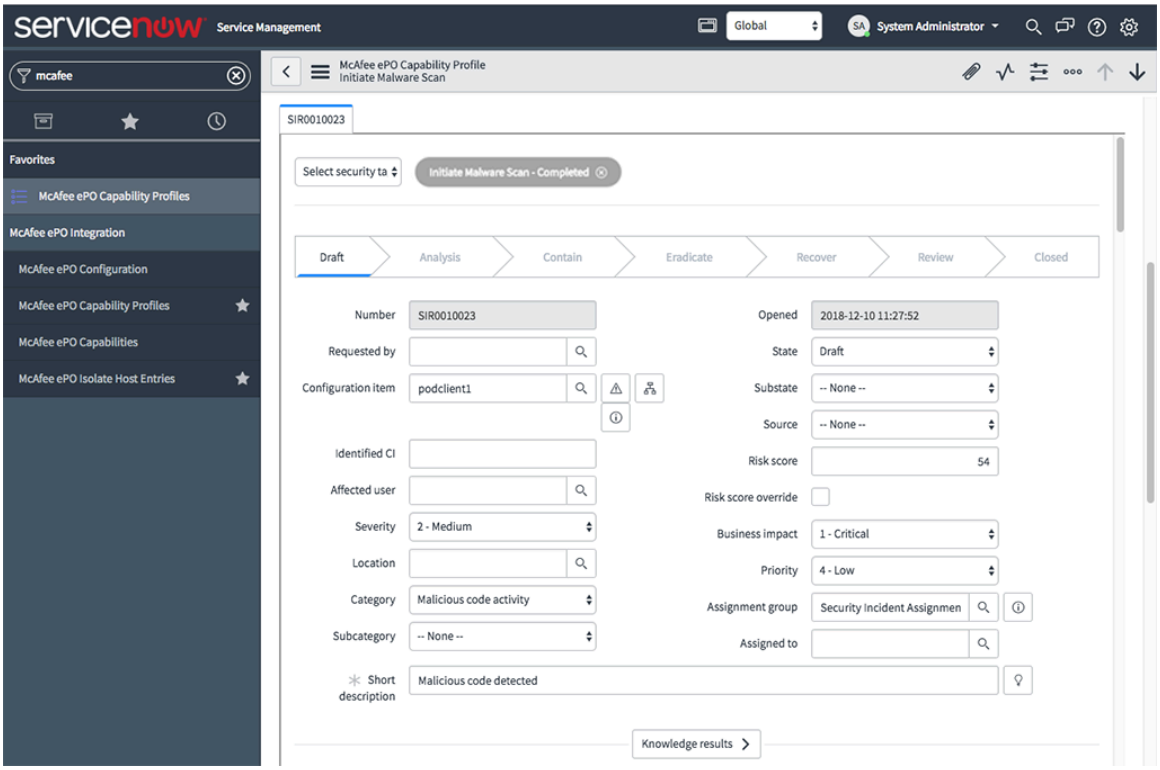
스캔은 네트워크 사용자에게 미치는 영향을 최소화하기 위해 피크 작업 시간 이후에 실행되도록 예약되는 경우가 있습니다. 스캔이 즉시 완료되지 않을 수 있습니다. 이 경우 보안 인시던트 위에 검사가 예약되었음을 나타내는 보안 태그가 표시됩니다. 워크플로우의 상태는 작업 메모를 참조하십시오. 워크플로우가 시작되고 성공적으로 완료될 때의 작업 메모 목록. 이 예의 경우 다음 그림의 작업 메모는 스캔이 시작되었고 성공적으로 완료되었음을 보여줍니다. 위협 이벤트 나열 기능도 검사의 일부로 시작되고 성공적으로 완료되었습니다.

다음 그림은 관련 보안 인시던트에 대한 보안 태그의 예를 보여줍니다.

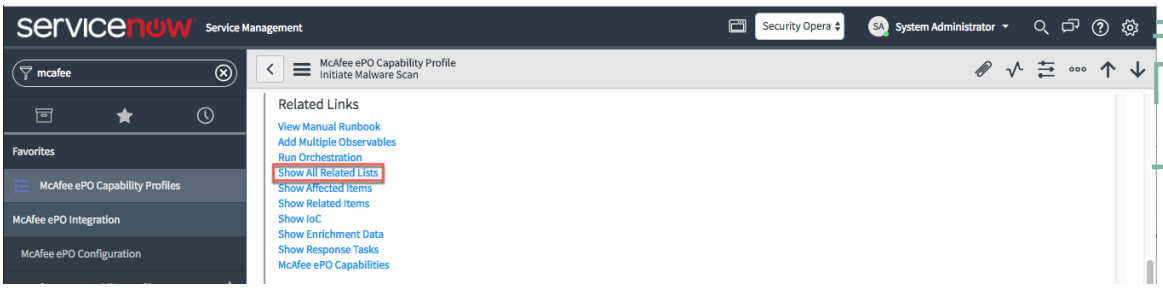


보안 인시던트에서 스캔이 성공적으로 완료되면 예약된 태그가 완료된 태그로 자동 대체됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

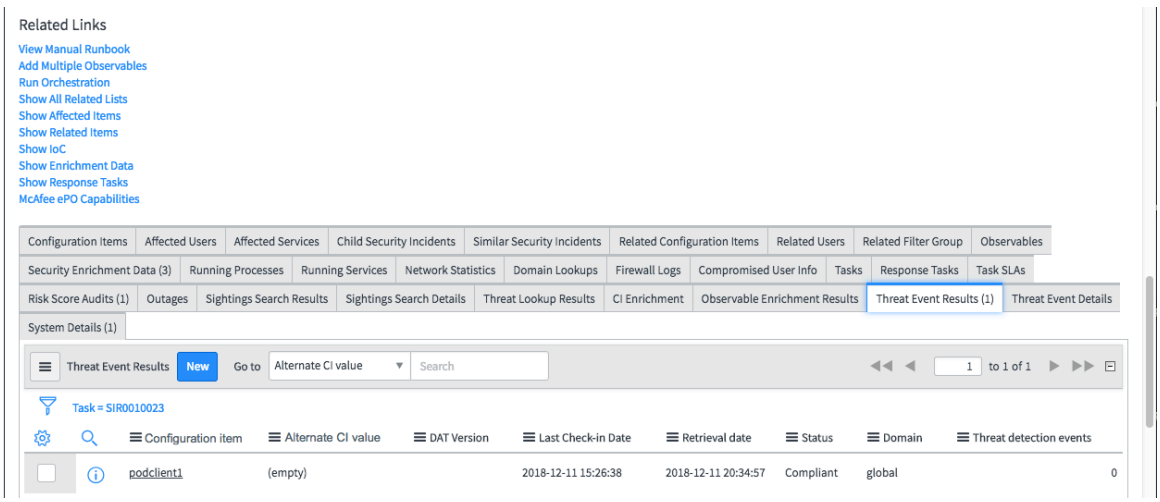


7. 검사가 성공적으로 완료되었는지 확인한 후 보안 인시던트에서 스크롤하여 관련 링크를 확인하고 모든 관련 목록 표시를 클릭합니다.



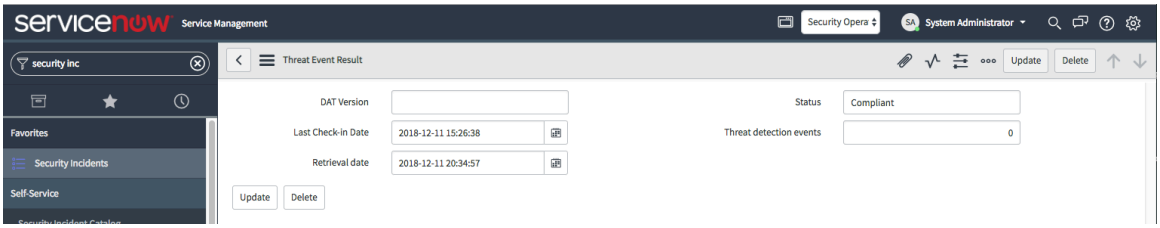
위협 이벤트 결과 및 위협 이벤트 상세 정보 목록이 탭으로 표시됩니다.

8. 위협 이벤트 상세 정보 목록을 선택하지 않은 경우 선택하여 결과를 봅니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

9. 소스 열에서 항목을 클릭하여 기록을 열고 보강 데이터를 봅니다.



보강 데이터에는 다음 정보가 포함됩니다.

- 검사 중에 일치한 CI 필드 값입니다.
- 시간대가 있는 마지막 체크인 날짜입니다. 이 데이터는 콘솔에서 가장 최근 데이터를 가져온 McAfee ePO 시간을 현지 시간으로 나타냅니다.
- 원시 데이터

이 프로파일에 대해 설정한 자동 트리거 기준과 일치하는 보안 인시던트에 대한 스캔 워크플로우가 성공적으로 완료되었는지 성공적으로 확인했습니다.

10. 계속하려면 하나를 선택합니다.

보안 인시던트를 테스트하고 호스트 격리에 대한 요청을 승인합니다.

테스트 및 미리 보기 단계를 사용하면 호스트 분리 및 호스트 분리 제거 워크플로 결과가 프로파일에 대해 예상대로 반환되는지 확인할 수 있습니다.

시작하기 전에

필요한 역할: sn_si.admin

이 태스크 정보

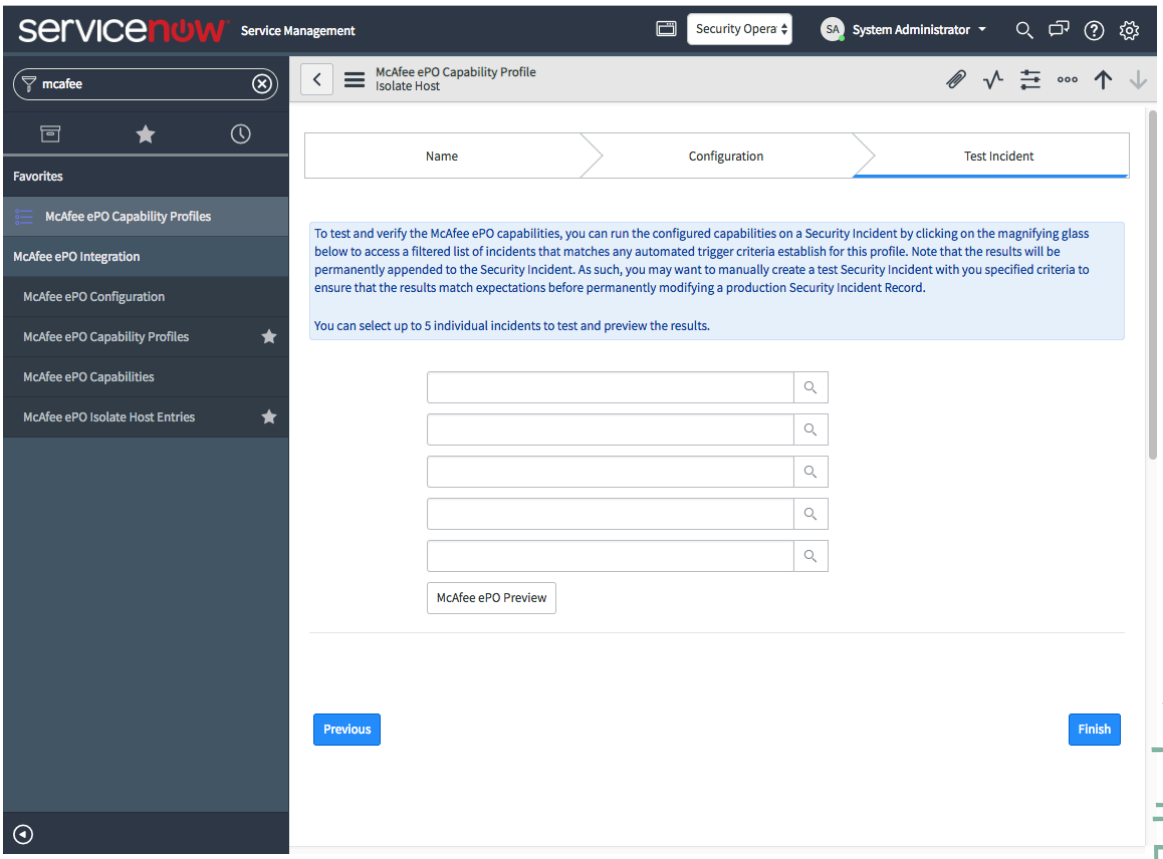
구성의 이 단계에서 sn_si.admin 역할을 가진 사용자는 호스트 격리 기능으로 구성한 프로파일이 보안 인시던트와 일치하는 자산 ID를 예상대로 반환하는지 확인합니다. 프로파일의 설정과 일치하는 보안 이벤트 조건이 발생할 때 만들어지는 실제 ServiceNow AI Platform 보안 인시던트 응답 (SIR) 보안 인시던트를 봅니다.

호스트 시스템을 격리하는 요청이 제출된 후 승인자 역할을 가진 사용자로 요청을 처리합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

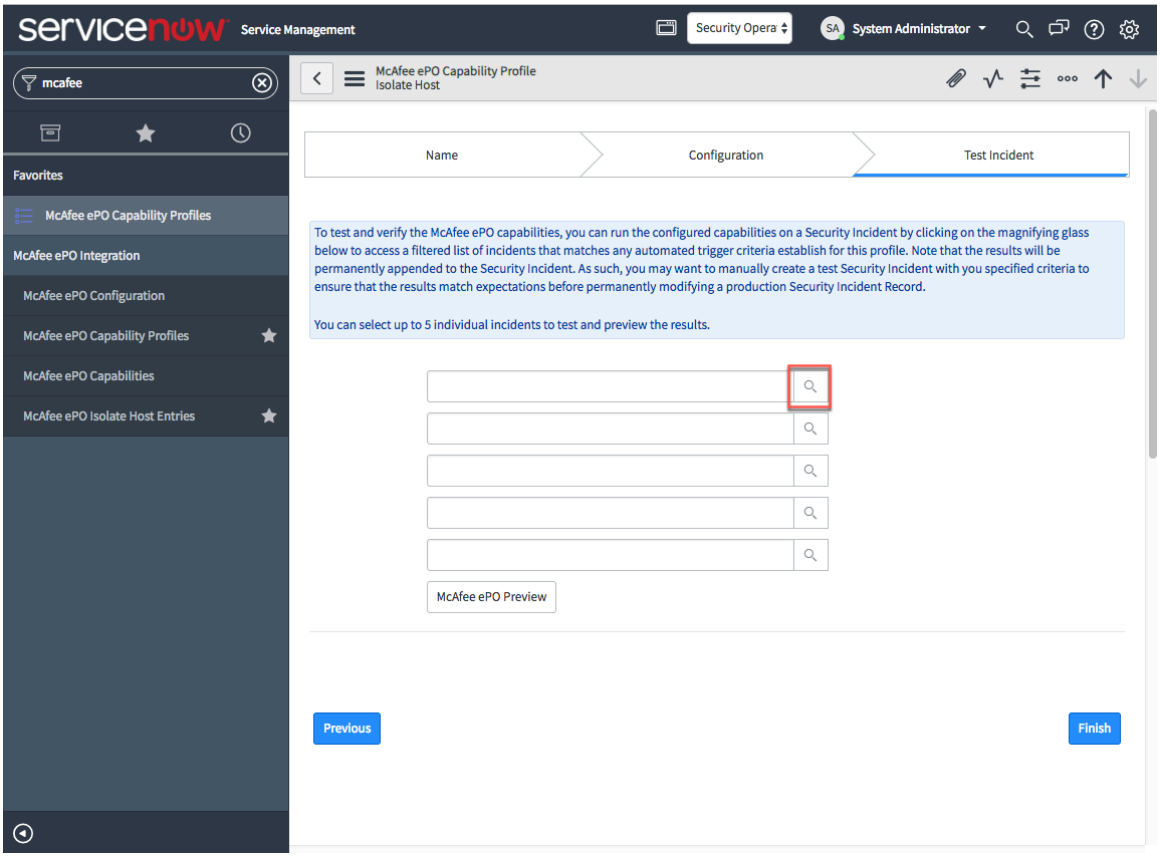
1. 인시던트 테스트 페이지가 표시되지 않으면 진행률 표시줄에서 인시던트 테스트를 클릭합니다.



프로파일에 대한 테스트 인시던트 페이지가 표시됩니다. 이 예에서는 이전 섹션에서 생성하고 구성한 호스트 격리™ 프로파일이 표시됩니다.

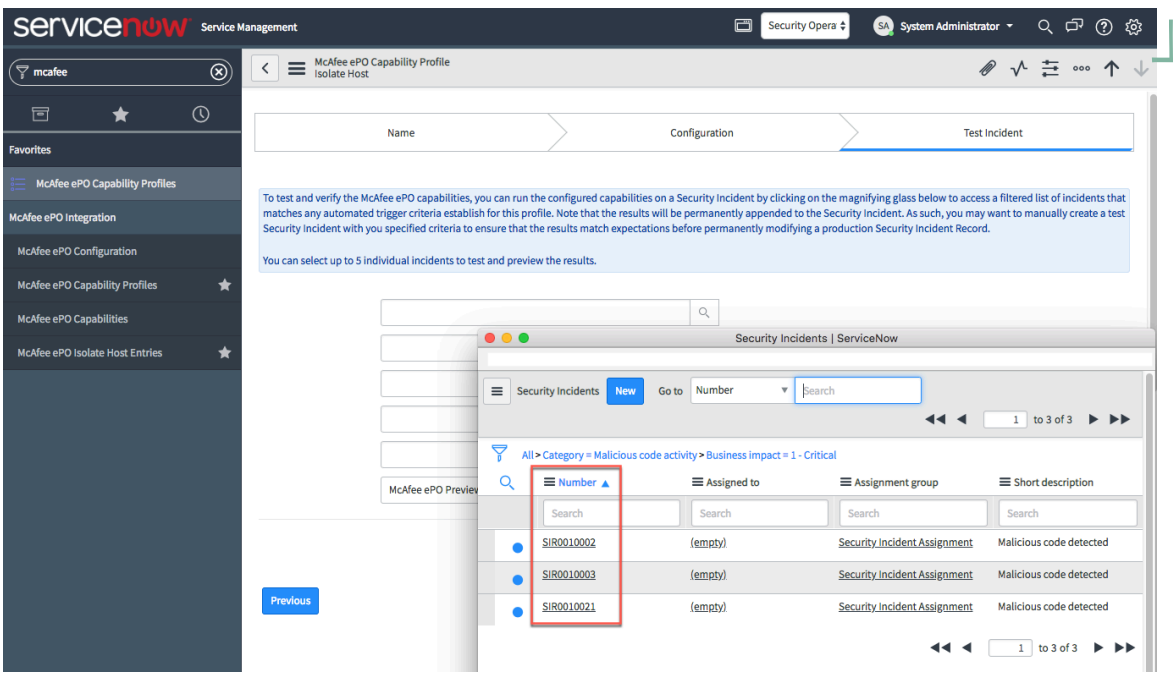
2. 상단 필드 오른쪽에서 검색 아이콘을 클릭하여 미리 볼 보안 인시던트를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



3. 표시되는 목록의 번호 열에서 미리 보기에 표시할 항목을 선택합니다.

프로파일에 대해 설정한 기준과 일치하는 보안 인시던트만 표시됩니다.

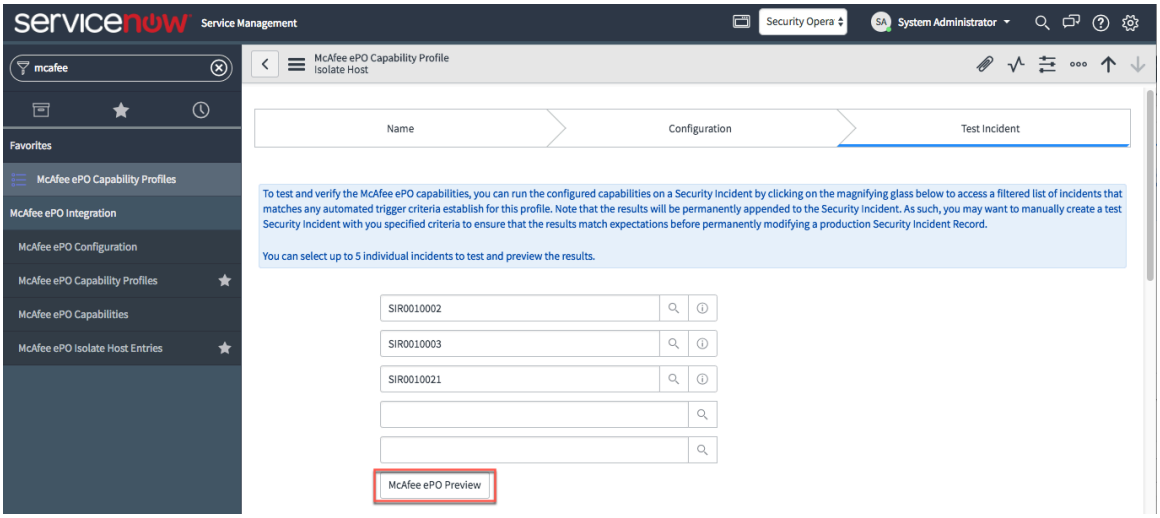


보안 인시던트가 페이지에 표시됩니다.

4. 미리 보려는 모든 인시던트가 필드에 표시될 때까지 2단계와 3단계를 반복합니다.
미리 보기에 보안 인시던트를 최대 5개까지 선택합니다.

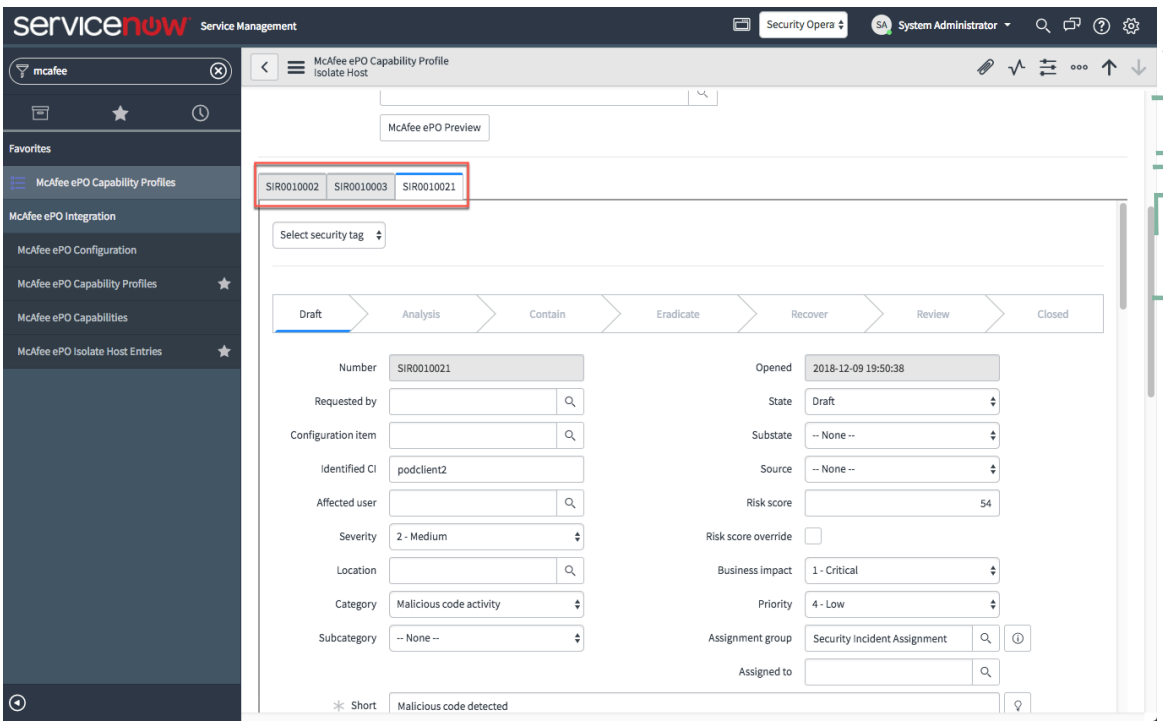
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. McAfee ePO 미리 보기를 클릭하여 보안 인시던트를 확인합니다.



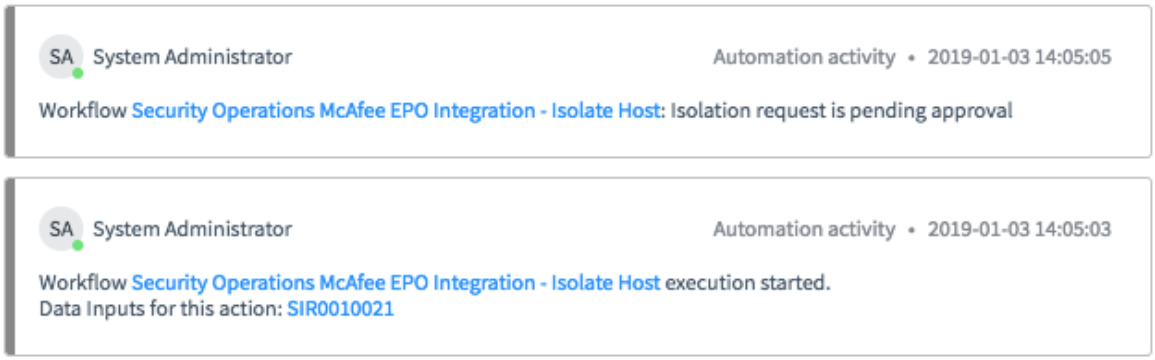
프로파일과 일치하는 보안 이벤트 조건에 대해 생성된 인시던트가 탭에 표시됩니다.

주:
이때 테스트 인시던트 페이지에서 나가면 이 필드에서 보안 인시던트가 지워집니다.



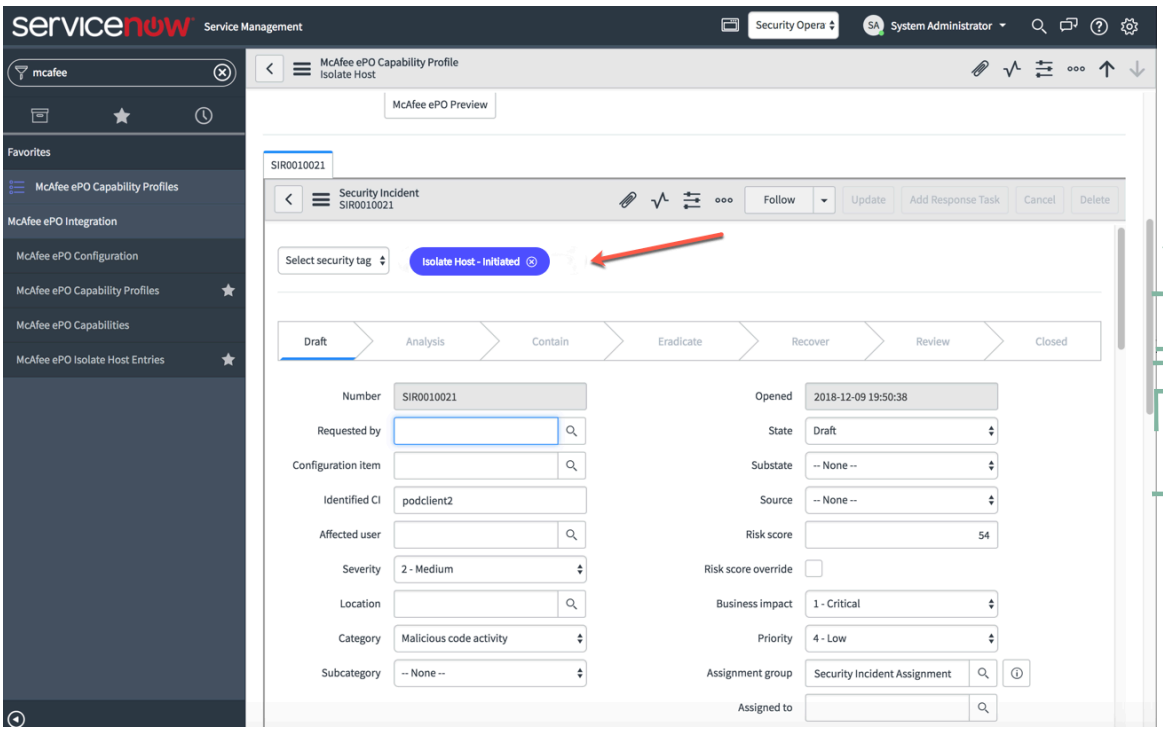
6. 탭을 선택하고 보안 인시던트에서 스크롤하여 작업 메모를 봅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



이 예에서는 이전 이미지의 SIR0010021 선택됩니다. 호스트 분리 워크플로우가 시작되는 작업 메모 목록입니다. 이 프로파일에 대해 승인 필요 옵션이 활성화되어 있기 때문에 작업 메모는 요청이 ## ## #임을 나타냅니다.

인시던트 맨 위에 요청이 시작되었음을 나타내는 보안 태그가 표시됩니다(### ## - ###).



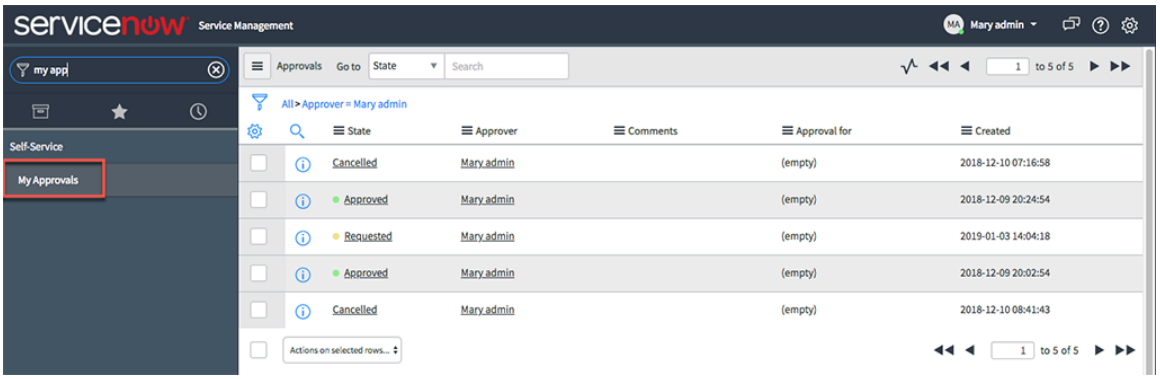
호스트 격리 역량에 대한 프로파일과 일치하는 보안 인시던트를 찾고 보안 인시던트를 확인했습니다.

7. 승인 그룹에 속한 사용자인 경우 다음 단계에 따라 요청을 처리합니다.

a. 인스턴스에서 내 승인 으로 이동합니다.

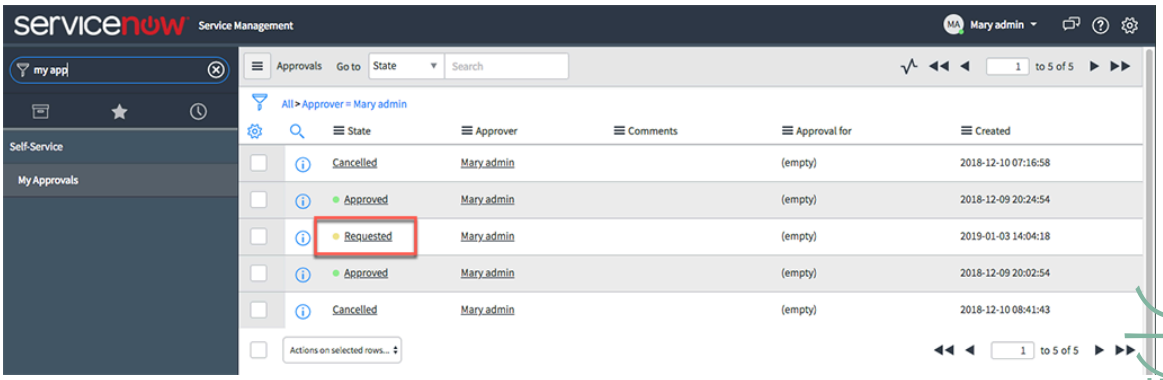
이 예시에서 승인자의 사용자 이름은 Mary admin™입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

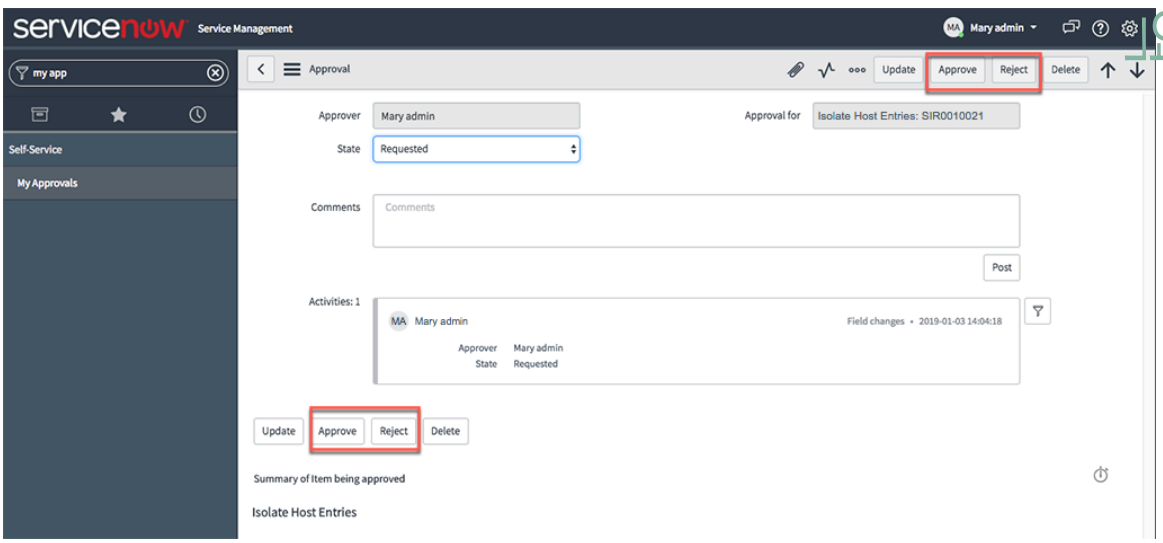


승인 목록이 표시됩니다.

b. 상태 열에서 항목을 클릭하여 승인 기록을 엽니다.



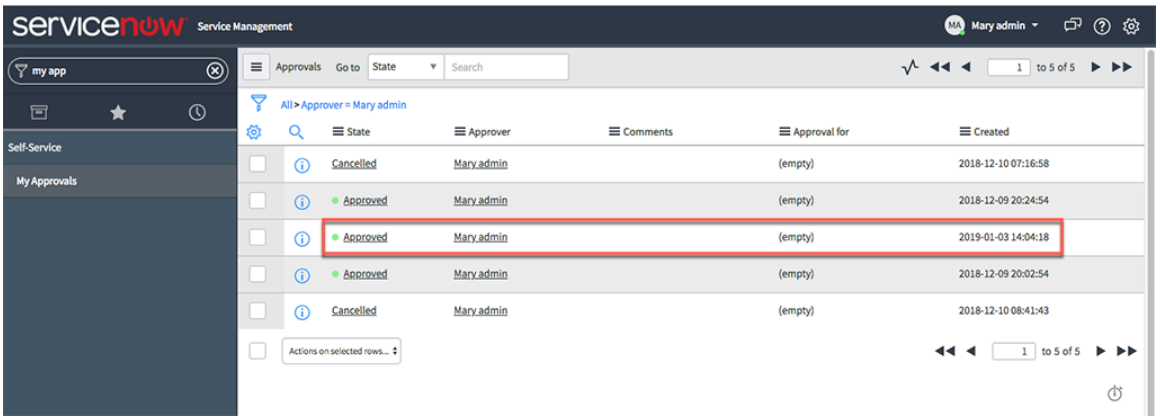
c. 표시되는 승인 기록에서 승인 또는 거부를 클릭합니다.



요청을 처리한 후 워크플로우를 실행하는 데 약간의 시간이 걸릴 수 있습니다. 맨 위에 있는 기록에서 트랜잭션이 몇 초 이상 걸리는 경우 다음 그림과 같이 메시지가 표시됩니다.

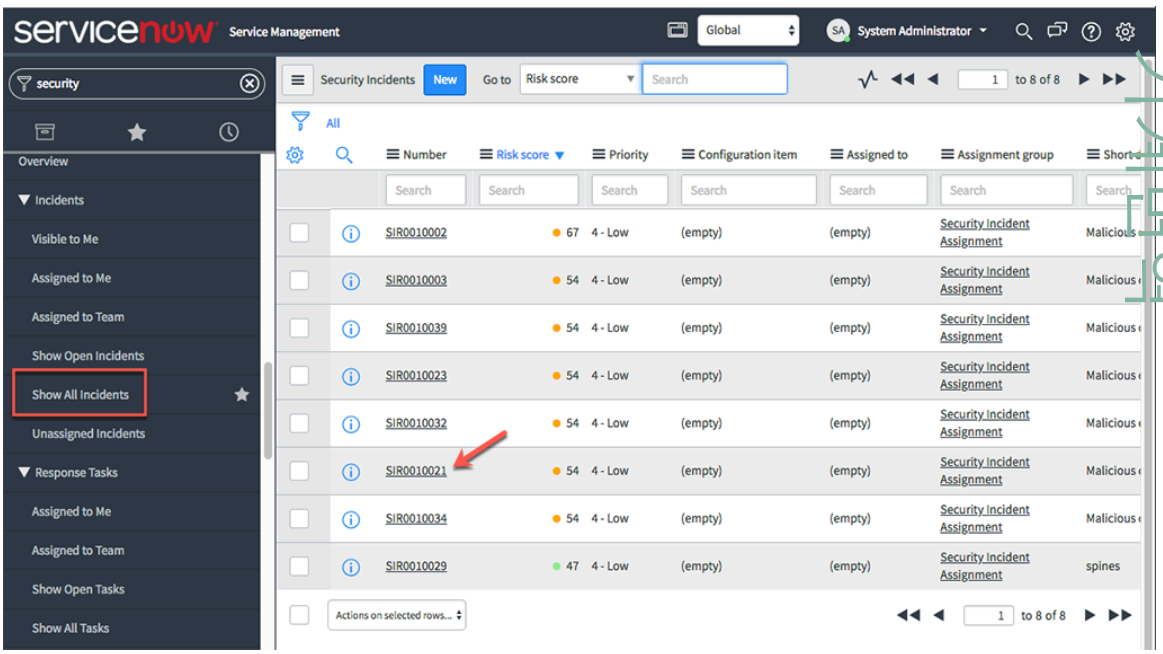
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

잠시 후 표시되는 승인 기록에서 상태 열이 ## 됨에서 ###으로 변경됩니다. 이 요청에 대한 호스트 컴퓨터를 격리하는 데 추가 승인이 필요하지 않습니다. 요청이 거부되면 호스트가 격리되지 않고 요청이 보류 상태로 유지됩니다. sn_si.analyst 역할을 가진 사용자가 요청이 거부된 경우 엔드포인트를 격리하려면 새 요청을 제출해야 합니다.



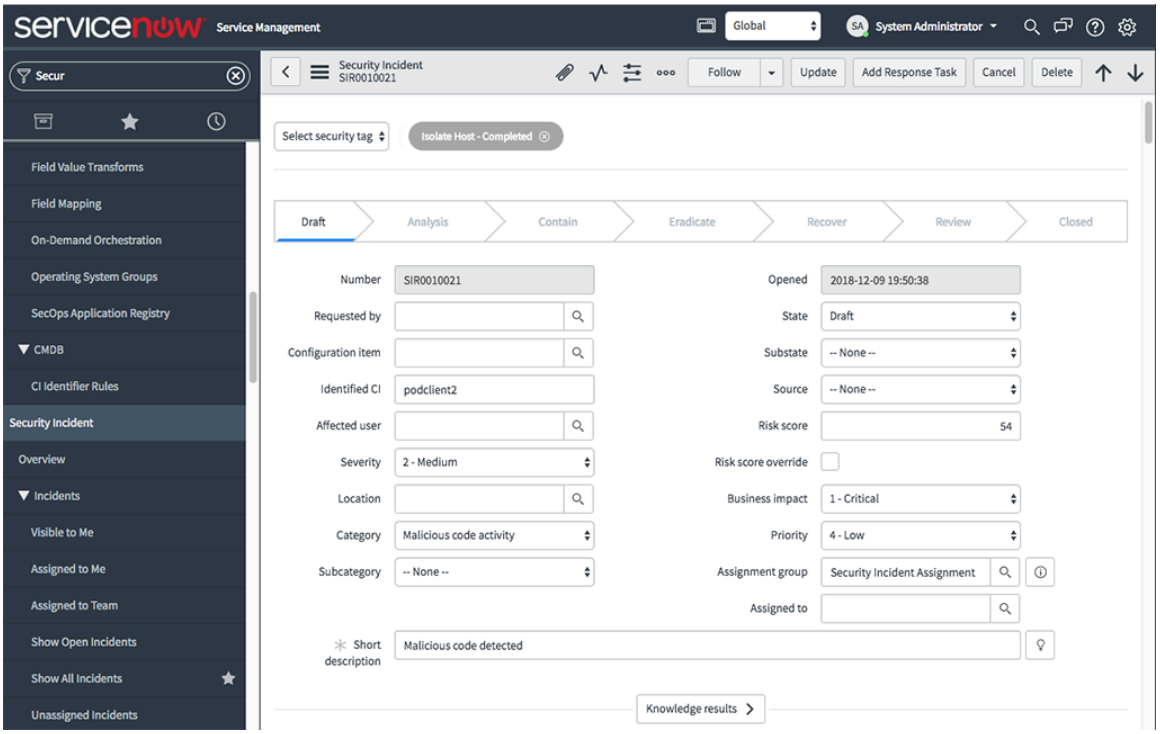
위 그림의 호스트 컴퓨터를 격리하는 요청이 승인됩니다.

d. 다음으로 이동 보안 인시던트 〉 인시던트 〉 모든 인시던트 표시 그리고 번호 열에서 항목을 클릭하여 작업 중인 보안 인시던트를 엽니다.

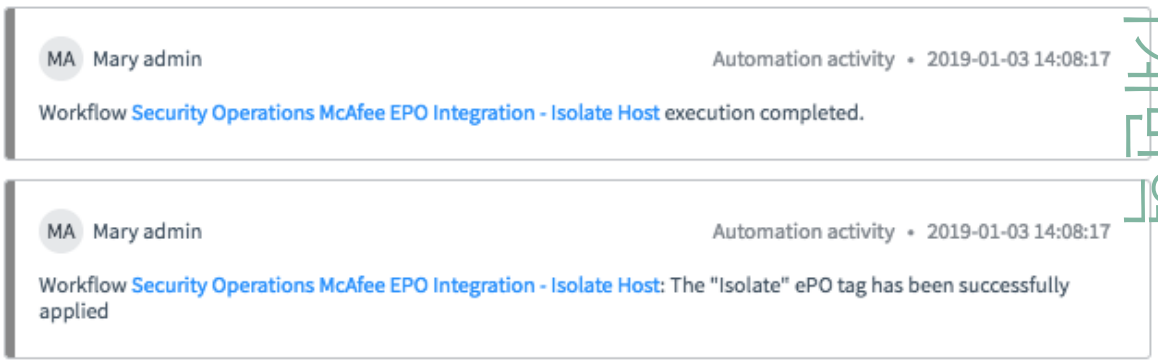


표시되는 보안 인시던트에서 호스트 격리 - 완료됨™ 태그가 호스트 격리 - 시작됨™ 태그를 대체합니다. 이 예에서는 호스트 분리 워크플로우가 성공적입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



보안 인시던트에 대한 작업 메모에는 호스트 격리가 완료되고 승인자인 Mary admin™이 나열됨도 표시됩니다.



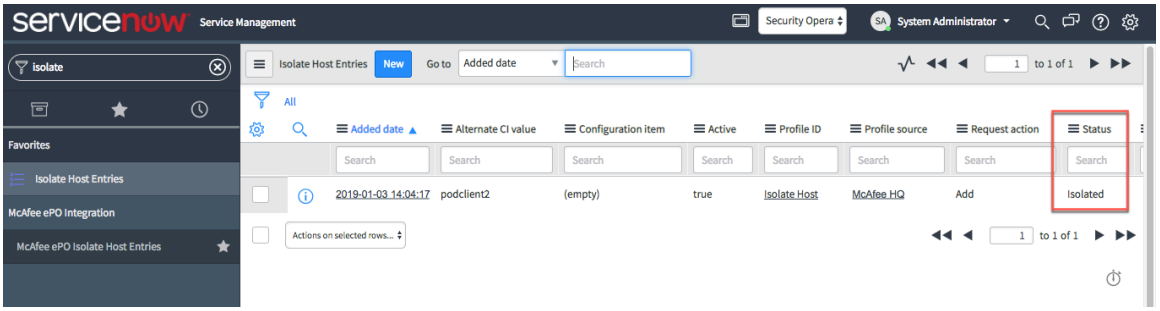
중요사항:
보안 인시던트에 대한 보안 태그 및 작업 메모에 호스트 격리 워크플로우가 성공적으로 완료되었다고 표시되지만 콘솔로 McAfee ePO 돌아가서 호스트 시스템이 네트워크에서 격리되었는지 확인합니다.

자산에 대한 조사를 완료한 후 인스턴스의 호스트 격리 항목™ 테이블에서 ServiceNow AI Platform# 격리 제거 워크플로우를 시작하여 호스트를 네트워크로 반환합니다.

8. 호스트를 격리에서 제거하고 네트워크로 되돌리려면 다음 단계를 수행합니다.

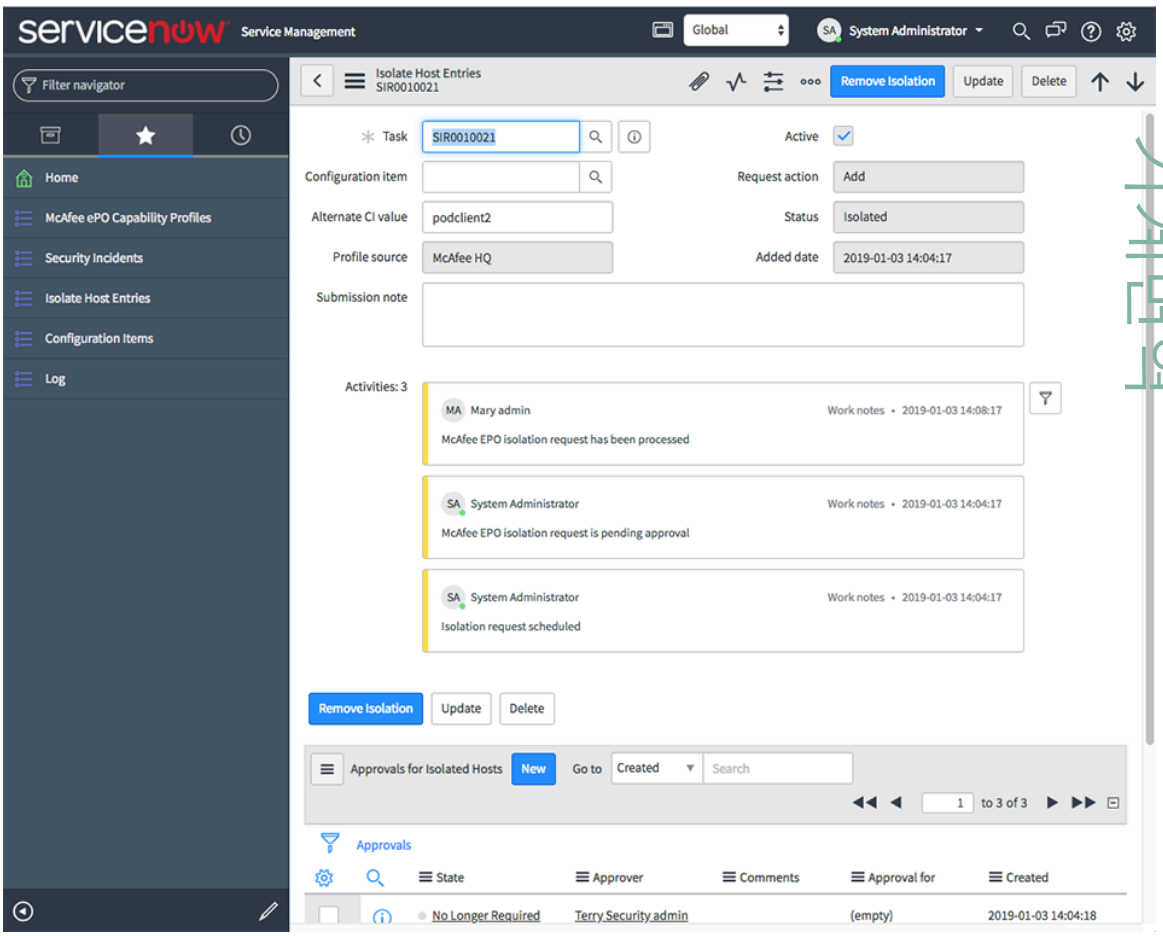
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. McAfee ePO 호스트 항목 격리 테이블이 표시되지 않으면 **McAfee epO** 통합 〉 **Mcafee epO** 통합 호스트 항목 격리.



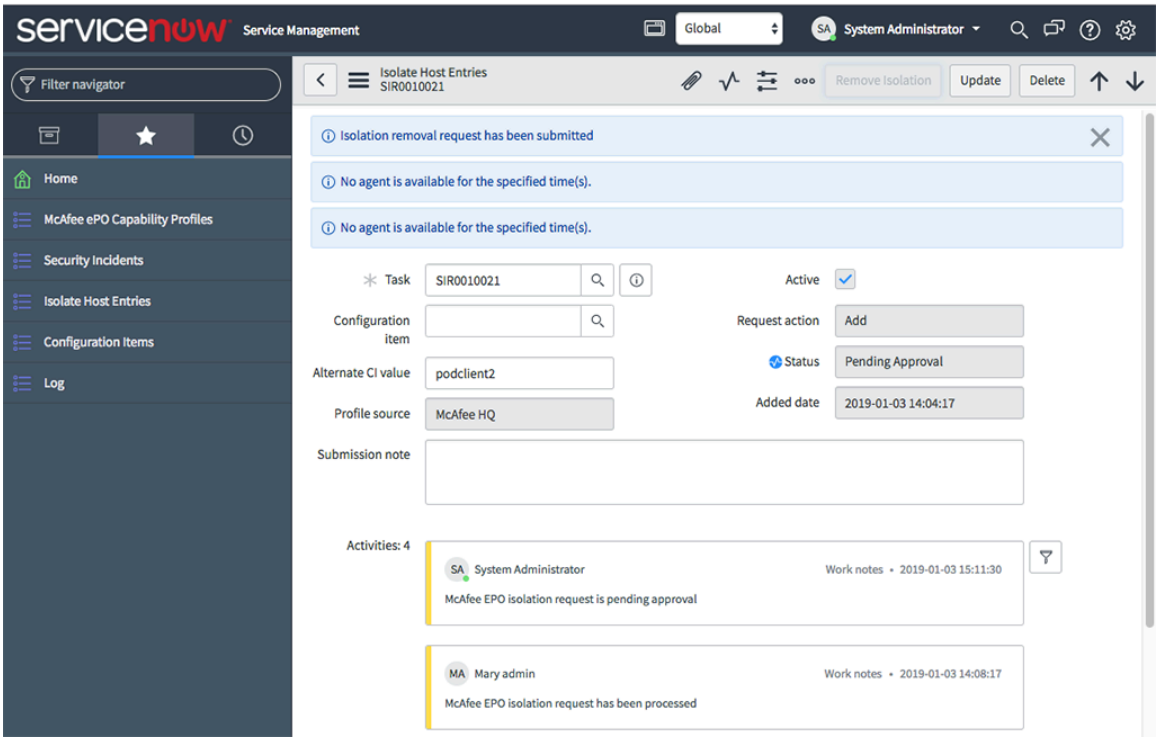
호스트 항목 격리 목록이 표시됩니다. 목록 상단의 상태 열에서 격리한 자산을 검색합니다.

b. 추가된 날짜 열에서 항목을 클릭하여 기록을 엽니다.
호스트 항목 격리 기록이 표시됩니다. 보안 인시던트와 연관된 모든 작업에 대한 감사 추적이 작업 메모에 표시됩니다. 다음 그림에서 작업 메모의 마지막 항목은 성공적인 호스트 격리입니다. 격리가 완료된 날짜는 추가된 날짜 필드(2019-01-03 14:04:17)에 표시됩니다.



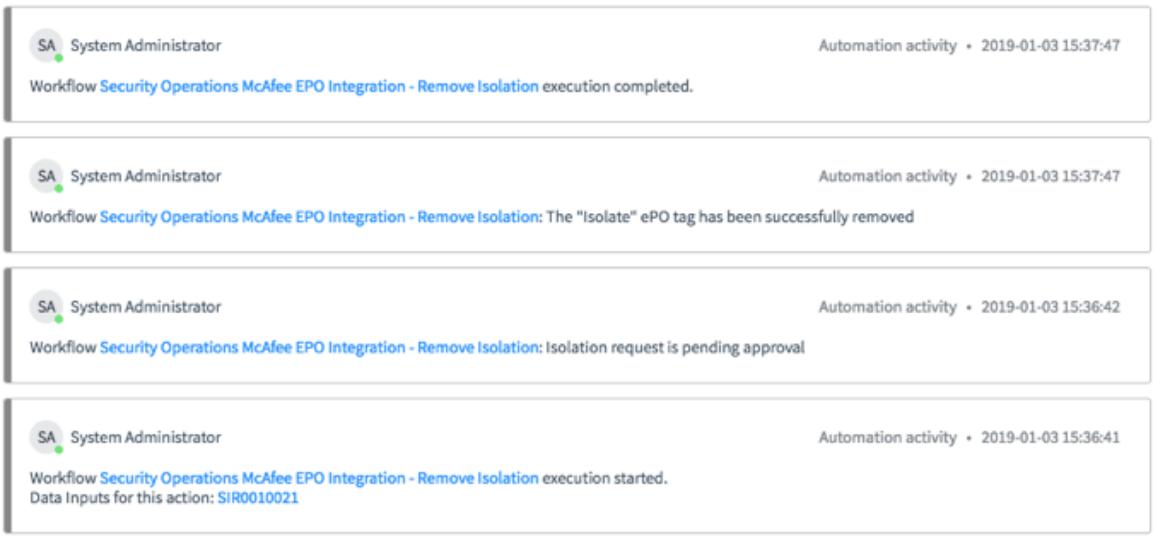
c. **Remove** Isolation(격리 제거)을 클릭하여 시스템을 네트워크에 복원하는 워크플로우를 시작합니다.
호스트 항목 격리 기록이 표시됩니다. 기록 상단에 요청이 제출되었음을 나타내는 메시지가 표시됩니다. 상태가 격리 에서 승인 보류 중으로 변경되고 작업 메모가 기록됩니다. 이 경우 시스템 관리자가 컴퓨터를 네트워크로 복원하도록 요청했습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



d. 요청에 대한 알림을 받은 후 호스트 격리에 대한 승인 권한이 있는 사용자는 인스턴스에서 내 승인 으로 이동하여 격리 제거 요청에 대한 기록을 엽니다.

e. 승인을 클릭하여 요청을 승인하고 자산을 네트워크로 반환합니다.
또는 거부 를 클릭하여 요청을 승인 보류 중 상태로 유지합니다. 요청이 거부되면 호스트를 격리하기 위해 새 요청을 제출해야 합니다. 호스트 분리 제거 요청을 승인하면 보안 인시던트의 태그가 제거됩니다. 작업 메모는 격리 제거 요청에 대한 감사 추적을 생성합니다. 이 예시에서는 시스템 관리자가 요청을 시작하고 승인했습니다.



보안 인시던트에 대한 보안 태그 및 작업 메모는 호스트 분리 제거 워크플로가 성공적으로 완료되었음을 나타냅니다. 호스트가 네트워크에 다시 있는지 확인하려면 콘솔로 McAfee ePO 돌아가서 호스트 시스템이 현재 활성 상태인지 확인합니다.

9. 계속하려면 하나를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작 및 완료 태그 이름과 색상 편집

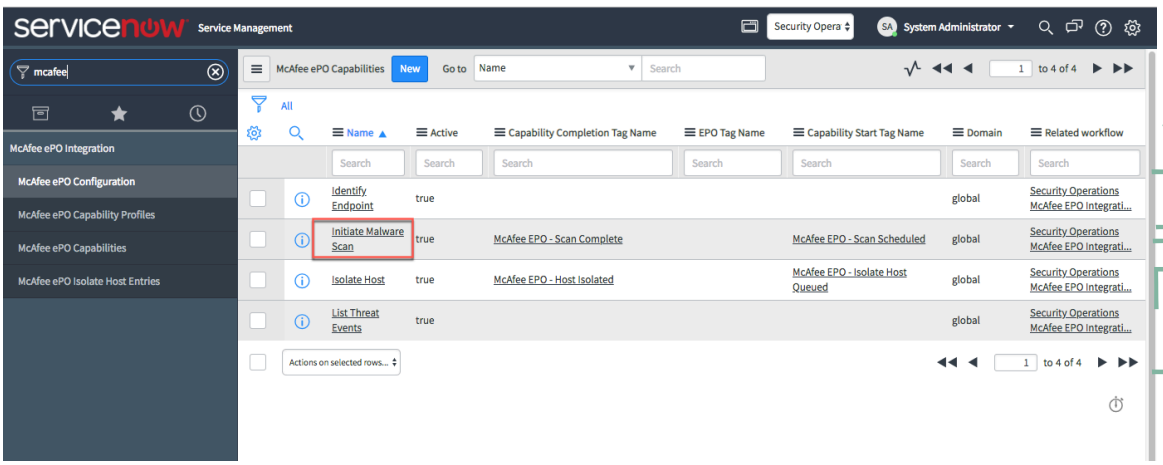
맬웨어 검사 시작 및 호스트 격리 역량에 대한 시작 및 완료 태그의 이름과 색상을 편집하는 것을 선호할 수 있습니다. 시작 및 완료 태그는 (SIR) 보안 인시던트에서 ServiceNow AI Platform 보안 인시던트 응답 호출되는 기능을 빠르게 식별하는 데 도움이 됩니다.

시작하기 전에
필요한 역할: sn_si.admin

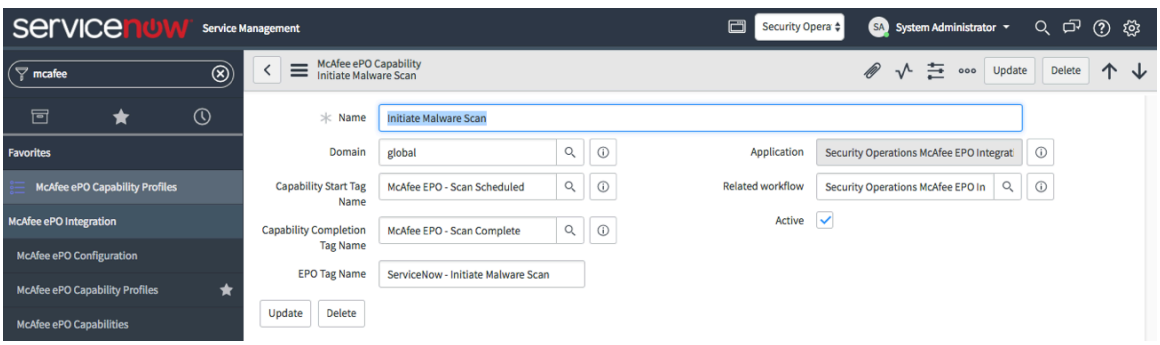
이 태스크 정보
sn_si.admin 역할을 가진 사용자는 보안 인시던트에 SIR 표시되는 보안 태그의 색상과 이름을 편집하는 것을 선호할 수 있습니다. 보안 태그 그룹에 태그를 할당하면 인스턴스에서 보안 태그 그룹을 구성할 수도 있습니다 ServiceNow AI Platform# . 예를 들어 역량의 시작 태그는 한 색상이고 완성 태그는 다른 색상이 되도록 태그의 색상을 변경할 수 있습니다. 이러한 다양한 색상은 스캔이 시작되고 성공적으로 완료된 시기를 빠르게 식별하는 데 도움이 될 수 있습니다. 보안 태그 그룹 및 태그를 설정하는 방법에 대한 자세한 내용은 보안 태그 그룹 및 태그 설정을 참조하세요.

프로시저

1. 보안 태그의 이름과 색상을 편집하려면 **McAfee EPO** 기능으로 이동하여 이름 열에서 목록의 항목을 클릭합니다.



역량에 대한 기록이 표시됩니다.



2. 태그를 편집하려면 태그 이름 오른쪽에 있는 정보 아이콘을 클릭하고 태그 기록을 엽니다.

표시되는 기록에서 필드를 편집합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 계속하려면 하나를 선택합니다.

McAfee ESM - 이메일 파서 통합

ESM - 이메일 파서 통합은 ESM의 이메일 알림을 사용하여 보안 인시던트를 생성하는 이메일 파서에서 지원됩니다.

McAfee ESM - 이메일 파서 통합 구성

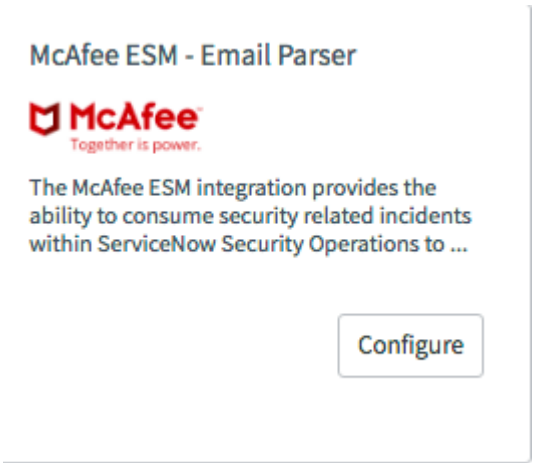
McAfee ESM - 이메일 파서 통합은 ESM의 이메일 알림을 사용하여 보강 및 응답 워크플로우를 구동합니다.

시작하기 전에
필요한 역할: sn_si_admin

이 태스크 정보
통합에 사용할 수 있도록 McAfee ESM 이메일 파서 템플릿이 제공됩니다. 통합이 발생하기 전에 구성하고 활성화해야 합니다. 파서를 업데이트하면 활성화됩니다.

프로시저

1. 다음으로 이동 모두 〉 보안 운영 〉 통합 〉 통합 구성.
   사용 가능한 보안 통합은 일련의 카드로 표시됩니다.



2. McAfee ESM - Email Parser 카드에서 구성을 클릭합니다.
3. **McAfee ESM -** 이메일 파서 구성 대화 상자에서 이메일 파서 구성 링크를 클릭합니다.
4. **McAfee ESM** 링크를 클릭하여 제공된 템플릿 이메일 파서의 설정을 편집합니다.
   최소한 '### ###' 필드를 채우십시오. 고유한 이메일 파서를 생성하려면 문서를 참조하십시오 보안 운영에서 이메일 파서 생성.
5. 활성 상자를 선택합니다.
6. 이메일 파서 양식에서 업데이트를 클릭합니다.
   이메일 파서가 활성 상태입니다. 통합 구성으로 돌아갈 필요가 없습니다.

McAfee ESM - 인시던트 보강 통합

McAfee ESM - 인시던트 보강 통합은 로그를 검색하고 관련 사이팅 정보를 보안 인시던트에 추가합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

탐색	설정
보안 인시던트 응답 통합	• 인시던트 보강 통합 시작하기 McAfee ESM • 사이팅 검색 구성 기록 생성

사용	개발
• 사이팅 검색 실행 • Security Operations Integration - 사이팅 검색 플로우 • 보안 운영 - McAfee ESM 사이팅 검색 플로우 • 사이팅 검색 상세 정보 보기 • 사이팅 검색 결과 보기	• ServiceNow 보안 운영 통합 개발 가이드라인 • 통합 작성을 위한 팁 • 개발자 교육 • 개발자 설명서

문제 해결 및 도움받기

- 통합 문제 해결
- 보안 운영 커뮤니티에서 질문 또는 답변하기
- 알려진 오류 포털에서 알려진 오류 문서 검색

- 연락처 고객 서비스 및 지원

인시던트 보강 통합 시작하기 **McAfee ESM**

McAfee ESM 는 바이러스, 스파이웨어, 트로이 목마 및 기타 맬웨어 위협 보안 운영으로부터 엔드포인트를 보호하고 . 인시던트 보강 통합을 사용하려면 McAfee ESM 먼저 다음 ServiceNow Store 에서 다운로드하고 적절한 API 기준 URL 및 로그인 자격 증명을 추가해야 합니다.

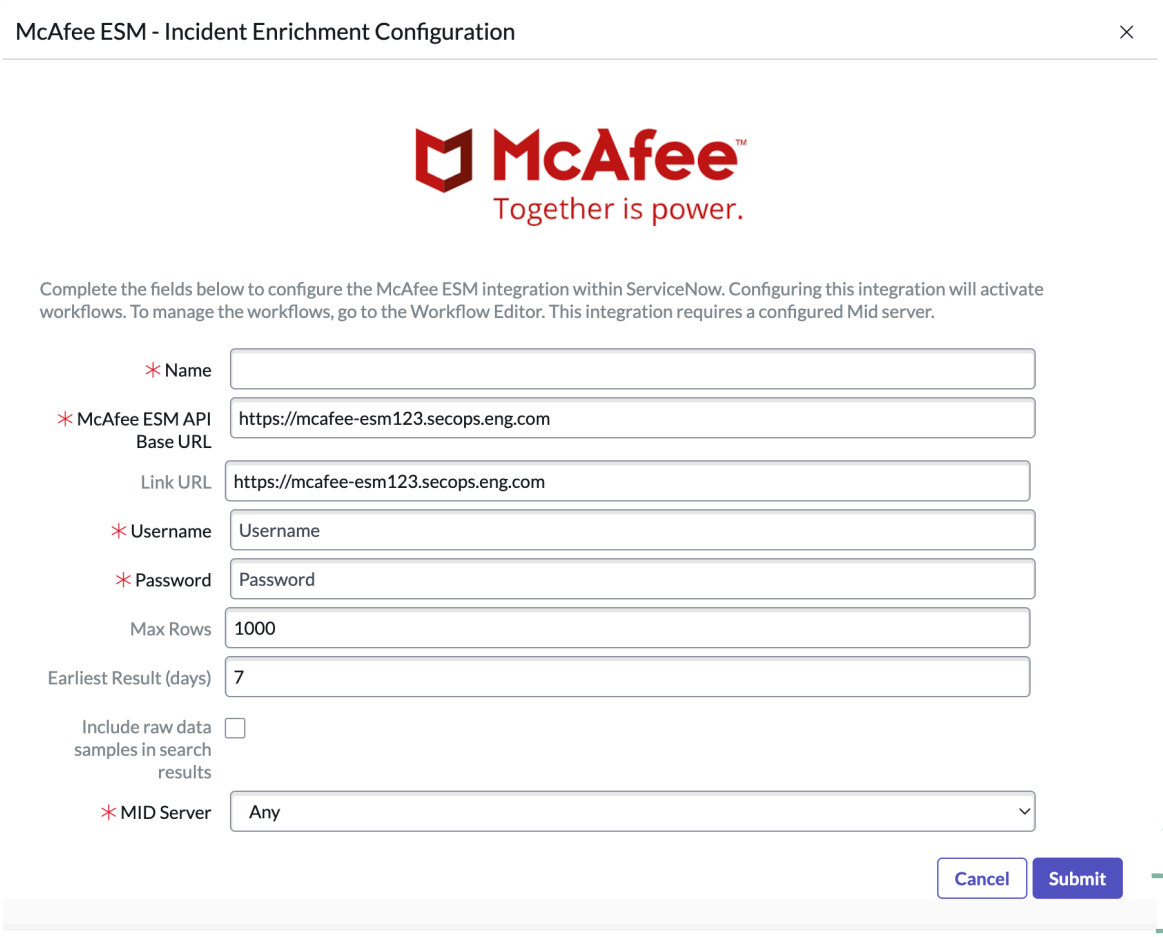
시작하기 전에

필요한 역할: sn_si_admin

프로시저

1. 에서 통합을 다운로드합니다. ServiceNow Store.
2. 설치가 완료되면 보안 운영 〉 통합 〉 통합 구성.
   사용 가능한 보안 통합은 일련의 카드로 표시됩니다.
3. - 인시던트 보강 카드에서 McAfee ESM새로 만들기를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 필요에 따라, 필드를 채웁니다.

필드	설명
이름	이 구성의 이름입니다.
McAfee ESM API 기본 URL	McAfee ESM 사이트에서 가져온 기본 URL입니다.
링크 URL	〔선택사항〕 사용 가능한 경우 McAfee ESM 인스턴스에 연결하는 링크 URL입니다. **주:** 오류가 발생하면 McAfee ESM API 기본 URL을 사용하십시오.
사용자 이름	McAfee ESM 사용자 이름입니다.
암호	McAfee ESM 암호입니다.
최대 행 수	검색할 행의 최대 수입니다.
가장 빠른 결과 (일)	일수 단위로 보려는 가장 빠른 결과입니다.
검색 결과에 원시 데이터 샘플 포함	사이팅 검색 결과에 원시 데이터 샘플을 포함하려면 이 옵션을 선택합니다. 반환되는 데이터의 양은 보안 인시던트 응답 속성의원시 데이터 속성 행 수의 설정에 따라 달라집니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
MID 서버	활성 MID 서버를 사용하려면 임의 를 선택하고, 특정 MID 서버 이름을 선택합니다.

주:
이 통합을 구성하면 워크플로우가 활성화됩니다. 워크플로우를 관리하려면 워크플로우 편집기로 이동합니다.

5. 제출을 클릭합니다.
   통합 구성 카드가 표시됩니다.
6. 새 구성 카드를 볼 때 구성 또는 삭제를 클릭하여 구성을 변경하거나 삭제할 수 있습니다.
7. 통합 구성 카드의 원래 목록으로 돌아가려면 구성 표시 드롭다운 목록에서 아니요를 선택합니다.

Microsoft Azure Sentinel 통합

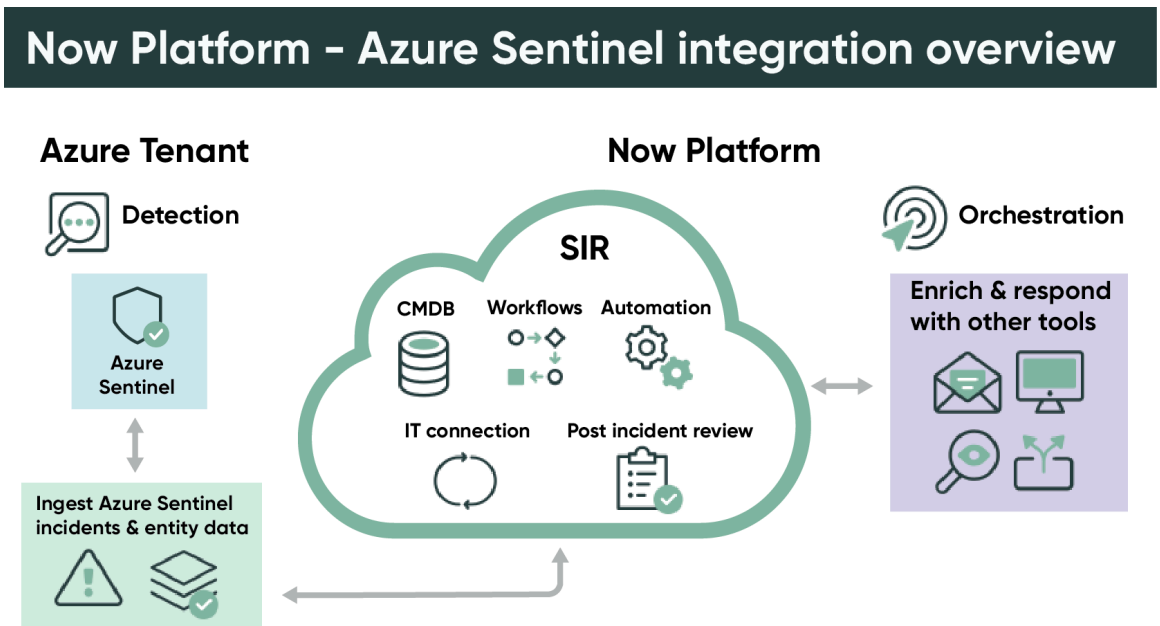
Microsoft Azure Sentinel 는 클라우드 기반 SIEM(Security Information Event Management) 및 SOAR(Security Orchestration Automated Response) 솔루션입니다. 통합을 사용하여 Microsoft Azure Sentinel Azure Sentinel 인시던트를 수집하고 에서 보안 인시던트를 자동으로 생성할 수 있습니다 보안 인시던트 응답.

스토어에서 앱 요청

ServiceNow Store 웹 사이트를 방문하면 사용 가능한 모든 앱을 확인하고 스토어에 요청을 제출하는 방법에 대한 정보를 참조할 수 있습니다. 출시된 모든 앱의 누적 릴리스 정보는 ServiceNow Store 버전 기록 릴리스 정보 를 참조하십시오.

개요

애플리케이션과 통합하는 방법을 Microsoft Azure Sentinel 알아보려면 다음 다이어그램을 ServiceNow AI Platform 보안 운영 참조하십시오.



주요 기능

이 통합의 주요 기능을 사용하여 다음 작업을 수행합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 보안 인시던트 후보인 인시던트를 검색하고 Microsoft Azure Sentinel 이러한 보안 인시던트 생성을 자동화합니다.
- 인시던트 및 엔터티 필드를 보안 인시던트 필드에 매핑 Microsoft Azure Sentinel 합니다 SIR .
- 인시던트를 필터링 Microsoft Azure Sentinel 합니다.
- 중복 보안 인시던트를 생성할 필요가 없도록 인시던트를 기존 미해결 보안 인시던트에 집계합니다.
- 보안 인시던트를 만들고 종결할 수 있도록 보안 인시던트 응답에 대한 인시던트 상태 업데이트를 자동화 Microsoft Azure Sentinel 합니다.

> **주:**
> ServiceNow 보안 인시던트 생성 또는 종결에 따라 인시던트의 상태를 Microsoft Azure Sentinel 업데이트합니다. 이 업데이트에는 집계된 인시던트와 새 인시던트에 대한 코멘트도 포함됩니다.

- 주기적으로 보안 인시던트를 생성하도록 인시던트 수집을 예약합니다.
- 인시던트 코멘트를 작업 메모와 SIR 동기화합니다Microsoft Azure Sentinel.

이 통합에 대해 알아보기

문서 식별자	문서 제목
Microsoft 제품 설명서 웹 사이트	Microsoft 제품 설명서 웹 사이트
ServiceNow 제품 설명서 웹 사이트	ServiceNow 제품 설명서 웹 사이트

통합 시작하기 **Microsoft Azure Sentinel**

for Security Operation 플러그인을 활성화하고 설정하여 Microsoft Azure Sentinel - Incident Ingestion 인스턴스 및 보안 인시던트 응답 제품과 인터페이스합니다ServiceNow AI Platform.

통합을 사용하려면 Microsoft Azure Sentinel 먼저 다음 ServiceNow Store에서 다운로드해야 합니다.

필요한 역할: Microsoft Azure 애플리케이션 개발자, Microsoft Azure 테넌트 관리자.

다음 설정 검사 목록을 검토하고 원활한 통합을 위한 모든 작업을 완료했는지 확인합니다.

검사 목록

설정 작업	설명
필수 ServiceNow AI Platform 및 보안 인시던트 응답 역할을 할당하고 확인합니다.	예상 결과를 구성하고 검증하려면 다음 역할이 필요합니다. • 관리자 역할은 에서 ServiceNow Store 통합을 설치하고 sn_si.ingestion_profile_admin 역할을 할당합니다. • sn_si.ingestion_profile_admin 역할은 다음 작업을 수행합니다. ○ 통합을 구성합니다. ○ 인시던트 프로파일을 생성합니다. ○ Microsoft Azure Sentinel 인시던트 데이터 필드를 보안 인시던트 필드에 매핑합니다. ○ 진행 중인 인시던트 수집을 예약합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

검사 목록

설정 작업	설명
	○ 인시던트가 생성되거나 종결되면 인시던트 업데이트를 보안 인시던트 응답 활성화합니다. ○ 보안 인시던트 분석가(sn_si.analyst) 역할을 할당합니다.
필요한 역할을 할당합니다 Microsoft Azure .	애플리케이션을 등록하고 구성하려면 다음 역할이 필요합니다 Microsoft Azure . • 애플리케이션을 등록할 애플리케이션 개발자입니다. • 테넌트 관리자가 관리자 동의 엔드포인트를 호출하여 애플리케이션에 권한을 부여합니다.
ServiceNow 이 통합을 구성하기 전에 통합을 지원하는 데 필요한 핵심 애플리케이션이 설치되고 활성화되었는지 확인합니다.	Starter Pack Installer [com.glide.hub.integrations] 플러그인이 ServiceNow 통합 허브 필요합니다. 플러그인(com.snc.security_incident)이 보안 인시던트 응답 필요합니다. 이 플러그인은 제품을 지원하는 데 필요한 모든 종속성을 보안 인시던트 응답 자동으로 설치합니다. 통합에 필요한 다른 보안 운영 애플리케이션을 설치하고 활성화하기 전에 이 플러그인을 설치하고 활성화합니다. 에서 ServiceNow Store다음 보안 운영 애플리케이션이 설치되고 활성화되는지 확인합니다. 이러한 애플리케이션이 아직 설치되어 있지 않은 경우 원활한 설치를 위해 다음 순서로 각 애플리케이션을 설치하고 한 번에 하나씩 활성화해야 합니다. **1.** 보안 인시던트 응답 **2.** 보안 인시던트 응답 UI **3.** ServiceNow 통합 허브 런타임 (com.glide.hub.integration.runtime) **4.** ServiceNow IntegrationHub Action Step - REST (com.glide.hub.action_step.rest)
에서 애플리케이션 등록 및 구성 Microsoft Azure 입구.	포털에 애플리케이션을 Microsoft Azure 등록하고 사용자에게 애플리케이션에 대한 읽기 및 쓰기 권한을 부여합니다.

포털 등록 및 구성 **Microsoft Azure**

포털에 애플리케이션을 Microsoft Azure 등록하고 사용자에게 애플리케이션에 대한 읽기 및 쓰기 권한을 부여합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: Microsoft Azure 애플리케이션 개발자, Microsoft Azure 테넌트 관리자

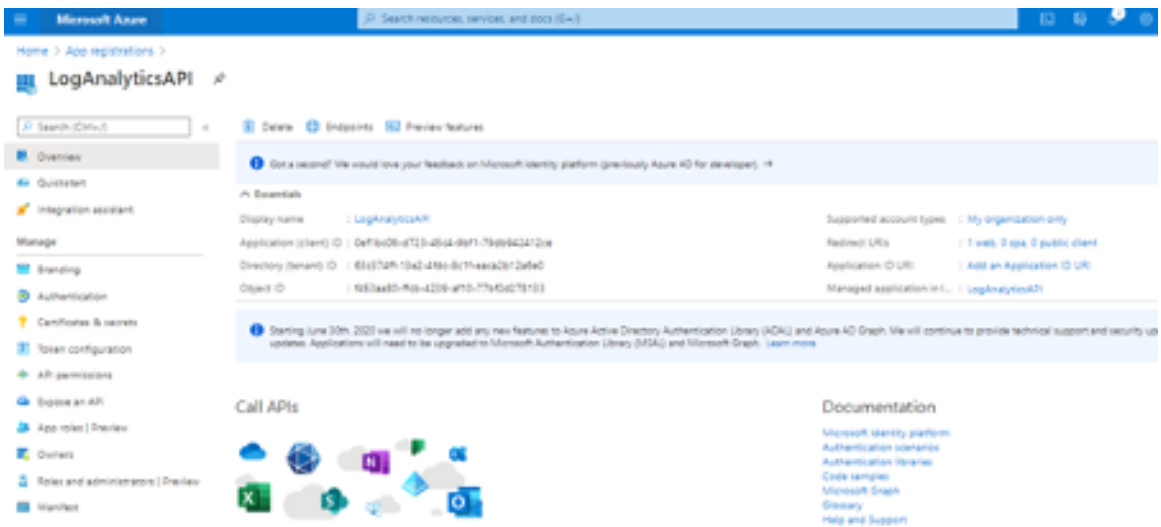
프로시저

1. 포털에 로그인합니다 Microsoft Azure .
2. 앱 등록을 검색하여 선택합니다.
3. 신규 등록을 클릭합니다.
4. 양식에서 필드를 채웁니다.

애플리케이션 등록 양식

필드	설명
이름	애플리케이션의 사용자용 표시 이름입니다. 예: LogAnalyticsAPI.
지원되는 계정 유형	이 애플리케이션을 사용하거나 API에 액세스할 수 있는 계정 유형입니다.
리디렉션 URI	리디렉션 URI입니다. 사용자를 성공적으로 인증한 후 인증 응답이 이 URI로 전달됩니다.

5. 등록을 클릭합니다.
애플리케이션을 성공적으로 등록하면 개요 페이지가 표시됩니다.



6. 다음으로 이동 관리 〉 인증서 및 비밀.
7. 클라이언트 암호 섹션에서 새 클라이언트 암호를 클릭합니다.
나중에 클라이언트 비밀을 볼 수 없으므로 이 단계에서 지금 클라이언트 비밀을 복사하여 저장해야 합니다. 클라이언트 암호를 잊어버린 경우 4단계와 5단계의 지침에 따라 새 클라이언트 암호를 생성할 수 있습니다.
8. 다음으로 이동 관리 〉 **API** 권한.
9. 권한 추가를 클릭합니다.
10. API 권한 요청 창에서 조직에서 사용하는 **API** 탭을 클릭합니다.
11. **Log Analytics API** 앱 이름을 검색하여 선택합니다.
12. Log Analytics API 권한에서 애플리케이션 권한을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 권한을 사용하도록 설정하면 애플리케이션이 로그인한 사용자 없이 백그라운드 서비스 또는 디먼으로 실행됩니다.

13. 데이터 섹션에서 **Data.Read**를 선택합니다
14. 권한 추가를 클릭합니다.
    권한이 업데이트됩니다.
15. 13단계에서 사용하도록 설정한 Data.Read API 권한에 대해 기본 디렉터리에 대한 관리자 동의 부여 옵션을 사용하도록 설정합니다.
16. **Log Analytics** 작업 영역을 검색하여 선택합니다.
17. Sentinel Log Analytics 작업 영역을 선택합니다.
    이제 Sentinel Log Analytics 작업 영역 개요 페이지가 표시됩니다.
18. 다음으로 이동 액세스 제어**(IAM)** 〉 역할 할당.
19. 추가를 클릭하고 역할 할당 추가를 선택합니다.
20. 양식에서 필드를 채웁니다.

역할 할당 추가 양식

필드	설명
역할	이 애플리케이션을 사용할 수 있는 계정 유형입니다. **Azure Sentinel** 응답자를 선택합니다.
다음에 대한 액세스 권한 할당	사용자가 정의하는 권한 범위입니다. 사용자, 그룹 또는 서비스 주체를 선택합니다.
선택	4단계의 앞부분에서 생성한 애플리케이션입니다. 예: LogAnalyticsAPI.

21. 저장을 클릭합니다.

통합 설치 및 구성 **Microsoft Azure Sentinel**

인스턴스에서 통합을 ServiceNow StoreServiceNow AI Platform 설치하고 구성하여 Microsoft Azure Sentinel Azure Sentinel 인시던트 수집을 시작합니다.

시작하기 전에

필요한 역할: sn_si.ingestion_profile_admin

> **주:**
> sn_si.admin 역할은 기본적으로 필수 권한을 상속하므로 sn_si.admin 역할을 가진 사용자는 프로필 관리자가 사용할 수 있는 모든 작업을 수행할 수 있습니다.

프로시저

1. Microsoft Azure Sentinel 에서 ServiceNow Store 통합을 다운로드하여 설치합니다.
2. 다음으로 이동 보안 운영 〉 통합 〉 통합 구성.
3. 타일을 Microsoft Azure Sentinel 검색하고 구성을 클릭합니다.
4. 양식에서 필드를 채웁니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Microsoft Azure Sentinel - 인시던트 수집 구성 양식

필드	설명
이름	Microsoft Azure Cloud 인스턴스 구성의 이름입니다.
ID URL	테넌트의 ID URL입니다 Microsoft Azure Cloud . 예: login.microsoftonline.com. 자세한 내용은 Microsoft Azure 설명서를 참조하십시오.
Azure 자원 관리자	테넌트용 Azure Resource Manager 엔드포인트.Microsoft Azure Cloud 예를 들어 management.azure.com. 자세한 내용은 Microsoft Azure 설명서를 참조하십시오.
테넌트 ID	Microsoft Azure Sentinel 테넌트 ID입니다. 포털의 모든 인시던트가 검색되는 인스턴스입니다 Microsoft Azure .
클라이언트 ID	포털에 등록한 애플리케이션의 클라이언트 ID입니다 Microsoft Azure .
클라이언트 비밀	등록된 애플리케이션의 클라이언트 비밀입니다.
구독 ID	등록된 애플리케이션의 구독 ID입니다.
자원 그룹 이름	등록된 애플리케이션의 자원 그룹 이름입니다.
작업 공간 이름	등록된 애플리케이션의 작업 공간 이름입니다.

5. 제출을 클릭합니다.

결과
구성을 성공적으로 확인하고 제출하면 각 인시던트 수집 서버 구성이 보안 통합 페이지에 타일로 저장됩니다.

에 대한 프로파일 생성 **Microsoft Azure Sentinel**

인스턴스에 인시던트 프로파일을 ServiceNow AI Platform 생성하고 보안 인시던트를 만들기에 적합한 인시던트를 결정합니다 Microsoft Azure Sentinel .

시작하기 전에
필요한 역할: sn_si.ingestion_profile_admin

> **주:**
> sn_si.admin 역할은 기본적으로 필수 권한을 상속하므로 sn_si.admin 역할을 가진 사용자는 프로필 관리자가 사용할 수 있는 모든 작업을 수행할 수 있습니다.

이 태스크 정보
통합을 통해 무단 액세스 시도 및 맬웨어와 같은 다양한 유형의 인시던트를 만들 수 있습니다. 이러한 인시던트는 인스턴스에서 구성한 ServiceNow AI Platform 프로파일을 기반으로 생성됩니다. 모든 인시던트는 처음에 프로파일에 구성된 인시던트 유형에 대해 만들어집니다. 생성된 인시던트를 추가로 필터링하여 보안 인시던트를 생성하는 인시던트를 지정할 수 있습니다.

테넌트의 Microsoft Azure 선택 기준을 충족하고 API를 Microsoft Azure Sentinel 통해 사용할 수 있는 모든 인시던트는 처음에 인스턴스에 수집 ServiceNow AI Platform 됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 **Microsoft Azure Sentinel** 통합 〉 **Azure Sentinel** 인시던트 프로파일.
2. 새로 만들기를 클릭합니다.
3. 양식에서 필드를 채웁니다.

Microsoft Azure Sentinel - 인시던트 수집 구성 양식

필드	설명
이름	프로파일의 이름입니다. 이 이름은 프로파일 유형을 식별하는 데 도움이 되며 이 프로파일과 연결된 보안 태그의 기본 이름이기도 합니다.
활성	프로파일이 활성 상태임을 나타내는 표시기입니다. 프로파일이 활성 상태이면 가 ServiceNow AI Platform Azure Sentinel 인시던트를 적극적으로 폴링하고 있으며 필터링 조건이 일치할 때 해당 보안 인시던트가 생성 SIR 됨을 의미합니다.
소스	Microsoft Azure 인시던트를 수집하도록 구성한 테넌트입니다. 여러 테넌트가 구성된 경우 프로파일에 대해 수집하려는 인시던트 유형에 적합한 테넌트를 선택합니다.
순서	플로우 우선순위입니다. 이 필드의 값은 둘 이상의 프로파일이 트리거 조건을 공유할 때 플로우가 실행되는 순서를 나타냅니다. 숫자가 가장 낮은 플로우의 우선순위가 가장 높습니다. 작업 순서를 설정하려면 값을 입력합니다. 예를 들어 100, 200, 300, 400입니다. 기본값은 100입니다.
설명	이 프로파일을 다른 프로파일과 구별하는 데 도움이 되는 추가 텍스트입니다.

4. 매핑 섹션으로 이동하려면 계속을 클릭합니다.

다음에 수행할 작업
개별 Microsoft Azure Sentinel 인시던트 필드를 보안 인시던트의 필드에 매핑합니다 ServiceNow AI Platform SIR .

Microsoft Azure Sentinel 인시던트 필드 매핑

매핑된 데이터로 인시던트를 생성할 수 있도록 개별 Microsoft Azure Sentinel 인시던트 필드를 보안 인시던트의 SIR 필드에 매핑합니다.

시작하기 전에
필요한 역할: sn_si.ingestion_profile_admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
sn_si.admin 역할은 기본적으로 필수 권한을 상속하므로 sn_si.admin 역할을 가진 사용자는 프로필 관리자가 사용할 수 있는 모든 작업을 수행할 수 있습니다.

프로시저

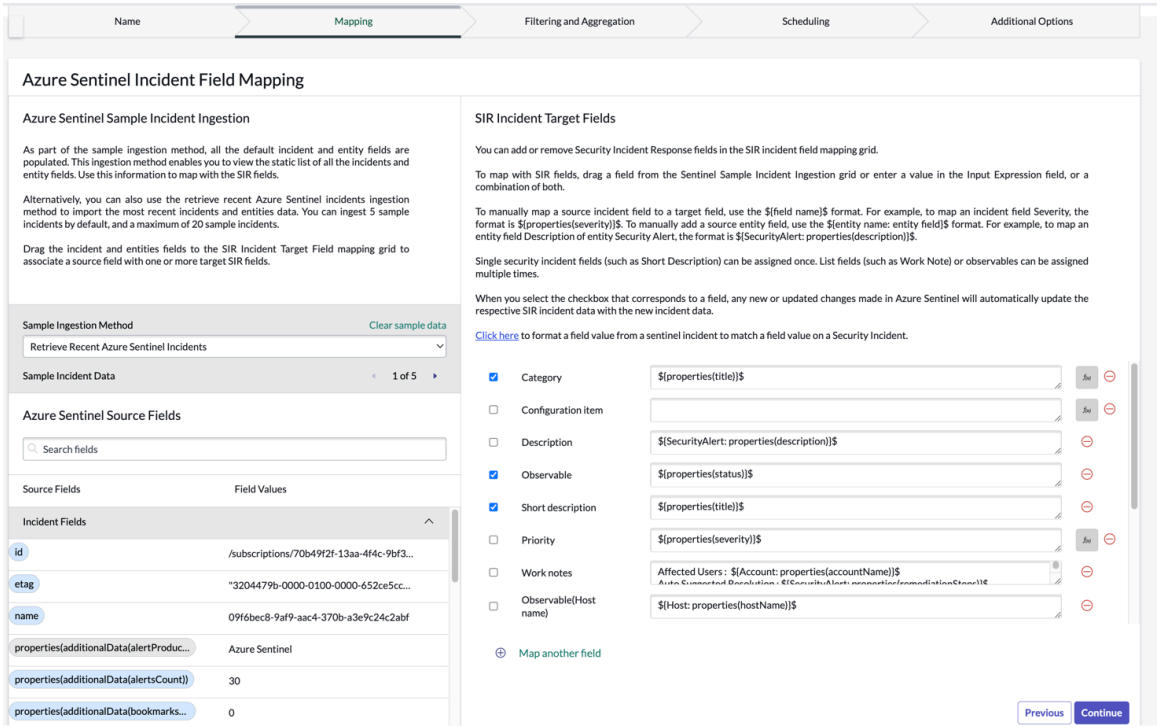
1. 매핑 페이지의 Azure Sentinel 필드 매핑 섹션에서 샘플 수집 방법 중 하나를 선택합니다.

샘플 수집 방법

필드	설명
모든 기본 인시던트 및 엔터티 필드	이 수집 방법을 사용하여 모든 인시던트 및 엔터티 필드의 정적 목록을 봅니다. 이 메서드에는 값 없이 기본 필드 이름만 포함됩니다. 이 정보를 사용하여 필드와 매핑할 수 있습니다 SIR .
최근 Azure Sentinel 인시던트 검색	이 수집 방법을 사용하여 가장 최근의 인시던트 및 엔터티 데이터를 임포트합니다. Azure Sentinel 인시던트에 엔터티 데이터가 포함되어 있으면 엔터티 데이터가 검색되고 Azure Sentinel 소스 필드 섹션에서 매핑할 수 있습니다. 경우에 따라 Azure Sentinel 인시던트에 엔터티 데이터가 포함되어 있지 않을 수 있으므로 이러한 시나리오에서 엔터티 필드를 매핑할 수 없습니다. Azure Sentinel 인시던트에 여러 경고가 포함된 경우 인시던트의 일부인 가장 빠른 경고가 매핑 섹션에 표시됩니다. 수집 중에도 가장 빠른 보안 경보 필드 값이 사용됩니다. 기본적으로 5개의 샘플 인시던트를 수집할 수 있으며 최대 20개의 샘플 인시던트를 수집할 수 있습니다. 샘플 인시던트 필드 값은 프로파일이 샘플 인시던트를 수집할 때 채워집니다. 이러한 인시던트를 **SIR** 인시던트 대상 필드에 매핑할 수 있습니다. 인시던트 필드와 값이 개별 탭으로 표시됩니다.
샘플 데이터 임포트	샘플 데이터 임포트를 클릭하여 Azure Sentinel에서 샘플 인시던트를 임포트합니다. 이 버튼은 최근 Azure Sentinel 인시던트 수집 검색 방법을 선택할 때 나타납니다. 서버에서 샘플 인시던트 Microsoft Azure Sentinel 를 검색하는 데 시간이 걸릴 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	검색된 이 인시던트를 **SIR** 인시던트 대상 필드에 매핑합니다. 인시던트 필드와 값이 개별 탭으로 표시됩니다.



2. 보안 인시던트에 표시되는 기본 필드에 필드를 추가하려면 다음 작업을 수행합니다.

a. SIR 인시던트 대상 필드 섹션에서 Map another field 다른 필드 매핑 버튼.
표시할 새 필드에 대한 필드를 선택할 수 있는 필드 목록이 SIR 표시됩니다.

b. 보안 인시던트 열에서 표시되는 목록을 확장한 다음 필드를 선택합니다.

주:
동일한 보안 인시던트에 여러 옵저버블을 표시할 수 있습니다. 예를 들어 옵저버블 필드는 서로 다른 값으로 여러 번 매핑될 수 있습니다. 마찬가지로 구성 항목 및 작업 메모 필드는 여러 값을 지원합니다. 여러 값을 지원할 수 없는 필드에 두 값을 매핑하려고 하면 이 필드가 여러 값을 지원하지 않는다는 오류 메시지가 표시됩니다. 마찬가지로 보안 인시던트의 필드에 여러 옵션을 선택할 수 있는 목록이 있고 목록에 표시되지 않은 해당 필드에 옵션을 매핑하려고 하면 필드가 보안 인시던트에 채워지지 않습니다.

c. Azure Sentinel 소스 필드 섹션에서 필드를 끌어서 놓아 새 필드에 매핑합니다.

d. 필드에 해당하는 확인란을 선택하면 Azure Sentinel에서 새로 변경하거나 업데이트된 변경 내용이 있으면 해당 SIR 인시던트 데이터가 새 인시던트 데이터로 자동으로 업데이트됩니다.

주:
기본 시스템에서 SIR에 연결된 새 경보와 관련된 업데이트를 받으려면 Microsoft Azure Sentinel 시스템 속성 sn_sec_sentinel.incident_updates가 기본적으로 True로 설정됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 기본적으로 영향을 받는 사용자, 구성 항목 및 옵저버블 필드가 선택되어 있습니다. 즉, 새로운 옵저버블이나 관련 구성 항목이 있거나 영향을 받는 사용자가 인시던트에 추가될 때마다 해당 폴링 간격 동안 해당 정보가 자동으로 추출되어 보안 인시던트 응답(SIR)의 관련 목록에 채워집니다.
- 다른 필드의 경우 Azure Sentinel 내의 Azure Sentinel 인시던트 기록에서 수행된 새 변경 내용 또는 업데이트된 변경 내용에 대한 필드에 해당하는 확인란을 선택해야 합니다. 이렇게 하면 해당 SIR 인시던트 데이터가 새 인시던트 데이터로 자동 업데이트됩니다.

중요사항:
기존 데이터를 재정의하면 분석가가 작업할 데이터가 불안정해질 수 있으며 보안 인시던트의 필드 값으로 설정된 다른 자동화도 영향을 받을 수 있으므로 이 기능을 선택하기 전에 실사를 수행해야 합니다. 따라서 재정의 기능을 선택하기 전에 실사를 수행하는 것이 매우 중요합니다.

3. 필드를 제거하려면 SIR 인시던트 대상 필드 섹션의 입력 식 필드 옆에 있는 ⊖ 항목 제거 버튼을 사용합니다.
4. Azure Sentinel 소스 필드 섹션의 필드 값을 SIR 인시던트 대상 필드 섹션의 필드에 매핑하려면 다음 작업 중 하나를 사용합니다.

   a. 필드 이름(예: id)을 끌어서 SIR 인시던트 대상 필드 열의 필드 이름 옆에 놓습니다.

   Azure Sentinel 소스 필드 섹션의 모든 값을 SIR 인시던트 대상 필드 섹션의 필드와 일치시킬 수 있습니다. 필드는 색상으로 구분되므로 매핑 프로세스에서 인시던트 필드를 간과하거나 중복하는 일이 없습니다. 연한 파란색 필드는 인시던트 필드가 아직 선택되지 않았으며 보안 인시던트에 매핑되지 않았음을 나타냅니다. 수신 인시던트 필드를 보안 인시던트의 둘 이상의 필드와 연결하는 것을 선호할 수 있습니다. 회색 필드는 필드가 선택되었고 보안 인시던트의 필드에 매핑되었음을 나타냅니다. 이렇게 하면 보안 인시던트에 추가된 필드 값과 나머지 중요한 인시던트 정보가 매핑되지 않은 상태로 남아 있는지 시각화할 수 있습니다.

   b. 텍스트와 필드의 조합을 추가할 수 있습니다.
   예를 들어 #### ### ${name}$###. 여기서 #### ### Azure Sentinel 소스 필드 섹션에서 ${name}$ 이 매핑되는 동안 수동으로 입력할 수 있습니다.

   c. 소스 인시던트 또는 엔터티 필드를 직접 수동으로 입력하고 대상 필드에 매핑할 수 있습니다.
   - 소스 인시던트 필드를 수동으로 매핑하려면 ${field name}$ 형식을 사용합니다. 예를 들어 인시던트 필드 심각도를 매핑하려면 ### ${properties(severity)}$입니다.
   - 원본 엔터티 필드를 수동으로 추가하려면 ${entity name: entity field}$ 형식을 사용합니다. 예를 들어 엔터티 필드 Description of entity Security Alert를 매핑하려면 형식은 ${SecurityAlert: properties(description)}$입니다.

이 통합은 특정 옵저버블 하위 유형을 분류합니다. Azure Sentinel 필드를 SIR 옵저버블 필드와 매핑하면 옵저버블이 ServiceNow AI Platform 자동 분류됩니다. 들어오는 Azure Sentinel 옵저버블을 의 옵저버블 유형에 SIR일반적으로 매핑하려면 옵저버블 필드에 Azure Sentinel 필드를 끌어서 놓습니다. 그러나 에서 들어오는 Azure Sentinel 옵저버 SIR블에 대한 옵저버블 유형을 알고 있는 경우 옵저버블 유형 필드에 구체적으로 매핑합니다 SIR . 에서 SIR 특정 옵저버블 유형의 예로는 Observable(도메인 이름), Observable(이메일 주소), Observable(IP 주소(V4)) 및 Observable(호스트 이름)이 있습니다.

들어오는 Azure Sentinel 필드에 정보가 포함되어 MITRE-ATT&CK 있으면 기술 필드에 매핑합니다 MITRE-ATT&CK . 들어오는 Azure Sentinel 필드에 기술 ID 또는 기술 이름이 포함되어 MITRE-ATT&CK 있는지 확인합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

의 인시던트 필드 값이 Microsoft Azure Sentinel SIR 보안 인시던트의 필드로 직접 변환되지 않을 수도 있습니다. 이러한 값의 경우 스크립트 편집기를 사용하여 매핑 단계 중에 보안 인시던트의 필드 값에 대한 형식을 지정할 수 있습니다. 비슷하지만 동일하지는 않은 값의 형식을 지정하려면 스크립트 편집기를 사용하십시오.

5. Azure Sentinel 인시던트의 새 필드에 대한 필드 번역의 형식을 보안 인시던트의 필드 값과 일치하도록 지정하려면 **SIR** 인시던트 대상 필드 헤더에서 여기를 클릭 링크를 클릭하십시오.
6. 필드 번역을 지원하는 필드를 수정하려면 스크립트 형식 필드 번역 아이콘을 클릭하십시오.

   필드 번역을 지원하는 필드는 범주, 구성 항목 및 우선순위입니다. 예를 들어 범주 옆에 있는 아이콘을 클릭합니다. Azure Sentinel 필드 변환 스크립트 편집기가 열립니다.
7. 스크립트에 대한 변경 내용을 입력하고 업데이트를 클릭하여 변경 내용을 저장하고 매핑 페이지로 돌아갑니다.
   예를 들어 범주의 경우 스크립트 편집기에서 다음을 정의합니다.

   ```
   "<Incoming Sentinel Incident Field Value>" : "<Category to assign to the Security Incident>".
   ```

   이 매핑을 통해 프로파일은 구성된 범주만 사용합니다.
8. 필드 값을 추가하거나 제거하여 매핑을 계속합니다.
   인시던트 생성 조건 작성기에서 동일한 필드 값을 사용하여 수신 인시던트가 보안 인시던트를 만들기 위해 충족해야 하는 추가 기준을 정의할 수 있습니다.
9. 필터링 및 집계 섹션으로 이동하려면 계속을 클릭합니다.

다음에 수행할 작업

보안 인시던트를 생성할 인시던트를 지정할 수 있도록 필터 조건을 정의하고 설정합니다. 인시던트 생성 조건 작성기(필터링 및 집계 섹션)에서 동일한 필드 값(매핑 섹션에 정의됨)을 사용하여 수신 인시던트가 보안 인시던트를 만들기 위해 충족해야 하는 추가 기준을 정의할 수 있습니다.

필터 및 집계 기준 정의

보안 인시던트를 생성해야 하는 수신 Microsoft Azure Sentinel 인시던트를 지정할 수 있도록 필터 조건을 정의하고 설정할 수 있습니다. 인시던트를 생성하는 대신 수신 인시던트를 미해결 보안 인시던트에 추가할 수 있는 추가 인시던트 필드 기준을 정의할 수도 있습니다.

보안 인시던트에 대한 필터링 조건 설정

필터링 조건이 일치하는 경우에만 보안 인시던트가 생성되도록 필터링 조건을 설정합니다.

시작하기 전에

필요한 역할: sn_si.ingestion_profile_admin

> **주:**
> sn_si.admin 역할은 기본적으로 필수 권한을 상속하므로 sn_si.admin 역할을 가진 사용자는 프로필 관리자가 사용할 수 있는 모든 작업을 수행할 수 있습니다.

이 태스크 정보

이러한 유형의 필터링은 보안 인시던트를 격리하고 생성하는 보안 인시던트 수를 제한하는 데 도움이 됩니다. 추가 필터링 기준을 설정하면 쿼리 또는 트리거된 인시던트 구성을 변경할 필요 없이 필요한 인시던트만 수집됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 보안 인시던트가 생성되도록 수신 Microsoft Azure Sentinel 인시던트가 충족해야 하는 기준을 정의하려면 조건에 따라 필터링을 선택합니다.

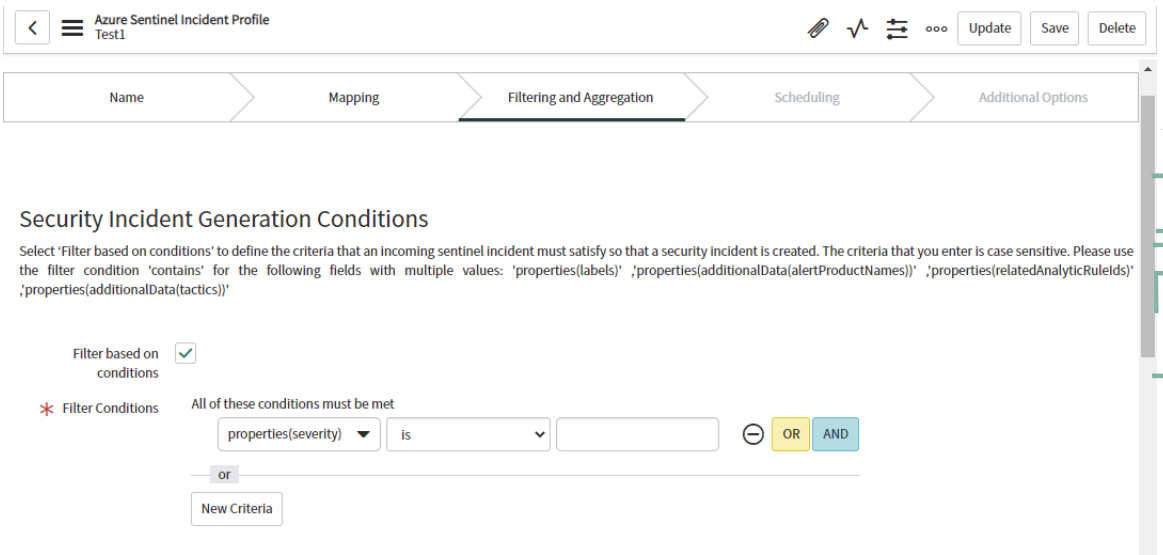
   필터 조건의 첫 번째 필드에 있는 옵션은 수집한 인시던트에 대한 Azure Sentinel 샘플 인시던트 수집 섹션에 표시되는 필드와 일치합니다. 이러한 필드는 동적이며 수집하는 인시던트에 따라 변경됩니다. 입력하는 기준은 대/소문자를 구분합니다. 정의하는 기준이 인시던트 값과 일치하는지 확인합니다.

   여러 값이 있는 다음 필드에 대해 필터 조건 *##* 을 사용합니다.

   - properties(labels)
   - properties(additionalData(alertProductNames))
   - properties(relatedAnalyticRuleIds)
   - properties(additionalData(tactics))

   필터 조건은 문자열만 검색할 수 있으므로 데이터가 올바르게 필터링되도록 위 필드에 *## `contains`* 필터 조건을 사용해야 합니다.

보안 인시던트 생성 조건



2. 조건 작성기의 목록과 필드를 사용하여 첫 번째 행의 필터를 설정합니다.
3. 조건을 더 추가하려면 **AND** 또는 **OR**을 클릭합니다.
   - **AND**를 선택하면 모든 조건이 일치해야 합니다.
   - **OR**을 선택하면 두 조건을 일치시킬 수 있습니다.
4. 두 번째 필터 조건을 설정하려면 새 기준을 클릭합니다.

집계 조건 정의

중복될 가능성이 있는 유사한 인시던트를 생성하는 대신 수신 인시던트를 기존 SIR 보안 인시던트로 집계하는 추가 인시던트 집계 기준을 정의합니다. 각 프로파일에 대해 필드 일치 값 기준을 사용하는 경우 이 추가 집계는 모든 관련 인시던트 데이터를 단일 보안 인시던트에 배치하여 활성 상태의 중복 보안 인시던트 수를 줄일 수 있습니다.

시작하기 전에
필요한 역할: sn_si.ingestion_profile_admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

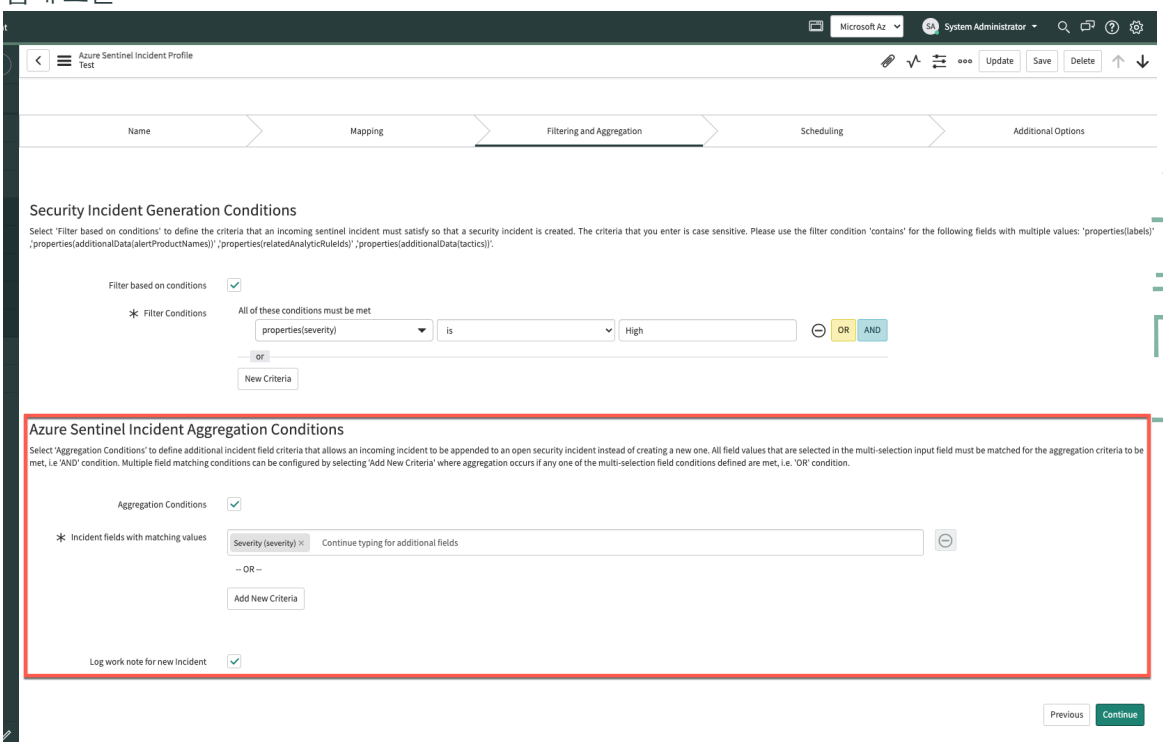
주:
sn_si.admin 역할은 기본적으로 필수 권한을 상속하므로 sn_si.admin 역할을 가진 사용자는 프로필 관리자가 사용할 수 있는 모든 작업을 수행할 수 있습니다.

이 태스크 정보
새 인시던트가 매핑 단계의 집계 필드 조건에서 선택한 모든 값과 일치하는 경우, 인시던트는 동일한 필드 값을 사용하여 가장 최근에 열린 보안 인시던트에 자동으로 추가됩니다. 보안 인시던트를 담당하는 sn_si.analyst 역할을 가진 사용자는 보안 인시던트의 관련 목록에서 추가된 모든 집계 인시던트를 볼 수 있습니다.
보안 인시던트의 모든 집계 인시던트가 Azure Sentinel 집계 인시던트 관련 목록에 표시됩니다. 이 목록은 관련 타임스탬프 및 집계된 필드 값에 대해 자세히 설명합니다. 이 정보는 기존 보안 인시던트에 인시던트가 추가되는 이유를 이해하는 데 도움이 됩니다.

프로시저

1. 새 인시던트를 생성하는 대신 수신 Microsoft Azure Sentinel 인시던트를 미해결 보안 인시던트에 추가할 수 있는 추가 인시던트 필드 기준을 정의하려면 다음 그림과 같이 집계 조건 옵션을 선택합니다.

집계 조건



2. 일치하는 값이 있는 인시던트 필드 필드에 인스턴스의 기존 보안 인시던트 ServiceNow AI Platform와 일치시키려는 필드 값을 입력합니다.
집계 기준이 충족되고 이 수신 인시던트를 기존 보안 인시던트에 추가할 수 있도록 다중 선택 입력 필드에서 선택한 모든 필드 값이 일치해야 합니다. 이 선택은 여러 필드 값을 가질 수 있는 옵저버블 및 구성 항목과 같은 필드가 매핑되는 *AND* 조건을 의미합니다. 값의 하위 집합만 일치하면 Azure Sentinel 인시던트 집계 조건이 충족되지 않고 새 보안 인시던트가 생성됩니다.
3. 여러 필드 일치 조건을 추가하려면 새 기준 추가를 클릭합니다.
사용자가 정의하는 다중 선택 필드 조건 중 하나가 충족되면 집계가 발생합니다. 이 선택은 *OR* 조건을 의미합니다.
4. 새 인시던트가 보안 인시던트에 추가될 때 해당 인시던트에 대한 작업 메모를 업데이트하려면 새 인시던트에 대한 작업 메모 기록을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업 메모는 새 인시던트가 추가되었음을 기록하고 인시던트 상세 정보에 대한 링크를 포함합니다. 로그 작업 메모는 매핑 섹션의 작업 메모 필드에 추가하는 상세 정보도 업데이트합니다.

5. 일정을 구성하려면 계속을 클릭합니다.

다음에 수행할 작업
프로파일의 기준과 일치하는 인시던트 데이터 및 수집된 인시던트를 검색하도록 일정을 설정합니다.

Microsoft Azure Sentinel 인시던트 검색 예약

인시던트 데이터를 검색하고 프로파일의 기준과 일치하는 인시던트를 수집 Microsoft Azure Sentinel 하도록 일정을 설정합니다.

시작하기 전에
필요한 역할: sn_si.ingestion_profile_admin

> **주:**
> sn_si.admin 역할은 기본적으로 필수 권한을 상속하므로 sn_si.admin 역할을 가진 사용자는 프로필 관리자가 사용할 수 있는 모든 작업을 수행할 수 있습니다.

이 태스크 정보
인시던트 프로파일 구성과 일치하는 향후 Microsoft Azure Sentinel 인시던트를 폴링할 빈도를 계획할 수 있습니다.

자동 인시던트 수집을 사용하려면 프로파일을 활성화하기 전에 예약 및 인시던트 검색을 구성해야 합니다. 초기 수집에 대한 특정 날짜 및 시간을 정의하려면 인시던트 수집 시간 설정을 활성화합니다. 후속 수집은 폴링 간격 기간을 기반으로 합니다.

폴링 간격은 각 프로파일에 대해 개별적으로 구성됩니다. 다양한 폴링 간격은 인시던트 통합의 성능에 영향을 줄 수 있습니다 Microsoft Azure Sentinel . 일정을 예약할 때 인시던트의 긴급도에 따라 시스템 부하의 균형을 맞추도록 계획합니다. 모든 프로필에 대해 1분 기본값이 설정됩니다. 인시던트의 긴급도와 시스템의 예상 로드에 따라 이 설정을 수정할 수 있습니다.

특정 폴링 간격으로 인시던트에 추가되는 모든 경보는 프로세스가 실행된 다음 Azure Sentinel 경보 관련 목록에 추가되고 작업 메모도 게시됩니다.

프로시저

1. 예약 양식의 필드에 내용을 입력합니다.

   테넌트에서 인시던트를 끌어오는 방법과 시기를 정의하도록 Microsoft Azure 일정을 구성합니다.

   일정 양식

필드	설명
지속적 이벤트 수집	인스턴스가 새 인시던트에 대해 테넌트에서 Microsoft Azure 끌어오는 지속적 인시던트 수집 ServiceNow AI Platform 입니다. 트리거된 인시던트가 발견되고 인시던트 생성 필터링 기준이 일치하면 보안 인시던트가 생성됩니다.
폴링 증분(분)	분 단위로 정의된 폴링 빈도입니다.
시던트 수집 시간 설정	구성된 날짜 및 시간을 기준으로 하는 인시던트 수집입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	이 옵션을 사용하여 초기 수집에 대한 특정 날짜 및 시간을 정의할 수 있습니다. 후속 수집은 폴링 간격 기간을 기반으로 합니다.
입력 인시던트 수집 시간	인시던트 수집을 위해 지정하는 날짜 및 시간입니다.
일회성 검색	기록 Azure Sentinel 인시던트를 한 번 검색한 다음 데이터를 조정하려면 이 확인란을 선택합니다. 이 확인 표시를 선택하면 애플리케이션은 약 최대 6개월 동안 열린 모든 Azure Sentinel 인시던트와 닫힌 Azure Sentinel 인시던트를 끌어옵니다. 데이터를 처리할 때 진행 중인 인시던트와 기록 데이터를 모두 끌어오지만, 진행 중인 인시던트의 처리가 기록 끌어오기보다 우선하며, 그렇지 않으면 수집 중인 인시던트 수뿐만 아니라 기간에 따라 기록 끌어오기에 시간이 걸릴 수 있습니다. **주:** 검색된 기록 Azure Sentinel 인시던트는 보안 인시던트 응답 애플리케이션 내에서 중복을 방지하기 위해 중복 제거 검사를 거칩니다.
날짜 이후	Azure Sentinel에서 기록 인시던트를 수집한 이후의 날짜입니다. **주:** 인시던트 데이터는 대략 지난 6개월 동안 가져온 것입니다.

예약 페이지를 사용하면 테넌트에서 인시던트를 끌어오는 방법과 시기를 정의할 수 있습니다 Microsoft Azure .

2. 추가 옵션 페이지로 이동하려면 계속을 클릭합니다.

인시던트 상태별로 SIR 인시던트 업데이트 및 종결 자동화

인시던트 상태에 따라 인시던트 업데이트 및 종결을 자동화합니다 SIR . 통합 Microsoft Azure Sentinel 에는 양방향 인터페이스가 있어 두 인시던트가 보안 인시던트를 생성하고 보안 인시던트가 생성되거나 종결된 후 인시던트를 업데이트할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.ingestion_profile_admin

주:
sn_si.admin 역할은 기본적으로 필수 권한을 상속하므로 sn_si.admin 역할을 가진 사용자는 프로필 관리자가 사용할 수 있는 모든 작업을 수행할 수 있습니다.

프로시저

1. 양식에 상세 정보를 입력합니다.
에서 SIR보안 인시던트를 만들거나 종결할 때 지침에 따라 인시던트를 업데이트하기 위한 구성을 완료합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

인시던트 업데이트 자동화 양식

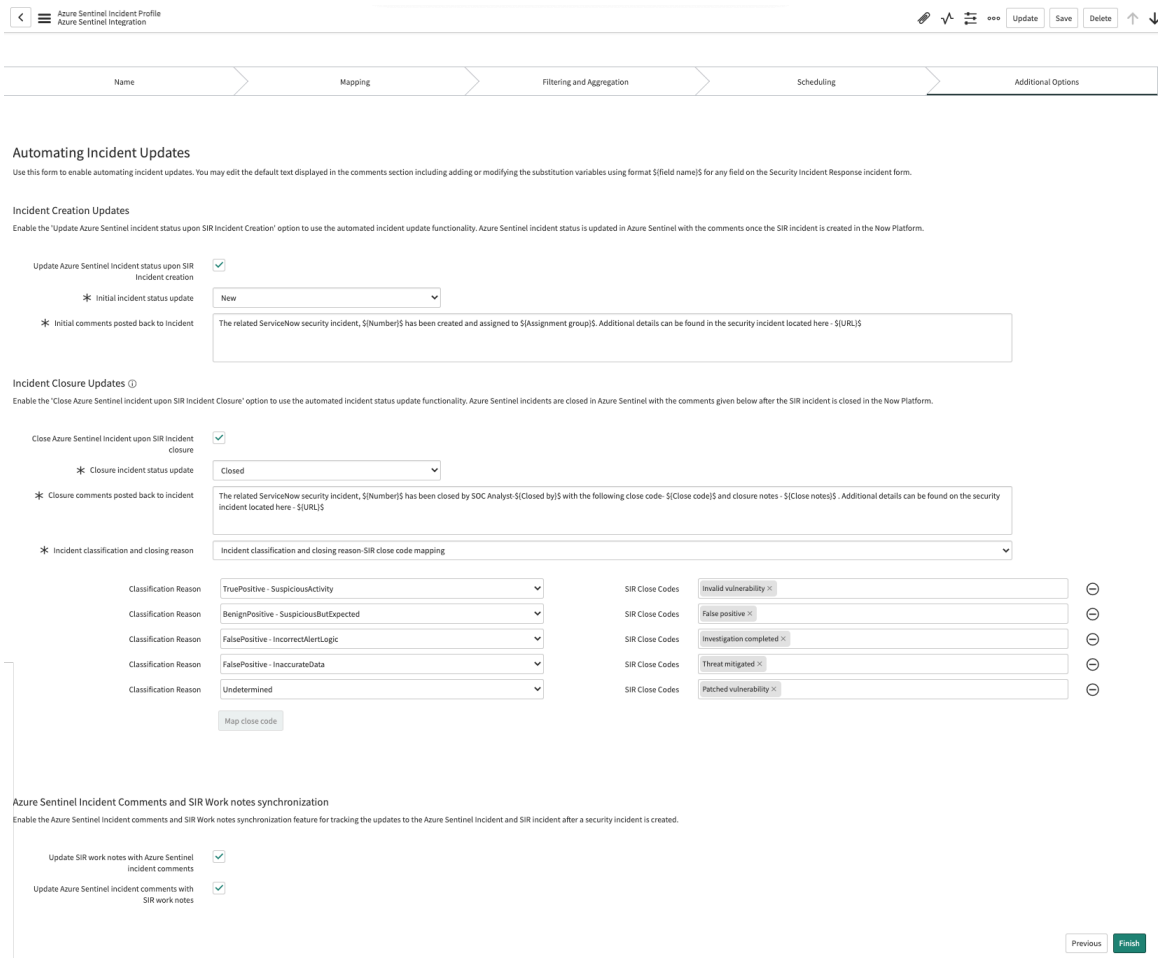
범주	필드	설명
인시던트 작성 업데이트	SIR 인시던트 작성 시 Azure Sentinel 인시던트 상태 업데이트	자동화된 인시던트 업데이트 기능을 사용할 수 있는 옵션입니다. Microsoft Azure Sentinel 인시던트 상태는 에서 ServiceNow AI Platform인시던트가 생성된 후의 SIR 설명과 함께 인시던트에서 Microsoft Azure 업데이트됩니다.
	초기 인시던트 상태 업데이트	환경에서 업데이트된 Microsoft Azure Sentinel 초기 인시던트 상태입니다. 상태로 새로 만들기 또는 활성을 선택할 수 있습니다.
	인시던트에 다시 게시된 초기 설명	환경에서 인시던트에 게시된 초기 코멘트입니다 Microsoft Azure Sentinel . 인시던트 양식의 필드에 SIR $ $ 형식을 사용하여 대체 변수를 추가하거나 수정하여 코멘트 섹션에 표시되는 기본 텍스트를 편집합니다.
인시던트 종결 업데이트	SIR 인시던트 종결 시 Azure Sentinel 인시던트 종결	자동화된 인시던트 상태 업데이트 기능을 사용할 수 있는 옵션입니다. Microsoft Azure Sentinel 인시던트가 에서 종결된 후 SIR 제공된 설명과 함께 인시던트에서 종결 Microsoft AzureServiceNow AI Platform됩니다.
	종결 인시던트 상태 업데이트	에서 SIR인시던트가 종결될 때 인시던트의 Microsoft Azure Sentinel 상태 업데이트 .
	종결 설명 인시던트에 다시 게시됨	에서 SIR인시던트가 종결될 때 인시던트의 Microsoft Azure Sentinel 인시던트에 게시되는 코멘트입니다. 인시던트 양식의 필드에 SIR $ $ 형식을 사용하여 대체 변수를 추가하거나 수정하여 코멘트 섹션에 표시되는 기본 텍스트를 편집합니다.
	인시던트 분류 및 종결 사유	환경에서 인시던트를 종료하는 데 사용되는 인시던트 분류 및 종결 사유 Microsoft Azure Sentinel 방법입니다. 기본 인시던트 분류 및 종결 사유 방법을 선택하여 환경에서 인시던트 Microsoft Azure Sentinel 를 종결합니다. 이 방법을 선택하는 경우 기본 인시던트 분류 및 종결 사유를 정의해야 합니다. SIR에서 인시던트를 종결하면 Azure Sentinel의 인시던트

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

범주	필드	설명
		상태도 지정된 기본 인시던트 분류 및 종결 이유와 함께 종결됩니다. 인시던트를 종결하고 분류 사유 SIR 를 종결 코드와 매핑하려면 인시던트 분류 및 종결 사유-**SIR** 종결 코드 매핑 방법을 선택합니다. 여러 종 SIR 결 코드를 단일 분류 이유에 매핑할 수 있습니다. 종결 코드를 사용하여 인시던트 SIR 를 종결하면 Azure Sentinel의 인시던트 상태도 매핑된 인시던트 분류 및 종결 이유와 함께 종결됩니다. 분류 이유와 SIR 종결 코드가 매핑되지 않았거나 일치하는 항목을 찾을 수 없으면 환경에서 기본 분류 이유를 "미확인"으로 사용하여 인시던트가 Microsoft Azure Sentinel 종결됩니다.
Azure Sentinel 인시던트 설명 및 SIR 작업 메모 동기화	Azure Sentinel 인시던트 설명으로 SIR 작업 메모 업데이트	작업 메모의 SIR 설명을 업데이트 Microsoft Azure Sentinel 하기 위해 선택할 수 있는 옵션입니다. 작업 메모의 SIR 코멘트는 프리픽스 `Sentinel# ###`와 함께 나타납니다. 코멘트에는 Sentinel ID, 분석가 상세 정보 및 타임 스탬프도 포함되어 있습니다.
	SIR 작업 메모로 Azure Sentinel 인시던트 설명 업데이트	인시던트 설명에서 작업 메모를 업데이트 SIR 하기 위해 선택할 수 있는 Microsoft Azure Sentinel 옵션입니다. 의 주석은 Microsoft Azure Sentinel`ServiceNow# ##` 프리픽스와 함께 나타납니다.

다음 예는 인시던트 업데이트를 자동화하는 데 사용할 수 있는 구성 옵션을 보여줍니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



2. 마침을 클릭합니다.

다음에 수행할 작업

프로파일이 대기 중 상태로 전환됩니다. 설정 및 구성이 완료되었다는 확인 메시지가 표시되면 프로파일을 활성화할 수 있습니다.

Microsoft Azure Sentinel 프로파일 복사

프로파일을 생성하는 대신 기존 프로파일 및 관련 설정을 복사합니다. 여러 프로필을 만들 때 이러한 프로필을 복사하여 기존 프로필의 설정을 다시 사용할 수 있습니다.

시작하기 전에

필요한 역할: sn_si.ingestion_profile_admin

> **주:**
> sn_si.admin 역할은 기본적으로 필수 권한을 상속하므로 sn_si.admin 역할을 가진 사용자는 프로필 관리자가 사용할 수 있는 모든 작업을 수행할 수 있습니다.

이 태스크 정보

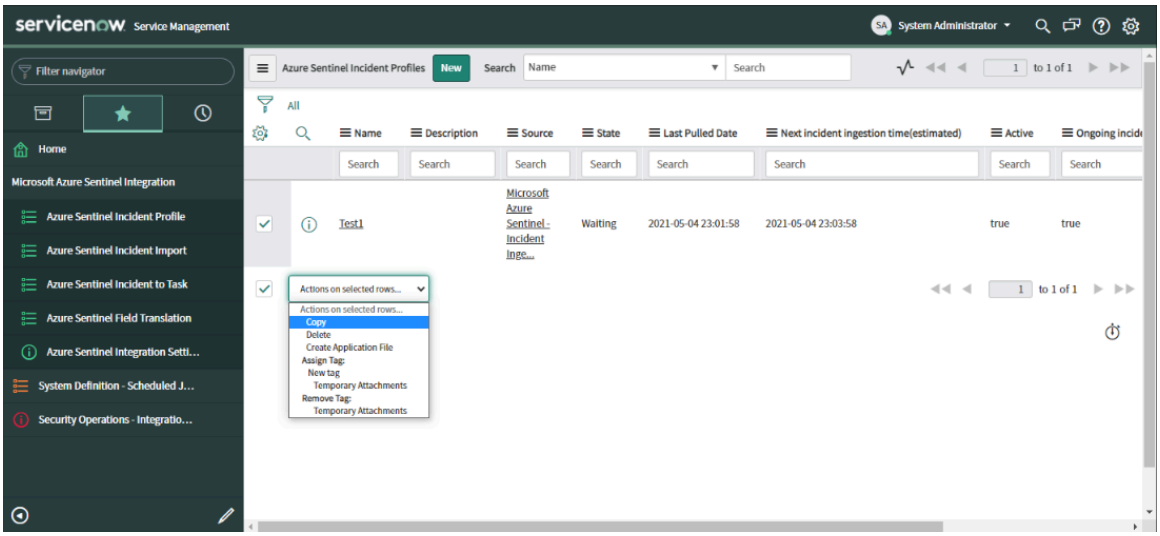
프로파일을 복사하면 중복된 프로파일이 작성되지 않도록 프로파일 이름이 처음에 수정됩니다. 복사된 프로파일도 꺼져 (false로 설정) 구성을 완료하기 전에 실수로 활성화하지 않도록 합니다. 이미 미리 보고 확인한 보안 인시던트에 대해 프로파일을 복사하고 기존 맵을 사용할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

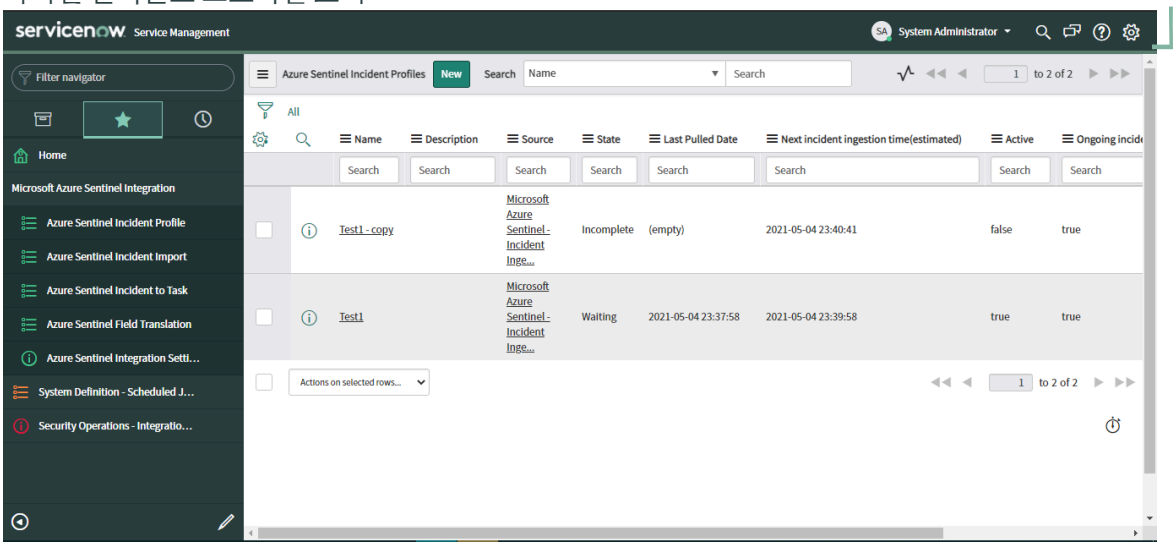
1. 다음으로 이동 모두 〉 **Microsoft Azure Sentinel** 통합 〉 **Azure Sentinel** 프로파일.
2. Azure Sentinel 프로필 목록에서 복사할 프로필을 선택한 다음 선택한 행의 작업 목록에서 다음 예제와 같이 복사 를 클릭합니다.

프로파일 복사



다음 예와 같이 프로파일이 복사되어 목록에 표시됩니다. 복사본에는 매핑 및 일정 구성을 포함하여 원래 프로필의 모든 설정이 포함됩니다. 프로필 이름에 "사본"이라는 단어가 포함되어 있습니다. 원본 프로파일이 활성화되더라도(true) 이 시점에서 복사본이 꺼집니다(false). 복사된 프로파일의 값을 편집하고 필요에 따라 구성 설정이 새 프로파일에 적용되도록 이름을 바꿀 수 있습니다.

복사된 인시던트 프로파일 보기



기존 프로파일에서 새 프로파일로 설정을 복사했습니다. 활성 열 상태가 false로 설정되어 프로파일을 활성화해야 합니다.

SIR 인시던트 수집 후 양식

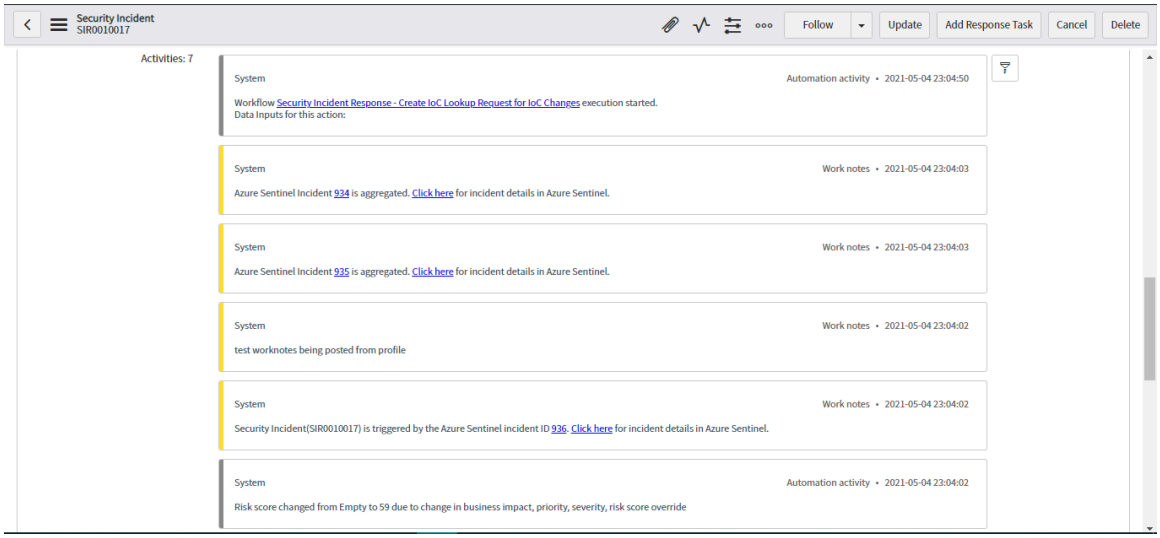
ServiceNow AI Platform 인시던트를 Microsoft Azure Sentinel 수집하면 보안 인시던트가 생성되고 해당 보안 인시던트 기록이 업데이트됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업 메모

작업 메모는 인시던트가 집계될 때와 인시던트 집계 기준에서 새 인시던트에 대한 작업 메모 기록 옵션을 구성한 경우에 게시됩니다. 다음 예는 의 SIR작업 메모를 보여줍니다.

에서 작업 메모 보기 **SIR**



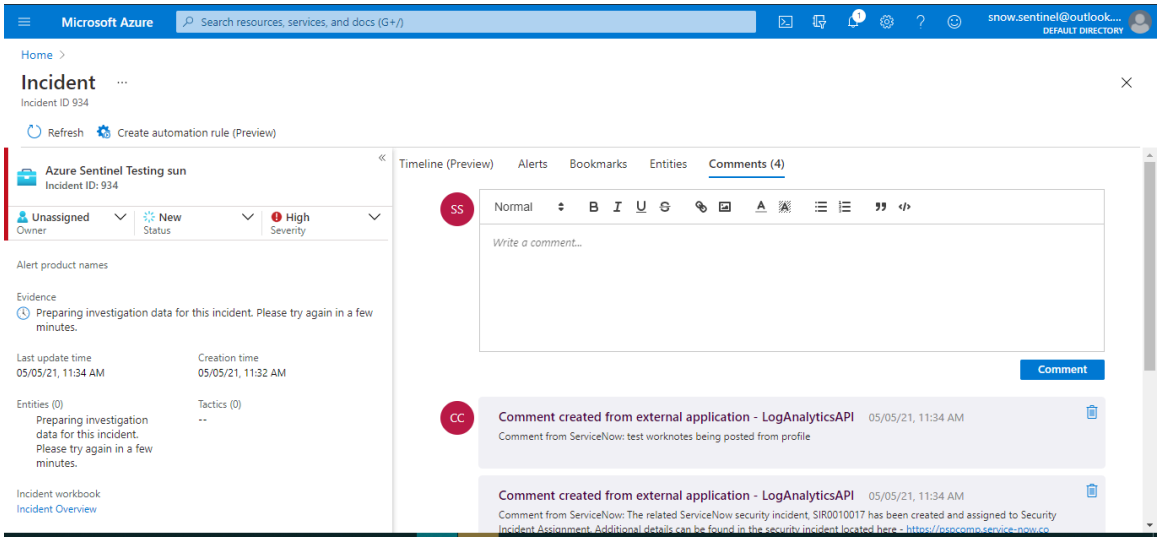
인시던트 번호를 클릭하면 원시 인시던트 데이터가 포함된 내부 인시던트 임포트 기록을 볼 수 있습니다. 다음 예제에서는 의 SIR원시 인시던트 데이터를 보여 줍니다.

에서 인시던트 원시 데이터 보기 **SIR**

여기를 클릭 링크를 클릭하면 환경에서 기록을 Microsoft Azure Sentinel 볼 수 있습니다. 다음 예는 환경의 기록을 Microsoft Azure Sentinel 보여줍니다.

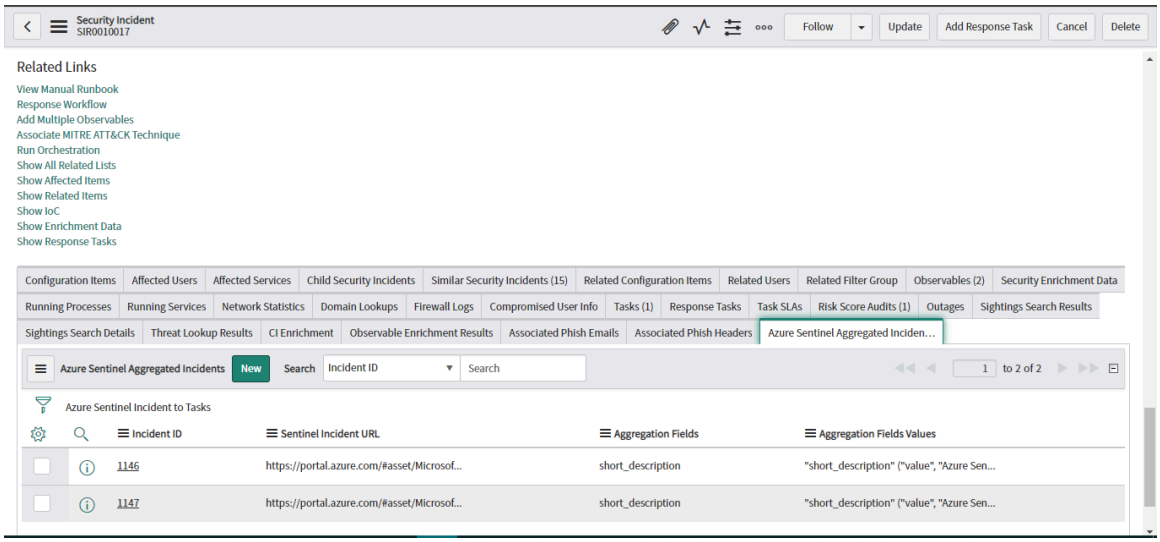
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Azure Sentinel에서 인시던트 기록 보기



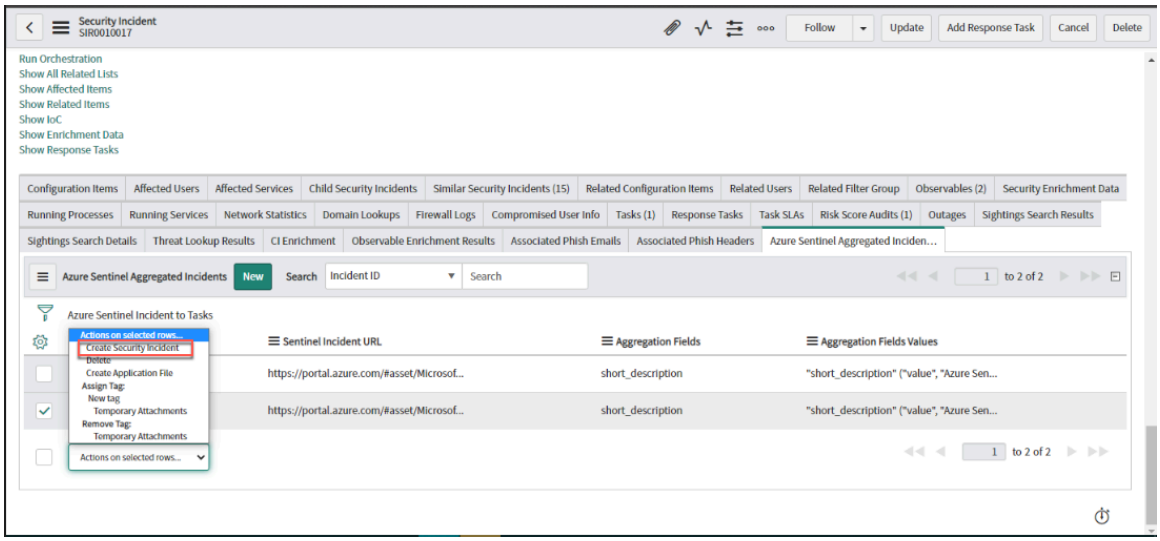
집계된 **Sentinel** 인시던트

집계된 Sentinel 인시던트 보기: 보안 인시던트로 집계된 인시던트를 봅니다. 다음으로 이동 모든 관련 목록 표시 〉 집계된 **Microsoft Azure Sentinel** 인시던트.



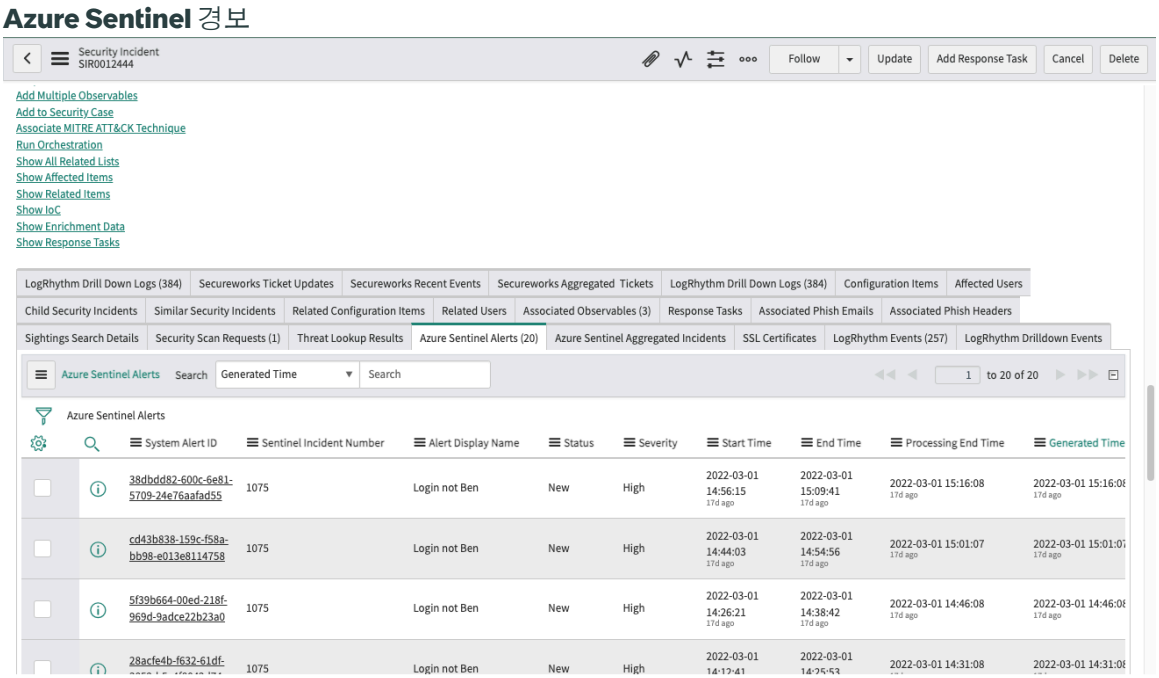
보안 인시던트 생성: 목록에서 인시던트를 선택하고 작업 메뉴를 클릭한 다음 보안 인시던트 만들기를 클릭합니다. 이 옵션은 인시던트에 대한 새 보안 인시던트를 생성하고 이 인시던트는 상위 보안 인시던트에서 집계 해제됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



Azure Sentinel 경보

보안 인시던트를 트리거한 Sentinel 인시던트와 관련된 경보를 보려면 다음으로 이동하십시오. 모든 관련 목록 표시 〉 **Azure Sentinel** 경보.



Microsoft Azure Sentinel 통합 설정 검토

Microsoft Azure Sentinel 환경에 맞게 시스템 속성을 수정할 수 있도록 통합 설정을 검토합니다.

시작하기 전에
필요한 역할: sn_si.ingestion_profile_admin

주:
sn_si.admin 역할은 기본적으로 필수 권한을 상속하므로 sn_si.admin 역할을 가진 사용자는 프로필 관리자가 사용할 수 있는 모든 작업을 수행할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 **Microsoft Azure Sentinel** 통합 〉 **Azure Sentinel** 통합 설정.
2. 필요에 따라 다음 설정을 수정합니다.

Microsoft Azure Sentinel 통합 설정

속성 이름	설명
샘플 데이터를 가져올 수 있는 일 수를 제한하십시오. 샘플_데이터에 대한 sn_sec_sentinel.max_num_of_days	환경에서 샘플 데이터를 Microsoft Azure Sentinel 가져올 수 있는 최대 일 수입니다. 유형: 정수 기본값: 7
SIR에 연결된 새 경보와 관련된 업데이트를 수신합니다. sn_sec_sentinel.incident_updates	인시던트 업데이트를 받는 옵션을 활성화합니다. 유형: 부울 기본값: True
필드 매핑에서 Microsoft Azure Sentinel 값을 분할하는 구분 기호 문자입니다. sn_sec_sentinel.delimiter	필드 매핑에서 Microsoft Azure Sentinel 값을 분할하는 구분 기호 문자입니다. 유형: 문자열 기본값: ', '(공백 포함한 쉼표)
가져올 수 있는 샘플 인시던트 수를 제한하십시오. sn_sec_sentinel.max_num_of_sample_incident_per_call	수집을 위해 환경에서 가져오는 Microsoft Azure Sentinel 샘플 인시던트의 최대 수입니다. 유형: 정수 기본값: 5 샘플 최대값: 20
단일 인시던트로 집계할 수 있는 Sentinel 인시던트의 수를 제한하십시오. sn_sec_sentinel.max_aggregations_per_si	보안 인시던트에 대한 인시던트 집계 제한입니다. 예를 들어 인시던트가 102개 있는 경우 처음 100개는 보안 incident_1로 집계되고 나머지 2개는 보안 incident_2로 집계됩니다. 유형: 정수 기본값: 100
24시간 동안 만들 수 있는 보안 인시던트 수를 제한하십시오. sn_sec_sentinel.max_si_per_day	에서 ServiceNow AI Platform24시간 동안 생성할 수 있는 최대 보안 인시던트 수입니다. 유형: 정수 기본값: 1000

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성 이름	설명
하나의 REST 호출로 인시던트 데이터를 가져오기 위한 최대 페이지 매김 제한입니다. sn_sec_sentinel.max_page_size	환경에서 하나의 REST 호출로 인시던트 데이터를 가져오기 위한 페이지 매김 제한입니다 Microsoft Azure Sentinel . 유형: 정수 기본값: 100
인시던트의 API 버전 값입니다. sn_sec_sentinel.sentinel_security_incident_api_version	Sentinel 인시던트를 검색하기 위한 Microsoft API 버전입니다. 기본값: 2021-10-01
경보에 대한 API 버전 값입니다. sn_sec_sentinel.sentinel_security_alert_api_version	Sentinel 경보 검색을 위한 Microsoft API 버전입니다. 기본값: 2021-10-01
엔터티에 대한 API 버전 값입니다. sn_sec_sentinel.sentinel_security_entities_api_version	Sentinel 엔터티를 검색하기 위한 Microsoft API 버전입니다. 기본값: 2021-10-01
sn_sec_sentinel.logging.verbosity	애플리케이션의 로그 세부 정보 표시 수준으로, 정보 유형의 이름을 의미합니다. 값을 다음 옵션으로 업데이트할 수도 있습니다. ○ 오류 ○ 경고 ○ 정보 ○ **debug** 기본값: 정보.

3. 저장을 클릭합니다.
   수정된 통합 설정은 프로파일에 정의된 대로 다음 폴링 간격에 적용됩니다.

도메인 분리

이 애플리케이션에는 도메인 분리가 지원됩니다. 도메인 분리를 사용하여 데이터, 프로세스 및 관리 작업을 도메인이라는 논리적 그룹으로 분할할 수 있습니다. 어떤 사용자가 데이터를 보고 액세스할 수 있는지를 포함하여 이러한 분리의 여러 측면을 제어할 수 있습니다.

지원 수준: 기본

- 비즈니스 논리: 데이터가 애플리케이션의 서비스 제공자 사용 사례에 적합한 도메인으로 들어가도록 보장합니다.
- 애플리케이션은 런타임에서 도메인 분리를 지원합니다. 도메인 분리에는 사용자 인터페이스, 캐시 키, 보고서, 롤업, 집계 등에서의 분리가 포함됩니다.
- 인스턴스 소유자는 여러 테넌트에서 작동하도록 애플리케이션을 설정해야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

샘플 사용 사례: 서비스 제공자(SP)가 채팅을 사용하여 테넌트 고객의 메시지에 응답할 때 고객이 SP의 응답을 볼 수 있어야 합니다.

지원 수준에 대한 자세한 내용은 도메인 분리를 위한 애플리케이션 지원 을 참조하십시오.

통합에서 도메인 분리가 **Microsoft Azure Sentinel** 작동하는 방식

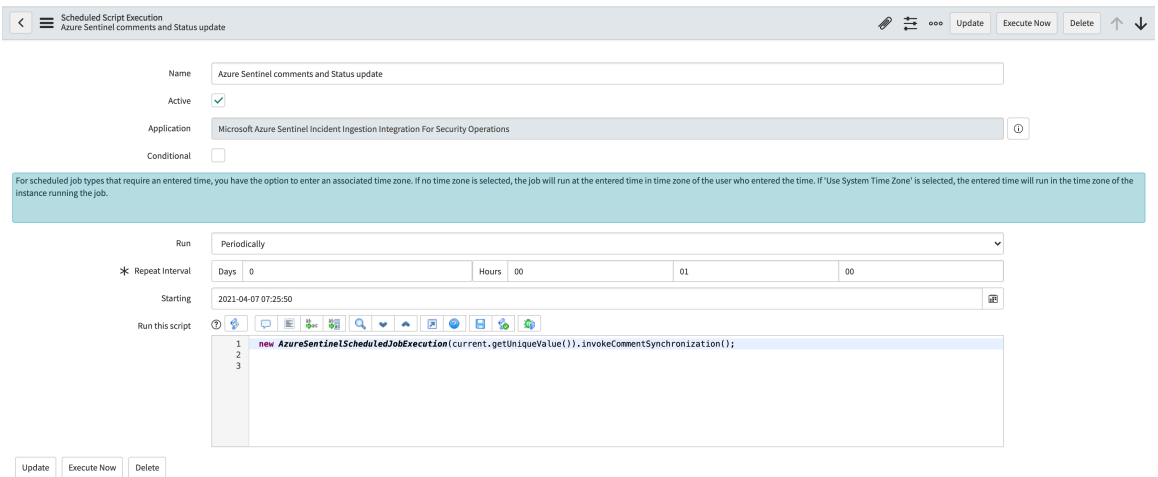
도메인 분리를 수행하려면 다음 단계를 따르십시오.

- 해당 도메인에서 sn_si.admin 역할을 가진 사용자를 생성합니다.

  주:
  프로필을 만들 때 도메인 선택기를 사용하여 도메인을 선택합니다. 상위 도메인에서 사용자를 만든 후 나중에 프로필의 도메인을 변경하지 마십시오. 프로파일의 각 도메인마다 sn_si.admin 역할을 가진 사용자가 있어야 합니다. 이 사용자를 사용하여 프로파일에서 설정을 만들거나 수정합니다.

- 기존 예약된 작업을 사용하지 않도록 설정합니다.
- 모든 도메인에 대해 다음 예약된 작업을 복제합니다.
  - 경보 및 엔터티를 가져오는 Azure Sentinel
  - Azure Sentinel 의견 동기화
  - Azure Sentinel 상태 업데이트
  - Azure Sentinel 프로파일 프로세스
  - Azure Sentinel 프로세스 원시 데이터
  - Azure Sentinel 데이터 정리
  - Azure Sentinel 이력 주석 끌어오기
- 시스템 사용자에서 해당 도메인의 sn_si.admin 역할을 가진 사용자로 다른 이름으로 실행을 변경한 다음 예약된 작업을 실행합니다.

다음 예제에서는 Azure Sentinel 주석 및 상태 업데이트 작업을 복제하고 시스템 사용자로 작업을 실행하는 방법을 보여 줍니다.



관련 정보

서비스 제공자용 도메인 분리

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

와의 비교 **Microsoft Azure Sentinel** 및 **Microsoft Graph** 보안 **API** 통합 **SIR**

AND Microsoft Graph 보안 API 통합의 차이점을 Microsoft Azure Sentinel 보고 인스턴스와의 올바른 통합을 선택할 수 있습니다ServiceNow AI Platform.

Microsoft Azure Sentinel - Incident Ingestion 개요

Microsoft Azure Sentinel 는 클라우드 기반 SIEM(보안 정보 이벤트 관리) 및 SOAR(보안 오케스트레이션 자동화 응답) 솔루션입니다. Microsoft Azure Sentinel 전사적으로 지능형 보안 분석 및 위협 인텔리전스를 제공합니다. 경보 탐지, 위협 가시성, 사전 예방적 헌팅 및 위협 대응을 위한 단일 솔루션을 제공합니다.

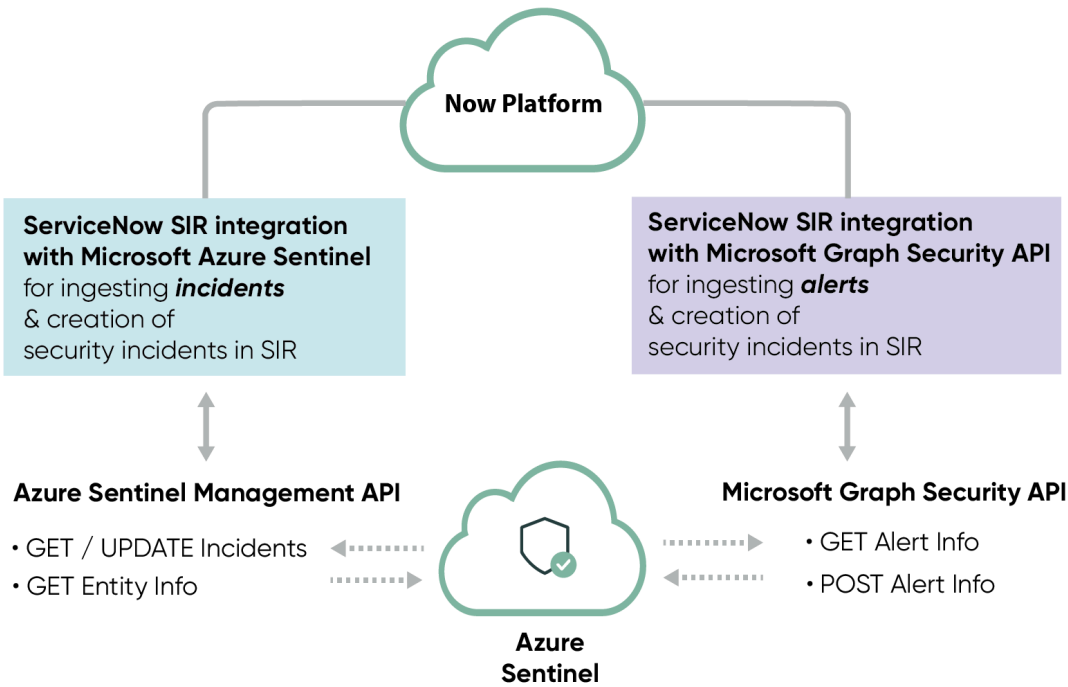
Microsoft Graph 보안 **API** 개요

이 Microsoft Graph 보안 API 서비스는 여러 보안 공급자(Microsoft 및 ServiceNow 파트너의 기본)를 연결하기 위한 단일 프로그래밍 인터페이스를 제공하는 중간 서비스(또는 브로커)입니다.

통합은 Microsoft Graph 보안 API Azure Microsoft Graph 보안 API Sentinel, Microsoft Defender Advanced Threat Protection 및 Azure Advanced Threat Protection과 같은 다양한 Microsoft 보안 기술과 연결하여 이러한 문제를 해결합니다. Microsoft 보안 제공자의 경보가 수집되고 에 보안 인시던트가 자동으로 생성됩니다.보안 인시던트 응답

기능 차이점 요약

Azure Sentinel and Graph Security API (Microsoft architecture)



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Microsoft Azure Sentinel 대 **Microsoft Graph** 보안 **API**

Microsoft Azure Sentinel	Microsoft Graph 보안 API
엔터티 정보(사용 가능한 경우)와 함께 인시던트를 수집하고 Microsoft Azure Sentinel 에서 SIR보안 인시던트 생성을 자동화합니다.	표준 스키마에서 여러 보안 공급자(Azure Sentinel 포함)의 경보를 수집하고 에서 SIR보안 인시던트 생성을 자동화합니다.
Microsoft Azure Sentinel 보안 인시던트를 만들고 종결할 수 있도록 보안 인시던트 응답에 대한 인시던트 상태 업데이트를 자동화합니다. 주: ServiceNow 보안 인시던트 생성 또는 종결에 따라 인시던트의 상태를 Microsoft Azure Sentinel 업데이트합니다.	선택한 보안 제공자에 대한 경보 업데이트(경보 상태 변경 및 경보 종결)를 지원합니다. 주: 지원되는 보안 공급자에 대한 Microsoft Graph 보안 API 자세한 내용은 Microsoft 설명서를 참조하십시오.
시나리오에 다음 조건이 포함된 경우 이 통합을 사용합니다. • 예비 인시던트 조사가 진행 Microsoft Azure Sentinel 중이며 후속 조사가 진행 중입니다. SIR • 인시던트 수집 Microsoft Azure Sentinel 대상 SIR	시나리오에 다음 조건이 포함된 경우 이 통합을 사용합니다. • 에서 SIR인시던트 조사를 수행합니다. • 에서 SIR경보를 수집합니다Microsoft Azure Sentinel. • 에서는 Microsoft Azure Sentinel인시던트가 생성되지 않습니다.
경보는 의 Microsoft Azure Sentinel엔터티입니다. Management API를 사용하여 독립 실행형 또는 특정 경보를 Microsoft Azure Sentinel 검색할 수 없습니다. 인시던트와 관련된 경보 데이터만 검색할 수 있습니다. 이 통합을 사용하여 사용할 수 있는 경보 데이터는 를 Microsoft Graph 보안 API사용하여 사용할 수 있는 경보 데이터보다 풍부합니다.	Microsoft Azure Sentinel 정규화된 경보 데이터를 사용할 수 있습니다. Microsoft Azure Sentinel 에서 내부적으로 Microsoft Graph 보안 API매핑되고 에서 사용할 수 Microsoft Graph 보안 API있는 경보 필드를 이 통합에서 사용할 수 있습니다.
	이 통합을 사용하여 경보를 Microsoft Azure Sentinel 업데이트할 수 없습니다.

Microsoft Defender for Endpoint 통합

이를 Microsoft Defender for Endpoint 통해 모든 엔드포인트에서 알려진 위협과 알려지지 않은 위협을 사전 예방적으로 검사, 분석 및 억제할 수 있습니다.

통합을 Microsoft Defender for Endpoint 통해 보안 분석가는 도구 사이를 이동할 필요 없이 보안 인시던트를 효율적으로 조사하고 정정할 수 있습니다.

이 통합을 사용하여 호스트 상세 정보, 로그인한 사용자의 상세 정보, 관련 컴퓨터 상세 정보 및 기타 보강 역량을 검색하는 구성을 만들 수 있습니다. 네트워크에 액세스하지 못하도록 시스템을 격리하거나 시스템을 격리에서 제거하도록 요청할 수 있습니다. 승인자는 요청을 수락하거나 거부할 수 있습니다.

스토어에서 앱 요청

ServiceNow Store 웹 사이트를 방문하면 사용 가능한 모든 앱을 확인하고 스토어에 요청을 제출하는 방법에 대한 정보를 참조할 수 있습니다. 출시된 모든 앱의 누적 릴리스 정보는 ServiceNow Store 버전 기록 릴리스 정보 를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주요 기능

Microsoft Defender for Endpoint 다음과 같은 주요 기능이 있습니다.

- 엔터프라이즈 보안 검색을 통해 엔드포인트 전반의 잠재적인 악성 옵저버블을 확인하고 정정 작업을 수행합니다.
- 호스트 격리, 격리 제거, 앱 실행 제한, 안티바이러스 검사 실행, 앱 제한 제거, 파일 중지 및 격리 등의 대응 작업을 수행합니다.
- 표시기를 만들거나 업데이트합니다.
- 옵저버블 보강을 수행하고 표시기와 관련된 데이터를 검색합니다.

Microsoft Defender for Endpoint

탐색 엔드포인트용 Microsoft Defender 시작	설치 애플리케이션을 설치하고 통합을 위한 소스 구성	구성 엔드포인트용 Microsoft Defender에 대한 프로파일 및 보안 인시던트 구성
역량 프로파일 엔드포인트용 Microsoft Defender 통합을 위한 역량 프로파일을 생성합니다.	추가 구성 엔드포인트용 Microsoft Defender 수행할 수 있는 추가 구성	기타 엔드포인트용 Microsoft Defender를 사용하여 사이팅 검색 및 표시기에 대한 프로필을 만들고 구성합니다.

포털에서 등록 **Microsoft Defender for EndpointMicrosoft Azure** 및 구성

Microsoft Defender for Endpoint Microsoft Azure 포털에 애플리케이션을 등록하고 애플리케이션에 대한 읽기 및 쓰기 권한을 부여합니다.

시작하기 전에

필요한 역할: 애플리케이션 개발자, 테넌트 관리자.

프로시저

1. Microsoft Azure 포털에 로그인합니다.
2. 검색 상자에 App registrations# 입력하고 **New** registration을 클릭합니다.
3. 애플리케이션의 이름과 리디렉션 URI를 입력하고 등록을 클릭합니다.
   예제 이름은 ###### Microsoft Defender입니다. 리디렉션 URI는 애플리케이션에 대한 관리자 동의를 제공하는 동안 사용됩니다.
4. 앱 등록 페이지에서 3단계에서 등록한 애플리케이션을 선택합니다.
5. 관리에서 인증서 및 비밀을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

6. 클라이언트 암호를 만들려면 새 클라이언트 암호를 선택합니다.
7. 클라이언트 비밀을 복사하여 저장합니다.

   클라이언트 비밀을 잊어버린 경우 새 클라이언트 비밀을 생성할 수 있습니다.

8. 다음으로 이동 관리 〉 **API** 권한.
9. 권한 추가를 클릭합니다.
10. API 권한 요청 창에서 조직에서 사용하는 **API** 탭을 클릭합니다.
11. **WindowsDefenderATP**를 검색하여 선택합니다.
12. WindowsDefenderATP 권한에서 애플리케이션 권한을 선택합니다.
    이 권한을 사용하도록 설정하면 애플리케이션이 로그인한 사용자 없이 백그라운드 서비스 또는 디먼으로 실행됩니다.
13. 다음 애플리케이션 수준 권한을 추가하고 새로 추가된 API 권한에 대한 관리자 동의를 부여합니다.

권한	권한 표시 이름
Machine.Read.All	모든 컴퓨터 프로파일 읽기
User.Read.All	사용자 프로파일 읽기
Machine.Isolate	격리 기계
Machine.RestrictExecution	코드 실행 제한
머신.스캔	스캔 머신
Machine.StopAndQuarantine	중지 및 격리
URL을 입력합니다. 읽기.모두	URL 읽기
파일.모두 읽기.	파일 프로파일 읽기
IP.읽기.모두	IP 주소 프로파일 읽기
Ti.ReadWrite.All	읽기 및 쓰기 표시기

통합 시작하기 **Microsoft Defender for Endpoint**

다음 섹션에는 ServiceNow Store에서 애플리케이션을 설치하기 Microsoft Defender for Endpoint 전에 인스턴스에서 완료해야 ServiceNow AI Platform# 하는 설정 작업이 나열되어 있습니다.

시작하기 전에
필요한 역할: 관리자

원활한 설치 및 구성을 위해 애플리케이션을 다운로드하고 설치하기 전에 다음 테이블을 참조하고 나열된 작업을 모두 완료했는지 확인하십시오.

설정 작업	설명
필수 ServiceNow AI Platform 역할과 보안 인시던트 응답(SIR) 역할을 할당했는지 확인합니다.	다음과 같은 역할이 필요합니다. 1. 통합을 위해 애플리케이션을 설치하려면 시스템 관리자(관리자) 역할이 있어야 합니다. 2. 통합을 구성하고 프로파일을 생성, 활성화 및 제거하려면 보안 인시던트 관리자 (sn_si.admin) 역할이 있어야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설정 작업	설명
	3. 보안 인시던트를 작업하려면 보안 인시던트 분석가(sn_si.analyst) 역할이 있어야 합니다. 이 역할을 가진 사용자는 통합에서 사용할 수 있는 모든 기능을 시작할 수 있습니다.
애플리케이션을 설치하기 전에 통합을 지원하는 데 필요한 ServiceNow Core 애플리케이션이 설치되고 활성화되었는지 확인합니다.	에서 ServiceNow Store다음 보안 운영 애플리케이션이 설치되고 활성화되는지 확인합니다. 이러한 애플리케이션이 아직 설치되어 있지 않은 경우 원활한 설치를 위해 다음 순서대로 각 애플리케이션을 한 번에 하나씩 설치하고 활성화해야 합니다. **1.** 보안 인시던트 응답 **2.** ServiceNow 통합 허브 런타임 (com.glide.hub.integration.runtime) **3.** ServiceNow IntegrationHub Action Step - REST (com.glide.hub.action_step.rest)
프로파일에 대한 승인 옵션을 활성화하기 전에 승인 그룹을 생성했는지 확인하십시오.	선택적 승인 워크플로우를 사용하여 호스트 시스템을 격리하고, 다시 네트워크로 복원하고, 엔드포인트에서 추가 작업을 실행할 수 있습니다. 조직에서 이러한 작업에 대한 추가 제어 수준을 원하는 경우 프로파일을 구성하는 동안 승인 필요 옵션을 활성화합니다. 프로파일을 사용할 수 있는 시나리오에서는 승인을 위한 프로파일 구성이 우선합니다. 프로파일을 사용할 수 없는 시나리오에서는 기본 설정에 따라 승인이 처리됩니다. 보안 관리자는 프로파일과 기본 설정을 구성하면서 승인을 설정할 수 있습니다. 인스턴스의 그룹 목록에서 승인 그룹을 사용할 수 있어야 합니다. sn_si.analyst 역할을 가진 사용자가 제출한 요청을 모니터링하고 처리하려면 승인 그룹의 각 구성원이 에서 ServiceNow AI Platform#내 승인으로 이동해야 합니다. 또는 승인자가 승인 모듈에서 통합을 위해 독점적으로 Microsoft Defender for Endpoint 제출된 요청을 찾을 수 있습니다. 사용자 그룹을 만드는 방법에 대한 자세한 내용은 사용자 그룹 만들기를 참조하세요.

다음에 수행할 작업

통합을 위한 Microsoft Defender for Endpoint 인스턴스를 성공적으로 설정 ServiceNow AI Platform# 했습니다. 다음 단계는 통합을 위해 ServiceNow Store에서 애플리케이션을 설치하는 Microsoft Defender for Endpoint 것입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

애플리케이션 설치 및 통합 구성 **Microsoft Defender for Endpoint**

인스턴스에서 통합을 ServiceNow StoreServiceNow AI Platform 설치하고 구성합니다Microsoft Defender for Endpoint. 구성을 사용하여 역량 프로파일 생성을 시작합니다.

시작하기 전에

필요한 역할: sn_si.admin

프로시저

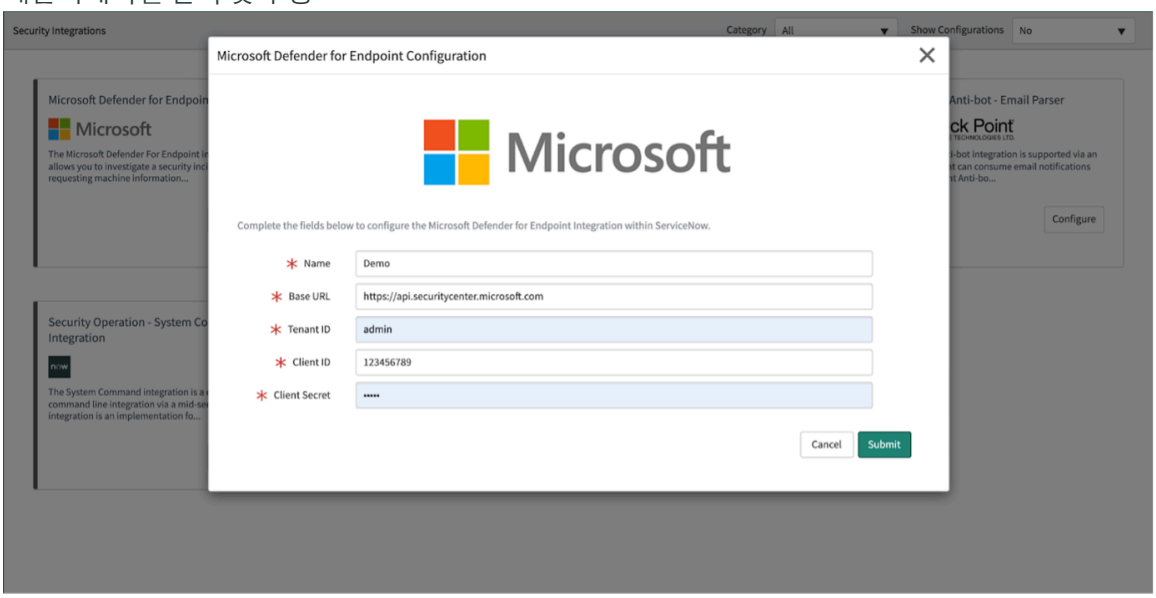
1. 에서 ServiceNow Store 엔드포인트용 Microsoft Defender 통합을 다운로드하고 설치합니다.
2. 다음으로 이동 보안 운영 〉 통합 〉 통합 구성.
3. 엔드포인트용 Microsoft Defender 타일을 검색하고 구성을 클릭합니다.
4. 양식의 다음 필드에 내용을 입력합니다.

엔드포인트용 **Microsoft Defender** 구성

이름	Microsoft Defender for Endpoint 인스턴스 구성의 이름입니다.
기본 URL	에 대한 서비스 기반 URL Microsoft Defender for Endpoint
테넌트 ID	테넌트 ID입니다 Microsoft Defender for Endpoint . 모든 작업이 이 인스턴스에서 수행됩니다.
클라이언트 ID	Microsoft Azure 포털에 등록한 애플리케이션의 클라이언트 ID입니다.
클라이언트 비밀	등록된 애플리케이션의 클라이언트 비밀입니다.

5. 제출을 클릭합니다.

애플리케이션 설치 및 구성



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

결과
Microsoft Defender for Endpoint 새 구성 기록과 함께 구성 목록이 표시됩니다. 에 Microsoft Defender for Endpoint대한 구성을 완료했습니다.

Microsoft Defender for Endpoint 기본 설정

설치를 완료한 후 수행해야 하는 추가 구성 설정이 있습니다.

설치가 완료되면 왼쪽 탐색 창의 애플리케이션에서 기본 설정 모듈을 Microsoft Defender for Endpoint 찾을 수 있습니다. 여기에는 다양한 Microsoft Defender for Endpoint 기능에 대한 기본 설정이 포함되어 있습니다.

필요한 역할: sn_si.admin, sn_si.analyst(읽기 전용).

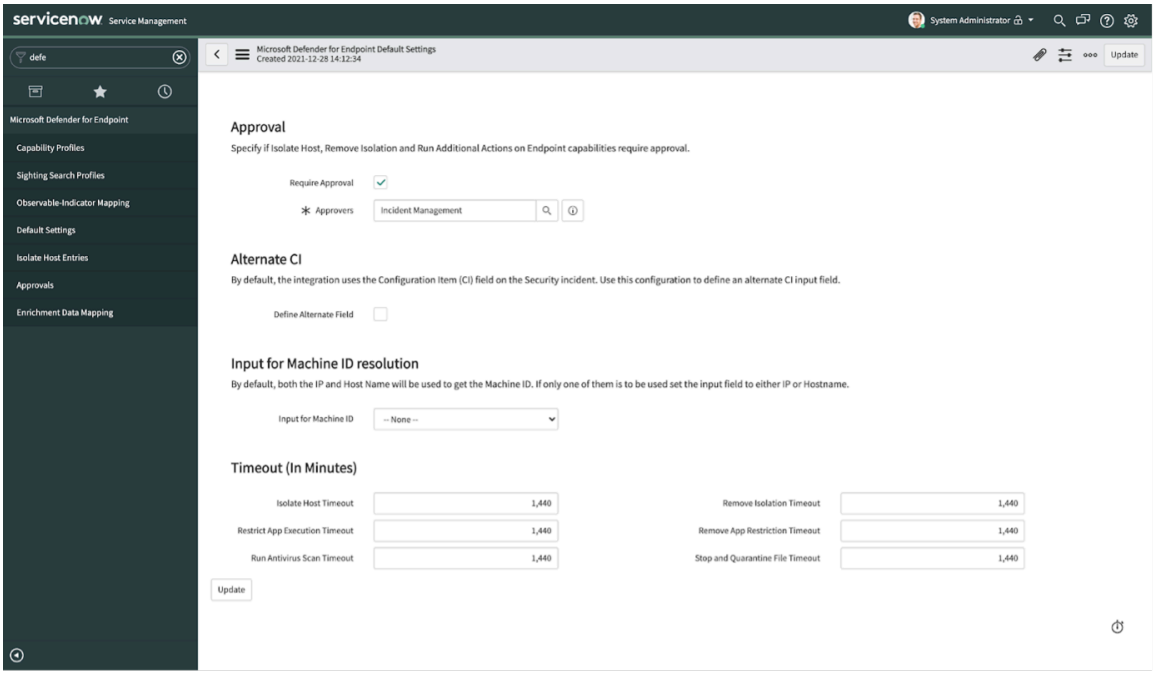
추가 구성

다음은 추가 구성 설정입니다.

- 승인: 이 승인은 특히 호스트 격리 작업, 호스트 격리 제거 작업 및 앱 실행 제한, 애플리케이션 제한 제거 및 바이러스 백신 검사 실행과 같은 추가 작업에 대한 것입니다. 관련 목록에서 직접 작업이 트리거되고 기존 프로파일이 없는 경우에만 이 승인을 사용할 수 있습니다. 이러한 기능에 대한 기존 프로파일이 있는 경우 프로파일의 승인 구성이 우선합니다.
  - 승인 필요: 승인 필요를 활성화하면 양식에서 승인자 필드를 사용할 수 있습니다.
  - 승인자: 승인자 그룹의 목록입니다. 요청을 제출한 후 요청을 완료하려면 그룹의 승인이 필요합니다.
- 대체 **CI:** 이 확인란을 활성화하면 대체 CI를 기능에 전달하는 데 사용할 수 있는 필드 목록이 제공됩니다. 기본적으로 통합은 보안 인시던트의 CI(구성 항목) 필드를 사용합니다. 이 구성은 엔드포인트에서 추가 작업 실행 기능에만 적용할 수 있습니다. 이 구성을 사용하여 엔드포인트에서 추가 작업 실행 기능에만 사용할 대체 CI 입력 필드를 정의합니다. 다른 기능을 사용하려면 프로파일 섹션의 구성을 사용합니다. 프로파일이 대체 CI를 정의하지 않는 경우 역량은 보안 인시던트 양식의 CI 필드를 사용합니다.
- 에이전트 **ID** 확인을 위한 입력: 기본적으로 IP 및 호스트 이름은 에이전트 ID를 가져오는 데 사용됩니다. 이 중 하나만 사용하려면 입력 필드를 IP 또는 호스트 이름으로 설정합니다.
- 시간 초과:
  - 호스트 격리 시간 제한(분): 호스트 격리 역량의 실행 임계치를 나타냅니다.
  - 격리 제거 시간 제한(분): 격리 시간 제한 제거 역량의 실행 임계치를 나타냅니다.
  - 앱 실행 제한 시간 제한(분): 앱 실행 제한 역량의 실행 임계치를 나타냅니다.
  - 앱 제한 제거 시간 제한(분): 앱 제한 제거 역량의 실행 임계치를 나타냅니다.
  - 바이러스 스캔 실행 시간 제한(분): 바이러스 스캔 실행 역량의 실행 임계치를 나타냅니다.
  - 파일 중지 및 격리 시간 제한(분): 파일 중지 및 격리 기능에 대한 실행 임계치를 나타냅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

기본값 설정



Microsoft Defender for Endpoint 표시기 유형 매핑

ServiceNow 옵저버블 유형을 표시기 유형과 매핑합니다 Microsoft Defender for Endpoint . 이 매핑은 Microsoft Defender 옵저버블 보강 및 표시기 만들기 작업에 사용됩니다.

시작하기 전에

필요한 역할: sn_si.admin 또는 sn_si.analyst(읽기 전용)

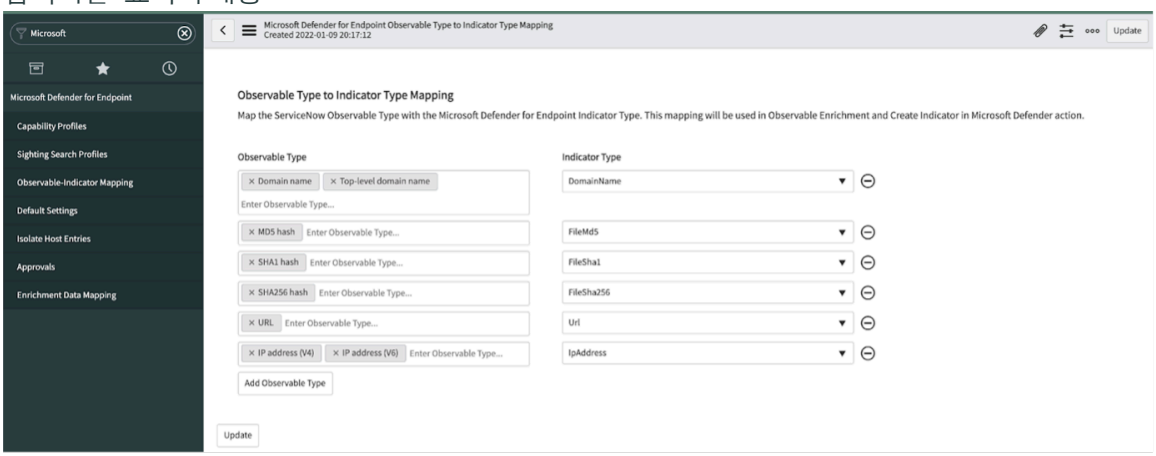
이 태스크 정보

옵저버블 유형이 표시기 유형에 매핑되지 않은 시나리오에서 이러한 옵저버블은 엔드포인트용 Microsoft Defender 옵저버블 보강 및 표시기 만들기에 적합하지 않습니다.

프로시저

1. 다음으로 이동 엔드포인트용 **Microsoft Defender** 〉 옵저버블-표시기 매핑.

옵저버블-표시기 매핑



2. 다음 방법 중 하나로 옵저버블 유형을 추가하거나 업데이트합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 새 매핑을 추가하려면 옵저버블 유형 추가를 클릭합니다.
- 옵저버블을 표시기 유형 매핑으로 업데이트하려면 기존 행을 클릭합니다.

3. 매핑을 저장하려면 업데이트를 클릭합니다.

통합에 **Microsoft Defender for Endpoint** 대한 역량 프로파일 생성

프로파일을 생성하고 프로파일을 실행할 기능을 선택합니다 Microsoft Defender for Endpoint .

시작하기 전에

필요한 역할: sn_si.admin

이 태스크 정보

프로파일은 역량을 클럽이나 그룹으로 묶기 위해 작성되므로 분석가가 조사 또는 정정을 쉽게 수행할 수 있습니다. 프로파일에 다음 기능을 추가할 수 있습니다.

- 호스트 상세 정보 가져오기
- 로그온한 사용자 가져오기
- 호스트 격리
- 격리 제거

프로파일을 만드는 동안에는 호스트 격리 및 호스트 격리 제거 기능을 다른 기능과 함께 묶을 수 없습니다. 이러한 기능에 대한 프로필은 개별적으로 만들어야 합니다. 반면에 호스트 세부 정보 가져오기 및 로그온한 사용자 가져오기 기능은 함께 사용할 수 있습니다. 프로필을 개별적으로 만들거나 요구 사항에 따라 전체 또는 일부를 묶을 수 있습니다.

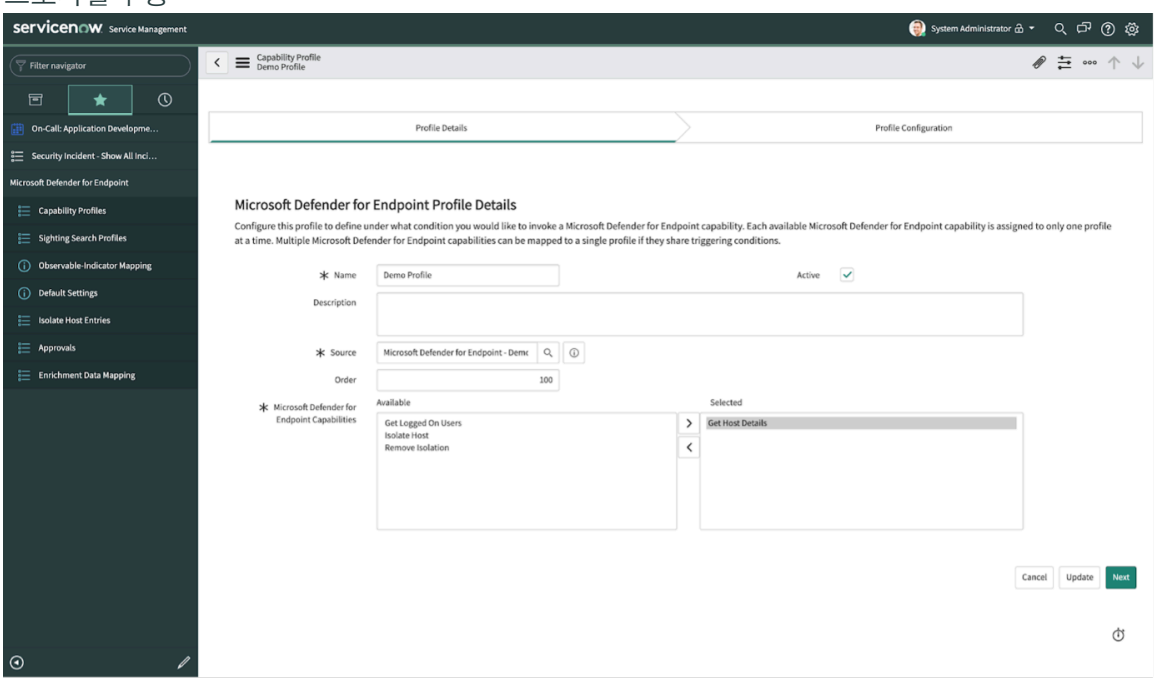
주:
프로파일에 역량이 포함되면 동일한 소스의 다른 프로파일에 포함될 수 없습니다.

프로시저

1. 다음으로 이동 엔드포인트용 **Microsoft Defender** 〉 역량 프로파일.

   엔드포인트용 Microsoft Defender 기능 프로필 목록이 표시됩니다.

프로파일 구성



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

2. 클릭 신규.
3. 양식에서 필드를 채웁니다.

역량 프로파일 양식

필드	설명
이름	역량 프로파일의 Microsoft Defender for Endpoint 이름입니다. 이 이름은 프로파일 유형을 식별하고 설명하는 데 도움이 됩니다.
설명	프로파일에 대한 추가 정보로, 프로파일에 대한 자세한 설명을 제공합니다.
소스	소스의 Microsoft Defender for Endpoint 이름입니다. 구성된 소스만 목록에서 사용할 수 있습니다.
엔드포인트용 Microsoft Defender 기능	프로파일의 Microsoft Defender for Endpoint 기능입니다. 사용 가능 열에서 이 프로파일에 대해 원하는 기능을 선택하고 선택됨 열로 이동합니다.
순서	플로우 우선순위입니다. 기본값은 100입니다. 이 필드의 값은 둘 이상의 프로파일이 트리거 조건을 공유할 때 플로우가 실행되는 순서를 나타냅니다. 숫자가 가장 낮은 플로우의 우선순위가 가장 높습니다. 작업 순서를 설정하려면 값을 입력합니다. 예를 들어 100, 200, 300, 400입니다.
활성	프로파일이 활성 상태임을 나타내는 옵션입니다. 프로파일이 활성화되면 구성에 지정한 필터링 조건과 일치하는 보안 인시던트가 생성되면 프로파일이 자동으로 트리거됩니다.

4. 프로파일 구성을 계속하려면 다음을 클릭합니다. 다음.

다음에 수행할 작업

다음 단계는 프로필을 구성하는 것입니다. 프로필에 대한 설정을 구성하기 전에 프로필 방법과 구성 및 트리거 조건을 검토하는 것이 좋습니다. 자세한 내용은 구성 항목의 트리거 조건 문서를 참조하십시오.

구성 항목의 트리거 조건

프로필을 만들고 프로필에서 실행할 기능을 선택한 Microsoft Defender for Endpoint 후 특정 조건 집합이 충족되는 경우에만 프로필이 실행되도록 프로필 설정을 구성합니다.

구성 항목에서 조건을 트리거하는 방법

트리거 조건과 일치하는 보안 인시던트가 생성될 때마다 프로파일이 자동으로 실행되도록 트리거 조건을 설정할 수 있습니다. 트리거 조건이 설정되지 않은 경우 보안 인시던트에서 EDR 프로파일 실행 양식을 클릭하고 프로파일을 선택하여 이러한 프로파일을 수동으로 실행할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

기본적으로 통합은 보안 인시던트의 CI(구성 항목) 필드를 사용합니다. 이 값은 자산 ID를 에 저장된 ServiceNow AI Platform 구성 관리 데이터베이스(CMDB)정보와 일치시키는 데 사용됩니다. 보안 인시던트가 생성되고 프로파일이 자동 또는 수동으로 CMDB 실행되면 CI 필드의 값을 기반으로 호스트 이름 또는 IP 주소를 검색하기 위해 검색됩니다. 호스트 이름 또는 IP는 에이전트 ID Microsoft Defender for Endpoint 를 확인하여 엔드포인트를 식별하는 데 사용됩니다.

이상적인 시나리오에서는 데이터베이스에서 일치하는 값을 찾고 일치하는 자산에 대한 데이터를 콘솔에서 수집합니다 Microsoft Defender for Endpoint . 다양한 역량에 대한 데이터를 인스턴스로 ServiceNow AI Platform 구성 관리 데이터베이스(CMDB) 가져와 보안 인시던트의 관련 목록에 표시합니다. 보안 인시던트의 CI(구성 항목) 필드가 데이터베이스와 일치하는 호스트 이름 또는 IP 주소로 채워지지 않은 경우 호스트 이름 또는 IP가 포함된 보안 인시던트의 대체 필드를 선택하여 에이전트 ID 확인을 수행할 수 있습니다.

프로파일 설정의 구성 단계에서 엔드포인트 식별을 위한 대체 CI 필드를 선택하여 에서 엔드포인트를 Microsoft Defender for Endpoint식별할 수 있습니다. 생성한 사용자 지정 필드를 포함하여 보안 인시던트의 모든 필드를 대체 CI 트리거 필드로 선택할 수 있습니다. 이 대체 CI 필드를 백업으로 선택하면 인시던트 생성 시 연관된 보안 인시던트에 CI 필드가 채워지지 않아도 프로파일이 실행됩니다.

주:
대체 CI 필드는 프로파일에 추가할 수 있는 기능에 대해서만 고려됩니다. 이러한 기능에는 호스트 상세 정보 가져오기, 로그온한 사용자 가져오기, 호스트 격리 및 격리 제거가 포함됩니다. 모든 추가 작업의 경우 기본 설정 모듈에서 대체 CI를 구성해야 합니다.

통합에 **Microsoft Defender for Endpoint** 대한 프로파일 및 보안 인시던트 구성

프로파일을 생성하고 프로파일을 실행할 기능을 선택합니다 Microsoft Defender for Endpoint . 정의된 조건에서만 프로파일을 트리거할 수 있도록 설정을 구성해야 합니다.

시작하기 전에
필요한 역할: sn_si.admin, sn_si.analyst(읽기 전용)

이 태스크 정보
지정한 조건이 충족되는 경우에만 실행되도록 프로파일을 구성합니다. 필요한 경우 CI(구성 항목) 필드에 대한 대체 입력 필드를 선택하고 트리거 조건을 충족하는 보안 인시던트가 생성될 때 프로파일이 자동으로 트리거될 수 있도록 필터링 조건을 설정할 수 있습니다.

주:
프로파일 상세 정보 페이지에 들어간 후에만 프로파일 구성 페이지로 이동할 수 있습니다.

프로시저

1. 다음으로 이동 엔드포인트용 **Microsoft Defender** 〉 역량 프로파일.
2. 프로파일 상세 정보 섹션을 완료한 후 다음.
   섹션을 검토하고 구성합니다.
3. 인시던트 기준 정의(자동화) 섹션에서 인시던트 기준 정의 옵션을 선택하여 프로파일의 역량을 자동으로 트리거 Microsoft Defender for Endpoint 합니다.
   인시던트 기준 정의(자동화): 프로필에 대한 엔드포인트용 Microsoft Defender 기능을 자동으로 트리거하는 보안 인시던트 조건을 정의합니다. 인시던트 기준 정의 옵션을 선택하지 않으면 보안 인시던트에서 프로파일과 기본 기능을 수동으로 호출할 수 있습니다.

   주:
   호스트 격리 및 호스트 제거 격리 기능은 자동으로 트리거할 수 없습니다.

   a. 필터 조건에서 필수 필드를 선택합니다.

   b. 새 기준을 추가하고 **OR** 또는 **AND** 조건도 정의합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 승인 섹션에서 승인 필요 확인란을 선택하여 추가 제어 수준을 제공합니다.

   이 옵션을 선택하면 호스트 컴퓨터를 격리하고, 네트워크로 복원하고, 파일을 가져오기 위해 엔드포인트용 Microsoft Defender 기능을 사용할 때 더 많은 제어 권한을 갖습니다.

   프로파일 구성의 승인 옵션은 각각 호스트 격리 및 호스트 격리 제거 기능에만 나타납니다.

5. 추가 구성 섹션에서 대체 필드 정의 옵션을 선택하여 대체 입력 필드를 정의합니다.
   추가 구성: 보안 인시던트의 CI(구성 항목) 필드가 호스트 이름 또는 데이터베이스와 일치하는 IP 주소로 채워지지 않은 경우 보안 인시던트에서 대체 필드를 선택하여 엔드포인트용 Microsoft Defender API를 쿼리할 수 있습니다.

   > **주:**
   > 자세한 내용은 구성 항목의 트리거 조건 문서를 참조하십시오.

   a. 대체 필드 정의 옵션을 선택합니다.

   b. 다음에서 입력 필드를 선택합니다. 대체 **CI** 트리거 필드.

6. 태그 섹션에서 태그 표시 확인란을 선택하여 보안 인시던트에 태그 지정을 활성화하고, 태그 사용 시 프로파일 이름 앞에 접두사가 붙습니다.

   프로파일 시작됨, 프로파일 완료 및 프로파일 실패 태그에 대한 태그를 사용하여 보안 인시던트에 선택적으로 태그를 지정할 수 있습니다. 기본적으로 이 옵션은 모든 프로파일에 대해 꺼져 있습니다.

7. 클릭 완료.

트리거 조건 필터 확인

프로파일의 유효성을 검사하고 구성한 트리거 조건 필터가 예상대로 작동하는지 확인합니다.

시작하기 전에
필요한 역할: sn_si.admin 또는 sn_si.analyst

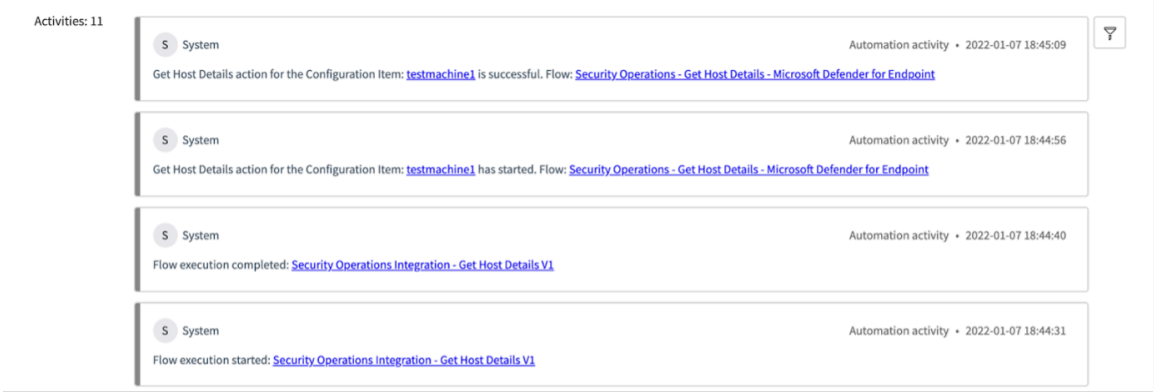
이 태스크 정보
프로파일을 활성화한 후에는 구성된 트리거 조건에 따라 보안 인시던트의 ServiceNow AI Platform# 쿼리 결과를 볼 수 있습니다.

프로시저

1. 다음으로 이동 보안 인시던트 〉 모든 인시던트 표시.
2. 새 보안 인시던트를 만들려면 다음을 선택합니다. 신규.
3. 해당 프로파일을 트리거하려면 역량 프로파일에 지정된 대로 필터 조건을 제공합니다.
4. 클릭 저장.
5. 작업 메모 및 활동 섹션을 확인하려면 시작된 프로파일, 프로파일 완료 또는 프로파일 실패 태그로 태그가 지정된 기록을 보고 확인합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업 메모 및 활동



6. 관련 목록의 모든 데이터를 확인하려면 모든 관련 목록 표시를 클릭합니다.
7. 상세 정보를 확인하려면 관련 목록 탭을 클릭합니다.
   예: 호스트 상세 정보.

다음에서 역량 트리거 **Microsoft Defender for Endpoint** 관련 링크

관련 링크에서 보안 인시던트를 검토한 후 역량 프로파일을 수동으로 트리거합니다.

시작하기 전에

필요한 역할: sn_si.admin 또는 sn_si.analyst

이 태스크 정보

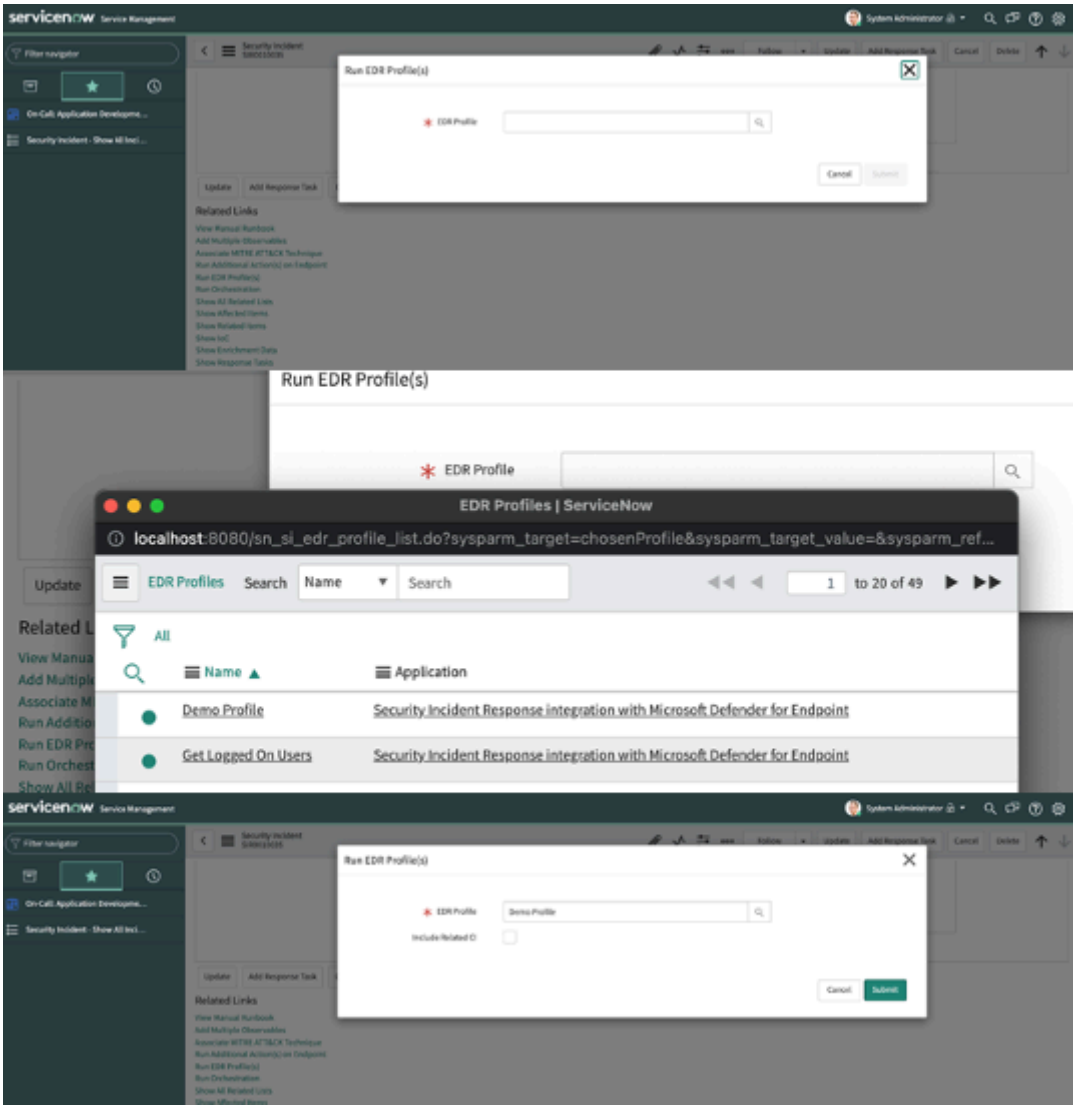
CI 또는 보안 인시던트의 대체 CI에 대한 프로파일을 실행하는 것 외에도 대화 상자에서 관련 **CI** 포함을 선택하여 구성 항목 관련 목록에 있는 CI 값에 대한 프로파일을 실행할 수도 있습니다. 이렇게 하면 관련 목록에 있는 CI 값에 대한 데이터도 검색됩니다. 또는 관련 목록에 있는 CI 값에 대해서만 프로파일을 실행할 수 있습니다.

프로시저

1. 다음으로 이동 보안 인시던트 〉 모든 인시던트 표시.
2. 정보로 검토하려는 보안 인시던트를 Microsoft Defender for Endpoint 선택합니다.
3. 관련 링크 섹션에서 **EDR** 프로파일 실행을 클릭합니다.
4. 사용 가능한 프로파일 목록에서 프로파일을 찾아 선택하고 제출을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로파일 선택



선택한 프로파일이 수동으로 트리거됩니다.

5. 작업 메모 및 활동 섹션을 확인합니다.
6. 태그를 보고 관련 목록에서 데이터를 확인합니다.

구성 항목 관련 목록에서 트리거 **Microsoft Defender for Endpoint**

구성 항목 관련 목록에서 역량 프로파일을 수동으로 트리거합니다.

시작하기 전에
필요한 역할: sn_si.admin 또는 sn_si.analyst

프로시저

1. 다음으로 이동 보안 인시던트 〉 모든 인시던트 표시.
2. 정보로 검토하려는 보안 인시던트를 Microsoft Defender for Endpoint 선택합니다.
3. 클릭 모든 관련 목록 표시.
4. 구성 항목 관련 목록을 클릭합니다.
5. 추가된 구성 항목을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

6. 선택한 행에 대한 작업에서 역량을 선택합니다.
   선택한 역량이 수동으로 트리거됩니다.
7. 작업 메모 및 활동 섹션을 확인합니다.
8. 태그를 보고 관련 목록에서 데이터를 확인합니다.

의 추가 구성 **Microsoft Defender for Endpoint**

통합은 Microsoft Defender for Endpoint 표준 작업 이외의 추가 작업 실행을 지원합니다.

다음과 Microsoft Defender for Endpoint 같은 추가 구성을 지원합니다.

에서 호스트 격리 기능 구성 **Microsoft Defender for Endpoint**

공격의 심각도에 따라 호스트가 네트워크에 Microsoft Defender for Endpoint 액세스하지 못하도록 격리합니다. 네트워크에서 호스트를 격리하면 다른 호스트에 대한 다른 악의적인 활동이나 잠재적 공격을 방지할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.admin 또는 sn_si.analyst

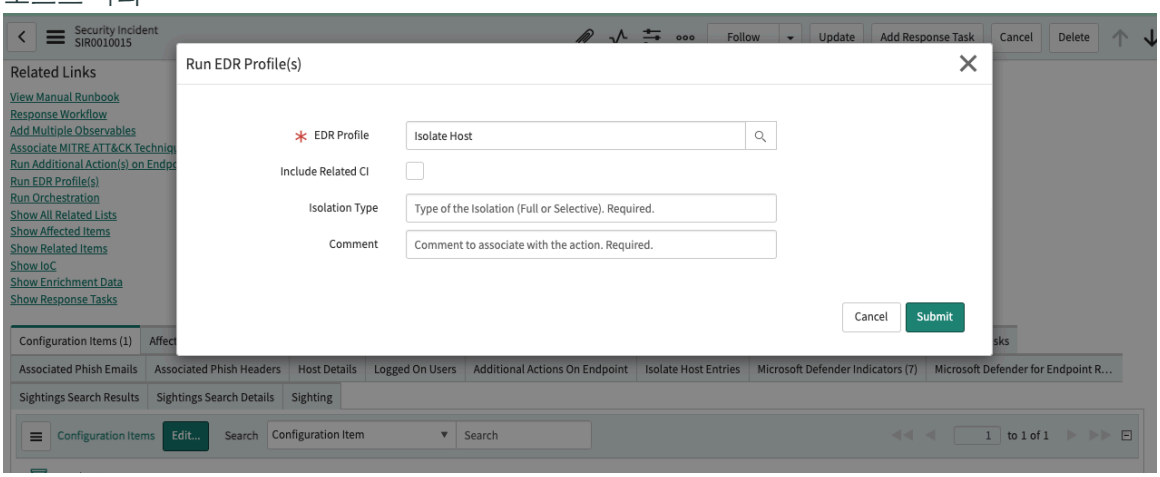
호스트 격리 역량에 대한 요구 사항

역량	필수	설명
호스트 격리	격리 유형	(필수) 격리 유형(전체 또는 선택)입니다.
	설명	(필수) 작업과 연결할 코멘트입니다.

프로시저

1. 다음으로 이동 보안 인시던트 〉 모든 인시던트 표시.
2. 엔드포인트용 Microsoft Defender 정보로 검토하려는 보안 인시던트를 선택합니다.
3. 관련 링크 섹션에서 **EDR** 프로파일 실행을 클릭합니다.
4. 사용 가능한 프로파일 목록에서 호스트 격리 기능을 선택한 프로파일을 찾아 선택하고 제출을 클릭합니다.

호스트 격리



또는 다음 단계를 수행할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 관련 목록 섹션에서 모든 관련 목록 표시를 클릭합니다.

b. 구성 항목 관련 목록을 클릭합니다.

c. 호스트 격리를 선택하고 해당 기능을 선택합니다.

5. 자동화 활동 및 활동 섹션을 확인하고 데이터가 예상과 같은지 확인합니다.

6. 데이터를 보고 관련 목록에서 호스트 분리 상세 정보를 확인합니다.

에서 호스트 격리 제거 기능 구성 **Microsoft Defender for Endpoint**

필요한 경우 에서 이전에 네트워크에서 Microsoft Defender for Endpoint격리된 호스트의 격리를 제거합니다. 다른 호스트에 대한 다른 악의적인 활동이나 잠재적 공격을 방지할 수 있습니다.

시작하기 전에

격리 역량 제거 요구 사항

역량	필수 입력	설명
격리 제거	설명	(필수) 작업과 연결할 코멘트입니다.

필요한 역할: sn_si.admin 또는 sn_si.analyst

프로시저

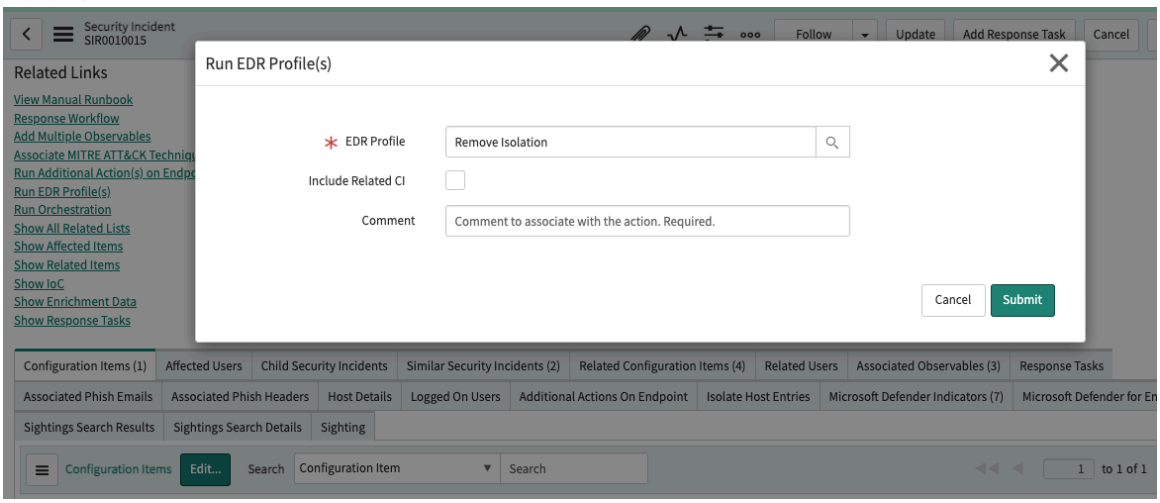
1. 다음으로 이동 보안 인시던트 〉 모든 인시던트 표시.

2. 엔드포인트용 Microsoft Defender 정보로 검토하려는 보안 인시던트를 선택합니다.

3. 관련 링크 섹션에서 **EDR** 프로파일 실행을 클릭합니다.

4. 사용 가능한 프로파일 목록에서 격리 제거 기능을 선택한 프로파일을 찾아 선택하고 제출을 클릭합니다.

격리 제거



또는 다음 단계를 수행할 수 있습니다.

a. 관련 목록 섹션에서 모든 관련 목록 표시를 클릭합니다.

b. 구성 항목 관련 목록을 클릭합니다.

c. **Remove** Isolation(격리 제거)을 선택하고 해당 기능을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. 자동화 활동 및 활동 섹션을 확인합니다.
6. 데이터를 보고 관련 목록에서 호스트 분리 상세 정보를 확인합니다.
7. 실행의 자동화 활동을 확인합니다.

에서 바이러스 스캔 실행 기능 구성 **Microsoft Defender for Endpoint**

원격으로 바이러스 백신 검사를 시작하여 손상된 장치에 있을 수 있는 맬웨어를 식별하고 해결할 수 있습니다. 조사 또는 응답 프로세스의 일부로 검사를 실행합니다.

시작하기 전에
필요한 역할: sn_si.admin 또는 sn_si.analyst

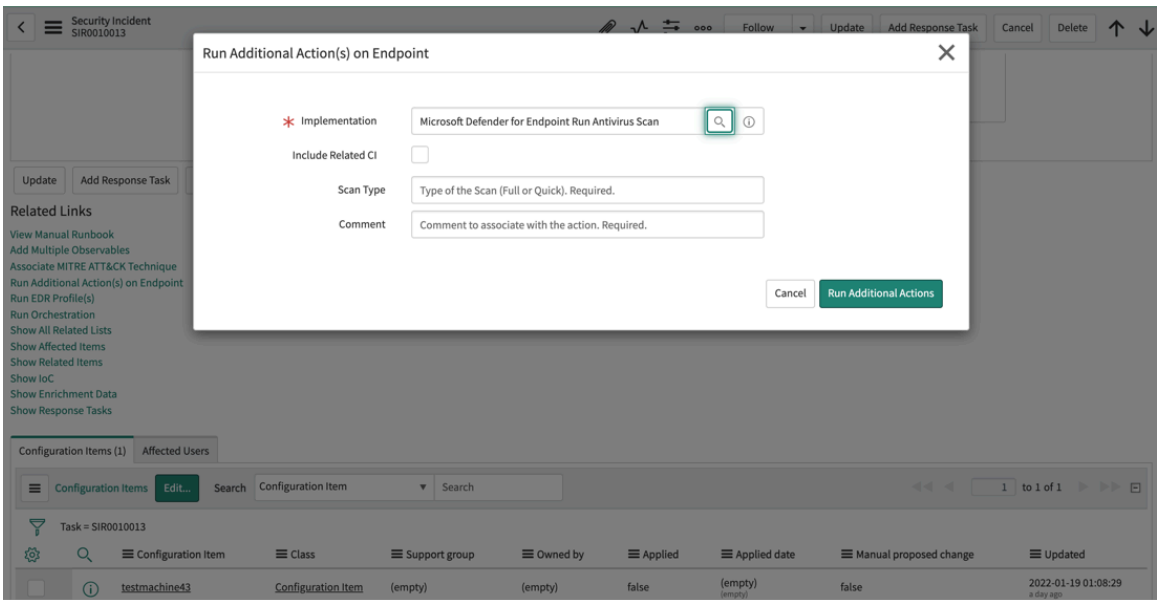
바이러스 백신 검사 역량 실행 요구 사항

입력	설명
스캔 유형	(필수) 검사 유형(전체 또는 빠름)입니다.
설명	(필수) 작업과 연결할 코멘트입니다.

프로시저

1. 다음으로 이동 보안 인시던트 〉 모든 인시던트 표시.
2. 엔드포인트용 Microsoft Defender 정보로 검토하려는 보안 인시던트를 선택합니다.
   a. 관련 링크 섹션에서 이 버튼을 클릭합니다. 엔드포인트에서 추가 작업 실행.
   b. 필요한 역량을 찾아 선택합니다.
   예를 들어 바이러스 백신 검색 기능 실행을 클릭합니다.

바이러스 백신 검사 실행



또는 다음 단계를 수행할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 관련 목록 섹션에서 모든 관련 목록 표시를 클릭합니다.

b. 구성 항목 관련 목록을 클릭합니다.

c. 추가된 구성 항목을 선택하고 선택한 행에 대한 작업에서 엔드포인트에서 추가 작업 실행을 선택합니다.

바이러스 스캔 실행 기능 구현을 선택하면 추가 스캔 유형 및 설명 입력 필드가 표시됩니다.

3. 실행할 스캔 유형 (빠른 또는 전체)을 선택하고 스캔을 실행하기 전에 설명을 추가합니다.

4. 바이러스 검사를 시작하려면 추가 작업 실행을 클릭합니다.

5. 실행의 자동화 활동을 보고 검증합니다.

6. 엔드포인트에 대한 추가 작업 관련 목록에서 작업의 상태를 확인합니다.

에서 앱 실행 제한 기능 구성 **Microsoft Defender for Endpoint**

공격을 억제하려면 장치를 제한하거나 잠그고 잠재적으로 악의적인 프로그램의 후속 시도가 실행되지 않도록 합니다.

시작하기 전에

앱 실행 역량 제한 요구 사항

입력	설명
설명	(필수) 작업과 연결할 코멘트)

필요한 역할: sn_si.admin 또는 sn_si.analyst

프로시저

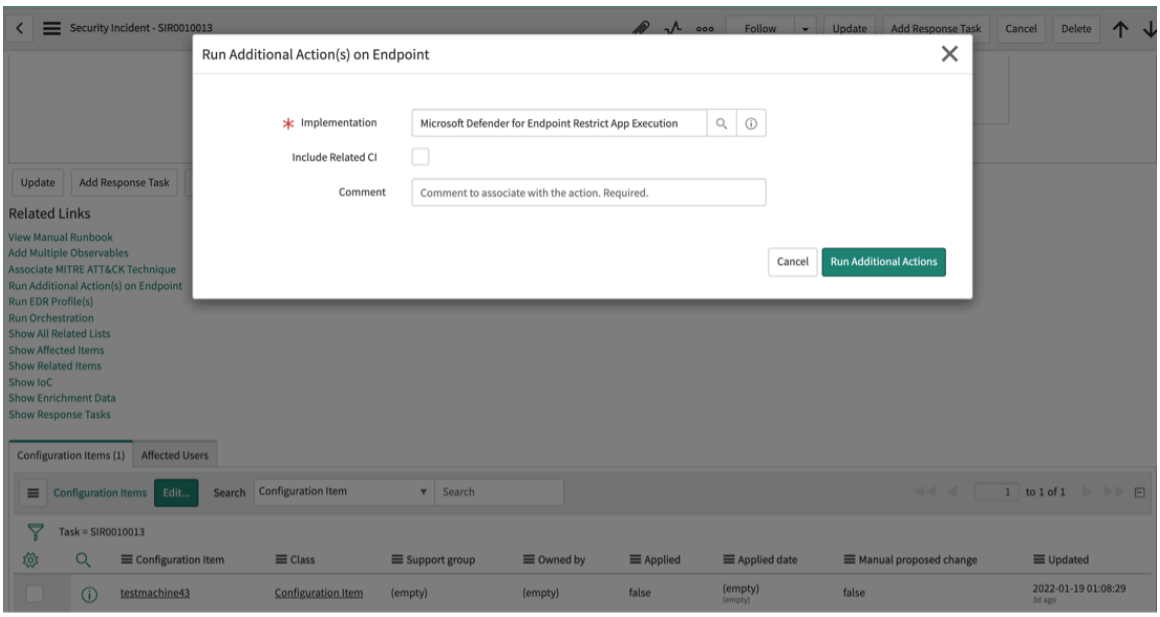
1. 다음으로 이동 보안 인시던트 〉 모든 인시던트 표시.

2. 엔드포인트용 Microsoft Defender 정보로 검토하려는 보안 인시던트를 선택합니다.

a. 관련 링크 섹션에서 이 버튼을 클릭합니다. 엔드포인트에서 추가 작업 실행.

b. 앱 실행 제한 역량을 찾아 선택합니다.

앱 실행 제한



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

또는 다음 단계를 수행할 수 있습니다.

a. 관련 목록 섹션에서 모든 관련 목록 표시를 클릭합니다.

b. 구성 항목 관련 목록을 클릭합니다.

c. 추가된 구성 항목을 선택합니다.

d. 선택한 행에 대한 작업에서 엔드포인트에서 추가 작업 실행을 선택합니다.

3. 컴퓨터에서 앱 실행 제한을 사용하도록 설정하려면 추가 작업 실행을 클릭합니다.

4. 실행의 자동화 활동을 보고 검증합니다.

5. 엔드포인트에 대한 추가 작업 관련 목록에서 작업의 상태를 확인합니다.

에서 앱 제한 제거 기능 구성 **Microsoft Defender for Endpoint**

필요한 경우 장치에서 애플리케이션의 제한을 제거합니다.

시작하기 전에

필요한 역할: sn_si.admin 또는 sn_si.analyst

앱 제한 제거 역량 요구 사항

입력	설명
설명	(필수) 작업과 연결할 코멘트)

프로시저

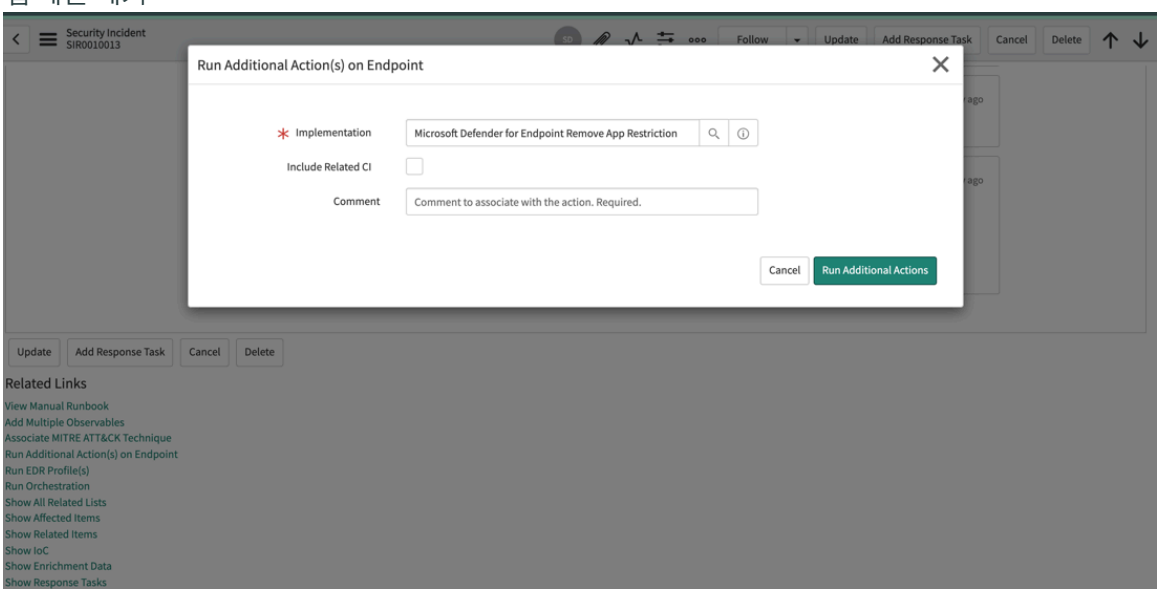
1. 다음으로 이동 보안 인시던트 〉 모든 인시던트 표시.

2. 엔드포인트용 Microsoft Defender 정보로 검토하려는 보안 인시던트를 선택합니다.

a. 관련 링크 섹션에서 이 버튼을 클릭합니다. 엔드포인트에서 추가 작업 실행.

b. 앱 제한 제거 기능을 찾아 선택합니다.

앱 제한 제거



또는 다음 단계를 수행할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 관련 목록 섹션에서 모든 관련 목록 표시를 클릭합니다.

b. 구성 항목 관련 목록을 클릭합니다.

c. 추가된 구성 항목을 선택합니다.

d. 엔드포인트에서 추가 작업 실행을 선택합니다.
추가 의견 입력 필드가 표시됩니다.

3. 앱 제한을 제거하려면 추가 작업 실행을 클릭합니다.

4. 실행의 자동화 활동을 보고 검증합니다.

5. 엔드포인트에 대한 추가 작업 관련 목록에서 작업의 상태를 확인합니다.

의 **Defender** 역량에서 관련 머신 가져오기 구성 **Microsoft Defender for Endpoint**

특정 옵저버블의 관련 머신 목록을 가져옵니다.

시작하기 전에

주:
지원되는 옵저버블 유형은 도메인 이름, SHA1 해시 및 사용자 이름입니다.

필요한 역할: sn_si.admin 또는 sn_si.analyst

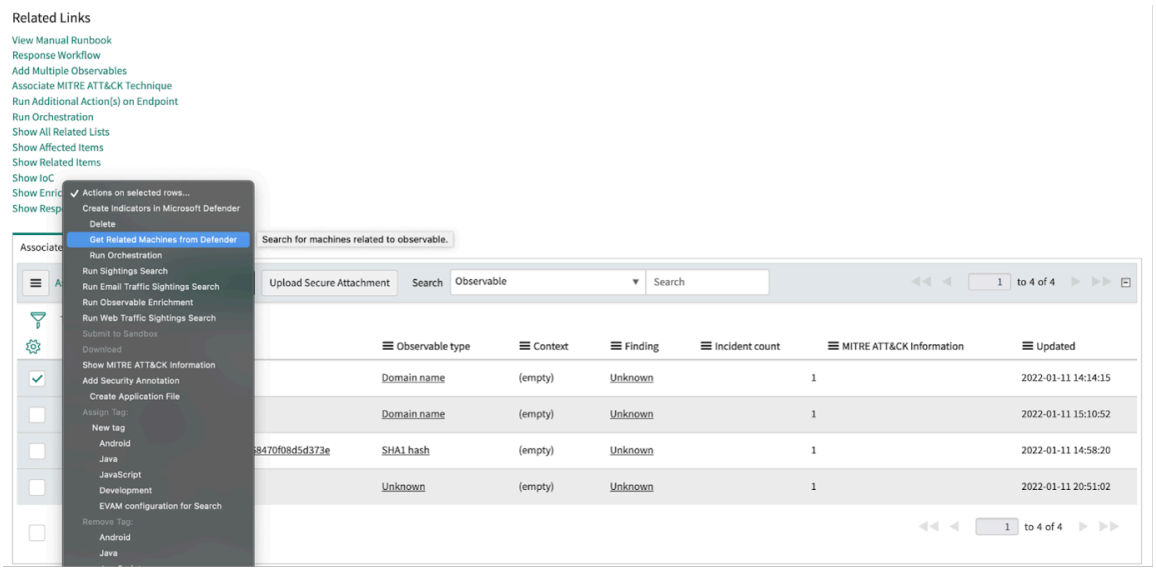
이 태스크 정보
특정 옵저버블에 액세스한 머신 목록을 검색할 수 있습니다. 엔드포인트용 Microsoft Defender 관련 머신 세부 정보 테이블에 목록을 저장할 수 있습니다. 연결된 옵저버블 관련 목록에서 Defender 역량에서 관련 머신 가져오기를 트리거할 수 있습니다.

프로시저

1. 다음으로 이동 보안 인시던트 〉 모든 인시던트 표시.

2. 엔드포인트용 Microsoft Defender 정보로 검토하려는 보안 인시던트를 선택합니다.

Defender에서 관련 머신 가져오기



3. 관련 링크 섹션에서 **IoC** 표시를 클릭합니다.

4. 연결된 옵저버블 관련 목록을 클릭합니다.

5. 연결된 옵저버블을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

6. 작업 목록에서 **Defender** 기능에서 관련 컴퓨터 가져오기 를 선택합니다.
7. 자동화 활동 및 활동 섹션을 확인합니다.
8. 데이터를 보고 관련 목록에서 엔드포인트용 Microsoft Defender 관련 머신 세부 정보의 유효성을 검사합니다.
9. 실행의 자동화 활동을 보고 검증합니다.

에서 파일 중지 및 격리 기능 구성 **Microsoft Defender for Endpoint**

Microsoft Defender 플랫폼에서 파일을 중지하고 격리합니다.

시작하기 전에
지원되는 옵저버블 유형: SHA1 해시.

중지 및 격리 파일 역량에 대한 요구 사항

입력	설명
설명	(필수) 작업과 연결할 코멘트)

필요한 역할: sn_si.admin 또는 sn_si.analyst

이 태스크 정보
파일 중지 및 격리 작업은 SHA1 유형의 특정 옵저버블에 대해서만 실행할 수 있습니다. 엔드포인트 테이블의 추가 작업에 대한 상세 정보를 저장합니다. 엔드포인트용 Microsoft Defender 관련 머신 세부 정보 관련 목록에서 파일 중지 및 격리 기능을 트리거할 수 있습니다.

프로시저
1. 다음으로 이동 보안 인시던트 〉 모든 인시던트 표시.
2. 엔드포인트용 Microsoft Defender 정보로 검토하려는 보안 인시던트를 선택합니다.
3. 관련 링크 섹션에서 모든 관련 목록 표시를 클릭합니다.
4. 엔드포인트용 Microsoft Defender 관련 머신 세부 정보 관련 목록을 클릭합니다.
5. 하나 이상의 기록을 선택합니다.
6. 선택한 행에 대한 작업에서파일 중지 및 격리 기능을 선택합니다.
7. 자동화 활동 및 활동 섹션을 확인합니다.
8. 데이터를 보고 관련 목록에서 데이터를 확인합니다.
9. 실행의 자동화 활동을 보고 검증합니다.

통합을 통해 **Microsoft Defender for Endpoint** 사이팅 검색을 위한 프로파일 생성 및 구성

를 Microsoft Defender for Endpoint사용하여 사이팅 검색 프로파일을 자동으로 생성하고 구성합니다.

시작하기 전에
필요한 역할: sn_si.admin, sn_si.admin

이 태스크 정보
사이팅 검색 워크플로우를 사용하여 사이팅 검색을 수행할 수 있습니다. 이 워크플로우는 옵저버블 목록을 수락하고, 구현 역량을 찾고, 사이팅 검색 구성을 기반으로 쿼리를 만들고, 구성된 워크플로우를 기반으로 검색을 실행합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

자동 Microsoft Defender for Endpoint 사이팅 검색을 구성할 수 있는 기본 시스템 사이팅 검색 프로파일을 제공합니다. 이 프로파일을 사용하면 조직의 관련 옵저버블 사이팅 정보에 액세스할 수 있으며 다른 조직의 사이팅도 볼 수 있습니다.

프로시저

1. 다음으로 이동 통합 〉 사이팅 검색 구성.
2. 새로 만들기를 클릭합니다.
3. 양식의 다음 필드에 내용을 입력합니다.

사이팅 검색 구성 양식

필드	설명
이름	사이팅 검색 프로파일의 이름입니다.
저장된 검색 여부	검색 구성을 저장하는 옵션입니다. 저장된 검색 구성 쿼리는 예제 쿼리입니다. 환경에 대한 매개변수로 대체하고 필요에 따라 저장된 추가 검색 구성을 생성할 수 있습니다.
관찰 검색 소스	통합에서 사이팅 검색을 위해 구성된 소스입니다 Microsoft Defender for Endpoint .
검색	쿼리를 구성하는 네이티브 검색 문자열입니다.
활성	저장된 검색 구성을 활성화하는 옵션입니다. 활성 검색 구성만 사이팅 검색을 수행할 수 있습니다.
옵저버블 유형	옵저버블 범주의 유형입니다. 예를 들어 IP 주소, 해시 값, URL 및 도메인 이름이 있습니다.
검색당 최대 옵저버블	검색 쿼리에서 볼 수 있는 최대 옵저버블 수입니다. 이 통합에 대해 이 값을 1로 설정합니다.
사이팅 검색 매개변수	지정된 로그 저장소에서 지원하는 논리 및 기타 연산자를 포함하는 보다 복잡한 쿼리를 정의하는 매개변수입니다.

4. 제출을 클릭합니다.

에서 수동 사이팅 검색 수행 **Microsoft Defender for Endpoint**

개별 또는 여러 옵저버블을 선택하고 수동 사이팅 검색을 Microsoft Defender for Endpoint 수행하여 시간 경과에 따른 위협의 확산을 확인합니다.

시작하기 전에

필요한 역할: sn_si.admin, sn_si.analyst

이 태스크 정보

지원되는 옵저버블 유형은 다음과 같습니다.

- 도메인 이름
- IP 주소(V4)
- IP 주소(V6)
- MD5 해시

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- SHA1 해시
- SHA256 해시

프로시저

1. 보안 인시던트로 이동합니다.
2. 기존 SIR을 열거나 새 SIR을 생성합니다.
3. 관련 링크에서 **IoC** 표시를 클릭합니다.
4. 연결된 옵저버블 관련 목록을 클릭합니다.
5. 옵저버블을 선택합니다.
6. 작업 목록에서 옵저버블 보강 실행을 클릭합니다.
7. 선택한 행에 대한 작업에서 옵저버블을 선택하고 사이팅 검색 실행을 클릭합니다.

   주:
   사이팅 검색은 도메인 이름, IP 주소(V4), IP 주소(V6), MD5 해시, SHA1 해시 및 SHA256 해시 옵저버블 유형에 대해 각각 지원됩니다.

8. 검색할 시간 범위를 지정하고 검색을 클릭합니다.

   주:
   엔드포인트용 Microsoft Defender 지난 30일 동안만 사이팅 검색을 지원합니다. 범위 쿼리가 지난 30일보다 이전인 경우 사이팅 검색은 데이터를 검색하지 않습니다. 범위 쿼리가 지난 30일과 겹치는 경우 지난 30일의 사이팅만 검색되고 범위 쿼리가 지난 30일 내에 있는 경우 정의된 시작 시간부터 현재 시간까지의 사이팅이 검색됩니다.

9. 검색이 완료되면 관련 목록에서 결과와 상세 정보를 확인합니다.
10. 사이팅 검색 상세 정보를 보려면 사이팅 검색 상세 정보를 클릭합니다.
11. 사이 팅 탭에서 상세 정보를 확인하고 사이 팅 검색 결과 탭을 클릭하여 검색 결과를 확인합니다.

    요약 필드에서 특정 사이팅과 관련된 추가 정보를 볼 수 있습니다.

에서 자동 옵저버블 보강 수행 **Microsoft Defender for Endpoint**

에서 Microsoft Defender for Endpoint 자동 옵저버블 보강을 수행하여 다양한 소스의 추가 정보로 옵저버블을 보강합니다.

시작하기 전에
보안 인시던트 응답 시스템 속성을 활성화했는지 확인합니다. 이 옵션은 옵저버블이 보안 인시던트에 연결될 때마다 SIR에서 옵저버블 보강 역량을 트리거합니다.

필요한 역할: sn_si.admin, sn_si.analyst

이 태스크 정보
인시던트 응답 조사 중에 이 기능을 사용하여 식별된 위협을 억제할 수 있습니다. 새 옵저버블이 보안 인시던트와 연결되면 엔드포인트용 Microsoft Defender 기능에서 옵저버블 보강이 자동으로 실행되도록 설정할 수 있습니다.

프로시저

1. 다음으로 이동 보안 인시던트 〉 모든 인시던트 표시.
2. 엔드포인트용 Microsoft Defender 정보로 검토하려는 보안 인시던트를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 새 옵저버블이 보안 인시던트와 연결되면 자동화 활동을 확인합니다.
4. 보안 인시던트의 표시기 관련 목록에서 결과를 보강한 결과를 봅니다.
   다음 표를 사용하여 옵저버블 보강에 대한 자세한 내용을 확인할 수 있습니다.

Microsoft Defender 표시기

필드	설명
표시기 ID	표시기 엔터티의 ID입니다. 열기를 클릭하여 인스턴스의 기록을 자세히 봅니다.ServiceNow AI Platform
옵저버블	결과와 연결된 옵저버블입니다.
직위	표시기의 제목입니다.
표시기 유형	표시기의 유형입니다.
작업	표시기에서 수행한 작업입니다.
권장 작업	표시기에 대한 권장 작업입니다.
통합 벤더	데이터가 검색되는 Defender 소스 통합입니다.
만료 날짜	표시기의 만료 시간입니다.
검색 날짜	보강 기록이 생성된 날짜입니다.

에서 수동 옵저버블 보강 수행 **Microsoft Defender for Endpoint**

개별 또는 여러 옵저버블을 선택하고 수동 옵저버블 보강을 수행하여 의 Microsoft Defender for Endpoint추가 정보로 옵저버블을 보강합니다.

시작하기 전에

필요한 역할: sn_si.analyst

이 태스크 정보

통합을 Microsoft Defender for Endpoint 통해 옵저버블-표시기 매핑 모듈에 매핑된 모든 옵저버블 유형에 대해 옵저버블을 보강할 수 있습니다.

프로시저

1. 다음으로 이동 보안 인시던트 〉 모든 인시던트 표시.
2. 엔드포인트용 Microsoft Defender 정보로 검토하려는 보안 인시던트를 선택합니다.
3. 모든 관련 목록 표시를 클릭합니다.
4. 연결된 옵저버블 탭을 클릭합니다.
5. 옵저버블을 선택합니다.
6. 작업 목록에서 옵저버블 보강 실행을 클릭합니다.
7. 엔드포인트용 Microsoft Defender 소스를 선택하고 선택됨 열로 이동하여 선택한 옵저버블을 보강하는 데 사용할 구현을 지정합니다.
8. 제출을 클릭합니다.
9. 실행 상태를 확인하려면 작업 메모를 확인하십시오.
10. 결과를 보려면 **Microsoft Defender** 표시기 탭을 클릭합니다.
    다음 표를 사용하여 옵저버블 보강에 대한 자세한 내용을 확인할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Microsoft Defender 표시기

필드	설명
표시기 ID	표시기 엔터티의 ID입니다. 열기를 클릭하여 인스턴스의 기록을 자세히 봅니다.ServiceNow AI Platform
옵저버블	결과와 연결된 옵저버블입니다.
직위	표시기의 제목입니다.
표시기 유형	표시기의 유형입니다.
작업	표시기에서 수행한 작업입니다.
권장 작업	표시기에 대한 권장 작업입니다.
통합 벤더	데이터가 검색되는 Defender 소스 통합입니다.
만료 날짜	표시기의 만료 시간입니다.
검색 날짜	보강 기록이 생성된 날짜입니다.

Microsoft Defender for Endpoint에서 표시기 만들기

를 Microsoft Defender for Endpoint사용하여 보안 인시던트의 연결된 옵저버블에서 표시기를 생성합니다.

시작하기 전에
필요한 역할: sn_si.admin, sn_si.analyst

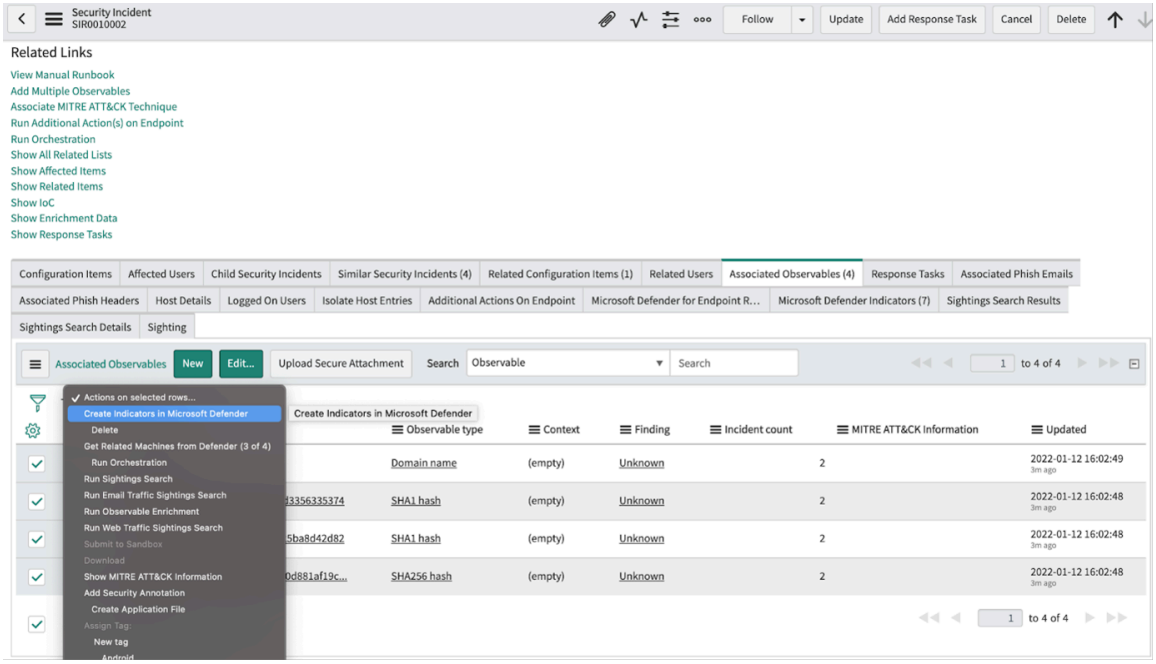
이 태스크 정보
통합을 Microsoft Defender for Endpoint 통해 옵저버블-표시기 매핑 모듈에 매핑된 모든 옵저버블 유형에 대해 옵저버블을 보강할 수 있습니다.

표시기 만들기는 탐지 및 차단 예방 및 대응을 위한 표시기 목록을 설정하는 기능을 제공합니다. 보안 인시던트의 연결된 옵저버블에서 표시기를 생성할 수 있습니다.

프로시저

1. 다음으로 이동 보안 인시던트 〉 모든 인시던트 표시.
2. 엔드포인트용 Microsoft Defender에서 표시기를 만들려는 옵저버블이 포함된 보안 인시던트를 선택합니다.
3. 연결된 옵저버블 관련 목록을 클릭합니다.
4. 기존 옵저버블을 추가하거나 새 옵저버블을 생성합니다.
5. 옵저버블을 선택합니다.
6. 선택한 행에 대한 작업에서**Microsoft** Defender에서 표시기 만들기를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



7. 양식에서 필드를 채웁니다.

필드	설명
선택한 옵저버블	영향을 받는 옵저버블입니다. 이 작업은 여러 옵저버블에 대한 표시기를 만드는 데 사용할 수 있습니다. 옵저버블을 선택 취소하려면 목록에서 옵저버블을 선택 취소하면 됩니다. **주:** 지원되는 옵저버블 형식이 매핑되지 않은 경우 이러한 옵저버블에 대한 표시기가 Microsoft Defender에 만들어지지 않습니다.
직위	표시기의 제목입니다.
설명	표시기에 대한 설명입니다.
만료 시간	표시기의 만료 시간입니다.
권장 작업	표시기에 대해 수행해야 하는 권장 작업입니다.
소스	표시기를 생성하기 위한 통합 구성입니다.
작업	조직에서 표시기가 발견되면 수행할 작업입니다. 가능한 값은 다음과 같습니다. ○ 경고 ○ 블록 ○ 감사 ○ '차단 및 수정 ○ 허용됨
애플리케이션	표시기와 연결된 엔드포인트용 Microsoft Defender 애플리케이션입니다. 이 필드는 새

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	표시기에만 적용할 수 있으며 기존 표시기에는 사용할 수 없습니다.
심각도	표시기의 심각도입니다. 가능한 값은 다음과 같습니다. ○ 낮음 ○ 보통 ○ 높음
RBAC 그룹 이름	표시기가 적용될 RBAC 그룹 이름입니다. 이름은 쉼표로 구분된 목록에 있습니다.

8. 표시기 작성 클릭
9. 활동 및 UI 메시지의 유효성을 검사합니다.
10. **Microsoft Defender** 표시기 탭을 클릭하여 결과를 봅니다.

에서 표시기 업데이트 **Microsoft Defender for Endpoint**

목록 컨텍스트 메뉴 또는 Microsoft Defender 표시기의 양식 뷰에서 각각 기존 표시기 Microsoft Defender for Endpoint 를 업데이트합니다.

시작하기 전에
필요한 역할: sn_si.admin, sn_si.analyst

프로시저

1. 다음으로 이동 보안 인시던트 〉 모든 인시던트 표시.
2. 모든 관련 목록 표시를 클릭한 다음 **Microsoft Defender** 표시기 탭을 클릭합니다.

   주:

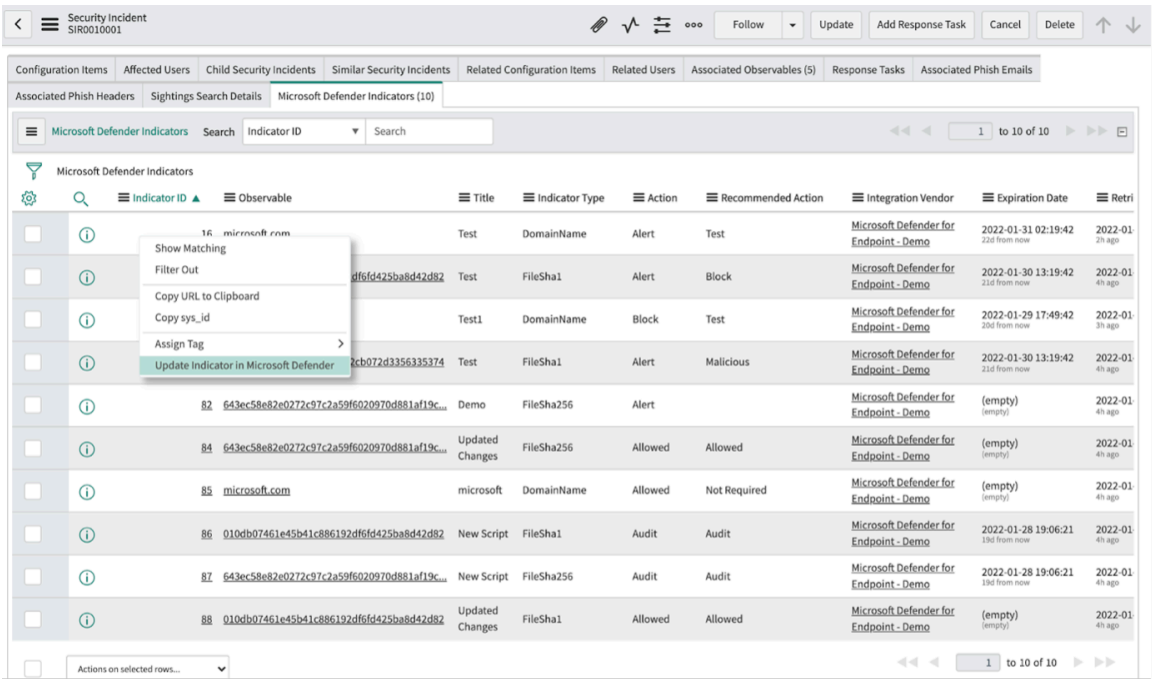
   보안 인시던트 관련 목록에 표시되는 Microsoft Defender 표시기에 대한 관련 목록을 구성해야 합니다. 자세한 내용은 양식 UI 작업을 참조하십시오.

3. 다음 방법 중 하나로 엔드포인트용 Microsoft Defender 표시기를 업데이트합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

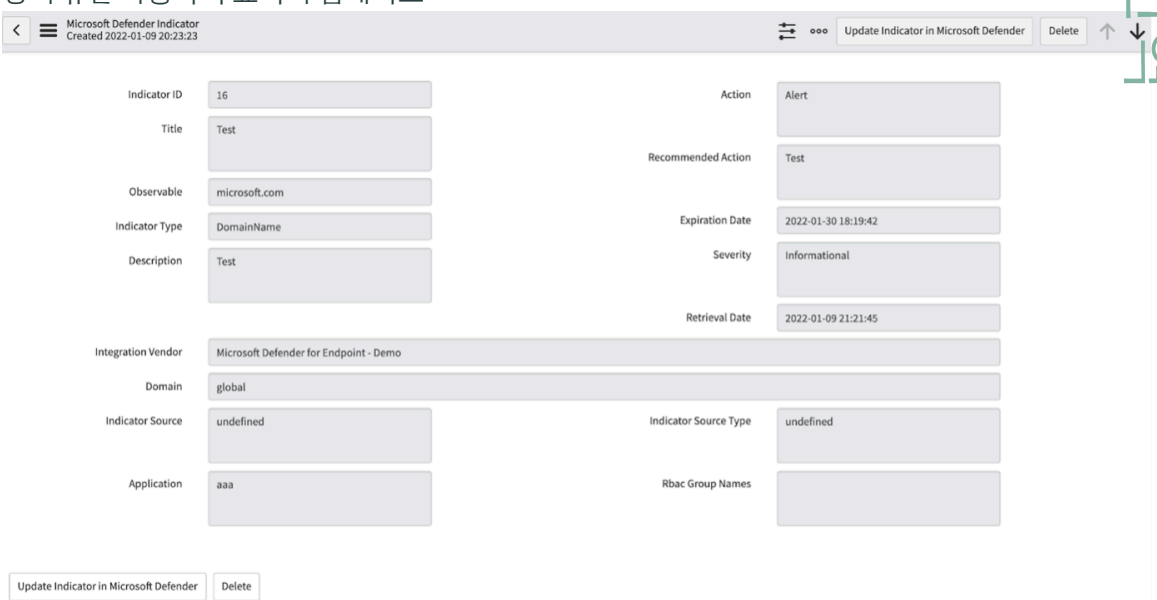
- 목록 상황에 맞는 메뉴에서 표시기를 업데이트하려면 업데이트할 표시기의 행을 선택하고 **Microsoft Defender** 옵션에서 표시기 업데이트를 클릭합니다.

  목록 컨텍스트 메뉴를 사용하여 표시기 업데이트



- 양식 뷰에서 표시기를 업데이트하려면 양식 뷰에서 **Microsoft** Defender의 표시기 업데이트를 클릭하십시오.

  양식 뷰를 사용하여 표시기 업데이트



4. 양식에서 필드를 채웁니다.

Microsoft Defender 표시기 양식

필드	설명
직위	표시기의 제목입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
설명	표시기에 대한 설명입니다.
만료 시간	표시기의 만료 시간입니다.
권장 작업	표시기에 대해 수행할 권장 작업입니다.
소스	표시기를 생성하기 위한 통합 구성입니다.
작업	조직에서 표시기가 발견되면 수행되는 작업입니다. 가능한 값은 다음과 같습니다. ○ 경고 ○ 블록 ○ 감사 ○ **BlockAndRemediate** ○ 허용됨
애플리케이션	표시기와 연결된 엔드포인트용 Microsoft Defender 애플리케이션입니다. 이 필드는 새 표시기에만 적용할 수 있으며 기존 표시기에는 사용할 수 없습니다.
심각도	표시기의 심각도입니다. 가능한 값은 다음과 같습니다. ○ 낮음 ○ 보통 ○ 높음
RBAC 그룹 이름	표시기가 적용되는 RBAC 그룹 이름입니다. 이름은 쉼표로 구분된 목록에 있습니다.

5. 표시기 업데이트를 클릭합니다.

6. 활동 및 UI 메시지의 유효성을 검사합니다.

통합의 **Microsoft Defender for Endpoint** 도메인 분리

도메인 분리는 통합에서 Microsoft Defender for Endpoint 지원됩니다. 도메인 분리를 사용하여 데이터, 프로세스 및 관리 작업을 도메인이라는 논리적 그룹으로 분할할 수 있습니다. 그런 다음 사용자가 데이터를 보고 액세스할 수 있는 것을 포함하여 이러한 분리의 여러 가지 측면을 제어할 수 있습니다.

지원 수준

지원: 기본

도메인 분리에 다음 단계를 사용합니다.

1. 해당 도메인에서 sn_si.admin 역할을 가진 사용자를 생성합니다.

2. Microsoft Defender for Endpoint 적절한 도메인에서 통합 절차를 수행합니다.

통합의 **Microsoft Defender for Endpoint** 요율 제한 구성

API의 속도 제한과 통합 속도 제한 Microsoft Defender for Endpoint 에 대한 시간 제한을 구성합니다.

시작하기 전에

필요한 역할: sn_si.admin, sn_si.analyst(읽기 전용)

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 탐색 필터에 sys.properties.list를 입력합니다.
   시스템 속성 [sys_properties] 테이블에 전체 속성 목록이 나타납니다.
2. 요구 사항에 따라 다음 속성을 검색하고 수정합니다.

속성 이름	설명
sn_sec_defender_ep.rate_limit_timeout_in_minutes	지정된 시간 범위 내에 요청이 실행되지 않으면 실행이 중지되고 적절한 오류 메시지가 표시됩니다. 기본값: 75.
sn_sec_defender_ep.request_per_hour_limit	구성된 API 호출이 1시간 이내에 동일한 엔드포인트에서 수행되면 임계치에 도달하거나 구성된 시간 제한에 도달할 때까지 요청이 큐에 대기합니다. 기본값: 1500.
sn_sec_defender_ep.request_per_minute_limit	구성된 API 호출이 1분 이내에 동일한 엔드포인트에서 수행되면 임계치에 도달하거나 구성된 시간 제한에 도달할 때까지 요청이 큐에 대기합니다. 기본값: 100.
sn_sec_defender_ep.import_indicator_request_per_minute_limit	1분 이내에 엔드포인트에서 구성된 API 호출이 수행되면 임계치에 도달하거나 구성된 시간 제한에 도달할 때까지 요청이 큐에 대기합니다. 기본값: 30.

Microsoft Exchange Online 통합

에 의한 ServiceNow통합 애플리케이션의 경우, ServiceNow AI Platform# 보안 인시던트 응답 ()SIR 제품은 Office 365 제품군의 클라우드 기반 서비스 Microsoft 중 하나인 서비스와 통합됩니다Microsoft Exchange Online.Microsoft Exchange Online SOC(보안 운영 센터) 분석가는 회사 이메일 환경에서 보안 관련 위협을 검색하고 이메일 검색 및 삭제 기능을 사용하여 피싱 이메일을 제거 및 해결할 수 있습니다.

Microsoft Exchange Online 통합 개요

보안 인시던트 분석가가 보안 분석가 인터페이스에서 통합을 실행하면 워크플로우가 검색 기준과 일치하는 이메일 메시지 상세 정보를 반환합니다. 이메일 검색은 제목과 보낸 사람 및 받는 사람 이메일 주소를 포함하는 조건을 기반으로 합니다. 이메일 검색이 완료되면 의심스러운 이메일을 Microsoft Exchange Online 서비스에서 삭제할 수 있으며, 이메일을 삭제하기 전에 승인을 요청하도록 선택적 승인 프로세스를 구성할 수 있습니다.

이 이메일 검색 및 삭제 통합은 광범위한 피싱 응답, 인시던트, 워크플로우 또는 Runbook과 함께 사용할 수 있습니다. 회사 사용자 또는 직원이 의심스러운 이메일을 수신하고 회사의 피싱 대응 팀 또는 받은 편지함에 보고하면 보고된 이메일이 보안 인시던트로 전달 ServiceNow AI Platform 되고 분류됩니다. 이메일이 피싱 공격임을 확인한 후 피싱 인시던트 조사를 담당하는 분석가는 이메일 검색을 시작하여 다른 회사 사용자가 이 피싱 이메일을 받았는지 확인할 수 있습니다. 검색을 통해

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

동일한 피싱 캠페인에서 관련 이메일을 찾고 이메일을 수신하고 읽었으며 잠재적으로 악성 URL을 클릭하거나 첨부 파일을 열었을 수 있는 다른 잠재적 피해자를 식별할 수 있습니다.

주요 기능

통합에는 다음과 같은 주요 기능이 포함됩니다.

- 이메일 메시지의 보낸 사람, 받는 사람 및 제목 필드의 조합을 기반으로 보안 인시던트 응답에서 피싱 위협에 대한 검색 기준을 구성합니다.
- 크고 긴 이메일 검색의 경우 검색이 성공적으로 완료되면 보안 인시던트 분석가에게 일치하는 메시지 수와 함께 이메일이 전송됩니다.
- 개별 메일의 상태는 수신자가 의심스러운 이메일을 읽었거나 삭제했는지 알려줍니다.
- 구성된 경우 선택적 승인 프로세스를 통해 의심스러운 이메일이 사전 승인 없이 삭제되지 않습니다.
- 삭제된 이메일 수를 포함하는 삭제 요청에 대한 전체 감사 추적이 보안 인시던트의 작업 메모에 기록됩니다.
- 태그 지정이 구성된 경우 이메일 검색 및 삭제 워크플로우가 시작되고 보안 인시던트에서 성공적으로 완료될 때 보안 태그가 기록됩니다.

지원되는 **Microsoft Exchange Online** 버전

이 통합은 Office 365 제품군의 일부인 Microsoft 서비스를 지원합니다Microsoft Exchange Online. 통합은 호스팅 Microsoft 된 Exchange 환경을 지원하지 않습니다. Microsoft 는 Exchange 2016 버전에서 서비스를 실행합니다 Microsoft Exchange Online .

필수 구성요소

모든 ServiceNow AI Platform 버전에는 com.snc.si_dep 플러그인이 필요합니다. 이 플러그인은 제품을 지원하는 데 필요한 모든 종속성을 보안 인시던트 응답 자동으로 설치합니다. 다른 보안 운영 애플리케이션을 설치 및 활성화하기 전에 이 플러그인을 설치하고 활성화하십시오.

에서 ServiceNow Store다음 보안 운영 애플리케이션을 설치하고 활성화해야 합니다. 원활한 설치를 위해 아래 나열된 순서대로 한 번에 하나의 애플리케이션을 설치하고 활성화합니다.

1. 보안 통합 프레임워크
2. Security Support Common
3. 보안 지원 오케스트레이션
4. 보안 인시던트 응답

Microsoft Azure 계정 설정

이 통합을 위해 애플리케이션을 설치하기 ServiceNow 전에 Azure Portal에서 Microsoft 다음 설정 작업을 완료합니다. 이 계정을 사용하면 테넌트에서 이메일 메시지 세부 정보에 액세스할 수 Microsoft Exchange Online 있습니다.

시작하기 전에
필요한 역할: Microsoft Azure Portal 관리자

이 계정은 테넌트에 Microsoft Exchange Online 액세스하여 추가 이메일 메시지 세부 정보를 수집하고 이메일 메시지를 삭제하는 데 필요합니다. 이 계정은 Azure Portal에서 Microsoft 설정됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음 작업의 이미지는 권한이 있고 독점적이며 의 Microsoft허가를 받아 사용됩니다. 이 콘텐츠는 에 의해 Microsoft업데이트될 수 있습니다. 최신 콘텐츠에 액세스할 수 있는지 확인하려면 Microsoft 문서 웹 사이트를 참조하세요.

다음 이미지에서 ServiceNow Inc. 는 Azure 포털 예제의 계정 이름으로 표시됩니다. Azure Portal 계정에서 Azure Portal의 계정에 대한 회사 이름이 표시됩니다.

프로시저

Azure Portal에서 OAUTH 인증을 위한 애플리케이션 ID를 Microsoft 만들지 않은 경우 다음 단계를 수행합니다.

a. Azure Portal 관리자 자격 증명을 사용하여 Azure Portal에 Microsoft 로그인합니다.

b. 검색 상자에 **App** registrations를 입력합니다.

c. 새 등록을 선택합니다.

d. 표시되는 애플리케이션 등록 양식을 작성합니다.

필드	설명
이름	애플리케이션의 이름입니다. 이 예에서는 ServiceNow Exchange Online ## 이 입력됩니다.
지원되는 계정 유형	이 계정의 경우 지원되는 계정 유형에서 이 조직 디렉터리의 계정만(조직 이름)을 선택합니다. 이 도메인은 이메일 검색에 사용됩니다.
리디렉션 URL(선택 사항)	이 필드에 대한 값을 입력하면 통합에서 사용되지 않습니다.

e. 등록을 선택합니다.
애플리케이션 ID가 생성됩니다. 이 ID는 사용자 이름과 유사합니다. 에 설명된 Microsoft Exchange Online 통합 구성인스턴스의 구성 단계 ServiceNow AI Platform 중에 구성 페이지의 **OAUTH** 애플리케이션 **ID** 필드에 이 값을 입력합니다.

f. 관리에서 매니페스트를 선택합니다.

g. **requiredResourceAccess** 항목(52줄 또는 그 이상)을 찾습니다.

h. 다음 코드 스니펫을 사용하여 **resourceAppId**, **resourceAccess id** 및 **resourceAccess** 유형 값을 수정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
"requiredResourceAccess": [
        {
                "resourceAppId": "00000003-0000-0000-c000-000000000000",
                "resourceAccess": [
                        {
                                "id": "e2a3a72e-5f79-4c64-b1b1-878b674786c9",
                                "type": "Role"
                        },
                        {
                                "id": "dd98c7f5-2d42-42d3-a0e4-633161547251",
                                "type": "Role"
                        }
                ]
        }
 ],
```

i. 저장을 선택합니다.

j. 관리에서 **API** 권한을 선택합니다.

k. 권한 추가를 선택합니다.

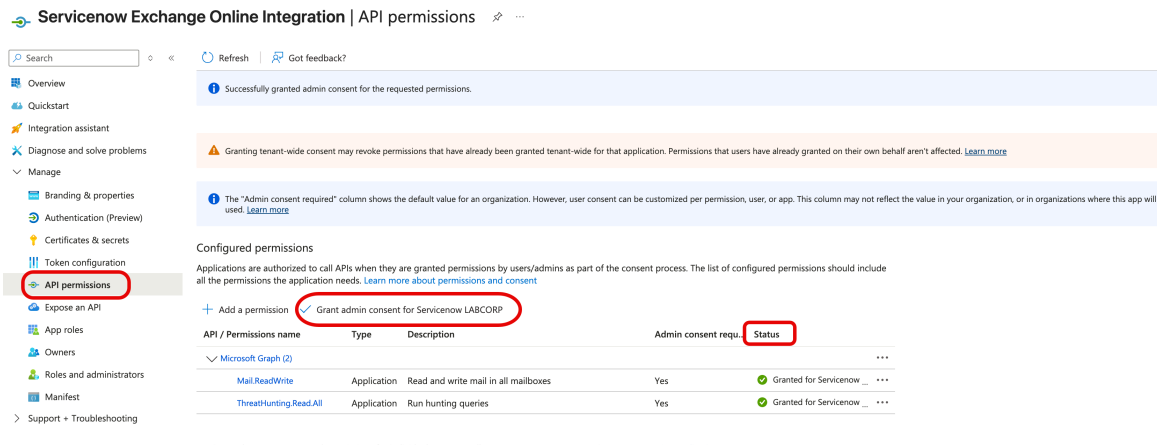
l. 표시되는 API 권한 요청 창에서 **Microsoft Graph**를 선택합니다.

m. 표시되는 API 권한 요청 창에서 애플리케이션 권한을 선택합니다.

n. 표시되는 사용 권한 선택 필드에 **Threat** 를 입력하고 **ThreatHunting.Read.All** 확인란을 선택합니다.

o. 〈조직〉에 대한 관리자 동의 부여를 선택합니다.

p. 예를 선택합니다.
이제 〈조직〉에 대한상태 값이 부여되어야



합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 수행할 작업
통합을 위한 인스턴스를 설정할 ServiceNow AI Platform# 준비가 되었습니다.

애플리케이션 설치 **Microsoft Exchange Online**

인스턴스에서 통합을 실행하기 전에 에서 ServiceNow Store통합을 위한 Microsoft Exchange Online 애플리케이션을 설치합니다.

시작하기 전에
인스턴스에서 애플리케이션을 ServiceNow StoreServiceNow AI Platform 설치하기 전에 필수 검사 목록에 나열된 모든 작업을 완료합니다.

필요한 역할: 관리자

프로시저

1. 통합을 위해 애플리케이션을 설치하지 않은 경우 이를 확인하고 보안 운영 통합 설치 단계에 따라 설치합니다.
2. 에서 ServiceNow Store애플리케이션을 설치한 후 인스턴스에 연결 ServiceNow AI Platform 하도록 구성합니다.

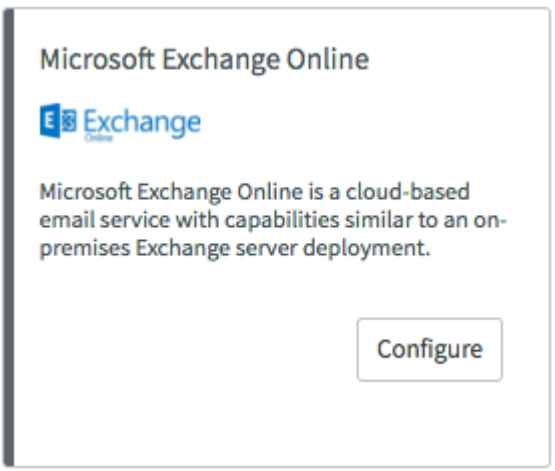
Microsoft Exchange Online 통합 구성

에서 ServiceNow Store애플리케이션을 설치한 후 인스턴스에 연결 ServiceNow AI Platform 하도록 구성합니다. 이 활성화는 검색 및 삭제 워크플로우를 활성화합니다.

시작하기 전에
필요한 역할: sn_si.admin

프로시저

1. 인스턴스에서 ServiceNow AI Platform 다음으로 이동합니다. 보안 운영 > 통합 > 통합 구성.
2. 타일을 Microsoft Exchange Online 찾습니다.
3. 구성을 클릭합니다.

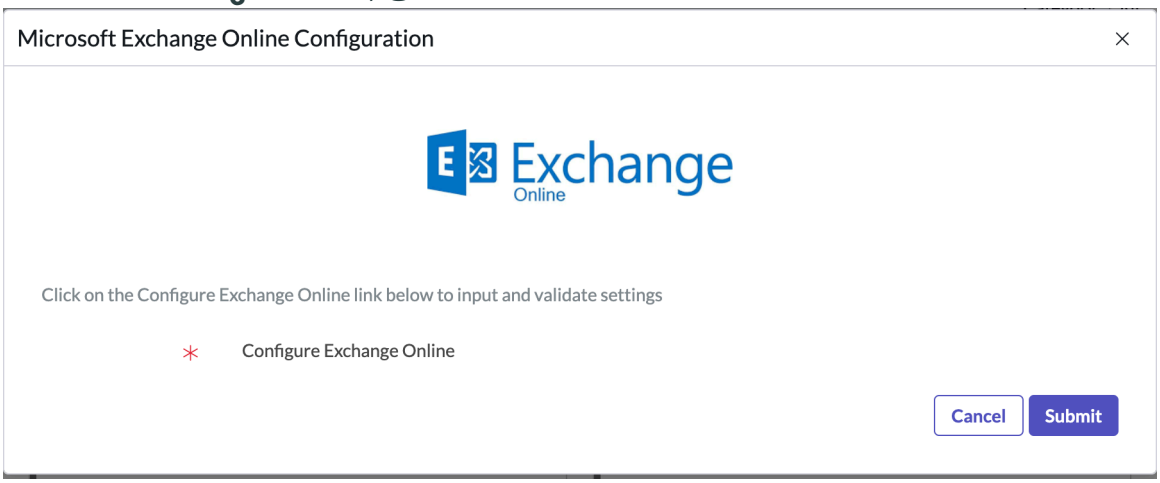


4. Microsoft Exchange Online 표시되는 구성 대화 상자에서 **Exchange Online** 구성을 클릭합니다.

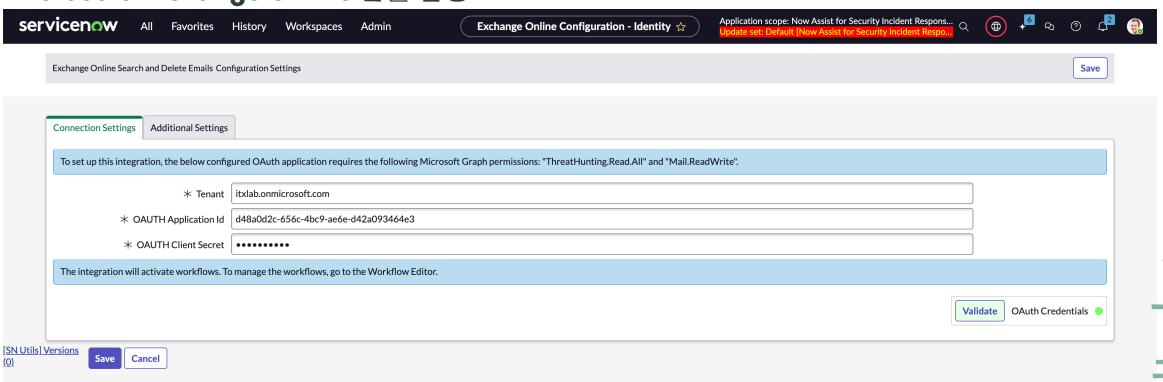
   완료되고 확인된 양식의 예가 테이블 다음에 나옵니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

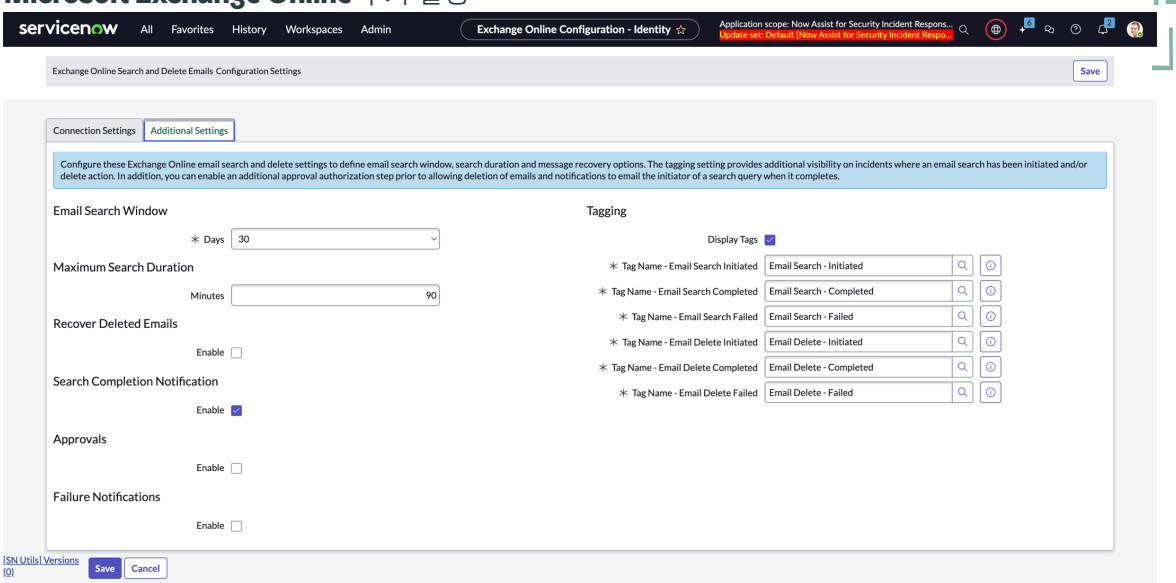
Microsoft Exchange Online 구성



Microsoft Exchange Online 연결 설정



Microsoft Exchange Online 추가 설정



5. 계속하려면 하나를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Trouble?
오류 메시지가 표시되거나 유효성 검사 단추 오른쪽에 있는 표시기 중 하나 이상이 빨간색이면 입력한 사용자 계정 자격 증명이 유효한지 확인합니다. 자격 증명을 입력하고 저장을 다시 클릭합니다.

확인 실패

확인 버튼과 색이 지정된 아이콘에 대한 자세한 내용은 다음 테이블을 참조하십시오.

확인 버튼 및 표시기의 상태	설명
확인 버튼은 녹색이고 모든 작은 색상 표시기는 녹색입니다.	MID 서버 연결 및 자격 증명이 유효함을 나타냅니다.
확인 버튼은 연한 빨간색에 파란색 테두리가 있고 작은 색상의 표시기 하나 또는 전부가 주황색입니다.	유효성 확인이 진행 중입니다. 확인을 완료하는 데 몇 분 정도 더 걸릴 수 있습니다.
확인 단추가 연한 빨간색이고 작은 색 표시기 하나 또는 전부가 빨간색입니다.	• Exchange Online 인증서 기반 인증 또는 OAuth 자격 증명 단추가 빨간색: Exchange Online 자격 증명이 잘못되었음을 나타냅니다. • Exchange Online 인증서 기반 인증 및 MID 서버 준비 단추가 빨간색: MID 서버에 연결할 수 없으므로 MID 서버를 통한 Exchange Online 인증서 기반 인증이 실패했음을 나타냅니다. • Exchange Online 인증서 기반 인증 표시기는 빨간색이지만 MID Server 준비 단추가 녹색: MID Server가 활성 상태이고 올바르게 구성되었지만 Exchange Online 인증서 기반 인증이 올바르지 않음을 나타냅니다.

이메일 검색 기준 정의 및 서비스 검색 **Microsoft Exchange Online** 요청

sn_si.analyst 역할을 가진 사용자는 검색 기준을 정의하고 보안 인시던트 기록의 인시던트 상세 정보를 기반으로 이메일 검색 요청을 제출합니다.

시작하기 전에
필요한 역할: sn_si.analyst

이 절차의 그림은 시스템 설정에서 선택한 탭 양식 과 함께 표시됩니다. 탭 폼을 선택하고 지우는 방법에 대한 자세한 내용은 ServiceNow 제품 설명서 웹 사이트에서 폼 레이아웃 구성의 탭 폼 표시 섹션을 참조하십시오.

필요한 역할: sn_si.analyst

이 태스크 정보
검색 쿼리 및 검색 결과와 일치하는 개별 메시지의 상태는 보안 인시던트 기록에 보고됩니다. 이메일 알림을 사용하는 경우 이메일 메시지에서 검색 결과를 볼 수 있습니다.

검색 기준에는 메시지 보낸 사람 주소, 받는 사람 주소 또는 제목 이름이 포함될 수 있습니다. 다음과 같은 메시지 제목, 보낸 사람 및 받는 사람 검색 매개 변수 조합은 단일 피싱 캠페인의 일부일 수 있는 피싱 관련 전자 메일 메시지를 찾는 데 자주 사용됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 피싱 계정에서 보낸 모든 원본 이메일 찾기: 보낸 사람으로 검색합니다.
- 단일 피싱 캠페인에 대한 모든 원본 이메일 찾기: 제목 및 보낸 사람으로 검색합니다.
- 단일 피싱 캠페인에 대해 수신된 모든 이메일 찾기(원본 및 전달된 모든 발신자): 제목으로 검색합니다.
- 단일 사용자의 단일 피싱 이메일에 대해 전달된 모든 이메일 찾기: 수신자 + 제목으로 검색.
- 단일 사용자에게 전송된 모든 피싱 관련 이메일 찾기: 보낸 사람 + 받는 사람으로 검색합니다.

주:
검색은 초기 설정 중에 더 짧은 검색 기간을 구성하지 않은 한, 지난 30일 이내에 주고받은 이메일에 대해 수행됩니다. 이메일을 삭제하려면 먼저 이메일 검색이 성공해야 합니다.

다음 예는 보안 인시던트에서 ServiceNow AI Platform 검색을 시작하는 방법을 보여줍니다. 조직의 서버에서 피싱 공격으로 의심되는 이메일의 원본 이메일을 기반으로 보안 인시던트가 Microsoft Exchange Online 생성됩니다. 이 예에서 검색 기준은 보낸 사람(보낸 사람)과 제목이며, 여기서 보낸 사람은 phisher@cbazyx.com 이고 제목 은 ### ###입니다.

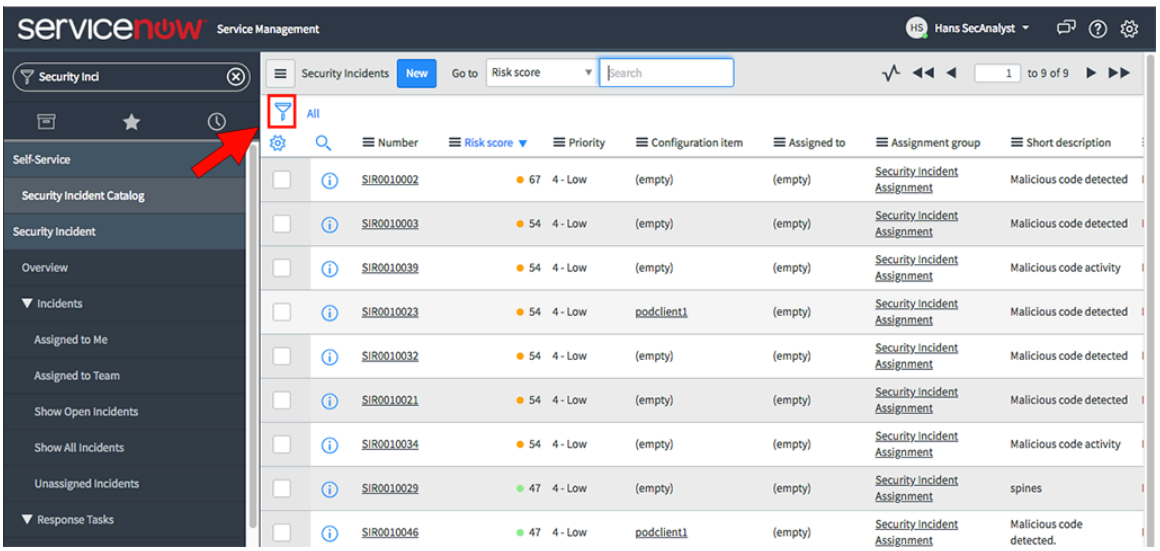
검색에서 입력한 검색 조건과 일치하는 키워드가 포함된 텍스트 문자열을 찾으면 주제에 대한 검색 결과가 반환됩니다. 이 예에서 제목은 ### ###입니다. **AND** 연산자를 사용하여 보낸 사람 및 제목 검색 조건을 구분하여 지정된 검색 기준을 포함하는 모든 전자 메일 메시지에 대한 결과를 반환합니다. 다음 단계에서는 특정 피싱 계정에서 보낸 제목 줄 텍스트가 포함된 이메일만 찾는 검색을 설정하는 방법을 설명합니다.

프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 모든 인시던트 표시 을 클릭하고 작업 중인 보안 인시던트를 찾습니다.
2. 또는 피싱 이벤트에 의해 생성된 보안 인시던트만 표시되도록 다음 단계에 따라 필터를 설정하고 실행합니다.

   a. 다음으로 이동 보안 인시던트 〉 모든 인시던트 표시 을 클릭하여 보안 인시던트 목록을 엽니다.

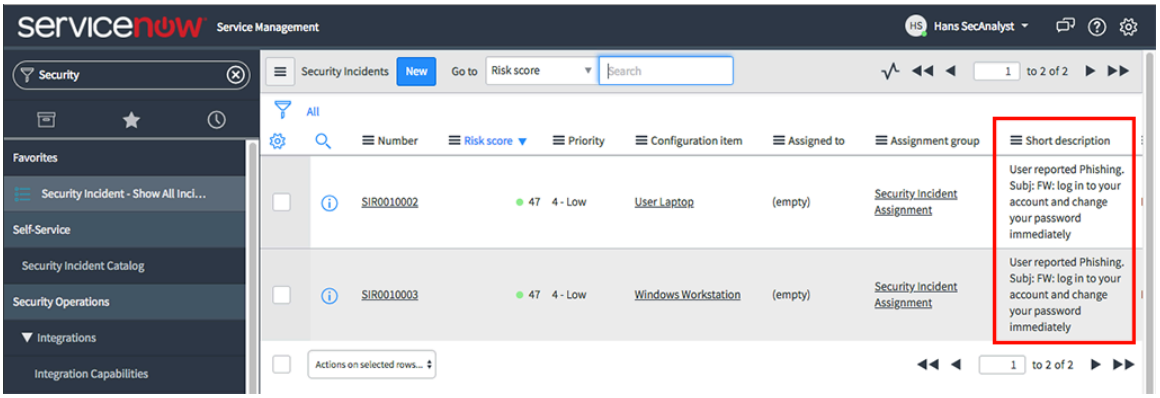
   b. 표시되는 목록의 왼쪽 위 모서리에서 필터 아이콘을 클릭합니다.



   c. 표시되는 필드에서 간단한 설명 〉 포함 선택 목록에서 **User reported** phishing(사용자 보고 피싱)을 입력하고 Run(실행)을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

피싱 관련 보안 인시던트가 표시됩니다.

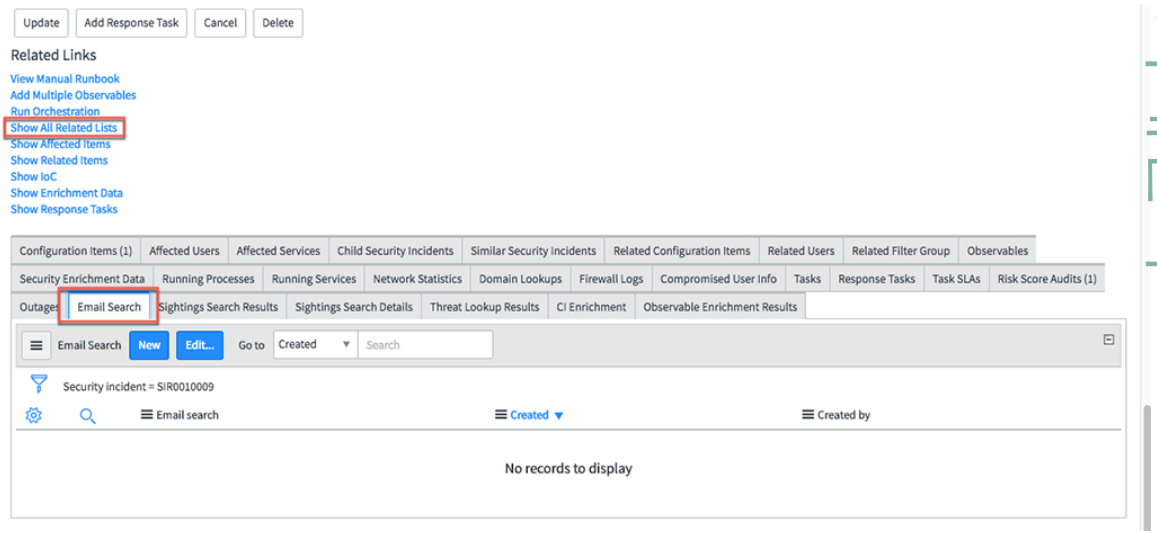


d. 짧은 설명 열의 텍스트를 사용하면 작업 중인 보안 인시던트를 찾는 데 도움이 됩니다.

e. 번호 열에서 보안 인시던트를 클릭하여 기록을 엽니다.

3. 보안 인시던트 기록의 아래쪽으로 스크롤한 다음 이메일 검색 관련 목록을 클릭합니다.

이메일 검색 관련 목록이 표시되어 있지 않으면 모든 관련 목록 표시 관련 링크를 클릭하여 이 관련 목록을 표시합니다.



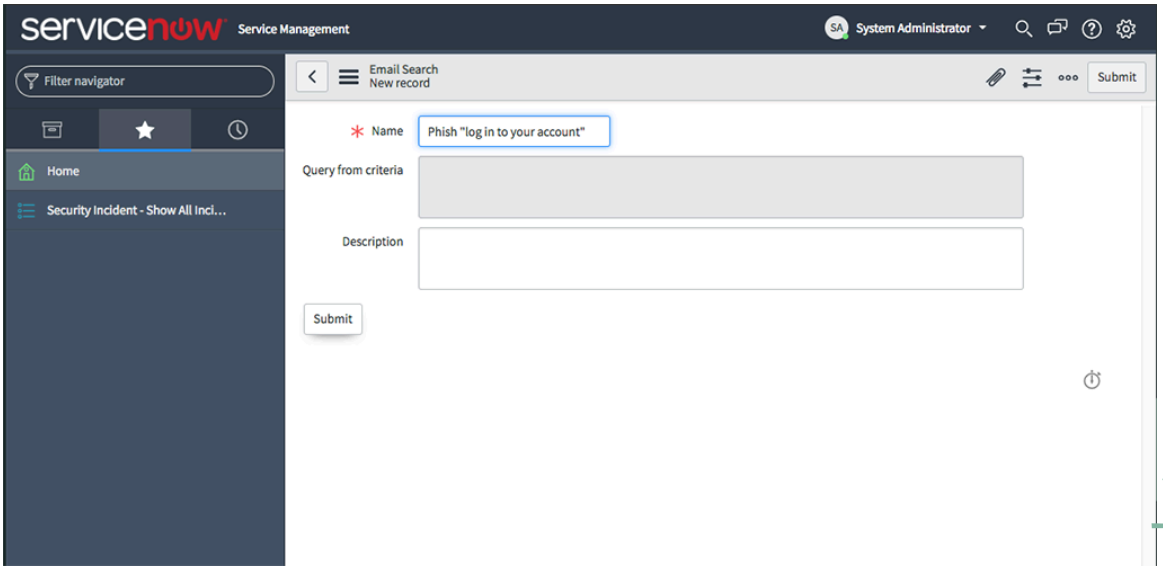
4. 이메일 검색 관련 목록에서 새로 만들기를 클릭하여 새 이메일 검색 기록을 만듭니다.
이메일 검색 양식이 표시됩니다. 약간의 수정을 통해 동일한 피싱 관련 인시던트에 대해 이 검색 쿼리를 다시 실행하기로 결정한 경우 이 검색 쿼리 기록을 다시 사용할 수 있습니다. 그러나 피싱 캠페인은 동적이고 보낸 사람 및 메시지 필드가 자주 변경되기 때문에 다른 피싱 관련 인시던트에 대해 이 검색을 사용할 가능성은 거의 없습니다.

5. 옵션: 기존 검색 쿼리 기록을 편집하려면 편집을 클릭합니다.

6. 이메일 검색 양식의 필드에 내용을 입력합니다.

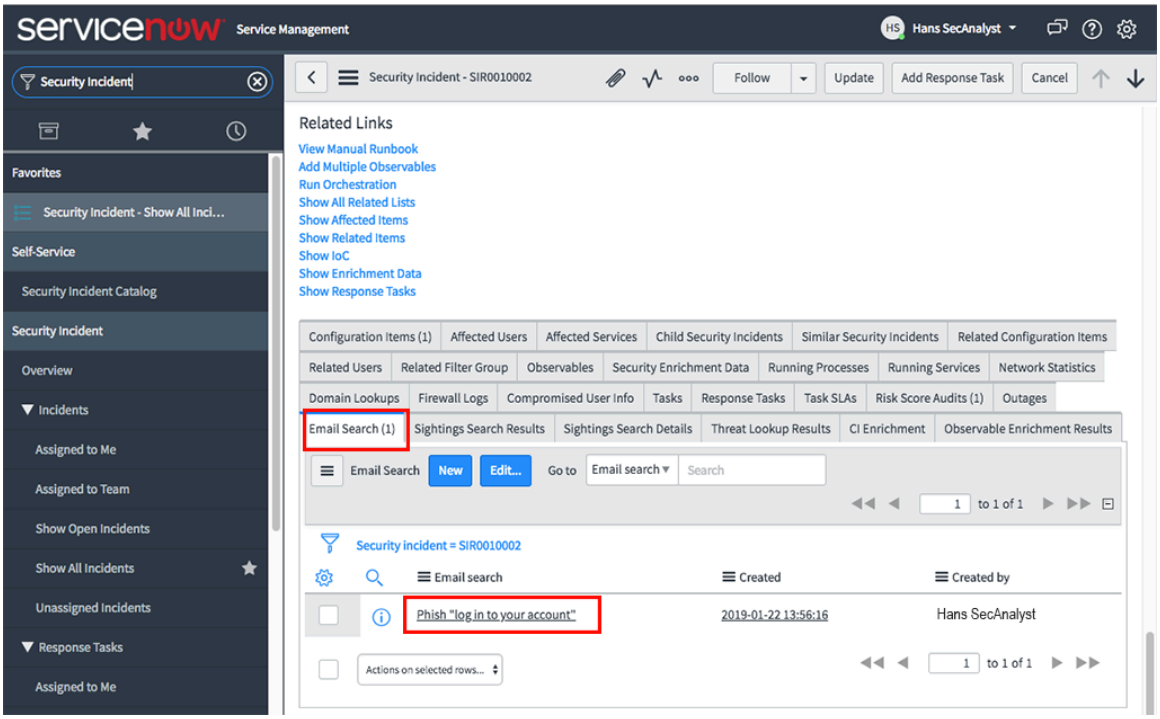
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
이름	검색 유형을 설명하는 정보입니다. 이 예제에서 보낸 사람 + 제목 검색의 이름은 ## "### ###"입니다.
설명	이메일 서버의 검색에 대한 정보입니다. 이 검색의 예는 From=phisher@cbazyx.com + Subject=### ###입니다.

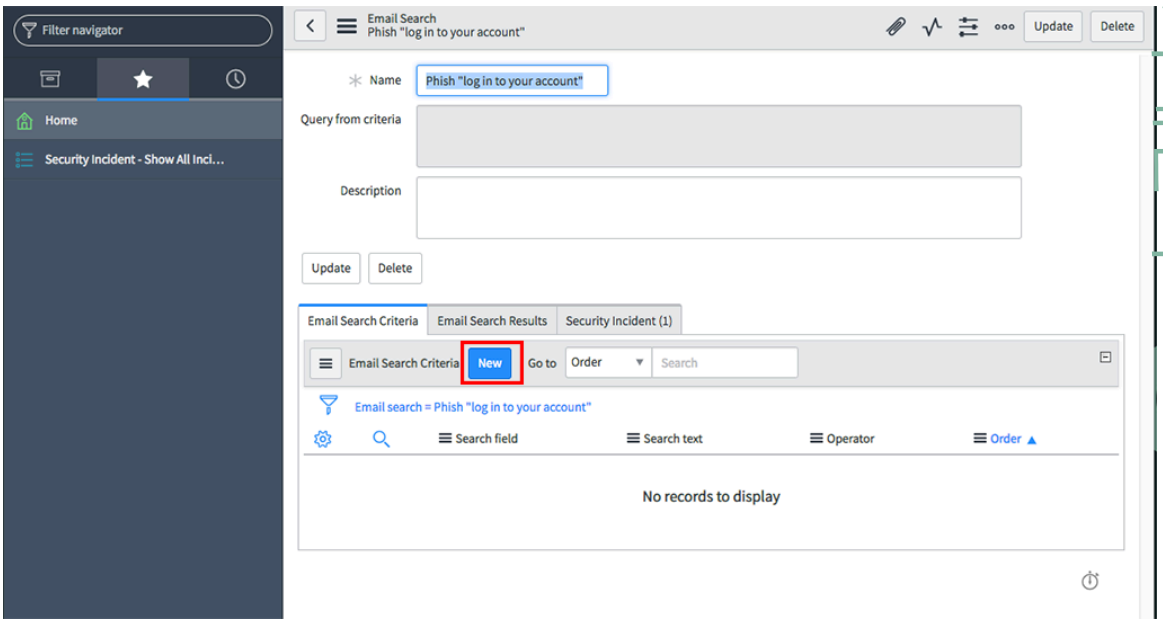


7. 제출을 클릭합니다.
   보안 인시던트가 표시되며, 이메일 검색 관련 목록의 이메일 검색 열에 이메일 검색 이름이 표시됩니다. 이 새 검색 쿼리를 사용하려면 먼저 검색 기록에 대해 검색 기준을 정의해야 합니다.
8. 검색 조건을 정의하려면 전자 메일 검색 관련 목록을 선택한 상태에서 전자 메일 검색 열에서 피시 "계정에 로그인"을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



9. 표시되는 이메일 검색 기록에서 이메일 검색 기준 관련 목록을 클릭하고 신규를 클릭합니다.



10. 이메일 검색 기준 양식의 필드에 내용을 입력합니다.

완료된 양식의 예가 테이블 다음에 나옵니다.

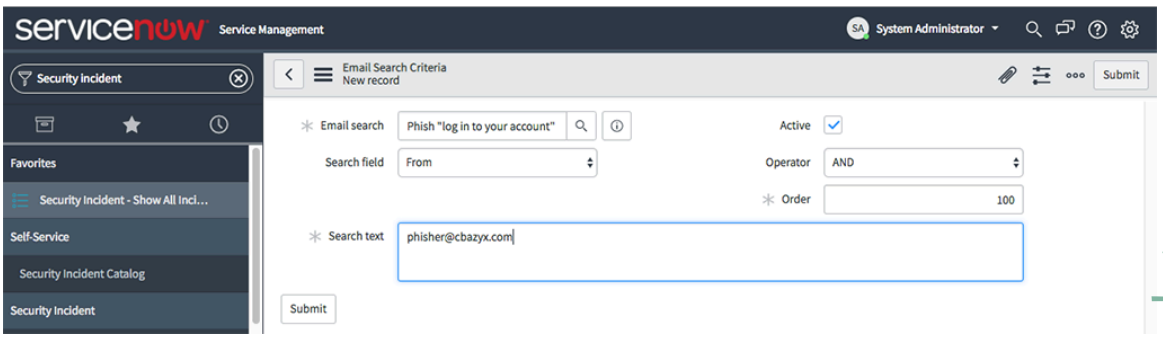
필드	설명
이메일 검색	이메일 검색 기록에 입력한 이름으로 필드가 자동으로 채워집니다.
검색 아이콘	목록을 사용하여 조회합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

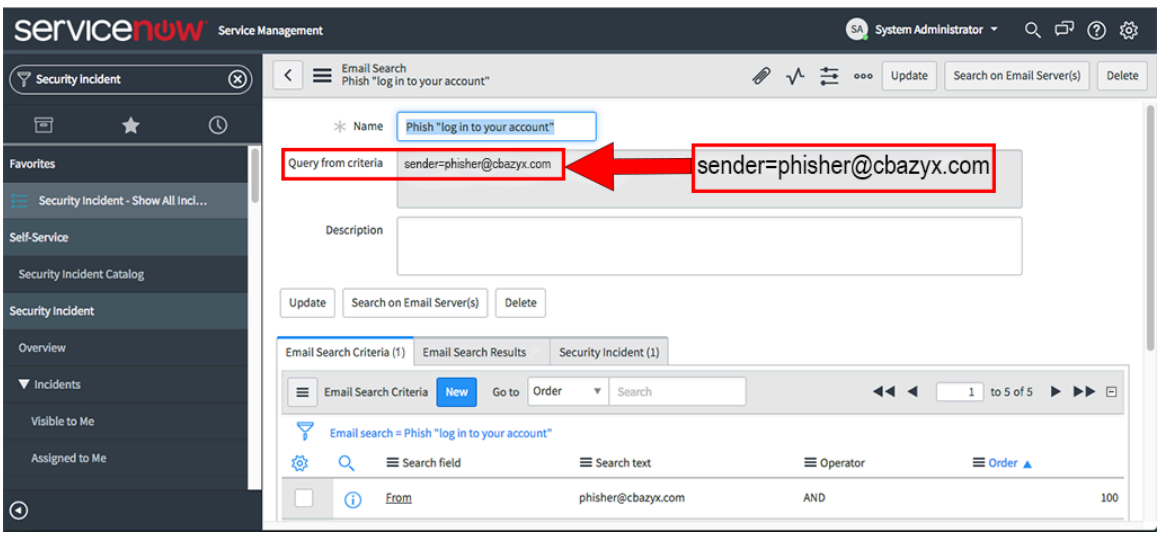
필드	설명
	저장된 검색 목록입니다. 아이콘을 클릭하여 저장된 이메일 검색 목록을 엽니다. 이 목록에서 항목을 클릭하여 현재 검색을 제거하고 이전에 저장한 이메일 검색을 선택합니다.
정보 아이콘	이메일 검색 기록을 보는 데 사용되는 아이콘입니다. 아이콘을 클릭하여 이메일 검색 기록을 봅니다.
검색 필드	검색 기준(제목, 보낸 사람 또는 수신자) 선택 목록에서 검색 기준을 선택하고 텍스트 필드에서 검색할 값을 정의합니다. 이 예에서는 보낸 ## phisher@cbazyx.com (피싱 전자 메일 보낸 사람의 전자 메일 주소)로 시작합니다.
활성	검색을 활성화하기 위한 옵션입니다. 검색은 기본적으로 활성화됩니다. 이 옵션의 선택을 취소하면 이 기록은 검색에 포함되지 않습니다.
운영자	연산자(**AND**, **OR)**를 사용하여 검색을 추가로 정의합니다. **AND**: 시스템은 **AND** 로 구분된 조건을 검색하고 모든 조건이 충족되는 경우에만 결과를 반환합니다. 보낸 사람 플러스 제목 검색의 경우 전자 메일 검색 중에 두 검색 조건이 모두 충족되도록 **AND** 연산자를 사용합니다. 이 예제에서는 쿼리가 From (Sender) = phisher@cbazyx.com **AND Subject** = ### ###되도록 **AND** 연산자를 사용합니다. **OR: OR**로 구분된 조건이 충족되면 시스템에서 결과를 검색하여 반환합니다. 예를 들어 보낸 사람(보낸 사람) = phisher@cbazyx.com 또는 보낸 사람 (보낸 사람) = phisher-2@cbazyx.com 입니다.
순서	검색 조건을 세 개 이상 입력하는 경우 순서를 사용하여 조건의 우선순위를 지정합니다. 기본값은 100입니다. 각 조건에 대해 1에서 100 사이의 값을 입력합니다(예: 100, 95, 90, 80). 가장 낮은 번호가 할당된 조건은 조건 그룹 내에서 검색 우선순위가 가장 높습니다.
검색 텍스트	검색할 텍스트 값(키워드)(이메일 주소 또는 제목 라인)입니다. 검색 필드에는 검색에 사용되는 텍스트(예: phisher@cbazyx.com)가 포함되어 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	검색에서 보낸 사람(보낸 사람) 및 받는 사람 검색에 대한 결과를 정확하게 반환하려면 검색 문자열이 정확히 일치해야 합니다. 주제 검색의 경우 검색 문자열에 더 큰 문자열의 일부인 키워드가 포함될 수 있습니다. 예를 들어, 제목에는 FW: ### ##### ## ### ##하십시오. 예를 들어, Log in to your account 는 log in to your account and change your password immediately 문자열의 정확한 키워드입니다. 포함 유형의 검색을 지원하는 데 와일드카드(*) 지정이 필요하지 않습니다. 현재 더 큰 텍스트 문자열에 속하지 않는 정확한 검색 문자열을 일치시키기 위한 필터링 방법이 없습니다.



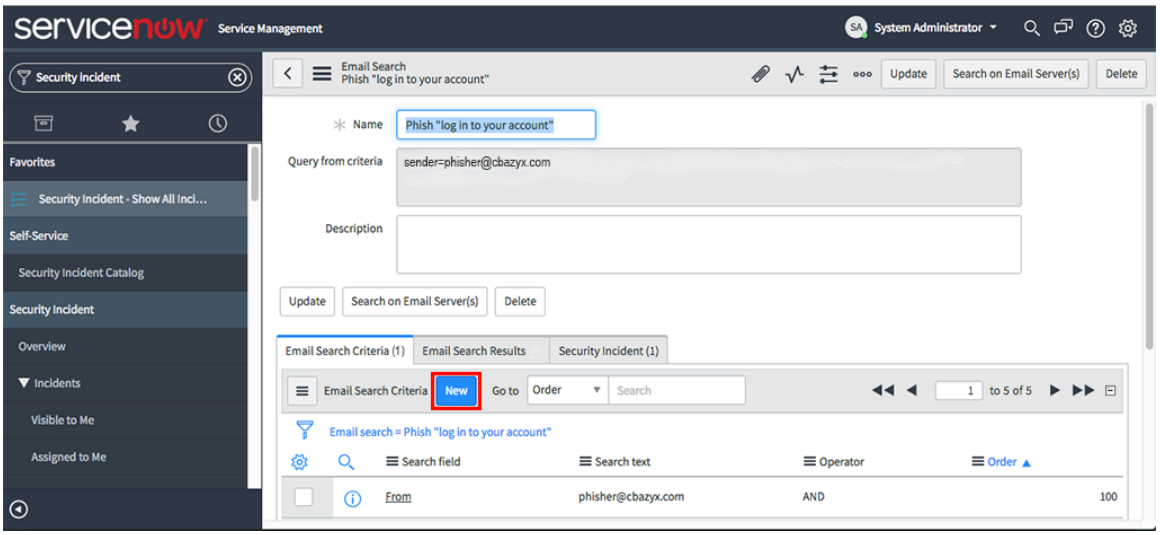
11. 제출을 클릭합니다.
이메일 검색 기록이 표시됩니다. 쿼리 원본 기준 필드에 보낸 사람(보낸 사람)에 대해 추가한 검색 기준이 표시됩니다.



12. 쿼리에 원하는 제목과 보낸 사람 조건이 포함되도록 이 이메일 검색 기준을 추가 정보로 업데이트하려면 다른 검색 조건을 추가하는 단계를 수행합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

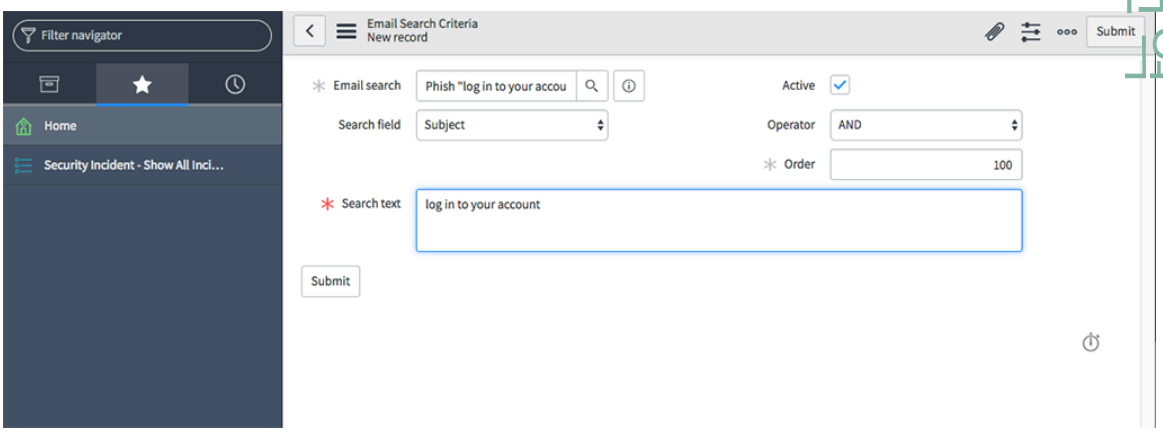
a. 이메일 검색 기준 관련 목록에서 새로 만들기를 클릭합니다.



b. 표시되는 이메일 검색 기준 기록의 검색 필드목록에서 제목을 선택합니다.

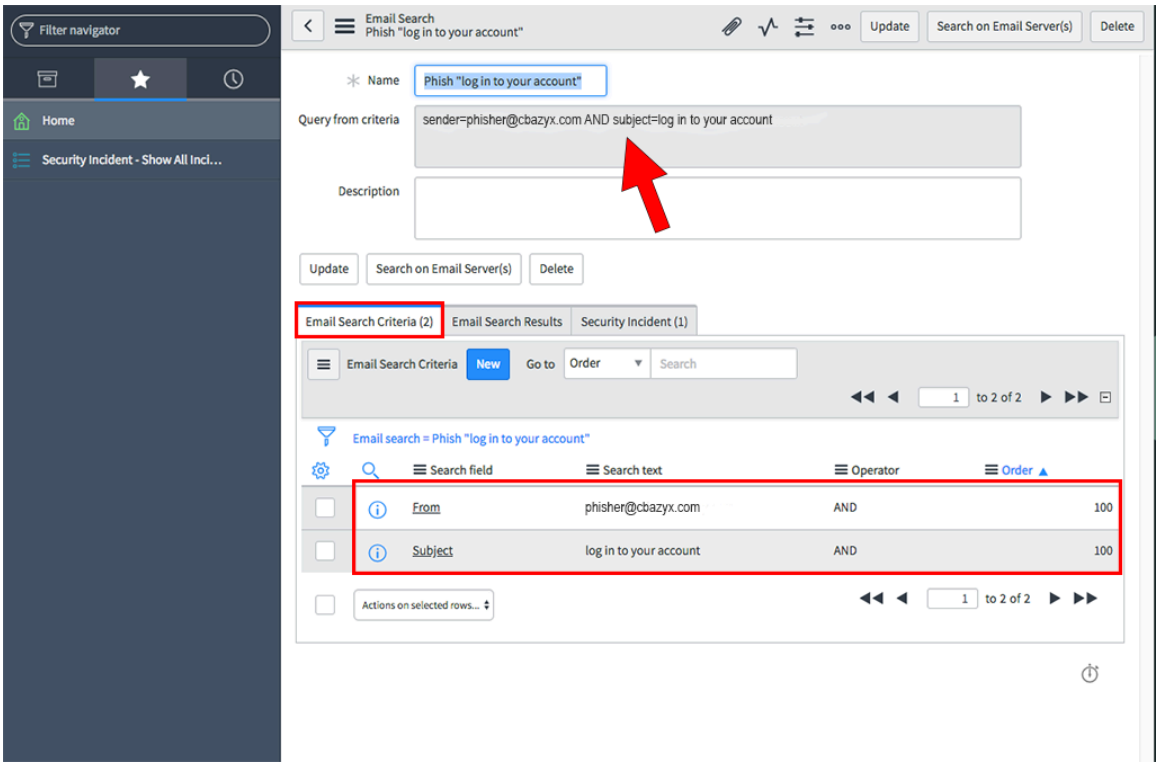
c. 연산자 목록에서**AND** 또는 **OR**을 선택합니다.
OR를 선택하면 제목 줄 텍스트 문자열의 키워드가 일치하거나 이메일 주소 조건이 일치하면 검색 결과가 반환됩니다. 이 예에서는 **AND**가 선택되어 있으므로 검색에서 제목 텍스트 문자열의 키워드를 포함하고 보낸 사람의 이메일 주소와 일치하는 이메일에 대해서만 결과를 반환합니다.

d. 검색 텍스트 필드에 제목 라인 텍스트에 대한 값을 입력하고 ### ######.



e. 제출을 클릭합니다.
새 조건이 이메일 검색 기준 관련 목록에 표시되며, 두 조건 모두 쿼리 원본 기준 필드에 **AND** 연산자로 구분되어 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



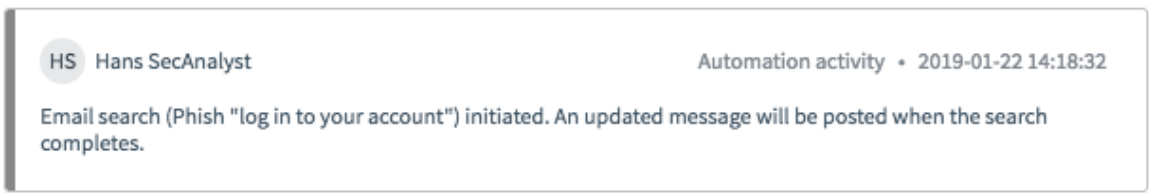
f. 옵션: 검색 조건이 두 개 이상이고 **AND** 를 선택하여 각 조건을 구분하는 경우 순서 값을 설정하여 우선 순위를 지정합니다.

g. 원하는 경우 검색 기준을 추가, 수정 또는 제거하고 업데이트를 클릭하여 기록에 대한 변경 내용을 저장합니다.

13. 계속하려면 하나의 옵션을 선택하십시오.

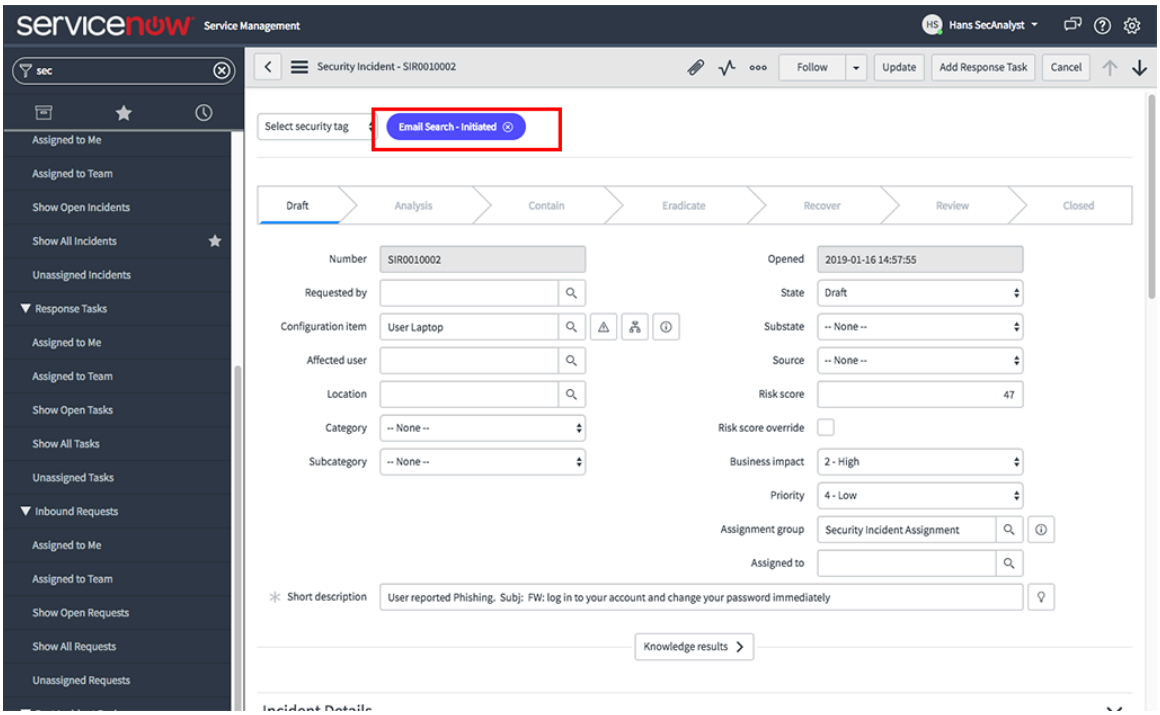
14. 이메일 검색을 시작하려면 이메일 검색 기록에서 이메일 서버에서 검색을 클릭합니다.
검색 요청이 제출되었음을 나타내는 메시지가 표시됩니다.

보안 인시던트 기록에 검색이 시작되었음을 나타내는 작업 메모가 표시됩니다.



태그 지정을 사용하는 경우 보안 인시던트 기록 상단에 ### ## - ### 보안 태그가 표시됩니다.

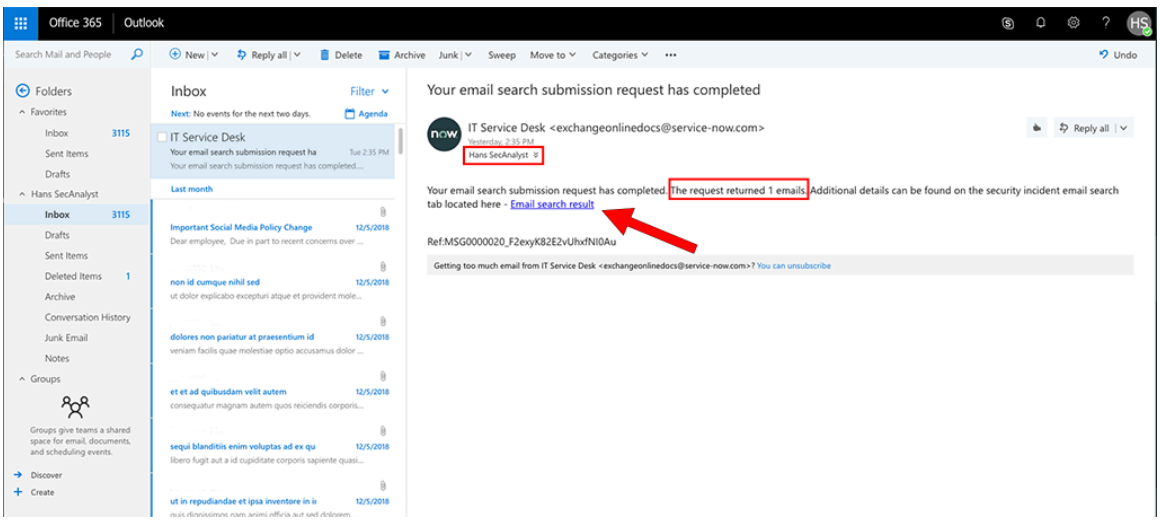
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



검색이 성공적으로 완료된 후 이메일 알림을 사용하는 경우 검색을 시작한 개인의 이메일 주소로 이메일이 전송됩니다.

이 예에서는 sn_si.analyst 역할을 가진 사용자인 Hans SecAnalyst가 이 검색을 제출했습니다. 다음 이미지는 이 알림이 의 계정으로 Microsoft Exchange Online전송되는 것을 보여줍니다. 그러나 이러한 알림은 필요에 따라 다른 이메일 서비스로 전송될 수 있습니다.

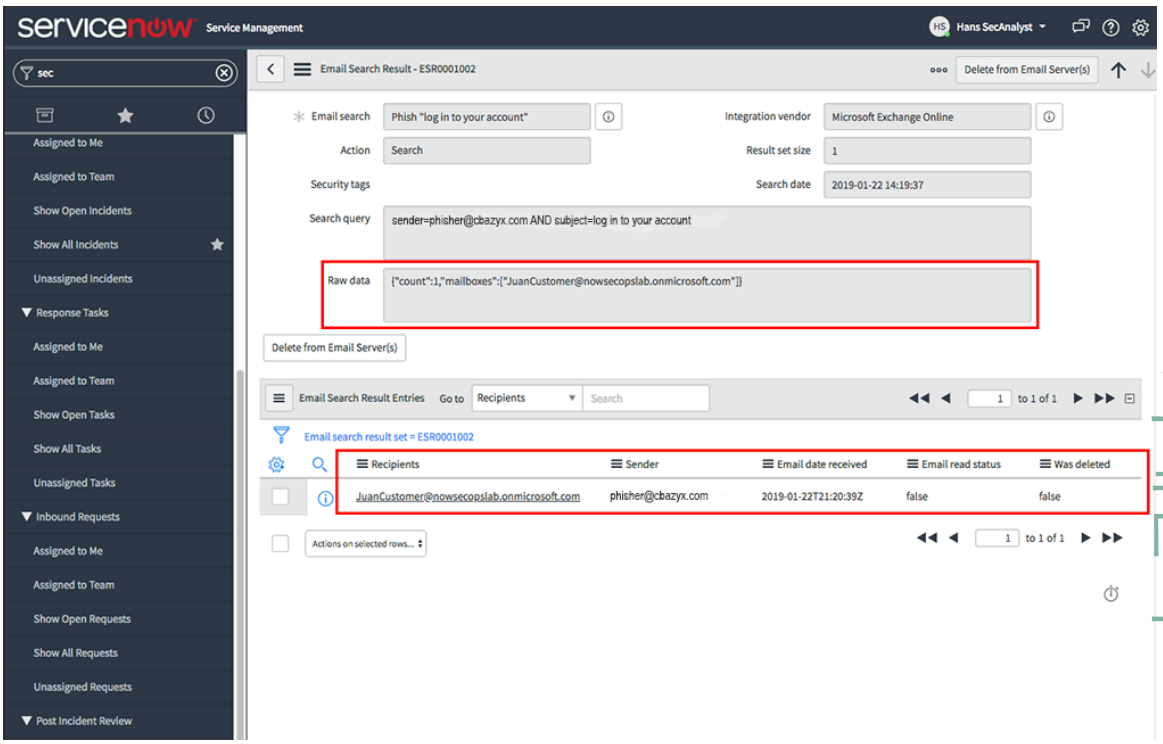
이 알림을 사용하면 후속 조치 및 삭제가 필요한 일치하는 결과를 볼 수 있습니다. 다음 예에서는 검색 기준과 일치하는 이메일이 하나 있음을 보여줍니다. 인스턴스의 이메일 검색 결과 기록 ServiceNow AI Platform 에 대한 이메일 검색 결과 링크도 제공됩니다. 검색 기록을 보려면 이 링크를 클릭합니다.



15. 이 이메일에서 검색 결과를 보려면 이메일 검색 결과 링크를 클릭합니다.
이메일 검색 결과 기록이 표시됩니다. 이 기록에서 다음 데이터를 검증하고 검토할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

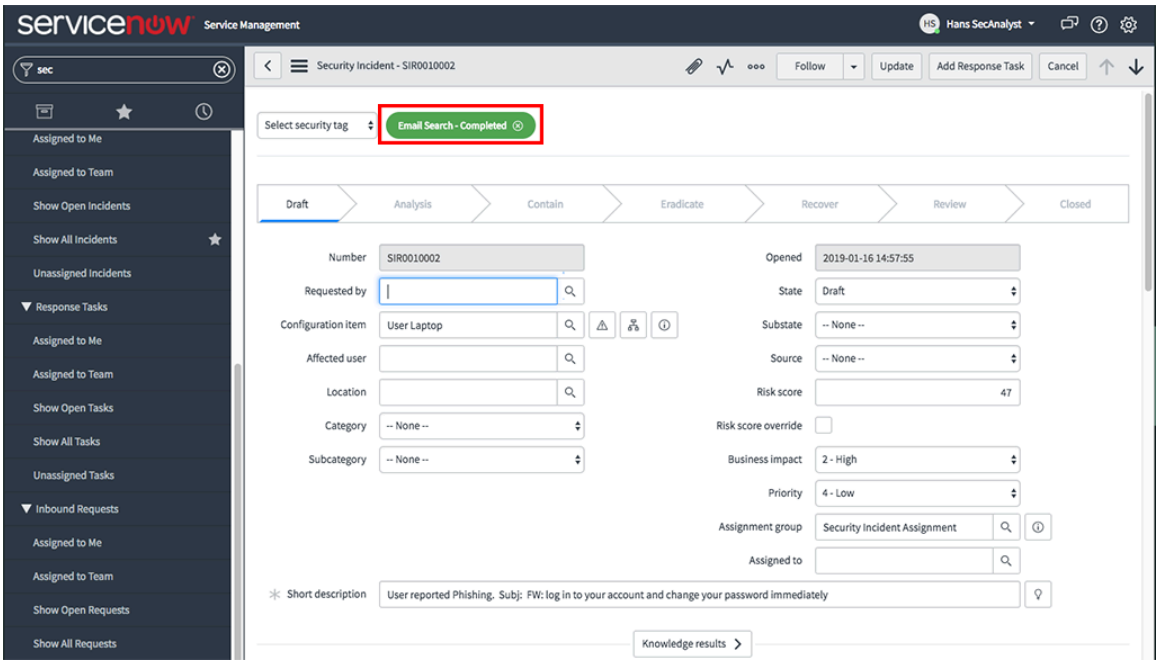
- 원시 데이터 필드에는 검색 기준 {"count":1}과 일치하는 이메일 수에 대한 이메일 개수와 이메일이 발견된 사서함 주소가 표시됩니다["JuanCustomer@nowsecopslab.onmicrosoft.com"].
- 수신자 열에서 수신자는 (JuanCustomer@nowsecopslab.onmicrosoft.com)입니다.
- ## ## 열에 이메일 원본이 표시됩니다.
- ### ## ## 열에는 피싱 캠페인 타임라인을 추적하는 데 도움이 되도록 이메일을 받은 날짜 및 시간이 표시됩니다.
- ### ## ## 열에서 이 예의 이메일은 읽히지 않았습니다(false). 이메일을 읽은 경우 true 가 표시됩니다.
- 삭제 # 열에서 이 예제의 이메일은 삭제되지 않았습니다. 이메일이 삭제된 경우 true 가 표시됩니다.



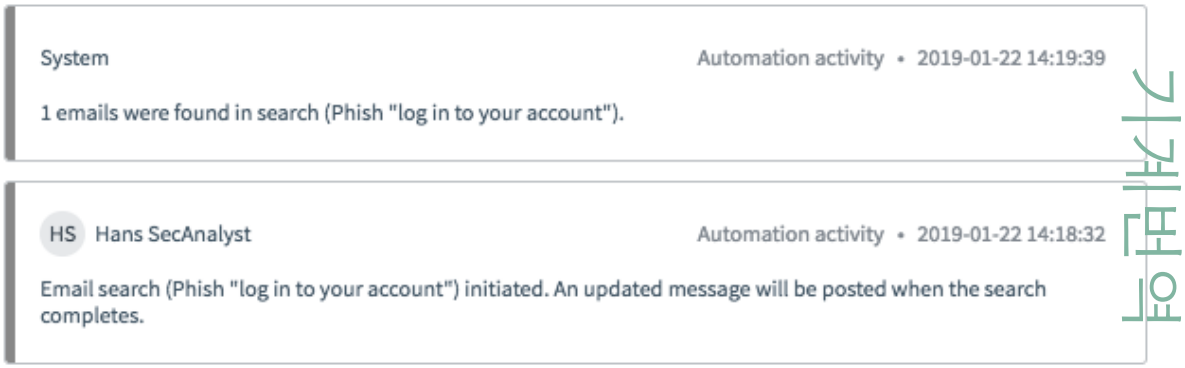
16. 또는 보안 인시던트의 검색 결과를 보려면 다음 단계를 수행합니다.

a. 다음으로 이동 보안 인시던트 〉 인시던트 을 클릭하고 작업 중인 보안 인시던트를 엽니다. 기록 상단에서 검색이 성공적으로 완료되면 ### ## - ### 보안 태그가 ### ## - ### 보안 태그를 대체합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



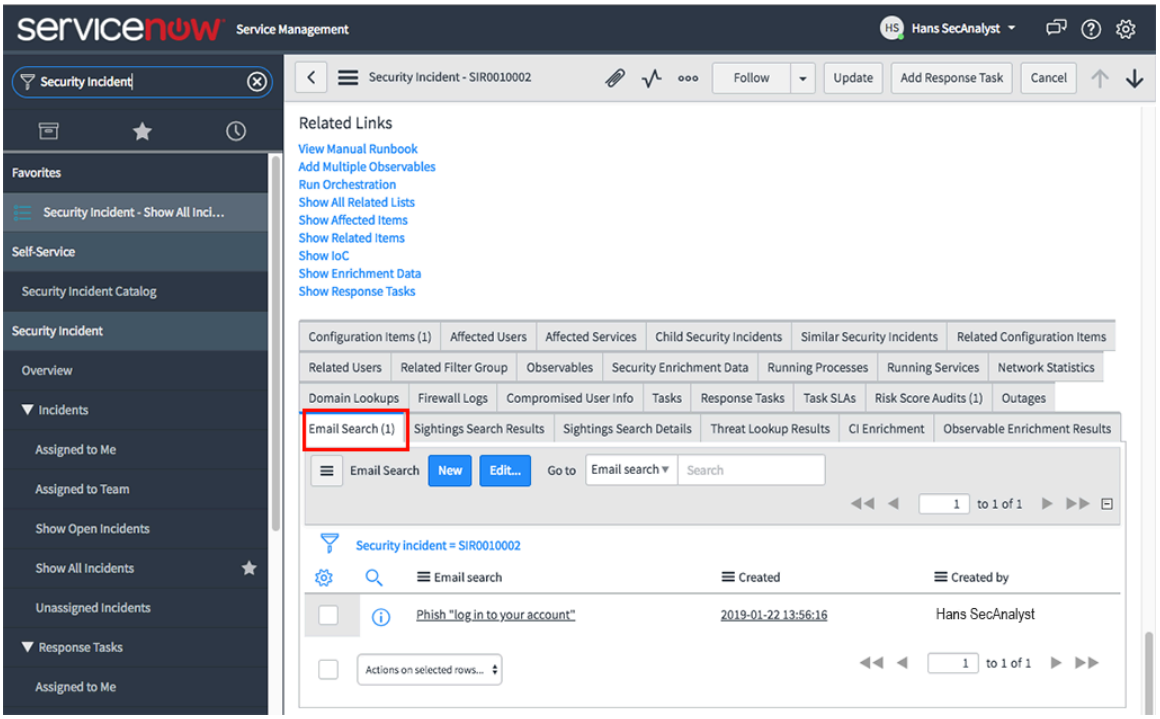
검색이 성공적으로 완료되었고 일치하는 이메일이 하나 발견되었다는 작업 메모가 표시됩니다.



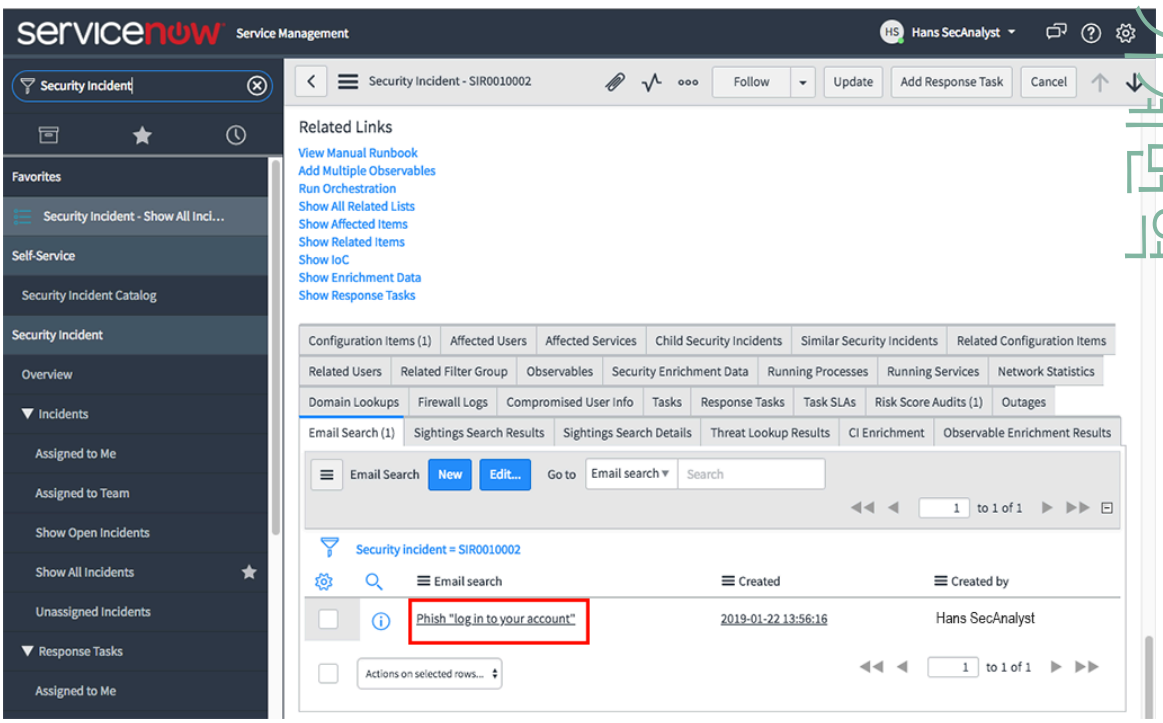
b. 보안 인시던트 기록의 아래쪽으로 스크롤한 다음 이메일 검색 관련 목록을 클릭합니다.

이메일 검색 관련 목록이 표시되어 있지 않으면모든 관련 목록 표시 관련 링크를 클릭하여 이 관련 목록을 표시합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



c. 이메일 검색 관련 목록을 선택한 상태에서 이메일 검색 열에서 검색 이름을 클릭합니다.

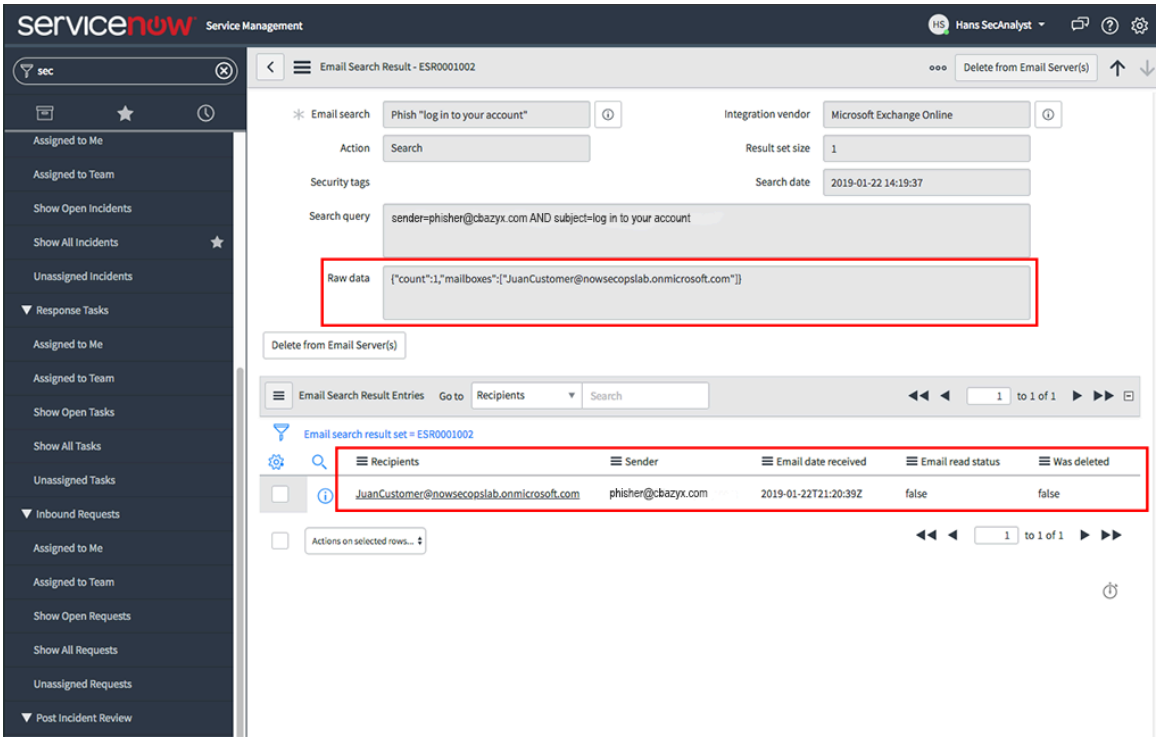


d. 이메일 검색 기록에서 이메일 검색 결과 관련 목록을 클릭합니다.

e. 검색 날짜 열에서 검색 날짜를 클릭하여 데이터를 표시합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이메일 검색 결과 기록이 표시됩니다.



이메일 검색이 성공적으로 완료되면 결과를 평가합니다. 이메일에 정정이 필요하다고 판단되면 이제 이메일을 삭제하거나 삭제 승인을 요청할 수 있습니다.

Microsoft Exchange 온라인 서비스의 이메일에 대한 삭제 승인 요청

이메일 검색이 성공적으로 완료되고 일치하는 메시지가 식별되면 Microsoft Exchange Online 서비스에서 보안 인시던트 및 피싱 캠페인과 관련된 모든 의심스러운 이메일을 영구적으로 삭제할 수 있습니다.

시작하기 전에

필요한 역할: sn_si.analyst

시스템은 최근에 성공한 검색 결과에 대해 삭제를 수행합니다.

이 태스크 정보

승인 및 이메일 알림을 사용하는 경우 이메일을 제거하기 전에 승인 그룹에 이메일 삭제 요청을 보냅니다.

받은 모든 메시지와 함께 이메일 검색 결과가 표시됩니다. 피싱 이메일이 성공적으로 삭제되었는지 확인하기 위해 삭제 결과는 연결된 보안 인시던트의 작업 메모에 게시됩니다. 태그 지정을 활성화하면 관련 보안 인시던트에도 보안 태그가 표시됩니다. 이메일이 성공적으로 삭제되지 않으면 작업 메모에도 알림이 표시됩니다.

조직 정책에 따라 피싱 이메일을 삭제하기 전에 승인을 요청해야 할 수 있습니다. 삭제 승인 프로세스에는 삭제할 이메일 수와 잠재적으로 다른 메시지 상세 정보에 대한 액세스 등에 대한 정보가 필요합니다. 삭제 요청을 처리하기 위해 이메일 알림에서 승인자에게는 일치하는 이메일 메시지 수, 전체 메시지 상세 정보에 액세스하기 위한 보안 인시던트 링크, 승인 또는 거부 링크가 제공됩니다. 이 이메일의 링크를 통해 승인자는 이메일 알림에서 삭제 요청을 수락하거나 거부할 수 있습니다. 작업 메모에서 승인 상태가 변경된 시기를 추적하는 타임 스탬프가 있는 전체 감사 추적도 사용할 수 있습니다. 승인 그룹이 할당된 경우 그룹의 사용자 한 명이 전체 그룹에 대한 요청을 처리할 수 있습니다. 승인 그룹의 각 구성원은 요청에 대한 이메일 알림을 받습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

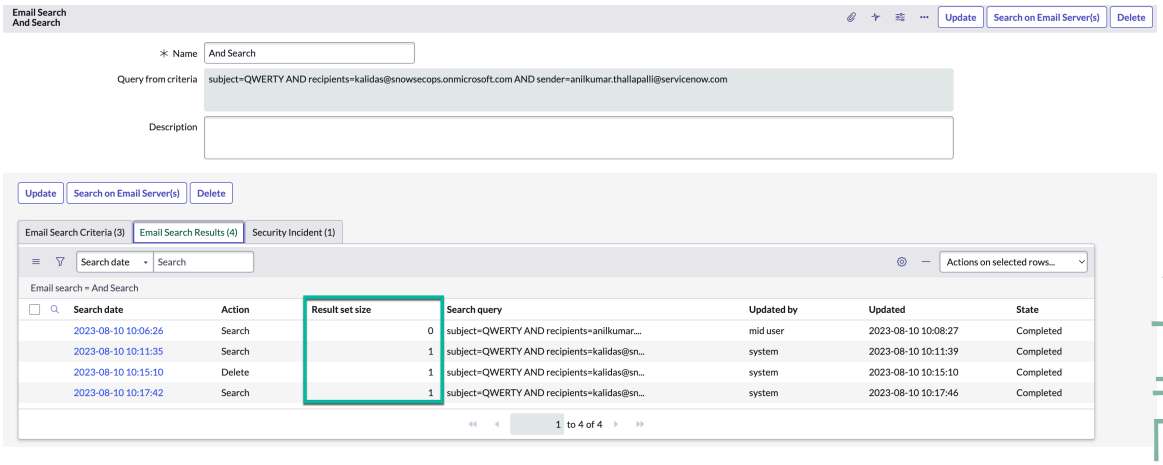
sn_si.analyst 역할을 가진 사용자가 이메일 정정이 필요하다고 판단되는 경우 필요한 단계에 따라 이메일을 삭제합니다. 승인이 활성화된 경우 서비스에서 이메일을 Microsoft Exchange Online 삭제하기 위한 승인을 요청합니다.

프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 > 모든 인시던트 표시.
2. 이메일 검색 관련 목록을 클릭합니다.
3. 이메일 검색 관련 목록을 선택한 상태에서 이메일 검색 열에서 검색 이름을 클릭합니다.
   검색 결과는 이메일 검색 결과 관련 목록에 표시됩니다.

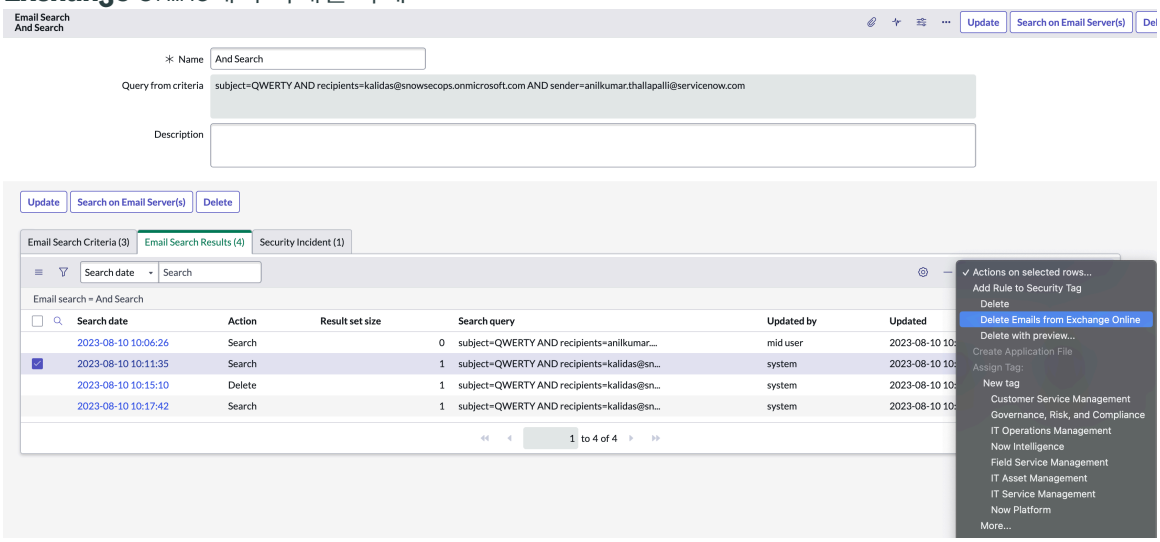
   이 예에서는 이 검색이 검색 기준과 일치하는 이메일을 찾았습니다. 기록에 나열된 검색 작업은 두 가지입니다. 한 검색에는 일치하는 이메일이 없고(0), 다른 검색에는 일치하는 이메일이 하나 있습니다(1).

이메일 검색 결과 세트 크기



4. 검색과 관련된 이메일 항목을 삭제하려면 검색 날짜 열 왼쪽에서 검색 결과 세트의 확인란을 선택합니다.
   목록에서 단일 결과 세트 또는 여러 결과 세트를 선택할 수 있습니다.
5. 삭제할 결과 세트를 선택합니다.

Exchange Online에서 이메일 삭제



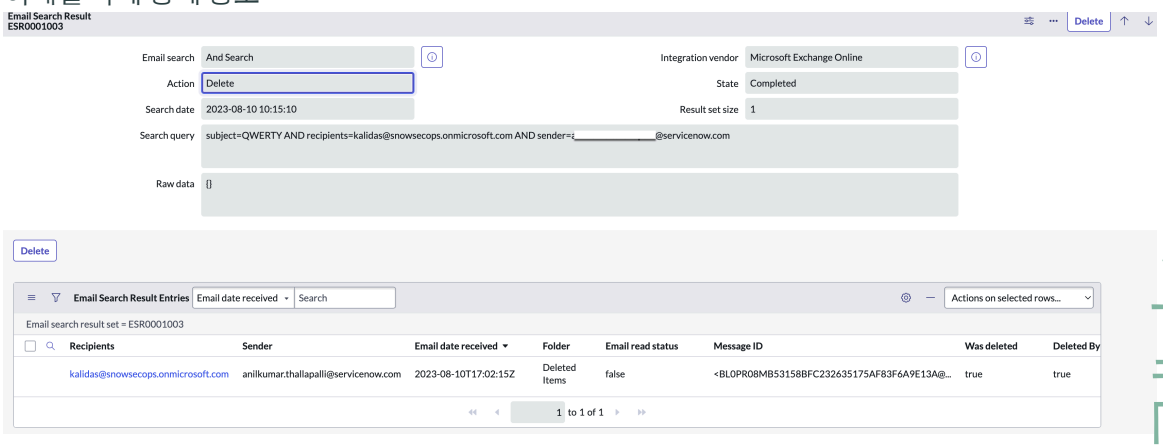
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

6. 전자 메일 검색 결과 관련 목록 아래쪽의 선택한 행에 대한 작업 목록에서 **Exchange** Online에서 전자 메일 삭제를 선택하여 Exchange Online 서버에서 하나 이상의 결과 집합과 연결된 모든 전자 메일 항목을 삭제합니다.
결과 세트에 이메일이 두 개 이상 포함되어 있는 경우 이메일 검색 결과 기록을 열고 개별 이메일을 선택하여 삭제할 필요가 없습니다. 이메일 검색 결과 기록의 삭제됨 열에서 ### 상태인 모든 이메일 항목은 **Exchange** Online에서 이메일 삭제를 선택하면 삭제됩니다.

   결과 세트의 이메일 항목이 이미 삭제된 경우 이메일 검색 결과 기록의 삭제됨 열에 있는 상태가 true입니다. 이러한 항목은 다시 삭제되지 않습니다.

   구성 단계에서 승인 옵션을 사용하지 않도록 설정한 경우 **Exchange** Online에서 이메일 삭제를 선택하면 결과 세트와 연결된 이메일이 삭제됩니다. 결과 집합 자체는 삭제되지 않습니다. 그러나 결과 집합의 삭제된 모든 이메일 항목의 상태는 이메일 검색 결과 기록의 삭제됨 열에서 true 로 업데이트됩니다. 승인 기능에 대한 자세한 내용은 다음 문서를 참조하십시오 Microsoft Exchange Online 통합 구성.

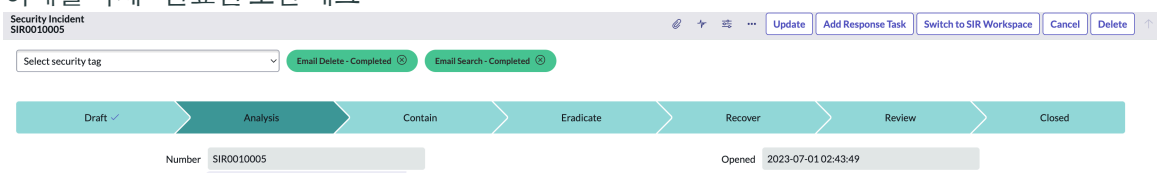
   이메일 삭제 상세 정보



   이러한 전자 메일은 검색을 수행한 테넌트에서 Microsoft Exchange Online 삭제됩니다. 이메일이 성공적으로 삭제되면 작업 메모가 표시됩니다.

   보안 인시던트 기록에 ### ## - ## 됨 보안 태그가 표시됩니다.

   이메일 삭제 - 완료된 보안 태그



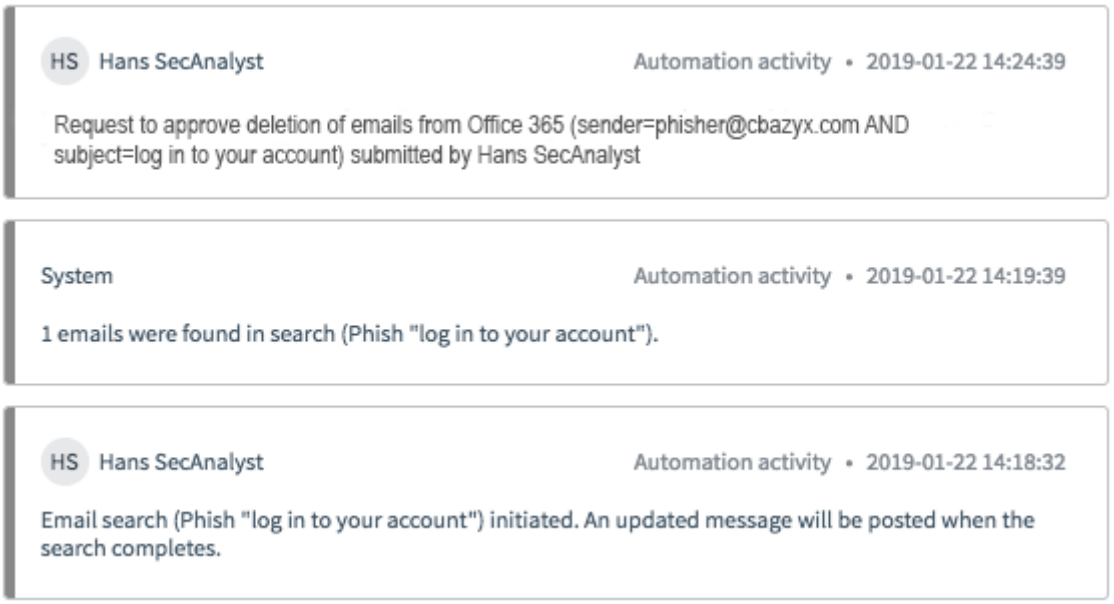
   삭제 요청에 대한 승인이 비활성화된 경우 테넌트에서 Microsoft Exchange Online 이메일을 성공적으로 삭제했습니다.

   구성 단계에서 삭제 요청에 대한 승인이 활성화된 경우 **Exchange** Online에서 이메일 삭제를 선택하면 구성 단계에서 선택한 승인 그룹의 각 구성원에게 이메일 알림이 전송됩니다.

   구성 단계 중에 태그 지정을 사용하도록 설정하면 ### ## - ### 보안 태그가 관련 보안 인시던트 기록에 표시됩니다. 태그 지정에 대한 자세한 내용은 다음 문서를 참조하십시오 Microsoft Exchange Online 통합 구성.

   sn_si.analyst 역할의 사용자(Hans SecAnalyst)가 이메일 삭제 요청을 제출했다는 작업 메모가 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

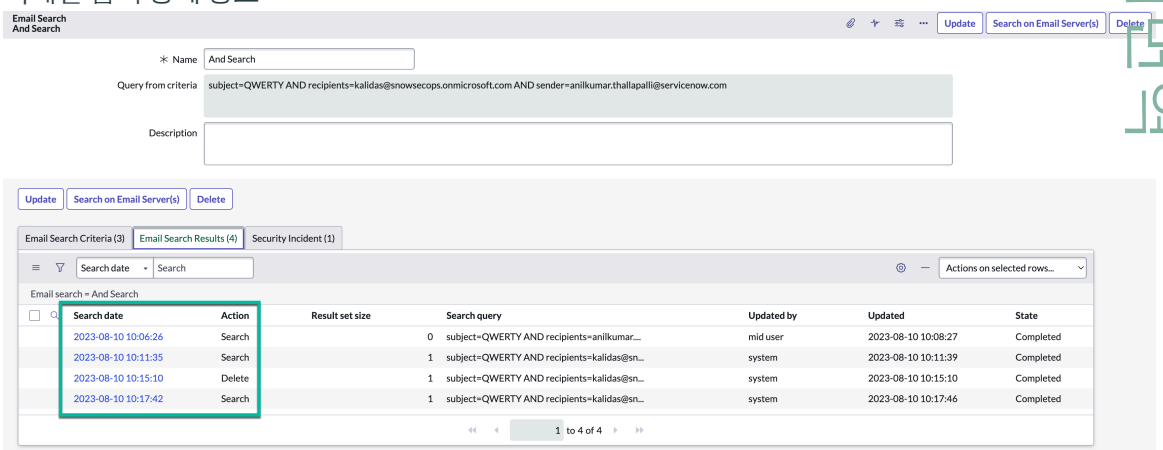


승인이 활성화된 경우 다음 단계는 삭제 요청을 처리하는 것입니다.

7. 또는 검색 기록을 삭제하거나 삭제 요청을 제출하기 전에 검색 기록의 세부 정보 및 개별 이메일 항목을 보려면 다음 단계를 수행합니다.

   a. 이메일 검색 결과 관련 목록을 선택한 상태에서 검색 날짜 열에서 검토하려는 검색 날짜를 클릭합니다.

이메일 검색 상세 정보



이메일에 대한 다음 정보가 표시됩니다.

- 수신자
- 보낸 사람
- 이메일 수신 날짜
- 이메일 읽음 상태(true 또는 false)
- 삭제됨(true 또는 false)

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 통합에 의해 삭제됨(true 또는 false)

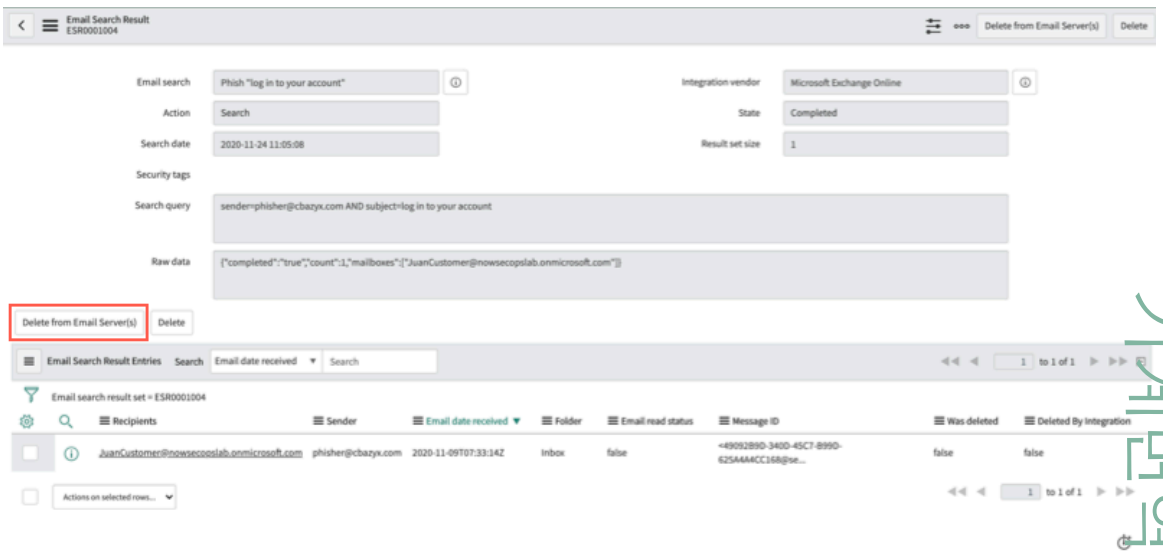
  주:

  분석가가 이메일 서버에서 삭제를 시작할 때 이메일이 삭제되면 값이 true로 설정됩니다.

  작업 메모는 통합 및 사용자가 삭제한 기록을 포함하여 삭제된 총 기록 수로 업데이트됩니다.

b. 데이터를 검토한 후 모든 이메일을 삭제하거나 모든 이메일 삭제 요청을 보내려면 이메일 서버에서 삭제를 클릭합니다.

앞의 예에서 설명한 것처럼 검색 결과 기록에 나열된 이메일이 두 개 이상 있는 경우 개별 이메일을 선택하여 제거할 필요가 없습니다. 삭제 요청은 최신 검색 결과에서 삭제됨 열에 false가 표시된 경우 검색과 관련된 모든 이메일을 제거합니다.



승인이 활성화된 경우 이메일 삭제 요청을 성공적으로 제출한 것입니다. 보안 태그와 작업 메모는 이전 예시에 설명한 대로 관련 보안 인시던트 기록에 표시됩니다. 승인자로서 다음 단계는 삭제 요청을 처리하는 것입니다.

통합에 **Microsoft Exchange Online** 대한 삭제 이메일 요청 승인

인스턴스에서 승인 옵션이 활성화된 ServiceNow AI Platform 경우, 이메일 삭제 요청이 이메일을 통해 승인 그룹의 각 구성원에게 전송됩니다. 구성 단계에서 승인 그룹을 선택합니다. 승인은 조직에 이메일 삭제에 대한 추가 제어 수준을 제공합니다.

시작하기 전에
Exchange Online 전자 메일 검색 및 삭제 구성 설정 양식의 추가 설정 탭에서 승인 옵션을 선택했는지 확인합니다.

승인 요청에 대해 인스턴스에서 이메일 이메일 전송 사용설정 및 이메일 수신 사용 옵션을 ServiceNow AI Platform 활성화했는지 확인합니다.

sn_si.analyst 역할을 가진 사용자가 삭제 이메일 요청을 제출하면 기본적으로 이러한 요청은 이메일을 통해 sn_si.admin으로 전송됩니다. 승인 그룹을 생성한 경우 그룹의 각 구성원이 알림을 받습니다. 승인자는 이메일 알림에서 직접 이메일 삭제 요청을 처리할 수 있습니다. 또는 인스턴스의

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이메일 검색 결과 기록 ServiceNow AI Platform 에서 요청을 처리할 수 있습니다. 이 항목에서는 두 가지 승인 방법을 보여줍니다.

다음 정보는 이메일 알림의 요청을 설명합니다.

이메일 검색 결과 기록 번호

감사 추적의 일부로 검색 기록 ServiceNow AI Platform 에 할당된 고유 번호입니다.

요청을 제출한 분석가의 이름

감사 추적의 일부로 요청을 제출한 사람의 이름입니다.

보안 인시던트에 연결

피싱 이벤트와 관련된 보안 인시던트에 대한 링크입니다. 이메일에서 직접 작업 메모, 이메일 검색 및 이메일 검색 결과를 사용하여 보안 인시던트를 봅니다.

링크 승인 또는 거부

이메일 알림에서 요청을 승인하거나 거부하는 링크입니다. 두 링크 중 하나를 클릭하면 시스템이 관련 워크플로우를 자동으로 시작하고 작업 메모가 보안 인시던트 기록에 게시됩니다.

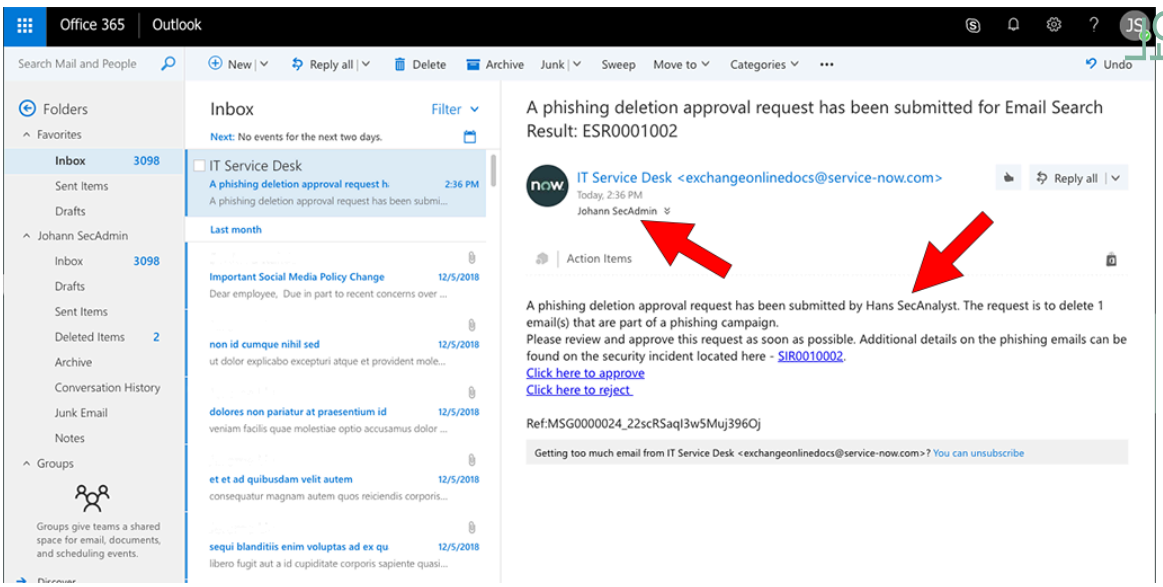
필요한 역할: sn_si.admin 또는 할당된 승인 그룹의 모든 구성원.

프로시저

1. 이메일 알림에서 삭제 요청을 처리하려면 다음 단계를 수행합니다.

a. 승인자는 사용자 계정에서 구성한 ServiceNow AI Platform 이메일 계정에서 알림 이메일을 찾습니다.

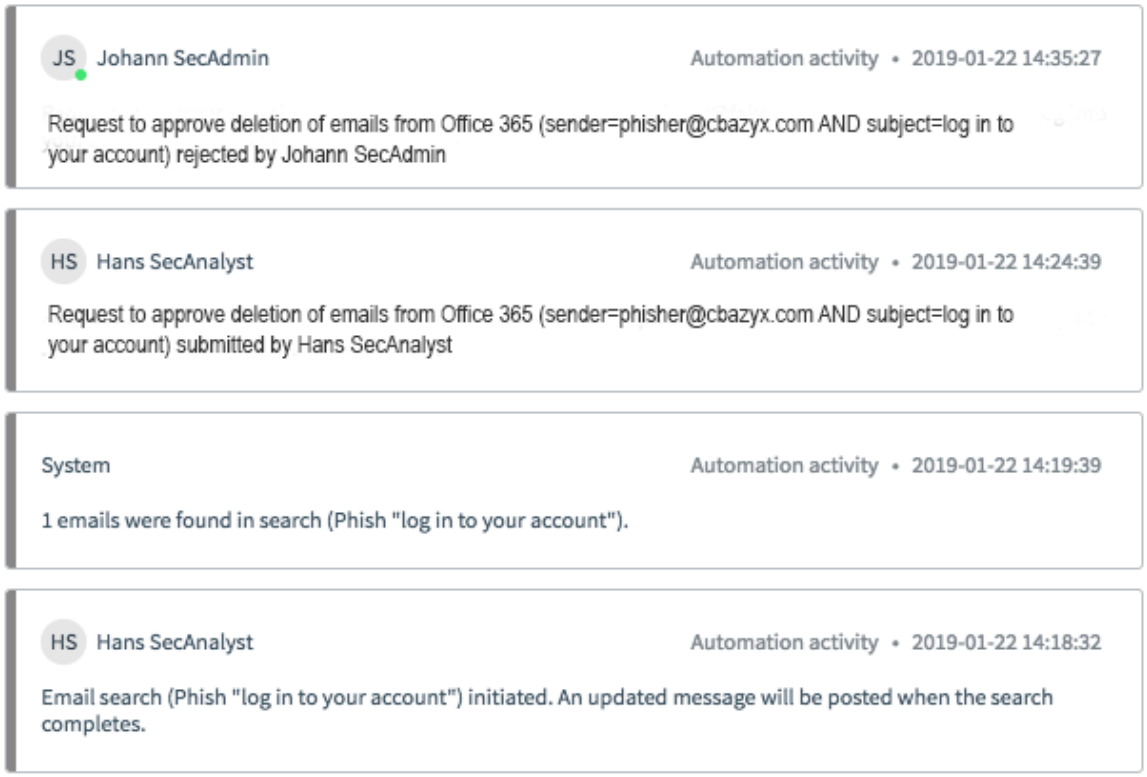
이 예시에서는 sn_si.analyst 역할의 사용자(Hans SecAnalyst)가 이메일 하나를 삭제해 달라는 요청을 제출합니다. Johann SecAdmin은 승인 그룹의 구성원입니다.



b. 이메일 알림에서 계속하려면 하나의 옵션을 선택하십시오.

다음 이미지는 이 예시와 관련된 보안 인시던트 기록의 작업 메모에서 생성된 감사 추적의 예를 보여줍니다. 승인자가 이메일 알림에서 요청을 거부하면 요청을 거부한 사람이 작업 메모를 게시합니다. Johann SecAdmin이 이 요청을 거부합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



ServiceNow AI Platform 요청을 거부한 사람(Johann SecAdmin)의 경우 셀프 서비스 > 내 승인, ### 이 상태 열에 표시됩니다.

승인 그룹의 단일 구성원이 요청을 거부한 후 sn_si.analyst 역할을 가진 사용자로서 해당 이메일을 삭제해야 한다고 판단되면 해당 이메일을 삭제하기 위한 새 요청을 제출해야 합니다.

이 예에서는 요청이 거부된 후 sn_si.analyst 역할을 가진 사용자가 새 요청을 제출합니다.

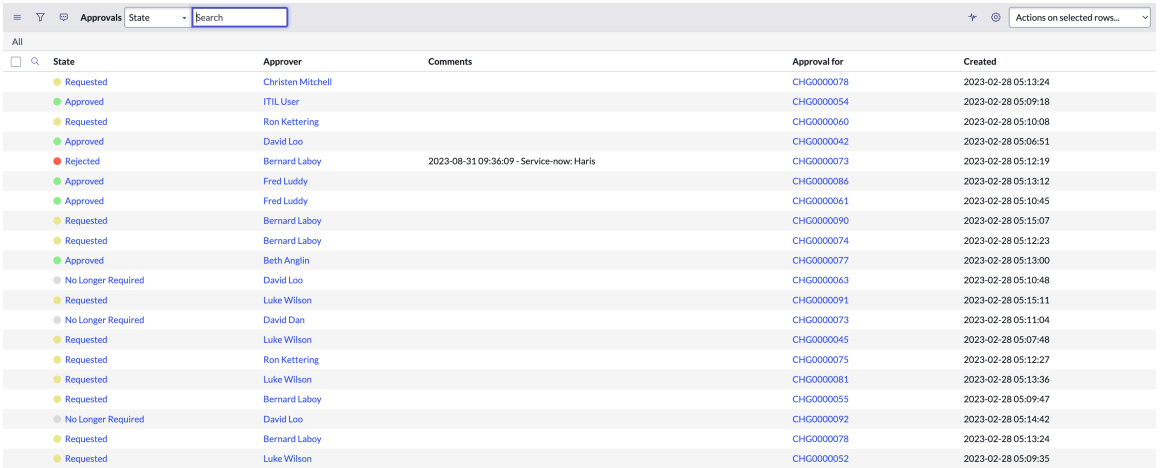
승인 그룹의 또 다른 구성원인 John Approver는 앞의 예시에 표시된 것과 비슷한 이메일을 받습니다. 승인자 John도 이 요청을 처리할 수 있습니다.

2. 또는 승인자가 다음으로 이동할 수 있습니다. 셀프 서비스 > 내 승인 ServiceNow AI Platform 인스턴스에서 삭제 요청을 보고 처리합니다.
내 승인에서 요청을 처리하려면 다음 단계를 따르십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 다음으로 이동 셀프 서비스 > 내 승인.

내 승인 목록



Approvals | State | Search | Actions on selected rows...

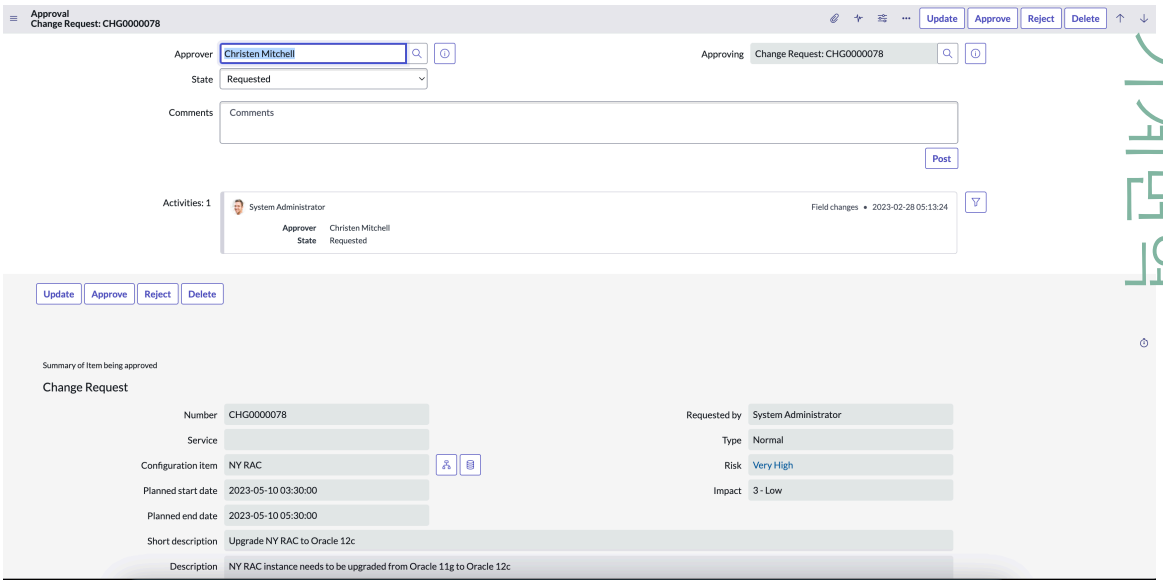
All

State	Approver	Comments	Approval for	Created
Requested	Christen Mitchell		CHG0000078	2023-02-28 05:13:24
Approved	ITIL User		CHG0000054	2023-02-28 05:09:18
Requested	Ron Kettering		CHG0000060	2023-02-28 05:10:08
Approved	David Loo		CHG0000042	2023-02-28 05:06:51
Rejected	Bernard Laboy	2023-08-31 09:36:09 - Service-now: Haris	CHG0000073	2023-02-28 05:12:19
Approved	Fred Luddy		CHG0000086	2023-02-28 05:13:12
Approved	Fred Luddy		CHG0000061	2023-02-28 05:10:45
Requested	Bernard Laboy		CHG0000090	2023-02-28 05:15:07
Requested	Bernard Laboy		CHG0000074	2023-02-28 05:12:23
Approved	Beth Anglin		CHG0000077	2023-02-28 05:13:00
No Longer Required	David Loo		CHG0000063	2023-02-28 05:10:48
Requested	Luke Wilson		CHG0000091	2023-02-28 05:15:11
No Longer Required	David Dan		CHG0000073	2023-02-28 05:11:04
Requested	Luke Wilson		CHG0000045	2023-02-28 05:07:48
Requested	Ron Kettering		CHG0000075	2023-02-28 05:12:27
Requested	Luke Wilson		CHG0000081	2023-02-28 05:13:36
Requested	Bernard Laboy		CHG0000055	2023-02-28 05:09:47
No Longer Required	David Loo		CHG0000092	2023-02-28 05:14:42
Requested	Bernard Laboy		CHG0000078	2023-02-28 05:13:24
Requested	Luke Wilson		CHG0000052	2023-02-28 05:09:35

b. 상태 열에서 요청된 항목을 클릭합니다.

표시되는 승인 기록에는 검색, 검색 요청 및 검색 결과에 대한 데이터가 나열됩니다.

승인 세부 정보



Approval
Change Request: CHG0000078

Update | Approve | Reject | Delete

Approver: Christen Mitchell
State: Requested
Approving: Change Request: CHG0000078
Comments
Post
Activities: 1
System Administrator — Field changes • 2023-02-28 05:13:24
Approver: Christen Mitchell
State: Requested

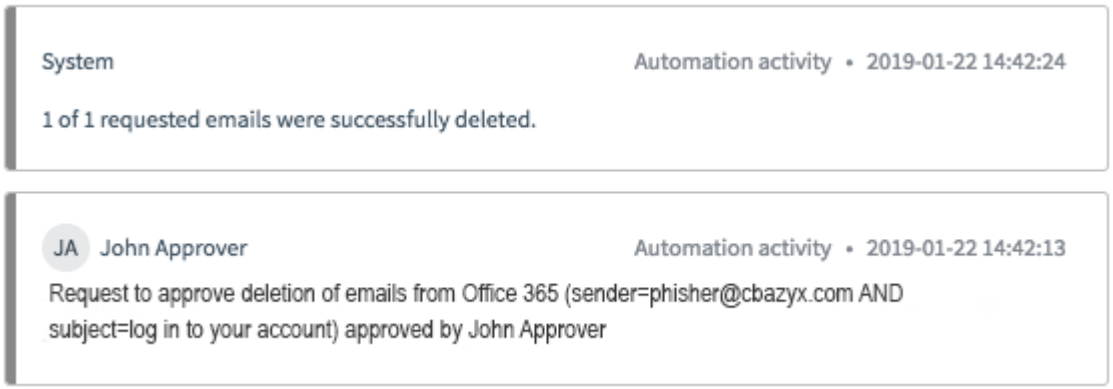
Update | Approve | Reject | Delete

Summary of Item being approved
Change Request

Number	CHG0000078	Requested by	System Administrator
Service		Type	Normal
Configuration item	NY RAC	Risk	Very High
Planned start date	2023-05-10 03:30:00	Impact	3 - Low
Planned end date	2023-05-10 05:30:00		
Short description	Upgrade NY RAC to Oracle 12c		
Description	NY RAC instance needs to be upgraded from Oracle 11g to Oracle 12c		

c. 이 기록에서 승인을 클릭하여 요청을 승인합니다.
요청이 승인되면 시스템은 이메일을 제거하기 위해 삭제 워크플로우를 시작합니다. 다음 이미지는 이 예시와 관련된 보안 인시던트 기록의 작업 메모에서 생성된 감사 추적의 예를 보여줍니다. 이 삭제 요청이 다시 제출되면 승인됩니다. 요청을 승인하는 데 사용되는 방법에 관계없이 성공적으로 삭제된 이메일 수는 작업 메모에 게시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



이메일이 성공적으로 삭제된 후 관련 보안 인시던트 기록에서 태그 지정을 사용하는 경우 ### ## - ### 태그가 ### ## - ### 태그를 대체합니다.

인 셀프 서비스 > 내 승인 승인자(John Approver)의 경우 ### ## 됨에서 ###으로 변경됩니다.

인 셀프 서비스 > 내 승인 승인 그룹의 다른 구성원(예: Johann SecAdmin)의 경우, 요청이 승인되면 상태가 # ## #### ## 으로 변경됩니다.

3. 또는 관련 보안 인시던트 기록의 이메일 검색 결과 기록에서 이메일이 삭제되었는지 확인하려면 다음 단계를 따르십시오.

a. 다음으로 이동 보안 인시던트 > 모든 인시던트 표시 피싱 관련 보안 인시던트를 찾습니다.
기록 하단에 관련 목록이 표시됩니다.

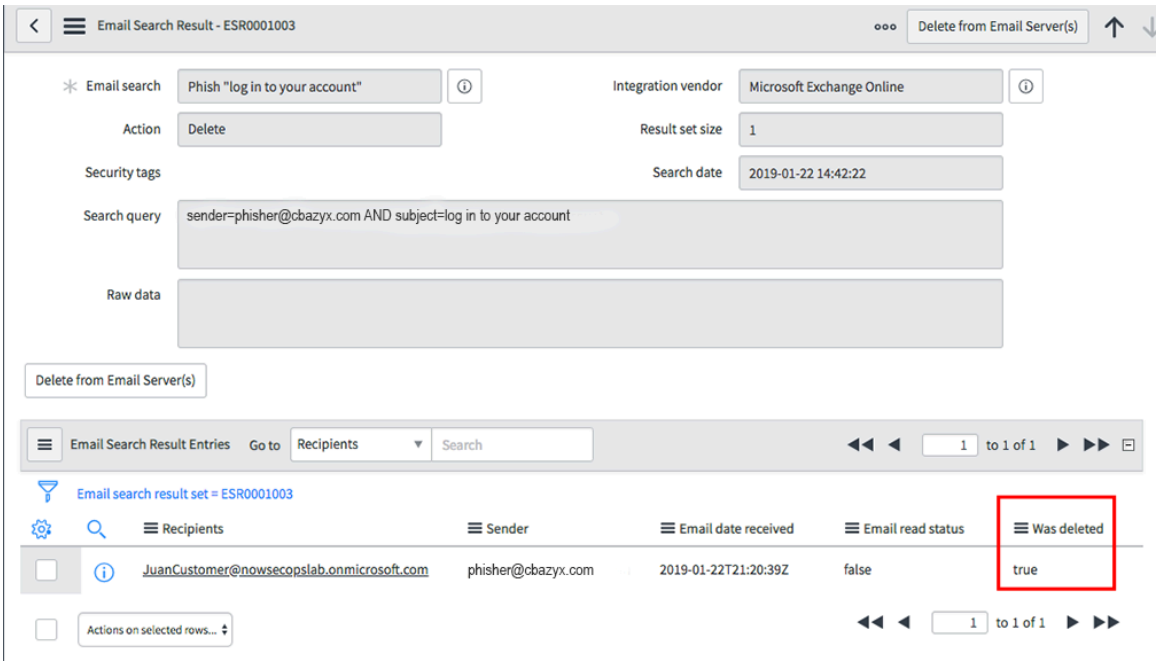
b. 이메일 검색 관련 목록을 클릭합니다.

c. 전자 메일 검색 열에서 검색 이름을 클릭합니다(##: "### ###").
이메일 검색 기록이 표시됩니다. 이메일 검색 관련 목록이 표시되지 않으면 모든 관련 목록 표시링크를 클릭합니다.

d. 이메일 검색 결과 관련 목록을 클릭합니다.
검색 날짜 열에서 이메일 검색 및 삭제 작업이 해당 날짜와 함께 표시됩니다.

e. 검색 날짜 열에서 삭제 작업에 해당하는 항목을 클릭합니다.
표시되는 이메일 검색 결과 기록에서 삭제됨 열 상태에는 이메일이 삭제됨(true)이 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



이메일 알림과 승인 기록 모두에서 이메일 삭제 요청을 승인하고 이메일이 삭제되었음을 확인했습니다. 이메일 검색 결과 기록을 찾는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 이메일 검색 기준 정의 및 서비스 검색 Microsoft Exchange Online 요청.

서비스에서 삭제된 이메일 **Microsoft Exchange Online** 복구

(선택 사항) 인시던트 정정 시 이 통합의 워크플로우에 의해 삭제된 이메일을 복구해야 하는 경우, Microsoft Exchange 관리자는 삭제된 이메일을 복구할 수 있습니다.

시작하기 전에
이 통합으로 이메일을 삭제하는 방법에 대한 자세한 내용은 문서를 참조하십시오 Microsoft Exchange Online 통합 구성.

사용자 사서함에서 삭제된 항목을 복구하는 방법에 대한 정보를 포함하여 Office 365 제품의 관리 역할에 Microsoft 대한 자세한 내용은 Exchange Online 관리자 역할 정보를 참조하세요.

필요한 역할: admin, Microsoft Exchange 관리자

이 태스크 정보
구성 단계 중에 추가 설정 탭에서 삭제된 이메일 복구 옵션을 선택하면 테넌트에서 삭제된 이메일을 복구할 수 있습니다 Microsoft Exchange Online . 이 통합의 삭제 워크플로우를 사용하여 삭제된 전자 메일은 서비스의 사용자 Microsoft Exchange Online 사서함에 있는 복구 가능한 항목 폴더의 지운 편지함 하위 폴더에 배치됩니다. 사용자가 지운 편지함 폴더를 볼 수 있도록 테넌트에서 Microsoft Exchange Online 사용자의 계정이 구성된 경우 사용자는 웹에서 Outlook 서비스를 사용하여 Microsoft 이러한 전자 메일을 복구할 수 있습니다. Microsoft Exchange Online 또는 관리자는 사용자의 지운 편지함 폴더에서 삭제된 이메일을 복구할 수 있습니다. 자세한 내용은 Outlook Web App에서 삭제된 항목 또는 전자 메일 복구를 참조하세요.

필요한 역할: Microsoft Exchange Online 삭제된 이메일을 복구하기 위한 관리자 또는 Microsoft 전역 관리자.

필요한 역할: sn_si.admin 비활성화 ServiceNow AI Platform 된 이메일 복구 옵션을 활성화합니다.

필요한 역할: 이메일 검색을 완료하고 복구 전에 이메일이 성공적으로 삭제되었는지 확인하기 위한 sn_si.analyst ServiceNow AI Platform 입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

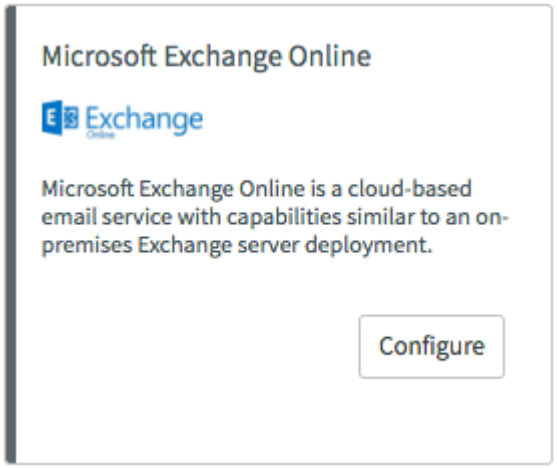
프로시저

이메일 복구 옵션을 활성화하려면 다음 단계를 따르세요.

a. 다음으로 이동 보안 운영 〉 통합 〉 구성.

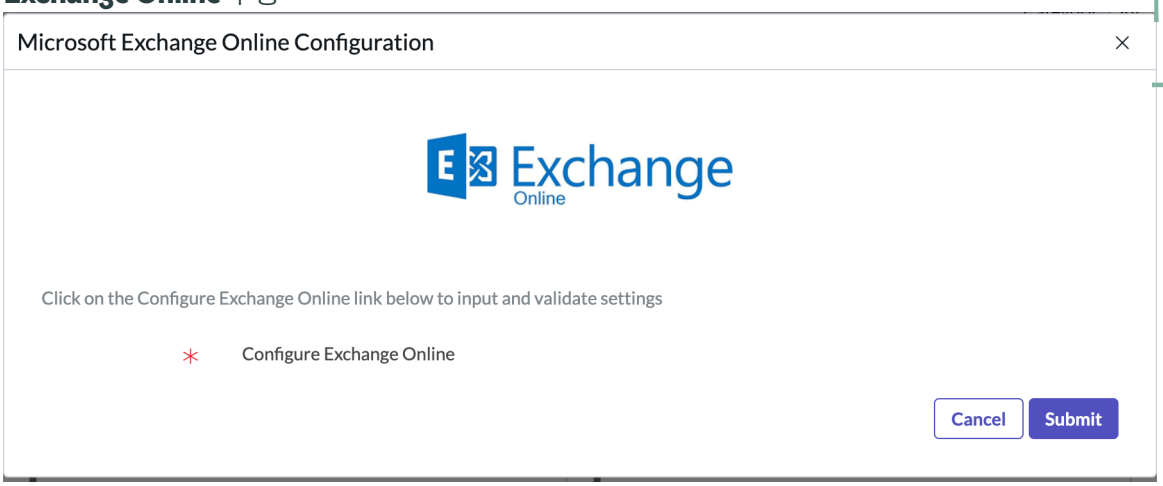
b. 타일을 Microsoft Exchange Online 찾습니다.

c. 구성을 클릭합니다.



d. Microsoft Exchange Online 표시되는 구성 대화 상자에서 **Exchange Online** 구성을 클릭합니다.

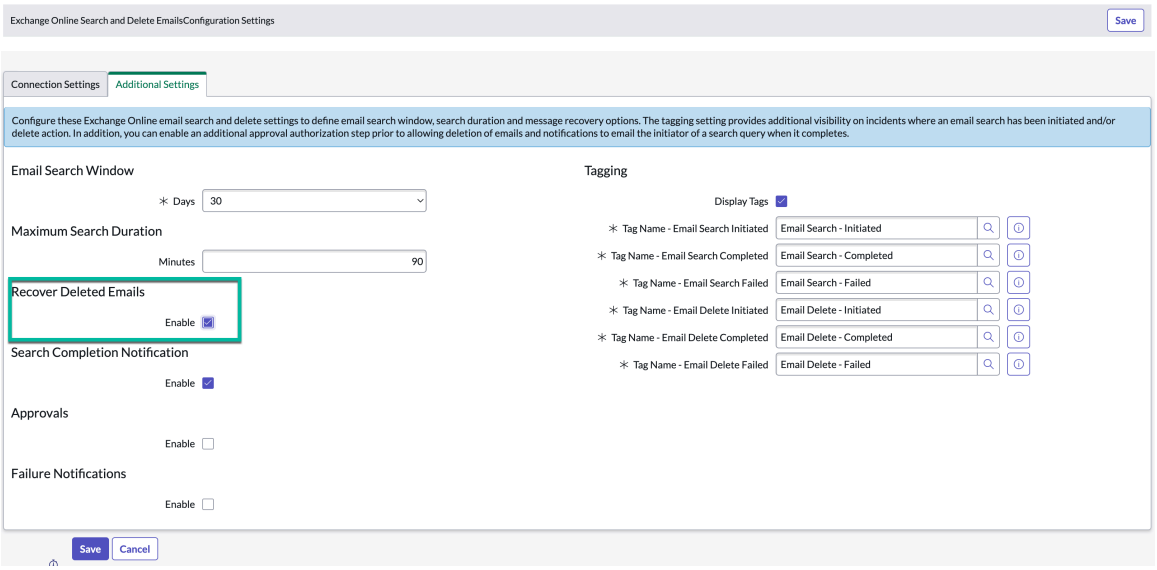
Exchange Online 구성



e. ## # ## ## ##의 ## ## 탭에서 사용 확인란을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

삭제된 이메일 복구



f. 다른 설정을 확인하고 제출을 클릭합니다.

g. 복구하려는 이메일 메시지에 대해 이메일 메시지 검색 및 삭제가 성공적으로 완료되었는지 확인하려면 이메일 검색 및 삭제 워크플로우를 로깅한 보안 인시던트로 이동합니다.

h. 작업 메모를 찾아 시스템에서 메시지를 성공적으로 삭제했는지 확인합니다.

i. Microsoft Exchange Online 관리자 또는 전역 관리자로 Office 365 계정에 로그인합니다Microsoft.

j. 설명서 웹 사이트의 Outlook Web App Microsoft 에서 삭제된 항목 또는 전자 메일 복구에 설명된 단계를 따릅니다.

통합에 **Microsoft Exchange Online** 대한 보안 태그 편집

통합을 위해 인스턴스에 있는 ServiceNow AI Platform# 보안 태그의 이름과 색상을 편집할 수 있습니다 Microsoft Exchange Online . 이러한 보안 태그를 사용하면 이메일 검색이 완료되거나 실패하는 시기를 빠르게 식별할 수 있습니다. 또한 이메일 삭제 요청이 시작되는 시기와 이메일 항목이 성공적으로 삭제되는 시기도 식별합니다.

시작하기 전에

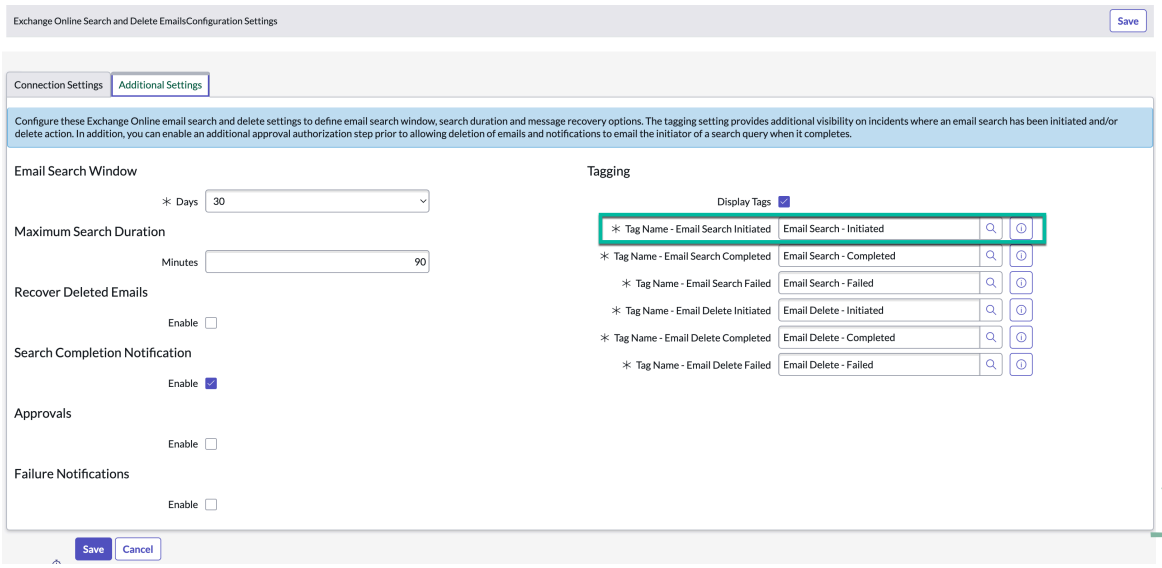
기본적으로 구성 단계 중에 태그 표시 옵션을 선택하면 인스턴스에서 보안 태그가 활성화됩니다ServiceNow AI Platform#. 태그 색상과 이름을 편집하고 보안 태그 그룹에 태그를 할당하여 인스턴스에서 구성할 ServiceNow AI Platform# 수 있습니다. 예를 들어, 기능의 시작 태그는 한 가지 색상이 되고 완성 태그는 인스턴스에서 활성화된 다른 보안 태그와 일치하도록 태그의 색상을 변경할 수 있습니다 ServiceNow AI Platform# . 이러한 다양한 색상은 워크플로우가 시작되고 성공적으로 완료되는 시기를 빠르게 식별하는 데 도움이 됩니다. 통합에 대한 태그 지정을 비활성화하지 않고 특정 태그가 필요하지 않다고 결정한 경우 태그 기록에서 단일 태그를 비활성화할 수도 있습니다. 사용하지 않도록 설정하면 이 태그는 관련 보안 인시던트에 더 이상 표시되지 않습니다. 보안 태그 그룹 및 태그를 설정하는 방법에 대한 자세한 내용은 ServiceNow 제품 설명서 웹 사이트에서 보안 태그 그룹 및 태그 설정을 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필요한 역할: sn_si.admin

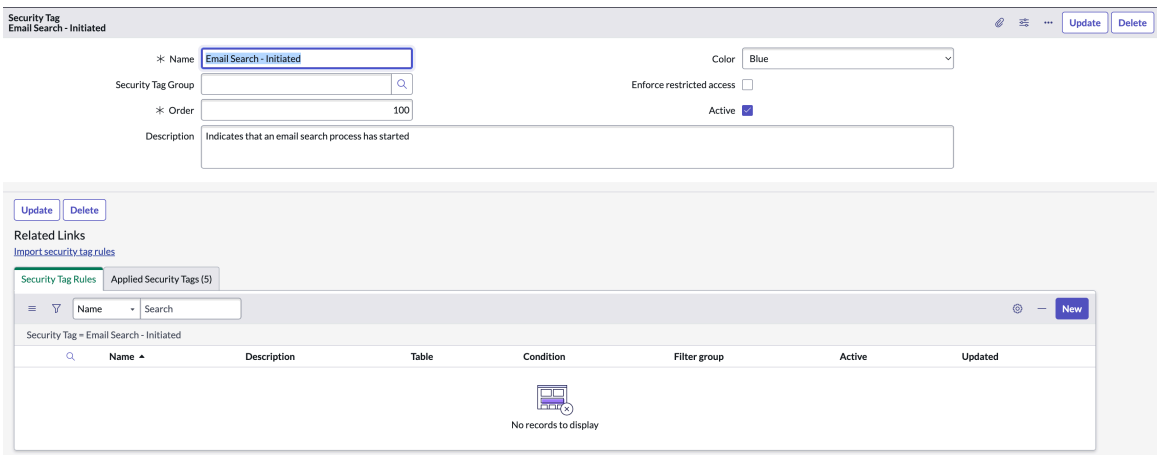
프로시저

1. 다음으로 이동 모두 〉 보안 운영 〉 통합 〉 **Exchange Online** 설정.
2. 추가 설정 탭을 클릭하여 선택합니다.
3. 표시되는 탭에서 태그 표시 옵션의 선택이 취소된 경우 선택하여 태그 이름을 표시합니다.
4. 태그 이름이 표시되면 태그 오른쪽에 있는 정보 아이콘을 클릭합니다.



5. 표시되는 Security Tag(보안 태그) 대화 상자에서 **Open** Record(기록 열기)를 클릭합니다.
6. 표시되는 기록에서 필드를 편집합니다.

7. 변경 사항을 저장하려면 업데이트를 클릭합니다.



이제 보안 태그에 대한 태그 기록을 성공적으로 편집했습니다.

Microsoft Exchange On-Premises 통합

온프레미스 통합은 Microsoft Exchange 보안 분석가가 온프레미스 인스턴스에서 피싱 및 스피어 피싱 이메일 위협을 억제하고 근절할 수 있는 도구를 제공합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

탐색	설정
보안 인시던트 응답 통합	Microsoft Exchange On-Premises 통합 시작하기

사용	개발
피싱 이메일 검색 및 삭제	• ServiceNow 보안 운영 통합 개발 가이드라인 • 통합 작성을 위한 팁 • 개발자 교육 • 개발자 설명서 • 애플리케이션과 함께 설치되는 구성요소 찾기

문제 해결 및 도움받기

- 통합 문제 해결
- 보안 운영 커뮤니티에서 질문 또는 답변하기
- 알려진 오류 포털에서 알려진 오류 문서 검색

- 연락처 고객 서비스 및 지원

Microsoft Exchange On-Premises 통합 시작하기

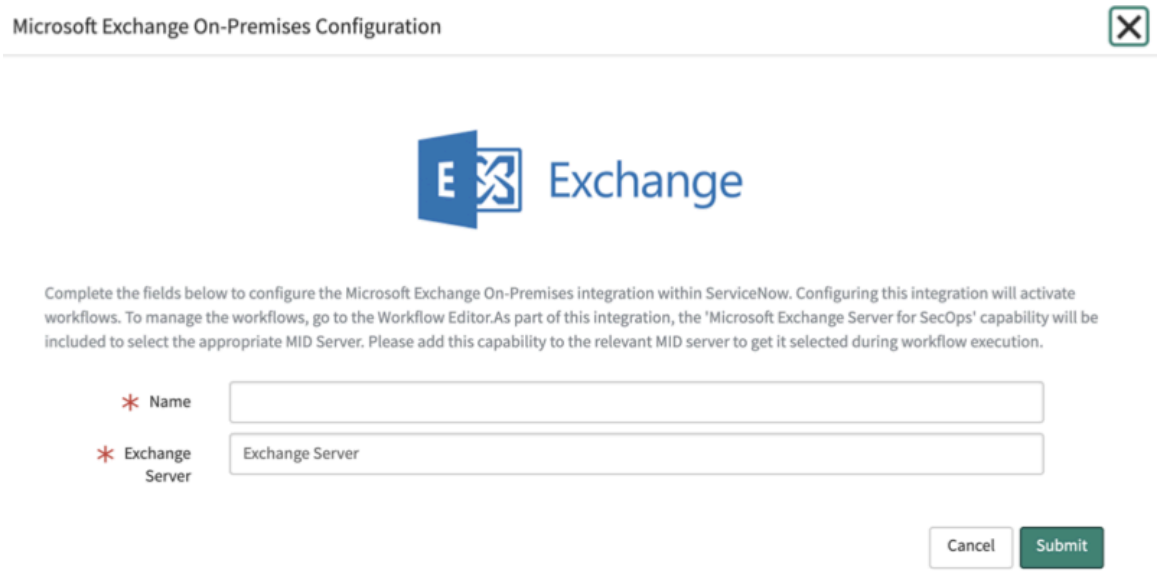
온프레미스 통합은 Microsoft Exchange 보안 분석가가 온프레미스 인스턴스에서 피싱 및 스피어 피싱 이메일 위협을 억제하고 정정할 수 있는 도구를 제공합니다. 온 프레미스 통합을 사용하려면 Microsoft Exchange 먼저 에서 ServiceNow Store 다운로드하여 적절한 Exchange 및 MID 서버를 식별해야 합니다.

시작하기 전에
필요한 역할: sn_si_admin

프로시저

1. 에서 통합을 다운로드합니다. ServiceNow Store.
2. 설치 OS가 완료되면 보안 운영 〉 통합 〉 통합 구성.
   사용 가능한 보안 통합은 일련의 카드로 표시됩니다.
3. 온프레미스 카드에서 Microsoft Exchange새로 만들기를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 필요에 따라, 필드를 채웁니다.

필드	설명
이름	이 구성의 이름입니다.
Exchange 서버	사용할 Exchange 서버를 지정합니다.

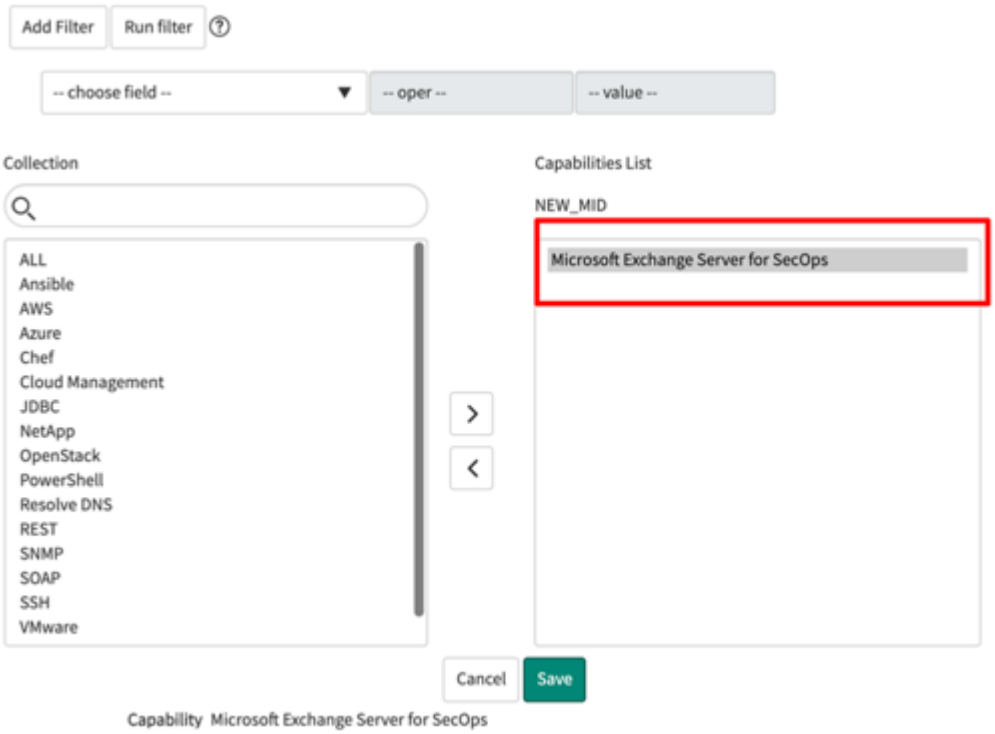
> 주:
> 이 통합을 구성하면 플로우가 활성화됩니다. 플로우를 관리하려면 워크플로우 스튜디오/플로우 디자이너로 이동합니다.

5. 제출을 클릭합니다.
   통합 구성 카드가 표시됩니다.
6. 새 구성 카드를 볼 때 구성 또는 삭제를 클릭하여 구성을 변경하거나 삭제할 수 있습니다.
7. 통합 구성 카드의 원래 목록으로 돌아가려면 구성 표시 드롭다운 목록에서 아니요를 선택합니다.
8. 다음으로 이동 오케스트레이션 〉 **MID** 서버.
9. 기록을 열고 Exchange 서버에 연결할 수 있는 MID 서버의 상태와 해당 상태 옵션이 작동 중으로 설정되어 있고 확인됨 옵션이 예로 설정되어 있는지 확인합니다.
10. MID 서버 역량 추가하기:
    - 기능을 추가할 해당 MID 서버를 선택합니다.
    - 기능 관련 목록을 클릭하고 편집을 클릭합니다.

MID 서버 역량

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 모두 제거하고 SecOps용 **Microsoft Exchange** Server를 추가합니다.



- 관련 목록 섹션에서 **IP** 범위를 선택하고 값을 모두 또는 원하는 값으로 설정합니다.
- 관련 목록 섹션에서 지원되는 애플리케이션을 선택하고 값을 모두 또는 오케스트레이션으로 설정합니다.
- 기록을 저장합니다.

11. 연결 및 자격 증명을 확인합니다.
12. 자격 증명이 확인되면 ServiceNow 인스턴스의 구성이 완료되고 이 통합을 사용하여 이메일 검색 및 삭제 작업을 수행할 준비가 됩니다.

Microsoft Exchange - 이메일 검색 및 삭제 플로우 수행

Microsoft Exchange - 이메일 검색 및 삭제 수행 플로우가 실행되면 제공된 검색 쿼리를 사용하여 Exchange 서버를 검색하고 상세 정보를 온 프레미스 인스턴스에 반환합니다.

시작하기 전에
필요한 역할: sn_si.analyst

이 태스크 정보
Microsoft Exchange - 이메일 검색 및 삭제 수행 플로우는 이메일 검색이 설정되고 이메일 서버에서 삭제 또는 이메일 서버에서 검색 버튼을 누르면 실행됩니다.

이 통합과 관련된 작업은 여기에 설명되어 있습니다. 다른 작업에 대한 자세한 내용은 다음 문서를 참조하십시오 일반 Security Operations 통합 플로우 및 오케스트레이션 활동.

플로우 작업에는 다음이 포함됩니다.

- 준수 검색 작업 작성
- 준수 검색 상태 확인 작업

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

준수 검색 미리보기 작업 작성

준수 검색 미리 보기 만들기 작업은 Exchange 서버에서 만들어진 준수 검색에 대해 미리 보기 유형의 새 준수 검색 작업을 만듭니다.

입력 변수

입력 변수는 작업의 초기 동작을 결정합니다.

변수	설명
targetId	Exchange 서버가 있는 필수 대상 호스트 식별자 필드입니다.
searchName	Exchange 서버에서 작성된 준수 검색의 필수 이름입니다.

종료 조건

이 작업에 대한 가능한 종료 조건은 다음과 같습니다.

종료 조건

변수	설명
완료	준수 검색 작업이 성공적으로 생성되면
작업 생성 오류	Exchange 서버의 예외로 인해 준수 검색 작업을 만들지 못한 경우.
오류	플로우 작업에서 예외가 발생한 경우.

미리 보기 작업 상태 확인

미리 보기 작업 상태는 미리 보기 유형의 준수 검색 작업의 상태를 확인하고 수신자, 보낸 사람, 제목, 받은 이메일 날짜 등 찾은 이메일의 미리 보기 정보를 반환합니다.

입력 변수

입력 변수는 활동의 초기 동작을 결정합니다.

변수	설명
targetId	Exchange 서버가 있는 필수 대상 호스트 식별자 필드입니다.
searchName	Exchange 서버에서 작성된 준수 검색의 필수 이름입니다.

출력 변수

출력 변수에는 후속 작업에서 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
response	준수 검색 작업의 상태와 준수 검색의 일부로 검색된 이메일의 미리 보기 정보를 포함합니다.

종료 조건

이 작업에 대한 가능한 종료 조건은 다음과 같습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

종료 조건

변수	설명
미리 보기 진행 중	준수 검색 작업의 상태가 진행 중인 경우.
메일을 찾을 수 없음	준수 검색 작업의 상태가 완료되고 준수 검색의 일부로 이메일을 찾을 수 없는 경우.
미리 보기 완료	준수 검색 작업의 상태가 완료되고 준수 검색의 일부로 이메일이 발견되는 경우
상태 확인 중 오류 발생	Exchange 서버의 예외로 인해 상태 확인에 실패한 경우.
오류	워크플로우 활동에서 예외가 발생한 경우.

준수 검색 삭제 작업 작성

준수 검색 삭제 만들기 작업은 만들어진 준수 검색에 대해 Exchange 서버에서 제거 유형의 새 준수 검색 작업을 만듭니다.

입력 변수

입력 변수는 작업의 초기 동작을 결정합니다.

변수	설명
targetId	Exchange 서버가 있는 필수 대상 호스트 식별자 필드입니다.
searchName	Exchange 서버에서 작성된 준수 검색의 필수 이름입니다.

종료 조건

이 작업에 대한 가능한 종료 조건은 다음과 같습니다.

종료 조건

변수	설명
완료	준수 검색 작업이 성공적으로 생성되면
작업 생성 오류	Exchange 서버의 예외로 인해 준수 검색 작업을 만들지 못한 경우.
오류	플로우 작업에서 예외가 발생한 경우.

삭제 작업 상태 확인

삭제 확인 작업 상태는 제거 유형의 준수 검색 작업의 상태를 확인하고 준수 검색의 일부로 검색된 이메일에 대해 Exchange 서버에서 일시 삭제 작업을 수행합니다.

입력 변수

입력 변수는 작업의 초기 동작을 결정합니다.

변수	설명
targetId	Exchange 서버가 있는 필수 대상 호스트 식별자 필드입니다.
searchName	Exchange 서버에서 작성된 준수 검색의 필수 이름입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

출력 변수

출력 변수에는 후속 작업에서 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
response	준수 검색 작업의 일부로 발견된 준수 검색 작업의 상태와 삭제된 이메일 수를 포함합니다.

종료 조건

이 작업에 대한 가능한 종료 조건은 다음과 같습니다.

종료 조건

변수	설명
삭제 진행 중	준수 검색 작업의 상태가 진행 중인 경우.
메일을 찾을 수 없음	준수 검색 작업의 상태가 완료되고 준수 검색의 일부로 이메일이 삭제되지 않는 경우.
삭제 완료	준수 검색 작업의 상태가 완료되고 준수 검색의 일부로 이메일이 삭제되는 경우
상태 확인 중 오류 발생	Exchange 서버의 예외로 인해 상태 확인에 실패한 경우.
오류	플로우 작업에서 예외가 발생한 경우.

준수 검색 작업 제거

준수 검색 제거 작업은 Exchange 서버에서 작성된 준수 검색을 제거합니다.

입력 변수

입력 변수는 작업의 초기 동작을 결정합니다.

변수	설명
targetId	Exchange 서버가 있는 필수 대상 호스트 식별자 필드입니다.
searchName	Exchange 서버에서 작성된 준수 검색의 필수 이름입니다.

Microsoft Graph 보안 **API** 경보 수집 통합

Microsoft Graph 보안 API 통합을 사용하여 Microsoft Graph 보안 제공자로부터 경보를 수집하고 보안 인시던트를 자동으로 생성합니다.

개요

는 Microsoft Graph 보안 API 여러 보안 공급자(Microsoft 및 ServiceNow 파트너의 기본)를 연결하기 위한 단일 프로그래밍 인터페이스를 제공하는 중간 서비스(또는 브로커)입니다.

통합은 Microsoft Graph 보안 API Azure Microsoft Graph 보안 API Sentinel, Microsoft Defender Advanced Threat Protection 및 Azure Advanced Threat Protection과 같은 다양한 Microsoft

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 기술과 연결하여 이러한 문제를 해결합니다. Microsoft 보안 제공자의 경보가 수집되고 에 보안 인시던트가 자동으로 생성됩니다.보안 인시던트 응답

주요 기능

이 통합에는 다음과 같은 주요 기능이 포함됩니다.

- 보안 인시던트 후보인 경보를 Microsoft Graph 보안 API 검색하고 보안 인시던트 생성을 자동화합니다.
- 경보 필드를 보안 인시던트 필드에 매핑합니다.
- 중복 보안 인시던트를 생성하는 대신 유사한 경보를 기존 오픈 보안 인시던트에 집계합니다.
- 경보 필드 값을 미리 보고 보안 인시던트에서 매핑의 유효성을 검사합니다.
- 보안 인시던트 생성 및 종결에 대한 자동 경보 상태 업데이트.
- 정기적으로 보안 인시던트를 작성하도록 경보의 예약된 수집을 설정합니다.

Microsoft Graph 보안 **API** 통합을 위한 **Now Platform** 인스턴스 설정

다음 섹션에서는 에서 애플리케이션을 ServiceNow Store설치하기 전에 인스턴스에서 완료해야 ServiceNow AI Platform# 하는 설정 작업을 나열합니다.

시작하기 전에

필요한 역할: 관리자

이 태스크 정보

원활한 설치 및 구성을 위해 애플리케이션을 다운로드하고 설치하기 전에 다음 테이블을 참조하고 나열된 작업을 모두 완료했는지 확인하십시오.

설정 작업	설명
필수 ServiceNow AI Platform# 및 보안 인시던트 응답 역할을 할당했는지 확인합니다.	인스턴스에서 통합을 ServiceNow AI Platform# 설치, 설정 및 사용하려면 다음 역할이 필요합니다. • 관리자 역할(admin)의 ServiceNow AI Platform# 사용자는 보안 인시던트 관리자(sn_si.admin) 역할을 사용하여 ServiceNow Store 애플리케이션을 설치하고 할당합니다. • sn_si.admin 역할을 가진 사용자는 다음 ServiceNow AI Platform#에서 다음 작업을 감독합니다. ○ 경보 프로파일의 이름을 지정하고, 생성하고, 편집합니다. ○ Microsoft Graph 보안 API 경보 데이터 필드를 선택하고 보안 인시던트 필드에 매핑합니다. ○ 구성을 완료하기 전에 보안 인시던트 상세 정보가 정확한지 미리 봅니다. ○ 진행 중인 경보 수집을 예약합니다. ○ 인시던트가 보안 인시던트 응답 생성되고 종결되면 경보 업데이트를 활성화합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설정 작업	설명
	◦ 보안 인시던트 분석가(sn_si.analyst) 역할을 할당합니다. ◦ sn_si.analyst 사용자는 보안 인시던트에 대한 작업을 수행합니다. 역할 및 사용자에게 역할을 할당하는 방법에 대한 자세한 내용은 ServiceNow 제품 설명서 웹 사이트의 역할을 참조하십시오.
포털에 애플리케이션을 등록합니다 Microsoft Azure .	경보를 수집하려면 먼저 포털에서 애플리케이션을 Microsoft Azure 구성해야 합니다. 자세한 내용은 Microsoft Azure 포털 구성 문서를 참조하십시오.
ServiceNow 통합을 위해 애플리케이션을 설치하기 전에 통합을 지원하는 데 필요한 핵심 애플리케이션이 설치되고 활성화되었는지 확인합니다.	에서 ServiceNow Store다음 보안 운영 애플리케이션이 설치되고 활성화되는지 확인합니다. 설치되지 않은 경우 원활한 설치를 위해 다음 순서로 한 번에 하나의 애플리케이션을 설치하고 활성화합니다. **1.** 보안 인시던트 응답 **2.** 보안 운영용 이벤트 및 경보 수집: 이 애플리케이션에는 다음이 필요합니다. ◦ com.glide.hub.integration.runtime => ServiceNow 통합 허브 런타임 ◦ com.glide.hub.action_step.rest => ServiceNow 통합 허브 작업 단계 - REST 주: 통합 허브 구성요소는 이벤트 및 경보 수집 플러그인과 함께 설치됩니다. 설치되지 않은 경우 고객 지원에 문의하여 도움을 받으십시오. 핵심 애플리케이션 설치에 보안 운영 대한 자세한 내용은 해당 애플리케이션 활성화 ServiceNow Store문서를 참조하십시오제품 또는 애플리케이션에 대한 보안 운영 권리 가져오기.

Microsoft Azure 포털 구성

를 Microsoft Graph 보안 API사용하여 Microsoft Azure 테넌트에서 사용할 수 있는 애플리케이션에 대한 보안 경고를 검색하려면 포털에 애플리케이션을 Microsoft Azure 등록하고 애플리케이션에 대한 읽기 및 쓰기 접근 권한을 보안 이벤트에 부여해야 합니다.

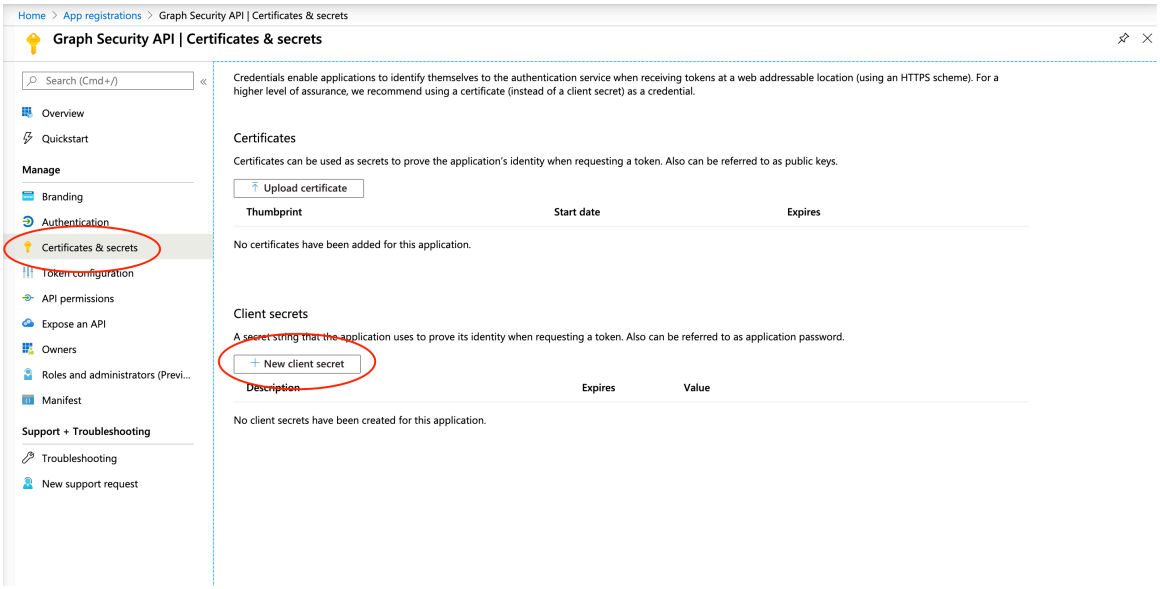
시작하기 전에
필요한 역할:

- 애플리케이션 개발자: 애플리케이션을 등록하는 데 필요합니다.
- 테넌트 관리자: Microsoft Azure 테넌트 관리자는 관리자 동의 끝점을 호출하여 응용 프로그램에 대한 권한을 부여해야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. Microsoft Azure 포털에 로그인합니다.
2. 검색 상자에 **App** registrations를 입력합니다.
3. 신규 등록을 클릭합니다.
4. 애플리케이션의 이름과 리디렉션 URI(예: http://localhost)를 입력하고 등록을 클릭합니다.
   리디렉션 URI는 애플리케이션에 대한 관리자 동의를 제공하는 동안 사용됩니다.
5. 앱 등록 페이지에서 등록한 애플리케이션(예: Graph 보안 데모)을 선택합니다.
6. 관리에서 인증서 및 비밀을 선택합니다.

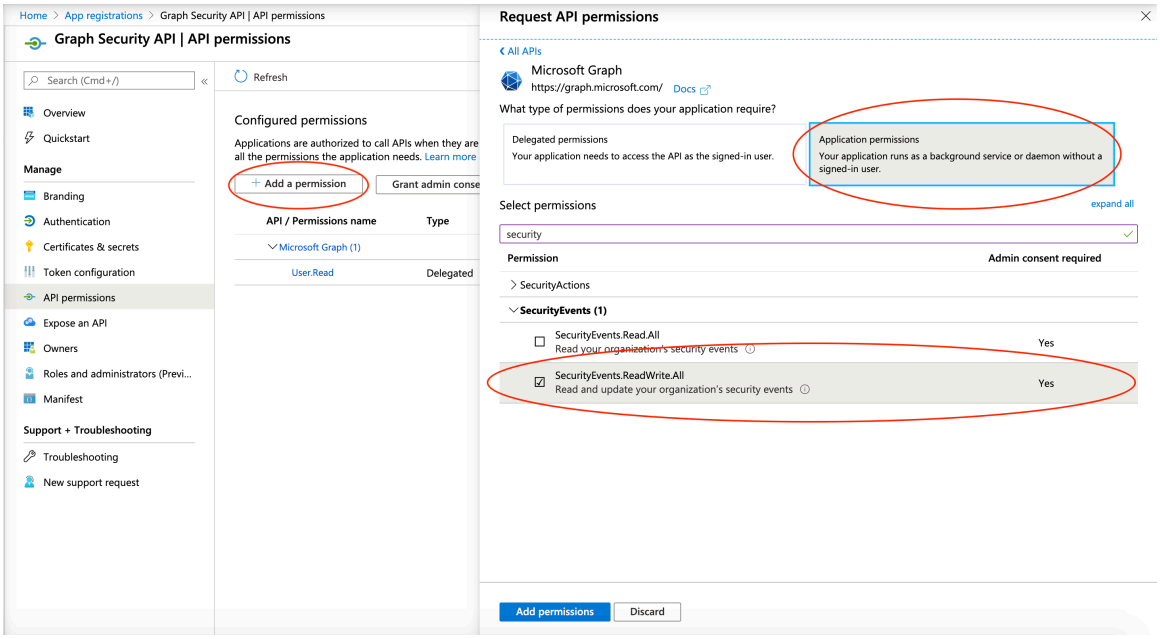


7. 새 클라이언트 비밀을 선택하여 클라이언트 비밀을 만듭니다.
   클라이언트 비밀을 복사하여 나중에 볼 수 없도록 저장합니다. 클라이언트 비밀을 잊어버린 경우 새 클라이언트 비밀을 생성할 수 있습니다.

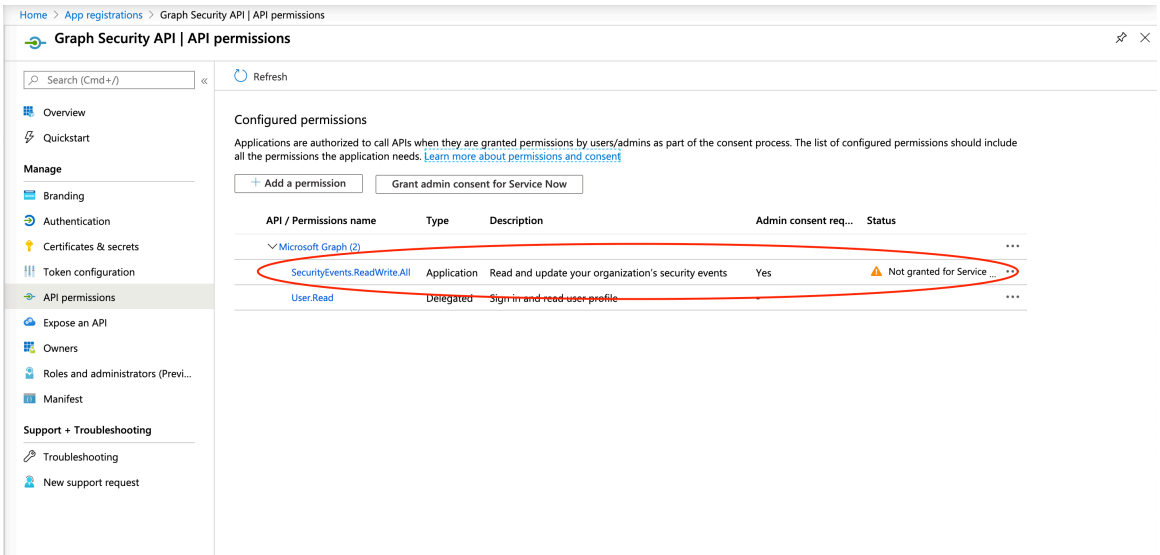
   주:
   클라이언트 암호를 잊어버린 경우 4단계와 5단계의 지침에 따라 새 클라이언트 암호를 생성할 수 있습니다.

8. 개요 페이지에서 **API** 권한 보기를 클릭합니다.
9. SecurityEvents.ReadWrite.All 보안 이벤트에 대한 새 애플리케이션 수준 API 권한을 추가합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



10. 새로 추가된 API 권한에 대한 관리자 동의를 부여합니다.
자세한 내용은 Microsoft Graph 권한 참조 Microsoft Graph 권한 모델을 참조하세요.



11. 테넌트 관리자로 로그인하고 애플리케이션에 대한 동의를 제공합니다.
단계는 다음과 같습니다.

a. 다음 URL로 이동합니다. https://login.microsoftonline.com/common/adminconsent?client_id=APPLICATION_ID&state=12345

등록한 애플리케이션의 APPLICATION_ID 입력합니다.

12. 수락을 클릭하여 위에서 만든 애플리케이션에서 요청한 권한을 수락합니다.
그런 다음 애플리케이션을 사용하여 보안 이벤트를 읽을 수 있습니다. 자세한 내용은 Microsoft Graph 보안 권한 부여 설명서를 참조하세요.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

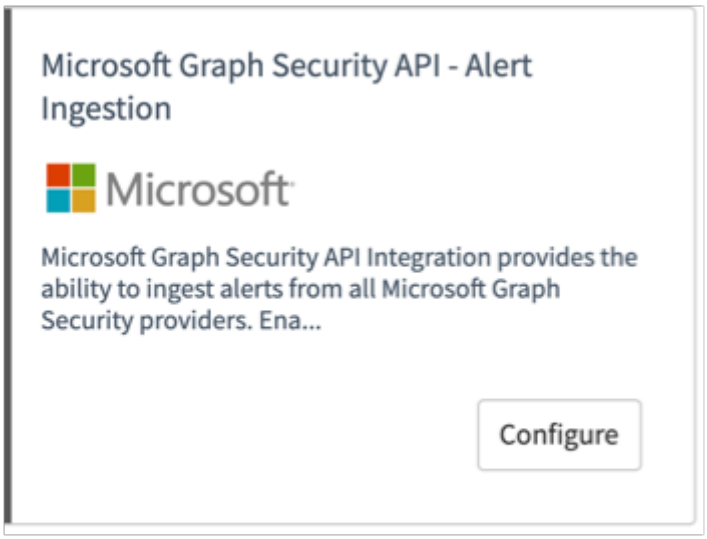
Microsoft Graph Security API 경보 수집 통합을 위한 **ServiceNow** 애플리케이션 설치 및 구성

인스턴스에서 통합을 ServiceNow AI Platform# 실행하기 전에 다음 설치 및 구성 단계를 완료하여 애플리케이션이 인스턴스의 및 보안 운영 제품과 ServiceNow AI Platform 제대로 통합 보안 인시던트 응답 되도록 합니다.

시작하기 전에
필요한 역할: sn_si.admin

프로시저

1. 통합을 위해 애플리케이션을 ServiceNow Store 설치하지 Microsoft Graph 보안 API 않은 경우 를 참조 보안 운영 통합 설치 하고 단계에 따라 설치합니다.
2. 애플리케이션을 성공적으로 설치한 후 통합 〉 통합 구성 을 클릭하고 Microsoft Graph 보안 API - 경보 수집 타일을 찾습니다.



3. 애플리케이션을 구성하려면 구성을 클릭합니다.
4. 표시되는 경보 수집 구성 대화 상자에서 필드에 내용을 입력합니다.
5. 제출을 클릭합니다.
   성공적으로 확인 및 제출되면 각 경보 수집 서버 구성이 보안 통합 페이지에 타일로 저장됩니다. 저장된 구성 타일이 보안 통합 페이지에 표시되지 않으면 페이지 오른쪽 상단 모서리에 있는 구성 선택 목록 표시에서 예를 클릭합니다.

다음에 수행할 작업
애플리케이션을 성공적으로 설치하고 구성했습니다. 다음 단계는 경보 프로필을 만드는 것입니다.

Microsoft Graph 보안 **API** 경보 수집 통합을 위한 프로파일 생성

sn_si.admin 역할을 가진 사용자는 인스턴스에 경보 프로필을 ServiceNow AI Platform 만들고 보안 인시던트를 생성하는 경보를 결정합니다. 수집된 경보에서 보안 인시던트가 생성되기 전에 실제 보안 인시던트가 표시되는 방식을 미리 볼 수 있도록 경보의 필드 값이 보안 인시던트의 ServiceNow AI Platform 레이아웃에 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_si.admin

이 태스크 정보
통합을 통해 무단 접근 시도 및 맬웨어 등 다양한 유형의 경보를 수집할 수 있습니다. 이러한 경보는 인스턴스 환경에서 구성한 보안 운영 프로파일을 기반으로 수집됩니다. 모든 경보는 처음에 프로파일에 구성된 경보 유형에 대해 수집됩니다. 수집된 경보를 추가로 필터링하여 보안 인시던트를 생성하는 경보를 지정할 수 있습니다.

예를 들어 고위험으로 식별된 경보에 대해서만 보안 인시던트를 생성하는 필터를 선호할 수 있습니다. 프로파일이 활성화되고 수집된 경보에서 보안 인시던트를 생성하기 전에 필터링된 경보의 개별 필드 값이 미리 보기를 위해 보안 인시던트 레이아웃의 해당 필드에 매핑됩니다. 테넌트의 Microsoft Azure 선택 기준을 충족하고 위에서 Microsoft Graph 보안 API 사용할 수 있는 모든 경보는 처음에 인스턴스에 수집됩니다 ServiceNow AI Platform .

프로파일의 소스 식별

프로파일의 이름과 소스를 지정합니다.

시작하기 전에
필요한 역할: sn_si.admin

프로시저

1. 인스턴스에서 경보 ServiceNow AI Platform 에 대한 프로필을 만들려면 다음으로 이동합니다. **Microsoft Graph** 보안 **API** 통합 〉 **Microsoft Graph** 보안 **API** 프로파일.
2. 새로 만들기를 클릭합니다.
3. 필드에 내용을 입력합니다.

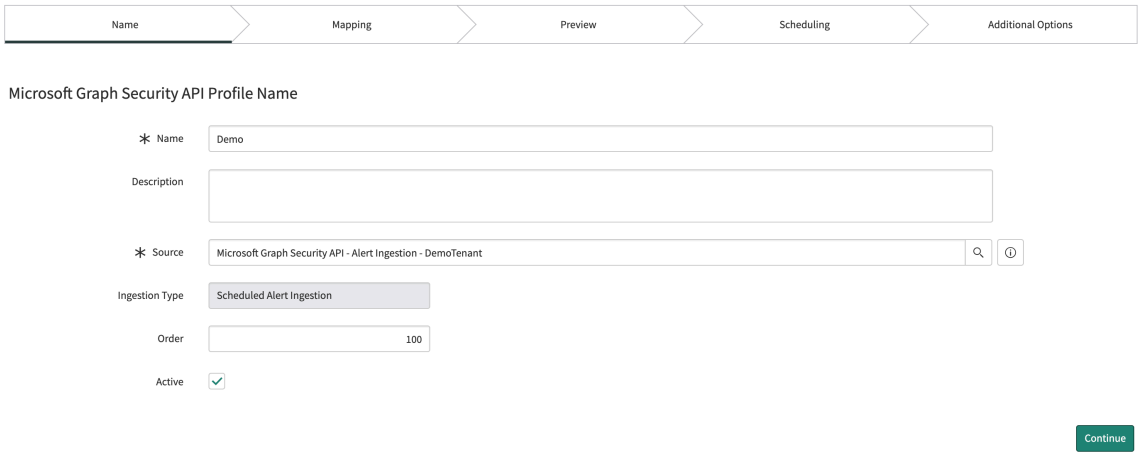
   완료된 양식의 예가 테이블 다음에 나옵니다.

필드	설명
이름	프로파일의 고유한 이름입니다. 이름이 고유하지 않으면 오류가 표시되고 중복된 프로파일 이름은 저장되지 않습니다. 인스턴스의 프로파일 이름은 ServiceNow AI Platform 고유해야 합니다.
활성	확인란은 기본적으로 선택이 취소되어 있습니다. 이 옵션을 사용하지 않도록 설정하면 프로파일이 활성화되지 않습니다. 주: 프로파일을 활성화하기 전에 프로파일의 모든 섹션을 완료해야 합니다.
소스	경보를 수집하도록 구성한 테넌트입니다 Microsoft Azure . 여러 테넌트가 구성된 경우 프로파일에 대해 수집하려는 경보 유형에 적합한 테넌트를 선택합니다. 값을 입력해야 합니다.
순서	기본값은 100입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	여러 프로필을 만든 경우 둘 이상의 프로필이 동일한 트리거 조건을 공유할 때 이 값은 런타임 실행 우선 순위를 제공합니다. 순서 값이 낮을수록 우선순위가 높습니다.
(선택 사항) 묘사	이 프로파일을 다른 프로파일과 구별하는 데 도움이 되는 추가 텍스트입니다.

다음 그림은 완성된 폼의 예입니다.



다음에 수행할 작업
다음 단계는 경보 필드를 매핑하는 것입니다.

Microsoft Graph Security API 경보 수집 통합에 대한 경보 필드 매핑

예약된 경보 수집을 위한 소스를 식별한 후 다음 단계는 개별 경보 필드를 보안 인시던트의 필드에 매핑하는 ServiceNow AI Platform SIR 것입니다.

매핑 단계의 경우 먼저 테넌트에서 샘플 경보를 Microsoft Azure 수집해야 합니다. 그런 다음 모든 관련 경보 필드 데이터가 인시던트 양식의 적절한 위치에 SIR 매핑되었는지 확인한 다음 미리 보기 섹션에서 인시던트를 시각화 SIR 해야 합니다.

샘플 경보 필드의 매핑에는 다음이 포함됩니다.

- 샘플 Microsoft Graph 보안 API 경보 수집
- 보안 인시던트 응답 필드에 경보 매핑

샘플 **Microsoft Graph** 보안 **API** 경보 수집

테넌트에서 샘플 경보를 Microsoft Azure 수집합니다.

시작하기 전에
필요한 역할: sn_si.admin

프로시저

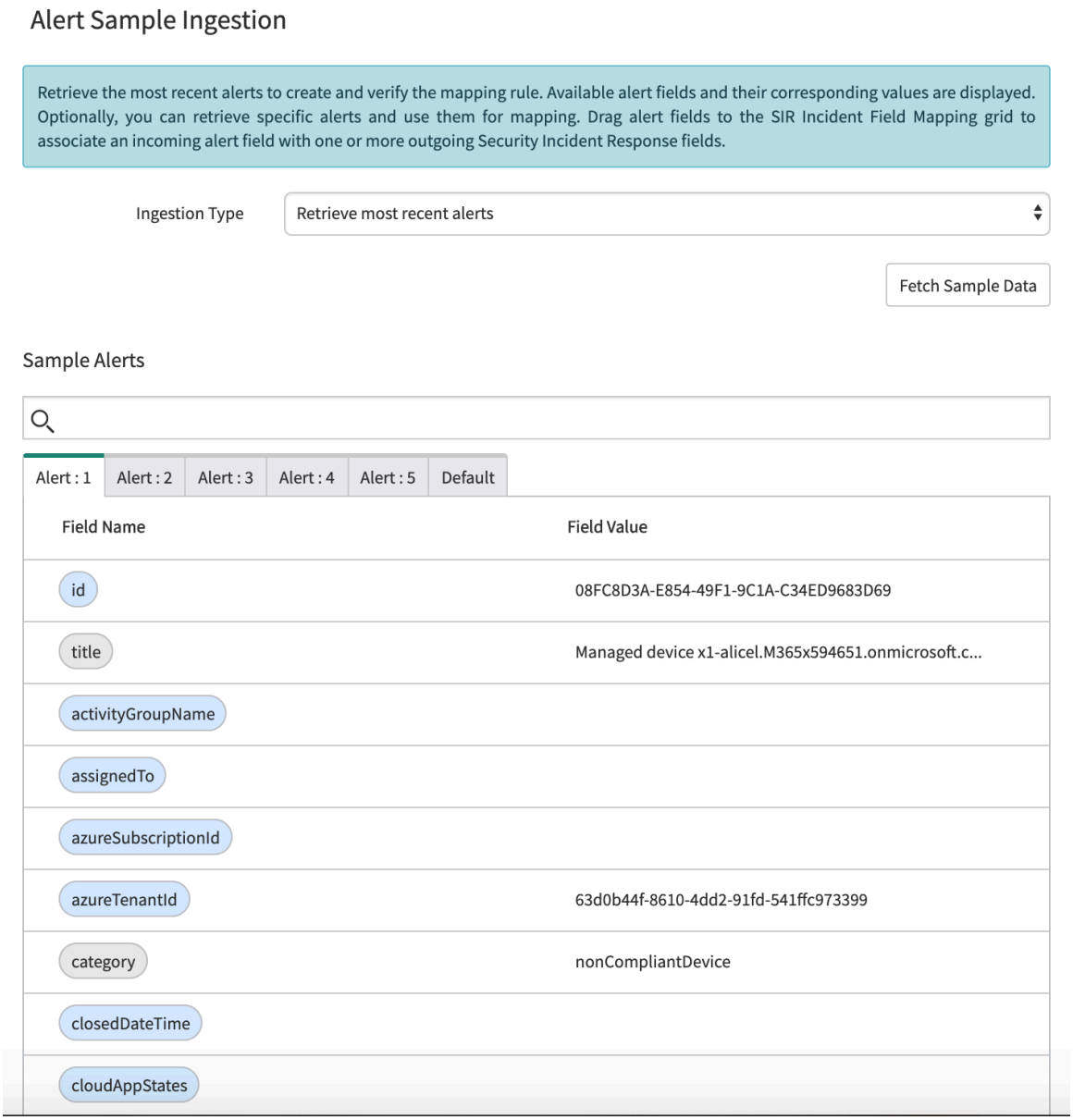
1. 가장 최근의 샘플 경보 5개를 끌어오거나 매핑 환경에 사용하려는 특정 경보에 대한 고유 경보 ID를 제공할 수 있습니다.
   수집 기본 설정 선택 목록에서 다음 중 하나를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 최근 경보 검색: 가장 최근 경보 5개가 검색됩니다.
- 경보 ID를 기준으로 경보 선택: 검색할 경보의 경보 ID를 지정합니다. 쉼표로 구분된 최대 5개의 경보 ID를 지정할 수 있습니다.

2. 샘플 데이터 가져오기를 클릭하여 테넌트에서 Microsoft Azure 최신 샘플 경보 데이터를 끌어옵니다.
   샘플 경보를 끌어오는 데 몇 분 정도 걸릴 수 있습니다.

   샘플 경보 필드 값은 프로파일에서 샘플 경보를 수집할 때 양식 왼쪽에 채워집니다. 보안 인시던트 필드에 매핑 SIR 되는 경보입니다. 경보 필드와 값 결과는 개별 탭으로 표시됩니다.



다음에 수행할 작업

샘플 데이터를 가져온 후 다음 단계는 경보 필드를 보안 인시던트에 매핑하는 것입니다.

보안 인시던트 응답 필드에 경보 매핑

트리거된 경보의 개별 경보 필드를 보안 인시던트의 ServiceNow AI Platform 필드에 매핑합니다.

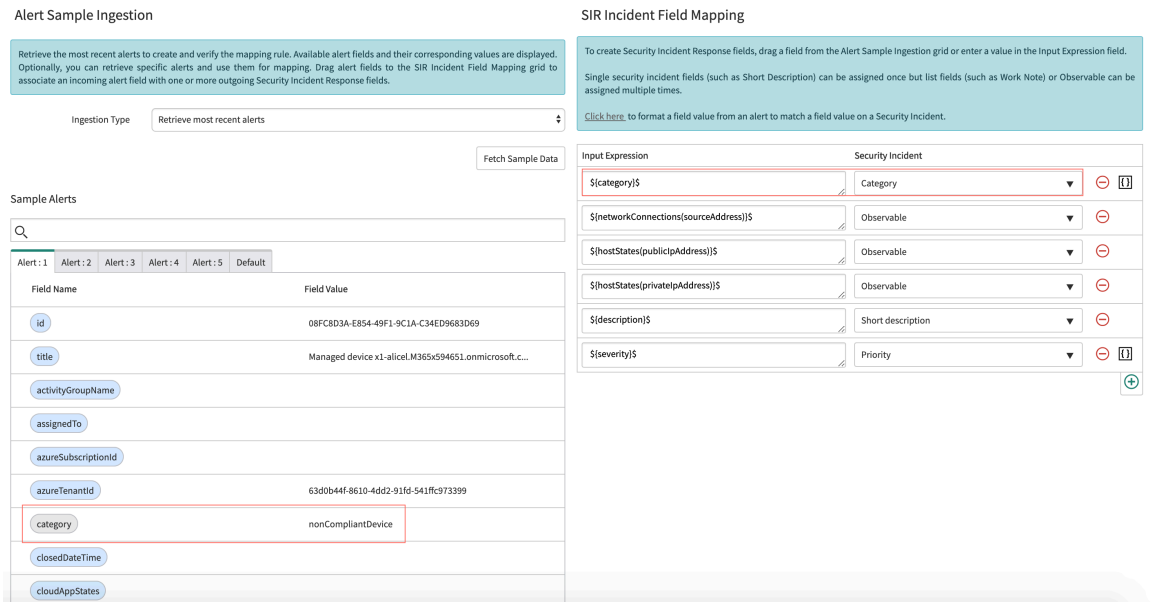
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

경보 필드 매핑

sn_si.admin 역할이 있는 사용자는 왼쪽의 샘플 경보 섹션에 있는 필드를 사용하여 오른쪽 패널에 있는 SIR 인시던트 필드 매핑 열의 보안 인시던트 필드에 매핑합니다. 왼쪽에서 경보 필드를 오른쪽의 인시던트 매핑 섹션에 끌어서 놓아 SIR 매핑 구성을 편집합니다. 오른쪽의 매핑은 수신 경보 필드를 발신 보안 인시던트 필드와 연결합니다.

1. 샘플 데이터를 가져온 후 다음 단계는 경보 필드를 보안 인시던트에 매핑하는 것입니다. 양식 왼쪽의 필드 값을 양식 오른쪽에 있는 보안 인시던트의 필드에 매핑하려면 양식 왼쪽에 있는 파란색 필드 이름을 길게 클릭합니다.
2. 필드 이름(예: ##)을 끌어서 보안 인시던트 열의 필드 이름 옆에 있는 입력 식 열의 필드에 놓습니다.

   필드 값이 입력 식 열에 표시됩니다. 다음 이미지에서 ## 는 보안 인시던트의 ## 필드에 매핑되어 있습니다.



그러나 왼쪽의 모든 값을 오른쪽의 필드와 일치시킬 수 있습니다. 미리 보기 단계에서 보안 인시던트에 값이 올바르게 매핑되었는지 확인합니다.

매핑 프로세스에서 경보 필드가 간과되거나 중복되지 않도록 하기 위해 필드는 색으로 구분됩니다. 경보 필드를 색상으로 구분하면 이미 매핑한 경보 값이 회색으로 표시되고 나머지 매핑되지 않은 모든 필드는 파란색으로 표시될 때 해당 값을 추적할 수 있습니다. 이렇게 하면 보안 인시던트에 추가된 필드 값과 나머지 중요한 경보 정보가 매핑되지 않은 상태로 남아 있는지 시각화하는 데 도움이 됩니다.

왼쪽의 연한 파란색 필드는 경보 필드가 아직 선택되지 않았으며 보안 인시던트에 매핑되지 않았음을 나타냅니다. 수신 경보 필드를 보안 인시던트의 둘 이상의 필드와 연결하는 것을 선호할 수 있습니다. 회색 필드는 필드가 선택되었고 보안 인시던트의 필드에 매핑되었음을 나타냅니다. 이 색상 코딩은 매핑을 추적하는 데 도움이 됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

a. 입력 식 필드에 값을 수동으로 입력하려면 ${fieldname}$ 형식으로 입력합니다. 경보 필드가 보안 인시던트 필드에 매핑됩니다.

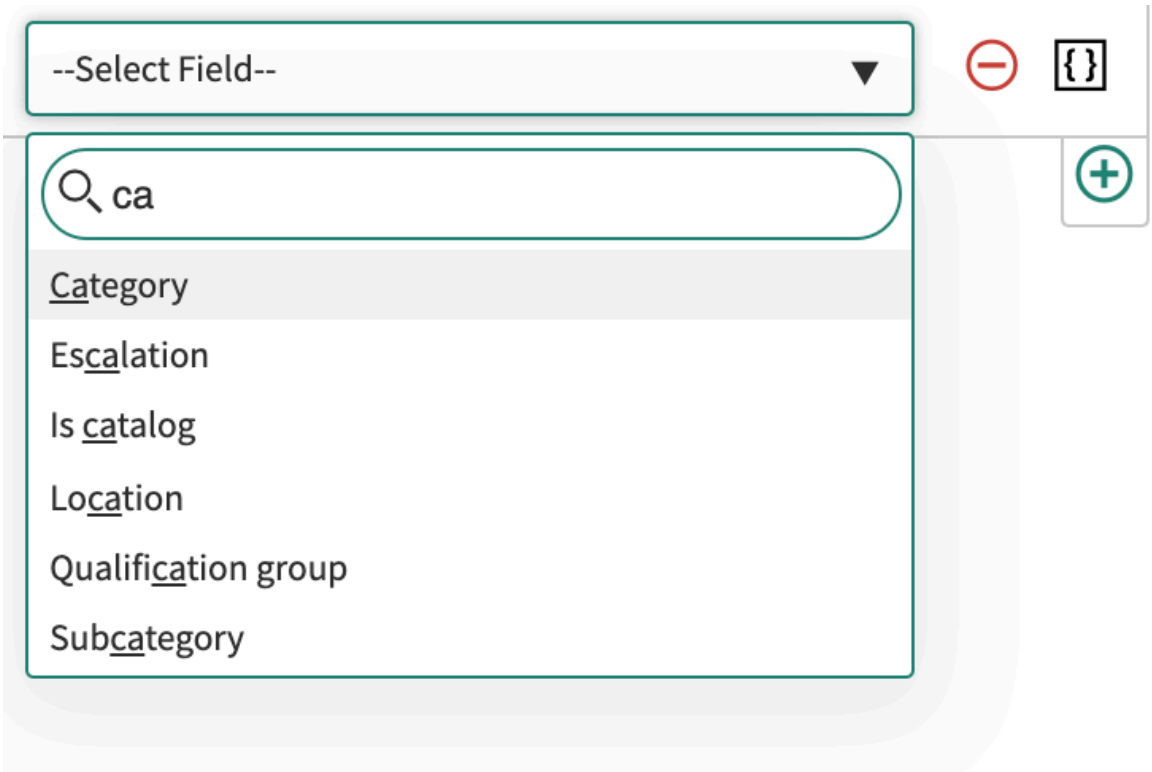
b. 수집된 경보 MITRE-ATT&CK 를 보안 인시던트 매핑 섹션의 프레임워크 필드에 매핑할 수 없습니다. 필드를 매핑하는 경우 보안 인시던트 양식의 프레임워크 섹션에서 카드의 MITRE-ATT&CK 일부로 MITRE-ATT&CK 정보를 사용할 수 없습니다. 기술을 연결하려면 MITRE-ATT&CK 모듈에서 위협 인텔리전스 프레임워크의 MITRE-ATT&CK 일부로 사용할 수 있는 자동 추출 기능을 사용하십시오.

3. 양식 오른쪽의 보안 인시던트에 표시되는 기본 필드에 필드를 추가하려면 다음 단계를 따르십시오.

a. 양식 오른쪽의 SIR 인시던트 필드 매핑 섹션 그리드 하단에서 더하기(+) 아이콘을 클릭합니다. 새 필드가 표시됩니다.

b. 보안 인시던트 열에서 표시되는 선택 목록을 확장하고 필드를 선택합니다.

새 필드의 확장된 선택 목록에서 일부 필드는 음영 처리됩니다. 다음 그림에서 범주는 보안 인시던트에 매핑되었기 때문에 회색 배경입니다. 양식 왼쪽에 있는 경보 필드에 대한 색상 코딩과 유사하게 오른쪽에 있는 보안 인시던트 필드에 대한 이 색상 코딩은 이미 매핑 SIR 된 인시던트 필드를 추적하는 데 도움이 됩니다.



주:
동일한 보안 인시던트에 여러 옵저버블을 표시할 수 있으므로 옵저버블 필드를 서로 다른 값으로 여러 번 매핑할 수 있습니다. 마찬가지로 구성 항목 및 작업 메모 필드는 여러 값을 지원합니다. 여러 값을 지원할 수 없는 필드에 두 값을 매핑하려고 하면 인시던트를 미리 볼 때 필드에 값이 없다는 오류 메시지가 표시됩니다. 마찬가지로 보안 인시던트의 필드에 여러 옵션을 선택할 수 있는 선택 목록이 있고 선택 목록에 표시되지 않는 해당 필드에 옵션을 매핑하려고 하면 보안 인시던트에 필드가 채워지지 않습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

c. 또는 새 행의 검색 필드에 값을 입력합니다.

d. 양식의 왼쪽에서 왼쪽 단추를 클릭하여 입력 식 필드에 넣을 경보 ID를 선택합니다. 끌어서 놓기 기능을 사용하여 새 필드 옆에 매핑합니다.

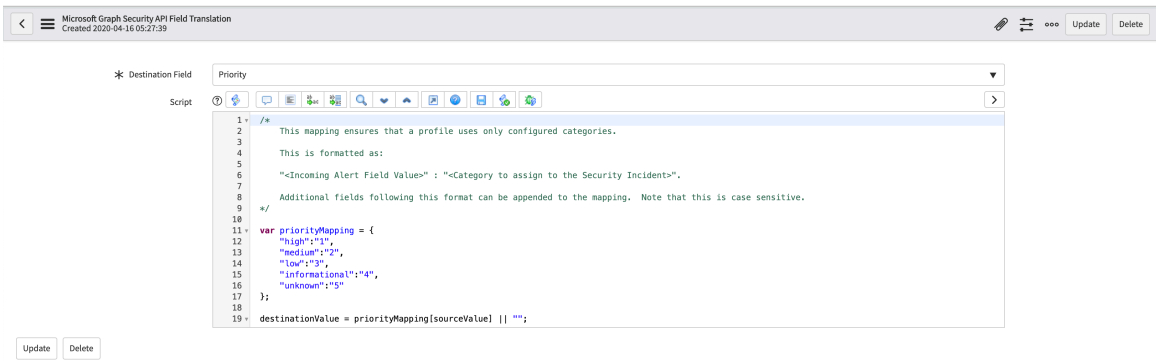
4. 매핑에 필드 값을 추가하거나 제거하여 매핑을 계속합니다.

5. 앞의 필드 매핑 단계를 완료한 후에는 인시던트 생성 조건 작성기에서 동일한 필드 값을 사용하여 수신되는 경보가 보안 인시던트를 만들기 위해 충족해야 하는 추가 기준을 정의할 수 있습니다. 인시던트 생성 조건을 설정하려면 다음 단계를 수행합니다.

필드 형식 변환

경우에 따라 의 Microsoft Graph 보안 API 경보 필드 값이 SIR 보안 인시던트의 필드로 직접 변환되지 않을 수 있습니다. 이러한 값의 경우 스크립트 편집기를 사용하여 매핑 단계 중에 보안 인시던트의 필드 값에 대한 형식을 지정할 수 있습니다. 비슷하지만 동일하지는 않은 값의 형식을 지정하려면 스크립트 편집기를 사용하십시오. 예를 들어 스크립트 편집기를 사용하면 맬웨어 경보 및 바이러스 감염의 범주 값이 소스 범주에 대해 서로 다를 수 있지만 형식 필드 번역 기능을 사용하면 두 값 모두 SIR 보안 인시던트의 범주 필드에서 공통 악성 코드 활동으로 변환할 수 있습니다.

스크립트 편집기를 사용하려면 {} 아이콘을 클릭합니다. 스크립트 편집기가 표시됩니다.



인시던트 생성 조건

매핑 섹션이 완료되면 필터 조건을 설정하여 보안 인시던트를 생성할 경보와 필터링할 경보(예: 우선순위가 낮은 경보)를 지정할 수 있습니다. 인시던트 생성 조건 작성기에서 동일한 필드 값을 사용하여 수신되는 경보가 보안 인시던트를 만들기 위해 충족해야 하는 추가 기준을 정의할 수 있습니다. 인시던트 생성 조건을 설정하려면 다음 단계를 수행합니다.

1. 양식에서 인시던트 생성 조건 섹션으로 스크롤하고 조건에 따라 필터링 옵션을 선택합니다. 필터 조건 작성기가 표시됩니다. 이러한 필터를 사용하여 필드에 설명된 특정 조건과 일치하는 보안 인시던트를 생성합니다.

   필터 조건 작성기의 첫 번째 필드에 대한 선택 목록의 옵션은 수집한 경보에 대한 경보 샘플 수집 섹션에 표시되는 필드와 일치합니다. 이러한 필드는 동적이며 수집하는 경보에 따라 변경됩니다. 입력하는 기준은 대/소문자를 구분하며 경보 값과 정확히 일치해야 합니다. 필터 필드에 입력할 값에 대해 잘 모르는 경우 Microsoft Azure 테넌트로 돌아가서 키워드에 대한 경고를 검토하는 것이 좋습니다.

2. 조건 작성기의 선택 목록과 필드를 사용하여 첫 번째 행에 대한 필터를 설정합니다.

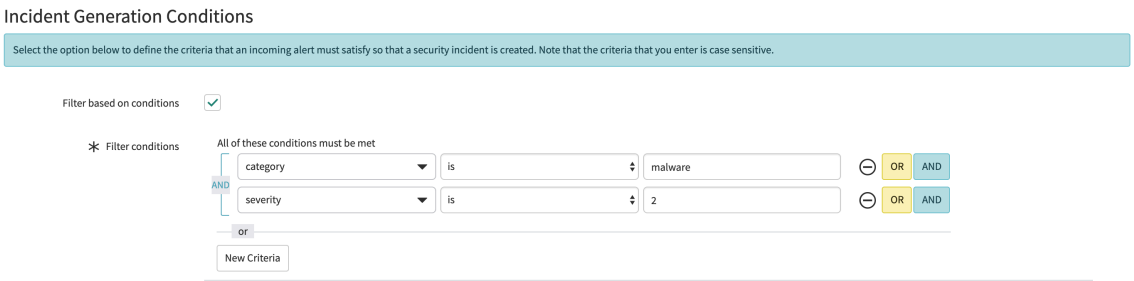
3. 조건을 더 추가하려면 필드 오른쪽에서 AND 또는 **OR**을 클릭합니다.

   - **AND**를 선택하면 모든 조건이 일치해야 합니다.
   - **OR**을 선택하면 두 조건을 일치시킬 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 두 번째 행에서 두 번째 필터 조건을 설정합니다

   다음 이미지는 보안 인시던트가 생성되기 전에 일치해야 하는 두 가지 조건이 있는 예입니다.



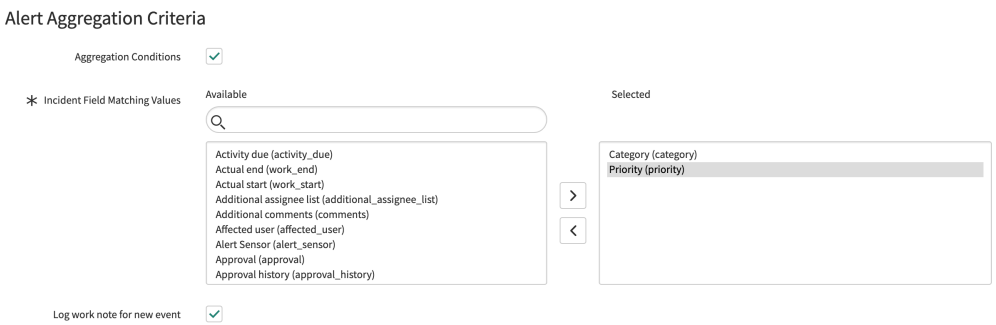
   입력한 두 필터링 조건이 일치하는 경우에만 보안 인시던트가 생성되도록 트리거 조건을 설정했습니다.

   이러한 유형의 필터링은 보안 경고를 격리하는 데 유용하며 생성하는 보안 인시던트 수를 제한합니다. 추가 필터링 기준이 설정되면 쿼리 또는 트리거된 경보 구성을 변경할 필요 없이 필요한 경보만 수집됩니다.

유사한 경보를 처리하고 중복 인시던트를 방지하기 위한 경보 집계 기준

중복될 가능성이 있는 유사한 인시던트를 만드는 대신 수신 경보를 기존 SIR 보안 인시던트로 집계하는 추가 경보 집계 기준을 정의합니다. 이 추가 집계 기능은 각 프로파일에 대해 필드 일치 값 기준을 사용하여 모든 관련 경보 데이터를 단일 보안 인시던트에 배치함으로써 활성 상태의 중복 보안 인시던트 수를 줄일 수 있습니다. 기준을 설정하려면 다음 단계를 수행합니다.

1. 폼에서 경보 집계 기준 섹션으로 스크롤한 후 집계 조건 옵션을 선택합니다. 인시던트 필드 일치 값 열이 표시됩니다. 이러한 필드 이름은 보안 인시던트에 구성된 SIR 사용자 지정 필드를 포함하는 보안 인시던트의 필드입니다.
2. 사용 가능 목록에서 기존 보안 인시던트 ServiceNow AI Platform 와 일치시킬 필드 값을 선택하고 선택됨 목록으로 이동합니다. 이 수신 경보를 기존 보안 인시던트에 추가하려면 선택하는 모든 필드 값이 일치해야 합니다. 여기에는 옵저버블 및 구성 항목과 같이 여러 경보 필드 값이 매핑될 수 있는 필드가 포함됩니다. 모든 값이 일치해야 합니다. 값의 하위 집합만 일치하면 경보 집계 조건이 충족되지 않고 새 보안 인시던트가 생성됩니다. 다중 값 필드 매핑에 대한 아래 스크린샷을 참조하십시오.



   새 경보가 매핑 단계의 집계 필드 조건에서 선택한 모든 값과 일치하면 가장 최근에 열린 보안 인시던트에 동일한 필드 값으로 경보가 자동으로 추가됩니다. 보안 인시던트를 담당하는 sn_si.analyst 역할을 가진 사용자는 보안 인시던트의 관련 목록에서 추가된 모든 집계 경보를 볼 수 있습니다. 보안 인시던트에 대한 모든 집계 경보는 집계된 Microsoft Graph 경보 관련 목록에 표시됩니다. 이 목록에는 관련 타임 스탬프 및 집계된 필드 값이 자세히 설명되어 있습니다. 이 정보는 기존 보안 인시던트에 경보가 추가되는 이유를 이해하는 데 도움이 됩니다. 이 탭이

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

표시되지 않으면 관련 링크 아래에 있는 기록의 왼쪽으로 스크롤하여 모든 관련 목록 표시 링크를 클릭합니다.

3. (선택 사항) 보안 인시던트에 최근에 추가된 새 경보에 대한 작업 메모를 기록하려면 이 확인란을 선택하여 이 옵션을 활성화합니다. 작업 메모는 경보 상세 정보 및 매핑 섹션의 작업 메모 필드에 추가되었을 수 있는 기타 상세 정보에 대한 링크와 함께 새 경보가 추가되었음을 기록합니다.

   경보 값을 보안 인시던트의 SIR 필드에 매핑했습니다. 또한 필터링 기준을 사용하여 보안 인시던트 생성을 제한하는 추가 조건을 구성했습니다. 또한 기존 SIR 보안 인시던트에 경보 또는 이벤트를 추가했습니다.

4. 계속을 클릭하여 프로파일 구성을 계속합니다. 다음 단계는 SIR 보안 인시던트에서 매핑한 필드를 미리 보는 것입니다

Microsoft Graph 보안 **API** 통합에 대한 보안 인시던트 미리 보기

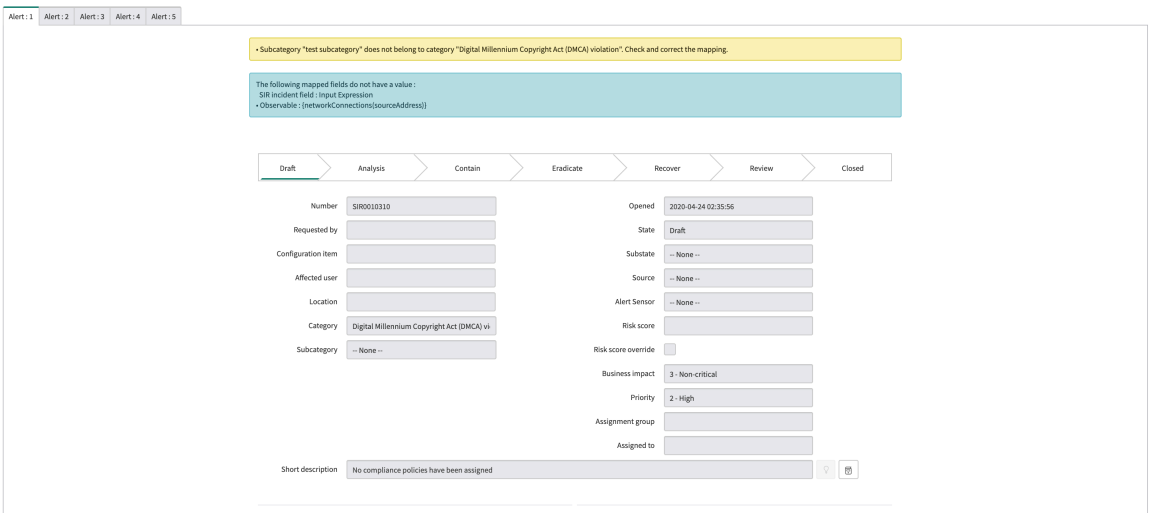
매핑 단계를 완료한 후 보안 인시던트에서 ServiceNow AI Platform SIR 매핑한 값을 미리 봅니다. 이 미리 보기 단계를 통해 보안 인시던트에 표시할 경보 필드를 모두 매핑했는지 확인할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.admin

이 태스크 정보
sn_si.admin 역할을 가진 사용자는 보안 인시던트를 미리 보고 필요에 따라 매핑을 다시 편집하여 오류가 있는 필드를 수정하거나 누락된 데이터를 채웁니다. 미리 보기가 성공적으로 완료되지 않으면 예약 단계로 진행할 수 없습니다. SIR 보안 인시던트 미리 보기는 제품에 실제 인시던트 보안 인시던트 응답 로 저장되지 않습니다.

프로시저

1. 보안 인시던트 미리 보기가 표시되지 않으면 진행률 표시줄에서 미리 보기를 클릭합니다.
   수집된 모든 경보와 매핑 페이지에 정의된 필드 매핑이 표시됩니다.
2. 경보 ID를 클릭하면 보안 인시던트의 미리 보기를 볼 수 있습니다.
   이 뷰는 읽기 전용 뷰이며 이 보안 인시던트의 기록은 저장되지 않습니다.
3. 보안 인시던트에서 경보 값의 필드 매핑을 검토합니다.



앞의 이미지는 수집된 샘플의 매핑 오류가 있는 미리 보기의 예입니다.

4. 이 오류를 해결하려면 진행률 표시줄에서 매핑 을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. 매핑을 편집하여 잘못된 값을 수정하거나 누락된 데이터를 채웁니다.

6. 매핑을 다시 미리 보고 오류 메시지에 설명된 오류를 계속 수정합니다.

다음에 수행할 작업
오류 메시지가 표시되지 않고 보안 인시던트의 필드 매핑에 만족하는 경우 다음 단계는 일정을 정의하는 것입니다.

Microsoft Graph 보안 **API** 통합 일정 정의

경보 검색에 대한 기본 설정을 확인하거나 필요한 경우 일정을 수정합니다. 이 단계를 통해 날짜 범위를 기준으로 경보 검색을 필터링할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.admin

이 태스크 정보
경보 프로파일 구성과 일치하는 향후 경보를 폴링할 빈도를 선택할 수도 있습니다. 자동 경보 수집 프로파일의 경우 프로파일이 활성화되기 전에 예약 및 경보 검색을 확인하고 수정합니다. 이 단계는 예약된 경보 프로파일에 필요합니다.

sn_si.admin 역할을 가진 사용자는 프로파일별로 이러한 폴링 간격을 구성합니다. 경보 수집 통합의 Microsoft Graph 보안 API 성능은 다양한 폴링 간격의 영향을 받습니다. 일정을 예약할 때 시스템 부하와 인시던트 긴급도의 균형을 맞추는 것이 좋습니다. 모든 프로파일에 대해 5분 기본값이 설정되지만 인시던트의 긴급도와 시스템의 예상 로드에 따라 이 설정을 수정하는 것이 좋습니다.

프로시저

1. 진행률 표시줄에 스케줄링 페이지가 표시되지 않으면 스케줄링을 선택합니다.

2. 테넌트에서 경보를 Microsoft Azure 끌어오는 방법과 시기를 예약하려면 하나를 선택합니다.

3. 계속을 클릭하여 추가 옵션 페이지로 이동합니다.

SIR 인시던트 상태에 따라 경보 업데이트 및 종결을 자동화

Microsoft Graph 보안 API 경보 수집 통합에는 두 경보가 보안 인시던트를 생성할 수 있는 양방향 인터페이스가 있으며, 보안 인시던트가 생성되거나 종결되면 인시던트 번호, 할당 그룹, SIR 인시던트 URL 등의 관련 인시던트 상세 정보로 SIR 경보를 업데이트할 수 있는 기능이 있습니다. T

시작하기 전에
필요한 역할: sn_si.admin

주:
초기 및 종결 경보 상태는 서비스 제공자가 이 기능을 지원하는 경우에만 업데이트됩니다. 자세한 내용은 설명서 및 보안 공급자 설명서를 참조하십시오 Microsoft Graph 보안 API .

프로시저

1. 진행률 표시줄에 추가 옵션 페이지가 표시되지 않으면 추가 옵션을 선택합니다.

2. 아래 지침에 따라 보안 인시던트가 생성될 때 경보를 업데이트하기 위한 구성을 완료합니다.

3. Finish(마침)를 클릭하여 구성을 완료하고 프로파일을 **Waiting** 상태로 이동합니다.
확인 대화 상자가 표시됩니다. 통합에 대한 설정 및 구성을 성공적으로 완료했습니다. 이 프로파일을 활성화하여 일정에 따라 테넌트에서 경보를 Microsoft Azure 끌어옵니다. 24시간 내에 최대 1,000개의 보안 인시던트를 생성할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Microsoft Graph 보안 **API** 통합 구성 설정

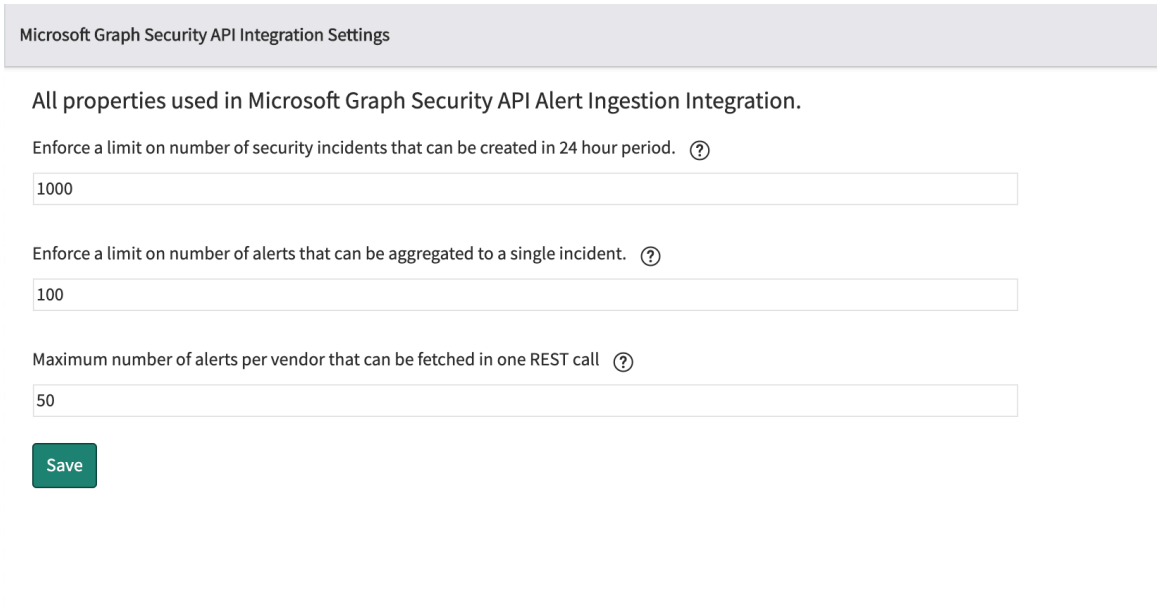
이 옵션을 사용하여 수집 통합 기본 시스템 속성을 수정합니다 Microsoft Graph 보안 API .

시작하기 전에
필요한 역할: sn_si.admin

이 태스크 정보
기본 구성 속성을 수정하여 24시간 동안 만들 수 있는 보안 인시던트 수 또는 하나의 보안 인시던트에 집계할 수 있는 경보 수를 제한합니다.

시스템 속성을 수정하려면 *sn_si.admin* 역할의 사용자로 로그인하고 **Microsoft Graph** 보안 **API** 통합 〉 **Microsoft Graph** 보안 **API** 통합 설정.

기본 구성 설정이 표시됩니다. 필요한 경우 이러한 설정을 수정할 수 있습니다.



수정된 통합 설정은 프로파일에 정의된 다음 폴링 간격 동안 적용됩니다.

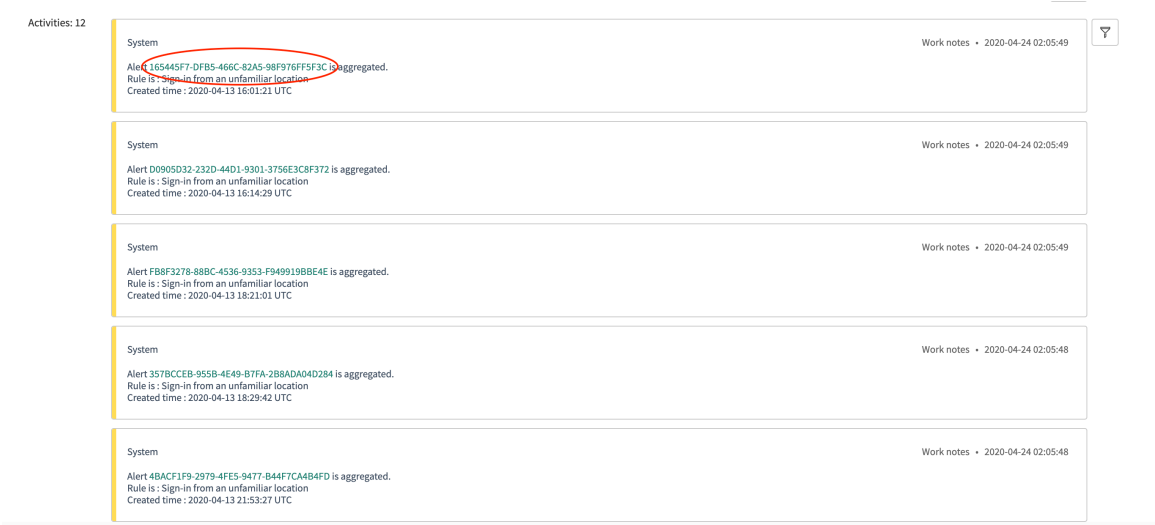
경보 수집 후 보안 인시던트 응답 양식

경보가 Microsoft Graph 보안 API 수집되면 보안 인시던트가 생성되고 해당 업데이트가 보안 인시던트 기록에 적용됩니다.

작업 메모

에 설명된 보안 인시던트 응답 필드에 경보 매핑대로 경보 집계 기준에서 새 경보에 대한 작업 메모 기록 옵션을 선택한 경우 경보가 집계될 때 작업 메모가 게시됩니다.

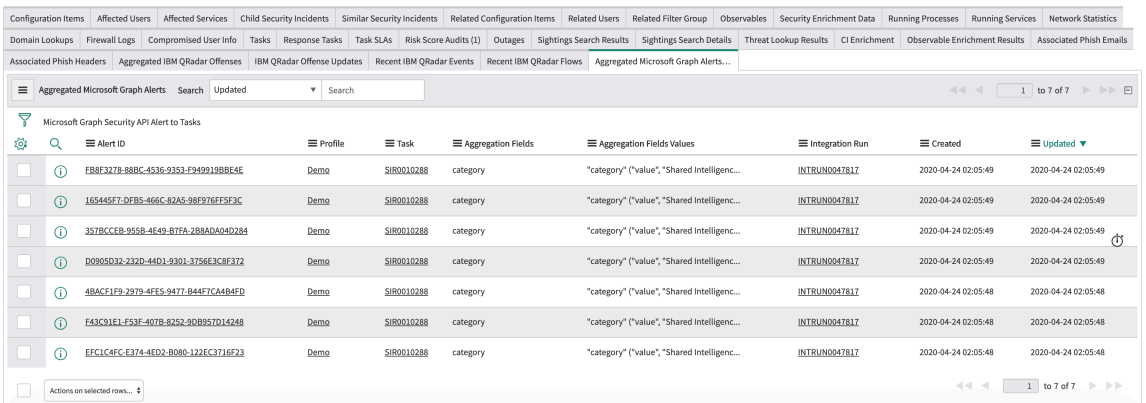
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



경보 링크를 클릭하여 원시 경보 데이터가 포함된 내부 경보 임포트 기록으로 이동합니다.

집계된 경보

클릭 관련 목록 〉 집계된 **Microsoft Graph** 보안 경보 보안 인시던트에 대해 집계된 경보를 보기 위해



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 보안 인시던트 생성: 목록에서 경보를 선택하고 작업 메뉴를 클릭한 다음 보안 인시던트 생성을 클릭합니다. 이 옵션은 경보에 대한 새 보안 인시던트를 생성하고 이 경보는 상위 보안 인시던트에서 세분화됩니다.
- 경보 기록 삭제: 목록에서 경보를 선택하고 작업 메뉴를 클릭한 다음 삭제를 클릭합니다. 이 옵션은 경보 레코드를 삭제합니다.

선택 사항: **Microsoft Graph** 보안 **API** 프로파일 복사

새 프로파일을 생성하는 대신 기존 프로파일 및 관련 설정을 복사합니다. 여러 프로필을 만드는 경우 기존 프로필의 설정을 다시 사용하려면 프로필을 복사하여 시간을 절약할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.admin

이 태스크 정보
sn_si.admin 역할을 가진 사용자가 프로파일을 복사하는 경우 프로파일 중복을 방지하기 위해 프로파일 이름이 처음에 수정됩니다. 또한 복사된 프로파일이 비활성화(false)되므로 컨피그레이션을 완료하기 전에 실수로 활성화되지 않습니다. 이미 미리 보고 확인한 보안 인시던트에 대해 프로파일을 복사하고 기존 맵을 사용합니다.

프로시저

1. 다음으로 이동 모두 〉 **Microsoft Graph** 보안 **API** 통합 〉 **Microsoft Graph** 보안 **API** 프로파일.
2. Microsoft Graph 보안 API 표시되는 프로파일 목록에서 복사할 프로파일을 선택하고 선택한 행에 대한 작업 선택 목록에서 복사를 클릭합니다.
   프로파일이 복사되어 목록에 표시됩니다. 복사본에는 매핑 및 일정 구성을 포함하여 원래 프로필의 모든 설정이 포함됩니다. 프로파일의 이름에는 사본이 포함되어 있습니다. 원본 프로파일이 활성화되었지만(true) 이 시점에서는 복사본이 비활성화됩니다(false). 복사된 프로파일의 값을 편집하고 필요에 따라 구성 설정이 새 프로파일에 적용되도록 이름을 바꿀 수 있습니다.

   기존 프로파일에서 새 프로파일로 설정을 복사했습니다. 프로파일을 활성화해야 하므로 활성 열 상태가 false로 설정됩니다.

다음에 수행할 작업
구성 단계를 완료한 후 새 프로파일을 활성화(활성화)하라는 메시지가 표시됩니다.

도메인 분리 및 **Microsoft Graph** 보안 **API** 경보 수집

이 애플리케이션에는 도메인 분리가 지원됩니다. 통합은 Microsoft Graph 보안 API Microsoft Graph 보안 제공자로부터 경보를 수집하고 보안 인시던트를 자동으로 생성합니다. 도메인 분리를 사용하여 데이터, 프로세스 및 관리 작업을 도메인이라는 논리적 그룹으로 분할할 수 있습니다. 어떤 사용자가 데이터를 보고 액세스할 수 있는지를 포함하여 이러한 분리의 여러 측면을 제어할 수 있습니다.

지원 수준: 기본

- 비즈니스 논리: 데이터가 애플리케이션의 서비스 제공자 사용 사례에 적합한 도메인으로 들어가도록 보장합니다.
- 애플리케이션은 런타임에서 도메인 분리를 지원합니다. 도메인 분리에는 사용자 인터페이스, 캐시 키, 보고서, 롤업, 집계 등에서의 분리가 포함됩니다.
- 인스턴스 소유자는 여러 테넌트에서 작동하도록 애플리케이션을 설정해야 합니다.

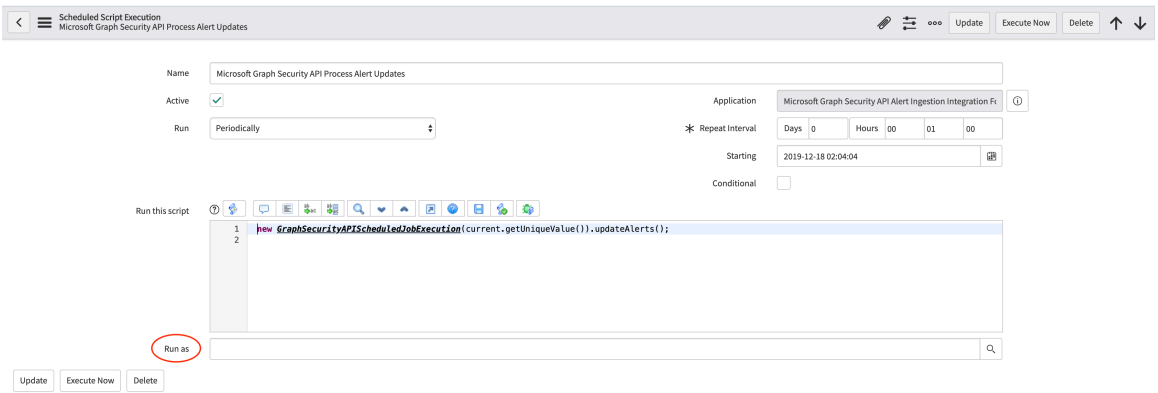
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

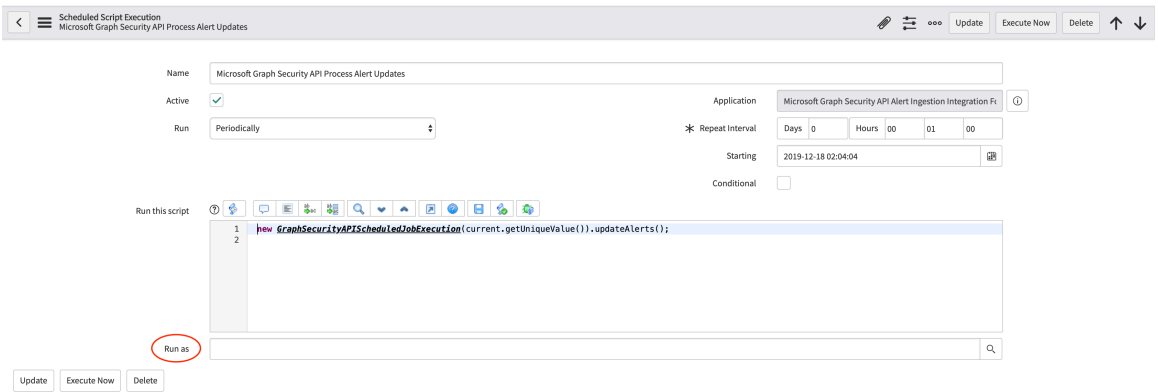
샘플 사용 사례: 서비스 제공자(SP)가 채팅을 사용하여 테넌트 고객의 메시지에 응답할 때 고객이 SP의 응답을 볼 수 있어야 합니다.

지원 수준에 대한 자세한 내용은 도메인 분리를 위한 애플리케이션 지원 을 참조하십시오.

에서 도메인 분리가 작동하는 방식 **Microsoft Graph** 보안 **API**

도메인 분리를 수행하려면 프로파일 프로세스 및 SIR 프로세스 경보 업데이트 예약된 작업을 복제 Microsoft Graph 보안 API 하고 사용자로 실행을 변경합니다. 기본적으로 시스템 사용자는 이러한 예약된 작업을 실행합니다. 해당 도메인에서 sn_si.admin 역할을 가진 사용자로 실행을 변경하고 예약된 작업을 실행합니다.





관련 정보

서비스 제공자용 도메인 분리

Microsoft Graph 보안 **API** 통합에서 플로우 디자이너 및 통합 허브 사용량

Flow Designer와 통합 허브 기능을 사용하여 통합의 Microsoft Graph 보안 API 일부로 여러 하위 플로우와 작업이 빌드되었습니다.

다음과 같은 하위 플로우를 사용할 수 있습니다.

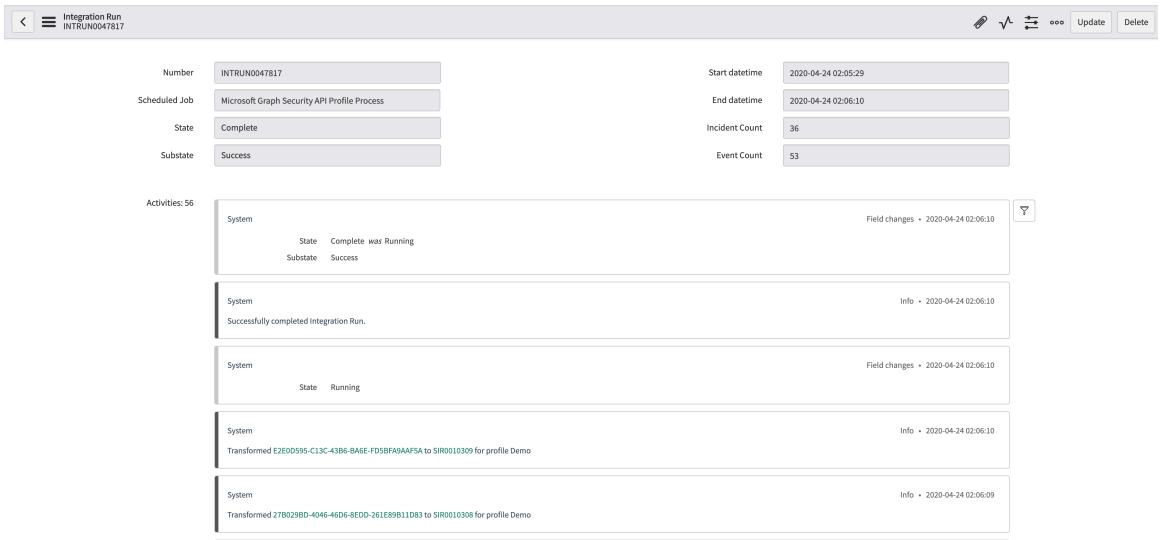
- Microsoft Graph 보안 API 구성 확인: 구성 타일에서 초기 설정에서 자격 증명의 유효성을 검사하는 데 사용됩니다.
- REST 호출 대상 Microsoft Graph 보안 API: REST 호출을 사용하여 Microsoft Graph 보안 API와의 상호 작용에 사용됩니다.
- 샘플 경보 검색: 샘플 데이터를 가져오기 위해 프로파일 설정의 매핑 섹션에서 사용됩니다. 이 하위 플로우는 비동기식으로 트리거됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Microsoft Graph 보안 API 통합 문제 해결

이 섹션에서는 경보 수집 통합과 Microsoft Graph 보안 API 관련된 중요한 문제 해결 팁과 자주 묻는 질문을 다룹니다.

- 통합 실행: 예약된 작업이 실행을 시작하면 로그, 오류 및 경고가 포함된 통합 실행 기록이 표시됩니다. 끌어온 경보 수와 예약된 작업 실행에서 생성된 인시던트 수도 표시됩니다. sn_si.analyst 역할을 가진 사용자는 통합 실행 중에 오류/프로파일 끌어오기에 실패한 경우 확인할 수 있습니다. sn_si.analyst 역할을 가진 사용자는 발생한 오류에 대해 sn_event_ingestion_integration_run 테이블을 확인할 수 있습니다. 통합 문제를 해결하려면 먼저 통합 실행을 확인해야 합니다. 오류는 예약된 작업 실행 every every scheduled job에 대한 통합 실행 기록에 작업 메모로 기록됩니다.



- 불완전한 프로필: 프로필을 구성하는 동안 추가 옵션()SIR 인시던트 상태에 따라 경보 업데이트 및 종결을 자동화 섹션에서 마침 단추를 클릭하여 프로필이 수집 대기 중임을 나타내는 대기 상태로 이동되도록 해야 합니다.
- 프로파일 확인: 통합이 올바르게 작동하는지 확인하려면 프로파일 상태, 프로파일의 마지막 끌어온 날짜, 경보 임포트 테이블, 작업 테이블 기록에 대한 경보를 확인합니다.
- **SSL** 문제: 를 Microsoft Graph 보안 API통해 연결할 때 인스턴스에 만료되지 않은 유효한 CA 인증서가 있는지 확인합니다. RSA 또는 자체 인증서를 플랫폼으로 임포트하고 인증서의 일반 이름이 호스트 이름과 일치하는지 확인할 수 있습니다. 자세한 내용은 KB0778285 참조하십시오.

Palo Alto Networks - AutoFocus 통합

통합 기본 시스템에는 Palo Alto Networks - AutoFocus 인스턴스와 통합하는 Palo Alto Networks - AutoFocus 데 사용할 수 있는 워크플로우 및 일련의 워크플로우 활동이 포함되어 있습니다.

탐색	설정
보안 인시던트 응답 통합	통합 활성화 및 구성 Palo Alto Networks - AutoFocus
사용	개발

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- Security Operations Palo Alto Networks - 값 워크플로우 확인 및 차단
- 자동 포커스 세션 정보 가져오기 보강 플로우
- ServiceNow 보안 운영 통합 개발 가이드라인
- 통합 작성을 위한 팁
- 개발자 교육
- 개발자 설명서
- 애플리케이션과 함께 설치되는 구성요소 찾기

문제 해결 및 도움받기

- 통합 문제 해결
- 보안 운영 커뮤니티에서 질문 또는 답변하기
- 알려진 오류 포털에서 알려진 오류 문서 검색

- 연락처 고객 서비스 및 지원

통합 활성화 및 구성 **Palo Alto Networks - AutoFocus**

통합 구성 기능을 사용하면 를 비롯한 Palo Alto Networks - AutoFocus타사 보안 통합을 빠르게 활성화하고 설정할 수 있습니다. 를 Palo Alto Networks - AutoFocus사용하려면 먼저 에서 ServiceNow Store다운로드해야 합니다.

시작하기 전에
필요한 역할: sn_si_admin

프로시저

1. 에서 처음으로 애플리케이션 ServiceNow Store 다운로드.
2. 설치가 완료되면 Palo Alto Networks 지원 사이트에 액세스하여 API 키를 가져옵니다.
3. 인스턴스에서 다음으로 이동합니다. 보안 운영 〉 통합 구성.
4. Palo Alto Networks AutoFocus 카드에서 구성을 클릭합니다.
5. Palo Alto Networks 지원 사이트에서 받은 **API** 키를 입력(또는 붙여넣기)합니다.
6. 제출을 클릭합니다.

자동 포커스 세션 정보 가져오기 보강 플로우

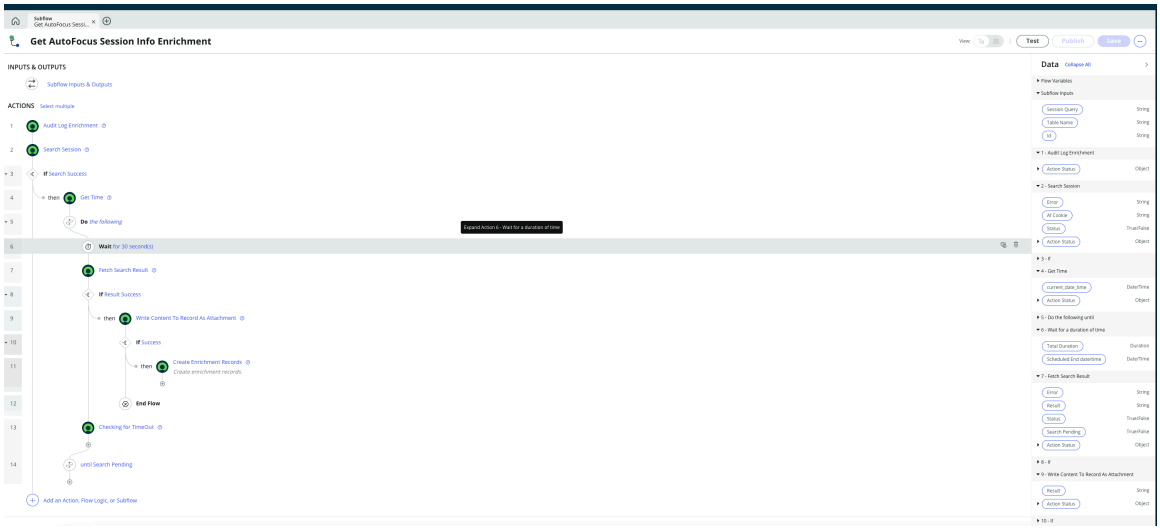
Security Operations Palo Alto Networks - Get AutoFocus Session Info Enrichment 플로우가 실행되면 지정된 소스 IP에 대한 정보를 수집하기 위해 AutoFocus를 사용하여 검색 쿼리를 큐에 대기합니다. AutoFocus에 해당 IP 주소에서 시작된 이전 세션에 대한 지식이 있는 경우 JSON 형식의 보고서가 반환됩니다.

시작하기 전에
필요한 역할: sn_si.analyst

이 태스크 정보
보안 운영 **Palo Alto Networks -** 자동 포커스 세션 정보 가져오기 보강 플로우는 보안 인시던트의 소스 **IP** 필드가 수정되고 기록이 업데이트될 때 실행됩니다. 플로우는 IP 주소를 가져오고 AutoFocus에 쿼리 요청을 제출합니다. AutoFocus가 이전에 IP 주소에서 시작된 세션을 식별한 경우 JSON 형식의 보고서가 반환됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 운영 **Palo Alto Networks - Wildfire** 데이터 보강 플로우 가져오기



프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 열린 인시던트 표시.
2. **Indicators of** Compromise(침해 지표) 탭을 클릭하고 **Source** IP(소스 **IP**) 필드를 채웁니다.
3. 업데이트를 클릭합니다.
   AutoFocus는 IP 주소에서 정보를 스캔하고 JSON 형식의 텍스트 파일이 보안 인시던트에 첨부됩니다.

   이 통합과 관련된 작업은 여기에 설명되어 있습니다. 다른 작업에 대한 자세한 내용은 다음 문서를 참조하십시오 일반 Security Operations 통합 플로우 및 오케스트레이션 활동.

AutoFocus 검색 세션 작업

AutoFocus 검색 세션 플로우 작업은 보안 인시던트에 할당된 IP 주소에서 AutoFocus로 정보를 업로드하고 검색 쿼리를 위해 큐에 대기시킵니다.

입력 변수

> **주:**
>
> 작업이 실행되면 지정된 소스 IP에 대한 정보를 수집하기 위해 AutoFocus를 사용하여 검색 쿼리를 큐에 대기합니다. AutoFocus가 이전에 해당 IP 주소에서 시작된 세션을 식별한 경우 JSON 형식의 보고서가 반환됩니다.

입력 변수는 작업의 초기 동작을 결정합니다.

입력 변수

변수	설명
searchSessionQuery〔문자열〕	세션 정보에 대한 검색 쿼리입니다.

검색 결과 가져오기 작업

검색 결과 가져오기 플로우 작업은 쿠키로 식별된 검색 결과를 **AutoFocus** 검색 세션 작업으로 시작된 검색 쿼리로 가져옵니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

입력 변수

입력 변수는 작업의 초기 동작을 결정합니다.

입력 변수

변수	설명
afcookie 〔문자열〕	에 의해 AutoFocus 검색 세션 작업생성된 검색 요청에 대한 AutoFocus 쿠키입니다.

출력 변수

출력 변수에는 후속 작업에서 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
searchPending 〔부울〕	검색 요청이 AutoFocus에서 계속 처리되는 경우 예입니다.
결과 〔string〕	검색 결과 데이터입니다.
status 〔부울〕	검색이 완료되고 결과가 성공적으로 생성되면 True입니다.
오류 〔string〕	작업에서 발생한 오류(있는 경우)입니다.

Palo Alto Networks - Firewall 통합

통합을 MID 서버 수행하려면 Palo Alto Networks - Firewall SSH 자격 증명을 사용하여 설정해야 합니다. 방화벽이 아직 설정되지 않은 경우 하나를 추가합니다.

탐색	설정
보안 인시던트 응답 통합	• Palo Alto Networks 방화벽 통합 활성화 및 구성 • MID 서버에 대한 SSH 자격 증명 설정
사용	**개발**
Palo Alto Networks 방화벽 시작 관리자 워크플로우	• ServiceNow 보안 운영 통합 개발 가이드라인 • 통합 작성을 위한 팁 • 개발자 교육 • 개발자 설명서 • 애플리케이션과 함께 설치되는 구성요소 찾기

문제 해결 및 도움받기

- 통합 문제 해결
- 보안 운영 커뮤니티에서 질문 또는 답변하기

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 알려진 오류 포털에서 알려진 오류 문서 검색
- 연락처 고객 서비스 및 지원

MID 서버에 대한 **SSH** 자격 증명 설정

Palo Alto Networks 방화벽은 MID 서버에 API 호출을 보냅니다. 따라서 MID 서버에 대해 SSH 자격 증명이 생성되었는지 확인합니다.

시작하기 전에

- 오케스트레이션 플러그인을 활성화해야 합니다.

필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 〉 오케스트레이션 〉 자격 증명 및 연결 〉 자격 증명.
2. 새로 만들기를 클릭합니다.
3. 인터셉터 화면에서 **SSH** 자격 증명을 클릭합니다.
4. 필요에 따라, 필드를 채웁니다.

SSH 자격 증명

필드	설명
이름	자격 증명의 이름을 입력합니다.
활성	이 자격 증명을 활성화하려면 이 확인란을 선택합니다.
적용 대상	모든 **MID** 서버 또는 특정 **MID** 서버를 선택합니다.
MID 서버	특정 **MID** 서버를 선택한 경우 잠금 아이콘을 클릭하고 이러한 자격 증명을 적용할 MID 서버를 선택합니다.
순서	서버에서 자격 증명을 시도하는 순서를 선택합니다. 더 작은 숫자가 먼저 시도됩니다.
사용자 이름	이 자격 증명과 연결된 사용자의 사용자 이름을 입력합니다(있는 경우).
암호	사용자 이름을 입력한 경우 사용자의 암호를 입력합니다.
태그	검색 기준에 사용할 태그를 입력합니다. 태그 필드에는 이름과 같은 값이 포함되어야 합니다.

Palo Alto Networks 방화벽 통합 활성화 및 구성

통합 구성 기능을 사용하면 를 비롯한 Palo Alto Networks - Firewall타사 보안 통합을 빠르게 활성화하고 설정할 수 있습니다. 를 Palo Alto Networks - Firewall사용하려면 먼저 에서 ServiceNow Store다운로드해야 합니다.

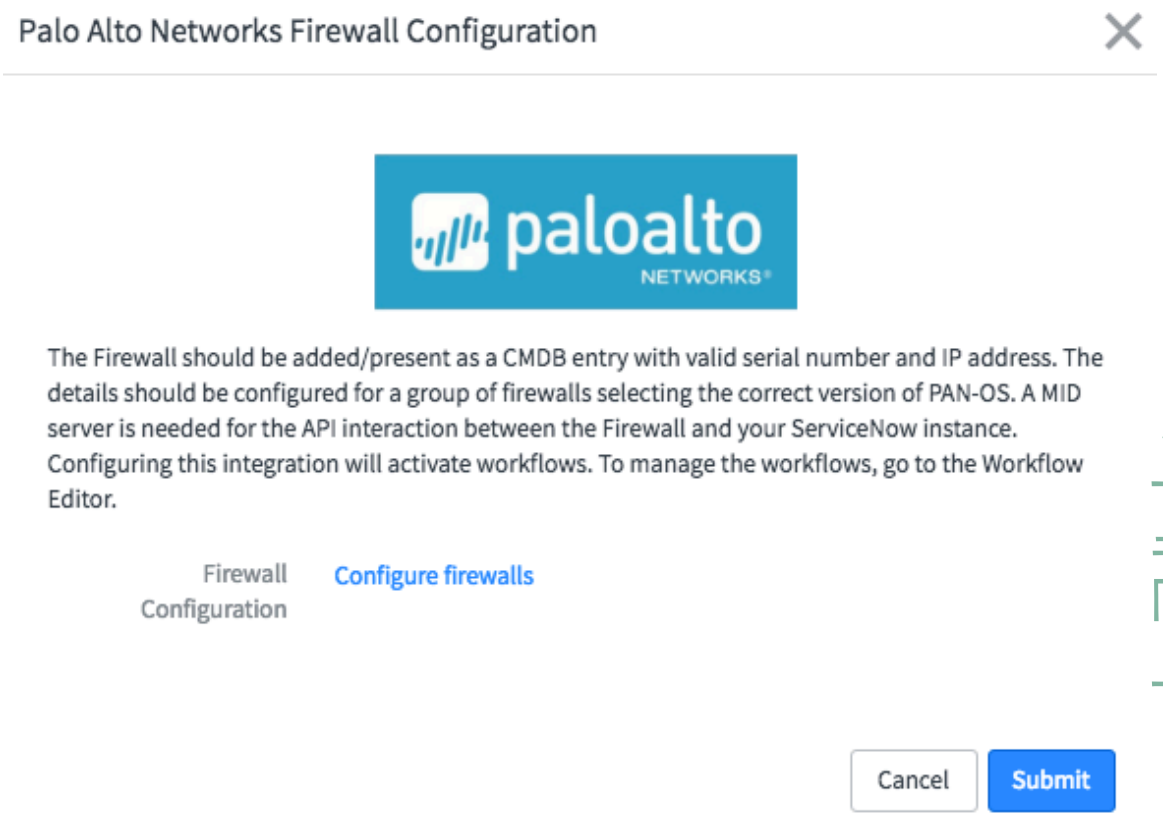
시작하기 전에

필요한 역할: sn_si_admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 통합을 활성화하고 구성하기 전에 Palo Alto Networks 방화벽 대시보드에 액세스합니다.
   방화벽 차단에 사용하는 IP 동적 목록, URL 동적 목록 또는 도메인 동적 목록의 이름을 기록해 둡니다.
2. 에서 통합을 다운로드합니다. ServiceNow Store.
3. 설치가 완료되면 보안 운영 〉 통합 구성.
   사용 가능한 보안 통합은 일련의 카드로 표시됩니다.
4. Palo Alto Networks 방화벽 카드에서 Configure(구성)를 클릭합니다.



5. 방화벽 구성을 클릭합니다.
6. 방화벽 구성 화면에서 새로 만들기를 클릭합니다.
7. 양식의 필드에 적절히 입력합니다.

필드	설명
방화벽	잠금 아이콘을 클릭하고 구성할 방화벽을 선택합니다.
방화벽 버전	Palo Alto Networks 방화벽 버전을 선택합니다.**PAN-OS-7.1** 이 권장 버전입니다. 이전 버전을 선택하면 일관되지 않은 결과가 반환 될 수 있습니다.
사용자 이름	REST 엔드포인트를 통해 방화벽에 연결할 때 사용할 사용자 이름을 입력합니다.
암호	연결하는 사용자의 암호를 입력합니다.
IP 동적 목록	IP 주소에 사용하는 외부 동적 목록 또는 동적 차단 목록의 이름을 입력합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
URL 동적 목록	URL에 사용하는 외부 동적 목록 또는 동적 차단 목록의 이름을 입력합니다.
도메인 동적 목록	도메인에 사용하는 외부 동적 목록 또는 동적 차단 목록의 이름을 입력합니다.

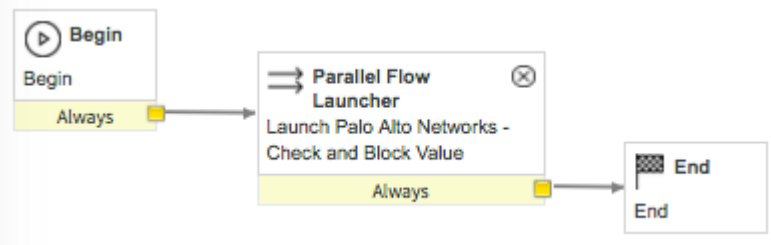
8. 제출을 클릭합니다.

Palo Alto Networks 방화벽 시작 관리자 워크플로우

보안 운영 통합 **Palo Alto Networks** 방화벽 시작 관리자 워크플로우는 보안 운영 통합 **-** 차단 요청 기능 워크플로우로 시작된 Palo Alto Networks 방화벽 구현입니다.

시작하기 전에
필요한 역할: sn_si.analyst

이 태스크 정보
워크플로우 프로세스 활동에는 다음이Security Operations Palo Alto Networks - 값 워크플로우 확인 및 차단 포함됩니다.



Security Operations Palo Alto Networks - 값 워크플로우 확인 및 차단

잠재적 위협을 식별하기 위해 보안 인시던트가 생성되고 분류되면 **Security Operations Palo Alto Networks -** 값 확인 및 차단 워크플로우를 통해 에 Palo Alto Networks - Firewall정의된 외부 동적 목록을 사용하여 IP 주소, URL 및 도메인을 자동으로 확인하고 업데이트할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.analyst

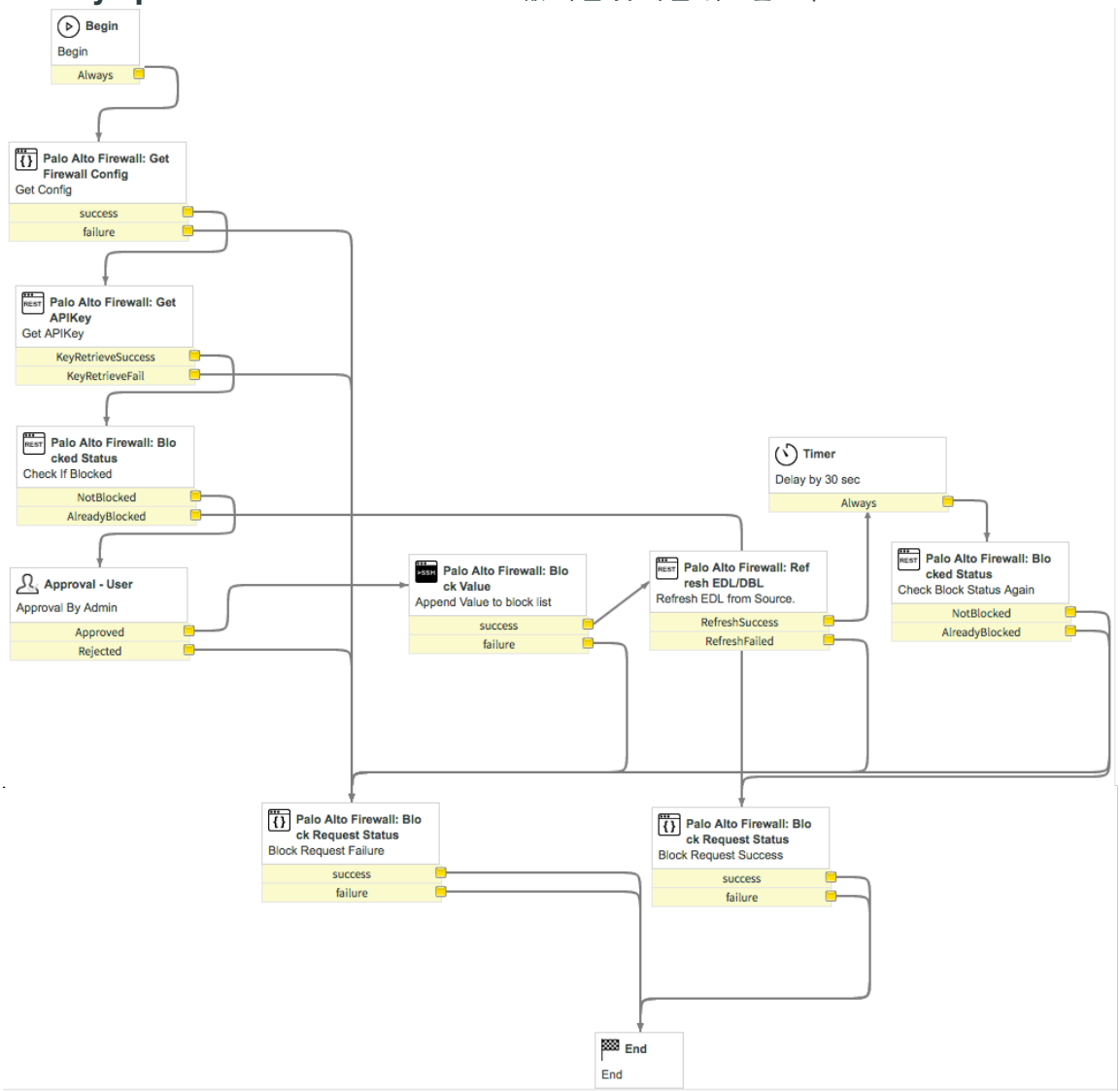
이 태스크 정보
방화벽 차단 요청이 제출되면 **Security Operations Palo Alto Networks -** 값 확인 및 차단 워크플로우가 실행됩니다. 차단 요청은 사용할 방화벽, 확인 및 차단할 옵저버블 유형(필요한 경우) 및 블록 값을 지정합니다. 즉, 문제의 IP 주소, URL 또는 도메인입니다.

워크플로우 실행 중에 **Palo Alto Networks** 통합 〉 방화벽 〉 명령 실행됩니다. Show type 명령(예: Show-IP-ExternalDynamicList)은 값이 방화벽에 있는지 여부를 확인합니다. 새로 고침 유형 명령(예: Refresh-IP-ExternalDynamicList)은 방화벽에 없는 값을 차단 목록에 추가합니다.

차단 상태 활동이 실행된 후 워크플로우를 진행하려면 시스템 관리자의 승인이 필요합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Security Operations Palo Alto Networks - 값 확인 및 차단 워크플로우



프로시저

1. 다음으로 이동 **Palo Alto Networks** 통합 〉 방화벽 〉 요청 차단.
2. 새로 만들기를 클릭합니다.
3. 양식의 필드에 적절히 입력합니다.

필드	설명
방화벽	사용할 방화벽을 선택합니다.
블록 유형	확인할 값의 유형을 선택합니다. ○ IP ○ URL ○ DOMAIN
블록 값	방화벽에서 확인할 선택한 유형의 값을 입력합니다.

4. 제출을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Palo Alto 방화벽 - 요청 상태 차단 활동

이 활동은 방화벽 차단 요청 상태를 성공 또는 실패로 설정하기 위해 다른 활동에서 호출됩니다.

입력 변수

입력 변수는 활동의 초기 동작을 결정합니다.

입력 변수

변수	설명
firewallBlockRequestSysid 〔문자열〕	방화벽 차단 요청의 시스템 ID입니다. 이 입력 변수는 필수입니다.
상태 〔string〕	새로 고침 작업이 성공했는지 또는 실패했는지 여부를 나타냅니다.

출력 변수

출력 변수에는 후속 활동에 사용할 수 있는 데이터가 포함됩니다. 출력은 방화벽 구성의 데이터와 동적으로 생성된 데이터로 구성됩니다.

출력 변수

변수	설명
결과 〔string〕	새로 고침 작업의 성공 또는 실패 여부를 나타냅니다.

Palo Alto 방화벽 - 블록 값 활동

워크플로우가 방화벽에 없는 값을 식별하면 승인을 위해 레코드가 라우팅됩니다. 승인 시 이 활동은 SSH 자격 증명을 통해 MID 서버에 연결하고 방화벽 외부 차단 목록에 값을 추가하는 스크립트를 호출합니다.

입력 변수

입력 변수는 활동의 초기 동작을 결정합니다.

> **주:**
> 이 활동에 대한 입력 변수를 수동으로 입력한 다음 워크플로우를 게시해야 합니다.
> 워크플로우가 게시되지 않으면 관리자가 아닌 사용자에 대한 입력 변수가 저장되지 않습니다.

입력 변수

변수	설명
toBeBlockedValue 〔문자열〕	아직 없는 경우 EDL에 추가할 값입니다. 이 입력 변수는 필수입니다.
typeToBeBlocked 〔문자열〕	차단할 값의 유형입니다(IP, URL 또는 도메인). 이 입력 변수는 필수입니다.
targetHost 〔문자열〕	스크립트가 실행되는 MID 서버입니다.
SSHCredentialTag 〔문자열〕	MID 서버에 정의된 SSH 자격 증명 태그입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

입력 변수

변수	설명
scriptCommand〔문자열〕	EDL에 값을 추가하는 데 사용되는 AppendValueToList.sh 스크립트입니다. MID 서버에 대한 전체 경로가 필요합니다.

출력 변수

출력 변수에는 후속 활동에 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
결과〔string〕	결과는 EDL로 전달됩니다.

Palo Alto 방화벽 - 차단 상태 활동

이 활동은 값(IP, URL 또는 도메인)이 방화벽의 해당 EDL/DBL(외부 동적 목록/동적 차단 목록)에 포함되어 있는지 확인합니다. EDL/DBL 세부 정보는 운영 명령을 사용하여 방화벽에서 가져오며 값이 방화벽에서 차단되었는지 확인하기 위한 루틴이 수행됩니다.

입력 변수

입력 변수는 활동의 초기 동작을 결정합니다. 나열된 모든 입력 변수 항목은 필수입니다.

입력 변수

변수	설명
valueToBeChecked〔문자열〕	차단 요청의 값입니다.
showEDLDetailsCommand〔문자열〕	값이 방화벽에 있는지 확인하는 데 사용되는 외부 동적 목록 명령입니다.
FirewallIpAddress〔문자열〕	사용된 방화벽의 IP 주소입니다.
FirewallApiKey〔문자열〕	방화벽 API 키입니다.

출력 변수

출력 변수에는 후속 활동에 사용할 수 있는 데이터가 포함됩니다. 출력은 방화벽 구성의 데이터와 Palo Alto 방화벽 운영 명령 API 메시지를 사용하여 동적으로 생성된 데이터로 구성됩니다.

출력 변수

변수	설명
명령 결과〔문자열〕	show EDL Details 명령에 대한 방화벽의 결과입니다.
blockedStatus〔부울〕	True는 차단됨을 나타냅니다. False는 차단되지 않음을 나타냅니다.
명령 응답〔문자열〕	show EDL Details 명령에 대해 방화벽에서 가져온 응답 상태입니다.

Palo Alto 방화벽: **API** 키 가져오기 작업

이 작업은 방화벽에서 API 키를 검색합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

입력 변수

입력 변수는 작업의 초기 동작을 결정합니다. 나열된 모든 입력 변수 항목은 필수입니다.

입력 변수

변수	설명
사용자 이름〔string〕	방화벽 관리자의 사용자 이름입니다.
암호〔string〕	방화벽 관리자 암호입니다.
FirewallIpAddress〔문자열〕	방화벽의 IP 주소입니다.

출력 변수

출력 변수에는 후속 작업에서 사용할 수 있는 데이터가 포함됩니다. 출력은 방화벽 구성의 데이터와 동적으로 생성된 데이터로 구성됩니다.

출력 변수

변수	설명
APIKey〔문자열〕	방화벽 API 키입니다.

Palo Alto 방화벽: 방화벽 구성 작업 가져오기

Palo Alto 방화벽: 방화벽 구성 가져오기 플로우 작업은 데이터베이스에서 모든 관련 방화벽 구성 정보를 가져오고 후속 작업에서 사용할 수 있도록 합니다.

입력 변수

입력 변수는 작업의 초기 동작을 결정합니다.

입력 변수

변수	설명
firewallSysid〔문자열〕	방화벽의 시스템 ID입니다. 이 입력 변수는 필수입니다.
typeOfValueToBeBlocked〔문자열〕	방화벽에서 차단할 값의 유형입니다(IP, URL 또는 도메인).
firewallIPAddress〔문자열〕	방화벽의 IP 주소입니다.

출력 변수

출력 변수에는 후속 작업에서 사용할 수 있는 데이터가 포함됩니다. 출력은 방화벽 구성의 데이터와 동적으로 생성된 데이터로 구성됩니다.

출력 변수

변수	설명
ipEDLName〔문자열〕	IP 주소의 외부 동적 목록 이름입니다.
urlEDLName〔문자열〕	URL의 외부 동적 목록 이름입니다.
domainEDLName〔문자열〕	도메인의 외부 동적 목록 이름입니다.
firewallVersionSysId〔문자열〕	방화벽 버전의 시스템 ID입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

출력 변수

변수	설명
refreshEDLCommand〔문자열〕	소스에서 EDL을 새로 고치는 데 사용할 명령입니다.
ShowEDLDetailsCommand〔문자열〕	EDL 상세 정보를 가져오는 데 사용할 명령입니다.
status〔부울〕	예는 성공을 나타냅니다. False는 실패를 나타냅니다.
오류〔string〕	작업에서 발생한 오류(있는 경우)입니다.
엔드포인트〔Encrypted〕	데이터베이스의 암호화된 엔드포인트입니다.

Palo Alto 방화벽 **- EDL/DBL** 활동 새로 고침

이 활동은 방화벽에서 운영 명령을 실행하여 방화벽에 구성된 소스에서 외부 동적 목록을 새로 고칩니다. 이 작업의 출력은 새로 고침 작업이 큐에 대기되었는지 여부를 나타냅니다.

입력 변수

입력 변수는 활동의 초기 동작을 결정합니다. 나열된 모든 입력 변수 항목은 필수입니다.

입력 변수

변수	설명
FirewalllpAddress〔문자열〕	새로 고침할 방화벽의 IP 주소입니다.
FirewallApiKey〔문자열〕	새로 고침된 방화벽 API 키입니다.
FirewallCommand〔문자열〕	새로 고침 작업을 대기시키기 위해 실행할 운영 명령입니다.

출력 변수

출력 변수에는 후속 활동에 사용할 수 있는 데이터가 포함됩니다. 출력은 방화벽 구성의 데이터와 동적으로 생성된 데이터로 구성됩니다.

출력 변수

변수	설명
활동. Output.result〔문자열〕	새로 고침 작업이 실행을 위해 큐에 대기되었는지 여부(성공 또는 실패)를 나타내는 텍스트 문자열입니다.

로그 데이터 플로우 가져오기

, , 및 Palo Alto Networks - Firewall 활성화되면 보안 인시던트의 옵저버블에 대한 소스 IP가 변경될 때 보안 운영 **Palo Alto Networks -** 로그 데이터 가져오기 플로우가 자동으로 실행됩니다. 위협 인텔리전스보안 인시던트 응답

시작하기 전에

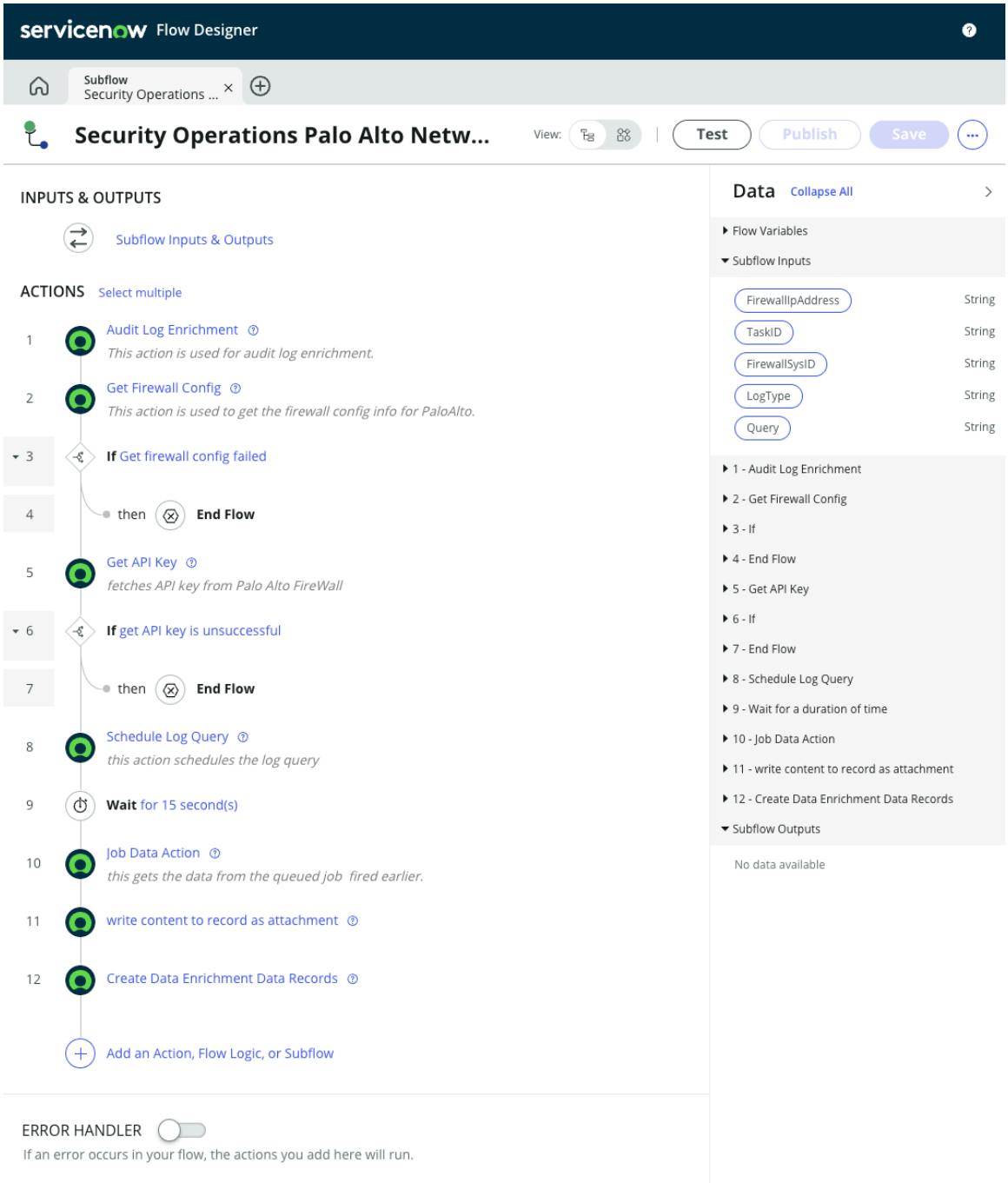
필요한 역할: sn_si.analyst

이 태스크 정보

플로우 실행 중에 데이터베이스에서 방화벽 구성 정보가 검색되고 방화벽에서 API 키가 검색됩니다. 로그 가져오기 작업은 방화벽에서 검색 쿼리를 큐에 대기시킵니다. 쿼리가 실행되면 방화벽에서 위협 로그 데이터를 검색하는 데 사용되는 작업 ID가 반환됩니다. 로그 데이터를 XML 파일로 보안 인시던트에 첨부합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 운영 **Palo Alto Networks -** 로그 데이터 가져오기 플로우



프로시저

1. 옵저버블이 포함된 보안 인시던트로 이동합니다.
2. 보안 인시던트 옵저버블 탭을 클릭합니다.
3. 소스 **IP**에서 IP 주소를 추가하거나 수정합니다.
4. 업데이트를 클릭합니다.
   보안 운영 **Palo Alto Networks -** 로그 데이터 가져오기 플로우가 실행되고 보강된 위협 로그 데이터가 보안 인시던트에 첨부됩니다. 또한 이 정보는 구문 분석되어 보강 데이터 탭 아래의 방화벽 로그 섹션에 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Palo Alto 방화벽: API 키 가져오기 작업

이 작업은 방화벽에서 API 키를 검색합니다.

입력 변수

입력 변수는 작업의 초기 동작을 결정합니다. 나열된 모든 입력 변수 항목은 필수입니다.

입력 변수

변수	설명
사용자 이름 〔string〕	방화벽 관리자의 사용자 이름입니다.
암호 〔string〕	방화벽 관리자 암호입니다.
FirewallIpAddress 〔문자열〕	방화벽의 IP 주소입니다.

출력 변수

출력 변수에는 후속 작업에서 사용할 수 있는 데이터가 포함됩니다. 출력은 방화벽 구성의 데이터와 동적으로 생성된 데이터로 구성됩니다.

출력 변수

변수	설명
APIKey 〔문자열〕	방화벽 API 키입니다.

Palo Alto 방화벽: 방화벽 구성 작업 가져오기

Palo Alto 방화벽: 방화벽 구성 가져오기 플로우 작업은 데이터베이스에서 모든 관련 방화벽 구성 정보를 가져오고 후속 작업에서 사용할 수 있도록 합니다.

입력 변수

입력 변수는 작업의 초기 동작을 결정합니다.

입력 변수

변수	설명
firewallSysid 〔문자열〕	방화벽의 시스템 ID입니다. 이 입력 변수는 필수입니다.
typeOfValueToBeBlocked 〔문자열〕	방화벽에서 차단할 값의 유형입니다(IP, URL 또는 도메인).
firewallIPAddress 〔문자열〕	방화벽의 IP 주소입니다.

출력 변수

출력 변수에는 후속 작업에서 사용할 수 있는 데이터가 포함됩니다. 출력은 방화벽 구성의 데이터와 동적으로 생성된 데이터로 구성됩니다.

출력 변수

변수	설명
ipEDLName 〔문자열〕	IP 주소의 외부 동적 목록 이름입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

출력 변수

변수	설명
urlEDLName 〔문자열〕	URL의 외부 동적 목록 이름입니다.
domainEDLName 〔문자열〕	도메인의 외부 동적 목록 이름입니다.
firewallVersionSysId 〔문자열〕	방화벽 버전의 시스템 ID입니다.
refreshEDLCommand 〔문자열〕	소스에서 EDL을 새로 고치는 데 사용할 명령입니다.
ShowEDLDetailsCommand 〔문자열〕	EDL 상세 정보를 가져오는 데 사용할 명령입니다.
status 〔부울〕	예는 성공을 나타냅니다. False는 실패를 나타냅니다.
오류 〔string〕	작업에서 발생한 오류(있는 경우)입니다.
엔드포인트 〔Encrypted〕	데이터베이스의 암호화된 엔드포인트입니다.

Palo Alto 방화벽 - 로그 작업 가져오기

Palo Alto 방화벽: 로그 가져오기 플로우 작업은 방화벽에 대한 쿼리를 예약하여 로그를 검색하고 로그 데이터를 검색하는 데 사용되는 JobID를 반환합니다.

입력 변수

입력 변수는 작업의 초기 동작을 결정합니다.

입력 변수

변수	설명
FirewallIpAddress 〔문자열〕	방화벽의 IP 주소입니다. 이 입력 변수는 필수입니다.
FirewallApiKey 〔문자열〕	방화벽의 API 액세스 키입니다. 이 입력 변수는 필수입니다.
FirewallLogType 〔문자열〕	검색할 로그 데이터의 유형입니다(위협으로 설정). 이 입력 변수는 필수입니다.
FirewallLogFilterQuery 〔문자열〕	방화벽에서 로그를 검색하기 위해 실행할 쿼리입니다. 이 입력 변수는 필수입니다.
LogDirection 〔문자열〕	로그를 가장 오래된 순(뒤로) 또는 최신 순(앞으로) 표시할지 여부를 지정합니다.
LogNumber 〔문자열〕	검색할 로그 수를 지정합니다.
LogSkipCount 〔문자열〕	로그 검색을 수행할 때 건너뛸 로그 수를 지정합니다.

출력 변수

출력 변수에는 후속 작업에서 사용할 수 있는 데이터가 포함됩니다. 출력은 방화벽 구성의 데이터와 동적으로 생성된 데이터로 구성됩니다.

출력 변수

변수	설명
QueuedJobID 〔문자열〕	방화벽에서 반환된 작업 ID입니다.
JobScheduled 〔문자열〕	작업을 방화벽으로 보냈는지 여부(성공 또는 실패)를 지정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

출력 변수

변수	설명
오류 〔string〕	반환된 모든 오류입니다.

Palo Alto 방화벽 - 작업 데이터 작업

Palo Alto 방화벽: 로그 가져오기 작업이 검색 쿼리를 대기하도록 방화벽에 보내고 작업이 실행되면 **Palo Alto** 방화벽: 작업 데이터 작업 작업이 방화벽에서 위협 로그 데이터를 검색합니다.

입력 변수

입력 변수는 작업의 초기 동작을 결정합니다. 모든 입력 필드는 필수입니다.

입력 변수

변수	설명
FirewalllpAddress 〔문자열〕	방화벽의 IP 주소입니다.
FirewallApiKey 〔문자열〕	방화벽의 API 액세스 키입니다.
JobID 〔문자열〕	큐에 대기 중인 작업의 ID입니다.

출력 변수

출력 변수에는 후속 작업에서 사용할 수 있는 데이터가 포함됩니다. 출력은 방화벽 구성의 데이터와 동적으로 생성된 데이터로 구성됩니다.

출력 변수

변수	설명
명령 상태 〔문자열〕	방화벽에서 데이터를 검색했는지 여부(성공 또는 실패)를 지정합니다.
JobData 〔문자열〕	방화벽에서 수집한 데이터입니다.
오류 〔string〕	반환된 모든 오류입니다.

Palo Alto Networks - WildFire 통합

Palo Alto Networks - WildFire 은 시스템 방화벽과 상호 작용하는 클라우드 기반 애플리케이션입니다.

탐색

보안 인시던트 응답 통합

설정

Palo Alto Networks - WildFire 활성화

사용

WildFire 데이터 보강 플로우 가져오기

개발

- ServiceNow 보안 운영 통합 개발 가이드라인
- 통합 작성을 위한 팁
- 개발자 교육

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 개발자 설명서
- 애플리케이션과 함께 설치되는 구성요소 찾기

문제 해결 및 도움받기

- 통합 문제 해결
- 보안 운영 커뮤니티에서 질문 또는 답변하기
- 알려진 오류 포털에서 알려진 오류 문서 검색

- 연락처 고객 서비스 및 지원

Palo Alto Networks - WildFire 활성화

Security Operations Palo Alto Networks - WildFire 통합을 사용하려면 먼저 에서 ServiceNow Store통합을 다운로드해야 합니다.

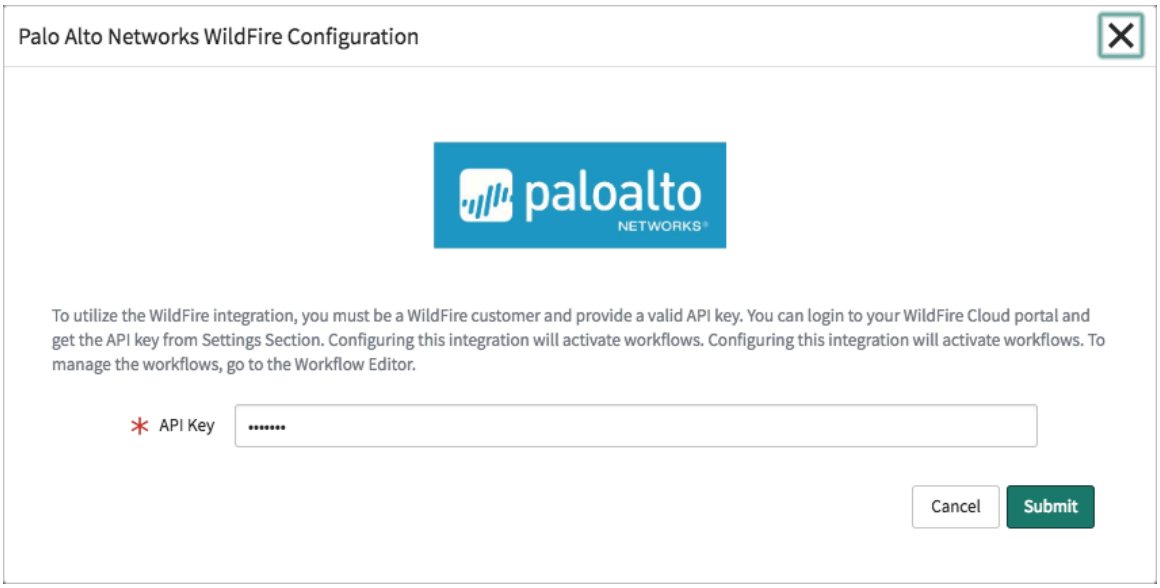
시작하기 전에
필요한 역할: 관리자

프로시저

1. 에서 통합을 다운로드합니다. ServiceNow Store.
2. 다음으로 이동 보안 운영 〉 통합 〉 통합 구성.
   사용 가능한 보안 통합은 일련의 카드로 표시됩니다.

3. 카드에서 Configure(구성)를 Carbon Black 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. API 키를 입력하고 제출을 클릭합니다.
   통합 구성 카드가 표시됩니다.
5. 통합 구성 카드의 원래 목록으로 돌아가려면 구성 표시 드롭다운 목록에서 아니요를 선택합니다.

WildFire 데이터 보강 플로우 가져오기

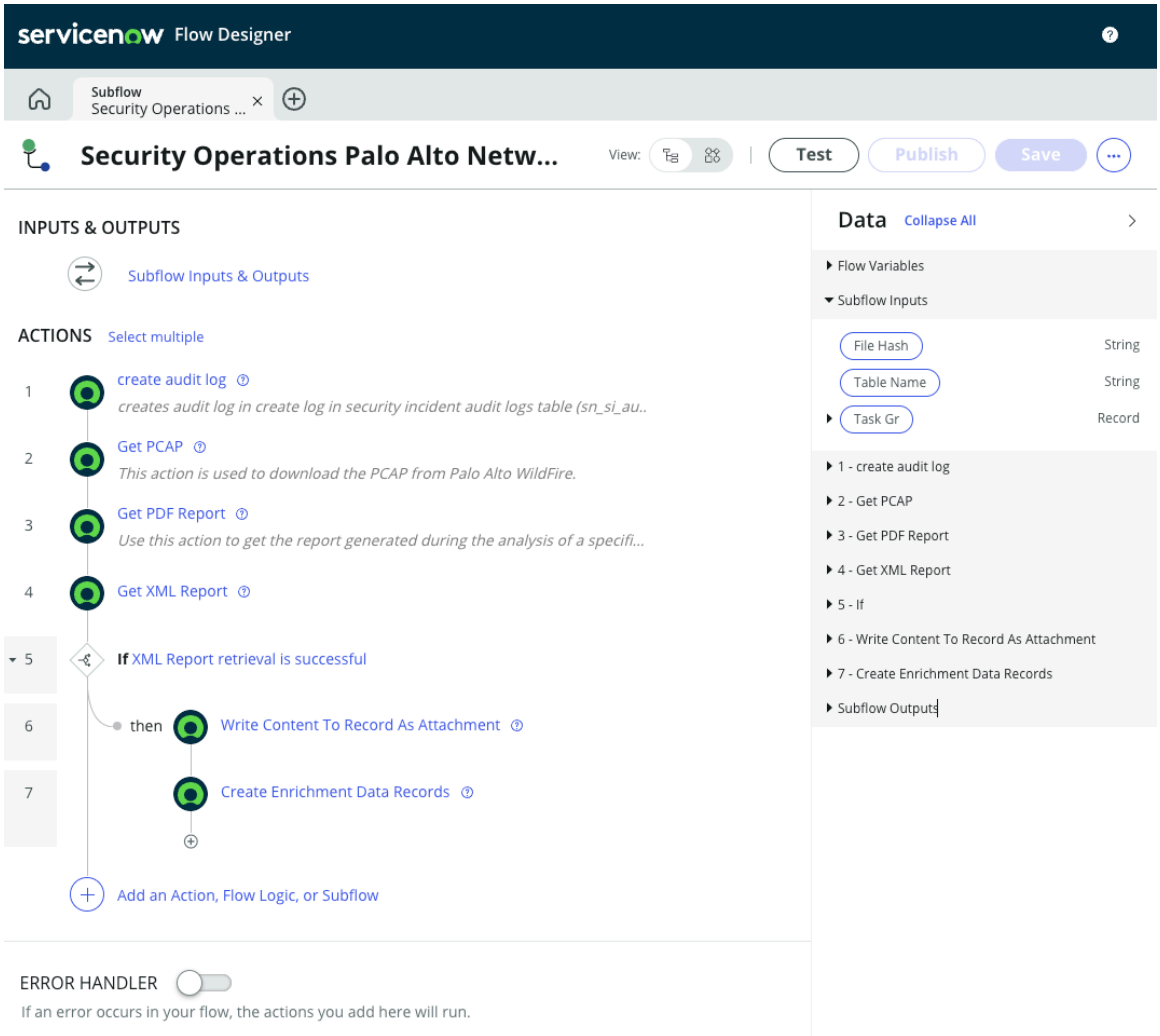
Security Operations Palo Alto Networks - Get WildFire Data Enrichment 플로우가 실행되면 해시 파일이 WildFire에 업로드됩니다. 데이터가 보강되고 잠재적인 맬웨어 공격을 처리하는 데 도움이 되도록 보고서가 인스턴스에 다운로드됩니다.

시작하기 전에
필요한 역할: sn_si.analyst

이 태스크 정보
보안 운영 **Palo Alto Networks - WildFire** 데이터 보강 가져오기 플로우는 Palo Alto Network Firewall 애플리케이션에서 수신한 경보로 인해 보안 인시던트가 생성될 때 실행됩니다. 방화벽에서 받은 이메일 알림의 맬웨어 해시가 보안 인시던트의 **IoC** 탭에 입력되고 기록이 업데이트됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 운영 **Palo Alto Networks - WildFire** 데이터 보강 플로우 가져오기



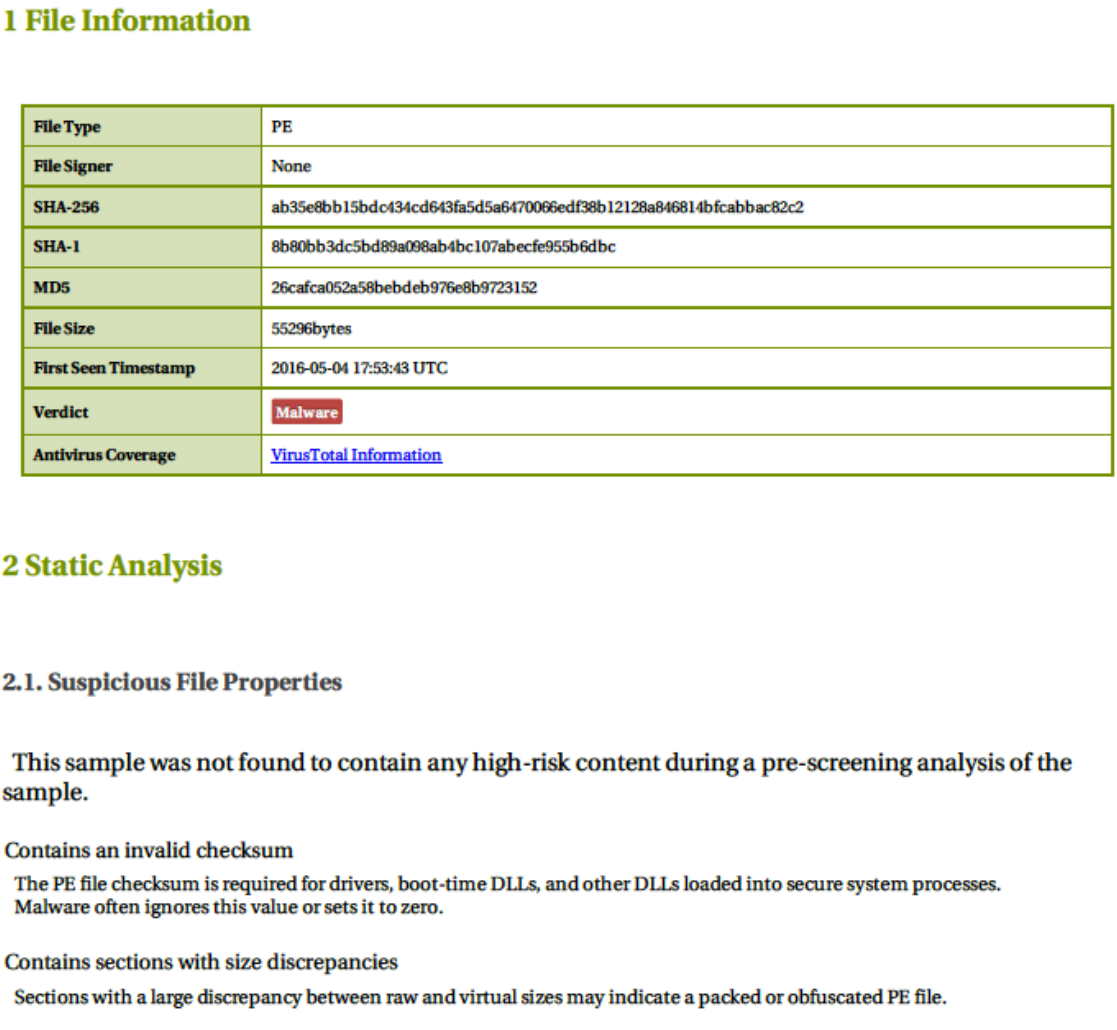
프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 열린 인시던트 표시.
2. 방화벽에서 받은 이메일 알림에 따라 생성된 보안 인시던트를 찾아 엽니다.
3. 침해 표시기 탭을 클릭하고 맬웨어 해시를 경보에서 받은 해시로 채웁니다.
4. 업데이트를 클릭합니다.
   플로우로 인해 해시 파일이 데이터가 보강되는 WildFire에 업로드됩니다. PDF 및 XML 형식의 보고서는 잠재적인 맬웨어 공격을 처리하는 데 도움이 되도록 인스턴스의 기록(보안 인시던트 또는 IoC)에 첨부됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
보강된 데이터에 패킷 캡처 정보가 포함된 경우 PCAP 정보도 다운로드됩니다. PCAP 데이터는 파일이 수행한 작업을 캡처합니다. 예를 들어 파일이 연결된 서버를 보고할 수 있습니다. PCAP 파일을 보려면 Wireshark 와 같은 패킷 분석기가 필요합니다.

Wildfire에서 생성된 샘플 **PDF**



1 File Information

File Type	PE
File Signer	None
SHA-256	ab35e8bb15bdc434cd643fa5d5a6470066edf38b12128a846814bfcabbac82c2
SHA-1	8b80bb3dc5bd89a098ab4bc107abecfe955b6dbc
MD5	26cafca052a58bebdeb976e8b9723152
File Size	55296bytes
First Seen Timestamp	2016-05-04 17:53:43 UTC
Verdict	Malware
Antivirus Coverage	VirusTotal Information

2 Static Analysis

2.1. Suspicious File Properties

This sample was not found to contain any high-risk content during a pre-screening analysis of the sample.

Contains an invalid checksum

The PE file checksum is required for drivers, boot-time DLLs, and other DLLs loaded into secure system processes. Malware often ignores this value or sets it to zero.

Contains sections with size discrepancies

Sections with a large discrepancy between raw and virtual sizes may indicate a packed or obfuscated PE file.

WildFire - PCAP 작업 가져오기

WildFire: Get PCAP 플로우 작업은 WildFire에서 지정된 파일 해시를 분석하는 동안 생성된 PCAP(패킷 캡처) 정보를 가져옵니다. 이 작업의 결과는 **TableName** 및 **RecordId**로 식별되는 특정 기록에 첨부됩니다.

입력 변수

입력 변수는 작업의 초기 동작을 결정합니다.

입력 변수

변수	설명
FileSHA256Hash 〔문자열〕	Palo Alto Network Firewall 애플리케이션에서 받은 파일의 해시입니다.
테이블 이름 〔문자열〕	영향을 받는 테이블입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

입력 변수

변수	설명
RecordId〔문자열〕	업데이트 중인 보안 인시던트 또는 IoC입니다.

출력 변수

출력 변수에는 후속 작업에서 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
commandStatus〔부울〕	결과를 성공적으로 가져와서 첨부하면 True입니다.
errorMessage	작업에서 발생한 오류(있는 경우)입니다.

WildFire - PDF 보고서 작업 가져오기

WildFire: PDF 보고서 가져오기 플로우 작업은 WildFire에서 지정된 파일 해시를 분석하는 동안 생성된 보고서를 PDF 형식으로 가져옵니다. 이 작업의 결과는 **TableName** 및 **RecordId**로 식별되는 특정 기록에 첨부됩니다.

입력 변수

입력 변수는 작업의 초기 동작을 결정합니다.

입력 변수

변수	설명
테이블 이름〔문자열〕	영향을 받는 테이블입니다.
FileSHA256Hash〔문자열〕	Palo Alto Network Firewall 애플리케이션에서 받은 파일의 해시입니다.
RecordId〔문자열〕	업데이트 중인 보안 인시던트 또는 IoC입니다.

출력 변수

출력 변수에는 후속 작업에서 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
commandStatus〔부울〕	결과를 성공적으로 가져와서 첨부하면 True입니다.
errorMessage	작업에서 발생한 오류(있는 경우)입니다.

WildFire - XML 보고서 작업 가져오기

WildFire: XML 보고서 가져오기 플로우 작업은 WildFire에서 지정된 파일 해시를 분석하는 동안 생성된 보고서를 XML 형식으로 가져옵니다. 이 작업의 결과는 **TableName** 및 **RecordId**로 식별되는 특정 기록에 첨부됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

입력 변수

입력 변수는 작업의 초기 동작을 결정합니다.

입력 변수

변수	설명
테이블 이름 〔문자열〕	영향을 받는 테이블입니다.
FileSHA256Hash 〔문자열〕	Palo Alto Network Firewall 애플리케이션에서 받은 파일의 해시입니다.
RecordId 〔문자열〕	업데이트 중인 보안 인시던트 또는 IoC입니다.

출력 변수

출력 변수에는 후속 작업에서 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
commandStatus 〔부울〕	결과를 성공적으로 가져와서 첨부하면 True입니다.
errorMessage	작업에서 발생한 오류(있는 경우)입니다.

Palo Alto Networks Next-Generation Firewall 통합

설치 및 구성된 후에는 보안 인시던트 분석가가 이 통합을 통해 ()SIR 제품과 함께 EDL(외부 동적 목록) 기능을 사용하여 악성 IP 주소, URL 및 도메인을 차단합니다 ServiceNow 보안 인시던트 응답 . 보안 인시던트 분석가는 보안 인시던트에서 악성 ServiceNow SIR 으로 확인된 옵저버블에서 EDL에 대한 항목을 생성합니다.

EDL은 외부 웹 서버에서 호스팅되는 텍스트 파일입니다. 이 통합의 경우 이 웹 서버가 ServiceNow AI Platform 목록, IP 주소, URL 및 도메인에 포함된 객체를 임포트하고 정책을 적용할 수 있는 인스턴스 Palo Alto Networks Next-Generation Firewall 입니다.

EDL 항목에 정책을 적용하기 위해 정책 규칙 또는 프로파일에서 목록이 참조됩니다. EDL 항목이 수정되면 방화벽은 구성된 간격으로 목록을 동적으로 임포트하고 방화벽에서 구성 변경이나 커밋 없이 정책을 적용합니다. 이 통합을 ServiceNow AI Platform 위해 이(가) 구성된 검색 간격으로 인증 Palo Alto Networks Next-Generation Firewall 하여 검색한 EDL 항목이 포함된 테이블을 생성했습니다.

통합에는 다음과 같은 기능이 포함됩니다.

- 서로 다른 방화벽 거부 또는 허용 정책에 적용되는 여러 EDL을 생성할 수 있는 유연성.
- 차단되는 사이트 유형(피싱, 맬웨어 및 허용 목록에 지정된 사이트)에 대한 자세한 보고입니다.
- ServiceNow AI Platform 옵저버블 유형(URL, 도메인, IP 주소)별로 EDL 항목으로 보안 인시던트 태그 지정.
- 이전 항목을 자동으로 만료 또는 제거하여 EDL 목록 크기를 유지하도록 EDL 만료 기간을 구성합니다.
- EDL 목록 간에 EDL 항목을 검색, 삭제 또는 마이그레이션합니다.
- 위협 인텔리전스 결과와 항목이 차단된 이유에 대한 세부 정보가 포함된 옵저버블 기록 및 보안 인시던트에 EDL 항목을 연결합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

통합하려면 제품의 (com.snc.security_incident) 및 (com.snc.secops.orchestration) 플러그인을 보안 인시던트 응답 활성화해야 합니다.

이 통합은 (PAN-OS 8.x)만 지원합니다 Palo Alto Networks . 이전 버전은 지원되지 않습니다.

이 통합은 의 ServiceNow AI Platform#Kingston, London, Madrid 및 New York 릴리스와 호환됩니다.

주:
다음 항목에 번호가 매겨져 있습니다. 예상 결과의 원활한 설치, 구성 및 검증을 위해 제시된 순서대로 주제를 따르십시오.

에 대한 인증서 프로필 생성 **Palo Alto Networks Next-Generation Firewall**

통합하려면 서버와 서버 간의 ServiceNow AI Platform# 보안 연결을 확인하고 인증하기 위한 인증서 프로파일이 Palo Alto Networks Next-Generation Firewall 필요합니다.

필요한 역할: Palo Alto Networks Next-Generation Firewall 관리자.

A Palo Alto Networks Next-Generation Firewall 는 ServiceNow AI Platform# 인스턴스를 인증하고, 데이터베이스 테이블에서 EDL 항목을 검색하고, 항목을 해당 방화벽 정책 규칙에 통합합니다. 이 검색에는 PAN 방화벽 관리자가 API에 액세스하는 ServiceNow AI Platform# 데 사용하는 인스턴스의 API 사용자 계정 역할이 ServiceNow AI Platform# 필요합니다.

DigiCertificates를 다운로드하고 인증서 프로필을 구성하는 방법은 아래 단계를 따르십시오.

1. 사용 사례에 따라 DigiCert 또는 Entrust CA Gateway 인증서를 다운로드합니다. 자세한 내용은 의 Now Support 지식베이스KB1702083 문서를 참조하십시오.
2. 인증서 프로필을 구성합니다. 자세한 내용은 Palo Alto Networks 설명서를 참조하십시오.

관련 정보

PAN-OS 10.0 관리자 설명서의 "인증서 프로필 구성"

설정 및 설치 **Palo Alto Networks Next-Generation Firewall**

설치하기 전에 다음 설정 검사 목록을 완료합니다. 이러한 설정 작업은 원활한 설치를 위해 필요합니다.

시작하기 전에
필요한 역할: (admin)

설정 작업	설명
필수 ServiceNow AI Platform 및 보안 인시던트 응답 역할이 할당되어 있는지 확인합니다.	다음과 같은 역할이 필요합니다. • 시스템 관리자(admin)가 앱을 설치하고 보안 인시던트 관리자(sn_si.admin) 역할을 할당합니다. • 보안 인시던트 관리자(sn_si.admin)는 구성을 감독하고 EDL을 생성, 활성화 및 제거합니다. 이 역할은 sn_si.analyst 역할도 할당합니다. • (관리자)는 방화벽이 ServiceNow AI Platform# 에서 EDLServiceNow AI Platform#을 검색할 수 있도록 인증 Palo Alto Networks 에 필요한 자격 증명을 입력하는 데만 사용되는 API 계정 역할

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설정 작업	설명
	(sn_sec_panfw.api_account_access)을 할당합니다. • (sn_si.analyst) 또는 SOC(보안 운영 센터) 분석가는 EDL 항목을 생성하고 보안 인시던트를 처리합니다.
버전-OS 9.x 및 10.x를 사용하고 Palo Alto Networks Next-Generation Firewall 있는지 확인하십시오.	이 통합은 OS 9.0 이상만 지원합니다 Palo Alto Networks Next-Generation Firewall .
설명서에서 Palo Alto NetworksPalo Alto Networks 권장하는 대로 EDL 프로파일, 보안 정책 규칙 및 인증서 프로파일을 설정합니다.	Palo Alto NetworksPaloalto Networks 설명서 웹 사이트에서 일반 설명서 및 요구 사항을 참조하십시오.
DigiCert 루트 인증 기관 인증서를 다운로드하고 구성했는지 확인합니다.	통합하려면 서버와 Palo Alto Networks Next-Generation Firewall 서버 간의 ServiceNow AI Platform 보안 연결을 검증하고 인증하기 위해 이 인증서가 필요합니다. 인증서 설정에 대한 자세한 내용은 PAN-OS 10.0 관리자 가이드의 "인증서 프로파일 구성"을 참조하십시오. 다운로드하려면 DigiCert 신뢰할 수 있는 루트 기관 인증서를 참조하세요에 대한 인증서 프로필 생성 Palo Alto Networks Next-Generation Firewall.
ServiceNow 통합을 위해 애플리케이션을 설치하기 전에 통합을 지원하는 데 필요한 핵심 애플리케이션이 설치되고 활성화되었는지 확인합니다.	Madrid 이상 릴리스 요구 사항 Madrid 릴리스 및 이후 제품군 릴리스의 경우 Dependency 플러그인(com.snc.si_dep)이 보안 인시던트 응답 필요합니다. 이 플러그인은 제품을 지원하는 데 필요한 모든 종속성을 보안 인시던트 응답 자동으로 설치합니다. 통합에 필요한 다른 보안 운영 애플리케이션을 설치하고 활성화하기 전에 이 플러그인을 설치하고 활성화합니다. 에서 ServiceNow Store다음 보안 운영 애플리케이션이 설치되고 활성화되는지 확인합니다. 설치되지 않은 경우 원활한 설치를 위해 다음 순서로 한 번에 하나의 애플리케이션을 설치하고 활성화합니다. **1.** 보안 인시던트 응답 **2.** 보안 통합 프레임워크 **3.** Security Support Common **4.** 보안 지원 오케스트레이션 통합을 위한 인스턴스 설정에 ServiceNow AI Platform 대한 자세한 내용은 해당 문서를 애플리케이션 활성화 ServiceNow Store참조하십시오제품 또는 애플리케이션에 대한 보안 운영 권리 가져오기.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설정 작업	설명
조직에 이메일 삭제에 대한 변경 관리 및 승인 프로세스가 있는 ServiceNow AI Platform# 경우 이메일 보내기/받기 기능이 활성화되어 있는지 확인합니다.	인스턴스에서 이메일 보내기/받기 기능이 활성화되어 ServiceNow AI Platform# 있는지 확인하려면 이메일 속성 〉 관리 〉 이메일 속성. 아웃바운드 이메일 구성에서 이메일 전송 및 이메일 수신 이 선택되었는지 확인합니다.

프로시저

통합을 위해 애플리케이션을 설치하지 않은 경우 이를 확인하고 보안 운영 통합 설치 단계에 따라 설치합니다.

에 대한 **API** 계정 역할 생성 **Palo Alto Networks Next-Generation Firewall**

이 통합을 위해서는 인스턴스에 ServiceNow AI Platform# API 계정 역할이 필요합니다. 이 계정과 연결된 사용자 이름 및 암호가 생성 ServiceNow AI Platform# 되고 입력 Palo Alto NetworksPalo Alto Networks Next-Generation Firewall 되므로 EDL 항목을 검색할 때 인증됩니다 ServiceNow AI Platform# .

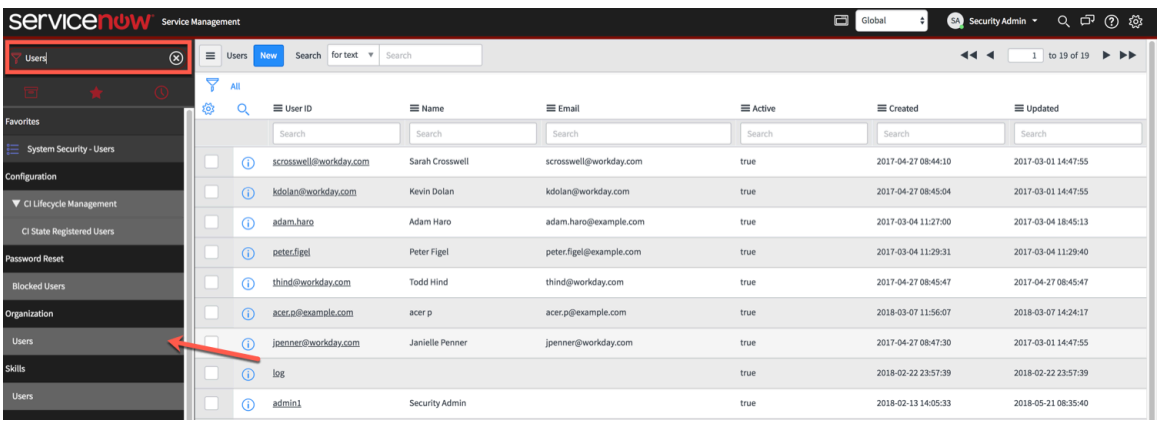
시작하기 전에
필요한 역할: 관리자

이 태스크 정보
ServiceNow AI Platform# 관리자는 API 계정 역할(sn_sec_panfw.api_account_access)을 생성합니다. 이 계정은 방화벽이 에서 EDLServiceNow AI Platform#을 검색할 수 있도록 인증 Palo Alto Networks 에 필요한 자격 증명을 입력하는 데만 사용됩니다. 이 계정은 인스턴스에서 별도의 고유한 API 사용자 계정 ServiceNow AI Platform# 이며 관리자에게 할당됩니다 Palo Alto Networks Next-Generation Firewall .

프로시저

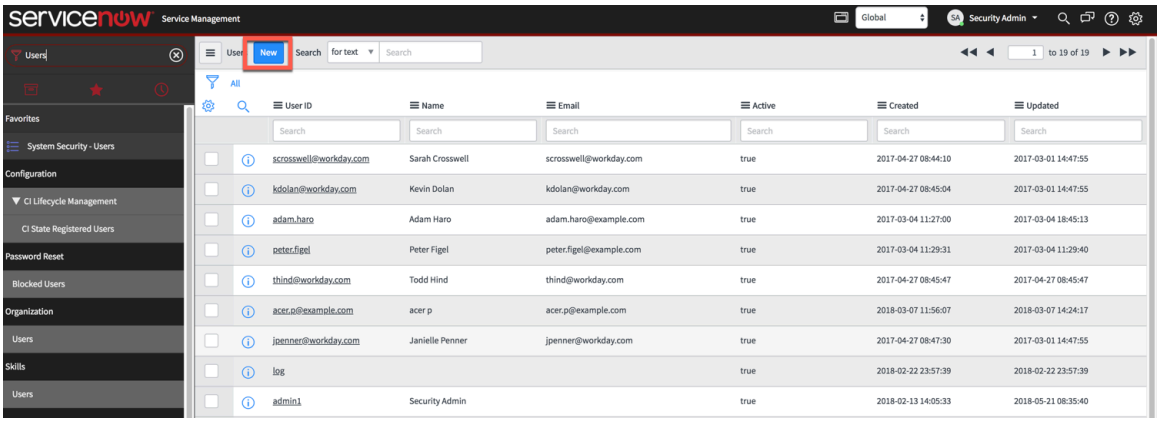
1. 다음으로 이동 모두 〉 조직 〉 사용자.

2. 사용자 모듈을 클릭합니다.



3. 표시되는 사용자 목록에서 새로 만들기를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

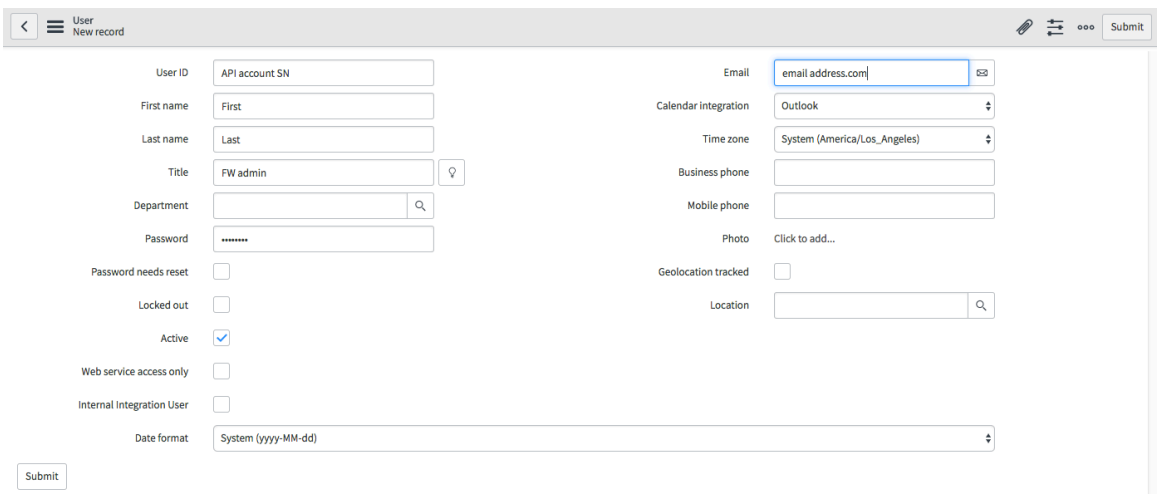


새 사용자 양식이 표시됩니다.

4. 양식을 작성합니다.

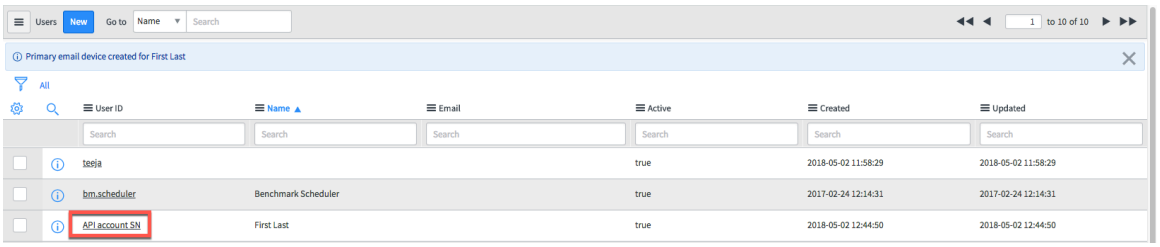
> **주:**
> 다음 표와 그림에 표시된 사용자 ID, 제목 및 전자 메일 주소의 값은 예제 값입니다.

필드	설명
사용자 ID	인스턴스의 역할에 대한 고유 사용자 ID입니다 ServiceNow AI Platform#. 이 사용자 ID는 사이트의 외부 동적 목록 대화 상자의 클라이언트 인증 섹션에 있는 사용자 이름 필드에 입력됩니다Palo Alto Networks. API ## SN을 예로 들 수 있습니다.
이름	할당하려는 사람입니다.
성	할당하려는 사람입니다.
직위	직함(예: FW ###).
암호	이 역할에 대해 생성된 고유한 암호입니다. 이 암호는 사이트의 외부 동적 목록 대화 상자의 Palo Alto Networks클라이언트 인증 섹션에 있는 암호 필드에 입력됩니다.
이메일	고유한 이메일 주소입니다.

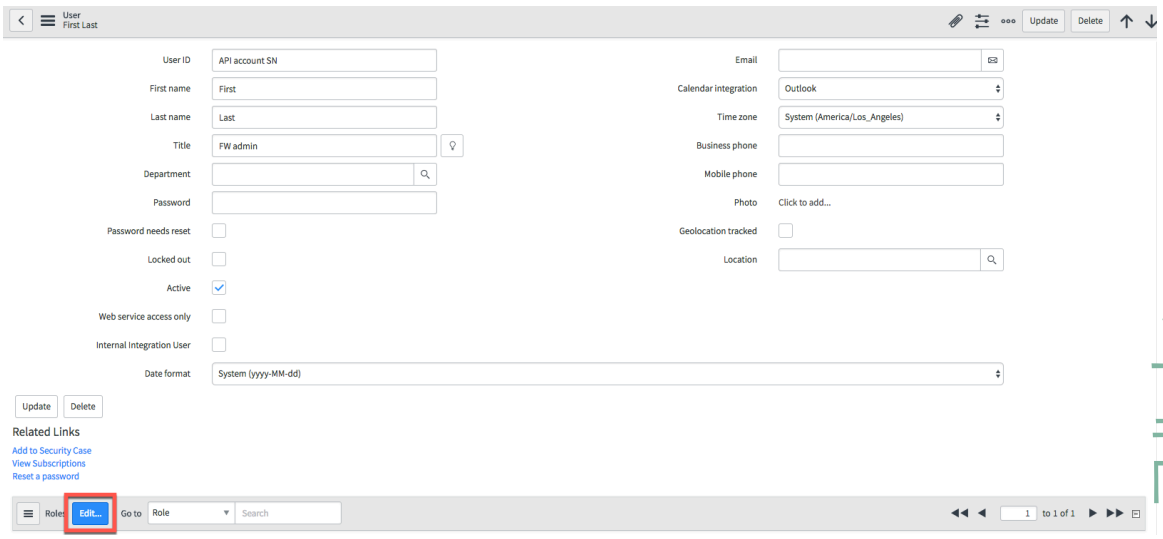


© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

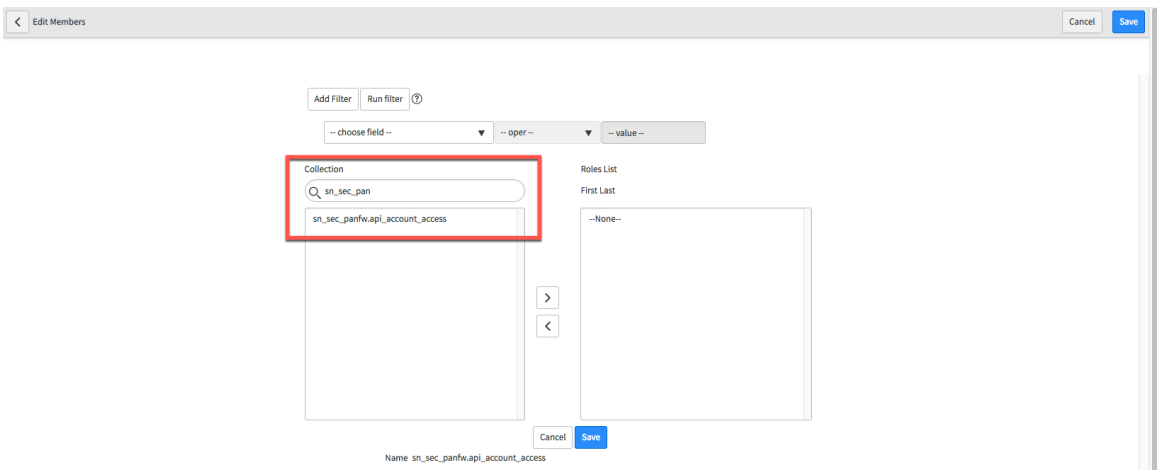
5. 제출을 클릭합니다.
   제출한 후에는 역할을 할당할 수 있습니다.
6. 사용자 목록의 사용자 **ID** 열에서 입력한 사용자 ID의 이름(예: API ## SN)을 클릭합니다.



7. 역할 섹션의 열린 기록에서 편집을 클릭합니다.

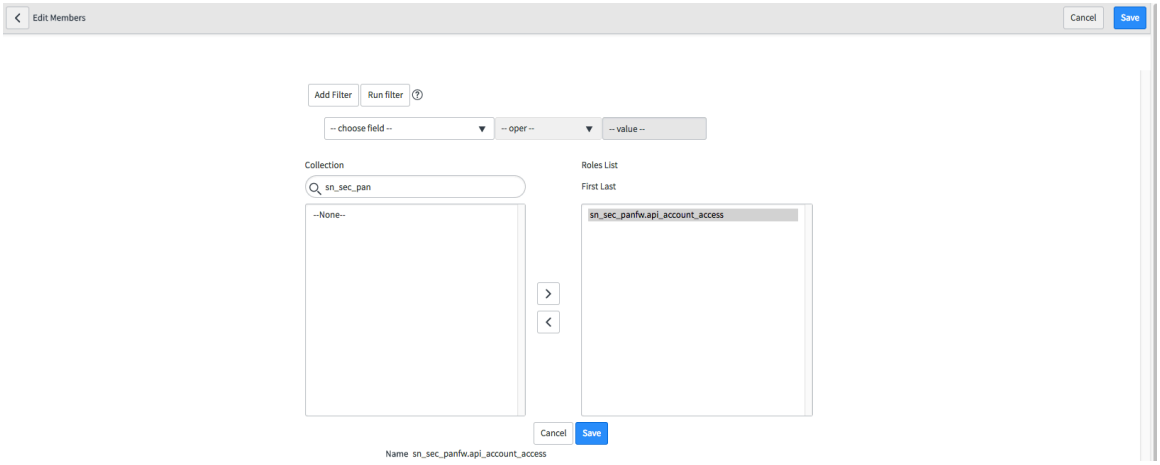


8. 표시되는 구성원 편집양식의 컬렉션 필드에 sn_sec_panfw.api_account_access를 입력합니다.
   컬렉션 필드 아래의 열에 역할이 표시됩니다.



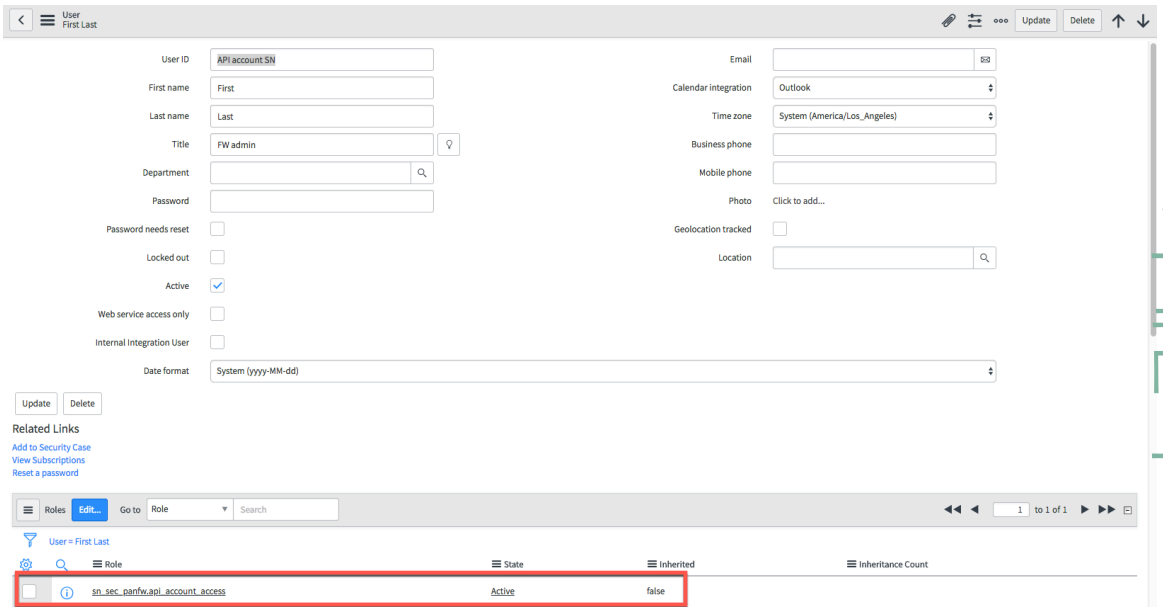
9. 컬렉션 열에서 sn_sec_panfw.api_account_access를 선택한 후 역할 목록으로 이동합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



10. 저장을 클릭합니다.

11. 사용자로 이동하여 목록의 사용자 열에서 역할(API ## SN)에 대해 생성한 ID 이름을 클릭합니다.



사용자 기록이 표시됩니다. 이 기록은 사용자 계정이 할당되었음을 확인합니다. 상태는 활성 상태이며 역할은 상속되지 않습니다.

에 지원되는 외부 동적 목록 **Palo Alto Networks Next-Generation Firewall**

통합은 ServiceNow Palo Alto Networks Next-Generation Firewall IP, URL 및 도메인 옵저버블을 허용하는 EDL(외부 동적 목록)을 지원합니다.

지원되는 **EDL** 및 옵저버블

외부 동적 목록은 외부 웹 서버에서 호스팅되는 텍스트 파일이며, 이 통합에서는 인스턴스가 해당됩니다ServiceNow AI Platform. Palo Alto Networks Next-Generation Firewall 그런 다음 목록에 포함된 개체(IP 주소, URL, 도메인)를 가져와 정책을 적용할 수 있습니다. EDL 항목에 정책을 적용하기 위해 정책 규칙 또는 프로파일에서 목록이 참조됩니다.

이 통합은 다음 세 가지 유형의 EDL을 지원합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- IP(여기에는 단일 IP 주소 및 CIDR 주소 블록(범위)이 포함됨)
- URL
- 도메인

다음 테이블에는 이 통합에서 지원하는 옵저버블에 대한 설명과 각 유형에 대한 예제 형식이 나와 있습니다.

지원되는 옵저버블 및 예제 형식

옵저버블	예제 형식	설명
IP 주소	• 95.153.103.54(IPv4) • (IPv6): 2001:00B8:130F:FE03:0000:09C0:080F:130B	고유한 단일 인터페이스 주소를 나타냅니다. 통합은 IPv4, IPv6 및 CIDR 형식을 지원합니다. IP 주소 옵저버블에 대한 지원에는 CIDR(Classless Inter-Domain Routing) 범위(예: 95.153.100.0/22)가 포함됩니다. 참고: CIDR 범위의 일부로 이미 차단한 EDL에 단일 IP 주소를 연결하려고 하면 오류 메시지가 표시됩니다. 예를 들어 단일 주소 95.153.103.54는 95.153.100.0/22(95.153.100.0-95.153.103.255)로 표현되는 CIDR 범위의 일부입니다.
URL	• www.example.com • www.example.com/article.html • example.com • *.example.com	와일드카드가 지원됩니다. EDL ServiceNow AI Platform 형식 요구 사항을 준수 Palo Alto Networks 하도록 URL 항목의 형식이 다시 지정됩니다.
도메인	• www.example.com • example.com • mail.example.com	와일드카드는 지원되지 않습니다.

형식 지정 지침 및 EDL에 대한 자세한 내용은 웹 사이트의 PAN-OS 10.0 관리자 가이드에서 "외부 동적 목록에 대한 형식 지정 지침" 을 Palo Alto Networks 참조하십시오.

Palo Alto Networks Next-Generation Firewall용 **EDL** 생성

인스턴스에 EDL(외부 동적 목록)을 ServiceNow AI Platform 생성합니다. 승인 및 활성화되면 SIR(On Incident)에서 악성 ServiceNow AI Platform 보안 인시던트 응답 으로 확인된 옵저버블에서 EDL에 대한 항목을 생성하고 차단 승인을 요청할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_si.admin

이 태스크 정보
방화벽이 목록에 포함된 객체(IP 주소, URL, 도메인)를 임포트하고 정책을 적용할 수 있도록 인스턴스에 EDL ServiceNow AI Platform 을 생성합니다. EDL 항목에 정책을 적용하기 위해 정책 규칙 또는 프로파일에서 목록이 참조됩니다.

다음 섹션의 그림은 시스템 설정에서 탭 구분 양식 이 선택 취소된 상태로 표시됩니다. 탭 양식 선택 및 지우기에 대한 자세한 내용은 의 Configuring the form layout "탭 양식 표시" 섹션을 참조하십시오.

프로시저

1. 애플리케이션 설치가 완료되면 통합 〉 통합 구성.
2. 타일을 Palo Alto Networks Next-Generation Firewall 찾아 구성을 클릭합니다.

3. 새 **EDL** 목록 만들기를 클릭합니다.

4. 양식에서 필드를 채웁니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Palo Alto Networks 방화벽 외부 동적 목록 양식

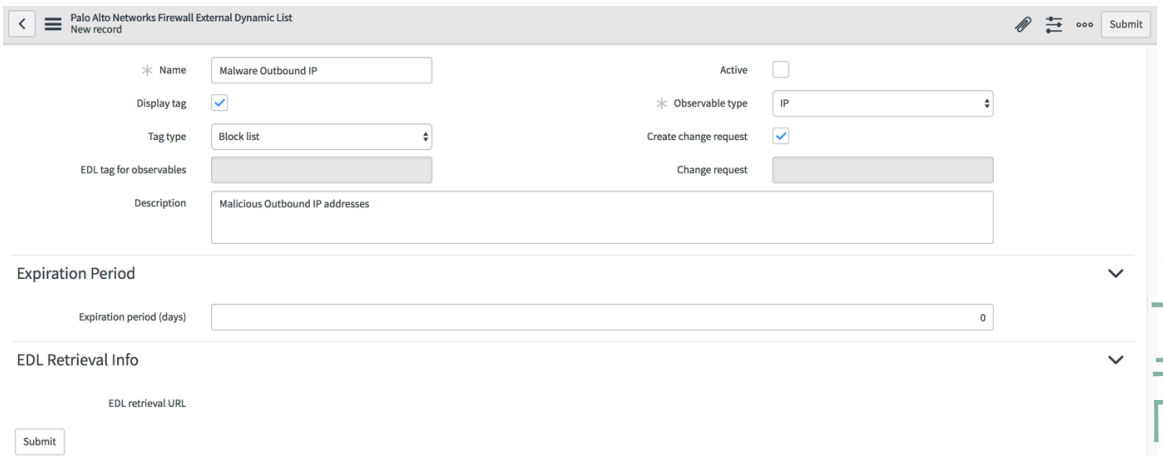
필드	설명
이름	Palo Alto Networks 방화벽 동적 목록 이름입니다. 보안 분석가가 이름으로 EDL의 의도를 쉽게 인식할 수 있도록 이 필드에 옵저버블 유형(URL, IP, 도메인)을 포함합니다. 또한 이름은 이러한 EDL 개체가 매핑되는 방화벽 정책을 명확하게 나타내야 합니다. EDL 이름의 예로는 아웃바운드 맬웨어 IP 또는 아웃바운드 피싱 URL이 있습니다.
활성	이 확인란은 EDL이 비활성 상태임을 나타내기 위해 기본적으로 선택이 취소되어 있습니다. 비활성화되면 EDL은 추가 항목을 받을 수 없습니다. 이 확인란을 선택하면 EDL이 활성화되고 EDL 항목에 사용할 수 있습니다.
태그 표시	EDL에서 옵저버블이 차단된 경우 옵저버블 및 관련 보안 인시던트 기록에 자동으로 태그를 지정하려면 확인란이 기본적으로 선택되어 있습니다. 선택하면 옵저버블 필드에 대한 태그 유형 및 EDL 태그를 양식에서 사용할 수 있습니다. 주: 태그 이름은 기본적으로 *EDL* 접두사(예: EDL-Malware OutBound IP)를 사용하여 이름 필드에 입력한 값에서 생성됩니다. 태그 이름과 색상을 변경할 수 있습니다. 참조: (선택 사항) 의 보안 태그 이름 편집 Palo Alto Networks Next-Generation Firewall. EDL이 저장되면 옵저버블에 대한 EDL 태그 필드에 태그 이름이 표시됩니다. 이 확인란의 선택을 취소하면 태그가 생성되지 않으며 양식에서 옵저버블에 대한 태그 유형 및 EDL 태그를 사용할 수 없습니다.
옵저버블 유형	선택 목록에서 이 EDL이 허용하는 옵저버블 유형(IP(CIDR 포함), URL 또는 도메인)을 선택합니다.
태그 유형	선택 목록에서 사용할 수 있는 태그입니다. 차단 목록은 차단하려는 Palo Alto Networks Next-Generation Firewall 옵저버블 목록입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	허용 목록은 허용하려는 Palo Alto Networks Next-Generation Firewall 옵저버블 목록입니다. 기본적으로 차단 목록 태그 색은 검은색이고 허용 목록 태그 색은 회색입니다. 색상을 변경할 수 있습니다. 참조: (선택 사항) 의 보안 태그 이름 편집 Palo Alto Networks Next-Generation Firewall.
변경 요청 생성	이 확인란은 EDL 기록에 첨부된 변경 요청 및 변경 작업을 ServiceNow AI Platform 인스턴스에 자동으로 생성하기 위해 기본적으로 선택되어 있습니다. 변경 요청은 서버에서 EDL 목록 검색 URL Palo Alto Networks Next-Generation Firewall 을 구성하는 데 사용됩니다. 방화벽 관리자가 방화벽 정책 또는 규칙 변경에도 사용하는 ServiceNow AI Platform 경우 이 옵션을 사용하는 것이 좋습니다. 요청을 생성한 경우 요청이 종결되면 EDL 목록이 자동으로 활성화됩니다. 방화벽 관리자로부터 구성이 Palo Alto Networks 완료되었다는 이메일을 통해 알림을 받은 후 EDL을 수동으로 활성화하려면 확인란의 선택을 취소합니다. 변경 요청 생성 확인란의 선택을 취소하면 변경 요청 필드를 사용할 수 없습니다.
옵저버블에 대한 **EDL** 태그	이 필드는 태그 표시 확인란이 선택된 경우에만 표시됩니다. EDL이 이름 필드의 기본값으로 저장된 후 필드가 자동으로 채워집니다. 기본 태그 이름 및 색상 변경에 대한 자세한 내용은 다음을 참조하십시오. (선택 사항) 의 보안 태그 이름 편집 Palo Alto Networks Next-Generation Firewall
변경 요청	변경 요청 생성 확인란을 선택한 경우 EDL이 저장되면 인스턴스에 변경 요청 번호가 표시됩니다 ServiceNow AI Platform . 변경 요청 생성 확인란의 선택을 취소하면 이 필드가 표시되지 않습니다.
설명	Palo Alto Networks 방화벽 동적 목록에 대한 설명입니다. 이름에는 일반적으로 이 EDL에 있을 것으로 예상되는 사이트 및 옵저버블 유형이 포함되며 이 필드를 사용하여 자세한 내용을 확인할 수 있습니다.
만료 기간(일)	EDL의 만료 기간입니다.

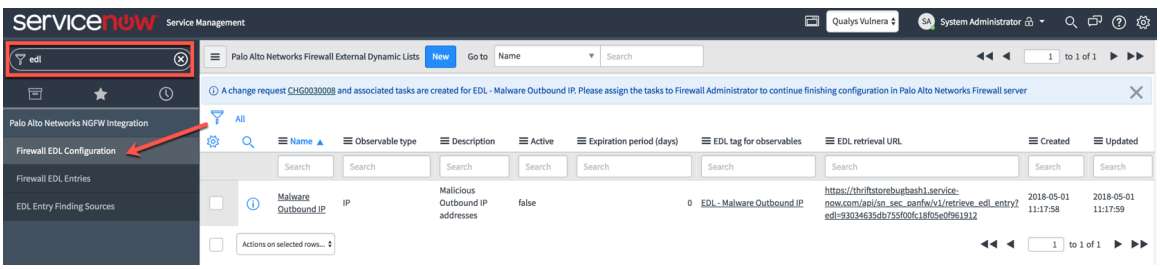
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	0(기본값)은 EDL 항목이 만료되지 않음을 나타냅니다. 이 값을 변경하면 입력한 일수 동안 이 항목이 활성화됩니다. 최솟값은 1로 입력할 수 있으며 최댓값은 없습니다. 예를 들어 5월 1일 오후 2시 1분에 30 일을 입력하면 EDL은 5월 31일 오후 2시 1분에 만료됩니다. 그러면 개별 항목을 기준으로 값을 재정의하지 않는 한 이 EDL의 모든 항목은 기본적으로 이 값을 상속합니다.



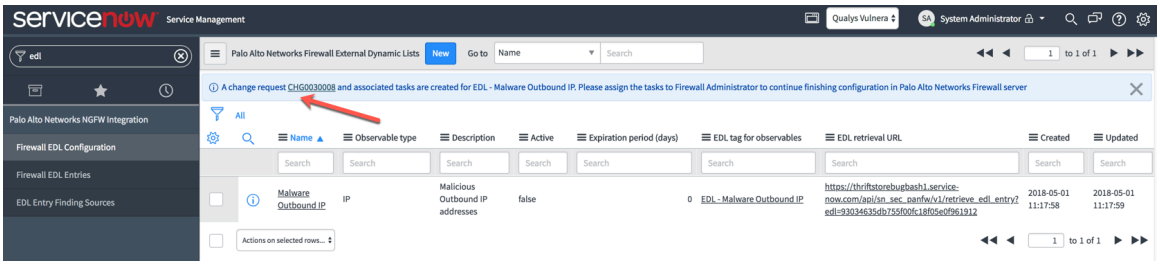
5. 제출을 클릭합니다.

6. Palo Alto Networks 방화벽 외부 동적 목록 목록이 표시되지 않으면 **Palo Alto Networks NGFW** 통합 〉 방화벽 **EDL** 구성 을 클릭하고 방화벽 **EDL** 구성을 클릭합니다.

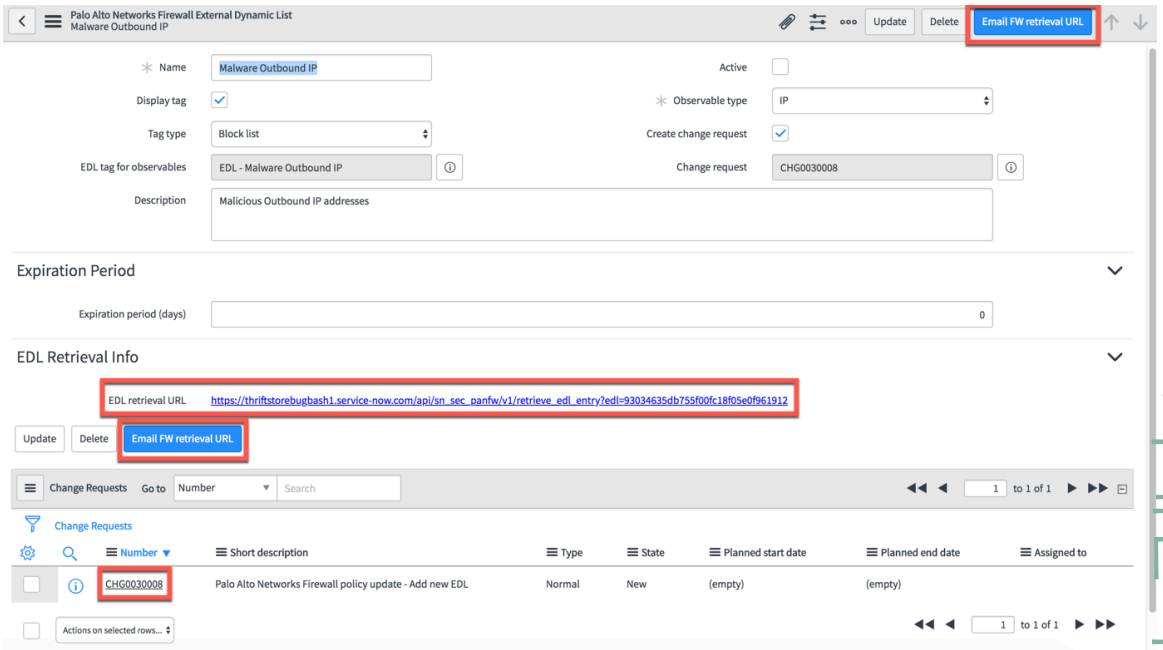


새 EDL이 표시됩니다. EDL 상태가 여전히 비활성(False)이므로 EDL을 항목을 수락할 수 없습니다. 변경 요청 생성이 구성된 경우 변경 요청과 인스턴스에 작업이 생성 ServiceNow AI Platform 되었음을 나타내는 메시지가 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



7. 이름 열에서 항목을 클릭하여 기록을 엽니다.
EDL 기록이 표시됩니다. 이 예에서는 악성코드 아웃바운드 IP EDL을 보여줍니다. 다음 필드, 옵션 및 링크는 제출 후 새 기록에 표시되고 다음 테이블에 설명되어 있습니다.



EDL 기록의 검색 URL 및 변경 요청 링크

옵션	설명
이메일 **FW** 검색 **URL**	EDL 링크를 구성에 Palo Alto Networks 사용할 수 있다는 알림을 방화벽 관리자에게 이메일로 전송합니다.
EDL 검색 URL	이 URL은 웹 사이트의 목록 만들기 탭에 Palo Alto Networks 있는 외부 동적 목록 인증 대화 상자의 원본 필드에 배치됩니다. 방화벽 관리자가 방화벽에서 Palo Alto Networks 구성에 사용하는 URL 링크가 Palo Alto Networks 자동으로 생성되어 표시됩니다. **주:** 시스템 설정이 탭 유형 양식으로 설정되어 있는 경우 이 링크는 기록 하단의 **EDL** 검색 정보 탭에 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵션	설명
ServiceNow AI Platform 변경 요청	구성되면 변경 요청 기록에 대한 링크가 변경 요청 섹션에 표시되고, 요청 번호는 변경 요청 필드에 표시됩니다.
업데이트	데이터를 수정하고 편집 가능한 필드를 업데이트합니다.
삭제	기록을 삭제합니다.

8. 필요에 따라 EDL을 더 생성하고 추가합니다.
   EDL은 외부 동적 리스트 리스트에 Palo Alto Networks 표시됩니다.

다음에 수행할 작업
수동으로 또는 변경 요청과 함께 EDL을 ServiceNow AI Platform 활성화합니다.

EDL 활성화

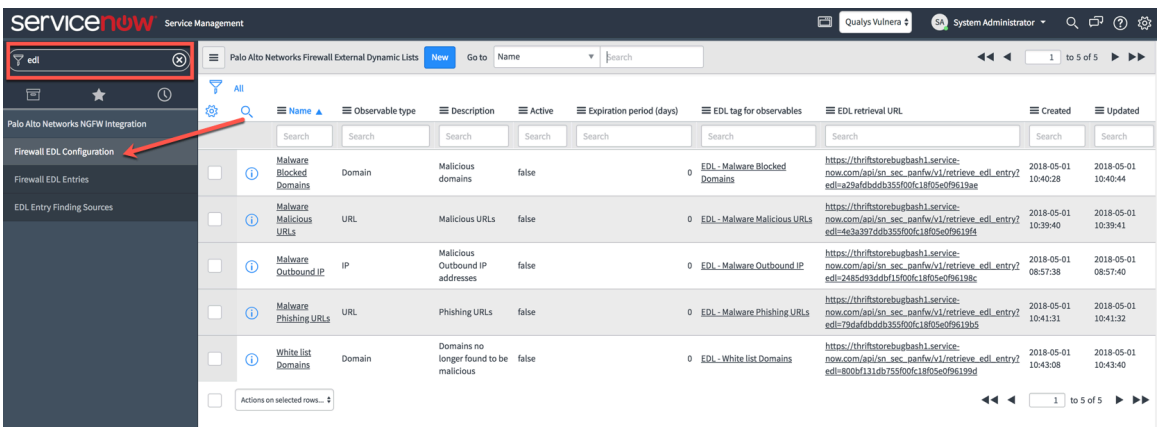
EDL(외부 동적 목록)이 생성 ServiceNow AI Platform# 되고 URL을 사용할 수 있게 되면 방화벽 관리자는 에서 Palo Alto Networks Next-Generation FirewallEDL을 Palo Alto Networks 구성합니다. 검색 URL은 방화벽 관리자가 서버에서 EDL Palo Alto Networks Next-Generation Firewall 을 구성하는 데 사용됩니다Palo Alto Networks. EDL 항목을 수락하려면 먼저 EDLServiceNow AI Platform#을 Palo Alto Networks 에서 구성하고 .

시작하기 전에
필요한 역할: sn_si.admin

이 태스크 정보
EDL을 구성한 후 보안 인시던트 관리자는 EDL을 수동으로 활성화하거나, 변경 요청 완료 시 EDL이 ServiceNow AI Platform# 자동으로 활성화됩니다. EDL을 승인하고 비활성 상태에서 활성 상태로 전환해야 EDL 항목을 수락할 수 있습니다.

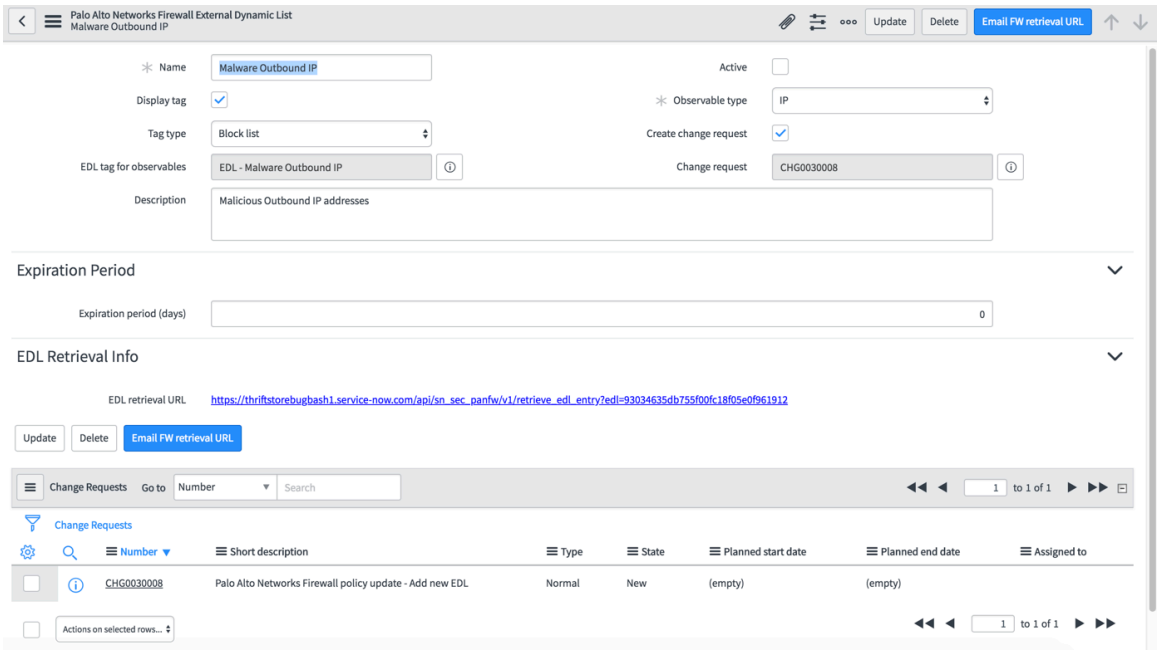
프로시저

1. 다음으로 이동 모두 〉 **Palo Alto Networks NGFW** 통합 〉 방화벽 **EDL** 구성 을 클릭하고 방화벽 **EDL** 구성 모듈을 선택합니다.



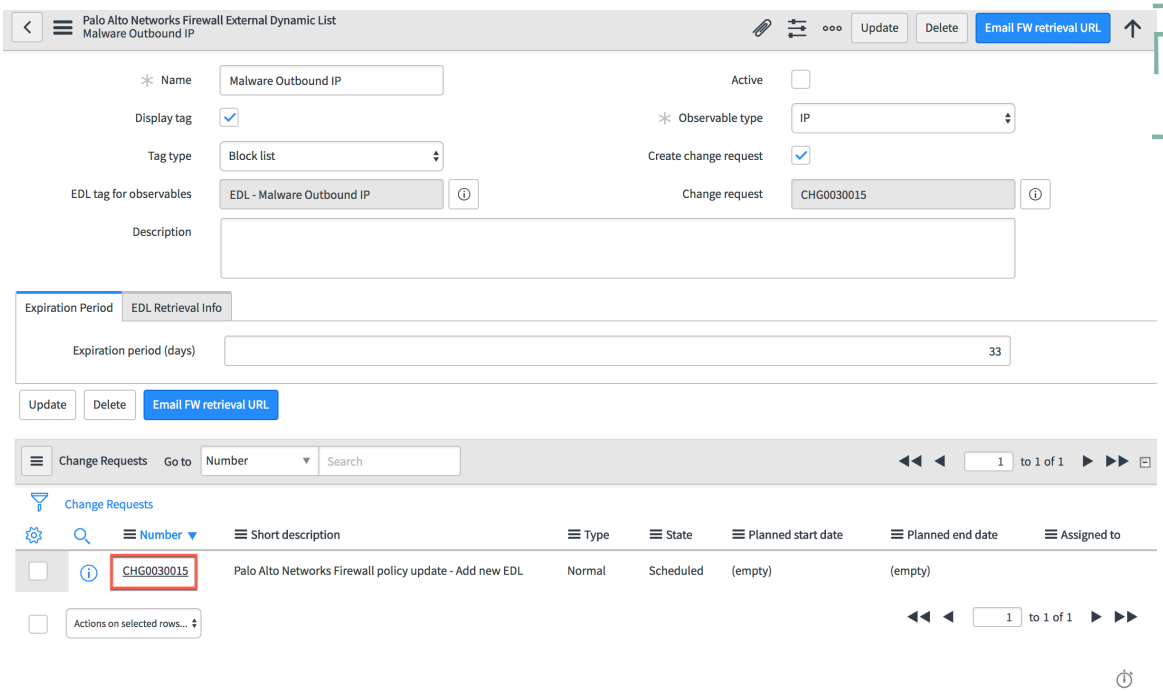
2. 표시되는 Palo Alto Networks 방화벽 동적 목록 목록의 이름 열에서 새 EDL을 선택합니다.
3. 표시되는 기록에서 이메일 **FW** 검색 **URL** 버튼, 활성 EDL 검색 URL 링크, 변경 요청(구성된 경우) ServiceNow AI Platform# 섹션의 변경 요청을 확인합니다.
   활성 확인란의 선택이 취소되어 있는지 확인합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



주:
시스템 설정에서 탭 지정 양식을 지우면 이전 그림과 같이 EDL 검색 URL이 **EDL** 검색 정보 섹션에 표시됩니다.

다음 그림은 시스템 설정에서 탭 구분 양식이 선택된 탭으로 표시되는 **EDL** 검색 정보를 보여줍니다. **EDL** 검색 정보 탭을 클릭하여 검색 URL을 표시합니다. 변경 요청(**CHG0030015**)에 대한 링크도 표시됩니다.



4. 구성을 완료하고 EDL을 비활성에서 활성으로 이동하려면 다음 옵션 중 하나를 선택하여 방화벽 관리자에게 검색 URL을 사용할 수 있음을 알려야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

방화벽 관리자에게 검색 URL을 사용할 수 있음을 알리고 EDL이 에서 구성 Palo Alto Networks되었는지 확인한 후 보안 인시던트 관리자로서 다음 단계는 EDL을 활성화하는 것입니다. EDL을 수동으로 활성화하거나, 변경 요청 양식(구성된 경우)을 사용하여 EDL을 ServiceNow AI Platform 활성화합니다.

관련 정보

EDL 구성

수동으로 **EDL** 활성화

Palo Alto Networks 방화벽 관리자가 를 ServiceNow AI Platform사용하지 않고 사용자가 구성되었다는 알림을 Palo Alto Networks Next-Generation Firewall 직접 받는 경우 EDL(외부 동적 목록)을 수동으로 활성화할 수 있습니다.

시작하기 전에

에서 Palo Alto NetworksEDL 개체, 정책 및 소스 URL을 생성한 EDL에 할당합니다. 에 대한 Palo Alto Networks Next-Generation Firewall EDL 구성에 대한 자세한 내용은 을 Palo Alto Networks참조하십시오 EDL 구성.

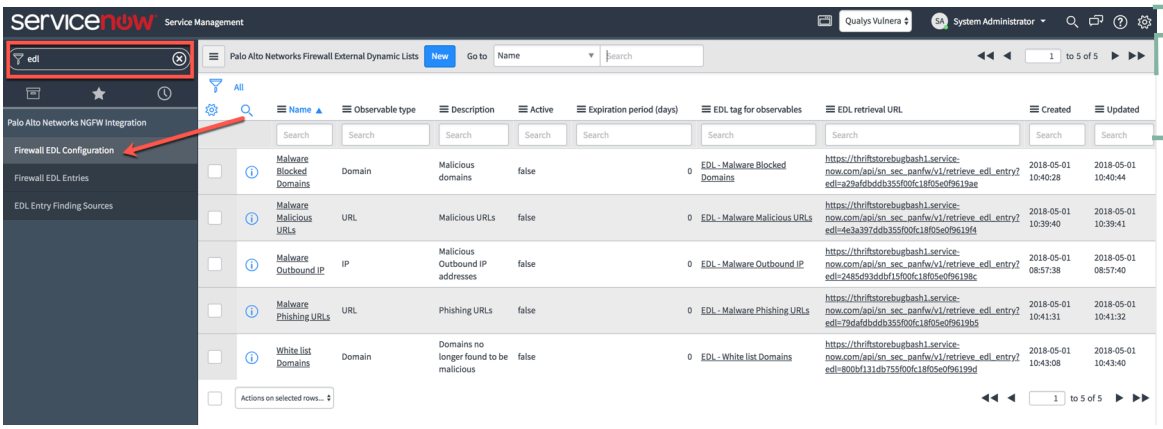
필요한 역할: sn_si.admin

이 태스크 정보

ServiceNow AI Platform 보안 인시던트 관리자는 에서 Palo Alto Networks Next-Generation FirewallEDL 구성이 완료되면 방화벽 관리자가 알림을 받습니다Palo Alto Networks.

프로시저

1. 다음으로 이동 모두 〉 **Palo Alto Networks NGFW** 통합 〉 방화벽 **EDL** 구성.

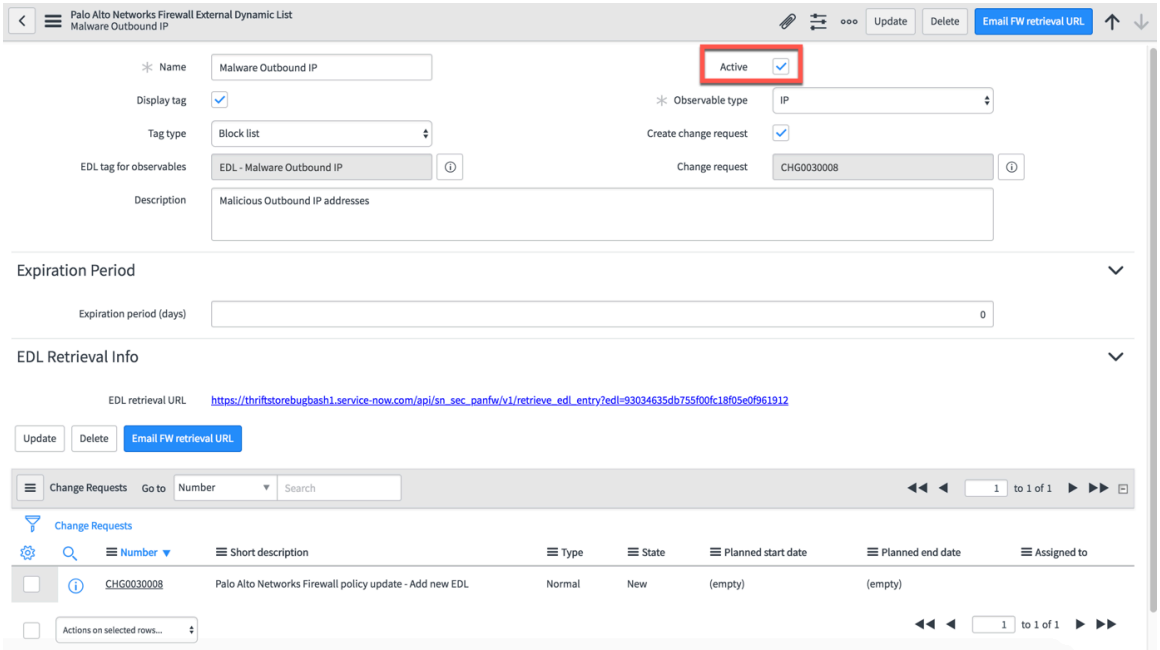


2. 방화벽 **EDL** 구성 모듈을 선택합니다.

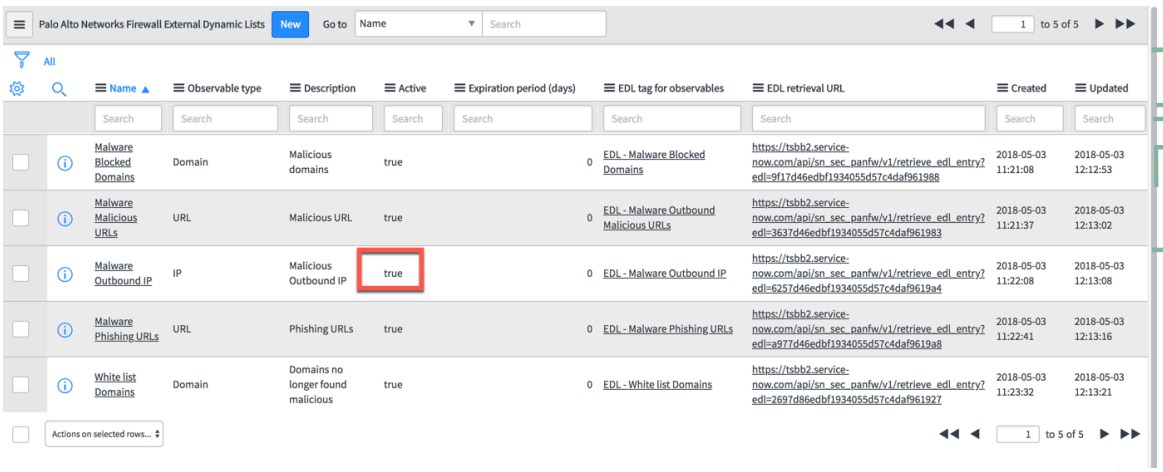
3. Palo Alto Networks 방화벽 외부 동적 목록 목록에서 이름 열의 항목을 클릭하여 엽니다.

4. 열리는 기록에서 활성 확인란을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



5. 업데이트를 클릭합니다.
Palo Alto Networks 방화벽 외부 동적 목록 목록의 활성 열에서 EDL의 상태에 ## true 가 표시됩니다.



결과
EDL이 활성화되고 EDL 항목을 수신할 준비가 되었습니다.

다음에 수행할 작업
보안 인시던트 또는 차단 목록에서 EDL 항목을 제출합니다.

EDL 구성

Palo Alto Networks 방화벽 관리자는 에서 검색 URL을 사용할 수 ServiceNow AI Platform있다는 알림을 받으면 EDL Palo Alto Networks Next-Generation Firewall 을 구성합니다. EDL이 EDL 항목을 수락하려면 먼저 에서 구성하고 Palo Alto Networks에서 활성화해야 ServiceNow AI Platform#합니다.

시작하기 전에
필요한 역할: Palo Alto Networks firewall administrator

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

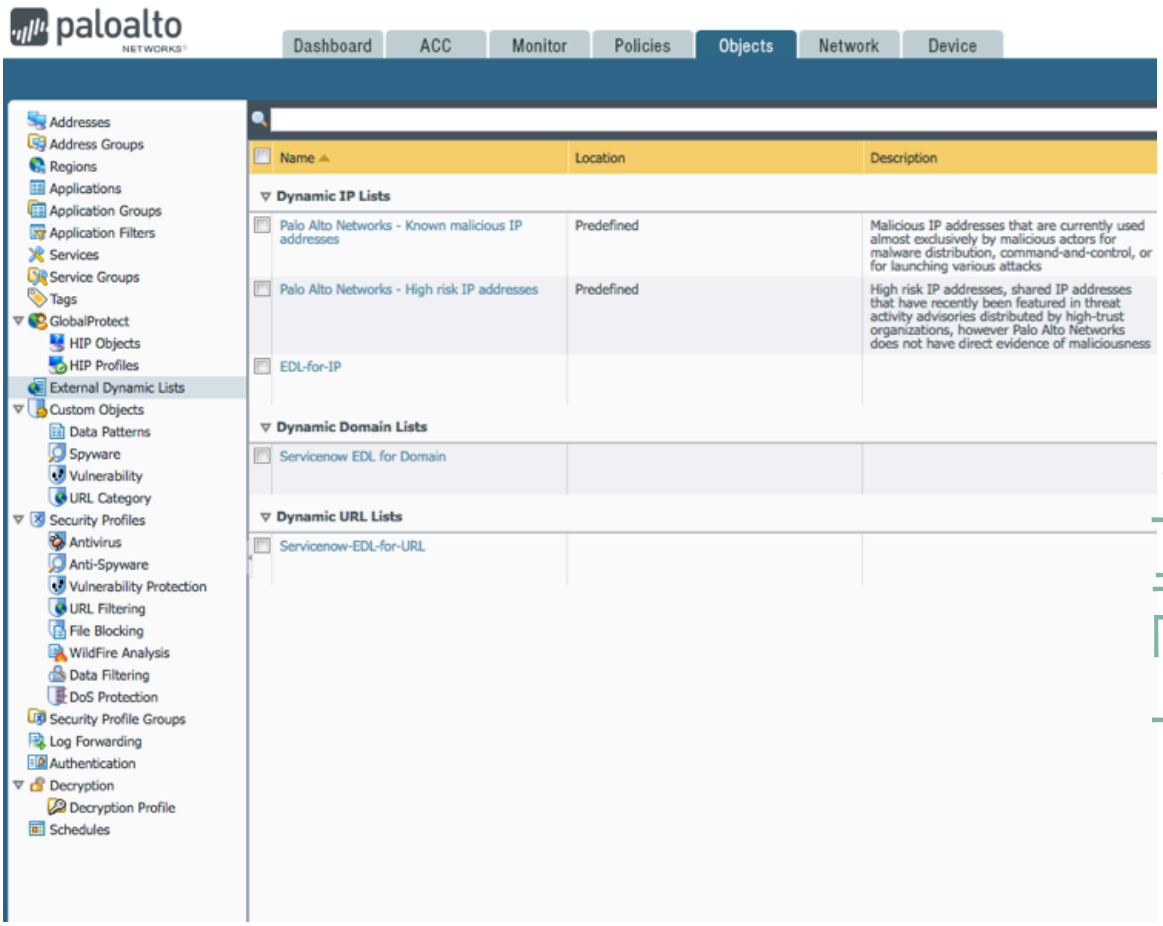
이 태스크 정보

Palo Alto Networks Next-Generation Firewall 관리자는 EDL 개체를 만들고 소스(검색) URL 및 정책을 EDL에 할당합니다. 이러한 작업은 에서 ServiceNow AI PlatformEDL이 활성화되기 전에 수행됩니다Palo Alto Networks.

다음 섹션의 이미지는 권한에 의해 사용되며 PRIVILEGED 및 PROPRIETARY입니다.

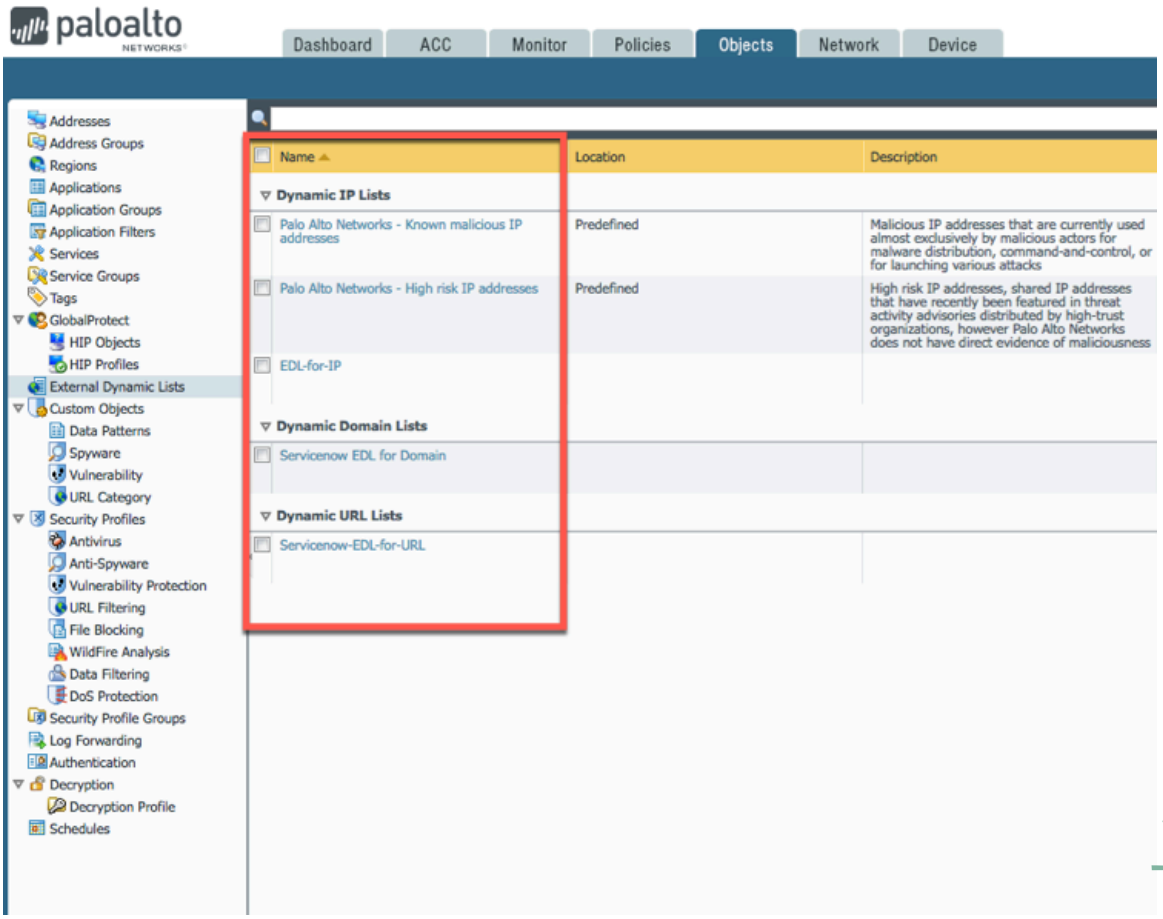
프로시저

1. 방화벽에 EDL을 구성하지 않은 경우 외부 동적 목록 〉 객체 in Palo Alto Networks.



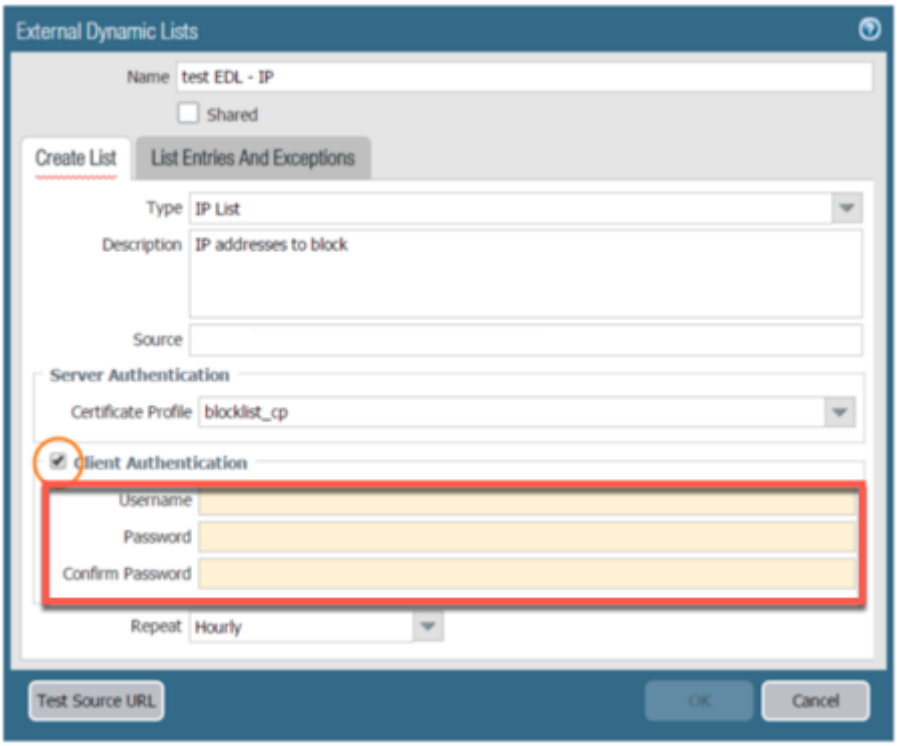
2. 이름 열의 목록에서 구성할 EDL을 ServiceNow 선택합니다(예: URL의 경우 **ServiceNow EDL**).

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

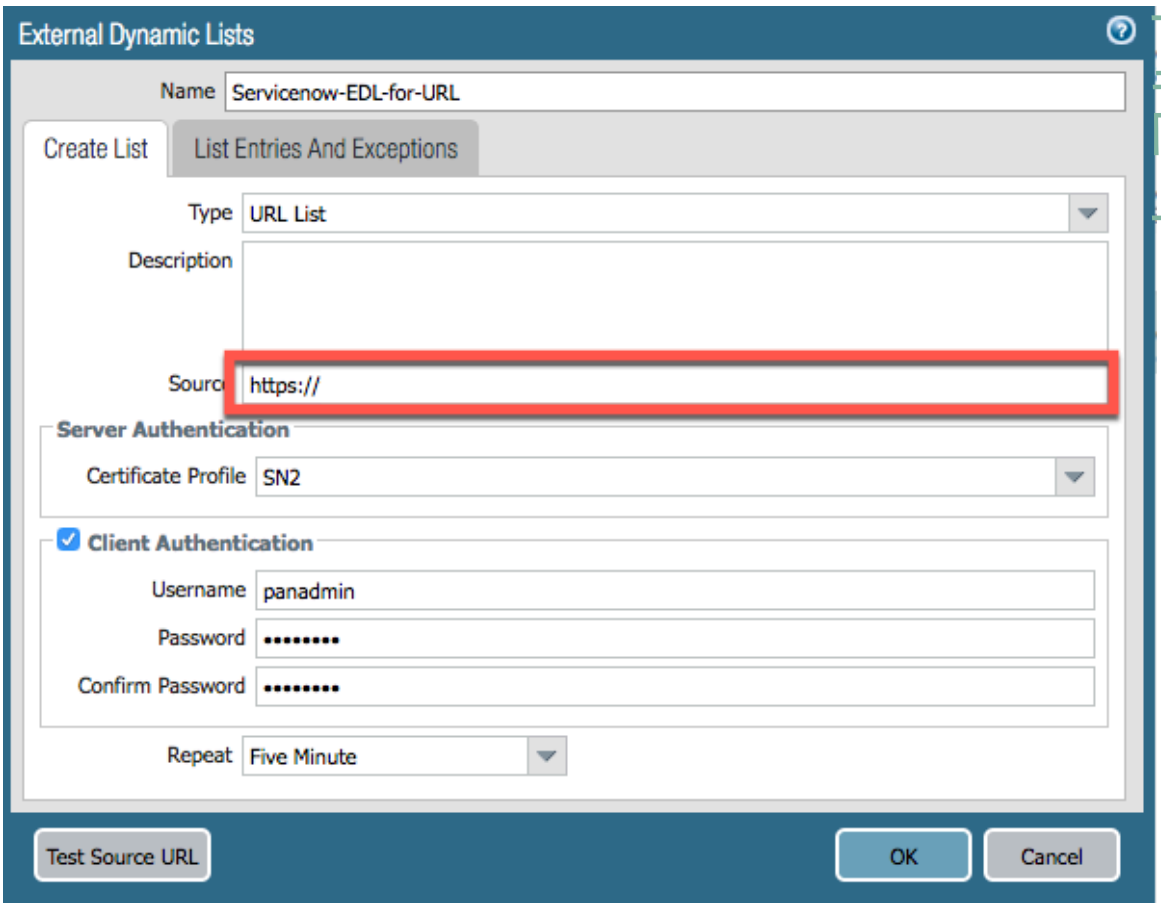


3. 외부 동적 목록 대화 상자에서 사용자 이름 및 암호를 입력하여 인증합니다 ServiceNow AI Platform#.
   이러한 자격 증명은 인스턴스에서 API 계정 역할(sn_sec_panfw.api_account_access) ServiceNow에 대해 생성한 사용자 이름과 암호입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 소스 필드에 인스턴스의 EDL 목록에서 작성된 URL을 ServiceNow 입력합니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. 예를 들어 선택 목록에서 인증서 프로파일(예: SN2)을 선택합니다.

6. 확인을 클릭합니다.

변경 요청 포함에 대한 **Palo Alto Networks Next-Generation Firewall EDL** 활성화

구성된 경우 변경 요청 양식은 ServiceNow EDL(외부 동적 목록)을 활성화하는 데 사용됩니다. 방화벽 관리자가 방화벽 정책 또는 규칙 변경에도 사용하는 ServiceNow AI Platform 경우 이 옵션을 사용하는 것이 좋습니다. EDL이 자동으로 활성화되고 변경 요청이 종결될 때 EDL 항목을 받을 준비가 됩니다 ServiceNow AI Platform .

시작하기 전에

주:
다음 섹션의 그림은 시스템 설정에서 선택한 탭 양식 과 함께 표시됩니다. 탭 폼 선택 및 지우기에 대한 자세한 내용은 ServiceNow 제품 설명서 웹 사이트에서 폼 레이아웃 구성의 탭 폼 표시 섹션을 참조하십시오.

필요한 역할: 변경 요청 및 변경 작업 승인을 위한 sn_si.admin

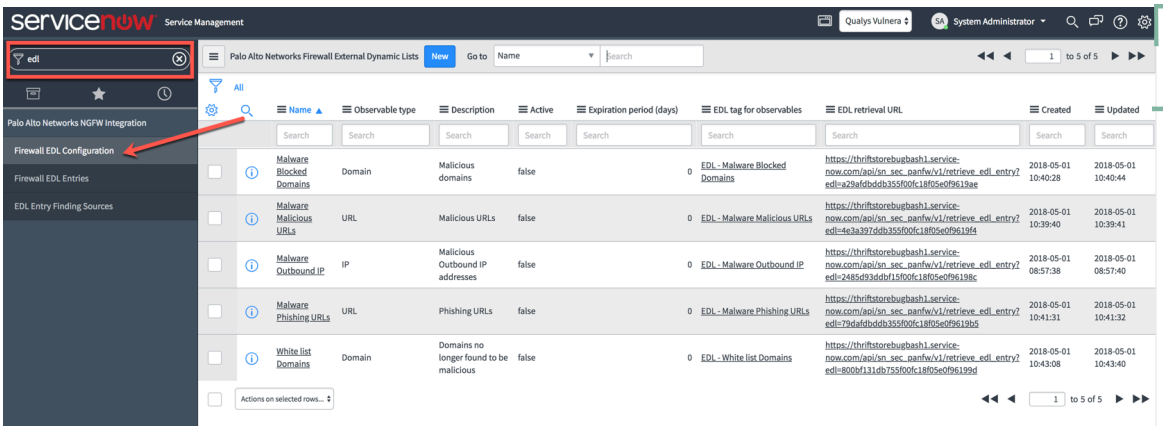
Palo Alto Networks 에서 구성 작업을 완료하기 위한 방화벽 관리자 Palo Alto Networks

이 태스크 정보

구성된 경우 변경 요청을 모니터링하고 ServiceNow AI Platform 를 Palo Alto Networks Next-Generation Firewall구성하는 데 필요한 모든 작업을 할당합니다. 이러한 작업이 완료되면 변경 요청을 종결 ServiceNow AI Platform 하여 EDL을 자동으로 활성화합니다.

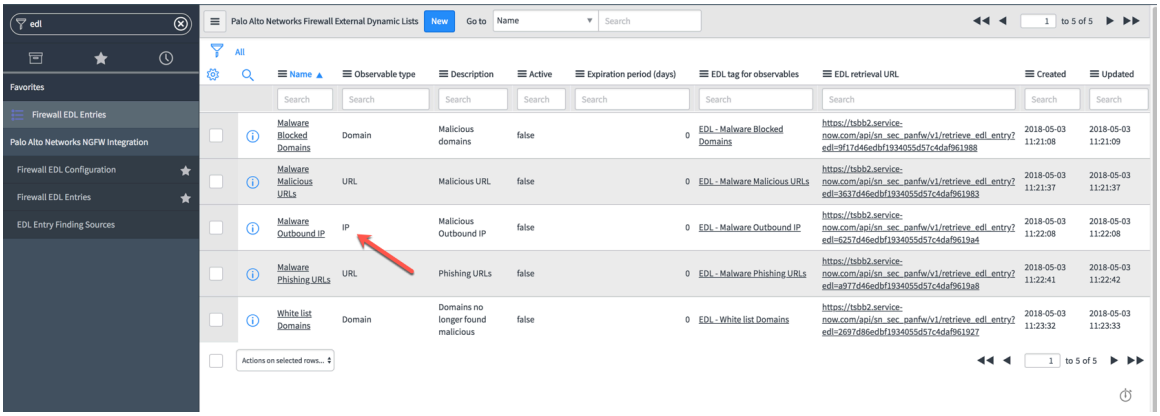
프로시저

1. 다음으로 이동 모두 〉 **Palo Alto Networks NGFW** 통합 〉 방화벽 **EDL** 구성.

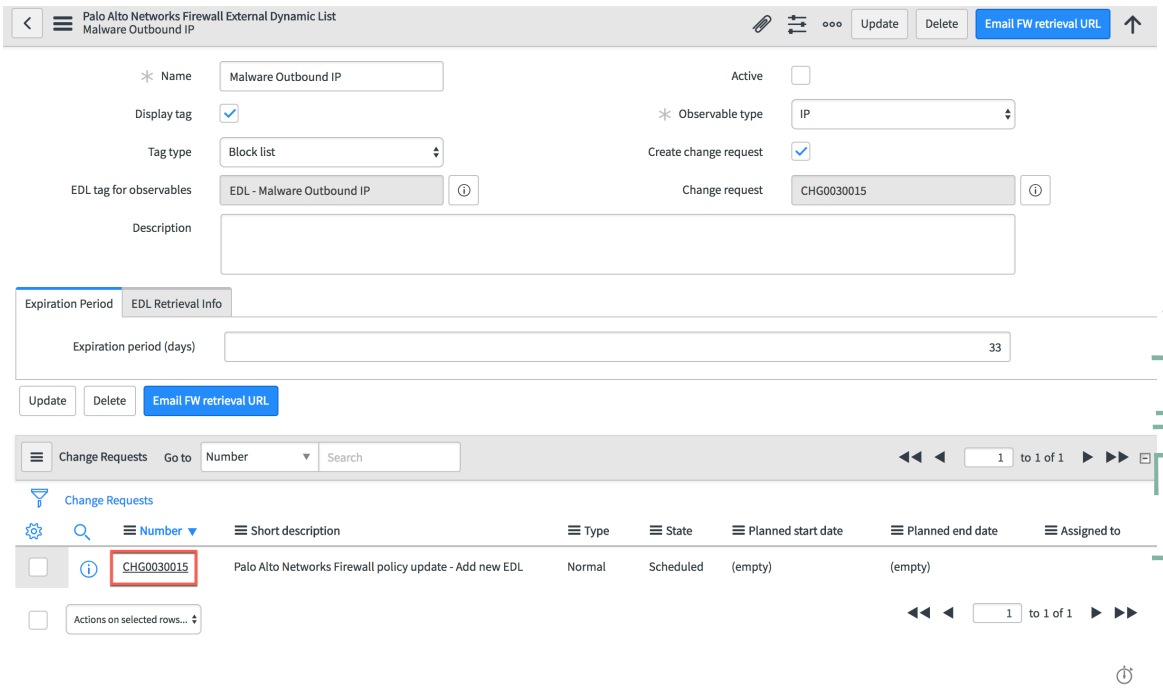


2. EDL 모듈을 선택하고 이름 열에서 EDL을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

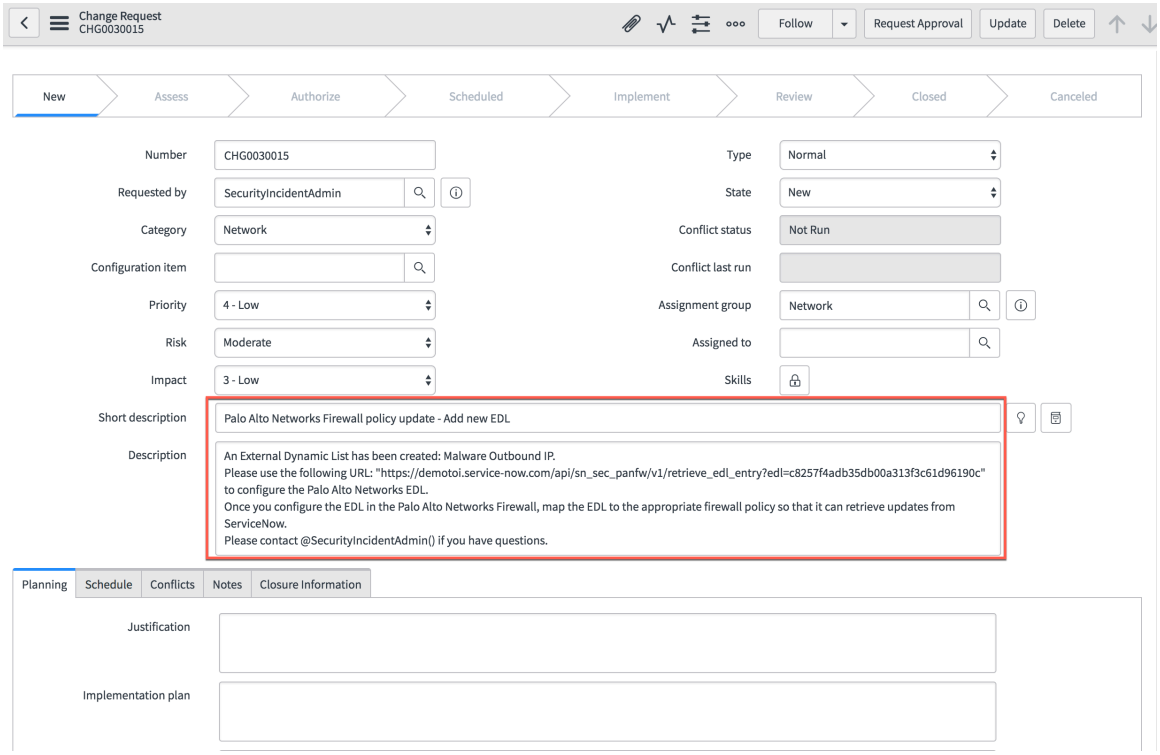


3. 열려 있는 EDL 기록에서 변경 요청 관련 목록의 변경 요청 번호를 클릭합니다.

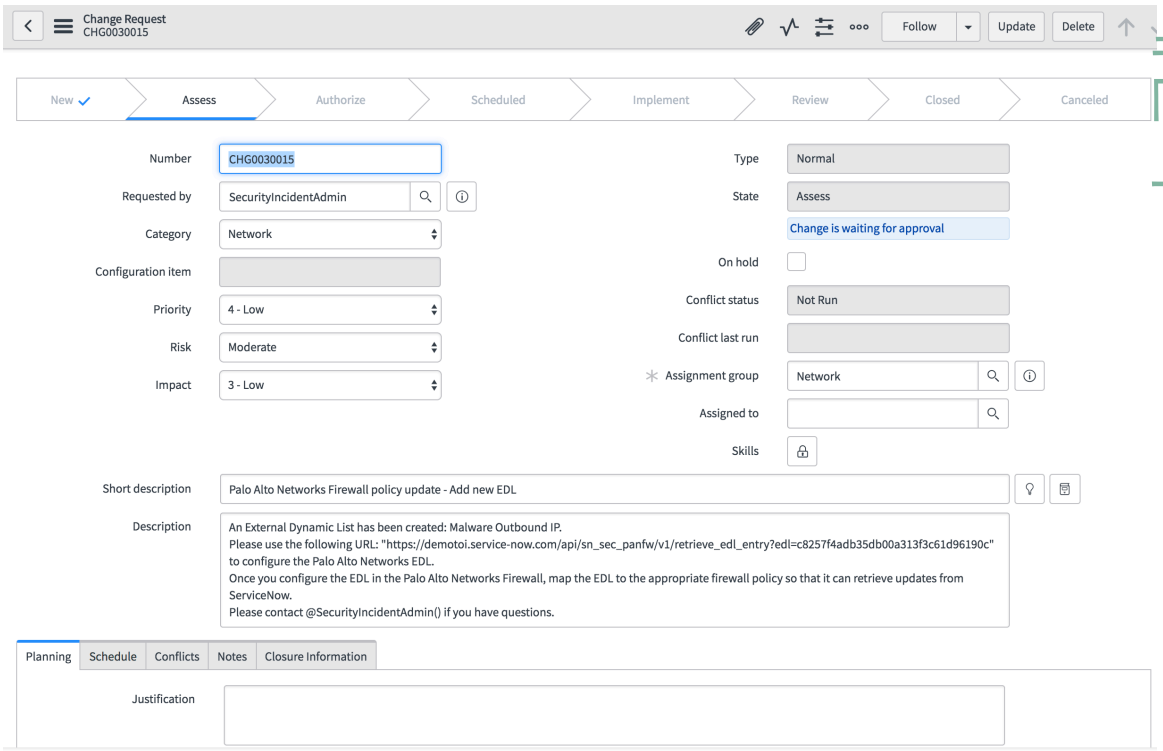


변경 요청 기록이 표시됩니다. 설명 필드에는 EDL을 구성하는 데 사용되는 검색 URL이 Palo Alto Networks 나열됩니다. EDL을 적절한 Palo Alto Networks Next-Generation Firewall 정책에 매핑하는 방법에 대한 세부 정보도 포함되어 있습니다. 간단한 설명필드에서 주석은 새 EDL을 추가하라는 요청이 있음을 나타냅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



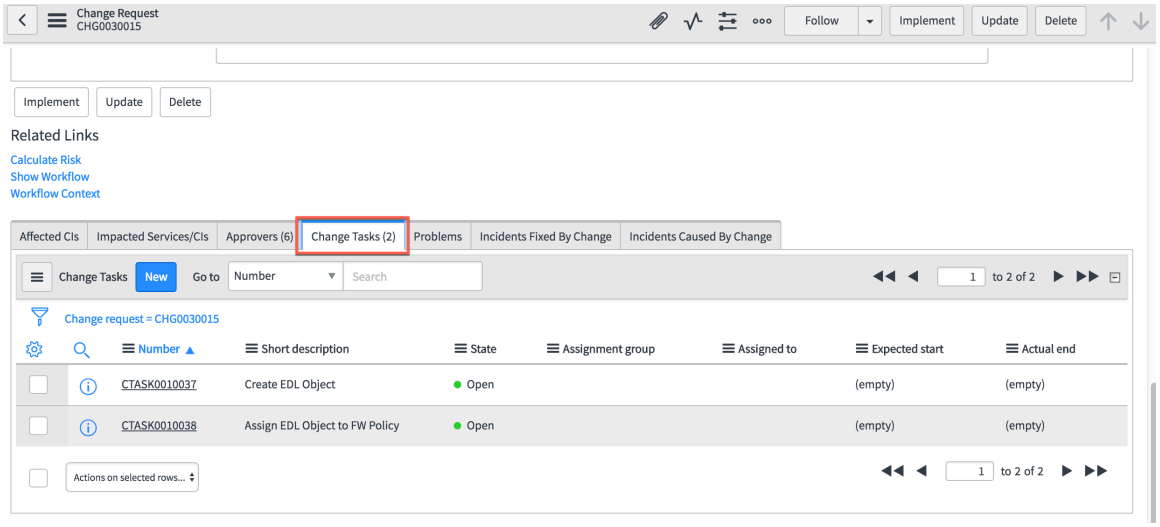
4. 기록의 오른쪽 위 모서리에서 **Request Approval**(승인 요청)을 클릭합니다.
상태가 평가로 변경되고, 변경 요청이 승인을 기다리고 있다는 메시지가 표시됩니다.



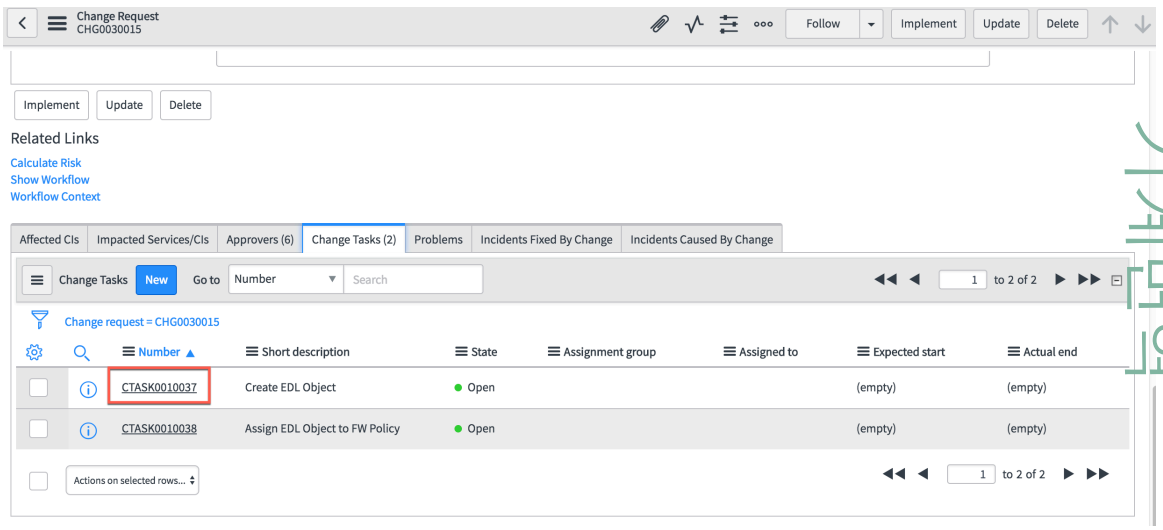
5. 변경 요청을 완료하고 EDL을 활성화하려면 단계에 따라 작업을 할당하고 변경 요청을 종결합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 표시되지 않으면 변경 요청을 열고 변경 작업 탭을 선택합니다.



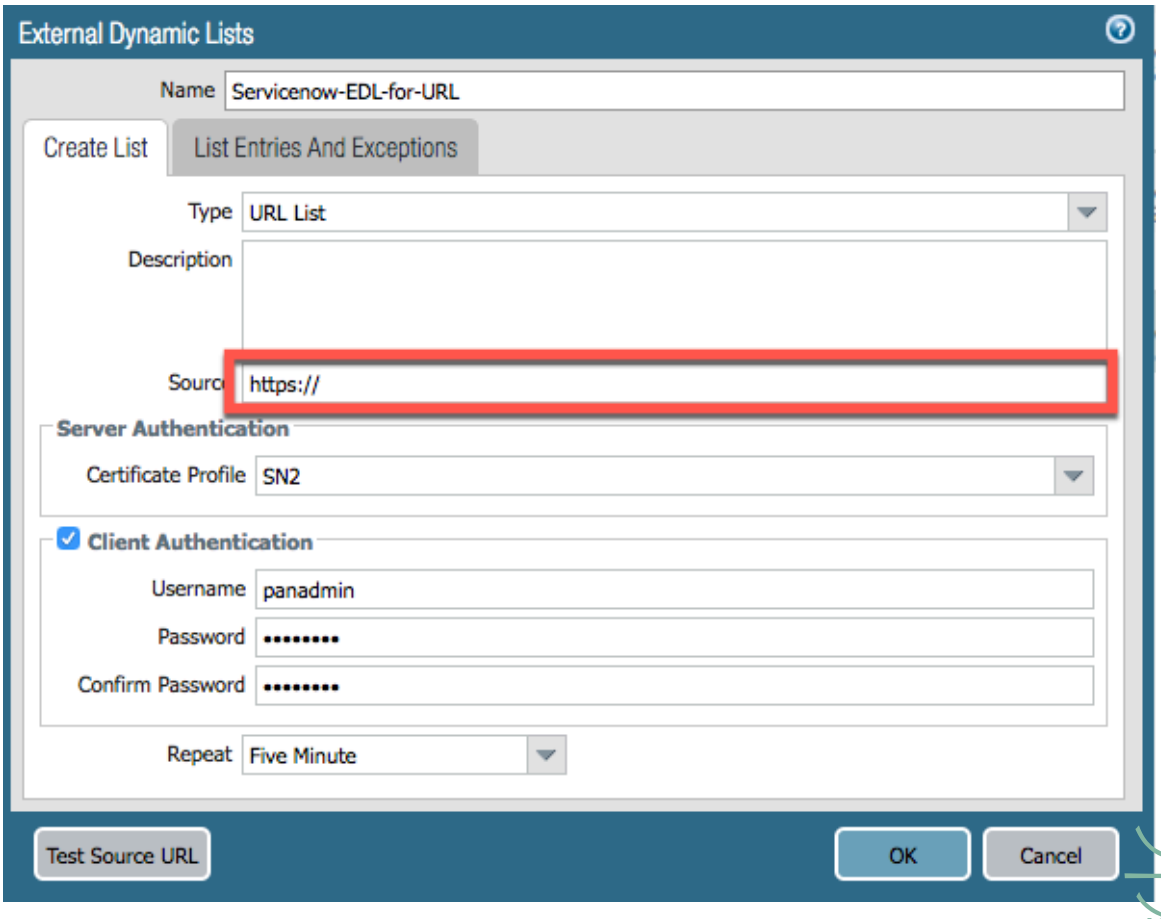
b. EDL 객체 생성과 연관된 작업을 클릭하여 엽니다.



c. 표시되는 기록에서 방화벽 관리자에게 작업을 Palo Alto Networks 할당하고 업데이트를 클릭합니다.
방화벽 관리자에게 알림이 전송되고 .Palo Alto Networks Next-Generation Firewall

EDL 개체를 ServiceNow AI Platform 만들기 위해 검색 URL이 다음 위치에 복사 Palo Alto Networks 됩니다. 외부 동적 목록 〉 목록 작성 〉 소스.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

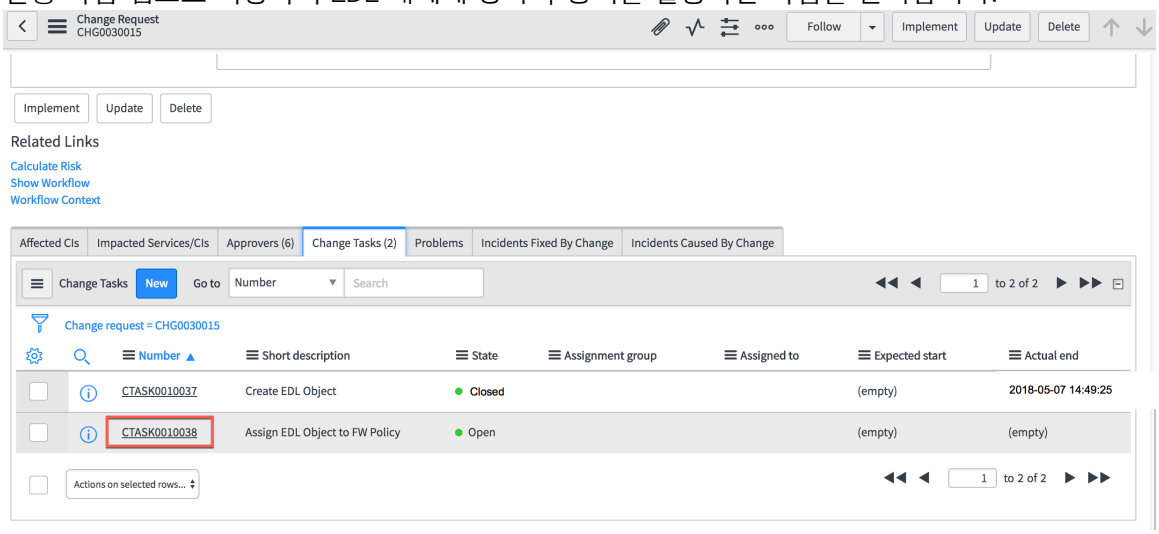


이미지는 권한에 의해 사용되며 특권 및 독점입니다.

d. EDL 개체가 에서 생성Palo Alto NetworksServiceNow AI Platform되었는지 확인한 후 에서 EDL 개체 생성과 관련된 변경 요청으로 이동하고 작업 닫기를 클릭합니다.

이 예의 작업 기록에서 이 작업에 대한 CTASK0010037 종결되었습니다.

e. 변경 작업 탭으로 이동하여 EDL 개체에 방화벽 정책을 할당하는 작업을 클릭합니다.

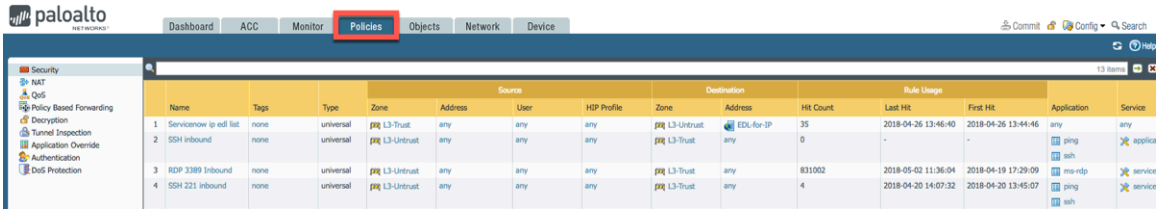


CTASK0010037 상태는 ##입니다.

f. 기록을 열고 다음 작업을 할당합니다.

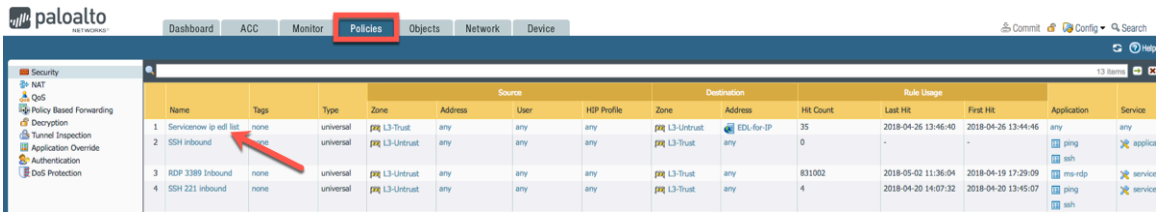
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업이 할당 Palo Alto Networks되면 방화벽 관리자는 정책 탭으로 이동하여 정책을 할당합니다.



이미지는 권한에 의해 사용되며 특권 및 독점입니다.

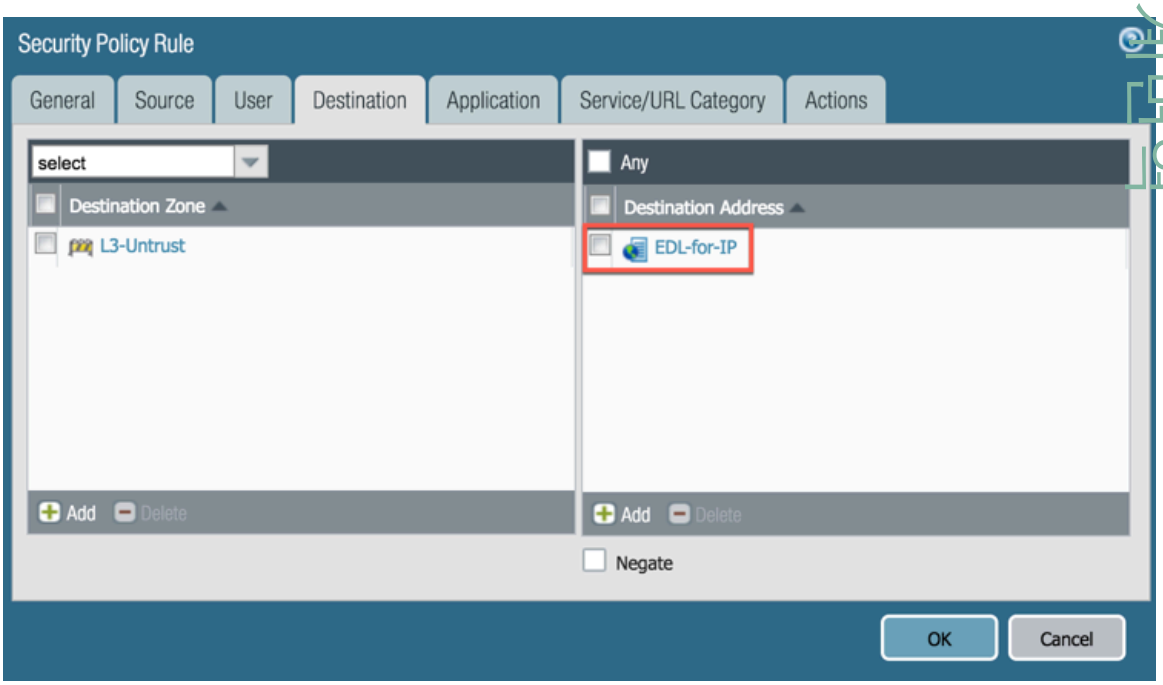
g. 이름 열에서 EDL을 추가할 보안 정책 규칙(예: **ServiceNow ip edl** 목록)을 찾아 클릭합니다.



이미지는 권한에 의해 사용되며 특권 및 독점입니다.

h. 보안 정책 규칙 대화 상자에서 대상탭을 선택하여 대상 주소 필드에 EDL을 추가합니다.

i. 사용 가능한 모든 EDL을 보려면 추가 아이콘을 클릭합니다.



이미지는 권한에 의해 사용되며 특권 및 독점입니다.

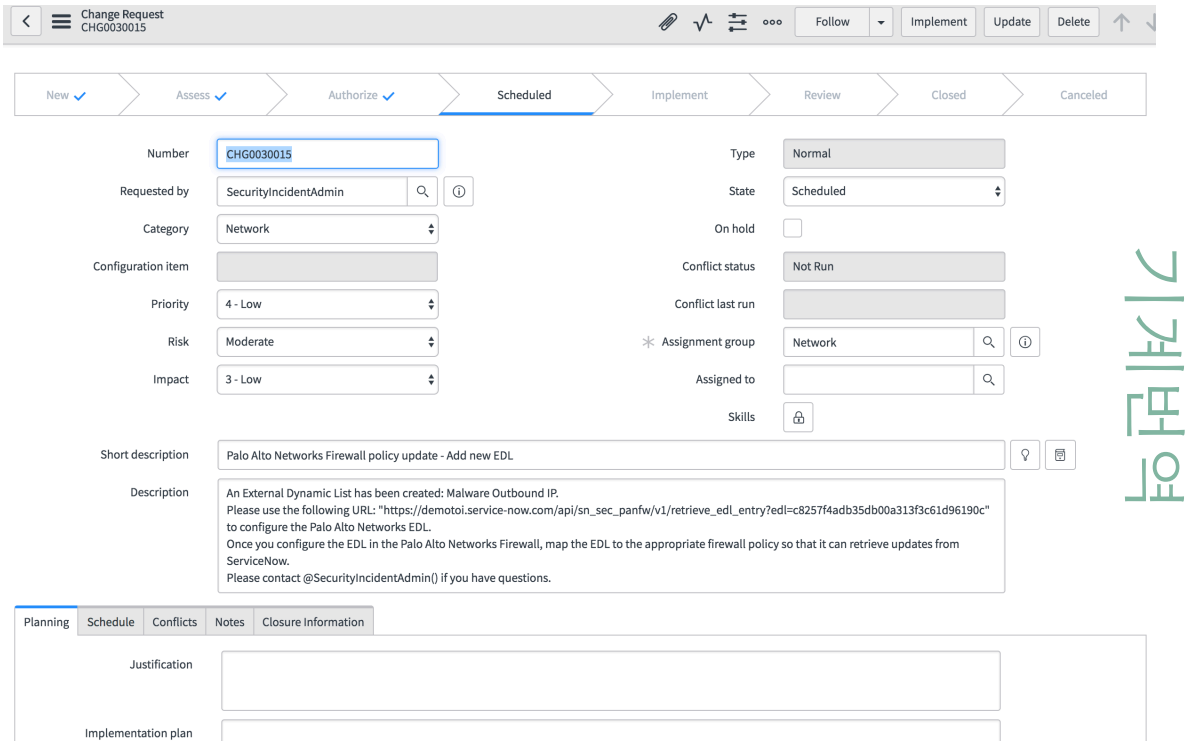
j. 확인을 클릭합니다.

k. EDL 오브젝트가 보안 정책에 ServiceNow AI Platform지정되었는지 확인한 후 에서 변경 요청으로 이동하여 EDL 오브젝트 지정과 연관된 태스크를 열고 태스크 닫기를 클릭하십시오. 두 작업이 모두 종결되면 변경 요청을 승인할 준비가 됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

l. 변경 요청 기록에서 승인자 관련 목록을 클릭하고 상태 열에서 항목을 선택하여 EDL 생성에 사용되는 요청을 엽니다.

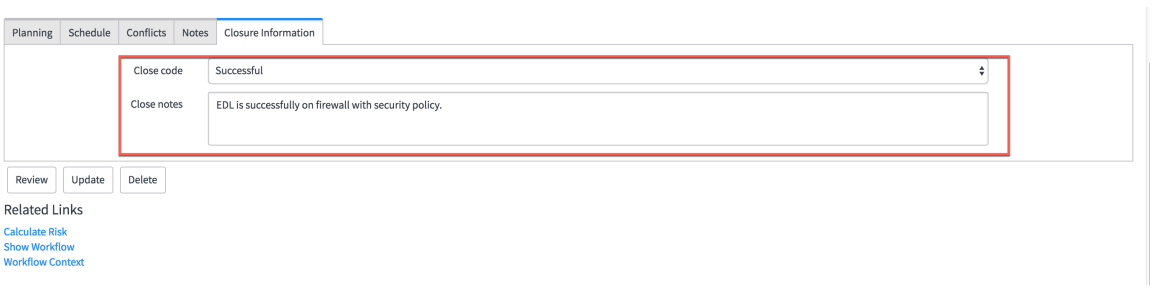
m. 오픈 승인 요청 양식에서 승인을 클릭합니다.
변경 요청 상태가 예약됨으로 전환됩니다.



n. 구현을 클릭합니다.

o. 종결 처리 정보 관련 탭을 클릭하고 메모를 입력하여 요청을 종결합니다.

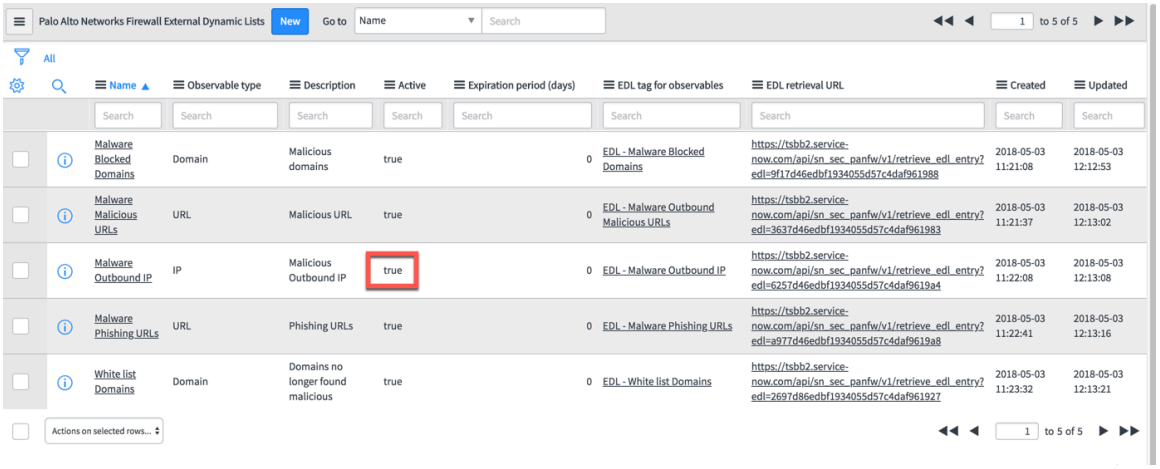
변경 요청을 종결하려면 이 필드의 항목이 필수입니다.



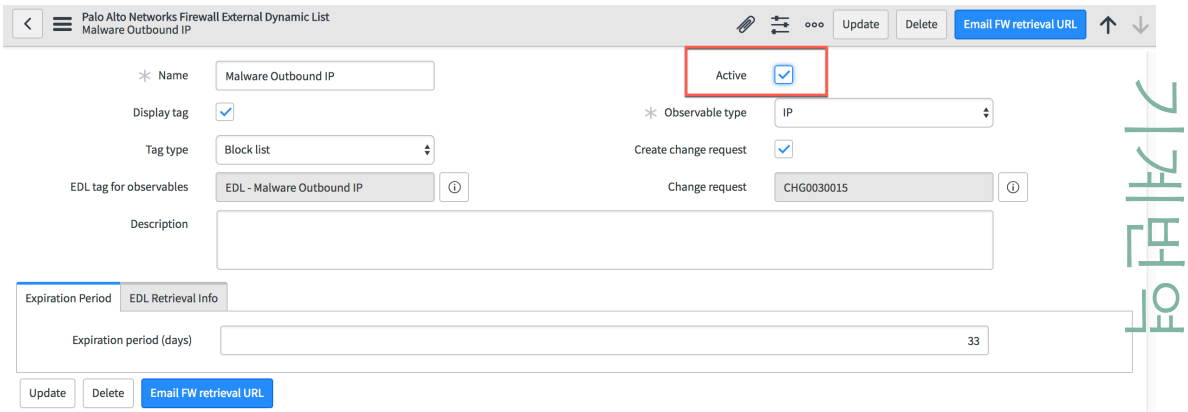
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

변경 요청이 종결되면 EDL이 자동으로 활성화됩니다. EDL이 활성화되었는지 확인하지 않은 경우 다음으로 이동합니다. **Palo Alto Networks NGFW** 통합 〉 방화벽 **EDL** 구성.

목록의 활성 열에서 EDL의 상태가 (true)임을 확인합니다.



이름 열에서 EDL 이름을 클릭하고 열려 있는 기록에서 활성 확인란도 선택되어 있는지 확인합니다.



이제 EDL이 EDL 항목을 수락할 준비가 되었습니다.

다음에 수행할 작업

보안 인시던트 또는 차단 목록에서 EDL 항목을 제출합니다.

에 대한 보안 인시던트 기록에서 **EDL** 항목 제출 **Palo Alto Networks Next-Generation Firewall**

보안 인시던트 기록에 첨부된 옵저버블은 승인을 위해 EDL에 대한 EDL(외부 동적 목록) 항목으로 제출됩니다. EDL 항목에 대한 승인 프로세스는 미리 구성된 워크플로우의 일부입니다. 방화벽은 EDL 목록에 포함된 EDL 항목(IP 주소, URL, 도메인)을 가져오고 정책을 적용합니다.

시작하기 전에

필요한 역할: EDL 항목을 제출하기 위한 sn_si.analyst. EDL 항목을 승인하려면 다음을 수행합니다. 승인은 기본적으로 sn_si.admin에 할당되지만 조직에서 요구하는 대로 이 권한을 할당할 수 있습니다.

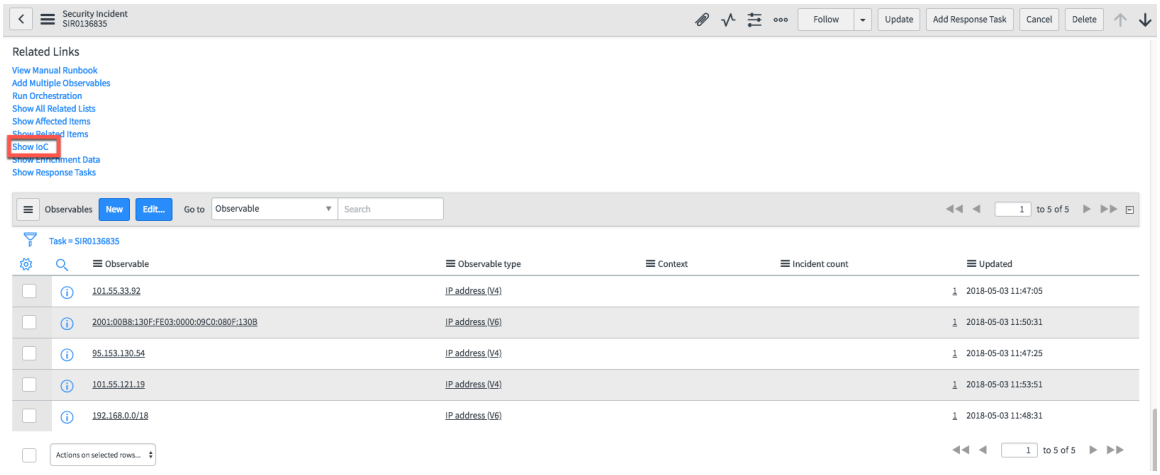
이 태스크 정보

sn_si.analyst 역할을 가진 사용자는 보안 인시던트 기록에 첨부된 옵저버블에 대한 차단을 요청하여 EDL 항목을 제출합니다. 제출되면 보류 중 상태의 EDL 항목이 생성되고 승인을 위해 전송됩니다. 다음 예는 URL 옵저버블에 대한 차단 요청을 보여줍니다.

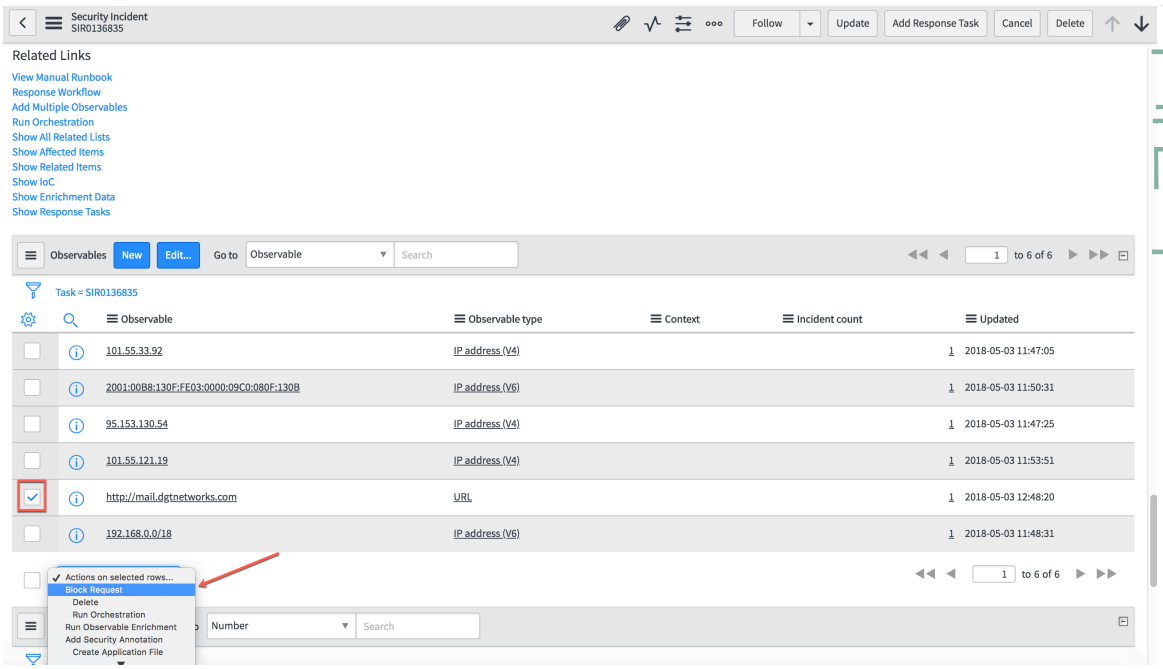
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 인시던트 〉 모든 인시던트 표시을 클릭하고 보안 인시던트 기록을 클릭하여 엽니다.
2. **IoC** 표시 관련 링크를 클릭합니다.



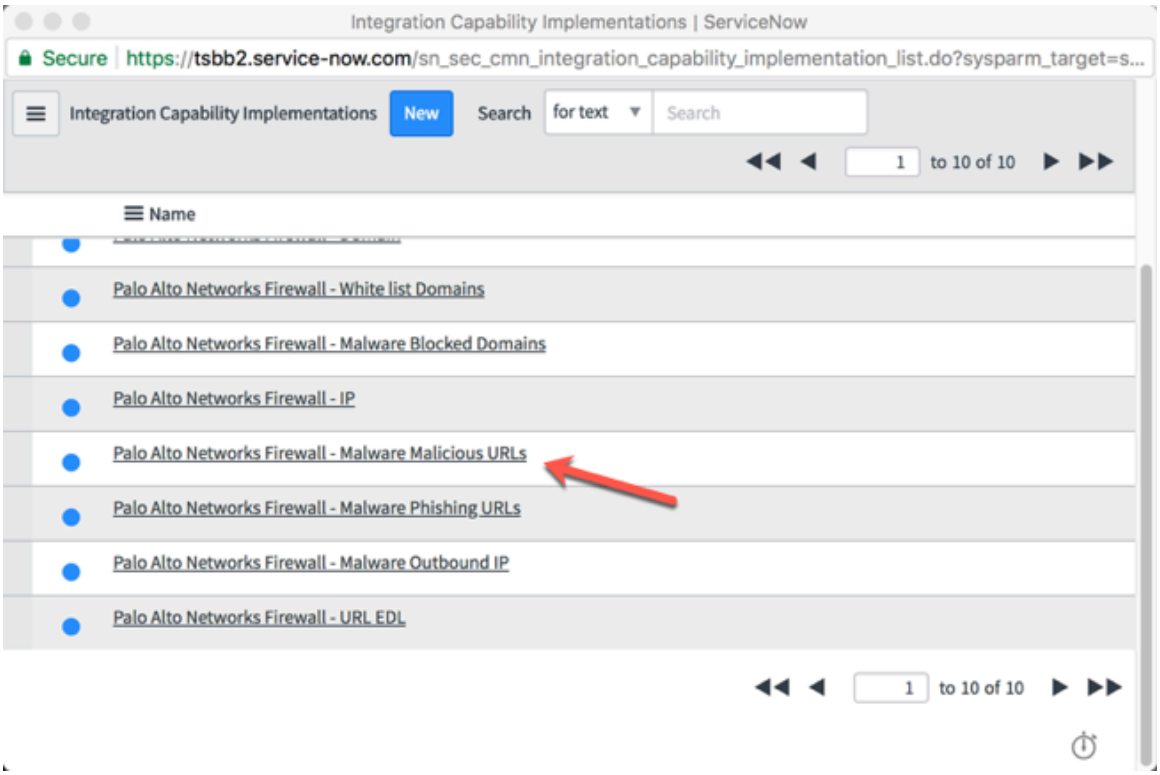
3. 옵저버블 관련 목록에서 차단할 옵저버블을 선택하고 선택한 행에 대한 작업 목록에서 차단 요청을 선택합니다.



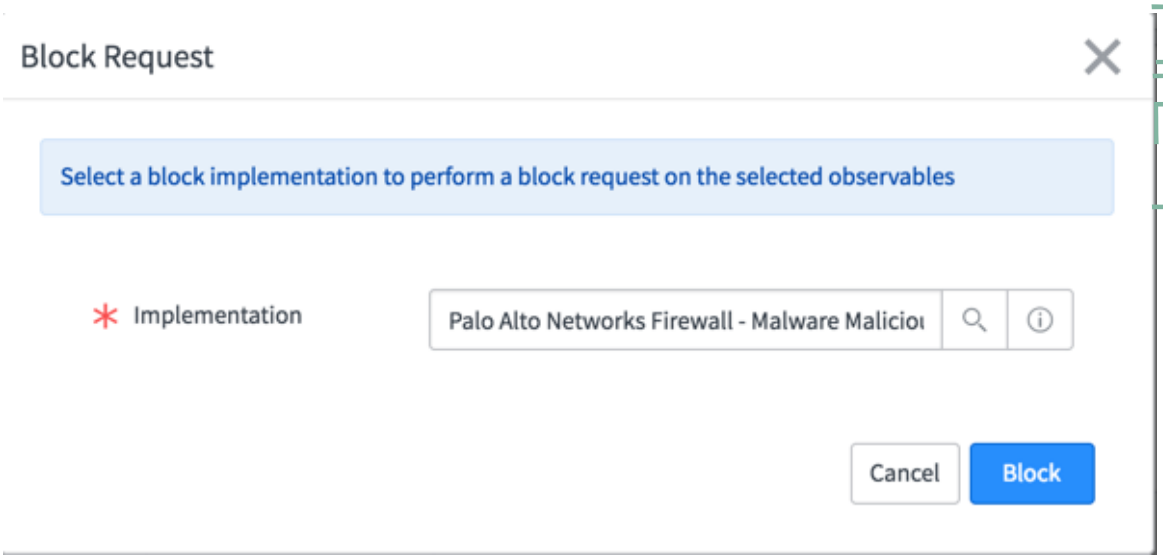
4. 표시되는 대화 상자에서 검색 아이콘( )을 클릭합니다.
5. 표시되는 목록에서 이 항목을 연결할 EDL을 선택합니다.

> 주:
> 이 예에서는 항목 옵저버블 유형(URL)이 EDL 옵저버블 유형(URL)과 일치해야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

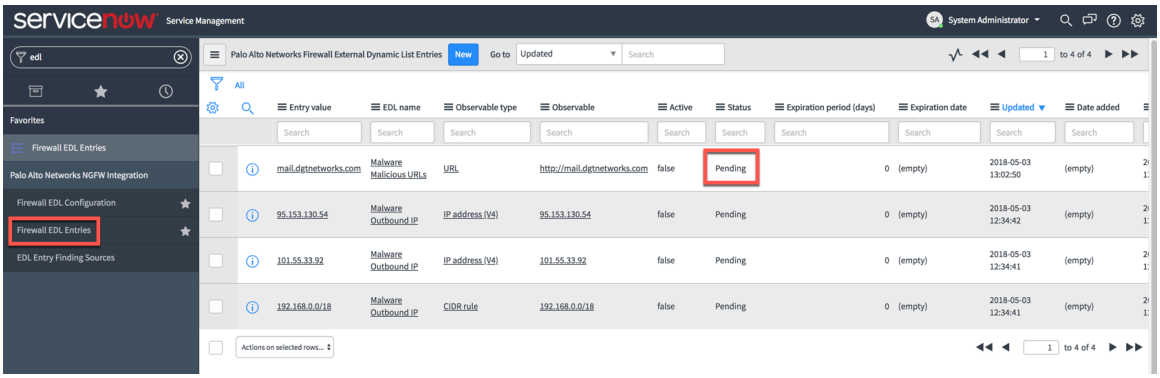


6. 구현 필드에 EDL 이름이 표시된 블록 요청 대화 상자에서 블록을 클릭합니다.



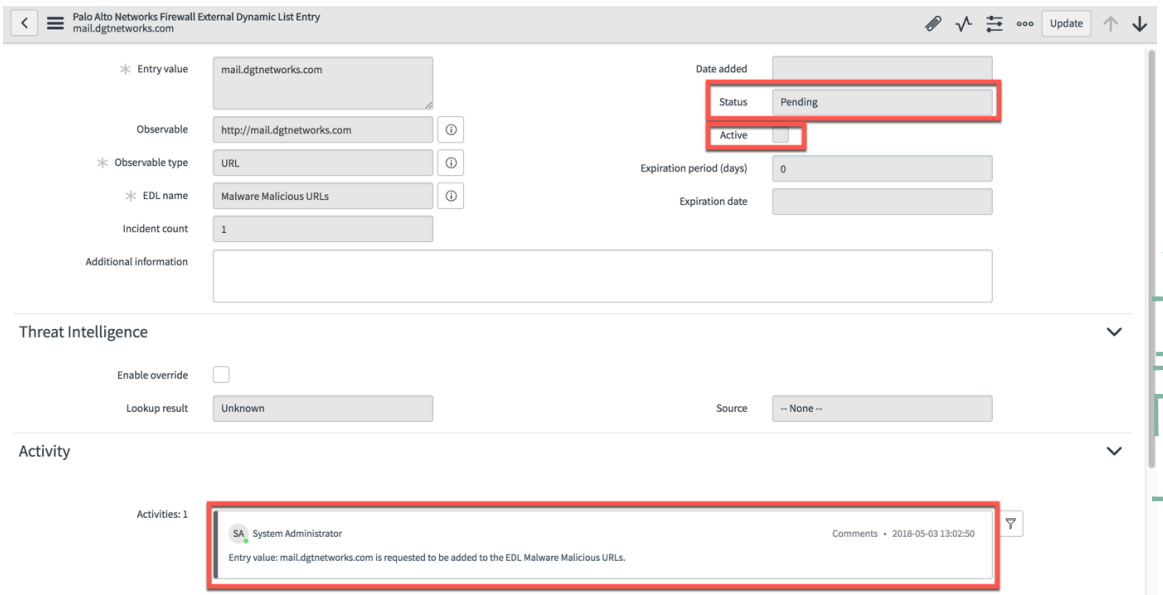
7. 다음으로 이동 **Palo Alto Networks NGFW** 통합 〉 방화벽 **EDL** 항목 을 클릭하고 방화벽 **EDL** 항목을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



8. Palo Alto Networks 방화벽 외부 동적 목록 항목 목록의 항목 값 열에서 옵저버블을 클릭하여 기록을 엽니다.

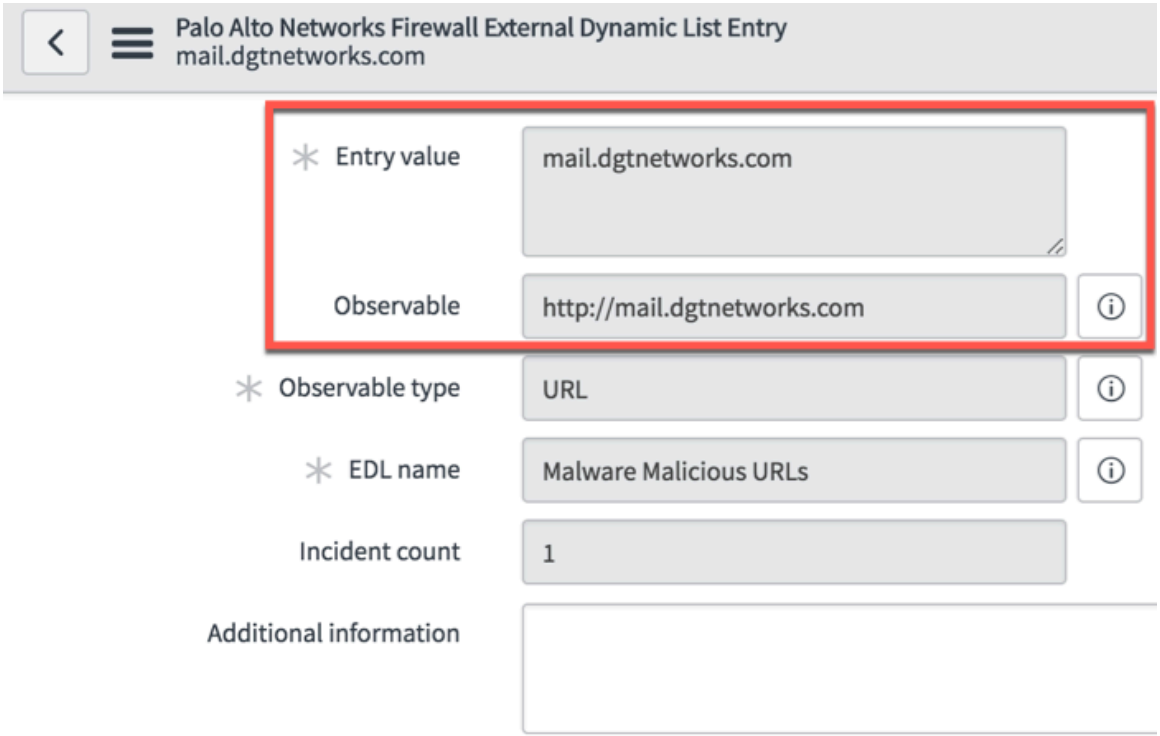
이 예에서는 **mail.dgtnetworks.com** 에 대한 기록이 표시됩니다.



상태가 보류 중이고, 활성 확인란의 선택이 취소되어 있으며, 옵저버블 추가 요청이 작업 메모에 표시됩니다. 이 EDL 항목 요청을 승인할 준비가 되었습니다.

항목 값 및 옵저버블 필드에는 URL 옵저버블에 대한 다양한 형식이 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



필드 옆의 아이콘은 옵저버블 테이블에 대한 링크입니다ServiceNow AI Platform#.

필드(http://mail.dgtnetworks.com)의 값은 옵저버블 테이블에 연결되며 인시던트 트리거 이벤트에서 보안 인시던트 응답 가져온 형식과 일치합니다.

EDL ServiceNow AI Platform# URL 형식과 호환 Palo Alto Networks 되도록 EDL 항목을 자동으로 수정할 수 있습니다.

이 예에서 옵저버블은 http://mail.dgtnetworks.com(http:// 프로토콜)를 사용하여 생성되었으며 이 형식은 옵저버블 필드에 표시됩니다. http:// 프로토콜은 에 의해 ServiceNow AI Platform# 옵저버블에서 자동으로 제거되므로 호환 Palo Alto Networks 되며 검색할 수 있습니다. 결과적으로 ## # 필드에 mail.dgtnetworks.com 표시됩니다.

다음에 수행할 작업
EDL 항목을 승인합니다.

관련 정보

에 대한 EDL 항목 예외 Palo Alto Networks Next-Generation Firewall

에 대한 차단 목록에서 **EDL** 항목 제출 **Palo Alto Networks Next-Generation Firewall**

악성으로 판단되고 특정 ServiceNow AI Platform 보안 인시던트와 연결되지 않은 옵저버블의 경우 차단 목록에서 EDL(External Dynamic List) 항목을 제출합니다.

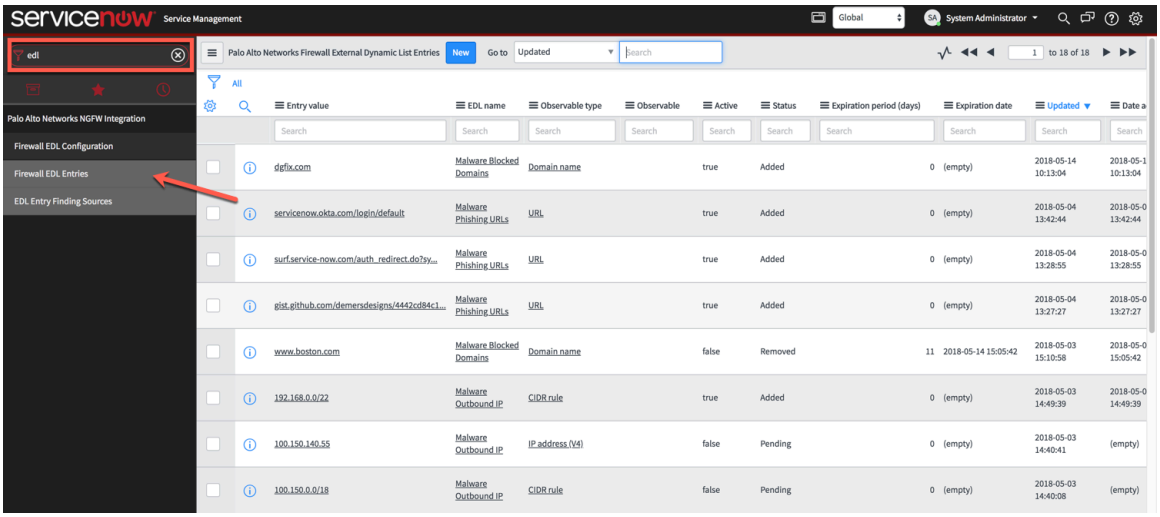
시작하기 전에
필요한 역할: sn_si.analyst

이 태스크 정보
악성으로 판단한 옵저버블을 차단하거나, 악성이 아닌 옵저버블을 허용하고 옵저버블이 특정 ServiceNow AI Platform 보안 인시던트 기록과 연결되지 않은 경우 차단 목록에서 직접 EDL 항목을 제출합니다. 이러한 유형의 EDL 항목의 예로는 특정 사이트의 URL 또는 도메인이 있을 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 **Palo Alto Networks NGFW** 통합 〉 방화벽 **EDL** 항목.



2. 방화벽 **EDL** 항목 모듈을 클릭합니다.

3. Palo Alto Networks 방화벽 외부 동적 목록 항목 목록에서 새로 만들기를 클릭합니다.

4. 표시되는 새 기록의 항목 값 필드에 옵저버블 값을 입력합니다.
이 항목의 두 가지 가능한 결과:

양식의 나머지 필드는 자동으로 완성됩니다.

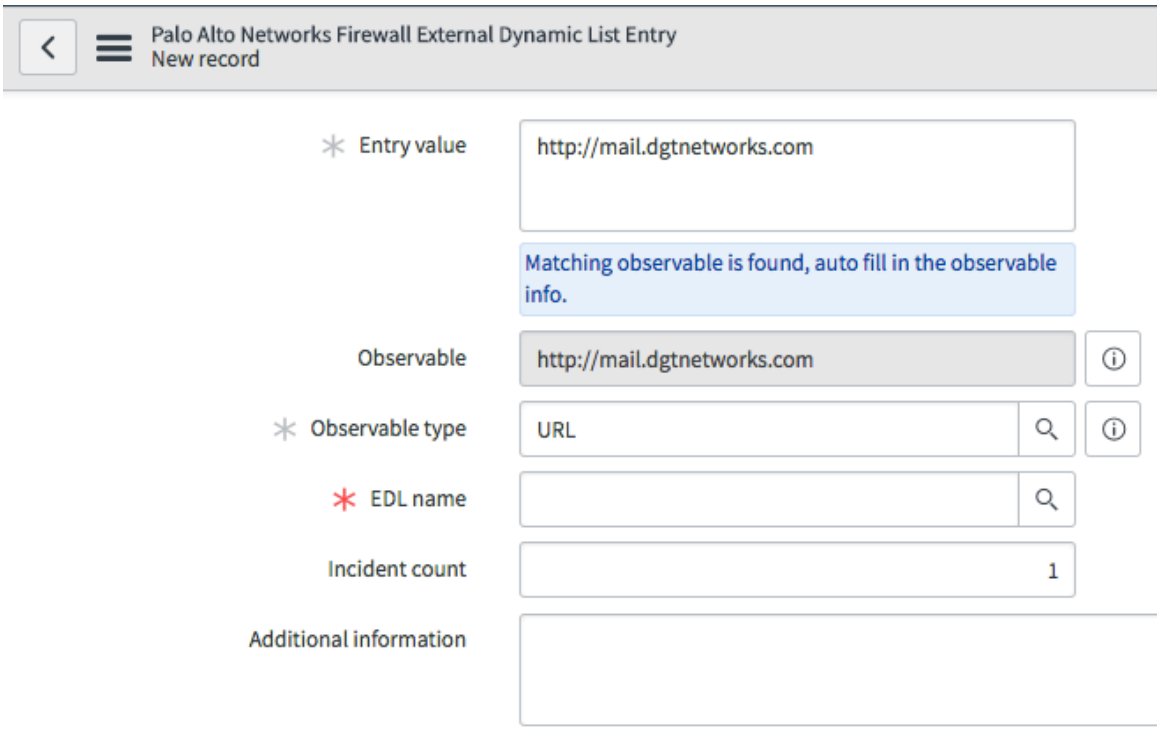
일치하는 옵저버블이 발견되고 일치하는 옵저버블이 존재한다는 메시지가 표시됩니다. 이 항목을 첨부할 EDL을 선택하고 제출을 클릭합니다. 만료 기간을 설정하기 전에 이 항목을 연결할 EDL을 선택합니다.

양식을 작성하라는 메시지가 표시됩니다.

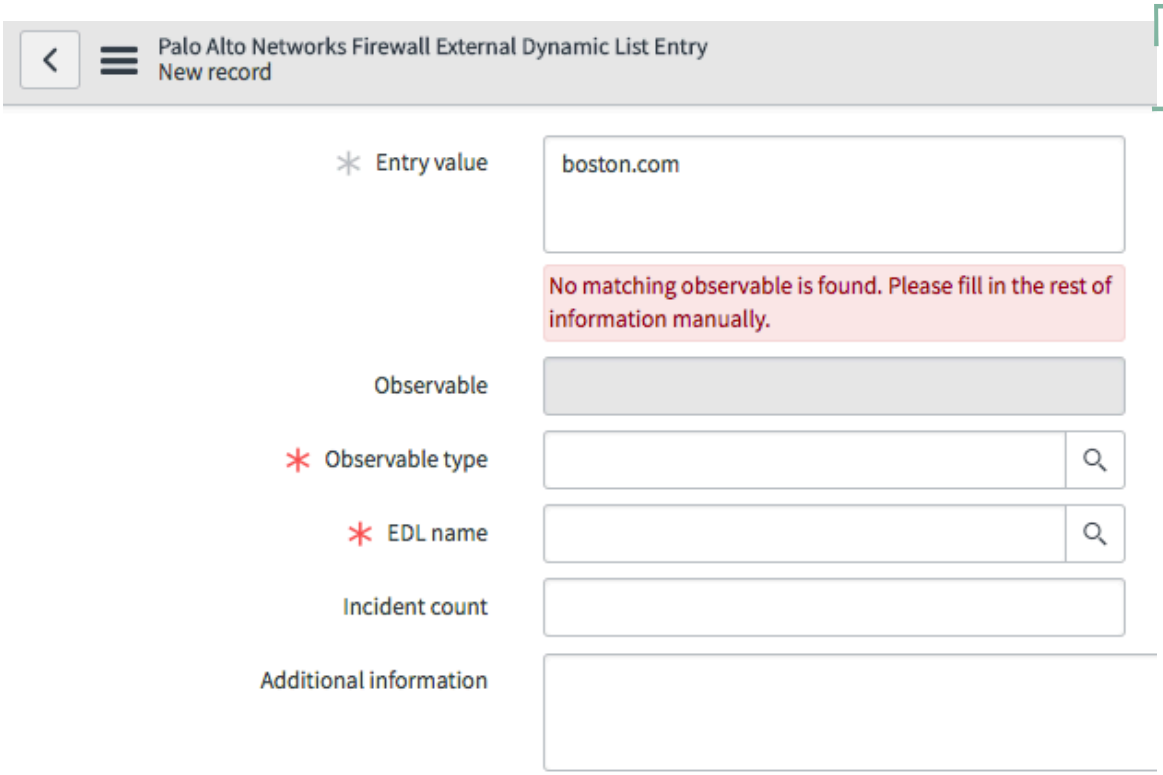
일치하는 옵저버블을 찾을 수 없습니다. 양식을 작성해야 합니다. 완료 후 옵저버블을 연결할 EDL을 선택하고 제출을 클릭합니다. 옵저버블 기록이 생성됩니다.

다음 그림은 기존 도메인 옵저버블의 예와 필드가 자동으로 완성되는 방법을 보여줍니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



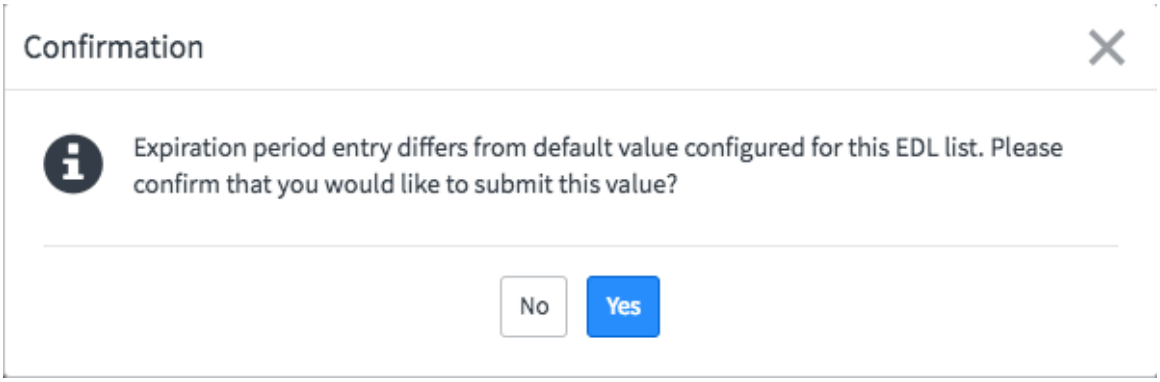
5. 검색 아이콘을 클릭하여 항목을 첨부할 EDL을 선택합니다.
6. 제출을 클릭합니다.
   워크플로우에 이메일 승인이 구성되어 있으면 승인 이메일 요청이 전송됩니다.
7. 나머지 정보를 수동으로 입력하도록 요청하는 메시지가 표시되면 필드에 내용을 입력합니다.



8. 제출을 클릭합니다.

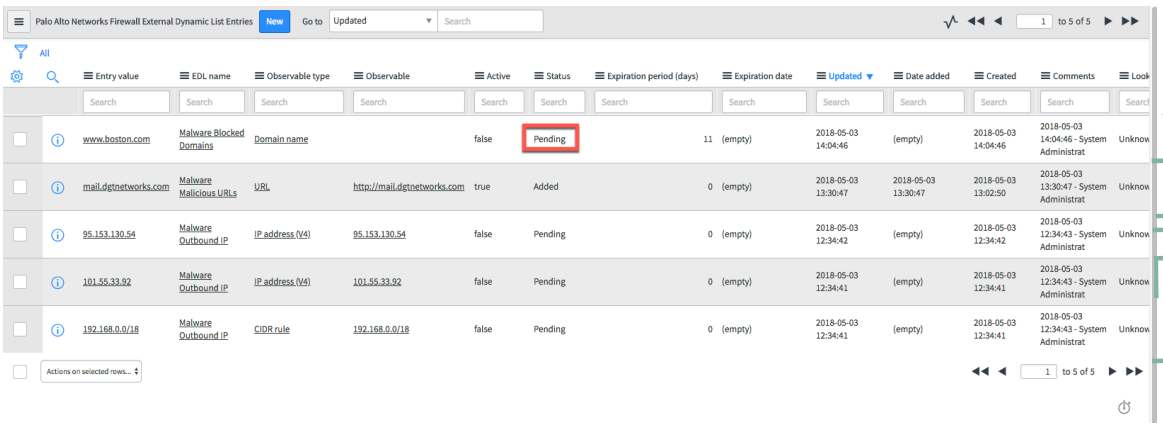
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

EDL 항목의 기본 만료 기간을 변경한 경우 해당 기간이 선택한 EDL과 다르다는 경고 확인 대화 상자가 표시됩니다.



9. 만료 기간을 구성하는 하나의 옵션을 선택합니다.

10. 표시되지 않으면 **Palo Alto Networks** 방화벽 외부 동적 목록 항목 목록으로 이동하여 항목의 상태가 보류 중인지 확인합니다.



이제 항목을 승인할 준비가 되었습니다.

다음에 수행할 작업
EDL 항목을 승인합니다.

관련 정보

에 대한 EDL 항목 예외 Palo Alto Networks Next-Generation Firewall

EDL 항목 승인

EDL(외부 동적 목록) 항목에 대한 승인 프로세스는 미리 구성된 워크플로우의 일부입니다. EDL에서 항목이 활성화되기 전에 EDL 항목을 승인합니다. EDL 항목을 승인하면 방화벽이 항목을 검색하고 그 시점부터 옵저버블이 차단됩니다.

시작하기 전에
필요한 역할: EDL 항목에 대한 승인은 기본적으로 sn_si.admin에 할당되지만 조직에서 요구하는 대로 이 권한을 할당할 수 있습니다. 다음 예시 ServiceNow AI Platform 에서는 관리자에게 승인 권한이 있습니다.

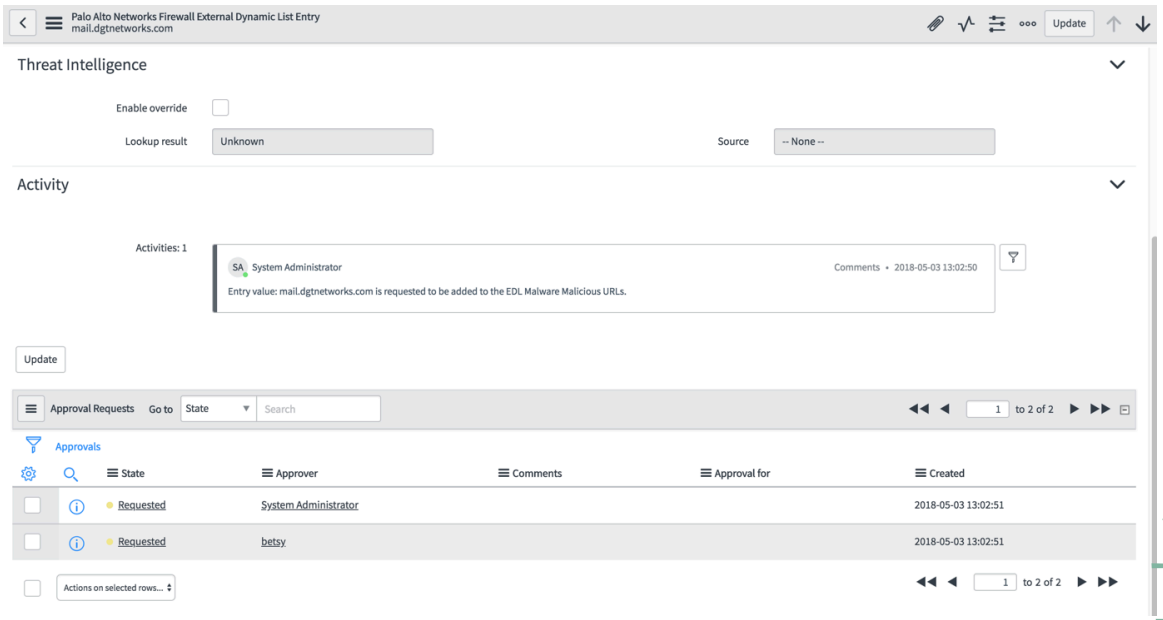
이 태스크 정보
승인 프로세스를 사용하는 경우 EDL 항목은 승인될 때까지 EDL에서 활성화되거나 비활성화되지 않습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

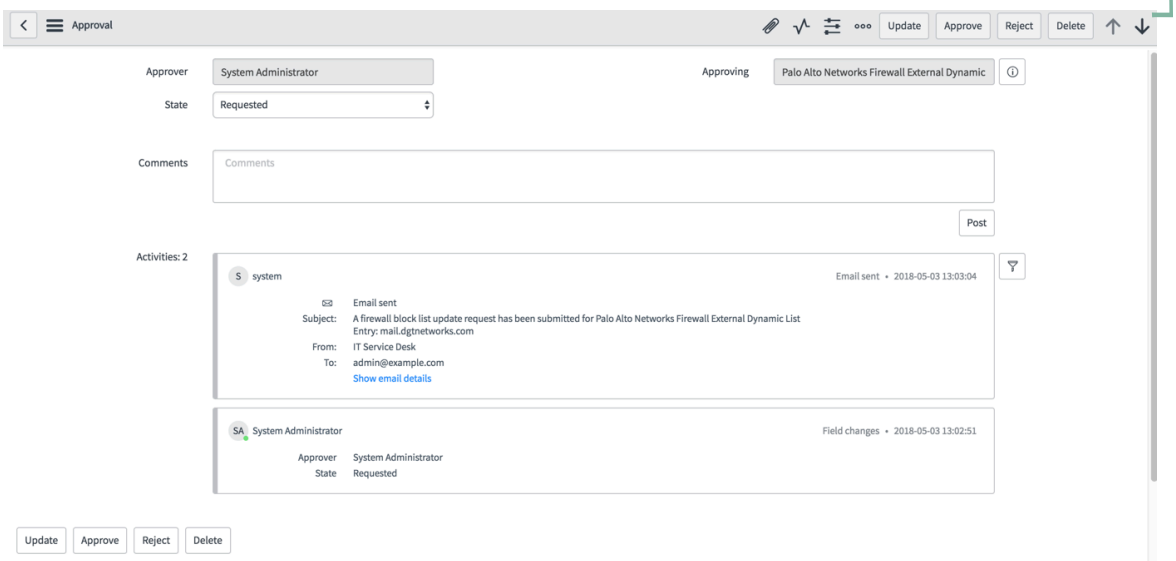
프로시저

1. 다음으로 이동 모두 〉 **Palo Alto Networks NGFW** 통합 〉 방화벽 **EDL** 항목 을 클릭하고 EDL 기록을 엽니다.
2. EDL 기록에서 승인 요청 섹션으로 스크롤합니다.

   주:
   시스템 설정에서 탭 구분 양식을 선택한 경우에는 섹션이 기록에 탭으로 표시됩니다.

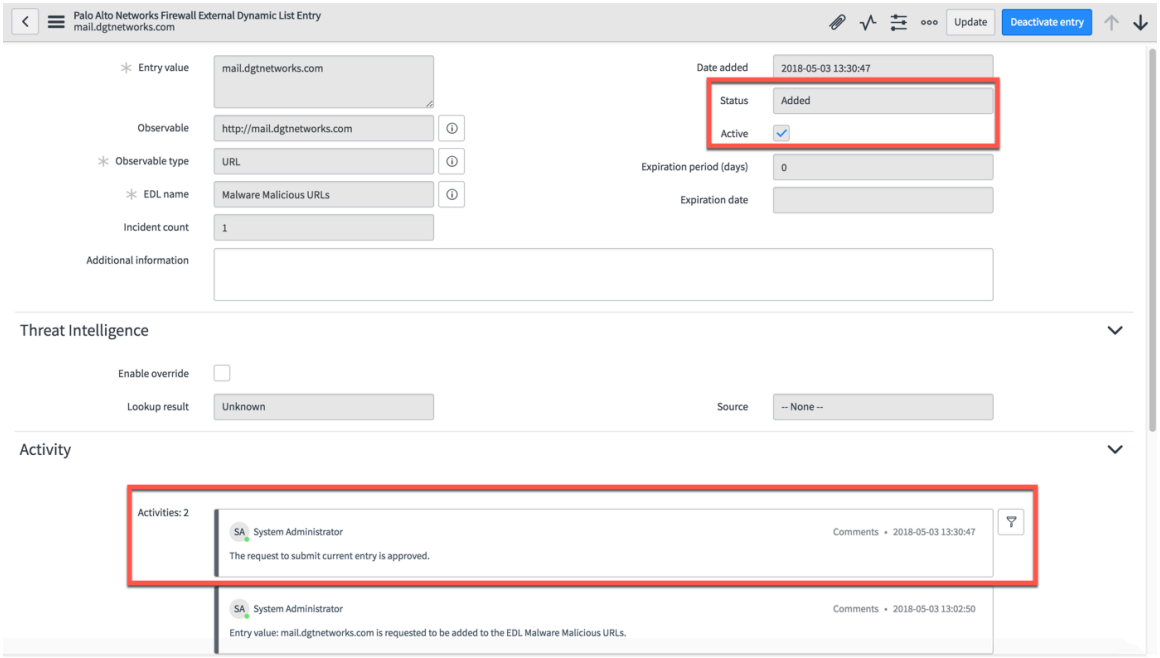


3. 승인 요청의 상태 열에서 항목을 클릭하여 엽니다.
   승인 기록이 표시됩니다.

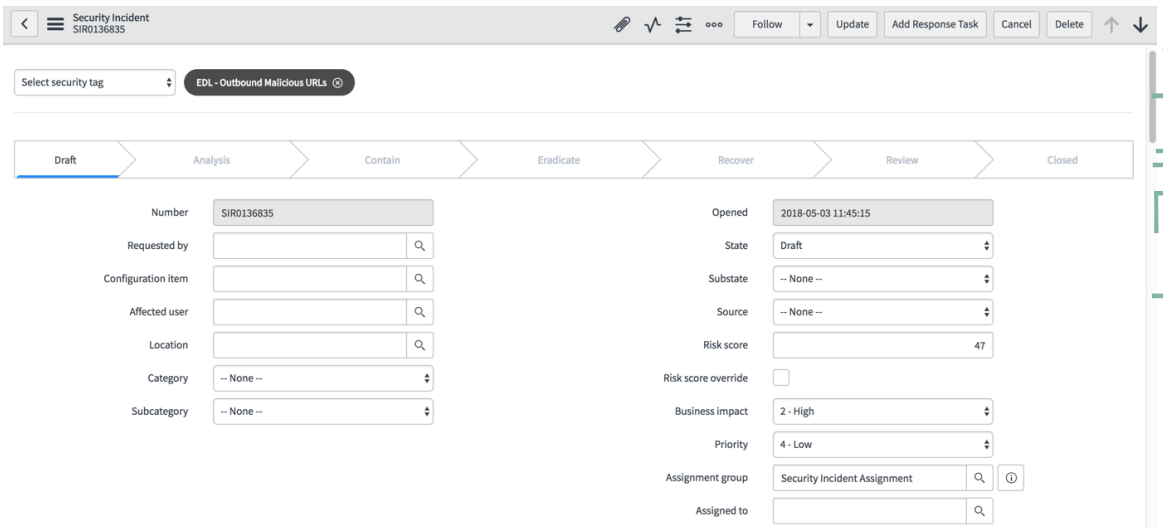


4. EDL 항목을 승인하기 위해 하나의 옵션을 선택합니다.
   EDL 항목을 승인하고 활성화되면 다음 Palo Alto Networks Next-Generation Firewall 검색 간격 후에 EDL 항목을 검색합니다. 항목이 검색되면 해당 시점부터 옵저버블이 차단됩니다. 다음 그림에서는 활성 확인란이 선택되어 있고 상태가 추가됨이며 작업 메모에 요청이 승인되었음을 나타냅니다.

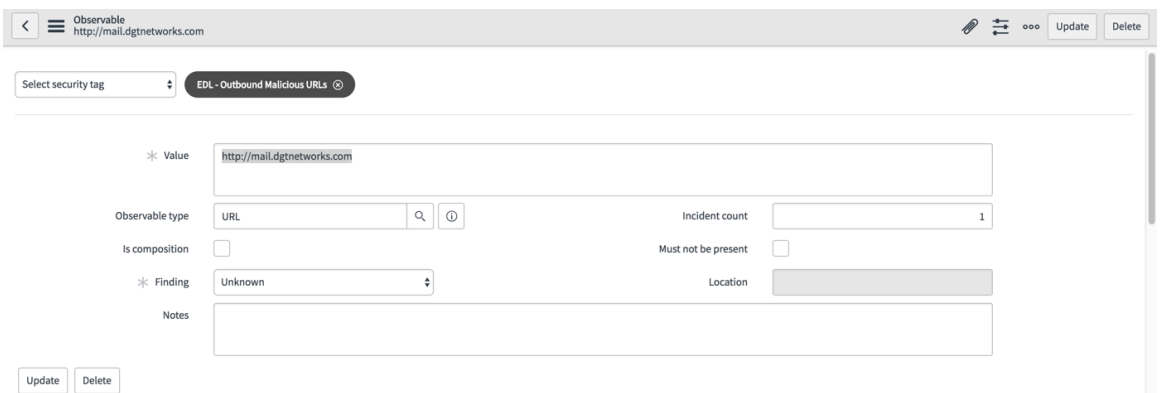
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



EDL 항목이 승인되고 활성화되면 보안 인시던트 기록에 보안 태그가 표시됩니다. 태그가 기록 상단에 표시됩니다.



보안 태그는 옵저버블 기록에도 표시됩니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

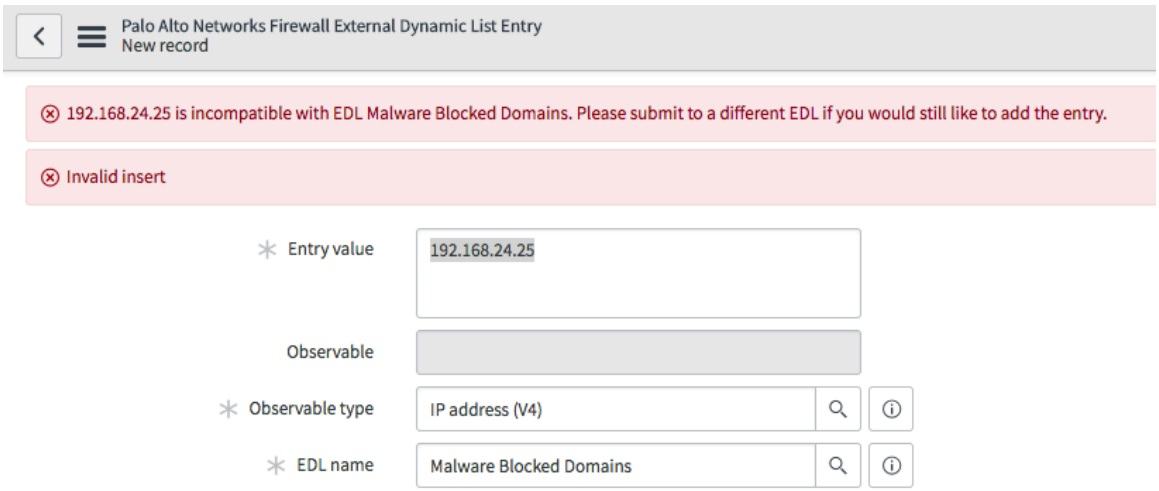
에 대한 **EDL** 항목 예외 **Palo Alto Networks Next-Generation Firewall**

EDL(External Dynamic List) 항목을 EDL에 추가하는 데는 제한이 있습니다. EDL 항목을 EDL에 추가하려고 할 때 중복, 호환성 또는 CIDR(Classless Inter-Domain Routing) 충돌이 있는 경우 이러한 오류를 해결하는 데 도움이 되는 오류 메시지가 표시됩니다.

호환성 예외

각 EDL은 해당 옵저버블 유형과 호환되는 항목만 허용합니다. 도메인 EDL을 생성하는 경우 옵저버블 IP 주소를 첨부하려고 하면 호환되지 않는 오류 메시지가 표시됩니다. 예를 들어 도메인 EDL은 다음 그림과 같이 도메인 옵저버블만 수락할 수 있습니다.

호환성 오류

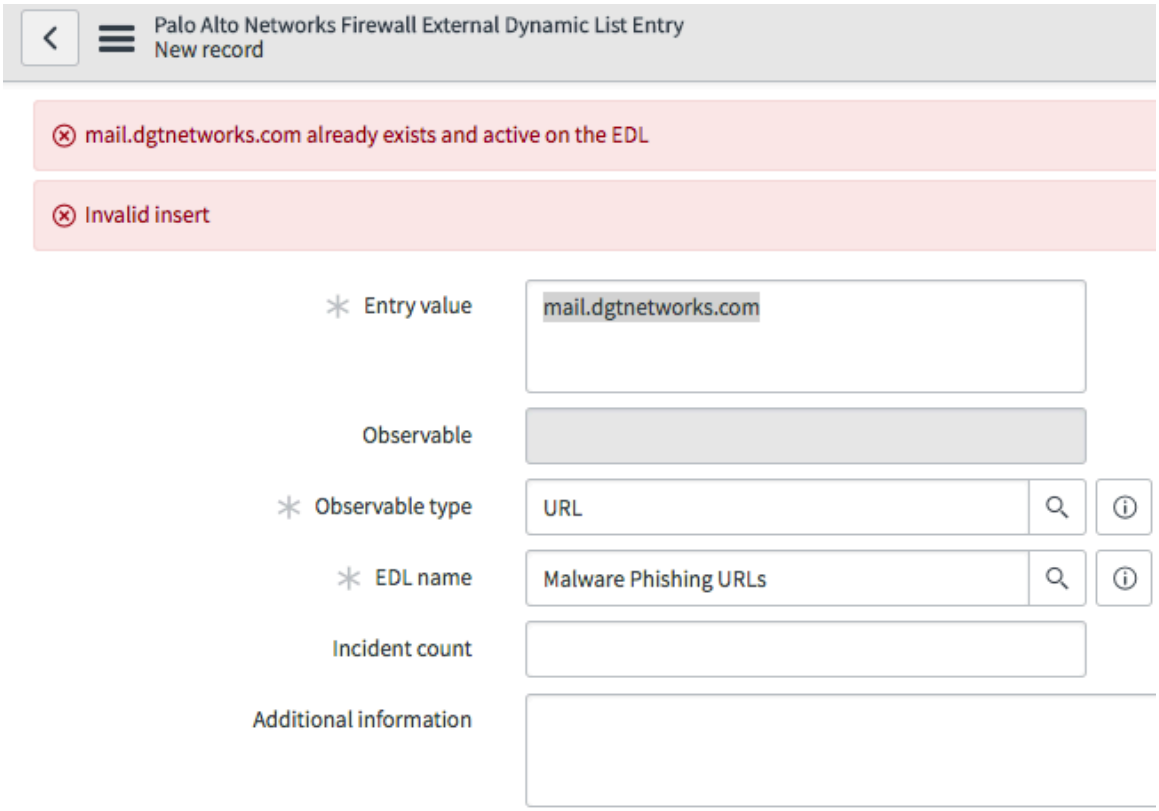


중복 예외

옵저버블 유형은 동일한 옵저버블 유형의 여러 EDL에서 옵저버블을 활성화할 수 없습니다. URL 옵저버블이 URL EDL에서 이미 활성화되어 있는 경우 피싱 URL EDL에서 동일한 옵저버블을 활성화하려고 하면 중복 오류 메시지가 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

중복 오류

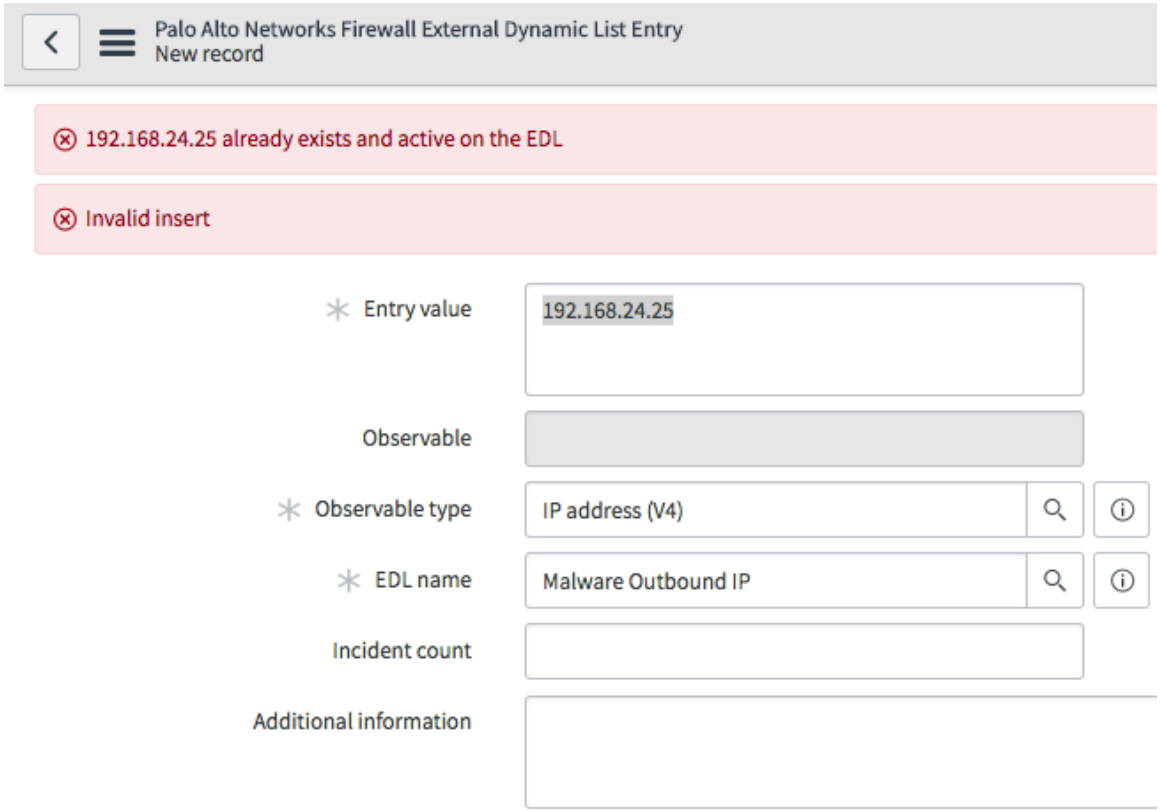


CIDR(Classless Inter-Domain Routing) 예외

EDL에 단일 IP 주소를 연결하려고 할 때 이 IP 주소가 이미 EDL에 있는 CIDR 옵저버블의 일부인 경우 CIDR 상충 오류가 표시됩니다. 이 오류는 단일 IP 주소가 CIDR 옵저버블의 일부로 EDL에 이미 포함되어 있음을 나타냅니다. 예를 들어, 192.168.24.25 은 CIDR 블록 192.168.0.0/22의 일부입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

CIDR 충돌



(선택 사항) 의 보안 태그 이름 편집 **Palo Alto Networks Next-Generation Firewall**

EDL(외부 동적 목록) 레코드를 만들 때 태그 표시 확인란을 선택하면 보안 태그의 태그 이름과 색상을 편집할 수 있습니다. 보안 태그는 이미 차단된 옵저버블을 추적하는 데 도움이 됩니다.

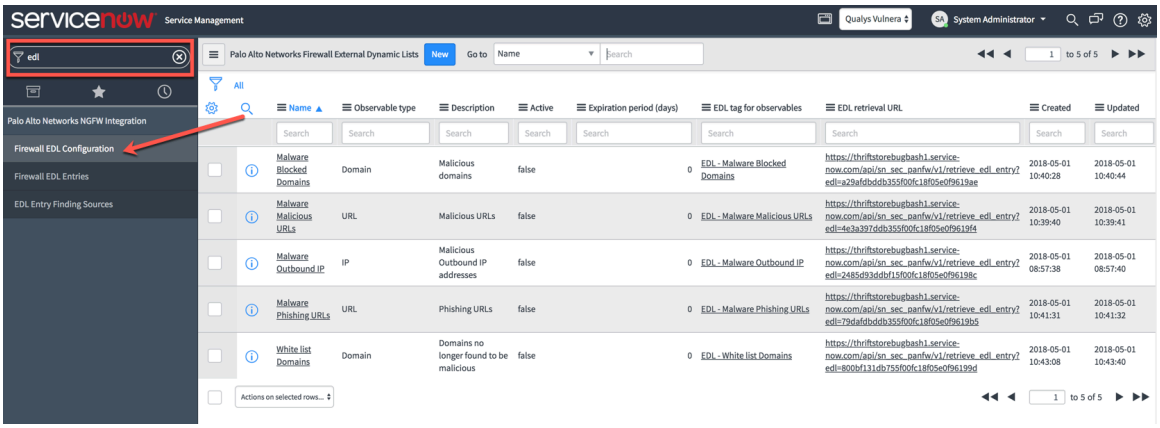
시작하기 전에
필요한 역할: sn_si.admin

이 태스크 정보
보안 태그를 사용하면 차단 목록에 옵저버블이 있는 보안 인시던트를 빠르게 식별할 수 있습니다. 또한 태그는 옵저버블이 이미 차단되었는지 또는 EDL에서 제거되었는지 식별하는 데 도움이 됩니다. 기본적으로 보안 태그의 색은 차단 목록 항목의 경우 검은색이고 허용 목록 항목의 경우 회색입니다. 특정 태그를 더 쉽게 인식할 수 있도록 태그의 이름과 색상을 변경할 수 있습니다.

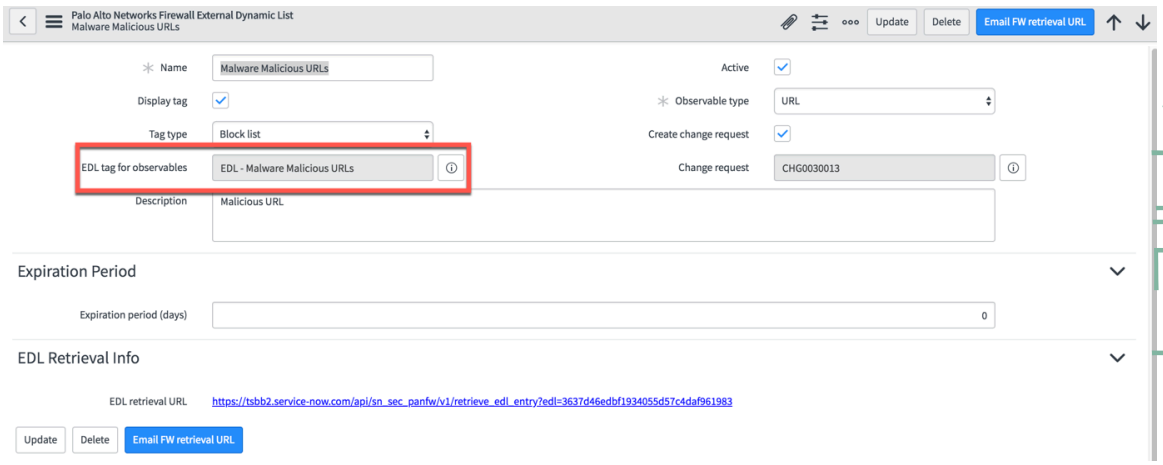
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

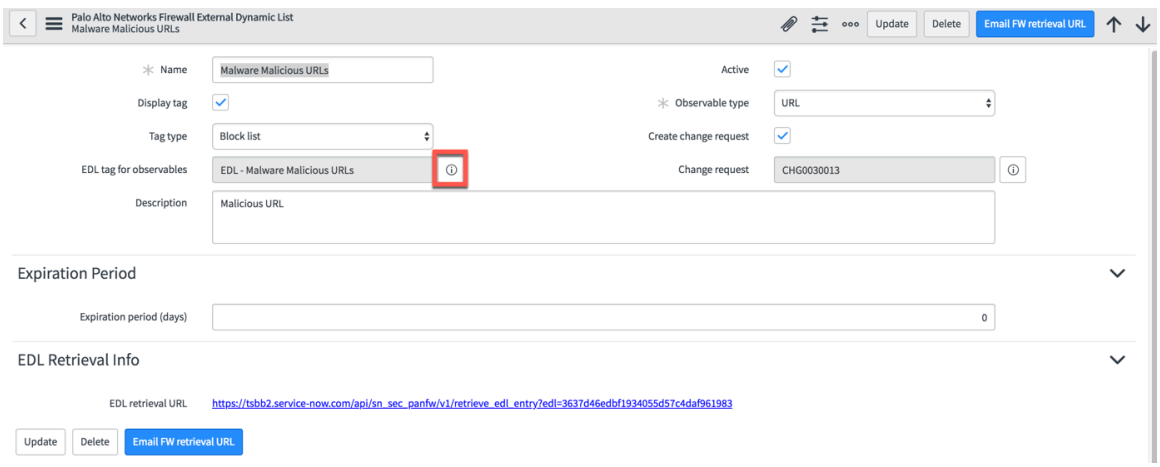
1. 다음으로 이동 모두 〉 **Palo Alto Networks NGFW** 통합 〉 방화벽 **EDL** 구성.



2. 이름 열에서 항목을 클릭하여 엽니다
EDL 기록이 표시됩니다. 기본적으로 보안 태그 이름은 EDL을 만들 때 EDL의 이름 필드에 입력한 값과 동일합니다. 기본적으로 이름에는 *EDL* 접두사(예: EDL – 맬웨어 악성 URL)도 포함됩니다.

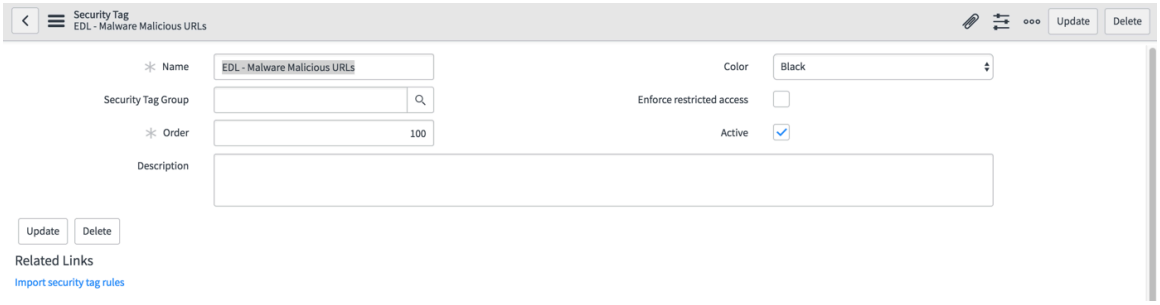


3. 옵저버블에 대한 **EDL** 태그 옆에 있는 정보 아이콘(ⓘ)을 클릭한 다음 기록 열기를 클릭합니다.

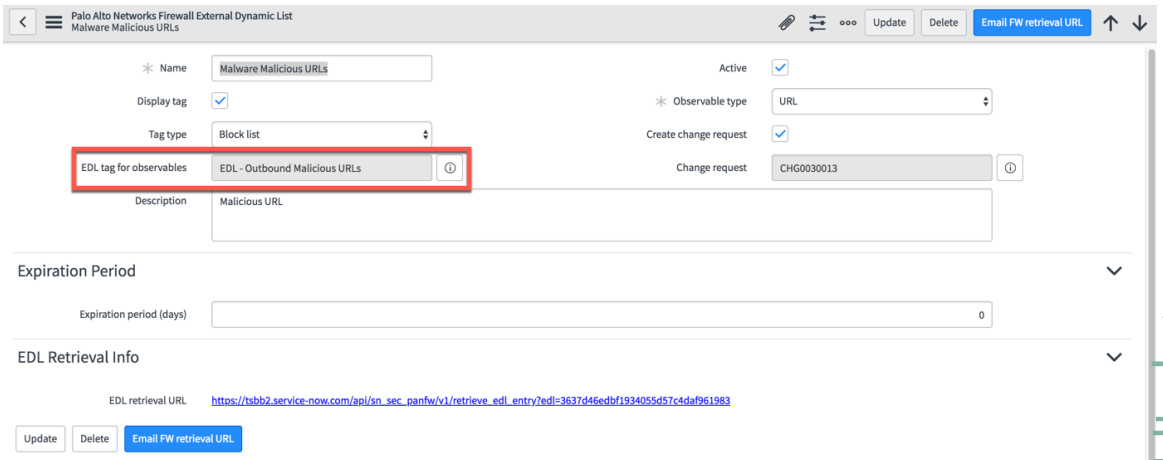


보안 태그 양식이 표시됩니다.

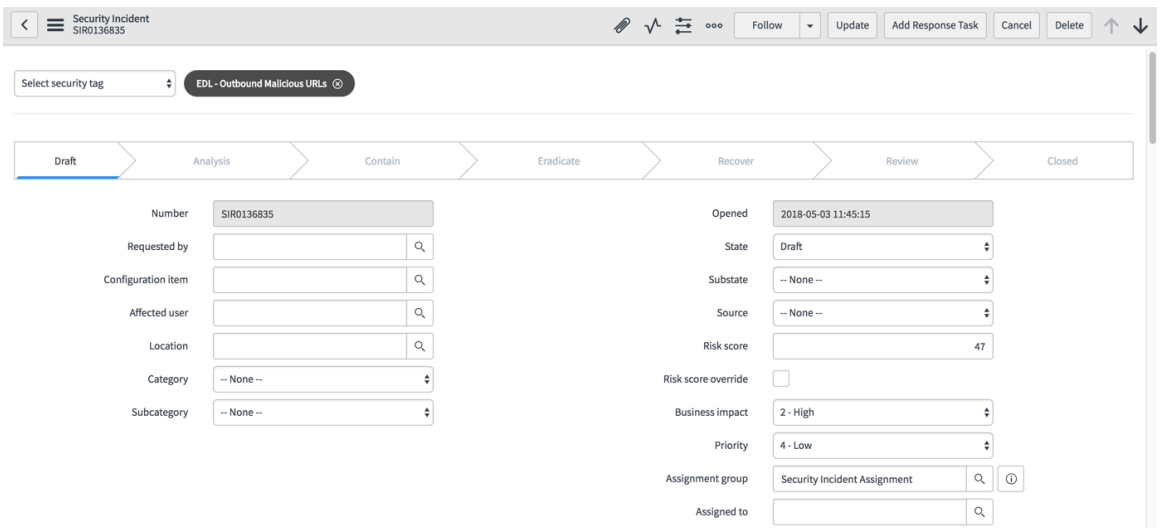
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 이름 필드에서 보안 태그 이름을 수정하고 업데이트를 클릭합니다.
업데이트된 EDL 기록이 수정된 태그 이름으로 표시됩니다. 다음 예시에서는 ##### 가 태그 이름에 추가되었습니다. 새 태그 이름에 EDL 프리픽스를 유지하면 통합과 Palo Alto Networks Next-Generation Firewall 연결된 태그를 식별할 수 있습니다.



보안 태그는 옵저버블이 EDL에 추가될 때마다 보안 인시던트 기록 및 옵저버블 기록의 각 옵저버블 유형(IP, URL, 도메인)에 대해 표시됩니다.



옵저버블이 EDL에 이미 추가되었고 이 옵저버블에 대한 보안 인시던트에 보안 태그가 표시되는 경우 EDL 보안 태그도 생성되는 후속 보안 인시던트 기록에 자동으로 표시됩니다. 이 중복은

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵저버블이 이미 차단 목록에 있음을 알려줍니다. 이 옵저버블을 추가하고 다시 차단할 필요가 없습니다.

옵저버블이 더 이상 차단되지 않으면 보안 인시던트 기록 또는 옵저버블 기록에 보안 태그가 표시되지 않습니다. 이 경우 보안 태그가 없으면 옵저버블의 만료 날짜가 지났거나 옵저버블이 EDL에서 비활성화되었을 수 있습니다.

제거

인스턴스에서 제거하고 Palo Alto Networks Next-Generation FirewallServiceNow AI Platform 통합에서 나머지 부분을 모두 제거하려면 설명서 사이트에서 애플리케이션 제거 지침을 참조하십시오 ServiceNow .

시작하기 전에
필요한 역할: 시스템 관리자(admin)
ServiceNow 제품 설명서 웹 사이트에서 애플리케이션 제거를 참조하십시오.

PhishTank 통합

PhishTank 는 사용자가 의심되는 위협을 제출하고 시스템의 다른 사용자가 피싱 위협이 합법적인지 여부를 결정하기 위해 투표하는 커뮤니티 기반 피싱 확인 시스템입니다. 위협 인텔리전스 결과를 제품과 통합 ServiceNow AI Platform 보안 운영 하면 분석가가 피싱 관련 보안 인시던트 또는 조사에 대한 추가적인 통찰력을 얻을 수 있습니다.

통합은 PhishTank 잠재적인 피싱 사이트 URL에 대한 조회를 수행합니다.

워크플로우는 새 옵저버블이 보안 인시던트에 도착하면 이를 확인합니다. 옵저버블이 API 통합에서 인식되는 유형인 경우 옵저버블이 평가됩니다. 악성으로 확인된 옵저버블에 태그가 지정됩니다.

PhishTank 설치 및 구성

인스턴스에서 통합을 실행하기 전에 설치 및 구성 단계를 PhishTank 완료하여 애플리케이션이 .ServiceNow AI Platform 보안 운영

시작하기 전에
설치하기 전에 다음 설정 검사 목록을 완료합니다. 이러한 설정 작업은 원활한 설치 및 구성을 위해 필요합니다.

작업 설정	설명
인스턴스에 필요한 ServiceNow AI Platform 역할을 할당했는지 확인합니다.	예상 결과의 설치, 구성 및 검증에 필요한 역할은 다음과 같습니다. • 시스템 관리자(admin)가 앱을 설치하고 보안 인시던트 관리자(sn_si.admin) 역할을 할당합니다. • 보안 인시던트 관리자(sn_si.admin)는 구성을 감독하고 예상 결과를 검증합니다. 이 역할은 모듈에 대한 보안 운영 액세스 권한도 갖습니다.
API 키를 가져옵니다.	PhishTank API 키에 대한 정보를 확인하고 계정을 만들려면 웹 사이트를 방문하십시오.
ServiceNow 통합을 위해 애플리케이션을 설치하기 전에 통합을 지원하는 데 필요한 핵심 애플리케이션이 설치되고 활성화되었는지 확인합니다.	Madrid 이상 릴리스 요구 사항 Madrid 릴리스 및 이후 제품군 릴리스의 경우 Dependency 플러그인(com.snc.si_dep)이

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업 설정	설명
	보안 인시던트 응답 필요합니다. 이 플러그인은 제품을 지원하는 데 필요한 모든 종속성을 보안 인시던트 응답 자동으로 설치합니다. 통합에 필요한 다른 보안 운영 애플리케이션을 설치하고 활성화하기 전에 이 플러그인을 설치하고 활성화합니다. 에서 ServiceNow Store다음 보안 운영 애플리케이션이 설치되고 활성화되는지 확인합니다. 설치되지 않은 경우 원활한 설치를 위해 다음 순서로 한 번에 하나의 애플리케이션을 설치하고 활성화합니다. **1.** 보안 인시던트 응답 **2.** 보안 통합 프레임워크 **3.** Security Support Common **4.** 보안 지원 오케스트레이션 통합을 위한 인스턴스 설정에 ServiceNow AI Platform 대한 자세한 내용은 해당 문서를 애플리케이션 활성화 ServiceNow Store참조하십시오제품 또는 애플리케이션에 대한 보안 운영 권리 가져오기.

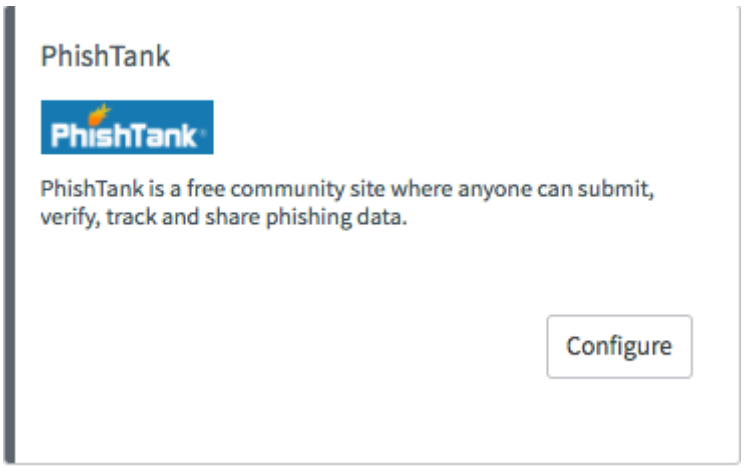
필요한 역할: 관리자

프로시저

1. 통합을 위해 애플리케이션을 설치하지 않은 경우 이를 확인하고 보안 운영 통합 설치 단계에 따라 설치합니다.

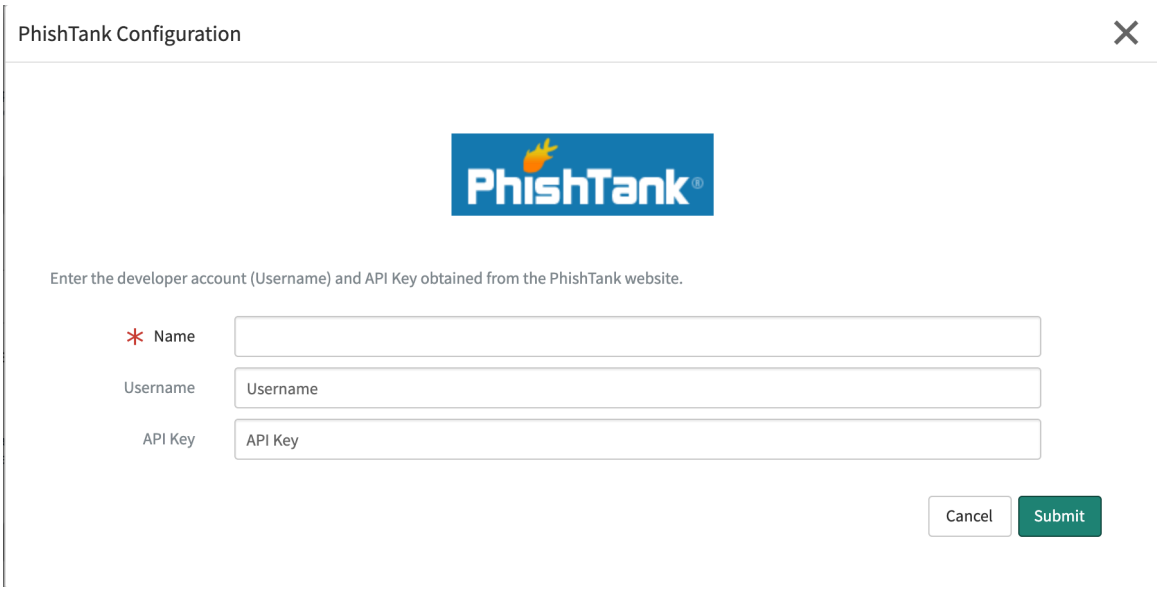
2. 설치가 완료되면 통합 〉 통합 구성 타일을 PhishTank 찾습니다.

3. 구성을 클릭합니다.



4. PhishTank 구성 대화 상자에서 구성 이름, 사용자 이름(PhishTank에서 만든 개발자 계정) 및 웹 사이트에서 가져온 PhishTank API 키를 입력하고 제출을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



5. 구성이 성공했는지 확인합니다.
   오류 메시지가 표시되지 않는 한 구성이 성공적으로 완료된 것입니다.

   Trouble?

   구성 PhishTank 중에 오류 메시지가 표시되면 API 키가 잘못되었을 수 있습니다.

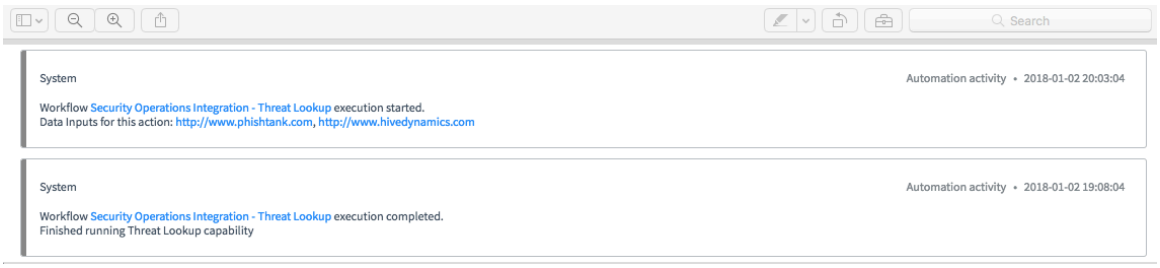
에 대한 예상 결과 확인 **PhishTank**

옵저버블은 보안 인시던트에 의해 자동으로 생성되고 애플리케이션에서 검사됩니다. 조회 결과는 보안 인시던트 기록 하단의 위협 조회 결과 탭에 표시됩니다.

시작하기 전에
필요한 역할: sn_si.analyst

프로시저

1. 작업 중인 보안 인시던트 양식을 열고 조회가 성공적으로 실행되었는지 확인합니다.

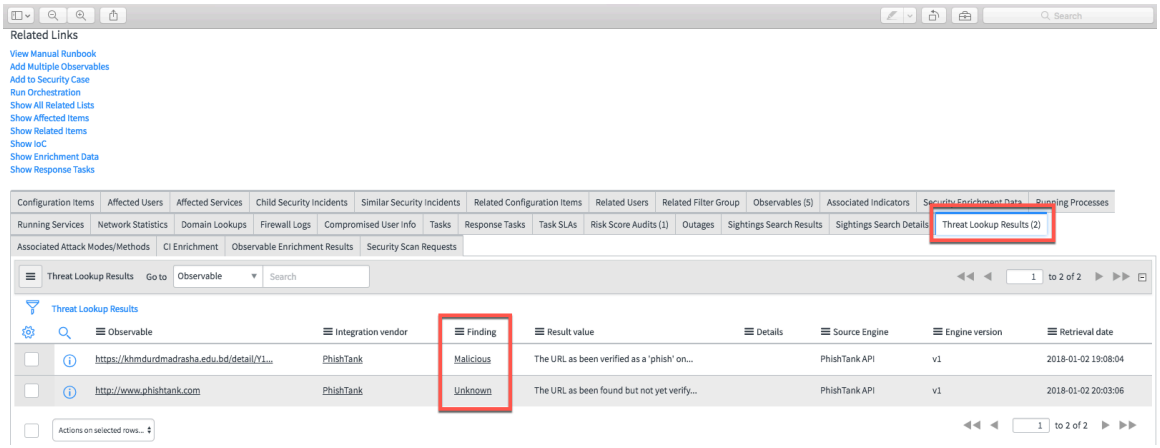


   애플리케이션이 구성되면 인시던트 생성 시 플로우가 자동으로 시작됩니다. 그러면 조회의 실행 및 완료 상태가 보안 인시던트 기록의 작업 메모에 표시됩니다.

2. 자세한 내용은 작업 메모를 검토하고, 조회가 성공적으로 실행되었는지 확인할 수 없는 경우 진행 방법을 확인하십시오.
3. 보안 인시던트의 하단으로 이동하여 모든 관련 목록 표시 관련 링크를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

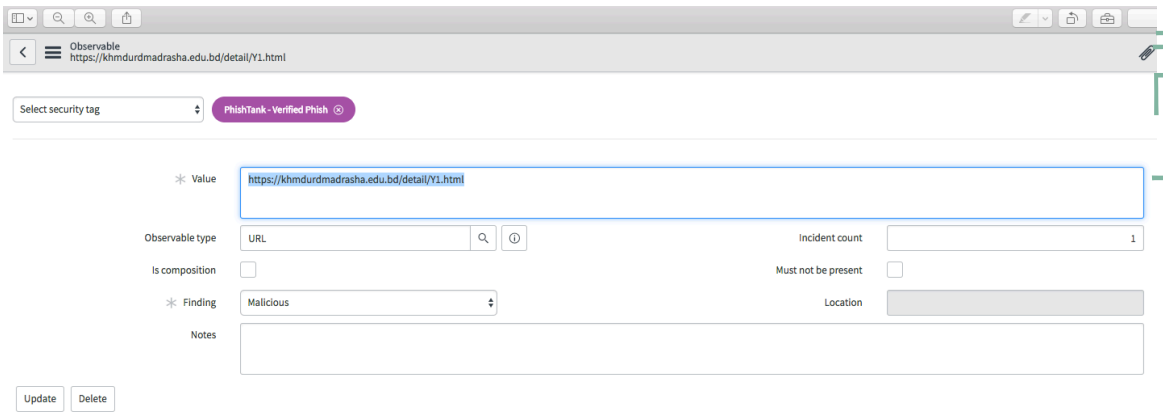
주:
다음 단계의 그림은 시스템 설정에서 탭 양식 설정이 활성화된 상태로 표시됩니다. 탭 폼이 표시되지 않으면 배너 프레임의 오른쪽 위 모서리에서 설정 기어 아이콘을 클릭합니다. 표시되는 시스템 설정 대화 상자에서 폼을 클릭하고 탭 폼 및 폼 사용이 선택되어 있는지 확인합니다.



보안 인시던트 기록 하단의 위협 조회 결과 탭에 조회 결과가 표시됩니다.

발견 사항 열은 악성으로 확인되지 않은 기록에 대해 # # ##으로 표시됩니다. 결과가 악성으로 일치하면 Find(결과) 열에 Malicious (##)이 표시됩니다.

4. 옵저버블 열에서 옵저버블을 클릭하여 기록을 열고 자세한 정보를 표시합니다.

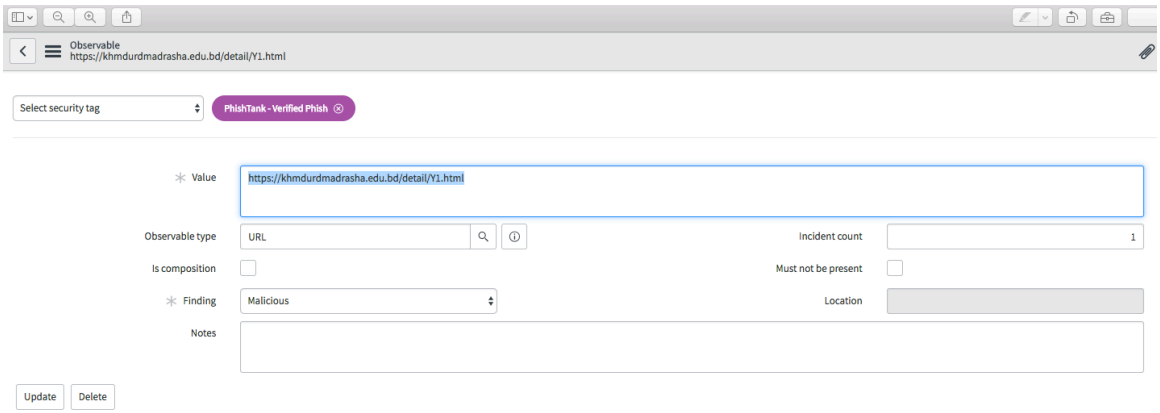


옵저버블 기록에서 악성과 일치하는 조회의 경우 **Finding**(찾기) 필드에 Malicious (악#)이 표시됩니다. 옵저버블에는 악성으로 확인된 소스(이 경우 애플리케이션)가 태그되어 위협 인텔리전스 있습니다 PhishTank .

5. 원시 데이터를 확인하려면 보안 인시던트로 다시 이동하여 옵저버블 옆에 있는 파란색 정보 아이콘을 클릭합니다.

6. 표시되는 창에서 기록 열기를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



API에서 생성한 링크 및 결과와 함께 표시되는 찾기 필드입니다.

Trouble?
위협 조회 결과 탭에 결과가 표시되지 않으면 옵저버블이 통합에서 조회를 위해 지원하는 유형인지 확인합니다.

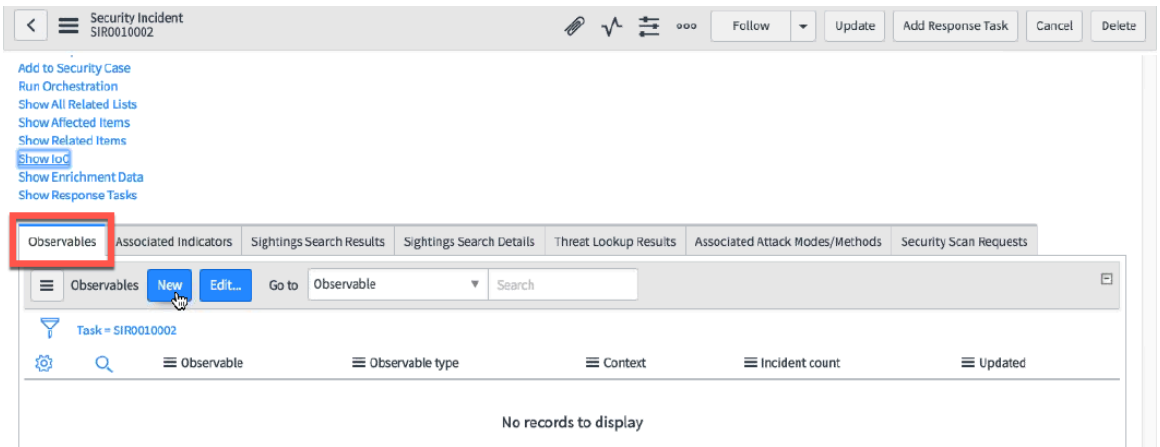
(선택 사항) 다음에 대한 옵저버블을 수동으로 첨부 **PhishTank**

옵저버블을 보안 인시던트에 수동으로 연결할 수 있습니다. 초기 이벤트 트리거에서 보안 인시던트에 첨부되지 않은 옵저버블에 대해 위협 조회를 수행하려는 경우 옵저버블을 수동으로 연결합니다. 또한 관련 옵저버블에 대한 자세한 정보가 필요한 경우에도 이 작업을 수행할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.analyst

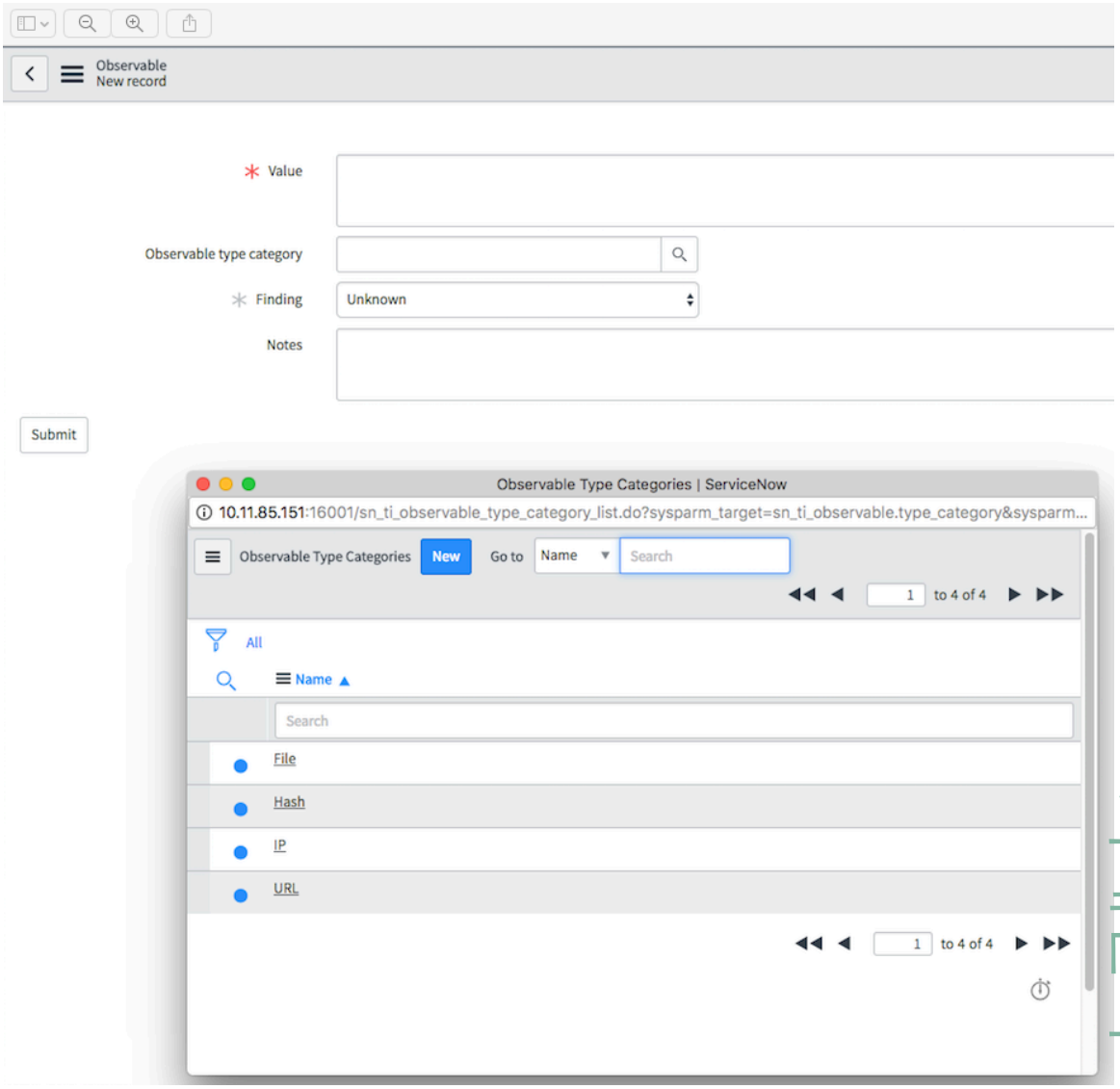
프로시저

1. 열려 있는 보안 인시던트로 이동합니다.
2. 오픈 보안 인시던트 기록에서 관련 링크의 **IoC** 표시링크를 클릭하여 옵저버블 탭을 표시합니다.



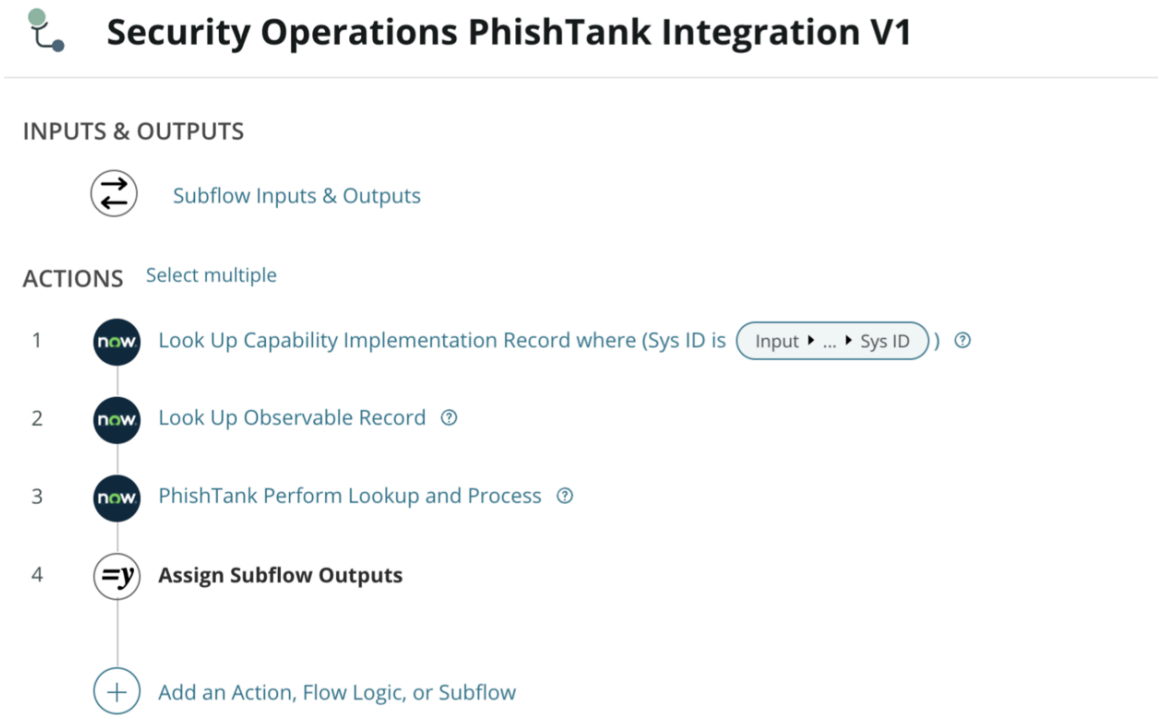
3. 새로 만들기를 클릭합니다.
   옵저버블 양식이 표시됩니다.
4. 값 필드에 URL을 입력합니다.
5. 검색 아이콘을 클릭하고 옵저버블 유형 범주 대화 상자에서 목록의 **URL** 을 클릭하여 필드를 채웁니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

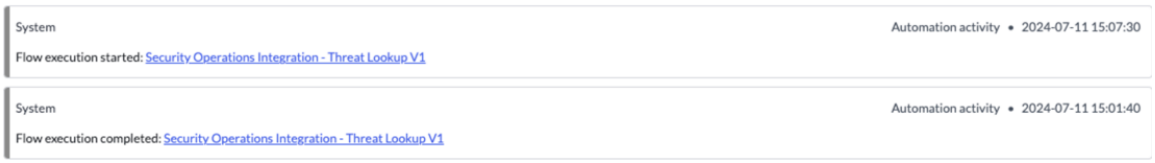


6. 제출을 클릭합니다.
플로우가 시작되고 새 옵저버블이 있는지 확인합니다. 실행 및 완료 상태는 보안 인시던트 기록의 작업 메모 섹션에 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

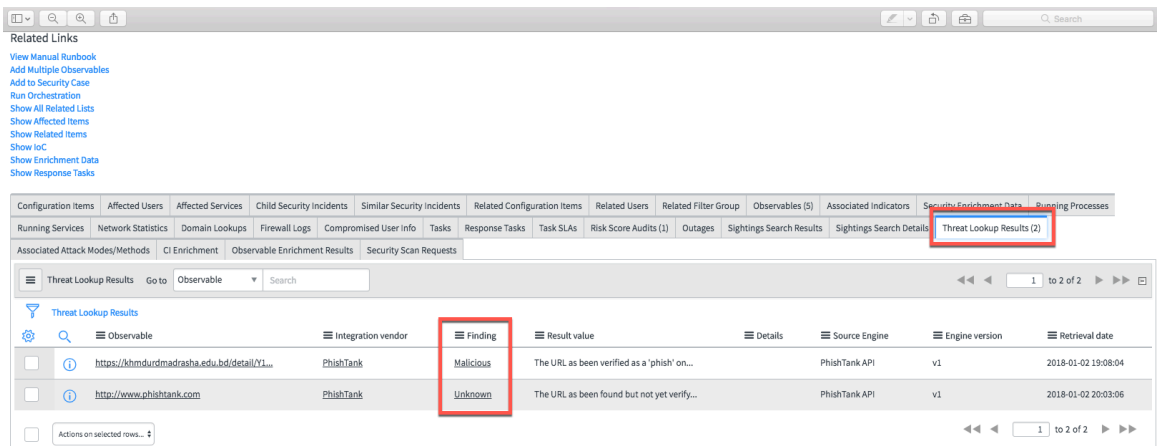


7. 보안 인시던트로 이동하여 작업 메모를 검토합니다.



8. 보안 인시던트 하단의 모든 관련 목록 표시 관련 링크를 클릭합니다.

9. 위협 조회 결과 탭을 클릭하여 결과를 확인합니다.



10. 옵저버블 열에서 지정된 옵저버블 옆에 있는 파란색 정보 아이콘을 클릭하면 자세한 정보와 원시 데이터를 볼 수 있습니다.

11. 표시되는 대화 상자에서 기록 열기를 클릭합니다.

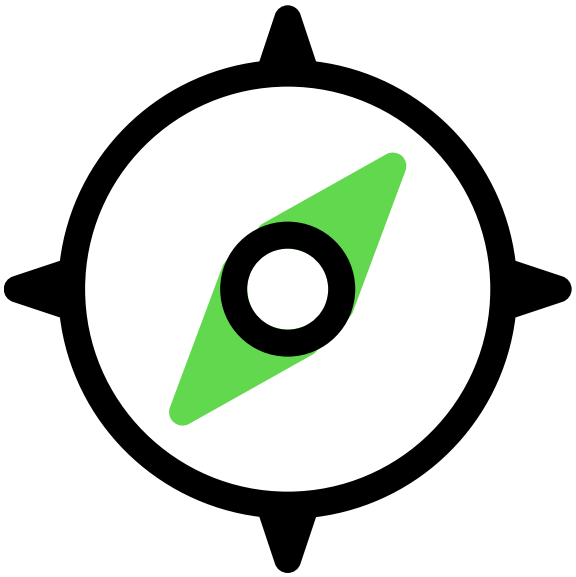
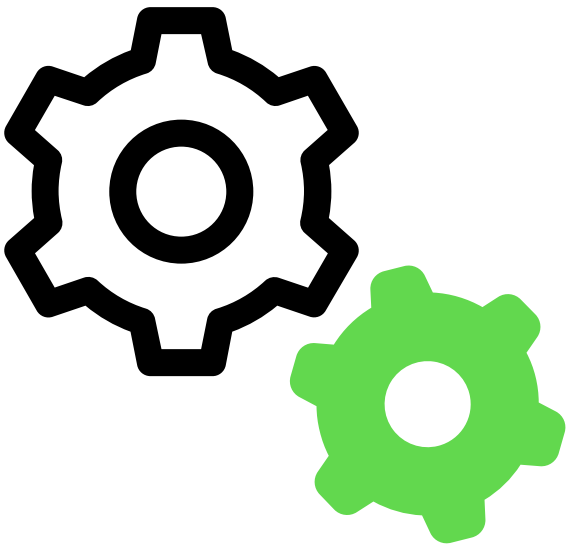
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Trouble?
자세한 내용은 작업 메모를 검토하고, 조회가 성공적으로 실행되었는지 확인할 수 없는 경우 진행 방법을 확인하십시오.

Proofpoint 보안 운영을 위한 통합

SIR 통합은 Proofpoint 에서 Proofpoint이벤트 수집을 지원합니다. SIR은 분석가가 검토하거나 작업할 수 있는 수집된 각 이벤트에 대해 인시던트를 생성합니다.

시작하기

탐색	구성
	
통합에 대해 Proofpoint 알아보기	SIR 작업 공간에 맞게 구성 Proofpoint

Proofpoint Security Operations를 위한 통합 탐색

에서 이벤트를 Proofpoint수집하도록 SIR의 이벤트 프로파일을 구성할 수 있습니다. SIR은 분석가가 검토하거나 작업할 수 있는 수집된 각 이벤트에 대해 인시던트를 생성합니다.

Proofpoint 보안 운영 사용자를 위한 통합

사용자

사용자	설명
보안 관리자	수집된 이벤트를 필터링하기 위한 이벤트 프로파일을 생성합니다. SIR은 이러한 수집된 이벤트에 대한 인시던트를 생성합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Proofpoint Integration for Security Operations 의 이점

Proofpoint Integration for Security Operations 의 이점

혜택	기능	사용자
이벤트 데이터를 인스턴스로 끌어오고 보안 인시던트를 생성합니다. 단일 위치에서 의심스럽거나 악성으로 간주되는 이벤트에 대한 보안 인시던트를 검토합니다.	전달된 이메일 메시지와 허용된 클릭이 나중에 악성으로 간주되는 경우 직원이 이러한 메시지를 열어 상호작용했을 가능성이 있습니다. 검토할 메시지를 추적하려면 통합의 메시지 트래픽에 대해 생성 및 구성한 이벤트 프로파일을 기반으로 보안 인시던트를 자동으로 생성합니다. 또한 감사 목적으로 차단된 메시지 및 클릭에 대한 보안 인시던트 생성을 활성화할 수도 있습니다.	관리자

다음으로 살펴볼 내용

Proofpoint 구성 및 사용에 대한 자세한 내용은 다음을 참조하십시오.

- Proofpoint Security Operations를 위한 통합 구성
- Proofpoint 통합 설정 검토
- Proofpoint 분석 대시보드 보기

Proofpoint Security Operations를 위한 통합 구성

Proofpoint 보안 운영용 통합의 구현을 구성합니다.

구성 개요

1. Proofpoint 통합 설치 및 구성.

   통합 애플리케이션을 다운로드, 설치 및 활성화합니다.

2. Proofpoint 보안 운영 통합에 대한 이벤트 프로파일 생성.

   제품에서 Proofpoint 임포트할 이벤트와 임포트한 데이터에서 보안 인시던트를 생성하는 데 사용할 조건을 식별하는 이벤트 프로파일을 생성합니다.

3. Proofpoint Security Operations를 위한 통합 구성

   이벤트 프로파일 생성을 위한 통합 설정을 검토합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Proofpoint 통합 설치 및 구성

인스턴스에서 Proofpoint Integration for Security Operations 애플리케이션을 ServiceNow# StoreServiceNow AI Platform 설치하고 구성합니다.

시작하기 전에
필요한 역할: sn_si_admin

프로시저

1. Proofpoint 에서 ServiceNow# Store 애플리케이션에 대한 보안 운영 통합을 다운로드하여 설치합니다.
   자세한 내용은 ServiceNow Store 애플리케이션 설치를 참조하십시오.
2. 다음으로 이동 보안 운영 〉 통합 〉 통합 구성.
3. 타일에 Proofpoint 대한 보안 운영 통합을 찾아 구성을 선택합니다.
4. 양식에서 필드를 채웁니다.

Proofpoint 통합 구성 양식

필드	설명
이름	보안 운영 구성을 위한 통합의 Proofpoint 이름입니다.
서비스 원칙	테넌트의 Proofpoint 사용자 이름입니다.
비밀	테넌트의 Proofpoint ID입니다.

5. 제출을 선택합니다.

결과
구성을 성공적으로 확인하고 제출하면 통합이 보안 통합 페이지에 타일로 저장됩니다.

Proofpoint 보안 운영 통합에 대한 이벤트 프로파일 생성

제품에서 Proofpoint 임포트할 이벤트를 식별하는 이벤트 프로파일을 생성합니다.

이 태스크 정보
이벤트 유형, 매핑 및 임포트 일정을 구성하여 이벤트 프로파일을 생성합니다. 페이지의 진행률 표시줄에 모든 단계가 표시되고 현재 활성 구성에 대해 강조 표시됩니다.

시작하기 전에
필요한 역할: sn_si_admin

프로시저

1. 다음으로 이동 모두 〉 Proofpoint와의 **SIR** 통합 〉 **Proofpoint** 이벤트 프로파일.
2. 이벤트 프로필 페이지에서 새로 만들기를 선택합니다.
3. 양식에서 필드를 채웁니다.

   이름부터 진행률 표시줄이 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Proofpoint 프로파일 양식

필드	설명
이름	이벤트 프로파일의 이름입니다. 연결된 이벤트 유형을 포함하는 이름을 사용하는 것이 좋습니다. ○ 클릭수 차단됨 ○ 클릭수 허용됨 ○ 메시지 차단됨 ○ 메시지 배달됨
소스	통합 구성 페이지에서 통합에 대해 구성된 소스입니다.
순서	이 프로파일이 실행되는 순서입니다. 기본값은 100입니다.
활성	프로파일을 활성화하기 위한 옵션입니다.
설명	이 이벤트 프로파일에 대한 선택적 설명입니다.

4. 계속을 선택합니다.
5. 하나 이상의 이벤트 유형을 사용 가능 열에서 선택됨 열로 이동하여 선택합니다.
   사용 가능한 이벤트 유형은 다음과 같습니다.
   - 클릭수 차단됨
   - 클릭수 허용됨
   - 메시지 차단됨
   - 메시지 배달됨
6. 계속을 선택합니다.

   선택한 이벤트 유형과 관련된 구성 단계가 진행률 표시줄에 표시됩니다.

   소스 필드의 값은 사용자 환경의 TAP(대상 공격 보호) 데이터에서 참조로 제공됩니다.

   소스 필드 데이터와 대상 필드의 기본 매핑이 페이지에 표시됩니다. 기본 데이터가 가이드로 포함되어 있지만 이 매핑을 수정할 수 있습니다.
7. 옵션: **f(x)** 아이콘을 선택하면 애플리케이션에 포함된 기본 번역을 볼 수 있습니다.

   (Optional) 필드의 여러 값은 쉼표로 구분됩니다.
8. 계속을 선택합니다.
9. 필터링 및 집계 페이지에서 다음 표의 속성을 구성합니다.

필터링 및 집계 속성

옵션	설명
메시지 이벤트에 대한 조건을 기준으로 필터링	메시지 이벤트를 기반으로 필터링을 활성화하는 옵션입니다.
메시지 이벤트 필터 조건	메시지 이벤트 필터 조건입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵션	설명
클릭 이벤트에 대한 조건을 기준으로 필터링	클릭 이벤트를 기반으로 필터링을 활성화하는 옵션입니다.
클릭 이벤트 필터 조건	이벤트 필터 조건을 클릭합니다.
집계 조건	새 인시던트를 생성하는 대신 수신 인시던트를 미해결 보안 인시던트에 추가할 수 있도록 허용하는 옵션입니다.
일치하는 값이 있는 인시던트 필드	집계에 보안 인시던트 응답 포함할 인시던트에 대해 값이 일치해야 하는 필드를 추가합니다.
새 인시던트에 대한 작업 메모 기록	작업 메모를 상위에 보안 인시던트 응답기록할 수 있도록 하는 옵션입니다.
ThreatID 관계 사용	ThreatID가 일치하는 모든 인시던트의 집계를 활성화하는 옵션입니다.

10. 계속을 선택합니다.
11. 임포트 유형 중 하나와 이벤트 데이터를 임포트할 빈도를 선택합니다.
12. 마침을 선택합니다.

결과
새로 만든 이벤트 프로파일은 이벤트 프로파일 페이지의 기존 이벤트 프로파일 목록에 포함됩니다.

Proofpoint 통합 설정 검토

사용자 환경에 맞게 시스템 속성을 수정할 수 있도록 Proofpoint 통합 설정을 검토합니다.

시작하기 전에
필요한 역할: sn_si_admin

프로시저

1. 다음으로 이동 모두 〉 Proofpoint와의 **SIR** 통합 〉 **Proofpoint** 통합 설정.
2. 다음 설정을 수정합니다.

Proofpoint 통합 설정

속성 이름	설명
restAPI 호출에 대한 시간 제한입니다. sn_sec_proofpoint.http_timeout	API 호출에서 데이터를 가져오는 시간 제한(초)입니다. 유형: 정수 기본값: 3000
로깅 수준 - 디버그, 정보, 경고, 오류 sn_sec_proofpoint.logging_verbosity	애플리케이션의 로그 세부 정보 표시 수준으로, 정보 유형의 이름을 의미합니다. 값을 다음 옵션으로 업데이트할 수 있습니다. ○ 오류 ○ 경고

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성 이름	설명
	○ 정보 ○ 디버그 기본값: 정보
단일 인시던트로 집계할 수 있는 Proofpoint 이벤트의 수를 제한하십시오. sn_sec_proofpoint.max_aggregations_per_si	하나의 인시던트로 집계할 수 있는 최대 Proofpoint 이벤트 수입니다. 유형: 정수 기본값: 100
24시간 동안 만들 수 있는 보안 인시던트 수를 제한하십시오. sn_sec_proofpoint.max_si_per_day	24시간 내에 만들 수 있는 최대 인시던트 수입니다. 유형: 정수 기본값: 1000
요일은 상위 클리커, VAP에 대한 API 호출에 사용해야 합니다. sn_sec_proofpoint.default_days	상위 클리커 및 VAP에 대해 가져올 데이터의 일 수입니다. 값을 다음 옵션으로 업데이트할 수도 있습니다. ○ 14 ○ 30 ○ 90 유형: 정수 기본값: 90
부울 플래그, 활성화된 경우 API를 호출하고 상위 클리커 상세 정보를 채웁니다. sn_sec_proofpoint.call_topclickers_api	상위 클리커 데이터를 활성화하고 가져오는 옵션을 활성화합니다. 유형: 부울 기본값: True
부울 플래그, 활성화된 경우 API를 호출하고 VAP 세부 정보를 채웁니다. sn_sec_proofpoint.call_vap_api	VAP 데이터를 활성화하고 가져오는 옵션을 활성화합니다. 유형: 부울 기본값: False
topClickers, VAP 사용자에 대해 표시할 최대 사용자 수를 제한하기 위한 것입니다. sn_sec_proofpoint.maxresults	상위 클리커 및 VAP 사용자에 대해 표시할 최대 사용자 수입니다. 유형: 정수 기본값: 100
Proofpoint 이벤트의 예약된 폴링 중 중복 기간 사용을 활성화/비활성화합니다. sn_sec_proofpoint.allow_overlap	예약된 폴링이 구성된 경우 중복 기간을 사용하거나 사용하지 않도록 설정합니다. 유형: 부울

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성 이름	설명
	기본값: False
중복이 활성화된 경우 ProofpointEvent의 예약된 폴링 중에 사용할 중복 시간(분)입니다. sn_sec_proofpoint.overlap_time	예약된 폴링이 구성될 때의 중복 시간(분)입니다. 유형: 정수 기본값: 5

3. 저장을 선택합니다.

결과
새 값으로 통합 설정을 구성합니다.

Proofpoint 분석 대시보드 보기

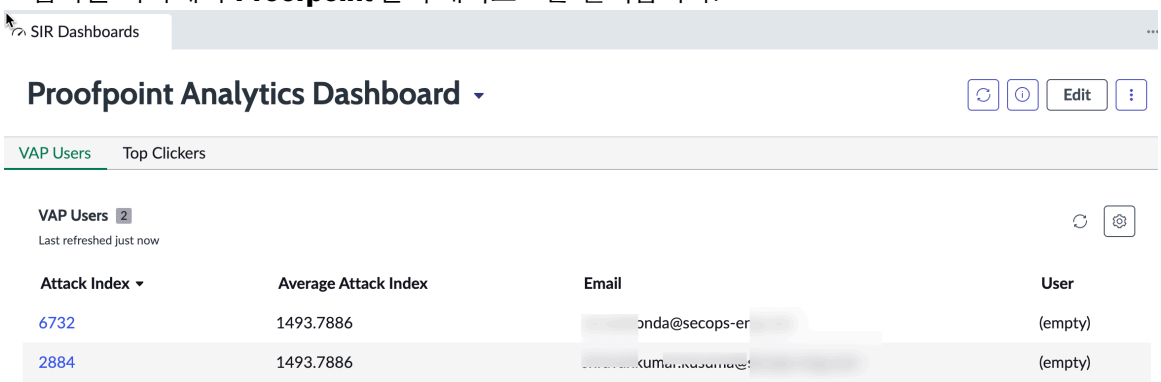
분석 대시보드는 Proofpoint VAP 사용자 및 상위 클리커에 대한 세부 정보를 제공합니다.

이 태스크 정보
주로 보안 공격의 대상이 되는 사용자는 VAP 사용자로 간주됩니다. 의심스러운 피싱 링크를 자주 클릭하는 직원은 상위 클리커로 간주됩니다.

시작하기 전에
필요한 역할: sn_si_admin

프로시저

1. 다음으로 이동 모두 〉 작업 공간 〉 보안 인시던트 응답 작업 공간.
2. **SIR** 대시보드를 선택합니다.
3. 드롭다운 목록에서 **Proofpoint** 분석 대시보드를 선택합니다.



4. VAP 사용자에 대한 정보를 봅니다.
   a. **VAP** 사용자 탭을 선택하여 **VAP** 사용자 목록을 봅니다.
   b. 사용자 이름을 선택하여 VAP 사용자의 상세 정보를 봅니다.
5. 상위 클리커에 대한 정보를 봅니다.
   a. 상위 클리커 탭을 선택하여 상위 클리커 목록을 봅니다.
   b. 사용자 이름을 선택하여 상위 클리커의 상세 정보를 봅니다.

Reverse Whois 통합

Reverse Whois 는 개인 또는 조직이 등록한 도메인 이름을 검색하는 서비스입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 인시던트에 첨부하는 옵저버블에서 검색어를 사용하여 도메인 조회를 수행합니다. API는 Reverse Whois 입력한 검색어를 기반으로 도메인 레코드를 검색하고 해당 검색어에 해당하는 모든 레코드를 반환합니다.

분석가는 보안 인시던트 조사를 위해 통합과 함께 Whois 이 통합을 사용하는 경우가 있습니다. 통합은 Whois 통합의 Reverse Whois 도메인 조회를 기반으로 추가 보강 정보를 제공합니다.

Reverse Whois 설치 및 구성

인스턴스에서 통합을 실행하기 전에 설치 및 구성 단계를 완료하여 애플리케이션이 제품과 제대로 통합 보안 운영 되도록 Reverse Whois 합니다.

시작하기 전에

설치하기 전에 다음 설정 검사 목록을 완료합니다. 이러한 설정 작업은 원활한 설치 및 구성을 위해 필요합니다.

설정 작업	설명
필요한 ServiceNow 역할을 할당했는지 확인합니다.	예상 결과의 설치, 구성 및 검증에 필요한 역할은 다음과 같습니다. • 시스템 관리자(admin)가 앱을 설치하고 보안 인시던트 관리자(sn_si.admin) 역할을 할당합니다. • 보안 인시던트 관리자(sn_si.admin)가 구성을 감독합니다. 보안 인시던트 관리자는 보안 인시던트 분석가(sn_si.analyst) 역할도 할당합니다. • 보안 인시던트 분석가(sn_si.analyst)는 보안 인시던트를 사용하여 Reverse Whois 도메인 조회를 수행하고 보안 인시던트를 분석하고 작업합니다.
API 키를 가져옵니다.	API 키에 대한 자세한 내용을 확인하고 계정을 만들려면 WhoisXML API 웹 사이트인 WhoisXML API 웹 사이트를 방문하십시오. 구성하려면 API 키를 입력해야 합니다.
ServiceNow 통합을 위해 애플리케이션을 설치하기 전에 통합을 지원하는 데 필요한 핵심 애플리케이션이 설치되고 활성화되었는지 확인합니다.	Madrid 이상 릴리스 요구 사항 Madrid 릴리스 및 이후 제품군 릴리스의 경우 Dependency 플러그인(com.snc.si_dep)이 보안 인시던트 응답 필요합니다. 이 플러그인은 제품을 지원하는 데 필요한 모든 종속성을 보안 인시던트 응답 자동으로 설치합니다. 통합에 필요한 다른 보안 운영 애플리케이션을 설치하고 활성화하기 전에 이 플러그인을 설치하고 활성화합니다. 에서 ServiceNow Store다음 보안 운영 애플리케이션이 설치되고 활성화되는지 확인합니다. 설치되지 않은 경우 원활한 설치를 위해 다음 순서로 한 번에 하나의 애플리케이션을 설치하고 활성화합니다.

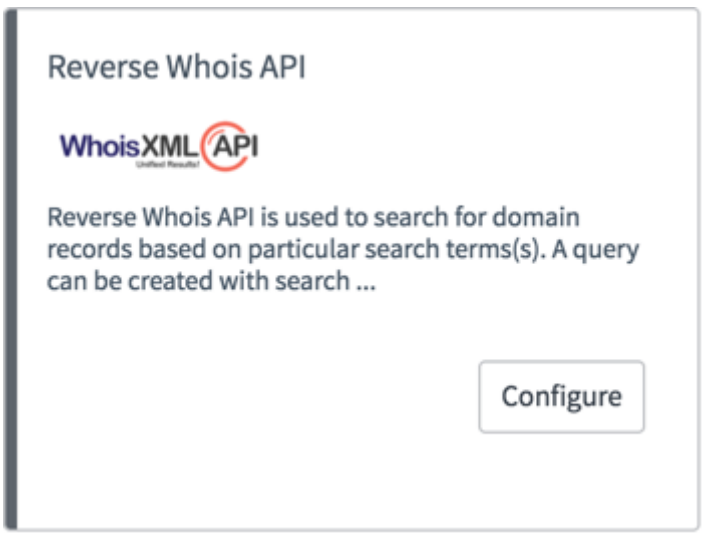
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설정 작업	설명
	1. 보안 인시던트 응답 **2.** 보안 통합 프레임워크 **3.** Security Support Common **4.** 보안 지원 오케스트레이션 통합을 위한 인스턴스 설정에 ServiceNow AI Platform 대한 자세한 내용은 해당 문서를 애플리케이션 활성화 ServiceNow Store참조하십시오제품 또는 애플리케이션에 대한 보안 운영 권리 가져오기.

필요한 역할: 관리자

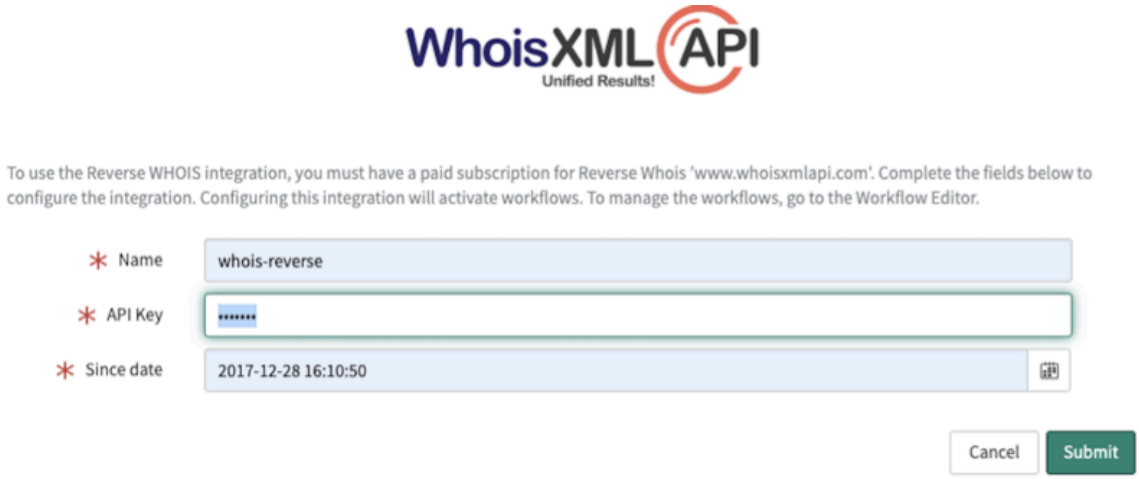
프로시저

1. 애플리케이션을 이미 설치하고 구성한 Reverse Whois 경우 다음 단계를 수행합니다.
   a. 기존 구성을 삭제합니다.
   b. 가져온 API 키를 사용하여 새 구성을 설치하고 생성합니다.
2. 통합을 위해 애플리케이션을 설치하지 않은 경우 이를 확인하고 보안 운영 통합 설치 단계에 따라 설치합니다.
3. 설치가 완료되면 통합 〉 통합 구성 를 클릭하고 API 타일을 Reverse Whois 찾습니다.
4. 구성을 클릭합니다.



5. **Reverse Whois API** 구성 대화 상자에 XML API 웹 사이트에서 가져온 Whois API 키를 입력합니다.
6. 다음 표에서 하나의 옵션을 선택하여 검색어에 대한 도메인 조회를 필터링합니다. 이러한 구성 설정은 변경하고 모든 Reverse Whois API 검색에 적용할 때까지 저장된 상태로 유지됩니다.

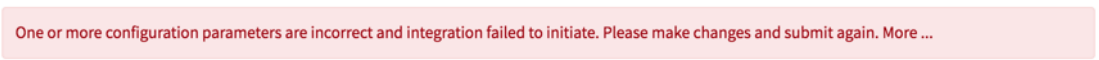
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



7. 제출을 클릭합니다.
   오류 메시지가 표시되지 않는 한 구성이 성공적으로 완료된 것입니다.

Trouble?
오류 메시지가 표시되는 경우 API 키가 잘못되었을 수 있습니다.

오류 메시지



(선택 사항) 설치 및 구성 **Whois**

Whois 플러그인을 설치하여 API에서 Reverse Whois 도메인 조회에 대한 추가 보강 정보를 제공합니다. 이 조회는 등록 날짜, 등록 대행자 이름 및 출신 국가와 같은 도메인에 대한 추가 보강 데이터를 제공합니다.

시작하기 전에

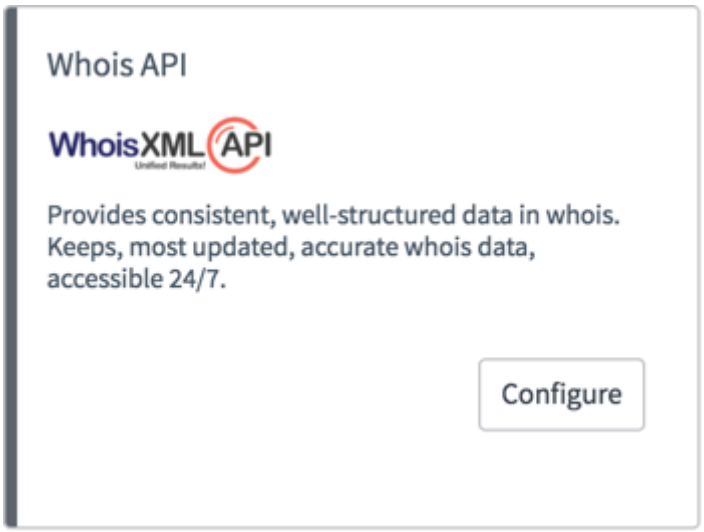
1. 애플리케이션에 대한 권리를 요청하지 않은 경우 ServiceNow Store에서 애플리케이션을 참조하십시오 제품 또는 애플리케이션에 대한 보안 운영 권리 가져오기Whois .
2. 제품 웹 사이트인 WHOIS API 웹 사이트에서 API 키에 대한 Whois 자격 증명을 가져옵니다.

필요한 역할: 관리자

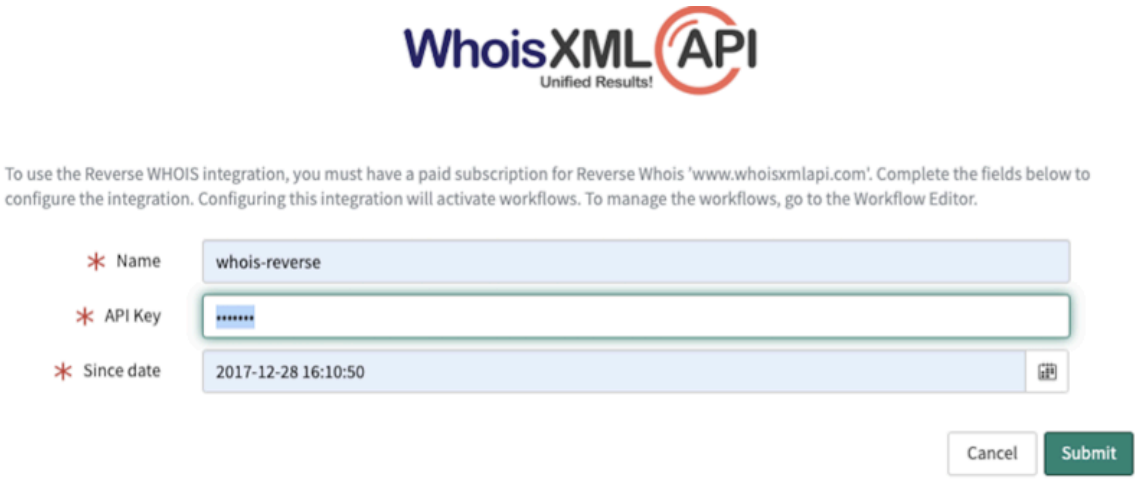
프로시저

1. 애플리케이션을 설치하지 않은 경우 단계를 참조 보안 운영 통합 설치 하고 단계에 따라 설치합니다.
2. 설치가 완료되면 통합 〉 통합 구성 를 클릭하고 API 타일을 Whois 찾습니다.
3. 구성을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



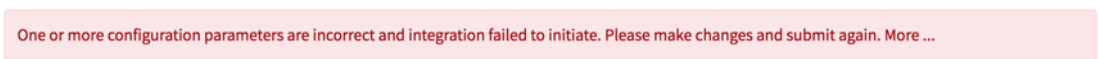
4. **Whois API** 구성 대화 상자에서 제품 웹 사이트에서 가져온 API 키를 입력합니다.



5. 제출을 클릭합니다.
   오류 메시지가 표시되지 않는 한 구성이 성공적으로 완료된 것입니다. 이제 통합에서 반환된 도메인에서 보강 조회를 실행할 수 있습니다 Reverse Whois .

Trouble?
오류 메시지가 표시되는 경우 API 키가 잘못되었을 수 있습니다.

문제 해결



에 대한 조회 시작 **Reverse Whois**

보안 인시던트 기록에 수동으로 첨부하는 옵저버블의 검색어를 사용하여 도메인 조회를 시작합니다.

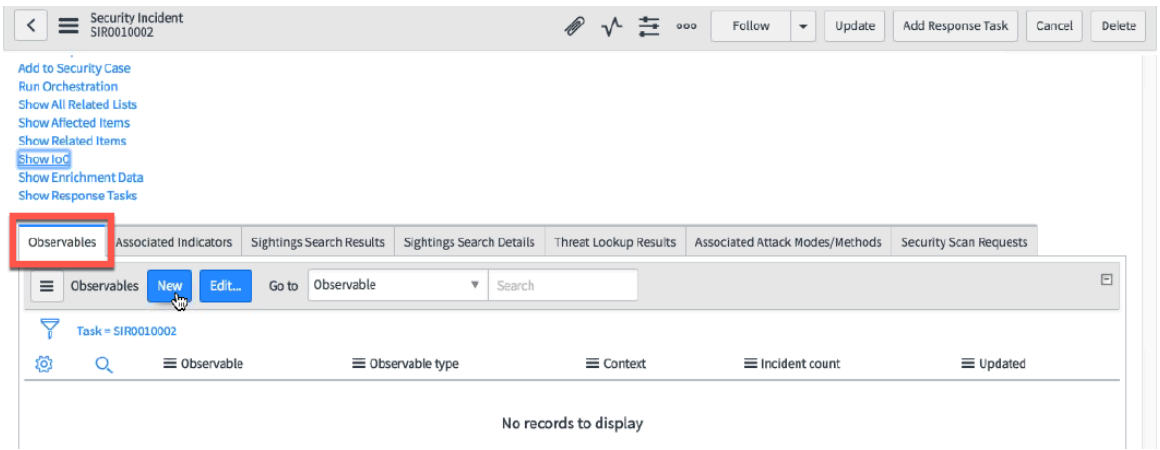
시작하기 전에
필요한 역할: sn_si.analyst

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 열려 있지 않으면 다음으로 이동하십시오. 보안 인시던트 〉 인시던트 〉 모든 인시던트 표시 을 클릭하고 작업 중인 보안 인시던트를 엽니다.
2. 기록 하단에서 **IoC** 관련 링크 표시를 클릭하여 옵저버블 탭을 표시합니다.

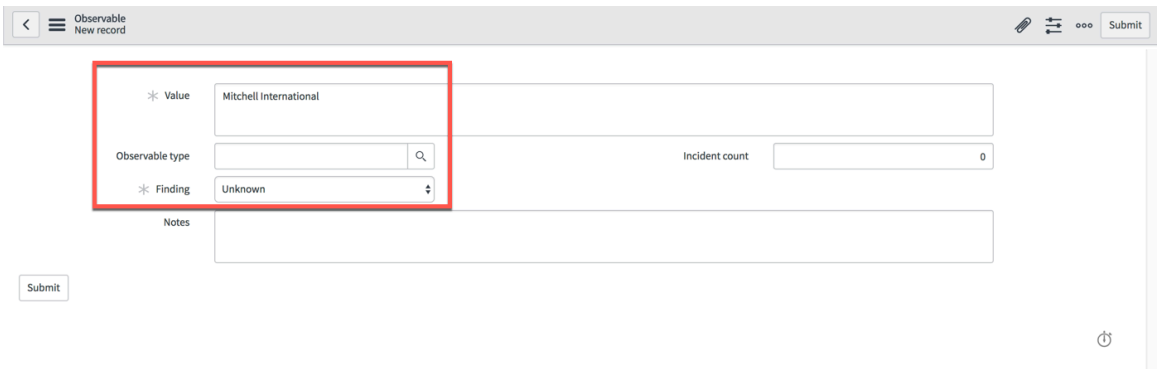
   주:
   다음 단계의 그림은 시스템 설정에서 탭 양식 설정이 활성화된 상태로 표시됩니다. 보안 인시던트에 대한 탭이 표시되지 않으면 배너 프레임 오른쪽 위 모서리에서 설정 기어 아이콘을 클릭합니다. 표시되는 시스템 설정 대화 상자에서 폼을 클릭하고 탭 폼 및 폼 사용이 선택되어 있는지 확인합니다.



3. 옵저버블 탭에서 새로 만들기를 클릭합니다.
4. 필드에 내용을 입력합니다.

   새 기록의 필수 필드

필드	설명
값	도메인에 대한 고유한 검색어입니다.
옵저버블 유형	이 필드는 자동으로 지워집니다.
찾기	이 필드는 알 수 없음으로 자동 설정됩니다.



5. 제출을 클릭합니다.
   보안 인시던트 기록으로 돌아가고 플로우가 조회를 시작합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 수행할 작업
보안 인시던트에 대한 조회 결과를 확인합니다. 에 대한 예상 결과 확인 Reverse Whois 문서를 참조하십시오.

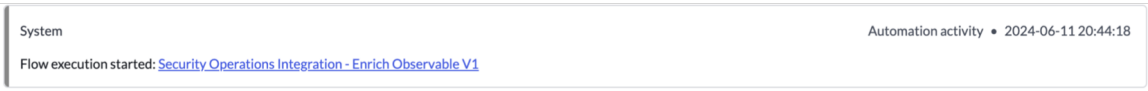
에 대한 예상 결과 확인 **Reverse Whois**

보강 결과는 보안 인시던트 기록 하단의 **ReverseWhois** 도메인 탭에 표시됩니다. 조회 결과를 찾아 조회가 성공적으로 실행되었는지 확인합니다.

시작하기 전에
필요한 역할: sn_si.analyst

프로시저

1. 아직 열리지 않은 경우 다음으로 이동하십시오. 보안 인시던트 〉 인시던트 〉 모든 인시던트 표시 로 이동하여 작업 중인 보안 인시던트를 찾습니다.

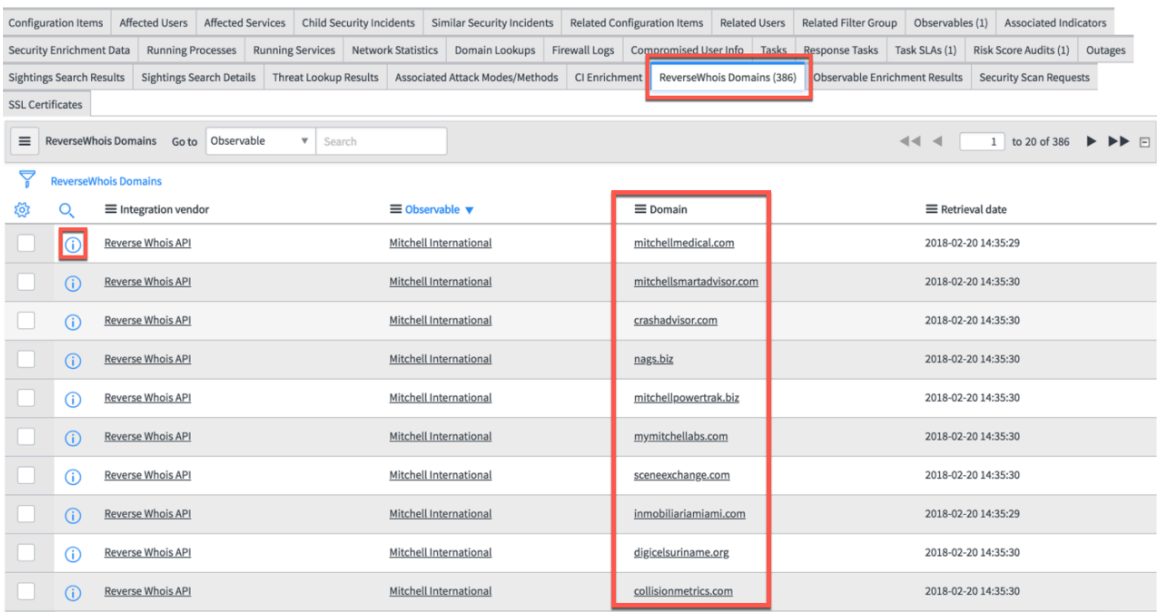


애플리케이션이 구성되고 옵저버블을 연결하면 플로우가 자동으로 시작됩니다. 보안 인시던트 기록의 작업 메모에는 조회의 실행 및 완료 상태가 표시됩니다.

2. 조회가 성공적으로 실행되었는지 확인할 수 없는 경우 작업 메모에서 진행 방법에 대한 자세한 내용을 검토하십시오.

3. 보안 인시던트의 하단으로 이동하여 모든 관련 목록 표시 관련 링크를 클릭합니다.

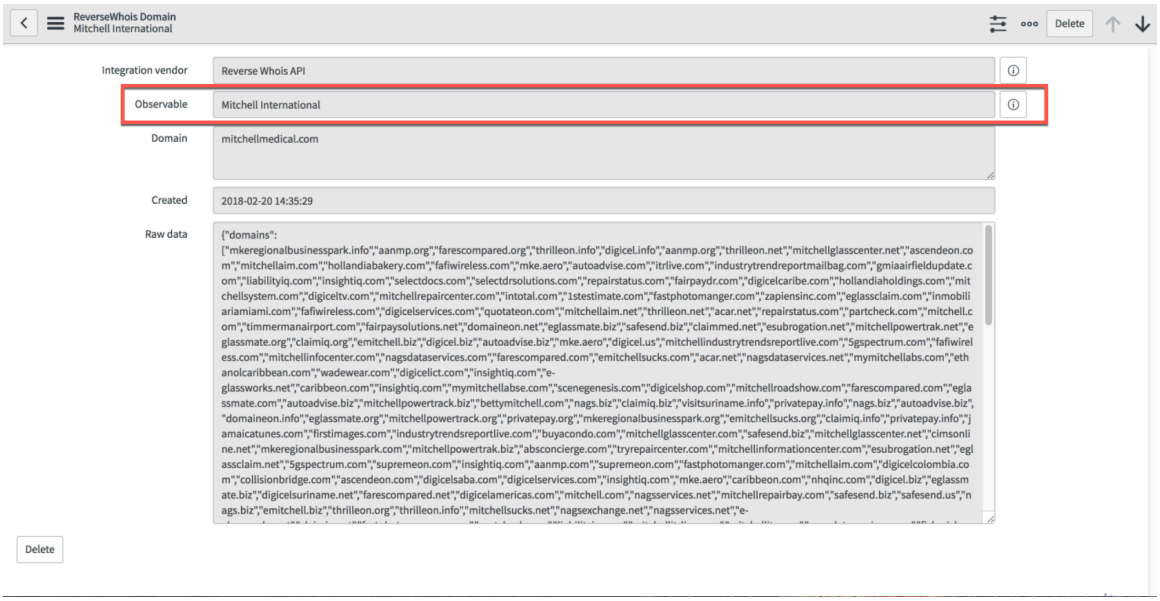
주:
다음 그림에 표시된 필터링된 조회 결과의 경우 API 구성 타일의 Reverse Whois 구성 설정은 날짜 이후 필드에 **1991-06-01**이 입력된 상태로 저장되었습니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

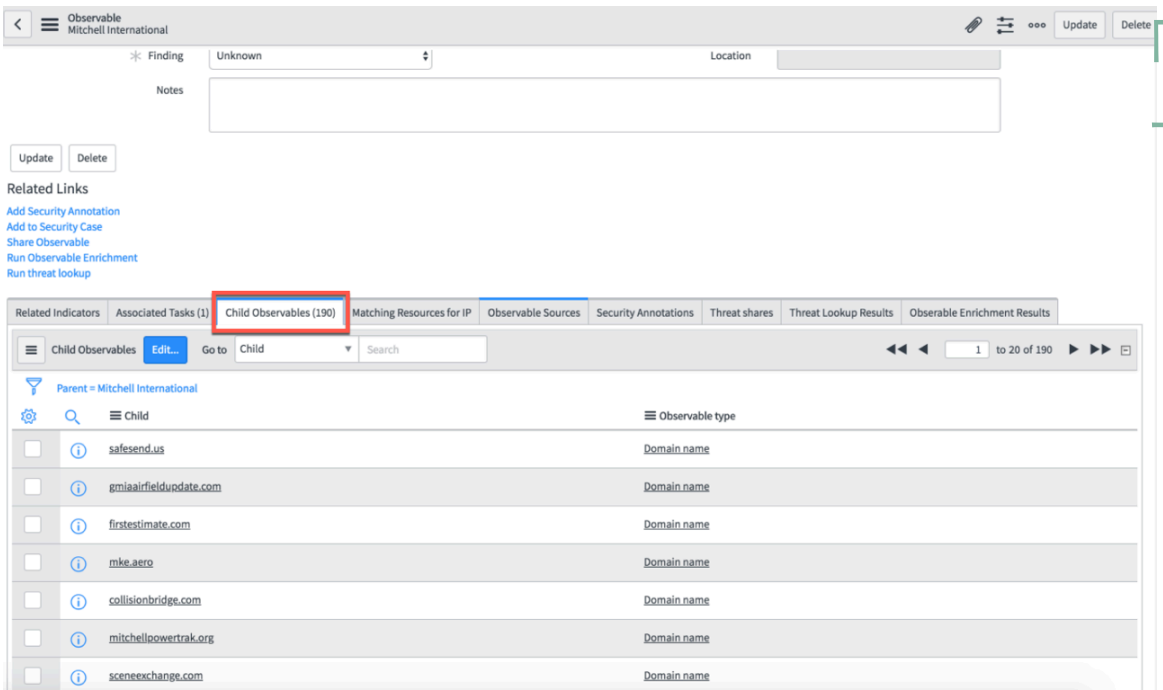
보강 결과가 **ReverseWhois** 도메인 탭에 표시됩니다. 이 옵저버블에 대한 활성 도메인이 도메인 열에 표시됩니다.

4. 항목 옆에 있는 파란색 정보 아이콘을 클릭한 다음 표시되는 대화 상자에서 기록 열기 를 클릭합니다.



기록은 원시 데이터를 포함한 향상된 상세 정보와 함께 표시됩니다.

5. 보안 인시던트로 다시 이동하고 **ReverseWhois** 도메인 탭을 선택한 상태에서 옵저버블 열에서 옵저버블을 클릭하여 기록을 엽니다.



하위 옵저버블은 옵저버블 기록의 하위 옵저버블 탭에 표시됩니다. 하위 옵저버블은 애플리케이션에 반환된 도메인이 있는 경우에만 Reverse Whois 생성됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Trouble?
조회가 성공적으로 완료되지 않으면 입력한 검색어가 통합에서 지원되는지 확인합니다. 자세한 내용은 작업 메모를 검토하십시오.

다음에 수행할 작업
도메인 조회 결과에 대한 더 많은 보강 데이터를 보려면 통합을 실행하여 Whois 통합에서 반환된 하위 옵저버블에 대해 보강 조회를 Reverse Whois 수행할 수 있습니다. 하위 옵저버블에 대한 이 보강 데이터에는 등록 날짜, 등록 기관 이름 및 출신 국가에 대한 정보가 포함됩니다.

(선택 사항) 보강 조회 실행 및 다음에 대한 예상 결과 확인 **Whois**

Whois 통합을 실행하여 통합에서 반환된 도메인에서 보강 조회를 Reverse Whois 수행합니다.

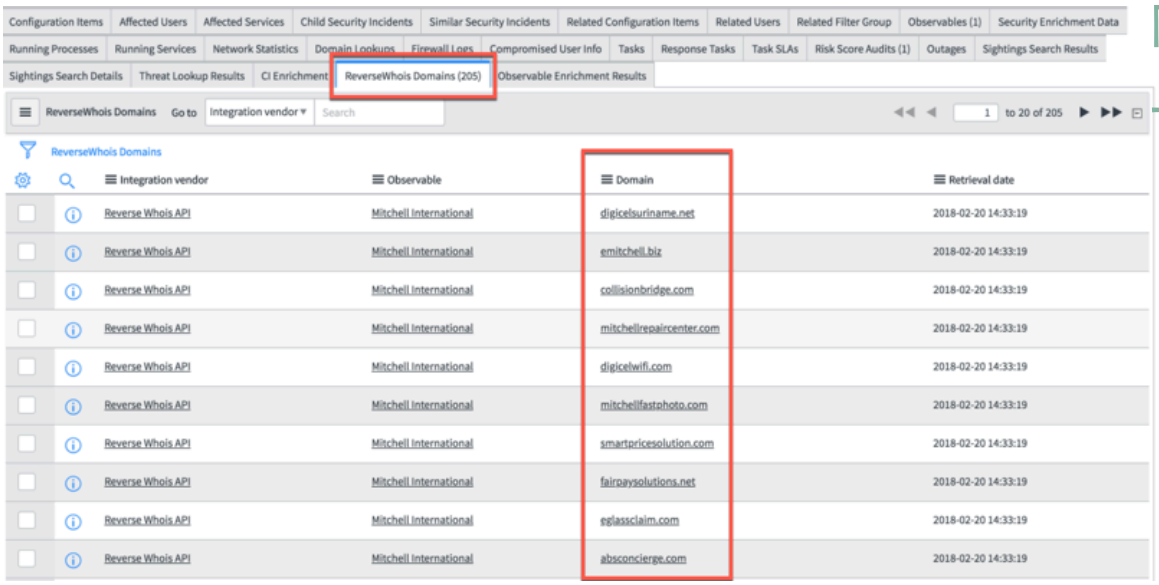
시작하기 전에
및 Whois 플러그인을 설치하고 구성 Reverse Whois 했는지 확인합니다. 플러그인으로 Reverse Whois 도메인 조회를 성공적으로 실행한 후에만 이러한 단계를 수행합니다.

필요한 역할: sn_si.analyst

이 태스크 정보
결과는 옵저버블 기록의 옵저버블 보강 결과 탭에 표시됩니다.

프로시저

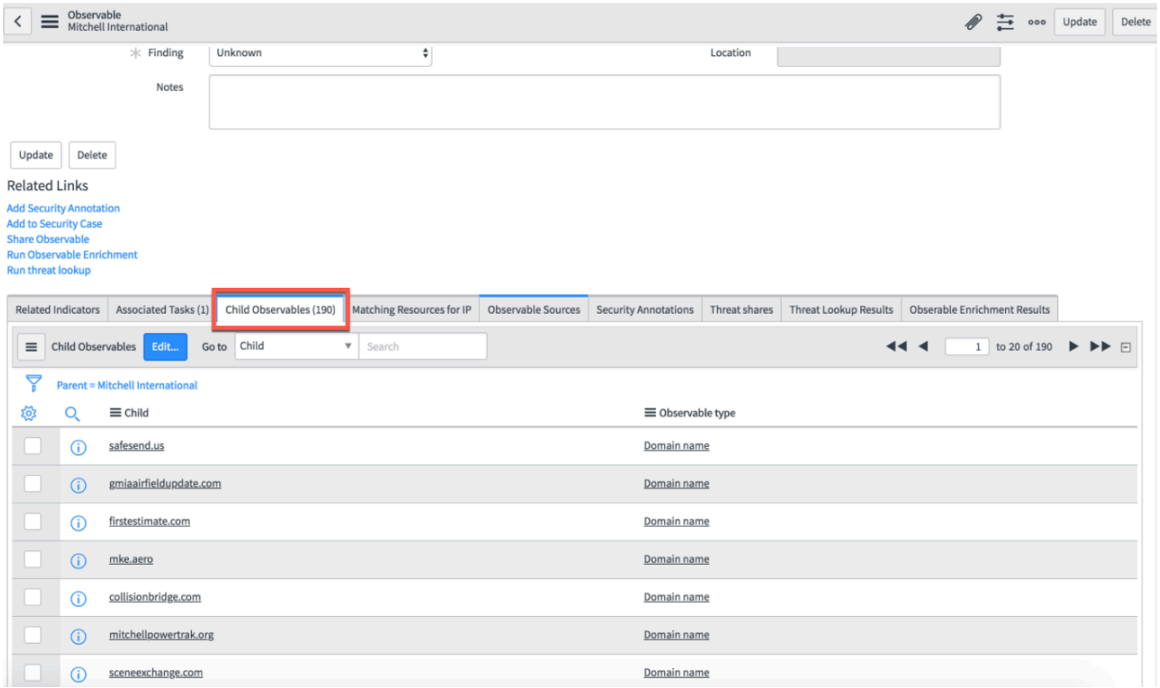
1. 다음으로 이동 모두 〉 보안 인시던트 〉 인시던트 〉 모든 인시던트 표시 도메인 조회를 성공적으로 실행한 작업 중인 보안 인시던트를 찾습니다.
2. 기록을 열고 모든 관련 목록 표시 관련 링크를 클릭합니다.
3. 기록 하단에서 **Reverse Whois Domains(Whois** 도메인 역) 탭을 선택합니다.



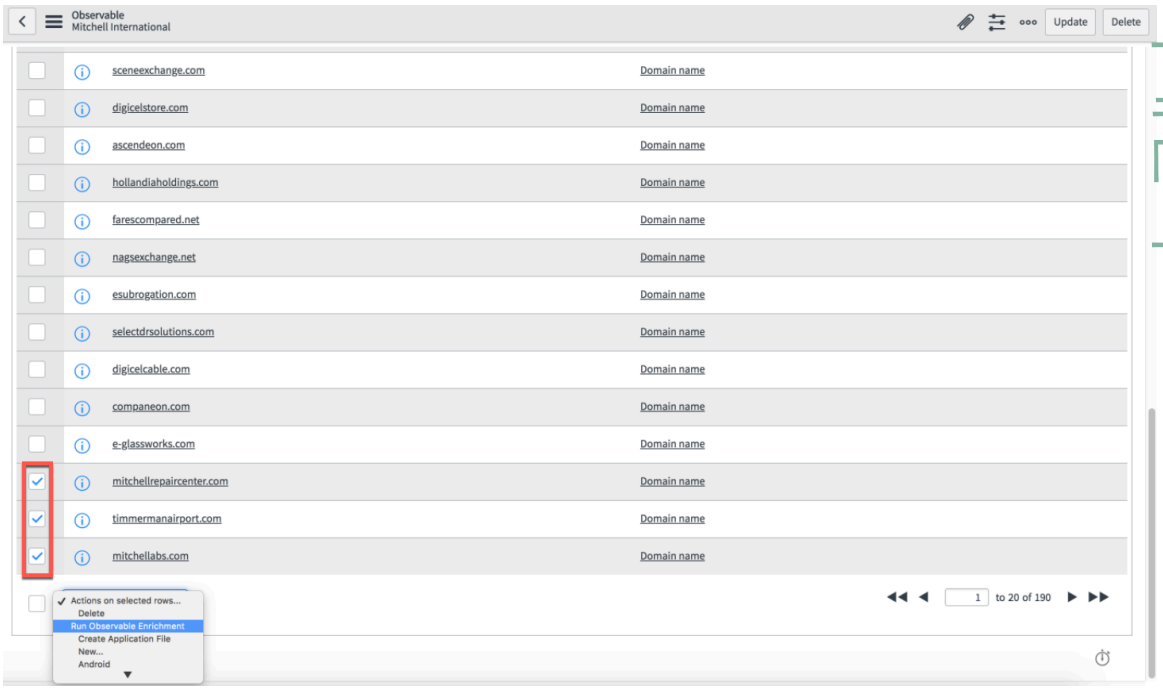
도메인 열에 반환된 도메인 목록이 표시됩니다.

4. 옵저버블 열에서 옵저버블을 클릭합니다.
하위 옵저버블 탭에 하위 옵저버블이 표시됩니다. 하위 옵저버블은 애플리케이션에서 옵저버블의 초기 검사에서 Reverse Whois 도메인을 반환하는 경우에만 생성됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



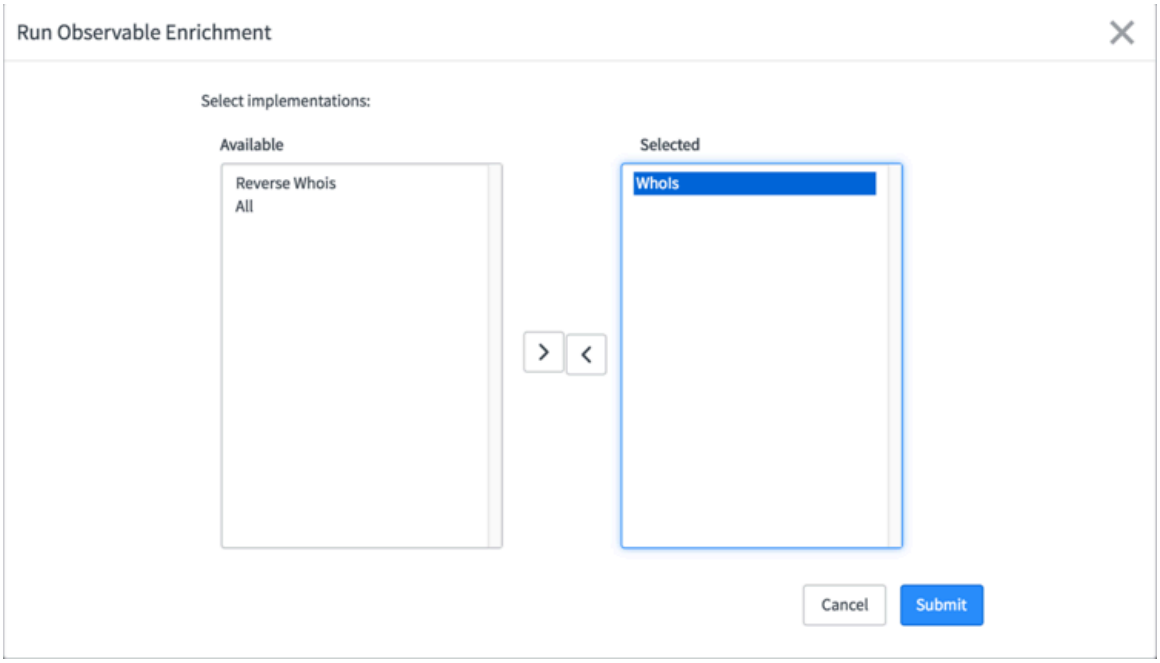
5. 옵저버블 보강을 실행할 하위 옵저버블을 선택하고 선택한 행 선택 목록에 대한 작업에서옵저버블 보강 실행을 선택합니다.



옵저버블 보강 실행 대화 상자가 표시됩니다.

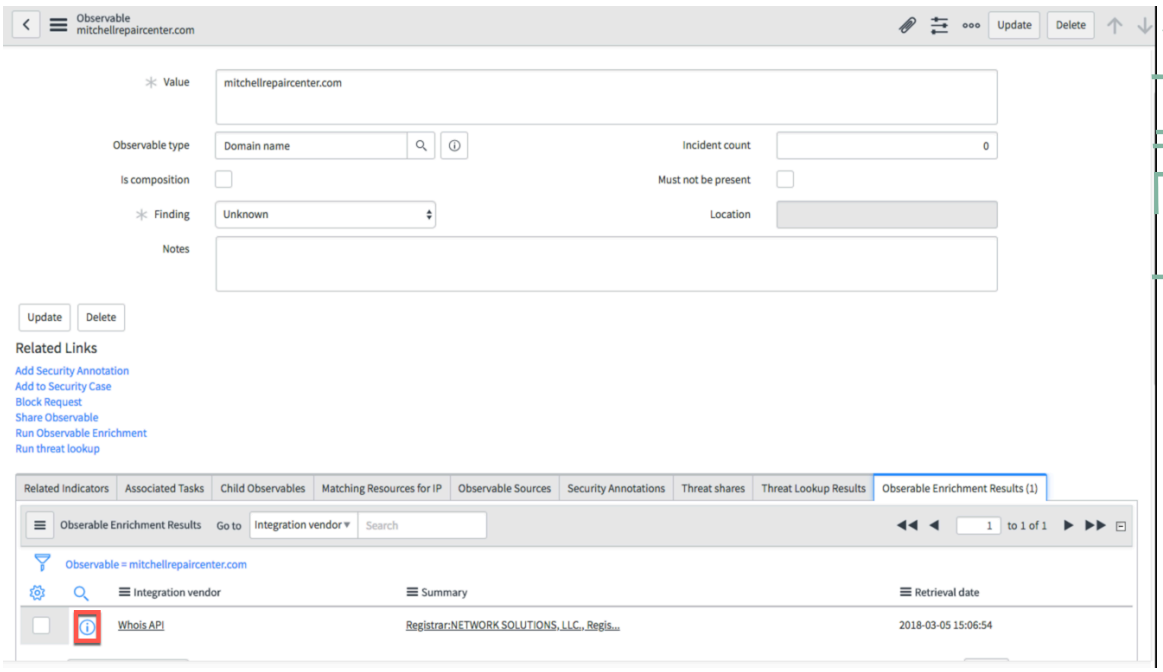
6. Whois 통합을 사용 가능에서 선택됨으로 옮기고 제출을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



결과는 옵저버블 기록의 옵저버블 보강 결과 탭에 표시됩니다.

7. 파란색 정보 아이콘을 클릭한 다음 표시되는 대화 상자에서 기록 열기 를 클릭합니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

등록 날짜, 등록기관 이름 및 출신 국가와 같은 원래 도메인 조회와 관련된 원시 데이터와 자세한 정보가 표시됩니다.

Trouble?
하위 옵저버블 또는 보강 결과를 찾을 수 없는 경우 통합이 성공적으로 실행되고 도메인이 Reverse Whois 반환되었는지 확인합니다. 또한 자세한 내용은 기록의 작업 메모를 참조하십시오.

관련 정보

Reverse Whois 설치 및 구성

에 대한 예상 결과 확인 Reverse Whois

RISKIQ와 **WHOISIQ** 통합

제품과 WHOISIQ API ServiceNow AI Platform# 보안 운영 를 RISKIQ 통합하면 보안 분석가에게 추가 보강 데이터와 웹 사이트의 유효성에 대한 통찰력이 제공됩니다.

SSL 인증서 API는 RISKIQ 발급 인증 기관, 인증서를 요청하는 조직, 인증서가 발급된 엔터티 및 도메인에 대한 상세 정보를 포함하는 SSL 인증서에 대한 조회를 수행합니다. SSL 인증서 조회는 보안 인시던트가 생성될 때 자동으로 수행됩니다.

API는 RISKIQ WHOISIQ 도메인, 이메일, 네임서버, 조직, 주소 및 전화 번호와 같은 다른 옵저버블 유형에 대한 조회를 수행합니다. URL 및 도메인 옵저버블은 보안 인시던트가 생성될 때 자동으로 보강됩니다.

통합하려면 및 위협 인텔리전스 제품이 필요합니다보안 인시던트 응답.

및 에 지원되는 **RISKIQ** 옵저버블 **RISKIQ WHOISIQ**

API는 RISKIQ IP 주소, 파일 해시, 인증서 일련 번호, 도메인 및 URL 옵저버블에 대한 자동 SSL 인증서 조회를 지원합니다. URL 및 도메인 옵저버블은 API를 통해 자동으로 보강됩니다 WHOISIQ . API를 WHOISIQ 사용하여 다른 유형의 옵저버블에 대한 옵저버블을 보강하려면 옵저버블을 생성하고 옵저버블 테이블에서 수동으로 조회를 실행합니다.

지원되는 옵저버블

다음 테이블에는 이 통합에 사용되는 API 유형과 각 API가 지원하는 옵저버블이 나와 있습니다. 또한 이 테이블은 보안 인시던트가 생성될 때 조회가 자동으로 발생하는지 또는 옵저버블 테이블에서 조회가 수동으로 실행되는지 여부를 나타냅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

지원되는 옵저버블 및 조회

API	지원되는 옵저버블	조회(자동 또는 수동)
RISKIQ SSL 인증서 API	• IP 주소 • 파일 해시(인증서 지문)입니다. 파일 해시의 예는 다음 그림을 참조하십시오. • 인증서 일련 번호 또는 일련 번호. 이 문자열은 엔터티의 고유 ID입니다. 인증서 일련 번호의 예는 다음 그림을 참조하십시오. • 도메인(www.site.com 또는 site.com) • URL 주: 자동 스캔은 https:// 프로토콜을 사용하여 URL 형식에 대해 실행됩니다(예: https://example.com/index.html	인시던트 생성 시 자동 조회입니다. 결과는 보안 인시던트 기록의 **SSL** 인증서 탭에 표시됩니다.
RISKIQ WHOISIQ API를 참조하십시오.	• 도메인 • URL	인시던트 생성 시 자동 조회입니다. 결과는 보안 인시던트 기록의 옵저버블 보강 결과 탭에 표시됩니다.
RISKIQ WHOISIQ API를 참조하십시오.	• 이메일 주소 • 조직 이름 • 전화 번호 • 우편물 발송 주소	수동 조회는 옵저버블 테이블에서 실행됩니다. 결과는 옵저버블 기록의 옵저버블 보강 결과 탭에 표시됩니다.

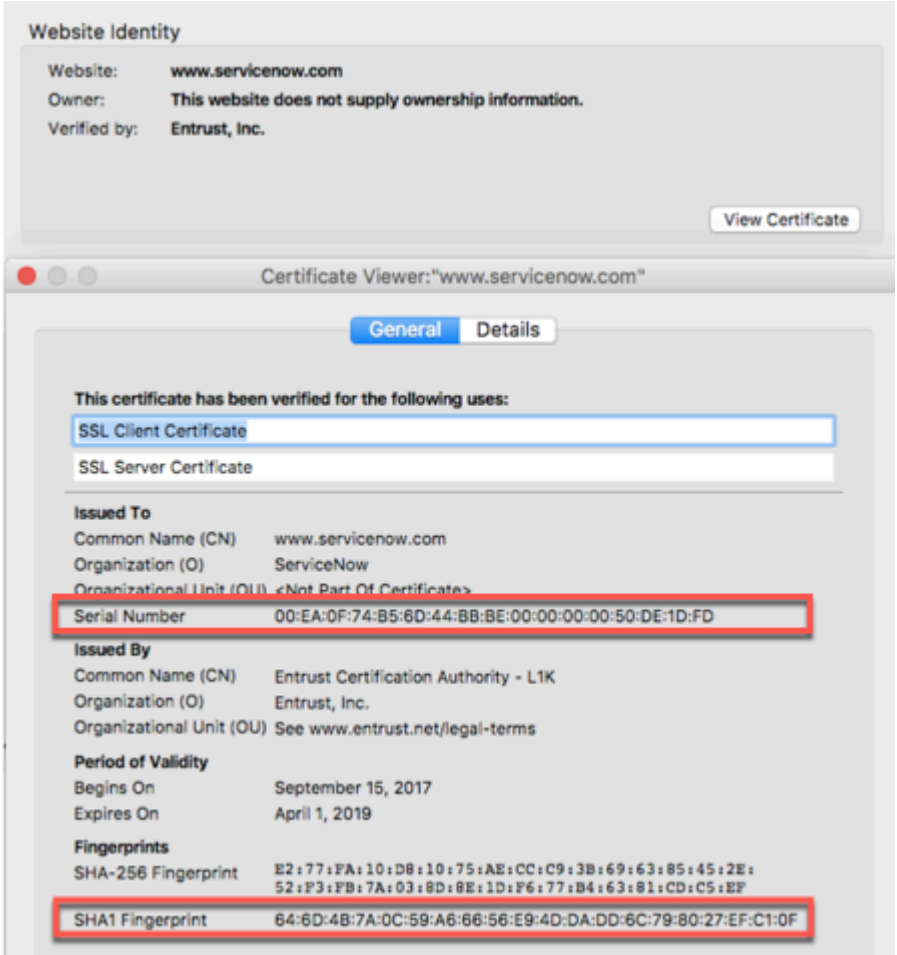
파일 해시 및 인증서 일련 번호의 예

이 그림은 이 통합에 대한 SSL 인증서 조회에 사용되는 파일 해시 및 인증서 일련 번호 옵저버블의 예를 보여줍니다. 파일 해시는 SHA-1 지문을 참조합니다. 이 값은 콜론 구분 기호 없이 인스턴스에 표시됩니다 ServiceNow AI Platform . 예: 646D4B7A0C59A66656E94DDADD6C798027EFC10F.

인증서 일련 번호 옵저버블은 엔터티의 고유 ID 또는 일련 번호를 나타냅니다. 이 값은 콜론 구분 기호 없이도 표시됩니다. 예: 00EA0F74B56D44BBBE0000000050DE1DFD.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

파일 해시 및 인증서 일련 번호



설치 및 구성 **RISKIQ** 및 **WHOISIQ**

인스턴스에서 통합을 실행하기 전에 설치 및 구성 단계를 RISKIQ 완료하여 및 WHOISIQ 애플리케이션이 .ServiceNow AI Platform 보안 운영

시작하기 전에

필요한 역할: admin, RISKIQWHOISIQ admin

설치하기 전에 다음 설정 검사 목록을 완료합니다. 이러한 설정 작업은 원활한 설치 및 구성을 위해 필요합니다.

설정 작업	설명
필요한 역할을 할당했는지 확인합니다.	예상 결과의 설치, 구성 및 검증에 필요한 역할은 다음과 같습니다. • 시스템 관리자(admin)가 앱을 설치하고 보안 인시던트 관리자(sn_si.admin) 역할을 할당합니다. • 보안 인시던트 관리자(sn_si.admin)는 구성을 감독하고 예상 결과를 확인합니다. 또한 이 역할은 모듈에 액세스할 보안 운영 수 있으며

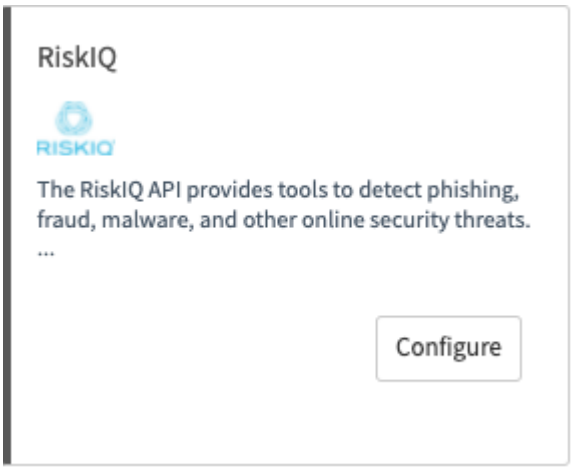
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설정 작업	설명
	보안 인시던트 분석가(sn_si.analyst) 역할을 할당합니다. • 보안 인시던트 분석가(sn_si.analyst)는 보안 인시던트 기록을 다룹니다.
사용자 이름 및 API 키를 가져옵니다.	API 키 및 계정 생성 방법에 대한 자세한 내용은 웹사이트를 방문하십시오: RISKIQ 웹사이트. 구성하려면 API 키를 입력해야 합니다.
ServiceNow 통합을 위해 애플리케이션을 설치하기 전에 통합을 지원하는 데 필요한 핵심 애플리케이션이 설치되고 활성화되었는지 확인합니다.	Madrid 이상 릴리스 요구 사항 Madrid 릴리스 및 이후 제품군 릴리스의 경우 Dependency 플러그인(com.snc.si_dep)이 보안 인시던트 응답 필요합니다. 이 플러그인은 제품을 지원하는 데 필요한 모든 종속성을 보안 인시던트 응답 자동으로 설치합니다. 통합에 필요한 다른 보안 운영 애플리케이션을 설치하고 활성화하기 전에 이 플러그인을 설치하고 활성화합니다. 에서 ServiceNow Store다음 보안 운영 애플리케이션이 설치되고 활성화되는지 확인합니다. 설치되지 않은 경우 원활한 설치를 위해 다음 순서로 한 번에 하나의 애플리케이션을 설치하고 활성화합니다. **1.** 보안 인시던트 응답 **2.** 보안 통합 프레임워크 **3.** Security Support Common **4.** 보안 지원 오케스트레이션 통합을 위한 인스턴스 설정에 ServiceNow AI Platform 대한 자세한 내용은 해당 문서를 애플리케이션 활성화 ServiceNow Store참조하십시오제품 또는 애플리케이션에 대한 보안 운영 권리 가져오기.

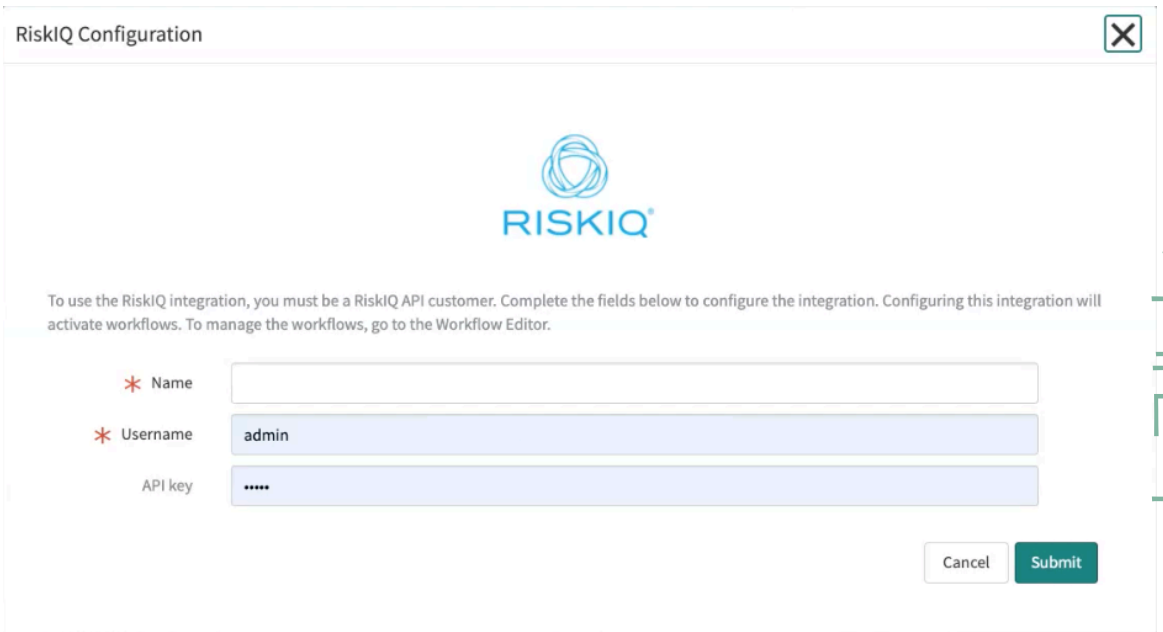
프로시저

1. 통합을 위해 애플리케이션을 설치하지 않은 경우 이를 확인하고 보안 운영 통합 설치 단계에 따라 설치합니다.
2. 설치가 완료되면 다음으로 이동합니다. 보안 운영 〉 통합 〉 통합 구성 를 클릭하고 API 타일을 찾습니다.
3. 구성을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



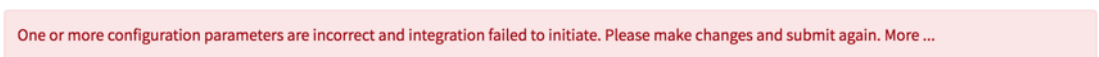
4. 표시되는 RiskIQ 구성 대화 상자에서 사용자 이름 및 **API** 키를 입력합니다.



5. 제출을 클릭합니다.
6. 구성이 성공했는지 확인합니다.
   구성이 성공적으로 완료되면 통합 타일이 있는 보안 통합 페이지가 표시됩니다.

Trouble?
오류 메시지가 표시되면 사용자 이름 또는 API 키가 잘못되었을 수 있습니다. 사용자 이름과 API 키가 올바른지 확인합니다.

문제 해결



SSL 인증서 조회에 대한 **RISKIQ** 예상 결과 확인

보안 인시던트로 인해 URL, 도메인, IP 주소, 인증서 파일 해시(SHA-1 지문) 및 인증서 일련 번호에 대한 옵저버블이 생성되면 보안 인시던트 분석가는 SSL 인증서 조회 결과를 사용하여 사이트에 신뢰할 수 있는 공용 CA(인증 기관)에서 발급한 인증서가 있는지 확인합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_si.analyst

이 태스크 정보
지원되는 옵저버블의 ServiceNow AI Platform 경우 가장 최근에 발생한 URL, 도메인, IP 주소, 인증서 파일 해시(SHA-1 지문) 및 인증서 일련 번호를 검사합니다. 스캔 결과의 가능한 결과는 다음과 같습니다.

정확히 일치하는 항목이 발견되었습니다.

SSL 인증서의 유효한 발급자가 보안 인시던트 기록에 나열되어 있습니다.

인증서 결과를 찾을 수 없습니다.

보안 인시던트 기록에 결과가 나열되지 않습니다.

자체 서명되었거나 내부적으로 생성된 인증서와 정확히 일치하는 항목이 있습니다.

내부적으로 생성된 SSL 인증서에 대한 결과가 보안 인시던트 기록에 표시됩니다.

기본 SSL 인증서와 정확히 일치하는 항목을 찾을 수 없습니다

조회 값이 여러 항목을 반환하고 기본 인증서를 식별할 수 없습니다. 요약 메시지가 보안 인시던트 기록에 표시됩니다.

프로시저

1. 옵저버블을 보고 조회 결과를 확인하려면 작업 중인 보안 인시던트 기록을 열고 작업 메모를 찾습니다.

Example
이 통합에 대해 발생할 수 있는 조회 결과의 예를 설명하기 위해 다음 옵저버블을 사용하여 보안 인시던트가 생성되었다고 가정해 보겠습니다.

- community.servicenow.com
- invalidsubdomain.servicenow.com
- mail.dgnetworks.com
- ServiceNow.com

옵저버블 및 조회 결과 위치

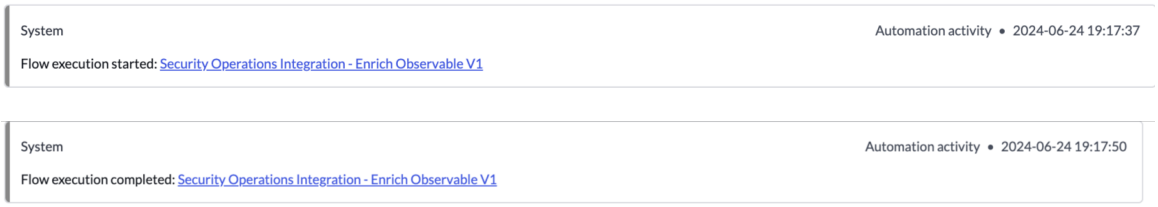
옵저버블(예)	스캔 결과	설명 및 위치
community.servicenow.com	SHA1 해시가 있는 인증서를 찾았습니다.	정확히 일치하는 항목이 발견되고 유효한 SSL 인증서 발급자가 나열됩니다. 정확히 일치하는 결과는 보안 인시던트 기록의 **SSL** 인증서 탭에 표시됩니다.
invalidsubdomain.servicenow.com	인증서를 찾을 수 없습니다.	인증서 결과를 찾을 수 없음을 나타내는 요약이 보안 인시던트 기록의 옵저버블 보강 결과 탭에 표시됩니다.
mail.dgnetworks.com	SHA1 해시가 포함된 인증서를 찾았습니다.	자체 서명되었거나 내부에서 생성된 인증서와 정확히 일치하는 항목이 나열됩니다. 결과는 보안 인시던트 기록의 **SSL** 인증서 탭에 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵저버블(예)	스캔 결과	설명 및 위치
ServiceNow.com	검색에서 138개의 인증서가 반환되었으며 단일 기본 인증서를 식별할 수 없습니다.	조회 값이 여러 인증서를 반환하기 때문에 기본 SSL 인증서와 정확히 일치하는 항목을 찾을 수 없습니다. 기본 인증서를 찾을 수 없음을 나타내는 요약이 보안 인시던트 기록의 옵저버블 보강 결과 탭에 표시됩니다.

애플리케이션이 구성되면 플로우가 자동으로 시작됩니다. 조회 상태와 옵저버블이 작업 메모에 표시됩니다.

2. 조회가 성공적으로 실행되었는지 확인합니다.



Trouble?
예상 결과를 볼 수 없는 경우 통합을 위한 SSL 인증서 조회에서 옵저버블을 지원하는지 확인합니다.

관련 정보

및 에 지원되는 RISKIQ 옵저버블 RISKIQ WHOISIQ

RISKIQ 정확히 일치하는 항목을 반환하는 **SSL** 인증서 조회

RISKIQ 정확히 일치하는 SSL 인증서 조회 결과는 보안 인시던트 기록의 **SSL** 인증서 탭에 표시됩니다. 정확히 일치하면 보안 인시던트 분석가가 웹 사이트의 유효성을 판단하는 데 도움이 되는 유효한 인증 기관 이름을 제공합니다.

Example: 유효한 **SSL** 인증서와 정확히 일치

다음 예에서는 조회 결과와 정확히 일치하는 유효한 SSL 인증서 발급자를 보여줍니다. 단계에 따라 결과 및 원시 데이터를 봅니다.

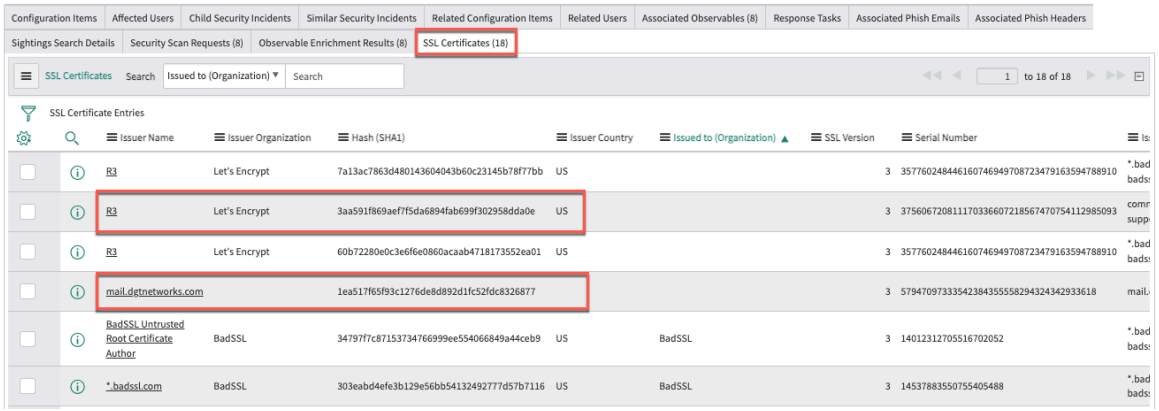
주:
다음 예제의 그림은 시스템 설정에서 탭 양식 설정이 활성화된 상태로 표시됩니다. 화면이 아래 표시된 보기와 일치하지 않으면 단계에 따라 탭 양식을 설정하십시오.

1. 배너 프레임 오른쪽 상단 모서리에서 설정 아이콘을 클릭합니다.
2. 표시되는 시스템 설정 대화 상자에서 폼을 클릭하고 탭 폼 및 폼 사용이 선택되어 있는지 확인합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

1. 보안 인시던트 기록에서 **SSL** 인증서 탭을 클릭합니다.

SSL 인증서 탭



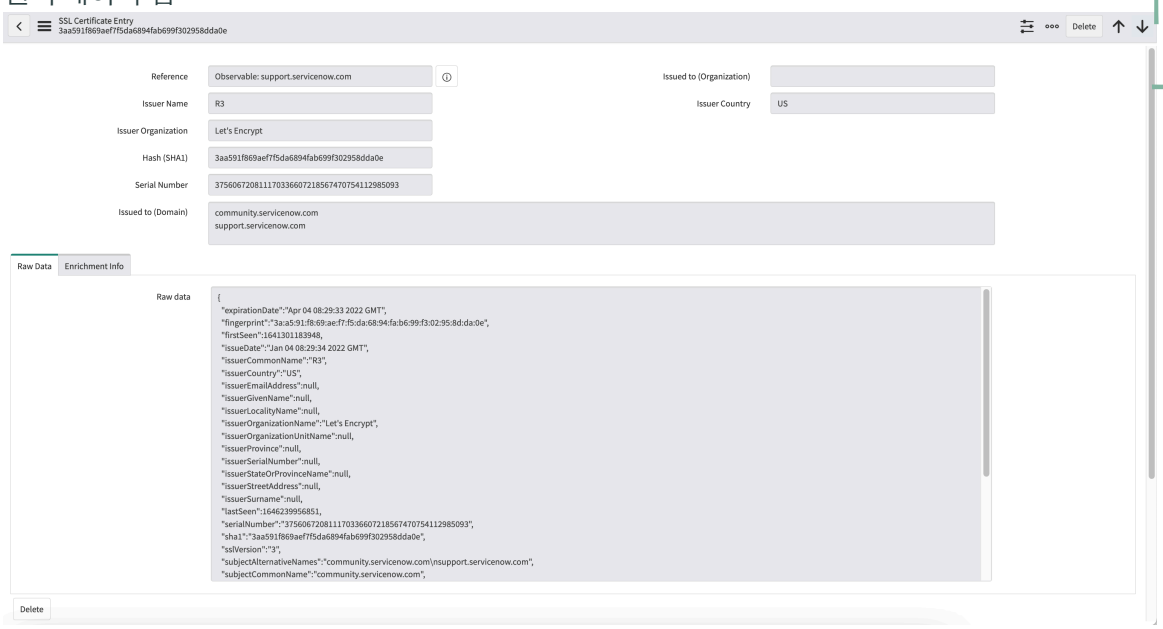
인증서 발급자의 이름, 발급자의 조직 및 인증서 발급 대상(조직)에 대한 정보가 다른 데이터와 함께 표시됩니다.

발급자 이름 열에 18개 항목이 표시됩니다. 두 번째 항목(R3)은 발급자 조직 열에 유효한 인증 기관 이름(Let's Encrypt)을 제공합니다.

두 번째 항목(mail.dgtnetworks.com)에 대해 발급자 조직 및 발급 대상 열에 정보가 표시되지 않습니다.

2. 발급자 이름열에서 두 번째 항목인 (**R3**)을 클릭하여 항목 기록을 엽니다. 또는 항목 옆에 있는 정보 아이콘을 클릭한 다음 기록 열기를 클릭합니다.
3. 원시 데이터 탭을 선택합니다.

원시 데이터 탭



SSL 인증서 항목 기록에는 엔터티 이름 열 아래의 원시 데이터 탭에 있는 옵저버블과 기타 데이터가 포함됩니다.

참고: 범주 열에서 ##과 ####엔터티 이름 열의 인식 가능한 엔터티에 해당합니다. 이 인증서의 발급자는 신뢰할 수 있는 공용 인증 기관에서 발급했을 가능성이 높습니다. 또한 ##와 #### 서로 다른 엔터티입니다. 이러한 개별 엔터티는 인증서가 알 수 없는 인증 기관에서 내부적으로 서명된 인증서가 아님을 나타냅니다.

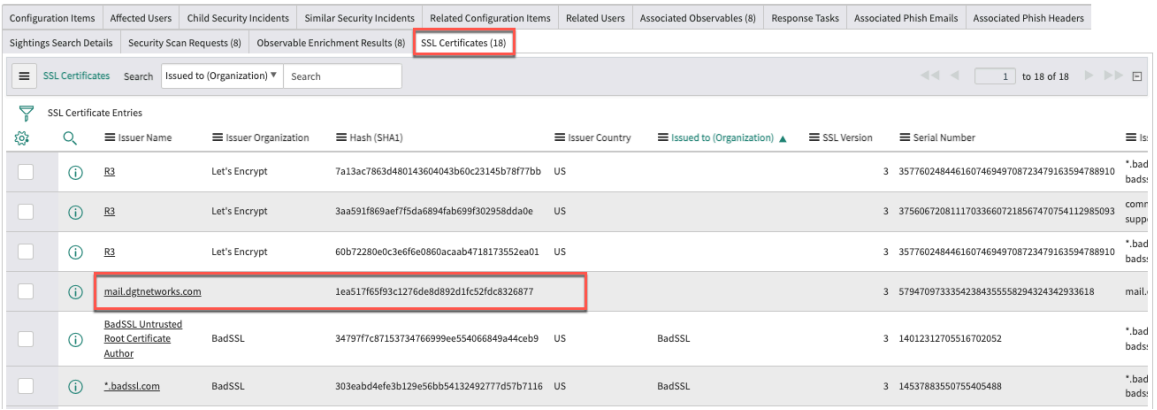
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Example: 자체 서명된 **SSL** 인증서와 정확히 일치

다음 예는 조회에서 자체 서명된 SSL 인증서에 대한 결과를 보여줍니다. 단계에 따라 결과 및 원시 데이터를 봅니다.

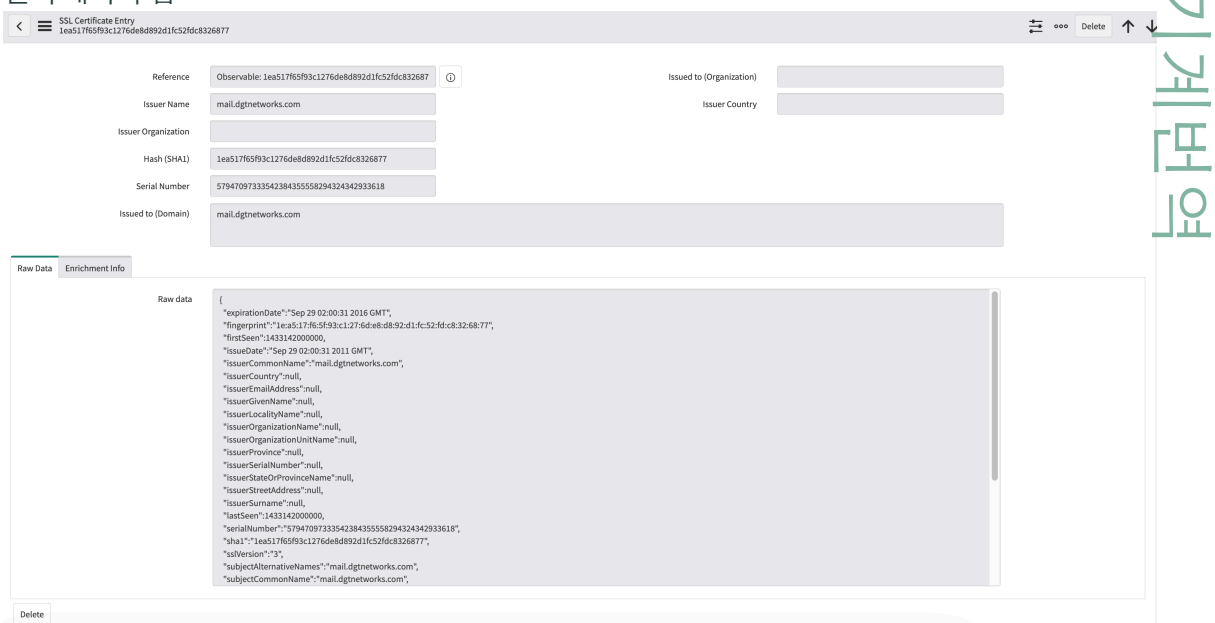
1. 보안 인시던트 기록으로 다시 이동합니다. 발급자 이름 열에서 다른 항목 (**mail.dgtnetworks.com**)을 클릭합니다.

SSL 인증서 탭



2. 열려 있는 기록에서 원시 데이터 탭을 선택합니다.

원시 데이터 탭



범주 열은 ###(mail.dgtnetworks.com 및 dgtsb# #####. DGTNetworks.local)은 신뢰할 수 있는 공용 인증 기관이 아닙니다. 또한 ###### 가 동일한 엔터티(dgtsb. DGTNetworks.local)을 포함하며 각각 옵저버블의 이름(dgtsbs)을 포함합니다. 이 인증서는 자체 서명된 인증서일 수 있습니다. 자체 서명된 인증서는 알려진 인증 기관에서 발급한 것이 아니므로 추가 조사가 필요할 수 있습니다.

RISKIQ 여러 인증서를 반환하거나 인증서를 반환하지 않는 **SSL** 인증서 조회

보안 인시던트 분석가는 여러 SSL 인증서 결과를 사용하여 사이트가 공통적이고 인식 가능한 엔터티의 일부인지 여부를 확인할 수 있습니다. SSL 인증서 없음 결과는 이름이 모호하거나 의심스러운 사이트에 신뢰할 수 있는 인증서가 없음을 나타낼 수 있습니다. SSL 인증서를 반환하지

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

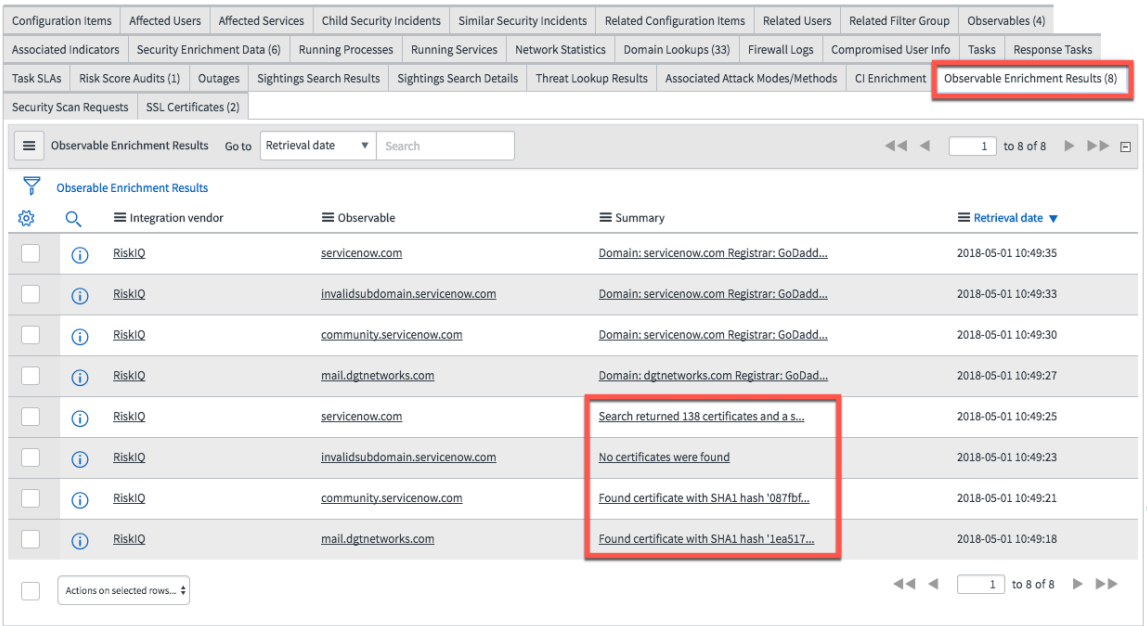
않거나 여러 SSL 인증서를 반환하는 옵저버블에 대한 조회 결과는 보안 인시던트 기록의 옵저버블 보강 결과 탭에 표시됩니다.

Example: SSL 인증서 결과 없음 또는 여러 SSL 인증서 결과

단계에 따라 SSL 인증서를 반환하지 않거나 여러 인증서를 반환하는 옵저버블에 대한 결과를 확인합니다.

1. 보안 인시던트 기록에서 옵저버블 보강 결과 탭을 클릭합니다.

옵저버블 보강 결과 탭



및 WHOISIQ 조회에 대한 RISKIQ 옵저버블 보강 결과가 표시됩니다.

Observable 열에서 servicenow.com**Summary** 열의 Search returned 138 certificates 메시지에 해당합니다. 마찬가지로 invalidsubdomain.servicenow.com요약열에서 #### ## # ##에 해당합니다. 이러한 요약은 여러 SSL 인증서가 발견되었으며 각각 SSL 인증서와 정확히 일치하는 항목이 없음을 나타냅니다.

2. **Observable** 열에서 **servicenow.com** 클릭합니다.

여러 **SSL** 인증서

레코드에 표시되는 요약 메시지는 servicenow.com 에 대해 SSL 인증서에 대한 여러 결과가 반환되었으며 기본 SSL 인증서를 일치시킬 수 없음을 나타냅니다. 이 메시지는 servicenow.com 와 같은 공통 도메인 이름을 포함하는 조회에서 종종 반환됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

공통 도메인에 대한 자세한 정보가 필요한 경우 API를 RISKIQ 사용하여 직접 검색을 수행할 수 있습니다.

3. **Observable Enrichment** Results(옵저버블 보강 결과) 탭으로 다시 이동하고 Observable(옵저버블) 열에서 **invalidsubdomain.servicenow.com** 클릭합니다.

SSL 인증서 없음

주:

- 현재 옵저버블에 대한 SSL 인증서를 찾을 수 없는 경우 요약 필드에 #### ## # ### 메시지가 표시됩니다.
- 현재 옵저버블에 대한 활성 SSL 인증서를 찾을 수 없는 경우 요약 필드에 ## #### ## # ###### 메시지가 표시됩니다.

URL 조회에 대한 **WHOISIQ** 예상 결과 확인

보안 인시던트가 URL 또는 도메인에 대한 옵저버블을 생성하면 API는 WHOISIQ 보안 인시던트 생성 시 옵저버블 보강을 자동으로 수행합니다. 조회 결과는 보안 인시던트 기록의 옵저버블 보강 결과 및 **SSL** 인증서 탭에 표시됩니다.

시작하기 전에

주:
다음 단계의 그림은 시스템 설정에서 탭 양식 설정이 활성화된 상태로 표시됩니다.

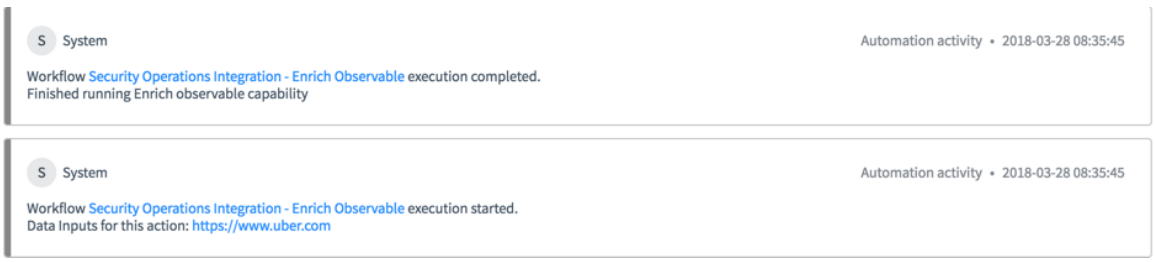
필요한 역할: sn_si.analyst

이 태스크 정보

옵저버블 보강 결과는 보안 인시던트 기록 하단의 옵저버블 보강 결과 탭에 표시됩니다. 지원되는 옵저버블의 경우 SSL 인증서 검색도 실행되고 결과가 **SSL** 인증서 탭에 표시됩니다.

프로시저

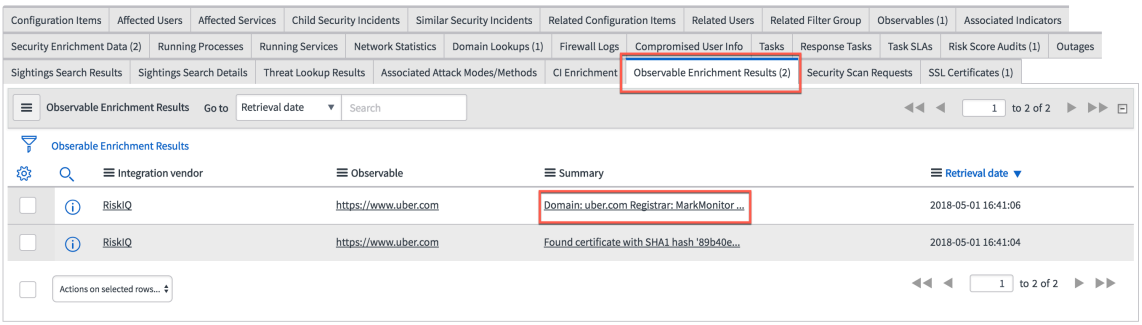
1. 작업 중인 보안 인시던트 기록을 열고 작업 메모에서 조회가 성공적으로 실행되었는지 확인합니다.



애플리케이션이 구성되면 인시던트 생성 시 플로우가 자동으로 시작됩니다. 조회의 실행 및 완료 상태는 보안 인시던트 기록의 작업 메모에 표시됩니다.

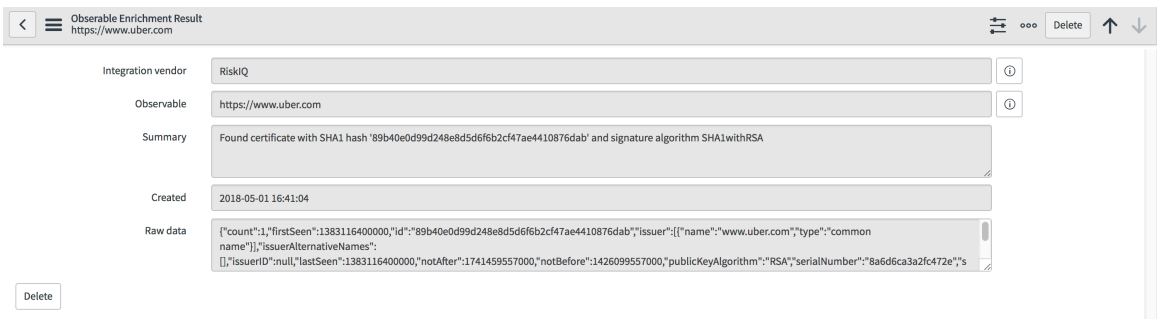
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

2. 조회가 성공적으로 실행되었는지 확인할 수 없는 경우 작업 메모에서 진행 방법에 대한 자세한 내용을 검토하십시오.
3. 열린 보안 인시던트에서 모든 관련 목록 표시 관련 링크를 클릭합니다.
4. 옵저 버블 보강 결과 탭을 클릭하여 선택합니다.
5. 요약 열에서 첫 번째 항목인 **Domain: uber.com Registrar:** Markmonitor…를 클릭합니다.



표시되는 레코드에는 도메인에 대한 정보가 포함되어 있습니다.

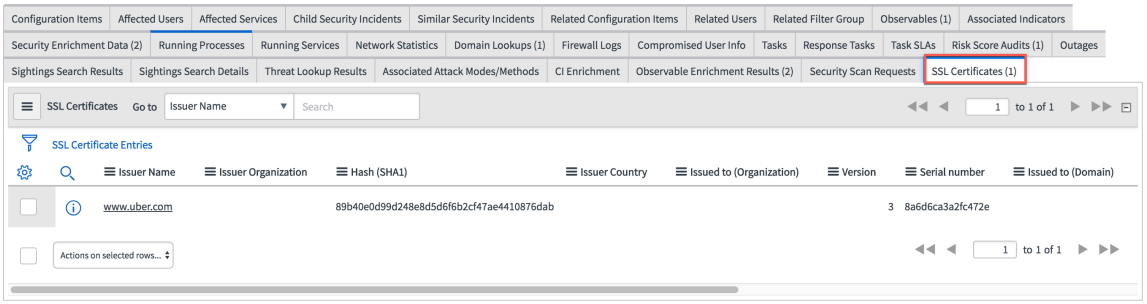
6. **Observable Enrichment** Results(옵저버블 보강 결과) 탭으로 다시 이동하고 Summary(요약) 열에서 두 번째 항목인 **Found certificate with SHA1 hash...(SHA1** 해시가 있는 인증서 찾음...)를 클릭합니다.



이 기록은 파일 해시가 포함된 SSL 인증서가 발견되었음을 나타냅니다.

7. 보안 인시던트 기록으로 다시 이동하여 **SSL** 인증서 탭을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



파일 해시에 대한 SSL 인증서 결과도 여기에 표시됩니다.

Trouble?
예상 결과를 볼 수 없는 경우 작업 메모를 검토합니다. 또한 통합에서 옵저버블이 조회에 지원되는지 확인합니다.

관련 정보

및 에 지원되는 RISKIQ 옵저버블 RISKIQ WHOISIQ

수동 **WHOISIQ** 조회를 위한 옵저버블 생성

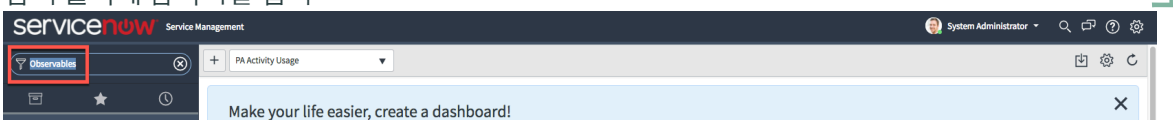
보안 인시던트 분석가는 API를 통한 WHOISIQ 옵저버블 보강의 정보를 사용하여 조직의 이메일 주소, 이름 및 전화번호에 대해 자세히 알아봅니다.

시작하기 전에
필요한 역할: sn_si.analyst

프로시저

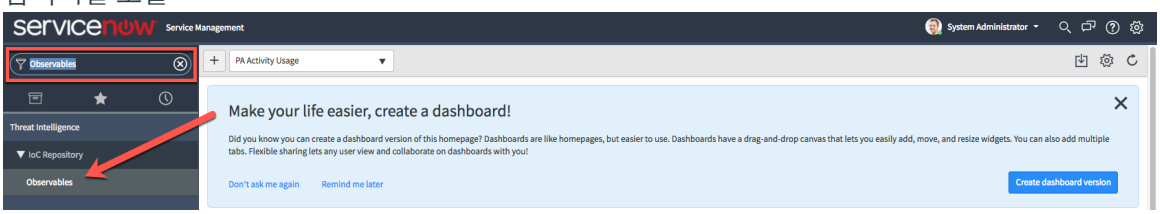
1. 다음으로 이동 모두 〉 **IoC** 리포지토리 〉 옵저버블.

탐색 필터에 옵저버블 입력



탐색 패널 아래에 옵저버블 모듈이 표시됩니다.

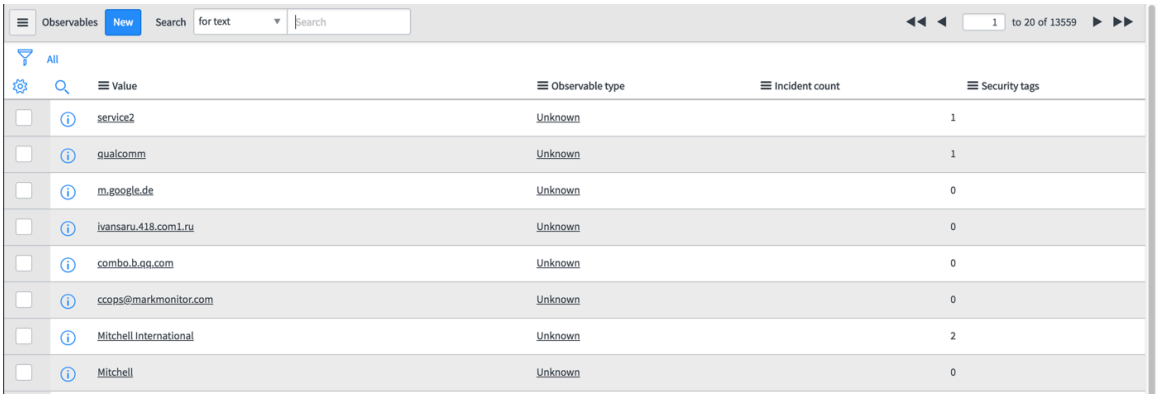
옵저버블 모듈



2. 옵저버블 모듈을 클릭하여 옵저버블 목록을 표시합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

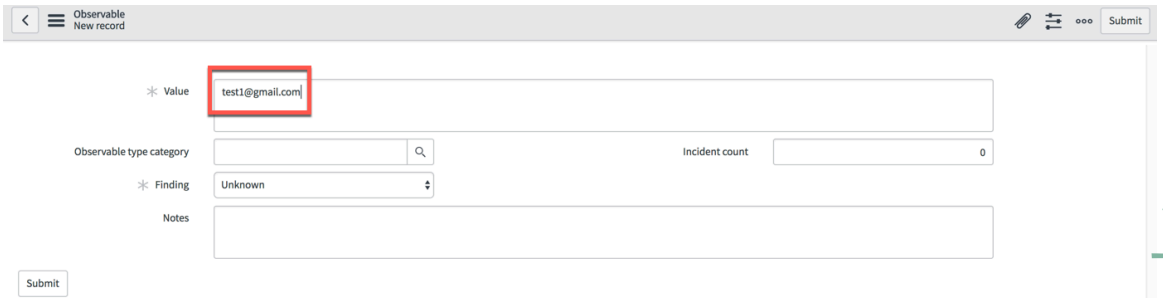
옵저버블 목록



3. 새로 만들기를 클릭하여 새 옵저버블을 생성합니다.

4. 옵저버블 양식의 필드에 내용을 입력합니다.

새 옵저버블 생성



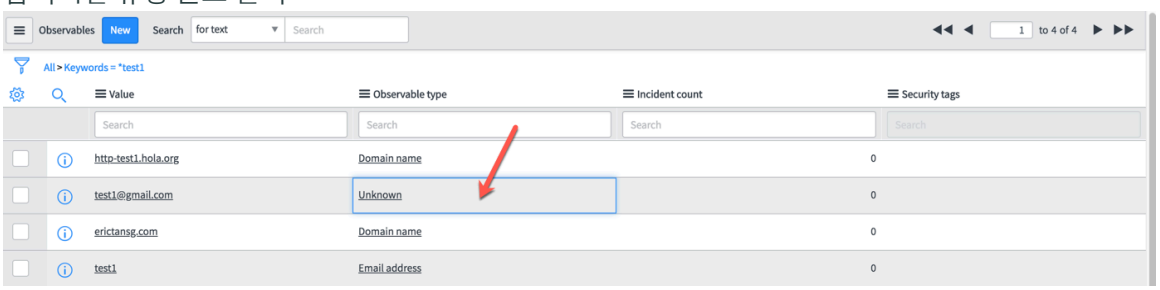
5. 제출을 클릭합니다.
옵저버블 목록으로 돌아갑니다. 값 열에 새 옵저버블이 표시됩니다.

> **주:**
> 표시되는 목록의 일부에서 옵저버블을 찾을 수 없는 경우 검색 기능을 사용하여 찾습니다.

6. 옵저버블 유형 필드를 편집하여 옵저버블과 일치하도록 유형을 알 수 없음에서 이메일 주소로 변경합니다.

a. 옵저버블 유형 열에서 알 수 없음 텍스트의 오른쪽을 한 번 클릭하여 선택합니다.

옵저버블 유형 필드 선택



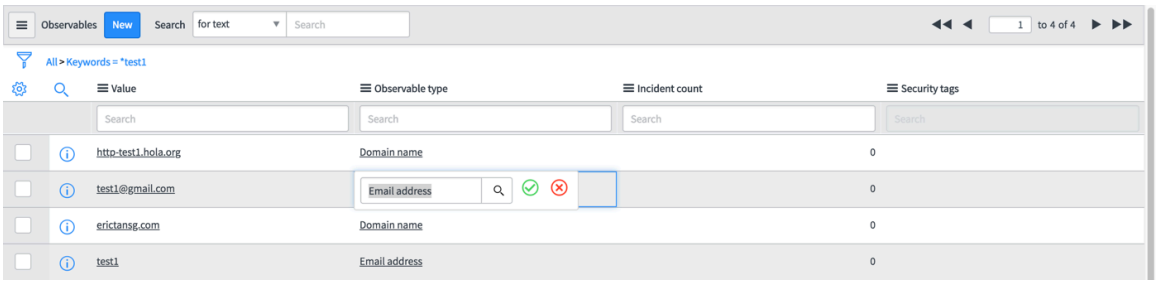
선택한 필드는 파란색 외곽선으로 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

b. 필드가 파란색 윤곽선으로 표시된 상태에서 강조 표시된 필드 안의 아무 곳이나 두 번 클릭하여 편집기를 엽니다.

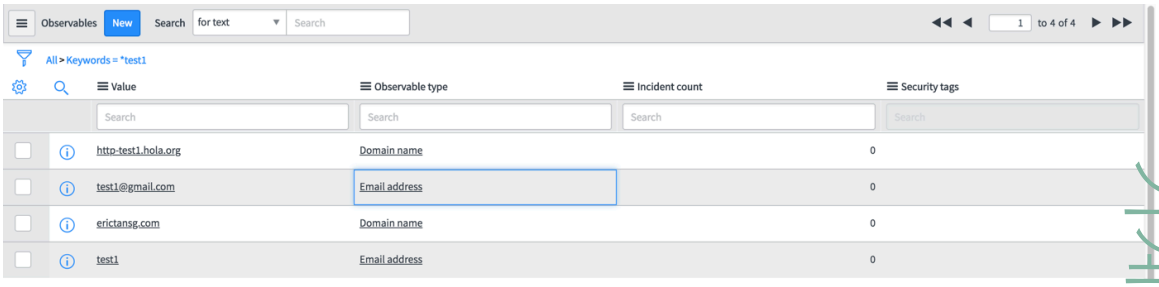
c. 표시되는 필드에 옵저버블 유형(`### ##`)을 입력하고 녹색 확인 표시를 클릭하여 값을 저장합니다.

옵저버블 유형 필드 편집



목록의 옵저버블 유형 열에 새 옵저버블에 대한 ### ### 표시됩니다.

업데이트된 옵저버블 유형 필드



다음에 수행할 작업

조회를 위해 옵저버블을 생성하고 편집한 경우 API를 사용하여 옵저버블 기록에서 옵저버블 보강 조회를 WHOISIQ 실행합니다.

수동 **WHOISIQ** 조회에 대한 예상 결과 확인

보안 인시던트가 자동으로 생성되지 않는 경우 옵저버블에 대해 수동 조회를 실행합니다. 이메일 주소, 조직 이름, 전화번호 또는 우편 주소에 API를 WHOISIQ 사용하는 옵저버블 보강 조회의 경우 옵저버블 테이블에서 수동으로 조회를 시작합니다.

시작하기 전에

필요한 역할: sn_si.analyst

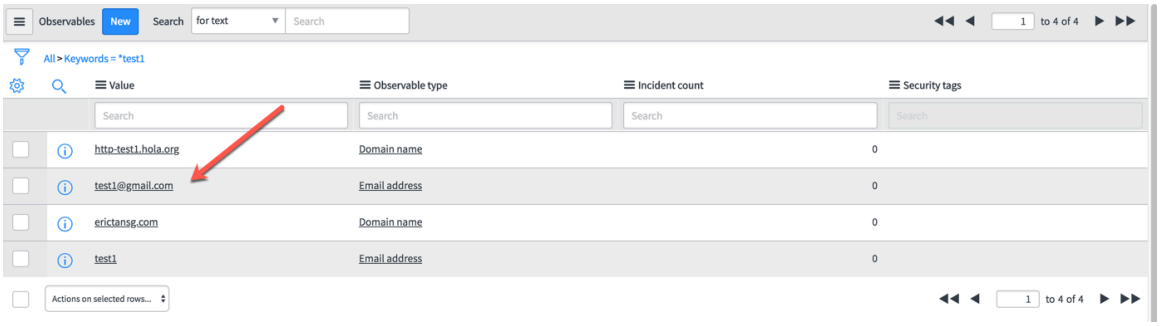
이 태스크 정보

API를 사용하여 수동 조회를 위한 옵저버블을 WHOISIQ 생성합니다. 옵저버블을 만들고 편집하는 방법에 대한 자세한 내용은 문서를 수동 WHOISIQ 조회를 위한 옵저버블 생성참조하십시오.

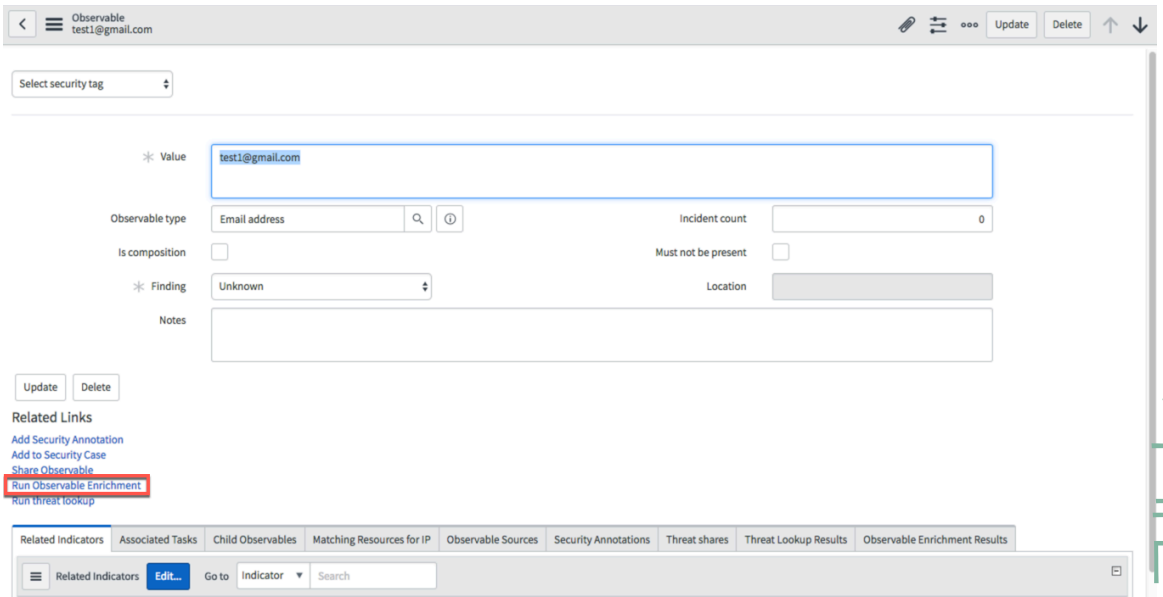
프로시저

1. 다음으로 이동 모두 〉 **IoC** 리포지토리 〉 옵저버블 을 클릭하고 작업 중인 목록에서 옵저버블을 찾습니다.
2. 값 열에서 옵저버블을 클릭하여 기록을 엽니다.

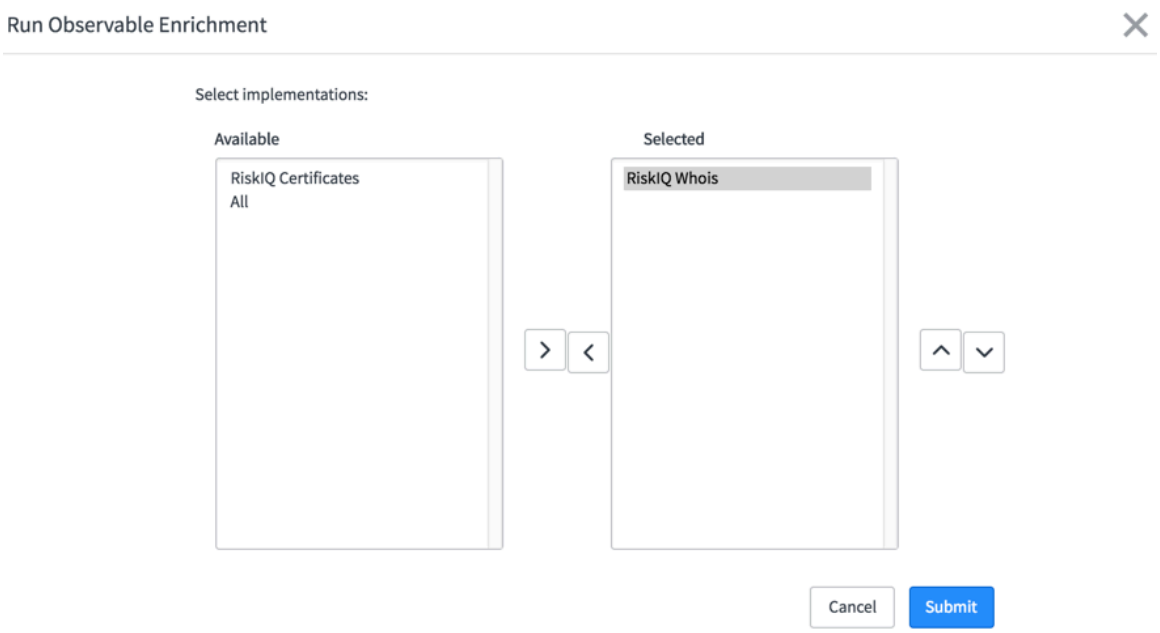
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



3. 옵저버블 보강 실행 관련 링크를 클릭하여 조회를 실행합니다.



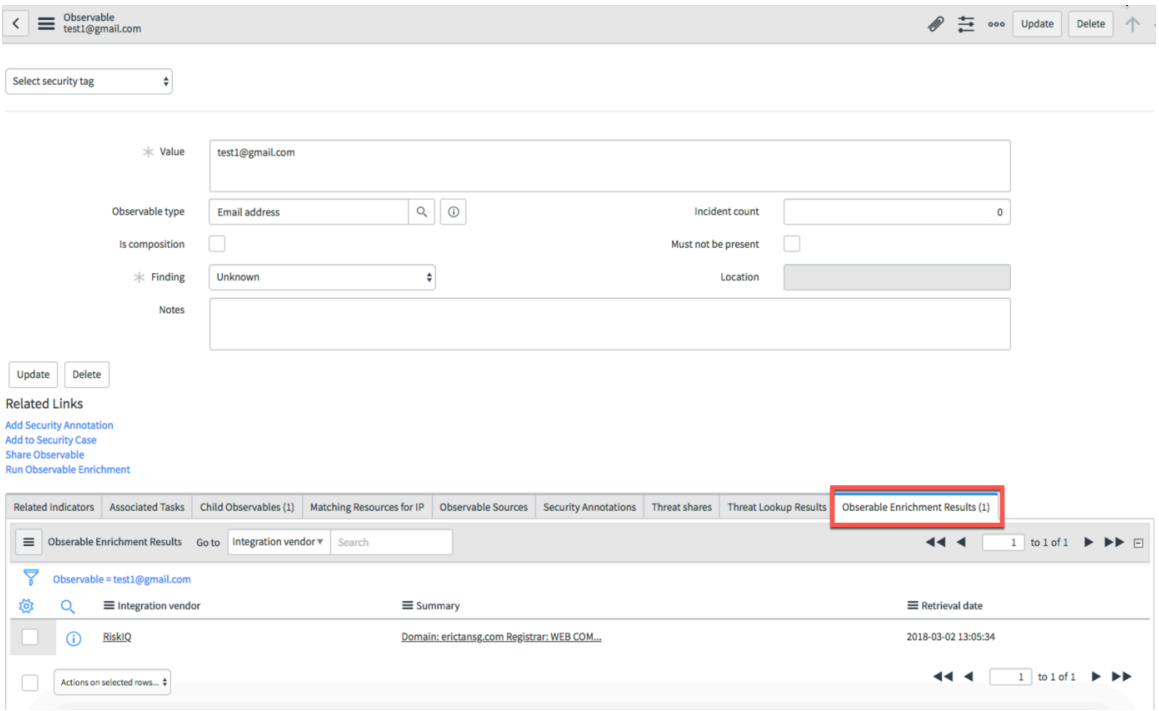
4. 옵저버블 보강 실행 창에서 **RiskIQ** Whois를 선택됨 목록으로 이동합니다.



5. 제출을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

조회 결과는 옵저버블 기록의 옵저버블 보강 결과 탭에 표시됩니다.



Trouble?
옵저버블에 대한 결과가 반환되지 않으면 요약 열에 메시지가 표시됩니다. 결과가 표시되지 않으면 옵저버블이 API에서 지원되는지 확인합니다.

관련 정보

및 에 지원되는 RISKIQ 옵저버블 RISKIQ WHOISIQ

Shodan 통합

Shodan 은 전 세계 연결된 장치의 서비스 배너 정보를 분석하는 검색 엔진입니다. 서비스 배너에는 호스트 이름, 장치 유형, 운영 체제, 지리적 위치 및 연결된 ISP와 같은 컴퓨터 시스템에 대한 정보가 포함됩니다. 제품과 통합 ServiceNow AI Platform 보안 운영 되면 이 서비스 배너 정보는 분석가에게 보안 인시던트 또는 조사를 위한 추가 보강 데이터 및 통찰력을 제공합니다.

통합하려면 및 위협 인텔리전스 플러그인이 보안 인시던트 응답 필요합니다.

통합은 Shodan 다음 옵저버블에 대해 보강을 수행합니다.

- IP 주소
- URL

애플리케이션은 5분마다 새 옵저버블을 확인합니다. 옵저버블이 통합에서 Shodan 인식되는 유형이면 옵저버블이 보강됩니다.

설치 및 구성

인스턴스에서 통합을 실행하기 전에 설치 및 구성 단계를 Shodan 완료하여 애플리케이션이 .ServiceNow AI Platform 보안 운영

시작하기 전에

설치하기 전에 다음 설정 검사 목록을 완료합니다. 이러한 설정 작업은 원활한 설치 및 구성을 위해 필요합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

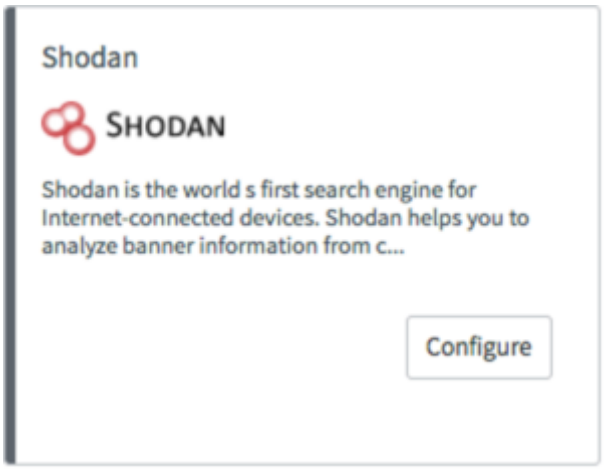
작업 설정	설명
인스턴스에 필요한 ServiceNow AI Platform 역할을 할당했는지 확인합니다.	예상 결과의 설치, 구성 및 검증에 필요한 역할은 다음과 같습니다. • 시스템 관리자(admin)가 앱을 설치하고 보안 인시던트 관리자(sn_si.admin) 역할을 할당합니다. • 보안 인시던트 관리자(sn_si.admin)는 구성을 감독하고 예상 결과를 검증합니다. 이 역할은 모듈에 대한 보안 운영 액세스 권한도 갖습니다.
API 키를 가져옵니다 Shodan .	계정을 만들고 웹 사이트: Shodan 웹 사이트에서 API 키를 Shodan 가져옵니다.
ServiceNow 통합을 위해 애플리케이션을 설치하기 전에 통합을 지원하는 데 필요한 핵심 애플리케이션이 설치되고 활성화되었는지 확인합니다.	Madrid 릴리스 및 이후 제품군 릴리스의 경우 Dependency 플러그인(com.snc.si_dep)이 보안 인시던트 응답 필요합니다. 이 플러그인은 제품을 지원하는 데 필요한 모든 종속성을 보안 인시던트 응답 자동으로 설치합니다. 통합에 필요한 다른 보안 운영 애플리케이션을 설치하고 활성화하기 전에 이 플러그인을 설치하고 활성화합니다. 에서 ServiceNow Store다음 보안 운영 애플리케이션이 설치되고 활성화되는지 확인합니다. 설치되지 않은 경우 원활한 설치를 위해 다음 순서로 한 번에 하나의 애플리케이션을 설치하고 활성화합니다. **1.** 보안 인시던트 응답 **2.** 보안 통합 프레임워크 **3.** Security Support Common **4.** 보안 지원 오케스트레이션 통합을 위한 인스턴스 설정에 ServiceNow AI Platform 대한 자세한 내용은 해당 문서를 애플리케이션 활성화 ServiceNow Store참조하십시오제품 또는 애플리케이션에 대한 보안 운영 권리 가져오기.

필요한 역할: 관리자

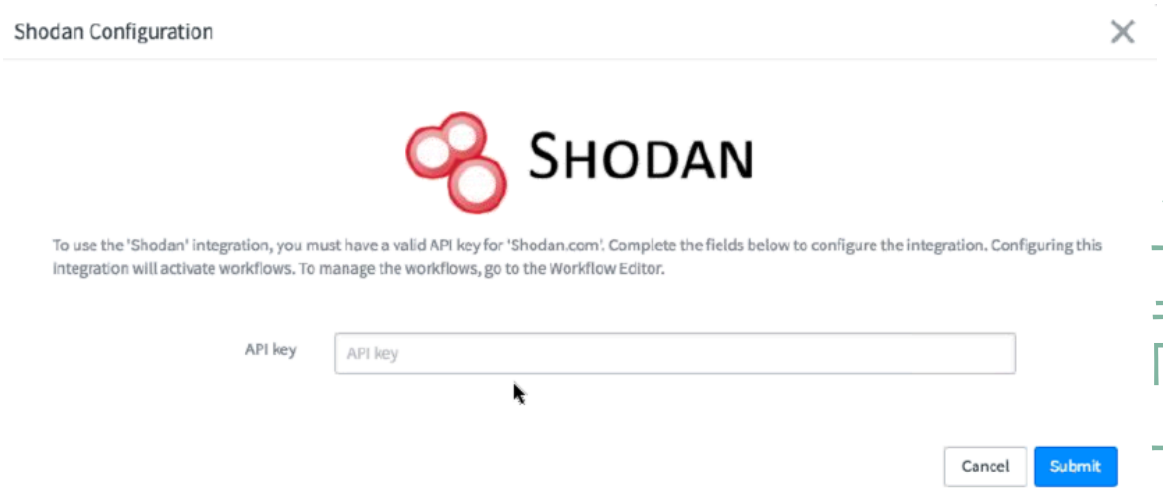
프로시저

1. 통합을 위해 애플리케이션을 설치하지 않은 경우 이를 확인하고 보안 운영 통합 설치 단계에 따라 설치합니다.
2. 설치가 완료되면 통합 > 통합 구성 타일을 Shodan 찾습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



3. 구성을 클릭합니다.
4. **Shodan** 구성 대화 상자에서 웹 사이트에서 가져온 Shodan API 키를 입력하고 제출을 클릭합니다.



5. 구성이 성공했는지 확인합니다.
   오류 메시지가 표시되지 않는 한 구성이 성공적으로 완료된 것입니다.

   Trouble?

   구성 Shodan 중에 오류 메시지가 표시되면 API 키가 잘못되었을 수 있습니다.

예상 결과 확인

옵저버블은 보안 인시던트에 의해 자동으로 생성되고 애플리케이션에서 검사됩니다. 보강 결과는 옵저버블 보강 결과 및 네트워크 배너 탭에 표시됩니다.

시작하기 전에

필요한 역할: sn_si.analyst.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

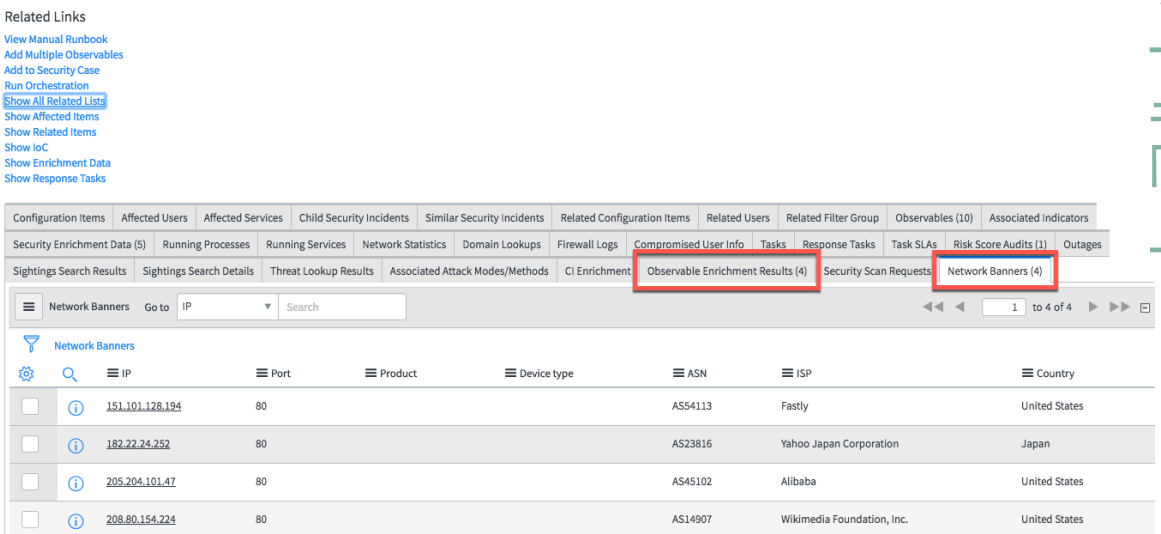
1. 작업 중인 보안 인시던트를 열고 조회가 성공적으로 실행되었는지 확인합니다.

애플리케이션이 구성되면 인시던트 생성 시 워크플로우가 자동으로 시작됩니다. 조회의 실행 및 완료 상태가 보안 인시던트의 작업 메모에 표시됩니다.

2. 자세한 내용은 작업 메모를 검토하고, 조회가 성공적으로 실행되었는지 확인할 수 없는 경우 진행 방법을 확인하십시오.

3. 보안 인시던트의 맨 아래로 이동하여 관련 링크에서 모든 관련 목록 표시 링크를 클릭합니다.

> **주:**
> 다음 단계의 그림은 시스템 설정에서 탭 양식 설정이 활성화된 상태로 표시됩니다. 탭 폼이 표시되지 않으면 배너 프레임의 오른쪽 위 모서리에서 설정 기어 아이콘을 클릭합니다. 표시되는 시스템 설정 대화 상자에서 폼을 클릭하고 탭 폼 및 폼 사용이 선택되어 있는지 확인합니다.



결과는 보안 인시던트 하단의 옵저버블 보강 결과 및 네트워크 배너 탭에 표시됩니다.

4. 네트워크 배너 탭을 선택하고 옵저버블 옆에 있는 파란색 정보 아이콘을 클릭합니다.

5. 표시되는 대화 상자에서 기록 열기 를 클릭하여 원시 데이터 및 자세한 내용을 봅니다.

Trouble?
옵저버블 보강 결과 및 네트워크 배너 탭에 결과가 표시되지 않으면 옵저버블이 통합에서 조회를 위해 지원되는 유형인지 확인합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

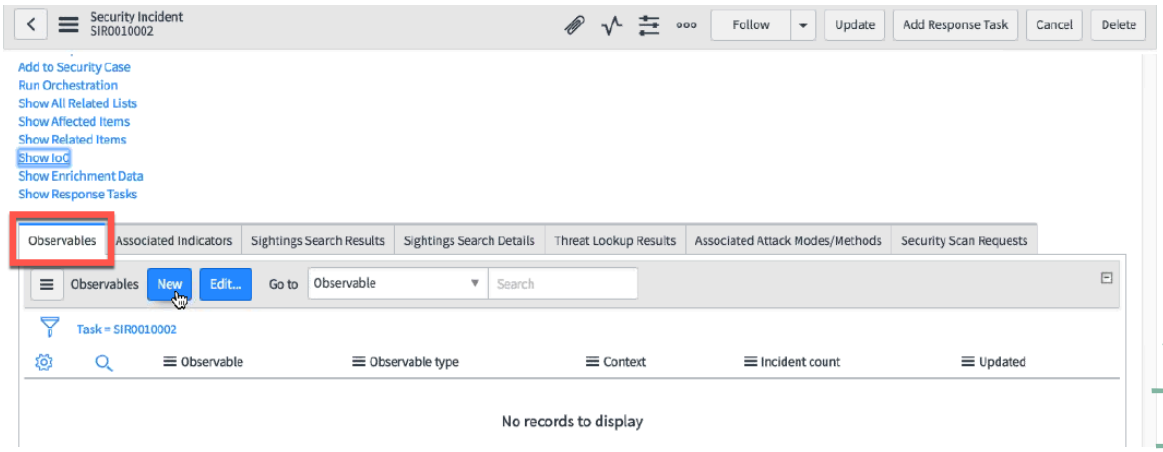
(선택 사항) 다음에 대한 옵저버블을 수동으로 첨부 **Shodan**

옵저버블을 보안 인시던트에 수동으로 연결할 수 있습니다. 초기 이벤트 트리거에서 보안 인시던트에 첨부되지 않은 옵저버블에 대해 위협 조회를 수행하려는 경우 옵저버블을 수동으로 연결합니다. 또한 관련 옵저버블에 대한 자세한 정보가 필요한 경우에도 이 작업을 수행할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.analyst

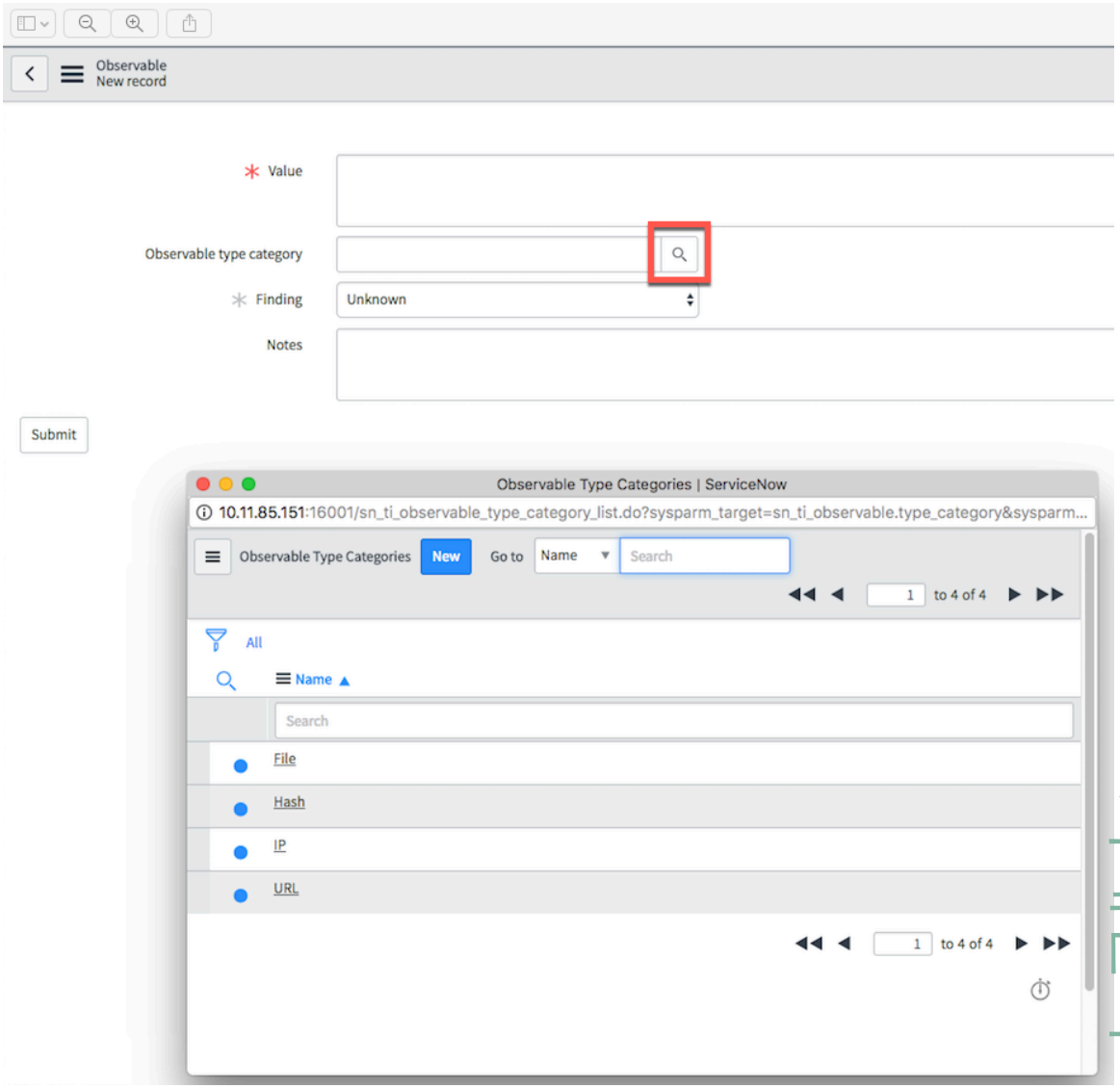
프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 인시던트 〉 모든 인시던트 표시 및 옵저버블을 연결할 보안 인시던트를 엽니다.
2. 기록 하단의 관련 링크에서 **IoC** 표시링크를 클릭합니다.



3. 옵저버블 탭에서 새로 만들기를 클릭합니다.
   옵저버블 양식이 표시됩니다.
4. 값 필드에 옵저버블(IP 주소 또는 URL)을 입력합니다.
5. 검색 아이콘을 클릭하고 옵저버블 유형 범주 대화 상자의 목록에서 원하는 옵저버블 유형을 클릭하여 필드를 채웁니다.

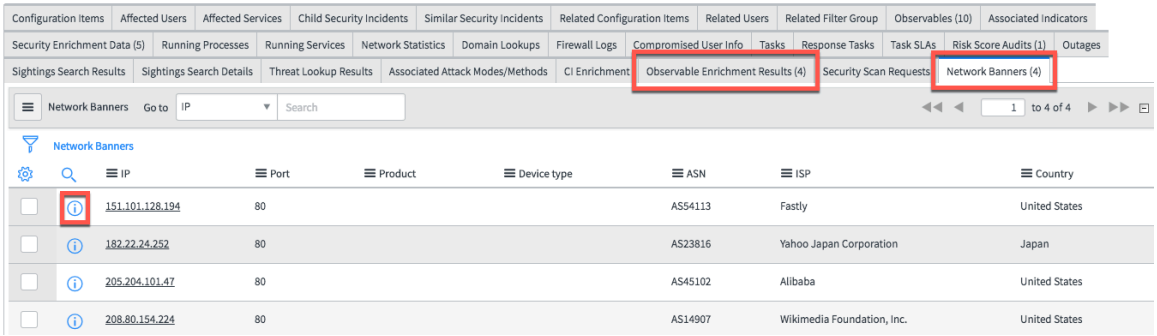
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



6. 제출을 클릭합니다.
   워크플로우가 시작되고 새 옵저버블이 있는지 확인합니다. 실행 및 완료 상태는 보안 인시던트 기록의 작업 메모 섹션에 표시됩니다.
7. 보안 인시던트로 이동하여 작업 메모를 검토합니다.

8. 기록 하단에서 모든 관련 목록 표시 관련 링크를 클릭합니다.
9. 결과를 보려면 옵저버블 보강 결과 또는 네트워크 배너 탭을 클릭하고, 특정 항목에 대한 자세한 내용을 보려면 옵저버블 옆에 있는 파란색 정보 아이콘을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



10. 표시되는 대화 상자에서 기록 열기 를 클릭하여 원시 데이터 및 자세한 정보를 봅니다.
11. 옵션: 검색 아이콘 근처의 파란색 설정 아이콘을 클릭하여 열 출력 및 순서를 개인화합니다.
12. 목록 개인화 열에서 사용 가능한 설정을 선택하고 선택된 열로 이동한 다음 확인을 클릭합니다.

Trouble?
조회가 성공적으로 실행되었는지 확인할 수 없는 경우 자세한 정보 및 진행 방법에 대해서는 작업 메모를 검토하십시오.

Secureworks CTP 티켓 수집 통합

Secureworks Counter Threat Platform 티켓 수집 통합을 사용하면 티켓을 자동으로 가져와서 Secureworks CTP 보안 인시던트로 변환하고 자동화된 응답 작업을 수행할 수 있습니다.

이 통합의 주요 기능은 다음과 같습니다.

- 미리 정의된 일정에 따라 선택한 티켓(첨부 파일 포함)의 자동 수집입니다.
- 티켓 및 이벤트 필드를 보안 인시던트 응답 필드에 매핑합니다.
- 티켓 필드에 매핑된 보안 인시던트의 미리 보기입니다.
- 티켓의 필터링 및 집계.
- 티켓과 연결된 이벤트의 요청 시 검색입니다.
- 티켓의 주요 업데이트를 정기적으로 추적합니다.
- SIR 인시던트 상태에 따라 티켓 업데이트 및 종결 자동화
- 마스터 티켓 업데이트.
- 작업 메모와 보안 인시던트 응답 Secureworks 작업 로그의 동기화.

ServiceNow AI Platform 티켓 수집 통합을 위한 **Secureworks CTP** 인스턴스 설정

다음 섹션에서는 에서 애플리케이션을 ServiceNow Store설치하기 전에 인스턴스에서 완료해야 ServiceNow AI Platform 하는 설정 작업을 나열합니다.

시작하기 전에
필요한 역할: sn_si.admin

이 태스크 정보
원활한 설치 및 구성을 위해 애플리케이션을 다운로드하고 설치하기 전에 다음 테이블을 참조하고 나열된 작업을 모두 완료했는지 확인하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설정 작업	설명
필수 ServiceNow AI Platform 및 보안 인시던트 응답 역할을 할당했는지 확인합니다.	인스턴스에서 통합을 ServiceNow AI Platform 설치, 설정 및 사용하려면 다음 역할이 필요합니다. • 관리자 역할(admin)을 가진 ServiceNow AI Platform 사용자는 에서 애플리케이션을 ServiceNow Store 설치하고 관리자(sn_si.admin) 역할을 할당합니다 SIR . • sn_si.admin 역할을 가진 사용자는 다음 ServiceNow AI Platform에서 다음 작업을 감독합니다. ◦ 프로파일의 이름을 지정하고, 만들고, 편집합니다. ◦ 티켓 필드를 선택하고 보안 인시던트 필드에 매핑 Secureworks CTP 합니다. ◦ 구성을 완료하기 전에 보안 인시던트 상세 정보가 정확한지 미리 봅니다. ◦ 진행 중인 티켓 수집을 예약합니다. ◦ SIR SIR 인시던트가 생성되고 종결될 때 티켓 업데이트를 활성화합니다. ◦ 보안 인시던트 분석가(sn_si.analyst) 역할을 할당합니다. ◦ sn_si.analyst 사용자는 보안 인시던트에 대한 작업을 수행합니다. 역할 및 사용자에게 역할을 할당하는 방법에 대한 자세한 내용은 다음을 참조하십시오. Managing roles
다음 버전을 사용하고 있는지 확인합니다. • Secureworks 티켓 API 4.0 • Secureworks 이벤트 API 1.0 • Secureworks 보강 API 1.0	포털에 대한 액세스 Secureworks CTP 권한이 있는 경우 이 통합에 필요한 API에 액세스할 수 있습니다. API에 필요한 다른 특수 설정은 없습니다.
ServiceNow 통합을 위해 애플리케이션을 설치하기 전에 통합을 지원하는 데 필요한 핵심 애플리케이션이 설치되고 활성화되었는지 확인합니다.	에서 ServiceNow Store다음 보안 운영 애플리케이션이 설치되고 활성화되는지 확인합니다. 설치되지 않은 경우 원활한 설치를 위해 다음 순서로 한 번에 하나의 애플리케이션을 설치하고 활성화합니다. **1.** 보안 인시던트 응답 **2.** 다음에 대한 보안 운영 이벤트 및 경보 수집(SIEM 통합에 필요): 이 애플리케이션에는 다음이 필요합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설정 작업	설명
	○ com.glide.hub.integration.runtime => ServiceNow 통합 허브 런타임 ○ com.glide.hub.action_step.rest => ServiceNow 통합 허브 작업 단계 - REST 주: 통합 허브 구성요소는 이벤트 및 경보 수집 플러그인과 함께 설치됩니다. 설치되지 않은 경우 고객 지원에 문의하여 도움을 받으십시오. 핵심 애플리케이션 설치에 보안 운영 대한 자세한 내용은 해당 애플리케이션 활성화 ServiceNow Store문서를 참조하십시오제품 또는 애플리케이션에 대한 보안 운영 권리 가져오기.

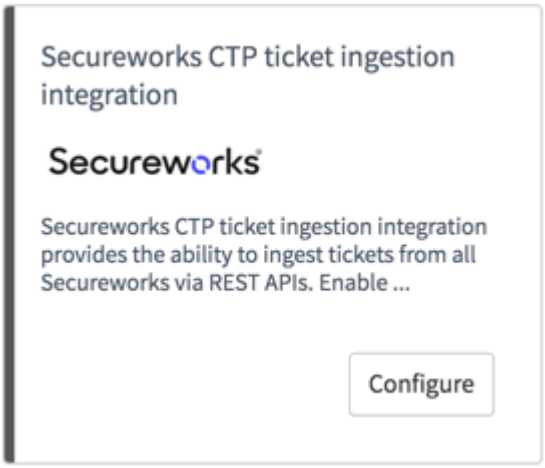
Secureworks CTP 티켓 수집 통합을 위한 애플리케이션 설치 및 구성 **ServiceNow**

인스턴스에서 통합을 ServiceNow AI Platform 실행하기 전에 다음 설치 및 구성 단계를 완료하여 애플리케이션이 인스턴스의 및 보안 운영 제품과 ServiceNow AI Platform 제대로 통합 보안 인시던트 응답 되도록 합니다.

시작하기 전에
필요한 역할: sn_si.admin

프로시저

1. 통합용 에서 티켓 애플리케이션을 ServiceNow Store 설치하지 Secureworks CTP 않은 경우 를 참조 보안 운영 통합 설치 하고 단계에 따라 설치합니다.
2. 애플리케이션을 성공적으로 설치한 후 통합 〉 통합 구성 티켓 수집 통합 타일을 Secureworks CTP 찾습니다.



3. 애플리케이션을 구성하려면 새로 만들기를 클릭합니다.
4. 또는 구성 단추가 타일에 표시되면 클릭하여 기존 구성을 편집합니다.
5. 표시되는 대화 상자에서 필드에 내용을 입력합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

6. 제출을 클릭합니다.
   성공적으로 확인 및 제출되면 각 구성이 보안 통합 페이지에 타일로 저장됩니다.

결과
저장된 구성 타일이 보안 통합 페이지에 표시되지 않는 경우. 페이지 오른쪽 상단 모서리에 있는 구성 선택 표시 목록에서 예를 클릭합니다.

Secureworks CTP 티켓 수집 통합을 위한 프로파일 생성

인스턴스에 프로파일을 ServiceNow AI Platform 생성하고 수집해야 하는 티켓과 보안 인시던트를 생성하는 데 사용할 티켓을 결정합니다. 수집된 티켓에서 보안 인시던트가 생성되기 전에 티켓의 필드 값이 보안 인시던트의 ServiceNow AI Platform 레이아웃에 표시되므로 실제 보안 인시던트가 표시되는 방식을 미리 볼 수 있습니다.

통합을 통해 인스턴스 환경에서 구성하는 보안 운영 프로파일을 기반으로 티켓을 수집할 수 있습니다. 모든 티켓은 처음에 프로필에서 구성된 티켓 유형에 대해 수집됩니다. 그런 다음 수집된 티켓을 추가로 필터링하여 보안 인시던트를 생성하는 티켓을 지정할 수 있습니다.

예를 들어 고위험으로 식별된 티켓에 대해서만 보안 인시던트를 생성하는 필터를 선호할 수 있습니다. 프로필이 활성화되고 수집된 티켓에서 보안 인시던트를 생성하기 전에 티켓의 개별 필드 값이 미리 보기를 위해 보안 인시던트 레이아웃의 해당 필드에 매핑됩니다.

프로파일의 소스 식별

프로파일의 이름과 소스를 지정합니다.

시작하기 전에
필요한 역할: sn_si.admin

프로시저

1. 인스턴스에서 티켓 ServiceNow AI Platform 에 대한 프로필을 만들려면 다음으로 이동합니다. **Secureworks** 티켓 수집 통합 〉 **Secureworks** 프로파일.
2. 새로 만들기를 클릭합니다.
3. 필드에 내용을 입력합니다.

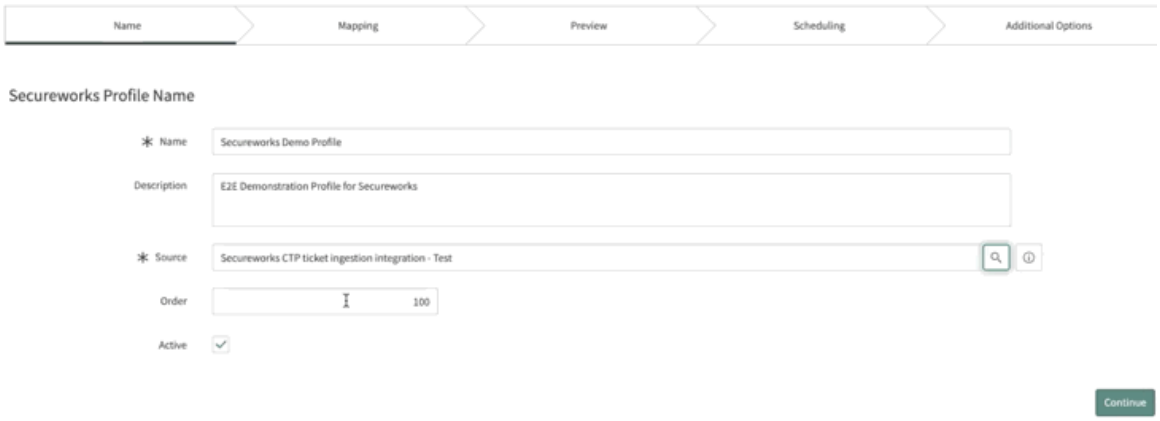
   완료된 양식의 예가 테이블 다음에 나옵니다.

필드	설명
이름	프로파일의 고유한 이름입니다. 이름이 고유하지 않으면 오류가 표시되고 중복된 프로파일 이름은 저장되지 않습니다. 인스턴스의 프로파일 이름은 ServiceNow AI Platform 고유해야 합니다.
소스	데이터를 수집할 소스를 선택합니다.
순서	기본값은 100입니다. 여러 프로필을 만든 경우 둘 이상의 프로필이 동일한 트리거 조건을 공유할 때 이 값은 런타임 실행 우선 순위를 제공합니다. 순서 값이 낮을수록 우선순위가 높습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
활성	이 옵션은 기본적으로 선택이 취소되어 있습니다. 이 옵션을 사용하지 않도록 설정하면 프로파일이 활성화되지 않습니다. 주: 프로파일을 활성화하기 전에 프로파일의 모든 섹션을 완료해야 합니다.

다음 그림은 완성된 폼의 예입니다.



다음에 수행할 작업
티켓 필드를 매핑합니다.

SecureWorks CTP 통합을 위한 티켓 필드 매핑

티켓 및 이벤트 필드를 보안 인시던트 양식의 필드에 매핑합니다.

매핑 단계에서는 먼저 샘플 티켓을 수집한 다음 모든 관련 티켓 필드가 양식의 적절한 위치에 보안 인시던트 응답 매핑되는지 확인한 다음 미리 보기 섹션에서 보안 인시던트를 시각화해야 합니다.

샘플 티켓 필드의 매핑에는 다음이 포함됩니다.

- 샘플 데이터 가져오기 및 채우기: 다음을 참조하십시오. 샘플 Secureworks 티켓 수집
- 티켓 필드를 보안 인시던트에 매핑: 자세한 내용을 참조하십시오. 보안 인시던트 응답 필드에 Secureworks 티켓 필드 매핑

샘플 Secureworks 티켓 수집

수집할 샘플 티켓을 선택합니다.

시작하기 전에
필요한 역할: sn_si.admin

프로시저

1. 매핑 양식이 표시되지 않으면 진행률 표시줄에서 매핑 을 클릭합니다.
2. 가장 최근의 샘플 티켓 5개를 가져오거나 매핑 환경에 사용하려는 특정 티켓에 대해 고유한 티켓 ID를 제공할 수 있습니다.
   수집 기본 설정 선택 목록에서 다음 중 하나를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 가장 최근 티켓 검색: 가장 최근 티켓 5개가 검색됩니다.
- 티켓 ID를 기준으로 티켓 선택: 검색할 티켓의 티켓 ID를 지정합니다. 쉼표로 구분된 티켓 ID를 최대 5개까지 지정할 수 있습니다.

3. 샘플 데이터 가져오기를 클릭하여 서버에서 최신 샘플 티켓 데이터를 Secureworks CTP 가져옵니다.
   샘플 티켓을 받는 데 몇 분 정도 걸릴 수 있습니다. 트랜잭션이 작동 중임을 나타내는 메시지가 화면 맨 위에 표시됩니다. 검색된 티켓은 개별 탭으로 표시됩니다. 티켓 데이터를 보려면 탭을 클릭하십시오. 각 티켓에 대해 티켓 필드와 해당 값 및 티켓을 트리거한 기여 이벤트의 상세 정보를 볼 수 있습니다.

   주:
   기여 이벤트의 상세 정보는 지난 7일 동안 발생한 경우에만 표시됩니다. 7일이 지난 이벤트는 표시되지 않습니다.

다음에 수행할 작업
샘플 데이터를 가져온 후 다음 단계는 티켓 필드를 보안 인시던트에 매핑하는 것입니다.

보안 인시던트 응답 필드에 **Secureworks** 티켓 필드 매핑

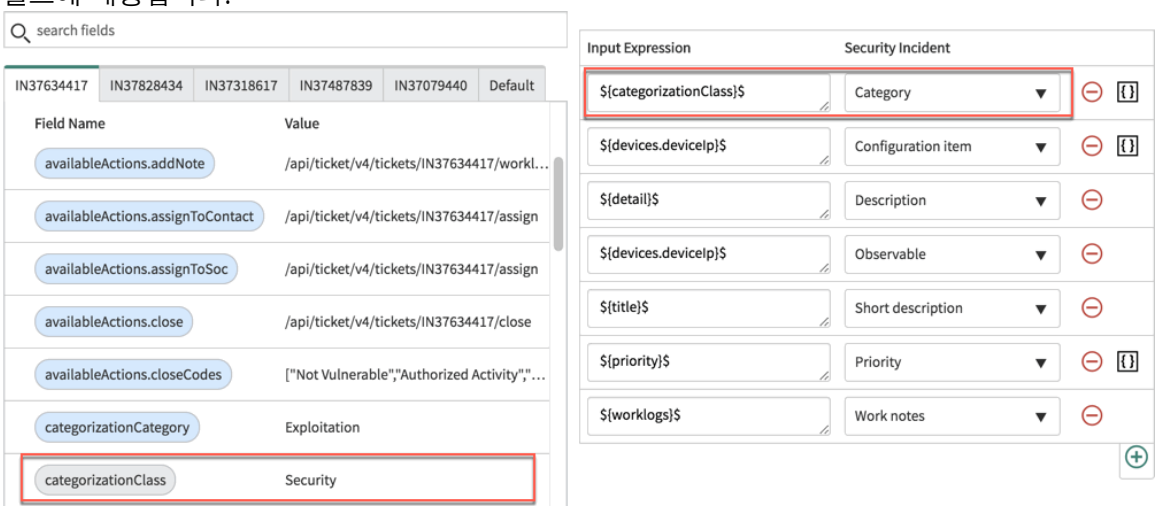
개별 티켓 또는 이벤트 필드를 보안 인시던트의 필드에 매핑합니다 ServiceNow AI Platform SIR .

티켓 필드 매핑

sn_si.admin 역할을 가진 사용자는 왼쪽에 있는 샘플 티켓 섹션의 필드를 사용하여 **SIR** 인시던트 필드 매핑 열의 보안 인시던트 필드에 매핑합니다. 티켓 또는 이벤트 필드를 왼쪽에서 끌어서 오른쪽의 SIR 인시던트 필드 매핑 섹션에 놓아 매핑 구성을 편집합니다. 오른쪽의 매핑은 수신 티켓 필드를 발신 보안 인시던트 필드와 연결합니다.

1. 양식 왼쪽의 필드 값을 양식 오른쪽에 있는 보안 인시던트의 필드에 매핑하려면 양식 왼쪽에 있는 파란색 필드 이름을 길게 클릭합니다.
2. 입력 식 열에 필드 이름을 수동으로 입력하거나 필드 이름을 끌어서 놓을 수 있습니다. 예를 들어 ### 입력하고 보안 인시던트 열의 필드 이름 옆에 있는 입력 식 열의 필드에 놓습니다.

   필드 값이 입력 식 열에 표시됩니다. 다음 이미지에서 categoryClass 는 보안 인시던트의 ## 필드에 매핑됩니다.



   주:
   입력 식 섹션에 이벤트 필드 이름을 수동으로 입력하는 경우 매핑되는 필드 이름 앞에 #### *${Event:eventfield}$*로 추가해야 합니다.

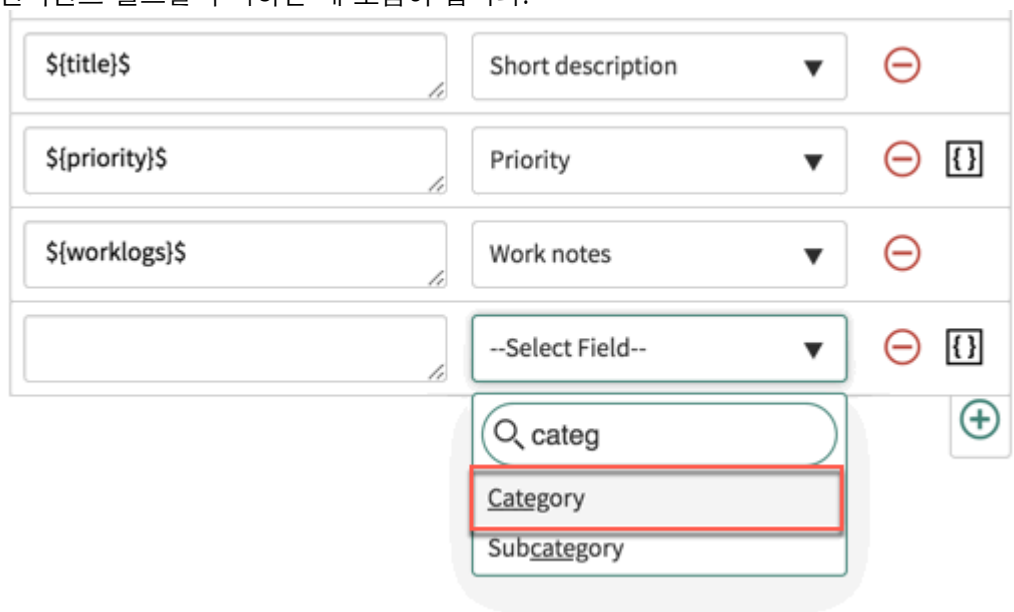
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

매핑 프로세스에서 티켓 또는 이벤트 필드가 간과되거나 중복되지 않도록 하기 위해 필드는 색으로 구분됩니다. 티켓 필드의 색상 코딩은 이미 매핑한 티켓 값이 회색으로 표시되고 나머지 매핑되지 않은 모든 필드는 파란색으로 나타날 때 티켓 값을 추적하는 데 도움이 됩니다. 이렇게 하면 보안 인시던트에 추가된 필드 값과 나머지 중요한 티켓 정보가 매핑되지 않은 상태로 남아 있는지 더 잘 시각화할 수 있습니다.

왼쪽의 연한 파란색 필드는 티켓 필드가 아직 선택되지 않았으며 보안 인시던트에 매핑되지 않았음을 나타냅니다. 수신 티켓 또는 이벤트 필드를 보안 인시던트의 둘 이상의 필드와 연결하는 것을 선호할 수 있습니다. 회색 필드는 필드가 선택되었고 보안 인시던트의 필드에 매핑되었음을 나타냅니다. 이 색상 코딩은 매핑을 추적하는 데 도움이 됩니다.

3. 양식 오른쪽의 보안 인시던트에 표시되는 기본 필드에 필드를 추가하려면 다음 단계를 따르십시오.
   a. 양식 오른쪽의 SIR 인시던트 필드 매핑 섹션 그리드 하단에서 더하기(+) 아이콘을 클릭합니다. 새 필드가 표시됩니다.
   b. 보안 인시던트 열에서 표시되는 선택 목록을 확장하고 필드를 선택합니다.

      새 필드의 확장된 선택 목록에서 일부 필드는 음영 처리됩니다. 다음 그림에서 범주는 보안 인시던트에 매핑되었기 때문에 회색 배경입니다. 양식 왼쪽에 있는 티켓 필드의 색상 코딩과 마찬가지로 오른쪽에 있는 보안 인시던트 필드에 대한 이 색상 코딩은 이미 매핑 SIR 된 인시던트 필드를 추적하는 데 도움이 됩니다.



> **주:**
> 동일한 보안 인시던트에 여러 옵저버블을 표시할 수 있으므로 옵저버블 필드를 서로 다른 값으로 여러 번 매핑할 수 있습니다. 마찬가지로 구성 항목 및 작업 메모 필드는 여러 값을 지원합니다. 여러 값을 지원할 수 없는 필드에 두 값을 매핑하려고 하면 인시던트를 미리 볼 때 필드에 값이 없다는 오류 메시지가 표시됩니다. 마찬가지로 보안 인시던트의 필드에 여러 옵션을 선택할 수 있는 선택 목록이 있고 선택 목록에 표시되지 않는 해당 필드에 옵션을 매핑하려고 하면 보안 인시던트에 필드가 채워지지 않습니다.

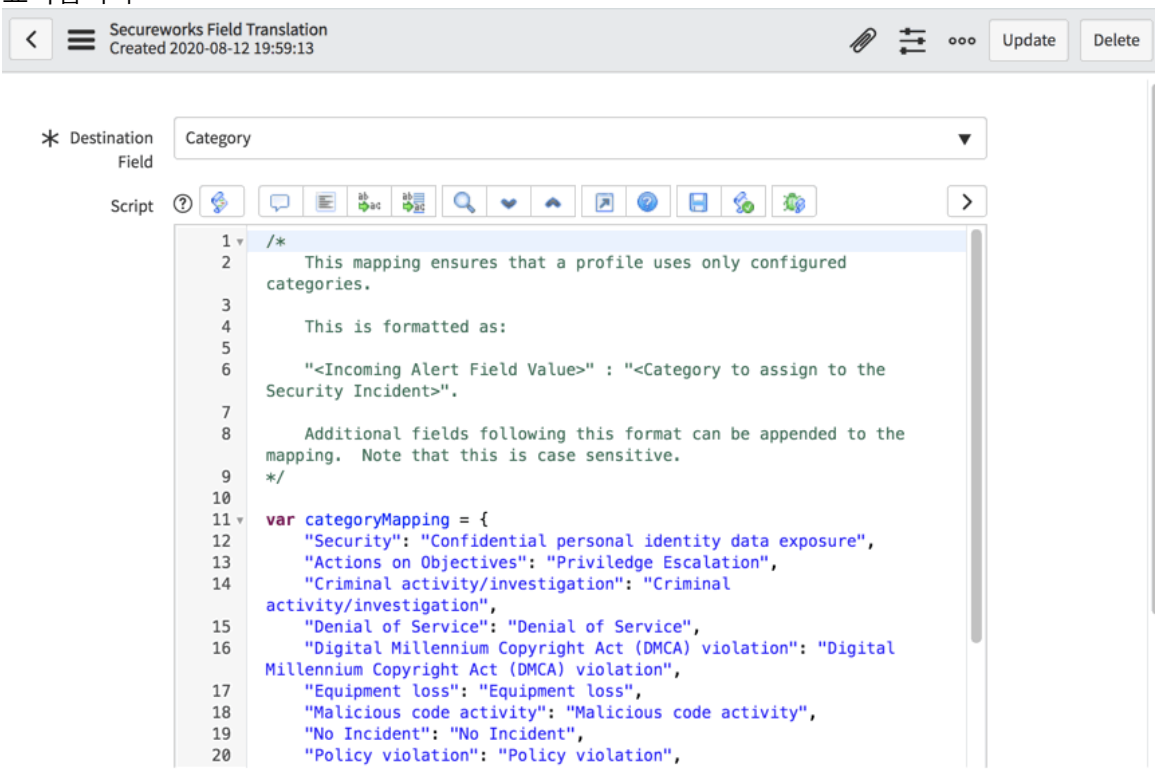
   c. 또는 새 행의 검색 필드에 값을 입력합니다.
   d. 양식 왼쪽에서 티켓 필드를 선택하여 오른쪽의 적절한 보안 인시던트 필드에 끌어서 놓습니다.
4. SIR 인시던트 필드 매핑 섹션의 필드 이름 옆에 있는 - 아이콘을 사용하여 필드를 제거합니다.
5. 매핑에 필드 값을 추가하거나 제거하여 매핑을 계속합니다.

필드 형식 변환

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

경우에 따라 티켓 필드가 보안 인시던트의 SIR 필드로 직접 변환되지 않을 수 있습니다. 이러한 값의 경우 스크립트 편집기를 사용하여 매핑 단계 중에 보안 인시던트의 필드 값에 대한 형식을 지정할 수 있습니다. 비슷하지만 동일하지는 않은 값의 형식을 지정하려면 스크립트 편집기를 사용하십시오. 예를 들어 스크립트 편집기를 사용하면 맬웨어 경보 및 바이러스 감염의 범주 값이 소스 범주에 대해 다를 수 있지만 두 값 모두 필드 번역 서식 지정 기능을 사용하여 보안 인시던트의 SIR 범주 필드에서 공통 악성 코드 활동으로 변환할 수 있습니다.

스크립트 편집기를 사용하려면 범주 필드 옆의 {} 아이콘을 클릭합니다. 스크립트 편집기가 표시됩니다



.

스크립트에 대한 변경 내용을 입력하고 업데이트를 클릭하여 변경 내용을 저장하고 매핑 페이지로 돌아갑니다.

인시던트 생성 조건

매핑 섹션이 완료되면 필터 조건을 설정하여 보안 인시던트를 생성해야 하는 티켓과 필터링해야 하는 티켓(예: 우선순위가 낮은 티켓)을 지정할 수 있습니다. 인시던트 생성 조건 작성기에서 동일한 필드 값을 사용하여 수신 티켓이 충족해야 보안 인시던트를 생성할 수 있는 추가 기준을 정의할 수 있습니다. 인시던트 생성 조건을 설정하려면 다음 단계를 수행합니다.

1. 양식에서 인시던트 생성 조건 섹션으로 스크롤하고 조건을 기준으로 필터링 확인란을 선택하여 옵션을 활성화합니다.

   필터 조건 작성기가 표시됩니다. 이러한 필터를 사용하여 필드에 설명된 특정 조건과 일치하는 보안 인시던트를 생성합니다.

   필터 조건 작성기의 첫 번째 필드에 대한 선택 목록의 옵션은 수집된 티켓의 샘플 티켓 수집 섹션에 표시되는 필드와 일치합니다. 이러한 필드는 동적이며 수집하는 티켓에 따라 변경됩니다. 입력하는 기준은 대소문자를 구분하며 티켓 값과 Secureworks CTP 정확히 일치해야 합니다. 필터 필드에 입력할 값을 잘 모르는 경우에는 콘솔로 돌아가서 Secureworks CTP 티켓에서 키워드를 검토하는 것이 좋습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
##, *##*, *## ##*, *###*, *availableactions* 및 *closeCodes* 티켓 필드에는 여러 값이 있을 수 있습니다(값이 배열에 저장됨). 필터 조건은 문자열만 검색할 수 있으므로 데이터가 올바르게 필터링되도록 이러한 필드에 *## Contains* 필터 조건을 사용해야 합니다.

2. 조건 작성기의 선택 목록과 필드를 사용하여 첫 번째 행에 대한 필터를 설정합니다.
3. 조건을 더 추가하려면 필드 오른쪽에서 AND 또는 **OR**을 클릭합니다.
   - **AND**를 선택하면 모든 조건이 일치해야 합니다.
   - **OR**을 선택하면 두 조건을 일치시킬 수 있습니다.
4. (선택 사항) 두 번째 행에서 두 번째 필터 조건을 설정합니다.

이러한 유형의 인시던트 생성 조건 필터링을 사용하면 티켓 범위를 좁히고 기본 규칙이나 필터를 수정하지 않고도 생성하는 불필요한 보안 인시던트 수를 제한할 수 있습니다. 추가 필터링 기준이 설정되면 모든 기준과 일치하는 티켓만 보안 인시던트에 매핑됩니다.

유사한 티켓을 처리하고 중복 인시던트를 방지하기 위한 티켓 집계 기준

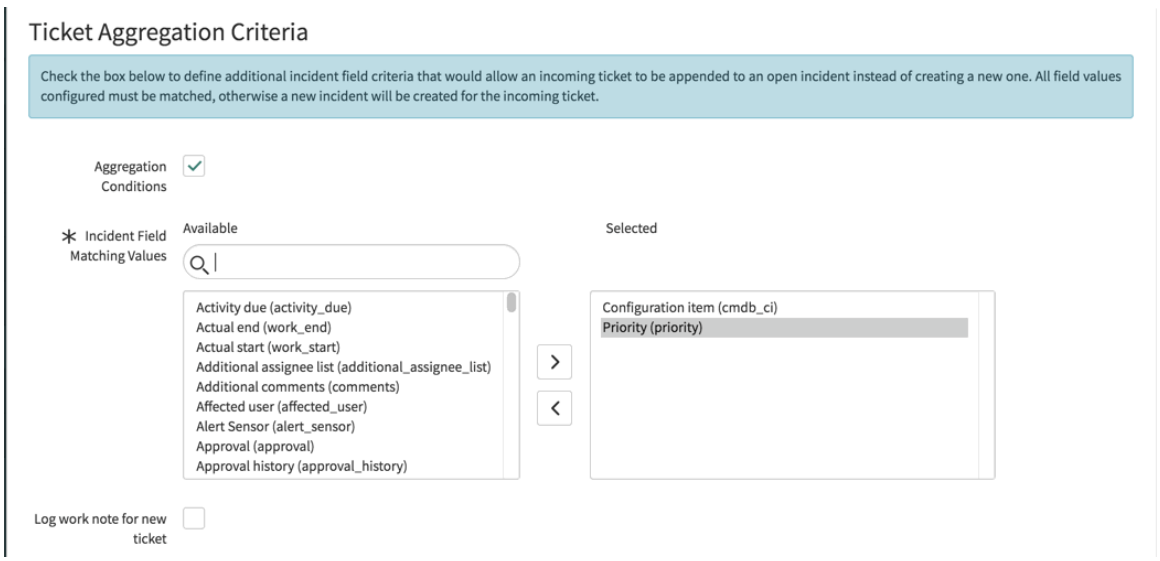
중복될 가능성이 있는 유사한 인시던트를 생성하는 대신 수신 티켓을 기존 SIR 보안 인시던트로 집계하는 추가 티켓 집계 기준을 정의합니다. 각 프로파일에 대해 필드 일치 값 기준을 사용하는 이 추가 집계 기능은 모든 관련 티켓 데이터를 단일 보안 인시던트에 배치함으로써 활성 상태의 중복 보안 인시던트 수를 줄일 수 있습니다. 기준을 설정하려면 다음 단계를 수행합니다.

1. 양식의 티켓 집계 기준 섹션으로 스크롤한 다음 집계 조건 확인란을 선택하여 이 옵션을 활성화합니다.

   인시던트 필드 일치 값 열이 표시됩니다. 이러한 필드 이름은 보안 인시던트에 구성된 SIR 사용자 지정 필드를 포함하는 보안 인시던트의 필드입니다.

2. 사용 가능 목록에서 NOW Platform의 기존 보안 인시던트와 일치시킬 필드 값을 선택하고 선택됨 목록으로 이동합니다.

   이 수신 티켓을 기존 보안 인시던트에 추가하려면 선택하는 모든 필드 값이 일치해야 합니다. 여기에는 옵저버블 및 구성 항목과 같이 여러 티켓 필드 값이 매핑될 수 있는 필드가 포함됩니다. 모든 값이 일치해야 합니다. 값의 하위 집합만 일치하면 티켓 집계 조건이 충족되지 않고 새 보안 인시던트가 생성됩니다. 다중 값 필드 매핑에 대한 아래 스크린샷을 참조하십시오.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

새 티켓이 매핑 단계의 집계 필드 조건에서 선택된 모든 값과 일치하면 새 티켓이 동일한 필드 값으로 가장 최근에 열린 보안 인시던트에 자동으로 추가됩니다. 보안 인시던트를 담당하는 sn_si.analyst 역할을 가진 사용자는 보안 인시던트의 관련 목록에서 추가된 모든 집계 티켓을 볼 수 있습니다. 이 목록에는 관련 타임 스탬프 및 집계된 필드 값이 자세히 설명되어 있습니다. 이 정보는 이러한 티켓이 기존 보안 인시던트로 집계되는 이유를 이해하는 데 도움이 됩니다. 이 탭이 보안 인시던트에 표시되지 않으면 관련 링크 아래의 기록 왼쪽으로 스크롤하여 모든 관련 목록 표시 링크를 클릭합니다.

> **주:**
> 기본 시스템에서는 Secureworks 집계 티켓 관련 목록을 사용할 수 없습니다. 관련 목록 레이아웃을 구성하고 다른 관련 목록과 함께 명시적으로 포함해야 합니다.

3. (선택 사항) 보안 인시던트에 최근에 추가된 새 티켓에 대한 작업 메모를 기록하려면 이 옵션을 활성화하는 확인란을 선택합니다. 작업 메모는 티켓 상세 정보 및 매핑 섹션의 작업 메모 필드에 추가되었을 수 있는 기타 세부 정보에 대한 링크와 함께 새 티켓이 추가되었음을 기록합니다.

   티켓의 Secureworks CTP 값을 보안 인시던트의 필드에 매핑했습니다. 또한 인시던트 생성 필터링 기준을 사용하여 보안 인시던트 생성을 제한하는 추가 조건을 구성했습니다. 또한 티켓 필드 값이 구성된 집계 기준과 일치할 때 기존 보안 인시던트에 티켓을 추가했습니다.

4. 계속을 클릭하여 프로파일 구성을 계속합니다. 다음 단계는 보안 인시던트에서 SIR 매핑한 필드를 미리 보는 것입니다

보안 인시던트에서 매핑된 값 미리 보기

매핑 단계를 완료한 후 보안 인시던트에서 SIR 매핑한 값을 미리 봅니다. 이 미리 보기 단계를 사용하면 보안 인시던트에 표시하려는 모든 티켓 필드를 매핑했는지 확인할 수 있습니다.

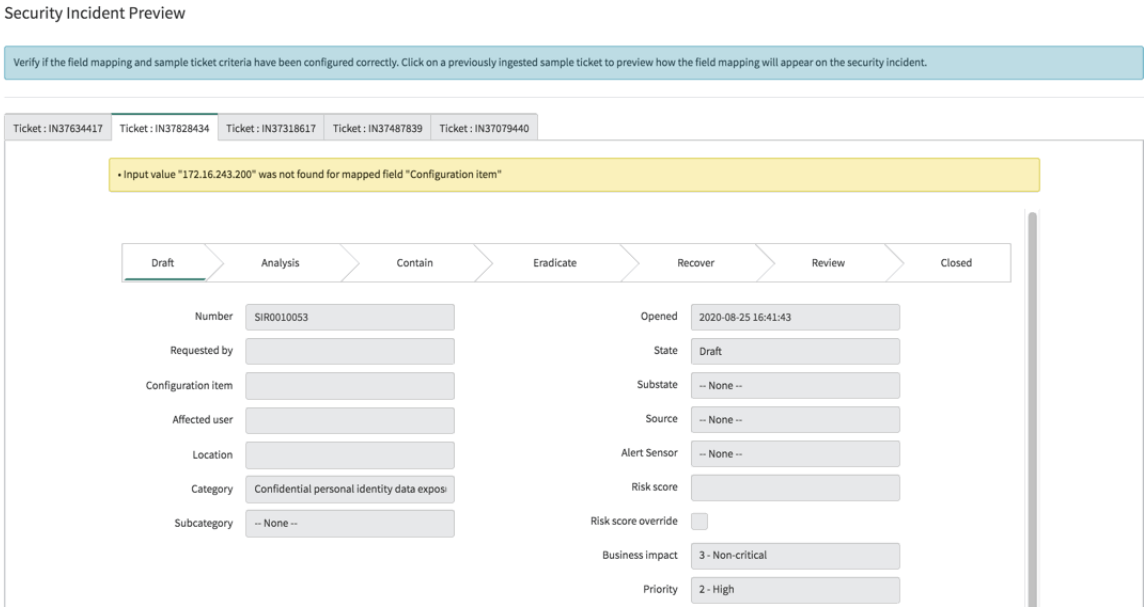
시작하기 전에
필요한 역할: sn_si.admin

이 태스크 정보
보안 인시던트를 미리 보고 필요에 따라 매핑을 다시 편집하여 오류가 있는 필드를 수정하거나 누락된 데이터를 채웁니다. 미리 보기가 성공적으로 완료되지 않으면 예약 단계로 진행할 수 없습니다. SIR 보안 인시던트 미리 보기는 보안 인시던트 응답 제품에 실제 인시던트로 저장되지 않습니다.

프로시저

1. 보안 인시던트 미리 보기가 표시되지 않으면 진행률 표시줄에서 미리 보기를 클릭합니다. 티켓은 탭으로 표시됩니다.
2. 탭을 클릭하여 보안 인시던트를 미리 봅니다.
   이 뷰는 읽기 전용 뷰이며 이 보안 인시던트의 기록은 저장되지 않습니다.
3. 보안 인시던트에서 티켓 값의 필드 매핑을 검토합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



앞의 이미지는 수집된 샘플의 매핑 오류가 있는 미리 보기의 예입니다.

4. 이 오류를 해결하려면 진행률 표시줄에서 매핑 을 클릭합니다.
5. 매핑을 편집하여 잘못된 값을 수정하거나 누락된 데이터를 채웁니다.
6. 매핑을 다시 미리 보고 오류 메시지에 설명된 오류를 계속 수정합니다.

다음에 수행할 작업

오류 메시지가 표시되지 않고 보안 인시던트의 필드 매핑에 만족하는 경우 일정을 정의합니다.

Secureworks CTP 티켓 수집 일정 정의

티켓 검색에 대한 기본 설정을 확인하거나 필요에 따라 일정을 수정합니다. 이 단계를 통해 날짜 범위와 폴링 간격을 기준으로 티켓 검색을 필터링할 수 있습니다.

시작하기 전에

필요한 역할: sn_si.admin

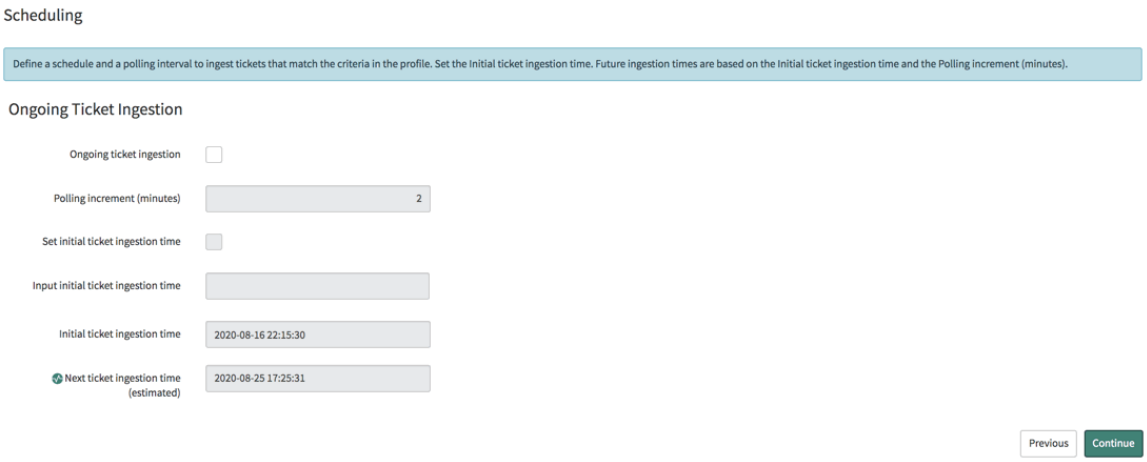
이 태스크 정보

티켓 프로필 구성과 일치하는 향후 티켓에 대해 폴링하는 빈도도 선택합니다. 프로파일별로 이러한 폴링 간격을 구성합니다. 일정을 예약할 때 시스템 부하와 인시던트 긴급도의 균형을 맞추는 것이 좋습니다. 모든 프로파일에 대해 1분 기본값이 설정되지만 인시던트의 긴급도와 시스템의 예상 로드에 따라 이 설정을 수정하는 것이 좋습니다.

프로시저

1. 진행률 표시줄에 스케줄링 페이지가 표시되지 않으면 스케줄링을 선택합니다.
2. 하나를 선택하여 포털에서 티켓을 가져오는 Secureworks CTP 방법과 시기를 예약합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



3. 계속을 클릭하여 추가 옵션 페이지로 이동합니다.

SIR 인시던트 상태에 따라 티켓 업데이트 및 종결 자동화

Secureworks CTP 티켓 수집 통합에는 두 티켓 모두 보안 인시던트를 생성할 수 있는 양방향 인터페이스가 있을 뿐만 아니라 보안 인시던트가 생성 및/또는 종료되면 보안 인시던트 번호, 할당 그룹, 보안 인시던트 URL 등과 같은 관련 인시던트 세부 정보로 티켓을 업데이트할 수 있는 기능이 있습니다.

시작하기 전에
필요한 역할: sn_si.admin

프로시저

1. 진행률 표시줄에 추가 옵션 페이지가 표시되지 않으면 추가 옵션을 선택합니다.
2. 보안 인시던트가 생성될 때 티켓을 업데이트하기 위한 구성을 완료합니다.

3. Finish(마침)를 클릭하여 구성을 완료하고 프로파일을 **Waiting** 상태로 이동합니다.
   확인 대화 상자가 표시됩니다. 프로파일을 성공적으로 설정했습니다. 이 프로파일을 활성화하여 일정에 따라 포털에서 티켓을 Secureworks CTP 끌어옵니다.

옵션: Secureworks CTP 프로파일 복사

새 프로파일을 생성하는 대신 기존 프로파일 및 관련 설정을 복사합니다. 여러 프로필을 만드는 경우 기존 프로필의 설정을 다시 사용하려면 프로필을 복사하여 시간을 절약할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.admin

이 태스크 정보
sn_si.admin 역할을 가진 사용자가 프로파일을 복사하는 경우 프로파일 중복을 방지하기 위해 프로파일 이름이 처음에 수정됩니다. 또한 복사된 프로파일이 비활성화(false)되므로 컨피그레이션을 완료하기 전에 실수로 활성화되지 않습니다. 이미 미리 보고 확인한 보안 인시던트에 대해 프로파일을 복사하고 기존 맵을 사용합니다.

프로시저

1. 다음으로 이동 모두 〉 **Secureworks** 티켓 수집 통합 〉 **Secureworks** 프로파일.
2. 표시되는 Secureworks 프로파일 목록에서 복사할 프로파일을 선택하고 선택한 행 선택 목록에 대한 조치 목록에서 복사를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로파일이 복사되어 목록에 표시됩니다. 복사본에는 매핑 및 일정 구성을 포함하여 원래 프로필의 모든 설정이 포함됩니다. 프로파일의 이름에는 (복사본)이 포함됩니다. 원본 프로파일이 활성화되었지만(true) 이 시점에서는 복사본이 비활성화됩니다(false). 복사된 프로파일의 값을 편집하고 필요에 따라 구성 설정이 새 프로파일에 적용되도록 이름을 바꿀 수 있습니다.

기존 프로파일에서 새 프로파일로 설정을 복사했습니다. 프로파일을 활성화해야 하므로 활성 열 상태가 false로 설정됩니다.

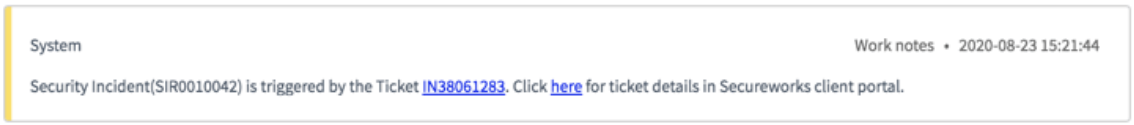
다음에 수행할 작업
구성 단계를 완료한 후 새 프로파일을 활성화(활성화)하라는 메시지가 표시됩니다.

티켓 수집 후 보안 인시던트 응답 양식 변경

티켓이 Secureworks CTP 수집되면 보안 인시던트가 생성되고 해당 업데이트가 보안 인시던트 기록에 적용됩니다.

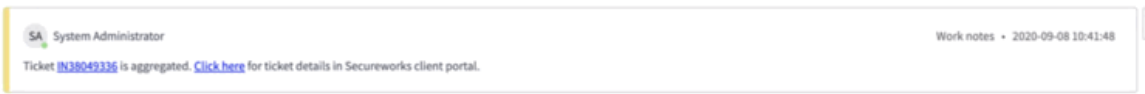
작업 메모

보안 인시던트를 트리거한 티켓의 상세 정보가 포함된 작업 메모가 게시됩니다.



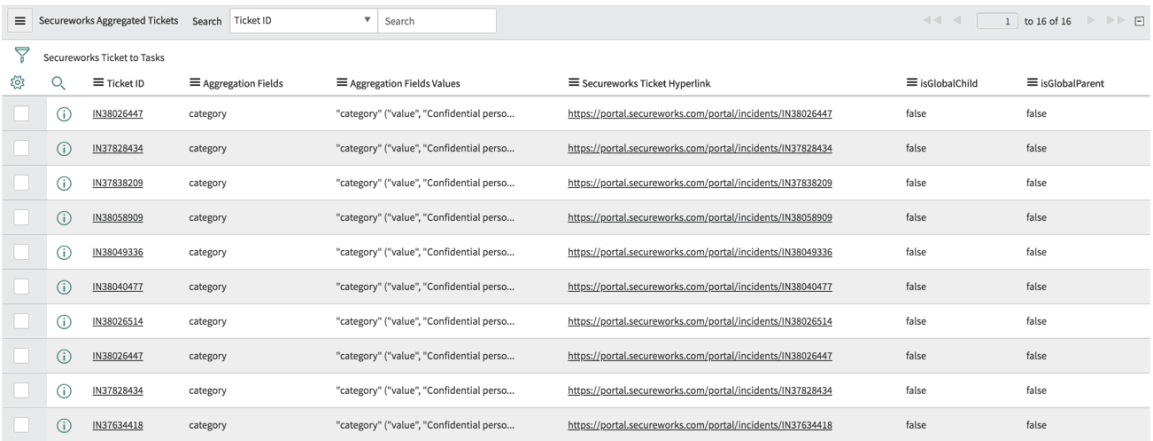
티켓 링크를 클릭하여 내부 Secureworks 작업에 대한 티켓 기록으로 이동합니다. 여기를 클릭 하이퍼링크는 티켓 상세 정보를 볼 수 있는 대시보드로 Secureworks CTP 이동합니다.

프로파일 생성: 매핑 페이지에 설명된 대로 티켓 집계 기준에서 새 티켓에 대한 작업 메모 기록 옵션을 선택한 경우 티켓이 집계될 때 작업 메모가 게시됩니다.



집계된 티켓

클릭 관련 목록 〉 **Secureworks** 집계 티켓 보안 인시던트에 대해 집계된 티켓을 보려면 티켓 하이퍼링크를 클릭하여 대시보드에서 Secureworks CTP 티켓을 봅니다.



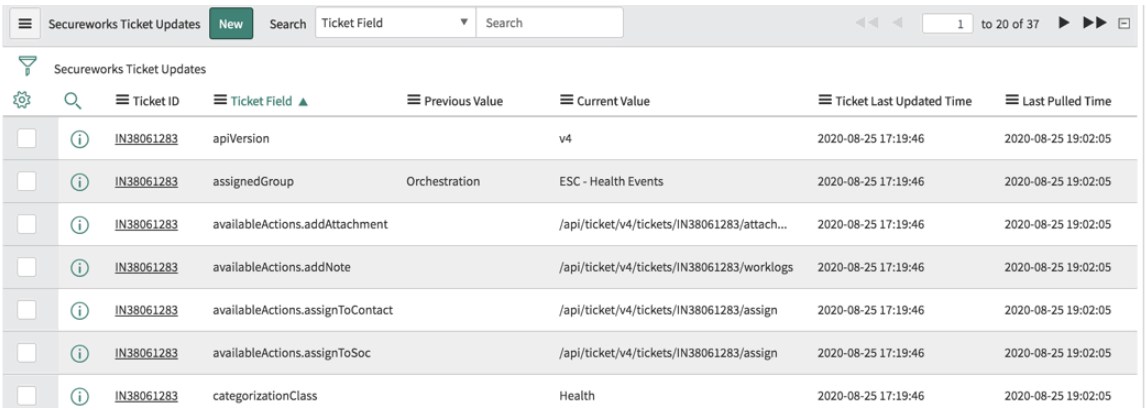
보안 인시던트 생성: 목록에서 티켓을 선택하고 작업 메뉴를 클릭한 다음 보안 인시던트 생성을 클릭합니다. 이 옵션은 티켓에 대한 새 보안 인시던트를 생성하고 이 티켓은 상위 보안 인시던트에서 세분화됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

티켓 기록 삭제: 목록에서 티켓을 선택하고 작업 메뉴를 클릭한 다음 삭제를 클릭합니다. 이 옵션은 티켓 기록을 삭제합니다.

Secureworks 티켓 업데이트

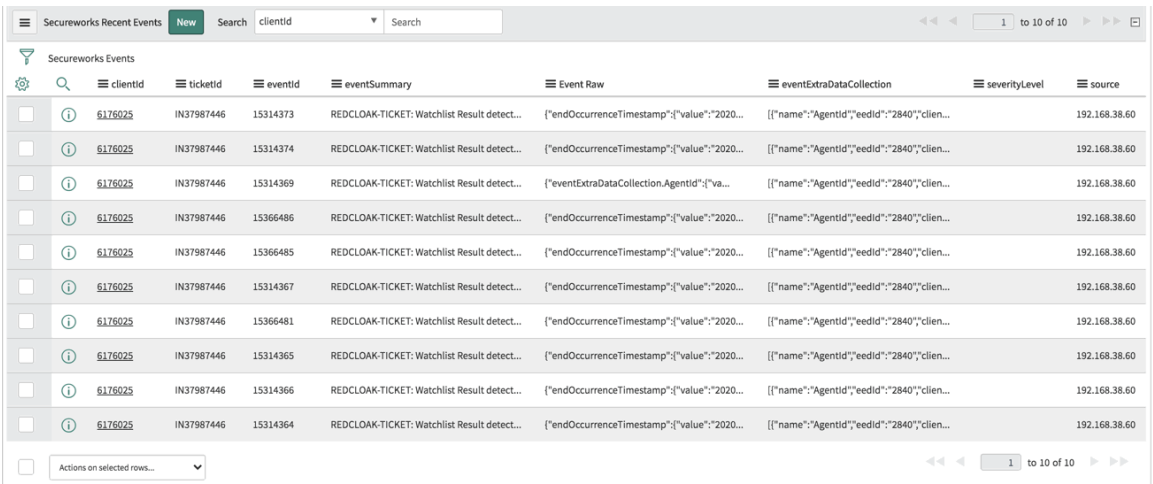
이것은 표준 티켓 필드를 표시하고 모든 폴링 간격 동안 티켓의 변경 내용을 추적합니다. 대시보드로 Secureworks CTP 이동하지 않고 티켓 업데이트를 직접 볼 수 있으므로 유용합니다. 값에 대한 변경 사항은 이전 값 및 현재 값 필드에 표시됩니다.



Ticket ID	Ticket Field	Previous Value	Current Value	Ticket Last Updated Time	Last Pulled Time
IN38061283	apiVersion		v4	2020-08-25 17:19:46	2020-08-25 19:02:05
IN38061283	assignedGroup	Orchestration	ESC - Health Events	2020-08-25 17:19:46	2020-08-25 19:02:05
IN38061283	availableActions.addAttachment		/api/ticket/v4/tickets/IN38061283/attach...	2020-08-25 17:19:46	2020-08-25 19:02:05
IN38061283	availableActions.addNote		/api/ticket/v4/tickets/IN38061283/worklogs	2020-08-25 17:19:46	2020-08-25 19:02:05
IN38061283	availableActions.assignToContact		/api/ticket/v4/tickets/IN38061283/assign	2020-08-25 17:19:46	2020-08-25 19:02:05
IN38061283	availableActions.assignToSoc		/api/ticket/v4/tickets/IN38061283/assign	2020-08-25 17:19:46	2020-08-25 19:02:05
IN38061283	categorizationClass		Health	2020-08-25 17:19:46	2020-08-25 19:02:05

Secureworks 최근 이벤트

관련 링크 아래에서 최근 **Secureworks** 이벤트 가져오기 옵션을 클릭하여 가장 최근의 Secureworks 이벤트를 봅니다.



clientId	ticketId	eventId	eventSummary	Event Raw	eventExtraDataCollection	severityLevel	source
6176025	IN37987446	15314373	REDCLOAK-TICKET: Watchlist Result detect...	{"endOccurrenceTimestamp":{"value":"2020...	[{"name":"AgentId","eedId":"2840","clien...		192.168.38.60
6176025	IN37987446	15314374	REDCLOAK-TICKET: Watchlist Result detect...	{"endOccurrenceTimestamp":{"value":"2020...	[{"name":"AgentId","eedId":"2840","clien...		192.168.38.60
6176025	IN37987446	15314369	REDCLOAK-TICKET: Watchlist Result detect...	{"eventExtraDataCollection.AgentId":{"va...	[{"name":"AgentId","eedId":"2840","clien...		192.168.38.60
6176025	IN37987446	15366486	REDCLOAK-TICKET: Watchlist Result detect...	{"endOccurrenceTimestamp":{"value":"2020...	[{"name":"AgentId","eedId":"2840","clien...		192.168.38.60
6176025	IN37987446	15366485	REDCLOAK-TICKET: Watchlist Result detect...	{"endOccurrenceTimestamp":{"value":"2020...	[{"name":"AgentId","eedId":"2840","clien...		192.168.38.60
6176025	IN37987446	15314367	REDCLOAK-TICKET: Watchlist Result detect...	{"endOccurrenceTimestamp":{"value":"2020...	[{"name":"AgentId","eedId":"2840","clien...		192.168.38.60
6176025	IN37987446	15366481	REDCLOAK-TICKET: Watchlist Result detect...	{"endOccurrenceTimestamp":{"value":"2020...	[{"name":"AgentId","eedId":"2840","clien...		192.168.38.60
6176025	IN37987446	15314365	REDCLOAK-TICKET: Watchlist Result detect...	{"endOccurrenceTimestamp":{"value":"2020...	[{"name":"AgentId","eedId":"2840","clien...		192.168.38.60
6176025	IN37987446	15314366	REDCLOAK-TICKET: Watchlist Result detect...	{"endOccurrenceTimestamp":{"value":"2020...	[{"name":"AgentId","eedId":"2840","clien...		192.168.38.60
6176025	IN37987446	15314364	REDCLOAK-TICKET: Watchlist Result detect...	{"endOccurrenceTimestamp":{"value":"2020...	[{"name":"AgentId","eedId":"2840","clien...		192.168.38.60

기본적으로 최대 50개의 이벤트가 표시됩니다. Secureworks 통합 설정에서 이 기본 설정을 수정할 수 있습니다.

Secureworks 티켓 및 해당 보안 인시던트를 봅니다

가져온 Secureworks CTP 티켓은 처음에 티켓 임포트 테이블에 저장됩니다. 필터 조건이 적용되기 전에 임포트된 모든 Secureworks CTP 티켓을 봅니다.

시작하기 전에
필요한 역할: sn_si.admin

프로시저

1. 다음으로 이동 모두 〉 **Secureworks** 티켓 수집 통합 〉 보안 티켓 임포트.
2. 집계되거나 필터 조건이 적용되기 전에 임포트한 모든 Secureworks CTP 티켓을 볼 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 티켓 ID를 클릭하면 원시 티켓 데이터를 볼 수 있습니다.
4. 다음으로 이동 **Secureworks** 티켓 수집 〉 작업에 대한 **Secureworks** 티켓.
   Secureworks CTP 해당 보안 인시던트가 있는 티켓이 표시됩니다.

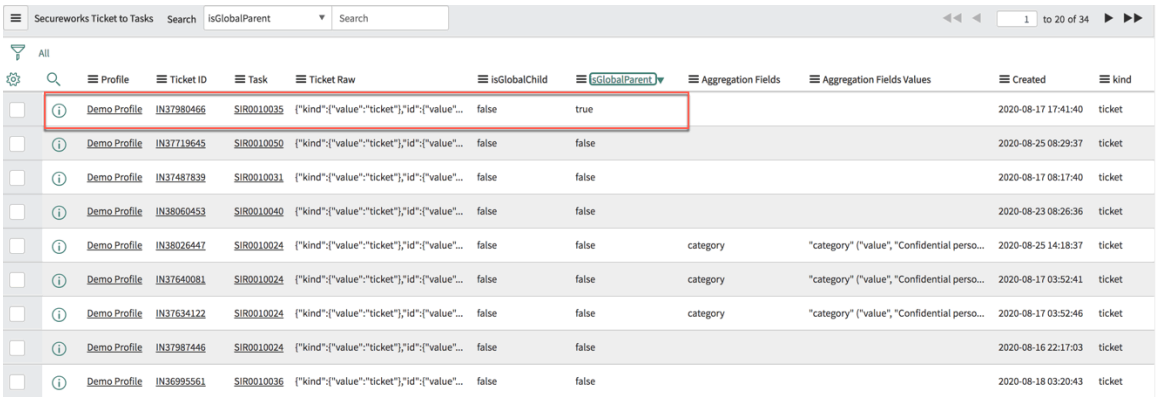
Secureworks CTP 마스터 티켓 종결 공지

마스터 티켓에 의해 Secureworks CTP 생성된 보안 인시던트를 종결하기 전에 마스터 티켓과 연결된 모든 하위 티켓이 종결되었는지 확인해야 합니다.

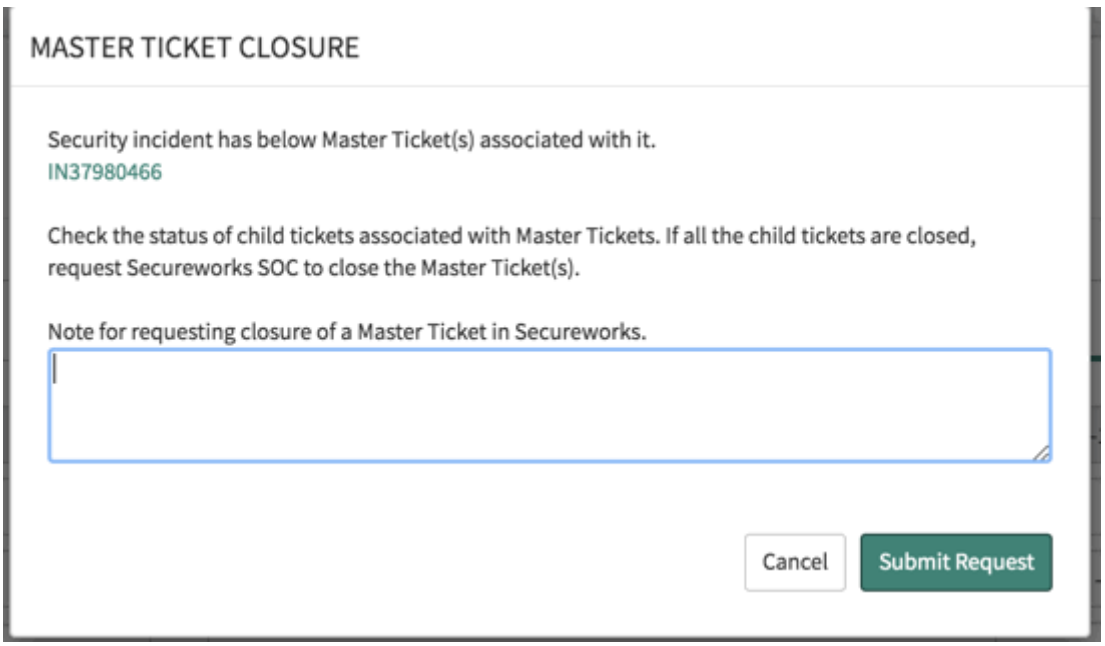
시작하기 전에
필요한 역할: sn_si.admin

프로시저

1. 다음으로 이동 모두 〉 **Secureworks** 티켓 수집 〉 작업에 대한 **Secureworks** 티켓.
   Secureworks CTP 해당 보안 인시던트가 있는 티켓이 표시됩니다.



2. **isGlobalParent** 필드가 예로 설정된 보안 인시던트를 클릭합니다**.**
3. 보안 인시던트 상태를 종결로 변경하고 종결 코드를 지정한 후 저장을 클릭합니다.
   다음과 같은 대화 상자가 표시됩니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 보안 인시던트는 Secureworks 마스터 티켓과 관련되어 있습니다. 마스터 티켓에는 하나 이상의 하위 티켓이 연결되어 있을 수 있습니다. 마스터 티켓을 종료하기 전에 먼저 이 마스터 티켓과 연결된 모든 하위 티켓이 종료되었는지 확인해야 합니다.

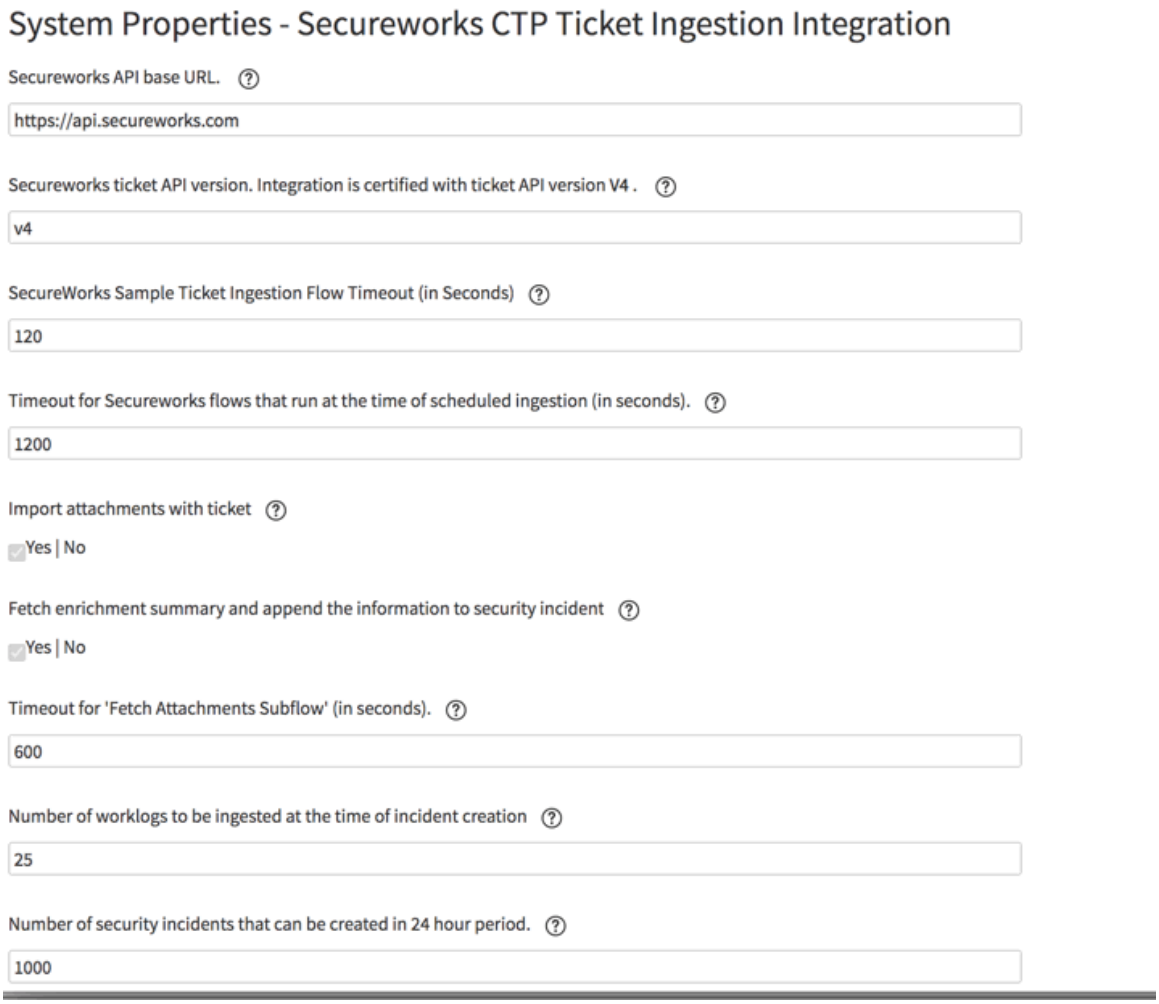
4. Secureworks에서 마스터 티켓의 종결을 요청하는 메모를 추가하고 요청 제출을 클릭합니다. 이제 마스터 티켓이 Secureworks SOC 팀에 재할당되었습니다.
5. 요청이 제출되면 보안 인시던트를 종결할 수 있습니다.
6. 다음으로 이동 애플리케이션 〉 모듈.

구성 설정

이 옵션을 사용하여 티켓 수집 통합 기본 시스템 속성을 수정합니다 Secureworks CTP .

시스템 속성을 수정하려면 *sn_si.admin* 역할의 사용자로 로그인하고 **Secureworks** 티켓 수집 통합 〉 **Secureworks** 통합 설정.

기본 구성 설정이 표시됩니다. 필요한 경우 이러한 설정을 수정할 수 있습니다.



수정된 통합 설정은 프로파일에 정의된 다음 폴링 간격 동안 적용됩니다.

Zscaler와의 **Security Incident Response** 통합

제품을 사용하여 Zscaler와의 Security Incident Response 통합Zscaler Internet Access 서버(ZIA) 로그를 ServiceNow AI Platform. 이 통합을 통해 대시보드를 보고, 사용자 지정 경보를 만들고, 보안 인시던트를 조사하는 데 도움을 줄 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

스토어에서 앱 요청

ServiceNow Store 웹 사이트를 방문하면 사용 가능한 모든 앱을 확인하고 스토어에 요청을 제출하는 방법에 대한 정보를 참조할 수 있습니다. 출시된 모든 앱의 누적 릴리스 정보는 ServiceNow Store 버전 기록 릴리스 정보를 참조하십시오.

개요

Zscaler 인터넷 및 웹 게이트웨이 제품은 클라우드에서 제공됩니다. 엔터프라이즈 보안 환경에 대한 주요 데이터 요소와 인사이트를 제공합니다. Zscaler와의 Security Incident Response 통합Zscaler Internet Access 제품을 ServiceNow AI Platform 인스턴스에 연결합니다. 에서 ServiceNow AI Platform제품을 사용하면 Zscaler 조직의 인터넷 사용에 대한 더 많은 인사이트를 얻을 수 있습니다.

통합의 주요 기능

이 통합에는 다음과 같은 주요 기능이 포함됩니다.

- 제품이 유지관리하는 전역 위협 라이브러리 대비 옵저버블의 평판 조회입니다 Zscaler .

  주:
  글로벌 위협 라이브러리에는 Zscaler 추세, 원산지 국가, 대상 대상, 볼륨 및 다양한 위협 범주별로 위협이 나열됩니다. 이 전역 위협 라이브러리를 사용하면 전역 위협 환경에 대한 옵저버블을 조사할 수 있습니다.

- 제품의 차단 목록 또는 허용 목록에서 옵저버블의 유지관리입니다 Zscaler .
- MD5 해시에 대해 제품에서 Zscaler 샌드박스 보고서를 가져오고 검토하는 기능입니다. 제품의 Cloud Sandbox 기능은 Zscaler 가상 환경에서 파일을 실행 및 분석하여 악성 행위를 탐지합니다.
- 사용자가 알 수 없는 악성 파일을 다운로드할 때 제품에서 Zscaler 생성되는 환자 0 이벤트의 보안 경보입니다.
- 제품에 정의된 Zscaler 대로 차단 목록 또는 허용 목록의 역할을 하는 여러 URL 범주 목록입니다.
- ServiceNow AI Platform 옵저버블이 추가되는 URL 범주를 식별하기 위해 태그를 지정할 수 있는 보안 인시던트입니다.
- 이전 항목을 자동으로 제거하여 URL 범주 목록 항목의 크기를 유지하는 만료 기간입니다.
- URL 범주 목록에서 옵저버블을 추가 및 제거하기 위한 승인 워크플로우입니다.
- 위협 인텔리전스 결과와 항목이 차단된 이유에 대한 세부 정보가 포함된 옵저버블 기록 및 보안 인시던트에 연결할 수 있는 URL 범주 항목입니다.

이 통합에 대해 알아보기

문서 식별자	문서 제목
Zscaler 제품 설명서 웹 사이트	ZScaler 제품 설명서 웹 사이트
ServiceNow 제품 설명서 웹 사이트	ServiceNow 제품 설명서 웹 사이트

Zscaler와의 **Security Incident Response** 통합 시작하기

인스턴스 및 보안 인시던트 응답 제품과 인터페이스 ServiceNow AI Platform 하도록 제품을 활성화하고 설정합니다Zscaler Internet Access.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

검사 목록

설정 작업	설명

필수 ServiceNow AI Platform 및 보안 인시던트 응답 역할을 할당하고 확인합니다.	다음 역할은 예상 결과를 구성하고 검증하는 데 필요합니다.
	• 관리자 역할은 에서 ServiceNow Store 통합을 설치하고 sn_si.admin 역할을 할당합니다.
	• sn_si.admin 역할은 다음 작업을 수행합니다.
	  ○ 통합을 구성합니다.
	  ○ URL 범주 목록을 작성, 활성화 및 제거합니다.
	  ○ sn_si.analyst 역할을 할당합니다.
	• sn_si.analyst 역할은 항목을 생성하고 보안 인시던트를 처리합니다.

이 통합을 구성하기 전에 핵심 애플리케이션이 설치되고 활성화되어 있는지 ServiceNow 확인합니다.	ServiceNow 통합 허브 엔터프라이즈 팩 설치 관리자 [com.glide.hub.integrations.enterprise] 플러그인이 필요합니다. 플러그인(com.snc.security_incident)이 보안 인시던트 응답 필요합니다. 이 플러그인은 제품에 대한 모든 의존성을 보안 인시던트 응답 자동으로 설치합니다. 통합을 위해 다른 보안 운영 애플리케이션을 설치하고 활성화하기 전에 이 플러그인을 설치하고 활성화합니다. 에서 ServiceNow Store다음 보안 운영 애플리케이션이 설치되고 활성화되는지 확인합니다. 이러한 애플리케이션이 아직 설치되어 있지 않으면 다음 순서대로 각 애플리케이션을 한 번에 하나씩 설치하고 활성화합니다. **1.** 보안 인시던트 응답 의존성(com.snc.si_dep) **2.** 보안 통합 프레임워크 **3.** Security Support Common **4.** 보안 지원 오케스트레이션 **5.** 위협 인텔리전스 공통 지원 **6.** Trusted Security Circles **7.** 보안 운영 설정 도우미 **8.** 보안 인시던트 응답

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

검사 목록

설정 작업	설명
Zscaler 버전을 확인합니다.	• 이 통합은 버전 1.0 이상에서 지원됩니다 Zscaler Internet Access . • 이 통합은 다음 Zscaler 버전에서 테스트됩니다. ◦ Windows용 Zscaler 클라이언트 커넥터 - 3.0 ◦ macOS용 Zscaler 클라이언트 커넥터 - 3.0 ◦ Linux용 Zscaler 클라이언트 커넥터 - 베타 ◦ Zscaler 클라우드 커넥터 - 6.1
필요한 Zscaler 권한이 있고 구성되었는지 확인 액세스 권한 Zscaler Internet Access API.	• 에 대한 Zscaler Internet Access관리자 자격 증명이 있어야 합니다. • 유효한 클라우드 서비스 API 구독이 있어야 합니다. Zscaler 지원팀에서 키를 제공해야 합니다. • 관리자 자격 증명(사용자 이름 및 암호)이 Zscaler Internet Access 있어야 합니다. API 인증은 API 키와 Zscaler Internet Access 관리자 자격 증명의 조합을 기반으로 합니다. 주: API 키 관리에 Zscaler Internet Access 대한 자세한 내용은 Zscaler 설명서를 참조하십시오.

API에 대한 **Zscaler Internet Access** 액세스 구성

인스턴스에 대한 액세스를 Zscaler Internet Access 구성하여 인스턴스와 Zscaler 서버 간의 ServiceNow AI Platform 보안 연결을 인증합니다.

시작하기 전에

필요한 역할: Zscaler Internet Access 관리자

이 태스크 정보

Zscaler 조직의 클라우드 서비스에 대한 API 구독을 사용하도록 설정하면 기본 URL을 사용하여 API 키 관리 페이지에서 사용할 수 Zscaler Internet Access 있습니다. 조직은 하나의 API 키 또는 토큰만 사용할 수 있습니다. 새 키 또는 토큰을 추가하기 전에 기존 키 또는 토큰을 삭제합니다.

API의 기준 URL은 ${Cloud_Name}/api/v1입니다. Zscaler 조직에 프로비저닝된 클라우드 이름을 확인하고 이를 사용하여 기본 URI에서 {Cloud_Name}을(를) 바꿉니다. 기본 URL의 몇 가지 예는 다음과 같습니다.

- example.zscalerbeta.net
- example.zscalerone.net
- example.zscalertwo.net

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- example.zscaler.net
- example.zscloud.net

주:
관리 포털에 대한 Zscaler Internet Access 자세한 내용은 Zscaler API 키 관리 설명서 및 Zscaler Portal 설명서를 참조하십시오.

프로시저

1. 관리 포털에 관리자로 Zscaler Internet Access 로그인합니다.
2. 다음으로 이동 관리 〉 클라우드 서비스 **API** 보안.
3. **API** 키 추가를 클릭합니다.
   API 키 추가 옵션이 표시되지 않으면 기존 키를 삭제합니다.
   새 API 키는 즉시 유효하며 탭에 표시됩니다.

결과
인스턴스에서 액세스를 Zscaler 구성할 기본 URL과 API 키를 검색했습니다 ServiceNow AI Platform .

Zscaler와의 **Security Incident Response** 통합 설치 및 구성

에서 ServiceNow Store 인터넷 액세스 제품을 설치하고 구성하여 Zscaler와의 Security Incident Response 통합 인스턴스에서 통합 ServiceNow AI Platform 사용을 시작합니다.

시작하기 전에
필요한 역할: sn_si.admin

프로시저

1. Zscaler와의 Security Incident Response 통합 에서 ServiceNow Store 제품을 다운로드하여 설치합니다.
2. 다음으로 이동 보안 운영 〉 통합 〉 통합 구성.
3. 타일을 Zscaler와의 Security Incident Response 통합 검색하고 구성 〉 새 구성 작성.
4. 양식에서 필드를 채웁니다.

Zscaler 구성 양식

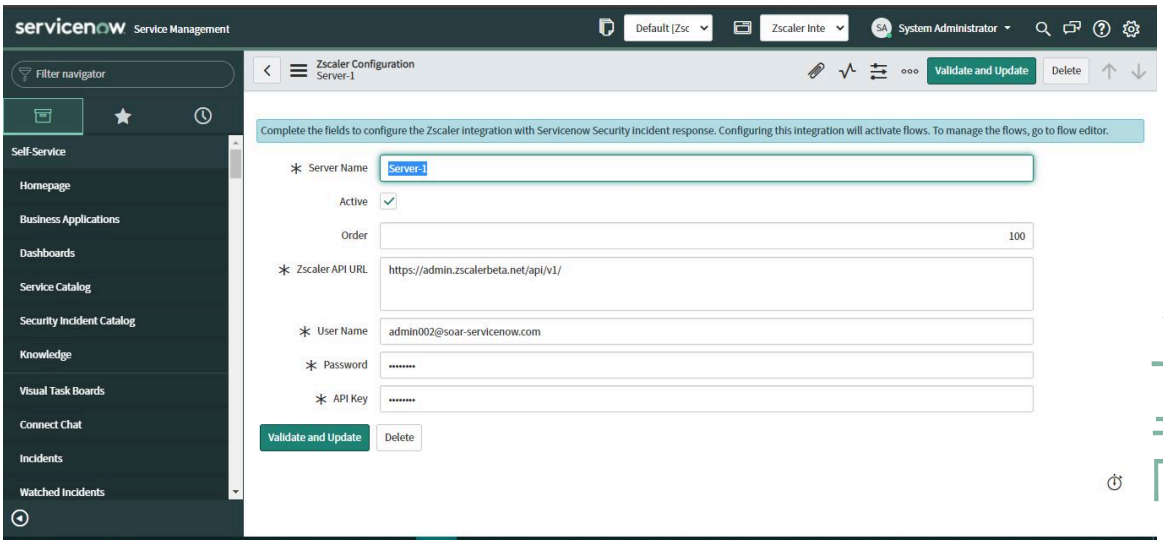
필드	설명
서버 이름	Zscaler 서버 이름입니다. 예: ZSserver.
활성	프로파일이 활성 상태임을 나타내는 표시기입니다.
순서	플로우 우선순위입니다. 이 필드의 값은 둘 이상의 프로파일이 트리거 조건을 공유할 때 워크플로우의 순서를 나타냅니다. 숫자가 가장 낮은 플로우의 우선순위가 가장 높습니다. 작업 순서를 설정하려면 값을 입력합니다. 예를 들어 100, 200, 300, 400입니다. 기본값은 100입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
Zscaler API URL	API를 호스팅하는 기본 URL입니다 Zscaler . 예를 들어 https://example.zscalerbeta.net
사용자 이름	관리자 계정의 사용자 이름입니다 Zscaler Internet Access .
암호	관리자 계정의 암호입니다 Zscaler Internet Access .
API 키	관리 포털에서 가져온 API 키입니다 Zscaler Internet Access .

다음 예는 Zscaler 구성 페이지를 보여줍니다.

Z스캘러 구성 페이지



5. Validate and Update(확인 및 업데이트)를 클릭합니다.

결과
이 구성을 확인하고 저장한 후 구성 페이지로 돌아갑니다 Zscaler .

URL 범주 목록 추가 Zscaler Internet Access

세분화된 필터링 및 정책 생성을 위해 쉽게 액세스할 수 있도록 인터넷 액세스 제품 ServiceNow AI Platform 에서 Zscaler 사용할 수 있는 URL 범주를 인스턴스에 추가하여 각 URL에 대한 작업을 지정합니다.

시작하기 전에
필요한 역할: sn_si.admin

이 태스크 정보
컨텐츠를 Zscaler와의 Security Incident Response 통합 필터링하는 데 도움이 되는 기본 허용 목록 및 거부 목록 URL 범주 목록을 제공합니다.

인스턴스에 추가하는 URL 범주는 ServiceNow AI Platform 이미 환경에 Zscaler Internet Access 있어야 합니다. 에서 URL 범주Zscaler를 생성하는 데 사용할 Zscaler와의 Security Incident Response 통합 수 없습니다.

주:
제품의 URL 범주 목록에 Zscaler 대한 자세한 내용은 URL 범주에 대한 Zscaler 설명서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 **ZScaler** 통합 〉 Z스캘러 **URL** 범주 목록.
2. 새로 만들기를 클릭합니다.
3. 양식에서 필드를 채웁니다.

Zscaler URL 범주 목록 양식

필드	설명
소스	서버 이름입니다. URL 범주 목록에서 이전에 구성한 Zscaler Internet Access 서버만 볼 수 있습니다.
활성	URL 범주 목록이 활성 상태임을 나타내는 표시기입니다.
URL 범주	소스를 선택한 후 활성화되는 필드입니다. 에서 Zscaler생성된 URL 범주 목록을 볼 수 있습니다.
만료 기간(일)	URL 범주 목록의 만료 기간입니다. 0(기본값)은 URL 범주 목록 항목이 만료되지 않음을 나타냅니다. 이 값을 변경하면 입력한 일수 동안 이 URL 범주에 추가된 모든 옵저버블이 활성화됩니다. 최솟값으로 1을 입력할 수 있습니다. 예를 들어, 만료 기간을 30일로 설정하면 30일 후에 범주 목록에서 항목이 제거됩니다.
태그 표시	보안 인시던트에 표시되는 보안 태그입니다 SIR . 태그 표시 옵션을 Zscaler 활성화하면 양식에서 옵저버블에 대한 태그 필드를 사용할 수 있습니다.
변경 요청 작성	URL 범주 목록에 첨부된 기록에 대한 인스턴스의 변경 요청 및 변경 작업 ServiceNow AI Platform 변경 요청 생성 옵션을 활성화하면 양식에서 변경 요청 필드를 사용할 수 있습니다.
승인 필요	승인자 그룹 목록입니다. 요청을 제출한 후 요청을 완료하려면 그룹의 승인이 필요합니다. 승인 필요 옵션을 활성화하면 옵저버블 추가를 위한 승인자와옵저버블 제거 승인자 필드를 양식에서 사용할 수 있습니다. ○ 옵저버블 추가를 위한 승인자: 조회를 사용하여 승인자를 선택하여 **Zscaler URL** 범주 목록 페이지에서 옵저버블을 추가합니다. 이 옵션을 사용하면 승인을 위한 사용자 그룹을 추가할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	○ 옵저버블 제거에 대한 승인자: **Zscaler URL** 범주 목록 페이지에서 조회를 사용하여 옵저버블 제거에 대한 승인자를 선택합니다. 이 옵션을 사용하면 승인 목록에서 사용자 그룹을 제거할 수 있습니다.
설명	URL 범주 목록에 대한 설명입니다 Zscaler . 이 필드를 사용하여 URL 범주 기록에 대한 상세 정보를 추가합니다.

4. 제출을 클릭합니다.
   제출에 성공하면 승인 그룹에 이메일 알림이 트리거됩니다.

보안 인시던트 기록에서 **URL** 범주 목록으로 옵저버블 제출

허용 또는 차단 요청을 사용하여 보안 인시던트 기록에 첨부된 옵저버블을 구성된 URL 범주 목록에 제출합니다. 보안 검사에 대한 허용 또는 차단 목록에 옵저버블을 추가하면 사용자가 해당 URL의 콘텐츠를 검토하고 신뢰할 수 있는 콘텐츠에 액세스할 수 있습니다.

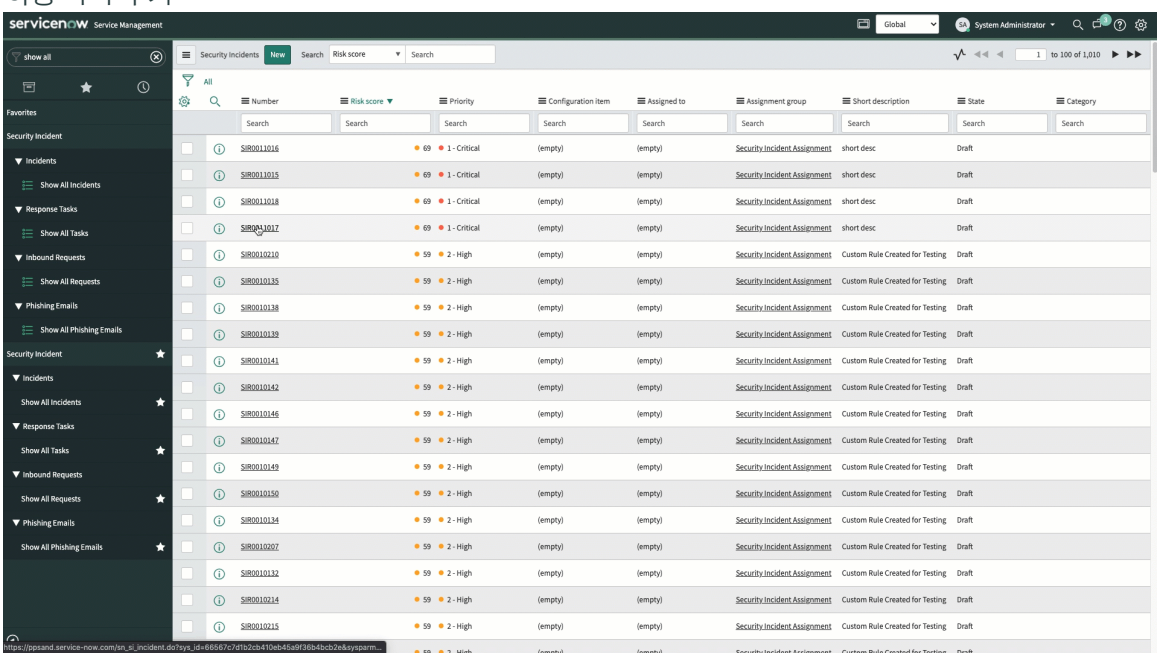
시작하기 전에
필요한 역할: sn_si.analyst

이 태스크 정보
연결된 옵저버블 관련 목록에서 허용 또는 차단 요청 작업을 사용하여 옵저버블 항목을 제출합니다. 옵저버블은 네트워크 또는 운영 체제에서 발견되는 아티팩트로, 침입을 나타낼 가능성이 높습니다. 이전에 구성한 URL 범주 목록을 사용하여 제출할 옵저버블을 선택합니다. 요청을 제출하면 승인 그룹이 승인 요청으로 전송됩니다.

프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 인시던트 〉 모든 인시던트 표시.
   이 예시에서는 보안 인시던트 및 옵저버블을 선택하고 허용 목록을 추가하는 방법을 보여줍니다.

허용 목록 추가



2. 허용 또는 차단 요청과 연결할 보안 인시던트를 Zscaler 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 모든 관련 목록 표시 및 연결된 옵저버블 탭을 클릭합니다.
옵저버블을 찾을 수 없으면 새로 만들기를 클릭합니다.
4. 옵저버블을 선택하고 작업 메뉴에서 요청 허용/차단을 클릭합니다.
5. 요청 허용/차단 대화 상자에서 옵저버블에 대한 허용 또는 차단 요청을 수행할지 여부를 선택합니다.
6. 제출을 클릭합니다.
7. 작업 메모를 보고 제출 상태와 보안 태그를 확인합니다.
상태에 대한 자세한 내용을 보거나 에 대한 워크플로우 스튜디오세부 정보를 분석하려면 작업 메모의 링크를 클릭합니다. 보안 태그는 응답 기록의 메타데이터이며 특정 유형의 보안 콘텐츠에 액세스할 수 있는 사용자를 정의합니다.
8. 선택한 옵저버블의 상태를 보려면 다음으로 이동합니다. **Zscaler** 통합 〉 **Zscaler URL** 범주 목록 항목.
9. Zscaler URL 범주 목록 항목 페이지에서 옵저버블을 클릭하여 기록을 봅니다.

URL 범주 목록에 옵저버블 승인

옵저버블 항목이 적절한 허용 또는 거부 목록에 포함되도록 URL 범주 목록에 추가된 옵저버블을 승인합니다.

시작하기 전에
필요한 역할: sn_si.analyst

프로시저

1. 다음으로 이동 모두 〉 **Zscaler** 통합 〉 **Zscaler** 승인.
2. 승인할 기록을 선택합니다.
3. 승인을 클릭합니다.
승인자 그룹은 승인 요청에 대한 이메일 알림을 받습니다. 승인자가 이메일에서 승인/거부 링크를 클릭하면 상태가 승인됨으로 변경됩니다.

URL 범주 목록에 보안 인시던트를 제출합니다.**Zscaler**

옵저버블 항목이 적절한 허용 또는 거부 목록에 있도록 특정 ServiceNow AI Platform 보안 인시던트 기록과 연결되지 않은 옵저버블에 대한 항목을 직접 제출합니다.

시작하기 전에
필요한 역할: sn_si.admin

이 태스크 정보
옵저버블 기록에서 직접 URL 범주 목록에 옵저버블을 추가할 수도 있습니다.

프로시저

1. 다음으로 이동 모두 〉 **Zscaler** 통합 〉 **Zscaler URL** 범주 목록 항목.
2. 새로 만들기를 클릭합니다.
3. 양식에서 필드를 채웁니다.

Zscaler URL 범주 목록 항목 양식

필드	설명
항목 값	옵저버블 이름입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	일치하는 옵저버블이 발견되면 양식의 나머지 부분이 자동으로 채워집니다. 일치하는 옵저버블이 없으면 나머지 정보를 수동으로 입력해야 합니다.
옵저버블	옵저버블과 연결된 값(예: IP 주소 또는 해시)입니다.
관찰 대상 유형	IP 주소 또는 파일 해시와 같은 옵저버블 분류입니다.
URL 범주 목록	URL 범주입니다. 예를 들어 조직에서 Office 365 서비스에 Zscaler example.com 사용하는 경우 example.com 전문 서비스 및 Office 365로 분류합니다.
소스	서버 이름입니다. URL 범주 목록에서 이전에 구성한 Zscaler 서버만 볼 수 있습니다.
인시던트 수	이 옵저버블이 나타나는 인시던트 수입니다. 이 값은 옵저버블이 수동으로 또는 워크플로우를 통해 다른 인시던트에 추가될 때 자동으로 업데이트됩니다.
활성	URL 범주 목록이 활성 상태임을 나타내는 표시기입니다.
상태	옵저버블이 승인 또는 거부되는 경우의 상태입니다.
만료 기간(일)	URL 범주 목록의 만료 기간입니다. 0(기본값)은 URL 범주 목록 항목이 만료되지 않음을 나타냅니다. 이 값을 변경하면 입력한 일수 동안 이 URL 범주에 추가하는 모든 옵저버블이 활성화됩니다. 최솟값으로 1을 입력할 수 있습니다. 예를 들어, 만료 기간을 30일로 설정하면 30일 후에 범주 목록에서 항목이 제거됩니다. **주:** URL 범주 목록 항목의 기본 만료 기간을 변경하면 해당 기간이 선택한 URL 범주 목록에 구성된 기간과 다르다는 경고가 표시됩니다.
추가 정보	옵저버블에 대한 상세 정보를 추가할 수 있는 필드입니다.

4. 제출을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

전역 위협 라이브러리를 사용하여 **Zscaler** 위협 조회 실행

제품의 전역 위협 라이브러리를 사용하여 옵저버블에 대한 위협 조회를 Zscaler Internet Access 실행합니다. Zscaler 는 옵저버블 유형 IP, URL 및 도메인에 대한 조회를 지원합니다.

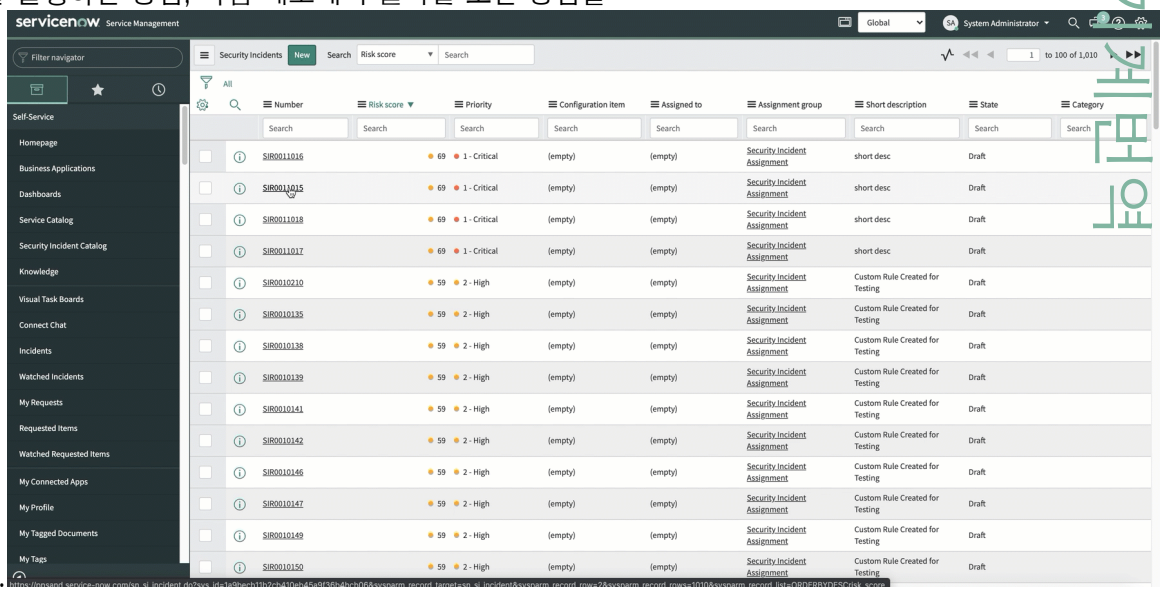
시작하기 전에
필요한 역할: sn_si.admin

이 태스크 정보
하나 이상의 옵저버블에 대해 위협 인텔리전스 조회를 수행하여 알려진 보안 위협과 연관이 있는지 여부를 확인할 수 있습니다. 옵저버블이 처음으로 보안 인시던트와 연결되면 의 ServiceNow AI Platform 모든 활성 위협 조회 구현은 자동 위협 조회를 수행합니다. 위협 조회 결과 관련 목록에 대한 결과를 볼 수 있습니다.

기본적으로 제품의 전역 위협 라이브러리에 대해 Zscaler Internet Access 위협 조회를 수행하기 위해 순서가 가장 낮은 구성이 선택됩니다. 위협 조회를 수동으로 수행할 수도 있습니다.

프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 인시던트 〉 모든 인시던트 표시.
2. 위협 조회를 실행할 보안 인시던트를 선택합니다.
3. 모든 관련 목록 표시 및 연결된 옵저버블 탭을 클릭합니다.
4. 옵저버블을 선택하고 작업 메뉴에서 위협 조회 실행을 클릭합니다.
   이 예시에서는 보안 인시던트 및 옵저버블을 선택하는 방법, 위협 조회를 실행하는 방법, 작업 메모에서 결과를 보는 방법을 보여줍니다.



결과
위협 조회를 시작한 후 작업 메모를 보고 제출 상태를 확인할 수 있습니다.

Sandbox 분석에 **Zscaler** 제출

Zscaler Internet Access 제품 샌드박스 서비스를 사용하여 가상 환경에서 파일을 분석하여 악의적인 동작을 탐지합니다.

시작하기 전에
필요한 역할: sn_si.admin

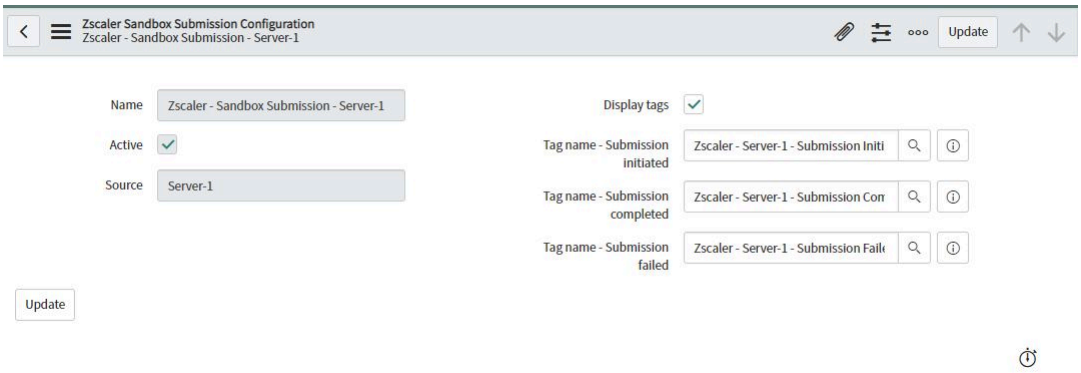
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보
구성을 생성 Zscaler 하면 Zscaler Zscaler 샌드박스 구성 모듈에서 기본적으로 샌드박스 제출이 생성됩니다.

이름 및 소스 필드는 자동으로 채워지고 구성은 기본적으로 활성화됩니다. 표시 태그와 활성 옵션만 편집할 수 있습니다. Zscaler Internet Access 제품을 사용하면 MD5 해시 유형 옵저버블에 대한 샌드박스 보고서만 가져올 수 있습니다.

MD5 해시와 연결된 파일에 대한 분석이 완료되어야 하며 해당 보고서는 샌드박스에 Zscaler 있어야 합니다. 보내는 MD5 해시에 보고서가 Zscaler없으면 오류 메시지가 표시됩니다.

Zscaler 샌드박스 제출



프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 인시던트 〉 모든 인시던트 표시.
2. 샌드박스 분석을 실행할 보안 인시던트를 선택합니다.
3. 모든 관련 목록 표시 및 연결된 옵저버블 탭을 클릭합니다.
4. MD5 해시 유형 옵저버블을 선택한 다음 Actions 메뉴에서 **Submit to Sandbox** 를 선택합니다. 기존 MD5 해시 유형 옵저버블을 찾을 수 없는 경우 MD5 해시 유형 옵저버블을 생성합니다.
5. 파일 제출(File Submission) 대화 상자의 제출 구성에서 **Zscaler -** 샌드박스 제출 **-** 서버**(Zscaler - Sandbox Submission - Server**) 옵션을 선택하고 샌드박스에 제출**(Submit to** Sandbox)을 클릭합니다.
   샌드박스 제출을 시작한 후에는 작업 메모를 보고 제출 상태를 확인할 수 있습니다. 보안 인시던트에도 태그가 추가됩니다.
6. 작업 메모에서 샌드박스 제출 결과 게시물의 링크를 클릭합니다.

결과
모든 관련 목록 표시 및 샌드박스 제출 결과 탭에서 결과를 볼 수도 있습니다.

환자 **0** 이벤트에 대한 이메일 경보 설정

악성 파일로부터 네트워크를 보호할 수 있도록 환자 0 이벤트와 같이 알 수 없는 잠재적인 악성 파일을 식별하고 검사하도록 제품을 구성합니다 Zscaler Internet Access .

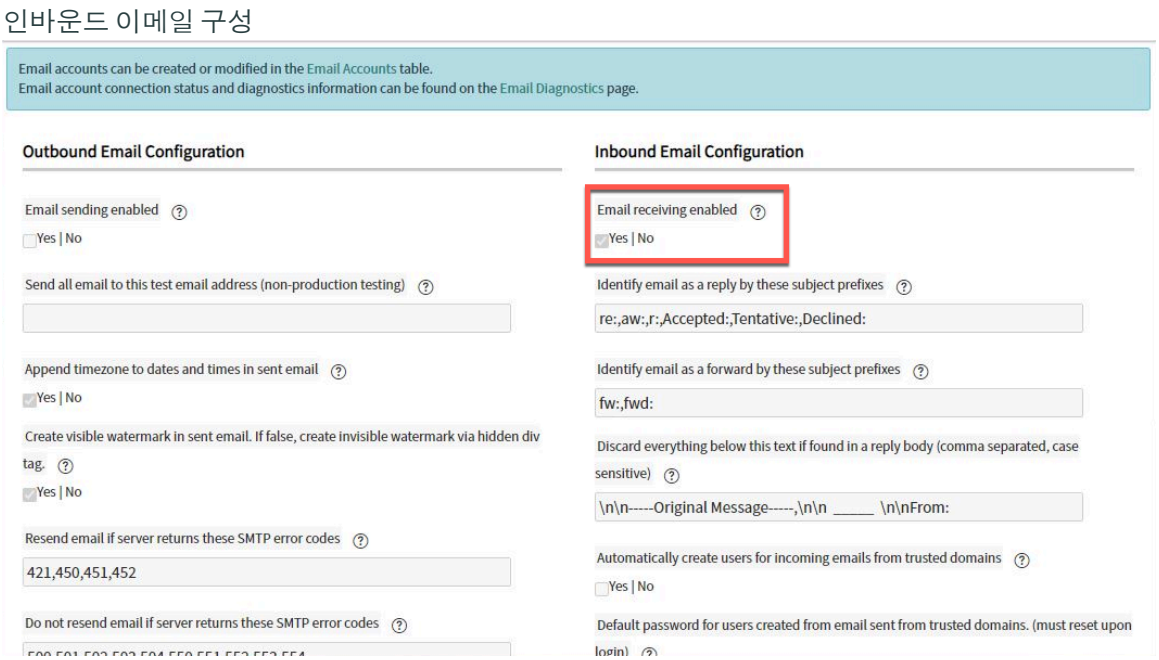
시작하기 전에
필요한 역할: sn_si.admin, Zscaler Internet Access admin

이 태스크 정보
환자 0는 다운로드가 허용되었지만 악성으로 확인된 알 수 없는 파일을 포함하는 경보 클래스입니다. 환자 0 이벤트는 심각한 것으로 분류됩니다. 환자 0 이벤트에 대해 정기적으로 이메일 경보를 수신하도록 설정할 ServiceNow AI Platform 수 있습니다.

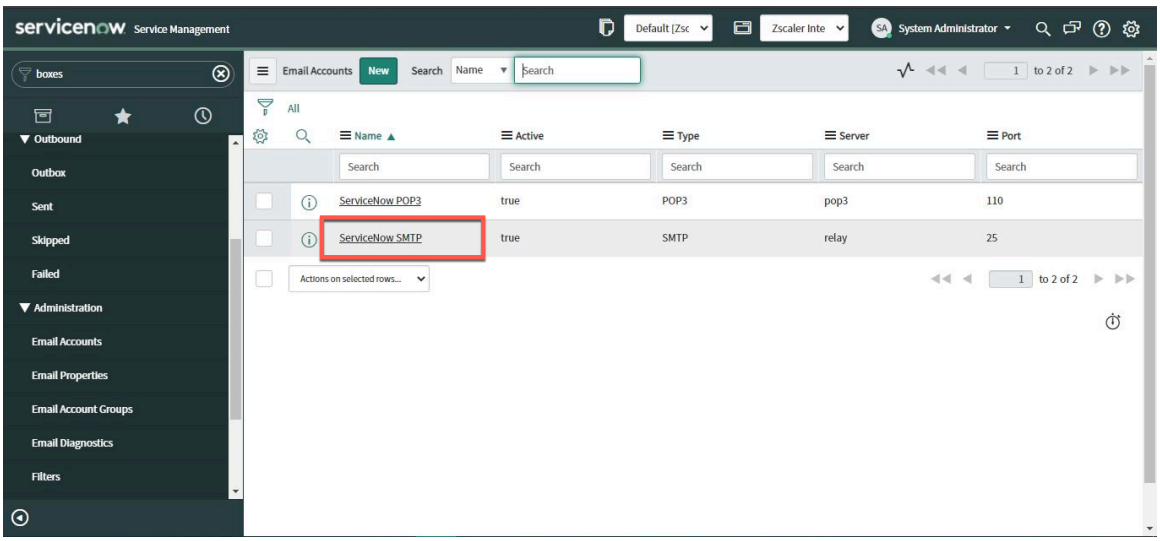
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 시스템 사서함 〉 관리 〉 이메일 속성.
2. 인바운드 이메일 구성 섹션에서 이메일 수신 사용 옵션을 선택합니다.



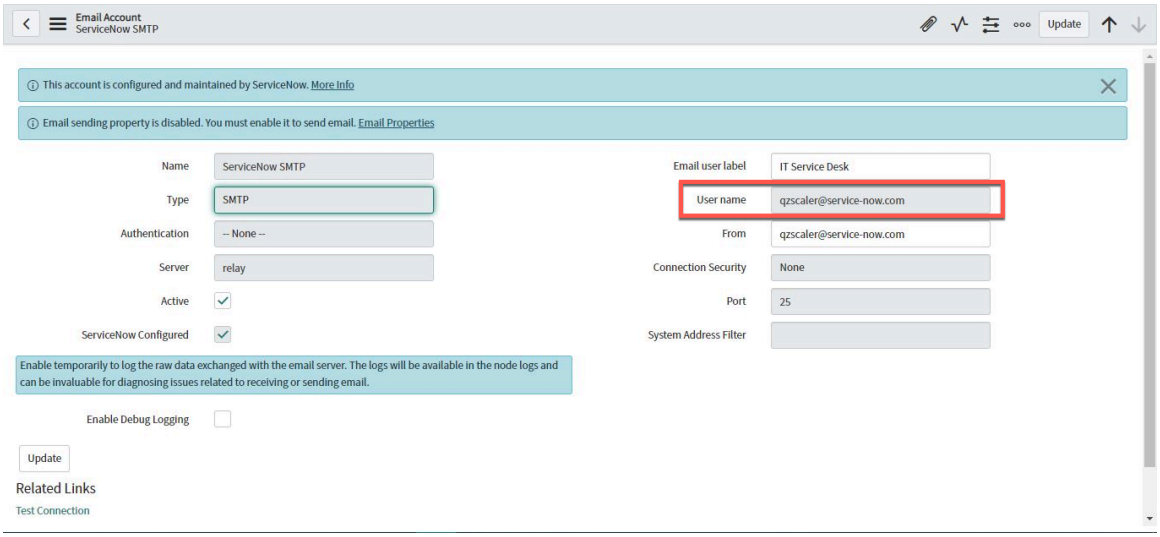
3. 저장을 클릭합니다.
4. 다음으로 이동 시스템 사서함 〉 관리 〉 이메일 계정.



5. **ServiceNow SMTP** 이메일 계정을 선택합니다.
   사용자 이름을 기록해 둡니다. 여기서 식별되는 사용자 이름은 환자 0 경보에 Zscaler 대해 구성하는 데 사용하는 이메일 주소입니다ServiceNow AI Platform.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

SMTP 계정의 사용자 이름 **ServiceNow AI Platform**



6. 관리 포털에 로그인합니다 Zscaler Internet Access .

   주:
   관리 포털에 대한 Zscaler Internet Access 자세한 내용은 Zscaler 설명서를 참조하십시오.

7. 다음으로 이동 관리 〉 경보 〉 경보 게시.
8. **Add Alert** Subscription(경보 구독 추가)을 클릭합니다.
9. 양식에서 필드를 채웁니다.

경보 구독 추가 양식

필드	설명
이메일	ServiceNow AI Platform SMTP 계정 이메일 주소입니다.
설명	환자 0 경보에 대한 상세 정보를 추가하기 위한 필드입니다.

10. 저장을 클릭합니다.

ServiceNow 보안 운영 Splunk용 추가 기능 개요

ServiceNow 보안 운영 소프트웨어 관리자는 에 대한 Splunk 추가 기능을 사용하여 Splunk 데이터를 수집하고 ServiceNow AI Platform.

추가 기능은 Splunkbase 에서 설치됩니다.

중요사항:
Splunk 는 MSP(관리형 서비스 제공자) 환경에서도 지원됩니다.

Splunk 통합 설정

Splunk용 추가 기능의 설정 절차 ServiceNow 보안 운영 에는 Splunk의 추가 기능 파일 다운로드, 추가 기능 설치, 보안 인시던트 및 이벤트가 생성되는 인스턴스 설정이 ServiceNow 포함됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필요한 역할

Splunk 통합 설정 절차를 수행하기 전에 ServiceNow 인스턴스에서 sn_si.integration_user 및 sn_si.analyst 역할을 가진 통합 사용자를 정의해야 합니다. 또한 임포트를 수행하려면 보안 테이블에 대한 읽기 및 쓰기 권한을 얻기 위한 import_transformer 역할이 필요합니다. sn_si.integration_user 역할은 역할의 import_transformer 부분으로 정의해야 합니다.

ServiceNow Security Operations 애플리케이션 다운로드

ServiceNow와 Splunk의 통합을 설정하는 첫 번째 단계는 Splunkbase에서 애플리케이션을 다운로드하는 ServiceNow 보안 운영 것입니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. Splunkbase를 엽니다.
2. ServiceNow 보안 운영 통합을 검색합니다.
3. 애플리케이션을 다운로드합니다.

Splunk용 **ServiceNow** 보안 운영 추가 기능 설치

SplunkServiceNow를 에 연결하려면 Splunk용 **ServiceNow** 보안 운영 추가 기능을 설치합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. Splunk를 엽니다.
2. **Apps** 기어 아이콘 또는 **Manage Apps** 바로 가기 메뉴 항목을 클릭합니다.
3. 파일에서 앱 설치를 클릭합니다.
4. 파일 선택을 클릭하고 sn_sec_ops.spl을 선택한 다음 업로드를 클릭합니다.
5. 메시지가 표시되면 을 다시 시작합니다 Splunk.
   ServiceNow 보안 운영 Splunk용 추가 기능이 설치되어 설정할 준비가 되었습니다.

인시던트 또는 이벤트가 생성되는 인스턴스를 설정하거나 변경합니다

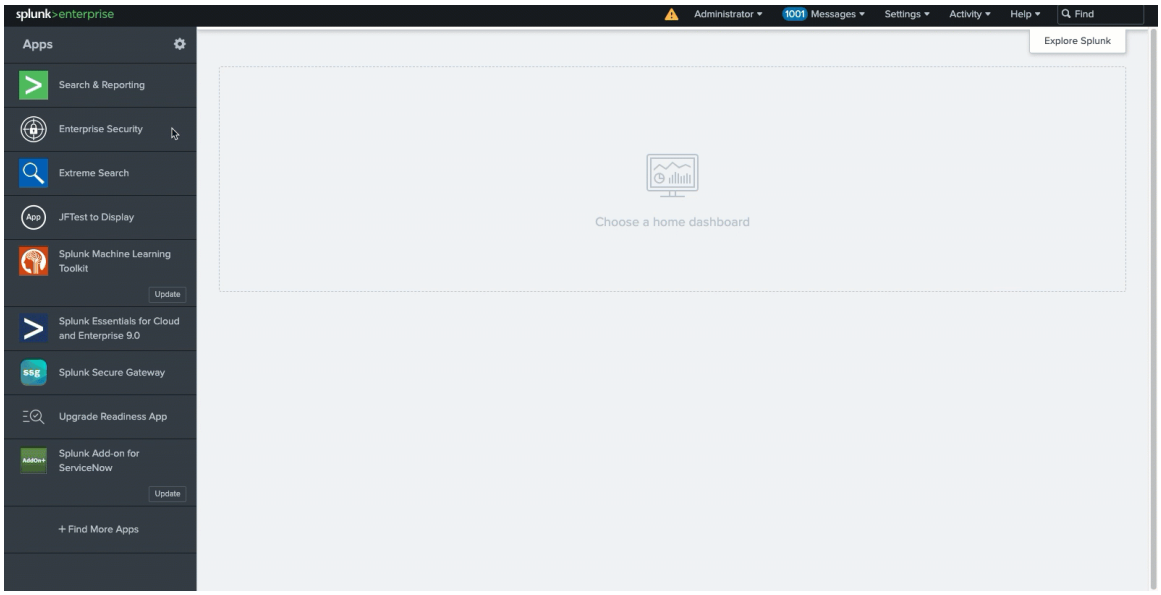
새 보안 인시던트 및 보안 이벤트가 생성되는 인스턴스를 설정하거나 변경하려면 ServiceNow 애플리케이션 목록에서 설정 작업을 사용합니다.

시작하기 전에
필요한 역할: sn_si.admin

프로시저

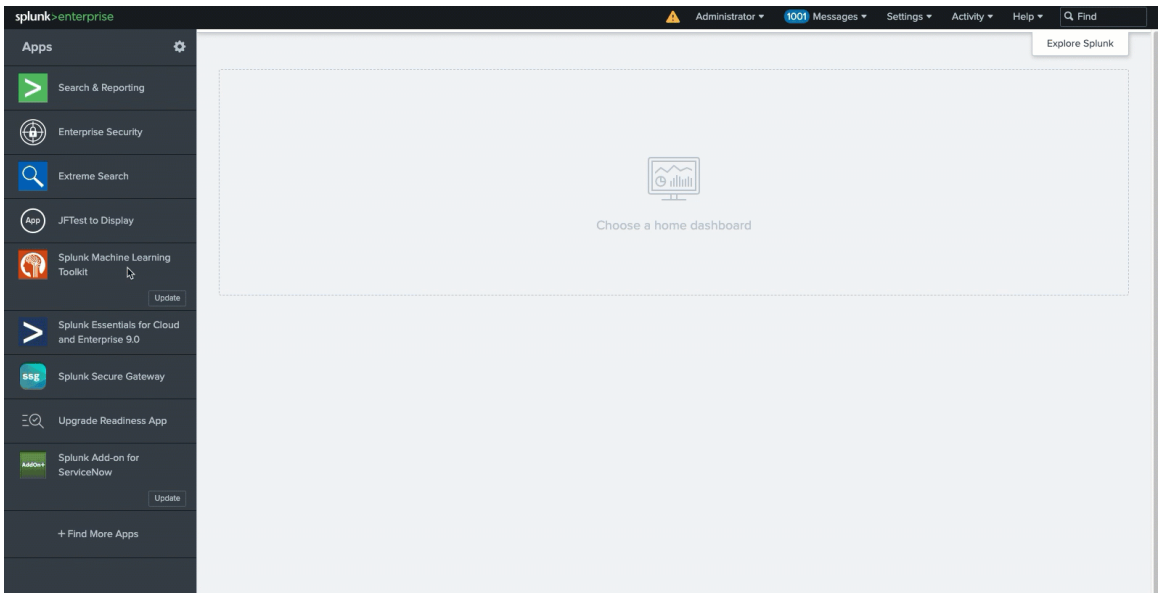
1. Splunk를 엽니다.
2. **Apps** 기어 아이콘 또는 **Manage Apps** 바로 가기 메뉴 항목을 클릭합니다.
3. 애플리케이션 목록에서 필터를 사용하여 **ServiceNow** 앱을 검색합니다.
4. **ServiceNow** 보안 운영 통합을 찾아 해당 설정 작업을 클릭합니다.
5. 양식에서 필드를 채웁니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



6. 저장을 클릭합니다.
7. 또는 **ServiceNow** 이벤트 수집 통합을 찾아 해당 설정 작업을 클릭합니다.

   ServiceNow 이벤트 수집 통합은 세 개의 서로 다른 탭으로 구성됩니다.
   - **Splunk** 기본: 기본 또는 기본 Splunk 구성입니다.
   - **Splunk** 보조: (선택 사항) 백업 또는 두 번째 Splunk 구성입니다.
   - 로깅 수준: 통합으로 생성된 보고 로그의 수준으로, 정보 유형의 이름을 의미합니다.
8. **Splunk** 기본 탭을 선택합니다.
9. 양식에서 필드를 채웁니다.



10. 옵션: **Splunk** 보조 탭을 선택합니다.
11. 옵션: 양식에서 필드를 채웁니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

12. 로깅 수준 탭을 선택합니다.
13. 양식에서 필드를 채웁니다.
14. 저장을 클릭합니다.
    확인이 성공적으로 완료되면 각 구성과 함께 보안 통합 페이지가 표시됩니다. 유효한 각 구성 타일에는 다음 그림과 같이 업데이트 및 삭제 버튼이 표시됩니다.

    주:
    기본 인증 또는 OAuth 2.0 인증만 사용해야 합니다. 인증 중 하나를 사용하도록 설정하고 해당 인증 세부 정보를 입력합니다. 둘 다 사용하도록 설정하면 오류가 표시됩니다.

    성공적으로 확인 및 제출되면 각 이벤트 수집 Splunk 서버 구성이 보안 통합 페이지에 타일로 저장됩니다. 저장된 구성 타일이 보안 통합 페이지에 표시되지 않으면 페이지의 오른쪽 상단 모서리에 있는 구성 표시 목록에서 예를 클릭합니다.

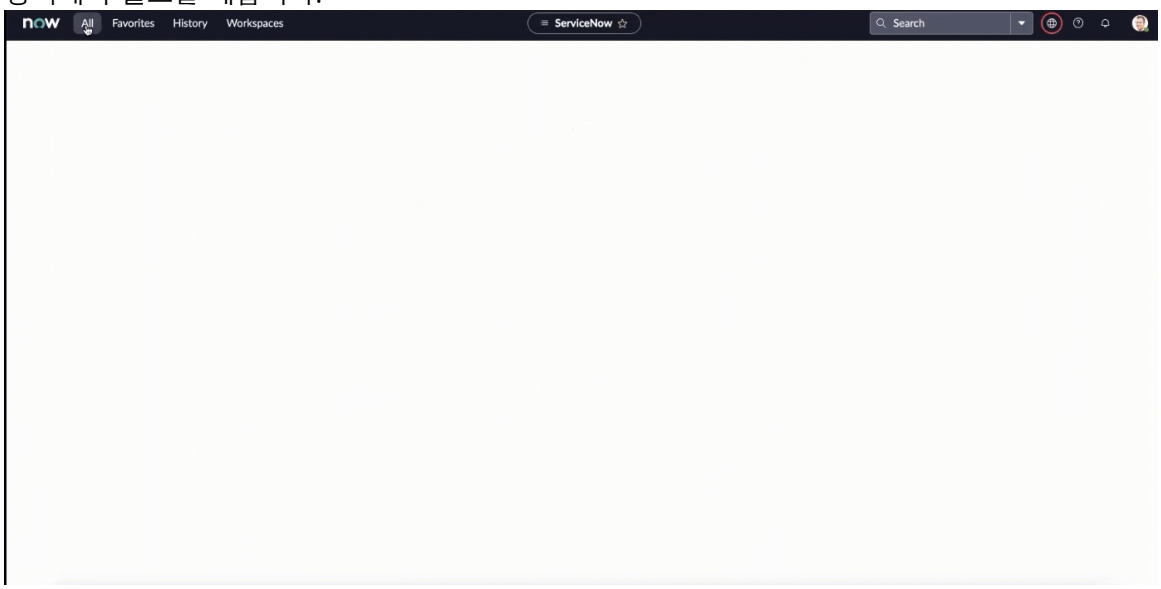
ServiceNow 인스턴스에서 애플리케이션 레지스트리 구성

OAuth 인증을 사용하려면 인스턴스에 애플리케이션을 등록합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 〉 시스템 **OAuth** 〉 애플리케이션 레지스트리.
2. 새로 만들기를 클릭합니다.
3. 외부 클라이언트용 **OAuth API** 엔드포인트 작성을 클릭합니다.
4. 양식에서 필드를 채웁니다.



5. 양식 헤더를 마우스 오른쪽 버튼으로 클릭하고 저장을 클릭합니다.
6. 제출을 클릭합니다.

수동 검색 명령

수동 검색 명령은 모든 검색 창에서 입력됩니다. 보안 인시던트나 이벤트를 생성할 수 있습니다. 명령 뒤에는 원하는 기록을 생성하는 데 사용되는 필드 이름과 값 쌍이 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 이벤트

보안 이벤트 명령 **snsecevent**는 보안 분류를 사용하여 이벤트를 ServiceNow 생성합니다.

이러한 이벤트는 자체적으로 검토하거나, 내부의 ServiceNow 경보 규칙 또는 수동 동작으로 이벤트 또는 이벤트 모음을 보안 인시던트로 전환할 수 있습니다.

이벤트가 보안 인시던트가 되고 각 매개변수가 이벤트로 전송되는 경우 이 데이터를 사용하여 다음과 같이 보안 인시던트를 채웁니다.

보안 이벤트

매개변수 이름	필수	사용	보안 인시던트에서 사용
노드	예	노드는 이벤트에 대한 서버 또는 구성 항목을 나타냅니다. 이상적으로 이 노드는 내의 기존 CI ServiceNow에 매핑됩니다.	보안 인시던트에서 사용
유형	예	이벤트의 범주입니다.	간단한 설명
resource	예	구성 항목입니다.	간단한 설명
소스	아니요	이 데이터의 출처입니다. 기본적으로 Splunk 서버는 데이터를 생성합니다.	활동 로그
external_url	아니요	이 이벤트와 관련된 Splunk 데이터로 다시 이동하는 데 사용할 ServiceNow 드릴다운 URL입니다. 기본적으로 이 URL에는 경보에 대한 결과 링크 또는 기본 Splunk 검색 페이지에 대한 링크가 포함되어 있습니다.	보안 인시던트 양식의 드릴다운 버튼을 통해 액세스하는 외부 URL
time_of_event	아니요	이벤트가 Splunk에 로그된 시간입니다.	해당 사항 없음
기타 모든 값(이 예시의 범주, 하위 범주)	아니요	이벤트의 정보 필드에 속하지 않는 모든 필드 보안 인시던트가 생성되면 이를 사용합니다.	필드가 있는데 채워지지 않은 경우 보안 인시던트에서 해당 값을 사용합니다. 예를 들어 이벤트를 통과한 범주는 새 보안 인시던트의 범주가 됩니다. 이 이름의 필드가 없으면 활동 로그에 값이 저장됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 인시던트

보안 인시던트 명령인 **snsecincident**가 인스턴스에 보안 인시던트 ServiceNow 를 생성합니다.

보안 인시던트

매개변수	필수	사용
short_description	예	인시던트에 대한 짧은 한 줄 설명입니다.
범주	아니요	보안 인시던트의 범주입니다. 이 범주가 없으면 새로 만들어집니다.
하위 범주	아니요	하위 범주입니다. 이 하위 범주가 없으면 새로 만들어집니다.
cmdb_ci	아니요	보안 인시던트의 구성 항목입니다. 이상적으로 이 항목은 . 내의 기존 CI ServiceNow에 매핑됩니다.
설명	아니요	인시던트에 대한 더 길고 자세한 설명입니다.

유용한 열이 많이 있습니다. 보안 인시던트 변환 맵의 모든 항목을 사용할 수 있습니다. 새 열이 보안 인시던트에 추가되면 변환 맵에 있는 한 해당 열도 사용됩니다. 몇 가지 유용한 열: 위치, 우선 순위, assignment_group, assigned_to, affected_user, attack_vector 및 watch_list.

Splunk 이벤트 작업

Splunk 로그를 검토할 때 이벤트 작업을 사용하여 로그의 모든 항목에서 보안 이벤트 및 보안 인시던트를 신속하게 생성할 수 있습니다.

이러한 작업 중 하나를 클릭하면 로그 항목의 데이터로 채워진 수동 검색 명령이 생성되고 이를 실행하여 새 레코드가 생성됩니다.

이러한 작업은 정규화된 데이터에 필드를 추가하도록 쉽게 구성할 수 있습니다. Splunk 내에서 설정 〉 필드 〉 워크플로우 작업, 수동 검색 필드를 사용하여 이러한 작업 중 하나를 선택하고 편집할 수 있습니다.

작업이 표시되는 위치와 필드를 선택하고, 검색 명령이 포함된 검색 문자열을 수정하여 기록을 생성할 수 있습니다.

단일 기록 **Splunk** 경보

경보 내에서, 경보가 실행될 때 만들 보안 이벤트 또는 보안 인시던트를 지정할 수 있습니다.

경보를 열거나 만들고, 작업을 편집할 때 원하는 기록 유형을 선택하고 경보 대화 상자를 채웁니다.

다중 기록, 사용자 지정 필드 **Splunk** 경보

다중 기록 경보(여러 **ServiceNow** 보안 인시던트 생성 및 여러 **ServiceNow** 보안 이벤트 생성 트리거 작업을 사용하여 정의됨)는 지원되는 모든 필드 집합이 있는 기록을 자동으로 만들 수 있습니다.

이들은 기본값이 제공된다는 점에서 다른 경보 작업과는 다르게 작동합니다. 그러나 대부분의 데이터는 해당 경보에 대한 검색 결과에서 가져옵니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
이전 버전의 추가 기능 및 이 설명서에서는 스크립트된 경보가 지원되었습니다. 해당 기능은 더 이상 사용되지 않으며 이 지침으로 대체되었습니다.

다중 기록, 사용자 지정 필드 생성 **Splunk** 경보

사용자 지정 필드가 있는 다중 기록 Splunk 경보를 생성하려면 채우려는 ServiceNow 열과 일치하도록 설계된 검색을 빌드해야 합니다.

시작하기 전에
필요한 역할: sn_si.admin

프로시저

1. 검색으로 이동합니다.
2. 검색 상자에서 기록 데이터를 생성하는 검색을 생성합니다.
   권장 검색 기준에 대한 예시 를 참조하십시오.
3. **Save** As(다른 이름으로 저장)를 클릭하고 Alert(경보)를 선택합니다.
4. 필요에 따라 이름, 권한 및 일정을 설정합니다.
5. 작업 추가를 클릭합니다.
6. 다음 중 하나를 선택합니다.
   - 검색 결과당 하나의 이벤트를 생성하려면 여러 **ServiceNow** 보안 이벤트 생성을 선택합니다.
   - 검색 결과당 하나의 인시던트를 만들려면 여러 **ServiceNow** 보안 인시던트 만들기를 선택합니다.
7. 필요에 따라 기본값을 설정합니다.
   검색 결과의 필드가 비어 있거나 없으면 기본값이 사용됩니다. 결과에 값이 있으면 기본값을 덮어씁니다.

다중 기록, 사용자 지정 필드 **Splunk** 경보 예시

사용자 지정 필드를 사용하여 여러 기록 Splunk 경보를 생성하는 경우 경보 데이터를 생성하기 위한 검색 기준을 정의해야 합니다. 보안 인시던트 및 보안 이벤트에 대한 검색 기준의 예가 표시됩니다.

보안 인시던트 검색

보안 인시던트의 경우 이 기준은 보안 인시던트 테이블의 열을 채우는 검색을 빌드합니다.

```
host=Development source="/CodeArchive/password/password_decrypt.cpp" |
eval contact_type="Monitoring" |
eval cmdb_ci=host |
eval subcategory="Sensitive Data Monitoring" |
eval description=_raw |
eval source_ip=found_ip
```

보안 이벤트 검색

보안 이벤트의 경우 이는 동일한 검색이지만 대신 이벤트 필드를 채웁니다. 이 이벤트가 보안 인시던트로 전환되고 이벤트에 존재하지 않는 필드가 채워지면 보안 인시던트로 이전됩니다. 그렇지 않으면 이벤트 및 경보의 추가 정보 필드에 남아 있습니다.

```
host=Development source="/CodeArchive/password/password_decrypt.cpp" |
eval type="Monitoring" |
eval node=host |
eval source=source
eval subcategory="Sensitive Data Monitoring" |
```


© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
eval description=_raw |
eval source_ip=found_ip
```

주:
사용하는 검색 기준은 검색에서 발견되는 만큼 기록을 추가합니다. 5개 또는 10,000,000,000개의 기록을 추가할 수 있습니다. 따라서 이것은 데이터의 대량 전송에 권장되는 방법이 아닙니다. 이 메서드의 의도는 ServiceNow 인스턴스에 REST 호출당 하나의 기록을 추가하는 것입니다.

Splunk 오류 보고

ServiceNow 인스턴스의 연결 문제가 발생할 때마다 Splunk에 해당 문제를 설명하는 정보와 함께 오류가 기록됩니다.

오류 메시지는 sourcetype이 **servicenow**인 **servicenow**라는 새 인덱스에 저장됩니다.

오류 로그를 검색하려면 검색에서 **servicenow** 인덱스를 지정해야 합니다. 또는 새 **ServiceNow** 인덱스를 기본 검색 인덱스에 추가하는 방법에 대한 최신 Splunk 설명서를 참조하십시오.

Splunk Enterprise Event Ingestion 에 대한 보안 운영 통합 기준 **ServiceNow**

Splunk Enterprise 이벤트 및 경보 데이터와 ()SIR 제품의 통합을 보안 인시던트 응답 통해 보안 인시던트 분석가는 보안 로그 및 관련 이벤트 데이터를 수집하고 처리할 수 있습니다.

개요

데이터는 실시간으로 수집되며 분석가가 잠재적인 사이버 위협을 식별하고 보고하는 데 사용됩니다. 수집된 보안 이벤트는 이 통합과 함께 자동으로 수집되는 트리거된 경보로 처리될 수 있습니다. 또한 개별 보안 이벤트를 요청 Splunk Enterprise 시 검색 및 보고 인터페이스에서 보안 인시던트 응답 제품으로 ServiceNow AI Platform 수동으로 전달하여 보안 인시던트를 생성할 수 있습니다. 검색 헤드 클러스터 구성을 사용하여 검색에서 Splunk Enterprise 주목할 만한 이벤트를 검색할 수 있습니다. 클러스터의 일부인 검색 헤드의 URL 및 API 포트를 사용하여 이를 수행할 수 있습니다.

이 통합은 보안 운영 센터(SOC) 분석가에게 이벤트 및 관련 경보 데이터에 대한 가시성을 제공합니다. 이 데이터는 추가 조사 및 정정을 위해 (SIR) 보안 인시던트에 ServiceNow AI Platform 보안 인시던트 응답 통합될 수 있습니다. 지속적으로 수집된 경보 및 전달된 이벤트에 대한 Splunk 프로필이 인스턴스에 생성됩니다 ServiceNow AI Platform . 이러한 프로파일은 보안 인시던트에 SIR 다양한 Splunk 경보 및 이벤트 필드가 표시되는 방식을 사용자 지정합니다. 고객별 요구에 맞게 편집하고 보강할 수 있는 경보 필드의 기본 매핑이 제공됩니다.

주요 기능

이 통합에는 다음과 같은 주요 기능이 포함됩니다.

- 여러 경보 수집 프로파일을 생성하여 피싱 및 맬웨어와 같은 특정 유형의 위협에 대한 SIR 보안 인시던트를 생성합니다.
- 콘솔에서 요청 시 이벤트 전달 Splunk 을 위한 여러 이벤트 프로파일을 생성하여 SIR 보안 인시던트를 생성합니다.
- 경보 및 이벤트 필드 값을 연관된 SIR 보안 인시던트 필드에 끌어서 놓기로 매핑 Splunk 합니다.
- 프로파일 구성을 확인하기 위한 샘플 경보 또는 이벤트를 기반으로 하는 보안 인시던트 레이아웃의 SIR 미리 보기입니다.
- 구성 가능한 간격으로 과거 경보뿐만 아니라 진행 중인 향후 경보를 수집합니다.
- 중복 보안 인시던트를 방지하기 위해 일치하는 필드 값을 기준으로 이벤트 또는 경보를 기존 SIR 보안 인시던트에 집계합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

지원되는 **ServiceNow AI Platform** 버전

com.snc.si_dep 플러그인이 필요합니다. 이 플러그인은 제품을 지원하는 데 필요한 모든 종속성을 보안 인시던트 응답 자동으로 설치합니다. 다른 보안 운영 애플리케이션을 설치 및 활성화하기 전에 이 플러그인을 설치하고 활성화하십시오.

에서 ServiceNow Store다음 보안 운영 애플리케이션을 설치하고 활성화해야 합니다. 원활한 설치를 위해 아래 나열된 순서대로 한 번에 하나의 애플리케이션을 설치하고 활성화합니다.

1. 보안 통합 프레임워크
2. Security Support Common
3. 보안 지원 오케스트레이션
4. 보안 인시던트 응답

핵심 애플리케이션 설치에 보안 운영 대한 자세한 내용은 해당 애플리케이션 활성화 ServiceNow Store문서를 참조하십시오제품 또는 애플리케이션에 대한 보안 운영 권리 가져오기.

ServiceNow 애드온

ServiceNow 용 Splunk Enterprise 보안 운영 이벤트 수집 추가 기능은 콘솔에서 인스턴스로 ServiceNow AI Platform 이벤트를 수동으로 Splunk Enterprise 전달하려는 경우에만 필요합니다. 이 ServiceNow 애드온은 splunkbase 에서 사용할 수 있습니다.

splunkbase의 애플리케이션에 대한 Splunk Enterprise 이 ServiceNow 보안 운영 이벤트 수집 애드온은 통합에서 지원하는 자동화된 경보 수집에 필요하지 않습니다.

Splunk 지원 버전

이 통합은 의 버전 6.0 이상을 Splunk Enterprise지원합니다. 통합은 엔터프라이즈 클라우드 서비스도 Splunk 지원합니다.

MID 서버

서버가 회사 네트워크 내에 배포된 경우 Splunk 이 통합을 수행하려면 인스턴스에 MID 서버가 ServiceNow AI Platform# 설치 및 구성되어 있어야 서비스에 연결할 Splunk 수 있습니다. 서비스를 사용하는 Splunk Cloud 경우에는 MID 서버가 필요하지 않습니다. MID Server에 대한 자세한 내용은 MID Server 를 참조하십시오.

통합 아키텍처 및 시스템 연결

주요 용어 및 외부 시스템 연결 세부 정보를 포함하여 통합 아키텍처에 대한 자세한 내용은 문서를 통합을 위한 Splunk Enterprise Event Ingestion 통합 아키텍처 및 외부 시스템 연결참조하십시오.

검사 목록

이러한 주제에 대한 인쇄 가능한 검사 목록은 다음 문서를 참조하십시오 주목할 만한 이벤트 수집 통합을 위한 Splunk Enterprise Security 검사 목록. 이 목록을 사용하여 통합 작업을 수행할 때의 진행률을 모니터링할 수 있습니다.

다음 주제에 사용된 이미지는 의 Kingston 릴리스 ServiceNow AI Platform에 대해 생성된 것입니다. San Diego 사용자 인터페이스에 대한 자세한 내용은 보안 분석가 작업 공간을 사용하여 보안 위협 관리를 참조하십시오.

다음 항목에 번호가 매겨져 있습니다. 애플리케이션의 원활한 설치 및 구성을 위해 아래 나열된 주제를 제시된 순서대로 따르십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

ServiceNow AI Platform® 통합을 위한 Splunk Enterprise Event Ingestion 인스턴스 설정

다음 섹션에서는 에서 애플리케이션을 ServiceNow Store설치하기 전에 인스턴스에서 완료해야 ServiceNow AI Platform# 하는 설정 작업을 나열합니다.

시작하기 전에

필요한 역할: 관리자

이 태스크 정보

원활한 설치 및 구성을 위해 애플리케이션을 다운로드하고 설치하기 전에 다음 테이블을 참조하고 나열된 작업을 모두 완료했는지 확인하십시오.

프로시저

1. 필수 ServiceNow AI Platform# 역할과 보안 인시던트 응답(SIR) 역할을 할당했는지 확인합니다.

   인스턴스에서 통합을 ServiceNow AI Platform# 설치, 설정 및 사용하려면 다음 역할이 필요합니다.

   - 관리자 역할(admin)의 ServiceNow AI Platform# 사용자는 보안 인시던트 관리자(sn_si.admin) 역할을 사용하여 ServiceNow Store 애플리케이션을 설치하고 할당합니다.
   - 이 통합에서 Splunk Enterprise 이벤트를 수동으로 전달하려면 관리자 역할을 가진 ServiceNow AI Platform# 사용자가 에서 (sn_sec_splunk_v2.api_account_access) 역할을 ServiceNow AI Platform#가진 사용자를 할당합니다. 이 역할을 사용하면 관리자 역할이 있는 Splunk Enterprise 사용자가 이 통합에 대한 수동 이벤트 전달에 필요한 API ServiceNow AI Platform# 에 액세스할 수 있습니다.

     인스턴스에서 자동으로 Splunk EnterpriseServiceNow AI Platform# 경보를 수집하는 경우 통합에 (sn_sec_splunk_v2.api_account_access) 역할이 필요하지 않습니다.
   - **sn_si.ingestion_profile_admin** 역할을 가진 사용자는 다음에서 다음 작업을 감독합니다.ServiceNow AI Platform#
     - 경보 및 이벤트 프로파일의 이름을 지정하고, 생성하고, 편집합니다.
     - 경보 및 이벤트의 값을 선택하여 보안 인시던트에 매핑합니다 ServiceNow AI Platform# .
     - 구성을 완료하기 전에 보안 인시던트 상세 정보가 정확한지 미리 봅니다.
     - 진행 중인 경보 수집을 예약합니다.
     - 보안 인시던트 분석가(sn_si.analyst) 역할을 할당합니다.
     - sn_si.analyst 사용자는 보안 인시던트에 대한 작업을 수행합니다.

   역할 및 사용자에게 역할을 할당하는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 Managing roles .

2. API 버전 6.0 이상을 Splunk 사용하고 있는지 확인합니다.

   콘솔에 액세스할 Splunk Enterprise 수 있는 경우 이 통합에 필요한 API에 액세스할 수 있습니다. API에 필요한 다른 특수 설정은 없습니다.

3. MID Server를 설치하고 구성했는지 확인하십시오.

   서버가 회사 네트워크 내에 배포된 경우 Splunk 서비스의 MID Server ServiceNow AI Platform# 가 서비스에 연결 Splunk 되어야 합니다. MID 서버에 대한 자세한 내용은 MID 서버를 참조하십시오.

   서비스를 사용하는 Splunk Cloud 경우에는 MID 서버가 필요하지 않습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. ServiceNow 통합을 지원하는 데 필요한 핵심 애플리케이션이 설치되고 활성화되었는지 확인합니다.

   Dependency 플러그인(com.snc.si_dep)이 보안 인시던트 응답 필요합니다. 이 플러그인은 제품을 지원하는 데 필요한 모든 종속성을 보안 인시던트 응답 자동으로 설치합니다. 통합에 필요한 다른 보안 운영 애플리케이션을 설치하고 활성화하기 전에 이 플러그인을 설치하고 활성화합니다.

   에서 ServiceNow Store다음 보안 운영 애플리케이션이 설치되고 활성화되는지 확인합니다. 설치되지 않은 경우 원활한 설치를 위해 다음 순서로 한 번에 하나의 애플리케이션을 설치하고 활성화합니다.

   a. 보안 인시던트 응답
   b. 보안 통합 프레임워크
   c. Security Support Common
   d. 보안 지원 오케스트레이션

   핵심 애플리케이션 설치에 보안 운영 대한 자세한 내용은 해당 애플리케이션 활성화 ServiceNow Store문서를 참조하십시오제품 또는 애플리케이션에 대한 보안 운영 권리 가져오기.

다음에 수행할 작업
통합을 위한 인스턴스를 성공적으로 설정 ServiceNow AI Platform# 했습니다. 다음 단계는 통합을 위해 애플리케이션을 ServiceNow Store 설치하는 Splunk Enterprise Event Ingestion 것입니다. 자세한 내용은 통합을 위한 Splunk Enterprise Event Ingestion 애플리케이션 설치 및 구성 ServiceNow 문서를 참조하십시오.

수집을 위해 콘솔에 검색을 Splunk Enterprise 저장하지 않았거나 콘솔과 보안 운영 인스턴스 제품 ServiceNow AI Platform# 에서 Splunk Enterprise 동시에 이 통합에 대한 초기 설정을 수행하는 경우 자세한 내용은 을 참조하십시오통합에 대한 Splunk Enterprise Event Ingestion 콘솔 검색 Splunk Enterprise 저장.

통합을 위해 콘솔에서 요청 시 Splunk Enterprise 이벤트를 수동으로 익스포트하려면 문서를 Splunk 이벤트 수집 통합을 위한 Splunk Enterprise 수동 이벤트 수집을 위한 환경 설정 참조하십시오.

통합을 위한 **Splunk Enterprise Event Ingestion** 애플리케이션 설치 및 구성 **ServiceNow**

인스턴스에서 통합을 ServiceNow AI Platform# 실행하기 전에 다음 설치 및 구성 단계를 완료하여 애플리케이션이 인스턴스의 및 보안 운영 제품과 ServiceNow AI Platform# 제대로 통합 보안 인시던트 응답 되도록 합니다.

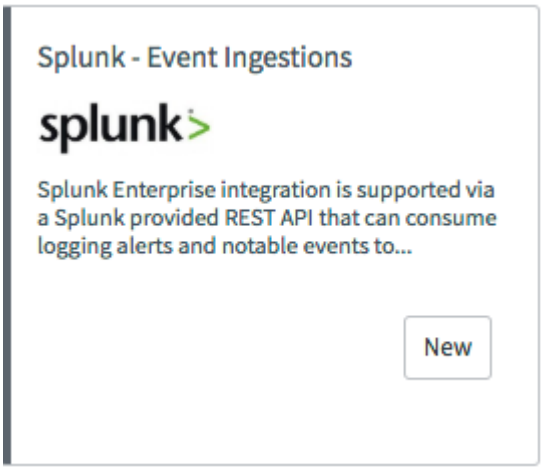
시작하기 전에
필요한 역할: sn_si.ingestion_profile_admin

> **주:**
> sn_si.admin 역할은 기본적으로 필수 권한을 상속하므로 sn_si.admin 역할을 가진 사용자는 프로필 관리자가 사용할 수 있는 모든 작업을 수행할 수 있습니다.

프로시저

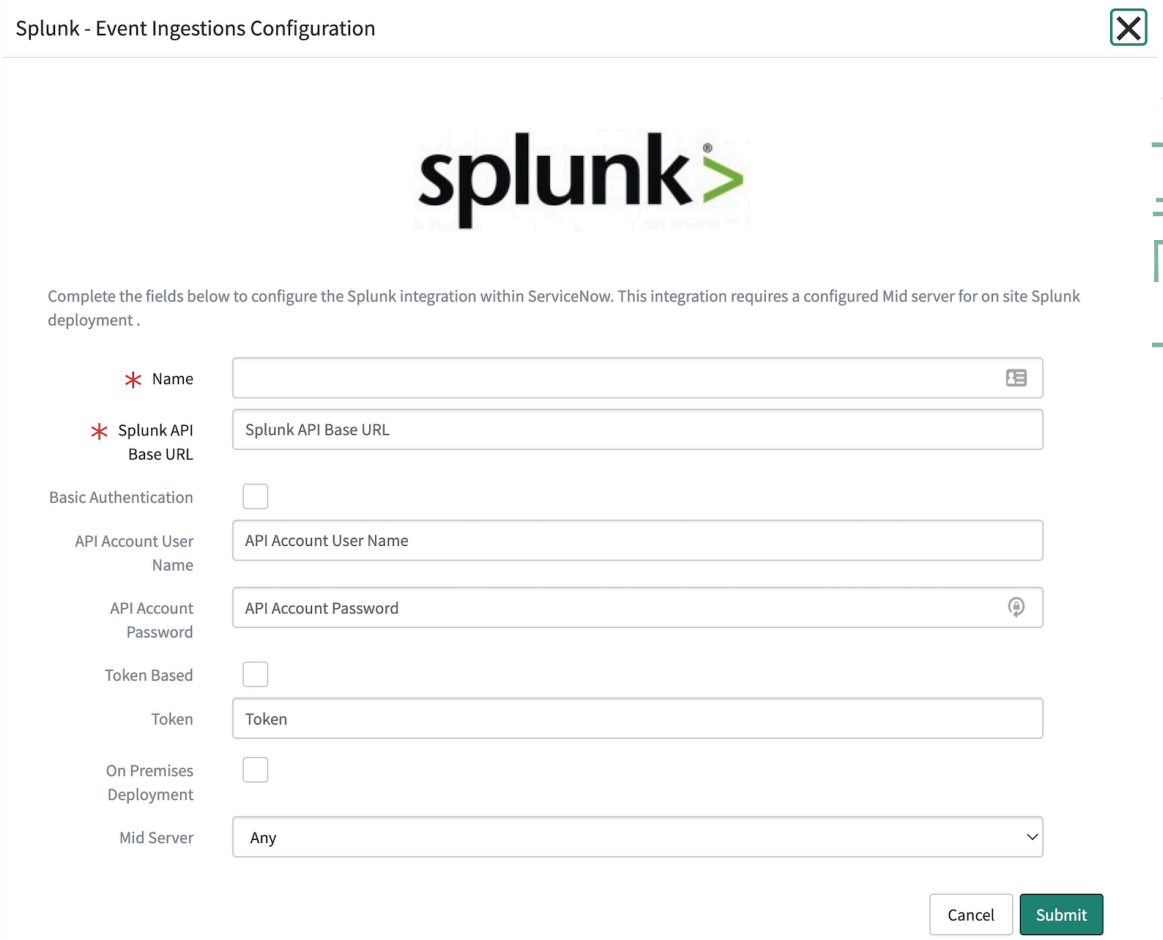
1. 통합을 위해 애플리케이션을 ServiceNow Store 설치하지 Splunk Enterprise Event Ingestion 않은 경우 를 참조 보안 운영 통합 설치 하고 단계에 따라 설치합니다.
2. 애플리케이션을 성공적으로 설치한 후 통합 〉 통합 구성 이벤트 수집 타일을 Splunk 찾습니다.
3. 애플리케이션을 구성하려면 새로 만들기를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 또는 구성 단추가 타일에 표시되면 클릭하여 기존 구성을 편집합니다.
5. 표시되는 이벤트 수집 구성 대화 상자에서 필드에 내용을 입력합니다.

   다음 그림은 MID 서버가 있는 온프레미스 버전의 Splunk Enterprise 구성에 대해 작성된 양식의 예입니다.



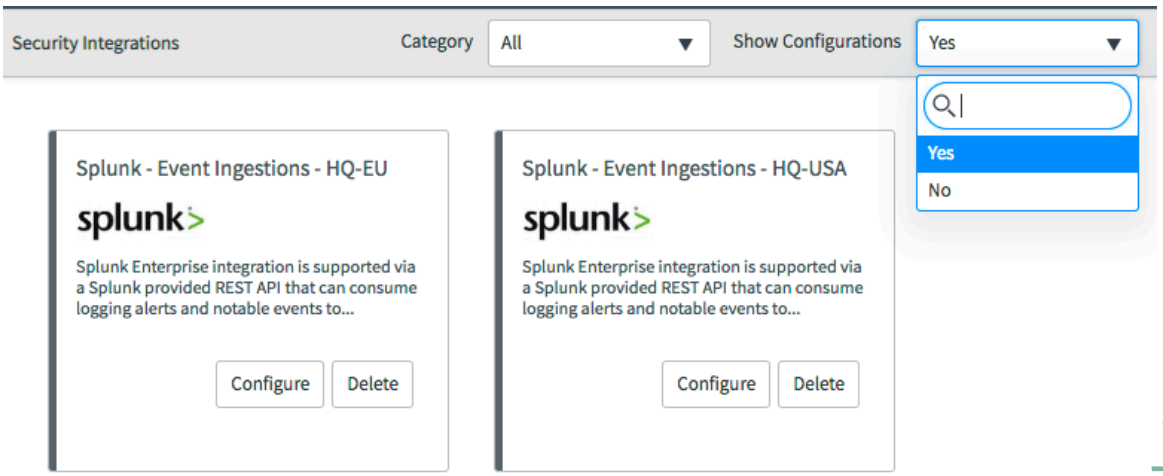
콘솔에서 수집하는 Splunk Enterprise 각 Splunk Enterprise 경보에는 인스턴스의 고유한 이벤트 프로파일이 ServiceNow AI Platform# 필요합니다. 그러나 이벤트 수집 구성 양식에서 구성하는 소스는 각 프로파일이 고유하게 Splunk 트리거된 경보를 수집하는 한 여러 ServiceNow AI Platform# 프로파일에 재사용할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

6. 제출을 클릭합니다.
확인이 성공적으로 완료되면 각 구성과 함께 보안 통합 페이지가 표시됩니다. 유효한 각 구성 타일에서 다음 그림과 같이 구성 및 삭제 버튼이 표시됩니다.

> **주:**
> 기본 인증 또는 토큰 기반 인증만 사용해야 합니다. 인증 중 하나를 사용하도록 설정하고 해당 인증 세부 정보를 입력합니다. 둘 다 사용하도록 설정하면 오류가 표시됩니다.

성공적으로 확인 및 제출되면 각 이벤트 수집 Splunk 서버 구성이 보안 통합 페이지에 타일로 저장됩니다. 저장된 구성 타일이 보안 통합 페이지에 표시되지 않으면 페이지 오른쪽 상단 모서리에 있는 구성 선택 목록 표시에서 예를 클릭합니다.



Trouble?

제출을 클릭한 후 오류 메시지가 표시되면 정보를 다시 입력하고 제출을 클릭하십시오.

다음에 수행할 작업
애플리케이션을 성공적으로 설치하고 구성했습니다. 다음 단계는 이벤트 프로파일을 만드는 것입니다.

Splunk 엔터프라이즈 이벤트 수집 설정 구성

Splunk 엔터프라이즈 이벤트 수집 설정을 사용하여 요구 사항에 따라 사전 설정 구성과 해당 값을 수정합니다.

시작하기 전에
필요한 역할: sn_si.ingestion_profile_admin

> **주:**
> sn_si.admin 역할은 기본적으로 필수 권한을 상속하므로 sn_si.admin 역할을 가진 사용자는 프로필 관리자가 사용할 수 있는 모든 작업을 수행할 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 **Splunk Integration** 〉 **Splunk Integration** 설정.
2. 양식에서 필드를 채웁니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Splunk Integration 설정

필드	설명
프로파일 작성 시 표시할 최대 경보 수입니다. sn_sec_splunk_v2.max_alerts_to_display	이벤트 프로파일을 생성하는 동안 표시할 최대 경보 수를 정의하는 옵션입니다. 기본적으로 이 값은 500으로 설정됩니다.
하루에 생성할 최대 보안 인시던트 수입니다. sn_sec_splunk_v2.max_si_per_day	하루에 만들 수 있는 최대 보안 인시던트 수를 정의하는 옵션입니다. 기본적으로 이 값은 1000으로 설정됩니다.
호출당 Splunk에서 가져올 최대 이벤트 수입니다. sn_sec_splunk_v2.max_events_per_call	각 호출에 대해 Splunk에서 검색할 최대 이벤트 수를 정의하는 옵션입니다. 기본적으로 이 값은 100으로 설정됩니다.
정보 제공 또는 디버깅을 위해 완료/오류 발생 후 항목이 큐 테이블에 남아 있는 일수입니다. sn_sec_splunk_v2.queue_item_expire	정보 또는 디버깅 목적으로 인해 완료 또는 오류 발생 후 항목이 큐 테이블에 남아 있는 일수를 정의하는 옵션입니다. 기본적으로 이 값은 14로 설정됩니다.
이벤트 임포트, 작업에 대한 이벤트 및 발생한 경보 데이터를 유지할 일 수입니다. sn_sec_splunk_v2.retention_period	이벤트 임포트, 작업에 대한 이벤트 및 발생한 경보 데이터를 보존할 일 수를 결정하는 옵션입니다. 기본적으로 이 값은 30으로 설정됩니다.
토큰 기반 인증 지원을 위한 기존 Splunk 소스 구성을 업데이트하려면 이 설정을 활성화합니다. 이 설정을 사용하도록 설정한 후에는 토큰 상세 정보로 통합 구성을 업데이트해야 합니다. sn_sec_splunk_v2.upgrade_existing_tile	기존 Splunk 소스 구성을 기존 버전의 토큰 기반 인증 지원으로 업데이트하는 옵션입니다. **주:** 새 버전으로 업그레이드하면 토큰 필드를 사용할 수 없게 됩니다. 토큰 기반 인증을 가져오려면 이 설정을 활성화해야 하며, 그 후에는 토큰 상세 정보로 통합 구성을 업데이트해야 합니다. 기본적으로 값은 아니요로 설정됩니다.
로깅 수준 - 디버그, 정보, 경고, 오류. sn_sec_splunk_v2.logging.verbosity	
Splunk 검색 유효 시간(초)입니다. sn_sec_splunk_v2.sid_ttl	기본적으로 이 값은 14로 설정됩니다.
Splunk에서 이벤트를 가져오는 동안 추가할 겹침(분) 수입니다(Splunk의 인덱싱 지연을 극복하기 위해). sn_sec_splunk_v2.overlap_time	기본적으로 이 값은 0으로 설정됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
수집 중에 Splunk 검색 쿼리를 발동하는 데 사용할 경보 규칙 배치 크기입니다. sn_sec_splunk_v2.rules_batch_size	기본적으로 이 값은 50으로 설정됩니다.
스파이크를 처리하기 위해 트리거된 경보당 이벤트 제한입니다. sn_sec_splunk_v2.spike_events_limit	기본적으로 이 값은 1000으로 설정됩니다.
필드 매핑에서 값을 분할하는 구분 기호 문자입니다. sn_sec_splunk_v2.delimiter	

3. 저장을 선택합니다.

이벤트 프로파일 생성 및 이름 지정

인스턴스에 이벤트 프로파일을 ServiceNow AI Platform 생성하고 보안 Splunk 인시던트를 생성하는 경보를 결정합니다.

시작하기 전에
필요한 역할: sn_si.ingestion_profile_admin

> **주:**
> sn_si.admin 역할은 기본적으로 필수 권한을 상속하므로 sn_si.admin 역할을 가진 사용자는 프로필 관리자가 사용할 수 있는 모든 작업을 수행할 수 있습니다.

이 태스크 정보
수집된 경보에서 (SIR)보안 인시던트가 생성되기 전 ServiceNow AI Platform 보안 인시던트 응답에는 실제 보안 인시던트가 표시되는 방식을 미리 볼 수 있도록 경보의 필드 값이 보안 인시던트의 레이아웃 ServiceNow AI Platform 에 표시됩니다.

사용 가능한 API Splunk 를 사용하는 통합 관점에서 이벤트는 개별 이벤트로 개별적으로 또는 수동으로 전달되거나 인스턴스 환경 ServiceNow AI Platform 으로 보안 운영 자동으로 수집되는 트리거된 경보로 결합됩니다. 통합 워크플로우는 무단 접근 시도, 멀웨어 등 다양한 유형의 경보를 수집합니다.

이러한 경보는 인스턴스 환경에서 구성한 보안 운영 프로파일을 기반으로 수집됩니다. 모든 경보는 처음에 프로파일에 구성된 경보 유형에 대해 수집됩니다. 수집된 경보를 추가로 필터링하여 보안 인시던트를 생성하는 경보를 지정할 수 있습니다. 예를 들어 고위험으로 식별된 경보에 대해서만 보안 인시던트를 생성하는 필터를 선호할 수 있습니다. 프로파일이 활성화되고 수집된 경보에서 보안 인시던트를 생성하기 전에 필터링된 경보의 개별 필드 값이 미리 보기를 위해 보안 인시던트 레이아웃의 해당 필드에 매핑됩니다.

인스턴스의 이벤트 프로파일 ServiceNow AI Platform 에 대한 경보 이름은 고유해야 하며 특정 시점에 하나의 활성 이벤트 프로파일에만 매핑할 수 있습니다. 다음은 통합 설정의 일부로 서비스에서 구성한 Splunk 트리거된 경보 이름입니다. 사용자 Splunk Enterprise 환경에서 경보를 구성하는 방법에 대한 자세한 내용은 문서를 참조하십시오 통합에 대한 Splunk Enterprise Event Ingestion 콘솔 검색 Splunk Enterprise 저장.

ServiceNow AI Platform 통합 워크플로우를 사용하여 특정 경보를 수집합니다. 엔터프라이즈 콘솔에서 선택 기준을 Splunk 충족하는 모든 경보는 처음에 인스턴스로 ServiceNow AI Platform 수집됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용자의 ServiceNow AI Platform 프로파일은 엔터프라이즈 콘솔의 Splunk 경보를 캡슐화 Splunk 한 것입니다. 프로파일과 함께 수집된 경보와 엔터프라이즈 콘솔에 대한 연결 Splunk 간에는 일대일 관계가 있습니다. 즉, 하나의 연결에 대한 하나의 경보입니다. 콘솔의 검색 헤드에 대한 단일 https 연결이 있습니다 Splunk Enterprise . 단일 검색 헤드에서 여러 경보가 발생할 수 있습니다. 콘솔에서 여러 검색 헤드에 Splunk Enterprise 연결하는 경우 이러한 경보를 수집하려면 인스턴스에 여러 프로필을 ServiceNow AI Platform 생성해야 합니다.

예약된 경보 수집을 위한 프로필을 생성하는 단계

프로시저

1. 경보 ServiceNow AI Platform 에 대한 이벤트 프로파일을 생성하려면 인스턴스에서 **Splunk ES** 통합 〉 **Splunk ES** 이벤트 프로파일.
2. 이벤트 프로파일 양식이 Splunk 표시되지 않으면 진행률 표시줄에서 이름을 클릭합니다.
3. 새로 만들기를 클릭합니다.
4. 필드에 내용을 입력합니다.

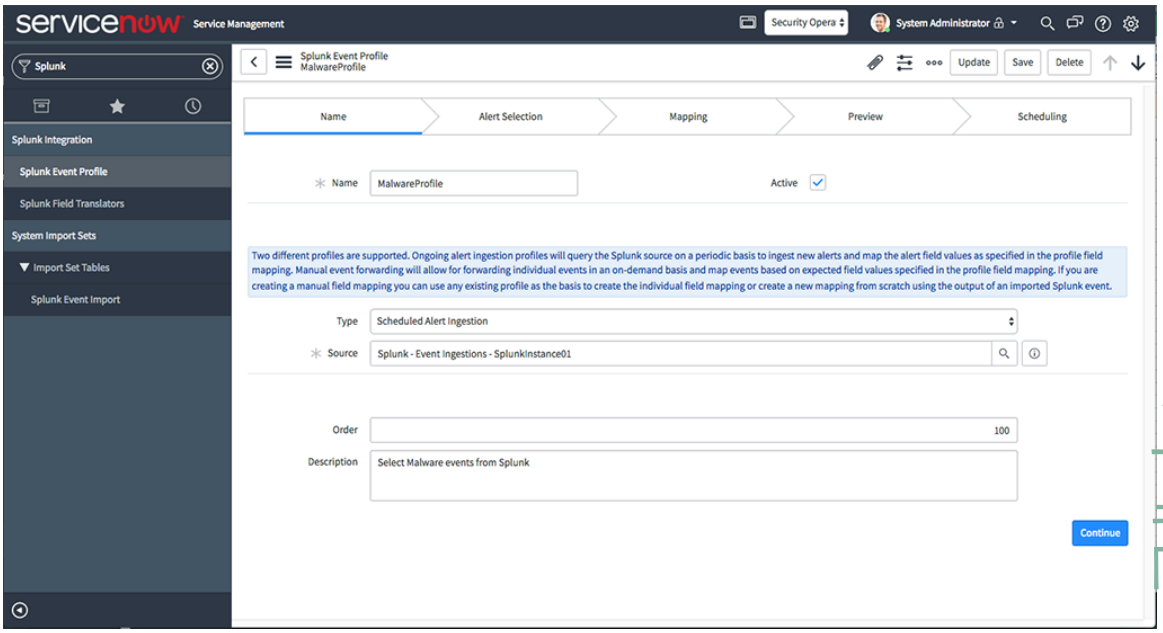
   완료된 양식의 예가 테이블 다음에 나옵니다.

필드	설명
이름	프로파일의 고유한 이름입니다. 이름이 고유하지 않으면 중복 프로파일 이름이 저장되지 않습니다. 인스턴스의 프로파일 이름은 ServiceNow AI Platform 고유해야 합니다.
활성	확인란은 기본적으로 선택이 취소되어 있습니다. 활성 옵션이 비활성화되어 모든 프로필 구성 단계를 완료하고 마침을 클릭할 때까지 선택할 수 없습니다.
유형	선택 목록에서 프로파일 유형을 선택합니다. ○ 예약된 경보 수집 - 이 유형의 프로파일은 사용자가 구성하는 일정에 따라 수집되는 트리거된 경보를 지원합니다. 필드에 내용을 입력하고 계속 을 클릭하여 프로파일의 경보 선택 단계로 이동합니다. ○ 수동 이벤트 전달 - 이 유형의 프로파일은 요청 시 콘솔에서 수동으로 Splunk Enterprise 전달되는 개별 이벤트를 지원합니다. 이러한 유형의 프로파일에 대한 양식을 작성하려면 다음 단계를 참조하십시오.
소스 유형	Splunk 경보를 수집하도록 구성한 서버 또는 검색 끝입니다. 여러 Splunk 서버가 구성된 경우 프로파일에 대해 수집하려는 경보 유형에 적합한 서버를 선택합니다. 값을 입력해야 합니다.
순서	기본값은 100입니다. 이 설정을 기본값으로 둡니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	여러 프로필을 만든 경우 둘 이상의 프로필이 동일한 트리거 조건을 공유할 때 이 값은 런타임 실행 우선 순위를 제공합니다. 숫자가 가장 낮은 프로파일의 워크플로우가 가장 높은 우선순위를 갖습니다.
(선택 사항) 묘사	이 프로파일을 다른 프로파일과 구별하는 데 도움이 되는 텍스트입니다.

다음 그림은 예약된 경보에 대해 작성된 양식의 예입니다.



5. 예약된 경보가 있는 프로파일의 경우 프로파일 구성을 계속하려면 하나의 옵션을 선택합니다.
수동 이벤트 전달을 위한 프로필을 생성하는 단계
6. 수동 이벤트 전달을 지원하는 프로필을 만들려면 다음 단계를 수행합니다.

엔터프라이즈 콘솔에서 요청 Splunk 시 전달하는 이벤트의 경우 개별 필드 매핑을 기존 프로파일에 기반할 수 있습니다. 또는 익스포트한 첨부 파일 데이터에 대한 새 매핑 그리드를 생성할 수 있습니다. 수동으로 전달하는 이벤트는 이벤트 프로파일에 예약되지 않습니다.

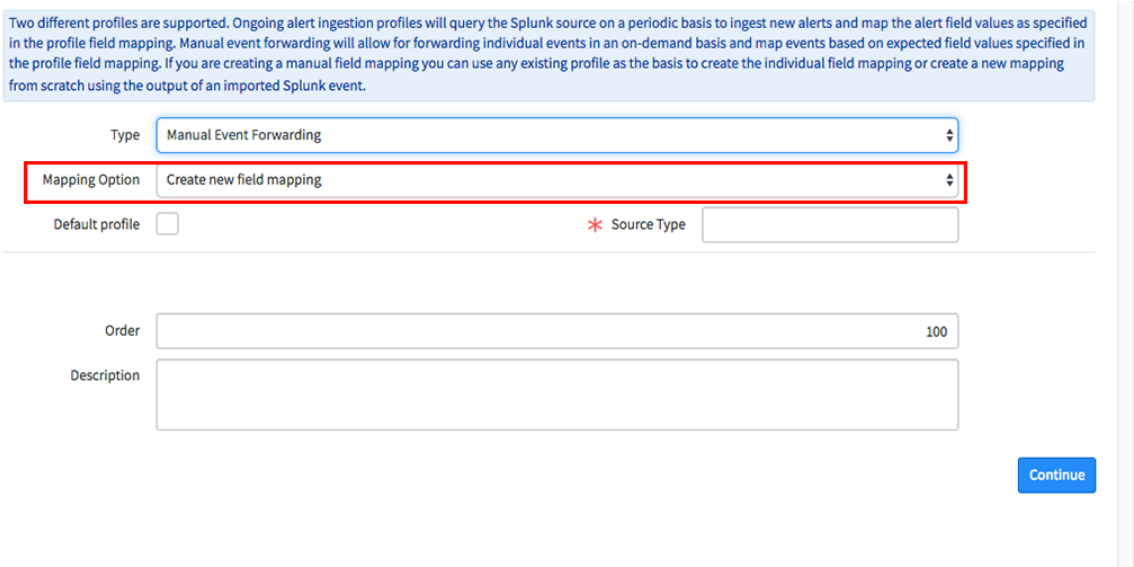
a. 아직 선택하지 않았다면 유형 필드의 선택 목록에서 수동 이벤트 전달을 선택합니다.

b. 표시되는 매핑 옵션 필드의 선택 목록에서 계속할 매핑 옵션 하나를 선택합니다.

매핑 옵션 선택 목록에서 사용 가능한 매핑 옵션에 대한 자세한 내용은 다음 그림과 표를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

새 필드 매핑 옵션 생성



새 필드 매핑 옵션 생성

옵션 또는 필드	설명
새 필드 매핑 옵션 생성	이벤트에 대한 새 필드 매핑입니다. 생성 중인 프로파일과 유사한 기존 필드 매핑이 없는 경우 이 옵션을 선택하여 새 맵을 생성합니다.
기본 프로파일	모든 Splunk 이벤트에 대한 기본 이벤트 전달 프로필입니다. 기본값은 지워져 있습니다 (사용 안 함). 이 옵션을 사용하도록 설정하면 이 프로파일이 수동 이벤트 전달을 위한 기본 프로파일이 됩니다. 이 프로파일은 활성 상태이며 보안 인시던트에 대한 모든 Splunk 이벤트 필드 매핑에 사용되는 유일한 프로파일입니다 SIR . 하나의 프로파일이 전달된 모든 이벤트에 적합합니다. 기본 프로파일 옵션이 활성화된 경우 소스 필드를 사용할 수 없습니다.
소스 유형	Splunk 서버. 기본 프로파일 옵션을 사용하는 경우 이 필드를 사용할 수 없습니다. 사용 가능한 경우 소스 유형 옵션을 사용하면 소스 유형에 따라 보안 인시던트 필드에 고유한 이벤트 필드 매핑을 사용할 수 있습니다 Splunk . 방화벽 로그 이벤트를 엔드포인트 탐지 이벤트와 다르게 관리하려는 경우 소스 유형이

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵션 또는 필드	설명
	다르 Splunk 면 소스 유형을 기반으로 다른 이벤트 프로파일을 생성하여 이 요구 사항을 충족할 수 있습니다.
순서	기본값은 100입니다. 이 설정을 기본값으로 둡니다. 많은 수의 프로파일을 만든 경우 둘 이상의 프로파일이 트리거 조건을 공유할 때 이 값은 런타임 실행 우선순위를 제공합니다. 숫자가 가장 낮은 프로파일의 워크플로우가 가장 높은 우선순위를 갖습니다.
(선택 사항) 묘사	이 프로파일을 다른 프로파일과 구별하는 데 도움이 되는 텍스트입니다.

새 필드 매핑이 있는 프로필의 경우 소스 유형 필드에 값을 입력했는지 확인하고 계속 을 클릭하여 구성의 매핑 단계로 진행합니다.

기존 필드 매핑이 있는 프로필의 자세한 내용은 다음 그림과 표를 참조하십시오.

필드 매핑 옵션에 대한 기존 프로파일 선택

필드 매핑 옵션에 대한 기존 프로파일 선택

옵션 또는 필드	설명
필드 매핑을 위한 기존 프로파일 선택	이벤트에 대한 기존 필드 매핑입니다. Copy from profile(프로파일에서 복사) 필드가 표시됩니다. 다음 단계에 따라 이 프로파일에 대한 기존 필드 매핑을 복사합니다. i. 표시되는 프로필에서 복사 필드 왼쪽에서 검색 아이콘을 클릭합니다. ii. Splunk 표시되는 이벤트 프로파일 목록에서 복사할 맵이 있는 프로파일 이름을 클릭합니다. 프로파일 이름이 프로파일에서 복사 필드에 표시됩니다.
기본 프로파일	모든 Splunk 이벤트에 대한 기본 이벤트 전달 프로필입니다. 기본값은 지워져 있습니다 (사용 안 함). 이 옵션을 사용하도록 설정하면 이 프로파일이 수동 이벤트 전달을 위한 기본 프로파일이 됩니다. 이 프로파일은 활성 상태인 유일한 프로파일입니다. 보안 인시던트에 대한 모든 Splunk 이벤트 필드 매핑에 SIR 사용됩니다. 하나의 프로파일이 전달된 모든 이벤트에 적합합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵션 또는 필드	설명
	기본 프로파일 옵션이 활성화된 경우 소스 필드를 사용할 수 없습니다.
소스 유형	Splunk 서버. 기본 프로파일 옵션을 선택한 경우 이 필드를 사용할 수 없습니다. 사용 가능한 경우 소스 유형 옵션을 사용하면 소스 유형에 따라 보안 인시던트 필드에 고유한 이벤트 필드 매핑을 사용할 수 있습니다 Splunk . 방화벽 로그 이벤트를 엔드포인트 탐지 이벤트와 다르게 관리하려는 경우 소스 유형이 다르 Splunk 면 소스 유형을 기반으로 다른 이벤트 프로파일을 생성하여 이 요구 사항을 충족할 수 있습니다.
순서	기본값은 100입니다. 이 설정을 기본값으로 둡니다. 여러 프로파일을 만든 경우 둘 이상의 프로파일이 트리거 조건을 공유할 때 이 값은 런타임 실행 우선순위를 제공합니다. 숫자가 가장 낮은 프로파일의 워크플로우가 가장 높은 우선순위를 갖습니다.
(선택 사항) 묘사	이 프로파일을 다른 프로파일과 구별하는 데 도움이 되는 텍스트입니다.

프로파일에 대한 기존 매핑을 선택하기 위한 양식의 맨 아래에서 마침 을 클릭하여 프로파일 구성을 완료합니다.

다음에 수행할 작업

예약된 경보와 수동 이벤트 전달 모두를 위한 프로파일을 생성하는 단계를 성공적으로 완료했습니다. 수동 이벤트 전달을 위한 프로필의 경우 프로필 구성을 완료했습니다. 다음 단계는 매핑 단계에서 첨부 파일 데이터를 로드하는 것입니다.
예약된 경보에 대한 프로필의 경우 다음 단계는 자동 수집할 경보를 선택하는 것입니다.

통합에 대해 **Splunk Enterprise Event Ingestion** 예약된 경보 선택

예약된 경보에 대한 프로파일을 생성한 후 보안 인시던트에 ServiceNow AI Platform 보안 인시던트 응답 매핑할 이 프로파일에 대한 경보를 선택합니다Splunk.

시작하기 전에

필요한 역할: sn_si.ingestion_profile_admin

주:
sn_si.admin 역할은 기본적으로 필수 권한을 상속하므로 sn_si.admin 역할을 가진 사용자는 프로필 관리자가 사용할 수 있는 모든 작업을 수행할 수 있습니다.

이 태스크 정보

인스턴스에서 사용 가능한 경보 ServiceNow AI Platform 를 보고 매핑에 사용할 수 있는 필드 값을 알 수 있습니다. 경보를 선택하여 보안 인시던트의 필드에 SIR 값을 매핑하기 전에 기본 양식

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

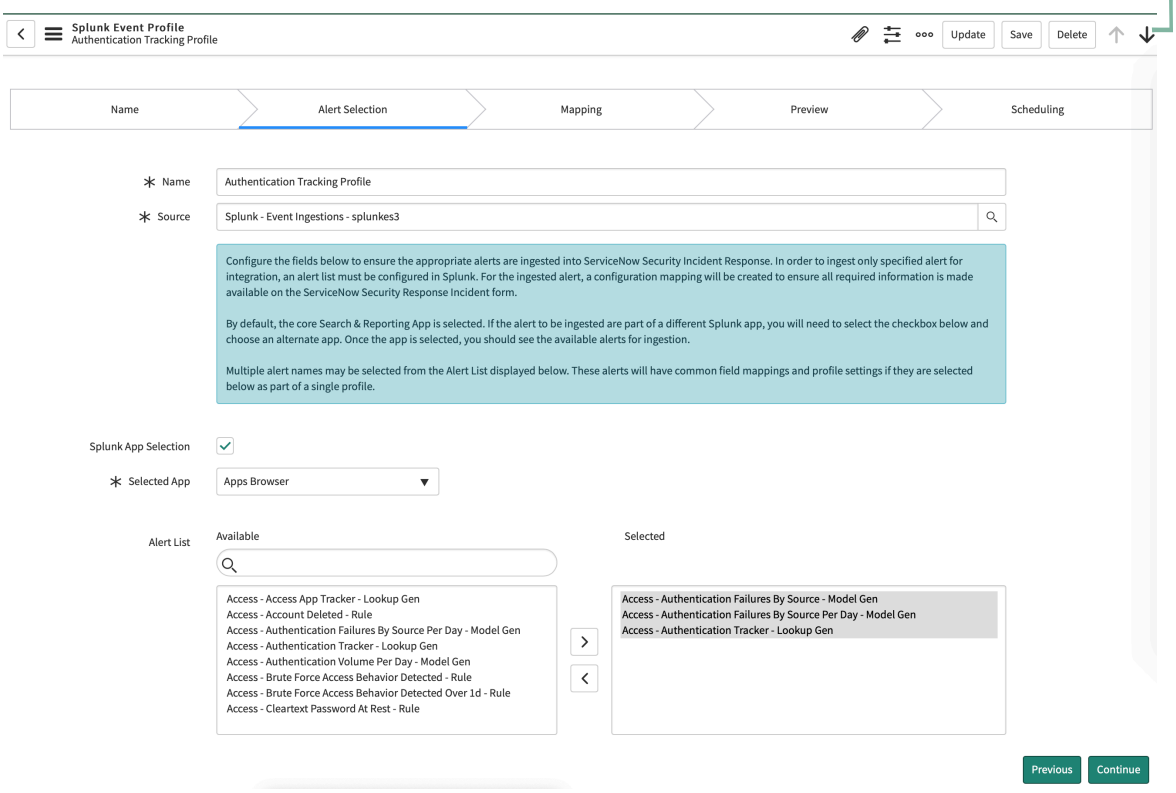
레이아웃에서 예상 결과를 수신하는지 확인합니다. 이 양식의 목록에서 하나의 경보만 선택할 수 있습니다.

프로시저

1. 경보 선택 페이지가 표시되지 않으면 진행률 표시줄에서 선택하여 표시합니다.
   기본적으로 핵심 검색 및 보고 앱이 선택됩니다.
2. 수집할 경보가 다른 Splunk 앱의 일부인 경우 **Splunk** 앱 선택을 선택하고 선택한 앱 목록에서 앱을 Splunk 선택합니다.
3. 경보 목록에서 경보를 선택하고 사용 가능 열에서 선택됨 열로 이동합니다.
   여러 경보를 선택할 수도 있습니다. 경보가 단일 프로파일의 일부로 선택된 경우 경보는 공통 필드 매핑 및 프로파일 설정을 갖게 됩니다.

   이 양식의 경보 목록은 콘솔 Splunk 의 경보 목록과 일치합니다. 이 양식에는 최대 500개의 경보가 표시됩니다. Splunk 콘솔의 경보 페이지에 나열된 경보가 500개를 초과하는 경우 인스턴스의 이 양식 ServiceNow AI Platform 에는 처음 500개의 경보만 표시됩니다.

옵션	설명
경보 목록 검색 필드에 텍스트를 입력합니다.	검색 필드 아래의 열은 입력한 텍스트를 기반으로 사용 가능한 옵션을 사용하여 필터링됩니다. 경보를 선택하고 화살표 키를 사용하여 선택한 경보를 사용 가능 에서 선택됨으로 옮깁니다.
경보 목록에서 경보를 두 번 클릭합니다.	선택됨 열이 선택 항목으로 채워집니다.
경보 목록에서 경보 규칙을 한 번 클릭합니다.	경보가 선택됩니다. 화살표 키를 사용하여 선택한 경보를 사용 가능 에서 선택됨으로 옮깁니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 계속하려면 하나의 옵션을 선택하십시오.

다음에 수행할 작업
예약된 경보 프로파일에 대한 경보를 성공적으로 선택했습니다. 다음 단계는 경보 값을 보안 인시던트의 필드에 매핑하는 것입니다.

통합을 위한 **Splunk Enterprise Event Ingestion** 경보 및 이벤트 매핑

예약된 경보 수집 또는 수동 이벤트 전달을 위한 소스를 식별한 후 다음 단계는 개별 이벤트 필드를 (SIR) 보안 인시던트의 필드에 매핑하는 ServiceNow AI Platform 보안 인시던트 응답 것입니다.

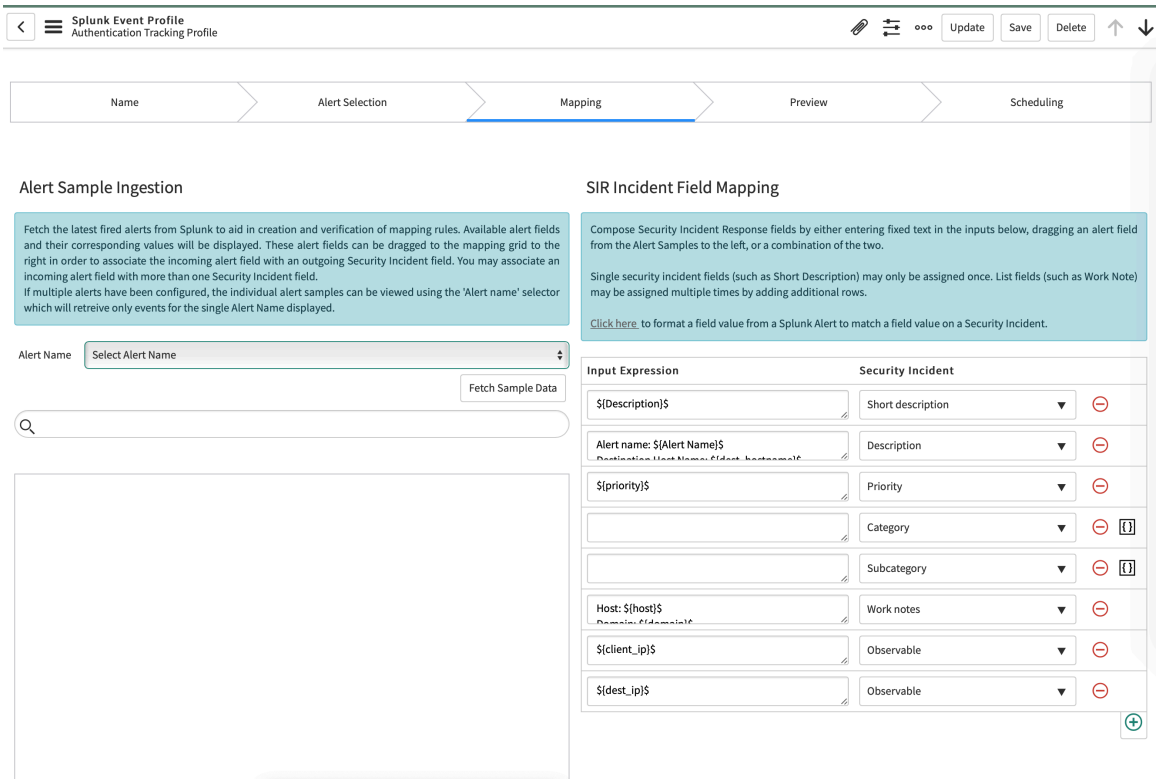
경보 및 이벤트 매핑 개요

매핑 단계의 경우 **sn_si.ingestion_profile_admin** 역할을 가진 사용자는 콘솔에서 샘플 경보 Splunk Enterprise 를 수집하거나 이벤트에 대한 이벤트 데이터를 익스포트합니다 Splunk Enterprise .

다음 그림은 각 유형의 이벤트 프로파일에 대해 제공되는 기본 매핑 그리드의 예입니다. 이 기본 매핑은 편집할 수 있습니다. 이렇게 수정하면 보안 인시던트를 채우는 필드를 사용자 지정할 수 있습니다. 매핑 단계에서는 이벤트 필드를 추가하거나 제거하면 보안 인시던트 필드 값에 미치는 영향을 SIR 시각화할 수 있습니다.

경보 이름을 선택하고 샘플 데이터Splunk 가져오기를 클릭하면 프로파일에서 샘플 경보를 수집할 때 양식 왼쪽에 경보 필드 값이 채워집니다. Splunk 보안 인시던트 필드에 매핑되는 경보 필드입니다SIR.

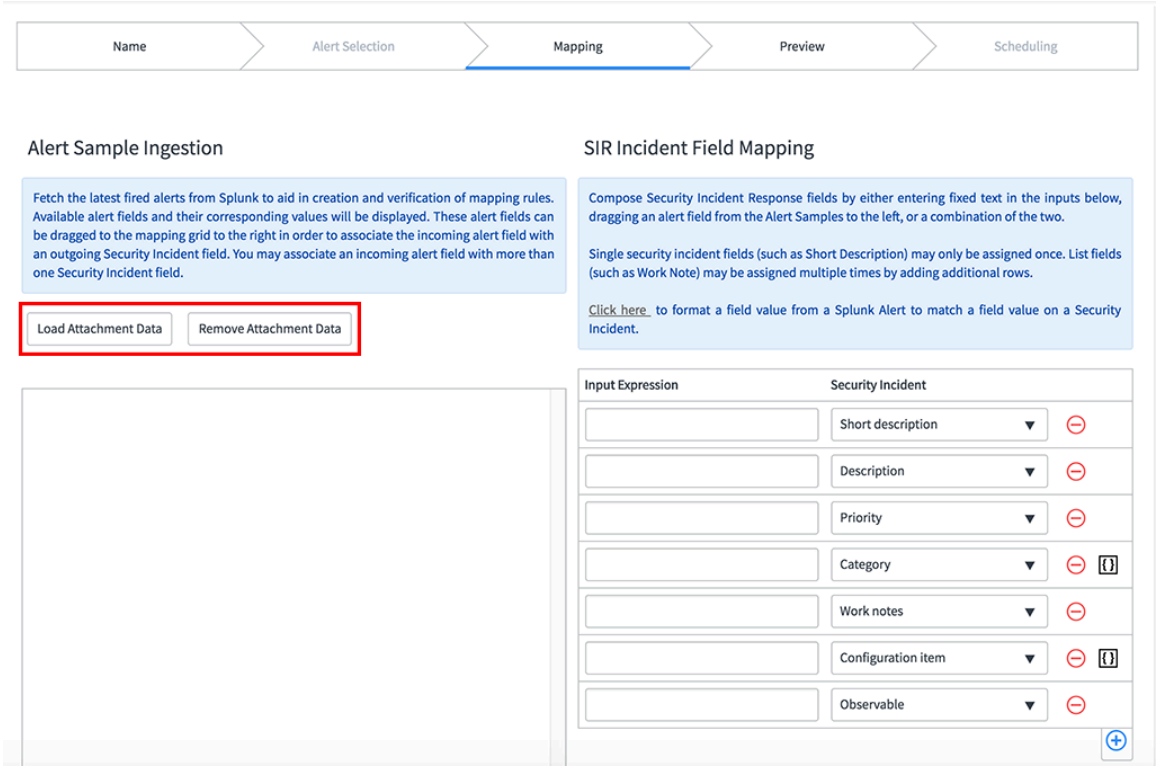
경보에 대한 기본 매핑 양식



전달된 이벤트에 Splunk 대한 첨부 파일 데이터를 로드하기 위해 클릭하면 양식 왼쪽에 이벤트 필드가 채워집니다. Splunk 보안 인시던트 필드에 매핑되는 데이터 필드입니다SIR.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

전달된 이벤트에 대한 기본 매핑 양식



필드 매핑 구성 단계에서 수집할 몇 가지 샘플 경보 Splunk 를 콘솔에서 검토하는 것을 선호할 수 있습니다. 이 단계는 진행률 표시줄에 매핑 이라고 표시됩니다. 이 페이지가 표시되지 않으면 진행률 표시줄에서 매핑 을 클릭합니다.

엔터프라이즈 콘솔에서 요청 Splunk 시 경보를 매핑하고 이벤트를 익스포트하는 데에는 다음과 같은 개념과 작업이 포함됩니다.

- 자동으로 수집된 경보 프로파일의 샘플 데이터를 가져옵니다. 콘솔에서 발생한 경보 Splunk Enterprise 에서 데이터를 가져오면(끌어오면) 사용 가능한 경보 필드와 해당 값이 매핑 양식의 왼쪽에 있는 기본 매핑 레이아웃에 표시됩니다. 끌어온 경보 ID의 값을 볼 수 있는 탭이 표시됩니다. 양식 왼쪽에 있는 경보 샘플 수집 섹션의 모든 중요 필드가 양식 오른쪽의 그리드에 매핑되는지 확인합니다.
- 필요한 경우 수동으로 전달된 이벤트 프로파일에 대한 이벤트 샘플 데이터를 로드합니다. 이러한 이벤트의 샘플 데이터는 콘솔에서 .xml 파일로 Splunk Enterprise 익스포트되어 인스턴스로 ServiceNow AI Platform# 로드됩니다. 임포트한 데이터는 양식 왼쪽의 경보 샘플 수집 섹션에 표시됩니다.
- 왼쪽에서 경보를 끌어서 오른쪽의 매핑 그리드에 놓아 매핑 구성을 편집합니다. 오른쪽의 매핑 그리드는 수신 경보 필드를 발신 보안 인시던트 필드와 연결합니다.
- 필드를 추가하거나 제거하여 매핑 그리드를 사용자 지정합니다. 제공된 색상 코딩으로 간과되거나 중복된 필드를 추적합니다.
- 애플리케이션에 수집할 SIR 경보와 필터링할 경보를 지정할 수 있도록 필터 조건을 설정합니다.
- 중복 인시던트를 방지하기 위해 수신 경보를 기존 SIR 보안 인시던트로 집계하는 추가 인시던트 필드 기준을 정의합니다. 이 추가 필터링은 모든 관련 보안 이벤트 데이터를 단일 보안 인시던트에 배치하여 활성 상태의 중복 보안 인시던트 수를 줄일 수 있습니다.
- 경우에 따라 엔터프라이즈 콘솔의 Splunk 이벤트 필드 값이 보안 인시던트의 SIR 필드로 직접 변환되지 않을 수 있습니다. 이러한 값의 경우 스크립트 편집기를 사용하여 매핑 단계 중에 보안 인시던트의 필드 값에 대한 형식을 지정할 수 있습니다. 비슷하지만 동일하지는 않은 값의 형식을

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

지정하려면 스크립트 편집기를 사용하십시오. 예를 들어 스크립트 편집기를 사용하면 콘솔의 Splunk 맬웨어 경보 및 바이러스 감염 필드 값이 모두 보안 인시던트의 범주 필드에 SIR 있는 악성 코드 활동으로 변환됩니다.

예약된 경보 프로파일

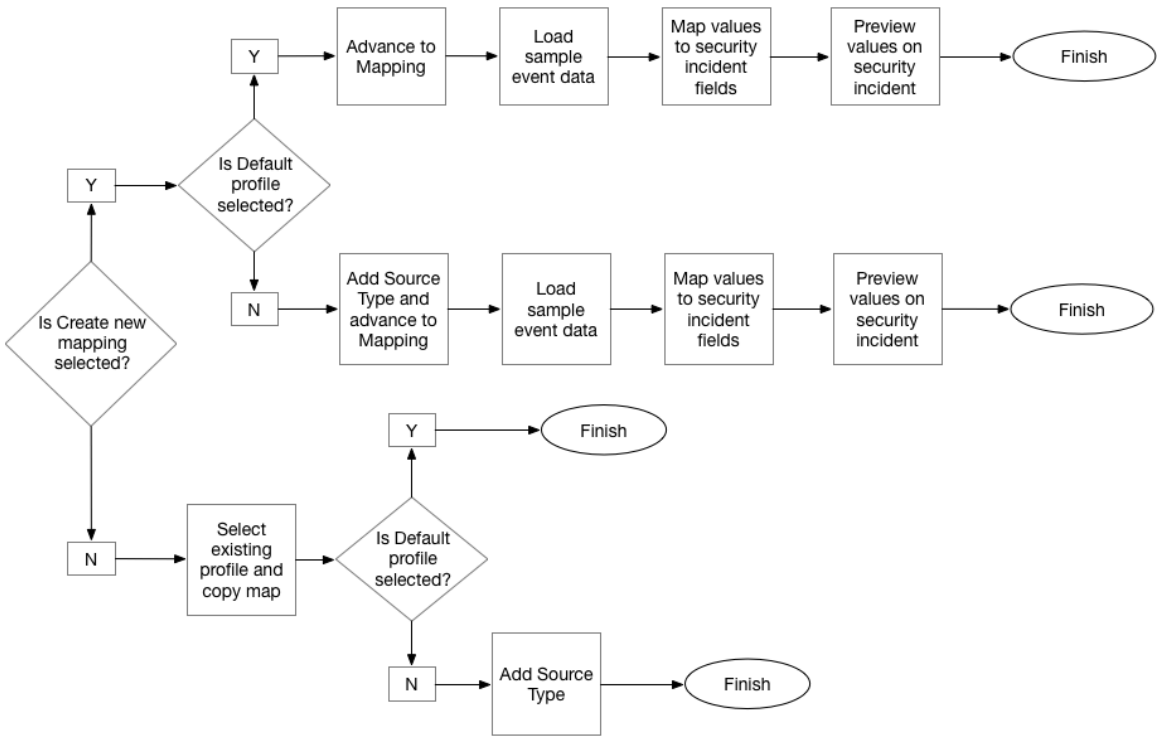
예약된 경보 프로필을 만든 후 구성에 대한 프로세스 흐름이 다음 그림에 표시됩니다.

예약된 경보 프로파일의 프로세스 흐름

수동 이벤트 전달 프로파일

이벤트에 대한 프로필을 만든 후 구성에 대한 프로세스 흐름이 다음 그림에 표시됩니다.

이벤트 프로파일의 프로세스 흐름



다음 단계는 트리거된 경보를 수집하거나 데이터를 익스포트하고 값을 보안 인시던트 필드에 매핑하는 SIR 것입니다.

통합에 대한 **Splunk Enterprise Event Ingestion** 경보 매핑

이벤트 필드 매핑 단계에서는 트리거된 경보 또는 임포트된 이벤트 데이터의 개별 이벤트 필드를 (SIR) 보안 인시던트의 ServiceNow AI Platform 보안 인시던트 응답 필드에 매핑합니다.

시작하기 전에
필요한 역할: sn_si.ingestion_profile_admin

주:
sn_si.admin 역할은 기본적으로 필수 권한을 상속하므로 sn_si.admin 역할을 가진 사용자는 프로필 관리자가 사용할 수 있는 모든 작업을 수행할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보

기본 보안 인시던트 필드의 미리 구성된 매핑 그리드를 편집할 수 있습니다. 이벤트 필드의 색상 코딩은 이미 매핑한 필드 값을 모니터링하는 데 도움이 됩니다. 이 단계는 편집 내용이 보안 인시던트의 필드에 미치는 영향을 시각화하는 데 도움이 됩니다.

양식 왼쪽의 경보 샘플 수집 열에서 오른쪽에 있는 SIR 인시던트 필드 매핑 열의 보안 인시던트 필드에 최대 5개의 경보를 매핑합니다.

양식 오른쪽의 매핑 그리드에서 필드를 추가하거나 제거하여 사용자 지정 맵을 생성합니다. 필드를 사용자 지정하면 보안 인시던트의 기본 매핑 그리드에 표시되지 않는 필드를 매핑 Splunk 할 수 있습니다 SIR .

프로시저

1. 매핑 양식이 표시되지 않으면 진행률 표시줄에서 매핑 을 클릭합니다.
2. 예약된 경보가 있는 프로파일의 경우 경보 샘플 수집 아래에서 경보 이름 에서 경보를 선택하고 샘플 데이터 가져오기 를 클릭하여 발생한 경보 Splunk Enterprise 의 최신 인스턴스를 콘솔에서 끌어옵니다.

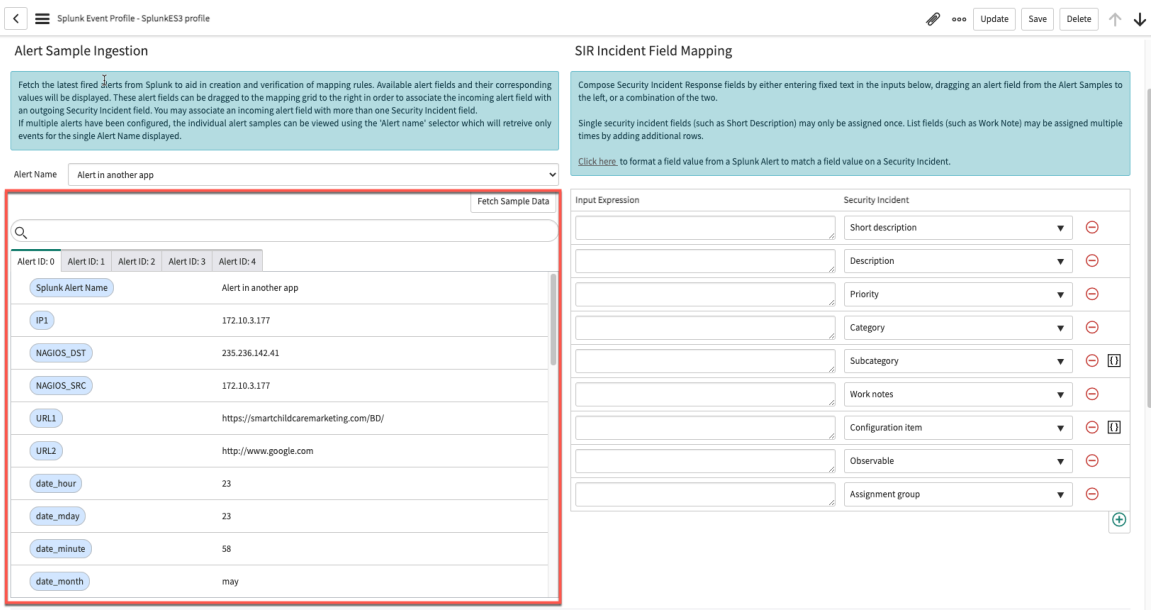
   경보는 탭으로 표시됩니다. 가장 최근의 경보를 최대 5개까지 수집할 수 있습니다.

   샘플 이벤트를 끌어오기에는 몇 분 정도 걸릴 수 있습니다. 트랜잭션이 작동 중임을 나타내는 메시지가 화면 맨 위에 표시됩니다.

   > **주:**
   > 추가 매핑 필드인 **Splunk** 경보 이름이 통합에 의해 추가되어 의 소스 경보 규칙에 Splunk이벤트를 추적할 수 있습니다. 이는 여러 Splunk 경보가 단일 프로파일로 결합되는 시나리오에서 유용할 수 있습니다.

   단일 필드에 여러 값이 포함되어 있으면 이러한 값이 구문 분석되어 SIR 인시던트 필드 매핑 섹션의 개별 필드 항목에 매핑됩니다. 예를 들어 소스 IP 주소, 자산 이름 또는 URL에는 여러 옵저버블 필드 항목 또는 여러 CI가 있을 수 있으며, 이러한 항목은 SIR 인시던트 필드 매핑 섹션의 개별 필드 항목에 구문 분석 및 매핑됩니다.

   다음 그림에서는 끌어오기가 완료된 후 수집된 경보 또는 임포트된 샘플 이벤트에 대한 필드 이름 값 쌍이 이 양식의 왼쪽에 표시됩니다. 이러한 값은 양식의 SIR 인시던트 필드 매핑 측면에 있는 보안 인시던트 필드에 매핑하는 값입니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 예약된 경보 프로파일의 경우 5단계로 진행하여 값을 매핑합니다.
4. 또는 콘솔에서 익스포트 Splunk Enterprise 하려는 이벤트 유형의 프로파일의 경우 다음 단계에 따라 인스턴스에 첨부 파일 데이터를 ServiceNow AI Platform# 업로드합니다.

   a. 아직 로그인하지 않았다면 콘솔에 로그인하십시오 Splunk Enterprise .

   b. 검색 탭으로 이동하여 익스포트하려는 이벤트 데이터가 있는 검색의 이름을 입력합니다.

      예를 들어 맬웨어는 이 통합의 워크플로우와 함께 전달할 수 있는 모든 맬웨어 이벤트에 사용되는 검색어입니다.

   c. 이벤트를 확장하고 필드 열에서 임포트할 필드를 선택합니다.

      이러한 필드는 익스포트되어 인스턴스의 매핑 페이지에 ServiceNow AI Platform# 표시되는 필드-값 쌍입니다.

   d. Splunk Enterprise 콘솔의 검색 페이지 오른쪽 상단에서 익스포트 아이콘을 클릭합니다.

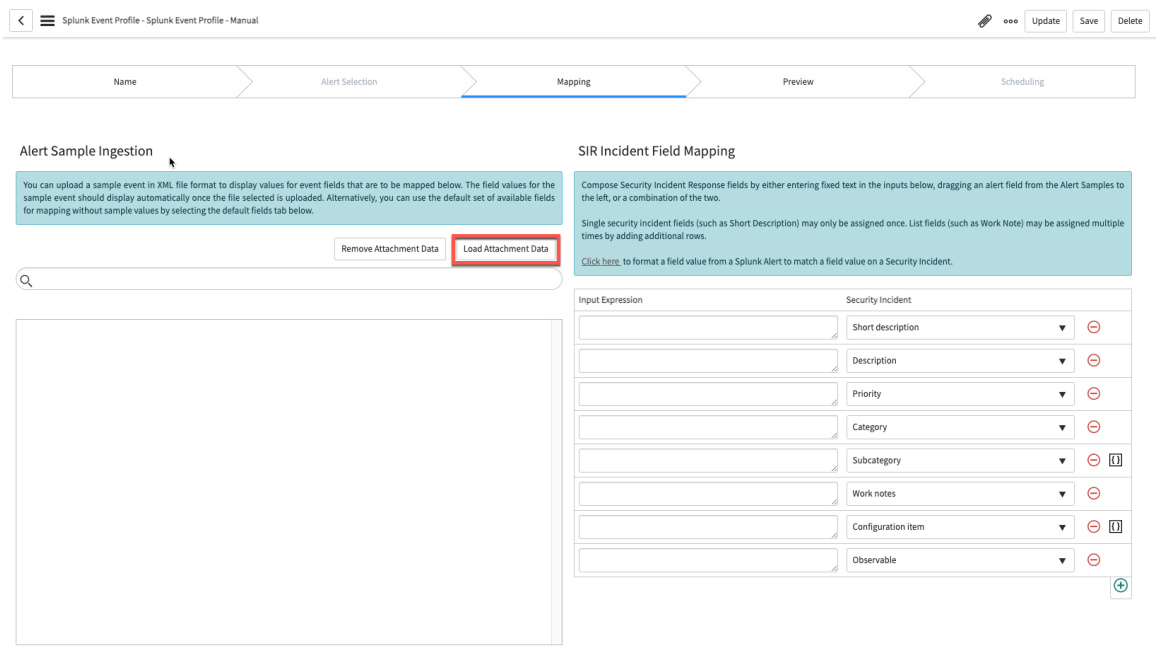
   e. 표시되는 대화 상자의 형식 필드 목록에서 **XML** 형식을 클릭합니다.

   f. 옵션: 새 파일 이름을 입력합니다.

   g. 익스포트를 클릭합니다.
   파일이 인스턴스에 다운로드 ServiceNow AI Platform# 됩니다.

   h. 인스턴스에 매핑 페이지가 아직 표시되어 ServiceNow AI Platform# 있지 않으면 진행률 표시줄에서 매핑 을 클릭합니다.

   i. 경보 샘플 수집 열에서 첨부 파일 데이터 로드를 클릭합니다.



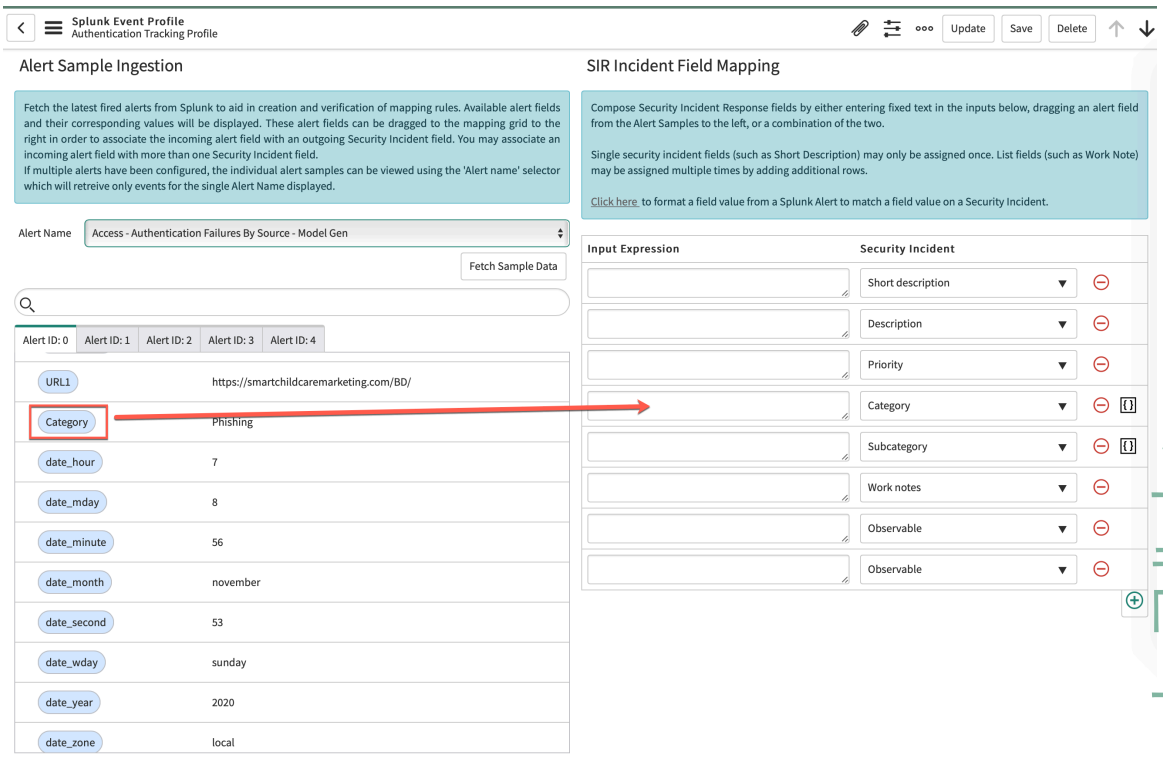
   j. 표시되는 대화 상자에서 파일 선택을 클릭하고 내보낸 .xml 파일을 탐색한 다음 열기를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이벤트에 대해 익스포트한 필드의 값 쌍이 매핑 양식의 왼쪽에 표시됩니다.

다음 그림에서는 수집된 예약된 경보에 대한 데이터 쌍이 이 양식의 왼쪽에 표시됩니다. 임포트한 이벤트의 값 쌍도 양식의 이 쪽에 표시됩니다. 이러한 값은 양식의 인시던트 필드 매핑 측면에 있는 보안 인시던트 필드에 매핑하는 필드 값입니다.

5. 양식 왼쪽의 필드 값을 양식 오른쪽에 있는 보안 인시던트의 필드에 매핑하려면 양식 왼쪽에 있는 파란색 필드 이름을 길게 클릭합니다.
6. 필드 이름(예: ##)을 끌어서 보안 인시던트 열의 필드 이름 옆에 있는 입력 식 열의 필드에 놓습니다.

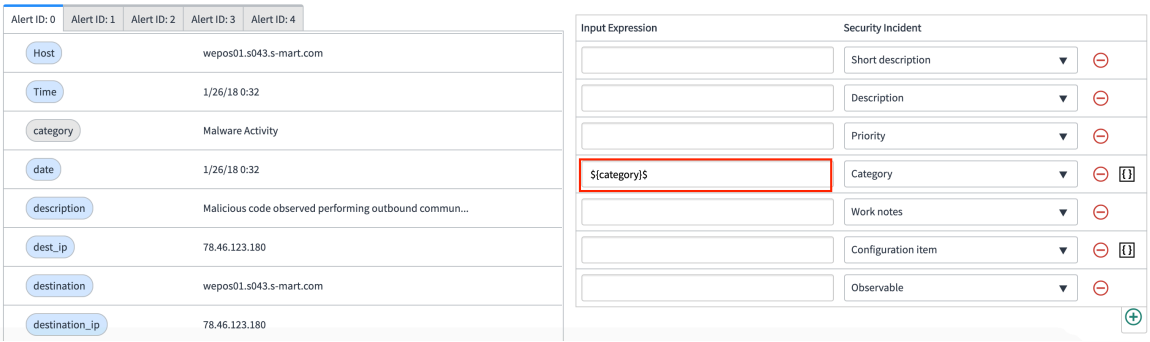


필드 값이 입력 식 열에 표시됩니다. 다음 이미지에서 ## 는 보안 인시던트의 ## 필드에 매핑되어 있습니다. 그러나 왼쪽의 모든 값을 오른쪽의 필드와 일치시킬 수 있습니다. 미리 보기 단계에서 보안 인시던트에 값이 올바르게 매핑되었는지 확인합니다.

매핑 프로세스에서 이벤트가 간과되거나 중복되지 않도록 하기 위해 필드는 색으로 구분됩니다. 왼쪽의 연한 파란색 필드는 필드가 아직 선택되지 않았으며 보안 인시던트에 매핑되지 않았음을 나타냅니다. 수신 경보 필드를 보안 인시던트의 둘 이상의 필드와 연결하는 것을 선호할 수 있습니다.

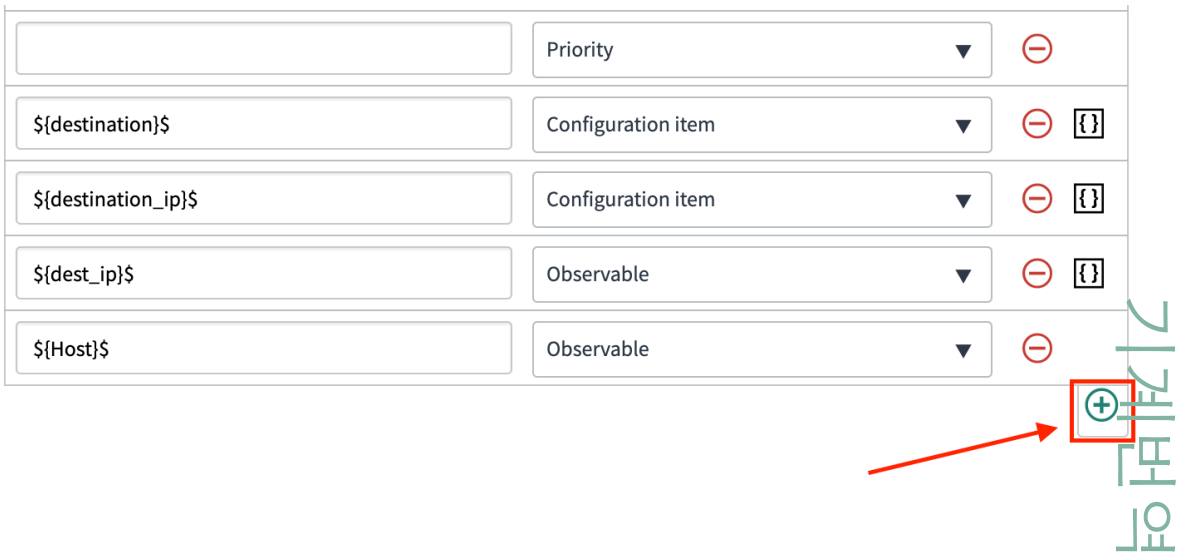
회색 필드는 필드가 선택되었고 보안 인시던트의 필드에 매핑되었음을 나타냅니다. 이 색상 코딩은 경우에 따라 경보 이벤트 필드가 한 번만 할당될 수 있기 때문에 매핑을 추적하는 데 도움이 됩니다. 예를 들어 짧은 설명과 같은 필드에는 값을 한 번만 할당할 수 있습니다. 그러나 매핑 그리드에 행을 추가하여 작업 메모와 같은 목록 필드를 여러 번 할당할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



7. 양식 오른쪽에 있는 보안 인시던트의 기본 매핑에 필드를 추가하려면 다음 단계를 수행합니다.

a. 양식 오른쪽의 SIR 인시던트 필드 매핑 섹션 그리드 하단에서 더하기 아이콘을 클릭합니다.

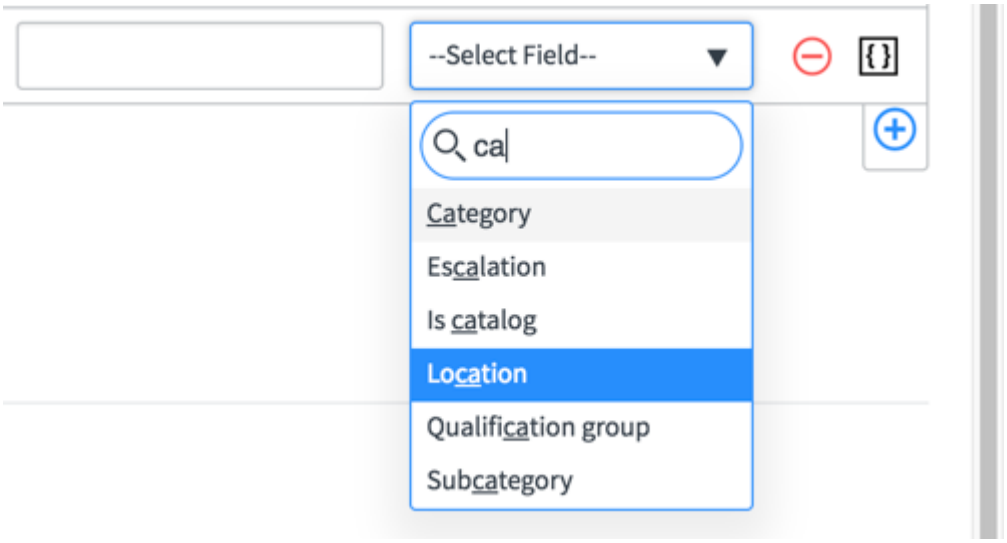


새 필드가 표시됩니다.

b. 보안 인시던트 열에서 표시되는 목록을 확장하고 필드를 선택합니다.

새 필드의 확장된 목록에서 일부 필드는 음영 처리됩니다. 다음 그림에서 ## 는 보안 인시던트에 매핑되었기 때문에 회색 배경입니다. 양식 왼쪽에 있는 경보 필드에 대한 색상 코딩과 비슷하게 오른쪽에 있는 보안 인시던트 필드에 대한 이 색상 코딩은 매핑을 추적하는 데 도움이 됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

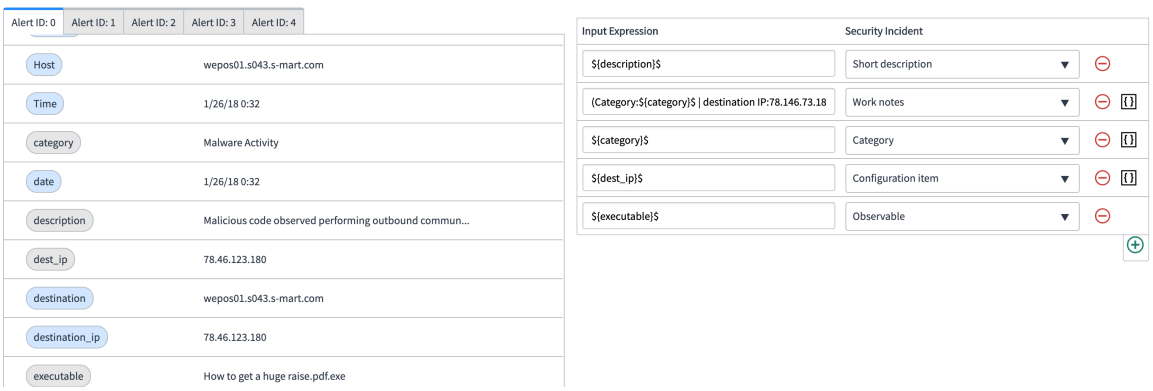


주:
동일한 보안 인시던트에 여러 옵저버블을 표시할 수 있도록 옵저버블 필드를 서로 다른 값으로 여러 번 매핑할 수 있습니다. 마찬가지로 구성 항목 및 작업 메모 필드는 여러 값을 지원합니다. 여러 값을 지원할 수 없는 필드에 두 값을 매핑하려고 하면 인시던트를 미리 볼 때 필드에 값이 없다는 오류 메시지가 표시됩니다. 마찬가지로 보안 인시던트의 필드에 여러 옵션을 선택할 수 있는 목록이 있고 목록에 표시되지 않은 해당 필드에 옵션을 매핑하려고 하면 보안 인시던트에 필드가 채워지지 않습니다.

c. 또는 새 행의 검색 필드에 값을 입력합니다.

d. 양식의 왼쪽에서 왼쪽 단추를 클릭하여 입력 식 필드에 넣을 경보 **ID** 를 선택합니다. 끌기 기능을 사용하여 새 필드 옆에 매핑합니다.

8. 필드를 추가 또는 제거하고 맵에 값을 추가하여 매핑을 계속합니다.
다음 그림은 편집된 매핑 그리드의 예입니다. 오른쪽의 하단 필드에는 작업 메모 필드가 추가되며 둘 이상의 값이 있습니다. 값은 공백과 문장 부호로 구분됩니다(Category:${category} | destination IP:78.146.73.180).



미리 보기에서 이러한 값은 보안 인시던트의 작업 메모에 표시됩니다. 값은 그리드에 추가한 필드에 대한 것이고 작업 메모 필드에 매핑된 값이 여러 개 있기 때문에 입력한 대로 값이 표시됩니다. 이 예에서는 필드에 입력한 공백과 구두점이 관련 항목 섹션에 보안 인시던트 미리 보기의 작업 메모로 표시됩니다.

다음 이미지는 이전 이미지의 값이 보안 인시던트에 표시되는 방식의 예입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Related Items

Field Name	Field Value
Work Note	Category: Malware Activity | destination IP: 78.46.123.180
Work Note	Source: MalwareDemoData Top 100 events with 15 host machines

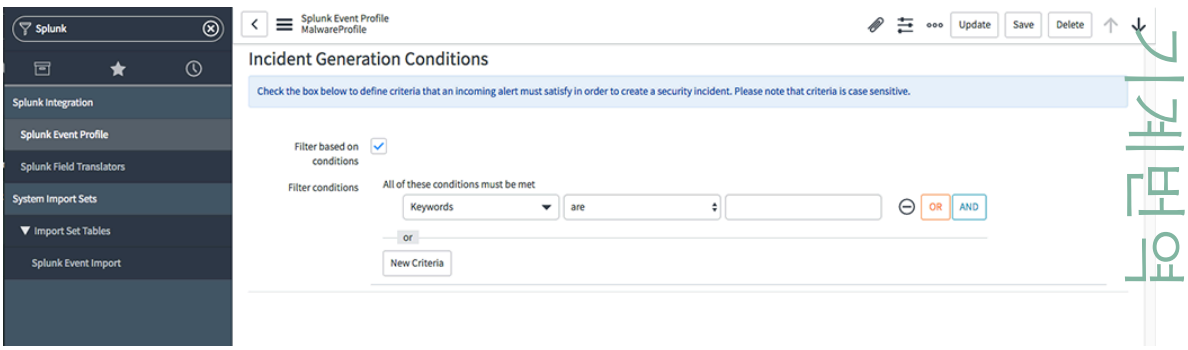
인시던트 생성 필터링 조건

9. 옵션: 이전 필드 수준 매핑 단계를 완료한 후 필터 조건 작성기에서 동일한 필드 값을 사용하여 수신되는 경보가 충족해야 보안 인시던트를 생성할 수 있는 추가 기준을 정의할 수 있습니다 SIR . 필터링 조건을 설정하려면 다음 단계를 수행합니다.

a. 양식에서 인시던트 생성 조건 섹션으로 스크롤하고 조건을 기준으로 필터링 확인란을 선택하여 옵션을 활성화합니다.

(Optional) 필터 조건 작성기가 표시됩니다. 이러한 필터를 사용하여 필드에 설명된 특정 조건과 일치하는 보안 인시던트를 생성합니다.

필터 조건 작성기의 첫 번째 필드에 대한 목록의 옵션은 수집한 경보에 대한 경보 샘플 수집 섹션에 표시되는 필드와 일치합니다. 이러한 필드는 동적이며 수집하는 경보 또는 수동으로 전달하는 이벤트에 따라 Splunk 변경됩니다. 입력하는 기준은 대/소문자를 구분하며 경보 또는 이벤트의 값과 Splunk Enterprise 정확히 일치해야 합니다. 필터 필드에 입력할 값을 잘 모르는 경우에는 콘솔로 돌아가서 Splunk Enterprise 키워드에 대한 경보 및 이벤트를 검토하는 것이 좋습니다.



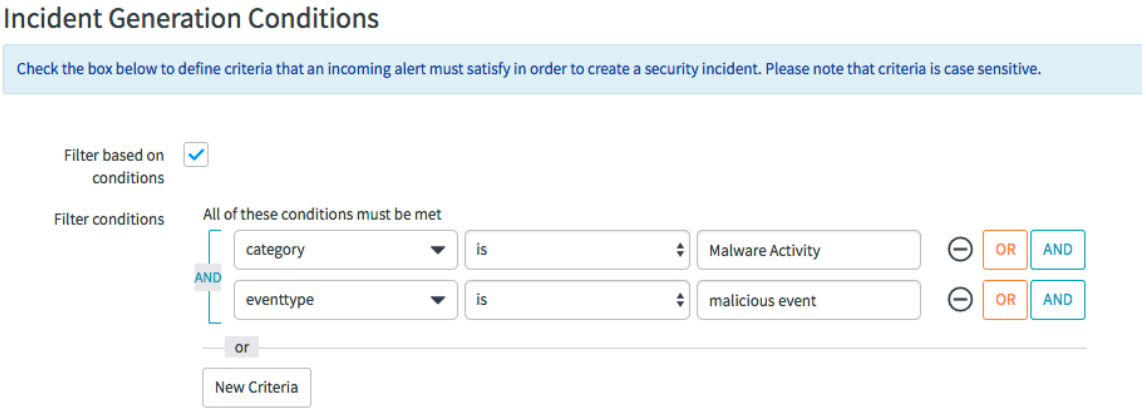
b. 조건 작성기의 목록과 필드를 사용하여 첫 번째 행에 대한 필터를 설정합니다.

c. 조건을 더 추가하려면 필드 오른쪽에서 AND 또는 **OR**을 클릭합니다.
AND를 선택하면 모든 조건이 일치해야 합니다. **OR**을 선택하면 두 조건을 일치시킬 수 있습니다.

d. 옵션: 두 번째 행에서 두 번째 필터 조건을 설정합니다.

(Optional) 다음 이미지는 보안 인시던트가 생성되기 전에 일치해야 하는 두 가지 조건이 있는 예입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



(Optional) 입력한 두 필터링 조건이 일치하는 경우에만 보안 인시던트가 생성되도록 트리거 조건을 설정했습니다.

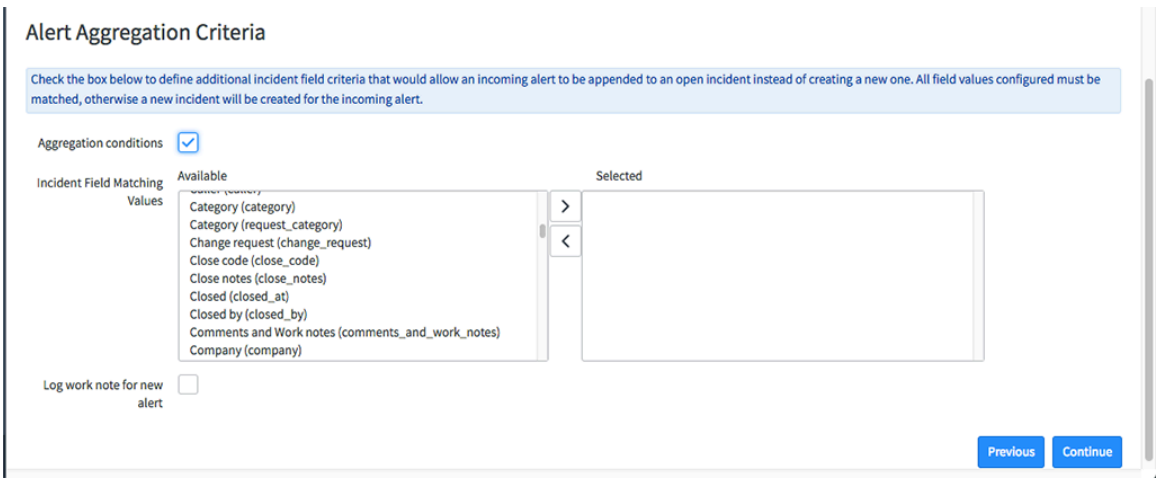
이러한 유형의 필터링은 보안 이벤트를 격리하는 데 유용하며 생성하는 보안 인시던트 수를 제한합니다. 추가 필터링 기준이 설정되면 쿼리 또는 트리거된 경보 구성을 변경할 Splunk 필요 없이 필요한 경보만 수집됩니다.

중복 인시던트를 방지하기 위한 경보 집계

10. 옵션: 중복 보안 인시던트가 생성되지 않도록 하려면 수신 경보가 미해결 보안 인시던트로 집계되도록 추가 인시던트 필드 기준을 정의합니다.
이 기준을 설정하려면 다음 단계를 수행합니다.

a. 양식의 경보 집계 기준 섹션으로 스크롤하고 집계 조건 확인란을 선택하여 이 옵션을 활성화합니다.

(Optional) 인시던트 필드 일치 값 열이 표시됩니다. 이러한 필드 이름은 보안 인시던트에 구성된 SIR 사용자 지정 필드를 포함하는 보안 인시던트의 필드입니다.

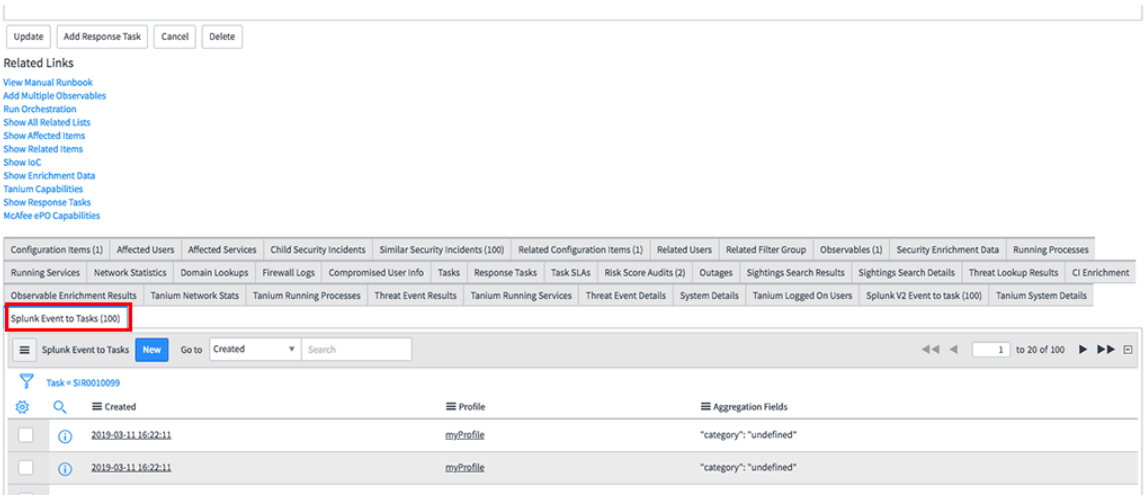


b. 사용 가능 목록에서 기존 보안 인시던트 ServiceNow AI Platform 와 일치시킬 필드 값을 선택하고 선택됨 목록으로 이동합니다.

(Optional) 이 수신 경보를 기존 보안 인시던트에 추가하려면 선택하는 모든 필드 값이 일치해야 합니다. 이 기준에 사용할 보안 인시던트의 필드 값을 검토하려면 다음으로 이동하십시오.
인시던트 〉 모든 인시던트 표시.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

새 경보가 매핑 단계의 집계 필드 조건에서 선택한 모든 값과 일치하면 가장 최근에 열린 보안 인시던트에 동일한 필드 값으로 경보가 자동으로 추가됩니다. 보안 인시던트를 담당하는 sn_si.analyst 역할을 가진 사용자는 보안 인시던트의 관련 목록에서 추가된 모든 집계 경보를 볼 수 있습니다. 보안 인시던트에 대해 집계된 모든 경보는 작업에 대한 이벤트 관련 목록에 표시됩니다 Splunk . 이 목록에는 관련 타임스탬프 및 집계된 필드 값이 자세히 설명되어 있습니다. 이 정보는 기존 보안 인시던트에 경보가 추가되는 이유를 이해하는 데 도움이 됩니다. 이 탭이 표시되지 않으면 관련 링크 아래에 있는 기록의 왼쪽으로 스크롤하여 모든 관련 목록 표시 링크를 클릭합니다.



c. 옵션: 보안 인시던트에 최근에 추가된 새 경보에 대한 작업 메모를 기록하려면 이 확인란을 선택하여 이 옵션을 활성화합니다.
작업 메모는 경보 상세 정보에 대한 링크와 함께 새 경보가 추가되었음을 기록합니다.

경보 또는 이벤트의 값을 Splunk 보안 인시던트의 SIR 필드에 매핑했습니다. 또한 필터링 기준을 사용하여 보안 인시던트 생성을 제한하는 추가 조건을 구성했습니다. 또한 기존 SIR 보안 인시던트에 경보 또는 이벤트를 추가했습니다.

11. 옵션: 스크립트 편집기를 열고 계속 편집합니다.

(Optional) 스크립트 편집기에 대한 자세한 내용은 문서를 참조하십시오 스크립트 편집기를 사용하여 통합에 대한 경보 값의 서식을 Splunk Enterprise Event Ingestion 지정합니다.

12. 하나를 선택하여 프로파일 구성을 계속합니다.

다음에 수행할 작업
다음 단계는 보안 인시던트에 매핑한 값을 미리 보는 것입니다.

통합에 대한 **Splunk Enterprise Event Ingestion** 보안 인시던트 미리 보기

매핑 단계를 완료한 후 (SIR) 보안 인시던트에서 ServiceNow AI Platform# 보안 인시던트 응답 매핑한 값을 미리 봅니다. 이 미리 보기 단계를 통해 보안 인시던트에 표시할 경보 필드를 모두 매핑했는지 확인할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.ingestion_profile_admin

주:
sn_si.admin 역할은 기본적으로 필수 권한을 상속하므로 sn_si.admin 역할을 가진 사용자는 프로필 관리자가 사용할 수 있는 모든 작업을 수행할 수 있습니다.

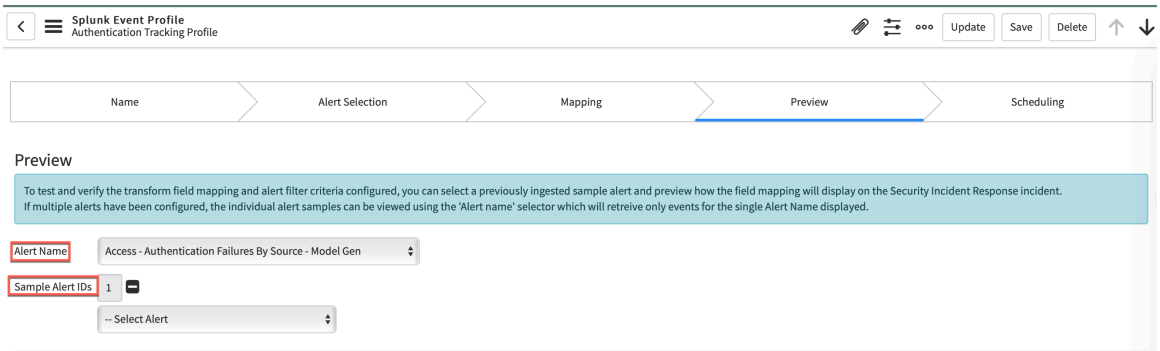
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보

보안 인시던트를 미리 보고 필요에 따라 매핑을 다시 편집하여 오류가 있는 필드를 수정하거나 누락된 데이터를 채웁니다. 미리 보기가 성공적으로 완료되지 않으면 예약 단계로 진행할 수 없습니다. SIR 보안 인시던트 미리 보기는 제품에 실제 인시던트 SIR 로 저장되지 않습니다.

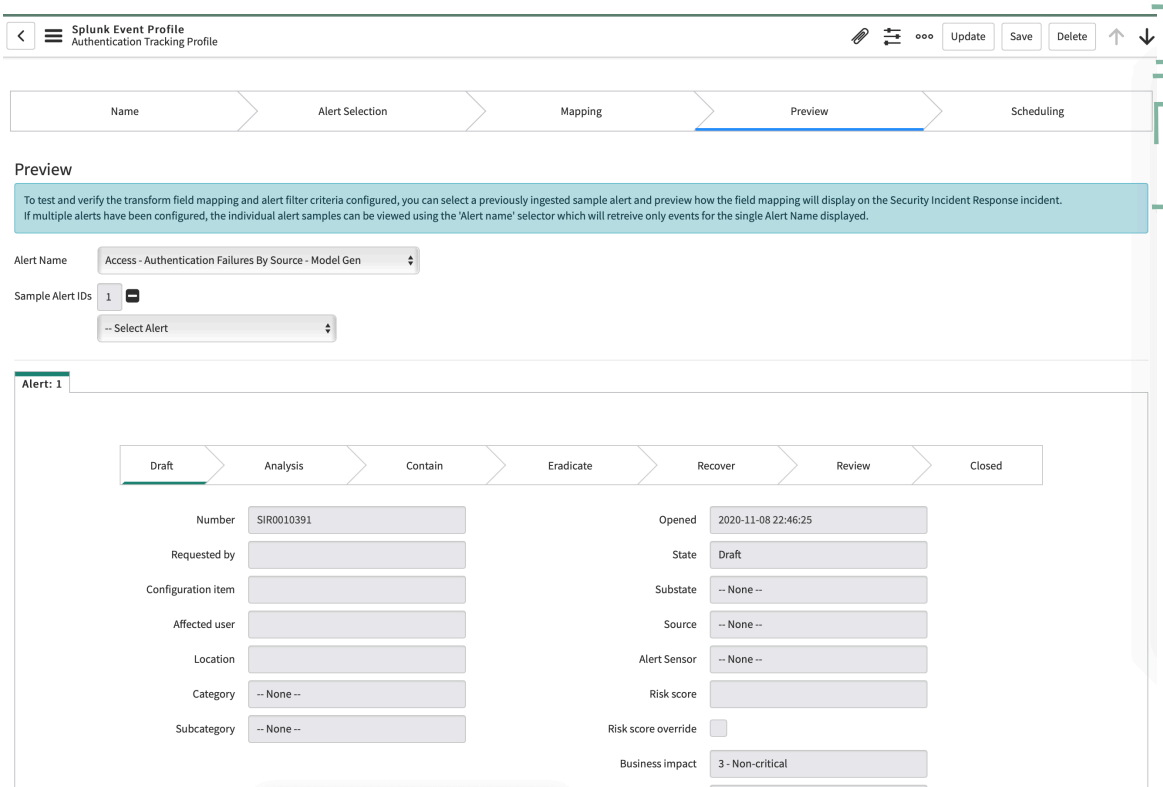
프로시저

1. 보안 인시던트 미리 보기가 표시되지 않으면 진행률 표시줄에서 미리 보기를 클릭합니다.
2. 경고 이름을 선택한 다음 샘플 경고 **ID** 목록에서 항목을 선택합니다.



보안 인시던트가 표시됩니다. 필드의 정보를 변경하지 마십시오. 이 뷰는 읽기 전용 뷰이며 이 보안 인시던트의 기록은 저장되지 않습니다.

3. 보안 인시던트에서 경보 값의 필드 매핑을 검토합니다.



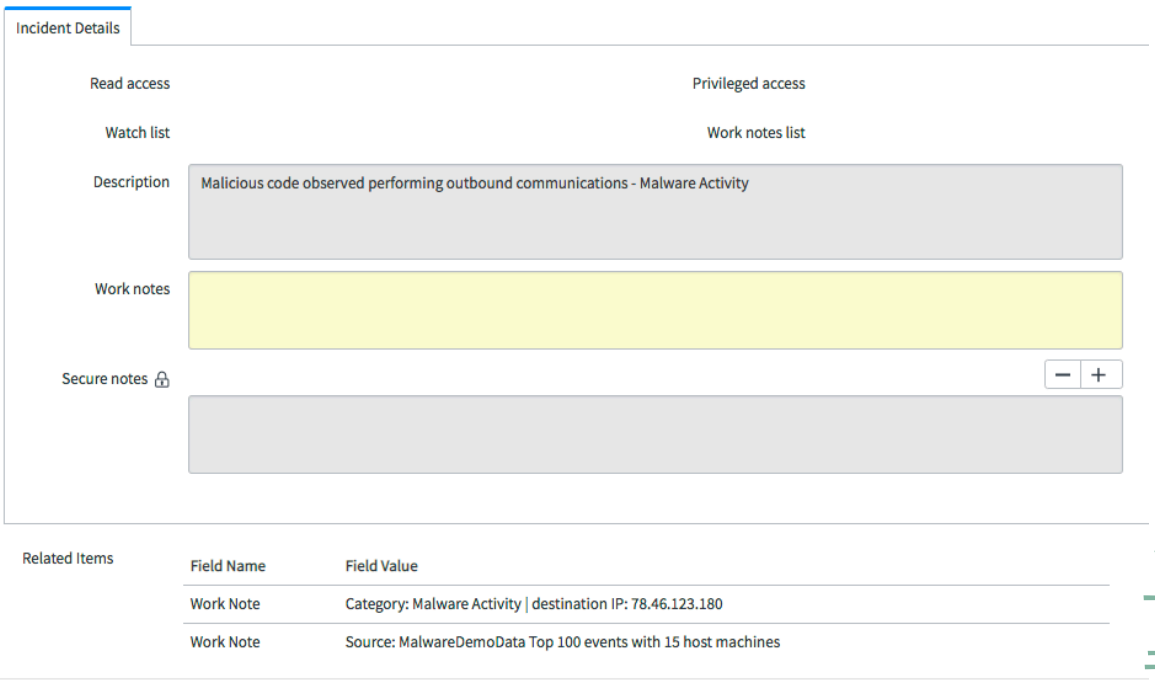
앞의 이미지는 매핑 오류가 있는 미리 보기의 예입니다. 이 예시에서는 값에 대한 보안 인시던트의 필드가 없거나 매핑한 값을 지원하지 않습니다. ## ## 필드에 대한 입력 값을 찾을 수 없음을 나타내는 오류 메시지가 표시됩니다.

4. 이 오류를 해결하려면 진행률 표시줄에서 매핑 을 클릭합니다.
5. 매핑을 편집하여 잘못된 값을 수정하거나 누락된 데이터를 채웁니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

6. 매핑을 다시 미리 보고 오류 메시지에 설명된 오류를 계속 수정합니다.

   다음 그림은 모든 오류 메시지가 해결된 후 보안 인시던트 하단 절반 SIR 에 있는 인시던트 상세 정보 탭의 예입니다. 이 예에서는 설명 및 작업 메모 필드가 매핑되었으며, 이러한 필드는 콘솔에서 가져온 Splunk Enterprise 값 쌍의 값으로 채워집니다. 첫 번째 작업 메모 필드에는 값이 없습니다. 이 필드는 매핑 단계 동안 매핑 그리드에서 비어 있었습니다. 값이 있는 추가 작업 메모 필드는 매핑 단계 중에 매핑 그리드에 추가되었습니다.



7. 오류를 수정하고 필드가 원하는 방식인지 확인한 후 계속하려면 하나의 옵션을 선택합니다.

다음에 수행할 작업

오류 메시지가 표시되지 않고 보안 인시던트의 필드 매핑에 만족하는 경우 다음 단계는 수행 통합에 대한 Splunk Enterprise Event Ingestion 경보 예약 및 검색입니다.

통합에 대한 **Splunk Enterprise Event Ingestion** 경보 예약 및 검색

자동 경보 수집 프로파일의 경우 이 단계는 이벤트 프로파일 구성의 마지막 단계입니다. 이 단계에서 경보 검색에 대한 기본 설정을 확인하거나 필요에 따라 일정을 수정할 수 있습니다. 이 단계를 통해 날짜 범위를 기준으로 경보 검색을 필터링할 수 있습니다.

시작하기 전에

필요한 역할: sn_si.ingestion_profile_admin

> **주:**
> sn_si.admin 역할은 기본적으로 필수 권한을 상속하므로 sn_si.admin 역할을 가진 사용자는 프로필 관리자가 사용할 수 있는 모든 작업을 수행할 수 있습니다.

이 태스크 정보

다음 그림과 같이 프로파일 구성에 대한 진행률 표시줄의 모든 단계를 완료한 후 수동 이벤트 전달을 위한 프로파일 구성을 완료했습니다. 콘솔에서 수동으로 Splunk Enterprise 전달된 이벤트에 사용할 수 있는 일정이 없습니다. 자동 경보 수집을 위한 프로필의 경우 예약 단계 중에 이전 경보를 수집할지 여부를 선택합니다. 경보 프로파일 구성과 일치하는 향후 경보를 폴링할 빈도를 선택할 수도 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

진행률 표시줄

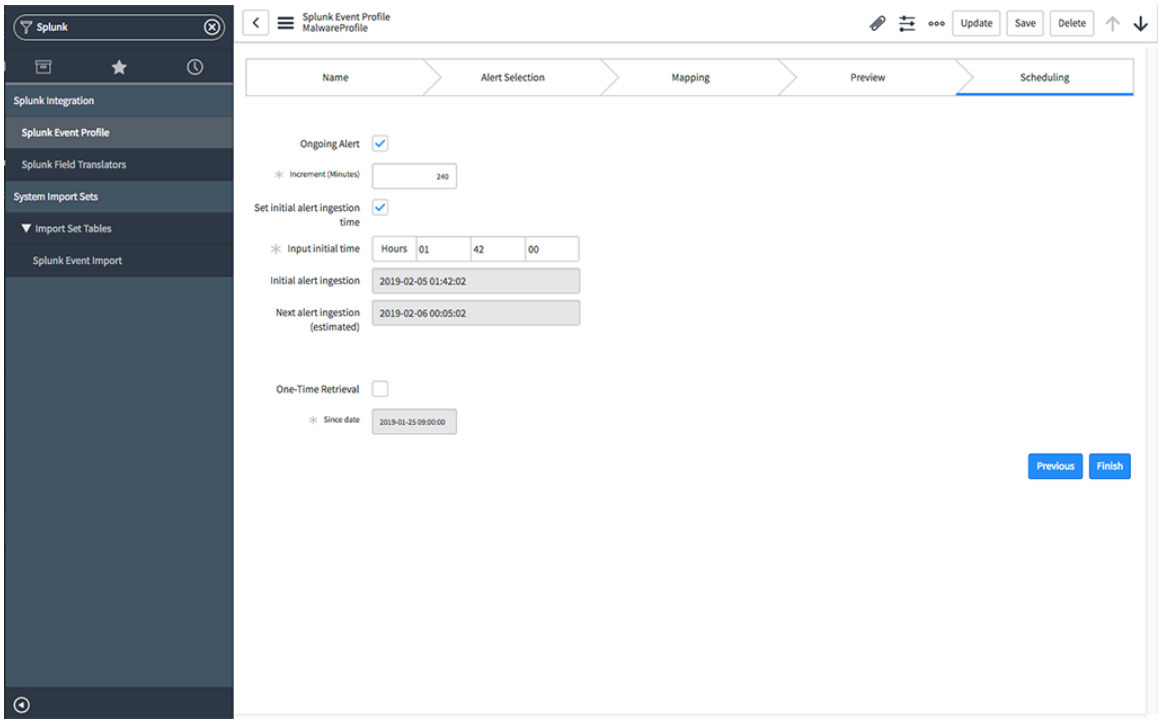
자동 경보 수집 프로파일의 경우 프로파일이 활성화되기 전에 예약 및 경보 검색을 확인하고 수정합니다. 이 단계는 예약된 경보 프로파일에 대한 이벤트 프로파일 구성 프로세스의 마지막 단계입니다.

프로파일별로 이러한 폴링 간격을 구성합니다. 이벤트 수집 통합의 Splunk 성능은 다양한 폴링 간격의 영향을 받습니다. 일정을 예약할 때 시스템 부하와 인시던트 긴급도의 균형을 맞추는 것이 좋습니다. 모든 프로파일에 대해 5분 기본값이 설정되지만 인시던트의 긴급도와 시스템의 예상 로드에 따라 이 설정을 수정하는 것이 좋습니다.

Splunk Enterprise 콘솔에서 증분 또는 특정 시간을 기반으로 트리거할 경보를 설정합니다. 이 설정을 사용하면 콘솔의 시간 증분이 인스턴스에서 설정한 ServiceNow AI Platform 일정과 동기화되도록 인스턴스의 일정을 ServiceNow AI Platform 구성할 수 있습니다Splunk Enterprise.

프로시저

1. 진행률 표시줄에 스케줄링 페이지가 표시되지 않으면 스케줄링을 선택합니다.
2. 콘솔에서 경보를 끌어오는 Splunk Enterprise 방법과 시기를 예약하려면 하나를 선택합니다.



예약의 예로, 현지 시간으로 하루에 한 번 오전 4시에 실행되는 일일 Splunk 경보가 있는 경우, 현지 시간으로 오전 4시 5분에 실행되도록 인스턴스의 해당 경보 프로필을 ServiceNow AI Platform 설정하여 경보를 즉시 캡처하고 보안 인시던트를 만들 수 있습니다. 초기 경보 수집 필드에 04 05 00을 입력합니다. 증분(분) 필드에 1440(24시간)을 입력하여 초기 경보 수집으로부터 24시간 동안 다음 경보 수집을 예약합니다. 초기 경보 수집 시간과 다음 경보 수집 시간이 모두 필드에 표시됩니다.

3. 이 예제의 설정을 구성하려면 다음 단계를 수행합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 예약 페이지가 표시되면 진행 중인 경보 확인란을 선택하여 이 옵션을 활성화합니다.

b. 증분(분) 필드에 1440(24시간)을 입력합니다.

c. 초기 경보 수집 및 다음 경보 수집 필드를 편집할 수 있도록 하려면 초기 경보 수집 선택 확인란을 클릭합니다.

d. 초기 경보 수집 필드에 04 05 00을 입력합니다.
다음 경보 수집(예상) 필드에 다음 경보 수집 시간이 표시됩니다.

4. Finish(마침)를 클릭하여 구성을 완료합니다.
확인 대화 상자가 표시됩니다. 통합에 대한 설정 및 구성을 성공적으로 완료했습니다. 이 프로파일이 활성화되고 일정에 따라 콘솔에서 경보를 Splunk Enterprise 가져옵니다. 24시간 동안 생성할 수 있는 보안 인시던트는 1,000개로 제한됩니다. 발생한 경보당 최대 100개의 이벤트가 발생합니다. 제한에 도달하면 후속 이벤트가 무시됩니다.

통합을 위한 **Splunk Enterprise Event Ingestion** 통합 아키텍처 및 외부 시스템 연결

다음 항목에서는 콘솔에서 트리거된 경보 Splunk Enterprise 수집을 지원하기 위해 개발된 통합 아키텍처에 대해 간략하게 설명합니다. 이 정보는 통합의 개념적 작업을 개략적으로 설명합니다. 또한 에서 ServiceNow Store애플리케이션을 설치하기 전에 필요한 설정 단계가 있는 이유도 설명합니다.

이 통합에 사용된 주요 용어

다음 주요 용어는 설치 및 구성 중에 사용됩니다. 이 약관에 대한 자세한 내용은 ServiceNow 제품 설명서 웹 사이트 와 Splunk 웹 사이트 및 Splunk 자원 페이지의 자원을 참조하십시오.

ServiceNow AI Platform

엔터프라이즈 ServiceNow 제품입니다. ServiceNow AI Platform 는 (),SIR ITSM(IT Service Management) 및 기타 제품과 같은 보안 인시던트 응답 개별 구성요소의 기반입니다.

ServiceNow Splunkbase 애드온

통합의 수동 이벤트 전달 옵션을 지원하는 콘솔에 설치된 Splunk Enterprise 애플리케이션입니다ServiceNow. 수동 이벤트 전달은 통합의 선택적 기능입니다. 이 ServiceNow Splunkbase 추가 기능은 통합에서 제공하는 자동화된 경보 수집에 필요하지 않습니다.

보안 인시던트 응답(SIR)

ServiceNow AI Platform 검색 및 초기 분석부터 방지, 근절 및 복구를 거쳐 최종 사후 인시던트 검토 및 종결에 이르는 보안 인시던트의 진행 상황을 추적하는 애플리케이션입니다.

Splunk Enterprise

인시던트 분석 및 관리에 사용되는 데이터를 수집하는 자동화된 SIEM(보안 인시던트 이벤트 관리) 제품 또는 클라우드 서비스입니다. 이 서비스는 이 가이드에서 콘솔이라고도 하는 호스트에 Splunk 있습니다.

Splunk 경보

서비스에서 설정한 매개변수를 기반으로 특정 데이터를 검색하기 위해 구성하고 저장하는 Splunk 검색입니다 Splunk Enterprise . 에서 경보 Splunk를 끌어올 때 해당 경보와 연결된 모든 이벤트도 끌어옵니다.

Splunk 트리거된 경보

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

결과를 반환하고 이러한 결과에 트리거된 경보로 플래그를 지정하는 콘솔의 Splunk Enterprise 구성된 검색입니다. 트리거된 경보는 이 통합을 위해 콘솔에서 인스턴스 ServiceNow AI Platform 로 수집 Splunk 됩니다. 트리거된 경보에는 하나 이상의 Splunk 이벤트가 있습니다.

Splunk 이벤트

서비스의 트리거된 경보를 Splunk 발생시키는 하나 이상의 데이터 요소입니다. 인스턴스에서 ServiceNow AI Platform 보안 Splunk 인시던트를 트리거 ServiceNow AI Platform 한 이벤트를 조회할 수 있습니다.

MID 서버

이 애플리케이션은 외부 애플리케이션, 데이터 소스 및 서비스 간의 데이터 이동 및 통신을 용이하게 합니다 ServiceNow AI Platform . 이 애플리케이션은 일반적으로 온프레미스 기술과의 통합에 필요하며, 이러한 Splunk Enterprise Event Ingestion 통합을 위해 MID 서버는 의 온프레미스 인스턴스와 의 온프레미스 인스턴스 Splunk Enterprise간의 ServiceNow AI Platform 통신을 용이하게 합니다. 인스턴스를 인스턴스와 Splunk Cloud 통합하는 ServiceNow AI Platform 경우에는 MID 서버가 필요하지 않습니다.

보안 인시던트 관리자(sn_si.admin)

이 역할이 있는 사용자는 인스턴스의 제품과의 SIR 통합 구성을 감독합니다 ServiceNow AI Platform .

보안 인시던트 분석가(sn_si.analyst)

이 역할을 가진 사용자는 제품의 보안 인시던트와 상호작용하고 이를 분석합니다 ServiceNow 보안 인시던트 응답 .

보안 인시던트 프로파일 관리자(sn_si.ingestion_profile_admin)

이 역할을 가진 사용자는 인스턴스의 제품에 ServiceNow AI Platform 대한 SIR Azure Sentinel, Splunk 및 Splunk ES 통합에 대한 플러그인을 구성하고 수집 프로필을 생성, 편집, 삭제 및 유지 관리합니다.

외부 시스템 연결

이벤트 프로파일은 단일 연결에 대해 생성하고, 이름을 지정하고, 구성하는 컨테이너이며, 특정 기준과 일치하는 가장 최근의 트리거된 경보를 Splunk 끌어오기 위해 서비스를 호출합니다. 프로파일과 일치하는 트리거된 경보를 에서 끌어온 Splunk후에는 이러한 경보 중 보안 인시던트로 표시할 경보를 ServiceNow AI Platform 보안 인시던트 응답 SIR 선택합니다. 경보 필드의 기본 뷰를 Splunk Enterprise 사용할 수 있으며, 필요에 맞게 경보 필드와 보안 인시던트의 필드 SIR 매핑을 편집합니다. 매핑을 미리 보고 보안 인시던트에 SIR 필요한 모든 경보 필드 값이 채워져 있는지 확인합니다. 경보 프로파일 구성을 완료하려면 경보 검색을 예약한 다음 프로파일을 활성화합니다. 에서 ServiceNow AI Platform프로파일을 활성화하면 기록 및 진행 중인 Splunk 경보를 자동으로 수집할 준비가 된 것입니다.

sn_si.admin 역할을 가진 사용자가 새로 트리거된 경보가 이전에 수집된 경보와 유사한 것을 확인하면 새로 트리거된 경보를 기존 SIR 보안 인시던트로 집계할 수 있습니다. 기존 보안 인시던트가 업데이트되는 시기와 새 보안 인시던트가 생성되는 시기를 정의하는 경보 프로파일에서 Splunk Enterprise 일치하는 대상 필드 값을 지정하는 기준을 설정합니다. 이벤트 프로파일에서 집계 기능이 활성화된 경우 임포트 세트가 변환되면 ServiceNow AI Platform 인스턴스는 대상 테이블에 대상 및 소스 필드에 동일한 값이 있는 기존 기록을 확인합니다. 대상 테이블에서 일치하는 값이 있는 기존 기록이 발견되면 해당 기록이 업데이트됩니다. 일치하는 기록이 없으면 대상 테이블에 새 기록이 생성됩니다. 이 옵션을 사용하면 집계 옵션을 사용하면 새로 트리거된 경보로 기존 보안 인시던트를 업데이트하므로 여러 보안 인시던트가 생성되는 경우를 방지할 수 있습니다. 집계 옵션을 사용하여 기록을 업데이트하는 방법에 대한 자세한 내용은 병합을 사용하여 기록 업데이트를 참조하십시오.

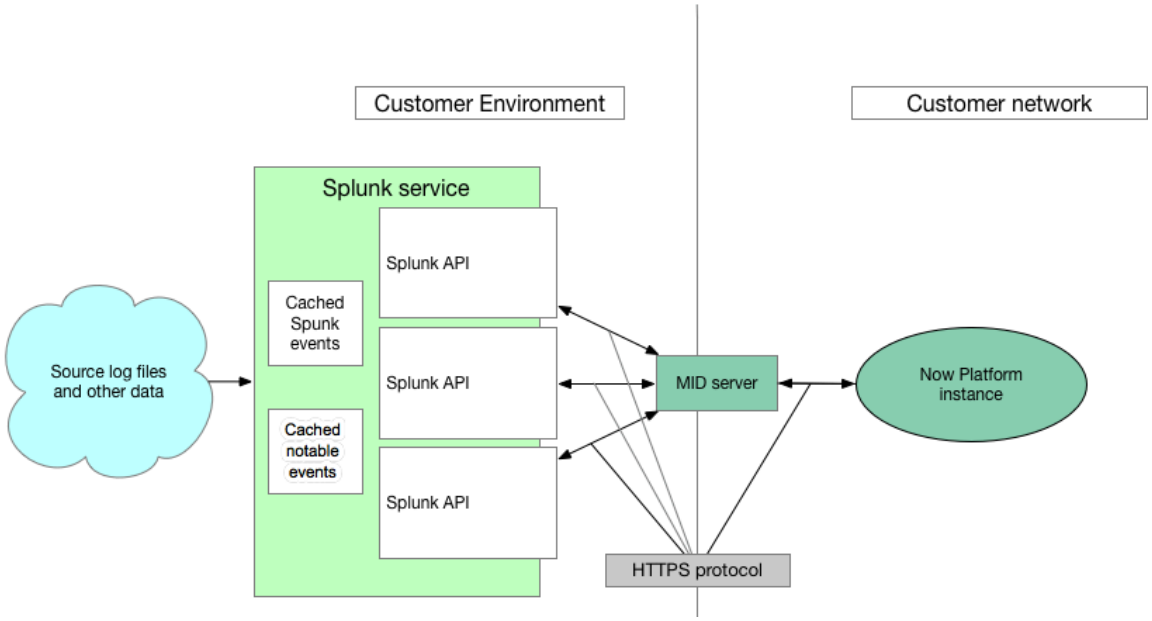
이 애플리케이션은 API 서비스를 사용하여 Splunk 서비스에서 정보를 Splunk 검색합니다. 통합이 제대로 작동하려면 MID 서버에서 이 환경으로의 아웃바운드 HTTPS 연결이 필요합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

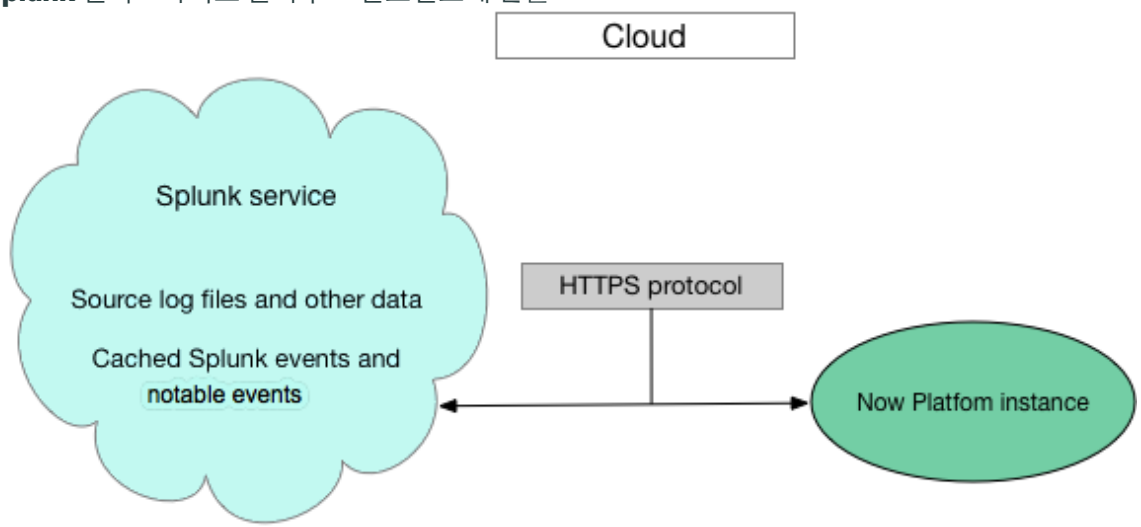
통합이 서비스에 연결되면 Splunk 통합은 보안 인시던트를 트리거하는 트리거된 경보 및 이벤트의 끌어오기 및 수집을 지원합니다.

기본 데이터 흐름은 다음 그림에 설명되어 있습니다. 각 그림에서 데이터를 ServiceNow AI Platform 끌어오는(수집) 중입니다. Splunk 예약된 경보에 대한 데이터를 푸시하지 않습니다.

단일 MID서버를 사용하는 온프레미스 **Splunk** 엔터프라이즈 서비스에 연결

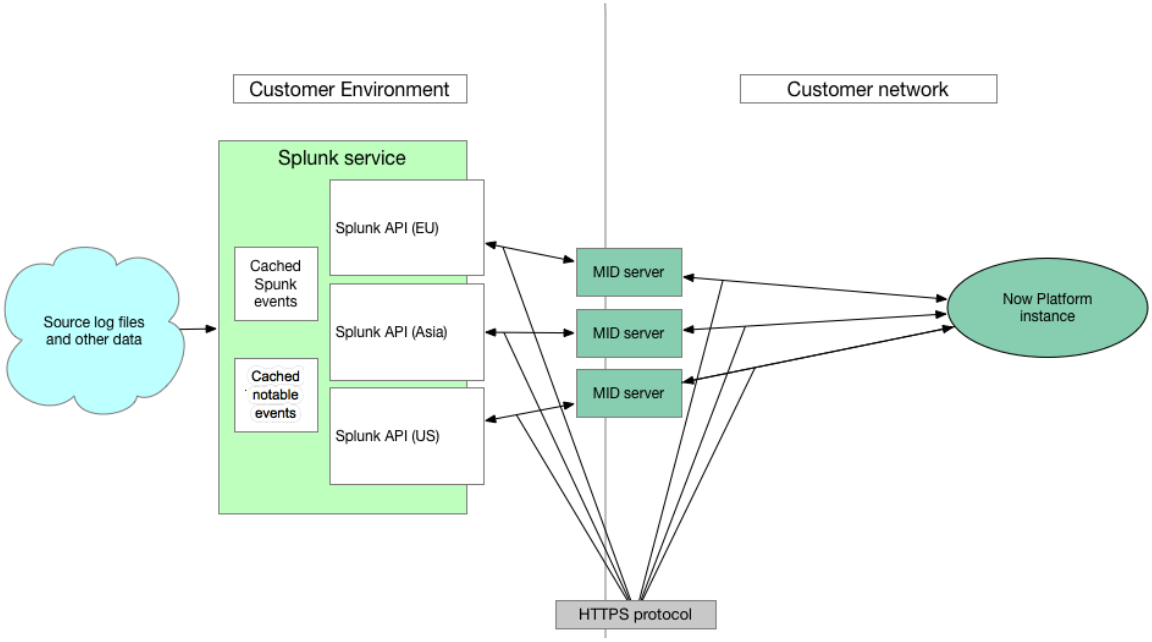


Splunk 엔터프라이즈 클라우드 인스턴스에 연결



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

여러 **MID** Server를 **Splunk** 사용하여 엔터프라이즈 서비스에 다중 연결



익스포트/임포트 기능을 사용하여 한 인스턴스에서 다른 인스턴스로 프로파일 복사 **Splunk Enterprise Event Ingestion**

한 인스턴스에서 다른 ServiceNow AI Platform 인스턴스로 ServiceNow AI Platform 프로파일 설정을 익스포트하고 임포트 Splunk Enterprise Event Ingestion 할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.ingestion_profile_admin

주:
sn_si.admin 역할은 기본적으로 필수 권한을 상속하므로 sn_si.admin 역할을 가진 사용자는 프로필 관리자가 사용할 수 있는 모든 작업을 수행할 수 있습니다.

이 태스크 정보
이 기능을 사용하면 보안 관리자가 모든 구성 설정을 다시 실행할 필요 없이 한 ServiceNow AI Platform 인스턴스(예: 비프로덕션)에서 테스트 및 검증된 프로파일을 다른 ServiceNow AI Platform 인스턴스(예: 프로덕션)에 복사할 수 있습니다. 익스포트하고 임포트되는 설정에는 프로파일 이름, 상관관계 규칙, 매핑, 필터, 집계 기준, 필드 번역, 가져온 샘플 데이터, 스케줄링 및 구성 타일 소스 정보가 포함됩니다.

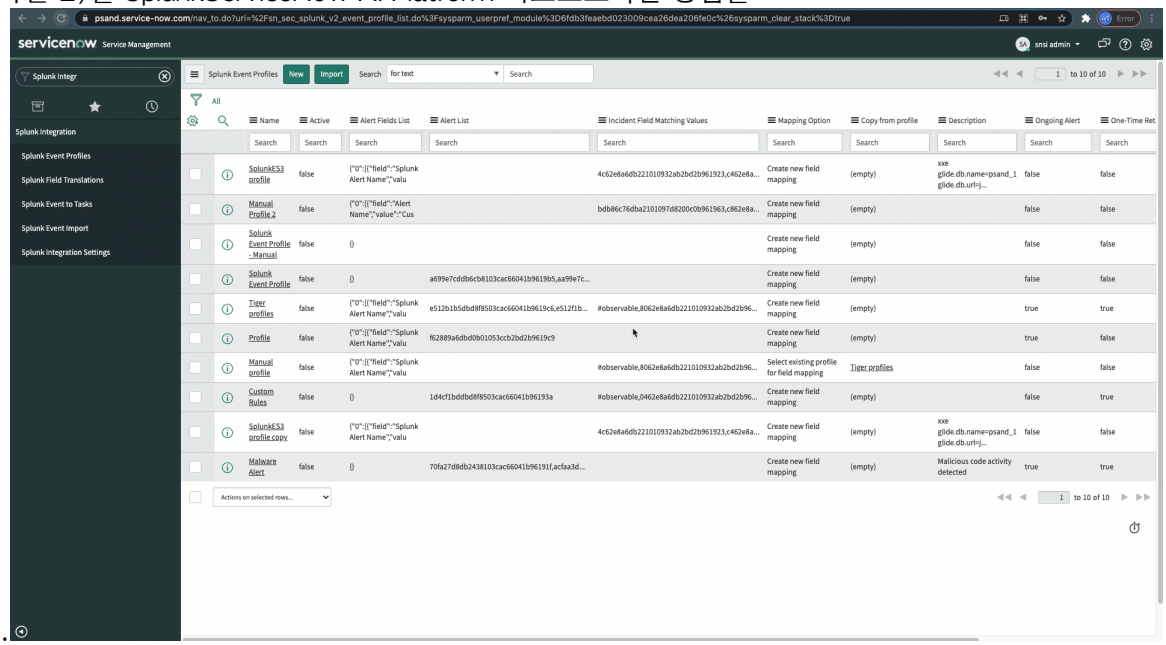
주:
수동 이벤트 전달 프로파일 유형을 익스포트하면 샘플 필드 매핑에 사용되는 첨부 파일 데이터는 복사되지만 첨부 파일 자체는 익스포트되지 않습니다.

프로시저

1. 다음으로 이동 모두 〉 **Splunk Integration** 〉 **Splunk** 이벤트 프로파일.
2. 다른 ServiceNow AI Platform 인스턴스로 익스포트할 프로파일을 선택합니다.
   익스포트할 프로파일을 여러 개 선택할 수 있습니다.
3. Actions(작업) 메뉴에서 Export(내보내기)를 클릭합니다.
4. 내보내기 완료 메시지가 나타나면 다운로드를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음 그림은 인스턴스(psand.service-now.com)에서 프로파일 (수동 프로파일 2)을 SplunkServiceNow AI Platform 익스포트하는 방법을 보여줍니다.

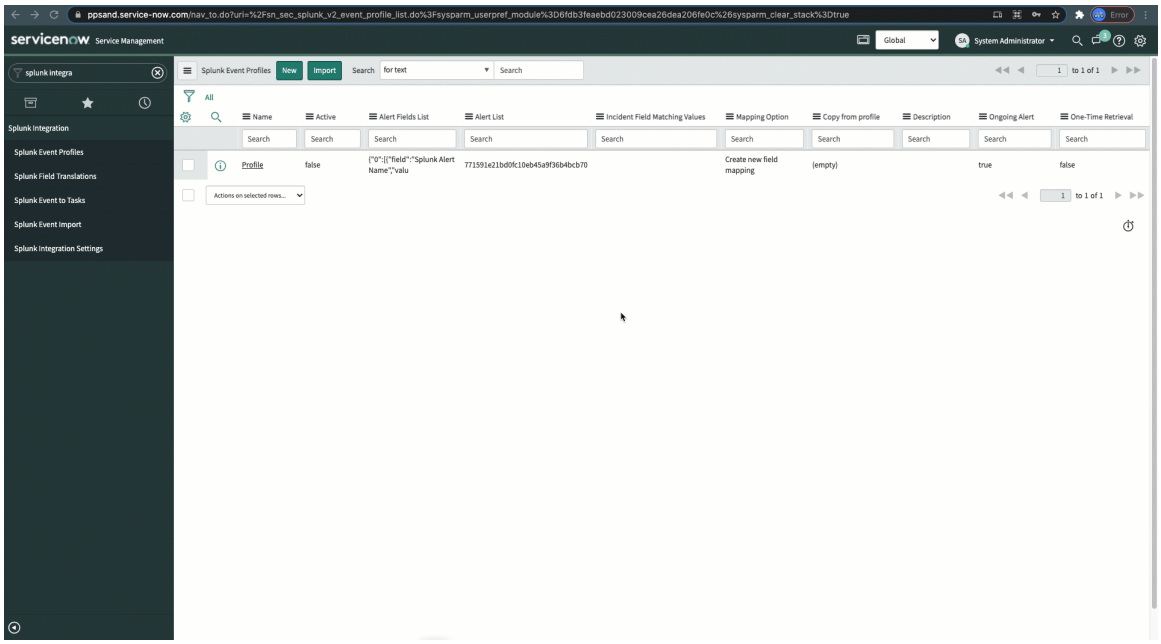


익스포트한 payload.xml 파일이 컴퓨터에 다운로드됩니다. 이 파일에는 프로파일 이름, 상관관계 규칙, 매핑, 필터, 집계 기준, 필드 번역, 가져온 샘플 데이터, 스케줄링 및 구성 타일 소스 정보가 포함되어 있습니다. 여러 프로필을 선택하고 다운로드하면 동일한 payload.xml 파일에 표시됩니다.

이제 다른 ServiceNow AI Platform 인스턴스에서 프로파일 임포트를 진행할 수 있습니다.

5. 다음으로 이동 **Splunk Integration** 〉 **Splunk** 이벤트 프로파일.
6. 임포트를 클릭합니다.
7. 파일 선택을 클릭하고 컴퓨터에서 xml 파일을 선택합니다.
8. 업로드를 클릭합니다.
9. **Close and Reload** Profiles(종단 닫기 및 다시 로드)를 클릭합니다.
   다음 그림은 인스턴스(psand.service-now.com)에서 다른 ServiceNow AI Platform 인스턴스 (ppsand.service-now.com)로 프로파일(수동 프로파일 2)을 ServiceNow AI Platform 임포트 Splunk 하는 방법을 보여줍니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



다른 ServiceNow AI Platform 인스턴스에서 프로파일을 성공적으로 임포트했습니다.

익스포트한 소스(Splunk API 계정 및 Splunk 서버 URL) 및 MID 서버 구성 설정이 유효하고 임포트한 ServiceNow AI Platform 인스턴스에서 사용할 수 있는지 확인합니다. Splunk Enterprise Event Ingestion 필요한 경우 구성을 업데이트합니다.

10. 옵션: 프로파일을 임포트한 후 MID 서버 설정을 확인합니다.
11. 옵션: 다음으로 이동 보안 운영 〉 통합 구성.
12. 옵션: 구성 타일을 Splunk Enterprise Event Ingestion 선택하고 업데이트를 클릭합니다.
13. 옵션: 필요에 따라 소스 및 MID 서버 상세 정보를 검토하고 업데이트합니다.

통합에 대한 **Splunk Enterprise Event Ingestion** 이벤트 프로파일 복사

새 프로파일을 생성하는 대신 기존 프로파일 및 관련 설정을 복사합니다. 여러 프로필을 만들고 기존 프로필의 설정을 다시 사용하려는 경우 시간을 절약하기 위해 경보 프로필을 복사하는 것이 좋습니다.

시작하기 전에
필요한 역할: sn_si.ingestion_profile_admin

> **주:**
> sn_si.admin 역할은 기본적으로 필수 권한을 상속하므로 sn_si.admin 역할을 가진 사용자는 프로필 관리자가 사용할 수 있는 모든 작업을 수행할 수 있습니다.

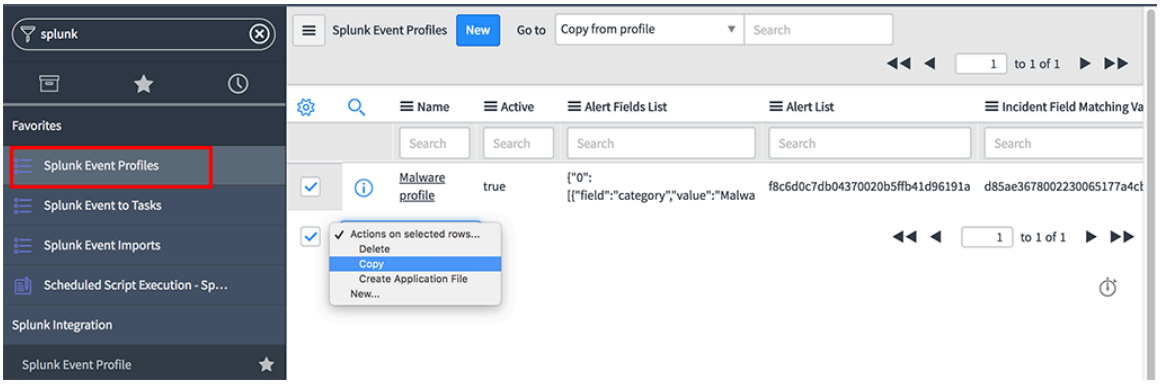
이 태스크 정보
기존 프로파일 및 관련 설정을 복사하는 것은 선택 사항입니다.

프로파일을 복사하는 경우 프로파일 중복을 방지하기 위해 처음에 프로파일 이름이 수정됩니다. 또한 복사된 프로파일이 비활성화(false)되므로 컨피그레이션을 완료하기 전에 실수로 활성화되지 않습니다. 이미 미리 보고 확인한 보안 인시던트에 대해 프로파일을 복사하고 기존 맵을 사용합니다.

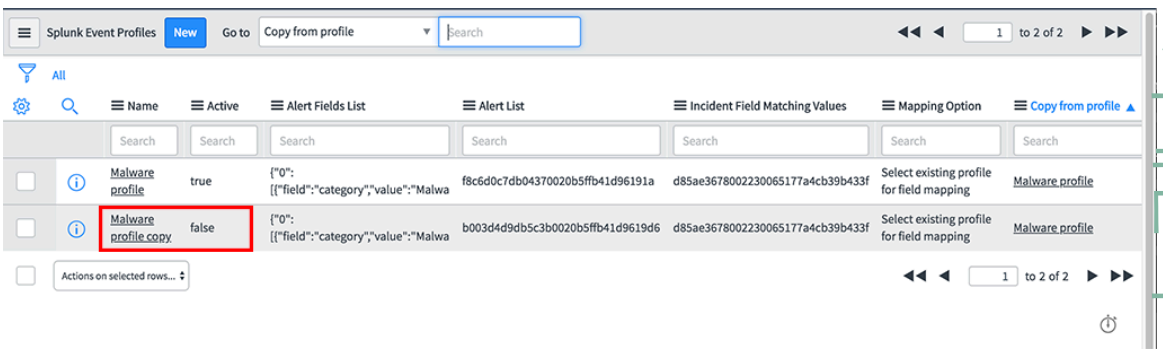
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 **Splunk Integration** 〉 **Splunk** 이벤트 프로파일.
2. Splunk 표시되는 이벤트 프로파일 목록에서 복사할 프로파일을 선택하고 선택한 행에 대한 작업 선택 목록에서 복사를 클릭합니다.



프로파일이 복사되어 목록에 표시됩니다. 복사본에는 매핑 및 일정 구성을 포함하여 원래 프로필의 모든 설정이 포함됩니다. 프로파일의 이름에는 사본이 포함되어 있습니다. 원본 프로파일이 활성화되었지만(true) 이 시점에서는 복사본이 비활성화됩니다(false). 복사된 프로파일의 값을 편집하고 필요에 따라 구성 설정이 새 프로파일에 적용되도록 이름을 바꿀 수 있습니다.



기존 프로파일에서 새 프로파일로 설정을 복사했습니다.

다음에 수행할 작업

구성 단계를 완료한 후 새 프로파일을 활성화(활성화)하라는 메시지가 표시됩니다.

Splunk 이벤트 수집 통합을 위한 **Splunk Enterprise** 수동 이벤트 수집을 위한 환경 설정

이 통합에 대해 콘솔에서 요청 Splunk Enterprise 시 이벤트를 수동으로 익스포트하려면 엔터프라이즈 콘솔 또는 Splunk 클라우드 인스턴스에 애플리케이션에 대한 Splunk Enterprise 보안 운영 이벤트 수집 애드온을 Splunk 설치하고 설정합니다ServiceNow.

시작하기 전에

수동 이벤트 수집에 필요한 splunkbase에서 애드온 플러그인을 설치하기 전에 이 통합 ServiceNow Store 에 대한 애플리케이션을 설치했는지 확인하십시오. 에서 ServiceNow Store통합을 위한 애플리케이션을 설치하지 않은 경우 를 참조 통합을 위한 Splunk Enterprise Event Ingestion 애플리케이션 설치 및 구성 ServiceNow 하고 지침에 따라 설치합니다.

필요한 역할: ServiceNow AI Platform 관리자(admin)

이 태스크 정보

보안 운영 이벤트 수집 애드온의 ServiceNow 설치 및 설정은 선택 사항입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

통합을 위해 콘솔에서 요청 시 Splunk Enterprise 이벤트를 수동 익스포트하려면 콘솔의 Splunk Enterprise splunkbase에서 보안 운영 이벤트 수집 추가 기능을 Splunk Enterprise 다운로드, 설치 및 설정합니다ServiceNow.

인스턴스에서 수동으로 익스포트한 이벤트 ServiceNow AI Platform 에서 보안 인시던트를 만들려면 이 ServiceNow 확장 추가 기능이 필요합니다. 이 ServiceNow 애플리케이션용 Splunk Enterprise 보안 운영 이벤트 수집 애드온은 splunkbase 에서 사용할 수 있습니다.

수동 이벤트 전달의 경우 콘솔에서 최대 두 개의 서로 다른 ServiceNow AI Platform 엔드포인트(인스턴스)를 식별할 수 있습니다 Splunk Enterprise . 이벤트를 엔드포인트 또는 엔드포인트에 수동으로 전달하여 보안 인시던트를 만듭니다. 예를 들어, 스테이징(개발) 인스턴스와 프로덕션 인스턴스를 모두 지정할 수 있습니다. 개별 인스턴스를 지정하고 각 인스턴스에 대한 기본 및 보조 워크플로우의 이름을 지정하여 서로 다른 이벤트를 전달할 위치를 선택할 수 있습니다.

프로시저

1. 에 대한 Splunk Enterprise보안 운영 이벤트 수집 추가 기능을 아직 설치하지 ServiceNow 않은 경우 다음 단계에 따라 설치하고 구성합니다.

   a. splunkbase 로 이동합니다.

   b. ServiceNow 보안 운영 에 대한 Splunk Enterprise보안 운영 이벤트 수집 추가 기능을 검색합니다.

      주:
      에 대한 Splunk Enterprise이벤트 수집 추가 기능을 선택 ServiceNow 보안 운영 했는지 확인합니다. 이 목록에 표시되는 추가 ServiceNow 애드온이 있습니다. 이러한 추가 기능은 서로 다른 ServiceNow Splunk 통합을 위한 것이며 이 통합에는 필요하지 않습니다.

   c. 애플리케이션을 다운로드합니다.

   d. 계정을 Splunk Enterprise 엽니다.

   e. 앱 페이지에서 기어 아이콘을 클릭하거나 메뉴 드롭다운 목록에서 앱 관리 바로 가기를 클릭합니다.

   f. 표시되는 앱 페이지의 왼쪽 상단에서 파일에서 앱 설치를 클릭합니다.

   g. 파일 선택을 클릭하고 에 대한 Splunk Enterprise보안 운영 이벤트 수집 추가 기능을 선택한 ServiceNow 다음 업로드를 클릭합니다.

   h. 메시지가 표시되면 을 다시 시작합니다 Splunk Enterprise.
   ServiceNow 용 Splunk Enterprise 보안 운영 이벤트 수집 추가 기능이 엔터프라이즈 콘솔에 설치됩니다Splunk Enterprise. 애드온을 설정하는 다음 단계입니다.

2. 애드온을 설정하려면 다음 단계를 따르십시오.

   a. 에서 Splunk Enterprise메뉴 드롭다운 목록에서 앱 기어 아이콘 또는 앱 관리를 클릭합니다.

   b. 표시되는 애플리케이션 목록의 작업 열에서 에 대한 이벤트 수집 추가 기능 설정을ServiceNow 보안 운영Splunk Enterprise클릭합니다.

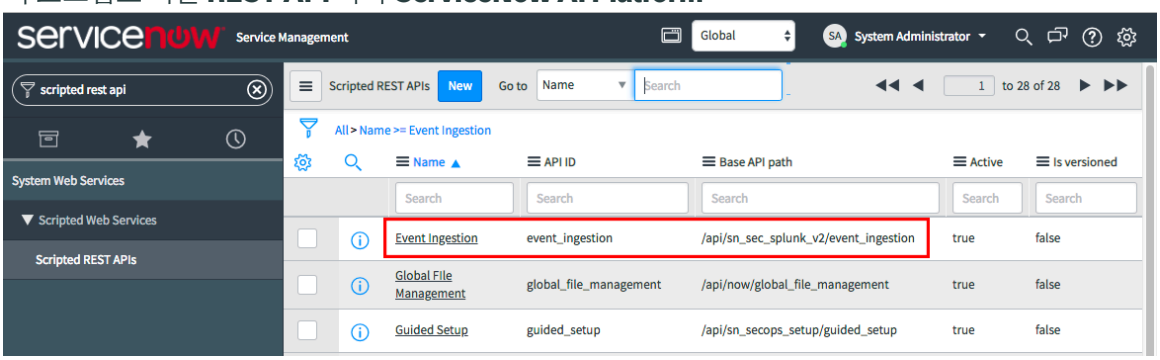
   c. 양식을 작성합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음 그림은 콘솔에서 작성된 양식의 Splunk Enterprise 예입니다.

다음 그림은 에 ServiceNow AI Platform있는 Scripted REST API 목록의 예입니다. 콘솔의 확장 Splunk Enterprise 용 Splunk Enterprise 보안 운영 이벤트 수집 추가 기능 설정 ServiceNow 의 일부로 양식에 입력한 인스턴스의 엔드포인트 값 ServiceNow AI Platform 위치가 목록에 표시됩니다.

의 스크립트 기반 **REST API** 목록 **ServiceNow AI Platform**



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 콘솔의 Splunk Enterprise 설정 양식에서 Save(저장)를 클릭하여 편집 내용을 저장합니다.

   잠시 후 콘솔 양식의 Splunk Enterprise 왼쪽 상단에 기록이 성공적으로 업데이트되었다는 메시지가 표시됩니다.

   양식을 저장한 후에는 콘솔에서 선택한 검색 이벤트의 이벤트 작업 선택 목록에서 양식에 생성한 인스턴스의 이름(워크플로우 작업 레이블) ServiceNow AI Platform 을 사용할 수 Splunk Enterprise 있습니다.

다음에 수행할 작업
콘솔에 검색을 Splunk Enterprise 아직 저장하지 않은 경우 다음 단계는 검색을 콘솔에 경보로 저장하는 것입니다 Splunk Enterprise .

통합에 대한 **Splunk Enterprise Event Ingestion** 콘솔 검색 **Splunk Enterprise** 저장

콘솔에 검색을 Splunk Enterprise 저장하는 다음 단계는 관리자 역할을 가진 Splunk Enterprise 사용자에게 제공됩니다.

시작하기 전에
콘솔에 저장된 기존 검색과 트리거된 경보 Splunk Enterprise 가 이미 있는 경우 이 통합에 대해 이러한 검색을 수정할 필요가 없습니다.

제품과 Splunk 이벤트 알림 서비스를 통합 ServiceNow AI Platform# 보안 운영 하면 에서 Splunk이벤트 및 경보 정보를 끌어옵니다.

경보를 보안 운영 사용자 환경에 수집하기 전에 경보로 저장하려는 관련 보안 이벤트를 Splunk Enterprise 자동으로 끌어올 수 있도록 콘솔에서 검색을 Splunk Enterprise 구성합니다.

콘솔에 중요한 보안 이벤트가 발생할 Splunk Enterprise 때 알림을 위해 설정된 검색 및 트리거된 경보가 없는 경우 다음 단계에 따라 검색을 저장합니다.

필요한 역할: Splunk Enterprise 관리자

프로시저

1. Splunk Enterprise 계정에 로그인합니다.
2. 검색 탭을 클릭합니다.
3. 표시되는 새 검색 필드에 경보 값(예: 맬웨어)을 입력합니다.
4. 검색과 관련된 이벤트를 보려면 새 검색 필드 오른쪽에 있는 검색 아이콘을 클릭하거나 Enter 키를 누릅니다.
   이벤트가 있는 검색 결과가 표시됩니다.
5. 검색을 경고로 저장하려면 페이지 오른쪽 위에서 다른 이름으로 저장 선택 목록을 확장하고 경고를 선택합니다.
6. 표시되는 양식의 필드에 내용을 입력합니다.

7. 저장을 클릭합니다.
   경보가 저장되고 검색 페이지의 경보 탭 아래에 표시됩니다.
   Splunk 서비스는 경보에서 구성한 기준과 일치하여 이벤트를 끌어옵니다. 이벤트를 캐시한 다음 인스턴스에 설정한 ServiceNow AI Platform 프로파일에서 이러한 이벤트를 요청합니다. 이벤트의 수집 끌어오기는 서비스의 캐시 Splunk 에서 발생하므로 사용자의 ServiceNow AI Platform 이러한 수집은 플랫폼의 성능에 Splunk 영향을 주지 않습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 수행할 작업
콘솔에서 통합에 필요한 설정을 성공적으로 완료했습니다 Splunk Enterprise . 에서 ServiceNow Store통합을 위한 애플리케이션을 아직 설치하지 않은 경우 다음 단계는 통합을 위한 애플리케이션을 설치하고 구성하는 것입니다.

스크립트 편집기를 사용하여 통합에 대한 경보 값의 서식을 **Splunk Enterprise Event Ingestion** 지정합니다

스크립트 편집기를 사용하여 매핑 단계 중에 보안 인시던트의 필드 값에 서식을 지정합니다.

시작하기 전에
끌어온 경보 값에서 직접 매핑된 필드와 수동으로 입력하는 경보 값 외에도, 선택적으로 스크립트 편집기를 사용하여 매핑 단계 중에 보안 인시던트의 필드 값에 대한 서식을 지정할 수 있습니다. 스크립트 편집기는 보안 인시던트에서 ServiceNow AI Platform# 보안 인시던트 응답 지원하는 값이 범주, CI(구성 항목) 및 옵저버블 필드에 매핑되도록 경보 값을 Splunk 변경합니다.

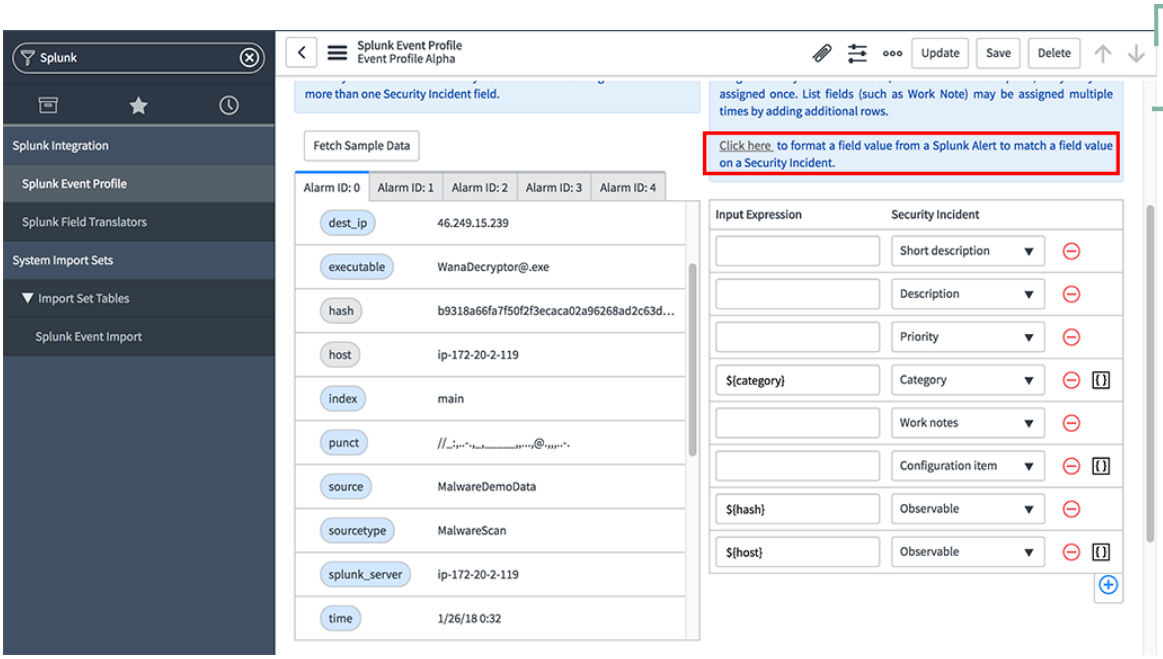
필요한 역할: sn_si.ingestion_profile_admin

> **주:**
> sn_si.admin 역할은 기본적으로 필수 권한을 상속하므로 sn_si.admin 역할을 가진 사용자는 프로필 관리자가 사용할 수 있는 모든 작업을 수행할 수 있습니다.

이 태스크 정보
경우에 따라 Splunk Enterprise 경보 값은 인시던트의 SIR 범주, CI(구성 항목) 및 옵저버블 필드에 매핑되며 지원되지 않습니다. 매핑된 값을 편집하는 것이 좋습니다. 경보 값을 Splunk Enterprise 보안 인시던트의 이러한 필드에서 SIR 지원하는 값으로 변환하려면 스크립트 편집기를 사용합니다.

프로시저

1. 매핑 양식이 표시되면 링크를 클릭하여 스크립트 편집기를 엽니다.



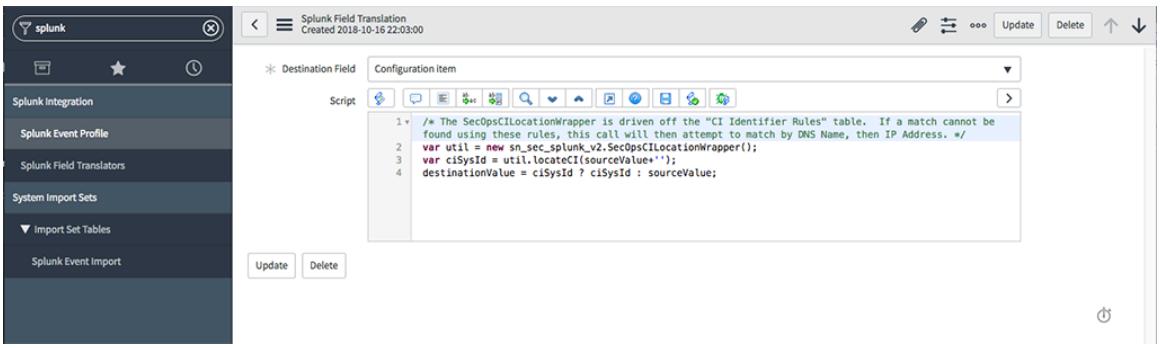
2. 선택 목록에서 편집할 값의 대상 필드를 선택합니다.
3. 또는 SIR 인시던트 필드 매핑 섹션에서 필드 옆에 있는 대괄호 아이콘 [{}] 을 클릭하여 해당 필드의 스크립트 편집기를 엽니다.

   경우에 따라 스크립트 포함이 구성 항목 필드에 적합할 수 있습니다. 예를 들어 경보의 경우 구성 항목의 값이 일치하지 않을 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음 그림과 같이 구성 항목 필드의 CMBD에서 ServiceNow AI Platform# 호스트 이름과 일치하는 항목을 찾을 수 없는 경우 IP 주소가 발견되면 구성 항목 필드를 채우도록 규칙을 편집할 수 있습니다. 경보에 대한 값이 없으면 보안 인시던트의 필드가 null로 설정됩니다.

대상 필드에 필드가 표시된 상태로 편집기가 열립니다. 다음 이미지는 ## ## 필드가 대상 필드인 편집기를 보여줍니다.



4. 스크립트에 대한 변경 내용을 입력하고 업데이트를 클릭하여 변경 내용을 저장합니다. Splunk 필드 번역 테이블이 표시됩니다.
5. 테이블을 닫고 매핑 양식으로 돌아갑니다.

통합을 위한 **Splunk Enterprise Event Ingestion** 검사 목록

이 검사 목록을 사용하여 통합의 모든 작업을 안내합니다. 다음 검사 목록에는 설정 및 설치 작업과 통합에 대한 예상 결과를 포함하는 사용 사례의 예가 포함되어 있습니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
다음 표를 사용하여 통합의 설정, 설치 및 구성으로 진행 상황을 추적합니다. 다음 단계로 이동하기 전에 단계에 대한 모든 작업을 완료합니다. 테이블의 각 행은 작업을 나열하고 작업을 수행하는 데 필요한 역할을 식별합니다. 설치 및 구성 안내서의 번호가 매겨진 주제도 참조됩니다.

필요한 역할: 아래의 각 단계에 대한 역할이 나열되어 있습니다.

프로시저

1. 관리자 역할이 있는 ServiceNow AI Platform 사용자가 인스턴스를 설정합니다 ServiceNow AI Platform .
   - 필요에 따라 사용자에게 **sn_si.ingestion_profile_admin** (또는 sn_si.admin) 및 sn_si.analyst 역할을 할당합니다.
   - 서버가 회사 네트워크 내에 배포된 경우 Splunk MID 서버를 설치하고 구성합니다.
   - 플러그인이 ServiceNow 보안 인시던트 응답 릴리스 ServiceNow AI Platform에 맞게 활성화되어 있는지 확인합니다.
   - 콘솔에서 인스턴스로 ServiceNow AI Platform 이벤트를 수동으로 Splunk Enterprise 전달하려면 엔터프라이즈 관리자 권한이 있는 Splunk Enterprise 사용자에게 (sn_sec_splunk_v2.api_account_access) 역할을 할당했는지 확인합니다.

   자세한 내용은 ServiceNow AI Platform 통합을 위한 Splunk Enterprise Event Ingestion 인스턴스 설정 문서를 참조하십시오.

   설정 단계를 성공적으로 완료하고 통합에 대한 예상 결과를 확인했습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

2. 관리자 역할이 있는 ServiceNow AI Platform 사용자는 에서 ServiceNow Store애플리케이션을 설치하고 구성합니다Splunk Enterprise Event Ingestion.
   a. 인스턴스에 애플리케이션을 ServiceNow AI Platform 다운로드하여 설치합니다.
   b. 애플리케이션을 구성하고 콘솔에 연결합니다 Splunk Enterprise .

   자세한 내용은 통합을 위한 Splunk Enterprise Event Ingestion 애플리케이션 설치 및 구성 ServiceNow 문서를 참조하십시오.

3. 옵션: 콘솔에서 인스턴스로 Splunk EnterpriseServiceNow AI Platform 이벤트를 수동으로 익스포트하려면 다음 작업을 수행합니다.
   a. Splunk Enterprise 관리자는 콘솔에서 splunkbase Splunk Enterprise 에 대한 Splunk Enterprise 보안 운영 이벤트 수집 추가 기능을 설치, 설정 및 활성화합니다ServiceNow.
   b. Splunk Enterprise 관리자가 아직 구성을 마치지 않았다면 콘솔에 검색을 경보 Splunk Enterprise 로 저장합니다.

      (Optional) 자세한 내용은 Splunk 이벤트 수집 통합을 위한 Splunk Enterprise 수동 이벤트 수집을 위한 환경 설정 및 통합에 대한 Splunk Enterprise Event Ingestion 콘솔 검색 Splunk Enterprise 저장 문서를 참조하십시오.

4. ServiceNow AI Platform **sn_si.ingestion_profile_admin** 역할을 가진 사용자가 이벤트 프로파일을 생성하고 이름을 지정합니다.

   선택 목록에서 프로파일 유형을 선택합니다. 옵션은 샘플 데이터를 수집하는 데 사용하는 예약된 경보 프로파일 또는 콘솔에서 첨부 파일 데이터를 수동으로 Splunk Enterprise 익스포트하는 데 사용하는 이벤트 프로파일입니다.

   - 예약된 경보의 경우 사용 가능한 경보를 선택합니다.
   - 수동으로 익스포트된 데이터에 대한 프로파일의 경우 새 맵을 작성하거나 기존 맵을 복사합니다.

   자세한 내용은 이벤트 프로파일 생성 및 이름 지정 문서를 참조하십시오.

5. ServiceNow AI Platform **sn_si.ingestion_profile_admin** 역할을 가진 사용자는 수집된 값 또는 보안 인시던트로 Splunk EnterpriseServiceNow AI Platform 익스포트되는 첨부 파일 데이터를 매핑합니다.
   a. 예약된 경보에 대한 샘플 데이터를 가져옵니다.
   b. 이벤트에서 Splunk Enterprise 첨부 파일 데이터를 수동으로 익스포트합니다.
   c. 기본 매핑 구성을 편집합니다.
   d. 필요에 따라 필터링 기준을 추가하고, 기존 보안 인시던트에 경보를 추가하고, 스크립트 편집기를 사용합니다.

   자세한 내용은 통합을 위한 Splunk Enterprise Event Ingestion 경보 및 이벤트 매핑 및 통합에 대한 Splunk Enterprise Event Ingestion 경보 매핑 문서를 참조하십시오.

6. ServiceNow AI Platform **sn_si.ingestion_profile_admin** 역할을 가진 사용자는 보안 인시던트에 ServiceNow AI Platform 표시되는 데이터를 Splunk Enterprise 미리 봅니다.

   오류 메시지가 표시되지 않도록 오류를 수정하거나 누락된 데이터를 추가합니다.

   자세한 내용은 통합에 대한 Splunk Enterprise Event Ingestion 보안 인시던트 미리 보기 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

7. ServiceNow AI Platform **sn_si.ingestion_profile_admin** 역할을 가진 사용자는 예약된 경보가 있는 프로파일에 대한 경보 검색을 예약합니다.

   자세한 내용은 통합에 대한 Splunk Enterprise Event Ingestion 경보 예약 및 검색 문서를 참조하십시오.

Splunk Enterprise Security 이벤트 수집 통합

Splunk Enterprise Security(SIR) 제품과 주목할 만한 이벤트 수집 통합을 보안 인시던트 응답 통해 보안 인시던트 분석가는 주목할 만한 이벤트 데이터(주목할 만한 이벤트라고 함)를 수집하고 처리할 수 있습니다.

Splunk Enterprise Security 이벤트 수집 통합 개요

데이터는 구성된 폴링 일정에 따라 지속적으로 수집되며 분석가가 잠재적인 사이버 위협을 식별하고 대응하는 데 사용됩니다. 수집된 보안 이벤트는 다음에서 Splunk Enterprise Security 주목할 만한 이벤트와 상관관계를 지정한 다음 이 통합을 통해 자동으로 수집될 수 있습니다. 또한 주목할 만한 개별 이벤트를 요청 Splunk Enterprise Security 시 인시던트 검토 콘솔과 보고 인터페이스에서 보안 인시던트 응답ServiceNow AI Platform 제품으로 수동 전달하여 보안 인시던트를 생성할 수 있습니다.

이 통합을 통해 SOC(보안 운영 센터) 분석가는 주목할 만한 이벤트 및 관련 기여 이벤트 데이터를 파악할 수 있습니다. 이 데이터는 추가 조사 및 정정을 위해 (SIR) 보안 인시던트에 ServiceNow AI Platform 보안 인시던트 응답 통합될 수 있습니다. 프로파일은 의 Splunk Enterprise Security상관 검색을 통해 작성되는 여러 가지 중요한 이벤트 유형을 처리하기 위해 인스턴스에 작성 ServiceNow AI Platform 됩니다. 이러한 프로파일은 보안 인시던트에 SIR 다양한 Splunk 이벤트 필드가 표시되는 방식을 사용자 지정합니다.

주요 기능

이 통합에는 다음과 같은 주요 기능이 포함됩니다.

- 여러 개의 주목할만한 이벤트 수집 프로필을 생성하여 피싱, 맬웨어, 무단 액세스 시도와 같은 특정 유형의 위협에 대한 SIR 보안 인시던트를 생성합니다.
- 인시던트 검토 콘솔에서 요청 시 이벤트 전달 Splunk ES 을 위한 여러 이벤트 프로파일을 생성하여 SIR 보안 인시던트를 생성합니다.
- 중요한 이벤트 필드 값을 연관된 SIR 보안 인시던트 필드에 끌어서 놓기로 매핑 Splunk 합니다.
- 이벤트 매핑 상세 정보를 확인하기 위해 샘플 주목할 만한 이벤트를 기반으로 하는 보안 인시던트 레이아웃의 SIR 미리 보기입니다.
- 구성 가능한 간격으로 주목할 만한 과거 이벤트뿐만 아니라 진행 중인 이벤트, 새로운 이벤트 및 업데이트된 중요 이벤트를 수집합니다.
- SIR 인시던트 생성 기준을 충족하지 않는 주목할 만한 이벤트(예: 우선순위가 낮은 이벤트, 아직 특정 상태를 달성하지 못한 이벤트 등)를 필터링합니다.
- 중복 보안 인시던트를 방지하기 위해 일치하는 필드 값을 기준으로 이벤트 또는 경보를 기존 SIR 보안 인시던트에 집계합니다.
- 양방향 인터페이스를 통해 SIR 인시던트 생성 및/또는 종결 조건에 따라 주목할 만한 이벤트를 업데이트하여 주목할 만한 이벤트 업데이트를 SIR 인시던트 상태와 동기화 ServiceNow 된 상태로 유지합니다Splunk ES.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

지원되는 **ServiceNow AI Platform** 버전

이 통합에는 com.snc.si_dep 플러그인이 필요합니다. 이 플러그인은 제품을 지원하는 데 필요한 모든 종속성을 보안 인시던트 응답 자동으로 설치합니다. 다른 보안 운영 애플리케이션을 설치 및 활성화하기 전에 이 플러그인을 설치하고 활성화하십시오.

에서 ServiceNow Store다음 보안 운영 애플리케이션을 설치하고 활성화해야 합니다. 원활한 설치를 위해 아래 나열된 순서대로 한 번에 하나의 애플리케이션을 설치하고 활성화합니다.

1. 보안 통합 프레임워크
2. Security Support Common
3. 보안 인시던트 응답

핵심 애플리케이션 설치에 보안 운영 대한 자세한 내용은 해당 애플리케이션 활성화 ServiceNow Store문서를 참조하십시오제품 또는 애플리케이션에 대한 보안 운영 권리 가져오기.

ServiceNow 애드온

ServiceNow 용 Splunk ES 보안 운영 이벤트 수집 추가 기능은 인시던트 검토 콘솔에서 인스턴스로 ServiceNow AI Platform 이벤트를 수동으로 Splunk Enterprise Security 전달하려는 경우에만 필요합니다. 이 ServiceNow 애드온은 splunkbase 에서 사용할 수 있습니다.

splunkbase의 애플리케이션에 대한 Splunk Enterprise 이 ServiceNow 보안 운영 이벤트 수집 애드온은 통합에서 지원하는 자동화된 경보 수집에 필요하지 않습니다.

Splunk 지원 버전

이 통합은 버전 8.0.1 및 애플리케이션 버전 6.2.1에서 Splunk EnterpriseSplunk Enterprise Security 테스트되었습니다.

MID 서버

이 통합을 위해서는 서버가 회사 네트워크 내에 배포될 때 Splunk 서비스에 연결하기 Splunk 위해 인스턴스에 MID 서버가 ServiceNow AI Platform# 설치 및 구성되어 있어야 합니다. 서비스를 사용하는 Splunk Cloud 경우에는 MID 서버가 필요하지 않습니다. MID 서버에 대한 자세한 내용은 MID 서버를 참조하십시오.

참조

참조	문서 식별자	문서 제목
1	Splunk 제품 웹 사이트	Splunk Enterprise Security 제품 웹 사이트.

검사 목록

이러한 주제에 대한 인쇄 가능한 검사 목록은 다음 문서를 참조하십시오 주목할 만한 이벤트 수집 통합을 위한 Splunk Enterprise Security 검사 목록. 이 목록을 사용하여 통합 작업을 수행할 때의 진행률을 모니터링할 수 있습니다.

이 통합에 사용되는 주요 용어

이 섹션에서는 이 통합에 사용된 몇 가지 주요 용어에 대해 설명합니다.

다음 주요 용어는 설치 및 구성 중에 사용됩니다. 이 약관에 대한 자세한 내용은 ServiceNow 제품 설명서 웹 사이트 와 Splunk 웹 사이트 및 Splunk 자원 페이지의 자원을 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

ServiceNow AI Platform

엔터프라이즈 ServiceNow 제품입니다. ServiceNow AI Platform 는 (),SIR ITSM(IT Service Management) 및 기타 제품과 같은 보안 인시던트 응답 개별 구성요소의 기반입니다.

ServiceNow Splunkbase 애드온

통합의 수동 이벤트 전달 옵션을 지원하는 콘솔에 설치된 Splunk Enterprise Security 애플리케이션입니다ServiceNow. 수동 이벤트 전달은 통합의 선택적 기능입니다. 이 ServiceNow Splunkbase 추가 기능은 에서 Splunk이벤트를 끌어오는 통합에서 제공하는 자동화된 주목할 만한 이벤트 수집에 필요하지 않습니다.

보안 인시던트 응답(SIR)

ServiceNow AI Platform 검색 및 초기 분석부터 방지, 근절 및 복구를 거쳐 최종 사후 인시던트 검토 및 종결에 이르는 보안 인시던트의 진행 상황을 추적하는 애플리케이션입니다.

Splunk Enterprise Security

Splunk Enterprise Security 는 팀이 지속적인 모니터링, 인시던트 응답, SOC 운영을 위해 조직 전체의 가시성과 보안 인텔리전스를 확보하고 경영진에게 비즈니스 위험에 대한 창을 제공하는 데 도움이 됩니다. Splunk Enterprise Security 는 유료 라이센스가 필요한 프리미엄 보안 솔루션입니다. 이 서비스는 이 가이드에서 콘솔이라고 하는 호스트 또는 Splunk 클라우드 오퍼링 Splunk 에 있습니다.

Splunk Enterprise Security 주목할 만한 이벤트

상관 관계 검색이 이벤트 또는 이벤트 패턴을 식별하면 주목할 만한 이벤트가 생성됩니다. 상관 관계 검색은 보안 데이터를 필터링하고 이벤트 간에 상관 관계를 지정하여 특정 유형의 인시던트(또는 이벤트 패턴)를 식별한 다음 주목할 만한 이벤트를 생성합니다.

Splunk 이벤트

서비스의 주목할 만한 이벤트를 Splunk 발생시키는 하나 이상의 데이터 요소입니다. 인스턴스에서 ServiceNow AI Platform 보안 Splunk 인시던트를 트리거 ServiceNow AI Platform 한 이벤트를 조회할 수 있습니다.

MID 서버

이 애플리케이션은 외부 애플리케이션, 데이터 소스 및 서비스 간의 데이터 이동 및 통신을 용이하게 합니다 ServiceNow AI Platform . 이 애플리케이션은 일반적으로 온프레미스 기술과의 통합에 필요하며, 이 Splunk Enterprise Security 이벤트 수집 통합의 경우 MID 서버는 의 인스턴스 및 온프레미스 인스턴스 Splunk Enterprise Security간의 ServiceNow AI Platform 통신을 용이하게 합니다. 인스턴스를 인스턴스와 Splunk Cloud 통합하는 ServiceNow AI Platform 경우에는 MID 서버가 필요하지 않습니다.

보안 인시던트 관리자(sn_si.admin)

이 역할이 있는 사용자는 인스턴스의 제품과의 SIR 통합 구성을 감독합니다 ServiceNow AI Platform .

보안 인시던트 분석가(sn_si.analyst)

이 역할을 가진 사용자는 제품의 보안 인시던트와 상호작용하고 이를 분석합니다 ServiceNow 보안 인시던트 응답 .

ServiceNow AI Platform® 통합을 위한 **Splunk Enterprise Security** 인스턴스 설정

다음 섹션에서는 에서 애플리케이션을 ServiceNow Store설치하기 전에 인스턴스에서 완료해야 ServiceNow AI Platform# 하는 설정 작업을 나열합니다.

필요한 역할: sn_si.ingestion_profile_admin.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
sn_si.admin 역할은 기본적으로 필수 권한을 상속하므로 sn_si.admin 역할을 가진 사용자는 프로필 관리자가 사용할 수 있는 모든 작업을 수행할 수 있습니다.

원활한 설치 및 구성을 위해 애플리케이션을 다운로드하고 설치하기 전에 다음 테이블을 참조하고 나열된 작업을 모두 완료했는지 확인하십시오.

1. 필수 ServiceNow AI Platform# 및 보안 인시던트 응답 (SIR) 역할을 할당했는지 확인합니다.

인스턴스에서 통합을 ServiceNow AI Platform# 설치, 설정 및 사용하려면 다음 역할이 필요합니다.

- 관리자 역할(admin)을 ServiceNow AI Platform# 가진 사용자는 보안 인시던트 관리자 (sn_si.admin) 역할을 사용하여 애플리케이션을 ServiceNow Store 설치합니다.
- 이 통합에서 주목할 만한 이벤트를 수동으로 Splunk Enterprise Security 전달하려면 admin 역할을 가진 ServiceNow AI Platform# 사용자가 에서 (sn_sec_splunkes.api_account_access) 역할을 ServiceNow AI Platform#가진 사용자를 할당합니다. 이 역할을 사용하면 관리자 역할이 있는 Splunk Enterprise Security 사용자가 이 통합에 대한 수동 이벤트 전달에 필요한 API ServiceNow AI Platform# 에 액세스할 수 있습니다.

  중요한 이벤트를 인스턴스에서 자동으로 Splunk Enterprise SecurityServiceNow AI Platform# 수집하는 경우 통합에 (sn_sec_splunkes.api_account_access) 역할이 필요하지 않습니다.

- **sn_si.ingestion_profile_admin** 역할을 가진 사용자는 다음에서 ServiceNow AI Platform#다음 작업을 감독합니다
  - . 이벤트 프로파일 이름 지정, 생성 및 편집.
  - 의 Splunk Enterprise Security 값을 선택하고 보안 인시던트에 매핑합니다 ServiceNow AI Platform# .
  - 구성을 완료하기 전에 보안 인시던트 상세 정보가 정확한지 미리 봅니다.
  - 진행 중인 주목할 만한 이벤트 수집을 예약합니다.
  - SIR 인시던트가 생성되고 종결될 때 주목할 만한 이벤트 업데이트를 활성화합니다.
  - 보안 인시던트 분석가(sn_si.analyst) 역할을 할당합니다.
  - sn_si.analyst 사용자는 보안 인시던트에 대한 작업을 수행합니다.

자세한 내용은 다음 문서를 참조하십시오 Managing roles .

2. 사용자 역할을 할당합니다 Splunk .

에서 Splunk 보안 분석가(ess_analyst) 사용자 역할 할당 서버에서 모든 통합 관련 작업을 Splunk 수행하기 위한 ES

3. API 버전 7.2.6 이상을 Splunk 사용하고 있는지 확인합니다. 이전 버전은 지원되지 않습니다.

콘솔에 액세스할 Splunk Enterprise Security 수 있는 경우 이 통합에 필요한 API에 액세스할 수 있습니다. API에 필요한 다른 특수 설정은 없습니다.

4. MID Server를 설치하고 구성했는지 확인하십시오.

MID 서버ServiceNow AI Platform# 서버가 회사 네트워크 내에 배포된 경우 Splunk 인스턴스에 있는 A가 서비스에 연결 Splunk 되어야 합니다. 자세한 내용은 MID 서버를 참조하십시오.

클라우드 서비스를 사용하는 Splunk Enterprise Security 경우에는 a MID 서버 가 필요하지 않습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. ServiceNow 통합을 지원하는 데 필요한 핵심 애플리케이션이 설치되고 활성화되었는지 확인합니다.

   보안 인시던트 응답 Dependency 플러그인(com.snc.si_dep)이 필요합니다. 이 플러그인은 제품을 지원하는 데 필요한 모든 종속성을 보안 인시던트 응답 자동으로 설치합니다. 통합에 필요한 다른 보안 운영 애플리케이션을 설치하고 활성화하기 전에 이 플러그인을 설치하고 활성화합니다.

   에서 ServiceNow Store다음 보안 운영 애플리케이션이 설치되고 활성화되는지 확인합니다. 설치되지 않은 경우 원활한 설치를 위해 다음 순서로 한 번에 하나의 애플리케이션을 설치하고 활성화합니다.

   a. 보안 인시던트 응답

   b. 보안 통합 프레임워크

   c. 보안 지원 공통
   핵심

   애플리케이션 설치에 보안 운영 대한 자세한 내용은 해당 애플리케이션 활성화 ServiceNow Store문서를 제품 또는 애플리케이션에 대한 보안 운영 권리 가져오기 참조하십시오.

통합을 위한 인스턴스를 성공적으로 설정 ServiceNow AI Platform# 했습니다. 다음 단계는 통합을 위해 에서 ServiceNow Store 주목할 만한 이벤트 수집 애플리케이션을 설치하는 Splunk Enterprise Security 것입니다. 자세한 내용은 주목할 만한 이벤트 수집 통합 설치 및 구성 Splunk Enterprise Security 문서를 참조하십시오.

통합을 위해 콘솔에서 주목할 만한 이벤트를 요청 시 Splunk Enterprise Security 수동 익스포트하려면 문서를 Splunk 주목할 만한 이벤트 수집 통합의 수동 이벤트 수집을 Splunk Enterprise Security 위한 환경 설정 참조하십시오.

주목할 만한 이벤트 수집 통합 설치 및 구성 **Splunk Enterprise Security**

인스턴스에서 통합을 ServiceNow AI Platform# 실행하기 전에 다음 설치 및 구성 단계를 완료하여 애플리케이션이 인스턴스의 및 보안 운영 제품과 ServiceNow AI Platform# 제대로 통합 보안 인시던트 응답 되도록 합니다.

시작하기 전에
필요한 역할: ess_analyst

Splunk 서버에서 모든 통합 관련 활동을 수행하도록 Splunk ES에서 보안 분석가(ess_analyst) 사용자 역할을 할당합니다.

프로시저

1. 통합을 위해 에서 ServiceNow Store 이벤트 수집 애플리케이션을 설치하지 Splunk Enterprise Security 않은 경우 를 참조 보안 운영 통합 설치 하고 단계에 따라 설치합니다.
2. 애플리케이션을 성공적으로 설치한 후 통합 〉 통합 구성 이벤트 수집 타일을 Splunk 찾습니다.
3. 애플리케이션을 구성하려면 새로 만들기를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 또는 구성 단추가 타일에 표시되면 클릭하여 기존 구성을 편집합니다.
5. 표시되는 이벤트 수집 구성 대화 상자에서 필드에 내용을 입력합니다.

   다음 그림은 MID 서버가 있는 온프레미스 버전의 Splunk Enterprise Security 구성에 대해 작성된 양식의 예입니다.

   인시던트 검토 콘솔에서 수집하는 Splunk Enterprise Security 주목할 만한 각 Splunk Enterprise Security 이벤트 유형에는 인스턴스에 고유한 이벤트 프로파일이 ServiceNow AI Platform# 필요합니다. 그러나 이벤트 수집 구성 양식에서 구성하는 소스는 각 프로필이 고유한 주목할만한 이벤트 유형을 수집하는 한 여러 ServiceNow AI Platform# 프로필에 다시 사용할 수 있습니다.

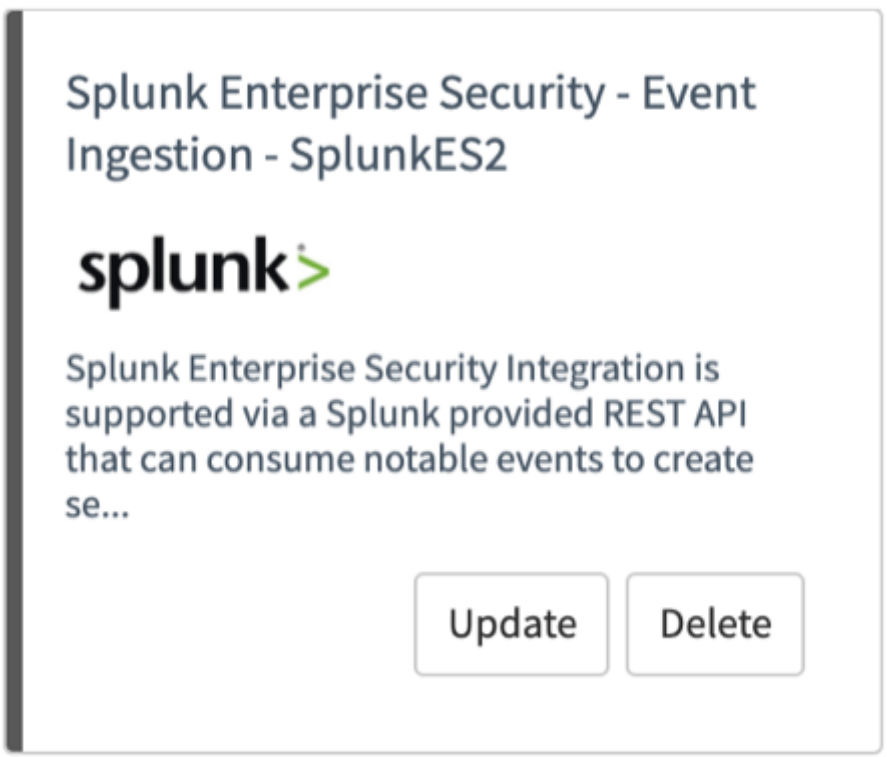
6. 제출을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

확인이 성공적으로 완료되면 각 구성과 함께 보안 통합 페이지가 표시됩니다. 유효한 각 구성 타일에는 다음 그림과 같이 업데이트 및 삭제 버튼이 표시됩니다.

주:
사용자는 기본 인증 또는 토큰 기반 인증을 사용해야 합니다. 둘 다 사용하도록 설정하면 다음 오류가 발생합니다.

주:
사용자가 기존 구성 타일을 토큰 기반으로 업데이트하려는 경우 엔터프라이즈 설정 모듈에서 Splunk 토큰 기반 인증 지원 설정에 대한 기존 Splunk 소스 구성을 업데이트하려면 이 설정 활성화를 활성화해야 합니다.



성공적으로 확인 및 제출되면 각 이벤트 수집 Splunk 서버 구성이 보안 통합 페이지에 타일로 저장됩니다. 저장된 구성 타일이 보안 통합 페이지에 표시되지 않으면 페이지 오른쪽 상단 모서리에 있는 구성 표시 목록에서 예를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 수행할 작업
애플리케이션을 성공적으로 설치하고 구성했습니다. 다음 단계는 이벤트 프로파일을 만드는 것입니다.

엔터프라이즈 보안 설정 구성 **Splunk**

Splunk ES(엔터프라이즈 보안) 설정을 사용하여 사전 설정 구성과 해당 값을 요구 사항에 따라 수정합니다.

시작하기 전에
필요한 역할: sn_si.ingestion_profile_admin

주:
sn_si.admin 역할은 기본적으로 필수 권한을 상속하므로 sn_si.admin 역할을 가진 사용자는 프로필 관리자가 사용할 수 있는 모든 작업을 수행할 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 **Splunk ES** 통합 〉 **Splunk ES** 설정.
2. 양식에서 필드를 채웁니다.

Splunk ES 설정

필드	설명
단일 인시던트로 집계할 수 있는 주목할 만한 이벤트의 수를 제한하십시오.	단일 인시던트로 집계하려는 중요 이벤트의 수를 제한하는 옵션입니다. 기본적으로 이 값은 100으로 설정됩니다.
24시간 동안 만들 수 있는 보안 인시던트 수를 제한하십시오.	24시간 동안 만들 수 있는 보안 인시던트 수를 제한하는 옵션입니다. 기본적으로 이 값은 1000으로 설정됩니다.
에서 Splunk수신한 각 필드에서 구문 분석할 값의 수를 제한하십시오.	에서 받은 Splunk각 필드에 대해 구문 분석할 값의 수를 제한하는 옵션입니다. 기본적으로 이 값은 1000으로 설정됩니다.
가져올 Splunk상관관계 규칙의 수입니다.	에서 Splunk검색할 상관 관계 규칙의 수를 정의하는 옵션입니다. 기본적으로 이 값은 500으로 설정됩니다.
검색 작업에 대한 Splunk 유효 기간(Time-to-Live) 매개변수(초)입니다.	검색에 대한 Splunk 유효 기간 매개변수를 초 형식으로 정의하는 옵션입니다. 기본적으로 이 값은 600으로 설정됩니다.
한 번의 검색으로 일괄 처리할 주목할 만한 유형의 수입니다.	단일 검색에서 배치하려는 주목할 만한 유형의 총 수를 정의하는 옵션입니다. 기본적으로 이 값은 20으로 설정됩니다.
검색 작업 메타데이터를 유지할 Splunk 일수 ServiceNow	Splunk 검색 작업 메타데이터를 ServiceNow유지하려는 일 수를 정의하는 옵션입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	기본적으로 이 값은 30으로 설정됩니다.
필드 매핑에서 값을 분할하는 구분 기호 문자입니다.	필드 매핑에서 값을 분할할 구분 기호를 정의하는 옵션입니다. 기본적으로 값은 (,)으로 설정됩니다.
에서 Splunk 이벤트를 가져오는 동안 추가할 중복 시간(분)(Splunk의 인덱싱 지연 극복)	에서 인덱싱 지연Splunk을 극복하기 위해 이벤트를 Splunk 검색하는 동안 추가할 중복 시간(분)을 정의하는 옵션입니다. 기본적으로 이 값은 30으로 설정됩니다.
업데이트된 주목할 만한 이벤트 끌어오기	업데이트된 중요 이벤트를 검색하는 옵션입니다. 기본적으로 값은 아니요로 설정됩니다.
토큰 기반 인증 지원을 위한 기존 Splunk 소스 구성을 업데이트하려면 이 설정을 활성화합니다. 이 설정을 사용하도록 설정한 후 토큰 상세 정보로 통합 구성을 업데이트해야 합니다.	기존 Splunk 소스 구성을 기존 버전의 토큰 기반 인증 지원으로 업데이트하는 옵션입니다. **주:** 새 버전으로 업그레이드하면 토큰 필드를 사용할 수 없게 됩니다. 토큰 기반 인증을 가져오려면 이 설정을 활성화해야 하며, 그 후에는 토큰 상세 정보로 통합 구성을 업데이트해야 합니다. 기본적으로 값은 아니요로 설정됩니다.
수집 중에 종결된 Notable을 끌어오려면 확인란을 활성화합니다.	종결된 이벤트를 ServiceNow Splunk ES 인스턴스로 끌어오는 옵션입니다. 선택하지 않으면 활성 이벤트만 인스턴스로 끌어와집니다. 기본적으로 값은 아니요로 설정됩니다.

3. 저장을 클릭합니다.

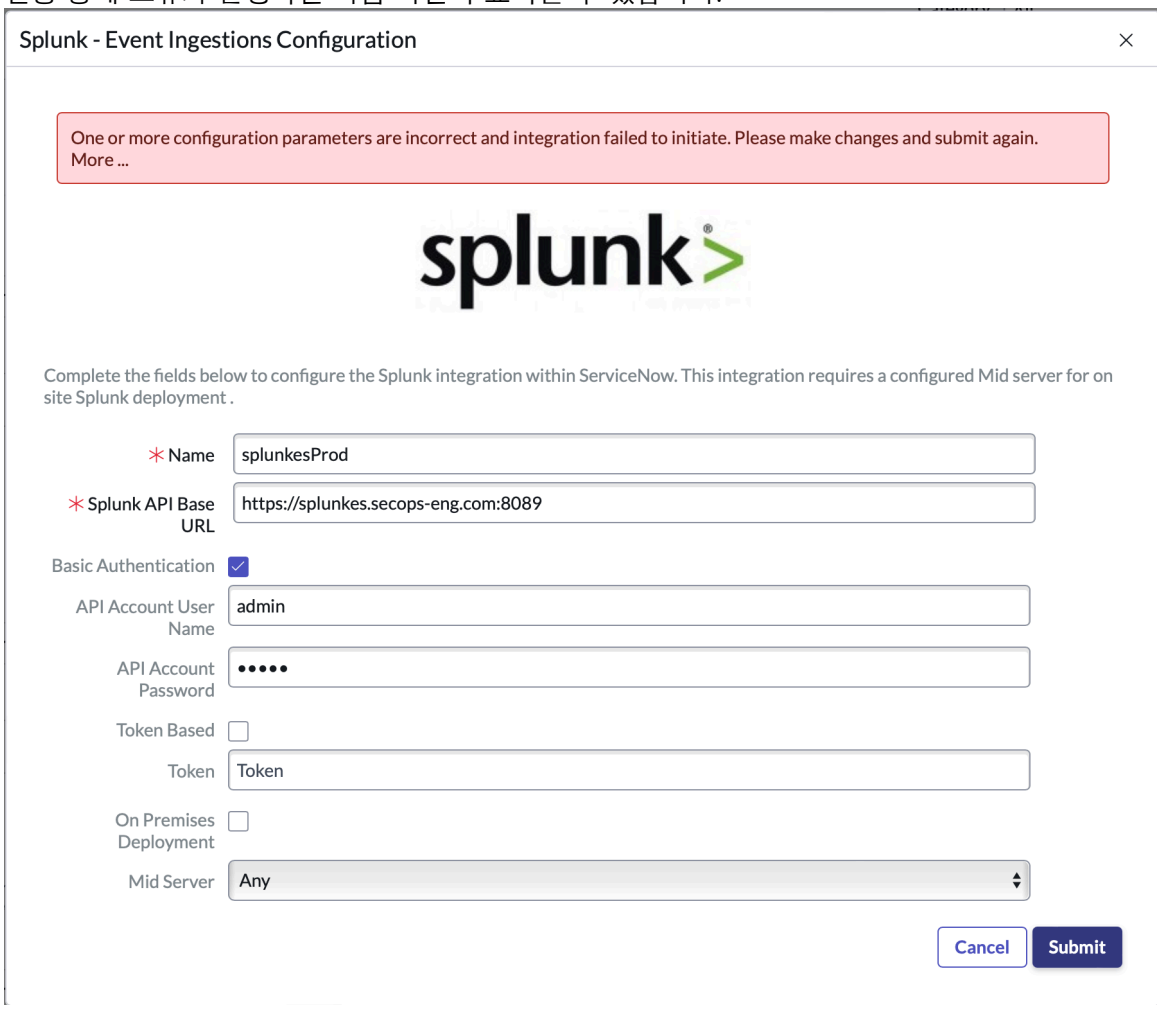
인증 오류

이 섹션에서는 몇 가지 일반적인 인증 오류와 이를 해결할 수 있는 방법에 대해 설명합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

인증서 확인 문제

인증 중에 오류가 발생하면 다음 화면이 표시될 수 있습니다.



API 계정 자격 증명과 Splunk 기준 URL 정보가 올바른지 확인한 경우 포트 8089 통신에 대한 Splunk 인증서 문제로 인해 이 오류가 발생할 수 있습니다. ServiceNow# 보안 연결을 설정하려면 인스턴스에 서버 호스트 이름과 일치하는 일반 이름의 유효한 인증서가 필요합니다. 자세한 내용은 인증서를 참조하십시오. 이 오류가 표시되면 시스템 로그를 확인하여 문제가 인증서 문제로 인한 것인지 확인할 수 있습니다.

다음과 유사한 오류 조건이 나타날 수 있습니다.

인증을 계속하려면 포트 8089에서 API 액세스를 위해 제공된 Splunk 기본 인증서를 교체해야 합니다. SSL 인증서를 교체하는 방법에 대한 자세한 지침은 KB0778285 를 참조하십시오.

이벤트 수집 통합을 위한 **Splunk Enterprise Security** 이벤트 프로파일 생성 및 이름 지정

인스턴스에 이벤트 프로파일을 ServiceNow AI Platform 생성하고 어떤 Splunk 중요 이벤트가 보안 인시던트를 생성하는지 결정합니다.

시작하기 전에
필요한 역할: sn_si.ingestion_profile_admin

주:
sn_si.admin 역할은 기본적으로 필수 권한을 상속하므로 sn_si.admin 역할을 가진 사용자는 프로필 관리자가 사용할 수 있는 모든 작업을 수행할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보

SIR수집된 중요 이벤트에서 보안 인시던트가 생성되기 전 ServiceNow AI Platform 보안 인시던트 응답 ()에는 실제 보안 인시던트가 생성되는 방식을 미리 볼 수 있도록 경보의 필드 값이 보안 인시던트의 ServiceNow AI Platform 레이아웃에 표시됩니다.

사용 가능한 API Splunk ES 를 사용하는 통합 관점에서 주목할 만한 이벤트는 개별적인 주목할 만한 이벤트로 개별적으로 수동 전달되거나 정의된 프로파일 유형에 따라 인스턴스 환경 ServiceNow AI Platform 으로 보안 운영 자동으로 수집됩니다.

예를 들어, 통합 워크플로우는 무단 접근 시도 및 맬웨어와 같은 다양한 유형의 주목할 만한 이벤트를 수집합니다. 이러한 주목할 만한 이벤트는 인스턴스 환경에서 구성하는 보안 운영 프로파일에 따라 수집됩니다.

모든 주목 항목은 처음에 프로파일에서 구성된 상관 관계 검색 유형에 대해 수집됩니다. 그런 다음 수집된 유명 인사를 추가로 필터링하여 보안 인시던트를 생성하는 유명 인사를 지정할 수 있습니다. 예를 들어, 고위험으로 식별된 주목할 만한 이벤트에 대해서만 보안 인시던트를 생성하는 필터를 선호할 수 있습니다. 프로필이 활성화되고 수집된 중요 이벤트에서 보안 인시던트를 생성하기 전에 중요 이벤트의 개별 필드 값이 미리 보기에 대한 보안 인시던트 레이아웃의 해당 필드에 매핑됩니다.

프로시저

1. 인스턴스의 이벤트 프로파일 ServiceNow AI Platform 이름은 고유해야 하며 특정 시점에 하나의 활성 이벤트 프로파일에만 매핑할 수 있습니다.
2. 통합 ServiceNow AI Platform 워크플로우를 사용하여 특정 유명 인사를 수집합니다.
   콘솔에서 선택 기준을 Splunk ES 충족하는 주목할 만한 모든 중요 이벤트는 처음에 인스턴스에 수집 ServiceNow AI Platform 됩니다.
3. your ServiceNow AI Platform 의 프로필은 콘솔에서 주목할 만한 이벤트를 캡슐화한 Splunk ES 것입니다.
   프로필과 함께 수집되는 주목할 만한 이벤트와 콘솔에 대한 연결 Splunk ES 사이에는 일대일 관계가 있습니다. 즉, 하나의 연결에 대해 하나의 주목할 만한 이벤트 유형이 있습니다.
4. 예약된 주목할 만한 이벤트에 대한 프로파일을 생성하려면 을 참조하십시오 예약된 중요 이벤트 수집을 위한 프로파일 설정.
5. 수동 이벤트 전달을 위한 프로파일을 생성하려면 을 참조하십시오 수동 이벤트 전달을 위한 프로필 설정.

예약된 중요 이벤트 수집을 위한 프로파일 설정

정의된 Splunk ES 프로파일에 따라 중요한 이벤트가 인스턴스 환경 ServiceNow AI Platform 으로 보안 운영 자동으로 수집됩니다.

다음 테이블에는 주목할 만한 이벤트의 예약된 수집을 위한 프로파일을 설정하기 위해 따라야 하는 작업 목록이 나와 있습니다.

예약된 중요 이벤트 수집을 위한 프로파일 설정 단계

작업	섹션
이벤트 프로파일 생성	일정이 예약된 중요 이벤트 수집을 위한 프로파일 생성 문서를 참조하십시오.
상관 관계 검색 이름을 기준으로 주목할 만한 이벤트 선택	이벤트 수집 통합을 위한 Splunk ES 프로파일의 상관 관계 규칙 이름을 기반으로 주목할 만한 이벤트 선택 문서를 참조하십시오.
주목할 만한 이벤트 필드 매핑	통합을 위한 Splunk Enterprise Security 주목할 만한 이벤트 필드 매핑 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예약된 중요 이벤트 수집을 위한 프로파일 설정 단계

작업	섹션
사용자 지정 매핑 생성	중요 이벤트 인시던트 검토 및 기여 이벤트 상세 정보(예약된 수집)에 대한 Splunk ES 매핑 생성 문서를 참조하십시오.
보안 인시던트 미리 보기	이벤트 수집 통합에 Splunk Enterprise Security 대한 보안 인시던트 미리 보기 문서를 참조하십시오.
신규 및 업데이트된 중요 이벤트 예약 및 검색	이벤트 수집 통합을 위해 Splunk Enterprise Security 새롭고 업데이트된 주목할 만한 이벤트 예약 및 검색 문서를 참조하십시오.
SIR 인시던트 상태에 따라 중요한 이벤트 업데이트 및 종결 자동화	SIR 인시던트 상태에 따라 중요한 이벤트 업데이트 및 종결 자동화 문서를 참조하십시오.

일정이 예약된 중요 이벤트 수집을 위한 프로파일 생성

중요한 이벤트를 자동으로 수집하도록 프로필을 설정할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.ingestion_profile_admin

주:
sn_si.admin 역할은 기본적으로 필수 권한을 상속하므로 sn_si.admin 역할을 가진 사용자는 프로필 관리자가 사용할 수 있는 모든 작업을 수행할 수 있습니다.

프로시저

1. 인스턴스에서 주목할 만한 이벤트 또는 상관 관계 규칙 유형에 ServiceNow AI Platform 대한 이벤트 프로파일을 생성하려면 다음으로 이동하십시오. **Splunk Integration** 〉 **Splunk** 이벤트 프로파일.
2. 이벤트 프로파일 양식이 Splunk 표시되지 않으면 진행률 표시줄에서 이름을 클릭합니다.
3. 새로 만들기를 클릭합니다.
4. 필드에 내용을 입력합니다.

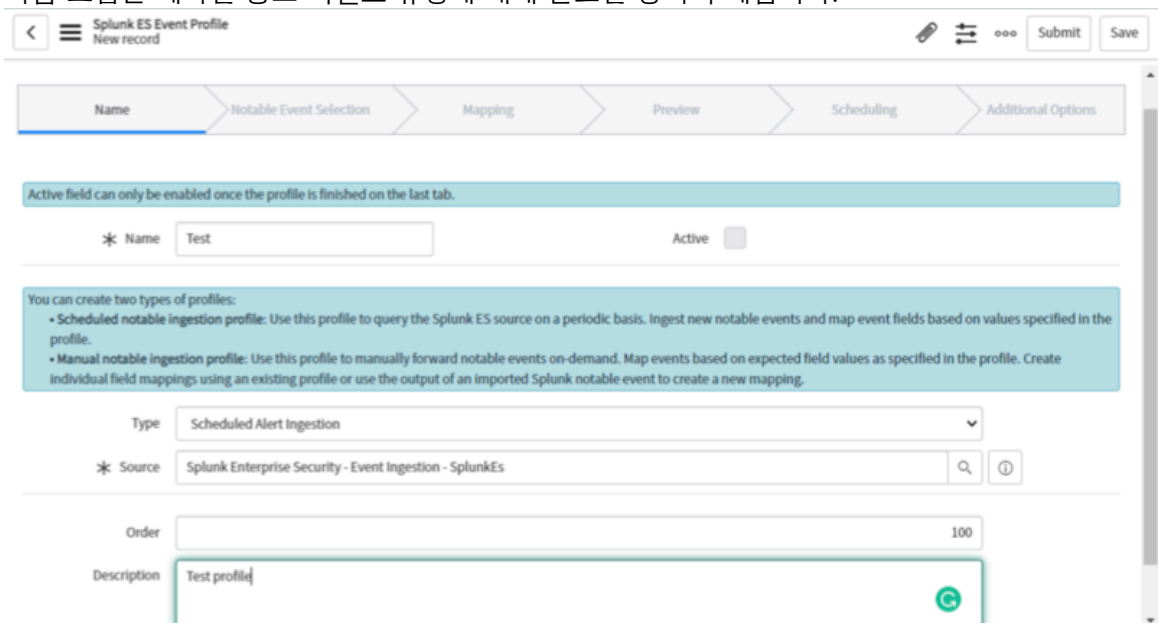
   완료된 양식의 예가 테이블 다음에 나옵니다.

필드	설명
이름	프로파일의 고유한 이름입니다. 이름이 고유하지 않으면 오류가 표시되고 중복된 프로파일 이름은 저장되지 않습니다. 인스턴스의 프로파일 이름은 ServiceNow AI Platform 고유해야 합니다.
활성	확인란은 기본적으로 선택이 취소되고 비활성화되어 있습니다. 프로파일을 활성화하기 전에 프로파일의 모든 섹션을 완료해야 합니다.
유형	선택 목록에서 프로파일 유형을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	○ 예약된 이벤트 수집: 이 유형의 프로필은 구성된 일정에 따라 수집되는 중요한 이벤트를 지원합니다. 필드에 내용을 입력합니다. ○ 수동 이벤트 전달: 이 유형의 프로파일은 요청 시 인시던트 검토 콘솔에서 수동으로 Splunk Enterprise Security 전달되는 중요한 이벤트를 지원합니다. 이러한 유형의 프로파일에 대한 양식을 작성하려면 다음 단계를 참조하십시오.
소스	Splunk 주목할 만한 이벤트를 수집하도록 구성한 서버 또는 검색 끝입니다. 여러 Splunk 서버가 구성된 경우 프로파일에 대해 수집할 중요 이벤트 유형에 적합한 서버를 선택합니다. 값을 입력해야 합니다.
순서	기본값은 100입니다. 여러 프로필을 만든 경우 둘 이상의 프로필이 동일한 트리거 조건을 공유할 때 이 값은 런타임 실행 우선 순위를 제공합니다. 숫자가 가장 낮은 프로파일의 워크플로우가 가장 높은 우선순위를 갖습니다.
(선택 사항) 묘사	이 프로파일을 다른 프로파일과 구별하는 데 도움이 되는 추가 텍스트입니다.

다음 그림은 예약된 중요 이벤트 유형에 대해 완료된 양식의 예입니다.



5. 일정이 예약된 중요 이벤트가 있는 프로파일의 경우 프로파일 구성을 계속하려면 하나의 옵션을 선택합니다.

다음에 수행할 작업
다음 단계는 자동 수집을 위해 중요한 이벤트를 선택하는 것입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이벤트 수집 통합을 위한 **Splunk ES** 프로파일의 상관 관계 규칙 이름을 기반으로 주목할 만한 이벤트 선택

예약된 중요 이벤트 유형 수집에 대한 프로파일을 생성한 후 해당 중요 이벤트를 보안 인시던트에 ServiceNow AI Platform 보안 인시던트 응답 매핑할 이 프로파일의 상관관계 규칙 이름을 선택합니다Splunk Enterprise Security.

시작하기 전에

필요한 역할: sn_si.ingestion_profile_admin

> **주:**
> sn_si.admin 역할은 기본적으로 필수 권한을 상속하므로 sn_si.admin 역할을 가진 사용자는 프로필 관리자가 사용할 수 있는 모든 작업을 수행할 수 있습니다.

이 태스크 정보

인스턴스에서 사용 가능한 상관관계 규칙을 ServiceNow AI Platform 확인하여 보안 인시던트를 수집하고 생성하려는 주목할 만한 이벤트 유형을 파악합니다. 상관관계 규칙을 선택합니다. 이 양식의 목록에서 주목할 만한 이벤트를 하나 이상 선택할 수 있습니다.

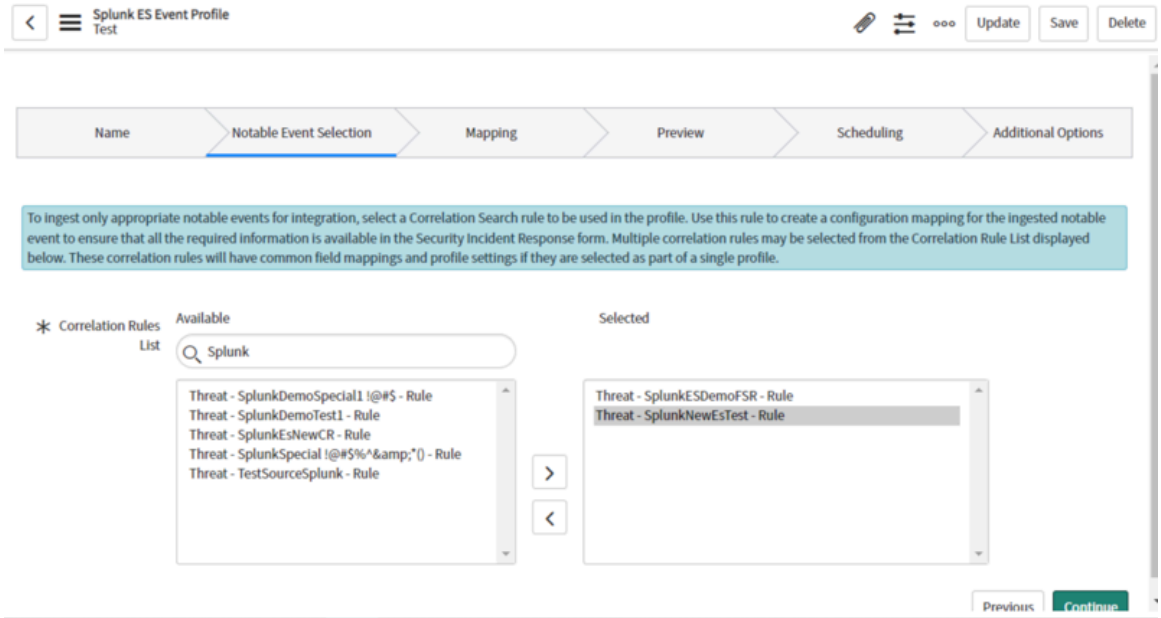
프로시저

1. 주목할 만한 이벤트 선택 페이지가 표시되지 않으면 진행률 표시줄에서 선택하여 표시합니다.
2. 상관관계 규칙 목록에서 다음 옵션 중 하나를 선택하여 단일 상관관계 규칙 또는 여러 상관관계 규칙을 선택하고 이동한 다음 사용 가능한 열에서 선택됨 열로 이동합니다.

   이 양식의 상관관계 규칙 목록은 인시던트 검토 콘솔의 상관관계 규칙 Splunk ES 목록과 일치합니다. 이 양식에는 최대 500개의 상관관계 규칙이 표시됩니다. 목록에 Splunk ES500개가 넘는 상관관계 규칙이 있는 경우 인스턴스의 이 양식 ServiceNow AI Platform 에는 처음 500개의 중요한 이벤트만 표시됩니다.

옵션	설명
상관관계 규칙 목록 검색 필드에 텍스트를 입력합니다.	검색 필드 아래의 열은 입력한 텍스트를 기반으로 사용 가능한 옵션을 사용하여 필터링됩니다. 상관관계 규칙을 선택하고 화살표 키를 사용하여 선택한 경보를 사용 가능에서 선택됨으로 이동합니다.
상관관계 규칙 목록에서 상관관계 규칙을 두 번 클릭합니다.	선택됨 열이 선택 항목으로 채워집니다.
상관관계 규칙 목록에서 상관관계 규칙을 한 번 클릭합니다.	상관관계 규칙이 선택됩니다. 화살표 키를 사용하여 선택한 상관관계 규칙을 사용 가능에서 선택됨으로 이동합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



3. 계속하려면 하나의 옵션을 선택하십시오.

다음에 수행할 작업

예약된 Splunk Enterprise Security 프로파일에 대한 상관관계 규칙을 성공적으로 선택했습니다. 다음 단계는 중요 이벤트 값을 보안 인시던트의 필드에 매핑하는 것입니다.

통합을 위한 **Splunk Enterprise Security** 주목할 만한 이벤트 필드 매핑

프로파일에 대한 특정 상관관계 규칙과 중요한 이벤트 유형을 식별한 후 다음 단계는 중요한 개별 이벤트 필드를 (SIR) 보안 인시던트의 ServiceNow AI Platform 보안 인시던트 응답 필드에 매핑하는 것입니다.

매핑 개요

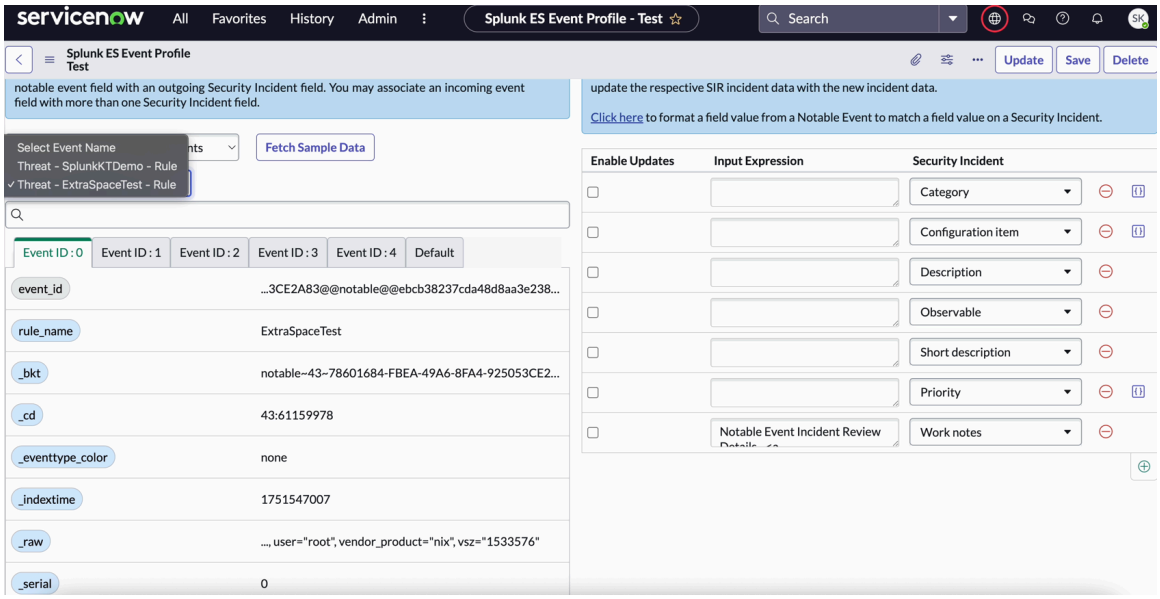
매핑 단계에서는 선택한 상관관계 규칙에 대해 샘플 주목할 만한 이벤트를 수집하거나 수동으로 전달된 주목할 만한 이벤트에 대해 주목할 만한 이벤트 데이터를 익스포트할 수 있습니다. 이벤트 매핑 프로세스는 생성하는 프로파일 유형에 관계없이 동일합니다.

다음 그림은 각 유형의 이벤트 프로파일에 대해 제공되는 기본 매핑 구성의 예입니다. 보안 인시던트를 채우는 필드를 사용자 지정할 수 있습니다. 이 매핑 단계에서는 관련된 모든 중요 이벤트 필드 데이터가 SIR 인시던트 양식의 적절한 위치에 매핑되도록 한 다음 미리 보기 섹션에서 SIR 인시던트를 시각화할 수 있습니다.

여러 상관 관계를 사용하는 경우 필요한 이벤트를 선택하여 주목할 만한 이벤트를 가져올 수 있습니다. 수집하도록 여러 경보를 구성한 경우 경보 이름을 사용하여 경보를 선택합니다.

클릭하여 데이터를 가져오면 Splunk 양식 왼쪽에 주목할 만한 이벤트 필드 이름과 해당 값이 채워집니다. Splunk 보안 인시던트 필드에 매핑할 수 있는 주목할 만한 이벤트 필드입니다SIR. 일부 필드는 SIR 보안 인시던트 필드에 여러 번 매핑될 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



콘솔에서 필드 매핑 구성 단계를 위해 수집할 몇 가지 중요한 이벤트 Splunk 샘플을 검토하는 것이 좋습니다. 이 단계는 진행률 표시줄에 매핑이라는 레이블이 지정됩니다. 이 페이지가 표시되지 않으면 진행률 표시줄에서 매핑 을 클릭합니다. 에서 주목할 만한 이벤트 Splunk Enterprise Security 샘플을 최대 5개까지 수집하여 주목할 만한 이벤트 필드 매핑 프로세스를 지원할 수 있습니다. 선택한 상관관계 규칙에 대해 가장 최근의 5개의 주목할 만한 이벤트를 수집하거나 주목할 만한 이벤트 ID를 기반으로 최대 5개의 특정 주목할 만한 이벤트를 수집할 수 있는 옵션이 있습니다.

다음은 주목할 만한 이벤트를 매핑하는 데 필요한 단계를 요약한 것입니다.

- 예약된 주목할 만한 이벤트 샘플 데이터 수집: 자동으로 수집된 주목할 만한 이벤트 프로파일에 사용되는 샘플 데이터의 경우, 샘플 데이터가 검색되면 사용 가능한 주목할 만한 이벤트 필드와 해당 값이 매핑 양식의 왼쪽에 있는 기본 매핑 레이아웃에 표시됩니다. 끌어온 특정 중요 이벤트 ID의 값을 볼 수 있는 탭이 표시됩니다. 양식 왼쪽에 있는 중요 이벤트 샘플 수집 섹션의 모든 중요 필드가 양식 오른쪽에 있는 보안 인시던트 필드에 매핑 ServiceNow 되는지 확인합니다.
- 필드 매핑: 왼쪽에서 주목할 만한 이벤트 필드를 오른쪽의 SIR 인시던트 매핑 섹션에 끌어서 ServiceNow 놓아 매핑 구성을 편집합니다. 오른쪽의 매핑은 들어오는 중요 이벤트 필드를 나가는 보안 인시던트 필드와 연결합니다.
- 매핑 환경: SIR 인시던트 필드 매핑 섹션 하단에 있는 + 아이콘을 사용하여 필드를 추가하거나 제거하여 매핑 그리드를 사용자 지정합니다. 제공된 색상 코딩으로 간과되거나 중복된 필드를 추적합니다(매핑된 필드는 회색으로 표시되고 파란색 필드는 매핑되지 않음).
- 인시던트 생성 조건: 매핑 섹션이 완료되면 필터 조건을 설정하여 보안 인시던트를 생성할 중요 이벤트와 필터링할 중요 이벤트(예: 우선순위가 낮은 중요 이벤트)를 지정할 수 있습니다. 이 작업은 중요 이벤트 매핑 섹션 아래에 있는 인시던트 생성 조건 섹션에서 수행됩니다.
- 이벤트 집계 기준: 중복될 가능성이 있는 유사한 인시던트를 생성하는 대신 수신되는 중요 이벤트를 기존 SIR 보안 인시던트로 집계하는 추가 이벤트 집계 기준을 정의합니다. 이 추가 집계 기능은 각 프로파일에 대해 필드 일치 값 기준을 사용하여 모든 관련 보안 중요 이벤트 데이터를 단일 보안 인시던트에 배치함으로써 활성 상태의 중복 보안 인시던트 수를 줄일 수 있습니다.
- 필드 형식 변환: 경우에 따라 엔터프라이즈 중요 이벤트의 이벤트 필드 값이 Splunk 보안 인시던트의 SIR 필드로 직접 변환되지 않을 수 있습니다. 이러한 값의 경우 스크립트 편집기를 사용하여 매핑 단계 중에 보안 인시던트의 필드 값에 대한 형식을 지정할 수 있습니다. 비슷하지만 동일하지는 않은 값의 형식을 지정하려면 스크립트 편집기를 사용하십시오. 예를 들어 스크립트 편집기를 사용하면 맬웨어 경보 및 바이러스 감염의 범주 값이 소스 범주에 대해 다를 수 있지만 두 값 모두 필드 번역 서식 지정 기능을 사용하여 보안 인시던트의 SIR 범주 필드에서 공통 악성 코드 활동으로 변환할 수 있습니다.

다음 단계는 중요 이벤트를 수집하고 값을 보안 인시던트 필드에 매핑하는 SIR 것입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

중요 이벤트 인시던트 검토 및 기여 이벤트 상세 정보(예약된 수집)에 대한 **Splunk ES** 매핑 생성

중요 이벤트 필드 매핑 단계에서는 중요 이벤트의 개별 이벤트 필드를 (SIR) 보안 인시던트의 필드로 매핑합니다 ServiceNow AI Platform 보안 인시던트 응답 .

시작하기 전에

필요한 역할: sn_si.ingestion_profile_admin

> **주:**
> sn_si.admin 역할은 기본적으로 필수 권한을 상속하므로 sn_si.admin 역할을 가진 사용자는 프로필 관리자가 사용할 수 있는 모든 작업을 수행할 수 있습니다.

이 태스크 정보

매핑 그리드는 상관관계 규칙 선택에서 선택한 주목할 만한 이벤트 유형에 대해 사용자 지정할 수 있습니다. 이벤트 필드의 색상 코딩은 이미 매핑한 이벤트 값이 회색으로 표시되고 나머지 매핑되지 않은 필드는 모두 파란색으로 나타날 때 추적하는 데 도움이 됩니다. 이렇게 하면 보안 인시던트에 추가된 필드 값과 나머지 중요 이벤트 정보가 매핑되지 않은 상태로 남아 있는지 더 잘 시각화할 수 있습니다.

양식 왼쪽의 중요 이벤트 샘플 수집 열에서 최대 5개의 중요 이벤트를 오른쪽에 있는 SIR 인시던트 필드 매핑 열의 보안 인시던트 필드에 매핑합니다.

양식의 오른쪽에 있는 매핑 그리드에서 필드를 추가하거나 제거하여 사용자 지정 매핑을 생성합니다. 보안 인시던트 응답 양식에 채워야 하는 일반적으로 중요한 필드인 기본 필드가 표시됩니다. 그러나 이러한 필드를 제거할 수 있으며 + 및 - 버튼을 사용하여 추가 필드를 표시할 수 있습니다. 양식 오른쪽의 매핑 그리드에서 필드를 추가하거나 제거하여 사용자 지정 맵을 생성합니다. 필드를 사용자 지정하면 보안 인시던트의 기본 매핑 그리드에 표시되지 않는 필드를 매핑 Splunk 할 수 있습니다 SIR .

프로시저

1. 매핑 양식이 표시되지 않으면 진행률 표시줄에서 매핑 을 클릭합니다.
2. 예약된 수집이 있는 프로필의 경우 주목할 만한 이벤트 샘플 수집 아래에서 샘플 데이터 가져오기를 클릭하여 선택한 상관관계 규칙에 대해 콘솔에서 최신 샘플 주목할 만한 이벤트를 Splunk Enterprise 가져옵니다.

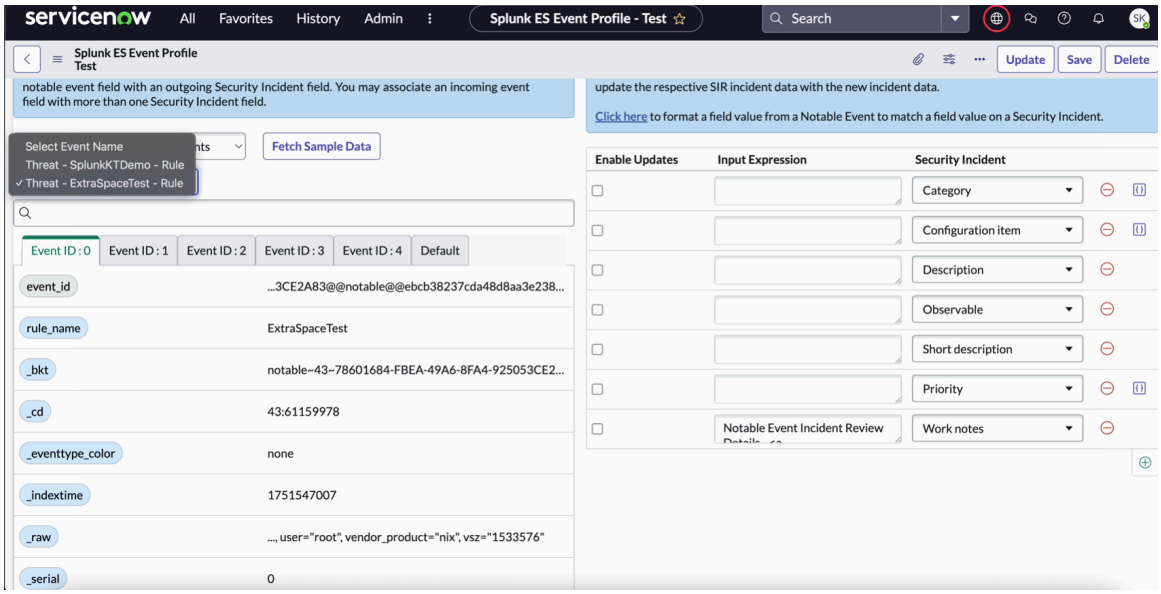
   > **주:**
   > 가장 최근의 샘플 주목할 만한 이벤트를 끌어오거나 주목할 만한 이벤트 매핑 경험에 사용할 특정 주목할 만한 이벤트의 고유한 주목할 만한 이벤트 ID를 제공할 수 있습니다.

   주목할 만한 이벤트 필드와 값 결과는 개별 탭으로 표시됩니다. 주목할 만한 이벤트를 최대 5개까지 수집할 수 있습니다.

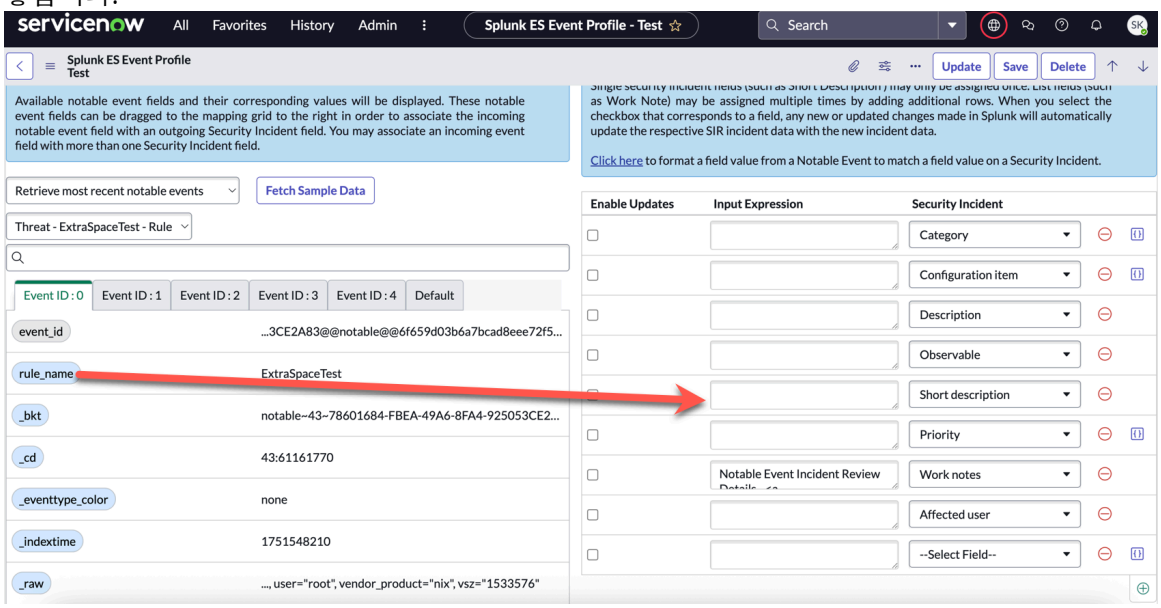
   주목할 만한 샘플 이벤트를 끌어오는 데 몇 분 정도 걸릴 수 있습니다. 트랜잭션이 작동 중임을 나타내는 메시지가 화면 맨 위에 표시됩니다.

   다음 그림에서는 수집 끌어오기가 완료된 후 수집된 주목할 만한 이벤트 또는 임포트된 샘플 이벤트에 대한 필드 이름 값 쌍이 이 양식의 왼쪽에 표시됩니다. 이러한 값은 양식의 SIR 인시던트 필드 매핑 측면에 있는 보안 인시던트 필드에 매핑하는 값입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



3. 양식 왼쪽의 필드 값을 양식 오른쪽에 있는 보안 인시던트의 필드에 매핑하려면 양식 왼쪽에 있는 파란색 필드 이름을 길게 클릭합니다.
4. 필드 이름(예: rule_name)을 끌어서 보안 인시던트 열의 필드 이름 옆에 있는 입력 식 열의 필드에 놓습니다.

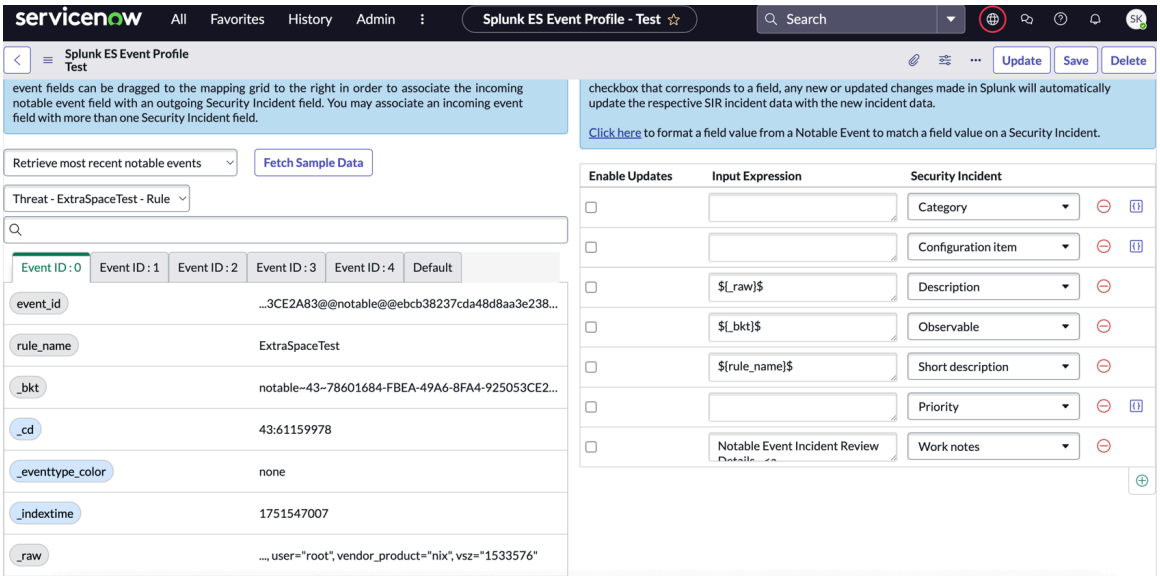


필드 값이 입력 식 열에 표시됩니다. 다음 이미지에서 rule_name 보안 인시던트의 ### ## 필드에 매핑되어 있습니다. 그러나 왼쪽의 모든 값을 오른쪽의 필드와 일치시킬 수 있습니다. 미리 보기 단계에서 보안 인시던트에 값이 올바르게 매핑되었는지 확인합니다.

매핑 프로세스에서 이벤트 필드가 간과되거나 중복되지 않도록 하기 위해 필드는 색으로 구분됩니다. 왼쪽의 연한 파란색 필드는 주목할 만한 이벤트 필드가 아직 선택되지 않았으며 보안 인시던트에 매핑되지 않았음을 나타냅니다. 수신되는 주목할 만한 필드를 보안 인시던트의 둘 이상의 필드와 연결하는 것을 선호할 수 있습니다.

회색 필드는 필드가 선택되었고 보안 인시던트의 필드에 매핑되었음을 나타냅니다. 이 색상 코딩은 매핑을 추적하는 데 도움이 됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

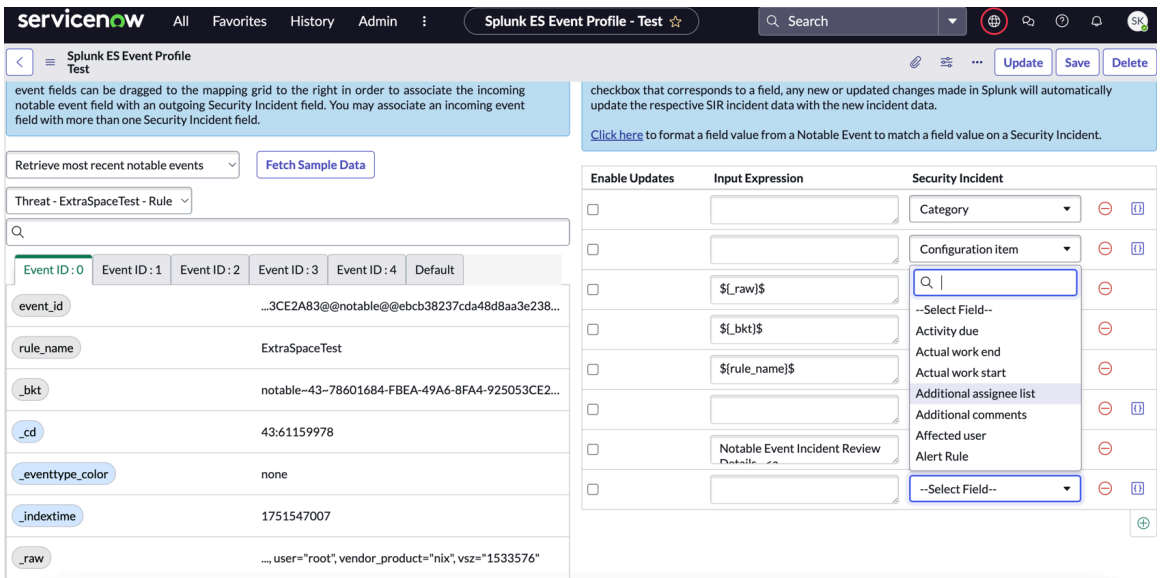


5. 양식 오른쪽의 보안 인시던트에 표시되는 기본 필드에 필드를 추가하려면 다음 단계를 따르십시오.

a. 양식 오른쪽의 SIR 인시던트 필드 매핑 섹션 그리드 하단에서 더하기 아이콘을 클릭합니다. 새 필드가 표시됩니다.

b. 보안 인시던트 열에서 표시되는 목록을 확장하고 필드를 선택합니다.

새 필드의 확장된 목록에서 일부 필드는 음영 처리됩니다. 다음 그림에서 rule_name 는 보안 인시던트에 매핑되었기 때문에 회색 배경입니다. 양식 왼쪽에 있는 중요 이벤트 필드에 대한 색상 코딩과 유사하게 오른쪽에 있는 보안 인시던트 필드에 대한 이 색상 코딩은 이미 매핑된 SIR 인시던트 필드를 추적하는 데 도움이 됩니다.



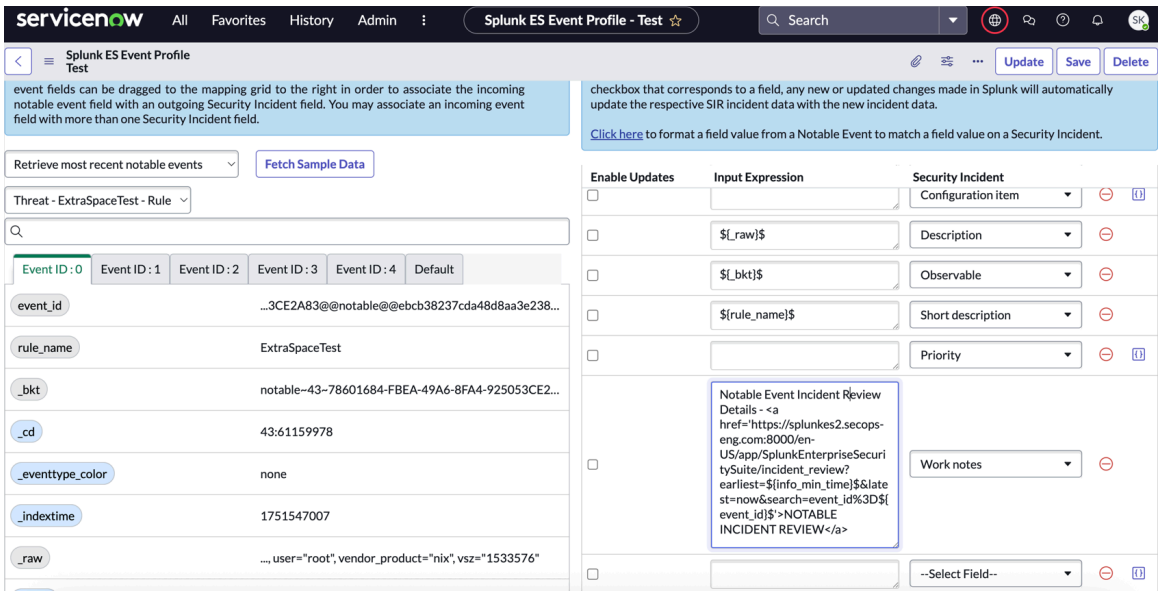
주:
동일한 보안 인시던트에 여러 옵저버블을 표시할 수 있도록 옵저버블 필드를 서로 다른 값으로 여러 번 매핑할 수 있습니다. 마찬가지로 구성 항목 및 작업 메모 필드는 여러 값을 지원합니다. 여러 값을 지원할 수 없는 필드에 두 값을 매핑하려고 하면 인시던트를 미리 볼 때 필드에 값이 없다는 오류 메시지가 표시됩니다. 마찬가지로 보안 인시던트의 필드에 여러 옵션을 선택할 수 있는 목록이 있고 목록에 표시되지 않은 해당 필드에 옵션을 매핑하려고 하면 보안 인시던트에 필드가 채워지지 않습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

c. 또는 새 행의 검색 필드에 값을 입력합니다.

d. 폼의 왼쪽에서 마우스 왼쪽 버튼을 클릭하여 입력 식 필드에서 원하는 이벤트 **ID** 를 선택합니다.

6. 매핑에 필드 값을 추가하거나 제거하여 매핑을 계속합니다.
다음 그림은 편집된 매핑의 예입니다. 오른쪽의 하단 필드에는 작업 메모 필드가 추가되며 둘 이상의 값이 있습니다. 긴 텍스트 문자열 필드의 경우 매핑 필드를 확장하여 전체 문자열을 확인하고 아래 스크린샷에 표시된 대로 필드의 오른쪽 아래 모서리를 당겨 필요에 따라 작업 메모 필드를 추가하여 크기를 조정할 수 있습니다.



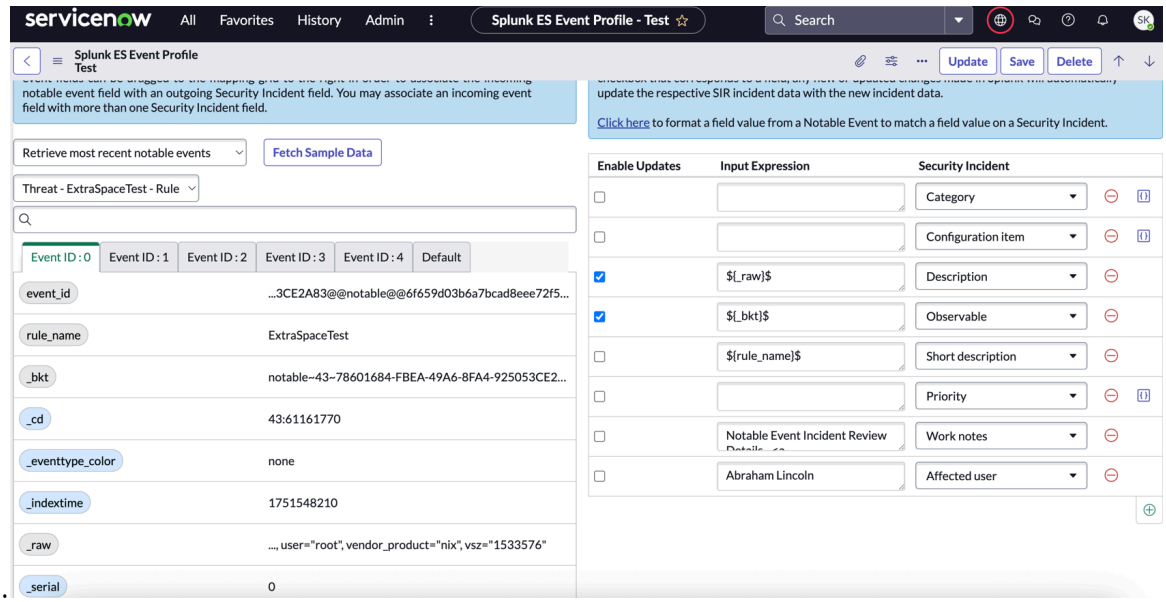
⚠ 경고:
SIR 인시던트 필드 매핑 섹션에서 입력 식 필드에 나와 있는 URL 및 포트 번호는 예시일 뿐이며 바로 사용 가능한 URL 또는 포트 번호가 아닙니다.

미리 보기에서 이러한 값은 보안 인시던트의 작업 메모에 표시됩니다. 이 값은 매핑 섹션에 추가한 필드에 대한 것이고 작업 메모 필드에 매핑된 값이 여러 개 있기 때문에 입력한 대로 값이 표시됩니다. 이 예에서는 필드에 입력한 공백과 구두점이 관련 항목 섹션에 보안 인시던트 미리 보기의 작업 메모로 표시됩니다.

다음 이미지는 이전 이미지의 값이 보안 인시던트에 표시되는 방식의 예입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

7. SIR의 매핑된 필드에 대한 업데이트를 수신하려면 입력 식에 대해 업데이트 사용 확인란을



선택합니다.

8. 옵션: 앞의 필드 매핑 단계를 완료한 후 인시던트 작성 조건 작성기에서 동일한 필드 값을 사용하여 들어오는 중요 이벤트가 보안 인시던트를 만들기 위해 충족해야 하는 추가 기준을 정의할 수 있습니다 SIR .
인시던트 생성 조건을 설정하려면 다음 단계를 수행합니다.

   a. 양식에서 인시던트 생성 조건 섹션으로 스크롤하고 조건을 기준으로 필터링 확인란을 선택하여 옵션을 활성화합니다.

      (Optional) 필터 조건 작성기가 표시됩니다. 이러한 필터를 사용하여 필드에 설명된 특정 조건과 일치하는 보안 인시던트를 생성합니다.

      필터 조건 작성기의 첫 번째 필드에 대한 목록의 옵션은 수집한 이벤트에 대한 중요 이벤트 샘플 수집 섹션에 표시되는 필드와 일치합니다. 이러한 필드는 동적이며 수집하는 중요한 이벤트 또는 수동으로 전달된 중요한 이벤트 샘플에 대해 선택한 이벤트에 따라 Splunk 변경됩니다. 입력하는 기준은 대/소문자를 구분하며 주목할 만한 이벤트의 값과 Splunk Enterprise Security 정확히 일치해야 합니다. 필터 필드에 입력할 값을 잘 모르는 경우에는 콘솔로 돌아가서 Splunk Enterprise Security 키워드에 대한 중요 이벤트를 검토하는 것이 좋습니다.

   b. 조건 작성기의 목록과 필드를 사용하여 첫 번째 행에 대한 필터를 설정합니다.

   c. 조건을 더 추가하려면 필드 오른쪽에서 AND 또는 **OR**을 클릭합니다.
      AND를 선택하면 모든 조건이 일치해야 합니다. **OR**을 선택하면 두 조건을 일치시킬 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

d. 옵션: 두 번째 행에서 두 번째 필터 조건을 설정합니다.

(Optional) 다음 이미지는 보안 인시던트가 생성되기 전에 일치해야 하는 두 가지 조건이 있는 예입니다.

(Optional) 입력한 두 필터링 조건이 모두 일치하는 경우에만 보안 인시던트가 생성되도록 인시던트 생성 조건을 설정했습니다.

이러한 유형의 인시던트 생성 조건 필터링을 사용하면 보안 이벤트 범위를 좁히고 에서 기본 상관관계 검색 또는 필터를 수정하지 않고도 생성되는 불필요한 보안 인시던트 수를 제한할 수 Splunk있습니다. 추가 필터링 기준이 설정되면 모든 기준과 일치하는 주목할 만한 이벤트만 인시던트에 매핑됩니다.

주:
이벤트 필드 이름에 따옴표(″), 하이픈(′), 밑줄(-), at(@) 또는 앰퍼샌드(&)와 같은 특수 문자가 있는 경우 매핑 번역을 위해 이러한 문자를 대체해야 할 수 있으며 중복 이벤트 이름이 작성될 수 있습니다. 매핑을 적절히 수행할 수 있지만 중복된 이벤트 이름이 있는 필드를 구분하기 위해 숫자 접미사가 추가됩니다. 예를 들어 첫 번째 이벤트 필드가 alerts.alert 이고 두 번째 이벤트 필드가 alerts@alerts인 경우 나머지 표준 텍스트 문자가 동일하므로 이러한 필드를 고유하게 식별할 수 없습니다. 이 경우 두 번째 이벤트 필드에 접미사가 추가되고 필드 이름이 alerts@alert(1)로 바뀝니다.

(Optional) 유사한 주목할 만한 사건을 처리하고 중복 인시던트를 방지하기 위한 이벤트 집계 기준

9. 옵션: 중복 보안 인시던트 생성을 방지하려면 들어오는 주목할 만한 이벤트가 미해결 보안 인시던트로 집계되도록 추가 이벤트 집계 기준을 정의합니다.
기준을 설정하려면 아래 단계를 수행합니다.

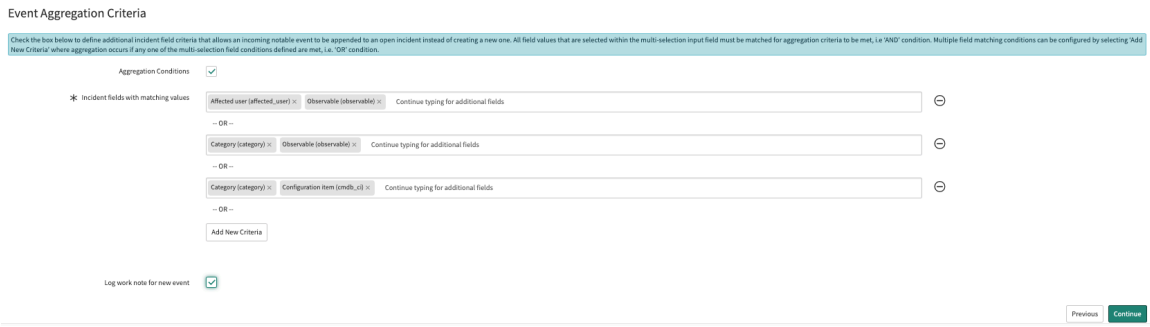
a. 양식의 이벤트 집계 기준 섹션으로 스크롤하고 집계 조건 확인란을 선택하여 이 옵션을 활성화합니다.

(Optional) 일치하는 값이 있는 인시던트 필드가 표시됩니다. 이러한 필드 이름은 보안 인시던트에 구성된 SIR 사용자 지정 필드를 포함하는 보안 인시던트의 필드입니다.

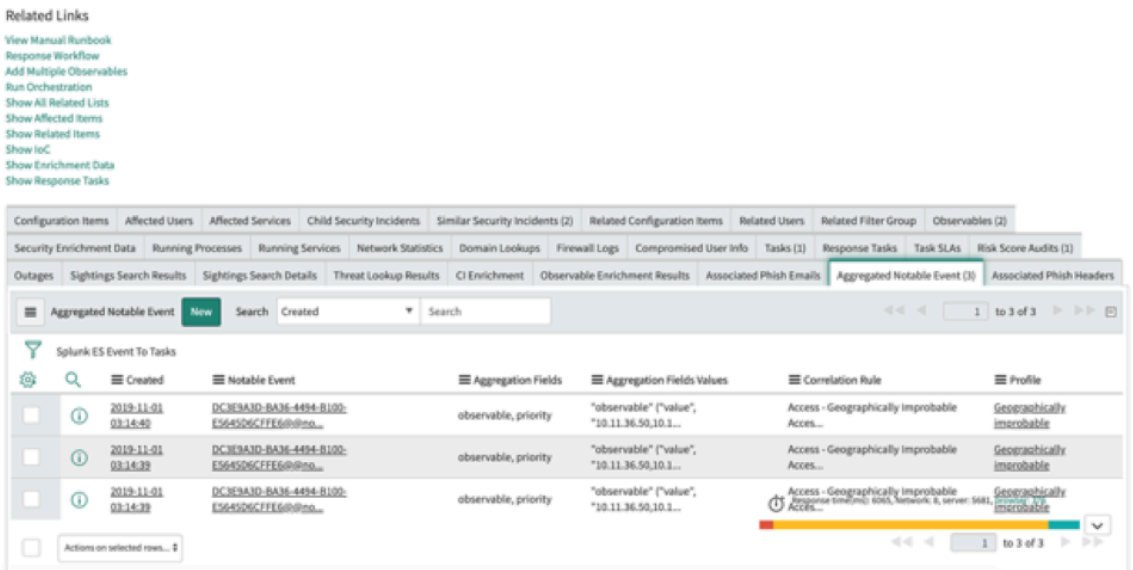
b. 다중 선택 입력 필드에서 의 기존 보안 인시던트 ServiceNow AI Platform와 일치시킬 필드 값을 선택합니다.

c. 새 기준 추가를 사용하여 여러 필드 일치 조건을 선택합니다.
다중 선택 입력 필드에서 선택하는 모든 필드 값은 AND 조건을 사용하여 집계 기준에 대해 일치합니다. 새 기준 추가를 클릭하여 정의된 다중 선택된 필드 조건 중 하나가 OR 조건을 사용하여 충족되면 집계가 발생하는 여러 필드 일치 조건을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



새로운 주목할 만한 이벤트가 매핑 단계의 집계 필드 조건에서 선택된 모든 값과 일치할 경우, 새로운 주목할 만한 이벤트는 동일한 필드 값을 가진 가장 최근에 열린 보안 인시던트에 자동으로 추가됩니다. 보안 인시던트를 담당하는 sn_si.analyst 역할을 가진 사용자는 보안 인시던트의 관련 목록에서 추가된 모든 주목할 만한 이벤트 집계를 볼 수 있습니다. 보안 인시던트에 대해 집계된 모든 중요 이벤트가 작업에 대한 이벤트 관련 목록에 표시됩니다 Splunk . 이 목록에는 관련 타임스탬프 및 집계된 필드 값이 자세히 설명되어 있습니다. 이 정보는 이러한 중요 이벤트가 기존 보안 인시던트에 집계되는 이유를 이해하는 데 도움이 됩니다. 이 탭이 표시되지 않으면 관련 링크 아래에 있는 기록의 왼쪽으로 스크롤하여 모든 관련 목록 표시 링크를 클릭합니다.



d. 옵션: 최근에 보안 인시던트에 추가된 새로운 중요 이벤트에 대한 작업 메모를 기록하려면 이 옵션을 활성화하는 확인란을 선택합니다.
작업 메모는 경보 상세 정보 및 매핑 섹션의 작업 메모 필드에 추가되었을 수 있는 기타 상세 정보에 대한 링크와 함께 새로운 주목할 만한 항목이 추가되었음을 기록합니다.

중요 이벤트의 값을 Splunk 보안 인시던트의 SIR 필드에 매핑했습니다. 또한 인시던트 생성 필터링 기준을 사용하여 보안 인시던트 생성을 제한하는 추가 조건을 구성했습니다. 또한 이벤트 필드 값이 구성된 집계 기준과 일치할 때 중요 이벤트를 기존 SIR 보안 인시던트에 추가했습니다.

10. 하나를 선택하여 프로파일 구성을 계속합니다.

다음에 수행할 작업
다음 단계는 보안 인시던트에 매핑한 값을 미리 보는 것입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이벤트 수집 통합에 **Splunk Enterprise Security** 대한 보안 인시던트 미리 보기

매핑 단계를 완료한 후 (SIR) 보안 인시던트에서 ServiceNow AI Platform# 보안 인시던트 응답 매핑한 값을 미리 봅니다. 이 미리 보기 단계를 사용하면 보안 인시던트에 표시할 중요한 필드를 모두 매핑했는지 확인할 수 있습니다.

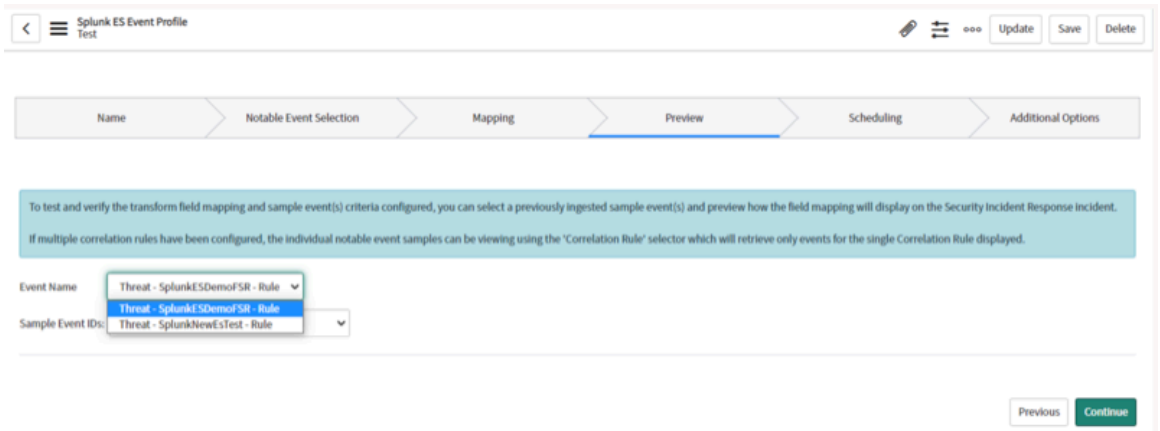
시작하기 전에
필요한 역할: sn_si.ingestion_profile_admin

주:
sn_si.admin 역할은 기본적으로 필수 권한을 상속하므로 sn_si.admin 역할을 가진 사용자는 프로필 관리자가 사용할 수 있는 모든 작업을 수행할 수 있습니다.

이 태스크 정보
보안 인시던트를 미리 보고 필요에 따라 매핑을 다시 편집하여 오류가 있는 필드를 수정하거나 누락된 데이터를 채웁니다. 미리 보기가 성공적으로 완료되지 않으면 예약 단계로 진행할 수 없습니다. SIR 보안 인시던트 미리 보기는 제품에 실제 인시던트 SIR 로 저장되지 않습니다.

프로시저

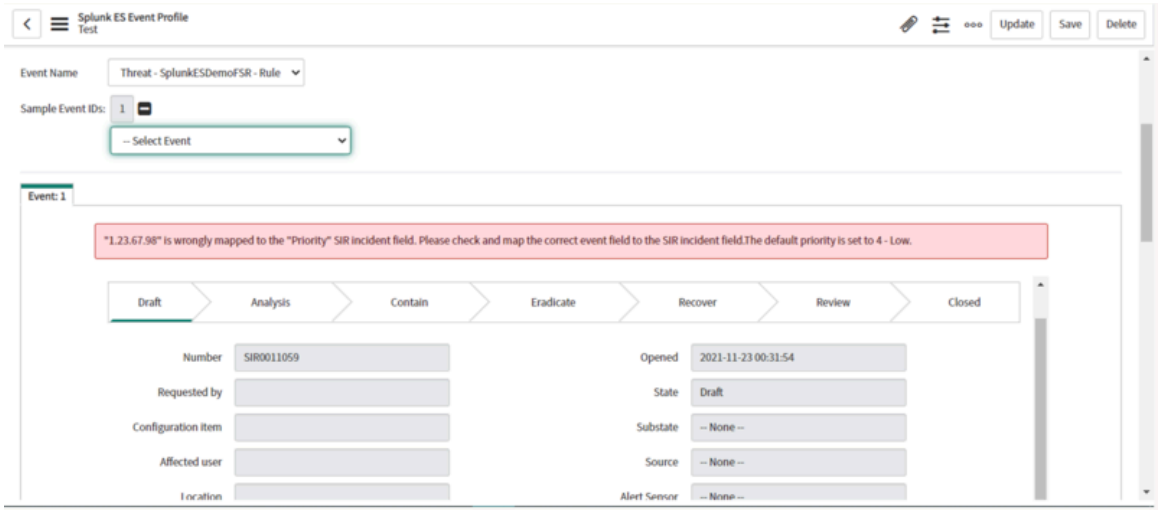
1. 보안 인시던트 미리 보기가 표시되지 않으면 진행률 표시줄에서 미리 보기를 클릭합니다.
2. 이벤트 이름 선택 목록에서 여러 이벤트가 사용된 경우 항목을 선택합니다.
3. 샘플 주목할 만한 이벤트 ID 선택 목록에서 이벤트 ID를 선택합니다.
4. 샘플 중요 이벤트 ID 선택 목록에서 항목을 선택합니다.



보안 인시던트가 표시됩니다. 필드의 정보를 변경하지 마십시오. 이 뷰는 읽기 전용 뷰이며 이 보안 인시던트의 기록은 저장되지 않습니다.

5. 보안 인시던트에서 중요한 이벤트 값의 필드 매핑을 검토합니다.

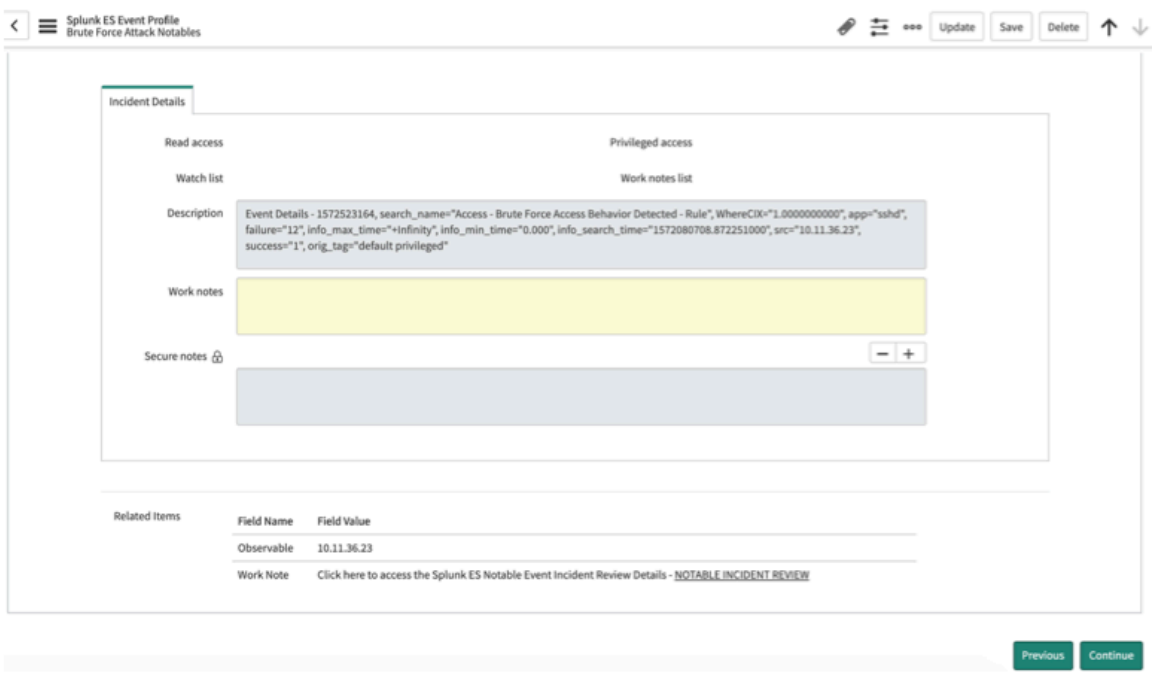
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



앞의 이미지는 매핑 오류가 있는 미리 보기의 예입니다. 이 예에서는 중요 이벤트의 필드 값이 SIR 인시던트 양식의 참조 필드에 허용되는 값을 갖지 않습니다. 고객 관리 데이터베이스(CMDB)의 ServiceNow#### ## 필드에 대한 입력 값을 찾을 수 없다는 오류 메시지가 표시됩니다. 따라서 이 매핑된 필드 값은 추가 수정 없이 SIR 보안 인시던트 양식에 표시되지 않습니다.

6. 이 오류를 해결하려면 진행률 표시줄에서 매핑 을 클릭합니다.
7. 매핑을 편집하여 잘못된 값을 수정하거나 누락된 데이터를 채웁니다.
8. 매핑을 다시 미리 보고 오류 메시지에 설명된 오류를 계속 수정합니다.

다음 그림은 모든 오류 메시지가 해결된 후 보안 인시던트 하단 절반 SIR 에 있는 인시던트 상세 정보 탭의 예입니다. 이 예에서는 설명 및 작업 메모 필드가 매핑되었으며, 이러한 필드는 주목할 만한 이벤트 샘플에서 가져온 값 쌍의 Splunk Enterprise Security 값으로 채워집니다. 첫 번째 작업 메모 필드에는 값이 없습니다. 이 필드는 매핑 단계 동안 매핑 그리드에서 비어 있었습니다. 값이 있는 추가 작업 메모 필드가 매핑 섹션에 추가되었습니다.



9. 오류를 수정하고 필드가 원하는 방식인지 확인한 후 계속하려면 하나의 옵션을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 수행할 작업

오류 메시지가 표시되지 않고 보안 인시던트의 필드 매핑에 만족하는 경우 다음 단계는 수행 통합에 대한 Splunk Enterprise Event Ingestion 경보 예약 및 검색입니다.

이벤트 수집 통합을 위해 **Splunk Enterprise Security** 새롭고 업데이트된 주목할 만한 이벤트 예약 및 검색

자동화된 주목할 만한 이벤트 수집 프로파일의 경우 이벤트 프로파일 구성에 이 단계가 필요합니다. 이 단계에서 중요 이벤트 검색에 대한 기본 설정을 확인하거나 필요에 따라 일정을 수정할 수 있습니다. 또한 이 단계에서는 날짜 범위를 사용하여 과거의 주목할 만한 이벤트를 검색할 수 있습니다.

시작하기 전에

필요한 역할: sn_si.ingestion_profile_admin

주:
sn_si.admin 역할은 기본적으로 필수 권한을 상속하므로 sn_si.admin 역할을 가진 사용자는 프로필 관리자가 사용할 수 있는 모든 작업을 수행할 수 있습니다.

이 태스크 정보

자동화된 주목할 만한 이벤트 수집을 위한 프로필의 경우 스케줄링 단계에서 과거의 주목할 만한 이벤트를 수집할지 여부를 선택합니다. 또한 경보 프로파일 구성과 일치하는 새로운 주목할 만한 이벤트 및 업데이트된 주목할 만한 이벤트를 폴링할 빈도를 선택합니다.

자동화된 중요 이벤트 수집 프로파일의 경우 프로파일이 활성화되기 전에 일정 및 경보 검색을 확인하고 수정합니다. 이 단계는 예약된 경보 프로파일에 대한 모든 이벤트 프로파일 구성 프로세스에 필요한 단계입니다.

프로파일별로 이러한 폴링 간격을 구성합니다. 이벤트 수집 통합의 Splunk 성능은 다른 폴링 간격의 영향을 받을 수 있습니다. 일정을 세울 때, 서버에서 폴링 오버헤드를 Splunk Enterprise Security 줄이는 것과 주목할 만한 이벤트가 생성되거나 업데이트될 때 가능한 한 빨리 알림을 받으려는 욕구 사이에서 균형을 맞추는 것이 좋습니다. 모든 프로파일에 대해 5분 기본값이 설정되어 있지만 필요한 경우 이 설정을 1분 정도로 수정하는 것을 선호할 수 있습니다.

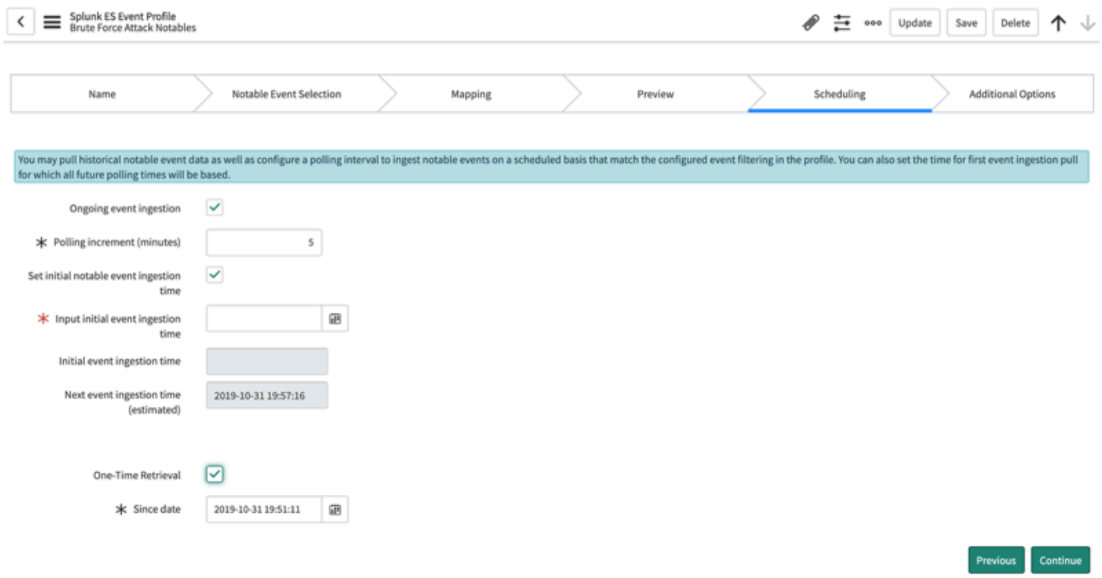
신규 및 업데이트된 주목할 만한 이벤트 끌어오기

폴링 일정이 설정되면 예약된 작업은 이전에 끌어왔지만 인시던트 필터링 기준을 충족하지 않는 신규 및 업데이트된 중요 이벤트를 모두 가져옵니다. 따라서 주목할 만한 이벤트가 처음 생성될 때는 존재하지 않을 수 있지만 업데이트가 발생한 후(예: 조사 단계 동안) 사용할 수 있는 기준에 따라 인시던트를 유연하게 생성할 수 있습니다. 특정한 주목할 만한 사건에 대한 인시던트가 생성되면 해당 주목할 만한 사건이 활성 ServiceNow# 보안 인시던트로 처리될 것으로 예상되므로 후속 업데이트는 무시됩니다. 그러나 이전에 수집되었지만 인시던트 생성 기준을 충족하지 못한 다른 모든 주목 항목은 활성 인시던트의 일부가 될 때까지 계속해서 인시던트 생성 기준에 대해 끌어오고 확인됩니다.

프로시저

1. 진행률 표시줄에 스케줄링 페이지가 표시되지 않으면 스케줄링을 선택합니다.
2. 콘솔에서 주목할 만한 이벤트를 끌어오는 Splunk Enterprise Security 방법과 시기를 예약하려면 하나를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



초기 중요 이벤트 수집 시간을 예약하는 예로, 현지 시간으로 하루에 한 번 실행되는 일일 Splunk 보안 검사가 있는 경우, 인스턴스에서 해당 중요 이벤트 프로파일 ServiceNow AI Platform 이 현지 시간으로 오전 4시 5분에 실행되도록 설정하여 보안 장애 이벤트를 즉시 캡처하고 보안 인시던트를 생성할 수 있습니다. 초기 이벤트 수집 필드에 04 05 00 을 입력합니다. 증분(분) 필드에 1440 (24시간)을 입력하여 초기 이벤트 수집으로부터 24시간 동안 다음 이벤트 수집을 예약합니다. 초기 이벤트 수집 시간과 다음 이벤트 수집 시간이 모두 필드에 표시됩니다.

3. 이 예제의 설정을 구성하려면 다음 단계를 수행합니다.

   a. 예약 페이지가 표시되면 진행 중인 이벤트 수집 확인란을 선택하여 이 옵션을 활성화합니다.

   b. 증분(분) 필드에 1440 (24시간)을 입력합니다.

   c. 초기 이벤트 수집 선택 확인란을 클릭하여 초기 이벤트 수집 및 다음 이벤트 수집 필드를 편집할 수 있습니다.

   d. 초기 이벤트 수집 필드에 04 05 00을 입력합니다.
   다음 이벤트 수집(예상) 필드에 다음 이벤트 수집 시간이 표시됩니다.

4. 다음 중 하나를 클릭하여 프로파일 구성을 계속합니다.

SIR 인시던트 상태에 따라 중요한 이벤트 업데이트 및 종결 자동화

보안 인시던트는 통합과의 Splunk Enterprise Security 양방향 인터페이스를 사용하여 생성된 후 생성 및 업데이트할 수 있습니다.

시작하기 전에
통합 Splunk Enterprise Security 에는 중요한 이벤트가 보안 인시던트를 생성하고 보안 인시던트가 생성 및/또는 종결된 후 중요한 이벤트를 업데이트할 수 있는 양방향 인터페이스가 있습니다.

관련 인시던트 상세 정보에는 인시던트 번호, 할당 그룹, SIR 인시던트 URL이 포함됩니다SIR. 이 섹션은 중요한 이벤트를 업데이트할 Splunk Enterprise Security 수 있는 선택적 기능을 제공하는 프로필 구성 설정의 마지막 부분입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필요한 역할: sn_si.ingestion_profile_admin

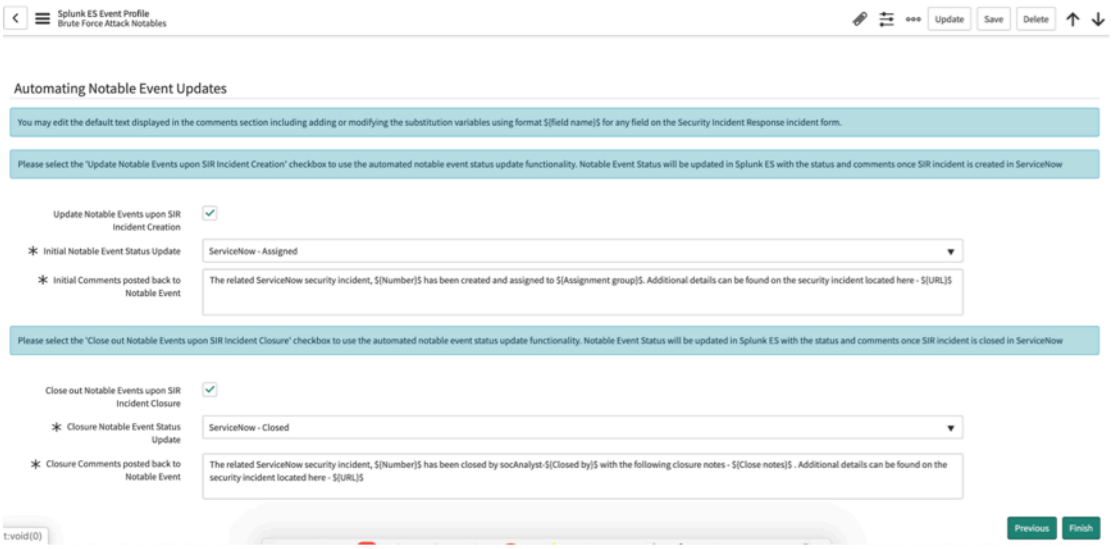
주:
sn_si.admin 역할은 기본적으로 필수 권한을 상속하므로 sn_si.admin 역할을 가진 사용자는 프로필 관리자가 사용할 수 있는 모든 작업을 수행할 수 있습니다.

프로시저

1. 진행률 표시줄에 추가 옵션 페이지가 표시되지 않으면 추가 옵션을 선택합니다.
2. 아래 지침에 따라 보안 인시던트 업데이트를 기반으로 중요한 이벤트를 업데이트하기 위한 구성을 완료하십시오.

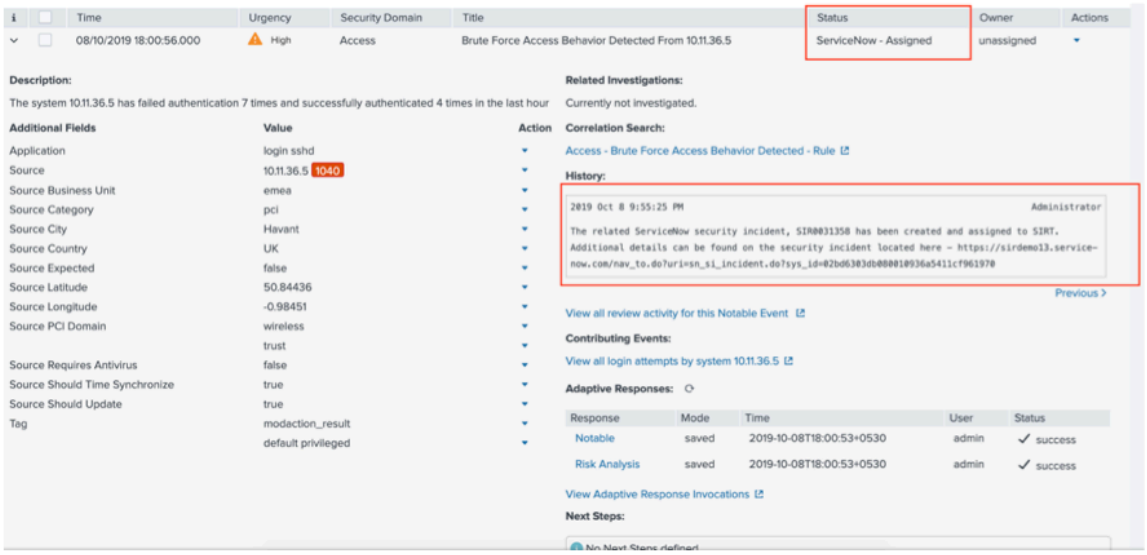
3. Finish(마침)를 클릭하여 구성을 완료합니다.
   확인 대화 상자가 표시됩니다. 통합에 대한 설정 및 구성을 성공적으로 완료했습니다. 이 프로파일을 활성화하여 일정에 따라 콘솔에서 중요한 이벤트를 Splunk Enterprise Security 끌어옵니다. 24시간 동안 생성할 수 있는 보안 인시던트는 1,000개로 제한됩니다. 발생한 경보당 최대 100개의 주목할 만한 이벤트가 발생할 수 있습니다. 제한에 도달한 후에는 이후의 주목할 만한 이벤트가 무시됩니다.

   다음 이미지는 기본값이 채워진 추가 옵션 탭을 보여 줍니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

추가 옵션 구성을 활성화하면 주목할 만한 이벤트 인시던트 검토에 상태 변경과 이력 설명에 대한 업데이트가 표시됩니다.



수동 이벤트 전달을 위한 프로필 설정

정의된 Splunk ES 프로파일에 따라 주목할 만한 이벤트는 별개의 주목할 만한 이벤트 보안 운영 로서 인스턴스 환경에 ServiceNow AI Platform 수동으로 전달됩니다.

주목할 만한 이벤트의 수동 전달을 위한 프로필을 설정하려면 다음과 같이 하십시오.

작업	섹션
이벤트 프로파일 생성	수동으로 전달된 이벤트에 대한 프로파일 생성 문서를 참조하십시오.
주목할 만한 이벤트 필드 매핑	통합을 위한 Splunk Enterprise Security 주목할 만한 이벤트 필드 매핑 문서를 참조하십시오.
사용자 지정 매핑 생성	중요 이벤트 인시던트 검토 및 기여 이벤트 상세 정보를 위한 Splunk ES 매핑 생성(수동 전달) 문서를 참조하십시오.
보안 인시던트 미리 보기	이벤트 수집 통합에 Splunk Enterprise Security 대한 보안 인시던트 미리 보기 문서를 참조하십시오.
Splunk 수동 수집을 위한 환경 설정	Splunk 주목할 만한 이벤트 수집 통합의 수동 이벤트 수집을 Splunk Enterprise Security 위한 환경 설정 문서를 참조하십시오.
SIR 인시던트 상태에 따라 중요한 이벤트 업데이트 및 종결 자동화	SIR 인시던트 상태에 따라 중요한 이벤트 업데이트 및 종결 자동화 문서를 참조하십시오.

수동으로 전달된 이벤트에 대한 프로파일 생성

수동 전달 이벤트에 대한 프로파일을 설정할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.ingestion_profile_admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
sn_si.admin 역할은 기본적으로 필수 권한을 상속하므로 sn_si.admin 역할을 가진 사용자는 프로필 관리자가 사용할 수 있는 모든 작업을 수행할 수 있습니다.

프로시저

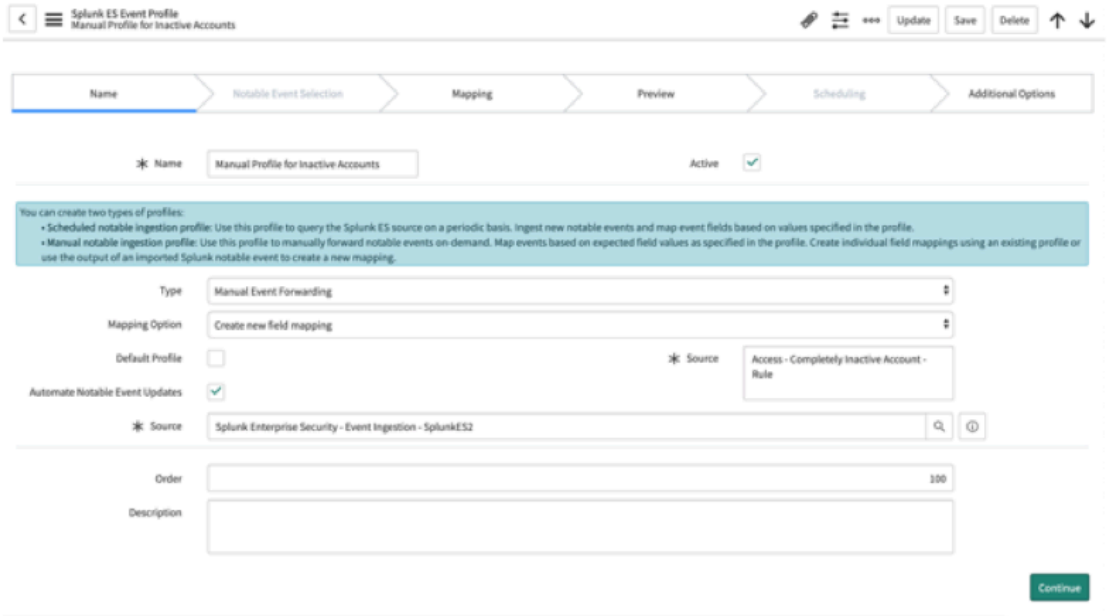
수동 이벤트 전달을 지원하는 프로필을 만들려면 다음 단계를 수행합니다.

콘솔에서 요청 Splunk Enterprise Security 시 전달하는 이벤트의 경우, 기존 프로파일을 기반으로 개별 필드 매핑을 수행할 수 있습니다. 또는 익스포트한 첨부 파일 데이터에 대한 새 매핑 그리드를 생성할 수 있습니다. 수동으로 전달하는 이벤트는 이벤트 프로파일에 예약되지 않습니다.

a. 아직 선택하지 않았다면 유형 필드의 선택 목록에서 수동 이벤트 전달을 선택합니다.

b. 표시되는 매핑 옵션 필드의 선택 목록에서 계속할 매핑 옵션 하나를 선택합니다.

매핑 옵션 선택 목록에서 사용 가능한 매핑 옵션에 대한 자세한 내용은 다음 그림과 표를 참조하십시오.



새 필드 매핑 옵션 생성

옵션 또는 필드	설명
새 필드 매핑 옵션 생성	이벤트에 대한 새 필드 매핑입니다. 생성 중인 프로파일과 유사한 기존 필드 매핑이 없는 경우 이 옵션을 선택하여 새 맵을 생성합니다.
기본 프로파일	모든 Splunk 이벤트에 대한 기본 이벤트 전달 프로필입니다. 기본값은 지워져 있습니다 (비활성화됨). 이 옵션을 사용하도록 설정하면 이 프로파일이 수동 이벤트 전달을 위한 기본 프로파일이 됩니다. 이 프로파일은 수동으로 전달된 이벤트의 소스에 일치하는 항목이 없을 때

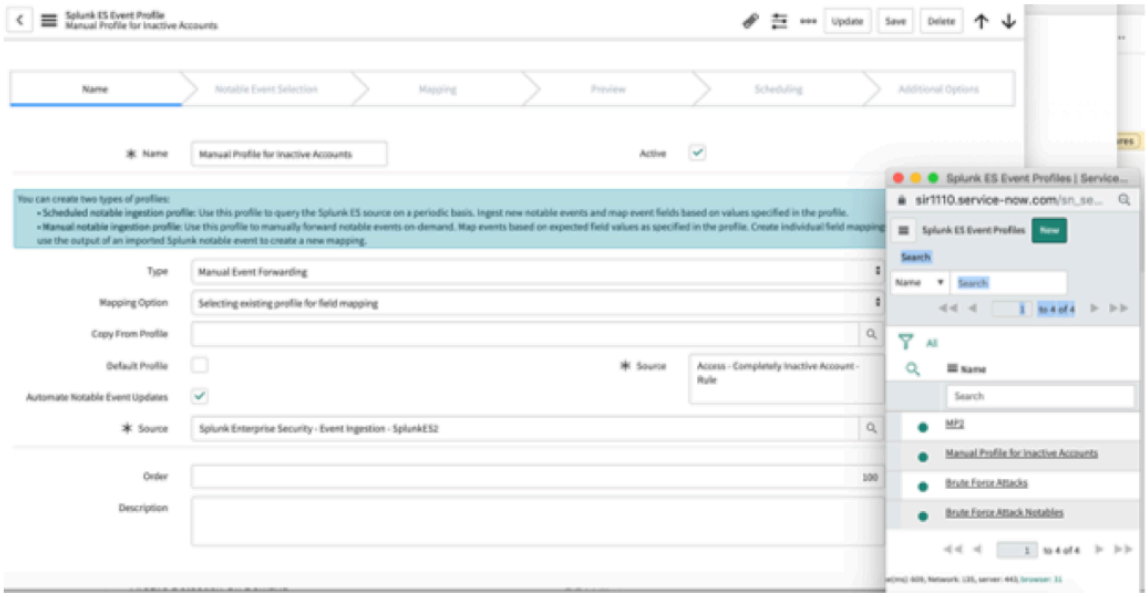
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵션 또는 필드	설명
	사용됩니다. 이는 출처를 알 수 없는 모든 이벤트의 기본 프로파일이 됩니다. 기본 프로파일 옵션이 활성화된 경우 소스 필드를 사용할 수 없습니다.
소스(중요 이벤트 필드)	이 필드는 일반적으로 주목할만한 상관관계 규칙(예: 무차별 암호 대입 공격)을 정의하는 필드입니다. 기본 프로파일 옵션을 사용하는 경우 이 필드를 사용할 수 없습니다. 사용 가능한 경우 이 필드를 사용하면 일반적으로 여러 이벤트 유형에 대해 다른 splunk 상관관계 규칙을 기반으로 보안 인시던트 필드에 고유한 이벤트 필드 매핑이 허용됩니다. 서로 다른 상관관계 규칙을 별도로 관리하려면 상관관계 규칙을 기반으로 다른 프로파일 이벤트 프로파일을 생성하여 이 요구 사항을 충족할 수 있습니다.
주목할 만한 이벤트 업데이트 자동화	주목할 만한 이벤트 상태를 업데이트하고 주목할 만한 이벤트에서 SIR 인시던트가 작성되거나 SIR 인시던트가 종결될 때 설명을 추가하려면 이 확인란을 선택합니다. 이는 SIR 인시던트를 생성하는 초기 트리거 중요 이벤트와 집계된 이벤트 모두에 대해 발생합니다.
소스(Splunk 서버)	주목할 만한 이벤트의 소스로 구성한 서버입니다 Splunk . 여러 Splunk 서버가 구성된 경우 프로파일에 대해 업데이트될 주목할 만한 이벤트 유형에 적합한 서버를 선택합니다. 값을 입력해야 합니다.
순서	기본값은 100입니다. 이 설정을 기본값으로 둡니다. 많은 수의 프로파일을 만든 경우 둘 이상의 프로파일이 트리거 조건을 공유할 때 이 값은 런타임 실행 우선순위를 제공합니다. 숫자가 가장 낮은 프로파일의 워크플로우가 가장 높은 우선순위를 갖습니다.
(선택 사항) 묘사	이 프로파일을 다른 프로파일과 구별하는 데 도움이 되는 텍스트입니다.

새 필드 매핑이 있는 프로필의 경우 소스 유형 필드에 값을 입력했는지 확인하고 계속 을 클릭하여 구성의 매핑 단계로 진행합니다.

기존 필드 매핑이 있는 프로필의 자세한 내용은 다음 그림과 표를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



필드 매핑 옵션에 대한 기존 프로파일 선택

옵션 또는 필드	설명
필드 매핑을 위한 기존 프로파일 선택	새로운 주목할 만한 이벤트 프로파일에 기존 필드 매핑을 재사용합니다. Copy from profile(프로파일에서 복사) 필드가 표시됩니다. 다음 단계에 따라 이 프로파일에 대한 기존 필드 매핑을 복사합니다. **i.** 표시되는 프로필에서 복사 필드 왼쪽에서 검색 아이콘을 클릭합니다. **ii.** Splunk 표시되는 ES 이벤트 프로파일 목록에서 복사할 맵이 있는 프로파일 이름을 클릭합니다. 프로파일 이름이 프로파일에서 복사 필드에 표시됩니다.
기본 프로파일	소스가 일치하지 않는 모든 Splunk 주목할 만한 이벤트에 대한 기본 이벤트 전달 프로필입니다. 기본값은 지워져 있습니다(사용 안 함). 이 옵션을 사용하도록 설정하면 이 프로파일이 수동 이벤트 전달을 위한 기본 프로파일이 됩니다. 기본 프로파일 옵션이 활성화된 경우 소스 필드를 사용할 수 없습니다.
소스(중요 이벤트 필드)	이 필드는 일반적으로 주목할만한 상관관계 규칙(예: 무차별 암호 대입 공격)을 정의하는 필드입니다. 기본 프로파일 옵션을 사용하는 경우 이 필드를 사용할 수 없습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵션 또는 필드	설명
	사용 가능한 경우 이 필드를 사용하면 일반적으로 여러 이벤트 유형에 대해 다른 splunk 상관관계 규칙을 기반으로 보안 인시던트 필드에 고유한 이벤트 필드 매핑이 허용됩니다. 서로 다른 상관관계 규칙을 별도로 관리하려면 상관관계 규칙을 기반으로 다른 프로파일 이벤트 프로파일을 생성하여 이 요구 사항을 충족할 수 있습니다.
주목할 만한 이벤트 자동화	중요 이벤트 상태를 업데이트하고 중요 이벤트에서 보안 인시던트가 생성되거나 보안 인시던트가 종결될 때 설명을 추가하려면 이 확인란을 선택합니다. 이는 보안 인시던트를 생성하는 주목할 만한 초기 이벤트 트리거와 집계된 이벤트 모두에 대해 발생합니다.
소스(Splunk 서버)	Splunk 주목할 만한 이벤트의 소스로 구성한 서버 또는 검색 끝입니다. 여러 Splunk 서버가 구성된 경우 프로파일에 대해 업데이트될 주목할 만한 이벤트 유형에 적합한 서버를 선택합니다. 값을 입력해야 합니다.
순서	기본값은 100입니다. 이 설정을 기본값으로 둡니다. 여러 프로파일을 만든 경우 둘 이상의 프로파일이 트리거 조건을 공유할 때 이 값은 런타임 실행 우선순위를 제공합니다. 숫자가 가장 낮은 프로파일의 워크플로우가 가장 높은 우선순위를 갖습니다.
(선택 사항) 묘사	이 프로파일을 다른 프로파일과 구별하는 데 도움이 되는 텍스트입니다.

프로파일에 대한 기존 매핑을 선택하기 위한 양식의 맨 아래에서 마침 을 클릭하여 프로파일 구성을 완료합니다.

중요 이벤트 인시던트 검토 및 기여 이벤트 상세 정보를 위한 **Splunk ES** 매핑 생성(수동 전달)

중요 이벤트 필드 매핑 단계에서는 중요 이벤트의 개별 이벤트 필드를 (SIR) 보안 인시던트의 ServiceNow AI Platform 보안 인시던트 응답 필드로 매핑합니다.

시작하기 전에

필요한 역할: sn_si.ingestion_profile_admin

> **주:**
> sn_si.admin 역할은 기본적으로 필수 권한을 상속하므로 sn_si.admin 역할을 가진 사용자는 프로필 관리자가 사용할 수 있는 모든 작업을 수행할 수 있습니다.

이 태스크 정보

양식 왼쪽의 중요 이벤트 샘플 수집 열에서 최대 5개의 중요 이벤트를 오른쪽에 있는 SIR 인시던트 필드 매핑 열의 보안 인시던트 필드에 매핑합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

양식의 오른쪽에 있는 매핑 그리드에서 필드를 추가하거나 제거하여 사용자 지정 매핑을 생성합니다. SIR 인시던트 양식에 채워야 하는 일반적으로 중요한 필드인 기본 필드가 표시됩니다. 그러나 이러한 필드를 제거할 수 있으며 + 및 - 버튼을 사용하여 추가 필드를 표시할 수 있습니다. 양식 오른쪽의 매핑 그리드에서 필드를 추가하거나 제거하여 사용자 지정 맵을 생성합니다. 필드를 사용자 지정하면 보안 인시던트의 기본 매핑 그리드에 표시되지 않는 필드를 매핑 Splunk 할 수 있습니다 SIR .

프로시저

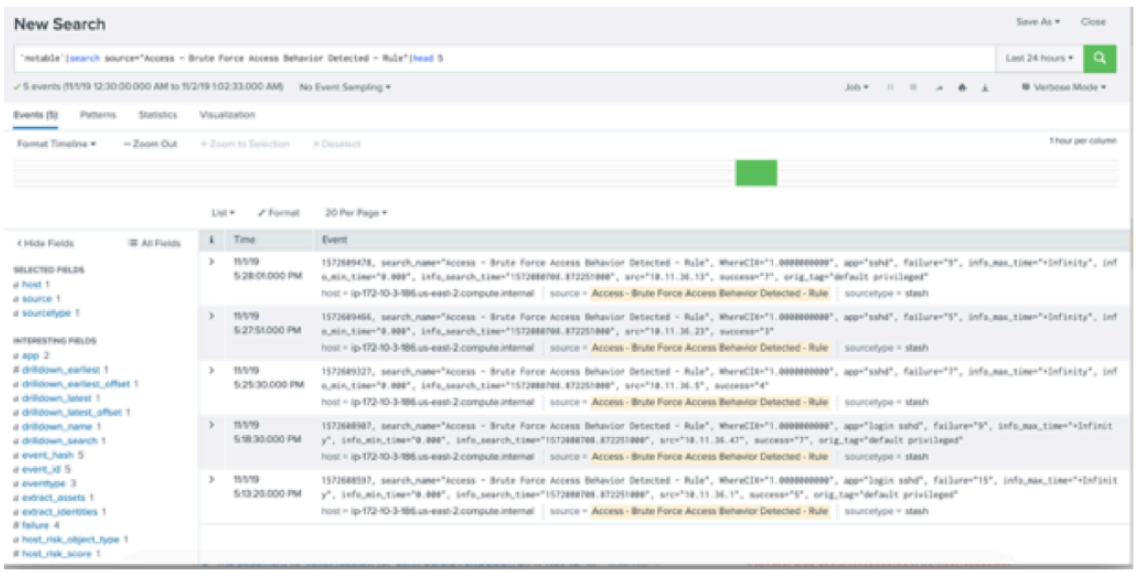
1. 매핑 양식이 표시되지 않으면 진행률 표시줄에서 매핑 을 클릭합니다.
2. 다음 단계에 따라 인스턴스에 첨부 파일 데이터를 ServiceNow AI Platform# 업로드합니다.

   a. 아직 로그인하지 않았다면 콘솔에 로그인하십시오 Splunk Enterprise .

   b. 검색 탭으로 이동하여 익스포트하려는 주목할 만한 이벤트 데이터가 있는 검색의 이름을 입력합니다.
   무차별 암호 대입 공격 동작 상관 관계 규칙에 대해 주목할 만한 이벤트를 검색하는 검색 형식의 예는 다음과 같습니다. 'notable'|search source="접근 - 무차별 암호 대입 접근 동작 탐지됨 - 규칙".

   c. 중요 이벤트를 확장하고 필드 열에서 임포트할 필드를 선택합니다.

   이러한 필드는 익스포트되어 인스턴스의 매핑 페이지에 ServiceNow AI Platform# 표시되는 필드-값 쌍입니다.



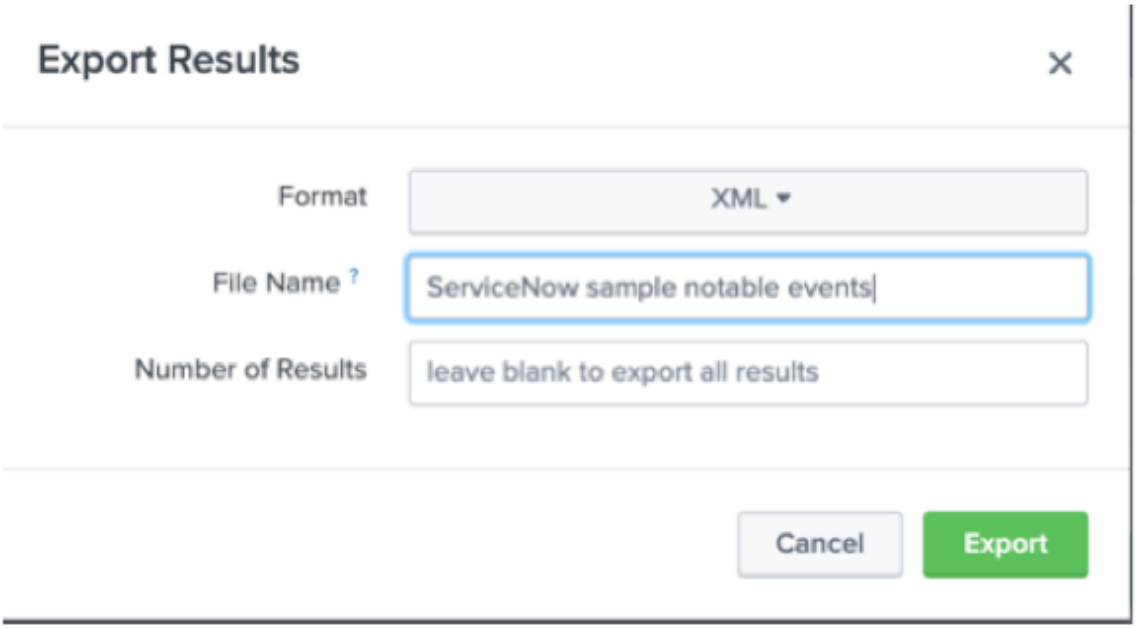
   d. Splunk Enterprise 콘솔의 검색 페이지 오른쪽 상단에서 익스포트 아이콘을 클릭합니다.

   e. 표시되는 대화 상자의 형식 필드에 대한 선택 목록에서 **XML** 형식을 클릭합니다.

   f. 옵션: 새 파일 이름을 입력합니다.

   g. 익스포트를 클릭합니다.

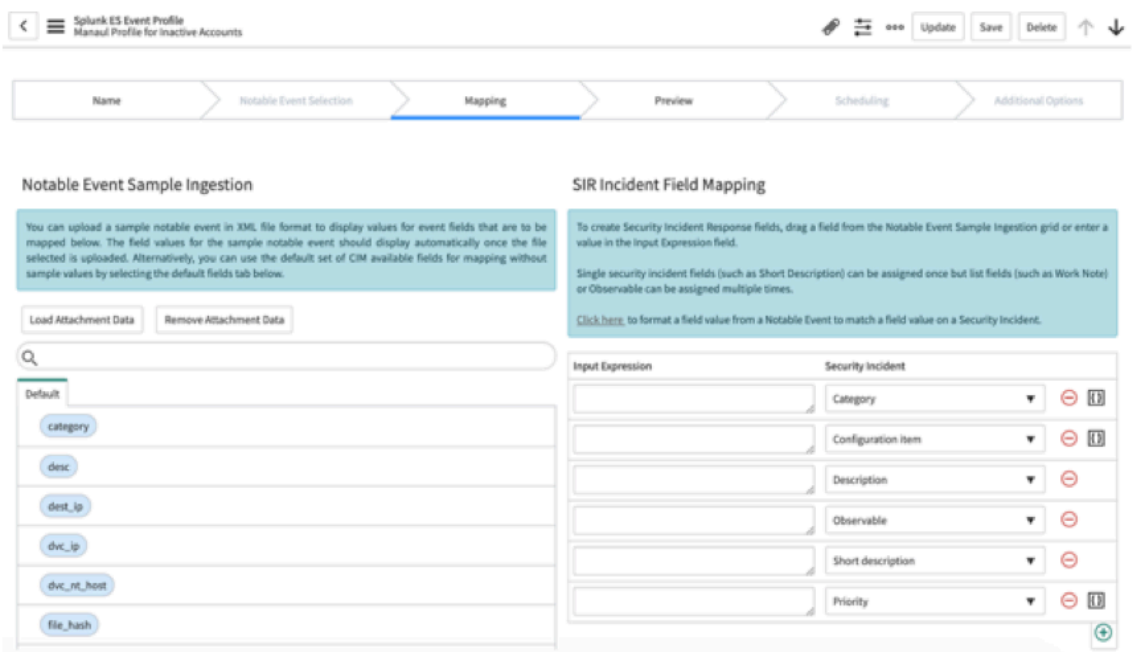
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



익스포트 Splunk 한 주목할 만한 이벤트 XML 파일을 이제 인스턴스에 업로드 ServiceNow AI Platform# 해야 합니다.

h. 인스턴스에 매핑 페이지가 아직 표시되어 ServiceNow AI Platform# 있지 않으면 진행률 표시줄에서 매핑 을 클릭합니다.

i. 주목할 만한 이벤트 샘플 수집 열에서 첨부 파일 데이터 로드를 클릭합니다.



j. 표시되는 대화 상자에서 파일 선택을 클릭하고 내보낸 .xml 파일을 탐색한 다음 열기를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

클릭하여 수동으로 전달된 이벤트에 Splunk ES 대한 첨부 파일 데이터를 로드하면 양식 왼쪽에 주목할 만한 이벤트 필드가 채워집니다. 이러한 값은 양식의 인시던트 필드 매핑 측면에 있는 보안 인시던트 필드에 매핑하는 필드 값입니다.
이벤트에 대해 익스포트한 필드의 값 쌍이 매핑 양식의 왼쪽에 표시됩니다.

3. 섹션의 5-10 중요 이벤트 인시던트 검토 및 기여 이벤트 상세 정보(예약된 수집)에 대한 Splunk ES 매핑 생성 단계를 수행합니다.

Splunk 주목할 만한 이벤트 수집 통합의 수동 이벤트 수집을 **Splunk Enterprise Security** 위한 환경 설정

이 통합에 대해 콘솔에서 요청 Splunk Enterprise Security 시 수동으로 이벤트를 익스포트하려면 엔터프라이즈 콘솔 또는 Splunk 클라우드 인스턴스에 애플리케이션에 Splunk 대한 Splunk Enterprise Security 보안 운영 이벤트 수집 Addon을 ServiceNow 설치하고 설정합니다.

시작하기 전에
엔터프라이즈 콘솔 또는 Splunk 클라우드 인스턴스에 애플리케이션용 Splunk Enterprise Security 보안 운영 이벤트 수집 애드온을 ServiceNow 설치하고 설정하는 것은 선택 사항입니다Splunk.

수동 이벤트 수집에 필요한 splunkbase에서 애드온 플러그인을 설치하기 전에 이 통합 ServiceNow Store 에 대한 애플리케이션을 설치했는지 확인하십시오. 에서 ServiceNow Store통합을 위한 애플리케이션을 설치하지 않은 경우 를 참조 주목할 만한 이벤트 수집 통합 설치 및 구성 Splunk Enterprise Security 하고 지침에 따라 설치합니다.

필요한 역할: Splunk Enterprise Security 관리자

이 태스크 정보
통합을 위해 콘솔에서 요청 시 Splunk Enterprise 이벤트를 수동 익스포트하려면 콘솔의 Splunk Enterprise Security splunkbase에서 보안 운영 이벤트 수집 추가 기능을 Splunk Enterprise Security 다운로드, 설치 및 설정합니다ServiceNow. 인스턴스에서 수동으로 익스포트한 이벤트 ServiceNow AI Platform 에서 보안 인시던트를 만들려면 이 ServiceNow 확장 추가 기능이 필요합니다.
이 ServiceNow 애플리케이션용 Splunk Enterprise Security 보안 운영 이벤트 수집 애드온은 splunkbase 에서 사용할 수 있습니다.

수동 이벤트 전달의 경우 콘솔에서 최대 두 개의 서로 다른 ServiceNow AI Platform 엔드포인트(인스턴스)를 식별할 수 있습니다 Splunk Enterprise Security . 이벤트를 엔드포인트 또는 엔드포인트에 수동으로 전달하여 보안 인시던트를 만듭니다. 예를 들어, 스테이징(개발) 인스턴스와 프로덕션 인스턴스를 모두 지정할 수 있습니다. 개별 인스턴스를 지정하고 각 인스턴스에 대한 기본 및 보조 워크플로우의 이름을 지정하여 서로 다른 이벤트를 전달할 위치를 선택할 수 있습니다.

프로시저

1. 에 대한 Splunk Enterprise Security보안 운영 이벤트 수집 추가 기능을 아직 설치하지 ServiceNow 않은 경우 다음 단계에 따라 설치하고 구성합니다.

   a. splunkbase 로 이동합니다.

   b. ServiceNow 보안 운영 에 대한 Splunk Enterprise Security보안 운영 이벤트 수집 추가 기능을 검색합니다.

      주:
      에 대한 Splunk Enterprise Security이벤트 수집 추가 기능을 선택 ServiceNow 보안 운영 했는지 확인합니다. 이 목록에 표시되는 추가 ServiceNow 애드온이 있습니다. 이러한 추가 기능은 서로 다른 ServiceNow Splunk 통합을 위한 것이며 이 통합에는 필요하지 않습니다.

   c. 애플리케이션을 다운로드합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

d. 계정을 Splunk Enterprise Security 엽니다.

e. 앱 페이지에서 기어 아이콘을 클릭하거나 메뉴 드롭다운 목록에서 앱 관리 바로 가기를 클릭합니다.

f. 표시되는 앱 페이지의 왼쪽 상단에서 파일에서 앱 설치를 클릭합니다.

g. 파일 선택을 클릭하고 에 대한 Splunk Enterprise Security보안 운영 이벤트 수집 추가 기능을 선택한 ServiceNow 다음 업로드를 클릭합니다.

h. 메시지가 표시되면 을 다시 시작합니다 Splunk Enterprise.
ServiceNow 용 Splunk Enterprise Security 보안 운영 이벤트 수집 추가 기능이 콘솔에 설치됩니다Splunk Enterprise Security. 애드온을 설정하는 다음 단계입니다.

2. 애드온을 설정하려면 다음 단계를 따르십시오.

a. 에서 Splunk Enterprise Security메뉴 드롭다운 목록에서 앱 기어 아이콘 또는 앱 관리를 클릭합니다.

b. 표시되는 애플리케이션 목록의 작업 열에서 에 대한 이벤트 수집 추가 기능 설정을ServiceNow 보안 운영Splunk Enterprise Security클릭합니다.

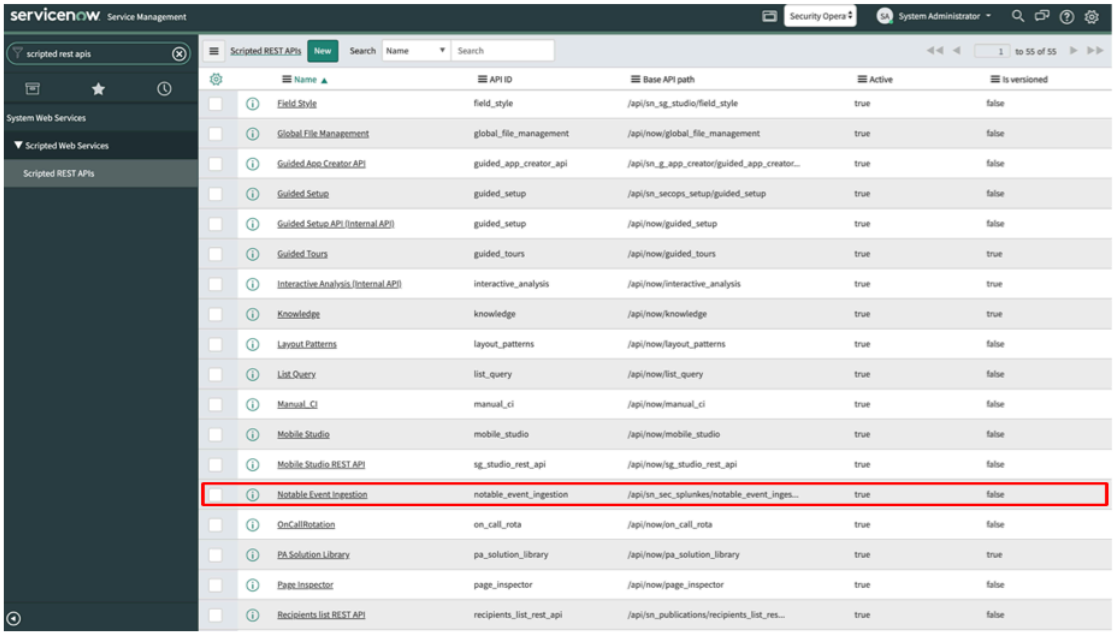
c. 양식을 작성합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음 그림은 콘솔에서 작성된 양식의 Splunk Enterprise Security 예입니다.

다음 그림은 에 ServiceNow AI Platform있는 Scripted REST API 목록의 예입니다. 콘솔의 확장 Splunk Enterprise Security 용 Splunk Enterprise Security 보안 운영 이벤트 수집 추가 기능 설정 ServiceNow 의 일부로 양식에 입력한 인스턴스의 엔드포인트 값 ServiceNow AI Platform 위치가 목록에 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



3. 콘솔의 Splunk Enterprise Security 설정 양식에서 Save(저장)를 클릭하여 편집 내용을 저장합니다.

   잠시 후 콘솔 양식의 Splunk Enterprise Security 왼쪽 상단에 기록이 성공적으로 업데이트되었다는 메시지가 표시됩니다.

   양식을 저장한 후에는 콘솔에서 선택한 검색 이벤트의 이벤트 작업 선택 목록에서 양식에 생성한 인스턴스의 이름(워크플로우 작업 레이블) ServiceNow AI Platform 을 사용할 수 Splunk Enterprise Security 있습니다.

다음에 수행할 작업

콘솔에 검색을 Splunk Enterprise Security 아직 저장하지 않은 경우 다음 단계는 검색을 콘솔에 경보로 저장하는 것입니다 Splunk Enterprise Security .

이벤트 수집 통합을 위한 **Splunk Enterprise Security** 이벤트 프로파일 복사

새 프로파일을 생성하는 대신 기존 프로파일 및 관련 설정을 복사합니다. 여러 프로필을 만들고 기존 프로필의 설정을 다시 사용하려는 경우 시간을 절약하기 위해 경보 프로필을 복사하는 것이 좋습니다.

시작하기 전에

필요한 역할: sn_si.ingestion_profile_admin

> **주:**
> sn_si.admin 역할은 기본적으로 필수 권한을 상속하므로 sn_si.admin 역할을 가진 사용자는 프로필 관리자가 사용할 수 있는 모든 작업을 수행할 수 있습니다.

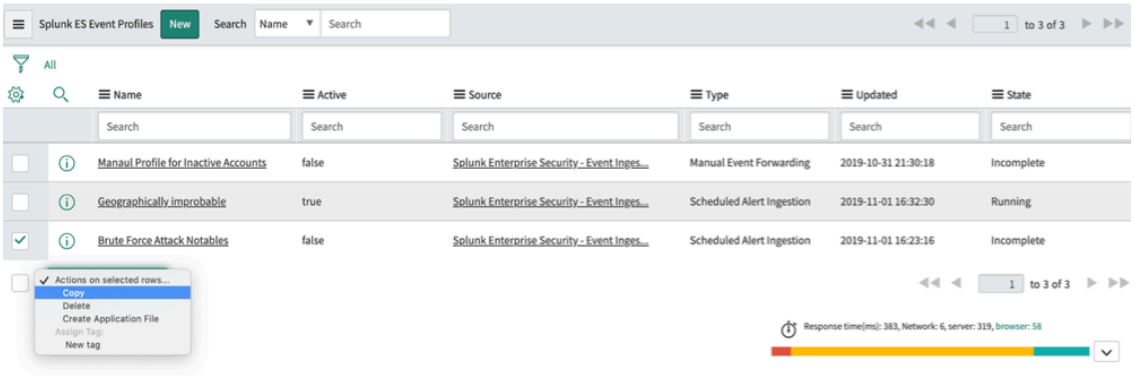
이 태스크 정보

프로파일을 복사하는 경우 프로파일 중복을 방지하기 위해 처음에 프로파일 이름이 수정됩니다. 또한 복사된 프로파일은 비활성화(false)되므로 구성을 완료하기 전에 실수로 활성화되지 않습니다. 이미 미리 보고 확인한 보안 인시던트에 대해 프로파일을 복사하고 기존 맵을 사용합니다.

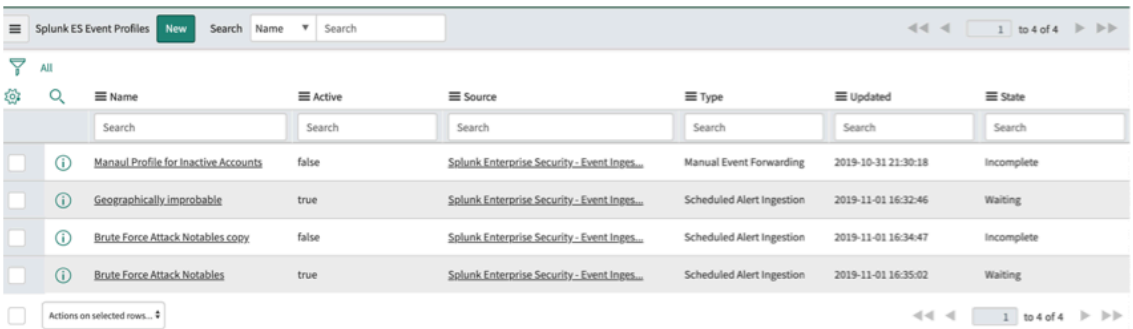
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 **Splunk Integration** 〉 **Splunk** 이벤트 프로파일.
2. Splunk 표시되는 이벤트 프로파일 목록에서 복사할 프로파일을 선택하고 선택한 행에 대한 작업 선택 목록에서 복사를 클릭합니다.



프로파일이 복사되어 목록에 표시됩니다. 복사본에는 매핑 및 일정 구성을 포함하여 원래 프로필의 모든 설정이 포함됩니다. 프로파일의 이름에는 사본이 포함되어 있습니다. 원본 프로파일이 활성화되더라도(true) 이 시점에서는 복사가 비활성화됩니다(false). 복사된 프로파일의 값을 편집하고 필요에 따라 구성 설정이 새 프로파일에 적용되도록 이름을 바꿀 수 있습니다.



기존 프로파일에서 새 프로파일로 설정을 복사했습니다.

다음에 수행할 작업

구성 단계를 완료한 후 새 프로파일을 활성화(활성화)하라는 메시지가 표시됩니다.

스크립트 편집기를 사용하여 이벤트 수집 통합에 대한 경보 값의 서식을 **Splunk Enterprise Security** 지정합니다

수집된 중요 이벤트 값에서 직접 매핑된 필드와 수동으로 입력하는 값 외에도 스크립트 편집기를 사용하여 매핑 단계 중에 보안 인시던트의 필드 값 형식을 지정합니다.

시작하기 전에

필요한 역할: sn_si.ingestion_profile_admin

> **주:**
> sn_si.admin 역할은 기본적으로 필수 권한을 상속하므로 sn_si.admin 역할을 가진 사용자는 프로필 관리자가 사용할 수 있는 모든 작업을 수행할 수 있습니다.

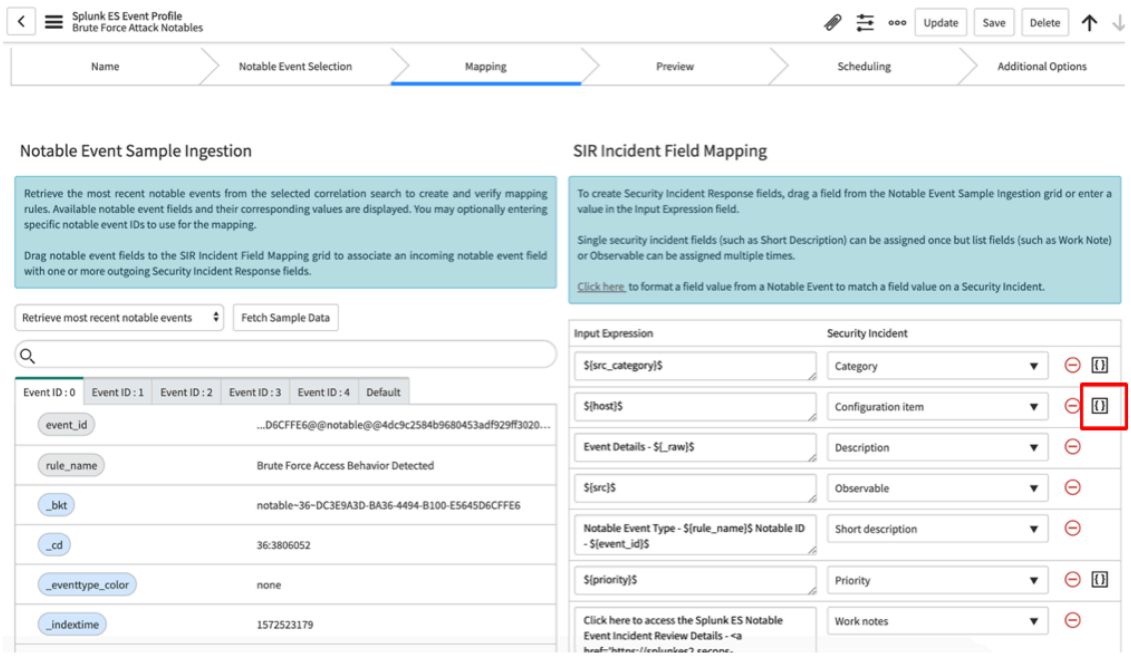
이 태스크 정보

Splunk Enterprise Security 경우에 따라 주목할 만한 이벤트 값이 인시던트의 범주, CI(구성 항목) 및 옵저버블 필드에 SIR 매핑되는 것은 지원되지 않습니다. 매핑된 값을 편집하는 것이 좋습니다. 중요 이벤트의 값을 Splunk Enterprise Security 보안 인시던트의 이러한 필드에서 SIR 지원하는 값으로 변환하려면 스크립트 편집기를 사용합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 매핑 양식이 표시되면 링크를 클릭하여 스크립트 편집기를 엽니다.



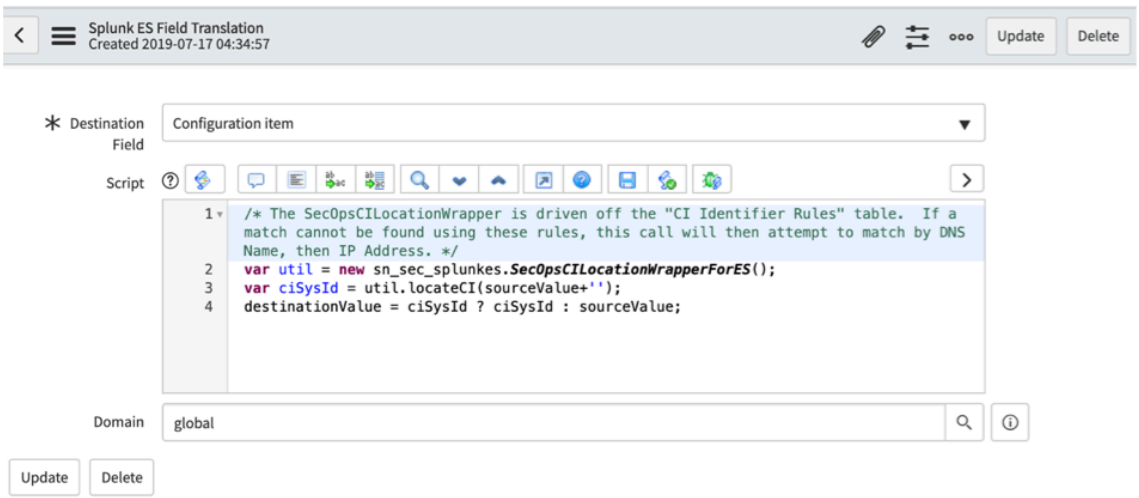
2. 선택 목록에서 편집할 값의 대상 필드를 선택합니다.

3. 또는 SIR 인시던트 필드 매핑 섹션에서 필드 옆에 있는 대괄호 아이콘 [{}] 을 클릭하여 해당 필드의 스크립트 편집기를 엽니다.

경우에 따라 스크립트 포함이 구성 항목 필드에 적합할 수 있습니다. 예를 들어, 중요한 이벤트의 경우 구성 항목의 값이 일치하지 않을 수 있습니다.

다음 그림과 같이 구성 항목 필드의 CMDB에서 ServiceNow AI Platform# 호스트 이름과 일치하는 항목을 찾을 수 없는 경우 IP 주소가 발견되면 구성 항목 필드를 채우도록 규칙을 편집할 수 있습니다. 경보에 대한 값이 없으면 보안 인시던트의 필드가 null로 설정됩니다.

대상 필드에 필드가 표시된 상태로 편집기가 열립니다. 다음 이미지는 ## ## 필드가 대상 필드인 편집기를 보여줍니다.



4. 스크립트에 대한 변경 내용을 입력하고 업데이트를 클릭하여 변경 내용을 저장합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Splunk 필드 번역 테이블이 표시됩니다.

5. 테이블을 닫고 매핑 양식으로 돌아갑니다.

익스포트/임포트 기능을 사용하여 한 인스턴스에서 다른 인스턴스로 프로파일 복사 **Splunk Enterprise Security**

한 인스턴스에서 다른 ServiceNow AI Platform 인스턴스로 ServiceNow AI Platform 프로파일 설정을 익스포트하고 임포트 Splunk Enterprise Security 할 수 있습니다.

시작하기 전에

익스포트하고 임포트할 수 있는 설정에는 프로파일 이름, 상관관계 규칙, 매핑, 필터, 집계 기준, 필드 번역, 가져온 샘플 데이터, 스케줄링 및 구성 타일 소스 정보가 포함됩니다.

필요한 역할: sn_si.ingestion_profile_admin

> **주:**
> sn_si.admin 역할은 기본적으로 필수 권한을 상속하므로 sn_si.admin 역할을 가진 사용자는 프로필 관리자가 사용할 수 있는 모든 작업을 수행할 수 있습니다.

이 태스크 정보

이 기능을 사용하면 보안 관리자가 모든 구성 설정을 다시 실행할 필요 없이 한 ServiceNow AI Platform 인스턴스(예: 비프로덕션)에서 테스트 및 검증된 프로파일을 다른 ServiceNow AI Platform 인스턴스(예: 프로덕션)에 복사할 수 있습니다. 익스포트하고 임포트되는 설정에는 프로파일 이름, 상관관계 규칙, 매핑, 필터, 집계 기준, 필드 번역, 가져온 샘플 데이터, 스케줄링 및 구성 타일 소스 정보가 포함됩니다.

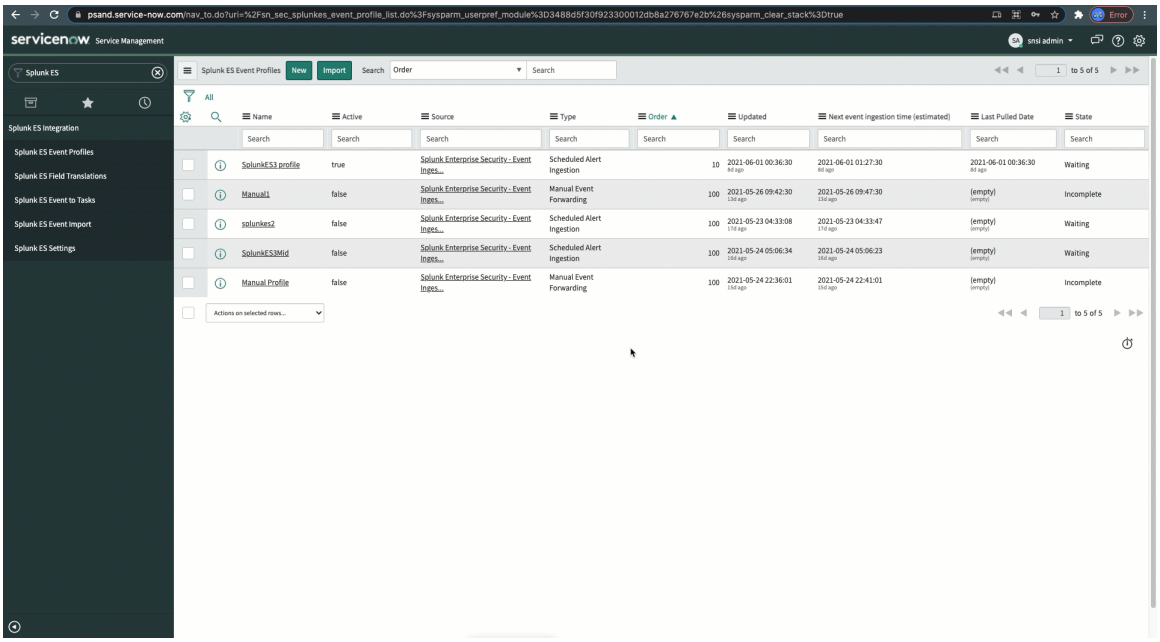
> **주:**
> 수동 이벤트 전달 프로파일 유형을 익스포트하면 샘플 필드 매핑에 사용되는 첨부 파일 데이터는 복사되지만 첨부 파일 자체는 익스포트되지 않습니다.

프로시저

1. 다음으로 이동 모두 〉 **Splunk ES** 통합 〉 **Splunk ES** 이벤트 프로파일.
2. 다른 ServiceNow AI Platform 인스턴스로 익스포트할 프로파일을 선택합니다.
   익스포트할 프로파일을 여러 개 선택할 수 있습니다.
3. Actions(작업) 메뉴에서 Export(내보내기)를 클릭합니다.
4. 내보내기 완료 메시지가 나타나면 다운로드를 클릭합니다.

   다음 그림은 인스턴스(psand.service-now.com)에서 프로파일(SplunkES3profile)을 익스포트하는 ServiceNow AI Platform 방법을 보여줍니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



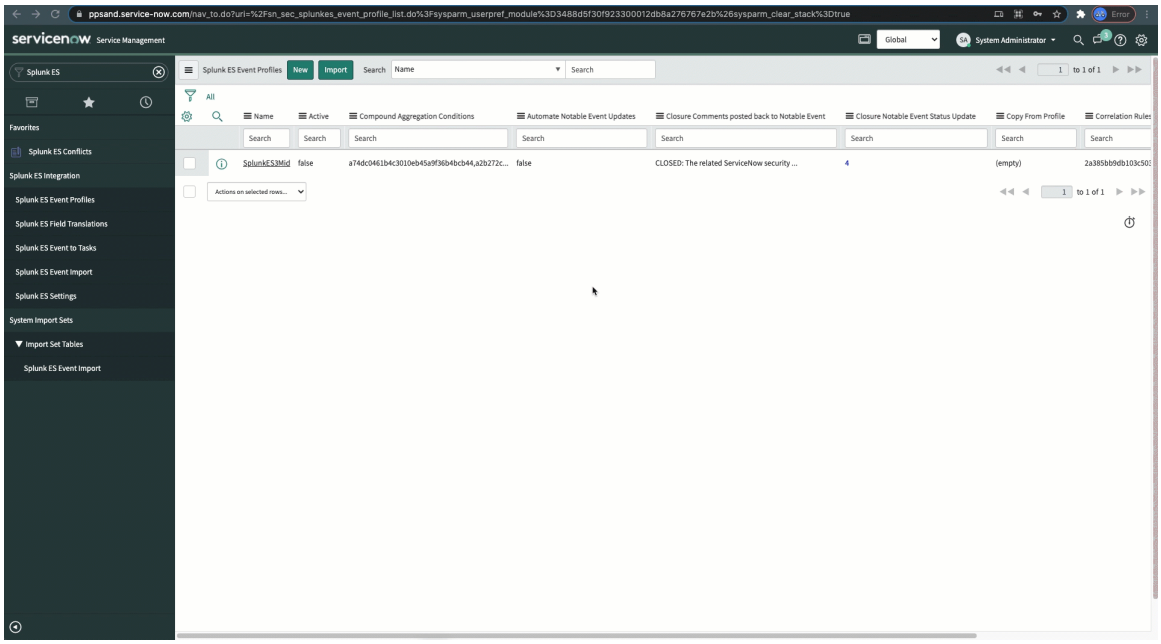
익스포트한 payload.xml 파일이 컴퓨터에 다운로드됩니다. 이 파일에는 프로파일 이름, 상관관계 규칙, 매핑, 필터, 집계 기준, 필드 번역, 가져온 샘플 데이터, 스케줄링 및 구성 타일 소스 정보가 포함되어 있습니다. 여러 프로필을 선택하고 다운로드하면 동일한 payload.xml 파일에 표시됩니다.

이제 다른 ServiceNow AI Platform 인스턴스에서 프로파일 임포트를 진행할 수 있습니다.

5. 다음으로 이동 **Splunk ES** 통합 〉 **Splunk ES** 이벤트 프로파일.
6. 임포트를 클릭합니다.
7. 파일 선택을 클릭하고 컴퓨터에서 xml 파일을 선택합니다.
8. 업로드를 클릭합니다.
9. **Close and Reload** Profiles(종단 닫기 및 다시 로드)를 클릭합니다.

다음 그림은 인스턴스(psand.service-now.com)에서 인스턴스(ppsand.service-now.com)로 프로파일(SplunkES3profile)을 ServiceNow AI Platform 임포트하는 ServiceNow AI Platform 방법을 보여줍니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



다른 ServiceNow AI Platform 인스턴스에서 프로파일을 성공적으로 임포트했습니다.

익스포트한 소스(Splunk API 계정 및 Splunk 서버 URL) 및 MID 서버 구성 설정이 유효하고 임포트한 ServiceNow AI Platform 인스턴스에서 사용할 수 있는지 확인합니다. Splunk Enterprise Security 필요한 경우 구성을 업데이트합니다.

10. 옵션: 프로파일을 임포트한 후 MID 서버 설정을 확인합니다.
11. 옵션: 다음으로 이동 보안 운영 〉 통합 구성.
12. 옵션: 구성 타일을 Splunk Enterprise Security 선택하고 업데이트를 클릭합니다.
13. 옵션: 필요에 따라 소스 및 MID 서버 상세 정보를 검토하고 업데이트합니다.

주목할 만한 이벤트 수집 통합을 위한 **Splunk Enterprise Security** 검사 목록

이 검사 목록을 사용하여 통합의 모든 작업을 안내합니다. 다음 검사 목록에는 설정 및 설치 작업과 통합에 대한 예상 결과를 포함하는 사용 사례의 예가 포함되어 있습니다.

시작하기 전에

필요한 역할: sn_si.ingestion_profile_admin, 관리자, sn_si.admin, sn_si.analyst, Splunk Enterprise Security 관리자

> **주:**
> sn_si.admin 역할은 기본적으로 필수 권한을 상속하므로 sn_si.admin 역할을 가진 사용자는 프로필 관리자가 사용할 수 있는 모든 작업을 수행할 수 있습니다.

이 태스크 정보

다음 표를 사용하여 통합의 설정, 설치 및 구성으로 진행 상황을 추적합니다. 다음 단계로 이동하기 전에 단계에 대한 모든 작업을 완료합니다. 테이블의 각 행은 작업을 나열하고 작업을 수행하는 데 필요한 역할을 식별합니다. 설치 및 구성 안내서의 번호가 매겨진 주제도 참조됩니다.

각 작업에 필요한 역할이 다음 테이블의 각 단계와 함께 나열됩니다.

프로시저

1. 통합의 설정, 설치 및 구성으로 진행 상황을 추적합니다.
   다음 단계로 이동하기 전에 단계에 대한 모든 작업을 완료합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

2. 표의 단계를 제시된 순서대로 따릅니다.

검사 목록

☐	관리자 역할이 있는 ServiceNow AI Platform 사용자가 인스턴스를 설정합니다 ServiceNow AI Platform . ○ 필요에 따라 사용자에게 **sn_si.ingestion_profile_admin** (또는 sn_si.admin) 및 sn_si.analyst 역할을 할당합니다. ○ 서버가 회사 네트워크 내에 배포된 경우 Splunk MID 서버를 설치하고 구성합니다. ○ 플러그인이 ServiceNow 보안 인시던트 응답 릴리스 ServiceNow AI Platform에 맞게 활성화되어 있는지 확인합니다. ○ (선택 사항) 콘솔에서 인스턴스로 ServiceNow AI Platform 이벤트를 수동으로 Splunk Enterprise Security 전달하려면 관리자 권한이 있는 Splunk Enterprise Security 사용자에게 (sn_sec_splunkes.api_account_access) 역할을 할당했는지 확인합니다. 자세한 내용은 ServiceNow AI Platform 통합을 위한 Splunk Enterprise Security 인스턴스 설정 문서를 참조하십시오.
☐	관리자 역할이 있는 ServiceNow AI Platform 사용자는 에서 ServiceNow Store애플리케이션을 설치하고 구성합니다Splunk Enterprise Security. **a.** 인스턴스에 애플리케이션을 ServiceNow AI Platform 다운로드하여 설치합니다. **b.** 애플리케이션을 구성하고 콘솔에 연결합니다 Splunk Enterprise Security . 자세한 내용은 주목할 만한 이벤트 수집 통합 설치 및 구성 Splunk Enterprise Security 문서를 참조하십시오.
☐	(선택 사항) 콘솔에서 인스턴스로 Splunk Enterprise SecurityServiceNow AI Platform 이벤트를 수동으로 익스포트하려면 다음 작업을 수행합니다. ○ Splunk Enterprise Security 관리자는 콘솔에서 **splunkbase** Splunk Enterprise Security 에 대한 Splunk Enterprise Security 보안 운영 이벤트 수집 추가 기능을 설치, 설정 및 활성화합니다ServiceNow. ○ Splunk Enterprise Security 관리자가 아직 구성을 마치지 않았다면, 검색을 콘솔에서 중요 이벤트 Splunk Enterprise Security 로 저장합니다. 자세한 내용은 Splunk 주목할 만한 이벤트 수집 통합의 수동 이벤트 수집을 Splunk Enterprise Security 위한 환경 설정 문서를 참조하십시오.
☐	ServiceNow AI Platform **sn_si.ingestion_profile_admin** 역할을 가진 사용자가 이벤트 프로파일을 생성하고 이름을 지정합니다. 선택 목록에서 프로파일 유형을 선택합니다. 옵션은 샘플 데이터를 수집하는 데 사용하는 예약된 경보 프로파일 또는 콘솔에서 첨부 파일 데이터를 수동으로 Splunk Enterprise Security 익스포트하는 데 사용하는 이벤트 프로파일입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

	○ 예약된 경보의 경우 사용 가능한 경보를 선택합니다. ○ 수동으로 익스포트된 데이터에 대한 프로파일의 경우 새 맵을 작성하거나 기존 맵을 복사합니다. 자세한 내용은 이벤트 수집 통합을 위한 Splunk Enterprise Security 이벤트 프로파일 생성 및 이름 지정 문서를 참조하십시오.
☐	ServiceNow AI Platform **sn_si.ingestion_profile_admin** 역할을 가진 사용자는 수집된 값 또는 보안 인시던트로 Splunk Enterprise SecurityServiceNow AI Platform 익스포트되는 첨부 파일 데이터를 매핑합니다. **a.** 예약된 경보에 대한 샘플 데이터를 가져옵니다. **b.** (선택 사항) 이벤트에서 Splunk Enterprise Security 첨부 파일 데이터를 수동으로 익스포트합니다. **c.** 기본 매핑 구성을 편집합니다. **d.** 필요에 따라 필터링 기준을 추가하고, 기존 보안 인시던트에 경보를 추가하고, 스크립트 편집기를 사용합니다. 자세한 내용은 통합을 위한 Splunk Enterprise Security 주목할 만한 이벤트 필드 매핑 및 중요 이벤트 인시던트 검토 및 기여 이벤트 상세 정보(예약된 수집)에 대한 Splunk ES 매핑 생성 문서를 참조하십시오.
☐	○ ServiceNow AI Platform **sn_si.ingestion_profile_admin** 역할을 가진 사용자는 보안 인시던트에 ServiceNow AI Platform 표시되는 데이터를 Splunk Enterprise 미리 봅니다. ○ 오류 메시지가 표시되지 않도록 오류를 수정하거나 누락된 데이터를 추가합니다. 자세한 내용은 이벤트 수집 통합에 Splunk Enterprise Security 대한 보안 인시던트 미리 보기 문서를 참조하십시오.
☐	ServiceNow AI Platform **sn_si.ingestion_profile_admin** 역할을 가진 사용자는 예약된 경보가 있는 프로파일에 대한 경보 검색을 예약합니다. 자세한 내용은 이벤트 수집 통합을 위해 Splunk Enterprise Security 새롭고 업데이트된 주목할 만한 이벤트 예약 및 검색 문서를 참조하십시오.

설정 단계를 성공적으로 완료하고 통합에 대한 예상 결과를 확인했습니다.

Splunk - Incident Enrichment 통합

인시던트 보강 통합은 Splunk 로그를 검색하고 관련 사이팅 정보를 보안 인시던트에 추가합니다.

탐색	설정
보안 인시던트 응답 통합	다음에 대한 검색 통합 시작하기 Splunk보안 운영
사용	개발

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 사이팅 검색 실행
- Security Operations Integration - 사이팅 검색 플로우
- 보안 운영 통합 - Splunk 사이팅 검색 플로우
- 사이팅 검색 상세 정보 보기
- 사이팅 검색 결과 보기
- ServiceNow 보안 운영 통합 개발 가이드라인
- 통합 작성을 위한 팁
- 개발자 교육
- 개발자 설명서
- 애플리케이션과 함께 설치되는 구성요소 찾기

문제 해결 및 추가 정보

- 통합 문제 해결
- 보안 운영 커뮤니티에서 질문 또는 답변하기
- 알려진 오류 포털에서 알려진 오류 문서 검색

- 연락처 고객 서비스 및 지원

다음에 대한 검색 통합 시작하기 **Splunk**보안 운영

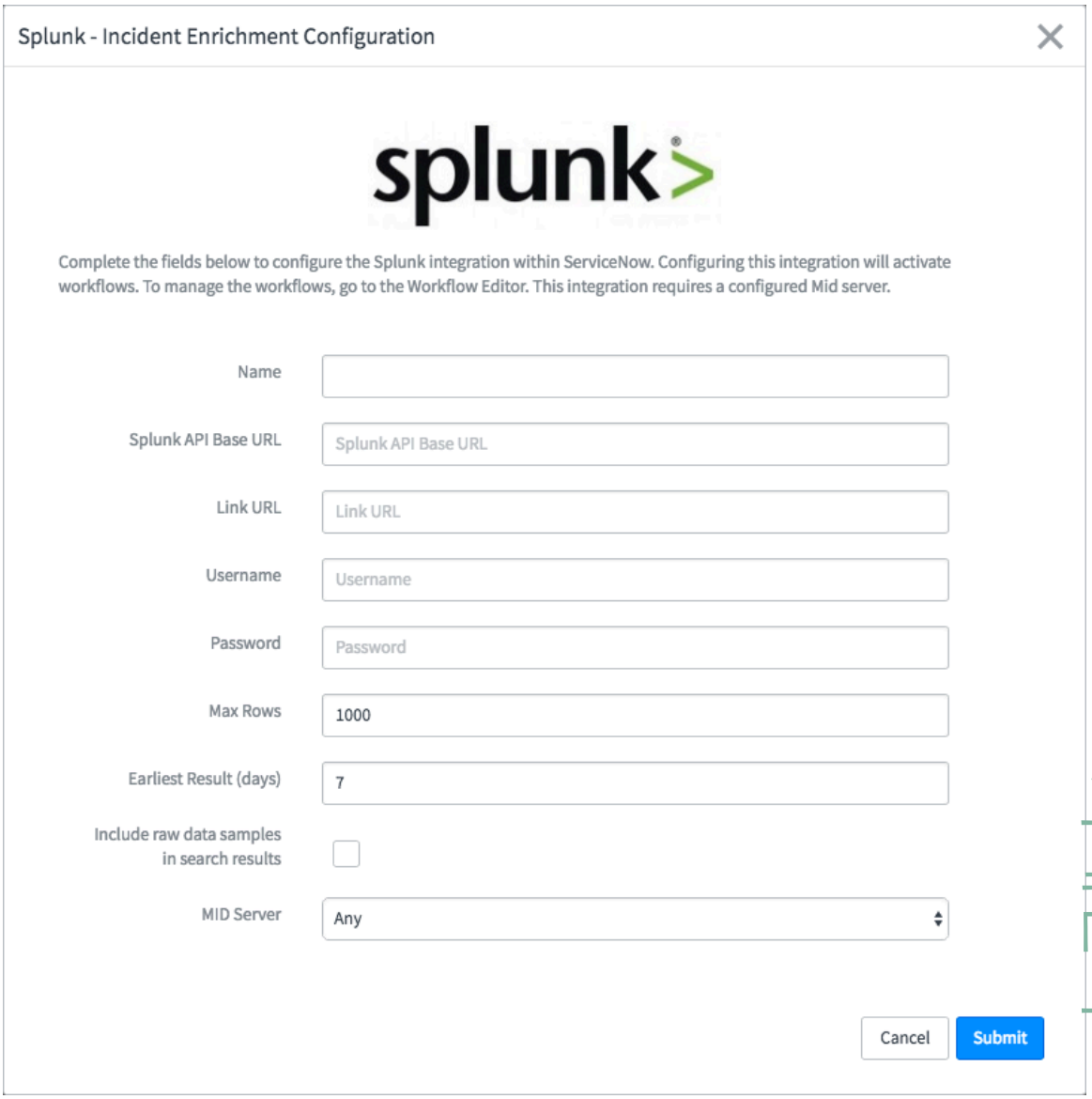
Splunk 소프트웨어는 기계에서 생성된 빅 데이터를 보안 운영검색, 모니터링 및 분석하고 . 인시던트 보강 통합을 사용하려면 Splunk 먼저 다음 ServiceNow Store 에서 다운로드하고 적절한 API 기준 URL 및 로그인 자격 증명을 추가해야 합니다.

시작하기 전에
필요한 역할: sn_si.admin

프로시저

1. 에서 통합을 다운로드합니다. ServiceNow Store.
2. 설치가 완료되면 프로파일에서 API 키 및 API ID에 액세스하고 Splunk 가져옵니다.
3. 인스턴스에서 다음으로 이동합니다. 보안 운영 〉 통합 구성.
   사용 가능한 보안 통합은 일련의 카드로 표시됩니다.
4. Splunk - 인시던트 보강 카드에서 새로 만들기를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



5. 필요에 따라, 필드를 채웁니다.

필드	설명
이름	이 구성의 이름입니다.
Splunk API 기준 URL	사이트에서 가져온 기본 URL입니다 Splunk .
링크 URL	〔선택사항〕 사용 가능한 경우 웹 인터페이스에 링크되는 링크 URL입니다 Splunk .
사용자 이름	Splunk 사용자 이름입니다.
암호	Splunk 암호입니다.
최대 행 수	검색할 행의 최대 수입니다.
가장 빠른 결과(일)	일수 단위로 보려는 가장 빠른 결과입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
검색 결과에 원시 데이터 샘플 포함	사이팅 검색 결과에 원시 데이터 샘플을 포함하려면 이 옵션을 선택합니다. 반환되는 데이터의 양은 보안 인시던트 응답 속성의원시 데이터 속성 행 수의 설정에 따라 달라집니다.
MID 서버	활성 MID 서버를 사용하려면 임의 를 선택하고, 특정 MID 서버 이름을 선택합니다.

주:
이 통합을 구성하면 워크플로우가 활성화됩니다. 워크플로우를 관리하려면 워크플로우 편집기로 이동합니다.

6. 제출을 클릭합니다.
   통합 구성 카드가 표시됩니다.
7. 새 구성 카드를 볼 때 구성 또는 삭제를 클릭하여 구성을 변경하거나 삭제할 수 있습니다.
8. 통합 구성 카드의 원래 목록으로 돌아가려면 구성 표시 드롭다운 목록에서 아니요를 선택합니다.

용 모바일 환경 보안 인시던트 응답

Android 또는 iOS 모바일 장치를 사용하여 SOC(Security Operations Center) 작업을 관리할 수 있습니다.

스토어에서 앱 요청

ServiceNow Store 웹 사이트를 방문하면 사용 가능한 모든 앱을 확인하고 스토어에 요청을 제출하는 방법에 대한 정보를 참조할 수 있습니다. 출시된 모든 앱의 누적 릴리스 정보는 ServiceNow Store 버전 기록 릴리스 정보 를 참조하십시오.

보안 인시던트 응답

인스턴스에 있는 ( ) 제품의 기본 개념 보안 인시던트 응답 에 익숙하지 않은 경우 위협 인텔리전스에 대한 자세한 내용과 이 제품이 조직에 대한 사이버 위협의 우선순위를 지정하고 해결하는 데 어떻게 도움이 되는지 확인하십시오보안 인시던트 응답 개요 대시보드. SIRServiceNow AI Platform#

개요

보안 운영 센터(SOC) 관리자 또는 보안 분석가 역할(sn_si.analyst)의 ServiceNow AI Platform 사용자는 모바일 장치에서 직접 인스턴스에 로그인할 ServiceNow AI Platform 수 있습니다. 를 보안 인시던트 대응 모바일 앱사용하면 가장 최신의 중요한 SIR 보안 인시던트와 응답 작업을 보고, 편집하고, 할당할 수 있습니다. 알림은 할당된 중요한 보안 인시던트가 도착하면 알려줍니다.

를 보안 인시던트 대응 모바일 앱사용하면 모바일 장치에서 다음과 SIR 같은 관련 작업을 수행할 수 있습니다.

- 중요한 보안 인시던트 및 응답 작업 목록을 봅니다.
- 미리 정의된 알림 기준을 충족하는 보안 인시던트 및 작업에 대한 자세한 알림을 받습니다.
- 미리 정의된 쿼리 또는 필터 집합을 기반으로 하는 보안 인시던트 또는 작업의 그룹화를 봅니다.
- 보안 인시던트의 작업 메모 및 관련 목록을 봅니다.
- 보안 인시던트를 업데이트하고 작업 메모 또는 첨부 파일을 추가합니다.
- 보안 인시던트에 대한 필드를 편집합니다.
- 본인 또는 보안 팀의 다른 구성원에게 보안 인시던트를 할당합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이러한 목록이 채워지면 다음을 보안 인시던트 대응 모바일 앱사용하여 보안 인시던트에 대한 SIR 다음 관련 목록을 볼 수 있습니다.

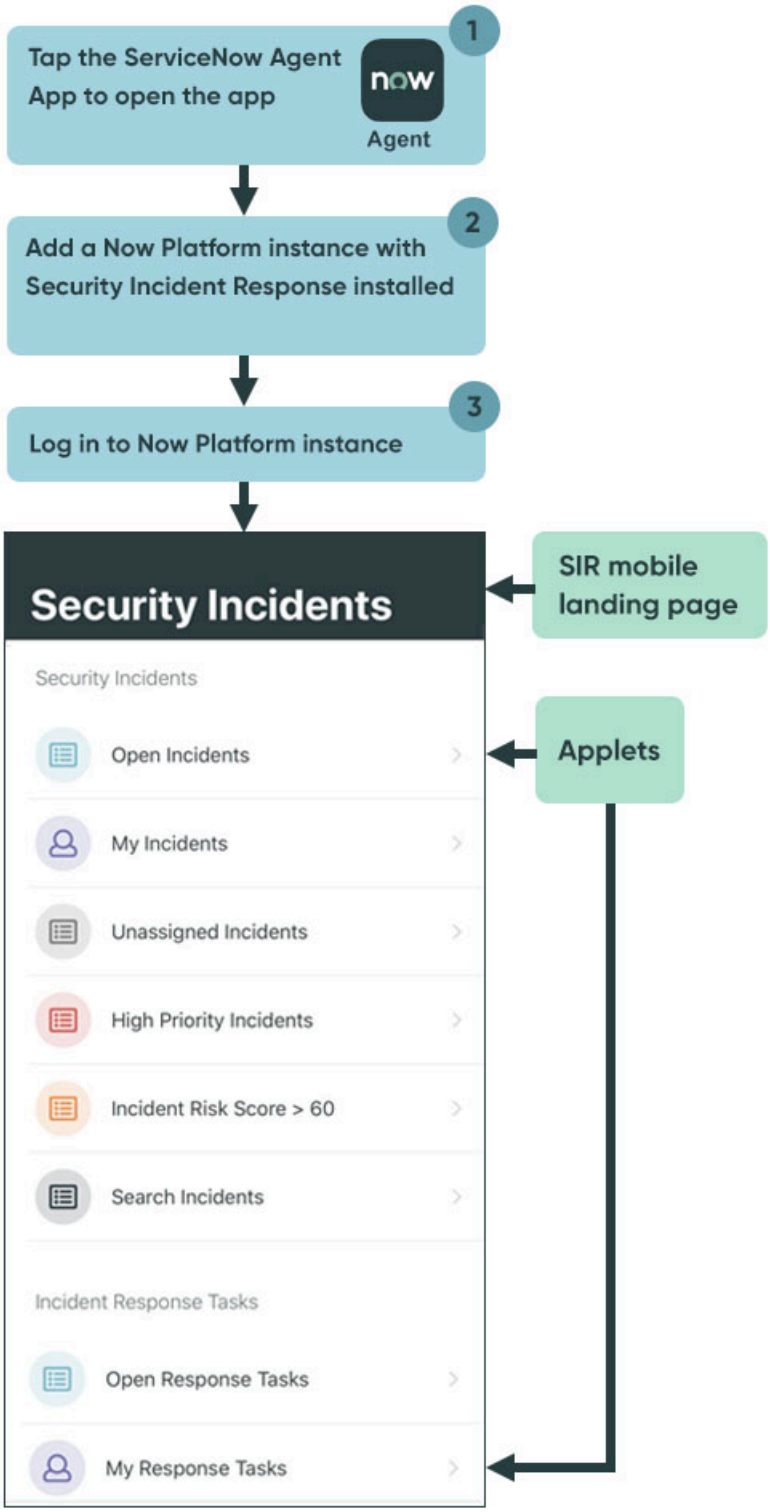
- 구성 항목
- 영향을 받는 사용자
- 영향을 받는 서비스
- 하위 보안 인시던트
- 유사한 보안 인시던트(지원하지 ServiceNow AI Platform않음)
- 옵저버블
- 응답 작업
- 작업
- 작업 SLA
- 첨부 파일(지원하지 ServiceNow AI Platform않음)

다음 그림은 모바일 장치에서 인스턴스에 로그인하는 ServiceNow AI Platform 방법과 로그인한 후 실행되는 방문 화면의 보안 인시던트 대응 모바일 앱 구조를 보여줍니다.

인스턴스를 설정하고 ServiceNow AI Platform 설치하는 보안 인시던트 대응 모바일 앱방법에 대한 단계별 지침은 문서를 에 대한 검사 목록 설정 보안 인시던트 대응 모바일 앱참조하십시오. 로그인 방법에 대한 지침은 문서를 참조하십시오 에 로그인 보안 인시던트 대응 모바일 앱.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 인시던트 대응 모바일 앱



애플리케이션

ServiceNow# 애플리케이션은 인스턴스 내에서 특정 특성 및 기능성을 제공하는 (SIR), 취약성 대응 (VR), 거버넌스, 리스크 및 컴플라이언스 ()GRC와 같은 보안 인시던트 응답 소프트웨어 구성요소입니다ServiceNow AI Platform. Core 애플리케이션과 인스턴스에 보안 인시던트 대응 모바일 앱ServiceNow AI Platform Core 애플리케이션을 설치하면 보안 인시던트 응답 로그인했을 때 Core 애플리케이션의 아이콘이 사용자 Android 또는 iOS 모바일 장치 하단에 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 인시던트 대응 모바일 앱 (보안 인시던트) 아이콘

폴더

각 ServiceNow# 모바일 애플리케이션에는 범주별로 애플릿을 구분하는 폴더가 있습니다. 방문 페이지의 이전 이미지에서 보안 인시던트 및 인시던트 응답 작업은 폴더입니다.

애플릿

애플릿은 애플리케이션 내의 다른 옵션입니다. 보안 인시던트 및 인시던트 대응 작업 섹션 아래의 아이콘은 의 사용 가능한 애플릿보안 인시던트 대응 모바일 앱입니다.

에 대한 검사 목록 설정 보안 인시던트 대응 모바일 앱

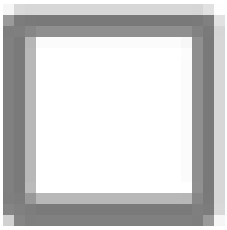
다음 검사 목록에는 를 보안 인시던트 대응 모바일 앱사용하기 전에 인스턴스 ServiceNow AI Platform# 와 모바일 장치에서 완료해야 하는 설정 작업이 포함되어 있습니다.

시작하기 전에
옵션으로, 이 검사 목록을 인쇄하고 이를 사용하여 에 필요한 보안 인시던트 대응 모바일 앱설정 작업을 안내합니다. 모바일 장치에서 보안 인시던트를 보고 편집할 SIR 수 있도록 목록의 각 항목이 완료되었는지 확인합니다.

검사 목록 항목은 강조 표시된 텍스트로 표시됩니다. 추가 정보는 오른쪽 열의 각 항목을 따릅니다. 이 작업의 예상 완료 시간: 15-20분.

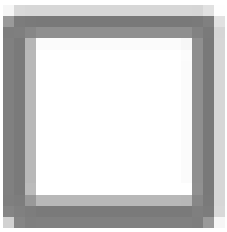
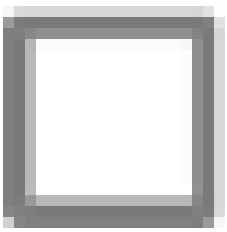
필요한 역할: admin, sn_si.analyst

모바일 검사 목록

항목	설명
	관리자 역할이 있는 사용자는 인스턴스에 코어 애플리케이션이 설치되어 ServiceNow AI Platform 있는지 보안 인시던트 응답 확인합니다. 모바일 장치에서 보는 인스턴스입니다 ServiceNow AI Platform . 주: 보안 인시던트 응답 핵심 애플리케이션과 ServiceNow AI Platform 인스턴스는 동일한 제품군 릴리스에 속해야 합니다. 1. 인스턴스에 핵심 애플리케이션이 설치되어 있는지 확인하려면 플러그인으로 이동하여 보안 인시던트 응답을 검색합니다. 2. 보안 인시던트 응답 코어 애플리케이션이 아직 설치되지 않은 경우 설치를 클릭하여 설치합니다. 핵심 애플리케이션 설치에 보안 인시던트 응답 대한 자세한 내용은 다음 문서를 참조하십시오 보안 인시던트 응답 설치 및 구성. 보안 인시던트 응답 핵심 애플리케이션이 플러그인에 표시되지 않는 경우 핵심 애플리케이션 설치 및 애플리케이션에 대한 권리에 대한 자세한 내용은 다음 문서를 참조하십시오보안 운영 그리고 ServiceNow Store.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모바일 검사 목록

항목	설명
	관리자 역할이 있는 사용자는 모바일 장치에서 보려는 인스턴스에 가 보안 인시던트 대응 모바일 앱 설치되어 ServiceNow AI Platform 있는지 확인합니다. 주: 보안 인시던트 대응 모바일 앱 및 ServiceNow AI Platform 인스턴스는 동일한 제품군 릴리스에 속해야 합니다. 에서 ServiceNow Store 다운로드하여 보안 인시던트 대응 모바일 앱 인스턴스의 ServiceNow AI Platform 에 설치합니다. 를 보안 인시던트 대응 모바일 앱설치하면 해당 종속성, com.glide.sg 및 com.glide.sg.agent_native_client도 설치됩니다. 이러한 종속성이 설치되어 있는지 확인하려면 다음을 수행합니다. **1.** 플러그인으로 이동합니다. **2.** 플러그인 ID(com.glide.sg 및 com.glide.sg.agent_native_client)를 검색합니다. **3.** 활성화되지 않은 경우 이러한 플러그인을 활성화합니다. 이러한 플러그인은 에 보안 인시던트 대응 모바일 앱필요합니다. 애플리케이션 설치 및 애플리케이션에 대한 권리에 대한 자세한 내용은 다음 문서를 참조하십시오 보안 운영 그리고 ServiceNow Store.
	관리자 역할이 있는 사용자는 ServiceNow AI Platform 인스턴스에 필요한 역할을 ServiceNow AI Platform 가진 모바일 사용자를 할당했는지 확인합니다. **1.** 사용자에게 할당된 역할을 보려면 다음으로 이동합니다. 사용자 및 그룹 〉 사용자. **2.** 사용자 이름과 역할 관련 목록을 차례로 선택합니다. 이 사용자에게 할당된 모든 역할이 표시됩니다. **3.** 사용자가 할당되었는지 확인하거나 사용자에게 IT 인프라 라이브러리 역할(itil)을 할당합니다. itil 역할을 가진 사용자는 보안 인시던트를 생성, 열기, 업데이트 및 종결할 수 있습니다. itil 역할을 가진 사용자만 작업을 할당할 수 있습니다. **4.** 사용자가 할당되었는지 확인하거나 보안 분석가 역할(sn_si.analyst)을 사용자에게 할당합니다. sn_si.analyst 역할을 가진 사용자는 보안 인시던트 기록을 읽고 편집할 수 있습니다. itil 역할을 할당하면 이 역할이 자동으로 추가됩니다. **5.** 필요한 할당 그룹을 생성하고 모바일 사용자를 해당 그룹에 할당했는지 확인합니다. 주: 모바일 애플리케이션 사용자가 많은 경우 그룹에 sn_si.analyst 역할을 할당할 수도 있습니다. 그룹에 추가하는 각 사용자는 이 역할을 상속합니다. 보안 분석가에 대한 자세한 내용은 다음 문서를 참조하십시오 보안 분석가 할당.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모바일 검사 목록

항목	설명
	사용자 및 사용자 및 그룹에 역할 할당에 대한 자세한 내용은 사용자 관리를 참조하십시오.
☐	sn_si.analyst 역할을 가진 사용자는 모바일 장치에 최신 ServiceNow# 에이전트 앱을 다운로드합니다. 에이전트 앱의 최신 버전은 Apple iOS App Store와 Play 스토어에서 사용할 수 있습니다 Google .
☐	sn_si.analyst 역할을 가진 사용자는 모바일 장치와 ServiceNow AI Platform 인스턴스에서 알림을 사용할 수 있는지 확인합니다. 알림은 중요한 보안 인시던트가 사용자 또는 할당 그룹에 할당될 때 알려줍니다. 시기 적절한 수정을 지원하려면 알림을 활성화한 후 에서 보안 인시던트 대응 모바일 앱 알림을 클릭하여 보안 인시던트로 직접 이동합니다. 모바일 장치에 표시되도록 인스턴스에서 알림을 ServiceNow AI Platform 활성화하려면 다음 단계를 따르십시오. **1.** 인스턴스에 다운로드하여 보안 인시던트 대응 모바일 앱ServiceNow AI Platform 설치했는지 확인합니다. **2.** 인스턴스의 시스템 설정에 ServiceNow AI Platform 있는 알림에서 **ServiceNow Mobile** 애플리케이션을 활성화했는지 확인합니다. 알림 설정에 대한 자세한 내용은 코어 UI에서 사용자 알림 기본 설정 지정을 참조하십시오. ServiceNow AI Platform 알림은 모바일 장치의 메시지 화면에도 표시됩니다. 모바일 장치의 설정에서도 알림이 활성화되어 있는지 확인합니다.

모바일 장치와 에 대한 보안 인시던트 대응 모바일 앱를 ServiceNow AI Platform 성공적으로 설정했습니다. 다음 단계는 모바일 장치로 인스턴스에 로그인하는 ServiceNow AI Platform 것입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

에 로그인 보안 인시던트 대응 모바일 앱

보안 인시던트 응답 모바일 앱을 열고 보안 인시던트 응답이 ServiceNow AI Platform# 있는 인스턴스를 모바일 장치에 추가합니다.

시작하기 전에

필요한 역할: sn_si.analyst

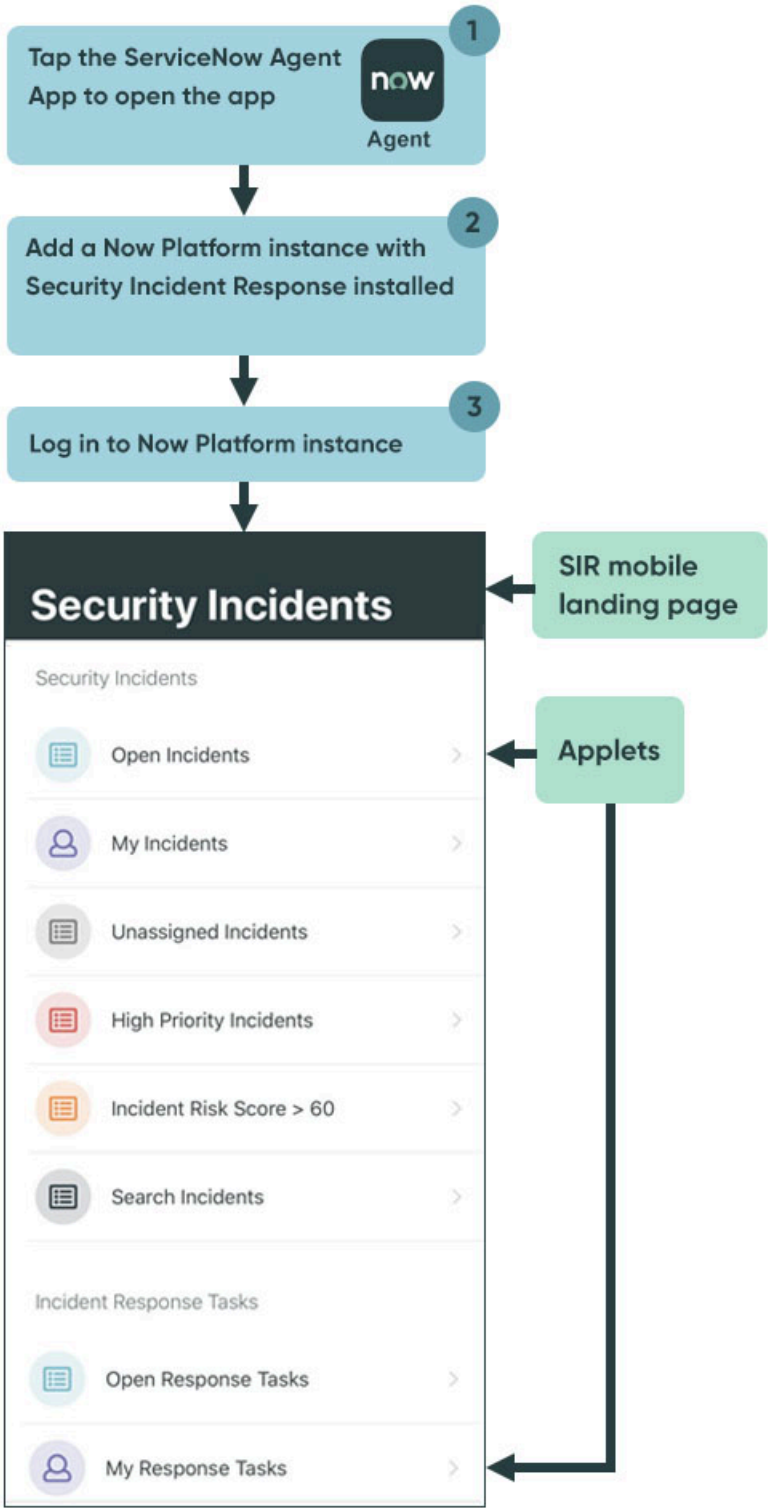
이 태스크 정보

이 작업 완료 시간: 5-10분.

설명된 에 대한 검사 목록 설정 보안 인시던트 대응 모바일 앱설정 단계를 완료했는지 확인합니다.

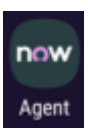
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 인시던트 대응 모바일 앱



프로시저

1. 모바일 장치에서 **ServiceNow Agent** 앱을 눌러 엽니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

인스턴스에 아직 로그인 ServiceNow AI Platform 하지 않은 경우 인스턴스 화면이 표시됩니다.

2. ServiceNow AI Platform 코어 애플리케이션이 있는 보안 인시던트 응답 인스턴스가 모바일 장치에 아직 추가되지 않은 경우 다음 단계에 따라 추가합니다.

   a. 표시되는 인스턴스 화면에서
   인스턴스의 주소를 ServiceNow AI Platform 입력하고 저장하라는 메시지가 표시되는 화면이 표시됩니다.

   b. 필드에 내용을 입력합니다.

필드	설명
인스턴스 주소를 입력하거나 QR 코드를 스캔합니다.	계속하려면 하나를 선택합니다. ▪ .service-now.com 앞에 인스턴스의 이름ServiceNow AI Platform(예: sirmobileny)을 입력합니다. ▪ 주소를 입력합니다. 이 주소는 모바일 장치에서 보려는 인스턴스의 URL ServiceNow AI Platform 입니다(예: https://sirmobileny.service-now.com). ▪ QR 코드를 스캔합니다.
(선택 사항) 별칭 입력	이 인스턴스의 별칭을 입력합니다. 장치에 여러 인스턴스가 추가된 경우 별칭을 사용하면 인스턴스를 빠르게 찾을 수 있습니다 ServiceNow AI Platform .

   c. 저장 및 로그인을 누릅니다.

3. ServiceNow 표시되는 로그인 화면에서 추가할 인스턴스의 사용자 이름과 암호를 ServiceNow AI Platform 입력하고 로그인을 누릅니다.
   보안 인시던트 방문 화면이 표시됩니다. 에 보안 인시던트 대응 모바일 앱성공적으로 로그인했습니다.

4. 로그인한 후 에서 보안 인시던트 대응 모바일 앱알림이 활성화되었는지 확인합니다.

   a. 하단의 방문 화면에서 알림을 탭합니다.

   b. 알림 화면에서 활성화되지 않은 경우 알림 활성화 를 누릅니다.
   의 ServiceNow AI Platform 알림은 의 보안 인시던트 대응 모바일 앱알림 화면에 표시됩니다.

5. 모바일 장치의 인스턴스에 로그인하면 이 장치가 기본 ServiceNow AI Platform 인스턴스가 됩니다. 장치에서 다른 ServiceNow AI Platform 항목을 보려면 기본 인스턴스에서 로그아웃해야 합니다. 로그아웃하려면 다음을 수행합니다.

   a. 설정 아이콘을 누릅니다.

   b. 로그아웃을 누릅니다.
   인스턴스 화면은 모바일 장치에 추가한 모든 ServiceNow AI Platform 인스턴스와 함께 표시됩니다.

   c. 옵션: 다른 인스턴스를 눌러 로그인하거나, 이전 단계에 따라 다른 인스턴스를 추가합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

장치에서 **ServiceNow** 에이전트 앱을 탭한 후 에 대한 보안 인시던트 대응 모바일 앱 인스턴스 화면이 표시되지 않으면 장치에서 **ServiceNow** 에이전트가 신뢰할 수 있는 앱으로 허용되는지 확인하십시오. 신뢰할 수 있는 앱으로 액세스를 허용하려면 장치의 설정 및 일반 장치 관리로 이동하고 옵션(Trust 앱 등)을 탭하여 액세스를 허용합니다.

로그인 화면에 자격 증명을 입력한 후에 오류 메시지가 표시되면 인스턴스의 사용자 이름과 암호가 ServiceNow AI Platform 올바른지 확인하십시오.

방문 화면을 보는 데 문제가 있는 경우 네트워크 연결을 확인합니다.

ServiceNow 에이전트 앱을 탭한 후 인스턴스 화면을 볼 수 없으면 장치에서 앱을 제거해 보십시오. Apple iOS App Store 또는 Google Play 스토어에서 최신 버전의 앱이 있는지 확인하고 다시 설치해 보십시오.

를 사용하여 미해결 보안 인시던트 보기, 편집 및 할당 보안 인시던트 대응 모바일 앱

보안 인시던트 분석가는 모바일 장치에서 미해결 보안 인시던트 응답 (SIR) 보안 인시던트를 보고, 편집하고, 할당합니다. 인시던트에 대한 자세한 내용은 관련 목록과 작업 메모의 감사 추적을 참조하십시오.

시작하기 전에
필요한 역할: sn_si.analyst

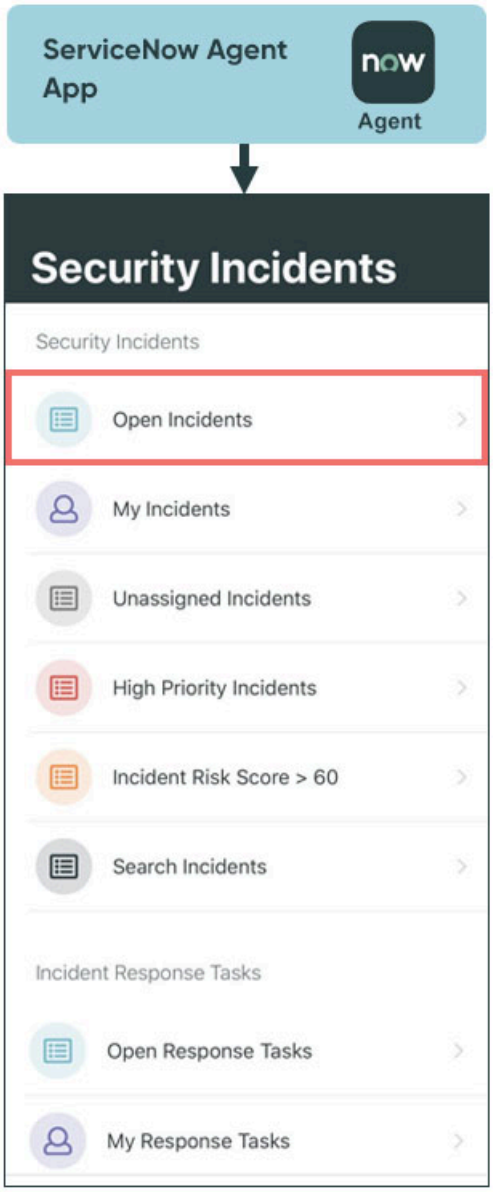
이 태스크 정보
기록 목록에서 미해결된 보안 인시던트를 자신에게 할당하거나 다시 할당합니다. 또는 기록의 상세 정보 및 관련 목록을 보거나 할당하기 전에 작업 메모를 추가합니다. 이 작업 완료 시간: 5-10분.

프로시저

1. 모바일 장치에서 인스턴스에 로그인 ServiceNow AI Platform 하지 않은 경우 문서를 참조하십시오 에 로그인 보안 인시던트 대응 모바일 앱.
2. 보안 인시던트 방문 페이지가 표시되면 미해결 인시던트를 누릅니다.

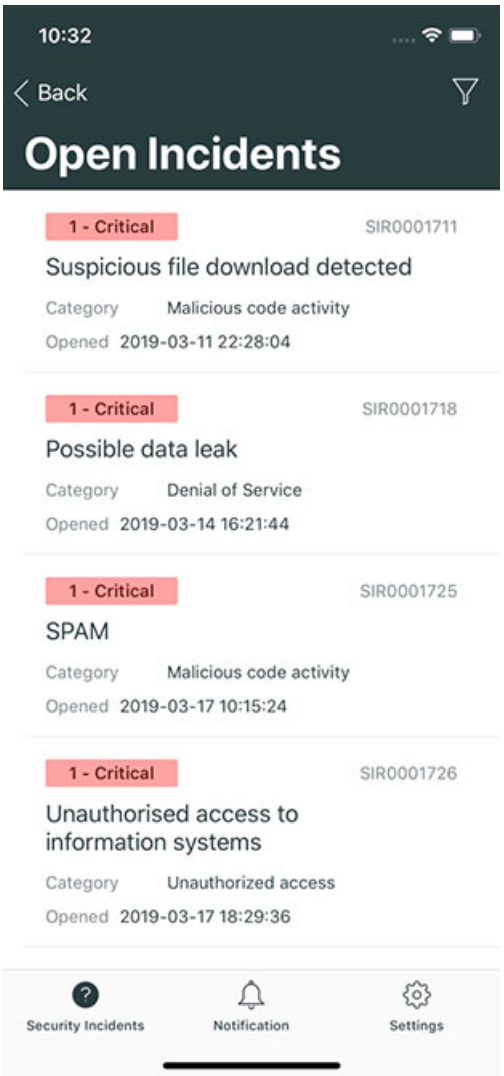
   로그인한 후 다른 보안 인시던트 대응 모바일 앱 곳으로 이동할 경우 언제든지 Now Agent 앱을 탭하여 마지막으로 표시한 화면으로 돌아갈 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



미해결 인시던트 화면에 미해결 보안 인시던트 기록 목록이 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



3. 옵션: 를 참조하여 를 사용하여 보안 인시던트 검색 보안 인시던트 대응 모바일 앱 특정 기준과 일치하는 보안 인시던트를 검색합니다.

   또는 필터 아이콘( )이 표시되면 필터를 설정하여 목록의 기록 수를 제한합니다 . 모바일 앱의 화면에서 기록을 필터링하는 것은 에서 ServiceNow AI Platform조건 작성기로 필터링하는 것과 비슷합니다.

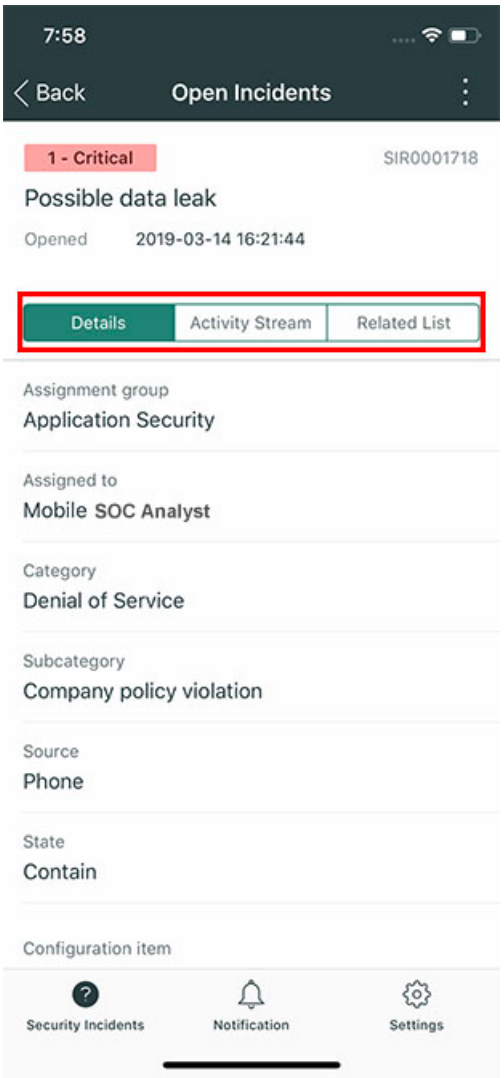
4. 자신에게 인시던트를 할당하거나 오픈 보안 인시던트 목록에서 직접 다시 할당하려면 기록을 왼쪽으로 살짝 밀어 메뉴를 엽니다.

5. 표시되는 메뉴에서 하나를 선택하여 계속합니다.

6. 또는 미해결 보안 인시던트 기록의 상세 정보를 보고 더 많은 관련 기록 및 관련 목록을 보려면 미해결 인시던트 화면이 표시된 상태에서 목록에서 기록을 누릅니다.

7. 표시되는 열린 기록에서 다음 표의 옵션 하나를 선택하여 계속합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



와 함께 사용자에게 할당된 보안 인시던트를 보고, 편집하고, 재할당합니다. 보안 인시던트 대응 모바일 앱

보안 인시던트 분석가는 자신에게 할당된 인시던트를 보고, 편집하고, 재할당합니다보안 인시던트 응답SIR. 인시던트에 대한 자세한 내용은 관련 목록과 작업 메모의 감사 추적을 참조하십시오.

시작하기 전에
필요한 역할: sn_si.analyst

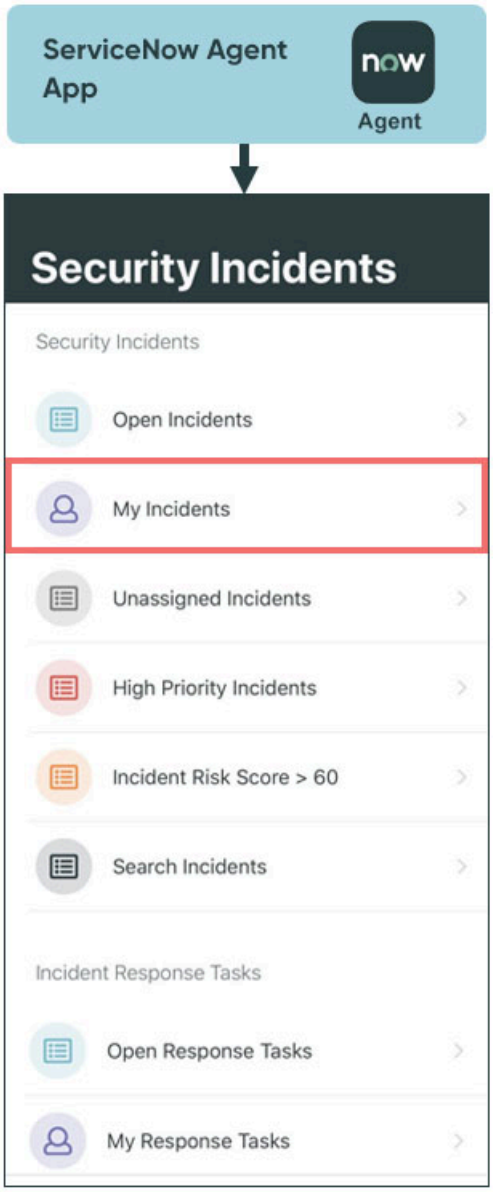
이 태스크 정보
기록 목록에서 미해결 보안 인시던트를 그룹의 다른 분석가에게 재할당합니다. 또는 기록의 상세 정보 및 관련 목록을 보거나 할당하기 전에 작업 메모를 추가합니다. 이 작업 완료 시간: 5-10분.

프로시저

1. 모바일 장치에서 인스턴스에 로그인 ServiceNow AI Platform 하지 않은 경우 문서를 참조하십시오 에 로그인 보안 인시던트 대응 모바일 앱.
2. 보안 인시던트 방문 화면이 표시되면 내 인시던트를 누릅니다.

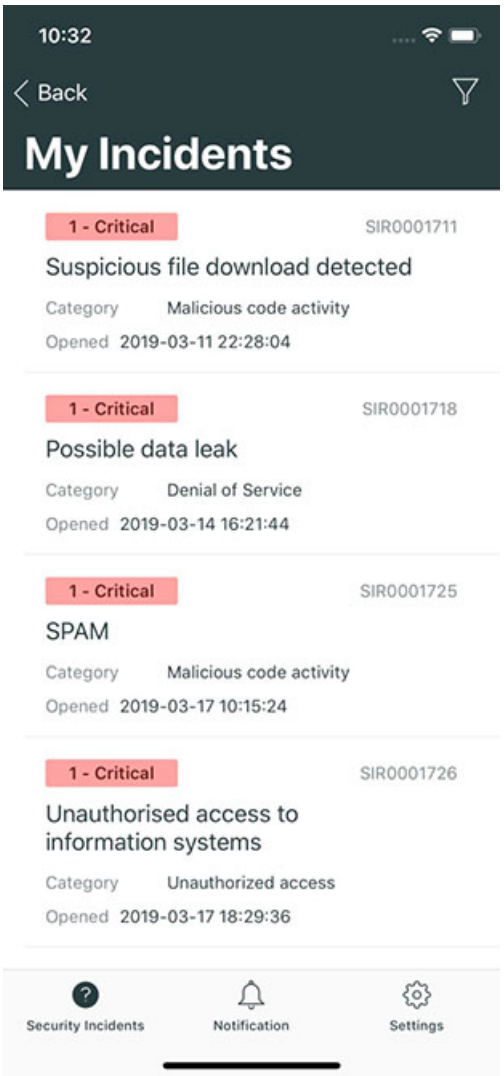
   로그인한 후 다른 보안 인시던트 대응 모바일 앱 곳으로 이동할 경우 언제든지 Now Agent 앱을 탭하여 마지막으로 표시한 화면으로 돌아갈 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



할당된 미해결 보안 인시던트 기록 목록과 함께 내 인시던트 화면이 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

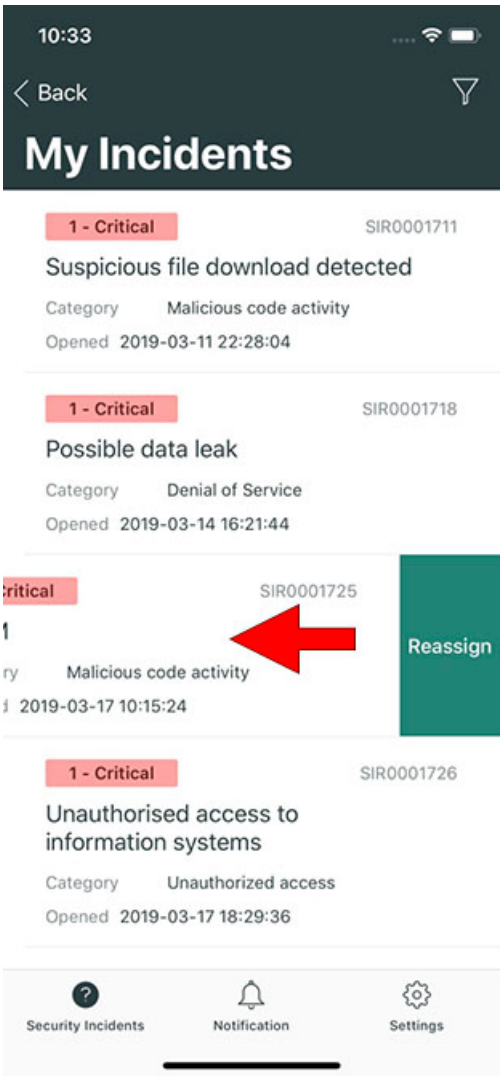


3. 옵션: 를 참조하여 를 사용하여 보안 인시던트 검색 보안 인시던트 대응 모바일 앱 특정 기준과 일치하는 보안 인시던트를 검색합니다.

   또는 필터 아이콘( )이 표시된 상태에서 필터를 설정하여 목록의 기록 수를 제한합니다 . 모바일 앱의 화면에서 기록을 필터링하는 것은 에서 ServiceNow AI Platform조건 작성기로 필터링하는 것과 비슷합니다.

4. 미해결 보안 인시던트 기록 목록이 표시된 상태에서 목록에서 직접 인시던트를 재할당하려면 기록을 왼쪽으로 살짝 밀어 메뉴를 엽니다.

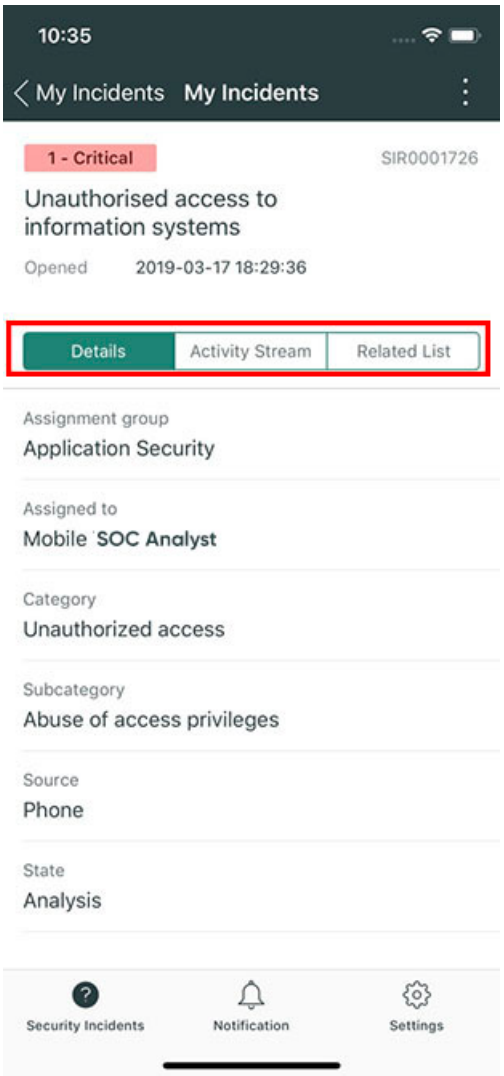
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



5. 표시되는 메뉴에서 할당 그룹 또는 할당 대상 필드를 편집합니다.

6. 또는 미해결 보안 인시던트 기록의 상세 정보를 보려면 내 인시던트 화면이 표시된 상태에서 목록에서 기록을 누릅니다.
7. 표시되는 열린 기록에서 다음 표의 옵션 하나를 선택하여 계속합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



을 사용하여 할당되지 않은 보안 인시던트를 보고, 편집하고, 할당합니다. 보안 인시던트 대응 모바일 앱

모바일 장치에서 미할당 보안 인시던트 응답 (SIR) 인시던트를 보고, 편집하고, 할당합니다. 인시던트에 대한 자세한 내용은 관련 목록과 작업 메모의 감사 추적을 참조하십시오.

시작하기 전에

필요한 역할: sn_si.analyst

이 태스크 정보

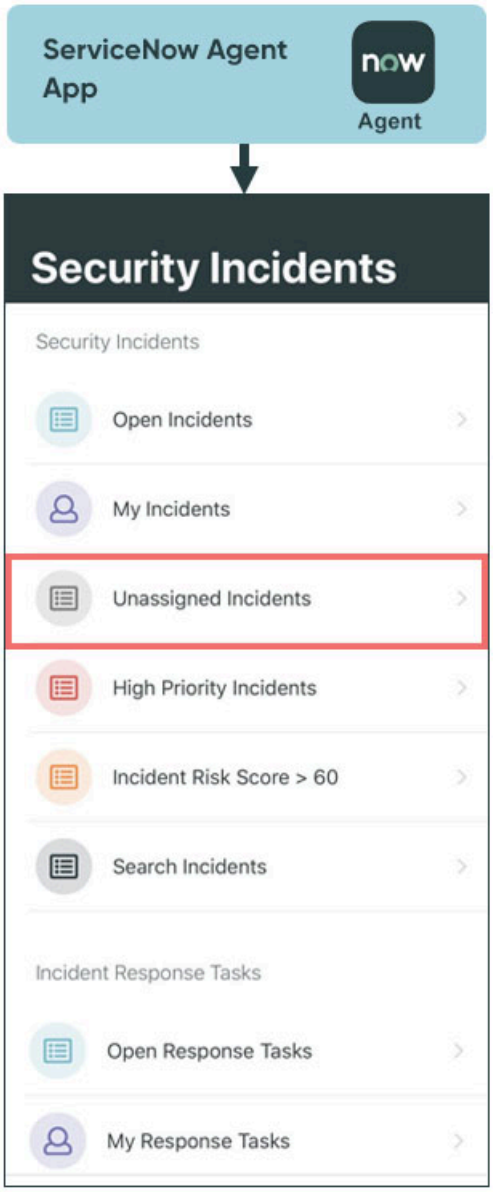
기록 목록에서 할당되지 않은 미해결 보안 인시던트를 본인 또는 그룹의 다른 분석가에게 할당합니다. 또는 기록의 상세 정보 및 관련 목록을 보거나 할당하기 전에 작업 메모를 추가합니다.
이 작업 완료 시간: 5-10분.

프로시저

1. 모바일 장치에서 인스턴스에 로그인 ServiceNow AI Platform 하지 않은 경우, 자세한 내용은 문서를 에 로그인 보안 인시던트 대응 모바일 앱참조하십시오.
2. 보안 인시던트 방문 화면이 표시되면 미할당 인시던트를 누릅니다.

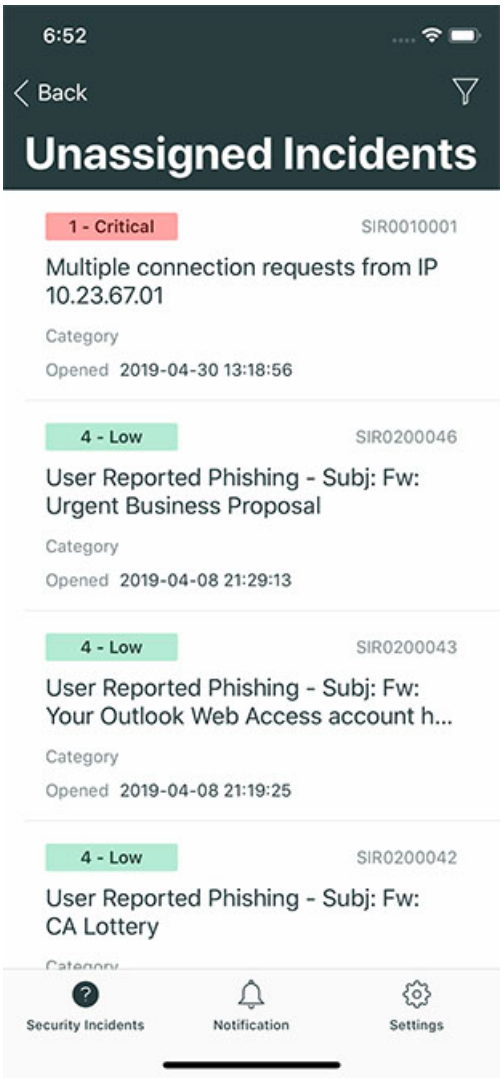
   로그인한 후 다른 보안 인시던트 대응 모바일 앱 곳으로 이동할 경우 언제든지 Now Agent 앱을 탭하여 마지막으로 표시한 화면으로 돌아갈 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



할당되지 않은 보안 인시던트 기록 목록과 함께 할당되지 않은 인시던트 화면이 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

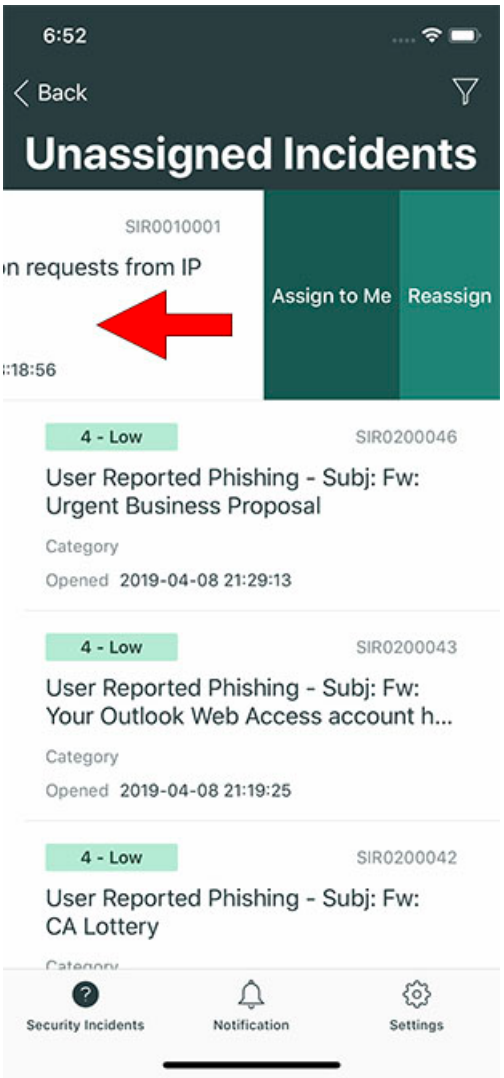


3. 옵션: 를 참조하여 를 사용하여 보안 인시던트 검색 보안 인시던트 대응 모바일 앱 특정 기준과 일치하는 보안 인시던트를 검색합니다.

   또는 필터 아이콘( )이 표시되면 필터를 설정하여 목록의 기록 수를 제한합니다 . 모바일 앱의 화면에서 기록을 필터링하는 것은 에서 ServiceNow AI Platform조건 작성기로 필터링하는 것과 비슷합니다.

4. 미할당된 미해결 보안 인시던트 기록 목록이 표시된 상태에서 미해결 보안 인시던트 기록을 목록에서 직접 할당하거나 재할당하려면 기록을 왼쪽으로 살짝 밀어 메뉴를 엽니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

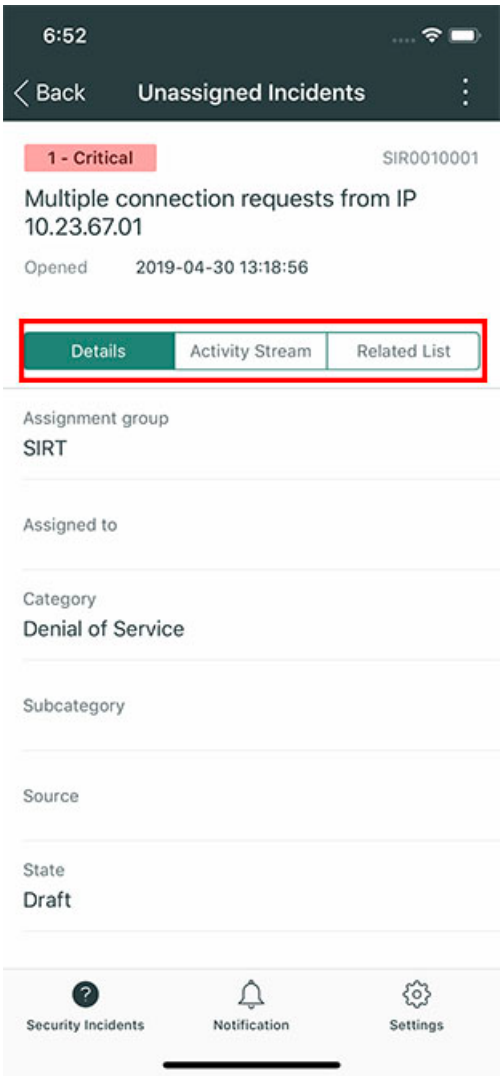


5. 계속하려면 메뉴에서 하나를 선택합니다.

6. 또는 미할당 인시던트 화면이 표시된 상태에서 목록의 기록을 누릅니다.

7. 표시되는 열린 기록에서 다음 표의 옵션 하나를 선택하여 계속합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



를 사용하여 우선순위가 높은 인시던트를 보고, 편집하고, 할당합니다. 보안 인시던트 대응 모바일 앱

모바일 장치에서 우선순위 보안 인시던트 응답 가 높은()SIR 인시던트를 보고, 편집하고, 할당합니다. 인시던트에 대한 자세한 내용은 관련 목록과 작업 메모의 감사 추적을 참조하십시오.

시작하기 전에

필요한 역할: sn_si.analyst

이 태스크 정보

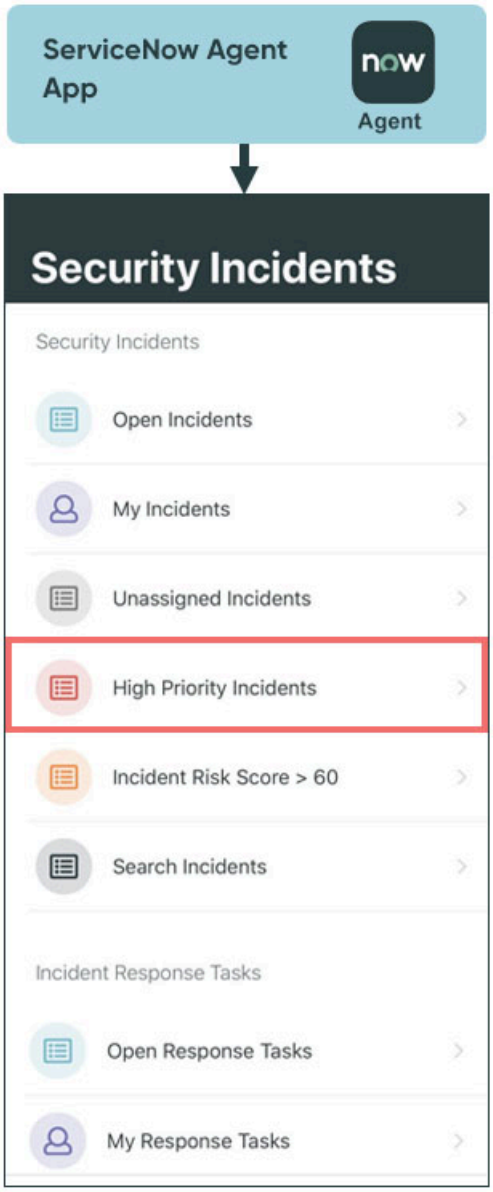
기록 목록에서 미해결된 중요 보안 인시던트를 본인 또는 그룹의 다른 분석가에게 할당합니다. 또는 기록의 상세 정보 및 관련 목록을 보거나 할당하기 전에 작업 메모를 추가합니다. 이 작업 완료 시간: 5-10분.

프로시저

1. 모바일 장치에서 인스턴스에 로그인 ServiceNow AI Platform 하지 않은 경우, 자세한 내용은 문서를 에 로그인 보안 인시던트 대응 모바일 앱참조하십시오.
2. 보안 인시던트 방문 화면이 표시되면 우선순위가 높은 인시던트를 누릅니다.

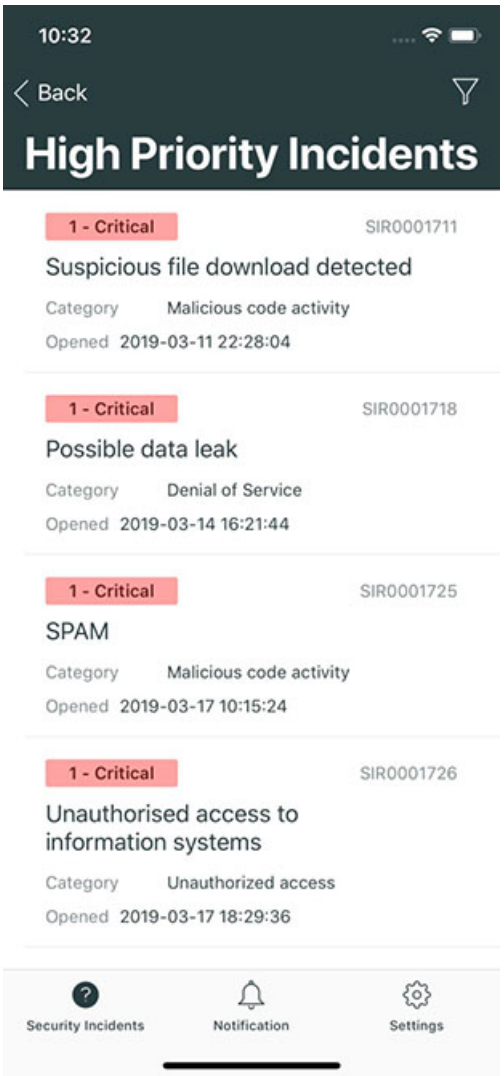
   로그인한 후 다른 보안 인시던트 대응 모바일 앱 곳으로 이동할 경우 언제든지 Now Agent 앱을 탭하여 마지막으로 표시한 화면으로 돌아갈 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



중요(높은 우선순위) 보안 인시던트 목록과 함께 높은 우선순위 인시던트 화면이 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

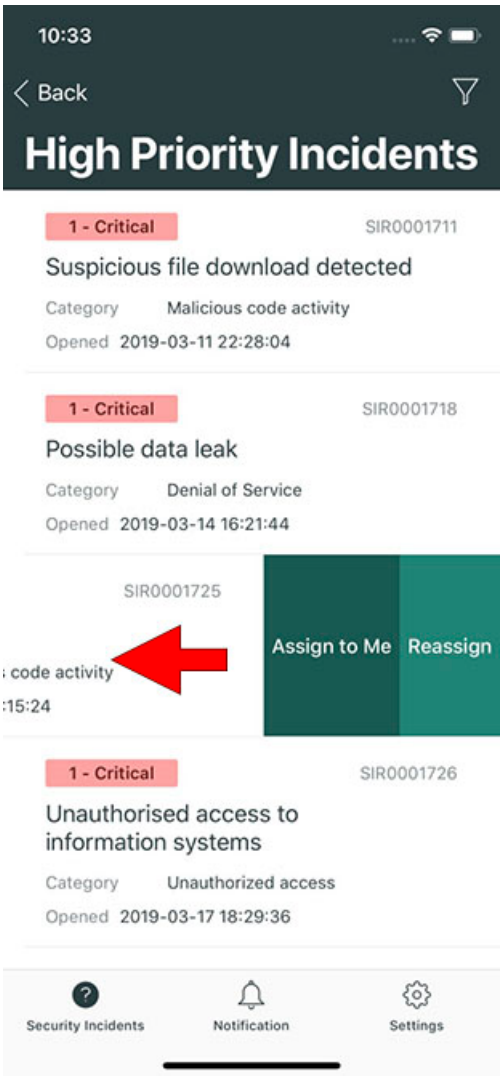


3. 옵션: 를 참조하여 를 사용하여 보안 인시던트 검색 보안 인시던트 대응 모바일 앱 특정 기준과 일치하는 보안 인시던트를 검색합니다.

   또는 필터 아이콘( )이 표시된 상태에서 필터를 설정하여 목록의 기록 수를 제한합니다 . 모바일 앱의 화면에서 기록을 필터링하는 것은 에서 ServiceNow AI Platform조건 작성기로 필터링하는 것과 비슷합니다.

4. 우선순위가 높은 보안 인시던트 기록 열기가 표시되면 기록을 왼쪽으로 살짝 밀어 메뉴를 엽니다.

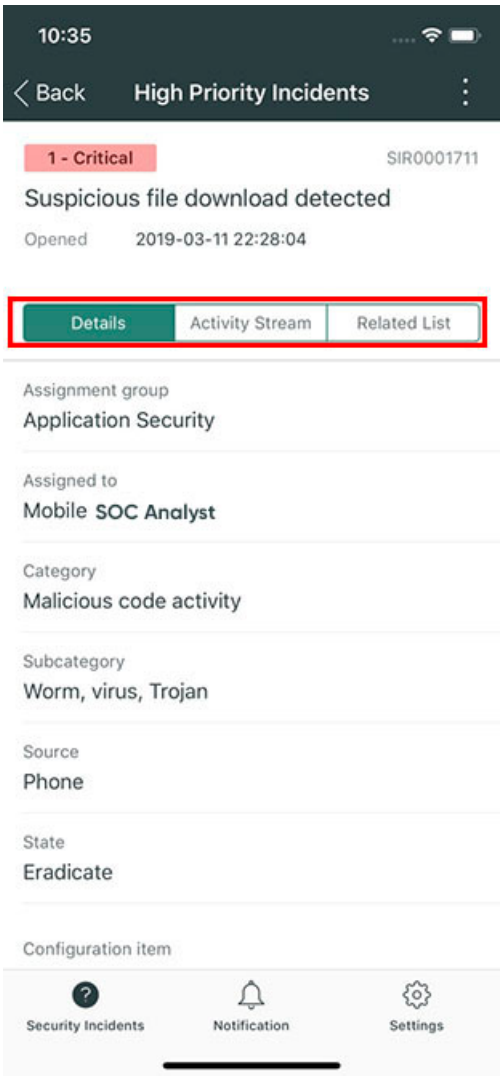
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



5. 계속하려면 하나를 선택합니다.

6. 우선순위가 높은 인시던트 화면이 표시된 상태에서 열린 보안 인시던트 기록의 상세 정보와 더 많은 관련 기록 및 관련 목록을 보려면 목록에서 기록을 누릅니다.
7. 표시되는 열린 기록에서 다음 표의 옵션 하나를 선택하여 계속합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



를 사용하여 위험 점수가 60보다 큰 보안 인시던트를 보고, 편집하고, 할당합니다. 보안 인시던트 대응 모바일 앱

모바일 장치에서 위험 점수 필드 값이 60보다 큰 인시던트를 보고 편집합니다보안 인시던트 응답SIR(). 인시던트에 대한 자세한 내용은 관련 목록과 작업 메모의 감사 추적을 참조하십시오.

시작하기 전에

필요한 역할: sn_si.analyst

이 태스크 정보

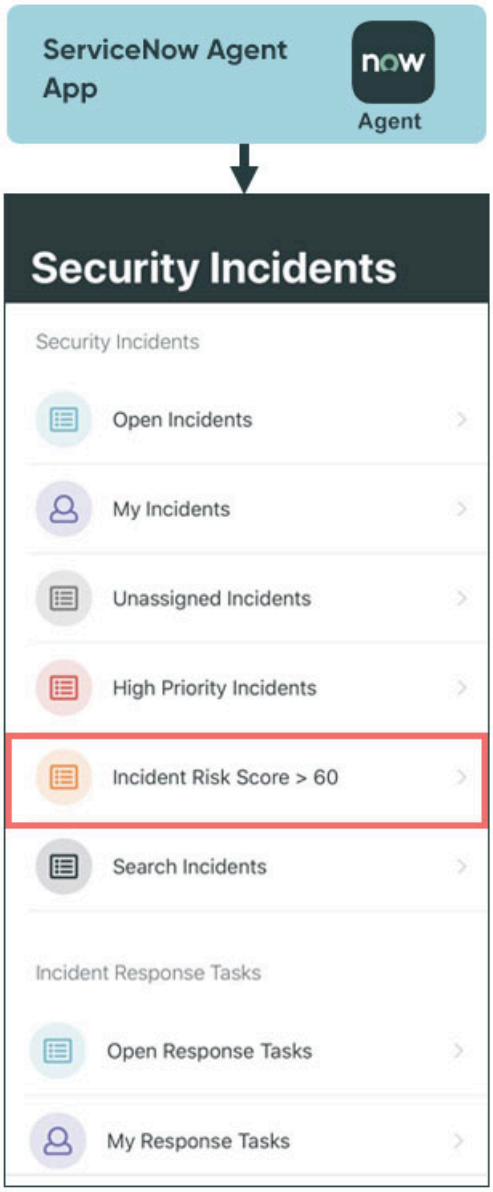
기록 목록에서 위험 점수가 60 이상인 미해결 보안 인시던트를 본인 또는 그룹의 다른 분석가에게 할당합니다. 또는 기록의 상세 정보 및 관련 목록을 보거나 할당하기 전에 작업 메모를 추가합니다. 이 작업 완료 시간: 5-10분.

프로시저

1. 모바일 장치에서 인스턴스에 로그인 ServiceNow AI Platform 하지 않은 경우, 자세한 내용은 문서를 에 로그인 보안 인시던트 대응 모바일 앱참조하십시오.
2. 보안 인시던트 방문 화면이 표시되면 위험 점수 **> 60**을 누릅니다.

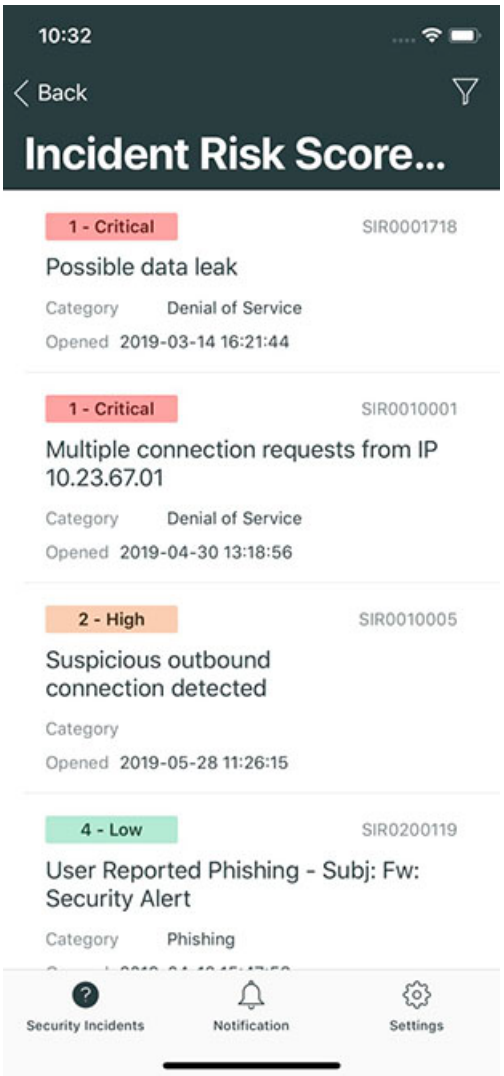
   로그인한 후 다른 보안 인시던트 대응 모바일 앱 곳으로 이동할 경우 언제든지 Now Agent 앱을 탭하여 마지막으로 표시한 화면으로 돌아갈 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



인시던트 위험 점수 화면에 보안 인시던트 목록이 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

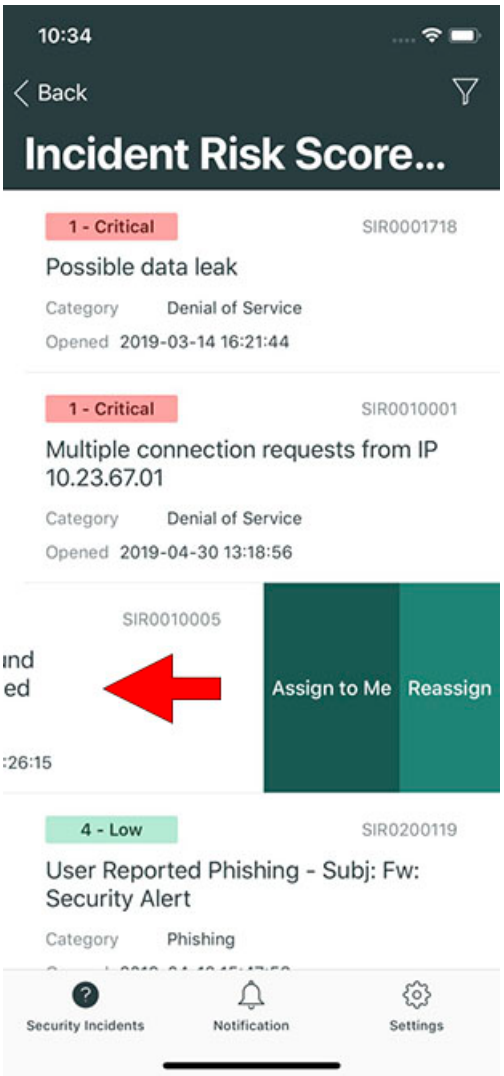


3. 옵션: 를 참조하여 를 사용하여 보안 인시던트 검색 보안 인시던트 대응 모바일 앱 특정 기준과 일치하는 보안 인시던트를 검색합니다.

   또는 필터 아이콘( )이 표시되면 필터를 설정하여 목록의 기록 수를 제한합니다 . 모바일 앱의 화면에서 기록을 필터링하는 것은 에서 ServiceNow AI Platform조건 작성기로 필터링하는 것과 비슷합니다.

4. 보안 인시던트를 자신에게 할당하거나 표시된 오픈 보안 인시던트 기록 목록에서 직접 재할당하려면 기록을 왼쪽으로 살짝 밀어 메뉴를 엽니다.

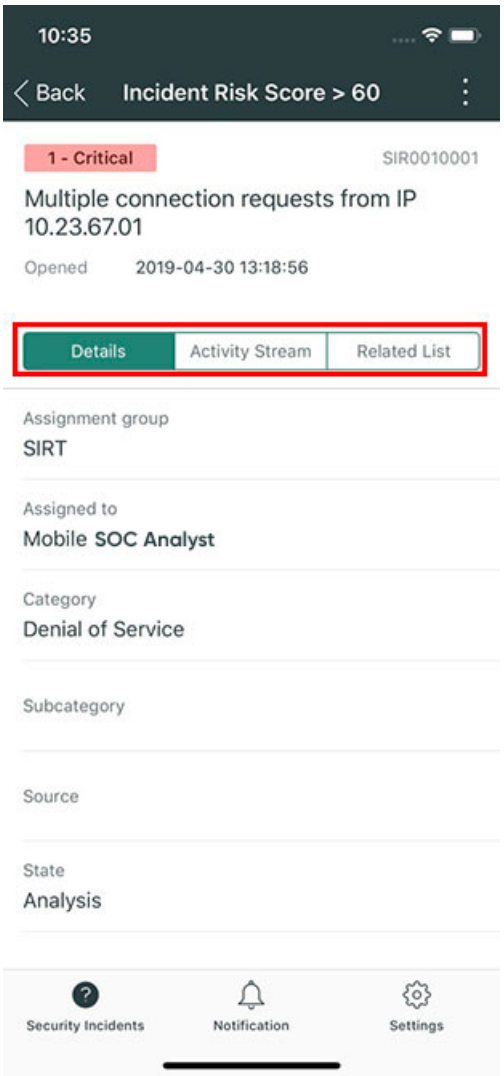
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



5. 계속하려면 하나를 선택합니다.

6. 또는 미해결 보안 인시던트 기록의 상세 정보를 보고 더 많은 관련 기록 및 관련 목록을 보려면 인시던트 위험 점수 화면이 표시된 상태에서 목록의 기록을 누릅니다.
7. 표시되는 열린 기록에서 다음 표의 옵션 하나를 선택하여 계속합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



를 사용하여 보안 인시던트 검색 보안 인시던트 대응 모바일 앱

보안 인시던트 응답 인스턴스에서 (SIR) 보안 인시던트를 ServiceNow AI Platform# 검색합니다. 입력한 특정 검색 조건과 일치하는 인시던트만 표시됩니다.

시작하기 전에
필요한 역할: sn_si.analyst

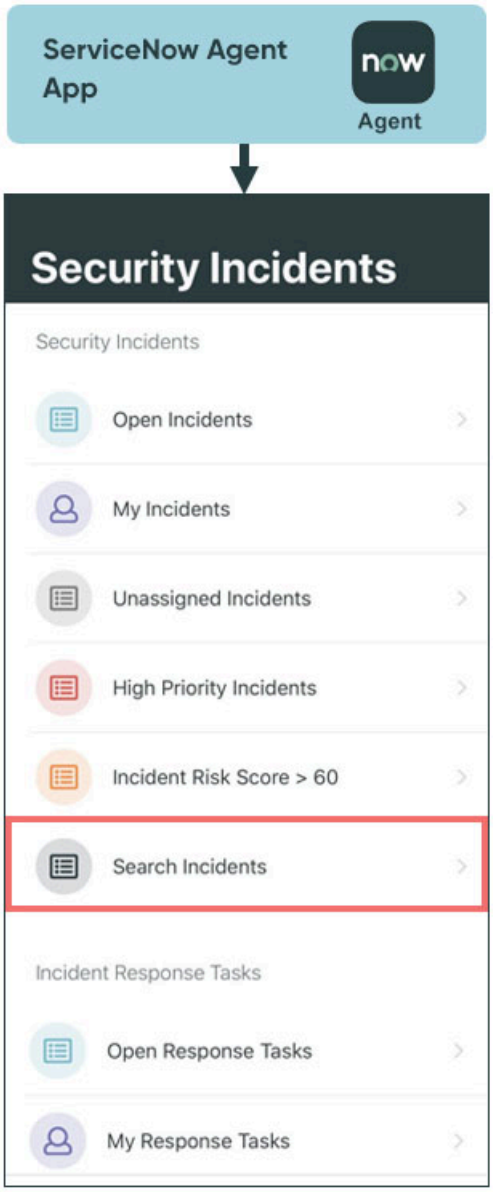
이 태스크 정보
이 작업 완료 시간: 5-10분.

프로시저

1. 모바일 장치에서 인스턴스에 로그인 ServiceNow AI Platform 하지 않은 경우, 자세한 내용은 문서를 에 로그인 보안 인시던트 대응 모바일 앱참조하십시오.
2. 보안 인시던트 방문 화면이 표시되면 인시던트 검색을 누릅니다.

   로그인한 후 다른 보안 인시던트 대응 모바일 앱 곳으로 이동할 경우 언제든지 Now Agent를 탭하여 마지막으로 표시한 화면으로 돌아갈 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



3. 반환되는 검색 결과 수를 제한하려면 양식에서 가능한 한 많은 필드를 채우는 것이 좋습니다. 검색 조건을 추가하려면 다음 테이블을 참조하십시오. 표 뒤의 지침에 따라 기존 검색 기준을 편집하거나, 검색 기준을 지우거나, 검색을 제출합니다.

이 필드 누르기	장치에 항목을 Android 추가하려면	장치에 추가하고 입력 iOS 하려면
번호	보안 인시던트의 영숫자 값(예: SIR0010004)을 입력합니다. 이 번호는 보안 인시던트의 오른쪽 상단에 표시됩니다. 이 기능은 숫자 문자열과 부분 숫자 문자열을 검색합니다. 더 세분화된 검색을 보려면 더 많은 숫자를 입력합니다. 와일드카드(*)는 허용되지 않습니다.	보안 인시던트의 영숫자 값(예: SIR0010004)을 입력합니다. 이 번호는 보안 인시던트의 오른쪽 상단에 표시됩니다. 이 기능은 숫자 문자열과 부분 숫자 문자열을 검색합니다. 더 세분화된 검색을 보려면 더 많은 숫자를 입력합니다. 와일드카드(*)는 허용되지 않습니다. 새 필드를 눌러 더 많은 기준을 입력하거나

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 필드 누르기	장치에 항목을 Android 추가하려면	장치에 추가하고 입력 iOS 하려면
	새 필드를 눌러 추가 기준을 입력하거나 검색을 제출합니다.	검색을 제출하려면 검색을 제출합니다.
간단한 설명	필드에 텍스트(예: ###)를 입력합니다. 이 기능은 간단한 설명 필드에서 텍스트 문자열과 부분 텍스트 문자열을 검색합니다. 더 세분화된 검색을 보려면 더 많은 텍스트를 입력합니다. 와일드카드(*)는 허용되지 않습니다. 새 필드를 눌러 추가 기준을 입력하거나 검색을 제출합니다.	필드에 텍스트(예: ###)를 입력합니다. 이 기능은 간단한 설명 필드에서 텍스트 문자열과 부분 텍스트 문자열을 검색합니다. 더 세분화된 검색을 보려면 더 많은 텍스트를 입력합니다. 와일드카드(*)는 허용되지 않습니다. 새 필드를 눌러 더 많은 기준을 입력하거나 검색을 제출하려면 검색을 제출합니다.
우선순위	항목을 추가하려면 하나 이상의 항목을 탭하거나 검색 아이콘을 누르고 검색 필드에 항목을 입력합니다. 확인 표시 아이콘을 눌러 인시던트 검색 화면으로 돌아갑니다.	항목을 추가하려면 하나 이상의 항목을 탭하거나 검색 아이콘을 누르고 검색 필드에 항목을 입력합니다. 완료를 눌러 인시던트 검색 화면으로 돌아갑니다.
범주	항목을 추가하려면 하나 이상의 항목을 탭하거나 검색 아이콘을 누르고 검색 필드에 항목을 입력합니다. 확인 표시 아이콘을 눌러 인시던트 검색 화면으로 돌아갑니다.	항목을 추가하려면 하나 이상의 항목을 탭하거나 검색 아이콘을 누르고 검색 필드에 항목을 입력합니다. 완료를 눌러 인시던트 검색 화면으로 돌아갑니다.
상태	항목을 추가하려면 하나 이상의 항목을 탭하거나 검색 아이콘을 누르고 검색 필드에 항목을 입력합니다. 확인 표시 아이콘을 눌러 인시던트 검색 화면으로 돌아갑니다.	항목을 추가하려면 하나 이상의 항목을 탭하거나 검색 아이콘을 누르고 검색 필드에 항목을 입력합니다. 완료를 눌러 인시던트 검색 화면으로 돌아갑니다.
담당자	목록에서 하나를 선택하거나 검색 아이콘을 누르고 검색 필드에 항목을 입력합니다. 할당 그룹 및 할당 대상 필드의 값을 지우려면 항목 없음에 대해 없음을 선택합니다.	목록에서 하나를 선택하거나 검색 아이콘을 누르고 검색 필드에 항목을 입력합니다. 할당 그룹 및 할당 대상 필드의 값을 지우려면 항목 없음에 대해 없음을 선택합니다.
할당 그룹	목록에서 하나를 선택하거나 검색 아이콘을 누르고 검색 필드에 항목을 입력합니다.	목록에서 하나를 선택하거나 검색 아이콘을 누르고 검색 필드에 항목을 입력합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 필드 누르기	장치에 항목을 Android 추가하려면	장치에 추가하고 입력 iOS 하려면
	할당 그룹 및 할당 대상 필드의 값을 지우려면 항목 없음에 대해 없음을 선택합니다.	할당 그룹 및 할당 대상 필드의 값을 지우려면 항목 없음에 대해 없음을 선택합니다.

장치의 경우 Android 인시던트 검색 화면이 표시되고 모든 조건을 입력한 상태에서 하나를 선택하여 계속합니다.

4. 장치의 경우 iOS 인시던트 검색 화면이 표시되면 화면을 선택하여 계속합니다.

5. 옵션: 검색에서 여러 레코드를 반환하는 경우 검색 결과를 세분화할 수 있습니다 를 사용하여 기록 필터링 보안 인시던트 대응 모바일 앱 .

를 사용하여 미해결 응답 작업을 보고, 편집하고, 할당합니다. 보안 인시던트 대응 모바일 앱

미해결 응답 작업을 보고, 편집하고, 할당합니다. 변경 내용은 상위 보안 인시던트의 보안 인시던트 응답 작업에 저장됩니다.

시작하기 전에
필요한 역할: sn_si.analyst

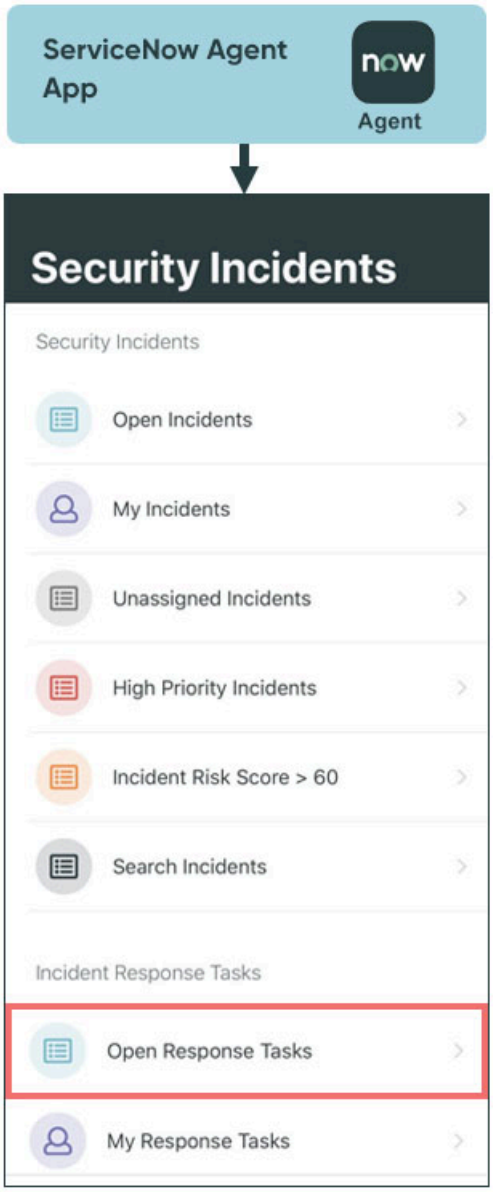
이 태스크 정보
기록 목록에서 할당되지 않은 미해결 응답 작업을 사용자 자신 또는 그룹의 다른 분석가에게 할당합니다. 또는 기록의 상세 정보를 보거나 할당하기 전에 작업 메모를 추가합니다. 이 작업 완료 시간: 5-10분.

프로시저

1. 모바일 장치에서 인스턴스에 로그인 ServiceNow AI Platform 하지 않은 경우, 자세한 내용은 문서를 에 로그인 보안 인시던트 대응 모바일 앱참조하십시오.
2. 보안 인시던트 방문 화면이 표시되면 응답 작업 열기를 누릅니다.

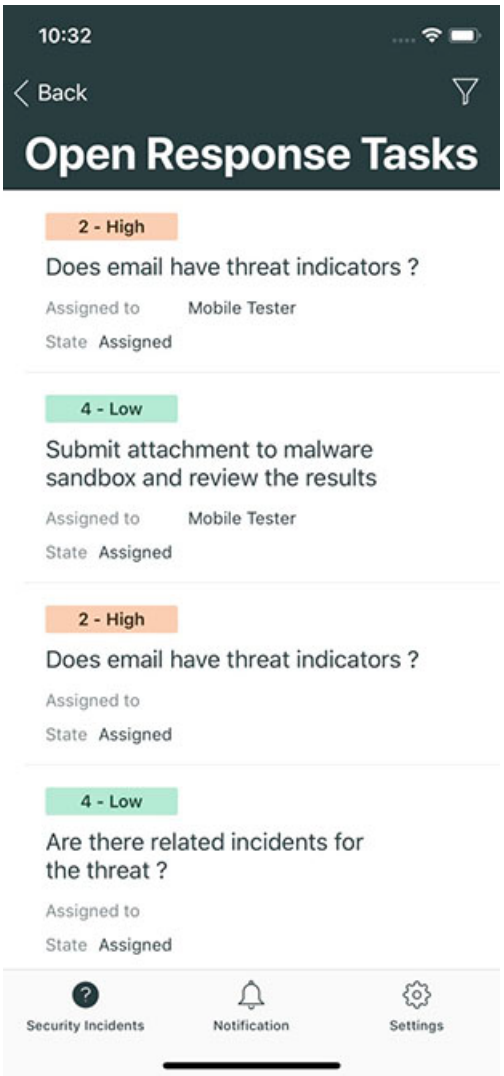
   로그인한 후 다른 보안 인시던트 대응 모바일 앱 곳으로 이동할 경우 언제든지 Now Agent 앱을 탭하여 마지막으로 표시한 화면으로 돌아갈 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



열린 응답 작업 화면에 열린 작업 목록이 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

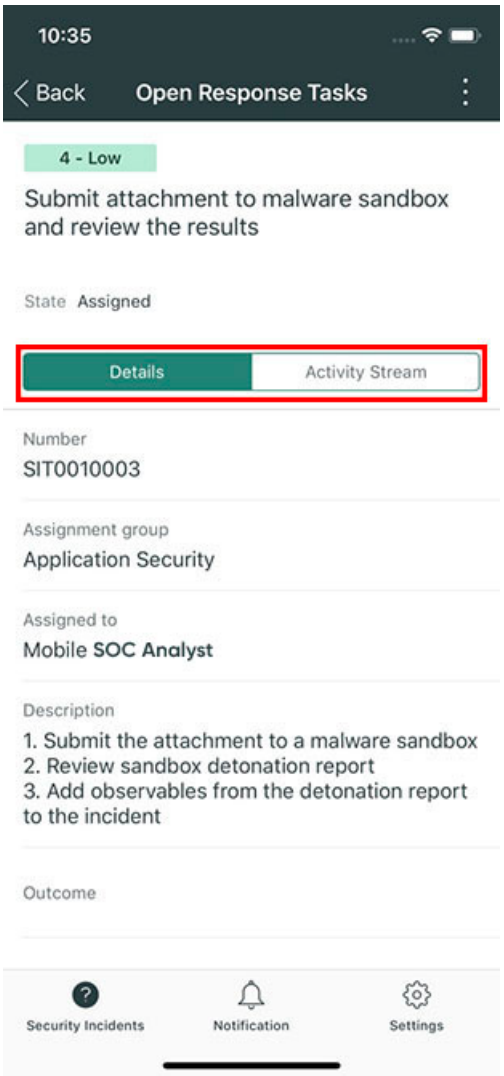


3. 옵션: 특정 기준과 일치하는 작업을 검색하려면 참조하십시오 를 사용하여 보안 인시던트 검색 보안 인시던트 대응 모바일 앱 .

   또는 필터 아이콘( )이 표시되면 필터를 설정하여 목록의 기록 수를 제한합니다 . 모바일 앱의 화면에서 기록을 필터링하는 것은 에서 ServiceNow AI Platform조건 작성기로 필터링하는 것과 비슷합니다.

4. 열린 응답 작업 목록이 표시된 상태에서 목록에서 직접 할당하거나 재할당하려면 기록을 왼쪽으로 밀어 메뉴를 엽니다.
5. 계속하려면 하나를 선택합니다.
6. 또는 오픈 응답 작업 기록의 상세 정보를 보려면 오픈 응답 작업 화면이 표시된 상태에서 목록에서 기록을 누릅니다.
7. 응답 작업 기록의 탭이 표시된 상태에서 다음 표에서 하나를 선택하여 계속합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



를 사용하여 응답 작업 보기, 편집 및 재할당 보안 인시던트 대응 모바일 앱

자신에게 할당된 응답 작업을 보고, 편집하고, 재할당합니다. 변경 내용은 상위 보안 인시던트의 보안 인시던트 응답 작업에 저장됩니다.

시작하기 전에
필요한 역할: sn_si.analyst

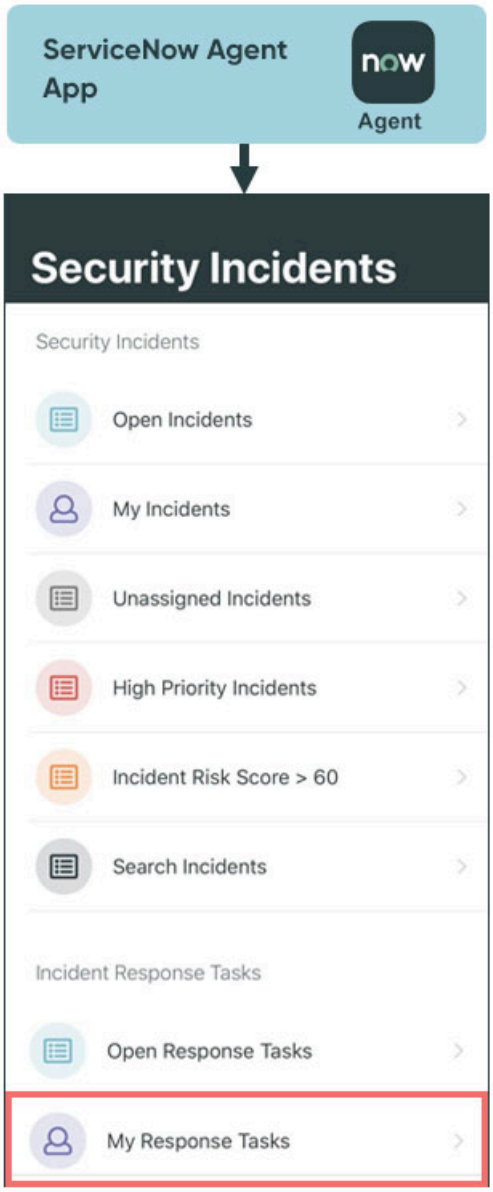
이 태스크 정보
기록 목록에서 본인에게 할당된 미해결 응답 작업을 그룹의 다른 분석가에게 재할당합니다. 또는 재할당하기 전에 기록의 상세 정보를 보거나 작업 메모를 추가합니다. 이 작업 완료 시간: 5-10분.

프로시저

1. 모바일 장치에서 인스턴스에 로그인 ServiceNow AI Platform 하지 않은 경우, 자세한 내용은 문서를 에 로그인 보안 인시던트 대응 모바일 앱참조하십시오.
2. 보안 인시던트 방문 화면이 표시되면 내 응답 작업을 누릅니다.

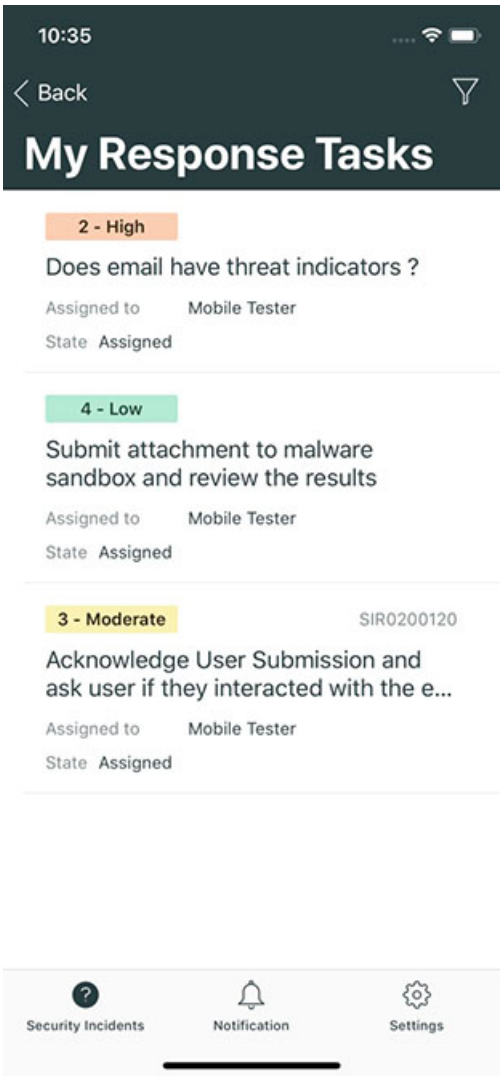
   로그인한 후 다른 보안 인시던트 대응 모바일 앱 곳으로 이동할 경우 언제든지 Now Agent(이행자) 앱을 탭하여 마지막으로 표시한 화면으로 돌아갈 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



할당된 응답 작업 목록과 함께 내 응답 작업 화면이 표시됩니다.

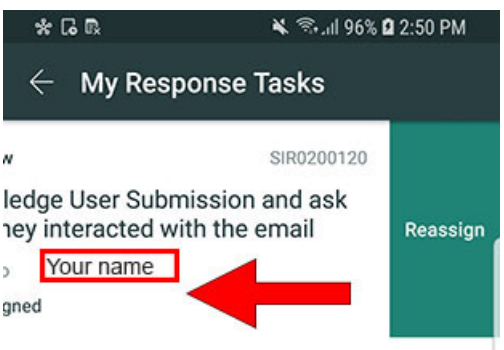
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



3. 옵션: 특정 기준과 일치하는 작업을 검색하려면 참조하십시오 를 사용하여 보안 인시던트 검색 보안 인시던트 대응 모바일 앱 .

   또는 필터 아이콘( )이 표시된 상태에서 필터를 설정하여 목록의 기록 수를 제한합니다 . 모바일 앱의 화면에서 기록을 필터링하는 것은 에서 ServiceNow AI Platform조건 작성기로 필터링하는 것과 비슷합니다.

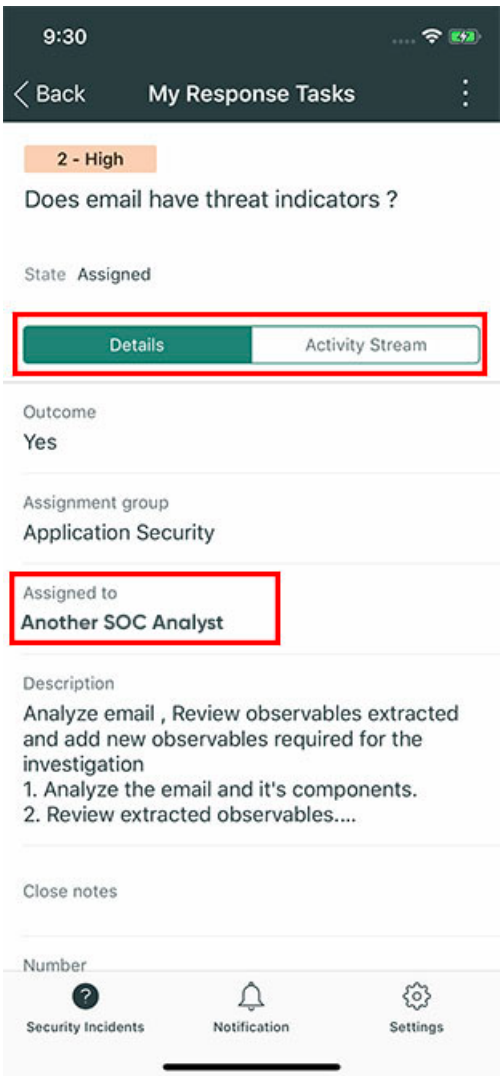
4. 자신에게 할당된 작업 기록 목록에서 직접 작업을 재할당하려면 기록을 왼쪽으로 살짝 밀어 메뉴를 엽니다.



5. 재할당을 탭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

6. 응답 작업을 다른 사람에게 할당 화면이 표시되면 필드를 눌러 확장하고 작업에 사용할 다른 그룹 또는 사용자를 선택합니다.
7. 보내기 아이콘( ) 또는 제출 을 눌러 변경 내용을 저장하고 응답 작업을 업데이트합니다. 기록이 업데이트되었음을 확인하는 메시지가 표시됩니다. 작업이 상위 보안 인시던트의 새 사용자에게 할당되고 ServiceNow AI Platform 인스턴스가 업데이트됩니다.
8. 열린 응답 작업의 상세 정보를 보고 작업 메모를 보려면 내 응답 작업 화면이 표시된 상태에서 목록에서 기록을 누릅니다.
9. 응답 작업의 필드가 표시된 상태에서 다음 표에서 하나를 선택하여 계속합니다.



를 사용하여 기록 필터링 보안 인시던트 대응 모바일 앱

화면에 표시되는 기록 수를 제한하려면 추가 필터를 설정합니다. 모바일 앱에서 기록을 필터링하는 것은 ServiceNow AI Platform에서 조건 작성기로 필터링하는 것과 비슷합니다.

시작하기 전에
필요한 역할: sn_si.analyst

이 태스크 정보
작업 완료 시간: 5분.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 검색 결과를 더 구체화하거나 표시되는 레코드 목록에 추가 필터 조건을 입력하려면 필터 아이콘( )을 누릅니다.
2. 필터 화면이 표시되면 필드를 눌러 확장합니다.
3. 표시되는 옵션에서 확인란을 누르거나 필터의 항목을 누릅니다.
   많은 필터가 여러 옵션을 선택할 수 있습니다.
4. 뒤로 화살표(Back.) 또는 완료 를 눌러 필드에 대한 변경 내용을 저장합니다.
   선택한 기준이 필터 화면에 표시됩니다. 조건과 일치하는 기록 수도 화면 위쪽에 표시됩니다.
   재설정을 눌러 필터를 제거하고 기본 설정을 복원합니다.
5. 옵션: 필터 화면이 표시된 상태로 1-4단계를 반복하여 필터 조건을 계속 설정합니다.
6. 눌러 AND 조건을 만듭니다.
   또는 OR 조건을 생성합니다.
7. 원하는 조건을 모두 추가한 후 필터 화면이 표시되면 완료를 누릅니다.
   화면에는 필터 조건과 일치하는 기록만 표시됩니다.

보안 인시던트 응답 오케스트레이션

보안 인시던트 응답 오케스트레이션 활동을 통해 사용자는 워크플로우 오케스트레이션을 사용하여 Windows 또는 UNIX 기반 시스템 및 환경과 상호작용하고 이 환경에서 데이터를 검색할 수 있습니다.

설정

를 사용하기 보안 인시던트 응답 오케스트레이션전에 CMDB 채우기, MID Server 구성 및 자격 증명 구성을 포함하여 시스템의 다양한 부분을 설정하는 단계를 수행합니다.

시작하기 전에

필요한 역할: 관리자

를 사용하려면 보안 인시던트 응답도메인 이름으로 완전히 채워진 CMDB가 필요합니다. 자세한 내용은 다음을 참조하십시오. 디스커버리 .

이 태스크 정보

프로시저

1. 플러그인 활성화 보안 인시던트 응답 .
2. MID Server 구성 .
3. Windows MID 서버 서비스 자격 증명을 구성합니다 .

보안 인시던트 응답 오케스트레이션 워크플로우 및 워크플로우 템플릿 이해

기본 시스템에는 보안 인시던트 기록과 함께 작동하도록 설계된 일련의 워크플로우 및 워크플로우 템플릿이 보안 인시던트 응답 포함되어 있습니다.

시작하기 전에

필요한 역할: sn_si.basic

이 태스크 정보

적절한 역할(sn_sec_cmn.admin)이 있다고 가정하여 모든 워크플로우와 워크플로우 템플릿을 필요에 더 잘 맞게 조정할 수 있습니다. 워크플로우는 Security Operations System 전체에서 다양한 작업을 수행하는 데 사용됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

그러나 워크플로우 템플릿은 보안 인시던트의 범주 필드에서 값을 선택하여 트리거됩니다. 이 경우 선택 항목과 연결된 워크플로 템플릿은 보안 분석가에게 특정 유형의 위협을 처리하는 방법을 지시하는 워크플로 템플릿을 시작합니다.

예를 들어 보안 인시던트의 범주 필드에서 서비스 거부를 선택하면 보안 인시던트 - DoS(서비스 거부) - 템플릿이 실행되고 분석가는 DOS의 대상이 비즈니스에 중요한지 여부를 결정하도록 지시됩니다. 이 경우 다음 작업으로 인해 보안 인시던트의 우선순위가 **1** - 중요로 설정된 후 다음 작업이 실행됩니다. 등등.

따라서 보안 인시던트 응답 워크플로우와 워크플로우 템플릿은 보안 인시던트 내의 특정 기능 집합에 사용되는 것을 제외하고는 본질적으로 동일합니다.

프로시저

1. 다음으로 이동 모두 〉 보안 운영 〉 워크플로우 〉 보안 워크플로우 보기.
2. 기본 시스템에 제공된 워크플로우 및 워크플로우 템플릿 목록이 표시됩니다.
   애플리케이션 제품군에서 보안 운영 생성한 새 워크플로우도 목록에 포함됩니다.
3. 보려는 워크플로우 또는 워크플로우 템플릿의 이름을 클릭합니다.

> **주:**
> 워크플로우는 여러 가지 방법으로 트리거할 수 있습니다. 워크플로우를 워크플로우 트리거와 연결한다고 해서 반드시 워크플로우가 활성 상태인 것은 아닙니다.

보안 인시던트 응답 오케스트레이션 워크플로우 및 활동

에는 보안 인시던트 응답 오케스트레이션여러 워크플로우와 활동이 포함됩니다.

sn_sec_cmn.admin 역할을 가진 사용자만 수행할 수 있습니다. 워크플로우 편집기 입니다.

IoC 변경에 대한 조회 요청 생성 워크플로우

보안 인시던트 대응 - **IoC** 변경에 대한 조회 요청 생성 플로우는 IoC가 추가되거나 변경되면 자동으로 실행되는 비즈니스 규칙에 의해 트리거됩니다. 맬웨어 검사는 새 데이터를 입력하고 새 데이터만 검사할 때만 트리거됩니다.

시작하기 전에
필요한 역할: sn_si.basic

이 태스크 정보
IoC가 비어 있으면 워크플로가 실행되지 않습니다. 이력 스캔은 유지되며 보안 스캔 요청 탭과 보안 인시던트의 작업 메모에서 볼 수 있습니다. 기존 보안 인시던트가 자동으로 업데이트됩니다.

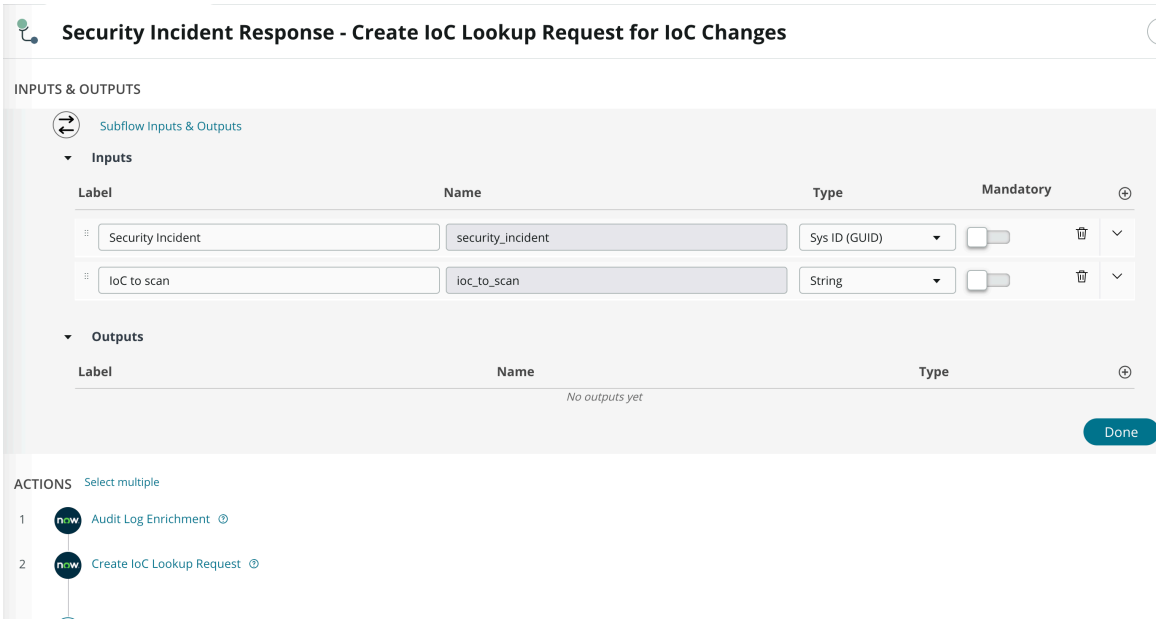
> **중요사항:**
>
> 보안 인시던트 응답 - **IoC** 변경에 대한 조회 요청 생성 워크플로우가 플로우 디자이너로 마이그레이션됩니다. 플로우는 sn_ti_scanner에 기록이 하나 이상 있는 경우에만 트리거됩니다.

Flow Designer 작업에는 다음이 포함됩니다.

- 감사 로그 보강
- IoC 조회 요청 활동 생성

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

IoC 변경 워크플로우



IoC 조회 요청 활동 생성

IoC 조회 요청 만들기 활동은 추가 또는 수정된 IoC 필드에 대한 맬웨어 조회 요청을 만드는 모든 워크플로우와 함께 사용할 수 있습니다.

결과

이 활동의 가능한 결과는 다음과 같습니다.

결과

결과	설명
성공	조회 요청이 작성되었습니다.
실패	조회 요청이 작성되지 않았습니다.

입력 변수

변수	설명
ioc문자열	JSON 형식의 IoC 정보입니다. IP, 해시, URL.
sild	보안 인시던트 시스템 식별자

출력 변수

출력 변수에는 후속 활동에 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
scnReqID	조회 요청 식별자

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 인시던트 응답 - 네트워크 통계 플로우 가져오기

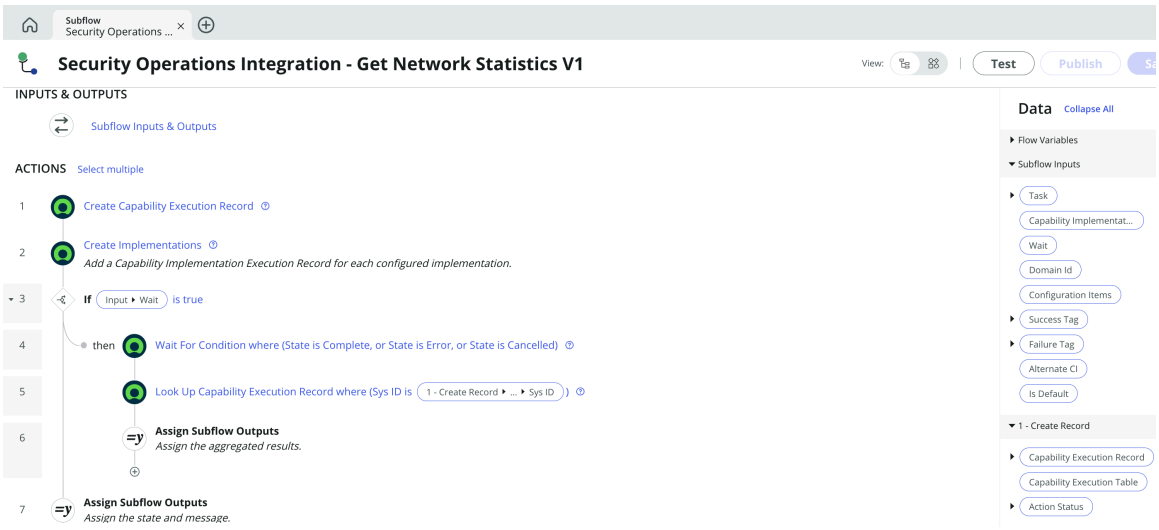
는 보안 인시던트 응답 〉 네트워크 통계 가져오기 플로우는 분석 상태의 보안 인시던트에 추가될 때 영향을 받는 Windows 기반 자원에 대한 네트워크 통계를 검색합니다.

시작하기 전에
필요한 역할: sn_si.analyst

이 태스크 정보
구성 항목이 포함된 새 보안 인시던트의 경우 상태가 분석으로 변경되면 플로우가 자동으로 실행됩니다.

기존 보안 인시던트는 분석 상태에서 새 구성 항목을 추가하면 자동으로 업데이트됩니다.

네트워크 통계 가져오기



플로우 프로세스 작업에는 다음이 포함됩니다.

구성 항목 FQDN 가져오기 플로우 작업

OS별 셸 스크립트 결정

Powershell에서 문을 실행하는 경우

실행 추적 - 플로우 작업 시작

netstat 플로우 작업을 통해 네트워크 통계 가져오기

역량 실행 추적 - 실패 플로우 작업

보강 데이터 기록 플로우 작업 생성

역량 실행 추적 - 실패 플로우 작업 - 보강 ID를 반환합니다.

역량 실행 추적 - 플로우 작업 완료

프로시저

1. 보안 인시던트를 엽니다.
2. 필요한 경우 상태를분석으로 업데이트합니다.
3. 구성 항목(컴퓨터, 서버 또는 이와 유사한 항목)을 추가합니다.
4. 업데이트를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 인시던트 응답 오케스트레이션 에서 네트워크 통계 정보를 제공합니다. 관련 링크 〉 보안 인시던트 보강 탭. 자세한 내용은 보안 운영 보강 데이터 매핑 문서를 참조하십시오.

이 플로우와 관련된 작업은 여기에 설명되어 있습니다. 다른 작업에 대한 자세한 내용은 다음 문서를 참조하십시오 일반 Security Operations 통합 플로우 및 오케스트레이션 활동.

보안 인시던트 대응 - 실행 중인 서비스 가져오기 워크플로우

보안 인시던트 대응 - 실행 중인 서비스 가져오기 워크플로우는 Windows 기반의 ServiceNow구성 항목(CI)에서 실행 중인 서비스 목록을 검색합니다. 이 워크플로우는 조사 진행 중에 인시던트를 향상하기 위해 사용됩니다.

시작하기 전에

필요한 역할: sn_si.analyst

이 태스크 정보

상태가 분석으로 변경된 후 Windows 보안 인시던트에 새 구성 항목을 추가하면 보안 인시던트 대응 - 실행 중인 서비스 가져오기 워크플로우가 자동으로 실행됩니다. 이 워크플로우에서 얻은 정보는 보안 인시던트의 보강 데이터 표시 탭에 나타납니다.

> **주:**
> 보안 인시던트가 초안 상태로 유지되면 보안 인시던트 대응 - 실행 중인 서비스 가져오기 워크플로우 가 실행되지 않습니다.

워크플로우 활동에는 다음이 포함됩니다.

감사 로그 보강 스크립트 활동

구성 항목 FQDN 가져오기 플로우 작업

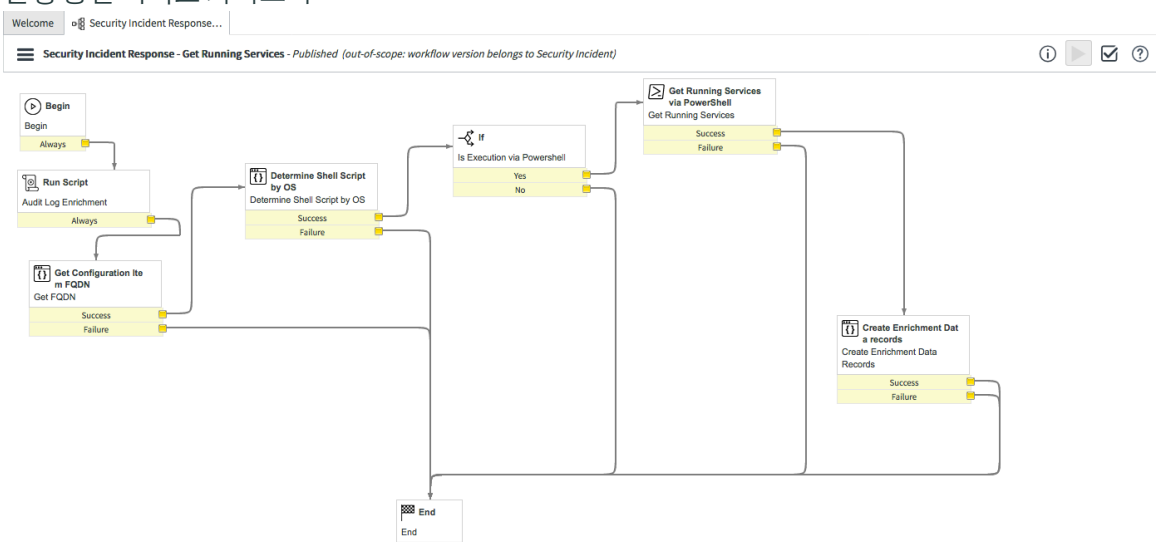
OS 활동별 셸 스크립트 결정

PowerShell 활동을 통한 실행 여부

실행 중인 서비스 가져오기 - WMI 보강 활동

보강 데이터 기록 플로우 작업 생성

실행 중인 서비스 가져오기



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 보안 인시던트를 엽니다.
2. 필요한 경우 상태를분석으로 업데이트합니다.
3. Windows 기반 구성 항목(서버, 랩톱 또는 이와 유사한 항목)을 추가합니다.
4. 업데이트를 클릭합니다.
   보안 인시던트 응답 에서 실행 중인 서비스 정보를 제공합니다. 관련 링크 〉 보안 인시던트 보강탭.
   자세한 내용은 보안 운영 보강 데이터 매핑 문서를 참조하십시오.

OS 활동별 셸 스크립트 결정

OS별 셸 스크립트 결정 워크플로우 활동은 워크플로우에서 사용할 운영 체제를 결정합니다

OS별 셸 스크립트 결정 활동은 구성 항목이 포함된 시스템에서 실행 중인 운영 체제에 따라 실행할 셸 스크립트를 결정하기 위해 모든 워크플로우와 함께 사용할 수 있습니다.

결과

이 활동의 가능한 결과는 다음과 같습니다.

결과

결과	설명
성공	운영 체제를 찾았습니다.
실패	운영 체제를 찾을 수 없습니다. 자세한 오류 정보는 활동 출력 오류에서 확인할 수 있습니다.

입력 변수

입력 변수는 활동의 초기 동작을 결정합니다.

변수	설명
ciSysId	구성 항목의 시스템 식별자입니다.
processType	테이블에서 끌어올 스크립트를 정의하는 내부 식별자입니다.

출력 변수

출력 변수에는 후속 활동에 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
프로세스 스크립트	실행 중인 프로세스를 수집하는 ECC 에이전트입니다.
executionTemplate	스크립트가 프로브를 통해 실행되는지 또는 PowerShell을 사용하는지 여부를 결정합니다.
enrichmentMappingId	응답 데이터를 변환하는 데 사용되는 보강 매핑의 시스템 식별자입니다.

실행 중인 서비스 가져오기 - WMI 보강

보안 인시던트 대응 - 실행 중인 서비스 가져오기 워크플로우는 보안 인시던트에 추가된 구성 항목에서 실행 중인 서비스를 수집합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

실행 중인 서비스 가져오기 - **WMI** 보강 활동은 Windows 호스트에 대해 실행 중인 서비스 정보를 검색하기 위해 자동으로 시작됩니다.

입력 변수

입력 변수는 활동의 초기 동작을 결정합니다.

입력 변수

변수	설명
대상 〔string〕	대상 시스템의 FQDN(정규화된 도메인 이름)입니다.

출력 변수

출력 변수에는 후속 활동에 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
응답 〔string〕	대상 시스템에서 현재 실행 중인 서비스를 나타내는 JSON 문자열입니다. JSON 데이터에는 다음이 포함됩니다. 이름 서비스의 이름 pid 실행 중인 서비스의 프로세스 식별자 service_type (선택 사항) 실행 중인 서비스의 유형입니다. start_name 서비스의 시스템 이름 path 실행 중인 서비스의 실행 파일 경로 start_mode 실행 중인 서비스의 시작 모드입니다. display_name 사용자에게 표시되는 실행 중인 서비스의 이름

제한

MID Server에서 **PowerShell**을 지원해야 합니다.

SHA-256 해시에는 PowerShell V4가 필요합니다.

procdump 플로우 실행

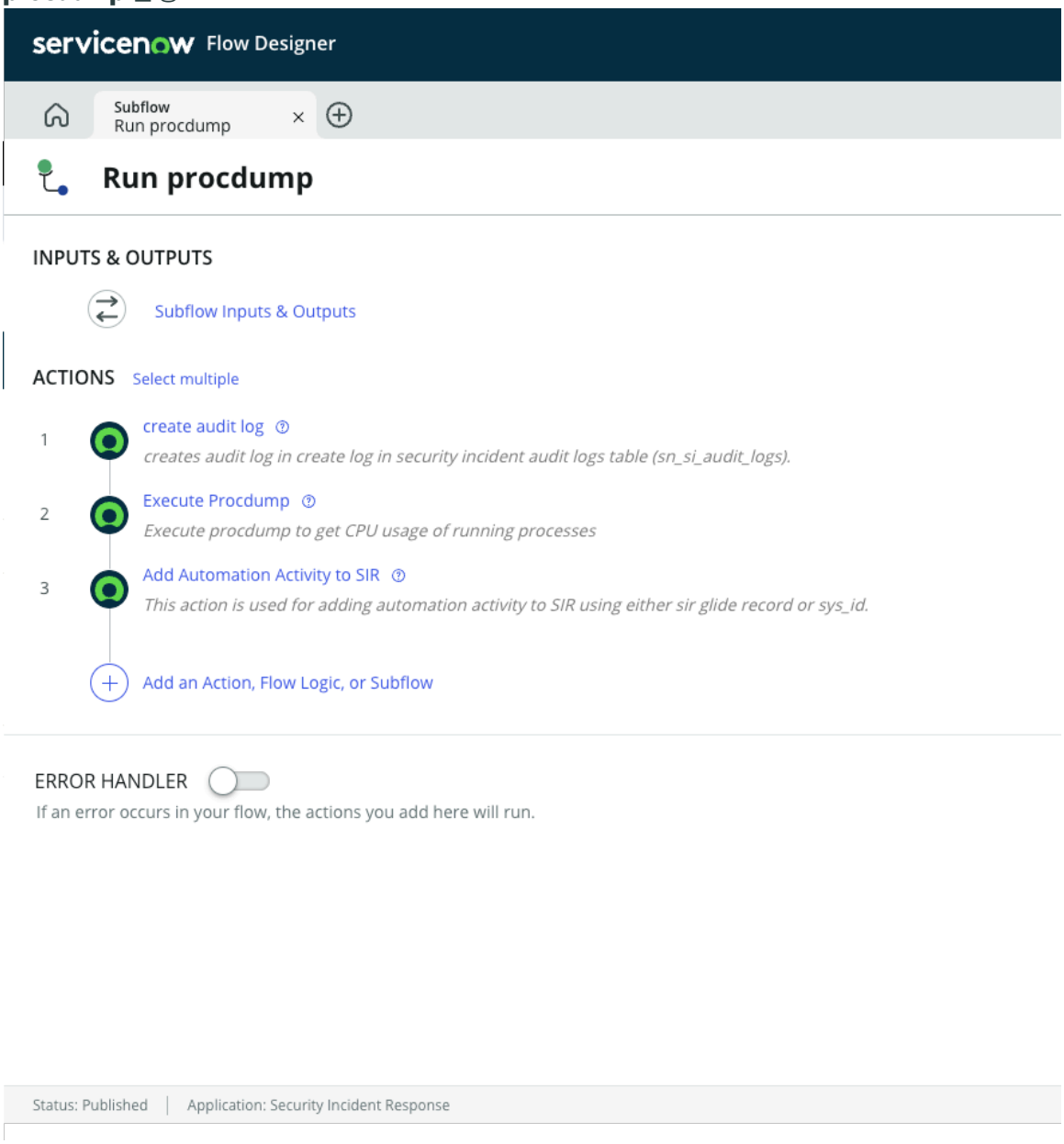
procdump 실행 플로우는 지정된 프로세스에서 프로세스 덤프를 실행하고 보안 분석가가 대상으로 지정할 수 있는 파일에 저장합니다.

필요한 역할: sn_si.analyst

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 플로우는 보강된 프로세스가 선택되고 **procdump** 실행 UI 작업이 실행될 때 트리거됩니다.

procdump 실행



procdump가 실패할 수 있는 이유는 다음과 같습니다.

- 잘못된 덤프 경로
- 잘못된 파일 공유 경로
- procdump가 실행 중인 Windows 머신의 정규화된 domin 이름을 가져올 수 없습니다.
- 프로세스 이름이 지정되지 않았습니다.
- PROCDUMP 환경 변수를 찾을 수 없습니다.
- 덤프 파일의 복사본이 덤프 경로에서 파일 공유 경로로 복사되지 않습니다.

procdump 작업 실행

Execute procdump 는 선택한 프로세스에서 procdump를 실행하고, 데이터를 파일로 덤프하고, 내부 네트워크의 공유 사이트에 게시하는 powershell 작업입니다. 그런 다음 분석가는 보안

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

인시던트에서 빨간색으로 강조 표시된 거부 목록에 나열된 프로세스를 보고 파일에 대한 추가 분석을 수행할 수 있습니다.

결과

이 동작의 가능한 결과는 다음과 같습니다.

결과

결과	설명
성공	procdump는 process_name에서 성공적으로 실행되었으며 자세한 내용은 actionOutput.response에서 확인할 수 있습니다.
실패	procdump가 process_name에서 실행하지 못했으며 자세한 내용은 actionOutput.response에서 확인할 수 있습니다.

입력 변수

입력 변수는 요청된 출력을 생성하는 데 사용됩니다.

입력 변수

변수	설명
targetId	〔필수〕 procdump를 실행할 대상 ID입니다.
process_name	〔필수〕 procdump의 프로세스 이름입니다.
dump_path	〔필수〕 생성된 덤프 파일이 저장될 로컬 파일 경로입니다.
dump_filename	〔필수〕 procdump에서 생성된 파일의 파일 이름입니다. 모든 특수 문자는 파일이 생성될 때 덤프 파일 이름에서 하이픈(-)으로 대체됩니다.
file_share_path	〔필수〕 덤프 파일을 복사할 파일 공유 경로입니다.

출력 변수

출력 변수에는 후속 작업에서 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
share_path	덤프 파일이 복사된 파일 공유 경로입니다.
response	procdump의 결과에 대한 JSON 표현입니다.
결과	procdump의 결과입니다.

보안 인시던트 - 응답 작업 결과 워크플로우 평가

보안 인시던트 - 응답 평가 작업 결과 워크플로우는 사용할 작업을 결정하고, 선택한 워크플로우에 대한 입력으로 제공된 결과 평가자 기록을 기반으로 선택한 워크플로우 및 평가 스크립트를 호출합니다.

시작하기 전에
필요한 역할: sn_si.write

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

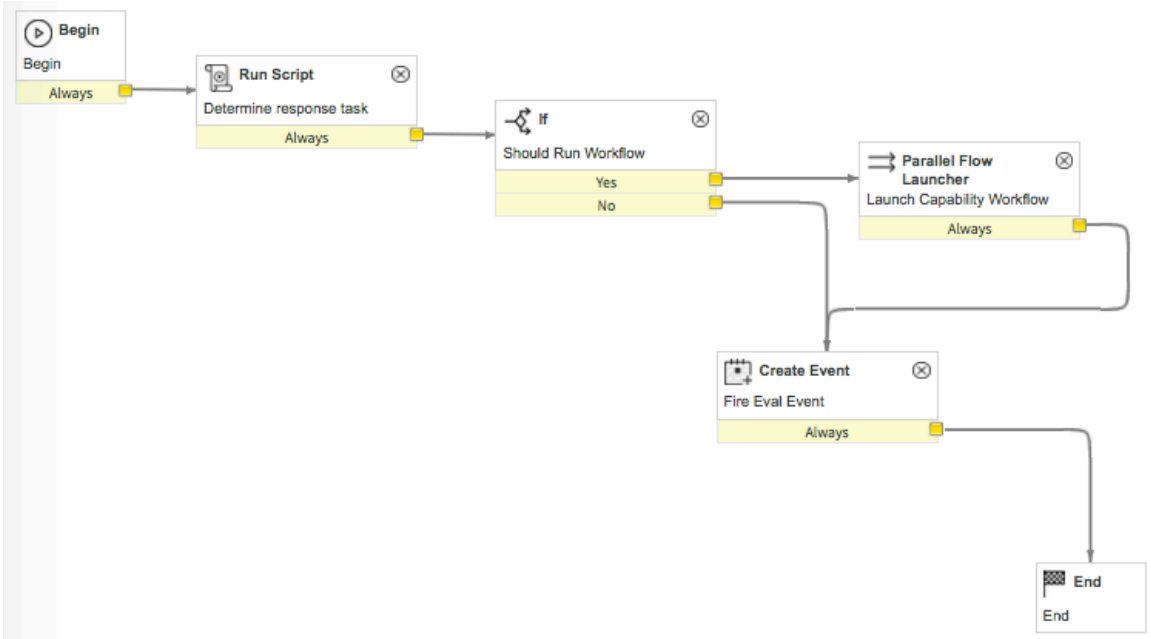
이 태스크 정보

이 워크플로우는 평가할 작업 작성 활동과 동시에 실행되어야 합니다. 평가 스크립트는 응답 작업에 적합한 결과를 결정하기 위해 응답 작업의 컨텍스트 정보를 사용하여 구성된 역량의 아티팩트(예: 사이팅, 검색 기록 또는 실행 중인 프로세스)를 쿼리합니다. 결과는 워크플로우 활동에 따라 달라질 수 있지만 일반적으로 예 또는 아니요입니다. 결과 평가자 기록을 생성할 때는 워크플로우가 구성되어 있고 작업 기반 역량 여부 확인란이 선택되어 있으며 작업 입력 변수 세트만 선택할 수 있습니다.

워크플로우 프로세스 활동에는 다음이 포함됩니다.

- 스크립트를 실행하여 응답 작업 결정
- 워크플로우를 실행해야 함
- 병렬 플로우 시작 관리자 시작 역량 워크플로우
- 평가 이벤트 생성

응답 작업 결과 평가



보안 인시던트 응답 워크플로우 템플릿

기본 보안 작업 관련 분석 절차를 수행할 수 있도록 워크플로우 템플릿이 제공됩니다 보안 인시던트 응답 오케스트레이션 . 템플릿을 그대로 사용하거나 특정 요구에 더 잘 맞는 워크플로우를 생성하도록 사용자 지정할 수 있습니다. 워크플로우 템플릿은 기본적으로 비활성화되어 있습니다.

sn_sec_cmn.admin 역할을 가진 사용자만 워크플로우를 편집할 수 있습니다.

보안 인시던트 기밀 데이터 노출 워크플로우 템플릿

보안 인시던트 - 기밀 데이터 노출 - 템플릿을 사용하면 중요한 데이터의 노출을 처리하도록 설계된 일련의 작업을 수행할 수 있습니다.

시작하기 전에

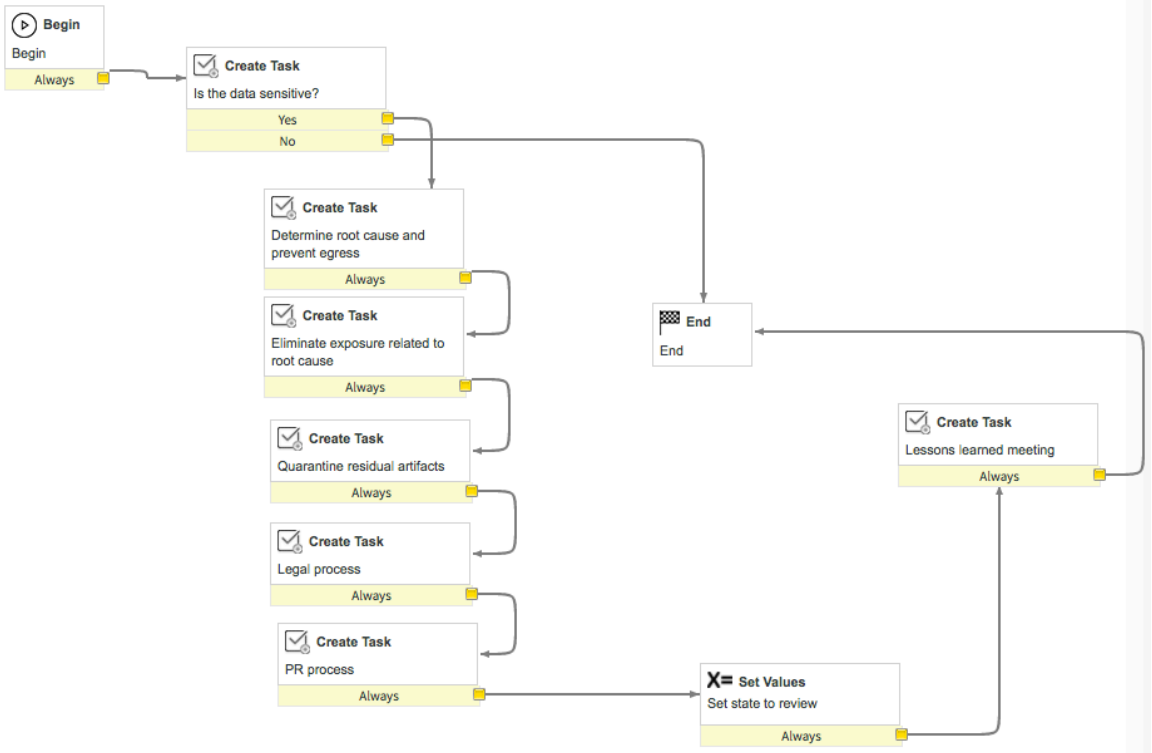
필요한 역할: sn_si.write

이 태스크 정보

워크플로우는 보안 인시던트의 범주 가 기밀 개인 계정 데이터 노출로 설정되거나 변경되면 트리거됩니다. 이 작업을 수행하면 워크플로우에서 첫 번째 활동에 대한 응답 작업이 생성됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

기밀 개인 계정 데이터 노출



프로시저

1. 중요한 데이터에 대한 노출을 처리할 보안 인시던트를 열거나 새 보안 인시던트를 생성합니다.
2. 범주에서 기밀 개인 계정 데이터 노출을 선택합니다.
3. 레코드를 저장합니다.
4. 아래로 스크롤하여 대응 작업 관련 목록을 엽니다.
   일련의 응답 작업 중 첫 번째 작업이 나타납니다. 기록이 저장될 때마다 이전 작업에 대한 응답으로 인해 다음 응답 작업이 생성되거나 플로우가 종료됩니다.

기밀 데이터 노출 템플릿의 응답 작업

응답 작업	설명	결과
데이터가 민감합니까?	이 보안 인시던트와 관련된 데이터가 중요한 데이터인지 기밀인지 확인합니다. 작업의 결과에서 예 또는 아니요를 선택합니다.	예를 선택한 경우 다음 응답 작업이 실행됩니다. 아니요를 선택하면 플로우가 종료됩니다.
근본 원인을 파악하고 송신을 방지합니다.	공격의 근본 원인을 확인하고 송신 필터링을 추가하여 반출을 중지하고 작업의 상태 필드를 적절하게 업데이트합니다.	작업 상태를 완료 종결 또는 취소됨으로 변경하면 다음 응답 작업이 실행됩니다.
근본 원인과 관련된 노출 제거	근본 원인에 따라 노출을 제거하는 단계를 수행하여 작업의 상태 필드를 적절하게 업데이트합니다.	작업 상태를 완료 종결 또는 취소됨으로 변경하면 다음 응답 작업이 실행됩니다.
잔여 아티팩트 격리	잔여 아티팩트를 격리하는 단계를 수행하여 작업의 상태 필드를 적절하게 업데이트합니다.	작업 상태를 완료 종결 또는 취소됨으로 변경하면 다음 응답 작업이 실행됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

응답 작업	설명	결과
법적 절차	이 분석의 법적 요구 사항을 충족하기 위한 단계를 수행하여 작업의 상태 필드를 적절하게 업데이트합니다.	작업 상태를 완료 종결 또는 취소됨으로 변경하면 다음 응답 작업이 실행됩니다.
PR 프로세스	이 분석의 PR 요구 사항을 충족하는 단계를 수행하여 작업의 상태 필드를 적절하게 업데이트합니다.	작업 상태를 완료 종결 또는 취소됨으로 변경하면 다음 응답 작업이 실행됩니다.
상태를 검토로 설정	필요한 조치가 없습니다.	보안 인시던트의 상태가자동으로 검토로 변경됩니다.
학습한 교훈 회의	학습한 교훈 회의를 수행하여 이 중요한 데이터에 대해 수행된 작업을 분류하고 작업의 상태 필드를 적절하게 업데이트합니다.	작업의 상태를 종결, 완료 또는 취소됨으로 변경하면 보안 인시던트는 종결할 때까지 검토 상태로 유지됩니다.

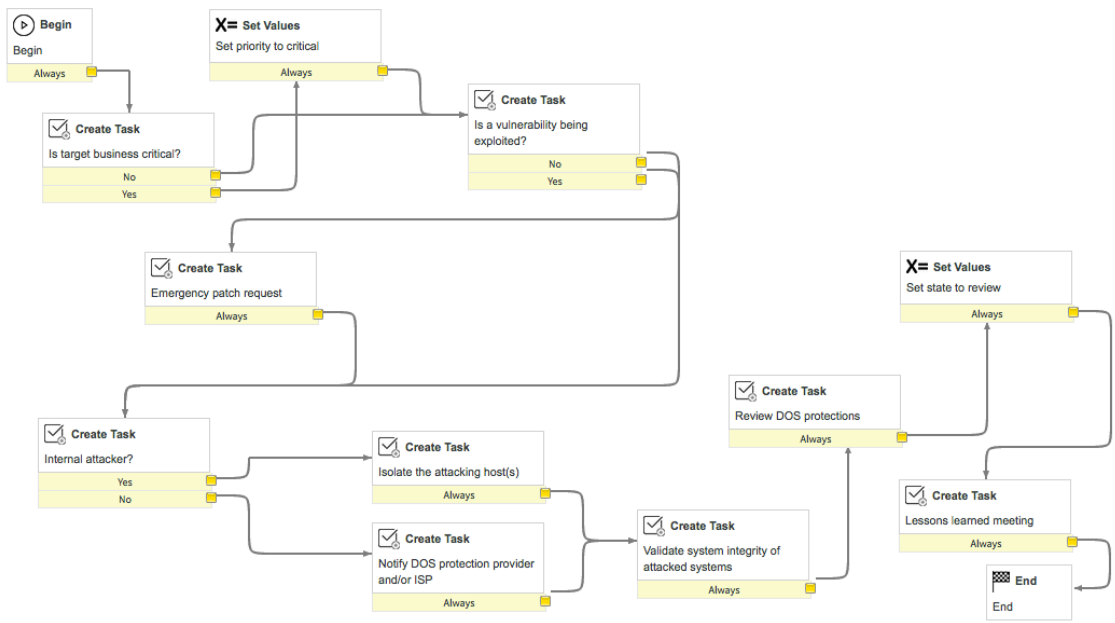
보안 인시던트 DoS(서비스 거부) 워크플로우 템플릿

보안 인시던트 - DoS(서비스 거부) - 템플릿을 사용하면 DOS(서비스 거부) 공격을 처리하도록 설계된 일련의 작업을 수행할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.write

이 태스크 정보
워크플로우는 보안 인시던트의 범주 가 서비스 거부로 설정된 경우 트리거됩니다. 이 작업을 수행하면 워크플로우에서 첫 번째 활동에 대한 응답 작업이 생성됩니다.

서비스 거부**(DOS)**



프로시저

1. 이 서비스 거부 발생에 대한 보안 인시던트를 열거나 새 보안 인시던트를 생성합니다.
2. 범주에서 서비스 거부를 선택합니다.
3. 레코드를 저장합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 아래로 스크롤하여 대응 작업 관련 목록을 엽니다.
일련의 응답 작업 중 첫 번째 작업이 나타납니다. 기록이 저장될 때마다 이전 작업에 대한 응답으로 인해 다음 응답 작업이 생성되거나 플로우가 종료됩니다.

DoS(서비스 거부) 템플릿의 응답 작업

응답 작업	작업	결과
대상 비즈니스가 중요합니까?	이 DOS 공격의 대상이 비즈니스에 중요한지 확인합니다. 작업의 결과에서 예 또는 아니요를 선택합니다.	예를 선택하면 우선순위를 중요로 설정 작업이 실행됩니다. 아니요를 선택하면 취약성을 악용하고 있습니까? 작업이 실행됩니다.
우선순위를 중요로 설정	필요한 조치가 없습니다.	보안 인시던트의 우선순위 가 자동으로 중요로 변경되고 취약성이 악용되고 있습니까? 작업이 실행됩니다.
취약성을 악용하고 있습니까?	이 DOS 공격이 소프트웨어 취약점을 악용하는지 여부를 확인합니다. 작업의 결과에서 예 또는 아니요를 선택합니다.	예를 선택하면 긴급 패치 요청 작업이 실행됩니다. 아니요를 선택하면 내부 공격자? 작업이 실행됩니다.
긴급 패치 요청	공격을 받는 시스템에 대한 긴급 패치 요청을 발행합니다. 작업의 상태 필드를 적절하게 업데이트합니다.	작업 상태를 완료 종결 또는 취소됨으로 변경한 경우 다음 응답 작업이 실행됩니다.
내부 공격자입니까?	이 DOS 공격의 소스가 조직 내부에 있는지 확인합니다. 작업의 결과에서 예 또는 아니요를 선택합니다.	예를 선택하면 공격 호스트 격리 작업이 실행됩니다. 아니요를 선택하면 **DOS** 보호 제공자 및/또는 **ISP** 작업 통지가 실행됩니다.
공격 호스트 격리	공격을 담당하는 내부 호스트를 격리하는 데 필요한 단계를 수행합니다. 작업의 상태 필드를 적절하게 업데이트합니다.	이 단계를 완료하면 공격받은 시스템의 시스템 무결성 확인 작업이 실행됩니다.
DOS 보호 제공자 및/또는 ISP에 알림	서비스 거부 보호 공급자 및/또는 인터넷 서비스 공급자에게 연락하여 공격을 알리는 데 필요한 단계를 수행합니다. 작업의 상태 필드를 적절하게 업데이트합니다.	작업 상태를 완료 종결 또는 취소됨으로 변경한 경우 다음 응답 작업이 실행됩니다.
공격받은 시스템의 시스템 무결성 검증	공격받은 컴퓨터의 무결성을 평가하고 유효성을 검사하는 데 필요한 단계를 수행합니다. 작업의 상태 필드를 적절하게 업데이트합니다.	작업 상태를 완료 종결 또는 취소됨으로 변경한 경우 다음 응답 작업이 실행됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

응답 작업	작업	결과
DOS 보호 검토	기존 DOS 보호 및 절차를 검토합니다. 필요한 사항을 변경합니다. 작업의 상태 필드를 적절하게 업데이트합니다.	작업 상태를 완료 종결 또는 취소됨으로 변경한 경우 다음 응답 작업이 실행됩니다.
상태를 검토로 설정	필요한 조치가 없습니다.	보안 인시던트의 상태가자동으로 검토로 변경됩니다. 학습한 교훈 회의 작업이 실행됩니다.
학습한 교훈 회의	학습한 교훈 회의를 수행하여 이 서비스 거부 인시던트에 대해 수행된 작업을 분류합니다. 작업의 상태 필드를 적절하게 업데이트합니다.	작업 상태를 종결, 완료 또는 취소됨으로 변경하면 플로우가 종료됩니다.

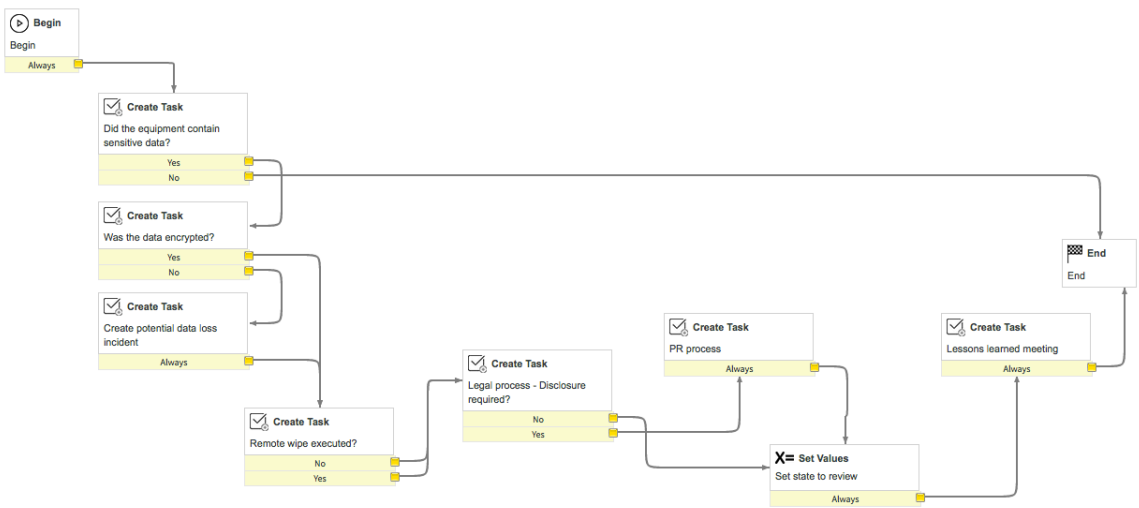
보안 인시던트 장비 분실 워크플로우 템플릿

보안 인시던트 - 장비 분실 - 템플릿을 사용하면 분실된 장비를 처리하도록 설계된 일련의 작업을 수행할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.write

이 태스크 정보
워크플로우는 보안 인시던트의 범주 가 장비 손실로 설정된 경우 트리거됩니다. 이 작업을 수행하면 워크플로우에서 첫 번째 활동에 대한 응답 작업이 생성됩니다.

장비 손실



프로시저

1. 장비 손실에 대한 보안 인시던트를 열거나 새 보안 인시던트를 생성합니다.
2. 범주에서 장비 손실을 선택합니다.
3. 레코드를 저장합니다.
4. 아래로 스크롤하여 대응 작업 관련 목록을 엽니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

일련의 응답 작업 중 첫 번째 작업이 나타납니다. 기록이 저장될 때마다 이전 작업에 대한 응답으로 인해 다음 응답 작업이 생성되거나 플로우가 종료됩니다.

분실 장비 템플릿의 응답 작업

응답 작업	작업	결과
장비에 중요한 데이터가 포함되어 있습니까?	이 보안 인시던트와 관련된 장비에 중요한 정보나 기밀 정보가 포함되어 있는지 확인합니다. 작업의 결과에서 적절하게 예 또는 아니요를 선택합니다.	예를 선택하면 데이터가 암호화되었습니까? 작업이 실행됩니다. 아니요를 선택하면 플로우가 종료됩니다.
데이터가 암호화되었습니까?	분실한 장치의 민감한 데이터가 암호화되었는지 확인합니다. 작업의 결과에서 적절하게 예 또는 아니요를 선택합니다.	예를 선택하면 원격 초기화가 생성되었습니까? 응답 작업이 실행됩니다. 아니요를 선택하면 잠재적 데이터 손실 인시던트응답 작업 만들기가 실행됩니다.
잠재적 데이터 손실 인시던트 생성	잠재적인 데이터 손실 인시던트를 만드는 데 필요한 단계를 수행합니다. 작업을 마친 후에는 작업의 상태를 적절하게 완료 또는 미완료 로 설정합니다.	원격 초기화가 생성되었습니까? 응답 작업이 실행됩니다.
원격 초기화를 생성했습니까?	분실된 장비의 원격 지우기를 실행하는 데 필요한 단계를 수행합니다. 작업의 결과에서 적절하게 예 또는 아니요를 선택합니다.	법무 프로세스 - 고지 필수 작업이 실행됩니다.
법적 절차 - 공개가 필요합니까?	이 분석의 법적 요구 사항을 충족하는 단계를 수행합니다. 법적 공개가 필요한 경우 예를 선택하고, 필요하지 않은 경우 아니요를 선택합니다.	학습한 교훈 회의 작업이 실행됩니다.
PR 프로세스	이 분석의 PR 요구 사항을 충족하는 데 필요한 단계를 수행합니다. 작업을 마친 후에는 작업의 상태를 적절하게 완료 또는 미완료 로 설정합니다.	상태를 검토로 설정 작업이 실행됩니다.
상태를 검토로 설정	아무 작업도 필요하지 않습니다.	보안 인시던트의 상태가자동으로 검토로 변경됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

응답 작업	작업	결과
학습한 교훈 회의	학습한 교훈 회의를 수행하여 이 장비 손실 인시던트에 대해 수행된 작업을 분류합니다. 작업을 마친 후에는 작업의 상태를 적절하게 완료 또는 미완료 로 설정합니다.	플로우가 종료됩니다.

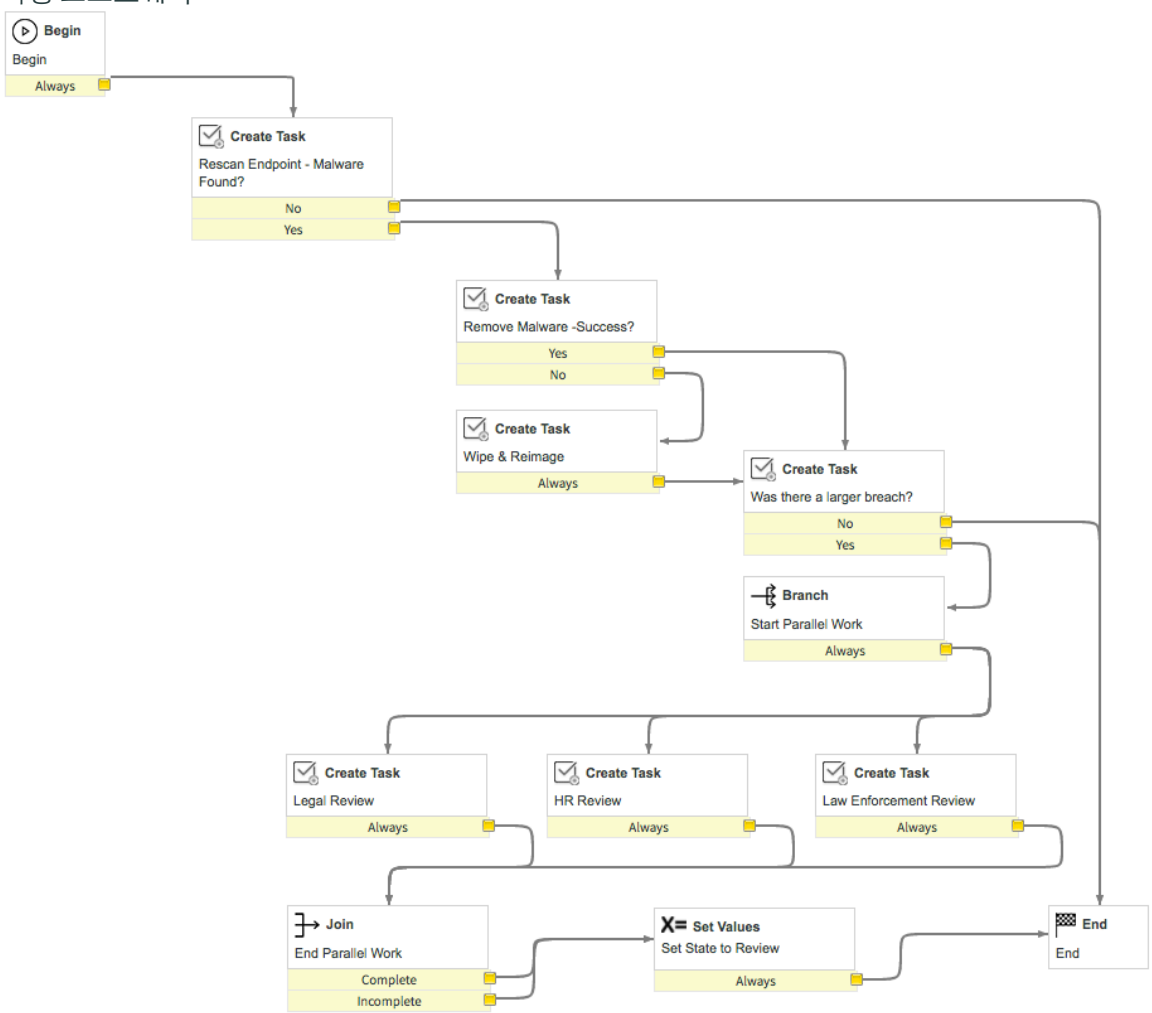
보안 인시던트 악성 소프트웨어 워크플로우 템플릿

보안 인시던트 - 악성 소프트웨어 - 템플릿을 사용하면 네트워크에서 악성 소프트웨어를 처리하도록 설계된 일련의 작업을 수행할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.write

이 태스크 정보
워크플로우는 보안 인시던트의 범주 가 악성 소프트웨어로 설정된 경우 트리거됩니다. 이 작업을 수행하면 워크플로우에서 첫 번째 활동에 대한 응답 작업이 생성됩니다.

악성 소프트웨어



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 이 잠재적 공격에 대한 보안 인시던트를 열거나 새 보안 인시던트를 생성합니다.
2. 범주에서 악성 코드 활동을 선택합니다.
3. 레코드를 저장합니다.
4. 아래로 스크롤하여 대응 작업 관련 목록을 엽니다.
   일련의 응답 작업 중 첫 번째 작업이 나타납니다. 기록이 저장될 때마다 이전 작업에 대한 사용자의 응답으로 인해 다음 응답 작업이 생성되거나 워크플로우가 종료됩니다.

악성 소프트웨어 템플릿의 응답 작업

응답 작업	작업	결과
스캔 엔드포인트 - 맬웨어를 찾았습니까?	검사를 실행한 후 맬웨어가 발견되었는지 확인합니다. 작업의 결과에서 예 또는 아니요를 선택합니다.	예를 선택하면 맬웨어 제거 - 성공? 작업이 실행됩니다. 아니요를 선택하면 플로우가 종료됩니다.
맬웨어 제거 - 성공?	맬웨어가 성공적으로 제거되었는지 여부를 확인합니다. 작업의 결과에서 예 또는 아니요를 선택합니다.	예를 선택하면 더 큰 위반이 있었습니까? 작업이 실행됩니다. 아니요를 선택하면 지우기 및 이미지로 다시 설치 작업이 실행됩니다.
지우기 및 이미지로 다시 설치	발견된 맬웨어를 성공적으로 제거하지 못한 경우 이 작업은 맬웨어에 감염된 컴퓨터에서 초기화 및 이미지로 다시 설치를 수행하도록 지시합니다.	작업이 완료되면 상태를 검토로 설정 작업이 실행됩니다.
더 큰 위반이 있었습니까?	악성 소프트웨어로 인한 위반이 처음 생각했던 것보다 큰지 여부를 확인합니다. 작업의 결과에서 예 또는 아니요를 선택합니다.	예를 선택하면 다음 작업이 병렬로 실행됩니다. ○ 법무 검토 ○ HR 검토 ○ 법 집행 검토 아니요를 선택하면 플로우가 종료됩니다.
법무 검토 HR 검토 법 집행 검토	이러한 각 부서에 필요한 단계를 수행하여 악성 소프트웨어를 근절하기 위해 수행한 프로세스를 검토합니다.	작업이 완료되면 상태를 검토로 설정 작업이 실행됩니다.
상태를 검토로 설정	필요한 조치가 없습니다.	보안 인시던트의 상태가자동으로 검토로 변경되고 플로우가 종료됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 인시던트 피싱 워크플로우 템플릿

보안 인시던트 - 피싱 - 템플릿을 사용하면 네트워크에서 스피어 피싱 이메일을 처리하도록 설계된 일련의 작업을 수행할 수 있습니다.

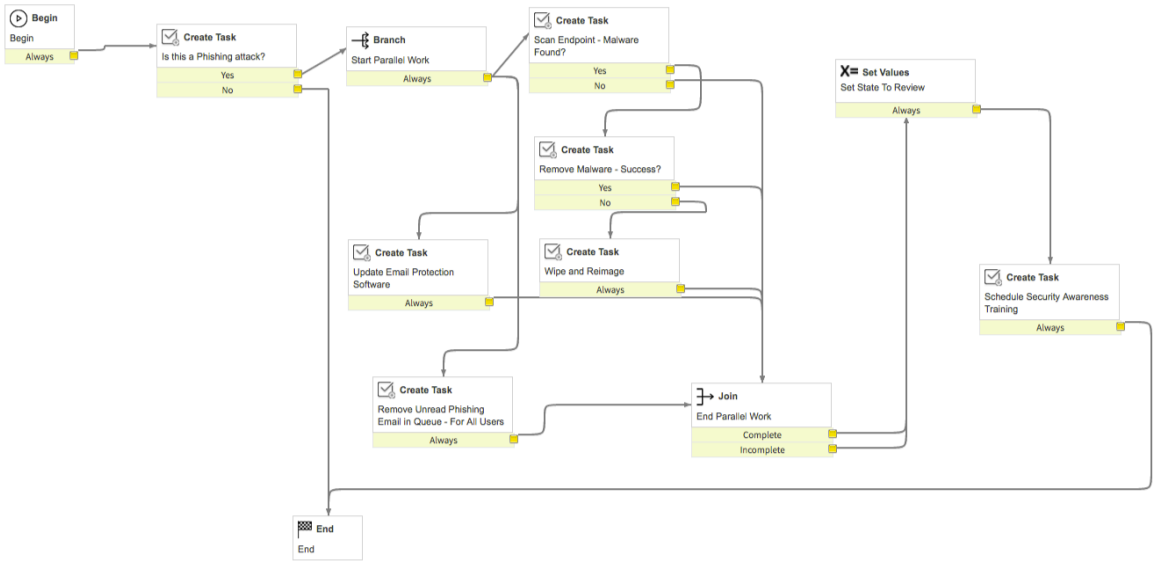
시작하기 전에

필요한 역할: sn_si.write

이 태스크 정보

워크플로우는 보안 인시던트의 범주 가 스피어 피싱으로 설정된 경우 트리거됩니다. 이 작업을 수행하면 워크플로우에서 첫 번째 활동에 대한 응답 작업이 생성됩니다.

스피어 피싱



프로시저

1. 이 잠재적인 스피어 피싱 공격에 대한 보안 인시던트를 열거나 새 보안 인시던트를 생성합니다.
2. 범주에서 스피어 피싱을 선택합니다.
3. 레코드를 저장합니다.
4. 아래로 스크롤하여 대응 작업 관련 목록을 엽니다.
   일련의 응답 작업 중 첫 번째 작업이 나타납니다. 기록이 저장될 때마다 이전 작업에 대한 사용자의 응답으로 인해 다음 응답 작업이 생성되거나 워크플로우가 종료됩니다.

Spear 피싱 템플릿의 응답 작업

응답 작업	작업	결과
이것이 피싱 공격입니까?	이것이 피싱 공격인지 확인합니다. 작업의 결과에서 예 또는 아니요를 선택합니다.	예를 선택하면 다음 작업이 병렬로 실행됩니다. ○ 스캔 엔드포인트 - 맬웨어를 찾았습니까? ○ 이메일 보호 소프트웨어 업데이트 ○ 큐에서 읽지 않은 피싱 이메일 제거 - 모든 사용자

기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

응답 작업	작업	결과
		아니요를 선택하면 플로우가 종료됩니다.
스캔 엔드포인트 - 맬웨어를 찾았습니까?	검사를 실행한 후 맬웨어가 발견되었는지 확인합니다. 작업의 결과에서 예 또는 아니요를 선택합니다.	예를 선택하면 맬웨어 제거 - 성공? 작업이 실행됩니다. 아니요를 선택하면 상태를 검토로 설정 작업이 실행됩니다.
맬웨어 제거 - 성공?	맬웨어가 성공적으로 제거되었는지 여부를 확인합니다. 작업의 결과에서 예 또는 아니요를 선택합니다.	예를 선택하면 상태를 검토로 설정 작업이 실행됩니다. 아니요를 선택하면 지우기 및 이미지로 다시 설치 작업이 실행됩니다.
지우기 및 이미지로 다시 설치	발견된 맬웨어를 성공적으로 제거하지 못한 경우 이 작업은 맬웨어에 감염된 컴퓨터에서 초기화 및 이미지로 다시 설치를 수행하도록 지시합니다.	작업이 완료되면 상태를 검토로 설정 작업이 실행됩니다.
이메일 보호 소프트웨어 업데이트	피싱 공격으로 확인되면 그에 따라 이메일 보호 소프트웨어를 업데이트하라는 메시지가 표시됩니다.	작업이 완료되면 상태를 검토로 설정 작업이 실행됩니다.
큐에서 읽지 않은 피싱 이메일 제거 - 모든 사용자	모든 사용자에 대해 큐에 있는 피싱 이메일을 제거하는 데 필요한 단계를 수행합니다.	작업이 완료되면 상태를 검토로 설정 작업이 실행됩니다.
상태를 검토로 설정	필요한 조치가 없습니다.	보안 인시던트의 상태가자동으로 검토로 변경됩니다. 보안 인식 교육 일정 예약 작업이 실행됩니다.
보안 인식 교육 예약	직원의 보안 인식을 강화하기 위한 교육을 예약합니다. 작업의 상태 필드를 적절하게 업데이트합니다.	작업이 완료되면 플로우가 종료됩니다.

보안 인시던트 정책 위반 워크플로우 템플릿

보안 인시던트 - 정책 위반 - 템플릿을 사용하면 보안 정책 위반을 처리하도록 설계된 일련의 작업을 수행할 수 있습니다.

시작하기 전에

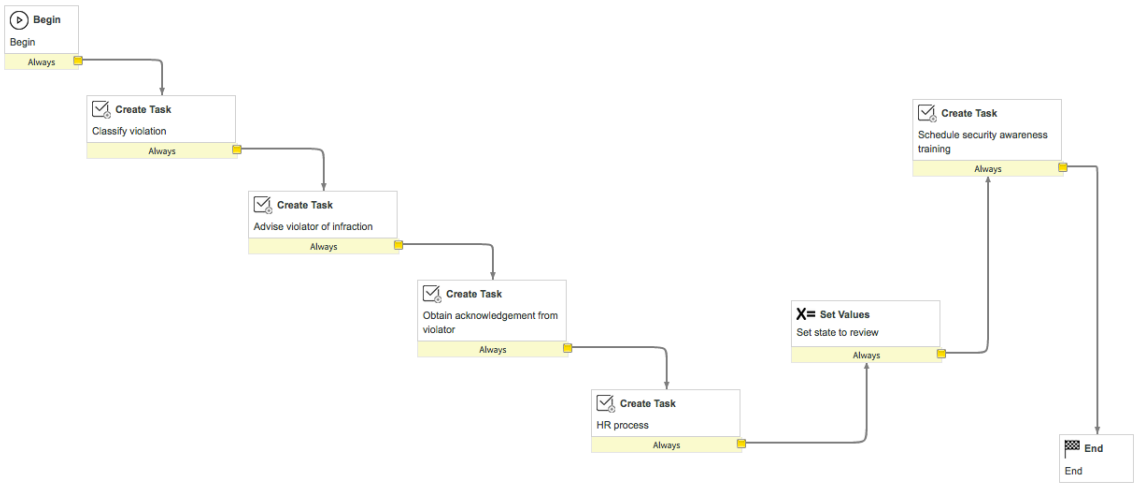
필요한 역할: sn_si.write

이 태스크 정보

워크플로우는 보안 인시던트의 범주 가 정책 위반으로 설정될 때 트리거됩니다. 이 작업을 수행하면 워크플로우에서 첫 번째 활동에 대한 응답 작업이 생성됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

정책 위반



프로시저

1. 정책 위반에 대한 보안 인시던트를 열거나 새 보안 인시던트를 생성합니다.
2. 범주에서 정책 위반을 선택합니다.
3. 레코드를 저장합니다.
4. 아래로 스크롤하여 대응 작업 관련 목록을 엽니다.
   일련의 응답 작업 중 첫 번째 작업이 나타납니다. 기록이 저장될 때마다 이전 작업에 대한 사용자의 응답으로 인해 다음 응답 작업이 생성되거나 워크플로우가 종료됩니다.

정책 위반 템플릿의 응답 작업

응답 작업	작업	결과
분류 위반	이 위반이 조직의 보안 정책을 위반하는 방법을 분류합니다. 작업을 완료한 후 작업의 상태 필드를 업데이트합니다.	위반자 위반자 대응 권고 작업이 실행됩니다.
위반자에게 위반 조언	위반자에게 위반의 성격을 전달합니다. 상태 필드를 전달한 후 작업의 상태 필드를 업데이트합니다.	위반자로부터 승인 받기 응답 작업이 실행됩니다.
위반자로부터 승인 받기	위반자로부터 위반 확인서를 받습니다. 작업의 상태 필드를 적절하게 업데이트합니다.	**HR** 프로세스 응답 작업이 실행됩니다.
HR 프로세스	이 위반에 대해 필요한 모든 정보를 HR에 전달하십시오. 작업의 상태 필드를 적절하게 업데이트합니다.	검토 응답 작업을 검토하도록 상태 설정 작업이 실행됩니다.
상태를 검토로 설정	아무 작업도 필요하지 않습니다.	보안 인시던트의 상태가자동으로 검토로 변경됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

응답 작업	작업	결과
보안 인식 교육 예약	보안 인식 교육을 실시하여 향후 유사한 보안 위반을 방지하는 방법에 대해 직원을 교육합니다. 작업의 상태 필드를 적절하게 업데이트합니다.	작업 상태를 종결, 완료 또는 취소됨으로 변경하면 플로우가 종료됩니다.

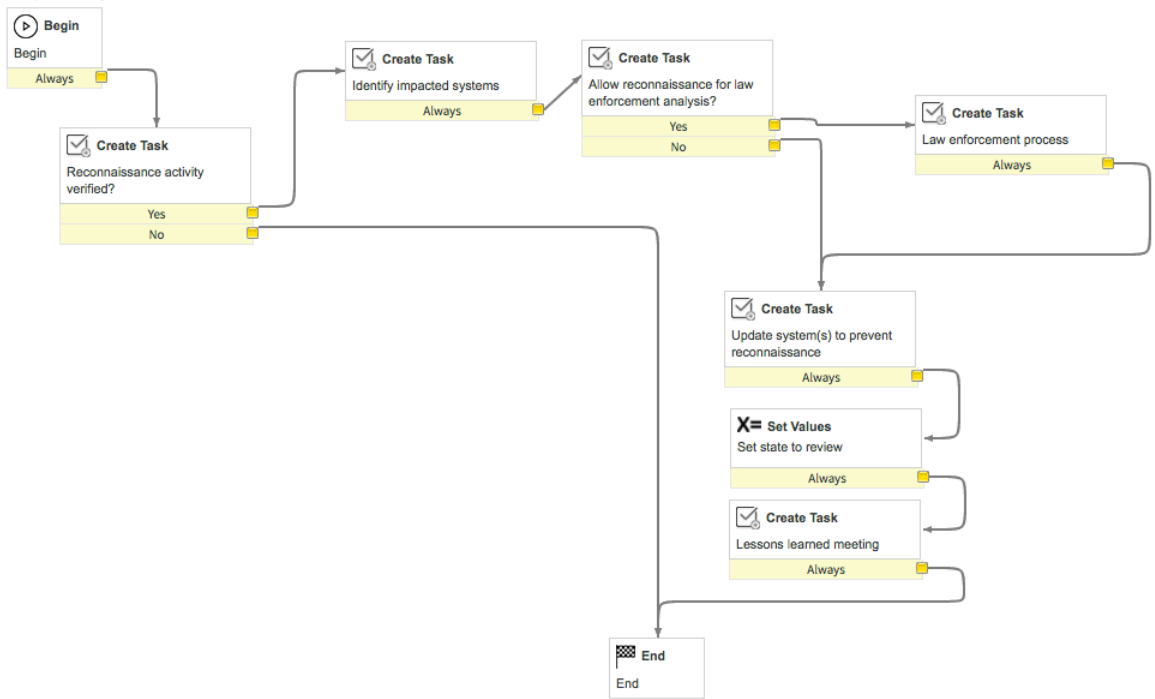
보안 인시던트 정찰 워크플로우 템플릿

정찰은 일반적으로 장치 또는 시스템을 악용하려는 추가 공격에 대한 예비 단계입니다. 보안 인시던트 - 정찰 - 템플릿을 사용하면 네트워크에서 정찰을 처리하도록 설계된 일련의 작업을 수행할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.write

이 태스크 정보
워크플로우는 보안 인시던트의 범주 가 정찰 활동으로 설정된 경우 트리거됩니다. 이 작업을 수행하면 워크플로우에서 첫 번째 활동에 대한 응답 작업이 생성됩니다.

정찰 활동



프로시저

1. 이 잠재적 공격에 대한 보안 인시던트를 열거나 새 보안 인시던트를 생성합니다.
2. 범주에서 정찰 활동을 선택합니다.
3. 레코드를 저장합니다.
4. 아래로 스크롤하여 대응 작업 관련 목록을 엽니다.
   일련의 응답 작업 중 첫 번째 작업이 나타납니다. 기록이 저장될 때마다 이전 작업에 대한 사용자의 응답으로 인해 다음 응답 작업이 생성되거나 워크플로우가 종료됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

정찰 템플릿의 응답 작업

응답 작업	작업	결과
정찰 활동이 확인되었습니까?	관찰된 정찰이 검증되었는지 여부를 확인합니다. 작업의 결과에서 예 또는 아니요를 선택합니다.	예를 선택하면 영향을 받는 시스템 식별 작업이 실행됩니다. 아니요를 선택하면 플로우가 종료됩니다.
영향을 받는 시스템 식별	정찰의 영향을 받는 시스템을 결정합니다.	이 작업이 완료되면 법 집행 분석을 위한 정찰 허용? 작업이 실행됩니다.
법 집행 분석을 위한 정찰을 허용하시겠습니까?	법 집행 기관에서 정찰을 분석할지 여부를 결정합니다. 작업의 결과에서 예 또는 아니요를 선택합니다.	예를 선택하면 법 집행 프로세스 작업이 실행됩니다. 아니요를 선택하면 정찰을 방지하기 위한 시스템 업데이트 작업이 실행됩니다.
법 집행 절차	회사에서 정의한 대로 법 집행 프로세스를 수행합니다.	이 작업이 완료되면 시스템을 업데이트하여 정찰 방지 작업이 실행됩니다.
정찰을 방지하기 위해 시스템을 업데이트합니다.	정찰의 영향을 받는 시스템을 업데이트하는 데 필요한 단계를 수행합니다.	이 작업이 완료되면 상태를 검토로 설정 작업이 실행됩니다.
상태를 검토로 설정	필요한 조치가 없습니다.	보안 인시던트의 상태가검토로 자동 변경되고 학습한 교훈 회의 작업이 실행됩니다.
학습한 교훈 회의	교훈 회의를 수행하여 이 정찰 인시던트에 수행된 작업을 분류합니다. 작업의 상태 필드를 적절하게 업데이트합니다.	이 작업이 완료되면 플로우가 종료됩니다.

보안 인시던트 **Rogue** 서버 또는 서비스 워크플로우 템플릿

보안 인시던트 - Rogue 서버 또는 서비스 - 템플릿을 사용하면 네트워크에 영향을 주는 Rogue 서버 또는 서비스의 활동을 처리하도록 설계된 일련의 작업을 수행할 수 있습니다.

시작하기 전에

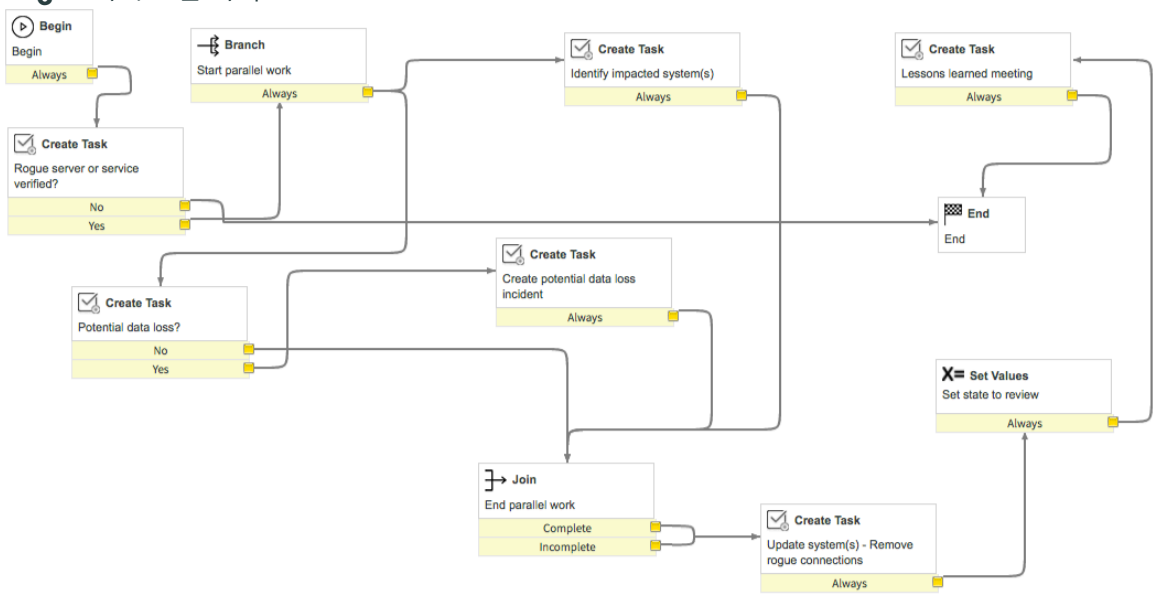
필요한 역할: sn_si.write

이 태스크 정보

워크플로우는 보안 인시던트의 범주 가 **Rogue** 서버 또는 서비스로 설정된 경우 트리거됩니다. 이 작업을 수행하면 워크플로우에서 첫 번째 활동에 대한 응답 작업이 생성됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Rogue 서버 또는 서비스



프로시저

1. 이 잠재적 공격에 대한 보안 인시던트를 열거나 새 보안 인시던트를 생성합니다.
2. 범주에서 **Rogue** 서버 또는 서비스 활동을 선택합니다.
3. 레코드를 저장합니다.
4. 아래로 스크롤하여 대응 작업 관련 목록을 엽니다.
   일련의 응답 작업 중 첫 번째 작업이 나타납니다. 기록이 저장될 때마다 이전 작업에 대한 사용자의 응답으로 인해 다음 응답 작업이 생성되거나 워크플로우가 종료됩니다.

Rogue 서버 또는 서비스 템플릿의 응답 작업

응답 작업	작업	결과
Rogue 서버 또는 서비스가 확인되었습니까?	Rogue 서버 또는 서비스와의 연결이 네트워크에서 확인되었는지 확인합니다. 작업의 결과에서 예 또는 아니요를 선택합니다.	예를 선택하면 다음 두 작업이 병렬로 실행됩니다. ○ 영향을 받는 시스템 식별 ○ 잠재적인 데이터 손실? 아니요를 선택하면 플로우가 종료됩니다.
영향을 받는 시스템 식별	Rogue 서버 또는 서비스와의 접촉으로 영향을 받는 시스템을 확인합니다.	이 작업이 완료되면 시스템 업데이트 - **Rogue** 연결 제거 작업이 실행됩니다.
잠재적인 데이터 손실?	Rogue 서버 또는 서비스와의 연결로 인해 잠재적인 데이터 손실이 발생했는지 여부를 확인합니다. 작업의 결과에서 예 또는 아니요를 선택합니다.	예를 선택하면 잠재적 데이터 손실 인시던트 만들기 작업이 실행됩니다. 아니요를 선택하면 시스템 업데이트 - **Rogue** 연결 제거 작업이 실행됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

응답 작업	작업	결과
잠재적 데이터 손실 인시던트 생성	잠재적인 데이터 손실에 대한 보안 인시던트를 생성하는 데 필요한 단계를 수행합니다.	이 작업이 완료되면 시스템 업데이트 - **Rogue** 연결 제거 작업이 실행됩니다.
시스템 업데이트 - 불량 연결 제거	불량 연결을 제거하는 데 필요한 단계를 수행합니다.	이 작업이 완료되면 상태를 검토로 설정 작업이 실행됩니다.
상태를 검토로 설정	필요한 조치가 없습니다.	보안 인시던트의 상태가검토로 자동 변경되고 학습한 교훈 회의 작업이 실행됩니다.
학습한 교훈 회의	단원 회의를 수행하여 이 Rogue 서버 또는 서비스 인시던트에 대해 수행된 작업을 분류합니다. 작업의 상태 필드를 적절하게 업데이트합니다.	이 작업이 완료되면 플로우가 종료됩니다.

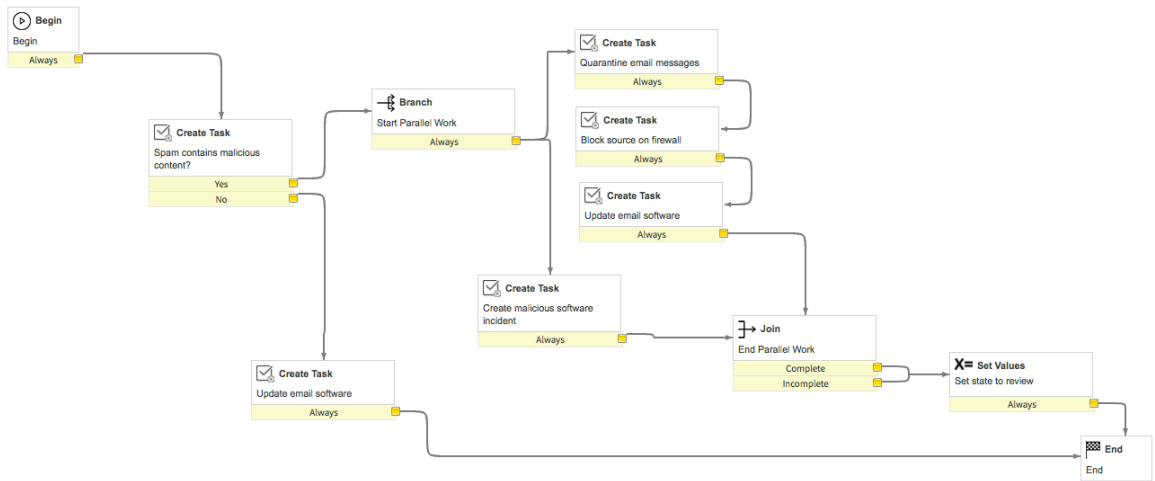
보안 인시던트 스팸 워크플로우 템플릿

보안 인시던트 - 스팸 - 템플릿을 사용하면 네트워크에서 이메일 스팸을 처리하도록 설계된 일련의 작업을 수행할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.write

이 태스크 정보
워크플로우는 보안 인시던트의 범주 가 스팸 소스로 설정되거나 변경될 때 트리거됩니다. 이 작업을 수행하면 워크플로우에서 첫 번째 활동에 대한 응답 작업이 생성됩니다.

스팸 소스



프로시저

1. 이메일 스팸을 처리할 보안 인시던트를 열거나 새 보안 인시던트를 생성합니다.
2. 범주에서 스팸 소스를 선택합니다.
3. 레코드를 저장합니다.
4. 아래로 스크롤하여 대응 작업 관련 목록을 엽니다.
   일련의 응답 작업 중 첫 번째 작업이 나타납니다. 기록이 저장될 때마다 이전 작업에 대한 사용자의 응답으로 인해 다음 응답 작업이 생성되거나 워크플로우가 종료됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

스팸 템플릿의 응답 작업

응답 작업	작업	결과
스팸에 악성 콘텐츠가 포함되어 있습니까?	스팸에 악성 소프트웨어가 포함되어 있는지 확인합니다. 작업의 결과에서 예 또는 아니요를 선택합니다.	예를 선택한 경우 다음 응답 작업이 실행됩니다. ○ 이메일 메시지 격리 ○ 악성 소프트웨어 인시던트 생성 아니요를 선택하면 이메일 소프트웨어 업데이트가 실행됩니다.
악성 소프트웨어 인시던트 생성	보안 인시던트를 만드는 단계를 수행하여 작업의 상태 필드를 적절하게 업데이트합니다.	작업 상태를 완료 종결 또는 취소됨으로 변경하면 이 응답 작업은 다음 세 개의 응답 작업이 완료될 때까지 대기합니다. 이후 보안 인시던트의 상태가 검토로 전환됩니다.
이메일 메시지 격리	스팸을 격리하는 단계를 수행하여 작업의 상태 필드를 적절하게 업데이트합니다.	작업 상태를 완료 종결 또는 취소됨으로 변경하면 다음 응답 작업이 실행됩니다.
방화벽의 소스 차단	방화벽에서 이메일 주소를 차단하는 단계를 수행하여 작업의 상태 필드를 적절하게 업데이트합니다.	작업 상태를 완료 종결 또는 취소됨으로 변경하면 다음 응답 작업이 실행됩니다.
이메일 소프트웨어 업데이트	차단 목록에 이메일 주소를 추가하고 작업의 상태 필드를 적절하게 업데이트합니다.	작업 상태를 완료 종결 또는 취소됨으로 변경하면 다음 응답 작업이 실행됩니다. 주: 스팸에 악성 콘텐츠가 포함되어 있습니까? 응답 작업에 아니요라고 답한 경우에도 이 응답 작업이 실행됩니다.
상태를 검토로 설정	필요한 조치가 없습니다.	보안 인시던트의 상태가자동으로 검토로 변경됩니다.

보안 인시던트 무단 접근 워크플로우 템플릿

보안 인시던트 - 무단 액세스 - 템플릿을 사용하면 네트워크에 대한 무단 액세스를 처리하도록 설계된 일련의 작업을 수행할 수 있습니다.

시작하기 전에

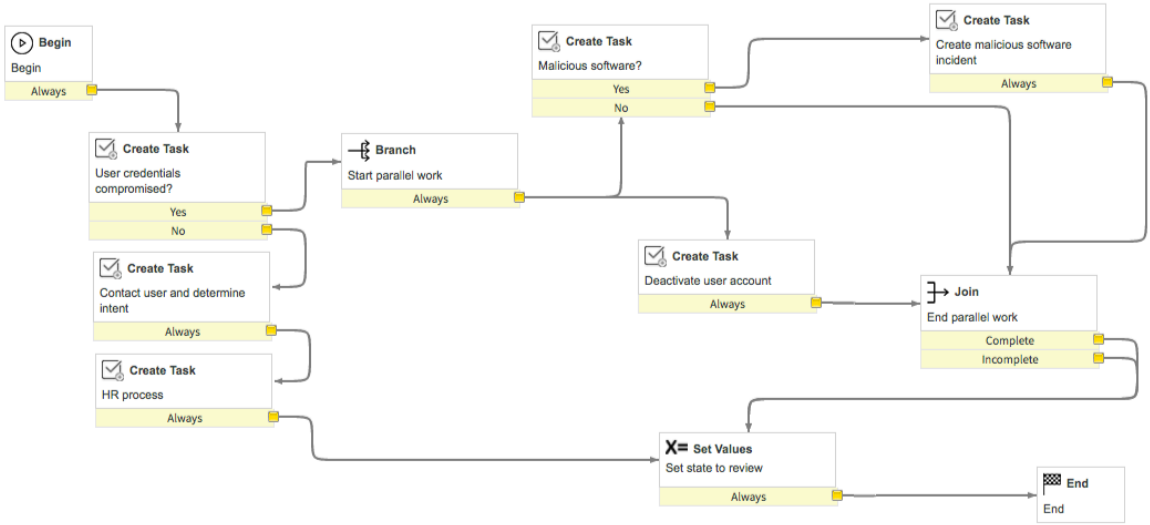
필요한 역할: sn_si.write

이 태스크 정보

워크플로우는 보안 인시던트의 범주 가 무단 액세스로 설정된 경우 트리거됩니다. 이 작업을 수행하면 워크플로우에서 첫 번째 활동에 대한 응답 작업이 생성됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

무단 접근



프로시저

1. 이 잠재적 공격에 대한 보안 인시던트를 열거나 새 보안 인시던트를 생성합니다.
2. 범주에서 무단 액세스를 선택합니다.
3. 레코드를 저장합니다.
4. 아래로 스크롤하여 대응 작업 관련 목록을 엽니다.
   일련의 응답 작업 중 첫 번째 작업이 나타납니다. 기록이 저장될 때마다 이전 작업에 대한 사용자의 응답으로 인해 다음 응답 작업이 생성되거나 워크플로우가 종료됩니다.

무단 액세스 템플릿의 응답 작업

응답 작업	작업	결과
사용자 자격 증명이 손상되었습니까?	사용자 자격 증명이 손상되었는지 여부를 확인합니다. 작업의 결과에서 예 또는 아니요를 선택합니다.	예를 선택하면 다음 두 작업이 병렬로 실행됩니다. ○ 악성 소프트웨어? ○ 사용자 계정 비활성화 아니요를 선택하면 사용자에게 연락하고 의도 확인 작업이 실행됩니다.
악성 소프트웨어?	무단 액세스로 인해 악성 소프트웨어가 도입되었는지 여부를 확인합니다. 작업의 결과에서 예 또는 아니요를 선택합니다.	예를 선택하면 악성 소프트웨어 인시던트 생성 작업이 실행됩니다. 아니요를 선택하면 상태를 검토로 설정 작업이 실행됩니다.
악성 소프트웨어 인시던트 생성	무단 액세스에 대한 보안 인시던트를 생성하는 데 필요한 단계를 수행합니다.	이 작업이 완료되면 상태를 검토로 설정 작업이 실행됩니다.
사용자 계정 비활성화	손상된 사용자 계정을 비활성화하는 데 필요한 단계를 수행합니다.	이 작업이 완료되면 상태를 검토로 설정 작업이 실행됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

응답 작업	작업	결과
사용자에게 연락하고 의도를 파악합니다.	무단 접근을 담당하는 사용자에게 연락하고 접근 시도 이유를 확인하는 데 필요한 단계를 수행합니다.	이 작업이 완료되면 **HR** 프로세스 작업이 실행됩니다.
HR 프로세스	필요한 경우 징계 조치를 구현하기 위해 인사 부서에 연락하는 데 필요한 단계를 수행합니다.	이 작업이 완료되면 상태를 검토로 설정 작업이 실행됩니다.
상태를 검토로 설정	필요한 조치가 없습니다.	보안 인시던트의 상태가자동으로 검토로 변경되고 플로우가 종료됩니다.

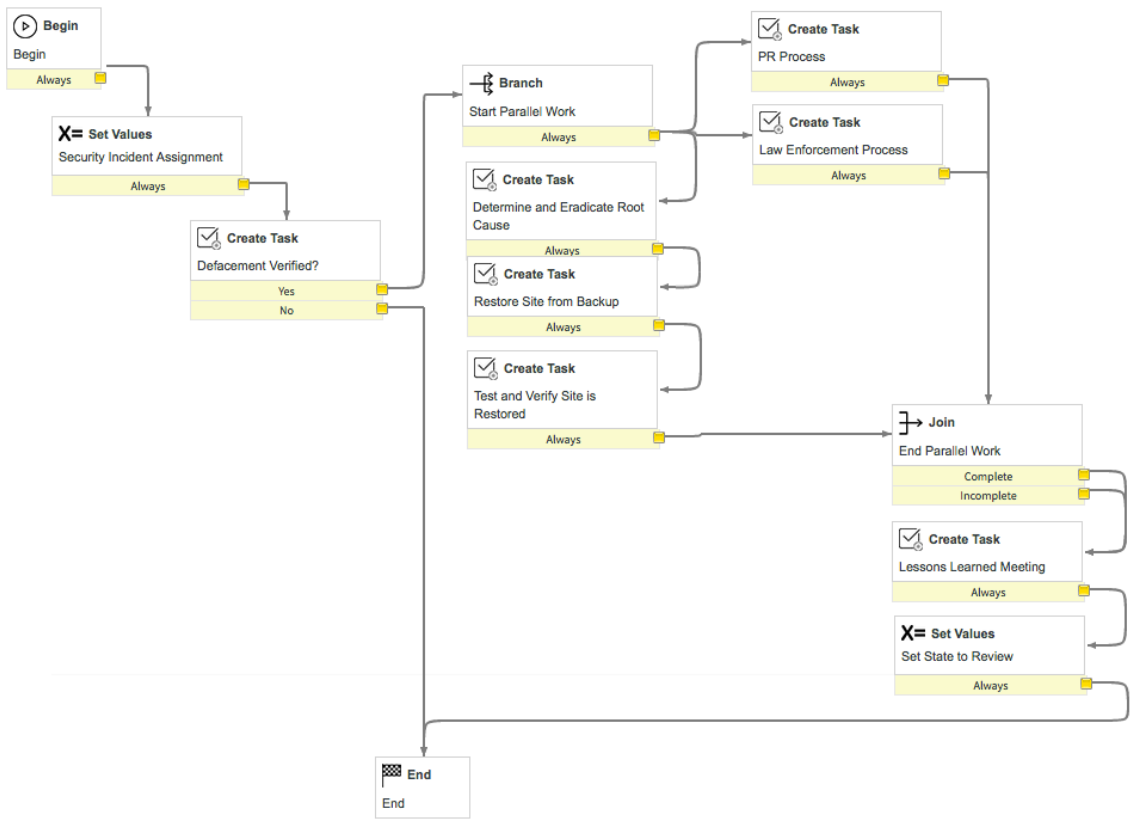
보안 인시던트 웹/BBS 변조 워크플로우 템플릿

보안 인시던트 - 웹/BBS 변조 - 템플릿을 사용하면 조직의 BBS 또는 웹 사이트 중 하나를 대상으로 하는 문서 훼손을 처리하도록 설계된 일련의 작업을 수행할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.write

이 태스크 정보
워크플로우는 보안 인시던트의 범주 가 웹/BBS 변조로 설정된 경우 트리거됩니다. 이 작업을 수행하면 워크플로우에서 첫 번째 활동에 대한 응답 작업이 생성됩니다.

웹/BBS 변조



프로시저

1. 이 웹 또는 BBS 변조 발생에 대한 보안 인시던트를 열거나 새 보안 인시던트를 생성합니다.

2. 범주에서 웹/BBS 변조를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 레코드를 저장합니다.
4. 아래로 스크롤하여 대응 작업 관련 목록을 엽니다.
   일련의 응답 작업 중 첫 번째 작업이 나타납니다. 기록이 저장될 때마다 이전 작업에 대한 사용자의 응답으로 인해 다음 응답 작업이 생성되거나 워크플로우가 종료됩니다.

웹/BBS 변조 템플릿의 응답 작업

응답 작업	작업	결과
보안 인시던트 할당	보고된 각 웹 사이트 또는 BBS 변조 인시던트에 대한 보안 인시던트를 생성합니다.	다음 응답 작업이 실행됩니다.
변조가 검증되었습니까?	웹사이트 또는 BBS가 실제로 훼손되었는지 여부를 확인합니다. 작업의 결과에서 예 또는 아니요를 선택합니다.	예를 선택하면 다음 응답 작업이 실행됩니다. ○ **PR** 프로세스 ○ 법 집행 절차 ○ 근본 원인 파악 및 근절 아니요를 선택하면 플로우가 종료됩니다.
PR 프로세스	웹사이트 또는 BBS가 훼손되었음을 대중에게 알리는 데 필요한 단계를 수행합니다. PR 프로세스가 완료되면 작업의 상태를 적절하게 완료 또는 미완료 로 설정합니다.	학습한 교훈 회의 작업이 실행됩니다.
법 집행 절차	공격과 관련하여 적절한 법 집행 기관과 협력하는 데 필요한 단계를 수행합니다. 작업을 마쳤으면 작업 상태를 적절하게 완료 또는 미완료 로 설정합니다.	학습한 교훈 회의 작업이 실행됩니다.
근본 원인 파악 및 근절	변조의 근본 원인을 발견하고 제거하는 데 필요한 단계를 수행합니다. 작업의 상태 필드를 적절하게 업데이트합니다.	작업 상태를 완료 종결 또는 취소됨으로 변경한 경우 다음 응답 작업이 실행됩니다.
백업에서 사이트 복원	웹 사이트 또는 BBS를 백업 및 복원하는 데 필요한 단계를 수행합니다. 작업의 상태 필드를 적절하게 업데이트합니다.	작업 상태를 완료 종결 또는 취소됨으로 변경한 경우 다음 응답 작업이 실행됩니다.
사이트가 복원되었는지 테스트하고 검증합니다.	사이트가 복원되었는지 확인합니다. 작업을 마쳤으면 작업 상태를 적절하게 완료 또는 미완료 로 설정합니다.	학습한 교훈 회의 작업이 실행됩니다.
학습한 교훈 회의	본 웹 사이트/BBS 변조 인시던트에 대해 수행된 작업을 분류하기 위해 학습한 교훈 회의를 실시합니다.	작업 상태를 종결, 완료 또는 취소됨으로 변경하면 상태를 검토 작업으로 설정 이 실행됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

응답 작업	작업	결과
	작업의 상태 필드를 적절하게 업데이트합니다.	
상태를 검토로 설정	필요한 조치가 없습니다.	보안 인시던트의 상태가자동으로 검토로 변경됩니다. 플로우가 종료됩니다.

보안 인시던트 응답 플로우 템플릿

기본 시스템에는 보안 인시던트 기록을 처리하는 Flow Designer를 사용하여 생성된 일련의 워크플로우 템플릿이 보안 인시던트 응답 포함되어 있습니다.

sn_sec_cmn.admin 역할을 가진 사용자만 보안 운영 워크플로우 템플릿을 추가하거나 편집할 수 있으며 플로우 템플릿을 업데이트하려면 sn_si_admin 역할을 가진 사용자가 필요합니다.

중요한 활성화 정보

워크플로우 편집기로 생성된 워크플로우 템플릿과 플로우 디자이너로 생성된 플로우 템플릿은 모두 기본적으로 비활성화되어 있습니다. 워크플로우 템플릿은 워크플로우 트리거를 사용하여 활성화할 수 있습니다. Flow Designer를 사용하여 Flow Designer 템플릿을 활성화할 수 있습니다.

주:
각 유형의 동일한 템플릿을 활성화하지 않도록 주의해야 합니다. 예를 들어 및 보안 인시던트 기밀 데이터 노출 워크플로우 템플릿보안 인시던트 기밀 데이터 노출 플로우 템플릿를 활성화하지 마십시오. 그럴 경우 워크플로우와 플로우가 모두 실행되고 중복 정보가 생성될 수 있습니다.

보안 인시던트 기밀 데이터 노출 플로우 템플릿

보안 인시던트 - 기밀 데이터 노출 - 템플릿을 사용하면 중요한 데이터의 노출을 처리하도록 설계된 일련의 작업을 수행할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.write

이 태스크 정보
이 플로우는 보안 인시던트의 범주 가 기밀 개인 계정 데이터 노출로 설정되거나 변경될 때 트리거됩니다.

프로시저

1. 중요한 데이터에 대한 노출을 처리할 보안 인시던트를 열거나 새 보안 인시던트를 생성합니다.
2. 범주에서 기밀 개인 계정 데이터 노출을 선택합니다.
3. 레코드를 저장합니다.
4. 아래로 스크롤하여 대응 작업 관련 목록을 엽니다.
   일련의 응답 작업 중 첫 번째 작업이 나타납니다. 기록이 저장될 때마다 이전 작업에 대한 응답으로 인해 다음 응답 작업이 실행되거나 플로우가 종료됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

기밀 데이터 노출 템플릿의 응답 작업

응답 작업	설명	결과
데이터가 민감합니까?	이 보안 인시던트와 관련된 데이터가 중요한 데이터인지 기밀인지 확인합니다. 작업의 결과에서 예 또는 아니요를 선택합니다.	예를 선택한 경우 다음 응답 작업이 실행됩니다. 아니요를 선택하면 플로우가 종료됩니다.
근본 원인을 파악하고 송신을 방지합니다.	공격의 근본 원인을 확인하고 송신 필터링을 추가하여 반출을 중지하고 작업의 상태 필드를 적절하게 업데이트합니다.	작업 상태를 완료 종결 또는 취소됨으로 변경하면 다음 응답 작업이 실행됩니다.
근본 원인과 관련된 노출 제거	근본 원인에 따라 노출을 제거하는 단계를 수행하여 작업의 상태 필드를 적절하게 업데이트합니다.	작업 상태를 완료 종결 또는 취소됨으로 변경하면 다음 응답 작업이 실행됩니다.
잔여 아티팩트 격리	잔여 아티팩트를 격리하는 단계를 수행하여 작업의 상태 필드를 적절하게 업데이트합니다.	작업 상태를 완료 종결 또는 취소됨으로 변경하면 다음 응답 작업이 실행됩니다.
법적 절차	이 분석의 법적 요구 사항을 충족하기 위한 단계를 수행하여 작업의 상태 필드를 적절하게 업데이트합니다.	작업 상태를 완료 종결 또는 취소됨으로 변경하면 다음 응답 작업이 실행됩니다.
PR 프로세스	이 분석의 PR 요구 사항을 충족하는 단계를 수행하여 작업의 상태 필드를 적절하게 업데이트합니다.	작업 상태를 완료 종결 또는 취소됨으로 변경하면 다음 응답 작업이 실행됩니다.
상태를 검토로 설정	필요한 조치가 없습니다.	보안 인시던트의 상태가자동으로 검토로 변경됩니다.
학습한 교훈 회의	학습한 교훈 회의를 수행하여 이 중요한 데이터에 대해 수행된 작업을 분류하고 작업의 상태 필드를 적절하게 업데이트합니다.	작업의 상태를 종결, 완료 또는 취소됨으로 변경하면 보안 인시던트는 종결할 때까지 검토 상태로 유지됩니다.

보안 인시던트 DoS(서비스 거부) 플로우 템플릿

보안 인시던트 - DoS(서비스 거부) - 템플릿을 사용하면 DOS(서비스 거부) 공격을 처리하도록 설계된 일련의 작업을 수행할 수 있습니다.

시작하기 전에

필요한 역할: sn_si.write

이 태스크 정보

이 플로우는 보안 인시던트의 범주 가 **DoS**(서비스 거부)로 설정된 경우에 트리거됩니다.

프로시저

1. 이 서비스 거부 발생에 대한 보안 인시던트를 열거나 새 보안 인시던트를 생성합니다.

2. 범주에서 서비스 거부를 선택합니다.

3. 레코드를 저장합니다.

4. 아래로 스크롤하여 대응 작업 관련 목록을 엽니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

일련의 응답 작업 중 첫 번째 작업이 나타납니다. 기록이 저장될 때마다 이전 작업에 대한 사용자의 응답으로 인해 다음 응답 작업이 생성되거나 워크플로우가 종료됩니다.

DoS(서비스 거부) 템플릿의 응답 작업

응답 작업	작업	결과
대상 비즈니스가 중요합니까?	이 DOS 공격의 대상이 비즈니스에 중요한지 확인합니다. 작업의 결과에서 예 또는 아니요를 선택합니다.	예를 선택하면 우선순위를 중요로 설정 작업이 실행됩니다. 아니요를 선택하면 취약성을 악용하고 있습니까? 작업이 실행됩니다.
우선순위를 중요로 설정	필요한 조치가 없습니다.	보안 인시던트의 우선순위 가 자동으로 중요로 변경되고 취약성이 악용되고 있습니까? 작업이 실행됩니다.
취약성을 악용하고 있습니까?	이 DOS 공격이 소프트웨어 취약점을 악용하는지 여부를 확인합니다. 작업의 결과에서 예 또는 아니요를 선택합니다.	예를 선택하면 긴급 패치 요청 작업이 실행됩니다. 아니요를 선택하면 내부 공격자? 작업이 실행됩니다.
긴급 패치 요청	공격을 받는 시스템에 대한 긴급 패치 요청을 발행합니다. 작업의 상태 필드를 적절하게 업데이트합니다.	작업 상태를 완료 종결 또는 취소됨으로 변경한 경우 다음 응답 작업이 실행됩니다.
내부 공격자입니까?	이 DOS 공격의 소스가 조직 내부에 있는지 확인합니다. 작업의 결과에서 예 또는 아니요를 선택합니다.	예를 선택하면 공격 호스트 격리 작업이 실행됩니다. 아니요를 선택하면 **DOS** 보호 제공자 및/또는 **ISP** 작업 통지가 실행됩니다.
공격 호스트 격리	공격을 담당하는 내부 호스트를 격리하는 데 필요한 단계를 수행합니다. 작업의 상태 필드를 적절하게 업데이트합니다.	이 단계를 완료하면 공격받은 시스템의 시스템 무결성 확인 작업이 실행됩니다.
DOS 보호 제공자 및/또는 ISP에 알림	서비스 거부 보호 공급자 및/또는 인터넷 서비스 공급자에게 연락하여 공격을 알리는 데 필요한 단계를 수행합니다. 작업의 상태 필드를 적절하게 업데이트합니다.	작업 상태를 완료 종결 또는 취소됨으로 변경한 경우 다음 응답 작업이 실행됩니다.
공격받은 시스템의 시스템 무결성 검증	공격받은 컴퓨터의 무결성을 평가하고 유효성을 검사하는 데 필요한 단계를 수행합니다. 작업의 상태 필드를 적절하게 업데이트합니다.	작업 상태를 완료 종결 또는 취소됨으로 변경한 경우 다음 응답 작업이 실행됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

응답 작업	작업	결과
DOS 보호 검토	기존 DOS 보호 및 절차를 검토합니다. 필요한 사항을 변경합니다. 작업의 상태 필드를 적절하게 업데이트합니다.	작업 상태를 완료 종결 또는 취소됨으로 변경한 경우 다음 응답 작업이 실행됩니다.
상태를 검토로 설정	필요한 조치가 없습니다.	보안 인시던트의 상태가자동으로 검토로 변경됩니다. 학습한 교훈 회의 작업이 실행됩니다.
학습한 교훈 회의	학습한 교훈 회의를 수행하여 이 서비스 거부 인시던트에 대해 수행된 작업을 분류합니다. 작업의 상태 필드를 적절하게 업데이트합니다.	작업 상태를 종결, 완료 또는 취소됨으로 변경하면 플로우가 종료됩니다.

보안 인시던트 장비 분실 플로우 템플릿

보안 인시던트 - 장비 분실 - 템플릿을 사용하면 분실된 장비를 처리하도록 설계된 일련의 작업을 수행할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.write

이 태스크 정보
이 플로우는 보안 인시던트의 범주 가 장비 손실로 설정된 경우 트리거됩니다.

프로시저

1. 이 서비스 거부 발생에 대한 보안 인시던트를 열거나 새 보안 인시던트를 생성합니다.
2. 범주에서 장비 손실을 선택합니다.
3. 레코드를 저장합니다.
4. 아래로 스크롤하여 대응 작업 관련 목록을 엽니다.
   일련의 응답 작업 중 첫 번째 작업이 나타납니다. 기록이 저장될 때마다 이전 작업에 대한 응답으로 인해 다음 응답 작업이 생성되거나 플로우가 종료됩니다.

분실 장비 템플릿의 응답 작업

응답 작업	작업	결과
장비에 중요한 데이터가 포함되어 있습니까?	이 보안 인시던트와 관련된 장비에 중요한 정보나 기밀 정보가 포함되어 있는지 확인합니다. 작업의 결과에서 적절하게 예 또는 아니요를 선택합니다.	예를 선택하면 데이터가 암호화되었습니까? 작업이 실행됩니다. 아니요를 선택하면 플로우가 종료됩니다.
데이터가 암호화되었습니까?	분실한 장치의 민감한 데이터가 암호화되었는지 확인합니다. 작업의 결과에서 적절하게 예 또는 아니요를 선택합니다.	예를 선택하면 원격 초기화가 생성되었습니까? 응답 작업이 실행됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

응답 작업	작업	결과
		아니요를 선택하면 잠재적 데이터 손실 인시던트응답 작업 만들기가 실행됩니다.
잠재적 데이터 손실 인시던트 생성	잠재적인 데이터 손실 인시던트를 만드는 데 필요한 단계를 수행합니다. 작업을 마친 후에는 작업의 상태를 적절하게 완료 또는 미완료 로 설정합니다.	원격 초기화가 생성되었습니까? 응답 작업이 실행됩니다.
원격 초기화를 생성했습니까?	분실된 장비의 원격 지우기를 실행하는 데 필요한 단계를 수행합니다. 작업의 결과에서 적절하게 예 또는 아니요를 선택합니다.	법무 프로세스 - 고지 필수 작업이 실행됩니다.
법적 절차 - 공개가 필요합니까?	이 분석의 법적 요구 사항을 충족하는 단계를 수행합니다. 법적 공개가 필요한 경우 예를 선택하고, 필요하지 않은 경우 아니요를 선택합니다.	학습한 교훈 회의 작업이 실행됩니다.
PR 프로세스	이 분석의 PR 요구 사항을 충족하는 데 필요한 단계를 수행합니다. 작업을 마친 후에는 작업의 상태를 적절하게 완료 또는 미완료 로 설정합니다.	상태를 검토로 설정 작업이 실행됩니다.
상태를 검토로 설정	아무 작업도 필요하지 않습니다.	보안 인시던트의 상태가자동으로 검토로 변경됩니다.
학습한 교훈 회의	학습한 교훈 회의를 수행하여 이 장비 손실 인시던트에 대해 수행된 작업을 분류합니다. 작업을 마친 후에는 작업의 상태를 적절하게 완료 또는 미완료 로 설정합니다.	플로우가 종료됩니다.

보안 인시던트 악성 소프트웨어 플로우 템플릿

보안 인시던트 - 악성 소프트웨어 - 템플릿을 사용하면 네트워크에서 악성 소프트웨어를 처리하도록 설계된 일련의 작업을 수행할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.write

이 태스크 정보
이 플로우는 보안 인시던트의 범주 가 악성 코드 활동으로 설정된 경우 트리거됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 이 잠재적 공격에 대한 보안 인시던트를 열거나 새 보안 인시던트를 생성합니다.
2. 범주에서 악성 코드 활동을 선택합니다.
3. 레코드를 저장합니다.
4. 아래로 스크롤하여 대응 작업 관련 목록을 엽니다.
   일련의 응답 작업 중 첫 번째 작업이 나타납니다. 기록이 저장될 때마다 이전 작업에 대한 응답으로 인해 다음 응답 작업이 생성되거나 플로우가 종료됩니다.

악성 소프트웨어 템플릿의 응답 작업

응답 작업	작업	결과
스캔 엔드포인트 - 맬웨어를 찾았습니까?	검사를 실행한 후 맬웨어가 발견되었는지 확인합니다. 작업의 결과에서 예 또는 아니요를 선택합니다.	예를 선택하면 맬웨어 제거 - 성공? 작업이 실행됩니다. 아니요를 선택하면 플로우가 종료됩니다.
맬웨어 제거 - 성공?	맬웨어가 성공적으로 제거되었는지 여부를 확인합니다. 작업의 결과에서 예 또는 아니요를 선택합니다.	예를 선택하면 더 큰 위반이 있었습니까? 작업이 실행됩니다. 아니요를 선택하면 지우기 및 이미지로 다시 설치 작업이 실행됩니다.
지우기 및 이미지로 다시 설치	발견된 맬웨어를 성공적으로 제거하지 못한 경우 이 작업은 맬웨어에 감염된 컴퓨터에서 초기화 및 이미지로 다시 설치를 수행하도록 지시합니다.	작업이 완료되면 상태를 검토로 설정 작업이 실행됩니다.
더 큰 위반이 있었습니까?	악성 소프트웨어로 인한 위반이 처음 생각했던 것보다 큰지 여부를 확인합니다. 작업의 결과에서 예 또는 아니요를 선택합니다.	예를 선택하면 다음 작업이 병렬로 실행됩니다. ○ 법무 검토 ○ HR 검토 ○ 법 집행 검토 아니요를 선택하면 플로우가 종료됩니다.
법무 검토 HR 검토 법 집행 검토	이러한 각 부서에 필요한 단계를 수행하여 악성 소프트웨어를 근절하기 위해 수행한 프로세스를 검토합니다.	작업이 완료되면 상태를 검토로 설정 작업이 실행됩니다.
상태를 검토로 설정	필요한 조치가 없습니다.	보안 인시던트의 상태가자동으로 검토로 변경되고 플로우가 종료됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 인시던트 피싱 플로우 템플릿

보안 인시던트 - 피싱 - 템플릿을 사용하면 네트워크에서 스피어 피싱 이메일을 처리하도록 설계된 일련의 작업을 수행할 수 있습니다.

시작하기 전에

필요한 역할: sn_si.write

이 태스크 정보

이 플로우는 보안 인시던트의 범주 가 스피어 피싱으로 설정된 경우 트리거됩니다.

프로시저

1. 이 잠재적인 스피어 피싱 공격에 대한 보안 인시던트를 열거나 새 보안 인시던트를 생성합니다.
2. 범주에서 스피어 피싱을 선택합니다.
3. 레코드를 저장합니다.
4. 아래로 스크롤하여 대응 작업 관련 목록을 엽니다.
   일련의 응답 작업 중 첫 번째 작업이 나타납니다. 기록이 저장될 때마다 이전 작업에 대한 응답으로 인해 다음 응답 작업이 생성되거나 플로우가 종료됩니다.

Spear 피싱 템플릿의 응답 작업

응답 작업	작업	결과
이것이 피싱 공격입니까?	이것이 피싱 공격인지 확인합니다. 작업의 결과에서 예 또는 아니요를 선택합니다.	예를 선택하면 다음 작업이 병렬로 실행됩니다. ○ 스캔 엔드포인트 - 맬웨어를 찾았습니까? ○ 이메일 보호 소프트웨어 업데이트 ○ 큐에서 읽지 않은 피싱 이메일 제거 - 모든 사용자 아니요를 선택하면 플로우가 종료됩니다.
스캔 엔드포인트 - 맬웨어를 찾았습니까?	검사를 실행한 후 맬웨어가 발견되었는지 확인합니다. 작업의 결과에서 예 또는 아니요를 선택합니다.	예를 선택하면 맬웨어 제거 - 성공? 작업이 실행됩니다. 아니요를 선택하면 상태를 검토로 설정 작업이 실행됩니다.
맬웨어 제거 - 성공?	맬웨어가 성공적으로 제거되었는지 여부를 확인합니다. 작업의 결과에서 예 또는 아니요를 선택합니다.	예를 선택하면 상태를 검토로 설정 작업이 실행됩니다. 아니요를 선택하면 지우기 및 이미지로

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

응답 작업	작업	결과
		다시 설치 작업이 실행됩니다.
지우기 및 이미지로 다시 설치	발견된 맬웨어를 성공적으로 제거하지 못한 경우 이 작업은 맬웨어에 감염된 컴퓨터에서 초기화 및 이미지로 다시 설치를 수행하도록 지시합니다.	작업이 완료되면 상태를 검토로 설정 작업이 실행됩니다.
이메일 보호 소프트웨어 업데이트	피싱 공격으로 확인되면 그에 따라 이메일 보호 소프트웨어를 업데이트하라는 메시지가 표시됩니다.	작업이 완료되면 상태를 검토로 설정 작업이 실행됩니다.
큐에서 읽지 않은 피싱 이메일 제거 - 모든 사용자	모든 사용자에 대해 큐에 있는 피싱 이메일을 제거하는 데 필요한 단계를 수행합니다.	작업이 완료되면 상태를 검토로 설정 작업이 실행됩니다.
상태를 검토로 설정	필요한 조치가 없습니다.	보안 인시던트의 상태가자동으로 검토로 변경됩니다. 보안 인식 교육 일정 예약 작업이 실행됩니다.
보안 인식 교육 예약	직원의 보안 인식을 강화하기 위한 교육을 예약합니다. 작업의 상태 필드를 적절하게 업데이트합니다.	작업이 완료되면 플로우가 종료됩니다.

보안 인시던트 정책 위반 플로우 템플릿

보안 인시던트 - 정책 위반 - 템플릿을 사용하면 보안 정책 위반을 처리하도록 설계된 일련의 작업을 수행할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.write

이 태스크 정보
이 플로우는 보안 인시던트의 범주 가 정책 위반으로 설정된 경우에 트리거됩니다.

프로시저

1. 정책 위반에 대한 보안 인시던트를 열거나 새 보안 인시던트를 생성합니다.
2. 범주에서 정책 위반을 선택합니다.
3. 레코드를 저장합니다.
4. 아래로 스크롤하여 대응 작업 관련 목록을 엽니다.
   일련의 응답 작업 중 첫 번째 작업이 나타납니다. 기록이 저장될 때마다 이전 작업에 대한 응답으로 인해 다음 응답 작업이 생성되거나 플로우가 종료됩니다.

정책 위반 템플릿의 응답 작업

응답 작업	작업	결과
분류 위반	이 위반이 조직의 보안 정책을 위반하는 방법을 분류합니다.	위반자 위반자 대응 권고 작업이 실행됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

응답 작업	작업	결과
	작업을 완료한 후 작업의 상태 필드를 업데이트합니다.	
위반자에게 위반 조언	위반자에게 위반의 성격을 전달합니다. 상태 필드를 전달한 후 작업의 상태 필드를 업데이트합니다.	위반자로부터 승인 받기 응답 작업이 실행됩니다.
위반자로부터 승인 받기	위반자로부터 위반 확인서를 받습니다. 작업의 상태 필드를 적절하게 업데이트합니다.	**HR** 프로세스 응답 작업이 실행됩니다.
HR 프로세스	이 위반에 대해 필요한 모든 정보를 HR에 전달하십시오. 작업의 상태 필드를 적절하게 업데이트합니다.	검토 응답 작업을 검토하도록 상태 설정 작업이 실행됩니다.
상태를 검토로 설정	아무 작업도 필요하지 않습니다.	보안 인시던트의 상태가자동으로 검토로 변경됩니다.
보안 인식 교육 예약	보안 인식 교육을 실시하여 향후 유사한 보안 위반을 방지하는 방법에 대해 직원을 교육합니다. 작업의 상태 필드를 적절하게 업데이트합니다.	작업 상태를 종결, 완료 또는 취소됨으로 변경하면 플로우가 종료됩니다.

보안 인시던트 정찰 플로우 템플릿

정찰은 일반적으로 장치 또는 시스템을 악용하려는 추가 공격에 대한 예비 단계입니다. 보안 인시던트 - 정찰 - 템플릿을 사용하면 네트워크에서 정찰을 처리하도록 설계된 일련의 작업을 수행할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.write

이 태스크 정보
이 플로우는 보안 인시던트의 범주 가 정찰 활동으로 설정된 경우 트리거됩니다.

프로시저

1. 이 잠재적 공격에 대한 보안 인시던트를 열거나 새 보안 인시던트를 생성합니다.
2. 범주에서 정찰 활동을 선택합니다.
3. 레코드를 저장합니다.
4. 아래로 스크롤하여 대응 작업 관련 목록을 엽니다.
   일련의 응답 작업 중 첫 번째 작업이 나타납니다. 기록이 저장될 때마다 이전 작업에 대한 응답으로 인해 다음 응답 작업이 생성되거나 플로우가 종료됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

정찰 템플릿의 응답 작업

응답 작업	작업	결과
정찰 활동이 확인되었습니까?	관찰된 정찰이 검증되었는지 여부를 확인합니다. 작업의 결과에서 예 또는 아니요를 선택합니다.	예를 선택하면 영향을 받는 시스템 식별 작업이 실행됩니다. 아니요를 선택하면 플로우가 종료됩니다.
영향을 받는 시스템 식별	정찰의 영향을 받는 시스템을 결정합니다.	이 작업이 완료되면 법 집행 분석을 위한 정찰 허용? 작업이 실행됩니다.
법 집행 분석을 위한 정찰을 허용하시겠습니까?	법 집행 기관에서 정찰을 분석할지 여부를 결정합니다. 작업의 결과에서 예 또는 아니요를 선택합니다.	예를 선택하면 법 집행 프로세스 작업이 실행됩니다. 아니요를 선택하면 정찰을 방지하기 위한 시스템 업데이트 작업이 실행됩니다.
법 집행 절차	회사에서 정의한 대로 법 집행 프로세스를 수행합니다.	이 작업이 완료되면 시스템을 업데이트하여 정찰 방지 작업이 실행됩니다.
정찰을 방지하기 위해 시스템을 업데이트합니다.	정찰의 영향을 받는 시스템을 업데이트하는 데 필요한 단계를 수행합니다.	이 작업이 완료되면 상태를 검토로 설정 작업이 실행됩니다.
상태를 검토로 설정	필요한 조치가 없습니다.	보안 인시던트의 상태가검토로 자동 변경되고 학습한 교훈 회의 작업이 실행됩니다.
학습한 교훈 회의	교훈 회의를 수행하여 이 정찰 인시던트에 수행된 작업을 분류합니다. 작업의 상태 필드를 적절하게 업데이트합니다.	이 작업이 완료되면 플로우가 종료됩니다.

보안 인시던트 **Rogue** 서버 또는 서비스 플로우 템플릿

보안 인시던트 - Rogue 서버 또는 서비스 - 템플릿을 사용하면 네트워크에 영향을 주는 Rogue 서버 또는 서비스의 활동을 처리하도록 설계된 일련의 작업을 수행할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.write

이 태스크 정보
이 플로우는 보안 인시던트의 범주 가 **Rogue** 서버 또는 서비스로 설정된 경우에 트리거됩니다.

프로시저

1. 이 잠재적 공격에 대한 보안 인시던트를 열거나 새 보안 인시던트를 생성합니다.

2. 범주에서 **Rogue** 서버 또는 서비스 활동을 선택합니다.

3. 레코드를 저장합니다.

4. 아래로 스크롤하여 대응 작업 관련 목록을 엽니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

일련의 응답 작업 중 첫 번째 작업이 나타납니다. 기록이 저장될 때마다 이전 작업에 대한 응답으로 인해 다음 응답 작업이 생성되거나 플로우가 종료됩니다.

Rogue 서버 또는 서비스 템플릿의 응답 작업

응답 작업	작업	결과
Rogue 서버 또는 서비스가 확인되었습니까?	Rogue 서버 또는 서비스와의 연결이 네트워크에서 확인되었는지 확인합니다. 작업의 결과에서 예 또는 아니요를 선택합니다.	예를 선택하면 다음 두 작업이 병렬로 실행됩니다. ○ 영향을 받는 시스템 식별 ○ 잠재적인 데이터 손실? 아니요를 선택하면 플로우가 종료됩니다.
영향을 받는 시스템 식별	Rogue 서버 또는 서비스와의 접촉으로 영향을 받는 시스템을 확인합니다.	이 작업이 완료되면 시스템 업데이트 **- Rogue** 연결 제거 작업이 실행됩니다.
잠재적인 데이터 손실?	Rogue 서버 또는 서비스와의 연결로 인해 잠재적인 데이터 손실이 발생했는지 여부를 확인합니다. 작업의 결과에서 예 또는 아니요를 선택합니다.	예를 선택하면 잠재적 데이터 손실 인시던트 만들기 작업이 실행됩니다. 아니요를 선택하면 시스템 업데이트 **- Rogue** 연결 제거 작업이 실행됩니다.
잠재적 데이터 손실 인시던트 생성	잠재적인 데이터 손실에 대한 보안 인시던트를 생성하는 데 필요한 단계를 수행합니다.	이 작업이 완료되면 시스템 업데이트 **- Rogue** 연결 제거 작업이 실행됩니다.
시스템 업데이트 - 불량 연결 제거	불량 연결을 제거하는 데 필요한 단계를 수행합니다.	이 작업이 완료되면 상태를 검토로 설정 작업이 실행됩니다.
상태를 검토로 설정	필요한 조치가 없습니다.	보안 인시던트의 상태가검토로 자동 변경되고 학습한 교훈 회의 작업이 실행됩니다.
학습한 교훈 회의	단원 회의를 수행하여 이 Rogue 서버 또는 서비스 인시던트에 대해 수행된 작업을 분류합니다. 작업의 상태 필드를 적절하게 업데이트합니다.	이 작업이 완료되면 플로우가 종료됩니다.

보안 인시던트 스팸 플로우 템플릿

보안 인시던트 - 스팸 - 템플릿을 사용하면 네트워크에서 이메일 스팸을 처리하도록 설계된 일련의 작업을 수행할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.write

이 태스크 정보
이 플로우는 보안 인시던트의 범주 가 스팸 소스로 설정되거나 변경될 때 트리거됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 이메일 스팸을 처리할 보안 인시던트를 열거나 새 보안 인시던트를 생성합니다.
2. 범주에서 스팸 소스를 선택합니다.
3. 레코드를 저장합니다.
4. 아래로 스크롤하여 대응 작업 관련 목록을 엽니다.
   일련의 응답 작업 중 첫 번째 작업이 나타납니다. 기록이 저장될 때마다 이전 작업에 대한 응답으로 인해 다음 응답 작업이 생성되거나 플로우가 종료됩니다.

스팸 템플릿의 응답 작업

응답 작업	작업	결과
스팸에 악성 콘텐츠가 포함되어 있습니까?	스팸에 악성 소프트웨어가 포함되어 있는지 확인합니다. 작업의 결과에서 예 또는 아니요를 선택합니다.	예를 선택한 경우 다음 응답 작업이 실행됩니다. ○ 이메일 메시지 격리 ○ 악성 소프트웨어 인시던트 생성 아니요를 선택하면 이메일 소프트웨어 업데이트가 실행됩니다.
악성 소프트웨어 인시던트 생성	보안 인시던트를 만드는 단계를 수행하여 작업의 상태 필드를 적절하게 업데이트합니다.	작업 상태를 완료 종결 또는 취소됨으로 변경하면 이 응답 작업은 다음 세 개의 응답 작업이 완료될 때까지 대기합니다. 이후 보안 인시던트의 상태가 검토로 전환됩니다.
이메일 메시지 격리	스팸을 격리하는 단계를 수행하여 작업의 상태 필드를 적절하게 업데이트합니다.	작업 상태를 완료 종결 또는 취소됨으로 변경하면 다음 응답 작업이 실행됩니다.
방화벽의 소스 차단	방화벽에서 이메일 주소를 차단하는 단계를 수행하여 작업의 상태 필드를 적절하게 업데이트합니다.	작업 상태를 완료 종결 또는 취소됨으로 변경하면 다음 응답 작업이 실행됩니다.
이메일 소프트웨어 업데이트	차단 목록에 이메일 주소를 추가하고 작업의 상태 필드를 적절하게 업데이트합니다.	작업 상태를 완료 종결 또는 취소됨으로 변경하면 다음 응답 작업이 실행됩니다. 주: 스팸에 악성 콘텐츠가 포함되어 있습니까? 응답 작업에 아니요라고 답한 경우에도 이 응답 작업이 실행됩니다.
상태를 검토로 설정	필요한 조치가 없습니다.	보안 인시던트의 상태가자동으로 검토로 변경됩니다.

보안 인시던트 무단 접근 플로우 템플릿

보안 인시던트 - 무단 액세스 - 템플릿을 사용하면 네트워크에 대한 무단 액세스를 처리하도록 설계된 일련의 작업을 수행할 수 있습니다.

시작하기 전에

필요한 역할: sn_si.write

이 태스크 정보

이 플로우는 보안 인시던트의 범주 가 무단 액세스로 설정된 경우 트리거됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 이 잠재적 공격에 대한 보안 인시던트를 열거나 새 보안 인시던트를 생성합니다.
2. 범주에서 무단 액세스를 선택합니다.
3. 레코드를 저장합니다.
4. 아래로 스크롤하여 대응 작업 관련 목록을 엽니다.
   일련의 응답 작업 중 첫 번째 작업이 나타납니다. 기록이 저장될 때마다 이전 작업에 대한 응답으로 인해 다음 응답 작업이 생성되거나 플로우가 종료됩니다.

무단 액세스 템플릿의 응답 작업

응답 작업	작업	결과
사용자 자격 증명이 손상되었습니까?	사용자 자격 증명이 손상되었는지 여부를 확인합니다. 작업의 결과에서 예 또는 아니요를 선택합니다.	예를 선택하면 다음 두 작업이 병렬로 실행됩니다. ○ 악성 소프트웨어? ○ 사용자 계정 비활성화 아니요를 선택하면 사용자에게 연락하고 의도 확인 작업이 실행됩니다.
악성 소프트웨어?	무단 액세스로 인해 악성 소프트웨어가 도입되었는지 여부를 확인합니다. 작업의 결과에서 예 또는 아니요를 선택합니다.	예를 선택하면 악성 소프트웨어 인시던트 생성 작업이 실행됩니다. 아니요를 선택하면 상태를 검토로 설정 작업이 실행됩니다.
악성 소프트웨어 인시던트 생성	무단 액세스에 대한 보안 인시던트를 생성하는 데 필요한 단계를 수행합니다.	이 작업이 완료되면 상태를 검토로 설정 작업이 실행됩니다.
사용자 계정 비활성화	손상된 사용자 계정을 비활성화하는 데 필요한 단계를 수행합니다.	이 작업이 완료되면 상태를 검토로 설정 작업이 실행됩니다.
사용자에게 연락하고 의도를 파악합니다.	무단 접근을 담당하는 사용자에게 연락하고 접근 시도 이유를 확인하는 데 필요한 단계를 수행합니다.	이 작업이 완료되면 **HR** 프로세스 작업이 실행됩니다.
HR 프로세스	필요한 경우 징계 조치를 구현하기 위해 인사 부서에 연락하는 데 필요한 단계를 수행합니다.	이 작업이 완료되면 상태를 검토로 설정 작업이 실행됩니다.
상태를 검토로 설정	필요한 조치가 없습니다.	보안 인시던트의 상태가자동으로 검토로 변경되고 플로우가 종료됩니다.

보안 인시던트 웹/BBS 변조 플로우 템플릿

보안 인시던트 - 웹/BBS 변조 - 템플릿을 사용하면 조직의 BBS 또는 웹 사이트 중 하나를 대상으로 하는 문서 훼손을 처리하도록 설계된 일련의 작업을 수행할 수 있습니다.

시작하기 전에

필요한 역할: sn_si.write

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보
이 플로우는 보안 인시던트의 범주 가 웹/BBS 변조로 설정된 경우 트리거됩니다.

프로시저

1. 이 웹 또는 BBS 변조 발생에 대한 보안 인시던트를 열거나 새 보안 인시던트를 생성합니다.
2. 범주에서 웹/BBS 변조를 선택합니다.
3. 레코드를 저장합니다.
4. 아래로 스크롤하여 대응 작업 관련 목록을 엽니다.
   일련의 응답 작업 중 첫 번째 작업이 나타납니다. 기록이 저장될 때마다 이전 작업에 대한 응답으로 인해 다음 응답 작업이 생성되거나 플로우가 종료됩니다.

웹/BBS 변조 템플릿의 응답 작업

응답 작업	작업	결과
보안 인시던트 할당	보고된 각 웹 사이트 또는 BBS 변조 인시던트에 대한 보안 인시던트를 생성합니다.	다음 응답 작업이 실행됩니다.
변조가 검증되었습니까?	웹사이트 또는 BBS가 실제로 훼손되었는지 여부를 확인합니다. 작업의 결과에서 예 또는 아니요를 선택합니다.	예를 선택하면 다음 응답 작업이 실행됩니다. ○ **PR** 프로세스 ○ 법 집행 절차 ○ 근본 원인 파악 및 근절 아니요를 선택하면 플로우가 종료됩니다.
PR 프로세스	웹사이트 또는 BBS가 훼손되었음을 대중에게 알리는 데 필요한 단계를 수행합니다. PR 프로세스가 완료되면 작업의 상태를 적절하게 완료 또는 미완료 로 설정합니다.	학습한 교훈 회의 작업이 실행됩니다.
법 집행 절차	공격과 관련하여 적절한 법 집행 기관과 협력하는 데 필요한 단계를 수행합니다. 작업을 마쳤으면 작업 상태를 적절하게 완료 또는 미완료 로 설정합니다.	학습한 교훈 회의 작업이 실행됩니다.
근본 원인 파악 및 근절	변조의 근본 원인을 발견하고 제거하는 데 필요한 단계를 수행합니다. 작업의 상태 필드를 적절하게 업데이트합니다.	작업 상태를 완료 종결 또는 취소됨으로 변경한 경우 다음 응답 작업이 실행됩니다.
백업에서 사이트 복원	웹 사이트 또는 BBS를 백업 및 복원하는 데 필요한 단계를 수행합니다. 작업의 상태 필드를 적절하게 업데이트합니다.	작업 상태를 완료 종결 또는 취소됨으로 변경한 경우 다음 응답 작업이 실행됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

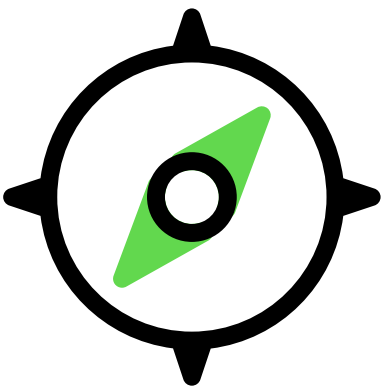
응답 작업	작업	결과
사이트가 복원되었는지 테스트하고 검증합니다.	사이트가 복원되었는지 확인합니다. 작업을 마쳤으면 작업 상태를 적절하게 완료 또는 미완료 로 설정합니다.	학습한 교훈 회의 작업이 실행됩니다.
학습한 교훈 회의	본 웹 사이트/BBS 변조 인시던트에 대해 수행된 작업을 분류하기 위해 학습한 교훈 회의를 실시합니다. 작업의 상태 필드를 적절하게 업데이트합니다.	작업 상태를 종결, 완료 또는 취소됨으로 변경하면 상태를 검토 작업으로 설정 이 실행됩니다.
상태를 검토로 설정	필요한 조치가 없습니다.	보안 인시던트의 상태가자동으로 검토로 변경됩니다. 플로우가 종료됩니다.

위협 인텔리전스

이 ServiceNow# 위협 인텔리전스 애플리케이션을 사용하면 IoC(침입 표시기)를 찾고 위협 인텔리전스 데이터로 보안 인시던트를 보강할 수 있습니다.

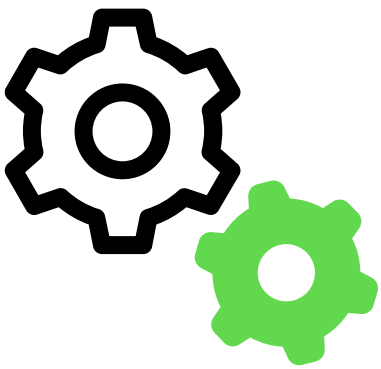
시작하기

탐색



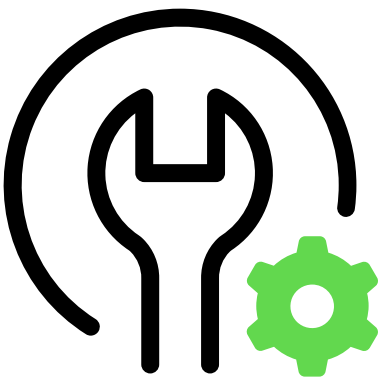
Threat Intelligence 개념과 주요 기능을 알아봅니다.

구성



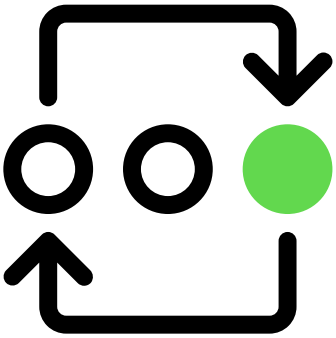
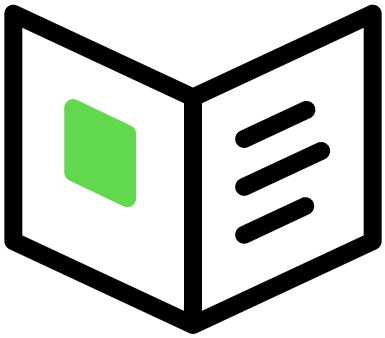
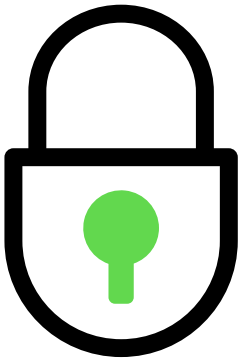
비즈니스 요구 사항을 충족하는 데 필요한 구성요소와 사용자 역할을 설정하고 학습합니다.

관리자



Threat Intelligence 속성을 설정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

통합	사용	MITRE ATT&CK 프레임워크
		
ServiceNow 및 외부 공급업체 애플리케이션과 통합하여 Threat Intelligence 역량을 확장합니다.	IoC(침해 표시기) 및 다양한 아티팩트를 관리합니다.	MITRE-ATT&CK 프레임워크를 관리하여 위협을 신속하게 식별하고 사이버 공격 대응을 조정합니다.

Security Case Management
의심스러운 활동에 대한 정보를 수집하여 보안 케이스 관리를 관리합니다.

학습 자원

- 개발자 교육
- 개발자 설명서
- 애플리케이션과 함께 설치되는 구성요소 찾기

문제 해결 및 도움 받기

- 질문하고 다음에 대한 다른 자원을 살펴보십시오. 위협 인텔리전스 안에 ServiceNow 커뮤니티
- 알려진 오류 포털에서 알려진 오류 문서 검색
- 연락처 고객 서비스 및 지원

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- Security Operations 리소스 라이브러리
- Security Operations 커뮤니티

위협 인텔리전스 이해

이 위협 인텔리전스 애플리케이션을 사용하면 회사의 STIX™(Structured Threat Information Expression) 데이터에 대한 참조 지점을 액세스하고 제공할 수 있습니다. 여기에는 위협 인텔리전스보안 케이스 관리 대상 캠페인 또는 상태 행위자가 조직에 가하는 위협을 분석할 수 있는 수단을 제공하는 애플리케이션이 포함되어 있습니다.

STIX는 사이버 위협 정보를 표준화되고 구조화된 방식으로 설명하기 위한 언어입니다. 위협 전문가는 STIX 데이터 및 TAXII™(Trusted Automated Exchange of Indicator Information) 프로필을 사용하여 공유 사이버 위협 정보를 사용하여 회사 및 다른 소스에서 이전에 식별된 위협을 격리할 수 있습니다. TAXII는 사이버 위협 정보의 광범위한 자동 교환을 가능하게 합니다.

위협 인텔리전스 는 STIX 버전 1.1, 2.0 및 2.1을 지원합니다.

STIX™ 및 TAXII™ 는 MITRE Corporation의 상표입니다.

스토어에서 앱 요청

ServiceNow Store 웹 사이트를 방문하면 사용 가능한 모든 앱을 확인하고 스토어에 요청을 제출하는 방법에 대한 정보를 참조할 수 있습니다. 출시된 모든 앱의 누적 릴리스 정보는 ServiceNow Store 버전 기록 릴리스 정보를 참조하십시오.

도메인 분리 및 위협 인텔리전스

도메인 분리는 보안 인시던트 응답의 위협 인텔리전스 일부로 제공되는 모듈에서 지원됩니다. 도메인 분리를 사용하여 데이터, 프로세스 및 관리 작업을 도메인이라는 논리적 그룹으로 분할할 수 있습니다. 어떤 사용자가 데이터를 보고 액세스할 수 있는지를 포함하여 이러한 분리의 여러 측면을 제어할 수 있습니다.

지원 수준: 기본

- 기본 수준 지원을 포함합니다.
- 비즈니스 논리: 서비스 제공자(SP)가 고객별로 프로세스를 만들거나 수정합니다. 사용 사례는 여러 SP 고객이 단일 인스턴스에서 애플리케이션을 올바르게 사용하는 것을 반영합니다.
- 인스턴스 소유자는 특정 애플리케이션에 필요한 대로 테넌트별 최소 실행 가능한 제품(MVP) 비즈니스 논리 및 데이터 매개변수를 구성해야 합니다.

샘플 사용 사례: 관리자가 한 테넌트에 대해서는 기록이 닫히지만 다른 테넌트에 대해서는 기록이 닫히지 않는 경우 설명이 필요하도록 설정할 수 있어야 합니다.

지원 수준에 대한 자세한 내용은 도메인 분리를 위한 애플리케이션 지원 을 참조하십시오.

개요

위협 인텔리전스 모듈(보안 인시던트 응답 애플리케이션의 일부)에서 도메인 분리를 사용하면 서비스 제공자(SP)가 다음과 같은 방법으로 위협 인텔리전스 리포지토리를 만들고 관리할 수 있습니다.

- 위협 소스 및 신뢰할 수 있는 TAXII(자동 표시기 정보 교환) 프로파일
- 옵저버블

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 영향을 받게 되는 표시기
- 위협 공격 모드/방법 및 고객 기반 전반에 걸친 케이스 관리를 통해 운영 비용을 절감하고 서비스 품질을 높입니다.

워크플로우, 대시보드, 보고서 등을 위한 별도의 고객 작업 공간을 마련하면 고객 데이터가 분리되어 다른 클라이언트에게 노출되지 않습니다.

버전 릴리스별 위협 인텔리전스 도메인 분리 지원

애플리케이션의 일부로 보안 인시던트 응답 Threat Intelligence 모듈에 대한 도메인 분리는 다음 제품 기능을 포함합니다.

- 보안 인시던트 옵저버블은 ID/자격 증명/범위가 인시던트를 생성하는 사용자의 적절한 도메인으로 전달됩니다. 인시던트에서 추출된 옵저버블은 보안 인시던트의 도메인에 저장됩니다.
- 사이버 위협 정보 피드를 제공하는 하나 이상의 TAXII 컬렉션을 다운로드하도록 TAXII 서비스 프로파일을 설정합니다. 구성은 프로파일이 설정되는 도메인에 저장됩니다.
- 구성이 수행되는 도메인의 IOC 리포지토리에 위협 피드 다운로드를 설정합니다.
- 자동으로 정보를 제공하는 위협 인텔리전스 소스의 도메인 또는 사용자가 새로운 공격 모드/방법을 수동으로 추가하는 도메인에서 공격 모드/방법을 생성합니다.
- 케이스와 연관된 인시던트, 옵저버블, CI, 사용자 및 침해 표시기(IOC)의 장기 조사를 위한 케이스 생성 케이스는 사용자가 만든 도메인에 저장됩니다.

주:
위의 모든 경우에 NOW Platform에서 분리된 도메인의 가시성에 대한 중요한 원칙이 적용됩니다. 항상 그렇듯이 상위 도메인의 인시던트는 하위 도메인의 아티팩트를 참조할 수 있지만 그 반대의 경우는 불가능합니다.

에서 도메인 분리가 위협 인텔리전스 작동하는 방식(의 보안 인시던트 응답일부로)

Threat Intelligence는 Professional 및 Enterprise 계층에서 Security Incident Response의 일부이지만 표준 계층에는 포함되지 않습니다. 따라서 별도의 플러그인이 필요합니다.
애플리케이션의 일부인 보안 인시던트 응답 위협 인텔리전스 모듈은 조직의 보안 인시던트와 관련된 위협 인텔리전스 정보를 생성하고 관리합니다. 다음 사용 사례는 도메인 분리를 인식합니다.

- 인시던트 생성 시 보안 인시던트 옵저버블 생성
  - 이메일 파서에서(플랫폼 기반, 사용자 보고 피싱, 사용자 지정)
  - 타사 SIEM(보안 정보 및 이벤트 관리) 저장소의 애플리케이션에서
  - SOC 분석가가 수동으로 입력
- 위협 피드 소스의 옵저버블 컬렉션 - TAXII 컬렉션의 위협 인텔리전스 소스
- 보안 인시던트 옵저버블 관리
  - 옵저버블을 관련 표시기와 연결
  - 옵저버블을 보안 인시던트와 연결
  - 옵저버블을 하위 옵저버블과 연결
  - 옵저버블을 위협 피드 소스에 연결
  - 옵저버블에 보안 주석 추가
- 침해 표시기 관리

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

  - 표시기를 관련 옵저버블과 연결
  - 표시기를 공격 모드/방법과 연결
  - 표시기를 표시기 유형과 연결
  - 위협 피드 소스에 표시기 연결
  - 표시기에 보안 주석 추가
- 케이스 관리
  - 케이스 생성(수동으로 또는 인시던트에서)
  - 새 케이스를 편집하여 상세 정보 추가(케이스 유형 및 심각도 선택, 인시던트, 옵저버블, 구성 항목, 사용자, 표시기 추가)
  - 케이스 삭제

도메인 분리 설정

Threat Intelligence에 대한 도메인 분리를 설정하는 데는 추가 단계가 필요하지 않습니다. 모든 Threat Intelligence 테이블은 인스턴스가 도메인으로 분리된 후 도메인 열을 획득합니다.

도메인 분리 데이터

데이터는 도메인으로 분리될 수 있으며 이는 다음을 의미합니다.

- 한 도메인의 보안 인시던트 옵저버블은 다른 도메인의 범위에서 볼 수 없습니다.
- 한 도메인의 손상 표시기는 다른 도메인의 범위에서 볼 수 없습니다.
- 한 도메인과 관련된 공격 모드/방법은 다른 도메인의 범위에서 볼 수 없습니다.
- 한 도메인과 연결된 TAXII 서비스 프로파일은 다른 도메인의 범위에서 볼 수 없습니다.
- 한 도메인과 연결된 위협 인텔리전스 소스는 다른 도메인의 범위에서 볼 수 없습니다.
- 한 도메인과 관련된 케이스는 다른 도메인의 범위에서 볼 수 없습니다.

위협 인텔리전스 속성은 전역 수준에서 설정되므로 도메인으로 구분되지 않습니다. 설정은 다음과 같습니다.

- IP 주소/URL에 대한 추가 정보를 검색할 도메인 이름
- 검색에 사용할 API 키
- 원격 스캐너로 보내기 전에 로컬 IoC 테이블 조회
- 로컬 옵저버블이 고려되는 일수
- 위협 인텔리전스 소스에서 받지 못한 경우 공격 모드/방법을 비활성으로 표시
- 지정된 일 수 동안 소스에서 수신되지 않은 경우 표시기를 비활성으로 표시

구성

위협 인텔리전스 기능 구성의 모든 측면은 도메인 분리 환경에 독립적입니다.

도메인별로 다음 작업을 구성할 수 있습니다.

1. TAXII 서비스 프로파일 생성
   - 검색 서비스 구성 선택
   - 컬렉션 서비스 구성 선택 - 사용자 및 사용자 그룹에 역할 할당

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

2. 위협 인텔리전스 소스 생성
   - 위협 인텔리전스 정보를 제공하는 REST 서비스를 구성합니다.
   - 위협 인텔리전스 정보 다운로드 예약
   - 소스에 할당할 위협 상세 정보 정보 선택
3. 공격 모드/방법 생성(수동)
   - 소스, 맬웨어 유형, 공격 메커니즘, 위협 액터 유형, 설명, 처리, 의도된 효과, 처음 발견됨, 마지막으로 발견됨
   - 관련 표시기, 하위 공격 모드/방법, 관련 보안 인시던트

     주:
     공격 모드/방법은 위협 피드 소스에서도 자동으로 생성됩니다.

4. 다음 위협 정보 범주에 대한 기본 목록 설정:
   - 공격 메커니즘
   - 디스커버리 방법
   - 피드
   - 표시기 유형
   - 의도된 효과
   - 알림
   - 옵저버블 유형
   - 속도 제한 정의
   - 위협 액터 유형
   - 공격 동기
   - 인프라 유형
   - 맬웨어 역량
   - 맬웨어 유형
   - 보고서 유형
   - 위협 액터 역할
   - 도구 유형

테넌트 도메인이 자체 애플리케이션 데이터를 관리하는 방법

- 테넌트 도메인 소유자는 자신의 TAXII 서비스 프로파일을 생성할 수 있습니다.
- 테넌트 도메인 소유자는 고유한 위협 인텔리전스 소스를 생성할 수 있습니다.
- 테넌트 도메인 소유자는 고유한 공격 모드/방법을 만들 수 있습니다.
- 테넌트 도메인 소유자는 위협 정보 범주에 대한 고유한 기본 목록을 만들 수 있습니다.

주:
비즈니스 논리 및 프로세스를 통해 인스턴스 소유자별로 위협 인텔리전스 소스 다운로드 일정을 도메인 분리할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관련 정보

서비스 제공자용 도메인 분리

위협 인텔리전스 설정

인스턴스에서 실행하려면 위협 인텔리전스 먼저 에서 ServiceNow Store다운로드해야 합니다. 속성을 설정하고 위협 소스를 정의할 수도 있습니다.

위협 인텔리전스 설치

인스턴스에서 실행하려면 위협 인텔리전스 먼저 에서 ServiceNow Store다운로드해야 합니다.

시작하기 전에

설치하기 전에 다음 설정 검사 목록을 완료합니다. 이러한 설정 작업은 원활한 설치 및 구성을 위해 필요합니다.

작업 설정	설명
인스턴스에 필요한 ServiceNow 역할이 있는지 확인합니다.	예상 결과의 설치, 구성 및 검증에 필요한 역할은 다음과 같습니다. • 아직 할당되지 않은 경우 시스템 관리자 〔admin〕가 애플리케이션을 설치하고 위협 관리자 [sn_ti.admin] 역할을 할당합니다. • 위협 관리자 〔sn_ti.admin〕는 구성을 감독하고 예상 결과를 검증합니다.

필요한 역할: 관리자

프로시저

다음에 대한 지침을 따릅니다. 에서 애플리케이션 다운로드 ServiceNow Store.

다음에 수행할 작업

속성 설정 위협 인텔리전스.

위협 인텔리전스 앱과 함께 설치되는 구성요소

위협 인텔리전스 플러그인을 활성화하면 테이블 및 사용자 역할을 포함한 여러 유형의 구성요소가 설치됩니다.

주:
애플리케이션 파일 테이블에는 이 애플리케이션과 함께 설치되는 구성요소가 나열됩니다. 이 테이블에 액세스하는 방법에 대한 지침은 애플리케이션과 함께 설치되는 구성요소 찾기 를 참조하십시오.

이 기능에 대한 데모 데이터를 사용할 수 있습니다.

설치되는 역할

역할 이름 **[name]**	설명	포함하는 역할
위협 관리자 [sn_ti.admin]	모든 위협 속성, SLA 및 알림을 완전히 제어할 수 있습니다.	sn_ti.쓰기

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

역할 이름 **[name]**	설명	포함하는 역할
위협 판독기 〔sn_ti.읽다〕	위협 정보에 대한 읽기 권한이 있습니다.	sn.sec_cmn.int_read
위협 작성자 〔sn_ti.쓰다〕	위협 정보에 대한 쓰기 권한이 있습니다. 공격 모드, 표시기 또는 옵저버블을 삭제할 수 없습니다. 위협 관리자만 삭제할 수 있습니다.	• sn_sec_cmn.int_write • sn_ti.읽기
MITRE 분석가 [sn_ti.mitre_analyst]	이 역할은 모듈 내의 위협 인텔리전스 모듈에 SIR 대한 MITRE-ATT&CK 읽기 권한을 활성화합니다.	• sn_ti.읽기 • sn_si.read

설치되는 테이블

테이블	설명
공격 메커니즘 [sn_ti_attack_mechanism]	취약성을 악용할 때 자주 사용되는 메커니즘을 기반으로 공격 패턴을 계층적으로 구성합니다. 이 뷰의 구성원인 범주는 시스템을 공격하는 데 사용되는 다양한 기술을 나타냅니다.
공격 모드/방식 [sn_ti_attack_mode]	공격 모드와 방법은 사이버 공격자의 행동을 나타냅니다. 그들은 적이 하는 일과 그 일을 하는 방법을 점점 더 세부적으로 특징짓는다.
디스커버리 방법 [sn_ti_discovery_method]	인시던트가 검색된 방법을 표현합니다.
피드 [sn_ti_feed]	위협 개요에서 위협 피드(RSS)를 구성하는 데 사용됩니다.
표시기 공격 모드/방법 [sn_ti_m2m_indicator_attack_mode]	공격 모드/방법을 표시기에 매핑하는 데 사용됩니다.
침해지표(IoC) [sn_ti_indicator]	사이버 보안 컨텍스트 내에서 관심 있는 아티팩트 및/또는 동작을 나타내기 위한 상황별 정보와 결합된 특정 옵저버블 패턴을 전달하는 데 사용됩니다.
침해지표(IoC) 메타데이터 [sn_ti_indicator_metadata]	TAXII 기록을 채우는 데 사용됩니다.
표시기 소스 [sn_ti_m2m_indicator_source]	특정 표시기를 보고하는 모든 소스를 수집하는 데 사용됩니다.
표시기 유형	특정 옵저버블 조건을 식별하는 패턴과 패턴의 의미, 작동 방식 및 시기 등에 대한

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테이블	설명
[sn_ti_indicator_type]	컨텍스트 정보로 구성된 사이버 위협 표시기의 특성을 지정합니다.
연동된 표시기 유형 [sn_ti_m2m_indicator_indicator_type]	표시기를 해당 유형과 연결
인시던트 수 [sn_ti_observable]	옵저버블과 연결된 보안 인시던트 수입니다.
의도된 효과 [sn_ti_intended_effect]	위협 액터의 의도된 효과를 표현하는 데 사용됩니다.
IP 스캔 결과 [sn_ti_ip_result]	IP 조회 결과를 표시하는 데 사용됩니다.
맬웨어 속도 제한 [sn_ti_rate_limit]	조회 소스에 사용할 요율 제한을 정의합니다.
맬웨어 스캔 [sn_ti_scan]	조회입니다. 조회할 항목, 조회 소스, 조회 결과 요약이 포함되어 있습니다.
맬웨어 스캔 큐 항목 [sn_ti_scan_q_entry]	조회 또는 처리를 위해 대기 중인 조회 기록입니다. 명시된 요율 한도 내에서 요청을 용이하게 합니다.
맬웨어 스캔 결과 [sn_ti_scan_result]	조회 결과를 표시합니다.
맬웨어 스캐너 [sn_ti_scanner]	조회 수행에 사용할 외부 공급업체 조회 소스를 정의합니다.
맬웨어 스캐너 속도 제한 [sn_ti_scanner_rate_limit]	조회 소스를 요율 제한과 연결합니다.
맬웨어 유형 [sn_ti_malware_type]	맬웨어 인스턴스 유형을 표현하는 데 사용됩니다.
옵저버블 [sn_ti_observable]	STIX의 옵저버블은 컴퓨터 및 네트워크 작동과 관련된 상태 저장 속성 또는 측정 가능한 이벤트를 나타냅니다.
옵저버블 컨텍스트 유형 [sn_ti_observable_context_type]	옵저버블에 대한 컨텍스트(소스, IP 주소의 대상 등)를 저장합니다.
옵저버블 표시기 [sn_ti_m2m_observable_indicator]	옵저버블을 표시기와 연결하는 데 사용됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테이블	설명
옵저버블 소스 [sn_ti_observable_source]	옵저버블을 위협 소스와 연결하는 데 사용됩니다.
관찰 대상 유형 [sn_ti_observable_type]	IP 주소와 같은 다양한 유형의 옵저버블을 나열합니다.
옵저버블 유형 범주 [sn_ti_observable_type_category]	옵저버블의 첫 번째 분류(예: IP 주소 및 URL)를 저장합니다. 옵저버블 유형을 보다 정확하게 결정하는 데 사용됩니다.
관련 공격 모드/방식 [sn_ti_m2m_attack_mode_attack_mode]	공격 모드를 서로 연관시키는 데 사용됩니다.
관련 옵저버블 [sn_ti_m2m_observables]	옵저버블을 서로 연결하는 데 사용됩니다.
스캔 유형 [sn_ti_scan_type]	파일, URL 및 IP에 대한 초기 기록이 있는 조회 유형의 정의입니다.
보안 케이스 [sn_ti_case]	케이스 관리를 사용하여 만든 보안 케이스 기록을 저장합니다.
보안 케이스 IoC [sn_ti_case_ioc]	옵저버블과 케이스 간의 관계를 관리하는 데 사용됩니다.
보안 케이스 관련 작업 [sn_ti_m2m_case_task]	작업(보안 인시던트, 변경 요청 등)과 보안 케이스 간의 관계를 관리하는 데 사용됩니다.
보안 케이스 관계 제외 [sn_ti_case_relationship_exclusion]	보안 케이스에서 관련 기록의 포함 및 제외에 대한 정의를 제공합니다.
사이팅 [sn_ti_sighting]	사이팅 검색 요청을 실행하는 데 사용되는 옵저버블과 사이팅 검색 상세 정보 결과 사이의 m2m 링크입니다.
사이팅 구성 항목 [sn_ti_m2m_sighting_ci]	구성 항목을 사이팅 검색에 매핑합니다.
사이팅 검색 상세 정보 [sn_ti_sighting_search_detail]	사이팅 검색의 상세 정보(예: 발견된 내부 외부 항목 수)
사이팅 검색 결과 [sn_ti_sighting_search]	사이팅 검색 실행을 위한 헤더입니다.
지원되는 옵저버블 유형	표시기 유형을 유효한 옵저버블 유형과 연결합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테이블	설명
[sn_ti_m2m_ind_type_obs_type]	
지원되는 스캔 유형 [sn_ti_supported_scan_type]	조회 유형을 조회 소스/벤더별 구현에 매핑합니다. 특정 조회 소스가 해당 형식을 지원함을 나타냅니다.
작업 공격 모드/방식 [sn_ti_m2m_task_attack_mode]	공격 모드를 작업과 연결합니다.
작업 표시기 [sn_ti_m2m_task_indicator]	표시기를 작업과 연결합니다.
작업 옵저버블 [sn_ti_m2m_task_observable]	옵저버블을 작업과 연결합니다.
작업 사이팅 [sn_ti_m2m_task_sighting]	사이팅 기록과 관련된 작업 기록(보안 인시던트 및 케이스)을 저장합니다.
TAXII 컬렉션 [sn_ti_taxii_collection]	TAXII 서버에서 임포트할 수 있는 사이버 위협 인텔리전스 피드를 정의합니다.
TAXII 프로파일 [sn_ti_taxii_profile]	사이버 위협 인텔리전스를 공유하기 위한 리포지토리를 정의합니다. TAXII 컬렉션을 포함합니다.
위협 액터 유형 [sn_ti_threat_actor_type]	추정된 의도 및 과거에서 관찰된 행동을 포함하여 사이버 공격 위협을 나타내는 악의적인 행위자(또는 공격자)의 특성을 제공합니다.
위협 인텔리전스 소스 [sn_ti_source]	위협 데이터를 임포트하기 위한 소스를 정의합니다.
연결된 공격 동기 [sn_ti_stix2_m2m_object_attack_motivation]	STIX 객체와 관련된 모든 공격 동기를 수집합니다.
연결된 인프라 유형 [sn_ti_stix2_m2m_infra_type]	인프라를 해당 유형과 연결합니다.
연결된 킬 체인 단계 [sn_ti_stix2_m2m_indicator_kill_chain_phase]	킬 체인 단계를 표시기에 연결합니다.
연결된 킬 체인 단계 [sn_ti_stix2_m2m_object_kill_chain_phase]	킬 체인 단계를 STIX 객체에 연결합니다.
관련된 맬웨어 역량	맬웨어를 해당 기능과 연결합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테이블	설명
[sn_ti_stix2_m2m_malware_capability]	
연결된 맬웨어 유형 [sn_ti_stix2_m2m_malware_malware_type]	맬웨어를 해당 유형과 연결합니다.
연결된 옵저버블 [sn_ti_stix2_m2m_malware_observable]	맬웨어와 관련된 모든 옵저버블을 수집합니다.
연결된 옵저버블 [sn_ti_stix2_m2m_observed_data_observable]	관찰 데이터와 연결된 모든 옵저버블을 수집합니다.
연결된 보고서 유형 [sn_ti_stix2_m2m_report_report_type]	위협 보고서를 해당 유형과 연결합니다.
연결된 위협 액터 역할 [sn_ti_stix2_m2m_threat_actor_threat_actor_role]	위협 액터를 해당 역할과 연결합니다.
연결된 위협 액터 유형 [sn_ti_stix2_m2m_threat_actor_threat_actor_type]	위협 액터를 해당 유형과 연결합니다.
연결된 도구 유형 [sn_ti_stix2_m2m_tool_tool_type]	도구를 해당 유형과 연결합니다.
공격 동기 [sn_ti_stix2_attack_motivation]	공격 동기는 공격의 강도와 지속성을 형성합니다. 위협 액터 및 침입 세트는 일반적으로 근본적인 감정이나 상황을 반영하는 방식으로 행동하며, 이를 통해 방어자에게 공격 방식을 알려줍니다.
공격 패턴 [sn_ti_stix2_attack_pattern]	악의적 사용자가 대상을 손상시키는 데 사용하는 방법을 설명하는 TTP 형식입니다.
캠페인 [sn_ti_stix2_campaign]	특정 대상 집합에 대해 일정 기간 동안 발생하는 일련의 악의적인 활동 또는 공격(웨이브로 명명됨)을 설명하는 적대적 동작 그룹화입니다.
동작 방침 [sn_ti_stix2_course_of_action]	인텔리전스 생산자가 인텔리전스에 대응하여 취할 수 있는 작업에 대한 소비자에 대한 권장 사항입니다.
외부 참조 [sn_ti_stix2_external_reference]	STIX 외부에 표시되는 정보에 대한 포인터입니다.
ID 사이팅 [sn_ti_stix2_m2m_sighting_identity]	사이팅과 관련된 모든 ID를 수집합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테이블	설명
ID [sn_ti_stix2_identity]	실제 개인, 조직 또는 그룹(예: ACME, Inc.) 및 개인, 조직, 시스템 또는 그룹 클래스(예: 금융 부문)입니다.
표시기 외부 참조 [sn_ti_stix2_indicator_external_reference]	표시기와 관련된 외부 참조를 나타냅니다.
표시기 사이팅 [sn_ti_stix2_indicator_sighting]	표시기의 사이팅을 나타냅니다.
인프라 유형 [sn_ti_stix2_infrastructure_type]	다양한 인프라 유형을 나타냅니다.
인프라 [sn_ti_stix2_infrastructure]	특정 목적(예: 공격의 일부로 사용되는 C2 서버, 방어의 일부인 장치 또는 서버, 공격의 대상이 되는 데이터베이스 서버 등)을 지원하기 위한 모든 시스템, 소프트웨어 서비스 및 관련된 물리적 또는 가상 리소스를 설명하는 TTP 유형입니다.
설치된 소프트웨어 [sn_ti_stix2_m2m_malware_analysis_sw]	맬웨어 분석과 관련된 모든 소프트웨어(SCO 소프트웨어 유형)를 수집합니다.
침입 세트 [sn_ti_stix2_intrusion_set]	단일 조직에 의해 조직된 것으로 여겨지는 공통 속성을 가진 적대적 행동 및 자원의 그룹화된 집합입니다.
킬 체인 단계 [sn_ti_stix2_kill_chain_phase]	킬 체인과 연결된 킬 체인 단계를 나타냅니다.
킬 체인 [sn_ti_stix2_kill_chain]	다양한 킬 체인을 나타냅니다.
위치 [sn_ti_stix2_location]	STIX를 통해 제공되는 지리적 위치를 나타냅니다.
맬웨어 분석 [sn_ti_stix2_malware_analysis]	멀웨어 인스턴스 또는 제품군에 대해 수행된 특정 정적 또는 동적 분석의 메타데이터와 결과입니다.
맬웨어 역량 [sn_ti_stix2_malware_capability]	맬웨어 제품군 또는 인스턴스가 나타내는 일반적인 기능을 나타냅니다.
맬웨어 운영 체제 [sn_ti_stix2_m2m_malware_operating_system]	맬웨어와 관련된 모든 운영 체제(SCO 소프트웨어 유형)를 수집합니다.
맬웨어 [sn_ti_stix2_malware]	악성 코드를 나타내는 TTP 형식입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테이블	설명
표시 정의 [sn_ti_stix2_marking_definition]	STIX 객체에 대한 처리 또는 공유 요구 사항을 나타냅니다.
객체 사이팅 [sn_ti_stix2_object_sighting]	STIX 객체의 사이팅을 나타냅니다.
객체-표시기 관계 [sn_ti_stix2_m2m_object_indicator]	STIX 객체와 STIX 표시기 간의 모든 관계를 수집합니다.
객체-객체 관계 [sn_ti_stix2_m2m_object]	표시기를 제외한 STIX 객체와 다른 STIX 객체 간의 모든 관계를 수집합니다.
객체-옵저버블 관계 [sn_ti_stix2_m2m_object_observable]	STIX 옵저버블과 STIX 객체 간의 모든 관계를 수집합니다.
관찰된 데이터 사이팅 [sn_ti_stix2_m2m_sighting_observed_data]	사이팅과 연관된 모든 관찰 데이터 객체를 수집합니다.
관찰 데이터 [sn_ti_stix2_observed_data]	STIX SCO(Cyber-Observable Objects)를 사용하여 파일, 시스템 및 네트워크와 같은 사이버 보안 관련 엔터티에 대한 정보를 전달합니다.
보고서 유형 [sn_ti_stix2_report_type]	위협 보고서의 기본 목적 또는 주제를 나타냅니다.
보고된 옵저버블 [sn_ti_stix2_m2m_malware_analysis_observable]	맬웨어 분석과 관련된 모든 옵저버블을 수집합니다.
STIX V2 객체 [sn_ti_stix2_object]	STIX 객체의 공통 상위 테이블입니다.
STIX V2 사이팅 [sn_ti_stix2_sighting]	STIX 사이팅 테이블의 공통 상위 테이블입니다.
위협 액터 역할 [sn_ti_stix2_threat_actor_role]	위협 액터가 수행할 수 있는 역할을 나타냅니다.
위협 액터 [sn_ti_stix2_threat_actor]	위협 행위자는 악의적인 의도로 운영되는 것으로 여겨지는 실제 개인, 그룹 또는 조직입니다.
위협 그룹화 [sn_ti_stix2_threat_grouping]	몇 가지 공통 컨텍스트를 공유하는 모든 STIX 객체를 그룹화합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테이블	설명
위협 메모 [sn_ti_stix2_threat_note]	해당 STIX 개체에 포함되지 않은 컨텍스트 및 추가 분석을 제공합니다.
위협 의견 [sn_ti_stix2_threat_opinion]	다른 엔터티에서 생성한 STIX 객체에 있는 정보의 정확도 평가를 제공합니다.
위협 보고서 [sn_ti_stix2_threat_report]	보고서는 컨텍스트 및 관련 세부 정보를 포함하여 위협 행위자, 맬웨어 또는 공격 기술에 대한 설명과 같은 하나 이상의 주제에 중점을 둔 위협 인텔리전스 모음입니다. 관련 위협 인텔리전스를 그룹화하여 포괄적인 사이버 위협 스토리로 게시하는 데 사용됩니다.
도구 유형 [sn_ti_stix2_tool_type]	공격을 수행하는 데 사용할 수 있는 도구의 범주입니다.
도구 [sn_ti_stix2_tool]	도구는 위협 행위자가 공격을 수행하는 데 사용하는 합법적인 소프트웨어입니다.
취약성 [sn_ti_stix2_vulnerability]	소프트웨어 및 일부 하드웨어 구성요소(예제 펌웨어)에 있는 계산 논리(예제 코드)의 요구 사항, 설계 또는 구현의 약점 또는 결함을 나타냅니다. 이러한 취약점은 해당 시스템의 기밀성, 무결성 또는 가용성에 부정적인 영향을 미치기 위해 직접적으로 악용될 수 있습니다.

속성 설정 위협 인텔리전스

위협 인텔리전스 속성을 사용하면 API 키 설정을 포함하여 시스템이 작동하는 다양한 측면을 제어할 수 있습니다.

시작하기 전에
필요한 역할: sn_ti.admin

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 관리 〉 속성.
2. 필요에 따라 다음 속성을 설정합니다.

위협 인텔리전스에 대한 속성

속성	설명
IP 주소/URL에 대한 추가 정보를 검색할 도메인 이름 sn_ti.ip_lookup.web_site	IoC 데이터베이스로 추가 정보를 검색하는 데 사용할 도메인 이름입니다. 이 속성은 ThreatAdditionalInfo 스크립트 포함에서 옵저버블 양식에 대한 추가 정보를 채우는 데 사용됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
	기본값: http://api.ipinfodb.com/v3/ip-country/ 주: pinfodb.com 타사 API는 추가 비용 없이 사용할 수 있으며 많은 상용 소프트웨어 프로그램에서 사용됩니다. 다른 도메인 이름으로 바꾸는 경우 다음 필드에 API 키도 제공해야 합니다.
도메인에 사용할 API 키(있는 경우) sn_ti.ip_lookup.api_key	IoC 데이터베이스로 추가 정보를 검색하는 데 사용할 API 키입니다. 이 속성은 ThreatAdditionalInfo 스크립트 포함에서 옵저버블 양식에 대한 추가 정보를 채우기 위해 sn_ti.ip_lookup.web_site 속성과 함께 사용됩니다.
옵저버블이 IoC와 연결되어 있거나 악성으로 확인되면 옵저버블에 대해 자동화된 위협 조회를 실행하지 마십시오. sn_ti.scan_ioc_before_sending 주: 다음 속성(sn_ti.scan_ioc_num_days)에서 기간을 정의해야 합니다.	옵저버블이 구성된 기간(일) 동안 악성이거나 IoC와 관련된 것으로 확인될 때 옵저버블에 대한 자동 위협 조회 실행을 중지하는 옵션입니다. 옵저버블에 대한 위협 조회를 실행해야 하는 경우 수동으로 실행할 수 있습니다. 기본값: 예
기간(일) sn_ti.scan_ioc_num_days	옵저버블의 자동화된 위협 조회를 건너뛸 때까지의 기간을 정의하는 옵션입니다. 기본값(일): 30
이미 실행된 경우 옵저버블에 대해 자동화된 위협 조회를 실행하지 마십시오. sn_ti.enable_threat_lookup_bypass 주: 다음 속성(sn_ti.threat_lookup_bypass_times)에서 기간을 정의해야 합니다.	옵저버블에 대한 위협 조회 결과를 이미 사용할 수 있는 경우, 구성된 기간이 지날 때까지 동일한 옵저버블에 대한 자동화된 위협 조회 재실행을 건너뛸 수 있는 옵션이 있습니다. 기본값: 아니오 주: 이 속성을 사용하도록 설정하는 경우 적절한 값을 추가해야 합니다.
기간(분) sn_ti.threat_lookup_bypass_time	옵저버블의 자동화된 위협 조회를 다시 실행할 수 있는 기간을 정의하는 옵션입니다. 기본값(분): 0

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
옵저버블 찾기에 대한 사용자 재정의의 유효 기간을 설정합니다. sn_ti.enable_observable_finding_system_override 주: 다음 속성 (sn_ti.observable_finding_override_expiry)에서 유효성을 정의해야 합니다.	옵저버블 결과에 대한 사용자 재정의의 유효 기간을 설정하는 옵션입니다. 이 유효 기간 동안 옵저버블의 위협 조회 찾기가 기본 시스템에 의해 변경되지 않습니다. 기본값: 아니요. 주: 이 속성을 사용하도록 설정하는 경우 적절한 값을 추가해야 합니다.
유효 기간(분) sn_ti.observable_finding_override_expiry	옵저버블 결과의 유효 기간을 정의하는 옵션입니다. 기본값(분): 없음
지정된 일수 동안 어떤 소스에서도 공격 모드/방법이 수신되지 않으면 비활성으로 표시 sn_ti.attack_mode_inactivate_days	기록이 비활성으로 표시되기 위해 공격 모드/방법을 마지막으로 수신한 날로부터의 일수입니다. 기본값: 360 주: 활성 확인란은 기본적으로 공격 모드/방법 양식에 표시되지 않습니다. 그러나 추가할 수 있습니다. 공격 모드/방법이 비활성 상태이면 다른 형태에서 선택할 수 없습니다.
지정된 일수 동안 어떤 소스에서도 표시기가 수신되지 않으면 비활성으로 표시 sn_ti.indicator_inactivate_days	비활성으로 표시할 기록에 대한 표시기를 마지막으로 받은 시점부터 일수입니다. 기본값: 180 주: 활성 확인란은 기본적으로 표시기 양식에 표시되지 않습니다. 그러나 추가할 수 있습니다. 표시기가 비활성 상태이면 다른 양식에서 선택할 수 없습니다.
구문 분석할 수 있는 STIX 첨부 파일의 최대 페이로드 크기(MB)입니다. sn_ti.stix.max_payload_size	구문 분석할 수 있는 STIX 첨부 파일의 최대 페이로드 크기를 지정합니다. 기본값: 없음 허용되는 최대값: 제한 없음.
TAXII 수집 데이터를 가져오기 위해 대기 하는 아웃바운드 HTTP 연결의 최대 시간 (초)	TAXII 수집 데이터의 다음 패킷을 가져오기 전에 아웃바운드 HTTP 연결이 대기하는 최대 시간을 지정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
sn_ti.taxii.http.max_timeout	기본값: 300
TAXII 서버에서 하나의 REST 호출로 검색된 최대 객체 수(TAXII 버전 2.0 및 2.1에만 적용) sn_ti.taxii.max_page_size	한 페이지에 대해 TAXII 서버에서 하나의 REST 호출로 검색되는 최대 객체 수를 지정합니다. 기본값: 5000 허용되는 최대값: 50000
실패한 TAXII 2.X REST 호출에 대한 최대 재시도 횟수 sn_ti.taxii2.retry_count	실패한 TAXII REST 호출에 대한 최대 재시도 횟수를 지정합니다. 기본값: 3

3. 저장을 클릭합니다.

위협 소스 정의

위협 소스 목록을 위협 인텔리전스 유지 관리할 수 있습니다. 각 소스에는 소스가 쿼리되는 빈도를 정의하는 기능이 포함되어 있습니다. 요청 시 위협 소스를 실행하여 필요한 STIX(Structured Threat Information eXpression) 데이터를 임포트할 수도 있습니다.

시작하기 전에
필요한 역할: sn_ti.admin

이 태스크 정보
위협 인텔리전스 는 위협 관련 정보를 가져오기 위해 STIX 및 TAXII(신뢰할 수 있는 표시기 정보의 자동 교환)라는 두 가지 기술을 사용합니다.

STIX는 침해 지표(IoC) 활동(예: IP 주소 및 파일 해시)뿐만 아니라 공격 모드/방법과 같은 위협에 대한 컨텍스트 정보를 포함하는 광범위한 사이버 위협 정보 세트를 나타내기 위한 표준화되고 구조화된 언어를 제공하며, 사이버 적의 동기, 역량 및 활동을 보다 완벽하게 특성화합니다. 따라서 STIX 데이터는 조직이 사이버 위협을 가장 잘 방어할 수 있는 방법에 대한 귀중한 정보를 제공합니다.

TAXII(신뢰할 수 있는 지표 정보의 자동 교환)는 사이버 위협 정보의 자동 교환을 용이하게 하는 데 사용됩니다. TAXII는 사이버 위협의 탐지, 예방 및 완화를 위해 조직 및 제품/서비스 경계를 넘어 실행 가능한 사이버 위협 정보를 공유할 수 있는 일련의 서비스 및 메시지 교환을 정의합니다. TAXII 프로파일은 STIX 형식 정보를 공유하기 위한 리포지토리로 설정할 수 있습니다. 각 프로필에는 하나 이상의 TAXII 컬렉션 또는 피드가 포함되어 있습니다.

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 소스 〉 위협 소스.
2. 새로 만들기를 클릭합니다.
3. 양식의 필드에 적절히 입력합니다.

필드	설명
이름	위협 소스의 이름입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
애플리케이션	이 기록을 포함하는 애플리케이션입니다.
활성	위협 소스를 활성화하려면 이 확인란을 선택합니다.
고급	통합 공장 스크립트 및 보고서 프로세서 필드에 스크립트를 표시하려면 이 확인란을 선택합니다.
설명	이 위협 소스에 대한 설명입니다.

4. 일정 섹션의 필드에 적절히 입력합니다.

필드	설명
실행	통합을 실행할 빈도(매일, 매주, 주기적으로 등)입니다. 앞에서 언급했듯이 이 필드의 설정에 따라 후속 필드가 표시됩니다.
일	통합을 실행하려는 날짜입니다. ○ 실행 필드에서 매주를 선택한 경우 이 필드에 요일이 표시됩니다. ○ 실행 필드에서 매월을 선택한 경우 이 필드에 월의 일수가 표시됩니다.
시간	통합을 시작할 시간입니다.
반복 간격	실행 필드에서 주기적으로를 선택한 경우 이 필드에는 통합이 다시 실행되기까지의 일 수와 시간이 표시됩니다.
시작 중	실행 필드에서 주기적으로를 선택한 경우 이 필드에는 주기적인 업데이트의 시작점으로 사용할 날짜 및 시간이 표시됩니다.
조건부	조건부 매개변수를 추가하려면 이 필드를 선택합니다.
조건	조건부 확인란을 선택한 경우 여기에 조건을 입력합니다.

5. 위협 상세 정보 섹션의 필드에 적절한 정보를 입력합니다.

필드	설명
표시기	데이터에서 명시적으로 제공하지 않는 경우 사용할 표시기입니다. 차단 목록의 경우 비어 있는 경우 각 옵저버블에 대해 새 표시기가 생성됩니다.
표시기 유형	생성된 표시기에 사용할 표시기 유형으로, 데이터에서 표시기 유형을 명시적으로 제공하지 않습니다.
공격 모드/방식	데이터가 명시적으로 제공하지 않을 때 사용할 공격 모드/방법입니다.
관찰 대상 유형	생성된 옵저버블에 사용할 옵저버블 유형으로, 데이터에서 옵저버블 유형을 명시적으로 제공하지 않습니다.〔SI1〕
가중치	신뢰도 계산에 사용할 이 소스의 가중치 값을 입력합니다.

주:
표시기, 표시기 유형, 공격 모드/방법 및 옵저버블 유형 필드의 사용은 구현에 따라 다릅니다. 기본 프로세서인 SimpleBlocklistProcessor는 도구 설명에 설명된 대로 동작합니다. 그러나 TAXII 위협 소스는 완전히 데이터 기반입니다. 모든 사용자 지정 위협 소스 프로세서는 자체 전략을 사용할 수 있습니다. 이러한 필드는 기본적으로 통합/프로세서에 노출되는 항목이며 구현에 따라 사용 방법이 결정됩니다.

6. 소스 상세 정보 섹션의 필드에 적절한 정보를 입력합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
엔드포인트	위협 소스에 액세스하는 위협 인텔리전스웹 서비스 엔드포인트 URL을 입력합니다. 잠금 아이콘을 클릭하여 URL을 잠급니다.
REST 메시지 사용	위협 소스에 액세스하기 위해 REST 메시지가 필요한 경우 이 확인란을 선택합니다. **REST** 메시지 및 **REST** 메서드 필드가 필수가 됩니다.
REST 메시지	조회 아이콘을 클릭하고 목록에서 REST 메시지를 선택하거나 신규 를 클릭하여 새 REST 메시지를 정의합니다.
REST 메서드	조회 아이콘을 클릭하고 목록에서 REST 메서드를 선택하거나 새로 만들기를 클릭하여 새 REST 메서드를 정의합니다.
통합 스크립트	기본 통합 스크립트는 **SimpleRESTSecurityDataIntegration**입니다. 간단한 REST 호출을 실행하고 응답을 첨부 파일로 저장한 다음 첨부 파일을 프로세서에 반환합니다. 이 스크립트는 대부분 조직의 요구 사항을 충족합니다. 그러나 원하는 경우 조회 아이콘을 클릭하고 다른 통합 스크립트를 선택하거나 새 통합 스크립트를 정의할 수 있습니다.
통합 공장 스크립트	고급 확인란을 선택하면 이 필드에 통합 스크립트를 구성하기 위한 실제 스크립트가 표시됩니다. 필요에 따라 스크립트를 편집할 수 있습니다. 이 기능은 사용자 지정 구현에 유용합니다. 기본 시스템의 통합에는 일반적으로 사용자 지정 생성자 논리가 필요하지 않습니다.
보고서 프로세서	기본 통합 스크립트는 **SimpleBlocklistProcessor**입니다. 이 스크립트는 단순 차단 목록(단순, URL 또는 IP 주소와 같은 옵저버블이 있는 단일 열 문서를 의미)을 수락하고 옵저버블을 생성하는 간단한 프로세서입니다. 다양한 위협 상세 정보 필드를 사용하여 옵저버블이 생성될 때 설정할 필드를 결정합니다.
프로세서 공장 스크립트	고급 확인란을 선택하면 이 필드에 프로세서를 구성하기 위한 실제 스크립트가 표시됩니다. 필요에 따라 스크립트를 편집할 수 있습니다. 이 스크립트는 일반적으로 사용자 지정 구현에 유용합니다. 기본 시스템의 통합에는 일반적으로 사용자 지정 생성자 논리가 필요하지 않습니다.

7. 제출을 클릭합니다.

> **주:**
> 위협 소스의 페이지 매김을 구성하는 방법에 대한 자세한 내용은 KB1213825 문서를 참조하십시오.

TAXII 프로파일 생성

STIX 형식 정보를 공유하기 위해 TAXII 프로필을 유지할 수 있습니다. 각 프로필에는 하나 이상의 TAXII 컬렉션 또는 피드가 포함되어 있습니다.

시작하기 전에
필요한 역할: sn_ti.admin

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 소스 〉 **TAXII** 프로파일.

2. 새로 만들기를 클릭합니다.

3. 다음 필드를 적절하게 작성합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 검색 서비스 구성 섹션의 필드에 적절히 입력합니다.

5. 수집 서비스 구성 섹션의 필드에 적절히 입력합니다.

6. 제출을 클릭합니다.

IoC 리포지토리

IoC 저장소에는 STIX 개체가 포함되어 있으며 이러한 각 개체에는 특정 정보가 포함되어 있습니다.

관계를 통해 STIX 객체를 결합하면 사이버 위협 인텔리전스(CTI)를 쉽고 복잡하게 표현할 수 있습니다.

위협 인텔리전스 는 STIX 버전 1.1, 2.0 및 2.1을 지원합니다.

공격 모드 및 방법

전술, 기술 및 절차(TTP)라고도 하는 공격 모드 및 방법은 사이버 공격자의 행동 방식을 나타냅니다. 그들은 이러한 적들이 하는 일과 그 일을 하는 방법을 점점 더 세부적으로 특징짓는다. 공격 모드 및 방법은 1.1에 STIX 적용됩니다.

예를 들어, 공격 모드/방법은 멀웨어를 사용하여 신용 카드 자격 증명을 훔치는 것일 수 있습니다. 또는 다른 관련 전술(낮은 수준의 세부 사항)은 악성 코드가 포함된 첨부 파일이 포함된 대상 이메일을 보내는 것일 수 있으며, 이 이메일은 열 때 실행되고, 키 입력에서 신용 카드 정보를 캡처하고, HTTP를 사용하여 명령 및 제어 서버와 통신하여 정보를 전송합니다.

공격 모드 및 방법은 1.1에 STIX 적용됩니다.

공격 모드/방법 정의

공격 모드 및 방법은 STIX 데이터와 함께 가져오지만 필요에 따라 새 모드/방법을 추가할 수 있습니다.

시작하기 전에
필요한 역할: sn_ti.admin

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **IoC** 리포지토리 〉 공격 모드/방식.

2. 새로 만들기를 클릭합니다.

3. 양식의 필드에 적절히 입력합니다.

필드	설명
분류 태그 선택	기록에 메타데이터를 추가하기 위해 분류 태그를 설정하고 활성화한 경우 하나 이상의 태그를 선택하여 공격 모드/방법의 민감도 정도를 지정할 수 있습니다. 분류 태그를 설정하거나 활성화하지 않은 경우에는 이 드롭다운 목록이 표시되지 않습니다.
직위	이 공격 모드/방법에 대한 설명이 포함된 이름을 입력합니다.
맬웨어 유형	이 공격 모드/방법에 대한 맬웨어 유형을 선택하십시오. 사용 가능한 맬웨어 유형은 벤더 서버에서 STIX 데이터로 검색됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
소스	이 공격 모드/방법에 대한 위협 데이터 소스를 선택합니다. 일부 데이터 소스는 기본 시스템에 포함되어 있습니다. 필요에 따라 새 데이터 소스를 생성할 수 있습니다.
공격 메커니즘	이 공격 모드/방법에 대한 공격 메커니즘을 선택하십시오. 공격 메커니즘은 시스템을 공격하는 데 사용되는 다양한 기술을 나타냅니다. 사용 가능한 공격 메커니즘은 공급업체 서버에서 STIX 데이터로 검색됩니다.
처음으로 발견됨	이 날짜는 벤더 서버에서 STIX 데이터로 검색됩니다.
마지막으로 발견됨	이 날짜는 벤더 서버에서 STIX 데이터로 검색됩니다.
위협 액터 유형	이 공격 모드/방법에 대한 위협 액터 유형을 선택합니다. 위협 행위자 유형은 사이버 공격 위협을 나타내는 악의적인 행위자(또는 공격자)를 특징으로하며, 여기에는 추정된 의도 및 역사적으로 관찰된 행동이 포함됩니다. 사용 가능한 위협 액터 유형은 벤더 서버에서 STIX 데이터로 검색됩니다.
설명	공격 모드/방법에 대한 설명을 입력합니다.
처리	이 공격 모드/방법을 처리하는 방법에 대한 지침을 입력합니다.
의도된 효과	이 유형의 공격에 대해 의도된 효과를 입력합니다.

4. 양식 헤더를 마우스 오른쪽 버튼으로 클릭하고 저장을 클릭합니다.
   다음 관련 목록을 보고 추가 정보를 볼 수 있습니다.

관련 목록	설명
관련 표시기	위협 소스에서 식별한 관련 IoC(침해 표시기)를 나열합니다.
하위 공격 모드/방식	상위 공격 모드/방법의 하위 공격 모드/방법을 나열합니다.
관련된 작업	상위 공격 모드/방법과 관련된 변경 내용을 나열합니다.

공격 모드/방법에 **IoC** 추가

지표를 STIX 데이터로 임포트하는 것 외에도 공격 모드/메소드에 IoC를 수동으로 추가할 수 있습니다.

시작하기 전에
필요한 역할: sn_ti.admin

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **IoC** 리포지토리 〉 공격 모드/방식.
2. IoC를 추가하려는 공격 모드를 클릭합니다.
3. 관련 표시기 관련 목록을 클릭합니다.
4. 편집을 클릭합니다.
5. 필요한 경우 필터를 사용하여 추가할 IoC를 찾습니다.
6. 슬러쉬버킷을 사용하여 관련 표시기 목록에 IoC를 추가합니다.
7. 저장을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관련 공격 모드 방법 추가

공격 모드/방법을 STIX 데이터로 가져오는 것 외에도 관련 공격 모드/방법을 수동으로 추가할 수 있습니다.

시작하기 전에
필요한 역할: sn_ti.admin

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **IoC** 리포지토리 〉 공격 모드/방식.
2. 관련 공격 모드/방법을 추가하려는 공격 모드를 클릭합니다.
3. 하위 공격 모드/방법 관련 목록을 클릭합니다.
4. 편집을 클릭합니다.
5. 필요에 따라 필터를 사용하여 현재 모드와 연결하려는 공격 모드/방법을 찾습니다.
6. 슬러쉬버킷을 사용하여 공격 모드/방법을 하위 공격 모드/방법 목록에 추가합니다.
7. 저장을 클릭합니다.

공격 모드/방법에 관련 작업 추가

관련 작업(예: 변경 사항 및 인시던트)을 STIX 데이터로 임포트하는 것 외에도 공격 모드/방법에 수동으로 추가할 수 있습니다.

시작하기 전에
필요한 역할: sn_ti.admin

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **IoC** 리포지토리 〉 공격 모드/방식.
2. 연결된 작업을 추가할 공격 모드를 클릭합니다.
3. 연관된 작업 관련 목록을 클릭합니다.
4. 편집을 클릭합니다.
5. 필요에 따라 필터를 사용하여 공격 모드/방법과 연결할 작업을 찾습니다.
6. 슬러쉬버킷을 사용하여 연관된 작업 목록에 작업을 추가합니다.
7. 저장을 클릭합니다.

영향을 받게 되는 표시기

침해 표시기(IoC)는 네트워크 또는 운영 체제에서 관찰되는 아티팩트로, 침입을 나타낼 가능성이 높습니다. 일반적인 IoC는 바이러스 서명 및 IP 주소, 맬웨어 파일 또는 URL의 MD5 해시 또는 도메인 이름입니다. IoC는 1.1 및 2.x에 STIX 적용됩니다.

IoC는 단일 옵저버블 또는 옵저버블 컬렉션(예: 알려진 단일 잘못된 URL 또는 특정 파일 및 몇 개의 특정 레지스트리 키 값 존재)일 수 있습니다.

인시던트 대응 및 컴퓨터 포렌식 프로세스에서 IoC가 식별되면 침입 탐지 시스템 및 바이러스 백신 소프트웨어를 사용하여 향후 공격 시도를 조기에 탐지하는 데 사용할 수 있습니다.

IoC는 1.1 및 2.x에 STIX 적용됩니다.

IoC 보기

지표라고도 하는 IoC는 일반적으로 위협 데이터 소스에서 STIX 데이터로 검색됩니다. 필요한 경우 IoC를 만들 수도 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_ti.write

프로시저

1. 예약된 작업이 정의된 데이터 소스에서 IoC 데이터를 검색한 후 다음으로 이동합니다. 위협 인텔리전스 〉 **IoC** 리포지토리 〉 표시기.
   검색된 IoC가 나열됩니다.
2. 보려는 IoC를 클릭합니다.
3. 다음 정보가 표시됩니다.

필드	설명
분류 태그 선택	레코드에 메타데이터를 추가하기 위해 보안 태그를 설정하고 활성화한 경우 하나 이상의 태그를 선택하여 IoC의 민감도를 지정할 수 있습니다. 보안 태그를 설정하거나 활성화하지 않은 경우에는 이 드롭다운 목록이 표시되지 않습니다.
직위	이 표시기를 설명하는 이름입니다.
처음으로 발견됨	시스템에서 이 표시기가 처음 관찰된 날짜입니다.
마지막으로 발견됨	시스템에서 이 표시기가 관찰된 최근 날짜입니다.
발생한 횟수	표시기가 발생한 횟수입니다.
소스 수	정의된 위협 소스에서 표시기를 임포트한 횟수입니다.
메모	표시기에 대한 추가 메모입니다. 이 필드에는 JSON 키/값 쌍도 포함될 수 있습니다.

4. 다음 관련 목록 중 하나를 클릭하여 추가 정보를 볼 수 있습니다.

관련 링크 및 관련 목록	설명
관계 표시	STIX 객체의 관계를 볼 수 있는 STIX 시각화 도우미를 엽니다. 관계 표시는 객체에 연관된 객체가 있는 경우에만 나타납니다.
관련 옵저버블	현재 표시기에 연결된 옵저버블을 나열합니다.
관련 공격 모드/방식	이 표시기와 관련된 것으로 확인된 관련 공격 모드/방법을 나열합니다.
연결된 유형	이 IoC와 관련된 다른 표시기 유형을 나열합니다.
표시기 소스	소스의 신뢰도와 함께 이 표시기의 소스를 나열합니다.
관련된 작업	IoC와 관련된 모든 작업, 변경 및 인시던트를 나열합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관련 링크 및 관련 목록	설명
표시기 메타데이터	메모 필드에 유효한 JSON 키/값 쌍이 포함되어 있는 경우, 구문 분석되고 표시됩니다. JSON 키/값 쌍이 없거나 JSON이 잘못된 경우 이 관련 목록이 표시되지 않습니다.
보안 주석	
표시기 외부 참조	
연결된 킬 체인 단계	이 객체와 연결된 킬 체인 단계를 나열합니다.
공격 패턴	이 객체와 관련된 공격을 분류하는 데 도움이 되는 공격 패턴을 나열합니다.
캠페인	이 객체와 연관된 캠페인을 나열합니다.
침입 세트	이 객체와 관련된 공통 속성이 있는 일련의 적대적 동작 및 자원을 나열합니다.
맬웨어	이 객체와 연결된 악성 코드를 나열합니다.
위협 액터	이 객체와 관련하여 악의적인 의도를 가지고 행동하는 개인, 그룹 또는 조직을 나열합니다.

IoC에 관련 옵저버블 추가

옵저버블을 STIX 데이터로 임포트하는 것 외에도 관련 옵저버블을 IoC에 수동으로 추가할 수 있습니다.

시작하기 전에
필요한 역할: sn_ti.write

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **IoC** 리포지토리 〉 표시기.
2. 관련 옵저버블을 추가할 표시기를 클릭합니다.
3. 관련 옵저버블 관련 목록을 클릭합니다.
4. 편집을 클릭합니다.
5. 필요한 경우 필터를 사용하여 IoC와 연결하려는 옵저버블을 찾습니다.
6. 슬러시버킷을 사용하여 옵저버블을 관련 옵저버블 목록에 추가합니다.
7. 저장을 클릭합니다.

IoC에 관련 공격 모드/방법 추가

관련 공격 모드/방법을 STIX 데이터로 가져오는 것 외에도 관련 공격 모드/방법을 IoC에 수동으로 추가할 수 있습니다.

시작하기 전에
필요한 역할: sn_ti.write

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **IoC** 리포지토리 〉 표시기.
2. 관련 공격 모드/방법을 추가할 표시기를 클릭합니다.
3. 관련 공격 모드/방법 관련 목록을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 편집을 클릭합니다.
5. 필요한 경우 필터를 사용하여 IoC와 연결하려는 공격 모드/방법을 찾습니다.
6. 슬러쉬버킷을 사용하여 공격 모드/방법을 관련 공격 모드/방법 목록에 추가합니다.
7. 저장을 클릭합니다.

연결된 표시기 유형 식별

IoC에 연결된 표시기 유형이 정의되지 않은 경우 모든 유형의 옵저버블을 추적합니다. 그러나 하나 이상의 표시기 유형을 IoC에 연결하면 IoC와 연결할 수 있는 옵저버블 유형이 제한됩니다.

시작하기 전에
필요한 역할: sn_ti.write

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **IoC** 리포지토리 〉 표시기.
2. 표시기 유형을 연결할 표시기를 클릭합니다.
3. 연결된 유형 관련 목록을 클릭합니다.
4. 편집을 클릭합니다.
5. 필요한 경우 필터를 사용하여 IoC와 연결할 표시기 유형을 찾습니다.
6. 슬러쉬버킷을 사용하여 표시기 유형을 연관된 유형 목록에 추가합니다.
7. 저장을 클릭합니다.

표시기 소스 식별

지표 소스는 일반적으로 위협 임포트 프로세스의 일부로 자동으로 추적되지만 더 많은 소스를 수동으로 추가할 수 있습니다.

시작하기 전에
필요한 역할: sn_ti.write

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **IoC** 리포지토리 〉 표시기.
2. 표시기 소스를 추가할 표시기를 클릭합니다.
3. 표시기 소스 관련 목록을 클릭합니다.
4. 편집을 클릭합니다.
5. 필요한 경우 필터를 사용하여 IoC와 연결할 표시기 소스를 찾습니다.
6. 슬러쉬버킷을 사용하여 표시기 소스를 표시기 소스 목록에 추가합니다.
7. 저장을 클릭합니다.

IoC에 연결된 작업 추가

관련 작업(예: 변경 사항 및 인시던트)을 STIX 데이터로 임포트하는 것 외에도 수동으로 IoC에 추가할 수 있습니다.

시작하기 전에
필요한 역할: sn_ti.write

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **IoC** 리포지토리 〉 표시기.
2. 연결된 작업을 추가할 IoC를 클릭합니다.
3. 연관된 작업 관련 목록을 클릭합니다.
4. 편집을 클릭합니다.
5. 필요한 경우 필터를 사용하여 IoC와 연결할 작업을 찾습니다.
6. 슬러쉬버킷을 사용하여 연관된 작업 목록에 작업을 추가합니다.
7. 저장을 클릭합니다.

옵저버블

옵저버블은 컴퓨터 및 네트워크 작동과 관련된 상태 저장 속성(예: 파일의 MD5 해시 또는 레지스트리 키 값) 또는 측정 가능한 이벤트(예: 레지스트리 키 만들기 또는 파일 삭제)를 나타냅니다. 옵저버블은 1.1 및 2.x에 STIX 적용됩니다.

사이버 옵저버블 집합은 사이버 위협의 동작을 나타내는 상황별 정보와 결합될 때 손상 지표를 식별하는 데 유용합니다.

옵저버블은 1.1 및 2.x에 STIX 적용됩니다.

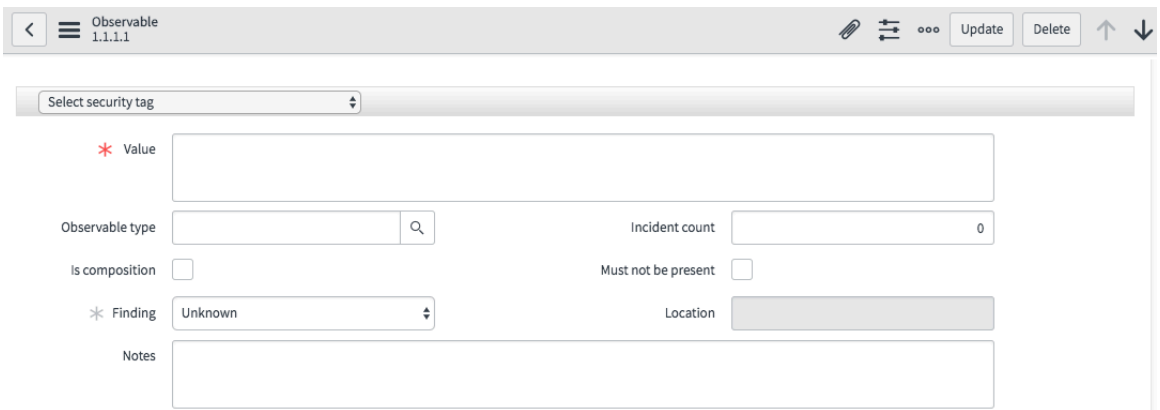
옵저버블 정의

옵저버블은 벤더 서버에서 STIX 데이터로 검색됩니다. 그러나 필요한 경우 옵저버블을 생성할 수 있습니다.

시작하기 전에
필요한 역할: sn_ti.admin

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **IoC** 리포지토리 〉 옵저버블.
2. 새로 만들기를 클릭합니다.



3. 양식의 필드에 적절히 입력합니다.

필드	설명
분류 태그 선택	보안 태그를 설정하고 활성화하여 기록에 메타데이터를 추가하는 경우 하나 이상의 태그를 선택하여 옵저버블의 민감도를 지정할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	보안 태그를 설정하거나 활성화하지 않은 경우에는 이 드롭다운 목록이 표시되지 않습니다.
값	옵저버블과 연결된 값(예: IP 주소 또는 해시)입니다. 주: IP 주소 또는 해시에 대한 위협 검사 , 반환된 맬웨어 또는 기타 오류가 발생하면 IP 주소 또는 해시 값이 옵저버블 〔sn_ti_observable〕 테이블에 자동으로 추가됩니다. 따라서 옵저버블 양식에서 검색할 수 있습니다.
옵저버블 유형	IP 주소 또는 파일 해시와 같은 옵저버블 분류를 선택합니다. 이러한 옵저버블 유형은 **Observable Types** 모듈에 정의되어 있습니다.
인시던트 수	옵저버블 값이 발생한 횟수입니다.
컴퍼지션임	이 필드는 옵저버블 기록이 저장된 후에만 표시됩니다. 옵저버블 유형이옵저버블 컴포지션 이외의 항목으로 설정되어 있고 이 새 옵저버블이 컴포지션인 경우 이 확인란을 선택합니다. 옵저버블 유형이 이미 옵저버블 컴포지션으로 설정된 경우 확인란이 선택되고 읽기 전용입니다. 옵저버블 컴포지션은 자식 옵저버블을 포함하는 옵저버블입니다.
찾기	다음 중 하나를 선택합니다. ○ 악성: 옵저버블이 조직에 해롭다는 것을 나타냅니다. ○ 의심스러움: 옵저버블이 조직에 해로울 수 있음을 나타냅니다. ○ **Clean**: 옵저버블이 조직에 해롭지 않음을 나타냅니다. ○ 알 수 없음: 옵저버블의 발견 사항이 아직 결정되지 않았음을 나타냅니다. ○ 기본값: 알 수 없음. 자세한 내용은 위협 조회 찾기 계산기 문서를 참조하십시오. 주: 업그레이드 후 기존 옵저버블은 악성으로 표시됩니다.
운영자	이 필드는 컴포지션 확인란이 선택된 경우에만 나타납니다. 이 필드의 설정에 따라 연결된 표시기가 있는지 여부를 결정할 때 옵저버블과 해당 하위 항목이 고려됩니다. 연결된 표시기가 존재하는 것으로 간주되기 위해 모든 하위 옵저버블이 있어야 하는 경우 이 필드를 **AND** 로 설정합니다. 연결된 표시기가 존재하는 것으로 간주하기 위해 하위 옵저버블이 있는 경우 **OR** 로 설정합니다.
존재하지 않아야 함	이 필드는 옵저버블 기록이 저장된 후에만 표시됩니다. 선택하는 경우 이 필드는 옵저버블의 부재가 잠재적인 문제(예: 레지스트리 키 누락)임을 나타냅니다.
위치	두 속성의 설정과 스크립트 포함 정의를 사용하면 이 필드에 로드할 더 많은 IoC 데이터 로드 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
메모	옵저버블에 대한 추가 메모를 입력합니다.

4. 양식 헤더를 마우스 오른쪽 버튼으로 클릭하고 저장을 클릭합니다.
이제 다음 관련 목록 중 하나를 클릭하여 추가 정보를 볼 수 있습니다.

관련 목록	설명
관련 표시기	위협 소스에서 식별한 표시기를 나열합니다.
관련된 작업	옵저버블과 연결된 변경 내용을 나열합니다.
하위 옵저버블	위협 소스에서 식별한 관련 옵저버블을 나열합니다.
IP에 대해 일치하는 자원	옵저버블이 IP 주소인 경우 이 목록에는 일치하는 IP 주소가 있는 모든 리소스(구성 항목)가 표시됩니다.
옵저버블 소스	소스의 신뢰도와 함께 이 옵저버블의 소스를 나열합니다.
보안 주석	이 옵저버블에 추가된 보안 주석을 나열합니다.

옵저버블에 관련 IoC 추가

옵저버블을 STIX 데이터로 임포트하는 것 외에도 관련 옵저버블을 IoC에 수동으로 추가할 수 있습니다.

시작하기 전에
필요한 역할: sn_ti.admin

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **IoC** 리포지토리 〉 옵저버블.
2. 관련 IoC를 추가할 옵저버블을 클릭합니다.
3. 관련 표시기 관련 목록을 클릭합니다.
4. 편집을 클릭합니다.
5. 필요한 경우 필터를 사용하여 옵저버블과 연결하려는 표시기를 찾습니다.
6. 슬러쉬버킷을 사용하여 관련 표시기 목록에 표시기를 추가합니다.
7. 저장을 클릭합니다.

옵저버블에 관련 작업 추가

관련 작업(예: 변경 사항 및 인시던트)을 STIX 데이터로 임포트하는 것 외에도 수동으로 옵저버블에 추가할 수 있습니다.

시작하기 전에
필요한 역할: sn_ti.admin

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **IoC** 리포지토리 〉 옵저버블.
2. 연결된 작업을 추가할 옵저버블을 클릭합니다.
3. 연관된 작업 관련 목록을 클릭합니다.
4. 편집을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. 필요한 경우 필터를 사용하여 옵저버블과 연결할 작업을 찾습니다.
6. 슬러쉬버킷을 사용하여 연관된 작업 목록에 작업을 추가합니다.
7. 저장을 클릭합니다.

관련 옵저버블 추가

옵저버블을 STIX 데이터로 임포트하는 것 외에도 관련 옵저버블을 수동으로 추가할 수 있습니다.

시작하기 전에
필요한 역할: sn_ti.admin

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **IoC** 리포지토리 〉 옵저버블.
2. 관련 옵저버블을 추가할 옵저버블을 클릭합니다.
3. 하위 옵저버블 관련 목록을 클릭합니다.
4. 편집을 클릭합니다.
5. 필요한 경우 필터를 사용하여 현재 옵저버블과 연결할 옵저버블을 찾습니다.
6. 슬러시버킷을 사용하여 옵저버블을 하위 옵저버블 목록에 추가합니다.
7. 저장을 클릭합니다.

더 많은 **IoC** 데이터 로드

두 속성의 설정과 스크립트 포함 정의에 따라 옵저버블 양식에서 IP 주소 및 웹 사이트에 대한 지리적 위치 정보를 로드할 수 있습니다. 추가 사용자 지정을 통해 국가 코드, 도시 이름과 같은 다른 정보를 추가할 수도 있습니다.

시작하기 전에
다음 두 속성을 설정해야 합니다.

- **IP** 주소/URL에 대한 추가 정보를 검색할 도메인 이름 [sn_ti.ip_lookup.web_site]
- 위 도메인에 사용할 **API** 키(있는 경우) [sn_ti.ip_lookup.api_key]

필요한 역할: sn_ti.admin

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **IoC** 리포지토리 〉 옵저버블.
2. 더 많은 IoC 데이터를 보려는 옵저버블의 IP 주소 또는 URL을 클릭합니다.
   위치 필드에는 IoC의 지리적 위치가 표시됩니다.
3. 데이터 보강 버튼을 클릭하여 추가 IoC 데이터를 로드합니다.
4. 옵저버블 양식을 구성하여 국가 코드 및 도시 코드와 같은 다른 위치 관련 필드를 추가할 수도 있습니다.

   주:
   더 많은 위치 관련 정보를 로드하려면 **ThreatAdditionalInfo** 스크립트 포함을 편집하고 추가 정보를 제공하는 웹 사이트에서 적절한 API 키를 제공합니다.

옵저버블 소스 식별

옵저버블에 정의된 소스가 없는 경우 모든 유형의 소스를 사용합니다. 그러나 옵저버블에 하나 이상의 위협 소스를 추가하면 사용되는 소스가 제한됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_ti.admin

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **IoC** 리포지토리 〉 옵저버블.
2. 옵저버블 소스를 추가할 옵저버블을 클릭합니다.
3. 옵저버블 소스 관련 목록을 클릭합니다.
4. 편집을 클릭합니다.
5. 필요한 경우 필터를 사용하여 옵저버블과 연결할 소스를 찾습니다.
6. 슬러시버킷을 사용하여 옵저버블 소스를 옵저버블 소스 목록에 추가합니다.
7. 저장을 클릭합니다.

옵저버블에 대한 조회 수행

하나 이상의 옵저버블에 대해 위협 인텔리전스 조회를 수행하여 알려진 보안 위협과 연관이 있는지 여부를 확인할 수 있습니다. 실행되는 스캔 구현은 활성화한 구현 구현에 따라 다릅니다.

시작하기 전에
조회를 수행하려면 먼저 Threat Intelligence 플러그인을 활성화해야 합니다. 하나 이상의 스캔 구현에 대한 플러그인도 설치해야 합니다.

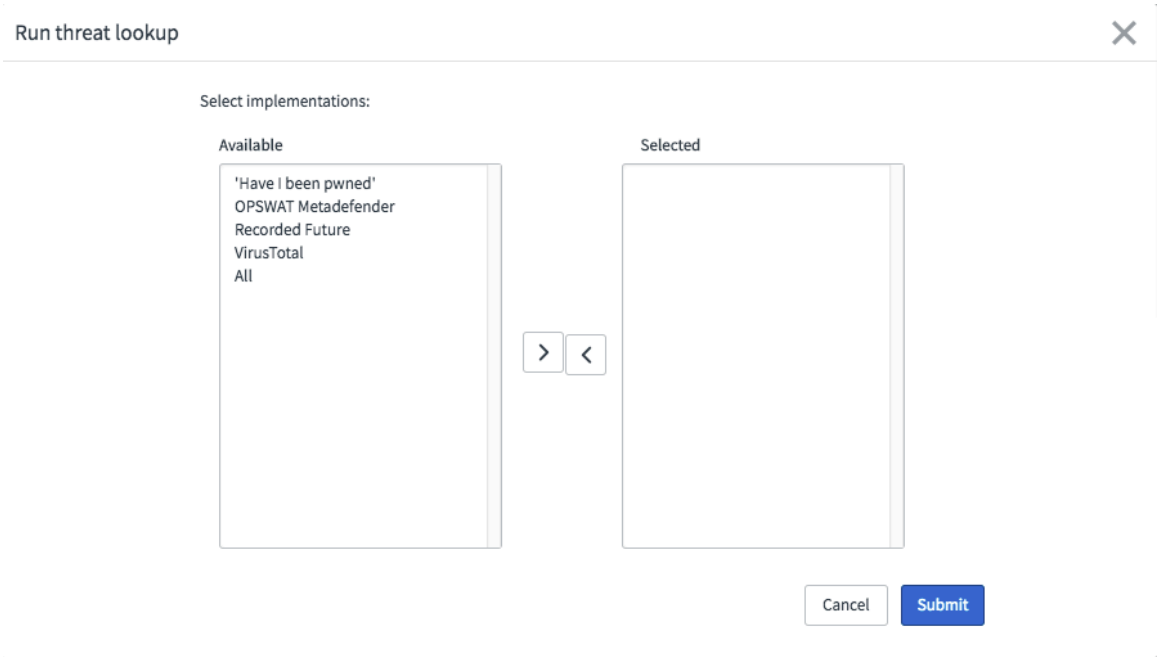
- CrowdStrike Falcon Intelligence 통합
- OPSWAT Metadefender
- 보안 운영 내가 pwned를 받았습니까?
- VirusTotal

필요한 역할: sn_ti.write

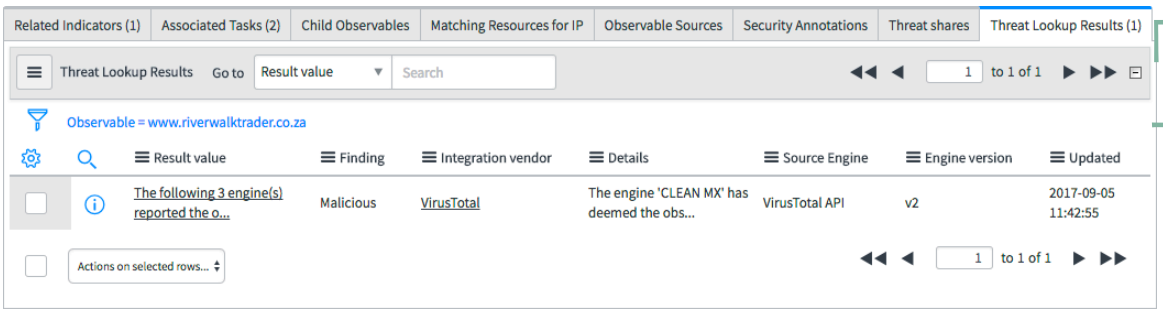
프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **IoC** 리포지토리 〉 옵저버블.
2. 다음 단계 중 하나를 수행합니다.
   - 둘 이상의 옵저버블에 대한 조회를 수행하려면 옵저버블을 선택하고 선택한 행에서 작업을 클릭한 다음 위협 조회 실행을 선택합니다.
   - 단일 옵저버블에 대한 조회를 수행하려면 옵저버블 기록을 열고 위협 조회 실행 관련 링크를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



3. 사용할 위협 조회 구현을 선택하거나 모두를 선택하여 모든 활성 구현을 사용하여 조회를 수행한 다음 제출을 클릭합니다.
   위협 조회가 시작되었음을 나타내는 메시지가 표시됩니다. 선택한 보안 운영 통합 - 위협 조회 플로우 위협 조회 구현에 대한 구현 워크플로우를 실행하고 실행합니다. 조회가 수행되고 결과가 생성됩니다.
4. 조회가 완료되면 위협 조회 결과 탭을 클릭하여 결과를 볼 수 있습니다.



최근 위협 조회 결과: 최근 위협 조회 결과 탭을 클릭하면 각 통합 벤더의 최신 또는 최근 위협 조회 결과를 볼 수도 있습니다.

> **주:**
> 최근 위협 조회 결과 탭은 기본 시스템의 일부가 아닙니다.

이 탭을 활성화하려면 다음을 수행합니다.

a. 폼 헤더를 마우스 오른쪽 버튼으로 클릭합니다.

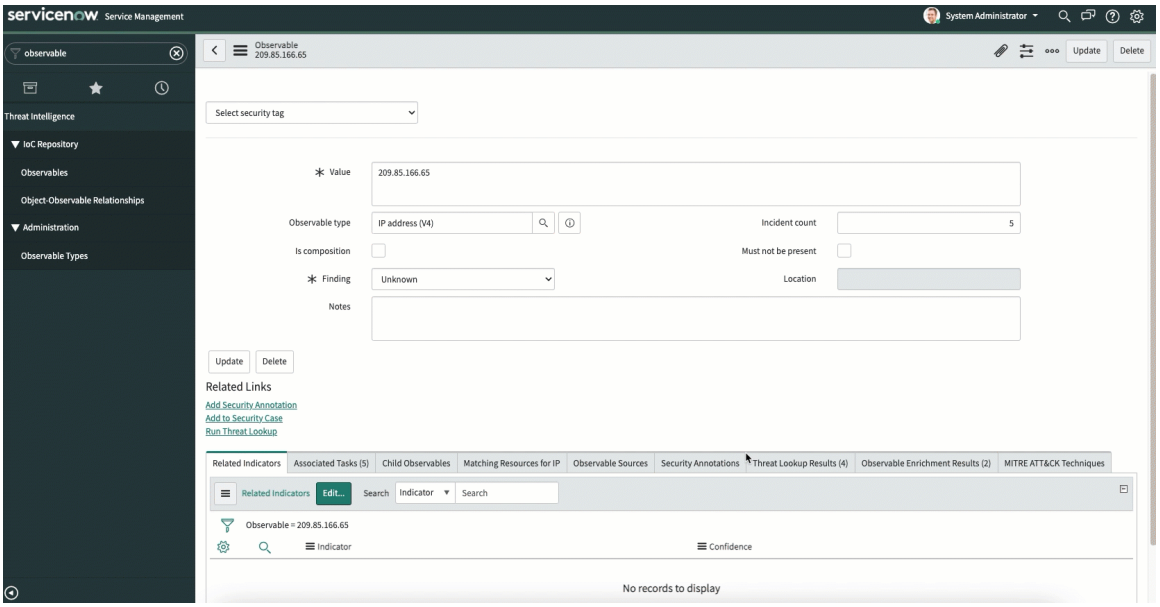
b. 다음으로 이동 구성 〉 관련 목록.

c. 사용 가능 목록에서 최근 위협 조회 결과를 찾아 선택됨 목록으로 이동합니다.

d. 저장을 클릭합니다.

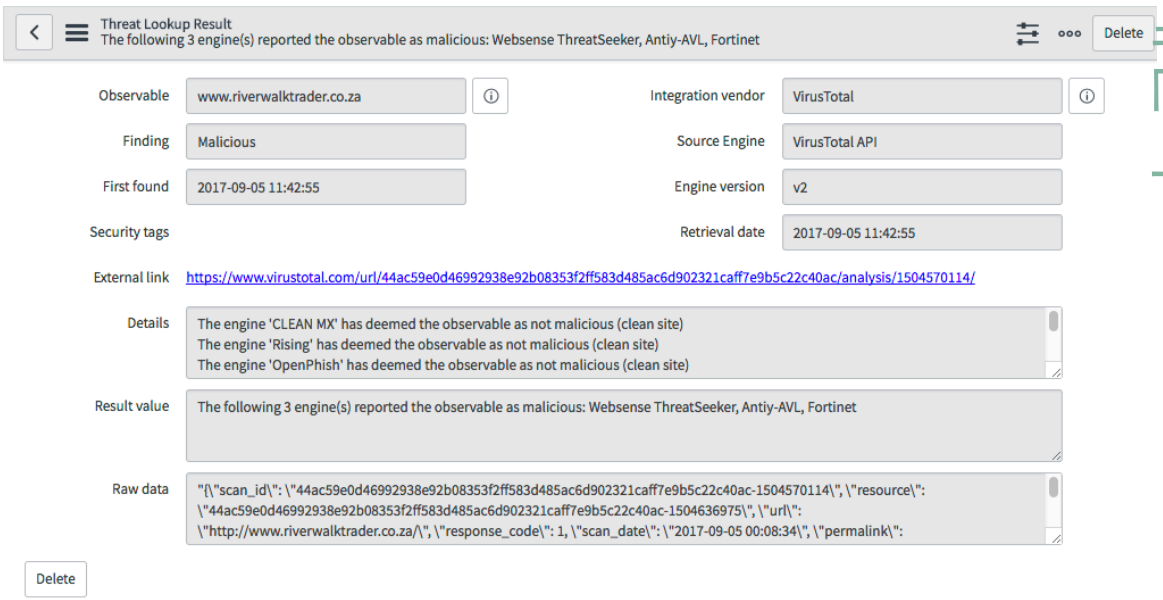
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이제 최근 위협 조회 결과 탭에서 각 통합 벤더의 최근 위협 조회 결과를 볼 수 있습니다.



5. 특정 조회에 대한 원시 결과를 포함하여 추가 상세 정보를 보려면 결과 값을 클릭합니다.

주:
VirusTotal 또는 OPSWAT Metadefender 구현을 사용하면 아래와 같이 세부 정보가 통합됩니다.



옵저버블에 대한 위협 보강 수행

하나 이상의 옵저버블에 대해 위협 인텔리전스 보강을 수행하여 알려진 보안 위협과 연관이 있는지 여부를 확인할 수 있습니다. 실행되는 구현은 활성화한 구현에 따라 다릅니다.

시작하기 전에

보강을 수행하려면 먼저 Threat Intelligence 플러그인을 활성화해야 합니다. 하나 이상의 보강 구현에 대한 플러그인도 설치해야 합니다.

- CrowdStrike Falcon Intelligence 통합
- OPSWAT Metadefender

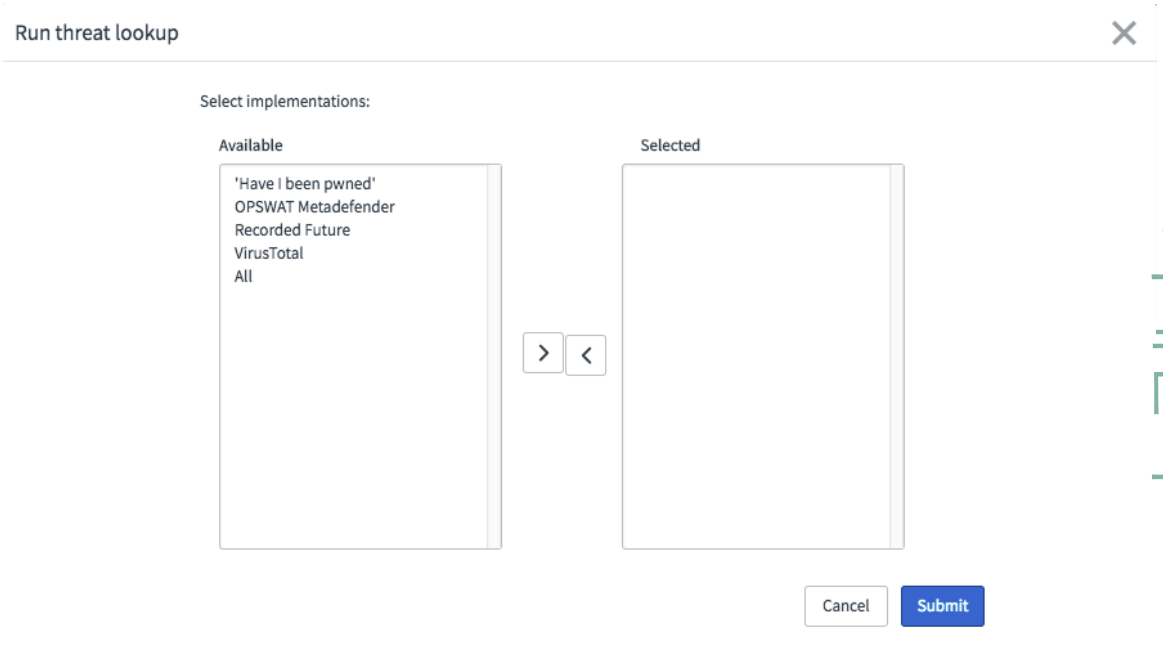
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 보안 운영 내가 pwned를 받았습니까?
- VirusTotal
- 누구인가?

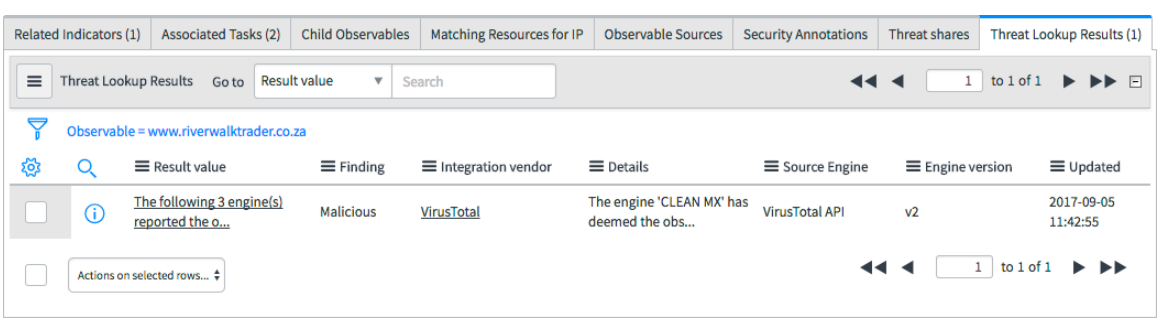
필요한 역할: sn_ti.admin

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **IoC** 리포지토리 〉 옵저버블.
2. 다음 단계 중 하나를 수행합니다.
   - 둘 이상의 옵저버블에 대한 조회를 수행하려면 옵저버블을 선택하고 선택한 행에서 작업을 클릭한 다음 위협 조회 실행을 선택합니다.
   - 단일 옵저버블에 대한 조회를 수행하려면 옵저버블 기록을 열고 위협 조회 실행 관련 링크를 클릭합니다.



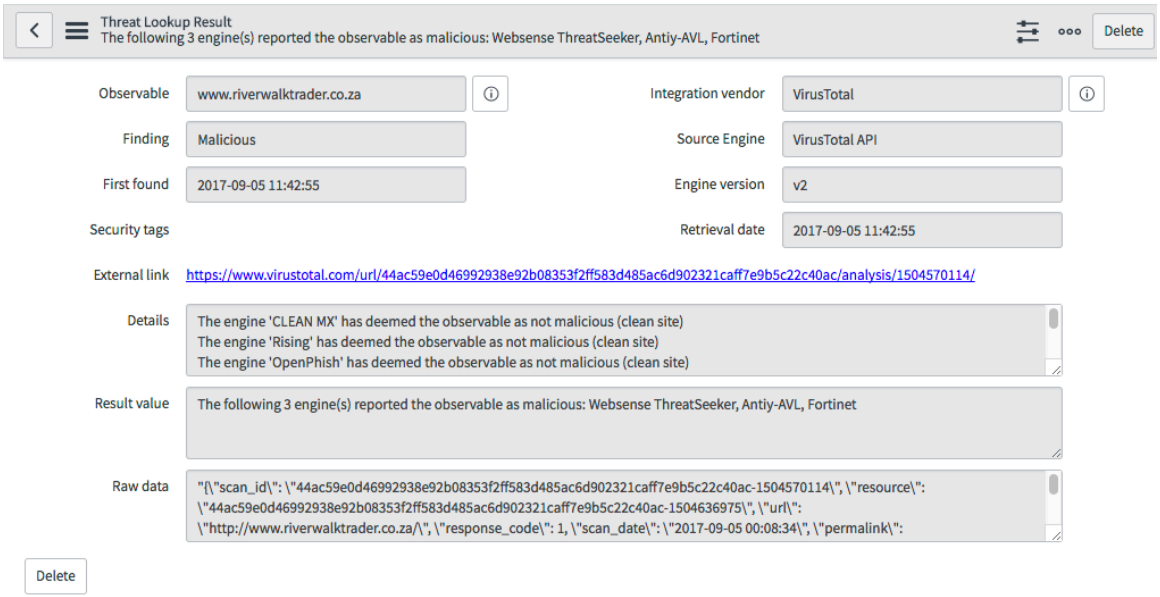
3. 사용할 위협 조회 구현을 선택하거나 모두를 선택하여 모든 활성 구현을 사용하여 조회를 수행한 다음 제출을 클릭합니다.
   위협 조회가 시작되었음을 나타내는 메시지가 표시됩니다. 선택한 보안 운영 통합 - 위협 조회 플로우 위협 조회 구현에 대한 구현 워크플로우를 실행하고 실행합니다. 조회가 수행되고 결과가 생성됩니다.
4. 조회가 완료되면 위협 조회 결과 탭을 클릭하여 결과를 볼 수 있습니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. 특정 조회에 대한 원시 결과를 포함하여 추가 상세 정보를 보려면 결과 값을 클릭합니다.

주:
VirusTotal 또는 OPSWAT Metadefender 구현을 사용하면 아래와 같이 세부 정보가 통합됩니다.



공격 패턴

공격 패턴은 공격자가 대상을 손상시키려고 시도하는 방법을 설명하는 전술, 기술 및 절차(TTP)의 한 유형입니다. 공격 패턴은 STIX 2.x에 적용됩니다.

공격 패턴은 공격을 분류하는 데 사용됩니다. 특정 공격을 따르는 패턴으로 일반화하고 공격이 수행되는 방식에 대한 자세한 정보를 제공합니다.

예를 들어 스피어 피싱은 공격자가 링크를 클릭하거나 첨부 파일을 열어 맬웨어를 전달하도록 하기 위해 신중하게 제작된 전자 메일 메시지를 당사자에게 보내는 일반적인 공격 유형입니다. 공격 패턴은 특정 위협 행위자에 의한 스피어 피싱(예: 대상이 콘테스트에서 우승한 경우)과 같이 보다 구체적입니다.

공격 패턴 정의

공격을 분류하는 데 도움이 되는 공격 패턴을 정의합니다.

시작하기 전에

필요한 역할: sn_ti.admin

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **IoC** 리포지토리 〉 공격 패턴.

2. 새로 만들기를 클릭합니다.

3. 양식에 있는 필드를 적절하게 작성합니다.

4. 제출을 클릭합니다.

다음에 수행할 작업

이제 다음 관련 목록 중 하나를 클릭하여 공격 패턴과 관련된 객체에 대한 추가 정보를 볼 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관련 링크 및 관련 목록	설명
관계 표시	STIX 객체의 관계를 볼 수 있는 STIX 시각화 도우미를 엽니다. 관계 표시는 객체에 연관된 객체가 있는 경우에만 나타납니다.
외부 참조	STIX가 아닌 정보를 참조하는 외부 참조를 나열합니다. 이 속성은 하나 이상의 외부 객체 식별자를 제공하는 데 사용됩니다.
연결된 킬 체인 단계	이 객체와 연결된 킬 체인 단계를 나열합니다.
캠페인	이 객체와 연관된 캠페인을 나열합니다.
작업 방침	공격을 방지하기 위한 기술적 또는 자동화된 응답(패치 적용, 방화벽 재구성)인 이 객체와 관련된 작업 과정을 나열합니다.
ID	이 객체와 연결된 ID 목록입니다.
표시기	이 개체와 연결된 위협 소스에서 식별한 관련 IoC(침해 표시기)를 나열합니다.
침입 세트	이 객체와 관련된 공통 속성이 있는 일련의 적대적 동작 및 자원을 나열합니다.
위치	이 객체에 지리적 컨텍스트를 제공하는 위치를 나열합니다.
맬웨어	이 객체와 연결된 악성 코드를 나열합니다.
위협 액터	이 객체와 관련하여 악의적인 의도를 가지고 행동하는 개인, 그룹 또는 조직을 나열합니다.
도구	위협 행위자가 이 개체와 관련된 공격을 수행하는 데 사용하는 합법적인 소프트웨어를 나열합니다.
취약성	공격자가 악용하는 소프트웨어 또는 하드웨어의 약점 또는 결함을 나열합니다. 이 개체와 관련되어 있습니다.

캠페인

캠페인은 적대적 행동의 그룹화입니다. 이러한 동작은 특정 대상 집합에 대해 시간이 지남에 따라 발생하는 일련의 악의적인 활동 또는 공격을 설명합니다. 캠페인은 STIX 2.x에 적용됩니다.

캠페인은 일반적으로 잘 정의된 목표를 가지고 있으며 침입 세트의 일부일 수 있습니다.

캠페인은 종종 침입 세트와 위협 행위자에 기인합니다. 위협 행위자는 침입 집합에서 알려진 인프라를 재사용하거나 해당 캠페인을 수행하기 위한 새로운 인프라를 설정할 수 있습니다.

캠페인은 그로 인해 발생하는 인시던트, 사람 또는 캠페인이 대상으로 하는 자원, 사용하는 자원에 공통된 목표를 가지고 있습니다.

예를 들어, 범죄 조직은 ACME 은행의 경영진을 공격합니다. 그들은 특정 변종 맬웨어와 새로운 서버를 사용하여 공격하여 다른 은행과의 합병에 대한 비밀 정보를 얻습니다.

캠페인 정의

캠페인을 정의하여 적대적 행동을 그룹화합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_ti.admin

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **IoC** 리포지토리 〉 캠페인.

2. 새로 만들기를 클릭합니다.

3. 양식에 있는 필드를 적절하게 작성합니다.

4. 제출을 클릭합니다.

다음에 수행할 작업
이제 다음 관련 목록 중 하나를 클릭하여 캠페인과 연관된 객체에 대한 추가 정보를 볼 수 있습니다.

관련 링크 및 관련 목록	설명
관계 표시	STIX 객체의 관계를 볼 수 있는 STIX 시각화 도우미를 엽니다. 관계 표시는 객체에 연관된 객체가 있는 경우에만 나타납니다.
외부 참조	STIX가 아닌 정보를 참조하는 외부 참조를 나열합니다. 이 속성은 하나 이상의 외부 객체 식별자를 제공하는 데 사용됩니다.
공격 패턴	이 객체와 관련된 공격을 분류하는 데 도움이 되는 공격 패턴을 나열합니다.
ID	이 객체와 연결된 ID 목록입니다.
표시기	이 개체와 연결된 위협 소스에서 식별한 관련 IoC(침해 표시기)를 나열합니다.
인프라	시스템, 소프트웨어 서비스 및 이 객체와 연결된 연결된 모든 물리적 또는 가상 자원을 나열합니다.
침입 세트	이 객체와 관련된 공통 속성이 있는 일련의 적대적 동작 및 자원을 나열합니다.
위치	이 객체에 지리적 컨텍스트를 제공하는 위치를 나열합니다.
맬웨어	이 객체와 연결된 악성 코드를 나열합니다.
위협 액터	이 객체와 관련하여 악의적인 의도를 가지고 행동하는 개인, 그룹 또는 조직을 나열합니다.
도구	위협 행위자가 이 개체와 관련된 공격을 수행하는 데 사용하는 합법적인 소프트웨어를 나열합니다.
취약성	공격자가 악용하는 소프트웨어 또는 하드웨어의 약점 또는 결함을 나열합니다. 이 개체와 관련되어 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업 방침

동작 방침은 공격을 방지하거나 진행 중인 공격에 대응하기 위해 취하는 동작입니다. 작업 과정은 STIX 2.x에 적용됩니다.

동작 방침에서는 기술 또는 자동 대응(패치 적용, 방화벽 재구성)에 대해 설명합니다. 또한 직원 교육 또는 정책 변경과 같은 상위 수준의 작업을 설명할 수도 있습니다.

예를 들어 취약성을 완화하기 위한 동작 방침은 취약성을 수정하는 패치를 적용하는 것을 설명할 수 있습니다.

작업 방침 정의

공격을 방지하거나 진행 중인 공격에 대응하기 위한 작업 과정을 정의합니다.

시작하기 전에

필요한 역할: sn_ti.admin

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **IoC** 리포지토리 〉 작업 방침.
2. 새로 만들기를 클릭합니다.
3. 양식에 있는 필드를 적절하게 작성합니다.
4. 제출을 클릭합니다.

다음에 수행할 작업

다음 관련 목록 중 하나를 클릭하면 작업 과정과 연결된 객체에 대한 추가 정보를 볼 수 있습니다.

관련 링크	설명
관계 표시	STIX 객체의 관계를 볼 수 있는 STIX 시각화 도우미를 엽니다. 관계 표시는 객체에 연관된 객체가 있는 경우에만 나타납니다.
외부 참조	STIX가 아닌 정보를 참조하는 외부 참조를 나열합니다. 이 속성은 하나 이상의 외부 객체 식별자를 제공하는 데 사용됩니다.
공격 패턴	이 객체와 관련된 공격을 분류하는 데 도움이 되는 공격 패턴을 나열합니다.
표시기	이 개체와 연결된 위협 소스에서 식별한 관련 IoC(침해 표시기)를 나열합니다.
맬웨어	이 객체와 연결된 악성 코드를 나열합니다.
도구	위협 행위자가 이 개체와 관련된 공격을 수행하는 데 사용하는 합법적인 소프트웨어를 나열합니다.
취약성	공격자가 악용하는 소프트웨어 또는 하드웨어의 약점 또는 결함을 나열합니다. 이 개체와 관련되어 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

ID

ID는 실제 개인, 조직 또는 그룹(ACME, Inc.) 및 개인, 시스템 또는 그룹 클래스(금융 부문)를 나타냅니다. ID는 STIX 2.x에 적용됩니다.

ID SDO는 기본 식별 정보, 연락처 정보 및 ID가 속한 섹터를 캡처할 수 있습니다. ID는 공격의 대상, 정보 소스, 개체 생성자 및 위협 행위자 ID를 나타냅니다.

ID 정의

실제 개인, 조직 또는 그룹을 나타내는 ID를 정의합니다.

시작하기 전에
필요한 역할: sn_ti.admin

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **IoC** 리포지토리 〉 **ID**.
2. 새로 만들기를 클릭합니다.
3. 양식에 있는 필드를 적절하게 작성합니다.
4. 제출을 클릭합니다.

다음에 수행할 작업
ID와 연결된 객체에 대한 추가 정보를 보려면 다음 관련 목록 중 하나를 클릭하십시오.

관련 링크 및 관련 목록	설명
관계 표시	STIX 객체의 관계를 볼 수 있는 STIX 시각화 도우미를 엽니다. 관계 표시는 객체에 연관된 객체가 있는 경우에만 나타납니다.
외부 참조	STIX가 아닌 정보를 참조하는 외부 참조를 나열합니다. 이 속성은 하나 이상의 외부 객체 식별자를 제공하는 데 사용됩니다.
공격 패턴	이 객체와 관련된 공격을 분류하는 데 도움이 되는 공격 패턴을 나열합니다.
캠페인	이 객체와 연관된 캠페인을 나열합니다.
침입 세트	이 객체와 관련된 공통 속성이 있는 일련의 적대적 동작 및 자원을 나열합니다.
위치	이 객체에 지리적 컨텍스트를 제공하는 위치를 나열합니다.
맬웨어	이 객체와 연결된 악성 코드를 나열합니다.
위협 액터	이 객체와 관련하여 악의적인 의도를 가지고 행동하는 개인, 그룹 또는 조직을 나열합니다.
도구	위협 행위자가 이 개체와 관련된 공격을 수행하는 데 사용하는 합법적인 소프트웨어를 나열합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

인프라

인프라 SDO는 전술, 기술 및 절차(TTP)의 한 유형을 나타냅니다. 공격의 특정 목적을 지원하기 위한 모든 시스템, 소프트웨어 서비스 및 관련된 물리적 또는 가상 자원을 설명합니다. 인프라는 STIX 2.x에 적용됩니다.

공격 요소는 다른 SDO 또는 SCO로 표시됩니다. 그러나 인프라 SDO는 인프라를 구성하는 명명된 데이터 그룹을 나타냅니다.

인프라의 예로는 공격에 사용되는 C2 서버, 장치 또는 방어의 일부인 서버 또는 공격의 대상이 되는 데이터베이스 서버가 있습니다.

인프라 정의

인프라스트럭처, 즉 공격의 특정 목적을 지원하기 위한 시스템, 소프트웨어 서비스 및 관련된 물리적 또는 가상 자원을 정의합니다.

시작하기 전에

필요한 역할: sn_ti.admin

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **IoC** 리포지토리 〉 인프라.
2. 새로 만들기를 클릭합니다.
3. 양식에 있는 필드를 적절하게 작성합니다.
4. 제출을 클릭합니다.

다음에 수행할 작업

이제 다음 관련 목록 중 하나를 클릭하여 추가 정보를 볼 수 있습니다. 다른 개체를 인프라와 연결할 수도 있습니다.

관련 링크 및 관련 목록	설명
관계 표시	STIX 객체의 관계를 볼 수 있는 STIX 시각화 도우미를 엽니다. 관계 표시는 객체에 연관된 객체가 있는 경우에만 나타납니다.
외부 참조	STIX가 아닌 정보를 참조하는 외부 참조를 나열합니다. 이 속성은 하나 이상의 외부 객체 식별자를 제공하는 데 사용됩니다.
연결된 유형	이 객체와 연결된 표시기 유형을 나열합니다.
연결된 킬 체인 단계	이 객체와 연결된 킬 체인 단계를 나열합니다.
연결된 옵저버블	이 객체와 연결된 옵저버블을 나열합니다.
연결된 인프라	시스템, 소프트웨어 서비스 및 이 객체와 연결된 연결된 모든 물리적 또는 가상 자원을 나열합니다.
캠페인	이 객체와 연관된 캠페인을 나열합니다.
표시기	이 개체와 연결된 위협 소스에서 식별한 관련 IoC(침해 표시기)를 나열합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관련 링크 및 관련 목록	설명
침입 세트	이 객체와 관련된 공통 속성이 있는 일련의 적대적 동작 및 자원을 나열합니다.
위치	이 객체에 지리적 컨텍스트를 제공하는 위치를 나열합니다.
맬웨어	이 객체와 연결된 악성 코드를 나열합니다.
관찰 데이터	이 객체와 연결된 관찰 데이터를 나열합니다.
위협 액터	이 객체와 관련하여 악의적인 의도를 가지고 행동하는 개인, 그룹 또는 조직을 나열합니다.
도구	위협 행위자가 이 개체와 관련된 공격을 수행하는 데 사용하는 합법적인 소프트웨어를 나열합니다.
취약성	공격자가 악용하는 소프트웨어 또는 하드웨어의 약점 또는 결함을 나열합니다. 이 개체와 관련되어 있습니다.

침입 세트

침입 세트는 공통 속성을 가진 적대적 행동 및 자원의 그룹화된 집합입니다. 침입 세트에는 일반적으로 단일 조직이 포함됩니다. 침입 세트는 STIX 2.x에 적용됩니다.

침입 세트는 여러 캠페인 또는 기타 활동을 캡처할 수 있습니다. 이러한 활동은 일반적으로 알려지거나 알려지지 않은 위협 액터를 나타내는 속성을 공유합니다.

새로운 활동은 공격 배후의 위협 액터를 알지 못하는 경우에도 침입 세트에 기인할 수 있습니다. 위협 액터는 하나의 침입 세트 지원에서 다른 침입 세트 지원으로 이동하거나 여러 침입 세트를 지원할 수 있습니다.

침입 세트는 전체 공격 패키지이며 잠재적으로 여러 목적을 달성하기 위해 여러 캠페인에서 장기간에 걸쳐 사용될 수 있습니다.

침입 세트 정의

공통 속성을 가진 적대적 행동 및 자원의 그룹화된 집합인 침입 집합을 정의합니다.

시작하기 전에

필요한 역할: sn_ti.admin

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **IoC** 리포지토리 〉 위탁 세트.
2. 새로 만들기를 클릭합니다.
3. 양식에 있는 필드를 적절하게 작성합니다.
4. 제출을 클릭합니다.

다음에 수행할 작업

침입 집합과 연결된 개체에 대한 추가 정보를 보려면 다음 관련 목록 중 하나를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관련 링크 및 관련 목록	설명
관계 표시	STIX 객체의 관계를 볼 수 있는 STIX 시각화 도우미를 엽니다. 관계 표시는 객체에 연관된 객체가 있는 경우에만 나타납니다.
외부 참조	STIX가 아닌 정보를 참조하는 외부 참조를 나열합니다. 이 속성은 하나 이상의 외부 객체 식별자를 제공하는 데 사용됩니다.
연결된 공격 동기	이 침입 세트가 달성하려는 부차적인 동기를 나열합니다.
공격 패턴	이 객체와 관련된 공격을 분류하는 데 도움이 되는 공격 패턴을 나열합니다.
캠페인	이 객체와 연관된 캠페인을 나열합니다.
ID	이 객체와 연결된 ID 목록입니다.
표시기	이 개체와 연결된 위협 소스에서 식별한 관련 IoC(침해 표시기)를 나열합니다.
위치	이 객체에 지리적 컨텍스트를 제공하는 위치를 나열합니다.
맬웨어	이 객체와 연결된 악성 코드를 나열합니다.
위협 액터	이 객체와 관련하여 악의적인 의도를 가지고 행동하는 개인, 그룹 또는 조직을 나열합니다.
도구	위협 행위자가 이 개체와 관련된 공격을 수행하는 데 사용하는 합법적인 소프트웨어를 나열합니다.
취약성	공격자가 악용하는 소프트웨어 또는 하드웨어의 약점 또는 결함을 나열합니다. 이 개체와 관련되어 있습니다.

위치

위치는 지리적 위치를 나타냅니다. 위치는 주로 다른 SDO에 컨텍스트를 제공하는 데 사용됩니다. 위치는 STIX 2.x를 신청합니다.

위치에는 지역(북미), 시민 주소(뉴욕, 미국), 위도 및 경도의 일부 또는 전부가 포함될 수 있습니다.

위치 SDO는 ID 또는 침입 집합이 해당 위치에 있음을 나타내기 위해 ID 또는 침입 집합과 관련될 수 있습니다. 또한 맬웨어 또는 공격 패턴과 관련되어 대상 피해자가 특정 위치에 있음을 나타낼 수 있습니다.

예를 들어, 위치는 부르주아 제비 침입 집합이 동유럽에서 유래했음을 설명하기 위해 관계에서 사용될 수 있습니다.

다음 속성 또는 속성 집합 중 하나 이상을 제공해야 합니다.

- 지역
- 국가
- 위도 및 경도

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

위치 정의

다른 SDO에 더 많은 컨텍스트를 제공하기 위해 지리적 위치를 정의하십시오.

시작하기 전에
필요한 역할: sn_ti.admin

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **IoC** 리포지토리 〉 위치.

2. 새로 만들기를 클릭합니다.

3. 양식에 있는 필드를 적절하게 작성합니다.

4. 제출을 클릭합니다.

다음에 수행할 작업
다음 관련 목록 중 하나를 클릭하면 해당 위치와 연관된 객체에 대한 추가 정보를 볼 수 있습니다.

관련 링크 및 관련 목록	설명
관계 표시	STIX 객체의 관계를 볼 수 있는 STIX 시각화 도우미를 엽니다. 관계 표시는 객체에 연관된 객체가 있는 경우에만 나타납니다.
외부 참조	STIX가 아닌 정보를 참조하는 외부 참조를 나열합니다. 이 속성은 하나 이상의 외부 객체 식별자를 제공하는 데 사용됩니다.
공격 패턴	이 객체와 관련된 공격을 분류하는 데 도움이 되는 공격 패턴을 나열합니다.
캠페인	이 객체와 연관된 캠페인을 나열합니다.
ID	이 객체와 연결된 ID 목록입니다.
인프라	시스템, 소프트웨어 서비스 및 이 객체와 연결된 연결된 모든 물리적 또는 가상 자원을 나열합니다.
침입 세트	이 객체와 관련된 공통 속성이 있는 일련의 적대적 동작 및 자원을 나열합니다.
맬웨어	이 객체와 연결된 악성 코드를 나열합니다.
위협 액터	이 객체와 관련하여 악의적인 의도를 가지고 행동하는 개인, 그룹 또는 조직을 나열합니다.
도구	위협 행위자가 이 개체와 관련된 공격을 수행하는 데 사용하는 합법적인 소프트웨어를 나열합니다.

맬웨어

멀웨어는 악성 코드를 나타내는 TTP의 일종입니다. 시스템에 은밀하게 삽입되는 프로그램을 말합니다. 맬웨어는 STIX 2.x에 적용됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

멀웨어의 목적은 피해자의 데이터, 애플리케이션 또는 운영 체제(OS)의 기밀성, 무결성 또는 가용성을 손상시키는 것입니다.

맬웨어 SDO는 분석에서 파생된 데이터에서 맬웨어 인스턴스와 제품군을 특성화, 식별 및 분류합니다. 이 SDO는 멀웨어의 작동 방식과 기능에 대한 자세한 정보를 캡처합니다.

맬웨어 정의

악성 코드를 나타내는 맬웨어를 정의합니다.

시작하기 전에
필요한 역할: sn_ti.admin

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **IoC** 리포지토리 〉 맬웨어.
2. 새로 만들기를 클릭합니다.
3. 양식에 있는 필드를 적절하게 작성합니다.
4. 제출을 클릭합니다.

다음에 수행할 작업
다음 관련 목록 중 하나를 클릭하면 맬웨어와 관련된 객체에 대한 추가 정보를 볼 수 있습니다.

관련 링크 및 관련 목록	설명
관계 표시	STIX 객체의 관계를 볼 수 있는 STIX 시각화 도우미를 엽니다. 관계 표시는 객체에 연관된 객체가 있는 경우에만 나타납니다.
외부 참조	STIX가 아닌 정보를 참조하는 외부 참조를 나열합니다. 이 속성은 하나 이상의 외부 객체 식별자를 제공하는 데 사용됩니다.
연결된 유형	이 객체와 연결된 표시기 유형을 나열합니다.
연결된 역량	이 객체와 식별되고 연결된 역량을 나열합니다.
연결된 킬 체인 단계	이 객체와 연결된 킬 체인 단계를 나열합니다.
연결된 옵저버블	이 객체와 연결된 옵저버블을 나열합니다.
연결된 맬웨어	이 객체로 식별된 관련 맬웨어를 나열합니다.
연결된 운영 체제	객체를 실행할 수 있는 운영 체제입니다. 이는 가상화된 운영 체제뿐만 아니라 베어 메탈에서 실행되는 운영 체제에도 적용됩니다.
공격 패턴	이 객체와 관련된 공격을 분류하는 데 도움이 되는 공격 패턴을 나열합니다.
캠페인	이 객체와 연관된 캠페인을 나열합니다.
작업 방침	공격을 방지하기 위한 기술적 또는 자동화된 응답(패치 적용, 방화벽 재구성)인 이 객체와 관련된 작업 과정을 나열합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관련 링크 및 관련 목록	설명
ID	이 객체와 연결된 ID 목록입니다.
표시기	이 개체와 연결된 위협 소스에서 식별한 관련 IoC(침해 표시기)를 나열합니다.
인프라	시스템, 소프트웨어 서비스 및 이 객체와 연결된 연결된 모든 물리적 또는 가상 자원을 나열합니다.
침입 세트	이 객체와 관련된 공통 속성이 있는 일련의 적대적 동작 및 자원을 나열합니다.
위치	이 객체에 지리적 컨텍스트를 제공하는 위치를 나열합니다.
맬웨어 분석	이 객체와 연결된 맬웨어 분석 기록을 나열합니다.
보고된 옵저버블	이 객체의 일부로 보고된 옵저버블을 나열합니다.
위협 액터	이 객체와 관련하여 악의적인 의도를 가지고 행동하는 개인, 그룹 또는 조직을 나열합니다.
도구	위협 행위자가 이 개체와 관련된 공격을 수행하는 데 사용하는 합법적인 소프트웨어를 나열합니다.
취약성	공격자가 악용하는 소프트웨어 또는 하드웨어의 약점 또는 결함을 나열합니다. 이 개체와 관련되어 있습니다.

맬웨어 분석

맬웨어 분석은 맬웨어의 메타데이터와 결과를 캡처합니다. 맬웨어 분석은 STIX 2.x에 적용됩니다.

맬웨어 분석에는 맬웨어 인스턴스 또는 제품군에서 수행되는 정적 또는 동적 분석이 포함됩니다.

맬웨어 분석 정의

멀웨어 인스턴스 또는 패밀리에서 수행된 특정 정적 또는 동적 분석의 메타데이터와 결과를 캡처하는 멀웨어 분석을 정의합니다.

시작하기 전에

필요한 역할: sn_ti.admin

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **IoC** 리포지토리 〉 맬웨어 분석.
2. 새로 만들기를 클릭합니다.
3. 양식에 있는 필드를 적절하게 작성합니다.
4. 제출을 클릭합니다.

다음에 수행할 작업

맬웨어 분석과 관련된 객체에 대한 추가 정보를 보려면 다음 관련 목록 중 하나를 클릭하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관련 링크 및 관련 목록	설명
관계 표시	STIX 객체의 관계를 볼 수 있는 STIX 시각화 도우미를 엽니다. 관계 표시는 객체에 연관된 객체가 있는 경우에만 나타납니다.
외부 참조	STIX가 아닌 정보를 참조하는 외부 참조를 나열합니다. 이 속성은 하나 이상의 외부 객체 식별자를 제공하는 데 사용됩니다.
연결된 맬웨어	이 객체로 식별된 관련 맬웨어를 나열합니다.
보고된 옵저버블	이 객체의 일부로 보고된 옵저버블을 나열합니다.
설치된 소프트웨어	맬웨어 인스턴스 또는 제품군의 동적 분석에 사용되는 운영 체제에 설치된 모든 비표준 소프트웨어를 나열합니다.

관찰 데이터

관찰 데이터는 STIX SCO(Cyber-Observable Objects)를 사용하여 파일, 시스템 및 네트워크와 같은 사이버 보안 관련 엔터티에 대한 정보를 전달합니다. 관찰 데이터는 STIX 2.x에 적용됩니다.

관찰 데이터는 단일 엔터티(파일, 네트워크 연결)에 대한 단일 관찰과 엔터티에 대한 여러 관찰 집계를 모두 캡처합니다.

관찰 데이터 단독으로(관계 없이) 사용하여 모든 소스에서 수집된 원시 데이터를 전달할 수 있습니다. 소스에는 분석 보고서, 샌드박스, 네트워크 및 호스트 기반 탐지 도구가 포함됩니다.

예를 들어 관찰 데이터는 IP 주소, 네트워크 연결, 파일 또는 레지스트리 키에 대한 정보를 캡처할 수 있습니다. 관찰 데이터는 정보 주장이 아니며, 그것이 의미하는 바에 대한 맥락이 없는 원시 정보일 뿐입니다.

관찰 데이터 정의

STIX SCO(Cyber-Observable Objects)를 사용하여 파일, 시스템 및 네트워크와 같은 사이버 보안 관련 엔터티에 대한 정보를 전달하는 관찰 데이터를 정의합니다.

시작하기 전에
필요한 역할: sn_ti.admin

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **IoC** 리포지토리 〉 관찰 데이터.
2. 새로 만들기를 클릭합니다.
3. 양식에 있는 필드를 적절하게 작성합니다.
4. 제출을 클릭합니다.

다음에 수행할 작업
관찰 데이터와 연결된 객체에 대한 추가 정보를 보려면 다음 관련 목록 중 하나를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관련 링크 및 관련 목록	설명
관계 표시	STIX 객체의 관계를 볼 수 있는 STIX 시각화 도우미를 엽니다. 관계 표시는 객체에 연관된 객체가 있는 경우에만 나타납니다.
외부 참조	STIX가 아닌 정보를 참조하는 외부 참조를 나열합니다. 이 속성은 하나 이상의 외부 객체 식별자를 제공하는 데 사용됩니다.
연결된 옵저버블	이 객체와 연결된 옵저버블을 나열합니다.
표시기	이 개체와 연결된 위협 소스에서 식별한 관련 IoC(침해 표시기)를 나열합니다.
인프라	시스템, 소프트웨어 서비스 및 이 객체와 연결된 연결된 모든 물리적 또는 가상 자원을 나열합니다.

위협 액터

위협 액터는 악의적인 의도로 행동하는 개인, 그룹 또는 조직입니다. 위협 액터는 STIX 2.x에 적용됩니다.

위협 액터는 침입 세트가 아니지만 시간이 지남에 따라 다양한 침입 세트, 그룹 또는 조직을 지원하거나 소속될 수 있습니다.

위협 액터는 자신의 리소스와 침입 세트의 리소스를 사용하여 공격을 수행하고 대상에 대해 캠페인을 실행합니다.

동기, 역량, 목표, 정교함 수준, 과거 활동, 액세스할 수 있는 자원 및 조직에서의 역할을 기준으로 위협 액터를 식별할 수 있습니다.

위협 액터 정의

악의적인 의도로 행동하는 개인, 그룹 또는 조직인 위협 행위자를 정의합니다.

시작하기 전에

필요한 역할: sn_ti.admin

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **IoC** 리포지토리 〉 위협 액터.
2. 새로 만들기를 클릭합니다.
3. 양식에 있는 필드를 적절하게 작성합니다.
4. 제출을 클릭합니다.

다음에 수행할 작업

다음 관련 목록 중 하나를 클릭하여 위협 액터와 연결된 객체에 대한 추가 정보를 봅니다.

관련 링크 및 관련 목록	설명
관계 표시	STIX 객체의 관계를 볼 수 있는 STIX 시각화 도우미를 엽니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관련 링크 및 관련 목록	설명
	관계 표시는 객체에 연관된 객체가 있는 경우에만 나타납니다.
외부 참조	STIX가 아닌 정보를 참조하는 외부 참조를 나열합니다. 이 속성은 하나 이상의 외부 객체 식별자를 제공하는 데 사용됩니다.
연결된 유형	이 객체와 연결된 표시기 유형을 나열합니다.
관련된 역할	위협 액터와 연결된 역할을 나열합니다.
연결된 공격 동기	위협 액터와 연관된 공격 동기를 나열합니다.
공격 패턴	이 객체와 관련된 공격을 분류하는 데 도움이 되는 공격 패턴을 나열합니다.
캠페인	이 객체와 연관된 캠페인을 나열합니다.
ID	이 객체와 연결된 ID 목록입니다.
표시기	이 개체와 연결된 위협 소스에서 식별한 관련 IoC(침해 표시기)를 나열합니다.
인프라	시스템, 소프트웨어 서비스 및 이 객체와 연결된 연결된 모든 물리적 또는 가상 자원을 나열합니다.
침입 세트	이 객체와 관련된 공통 속성이 있는 일련의 적대적 동작 및 자원을 나열합니다.
위치	이 객체에 지리적 컨텍스트를 제공하는 위치를 나열합니다.
맬웨어	이 객체와 연결된 악성 코드를 나열합니다.
도구	위협 행위자가 이 개체와 관련된 공격을 수행하는 데 사용하는 합법적인 소프트웨어를 나열합니다.
취약성	공격자가 악용하는 소프트웨어 또는 하드웨어의 약점 또는 결함을 나열합니다. 이 개체와 관련되어 있습니다.

위협 그룹화

위협 그룹화 개체는 참조된 STIX 개체에 공유 컨텍스트가 있음을 명시적으로 어설션합니다. 위협 그룹화는 STIX 2.x에 적용됩니다.

위협 그룹화 개체는 충분한 분석이 주어지면 인시던트 또는 위협 보고서를 STIX 보고서 개체로 전달하기 위해 성숙한 데이터 집합을 나타냅니다. 예를 들어, 그룹화는 보안 이벤트 또는 인시던트에 대해 진행 중인 조사의 특성을 나타내는 데 사용할 수 있습니다.

위협 그룹화 개체를 사용하여 참조된 STIX 개체가 진행 중인 분석 프로세스와 관련이 있는지 어설션할 수도 있습니다. 예를 들어 위협 분석가는 신뢰 커뮤니티의 다른 사용자와 협력하여 일련의 캠페인 및 표시기를 검사할 수 있습니다.

위협 그룹화 SDO에는 콘텐츠에서 공유하는 컨텍스트에 대한 명시적 설명, 텍스트 설명 및 그룹화 이름과 함께 SDO, SCO 및 SRO에 대한 참조 목록이 포함되어 있습니다.

위협 그룹화 정의

위협 그룹화를 공유 컨텍스트가 있는 개체로 정의합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_ti.admin

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **IoC** 리포지토리 〉 위협 그룹화.
2. 새로 만들기를 클릭합니다.
3. 양식에 있는 필드를 적절하게 작성합니다.
4. 제출을 클릭합니다.

다음에 수행할 작업
위협 그룹화와 연결된 개체에 대한 추가 정보를 보려면 다음 관련 목록 중 하나를 클릭합니다.

관련 링크 및 관련 목록	설명
관계 표시	STIX 객체의 관계를 볼 수 있는 STIX 시각화 도우미를 엽니다. 관계 표시는 객체에 연관된 객체가 있는 경우에만 나타납니다.
그룹화된 객체	위협 그룹화의 일부로 그룹화된 객체를 나열합니다.
그룹화된 표시기	위협 그룹화의 일부로 그룹화된 표시기를 나열합니다.
그룹화된 옵저버블	위협 그룹화의 일부로 그룹화된 옵저버블을 나열합니다.

표시 정의

표시 정의 개체는 특정 표시를 나타냅니다.

데이터 표시는 데이터 사용 및 공유 방법에 대한 제한, 권한 및 기타 지침을 나타냅니다.

예를 들어 데이터를 다시 공유해서는 안 되거나 저장 시 암호화해야 한다는 제한과 함께 데이터를 공유할 수 있습니다.

STIX에서 데이터 표시는 표시 정의 개체를 사용하여 지정됩니다. 이러한 정의는 객체 표시를 사용하는 STIX 객체와 세분화된 표시를 통해 STIX 객체의 개별 속성에 적용됩니다.

표시 정의 정의

특정 데이터 표시를 나타내는 표시 정의를 정의합니다.

시작하기 전에
필요한 역할: sn_ti.admin

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **IoC** 리포지토리 〉 표시 정의.
2. 새로 만들기를 클릭합니다.
3. 양식에 있는 필드를 적절하게 작성합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 제출을 클릭합니다.

다음에 수행할 작업

다음 관련 목록 중 하나를 클릭하면 표시 정의와 연관된 객체에 대한 추가 정보를 볼 수 있습니다.

관련 링크 및 관련 목록	설명
관계 표시	STIX 객체의 관계를 볼 수 있는 STIX 시각화 도우미를 엽니다. 관계 표시는 객체에 연관된 객체가 있는 경우에만 나타납니다.
표시된 객체	표시 정의로 표시된 객체의 목록입니다.
표시된 표시기	표시 정의로 표시된 표시기 목록입니다.

위협 메모

위협 메모는 메모와 관련된 STIX 개체, 표시 정의 개체 또는 언어 콘텐츠 개체에 포함되지 않은 추가 분석을 제공하기 위해 정보 텍스트를 전달합니다. 위협 메모는 STIX 2.x에 적용됩니다.

예를 들어 분석가는 다른 조직에서 만든 캠페인 객체에 메모를 추가할 수 있습니다. 메모는 해커 포럼에서 해당 캠페인과 관련된 게시물을 보았음을 나타낼 수 있습니다.

메모는 일반적으로 인간 분석가가 작성하고 인간 중심의 텍스트로 구성되며 메모를 작성한 작성자를 캡처하는 추가 속성을 포함합니다.

위협 메모 정의

기존 객체에서 사용할 수 없는 추가 컨텍스트 또는 분석을 제공하기 위해 정보를 전달하는 위협 메모를 정의합니다.

시작하기 전에

필요한 역할: sn_ti.admin

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **IoC** 리포지토리 〉 위협 메모.
2. 새로 만들기를 클릭합니다.
3. 양식에 있는 필드를 적절하게 작성합니다.

4. 제출을 클릭합니다.

다음에 수행할 작업

위협 메모와 연결된 개체에 대한 추가 정보를 보려면 다음 관련 목록 중 하나를 클릭합니다.

관련 링크 및 관련 목록	설명
관계 표시	STIX 객체의 관계를 볼 수 있는 STIX 시각화 도우미를 엽니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관련 링크 및 관련 목록	설명
	관계 표시는 객체에 연관된 객체가 있는 경우에만 나타납니다.
연결된 객체	위협 메모가 적용되는 개체의 목록입니다.
연동된 표시기	위협 메모가 적용되는 표시기 목록입니다.
연결된 옵저버블	이 객체와 연결된 옵저버블을 나열합니다.

위협 의견

의견은 다른 엔터티에서 생성한 STIX 개체에 있는 정보의 정확성에 대한 평가입니다. 위협 의견은 STIX 2.x에 적용됩니다.

의견 속성은 고정 척도를 사용하여 동의 또는 불일치 수준을 캡처합니다. 또한 고정 척도는 의견 간에 일관된 통계 연산을 가능하게 하는 숫자 매핑을 지원합니다.

예를 들어, 소비 조직의 분석가는 캠페인 개체에 "매우 동의하지 않는다"고 말하고 그 이유에 대한 설명을 제공할 수 있습니다.

의견은 주관적이며 사양은 이를 가장 잘 해석하는 방법을 다루지 않습니다.

인간 분석가는 의견을 만들고 인간 중심의 텍스트로 구성되며, 의견을 작성한 저자를 포착하기 위한 추가 속성을 포함합니다.

위협 의견 정의

위협 의견을 STIX 객체에 있는 정보의 정확성에 대한 평가로 정의합니다.

시작하기 전에

필요한 역할: sn_ti.admin

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **IoC** 리포지토리 〉 위협 의견.
2. 새로 만들기를 클릭합니다.
3. 양식에 있는 필드를 적절하게 작성합니다.
4. 제출을 클릭합니다.

다음에 수행할 작업

위협 의견과 연결된 개체에 대한 추가 정보를 보려면 다음 관련 목록 중 하나를 클릭합니다.

관련 링크 및 관련 목록	설명
관계 표시	STIX 객체의 관계를 볼 수 있는 STIX 시각화 도우미를 엽니다. 관계 표시는 객체에 연관된 객체가 있는 경우에만 나타납니다.
연결된 객체	위협 의견이 적용되는 객체의 목록입니다.
연동된 표시기	위협 의견이 적용되는 표시기 목록입니다.
연결된 옵저버블	이 객체와 연결된 옵저버블을 나열합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

위협 보고서

위협 보고서는 하나 이상의 주제에 초점을 맞춘 위협 인텔리전스 모음입니다. 위협 보고서는 STIX 2.x에 적용됩니다.

위협 보고서에는 위협 행위자, 맬웨어, 공격 기술에 대한 설명(컨텍스트 및 관련 세부 정보 포함)이 포함됩니다. 관련 위협 인텔리전스를 그룹화하여 포괄적인 사이버 위협 스토리로 게시하는 데 사용됩니다.

위협 보고서 SDO에는 텍스트 설명 및 보고서 이름과 함께 STIX 개체에 대한 참조 목록이 포함되어 있습니다.

위협 보고서 정의

컨텍스트 및 관련 상세 정보를 포함하여 위협 행위자, 맬웨어, 공격 기술을 설명하는 위협 보고서를 정의합니다.

시작하기 전에
필요한 역할: sn_ti.admin

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **IoC** 리포지토리 〉 위협 보고서.
2. 새로 만들기를 클릭합니다.
3. 양식에 있는 필드를 적절하게 작성합니다.
4. 제출을 클릭합니다.

다음에 수행할 작업
위협 보고서와 연결된 개체에 대한 추가 정보를 보려면 다음 관련 목록 중 하나를 클릭합니다.

관련 링크 및 관련 목록	설명
관계 표시	STIX 객체의 관계를 볼 수 있는 STIX 시각화 도우미를 엽니다. 관계 표시는 객체에 연관된 객체가 있는 경우에만 나타납니다.
연결된 유형	이 객체와 연결된 표시기 유형을 나열합니다.
보고된 객체	위협 보고서에 보고된 개체 목록입니다.
보고된 표시기	위협 보고서에 보고된 표시기 목록입니다.
보고된 옵저버블	위협 보고서에 보고된 옵저버블 목록입니다.

사이팅

목격은 표시기 또는 물체가 보였음을 나타냅니다. 개체는 맬웨어, 도구, 위협 액터 등일 수 있습니다.

목격은 표적이 누구이고 무엇인지, 공격이 어떻게 수행되는지를 추적하고 공격 행동의 추세를 추적합니다.

사이팅 관계 객체에는 일반 관계 객체에 없는 추가 속성이 포함되어 있습니다. 이러한 추가 속성은 사이팅 관계와 관련된 데이터를 나타냅니다.

예를 들어, 카운트 또는 어떤 것이 몇 번 보였는지를 나타냅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

목격은 관계로 포착되는데, 왜냐하면 목격된 무언가가 없다면 목격을 가질 수 없기 때문입니다.

- 멀웨어, 캠페인 또는 기타 SDO와 같이 발견된 사항
- 그것을 목격한 사람 및/또는 목격된 장소는 정체성으로 표시됩니다
- 시스템 및 네트워크에서 본 것(관찰 데이터로 표시)

표시기 사이팅 정의

표시기가 보였음을 나타내는 사이팅을 정의합니다.

시작하기 전에

필요한 역할: sn_ti.admin

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **IoC** 리포지토리 〉 표시기 목격.
2. 새로 만들기를 클릭합니다.
3. 양식에 있는 필드를 적절하게 작성합니다.
4. 제출을 클릭합니다.

다음에 수행할 작업

표시기 사이팅과 관련된 객체에 대한 추가 정보를 보려면 다음 관련 목록 중 하나를 클릭하십시오.

관련 목록	설명
외부 참조	STIX가 아닌 정보를 참조하는 외부 참조를 나열합니다. 이 속성은 하나 이상의 외부 객체 식별자를 제공하는 데 사용됩니다.
ID	이 객체와 연결된 ID 목록입니다.
관찰 데이터	이 객체와 연결된 관찰 데이터를 나열합니다.

객체 사이팅 정의

개체(맬웨어, 도구, 위협 액터 등)가 보임을 설명하는 개체 사이팅을 정의합니다.

시작하기 전에

필요한 역할: sn_ti.admin

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **IoC** 리포지토리 〉 객체 사이팅.
2. 새로 만들기를 클릭합니다.
3. 양식에 있는 필드를 적절하게 작성합니다.
4. 제출을 클릭합니다.

다음에 수행할 작업

다음 관련 목록 중 하나를 클릭하면 객체 사이팅과 연관된 객체에 대한 추가 정보를 볼 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관련 목록	설명
외부 참조	STIX가 아닌 정보를 참조하는 외부 참조를 나열합니다. 이 속성은 하나 이상의 외부 객체 식별자를 제공하는 데 사용됩니다.
ID	이 객체와 연결된 ID 목록입니다.
관찰 데이터	이 객체와 연결된 관찰 데이터를 나열합니다.

도구

도구는 위협 행위자가 공격을 수행하는 데 사용하는 합법적인 소프트웨어입니다. 도구는 STIX 2.x에 적용됩니다.

도구를 사용하면 위협 행위자가 캠페인을 실행하기 위해 도구를 사용하는 방법과 시기를 알 수 있습니다. 맬웨어와 달리 이러한 도구 또는 소프트웨어 패키지는 종종 시스템에서 발견되며 고급 사용자, 관리자, 네트워크 관리자 또는 일반 사용자를 위한 합법적인 목적을 가지고 있습니다.

예를 들어 원격 액세스 도구(RDP) 및 네트워크 검색 도구(Nmap)는 위협 행위자가 공격 중에 사용하는 도구입니다.

도구 정의

도구를 공격을 수행하는 데 사용되는 합법적인 소프트웨어로 정의합니다.

시작하기 전에

필요한 역할: sn_ti.admin

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **IoC** 리포지토리 〉 도구.
2. 새로 만들기를 클릭합니다.
3. 양식에 있는 필드를 적절하게 작성합니다.
4. 제출을 클릭합니다.

다음에 수행할 작업

다음 관련 목록 중 하나를 클릭하면 공구 객체와 연관된 객체에 대한 추가 정보를 볼 수 있습니다.

관련 링크 및 관련 목록	설명
외부 참조	STIX가 아닌 정보를 참조하는 외부 참조를 나열합니다. 이 속성은 하나 이상의 외부 객체 식별자를 제공하는 데 사용됩니다.
연결된 킬 체인 단계	이 객체와 연결된 킬 체인 단계를 나열합니다.
연결된 유형	이 객체와 연결된 표시기 유형을 나열합니다.
공격 패턴	이 객체와 관련된 공격을 분류하는 데 도움이 되는 공격 패턴을 나열합니다.
캠페인	이 객체와 연관된 캠페인을 나열합니다.
작업 방침	공격을 방지하기 위한 기술적 또는 자동화된 응답(패치 적용, 방화벽 재구성)인 이 객체와 관련된 작업 과정을 나열합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관련 링크 및 관련 목록	설명
ID	이 객체와 연결된 ID 목록입니다.
표시기	이 개체와 연결된 위협 소스에서 식별한 관련 IoC(침해 표시기)를 나열합니다.
인프라	시스템, 소프트웨어 서비스 및 이 객체와 연결된 연결된 모든 물리적 또는 가상 자원을 나열합니다.
침입 세트	이 객체와 관련된 공통 속성이 있는 일련의 적대적 동작 및 자원을 나열합니다.
위치	이 객체에 지리적 컨텍스트를 제공하는 위치를 나열합니다.
맬웨어	이 객체와 연결된 악성 코드를 나열합니다.
위협 액터	이 객체와 관련하여 악의적인 의도를 가지고 행동하는 개인, 그룹 또는 조직을 나열합니다.
취약성	공격자가 악용하는 소프트웨어 또는 하드웨어의 약점 또는 결함을 나열합니다. 이 개체와 관련되어 있습니다.
관계 표시	STIX 객체의 관계를 볼 수 있는 STIX 시각화 도우미를 엽니다. 관계 표시는 객체에 연관된 객체가 있는 경우에만 나타납니다.

취약성

취약성은 공격자가 악용하는 소프트웨어 또는 하드웨어 구성요소의 약점 또는 결함입니다. STIX 2.x에 적용되는 취약성입니다.

약점 또는 결함은 소프트웨어 또는 하드웨어 구성요소에 있는 코드의 요구 사항, 디자인 또는 구현에 있습니다. 이 약점은 해당 시스템의 기밀성, 무결성 또는 가용성에 부정적인 영향을 미치기 위해 직접 악용됩니다.

CVE는 공개적으로 알려진 문제(CVE)에 대한 일반적인 이름을 제공하는 정보 보안 취약성 및 노출 목록입니다.

예를 들어 맬웨어가 CVE-2015-12345를 악용하는 경우 맬웨어 개체가 CVE-2015-12345를 참조하는 취약성 개체에 연결될 수 있습니다.

취약성 정의

취약성을 공격자가 악용하는 소프트웨어 또는 하드웨어 구성요소의 약점 또는 결함으로 정의합니다.

시작하기 전에

필요한 역할: sn_ti.admin

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **IoC** 리포지토리 〉 취약성.
2. 새로 만들기를 클릭합니다.
3. 양식에 있는 필드를 적절하게 작성합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 제출을 클릭합니다.

다음에 수행할 작업
취약성 객체와 연결된 객체에 대한 추가 정보를 보려면 다음 관련 목록 중 하나를 클릭하십시오.

관련 링크 및 관련 목록	설명
관계 표시	STIX 객체의 관계를 볼 수 있는 STIX 시각화 도우미를 엽니다. 관계 표시는 객체에 연관된 객체가 있는 경우에만 나타납니다.
외부 참조	STIX가 아닌 정보를 참조하는 외부 참조를 나열합니다. 이 속성은 하나 이상의 외부 객체 식별자를 제공하는 데 사용됩니다.
공격 패턴	이 객체와 관련된 공격을 분류하는 데 도움이 되는 공격 패턴을 나열합니다.
캠페인	이 객체와 연관된 캠페인을 나열합니다.
작업 방침	공격을 방지하기 위한 기술적 또는 자동화된 응답(패치 적용, 방화벽 재구성)인 이 객체와 관련된 작업 과정을 나열합니다.
인프라	시스템, 소프트웨어 서비스 및 이 객체와 연결된 연결된 모든 물리적 또는 가상 자원을 나열합니다.
침입 세트	이 객체와 관련된 공통 속성이 있는 일련의 적대적 동작 및 자원을 나열합니다.
맬웨어	이 객체와 연결된 악성 코드를 나열합니다.
위협 액터	이 객체와 관련하여 악의적인 의도를 가지고 행동하는 개인, 그룹 또는 조직을 나열합니다.
도구	위협 행위자가 이 개체와 관련된 공격을 수행하는 데 사용하는 합법적인 소프트웨어를 나열합니다.

관계

관계 객체를 사용하여 두 개의 SDO 또는 STIX SCO(Cyber-Observable Objects)를 함께 연결하여 서로 어떻게 관련되어 있는지 설명합니다.

STIX 관계 객체(SRO)는 다양한 STIX 객체 간의 관계 유형을 나타냅니다. 다음과 같은 관계 객체를 사용할 수 있습니다.

- 객체-객체 관계: 이 객체는 표시기 객체를 제외한 SDO 간의 관계를 정의합니다. 개체-개체 정의 관계의 예는 공격 패턴이 맬웨어를 전달하는 것입니다.
- 객체-표시기 관계: 이 객체는 표시기 객체와 다른 SDO 간의 관계를 정의합니다. 객체-표시기 정의 관계의 예로는 표시기가 캠페인의 증거를 감지하는 경우를 들 수 있습니다.
- 객체-옵저버블 관계: 이 객체는 SDO와 옵저버블 객체(SCO) 간의 관계를 정의합니다. 객체-옵저버블 정의 관계의 예는 인프라가 잠재적인 공격에 대한 정보를 제공하는 사이버 옵저버블 객체로 구성된다는 것입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

STIX 객체 관계

관계 객체	예시 소스	예제 대상	예시 설명
객체-객체 관계	공격 패턴	맬웨어	이 관계는 이 공격 패턴이 이 맬웨어 인스턴스(또는 제품군)를 전달하는 데 사용됨을 설명합니다.
객체-표시기 관계	표시기	공격 패턴, 캠페인, 인프라, 침입 세트, 멀웨어, 위협 액터, 도구	이 관계는 표시기가 관련 공격 패턴, 캠페인, 인프라, 침입 세트, 멀웨어, 위협 액터 또는 도구의 증거를 탐지할 수 있음을 설명합니다. 증거가 직접적이지 않을 수 있습니다. 예를 들어, 표시기는 특정 캠페인에서 일반적으로 사용되는 맬웨어와 같은 캠페인의 2차 증거를 감지할 수 있습니다.
객체-옵저버블 관계	인프라	관찰 데이터	이 관계는 표시기가 관찰된 데이터 객체의 정보를 기반으로 생성됨을 설명합니다. 객체-옵저버블 정의 관계의 예는 인프라가 잠재적인 공격에 대한 정보를 제공하는 사이버 옵저버블 객체로 구성된다는 것입니다.

객체-객체 관계 정의

표시기 객체를 제외한 SDO 간의 관계를 정의합니다.

시작하기 전에
필요한 역할: sn_ti.admin

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **IoC** 리포지토리 〉 객체-객체-관계.

2. 새로 만들기를 클릭합니다.

3. 양식에 있는 필드를 적절하게 작성합니다.

4. 제출을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

객체-표시기 관계 정의

표시기 객체와 다른 SDO 간의 관계를 정의합니다.

시작하기 전에
필요한 역할: sn_ti.admin

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **IoC** 리포지토리 〉 객체-표시기-관계.
2. 새로 만들기를 클릭합니다.
3. 양식에 있는 필드를 적절하게 작성합니다.
4. 제출을 클릭합니다.

객체-옵저버블 관계 정의

SDO와 옵저버블 객체(SCO) 간의 관계를 정의합니다.

시작하기 전에
필요한 역할: sn_ti.admin

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **IoC** 리포지토리 〉 객체-옵저버블-관계.
2. 새로 만들기를 클릭합니다.
3. 양식에 있는 필드를 적절하게 작성합니다.
4. 제출을 클릭합니다.

STIX 비주얼라이저

STIX 비주얼라이저는 STIX 객체의 구조와 그 관계를 시각적으로 나타냅니다.

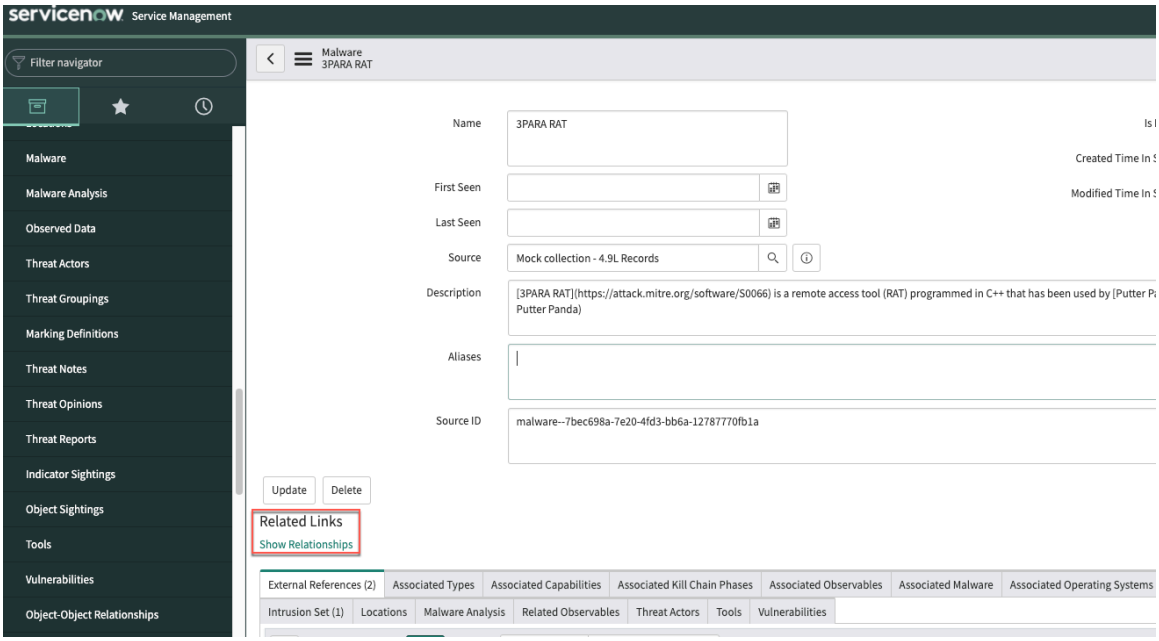
상세 정보 창에서 선택한 객체 또는 관계에 대한 자세한 정보를 확인할 수 있습니다.

관계 그래프는 객체에 대한 관계를 보여주고 조사할 수 있는 컨텍스트를 제공합니다. 그래프에서 노드를 클릭하면 자세한 내용을 볼 수 있습니다.

주:
STIX Visualizer는 보고서 및 관찰 데이터 개체를 제외한 모든 SDO에 사용할 수 있습니다.

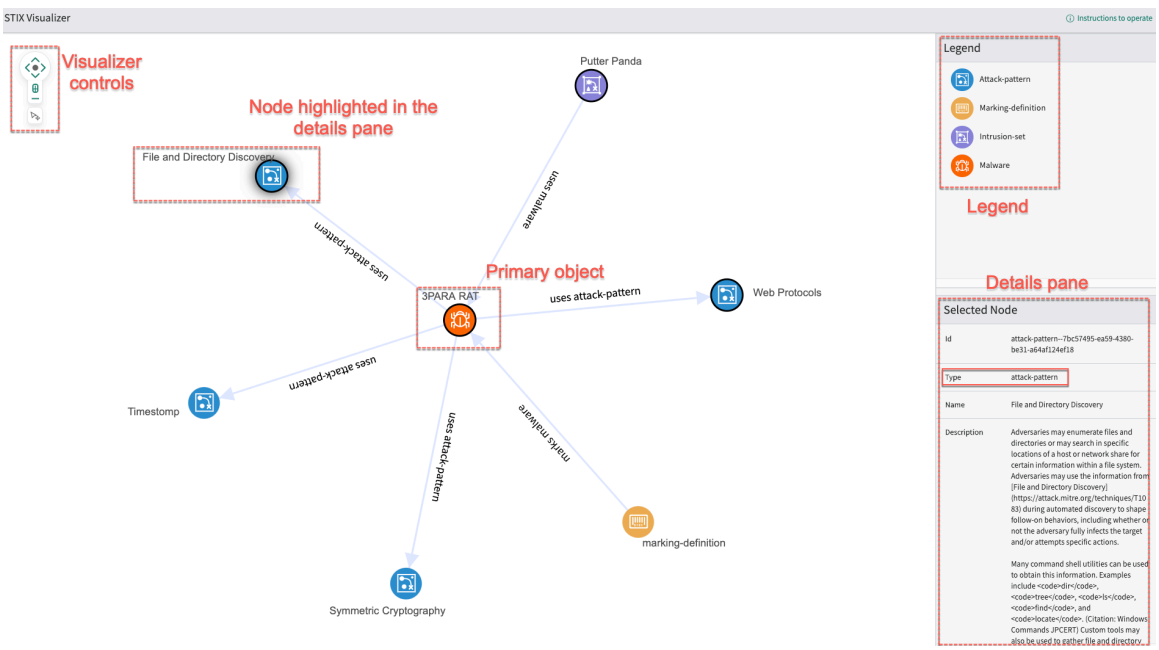
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

STIX Visualizer에 액세스



STIX Visualizer를 보려면 SDO에 대한 관련 링크 섹션에서 관계 표시를 클릭합니다.

STIX Visualizer에서 상세 정보 보기



시각화 도우미에서 개체 및 해당 관계를 볼 수 있으며, 이를 통해 자세히 조사할 수 있는 컨텍스트를 얻을 수 있습니다. 시각화 도우미는 색상과 아이콘을 사용하여 개체에 대한 다양한 정보를 나타냅니다.

객체를 확대하거나, 노드를 끌거나, 고정하여 특정 관계에 초점을 맞출 수 있습니다.

객체를 클릭하여 상세 정보 창을 엽니다. 상세 정보 창에서 객체와 관련된 자세한 정보를 확인할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

MITRE-ATT&CK™ 프레임워크 개요

프레임워크는 MITRE-ATT&CK 조직에서 사이버 공격에 대하여 특정 위협 모델과 방법론을 개발하기 위해 접근할 수 있는 공통적인 전술, 기술 및 절차(TTP)의 지식베이스입니다.

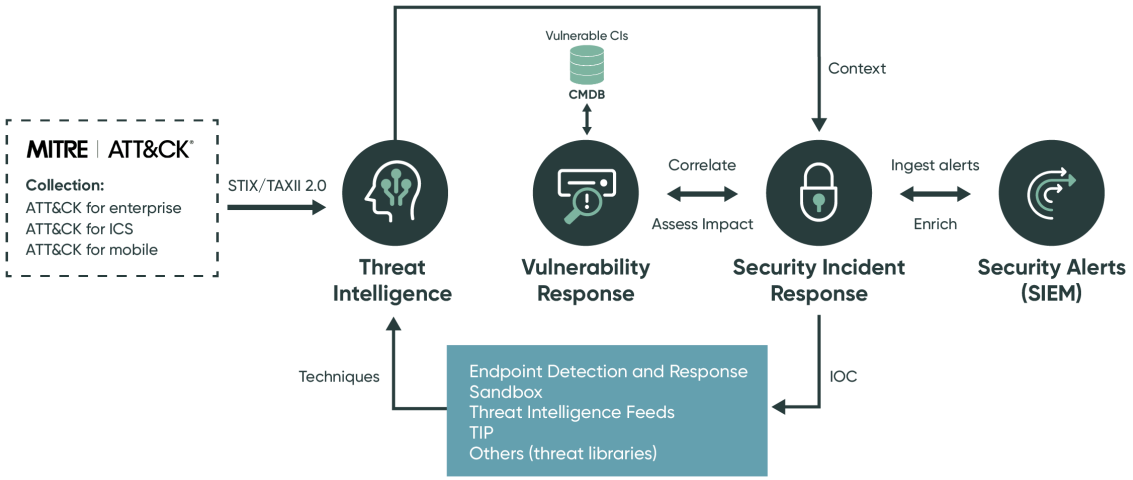
개요

ATT&CK(Adversarial Tactics, Techniques, and Common Knowledge) 프레임워크는 MITRE 사이버 공격의 여러 단계에서 사용되는 다양한 적대적 기술을 문서화하고 추적합니다.

프레임워크의 지식 기반을 사용하여 MITRE-ATT&CK 사이버 위협 인텔리전스 커뮤니티는 위협을 신속하게 식별하고 사이버 공격 대응을 조정할 수 있습니다.

MITRE-ATT&CK 보안 운영

다음 다이어그램을 MITRE-ATT&CK 통해 정보가 애플리케이션과 함께 보안 운영 흐르는 방식을 알아봅니다.



- 는 미리 로드됨 TAXII 클라이언트 데이터 수집위협 인텔리전스을 수집하기 위해 TAXII 서버에 연결합니다.
- 기존 SIEM(보안 정보 및 이벤트 관리자) 통합은 관련 TTP와 함께 위협 데이터(경보 및 이벤트)를 수집하며 보안 인시던트와 연결됩니다.
- IoC가 보안 인시던트위협 인텔리전스와 연결되면 위협 피드에서 관련 정보를 자동으로 검색하고 추가 분석을 위해 IoC를 EDR, Sandbox 또는 TIP와 같은 타사 소스로 보냅니다.
- 제3자 소스에 MITRE-ATT&CK 정보가 포함되어 있는 경우 위협 인텔리전스 기술 정보 추출 상관 관계 및 분석을 위해 리포지토리의 위협 인텔리전스 데이터를 보강합니다.
- MITRE-ATT&CK 는 또한 각 기술에 대한 CVE 컨텍스트 정보를 공유합니다. 보안 팀은 악용 취약성 대응 된 기술을 검토하여 비즈니스에 중요한 자산이 위협받는지 확인할 수 있습니다.

MITRE-ATT&CK 매트릭스, 전술 및 기술

프레임워크의 MITRE-ATT&CK 핵심은 적의 전술과 기술의 매트릭스입니다. 전술의 시퀀스는 공격자가 인시던트 단계에서 달성하려고 하는 것을 나타냅니다. 보안 팀이 이 시퀀스를 이해하면 공격자의 다음 움직임을 예측하고 킬 체인을 끊을 수 있습니다. ATT&CK는 다음 매트릭스로 구성됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- Enterprise ATT&CK: 엔터프라이즈 네트워크 및 클라우드에서 악의적 사용자가 손상시키고 운영하기 위해 취하는 동작과 작업을 설명합니다.

  주:
  Pre ATT&CK 매트릭스는 엔터프라이즈 매트릭스에서 MITRE 더 이상 사용되지 않으며 엔터프라이즈 매트릭스와 병합됩니다.

- ICS ATT&CK: ICS(산업 제어 시스템) 네트워크 내에서 작동하는 동안 악의적 사용자가 수행하는 작업을 설명합니다.
- 모바일 ATT&CK: 모바일 장치에 초점을 맞춘 악의적 동작 및 작업을 설명합니다.

전술은 ATT&CK 기술의 이유를 나타냅니다. 행동을 수행하기 위한 상대의 전술적 목표입니다.

기술은 공격자가 작업을 수행하여 전술적 목표를 달성하는 방법을 나타냅니다.

기술은 하나 이상의 전술과 연관될 수 있습니다. 예를 들어, 액세스 토큰 조작은 악의적 사용자가 권한 에스컬레이션 또는 방어 회피 전술을 달성하는 데 사용됩니다.

인시던트 응답에 의도 기반 접근 방식 사용

의도 기반 응답은 조직에서 보안 인시던트의 상관 관계를 파악하고 광범위한 공격을 식별하는 데 도움이 될 수 있는 동적인 상황별 킬 체인 프레임워크를 사용합니다. 보안 팀은 의도 기반 응답을 사용하여 조직이 어떻게 공격을 받고 있으며 공격자가 다음에 무엇을 할 수 있는지 이해할 수 있습니다. 이러한 유형의 응답을 사용하면 공격자의 동작을 예측하여 리소스를 효과적으로 집중할 수 있습니다.

를 사용하여 보안 인시던트 응답보안 팀은 IP 주소, 파일 해시 및 도메인과 같은 침해 표시기(IOC)에 중점을 두어 분석에서 억제까지 각 보안 인시던트의 수명주기를 관리할 수 있습니다.

프레임워크와 MITRE-ATT&CK 통합 보안 인시던트 응답 하면 보안 인시던트가 더 큰 전사적 공격의 링크로 처리됩니다.

조직이 보안 운영에서 얻을 수 있는 이점 **MITRE-ATT&CK**

MITRE-ATT&CK 프레임워크를 사용하면 조직에서 다음을 수행하는 데 도움이 됩니다.

- 보안 분석가 MITRE-ATT&CK 에게 전술, 기술 및 절차(TTP)를 제공하여 보안 인시던트를 보다 효과적으로 분석하고 대응할 수 있도록 합니다.
- 프레임워크의 컨텍스트에서 위협을 탐지하고 억제하기 위한 플레이북을 사용하여 인시던트 워크플로우를 자동화합니다 MITRE-ATT&CK .
- 정보를 사용하여 MITRE-ATT&CK 손상 및 위협 헌팅 표시기의 우선순위를 지정합니다.
- 프레임워크의 컨텍스트에서 조직의 높은 수준의 보안 태세를 MITRE-ATT&CK 이해합니다.

MITRE-ATT&CK 관리

에서 데이터 소스를 설정 및 매핑하고, 전체 기술 탐지 범위를 매핑하고, 리포지토리를 MITRE-ATT&CK 유지 관리할 수 있습니다 ServiceNow AI Platform.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프레임워크 시작하기 **MITRE-ATT&CK**

프레임워크 설정을 MITRE-ATT&CK 시작하기 전에 다음 정보를 검토합니다.

검사 목록

설정 작업	설명
필수 ServiceNow AI Platform, 위협 인텔리전스및 보안 인시던트 응답 역할을 할당했는지 확인합니다.	기능 전반에 걸쳐 사용되는 역할은 다음과 같습니다 MITRE-ATT&CK . • 관리자(admin)는 에서 ServiceNow Store 애플리케이션을 설치하고 보안 인시던트 관리자(sn_si.admin) 및 위협 인텔리전스 관리자(sn_ti.admin) 역할을 할당합니다. • sn_ti.admin • sn_si.admin • sn_si.analyst • sn_ti.읽기 • sn_ti.쓰기 • sn_ti.mitre_analyst - MITRE 분석가 역할은 위협 인텔리전스 지원 공통 보안 인시던트 응답 간의 기능에 대한 교차 탐색을 MITRE 허용하기 위해 도입되었습니다. 이 역할을 사용하면 모듈과 보안 인시던트 응답 모듈을 모두 위협 인텔리전스 MITRE 읽기 전용 모드로 볼 수 있습니다. • sn_si.read 자세한 내용은 Threat Intelligence 설정을 참조하십시오.
ServiceNow 모듈을 지원하는 MITRE-ATT&CK 데 필요한 핵심 애플리케이션이 설치되고 활성화되었는지 확인합니다.	에서 ServiceNow Store다음 보안 운영 애플리케이션이 설치되고 활성화되는지 확인합니다. 설치되지 않은 경우 원활한 설치를 위해 다음 순서로 한 번에 하나의 애플리케이션을 설치하고 활성화합니다. • Threat Intelligence 지원 sn_ti_seismic(일반 UI 구성요소) - 버전 1.0 이상 • Threat Intelligence Support Common - 버전 12.0 이상 • 위협 인텔리전스 - 버전 12.0 이상 • 보안 인시던트 응답 - 버전 12.0 이상 통합을 위한 인스턴스 설정에 ServiceNow AI Platform 대한 자세한 내용은 보안 운영 제품 또는 애플리케이션에 대한 권리 가져오기 및 ServiceNow Store 애플리케이션 활성화를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

검사 목록

설정 작업	설명
도메인 분리	데이터, 프로세스 및 관리 작업을 분리하려면 도메인 분리 섹션을 확인합니다.

MITRE 대상 **STIX** 데이터 모델 이해

에서 MITRESTIX 사용하는 용어를 검토하고 에서 ServiceNow AI Platform프레임워크를 효율적으로 사용하고 이해합니다MITRE-ATT&CK™.

MITRE 매핑할 **STIX** 객체

STIX 는 사이버 위협 정보를 표준화되고 구조화된 방식으로 설명하기 위한 언어입니다. 모듈의 상위 데이터 모델은 위협 인텔리전스 객체입니다 STIX . MITRE 객체는 상위 STIX 데이터 모델의 하위 집합입니다. MITRE-ATT&CK 프레임워크 MITRE 에서 특정 레이블 및 객체로 유사한 STIX 정보를 제공합니다.

MITRE객체 매핑에 **STIX**

MITRE 용어	STIX 용어
기술	공격 패턴
완화	동작 방침
그룹	침입 세트
맬웨어	맬웨어
도구	도구

모듈에서 위협 인텔리전스 데이터 확장

위협 소스 목록을 위협 인텔리전스 유지 관리하고 광범위한 사이버 위협 정보 세트가 포함된 필요한 STIX 데이터를 임포트할 수 있습니다. 또한 프로필을 사용하여 TAXII 사이버 위협 정보의 자동화된 교환을 용이하게 할 수 있습니다.

주:
자세한 내용은 위협 소스 정의 및 TAXII 프로파일 생성을 참조하세요.

모듈에서 **MITRE-ATT&CK** 데이터 확장

Malware, Group, Mitigation 및 Tool 개체를 리포지토리의 기술로 확장할 수 있습니다 MITRE-ATT&CK .

MITRE ATT&CK 리포지토리 모듈에서 객체를 생성하고 기술과 새 객체 간의 관계를 설정할 수 있지만 이 모듈에서 관계 유형을 정의할 수는 없습니다. 관계 유형을 정의하려면 다음으로 이동하십시오. 위협 인텔리전스 〉 **IoC** 리포지토리 〉 객체-객체 관계 모듈.

기존 기술과 기존 객체 간의 관계 유형을 매핑하는 경우 기술을 대상 객체로 정의하고 객체를 소스 객체로 정의해야 합니다. 이렇게 하려면 **IoC** 리포지토리 〉 객체-객체 관계 모듈.

그룹을 생성하여 공격 패턴과 연결할 수 있지만 MITRE ATT&CK 리포지토리에서는 그룹과 공격 패턴 간의 관계만 설정할 수 있습니다. 객체 간 관계 유형을 정의하려면 IoC 리포지토리에서 이를 수행해야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
자세한 내용은 다음을 참조하십시오. 뻗치다 MITRE-ATT&CK 데이터 및 IoC 저장소.

도메인 분리 및 **MITRE-ATT&CK**

이 도메인 분리 개요는 에 MITRE-ATT&CK관련됩니다. 도메인 분리를 사용하여 데이터, 프로세스 및 관리 작업을 도메인이라는 논리적 그룹으로 분할할 수 있습니다. 그런 다음 사용자가 데이터를 보고 액세스할 수 있는 것을 포함하여 이러한 분리의 여러 가지 측면을 제어할 수 있습니다.

지원 수준

지원: 기본.

에서 도메인 분리가 작동하는 방식 **MITRE-ATT&CK**

도메인 분리를 수행하려면 다음 단계를 따르십시오.

- 해당 도메인에서 필요한 sn_ti.admin 역할을 가진 사용자를 생성합니다.
- 모든 도메인에 다음을 복제합니다.
  - TAXII 컬렉션

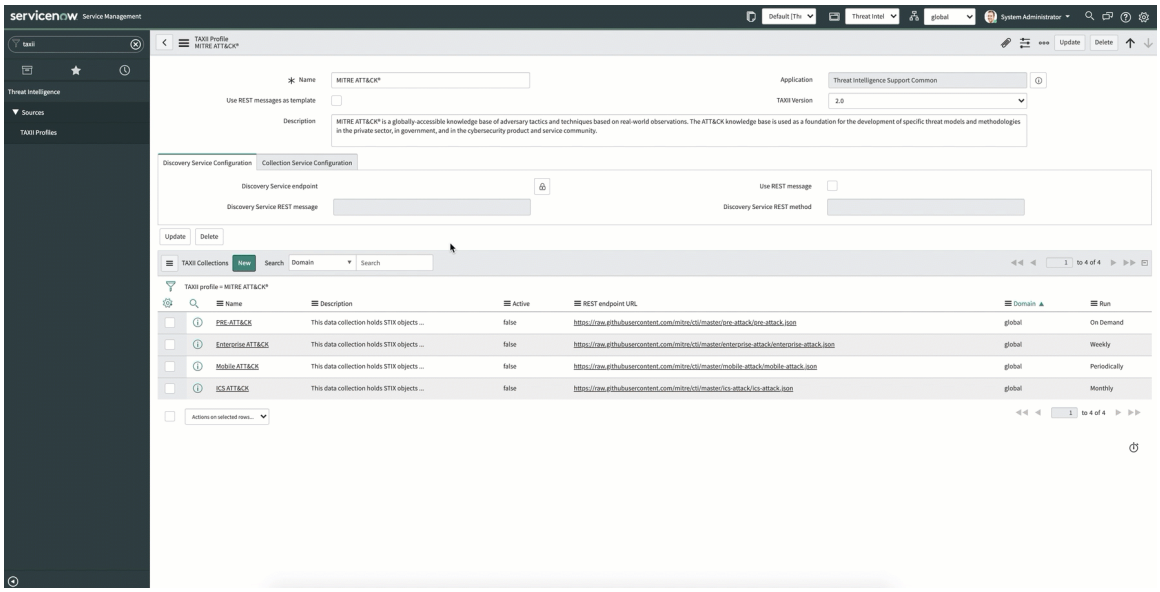
    주:
    - 전역 도메인에서 컬렉션을 활성화하지 마십시오. 복제되어 도메인에서 사용할 수 있는 컬렉션만 활성화합니다.
    - 컬렉션의 '다음으로 실행 ' 필드를 해당 도메인에서 sn_ti.admin 역할을 가진 사용자로 변경합니다.
  - 기술 범위 정의
  - 기술 추출 규칙
  - 탐지 규칙 – MITRE ATT&CK 매핑
  - 완화 범위
    - 모든 완화 범위 정의 기록을 복사합니다.
    - 완화 범위 계산기를 복사하거나 해당 도메인에 대한 새 계산기를 생성합니다.
  - 위협 그룹 - 기술 히트맵 정의

TAXII 컬렉션 복제

1. 다음으로 이동 위협 인텔리전스 〉 소스 〉 **TAXII** 프로파일.
2. 헤더 표시줄에서 도메인 선택기를 사용하여 도메인을 선택합니다.
3. 조직과 관련된 TAXII 컬렉션(Enterprise ATT&CK, Mobile ATT&CK 또는 ICS ATT&CK)을 선택합니다.
4. 헤더 막대를 마우스 오른쪽 버튼으로 클릭하고 삽입 및 유지를 선택합니다. 선택한 도메인 아래에 중복 TAXII 컬렉션이 생성됩니다.
5. MITRE ATT&CK TAXII 프로파일로 다시 이동하여 중복된 TAXII 컬렉션을 확인합니다.

다음 그림에서는 도메인 TOP/Initech을 선택하고, 도메인에서 TAXII 컬렉션을 복제하고, 복제된 TAXII 컬렉션을 확인하는 방법을 보여 줍니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



MITRE-ATT&CK™ 프레임워크 설정

MITRE-ATT&CK 조직에서 위협 탐지를 위한 컬렉션을 설정할 MITRE-ATT&CK 수 있도록 프로필을 활성화하고 예약된 작업을 설정합니다.

시작하기 전에

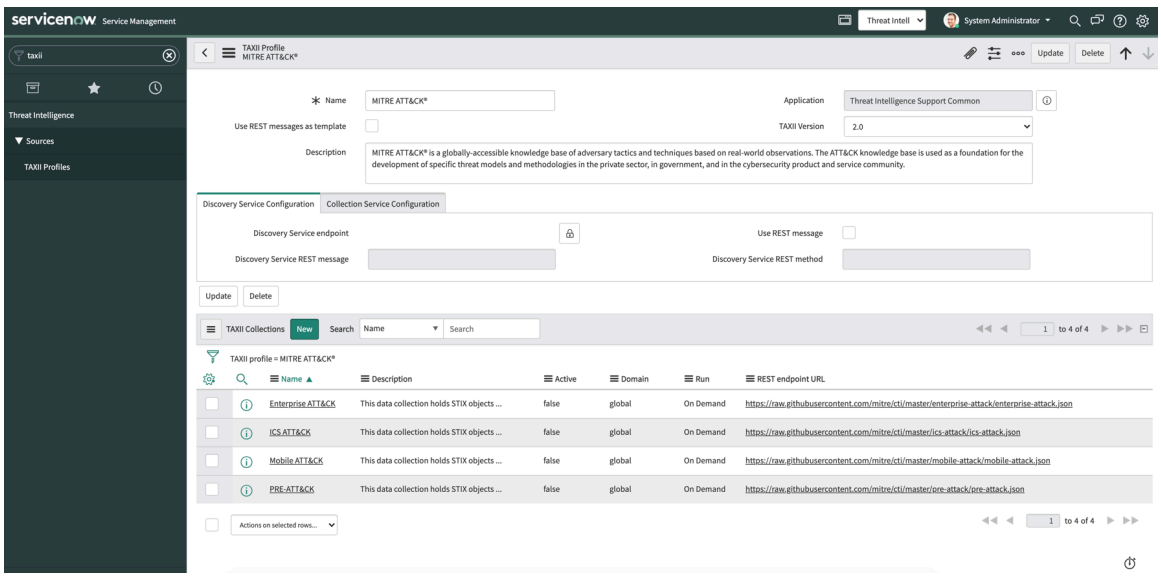
필요한 역할: sn_ti.admin

이 태스크 정보

구조화된 위협 정보 표현(STIX™)은 사이버 위협 정보를 표준화되고 구조화된 방식으로 설명하기 위한 언어입니다. STIX 데이터 및 신뢰할 수 있는 지표 정보() 프로필의 자동화된 교환을TAXII™ 사용하여 보안 팀은 공유된 사이버 위협 정보를 사용하여 회사 및 다른 소스에서 이전에 식별된 위협을 격리할 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 소스 〉 **TAXII** 프로파일.
   사용 가능한 TAXII 프로파일이 표시됩니다.
2. 기본 시스템과 함께 제공되는 **MITRE ATT&CK** 프로필을 클릭합니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 컬렉션을 활성화하려면 TAXII 조직과 관련된 컬렉션(Enterprise ATT&CK, Mobile ATT&CK 또는 ICS ATT&CK)에 대해 TAXII활성 옵션을 true로 설정합니다.

TAXII 컬렉션	설명
엔터프라이즈 ATT&CK	악의적 사용자가 엔터프라이즈 네트워크 및 클라우드에서 손상시키고 운영하기 위해 취하는 동작과 작업을 설명합니다. 주: Pre ATT&CK 매트릭스는 엔터프라이즈 매트릭스에서 MITRE 더 이상 사용되지 않으며 엔터프라이즈 매트릭스와 병합됩니다.
모바일 ATT&CK	모바일 장치에 초점을 맞춘 악의적 동작 및 작업을 설명합니다.
ICS ATT&CK	ICS(산업 제어 시스템) 네트워크 내에서 작업하는 동안 악의적 사용자가 취하는 작업에 대해 설명합니다.

4. 컬렉션을 정기적으로 새로 고치려면 조직에 맞게 실행 옵션을 설정합니다. 기본적으로 이 옵션은 요청 시로 설정됩니다.

주:

a. 컬렉션은 Core 플러그인의 위협 인텔리전스 일부로 패키지됩니다. Threat Intelligence Support Common 버전 12.0 이상 및 Threat Intelligence 버전 12.0 이상을 설치하거나 업데이트하면 수집 데이터가 자동으로 채워집니다.

b. 조직에서 사용하려는 컬렉션에 대해서만 컬렉션을 활성화 TAXII 하고 다른 컬렉션은 비활성화합니다. 예를 들어 엔터프라이즈 ATT&CK 매트릭스를 사용하려면 컬렉션 수준과 매트릭스 수준에서 엔터프라이즈 ATT&CK TAXII 를 활성화합니다. 수집 및 매트릭스 수준에서 다른 Mobile ATT&CK 및 ICS ATT&CK 매트릭스 TAXII 를 비활성화합니다.

c. TAXII 컬렉션 관련 목록에서 실행 옵션을 매일로 선택하면 오류가 발생하고 옵션이 요청 시로 기본 설정됩니다. 이 오류는 서버의 부하를 최적화하기 위해 매일 데이터 새로 고침을 MITRE-ATT&CKMITRE 예약하는 것이 제한되기 때문에 발생합니다. MITRE 또한 ATT&CK 데이터는 일년에 두 번만 업데이트됩니다.

d. TAXII 컬렉션을 활성화하지 않으면 컬렉션이 TAXII 새로 고쳐지지 않습니다.

e. 기존 컬렉션에 MITRE 대한 업데이트는 각 컬렉션에서 '실행' 빈도를 예약하여 서버에서 검색할 수 있습니다.

f. 리포지토리 데이터(맬웨어, 그룹, 완화 및 기술에 대한 도구 객체)에 대해 MITRE-ATT&CK 수행한 사용자 지정은 예약된 업데이트 중에 저장됩니다.

g. MITREMITRE-ATT&CK 일부 개체가 해지되거나 사용되지 않는 것으로 식별되거나, 새 개체가 추가되거나, 기존 개체가 수정된 지식베이스를 업데이트합니다. 가 어떤 전술이나 기술을 취소하는 경우 MITRE 이러한 객체는 에서 취소된 ServiceNow AI Platform것으로 표시됩니다. 취소된 객체는 저장소에 보관되지만 ServiceNow AI Platform.

다음에 수행할 작업

TAXII 프로파일 설정이 완료되면 MITRE-ATT&CK 저장소 데이터가 정기적으로 ServiceNow AI Platform#. 다음으로 이동하여 이 데이터를 볼 수 있습니다. **MITRE ATT&CK** 리포지토리 〉 매트릭스 및 **MITRE ATT&CK** 리포지토리 〉 기술.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

매트릭스 관리

컬렉션에서 임포트한 매트릭스를 MITRE TAXII 관리합니다. 매트릭스는 전술과 기술의 모음입니다. 매트릭스를 보고 리포지토리에서 컬렉션을 사용할 수 있는지 검토할 수 있습니다 MITRE-ATT&CK .

시작하기 전에

주:
조직에서 사용하려는 매트릭스만 활성으로 설정되어 있고 다른 매트릭스는 비활성화되어 있는지 검토하고 확인합니다. 예를 들어 엔터프라이즈 ATT&CK 매트릭스를 사용하려는 경우 엔터프라이즈 ATT&CK 매트릭스는 TAXII 컬렉션 수준과 매트릭스 수준에서 활성화됩니다. 수집 및 매트릭스 수준에서 다른 Mobile ATT&CK 및 ICS ATT&CK 매트릭스 TAXII 를 비활성화합니다.

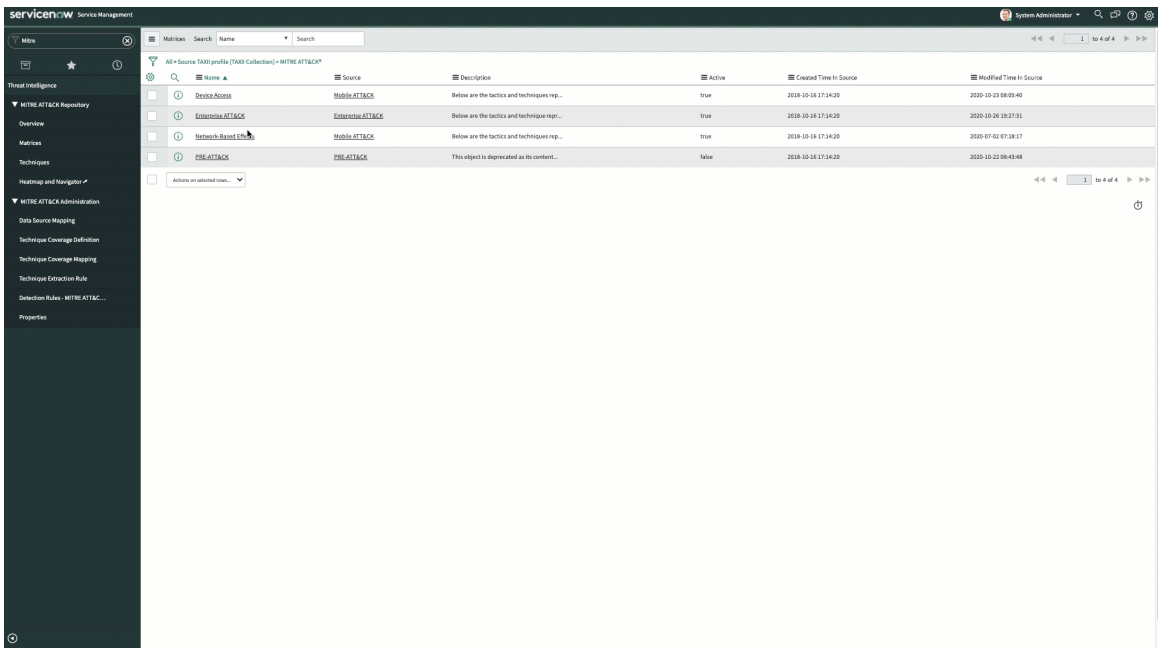
필요한 역할:

- sn_ti.admin: 액세스 삭제
- sn_ti.read: 읽기 액세스
- sn_ti.write: 생성, 쓰기 권한

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **MITRE ATT&CK** 리포지토리 〉 매트릭스.
   모든 매트릭스는 기본적으로 비활성화되어 있습니다.
2. 행렬을 활성화하려면 활성을 가리키고 두 번 클릭한 다음 **true**를 선택합니다.
3. 연관된 모든 정보를 보려면 매트릭스를 클릭합니다.
4. 이 컬렉션과 연결된 모든 전술을 보려면 **MITRE** 전술 탭을 클릭합니다.
5. 선택한 방법과 관련된 추가 상세 정보 및 기술을 보려면 방법을 클릭합니다.
6. **MITRE ATT&CK** 기술 탭에서 기술을 선택합니다.
7. 관련 목록 아래에서 선택한 기술에 사용할 수 있는 연결을 봅니다.

   다음 그림에서는 Enterprise ATT&CK 매트릭스에서 초기 액세스(TA0001) 전술, 피싱(T1566) 기술로의 탐색 경로를 볼 수 있습니다. 공격 패턴 - 피싱 기술 페이지에서 전술, 하위 기술, 그룹, 완화, 외부 참조, 맬웨어 및 도구와 같은 관련 목록을 볼 수 있습니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 수행할 작업

선택한 기술을 기반으로 이러한 관련 목록 객체 중 일부에서 정보를 확장할 수 있습니다. 예를 들어 그룹, 완화, 외부 참조, 맬웨어 및 도구에 대한 새 정보를 추가할 수 있습니다.

기술 관리

컬렉션에서 MITRE TAXII 임포트한 기술을 관리합니다. 이 기술에는 공격자가 주어진 전술을 사용하기 위해 개발한 다양한 방법이 포함되어 있습니다. 조직과 관련이 없는 기술을 검토하고 비활성화할 수 있습니다. 에서는 STIX기술을 공격 패턴이라고 합니다.

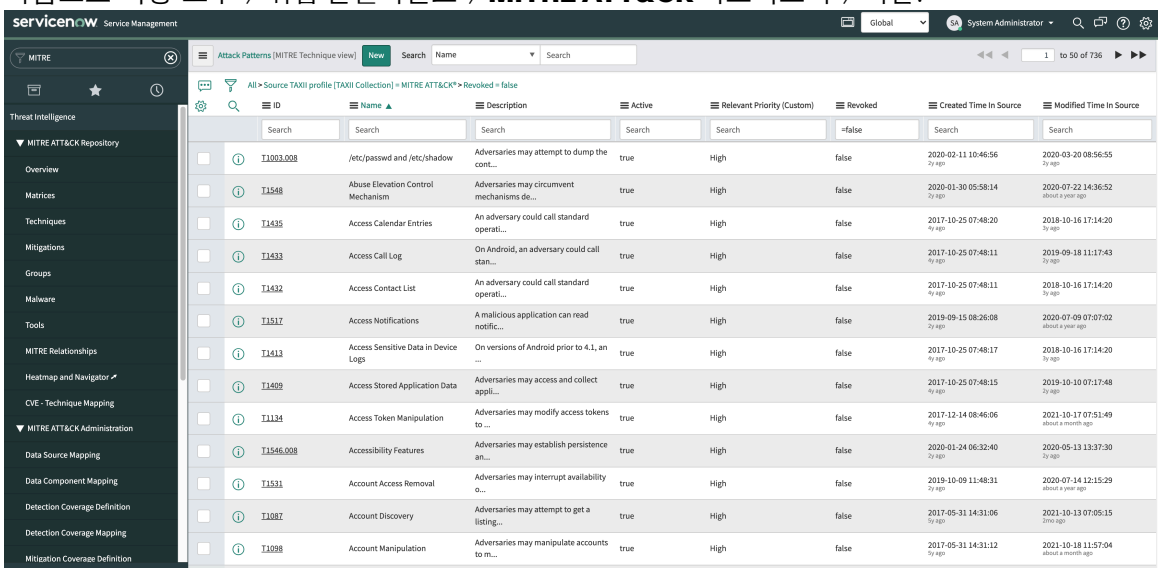
시작하기 전에

필요한 역할:

- sn_ti.admin: 액세스 삭제
- sn_si.admin: 생성, 쓰기, 삭제 권한
- sn_ti.read: 읽기 액세스
- sn_ti.write: 생성, 쓰기 권한

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **MITRE ATT&CK** 리포지토리 〉 기술.



이제 기술 및 하위 기술 목록이 나열됩니다.

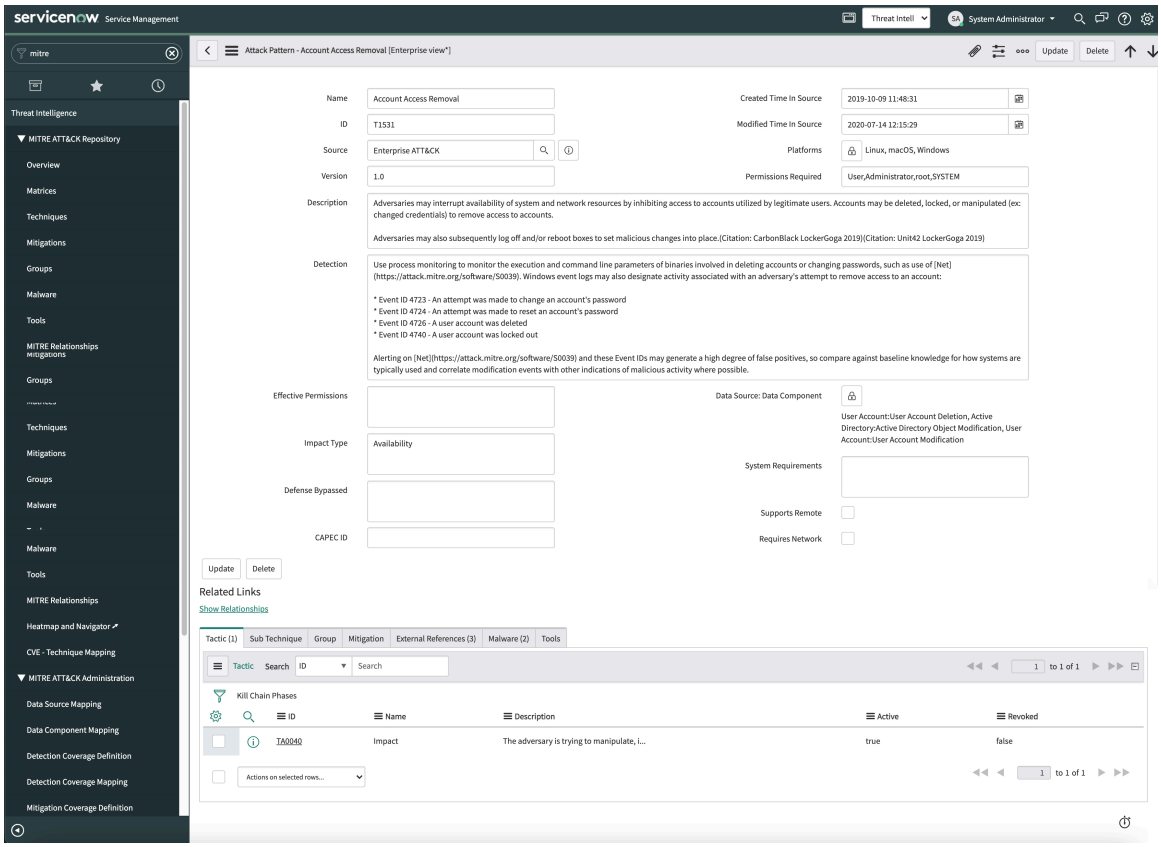
2. 조직과 관련이 없는 기술을 검토하고 비활성화하려면 선택한 기술의 목록 뷰로 이동하여 활성 열에서 설정을 **false**로 업데이트하고 설정을 저장합니다.
리포지토리의 다른 객체에서 사용하지 않는 기술을 비활성화합니다 MITRE-ATT&CK .

3. 기술의 우선순위를 지정하려면 관련 우선순위(사용자 지정) 필드에서 우선순위를 할당합니다. 기본 시스템 관련 우선순위가 없음으로 설정됩니다. 관련 우선순위(사용자 지정) 필드는 컬렉션에서 MITRE-ATT&CK TAXII 임포트되는 것이 아니라 에 도입된 ServiceNow AI Platform사용자 지정 필드입니다. 관련 우선순위 정보를 사용하여 대시보드에서, 데이터 소스 매핑 중 또는 히트맵 분석 시 기술을 필터링하고 우선순위를 지정할 수 있습니다.

4. 기술을 클릭하면 이 기술과 관련된 모든 정보를 볼 수 있습니다.

   다음 그림에서는 각 계정 액세스 제거 기술, 해당 ID, 소스 및 기타 관련 정보에 대한 세부 정보를 볼 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



주:
데이터 소스: 데이터 구성요소 요소가 도입되어 MITRE 이전 데이터 소스 필드를 대체합니다. 데이터 구성요소는 데이터 소스에 컨텍스트의 추가 하위 계층을 제공합니다. 리포지토리에 MITRE-ATT&CK 이전 TAXII 컬렉션이 포함되어 있는 경우 데이터 소스 필드를 볼 수 있습니다. 그렇지 않으면 데이터 소스: 데이터 구성요소 필드에서 데이터 구성요소의 추가 컨텍스트와 함께 데이터 소스를 볼 수 있습니다. 소스가 Enterprise ATT&CK인 경우에만 새 데이터 구성요소 필드를 볼 수 있습니다. 자세한 내용은 데이터 구성요소 매핑을 참조하십시오.

5. 이러한 객체의 관계를 보려면 관계 표시를 클릭합니다.

다음에 수행할 작업
이러한 관련 목록 객체 중 일부에서 정보를 확장할 수 있습니다. 예를 들어 그룹, 완화 및 외부 참조에 대한 새 정보를 추가할 수 있습니다.

완화 관리

컬렉션에서 MITRE TAXII 임포트한 완화 조치를 관리합니다. 완화를 사용하면 악의적 사용자가 조직에 대해 기술 또는 하위 기술을 성공적으로 실행하지 못하도록 방지할 수 있습니다. 에서 STIX완화는 동작 방침으로 알려져 있습니다.

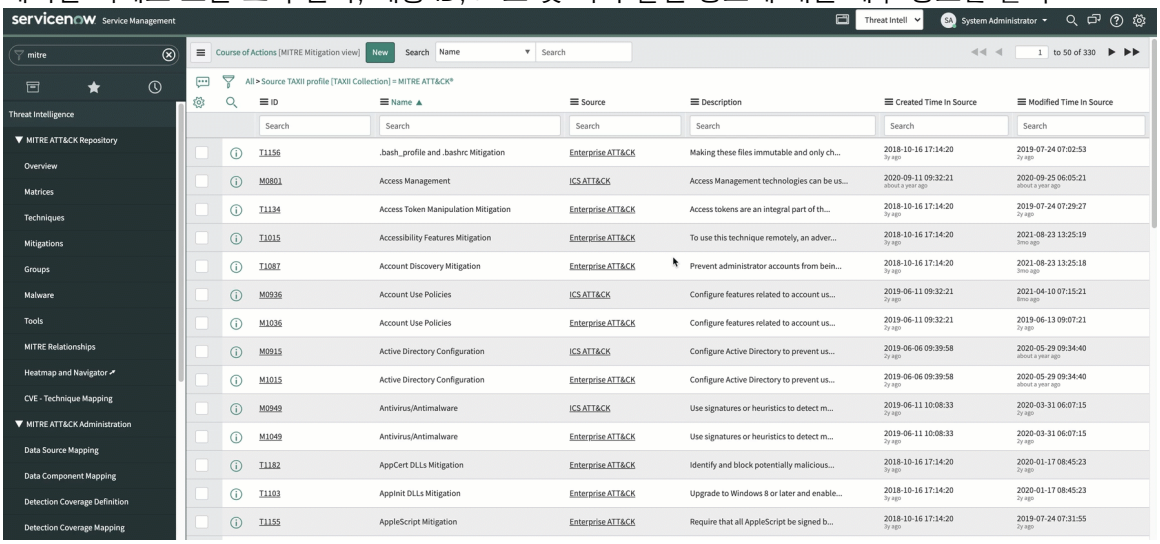
시작하기 전에
필요한 역할:

- sn_ti.admin: 액세스 삭제
- sn_ti.read: 읽기 액세스
- sn_ti.write: 생성, 쓰기 권한

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **MITRE ATT&CK** 리포지토리 〉 완화.
   이제 완화 조치가 나열됩니다.
2. 연관된 모든 정보를 보려면 완화를 클릭하십시오.
   다음 그림에서는 액세스 토큰 조작 완화, 해당 ID, 소스 및 기타 관련 정보에 대한 세부 정보를 볼 수 있습니다.



3. 이러한 객체의 관계를 보려면 관계 표시를 클릭합니다.

다음에 수행할 작업
기술 모듈을 사용하여 완화 데이터를 추가하거나 수정합니다.

그룹 관리

컬렉션에서 MITRE TAXII 임포트한 그룹을 관리합니다. 그룹은 보안 커뮤니티에서 공통 이름으로 추적되는 관련 침입 활동의 집합입니다. 분석가는 위협 그룹, 활동 그룹, 위협 행위자, 침입 세트 및 캠페인과 같은 다양한 용어를 사용하여 활동 클러스터를 추적합니다. 에서는 STIX그룹을 침입 집합이라고 합니다.

시작하기 전에
필요한 역할:

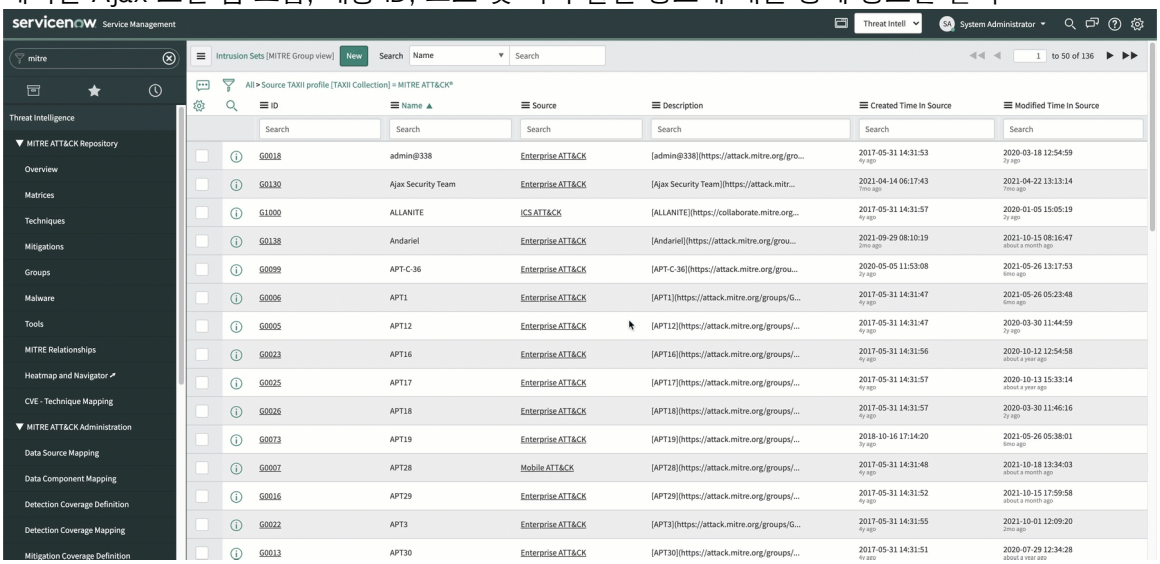
- sn_ti.admin: 액세스 삭제
- sn_ti.read: 읽기 액세스
- sn_ti.write: 생성, 쓰기 권한

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **MITRE ATT&CK** 리포지토리 〉 그룹.
   나열된 그룹을 볼 수 있습니다.
2. 연관된 모든 정보를 보려면 그룹을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음 그림에서는 Ajax 보안 팀 그룹, 해당 ID, 소스 및 기타 관련 정보에 대한 상세 정보를 볼 수 있습니다.



3. 이러한 객체의 관계를 보려면 관계 표시를 클릭합니다.

> **주:**
> 심층 조사를 위해 위협 그룹을 보안 케이스에 연결하려면 보안 케이스에 추가를 클릭합니다.

다음에 수행할 작업
기술 모듈을 사용하여 그룹 데이터를 추가하거나 수정합니다.

맬웨어 관리

컬렉션에서 MITRE TAXII 가져온 맬웨어 정보를 관리합니다. 멀웨어는 악성 코드를 나타내는 TTP의 일종입니다. 시스템에 은밀하게 삽입되는 프로그램을 말합니다. 멀웨어의 목적은 피해자의 데이터, 애플리케이션 또는 운영 체제(OS)의 기밀성, 무결성 또는 가용성을 손상시키는 것입니다.

시작하기 전에
필요한 역할:

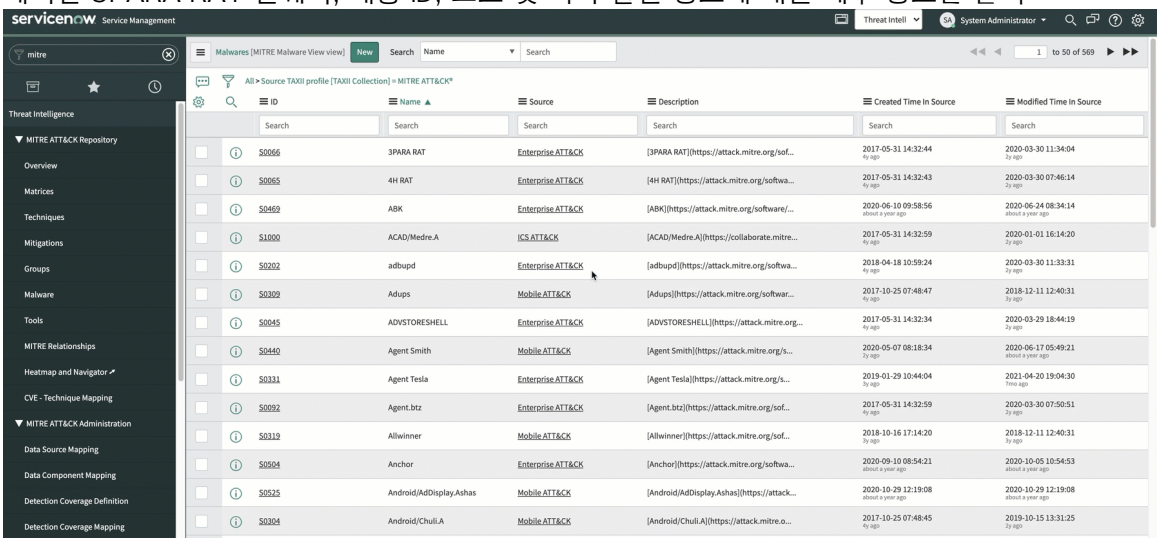
- sn_ti.admin: 액세스 삭제
- sn_ti.read: 읽기 액세스
- sn_ti.write: 생성, 쓰기 권한

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **MITRE ATT&CK** 리포지토리 〉 맬웨어.
   나열된 맬웨어를 볼 수 있습니다.
2. 모든 관련 정보를 보려면 맬웨어를 클릭하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음 그림에서는 3PARA RAT 멀웨어, 해당 ID, 소스 및 기타 관련 정보에 대한 세부 정보를 볼 수 있습니다.



3. 이러한 객체의 관계를 보려면 관계 표시를 클릭합니다.

다음에 수행할 작업

기술 모듈을 사용하여 맬웨어 데이터를 추가하거나 수정합니다.

도구 관리

컬렉션에서 MITRE TAXII 임포트한 도구 정보를 관리합니다. 도구는 위협 행위자가 공격을 수행하는 데 사용하는 합법적인 소프트웨어입니다.

시작하기 전에

필요한 역할:

- sn_ti.admin: 액세스 삭제
- sn_ti.read: 읽기 액세스
- sn_ti.write: 생성, 쓰기 권한

이 태스크 정보

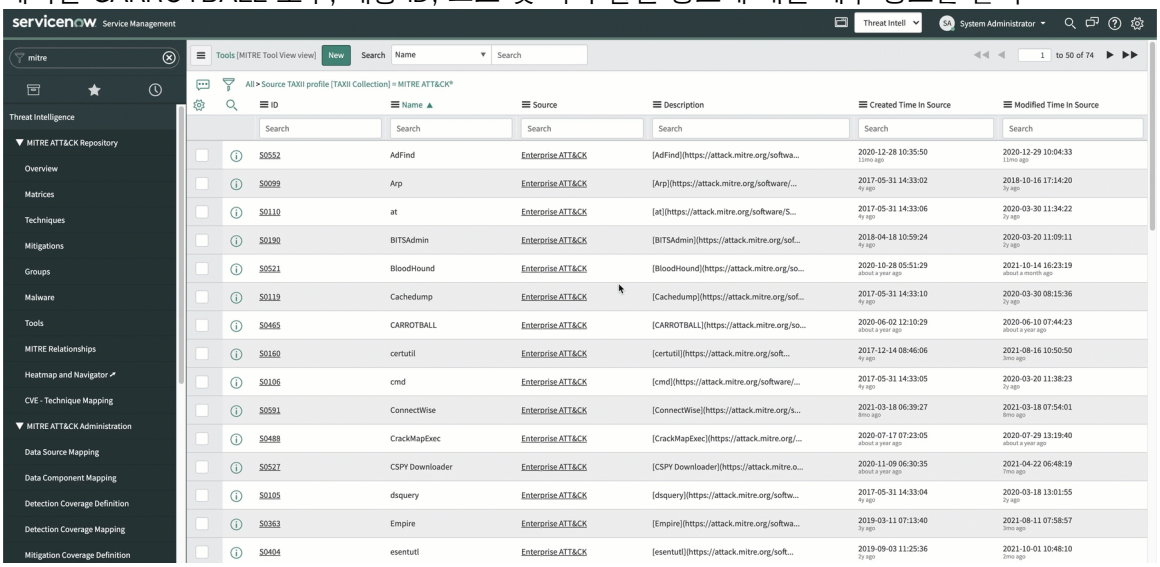
도구를 사용하면 위협 행위자가 캠페인을 실행하기 위해 도구를 사용하는 방법과 시기를 알 수 있습니다. 맬웨어와 달리 이러한 도구 또는 소프트웨어 패키지는 종종 시스템에서 발견되며 고급 사용자, 관리자, 네트워크 관리자 또는 일반 사용자를 위한 합법적인 목적을 가지고 있습니다.

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **MITRE ATT&CK** 리포지토리 〉 도구.
   나열된 도구를 볼 수 있습니다.
2. 도구를 클릭하면 관련된 모든 정보를 볼 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음 그림에서는 CARROTBALL 도구, 해당 ID, 소스 및 기타 관련 정보에 대한 세부 정보를 볼 수 있습니다.



3. 이러한 객체의 관계를 보려면 관계 표시를 클릭합니다.

다음에 수행할 작업
기술 모듈을 사용하여 도구 데이터를 추가하거나 수정합니다.

관계 관리 **MITRE**

컬렉션에서 MITREMITRE TAXII 임포트한 관계 정보를 관리합니다.

시작하기 전에
필요한 역할:

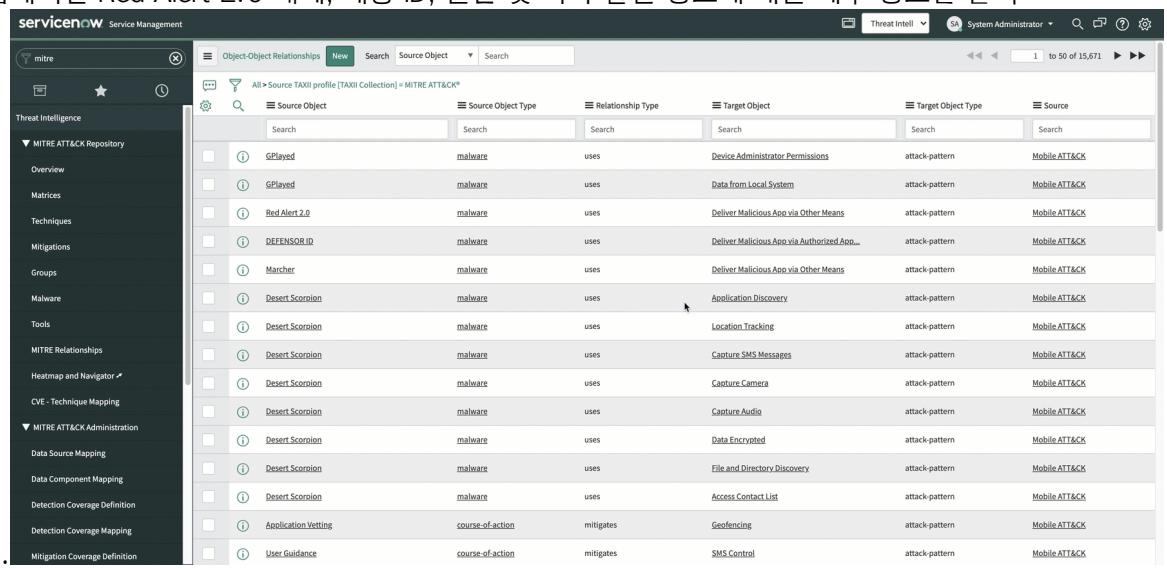
- sn_ti.admin: 액세스 삭제
- sn_ti.read: 읽기 액세스
- sn_ti.write: 생성, 쓰기 권한

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **MITRE ATT&CK** 리포지토리 〉 **MITRE** 관계.
   나열된 도구를 볼 수 있습니다.
2. 연관된 모든 정보를 보려면 소스 객체를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음 그림에서는 Red Alert 2.0 개체, 해당 ID, 원본 및 기타 관련 정보에 대한 세부 정보를 볼 수 있습니다.



3. 이러한 객체의 관계를 보려면 관계 표시를 클릭합니다.

다음에 수행할 작업
기술 모듈을 사용하여 MITRE 관계 데이터를 추가하거나 수정합니다.

CVE 및 기술 매핑 관리

컬렉션을 임포트 MITRE TAXII 한 후 매핑되는 CVE 및 기술 정보를 관리합니다.

시작하기 전에
필요한 역할:

- sn_ti.admin: 액세스 삭제
- sn_si.admin: 생성, 쓰기, 삭제 권한
- sn_ti.read: 읽기 액세스
- sn_ti.write: 생성, 쓰기 권한

주:
CVE-Technique 매핑 모듈은 Vulnerability Response 제품이 사용자 환경에 설치된 경우에만 사용할 수 있습니다.

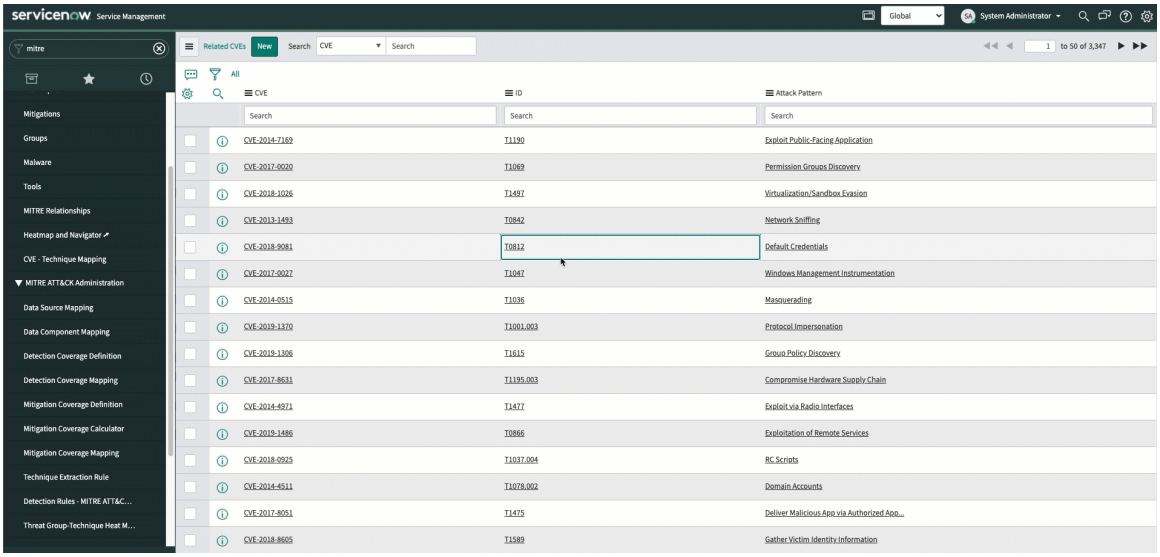
이 태스크 정보
컬렉션을 가져오 MITRE TAXII 면 환경의 CVE 및 관련 MITRE-ATT&CK 기술과의 관계를 볼 수 있습니다. CVE 및 공격 패턴과의 연결을 생성할 수도 있습니다.

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **MITRE ATT&CK** 리포지토리 〉 **CVE -** 기술 매핑.
   나열된 CVE 및 기술을 볼 수 있습니다.
2. CVE를 클릭하여 취약성 데이터베이스 항목을 봅니다.

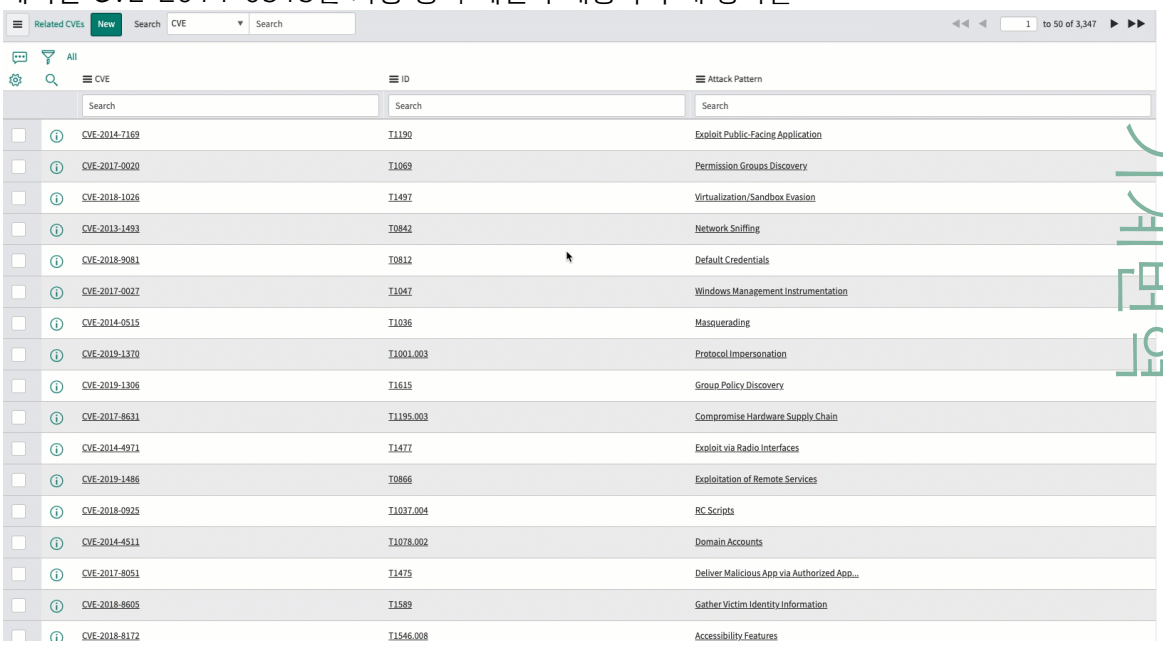
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음 그림에서는 CVE 목록 및 CVE-2014-7169에 대한 취약성 데이터베이스 항목에 대한 세부 정보를 볼 수



있습니다.

3. 항목을 추가하려면 새로 만들기를 클릭하고 CVE를 공격 패턴에 매핑한 다음 제출을 클릭합니다. 다음 그림에서는 CVE-2014-0515를 가장 공격 패턴과 매핑하여 새 항목을



만듭니다.

데이터 확장 **MITRE-ATT&CK**

리포지토리 데이터를 ServiceNow AI Platform 보강하여 확장합니다MITRE-ATT&CK.

시작하기 전에

필요한 역할:

- sn_ti.admin: 액세스 삭제
- sn_ti.read: 읽기 액세스
- sn_ti.write: 생성, 쓰기 권한

이 태스크 정보

Malware, Group, Mitigation 및 Tool 개체를 리포지토리의 기술로 확장할 수 있습니다 MITRE-ATT&CK .

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

MITRE ATT&CK 리포지토리 모듈에서 새 객체를 생성하고 기술과 새 객체 간의 관계를 설정할 수 있지만 이 모듈에서 관계 유형을 정의할 수는 없습니다. 관계 유형 정의에 대한 자세한 내용은 객체 대 객체 관계를 참조하십시오. 관계 유형을 정의하려면 다음으로 이동하십시오. 위협 인텔리전스 〉 **IoC** 리포지토리 〉 객체-객체 관계 모듈.

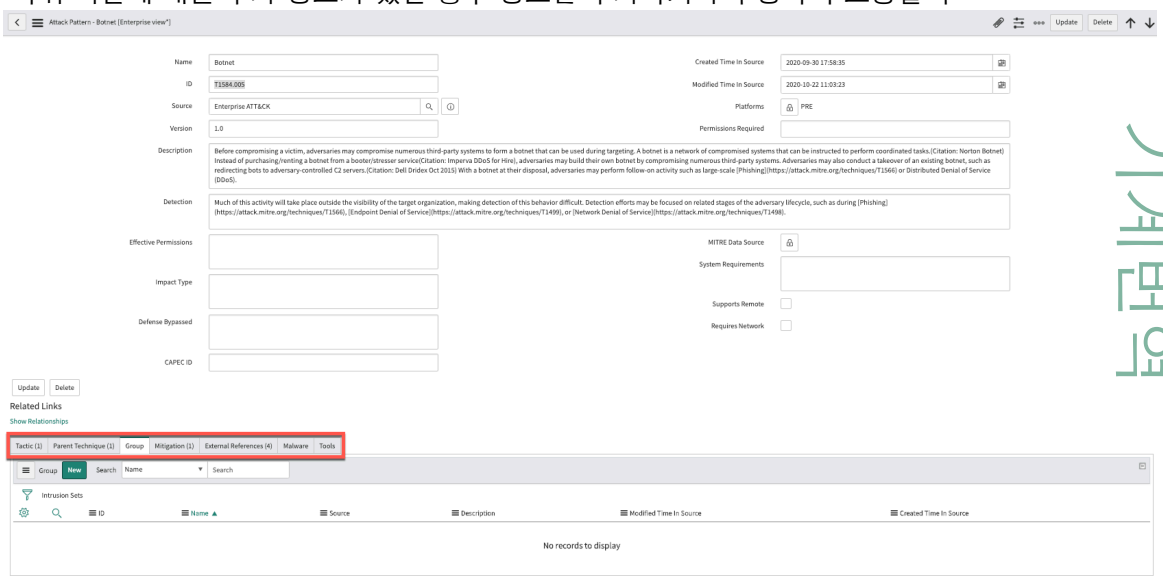
기존 기술과 기존 객체 간의 관계 유형을 매핑하는 경우 기술을 대상 객체로 정의하고 객체를 소스 객체로 정의해야 합니다. 이렇게 하려면 **IoC** 리포지토리 〉 객체-객체 관계 모듈.

그룹을 생성하여 공격 패턴과 연결할 수 있지만 MITRE ATT&CK 리포지토리에서는 그룹과 공격 패턴 간의 관계만 설정할 수 있습니다. 객체 간 관계 유형을 정의하려면 IoC 리포지토리에서 이를 수행해야 합니다.

주:
개체에 대한 모든 사용자 지정 내용은 예약된 업데이트 중에 저장됩니다.

프로시저

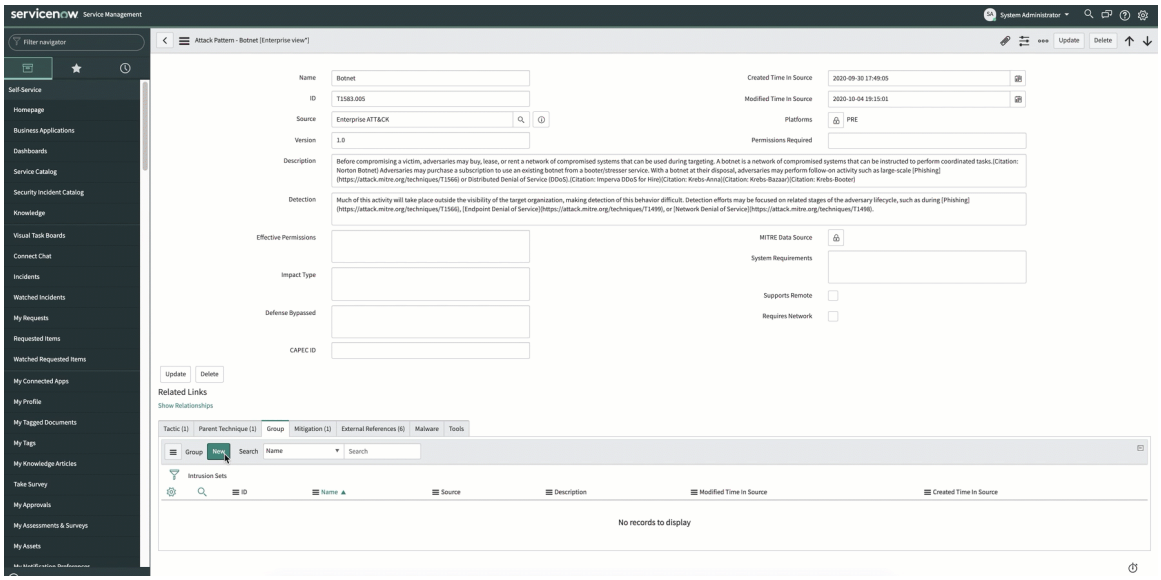
1. 다음으로 이동 위협 인텔리전스 〉 **MITRE ATT&CK** 리포지토리 〉 기술.
2. 기술 또는 하위 기술을 클릭하면 이 기술과 관련된 모든 정보를 볼 수 있습니다.
   다음 그림에서는 봇넷(T1584.005) 기술이 어떤 그룹과도 연결되지 않은 것을 볼 수 있습니다.
   기술 또는 하위 기술에 대한 추가 정보가 있는 경우 정보를 추가하거나 수정하여 보강할 수 있습니다.



3. 관련 목록을 클릭하여 데이터를 보강하고 새 그룹에 연결합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음 그림에서는 Custom1 그룹이 봇넷 하위 기술과 연결되어 있습니다.



데이터 소스 및 탐지 도구 매핑 정의

전술 및 기술에 대한 데이터 소스 및 탐지 도구 매핑을 MITRE-ATT&CK 정의합니다. 데이터 소스 매핑은 데이터 소스의 관련성 및 가용성에 대한 인사이트과 사용자 환경에서 데이터 소스를 모니터링하기 위한 탐지 도구를 제공합니다.

시작하기 전에

필요한 역할:

- sn_ti.admin, sn_si.admin: 쓰기, 삭제 권한
- sn_ti.read: 읽기 액세스

이 태스크 정보

조직에서 기술을 효과적으로 탐지하는 데 필요한 데이터 소스와 탐지 도구를 식별할 수 있습니다.

예를 들어 조직에서 5가지 기술에 중점을 두는 경우 이러한 원본을 모니터링하려면 10개의 데이터 원본과 10개의 탐지 도구가 필요할 수 있습니다. 조직에 두 개의 데이터 원본과 다섯 개의 검색 도구가 없다는 것을 확인했다고 가정해 보겠습니다. 이 연습에서는 데이터 소스, 조직과의 관련성을 파악하고 범위의 격차를 식별할 수 있습니다. 또한 올바른 데이터 원본과 검색 도구를 사용하여 환경을 개선하는 데 집중할 수 있습니다.

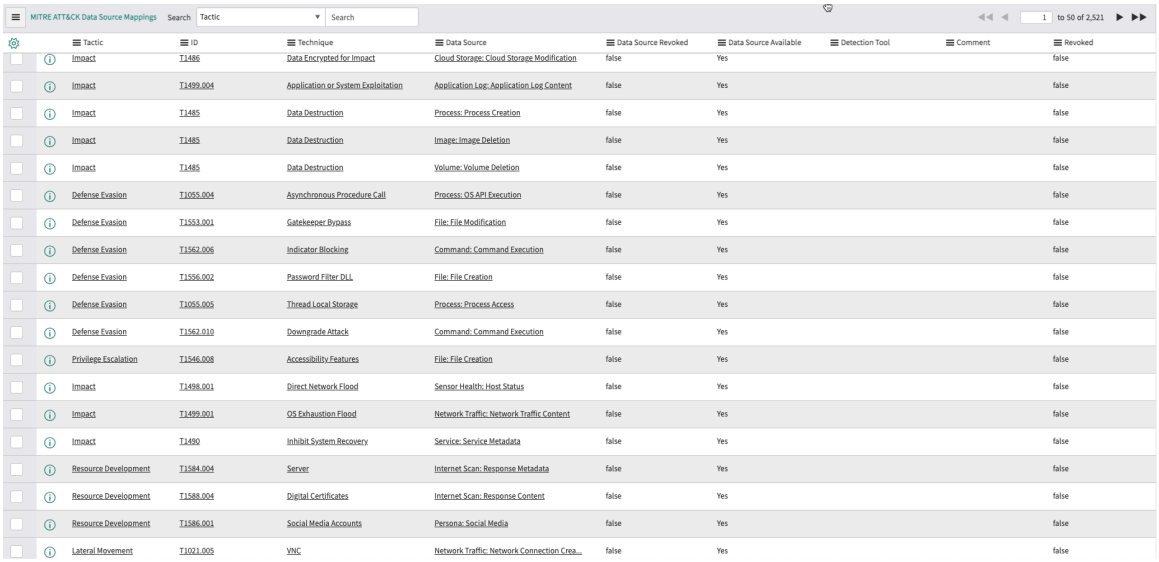
모든 활성 전술, 기술, ID 및 데이터 소스는 다음을 기반으로 자동으로 채워집니다. TAXII 프로파일

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **MITRE ATT&CK** 관리 〉 데이터 소스 매핑.

   다음 그림에서는 컬렉션 업데이트에 따라 채워진 전술, 기술 및 해당 ID 목록을 보여 줍니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



Tactic	ID	Technique	Data Source	Data Source Revoked	Data Source Available	Detection Tool	Comment	Revoked
Impact	T1486	Data Encrypted for Impact	Cloud Storage: Cloud Storage Modification	false	Yes			false
Impact	T1499.004	Application or System Exploitation	Application Log: Application Log Content	false	Yes			false
Impact	T1485	Data Destruction	Process: Process Creation	false	Yes			false
Impact	T1485	Data Destruction	Image: Image Deletion	false	Yes			false
Impact	T1485	Data Destruction	Volume: Volume Deletion	false	Yes			false
Defense Evasion	T1055.004	Asynchronous Procedure Call	Process: OS API Execution	false	Yes			false
Defense Evasion	T1553.001	Gatekeeper Bypass	File: File Modification	false	Yes			false
Defense Evasion	T1562.006	Indicator Blocking	Command: Command Execution	false	Yes			false
Defense Evasion	T1556.002	Password Filter DLL	File: File Creation	false	Yes			false
Defense Evasion	T1055.005	Thread Local Storage	Process: Process Access	false	Yes			false
Defense Evasion	T1562.010	Downgrade Attack	Command: Command Execution	false	Yes			false
Privilege Escalation	T1546.008	Accessibility Features	File: File Creation	false	Yes			false
Impact	T1498.001	Direct Network Flood	Sensor Health: Host Status	false	Yes			false
Impact	T1499.001	OS Exhaustion Flood	Network Traffic: Network Traffic Content	false	Yes			false
Impact	T1490	Inhibit System Recovery	Service: Service Metadata	false	Yes			false
Resource Development	T1584.004	Server	Internet Scan: Response Metadata	false	Yes			false
Resource Development	T1588.004	Digital Certificates	Internet Scan: Response Content	false	Yes			false
Resource Development	T1586.001	Social Media Accounts	Persona: Social Media	false	Yes			false
Lateral Movement	T1021.005	VNC	Network Traffic: Network Connection Crea...	false	Yes			false

필드	설명
방법	상대방의 목표 또는 작업 수행 이유입니다.
ID	기술의 고유한 정체성.
기술	공격자가 작업을 수행하여 전술적 목표를 달성하는 방법입니다.
데이터 소스	기술과 연결된 데이터 소스입니다.
데이터 소스 해지됨	true로 설정하면 데이터 소스가 해지되지만 데이터 소스 매핑은 계속 유지됩니다. 에서 MITRE데이터 소스 값을 찾을 수 없는 경우 해지된 데이터 소스 값은 자동으로 true로 표시됩니다. 업데이트된 MITRE 데이터에서 기술 및 데이터 소스 관계가 누락된 경우 기록에 대한 데이터 소스 매핑이 취소됩니다. 기본값: false
데이터 소스 사용 가능	데이터 소스의 가용성입니다.
탐지 도구	사용되는 기술을 탐지하여 데이터 소스를 보완하는 도구입니다. 탐지 도구는 의 SIR경보 센서와 매핑됩니다.
해지함	업데이트된 MITRE 데이터에서 기술 및 데이터 소스 관계가 누락된 경우 기록에 대한 데이터 소스 매핑이 취소됩니다. 기본값: false

2. 나열된 데이터 소스를 검토하고 환경에 따라 사용 가능한 데이터 소스 필드의 값을 수정합니다.

3. 주:
   목록 뷰에서는 이 항목을 편집할 수 없습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

탐지 도구 필드에서 다음 단계를 수행합니다.

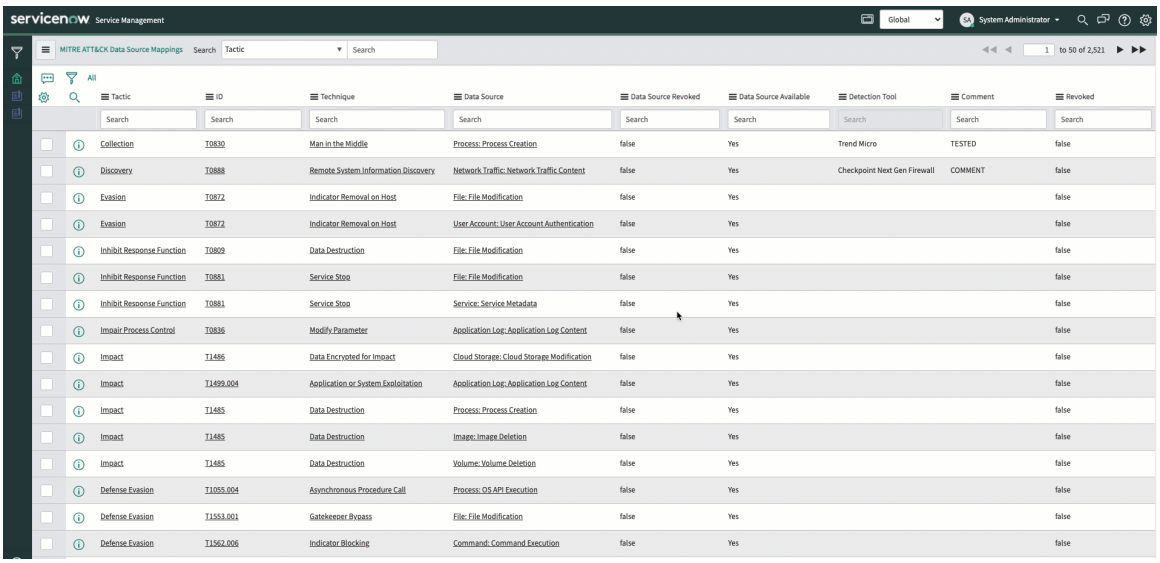
a. 정보 아이콘을 클릭하고 기록 열기를 클릭합니다.

b. 탐지 도구 항목의 잠금을 해제합니다.

c. 조회 목록을 사용하여 탐지 도구를 선택합니다. 탐지 도구를 여러 개 선택할 수 있습니다.

d. 업데이트를 클릭합니다.

다음 그림에는 데이터 원본을 모니터링하기 위해 여러 검색 도구가 추가되었습니다.



데이터 소스 및 데이터 구성요소 매핑 정의

최신 TAXII 컬렉션을 사용하고 데이터 소스, 데이터 구성요소 및 다양한 기술 간의 관계를 유지하려는 경우 데이터 구성요소 매핑을 사용합니다. 데이터 원본을 데이터 구성요소의 추가 컨텍스트와 매핑하여 데이터 원본에 컨텍스트의 추가 하위 계층을 제공하여 악의적 동작을 MITRE-ATT&CK 더 잘 이해할 수 있도록 합니다.

시작하기 전에

필요한 역할:

- sn_ti.admin, sn_si.admin: 쓰기, 삭제 권한
- sn_ti.read: 읽기 액세스

이 태스크 정보

데이터 소스와 데이터 구성요소를 매핑하면 데이터 소스 또는 구성요소와 조직과 관련된 기술에 대한 가시성을 확보할 수 있습니다.

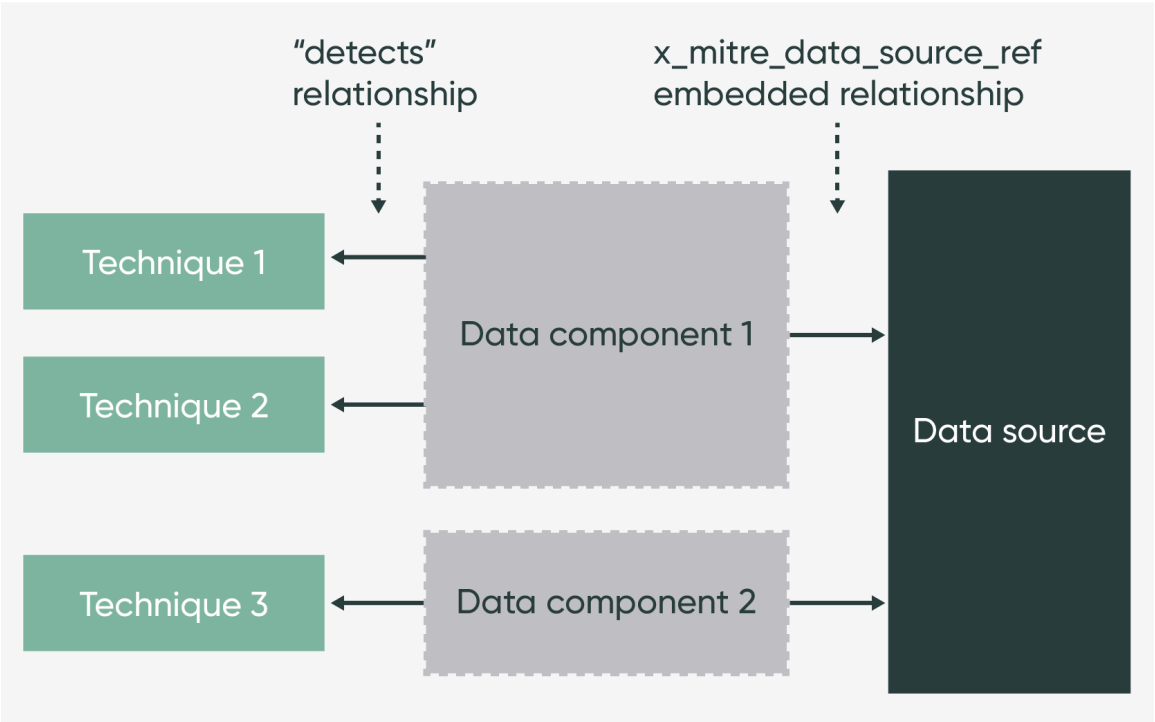
예를 들어 조직에서 7가지 기술에 중점을 두는 경우 이러한 소스를 모니터링하려면 5개의 데이터 소스와 10개의 데이터 구성요소가 필요할 수 있습니다. 내부 도구를 평가한 결과 조직에 2개의 데이터 원본과 4개의 데이터 구성 요소가 없는 것으로 나타났습니다. 이 매핑 연습은 데이터 소스, 구성요소 및 기술, 조직과의 관련성에 대한 가시성을 제공하고 범위의 격차를 식별할 수 있도록 합니다. 따라서 올바른 데이터 소스와 경보 센서에 투자를 집중하여 악의적 위협을 탐지하고 완화할 수 있습니다.

프레임워크에는 MITRE-ATT&CK 데이터 소스에 대해 업데이트된 구조(데이터 소스: 데이터 구성요소)가 포함되어 있습니다. 이 새로운 형태의 데이터 소스는 데이터 소스에 대한 추가 컨텍스트를 제공합니다. 데이터 원본 개체는 데이터 원본의 이름뿐만 아니라 수집된 데이터(파일, 프로세스, 네트워크 트래픽 등)에 대한 주요 세부 정보 및 악의적 동작을 탐지하는 데 필요한 특정 값 또는 속성을 제공합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음 그림에서는 데이터 원본 및 데이터 구성 요소에 대한 구조 표현을 MITRE-ATT&CK STIX™ 보여줍니다. 사용자 지정 STIX™ 개체로 캡처된 데이터 소스와 데이터 구성요소를 모두 볼 수 있습니다. 그림에서는 각 데이터 소스에 하나 이상의 데이터 구성요소가 포함되어 있고 각 데이터 구성요소가 하나 이상의 기술을 탐지함을 보여줍니다.

데이터 소스 및 데이터 구성요소의 일반 구조

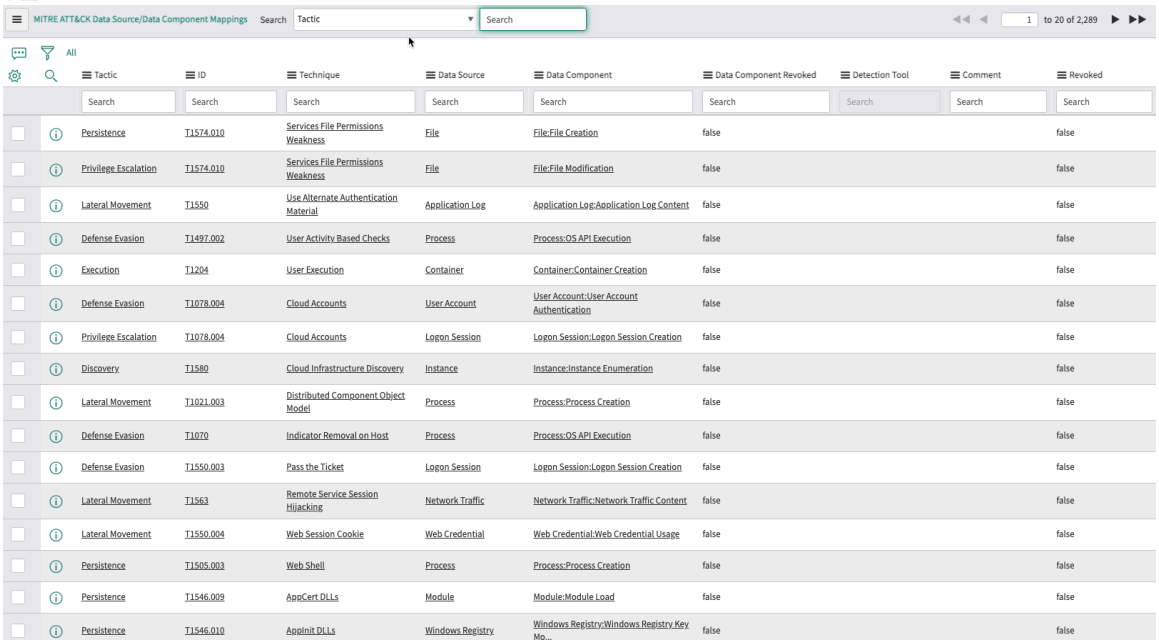


리포지토리에 이전 TAXII 컬렉션이 포함되어 있고 데이터 원본을 다양한 기술에 매핑한 경우 MITRE-ATT&CK데이터 원본 매핑을 계속 사용할 수 있습니다. 그러나 최신 TAXII 컬렉션을 사용하고 데이터 소스, 데이터 구성요소 및 다양한 기술 간의 관계를 유지하려는 경우 데이터 구성요소 매핑을 사용합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **MITRE ATT&CK** 관리 〉 데이터 구성요소 매핑.
   다음 그림에서는 컬렉션 업데이트를 기반으로 하는 데이터 소스 및 데이터 구성요소와 함께 전술, ID, 기술 목록을



Tactic	ID	Technique	Data Source	Data Component	Data Component Revoked	Detection Tool	Comment	Revoked
Persistence	T1574.010	Services File Permissions Weakness	File	File:File Creation	false			false
Privilege Escalation	T1574.010	Services File Permissions Weakness	File	File:File Modification	false			false
Lateral Movement	T1550	Use Alternate Authentication Material	Application Log	Application Log:Application Log Content	false			false
Defense Evasion	T1497.002	User Activity Based Checks	Process	Process:OS API Execution	false			false
Execution	T1204	User Execution	Container	Container:Container Creation	false			false
Defense Evasion	T1078.004	Cloud Accounts	User Account	User Account:User Account Authentication	false			false
Privilege Escalation	T1078.004	Cloud Accounts	Logon Session	Logon Session:Logon Session Creation	false			false
Discovery	T1580	Cloud Infrastructure Discovery	Instance	Instance:Instance Enumeration	false			false
Lateral Movement	T1021.003	Distributed Component Object Model	Process	Process:Process Creation	false			false
Defense Evasion	T1070	Indicator Removal on Host	Process	Process:OS API Execution	false			false
Defense Evasion	T1550.003	Pass the Ticket	Logon Session	Logon Session:Logon Session Creation	false			false
Lateral Movement	T1563	Remote Service Session Hijacking	Network Traffic	Network Traffic:Network Traffic Content	false			false
Lateral Movement	T1550.004	Web Session Cookie	Web Credential	Web Credential:Web Credential Usage	false			false
Persistence	T1505.003	Web Shell	Process	Process:Process Creation	false			false
Persistence	T1546.009	AppCert DLLs	Module	Module:Module Load	false			false
Persistence	T1546.010	AppInit DLLs	Windows Registry	Windows Registry:Windows Registry Key Mo...	false			false

보여줍니다.

필드	설명
방법	상대방의 목표 또는 작업 수행 이유입니다.
ID	기술의 고유한 정체성.
기술	공격자가 작업을 수행하여 전술적 목표를 달성하는 방법입니다.
데이터 소스	기술과 연결된 데이터 소스입니다.
데이터 구성요소	데이터 소스와 연결된 데이터 구성요소입니다. 데이터 구성요소에는 상위 데이터 소스가 하나만 있을 수 있습니다.
데이터 구성요소 해지됨	데이터 구성요소가 지식베이스에서 MITRE-ATT&CK 해지되었는지 식별합니다.
탐지 도구	사용되는 기술을 탐지하여 데이터 소스를 보완하는 도구입니다. 탐지 도구는 의 SIR경보 센서와 매핑됩니다.
설명	데이터 소스 및 데이터 구성요소 매핑에 대한 설명입니다.
해지함	기술 매핑에 대한 데이터 구성요소가 에 의해 MITRE-ATT&CK취소되는지 여부를 식별합니다.

2. 나열된 데이터 소스 및 데이터 구성요소를 검토하고 환경에 따라 값을 수정합니다.
3. 다음 단계에 따라 데이터 구성요소를 추가합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 다음으로 이동 위협 인텔리전스 〉 **MITRE ATT&CK** 관리 〉 기술.

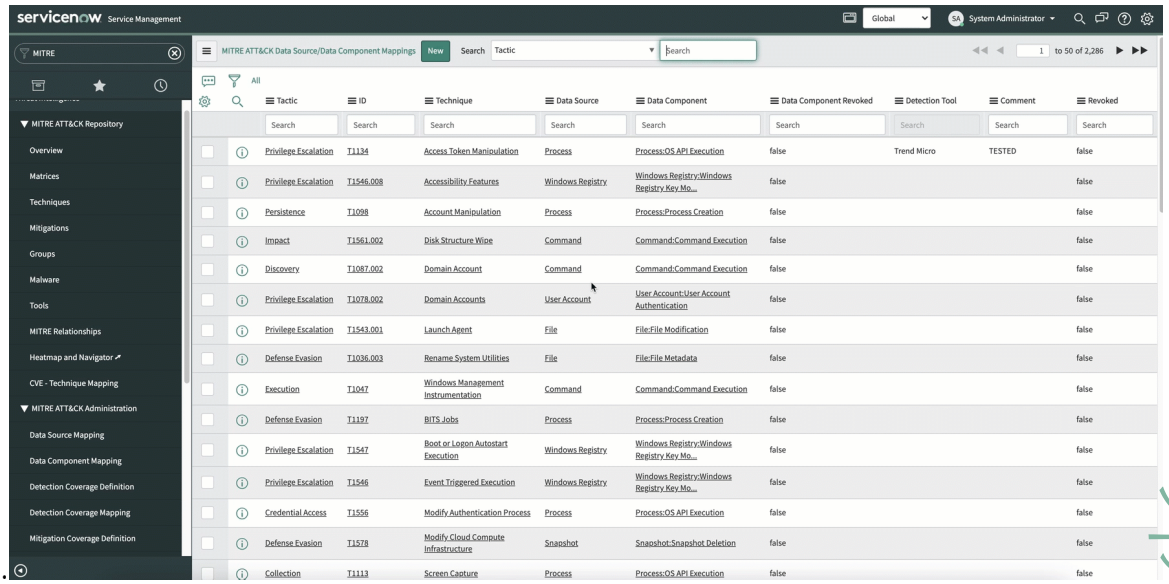
b. 데이터 소스를 수정하려는 기술(데이터 구성요소 정보)을 클릭합니다.

c. 데이터 원본 잠금 해제: 데이터 구성 요소입니다.

d. 조회 목록을 사용하여 데이터 구성요소를 선택합니다 MITRE-ATT&CK .

e. 잠금 데이터 원본: 데이터 구성요소입니다.

f. 업데이트를 클릭합니다.
다음 그림에서는 데이터 구성요소를 추가하는 방법을 보여



줍니다.

기술 탐지 범위 정의

조직에서 측정해야 하는 기술 탐지 범위를 정의하고 특정 악의적 기술을 탐지합니다.

시작하기 전에

- 필요한 역할: sn_ti.admin, sn_si.admin: 쓰기 액세스
- 필요한 역할: sn_ti.read: read access

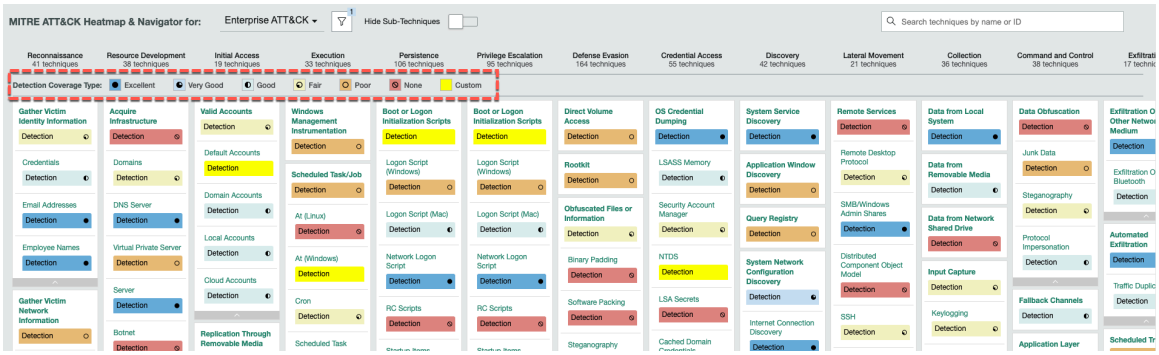
이 태스크 정보

기술 범위 정의는 전체 기술 탐지 매핑에 사용됩니다. 기본 시스템 기술 적용 범위를 사용할 수 있습니다. 기본 시스템 기술 범위는 보장 유형 없음, 나쁨, 보통, 좋음, 매우 좋음, 훌륭함으로 구성됩니다. 기본 시스템 기술 범위는 미리 정의된 색상과도 연결됩니다. 보장 유형 항목 및 색상을 사용자 지정하거나 고유한 항목을 생성할 수 있습니다. 예를 들어, 기본 시스템 범위 유형을 해당 사항 없음, 부분 범위 및 전체 범위로 수정할 수 있습니다. 또는 0-25%, 25-50% 및 50-100%와 같은 범위 유형에 대한 숫자 측정값을 만들 수도 있습니다. 기본 시스템 범위에 대한 수정 유형은 공유된 예제에 국한되지 않습니다.

보장 유형 및 색상에 대한 사용자 지정은 전체 기술 탐지 매핑 과 히트맵에도 사용됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
기본 시스템 범위 정의를 수정하면 범위 유형 아이콘이 히트맵의 기술과 함께 표시되지 않습니다. 히트맵은 기본 시스템에서 정의한 기술, 탐지 범위 및 검사 색상과 동일한 필드를 수정할 때 예상대로 작동합니다. 그러나 전체 기술 탐지 범위에서 기존 필드를 삭제하면 히트맵에 보장 유형 아이콘이 표시되지 않습니다.



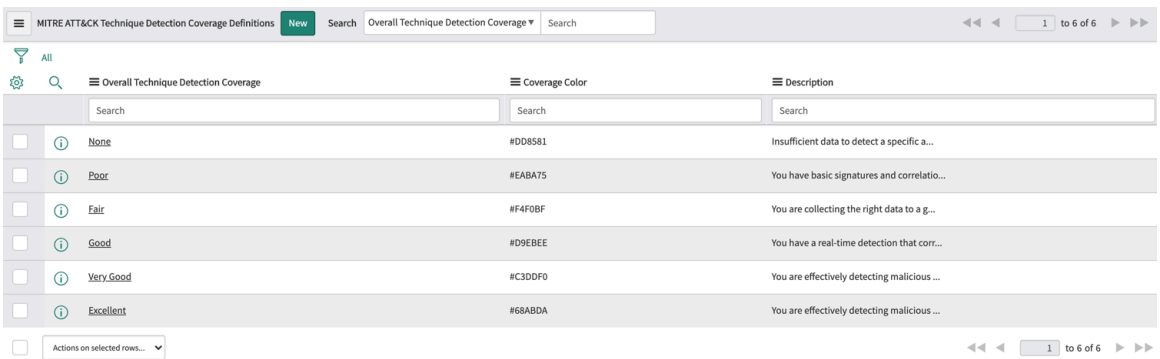
프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **MITRE ATT&CK** 관리 〉 탐지 범위 정의.
2. 전체 기술 탐지 항목을 검토하고 환경에 맞게 항목을 사용자 지정합니다.

탐지 범위 정의

필드	설명
전체 기술 탐지 범위	전체 기술 탐지 범위의 이름입니다. 기본 시스템 기술 범위는 없음, 나쁨, 보통, 좋음, 매우 좋음 또는 훌륭함으로 구성됩니다.
범위 색상	탐지 범위 점수에 할당되는 색상입니다. 정의하는 색상은 히트맵의 기술 탐지 범위에 사용됩니다. 16진수 코드와 RGB(A) 값을 사용하여 색을 사용자 지정할 수 있습니다.
설명	전체 기술 탐지 범위입니다. 점수 매기기 정의에서 기본 시스템 정의를 참조하십시오.

다음 그림에서는 검색 범위 정의 목록을 보여 줍니다.



3. 항목을 추가하려면 새로 만들기를 클릭하고 항목을 완성한 다음 제출을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

MITRE-ATT&CK 점수 매기기 정의

조직에서 특정 공격자 기술을 얼마나 효과적으로 탐지할 수 있는지 측정할 수 있도록 조직의 MITRE-ATT&CK 채점 시스템을 정의합니다.

점수 매기기 정의

포인트	점수 매핑	설명
안 함	0	데이터가 부족하여 특정 악의적 기술을 탐지할 수 없습니다.
불량	1	특정 악의적 기술을 탐지하기 위한 기본 서명 및 상관 관계 규칙이 마련되어 있습니다. 위협 탐지는 실시간이 아니며 기술의 최소 측면만 다룹니다. 예를 들어 헌팅은 한 번에 하나의 끝점에서만 발생합니다. 귀하의 조직에는 사냥꾼이 이상값을 찾기 위해 검토하고 다른 이벤트와 연관시켜야 하는 수천 또는 수백 개의 이벤트가 있을 수 있습니다. 가양성 수가 많습니다.
보통	2	올바른 데이터를 상당 부분 수집하고 데이터 품질은 공정합니다. 예를 들어 조직에서 Sysmon 로그, ETW, PowerShell 로그 등을 추가하기 시작할 수 있습니다. 그러나 위협 탐지는 여전히 실시간으로 이루어지지 않습니다. 조직에는 데이터를 효과적으로 집계하고 분석하는 데 적합한 도구가 없을 수 있습니다. 헌터는 데이터를 정확하게 분석하기 위해 수동으로 쿼리를 실행하고 상관 관계를 지정해야 합니다. 가양성 수가 많습니다.
좋음	3	엔드포인트 전체에서 여러 데이터의 상관 관계를 지정하고 통합하는 실시간 탐지입니다. 위협 탐지는 기술 절차의 여러 측면을 다룹니다. 공격자는 회피 및 난독 처리로 탐지를 우회할 수 있습니다. 조직에서 가양성을 쉽게 식별하고 필터링할 수 있습니다. 조직은 기본 데이터 과학 기술을 사용하여 중앙 리포지토리의 데이터를 분석합니다.
매우 좋음	4	실시간으로 악성 기술을 효과적으로 탐지하고 기술 절차의 대부분의 측면을 다룹니다. 상대방이 회피 및 난독화 방법으로 탐지를 우회할 가능성은 양호 수준보다 어렵습니다. 조직에서 가양성을 쉽게 식별하고 필터링할 수 있습니다. 조직은 고급 데이터 과학 기술을 사용하여 악의적 기술을 탐지합니다.
우수	5	실시간으로 악성 기술을 효과적으로 탐지하고 기술 절차의 모든 측면을 다룹니다. 조직은 적절한 자동화 및 데이터 품질로 환경을 잘 이해하고 있습니다. 악의적 사용자가 회피 및 난독화 방법으로 탐지를 우회할 가능성은 이 수준에서 불가능합니다. 거짓 부정의 수가 적습니다.

기술 탐지 범위를 기술에 매핑

조직에서 특정 악의적 기술을 탐지할 수 있는 기술을 사용하여 전체 기술 탐지 범위를 매핑합니다.

시작하기 전에

- 필요한 역할: sn_ti.admin, sn_si.admin: 쓰기 액세스
- 필요한 역할: sn_ti.read: read access

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보

기술 탐지 범위를 사용하여 조직의 전반적인 기술 탐지 범위에 대한 개요를 확인할 수 있습니다. 예를 들어 악의적 사용자가 조직을 공격하는 경우 공격자의 기술을 탐지해야 하는 범위를 볼 수 있습니다.

활성화한 모든 컬렉션 및 기술에 대해 기술 및 ID가 자동으로 채워집니다. 정의한 검사 유형 및 점수 매기기 정의 는 전체 기술 탐지 범위에서 선택할 수 있는 옵션으로 사용할 수 있습니다.

전체 기술 탐지 범위를 기술과 매핑하여 매핑을 완료할 수 있습니다. 기술은 하나의 전체 기술 탐지 범위에만 연결할 수 있습니다.

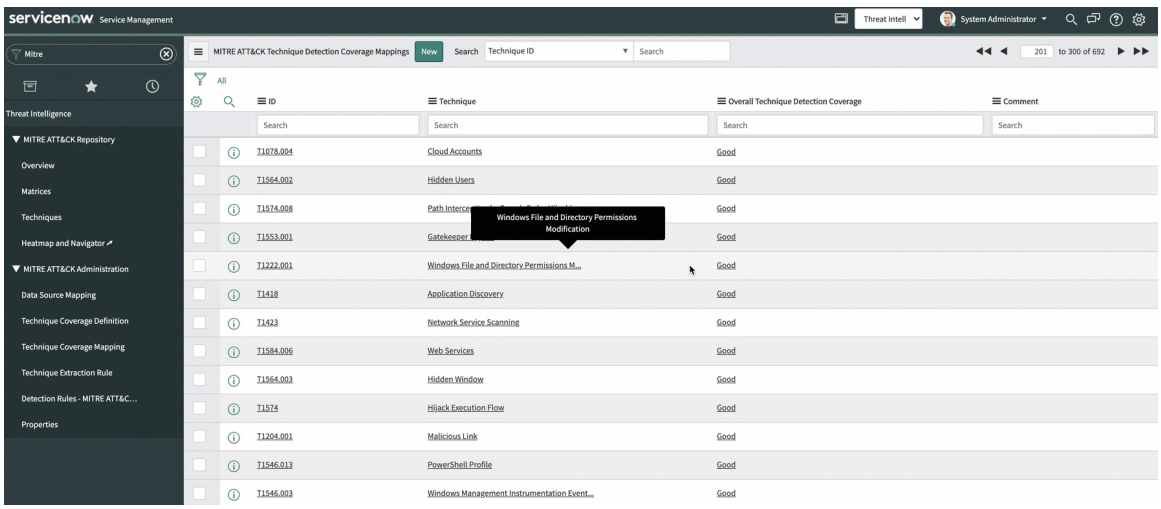
정의하는 기술 탐지 범위 매핑은 히트맵의 범위 시각화에 사용됩니다.

주:
조직별 계산을 사용하여 전체 기술 탐지 범위에 도달할 수 있습니다. 점수 매기기 정의를 정의하는 데 필요한 경우 위반 및 공격 시뮬레이션(BAS) 제품, 사이버 분석 리포지토리(CAR) 또는 기타 방법을 사용할 수 있으며 이 절차에서 전체 기술 탐지 범위 매핑에 사용할 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **MITRE ATT&CK** 관리 〉 탐지 범위 매핑.

   이 그림에서는 Cloud Accounts (T1078.004) 하위 기술이 조직에서 우수한 커버리지를 가지고 있으며 Overall Technique Detection Coverage가 **Excellent**에 매핑되어 있음을 알 수 있습니다.



2. 각 기술을 검토하고 탐지 범위 정의 와 조직의 검사 가용성에 따라 전체 기술 탐지 범위를 매핑합니다.

완화 범위 정의

조직에서 특정 기술로 인해 발생하는 공격을 얼마나 잘 방지할 수 있는지에 대한 가시성을 확보할 수 있도록 기술과 연결된 각 완화에 대한 완화 범위를 정의합니다.

시작하기 전에

- 필요한 역할: sn_ti.admin, sn_si.admin: 생성, 쓰기, 삭제 권한
- 필요한 역할: sn_ti.read: read access

이 태스크 정보

완화 범위 정의는 전체 완화 및 기술 범위 매핑에 사용됩니다. 기본 시스템 완화 적용 범위를 사용할 수 있습니다. 기본 시스템 완화 범위는 보장 유형 없음, 나쁨, 보통, 좋음, 매우 좋음 및 우수로 구성됩니다. 기본 시스템 완화 범위는 미리 정의된 색상 및 범위 백분율과도 연결됩니다. 보장 유형

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

(보장 유형 추가 또는 제거), 하한 및 상한 한도에 대한 보장 백분율 및 색상을 사용자 지정하거나 사용자 지정 완화 보장을 생성할 수 있습니다.

범위 유형, 색상 또는 백분율에 대한 사용자 지정은 완화 범위 매핑과 히트맵에도 사용됩니다.

프로시저

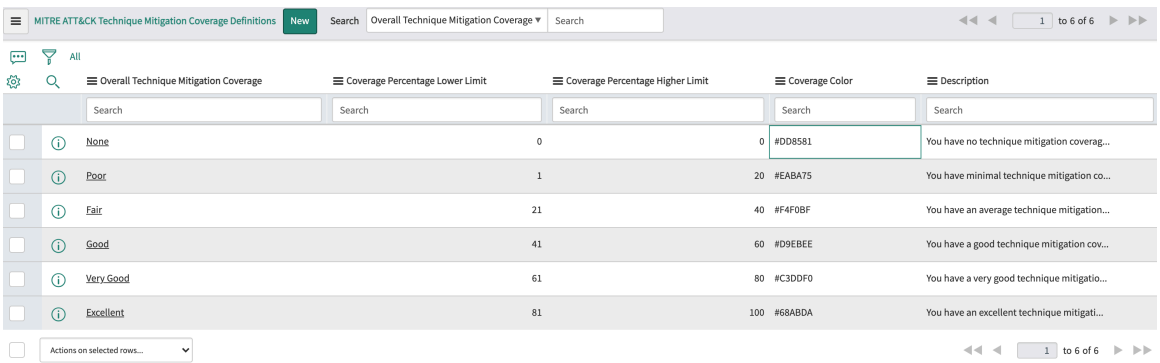
1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **MITRE ATT&CK** 관리 〉 완화 범위 정의.
2. 완화 탐지 항목을 검토하고 환경에 맞게 항목을 사용자 지정합니다.

기술 완화 범위 정의

필드	설명
전체 기술 완화 범위	기술 완화 범위의 이름입니다. 기본 시스템 완화 범위는 없음, 나쁨, 보통, 좋음, 매우 좋음 또는 훌륭함으로 구성됩니다.
범위 백분율 하한	완화 범위의 하한값입니다. 0에서 100 사이의 숫자 값을 정의합니다.
범위 백분율 상한	완화 범위의 더 높은 백분율 제한입니다. 0에서 100 사이의 숫자 값을 정의합니다.
범위 색상	탐지 범위 점수에 할당되는 색상입니다. 정의하는 색상은 히트맵의 기술 완화 범위에 사용됩니다. 16진수 코드와 RGB(A) 값을 사용하여 색을 사용자 지정할 수 있습니다.
설명	전반적인 완화 탐지 범위입니다. 기술 완화 범위 정의에서 기본 시스템 정의를 참조하십시오.

주:
백분율 한도(하한 또는 더 높음)를 사용자 지정하는 경우 범위 백분율 범위가 겹치지 않도록 합니다. 예를 들어 범위 기록의 범위가 0에서 20까지인 경우 범위 백분율 범위가 겹치지 않도록 다음 연속 기록의 하한 범위가 21 이상이어야 합니다.

다음 그림에서는 완화 범위 정의 목록을 보여 줍니다.



3. 항목을 추가하려면 새로 만들기를 클릭하고 항목을 완성한 다음 제출을 클릭합니다.

기술 완화 범위 정의

특정 공격자 기술을 효과적으로 측정하고 탐지할 수 있도록 조직의 완화 범위를 정의합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

MITRE ATT&CK 기술 완화 범위 정의

전체 기술 완화 범위	범위 백분율 하한	범위 백분율 상한	범위 색상	설명
안 함	0	0	#DD8581	기술 완화 범위가 없으며 방어 통제는 어떤 시나리오에서도 공격을 방지할 수 없습니다.
불량	1	20	#EABA75	최소한의 기술 완화 범위가 있습니다. 공격 가능성은 매우 높으며 방어 제어는 시나리오의 0-20%에서 공격을 방지할 수 있습니다.
보통	21	40	#F4F0BF	평균적인 기술 완화 범위가 있습니다. 공격 가능성이 높으며 방어 제어는 시나리오의 21-40%에서 공격을 방지할 수 있습니다.
좋음	41	60	#D9EBEE	당신은 좋은 기술 완화 범위를 가지고 있습니다. 그러나 공격 가능성은 상대적으로 높으며 방어 제어는 시나리오의 41-60%에서 공격을 방지할 수 있습니다.
매우 좋음	61	80	#C3DDF0	당신은 아주 좋은 기술 완화 범위를 가지고 있습니다. 공격 가능성은 낮으며 방어 제어는 시나리오의 61-80%에서 공격을 방지할 수 있습니다.
우수	81	100	#68ABDA	뛰어난 기술 완화 범위를 가지고 있으며

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

MITRE ATT&CK 기술 완화 범위 정의

전체 기술 완화 범위	범위 백분율 하한	범위 백분율 상한	범위 색상	설명
				이 기술을 사용한 공격 가능성은 매우 낮으며 방어 제어는 시나리오의 81%에서 100%에서 공격을 방지할 수 있습니다.

완화 범위를 기술에 매핑

조직의 전반적인 완화 전략을 검색할 수 있는 기술을 사용하여 완화 범위를 매핑합니다.

시작하기 전에

- 필요한 역할: sn_ti.admin, sn_si.admin: 쓰기, 삭제 접근 권한
- 필요한 역할: sn_ti.read: read access

이 태스크 정보

완화를 사용하면 악의적 사용자가 조직에 대해 기술 또는 하위 기술을 성공적으로 실행하지 못하도록 방지할 수 있습니다. 각 MITRE-ATT&CK 기술에는 공격 가능성을 줄이기 위해 조직에 배포할 수 있는 완화 기능이 포함되어 있습니다. 완화 범위를 사용하여 조직의 전반적인 완화 전략에 대한 개요를 확인할 수 있습니다. 예를 들어 악의적 사용자가 조직을 공격하는 경우 공격자의 기술을 완화해야 하는 범위가 표시됩니다.

활성화한 모든 컬렉션 및 기술에 대해 기술 및 완화 정보가 자동으로 채워집니다. 정의한 완화 범위 정의를 사용하여 기술 완화 범위에서 선택할 수 있습니다.

조직과 관련된 완화 조치를 식별할 수 있습니다. 완화 조치가 적절한 경우 완화 전략이 배포되었는지 정의할 수 있습니다. 전략이 조직의 SOC 정책의 일부로 적용되는지 여부를 지정할 수 있습니다. 또한 조직에 공격자의 기술을 완화하기 위한 예방 도구가 있는지 확인하고 조직에서 보안 위험을 최소화하기 위해 배포한 보안 제어를 매핑할 수 있습니다. 각 기록에 대한 완화 범위(백분율)를 채웁니다.

각 기술에 대한 정보를 매핑한 후 완화 범위 계산기 는 계산된 기술 완화 범위를 자동으로 채웁니다. 모든 기술에 대한 전체 완화 범위를 계산하려면 기술 완화 매핑 기록이 활성 상태이고 조직과 관련이 있어야 합니다. 비활성 상태이고 관련이 없는 기록은 전체 기술 완화 범위를 계산하는 데 고려되지 않습니다. 계산된 기술 완화 범위 및 완화 범위 정의의 값에 따라 전체 기술 완화 범위(계산됨)가 채워집니다.

범위 유형, 색상 또는 백분율에 대한 사용자 지정은 완화 범위 매핑과 히트맵에도 사용됩니다.

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **MITRE ATT&CK** 관리 〉 완화 범위 매핑.
2. 완화 매핑에 대한 각 기술을 검토하고 완화 범위(백분율) 를 업데이트하여 조직의 범위 가용성을 계산합니다.

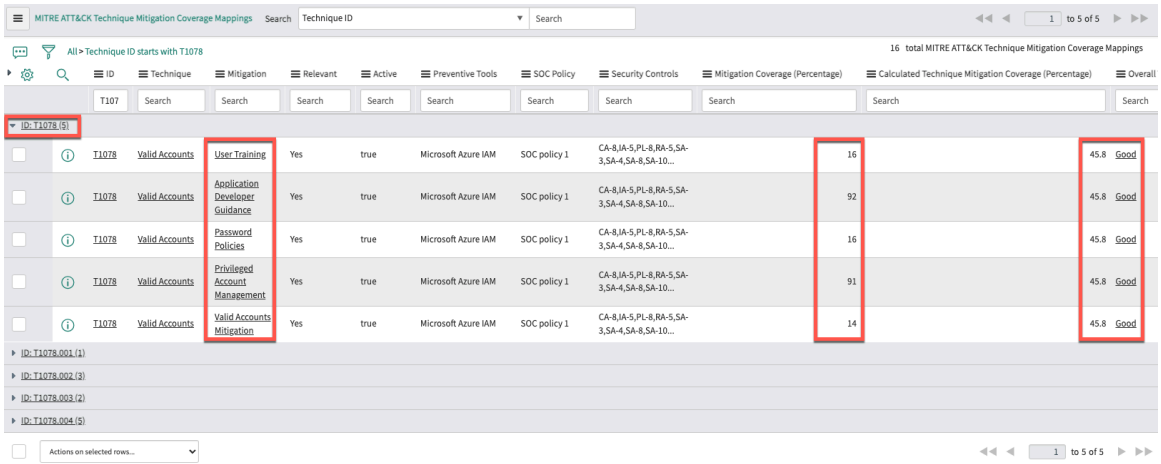
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

기술 완화 범위 매핑

필드	설명
ID	기술의 고유한 정체성. 활성화한 모든 컬렉션 및 기술에 대해 ID가 자동으로 채워집니다.
기술	공격자가 작업을 수행하여 전술적 목표를 달성하는 방법입니다. 활성화한 모든 컬렉션 및 기술에 대해 기술 정보가 자동으로 채워집니다.
완화	악의적 사용자가 조직에 대해 기술 또는 하위 기술을 성공적으로 실행하지 못하도록 방지할 수 있는 완화입니다. 활성화한 모든 컬렉션 및 기술에 대한 완화 정보가 자동으로 채워집니다.
관련됨	완화가 조직과 관련이 있는지 여부를 지정하는 옵션입니다.
활성	완화 전략이 조직에 배포되는지 여부를 지정하는 옵션입니다. 이는 기술 완화 범위를 계산하는 데 필요한 필수 옵션입니다.
예방 도구	조직에 공격자의 기술을 완화하기 위한 예방 도구가 있는지 지정하는 옵션입니다.
SOC 정책	조직의 완화 전략을 정의하는 SOC 정책입니다.
보안 통제	조직의 보안 통제에는 보안 위험을 최소화하기 위한 완화 전략이 포함되어 있습니다.
완화 범위(백분율)	기술 완화 범위를 계산하는 점수 시스템. 0에서 100 사이의 숫자 값을 정의합니다. 이는 기술 완화 범위를 계산하는 데 필요한 필수 옵션입니다.
계산된 기술 완화 범위(백분율)	계산된 기술 완화 범위(백분율)입니다. 이 값은 완화 범위 계산기에 정의된 수식에 따라 결정됩니다.
전체 기술 완화 범위(계산됨)	전반적인 기술 완화 범위입니다. 이 값은 조직에 대해 정의된 완화 범위에 따라 결정됩니다.
설명	기술 및 완화 범위 매핑에 대한 설명입니다.
해지함	완화 범위 매핑에 대한 기술이 취소됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 그림에서는 유효한 계정 기술에 5개의 완화가 연결되어 있으며, 각 완화 범위는 사용자 교육에 대해 16개, 애플리케이션 개발자 지침에 대해 92개, 암호 정책에 대해 16개, 권한 있는 계정 관리에 대해 91개, 유효한 계정 완화에 대해 14개입니다. 계산된 기술 완화 범위는 45.8%입니다.



전체 기술 완화 범위 계산기

전체 기술 완화 범위는 완화 범위 계산기에 정의된 수식에 따라 결정됩니다.

시작하기 전에

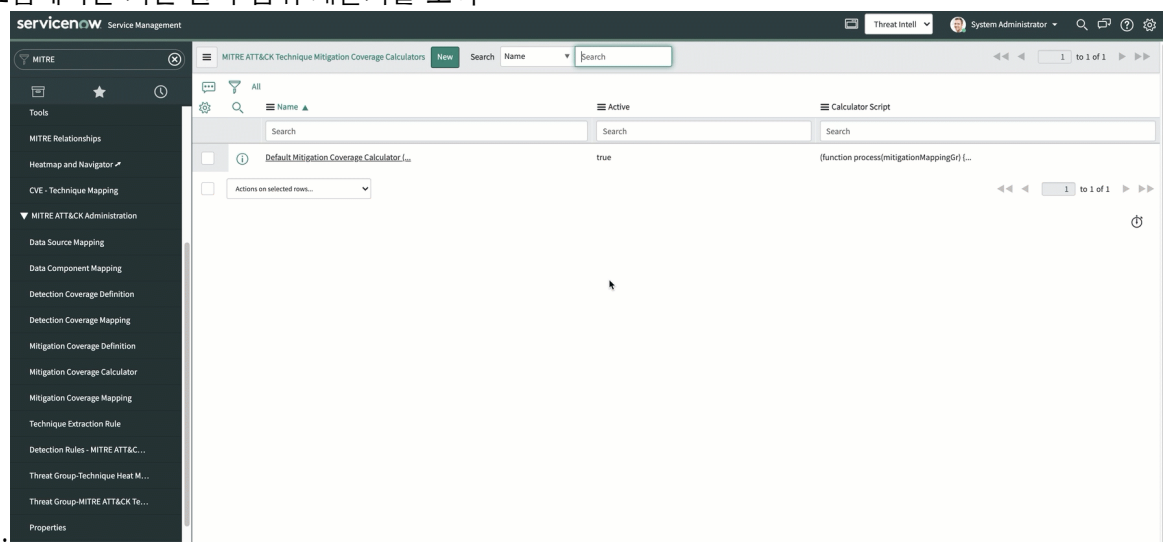
- 필요한 역할: sn_ti.admin, sn_si.admin: 생성, 쓰기, 삭제 권한
- 필요한 역할: sn_ti.read: read access

이 태스크 정보

- 도메인당 하나의 완화 범위 계산기만 활성으로 설정할 수 있습니다.
- 기본 시스템 완화 범위 계산기는 평균 계산기입니다.
- 계산기 스크립트를 사용자 지정할 때 최종 출력은 0에서 100 사이의 숫자 값이어야 합니다.
- 완화 범위 정의는 최종 출력의 범위에 따라 적용됩니다.

프로시저

다음으로 이동 모두 〉 위협 인텔리전스 〉 **MITRE ATT&CK** 관리 〉 완화 범위 계산기.
다음 그림에서는 기본 완화 범위 계산기를 보여줍니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

탐지 규칙 생성 및 매핑

탐지 규칙을 생성하고 전술 및 기술에 대해 매핑합니다. 이 매핑을 사용하면 조직의 탐지 규칙에 대한 범위를 볼 수 있습니다.

시작하기 전에

필요한 역할:

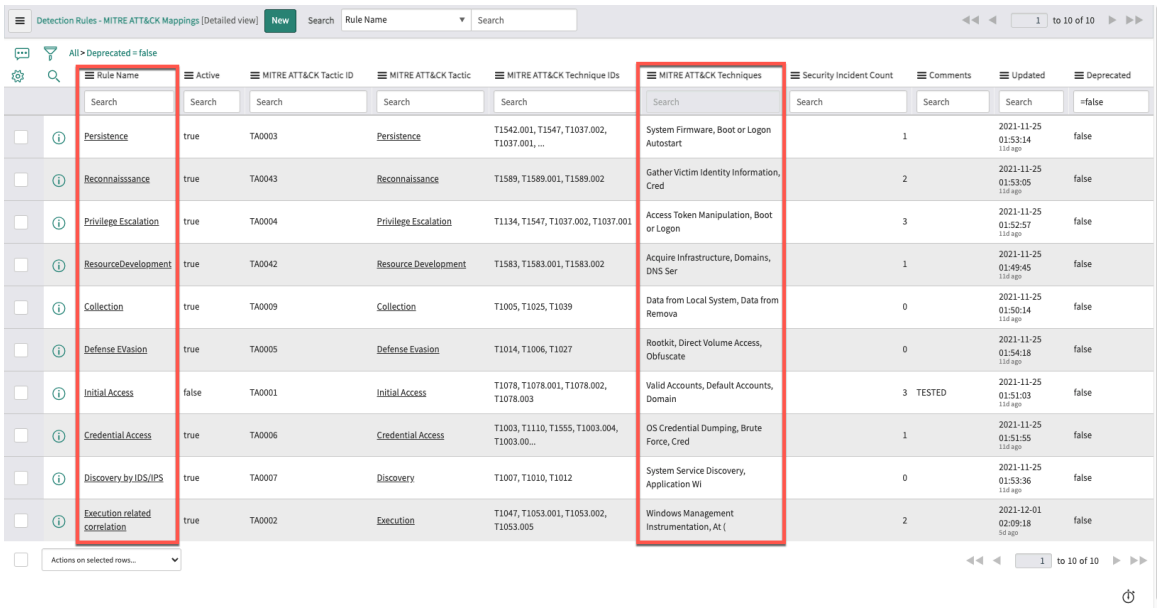
- sn_ti.admin, sn_si.admin: 생성, 쓰기, 삭제 권한
- sn_ti.read: 읽기 액세스

이 태스크 정보

탐지 규칙 매핑을 사용하면 조직에서 특정 기술을 식별하는 데 사용할 수 있는 탐지 규칙을 확인할 수 있습니다.

매핑의 주요 목적은 조직에 특정 기술을 사용하는 악의적 사용자의 공격으로 인해 경보 또는 이벤트가 트리거되는 시기를 식별하는 데 필요한 탐지 규칙이 있는지 가시성을 제공하는 것입니다.

예를 들어 다양한 기술에 매핑된 검색 규칙 목록을 보여 주는 다음 그림을 볼 수 있습니다. 다음에서 이 정보를 볼 수도 있습니다. the MITRE-ATT&CK 탐색기.



기본 시스템 SIEM 자동 추출 규칙을 사용하지 않으려면 탐지 규칙 매핑을 기반으로 TTP의 MITRE-ATT&CK 자동 롤업을 활성화합니다. 경보 규칙 이름 필드에 보안 인시던트를 트리거하는 경보 또는 이벤트 규칙을 채울 수 있습니다. SIEM 통합, 이메일 구문 분석, 수동 생성 등을 사용하여 경보 규칙 이름 필드를 채울 수도 있습니다. 자세한 내용은 탐지 규칙의 롤업 MITRE-ATT&CK 정보 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

탐지 규칙 기능이 업데이트되어 단일 전술을 여러 기술에 매핑하는 것을 포함합니다. 이전에는 단일 전술을 단일 기술로 매핑할 수 있었습니다. 플러그인을 버전 12.0.4에서 상위 버전으로 업그레이드하는 위협 인텔리전스 경우 모듈의 탐지 규칙을 MITRE-ATT&CK 사용하기 전에 다음 사항을 검토하십시오.

- 규칙 이름, 경보 센서, 소스, 범주, 하위 범주 및 MITRE-ATT&CK 방법 필드가 공통적인 경우 여러 기록이 단일 기록으로 병합됩니다.
- 이전 기록은 사용되지 않는 열에서 true로 표시되고 활성 열에서 false로 표시됩니다.
- 새로 병합된 기록을 사용할 수 있으며 사용되지 않음 열에서 false로, 활성 열에서 true로 표시됩니다.
- 업그레이드를 확인하고 모든 탐지 규칙이 성공적으로 마이그레이션되었는지 확인한 후에는 사용되지 않음 열에서 true로 표시된 이전 기록을 삭제할 수 있습니다.

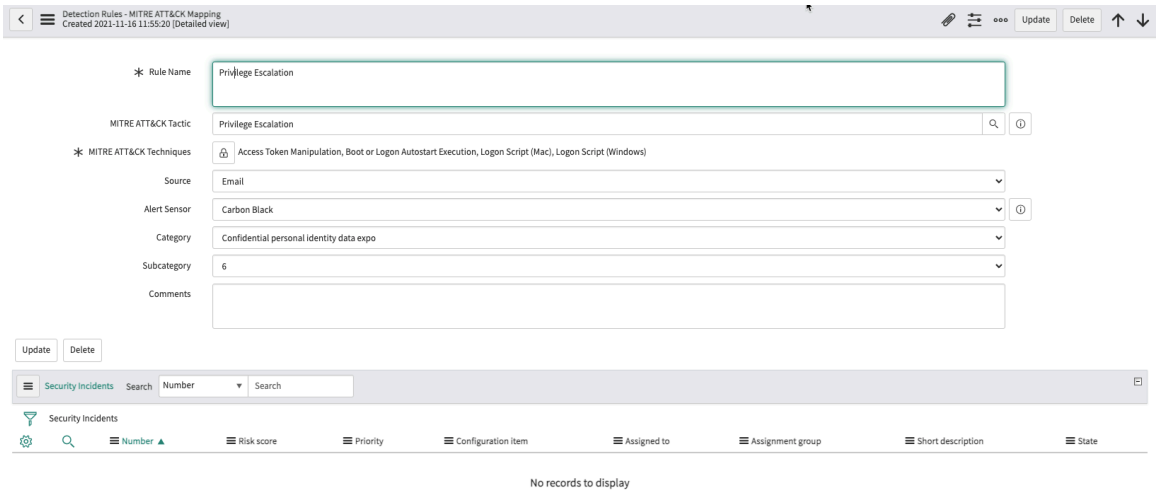
프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **MITRE ATT&CK** 관리 〉 탐지 규칙 **- MITRE ATT&CK** 매핑.
2. 다음 방법 중 하나를 사용하여 탐지 규칙을 생성합니다.
   방법 1: 검색 규칙을 수동으로 만듭니다.
   a. 새로 만들기를 클릭하고 양식의 필드에 내용을 입력합니다.

탐지 규칙 **- MITRE-ATT&CK** 매핑

필드	설명
규칙 이름	탐지 규칙의 이름입니다.
MITRE-ATT&CK 전술	관련 MITRE-ATT&CK 전술.
MITRE-ATT&CK 기술을	관련 MITRE-ATT&CK 기술. 단일 전술에 대해 여러 기술을 선택할 수 있습니다.
소스	이메일, 방화벽, 네트워크 모니터링 등과 같은 보안 인시던트의 소스입니다.
경보 센서	경보 또는 이벤트 데이터(예: CarbonBlack, CrowdStrike, McAfee)를 수집하는 보안 통합입니다.
하위 범주	문제를 추가로 정의하는 하위 범주입니다.
범주	보안 문제의 유형을 식별하는 범주입니다.
MITRE-ATT&CK 기술	관련 MITRE-ATT&CK 기술. 단일 전술에 대해 여러 기술을 선택할 수 있습니다.
보안 인시던트 수	기술이 추가된 보안 인시던트 수입니다. 경보 규칙에서 보안 인시던트까지 자동으로 정보를 롤업 MITRE-ATT&CK 하도록 설정한 경우 이 수가 나타납니다.
사용하지 않음	탐지 규칙 매핑은 더 이상 사용되지 않습니다.
활성	탐지 규칙이 활성 상태이고 사용자 환경에 배포되어 있는지 여부를 지정하는 옵션입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



b. 제출을 클릭합니다.
방법 2: 검색 규칙을 가져오고 만듭니다.

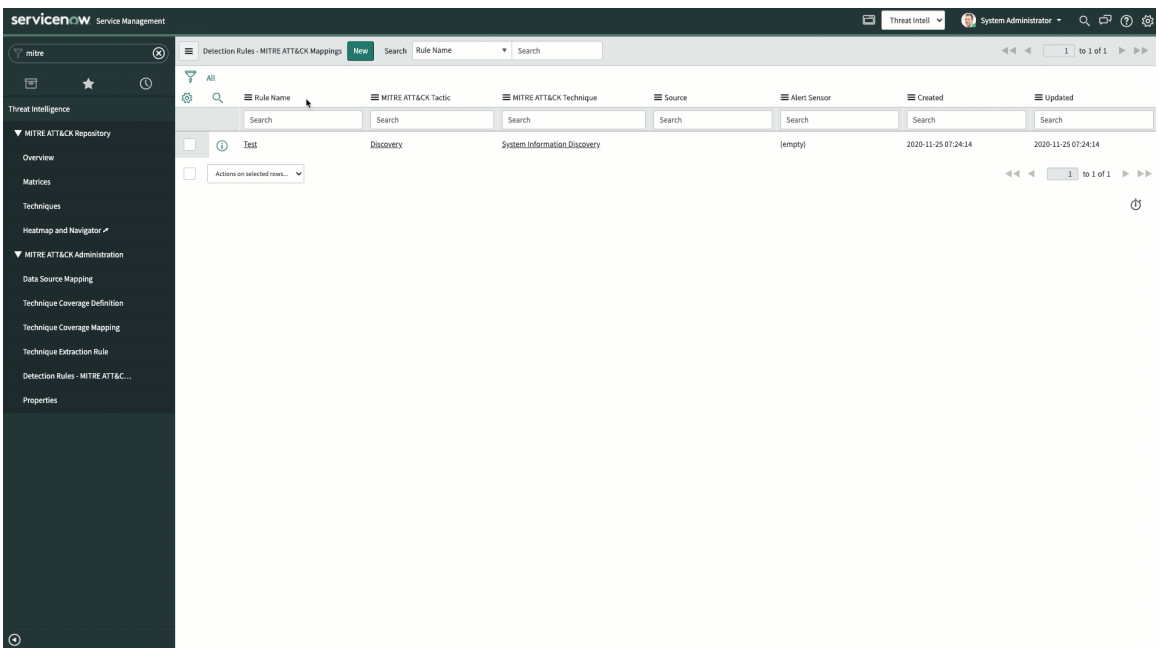
a. 규칙 이름 열 헤더를 마우스 오른쪽 버튼으로 클릭합니다.

b. 목록에서 임포트를 클릭합니다.

c. **Excel** 템플릿 만들기를 클릭합니다.

d. 익스포트가 완료된 후 다운로드를 클릭합니다. 파일 이름이 sn_ti_alert_rules_mitre_attack_technique_mapping Excel 템플릿이 컴퓨터에 다운로드됩니다.

다음 그림에서는 Excel 템플릿을 익스포트하고, 스프레드시트에 세부 정보를 입력하고, 파일을 업로드하고, 필드를 미리 보고, 다시 ServiceNow AI Platform.



e. 스프레드시트를 열고 두 번째 시트 탭을 선택한 다음 입력한 내용을 검토합니다. 양식의 필드에 내용을 입력한 다음 파일을 저장합니다.

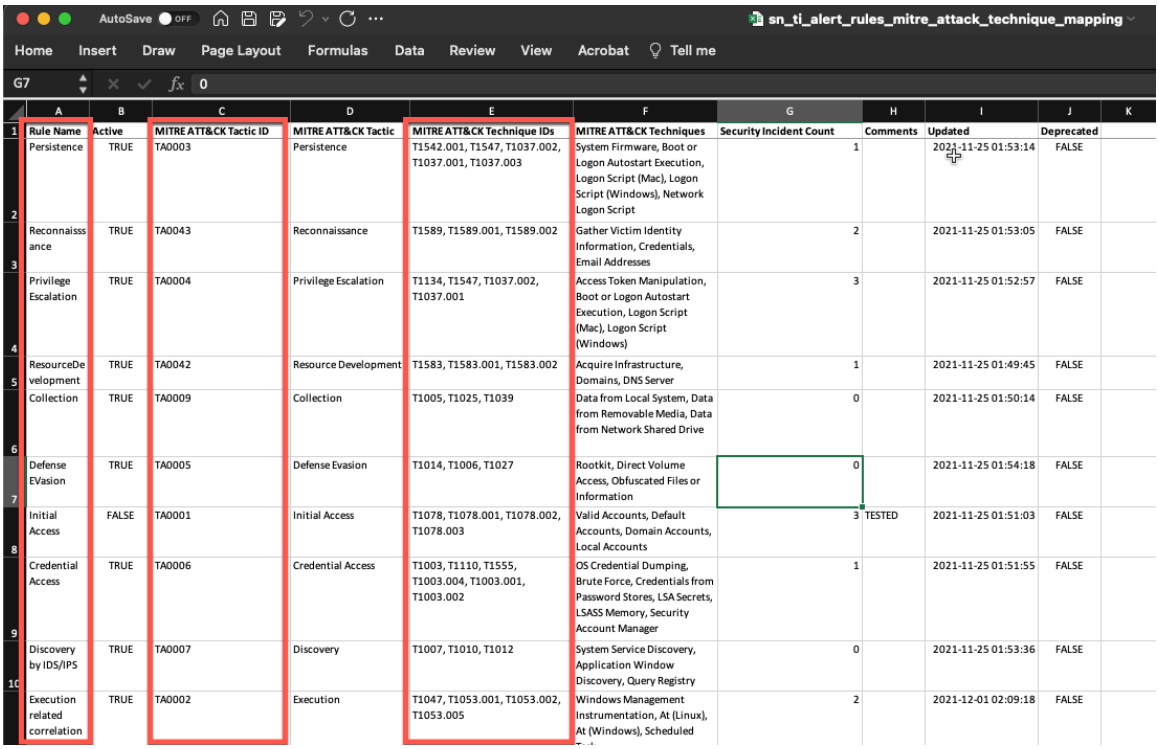
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

템플릿 임포트

필드	설명
규칙 이름	탐지 규칙 이름입니다.
활성	탐지 규칙이 활성 상태이고 사용자 환경에 배포되어 있는지 여부를 지정하는 옵션입니다.
경보 센서	경보 또는 이벤트 데이터(예: CarbonBlack, CrowdStrike, McAfee)를 수집하는 보안 통합입니다.
범주	보안 문제의 유형을 식별하는 범주입니다.
설명	탐지 규칙에 대한 설명입니다.
사용하지 않음	탐지 규칙 매핑은 더 이상 사용되지 않습니다.
MITRE-ATT&CK 기술 ID	MITRE-ATT&CK 접근성 기능에 대한 기술 ID입니다(예: T1546.008).
MITRE-ATT&CK 방법 ID	MITRE-ATT&CK 지속성을 위한 TA0003과 같은 방법 ID입니다.
보안 인시던트 수	기술이 추가된 보안 인시던트 수입니다. 경보 규칙에서 보안 인시던트까지 자동으로 정보가 롤업 MITRE-ATT&CK 되도록 설정하고 탐지 규칙이 활성 상태인 경우 이 개수가 나타납니다.
소스	이메일, 방화벽, 네트워크 모니터링 등과 같은 보안 인시던트의 소스입니다.
하위 범주	문제를 추가로 정의하는 하위 범주입니다.
MITRE-ATT&CK 전술	관련 MITRE-ATT&CK 전술.
MITRE-ATT&CK 기술	관련 MITRE-ATT&CK 기술.

다음 그림에서는 스프레드시트 템플릿을 보여 줍니다. 필수 필드(규칙 이름, MITRE-ATT&CK 방법 ID 및 MITRE-ATT&CK 기술 ID)가 빨간색으로 강조 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



Rule Name	Active	MITRE ATT&CK Tactic ID	MITRE ATT&CK Tactic	MITRE ATT&CK Technique IDs	MITRE ATT&CK Techniques	Security Incident Count	Comments	Updated	Deprecated
Persistence	TRUE	TA0003	Persistence	T1542.001, T1547, T1037.002, T1037.001, T1037.003	System Firmware, Boot or Logon Autostart Execution, Logon Script (Mac), Logon Script (Windows), Network Logon Script	1		2021-11-25 01:53:14	FALSE
Reconnaissance	TRUE	TA0043	Reconnaissance	T1589, T1589.001, T1589.002	Gather Victim Identity Information, Credentials, Email Addresses	2		2021-11-25 01:53:05	FALSE
Privilege Escalation	TRUE	TA0004	Privilege Escalation	T1134, T1547, T1037.002, T1037.001	Access Token Manipulation, Boot or Logon Autostart Execution, Logon Script (Mac), Logon Script (Windows)	3		2021-11-25 01:52:57	FALSE
ResourceDevelopment	TRUE	TA0042	Resource Development	T1583, T1583.001, T1583.002	Acquire Infrastructure, Domains, DNS Server	1		2021-11-25 01:49:45	FALSE
Collection	TRUE	TA0009	Collection	T1005, T1025, T1039	Data from Local System, Data from Removable Media, Data from Network Shared Drive	0		2021-11-25 01:50:14	FALSE
Defense EVasion	TRUE	TA0005	Defense Evasion	T1014, T1006, T1027	Rootkit, Direct Volume Access, Obfuscated Files or Information	0		2021-11-25 01:54:18	FALSE
Initial Access	FALSE	TA0001	Initial Access	T1078, T1078.001, T1078.002, T1078.003	Valid Accounts, Default Accounts, Domain Accounts, Local Accounts	3	TESTED	2021-11-25 01:51:03	FALSE
Credential Access	TRUE	TA0006	Credential Access	T1003, T1110, T1555, T1003.004, T1003.001, T1003.002	OS Credential Dumping, Brute Force, Credentials from Password Stores, LSA Secrets, LSASS Memory, Security Account Manager	1		2021-11-25 01:51:55	FALSE
Discovery by IDS/IPS	TRUE	TA0007	Discovery	T1007, T1010, T1012	System Service Discovery, Application Window Discovery, Query Registry	0		2021-11-25 01:53:36	FALSE
Execution related correlation	TRUE	TA0002	Execution	T1047, T1053.001, T1053.002, T1053.005	Windows Management Instrumentation, At (Linux), At (Windows), Scheduled	2		2021-12-01 02:09:18	FALSE

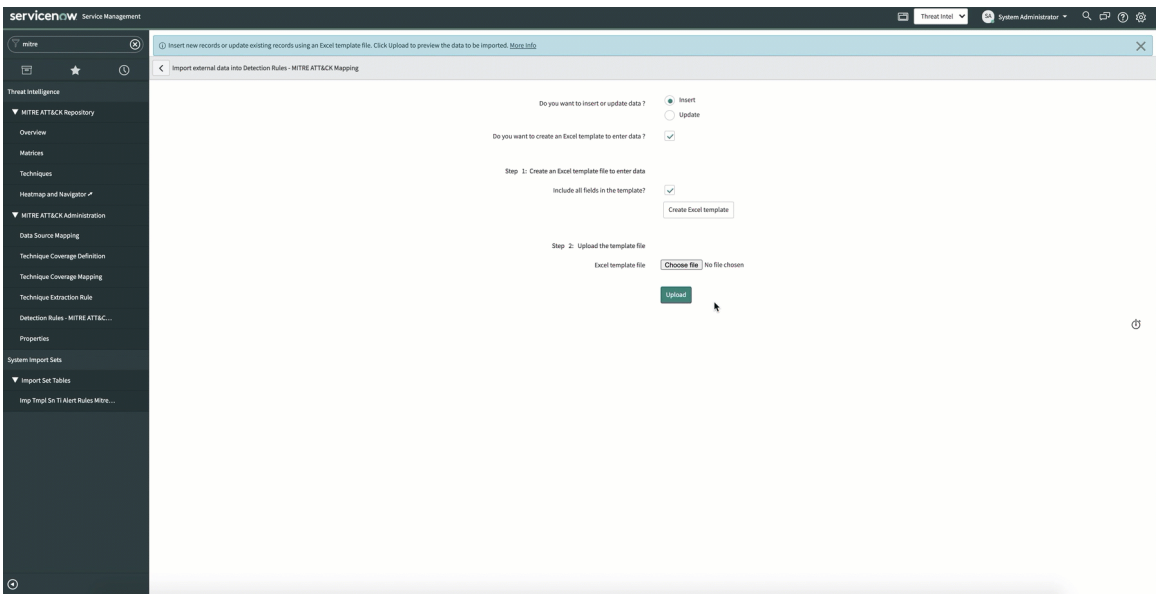
f. 파일 선택을 클릭하고 컴퓨터에서 스프레드시트를 선택합니다.

g. 업로드를 클릭합니다.

h. 임포트한 데이터 미리 보기를 클릭합니다.

i. 매핑을 미리 보고 임포트 완료를 클릭합니다.

다음 그림에서는 스프레드시트를 업로드하고, 데이터를 미리 보고, 오류를 검토하고, 탐지 규칙 매핑 임포트 프로세스를 완료하는 방법을 보여줍니다.



정보 임포트 **MITRE-ATT&CK** 를 위한 자동 추출 기술 규칙

기본 시스템 자동 추출 규칙을 사용하여 기존 외부 공급업체 통합에서 정보를 임포트 MITRE-ATT&CK 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

위협 조회 자동 추출 규칙 사용

위협 조회 자동 추출 규칙을 사용하여 기존 위협 인텔리전스 외부 공급업체 통합에서 정보를 임포트 MITRE-ATT&CK 합니다.

시작하기 전에

필요한 역할:

- sn_ti.admin, sn_si.admin: 생성, 쓰기, 삭제 권한
- sn_ti.read: 읽기 액세스

이 태스크 정보

위협 인텔리전스 샌드박스 또는 TIP와 같은 통합이 프레임워크를 MITRE-ATT&CK 지원하고 MITRE-ATT&CK 정보가 각 통합 수준에서 구문 분석되면 각 위협 조회 결과 기록에 정보가 표시됩니다. 그러나 모든 위협 인텔리전스 통합이 MITRE-ATT&CK 정보를 구문 분석하는 것은 아닙니다. 위협 조회 전역 자동 추출 규칙은 모든 위협 인텔리전스 통합에서 정보를 추출 MITRE-ATT&CK 할 수 있습니다.

위협 조회 결과에서 보안 인시던트로 정보를 자동으로 롤업 MITRE-ATT&CK 하도록 선택할 수 있습니다. 위협 조회 결과를 보안 인시던트로 자동 롤업하려면 시스템 속성을 활성화합니다. 또는 각 개별 위협 조회에 대한 정보를 수동으로 롤업할 수 있습니다.

통합이 기술 또는 방법과 같은 정보를 제공하는 MITRE-ATT&CK 경우 위협 인텔리전스 기본 시스템은 위협 인텔리전스 외부 공급업체 통합 원시 페이로드에서 위협 조회 결과 기록으로 정보를 자동으로 추출 MITRE-ATT&CK 합니다.

위협 조회 기록의 MITRE-ATT&CK 원시 페이로드 필드에서 정보를 사용할 수 없는 경우 외부 공급업체 통합에서 자동 추출하기 위한 고유한 규칙을 정의해야 합니다.

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **MITRE ATT&CK** 관리 〉 기술 추출 규칙.
2. 새로 만들기를 클릭합니다.
3. 양식에서 필드를 채웁니다.

기술 추출 규칙 양식

필드	설명
이름	자동 추출 규칙 이름입니다.
규칙 유형	자동 추출 규칙 유형입니다. 위협 조회를 선택합니다.
자동 추출 무시	기본적으로 설정이 취소되어 있습니다. 이 설정을 사용하면 기술을 자동으로 추출할 수 있습니다 MITRE-ATT&CK .
소스 엔진	소스 엔진.
전역	소스 엔진 설정입니다. 소스 엔진을 전역으로 설정하면 모든 위협 조회 통합 결과에서 추출이 실행됩니다.
설명	자동 추출 규칙에 대한 설명입니다.
프로세스 방법	원시 페이로드의 기술 정보를 연결하기 위해 지정하는 정규 표현식 또는 스크립트 메서드입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
정규 표현식 추출	정규 표현식 추출 방법을 사용할 때 대상 필드에 대해 지정하는 옵션입니다. 정규 표현식이 기본값입니다.
스크립트 추출	스크립트를 실행할 때 선택하는 프로세스입니다. 스크립트에서는 다음을 검토합니다. ○ threatLookupResultSysId: 위협 조회 결과 기록의 sys_id ○ sourceName: 위협 조회 소스의 이름입니다.
전술 추출	원시 페이로드에서 방법 관련 정보를 추출하기 위해 지정하는 옵션입니다. 페이로드에 특정 방법 및 기술 관련 정보가 포함되어 있는 경우 해당 정보를 추출하여 보안 인시던트에 추가할 수 있습니다.

4. 제출을 클릭합니다.

SIEM 자동 추출 규칙 사용

SIEM 자동 추출 규칙을 사용하여 기존 보안 운영 SIEM 외부 공급업체 통합에서 정보를 임포트 MITRE-ATT&CK 합니다.

시작하기 전에
필요한 역할:

- sn_ti.admin, sn_si.admin: 생성, 쓰기, 삭제 권한
- sn_ti.read: 읽기 액세스

이 태스크 정보
기술 추출 규칙은 Splunk, IBM QRadar 및 ArcSight 통합과 같은 모든 기본 시스템 보안 운영 SIEM 통합에 사용할 수 있습니다. ServiceNow AI Platform 이러한 SIEM 통합에서 수집 경보 또는 이벤트 데이터에 정보가 포함되어 MITRE-ATT&CK 있으면 원시 페이로드를 ServiceNow AI Platform 처리하고 정보를 자동 추출 MITRE-ATT&CK 합니다.

기본 ServiceNow AI Platform 시스템 SIEM 통합이 포함되어 있으면 기술 추출 규칙이 모듈에 이미 생성되어 있다는 의미입니다 MITRE-ATT&CK . 필요에 따라 규칙을 검토하고 수정해야 합니다.

SIEM 자동 추출 규칙 또는 경보 규칙을 한 번에 사용하도록 설정합니다.

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **MITRE ATT&CK** 관리 〉 기술 추출 규칙.
2. 새로 만들기를 클릭합니다.
3. 양식에서 필드를 채웁니다.

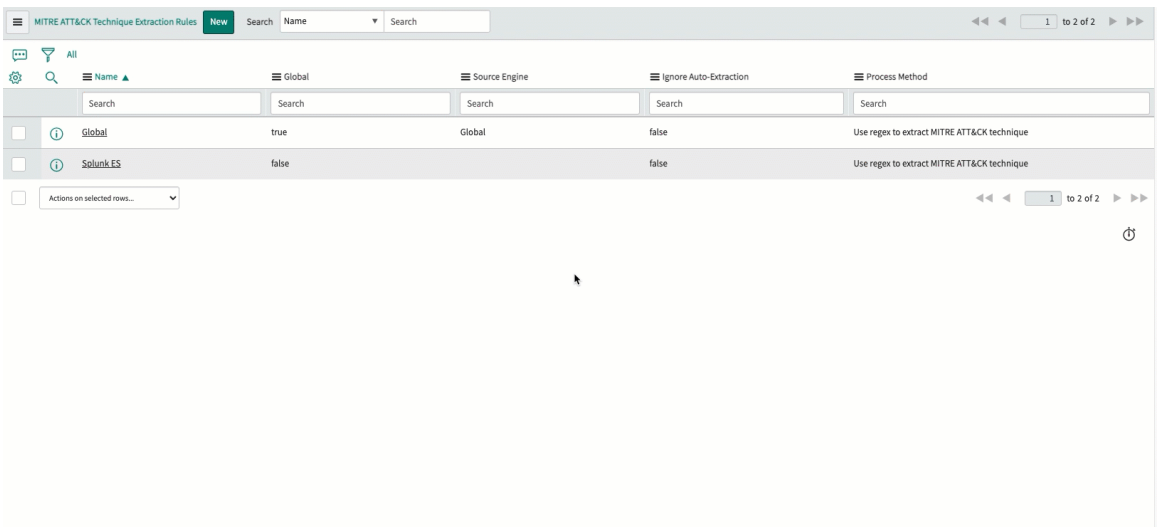
기술 추출 규칙 양식

필드	설명
이름	자동 추출 규칙 이름입니다.
규칙 유형	자동 추출 규칙 유형입니다. **SIEM**을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
자동 추출 무시	기본적으로 설정이 취소되어 있습니다. 이 설정을 사용하면 기술을 자동으로 추출할 수 있습니다 MITRE-ATT&CK .
임포트 테이블	기본 시스템 SIEM 통합을 위해 자동으로 매핑되는 임포트 테이블입니다. 이 필드에서 다른 SIEM 통합에 대한 정보를 검토하고 MITRE-ATT&CK 그에 따라 매핑합니다.
임포트 필드	기본 시스템 SIEM 통합을 위해 자동으로 매핑되는 임포트 필드입니다. 이 필드에서 다른 SIEM 통합에 대한 정보를 검토하고 MITRE-ATT&CK 그에 따라 매핑합니다.
설명	자동 추출 규칙입니다.
프로세스 방법	원시 페이로드의 기술 정보를 연결하기 위해 지정하는 정규 표현식 또는 스크립트 메서드입니다.
정규 표현식 추출	정규 표현식 메서드를 사용할 때 대상 필드에 대해 지정하는 옵션입니다. 정규 표현식 추출이 기본 프로세스 방법입니다.
스크립트 추출	정보 추출 방법을 MITRE-ATT&CK 사용자 지정하려는 경우 사용하는 스크립트 프로세스 방법입니다.
전술 추출	원시 페이로드에서 방법 관련 정보를 추출하기 위해 지정하는 옵션입니다. 페이로드에 특정 방법 및 기술 관련 정보가 포함되어 있는 경우 해당 정보를 추출하여 보안 인시던트에 추가할 수 있습니다.

다음 그림에는 양식 뷰에 있는 SIEM 기술 추출 규칙의 Splunk Enterprise 예를 볼 수 있습니다. 이 규칙은 다른 모든 SIEM 기술 추출 규칙과 유사합니다.



4. 제출을 클릭합니다.

위협 그룹 및 **MITRE-ATT&CK** 기술 매핑 검토

컬렉션에서 MITRE TAXII 가져온 위협 그룹 및 기술 개체를 개체 관계 매핑 정보로 검토합니다. 이 매핑을 사용하면 기술 그룹과 해당 기술 매핑을 볼 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

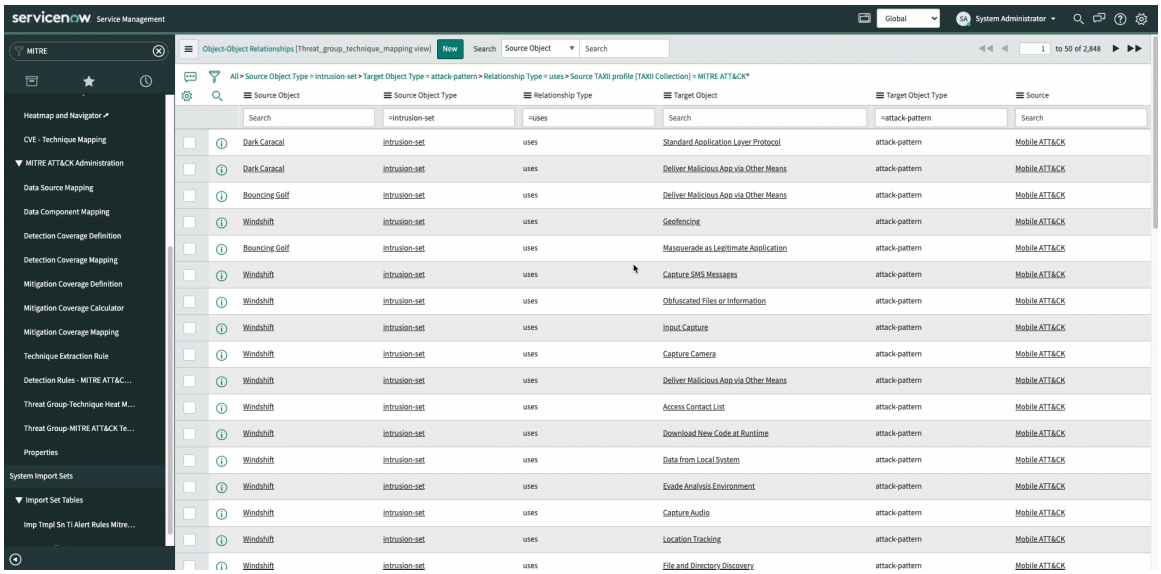
시작하기 전에
필요한 역할:

- sn_ti.admin, sn_si.admin: 생성, 쓰기, 삭제 권한
- sn_ti.read: 읽기 액세스

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **MITRE ATT&CK** 관리 〉 위협 그룹-**MITRE ATT&CK** 기술.
2. **Source** Object(소스 개체)를 마우스 오른쪽 버튼으로 클릭하고 **Group By Source** Object(원본 개체별 그룹화)를 선택하여 위협 그룹과 연결된 모든 공격 패턴을 확인합니다.

   다음 그림은 위협 그룹 admin@338와 엔터프라이즈 공격 소스의 일부인 이 위협 그룹이 채택한 다양한 공격 패턴을 보여 줍니다.



기술 히트맵 정의에 대한 위협 그룹

히트맵에서 위협 그룹이 조직을 공격하는 데 사용하는 공격 패턴을 측정하고 탐지할 수 있도록 위협 그룹 대 기술 히트맵 정의를 정의합니다. 공격자 수가 많을 때 특정 기술을 사용한 공격의 확률이 높아집니다.

시작하기 전에
필요한 역할:

- sn_ti.admin, sn_si.admin: 쓰기 권한
- sn_ti.read: 읽기 액세스

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **MITRE ATT&CK** 관리 〉 위협 그룹 기술 히트맵 정의.
2. 위협 그룹 기술 히트맵 정의를 검토하고 사용자 환경에 맞게 항목을 사용자 지정합니다.

위협 그룹 기술 히트맵 정의

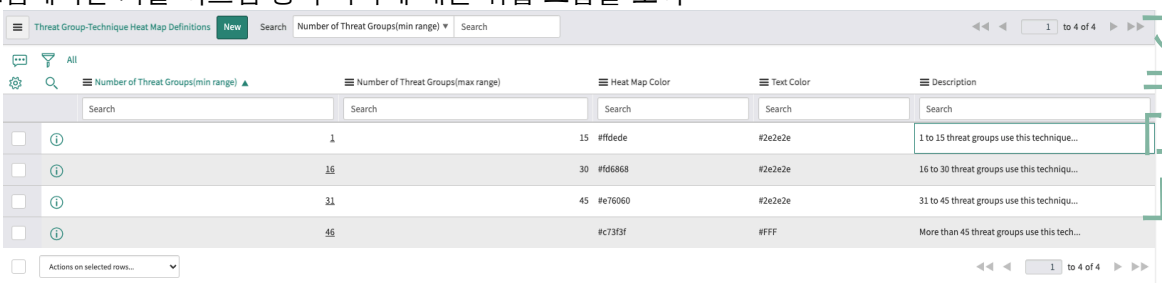
필드	설명
위협 그룹 수(최소 범위)	특정 기술을 사용하는 최소 위협 그룹 수입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
위협 그룹 수(최대 범위)	특정 기술을 사용하는 최대 위협 그룹 수입니다. 공격자 수가 많을 때 특정 기술을 사용한 공격의 확률이 높아집니다.
히트맵 색상	위협 그룹 범주에 할당된 색상입니다. 정의하는 색상은 히트맵에서 위협 그룹 범주를 강조 표시하는 데 사용됩니다. 16진수 코드와 RGB(A) 값을 사용하여 색을 사용자 지정할 수 있습니다.
텍스트 색상	위협 그룹 텍스트에 할당된 색상입니다. 정의하는 색상은 히트맵에서 위협 그룹을 강조 표시하는 데 사용됩니다. 16진수 코드와 RGB(A) 값을 사용하여 색을 사용자 지정할 수 있습니다.
설명	위협 그룹 범위 및 정의에 대한 설명입니다.

주:
위협 그룹 범위(최소 또는 최대)를 사용자 지정하는 경우 위협 그룹 수 범위가 겹치지 않도록 합니다.

다음 그림에서는 기술 히트맵 정의 목록에 대한 위협 그룹을 보여줍니다.



3. 항목을 추가하려면 새로 만들기를 클릭하고 항목을 완성한 다음 제출을 클릭합니다.

MITRE-ATT&CK 시스템 속성 검토

MITRE-ATT&CK 시스템 속성 값을 검토합니다.

시작하기 전에
필요한 역할: sn_ti.admin, sn_si.admin

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **MITRE ATT&CK** 관리 〉 속성.
2. 양식에서 필드를 채웁니다.

MITRE-ATT&CK 속성 양식

필드	설명
옵저버블에서 보안 인시던트로 MITRE ATT&CK 정보를 자동으로 롤업 〔sn_ti.롤업_mitre_att&ck_technique_observable_si〕	옵저버블에서 보안 인시던트로 정보 롤업 MITRE-ATT&CK . 자세한 내용은 옵저버블과 MITRE ATT&CK 정보 연결을 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	기본값: 예
위협 조회 결과에서 보안 인시던트로 MITRE ATT&CK 정보를 자동으로 롤업 〔sn_ti.롤업_mitre_att&ck_technique_threat_lookup_si〕	위협 조회 결과의 정보를 보안 인시던트로 롤업 MITRE-ATT&CK 합니다. 자세한 내용은 위협 조회 자동 추출을 참조하세요. 기본값: 예
경보 규칙에서 보안 인시던트로 MITRE ATT&CK 정보를 자동으로 롤업 〔sn_ti.롤업_mitre_att&ck_technique_alert_rule_si〕	경보 규칙에서 보안 인시던트까지 TTP 정보를 자동으로 롤업 MITRE-ATT&CK 합니다. 자세한 내용은 맵 탐지 규칙을 참조하십시오. 기본값: 아니오
하위 보안 인시던트에서 상위 보안 인시던트로 MITRE ATT&CK 정보를 자동으로 롤업 [sn_ti.rollup_mitre_att&ck_technique_child_si_si]	하위 보안 인시던트에서 상위 보안 인시던트로 정보를 자동으로 롤업 MITRE-ATT&CK 합니다. 기본값: 예
이 속성을 활성화하면 "탐지 규칙 - MITRE ATT&CK 매핑" 테이블의 탐지 규칙을 사용하여 범주 및 하위 범주와 같은 보안 인시던트 필드를 매핑할 수 있습니다. [sn_ti.enable_category_mapping_with_alert_rule]	탐지 규칙 - MITRE ATT&CK 매핑 페이지의 범주 및 하위 범주입니다. 기본값: 아니오
"CVE - VUL 수"를 계산하는 시간(시간) [sn_ti.time_to_calculate_cve_vits_count]	CVE 및 VUL 정보를 계산하기 위해 예약된 시간(시간)입니다. 기본값: 24

3. 저장을 클릭합니다.

위협 탐지 및 분석에 사용 **MITRE-ATT&CK**

MITRE-ATT&CK 및 모듈 전반 위협 인텔리전스 의 SIR 프레임워크를 사용하여 조직에 대한 위협을 탐지하고 분석합니다.

정보를 보안 인시던트와 연결 **MITRE-ATT&CK™**

더 나은 보안 인시던트 및 위협 분석을 위해 전술과 기술을 보안 인시던트와 연결합니다 MITRE-ATT&CK .

시작하기 전에

필요한 역할: sn_si.analyst

이 태스크 정보

MITRE-ATT&CK 보안 인시던트와 위협 정보의 상관 관계를 파악하여 더 나은 분석을 수행할 수 있도록 보안 인시던트에 전술 및 기술 정보를 추가합니다. 예를 들어 조직은 보고서 또는 외부의 다른 소스와 같은 위협 인텔리전스 외부 공급업체 소스로부터 전술, 기술 및 절차(TTP) 관련 정보를 받을 수 있습니다 보안 인시던트 응답. 그런 다음 더 나은 상관 관계 및 위협 분석을 위해 이 정보를 다시 추가합니다 SIR .

위협 조회 자동 추출 결과, 옵저버블 또는 하위 보안 인시던트에서 보안 인시던트로 정보를 자동으로 롤업 MITRE-ATT&CK 하도록 선택할 수 있습니다. 보안 인시던트에 대한 자동 롤업의 경우 시스템

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성을 활성화합니다. 또는 각 개별 위협 조회 또는 옵저버블에 대한 정보를 수동으로 롤업할 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 모든 인시던트 표시.
2. 정보를 보강할 보안 인시던트를 MITRE-ATT&CK 선택합니다.
3. **MITRE ATT&CK** 기술 연결 관련 링크를 클릭합니다.
   MITRE ATT&CK 기술 연결 창이 나타납니다.

   이 그림은 관련 목록으로 이동하여 연결 MITRE-ATT&CK 기술을 찾고, 소스 Enterprise ATT&CK를 검토하고, 방법 영향을 추가하고, 기술 시스템 종료/재부팅을 추가하는 방법을 보여줍니다.

   MITRE 정보를 보안 인시던트와 연결
4. 소스를 선택합니다.

   주:
   활성화된 컬렉션 과 매트릭스 만 소스 목록에 나타납니다.

   소스와 관련된 전술과 기술을 선택할 수 있습니다. 여러 소스를 연결할 수도 있습니다.
5. 전술과 기술을 선택하십시오.
6. 옵션: 보안 인시던트와의 관련성에 따라 정보를 검토하고 다음을 수행합니다.
   - 연결을 완전히 제거하려면 bin 아이콘을 클릭합니다. 이 아이콘을 클릭하면 소스와 관련 전술 및 기술이 삭제됩니다.
   - 방법을 제거하려면 방법 옆에 있는 빼기 아이콘을 클릭합니다.
   - 기술을 제거하려면 기술 옆에 있는 x 아이콘을 클릭합니다.
7. 저장을 클릭합니다.

결과
이 MITRE-ATT&CK 정보는 보안 인시던트와 연결됩니다. 이제 **MITRE ATT&CK** 카드에서 관련 정보를 볼 수 있습니다.

종결된 보안 인시던트에 정보 연결 **MITRE-ATT&CK**

이제 전술과 기술을 종결된 보안 인시던트에 연결하여 MITRE-ATT&CK 보안 인시던트 및 위협 분석을 개선할 수 있습니다.

MITRE 정보를 보안 인시던트와 연결

MITRE-ATT&CK 카드를 사용하여 보안 인시던트에서 관련 정보 보기

카드를 사용하여 MITRE-ATT&CK 보안 인시던트에서 관련 정보를 볼 MITRE-ATT&CK 수 있습니다.

위협 조회, 옵저버블 또는 SIEM 통합에서 정보가 롤업된 후 보안 인시던트에 추가됩니다. 그런 다음 집계된 정보가 카드에 표시됩니다 MITRE-ATT&CK . **MITRE ATT&CK** 카드에는 두 가지 뷰가 있습니다.

- 네비게이터 뷰: 네비게이터와 MITRE-ATT&CK 유사한 이 뷰에는 옵저버블 또는 위협 조회 테이블에서 수동으로 추가하거나 롤업한 모든 기술이 표시됩니다. 기술의 원본 표시 는 수동으로 롤업되었거나 소스를 통해 롤업된 경우 기술의 소스를 표시합니다. **Show ID** 는 기술 ID를 표시합니다.

  다음 그림은 **MITRE ATT&CK** 카드 탐색기 보기로 이동하는 방법을 보여줍니다. 사용 가능한 링크 중 하나를 클릭하면 모듈에서 위협 인텔리전스 정보가 열립니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

MITRE ATT&CK 카드: 네비게이터 뷰 및 목록 뷰

- 목록 뷰: 이 뷰는 데이터를 목록 또는 테이블 형식으로 표시합니다. 이 뷰에서는 여러 테이블과 그룹에 분산된 모든 데이터를 볼 수 있습니다.

  다음 그림은 MITRE ATT&CK 카드 목록 보기로 이동하는 방법을 보여줍니다. 사용 가능한 링크 중 하나를 클릭하면 모듈에서 위협 인텔리전스 정보가 열립니다.

옵저버블과 정보 연결 **MITRE-ATT&CK**

전술 및 기술을 옵저버블에 연결하여 MITRE-ATT&CK 세분화된 수준에서 보안 인시던트 및 위협 분석을 개선합니다.

시작하기 전에
필요한 역할: sn_si.analyst

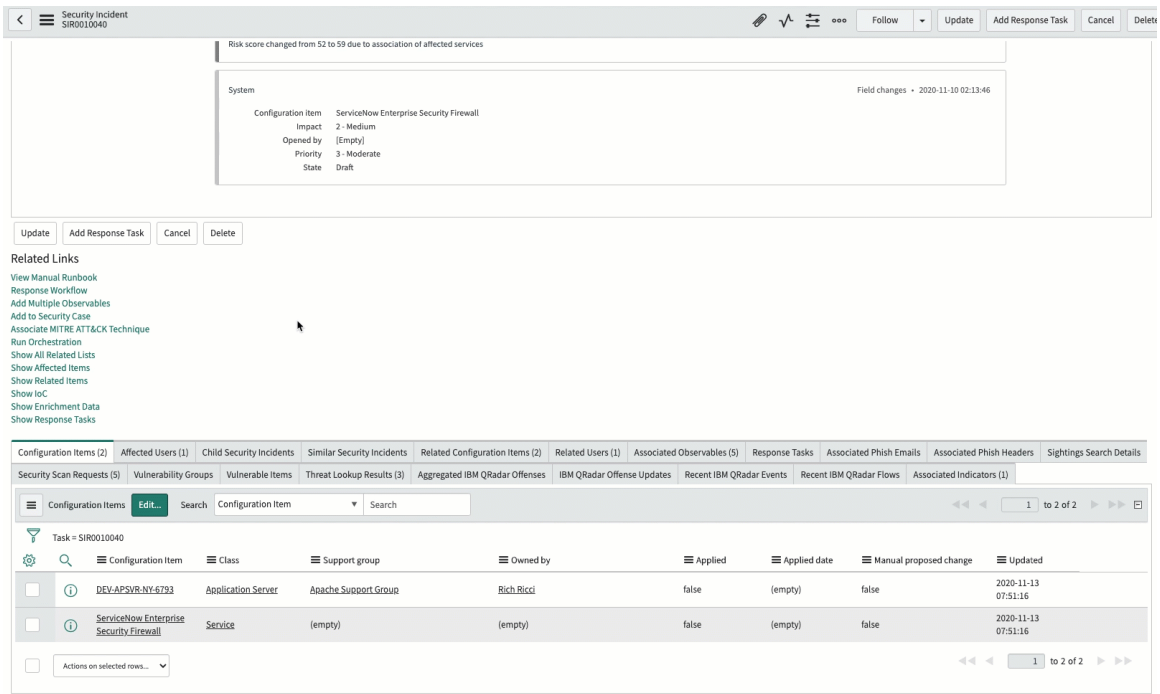
이 태스크 정보
일부 SIEM은 이벤트, 경고 또는 옵저버블과 함께 정보를 제공할 MITRE-ATT&CK 수 있습니다. 세분화된 수준에서 정보를 연결하기 MITRE-ATT&CK 위해 옵저버블에 정보를 추가할 수 있습니다.

옵저버블에서 보안 인시던트로 정보를 자동으로 롤업 MITRE-ATT&CK 하도록 선택할 수 있습니다. 옵저버블을 보안 인시던트로 자동 롤업하려면 시스템 속성을 활성화합니다. 또는 각 옵저버블에 대한 정보를 수동으로 롤업할 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 모든 인시던트 표시.
2. 정보를 보강할 보안 인시던트를 MITRE-ATT&CK 선택합니다.
3. 모든 관련 목록 표시 및 연결된 옵저버블 탭을 클릭합니다.
4. 연결할 옵저버블을 가리키고 마우스 오른쪽 버튼을 클릭한 다음 **MITRE ATT&CK** 기술 연결을 선택합니다.

   다음 그림에서는 관련 목록에서 **MITRE ATT&CK** 기술 연결로 이동하고, 소스를 검토하고, 방법 및 기술을 추가하는 방법을 볼 수 있습니다.



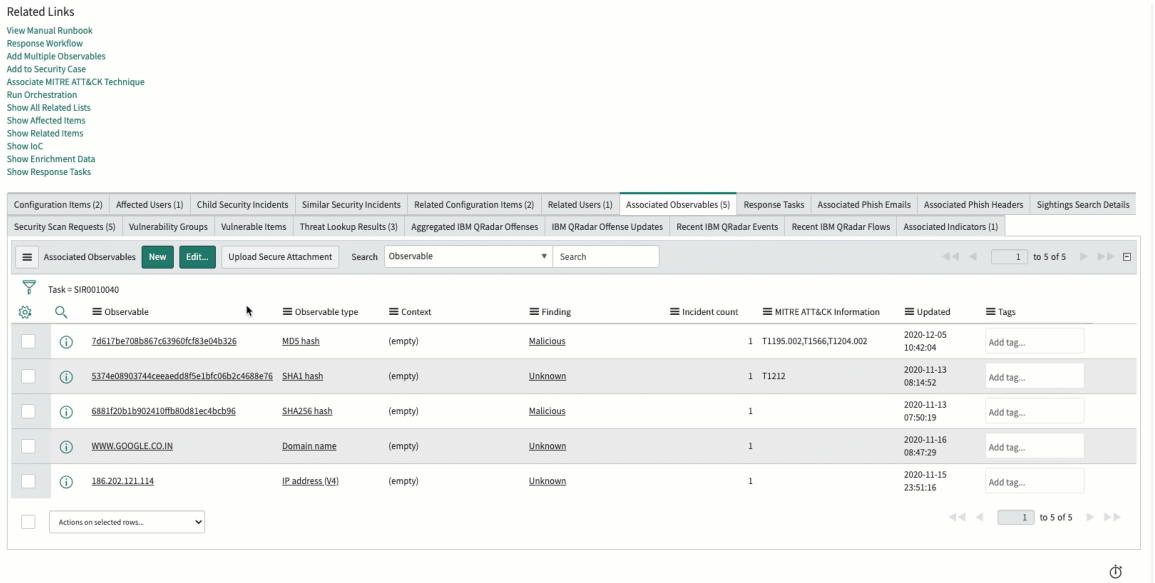
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. 소스 목록에서 소스를 검토합니다.

   주:
   활성화된 컬렉션 과 매트릭스 만 소스 목록에 나타납니다.

6. 방법 및 기술을 검토하고 옵저버블과의 관련성에 따라 추가하거나 제거합니다.
7. 저장을 클릭합니다.
   추가한 전술 및 기술이 옵저버블 관련 목록의 정보 열에 나타납니다 MITRE-ATT&CK .
8. 옵저버블을 선택하고 작업 메뉴에서 **MITRE ATT&CK** 정보를 SI로 롤업을 클릭합니다.
   활성화한 경우 의 자동 롤업 MITRE-ATT&CK 옵저버블에서 보안 인시던트까지 정보을 누르면 정보가 자동으로 롤업됩니다. 자동 롤업을 사용하도록 설정하지 않은 경우 이 작업을 수동으로 수행해야 합니다.

   다음 그림에서는 옵저버블을 선택하고 이 MITRE-ATT&CK 정보를 보안 인시던트에 롤업하는 방법을 보여줍니다.



9. 옵저버블과 연결된 기술의 집계된 뷰를 보려면 목록에서 옵저버블을 두 개 이상 선택한 다음 선택한 행 목록의 작업 메뉴에서 **MITRE ATT&CK** 정보 표시를 클릭합니다.

결과
선택한 옵저버블에 대한 MITRE ATT&CK 정보의 집계 뷰가 표시됩니다.

정보를 보안 케이스와 연결 **MITRE-ATT&CK**

전술과 기술을 보안 케이스에 연결하여 MITRE-ATT&CK 세분화된 수준에서 보안 케이스 관리 및 위협 분석을 개선합니다.

시작하기 전에
필요한 역할: sn_si.analyst

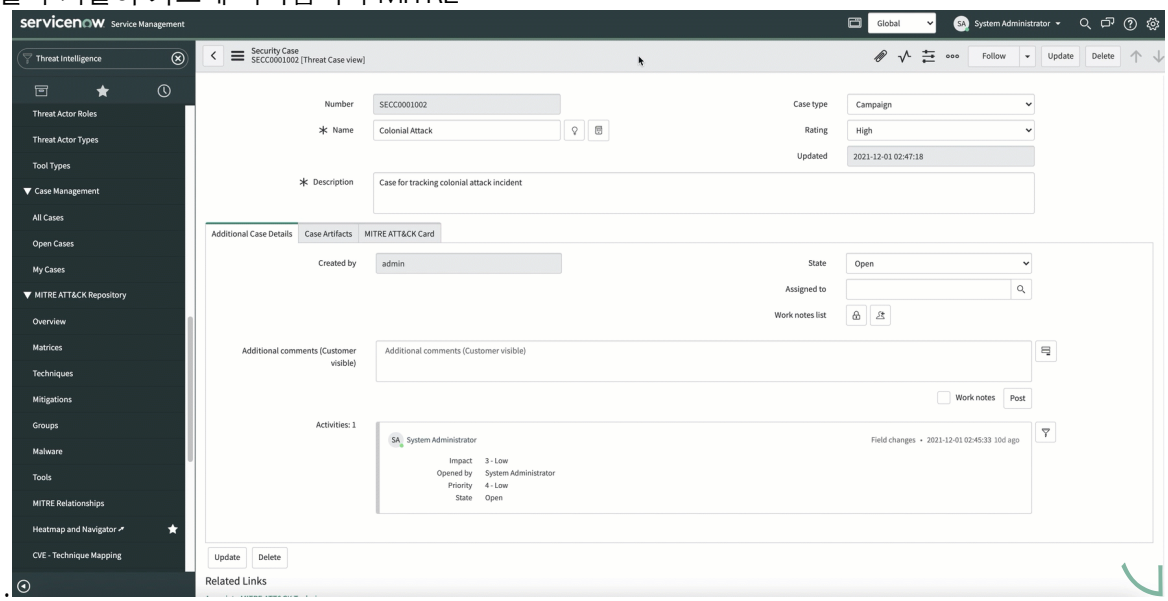
프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 케이스 관리 〉 모든 케이스.
2. MITRE-ATT&CK 정보로 보강할 보안 케이스를 선택합니다.
3. 관련 목록에서 **MITRE ATT&CK** 기술 연결을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음 그림에서는 관련 목록에서 **MITRE ATT&CK** 기술 연결로 이동하고, 소스를 검토하고, 방법 및 기술을 추가하는 방법을 볼 수 있습니다.

4. 소스 목록에서 소스를 검토합니다.
5. 방법 및 기술을 검토하고 케이스와의 관련성에 따라 추가하거나 제거합니다.
6. 저장을 클릭합니다.
   추가한 전술과 기술이 카드에 나타납니다 MITRE-ATT&CK .



위협 조회 결과를 사용하여 정보 롤업 **MITRE-ATT&CK**

정보의 자동 롤업 MITRE-ATT&CK 을 활성화하지 않은 경우 수동으로 이 작업을 수행할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.analyst

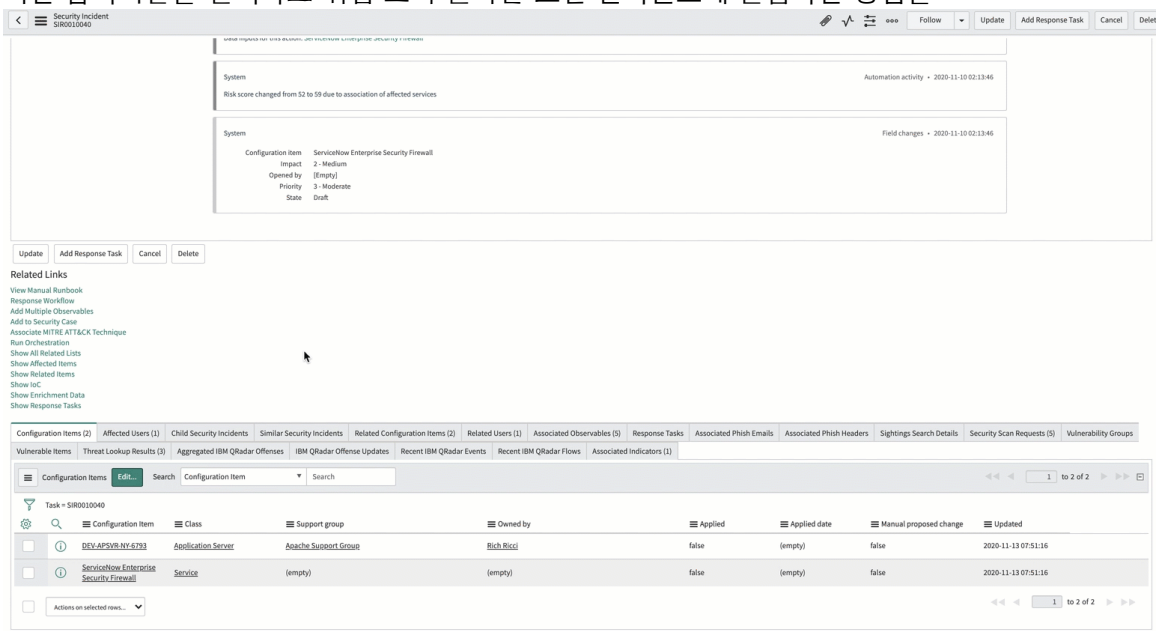
이 태스크 정보
활성화한 경우 의 자동 롤업 MITRE-ATT&CK 위협 조회 결과의 정보 보안 인시던트에 정보가 자동으로 롤업됩니다. 자동 롤업을 활성화하지 않은 경우 수동으로 이 작업을 수행할 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 모든 인시던트 표시.
2. 정보를 보강할 보안 인시던트를 MITRE-ATT&CK 선택합니다.
3. 모든 관련 목록 표시 및 위협 조회 결과 탭을 클릭합니다.
4. 옵저버블을 선택하고 작업 메뉴에서 **MITRE ATT&CK** 정보를 SI로 롤업을 클릭합니다.
   여러 옵저버블을 선택하고 정보를 롤업할 수 있습니다.
5. 다시 로드를 클릭하여 변경 내용을 확인합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음 그림에서는 옵저버블을 선택하고 위협 조회 결과를 보안 인시던트에 롤업하는 방법을



보여줍니다.
카드를 보고 MITRE-ATT&CK 위협 조회 결과가 보안 인시던트로 롤업되었는지 확인할 수 있습니다.

탐지 규칙의 롤업 **MITRE-ATT&CK** 정보

더 나은 보안 인시던트 및 위협 분석을 위해 탐지 규칙에서 보안 인시던트로 정보의 롤업 MITRE-ATT&CK 을 활성화합니다.

시작하기 전에
필요한 역할: 없음.

다음을 수행했는지 확인합니다.

- 속성 모듈의 경보 규칙에서 보안 인시던트 속성으로 롤업 MITRE ATT&ACK 정보를 자동으로 활성화합니다. 기본적으로 이 옵션은 사용되지 않습니다. 자세한 내용은 MITRE-ATT&CK 시스템 속성 검토를 참조하십시오.
- 탐지 규칙 - MITRE ATT&CK TTP 매핑 모듈에서 탐지 규칙을 TTP에 MITRE-ATT&CK 매핑합니다. 탐지 규칙 이름은 보안 인시던트를 트리거하는 경보 규칙 이름과 일치해야 합니다. 자세한 내용은 탐지 규칙 생성 및 매핑 문서를 참조하십시오.

이 태스크 정보
기본 시스템 SIEM 자동 추출 규칙을 사용하지 않으려면 탐지 규칙 매핑을 기반으로 TTP의 MITRE-ATT&CK 자동 롤업을 활성화합니다. 경보 규칙 이름 필드에 보안 인시던트를 트리거하는 경보 또는 이벤트 규칙을 채울 수 있습니다. SIEM 통합, 이메일 구문 분석, 수동 생성 등을 사용하여 경보 규칙 이름 필드를 채울 수도 있습니다.

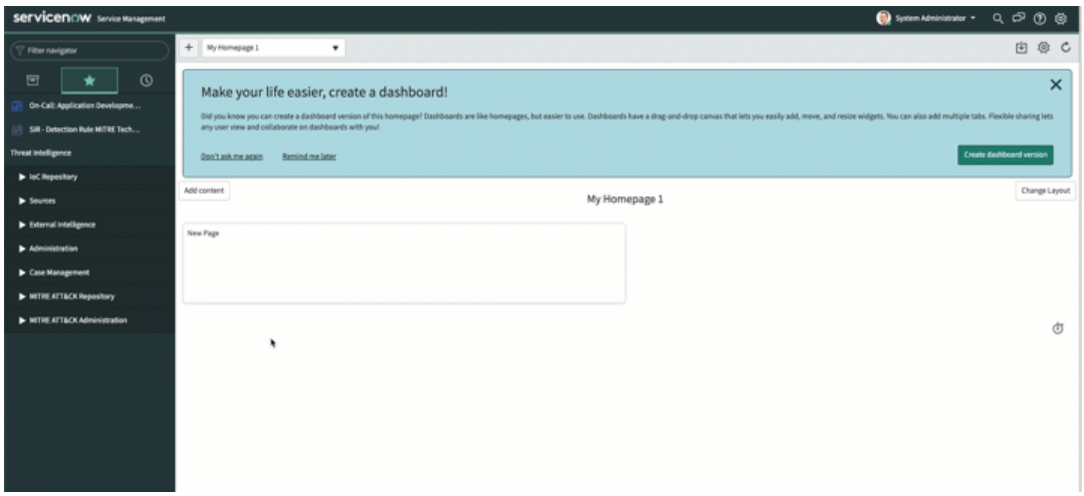
프로시저

1. 다음으로 이동 **MITRE ATT&CK** 관리 〉 속성.
2. 경보 규칙에서 보안 인시던트 속성으로 자동 롤업 MITRE ATT&ACK 정보를 사용하도록 설정하고 저장을 클릭합니다.
   기본적으로 이 옵션은 사용되지 않습니다.
3. 보안 인시던트의 경보 규칙 이름 필드에 필요한 경보 규칙을 채워야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
정확한 경보 규칙 이름을 추가해야 합니다. 여러 규칙을 추가하려면 쉼표 구분 기호를 사용하여 규칙을 추가해야 합니다.

4. 양식을 마우스 오른쪽 버튼으로 클릭하고 저장을 클릭합니다.
보안 인시던트의 경보 규칙 이름 값이 탐지 규칙 - MITRE ATT&CK TTP 매핑 모듈의 기록과 일치하면 경보 규칙과 관련된 해당 기술 및 전술이 보안 인시던트에 자동으로 연결됩니다.



5. 보안 인시던트를 열고 **MITRE ATT&CK** 카드를 선택한 다음 기술이 롤업되었는지 확인합니다.
6. 기술의 원본을 보려면 **Show origin of** techniques 옵션을 활성화합니다.
기술의 출처는 탐지 규칙이어야 합니다.

하위 보안 인시던트에서 정보 롤업 **MITRE-ATT&CK**

정보의 자동 롤업 MITRE-ATT&CK 을 활성화하지 않은 경우 수동으로 이 작업을 수행할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.analyst

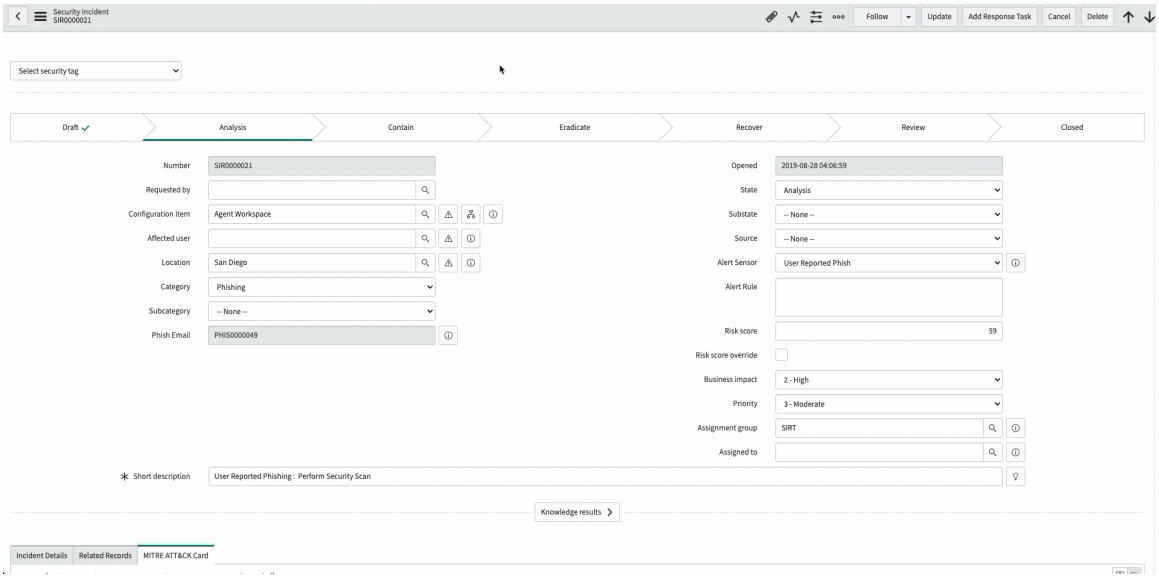
이 태스크 정보
활성화한 경우 의 자동 롤업 MITRE-ATT&CK 하위 보안 인시던트의 정보을 누르면 정보가 자동으로 롤업됩니다. 자동 롤업을 활성화하지 않은 경우 수동으로 이 작업을 수행할 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 인시던트 〉 모든 인시던트 표시.
2. 하위 MITRE-ATT&CK 정보로 보강할 상위 보안 인시던트를 선택합니다.
3. 모든 관련 목록 표시 및 하위 보안 인시던트 탭을 클릭합니다.
4. 하위 보안 인시던트를 선택하고 작업 메뉴에서 **MITRE ATT&CK** 정보를 SI에 롤업을 클릭합니다.
MITRE ATT&CK 정보를 롤업하기 전에 **MITRE ATT&CK** 정보 표시를 클릭하여 하위 보안 인시던트의 MITRE 정보를 볼 수 있습니다.
5. 다시 로드를 클릭하여 변경 내용을 확인합니다.
6. **MITRE ATT&CK** 카드를 클릭하여 기술의 기원을 확인합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음 그림은 하위 보안 인시던트를 선택하고 해당 MITRE-ATT&CK 정보를 상위 보안 인시던트에 롤업하는 방법을



보여줍니다.

MITRE-ATT&CK 카드를 보고 하위 보안 인시던트 MITRE-ATT&CK 정보가 상위 보안 인시던트로 롤업되었는지 확인할 수 있습니다.

특정 필터를 사용하여 **MITRE-ATT&CK** 링크 분석 및 위협 헌팅 수행

옵저버블, 보안 인시던트 및 MITRE-ATT&CK 관련 정보의 상관 관계를 지정하고 링크 분석을 수행하여 조직에서 위협 헌팅을 시작할 수 있도록 합니다.

시작하기 전에

필요한 역할: sn_ti.mitre_analyst, sn_si.read

이 태스크 정보

보안 인시던트를 MITRE-ATT&CK 정보와 연결한 후에는 위협 헌팅을 MITRE-ATT&CK 위한 특정 필터를 사용할 수 있습니다. MITRE-ATT&CK 기존 보안 인시던트 응답 필터와 필터를 사용하여 상관 관계를 지정하고 링크 분석을 수행합니다.

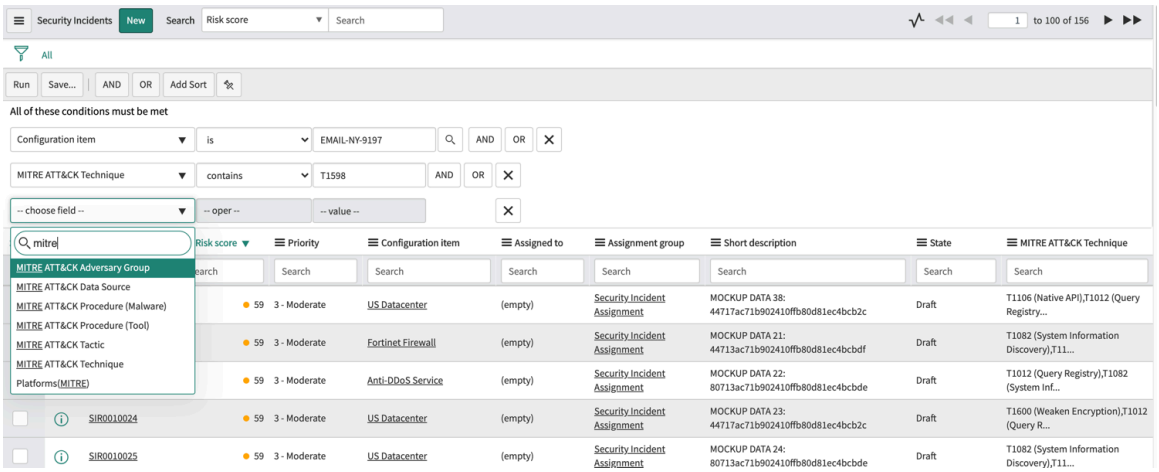
프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 모든 인시던트 표시.
2. 개인 설정 목록 업데이트를 클릭하여 열을 추가합니다MITRE.
3. 관련 정보 및 보안 인시던트 또는 옵저버블과의 연결을 볼 MITRE 수 있도록 필터 조건을 선택합니다.
   - MITRE-ATT&CK 반대 그룹
   - MITRE-ATT&CK 데이터 소스
   - MITRE-ATT&CK 절차(맬웨어)
   - MITRE-ATT&CK 절차(도구)
   - MITRE-ATT&CK 전술
   - MITRE-ATT&CK 기술
4. 위의 기준에 따라 필터 조건을 생성하고 실행을 클릭하여 링크 분석을 수행하거나 보안 인시던트, 옵저버블, MITRE-ATT&CK 관련 정보 간의 상관관계를 지정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
MITRE-ATT&CK 데이터는 문자열로 저장되며 필터 조건의 연산자로만 **contains**를 사용할 수 있습니다.

예를 들어 CI(구성 항목)가 손상되었는지 검토하려면 CI를 선택합니다. 그런 다음 기술 ID를 추가하여 CI와 현재 기술의 상관관계를 MITRE-ATT&CK 지정합니다. 그런 다음 정보의 상관 관계 지정 및 위협 헌팅에 대한 필터 기준을 계속 작성할 수 있습니다.



MITRE-ATT&CK 히트맵 및 네비게이터

히트맵과 네비게이터를 MITRE-ATT&CK 사용하여 기본 탐색을 수행하고 전체 기술 탐지 범위를 시각화할 수 있습니다.

MITRE-ATT&CK 히트맵 및 네비게이터 개요

ATT&CK 행렬의 기본 탐색 및 관찰을 위해 기본 필터와 함께 탐색기를 사용할 수 있습니다. 히트맵은 조직에 적용 범위가 없는 사각지대를 포함하여 탐지 범위의 스펙트럼을 강조 표시합니다. 기술 탐지 범위를 매핑한 후에 사용할 수 있습니다.

히트맵과 내비게이터를 사용하여 다음을 수행할 수 있습니다.

- 조직의 탐지 역량을 빠르고 효율적으로 식별하고 기술 탐지 범위의 격차를 강조 표시합니다.
- 위협을 헌팅하고 관련 기능을 사용하여 위협의 상관 관계를 지정합니다.

히트맵 및 네비게이터에 **MITRE-ATT&CK** 액세스

ATT&CK를 사용할 수 있는 매트릭스를 시각화할 수 있도록 히트맵과 네비게이터에 MITRE-ATT&CK 액세스합니다.

시작하기 전에
필요한 역할: sn_ti.read, sn_ti.mitre_analyst

이 태스크 정보
히트맵을 검토하고, 필터를 사용하여 상관 관계를 지정하고, 조직의 정보, 옵저버블 및 보안 인시던트에 MITRE-ATT&CK 대한 링크 분석을 수행할 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **MITRE ATT&CK** 리포지토리 〉 히트맵 및 네비게이터.
   히트맵과 탐색기가 새 탭에서 열립니다.
2. 히트맵을 채울 소스를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

> **주:**
> 활성화된 컬렉션 과 매트릭스 만 소스 목록에 나타납니다.

다음 그림에서는 히트맵 및 탐색기로 이동하는 방법과 소스(이 예에서는 Enterprise ATT&CK)를 선택하는 방법을 보여줍니다.

히트맵을 채울 소스를 탐색하고 선택합니다

3. 검색 상자를 사용하여 이름 또는 ID를 사용하여 특정 방법이나 기술을 빠르게 찾을 수 있습니다.

   다음 그림에서는 전술, 기술 또는 여기에 포함된 정보를 검색하는 방법을 보여 줍니다. 검색을 사용하여 특정 전술이나 기술을 빠르게 드릴다운합니다.

4. 필터를 클릭하고 기본 또는 고급 필터에서 필터를 선택합니다.
5. 적용을 클릭하고 다음과 같이 필터를 제어합니다.
   - 필터를 저장하려면 사용자 지정 뷰를 생성합니다. 3개의 사용자 지정 뷰를 생성하고 저장할 수 있습니다.
   - 선택한 필터를 제거하려면 **Restore Default** Filters(기본 필터 복원)를 클릭하여 기본 저장 뷰를 로드합니다.
   - 모든 필터와 기존 뷰를 삭제하려면 모든 필터 지우기를 클릭합니다.

   > **주:**
   > 저장되는 뷰는 특정 사용자에게만 해당됩니다.

6. 히트맵 뷰에서 모든 하위 기술을 제거하려면 하위 기술 숨기기를 클릭합니다.
   기술에 하위 기술이 있는 경우 확장 아이콘을 클릭하여 하위 기술을 볼 수 있습니다.

사용자 지정 뷰 사용

히트 맵과 네비게이터의 MITRE-ATT&CK 사용자 지정 뷰를 사용하면 다음에 히트 맵에 도착할 때 즐겨 찾는 필터를 저장하고 볼 수 있습니다.

> **주:**
> 사용자당 모든 MITRE-ATT&CK 컬렉션에 대해 3개의 사용자 지정 뷰를 생성하고 저장할 수 있습니다.

뷰 생성

기본 또는 고급 필터에서 필요한 필터를 선택한 후 필터 헤더에서 줄임표(...) 단추를 클릭하고 새 뷰 만들기를 선택합니다. 사용자 지정 뷰 이름을 입력하고 뷰를 저장합니다.

기본 뷰

이것을 기본 뷰로 저장을 클릭하여 다음에 히트 맵에 도착할 때 뷰를 직접 로드합니다. 각 컬렉션에 대해 기본 뷰를 설정할 수 있습니다.

> **주:**
> 이전 버전에서 플러그인을 업그레이드하는 위협 인텔리전스 경우 이전 버전의 기존 기본 뷰가 사용자 지정 뷰로 나타납니다.

그림은 히트맵에서 사용자 지정 뷰를 만드는 방법을 보여줍니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

뷰 업데이트

필요한 기본 또는 고급 필터를 수정하여 기존 사용자 지정 뷰를 업데이트할 수 있습니다. 사용자 지정 보기를 선택하고 필요에 따라 필터를 업데이트한 다음 필터 헤더에서 줄임표(...) 단추를 클릭하고 보기 업데이트를 선택하여 필터를 저장합니다.

이 그림은 사용자 정의 뷰를 업데이트하는 방법을 보여줍니다.

사용자 지정 뷰 관리

각 사용자 지정 뷰 옆에 있는 확인란을 사용하여 선택한 사용자 지정 뷰 필터를 적용합니다.

각 사용자 정의 뷰 이름 옆에 있는 줄임표(...) 버튼을 클릭하여 다음과 같이 사용자 정의 뷰를 제어합니다.

- 기본 뷰를 설정합니다.
- 사용자 지정 뷰를 기본 뷰로 제거합니다. 이렇게 해도 사용자 지정 뷰는 삭제되지 않습니다.
- 사용자 지정 뷰의 이름을 바꿉니다.
- 사용자 지정 뷰를 삭제합니다.

이 그림에서는 사용자 지정 뷰를 관리하는 방법을 보여 줍니다.

저장된 뷰 익스포트

저장된 사용자 지정 보기를 JSON 파일로 내보내려면 필터 헤더에서 줄임표(...)를 클릭하고 저장된 보기 내보내기를 선택합니다. 로컬 컴퓨터에 다운로드할 사용자 지정 보기의 다운로드 아이콘을 클릭합니다.

이 그림에서는 사용자 지정 뷰를 내보내는 방법을 보여 줍니다.

뷰 임포트

JSON 파일만 임포트할 수 있습니다. 사용자 지정 뷰를 가져오려면 필터 헤더에서 줄임표(...) 단추를 클릭하고 뷰 임포트**(json)**를 선택합니다.

뷰를 임포트할 때 다음 조건을 검토합니다.

- JSON 파일 형식만 임포트할 수 있습니다.
- 한 번에 하나의 뷰 또는 파일만 임포트할 수 있습니다.
- 필터에 이미 세 개의 사용자 지정 뷰가 있는 경우 임포트할 수 없습니다. 사용자 지정 뷰를 삭제하고 뷰를 임포트합니다.
- 기존 사용자 지정 뷰 이름이 있는 뷰는 임포트할 수 없습니다. 임포트하기 전에 뷰 이름을 바꿉니다.

이 그림에서는 뷰를 임포트하는 방법을 보여 줍니다.

기본 필터가 있는 탐색기

탐색기에서 MITRE-ATT&CK 기술을 필터링하려면 기본 필터를 사용합니다. 저장소의 MITRE-ATT&CK 정보를 선택할 수 있습니다.

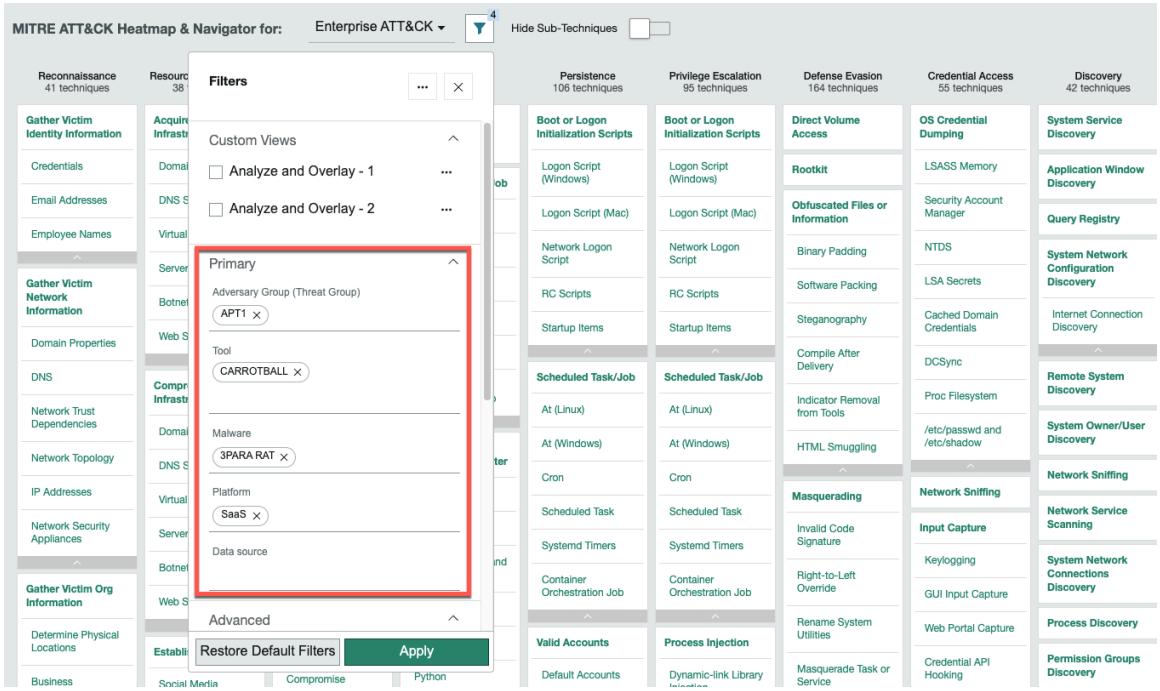
필터	설명
반대 그룹(위협 그룹)	보안 커뮤니티에서 공통 이름으로 추적되는 관련 침입 활동 집합입니다. 그룹은 다양한 위협 그룹,

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필터	설명
	활동 그룹, 위협 행위자, 침입 세트 및 캠페인을 의미할 수 있습니다. 반대 그룹(위협 그룹) 필터에 여러 그룹을 추가할 수 있습니다. 예를 들어 APT1 및 AT12는 둘 다 중국에 기인하는 위협 그룹이므로 추가합니다. 두 그룹 모두 서로 다른 출처를 대상으로 할 수 있지만 유사한 기술을 사용할 수 있습니다.
도구	위협 행위자가 공격을 수행하는 데 사용하는 합법적인 소프트웨어입니다. 위협 행위자가 사용하는 방법과 도구를 알고 있으면 위협 행위자가 캠페인을 실행하는 방법을 이해할 수 있습니다. 도구에는 엔터프라이즈 시스템에서 찾을 수 없는 소프트웨어와 Microsoft Windows 유틸리티와 같은 환경에 이미 있는 운영 체제의 일부로 사용할 수 있는 소프트웨어가 모두 포함됩니다. 예를 들어 gsecdump는 APTI1 악의적 그룹이 Microsoft Windows 운영 체제에서 암호 해시 및 LSA 비밀(로컬 보안 기관)을 가져오는 데 사용하는 공개적으로 사용 가능한 자격 증명 덤퍼입니다.
맬웨어	상용, 사용자 지정 클로즈드 소스 또는 오픈 소스 소프트웨어로 악의적 사용자가 악의적인 목적으로 사용할 수 있습니다. PlugX, CHOPSTICK 등을 예로 들 수 있습니다
플랫폼	특정 플랫폼을 대표 MITRE-ATT&CK 하는 전술 및 기술입니다. 예를 들어 MITRE-ATT&CK Enterprise ATT&CK 매트릭스에서 Microsoft Windows, macOS, Linux, PRE, AWS, GCP, Azure, Azure AD, Office 365, SaaS, Network 플랫폼을 지원합니다.
데이터 소스	환경에서 수집하고 기술을 검색하는 MITRE-ATT&CK 데 사용하는 데이터 소스입니다. 예를 들어 DLL 모니터링 및 브라우저 확장이 있습니다.

다음 그림은 탐색기에서 MITRE-ATT&CK 사용할 수 있는 모든 기본 필터를 보여줍니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



기본 및 고급 기능이 있는 히트맵 사용

고급 필터가 있는 히트맵을 사용하면 보안 인시던트와 MITRE-ATT&CK 정보의 상관관계를 지정하여 분석을 수행할 수 있습니다.

기술 **ID** 보기

기술 **ID** 표시 필터를 선택하면 기술 이름과 함께 기술 ID를 볼 MITRE-ATT&CK 수 있습니다.

히트맵에서 기술 ID 보기

우선순위별 관련 기술 보기

탐색기에서 관련 우선순위를 기준으로 기술을 필터링하려면 기술 관련 우선순위 필터를 기준으로 필터링을 선택하고 메뉴에서 관련 우선순위 를 선택합니다. 필터링에 여러 우선순위를 할당할 수 있습니다. 히트맵에서 기술을 가리켜 기술의 우선순위를 알 수도 있습니다.

관련 우선순위 정보는 기술 관련 우선순위 필드에서 설정한 우선순위를 기반으로 합니다.

이 그림에서는 관련 우선순위를 기준으로 필터링하는 방법을 보여줍니다.

기술 탐지 범위 보기

히트맵에서 전체 기술 탐지 범위를 보려면 기술 탐지 범위 표시 필터를 선택합니다. 히트맵은 적용 범위가 없는 사각지대를 포함하여 감지 범위의 시각적 스펙트럼을 강조 표시합니다. 기본 시스템 점수 정의 및 색상은 기술 탐지 범위에서 정의되었습니다. 이 정보는 전체 기술 탐지 범위에서 자동으로 추출되었습니다.

예를 들어 히트맵에서 빨간색으로 표시된 영역은 탐지 부족을 나타냅니다. 파란색으로 표시된 영역은 전체 검색 기능이 있음을 나타냅니다. 주황색, 노란색 및 연한 파란색으로 표시된 영역은 부분 검색 기능을 나타냅니다.

- 색상 시각화는 사용자가 정의한 기술 정의와 색상 코딩 을 기반으로 합니다.
- 범위 시각화는 정의한 기술 탐지 범위 매핑 을 기반으로 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 기본 시스템 범위 정의를 수정하면 범위 유형 아이콘이 히트맵의 기술과 함께 표시되지 않습니다.

  주:
  히트맵은 기본 시스템에서 정의한 기술, 탐지 범위 및 검사 색상과 동일한 필드를 수정할 때 예상대로 작동합니다.

이 그림에서는 모든 기술 및 하위 기술에 대한 기술 탐지 범위와 범위 유형을 해당 색상 및 아이콘과 함께 볼 수 있습니다.

히트맵 기술 탐지 범위

기술 완화 범위 보기

히트맵에서 전체 기술 완화 범위를 보려면 기술 완화 범위 표시 필터를 선택합니다. 히트맵은 적용 범위가 없는 영역을 포함하여 완화 범위의 시각적 스펙트럼을 강조 표시합니다. 완화 범위, 색상 및 백분율 범위는 완화 범위 정의에 정의되어 있습니다. 이 정보는 전체 기술 완화 범위에서 추출됩니다.

예를 들어 빨간색으로 강조 표시된 기술은 완화 범위가 없음을 나타내고, 주황색은 완화 범위가 좋지 않음을 나타내고, 파란색은 완화 범위가 우수함을 나타냅니다.

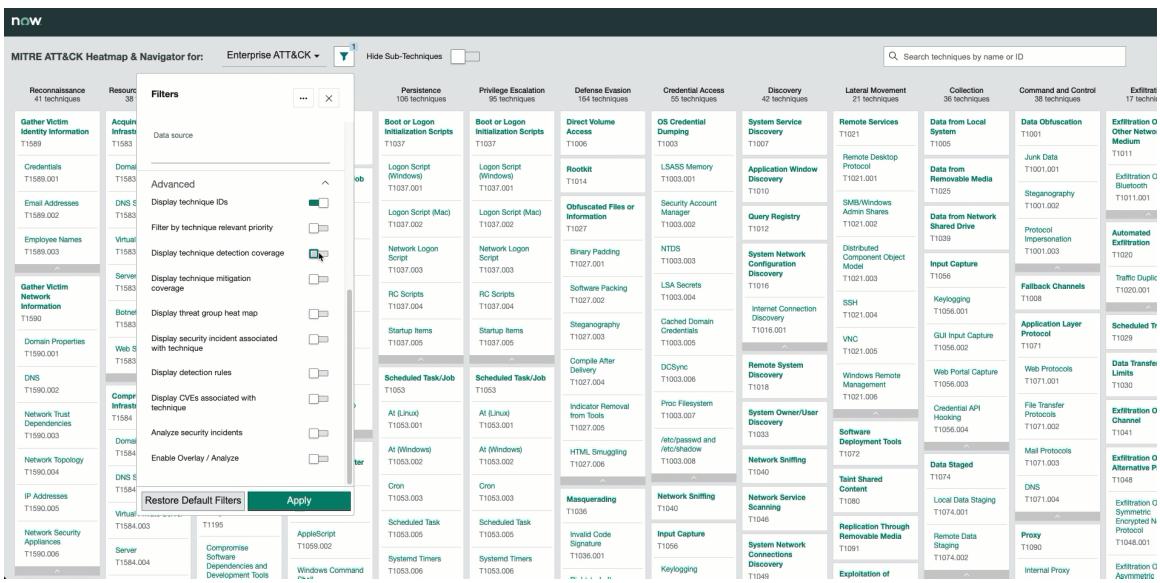
- 색상 시각화는 사용자가 정의하는 기술 완화 정의 및 색상 코딩 을 기반으로 합니다.
- 범위 시각화는 사용자가 정의하는 기술 완화 범위 매핑 을 기반으로 합니다.
- 기본 시스템 완화 범위 정의를 수정하면 완화 범위 유형 아이콘이 히트맵의 기술과 함께 표시되지 않습니다.

  주:
  히트맵은 기본 시스템에서 정의한 기술, 완화 범위 및 범위 색상과 동일한 필드를 수정할 때 예상대로 작동합니다.

이 그림은 기술 완화 범위 히트맵을 보여줍니다

탐지 및 완화 범위 보기

기술 탐지 및 기술 완화 범위 필터를 함께 사용하여 기술 탐지의 관련성에 대한 인사이트를 얻고 조직의 범위를 완화할 수 있습니다.



이 그림에서는 검색 필터와 완화 필터를 함께 사용하는 방법을 보여 줍니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

위협 그룹 보기

히트맵에서 위협 그룹 기술 정보를 보려면 **Display threat group heat** map(위협 그룹 히트맵 표시)을 선택합니다. 특정 기술을 사용하는 위협 그룹의 수를 측정할 수 있습니다. 공격자 수가 많을 때 특정 기술을 사용한 공격의 확률이 높아집니다. 위협 그룹 범위 및 히트맵 색상은 위협 그룹 기술 히트맵 정의에 정의되어 있습니다.

- 히트맵 및 텍스트에 대한 색상 시각화는 기술 히트맵 정의에 대한 위협 그룹을 기반으로 합니다.
- 위협 그룹 범위 시각화는 위협 그룹과 기술 매핑을 기반으로 합니다.
- 기술 탐지 범위 또는 기술 완화 범위가 활성화된 경우 위협 그룹 히트 맵 필터 표시를 사용할 수 없습니다. 이 그림은 히트맵의 위협 그룹 정보를 보여줍니다.

기술과 관련된 보안 인시던트 보기

조직에서 자주 악용되어 보안 인시던트를 유발한 기술을 보려면 기술과 관련된 보안 인시던트 표시를 클릭합니다. 분석을 위해 새 창에서 열리는 링크를 클릭하면 연관된 각 보안 인시던트에 대한 자세한 정보를 볼 수 있습니다. 기술과 관련된 보안 인시던트입니다.

- 우선순위: 보안 인시던트 우선순위 를 선택하여 보안 인시던트 우선순위로 필터링합니다.
- 날짜 범위: 보안 인시던트 날짜 범위를 선택하여 날짜 범위를 기준으로 보안 문제를 필터링합니다.
- 가양성: 가양성 보안 인시던트 필터링 을 선택하여 가양성 문제를 제거합니다. 이 필터를 선택하면 히트맵에 표시되는 보안 인시던트 수가 줄어듭니다.

이 필터를 표시 기술 탐지 범위 필터와 함께 사용하면 선택한 날짜까지 조직에 대한 기술 탐지 범위의 관련성에 대한 인사이트를 제공합니다.

예를 들어 두 필터를 모두 켜면 방어 회피 전술에서 가장 기술이 적용되지 않는 것을 볼 수 있습니다. 더 자세히 살펴보면 가장 기술은 가장 작업 또는 서비스와 관련이 있으며 여기에는 연결된 보안 인시던트도 있습니다. 이는 Masquerading 기술에 대한 기술 탐지 범위에 차이가 있음을 보여주며 전체 기술 탐지 범위를 수정할 수 있습니다.

탐지 규칙 보기

특정 기술에 대해 정의된 탐지 규칙이 있는지 보려면 탐지 규칙 표시를 클릭합니다. 또한 연결된 각 탐지 규칙을 해당 정의와 함께 볼 수도 있습니다.

이 정보는 사용자가 정의한 탐지 규칙 매핑 을 기반으로 합니다. 연결된 탐지 규칙을 봅니다.

기술과 관련된 **CVE** 보기

각 기술과 연관된 CVE(Common Vulnerabilities and Exposures) 정보를 보려면 기술과 관련된 **CVE** 표시를 클릭하십시오. 기술 정보에 대한 CVE는 CVE - 기술 매핑 모듈에서 사용할 수 있는 정보를 기반으로 합니다. 이를 통해 알려진 취약성에 대한 인사이트를 얻을 수 있으며 공격자가 잠재적으로 조직을 악용할 수 있는지 여부를 알 수 있습니다.

> **중요사항:**
> 히트맵이 VIT와 연결된 관련 CVE만 표시하도록 개선되었습니다

CVE 및 기술과 연결된 VIT 를 보려면 **CVE** 및 기술과 연결된 **VIT** 표시를 선택합니다. 또한 VIT 없이 기술을 추가로 필터링하려면 **VIT** 없이 기술 숨기기를 선택합니다. 사용자가 보는 CVE 및 VIT 정보는 사용자 환경의 제품에서 취약성 대응 가져옵니다. 히트맵에서 필터링된 CVE 및 VIT 목록을 보고 히트맵에서 모든 기술에 대한 각 CVE 또는 VIT로 이동할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

- 기술과 연관된 **CVE** 표시는 제품이 사용자 환경에 설치된 경우에만 취약성 대응 사용할 수 있습니다.
- VIT 및 CVE 정보는 에서 설정한 예약된 작업을 기반으로 계산됩니다. MITRE-ATT&CK 속성. 기본 시스템 일정 작업은 24시간으로 설정됩니다.

이 필터를 기술과 관련된 보안 인시던트 표시 필터와 함께 사용하면 알려진 취약성으로 인해 조직에서 보안 인시던트가 발생했는지 여부를 파악할 수 있습니다.

각 CVE에 대한 자세한 정보를 보고 CVE가 조직과 관련이 있는지 분석할 수 있습니다. 이렇게 하려면 취약성 항목을 확인합니다. 취약성 항목이 생성되면 모듈에서 관련 CI 정보에 대한 자세한 정보를 볼 수 있습니다 취약성 대응 . 또한 심각도와 우선순위를 검토하여 정보에 입각한 결정을 내릴 수 있습니다. CVE를 검토하여 정보에 입각한 결정을 내립니다.

보안 인시던트 분석

보안 인시던트를 분석하고 공격에 악의적 사용자가 사용하는 기술을 검토하려면 보안 인시던트 분석을 클릭합니다. 쉼표로 구분된 문자열을 사용하여 분석을 위해 여러 보안 인시던트를 추가할 수 있습니다.

이 필터는 보안 인시던트를 분석하는 데 도움이 됩니다. 인시던트가 발생한 이유, 악용된 기술, 알려진 위협 행위자가 관련되어 있는지, 위협 행위자가 공격에 특정 시퀀스를 사용했는지 등을 알 수 있습니다. 여러 보안 인시던트를 동시에 분석할 수 있으므로 정보의 상관 관계를 지정하여 서로 관련이 있는지 또는 격리된 인시던트인지 확인할 수 있습니다. 보안 인시던트가 관련되어 있고 패턴을 관찰하는 경우 킬 체인에서 진행 상황을 검토하여 공격을 차단하거나 조직에 대한 방어 전략을 수립할 수 있습니다.

보안 인시던트 분석 필터를 악의적 그룹과 같은 기본 필터와 함께 사용하는 경우 알려진 악의적 사용자가 관련되어 있는지 상관 관계를 지정할 수 있습니다. 예를 들어 여러 보안 인시던트를 분석할 때 보안 인시던트와 관련된 기술이 킬 체인의 형태로 존재합니다. 정보를 악의적 사용자와 겹치면 보안 인시던트와 관련된 기술과 악의적 공격자와 관련된 기술 간에 중복되는 것을 확인할 수 있습니다. 두 필터가 모두 활성화된 경우 중복된 기술 정보만 표시됩니다.

보안 인시던트 분석

오버레이를 사용하여 보안 인시던트 및 악의적 그룹 분석

오버레이/분석 사용 필터를 사용하여 악의적 동작을 확인하고, 하나 이상의 보안 인시던트를 분석하고, 정보의 상관 관계를 지정하여 공격이 고립된 인시던트인지 알려진 악의적 사용자가 조직한 공격인지 확인합니다.

예를 들어 이제 보안 인시던트와 위협 악의적 킬 체인 동작을 동일한 보기에서 볼 수 있습니다. 이 보기는 공격 및 알려진 악의적 동작을 알려주는 겹침 정보를 제공합니다. 이를 통해 이것이 고립된 공격인지 알려진 악의적 공격에 의한 조정된 공격인지 분석할 수 있습니다.

오버레이 분석 필터를 사용하도록 설정하면 반대 그룹 필터를 제외한 모든 기본 필터가 무시되고 뷰를 생성하는 동안 기술 관련 우선순위별 고급 필터가 무시됩니다.

오버레이 분석 필터를 활성화한 후 색상표를 사용하여 다음에 대한 색상을 할당합니다.

- 보안 인시던트 분석
- 반대 그룹
- 오버레이

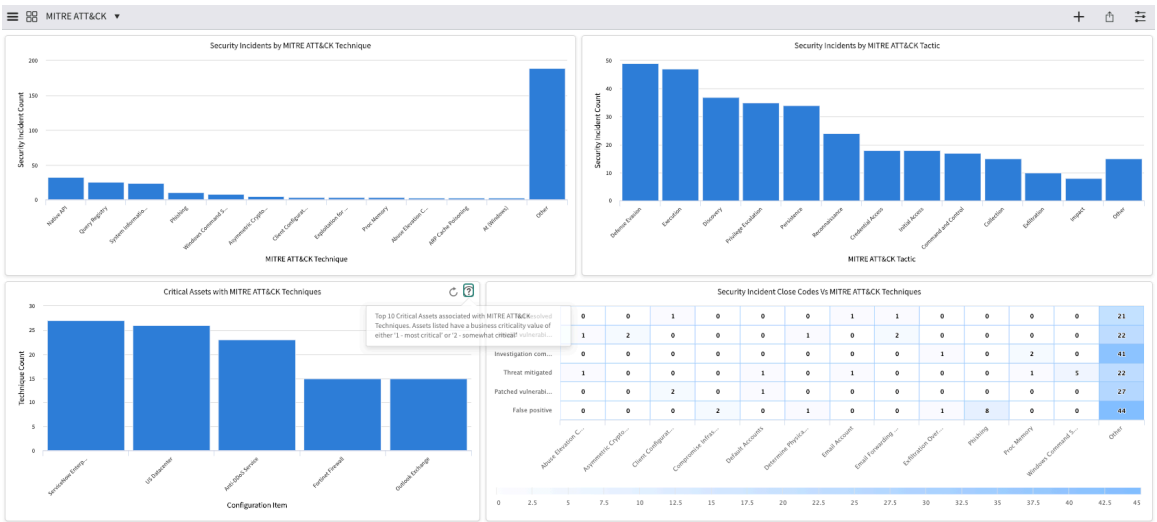
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음 그림은 공격자 그룹 APT18이 킬 체인의 여러 기술과 전술에 분산되어 있음을 보여줍니다. 또한 분석 결과, 추적 중인 악의적 그룹 및 보안 인시던트를 오버레이하는 세 가지 기술이 있음을 알 수 있습니다. 이 그림은 악의적 및 보안 인시던트 오버레이 정보를 보여줍니다.

MITRE-ATT&CK 대시보드 사용

대시보드는 MITRE-ATT&CK 조직에서 사용되는 데이터 소스 범위, 전술 및 기술에 대한 경영적 뷰를 제공합니다.

개요 모듈에는 MITRE-ATT&CK 추세와 보고서를 포함한 보안 인시던트에 대한 정보가 표시됩니다 MITRE-ATT&CK . 위젯의 원하는 부분(막대, 데이터 요소, 테이블 등)을 클릭하여 해당 부분과 관련된 데이터를 볼 수 있습니다.



MITRE-ATT&CK 대시보드를 사용하여 보안 관련 데이터 보기

MITRE-ATT&CK 대시보드를 사용하여 조직에서 사용되는 데이터 소스 범위, 전술 및 기술에 대한 개요를 확인합니다.

시작하기 전에
필요한 역할: sn_si.ciso, sn_si.analyst, sn_si.manager, sn_ti.read

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 **MITRE ATT&CK** 리포지토리 〉 개요.
2. 추가 상세 정보를 보려면 다음 위젯 중 하나를 클릭하십시오.
   - 기술별 MITRE-ATT&CK 보안 인시던트
   - 방법별 MITRE-ATT&CK 보안 인시던트
   - 기술을 갖춘 MITRE-ATT&CK 중요 자산
   - 보안 인시던트 종결 코드 대 MITRE-ATT&CK 기술
   - 탐지 범위별 MITRE-ATT&CK 기술
   - 완화 범위별 MITRE-ATT&CK 기술
   - MITRE-ATT&CK 기술별 위협 그룹
   - MITRE-ATT&CK 기술별 CVE

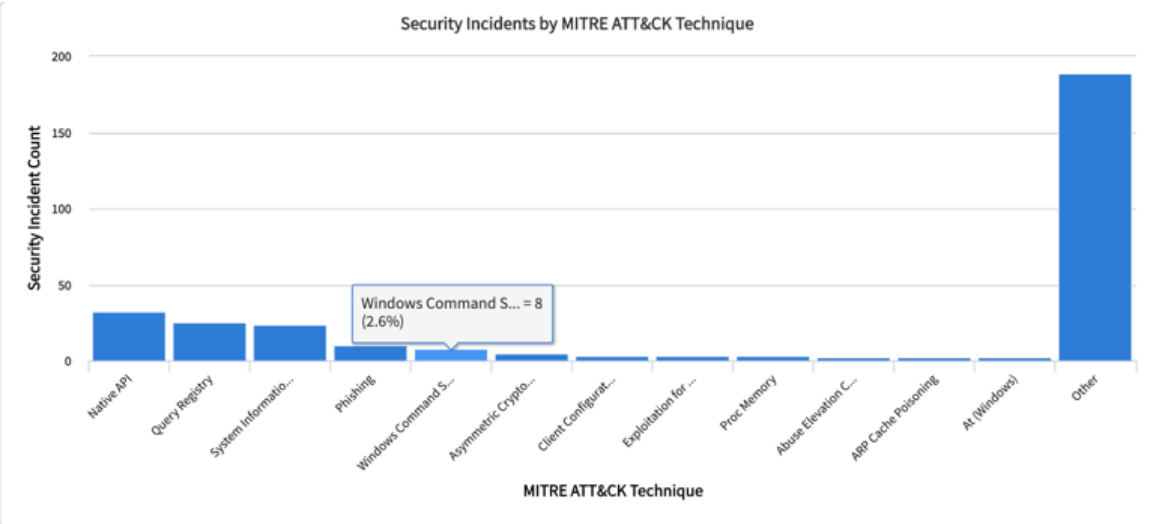
MITRE-ATT&CK 위젯

MITRE-ATT&CK 개요 모듈은 사용자 환경의 보안 인시던트 정보와 정보를 상호 연결할 MITRE-ATT&CK 수 있는 위젯으로 구성됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

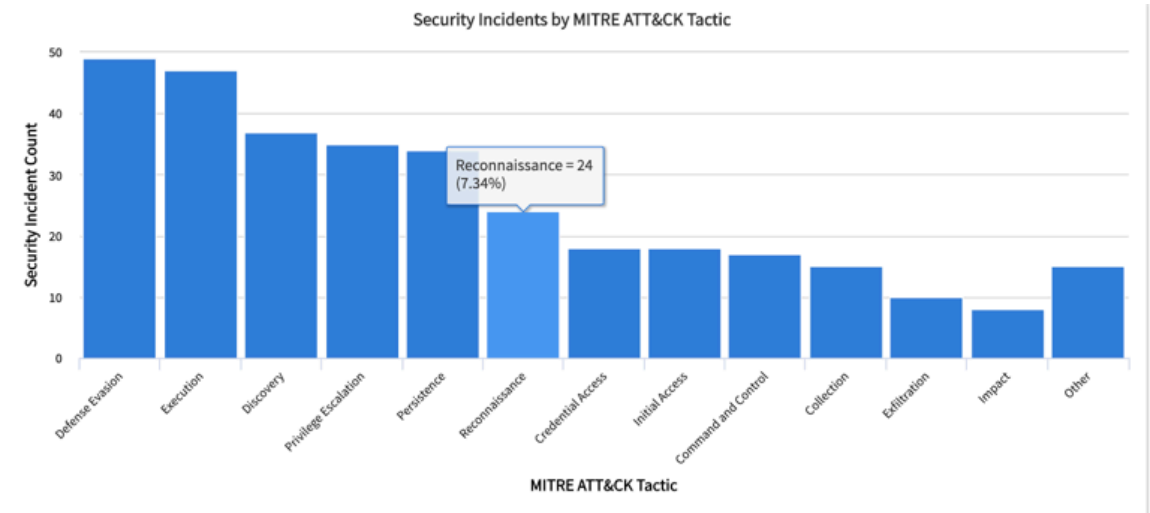
기술별 **MITRE-ATT&CK** 보안 인시던트 예

이 예시에서는 **MITRE ATT&CK** 기술별 보안 인시던트 위젯에 지난 90일 동안 조직 환경의 보안 인시던트별 기술이 표시됩니다.



방법별 **MITRE-ATT&CK** 보안 인시던트 예

이 예시에서는 **MITRE ATT&CK** 전술별 보안 인시던트 위젯 에 지난 90일 동안 조직 환경의 보안 인시던트별 상위 전술이 표시됩니다.

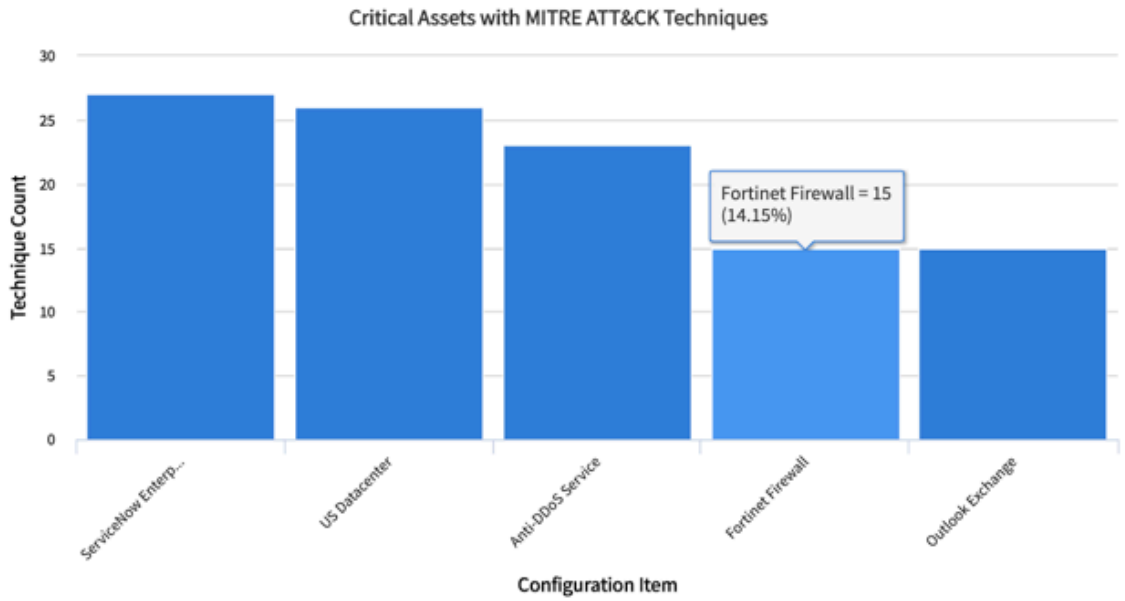


기술을 사용하는 **MITRE-ATT&CK** 중요한 자산의 예

이 예시에서는 **MITRE ATT&CK** 기술이 있는 중요 자산 위젯에 기술과 연관된 MITRE-ATT&CK 상위 10개의 중요 자산이 표시됩니다. 자산의 비즈니스 중요도는 1(가장 중요) 또는 2(다소 중요)입니다.

이 보고서를 통해 조직은 중요 자산에 대한 공격을 수행하는 데 사용되는 기술의 유형과 수를 볼 수 있습니다.

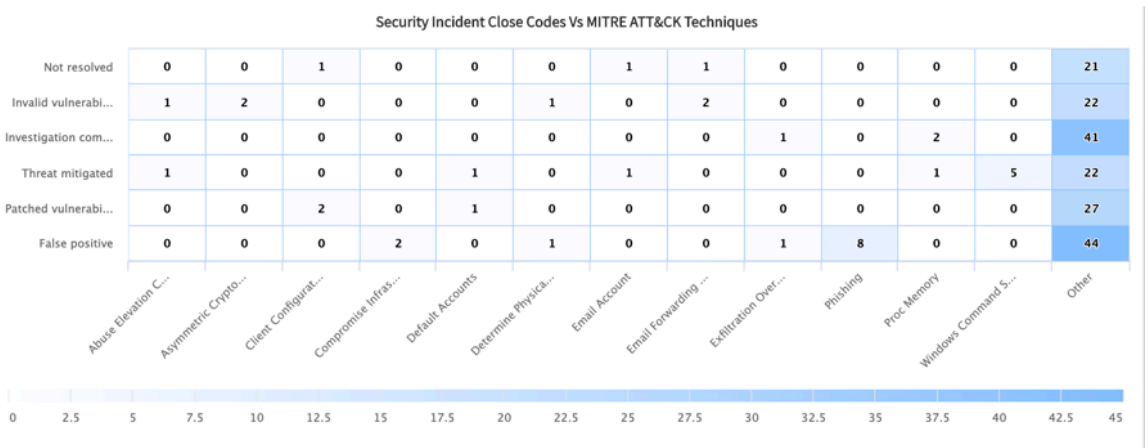
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



보안 인시던트 종결 코드 대 **MITRE-ATT&CK** 기술의 예

이 예에서 보안 인시던트 종결 코드 대 *MITRE-ATT&CK* 기술 위젯은 조직 환경에서 식별된 최상위 기술에 대해 매핑된 보안 인시던트 종결 코드를 표시합니다.

x축은 기업에 대한 공격을 수행하는 데 사용된 상위 기술을 표시하고 y축은 닫힌 코드를 표시합니다.

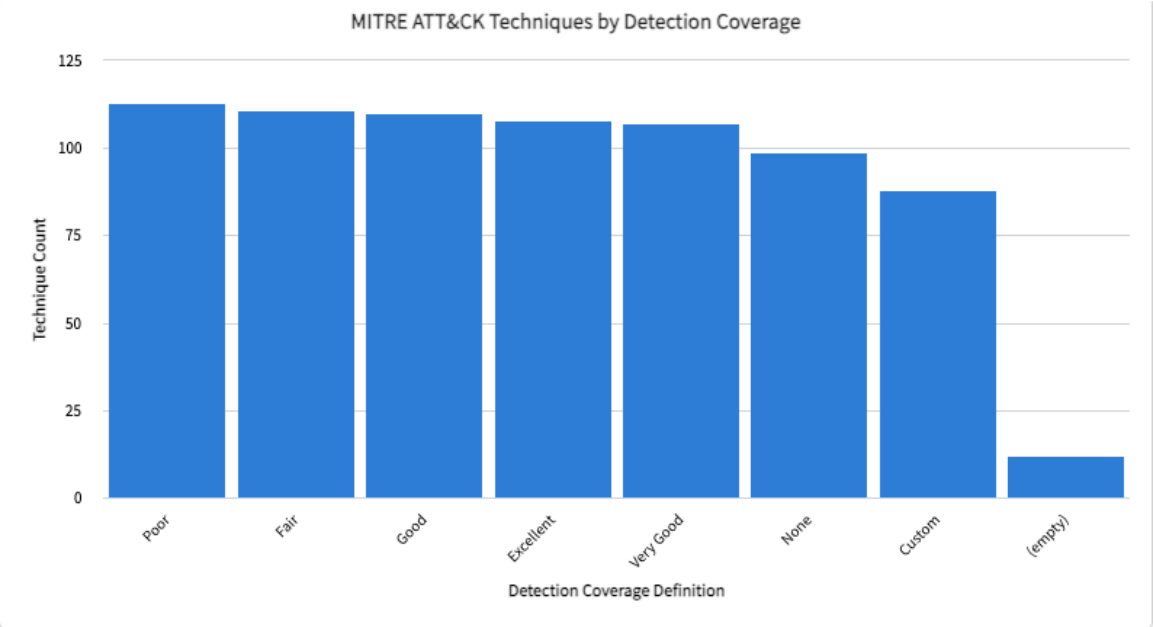


기술별 **MITRE-ATT&CK** 탐지 범위의 예

이 예에서 탐지 범위별 **MITRE-ATT&CK** 기술 위젯은 사용자 환경의 탐지 범위별로 기술 수를 표시합니다.

x축에는 기술 수가 표시되고 y축에는 감지 범위 유형이 표시됩니다.

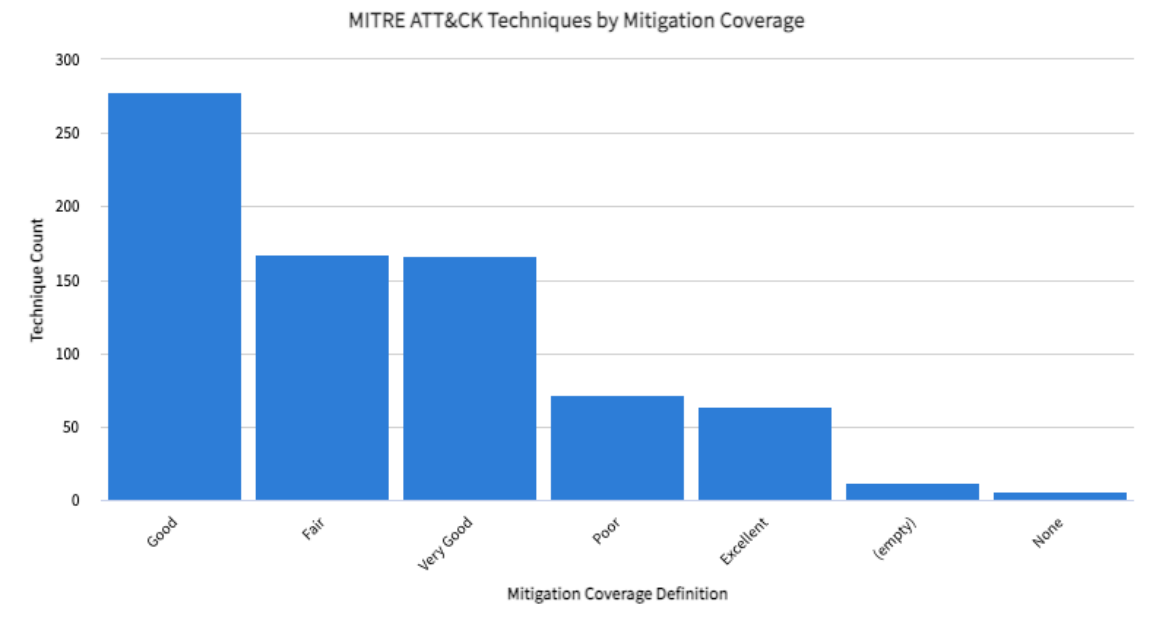
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



기술별 **MITRE-ATT&CK** 완화 범위의 예

이 예에서 **MITRE-ATT&CK** 완화 범위별 기술 위젯은 사용자 환경의 완화 범위별 기술 수를 표시합니다.

x축에는 기술 수가 표시되고 y축에는 완화 범위 유형이 표시됩니다.

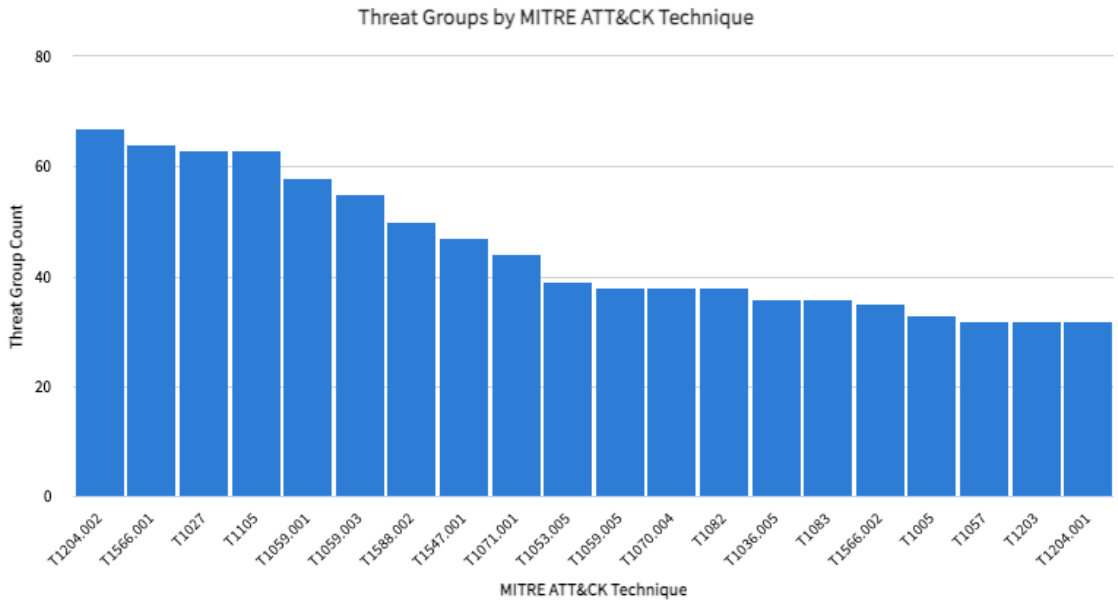


기술별 **MITRE-ATT&CK** 위협 그룹의 예

이 예에서 **Threat Groups by MITRE-ATT&CK Technique(MITRE-ATT&CK** 기술별 위협 그룹) 위젯에는 위협 그룹 수별로 기술이 표시됩니다. 이 위젯에는 위협 그룹 수가 가장 많은 20개의 기술이 표시됩니다.

x축에는 위협 그룹 수가 표시되고 y축에는 기술이 표시됩니다 MITRE-ATT&CK .

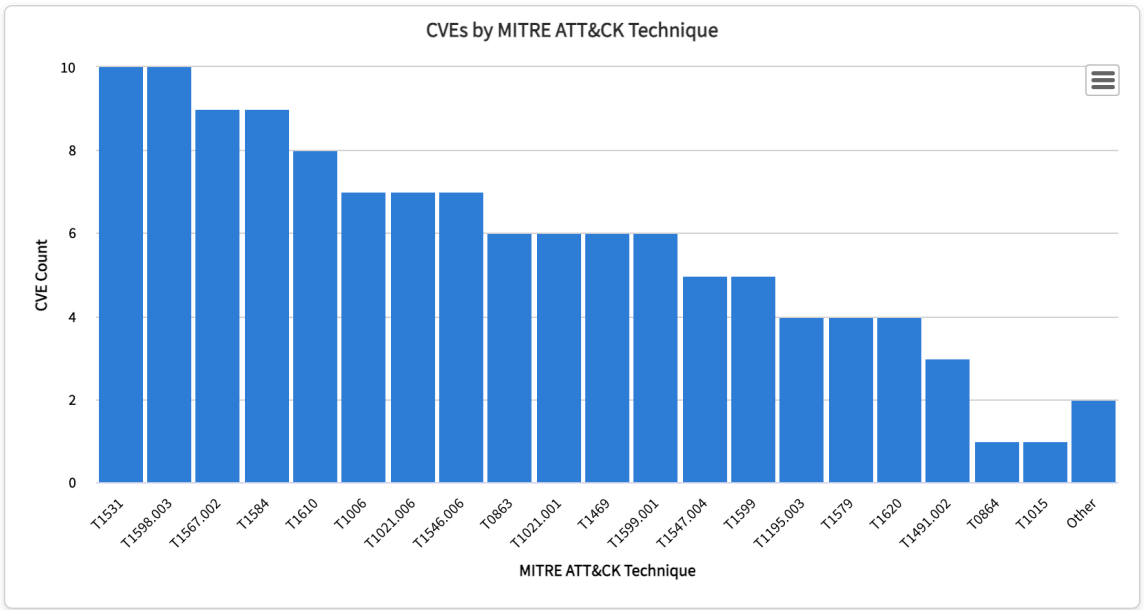
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



기술별 **MITRE-ATT&CK CVE** 예

이 예에서 **MITRE-ATT&CK** 기술별 **CVE** 위젯은 사용자 환경에서 관련 CVE 수가 있는 기술을 표시합니다.

x축에는 관련 CVE 수가 표시되고 y축에는 기술이 표시됩니다 MITRE-ATT&CK .



위협 인텔리전스 관리

위협 인텔리전스 활성화 시 기본 시스템을 사용할 준비가 되었습니다. 관리 애플리케이션 메뉴의 특정 모듈에 기록을 추가할 수 있지만 대부분은 이미 산업 표준 정보로 채워져 있습니다.

탐색 모음의 관리 모듈에서 다음 애플리케이션을 사용할 수 있습니다.위협 인텔리전스

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Threat Intelligence 관리 애플리케이션

애플리케이션	설명
속성	위협 인텔리전스 속성을 사용하면 API 키 설정을 포함하여 시스템이 작동하는 다양한 측면을 제어할 수 있습니다.
공격 메커니즘	이 모듈은 취약성을 악용할 때 자주 사용되는 메커니즘을 기반으로 공격 패턴을 계층적으로 구성합니다.
공격 동기	이 모듈에서는 위협 액터 또는 침입 집합에 의한 공격의 강도를 형성하는 가능한 공격 동기를 나열합니다.
디스커버리 방법	이 모듈에서는 보안 인시던트를 검색하는 방법을 설명합니다.
피드	이 기능은 더 이상 사용되지 않습니다.
표시기 유형	이 모듈은 특정 옵저버블 조건을 식별하는 패턴으로 구성된 사이버 위협 지표와 패턴의 의미, 패턴이 작동하는 방식 및 시기에 대한 컨텍스트 정보를 특성화하는 데 사용됩니다.
인프라 유형	이 모듈에서는 가능한 인프라 분류를 나열합니다.
의도된 효과	이 애플리케이션은 위협 액터의 의도된 효과를 표현하는 데 사용됩니다.
맬웨어 역량	이 모듈에는 맬웨어의 가능한 기능이 나열되어 있습니다.
맬웨어 유형	이 모듈에는 가능한 맬웨어 분류가 나열되어 있습니다.
알림	이 모듈은 이메일 알림. 여기에는 전송 시기, 받은 사람 및 포함된 내용을 지정하는 것이 포함됩니다.
관찰 대상 유형	이 모듈에는 IP 주소 또는 파일 해시와 같은 옵저버블의 가능한 분류가 나열됩니다.
보고서 유형	이 모듈에는 위협 보고서의 가능한 분류가 나열되어 있습니다.
위협 액터 역할	이 모듈에는 위협 액터가 수행하는 역할이 나열됩니다.
위협 액터 유형	이 모듈에서는 사이버 공격 위협을 나타내는 악의적인 행위자(또는 공격자)를 특성화하며, 여기에는 추정된 의도와 역사적으로 관찰된 행동이 포함됩니다.
위협 조회 찾기 계산기	이 모듈은 받은 응답에 따라 결과를 계산합니다. 계산된 결과를 제공하는 타사 통합의 경우 위협 조회 찾기 계산기는 결과를 시스템에서 지원되는 결과에 매핑합니다. 자세한 내용은 위협 조회 찾기 계산기 문서를 참조하십시오.
도구 유형	이 모듈에서는 가능한 도구 분류를 나열합니다.

위협 조회 찾기 계산기

위협 조회 찾기 계산기를 사용하면 받은 응답에 따라 옵저버블 결과를 계산할 수 있습니다.

통합에 대한 위협 조회 찾기 계산기를 생성하고 스크립트를 사용하여 다양한 옵저버블 결과를 식별하는 방법을 결정할 수 있습니다. 위협 조회 찾기 계산기에는 기본 시스템과 함께 제공되는 샘플 스크립트가 포함되어 있으며, 이 스크립트를 사용하여 옵저버블 찾기를 식별하거나 요구 사항에 따라 이 스크립트를 수정할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

계산된 결과를 제공하는 외부 공급업체 통합의 경우 위협 조회 찾기 계산기는 결과를 기본 시스템에서 지원되는 결과에 매핑합니다.

위협 조회 결과 롤업

다양한 통합 벤더의 옵저버블에 대한 위협 조회 결과가 여러 개 있는 경우 모든 벤더의 최근 위협 조회 결과가 고려되고 전체 옵저버블 결과가 다음과 같이 표시됩니다.

위협 조회 결과 롤업

최신 옵저버블 찾기	전체 옵저버블 찾기
악성	통합 벤더 중 하나가 옵저버블을 악성으로 보고하면 전체 옵저버블 결과가 악성으로 표시됩니다.
의심스러움	통합 벤더 중 옵저버블을 악성으로 보고한 벤더가 없는 경우, 그 중 한 벤더가 이를 의심스러움으로 보고하면 전체 옵저버블 발견 사항이 의심스러움으로 표시됩니다.
정리	모든 통합 벤더가 옵저버블을 정상으로 보고하면 전체 옵저버블 결과가 정상으로 표시됩니다.
알 수 없음	통합 벤더 중 옵저버블을 악성 또는 의심스러움으로 보고한 벤더가 없고 그 중 하나가 알 수 없음으로 보고하는 경우, 전체 옵저버블 발견 사항은 알 수 없음으로 표시됩니다.

위협 조회 찾기 계산기 사용

위협 조회 찾기 계산기를 사용하여 통합에 대한 옵저버블 찾기를 계산합니다.

시작하기 전에
필요한 역할: sn_ti.admin

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 관리 〉 위협 조회 찾기 계산기.
2. 새로 만들기를 클릭합니다.
3. 양식에서 필드에 입력합니다.
4. 업데이트를 클릭합니다.

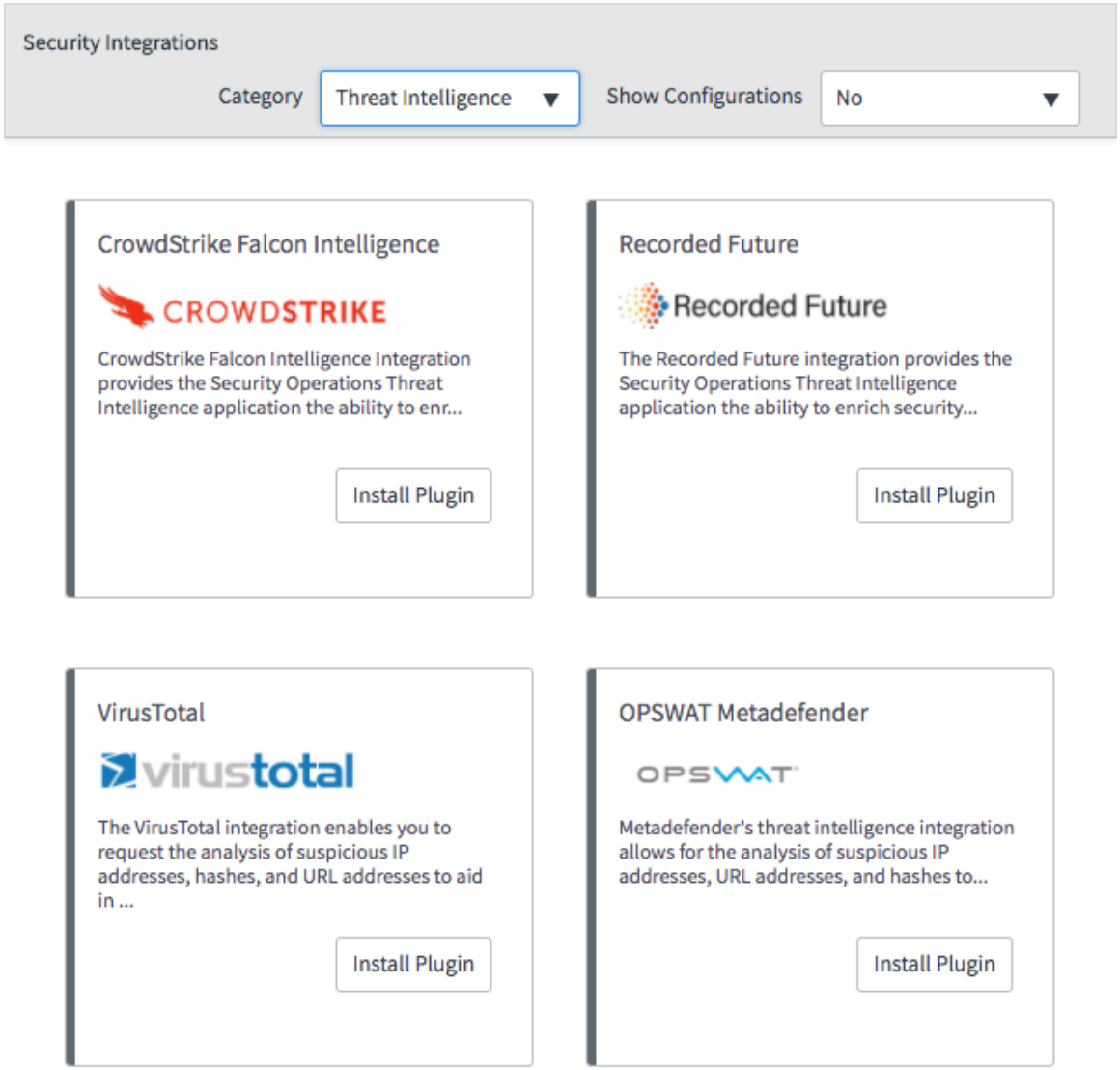
위협 인텔리전스 통합

기본 시스템에는 위협 인텔리전스 타사 맬웨어 탐지 소프트웨어 패키지에 대한 통합이 포함됩니다. 이 섹션에서는 플러그인을 활성화하고 타사 통합을 구성 ServiceNow 하기 위한 지침을 제공합니다. 또한 자체 통합을 개발하기 위한 몇 가지 기본 지침과 기본 시스템에 포함된 특정 통합에 대한 세부 정보가 포함되어 있습니다.

통합 구성

기본 시스템에는 활성화하고 사용할 수 있는 각 통합 구현에 대한 일련의 "카드"가 포함되어 있습니다. 또한 플러그인에 종속되어 보안 운영 있는 ServiceNow Store에 게시된 모든 통합에 대한 카드가 표시됩니다. 통합 카드는 선택하여 볼 수 있습니다. 보안 운영 〉 통합 구성.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



범주 드롭다운 메뉴를 사용하여 표시되는 통합을 필터링할 수 있습니다. **Show Configurations** 드롭다운 메뉴를 사용하면 생성을 허용하는 구현의 여러 인스턴스를 볼 수 있습니다.

통합 카드의 버튼

통합 카드는 통합의 현재 상태와 카드의 소스에 따라 서로 다른 버튼을 표시합니다.

단추	설명
플러그인 설치	통합을 활성화하려면 해당 플러그인을 설치하려면 이 버튼을 클릭하십시오. 플러그인이 설치되면 버튼이 구성으로 변경됩니다.
구성	통합 구성을 위한 정보를 입력하려면 이 버튼을 클릭합니다. 일부 통합의 경우 타사 통합 웹 사이트에서 가져온 API 키 또는 URL을 입력해야 할 수 있습니다.
신규	Carbon Black 및 IBM QRadar와 같은 특정 통합을 사용하면 동일한 통합의 여러 구현을 정의할 수 있습니다. 이러한 통합의 경우 플러그인이 활성화된 후 새로 만들기를 클릭합니다. 카드를 사용하면 플러그인을 설치하고(해당되는 경우) 사용할 구현을 구성할 수 있습니다.
페이지 열기	기본 시스템에서 인스턴스는 플러그인에 종속 보안 운영 된 애플리케이션에 대해 ServiceNow Store에 대한 쿼리를 수행합니다. 이러한 애플리케이션이 발견되고 연결된 애플리케이션 플러그인이 활성화되면 해당 애플리케이션에 대한 통합 카드가 다른 보안

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

단추	설명
	통합 카드와 함께 표시됩니다. 페이지 열기를 클릭하여 통합을 구성할 외부 공급업체 애플리케이션의 웹 사이트에 액세스합니다. 구성을 완료하면 페이지 열기 버튼이 구성으로 변경됩니다.

CrowdStrike Falcon Intelligence 통합

CrowdStrike Falcon 인텔리전스 보안 인시던트 및 관련 옵저버블에 대한 데이터를 보강합니다 위협 인텔리전스 .

탐색

- CrowdStrike Falcon 인텔리전스 통합 개요
- 보안 인시던트 응답 통합

설정

통합 활성화 및 구성 CrowdStrike Falcon 인텔리전스

사용

- 옵저버블에 대한 조회 수행
- 위협 조회 - CrowdStrike Falcon 인텔리전스 플로우

개발

- ServiceNow 보안 운영 통합 개발 가이드라인
- 통합 작성을 위한 팁
- 개발자 교육
- 개발자 설명서
- 애플리케이션과 함께 설치되는 구성요소 찾기

문제 해결 및 도움받기

- 통합 문제 해결
- 보안 운영 커뮤니티에서 질문 또는 답변하기
- 알려진 오류 포털에서 알려진 오류 문서 검색
- 연락처 고객 서비스 및 지원

CrowdStrike Falcon 인텔리전스 통합 개요

CrowdStrike Falcon 인텔리전스 쉽게 통합할 수 있는 사이버 보안 인텔리전스를 보안 운영제공합니다.

주:
통합을 구현하려면 플러그인이 위협 인텔리전스CrowdStrike Falcon 인텔리전스 필요합니다.

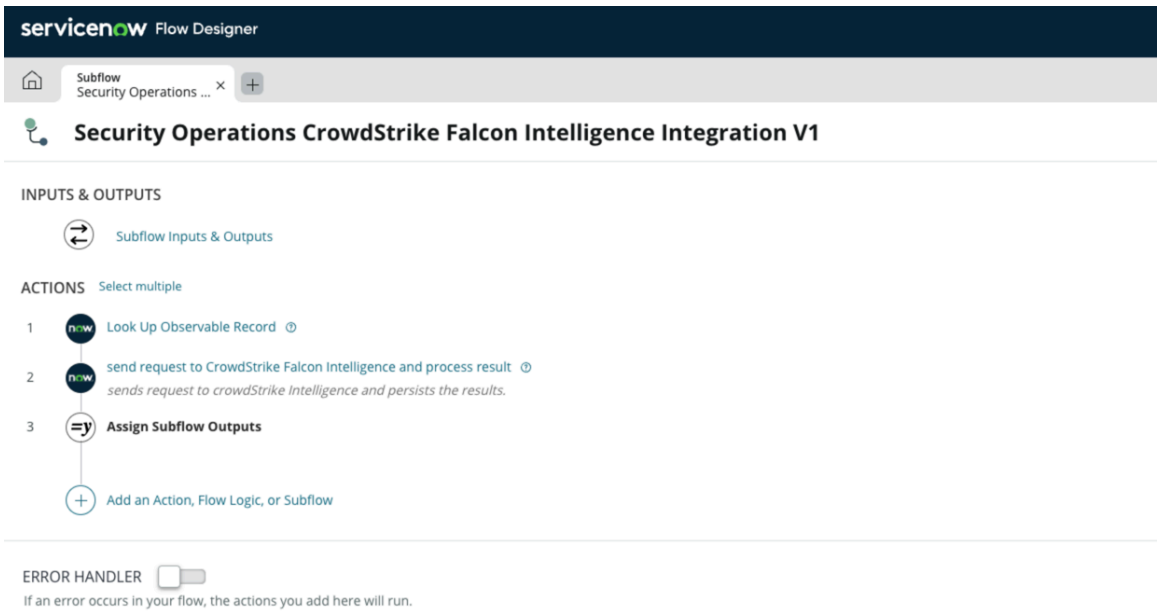
위협 조회 **- CrowdStrike Falcon** 인텔리전스 플로우

위협 조회 - CrowdStrike Falcon 인텔리전스 플로우 디자이너는 선택한 옵저버블에 대해 조회를 수행합니다. 옵저버블이 에서 인식 CrowdStrike Falcon 인텔리전스하는 유형인 경우 옵저버블에 맬웨어가 있는지 검사되고 결과가 반환됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 플로우는 하나 이상의 옵저버블을 감시 목록에 게시하고 CrowdStrike Falcon Intelligence 구현이 선택된 경우에 트리거 보안 운영 통합 - 위협 조회 기능 됩니다. 감시 목록이 게시된 후 CrowdStrike Falcon Host 소프트웨어에서 볼 수 있습니다.

필요한 역할: 관리자



이 플로우 디자이너가 사용하는 활동에 대한 자세한 내용은 다음 문서를 일반 Security Operations 통합 플로우 및 오케스트레이션 활동참조하십시오.

통합 활성화 및 구성 **CrowdStrike Falcon** 인텔리전스

통합 구성 기능을 사용하면 통합을 포함하여 외부 공급업체 보안 통합을 빠르게 활성화하고 설정할 수 있습니다 CrowdStrike Falcon 인텔리전스 . 를 CrowdStrike Falcon 인텔리전스사용하려면 먼저 에서 ServiceNow Store 다운로드하고 적절한 API 키와 ID를 추가해야 합니다.

시작하기 전에
필요한 역할: 관리자

- 위협 인텔리전스 통합을 사용하려면 CrowdStrike Falcon 인텔리전스 플러그인을 설치하고 활성화해야 합니다.
- 프로파일에서 CrowdStrike Falcon 인텔리전스 API 클라이언트 ID 및 API 클라이언트 비밀을 가져옵니다.
- 이전 버전에서 통합을 업그레이드하는 CrowdStrike Falcon 인텔리전스 경우 기존 구성을 삭제하고 새 구성을 설정해야 합니다. 통합은 OAUTH2 인증을 지원합니다. 이 업데이트를 수행하려면 **API** 클라이언트 **ID** 와 **API** 클라이언트 암호를 입력하여 인증하고 구성을 완료해야 합니다.
- CrowdStrike Falcon 인텔리전스 포털 **API** 범위에서표시기**(Falcon X)** 또는 IOC(침해 표시기)에 대한 읽기 설정을 활성화합니다.

프로시저

1. 에서 통합을 다운로드합니다. ServiceNow Store.
2. 인스턴스에서 다음으로 이동합니다. 보안 운영 〉 통합 〉 통합 구성.
   사용 가능한 보안 통합은 일련의 카드로 표시됩니다.
3. 카드에서 Configure(구성)를 CrowdStrike Falcon 인텔리전스 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 양식의 필드에 내용을 입력하여 구성을 완료합니다.

CrowdStrike Falcon 인텔리전스 구성

필드	설명
이름	통합의 이름입니다(예: `demo-1`).
API 클라이언트 **ID**	포털에서 계정 프로파일의 설정 섹션에서 얻은 클라이언트 ID입니다 CrowdStrike Falcon 인텔리전스 .
API 클라이언트 비밀	포털에서 계정 프로파일 CrowdStrike Falcon 인텔리전스 의 설정 섹션에서 가져온 클라이언트 비밀 키입니다.

5. 제출을 클릭합니다.

결과
구성된 CrowdStrike Falcon 인텔리전스 후에는 보안 인시던트의 옵저버블 위협 인텔리전스 과 옵저버블에 대한 조회를 수행하기 위해 선택할 수 있습니다.

관련 정보

옵저버블에 대한 조회 수행

Have I been pwned? 통합

통합을 보안 운영 Have I been pwned? 통해 도메인 이름 및 이메일 주소에 대한 조회를 제출하여 데이터 위반으로 인해 사용자 개인 데이터가 손상되었는지 여부를 확인할 수 있습니다.

탐색	설정
보안 인시던트 응답 통합	• Have I been pwned? 통합 설정 • 활성화
사용	**개발**
옵저버블에 대한 조회 수행 위협 조회 - Have I been pwned? 플로우	• ServiceNow 보안 운영 통합 개발 가이드라인 • 통합 작성을 위한 팁 • 개발자 교육 • 개발자 설명서 • 애플리케이션과 함께 설치되는 구성요소 찾기

문제 해결 및 도움받기

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 통합 문제 해결
- 보안 운영 커뮤니티에서 질문 또는 답변하기
- 알려진 오류 포털에서 알려진 오류 문서 검색

- 연락처 고객 서비스 및 지원

Have I been pwned? 통합 설정

Have I been pwned? 는 데이터 침해로 인해 온라인 계정이 손상되거나 "pwned"되어 누군가가 위험에 처했을 수 있는지 평가하는 데 사용되는 무료 리소스입니다. 와 쉽게 통합됩니다 보안 운영.

통합을 사용하려면 Have I been pwned? 먼저 플러그인을 활성화해야 합니다. 필요한 경우 X509 SSL 인증을 업데이트할 수도 있습니다.

통합을 보안 인시던트 응답구현하려면 , 위협 인텔리전스및 보안 운영 Have I been pwned? 플러그인이 보안 운영 Have I been pwned? 필요합니다.

위협 조회 **- Have I been pwned?** 플로우

위협 조회 - Have I been pwned? 플로우는 선택한 옵저버블에 대해 조회를 수행합니다. 옵저버블이에서 인식 Have I been pwned?하는 유형인 경우 옵저버블에 맬웨어가 있는지 검사되고 결과가 반환됩니다.

필요한 역할: sn_si_admin

이 플로우는 하나 이상의 옵저버블에 대해 위협 조회를 수행하고 구현이 선택될 때 트리거 보안 운영 통합 - 위협 조회 기능 됩니다 Have I been pwned? . 자세한 내용은 옵저버블에 대한 조회 수행 문서를 참조하십시오.

내가 **pwned** 흐름이었습니까?

이 플로우에서 사용하는 활동에 대한 자세한 내용은 다음 문서를 일반 Security Operations 통합 플로우 및 오케스트레이션 활동참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

활성화

통합 구성 기능을 사용하면 통합을 포함하여 외부 공급업체 보안 통합을 빠르게 활성화하고 설정할 수 있습니다 보안 운영 Have I been pwned? . 통합을 사용하려면 Have I been pwned? 먼저 다음 ServiceNow Store에서 다운로드해야 합니다.

시작하기 전에

- 위협 인텔리전스 통합을 사용하려면 보안 운영 Have I been pwned? 플러그인을 설치하고 활성화해야 합니다.

필요한 역할: sn_si_admin

프로시저

에서 통합을 다운로드합니다. ServiceNow Store.
이 통합은 개방형 API를 지원하며 추가 구성이 필요하지 않습니다. Have I been pwned? 이제 보안 인시던트의 옵저버블 위협 인텔리전스 과 옵저버블에 대한 조회를 수행하기 위해 선택할 수 있습니다.

관련 정보

옵저버블에 대한 조회 수행

X.509 인증서 업데이트

통합에 SSL 연결이 필요한 경우 외부 공급업체 벤더가 제공한 인증서를 아직 신뢰 ServiceNow 하지 않거나 만료된 경우가 있습니다. 이 작업은 선택 사항입니다.

시작하기 전에
필요한 역할: admin

프로시저

1. 외부 공급업체 벤더로부터 SSL 인증서를 받습니다.
   예를 들어, 다음과 같이 Firefox 브라우저의 SSL 엔드포인트에서 X.509 인증서(PEM)를 임포트할 수 있습니다.

   a. 브라우저 주소 표시줄에 엔드포인트 URL을 입력합니다.
      예: https://<3rdparty>/.

   b. 주소란에서 자물쇠 아이콘을 클릭합니다.

   c. 추가 정보를 클릭하고 보안 탭을 클릭합니다.

   d. **View** Certificate(인증서 보기)를 클릭하고 Detail(세부 정보) 탭을 클릭합니다.

   e. 내보내기를 클릭하여 PEM을 로컬 파일 시스템에 저장합니다.

   f. 저장된 파일을 텍스트 편집기 도구에서 열고 내용을 클립보드에 복사합니다.
      `-----BEGIN CERTIFICATE-----`로 시작하고 `-----END CERTIFICATE-----`로 끝나야 합니다.

2. 다음으로 이동 시스템 정의 〉 인증서.
3. 새로 만들기를 클릭하고 통합에 대한 새 기록을 생성합니다.
4. **PEM** 인증서에서 이전에 다운로드하여 클립보드에 복사한 인증서를 붙여넣습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. ID 제공자 기록에 인증서를 추가합니다.
   a. 다음으로 이동 복수 제공자 **SSO** 〉 **ID** 제공자.
   b. 새 인증서를 만들 활성 기본 ID 제공자를 선택합니다.
   c. 아래로 스크롤하여 **X.509** 인증서 관련 목록을 클릭하고 편집을 클릭합니다.
   d. 새로 만든 인증서를 선택됨 열로 이동합니다.
6. 저장을 클릭합니다.
   기록의 다른 필드는 자동으로 생성됩니다.

> **주:**
> 만료된 인증서가 있는 경우 인증서를 제거해야 합니다. 만료된 인증서를 제거하는 방법에 대한 자세한 내용은 KB0691439 만료되는 SAML 인증서 교체 를 참조하십시오.

MISP Integration for Security Operations

를 사용하면 MISP Integration for Security Operations사이팅 검색, 옵저버블 보강으로 보안 인시던트를 조사하고 에서 이벤트를 생성하거나 업데이트할 수 있습니다 MISP. 를 사용하면 MISP대상 공격을 더 빠르게 조사하고, 탐지 비율을 개선하고, 사용자 환경에서 가양성 수를 줄일 수 있습니다.

스토어에서 앱 요청

ServiceNow Store 웹 사이트를 방문하면 사용 가능한 모든 앱을 확인하고 스토어에 요청을 제출하는 방법에 대한 정보를 참조할 수 있습니다. 출시된 모든 앱의 누적 릴리스 정보는 ServiceNow Store 버전 기록 릴리스 정보 를 참조하십시오.

MISP 개요

MISP, 를 사용하면 Malware Information Sharing Platform신뢰할 수 있는 구성원 커뮤니티 내에서 표적 맬웨어 및 공격에 대한 위협 인텔리전스 및 IoC(침해 지표)를 교환하고 공유할 수 있습니다. 비공개 또는 공개 커뮤니티와 정보를 공유할 MISP 수도 있습니다. 정보를 교환 MISP 하면 대상 공격을 더 빠르게 조사하고, 탐지 비율을 높이고, 사용자 환경에서 가양성 수를 줄일 수 있습니다.

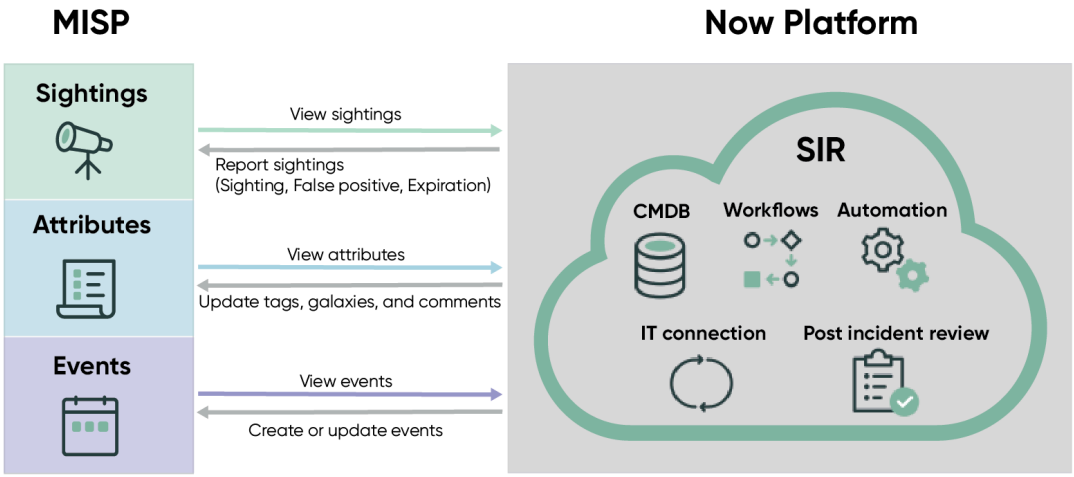
MISP 보안 운영

다음 예를 예로 들어 보안 운영 애플리케이션에서 정보가 이동하는 방식을 MISP 알아보십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

MISP 및 보안 운영 개요

Now Platform - MISP integration overview



주요 기능

이 통합에는 다음과 같은 주요 기능으로 수행할 수 있는 작업이 포함됩니다.MISP

- 비공개 및 공개에 연결 MISP 인스턴스.
- 옵저버블의 수동 및 자동 사이팅 검색 지원
- 케이스 관리에서 사이팅 검색을 실행합니다.
- 속성으로 사이팅을 보고하거나 업데이트합니다.
  - 옵저버블을 사이팅으로 보고(전역)
  - 옵저버블을 긍정 오류로 보고(전역)
  - 옵저버블을 만료로 보고
- 수동 및 자동 옵저버블 보강 지원 결과에는 MISP 옵저버블과 연결된 속성 및 이벤트 정보가 포함됩니다.
- 태그, 갤럭시, 주석의 MISP 추가 또는 업데이트를 포함한 속성 보강
- 에서 이벤트 생성 MISP 보낸 사람 SIR: 에서 SIR이벤트의 MISP 수동 및 자동 생성을 지원합니다.
- MISP태그, 갤럭시, 속성 추가 또는 업데이트를 포함하는 이벤트를 SIR 업데이트합니다.
- 보안 인시던트 관련 옵저버블을 속성에 대한 속성으로 추가 MISP 이벤트.
- 자동 추출 MITRE-ATT&CK™ 정보 출처 MISP 속성 정보를 보안 인시던트에 SIR 연결합니다.
- 자동으로 추가 SIR MITRE-ATT&CK™ 정보를 은하로 MISP 이벤트.

핵심 개념

이 통합에는 알아야 할 다음과 같은 주요 개념이 포함됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- MISP 는 위협 인텔리전스 플랫폼(TIP)입니다. TIP를 사용하여 보안 위협 데이터를 실시간으로 수집, 상관 관계, 분류, 공유 및 통합하여 작업의 우선 순위 지정을 지원하고 공격 방지, 탐지 및 대응을 지원합니다.
- MISP 은 Threat Intelligence Management(TIM)입니다. TIM을 사용하면 컨텍스트를 통해 위협 데이터를 위협 인텔리전스로 전환하고 사용자 정의 점수 매기기 및 관련성에 따라 위협의 우선순위를 자동으로 지정할 수 있습니다.
- MISP 데이터 계층
  - 이벤트는 상황에 맞게 연결된 정보를 캡슐화한 것입니다.
  - 속성은 개별 데이터 요소로, 표시기 또는 지원 데이터일 수 있습니다.
  - 객체는 사용자 지정 템플릿 속성 컴퍼지션입니다.
  - 객체 참조는 다른 구성 요소 간의 관계입니다.
  - 목격은 탐지된 데이터 포인트의 시간별 발생입니다.
- MISP 컨텍스트 계층
  - 태그는 이벤트 또는 속성에 첨부된 레이블이며 분류에서 가져올 수 있습니다.
  - 은하군은 은하에서 온 사건이나 속성에 라벨을 붙이는 데 사용할 수 있는 지식베이스 항목이다.
  - 클러스터 관계는 클러스터 간에 미리 정의된 관계를 나타냅니다.
- 표시기에는 의심스럽거나 악의적인 사이버 활동을 탐지하는 데 사용할 수 있는 패턴이 포함되어 있습니다.
- 의 MISP 속성은 네트워크 표시기(IP 주소), 시스템 표시기(메모리의 문자열) 또는 은행 계좌 정보일 수 있습니다. 의 MISP 속성은 다른 SIEM 또는 와 같은 STIX형식의 옵저버블로 알려져 있습니다.
  - 유형은 속성을 설명합니다. 예: MD5 또는 URL
  - 속성 범주는 속성을 설명합니다. 페이로드 배달을 예로 들 수 있습니다.
  - IDS 태그는 속성이 감지에 자동으로 사용될 수 있는지 여부를 결정합니다.

주:
개념에 대한 MISP 자세한 내용은 MISP 설명서 웹 사이트를 참조하십시오

조직의 이점 **MISP Integration for Security Operations**

보안 분석가는 위협 환경에 대한 상황 인식을 확보하고 유지 관리해야 하며, 이는 압도적인 양의 위협 데이터를 수동으로 통합하고 통합해야 함을 의미합니다. 이 데이터를 수집, 통합 및 통합하는 데 귀중한 시간이 소요되므로 위협 탐지 및 분석이 느려집니다. MISP Integration for Security Operations 분석가가 보안 인텔리전스를 MISP 기존 ServiceNow AI Platform 인스턴스에 통합하여 더 많은 위협을 탐지하고 신속하게 대응할 수 있습니다.

를 사용하여 MISP Integration for Security Operations조직은 다음 작업을 수행할 수 있습니다.

- 보안 분석가가 올바른 컨텍스트로 신속하게 대응할 수 있도록 합니다.
- 위협을 탐지하고 억제하기 위한 인시던트 플로우를 자동화하여 보안 팀의 효율성을 개선합니다.
- 수동 조사 시간을 줄이고 보안 분석가가 .ServiceNow AI Platform

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 통합에 대해 알아보기

문서 식별자	문서 제목
MISP 설명서 웹 사이트	MISP 설명서 웹 사이트
ServiceNow 제품 설명서 웹 사이트	ServiceNow 제품 설명서 웹 사이트

MISP 관리

에서 통합을 설정하여 MISP 사이팅 검색, 옵저버블 보강을 수행하고 에서 이벤트를 생성 및 업데이트할 수 있습니다MISP.ServiceNow AI Platform

MISP Integration for Security Operations 시작하기

설정하기 MISP Integration for Security Operations전에 다음 정보를 검토합니다.

검사 목록

설정 작업	설명
필수 ServiceNow AI Platform, 위협 인텔리전스및 보안 인시던트 응답 역할을 할당했는지 확인합니다.	의 기능에서 MISP 사용되는 역할은 다음과 같습니다.ServiceNow AI Platform • 관리자(admin)는 에서 ServiceNow Store 애플리케이션을 설치하고 보안 인시던트 관리자(sn_si.admin) 및 위협 인텔리전스 관리자(sn_ti.admin) 역할을 할당합니다. • sn_si.admin 및 sn_ti.admin은 통합을 구성하고 자동 MISP 이벤트 생성 프로파일을 설정할 수 있습니다. • sn_sec_misp.write - 분석가 역할에는 MISP 이벤트 및 속성 데이터를 포함하는 데이터에 대한 MISP 읽기 및 쓰기 권한이 있습니다. 자세한 내용은 Threat Intelligence 설정을 참조하십시오.
필요한 MISP 사용자 역할을 할당합니다.	다음 항목 검토: MISP 사용하는 데 필요한 사용자 역할 및 권한 MISP Integration for Security Operations. 주: 의 MISP사용자 역할에 대한 자세한 내용은 MISP 설명서 웹 사이트의 역할 섹션을 참조하십시오.
버전 2.4.137 이상을 사용하고 MISP 있는지 확인합니다.	최소 MISP Integration for Security Operations 한으로 테스트됩니다. MISP 버전 2.4.137.
ServiceNow 모듈을 지원하는 MISP 데 필요한 핵심 애플리케이션이 설치되고 활성화되었는지 확인합니다.	에서 ServiceNow Store다음 보안 운영 애플리케이션이 설치되고 활성화되는지 확인합니다. 설치되지 않은 경우 원활한 설치를 위해 다음 순서로 한 번에 하나의 애플리케이션을 설치하고 활성화합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

검사 목록

설정 작업	설명
	• 보안 인시던트 응답 • ServiceNow 통합 허브 런타임 (com.glide.hub.integration.runtime) • ServiceNow IntegrationHub Action Step - REST (com.glide.hub.action_step.rest) 통합을 위한 인스턴스 설정에 ServiceNow AI Platform 대한 자세한 내용은 보안 운영 제품 또는 애플리케이션에 대한 권리 가져오기 및 ServiceNow Store 애플리케이션 활성화를 참조하십시오.
도메인 분리	데이터, 프로세스 및 관리 작업을 분리하려면 도메인 분리 섹션을 확인합니다.

MISP 사용자 역할 및 권한

통합에 MISP Integration for Security Operations 필요한 사용자 역할을 검토합니다.

옵저버블 보강 및 사이팅 검색 권한

주:

- 모든 **ServiceNow *MISP*** 통합 기능에는 조직 이벤트 및 인증 키 액세스를 관리할 수 있는 기본 권한이 필요합니다. 계속하기 전에 이러한 기본 권한이 있는지 확인합니다.
- 로컬 갤럭시를 추가하려면 통합을 구성하는 사용자가 해당 ***MISP*** 서버의 호스트 조직에 속해야 합니다.

MISP 역량	술래	태그 편집기
옵저버블 보강(읽기 전용)	✓	✓
사이팅 검색(읽기 전용)	✓	✓

사이팅 권한 보고

MISP 역량	사이팅 크리에이터
사이팅 보고	✓

속성 및 이벤트 권한

MISP 역량	술래	태그 편집기
이벤트/속성 태그 편집	✓	✓
이벤트/속성 갤럭시 편집	✓	✓

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성 및 이벤트 권한

MISP 역량	술래	태그 편집기
속성 의견 편집	✓	✓
이벤트에 새 속성 추가	✓	✓
MISP에서 이벤트 작성	✓	✓

설치 및 구성 **MISP Integration for Security Operations**

데이터를 사용하여 MISP 보안 인시던트 조사를 시작할 수 있도록 인스턴스에 를 ServiceNow AI PlatformMISP Integration for Security OperationsServiceNow Store 설치하고 구성합니다.

시작하기 전에

MISP 서버에 유효한 SSL 인증서를 설치했는지 확인하십시오.

필요한 역할: sn_si.admin

프로시저

1. MISP Integration for Security Operations 에서 ServiceNow Store 다운로드하여 설치하십시오.
2. 다음으로 이동 보안 운영 〉 통합 〉 통합 구성.
3. -SIR/TI 통합 타일을 MISP 검색하고 구성을 클릭합니다.
4. 양식에서 필드를 채웁니다.

MISP - SIR/TI 통합 구성 양식

필드	설명
이름	MISP 인스턴스 구성의 이름입니다.
MISP 서버 URL	MISP 서버의 REST 엔드포인트 역할을 하는 서버의 URL입니다MISP.
API 키	서버의 사용자 계정에 MISP 대해 구성된 API 키입니다. API 키는 서버의 **Authkey**MISP 에 해당합니다.
직접 배포	서버가 온 프레미스 인스턴스에 배포되는 경우 MISP 선택할 수 있는 옵션입니다. 온-프레미스 배포 옵션을 선택하는 경우 를 MID 서버 사용하여 서버에 연결해야 MISP 합니다.
MID 애플리케이션	와 통신하는 데 사용되는 MID 애플리케이션 이름을 식별하는 문자열 필드입니다 MISP. 이 필드는 직접 배포 옵션을 선택하는 경우에 필요합니다. 애플리케이션에 대해 MID 서버를 구성하는 방법에 대한 자세한 내용은 각 애플리케이션에 대해 MID 서버 구성을 참조하십시오.

5. 제출을 클릭합니다.

결과

구성을 성공적으로 확인하고 제출하면 SIR/TI 통합이 MISP 보안 통합 페이지에 타일로 저장됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

MISP 통합 설정 검토

MISP Integration for Security Operations 설정을 검토하고 환경에 맞게 기본 시스템 속성을 수정합니다.

시작하기 전에
필요한 역할: sn_si.admin, sn_ti.admin

프로시저

1. 다음으로 이동 모두 〉 **MISP** 통합 〉 통합 설정.
2. 필요에 따라 다음 설정을 수정합니다.

MISP 통합 설정

속성 이름		설명
관찰 대상 보강	새 데이터를 가져오기 전 시간(시간)	새 데이터를 가져올 수 있을 때까지 걸리는 시간(시간)입니다. 유형: 정수 기본값: 24
검색 찾기	새 옵저버블이 보안 인시던트와 연결된 경우 Sighting 검색 자동 실행	새 옵저버블이 보안 인시던트와 연결될 때마다 실행되는 사이팅 검색입니다. 기본값: 예
	MISP에서 사이팅 검색을 위한 검색 간격(일)	에서 사이팅 검색 데이터가 검색되는 MISP일 수입니다. 이 옵션은 자동 사이팅 검색 기능에만 사용합니다. 기본값: 90
데이터 동기화	태그를 가져오고 MISP와 동기화할 간격 기간(분)	MISP 통합 구성 시 가져오는 태그입니다. 데이터가 에 ServiceNow AI Platform있으면 이 속성은 서버와 데이터가 MISP 동기화되는 빈도를 정의합니다. 값은 분 단위로 정의됩니다. 기본값: 1440(분 또는 24시간)
	구성된 소스에서 MISP Galaxies를 새로 고치는 간격 기간(분)	MISP 통합 구성 시 가져온 갤럭시입니다. 데이터가 에 ServiceNow AI Platform있으면 이 속성은 서버와 데이터가 MISP 동기화되는 빈도를 정의합니다. 값은 분 단위로 정의됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성 이름		설명
		기본값: 1440(분 또는 24시간)
	조직을 가져오고 MISP와 동기화할 간격 기간(분)	MISP 통합 구성 시 가져온 조직입니다. 데이터가 에 ServiceNow AI Platform있으면 이 속성은 서버와 데이터가 MISP 동기화되는 빈도를 정의합니다. 값은 분 단위로 정의됩니다. 기본값: 1440(분 또는 24시간)
MITRE™ 기술 추출	MISP 옵저버블 보강 결과(태그)에서 보안 인시던트까지 기술을 자동으로 롤업 MITRE-ATT&CK	옵저버블 보강 결과(태그)에서 MISP 보안 인시던트로 정보를 롤업 MITRE-ATT&CK 합니다. 기본값: 예
	MISP 옵저버블 보강 결과(갤럭시)에서 보안 인시던트까지 기술을 자동으로 롤업 MITRE-ATT&CK	옵저버블 보강 결과(갤럭시)에서 MISP 보안 인시던트로 정보를 롤업 MITRE-ATT&CK 합니다. 기본값: 예

주:

- 의 기술 추출 기능을 MISP사용하려면 MITRE™ 다음을 수행해야 합니다. 활성화 MITRE-ATT&CK 기능의 위협 인텔리전스 모듈.
- 은 MISP Integration for Security Operations 하와 MISP 태그에 대한 MISPMISP 두 가지 기본 시스템 MITRE-ATT&CK 기술 추출 규칙을 소개합니다. 의 MITRE-ATT&CK자동 추출 규칙에 대한 자세한 내용은 MITRE-ATT&CK 정보를 가져오기 위한 자동 추출 기술 규칙을 참조하십시오.

3. 저장을 클릭합니다.

결과
수정된 통합 설정이 저장되고 적용됩니다.

사이팅 검색 구성 **MISP**

ServiceNow AI Platform 인스턴스에서 옵저버블에 대한 사이팅 검색을 수행하도록 MISP 구성합니다. 이 정보를 사용하여 위협이 발생하는 빈도를 확인할 수 있습니다.

시작하기 전에

- 다음 항목 검토: MISP 사용자 역할 및 권한 양방향 기능을 사용하는 MISP 데 필요합니다.
- 필요한 역할: sn_si.admin, sn_ti.admin

이 태스크 정보

Security Operations Integration - 사이팅 검색 워크플로우는 사이팅 검색을 실행합니다. 이 워크플로우는 옵저버블 목록을 수락하고, 구현 역량을 찾고, 사이팅 검색 구성을 기반으로 쿼리를 만들고, 구성된 워크플로우를 기반으로 검색을 실행합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

자동 MISP Integration for Security Operations 사이팅 검색을 구성할 수 있는 기본 시스템 사이팅 검색 프로파일을 제공합니다. 이 프로파일을 사용하면 조직의 관련 옵저버블 사이팅 정보에 액세스하고 다른 조직의 외부 사이팅도 볼 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 **MISP** 통합 〉 사이팅 검색 구성.
2. 새로 만들기를 클릭합니다.
3. 양식에서 필드를 채웁니다.

사이팅 검색 구성 양식

필드	설명
이름	역량 프로파일의 이름입니다.
저장된 검색 여부	이 옵션을 선택할 때 저장되는 검색 구성입니다. 저장된 검색 구성 쿼리는 예제 쿼리입니다. 환경에 대한 매개변수로 대체하고 필요에 따라 저장된 검색 구성을 추가로 생성할 수 있습니다.
관찰 검색 소스	사이팅 검색을 위한 소스입니다. MISP 로그 저장소를 소스로 선택합니다.
활성	저장된 검색 구성을 활성화하는 옵션입니다. 활성 검색 구성만 사이팅 검색을 수행할 수 있습니다.
옵저버블 유형	IP 주소, 해시 값, URL 및 도메인 이름과 같은 옵저버블 유형입니다.
검색당 최대 옵저버블	검색 쿼리에서 볼 수 있는 최대 옵저버블 수입니다.
검색	기본 검색 문자열은 `$(observable)`입니다. 그러나 로그 저장소에서 지원되는 매개변수를 지정하여 사용자 고유의 MISP 검색 쿼리를 정의합니다.

4. 제출을 클릭합니다.

결과
사이팅 검색 구성 프로파일을 생성했습니다 MISP .

자동 이벤트 생성 방법 구성

에서 MISP이벤트를 자동으로 작성하도록 구성합니다ServiceNow AI Platform.

시작하기 전에

- 다음 항목 검토: MISP 사용자 역할 및 권한 양방향 기능을 사용하는 MISP 데 필요합니다.
- 필요한 역할: sn_si.admin, sn_ti.admin

프로시저

1. 다음으로 이동 모두 〉 **MISP** 통합 〉 자동 이벤트 작성 프로파일.
2. 새로 만들기를 클릭합니다.
3. 양식에서 필드를 채웁니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이름 양식

필드	설명
이름	자동 이벤트 생성 프로파일의 이름입니다.
설명	프로파일에 대한 간략한 설명입니다. 더 자세한 설명은 이벤트 생성의 다음 단계에서 속성을 통해 공유됩니다.
순서	트리거 조건이 충족될 때 프로파일의 순서입니다. 기본값은 100입니다. 이 설정을 기본값으로 둡니다. 여러 프로필을 만드는 경우 둘 이상의 프로필이 트리거 조건을 공유할 때 이 값은 런타임 실행 우선 순위를 제공합니다. 가장 낮은 번호의 프로파일이 가장 높은 우선순위를 갖습니다.
소스	MISP 이벤트 생성 소스입니다.
활성	프로파일의 활성 또는 비활성 여부를 나타내는 옵션입니다. 이 옵션은 기본적으로 선택이 취소되어 프로파일이 꺼져 있음을 나타냅니다. 이 프로파일은 모든 프로파일 구성 단계를 완료하고 마침을 클릭할 때까지 활성화되지 않습니다.

4. 계속을 클릭합니다.

이벤트 트리거 조건 구성

조건이 충족될 때 이벤트를 MISP 자동으로 트리거할 수 있도록 에서 ServiceNow AI Platform 이벤트 트리거 조건을 구성합니다.

시작하기 전에
필요한 역할: sn_sec_misp.write

프로시저

1. 트리거 조건 양식에서 이벤트를 트리거할 수 있는 세부 정보를 입력합니다.
보안 인시던트 필드 또는 옵저버블 필드를 기반으로 하는 트리거 조건을 제공하여 복합 논리를 빌드할 수 있습니다. 옵저버블에 해당하는 이벤트가 MISP없는 경우 에서 MISP 이벤트를 생성할 수도 있습니다. 세 가지 트리거 조건(보안 인시던트 필드를 기반으로 트리거, 옵저버블 필드를 기반으로 트리거, 옵저버블에 MISP에 해당 이벤트가 없는 경우)을 조합하여 복합 논리를 빌드하도록 선택할 수 있습니다. 트리거를 여러 개 선택하는 경우 AND 조건을 사용하여 조인할 수 있습니다. OR 조건을 사용해야 하는 경우 새 조건으로 프로파일을 만드는 것이 좋습니다.

이벤트 트리거 조건 양식

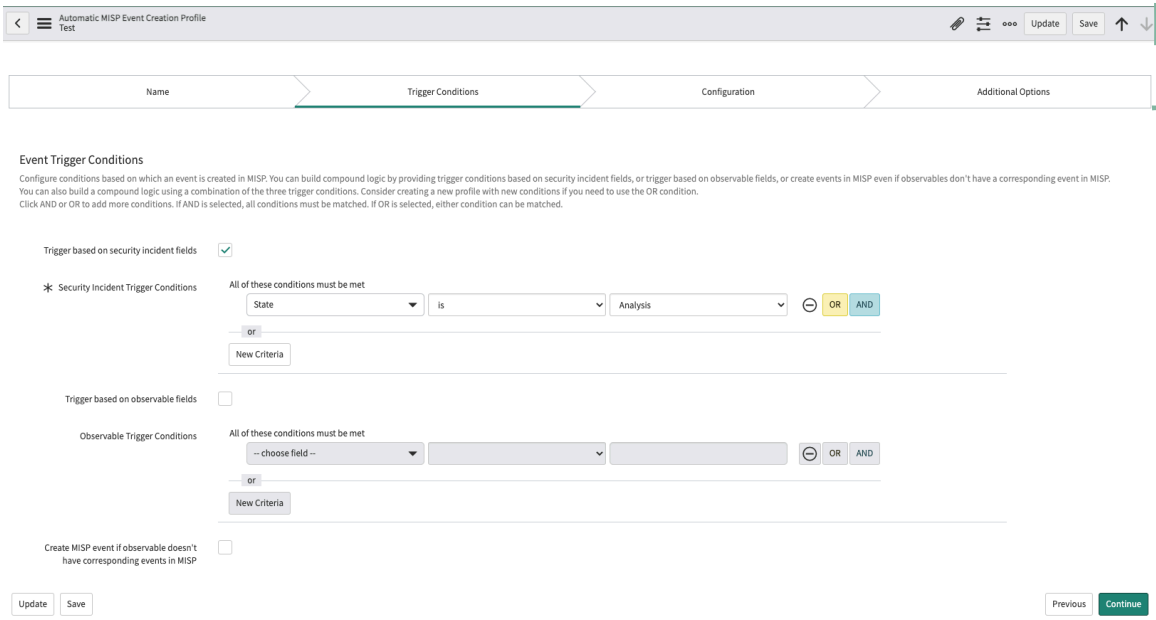
필드	설명
보안 인시던트 필드를 기반으로 트리거	MISP 모든 보안 인시던트 트리거 조건이 충족될 경우 생성할 수 있는 이벤트입니다.
보안 인시던트 트리거 조건	조건 작성기의 목록과 필드를 사용하여 설정할 수 있는 첫 번째 행의 필터입니다. 조건을

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	더 추가하려면 AND 또는 OR을 클릭합니다. AND를 선택하면 모든 조건이 일치해야 합니다. OR을 선택하면 두 조건을 일치시킬 수 있습니다. 두 번째 필터 조건을 설정하려면 새 기준을 클릭합니다.
옵저버블 필드를 기반으로 트리거	MISP 모든 옵저버블 트리거 조건이 충족될 경우 생성할 수 있는 이벤트입니다.
옵저버블 트리거 조건	조건 작성기의 목록과 필드를 사용하여 설정할 수 있는 첫 번째 행의 필터입니다. 조건을 더 추가하려면 AND 또는 OR을 클릭합니다. AND를 선택하면 모든 조건이 일치해야 합니다. OR을 선택하면 두 조건을 일치시킬 수 있습니다. 두 번째 필터 조건을 설정하려면 새 기준을 클릭합니다.
옵저버블에 MISP 상의 해당 이벤트가 없는 경우 MISP 이벤트 작성	MISP 옵저버블에 해당하는 이벤트가 MISP없는 경우 생성할 수 있는 이벤트입니다.

이벤트 트리거 조건

다음 예제에서는 이벤트 생성 프로파일을 설정할 MISP 때의 이벤트 트리거 조건을 보여줍니다.



2. 계속을 클릭합니다.

MISP 이벤트 필드 매핑

MISP 이벤트가 생성될 때 MISP 보안 인시던트 정보를 사용할 수 있도록 의 ServiceNow AI Platform 이벤트 필드를 매핑합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_sec_misp.write

프로시저

1. 양식에서 필드를 채웁니다.

기본 **MISP** 이벤트 필드 매핑 양식

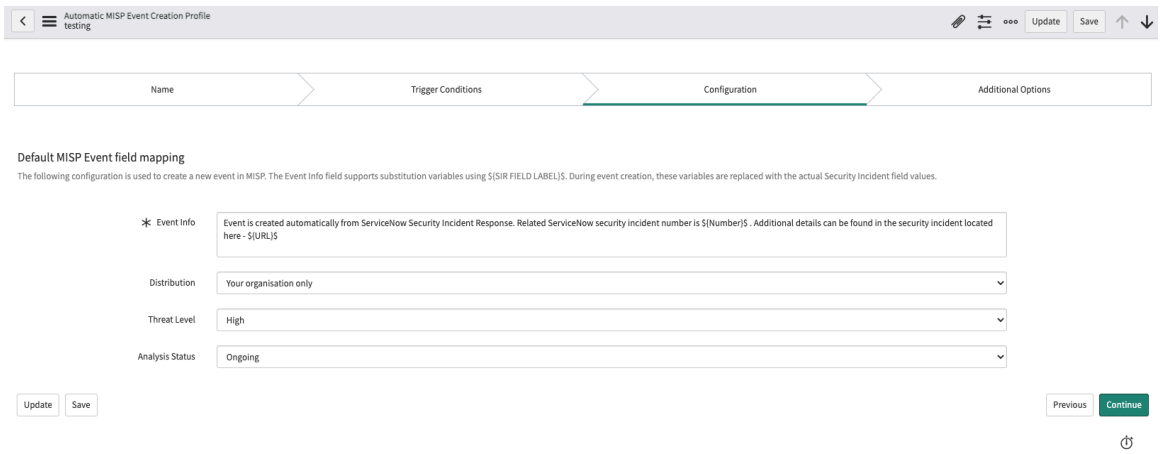
필드	설명
이벤트 정보	에서 자동으로 생성되는 이벤트 정보입니다 ServiceNow AI Platform 보안 인시던트 응답. 이벤트 정보 필드는 ${SIR FIELD LABEL}$을 사용하여 대체 변수를 지원합니다. 이벤트를 생성하는 동안 이러한 변수는 실제 보안 인시던트 필드 값으로 대체됩니다. ${URL}$ 대체 변수는 보안 인시던트의 URL로 대체됩니다.
배포	이벤트가 게시된 후 이 이벤트를 볼 수 있는 사용자를 제어하는 옵션입니다. 이 옵션은 이벤트를 다른 서버와 동기화할지 여부도 제어합니다. 분포는 속성에 상속되며 가장 제한적인 설정이 우선합니다. 배포 옵션은 다음과 같습니다. ○ 내 조직만: 조직의 구성원만 이 이벤트를 볼 수 있습니다. 조직 구성원 중 한 명이 이벤트를 다른 인스턴스로 끌어올 수 있으며, 해당 인스턴스에서는 조직만 해당 이벤트를 볼 수 있는 접근 권한이 있습니다. 이 설정의 이벤트는 동기화되지 않습니다. ○ 이 커뮤니티만: 자신의 조직, 이 MISP 서버의 조직 및 이 서버와 동기화되는 서버를 실행하는 MISP 조직을 포함하여 커뮤니티에 MISP 속한 사용자가 이벤트를 볼 수 있도록 합니다. 연결된 서버에 연결하는 다른 조직에서는 이벤트를 볼 수 없습니다. ○ 연결된 커뮤니티: 커뮤니티의 일부인 MISP 사용자가 이 MISP 서버의 모든 조직, 이 서버와 동기화되는 서버의 모든 조직 MISP 및 두 홉 떨어져 있는 모든 서버에 연결하는 서버의 호스팅 조직을 포함하여 이벤트를 볼 수 있도록 합니다. 2홉 떨어져 있는 연결된 서버에 연결된 다른 조직은 이벤트를 볼 수 없도록 제한됩니다. ○ 모든 커뮤니티: 이벤트를 모든 MISP 커뮤니티와 공유합니다.
위협 수준	이벤트의 위험 수준을 나타내는 필드입니다. 인시던트를 세 가지 위협 범주(낮음, 중간, 높음)로 분류할 수 있습니다. 이 필드는 정의되지 않은 상태로 둘 수도 있습니다. 옵션은 다음과 같습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	○ 낮음: 일반 대량 맬웨어 ○ 중간: 지능형 지속 위협(APT) ○ 높음: 정교한 APT 및 0일 공격
분석 상태	다음과 같은 가능한 옵션이 있는 이벤트 분석의 현재 스테이지입니다. ○ 초기: 분석이 이제 막 시작되었습니다. ○ 진행 중: 분석이 진행 중입니다. ○ 완료됨: 분석이 완료되었습니다.

다음 예는 MISP에서 이벤트를 작성하는 데 사용할 수 있는 양식을 보여줍니다.

기본 **MISP** 이벤트 필드 매핑



2. 계속을 클릭합니다.

옵저버블을 이벤트에 대한 속성 **MISP** 으로 매핑 또는 연결 **SIR**

보안 인시던트 응답 속성 유형과 SIR 옵저버블이 MISP 다를 수 있으므로 옵저버블 유형을 MISP 속성 유형에 매핑합니다.

시작하기 전에
필요한 역할: sn_sec_misp.write

이 태스크 정보
는 MISP Integration for Security Operations 옵저버블을 이벤트에 속성 MISP 으로 추가할 SIR 때 사용하는 기본 시스템 매핑을 제공합니다.

사용자 환경에 맞게 기본 시스템 매핑을 수정하도록 선택할 수 있습니다. 예를 들어 여러 SIR 옵저버블을 하나의 MISP 속성 유형에만 매핑할 수 있습니다. 옵저버블 유형이 매핑되지 않은 경우 기본적으로 다른 MISP 속성 유형이 선택됩니다.

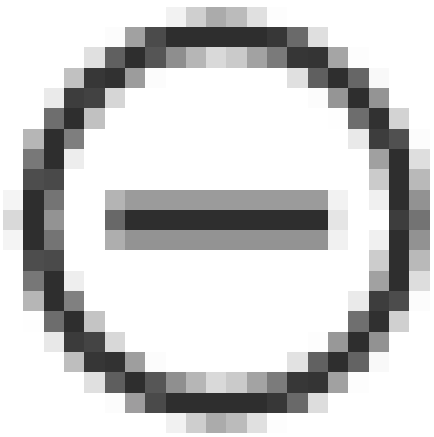
프로시저

1. 추가 옵션 양식에서 옵저버블 및 MISP 속성 유형을 매핑합니다SIR.

2. 보안 인시던트 응답 다음 표에 설명된 대로 옵저버블 유형을 MISP 속성 유형에 매핑합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

SIR 옵저버블 및 **MISP** 속성 유형 매핑

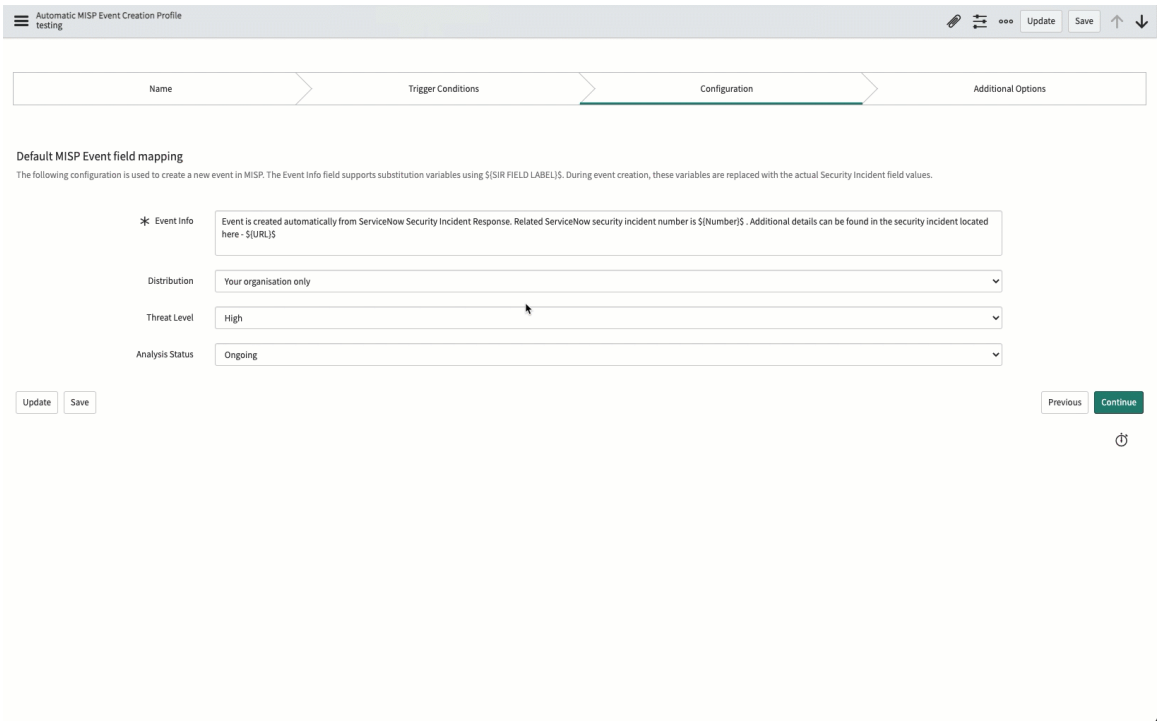
필드	설명
연결된 모든 옵저버블을 속성으로 추가	보안 인시던트 MISP 에서 사용 가능한 옵저버블을 이벤트에 속성으로 추가하기 위해 활성화하는 옵션입니다. 이 옵션은 옵저버블 유형-속성 유형 매핑 섹션에서 매핑을 활성화합니다.
옵저버블 유형-속성 유형 매핑	옵저버블 유형을 속성 유형에 매핑 SIR 하는 MISP 옵션입니다. 예를 들어 의 SIR CVE 번호를 의 MISP취약성 속성에 매핑할 수 있습니다. 옵저버블 유형은 하나의 MISP 속성 유형에만 추가할 SIR 수 있습니다. 기본 시스템은 옵저버블 유형을 속성 유형에 매핑 SIRMISP 하는 기능을 제공합니다. SIR 옵저버블 유형이 속성 유형에 매핑 MISP 되지 않은 경우 옵저버블은 의 다른 속성 유형에 MISP매핑됩니다. 새 매핑을 추가하려면 옵저버블 유형 추가를 클릭하고 옵저버블 유형을 검색 SIR 한 다음 해당 MISP 속성 유형에 매핑합니다. 매핑 제거 아이콘을  클릭합니다 AND MISP 속성 매핑 연결을 제거합니다SIR. **주:** 속성 유형에 대한 MISP 자세한 내용은 MISP 설명서를 참조하십시오.
보안 태그를 기준으로 옵저버블 필터링	선택한 보안 태그를 기준으로 옵저버블을 필터링하는 옵션입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	보안 태그: 옵저버블을 필터링하는 태그를 추가합니다. 예를 들어 "공유 차단" 또는 "TLP: 흰색"이라는 태그를 추가하는 경우 옵저버블 중 하나에 이러한 태그가 연결되어 있으면 MISP 이벤트 작성 중에 이러한 옵저버블이 MISP 이벤트에 속성으로 추가되지 않습니다.
옵저버블 찾기가 악성일 때 속성 IDS 플래그 설정	에서 옵저버블이 악성 SIR으로 표시된 경우 의 MISP 해당 속성에 IDS 플래그가 활성화되어 있음을 알 수 있는 옵션입니다. IDS 플래그가 설정되지 않은 경우, 속성은 상황별 정보로 간주되며 자동 침입 탐지에 사용되지 않습니다.

다음 예시에서는 추가 옵션 페이지로 이동하는 방법을 보여줍니다. 이 페이지에서 SIR 옵저버블 및 MISP 속성 유형 매핑을 활성화하고, IPV6 네트워크 및 IPV4 네트워크와 같은 새 SIR 옵저버블 유형을 추가하고, 속성 유형 도메인 IP 주소에 매핑 MISP 할 수 있습니다.

옵저버블 및 **MISP** 속성 유형 매핑 **SIR**



정보를 이벤트와 **MISP** 동기화 **MITRE-ATT&CK**

더 나은 보안 인시던트 및 위협 분석을 위해 정보를 속성과 MISP 동기화 MITRE-ATT&CK 합니다.

시작하기 전에
필요한 역할: sn_sec_misp.write

프로시저

추가 옵션 양식에서 정보를 속성과 MISP 동기화 MITRE-ATT&CK 하는 옵션을 검토합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

고급 옵션 양식

필드	설명
보안 인시던트 MITRE-ATT&CK™ 기술을 이벤트에 로컬 갤럭시 MISP 로 동기화	보안 인시던트 MITRE-ATT&CK™ 기술을 이벤트의 로컬 갤럭시로 동기화 ServiceNow AI Platform SIR 하는 MISP 옵션입니다. 주: 로컬 갤럭시를 추가하려면 통합을 구성한 사용자가 해당 MISP 서버의 호스트 조직에 속해야 합니다.
보안 인시던트 MITRE-ATT&CK™ 기술을 글로벌 갤럭시 MISP 로 이벤트에 동기화	보안 인시던트 MITRE-ATT&CK™ 기술을 이벤트의 전역 갤럭시로 동기화 ServiceNow AI Platform SIR 하는 MISP 옵션입니다.

결과
에서 이벤트를 MISPServiceNow AI Platform자동으로 만들 수 있는 프로파일을 만들었습니다. 이제 연결된 MISP 이벤트 관련 목록에서 이벤트를 볼 수 있습니다.

이벤트에 **MISP** 태그 추가

작성된 MISP 이벤트에 MISP 태그를 추가합니다.

시작하기 전에
필요한 역할: sn_sec_misp.write

프로시저

1. 추가 옵션 양식에서 양식 뷰의 이벤트 섹션에 추가할 **MISP** 태그 선택 으로 이동합니다.
2. 생성된 이벤트에 태그를 추가하는 옵션을 검토합니다.

고급 옵션 양식

필드	설명
작성된 MISP 이벤트에 태그 추가	ServiceNow에서 작성된 이벤트에 MISP 태그를 자동으로 추가할 수 있는 옵션입니다.
태그(로컬)	선택한 태그가 MISP 이벤트에 로컬 태그로 추가됩니다.
태그(전역)	선택한 태그가 MISP 이벤트에 전역 태그로 추가됩니다.

3. 저장을 클릭합니다.

결과
MISP 태그를 추가하면 이벤트를 분류하는 데 도움이 됩니다.

MISP 이벤트 데이터

이벤트 데이터를 검토하여 MISP 이벤트에 대한 MISP 자세한 정보를 볼 수 있습니다.

MISP 목록 뷰의 이벤트 데이터

다음에서 목록 뷰에 액세스 **MISP** 〉 **MISP** 이벤트 데이터.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

목록 뷰를 사용하여 이벤트 데이터에 대한 MISP 간략한 개요를 확인합니다.

MISP 이벤트 목록 뷰

필드	설명
이벤트 ID	이벤트를 처음 만들거나 서버로 가져올 MISP 때 MISP 할당된 이벤트 ID입니다.
정보	이벤트에 대한 간단한 설명입니다.
분석	다음과 같은 가능한 옵션이 있는 이벤트 분석의 현재 스테이지입니다. • 초기: 분석이 이제 막 시작되었습니다. • 진행 중: 분석이 진행 중입니다. • 완료됨: 분석이 완료되었습니다.
위협 수준	이벤트의 위험 수준입니다. 인시던트는 세 가지 위협 범주(낮음, 중간, 높음)로 분류할 수 있습니다. 이 필드는 정의되지 않은 상태로 둘 수 있습니다. 옵션은 다음과 같습니다. • 낮음: 일반 대량 맬웨어 • 중간: 지능형 지속 위협(APT) • 높음: 정교한 APT 및 0일 공격
MISP 태그	이벤트와 연결된 태그입니다 MISP .
MISP 갤럭시	이벤트와 MISP 연결된 갤럭시입니다.
소유자 조직	인스턴스에서 이벤트를 MISP 소유한 조직입니다. 이 필드는 관리자에게만 표시됩니다.
작성자 조직	인스턴스에서 이벤트를 MISP 생성한 조직입니다.
배포	개별 속성의 분포입니다. 속성의 배포 수준은 이벤트와 다를 수 있습니다.
MISP 이벤트 하이퍼링크	MISP 서버에 저장된 MISP 이벤트에 연결합니다.
MISP 소스	MISP 이벤트가 생성된 소스입니다.

MISP 양식 뷰의 이벤트 데이터

양식 뷰를 사용하여 이벤트에 대한 MISP 자세한 정보를 확인합니다.

MISP 이벤트 양식 뷰

필드	설명
이벤트 ID	이벤트를 처음 만들거나 서버로 가져올 MISP 때 MISP 할당된 이벤트 ID입니다.
UUID	이벤트와 속성을 고유하게 식별하는 ID입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

MISP 이벤트 양식 뷰

필드	설명
작성자 조직	인스턴스에서 이벤트를 MISP 생성한 조직입니다.
소유자 조직	인스턴스에서 이벤트를 MISP 소유한 조직입니다. 이 필드는 관리자에게만 표시됩니다.
작성자 사용자	에서 MISP이벤트를 생성한 사용자입니다.
마지막 변경	이벤트가 마지막으로 수정된 날짜입니다.
MISP 소스	MISP 이벤트가 생성된 소스입니다.
작성된 날짜(MISP)	이벤트를 만들었거나 서버에서 처음 가져온 MISP 날짜입니다.
위협 수준	이벤트의 위험 수준입니다. 인시던트는 세 가지 위협 범주(낮음, 중간, 높음)로 분류할 수 있습니다. 이 필드는 정의되지 않은 상태로 둘 수 있습니다. 옵션은 다음과 같습니다. • 낮음: 일반 대량 맬웨어 • 중간: 지능형 지속 위협(APT) • 높음: 정교한 APT 및 0일 공격
분석	다음과 같은 가능한 옵션이 있는 이벤트 분석의 현재 스테이지입니다. • 초기: 분석이 이제 막 시작되었습니다. • 진행 중: 분석이 진행 중입니다. • 완료됨: 분석이 완료되었습니다.
배포	개별 속성의 분포입니다. 속성의 배포 수준은 이벤트와 다를 수 있습니다.
게시 날짜:	이벤트 게시 여부의 상태입니다. 게시하면 이벤트의 속성을 모든 적격 익스포트에 사용할 수 있으며 이벤트 경보를 구독한 사용자에게 알릴 수 있습니다.
MISP 이벤트 하이퍼링크	MISP 서버에 저장된 MISP 이벤트에 연결합니다.
정보	이벤트에 대한 간단한 설명입니다.
태그(로컬)	호스트 조직의 MISP 인스턴스에서 동기화 및 익스포트 필터링을 위한 태그 지정을 활성화하는 데 사용할 수 있는 태그입니다. MISP 로컬 태그를 사용할 때 이벤트가 수정되지 않습니다. 로컬 태그는 다른 MISP 인스턴스 및 공유 커뮤니티와 동기화되기 전에 항상 제거됩니다.
태그(전역)	다른 인스턴스 및 공유 커뮤니티와 MISP 공유하고 동기화하기 위해 전역적으로 사용할 수 있는 태그입니다. 인스턴스에 전역 태그를 MISP 추가할 때 이벤트를 수정할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

MISP 이벤트 양식 뷰

필드	설명
갤럭시(로컬)	호스트 조직의 MISP 인스턴스에서 동기화 및 익스포트 필터링에 사용할 수 있는 갤럭시입니다. MISP 로컬 갤럭시를 사용할 때 이벤트는 수정되지 않습니다. 이러한 로컬 은하는 다른 MISP 인스턴스 및 공유 커뮤니티와 동기화되기 전에 항상 제거됩니다.
갤럭시(전역)	다른 MISP 인스턴스 및 공유 커뮤니티와 공유하고 동기화할 수 있는 전역적으로 사용할 수 있는 갤럭시입니다. 글로벌 갤럭시 MISP 를 추가할 때 이벤트를 수정할 수 있습니다.

연결된 MISP 이벤트

연결된 MISP 이벤트 목록 뷰를 사용하여 보안 인시던트의 컨텍스트에서 수동 또는 자동으로 생성된 이벤트를 볼 수 있습니다.

연결된 MISP 이벤트

필드	설명
보안 인시던트	SIR 보안 인시던트. 보안 인시던트를 클릭하여 보안 인시던트를 확인합니다.
MISP 이벤트	MISP 이벤트 ID입니다. MISP 에서 이벤트를 ServiceNow AI Platform보려면 MISP 이벤트를 클릭합니다.
MISP 소스	MISP 이벤트가 생성된 소스입니다. MISP 소스를 클릭하여 소스를 봅니다.
이벤트 작성 모드	이벤트 생성 프로파일을 사용하여 이벤트가 수동 또는 자동으로 생성되었는지 여부에 대한 상태입니다. MISP 관련 MISP 이벤트를 보려면 이벤트를 클릭하십시오.
자동 이벤트 작성 프로파일	자동 이벤트를 생성하는 데 사용되는 이벤트 생성 프로파일입니다. 자동 MISP 이벤트 작성 프로파일을 보려면 프로파일을 클릭하십시오.

MISP 사용자 정보

사용자 정보 페이지를 사용하여 MISP 에 연관된 모든 사용자를 볼 수 있습니다 ServiceNow AI Platform MISP Integration for Security Operations.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

MISP 사용자 정보

필드	설명
소스	사용자 계정의 소스입니다 MISP .
사용자 ID	사용자 계정을 만들 때 서버에서 할당 MISP 하는 사용자 ID입니다.
사용자 이메일	사용자의 이메일 주소입니다. 조직 관리자만 조직 사용자의 이메일 주소를 볼 수 있습니다.
조직	사용자가 속한 조직입니다.
역할 이름	사용자에게 귀속되는 사용자 권한을 정의하는 역할 이름입니다. 의 MISP역할에 대한 자세한 내용은 MISP 설명서를 참조하십시오.
역할 ID	의 사용자 역할 ID입니다 MISP. 예를 들어 영구 관리자, 영구 감사 또는 영구 태거 등이 있습니다.
권한	사용자가 보유하는 권한입니다. MISP에서 사용할 수 있는 권한은 다음과 같습니다. • 읽기 전용 • 자체 이벤트 관리 • 조직 이벤트 관리 • 조직 이벤트 게시 관리
사이팅 권한	사용자가 사이팅 검색을 수행하는 데 사용할 수 있는 권한입니다.
태거 권한	사용자가 태그 지정을 수행할 수 있는 권한입니다.

도메인 분리 및 **MISP**

MISP에서는 도메인 분리가 지원됩니다. 도메인 분리를 사용하여 데이터, 프로세스 및 관리 작업을 도메인이라는 논리적 그룹으로 분할할 수 있습니다. 그런 다음 사용자가 데이터를 보고 액세스할 수 있는 것을 포함하여 이러한 분리의 여러 가지 측면을 제어할 수 있습니다.

지원 수준

지원: 기본.

에서 도메인 분리가 작동하는 방식 **MISP**

도메인 분리를 수행하려면 다음 단계를 따르십시오.

- 도메인에서 필요한 역할을 가진 사용자를 생성합니다.
- MISP Integration for Security Operations 도메인에서 절차를 수행합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

MISP 통합 문제 해결

이 섹션에서는 MISP 통합을 설정하거나 실행할 때 발생할 수 있는 일반적인 문제를 해결하는 데 도움이 될 수 있는 중요한 문제 해결 팁을 다룹니다.

SSL 문제

MISP 통합을 통해 연결할 때 MISP 서버에 만료되지 않은 유효한 CA 인증서를 설치했는지 확인하십시오. RSA 또는 자체 인증서를 플랫폼으로 임포트하고 인증서의 일반 이름이 호스트 이름과 일치하는지 확인할 수 있습니다. 자세한 내용은 설치 및 구성 MISP Integration for Security Operations 및 MISP 사용자 역할 및 권한 문서를 참조하십시오.

위협을 조사하고 분석하는 데 사용 MISP

모듈과 ServiceNow AI Platform SIR 모듈의 데이터를 ServiceNow AI Platform 위협 인텔리전스 사용하여 MISP 조직에 대한 위협을 조사하고 분석할 수 있습니다.

에서 사이팅 검색 MISP

인스턴스의 옵저버 MISP 블에 대해 사이팅 검색을 수행하여 네트워크에서 피싱 공격 또는 악성 IP 또는 URL을 사용한 통신과 같은 특정 유형의 공격이 발생하는 빈도를 확인할 수 있습니다. 각 발생은 사이팅으로 간주됩니다.

의 사이팅 MISP

목격은 표시기, 물체 또는 속성이 보였고 그 유효성이 확인되었음을 나타냅니다. Sightings in MISP은 이벤트의 속성에 응답할 수 있는 시스템입니다. 사용자가 주어진 속성을 보았는지 쉽게 확인할 수 있는 방법을 제공하여 신뢰성을 높이도록 설계되었습니다. 속성은 여러 번 볼 수 있습니다.

> **주:**
> 옵저버블은 MISP에서 속성으로 알려져 있습니다.

일부 속성은 가양성으로 간주되며, 이는 유효한 사이팅이 아님을 의미합니다. 1주일 동안만 실행되는 피싱 캠페인과 같은 다른 속성은 특정 기간 동안만 유효합니다. 특정 기간 동안 유효한 속성에 만료 날짜를 할당할 수 있지만 각 조직은 속성에 유효한 만료 날짜를 하나만 할당할 수 있습니다.

해당 MISP 서버에서 로컬로 표시된 조직의 사용자가 만든 MISP 사이팅을 내부 사이팅이라고 합니다. 해당 MISP 서버에서 원격으로 표시된 조직의 사용자가 만든 MISP 사이팅을 외부 사이팅이라고 합니다.

에서 사이팅 검색 SIR

Security Operations Integration - 사이팅 검색 워크플로우는 사이팅 검색을 실행합니다. 이 플로우는 옵저버블 목록을 수락하고, 구현 역량을 찾고, 사이팅 검색 구성을 기반으로 쿼리를 생성하고, 구성된 플로우를 기반으로 검색을 실행합니다.

사이팅 검색은 분석가가 시간 경과에 따른 위협의 확산을 확인하는 데 도움이 됩니다. 보안 인시던트에서 개별 또는 여러 옵저버블과 검색 날짜 범위를 선택할 수 있습니다. 결과는 보안 인시던트 사이팅, 사이팅 검색 결과 및 사이팅 검색 정보 관련 목록에 포함됩니다.

인시던트 분석을 시작할 때 사이 ServiceNow AI Platform팅 검색을 자동으로 수행 하거나 옵저버블 사이팅 검색을 수동으로 수행하여 동일한 피싱 공격의 영향을 받는 조직의 다른 사용자를 식별하도록 설정할 수 있습니다.

에서 자동 사이팅 검색 사용 MISP

새 옵저버블이 보안 인시던트와 연결될 때마다 보안 운영 통합 - 사이팅 검색 워크플로우가 트리거되도록 사이팅 검색을 MISP 자동으로 실행하도록 설정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
Verify that the 에 대한 사이팅 검색 구성 프로파일 MISP 이(가) 활성 상태입니다.

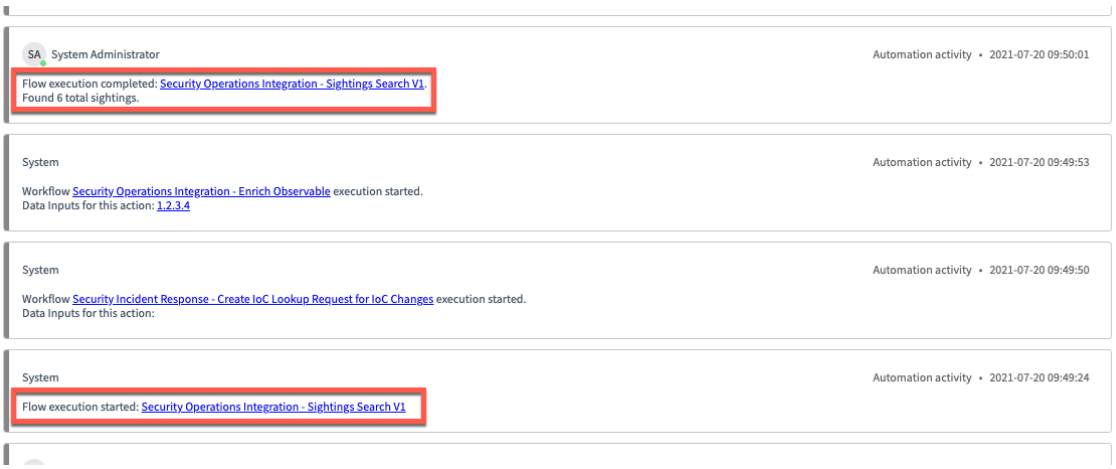
필요한 역할: sn_si.analyst

이 태스크 정보
사용하도록 설정하는 경우 다음에서 자동으로 실행되는 사이팅 검색 기능 MISP 통합 구성, 새 옵저버블이 보안 인시던트와 연결되면 의 MISP 사이팅 검색이 트리거됩니다. 기본적으로 새 옵저버블이 보안 인시던트와 연결된 경우 **Sighting** 검색 자동 실행 옵션이 활성화되어 있습니다.

프로시저

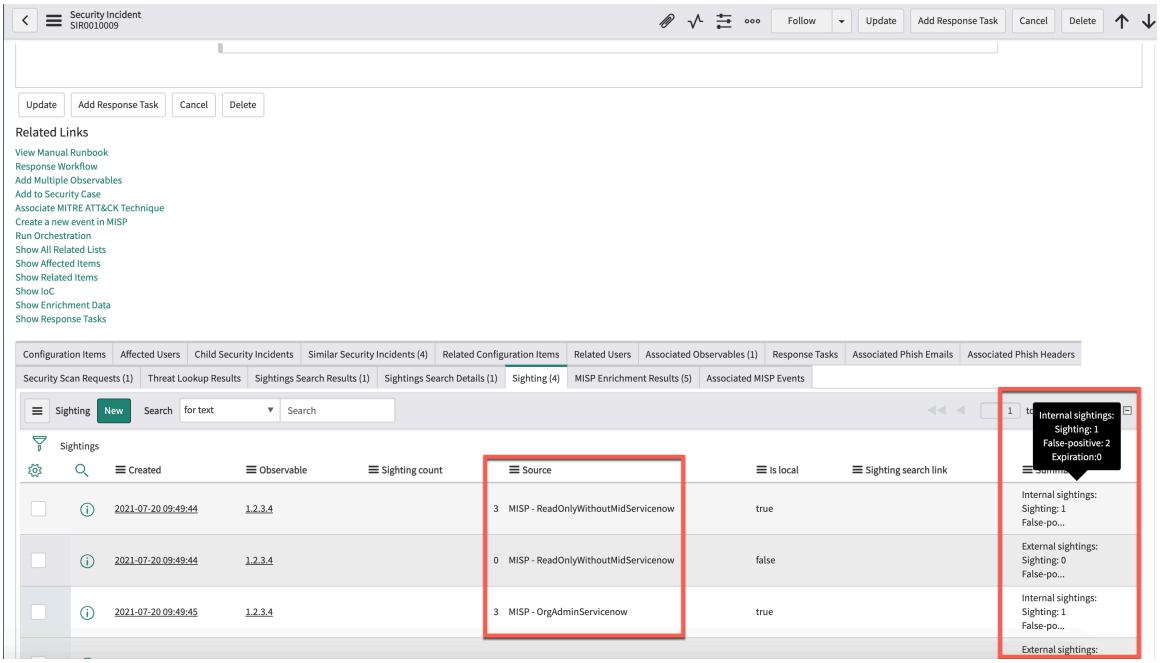
1. 다음으로 이동 모두 〉 보안 인시던트 〉 모든 인시던트 표시.
2. 사이팅 검색 데이터에서 보려는 옵저버블이 포함된 보안 인시던트를 MISP 선택합니다.
3. 새 옵저버블이 보안 인시던트와 연결된 후 작업 메모를 검토합니다.
   작업 메모는 보안 운영 통합 - 사이팅 검색 워크플로우 가 트리거되면 게시됩니다.

   다음 예는 작업 메모 섹션을 보여줍니다.



4. 모든 이벤트(전역)에서 표시되고 워크플로우 실행이 완료된 후 내부 또는 외부 사이팅으로 분류된 옵저버블의 집계 정보를 봅니다.
   사이팅, 사이팅 검색 결과 및 사이팅 검색 정보 관련 목록에서 정보를 확인합니다. 다음 예는 사이팅 관련 목록에 생성된 사이팅 검색 기록을 보여줍니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



사이팅 검색 기록

필드	설명
작성됨	사이팅 검색 기록이 생성된 날짜 및 시간입니다.
옵저버블	쿼리로 검색되는 옵저버블입니다.
관찰 카운트	내부 및 외부 사이팅의 수입니다.
소스	옵저버블의 소스입니다. 옵저버블이 조직의 옵 MISP 저버블인 경우 기록 앞에 MISP라는 단어가 붙습니다.
로컬 여부	내부 사용자가 사이팅을 보고했는지 여부의 상태입니다.
사이팅 검색 링크	인스턴스의 사이팅 검색 링크입니다 MISP .
요약	기록과 연결된 사이팅의 유형입니다. Sighting의 세 가지 유형은 Sighting, False-positive 및 Expiration입니다. 요약 열은 가 MISP Integration for Security Operations 설치된 경우에만 나타납니다. 이외의 MISP 소스가 나타나면 해당 기록에 대한 요약 열 항목이 비어 있습니다.

에서 수동 사이팅 검색 수행 **MISP**

옵저버블을 하나 또는 여러 개 선택하고 애플리케이션에서 수동 사이팅 검색을 ServiceNow AI Platform MISP Integration for Security Operations 수행하여 시간 경과에 따른 위협의 확산을 확인합니다.

시작하기 전에

- 다음 항목 검토: MISP 사용자 역할 및 권한 양방향 기능을 사용하기 위한 것입니다 MISP .
- 필요한 역할: sn_si.analyst

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

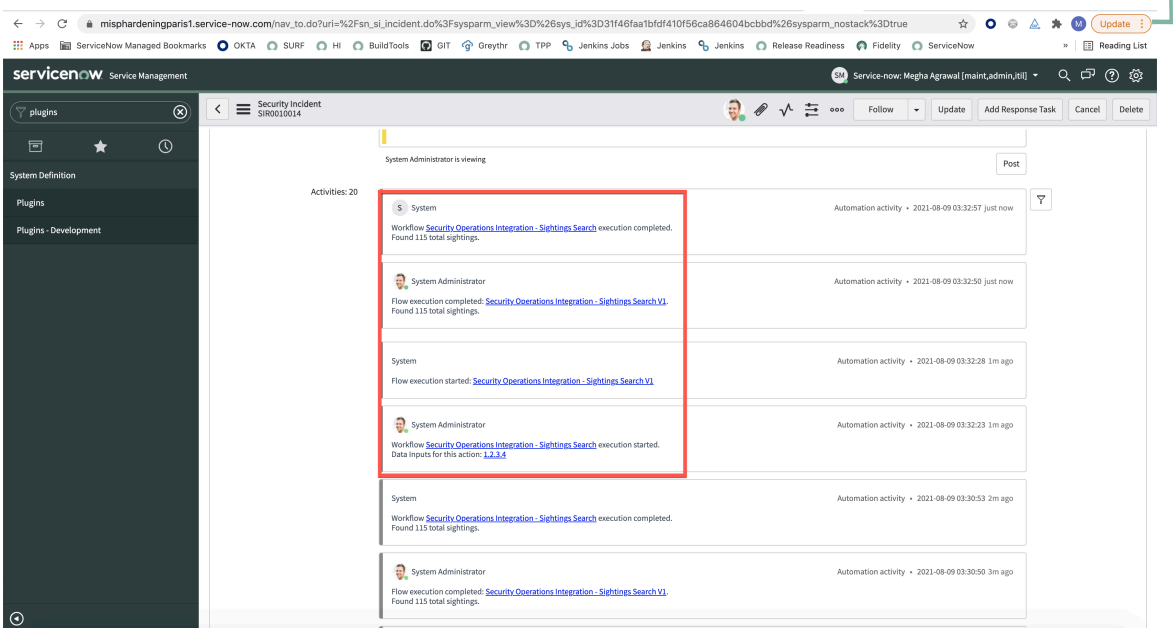
프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 모든 인시던트 표시.
2. 사이팅 검색을 실행할 옵저버블이 포함된 보안 인시던트를 MISP 선택합니다.
3. 모든 관련 목록 표시 및 연결된 옵저버블 탭을 클릭합니다.
4. 옵저버블을 선택하고 작업 메뉴에서 사이팅 검색 실행을 클릭합니다.
   사이팅 검색을 위해 여러 옵저버블을 선택할 수 있습니다.
   사이팅 검색 실행 대화 상자가 열립니다.
5. 사이팅 검색 데이터를 검색할 날짜 범위를 지정합니다.

사이팅 검색 실행 대화 상자

필드	설명
마지막	검색할 인시던트가 생성되기 전의 시간 또는 일 수입니다. 기본값은 7일입니다. 한도는 99시간 또는 일입니다.
다음 날짜 사이	검색할 날짜 범위입니다. 기본 날짜는 다음과 같습니다. ○ 인시던트가 생성된 날짜 및 시간입니다. ○ 인시던트가 열리기 7일 전의 날짜 및 시간입니다.

6. 검색을 클릭합니다.
   다음 예는 작업 메모의 수동 사이팅 검색 결과를 보여줍니다.



결과
사이팅 검색 기록이 생성됩니다. 워크플로우 실행이 완료되면 모든 이벤트(전역)에서 표시되고 내부 또는 외부 사이팅으로 분류된 옵저버블의 집계 정보를 볼 수 있습니다. 집계 및 연관된 사이팅 데이터는 사이팅, 사이팅 검색 결과 및 사이팅 검색 상세 정보 관련 목록 아래의 보안 인시던트에 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사이팅을 에 보고 **MISP**

위협 데이터 목격을 보고하여 데이터의 가양성에 대응하고 진정한 긍정 위협이 발생할 때 인식을 높일 수 있습니다. 특정 옵저버블 또는 속성에 대한 만료 날짜를 추가할 수도 있습니다.

시작하기 전에

- 다음 항목 검토: MISP 사용자 역할 및 권한 양방향 기능을 사용하기 위한 것입니다 MISP .
- 필요한 역할: sn_si.analyst

이 태스크 정보

이를 MISP Integration for Security Operations 통해 모든 이벤트에서 사이팅을 전역에 보고할 MISP 수 있습니다. 사이팅을 특정 이벤트에 보고하려면 인스턴스를 사용하고 로컬에서 MISP 사이팅을 보고해야 합니다.

사이팅 MISP을 에 보고하려면 인스턴스에서 옵저버블 또는 속성을 사용할 수 MISP 있어야 합니다.

프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 모든 인시던트 표시.
2. 사이팅 MISP 을 보고할 옵저버블이 포함된 보안 인시던트를 선택합니다.
3. 모든 관련 목록 표시 및 사이팅 관련 목록을 클릭합니다.
4. 옵저버블을 선택하고 작업 메뉴에서 다음 옵션 중 하나를 선택합니다.
   소스와 관련되지 않은 옵저버블을 MISP 선택하면 작업 메뉴에 관련 MISP 소스의 개수가 표시됩니다. 다음 예는 8개의 옵저버블 중 4개를 와 관련된 MISP것으로 보여줍니다. 다음 예에서는 작업 메뉴와 제출할 관련 옵저버블을 보여줍니다.

제출할 관련 옵저버블을 보여주는 작업 메뉴

5. 옵션: **MISP:** 옵저버블 사이팅 보고 옵션을 선택한 경우 옵저버블 사이팅을 MISP에 보고 대화 상자의 필드를 채워야 합니다.

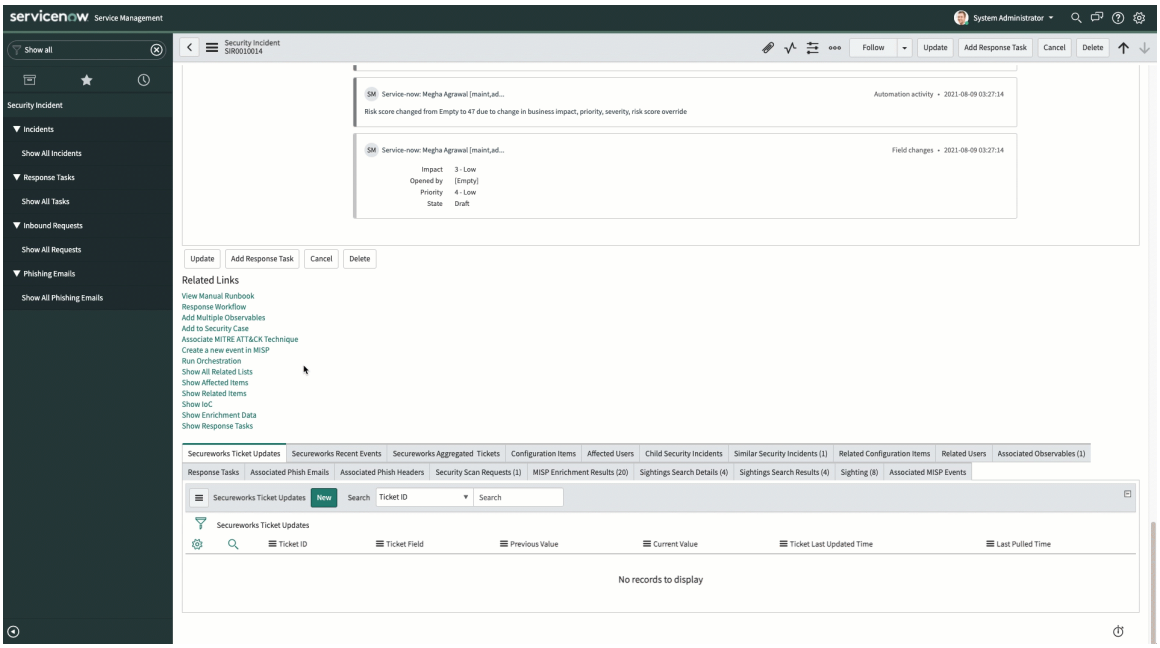
옵저버블 사이팅을 **MISP** 대화 상자에 보고

필드	설명
소스	사이팅의 소스에 MISP 해당하는 소스 필드입니다.
날짜	옵저버블이 관찰된 날짜에 해당하는 날짜 필드입니다. 날짜가 비어 있으면 현재 날짜와 시간이 에 채워 MISP집니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음 예시에서는 보안 인시던트의 사이팅 관련 목록으로 이동하는 방법을 보여줍니다. 해당 목록에서 옵저버블을 선택하고 옵저버블 사이팅을 에 보고할 수 있습니다 MISP. 성공 메시지는 사이팅이 에 성공적으로 제출 MISP되었음을 보여줍니다.

옵저버블 사이팅을 MISP에 보고합니다.



a. 사이팅 보고를 클릭합니다.

6. 옵션: **MISP:** 옵저버블을 긍정 오류로 보고 옵션을 선택한 경우 옵저버블을 긍정 MISP 오류로 보고 대화 상자의 필드를 채워야 합니다.

옵저버블을 긍정 **MISP** 오류로 보고 대화 상자에

필드	설명
소스(선택 사항)	소스에 해당하는 소스 필드입니다 MISP . 이 필드를 사용하여 옵저버블을 긍정 오류로 선언합니다.
날짜	옵저버블이 긍정 오류로 발견된 날짜에 해당하는 날짜 필드입니다. 날짜가 비어 있으면 현재 날짜와 시간이 에 채워 MISP집니다.

a. 오탐지 보고를 클릭합니다.

7. 옵션: **MISP:** 옵저버블을 만료됨으로 보고 옵션을 선택한 경우 옵저버블 만료 보고 MISP 대화 상자의 필드를 채워야 합니다.

옵저버블 만료를 MISP에 보고 대화 상자

필드	설명
소스	소스에 해당하는 소스 필드입니다 MISP . 이 필드를 사용하여 옵저버블을 만료됨으로 설정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
날짜	옵저버블이 만료된 날짜에 해당하는 날짜 필드입니다. 날짜가 비어 있으면 현재 날짜와 시간이 에 채워 MISP집니다.

a. **Report** Expiry(만료 보고)를 클릭합니다.

결과
사이팅이 MISP 서버에 성공적으로 업데이트됩니다.

에서 옵저버블 보강 **MISP**

인시던트 응답 조사 중에 다양한 MISP 소스의 추가 정보로 옵저버블을 보강하여 식별된 위협을 억제할 수 있습니다.

에서 자동 옵저버블 보강 활성화 **MISP**

새 옵저버블이 보안 인시던트와 연결된 경우 자동 옵저버블 보강 ServiceNow AI Platform MISP 을 활성화합니다.

시작하기 전에

- 보안 인시던트 응답예약된 작업 활성화 또는 비활성화, 보안 인시던트 옵저버블 조회 옵션에 대한 시스템 속성을 활성화하여 에서 SIR옵저버블 보강 기능을 트리거합니다.
- 필요한 역할: sn_si.analyst

프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 모든 인시던트 표시.
2. 옵저버블 데이터를 MISP 보강하려는 옵저버블이 포함된 보안 인시던트를 선택합니다.
3. 새 옵저버블이 보안 인시던트와 연결된 후 작업 메모를 검토합니다.

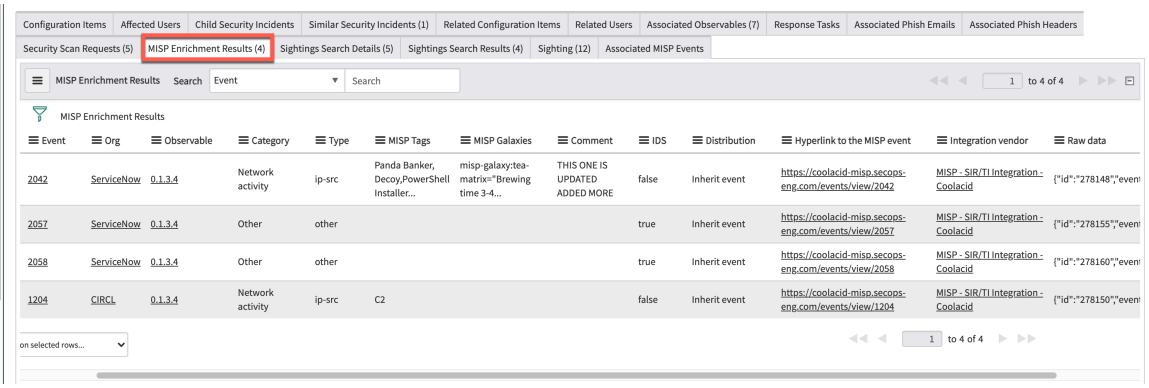
   다음 예는 보안 운영 통합 - 옵저버블 보강 플로우 가 트리거될 때 작업 메모가 게시되는 것을 보여줍니다.

4. MISP 보안 인시던트의 보강 결과 관련 목록에서 플로우 실행이 완료된 후 보강 결과를 봅니다.

   주:
   보강 결과 관련 목록이 보안 인시던트 관련 목록에 나타나도록 MISP 구성해야 합니다. 자세한 내용은 관련 목록 구성을 참조하십시오.

   다음 예제에서는 의 MISP보강 결과를 보여 줍니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



다음 표에서는 MISP 보강 결과를 보여줍니다.

MISP 보강 결과

필드	설명
이벤트	이벤트의 ID입니다. 열기를 클릭하여 인스턴스의 기록을 ServiceNow AI Platform 봅니다.
조직	원래 이벤트를 생성한 조직입니다.
옵저버블	이벤트와 연결된 옵저버블입니다.
범주	속성의 범주입니다. MISP 문서에서 범주 목록을 봅니다.
유형	속성의 유형입니다. MISP 설명서에서 유형 목록을 봅니다.
MISP 태그	속성과 MISP 연결된 태그의 목록입니다.
MISP 갤럭시	속성과 MISP 연결된 은하의 목록입니다.
설명	속성에 대한 자세한 설명을 위한 상황별 설명입니다. 이러한 의견은 상관 관계에 사용되지 않으며 순전히 정보 제공입니다.
IDS	모든 적격 익스포트에 포함할 수 있는 침해 표시기입니다.
배포	게시된 후 속성의 분포입니다. 속성의 배포 수준은 이벤트와 다를 수 있습니다. 두 경우 모두 가장 낮은 배포 수준이 사용됩니다.
MISP 이벤트 하이퍼링크	MISP 서버에 저장된 MISP 이벤트에 연결합니다.
통합 벤더	향상을 위한 데이터를 제공하는 통합 벤더입니다.
원시 데이터	속성과 MISP 연결된 원시 데이터입니다.

에서 수동 옵저버블 보강 수행 **MISP**

개별 또는 여러 옵저버블을 선택하고 수동 옵저버블 보강을 수행하여 다양한 MISP 소스의 추가 정보로 옵저버블을 보강할 수 있습니다.

시작하기 전에

- 다음 항목 검토: MISP 사용자 역할 및 권한 양방향 기능을 사용하기 위한 것입니다 MISP .
- 필요한 역할: sn_si.analyst

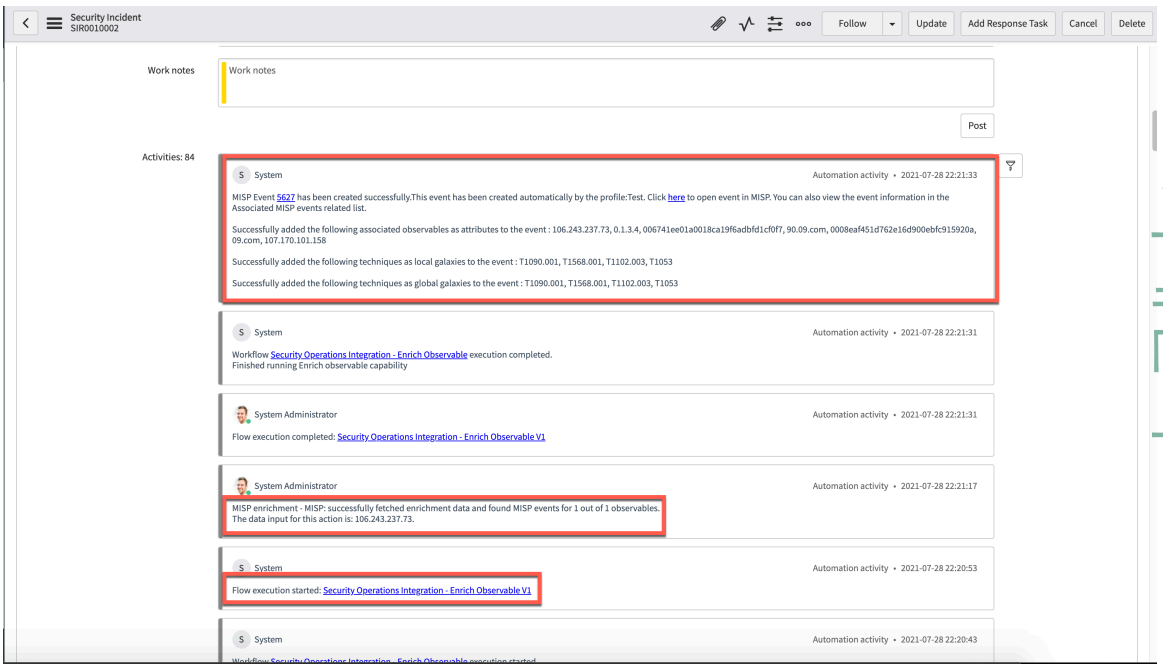
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 모든 인시던트 표시.
2. 보강을 수행할 옵저버블이 포함된 보안 인시던트를 선택합니다.
3. 모든 관련 목록 표시 및 연결된 옵저버블 탭을 클릭합니다.
4. 옵저버블을 선택하고 작업 메뉴에서 옵저버블 보강 실행을 클릭합니다.
   사이팅 검색을 위해 여러 옵저버블을 선택할 수 있습니다.
   옵저버블 보강 실행 대화 상자가 나타납니다.
5. MISP 소스를 선택하고 선택됨 열에서 선택한 옵저버블을 보강할 구현을 선택합니다.
6. 제출을 클릭합니다.
   작업 메모에 Security Operations Integration - 옵저버블 보강 워크플로우 가 트리거되었음을 보여줍니다. 관련 구현 워크플로우가 실행되어 보강을 수행합니다. 보안 인시던트의 작업 메모를 보고 상태를 볼 수 있습니다.

   다음 예제에서는 수동 옵저버블 보강에 대한 작업 메모를 보는 방법을 보여줍니다.

수동 옵저버블 보강을 위한 작업 메모



보강 메시지에는 생성된 이벤트가 나열됩니다. 또는 MISP 인스턴스에서 이벤트를 ServiceNow AI Platform 보고 MISP 보강 결과 탭에서 기록의 상세 정보를 볼 수 있습니다.

속성에 태그 **MISP** 추가 또는 제거

에서 MISP 태그를 추가하거나 제거하여 이벤트 또는 속성을 분류합니다. 전역적으로 태그 지정을 사용하여 분류를 활성화하거나, 분류 중에 이벤트가 수정되는 것을 원하지 MISP 않을 때 태그를 로컬에서 사용할 수 있습니다.

시작하기 전에

- 다음 항목 검토: MISP 사용자 역할 및 권한 양방향 기능을 사용하기 위한 것입니다 MISP .
- 편집 중인 속성이 사용자와 동일한 조직에 MISP 속해 있는지 확인합니다.
- 사용할 수 있는 태그와 갤럭시는 소스 및 해당 배포 권한을 기반으로 MISP 합니다.
- 필요한 역할: sn_sec_misp.write

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 모든 인시던트 표시.
2. 태그를 추가하려는 옵저버블, 속성 또는 이벤트가 포함된 보안 인시던트를 선택합니다.
3. 모든 관련 목록 표시 및 MISP 보강 결과 관련 목록을 클릭합니다.
4. 미리 보기 아이콘을 클릭합니다 ⓘ . 기록 옆에 있는 다음 기록 열기를 클릭합니다.
   다음 예제에서는 **MISP** 보강 결과를 검토하는 방법과 보강 기록을 여는 MISP 방법을 보여줍니다.

   MISP 보강 결과 기록
   MISP 보강 결과 기록 열기

5. MISP 보강 결과 기록을 검토합니다.

MISP 보강 결과

필드	설명
옵저버블	
이벤트	이벤트를 처음 만들거나 로 가져올 MISP때 서버에서 할당 MISP 한 이벤트 ID입니다. 이벤트 데이터 페이지에서 이벤트 데이터를 MISP 보려면 이벤트를 미리 보거나 기록을 클릭하십시오.
조직	속성을 생성한 조직입니다 MISP .
범주	의 MISP특정 이벤트에 추가하는 속성의 범주입니다. 내부 참조, 네트워크 활동, 금융 사기 등의 옵션을 선택할 수 있습니다.
유형	MISP 속성의 유형입니다.
통합 벤더	옵저버블 보강을 위한 데이터를 제공하는 통합 벤더입니다.
작성된 날짜(MISP)	이벤트가 처음 생성되거나 로 임포트된 MISP날짜입니다.
IDS	에서 SIR옵저버블이 악성으로 표시되는지 여부의 상태입니다. 의 MISP 해당 속성도 true로 표시됩니다.
배포	이 이벤트가 게시된 후 볼 수 있는 사람과 같은 배포 옵션 통제. 이 옵션은 이벤트를 다른 서버와 동기화할지 여부도 제어합니다. 분포는 속성에 상속되며 가장 제한적인 설정이 우선합니다. 배포 옵션은 다음과 같습니다. ○ 내 조직만: 조직의 구성원만 이 이벤트를 볼 수 있습니다. 조직 구성원 중 한 명이 내 조직만 접근할 수 있는 다른 인스턴스로 이벤트를 끌어올 수 있습니다. 이 설정의 이벤트는 동기화되지 않습니다. ○ 이 커뮤니티만: 자신의 조직, 이 MISP 서버의 조직 및 이 서버와 동기화되는 서버를 실행하는 MISP 조직을 포함하여 커뮤니티에

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	MISP 속한 사용자가 이벤트를 볼 수 있도록 합니다. 이러한 연결된 서버에 연결된 다른 조직은 이벤트를 볼 수 없습니다. ○ 연결된 커뮤니티: 이 MISP 서버의 모든 조직, 이 서버와 동기화되는 서버의 모든 조직 MISP 및 두 홉 떨어져 있는 서버에 연결하는 서버의 호스팅 조직을 포함하여 커뮤니티에 MISP 속한 사용자가 이벤트를 볼 수 있도록 합니다. 2홉 떨어져 있는 연결된 서버에 연결된 다른 조직은 이벤트를 볼 수 없도록 제한됩니다. ○ 모든 커뮤니티: 이벤트를 모든 커뮤니티와 MISP 공유하여 이벤트를 자유롭게 사용할 수 있도록 합니다.
MISP 이벤트 하이퍼링크	MISP 서버에 저장된 MISP 이벤트에 연결합니다.
원시 데이터	옵저버블 보강 데이터 기록에 대한 원시 상세 정보입니다.
설명	속성에 대해 추가하는 코멘트입니다. 이러한 의견은 정보 제공의 목적으로만 사용되며 상관 관계에 사용되지 않습니다.
태그(로컬)	호스트 조직의 MISP 인스턴스에서 동기화 및 익스포트 필터링을 위한 태그 지정을 활성화하는 데 사용할 수 있는 태그입니다. MISP 로컬 태그를 사용할 때 이벤트가 수정되지 않습니다. 이러한 태그는 다른 MISP 인스턴스 및 공유 커뮤니티와 동기화되기 전에 항상 제거됩니다.
태그(전역)	다른 인스턴스 및 공유 커뮤니티와 MISP 공유하고 동기화하기 위해 전역적으로 사용할 수 있는 태그입니다. 인스턴스에 전역 태그를 MISP 추가하면 이벤트가 수정됩니다.
갤럭시(로컬)	호스트 조직의 MISP 인스턴스에서 동기화 및 익스포트 필터링에 사용할 수 있는 갤럭시입니다. MISP 로컬 갤럭시를 사용할 때 이벤트는 수정되지 않습니다. 이러한 은하계는 다른 MISP 인스턴스 및 공유 커뮤니티와 동기화되기 전에 항상 제거됩니다.
갤럭시(전역)	다른 MISP 인스턴스 및 공유 커뮤니티와 공유하고 동기화할 수 있는 전역적으로 사용할 수 있는 갤럭시입니다. 전역 갤럭시를 MISP 추가하면 이벤트가 수정됩니다.

6. 로컬 또는 전역 태그를 편집하려면 편집 아이콘 다음 옵션 중 하나에서 다음을 수행합니다.

- 태그(로컬)
- 태그(전역)

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

7. MISP 속성 태그 대화 상자에서 검색하고 추가할 태그의 이름을 입력합니다.
8. **MISP** 속성에 태그 업데이트를 클릭합니다.

   다음 예에서는 로컬 태그에 대한 편집 아이콘을 클릭하여 C3, 애드웨어, C2 및 봇넷 3101 태그를 검색 및 추가하고 MISP 서버를 태그로 업데이트할 수 있음을 보여줍니다. 확인 메시지는 에서 모든 태그가 업데이트 MISP되었음을 보여줍니다.

   MISP 속성에 로컬 태그 추가.
   서버에서 태그가 업데이트되었습니다 MISP .
9. 기록의 변경 내용을 보려면 성공 메시지에서 양식 다시 로드 를 클릭합니다.

이벤트 또는 속성에 갤럭시 **MISP** 추가 또는 제거

은 MISP 하를 추가하거나 제거하여 이러한 객체를 클러스터 MISP 로 분류하고 이벤트 또는 속성에 연결할 MISP 수 있습니다.

시작하기 전에

- 다음 항목 검토: MISP 사용자 역할 및 권한 양방향 기능을 사용하기 위한 것입니다 MISP .
- 로컬 갤럭시를 추가하려면 통합을 구성한 사용자가 해당 MISP 서버의 호스트 조직에 속해야 합니다.
- 사용할 수 있는 태그와 갤럭시는 소스 및 해당 배포 권한을 기반으로 MISP 합니다.
- 필요한 역할: sn_sec_misp.write

프로시저

1. 다음 옵션 중 하나에서 편집 아이콘

   - 갤럭시(로컬)
   - 갤럭시(전역)

2. MISP 이벤트 갤럭시 대화 상자에서 상세 정보를 입력합니다.

   MISP 이벤트 갤럭시 대화 상자

필드	설명
이벤트 ID	이벤트를 처음 만들거나 로 가져올 MISP때 서버에서 할당 MISP 한 이벤트 ID입니다.
네임스페이스	은하가 저장되는 네임스페이스입니다. 네임스페이스를 사용하여 유사한 은하를 그룹화할 수 있습니다.
갤럭시	클러스터 정보를 저장하는 갤럭시입니다.
클러스터	은하의 성단에 대한 정보.

3. 갤럭시를 **MISP** 속성으로 업데이트를 클릭합니다.
   다음 예제에서는 로컬 갤럭시에 대한 편집 아이콘을 클릭하여 더 이상 사용되지 않는 네임스페이스를 선택하고, 엔터프라이즈 공격 - 공격 패턴 갤럭시를 선택하고, 클러스터 정보를 추가할 수 있음을 보여줍니다. 갤럭시 정보가 업데이트되면 성공 메시지를 볼 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

를 통해 MISP에 갤럭시 정보 추가 ServiceNow AI Platform

4. 기록의 변경 내용을 보려면 성공 메시지에서 양식 다시 로드 를 클릭합니다.

결과
서버에서 갤럭시 정보가 성공적으로 업데이트되었습니다 MISP .

속성에 설명 **MISP** 추가

속성에 대한 MISP 주석을 추가합니다. 추가하는 의견은 정보 제공의 목적으로만 사용되며 데이터의 상관 관계 MISP 에는 사용되지 않습니다.

시작하기 전에

- 다음 항목 검토: MISP 사용자 역할 및 권한 양방향 기능을 사용하기 위한 것입니다 MISP .
- 편집 중인 속성이 사용자와 동일한 조직에 MISP 속해 있는지 확인합니다.
- 필요한 역할: sn_sec_misp.write

프로시저

1. 편집 아이콘을 클릭합니다
2. 속성 설명 필드에 설명을 입력합니다.
3. **MISP** 속성에 대한 설명 업데이트를 클릭합니다.
   다음 예제에서는 주석 필드 옆에 있는 편집 아이콘을 클릭하여 주석을 추가한 다음 속성을 업데이트할 MISP 수 있음을 보여 줍니다. 설명이 업데이트되면 성공 메시지를 볼 수 있습니다.

   를 ServiceNow AI Platform통해 MISP에 갤럭시 정보 추가 .

4. 기록의 변경 내용을 보려면 성공 메시지에서 양식 다시 로드 를 클릭합니다.

결과
코멘트가 서버에서 성공적으로 업데이트되었습니다 MISP .

MISP에서 이벤트 관리

에서 자동 또는 수동으로 이벤트를 MISP 생성할 수 있습니다 ServiceNow AI Platform. 에서 이벤트 데이터를 MISP 편집할 수도 있습니다 ServiceNow AI Platform.

에서 자동으로 생성된 이벤트 검증 **MISP**

인스턴스에서 이벤트 생성 프로파일을 구성한 후 자동으로 생성된 이벤트를 확인할 수 있습니다 ServiceNow AI Platform .

자동 이벤트 작성 프로파일

자동 이벤트 생성 프로파일 구성은 다음의 sn_si.admin 또는 sn_ti.admin 사용자 역할로 수행됩니다. **MISP** 통합 〉 자동 이벤트 작성 프로파일 모듈.

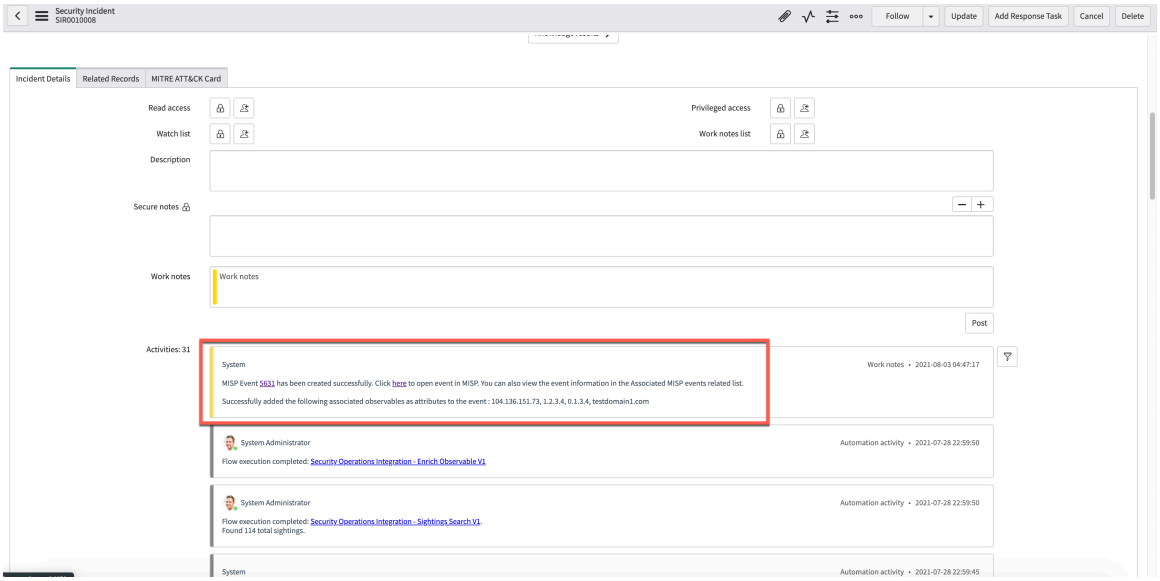
이벤트 데이터 보기 **MISP**

다음과 같은 방법으로 생성된 이벤트를 볼 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

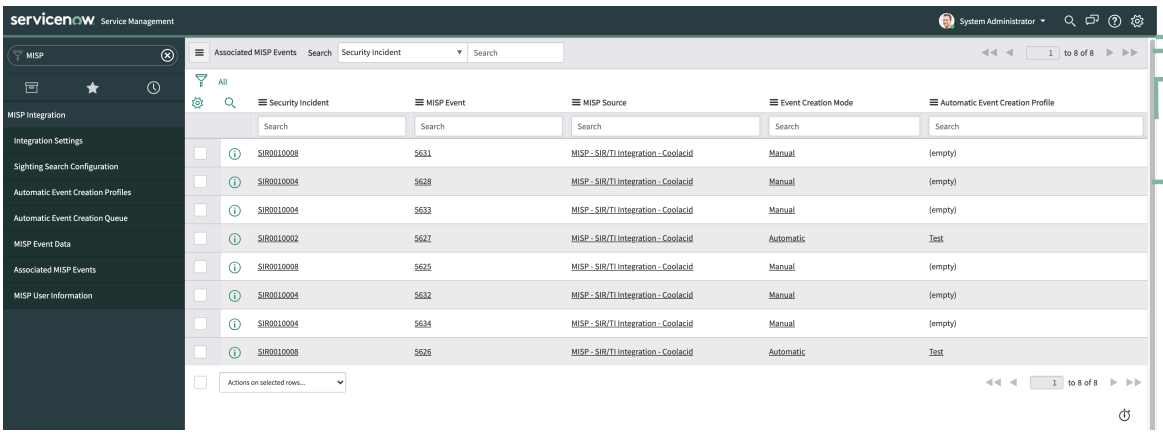
- 생성된 이벤트에 대한 작업 메모를 봅니다. 다음 예와 같이 인스턴스에서 이벤트 상세 정보를 ServiceNow AI Platform 볼 수 있으며 서버에 표시되는 MISP 방식으로도 볼 수 있습니다.

생성된 이벤트에 대한 작업 메모



- 연결된 MISP 이벤트 관련 목록을 클릭합니다. 여기서는 다음 예와 같이 보안 인시던트 및 MISP 자원과 관련된 이벤트를 볼 수 있습니다.

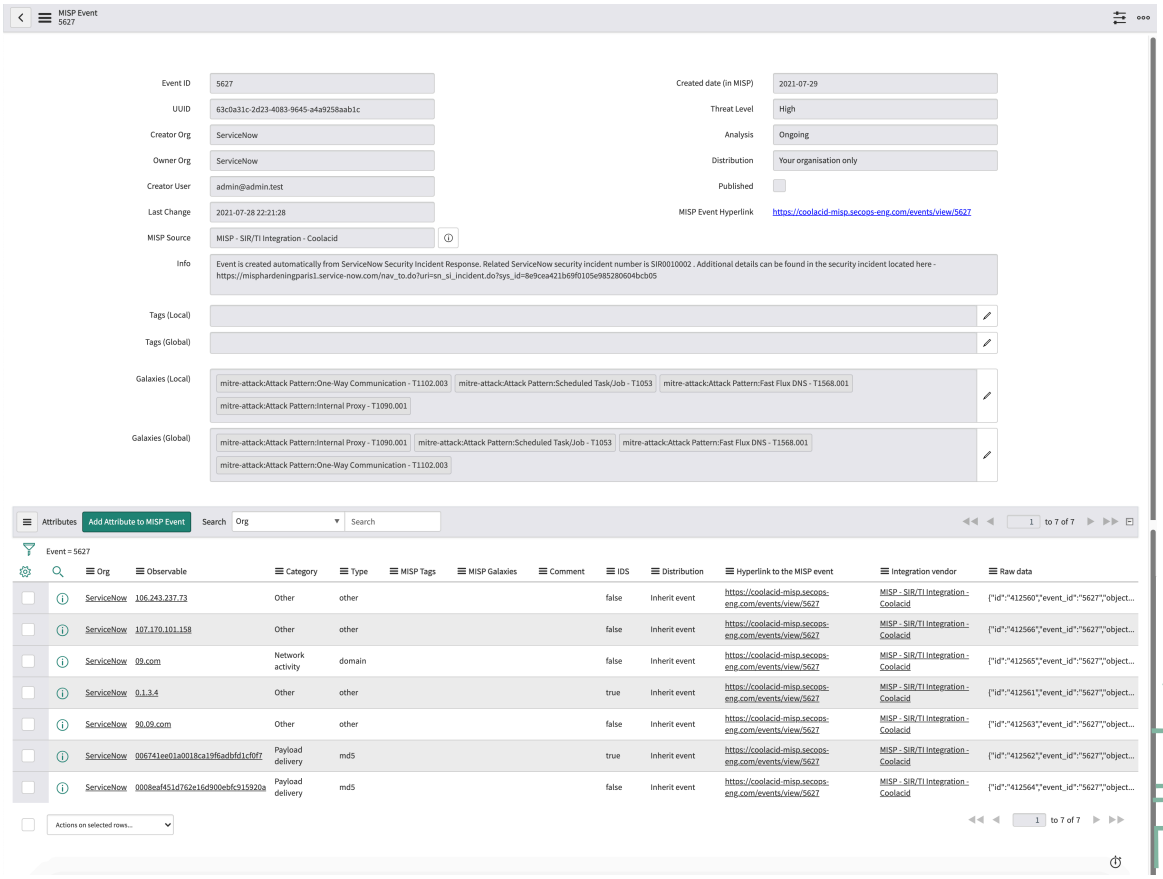
관련 이벤트 목록



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- MISP 다음 예와 같이 양식 뷰에서 이벤트 데이터를 보고 이벤트에 대한 MISP 자세한 정보를 검토합니다.

양식 뷰의 이벤트 데이터



MISP에서 수동으로 이벤트 작성

에서 ServiceNow AI Platform 이벤트를 MISP 수동으로 생성하여 속성 및 객체로 표시되는 상황별 관련 정보를 캡처합니다.

시작하기 전에

- 다음 항목 검토: MISP 사용자 역할 및 권한 양방향 기능을 사용하기 위한 것입니다 MISP .
- 필요한 역할: sn_sec_misp.write

프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 모든 인시던트 표시.
2. 이벤트를 생성하려는 옵저버블이 포함된 보안 인시던트를 선택합니다.
3. MISP에서 새 이벤트 만들기를 클릭합니다.
4. MISP에서 새 이벤트 작성 대화 상자에서 상세 정보를 입력합니다.

MISP 대화 상자에서 이벤트 작성

필드	설명
날짜	의 이벤트 생성 날짜입니다 MISP.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
이벤트 정보	에서 자동으로 생성되는 이벤트 정보입니다 ServiceNow AI Platform 보안 인시던트 응답.
위협 수준	이벤트의 위험 수준입니다. 인시던트를 세 가지 위협 범주(낮음, 중간, 높음)로 분류할 수 있습니다. 이 필드는 정의되지 않은 상태로 둘 수도 있습니다. 옵션은 다음과 같습니다. ○ 낮음: 일반 대량 맬웨어 ○ 중간: 지능형 지속 위협(APT) ○ 높음: 정교한 APT 및 0일 공격
소스	MISP 이벤트 생성 소스입니다.
배포	이벤트가 게시된 후 이 이벤트를 볼 수 있는 사용자를 제어하는 옵션입니다. 이 옵션은 이벤트를 다른 서버와 동기화할지 여부도 제어합니다. 분포는 속성에 의해 상속됩니다. 가장 제한적인 설정이 우선합니다. 배포 옵션은 다음과 같습니다. ○ 내 기관만: 조직의 구성원만 이 이벤트를 볼 수 있습니다. 조직 구성원 중 한 명이 내 조직만 접근할 수 있는 다른 인스턴스로 이벤트를 끌어올 수 있습니다. 이 설정의 이벤트는 동기화되지 않습니다. ○ 이 커뮤니티만: 자신의 조직, 이 MISP 서버의 조직 및 이 서버와 동기화되는 서버를 실행하는 MISP 조직을 포함하여 커뮤니티에 MISP 속한 사용자가 이벤트를 볼 수 있도록 합니다. 연결된 서버에 연결된 다른 조직에서는 이벤트를 볼 수 없습니다. ○ 연결된 커뮤니티: 이 MISP 서버의 모든 조직, 이 서버와 동기화되는 서버의 모든 조직MISP, 두 홉 떨어져 있는 모든 서버에 연결하는 서버의 호스팅 조직을 포함하여 커뮤니티의 MISP 일부인 사용자가 이벤트를

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드		설명
		볼 수 있도록 합니다. 이 서버에서 두 홉 떨어져 있는 연결된 서버에 연결된 다른 조직은 이벤트를 볼 수 없도록 제한됩니다. ○ 모든 커뮤니티: 이벤트를 모든 MISP 커뮤니티와 공유합니다.
분석		다음과 같은 가능한 옵션이 있는 이벤트 분석의 현재 스테이지입니다. ○ 초기: 분석이 이제 막 시작되었습니다. ○ 진행 중: 분석이 진행 중입니다. ○ 완료됨: 분석이 완료되었습니다.
고급 옵션	SIR 연결된 옵저버블을 MISP 이벤트 속성으로 추가	보안 인시던트 MISP 에서 사용 가능한 옵저버블을 이벤트에 속성으로 추가하는 옵션입니다. 이 옵션은 옵저버블 찾기가 악성일 때 속성 **IDS** 플래그 설정 옵션을 활성화합니다.
	옵저버블 찾기가 악성일 때 속성 IDS 플래그 설정	에서 SIR악성으로 표시된 옵저버블 . 의 MISP 해당 속성도 true로 표시됩니다.
	보안 태그를 기준으로 옵저버블 필터링	선택한 보안 태그를 기준으로 옵저버블을 필터링하는 옵션입니다. 이 옵션은 위협 인텔리전스에서 MISP 이벤트를 구분하고 관리하는 기능을 제공합니다. 보안 태그: 옵저버블을 필터링하는 태그를 추가합니다. 예를 들어 "공유 차단" 또는 "TLP: 흰색"이라는 태그를 추가하는 경우 옵저버블 중 하나에 이러한 태그가 연결되어 있으면 MISP 이벤트 작성 중에 이러한 옵저버블이 MISP 이벤트에 속성으로 추가되지 않습니다.
	보안 인시던트 MITRE ATT&CK 기술을 MISP 이벤트에 로컬 갤럭시로 동기화	보안 인시던트 MITRE-ATT&CK™ 기술을 이벤트의 로컬 갤럭시로 동기화 ServiceNow AI Platform SIR 하는 MISP 옵션입니다.

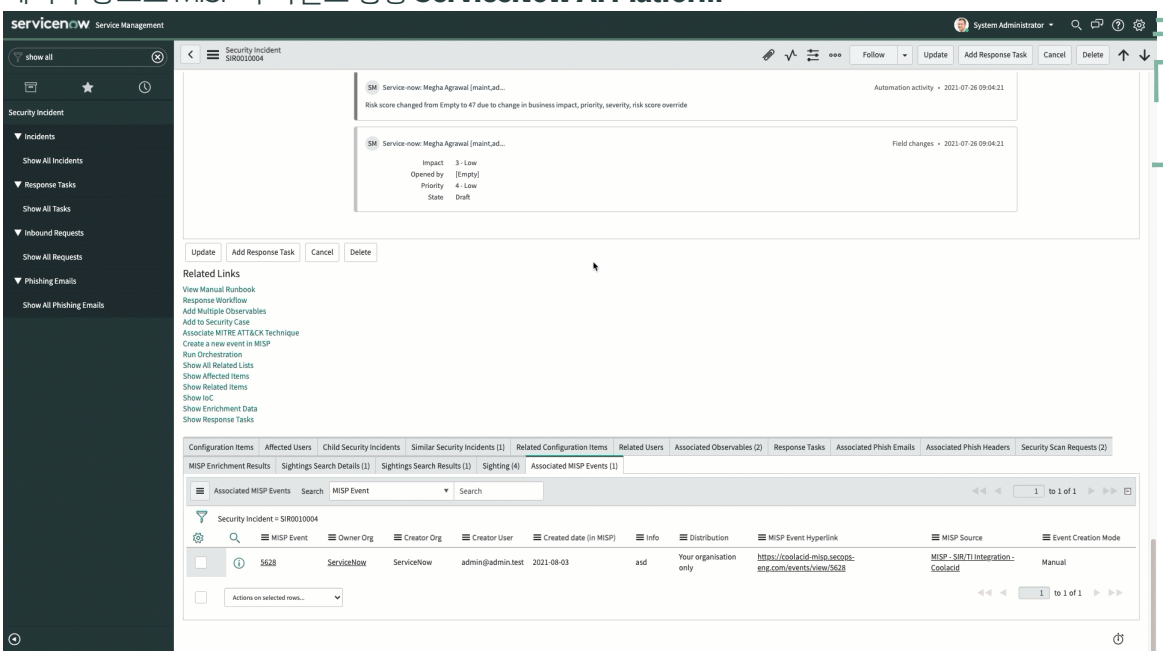
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드		설명
	보안 인시던트 MITRE ATT&CK 기술을 MISP 이벤트에 전역 갤럭시로 동기화	보안 인시던트 MITRE-ATT&CK™ 기술을 이벤트의 전역 갤럭시로 동기화 ServiceNow AI Platform SIR 하는 MISP 옵션입니다.
	MISP 이벤트에 태그 추가	ServiceNow에서 작성된 이벤트에 MISP 태그를 추가할 수 있는 옵션입니다. 이 옵션은 다음 옵션을 표시합니다. ○ 로컬(태그):선택한 태그가 MISP 이벤트에 로컬 태그로 추가됩니다. ○ 전역(태그):선택한 태그가 MISP 이벤트에 전역 태그로 추가됩니다.

5. 새 **MISP** 이벤트 작성을 클릭합니다.

다음 예는 에서 MISP이벤트를 생성하여 보안 인시던트의 결과를 볼 수 있음을 보여줍니다. 다음 예와 같이 작업 메모, 인스턴스의 이벤트 ServiceNow AI Platform 및 서버의 이벤트를 MISP 볼 수도 있습니다.

에서 수동으로 MISP의 이벤트 생성 **ServiceNow AI Platform**



다음과 같은 방법으로 결과를 볼 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 성공 메시지가 보안 인시던트 페이지 상단에 나타납니다. 인스턴스에서 이벤트 상세 정보를 ServiceNow AI Platform 볼 수 있으며 서버에 표시되는 MISP 대로 볼 수도 있습니다.
- 작업 메모에서 자세한 내용이 포함된 성공 메시지를 볼 수 있습니다. 인스턴스에 있는 이벤트 상세 정보를 ServiceNow AI Platform 볼 수 있으며 서버에 표시되는 대로 볼 수도 있습니다 MISP .
- 연결된 MISP 이벤트 관련 목록에서 보안 인시던트 및 자원과 관련된 이벤트를 볼 수 있습니다MISP.

이벤트에 속성 **MISP** 추가

이벤트에 유형, 범주 및 이벤트에 대한 기타 상황별 정보와 같은 속성을 이벤트에 추가합니다.

시작하기 전에

- 다음 항목 검토: MISP 사용자 역할 및 권한 양방향 기능을 사용하기 위한 것입니다 MISP .
- 속성을 추가하거나 업데이트하는 이벤트가 사용자와 동일한 조직에 MISP 속하는지 확인합니다.
- 필요한 역할: sn_sec_misp.write

프로시저

1. 다음으로 이동 모두 〉 **MISP** 〉 연결된 **MISP** 이벤트.
   보안 인시던트에서 연결된 MISP 이벤트 관련 목록으로 이동할 수도 있습니다.
2. 속성을 추가할 MISP 이벤트를 클릭합니다.
3. **MISP** 이벤트에 속성 추가를 클릭합니다.
4. 이벤트에 속성 추가 대화 상자에서 상세 정보를 입력합니다.

이벤트에 속성 추가 대화 상자

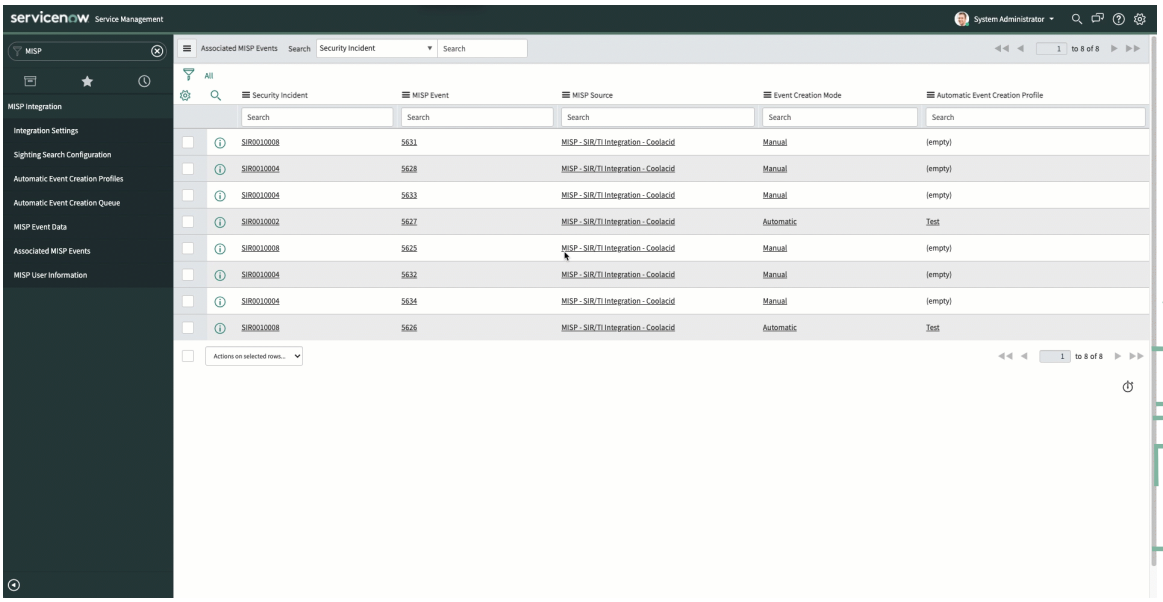
필드	설명
값	속성의 실제 값입니다. 선택한 속성 유형에 유효한 값을 기준으로 한 값에 대한 데이터를 입력합니다. 예를 들어 ip-src(소스 IP 주소) 유형의 속성의 경우 11.11.11.11이 유효한 값입니다. **주:** 이벤트와 컨텍스트를 공유하는 속성 또는 옵저버블만 선택할 수 있습니다. 옵저버블은 이미 의 속성을 MISP가질 수 없습니다.
범주	속성의 범주입니다. 범주는 이 속성에 대한 맬웨어의 측면을 설명합니다. 예를 들어 맬웨어 또는 네트워크 활동의 지속성 메커니즘이 있습니다.
유형	범주를 설명하는 유형입니다. 예를 들어 공격자가 공격에 IP 주소를 사용하는 경우 원본 이메일 주소 또는 첨부 파일을 통해 전송된 파일은 모두 맬웨어의 페이로드 전달을 설명할 수 있습니다. 이러한 유형의 속성에는 페이로드 제공 범주가 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
배포	이 속성을 볼 수 있는 사용자입니다. 분포는 속성에 의해 상속됩니다. 가장 제한적인 설정이 우선합니다.
속성을 IDS 서명으로 사용	에서 SIR악성으로 표시된 옵저버블 . 의 MISP 해당 속성도 true로 표시됩니다.
설명	속성에 대해 추가하는 코멘트입니다.

다음 예는 연결된 MISP 이벤트 목록에서 탐색하여 이벤트 레코드 5627을 보고 이벤트에 속성을 추가할 수 있음을 보여줍니다. 속성에는 값(testdomain.com), 범주(외부 분석), 유형(도메인)이 포함됩니다. IDS를 활성화할 수도 있습니다. 다음 예와 같이 이벤트 기록의 성공 메시지는 속성이 이벤트에 추가되었음을 보여줍니다.

MISP 이벤트에 속성 추가



5. **MISP** 이벤트에 속성 추가를 클릭합니다.

결과
속성 섹션에서 추가된 속성을 볼 수 있습니다.

이벤트에 태그 **MISP** 추가

태그를 ServiceNow AI Platform MISP 추가하여 이벤트 또는 속성을 분류합니다. 전역적으로 태그 지정을 사용하여 분류를 활성화하거나, 분류 중에 이벤트가 수정되는 것을 원하지 MISP 않을 때 태그를 로컬에서 사용할 수 있습니다.

시작하기 전에

- 다음 항목 검토: MISP 사용자 역할 및 권한 양방향 기능을 사용하기 위한 것입니다 MISP .
- 편집 중인 이벤트가 사용자와 동일한 조직에 MISP 속해 있는지 확인합니다.
- 사용할 수 있는 태그와 갤럭시는 소스 및 해당 배포 권한을 기반으로 MISP 합니다.
- 필요한 역할: sn_sec_misp.write

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 모든 인시던트 표시.
2. 태그를 추가할 이벤트가 포함된 보안 인시던트를 선택합니다.
3. 모든 관련 목록 표시 및 MISP 보강 결과 관련 목록을 클릭합니다.
4. 보강 결과 목록에서 이벤트 ID를 클릭합니다.
   다음에서 탐색할 수도 있습니다. **MISP** 〉 연결된 **MISP** 이벤트 모듈.
5. MISP 이벤트 기록을 검토합니다.

MISP 이벤트 양식 뷰

필드	설명
이벤트 ID	이벤트를 처음 만들거나 서버로 가져올 MISP 때 MISP 할당된 이벤트 ID입니다.
UUID	이벤트와 속성을 고유하게 식별하는 ID입니다.
작성자 조직	인스턴스에서 이벤트를 MISP 생성한 조직입니다.
소유자 조직	인스턴스에서 이벤트를 MISP 소유한 조직입니다. 이 필드는 관리자에게만 표시됩니다.
작성자 사용자	에서 MISP이벤트를 생성한 사용자입니다.
마지막 변경	이벤트가 마지막으로 수정된 날짜입니다.
MISP 소스	MISP 이벤트가 생성된 소스입니다.
작성된 날짜(MISP)	이벤트를 만들었거나 서버에서 처음 가져온 MISP 날짜입니다.
위협 수준	이벤트의 위험 수준입니다. 인시던트는 세 가지 위협 범주(낮음, 중간, 높음)로 분류할 수 있습니다. 이 필드는 정의되지 않은 상태로 둘 수 있습니다. 옵션은 다음과 같습니다. ○ 낮음: 일반 대량 맬웨어 ○ 중간: 지능형 지속 위협(APT) ○ 높음: 정교한 APT 및 0일 공격
분석	다음과 같은 가능한 옵션이 있는 이벤트 분석의 현재 스테이지입니다. ○ 초기: 분석이 이제 막 시작되었습니다. ○ 진행 중: 분석이 진행 중입니다. ○ 완료됨: 분석이 완료되었습니다.
배포	개별 속성의 분포입니다. 속성의 배포 수준은 이벤트와 다를 수 있습니다.
게시 날짜:	이벤트 게시 여부의 상태입니다. 게시하면 이벤트의 속성을 모든 적격 익스포트에 사용할 수 있으며 이벤트 경보를 구독한 사용자에게 알릴 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
MISP 이벤트 하이퍼링크	MISP 서버에 저장된 MISP 이벤트에 연결합니다.
정보	이벤트에 대한 간단한 설명입니다.
태그(로컬)	호스트 조직의 MISP 인스턴스에서 동기화 및 익스포트 필터링을 위한 태그 지정을 활성화하는 데 사용할 수 있는 태그입니다. MISP 로컬 태그를 사용할 때 이벤트가 수정되지 않습니다. 로컬 태그는 다른 MISP 인스턴스 및 공유 커뮤니티와 동기화되기 전에 항상 제거됩니다.
태그(전역)	다른 인스턴스 및 공유 커뮤니티와 MISP 공유하고 동기화하기 위해 전역적으로 사용할 수 있는 태그입니다. 인스턴스에 전역 태그를 MISP 추가할 때 이벤트를 수정할 수 있습니다.
갤럭시(로컬)	호스트 조직의 MISP 인스턴스에서 동기화 및 익스포트 필터링에 사용할 수 있는 갤럭시입니다. MISP 로컬 갤럭시를 사용할 때 이벤트는 수정되지 않습니다. 이러한 로컬 은하는 다른 MISP 인스턴스 및 공유 커뮤니티와 동기화되기 전에 항상 제거됩니다.
갤럭시(전역)	다른 MISP 인스턴스 및 공유 커뮤니티와 공유하고 동기화할 수 있는 전역적으로 사용할 수 있는 갤럭시입니다. 글로벌 갤럭시 MISP 를 추가할 때 이벤트를 수정할 수 있습니다.

6. 로컬 또는 전역 태그를 편집하려면 편집 아이콘 다음 옵션 중 하나에서 다음을 수행합니다.

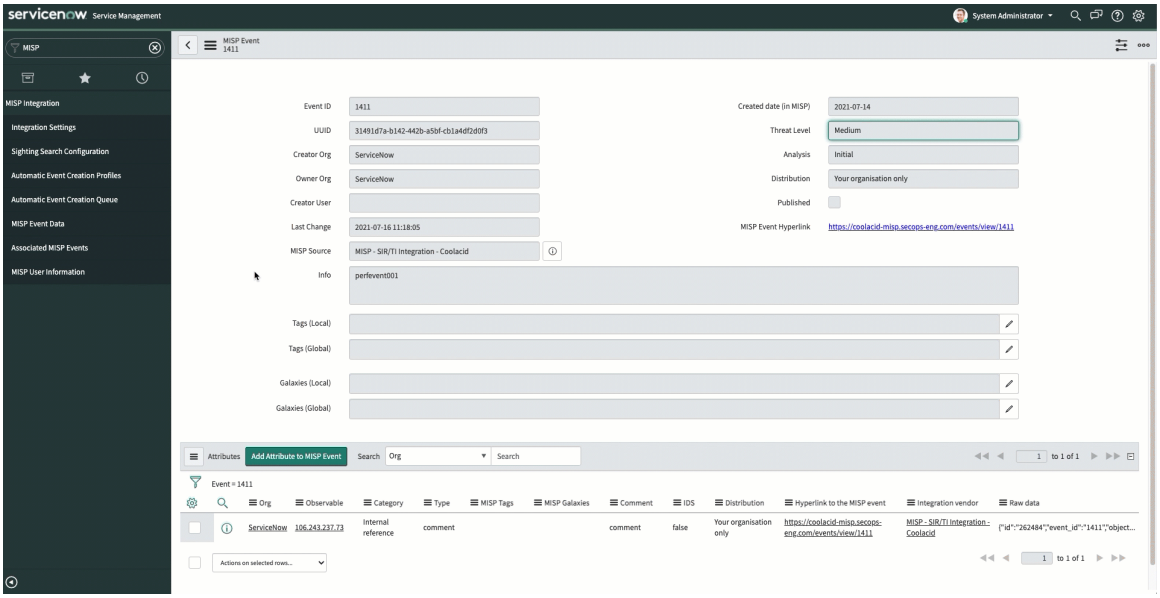
- 태그(로컬)
- 태그(전역)

7. MISP 이벤트 태그 대화 상자에서 태그 이름을 입력하여 태그를 검색하고 추가합니다.
8. **MISP** 이벤트에 태그 업데이트를 클릭합니다.

다음 예에서는 로컬 태그에 대한 편집 아이콘을 클릭하여 C3, 애드웨어, C2 및 봇넷 3101 태그를 검색 및 추가하고 MISP 서버를 태그로 업데이트할 수 있음을 보여줍니다. 확인 메시지는 모든 태그가 에서 업데이트 MISP되었음을 보여줍니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

MISP 이벤트로 태그 업데이트



9. 기록의 변경 내용을 보려면 성공 메시지에서 폼 다시 로드 를 클릭합니다.

결과
서버에서 태그가 업데이트되었습니다 MISP .

갤럭시를 이벤트 또는 속성으로 **MISP** 업데이트

은 ServiceNow AI Platform MISP 하계를 추가하거나 제거하여 이러한 객체를 인스턴스에서 클러스터 MISP 로 분류하고 이벤트 MISP 또는 속성에 연결할 수 있습니다.

시작하기 전에

- 다음 항목 검토: MISP 사용자 역할 및 권한 양방향 기능을 사용하는 MISP 데 필요합니다.
- 로컬 갤럭시를 추가하려면 통합을 구성한 사용자가 해당 MISP 서버의 호스트 조직에 속해야 합니다.
- 사용할 수 있는 태그와 갤럭시는 소스와 해당 배포 권한을 기반으로 MISP 합니다.
- 필요한 역할: sn_sec_misp.write

프로시저

1. 다음 옵션 중 하나에서 편집 아이콘

- 갤럭시(로컬)
- 갤럭시(전역)

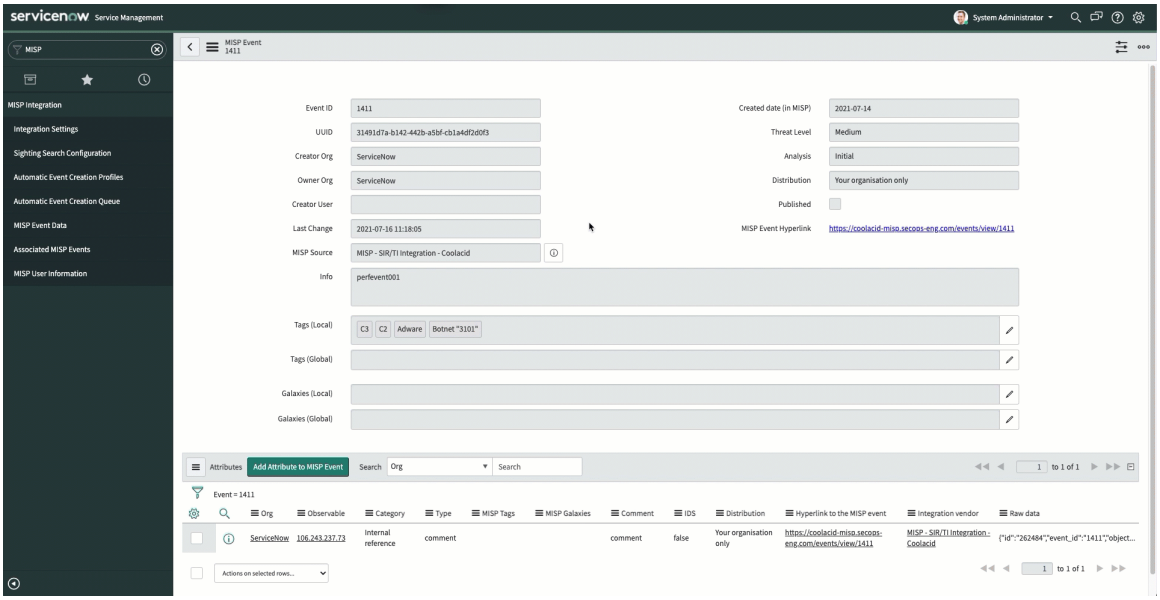
2. MISP 이벤트 갤럭시 대화 상자에서 입력하고 검색하여 태그를 추가합니다.

3. 갤럭시를 **MISP** 이벤트로 업데이트를 클릭합니다.

다음 예제에서는 로컬 갤럭시의 편집 아이콘을 클릭하고, 사용되지 않는 네임스페이스를 선택하고, 엔터프라이즈 공격 - 공격 패턴 갤럭시를 선택하고, 클러스터 정보를 추가하는 방법을 보여줍니다. 갤럭시 정보가 업데이트되면 성공 메시지를 볼 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

갤럭시 정보를 **MISP** 이벤트로 업데이트



서버에서 갤럭시가 성공적으로 MISP 업데이트되었습니다.

4. 기록의 변경 내용을 보려면 성공 메시지에서 폼 다시 로드 를 클릭합니다.

향상된 결과를 사용하여 **MISP** 정보 롤업 **MITRE-ATT&CK**

정보의 자동 롤업을 활성화하지 않은 경우 MISP 보강 결과를 수동으로 롤업 MISP 합니다.

시작하기 전에

필요한 역할: sn_si.analyst

이 태스크 정보

기본 시스템 자동 추출 규칙을 사용하여 통합에서 MITRE-ATT&CK 정보를 임포트합니다 MISP . 은 MISP Integration for Security Operations 하와 MISP 태그에 대한 MISPMISP 두 가지 기본 시스템 MITRE-ATT&CK 기술 추출 규칙을 소개합니다. 의 MITRE-ATT&CK자동 추출 규칙에 대한 자세한 내용은 MITRE-ATT&CK 정보를 가져오기 위한 자동 추출 기술 규칙을 참조하십시오.

활성화한 경우 다음의 자동 롤업 MITRE-ATT&CK 정보 사용 MISP 보강 결과 보안 인시던트에 정보가 자동으로 롤업됩니다. 자동 롤업을 활성화하지 않은 경우 이 작업을 수동으로 수행할 수 있습니다.

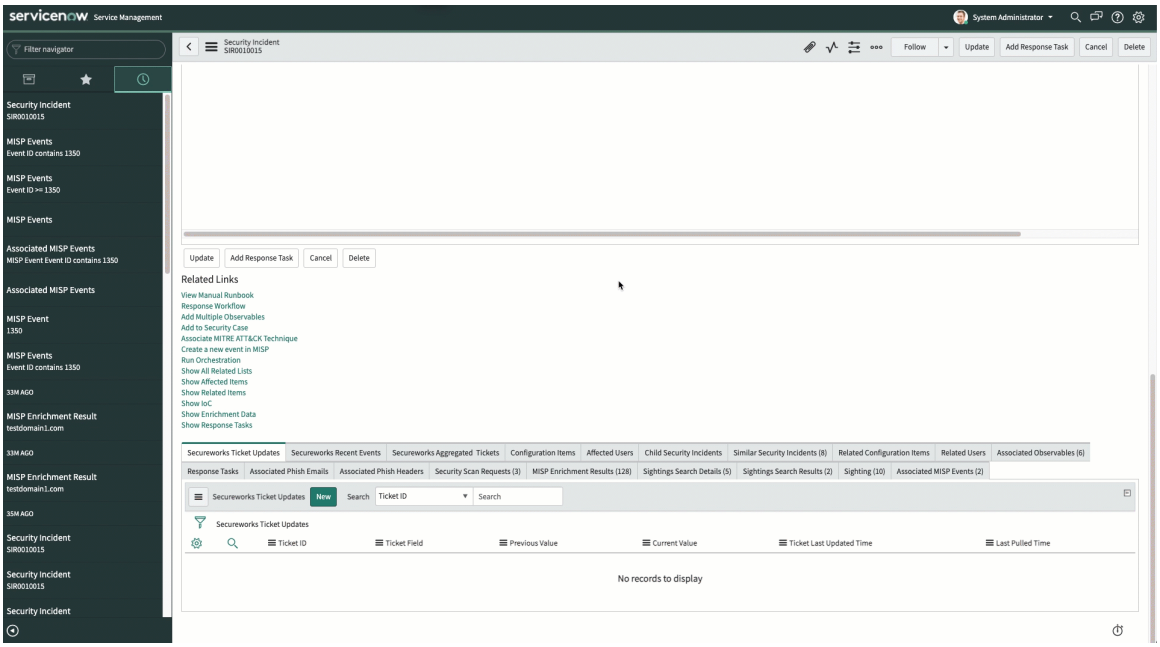
프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 모든 인시던트 표시.
2. 정보를 보강할 보안 인시던트를 MITRE-ATT&CK 선택합니다.
3. 모든 관련 목록 표시 및 **MISP** 보강 결과 탭을 클릭합니다.
4. 옵저버블을 선택하고 작업 메뉴에서 **MITRE ATT&CK** 정보를 SI로 롤업을 클릭합니다.
   여러 옵저버블을 선택한 다음 정보를 롤업할 수 있습니다.
5. 변경 사항을 확인하려면 다시 로드를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음 예에서는 옵저버블을 선택하고 보강 결과를 보안 인시던트에 롤업 MISP 하는 방법을 보여줍니다.

MITRE 정보를 보안 인시던트에 롤업



결과
카드를 보고 MITRE-ATT&CK MISP 보강 결과가 보안 인시던트로 롤업되었는지 확인할 수 있습니다.

OPSWAT Metadefender 통합

OPSWAT Metadefender 외부 공급업체 Metadefender 스캐너에서 탐지된 위협 데이터를 추적, 우선순위 지정 및 해결을 위해 애플리케이션에 다운로드할 위협 인텔리전스 수 있습니다.

탐색

- OPSWAT Metadefender 통합 개요
- 위협 인텔리전스 통합

설정

통합 활성화 및 구성 OPSWAT Metadefender

사용

옵저버블에 대한 조회 수행

개발

- ServiceNow 보안 운영 통합 개발 가이드라인
- 통합 작성을 위한 팁
- 개발자 교육
- 개발자 설명서
- 애플리케이션과 함께 설치되는 구성요소 찾기

문제 해결 및 도움받기

- 통합 문제 해결
- 보안 운영 커뮤니티에서 질문 또는 답변하기

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 알려진 오류 포털에서 알려진 오류 문서 검색
- 연락처 고객 서비스 및 지원

OPSWAT Metadefender 통합 개요

OPSWAT Metadefender 는 여러 맬웨어 방지 시스템에 대한 액세스를 제공하고 와 쉽게 통합 보안 운영되는 보안 솔루션입니다.

통합을 사용하려면 OPSWAT Metadefender 먼저 플러그인을 활성화하고 통합을 구성해야 합니다. 필요한 경우 X509 SSL 인증을 업데이트할 수도 있습니다.

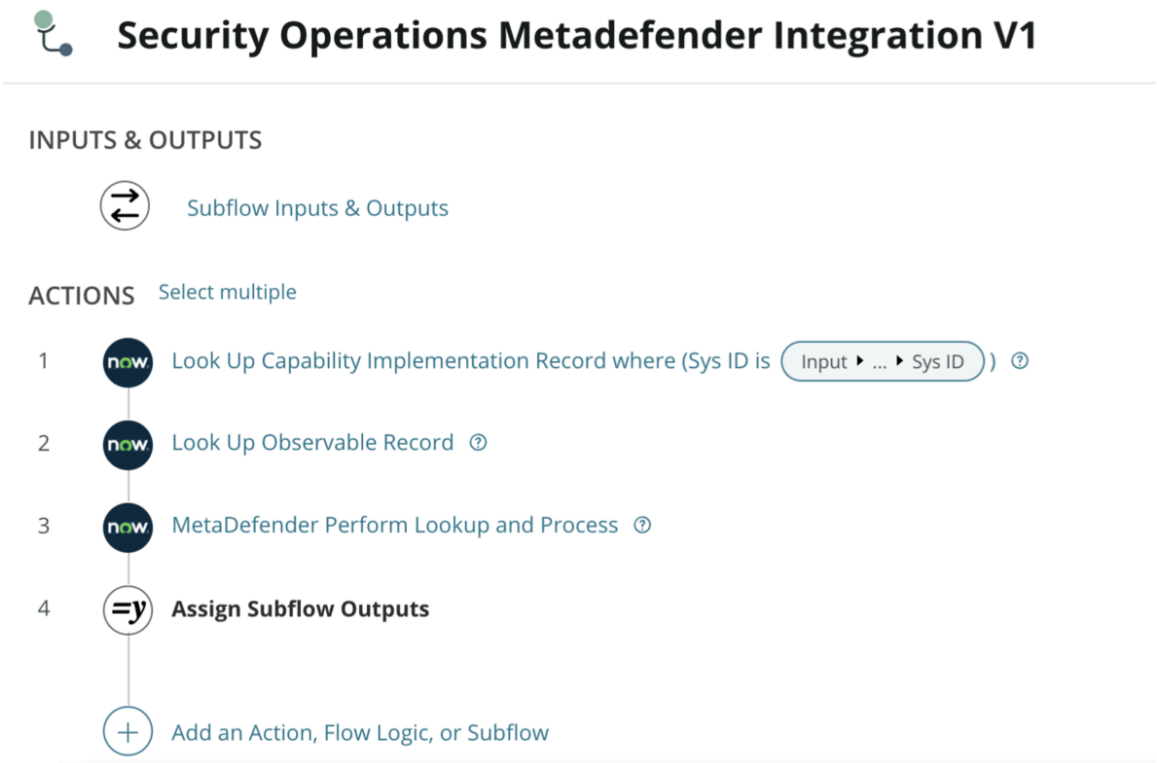
위협 조회 **- OPSWAT Metadefender** 플로우

위협 조회 - OPSWAT Metadefender 플로우는 선택한 옵저버블에 대한 조회를 수행합니다. 옵저버블이 OPSWAT Metadefender에서 인식하는 형식인 경우 옵저버블에 맬웨어가 있는지 검사되고 결과가 반환됩니다.

이 흐름은 하나 이상의 옵저버블에서 위협 조회를 수행하고 OPSWAT Metadefender 구현이 선택될 때 트리거 보안 운영 통합 - 위협 조회 기능 됩니다. 자세한 내용은 옵저버블에 대한 조회 수행 문서를 참조하십시오.

필요한 역할: sn_si.admin

위협 조회 **- OPSWAT Metadefender** 플로우



이 플로우에서 사용하는 활동에 대한 자세한 내용은 다음 문서를 일반 Security Operations 통합 플로우 및 오케스트레이션 활동참조하십시오.

통합 활성화 및 구성 **OPSWAT Metadefender**

통합을 사용하려면 OPSWAT Metadefender 먼저 다음 ServiceNow Store에서 다운로드해야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 에서 통합을 다운로드합니다. ServiceNow Store.
2. 통합이 완료되면 OPSWAT 포털에 액세스하고 Metadefender 클라우드 API 키를 가져옵니다.
3. 인스턴스에서 다음으로 이동합니다. 보안 운영 〉 통합 〉 통합 구성.
   사용 가능한 보안 통합은 일련의 카드로 표시됩니다.
4. OPSWAT Metadefender 카드에서 구성을 클릭합니다.
5. OPSWAT 포털에서 획득한 **API** 키를 입력하거나 붙여넣습니다.
6. 제출을 클릭합니다.

결과
구성된 후에는 OPSWAT Metadefender를 선택하여 보안 인시던트의 옵저버블 위협 인텔리전스 과 옵저버블에 대한 조회를 수행할 수 있습니다.

관련 정보

옵저버블에 대한 조회 수행

X.509 인증서 업데이트

통합에 SSL 연결이 필요한 경우 외부 공급업체 벤더가 제공한 인증서를 아직 신뢰 ServiceNow 하지 않거나 만료된 경우가 있습니다. 이 작업은 선택 사항입니다.

시작하기 전에
필요한 역할: admin

프로시저

1. 외부 공급업체 벤더로부터 SSL 인증서를 받습니다.
   예를 들어, 다음과 같이 Firefox 브라우저의 SSL 엔드포인트에서 X.509 인증서(PEM)를 임포트할 수 있습니다.

   a. 브라우저 주소 표시줄에 엔드포인트 URL을 입력합니다.
      예: https://<3rdparty>/.

   b. 주소란에서 자물쇠 아이콘을 클릭합니다.

   c. 추가 정보를 클릭하고 보안 탭을 클릭합니다.

   d. **View** Certificate(인증서 보기)를 클릭하고 Detail(세부 정보) 탭을 클릭합니다.

   e. 내보내기를 클릭하여 PEM을 로컬 파일 시스템에 저장합니다.

   f. 저장된 파일을 텍스트 편집기 도구에서 열고 내용을 클립보드에 복사합니다.
      `-----BEGIN CERTIFICATE-----`로 시작하고 `-----END CERTIFICATE-----`로 끝나야 합니다.

2. 다음으로 이동 시스템 정의 〉 인증서.
3. 새로 만들기를 클릭하고 통합에 대한 새 기록을 생성합니다.
4. **PEM** 인증서에서 이전에 다운로드하여 클립보드에 복사한 인증서를 붙여넣습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. ID 제공자 기록에 인증서를 추가합니다.
   a. 다음으로 이동 복수 제공자 **SSO** 〉 **ID** 제공자.
   b. 새 인증서를 만들 활성 기본 ID 제공자를 선택합니다.
   c. 아래로 스크롤하여 **X.509** 인증서 관련 목록을 클릭하고 편집을 클릭합니다.
   d. 새로 만든 인증서를 선택됨 열로 이동합니다.
6. 저장을 클릭합니다.
   기록의 다른 필드는 자동으로 생성됩니다.

> **주:**
> 만료된 인증서가 있는 경우 인증서를 제거해야 합니다. 만료된 인증서를 제거하는 방법에 대한 자세한 내용은 KB0691439 만료되는 SAML 인증서 교체 를 참조하십시오.

VirusTotal 통합

통합을 VirusTotal 통해 의심스러운 IP 주소, 파일, 파일 해시 및 URL 주소 분석을 요청하여 해당 주소 및 파일이 악성인지 여부를 확인하는 데 도움이 될 수 있습니다.

탐색	설정
위협 인텔리전스 통합	• VirusTotal 통합 설정 • VirusTotal 통합 활성화 및 구성
사용	**개발**
• 옵저버블에 대한 조회 수행 • 위협 조회 - VirusTotal 워크플로우	• ServiceNow 보안 운영 통합 개발 가이드라인 • 통합 작성을 위한 팁 • 개발자 교육 • 개발자 설명서 • 애플리케이션과 함께 설치되는 구성요소 찾기

문제 해결 및 도움받기

- 통합 문제 해결
- 보안 운영 커뮤니티에서 질문 또는 답변하기
- 알려진 오류 포털에서 알려진 오류 문서 검색
- 연락처 고객 서비스 및 지원

VirusTotal 통합 설정

VirusTotal 는 의심스러운 파일 및 URL을 분석하고 바이러스, 웜, 트로이 목마 및 모든 종류의 맬웨어를 신속하게 탐지할 수 있도록 하는 무료 서비스입니다. 와 쉽게 보안 운영통합됩니다.

통합을 사용하려면 VirusTotal 먼저 플러그인을 활성화하고 적절한 API 키를 추가해야 합니다. 필요한 경우 X509 SSL 인증을 업데이트할 수도 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

VirusTotal 조회 소스를 사용하는 경우 맬웨어가 발견되면 옵저버블이 생성됩니다. IP 조회의 경우 IP 주소를 공유하는 URL의 추가 목록이 생성되고 각 URL에 대해 옵저버블이 생성됩니다.

주:

- 통합을 구현 VirusTotal 하려면 플러그인이 위협 인텔리전스 필요합니다.
- 통합이 VirusTotal 버전 3 API로 업그레이드되었습니다.

VirusTotal 통합 활성화 및 구성

VirusTotal 통합을 사용하려면 먼저 ServiceNow Store.

시작하기 전에
필요한 역할: 관리자
위협 인텔리전스 VirusTotal을 사용하려면 먼저 설치 및 활성화해야 합니다. 통합이 VirusTotal 버전 3 API로 업그레이드되었습니다.

프로시저

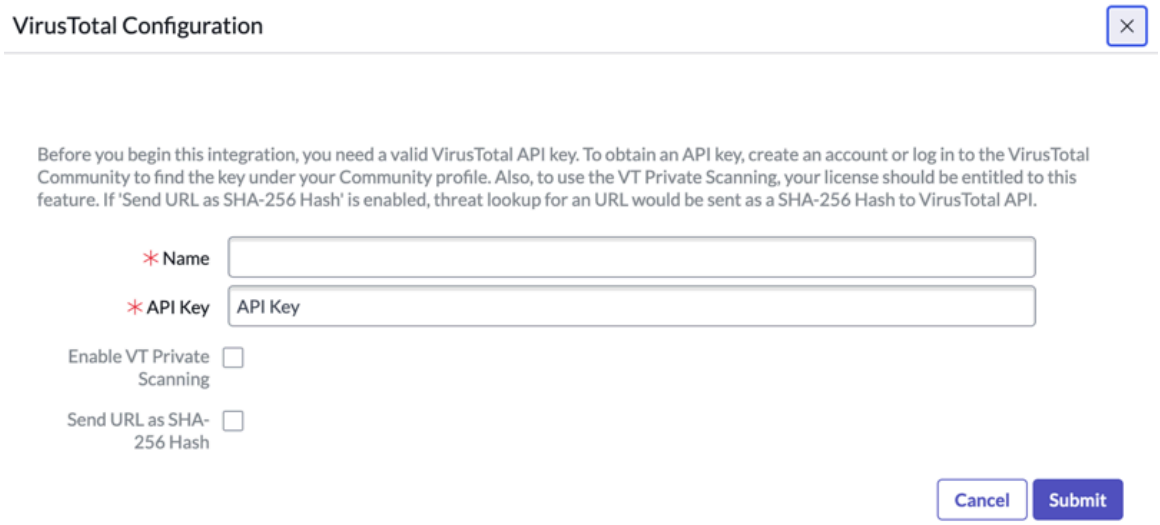
1. 에서 통합을 다운로드합니다. ServiceNow Store.
2. 설치가 완료되면 VirusTotal에 액세스하여 VirusTotal 프로필에서 API 키를 가져옵니다.
3. 인스턴스에서 다음으로 이동합니다. 보안 운영 〉 통합 구성.
   사용 가능한 보안 통합은 일련의 카드로 표시됩니다.
4. VirusTotal 카드에서 구성을 클릭합니다.

VirusTotal 구성

필드	설명
이름	통합의 이름입니다. 예: VirusTotal
API 키	VirusTotal 사이트에서 취득한 **API** 키를 입력하거나 붙여넣습니다.
VT 개인 스캔 사용	개인 정보를 보호하는 방식으로 VirusTotal을 사용하여 파일을 분석하려면 이 확인란을 선택합니다. 이 서비스를 통해 업로드된 파일은 조직 이외의 누구와도 공유되지 않으며 짧은 기간 동안만 VirusTotal에 남아 있습니다. 결과 분석도 일시적이며 VirusTotal 그룹에서만 볼 수 있습니다. 중요사항: VT 개인 스캔을 사용하려면 VirusTotal 라이센스에 이 기능이 있어야 합니다.
SHA-256 해시로 URL 보내기	위협 조회를 위한 해시로 URL을 보내고 통합에서 사용자의 개인 정보를 보호하려면 이 확인란을 선택합니다. 주: 사용하지 않도록 설정하면 URL이 Base64 인코딩으로 VirusTotal API에 전송됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. 제출을 클릭합니다.



결과
구성된 후에는 보안 인시던트에서 옵저버블 위협 인텔리전스 과 옵저버블에 대한 조회를 수행하기 위해 VirusTotal을 선택할 수 있습니다.

관련 정보

옵저버블에 대한 조회 수행

위협 조회 **- VirusTotal** 워크플로우

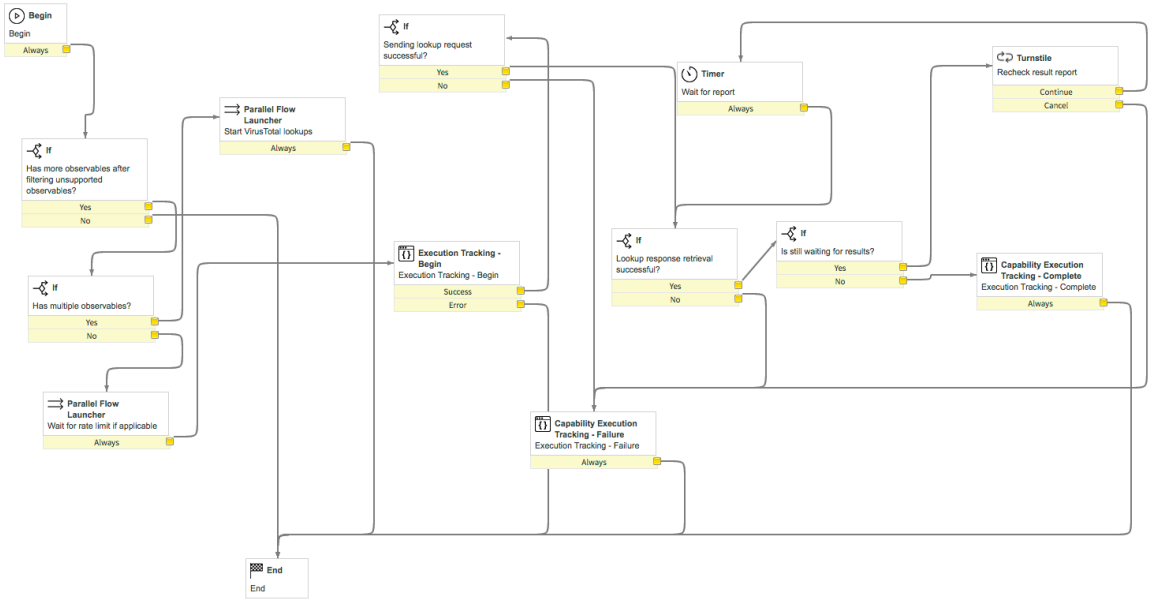
위협 조회 - VirusTotal 워크플로우는 선택한 옵저버블에 대해 조회를 수행합니다. 옵저버블이 에서 인식 VirusTotal하는 유형인 경우 옵저버블에 맬웨어가 있는지 검사되고 결과가 반환됩니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
이 워크플로우는 하나 이상의 옵저버블에 대해 위협 조회를 수행하고 구현이 선택될 때 트리거 보안 운영 통합 - 위협 조회 기능 됩니다 VirusTotal . 자세한 내용은 옵저버블에 대한 조회 수행 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

위협 조회 - **VirusTotal** 워크플로우



이 워크플로우에서 사용하는 활동에 대한 자세한 내용은 을 참조하십시오 일반 Security Operations 통합 플로우 및 오케스트레이션 활동.

WhoisXML API 통합

WhoisXML API 통합을 사용하면 도메인 이름 및 URL에 대한 Whois 조회를 제출하여 URL 옵저버블에 대한 컨텍스트를 얻고 위협에 대한 더 나은 결정을 내릴 수 있습니다.

탐색

위협 인텔리전스 통합

설정

- WhoisXML API 통합 설정
- Security Operations Whois 통합 활성화 및 구성

사용

위협 인텔리전스 - IoC 조회 워크플로우 실행

개발

- ServiceNow 보안 운영 통합 개발 가이드라인
- 통합 작성을 위한 팁
- 개발자 교육
- 개발자 설명서
- 애플리케이션과 함께 설치되는 구성요소 찾기

문제 해결 및 도움받기

- 통합 문제 해결
- 보안 운영 커뮤니티에서 질문 또는 답변하기

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 알려진 오류 포털에서 알려진 오류 문서 검색
- 연락처 고객 서비스 및 지원

WhoisXML API 통합 설정

Whois 통합을 사용하려면 먼저 플러그인을 활성화하고 자격 증명을 추가해야 합니다. 필요한 경우 X509 SSL 인증을 업데이트할 수도 있습니다.

WhoisXML API 통합을 구현하려면 및 WhoisXML API 통합 플러그인이 위협 인텔리전스 필요합니다.

Security Operations Whois 통합 활성화 및 구성

통합 구성 기능을 사용하면 Security Operations Whois 통합을 비롯하여 외부 공급업체 보안 통합을 빠르게 활성화하고 설정할 수 있습니다. Security Operations Whois 통합을 사용하려면 먼저 에서 ServiceNow Store다운로드해야 하며 WhoisXML API의 유효한 계정이 있어야 합니다.

시작하기 전에
위협 인텔리전스 보안 운영 Whois 통합을 사용하려면 먼저 설치 및 활성화해야 합니다.

필요한 역할: 관리자

프로시저

1. 에서 통합을 다운로드합니다. ServiceNow Store.
2. 설치가 완료되면 보안 운영 〉 통합 구성.
   사용 가능한 보안 통합은 일련의 카드로 표시됩니다.
3. Whois API 카드에서 구성을 클릭합니다.
4. WhoisXML API 계정에서 사용자 이름과 암호를 입력합니다.
5. 제출을 클릭합니다.

X.509 인증서 업데이트

통합에 SSL 연결이 필요한 경우 외부 공급업체 벤더가 제공한 인증서를 아직 신뢰 ServiceNow 하지 않거나 만료된 경우가 있습니다. 이 작업은 선택 사항입니다.

시작하기 전에
필요한 역할: admin

프로시저

1. 외부 공급업체 벤더로부터 SSL 인증서를 받습니다.
   예를 들어, 다음과 같이 Firefox 브라우저의 SSL 엔드포인트에서 X.509 인증서(PEM)를 임포트할 수 있습니다.

   a. 브라우저 주소 표시줄에 엔드포인트 URL을 입력합니다.
      예: `https://<3rdparty>/`.

   b. 주소란에서 자물쇠 아이콘을 클릭합니다.

   c. 추가 정보를 클릭하고 보안 탭을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

d. View Certificate(인증서 보기)를 클릭하고 Detail(세부 정보) 탭을 클릭합니다.

e. 내보내기를 클릭하여 PEM을 로컬 파일 시스템에 저장합니다.

f. 저장된 파일을 텍스트 편집기 도구에서 열고 내용을 클립보드에 복사합니다.
`-----BEGIN CERTIFICATE-----`로 시작하고 `-----END CERTIFICATE-----`로 끝나야 합니다.

2. 다음으로 이동 시스템 정의 〉 인증서.

3. 새로 만들기를 클릭하고 통합에 대한 새 기록을 생성합니다.

4. PEM 인증서에서 이전에 다운로드하여 클립보드에 복사한 인증서를 붙여넣습니다.

5. ID 제공자 기록에 인증서를 추가합니다.

a. 다음으로 이동 복수 제공자 **SSO** 〉 **ID** 제공자.

b. 새 인증서를 만들 활성 기본 ID 제공자를 선택합니다.

c. 아래로 스크롤하여 **X.509** 인증서 관련 목록을 클릭하고 편집을 클릭합니다.

d. 새로 만든 인증서를 선택됨 열로 이동합니다.

6. 저장을 클릭합니다.
기록의 다른 필드는 자동으로 생성됩니다.

> **주:**
> 만료된 인증서가 있는 경우 인증서를 제거해야 합니다. 만료된 인증서를 제거하는 방법에 대한 자세한 내용은 KB0691439 만료되는 SAML 인증서 교체를 참조하십시오.

옵저버블 **WhoIs** 워크플로 보강

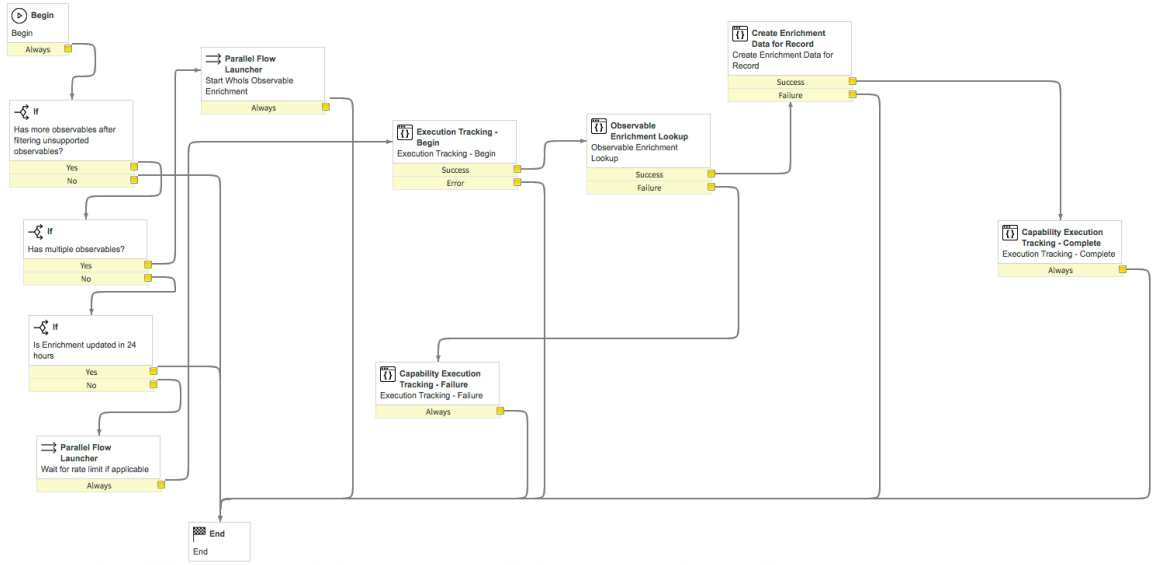
옵저버블 보강 **WhoIs** 워크플로우는 선택한 옵저버블에 대해 보강을 수행합니다. 관찰 가능 항목이 에서 WhoisXML API Integration인식하는 유형인 경우 관찰 가능 항목이 보강됩니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
이 워크플로우는 하나 보안 운영 통합 - 옵저버블 보강 기능 이상의 옵저버블에 대해 보강을 수행하고 WhoIs 구현이 선택될 때 트리거됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵저버블 **WhoIs** 워크플로 보강



이 통합과 관련된 활동은 여기에 설명되어 있습니다. 다른 활동에 대한 자세한 내용은 다음 문서를 참조하십시오 일반 Security Operations 통합 플로우 및 오케스트레이션 활동.

옵저버블 보강 조회 활동

옵저버블 보강 조회 워크플로우 활동은 옵저버블 보강 프로세스를 시작합니다.

옵저버블 보강 조회 활동을 모든 옵저버블 워크플로우와 함께 사용하여 보강을 시작할 수 있습니다.

결과

이 활동의 가능한 결과는 다음과 같습니다.

결과

결과	설명
성공	조회에 성공했습니다.
실패	조회를 수행하는 동안 오류가 발생했습니다. 자세한 오류 정보는 활동 출력 오류에서 확인할 수 있습니다.

입력 변수

입력 변수는 활동의 초기 동작을 결정합니다.

변수	설명
implementation_id	조회를 수행하는 데 사용되는 구현의 시스템 식별자입니다.
domain_id	조회가 수행되는 도메인의 도메인 식별자입니다.
observable_ids	원하는 작업을 수행할 하나 이상의 옵저버블입니다. ID는 워크플로우 입력으로 사용됩니다.
capabilityExcutionId	구현 워크플로우를 시작한 역량의 시스템 식별자입니다. Splunk, Elasticsearch와 같은 통합 기능 구현 워크플로우에만 필요합니다.
task_sys_id	워크플로우와 관련된 모든 작업의 시스템 식별자입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

출력 변수

출력 변수에는 후속 활동에 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
response_data	지정된 도메인에 대해 구현의 API 엔드포인트에서 반환되는 원시 데이터입니다.
mapping_id	보강 매핑의 식별자입니다. 예를 들어 WhoIs 통합은 각각 매핑 ID를 사용하여 IP와 URL의 두 가지 형식으로 데이터를 반환합니다.

Threat Intelligence 오케스트레이션

위협 인텔리전스 오케스트레이션 활동을 통해 사용자는 워크플로우 오케스트레이션을 사용하여 다른 보안 인시던트 또는 다른 시스템에서 위협이 이전에 목격된 적이 있는지 여부를 확인할 수 있습니다.

워크플로우 편집 보안 인시던트 응답 오케스트레이션 또는 사용자 지정 워크플로우 생성에 대한 자세한 내용은 워크플로우 시작하기 및 워크플로우 편집기 워크플로우 편집기를 참조하십시오.

Threat Intelligence 오케스트레이션 설정

를 사용하기 위협 인텔리전스 오케스트레이션전에 CMDB 채우기, MID Server 구성 및 자격 증명 구성을 포함하여 시스템의 다양한 부분을 설정하는 단계를 수행합니다.

시작하기 전에
필요한 역할: 관리자
이를 이용 위협 인텔리전스 오케스트레이션 하려면 도메인 이름으로 완전히 채워진 CMDB가 필요합니다. 자세한 내용은 다음을 참조하십시오. 디스커버리 .

이 태스크 정보

프로시저

1. 플러그인을 활성화합니다 위협 인텔리전스 .
2. MID Server 구성
3. MID 서버 서비스 자격 증명 구성
   이제 워크플로우 내에서 활동을 사용할 위협 인텔리전스 오케스트레이션 준비가 되었습니다.

Threat Intelligence 오케스트레이션 워크플로우 및 활동

기본 시스템에는 인스턴스의 작업을 자동화하는 데 사용할 수 있는 워크플로우 및 워크플로우 활동이 포함되어 있습니다.

위협 인텔리전스 - **IoC** 조회 워크플로우 실행

위협 인텔리전스 - **IoC** 조회 실행 워크플로우는 만료되지 않은 옵저버블이 있는지 확인하고, 있는 경우 조회가 완료로 설정되고 옵저버블의 데이터로 업데이트됩니다.

시작하기 전에
필요한 역할: sn_si.basic

주:
이 워크플로우는 비즈니스 규칙(기존 **IoC** 테이블로 채우기, 조회 큐에 대기, 옵저버블 업데이트)을 활동으로 대체합니다위협 인텔리전스 오케스트레이션.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

조회가 삽입되거나 업데이트되고 조건을 충족하면 조회 비즈니스 규칙이 이 워크플로우를 트리거합니다.

이 태스크 정보
위협 인텔리전스 - **IoC** 조회 실행 워크플로우는 만료되지 않은 옵저버블이 있는지 확인하고, 있는 경우 조회가 완료로 설정되고 옵저버블의 데이터로 업데이트됩니다. 옵저버블과 연결된 모든 표시기가 다시 활성화됩니다.

옵저버블이 만료되면 워크플로우는 조회를 실행하고 만료된 기존 옵저버블의 사이팅 개수 를 증가시킵니다.

상관 관계가 있는 옵저버블이 없으면 표시기가 있는 새 옵저버블이 생성됩니다.

워크플로우 프로세스 활동에는 다음이 포함됩니다.

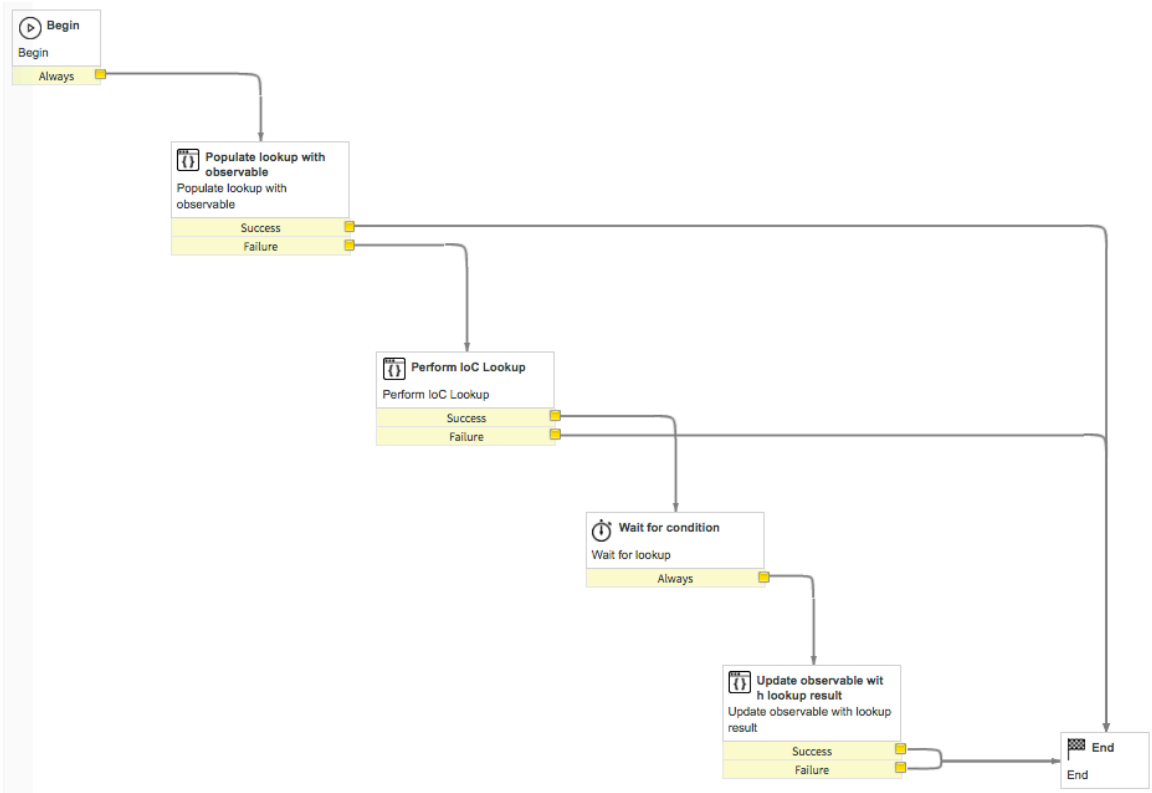
옵저버블 활동으로 조회 채우기

IoC 조회 활동 수행

조회 대기(핵심 활동)

조회 결과 활동으로 옵저버블 업데이트

Threat Intelligence - IoC 조회 워크플로우 실행



옵저버블 활동으로 조회 채우기

만료되지 않은 옵저버블이 발견되면 **Threat Intelligence** 오케스트레이션 - 옵저버블로 조회 채우기 워크플로우 활동은 기존 옵저버블의 데이터를 조회에 제공합니다. 이 활동은 조사 및 정정 프로세스를 가속화할 수 있습니다.

워크플로우에 의해 트리거될 때 조회 및 옵저버블로 채우기 는 활동에 입력으로 제공된 조회의 값 및 유형과 일치하는 조회에 대한 기존 옵저버블을 찾으려고 시도합니다.

옵저버블이 존재하고 만료되지 않은 경우 이 활동은 다음을 수행합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 옵저버블에 있는 정보로 조회를 업데이트합니다.
- 표시기가 비활성 상태인 경우 다시 활성화하고, 발생 횟수를 증가시키고, 마지막으로 표시된 날짜를 업데이트합니다.
- 상태를 완료로 설정합니다.

입력 변수

입력 변수는 활동의 초기 동작을 결정합니다.

입력 변수	설명
scanID〔문자열〕	조회 식별자

출력 변수

출력 변수에는 후속 활동에 사용할 수 있는 데이터가 포함됩니다.

출력 변수	설명
예	유효한 옵저버블 및 업데이트된 조회를 찾았습니다.
아니오	유효한 옵저버블을 찾지 못했습니다. 옵저버블이 누락되었거나 만료되었습니다.

IoC 조회 활동 수행

Threat Intelligence 오케스트레이션 **- IoC** 조회 수행 워크플로우 활동은 지정된 조회를 수행합니다. 이 활동은 조사 및 정정 프로세스를 가속화할 수 있습니다.

워크플로에 의해 트리거되면 **IoC** 조회 수행 은 scanID를 사용하고, 조회 기록을 조회하고, 조회 큐 항목을 만들어 큐에 조회를 추가합니다.

입력 변수

입력 변수는 활동의 초기 동작을 결정합니다.

입력 변수

변수	설명
scanID〔문자열〕	조회 식별자

출력 변수

출력 변수에는 후속 활동에 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
예	조회를 트리거했습니다.
아니오	조회를 트리거하지 않았습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

조회 결과 활동으로 옵저버블 업데이트

위협 인텔리전스 오케스트레이션 - 조회 결과로 옵저버블 업데이트 워크플로우 활동은 옵저버블 기록을 업데이트합니다. 옵저버블이 없는 경우 새 옵저버블을 생성합니다. 이 활동은 정보를 로깅하는 데 유용합니다.

워크플로우에 의해 트리거되면 조회 결과로 옵저버블을 업데이트 하면 새 관찰 수가 포함되도록 기존 옵저버블을 업데이트하고, 메모를 추가하고, 비활성 상태인 경우 표시기를 다시 활성화합니다. 표시기의 발생한 횟수 와 마지막으로 본 날짜도 업데이트됩니다.

상관 관계가 있는 옵저버블이 없는 경우 워크플로우는 다음과 같이 표시기가 있는 새 옵저버블을 생성합니다.

- IoC 조회를 실행합니다.
- 새 옵저버블 생성
- 옵저버블에 대한 표시기 생성
- 옵저버블에 관찰 카운트 를 추가합니다.
- 표시기에 발생한 횟수와 마지막으로 본 날짜를 추가합니다.
- 작성된 조회를 나타내는 메시지를 추가합니다.

.

입력 변수

입력 변수는 활동의 초기 동작을 결정합니다.

입력 변수

변수	설명
scanID〔문자열〕	조회 식별자입니다.

출력 변수

출력 변수에는 후속 활동에 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
예	옵저버블 업데이트 또는 작성에 성공했습니다.
아니오	옵저버블 업데이트 또는 작성에 실패했습니다.

기본 **IoC** 조회 소스 활동 실행

워크플로우 위협 인텔리전스 에 의해 트리거되면 - 기본 **IoC** 조회 소스 실행 조회 요청 ID를 받고 입력한 데이터 값에 따라 여러 조회를 작성합니다.

각 데이터 유형에 대해 각 조회 소스의 지원되는 조회 유형 테이블의 **include_in_bulk** 스캔 열이 평가됩니다. 예일 경우 조회가 조회 요청에 추가됩니다.

입력 변수

입력 변수는 활동의 초기 동작을 결정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

입력 변수

변수	설명
scan_request_id	조회 요청 시스템 식별자

출력 변수

출력 변수에는 후속 활동에 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
생성된 스캔 수	정수

Security Case Management

보안 케이스 관리 은 위협 헌팅에 참여하는 보안 분석가가 해당 환경에서 의심스러운 활동에 대한 정보를 수집할 수 있는 수단을 제공합니다. 보안 인시던트, 옵저버블, CI 및 영향을 받는 사용자와 같은 케이스 관련 기록을 케이스에 추가하여 광범위하고 구체적인 분석을 수용할 수 있습니다.

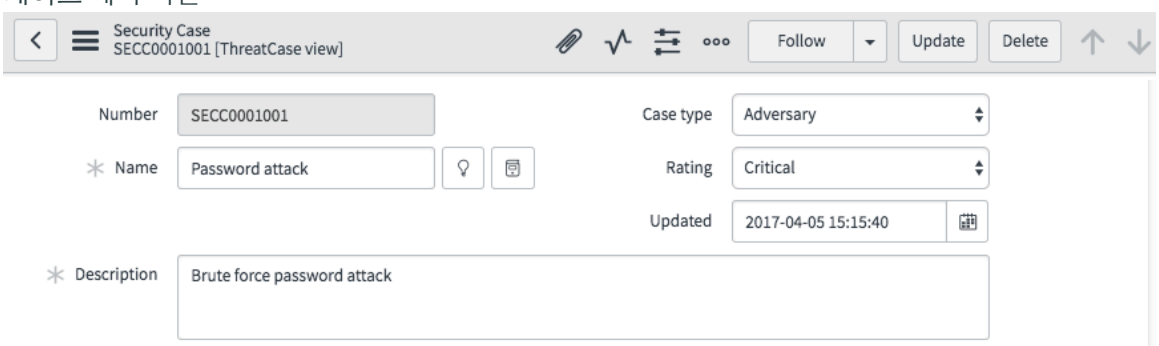
기록 및 관련 정보를 쉽게 피벗할 수 있는 기능을 통해 분석가는 표적 캠페인, 지능형 지속 위협 등에 직면하고 있는지 여부를 평가할 수 있습니다.

보안 케이스는 , 보안 인시던트 응답, 를 비롯한 보안 케이스 관리인스턴스의 다양한 소스에서 생성될 수 있습니다위협 인텔리전스. 구성 항목 [cmdb.ci] 및 사용자 [sys.user] 테이블에서 각각 구성 항목 및 영향을 받는 사용자로부터 케이스를 만들 수도 있습니다. 케이스를 만든 후에는 이러한 각 소스를 사용하여 기존 케이스에 귀중한 분석 자원을 추가할 수도 있습니다.

각 보안 케이스는 헤더 섹션, 추가 케이스 상세 정보가 있는 섹션, 특정 위협을 식별하고 처리하기 위한 논거를 구축하는 데 도움이 되는 레코드 컬렉션이 포함된 케이스 아티팩트 섹션의 세 가지 주요 섹션으로 구성됩니다.

케이스 헤더

케이스 헤더 섹션

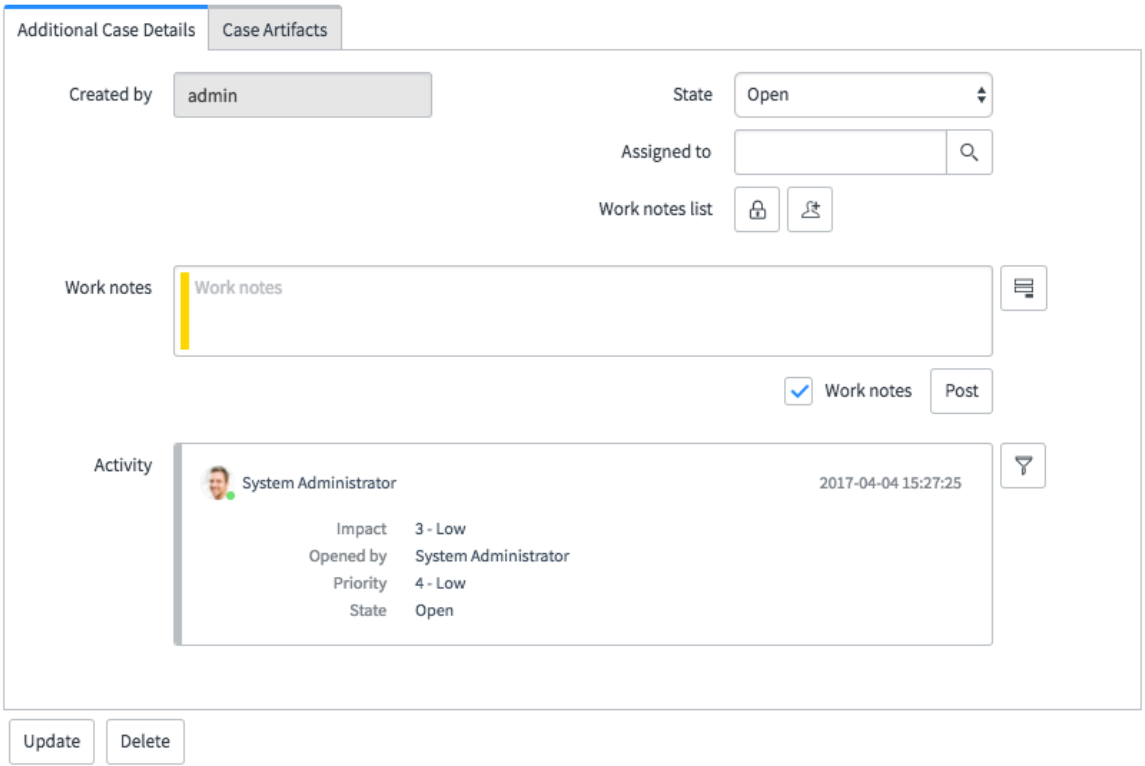


케이스 헤더는 보안 케이스를 식별하고 분류하는 데 사용되는 기본 정보를 제공합니다. 케이스 번호는 SECC 프리픽스를 사용합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

추가 케이스 상세 정보

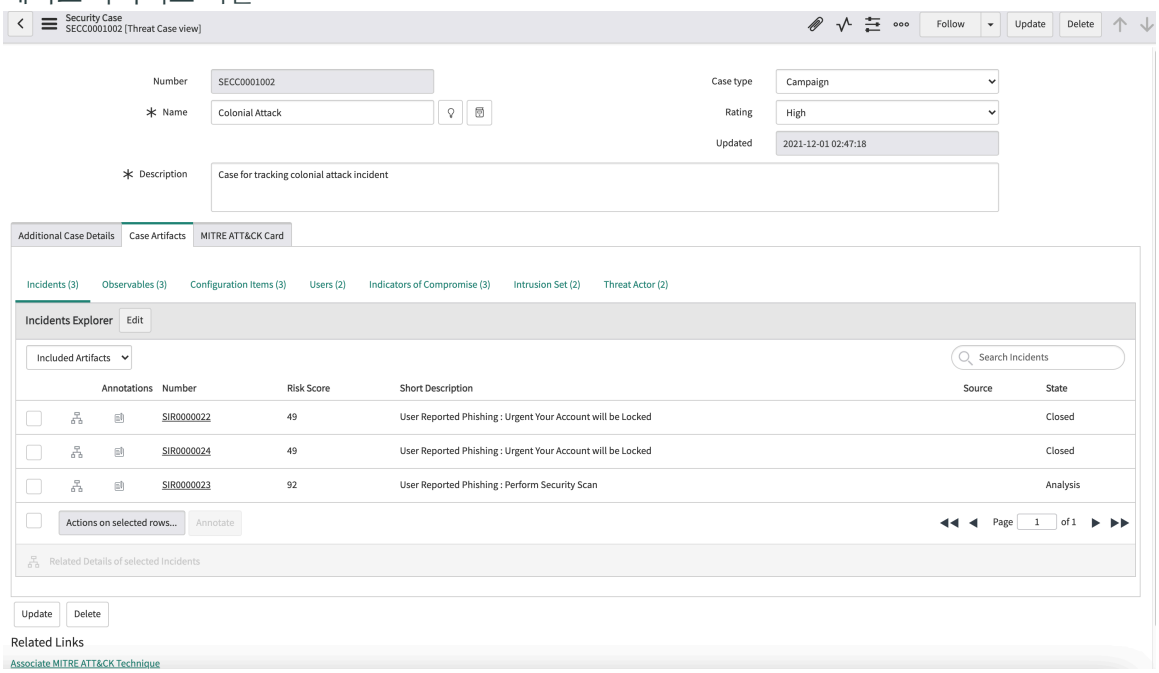
추가 케이스 상세 정보 섹션



추가 케이스 상세 정보 섹션에서는 현재 상태, 케이스에 대해 기록된 작업 메모 및 활동을 포함하여 케이스에 대해 이미 수행된 분석과 관련된 정보를 제공합니다.

케이스 아티팩트

케이스 아티팩트 섹션



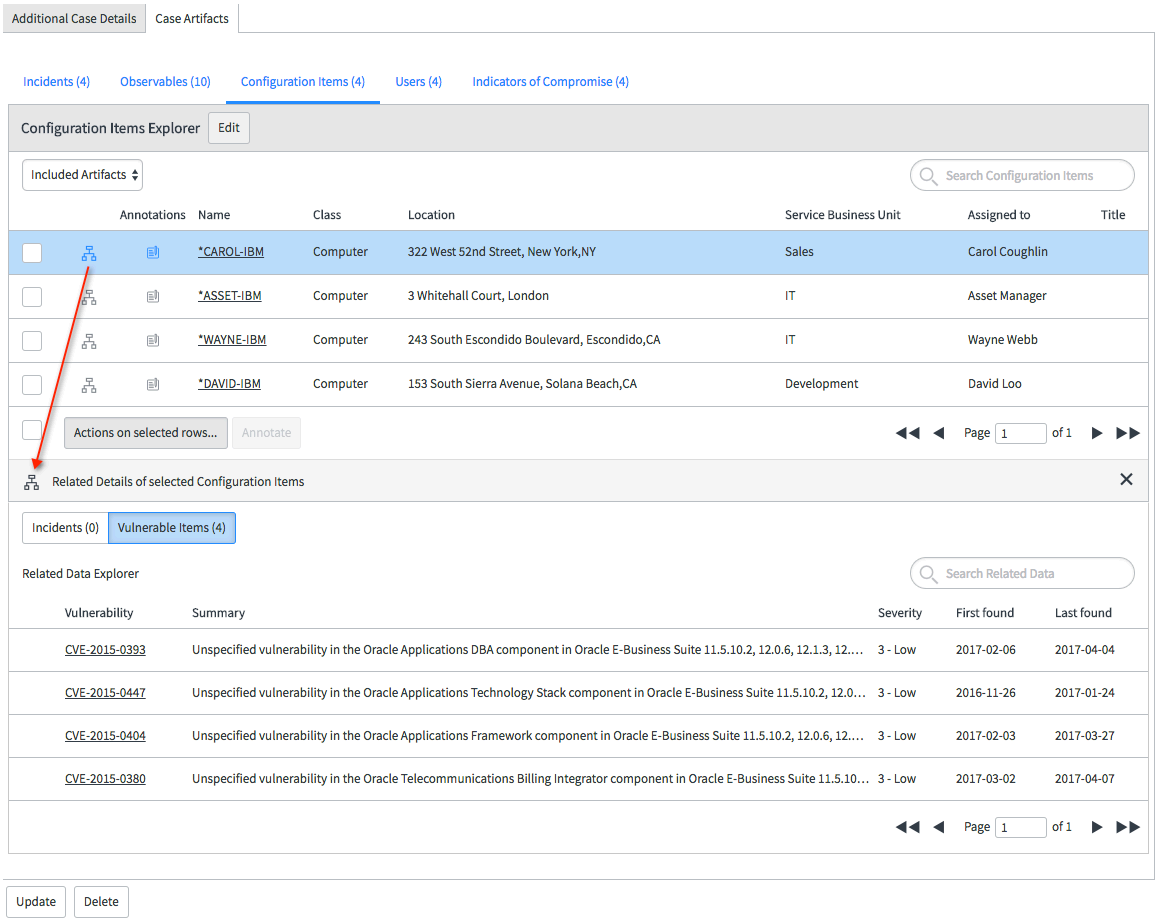
케이스 아티팩트 섹션에서는 보안 케이스에 포함된 일련의 정보 탭을 제공합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

각 탭의 내용 내에서 검색을 수행할 수 있습니다. 이미 안전한 것으로 평가되었거나 조사에 가치가 없는 특정 기록을 제외할 수도 있습니다. 제외된 기록은 삭제되지 않지만 보기에서 숨겨집니다. 필요한 경우 제외된 기록을 보고 다시 추가할 수 있습니다.

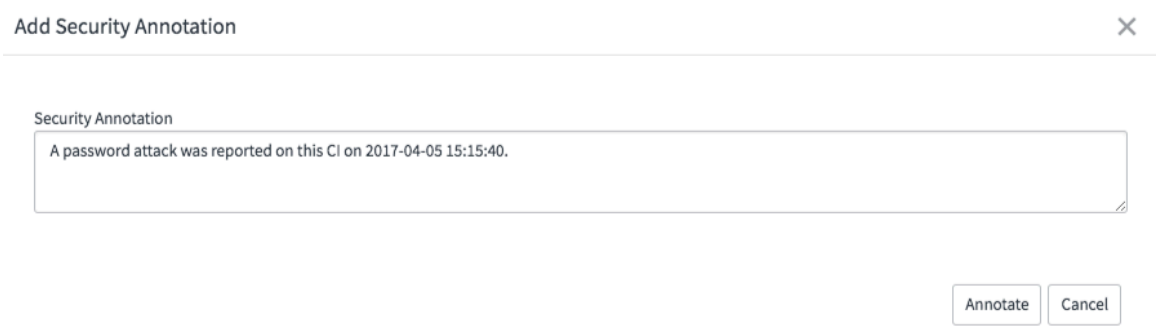
각 탭 내에서 추가 상세 정보 아이콘을 클릭하여 선택한 기록에 대한 관련 정보를 표시할 수 있습니다. 예를 들어 구성 항목 탭을 클릭하여 구성 항목 탐색기를 보고 특정 CI에 대해 추가 상세 정보를 클릭하면 해당 CI와 연관된 인시던트, 취약한 항목 및 주석을 볼 수 있습니다.

케이스 아티팩트 - 관련 상세 정보



기록을 선택하고 케이스 관련 아티팩트에 대해 주석 달기 버튼을 클릭하여 기록에 주석을 추가할 수도 있습니다. 주석은 각 분석가가 특정 아티팩트에 대해 작성할 수 있는 메모입니다.

보안 주석



분석가가 케이스를 검사하는 데 사용할 수 있는 다른 도구는 다음과 같습니다.

- 케이스의 옵저버블에 대해 사이팅 검색을 실행합니다.
- 보안 아티팩트 검색

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 케이스 관리에서 케이스 생성

케이스는 조직을 위협하는 캠페인 또는 상태 행위자에 대한 정보를 추적하는 데 사용됩니다. 케이스를 만든 후에는 아티팩트를 추가하여 단일 케이스 기록 내의 모든 관련 정보를 검토하고 분석할 수 있습니다.

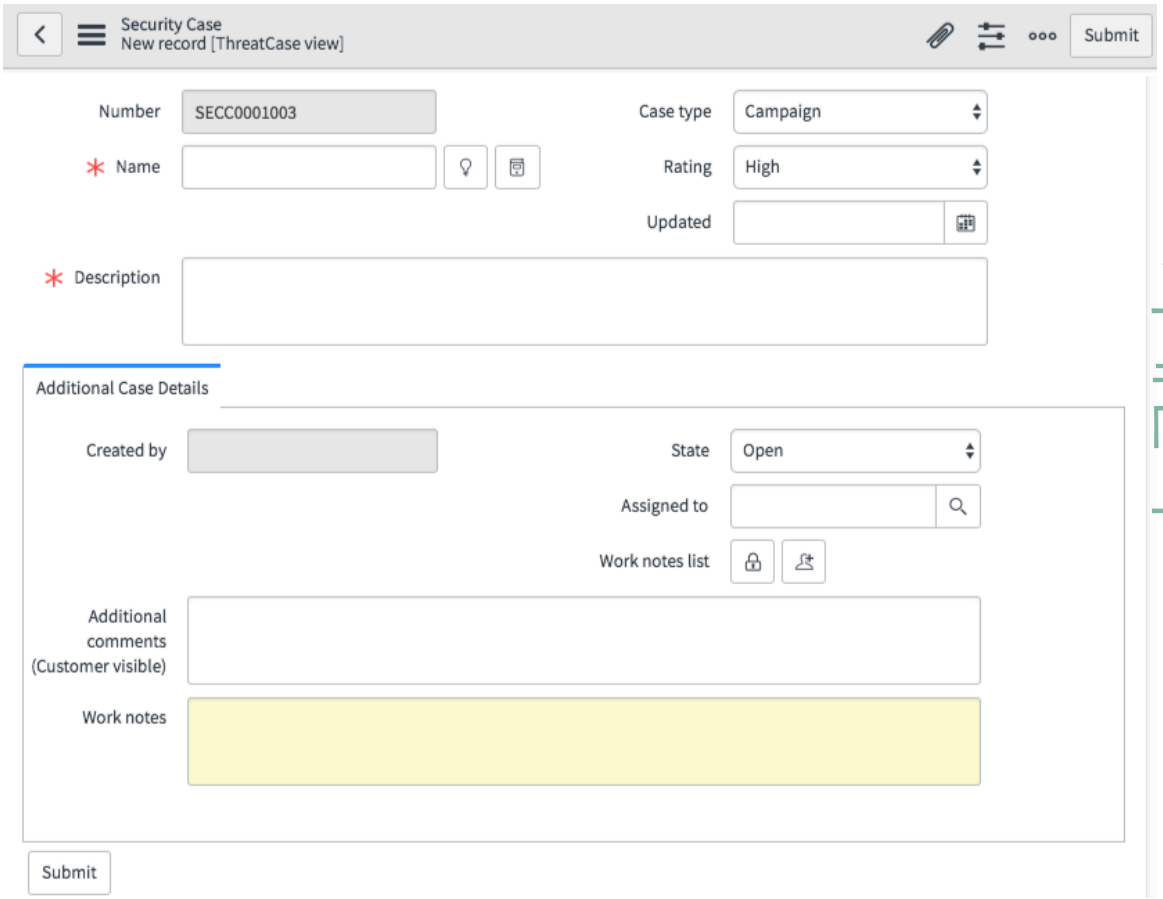
시작하기 전에

필요한 역할: sn_ti.case_use

r

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 케이스 관리 〉 모든 케이스.
   보안 케이스 목록이 열립니다.
2. 새로 만들기를 클릭합니다.
   보안 케이스 화면이 열립니다.



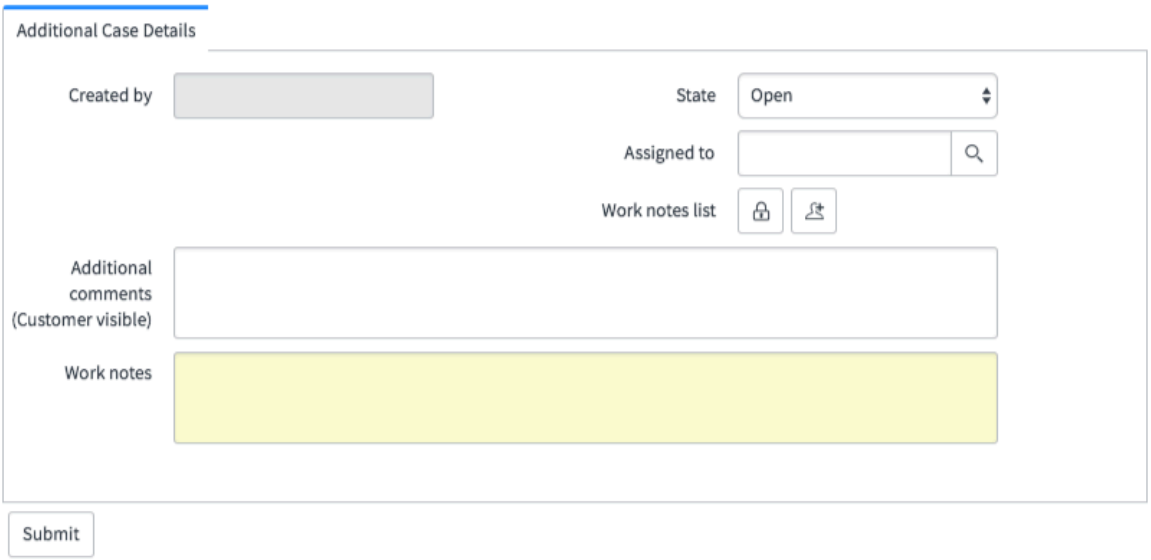
3. 필드에 적절하게 입력합니다.

필드	설명
케이스 번호	〔읽기 전용〕 케이스 번호입니다.
케이스 이름	케이스를 설명하는 이름을 입력합니다.
케이스 유형	조사 중인 케이스의 유형을 선택합니다.
평가 등급	이 케이스의 중요도를 선택합니다(중요도에서 낮음으로).

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
마지막 업데이트됨	〔읽기 전용〕 케이스가 마지막으로 업데이트된 날짜 및 시간입니다.
간단한 설명	케이스에 대한 간단한 설명입니다.

4. 추가 케이스 세부 정보 탭을 클릭합니다.



5. 필드에 적절하게 입력합니다.

필드	설명
작성자	〔읽기 전용〕 이 케이스를 생성한 사용자의 이름입니다.
상태	케이스의 현재 상태입니다. 케이스를 만들 때 상태는 기본적으로 초안으로 설정됩니다.
담당자	조회 아이콘을 클릭하고 분석가에게 케이스를 할당합니다.
작업 메모 공유자	잠금 아이콘을 클릭하고 작업 메모를 볼 수 있는 내부 사용자를 추가합니다.
추가 의견	필요한 경우 고객에게 표시될 케이스에 대한 메모를 입력합니다.
작업 메모	필요한 경우 케이스에 대한 작업 메모를 입력합니다.

6. 제출을 클릭합니다.
   기록이 저장된 후 케이스 아티팩트 탭을 클릭하여 케이스에 아티팩트를 추가할 수 있습니다.

케이스에 아티팩트 추가

케이스를 생성한 후에는 보안 인시던트, CI 및 손상 표시기와 같은 아티팩트를 케이스에 추가할 수 있습니다. 이러한 유물은 사건을 해결하는 데 단서 역할을 합니다.

시작하기 전에
위협 인텔리전스 를 사용하려면 보안 케이스 관리플러그인을 활성화해야 합니다.

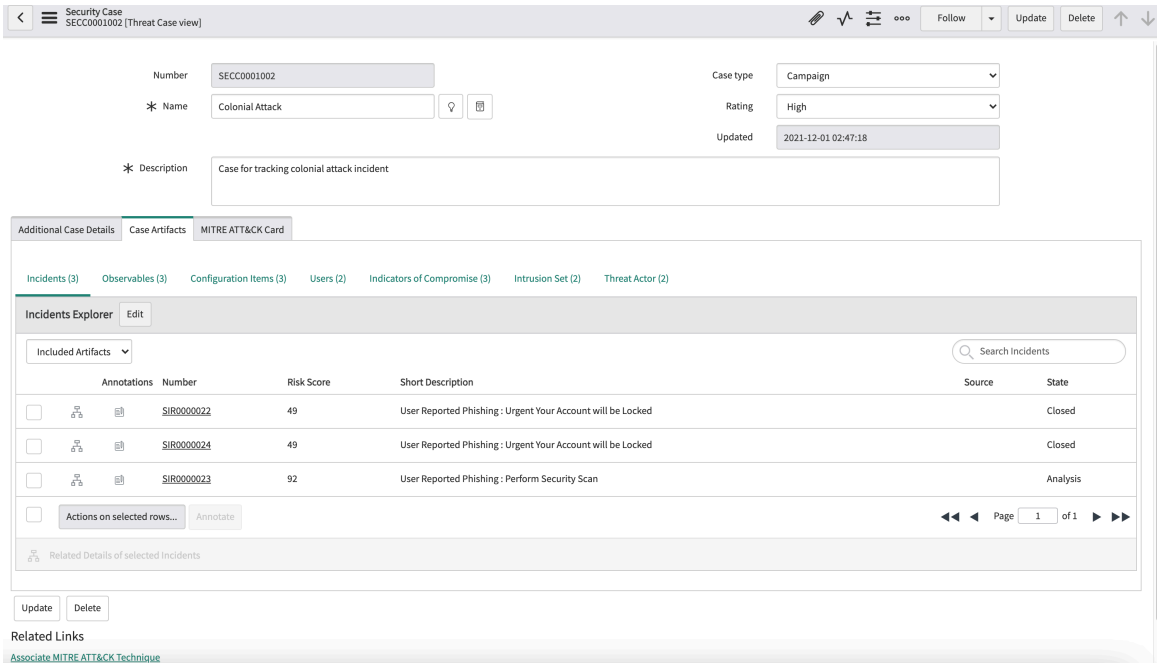
필요한 역할: sn_ti.case_user_write

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

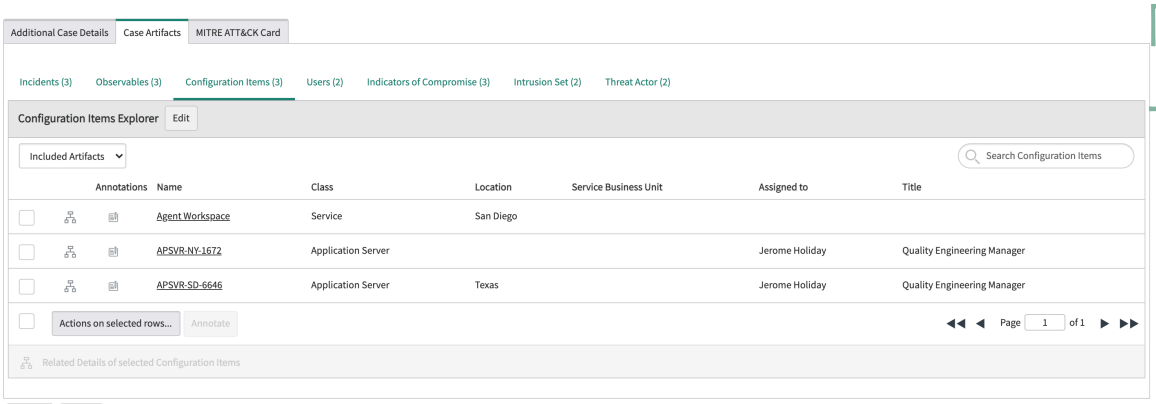
프로시저

1. 아티팩트를 추가할 케이스를 엽니다.

2. 케이스 아티팩트 관련 목록을 클릭합니다.

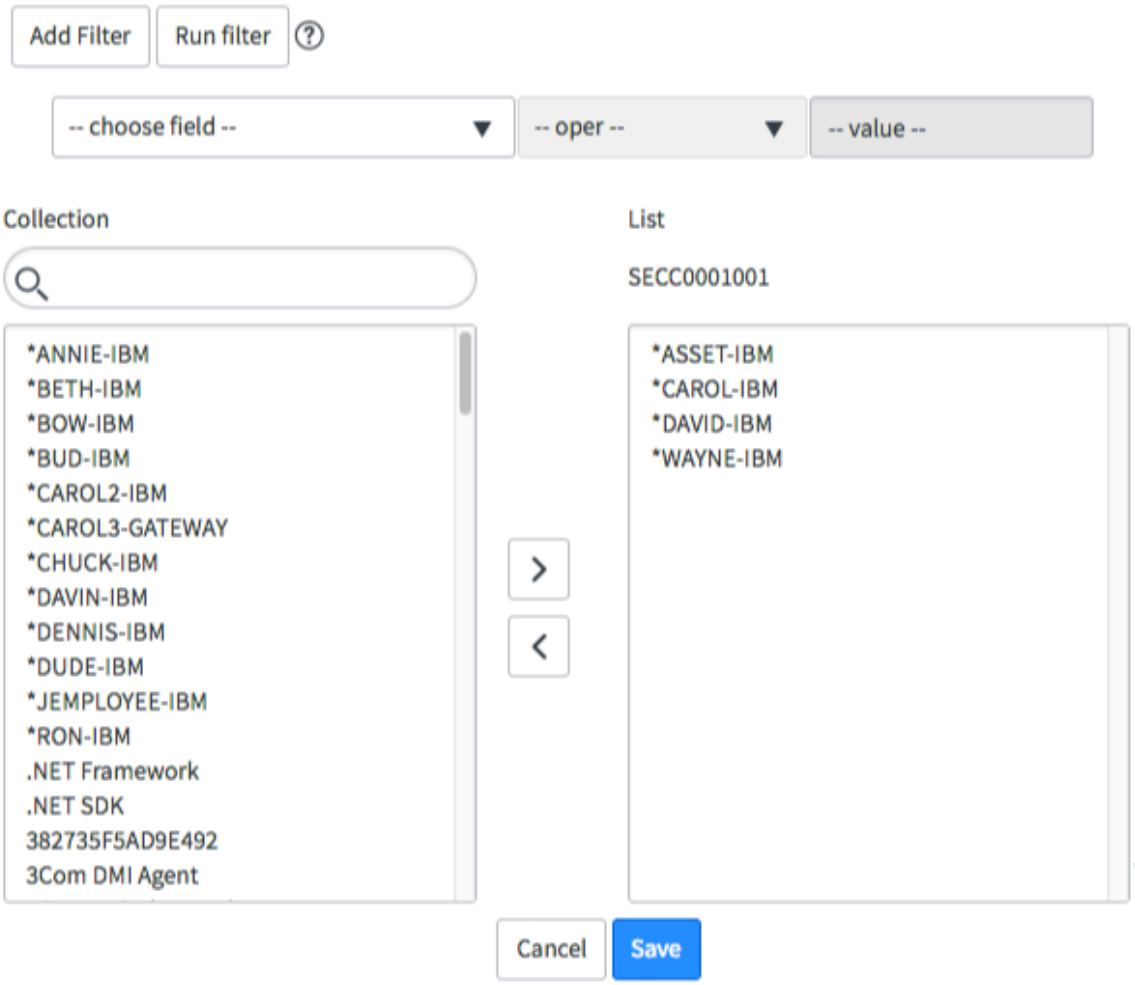


3. 케이스에 추가할 아티팩트 유형과 연결된 탭을 클릭합니다.
예를 들어 구성 항목을 클릭하여 케이스에 하나 이상의 CI를 추가합니다.



4. 편집을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



5. 슬러시버킷과 필터를 사용하여 케이스에 추가할 아티팩트 기록을 찾아 수집 버킷에서 목록 버킷으로 이동한 다음 저장을 클릭합니다.
   선택됨 탭에 목록이 나타나고 선택한 아티팩트가 목록에 추가됩니다.

관련 정보

- 기존 케이스에 IoC 및 옵저버블 추가
- 기존 케이스에 보안 인시던트 추가
- 기존 케이스에 CI 추가
- 영향을 받는 사용자를 기존 케이스에 추가

정보를 보안 케이스와 연결 **MITRE-ATT&CK**

전술과 기술을 보안 케이스에 연결하여 MITRE-ATT&CK 세분화된 수준에서 보안 케이스 관리 및 위협 분석을 개선합니다.

시작하기 전에
필요한 역할: sn_si.analyst

프로시저

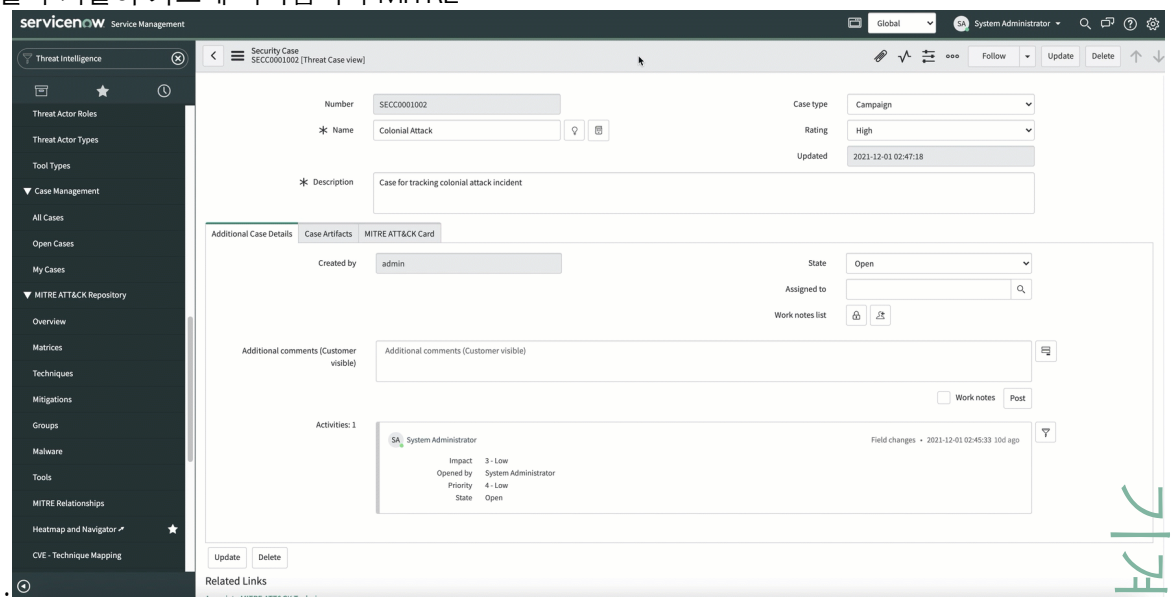
1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 케이스 관리 〉 모든 케이스.
2. MITRE-ATT&CK 정보로 보강할 보안 케이스를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 관련 목록에서 **MITRE ATT&CK** 기술 연결을 클릭합니다.

   다음 그림에서는 관련 목록에서 **MITRE ATT&CK** 기술 연결로 이동하고, 소스를 검토하고, 방법 및 기술을 추가하는 방법을 볼 수 있습니다.

4. 소스 목록에서 소스를 검토합니다.
5. 방법 및 기술을 검토하고 케이스와의 관련성에 따라 추가하거나 제거합니다.
6. 저장을 클릭합니다.
   추가한 전술과 기술이 카드에 나타납니다 MITRE-ATT&CK .



보안 아티팩트에서 케이스 생성

에서 보안 케이스 관리수동으로 케이스를 생성하는 것 외에도 보안 인시던트, 침해 표시기, 영향을 받는 사용자 및 구성 항목과 같은 보안 아티팩트에서 케이스를 생성할 수도 있습니다.

케이스의 **IoC** 및 옵저버블

에서 위협 인텔리전스IoC 및 옵저버블에서 케이스를 생성하고 기존 케이스에 IoC 및 옵저버블을 추가할 수 있습니다. 케이스에서 직접 옵저버블을 생성할 수도 있습니다.

IoC 또는 옵저버블에서 케이스 생성

에서 위협 인텔리전스아티팩트(IoC 또는 옵저버블)에서 케이스를 생성할 수 있습니다. IoC 또는 옵저버블을 사용하여 케이스를 생성한 후 를 사용하여 보안 케이스 관리 데이터를 분석할 수 있습니다.

시작하기 전에
위협 인텔리전스 를 사용하려면 보안 케이스 관리플러그인을 활성화해야 합니다.

필요한 역할: sn_ti.case_user_write

프로시저

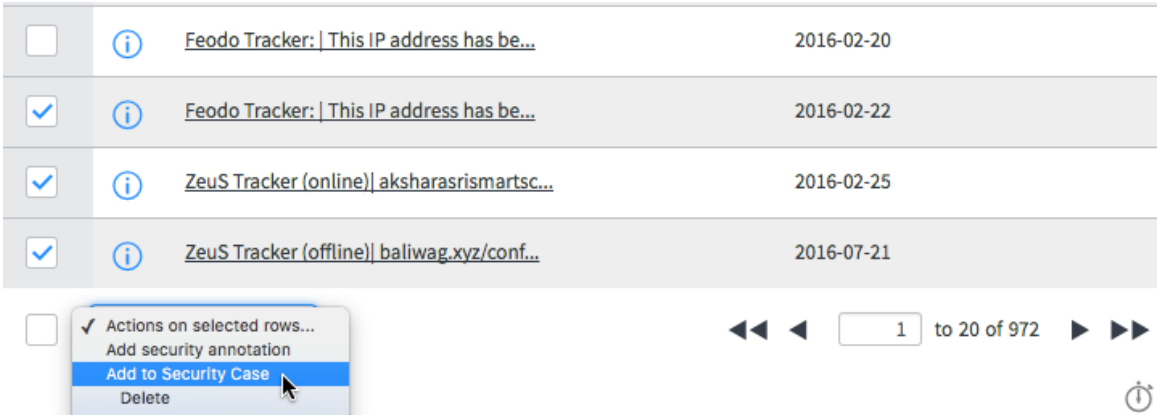
1. 케이스를 생성하는 데 사용할 아티팩트(IoC 또는 옵저버블)로 이동합니다.
   - IoC에서 케이스를 생성하려면 다음으로 이동합니다. 위협 인텔리전스 〉 **IoC** 리포지토리 〉 표시기.
   - 옵저버블에서 케이스를 생성하려면 다음으로 이동 위협 인텔리전스 〉 **IoC** 리포지토리 〉 옵저버블.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

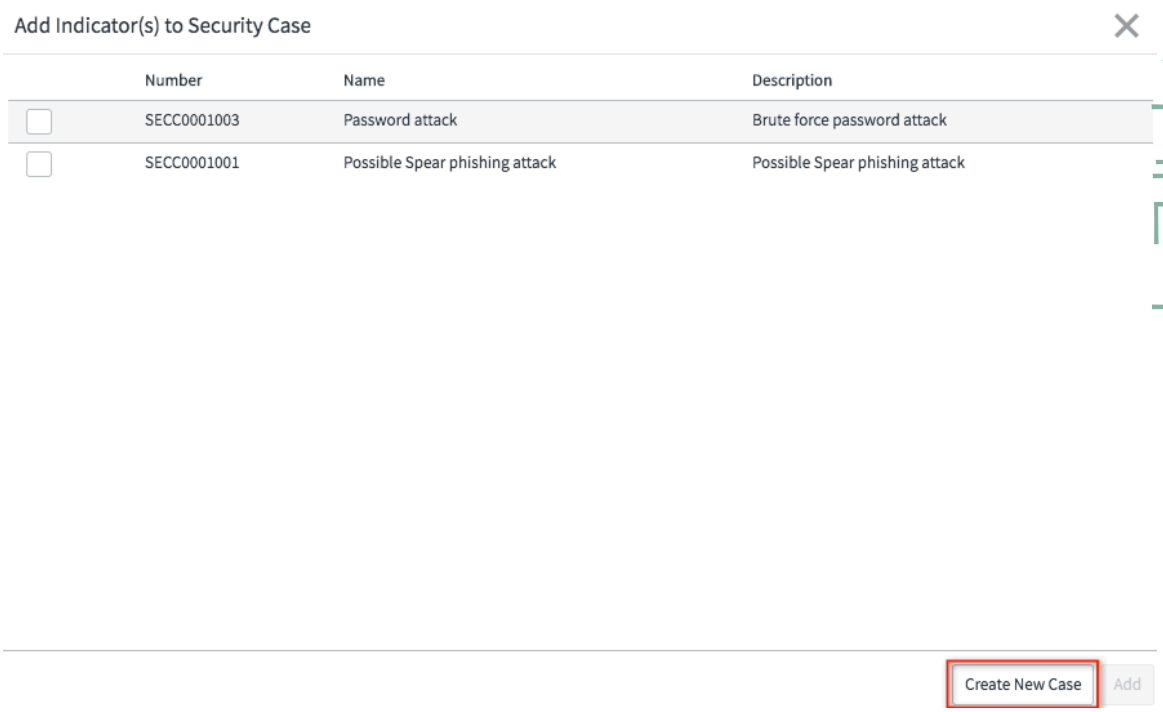
2. 목록에서 새 케이스에 추가할 아티팩트를 선택합니다.

   주:
   여러 IoC 또는 옵저버블을 선택하면 모두 케이스에 추가됩니다.

3. 선택한 항목에 대한 작업 드롭다운 목록에서 보안 케이스에 추가를 선택합니다.



보안 케이스에 추가 대화 상자가 열립니다. 할당된 케이스가 이미 있는 경우 목록에 표시됩니다.



4. 새 케이스 생성을 클릭합니다.
5. 필드에 내용을 입력합니다.

필드	설명
케이스 이름	이 케이스의 이름을 입력합니다.
설명	케이스 분석가에게 도움이 될 만한 설명을 입력합니다.

6. 제출을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

목록 맨 위에 있는 메시지는 의 케이스 보안 케이스 관리에 대한 링크와 함께 새 케이스가 만들어졌음을 나타냅니다.

7. 새 케이스를 보려면 링크를 클릭하십시오.

기존 케이스에 **IoC** 및 옵저버블 추가

기존 케이스에 IoC 및 옵저버블을 추가할 수 있습니다. 보안 인시던트가 케이스에 추가된 후 를 사용하여 보안 케이스 관리 데이터를 분석할 수 있습니다.

시작하기 전에

위협 인텔리전스 를 사용하려면 보안 케이스 관리플러그인을 활성화해야 합니다.

필요한 역할: sn_ti.case_user_write

프로시저

1. 기존 케이스에 추가할 아티팩트(IoC 또는 옵저버블)로 이동합니다.

- 하나 이상의 케이스에 IoC를 추가하려면 다음으로 이동합니다. 위협 인텔리전스 〉 **IoC** 리포지토리 〉 표시기.
- 하나 이상의 케이스에 옵저버블을 추가하려면 다음으로 이동하십시오. 위협 인텔리전스 〉 **IoC** 리포지토리 〉 옵저버블.

2. 목록에서 기존 케이스에 추가할 아티팩트 기록을 선택합니다.

> **주:**
> 여러 케이스를 선택하면 선택한 IoC 또는 옵저버블이 선택한 각 케이스에 추가됩니다.

3. 선택한 항목에 대한 작업 드롭다운 목록에서 보안 케이스에 추가를 선택합니다.
보안 케이스에 추가 대화 상자가 열립니다. 할당된 케이스가 이미 있는 경우 목록에 표시됩니다.

4. 선택한 IoC 또는 옵저버블을 추가할 케이스를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. 추가를 클릭합니다.
   메시지는 의 케이스 보안 케이스 관리에 대한 링크와 함께 선택한 기록이 케이스에 추가되었음을 나타냅니다.

케이스에서 옵저버블 생성

의 보안 케이스 관리케이스에서 새 옵저버블을 만들 수 있습니다.

시작하기 전에
필요한 역할: sn_ti.case_user

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 케이스 관리 〉 모든 케이스.
   보안 케이스 목록이 열립니다.
2. 기존 케이스를 열거나 새로 만들기를 클릭하여 새 케이스를 만듭니다.
3. 케이스 아티팩트 관련 링크를 클릭하고 옵저버블 탭을 클릭합니다.
4. 새로 만들기를 클릭하고 요청된 정보를 입력합니다.

필드	설명
값	〔읽기 전용〕 케이스 번호입니다.
옵저버블 유형	케이스를 설명하는 이름을 입력합니다.
옵저버블 유형 범주	조사 중인 케이스의 유형을 선택합니다.
인시던트 수	이 케이스의 중요도를 선택합니다(중요도에서 낮음으로).
찾기	〔읽기 전용〕 케이스가 마지막으로 업데이트된 날짜 및 시간입니다.
메모	케이스에 대한 간단한 설명입니다.

5. 추가 케이스 세부 정보 탭을 클릭합니다.
6. 필드에 적절하게 입력합니다.

필드	설명
작성자	〔읽기 전용〕 이 케이스를 생성한 사용자의 이름입니다.
상태	케이스의 현재 상태입니다. 케이스를 만들 때 상태는 기본적으로 초안으로 설정됩니다.
작업 메모 공유자	확인란을 클릭하여 케이스 기록의 추가 케이스 상세 정보 섹션에 작업 메모를 표시합니다.
작업 메모	필요한 경우 케이스에 대한 작업 메모를 입력합니다. 작업 메모 목록을 선택하면 케이스 기록의 추가 케이스 상세 정보 섹션에 작업 메모가 나타납니다.

7. 제출을 클릭합니다.
   필요한 경우 케이스 아티팩트 탭을 클릭하여 케이스에 아티팩트를 추가할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

케이스의 옵저버블에 대해 사이팅 검색을 실행합니다.

사이팅 검색 기능을 사용하여 옵저버블을 검색하여 발생 빈도를 확인할 수 있습니다. 각 발생은 사이팅으로 간주됩니다. 선택한 일 수 또는 날짜 범위 내의 사이팅 수로 검색을 제한할 수 있습니다.

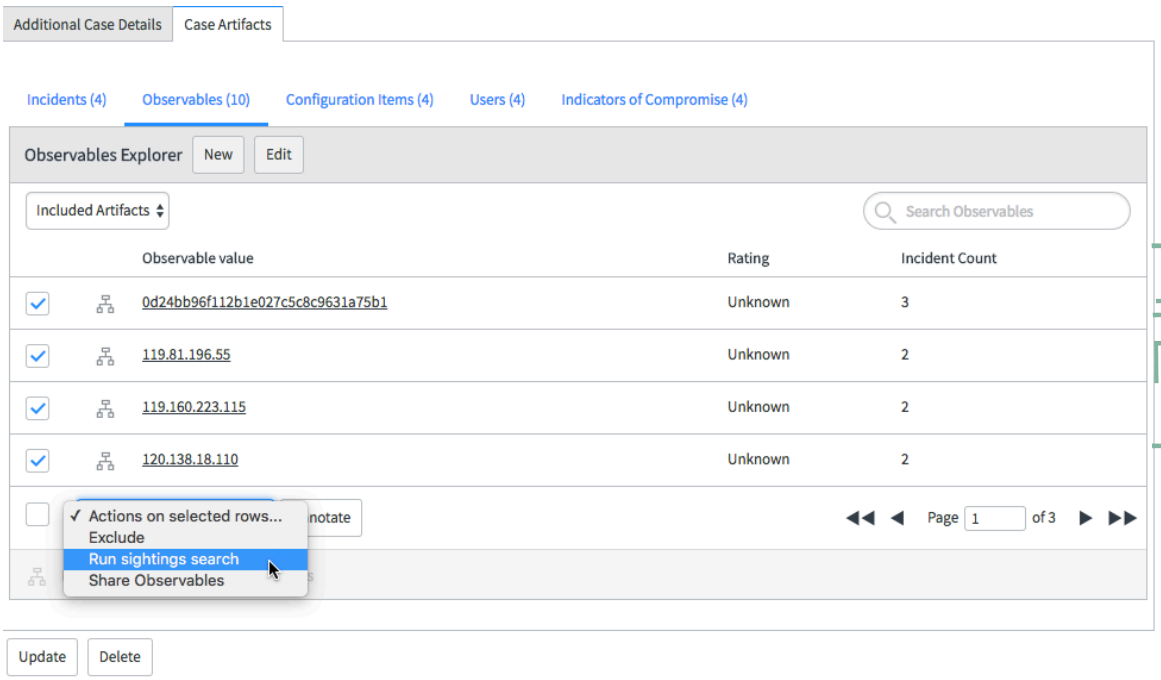
시작하기 전에

위협 인텔리전스 를 사용하려면 보안 케이스 관리플러그인을 활성화해야 합니다.

필요한 역할: sn_ti.case_user_write

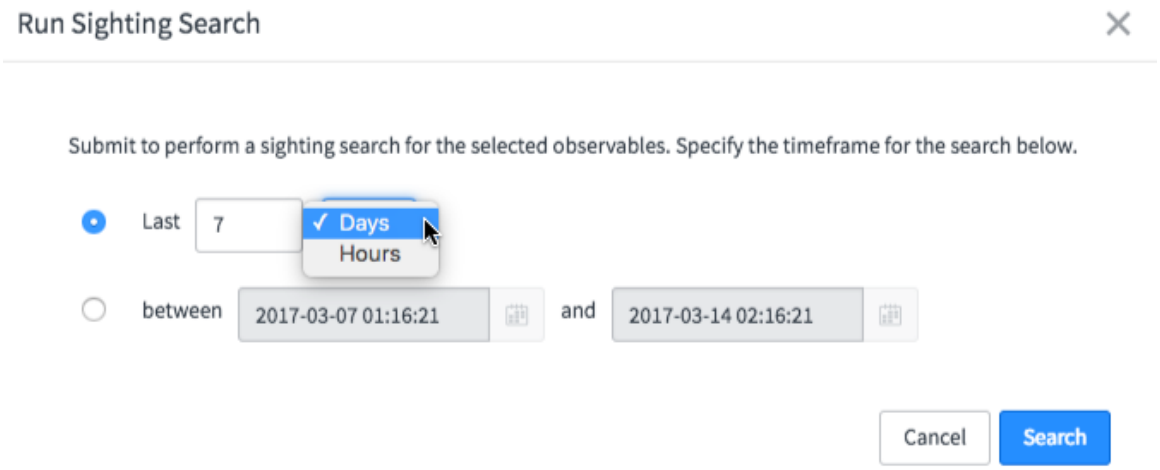
프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 케이스 관리 〉 모든 케이스.
2. 사이팅 검색을 실행할 옵저버블이 포함된 케이스를 엽니다.
3. 케이스 아티팩트 관련 링크를 클릭합니다.
4. 옵저버블 탭을 클릭합니다.
5. 사이팅을 검색할 옵저버블을 하나 이상 선택합니다.



6. 선택한 항목에 대한 작업 드롭다운 목록에서 사이팅 검색 실행을 선택합니다.
   사이팅 검색 실행 대화 상자가 나타납니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



7. 선택한 옵저버블의 사이팅을 검색할 일 또는 시간을 입력하거나 날짜 범위를 선택합니다.

8. 검색을 클릭합니다.

케이스의 보안 인시던트

에서 보안 인시던트 응답보안 인시던트, CI 및 영향을 받는 사용자로부터 케이스를 생성하고 이러한 아티팩트를 기존 케이스에 추가할 수 있습니다.

보안 인시던트에서 케이스 생성

에서 보안 인시던트 응답보안 인시던트로부터 케이스를 생성할 수 있습니다. 보안 인시던트를 사용하여 새 케이스를 생성한 후에는 데이터를 분석하는 데 사용할 보안 케이스 관리 수 있습니다.

시작하기 전에
위협 인텔리전스 를 사용하려면 보안 케이스 관리플러그인을 활성화해야 합니다.

필요한 역할: sn_ti.case_user_write

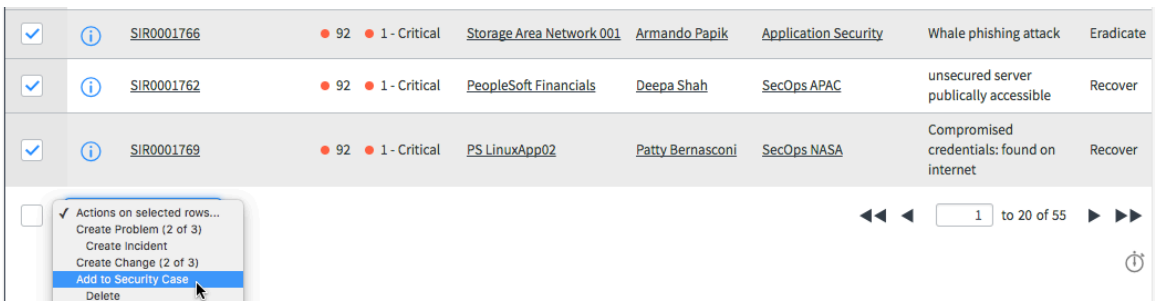
이 태스크 정보
케이스를 생성하는 데 사용할 보안 인시던트로 이동해야 합니다.

프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 인시던트 〉 열린 인시던트 표시.
보안 인시던트 목록이 열립니다. 목록에서 하나 이상의 보안 인시던트에서 새 케이스를 만들거나, 특정 보안 인시던트를 선택하고 양식에서 새 케이스를 만들 수 있습니다.

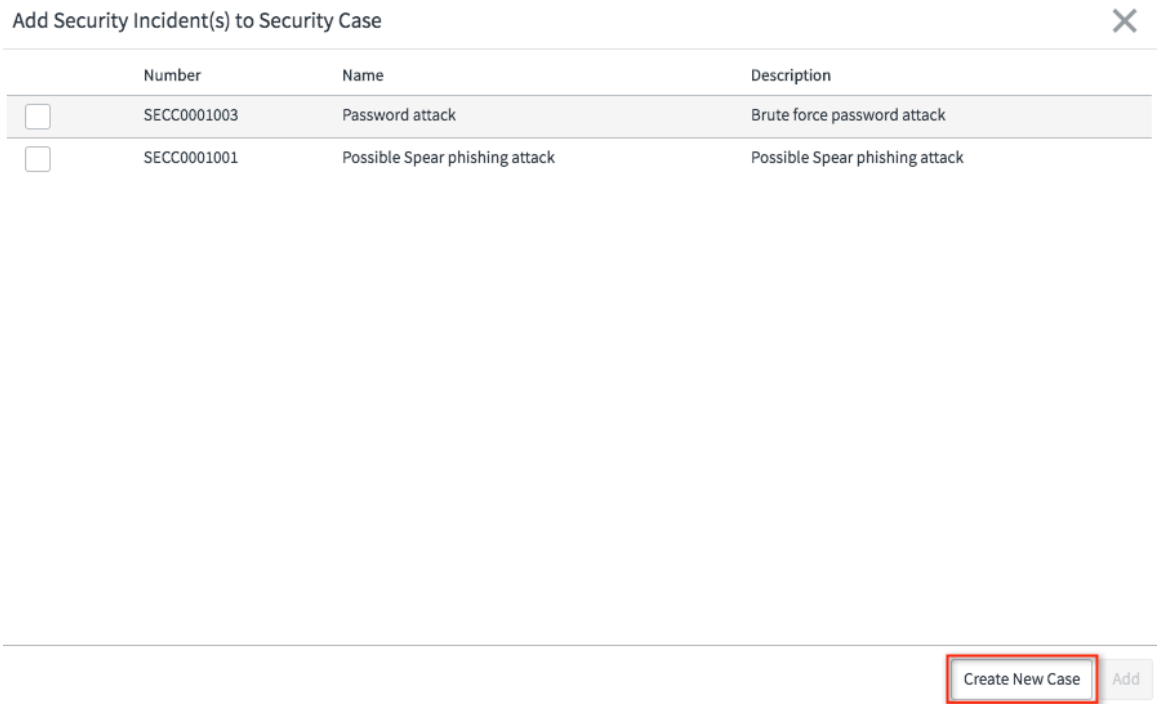
2. 목록에서 케이스를 만들려면 새 케이스에 추가할 아티팩트를 선택합니다.

3. 선택한 항목에 대한 작업 드롭다운 목록에서 보안 케이스에 추가를 선택합니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 케이스에 추가 대화 상자가 열립니다. 할당된 케이스가 이미 있는 경우 목록에 표시됩니다.



4. 새 케이스 생성을 클릭합니다.
5. 필드에 내용을 입력합니다.

필드	설명
케이스 이름	이 케이스의 이름을 입력합니다.
설명	케이스 분석가에게 도움이 될 만한 설명을 입력합니다.

6. 제출을 클릭합니다.
   목록 맨 위에 있는 메시지는 의 케이스 보안 케이스 관리에 대한 링크와 함께 새 케이스가 만들어졌음을 나타냅니다.
7. 새 케이스를 보려면 링크를 클릭하십시오.

기존 케이스에 보안 인시던트 추가

하나 이상의 기존 케이스에 보안 인시던트를 추가할 수 있습니다. 보안 인시던트가 케이스에 추가된 후 를 사용하여 보안 케이스 관리 데이터를 분석할 수 있습니다.

시작하기 전에
위협 인텔리전스 를 사용하려면 보안 케이스 관리플러그인을 활성화해야 합니다.

필요한 역할: sn_ti.case_user_write

이 태스크 정보
기존 케이스에 추가할 보안 인시던트로 이동해야 합니다.

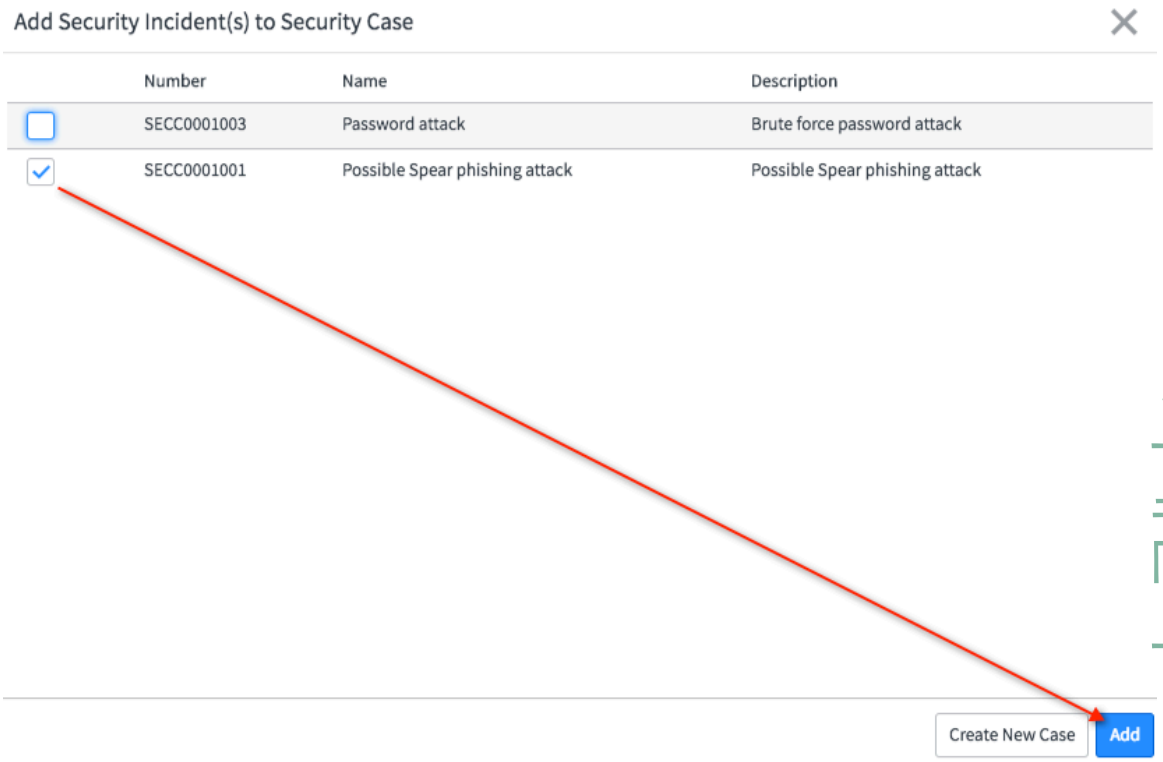
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 보안 인시던트 〉 인시던트 〉 열린 인시던트 표시.
   보안 인시던트 목록이 열립니다.
2. 목록에서 기존 케이스에 추가할 보안 인시던트를 하나 이상 선택합니다.

   주:
   여러 보안 인시던트를 선택하면 선택한 보안 인시던트가 선택한 각 케이스에 추가됩니다.

3. 선택한 항목에 대한 작업 드롭다운 목록에서 보안 케이스에 추가를 선택합니다.
   보안 케이스에 추가 대화 상자가 열리고 할당된 케이스가 표시됩니다.



4. 선택한 보안 인시던트를 추가할 케이스를 선택합니다.
5. 추가를 클릭합니다.
   메시지는 의 케이스 보안 케이스 관리에 대한 링크와 함께 선택한 기록이 케이스에 추가되었음을 나타냅니다.

케이스의 구성 항목

구성 항목 [cmdb_ci] 테이블에 있는 하나 이상의 CI(구성 항목)에서 새 케이스를 만들 수 있습니다. 기존 케이스에 CI를 추가할 수도 있습니다.

CI에서 케이스 생성

구성 항목 [cmdb_ci] 테이블의 구성 항목에서 보안 케이스를 만들 수 있습니다. CI를 사용하여 새 케이스를 만든 후 를 사용하여 보안 케이스 관리 데이터를 분석할 수 있습니다.

시작하기 전에

위협 인텔리전스 를 사용하려면 보안 케이스 관리플러그인을 활성화해야 합니다.

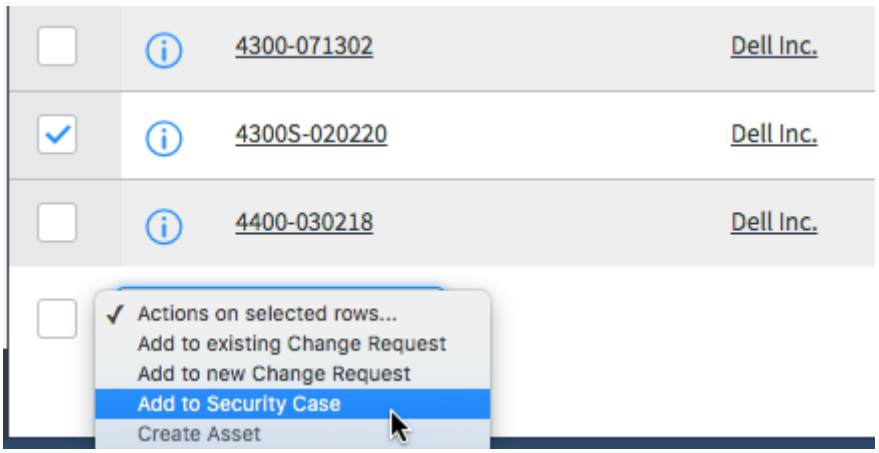
필요한 역할: sn_ti.case_user_write

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

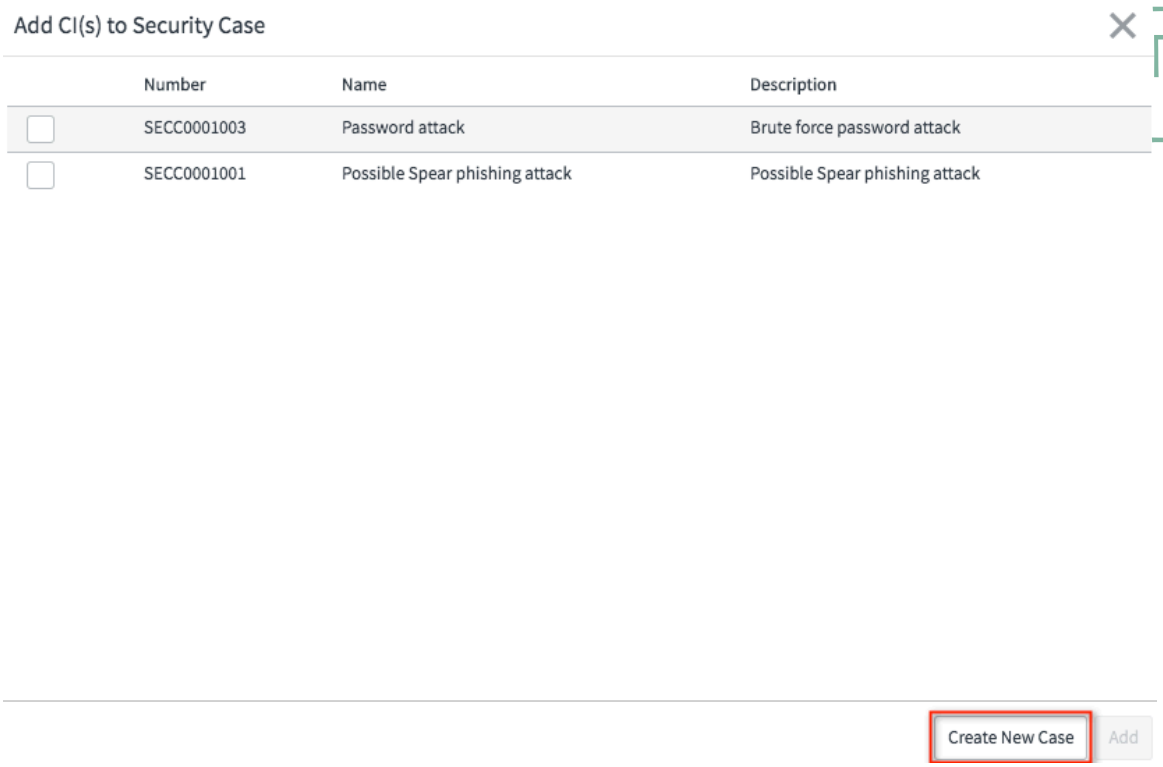
이 태스크 정보
케이스를 생성하는 데 사용할 구성 항목으로 이동해야 합니다.

프로시저

1. 다음으로 이동 모두 〉 구성 〉 기본 항목 〉 컴퓨터 컴퓨터의 CI를 보려면
   선택한 CI 유형의 목록이 열립니다. 목록에서 하나 이상의 CI에서 새 케이스를 만들거나, 특정 CI를 선택하고 양식에서 새 케이스를 만들 수 있습니다.
2. 목록에서 새 케이스에 추가할 CI를 선택합니다.
3. 선택한 항목에 대한 작업 드롭다운 목록에서 보안 케이스에 추가를 선택합니다.



보안 케이스에 추가 대화 상자가 열립니다. 할당된 케이스가 이미 있는 경우 목록에 표시됩니다.



4. 새 케이스 생성을 클릭합니다.
5. 필드에 내용을 입력합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
케이스 이름	이 케이스의 이름을 입력합니다.
설명	케이스 분석가에게 도움이 될 만한 설명을 입력합니다.

6. 제출을 클릭합니다.
   목록 맨 위에 있는 메시지는 의 케이스 보안 케이스 관리에 대한 링크와 함께 새 케이스가 만들어졌음을 나타냅니다.
7. 새 케이스를 보려면 링크를 클릭하십시오.

기존 케이스에 **CI** 추가

하나 이상의 기존 케이스에 구성 항목을 추가할 수 있습니다. CI가 케이스에 추가된 후 를 사용하여 보안 케이스 관리 데이터를 분석할 수 있습니다.

시작하기 전에
위협 인텔리전스 를 사용하려면 보안 케이스 관리플러그인을 활성화해야 합니다.

필요한 역할: sn_ti.case_user_write

이 태스크 정보
기존 케이스에 추가할 CI로 이동해야 합니다.

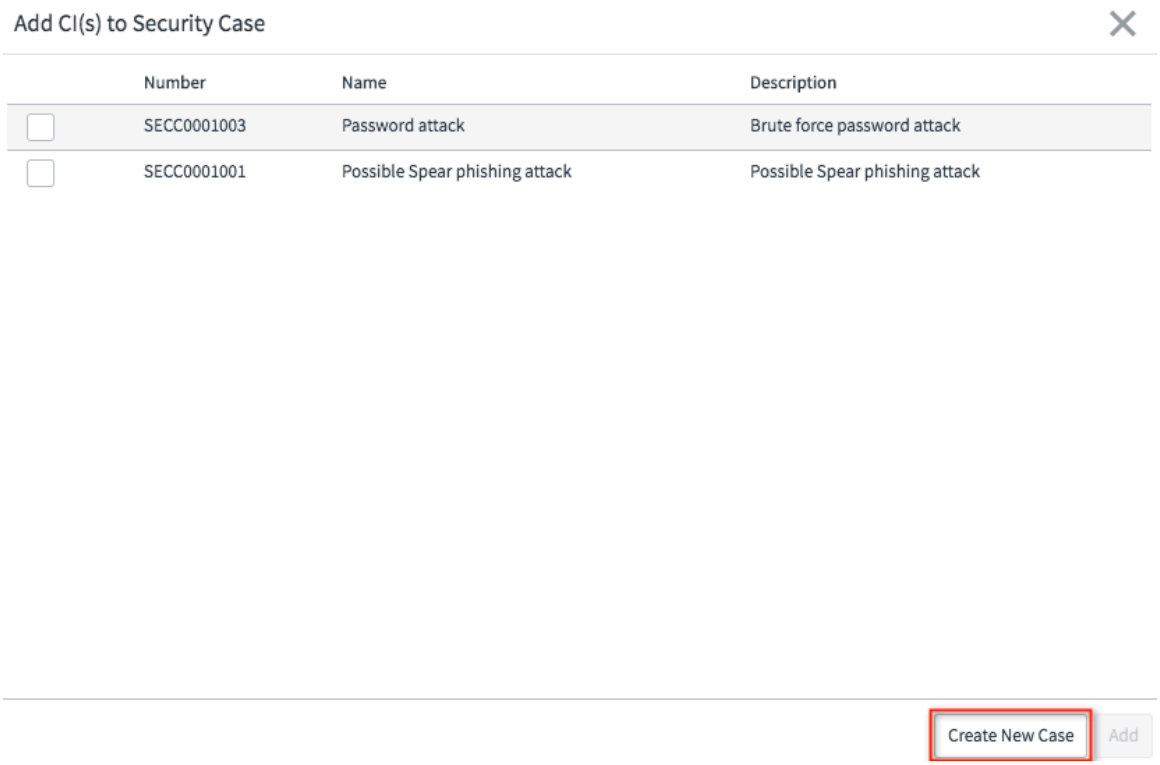
프로시저

1. 다음으로 이동 모두 〉 구성 〉 기본 항목 〉 컴퓨터 컴퓨터의 CI를 보려면 선택한 CI의 목록이 열립니다.
2. 목록에서 기존 케이스에 추가할 CI를 하나 이상 선택합니다.

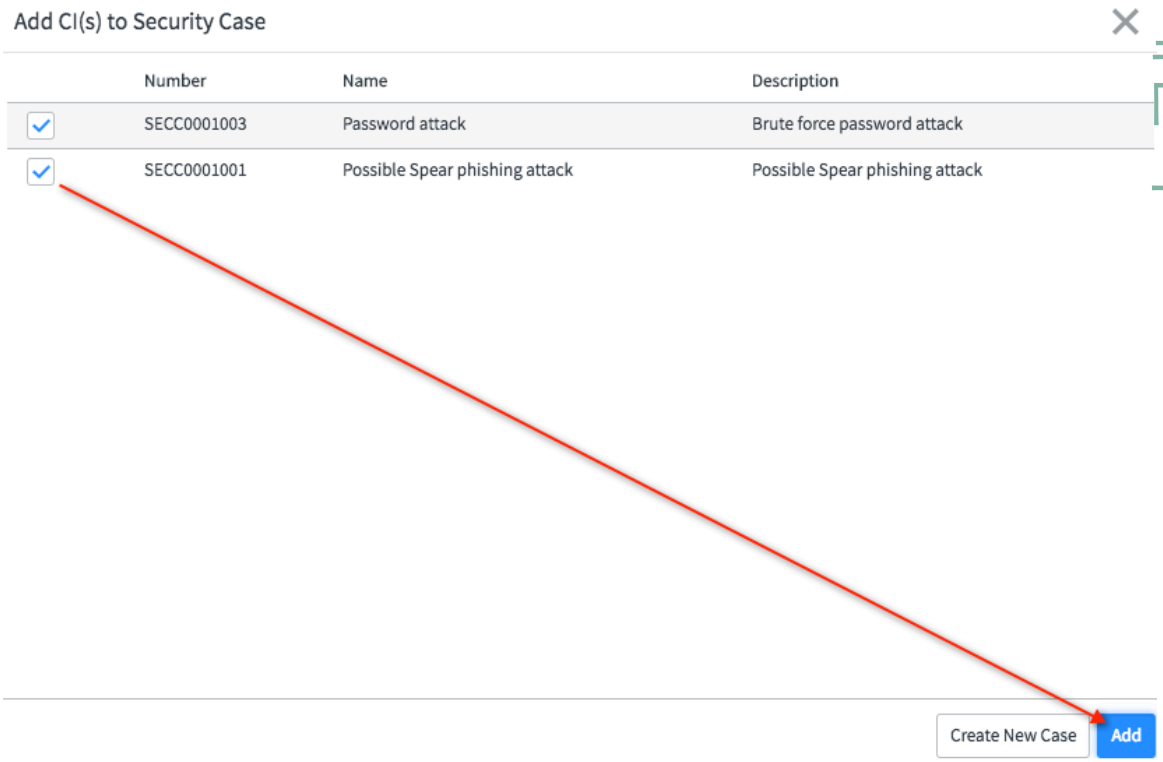
   주:
   여러 CI를 선택하면 선택한 CI가 선택한 각 케이스에 추가됩니다.

3. 선택한 항목에 대한 작업 드롭다운 목록에서 보안 케이스에 추가를 선택합니다.
   보안 케이스에 추가 대화 상자가 열리고 할당된 케이스가 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 선택한 CI를 추가할 케이스를 선택합니다.



5. 추가를 클릭합니다.
메시지는 의 케이스 보안 케이스 관리에 대한 링크와 함께 선택한 기록이 케이스에 추가되었음을 나타냅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

케이스의 영향을 받는 사용자

사용자 [sys_user] 테이블에서 영향을 받는 한 명 이상의 사용자로부터 새 케이스를 만들 수 있습니다. 기존 케이스에 사용자를 추가할 수도 있습니다.

영향을 받는 사용자로부터 케이스 생성

사용자 [sys_user] 테이블에서 영향을 받는 사용자의 보안 케이스를 만들 수 있습니다. 영향을 받는 사용자를 사용하여 새 케이스를 만든 후 를 사용하여 보안 케이스 관리 데이터를 분석할 수 있습니다.

시작하기 전에
위협 인텔리전스 를 사용하려면 보안 케이스 관리플러그인을 활성화해야 합니다.

필요한 역할: sn_ti.case_user_write

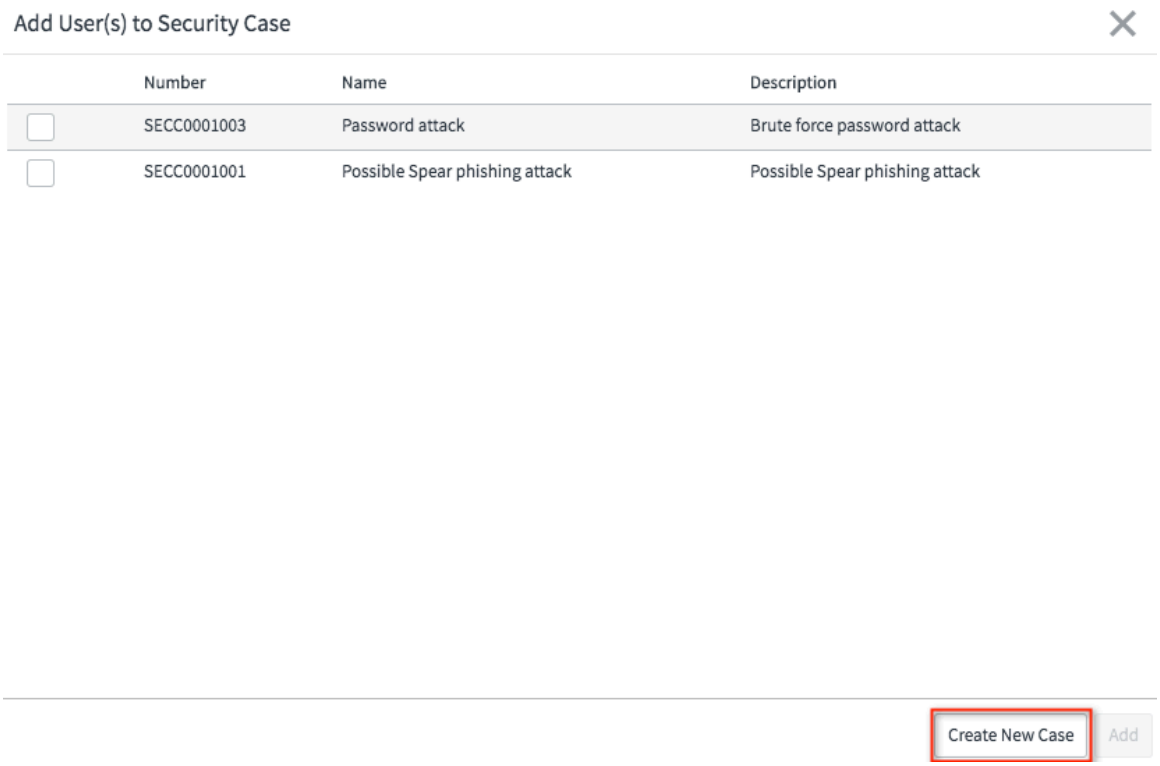
이 태스크 정보
케이스를 생성하는 데 사용할 사용자로 이동해야 합니다.

프로시저

1. 다음으로 이동 모두 〉 사용자 관리 〉 사용자.
   선택한 사용자에 대한 목록이 열립니다. 목록에서 하나 이상의 사용자 기록으로 새 케이스를 만들거나, 특정 사용자 기록을 선택하고 양식에서 새 케이스를 만들 수 있습니다.
2. 목록에서 새 케이스에 추가할 사용자를 선택합니다.
3. 선택한 항목에 대한 작업 드롭다운 목록에서 보안 케이스에 추가를 선택합니다.

보안 케이스에 추가 대화 상자가 열립니다. 할당된 케이스가 이미 있는 경우 목록에 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 새 케이스 생성을 클릭합니다.
5. 필드에 내용을 입력합니다.

필드	설명
케이스 이름	이 케이스의 이름을 입력합니다.
설명	케이스 분석가에게 도움이 될 만한 설명을 입력합니다.

6. 제출을 클릭합니다.
   목록 맨 위에 있는 메시지는 의 케이스 보안 케이스 관리에 대한 링크와 함께 새 케이스가 만들어졌음을 나타냅니다.
7. 새 케이스를 보려면 링크를 클릭하십시오.

영향을 받는 사용자를 기존 케이스에 추가

영향을 받는 사용자를 하나 이상의 기존 케이스에 추가할 수 있습니다. 사용자 기록이 케이스에 추가된 후 데이터를 분석하는 데 사용할 보안 케이스 관리 수 있습니다.

시작하기 전에
위협 인텔리전스 를 사용하려면 보안 케이스 관리플러그인을 활성화해야 합니다.

필요한 역할: sn_ti.case_user_write

이 태스크 정보
기존 케이스에 추가할 사용자 기록으로 이동해야 합니다.

프로시저

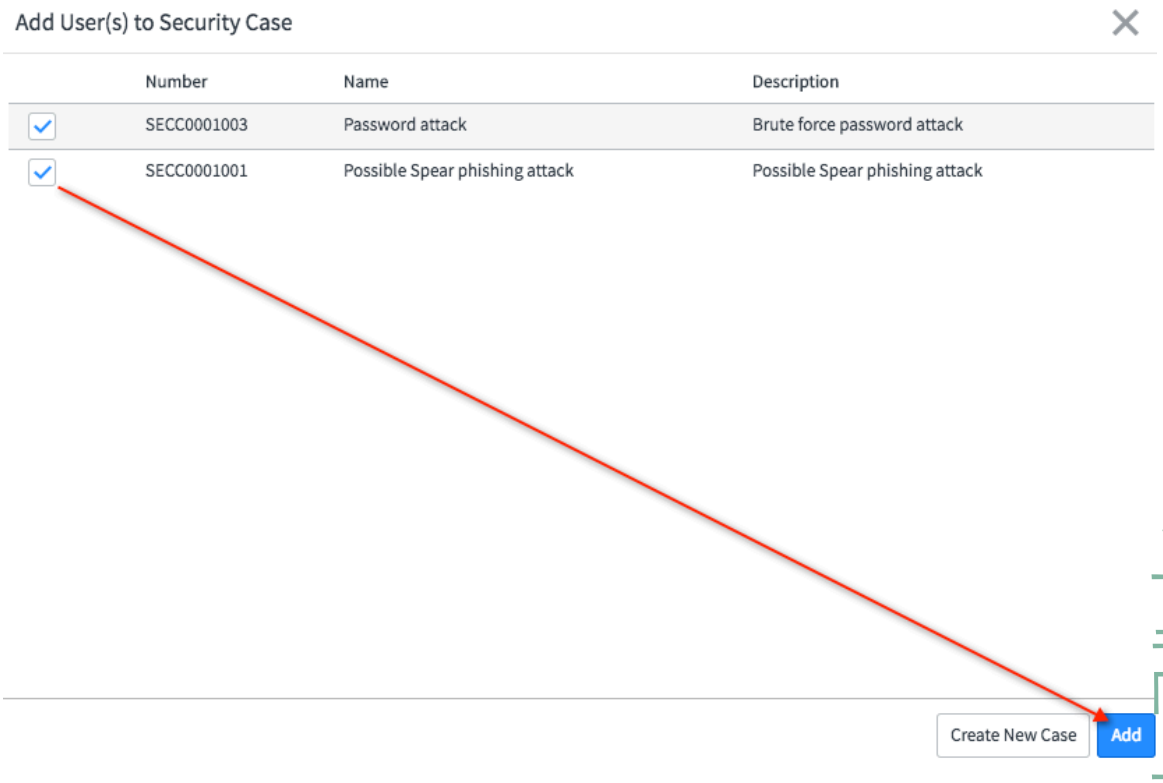
1. 다음으로 이동 모두 〉 사용자 관리 〉 사용자.
   사용자 기록 목록이 열립니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

2. 목록에서 기존 케이스에 추가할 사용자를 한 명 이상 선택합니다.

   주:
   여러 사용자를 선택하면 선택한 사용자 기록이 선택한 각 케이스에 추가됩니다.

3. 선택한 항목에 대한 작업 드롭다운 목록에서 보안 케이스에 추가를 선택합니다.
   보안 케이스에 추가 대화 상자가 열리고 할당된 케이스가 표시됩니다.



4. 선택한 사용자를 추가할 케이스를 선택합니다.
5. 추가를 클릭합니다.
   메시지는 의 케이스 보안 케이스 관리에 대한 링크와 함께 선택한 기록이 케이스에 추가되었음을 나타냅니다.

보안 아티팩트 분석

를 사용하여 보안 케이스 관리케이스를 생성하거나 IoC, 옵저버블, 보안 인시던트 등의 아티팩트에서 케이스를 생성한 후에는 아티팩트를 계속 추가하여 식별된 위협을 분석할 수 있습니다.

케이스 아티팩트 관련 상세 정보

케이스에 아티팩트를 추가하면 각 아티팩트에 대한 추가 관련 상세 정보도 자동으로 추가될 수 있습니다. 예를 들어 보안 인시던트를 추가하면 영향을 받는 CI 및 사용자 기록이 포함될 수 있습니다. 아티팩트 목록에서 나가지 않고 선택한 아티팩트에 대한 관련 상세 정보를 빠르게 볼 수 있습니다.

보안 인시던트 아티팩트에 대한 관련 상세 정보 보기

케이스에 보안 인시던트 아티팩트가 포함된 경우 케이스에서 참조하는 각 보안 인시던트에 포함된 모든 관련 상세 정보를 볼 수 있습니다.

시작하기 전에

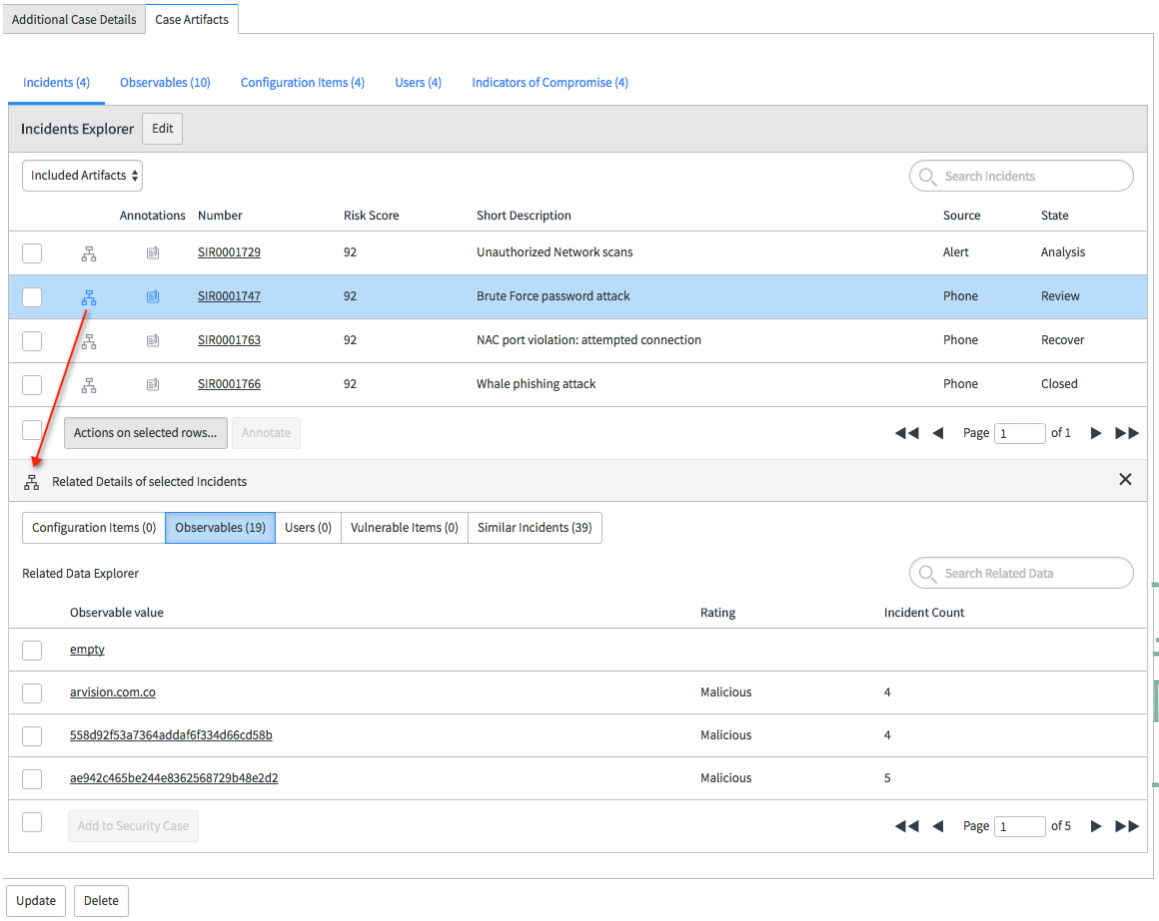
- 위협 인텔리전스 를 사용하려면 보안 케이스 관리플러그인을 활성화해야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필요한 역할: sn_ti.case_user_write

프로시저

1. 보안 인시던트 아티팩트가 포함된 케이스를 엽니다.
2. 인시던트 탭을 클릭합니다.
3. 관련 상세 정보를 보려는 보안 인시던트의 추가 상세 정보 아이콘을 클릭합니다.



4. 탭을 클릭하면 선택한 아티팩트에 대한 특정 유형의 상세 정보를 볼 수 있습니다.
5. 보안 주석 탭을 클릭하여 선택한 아티팩트에 대한 주석을 볼 수도 있습니다.

구성 항목 아티팩트에 대한 관련 상세 정보 보기

케이스에 구성 항목 아티팩트가 포함된 경우 케이스에서 참조하는 각 CI에 포함된 모든 관련 상세 정보를 볼 수 있습니다.

시작하기 전에

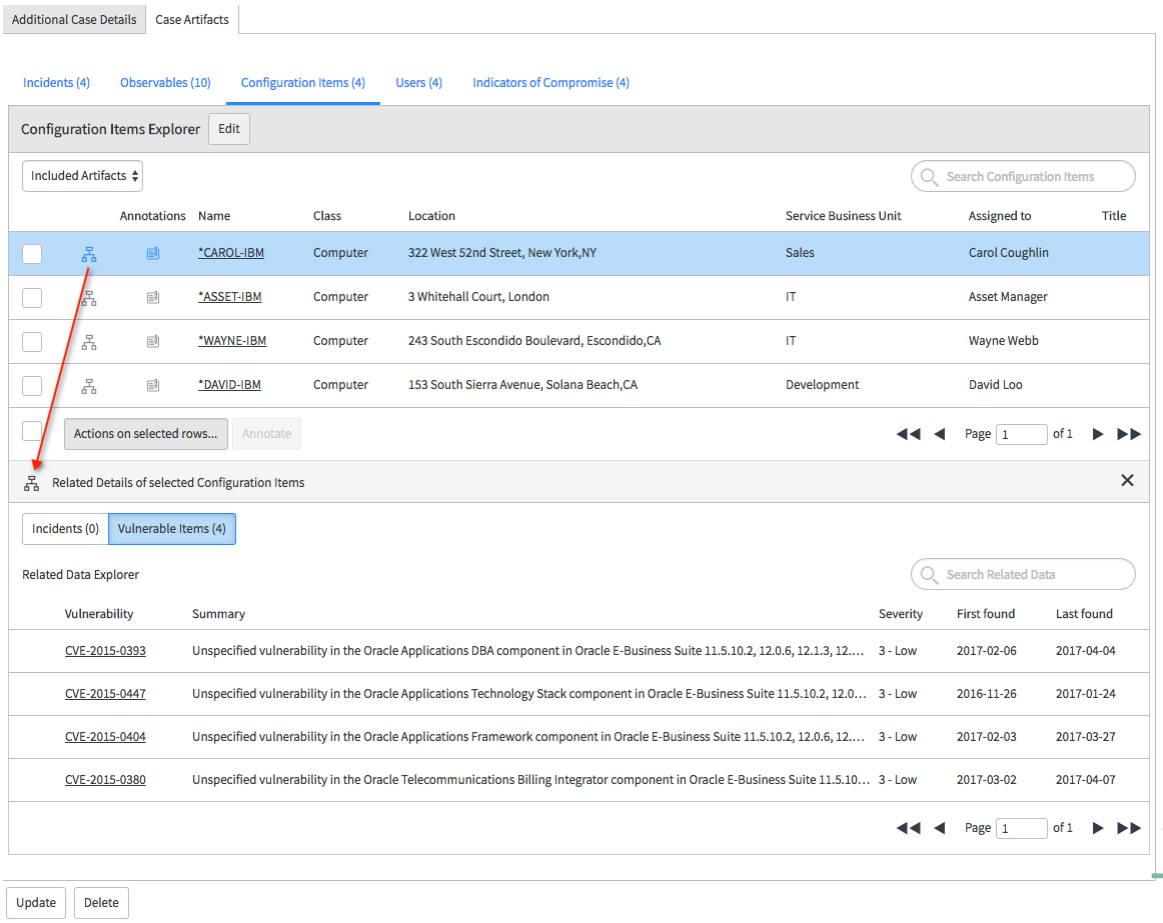
- 위협 인텔리전스 를 사용하려면 보안 케이스 관리플러그인을 활성화해야 합니다.

필요한 역할: sn_ti.case_user_write

프로시저

1. CI 아티팩트가 포함된 케이스를 엽니다.
2. 구성 항목 탭을 클릭합니다.
3. 관련 상세 정보를 보려는 CI 아티팩트의 추가 상세 정보를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 탭을 클릭하면 선택한 아티팩트에 대한 특정 유형의 상세 정보를 볼 수 있습니다.
5. 보안 주석 탭을 클릭하여 선택한 아티팩트에 대한 주석을 볼 수도 있습니다.

IoC 아티팩트에 대한 관련 상세 정보 보기

케이스에 IoC(침해 표시기) 아티팩트가 포함된 경우 케이스에서 참조하는 각 IoC에 포함된 모든 관련 상세 정보를 볼 수 있습니다.

시작하기 전에

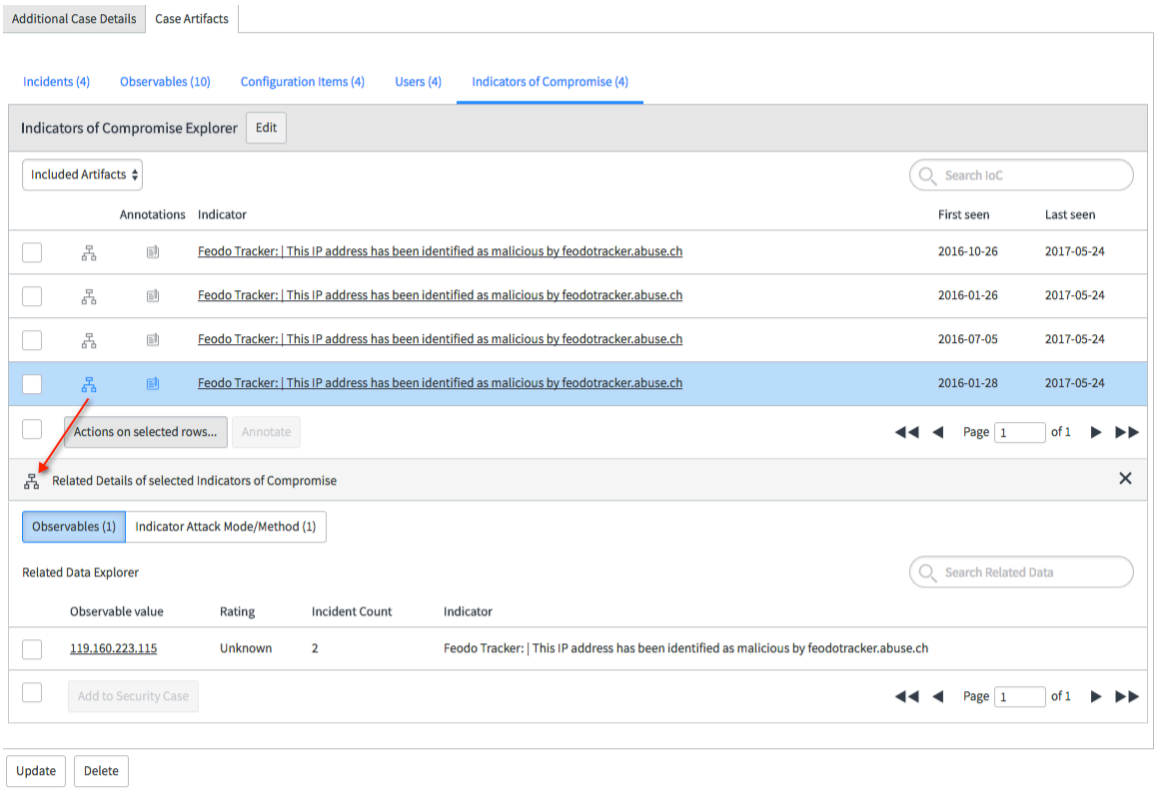
- 위협 인텔리전스 를 사용하려면 보안 케이스 관리플러그인을 활성화해야 합니다.

필요한 역할: sn_ti.case_user_write

프로시저

1. IoC 아티팩트가 포함된 케이스를 엽니다.
2. 침해 표시기 탭을 클릭합니다.
3. 관련 상세 정보를 보려는 IoC 아티팩트의 추가 상세 정보 아이콘을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 탭을 클릭하면 선택한 아티팩트에 대한 특정 유형의 상세 정보를 볼 수 있습니다.

5. 보안 주석 탭을 클릭하여 선택한 아티팩트에 대한 주석을 볼 수도 있습니다.

영향을 받는 사용자 아티팩트에 대한 관련 상세 정보 보기

케이스에 영향을 받는 사용자 아티팩트가 포함되어 있는 경우 케이스에서 참조하는 영향을 받는 각 사용자에 포함된 관련 상세 정보를 볼 수 있습니다.

시작하기 전에

- 위협 인텔리전스 를 사용하려면 보안 케이스 관리플러그인을 활성화해야 합니다.

필요한 역할: sn_ti.case_user_write

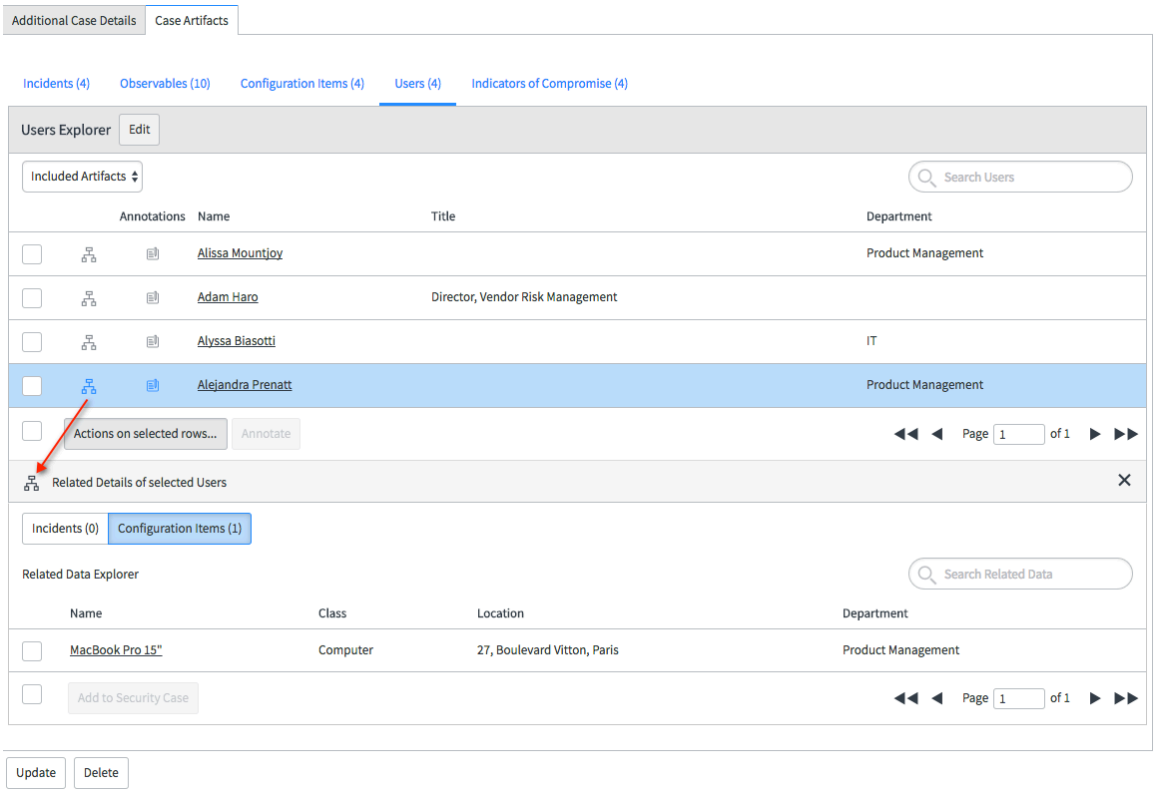
프로시저

1. 영향을 받는 사용자 아티팩트가 포함된 케이스를 엽니다.

2. 사용자 탭을 클릭합니다.

3. 관련 상세 정보를 보려는 영향을 받는 사용자 아티팩트에 대해 관련 상세 정보를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 탭을 클릭하면 선택한 아티팩트에 대한 특정 유형의 상세 정보를 볼 수 있습니다.

5. 보안 주석 탭을 클릭하여 선택한 아티팩트에 대한 주석을 볼 수도 있습니다.

옵저버블 아티팩트에 대한 관련 상세 정보 보기

케이스에 옵저버블 아티팩트가 포함된 경우 케이스에서 참조하는 각 옵저버블에 포함된 모든 관련 상세 정보를 볼 수 있습니다.

시작하기 전에

위협 인텔리전스 를 사용하려면 보안 케이스 관리플러그인을 활성화해야 합니다.

필요한 역할: sn_ti.case_user_write

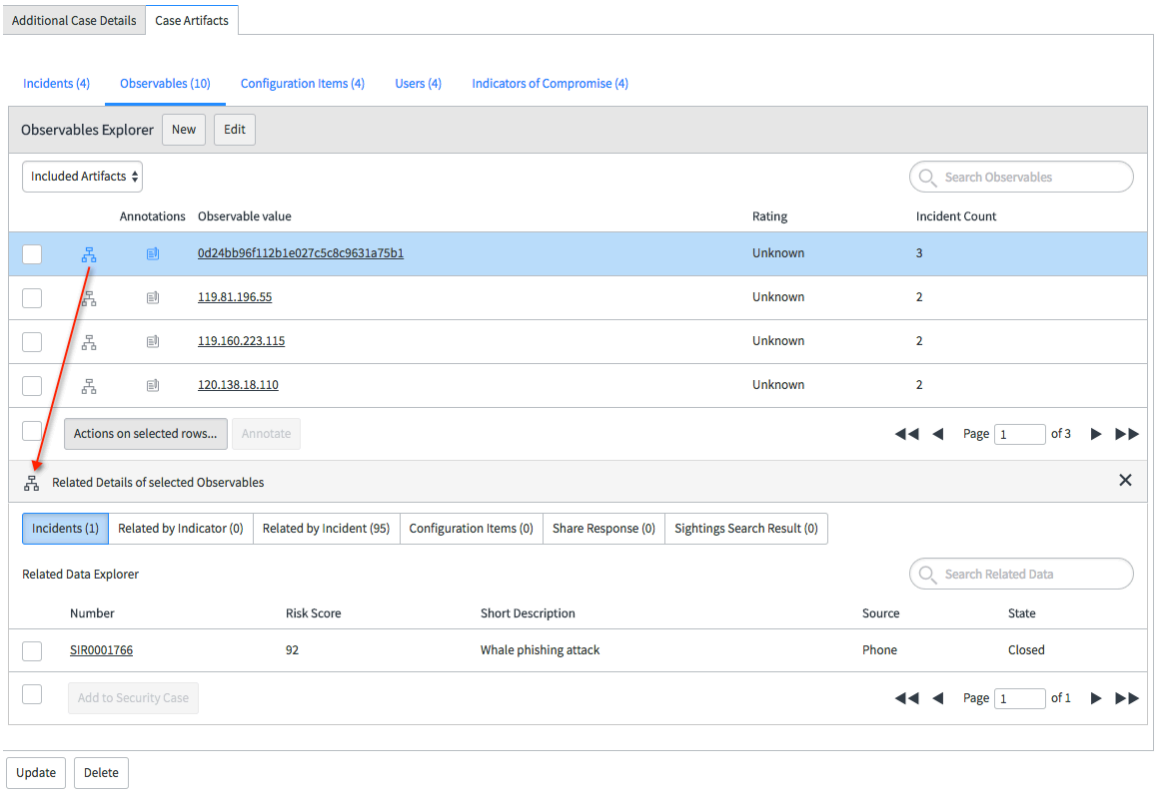
프로시저

1. 옵저버블 아티팩트가 포함된 케이스를 엽니다.

2. 옵저버블 탭을 클릭합니다.

3. 관련 상세 정보를 보려는 옵저버블 아티팩트의 추가 상세 정보 아이콘을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 탭을 클릭하면 선택한 아티팩트에 대한 특정 유형의 상세 정보를 볼 수 있습니다.

5. 보안 주석 탭을 클릭하여 선택한 아티팩트에 대한 주석을 볼 수도 있습니다.

보안 아티팩트 제외 및 포함

케이스에 할당된 지원 아티팩트 목록이 길어질 수 있으며 목록에서 특정 아티팩트를 제거하려는 경우가 있을 수 있습니다. 아티팩트를 영구적으로 제거하는 대신 목록에서 제외했다가 필요에 따라 나중에 목록으로 되돌릴 수 있습니다.

케이스에서 보안 아티팩트 제외

지원 아티팩트 목록에서 아티팩트를 제거할 수 있습니다. 영구적으로 제거되지 않으며 필요에 따라 케이스로 반환할 수 있습니다.

시작하기 전에

- 위협 인텔리전스 를 사용하려면 보안 케이스 관리플러그인을 활성화해야 합니다.

필요한 역할: sn_ti.case_user_write

프로시저

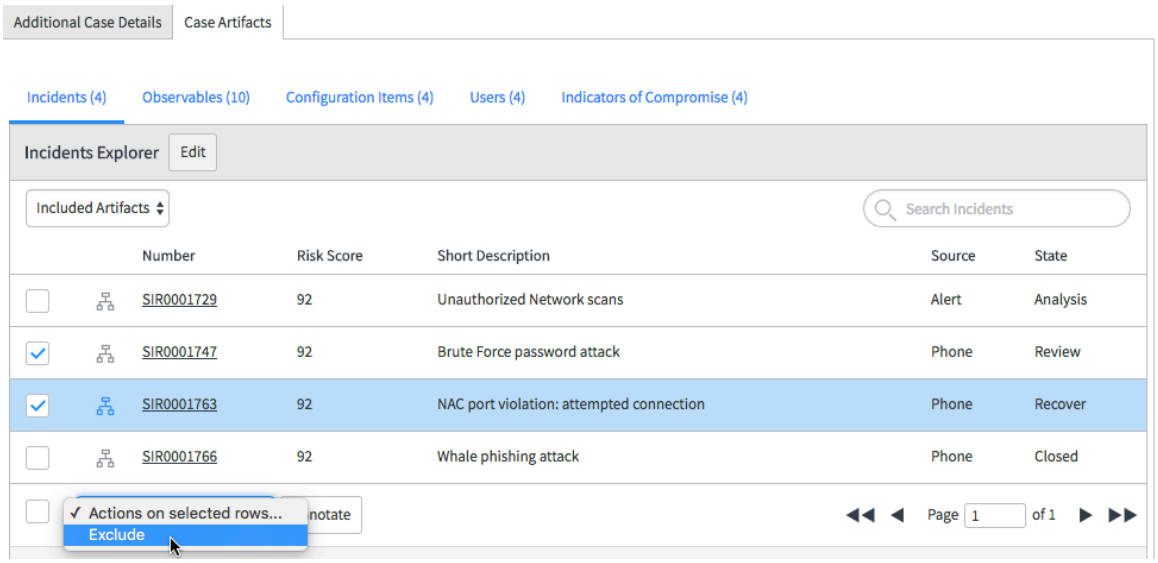
1. 목록에서 제외하려는 아티팩트가 포함된 케이스를 엽니다.

2. 케이스 아티팩트 관련 목록을 클릭합니다.

3. 제외할 아티팩트와 연결된 탭을 클릭합니다.
예를 들어 인시던트를 클릭하여 목록에서 보안 인시던트를 제외합니다.

4. 제외할 아티팩트 기록을 하나 이상 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



5. **Actions on selected** items(선택한 항목에 대한 작업) 드롭다운 목록에서 Exclude(제외)를 선택합니다.
6. 확인 상자에서 제외 를 클릭합니다.
   선택한 아티팩트가 목록에서 제거됩니다.

제외된 보안 아티팩트를 케이스로 반환

케이스의 목록에서 아티팩트를 제외한 후 해당 아티팩트에 대해 계속 작업할 수 있는 케이스로 리턴할 수 있습니다.

시작하기 전에

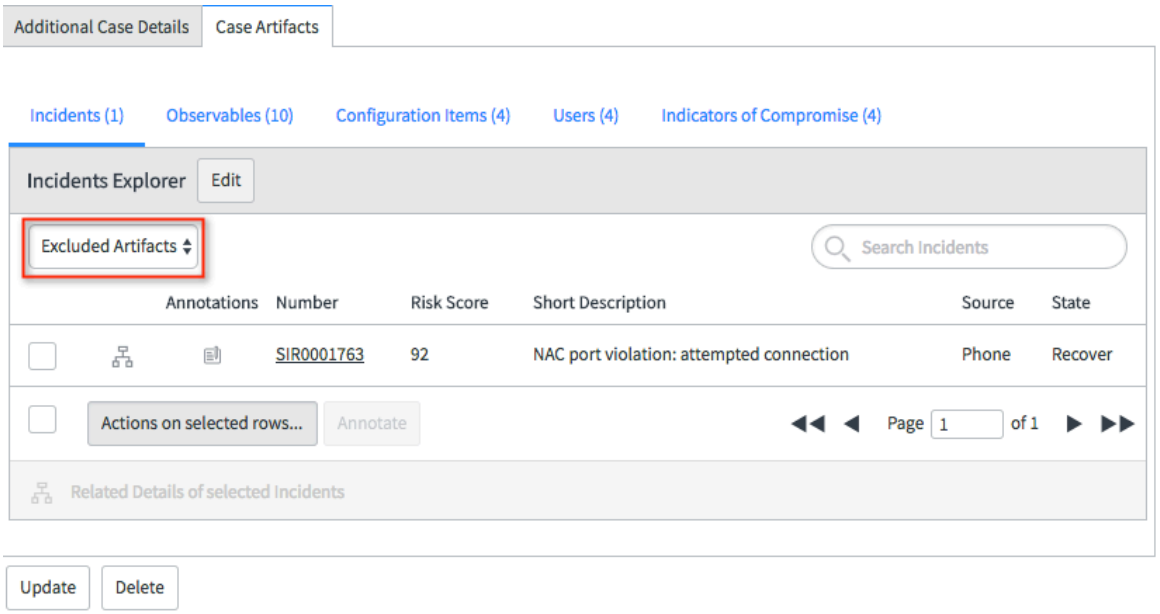
위협 인텔리전스 를 사용하려면 보안 케이스 관리플러그인을 활성화해야 합니다.

필요한 역할: sn_ti.case_user_write

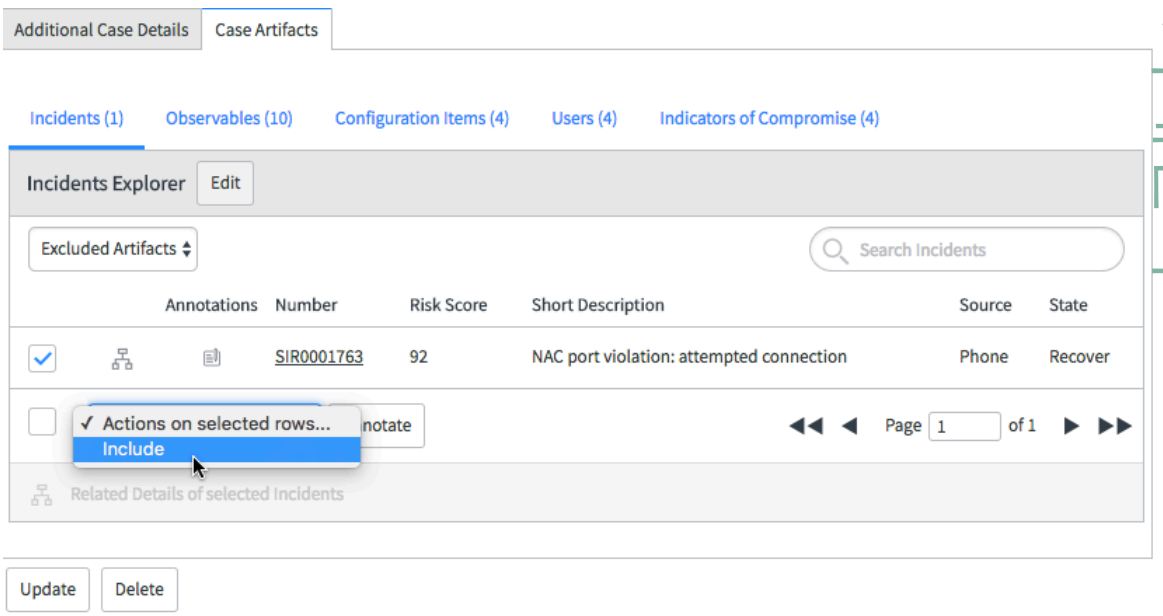
프로시저

1. 목록으로 돌아가려는 목록에서 이전에 제외했던 아티팩트가 포함된 케이스를 엽니다.
2. 케이스 아티팩트 관련 목록을 클릭합니다.
3. 목록으로 돌아가려는 아티팩트와 연관된 탭을 클릭합니다.
4. 아티팩트 필터 드롭다운 목록을 클릭하고 제외된 아티팩트를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



5. 포함 목록으로 돌아갈 아티팩트 기록을 하나 이상 선택합니다.
6. **Actions on selected** items(선택한 항목에 대한 작업) 드롭다운 목록에서 Include(포함)를 선택합니다.



7. 확인 상자에서 포함 을 클릭합니다.
   선택한 아티팩트가 제외된 아티팩트 목록에서 제거되고 케이스에 포함된 아티팩트 목록으로 반환됩니다.

보안 아티팩트에 주석 달기

케이스를 분석할 때 아티팩트에 주석을 추가할 수 있습니다.

시작하기 전에

위협 인텔리전스 를 사용하려면 보안 케이스 관리플러그인을 활성화해야 합니다.

필요한 역할:

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

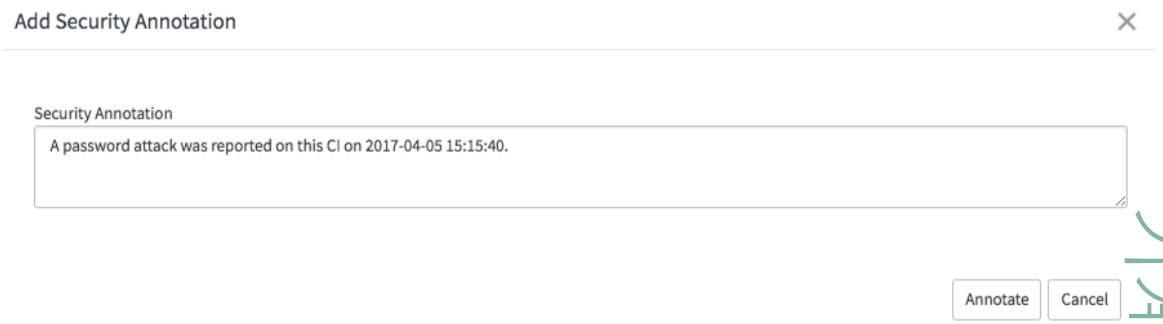
- 주석을 추가하는 sn_ti.case_user_write
- 주석을 보려면 sn_ti.case_user_read

프로시저

1. 주석을 추가할 아티팩트가 포함된 케이스를 엽니다.
2. 케이스 아티팩트 관련 목록을 클릭합니다.
3. 주석을 추가할 아티팩트와 연결된 탭을 클릭합니다.
   예를 들어 침해 표시기 를 클릭하여 IoC에 주석을 추가합니다.
4. 하나 이상의 아티팩트에 주석을 추가하려면 다음 단계를 수행합니다.

   a. 주석을 추가할 아티팩트를 선택합니다.

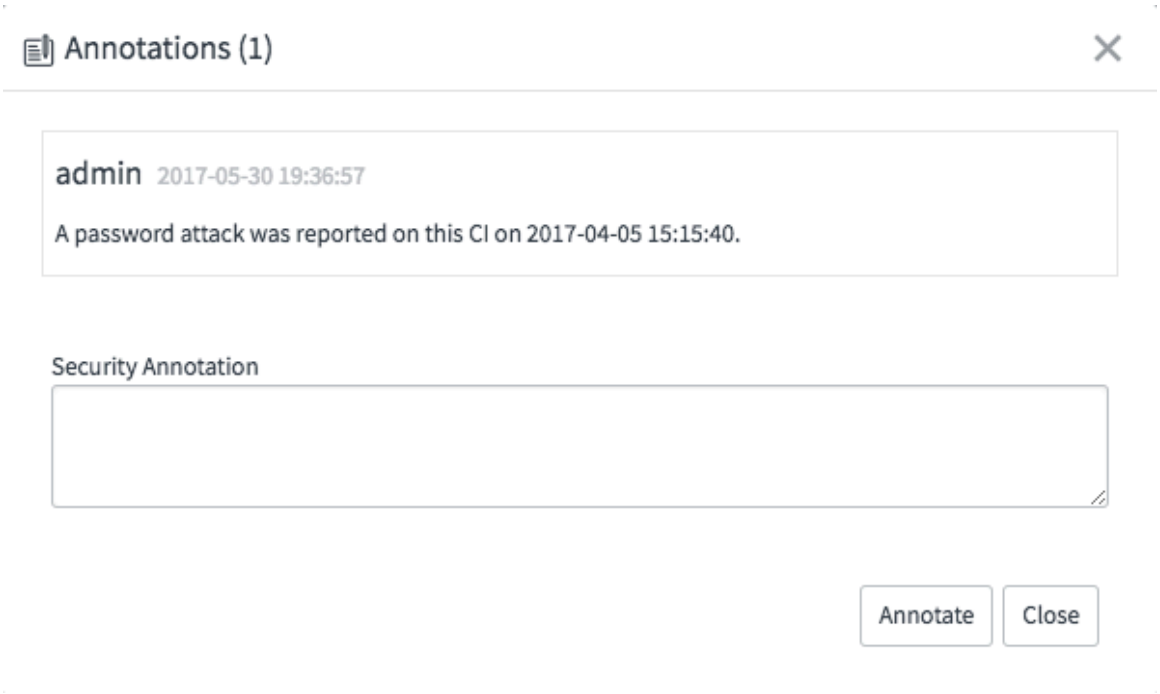
   b. 주석을 클릭합니다.



   c. 주석을 입력하고 주석을 클릭합니다.
   선택한 아티팩트에 주석이 추가됩니다.

5. 아티팩트에 대한 주석을 보려면 주석 보기(주석) 아이콘을 클릭합니다.
   기존 주석이 주석 대화 상자에 나타납니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



6. 보안 주석 상자에 아티팩트에 대한 새 주석을 입력하고 주석 달기를 클릭할 수도 있습니다.

보안 아티팩트 검색

모든 보안 아티팩트 목록에서 키워드 검색을 수행할 수 있습니다.

시작하기 전에

위협 인텔리전스 를 사용하려면 보안 케이스 관리플러그인을 활성화해야 합니다.

필요한 역할: sn_ti.case_user_write

프로시저

1. 보안 아티팩트가 포함된 케이스를 엽니다.

2. 키워드 검색을 수행할 보안 아티팩트의 탭을 클릭합니다.

3. 키워드 검색 상자에 찾으려는 아티팩트의 이름을 입력하기 시작합니다.
항목과 일치하는 아티팩트가 발견되면 표시됩니다.

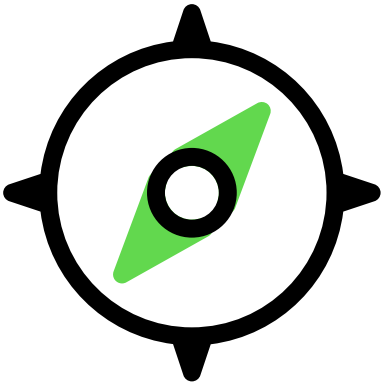
보안 태세 통제

엔터프라이즈 자산 인벤토리 및 보안 도구 범위에 대한 가시성을 확보합니다. 제품과 함께 제공된 정책을 사용하거나 자체 정책을 생성하여 엔드포인트 보호, 구성 관리, 취약성 검사와 같은 주요 보안 도구가 누락된 자산을 식별합니다. 사용자 환경과 관련된 보안 도구 구성에 대한 자산을 모니터링하고 애플리케이션의 보안 격차에 대한 정정 워크플로우를 구성 준수 자동화합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

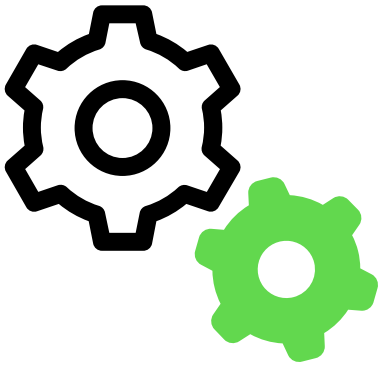
시작하기

탐색



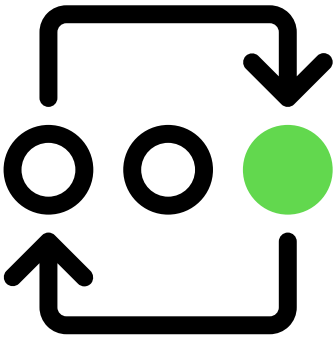
보안 태세 통제 개념 및 기능에 대해 알아보기

설치



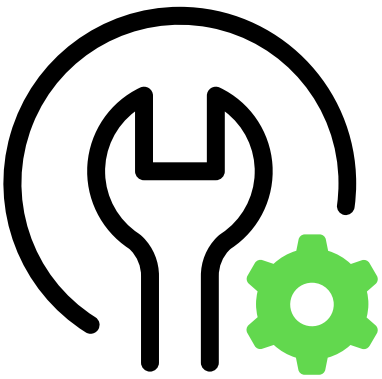
보안 태세 통제 애플리케이션 설치

통합



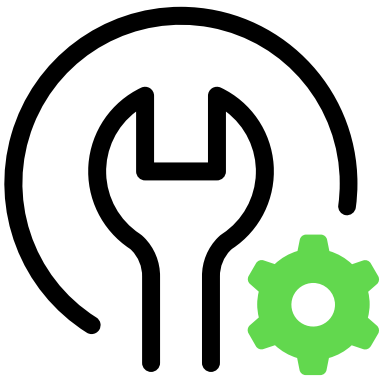
서비스 그래프 커넥터를 보안 태세 통제와 통합

사용



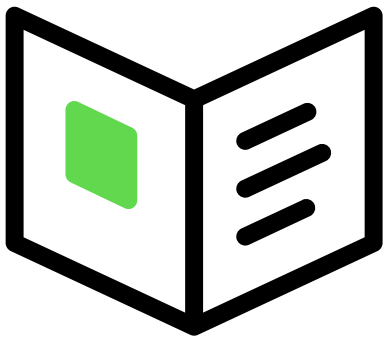
작업 공간을 사용하여 자산을 검색하고 보안 격차를 식별하는 방법에 대해 알아봅니다.

완화 통제 모니터링



사용 가능한 완화 제어를 통해 자산에 대한 어떤 위협을 완화하는지에 대한 인사이트 확보

참조



특정 유형의 도구 범위 간격을 식별하는 데 도움이 되는 시나리오에 대한 상세 정보를 얻습니다. 기본, 하위 및 복제된 정책의 예를 참조하고 지원되는 하드웨어 및 소프트웨어 서비스 그래프 커넥터 목록을 확인합니다.

기계번역

문제 해결 및 도움 받기

- Security Operations 리소스 라이브러리
- Security Operations 커뮤니티
- 알려진 오류 포털에서 알려진 오류 문서 검색
- 연락처 고객 서비스 및 지원

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 태세 통제 탐색

보안 태세 통제 를 사용하면 사이버 보안 팀이 전체 엔터프라이즈 자산 인벤토리에 대한 가시성을 확보하고 전반적인 보안 태세를 결정할 수 있습니다.

보안 분석가는 자산 인벤토리와 서비스 그래프 커넥터 및 ServiceNow 제품(예: 하드웨어 자산 관리 (HAM) 및 ITOM Discovery)에서 임포트한 데이터를 기반으로 보안 도구가 얼마나 잘 배포되고 자산을 포괄하는지에 대한 인사이트를 얻습니다.

또한 보안 분석가는 사용자 지정 정책을 생성하고 통찰력을 구성하여 자산의 내부 보안 표준 준수 여부를 모니터링할 수 있습니다. 취약성 관리자는 (SPC)의 보안 태세 통제 인사이트를 사용하여 고위험 자산의 취약성 정정 우선순위를 지정할 수 있습니다.

SPC 제품은 CSPM(Cloud Security Posture Management) 및 CAHM(Cyber Asset Hygiene Management)을 기반으로 합니다. 보안 태세 통제 는 별도의 구독을 통해 사용할 수 있는 두 개의 애플리케이션으로 ServiceNow# Store구성됩니다.

릴리스 버전	릴리스 정보
보안 태세 통제 코어: v6.2, v6.1, v6.0.	호환성 정보는 KB0856498 Vulnerability Response 호환성 매트릭스 및 릴리스 스키마 변경을 참조하십시오. Security Posture Control release notes
자산 보안 태세 관리: v5.3, v5.1, v5.0	
완화 통제 모니터링 v4.0, v3.0, v2.0	

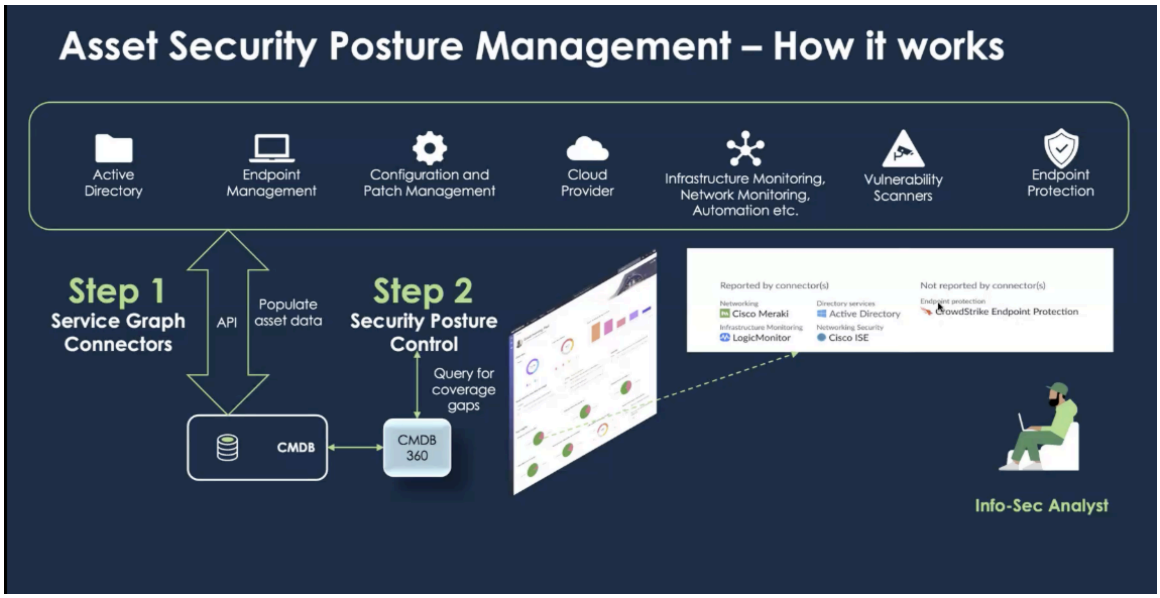
ServiceNow Store 웹 사이트를 방문하면 사용 가능한 모든 앱을 확인하고 스토어에 요청을 제출하는 방법에 대한 정보를 참조할 수 있습니다. 출시된 모든 앱의 누적 릴리스 정보는 ServiceNow Store 버전 기록 릴리스 정보 를 참조하십시오.

SPC 제품을 사용하여 Info-Sec 팀은 다음 작업을 수행할 수 있습니다.

- 온프레미스 및 클라우드 자산에 대한 보안 태세 인사이트를 봅니다. SPC 는 Info-Sec 팀이 엔드포인트 보호가 누락된 자산, 관리되지 않는 자산, 인터넷에 노출된 자산 및 취약성과 관련된 고위험 조합을 식별하는 데 도움이 됩니다.
- 내부 보안 도구 구성 표준을 준수하는지 자산을 모니터링합니다. 예를 들어 엔드포인트 보호 제품의 최신 버전을 사용하고 있는지 확인합니다.
- 구성 준수 애플리케이션에서 발견한 보안 태세 격차에 대한 정정 워크플로우를 자동화합니다 ServiceNow .
- 자산 메타데이터, 보안 도구 범위 데이터 및 취약성 데이터를 기반으로 사용자 지정 정책 및 인사이트를 생성합니다.
- 완화 통제 모니터링으로 다양한 보안 도구가 구성된 방식에 따라 사용 가능한 완화 통제를 통해 자산에 대한 위협을 완화할 수 있는 인사이트을 얻습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

자산 보안 태세 관리 작동 방식



자산 보안 태세 관리(ASPM)는 ServiceNow 제품과 함께 다양한 외부 공급업체 도구(서비스 그래프 커넥터)와의 API 통합을 사용하여 자산의 보안 도구 범위 격차를 식별합니다.

ASPM은 자산에 대해 CMDB에 채워진 데이터를 사용합니다. 자산 데이터는 다양한 범주의 모니터링 도구에서 임포트되고 비교되어 잠재적인 보안 격차를 식별합니다.

예를 들어 인프라 모니터링 및 네트워킹 도구를 다루는 도구에서 보고하는 CMDB에 채워진 자산 데이터가 있다고 가정해 보겠습니다. 그러나 동일한 자산에 대한 이 데이터는 엔드포인트 보호 도구에 의해 채워지거나 보고되지 않습니다. 이러한 다양한 도구에서 보고된 자산 데이터를 비교하면 끝점 보호 에이전트가 누락된 자산이 있음을 확인할 수 있습니다.

자산 보안 태세 관리 는 다양한 도구(서비스 그래프 커넥터) 및 ServiceNow 제품과 API 통합을 사용하여 자산의 보안 도구 범위 격차를 식별합니다. 범주에는 다음이 포함되지만 이에 국한되지는 않습니다.

- 디지털 직원 경험
- 디스커버리
- 엔드포인트 관리
- IT 자산 관리
- 인프라 모니터링
- 네트워킹
- 네트워크 보안
- 네트워크 성능 모니터링
- 구성 및 패치 관리
- 엔드포인트 보호
- 클라우드 제공자
- 애플리케이션 성능 모니터링
- 디렉터리 서비스
- 취약성 평가

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

워크플로우 보안 태세 통제

보안 도구 격차를 식별하는 데는 다음 단계가 포함됩니다.

1. 다양한 범주에서 사용 중인 도구와의 API 연결을 설정하고 활성화합니다. 필요한 API 연결에 대해 ServiceNow Store에서 제공되는 제품에 대한 서비스 그래프 커넥터를 사용할 수 있습니다. 지원되는 서비스 그래프 커넥터에 대한 자세한 내용은 다음 문서를 참조하십시오 Service Graph Connectors . 지원되는 서비스 그래프 커넥터는 별도의 구독을 통해 사용할 수 ServiceNow# Store 있습니다.
2. 애플리케이션과 함께 보안 태세 통제 제공되는 정책을 활성화합니다. 보안 태세 통제 제품은 다음 작업을 수행하여 보안 도구 격차를 찾습니다.
   a. CMDB에서 다양한 서비스 그래프 커넥터로 채워진 모든 고유 자산 목록을 식별합니다.
   b. 이 자산 풀의 특정 범주에서 보고되지 않은 자산을 식별합니다(예: Endpoint Protection). 평가 중인 활성 정책을 기반으로 자산이 식별됩니다.
   c. 특정 범주에서 보고되지 않은 것으로 식별된 자산은 애플리케이션에서 '발견 사항' 또는 '테스트 결과'로 보고됩니다 구성 준수 .
3. 구성 준수 애플리케이션으로 정정할 다른 팀에 "결과"를 자동으로 할당합니다.

고위험 조합

를 사용하면 자산 보안 태세 관리고위험 조합이 있는 자산을 식별할 수도 있습니다. 고위험 조합의 예는 보안 도구가 없고 심각한 취약성이 있으며 인터넷에 노출된 자산을 보여줄 수 있습니다.

애플리케이션과 함께 보안 태세 통제 제공되는 일부 정책은 중요한 취약성과 보안 도구 적용 범위 격차의 고위험 조합을 찾습니다. 그러나 이러한 조합 정책이 작동하려면 애플리케이션과 하나 이상의 취약성 스캐너 통합 제품(예: Qualys, Rapid7) 또는 Tenable Vulnerability Integration 애플리케이션이 설치되어 있어야 합니다취약성 대응. 이러한 애플리케이션은 ServiceNow Store에서 별도로 구독하여 사용할 수 있습니다.

완화 통제 모니터링

(SPC) 작업 공간 내에서 보안 태세 통제 다양한 보안 도구가 구성된 방식에 따라 사용 가능한 완화 제어를 통해 자산에 대한 위협이 완화되는지에 대한 인사이트를 얻을 수 있습니다. 자세한 내용은 완화 통제 모니터링을 참조하세요.

보안 태세 통제에 지원되는 애플리케이션 설치

이 통합에 필요한 애플리케이션은 에서 사용할 수 있습니다 ServiceNow Store. 일부 애플리케이션에는 별도로 다운로드하여 설치해야 하는 의존성이 있습니다.

시작하기 전에

필요한 역할: 모든 애플리케이션의 다운로드, 설치 및 활성화를 위한 관리자

프로시저

1. 필요한 애플리케이션을 ServiceNow Store 인스턴스에서 인스턴스 ServiceNow 로 다운로드합니다.

   보안 태세 통제 (SPC Core) 애플리케이션은 핵심 프레임워크를 제공하며 (ASPM)에 자산 보안 태세 관리 필요합니다. 구성 준수 애플리케이션과 해당 의존성을 사용하면 를 사용하여 자산 보안 태세 관리발견한 보안 제어 격차에 대한 정정 작업을 만들 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Asset Security Posture Management 애플리케이션

애플리케이션	앱 ID
자산 보안 태세 관리	(플러그인 ID: sn_sec_caasm)
ITOM 디스커버리 라이센스	(플러그인 ID: com.snc.itom.discovery.license)
보안 태세 통제 코어	(플러그인 ID: sn_sec_spc_core)
완화 통제 모니터링	(플러그인 ID: sn_sec_mit_ctr)
구성 준수(하위 앱 secops_shared_components 포함)	(플러그인 ID: sn_vulc)
Vulnerability Response 라이선싱 및 사용	(플러그인 ID: sn_vul_licensing)

클라우드 보안 태세 관리 애플리케이션

애플리케이션	앱 ID
검색 플러그인	(플러그인 ID: com.snc.discovery)
클라우드 구성 거버넌스	(플러그인 ID: sn_itom_ccg)
CCG 컨텐츠 팩	(플러그인 ID: sn_itom_ccg_cp)
CMDB CI Class Models	(플러그인 ID: sn_cmdb_ci_class)
클라우드 동작 라이브러리	(플러그인 ID: com.sn.itom.cal)

애플리케이션 다운로드 및 활성화에 대한 자세한 내용은 다음 항목을 참조하십시오.

- 에서 처음으로 애플리케이션 ServiceNow Store 다운로드.
- 애플리케이션 활성화 ServiceNow Store.

2. 애플리케이션을 다운로드한 후 모두 〉 시스템 애플리케이션 〉 모든 사용 가능 애플리케이션 〉 모두.
3. 다운로드한 애플리케이션을 찾아 설치를 선택하여 해당 종속성과 함께 활성화합니다. 애플리케이션과 함께 자동으로 설치되는 모든 종속성 애플리케이션이 애플리케이션 설치 대화 상자에 표시됩니다. 그러나 설치 중에 종속성 플러그인을 설치하라는 메시지가 표시되면 제공된 프롬프트를 따릅니다. 이전 테이블에 나열된 애플리케이션과 의존성이 모두 설치되고 활성화되었는지 확인합니다.

   애플리케이션이 성공적으로 활성화되면 대화 상자가 표시됩니다.

   에서 애플리케이션을 다운로드하고 설치하는 방법에 대한 자세한 내용은 다음을 ServiceNow Store참조하십시오.

   - 제품을 옵트인 ServiceNow 하려면 다음 Opt in to the ServiceNow Store products 의 단계를 따르십시오.
   - 에서 ServiceNow Store구입한 애플리케이션을 설치하려면 다음 Install a ServiceNow Store application 의 단계를 따르십시오.
   - 또는 다른 ServiceNow AI Platform 인스턴스의 애플리케이션에 대한 권리를 관리하려면 다음 Manage entitlements from your ServiceNow instance 의 단계를 따르십시오.
4. 애플리케이션을 설치하고 활성화한 후 다음 보안 태세 통제 그룹에 사용자를 할당합니다.

   이러한 그룹은 SPC 기록을 읽고 편집하는 데 필요한 모든 역할을 상속합니다.

   SPC 관리자 그룹

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 그룹의 사용자는 라이선싱 정보를 포함하여 제품의 모든 기록에 대한 전체 읽기 및 쓰기 액세스 권한을 갖습니다. 이 그룹에 대한 세분화된 역할에는 〔sn_sec_caasm.analyst, sn_sec_caasm.caasm_security_admin 및 sn_sec_spc_core.configure〕가 포함됩니다.

SPC 분석가 그룹

이 그룹의 사용자는 제품의 모든 기록에 대한 전체 읽기 및 쓰기 액세스 권한을 갖지만 라이선싱 정보를 볼 수는 없습니다. 이 그룹의 세분화된 역할에는 〔pa_power_user 및 sn_sec_spc_core.analyst〕가 포함됩니다.

SPC 분석가 읽기 전용 그룹

이 그룹의 사용자는 제품의 모든 기록에 대한 전체 읽기 권한을 갖지만 라이선싱 정보를 볼 수는 없습니다. 이 그룹의 세분화된 역할에는 〔pa_power_user, sn_sec_spc_core.analyst_read, sn_sec_caasm.read 및 cmdb_ms_user〕가 포함됩니다.

지원 애플리케이션 역할

앞의 표에 나열된 및 를 지원하는 SPC자산 보안 태세 관리애플리케이션에는 다음 역할이 필요합니다.

- 구성 준수 관리자 [sn_vulc.admin] - 애플리케이션을 구성 구성 준수 하고, 모든 기록에 대한 가시성을 가지며, 속성을 수정할 수 있습니다. 애플리케이션에서 역할을 구성 준수 할당합니다.
- 취약성 대응 관리자[sn_vulc.admin] - 취약성 대응 애플리케이션 및 취약성 위험 계산기를 구성합니다.
- MID 서버 [mid_server] - MID 서버를 구성합니다.

5. 옵션: CI 조회 규칙을 실행할 때 일부 CI(구성 항목) 클래스를 무시하도록 **ignoreCIClass** 〔sn_sec_cmn.ignoreCIClass〕 시스템 속성을 설정합니다.

(Optional) SPC 관리자 및 SPC 분석가는 제어하지 않으려는 자산에 대한 정보를 수집하지 않도록 특정 하드웨어 또는 가상 클래스를 무시해야 할 수 있습니다. 자세한 내용은 AND CI 클래스 무시 문서를 참조하십시오취약성 대응 CI 조회 규칙 생성.

6. 조정을 수정하고 CMDB 데이터 소스를 재계산하여 속성 값에 대한 진실의 소스를 설정합니다.

CMDB 360 대시보드는 CMDB 360 데이터의 집계 및 분석을 제공합니다. CMDB 360은 CI에 대한 속성 값을 보고하는 모든 검색 소스에 대한 데이터를 수집합니다. CMDB(Configuration Management Database) Workspace의 CMDB 360 뷰를 사용하여 활동을 추적하고 검색 소스의 잠재적인 문제를 식별합니다. 자세한 내용은 CMDB 360 view in CMDB Workspace 문서를 참조하십시오.

용 서비스 그래프 커넥터 보안 태세 통제

보안 태세 통제 는 보안 격차를 식별하는 데 사용되는 자산 데이터의 주요 소스로 API 통합 또는 서비스 그래프 커넥터를 사용합니다.

보안 태세 통제 는 현재 자산에 대한 다양한 데이터를 제공할 수 있는 SGC(서비스 그래프 커넥터)를 지원합니다. 이러한 통합 애플리케이션은 에서 사용할 수 있습니다 ServiceNow Store.

사용할 커넥터를 선택하고 애플리케이션을 다운로드한 후 활성화합니다. 스토어에서 지원되는 커넥터 목록은 더 많은 커넥터를 지원함에 따라 보안 태세 통제 늘어날 것입니다.

기능을 최대한 활용 보안 태세 통제 하려면 다음 서비스 그래프 커넥터 제품을 다운로드하고 활성화하여 아래 나열된 범주를 지원할 수 있습니다.

현재 지원되는 서비스 그래프 커넥터에는 보안 태세 통제 다음 범주가 포함됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 디지털 직원 경험
- 디스커버리
- 엔드포인트 관리: Microsoft Intune 또는 Jamf 장치 및 엔드포인트 관리.
- IT 자산 관리
- 인프라 모니터링
- 네트워킹
- 네트워크 보안
- 네트워크 성능 모니터링
- 구성 및 패치 관리: Microsoft SCCM 또는 IBM Bigfix
- Endpoint Protection: CrowdStrike 또는 SentinelOne.
- 클라우드 제공자: Amazon AWS Cloud, Microsoft Azure, . GCP

> **주:**
> 클라우드 검색이 활성화된 경우 이러한 서비스 그래프 커넥터 제품은 필요하지 않습니다.

- 애플리케이션 성능 모니터링
- 디렉터리 서비스(Active Directory) Microsoft Active Directory
- 취약성 평가: Qualys, Rapid7또는 Tenable.

설치한 후에는 인스턴스의 커넥터 테이블 〔sn_sec_spc_core_connector〕에서 커넥터와 해당 범주를 볼 수 있습니다.

자산 유형과 [sn_sec_spc_core_asset_type_connector] 테이블에서 CI 클래스 및 커넥터에 매핑되는 방식을 볼 수 있습니다.

이러한 테이블의 예와 자세한 내용은 AND를 에 지원되는 소프트웨어 서비스 그래프 커넥터 보안 태세 통제 참조하십시오에 지원되는 하드웨어 서비스 그래프 커넥터 보안 태세 통제. 광범위한 목록은 아니지만 지원되는 커넥터가 어떻게 다양한 데이터를 제공하는지 확인할 수 있습니다.

보안 태세 통제 는 취약성 스캐너 제품에서 보고한 설치된 소프트웨어와 SAM 및 기타 ServiceNow 제품에서 이미 고려된 스캐너에서 보고한 소프트웨어 간에 존재하는 불일치를 찾는 데 도움이 되는 서비스 그래프 커넥터와 함께 사용할 수 있는 SAM(소프트웨어 자산 관리) 및 하드웨어 자산 관리(HAM)과 같은 ServiceNow 제품을 지원합니다.

서비스 그래프 커넥터에 지원되는 애플리케이션의 다운로드, 구성 및 활성화에 대한 자세한 내용은 다음 주제를 참조하십시오.

- Service Graph Connectors .
- 에서 처음으로 애플리케이션 ServiceNow Store 다운로드.
- 애플리케이션 활성화 ServiceNow Store.

보안 태세 통제에 대한 정책

정책은 서비스 그래프 커넥터에서 임포트한 데이터를 기반으로 자산을 감사하여 잠재적인 위반을 찾는 데 도움을 줍니다.

정책

보안 태세 통제 정책은 자산-관계-속성 데이터 모델을 기반으로 합니다. 애플리케이션에 포함된 정책이 있으며 특정 기준을 찾기 위해 고유한 정책을 만들 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

정책의 기준은 해당 자산의 속성 또는 관련 엔터티의 속성에 대한 조건의 형태로 지정할 수 있습니다. 작업 공간의 정책 및 결과 모듈에 있는 정책 작성기에서 자산 유형(하드웨어, 소프트웨어) 및 연결(보고자, 보고되지 않음) 또는 엔터티(자산 소스, 서비스 그래프 커넥터 제품 또는 CMDB 메타데이터)를 찾는 정책을 정의하거나 다른 유형의 특정 기준을 일치시킬 수 있습니다.

정책을 수정하거나 생성하는 데 도움이 되는 방법은 다음과 같습니다.

- 자산 검색 모듈에서 조건을 설정하고 특정 서비스 그래프 커넥터 제품별 자산 또는 커넥터에서 보고한 특정 데이터가 있는 자산을 검색합니다. 검색을 정책으로 저장할 수 있습니다.
- 애플리케이션에 포함된 정책을 복제하여 더 광범위한 정책을 만듭니다. 기존 정책의 조건을 복사한 다음 다시 입력할 필요 없이 구체화할 수 있습니다.
- 새 정책의 시작점으로 선택한 기본 정책을 사용하여 새 정책(하위 정책)을 생성합니다.

자산 유형 및 정책

이러한 기본 또는 최상위 자산 유형을 정책 정의의 시작점으로 사용합니다.

하드웨어 자산

하드웨어 자산은 개인용 컴퓨팅 장치, 서버, 네트워크 장치, 클라우드 가상 머신 및 기타 하드웨어를 포함하는 모든 장치를 나타내는 추상화입니다. 정책은 소프트웨어 자산 관리(SAM) 및 ITOM 디스커버리와 같은 서비스 그래프 커넥터 제품 및 ServiceNow# 제품에서 임포트한 데이터를 기반으로 잠재적 위반에 대해 자산을 감사합니다.

소프트웨어 자산

소프트웨어 자산을 사용하면 서비스 그래프 커넥터에서 임포트한 데이터에서 보고한 설치된 소프트웨어, 취약성 스캐너 제품, Software Asset Management(SAM) 및 기타 ServiceNow 제품에서 이미 고려된 스캐너에서 보고한 소프트웨어 간에 존재하는 불일치를 찾을 수 있습니다.

엔터티 및 엔터티와 보조 엔터티의 관계

엔터티	관계	대상 엔터티	설명
하드웨어 자산	보고자	자산 소스	이 자산을 CMDB에 보고한 소스를 나타냅니다.
하드웨어 자산	보고자 전용	자산 소스	이 자산을 CMDB에 보고하는 유일한 소스를 나타냅니다.
하드웨어 자산	에 의해 보고되지 않음	자산 소스	이 자산을 CMDB에 보고하지 않은 소스를 나타냅니다.
하드웨어 자산	IRM 예외 포함	IRM 예외	통합 위험 관리의 예외 기록을 나타냅니다.
하드웨어 자산	취약성 사용	취약성	이 자산에서 발견된 취약성을 나타냅니다.
하드웨어 자산	구성 찾기 있음	구성	이 자산에서 발견된 구성 및 준수 문제를 나타냅니다.
하드웨어 자산	CMDB 메타데이터 포함	CMDB 메타데이터	이 자산에 대한 CMDB CI 속성의 컬렉션을 나타냅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

엔터티 및 엔터티와 보조 엔터티의 관계

엔터티	관계	대상 엔터티	설명
하드웨어 자산	커넥터 데이터 포함	서비스 그래프 커넥터	이 자산에 대해 선택한 서비스 그래프 커넥터에서 보고한 속성 컬렉션을 나타냅니다.
하드웨어 자산	집계된 데이터 포함	집계된 데이터	지정된 자산에 대해 여러 소스에서 보고한 집계 값이 있는 속성 컬렉션입니다. OS를 예로 들 수 있습니다.
하드웨어 자산	CI 클래스에서	CMDB CI 클래스	특정 CI 클래스 속성에 대한 조건을 정의하는 데 사용됩니다.
하드웨어 자산	클라우드 메타데이터 있음	클라우드 메타데이터	클라우드 메타데이터를 나타냅니다 (클라우드 VM에 적용 가능).
하드웨어 자산	인터넷에 노출된 포트가 있음	Open포트	인터넷에 개방된 포트를 나타냅니다 (클라우드 VM에 적용 가능).
소프트웨어	보고자	자산 소스	이 소프트웨어를 보고한 소스를 나타냅니다.
소프트웨어	보고자 전용	자산 소스	이 소프트웨어를 보고하는 유일한 소스를 나타냅니다.
소프트웨어	에 의해 보고되지 않음	자산 소스	이 소프트웨어를 보고하지 않은 소스를 나타냅니다.
소프트웨어	소프트웨어 세부 정보 포함	소프트웨어	예를 들어, 게시자 및 버전과 같은 소프트웨어 속성의 컬렉션을 나타냅니다.

정책 감사 및 데이터 채움의 예: CMDB의 **CI** 클래스

정책이 특정 서비스 그래프 커넥터에 의해 보고되거나 보고되지 않은 자산 클래스를 검색하려고 시도하는 경우 보안 태세 통제는 CMDB에서 해당 서비스 그래프 커넥터 또는 커넥터 범주에 의해 채워지거나 채워지지 않은 해당 자산 클래스와 관련된 모든 관련 CI(구성 항목) 클래스를 매핑합니다.

예를 들어 정책이 서비스 그래프 커넥터 Jamf Pro에서 보고하는 모든 하드웨어 자산을 찾는다고 가정해 보겠습니다. 다음 논리가 적용됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

1. 보안 태세 통제는 Jamf Pro의 "하드웨어 자산" 클래스에 매핑되는 CMDB의 CI 클래스를 식별합니다.

   주:
   다양한 서비스 그래프 커넥터는 CMDB의 서로 다른 CI 클래스를 채우며, '하드웨어 자산'에서 CI 클래스로의 매핑은 서비스 그래프 커넥터마다 다릅니다.

2. 보안 태세 통제 CMDB의 CI 클래스, 컴퓨터, 서버 및 프린터가 서비스 그래프 커넥터 Jamf Pro의 "하드웨어 자산" 자산 클래스에 매핑되는지 확인합니다.
3. 보안 태세 통제 그런 다음 CMDB의 Jamf Pro 서비스 그래프 커넥터로 서버, 컴퓨터 및 프린터의 세 가지 CI 클래스에 채워진 자산 기록을 쿼리하고 해당 자산을 반환합니다.

   다음 테이블의 'SPC에서 지원하는 CI 클래스' 열은 정책 평가의 일부로 보안 태세 통제 제품에서 쿼리하는 동안 고려하는 CI 기록 클래스를 나타냅니다. 이 테이블은 포괄적인 목록은 아니지만 이 테이블을 사용하여 다양한 범주 및 소스에서 수집된 데이터가 일반적으로 매핑되고 쿼리되는 방식을 확인할 수 있습니다.

애플리케이션에 포함된 정책

애플리케이션에 포함된 작업 공간에서 자산 프로파일 및 정책을 보안 태세 통제 활성화하여 보안 도구의 구성 또는 범위에 격차를 식별할 수 있습니다.

사용자 지정 정책 만들기

사용자 고유의 정책을 만드는 방법에 대한 자세한 내용은 을 참조하십시오 애플리케이션에서 고유한 정책 보안 태세 통제 생성 .

정책의 예는 다음 문서를 참조하십시오 에 대한 기본, 하위 및 복제된 정책의 예 보안 태세 통제.

정책을 만드는 데 필요한 단계에 대한 자세한 내용은 을 참조하십시오 에 대한 사용자 지정 정책 생성 및 활성화 보안 태세 통제 .

지원되는 SGC

지원되는 일부 서비스 그래프 커넥터의 목록은 해당 에 지원되는 소프트웨어 서비스 그래프 커넥터 보안 태세 통제문서를 에 지원되는 하드웨어 서비스 그래프 커넥터 보안 태세 통제 참조하십시오.

완화 통제 정책

(SPC) 작업 공간 내에서 보안 태세 통제 다양한 보안 도구가 구성된 방식에 따라 사용 가능한 완화 제어를 통해 자산에 대한 위협이 완화되는지에 대한 인사이트를 얻을 수 있습니다. 자세한 내용은 완화 통제 정책 문서를 참조하십시오.

애플리케이션에 포함된 보안 태세 통제 정책

애플리케이션에는 보안 태세 통제 중요한 사용 사례와 연결되며 궁극적으로 작업 공간의 방문 페이지(홈 모듈) SPC 에 있는 대시보드에 주요 인사이트로 표시되는 몇 가지 정책이 포함됩니다.

정책 보기

이러한 정책을 보려면 다음으로 이동합니다. 작업 공간 〉 보안 태세 통제 〉 정책 및 결과 〉 모두.

이러한 정책은 기본적으로 비활성화되어 있습니다. 반환된 결과(결과)를 보려면 먼저 활성화해야 합니다. 이러한 정책은 편집할 수 없지만 해당 조건을 시작점으로 복제하여 다른 정책을 만드는 데 사용할 수 있습니다. 자세한 내용은 에서 정책 클론 또는 하위 정책 생성 보안 태세 통제 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이러한 정책을 복제하여 고유한 사용자 지정 정책을 생성할 수 있지만, 복제한 정책은 애플리케이션에 포함된 주요 인사이트와 함께 홈 방문 페이지의 대시보드에 주요 인사이트로 반영되지 않습니다. 그러나 이러한 복제된 정책에 대한 결과를 구성하고 이러한 정책에서 반환된 결과를 볼 수 있습니다.

복제된 정책에 대한 사용자 지정 인사이트 또는 보고서를 구성하거나, 또는 이러한 복제된 정책에 대한 결과를 구성하여 정정을 관리할 수 있습니다. 또한 자체 사용자 지정 정책을 처음부터 생성하여 내부 요구 사항에 따라 보안 제어 범위를 모니터링할 수도 있습니다.

애플리케이션과 함께 제공되는 정책에는 다음과 같은 범주가 포함됩니다.

- 보안 통제 범위를 모니터링하는 정책(엔드포인트 보호 및 취약성 스캐너).
- 관리되지 않는 장치를 식별하는 정책.
- 보안 제어 누락, 인터넷 노출 등과 같은 중요한 조합을 포함하는 유해한 조합을 모니터링하는 정책입니다.
- 완화 통제 모니터링을 위한 API 통합에 대한 SPC 정책입니다.

생성한 정책을 클론하고 활성화한 후에는 작업 공간의 사용자 지정 인사이트 작성기 모듈(탐색기 패널의 마지막 모듈)에서 고유한 사용자 지정 인사이트 기록을 생성해야 합니다. 그런 다음에만 사용자 지정 인사이트 대시보드(작업 영역의 맨 위에서 두 번째 아이콘)에서 정책의 데이터를 볼 수 있습니다.

애플리케이션에 포함된 정책 및 자산 프로파일

애플리케이션에 포함된 정책 및 자산 프로파일을 사용하여 보안 도구의 전반적인 보안 태세 및 구성 격차에 대한 인사이트를 얻습니다. 작업 공간에서 보안 태세 통제 이러한 자산 프로파일 및 정책을 활성화하면 다음 도구의 구성 또는 범위의 격차를 식별할 수 있습니다.

- CrowdStrike
- Microsoft Intune, Defender 및 SCCM
- HCL 큰 수정
- Qualys
- Rapid7

사용자 지정 정책 만들기

사용자 고유의 정책을 만드는 방법에 대한 자세한 내용은 을 참조하십시오 애플리케이션에서 고유한 정책 보안 태세 통제 생성 .

정책의 예는 다음 문서를 참조하십시오 에 대한 기본, 하위 및 복제된 정책의 예 보안 태세 통제.

정책을 만드는 데 필요한 단계에 대한 자세한 내용은 을 참조하십시오 에 대한 사용자 지정 정책 생성 및 활성화 보안 태세 통제 .

완화 통제 모니터링에 사용되는 정책에 대한 자세한 내용은 을 참조하십시오 완화 통제 정책 .

애플리케이션에서 고유한 정책 보안 태세 통제 생성

사용자 환경의 자산과 관련된 데이터를 모니터링하기 위해 고유한 사용자 지정 정책을 만들 수 있습니다. 이러한 정책은 설치 및 활성화한 다양한 서비스 그래프 커넥터에서 임포트할 데이터를 기반으로 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작 방법

기존 정책을 복제하고 조건을 더 추가하거나 정책을 처음부터 새로 만들 수 있습니다. 사용자 지정 정책의 경우 다양한 서비스 그래프 커넥터로 채워진 공통 CMDB 속성에 대한 기준을 포함할 수 있습니다.

또는 기본 정책을 시작점으로 사용하고 승인된 예외에 대한 조건을 GRC(거버넌스, 위험 및 준수) 애플리케이션에 대한 정책과 함께 포함할 수 있습니다. 이러한 예외는 모니터링하지 않고 자산 수에 포함하려는 자산에 대한 것입니다.

사용자 지정 정책의 경우 OS, OS 버전 및 FQDN과 같은 메타데이터에 대한 조건을 포함할 수 있습니다(예: 이전 소프트웨어로 자산을 모니터링하는 데 도움이 됨). 이러한 속성은 지정된 자산에 대해 다양한 서비스 그래프 커넥터로 채워지는 공통 CMDB 속성입니다.

최상위 자산 유형과 이들의 관계에 대한 자세한 내용은 정책의 정책 조건 작성기에서 를 참조하십시오 애플리케이션에 포함된 보안 태세 통제 정책 .

정책의 예는 다음 문서를 참조하십시오 에 대한 기본, 하위 및 복제된 정책의 예 보안 태세 통제.

정책을 만드는 데 필요한 단계에 대한 자세한 내용은 을 참조하십시오 에 대한 사용자 지정 정책 생성 및 활성화 보안 태세 통제 .

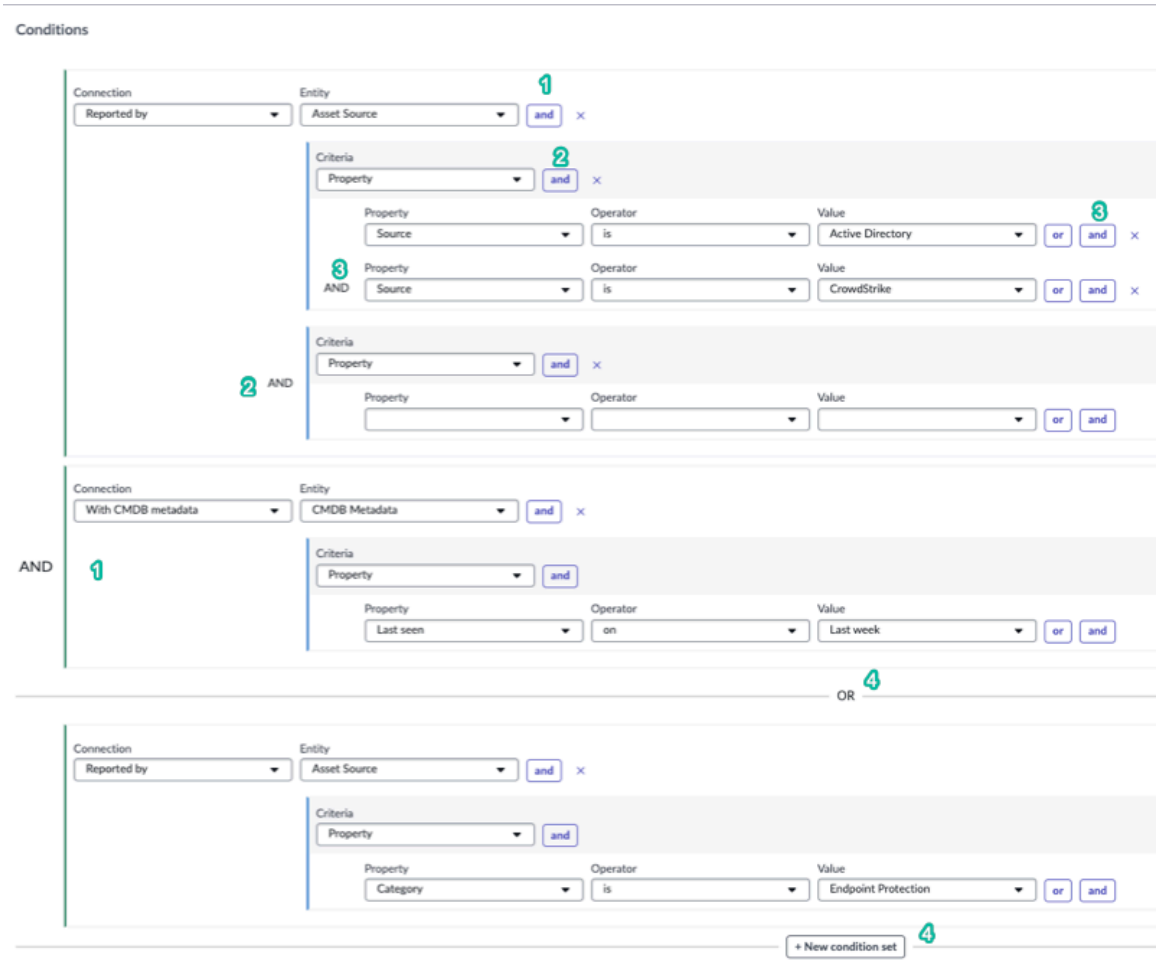
조건 작성기에서 **AND, OR** 데코레이터 사용

작업 공간의 정책 및 결과 모듈에서 조건 작성기를 사용하여 하드웨어 및 소프트웨어의 최상위 자산 유형에서 보조 엔터티로 이동합니다. 선택에 따라 필드가 표시되고 기준을 수정하거나 추가합니다.

조건 작성기의 AND, OR 데코레이터를 사용하면 정책에 대해 반환하려는 반환 데이터의 논리를 설정할 수 있습니다.

데코레이터	설명	이미지에 참조된 번호
새 조건 집합을 보려면 맨 위에 있는 연결 및 엔터티 필드 옆에 있는 **AND** 를 선택합니다.	현재 연결 엔터티 기준과 다른 연결 엔터티의 새 기준 사이에 논리 AND를 추가합니다.	1
새 기준 및 속성 조건 세트에 대한 기준 또는 속성 필드 오른쪽에 있는 **AND** 를 선택합니다.	현재 연결-엔터티 기준과 동일한 연결-엔터티 아래에 새 기준 사이에 논리 AND를 추가합니다.	2
새 속성 조건 세트를 보려면 속성 필드 오른쪽에 있는 **OR/AND** 를 선택합니다.	현재 속성과 동일한 Connection-Entity-Criteria의 새 속성 사이에 논리적 OR/AND 속성을 추가합니다.	3
새 조건 집합에 대해 **+** 새 조건 세트를 선택합니다.	모든 현재 기준의 조건 세트와 새 조건 세트 사이에 논리 OR을 추가합니다.	4

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



기본 정책, 복제 및 하위 정책 사용

여러 정책을 사용하여 자산을 평가하고 사용자 지정 인사이트를 생성할 수 있습니다. 사용자 지정 정책을 생성하거나 기존 정책을 빠르게 편집하는 데 도움이 되는 다음 옵션이 있습니다.

- 정책 클론 - 정책의 복사본을 만듭니다. 정책의 이름과 조건은 제목에 '사본'과 함께 표시됩니다. 조건이 표시되고 편집할 수 있습니다. 에서 활성화된 정책 편집 보안 태세 통제 문서를 참조하십시오.
- 하위 정책 생성 - 시작한 정책의 이름이 새 기록에 "기본 정책"으로 표시됩니다. 기본 정책의 조건은 새 정책에서 상속되고 비어 있는 새 조건 세트가 표시됩니다. 에서 정책 클론 또는 하위 정책 생성 보안 태세 통제 문서를 참조하십시오.
- 제외 정책 – 선택한 정책의 자산 찾기가 결과에서 제외되도록 사용자 지정 정책에 정책을 추가합니다. 에 대한 사용자 지정 정책 생성 및 활성화 보안 태세 통제 문서를 참조하십시오.

메타데이터 및 **CMDB** 필터링

보안 팀이 이전 소프트웨어로 자산을 모니터링하는 것이 중요할 수 있습니다. 하드웨어 자산 유형 다음에 "CMDB 메타데이터 포함" 연결로 시작하여 아래에 나열된 공통 속성을 포함하는 정책 기준을 지정할 수 있습니다. 이 목록은 모두 포함된 목록이 아닙니다. 이 메타데이터를 수집하려면 서비스 그래프 커넥터로 채워진 CMDB 메타데이터 연결에서 속성을 사용할 수 있어야 합니다.

- RAM
- 호스트 이름
- 일련 번호
- OS 도메인

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- OS 버전
- 디스크 공간
- 마지막으로 발견됨
- OS
- 처음 발견됨
- CPU 카운트
- MAC 제조업체
- NIC
- IP 주소
- 위치
- FQDN
- 네트워크 마스크
- IP 버전
- 일련 번호 유형
- OS 서비스 팩

v3.0 보안 태세 통제부터 :

"CMDB 메타데이터 포함" 연결을 사용하면 호스트 이름 속성을 추가하고 일치 정규 표현식 연산자를 사용하여 하드웨어 자산 유형에 대한 조건에 정규 표현식을 입력할 수 있습니다. 예를 들어, 'lp'를 입력하는 경우 호스트 이름에 두 번째와 세 번째 문자가 'lp'인 모든 랩톱을 찾을 수 있습니다.

"처음 발견됨": "처음 발견됨" 타임스탬프 속성으로 선택한 시간 범위 내에 소스에서 처음으로 검색된 자산입니다.

'마지막으로 발견됨': 모든 소스에서 '지난 n일 이내에 마지막으로 발견'된 자산입니다. 값으로 최대 30일의 일수를 입력합니다. 예를 들어, 지난 3일 동안 Active Directory에서 "마지막 로그온"으로 자산을 모니터링하려면 값으로 3을 입력합니다.

소프트웨어 자산 유형: "소프트웨어 상세 정보" 연결로 시작하는 경우 원하는 소프트웨어 데이터 및 메타데이터를 임포트하도록 소프트웨어 게시자를 찾거나 설치한 SGC를 사용합니다.

하드웨어 자산 유형의 경우 특정 모델 및 모델 정보를 기반으로 하는 장치에 대해 연결 "CMDB 메타데이터 포함"과 함께 연결 "모델 정보 있음"을 사용할 수 있습니다.

또한 하드웨어 자산 유형을 사용하면 소스(예: Qualys)에서 보고했지만 ServiceNow ITOM Discovery에서 보고하지 않은 모든 자산을 검색할 수 있습니다.

정책 스키마에 보안 태세 통제 대한 자세한 내용은 을 참조하십시오보안 태세 통제에 대한 정책.

GRC(거버넌스, 리스크 및 컴플라이언스) 애플리케이션의 예외 사항

IRM(통합 위험 관리) 예외는 GRC(거버넌스, 위험 및 준수) 제품에서 승인된 예외가 있는 자산입니다. 정책에는 이러한 자산을 모니터링하고 계산에 포함하지 않도록 예외에 대한 조건을 추가하는 옵션이 있습니다.

예를 들어, 일부 자산에는 IRM을 사용하는 특정 통제 목표에 대해 승인된 예외가 있을 수 있습니다. 반환된 일치 항목을 줄이기 위해 정보 보안 팀은 이미 승인된 IRM 예외를 사용하여 보안 제어 모니터링에서 해당 자산을 제외할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

에 대한 주요 인사이트 및 구성된 인사이트 보안 태세 통제

핵심 및 구성된(사용자 지정) 인사이트는 자산과 일치하는 평가 기준에 따라 생성되고 업데이트되는 시각적 보고서를 제공합니다. 인사이트는 대시보드에서 보안 제어 메트릭을 모니터링하는 데 도움이 됩니다.

주요 인사이트

자산 평가에 사용되는 기준은 애플리케이션에 포함된 정책에 의해 제공됩니다.

- 주요 인사이트는 애플리케이션에 포함된 정책을 사용합니다.
- 구성된 인사이트는 애플리케이션에 포함된 정책, 사용자 지정 정책 또는 이 둘의 조합을 사용하여 만들 수 있습니다.

보안 태세 통제 작업 공간의 홈(방문 페이지)에서 개요 아래의 주요 인사이트 섹션에는 애플리케이션과 함께 포함된 정책에 따라 생성 및 업데이트되는 시각적 보고서가 표시됩니다. 이러한 인사이트는 애플리케이션에도 포함되어 있으며 다음 정보를 표시합니다.

- 엔드포인트 보호 에이전트 설치됨: 엔드포인트 보호가 있거나 없는 총 자산 수입니다.
- 관리되는 장치 범위: 관리되지 않는 자산과 비교하여 관리되는 자산 수입니다.
- 취약성 스캔 적용 범위: 외부 공급업체 취약성 스캐너에서 알려진 취약성을 검사하지 않은 자산과 비교하여 검사한 총 자산 수입니다.
- 중요 취약성이 있는 자산: 중요 취약성이 있는 총 자산 수 중 자산 수입니다.
- 중요도별 취약한 항목: 심각도별로 세분화된 취약한 항목의 총 수입니다. 알려진 취약성이 CMDB의 자산과 일치하면 취약한 항목이 생성됩니다. 이 통찰력을 사용하려면 취약성 대응 애플리케이션과 하나 이상의 스캐너 통합(Qualys, Rapid7 또는 Tenable 취약성 통합)을 설치해야 합니다. 이러한 모든 애플리케이션은 에서 사용할 수 있습니다 ServiceNow# Store.
- 찾기별 상위 3개 정책: 자산에 대해 가장 많은 결과(일치)를 반환하는 정책입니다.

구성된 인사이트

주요 인사이트에서 찾을 수 없는 자세한 정보를 원하는 경우 고유한 인사이트를 생성할 수 있습니다. 이러한 구성된 인사이트를 생성하고 평가에 기존 정책 또는 사용자 지정 정책을 사용할 수 있습니다. 구성된 인사이트는 작업 공간의 상단에서 두 번째 아이콘인 구성된 인사이트 대시보드 모듈에 표시됩니다.

다음과 같은 유형의 인사이트를 구성할 수 있습니다.

- 비교 차트: 막대형 차트를 사용하여 여러 정책 간의 결과를 비교합니다.
- 정책 일치 수 위젯: 정책과 일치하는 장치 수를 봅니다.
- 정책 일치율 차트: 원형 차트에서 정책과 일치하는 장치의 백분율을 봅니다. 총 자산 풀을 SPC에서 모니터링하는 모든 자산 또는 현재 선택한 정책이 생성되는 기본 정책과 일치하는 자산으로 선택할 수 있습니다.
- 정책 추세 차트: 다양한 정책과 일치하는 자산의 추세를 봅니다.

구성된 인사이트를 만드는 단계에 대한 자세한 내용은 을 참조하십시오 보안 태세 통제를 위해 구성된 인사이트 생성 및 활성화 .

그룹

사용자 지정 인사이트 작성기 모듈에서 새 기록을 생성할 때 구성된 인사이트에 그룹을 생성하거나 할당해야 합니다. 그룹을 사용하면 구성된 인사이트 대시보드에서 보고서를 구성할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

인사이트를 그룹으로 구성할 수 있습니다. 각 그룹에는 21개의 위젯 또는 인사이트가 있을 수 있습니다.

작업 공간 보안 태세 통제 사용

작업 공간에는 보안 태세 통제 자산에 대한 임포트한 데이터를 구성, 사용 및 모니터링하는 데 사용하는 모듈이 포함되어 있습니다.

역할

SPC 관리자 그룹

이 그룹의 사용자는 라이선싱 정보를 포함하여 제품의 모든 기록에 대한 전체 읽기 및 쓰기 액세스 권한을 갖습니다. 이 그룹에 대한 세분화된 역할에는 〔sn_sec_caasm.analyst, sn_sec_caasm.caasm_security_admin 및 sn_sec_spc_core.configure〕가 포함됩니다.

SPC 분석가 그룹

이 그룹의 사용자는 제품의 모든 기록에 대한 전체 읽기 및 쓰기 액세스 권한을 갖지만 라이선싱 정보를 볼 수는 없습니다. 이 그룹의 세분화된 역할에는 〔pa_power_user 및 sn_sec_spc_core.analyst〕가 포함됩니다.

SPC 분석가 읽기 전용 그룹

이 그룹의 사용자는 제품의 모든 기록에 대한 전체 읽기 권한을 갖지만 라이선싱 정보를 볼 수는 없습니다. 이 그룹의 세분화된 역할에는 〔pa_power_user, sn_sec_spc_core.analyst_read, sn_sec_caasm.read 및 cmdb_ms_user〕가 포함됩니다.

지원 애플리케이션 역할

및 자산 보안 태세 관리를 지원하는 SPC 애플리케이션에는 다음 역할이 필요합니다.

- 구성 준수 관리자 [sn_vulc.admin] - 애플리케이션을 구성 구성 준수 하고, 모든 기록에 대한 가시성을 가지며, 속성을 수정할 수 있습니다. 애플리케이션에서 역할을 구성 준수 할당합니다.
- 취약성 대응 관리자[sn_vulc.admin] - 취약성 대응 애플리케이션 및 취약성 위험 계산기를 구성합니다.
- MID 서버 [mid_server] - MID 서버를 구성합니다.

작업 공간의 모듈

작업 공간에 액세스하려면 다음으로 이동하십시오. 작업 공간 〉 보안 태세 통제 홈(방문 페이지)이 표시됩니다. 작업 공간에는 보안 태세 통제 다음과 같은 모듈이 있습니다.

모듈

모듈	설명
홈	개요, 주요 인사이트 및 주요 사용 케이스 범위 섹션에서 데이터 시각화 및 기타 정보를 보고 자산을 모니터링하는 데 도움이 됩니다. 이 페이지에 제공된 정보를 통해 IT, IT 및 보안 관리자와 기타 주요 이해 관계자에게 전반적인 보안 태세의 상태를 보고할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈

모듈	설명
	에 대한 주요 인사이트 및 구성된 인사이트 보안 태세 통제 및 보안 태세 통제에 대한 정책 문서를 참조하십시오.
구성된 인사이트	생성, 구성 및 활성화하는 자산에 대한 데이터 시각화를 봅니다. 에 대한 주요 인사이트 및 구성된 인사이트 보안 태세 통제 문서를 참조하십시오.
자산 검색	설정한 조건에 따라 환경에서 자산을 빠르게 검색합니다. 해당 조건을 정책에 커밋하기 전에 일련의 조건이 있는 자산을 찾을 수 있는지 확인합니다. 검색 기준을 충족하는 자산의 미리 보기를 얻을 수 있도록 이러한 검색을 세분화할 수 있습니다. 준비가 되면 조건을 정책으로 저장할 수 있습니다. 보안 태세 통제에서 자산 검색 생성 문서를 참조하십시오.
자산 프로파일	자산 프로파일을 생성하고 정의하여 SPC 정책으로 다양한 범주의 장치를 모니터링합니다. 특정 유형의 자산에 대한 정책을 실행할 수 있도록 자산 프로파일을 정책에 통합합니다. 자산 프로파일을 기반으로 하도록 구성된 인사이트 대시보드에서 인사이트를 필터링합니다. 에서 자산 프로파일 생성 보안 태세 통제 문서를 참조하십시오.
정책 및 결과	정책 생성, 클론, 편집 및 활성화합니다. 애플리케이션에 포함된 정책이 있으며 직접 만들 수 있습니다. 정책은 자산을 감사하여 잠재적인 위반과 일치하는 항목을 찾습니다. 인사이트, 시각화 및 사용 사례는 정책에 따라 달라집니다. 보안 태세 통제에 대한 정책 문서를 참조하십시오. 정책 조건과 일치하는 자산은 발견 사항으로 보고되고 정정을 위해 애플리케이션에 매핑 구성 준수 됩니다. 보안 태세 통제: 결과 구성 및 보기 문서를 참조하십시오.
커넥터 및 사용 케이스 설정	설치된 SGC(서비스 그래프 커넥터) 및 API 통합을 활성화하고 상태를 확인합니다. 서비스 그래프 커넥터 및 API 통합은 자산에 대한 데이터를 임포트하는 데 사용하는 소스입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈

모듈	설명
	다양한 (SGC)가 지원되며 에서 ServiceNow# Store사용할 수 있습니다. 주요 사용 사례를 설정하고 모니터링합니다. 사용 사례는 특정 유형의 도구 범위 간격을 식별하는 데 도움이 되도록 구성하는 다양한 시나리오입니다. 각 사용 사례에는 자산의 잠재적 위반을 감사하는 정책이 필요합니다. 의 사용 사례, 정책 예시 및 지원되는 서비스 그래프 커넥터 보안 태세 통제 문서를 참조하십시오.
사용자 지정 인사이트 빌더	고유한 데이터 시각화를 생성합니다. 사용자 지정 인사이트는 정책 및 임포트된 데이터의 감사 결과에 의해 업데이트되는 시각적 보고서를 제공합니다. 활성화하면 사용자 지정 인사이트가 구성된 인사이트 모듈의 대시보드에 표시됩니다. 그룹을 사용하여 대시보드에서 인사이트에 대한 데이터가 표시되는 위치를 결정할 수 있습니다. 보안 태세 통제를 위해 구성된 인사이트 생성 및 활성화 문서를 참조하십시오.

작업 공간의 모듈을 사용하여 도구 범위의 격차 식별

보안 도구 격차를 식별하려면 다음 단계를 수행해야 합니다.

1. 다양한 범주에서 사용 중인 도구와의 API 연결을 설정하고 활성화합니다. 필요한 API 연결에 대해 ServiceNow Store에서 제공되는 제품에 대한 서비스 그래프 커넥터를 사용할 수 있습니다. 지원되는 서비스 그래프 커넥터에 대한 자세한 내용은 해당 Service Graph Connectors 문서를 용 서비스 그래프 커넥터 보안 태세 통제 참조하십시오. 지원되는 서비스 그래프 커넥터는 별도의 구독을 통해 사용할 수 ServiceNow# Store 있습니다.
2. 특정 기준에 따라 하나 이상의 자산 검색을 수행하여 인벤토리를 가져옵니다.
3. 보안 태세 통제 애플리케이션과 함께 제공되는 정책을 활성화합니다. 또한 자체 정책을 생성하고 자산 검색 결과에 따라 활성화할 수도 있습니다.
4. 자산을 모니터링하는 데 도움이 되도록 직접 구성된 인사이트를 생성하고 활성화합니다.
5. 다양한 보안 도구가 구성된 방식에 따라 사용 가능한 완화 제어를 통해 자산에 대한 위협을 완화할 수 있는 인사이트을 얻으려면 문서를 참조하십시오 와 함께 완화 통제 모니터링 사용 보안 태세 통제.
6. 구성 준수 애플리케이션에서 정정 워크플로우를 자동화하는 규칙을 설정합니다.

보안 도구 격차를 식별하는 데는 다음 단계가 포함됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

1. 애플리케이션과 함께 보안 태세 통제 제공되는 정책을 활성화합니다. 보안 태세 통제 제품은 다음 작업을 수행하여 보안 도구 격차를 찾습니다.
   a. CMDB에서 다양한 서비스 그래프 커넥터로 채워진 모든 고유 자산 목록을 식별합니다.
   b. 이 자산 풀의 특정 범주에서 보고되지 않은 자산을 식별합니다(예: Endpoint Protection). 평가 중인 활성 정책을 기반으로 자산이 식별됩니다.
   c. 특정 범주에서 보고되지 않은 것으로 식별된 자산은 애플리케이션에서 '발견 사항' 또는 '테스트 결과'로 보고됩니다 구성 준수 .
2. 구성 준수 애플리케이션으로 정정할 다른 팀에 "결과"를 자동으로 할당합니다.

사용자 지정 정책 만들기

사용자 고유의 정책을 만드는 방법에 대한 자세한 내용은 을 참조하십시오 애플리케이션에서 고유한 정책 보안 태세 통제 생성 .

정책을 만드는 데 필요한 단계에 대한 자세한 내용은 을 참조하십시오 에 대한 사용자 지정 정책 생성 및 활성화 보안 태세 통제 .

정책의 예는 다음 문서를 참조하십시오 에 대한 기본, 하위 및 복제된 정책의 예 보안 태세 통제.

애플리케이션에 포함된 보안 태세 통제 정책 활성화

애플리케이션에 포함된 정책을 활성화 보안 태세 통제 해야만 해당 정책과 일치하는 자산을 모니터링할 수 있습니다. 기본적으로 애플리케이션에 포함된 정책은 활성화되지 않습니다.

시작하기 전에

애플리케이션에 포함된 정책을 활성화하기 전에 필요한 모든 필수 구성 요소가 충족되는지 확인해야 합니다.

- 필요한 서비스 그래프 커넥터가 활성화되었는지 확인합니다.
- 해당하는 경우 취약성 대응과 같은 필수 애플리케이션이 설치 및 활성화되었는지 확인합니다.
- 완화 통제 모니터링에 사용되는 정책에 대한 자세한 내용은 단원을 참조하십시오 완화 통제 정책.

> **주:**
>
> 애플리케이션에 포함된 정책은 편집할 수 없지만 클론 정책 및 하위 정책 생성 기능을 사용하여 해당 기준에 따라 새 정책을 생성할 수 있습니다. 이러한 기능은 추가 옵션 메뉴(세로 점 3개)에서 사용할 수 있습니다.

필요한 역할: SPC 관리자 그룹 또는 SPC 분석가 그룹

프로시저

1. 다음으로 이동 작업 공간 〉 보안 태세 통제 〉 정책 및 결과 〉 모두.

   정책이 활성화되었는지 확인하려면 활성 열에서 해당 상태(true 또는 false)를 확인합니다.

2. 정책 기록을 클릭하여 엽니다.
3. 애플리케이션과 함께 포함된 정책 기록에 대해 다음과 같은 옵션을 사용할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵션	설명
정책 활성화	정책 조건과 일치하는 자산을 모니터링하고 결과를 생성하려면 정책을 활성화합니다. 사용 가능한 경우 정책 비활성화를 선택하여 이 정책에 대한 자산 평가 및 결과 생성을 중지합니다.
찾기 구성	정책에 대한 결과를 생성하려면 모달에서 예를 선택합니다. 할당 규칙 구성 링크를 선택하여 구성 준수 애플리케이션에서 할당 규칙을 설정하고 해결을 위해 정책에 대한 결과를 할당합니다. **주:** 자산 유형으로 "소프트웨어"를 사용하여 생성하는 정책의 경우 정책을 저장하고 사용자 지정 인사이트를 생성할 수 있지만 정책 기록에서 결과를 구성할 수는 없습니다.
정책 복제	표시된 정책의 모든 조건을 시작점으로 하여 새 정책을 생성합니다. 자세한 내용은 에 대한 사용자 지정 정책 생성 및 활성화 보안 태세 통제 문서를 참조하십시오.
하위 정책 생성	현재 정책의 조건을 상속하는 하위 정책을 생성합니다. 현재 정책 조건은 새 기록의 '기본 정책' 필드에 표시되며 조건을 더 추가합니다.
정책 비활성화(활성화된 정책에만 표시됨)	해당 정책에 대해 자산을 모니터링하거나 평가하지 않으려면 활성 정책을 비활성화합니다. 이 편집 옵션은 활성화된 정책 기록에서만 볼 수 있습니다.
찾기 보기	새 탭을 열고 사용 가능한 경우 일치하는 자산을 확인합니다. 발견 사항은 CTR 또는 정책에 대한 테스트 결과 기록으로도 참조됩니다.

에 대한 사용자 지정 정책 생성 및 활성화 보안 태세 통제

도구 범위 및 기타 고위험 조합에 대한 자산을 모니터링하기 위해 고유한 사용자 지정 정책을 생성합니다.

시작하기 전에

자세한 내용은 정책을 만드는 데 필요한 단계를 이해하는 데 도움이 되도록 다음을 참조하십시오 에 대한 기본, 하위 및 복제된 정책의 예 보안 태세 통제. 이 예시에서는 기본 정책을 만들고, 기본 정책을 사용하여 하위 정책을 만들고, 정책을 복제하는 데 필요한 단계를 안내합니다.

정책의 예는 다음 문서를 참조하십시오 에 대한 기본, 하위 및 복제된 정책의 예 보안 태세 통제.

필요한 역할: SPC 관리자 그룹 또는 SPC 분석가 그룹

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 작업 공간 〉 보안 태세 통제 〉 목록 〉 정책 〉 모두.
2. 새 정책을 선택합니다.
3. 상단의 이름 옆에 있는 연필 아이콘을 선택하여 메타데이터를 수정합니다.

   필드를 작성합니다.

밭	묘사
이름	정책의 고유한 이름입니다.
중요도	목록에서 하나를 선택합니다.
간단한 설명	정책에 대한 고유한 설명입니다.

4. 메타데이터 저장을 선택합니다.
5. 자산 유형의 경우 목록에서 on을 선택합니다.
6. 옵션: 아무 것도 선택하지 않거나 하나 또는 둘 다 선택하십시오.

   (Optional) 연결 및 엔터티 필드가 표시됩니다.
7. 연결 필드 목록에서 하나를 선택합니다.
   대상 엔터티 필드는 선택에 따라 자동으로 채워집니다. 새 기준 필드가 속성, 연산자 및 값 필드와 함께 표시됩니다. 자산 유형 및 관계 스키마에 대한 자세한 내용은 다음 문서를 참조하십시오 보안 태세 통제에 대한 정책.
8. 속성 목록에서 하나를 선택합니다.
9. 범주 또는 소스를 선택합니다.
10. 연산자를 선택하고 커넥터 범주(예: 엔드포인트 관리) 또는 범주 제품 이름(소스)을 입력합니다.
11. 옵션: 조건 작성기를 사용하여 조건 또는 조건 세트를 더 추가합니다.

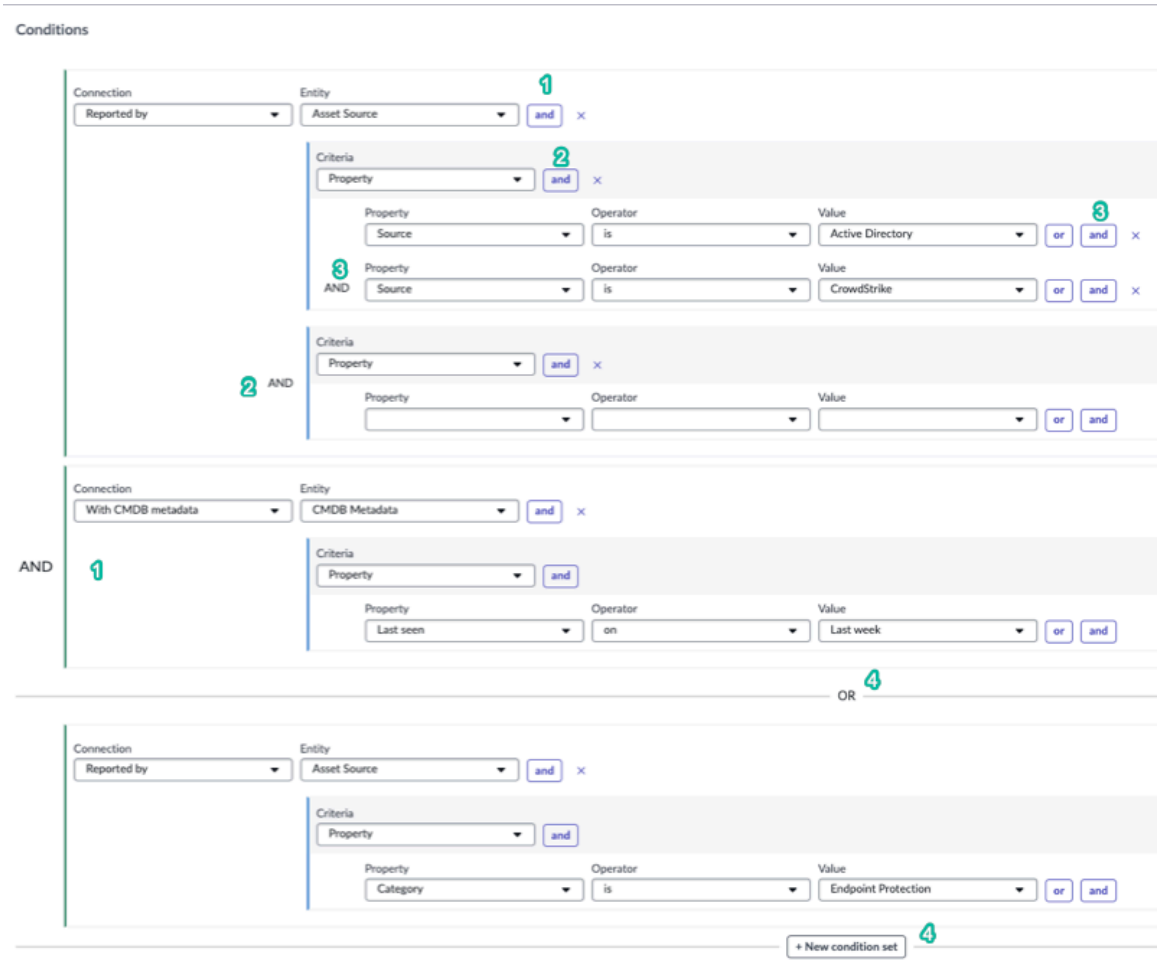
    (Optional) 조건 작성기를 사용하여 하드웨어 및 소프트웨어의 최상위 자산 유형에서 보조 엔터티로 이동합니다. 선택에 따라 필드가 표시되고 기준을 수정하거나 추가합니다.

    조건 작성기의 AND, OR 데코레이터를 사용하면 정책에 대해 반환하려는 반환 데이터의 논리를 설정할 수 있습니다. 자세한 내용은 다음 테이블과 이미지를 참조하십시오.

데코레이터	설명	이미지에 참조된 번호
새 조건 집합을 보려면 맨 위에 있는 연결 및 엔터티 필드 옆에 있는 **AND** 를 선택합니다.	현재 연결 엔터티 기준과 다른 연결 엔터티의 새 기준 사이에 논리 AND를 추가합니다.	1
새 기준 및 속성 조건 세트에 대한 기준 또는 속성 필드 오른쪽에 있는 **AND** 를 선택합니다.	현재 연결-엔터티 기준과 동일한 연결-엔터티 아래에 새 기준 사이에 논리 AND를 추가합니다.	2
새 속성 조건 세트를 보려면 속성 필드 오른쪽에 있는 **OR/AND** 를 선택합니다.	현재 속성과 동일한 Connection-Entity-Criteria의	3

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

데코레이터	설명	이미지에 참조된 번호
	새 속성 사이에 논리적 OR/AND 속성을 추가합니다.	
새 조건 집합에 대해 + 새 조건 세트를 선택합니다.	모든 현재 기준의 조건 세트와 새 조건 세트 사이에 논리 OR을 추가합니다.	4



12. 편집을 완료한 후 정책 저장을 선택합니다.
정책이 저장되었습니다. 지금 활성화하거나 나중에 다시 활성화하도록 선택할 수 있습니다.
13. 정책 저장 옆에 있는 추가 옵션 메뉴에서 결과 구성을 선택합니다.
14. 필드에 내용을 입력합니다.

옵션	설명
이 정책에 대한 결과를 생성하시겠습니까?	일치하는 자산에 대한 결과를 생성하려면 예를 선택합니다. 데이터를 임포트한 후 찾은 항목 보기를 선택하면 정책 기록에 표시됩니다. 결과를 생성하지 않으려면 아니요 를 선택합니다.
담당 규칙 구성	구성 준수 애플리케이션에서 정정 결과를 할당하기 위한 담당 규칙을 설정하려면 링크를

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵션	설명
	선택합니다. [sn_vulc_assignment_rule_list] 테이블에는 구성 준수에서 사용할 수 있는 기본 할당 규칙이 있습니다.

15. 구성 저장을 선택합니다.

    정책을 저장하고 활성화하면 다음 실행에서 예약된 서비스 그래프 커넥터에서 임포트한 데이터를 평가합니다. 작업 공간의 구성된 인사이트 대시보드에 데이터를 표시하려면 사용자 지정 인사이트 빌더 모듈에서 새 인사이트를 생성해야 합니다. 구성된 인사이트를 활성화하면 해당 데이터가 작업 공간의 구성된 인사이트 대시보드에 표시됩니다.

에서 활성화된 정책 편집 보안 태세 통제

자산에 더 잘 맞도록 조건을 사용자 지정하는 데 도움이 되도록 활성화된 정책을 편집할 수 있습니다.

시작하기 전에

애플리케이션에 포함된 정책은 편집할 수 없지만 해당 정책에서 하위 정책을 클론하고 만들 수는 있습니다. 에서 정책 클론 또는 하위 정책 생성 보안 태세 통제 문서를 참조하십시오.

정책을 편집하고 변경 내용을 게시하면 버전이 추적되고 정책 기록과 관련 테스트 결과에 버전 번호가 표시됩니다.

활성화된 정책을 편집하기 전에 편집하는 동안 정책에서 자산을 계속 평가하지 않도록 정책을 비활성화하는 것이 좋습니다.

필요한 역할: SPC 관리자 그룹 또는 SPC 분석가 그룹

프로시저

1. 다음으로 이동 작업 공간 〉 보안 태세 통제 〉 목록 〉 정책 〉 모두.
2. 정책 기록을 클릭하여 엽니다.
3. 정책 편집을 선택합니다.
   처음 편집하는 경우 활성화된 편집 모드 종료 버튼 옆에 비활성화된 버튼 2개(변경 사항 저장 및 변경 사항 게시)가 표시됩니다. 이전에 이 정책을 편집하고 초안으로 저장한 경우 #### ## ### #### .
4. 편집하고 하나를 선택하여 계속합니다.

옵션	설명
변경 내용 저장	변경 내용을 초안으로 저장하고 편집 모드로 돌아갑니다. 이 시점에서 변경 내용이 게시되지 않았으므로 정책으로 돌아가 나중에 편집을 계속할 수 있습니다.
변경 사항 게시	변경 내용을 새 버전의 정책으로 게시하고 편집 모드를 자동으로 종료합니다. 정책의 결과 보기 버튼에 있는 새 버전의 정책에 결과가 표시되는 데 다소 시간이 걸릴 수 있습니다. 새 버전의 정책을 게시하는 경우 변경한 정책에 대한 기존 결과를 종결할 수 있는 옵션이

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵션	설명
	있습니다. 변경된 정책에 대한 결과만 보려면 원래 정책의 기존 결과를 닫는 것이 좋습니다. 이 시점에서 취소하거나 편집 모드를 종료하면 이 정책에 대해 게시되지 않은 편집 내용이 있다는 메시지가 표시됩니다. 기존의 관련 테스트 결과(정보)를 종결하도록 선택하면 구성 준수 애플리케이션의 상태 전환 프로세스에 따라 테스트 결과 및 정정 작업 상태가 전환됩니다. 자세한 내용은 애플리케이션의 테스트 결과 및 정정 작업 상태 전환 보안 태세 통제 문서를 참조하십시오.
버전 이력 보기	게시된 변경 사항의 경우 버전이 추적되고 버전 번호가 정책 기록 및 관련 테스트 결과에 표시됩니다.
편집 모드 끝내기	변경 내용을 저장하지 않고 종료하거나 변경 내용을 저장한 후 게시하지 않고 종료합니다. 변경 내용을 저장하고 게시하지 않는 경우 새 버전을 게시해야 결과를 생성할 수 있습니다.
정책 비활성화(활성화된 정책에만 표시됨)	해당 정책에 대해 자산을 모니터링하거나 평가하지 않으려면 활성 정책을 비활성화합니다. 이 편집 옵션은 활성 정책 기록에서만 볼 수 있습니다.
찾기 보기	새 탭을 열고 사용 가능한 경우 일치하는 자산을 확인합니다. 결과는 정책에 대한 CTR 또는 테스트 결과 기록으로도 참조됩니다.

5. 정책을 초안으로 저장하고 편집 모드를 종료한 후 다음 옵션 중에서 선택합니다.

옵션	설명
정책 편집	편집 모드로 돌아갑니다.
정책 비활성화(활성화된 정책에만 표시됨)	해당 정책에 대해 자산을 모니터링하거나 평가하지 않으려면 활성 정책을 비활성화합니다. 이 옵션은 활성 정책 기록에서만 볼 수 있습니다.
추가 옵션 메뉴	
찾기 구성	정책에 대한 결과를 생성하려면 모달에서 예를 선택합니다. 보안 태세 통제: 결과 구성 및 보기 문서를 참조하십시오.
정책 복제	정책 기록의 복사본을 생성합니다. 에서 정책 클론 또는 하위 정책 생성 보안 태세 통제 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵션	설명
하위 정책 생성	이 정책을 기본으로 사용하여 새 정책을 생성합니다. 에서 정책 클론 또는 하위 정책 생성 보안 태세 통제 문서를 참조하십시오.
정책 삭제	정책 목록에서 정책 기록을 제거합니다.
찾기 보기	새 탭을 열고 사용 가능한 경우 일치하는 자산을 확인합니다. 발견 사항은 정책에 대한 테스트 결과 기록(CTR)에도 참조됩니다.
연결된 기록 보기	게시된 정책의 경우 사용 가능한 경우 사용자 지정 인사이트를 확인합니다. 보안 태세 통제를 위해 구성된 인사이트 생성 및 활성화 문서를 참조하십시오.

에서 정책 클론 또는 하위 정책 생성 보안 태세 통제

기존 정책을 복제하고 조건을 추가하여 사용자 지정 정책을 생성합니다. 기존 정책에서 하위 정책을 생성할 수도 있습니다.

시작하기 전에

정책을 클론하여 고유한 사용자 지정 정책을 만들 수 있습니다. 조건을 다시 입력하지 않고도 기존 정책을 확장할 수 있도록 정책을 기본으로 사용하여 정책을 복제하거나 하위 정책을 만들 수 있습니다. 기본 정책의 모든 조건은 하위 정책에서도 상속됩니다. 자세한 내용은 에서 정책 클론 또는 하위 정책 생성 보안 태세 통제 문서를 참조하십시오.

애플리케이션에 포함된 모든 정책을 복제할 수 있지만 정책 일치는 홈 방문 페이지의 대시보드에 주요 인사이트로 반영되지 않습니다. 애플리케이션에 포함된 정책에 대한 주요 인사이트만 홈 방문 페이지에 표시됩니다.

생성한 정책을 클론하고 활성화한 후에는 작업 공간의 사용자 지정 인사이트 빌더 모듈(탐색기 패널의 마지막 모듈)에서 직접 구성된 인사이트 기록을 생성해야 합니다. 그래야만 구성된 인사이트 대시보드(작업 영역 맨 위에서 두 번째 아이콘)에서 정책의 데이터를 볼 수 있습니다.

필요한 역할: SPC 관리자 그룹 또는 SPC 분석가 그룹

프로시저

1. 다음으로 이동 작업 공간 〉 보안 태세 통제 〉 목록 〉 정책 〉 모두.
2. 복제할 정책 기록을 선택합니다.
3. 정책 활성화 옆에 있는 추가 옵션 메뉴에서 하나를 선택합니다.
4. 옵션: 기본 정책을 선택하고 새 정책의 기준으로 정책을 선택합니다.

   (Optional) 기존 정책의 조건을 새 정책의 시작점으로 상속하려는 경우 이 옵션을 선택할 수 있습니다.
5. 옵션: 제외 정책을 선택하고 이 정책의 결과에서 제외하려는 정책을 선택합니다.
   제외된 정책과 일치하는 새 정책의 결과는 결과에 포함되지 않습니다.
6. 복제된 정책의 경우 조건을 편집합니다.
   조건 작성기의 자산-연결-엔터티 관계에 대한 자세한 내용은 다음 문서를 보안 태세 통제에 대한 정책참조하십시오. 조건 작성기의 데코레이터에 대한 자세한 내용은 다음 문서를 참조하십시오 애플리케이션에서 고유한 정책 보안 태세 통제 생성.
7. 변경 내용 저장으로 정책을 편집하고 저장합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

정책이 작업 공간의 목록 모듈에 있는 모두 목록에 표시됩니다.

8. 정책을 활성화하려면 다음에 설명된 에 대한 사용자 지정 정책 생성 및 활성화 보안 태세 통제단계를 수행합니다.
9. 옵션: 정책 삭제를 선택하여 정책을 삭제합니다.
   삭제 옵션은 애플리케이션과 함께 제공되는 정책 또는 결과를 생성한 정책에 대해 지원되지 않습니다. 결과가 있는 정책만 비활성화할 수 있습니다.

보안 태세 통제를 위해 구성된 인사이트 생성 및 활성화

인사이트를 직접 생성할 수 있습니다. 구성된 인사이트는 기존 정책 또는 고유한 사용자 지정 정책을 사용하여 만들 수 있는 인사이트입니다.

시작하기 전에

구성된 인사이트 대시보드에서 데이터를 보려면 먼저 인사이트 기록을 생성하고 활성화해야 합니다. 작업 공간의 구성된 인사이트 대시보드 모듈에는 최대 6개의 인사이트와 21개의 차트가 있을 수 있습니다.

사용자 지정 인사이트에 사용하는 모든 정책을 활성화해야 합니다.

자산 유형으로 "소프트웨어"를 사용하여 생성하는 정책의 경우 정책을 저장하고 사용자 지정 인사이트를 생성할 수 있지만 정책 기록에서 결과를 구성할 수는 없습니다.

필요한 역할: SPC 관리자 그룹 또는 SPC 분석가 그룹

프로시저

1. 다음으로 이동 작업 공간 〉 보안 태세 통제 〉 인사이트 작성기.

   이 방문 페이지에는 3개의 탭이 있습니다.

   활성

   활성화된 사용자 지정 인사이트입니다. 활성화된 사용자 지정 인사이트는 구성된 인사이트 방문 페이지(작업 공간 상단에서 두 번째 아이콘)에 표시됩니다.

   비활성

   비활성 사용자 지정 인사이트입니다. 비활성화된 인사이트는 인사이트와 이를 지원하는 지원 정책이 활성화될 때까지 구성된 인사이트 방문 페이지에 표시되지 않습니다.

   모두

   모든 활성 및 비활성 구성된 인사이트입니다.

2. 페이지 오른쪽에 있는 새 인사이트를 선택하여 새 기록을 생성합니다.
3. 유형 필드의 선택 목록에서 인사이트를 선택합니다.

옵션	설명
비교 차트	최대 5개의 보험에 대해 자산을 일치시키는 횟수를 비교합니다.
정책 일치 수 위젯	정책과 일치하는 총 자산 수입니다.
정책 일치율 차트	총 자산에서 정책과 일치하거나 일치하지 않는 백분율입니다.
정책 일치 추세 차트	정책과 일치하는 자산의 기록 추세입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 하나를 선택합니다.
   - 하드웨어 자산 또는 클라우드 가상 머신
   - 소프트웨어
5. 인사이트에 대한 그룹을 선택합니다.
   인사이트는 하나 이상의 그룹에 속해야 합니다. 사용자 지정 인사이트 작성기 모듈에서 새 기록을 생성할 때 구성된 인사이트에 그룹을 생성하거나 할당해야 합니다. 그룹을 사용하면 구성된 인사이트 대시보드에서 보고서를 구성할 수 있습니다.
6. 인사이트 데이터에 대해 원하는 정책과 해당 레이블을 선택합니다.
7. 저장을 선택합니다.
   인사이트는 비활성 인사이트 탭에 저장됩니다.
8. 새 인사이트를 활성화하려면 비활성 목록에서 기록을 열고 활성화를 선택합니다.
   데이터는 인사이트의 정책과 연결된 서비스 그래프 커넥터에 대해 다음으로 예약된 임포트에서 수집되고 데이터는 작업 공간의 사용자 지정 인사이트 대시보드 모듈에 표시됩니다.

에서 자산 프로파일 생성 보안 태세 통제

자산을 그룹화할 조건이 있는 자산 프로파일을 생성합니다. 이러한 자산 프로파일을 정책에 사용할 수 있습니다.

시작하기 전에

필요한 역할: SPC 관리자 그룹 또는 SPC 분석가 그룹

프로시저

1. 다음으로 이동 모두 〉 보안 태세 통제 작업 공간 〉 자산 프로파일.
2. 새로 만들기를 선택합니다.
   조건 작성기가 표시됩니다. 이름에는 프로파일을 만든 날짜 및 시간이 포함됩니다.
3. 펜 아이콘을 선택하여 고유한 이름으로 프로파일 이름을 편집합니다.
4. 메타데이터 저장을 선택합니다.
5. 연결 목록에서 하나를 선택합니다.

   자산 프로파일은 세 가지 연결 유형을 지원합니다.

   - **CMDB** 메타데이터 사용 - 호스트 이름, OS, OS 버전, 처음 및 마지막으로 발견됨(예: 네트워크 어댑터나 설치된 소프트웨어) 등의 CMDB CI 속성 컬렉션입니다.
   - 집계된 데이터 포함 - 지정된 자산에 대해 여러 소스에서 보고한 집계 값이 있는 속성 컬렉션입니다. 예를 들어 원본에서 OS 버전을 보고할 수 있는 다양한 방법(windows11, Win11, Windows 11 등)이 있습니다.
   - **CI** 클래스에서 - 컴퓨터, 서버, 가상 머신 인스턴스 등을 포함하는 CI 클래스의 컬렉션입니다.

   이 자산 프로파일 정책 작성기의 연산자 및 논리는 다음에 애플리케이션에서 고유한 정책 보안 태세 통제 생성설명된 것과 유사합니다.
6. 생성을 선택합니다.
   프로파일이 자산 프로파일 목록에 표시됩니다.

   자산 프로파일을 모든 정책에 연결할 수 있습니다.
7. 다음으로 이동 모두 〉 보안 태세 통제 작업 공간 〉 정책 및 결과.
8. 정책을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

9. 정책 및 프로필 섹션에서 하나 이상의 자산 프로필을 선택합니다.
10. 변경 사항 저장을 선택합니다.
    정책은 서비스 그래프 커넥터에서 임포트한 데이터를 기반으로 자산을 감사하고 추가한 자산 프로파일의 조건을 포함합니다. 자산 프로파일을 필터로 추가할 수 있습니다 보안 태세 통제를 위해 구성된 인사이트 생성 및 활성화 .
11. 다음으로 이동 모두 〉 보안 태세 통제 작업 공간 〉 구성된 인사이트.
    이 페이지에 데이터가 표시되기 전에 그래야 합니다 보안 태세 통제를 위해 구성된 인사이트 생성 및 활성화 .

    이 페이지의 시각화는 정책에 따라 구성되므로 자산 프로파일을 사용하여 필터링할 수 있습니다. 다음 단계에 따라 시각화에 대한 데이터를 필터링합니다.
12. 필터 아이콘을 선택합니다.
13. 선택을 선택합니다.
14. 사용 가능 열에서 자산 프로파일을 선택하고 적용됨 열로 이동합니다.
15. 적용을 선택합니다.
    사용자 지정 인사이트 시각화는 선택한 자산 프로필이 포함된 정책에 대한 데이터를 표시하도록 필터링됩니다. 필터 창의 메시지는 추가한 자산 프로파일의 결과로 필터링된 구성된 인사이트 수를 나타냅니다. 추세 데이터를 업데이트하려면 SPC 정책 실행 예약된 작업을 완료해야 하기 때문에 추세 데이터에 대한 업데이트가 지연될 수 있습니다.

에서 자산 프로파일 삭제 보안 태세 통제

자산 프로파일을 삭제할 수 있습니다. 자산 프로파일의 조건이 다음 정책 감사에 포함되지 않도록 자산이 정책에 연결된 경우 삭제합니다.

시작하기 전에
필요한 역할: SPC 관리자 그룹 또는 SPC 분석가 그룹

프로시저

1. 다음으로 이동 모두 〉 보안 태세 통제 작업 공간 〉 자산 프로파일.
2. 프로파일 기록을 선택합니다.
3. 추가 작업 메뉴 아이콘(⋮)을 선택하고 자산 프로파일 삭제를 선택합니다.
4. 옵션: 대화 상자에서 정책 검토 를 선택하여 이 프로필이 연결된 정책을 봅니다.
   자산 프로파일이 포함된 정책이 연결된 정책 탭에 나열됩니다.
5. 삭제할 자산 프로파일이 있는 탭을 선택합니다.
6. 추가 작업 메뉴 아이콘을 선택하고 자산 프로파일 삭제를 선택합니다.
   이는 하드 삭제입니다. 자산 프로파일의 조건은 정책에서 제거되며 최신 결과를 얻기 위해 다음 야간 정책 감사에 포함되지 않습니다.

보안 태세 통제: 결과 구성 및 보기

보안 태세 통제 작업 공간의 보안 태세 통제에서 정책 평가로 생성된 결과를 볼 수 있습니다.

결과 개요

일치하는 자산은 모두 '발견 사항'으로 보고됩니다. 정책 실행에서 생성될 결과를 구성하여 이러한 결과를 정정을 위해 다양한 팀에 할당하거나 보고에 사용할 수 있습니다. 보안 태세 통제는 이러한 결과를 구성 준수 모듈에 "테스트 결과"로 게시합니다. 할당, 그룹화(정정 작업 생성), 정정 대상, 예외와 관련된 구성 준수 애플리케이션의 모든 관리 통제는 보안 태세 통제에 의해 생성된 결과에 대해 지원됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

결과 유형:

도구 범위

이 유형은 보안 도구 범위 격차를 나타냅니다. 이 결과 유형은 "커넥터에 의해 보고됨" 및 "커넥터에 의해 보고되지 않음" 관계를 사용하는 정책에 적용할 수 있습니다.

인터넷 노출

이 유형은 클라우드 자산의 인터넷 노출을 나타냅니다. 이 결과 유형은 CloudVM에서 "Has-internet-exposed-port" 관계를 사용하는 정책에 적용할 수 있습니다.

고위험 조합

이 유형은 둘 이상의 위험 요소가 연결된 문제, 즉 중요한 취약성이 있는 자산과 엔드포인트 보호 에이전트가 누락된 문제를 나타냅니다.

정책에 사용되는 관계에 따라 결과 구성을 선택하면 사용 가능한 찾기 유형이 표시됩니다. 예를 들어 '중요한 취약성이 있는 클라우드 자산, 엔드포인트 보호 누락 및 SSH 포트 22가 인터넷에 열려 있음'과 같이 둘 이상의 위험 요소가 있는 정책에 대한 결과 구성을 선택하면 다음 옵션이 생성할 수 있는 찾기 유형으로 표시됩니다.

1. 고위험 조합
2. 도구 범위
3. 인터넷 노출

이 정책과 일치하는 모든 자산당 하나의 결과를 생성하는 "고위험 조합" 유형의 찾기를 생성하도록 선택할 수 있습니다. 또는 "도구 범위" 및 "인터넷 노출" 유형의 결과를 생성하도록 선택할 수 있으며, 이 경우 정책과 일치하는 각 자산당 두 개의 결과("도구 범위" 유형 중 하나와 "인터넷 노출" 유형 중 하나)가 생성됩니다.

찾기 유형 또는 테스트 결과를 사용하여 Configuration Compliance에서 담당 규칙을 작성하여 정정을 위해 이러한 문제를 각 팀에 라우팅할 수 있습니다. 예를 들어 '도구 범위' 결과를 IT 운영 팀에 보내고 '인터넷 노출'을 애플리케이션 팀에 보낼 수 있습니다.

그러나 정정 소유자 중 한 명이 문제를 해결하면 이러한 결과가 조합을 찾는 정책에서 생성되기 때문에 다른 결과가 자동으로 종결됩니다. 예를 들어 IT 운영 팀이 엔드포인트 보호 에이전트를 설치하여 "도구 범위" 찾기를 종결하는 경우, 이 결과는 문제의 조합을 찾는 정책에서 생성되기 때문에 자산이 인터넷에 연결되어 있더라도 이 정책에서 생성된 "인터넷 노출" 찾기가 자동으로 종결됩니다. 자산에 대한 인터넷 노출 문제를 추적하려면 자산에 대한 인터넷 노출만 찾고 다른 위험 요소는 찾지 않는 다른 정책을 만드는 것이 좋습니다.

결과를 볼 수 있는 위치

정책 평가에 의해 생성된 결과를 볼 수 있는 이러한 옵션이 있습니다.

- 다음으로 이동 보안 태세 통제 작업 공간 〉 목록 〉 정보 〉 모두.
- 정책 기록에서 결과 보기를 선택합니다.
- 구성 준수 애플리케이션에서 테스트 결과를 선택하고 소스가 **ServiceNow** SPC임을 기준으로 기록을 필터링합니다.

대시보드

보안 태세 통제 작업 공간의 홈(방문 페이지)에 다음과 같은 시각화가 표시됩니다.

개요

- 자산: 온프레미스 및 클라우드에서 모니터링되는 자산의 수입니다.
- 중요도별 찾기: 총 자산 중 중요한 찾기 수입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 상위 5개 소스로 모니터링되는 자산: 자산에 대해 보고하는 상위 5개 서비스 그래프 커넥터입니다.
- 클라우드 계정: AWS 및 Azure에서 모니터링하는 클라우드 계정의 수입니다.
- 열린 결과와 종결된 결과: 아직 처리 중이거나 해결 대기 중인 기록과 해결된 기록의 비교입니다.

주요 인사이트

- 엔드포인트 보호 에이전트가 설치됨: 엔드포인트 보호가 있거나 없는 자산의 총 수입니다.
- 관리되는 장치 범위: 관리되지 않는 자산과 비교한 관리 자산 수입니다.
- 취약성 스캔 적용 범위: 검사한 총 자산 수와 외부 공급업체 취약성 스캐너에서 알려진 취약성을 검사하지 않은 자산 수입니다.
- 중요 취약성이 있는 자산: 중요 취약성이 있는 총 자산 수 중 자산 수입니다.
- 중요도별 취약한 항목: 심각도별로 세분화된 취약한 항목의 총 수입니다. 알려진 취약성이 CMDB의 자산과 일치하면 취약한 항목이 생성됩니다.
- 찾기별 상위 3개 정책: 자산에 대해 가장 많은 결과(일치)를 반환하는 정책입니다.

주요 사용 케이스 범위

시각화 및 개선 지원을 선택하여 주요 사용 사례에 대해 활성화된 서비스 그래프 커넥터 및 정책을 확인합니다.

애플리케이션의 테스트 결과 및 정정 작업 상태 전환 보안 태세 통제

보안 태세 통제 애플리케이션에서 정책을 수정하면 결과(구성 테스트 기록) 및 관련 정정 작업의 상태가 영향을 받습니다.

테스트 결과와 정정 작업 간의 상태 전환 시나리오

일부 예외를 제외하고, 상태는 일반적으로 애플리케이션에서 테스트 결과와 정정 작업 구성 준수 간에 전환하는 것과 동일한 방식으로 보안 태세 통제에서 결과(테스트 결과)와 관련 정정 작업 간에 전환됩니다. 그러나 보안 태세 제어에서 정책을 수정하면 변경 사항이 결과 및 관련 정정 작업에서 상태가 전환되는 방식에 영향을 미칩니다.

다음 표는 정책을 편집 및 게시(편집), 비활성화 또는 삭제하는 경우 결과에서 상태가 어떻게 전환되는지 보여줍니다.

의 구성 준수상태 변경에 대한 자세한 내용은 를 참조하십시오 애플리케이션의 테스트 결과 및 정정 작업 상태 전환 구성 준수.

주:
의 구성 준수v14.9부터 다음 용어의 이름이 변경되었습니다.

용어 변경

v14.9 이전 용어	용어 **v14.9** 이상
테스트 결과 그룹	정정 작업
그룹 규칙	정정 작업 규칙
정책	테스트 그룹

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

정책 감사가 강화되어 폐기된 자산이 활성화된 정책에 의해 평가되지 않도록 합니다. 자산의 상태가 폐기 됨에서 활성으로 다시 전환되면 다음 정책 평가에 포함됩니다.

정책이 다음과 같은 경우...	다음에 대한 기존 찾기 기록의 필드 값...	다음으로 전환...
비활성화함	결과	원래 값 유지
	상태	종결됨
	해결	부실

정책이 다음과 같은 경우...	다음에 대한 기존 찾기 기록의 필드 값...	다음으로 전환...
선택한 기존 결과를 종결하는 옵션으로 편집됨	결과	원래 값 유지
	상태	종결됨
	해결	잘못된 결과

정책이 다음과 같은 경우...	다음에 대한 기존 찾기 기록의 필드 값...	다음으로 전환...
선택한 기존 결과를 유지하는 옵션으로 편집됨	결과	유효한(통과) 테스트 케이스는 원래 값을 유지하고 잘못된 테스트 케이스(실패)는 종결됩니다.
	상태	종결됨
	해결	잘못된 결과

정책이 다음과 같은 경우...	다음에 대한 기존 찾기 기록의 필드 값...	다음으로 전환...
삭제함	결과	원래 값 유지
	상태	종결됨
	해결	잘못된 결과

보안 태세 통제에서 자산 검색 생성

조건을 설정하고 특정 서비스 그래프 커넥터 제품별로 또는 커넥터에서 보고한 특정 데이터가 있는 자산을 검색합니다.

시작하기 전에

예를 들어, 메타데이터 세부 정보에 Windows 서버와 특정 버전이 CrowdStrike 있는 자산을 식별하려고 합니다.

필요한 역할: SPC 관리자 그룹 또는 SPC 분석가 그룹

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 작업 공간 〉 보안 태세 통제 〉 자산 검색.
2. 하나를 선택합니다.
   이 예에서는 자산 유형으로 하드웨어 자산을 선택합니다.
3. 옵션: 기존 정책의 조건을 시작으로 사용하고 기존 정책과 일치하는 자산을 각각 제외하려면 기본 정책 및 제외 정책을 선택합니다.
   선택한 정책이 표시됩니다.
4. 연결 필드에 대해 커넥터 데이터 사용을 선택합니다.
5. 엔터티에 대해 **CrowdStrike** 장치 정보를 선택합니다.
6. 속성, 연산자 및 값에 대해 〔에이전트 버전〕**[is]** 를 선택하고 버전(예: **6.26.14003.0**)을 입력합니다.
7. 장치 상세 정보를 다른 조건의 값으로 사용하여 엔터티 필드 CrowdStrike 오른쪽에 있는 AND 연산자를 선택합니다.
8. 연결 필드에 대해 **CMDB** 메타데이터 사용을 선택합니다.
   엔터티 필드는 CMDB 메타데이터로 채워집니다.
9. 기준 필드에 대한 속성을 선택합니다.
10. 속성, 연산자 및 값에 대해 **[OS]**〔포함〕을 선택하고 **Windows server**를 입력합니다.
11. 자산 보기를 선택합니다.
    잠시 후 일치하는 자산 탭에 결과가 표시됩니다. 일치하는 항목이 없으면 검색을 구체화할 수 있습니다. 조건을 올바르게 설정했다면 검색을 정책으로 저장하고 활성화할 수 있습니다. 다른 정책과 마찬가지로 이 기능은 활성화 후 지속적으로 백그라운드 작업으로 자산을 검색합니다.

에서 중복 구성 항목 해결 보안 태세 통제

구성 관리 데이터베이스에서 구성 항목(CI)에 대한 중복 항목을 해결하면 정책에 대한 정확한 감사를 받을 수 있습니다 SPC .

중복 구성 항목 개요

경우에 따라 자산 검색 소스, 즉 SGC(서비스 그래프 커넥터 제품)는 자산(구성 항목)에 대한 구성 관리 데이터베이스(CMDB)에 중복 항목을 생성할 수 있는 자산 데이터를 임포트합니다. 이러한 중복 CI 레코드는 두 개 이상의 자산이 동일한 이름으로 CMDB에 나열되어 있지만 CMDB 참조가 다른 경우에 발생합니다.

예를 들어 IP 주소 10.0.2.11로 이름이 지정된 자산이 CMDB 360 데이터[cmdb_multisource_data] 테이블에 두 번 나열되는 경우를 들 수 있습니다. 10.0.2.11에 대한 한 항목은 CMDB 참조 열에 10.0.2.11로 나열되고 다른 항목은 10.0.65.159로 나열됩니다. 이러한 자산은 동일한 검색 소스, SGC 제품 또는 둘 이상의 검색 소스에서 가져온 자산일 수 있습니다. 두 경우 모두 SPC 정책 및 자산 인벤토리에 문제가 발생하지 않도록 하려면 중복 CI를 제거해야 합니다.

중복 구성 항목 식별 및 제거

[sn_sec_spc_core_asset_cache] 테이블의 이름 열을 필터링하고 동일한 이름을 가진 자산을 확인하여 중복 CI를 식별할 수 있습니다.

중복을 식별하는 경우 CI 중복 제거 프로세스는 게시해야 하는 중복 제거 템플릿, 활성화할 시스템 속성, SPC 캐시된 자산 [sn_sec_spc_core_asset_cache] 테이블에서 중복 CI를 제거하는 예약된 작업을 통합합니다. 이 프로세스는 중복 항목을 제거하고 가장 관련성이 높은 항목이 있는 마스터 또는 정식 CI 기록을 보존합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

에서 중복 구성 항목 해결 보안 태세 통제

이 프로세스를 사용하여 SPC 캐시 자산 [sn_sec_spc_core_asset_cache] 테이블에서 중복 구성 항목을 제거합니다. 이 프로세스는 중복 기록을 제거하고 가장 관련성이 높은 항목이 있는 마스터 또는 정식 자산 기록을 보존합니다.

시작하기 전에

필요한 역할: CMDB 작업 공간 및 sn_sec_spc_core.admin에 액세스하여 예약된 작업을 시작하는 데 필요한 sn_cmdb_user

프로시저

1. 다음으로 이동 모두 〉 시스템 속성 〉 모든 속성.
2. sn_sec_spc core.is_ci_name_unique 시스템 속성을 찾습니다.

   CMDB 또는 자산 캐시 테이블에 나열된 모든 구성 항목의 이름이 고유한지 여부를 지정하는 속성에서 구성 가능한 값입니다.

   중복 CI를 식별하는 방법에 대한 자세한 내용은 을 참조하십시오 에서 중복 구성 항목 해결 보안 태세 통제 .
3. 기록을 선택하여 열고 값 필드를 **true**로 설정합니다.
4. 기록 업데이트합니다.
5. 다음으로 이동 **CMDB** 작업 공간 〉 관리 을 클릭하고 오른쪽의 Management tools(관리 도구) 아래에 있는 De-duplication template library(중복 제거 템플릿 라이브러리) 링크를 선택합니다.

   주:
   CMDB 작업 공간에 액세스하려면 sn_cmdb_user 역할이 필요합니다.
6. 중복 제거 템플릿 창에서 **SPC** 중복 제거 템플릿을 확장하고 이름 플립플롭 을 선택하여 엽니다.
7. 게시를 선택합니다.
8. 모달에서 게시 를 선택합니다.

   중복 제거 템플릿을 게시하고 sn_sec_spc core.is_ci_name_unique 시스템 속성을 활성화했습니다. 중복된 CI를 해결하는 작업을 생성하려면 중복 제거 작업 예약된 작업 생성을 실행해야 합니다.
9. 다음으로 이동 모두 〉 시스템 정의 〉 예약된 작업 〉 중복 제거 작업 생성 을 클릭하고 기록을 선택하여 엽니다.
10. 지금 실행을 선택합니다.
    백그라운드 작업이 큐에 대기 중이고 처리 중인지 확인합니다.
11. 다음으로 이동합니다. 백그라운드 작업 **[sn_sec_cmn_background_job]** 중복 제거 작업 생성 예약된 작업을 모니터링할 테이블입니다.
    예약된 작업이 성공적으로 완료되면(완료) 게시한 템플릿을 시작할 수 있습니다.
12. 다음으로 이동 **CMDB** 작업 공간 〉 관리 을 클릭하고 중복 제거 대시보드 보기를 선택합니다.
13. 실행 중을 선택하여 템플릿을 로드합니다.
14. 완료된 작업을 보려면 완료됨 탭을 선택합니다.

    SPC 캐시 자산 [sn_sec_spc_core_asset_cache] 테이블에 중복이 있는지 확인하기 전에 중복 제거 작업이 완료되었는지 확인해야 합니다.

    완료된 작업을 보려면 화면을 새로 고쳐야 할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

15. 예약된 작업이 성공적으로 완료되고 중복 제거 작업이 완료되었음을 확인했으면 SPC 캐시 자산 〔sn_sec_spc_core_asset_cache〕 테이블로 이동하여 이름 열을 필터링하고 중복 여부를 확인합니다.
    마스터 또는 정식 항목은 가장 관련성이 높은 CI 기록입니다. 그것은 탁자 위에 보존되어 있다. 중복이 없는 경우 CMDB 360 데이터〔cmdb_multisource_data〕 테이블에 중복이 있는지 확인합니다.
16. CMDB 360 데이터 〔cmdb_multisource_data〕 테이블로 이동합니다.
17. Col0을 기준으로 그룹화하고 SPC 캐시된 자산 〔sn_sec_spc_core_asset_cache〕 테이블의 이름 열에 해당하는 자산에 대해 다른 CMDB 참조가 있는지 확인합니다.
    중복된 항목이 발견되면 중복 제거 작업 생성 예약된 작업을 다시 실행합니다.

와 함께 완화 통제 모니터링 사용 보안 태세 통제

(SPC) 작업 공간 내에서 보안 태세 통제 다양한 보안 도구가 구성된 방식에 따라 사용 가능한 완화 제어를 통해 자산에 대한 위협이 완화되는지에 대한 인사이트를 얻을 수 있습니다.

완화 통제 모니터링

완화 통제 모니터링에 지원되는 보안 태세 통제 애플리케이션은 다음 문서를 참조하십시오 보안 태세 통제 탐색.

이 보안 태세 통제 애플리케이션은 세 가지 핵심 문제 영역에 중점을 둡니다.

- 자산 인벤토리 - 관리되지 않거나 알 수 없는 자산을 포함하는 모든 엔터프라이즈 자산을 식별합니다.
- 보안 통제 범위 및 상태 - 보안 통제로 보장 격차 식별
- 취약성 및 위협 완화 가시성 - 적용 가능한 완화 통제로 완화되는 자산에 대한 위협 또는 취약성을 식별합니다.

완화 통제 모니터링은 취약성 및 위협 완화 가시성에 속하는 기능을 보안 태세 통제 설명합니다.

필요한 역할:

- admin - 에서 ServiceNow# Store 애플리케이션을 설치하고 플러그인(ITOM 디스커버리)을 활성화합니다.
- SPC 관리자 그룹 및 SPC 분석가 그룹 - 이 그룹의 사용자는 제품 및 작업 공간의 모든 기록에 대한 전체 읽기 및 쓰기 액세스 권한을 갖습니다.
- SPC 분석가 읽기 전용 그룹 - 이 그룹의 사용자는 제품의 모든 기록에 대한 전체 읽기 권한을 갖습니다.

완화 통제, 모니터링 사용자 및 혜택

사용자

사용자	설명
사이버 보안 팀, 보안 분석가 및 관리자	• 관리되지 않거나 알 수 없는 자산을 포함한 모든 엔터프라이즈 자산에 대한 가시성을 확보합니다. • 보안 제어를 통한 적용 범위 격차, 자산에 대한 중요한 취약성 및 인터넷 노출과 같은 문제의 유해한 조합, 내부 보안 표준과의 편차를 식별합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용자

사용자	설명
취약성 관리 팀	자산의 취약성에 사용할 수 있는 완화에 대한 인사이트를 얻고 해당 취약성에 대한 위험 점수를 동적으로 조정합니다.
위협 방어 팀	특정 공격 기술에 대한 완화 또는 보안 통제 구성의 격차에 대한 인사이트를 얻습니다.

보안 태세 통제 및 완화 통제 모니터링 워크플로우

보안 태세 통제 는 웹 애플리케이션 방화벽 및 엔드포인트 보호 도구와 같은 보안 도구와 API 통합을 사용하여 자산에 대한 추가 구성 데이터를 임포트하고 분석하여 지정된 자산에 적용 가능한 완화 제어를 식별합니다. 이러한 API 통합은 에서 SPC 지원하고 서로 다른 데이터를 임포트하는 서비스 그래프 커넥터 통합과는 별개입니다. 작업 공간 내에서 SPC 이러한 API 통합을 구성합니다.

완화 통제 모니터링을 위해서는 서비스 그래프 커넥터 통합 또는 ITOM 디스커버리가 여전히 필요합니다. 예를 들어 엔드포인트 보호 구성에서 사용할 CrowdStrike 수 있는 완화 통제에 대한 추가 인사이트를 임포트하려면 서비스 그래프 커넥터와 CrowdStrike 에서 지원하는 SPC API 통합을 모두 CrowdStrike 활성화해야 합니다.

완화 통제 정책

및 보안 태세 통제 완화 통제 애플리케이션은 에서 SPC완화 통제 및 완화 통제 정책을 보는 데 필요합니다. 두 애플리케이션 모두 ServiceNow Store에서 제공됩니다.

에서 ServiceNow# Store응용 프로그램을 다운로드하고 설치하는 방법에 대한 자세한 내용은 다음 항목을 참조하십시오.

- 에서 처음으로 애플리케이션 ServiceNow Store 다운로드
- 보안 운영 통합 설치

완화 통제 정책을 보려면 SPC 관리자 그룹 및 SPC 분석가 그룹의 사용자가 다음으로 이동할 수 있습니다. 작업 공간 〉 보안 태세 통제 〉 정책 및 결과 〉 모두 SPC 작업 공간 탐색 패널에서

다음 완화 통제 정책이 애플리케이션에 포함되어 있으며 다른 SPC 정책과 함께 표시됩니다.

- SEH 덮어쓰기
- 힙 스프레이
- CrowdStrike NULL 페이지 할당
- CrowdStrike DEP 강제 적용
- CrowdStrike ASLR 강제 적용
- Microsoft Defender 제어 플로우 가드
- Microsoft Defender 힙 ASLR
- Microsoft Defender 필수 ASLR 및 상향식 ASLR
- SentinelOne 애플리케이션 제어
- SentinelOne 데이터 파일
- SentinelOne 실행 파일
- SentinelOne 익스플로잇
- SentinelOne IDR

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- SentinelOne 대화형 위협 탐지
- SentinelOne 측면 이동 감지
- SentinelOne 정적 AI
- SentinelOne 정적 AI - 의심
- SentinelOne 잠재적으로 원치 않는 애플리케이션
- SentinelOne 원격 셸
- SentinelOne 평판

완화 통제 범주

현재 다음 범주의 완화 통제가 지원됩니다 SPC.

- EDR(Exploit Protection) 완화 통제에 필요한 완화 통제 및 정책 완화 통제.
- WAF(Exploit Protection) 완화 제어. AWS WAF에 대한 정책을 생성해야 합니다. 자세한 내용은 완화 통제 모니터링을 위한 WAF 통합에 대한 AWS 정책 만들기 문서를 참조하십시오.

EDR(Exploit Protection) 완화 통제에 필요한 완화 통제 및 정책 완화 통제

이 완화 통제 범주는 엔드포인트 보호 에이전트 구성의 형태로 자산에서 사용할 수 있는 완화를 다룹니다. 이는 SentinelOne과 같은 CrowdStrike 엔드포인트 보호 에이전트에 적용됩니다.

'주소 공간 레이아웃 임의 지정 강제 적용' 및 'DEP 강제 적용'과 같은 익스플로잇 완화 설정을 .와 같은 CrowdStrike엔드포인트 보호 도구에서 활성화할 수 있습니다. SPC 는 애플리케이션에 포함된 정책 및 엔드포인트 보호 도구와의 API 통합을 통해 장치에서 이 구성을 자동으로 탐지합니다.

필요한 역할: SPC 관리자 그룹 및 SPC 분석가 그룹.

Exploit Protection(EDR) 완화 통제 탐지를 위한 **CrowdStrike** 필수 구성 요소

1. 서비스 그래프 커넥터를 활성화 CrowdStrike 했는지 확인합니다. 이 애플리케이션은 ServiceNow Store에서 다운로드할 수 있습니다. 설치 및 구성 정보는 앱 목록에 포함되어 있습니다. 자세한 내용은 완화 통제 모니터링을 위한 통합 설치 및 구성 CrowdStrike 문서를 참조하십시오.
2. 작업 공간에서 API 통합이 CrowdStrike 활성화되어 보안 태세 통제 있는지 확인합니다.

Exploit Protection(EDR) 완화 통제 탐지를 위한 **Microsoft** 필수 구성 요소

Microsoft 스크립트 작성자 역할을 포함하는 SCCM 자격 증명입니다. 스크립트 작성자 역할은 SCCM 서버에서 완화 정보를 임포트하는 데 필요한 스크립트를 만드는 데 필요한 권한을 제공합니다.

Microsoft Defender에 구성된 완화 통제를 식별하려면 SCCM 통합을 활성화해야 합니다.

자세한 내용은 Microsoft SCCM용 서비스 그래프 커넥터 및 Microsoft Defender 완화 통제 통합 설치 및 구성 문서를 참조하십시오.

- Defender – 익스플로잇 완화 – CFG

  Microsoft Defender 제어 흐름 가드.

- Defender – 익스플로잇 완화 – DEP

  Microsoft Defender 데이터 실행 방지.

- Defender – 익스플로잇 완화 – 필수 ASLR 및 상향식 ASLR

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Microsoft 수비수 힘 ASLR.

- MITRE 다룬 전술: 초기 접근, 실행, 자격 증명 접근, 방어 회피, 권한 에스컬레이션, 횡적 이동.

1. SentinelOne 서비스 그래프 커넥터를 활성화했는지 확인합니다.

   이 애플리케이션은 ServiceNow Store에서 다운로드할 수 있습니다. 설치 및 구성 정보는 앱 목록에 포함되어 있습니다. 자세한 내용은 및 SentinelOne 완화 통제 통합 설치 및 구성 SentinelOne용 서비스 그래프 커넥터 문서를 참조하십시오.

2. 보안 태세 통제 작업 공간에서 SentinelOne API 통합이 활성화되어 있는지 검증합니다.

완화 통제 모니터링을 위한 통합 설치 및 구성 **CrowdStrike**

서비스 그래프 커넥터 및 API 통합에는 CrowdStrike 별도의 구성 단계가 필요합니다. 자산 상세 정보를 임포트하도록 서비스 그래프 커넥터를 구성합니다 CrowdStrike . 에서 CrowdStrike모니터링하는 자산에 대한 완화 데이터를 수집하도록 API 통합을 구성합니다CrowdStrike.

시작하기 전에

- 인스턴스에 보안 태세 통제 및 완화 통제 모니터링 애플리케이션을 설치하고 활성화했는지 확인합니다. 이러한 애플리케이션은 ServiceNow 스토어에서 찾을 수 있습니다.
- CrowdStrike API 통합을 구성 CrowdStrike 하기 전에 서비스 그래프 커넥터를 설치하고 구성해야 합니다.

필요한 역할: 플러그인 설치를 위한 관리자, 작업 공간의 통합 구성을 위한 SPC 관리자 그룹 및 SPC 분석가 그룹.

프로시저

1. 서비스 그래프 커넥터 통합을 설치하고 구성하려면 CrowdStrike 다음 단계를 따르십시오.

   > **주:**
   > 용 CrowdStrike서비스 그래프 커넥터를 설치한 경우 API 통합을 구성하는 CrowdStrike 방법에 대한 2단계로 진행합니다.

   a. 다음으로 이동 커넥터 및 사용 케이스 설정 〉 서비스 그래프 커넥터 탭.

   b. Endpoint Protection 서비스 그래프 커넥터를 찾습니다 CrowdStrike .

   c. 에서 ServiceNow# Store서비스 그래프 커넥터에 CrowdStrike 대한 앱 목록으로 연결되는 링크를 선택합니다.

   d. 프롬프트에 따라 애플리케이션을 설치합니다.

   e. 구성 및 활성화에 도움이 되도록 종료하기 전에 앱 목록의 지원 링크 및 문서 섹션에서 설치 가이드를 다운로드하십시오.

   f. 다음으로 이동 **CrowdStrike** 〉 설정 인스턴스에 있습니다.

   g. 안내 설정의 프롬프트에 따라 설명서를 참조하여 SGC를 구성하고 활성화합니다.

2. 다음으로 이동 커넥터 및 사용 케이스 설정 〉 **SPC API** 통합.

   이 탭에는 완화 통제 소스(CrowdStrike, F5 Big IP 및 SCCM)가 나열되며, 완화 통제 모니터링 애플리케이션을 설치한 경우에만 작업 공간에 탭이 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

소스 카드에서 완화 소스의 상태(## 또는 ###)와 (6)으로 모니터링 CrowdStrike 되는 완화 통제 및 관련 정책을 볼 수 있습니다. 번호를 선택하면 목록을 볼 수 있습니다.

Sources(소스)의 Active(활성) 열에 Active(##)가 표시됩니다. 이는 소스(CrowdStrike SGC)가 활성 상태임을 나타내지만 완화 제어를 모니터링하려면 먼저 API 통합을 구성해야 CrowdStrike 합니다.

3. 다음을 선택합니다.
4. 이름 열에서 선택합니다 CrowdStrike .
5. 편집을 선택하고 필드를 입력합니다.

> **주:**
> 서비스 그래프 커넥터에 대해 CrowdStrike 제공한 API 통합에 대해 동일한 CrowdStrike 계정 정보 및 서버 상세 정보를 입력합니다. 이 정보를 통해 서비스 그래프 커넥터로 임포트한 자산 데이터와 일치하는 완화 데이터를 임포트할 수 있습니다.

필드	설명
이름	인스턴스 이름입니다. 이 이름을 변경하면 자격 증명을 테스트하지 않고 저장할 수 있습니다. 이름 필드에서 필드를 변경하는 경우 저장하고 종료하기 전에 연결을 테스트해야 합니다.
자산 크기 제한	모니터링되는 자산 수입니다.
클라이언트 ID	CrowdStrike ID
클라이언트 비밀	CrowdStrike 비밀
API URL	API URL(예: https://api.crowdstrike.com

6. 준비가 되면 연결 테스트를 선택합니다.
   연결에 성공하면 메시지가 표시됩니다.
7. 저장하고 종료를 선택합니다.
8. SPC API 통합 탭에서 카드의 세부 정보CrowdStrike 보기를 선택하고 소스와 API가 활성화되고 구성 진행률 표시줄이 완성되는지 확인합니다.
9. 옵션: 자격 증명 테스트에 실패하면 이전 자격 증명으로 되돌리 기를 선택하여 이전에 확인한 자격 증명을 삽입할 수 있습니다.
10. 다음 단계에 따라 CrowdStrike 통합을 실행합니다.

    a. 다음으로 이동 **CrowdStrike** 완화 통제 〉 통합.
    세 가지 통합이 있습니다.
    - CrowdStrike 예방 정책 통합
    - CrowdStrike 장치 제어 정책 통합
    - CrowdStrike 자산 인사이트 통합

    통합은 체인으로 연결되고 특정 순서로 실행됩니다. 한 통합이 성공적으로 완료되면 다음 통합이 시작됩니다.

    b. CrowdStrike 통합 실행을 시작하려면 이름 열에서 예방 정책 통합을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

c. 기록에서 활성 확인란을 선택하고 지금 실행을 선택합니다.

통합 기록의 통합 실행 탭에서 통합 실행 상태를 볼 수 있습니다.

통합은 기본적으로 매일 실행되도록 예약되어 있습니다.

자산 인사이트 통합은 CrowdStrike 마지막 통합 실행 이후 변경된 자산에 대한 정보만 임포트합니다. 장치 제어 정책 통합 및 예방 정책 통합은 CrowdStrikeCrowdStrike 각 실행에 대한 모든 데이터를 임포트합니다.

Microsoft SCCM용 서비스 그래프 커넥터 및 **Microsoft Defender** 완화 통제 통합 설치 및 구성

SCCM용 서비스 그래프 커넥터 및 Microsoft Defender 완화 통제 통합에는 별도의 구성 단계가 필요합니다.

시작하기 전에

자산 상세 정보를 임포트하려면 Service Graph Connector for SCCM을 설치, 활성화 및 구성해야 합니다. SCCM도 사용하는 Microsoft Defender 완화 통제 통합을 구성하여 SCCM용 서비스 그래프 커넥터에서 모니터링하는 자산에 구성된 완화 통제에 대한 추가 데이터를 수집합니다.

필요한 역할:

- 플러그인 설치 및 활성화를 위한 관리자
- 작업 공간의 통합 구성을 위한 SPC 관리자 그룹 및 SPC 분석가 그룹
- 스크립트 작성자 역할을 포함하는 Microsoft SCCM 자격 증명입니다. 스크립트 작성자 역할은 SCCM 서버에서 완화 정보를 임포트하는 데 필요한 스크립트를 만드는 데 필요한 권한을 제공합니다.

  주:
  이 역할을 생성하고 다음 권한을 할당해야 합니다.

  스크립트 작성자 역할

범주	권한	상태
컬렉션	스크립트 실행	아니요
사이트	읽기	예
SMS 스크립트	작성	예
SMS 스크립트	읽기	예
SMS 스크립트	삭제	예
SMS 스크립트	수정	예

- 스크립트 승인자 역할을 포함하는 Microsoft SCCM 자격 증명. 완화 정보를 임포트하기 위해 생성된 스크립트에는 스크립트 승인자 역할을 가진 사용자의 Microsoft SCCM 콘솔 승인이 필요합니다.

  주:
  이 역할을 생성하고 다음 권한을 할당해야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

스크립트 승인자

범주	권한	상태
컬렉션	스크립트 실행	아니요
사이트	읽기	예
SMS 스크립트	읽기	예
SMS 스크립트	승인	예
SMS 스크립트	수정	예

프로시저

1. Microsoft SCCM용 서비스 그래프 커넥터 통합을 설치하고 구성하려면 다음 단계를 따르십시오.

> **주:**
> Microsoft SCCM용 서비스 그래프 커넥터 통합을 설치한 경우 2단계로 이동하여 Microsoft Defender 완화 통제 통합을 구성합니다.

a. 다음으로 이동 커넥터 및 사용 케이스 설정 〉 서비스 그래프 커넥터 탭.

b. Microsoft SCCM용 서비스 그래프 커넥터 통합을 찾습니다.

c. 에서 ServiceNow# Store애플리케이션의 앱 목록으로 연결되는 링크를 선택합니다.

d. 프롬프트에 따라 애플리케이션을 설치합니다.

e. 구성 및 활성화에 도움이 되도록 종료하기 전에 앱 목록의 지원 링크 및 문서 섹션에서 설치 가이드를 다운로드하십시오.

f. 다음으로 이동 설정 인스턴스에 있습니다.

g. 안내 설정의 프롬프트에 따라 설명서를 참조하여 SGC를 구성하고 활성화합니다.

2. 다음으로 이동 커넥터 및 사용 케이스 설정 〉 **SPC API** 통합 Microsoft Defender 완화 통제 통합을 구성하기 위해.

이 탭에는 완화 통제 소스(CrowdStrike, F5 Big IP 및 Defender)가 나열되며, 완화 통제 모니터링 애플리케이션을 설치한 경우에만 작업 공간에 탭이 표시됩니다.

소스 카드에서 완화 소스의 상태(## 또는 ###)를 볼 수 있습니다.

Sources(소스)의 Active(활성) 열에 Active(##)가 표시됩니다. 이는 자산 데이터를 검색하기 위해 소스(Microsoft SCCM용 서비스 그래프 커넥터)가 활성 상태임을 나타내지만, 완화 통제를 모니터링하려면 먼저 SCCM을 사용하여 이러한 자산의 Defender 구성에 대한 추가 데이터를 가져오는 Microsoft Defender 완화 통제 통합을 구성해야 합니다.

3. 다음을 선택합니다.
SCCM 구성 페이지에는 Microsoft SCCM 완화 통제 인스턴스 링크 하나가 표시됩니다.

4. 이름 열에 제공된 인스턴스 링크를 선택합니다.

5. SCCM 자격 증명 구성 Microsoft SCCM 완화 통제 통합 모달의 필드를 작성합니다.

필드	설명
이름	필드는 인스턴스 이름으로 자동으로 채워집니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
연결	연결 정보로 자동으로 채워지는 필드입니다.
호스트	이전 필드에 제공된 연결 정보 내에 있는 SCCM 서버의 호스트 이름입니다.
사용자 이름	SCCM 서버에 액세스하기 위한 사용자 이름입니다.
암호	SCCM 서버에 액세스하기 위한 암호입니다.
MID 서버	목록에서 ServiceNow 관리 MID 서버를 선택합니다.
확인 상태	유효성 확인 시도 후 필드가 채워졌습니다. 연결에 성공하면 통합 인스턴스 상태가 유효합니다.
SG 커넥터 연결	Microsoft SCCM용 서비스 그래프 커넥터에 대한 목록에서 연결 및 자격 증명 별칭 옵션 하나를 선택합니다. Microsoft SCCM SGC에 대한 안내 설정 단계에서 이 연결을 설정합니다.
유효성 확인 상세 정보	확인 시도에 대한 자세한 정보입니다.

6. 자격 증명 저장 및 테스트를 선택합니다.
   다음 단계로 진행하려면 성공적인 연결을 위한 ### 응답이 필요합니다.
7. 다음을 선택합니다.
   완화 상세 정보를 검색하기 위해 PowerShell 스크립트가 자동으로 생성됩니다. 스크립트 승인을 확인하는 옵션과 함께 모달이 표시됩니다.
8. 스크립트를 승인하려면 스크립트 승인자 역할로 Microsoft SCCM 콘솔에 로그인하십시오.

   완화 상세 정보를 검색하기 위해 SCCM 구성 관리자에 PowerShell 스크립트가 생성되었습니다. 스크립트를 승인하려면 스크립트 승인자 권한이 있는 사용자 역할의 적절한 자격 증명으로 로그인해야 합니다. 승인되면 인스턴스에서 유효성을 검사할 수 있습니다 ServiceNow AI Platform .
9. 콘솔에서 **[ServiceNow SecOps]:** 시스템 완화 가져오기 스크립트를 찾아 승인합니다.

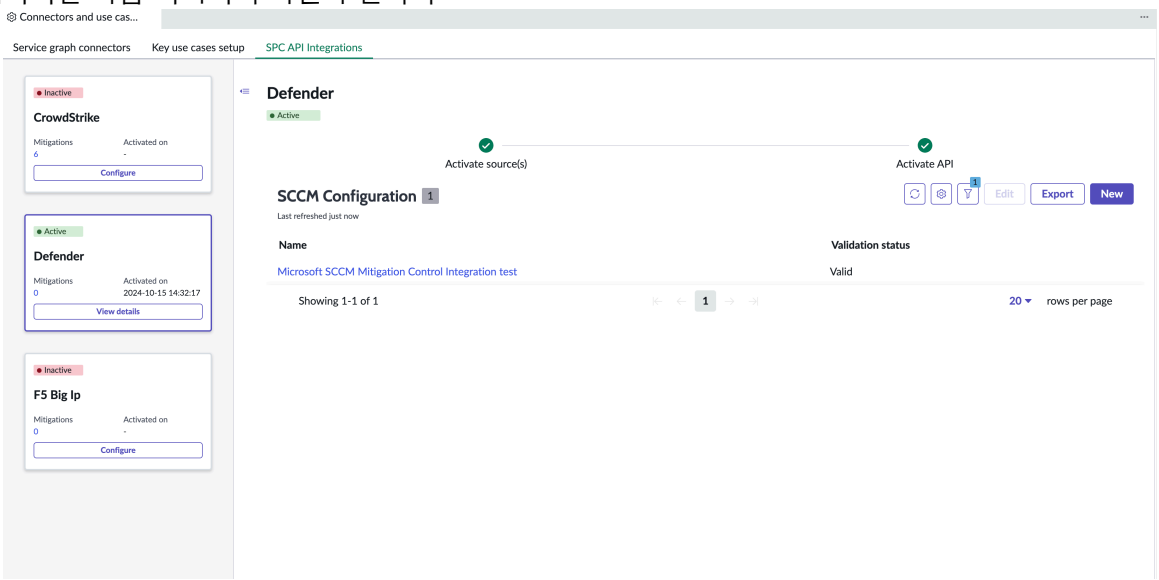
   주:
   SCCM 구성 관리자에서 스크립트 섹션은 소프트웨어 라이브러리 아래에 있습니다. 찾기: 〔ServiceNow SecOps〕: 시스템 완화 가져오기 스크립트를 승인합니다.

   이 스크립트는 사용자가 승인할 때까지 승인 대기 중 상태로 유지됩니다.

   위에서 설명한 대로 승인하지 않고도 인스턴스에서 스크립트를 ServiceNow AI Platform 확인할 수 있지만 오류 메시지인 ##### #### #####.가 표시됩니다.
10. 승인을 확인하려면 인스턴스로 ServiceNow AI Platform 돌아가서 PowerShell 스크립트 승인 승인 모달에서 스크립트 승인 확인을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

11. 완료를 선택합니다.
구성 페이지는 다음 이미지의 화면과 같아야 합니다.



Microsoft Defender 완화 통제 통합에 대한 여러 인스턴스 생성

Microsoft Defender 완화 통제 통합에 대해 여러 인스턴스를 구성할 수 있습니다.

시작하기 전에

필요한 역할:

- 작업 공간의 새 통합 인스턴스 구성을 위한 SPC 관리자 그룹 및 SPC 분석가 그룹
- 스크립트 작성자 역할을 포함하는 Microsoft SCCM 자격 증명입니다. 스크립트 작성자 역할은 SCCM 서버에서 완화 정보를 임포트하는 데 필요한 스크립트를 만드는 데 필요한 권한을 제공합니다.

  주:
  이 역할을 생성하고 다음 권한을 할당해야 합니다.

  스크립트 작성자 역할

범주	권한	상태
컬렉션	스크립트 실행	아니요
사이트	읽기	예
SMS 스크립트	작성	예
SMS 스크립트	읽기	예
SMS 스크립트	삭제	예
SMS 스크립트	수정	예

- 스크립트 승인자 역할을 포함하는 Microsoft SCCM 자격 증명. 완화 정보를 임포트하기 위해 생성된 스크립트에는 스크립트 승인자 역할을 가진 사용자의 Microsoft SCCM 콘솔 승인이 필요합니다.

  주:
  이 역할을 생성하고 다음 권한을 할당해야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

스크립트 승인자

범주	권한	상태
컬렉션	스크립트 실행	아니요
사이트	읽기	예
SMS 스크립트	읽기	예
SMS 스크립트	승인	예
SMS 스크립트	수정	예

프로시저

1. 다음으로 이동 커넥터 및 사용 케이스 설정 〉 **SPC API** 통합.
2. 새로 만들기를 선택합니다.
   새 Defender 인스턴스 모달이 표시됩니다.
3. 새 인스턴스의 이름을 입력하고 인스턴스 생성을 선택합니다.
   SPC API 통합 페이지가 애플리케이션과 함께 제공된 인스턴스와 새 인스턴스와 함께 표시됩니다.
4. 새 인스턴스에 대한 링크를 선택합니다.
5. 새 인스턴스에 대한 SCCM 자격 증명 구성 모달의 필드를 입력합니다.

필드	설명
이름	필드는 인스턴스 이름으로 자동으로 채워집니다.
연결	새 연결을 생성합니다. **a.** 모달 맨 위에 있는 연결 및 별칭 생성을 선택합니다. **b.** 연결 및 자격 증명 별칭 양식에서 필수 필드를 입력합니다. ▪ 이름 - 고유 이름입니다 ▪ 유형 - 연결 및 자격 증명 ▪ 연결 유형 - 기본 주: 지금은 제출 을 선택하지 마십시오. **c.** 회색 헤더의 아무 곳이나 마우스 오른쪽 버튼으로 클릭하고 저장을 선택합니다. 저장한 후 페이지가 새로 고쳐지고 관련 링크와 탭이 페이지 하단에 표시됩니다. **d.** 연결 탭을 선택한 상태에서 탭 오른쪽에서 새로 만들기를 선택합니다. 연결 양식이 표시됩니다. 필드를 작성합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명

	▪ 이름 - 고유 이름입니다
	▪ 자격 증명 - 검색 아이콘을 선택합니다. Windows 자격 증명을 찾아 링크를 선택합니다. Windows 자격 증명 양식의 필드에 내용을 입력합니다.
	  ▪ 이름 - 고유 이름입니다
	  ▪ 사용자 이름 - 자격 증명의 사용자 이름입니다. 이 페이지에 저장한 후 SCCM 자격 증명 구성 모달의 사용자 이름 필드에 참조할 사용자 이름입니다.
	  ▪ 암호 - 자격 증명의 암호입니다. 이 페이지에 저장한 후 SCCM 자격 증명 구성 모달의 암호 필드에 참조할 암호입니다.
	▪ 호스트 - 이 페이지에 저장한 후 SCCM 자격 증명 구성 모달의 호스트 필드에서 참조할 SCCM 서버의 호스트입니다.
	e. **MID** 서버 사용 확인란을 선택합니다. **MID** 선택을 위해 특정 MID 서버를 선택하고 MID 서버 목록에서 하나를 선택합니다.
	f. 회색 헤더의 아무 곳이나 마우스 오른쪽 버튼으로 클릭하고 저장을 선택합니다. 위의 d단계에서 설명한 연결 양식에 입력하는 자격 증명입니다.

호스트	이것은 위에서 설명한 대로 연결 페이지에 저장한 후 호스트 필드에서 참조하는 SCCM 서버의 호스트입니다.
사용자 이름	위에서 설명한 대로 연결 페이지에 저장한 후 사용자 이름 필드에서 참조하는 사용자 이름입니다.
암호	이는 위에서 설명한 대로 연결 페이지에 저장한 후 암호 필드에서 참조하는 암호입니다.
MID 서버	이는 위에서 설명한 대로 연결 페이지에 저장한 후 MID 서버 필드에서 참조되는 MID 서버입니다.
확인 상태	유효성 확인 시도 후 필드가 채워졌습니다. 연결에 성공하면 통합 인스턴스 상태가 유효합니다.
SG 커넥터 연결	Microsoft SCCM용 서비스 그래프 커넥터에 대한 목록에서 연결 및 자격 증명 별칭 옵션 하나를 선택합니다. Microsoft SCCM SGC에 대한 안내 설정 단계에서 이 연결을 설정합니다.
유효성 확인 상세 정보	확인 시도에 대한 자세한 정보입니다.

6. 다음으로 이동 커넥터 및 사용 케이스 설정 〉 **SPC API** 통합.

7. 새 인스턴스에 대한 링크를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

8. SCCM 자격 증명 구성 모달의 연결 필드에 대해 5단계에서 생성한 목록에서 연결을 선택합니다.

   아래 나열된 필드는 새 연결에 대해 입력한 정보에 따라 자동으로 채워집니다.

호스트	이것은 위에서 설명한 대로 연결 페이지에 저장한 후 호스트 필드에서 참조하는 SCCM 서버의 호스트입니다.
사용자 이름	위에서 설명한 대로 연결 페이지에 저장한 후 사용자 이름 필드에서 참조하는 사용자 이름입니다.
암호	이는 위에서 설명한 대로 연결 페이지에 저장한 후 암호 필드에서 참조하는 암호입니다.
MID 서버	이는 위에서 설명한 대로 연결 페이지에 저장한 후 MID 서버 필드에서 참조되는 MID 서버입니다.
확인 상태	유효성 확인 시도 후 필드가 채워졌습니다. 연결에 성공하면 통합 인스턴스 상태가 유효합니다.
SG 커넥터 연결	목록에서 연결 및 자격 증명 별칭 옵션을 하나 선택합니다.
유효성 확인 상세 정보	확인 시도에 대한 자세한 정보입니다.

9. 자격 증명 저장 및 테스트를 선택합니다.
   다음 단계로 진행하려면 성공적인 연결을 위한 ### 응답이 필요합니다.
10. 다음을 선택합니다.
    PowerShell 스크립트는 설명된 Microsoft SCCM용 서비스 그래프 커넥터 및 Microsoft Defender 완화 통제 통합 설치 및 구성대로 만들어집니다. 해당 항목의 단계에 따라 새 인스턴스에 대한 스크립트를 승인합니다.

및 **SentinelOne** 완화 통제 통합 설치 및 구성 SentinelOne용 서비스 그래프 커넥터

및 SentinelOne용 서비스 그래프 커넥터 완화 통제 통합을 위한 SentinelOne 통합에는 별도의 구성 단계가 필요합니다. 자산 상세 정보를 임포트하도록 설치하고 SentinelOne용 서비스 그래프 커넥터 구성합니다. 완화 통제 통합을 위한 SentinelOne 통합을 구성하여 에서 SentinelOne용 서비스 그래프 커넥터모니터링하는 자산에 대한 완화 데이터를 수집합니다.

시작하기 전에
필요한 역할:

- 플러그인 설치 및 활성화를 위한 관리자입니다.
- 작업 공간의 통합을 구성하기 위한 SPC 관리자 그룹 및 SPC 분석가 그룹입니다.
- SentinelOne 자격 증명.

프로시저

1. 통합을 설치하고 구성하려면 SentinelOne용 서비스 그래프 커넥터 다음 단계를 수행합니다.

   주:
   SentinelOne용 서비스 그래프 커넥터를 설치한 경우 2단계로 이동하여 완화 통제 통합을 위한 SentinelOne 통합을 구성합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 다음으로 이동 커넥터 및 사용 케이스 설정 〉 서비스 그래프 커넥터 탭.

b. 통합을 찾습니다 SentinelOne용 서비스 그래프 커넥터 .

c. 에서 ServiceNow# Store애플리케이션의 앱 목록으로 연결되는 링크를 선택합니다.

d. 프롬프트에 따라 애플리케이션을 설치합니다.

e. 구성 및 활성화에 도움이 되도록 종료하기 전에 앱 목록의 지원 링크 및 문서 섹션에서 설치 가이드를 다운로드하십시오.

f. 다음으로 이동 설정 인스턴스에 있습니다.

g. 안내 설정의 프롬프트에 따라 설명서를 참조하여 SGC를 구성하고 활성화합니다.

2. 다음으로 이동 커넥터 및 사용 케이스 설정 〉 **SPC API** 통합 완화 통제 통합을 위한 SentinelOne 통합을 구성하기 위해.

   이 탭에는 완화 통제 소스 CrowdStrike(, F5 Big Ip, Defender, SentinelOne)가 나열됩니다. 이 탭은 완화 통제 모니터링 애플리케이션을 설치한 경우에만 작업 공간에 표시됩니다.

   소스 카드에서 완화 소스의 상태(## 또는 ###)를 볼 수 있습니다.

   Sources(소스)의 Active(활성) 열에 Active(##)가 표시됩니다. 이는 소스(이 경우 SentinelOne용 서비스 그래프 커넥터)가 자산 데이터를 검색하기 위해 활성 상태임을 나타내지만, 임포트한 자산에 대한 완화 제어를 모니터링하려면 먼저 완화 통제 통합을 위한 SentinelOne 통합을 구성해야 합니다.

3. 다음을 선택합니다.
   SentinelOne 구성 페이지에는 완화 통제를 위한 SentinelOne 통합 인스턴스 링크 하나가 표시됩니다.

4. 이름 열에 제공된 인스턴스 링크를 선택합니다.

5. 완화 통제 통합을 위한 SentinelOne 통합의 필드를 작성합니다.

   주:

   에 대해 SentinelOne용 서비스 그래프 커넥터제공한 완화 통제 통합을 위한 SentinelOne 통합에 대해 동일한 SentinelOne 계정 정보 및 서버 상세 정보를 입력합니다. 이 정보를 통해 서비스 그래프 커넥터로 임포트한 자산 데이터와 일치하는 완화 데이터를 임포트할 수 있습니다.

   필드를 편집해야 하는 경우 펜 아이콘을 선택합니다.

필드	설명
인스턴스 이름	필드는 인스턴스 이름으로 자동으로 채워집니다.
API 키	API 키 정보로 자동으로 채워지는 필드입니다.
API URL	SentinelOne 서버의 호스트 이름(예: https//usea1-na.sentinelone.net)

6. 자격 증명 저장 및 테스트를 선택합니다.
   다음 단계로 진행하려면 성공적인 연결을 위한 ### 응답이 필요합니다.

7. 저장하고 종료를 선택합니다.

8. SPC API 통합 탭의 SentinelOne 카드에서 세부 정보 보기를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

소스 및 API가 활성화되고 구성 진행률 표시줄이 완료됩니다.

9. 옵션: 이전 자격 증명으로 되돌리기를 선택하여 이전에 유효성을 검사한 자격 증명을 삽입합니다.
10. 다음 단계에 따라 SentinelOne 자산 임포트 통합을 실행합니다.

    a. 다음으로 이동 **SentinelOne** 완화 통제 〉 통합.
    SGC SentinelOne 자산 임포트라는 통합이 하나 있습니다.

    b. 이름 열에서 **SentinelOne** 예방 정책 통합을 선택하여 통합을 시작합니다.

    c. 기록에서 활성 확인란을 선택하고 지금 실행을 선택합니다.

    통합 기록의 통합 실행 탭에서 통합 실행 상태를 볼 수 있습니다.

    통합은 기본적으로 매일 실행되도록 예약되어 있습니다.

    SentinelOne 자산 임포트 통합은 마지막 통합 실행 이후 변경된 자산에 대한 정보만 임포트합니다.

WAF(Exploit Protection) 완화 제어

이 완화 제어 범주는 Web Application Firewall 형태로 사용할 수 있는 완화를 포함합니다.

익스플로잇 보호**(WAF)**

보안 태세 통제 은 필요한 경우 ITOM IP 기반 검색의 (F5) 및 네트워크 트래픽 데이터와 같은 WAF 도구 F5 BIG-IP 와의 API 통합을 사용하여 WAF(웹 애플리케이션 방화벽) 뒤에서 실행되는 서버를 탐지합니다.

완화 제어는 웹 ACL 규칙과 관련된 모든 부하 분산 장치를 임포트하여 검색 및 서비스 매핑 패턴의 도움을 받아 가상 머신을 보호하는 규칙을 결정합니다.

필요한 역할: SPC 관리자 그룹 및 SPC 분석가 그룹.

를 사용한 **Exploit** Protection(WAF)의 필수 구성요소 **F5 BIG-IP**

1. F5 WAF 및 관련 애플리케이션 서버가 설정된 환경에서 F5 BIG-IP ITOM IP 기반 검색을 활성화했는지 확인합니다.
2. F5에 대한 F5 BIG-IP API 통합이 작업 공간에서 보안 태세 통제 활성화되어 있는지 확인합니다.

를 사용한 **Exploit** Protection(WAF)의 필수 구성요소 **Amazon Web Services AWS**

이 통합에 대한 데이터는 검색 및 서비스 매핑 패턴[sn_itom_pattern]과 완화 통제 모니터링 [sn_sec_mit_ctrl] 애플리케이션에서 임포트됩니다. 두 애플리케이션 모두 필요합니다. 가상 머신이 보호되고 있는지 확인하는 데 필요한 모든 웹 ACL, 웹 ACL 규칙 및 완화 데이터를 임포트할 수 있도록 아래 단계를 나열된 순서대로 따르십시오. 검색 패턴에 대한 AWS 자세한 내용은 을 참조하십시오AWS discovery using patterns .

1. 사용하려는 서비스 계정에서 웹 ACL 및 규칙을 AWS 정의합니다. 자세한 내용은 AWS WAF에서 웹 ACL 사용 섹션을 참조하세요.

> **주:**
> 자체 웹 ACL 규칙을 생성할 수 있지만 웹 ACL과 함께 작동하도록 특별히 설계된 관리형 규칙을 사용하는 AWS 것이 더 나을 수 있습니다. 웹 ACL에 대한 자체 사용자 지정 규칙을 생성하기로 선택한 경우 WAF와의 AWS 통합은 Contains SQL 삽입 공격 및 Contains XSS(교차 사이트 스크립팅) 삽입 공격과 일치하는 공격 유형만 지원합니다. 부하 분산 장치는 이 통합에서 지원하는 자산(자원)입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

2. 1단계에서 정의한 웹 ACL의 이름과 기본 작업을 검색할 수 있도록 인스턴스에 검색 및 서비스 매핑 패턴[sn_itom_pattern] 애플리케이션을 설치하고 활성화합니다. 자세한 내용은 보안 태세 통제에 지원되는 애플리케이션 설치 문서를 참조하십시오.
3. sn_itom_pattern.discover_aws_app_pool_members MID 서버 시스템 속성이 true로 설정되어 있는지 확인합니다. 이 속성을 활성화하려면 다음으로 이동합니다. 모두 〉 **MID** 서버 〉 속성.
4. 완화 통제 모니터링 [sn_sec_mit_ctrl] 애플리케이션을 설치하고 활성화했는지 확인하십시오. 이 애플리케이션에는 패턴 확장, 웹 ACL 규칙 및 관련 자원이 포함되어 있습니다. 이 패턴 확장을 사용하면 실제 웹 ACL 규칙 및 자원(자산)에 대한 연결(관계)을 인스턴스로 임포트할 수 있습니다.

F5 BIG-IP 완화 통제 모니터링을 위한 통합 구성

ITOM IP 기반 검색 애플리케이션과 API 통합에는 F5 BIG-IP 별도의 구성 단계가 필요합니다. 자산 상세 정보를 임포트하도록 ITOM IP 기반 검색 애플리케이션을 구성합니다. ITOM IP 기반 검색으로 모니터링되는 자산에 대한 완화 데이터를 수집하도록 API 통합을 구성합니다 F5 BIG-IP .

시작하기 전에

- ITOM IP 기반 검색은 연관된 애플리케이션 서버가 설치된 환경에서 F5 BIG-IP 실행되고 있어야 합니다.
- 온 프레미스 자산의 경우 MID 서버를 제공해야 합니다.
- 소스(ITOM)를 활성화하여 모니터링 중인 자산에 대한 데이터를 수집합니다.
- API 통합을 활성화하여 자산에 대한 완화 데이터를 수집합니다.

필요한 역할: 플러그인 설치 및 시스템 속성 생성을 위한 관리자, SPC 작업 공간의 통합 구성을 위한 관리자 그룹 및 SPC 분석가 그룹.

프로시저

1. 통합을 설치하고 구성하려면 다음 단계를 수행합니다.

   주:
   ITOM을 설치하고 활성화한 경우 (F5) API 통합을 구성하는 F5 BIG-IP 방법에 대한 2단계로 진행합니다.

   a. 다음으로 이동 커넥터 및 사용 케이스 설정 〉 서비스 그래프 커넥터 탭.
   b. F5 BIG-IP 카드를 선택합니다.
   c. **ITOM** 플러그인을 활성화하려면 **ITOM** 플러그인 링크를 선택합니다.
   d. 프롬프트를 따릅니다.
2. 다음으로 이동 커넥터 및 사용 케이스 설정 〉 **SPC API** 통합.

   이 탭에는 완화 통제 소스(CrowdStrike 및 F5 Big IP 및 SCCM)가 나열되며, 완화 통제 모니터링 애플리케이션을 설치한 경우에만 작업 공간에 탭이 표시됩니다.

   소스 카드에서 완화 소스의 상태(## 또는 ###)를 볼 수 있습니다.
3. 다음을 선택합니다.

   소스(ITOM)가 활성 상태이지만 완화 제어를 모니터링하려면 먼저 API 통합을 구성하고 활성화해야 F5 BIG-IP 합니다.
4. 이름 열에서 선택합니다 F5 BIG-IP .

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. 편집을 선택하고 필드를 입력합니다.

필드	설명
이름	인스턴스 이름입니다. 이 이름을 변경하면 자격 증명을 테스트하지 않고 저장할 수 있습니다. 이름 필드에서 필드를 변경하는 경우 저장하고 종료하기 전에 연결을 테스트해야 합니다.
사용자 이름	F5 BIG-IP 사용자 이름
암호	F5 BIG-IP 암호.
MID 서버	목록에서 MID 서버를 선택합니다.
API URL	포트 8443이 있는 API URL입니다(예: https://bigip.example.com:8443).

6. 준비가 되면 연결 테스트를 선택합니다.
연결에 성공하면 메시지가 표시됩니다.

   구성 단계 중에 연결을 테스트한 결과 ### #### ## - ### # ##: ### #### ## - ### # ## 오류가 발생하는 경우 다음 시스템 속성을 false로 설정합니다.

   - com.glide.communications.httpclient.verify_hostname
   - com.glide.communications.httpclient.verify_revoked_certificate

   관리자 역할이 있는 사용자는 시스템 속성 [sys_properties] 테이블에 나열되지 않은 경우 전역 범위에서 이러한 시스템 속성을 생성해야 합니다. 시스템 속성은 유형, 참/거짓(부울)입니다.

7. 저장하고 종료를 선택합니다.
8. F5 BIG-IP SPC API 통합 탭의 카드에서 소스 및 API가 활성화되고 구성 진행률 표시줄이 완성됩니다.
9. 옵션: 자격 증명 테스트에 실패하면 이전 자격 증명으로 되돌리 기를 선택하여 이전에 확인한 자격 증명을 삽입할 수 있습니다.
10. API 통합을 실행하려면 다음 단계를 따르십시오.

    a. 다음으로 이동 **F5 Big IP** 완화 통제 〉 통합

       5가지 통합이 있습니다. 통합은 체인으로 연결되고 특정 순서로 실행됩니다. 한 통합이 성공적으로 완료되면 다음 통합이 시작됩니다.

       - F5 Big IP 장치 통합
       - F5 Big IP 정책 통합
       - F5 Big IP 공격 서명 통합
       - F5 Big IP 가상 서버 통합
       - F5 Big IP 풀 구성원 통합

    b. 통합 체인을 시작하려면 이름 열에서 **F5 Big IP** 장치 통합을 선택합니다.

    c. 기록에서 활성 확인란을 선택하고 지금 실행을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

d. 통합 기록의 통합 실행 탭에서 통합 실행의 상태를 봅니다.
통합은 기본적으로 매일 실행되도록 예약되어 있습니다.

AWS 완화 통제 모니터링을 위한 **WAF** 통합 구성

가상 머신이 완화 제어 모니터링을 위한 WAF 통합으로 AWS 보호되는지 확인합니다.

시작하기 전에

데이터는 두 개의 개별 애플리케이션에서 임포트됩니다.

- 검색 및 서비스 매핑 패턴 애플리케이션은 서비스 계정에서 정의 AWS 한 웹 ACL의 이름과 기본 작업(허용 또는 차단)을 임포트합니다. 검색 패턴 Amazon AWS - # ACL(LP) 이 애플리케이션과 함께 활성화됩니다.
- 완화 통제 모니터링 애플리케이션은 실제 웹 ACL 규칙 및 애플리케이션 부하 분산 장치와 같은 관련 자원 간의 관계를 임포트합니다. 이 확장은 완화 통제 모니터링 애플리케이션의 일부로 포함되어 있습니다.

웹 ACL 및 규칙을 정의하는 단계를 완료하고 애플리케이션을 활성화하기 전에 설명한 WAF(Exploit Protection) 완화 제어 WAF 통합에 AWS 필요한 애플리케이션을 활성화했는지 확인합니다.

필요한 역할:

- 관리자 인스턴스에 플러그인을 설치할 수 있습니다 ServiceNow AI Platform# .
- SPC 작업 공간의 통합을 구성하기 위한 관리자 그룹입니다.
- AWS 사용할 서비스 계정의 자격 증명입니다 AWS .

프로시저

1. 다음으로 이동 모두 〉 보안 태세 통제 작업 공간 〉 커넥터 및 사용 케이스 설정 〉 **SPC API** 통합 탭.
2. **AWS WAF** 타일을 선택합니다.
3. 하나를 선택합니다.

옵션	설명
서비스 계정 보기	인스턴스에 구성된 사용 가능한 AWS 서비스 계정을 봅니다. 새 계정을 만들려면: **a.** 서비스 계정 보기를 선택합니다. **b.** 새로 만들기를 선택합니다. **c.** 필드에 내용을 입력합니다. ▪ 이름 - 서비스 AWS 계정의 이름입니다. Discovery 일정 및 자격 증명에 사용하는 계정입니다. ▪ 계정 ID - 서비스 계정의 계정 ID입니다 AWS . ▪ 데이터센터 유형 - **AWS** 데이터센터 선택 **[cmdb_ci_aws_datacenter]** **d.** 제출을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵션	설명
서비스 계정 구성	AWS 인스턴스에서 서비스 계정을 구성합니다.

4. 사용할 서비스 계정에 대한 AWS 검색 일정을 생성합니다.

   a. 다음으로 이동 모두 〉 디스커버리 〉 홈.

   b. 활성 일정 보기를 선택합니다.

   c. 일정 추가를 선택합니다.

   d. 클라우드 일정 추가를 선택하고 필드를 채웁니다.

필드	설명
제공자	AWS
일정 이름	다른 AWS 일정과 구분하기 쉽도록 일정의 고유한 이름을 입력합니다.
계정 추가	서비스 계정을 작성하려면 선택합니다.
계정 선택	기존 서비스 계정을 편집하려면 선택합니다.
계정 ID	서비스 계정의 계정 ID입니다 AWS .
MID 선택 유형	MID 서버를 제공해야 합니다. 다음 중 하나를 선택하십시오. ▪ MID 서버 자동 선택 ▪ 특정 MID 클러스터 ▪ 특정 MID 서버 MID 서버를 사용하여 개별 가상 머신에 대한 규칙 데이터를 임포트하려면 MID 서버 속성을 활성화해야 합니다. 이 속성을 확인하거나 설정하려면 다음으로 이동하십시오. 모두 〉 **MID** 서버 〉 속성 〉 **sn_itom_pattern.discover_aws_app_pool_members**. 값을 true로 설정합니다.
자격 증명	서비스 계정에 대한 검색 자격 증명입니다.
URL	
접근 역할 이름	
접근용 계정 선택	

   e. 테스트 계정을 선택합니다.
   계속하려면 먼저 확인이 성공적으로 이루어져야 합니다.

   f. 다음을 선택합니다.

   g. 검색할 데이터센터를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

h. **IP** 주소로 **VM** 검색 토글을 선택하고 목록에서 d단계에서 선택한 MID 서버를 선택합니다.

i. 다음을 선택합니다.

j. 디스커버리을 실행할 빈도와 시기를 선택합니다.

k. 마침 및 실행을 선택합니다.

설정한 검색 일정이 실행된 후 검색 패턴 **Amazon AWS - 웹 ACL(LP)** 이 실행되고 두 애플리케이션에서 데이터가 임포트됩니다.

완화 통제 모니터링을 위한 **WAF** 통합에 대한 **AWS** 정책 만들기

통합에서 임포트한 데이터를 기반으로 자산을 감사할 수 있도록 정책을 생성합니다.

시작하기 전에

필요한 역할: SPC 관리자 그룹 또는 SPC 분석가 그룹

프로시저

1. 다음으로 이동 작업 공간 〉 보안 태세 통제 〉 정책 및 결과 〉 모두.
2. 자산 유형에 대해 하드웨어 자산을 선택합니다.

   속성은 자산 검색 및 자산 프로파일에도 작동합니다.
3. 연결에서 보안 제어 구성을 선택합니다.
4. 엔터티에 대해 **AWS Insight**를 선택합니다.

   기준 필드가 ##로 자동으로 채워져 표시됩니다.
5. 새 연결 필드에 대해 **AWS** 관리 규칙 사용을 선택합니다.

   엔터티 필드는 ## ## 으로 자동으로 채워지고 기준 필드는 ##으로 자동으로 채워져 표시됩니다. 빈 속성, 연산자 및 값 필드가 표시됩니다.

   사용자 지정 AWS 규칙을 만든 경우 사용자 지정 일치 문 포함을 선택합니다. 엔터티 필드가 Match Statement로 채워집니다.
6. 목록에서 속성을 선택합니다.

   두 개 이상 추가할 수 있습니다.

   예를 들어, AWS Service Account에 있는 SQL 데이터베이스용 웹 ACL의 경우 다음 규칙이 표시될 수 있습니다.

   - SQLiExtendedPatterns_QUERYARGUMENTS
   - SQLiQUERYARGUMNETS
   - SQLi_BODY
   - SQLi_COOKIE
   - SQLi_URIPATH

   정책 작성기에서 이 속성은 SQLRuleSet-SQLi_BODY 허용으로 표시됩니다. 목록에서 허용 또는 차단 을 선택할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

7. 속성을 추가하려면 또는 을 선택합니다.
   정책 작성기를 사용하여 정책을 생성하는 방법에 대한 자세한 내용은 을 참조하십시오 에 대한 사용자 지정 정책 생성 및 활성화 보안 태세 통제 .
8. 정책을 완료했으면 변경 내용 저장을 선택합니다.
9. 결과를 보려면 정책을 활성화합니다.
10. 정책에서 결과를 보는 방법에 대한 자세한 내용은 을 참조하십시오 보안 태세 통제: 결과 구성 및 보기 .
11. 목록에서 기록을 열고 완화 통제 완화된 취약 항목 탭을 선택합니다.

    완화된 취약한 항목 탭에는 자산에서 발견된 완화 규칙의 결과로 완화된 CVE에 대한 정보가 포함된 모든 완화된 취약한 항목이 나열됩니다.

    - 검증된 소스 - AWS API, ITOM Discovery
    - WAF(웹 애플리케이션 방화벽)로 보호됨 - 예
    - WAF 유형 - AWS
    - 취약 항목 완전 완화 - 완화된 관련 취약 항목 수입니다.
    - 부분적으로 완화된 취약한 항목 - 처리 중인 연결된 취약한 항목 수입니다.
    - 작업별로 분류된 관리 대상 규칙 - "차단" 및 "허용" 작업이 있는 관리 대상 규칙입니다.

      정책에 대해 입력한 것보다 더 많은 규칙이 표시될 수 있습니다. 이러한 규칙은 규칙에서 CommonRuleSet (CRS)으로 식별됩니다.
    - 사용자 지정 규칙 - "차단" 및 "허용" 작업으로 분류된 사용자 지정 규칙입니다.
    - 홈페이지 대시보드의 완화가 있는 자산 타일에는 WAF(Exploit Protection) 시각화에서 WAF로 보호되는 자산이 나열됩니다.

탐지된 완화 보기

사용 가능한 완화 제어를 통해 완화되는 자산의 위협을 보려면 먼저 정책을 활성화해야 합니다.

시작하기 전에

및 Microsoft SCCM용 서비스 그래프 커넥터 및 Microsoft Defender 완화 통제 통합 설치 및 구성F5 BIG-IP 완화 통제 모니터링을 위한 통합 구성에 나열된 완화 통제 모니터링을 위한 통합 설치 및 구성 CrowdStrike요구 사항을 완료했는지 확인합니다.

필요한 역할: SPC 관리자 그룹 및 SPC 분석가 그룹.

프로시저

대시보드의 "MITRE 완화가 있는 자산" 위젯을 사용하여 보안 태세 통제에서 탐지된 완화가 있는 자산을 보려면 다음 단계를 따르십시오.

a. 다음으로 이동 작업 공간 〉 보안 태세 통제 〉 홈.

b. 주요 인사이트 섹션에서 MITRE 완화가 있는 자산 위젯을 검토합니다.

c. 위젯에서 완화 범주, **EDR(Exploit Protection)** 또는 **WAF(Exploit Protection)** 를 선택합니다.

d. 해당 완화 범주에서 탐지된 완화가 있는 자산 목록을 볼 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

e. 자산을 선택합니다.

f. 완화 통제 탭을 선택하여 검색된 완화 통제의 세부 정보를 확인합니다.

g. 이 완화 통제로 완화된 취약한 항목 목록을 보려면 완화된 취약 항목 탭을 선택합니다.

> 주:
> 이 탭을 채우 취약성 대응 려면 애플리케이션을 설치하고 활성화해야 합니다.

취약한 항목 매핑에 대한 완화 통제

완화 통제 데이터가 취약한 항목에 매핑됩니다. 취약성 및 취약한 항목과 관련된 기본 CVE(알반적인 취약성 및 노출)를 완화하는 데 사용되는 완화 통제 목록을 볼 수 있습니다.

자산에서 특정 완화 통제를 식별한 후 보안 태세 통제는 해당 통제로 완화되는 취약한 항목을 자동으로 식별합니다. 예를 들어 WAF(웹 애플리케이션 방화벽) 정책에서 서명의 일부인 CVE가 있는 모든 취약한 항목은 완화된 취약한 항목으로 표시됩니다. 이 식별은 취약성 관리 팀이 완화된 취약한 항목의 위험 점수를 자동으로 줄이는 데 유용할 수 있습니다.

취약한 항목 완화 통제 테이블

완화 통제 데이터를 완화된 취약한 항목(VIT)에 매핑하기 위해 취약한 항목 완화 통제 [sn_vul_vulnerable_item_mitigation_control] 테이블이 생성되었습니다. 이 표에는 취약성을 완화하는 데 사용된 완화된 VIT 및 탐지된 완화 통제와 취약한 항목과 연결된 취약성의 기본 CVE가 나열되어 있습니다. 완화된 CVE 기록에는 자산에 사용되는 완화 통제(예: EDR(Exploit Protection)에 대한 참조가 포함되어 있습니다.

예시 데이터는 다음 표에 나와 있습니다.

취약한 항목 완화 통제 데이터

완화 통제가 존재함	완화 통제 효과성	탐지된 완화 통제 유형	완화된 **CVE**	취약한 항목
예/아니요	보통	EDR(악용 방지)	CVE-2009-3373	VIT0018323

테이블에서 완화 통제 기록(탐지된 완화 통제 유형)을 열어 자산과 연결된 완화 통제를 통해 CVE 및 관련 CWE(일반적인 약점 열거) 취약성을 완화하는 방법에 대한 상세 정보를 검토합니다. 완화 통제 기록에는 완화된 CWE에 대한 상세 정보(예: 완화 설정이 CWE에 지정된 취약성을 충족하는 방법)가 포함되어 있습니다.

위험 계산기 및 위험 계산기 규칙

완화 정보는 특정 유형의 취약성 및 완화 통제가 연결된 VIT의 위험 점수를 다시 계산하는 데 도움이 되는 사용자 지정 위험 계산기 규칙을 설정하는 데 사용될 수 있습니다. 앞의 테이블을 기반으로 하는 이 예시 규칙의 경우 기본 위험 계산기는 탐지된 자산에 대해 완화 통제 유형인 EDR(Exploit Protection)이 있는 VIT에 대해 위험 점수를 60으로 계산합니다. 이 계산 점수는 이 완화가 적용된 취약성과 연결된 보통 위험 때문입니다.

다음 조건이 있는 위험 계산기 규칙의 예:

〔완화 통제 상세 정보〕〔일치하지 않음〕〔비어 있음〕 및 〔완화 통제 상세 정보, 검색된 완화 통제 유형〕〔다음과 같음〕 **[EDR(Exploit Protection)]**.

값:

〔위험 점수〕**[is][60]**

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

자세한 내용은 Vulnerability Response 위험 계산기의 위험 규칙에 대한 필드와 가중치 정의 문서를 참조하십시오.

의 사용 사례, 정책 예시 및 지원되는 서비스 그래프 커넥터 보안 태세 통제

사용 사례는 특정 유형의 도구 범위 간격을 식별하는 데 도움이 되도록 구성하는 다양한 시나리오입니다. 각 사용 사례에는 자산의 잠재적 위반을 감사하는 정책이 필요합니다. 특정 내부 보안 표준에 대한 요구 사항을 충족하는 데 도움이 되는 자체 정책을 정의할 수도 있습니다.

사용 사례

보안 태세 통제 애플리케이션은 애플리케이션에 포함된 다양한 사용 사례를 지원합니다. 사용 사례는 자산의 특정 유형의 도구 범위 격차, 클라우드 자산의 인터넷 노출 및 취약성과의 조합을 식별하는 데 도움이 됩니다. 지원되는 사용 사례에 필요한 정책도 제품에 포함되어 있습니다.

보안 태세 통제 작업 공간의 홈(방문) 페이지에서 일부 주요 사용 사례에 대한 적용 범위 상태를 볼 수 있습니다. 작업 공간 〉 보안 태세 통제 〉 홈 홈 모듈(방문 페이지)의

또는 다음의 "서비스 그래프 커넥터 지원됨" 및 "주요 사용 케이스 설정" 탭에서 지원되는 서비스 그래프 커넥터 및 일부 주요 사용 케이스에 대한 적용 범위 상태를 볼 수 있습니다 모두 〉 작업 공간 〉 보안 태세 통제 〉 커넥터 및 사용 케이스 설정 (기어 아이콘)을 클릭합니다.

주:

홈 방문 페이지의 주요 사용 사례 탭에 가능한 모든 사용 사례가 나열되지는 않습니다. 보안 태세 통제 제품 배포를 시작하는 데 도움이 되도록 활성화하는 몇 가지 중요한 사용 사례를 제공합니다.

애플리케이션과 함께 제공되는 지원되는 사용 사례에 대한 정책을 활성화하기 전에 다음 작업을 완료했는지 확인하십시오.

- 에 설명된 모든 필수 애플리케이션을 설치하고 구성했습니다.보안 태세 통제에 지원되는 애플리케이션 설치
- 각 사용 사례에 대해 다음 필요 조건 중 하나 이상을 충족했습니다.

1. 다양한 범주에 대해 현재 서비스 그래프 커넥터를 사용 중이거나 설치하고 활성화합니다.

   사용 사례의 범주에는 초기 인사이트를 얻기 위해 활성화해야 하는 서비스 그래프 커넥터와 보안 태세 통제가 모니터링하는 자산의 범위를 개선하기 위해 활성화할 수 있는 옵션이 있는 서비스 그래프 커넥터가 포함됩니다.

2. 현재 취약성 대응 애플리케이션을 사용 중이거나 직접 설치 및 활성화합니다.
3. 현재 "클라우드 보안 태세 관리"에서 AWS 및 Azure 계정에 대한 클라우드 계정 스캔을 사용 중이거나 구성하고 있습니다.

지원되는 각 사용 사례에 대한 특정 요구 사항은 다음 섹션에 설명되어 있습니다. 또한 사용 사례에 대해 보안 태세 통제와 함께 제공되는 하나 이상의 정책을 활성화해야 합니다. 이 개념은 다음 섹션에서도 다룹니다.

기본, 하위 및 복제된 정책의 예

다른 정책을 생성할 때 기본 정책의 조건을 재사용할 수 있는 방법 을 참조하십시오 에 대한 기본, 하위 및 복제된 정책의 예 보안 태세 통제 . 다음 예시에서는 기본, 하위 정책을 생성하고 기존 정책을 복제합니다. 이러한 예는 정책 및 결과 모듈에서 정책 작성기가 작동하는 방식을 이해하는 데에도 도움이 됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

지원되는 서비스 그래프 커넥터

지원되는 서비스 그래프 커넥터, 해당 도구 범주 및 임포트하는 에 지원되는 하드웨어 서비스 그래프 커넥터 보안 태세 통제에 지원되는 소프트웨어 서비스 그래프 커넥터 보안 태세 통제데이터 유형의 테이블을 참조하십시오.

보안 태세 통제 사용 사례: 엔드포인트 보호가 누락된 자산 감지

엔드포인트 보호 에이전트가 누락된 자산을 검색하려면 다음 필수 구성 요소가 필요합니다.

사용 사례에 따라 필요한 커넥터만 활성화하도록 선택할 수 있습니다.

1. Endpoint Protection 범주에서 하나 이상의 서비스 그래프 커넥터를 활성화합니다.
2. 다음 범주 중 하나에 대해 하나 이상의 서비스 그래프 커넥터를 활성화합니다.
   a. 디렉터리 서비스().Microsoft Active Directory
   b. 엔드포인트 관리: Microsoft Intune 또는 Jamf 장치 및 엔드포인트 관리.
   c. 구성 및 패치 관리: Microsoft SCCM 또는 IBM Bigfix
   d. 클라우드 제공자: Amazon AWS Cloud, Microsoft Azure, . GCP

   > **주:**
   > 클라우드 검색이 활성화된 경우 이러한 서비스 그래프 커넥터 제품은 필요하지 않습니다.

3. 〔선택사항〕 다음 범주 중 하나에 대해 서비스 그래프 커넥터를 활성화하여 전체 범위, 즉 보안 태세 통제에서 보고 및 모니터링되는 자산 수를 개선할 수 있습니다.
   a. 네트워크 보안
   b. 인프라 모니터링
   c. 네트워킹
   d. 애플리케이션 성능 모니터링 .

이러한 사전 요구 사항을 충족했는지 확인한 후에는 엔드포인트 보호가 누락된 자산 정책을 활성화해야 합니다 . 정책에 대한 자세한 내용은 을 보안 태세 통제에 대한 정책참조하십시오.

보안 태세 통제 사용 사례: 취약성 평가 도구에서 누락된 자산 탐지

취약성 평가 도구에서 누락된 자산을 탐지하려면 다음 필요 조건이 필요합니다.

목록의 각 서비스 그래프 커넥터에 대해 온프레미스 자산 또는 클라우드 자산을 모니터링하는 데 커넥터가 필요한지 확인할 수 있습니다. 사용 사례에 따라 필요한 커넥터만 활성화하도록 선택할 수 있습니다.

1. 취약성 평가 범주에서 하나 이상의 서비스 그래프 커넥터를 활성화합니다.
2. 다음 범주 중 하나에 대해 하나 이상의 서비스 그래프 커넥터를 활성화합니다.
   a. 디렉터리 서비스().Microsoft Active Directory
   b. 엔드포인트 관리: Microsoft Intune 또는 Jamf 장치 및 엔드포인트 관리.
   c. 구성 및 패치 관리: Microsoft SCCM 또는 IBM Bigfix
   d. 클라우드 제공자: Amazon AWS Cloud, Microsoft Azure, . GCP

   > **주:**
   > 클라우드 검색이 활성화된 경우 이러한 서비스 그래프 커넥터 제품은 필요하지 않습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 〔선택사항〕 다음 범주 중 하나에 대해 서비스 그래프 커넥터를 활성화하여 전체 범위, 즉 보안 태세 통제에서 보고 및 모니터링되는 자산 수를 개선할 수 있습니다.
   a. 네트워크 보안 .
   b. 네트워킹.
   c. 인프라 모니터링
   d. 애플리케이션 성능 모니터링 .

이러한 필수 구성 요소를 충족했는지 확인한 후에는 취약성이 있는지 검사되지 않은 자산 정책을 활성화해야 합니다. 정책에 대한 자세한 내용은 을 보안 태세 통제에 대한 정책참조하십시오.

보안 태세 통제 사용 사례: 관리되지 않는 자산 감지

이 사용 사례는 구성 및 패치 관리 에이전트가 누락된 자산을 검색하는 두 부분으로 구성됩니다.

구성 및 패치 관리 도구가 누락된 자산을 탐지하려면 다음 필요 조건이 필요합니다.

목록의 각 서비스 그래프 커넥터에 대해 온프레미스 자산 또는 클라우드 자산을 모니터링하는 데 커넥터가 필요한지 확인할 수 있습니다.

사용 사례에 따라 필요한 커넥터만 활성화하도록 선택할 수 있습니다.

1. 구성 및 패치 관리 범주에서 하나 이상의 서비스 그래프 커넥터를 활성화합니다.
2. 다음 범주 중 하나에 대해 하나 이상의 서비스 그래프 커넥터를 활성화해야 합니다.
   a. 디렉터리 서비스().Microsoft Active Directory
   b. Endpoint Protection: CrowdStrike 또는 SentinelOne.
   c. 취약성 평가: Qualys, Rapid7또는 Tenable.
   d. 구성 및 패치 관리: Microsoft SCCM 또는 IBM Bigfix
3. 〔선택사항〕 다음 범주 중 하나에 대해 서비스 그래프 커넥터를 활성화하여 전체 범위, 즉 보안 태세 통제에서 보고 및 모니터링되는 자산 수를 개선할 수 있습니다.
   a. 네트워킹.
   b. 인프라 모니터링
   c. 네트워크 보안
   d. 애플리케이션 성능 모니터링 .

이러한 필요 조건이 충족되었는지 확인한 후에는 다음 정책 중 하나 이상을 활성화해야 합니다. "클라우드 자산"으로 시작하는 모든 정책의 경우 "클라우드 제공자" 범주의 서비스 그래프 커넥터를 활성화해야 합니다. 정책에 대한 자세한 내용은 다음을 참조하십시오 보안 태세 통제에 대한 정책.

- 자산에 구성 및 패치 관리가 누락되었습니다.
- 클라우드 자산에 구성 및 패치 관리가 누락되었습니다.

보안 태세 통제 사용 사례: 엔드포인트 관리 솔루션이 누락된 자산 감지

엔드포인트 관리 솔루션이 누락된 자산을 탐지하려면 다음과 같은 필요 조건이 필요합니다.

사용 사례에 따라 필요한 커넥터만 활성화하도록 선택할 수 있습니다.

1. 엔드포인트 관리 범주에서 하나 이상의 서비스 그래프 커넥터를 활성화합니다.
2. 다음 범주 중 하나에 대해 하나 이상의 서비스 그래프 커넥터를 활성화해야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 디렉터리 서비스().Microsoft Active Directory

b. Endpoint Protection: CrowdStrike 또는 SentinelOne.

c. 취약성 평가: Qualys, Rapid7또는 Tenable.

d. 구성 및 패치 관리: Microsoft SCCM 또는 IBM Bigfix

이러한 필요 조건이 충족되었는지 확인한 후에는 자산 누락 엔드포인트 관리 솔루션 정책을 활성화해야 합니다. 정책에 대한 자세한 내용은 을 보안 태세 통제에 대한 정책참조하십시오.

보안 태세 통제 사용 사례: 취약성 및 보안 도구 범위 격차가 있는 자산 탐지

중요한 취약성이 있는 자산과 엔드포인트 보호와 같은 중요한 보안 도구가 누락된 자산을 식별하여 정정할 자산의 우선순위를 지정할 수 있습니다. 보안 태세 통제는 이 사용 사례를 지원하기 위해 제품에 포함된 몇 가지 정책을 제공합니다.

이 사용 케이스를 사용하려면 취약성 대응 애플리케이션을 설치하고 최소한 취약성 평가 제품(예: , , Rapid7또는 Tenable)Qualys과의 통합을 필요로 합니다.

다음 정책은 보안 도구 적용 범위가 누락된 중요한 취약성이 있는 자산에 대한 이 사용 사례를 지원하기 위해 보안 태세 통제 제품에 포함되어 있습니다.

1. 중요한 취약성이 있고 엔드포인트 보호가 누락된 자산입니다.

2. 중요한 취약성이 있고 구성 및 패치 관리가 누락된 자산입니다.

3. 중요한 취약성이 있고 엔드포인트 관리가 누락된 자산입니다.

보안 태세 통제 사용 사례: 클라우드 자산 및 고위험 조합의 인터넷 노출 감지

다양한 포트에서 클라우드 자산(가상 머신)의 잠재적인 인터넷 노출을 모니터링하여 이러한 자산의 취약성이 원격으로 악용되지 않도록 하는 것이 중요합니다. 이 사용 사례는 이러한 자산을 식별하는 데 도움이 됩니다.

보안 태세 통제를 사용하면 클라우드 자산의 구성을 평가하여 인터넷에 연결된 자산, 즉 인터넷 어디에서나 연결할 수 있는 자산과 자산이 노출되는 포트를 식별할 수 있습니다.

보안 태세 통제는 이러한 인사이트를 , 또는 Tenable과 같은 QualysRapid7외부 공급업체 스캐너의 보안 도구 범위 격차 및 취약성 데이터와 결합하여 고위험 조합을 식별합니다.

현재 이 사용 케이스는 AWS를 지원하며 다음과 같은 사전 조건이 필요합니다.

1. AWS용 서비스 그래프 커넥터는 구성한 것과 동일한 AWS 계정에 대해 활성화됩니다.

2. 보안 태세 통제에서 제품에 포함된 하나 이상의 정책을 활성화했습니다.

- SSH 포트 22가 있는 클라우드 자산이 인터넷에 열립니다.
- SSH 포트 22가 인터넷에 열려 있고 엔드포인트 보호가 없는 클라우드 자산입니다.
- HTTP 포트 80이 인터넷에 열려 있고 엔드포인트 보호가 없는 클라우드 자산입니다.
- 중요한 취약성이 있는 클라우드 자산 및 SSH 포트 22가 인터넷에 열려 있습니다(취약성 대응 필요).
- 중요한 취약성이 있고 엔드포인트 보호 및 SSH 포트 22가 없는 클라우드 자산이 인터넷에 열려 있습니다(취약성 대응 필요).
- 인터넷에 개방된 HTTP 포트, 중요한 취약성 및 엔드포인트 보호가 누락된 클라우드 자산(필수 취약성 대응).

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

에 지원되는 하드웨어 서비스 그래프 커넥터 보안 태세 통제

CI 클래스, 소스(제품) 및 도구 범주가 있는 지원되는 하드웨어 서비스 그래프 커넥터입니다. 이 목록은 완전하지 않으며 더 많은 제품이 추가됨에 따라 변경될 수 있습니다.

나열된 커넥터에 대한 검색 소스의 경우 'SG', 'SGO' 또는 'SGC'가 타사 제품의 제품 이름 앞에 옵니다(예: SG-AWS, SGO-Datadog 또는 SGC-AD(Active Directory). ServiceNow 제품의 경우 제품 이름 앞에 'SN' 또는 'ServiceNow'가 옵니다(예: ServiceNow 하드웨어 자산 관리의 경우 SNAssetManagement).

설치한 후에는 인스턴스의 커넥터 테이블 〔sn_sec_spc_core_connector〕에서 커넥터와 해당 범주를 볼 수 있습니다.

자산 유형과 [sn_sec_spc_core_asset_type_connector] 테이블에서 CI 클래스 및 커넥터에 매핑되는 방식을 볼 수 있습니다.

하드웨어 서비스 그래프 커넥터

자산 유형	CI 클래스	자산 소스	커넥터 범주
하드웨어 자산	cmdb_ci_computer	Active Directory	디렉터리 서비스
하드웨어 자산	cmdb_ci_server	AppDynamics	애플리케이션 성능 모니터링
하드웨어 자산	cmdb_ci_server	자동 목스	구성 및 패치 관리
하드웨어 자산	cmdb_ci_computer	자동 목스	구성 및 패치 관리
하드웨어 자산	cmdb_ci_computer	BigFix	구성 및 패치 관리
하드웨어 자산	cmdb_ci_server	BigFix	구성 및 패치 관리
하드웨어 자산	cmdb_ci_printer	Cisco 메라키	네트워킹
하드웨어 자산	cmdb_ci_server	Cisco 메라키	네트워킹
하드웨어 자산	cmdb_ci_iot	Cisco 메라키	네트워킹
하드웨어 자산	cmdb_ci_hc_device	Cisco 메라키	네트워킹
하드웨어 자산	cmdb_ci_netgear	Cisco 메라키	네트워킹
하드웨어 자산	cmdb_ci_computer	Cisco 메라키	네트워킹
하드웨어 자산	cmdb_ci_server	CrowdStrike	엔드포인트 보호
하드웨어 자산	cmdb_ci_server	Datadog	인프라 모니터링
하드웨어 자산	cmdb_ci_server	Dynatrace	애플리케이션 성능 모니터링
하드웨어 자산	cmdb_ci_computer	Dynatrace	애플리케이션 성능 모니터링
하드웨어 자산	cmdb_ci_computer	엑스트라홉 공개(x)	네트워크 보안
하드웨어 자산	cmdb_ci_hc_device	엑스트라홉 공개(x)	네트워크 보안
하드웨어 자산	cmdb_ci_server	엑스트라홉 공개(x)	네트워크 보안
하드웨어 자산	cmdb_ci_iot	엑스트라홉 공개(x)	네트워크 보안
하드웨어 자산	cmdb_ci_printer	엑스트라홉 공개(x)	네트워크 보안
하드웨어 자산	cmdb_ci_iot	포에스카우트	네트워크 보안

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

하드웨어 서비스 그래프 커넥터

자산 유형	CI 클래스	자산 소스	커넥터 범주
하드웨어 자산	cmdb_ci_hc_device	포에스카우트	네트워크 보안
하드웨어 자산	cmdb_ci_computer	포에스카우트	네트워크 보안
하드웨어 자산	cmdb_ci_server	포에스카우트	네트워크 보안
하드웨어 자산	cmdb_ci_printer	포에스카우트	네트워크 보안
하드웨어 자산	cmdb_ci_server	Intune	엔드포인트 관리
하드웨어 자산	cmdb_ci_computer	Intune	엔드포인트 관리
하드웨어 자산	cmdb_ci_printer	Jamf Pro	엔드포인트 관리
하드웨어 자산	cmdb_ci_server	Jamf Pro	엔드포인트 관리
하드웨어 자산	cmdb_ci_computer	Jamf Pro	엔드포인트 관리
하드웨어 자산	cmdb_ci_server	랜스위퍼	IT 자산 관리
하드웨어 자산	cmdb_ci_computer	랜스위퍼	IT 자산 관리
하드웨어 자산	cmdb_ci_printer	랜스위퍼	IT 자산 관리
하드웨어 자산	cmdb_ci_hc_device	로직모니터	인프라 모니터링
하드웨어 자산	cmdb_ci_printer	로직모니터	인프라 모니터링
하드웨어 자산	cmdb_ci_server	로직모니터	인프라 모니터링
하드웨어 자산	cmdb_ci_vm_instance	로직모니터	인프라 모니터링
하드웨어 자산	cmdb_ci_iot	로직모니터	인프라 모니터링
하드웨어 자산	cmdb_ci_computer	로직모니터	인프라 모니터링
하드웨어 자산	cmdb_ci_netgear	로직모니터	인프라 모니터링
하드웨어 자산	cmdb_ci_server	Microsoft Defender	엔드포인트 보호
하드웨어 자산	cmdb_ci_server	New Relic	애플리케이션 성능 모니터링
하드웨어 자산	cmdb_ci_computer	넥스씽크	디지털 직원 경험
하드웨어 자산	cmdb_ci_computer	Netskope	데이터 손실 방지
하드웨어 자산	cmdb_hardware_product_model	Netskope	데이터 손실 방지
하드웨어 자산	cmdb_ci_network_adapter	Netskope	데이터 손실 방지
하드웨어 자산	cmdb_software_instance	Netskope	데이터 손실 방지
하드웨어 자산	cmdb_sam_sw_install	Netskope	데이터 손실 방지
하드웨어 자산	sn_sec_sgc_netskop_client_attribute	Netskope	데이터 손실 방지
하드웨어 자산	cmdb_ci_server	원격 측정 열기	애플리케이션 성능 모니터링
하드웨어 자산	cmdb_ci_computer	Puppet	구성 및 패치 관리
하드웨어 자산	cmdb_ci_server	Puppet	구성 및 패치 관리
하드웨어 자산	cmdb_ci_computer	Qualys	취약성 평가

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

하드웨어 서비스 그래프 커넥터

자산 유형	CI 클래스	자산 소스	커넥터 범주
하드웨어 자산	cmdb_ci_server	Qualys	취약성 평가
하드웨어 자산	cmdb_ci_vm_instance	Qualys-ServiceNow	취약성 평가
하드웨어 자산	cmdb_ci_server	Qualys-ServiceNow	취약성 평가
하드웨어 자산	cmdb_ci_hardware	Rapid7	취약성 평가
하드웨어 자산	cmdb_ci_computer	SCCM	구성 및 패치 관리
하드웨어 자산	cmdb_ci_server	SCCM	구성 및 패치 관리
하드웨어 자산	cmdb_ci_printer	ScienceLogic	인프라 모니터링
하드웨어 자산	cmdb_ci_iot	ScienceLogic	인프라 모니터링
하드웨어 자산	cmdb_ci_server	ScienceLogic	인프라 모니터링
하드웨어 자산	cmdb_ci_computer	ScienceLogic	인프라 모니터링
하드웨어 자산	cmdb_ci_hc_device	ScienceLogic	인프라 모니터링
하드웨어 자산	cmdb_ci_vm_instance	ScienceLogic	인프라 모니터링
하드웨어 자산	cmdb_ci_hardware	ServiceNow HAM	하드웨어 자산 관리
하드웨어 자산	cmdb_ci_hardware	ServiceNow ITOM 디스커버리	디스커버리
하드웨어 자산	cmdb_ci_aws_datacenter	SentinelOne	엔드포인트 보호
하드웨어 자산	cmdb_ci_azure_datacenter	SentinelOne	엔드포인트 보호
하드웨어 자산	cmdb_ci_availability_zone	SentinelOne	엔드포인트 보호
하드웨어 자산	cmdb_ci_google_datacenter	SentinelOne	엔드포인트 보호
하드웨어 자산	cmdb_ci_cloud_service_account	SentinelOne	엔드포인트 보호
하드웨어 자산	cmdb_ci_cloud_subnet	SentinelOne	엔드포인트 보호
하드웨어 자산	cmdb_ci_compute_template	SentinelOne	엔드포인트 보호
하드웨어 자산	cmdb_ci_network	SentinelOne	엔드포인트 보호
하드웨어 자산	cmdb_ci_vm_instance	SentinelOne	엔드포인트 보호
하드웨어 자산	cmdb_key_value	SentinelOne	엔드포인트 보호
하드웨어 자산	cmdb_ci_os_template	SentinelOne	엔드포인트 보호
하드웨어 자산	cmdb_ci_server	SentinelOne	엔드포인트 보호
하드웨어 자산	cmdb_ci_computer	SentinelOne	엔드포인트 보호
하드웨어 자산	sn_sec_sgc_sntlone_asset_tags	SentinelOne	엔드포인트 보호
하드웨어 자산	cmdb_ci_ip_address	SentinelOne	엔드포인트 보호
하드웨어 자산	cmdb_ci_network_adapter	SentinelOne	엔드포인트 보호
하드웨어 자산	sn_sec_sgc_sntlone_additional_attributes	SentinelOne	엔드포인트 보호
하드웨어 자산	cmdb_ci_server	Tanium 자산	엔드포인트 관리
하드웨어 자산	cmdb_ci_computer	Tanium 자산	엔드포인트 관리

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

하드웨어 서비스 그래프 커넥터

자산 유형	CI 클래스	자산 소스	커넥터 범주
하드웨어 자산	cmdb_ci_ups	Tenable	취약성 평가
하드웨어 자산	cmdb_ci_ot_industrial_sensor	Tenable	취약성 평가
하드웨어 자산	cmdb_ci_ot_cnc	Tenable	취약성 평가
하드웨어 자산	cmdb_ci_hardware	Tenable	취약성 평가
하드웨어 자산	cmdb_ci_netgear	Tenable	취약성 평가
하드웨어 자산	cmdb_ci_ot_industrial_actuator	Tenable	취약성 평가
하드웨어 자산	cmdb_ci_ip_switch	Tenable	취약성 평가
하드웨어 자산	cmdb_ci_hub_network	Tenable	취약성 평가
하드웨어 자산	cmdb_ci_security	Tenable	취약성 평가
하드웨어 자산	cmdb_ci_server	Tenable	취약성 평가
하드웨어 자산	cmdb_ci_ot_rtu	Tenable	취약성 평가
하드웨어 자산	cmdb_ci_ot_ews	Tenable	취약성 평가
하드웨어 자산	cmdb_ci_ot_plc	Tenable	취약성 평가
하드웨어 자산	cmdb_ci_ot_control	Tenable	취약성 평가
하드웨어 자산	cmdb_ci_ot_dcs	Tenable	취약성 평가
하드웨어 자산	cmdb_ci_storage_server	Tenable	취약성 평가
하드웨어 자산	cmdb_ci_ot_hmi	Tenable	취약성 평가
하드웨어 자산	cmdb_ci_ot_control_module	Tenable	취약성 평가
하드웨어 자산	cmdb_ci_ot_industrial_robot	Tenable	취약성 평가
하드웨어 자산	cmdb_ci_ot_historian	Tenable	취약성 평가
하드웨어 자산	cmdb_ci_ot_industrial_drive	Tenable	취약성 평가
하드웨어 자산	cmdb_ci_iot	Tenable	취약성 평가
하드웨어 자산	cmdb_ci_ip_firewall	Tenable	취약성 평가
하드웨어 자산	cmdb_ci_computer	Tenable	취약성 평가
하드웨어 자산	cmdb_ci_unclassed_hardware	Tenable	취약성 평가
하드웨어 자산	cmdb_ci_ids_network	Tenable	취약성 평가
하드웨어 자산	cmdb_ci_ot_ied	Tenable	취약성 평가
하드웨어 자산	cmdb_ci_printer	Tenable	취약성 평가
하드웨어 자산	cmdb_ci_computer	VMWare Workspace ONE UEM	엔드포인트 관리
하드웨어 자산	cmdb_ci_server	VMWare Workspace ONE UEM	엔드포인트 관리
하드웨어 자산	cmdb_ci_printer	VMWare Workspace ONE UEM	엔드포인트 관리

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

하드웨어 서비스 그래프 커넥터

자산 유형	CI 클래스	자산 소스	커넥터 범주
하드웨어 자산	cmdb_ci_vm_instance	Wiz	클라우드 네이티브 애플리케이션 보호 플랫폼
하드웨어 자산	cmdb_ci_server	Wiz	클라우드 네이티브 애플리케이션 보호 플랫폼
하드웨어 자산	cmdb_ci_linux_server	Wiz	클라우드 네이티브 애플리케이션 보호 플랫폼
하드웨어 자산	cmdb_ci_win_server	Wiz	클라우드 네이티브 애플리케이션 보호 플랫폼

에 지원되는 소프트웨어 서비스 그래프 커넥터 보안 태세 통제

CI 클래스, 소스(제품) 및 도구 범주가 있는 지원되는 소프트웨어 서비스 그래프 커넥터입니다. 이 목록은 완전하지 않으며 더 많은 제품이 추가됨에 따라 변경될 수 있습니다.

설치한 후에는 인스턴스의 커넥터 테이블〔sn_sec_spc_core_connector〕에서 커넥터와 해당 범주를 볼 수 있습니다.

자산 유형과 [sn_sec_spc_core_asset_type_connector] 테이블에서 CI 클래스 및 커넥터에 매핑되는 방식을 볼 수 있습니다.

소프트웨어 서비스 그래프 커넥터

자산 유형	CI 클래스	자산 소스	커넥터 범주
소프트웨어	cmdb_ci_spkg	BigFix	구성 및 패치 관리
소프트웨어	cmdb_ci_spkg	Dynatrace	애플리케이션 성능 모니터링
소프트웨어	cmdb_ci_spkg	포에스카우트	네트워크 보안
소프트웨어	cmdb_ci_spkg	Intune	엔드포인트 관리
소프트웨어	cmdb_ci_spkg	Jamf Pro	엔드포인트 관리
소프트웨어	cmdb_ci_spkg	New Relic	애플리케이션 성능 모니터링
소프트웨어	cmdb_ci_spkg	넥스씽크	디지털 직원 경험
소프트웨어	cmdb_ci_spkg	Netskope	데이터 손실 방지
소프트웨어	cmdb_ci_spkg	Qualys-ServiceNow	취약성 평가
소프트웨어	cmdb_ci_spkg	SCCM	구성 및 패치 관리
소프트웨어	cmdb_ci_spkg	ServiceNow ITOM 디스커버리	디스커버리
소프트웨어	cmdb_ci_spkg	Tanium 자산	엔드포인트 관리

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

소프트웨어 서비스 그래프 커넥터

자산 유형	CI 클래스	자산 소스	커넥터 범주
소프트웨어	cmdb_ci_spkg	VMWare Workspace ONE UEM	엔드포인트 관리

에 대한 기본, 하위 및 복제된 정책의 예 보안 태세 통제

보다 복잡한 정책의 시작점으로 사용할 수 있는 광범위한 조건 집합이 포함된 고유한 기본 정책을 만들 수 있습니다.

예제

다음 예시는 하위 정책을 생성하거나 기존 정책을 복제하여 다른 정책을 생성할 때 기본 정책의 조건을 재사용할 수 있는 방법을 확인하는 데 도움이 됩니다. 이러한 예는 정책 및 결과 모듈에서 정책 작성기가 작동하는 방식을 이해하는 데에도 도움이 됩니다.

첫 번째 예인 기본 정책부터 시작합니다. 다른 예시에서는 기본 정책을 시작점으로 사용합니다.

주:
이 예시에서는 CrowdStrike 서비스 그래프 커넥터를 서비스 그래프 커넥터로 사용하지만 이미 설치한 모든 커넥터를 사용할 수 있습니다. 이 예시에서는 자산 일치를 찾기 위해 정책을 만들고 활성화합니다. 이러한 정책을 활성화한 후 언제든지 정책 및 결과 모듈에서 이러한 정책을 제거할 수 있습니다.

다음에 대한 보안 태세 통제 기본 정책 만들기(예)

다른 정책을 생성하는 데 사용할 수 있는 기본 정책을 생성하는 방법의 예시입니다.

시작하기 전에
필요한 역할: SPC 관리자 그룹 또는 SPC 분석가 그룹

프로시저

1. 다음으로 이동 모두 〉 보안 태세 통제 작업 공간 〉 정책 및 결과.
2. 새 정책을 선택합니다.
3. 왼쪽 상단에 있는 펜 아이콘을 선택하고 메타데이터 편집 모달의 필드에 내용을 입력합니다.
4. 메타데이터 저장을 선택합니다.
5. 조건 작성기에서 자산 유형에 대해 하드웨어 자산을 선택합니다.

   이 정책의 경우 기본 정책 및 제외 정책 옵션을 기본(꺼짐) 설정으로 둡니다.
6. 연결에서 집계된 데이터 포함을 선택합니다.

   이 정책의 경우 집계된 데이터는 Windows 10이 설치된 CMDB에서 자산을 찾는 데 도움이 됩니다. 예를 들어 일부 레코드는 스캐너마다 'Windows 10′을 보고하는 방식에 약간의 차이가 있을 수 있습니다. 집계된 데이터는 'Windows 10′의 이러한 모든 약간의 변형이 이 정책과 일치하도록 합니다.

   엔터티 및 기준 필드는 연결 필드에서 선택한 항목에 따라 자동으로 채워집니다.
7. 속성에 대해 **OS**를 선택합니다.
8. Windows 10의 값 유형에 대해 다음을 수행합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

9. 변경 사항 저장을 선택합니다.
   기본 정책이 정책 및 결과 모듈의 모든 목록에 표시되지만 활성화되지는 않습니다.
10. 기본 정책이 정책의 조건과 일치하는 자산을 모니터링하고 결과를 생성하도록 정책 활성화 를 선택합니다.

(예) 에 대한 보안 태세 통제 기본 정책에서 하위 정책 생성

기본 정책의 조건을 사용하여 하위 정책을 생성하는 방법의 예입니다.

시작하기 전에

이 하위 정책은 기본 정책의 조건을 상속하며, 하위 정책에 더 많은 조건을 추가하여 보다 구체적인 자산 상세 정보에 집중할 수 있습니다. 서비스 그래프 커넥터에서 CrowdStrike 보고하는 Windows 10이 설치된 모든 디바이스를 모니터링하는 새 정책을 원하고 다른 정책과 일치하는 디바이스를 제외하려고 합니다. 이 예에서는 IRM(통합 위험 관리) 예외에 대해 승인된 자산을 결과에서 제외합니다.

> **주:**
> CrowdStrike 서비스 그래프 커넥터가 설치되어 있지 않은 경우 설치된 커넥터를 사용할 수 있습니다.

필요한 역할: SPC 관리자 그룹 또는 SPC 분석가 그룹

프로시저

1. 다음으로 이동 모두 〉 보안 태세 통제 작업 공간 〉 정책 및 결과.
2. 활성 목록에서 첫 번째 예에서 만든 기본 정책 - Windows 10 장치를 찾고 선택하여 기록을 엽니다.
3. 추가 옵션 메뉴(세로 점 3개)를 선택하고 하위 정책 생성을 선택합니다.
   새 탭이 열리고 새 레코드와 함께 기본 정책 - Windows 10 장치가 기본 정책 필드에 표시됩니다.
4. 왼쪽 상단에 있는 펜 아이콘을 선택하고 메타데이터 편집 모달에서 필드를 채웁니다.
5. 메타데이터 저장을 선택합니다.
6. 조건 작성기에서 자산 유형에 대해 하드웨어 자산을 선택합니다.
7. 기본 정책 토글을 선택합니다.
8. 목록에서 예제 1, 기본 정책 **- Windows 10** 장치에 대해 만든 정책을 선택합니다.

   이 하위 정책은 기본 정책의 조건을 자동으로 상속합니다.
9. 제외 정책 토글을 선택합니다.
10. 목록에서 승인된 IRM 예외가 있는 자산을 선택합니다.

    > **주:**
    > 이 정책이 없는 경우 이 정책에서 제외하려는 목록에서 다른 정책을 선택할 수 있습니다.
    >
    > 이 정책과 일치하는 자산은 하위 정책에서 제외됩니다. 정책을 더 추가할 수 있습니다.
11. 보고자를 선택합니다.
12. 목록에서 **CrowdStrike** 를 선택합니다.
13. 변경 사항 저장을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

새 정책이 정책 및 결과 모듈의 모든 목록에 표시되지만 활성화되지는 않습니다.

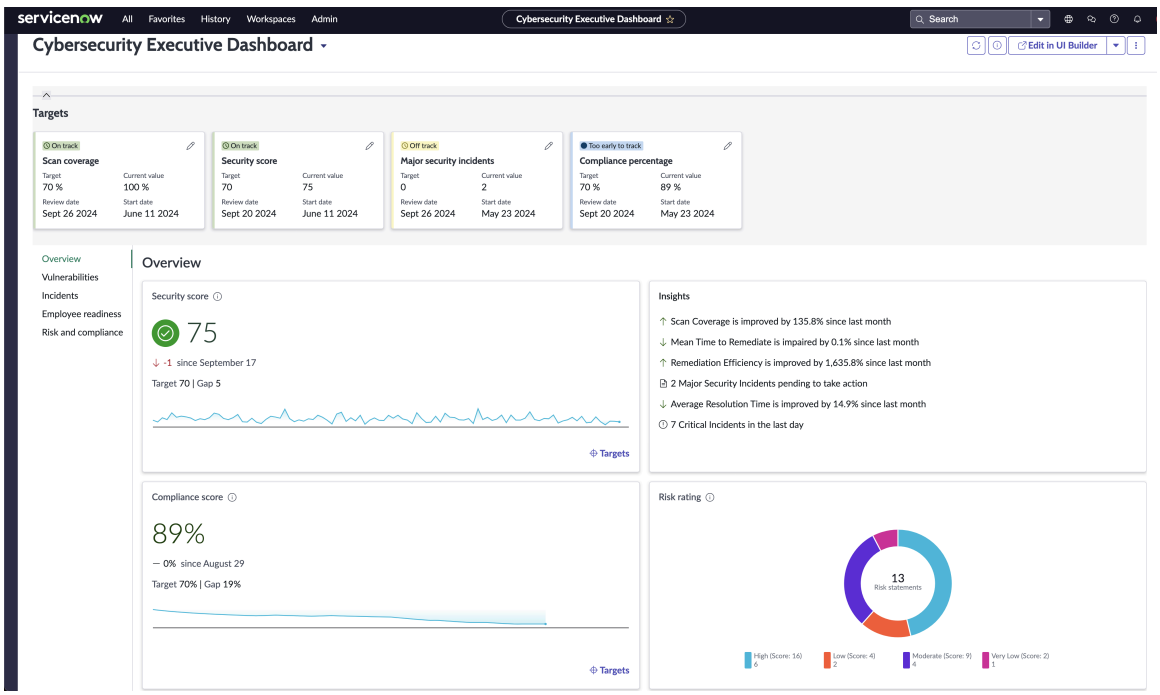
14. 기본 정책이 정책의 조건과 일치하는 자산을 모니터링하고 결과를 생성하도록 정책 활성화 를 선택합니다.

사이버 보안 임원 대시보드

사이버 보안 임원 대시보드는 최고 정보 보안 책임자(CISO) 및 사이버 보안 임원에게 조직의 보안 태세 및 이니셔티브에 대한 가시성을 제공하는 포괄적인 솔루션입니다. 대시보드는 보안 운영 제품군과 GRC(거버넌스, 위험 및 준수) ServiceNow 내의 다양한 제품의 데이터를 통합합니다.

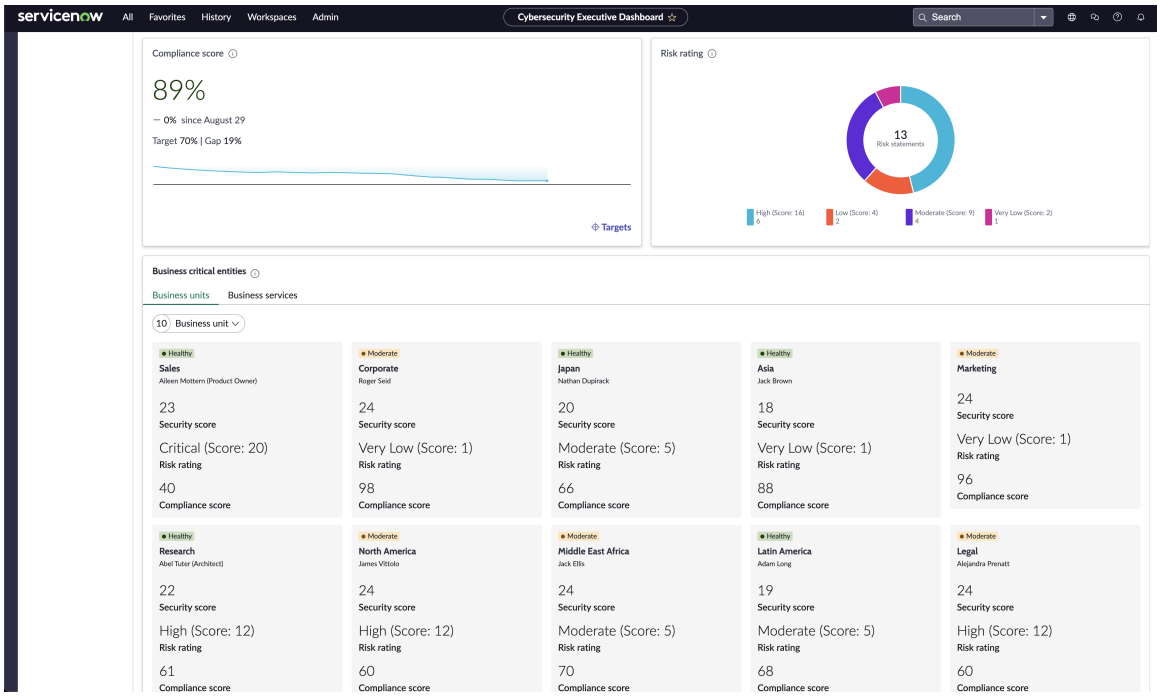
대시보드는 다음과 같은 기능을 제공합니다.

- 조직 전반의 보안 태세 점수 매기기
- 비즈니스 단위별 보안, 위험 및 준수 점수
- 사용자 지정 가능한 모니터링
- 조직의 보안 환경에 대한 통합 뷰
- 벤치마킹
- 사용자 친화적인 인터페이스
- KnowBe4 및 Office 365용 Microsoft Defender 피싱 시뮬레이션 메트릭에 대한 가시성



이러한 기능을 사용하면 중요한 보안 메트릭에 빠르게 액세스할 수 있으므로 사전 예방적 의사 결정이 가능합니다. 따라서 전반적인 보안 복원력과 준비 태세를 강화하는 데 없어서는 안 될 도구입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



필요한 **ServiceNow AI Platform** 역할

- 대시보드를 보고 공유할 CISO(sn_bod.ciso)
- sn_bod.ciso_admin 대시보드를 보고, 공유하고, 보안 태세 등급에 대한 가중치를 구성하려면
- GRC CISO 사용자(sn_grc_dashboards.grc_ciso_user)는 위험 및 준수 보고서를 볼 수 있습니다.

사이버 보안 임원 대시보드에 액세스

대시보드를 열려면 다음으로 이동합니다. 모두 〉 사이버 보안 임원 대시보드 〉 사이버 보안 임원 대시보드.

사용 사례

조직 내 다른 사람이 이 대시보드를 사용하는 방법의 예시는 다음 사용 사례를 참조합니다.

사용자	대시보드 사용
최고 정보 보안 책임자(CISO)	CISO는 조직의 취약성 관리, 인시던트 관리, 조직 보안 태세, 피싱 시뮬레이션 메트릭 등에 대한 인사이트를 얻습니다.

데이터 시각화

주:

위젯에 대한 자세한 내용을 보려면 정보 아이콘 ⓘ 을 선택합니다.

대상

메트릭	유형	설명
대상	백분율	메트릭에 적용할 대상 설정을 표시합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

대상

메트릭	유형	설명
		대상의 상태는 색상 코딩을 통해 표시됩니다. 검토 날짜가 지난 30일 이내이거나 다가오는 날짜인 모든 대상을 표시합니다. 시스템 속성을 사용하여 대상을 표시할 일 수를 설정할 수 있습니다 *sn_bod.show_targets_from*. 또한 이러한 대상을 편집할 수 있습니다. 자세한 내용은 대상 설정 문서를 참조하십시오.

메트릭	유형	설명
보안 점수	단일 점수	취약 항목, 보안 인시던트, 중요 보안 인시던트 및 잘못된 구성을 고려한 조직의 보안 태세에 대한 전체 점수입니다.
인사이트	하이라이트	전체 대시보드의 하이라이트입니다.
규정 준수 점수	단일 점수	총 통제 수 중 준수 통제 비율을 기준으로 계산된 규정 준수 점수의 도움을 받아 조직의 규정 준수 태세를 제공합니다.
위험 점수	단일 점수	위험 등급에 따른 위험 보고서 수를 제공합니다. 이를 통해 조직은 다양한 위험의 잠재적 영향과 가능성을 파악하여 이러한 위험의 우선순위를 정하고 관리할 수 있습니다.
비즈니스 중요 엔터티		
비즈니스 단위	단일 점수	취약성, 잘못된 구성, OT(운영 기술) 취약성, 보안 인시던트 및 주요 보안 인시던트와 관련된 위험을 고려하여 비즈니스 단위의 전반적인 보안 점수입니다. 비즈니스 단위의 상태 레이블은 보안 점수만을 기반으로 합니다. 이러한 레이블이 할당되는 방식을 보려면 위험 점수 가중치 [sn_sec_cmn_risk_score_weight_list.do] 테이블로 이동하여 비즈니스

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

메트릭	유형	설명
		엔터티를 검색합니다. "정상"과 같은 레이블은 미리 정의된 값 범위에 따라 할당됩니다. 예를 들어 0에서 39 사이의 보안 점수는 정상으로 표시됩니다. 이러한 레이블의 색 코딩은 UnifiedCISOutils 스크립트 포함에 지정됩니다. 레이블의 색상과 값 범위를 모두 구성할 수 있습니다. 비즈니스 단위 및 비즈니스 단위 책임자 이름이 할당되는 방식을 보려면 다음으로 이동하십시오. 모두 〉 조직 〉 비즈니스 단위. 주: 활성화한 플러그인에 따라 준수 점수, 위험 점수 및 보안 점수에 액세스할 수 있습니다. 준수 및 위험 점수를 보려면 GRC 플러그인을 활성화해야 합니다. 보안 점수를 보려면 보안 운영 관련 플러그인을 활성화해야 합니다. 자세한 내용은 Applications to active 섹션을 참조하십시오.
비즈니스 서비스	단일 점수	취약성, 잘못된 구성, OT(운영 기술) 취약성, 보안 인시던트 및 주요 보안 인시던트와 관련된 위험을 고려하여 비즈니스 서비스의 전반적인 보안 점수입니다. 이러한 레이블이 할당되는 방식을 보려면 위험 점수 가중치 [sn_sec_cmn_risk_score_weight_list.do] 테이블로 이동하여 비즈니스 엔터티를 검색합니다. 미리 정의된 값 범위에 따라 "정상", "보통" 및 "중요"와 같은 레이블이 할당됩니다. 예를 들어 0에서 39 사이의 보안 점수는 정상으로 표시됩니다. 이러한 레이블의 색 코딩은UnifiedCISOutils 스크립트 포함에 지정됩니다. 레이블의 색상과 값 범위를 모두 구성할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

메트릭	유형	설명
		비즈니스 단위 및 비즈니스 단위 책임자 이름이 할당되는 방식을 보려면 다음으로 이동하십시오. 모두 〉 조직 〉 비즈니스 단위. 주: 활성화한 플러그인에 따라 준수 점수, 위험 점수 및 보안 점수에 액세스할 수 있습니다. 준수 및 위험 점수를 보려면 GRC 플러그인을 활성화해야 합니다. 보안 점수를 보려면 보안 운영 관련 플러그인을 활성화해야 합니다. 자세한 내용은 Applications to active 섹션을 참조하십시오.

취약성

메트릭	유형	설명
정정 평균 시간(월간)	꺾은선형	한 달 동안 모든 자산(호스트, 컨테이너 및 애플리케이션)에서 취약성과 실패한 테스트 결과를 종결하는 데 걸린 평균 시간입니다. 또한 다음과 같은 메트릭을 제공합니다. • 대상: 취약성을 정정하기 위해 설정된 목표(일)입니다. • 격차: 취약성을 정정하는 데 걸린 목표와 실제 시간 간의 차이(일)입니다. • 업계 벤치마크: 같은 업계 내 동종 업체의 평균 메트릭입니다. • 글로벌 벤치마크: 글로벌 시장 동종 업체의 평균 메트릭 벤치마크 점수를 보는 방법을 참조하십시오 벤치마크 점수에 대한 옵트인 .
활성 취약성의 평균 기간(월간)	단일 점수	세 가지 유형의 취약한 항목의 월별 평균 기간입니다. 또한

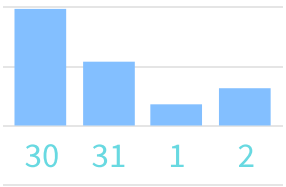
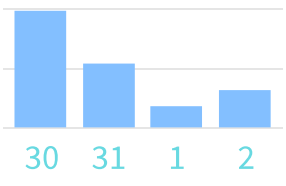
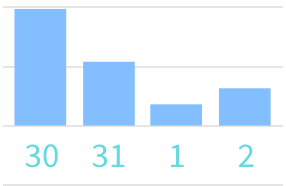
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약성

메트릭	유형	설명
		현재 월 경과 기간을 이전 월과 비교할 수 있습니다. 또한 다음과 같은 메트릭을 제공합니다. • 업계 벤치마크: 같은 업계 내 동종 업체의 평균 메트릭입니다. • 글로벌 벤치마크: 글로벌 시장 동종 업체의 평균 메트릭 • 대상: 취약성을 정정하기 위해 설정된 목표(일)입니다.
정정 효율성(월간)	단일 점수	월별 활성 취약한 항목 대비 월별 종결된 취약한 항목의 비율입니다. 또한 다음과 같은 메트릭을 제공합니다. • 전월의 백분율 변화입니다. • 대상: 취약성을 정정하기 위해 설정된 목표(백분율)입니다. • 격차: 대상 점수와 현재 점수 간의 격차입니다. • 업계 벤치마크: 같은 업계 내 동종 업체의 평균 메트릭입니다. • 글로벌 벤치마크: 글로벌 시장 동종 업체의 평균 메트릭
활성 상태인 취약성의 할당 그룹별 평균 기간	여러 줄	각 할당 그룹에 대한 활성 상태인 취약성의 평균 기간입니다.
위험 등급 및 기간별 취약성	히트맵	호스트, 컨테이너 및 애플리케이션에서 활성 상태인 취약성을 위험 등급 및 기간별로 분류합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약성

메트릭	유형	설명
할당 그룹별 정정 대상 준수	세로 막대 	정정 대상 내에서 종결된 취약성 및 잘못된 구성 수 대비 종결된 취약성 및 잘못된 구성 수 합계의 비율입니다.
스캔 보장 범위	백분율	의 모든 자산 중에서 지난 90일 동안 스캔한 자산의 백분율입니다 CMDB.
스캔된 자산과 스캔되지 않은 자산의 비교	가로 막대	지난 90일 동안 스캔한 자산과 CI 클래스별 총 CMDB 자산의 세부 항목
스캔한 자산	가로 막대	취약성과 구성 준수의 비교에 따라 지난 90일 동안 검사된 자산입니다.
활성 상태의 심각 결과 및 높은 결과 추세	다중 라인	심각 및 높은 위험 등급의 취약성 및 잘못된 구성의 일일 추세입니다.
자산 범주 및 위험 등급별 취약성	세로 막대 	활성 상태인 취약성과 잘못된 구성의 자산 범주 및 위험 등급(심각, 높음 및 중간)별 세부 항목입니다.
사유 및 할당 그룹에 의해 지연된 결과	세로 막대 	지연 사유 및 할당 그룹에 의해 지연된 활성 상태의 취약성과 잘못된 구성의 세부 항목입니다.
운영 기술(OT)		
활성 상태의 심각 취약성 및 높은 취약성의 추세	선	심각 및 높은 위험 등급에서 활성 상태인 OT 취약성의 일일 추세입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

취약성

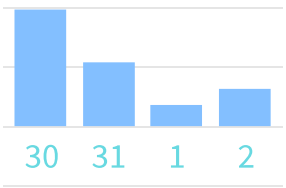
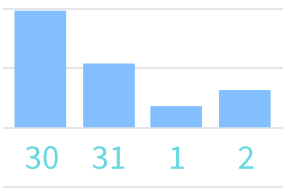
메트릭	유형	설명
정정 평균 시간(월간)	단일 점수	OT 취약성을 종결하는 데 걸린 평균 시간입니다. 종결된 OT 취약성의 총 기간 대비 총 OT 취약성 수의 비율입니다. 또한 다음과 같은 메트릭을 제공합니다. • 전월의 백분율 변화입니다. • 대상: 취약성을 정정하기 위해 설정된 목표(일)입니다. • 업계 벤치마크: 같은 업계 내 동종 업체의 평균 메트릭입니다. • 글로벌 벤치마크: 글로벌 시장 동종 업체의 평균 메트릭 벤치마크 점수를 보는 방법을 참조하십시오 벤치마크 점수에 대한 옵트인 .
위험 등급 및 기간별 취약성	히트맵	활성 OT 취약성의 위험 등급 및 기간별 세부 항목입니다.
활성 취약성의 평균 기간(월간)	꺾은선형 차트	OT 취약 항목의 월별 평균 기간입니다. 또한 현재 월 경과 기간을 이전 월과 비교할 수 있습니다.
상태 및 기간별 취약성	히트맵	활성 상태인 OT 취약성의 상태 및 기간별 세부 항목입니다.

인시던트

메트릭	유형	설명
중요 보안 인시던트	단일 점수	현재 활성 상태인 중요 보안 인시던트 수입니다.
평균 보안 인시던트 해결 시간(월간)	단일 점수	종결된 보안 인시던트의 월별 평균 해결 시간(일)입니다. 또한 다음과 같은 메트릭을 제공합니다. • 전월의 백분율 변화입니다. • 대상: 보안 인시던트를 정정하기 위해 일 단위로 설정된 목표입니다.

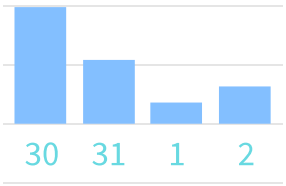
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

인시던트

메트릭	유형	설명
		• 격차: 해결하는 데 걸리는 실제 기간(일)과 정정하기 위해 설정된 대상 사이의 격차입니다. • 업계 벤치마크: 같은 업계 내 동종 업체의 평균 메트릭입니다. • 글로벌 벤치마크: 글로벌 시장 동종 업체의 평균 메트릭
평균 근절 시간(월간)	꺾은선형 차트	보안 인시던트를 근절하기 위한 월 평균 해결 일수입니다.
평균 식별 시간(월간)	단일 점수	보안 인시던트를 식별하기 위한 월별 평균 해결 일수입니다.
평균 포함 시간(월간)	단일 점수	보안 인시던트를 포함하기 위한 월별 평균 해결 일수입니다.
우선순위 및 범주별 활성 인시던트	히트맵	우선순위 및 범주별로 분류된 활성 상태인 보안 인시던트 수입니다.
종결 및 미해결 인시던트 추세	세로 막대 	종결 및 미해결 인시던트의 세부 항목입니다.
상태별 활성 인시던트	세로 막대 	상태를 기준으로 한 활성 인시던트의 세부 항목입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

직원 복귀 준비 상태

메트릭	유형	설명
월간 피싱 시뮬레이션 개요	세로 막대 	지난 6개월 동안 각 시뮬레이션의 총 사용자 합계와 함께 피싱 시뮬레이션에서 오픈, 클릭, 보고와 같은 작업을 수행한 사용자의 합계입니다.

위험 및 준수

위험 및 준수 위젯을 보려면 GRC 플러그인을 활성화해야 합니다. GRC 플러그인에 대한 자세한 내용은 활성화할 애플리케이션 섹션을 참조하십시오. GRC 위젯에 대한 자세한 내용은 다음 문서를 참조하십시오 용 위험 및 준수 대시보드 GRC: 메트릭.

표시기

호스트 SLA – 종결됨

이 지표는 매일 계산됩니다. 계산 시 전날에 종결된 모든 호스트 취약성의 총 기간을 고려합니다.

컨테이너 SLA – 종결됨

이 지표는 매일 계산됩니다. 계산 시 전날에 종결된 모든 컨테이너 취약성을 고려합니다.

애플리케이션 SLA – 종결됨

이 지표는 매일 계산됩니다. 계산 시 전날에 종결된 모든 애플리케이션 취약성의 총 기간을 고려합니다.

SLA 테스트 결과 - 통과함

이 지표는 매일 계산됩니다. 계산 시 전날에 통과한 모든 테스트 결과 취약성을 고려합니다.

호스트 SLA - 종결 횟수

이 지표는 매일 계산됩니다. 계산 시 전날에 종결된 모든 호스트 취약성의 수를 고려합니다.

컨테이너 SLA - 종결 횟수

이 지표는 매일 계산됩니다. 계산 시 전날에 종결된 모든 컨테이너 취약성의 개수를 고려합니다.

애플리케이션 SLA - 종결 횟수

이 지표는 매일 계산됩니다. 계산 시 전날에 종결된 모든 애플리케이션 취약성의 수를 고려합니다.

SLA 테스트 결과 – 통과 횟수

이 지표는 매일 측정됩니다. 계산 시 전날에 마지막으로 통과된 모든 테스트 결과 취약성의 수를 고려합니다.

스캔된 자산

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 지표는 매일 계산됩니다. 모든 CMDB CI 클래스에 걸쳐 지난 90일 이내에 마지막으로 스캔한 CI를 포함하여 sn_vul_analytics_scan_coverage_config 테이블에서 스캔한 CI의 합계를 고려합니다.

스캔 가능한 자산

이 지표는 매일 계산됩니다. 이는 존재하는 모든 CMDB CI 클래스에 대해 sn_vul_analytics_scan_coverage_config 테이블의 총 CI 합계를 고려합니다.

취약 항목

이 지표는 매일 계산됩니다. 계산 시 활성 취약한 항목 수를 고려합니다.

애플리케이션 취약한 항목

이 지표는 매일 계산됩니다. 계산 시점의 활성 애플리케이션 취약한 항목 수를 고려합니다.

컨테이너 취약한 항목

이 지표는 매일 계산됩니다. 계산 시 활성 컨테이너 취약한 항목 수를 고려합니다.

취약한 항목의 합산 기간

이 지표는 매일 계산됩니다. 계산 시 활성 취약한 항목의 합산 기간을 고려합니다.

애플리케이션 취약한 항목의 합산 기간

이 지표는 매일 계산됩니다. 계산 시 활성 애플리케이션 취약한 항목의 합산 기간을 고려합니다.

미해결된 취약 항목

이 지표는 매일 계산됩니다. 계산 시 미해결된 취약 항목을 고려합니다.

미해결된 컨테이너 취약 항목

이 지표는 매일 계산됩니다. 계산 시 열린 컨테이너에 취약한 항목을 고려합니다.

미해결된 애플리케이션 취약 항목

이 지표는 매일 계산됩니다. 계산 시 열려 있는 애플리케이션 취약 항목을 고려합니다.

활성 테스트 결과

이 지표는 매일 계산됩니다. 계산 시 열린 테스트 결과를 고려합니다.

지연된 VIT

이 지표는 매일 계산됩니다. 표시기 소스가 호스트 취약 항목입니다.

지연된 AVIT

이 지표는 매일 계산됩니다. 표시기 소스가 애플리케이션 취약한 항목으로 포함되어 있습니다.

지연된 CVIT

이 지표는 매일 계산됩니다. 표시기 소스가 컨테이너 취약한 항목입니다.

지연된 테스트 결과

이 지표는 매일 계산됩니다. 지연된 상태의 테스트 결과를 고려합니다.

미해결 구성 문제 - 테스트 결과

이 지표는 매일 계산됩니다. 통합 취약성 대응 대시보드의 테스트 결과로 표시기 소스가 있습니다.

SI-평균 식별 시간

이 지표는 매일 계산됩니다. 계산 시 정의가 식별 시간인 보안 인시던트를 고려합니다.

SI - 평균 지속 시간

이 지표는 매일 계산됩니다. 정의가 계산 당시의 인시던트 상태 기간인 보안 인시던트를 고려합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

미해결된 중요 보안 인시던트 수

이 지표는 매일 계산됩니다. 계산 시 열린 중요 보안 인시던트를 고려합니다.

종결된 보안 인시던트 수

이 지표는 매일 계산됩니다. 계산 시 종결된 보안 인시던트를 고려합니다.

닫힌 애플리케이션 취약한 항목

이 지표는 매일 계산됩니다. 계산 시 종결된 애플리케이션 취약한 항목을 고려합니다.

종결된 컨테이너 취약한 항목

이 지표는 매일 계산됩니다. 계산 시 닫힌 컨테이너 취약 항목을 고려합니다.

닫힌 취약한 항목

이 지표는 매일 계산됩니다. 계산 시 종결된 취약한 항목을 고려합니다.

취약 항목에 대한 최대 위험 점수 가져오기

이 지표는 매일 계산됩니다. 계산 시 취약한 항목에 대한 최대 위험 점수를 고려합니다.

컨테이너 취약 항목에 대한 최대 위험 점수 가져오기

이 지표는 매일 계산됩니다. 계산 시 컨테이너 취약한 항목에 대한 최대 위험 점수를 고려합니다.

애플리케이션 취약 항목에 대한 최대 위험 점수 가져오기

이 지표는 매일 계산됩니다. 계산 시 애플리케이션 취약한 항목에 대한 최대 위험 점수를 고려합니다.

VIT의 위험 점수 합계

이 지표는 매일 계산됩니다. 계산 시 취약한 항목의 위험 점수 합계를 고려합니다.

AVI의 위험 점수 합계

이 지표는 매일 계산됩니다. 계산 시 애플리케이션 취약한 항목의 위험 점수 합계를 고려합니다.

CVI의 위험 점수 합계

이 지표는 매일 계산됩니다. 계산 시 컨테이너 취약한 항목의 위험 점수 합계를 고려합니다.

잘못된 구성의 합산 위험 점수

이 지표는 매일 계산됩니다. 계산 시 테스트 결과의 위험 점수 합계를 고려합니다.

SI 인시던트에 대한 최대 위험 점수 가져오기

이 지표는 매일 계산됩니다. 계산 시 보안 인시던트의 최대 위험 점수를 고려합니다.

잘못된 구성 테스트 결과에 대한 최대 위험 점수 가져오기

이 지표는 매일 계산됩니다. 계산 시 잘못된 테스트 결과 구성에 대한 최대 위험 점수를 고려합니다.

잘못된 구성 테스트 결과에 대한 평균 위험 점수 가져오기

이 지표는 매일 계산됩니다. 계산 시 잘못된 테스트 결과 구성에 대한 평균 위험 점수를 고려합니다.

오픈 보안 인시던트 수

이 지표는 매일 계산됩니다. 계산 시 열려 있는 보안 인시던트를 고려합니다.

피싱 개요

이 지표는 매일 계산됩니다. 계산 시 보안 시뮬레이션 메트릭의 개수를 고려합니다.

MTTR 집계

취약성(호스트, 컨테이너 및 애플리케이션)을 종결하는 데 걸리는 평균 시간과 테스트 결과를 종결하는 데 걸린 시간(일)을 계산합니다. {{호스트 SLA - 종결됨}} +

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

{{애플리케이션 SLA - 종결됨}} + {{컨테이너 SLA - 종결됨}} + {{SLA 테스트 결과 - 통과}}) / ({{호스트 SLA - 종결 횟수}} + {{애플리케이션 SLA - 종결 횟수}} + {{SLA 테스트 결과 - 통과 횟수}} + {{컨테이너 SLA - 종결 횟수}})

현재 스캔 보장 범위

스캔한 항목 수와 같은 기간 동안 스캔할 수 있는 총 항목 수 간의 비율을 활용하여 백분율을 계산합니다. var scannedItems ={{스캔한 자산}}; var scannableItems = {{스캔 가능한 자산}}; var 해상도; if (scannedItems == 0)res = 0; elseres = scannedItems / scannableItems * 100; if (res 〉 100)res = 100; 해상도;

활성 취약한 항목의 평균 기간

활성 상태인 모든 취약한 항목(호스트, 컨테이너 및 애플리케이션)의 평균 기간을 일 단위로 계산합니다. ({{취약한 항목의 합산 기간}} + {{애플리케이션 취약한 항목의 합산 기간}} + {{컨테이너 취약한 항목의 합산 기간}}) / ({{취약한 항목}} + {{애플리케이션 취약한 항목}} + {{컨테이너 취약한 항목}})

연령 및 위험 등급별 활성 VIT

사용 기간 및 위험 평가 수준별로 분류된 모든 활성 취약한 항목(호스트, 컨테이너 및 애플리케이션)의 총 수를 계산합니다. {{미해결된 취약한 항목}} + {{미해결된 컨테이너 취약한 항목}} + {{미해결된 애플리케이션 취약한 항목}}

지연된 문제점

상태가 '연기됨'인 모든 취약한 항목(호스트, 컨테이너, 애플리케이션 및 테스트 결과)의 총 개수를 계산합니다. {{지연된 VIT}} + {{지연된 AVIT}} + {{지연된 테스트 결과}} + {{지연된 CVIT}}

종결 보안 인시던트의 평균 해결 시간

보안 인시던트를 종결하는 데 걸린 평균 시간(일)을 계산합니다. ({{종결된 보안 인시던트의 합산 기간}} / {{종결된 보안 인시던트의 수}}) /24

보안 점수

전체 보안 등급을 매일 계산합니다. 롤업된 위험 점수를 기준으로 계산됩니다. var secPostureRating = 100 - {{보안 점수}}; sec자세 등급;

보안 점수(비즈니스 단위)

취약 항목, 잘못된 구성, 보안 인시던트 및 중요 보안 인시던트의 롤업 위험 점수에 보안 태세 롤업 테이블에서 가져온 각 가중치를 곱한 최종 롤업된 위험 점수를 계산합니다. var numMajorIncidents = {{미해결된 중요 보안 인시던트 수}}, majorSIRiskScore, rollUpRiskScore; if(numMajorIncidents 〉 0) majorSIRiskScore = 100; else majorSIRiskScore = 0; rollUpRiskScore = ({{취약성 및 잘못된 구성 롤업된 위험 점수}} * 20 + {{OT 취약성 롤업된 위험 점수}} * 20 + {{SI 인시던트에 대한 최대 위험 점수 가져오기}} * 20 + majorSIRiskScore * 40)/100; 롤업리스크스코어;

보안 점수(비즈니스 서비스)

취약 항목, 잘못된 구성, 보안 인시던트 및 중요 보안 인시던트의 롤업 위험 점수에 보안 태세 롤업 테이블에서 가져온 각 가중치를 곱한 최종 롤업된 위험 점수를 계산합니다. var numMajorIncidents = {{미해결된 중요 보안 인시던트 수 - 서비스}}, majorSIRiskScore, rollUpRiskScore; if(numMajorIncidents 〉 0) majorSIRiskScore = 100; else majorSIRiskScore = 0; rollUpRiskScore = ({{취약성 및 잘못된 구성 롤업된 위험 점수 - 서비스}} * 20 + {{OT 취약성 롤업된 위험 점수 - 서비스}} * 20 + {{SI 인시던트에 대한 최대 위험 점수 가져오기 - 서비스}} * 20 + majorSIRiskScore * 40)/100; 롤업리스크스코어;

취약성 롤업된 위험 점수

최대 위험 점수, 취약한 항목의 평균 위험 점수 및 취약한 항목 수를 각각의 가중치와 곱한 취약성 롤업된 위험 점수를 계산합니다. var maxRiskScore = 100; var count = {{연령 및 위험 등급별 활성 VIT}}; var countRiskScore; if (0 == count) countRiskScore = 0; else if (count 〉 10000) countRiskScore = maxRiskScore; else

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

if (count 〉 1000) countRiskScore = (maxRiskScore * 0.80); else if (count 〉 100) countRiskScore = (maxRiskScore * 0.60); else if (count 〉 10) countRiskScore = (maxRiskScore * 0.40); 그렇지 않으면 countRiskScore = (maxRiskScore * 0.20); var vulRiskScore = ({{모든 취약한 항목의 최대 점수 얻기}} * 0 + {{모든 취약한 항목의 평균 위험 점수}} * 100 + countRiskScore * 0)/100; vulRiskScore;

모든 취약 항목에서 최대 점수 가져오기

최대 위험 점수, 취약한 항목의 평균 위험 점수 및 취약한 항목 수를 각각의 가중치와 곱한 취약성 롤업된 위험 점수를 계산합니다. var maxScoreForVI = {{취약한 항목에 대한 최대 위험 점수 가져오기}}, maxScoreForCVI = {{컨테이너 취약한 항목에 대한 최대 위험 점수 가져오기}}, maxScoreForAVI = {{애플리케이션 취약한 항목에 대한 최대 위험 점수 가져오기}}, maxScore; if (maxScoreForVI 〉= maxScoreForCVI && maxScoreForVI 〉= maxScoreForAVI) maxScore = maxScoreForVI; else if (maxScoreForCVI 〉= maxScoreForVI && maxScoreForCVI 〉= maxScoreForAVI) maxScore = maxScoreForCVI; else maxScore = maxScoreForAVI; 맥스 스코어;

모든 취약 항목에 대한 평균 위험 점수

모든 취약한 항목(호스트, 컨테이너 및 애플리케이션)의 평균 위험 점수를 계산합니다. var summedRiskScore = {{VIT의 위험 점수 합계}} + {{AVI의 위험 점수 합계}} + {{CVI의 위험 점수 합계}}, avgRiskScore; var totalVulCount = {{미해결된 취약한 항목}} + {{애플리케이션 취약한 항목 미해결}} + {{미해결된 컨테이너 취약한 항목}}; if(summedRiskScore == 0) avgRiskScore = 0; else if(totalVulCount .=0) avgRiskScore = summedRiskScore / totalVulCount; 평균 위험 점수;

잘못된 구성 롤업된 위험 점수

실패, 오류 또는 알 수 없음으로 범주화된 테스트 결과를 사용하여 잘못된 구성 롤업된 위험 점수를 계산합니다. var maxRiskScore = 100; var count = {{미해결 구성 문제 - 테스트 결과}}; var countRiskScore; if (0 == count) countRiskScore = 0; else if (count 〉 10000) countRiskScore = maxRiskScore; else if (count 〉 1000) countRiskScore = (maxRiskScore * 0.80); else if (count 〉 100) countRiskScore = (maxRiskScore * 0.60); else if (count 〉 10) countRiskScore = (maxRiskScore * 0.40); 그렇지 않으면 countRiskScore = (maxRiskScore * 0.20); var misRiskScore = ({{잘못된 구성 테스트 결과에 대한 최대 위험 점수 가져오기}} * 0 + {{잘못된 구성 테스트 결과에 대한 평균 위험 점수 가져오기}} * 100 + countRiskScore * 0)/100; misRiskScore;

평균 근절 시간

보안 인시던트를 근절하는 데 걸리는 평균 시간(일) 계산 {{SI - 보안 인시던트 상태 〉 평균 기간 = 근절}}/1440

평균 식별 시간

보안 인시던트를 식별하는 데 걸리는 평균 시간을 일 단위로 계산합니다. {{SI - 평균 식별 시간}} / 1440

평균 포함 시간

보안 인시던트를 억제하는 데 걸린 평균 시간을 일 단위로 계산합니다. {{SI - 보안 인시던트 상태 〉 평균 기간 = 포함}} / 1440

정정 대상 준수

테스트 결과, 취약한 항목, 컨테이너 취약한 항목 및 애플리케이션 취약한 항목에서 월별 정정 대상 준수 백분율을 계산합니다. 목표 준수는 설정된 목표를 달성한 항목 수에 따라 결정됩니다. ({{테스트 결과 SLA - 통과 횟수 〉 정정 상태(통합) = 대상 충족}} + {{컨테이너 SLA - 종결된 횟수 〉 정정 상태(통합) = 대상 충족}} + {{애플리케이션 SLA - 종결된 횟수 〉 정정 상태(통합) = 대상 충족}} + {{호스트 SLA - 종결된 횟수 〉 정정 상태(통합) = 대상 충족}}) / ({{테스트 결과 SLA - 통과 횟수}} + {{컨테이너 SLA - 종결 횟수}} + {{애플리케이션 SLA - 종결 횟수}} + {{호스트 SLA - 종결 횟수}}) * 100

월별 정정 효율성(모든 취약한 항목)

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

새로 식별된 취약한 항목과 대조적으로 종결된 취약한 항목, 컨테이너 취약한 항목 및 애플리케이션 취약한 항목의 월별 백분율을 계산합니다. var closedItems = {{호스트 SLA - 종결 횟수}} + {{컨테이너 SLA - 종결 횟수}} + {{애플리케이션 SLA - 종결 횟수}} + {{SLA 테스트 결과 - 통과 횟수}};

var newItems = {{호스트 VIT 어제 오픈됨/어제 다시 오픈됨}} + {{컨테이너 VIT 어제 오픈됨/다시 오픈됨}} + {{애플리케이션 VIT 어제 오픈됨/다시 오픈됨}} + {{테스트 결과 어제 오픈됨/다시 오픈됨}};

var res = 0; if (closedItems == 0) res = 0; 그렇지 않으면 (newItems .=0)res = closedItems / newItems * 100; if (res 〉 1000) res = 1000; 해상도;

호스트 VIT 어제 오픈됨/다시 오픈됨

이 지표는 매일 계산됩니다. 계산 시 전날에 마지막으로 열린 호스트 취약한 항목을 고려합니다.

애플리케이션 VIT 어제 오픈됨/다시 오픈됨

이 지표는 매일 계산됩니다. 계산 시 전날에 마지막으로 열린 애플리케이션 취약한 항목을 고려합니다.

컨테이너 VIT 어제 오픈됨/다시 오픈됨

이 지표는 매일 계산됩니다. 계산 시 전날에 마지막으로 열린 컨테이너 취약한 항목을 고려합니다.

테스트 결과 어제 오픈됨/다시 오픈됨

이 지표는 매일 계산됩니다. 계산 시 전날에 마지막으로 표시된 테스트 결과를 고려합니다.

OT 취약 항목

이 지표는 매일 계산됩니다. 계산 시 활성 OT 취약 항목이 있는 것으로 간주합니다.

닫힌 취약 항목의 OT 합산 기간

이 지표는 매일 계산됩니다. 계산 당일에 종결된 모든 OT 취약성의 총 기간을 고려합니다.

OT 닫힌 취약 항목

이 지표는 매일 계산됩니다. 계산 당일에 종결된 OT 취약 항목을 고려합니다.

OT 활성 상태인 취약 항목의 평균 기간

OT 취약 항목의 평균 기간을 계산합니다({{OT 취약 항목의 합산 기간}}/{{OT 취약 항목}}).

세부 항목

- 비즈니스 단위
- 비즈니스 서비스
- 위험 등급
- 연령 범위
- 담당 그룹(통합)
- 정정 대상 상태(닫힘)
- 자산 클래스
- 자산 범주
- 위험 등급 (통합)

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 지연 이유(통합)
- 보안 인시던트 상태
- 보안 인시던트 우선순위
- 보안 인시던트 범주
- 피싱 이벤트
- 지연 이유 비종결(통합)

활성화할 애플리케이션

위젯에 점수를 채우려면 다음 애플리케이션을 활성화해야 합니다. 사용 중인 애플리케이션에 따라 종속 애플리케이션을 활성화해야 합니다.

를 사용하는 경우	활성화
취약성 대응	• 취약성 대응용 Performance Analytics • 취약성 대응 공통 • 취약성 대응 • 컨테이너를 위한 취약성 대응 및 구성 준수 • 구성 준수
운영 기술	운영 기술용 취약성 대응
피싱 통합	• SecOps용 보안 시뮬레이션 및 교육 통합 • SecOps용 KnowBe4 통합 • SecOps용 Office365용 Microsoft Defender 통합
보안 인시던트 응답	• 보안 인시던트 응답의 퍼포먼스 분석 • 보안 인시던트 응답 • 중요 보안 인시던트 관리
거버넌스, 위험, 컴플라이언스	• GRC: 공통 대시보드 요소 • GRC: 위험 관리 작업 공간 • GRC: 고급 위험 • GRC: 준수 관리 작업 공간

데이터 수집을 위한 예약된 작업

다음 예약된 작업이 실행되어 새 데이터에 대한 점수를 자동으로 수집합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예약된 작업	빈도	설명
벤치마크 점수 업로드	요청 시	인스턴스에서 점수를 수집하여 중앙 인스턴스에 게시합니다. 벤치마크 알고리즘은 업계 최고 점수를 계산합니다.
벤치마크 점수 다운로드	요청 시	벤치마크 점수를 다운로드합니다. 벤치마크 점수 〔sn_bm_client_score_list〕 테이블에서 사용할 수 있습니다.

벤치마크 점수에 대한 옵트인

인스턴스를 ServiceNow 중앙 인스턴스에 등록하여 벤치마크 점수를 가져옵니다. 후자는 벤치마크 점수를 제공하기 위해 여러 산업의 정보를 유지합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
벤치마킹에 대한 자세한 내용은 다음 문서를 참조하십시오 Exploring Benchmarks .

프로시저

1. 중앙 인스턴스에 인스턴스를 등록하려면 다음 단계를 따르십시오.

a. 다음으로 이동 모두 〉 시스템 속성 〉 모든 속성.

b. 시스템 속성을 선택합니다 *sn_bm_client.central_instance_url* .

c. 값 필드에 벤치마크 중앙 인스턴스 URL을 입력합니다.

> **주:**
> 인스턴스가 프로비저닝되면 상세 정보가 자동으로 중앙 인스턴스에 푸시됩니다.

d. 위젯에서 옵트인을 선택하여 중앙 인스턴스와의 연결을 확인하고 설정합니다.

2. 중앙 인스턴스에 점수를 업로드하려면 다음 단계를 따르십시오.

a. 다음으로 이동 모두 〉 시스템 스케줄러 〉 예약된 작업

b. *Upload the benchmark scores* 예약된 작업을 선택합니다.

c. 업데이트를 선택합니다.
점수가 중앙 인스턴스에 업로드됩니다. 그러나 중앙 인스턴스의 예약된 작업은 한 달에 한 번 실행되어 대시보드 위젯의 점수를 업데이트합니다.

3. 중앙 인스턴스에서 점수를 다운로드하려면 다음 단계를 따르십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 다음으로 이동 모두 〉 시스템 스케줄러 〉 예약된 작업

b. *Download the benchmark scores* 예약된 작업을 선택합니다.

c. 지금 실행을 선택합니다.
점수는 벤치마크 점수(sn_bm_client_score_list) 테이블에서 확인할 수 있으며 이는 대시보드 위젯에 반영됩니다.

대상 설정

며칠 안에 대상을 설정하여 취약성, 보안 인시던트 및 잘못된 구성을 정정합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 위젯에서 대상을 선택하거나 KPI 세부 정보 페이지에서 대상 아이콘을 선택합니다.
2. 모든 사용자용 단추를 선택합니다.
3. 새 값 필드에 목표를 달성하려는 일수를 입력합니다.
4. 대상 시작 날짜를 선택합니다.
5. 목표 검토 날짜를 선택합니다.
6. 업데이트를 선택합니다.

Security Operations를 위한 보안 시뮬레이션 및 교육 통합

사이버 보안 임원 대시보드와 피싱 통합을 통합하여 눈에 띄는 사이버 보안 위협에 대한 조직의 방어를 강화합니다. 피싱 통합은 KnowBe4 및 Office 365용 Microsoft Defender 같은 타사 피싱 시뮬레이션 도구의 데이터를 원활하게 통합하여 사이버 보안 임원 대시보드를 향상시킵니다.

다음 통합은 사이버 보안 임원 대시보드의 기능을 향상시켜 조직의 보안 태세, 직원 준비 상태 및 피싱 공격에 대한 취약성에 대한 통합된 관점을 제공합니다.

- KnowBe4 통합
- Office 365용 Microsoft Defender 통합

Knowbe4 통합 구성

선도적인 사이버 보안 인식 교육 플랫폼인 KnowBe4와 통합하여 피싱 공격에 대한 직원의 취약성에 대한 즉각적인 통찰력을 확보하십시오. KnowBe4 통합을 통해 사이버 보안 교육 프로그램의 추세와 개선 영역을 식별하고, 전반적인 피싱 복원력을 모니터링하고, 조직의 보안 조치를 사전에 강화합니다.

시작하기 전에
필요한 역할: sn_sec_phish.admin 및 sn_sec_phish_kb4.kb4_admin

프로시저

1. 다음으로 이동 모두 〉 **KnowBe4** 통합 〉 **KnowBe4** 구성.
2. 새로 만들기를 선택합니다.
3. 양식에 상세 정보를 입력합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

KnowBe4 구성 양식

필드	설명
통합 인스턴스	통합 인스턴스의 이름입니다. 조회 아이콘을 사용하여 통합 인스턴스를 선택합니다.
기본 URL	KnowBe4와 통합할 URL입니다.
API 키	KnowBe4 계정에서 가져온 API 키입니다.
페이지	시뮬레이션을 가져와야 하는 페이지 번호입니다.
페이지 크기	포함해야 하는 시뮬레이션 수입니다.

a. 사용할 수 있는 통합 인스턴스가 없는 경우 새로 만들기를 선택합니다.

b. 양식에 상세 정보를 입력합니다.

통합 인스턴스 양식

필드	설명
이름	통합 인스턴스의 이름입니다.
애플리케이션	애플리케이션의 이름입니다(KnowBe4 Integration for SecOps).
통합	KnowBe4가 기본값입니다.
활성	기본값은 활성화(선택)입니다. 선택하지 않으면 인스턴스가 활성화되지 않습니다.
설명	통합 인스턴스에 대한 짧은 설명입니다.

4. 제출을 선택합니다.

5. 다음으로 이동 모두 〉 보안 시뮬레이션 및 교육 〉 통합.

6. Knowbe4 통합을 선택합니다.

7. 지금 실행을 선택하여 KnowBe4에서 데이터를 실행하고 수집합니다.

Office 365용 **Microsoft Defender** 통합 구성

Office 365용 Microsoft Defender와의 원활한 통합을 통해 사이버 보안 임원 대시보드 내에서 직접 피싱 시뮬레이션 메트릭에 대한 귀중한 인사이트를 얻을 수 있습니다.

시작하기 전에
필요한 역할: sn_sec_phish_msatk.ms_admin

이 태스크 정보
피싱 공격을 시뮬레이션하고 테넌트를 설정하는 방법에 대한 자세한 내용은 다음을 참조하세요.

- 공격 시뮬레이션 교육으로 피싱 공격 시뮬레이션
- 공격 시뮬레이션 교육 사용 시작하기
- 테넌트 설정

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 **Microsoft Attack** 통합 〉 **Microsoft Attack** 구성.
2. 새로 만들기를 선택합니다.
3. 양식에 상세 정보를 입력합니다.

Microsoft Attack 구성 양식

필드	설명
통합 인스턴스	통합 인스턴스의 이름입니다. 조회 아이콘을 사용하여 통합 인스턴스를 선택합니다.
테넌트 ID	Microsoft Azure 포털에서 생성된 애플리케이션의 테넌트 ID입니다.
클라이언트 ID	Microsoft Azure 포털에서 생성된 애플리케이션의 클라이언트 ID입니다.
클라이언트 비밀	Microsoft Azure 포털에서 작성된 애플리케이션의 클라이언트 비밀입니다.
책갈피	시뮬레이션을 가져와야 하는 날짜입니다.
토큰 URL	Microsoft 시뮬레이션 API에 액세스하기 위해 토큰이 만들어지는 기본 URL입니다.
모든 시뮬레이션 URL	Microsoft 시뮬레이션 API의 기본 URL입니다.

a. 사용할 수 있는 통합 인스턴스가 없는 경우 새로 만들기를 선택합니다.

b. 양식에 상세 정보를 입력합니다.

통합 인스턴스 양식

필드	설명
이름	통합 인스턴스의 이름입니다.
애플리케이션	애플리케이션의 이름입니다(Office 365용 Microsoft Defender).
통합	외부 공급업체 통합 참조(Microsoft Attack 통합)입니다.
활성	기본값은 활성화(선택)입니다. 선택하지 않으면 인스턴스가 활성화되지 않습니다.
설명	통합 인스턴스에 대한 짧은 설명입니다.

4. 제출을 선택합니다.
5. 다음으로 이동 모두 〉 보안 시뮬레이션 및 교육 〉 통합.
6. Microsoft Attack 통합을 선택합니다.
7. 지금 실행을 선택하여 Microsoft에서 데이터를 실행하고 수집합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

용 위험 및 준수 대시보드 GRC: 메트릭

위험 및 준수 대시보드는 규정 준수 및 위험 사용자에게 주요 의사 결정에 도움이 되는 단일 대시보드에서 위험 및 규정 준수 정보에 대한 포괄적인 개요를 제공합니다.

통합된 단일 솔루션 사이버 보안 임원 대시보드 에서 위험 및 준수 대시보드로 이동하여 애플리케이션의 위험 및 준수 메트릭을 거버넌스, 리스크 및 컴플라이언스 볼 수 있습니다.

대시보드는 다음과 같은 기능을 제공합니다.

- 준수 개요
- 위험 개요
- 개인정보 개요
- 비즈니스 연속성 개요
- 외부 공급업체 위험
- 감사 개요

위험 및 준수 대시보드에 액세스하기 위한 필수 구성요소

중요사항:
위험 및 준수 대시보드에 액세스할 수 있는 사이버 보안 및 위험 기능 플러그인을 활성화하려면 에 사이버 보안 임원 대시보드 대한 기본 액세스 권한이 있어야 합니다.

사이버 보안 및 위험 관련 데이터를 분리하기 위해 새로운 기능 도메인이 도입되었습니다. UI 작업 활성화 버튼을 선택하여 사이버 보안 및 위험 플러그인을 활성화할 수 있습니다. 기본적으로 이 기능 도메인은 비활성 상태입니다.

필요한 ServiceNow AI Platform 역할

기본 GRC 사용자 역할은 위험 및 준수 대시보드에서 보고서를 볼 수 있는 sn_grc_dashboards.grc_ciso_user입니다. 이 역할에는 다음이 포함됩니다.

- sn_compliance.reader
- sn_risk.reader

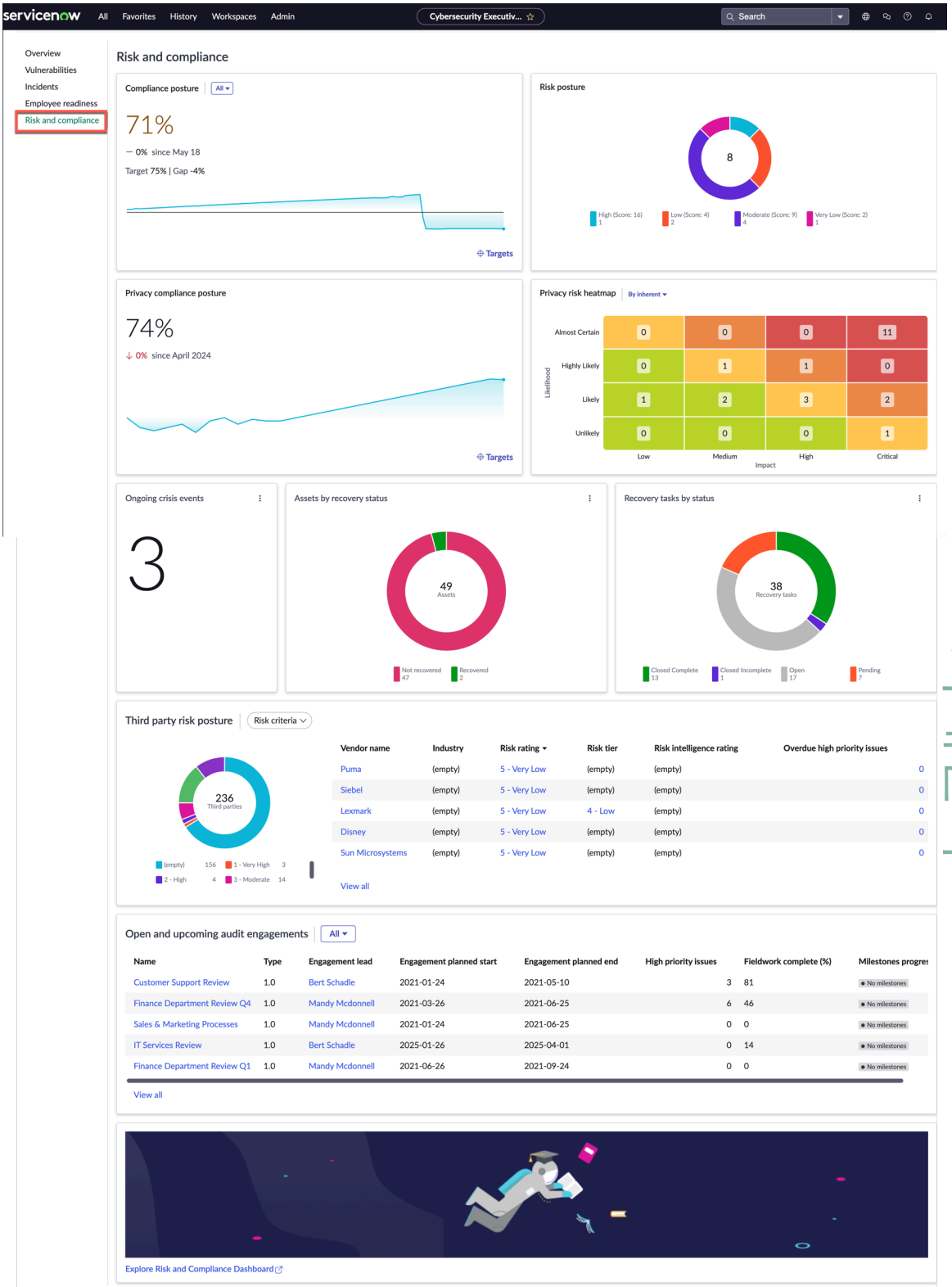
주:
그러나 사이버 보안 임원 대시보드에 로그인하고 보고 공유하려면 sn_bod.ciso 역할이 있어야 하며, 여기에서 위험 및 준수 대시보드로 이동할 수 있습니다.

위험 및 준수 대시보드에 액세스

1. 위험 및 준수 대시보드에 액세스하려면 다음으로 이동합니다. 모두 〉 사이버 보안 임원 대시보드 〉 사이버 보안 임원 대시보드.
2. 대시보드 왼쪽의 목록에서 위험 및 규정 준수 레이블을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

위험 및 규정 준수 메트릭을 위한 통합 사이버 보안 임원 대시보드



3. 데이터를 시각화하고 사용자를 위해 설계된 대시보드에서 사용할 수 있는 보고서와 솔루션을 보려면 위험 및 준수 대시보드 탐색 레이블을 선택합니다.

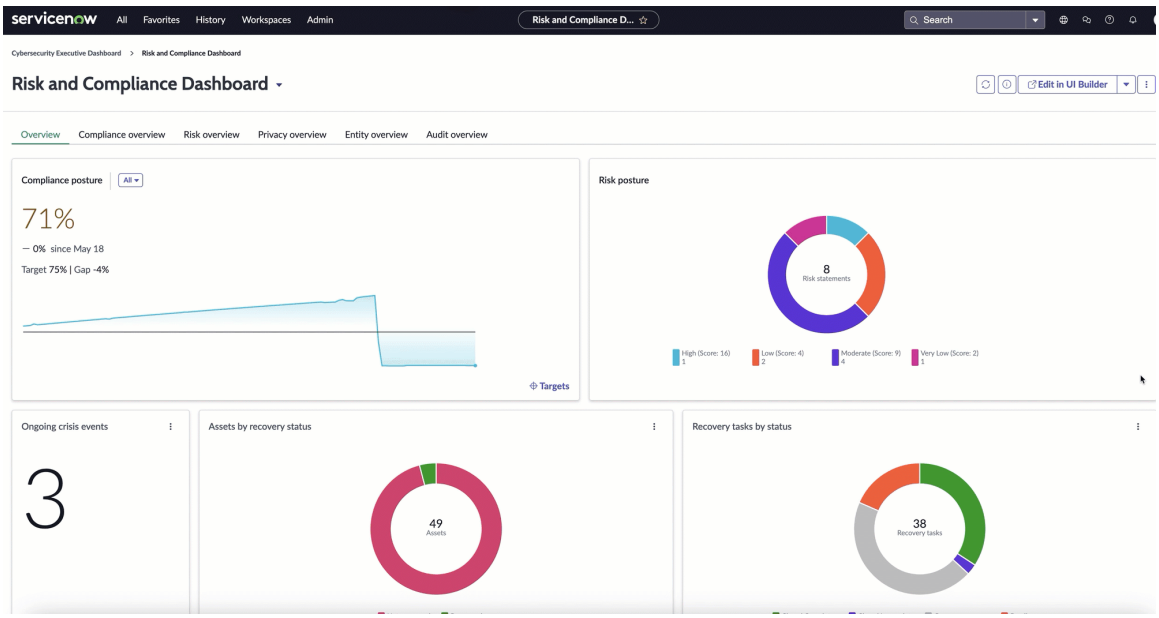
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

위험 및 준수 대시보드 보고서 및 솔루션

위험 및 준수 대시보드는 최고 정보 보안 책임자가 조직의 규정 준수 및 위험 태세를 이해할 수 있도록 주요 GRC 애플리케이션에서 사용할 수 있는 보고서의 포괄적인 분석 데이터를 제공하는 통합 대시보드입니다. 대시보드는 애플리케이션 제품군 내의 다양한 제품에서 ServiceNow GRC 얻은 데이터를 통합합니다.

주:
모든 보고서는 해당 작업 공간이 설치된 경우에만 사용할 수 있습니다.

위험 및 준수 대시보드



필요한 **ServiceNow AI Platform** 역할

준수 관련 보고서용

사용자에게 sn_grc_dashboards.grc_ciso_user 역할과 sn_bod.ciso 역할이 있어야 합니다.

위험 관련 보고서의 경우

사용자에게 sn_grc_dashboards.grc_ciso_user 역할과 sn_bod.ciso 역할이 있어야 합니다.

비즈니스 연속성 관리 관련 보고서

사용자에게 sn_bcm.viewer 역할과 sn_bod.ciso 역할이 있어야 합니다.

외부 공급업체 위험 관련 보고서의 경우

사용자에게 sn_vdr_risk_asmt.vendor_assessment_reviewer 역할과 sn_bod.ciso 역할이 있어야 합니다.

개인정보 보호 관련 보고서의 경우

사용자에게 sn_privacy.analyst 역할과 sn_bod.ciso 역할이 있어야 합니다.

감사 관련 보고서의 경우

사용자에게 sn_audit_ws.auditor 역할과 sn_bod.ciso 역할이 있어야 합니다.

위험 및 준수 대시보드에 액세스

대시보드를 열려면 다음으로 이동합니다. 모두 〉 사이버 보안 임원 대시보드 〉 사이버 보안 임원 대시보드.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

표시기

규정 준수 태세

- 규정 준수 백분율: 규정 준수 태세를 나타내는 수식 표시기입니다.
- 모든 통제: 수식 표시기를 지원하는 자동 표시기입니다.
- 규정 준수 통제: 수식 표시기를 지원하는 자동 표시기입니다.

개인정보 보호 규정 준수 태세

PA 표시기: 처리 활동 준수 점수 백분율.

세부 항목

기능 도메인입니다.

보고서

주:
모든 보고서는 해당 작업 공간이 설치된 경우에만 사용할 수 있습니다.

개요 탭

직위	유형	소스 테이블	설명
규정 준수 태세	라인 차트	통제 〔sn_compliance_control〕	규정 준수 관리자에게 사이버 보안 및 위험, 데이터 분석을 기반으로 IT 위험 및 규정 준수 태세를 제공합니다.
위험 태세	도넛형 차트	소스 테이블은 다음과 같습니다. • 위험 [sn_risk_risk] • 상세한 집계 위험 [sn_risk_advanced_risk_assessment_result] (애플리케이션이 설치되고 고급 위험 평가가 활성화된 경우 고급 위험)	위험 등급에 따라 위험 수를 제공합니다.
진행 중인 위기 이벤트	단일 점수	이벤트 유형이 실제인 복구 이벤트 〔sn_recovery_event〕	승인되거나 종결되지 않은 진행 중인 위기 이벤트의 총 수를 표시합니다.
복구 상태별 자산	도넛형 차트	자산 〔sn_recovery_event_asset〕	복구된 자산과 복구되지 않은 자산을 포함하여 진행 중인 위기 이벤트의 총 자산 수를 복구 상태별로 그룹화하여 제공합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

개요 탭

직위	유형	소스 테이블	설명
상태별 복구 작업	도넛형 차트	복구 작업 [sn_recovery_event_task]	진행 중인 위기 이벤트에 대한 다양한 상태의 복구 작업 상태를 제공합니다.

준수 개요 탭

직위	유형	소스 테이블	설명
권한 문서	도넛형 차트	권한 문서 [sn_compliance_authority_document]	차트에서 준수 및 미준수 권한 문서의 데이터를 제공합니다. 이 목록은 권한 문서에 대한 상세 정보, 개별 준수 점수(백분율), 권한 문서에 대한 우선 순위가 높은 문제 및 높은 위험 예외의 수, 준수 케이스의 수를 제공합니다.
정책	도넛형 차트	정책 [sn_compliance_policy]	차트의 규정 준수 및 미준수 정책 수를 제공합니다. 이 목록에는 정책의 상세 정보, 개별 준수 점수(백분율), 각 정책에서 제기된 우선 순위가 높은 문제 및 위험 예외 수, 규정 준수 케이스 수가 나와 있습니다.

위험 개요 탭

직위	유형	소스 테이블	설명
위험 태세	도넛형 차트	소스 테이블은 다음과 같습니다. • 위험 [sn_risk_risk] • 상세한 집계 위험 [sn_risk_advanced_risk_assessment_result] (애플리케이션이 설치되고 고급 위험 평가가 활성화된 경우 고급 위험)	위험 등급에 따라 위험 수를 제공합니다.
위험 태세	목록	GRC 컨텐츠 상태 [sn_grc_content_reports]	전반적인 위험 평가 결과를 이해하기 위해 각 조직 위험에 대한 위험 등급을 제공합니다. 이러한

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

위험 개요 탭

직위	유형	소스 테이블	설명
			등급을 통해 조직은 다양한 위험의 잠재적 영향과 가능성을 이해하고 이러한 위험의 우선순위를 지정하고 관리할 수 있습니다. 위험 태세 카드는 각 위험에 대해 다음 정보도 강조 표시합니다. • 위험 선호도: 정의된 위험 선호도 값입니다. • 높은 우선순위 문제: 우선순위가 높은 문제 수는 높음으로 정의됩니다. • 지연된 위험 응답 작업: 지연된 위험 응답 작업의 수입니다. • **KRI** 위반 **%**: 사전 정의된 임계치 또는 한도를 초과한 핵심 위험 표시기(KRI)의 백분율입니다.
외부 공급업체 위험 태세	도넛형 차트	외부 공급업체 위험 [sn_grc_dashboards_third_party_risk]	각 외부 공급업체에 대한 위험 등급을 제공합니다. 위험 등급은 외부 공급업체 또는 벤더를 위해 수행된 모든 평가의 점수와 등급을 고려한 전반적인 평가 등급입니다. 타사 위험 태세 카드는 각 외부 공급업체 또는 벤더에 대한 다음 정보도 강조 표시합니다. • 위험 기준: 특정 유형의 외부 공급업체에 적용되는 위험 도메인(다른 플랫폼 기능에서 위험 영역이라고도 함)의 그룹입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

위험 개요 탭

직위	유형	소스 테이블	설명
			• 위험 계층: 고유 위험 평가(IRQ)가 완료된 후 수집된 응답을 기반으로 결정되는 값입니다. • 위험 인텔리전스 등급: 위험 인텔리전스 제공자로부터 수집된 모든 점수의 집계입니다. • 지연된 위험 응답 작업: 지연된 위험 응답 작업의 수입니다.

개인정보 개요 탭

직위	유형	소스 테이블	설명
개인정보 보호 규정 준수 태세	선형	PA 표시기: 처리 활동 준수 점수 백분율 [pa_indicators]	월별 규정 준수 태세를 제공하고 모든 처리 활동의 전체 준수 점수를 참조하여 표시됩니다.
지연된 우선순위 높은 문제	단일 점수	문제 [sn_grc_issue]	기한이 지난 우선순위가 높은 모든 개인정보 보호 관련 문제에 대한 집중적인 개요를 제공하여 중요한 작업을 신속하게 식별하고 해결하여 규정 준수 및 데이터 보호를 보장합니다.
개인정보 위험 히트맵	히트맵	위험 평가 방법론 [sn_risk_advanced_risk_assessment_methodology]	개인정보 위험 평가 데이터를 히트맵 형태로 제공합니다. 개인정보 위험 평가는 중요도 점수가 높은 경우 수행되는 상세한 평가입니다. 처리 활동과 관련된 각 위험을 평가하고 처리 활동에 대해 집계된 위험 점수를 파악합니다. 개인정보 보호 위험을 평가한 후에는 위험

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

개인정보 개요 탭

직위	유형	소스 테이블	설명
			히트맵에서 개인정보 위험 태세를 볼 수 있습니다.

엔터티 개요 탭

직위	유형	소스 테이블	설명
엔터티	목록	엔터티 준수 상태 (sn_compliance_entities_reports)	엔터티의 전체 위험 등급에 기여하는 엔터티와 직접 연결된 위험 요약을 제공합니다. 또한 이 목록에는 엔터티의 규정 준수 점수와 엔터티와 연결된 미준수 통제의 결과로 발생하는 높은 우선순위의 문제 및 위험 예외가 표시됩니다.

감사 개요 탭

직위	유형	소스 테이블	설명
미해결 및 예정된 감사 참여	목록	참여 (sn_audit_engagement)	미해결 및 예정된 감사 계약 목록을 제공합니다. 이 목록은 또한 각 권한 문서에 대한 계약 리드, 각 계약의 계획된 시작 및 종료 날짜, 우선 순위가 높은 문제, 완료된 필드 작업의 백분율 및 진행 중인 마일스톤에 대한 세부 정보를 제공합니다.

필터

이름	유형	설명
위험 기준	보고서	선택한 위험 기준에 따라 도넛형 차트와 목록에 해당 위험 영역에 있는 외부 공급업체 또는 벤더가 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

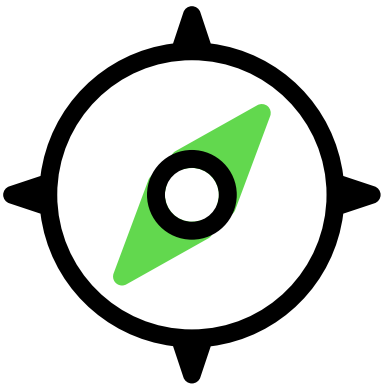
위협 인텔리전스 보안 센터

(위협 인텔리전스 보안 센터TISC) 플랫폼은 위협 인텔리전스의 집계, 관리 및 운영화를 위한 기술 솔루션을 제공합니다.

시작하기

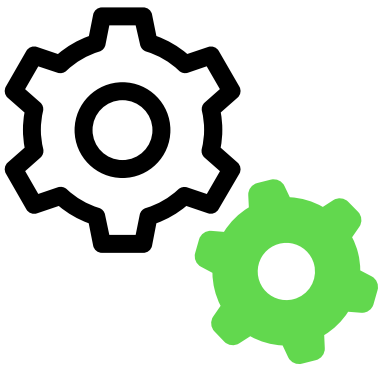
시작하려면 타일을 클릭합니다.

탐색



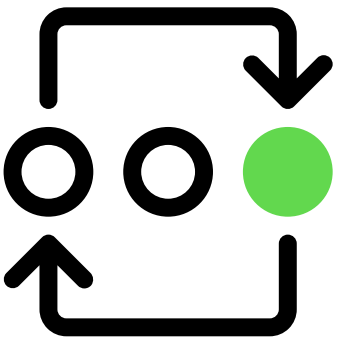
위협 인텔리전스 보안 센터가 주요 기능과 이점을 어떻게 도울 수 있는지 알아보십시오.

구성



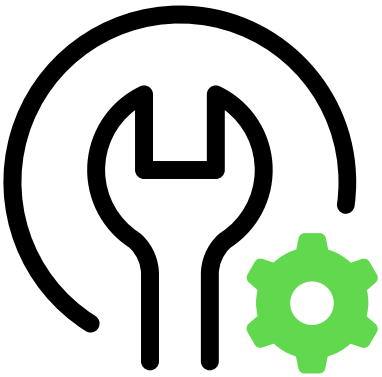
특정 요구 사항에 맞게 Threat Intelligence Security Center를 설정하고 구성합니다.

통합



위협 인텔리전스 보안 센터와 통합

관리자



위협 인텔리전스 보안 센터를 관리하고 사용자 지정합니다.

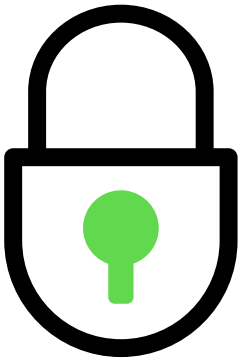
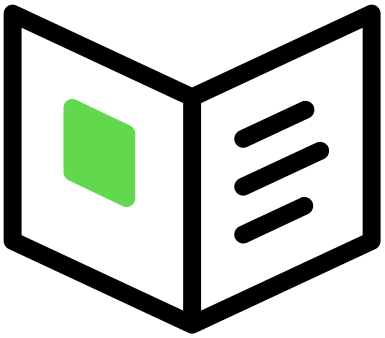
사용

위협 인텔리전스 보안 센터 라이브러리 및 개체를 관리합니다.

보고서 템플릿

케이스 관리 보고서를 관리하고 사용자 지정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

MITRE ATT&CK 리포지토리	TISC 데이터 보관 보관	참조
		
MITRE ATT&CK 리포지토리 데이터를 관리합니다.	관리, 데이터 보관 및 삭제 규칙입니다.	위협 인텔리전스 보안 센터에 대한 추가 정보를 얻으십시오.

스토어에서 앱 요청

ServiceNow Store 웹 사이트를 방문하면 사용 가능한 모든 앱을 확인하고 스토어에 요청을 제출하는 방법에 대한 정보를 참조할 수 있습니다. 출시된 모든 앱의 누적 릴리스 정보는 ServiceNow Store 버전 기록 릴리스 정보를 참조하십시오.

(sn_sec_tisc)를 설치하면 위협 인텔리전스 보안 센터 의 모든 종속 애플리케이션이 ServiceNow Store자동으로 설치됩니다.

기타 자원

보안 인시던트 응답 의 ServiceNow 커뮤니티포럼을 방문하십시오.

문제 해결 및 도움 받기

- 알려진 오류 포털에서 알려진 오류 문서 검색
- 연락처 고객 서비스 및 지원

위협 인텔리전스 보안 센터 탐색

위협 인텔리전스 보안 센터 (TISC)를 사용하면 위협 인텔리전스 팀과 공동 작업할 수 있으며 다양한 위협 인텔리전스 피드를 수집 및 처리할 수 있는 여러 기능과 필요한 정보를 분석, 공동 작업, 조치 및 공유할 수 있는 작업 공간이 있습니다.

애플리케이션에 대한 위협 인텔리전스 보안 센터 개요를 확인합니다.

https://player.vimeo.com/video/1020328039?h=33e58d6e14&badge=0&autopause=0&player_id=0&app_id=58479

Threat Intelligence Security Center는 데이터 수집, 중복 제거, 정규화 및 집계와 같은 데이터 처리, 위협 인텔리전스 분석, 위협 인텔리전스 보급 및 관리 작업을 제공하는 작업 공간을 관리하는 기능으로 향상되었습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주요 기능

위협 인텔리전스 보안 센터 는 보안 팀의 위협 인텔리전스 역량을 향상하도록 설계된 포괄적이고 강력한 기능 제품군을 제공합니다.

- 선별된 **OSINT** 위협 피드 카탈로그: 널리 사용되는 다양한 오픈 소스 위협 인텔리전스 피드에 대한 액세스를 제공하여 광범위한 적용 범위를 보장합니다.
- 프리미엄 피드 통합: OSINT 데이터와 함께 프리미엄 소스를 통합하여 위협 인텔리전스 품질을 향상시킵니다.
- 자동화된 옵저버블 추출: 업로드된 파일에서 모든 관련 옵저버블을 자동으로 식별하고 추출하여 데이터 수집을 간소화합니다.
- 다양한 데이터 집계: STIX, MISP, JSON 등을 포함한 여러 데이터 형식을 지원하여 원활한 피드 통합을 가능하게 합니다.
- 보강 및 확인: 긍정 오류를 제거하고, 신뢰 점수를 할당하고, 표시기를 확인하고, 귀중한 상황별 정보를 추가하여 데이터 품질을 개선합니다.
- 상관 관계 규칙 엔진: 옵저버블 간의 관계를 자동으로 설정하여 위협 패턴에 대한 심층적인 인사이트를 제공합니다.
- 사용자 지정 가능한 위협 점수 매기기: 보다 미묘하고 정확한 위협 평가를 위해 위협 점수를 미세 조정할 수 있습니다.
- 내부 인텔리전스 통합: 외부 피드를 취약성 보고서(VR), 보안 인시던트 응답(SIR), 자산, 서비스 및 CMDB의 내부 데이터와 결합합니다.
- 사용자별 대시보드: 위협 인텔리전스 가상 사용자에 따라 시각화 및 데이터 보기를 조정하여 사용자 경험과 관련성을 개선합니다.
- 그래픽 시각화 도구: 직관적인 그래픽 표현을 통해 복잡한 위협 인텔리전스 데이터를 쉽게 이해할 수 있습니다.
- 전담 분석가 작업 공간: 위협 인텔리전스 분석가가 최소한의 방해로 조사 및 분석에 집중할 수 있도록 간소화된 위협 인텔리전스 전용 분석가 작업 공간을 제공합니다.
- 케이스 관리를 통한 위협 헌팅: 작업 추적 및 케이스 처리를 통해 조사 워크플로우를 지원합니다.
- **MITRE ATT&CK** 통합: 향상된 상황별 분석을 위해 사용자가 케이스 기록을 MITRE ATT&CK 프레임워크 데이터와 연결할 수 있습니다.
- 원활한 **SIR** 통합: 와 보안 인시던트 응답 애플리케이션 간의 위협 인텔리전스 원활한 데이터 마이그레이션과 상호 위협 인텔리전스 보안 센터운용성을 보장합니다.
- 알림 및 경보 규칙: 진화하는 위협 인텔리전스를 기반으로 팀에 알리는 트리거 경보를 설정합니다.
- 데이터 보존 및 정리 정책: 조직에서 데이터 관리 규칙을 정의하여 애플리케이션 성능과 규정 준수를 유지할 수 있습니다.
- **Reporting & Collaboration**: 서식 있는 텍스트 편집기와 사용자 지정 가능한 템플릿을 사용하여 포괄적인 상태 보고서 및 조사 요약을 생성합니다.
- MSSP용 도메인 분리: 멀티 테넌트 환경을 지원하여 MSSP(관리형 보안 서비스 제공자)가 고객 데이터를 안전하게 분리할 수 있도록 합니다.
- 광범위한 **API** 통합: 다른 보안 도구 및 플랫폼과의 원활한 연결을 위해 TISC API를 제공합니다.

TISC 주요 용어

아래에 정의된 용어는 TISC(위협 인텔리전스 보안 센터) 전체에서 사용됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

용어 정의

용어	정의
데이터 처리	위협 인텔리전스 플랫폼(TIP)은 다양한 소스와 패턴에서 위협 인텔리전스 데이터를 수집, 집계 및 구성하는 기술 솔루션입니다. 위협 인텔리전스는 위협 행위자의 대상 및 공격 행동을 이해하기 위해 수집, 처리 및 분석되는 데이터입니다.
옵저버블	옵저버블은 컴퓨터 및 네트워크 작동과 관련된 상태 저장 속성(예: 파일의 MD5 해시 또는 레지스트리 키 값) 또는 측정 가능한 이벤트(예: 레지스트리 키 만들기 또는 파일 삭제)를 나타냅니다. 자세한 내용은 옵저버블 문서를 참조하십시오.
표시기	표시기에는 의심스럽거나 악의적인 사이버 활동을 탐지하는 데 사용할 수 있는 패턴이 포함되어 있습니다. 예를 들어 표시기를 사용하여 악성 도메인 집합을 나타내고 STIX 패턴 언어를 사용하여 이러한 도메인을 지정할 수 있습니다. 표시기 SDO에는 간단한 텍스트 설명, 동작을 감지하는 킬 체인 단계, 표시기가 유효하거나 유용한 시간 창, 구조화된 탐지 패턴을 캡처하는 데 필요한 패턴 속성이 포함되어 있습니다. 자세한 내용은 표시기 문서를 참조하십시오.
객체	STIX 도메인 객체(SDO) 집합을 정의하며, 각 개체는 일반적으로 CTI(사이버 위협 인텔리전스)에 표시되는 고유한 개념에 해당합니다. SDO 및 STIX 관계 객체(SRO)를 빌딩 블록으로 사용하여 개인은 광범위하고 포괄적인 사이버 위협 인텔리전스를 만들고 공유할 수 있습니다. 자세한 내용은 TISC 라이브러리 리포지토리 문서를 참조하십시오.
관계	관계는 두 옵저버블 또는 두 개의 SDO 또는 옵저버블과 SDO 간의 링크로, 오브젝트가 관련되는 방식을 설명합니다. 관계는 외부 STIX 관계 객체(SRO)를 사용하거나 경우에 따라 포함된 관계를 구성하는 식별자 참조를 저장하는 특정 속성을 통해 나타낼 수 있습니다. 자세한 내용은 관계 객체 문서를 참조하십시오.

홈페이지 보기 **TISC**

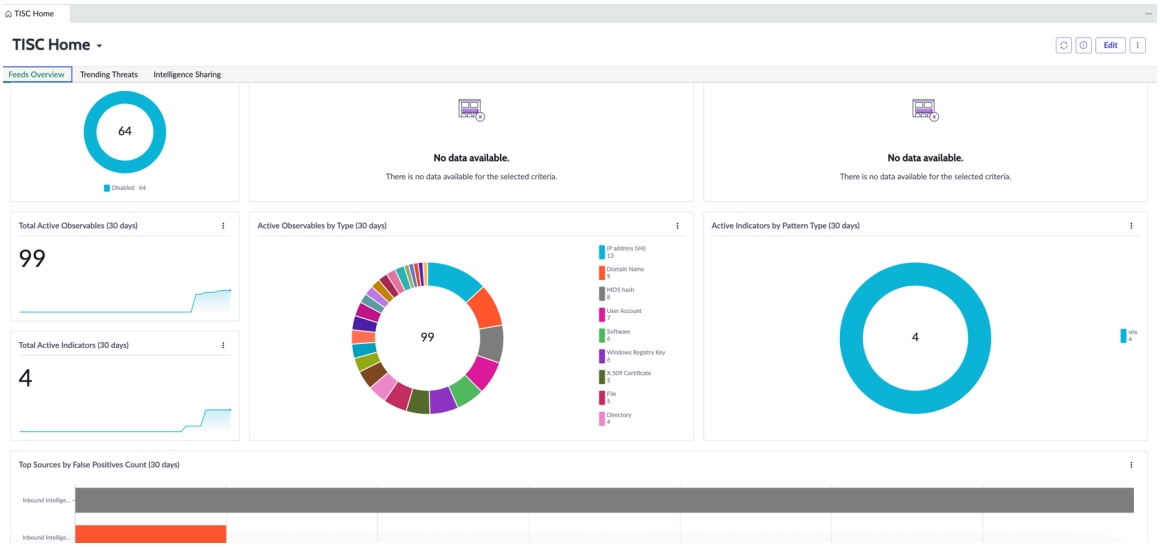
TISC 방문 페이지인 홈페이지를 사용하여 위협 인텔리전스 관련 데이터를 시각화합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 작업 공간 〉 위협 인텔리전스 보안 센터.
홈페이지가 TISC 표시됩니다.



2. TISC 다른 위젯 데이터로 홈페이지를 봅니다.
홈페이지 뷰는 피드 개요, 추세 위협 및 인텔리전스 공유의 세 가지 탭으로 구성됩니다. 홈페이지의 컨텐츠는 옵저버블, 표시기 및 데이터 피드와 같은 다양한 소스에서 가져옵니다.

a. 피드 개요: 이 탭은 데이터가 수집되는 다양한 소스와 데이터 수집을 위해 구성된 소스에 대한 개략적인 개요를 제공합니다.

피드 개요

위젯 이름	설명	작업
소스 수	시스템에서 초안, 활성화, 비활성화 등의 상태별로 소스 개수를 표시합니다.	이 위젯을 클릭하면 필터링된 기록이 있는 목록 페이지가 열립니다.
소스 유형별 활성 소스	소스 유형별로 활성 소스의 분포를 표시합니다.	이 위젯을 클릭하면 필터링된 기록이 있는 목록 페이지가 열립니다.
피드 형식별 활성 소스	피드 유형별로 활성화된 소스 수를 표시합니다.	이 위젯을 클릭하면 필터링된 기록이 있는 목록 페이지가 열립니다.
총 활성 옵저버블(30일)	지난 30일 동안 생성된 인텔리전스 기록의 볼륨별 상위 10개 소스를 표시합니다.	이 위젯을 클릭하면 선택한 필터에 대한 위젯의 KPI 세부 정보 페이지가 새 탭에서 열립니다.
유형별 활성 옵저버블	지난 30일 동안 생성된 옵저버블 집계의 상위 총 볼륨을 표시합니다.	이 위젯을 클릭하면 선택한 필터에 대한 위젯의 KPI 세부 정보 페이지가 새 탭에서 열립니다.
패턴 유형별 활성 표시기	지난 30일 동안 생성된 패턴 유형별 표시기 집계의 총 볼륨을 표시합니다.	이 위젯을 클릭하면 선택한 필터에 대한 위젯의 KPI 세부

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

위젯 이름	설명	작업
		정보 페이지가 새 탭에서 열립니다.
총 활성 표시기(30일)	지난 30일 동안 생성된 표시기 집계의 총 볼륨을 표시합니다.	이 위젯을 클릭하면 선택한 필터에 대한 위젯의 KPI 세부 정보 페이지가 새 탭에서 열립니다.
긍정 오류 갯수별 상위 소스(30일)	지난 30일 동안 생성된 긍정 오류 옵저버블의 총 볼륨 기준을 표시합니다.	이 위젯을 클릭하면 필터링된 기록이 있는 목록 페이지가 열립니다.

b. 추세 위협: 이 탭은 추세 위협에 대한 개략적인 개요를 제공합니다.

추세 위협

위젯 이름	설명	작업
최신 보고서(상위 10개)	보고서 및 링크 목록을 표시합니다 - 게시된 날짜별 상위 10개 순서입니다.	이 위젯을 클릭하면 필터링된 기록이 있는 목록 페이지가 열립니다.
최신 RSS 피드(상위 10개)	RSS 피드 및 링크 목록을 표시합니다(게시된 날짜별 상위 10개 순서).	이 위젯을 클릭하면 필터링된 기록이 있는 목록 페이지가 열립니다.
위협 점수 범위별 활성 옵저버블(30일)	위협 점수 범위별로 분포된, 지난 30일 동안 생성된 옵저버블 수를 표시합니다.	이 위젯을 클릭하면 선택한 필터에 대한 위젯의 KPI 세부 정보 페이지가 새 탭에서 열립니다.
평판별 활성 옵저버블(30일)	평판에 따라 분포된 지난 30일 동안 생성된 옵저버블 개수를 표시합니다.	이 위젯을 클릭하면 선택한 필터에 대한 위젯의 KPI 세부 정보 페이지가 새 탭에서 열립니다.
상위 태그(30일)	사용 빈도를 기준으로 지난 30일 동안 생성된 기록의 상위 태그를 표시합니다.	이 위젯을 클릭하면 선택한 필터에 대한 위젯의 KPI 세부 정보 페이지가 새 탭에서 열립니다.
가장 많이 대상이 된 섹터(30일)	지난 30일 동안 생성된 활동 중 보고된 활동별로 순위가 매겨진 상위 10개 섹터를 표시합니다.	이 위젯을 클릭하면 선택한 필터에 대한 위젯의 KPI 세부 정보 페이지가 새 탭에서 열립니다.

c. 인텔리전스 공유: 이 탭은 인텔리전스 공유에 대한 높은 수준의 개요를 제공합니다.

인텔리전스 공유

위젯 이름	설명	작업
인바운드 인텔리전스 - 기록 카운트(30일)	지난 30일 동안 받은 인바운드 인텔 기록 수를 유형(옵저버블, 객체, 표시기)별로 분류하여 표시합니다.	이 위젯을 클릭하면 필터링된 기록이 있는 목록 페이지가 열립니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

위젯 이름	설명	작업
아웃바운드 인텔리전스 - 기록 카운트(30일)	지난 30일 동안 공유된 아웃바운드 인텔 기록 수를 유형(옵저버블, 객체, 표시기)별로 분류하여 표시합니다.	이 위젯을 클릭하면 필터링된 기록이 있는 목록 페이지가 열립니다.
인바운드 인텔 - 상태별 배포(30일)	지난 30일 동안의 상태별 인바운드 인텔리전스 기록 분포를 표시합니다.	이 위젯을 클릭하면 필터링된 기록이 있는 목록 페이지가 열립니다.
아웃바운드 인텔 - 상태별 배포(30일)	지난 30일 동안의 상태별 아웃바운드 인텔리전스 기록 분포를 표시합니다.	이 위젯을 클릭하면 필터링된 기록이 있는 목록 페이지가 열립니다.
인바운드 인텔리전스 - 상위 공유 프로필(30일)	지난 30일 동안 받은 인바운드 정보를 기반으로 상위 프로필을 표시합니다.	이 위젯을 클릭하면 필터링된 기록이 있는 목록 페이지가 열립니다.
아웃바운드 인텔리전스 - 상위 공유 프로필(30일)	지난 30일 동안 공유된 아웃바운드 정보를 기반으로 상위 프로필을 표시합니다.	이 위젯을 클릭하면 필터링된 기록이 있는 목록 페이지가 열립니다.
인바운드 인텔리전스 - 가장 많이 공유된 유형(30일)	지난 30일 동안 가장 자주 받은 인텔 유형(객체, 표시기, 옵저버블)을 표시합니다.	이 위젯을 클릭하면 필터링된 기록이 있는 목록 페이지가 열립니다.
아웃바운드 인텔리전스 - 최대 공유 유형(30일)	지난 30일 동안 가장 자주 공유된 인텔 유형(객체, 표시기, 옵저버블)을 표시합니다.	이 위젯을 클릭하면 필터링된 기록이 있는 목록 페이지가 열립니다.
인바운드 인텔 - 형식별 배포(30일)	지난 30일 동안 인바운드 인텔리전스의 형식 분포(예: MISP, STIX)를 표시합니다.	이 위젯을 클릭하면 필터링된 기록이 있는 목록 페이지가 열립니다.
아웃바운드 인텔 - 형식별 배포(30일)	지난 30일 동안 아웃바운드 인텔리전스의 형식 분포(예: MISP, STIX)를 표시합니다.	이 위젯을 클릭하면 필터링된 기록이 있는 목록 페이지가 열립니다.

위협 인텔리전스 보안 센터 구성

고객에게 서비스와 지원을 제공하는 데 필요한 기능, 구성요소 및 통합을 설정합니다.

ServiceNow Store에서 **TISC** 애플리케이션 다운로드

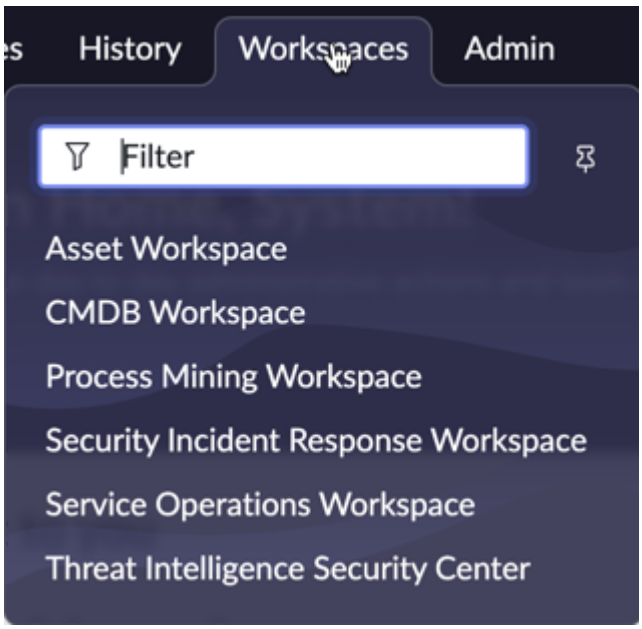
인스턴스에서 애플리케이션을 실행하려면 위협 인텔리전스 보안 센터 먼저 에서 ServiceNow# Store 다운로드하여 설치해야 합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음에 대한 지침을 따릅니다. 에서 애플리케이션 다운로드 ServiceNow Store 위협 인텔리전스 보안 센터 보안 운영 애플리케이션을 설치합니다.
2. 설치가 완료되면 다음으로 이동하여 작업 공간을 위협 인텔리전스 보안 센터 열 수 있습니다. 작업 공간 〉 ## ##### ## ##



다음에 수행할 작업
애플리케이션을 성공적으로 다운로드한 후 원활한 통합을 위해 이 섹션에 위협 인텔리전스 보안 센터 설정 언급된 모든 작업을 완료했는지 확인합니다.

위협 인텔리전스 보안 센터 설정

를 위협 인텔리전스 보안 센터사용하려면 먼저 스토어에서 다운로드 ServiceNow 해야 합니다.

설치되는 역할

다음 정보를 검토하고 원활한 통합을 위한 모든 작업을 완료했는지 확인합니다. 다음은 애플리케이션에 액세스하고 작업하도록 정의된 다양한 가상 사용자 목록입니다.

- 위협 인텔리전스 분석가(sn_sec_tisc.analyst)
- Threat Intelligence 관리자(sn_sec_tisc.admin)

TISC 역할에 적용할 수 있는 권리

설정	설명
필수 ServiceNow AI Platform 역할과 Threat Intelligence Security Center 역할을 할당하고 확인합니다.	예상 결과를 구성하고 검증하려면 다음 역할이 필요합니다. • 관리자는 스토어에서 TISC 애플리케이션을 ServiceNow 설치하고 sn_sec_tisc.admin으로 역할을 할당해야 합니다. • 이 sn_sec_tisc.admin 역할은 다음 작업을 수행합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

TISC 역할에 적용할 수 있는 권리

설정	설명
	○ 데이터를 수집하도록 데이터 소스를 구성합니다. 자세한 내용은 Threat Intelligence 피드 문서를 참조하십시오. ○ TISC에서 옵저버블 데이터를 보강하는 데 필요한 통합을 구성했습니다. 자세한 내용은 TISC 보강 통합 문서를 참조하십시오. ○ 임포트 도우미를 사용하여 데이터를 임포트하기 위한 데이터 임포트 승인 역할을 구성합니다. 자세한 내용은 데이터 임포트 작업 문서를 참조하십시오. ○ 옵저버블의 위협 점수를 자동으로 계산하는 데 필요한 기준을 사용하여 위협 점수 계산기를 구성합니다. 자세한 내용은 위협 점수 계산기 정의 문서를 참조하십시오. ○ 필요한 분류 및 분류 값을 구성합니다. 자세한 내용은 분류 생성 문서를 참조하십시오. ○ 조직과 관련된 MITRE ATT&CK 리포지토리를 구성합니다. 자세한 내용은 MITRE-ATT&CK 저장소 문서를 참조하십시오. **주:** sn_sec_tisc.admin은 sn_sec_tisc.analyst 역할을 할당할 수도 있습니다. • sn_sec_tisc.analyst 역할은 다음 작업을 수행합니다. ○ 애플리케이션 홈페이지를 사용하여 시스템의 데이터 개요를 봅니다. 자세한 내용은 홈페이지 보기 TISC 문서를 참조하십시오. ○ 위협 라이브러리 페이지의 인텔리전스 임포트 버튼을 사용하여 시스템에 데이터를 임포트합니다. 자세한 내용은 위협 인텔리전스 보안 센터 도서관 문서를 참조하십시오. ○ ▪ 위협 라이브러리 페이지에 제공된 검색을 사용하여 애플리케이션에 있는 데이터를 검색합니다. ▪ 위협 라이브러리의 다양한 소스에서 수집된 데이터를 관리합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

TISC 역할에 적용할 수 있는 권리

설정	설명
	▪ 옵저버블에 대해 다양한 보강 작업을 수행합니다. ▪ 케이스를 작성하고 관리합니다. 자세한 내용은 위협 분석가 워크벤치를 사용하여 케이스 생성 문서를 참조하십시오.

의존성 플러그인

플러그인	설명
이 애플리케이션을 설치하려면 다음 애플리케이션이 필요합니다. • 보안 케이스 관리 공통 작업 공간 구성요소 [com.snc.escm.ws_commons] • 위협 인텔리전스 지원 공통 [com.snc.threat] • 열 수준 암호화(com.glide.encryption) • 대형 JSON 및 XML 페이로드 작성기 API(com.glide.streaming_builder) • 보안 지원 Core(com.snc.security_support.core) • 노드 맵 경험 구성요소(sn_node_map) • 작업 공간에 대한 보고 UI 구성요소 (sn_sec_reporting) • 보안 운영용 서식 있는 텍스트 편집기 구성요소(sn_escm_rte) • 보안 통합 프레임워크(sn_sec_int) • 보안 지원 공통(sn_sec_cmn) • 보안 지원 오케스트레이션 (sn_sec_cmn_orch)	ServiceNow 이 통합을 구성하기 전에 통합을 지원하는 데 필요한 핵심 애플리케이션이 설치되고 활성화되었는지 확인합니다.

통합 위협 인텔리전스 보안 센터

이 섹션을 사용하여 통합을 이해합니다 위협 인텔리전스 보안 센터 .

통합 섹션에는 다음 하위 모듈이 포함되어 있습니다.

통합

모듈 이름	설명
카탈로그	사용 가능한 모든 위협 인텔리전스 피드 및 보강 통합이 여기에 타일/카드로 표시됩니다. 사용자는 이 섹션에서 새 피드 또는 통합을 만들 수 없습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

통합

모듈 이름	설명
위협 피드	이 섹션에는 위협 인텔리전스 피드와 관련된 세부 정보만 포함되어 있으며 사용자는 이 섹션에서 새 위협 인텔리전스 피드를 구성할 수 있습니다.
보강 통합	이 섹션에는 보강 통합과 관련된 세부 정보만 포함되어 있으며 사용자는 이 섹션에서 사용 가능한 보강 통합을 구성할 수 있습니다. 주: 보강 통합 섹션은 하나 이상의 보강 통합 플러그인이 설치된 경우에만 표시됩니다.

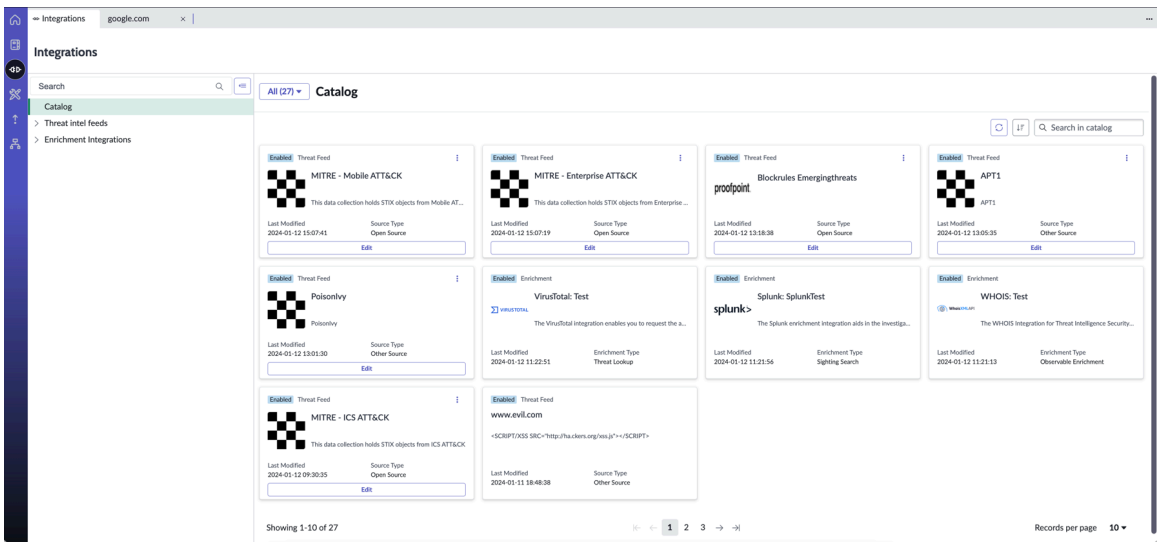
위협 인텔리전스 보안 센터 카탈로그

위협 인텔리전스 보안 센터 카탈로그는 애플리케이션에서 사용할 수 있는 위협 인텔리전스 피드 및 보강 통합의 선별된 목록으로, 필요한 정보를 추가한 후 활성화하고 설정된 빈도로 위협 인텔리전스 데이터를 자동으로 수집하도록 피드를 예약할 수 있습니다.

sn_sec_tisc.admin은 기존 소스 구성을 검색 및 편집하고, 카탈로그에서 구성을 활성화 또는 비활성화하고, 삭제할 수도 있습니다. 새 데이터 소스가 카탈로그에 추가되어 카탈로그에 새 구성 카드로 나타납니다.

필요한 역할:

- sn_sec_tisc.admin(만들기/업데이트)
- sn_sec_tisc.analyst(읽기)



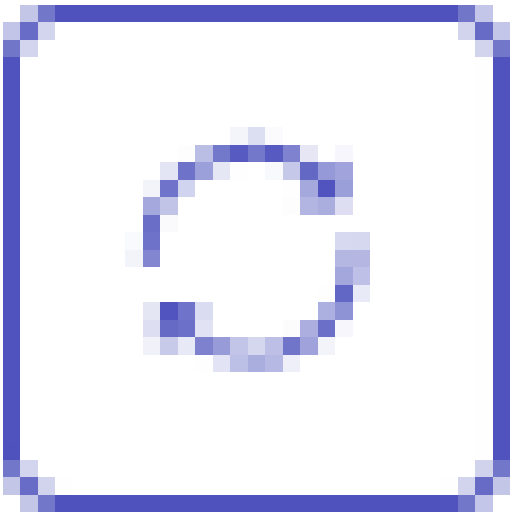
주:
카탈로그의 카드는 카드 상단에 있는 레이블(위협 피드/보강)로 구분됩니다.

카탈로그 뷰에 대한 작업

카탈로그 뷰에서는 다음 작업을 수행할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

카탈로그 뷰에 대한 작업

작업	설명
모두	이 드롭다운 메뉴를 사용하여 피드 및 통합을 현재 상태를 기준으로 필터링합니다. 다음 상태를 기준으로 필터링할 수 있습니다. • 모두: 페이지의 모든 피드 및 통합을 표시합니다. 이 옵션이 기본 옵션입니다. • 활성화됨: 활성화된 상태에 있는 모든 피드 및 통합을 표시합니다. • 비활성화됨: 비활성화된 상태에 있는 모든 피드 및 통합을 표시합니다. • 초안: 초안 상태에 있는 모든 피드와 통합을 표시합니다.
	이 작업을 사용하여 카탈로그를 새로 고칩니다.
	이 작업을 사용하여 다음을 기준으로 모든 피드와 통합을 정렬합니다. • 마지막으로 수정한 날짜(최신순) • 마지막으로 수정한 날짜(오래된 순) • 이름**(A-Z)** • 이름**(Z~A)**

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

카탈로그 뷰에 대한 작업

작업	설명
카탈로그에서 검색	이 작업을 사용하여 카탈로그 내의 이름 및 설명을 기반으로 피드/통합을 검색할 수 있습니다.

Threat Intelligence 피드

Threat Intelligence 피드를 사용하여 Threat Intelligence 피드 데이터 소스를 추가, 편집 또는 제거합니다.

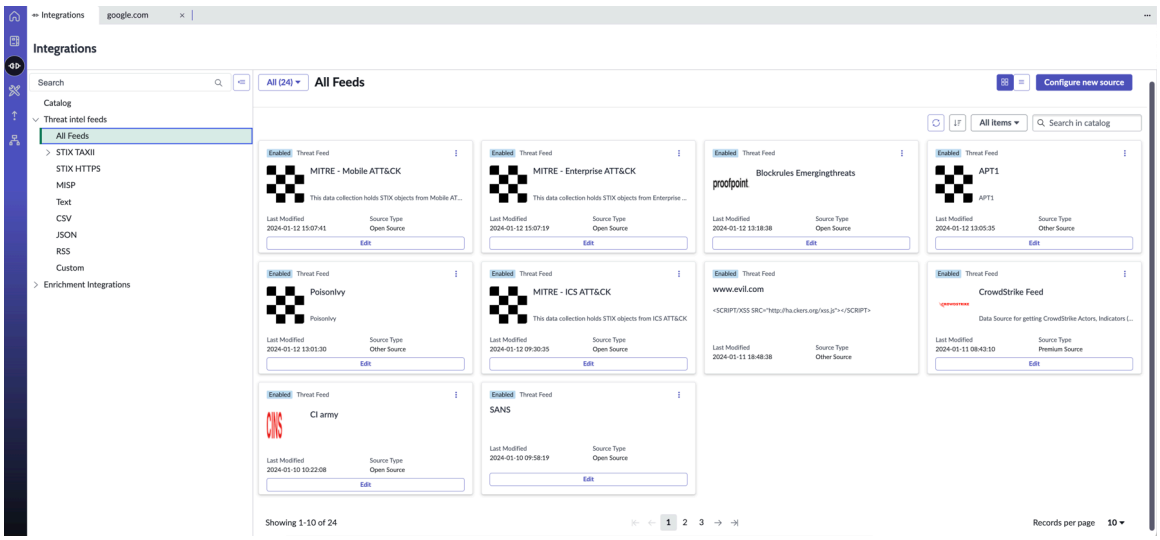
데이터 소스 피드는 통합 섹션의 위협 인텔리전스 카탈로그에서 사용할 수 있습니다.

위협 인텔리전스 피드에 대한 카탈로그는 사용 가능한 피드 데이터 소스를 타일 형식으로 표시하도록 작성되었으며 소스 구성의 세부 정보를 필터링, 검색 및 탐색하고 다양한 작업을 수행할 수 있는 기능이 있습니다.

모든 피드

기본 시스템에는 활성화하고 사용할 수 있는 각 피드에 대한 일련의 카드가 포함되어 있습니다.

피드는 다음으로 이동하여 볼 수 있습니다. 작업 공간 〉 위협 인텔리전스 보안 센터 〉 통합 〉 위협 인텔리전스 피드 〉 모든 피드.



모든 피드 뷰의 작업

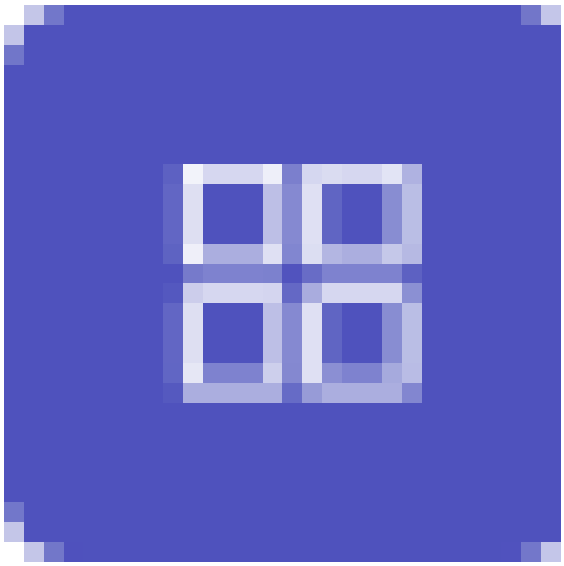
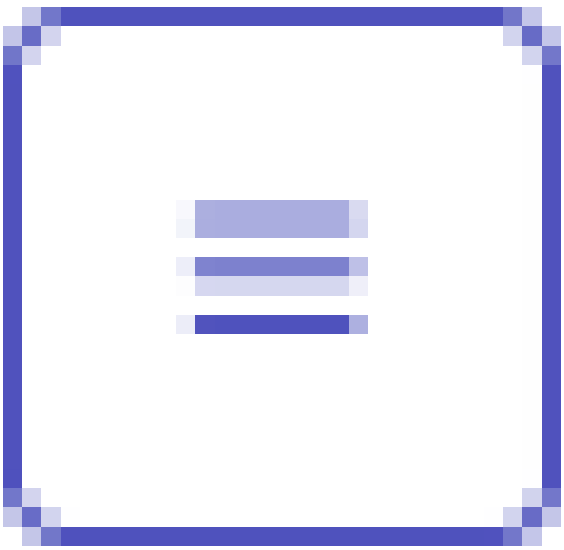
모든 피드 섹션에서는 다음 작업을 수행할 수 있습니다.

모든 통합 뷰에 대한 작업

작업	설명
모두	이 드롭다운 메뉴를 사용하여 현재 상태를 기준으로 피드를 필터링할 수 있습니다. 다음 상태를 기준으로 필터링할 수 있습니다.

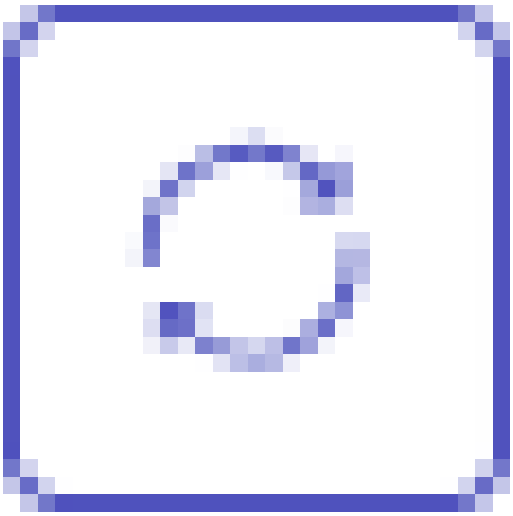
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모든 통합 뷰에 대한 작업

작업	설명
	• 모두: 페이지의 모든 피드를 표시합니다. 이 옵션이 기본 옵션입니다. • 사용: 사용 가능한 상태의 모든 피드를 표시합니다. • 사용 안 함: 사용 안 함 상태에 있는 모든 피드를 표시합니다. • 초안: 초안 상태의 모든 피드를 표시합니다.
	이 작업을 사용하여 카드 형태의 모든 피드를 볼 수 있습니다.
	이 작업을 사용하여 목록 뷰 형태의 모든 피드를 볼 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모든 통합 뷰에 대한 작업

작업	설명
	이 작업을 사용하여 페이지를 새로 고침합니다.
	이 작업을 사용하여 다음을 기준으로 모든 통합을 정렬합니다. • 마지막으로 수정한 날짜(최신순) • 마지막으로 수정한 날짜(오래된 순) • 이름**(A-Z)** • 이름**(Z~A)**
모든 항목	이 작업을 사용하여 소스 유형 또는 피드 유형별로 위협 인텔리전스 피드 타일을 필터링하고 나열합니다. 소스 유형: • 오픈 소스 • 기타 소스 • 프리미엄 소스 피드 유형: • CSV • 사용자 지정 피드 • JSON

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모든 통합 뷰에 대한 작업

작업	설명
	• MISP • RSS • STIX HTTPS • 텍스트
카탈로그에서 검색	이 작업을 사용하여 카탈로그 내의 이름 및 설명을 기준으로 피드를 검색할 수 있습니다.

위협 인텔리전스 피드의 유형

다음은 구성 및 활성화할 수 있는 위협 인텔리전스 피드 유형입니다.

Threat Intelligence 피드

유형	설명
TAXII 피드	STIX/TAXII 컬렉션 형식으로 사용할 수 있는 피드입니다.
STIX HTTPS	HTTPS 프로토콜의 REST API를 통해 액세스할 수 있는 STIX 형식의 Threat Intelligence 피드입니다.
MISP	MISP 형식 피드에 있는 피드입니다.
텍스트	텍스트 형식의 호스팅된 파일로 사용할 수 있는 피드입니다. **주:** 시스템은 URL, 도메인, 파일 이름, 해시 및 IP 주소에 대한 파일을 구문 분석하여 추출만 되고 다른 옵저버블 유형은 추출되지 않습니다.
CSV	CSV 형식의 호스팅된 파일로 사용할 수 있는 피드입니다. **주:** 시스템은 URL, 도메인, 파일 이름, 해시 및 IP 주소에 대한 파일을 구문 분석하여 추출만 되고 다른 옵저버블 유형은 추출되지 않습니다.
JSON	JSON 형식의 호스팅된 파일로 사용할 수 있는 피드입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Threat Intelligence 피드

유형	설명
	주: 시스템은 URL, 도메인, 파일 이름, 해시 및 IP 주소에 대한 파일을 구문 분석하여 추출만 되고 다른 옵저버블 유형은 추출되지 않습니다.
RSS	RSS 형식으로 사용할 수 있는 피드입니다. 애플리케이션은 데이터를 RSS 피드 기록으로 저장합니다.
사용자 지정	사용자 지정 파서를 사용하여 구성된 피드입니다. 주: 시스템은 URL, 도메인, 파일 이름, 해시 및 IP 주소에 대한 파일을 구문 분석하여 추출만 되고 다른 옵저버블 유형은 추출되지 않습니다.

절차의 다음 단계는 아래의 Threat Intelligence 피드각 특정 피드 유형 구성에 대한 해당 섹션을 참조하십시오.

새 위협 인텔리전스 피드 구성

새 위협 인텔리전스 피드를 구성합니다.

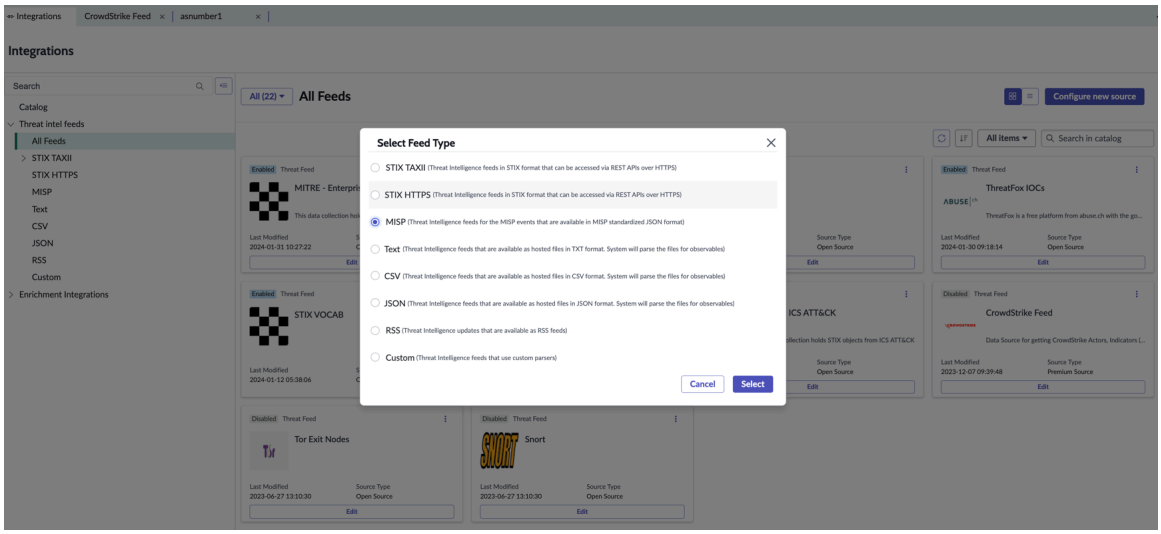
시작하기 전에
필요한 역할: sn_sec_tisc.admin

새 위협 인텔리전스 피드를 구성하려면 다음 절차를 따르십시오.

프로시저

1. 다음으로 이동 모두 〉 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 통합 아이콘을 클릭합니다.
3. 선택 위협 인텔리전스 피드 〉 모든 피드.
4. 새 소스 구성을 클릭합니다.
   다양한 피드 유형이 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



5. 각 피드 유형을 선택합니다.
6. 양식에서 필드를 채웁니다.

새 소스 구성

필드	설명
이름	피드의 이름을 입력합니다.
설명	피드에 대한 설명입니다.
피드 유형	피드 유형입니다. 예: MISP 기본적으로 이 값은 카탈로그에서 선택한 피드 유형에 따라 표시됩니다.
로고	소스 피드의 로고를 첨부합니다. 주: 크기는 72px/72px여야 합니다.
산업	항공 우주, 농업 등 사료를 적용할 수 있는 산업 범주를 선택합니다.
소스 유형	사용 가능한 소스 유형 목록에서 소스 유형을 선택합니다. 사용 가능한 소스 목록은 다음과 같습니다. ○ 정부 ○ ISAC ○ 오픈 소스 ○ 프리미엄 소스 ○ 기타 소스

7. 선택을 클릭합니다.
8. 구성 섹션의 필드에 적절한 정보를 입력합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

구성

필드	설명
만료 기간(일)	피드의 만료 기간을 일 단위로 입력합니다. 예를 들어 180일입니다. 주: 소스에서 수집된 데이터는 수집 후 180일 후에 만료됩니다.
REST 메시지 사용	에서 ServiceNow AI Platform제공하는 REST 메시지/REST 메서드 기능을 사용해야 하는 경우 **REST** 메시지 사용 확인란을 선택합니다. 이 확인란을 선택하지 않으면 애플리케이션은 **REST** 엔드포인트 **URL** 에 제공된 엔드포인트를 사용하여 피드에서 데이터를 가져옵니다. 자세한 내용은 설명서에서 ServiceNow AI Platform아웃바운드 REST 웹 서비스를 참조하세요. 주: REST 메시지를 선택하면 REST 메시지 및 REST 메서드 필드가 필수입니다.
REST 메시지	인스턴스에 이미 구성된 REST 메시지 기록 목록에서 REST 메시지 기록을 선택합니다. 자세한 내용은 설명서에서 ServiceNow AI Platform아웃바운드 REST 웹 서비스를 참조하십시오. 주: 특정 헤더를 확인해야 할 때 이 값을 선택하고 REST 메시지 옵션을 사용하여 REST 관련 기록을 정의합니다.
REST 메서드	선택한 REST 메시지에 대해 구성된 사용 가능한 REST 메서드 목록에서 REST 메서드를 선택합니다. 자세한 내용은 설명서에서 ServiceNow AI Platform아웃바운드 REST 웹 서비스를 참조하십시오.
신뢰도	이 특정 피드를 통해 수집되는 해당하는 모든 기록에 대한 신뢰도를 설정합니다. 주: 이 소스에 대한 신뢰도를 0-100 사이로 설정합니다.
데이터 구문 분석 메커니즘	적절한 데이터 구문 분석 메커니즘 옵션을 선택합니다. 사용 가능한 옵션은 다음과 같습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	○ 자동 **IoC** 추출: 이 옵션은 텍스트, CSV 또는 JSON 피드를 구성할 때 기본적으로 선택됩니다. ○ 사용자 지정 필드 매핑: 피드 데이터의 특정 필드를 옵저버블 속성에 매핑하는 방법을 정의하려면 이 옵션을 선택합니다. 선택한 후에는 필드 매핑 섹션에서 매핑을 구성할 수 있습니다. 사용자 지정 필드 매핑에 대한 자세한 내용은 다음 문서를 참조하십시오 사용자 지정 필드 매핑 구성. **주:** 데이터 구문 분석 메커니즘 옵션은 피드 보고서 프로세서 가 SimpleFeedDatasourceResponseProcessor로 설정된 텍스트, CSV 및 JSON 피드에만 사용할 수 있습니다.
REST 엔드포인트 URL	위협 인텔리전스 피드에서 데이터를 호스팅하는 REST 엔드포인트 URL을 입력합니다. **주:** MISP 피드 유형의 경우 /manifest.json 로 끝나는 REST 엔드포인트 URL이 지원됩니다.
인증 필요	새 위협 인텔리전스 피드에 인증이 필요한 경우 이 확인란을 선택합니다. **주:** 이는 REST 엔드포인트 URL을 사용하여 데이터를 검색하는 경우에만 적용할 수 있습니다.
인증 유형	소스 피드에 대한 인증 유형입니다. 다음은 사용자에 대해 기본 시스템 내에서 구성되고 프로비저닝되는 인증 유형입니다. ○ API ID / API 키 ○ API ID / API 비밀 ○ API 키 ○ API 키 / API 비밀 ○ API 사용자 이름 / API 암호 / API 키 ○ 기본 인증
요청과 함께 전달할 헤더	요청과 함께 전달될 모든 헤더는 요청 헤더 매핑에서 제공될 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	○ 헤더는 콜론(":")으로 구분된 키-값 쌍으로 제공되어야 합니다. ○ 각 헤더 키 값 쌍은 새 줄에 제공되어야 합니다. ○ 인증 매개변수를 헤더 값으로 제공하려면 필수 인증 레이블을 "${" 및 "}$"로 묶습니다. 예: x-api-key:${API Key}$.
고급	사용자 지정 통합 스크립트와 보고서 프로세서 스크립트를 정의하려면 이 확인란을 선택합니다. 주: 이 확인란을 선택하면 사용자 지정 스크립트를 선택할 수 있는 통합 스크립트 및 보고서 프로세서 필드가 표시됩니다.
통합 스크립트	통합 스크립트는 피드에 구성된 인증 매개변수와 헤더를 사용하여 REST 엔드포인트 URL에 대한 호출을 호출한 다음 스크립트는 특정 피드에서 사용할 수 있는 데이터를 가져옵니다. 기본 시스템 내에서 사용 가능한 사용자 지정 스크립트 포함은 다음과 같으며, 이는 통합 스크립트에 대한 애플리케이션 내에서 프로비저닝됩니다. ○ MITRESourceIntegration: MITRE 피드에서 데이터를 가져오는 데 사용됩니다. ○ RSSFeedDatasourceIntegration: RSS 피드에서 데이터를 가져오는 데 사용됩니다. ○ SimpleFeedDatasourceIntegration: 인증 또는 기본 인증 없이 단순 피드에서 데이터를 가져오는 데 사용됩니다. ○ SimpleMISPFeedDatasourceIntegration: 호스팅된 MISP 피드에서 데이터를 가져오는 데 사용됩니다. 기본 통합 스크립트는 선택한 피드 유형을 기반으로 합니다. 예를 들어 데이터를 처리하고 가져올 표준 형식인 MISP 피드 유형을 선택하면 통합 스크립트는 **SimpleMISPFeedDatasourceIntegration**입니다. 주: 사용자 지정 통합 스크립트의 경우 **FeedDatasourceIntegrationBase** 를 확장하여 스크립트 포함을 생성하고 필요한 메서드를 재정의할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
보고서 프로세서	보고서 프로세서 스크립트는 통합 스크립트를 사용하여 피드에서 가져온 데이터를 처리합니다. 기본 시스템에는 보고서 프로세서 스크립트를 지원하기 위해 애플리케이션 내에서 프로비저닝되는 다음과 같은 사용자 지정 스크립트가 포함됩니다. ○ AtomFeedDatasourceResponseProcessor: Atom 형식의 RSS 피드를 처리하는 데 사용됩니다. ○ MITRECollectionDataProcessor: MITRE 피드를 처리하는 데 사용됩니다. ○ RSSFeedDatasourceResponseProcessor: RSS 피드를 처리하는 데 사용됩니다. ○ SimpleDataplaneFeedResponseProcessor: 데이터플레인 피드를 처리하는 데 사용됩니다. ○ SimpleFeedDatasourceResponseProcessor: 옵저버블의 정규 표현식 추출을 사용하여 단순 피드를 처리하는 데 사용됩니다. ○ SimpleFeodotrackerFeedResponseProcessor: Feodotracker 피드를 처리하는 데 사용됩니다. ○ SimpleMISPFeedDatasourceResponseProcessor: 호스팅된 MISP 피드를 처리하는 데 사용됩니다. ○ TAXIIV2CollectionDataProcessor: TAXII 컬렉션 데이터 처리에 사용됩니다. MISP 피드에 대한 기본 보고서 프로세서는 SimpleMISPFeedDatasourceResponseProcessor입니다. 이 프로세서는 응용 프로그램에 의해 미리 구성되어 있으며 수정하거나 교체할 수 없습니다.

9. 스케줄링 섹션의 필드에 적절히 입력합니다.

예약

필드	설명
실행	레코드를 수집할 빈도를 설정합니다. 피드는 예약 작업 간격에 따라 실행되고 실행됩니다. 사용 가능한 작업 간격은 다음과 같습니다. ○ 매일 ○ 주별 ○ 월별

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	○ 주기적으로 ○ 한 번 ○ 요청 시 ○ 비즈니스 달력: 입력 시작 ○ 비즈니스 달력: 입력 종료 주: 기본적으로 빈도는 요청 시로 설정됩니다. 자세한 내용은 예약된 작업 및 선택한 스크립트를 자동으로 실행하는 방법을 참조하십시오.
데이터를 가져오는 위치	데이터를 가져와야 하는 시작 날짜입니다. 이 필드는 해당 소스에서 데이터를 수집해야 하는 시간으로 설정해야 합니다. 이 필드가 설정되면 다음 수집 실행은 구성된 시간에서 데이터를 가져오고 연속 수집 실행은 증분 데이터를 가져옵니다. 예를 들어 소스는 매시간 데이터를 수집하도록 예약되어 있습니다. 사용자는 1월 12일 오전 9:30에 1월 12일 오전 6:00까지 데이터 가져오기 를 설정하고, 1월 12일 오전 10:00에 트리거되는 수집 트리거는 1월 12일 오전 6:00부터 1월 12일 오전 10:00까지 데이터를 가져옵니다. 오전 11:00에 트리거되는 다음 수집은 1월 12일 오전 10:00부터 1월 12일 오전 11:00까지 증분 데이터만 가져옵니다. 주: 즉, 예약된 실행이 지정된 날짜부터 증분 방식으로 데이터를 가져옵니다. 중요사항: 또한 텍스트, CSV 및 JSON 피드에는 적용되지 않습니다.

태그

필드	설명
태그 선택	태그를 사용하여 이 소스에서 시스템으로 수집된 기록에 주석을 달거나 이어마크합니다. 검색 창에 태그 이름을 입력하여 애플리케이션에서 사용 가능한 태그를 선택하거나, 새 태그 이름을 입력하고 추가를 클릭하여 소스에 할당합니다.

10. 저장 작업을 클릭하여 피드를 저장하고 생성합니다.
제공된 상세 정보가 확인되고 기본적으로 피드 상태는 사용 안 함입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

11. 옵션: 피드 구성을 초안으로만 저장하려면 초안으로 저장 작업을 클릭합니다.
피드가 초안 상태로 저장되면 사용자가 피드를 활성화할 수 없습니다. 구성 상세 정보가 확실하지 않은 경우 초안으로 저장 옵션을 사용할 수 있습니다. 구성 상세 정보를 얻은 후 초안 버전에 나머지 정보를 채우고 생성할 수 있습니다.
12. 기록을 활성화하려면 활성화를 클릭하십시오.

    위협 인텔리전스 피드 기록이 활성화되면 기록을 실행하여 통합을 실행할 수 있습니다.

    주:
    - 위협 인텔리전스 피드 기록에 레이블이 지정되고 활성화됨으로 표시됩니다. 마찬가지로 비활성화 버튼을 클릭하여 위협 인텔리전스 피드를 비활성화할 수 있습니다.
    - 카탈로그 또는 위협 인텔리전스 피드 페이지에서 필요한 피드 타일의 작업 메뉴를 사용하여 특정 피드를 활성화, 비활성화 또는 삭제할 수도 있습니다.

13. 삭제를 클릭하여 위협 인텔리전스 피드 기록을 삭제합니다.
14. 통합 실행 섹션을 선택하여 실행 상세 정보를 확인합니다.

    주:
    위의 위협 인텔리전스 피드 구성 절차는 STIX TAXII를 제외한 다른 모든 위협 인텔리전스 피드 유형에 대해 동일합니다. STIX TAXII가 구성되는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 새 TAXII 피드 구성.

사용자 지정 필드 매핑 구성

필드 매핑을 사용하면 텍스트, CSV 또는 JSON과 같은 데이터 피드의 각 필드를 해석하고 해당 옵저버블에 할당하는 방법을 구성할 수 있습니다.

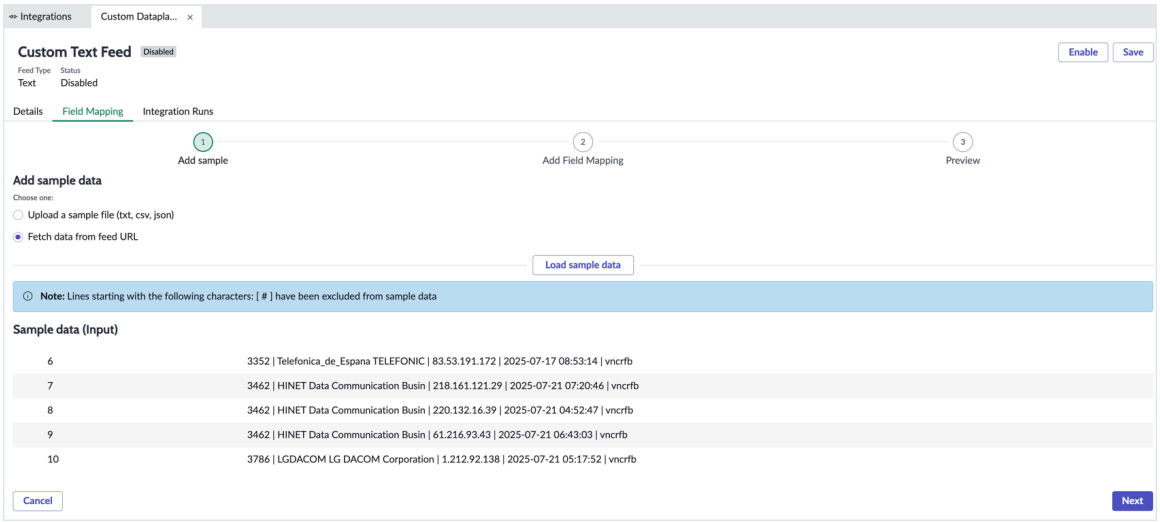
시작하기 전에
필요한 역할: sn_sec_tisc.admin

프로시저
1. 다음으로 이동 모두 〉 작업 공간 〉 위협 인텔리전스 보안 센터 〉 통합.
2. 선택 위협 인텔리전스 피드 〉 모든 피드 〉 텍스트.
3. 새 소스 구성을 선택합니다.
4. 필요에 따라 텍스트 피드 양식 상세 정보를 입력합니다.
자세한 내용은 새 위협 인텔리전스 피드 구성 문서를 참조하십시오.
5. 새 양식 뷰에서 구성 섹션의 데이터 구문 분석 메커니즘 필드로 드릴다운합니다.
데이터 구문 분석 메커니즘에 대한 자세한 내용은 다음 문서를 참조하십시오 새 위협 인텔리전스 피드 구성.
6. 사용자 지정 필드 매핑 옵션을 선택합니다.
7. 필드 매핑 섹션으로 이동합니다.
8. 구성을 선택하여 새 데이터 원본에 대한 필드 매핑을 추가합니다.
이 섹션에는 샘플 데이터 추가, 필드 매핑 및 매핑된 샘플 기록 미리 보기와 같은 세 단계가 포함됩니다.
9. 샘플 데이터를 추가하려면 샘플 데이터 로드를 선택합니다.
선택한 옵션의 샘플 데이터가 표시되고 ####### ## 데이터 행만 표시하고 #으로 시작하는 줄은 샘플 데이터에서 제외됩니다. 코멘트 식별자는 ### ## sn_sec_tisc.feed_comment_identifiers로 수정할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

응용 프로그램은 샘플 파일(예: .txt, .csv 또는 .json)에서 또는 구성된 피드 URL(세부 정보 섹션에 입력한 피드 URL 및 자격 증명)에서 직접 들어오는 데이터의 샘플을 가져옵니다. 이렇게 하면 필드 매핑을 정의하기 전에 데이터의 구조와 컨텐츠를 미리 볼 수 있습니다.

10. 샘플 파일 업로드 또는 피드 URL의 피드 데이터를 선택합니다.
이 샘플 데이터는 기본적으로 처음 10개의 기록을 가져오며, 검색할 이 총 기록 수는 ### ## sn_sec_tisc.feed_field_mapping_sample_count로 수정할 수 있습니다.



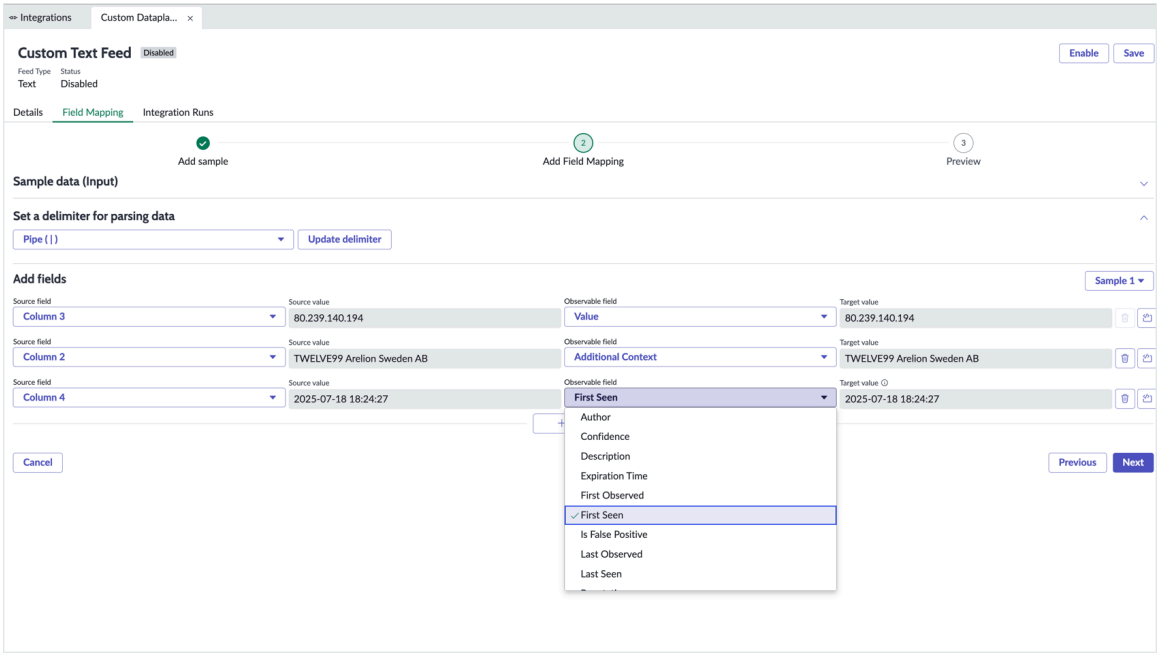
11. 다음을 선택하여 필드 매핑을 구성합니다.
12. 드롭 다운 목록에서 데이터 구문 분석을위한 구분 기호 설정 옵션을 선택합니다.
텍스트 피드로 작업할 때 구분 기호는 데이터를 개별 필드로 올바르게 구문 분석하는 데 필수적입니다.

    이 시나리오에서 텍스트 피드는 파이프 연산자(|)를 구분 기호로 사용하여 샘플 텍스트 데이터의 각 값을 별개의 열로 구분합니다. 이 구분 기호를 올바르게 식별하고 적용하는 것은 정확한 필드 매핑과 성공적인 데이터 수집을 보장하는 데 필수적입니다.

    주:
    CSV 피드의 경우 쉼표(,)가 기본 구분 기호이며 JSON 피드에는 구분 기호가 필요하지 않습니다.

13. 구분 기호 업데이트를 선택합니다.
필드 매핑을 위한 필드를 추가하는 옵션이 표시됩니다.
14. 드롭다운 목록에서 적절한 값을 선택하여 필드 매핑을 계속 추가합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



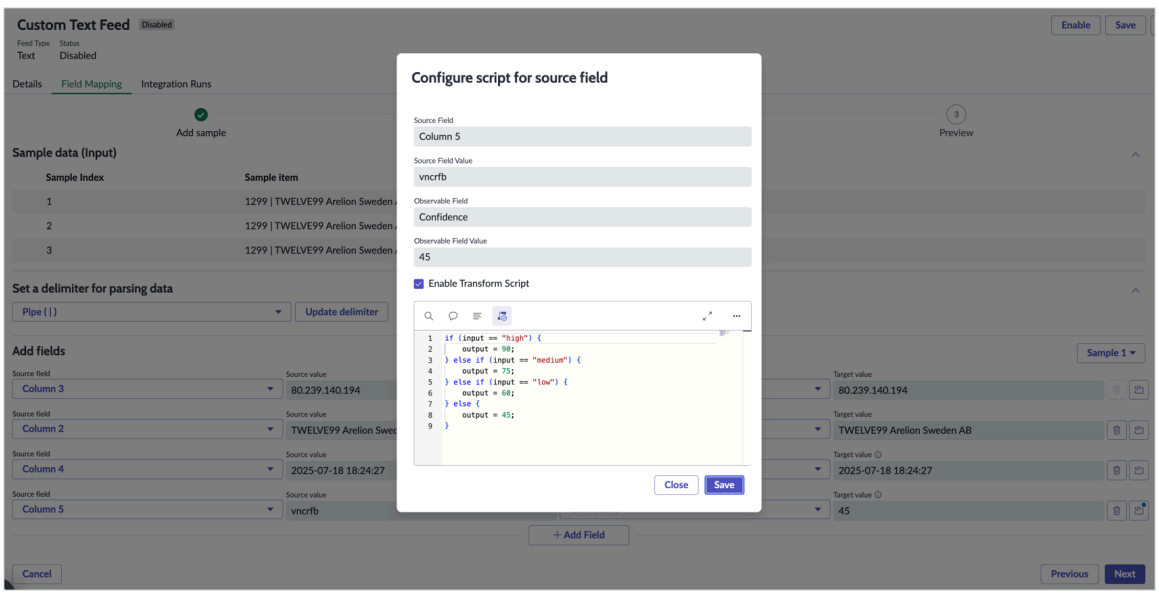
15. 변환 스크립트를 사용하여 입력 값을 변환하고 표준화한 후 옵저버블에 매핑합니다.

a. 변환 스크립트 사용/사용 안 함 아이콘을 선택하여 스크립트를 구성합니다.
소스 필드에 대한 스크립트 구성 대화 상자가 표시됩니다.

b. 소스 필드에 대한 스크립트 구성 대화 상자에서 변환 스크립트 사용 확인란을 선택합니다.

c. 스크립트를 추가하거나 수정합니다.

예를 들어 입력 필드에 낮음, 중간 또는 높음과 같은 값이 포함되어 있고 이러한 값을 숫자 신뢰도(0-100 사이)에 매핑하려는 경우 변환 스크립트를 사용하여 입력 값을 변환하고 옵저버블의 신뢰 도 필드에 매핑할 수 있습니다.

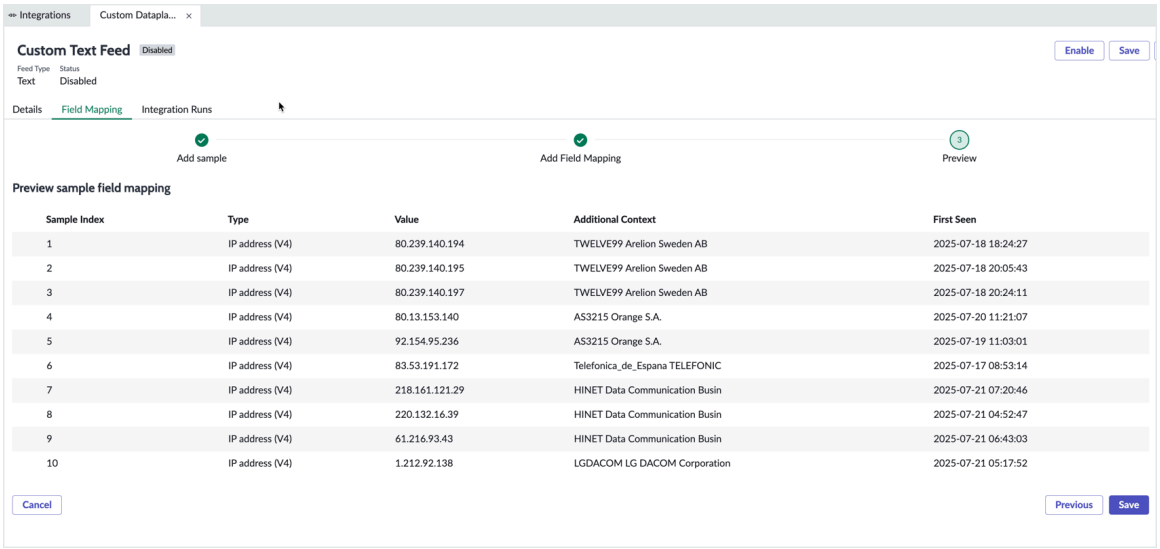


d. 저장을 선택하여 업데이트된 대상 값을 가져오는 스크립트를 저장합니다.

e. 소스 필드에 대한 스크립트 구성 대화 상자를 닫고 다음 단계를 진행합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

16. 다음을 선택하여 미리 보기 섹션에서 필드 매핑을 미리 봅니다.



17. 샘플 필드 매핑을 미리 보고 저장을 선택합니다.
필드 매핑이 성공적으로 저장되었음을 나타내는 확인 메시지가 표시됩니다.

샘플 필드 매핑의 일부로 애플리케이션은 사용자가 샘플 데이터에서 매핑한 옵저버블 유형(예: IP 주소 v4 등)을 자동으로 식별합니다. 이 메커니즘은 매핑 프로세스를 간소화하고 입력에 따라 적절한 옵저버블 유형이 할당되도록 합니다.

중요사항:
필드 매핑 통합 실행: 이 피드 유형에 대해 수행된 모든 통합 실행은 저장된 필드 매핑 구성을 사용합니다. 이렇게 하면 들어오는 데이터가 일관되게 구문 분석되고 구성 중에 정의된 구조에 따라 올바른 옵저버블 속성에 매핑됩니다.

주:
필드 매핑 편집을 선택하여 필드 매핑을 편집하고 필요한 경우 변경합니다. 편집을 계속할 것인지 확인하는 경고 메시지가 표시됩니다. 프롬프트를 확인하고 예를 선택하여 계속합니다. 업데이트된 샘플 데이터를 사용하여 필드 매핑을 필요에 맞게 변경하고 변경 내용을 저장합니다.

필드 매핑에 대한 모든 편집 내용은 이 피드에 대한 향후 통합 실행에 적용됩니다.

통합을 실행하기 전에 올바른 구문 분석을 위해 항상 변경 후 샘플 데이터를 확인하십시오.

위협 인텔리전스 피드 보기

이 섹션에서는 기본 시스템에 구성된 위협 인텔리전스 피드를 제공합니다.

STIX TAXII 피드 보기

기본 시스템에서 구성된 STIX TAXII 피드를 봅니다.

시작하기 전에
필요한 역할: sn_sec_tisc.admin

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 통합 아이콘을 클릭합니다.
3. **STIX TAXII**를 선택합니다.
기본 시스템 내의 MISP 피드는 다음 표에 설명되어 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

위협 피드	설명	URL
사이웨어 TAXII	Cyware Threat Intelligence eXchange(CTIX)는 조직 간에 사이버 위협 인텔리전스를 쉽게 공유할 수 있도록 설계된 플랫폼입니다.	https://threatfeed.cyware.com/ctixapi/ctix21/
기록된 미래 TAXII	Recorded Future는 조직이 사이버, 공급망, 물리적 및 사기 도메인 전반에서 위협을 식별하고 완화할 수 있도록 지원하는 독립적인 위협 인텔리전스 클라우드 플랫폼입니다.	https://api.recordedfuture.com/taxii2
펄스 다이브 TAXII	Pulsedive는 조직에 광범위한 사이버 위협 인텔리전스 서비스 및 도구를 제공하는 위협 인텔리전스 플랫폼입니다.	https://pulsedive.com/taxii2/api/

4. 피드를 편집하려면 편집을 클릭하십시오.

STIX HTTP 피드 보기

기본 시스템에서 구성된 STIX HTTP 피드를 봅니다.

시작하기 전에
필요한 역할: sn_sec_tisc.admin

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 통합 아이콘을 클릭합니다.
3. **STIX** HTTP를 선택합니다.
   다음 표에서는 기본 시스템 내의 STIX HTTP 피드에 대해 설명합니다.

위협 피드	설명	URL
MITRE - 모바일 ATT&CK	이 데이터 수집은 Mobile ATT&CK의 STIX 객체를 보유합니다.	https://raw.githubusercontent.com/mitre/cti/master/mobile-attack/mobile-attack.json
MITRE - ICS ATT&CK	이 데이터 수집은 ICS ATT&CK의 STIX 객체를 포함합니다.	https://raw.githubusercontent.com/mitre/cti/master/ics-attack/ics-attack.json
MITRE - 엔터프라이즈 ATT&CK	이 데이터 수집은 엔터프라이즈 ATT&CK의 STIX 객체를 보유합니다.	https://raw.githubusercontent.com/mitre/cti/master/enterprise-

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

위협 피드	설명	URL
		attack/enterprise-attack.json

4. 편집을 클릭하여 피드를 편집하고 필요한 업데이트를 수행합니다.

MISP 피드 보기

기본 시스템에 구성된 MISP 피드를 봅니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 통합 아이콘을 클릭합니다.
3. **MISP**를 선택합니다.
   기본 시스템 내의 MISP 피드는 다음 표에 설명되어 있습니다.

위협 피드	설명	URL
DigitalSide 위협 인텔 OSINT 피드	주로 맬웨어 분석과 손상된 URL, IP 및 도메인을 기반으로 하는 DigitalSide Threat-Intel OSINT 피드에서 오픈 소스 사이버 위협 인텔리전스 정보를 가져오는 데이터 소스입니다.	https://osint.digitalside.it/Threat-Intel/digitalside-misp-feed/manifest.json
URLhaus IOC	URLhaus는 맬웨어 배포에 사용되는 악성 URL을 공유하는 것을 목표로 abuse.ch 의 프로젝트입니다.	https://urlhaus.abuse.ch/downloads/misp/manifest.json
맬웨어 시장	MalwareBazaar는 정보 보안 커뮤니티, AV 공급업체 및 위협 인텔리전스 제공업체와 맬웨어 샘플을 공유하는 것을 목표로 하는 abuse.ch 의 프로젝트입니다.	https://bazaar.abuse.ch/downloads/misp/manifest.json
ThreatFox IOC	ThreatFox는 맬웨어와 관련된 IOC(Indicators of Compromise)를 정보 보안 커뮤니티, AV 공급업체 및 위협 인텔리전스 제공업체와 공유하는 것을 목표로 abuse.ch 의 무료 플랫폼입니다.	https://threatfox.abuse.ch/downloads/misp/manifest.json

주:
MISP 피드 유형의 경우 /manifest.json 로 끝나는 REST 엔드포인트 URL이 지원됩니다.

4. 피드를 편집하려면 편집을 클릭하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

텍스트 피드 보기

기본 시스템에 구성된 텍스트 피드를 봅니다.

시작하기 전에
필요한 역할: sn_sec_tisc.admin

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 통합 아이콘을 클릭합니다.
3. 텍스트 옵션을 선택합니다.
   다음은 기본 시스템 내에서 구성된 텍스트 피드 목록입니다.

위협 피드	설명	URL
헤일리의 무차별 암호 대입 IP	IP 주소별로 정렬된 지난 2년간의 공격하는 머신 IP 주소 목록을 제공합니다.	http://charles.the-haleys.org/ssh_dico_attack_hdeny_format.php/hostsdeny.txt
Blockrules 새로운 위협	ET(Emerging Threat) 인텔리전스는 의심스럽고 악의적인 활동과 관련된 IP를 식별하기 위해 실행 가능한 위협 인텔리전스 피드를 제공합니다.	https://rules.emergingthreats.net/blockrules/compromised-ips.txt
Nuug Pop3 Groper 웹	bsdly.net 에서 pop3 서비스에 로그온하려고 시도했지만 실패한 호스트 목록입니다.	https://home.nuug.no/%7Epeter/pop3gropers.txt
Tor 출구 노드	Tor 출구 노드는 TOR 네트워크에서 들어오는 트래픽을 감지하는 데 사용할 수 있습니다.	https://www.dan.me.uk/torlist/?exit
Talos Intelligence IP 금지 목록	Talos는 SourceFire의 취약성 연구 팀, Cisco Threat Research and Communications 그룹, Cisco Secure Applications 그룹을 결합하여 구성되었습니다. 결합된 전문 지식은 정교한 인프라와 네트워크, 엔드포인트, 클라우드 환경, 가상 시스템, 일상적인 웹 및 이메일 트래픽 전반에 걸친 Cisco의 독보적인 데이터 텔레메트리로 뒷받침됩니다.	https://www.talosintelligence.com/documents/ip-blacklist
SAN을 참조하십시오.	ISC는 수천 명의 인터넷 사용자와 조직에 무료 분석 및 경고 서비스를 제공합니다.	https://isc.sans.edu/feeds/topips.txt
흡입	Snort는 세계 최고의 오픈 소스 침입 방지 시스템(IPS)입니다. Snort IPS는 악성 네트워크 활동을 정의하는 데	https://snort.org/downloads/ip-block-list

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

위협 피드	설명	URL
	도움이 되는 일련의 규칙을 사용합니다.	
CI 군대	CINS Army 목록은 CINS Active Threat Intelligence 규칙 집합의 하위 집합으로, 다음 두 가지 기본 기준(1) IP의 최근 Rogue Packet 점수 계수가 매우 낮거나 2) IP가 전 세계에 배포된 지정된 수의 Sentinel에서 지정된 수의 '신뢰할 수 있는' 경고를 트립했습니다.	https://cinsscore.com/list/ci-badguys.txt
Proofpoint	방화벽 차단 목록의 원시 IP입니다. Spamhaus(www.spamhaus.org)에서 식별한 스팸 넷, DShield에서 식별한 상위 공격자 (www.dshield.org) 및 Abuse.ch	https://rules.emergingthreats.net/blockrules/emerging-Block-IPs.txt
차단 목록 Greensnow	GreenSnow는 컴퓨터 보안 분야에서 최고의 전문가로 구성된 팀이며, GreenSnow는 전 세계에있는 여러 컴퓨터에서 많은 IP를 수집합니다. GreenSnow는 스팸을 제외한 모든 종류의 공격에 대한 SpamHaus.org 와 비슷합니다.	https://blocklist.greensnow.co/greensnow.txt
CI 군대	CINS Army 목록은 CINS Active Threat Intelligence 규칙 집합의 하위 집합으로, 다음 두 가지 기본 기준(1) IP의 최근 Rogue Packet 점수 계수가 매우 낮거나 2) IP가 전 세계에 배포된 지정된 수의 Sentinel에서 지정된 수의 '신뢰할 수 있는' 경고를 트립했습니다.	https://cinsscore.com/list/ci-badguys.txt
차단 목록	www.blocklist.de 는 사기/남용 전문가가 제공하는 자발적인 무료 서비스로, 서버는 종종 SSH, 메일 로그인, FTP, 웹 서버 및 기타 서비스를 통해 공격을 받습니다.	https://lists.blocklist.de/lists/all.txt
Tor 출구 노드	Tor 출구 노드는 TOR 네트워크에서 들어오는 트래픽을 감지하는 데 사용할 수 있습니다.	https://www.dan.me.uk/torlist/?exit
봇스카우트 봇 IP	BotScout는 "봇"으로 알려진 자동화된 웹 스크립트가 포럼에 등록하고,	http://botscout.com/last_caught_cache.txt

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

위협 피드	설명	URL
	데이터베이스를 오염시키고, 스팸을 퍼뜨리고, 웹 사이트의 양식을 남용하는 것을 방지하는 데 도움이 됩니다.	
데이터플레인 VNC RFB	VNC 원격 프레임 버퍼 세션을 시작하는 것으로 식별되는 IP 주소입니다.	https://dataplane.org/signals/vncrfb.txt
데이터플레인 TELNET 로그인	TELNET 암호 인증을 통해 로그인을 시도하는 것으로 식별된 IP 주소.	https://dataplane.org/signals/telnetlogin.txt
데이터부 SSH 암호 인증	SSH 암호 인증을 통해 로그인을 시도하는 것으로 식별된 IP 주소입니다.	https://dataplane.org/signals/sshpwauth.txt
데이터부 SSH 클라이언트 연결	SSH 클라이언트 프로토콜 협상을 수행하는 것으로 식별된 IP 주소입니다.	https://dataplane.org/signals/sshclient.txt
Blockrules 새로운 위협	ET(Emerging Threat) 인텔리전스는 의심스럽고 악의적인 활동과 관련된 IP를 식별하기 위해 실행 가능한 위협 인텔리전스 피드를 제공합니다.	https://rules.emergingthreats.net/blockrules/compromised-ips.txt
데이터플레인 SMTP 인사말	원치 않는 HELO 또는 EHLO 명령을 실행하는 SMTP 클라이언트로 식별되는 IP 주소입니다.	https://dataplane.org/signals/smtpgreet.txt
데이터부 SIP 쿼리	SIP OPTIONS 쿼리를 보내는 것으로 식별된 IP 주소입니다.	https://dataplane.org/signals/sipquery.txt
데이터플레인 IP 프로토콜 41	개방형 IPv4 프로토콜 41 릴레이(예: IPv6 over IPv4)로 식별되는 IP 주소입니다.	https://dataplane.org/signals/proto41.txt
데이터부 SIP 초대	SIP INVITE 작업 전송으로 식별된 IP 주소입니다.	https://dataplane.org/signals/sipinvitation.txt
데이터부 DNS CH TXT version.bind	DNS CH TXT 버전을 전송하는 것으로 식별된 IP 주소입니다. BIND 쿼리.	https://dataplane.org/signals/dnsversion.txt
데이터부 DNS TCP	TCP 포트 53 쿼리를 통해 DNS를 보내는 것으로 식별된 IP 주소입니다.	https://dataplane.org/signals/dnstcp.txt
임의의 데이터 플레인 DNS 재귀가 필요함	모든 쿼리에서 재귀 DNS를 보내는 것으로 식별된 IP 주소입니다.	https://dataplane.org/signals/dnsrdany.txt
데이터부 DNS 재귀 필요함	재귀 DNS 쿼리를 보내는 것으로 식별된 IP 주소입니다.	https://dataplane.org/signals/dnsrd.txt
GitHub의 피싱 데이터베이스 활성 피싱 링크	Github에서 사용할 수 있는 피싱 데이터베이스에서 활성	https://raw.githubusercontent.com/mitchellkrogza/

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

위협 피드	설명	URL
	피싱 링크를 가져오기 위한 데이터 소스입니다.	Phishing.Database/master/phishing-links-ACTIVE.txt
GitHub의 피싱 데이터베이스 활성 도메인	Github에서 사용할 수 있는 피싱 데이터베이스에서 활성 도메인을 가져오기 위한 데이터 소스입니다.	https://raw.githubusercontent.com/mitchellkrogza/Phishing.Database/master/phishing-domains-ACTIVE.txt
GitHub의 피싱 데이터베이스 활성 IP	Github에서 사용할 수 있는 피싱 데이터베이스에서 활성 IP를 가져오기 위한 데이터 소스입니다.	https://raw.githubusercontent.com/mitchellkrogza/Phishing.Database/master/phishing-IPs-ACTIVE.txt
차단 목록 봇	지난 48시간 이내에 RFI-Attacks, REG-Bots, IRC-Bots 또는 BadBots에 대한 공격 공격을 실행한 것으로 보고된 모든 IP 주소.	https://lists.blocklist.de/lists/bots.txt
차단 목록 Apache 공격	서비스 Apache, Apache-DDOS, RFI-Attacks에 대한 공격을 실행한 것으로 지난 48시간 내에 보고된 모든 IP 주소입니다.	https://lists.blocklist.de/lists/apache.txt
Scopserv의 VoIP 블랙리스트	VoIP 금지 목록에서 차단 목록 지정 IP 목록을 검색합니다.	http://voipbl.org/update/?dm=bl
Threatview 도메인 차단 목록	피싱/제공 맬웨어/명령 및 통제에 대해 식별된 악성 도메인입니다.	https://threatview.io/Downloads/DOMAIN-High-Confidence-Feed.txt
위협 보기 MD5 해시 차단 목록	악성 파일의 MD5 해시 또는 관련 - 맬웨어, 랜섬웨어, 해킹 도구, 봇 등	https://threatview.io/Downloads/MD5-HASH-ALL.txt
Threatview URL 차단 목록	악성 URL은 멀웨어, 피싱, 봇넷, C2를 제공합니다.	https://threatview.io/Downloads/URL-High-Confidence-Feed.txt
Threatview SHA 파일 해시 차단 목록	맬웨어 실행과 관련이 있거나 알려진 파일의 SHA 해시입니다.	https://threatview.io/Downloads/SHA-HASH-FEED.txt
위협 뷰 IP 차단 목록	알려진 잘못된 IP 주소에 대한 악성 IP 차단 목록입니다.	https://threatview.io/Downloads/IP-High-Confidence-Feed.txt
Threatview C2 헌트 피드	인프라 호스팅 Threatview.io 별 사전 예방적 헌트 중에 찾은 명령 및 통제 서버	https://threatview.io/Downloads/High-Confidence-CobaltStrike-C2%20-Feeds.txt

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

위협 피드	설명	URL
Threatview OSINT 위협 피드	OSINT Source(Twitter 및 Pastebin)에서 수집한 악의적인 침해 표시기입니다.	https://threatview.io/Downloads/Experimental-IOC-Tweets.txt

4. 피드를 편집하려면 편집을 클릭하십시오.

CSV 피드 보기

기본 시스템에 구성된 CSV 피드를 봅니다.

시작하기 전에
필요한 역할: sn_sec_tisc.admin

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 통합 아이콘을 클릭합니다.
3. CSV를 선택합니다.
   기본 시스템 내의 CSV 피드는 다음 표에 설명되어 있습니다.

위협 피드	설명	URL
PhishStats	PhishStats의 지난 30일 동안의 피싱 URL.	https://phishstats.info/phish_score.csv
SSL 인증서 금지 목록 Abuse.ch	SSL 인증서 블랙리스트(CSV)는 SSLBL에 블랙리스트에 있는 모든 SSL 인증서의 SHA1 지문이 포함된 CSV입니다.	https://sslbl.abuse.ch/blacklist/sslblacklist.csv
봇넷 C2 IP 금지 목록	SSL 인증서는 하나 이상의 서버(IP 주소:포트 조합)와 연결할 수 있습니다. SSLBL은 SSLBL에서 금지 목록에 지정된 SSL 인증서로 실행 중인 IP 주소를 수집합니다. 일반적으로 봇넷 명령&통제 서버(C&C)입니다. 따라서 SSLBL은 감염된 시스템에서 인터넷으로 향하는 봇넷 C2 트래픽을 탐지하는 데 사용할 수 있는 이러한 IP가 포함된 블랙리스트를 게시하여 네트워크를 떠납니다.	https://sslbl.abuse.ch/blacklist/sslipblacklist.csv
피시탱크 온라인	해당 사항 없음	https://data.phishtank.com/data/online-valid.csv

4. 피드를 편집하려면 편집을 클릭하십시오.

JSON 피드 보기

기본 시스템에 구성된 JSON 피드를 봅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_sec_tisc.admin

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 통합 아이콘을 클릭합니다.
3. **JSON** 옵션을 선택합니다.
   다음은 기본 시스템 내에서 구성된 JSON 피드를 나열합니다.

위협 피드	설명	URL
Feodotracker C&C 호스트	Feodotracker에서 봇넷 C2 IP 차단 목록을 가져오는 데이터 소스	https://feodotracker.abuse.ch/downloads/ipblocklist_recommended.json
페오도트래커	Feodotracker에서 봇넷 C2 IP 차단 목록을 가져오는 데이터 소스	https://feodotracker.abuse.ch/downloads/ipblocklist.json

4. 피드를 편집하려면 편집을 클릭하십시오.

RSS 피드 보기

기본 시스템에 구성된 RSS 피드를 봅니다.

시작하기 전에
필요한 역할: sn_sec_tisc.admin

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 통합 아이콘을 클릭합니다.
3. **RSS** 옵션을 선택합니다.
   다음은 기본 시스템 내에서 구성된 RSS 피드 목록입니다.

위협 피드	설명	URL
RSS 피드 CISO2CISO.COM	CISO2CISO.com 의 RSS 피드 데이터	https://ciso2ciso.com/feed/
보안 RSS 피드에 대한 슈나이어	보안에 대한 슈나이어의 RSS 피드 데이터	https://www.schneier.com/feed/atom/
보안 RSS 피드에 대한 Krebs	KerbsonSecurity의 RSS 피드 데이터	https://krebsonsecurity.com/feed/
We Live 보안 RSS 피드	welivesecurity의 RSS 피드 데이터	http://feeds.feedburner.com/eset/blog
JISA Softech RSS 피드	JISA의 RSS 피드 데이터	https://www.jisasoftech.com/feed/

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

위협 피드	설명	URL
Cisco Newsroom 보안 RSS 피드	Cisco의 최신 보안 뉴스입니다.	https://newsroom.cisco.com/c/services/i/servlets/newsroom/rssfeed.json?feed=security
HelpNet 보안	기업 보안에 중점을 둔 정보 보안 뉴스입니다.	https://www.helpnetsecurity.com/feed/
보안 업무	최상위 미디어의 디지털 포렌식에 대한 정보입니다.	https://securityaffairs.com/feed
Volexity RSS 피드	Volexity에서 정보 보안 블로그의 RSS 피드 데이터.	https://www.volexity.com/blog/feed/
해커 뉴스 RSS 피드	"The Hacker News"의 RSS 피드 데이터	https://feeds.feedburner.com/TheHackersNews?format=xml
Graham Cluley RSS 피드	Graham Cluley의 RSS 피드 데이터	https://grahamcluley.com/feed/

4. 피드를 편집하려면 편집을 클릭하십시오.

사용자 지정 피드 보기

기본 시스템 내에서 제공되는 사용자 지정 피드를 봅니다.

시작하기 전에
필요한 역할: sn_sec_tisc.admin

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 통합 아이콘을 클릭합니다.
3. 사용자 지정을 선택합니다.
   다음 테이블 목록은 바로 사용 가능한 사용자 지정 피드입니다.

위협 피드	설명	URL
CrowdStrike 피드	CrowdStrike 행위자, 옵저버블 및 보고서 데이터를 가져오기 위한 소스입니다.	https://api.crowdstrike.com

4. 피드를 편집하려면 편집을 클릭하십시오.

CrowdStrike용 프리미엄 위협 피드 보기

CrowdStrike 피드를 사용하면 사용자가 CrowdStrike Falcon Intelligence 피드 TISC에서 표시기, 행위자, 보고서 및 관련 컨텍스트를 .

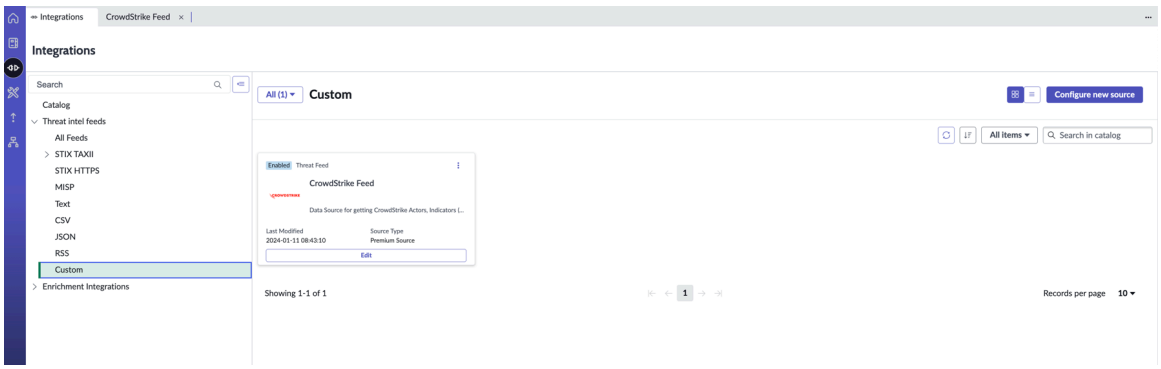
시작하기 전에
필요한 역할: sn_sec_tisc.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터 〉 통합.
2. 사용자 지정을 선택합니다.
3. *CrowdStrike* 피드 양식 페이지에서 편집 버튼을 클릭합니다.

   주:
   기본적으로 CrowdStrike 피드는 사용되지 않습니다. 피드를 사용하려면 구성을 편집해야 합니다.



4. 구성 상세 정보 섹션으로 드릴다운합니다.
5. 클라이언트 **ID** 및 클라이언트 비밀을 입력합니다.

   주:

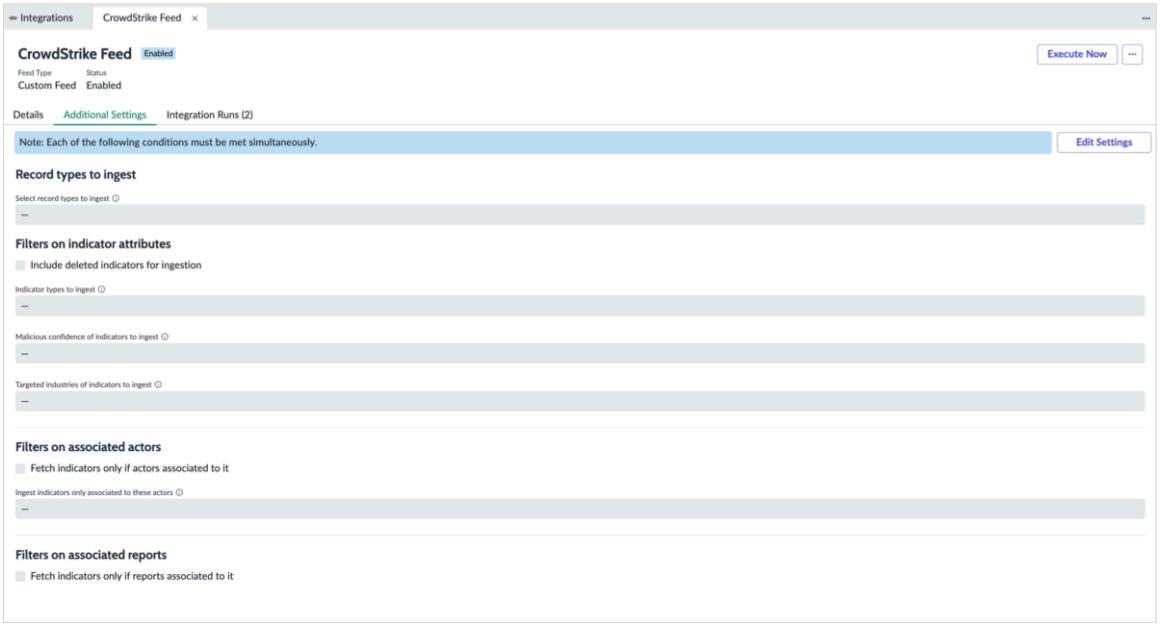
   a. 클라이언트 ID와 클라이언트 암호가 없는 경우 이를 생성해야 합니다. 클라이언트 ID 및 클라이언트 암호에 대한 자세한 내용은 첫 번째 API 클라이언트 정의 섹션을 참조하세요.

   b. 필요한 범위에 대해 클라이언트 ID 및 클라이언트 비밀 *CrowdStrike* 을 가져옵니다. 다음의 *CrowdStrike*클라이언트 ID 및 클라이언트 암호에 필요한 범위는 다음과 같습니다.

      - 지표(Falcon intelligence)
      - 배우(Falcon Intelligence)
      - 보고서(Falcon Intelligence)

6. 추가 설정으로 이동하여 에서 CrowdStrike표시기를 수집하는 동안 적용될 필터를 구성합니다.

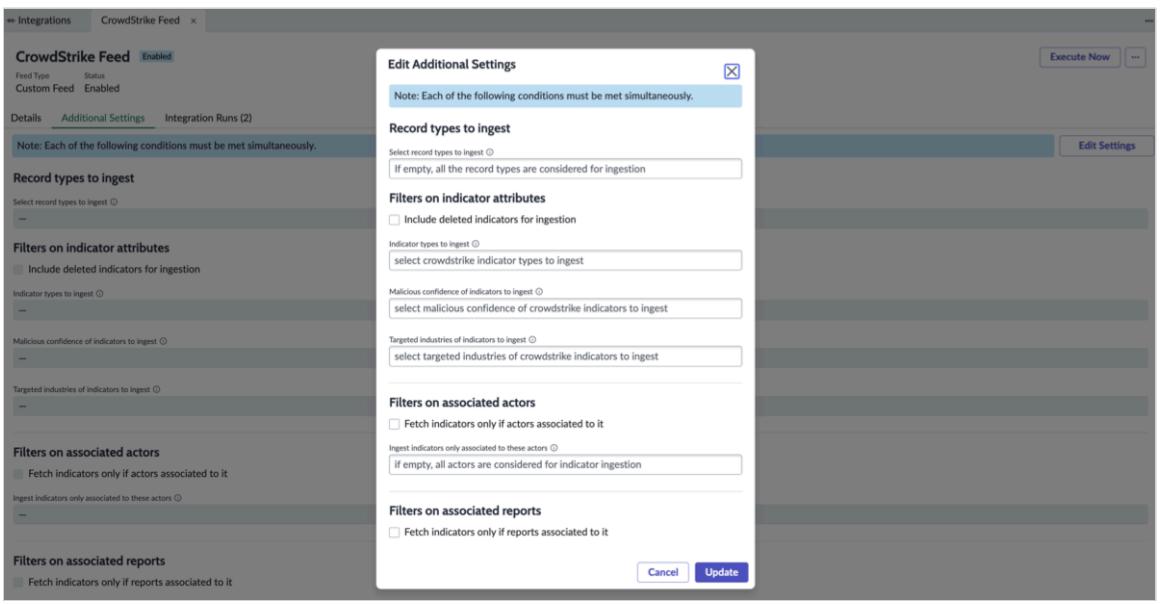
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



추가 설정 탭은 주로 애플리케이션에 데이터를 수집하는 방법을 제어하는 필터를 구성하는 데 사용됩니다.

이러한 필터를 사용하면 특정 요구 사항에 맞게 데이터 통합 프로세스를 사용자 지정하여 가장 관련성이 높은 정보만 포함되도록 할 수 있습니다.

7. 설정 편집을 클릭합니다.



8. 필요한 필터를 선택합니다.

> **주:**
> 구성된 모든 필터는 에서 CrowdStrike표시기를 수집하는 동안 함께 적용됩니다.

아래 섹션에서는 사용 가능한 각 옵션에 대한 자세한 설명을 제공합니다. 다음 표의 각 옵션을 검토하여 필터를 적용하여 애플리케이션에 수집된 데이터를 최적화하는 방법을 이해합니다.

9. 아래에서 사용 가능한 필터에서 필요한 값을 선택하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

추가 설정 편집

필드	설명
수집할 기록 유형	
수집할 기록 유형 선택	수집할 기록 유형을 선택합니다. 사용 가능한 기록 유형은 표시기, 보고서 및 행위자입니다. 주: 수집할 기록 유형으로 표시기 만 선택하면 해당 표시기와 연결된 관련 보고서 및 액터가 자동으로 수집되지 않습니다. 관련 보고서 및 행위자를 수집하려면 세 가지 기록 유형(표시기, 보고서 및 행위자)을 모두 선택해야 합니다.
표시기 속성에 대한 필터	
수집에 대한 삭제된 표시기 포함	삭제된 표시기를 수집할 수 있도록 하려면 이 확인란을 선택합니다. 주: 삭제된 표시기는 이전에 수집된 경우에만 옵저버블로 생성됩니다. CrowdStrike에서 삭제된 태그가 에서 제거된 CrowdStrike표시기에 추가됩니다.
수집할 표시기 유형	수집할 특정 CrowdStrike 표시기 유형을 선택합니다. 아무 것도 선택하지 않으면 기본적으로 사용 가능한 모든 표시기가 검색됩니다.
수집할 표시기의 악의적인 신뢰도	수집할 표시기의 CrowdStrike 악성 신뢰도 수준을 선택합니다. 비워 두면 악의적인 신뢰도에 관계없이 모든 지표를 가져옵니다 CrowdStrike .
수집할 표시기의 대상 산업	수집할 표시기와 CrowdStrike 연결된 대상 산업을 선택합니다. 아무 것도 선택하지 않으면 대상 산업에 관계없이 모든 표시기를 가져옵니다 CrowdStrike .
관련된 액터에 대한 필터	
액터가 연결된 경우에만 표시기 가져오기	표시기가 액터와 연결된 경우에만 가져오려면 이 확인란을 선택합니다.
이 액터에만 연결된 표시기 수집	수집 표시기와 관련된 쉼표로 구분된 액터 이름을 지정합니다. 제공되지 않은 경우 연결된 액터에 관계없이 모든 표시기를 가져옵니다 CrowdStrike .
관련된 보고서의 필터	
보고서가 관련된 경우에만 표시기 가져오기	보고서와 연결된 경우에만 표시기를 가져오려면 이 확인란을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
이 보고서에만 연결된 표시기 수집	수집 표시기와 관련된 보고서 이름을 쉼표로 구분하여 입력합니다. 비워 두면 모든 보고서가 수집 프로세스에 포함됩니다. 제공되지 않은 경우 연결된 보고서와 관계없이 모든 표시기를 가져옵니다 CrowdStrike .
연결된 맬웨어 제품군에 대한 필터	
맬웨어 제품군이 연결된 경우에만 표시기 가져오기	맬웨어 제품군과 연결된 경우에만 표시기를 가져오려면 이 확인란을 선택합니다.
이러한 맬웨어 제품군에만 연결된 표시기 수집	수집 표시기와 연결된 맬웨어 제품군 이름을 쉼표로 구분하여 입력합니다. 비워 두면 모든 맬웨어 제품군이 수집 프로세스에 포함됩니다. 제공되지 않은 경우 맬웨어 제품군에 관계없이 모든 표시기를 가져옵니다 CrowdStrike .
표시기 악의적인 신뢰도를 **TISC** 신뢰도에 매핑 주: 높음, 중간 및 낮음 값은 에서 받은 CrowdStrike소스 값 또는 악의적인 신뢰도입니다.	
높음	악의적인 신뢰도가 높은 표시기의 신뢰도 값(0–100)을 입력합니다. 주: 추가 설정에서 일치하는 악의적인 신뢰도 매핑이 발견되면 신뢰도 값을 수동으로 입력하더라도 상세 정보 섹션에 제공된 값을 재정의합니다.
중간	악의적인 신뢰도가 중간인 표시기의 신뢰도 값(0–100)을 입력합니다.
낮음	악의적인 신뢰도가 낮은 표시기의 신뢰도 값(0–100)을 입력합니다.
확인되지 않음	확인되지 않은 악의적인 신뢰도가 있는 표시기의 신뢰도 값(0–100)을 입력합니다.

주:
위에서 정의한 것과 동일한 추가 설정을 사용하여 새 피드를 만들 때 피드를 복제할 수 있습니다.

10. 추가 설정 대화 상자에서 업데이트를 클릭하여 수정된 추가 설정을 저장합니다.
11. 활성화를 클릭하여 수집을 위한 피드를 활성화합니다CrowdStrike.

주:
프리미엄 피드는 구성 중에 구문 분석되는 응답을 제외하고 다른 피드와 동일합니다. 특정 응답은 클라이언트 ID 및 클라이언트 비밀을 추가하여 구문 분석 CrowdStrike 됩니다.

에서 가져오는 `CrowdStrike`데이터 유형:

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 그 표시기 CrowdStrike 는 구성된 수집 시간 후에 업데이트되고 추가 설정의 일부로 구성된 필터와 일치합니다. 그런 다음 이러한 CrowdStrike 표시기는 의 옵저버블 TISC에 매핑됩니다. 다음에서 수집되는 표시기 유형은 다음과 같습니다.TISC

- SHA256 해시
- MD5 해시
- SHA1 해시
- URL
- 도메인
- IP 주소
- 뮤텍스 이름
- 파일 이름
- 이메일 주소
- 사용자 이름
- IP 주소 차단

b. 구성된 수집 시간 이후에 업데이트되는 위협 액터 CrowdStrike 는 의 TISC위협 액터에 매핑됩니다.

c. CrowdStrike 구성된 수집 시간 이후에 업데이트되는 보고서는 일치하는 속성에 따라 위협 TISC 보고서에 매핑됩니다.

d. 위에서 언급한 엔터티 외에도 다음과 같은 관련 데이터도 가져옵니다.

i. 이전에 수집된 표시기와 관련된 위협 액터, 보고서 및 표시기입니다.

ii. 현재 수집 프로세스 중에 수집된 모든 보고서와 연결된 위협 액터 및 표시기입니다.

> **주:**
> 추가 설정에 구성된 필터는 이전에 수집된 표시기, 보고서 또는 액터와 연결된 표시기를 수집할 때도 적용됩니다.

12. 옵션: 복제를 클릭하여 피드를 복제합니다.
자세한 내용은 중복 위협 인텔리전스 피드 문서를 참조하십시오.

CrowdStrike 시스템 속성

다음은 CrowdStrike의 시스템 속성에 대한 세부 정보입니다.

1. sn_sec_tisc.crowdstrike_actor_batch_size: 단일 API 호출에서 끌어올 액터 수를 나타냅니다. 참고: 통합에서 시스템에 필요한 것을 찾지 못하는 경우에만 적용할 수 있습니다.
   - 유형: 정수
   - 값: 250
2. sn_sec_tisc.crowdstrike_api_limit: CrowdStrike에서 한 번에 가져올 기록의 수입니다. 숫자가 높을수록 페이로드를 처리하는 데 더 많은 메모리가 사용됩니다.
   - 유형: 정수
   - 값: 1000
3. sn_sec_tisc.crowdstrike_indicator_batch_size: 단일 API 호출에서 끌어올 표시기 수를 나타냅니다. 참고: 통합에서 시스템에 필요한 것을 찾지 못하는 경우에만 적용할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 유형: 정수
- 값: 150

4. sn_sec_tisc.crowdstrike_offset_limit_total: CrowdStrike API에서 허용된 오프셋 및 한도의 총계입니다.
   - 유형: 정수
   - 값: 50000
5. sn_sec_tisc.crowdstrike_report_batch_size: 단일 API 호출에서 끌어올 보고서 수를 나타냅니다. 참고: 통합에서 시스템에 필요한 것을 찾지 못하는 경우에만 적용할 수 있습니다.
   - 유형: 정수
   - 값: 50

STIX TAXII 이해

STIX(Structured Threat Information Expression)는 사이버 위협 인텔리전스(CTI)를 교환하는 데 사용되는 언어 및 직렬화 형식입니다. TAXII(Trusted Automated Exchange of Intelligence Information)는 HTTPS를 통해 CTI(사이버 위협 인텔리전스)를 교환하는 데 사용되는 프로토콜입니다.

STIX에서는 의심, 타협 및 귀속의 모든 측면이 대상 및 설명 관계로 표현됩니다. STIX 정보는 분석가를 위해 시각적으로 표시하거나 기계가 빠르게 읽을 수 있도록 JSON으로 저장할 수 있습니다.

사이버 위협 인텔리전스(CTI)는 사이버 위협 인텔리전스를 모델링, 분석 및 공유해야 할 필요성을 해결하기 위해 일련의 정보 표현 및 프로토콜을 정의하기 위해 설립되었습니다. CTI는 주로 STIX(Structured Threat Information Expression) 및 TAXII(Trusted Automated Exchange of Indicator Information)의 개발 및 표준화에 중점을 둡니다.

새 TAXII 피드 구성

STIX 형식 정보를 공유하기 위해 TAXII 피드를 유지할 수 있습니다. 각 TAXII 피드에는 하나 이상의 TAXII 컬렉션이 포함되어 있습니다.

시작하기 전에
필요한 역할: sn_sec_tisc.admin

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 통합 아이콘을 클릭합니다.
3. 선택 위협 인텔리전스 피드 〉 **STIX TAXII** 〉 **TAXII** 피드.

   주:
   내의 모든 TAXII 컬렉션에 대한 프로파일 역할을 하도록 TAXII 피드를 구성합니다.

4. 새 소스 구성을 클릭합니다.
   새 TAXII 피드 구성 페이지가 표시됩니다.
5. 양식에서 필드를 채웁니다.

새 데이터 소스 작성

필드	설명
이름	피드의 이름을 입력합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
설명	피드에 대한 설명입니다.
소스 유형	피드에 제공되는 오픈 소스, 프리미엄 소스 등과 같은 소스 유형입니다. 사용 가능한 소스 유형은 다음과 같습니다. ○ 정부 ○ ISAC ○ 오픈 소스 ○ 프리미엄 소스 ○ 기타 소스
로고	소스 피드의 로고를 첨부합니다.
산업	항공 우주, 농업 등과 같이 피드 데이터 소스를 적용할 수 있는 산업 범주를 선택합니다.

구성 섹션의 필드에 적절한 정보를 입력합니다.

구성

필드	설명
TAXII 버전	구성해야 하는 TAXII 서버의 TAXII 버전을 선택합니다. 지원되는 버전은 2.0 및 2.1입니다.
구성 유형	TAXII 컬렉션을 가져오는 구성 유형을 제공합니다. 사용할 수 있는 값은 다음과 같습니다. ○ 디스커버리 서비스 **URL**: 디스커버리 서비스 URL을 선택하여 TAXII 서버의 디스커버리 서비스 내에서 사용 가능한 모든 API 루트에서 컬렉션을 가져옵니다. ○ **API** 루트 **URL**: API 루트 URL을 선택하여 TAXII 서버의 특정 API 루트에서 컬렉션을 가져옵니다.
인증	인증이 필요한 경우 드롭다운 목록에서 필요한 옵션을 선택합니다. 사용 가능한 옵션은 다음과 같습니다. ○ 없음: 인증이 필요하지 않은 경우 이 옵션을 선택합니다. ○ 기본: 사용자 이름과 암호를 제공하려면 이 옵션을 선택합니다. ○ **API** 키: API 키를 제공하려면 이 옵션을 선택합니다. ○ **REST** 메시지 선택: 다른 유형의 인증에 대해 이 옵션을 선택합니다. REST 메시지 옵션은 다음과 같습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	▪ **REST** 메시지 사용: 사전 빌드 REST 메시지를 빌드하기 위해 REST 메시지가 필요한 경우 이 상자를 선택합니다. 선택하지 않으면 엔드포인트 필드의 값이 사용됩니다. 조회 아이콘을 클릭하고 목록에서 REST 메시지를 선택합니다. ▪ **REST** 메서드: REST 메서드가 필요한 경우 이 상자를 선택합니다. 조회 아이콘을 클릭하고 목록에서 REST 메서드를 선택합니다. 주: REST 메시지 옵션을 선택하면 REST 메시지 및 REST 메서드 필드를 사용할 수 있게 됩니다.
URL	선택한 구성 유형에 따라 TAXII 서버 디스커버리 서비스 URL 또는 특정 API 루트 URL을 입력합니다.
고급 선택 항목	
고급	다른 통합 스크립트와 보고서 프로세서를 선택하려면 확인란을 선택합니다. 선택한 스크립트가 선택한 TAXII 버전과 호환되는지 확인합니다. TAXII 버전 및 인증에 따라 이러한 스크립트는 기본적으로 자동으로 채워집니다.
통합 스크립트	인증 유형(사용자 이름/암호/API 키 및 요청과 함께 전달될 헤더)과 같은 인증 매개변수를 사용하여 REST 엔드포인트 URL API에 대한 호출을 호출한 다음 스크립트는 특정 피드에 사용할 수 있는 옵저버블 또는 표시기 STIX 데이터를 가져옵니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	주: 가져온 데이터는 원시 데이터만 (생성된 기록 없음)이며 통합 프로세스에 첨부된 다음 통합 실행 섹션에서 볼 수 있습니다. 다음은 기본 시스템 내에서 통합 스크립트에 대한 애플리케이션 내에서 프로비저닝되는 사용자 지정 스크립트 포함입니다. ○ TAXIIV2_0QueryParamAPIKeyIntegrationScript ○ TAXIIV2_0BasicAuthIntegrationScript ○ TAXIIV2_1QueryParamAPIKeyIntegrationScript ○ TAXIIV2_1BasicAuthIntegrationScript 기본 통합 스크립트는 선택한 피드 유형을 기반으로 합니다. 스크립트 포함은 간단한 REST 호출을 실행하고 응답을 첨부 파일로 저장한 다음 첨부 파일을 프로세서에 반환합니다.
보고서 프로세서	보고서 프로세서는 REST 끝점 URL에 대한 호출을 호출합니다. 아래의 기본 시스템 내에는 통합 스크립트인 **TAXIIV2CollectionDataProcessor**에 대한 애플리케이션 내에서 프로비저닝되는 사용자 지정 스크립트 포함이 있습니다.

스케줄링 섹션의 필드에 적절히 입력합니다.

예약

필드	설명
컬렉션 실행 빈도	TAXII 수집 기록에 적용되는 일정 간격입니다. 필요한 경우 TAXII 컬렉션 양식 뷰에서 TAXII 컬렉션의 실행 빈도를 수정할 수 있습니다. 주: 이 설정은 가져온 모든 TAXII 컬렉션에 기본적으로 적용됩니다. 필요한 경우 TAXII 컬렉션의 설정을 재정의하는 옵션이 있습니다. 자세한 내용은 예약된 작업 및 선택한 스크립트를 자동으로 실행하는 방법을 참조하십시오.
데이터를 가져오는 위치	데이터를 가져와야 하는 시작 날짜입니다. 이 필드는 해당 소스에서 데이터를 수집해야 하는 시간으로 설정해야 합니다. 이 필드가 설정되면 다음 수집 실행은 구성된 시간에서 데이터를

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	가져오고 연속 수집 실행은 증분 데이터를 가져옵니다. 예를 들어 소스는 매시간 데이터를 수집하도록 예약되어 있습니다. 사용자는 1월 12일 오전 9:30에 1월 12일 오전 6:00까지 데이터 가져오기 를 설정하고, 1월 12일 오전 10:00에 트리거되는 수집 트리거는 1월 12일 오전 6:00부터 1월 12일 오전 10:00까지 데이터를 가져옵니다. 오전 11:00에 트리거되는 다음 수집은 1월 12일 오전 10:00부터 1월 12일 오전 11:00까지 증분 데이터만 가져옵니다. 주: 즉, 예약된 실행이 지정된 날짜부터 증분 방식으로 데이터를 가져옵니다.

6. 연결 확인을 클릭합니다.
   TAXII 피드 연결이 성공했음을 알리는 정보 메시지가 표시됩니다. 컬렉션을 가져오려면 다음 단계로 진행합니다.
7. **TAXII** 컬렉션 가져오기를 클릭합니다.

   주:
   오류가 있는 경우 TAXII 컬렉션을 가져오는 동안 오류가 발생했다는 오류 메시지가 표시되고 자세한 내용은 로그를 확인하십시오.

   TAXII 컬렉션은 TAXII 컬렉션 섹션 아래에 표시되며 기본적으로 비활성화되어 있습니다.
8. TAXII 컬렉션을 활성화하여 이러한 TAXII 컬렉션에서 사용할 수 있는 STIX 객체를 검색합니다.

중복 위협 인텔리전스 피드

위협 피드를 복제하면 연결된 모든 옵저버블, 표시기, 액터 등을 포함하여 기존 피드의 정확한 복사본을 만들 수 있습니다.

시작하기 전에
필요한 역할: sn_sec_tisc.admin

프로시저
1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 통합 아이콘을 클릭합니다.
3. 카탈로그 뷰에서 원하는 통합을 선택합니다.
   예를 들어 CrowdStrike
4. 피드 카드의 편집 버튼을 CrowdStrike 클릭하여 구성 양식을 엽니다.
5. 추가 작업 메뉴를 클릭하고 복제를 선택합니다.
   현재 피드 구성을 복제하고 새로 복제된 피드에 대한 링크가 있는 〔integrationname Feed-copy〕 이름의 새 피드를 만들었음을 나타내는 확인 메시지가 표시됩니다. (예: CrowdStrike 피드 복사)

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

TISC 보강 통합

기본 시스템에는 위협 인텔리전스 보안 센터 사전 구성된 통합이 포함되지 않습니다. 이 섹션에서는 타사 통합과 타사 통합을 모두 ServiceNow 구성하기 위한 지침을 제공합니다.

중요사항:

필요한 외부 공급업체 앱 통합을 설치했는지 확인합니다. 설치된 외부 공급업체 앱에 대한 옵저버블, 사이팅 검색 및 위협 조회 상세 정보만 볼 수 있습니다.

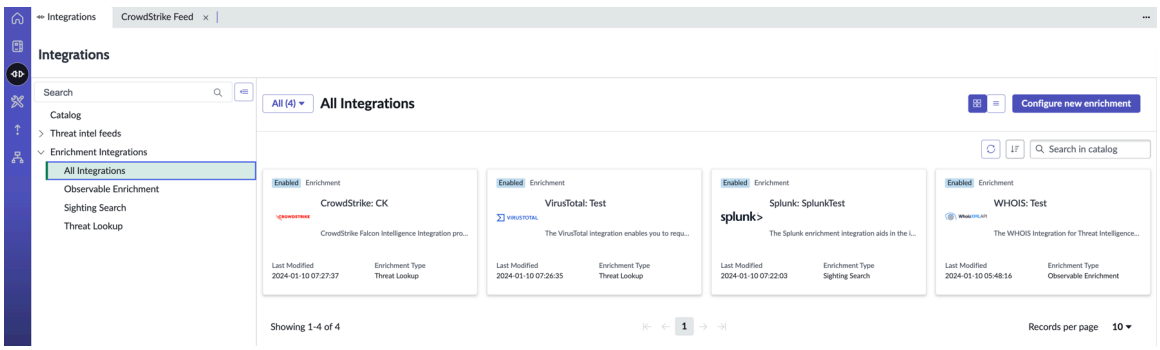
모든 통합 구성

모든 통합은 설치해야 하는 별도의 애플리케이션입니다. TISC는 외부 공급업체 공급업체와의 통합을 지원합니다. 설치된 모든 통합은 여기에서 구성할 수 있습니다.

이 섹션에는 활성화하고 사용할 수 있는 구성된 각 통합 구현에 대한 카드가 표시됩니다.

각 보강 유형의 섹션은 해당 보강 유형에 해당하는 통합 중 하나 이상이 설치된 경우에만 표시됩니다. 예를 들어, 위협 조회 섹션은 하나 이상의 위협 조회 통합이 설치된 경우에만 보강 통합 아래에 표시됩니다.

구성된 통합 카드는 다음으로 이동하여 볼 수 있습니다. 작업 공간 〉 위협 인텔리전스 보안 센터 〉 통합 〉 보강 통합 〉 모든 통합.



모든 통합 뷰에 대한 작업

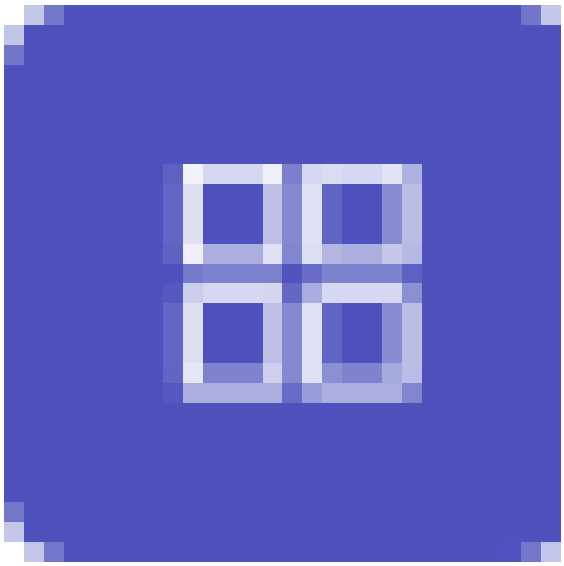
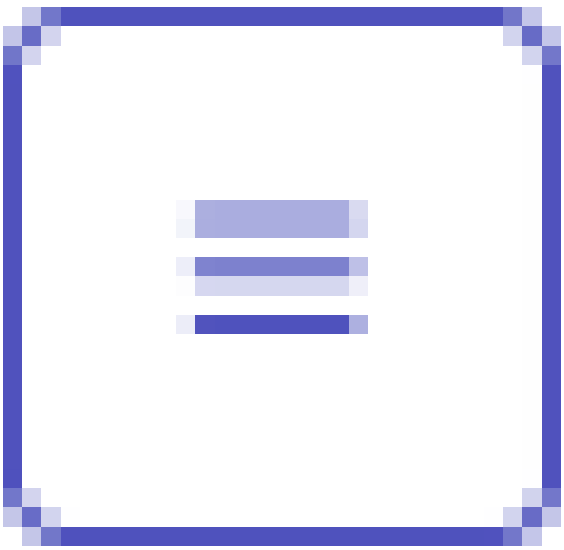
모든 통합 뷰에서는 다음 작업을 수행할 수 있습니다.

모든 통합 뷰에 대한 작업

작업	설명
모두	이 드롭다운 메뉴를 사용하여 현재 상태를 기준으로 통합을 필터링합니다. 다음 상태를 기준으로 필터링할 수 있습니다. • 모두: 페이지의 모든 통합을 표시합니다. 이 옵션이 기본 옵션입니다. • 활성화됨: 활성화된 상태에 있는 모든 통합을 표시합니다. • 비활성화됨: 비활성화된 상태의 모든 통합을 표시합니다. • 초안: 초안 상태인 모든 통합을 표시합니다.

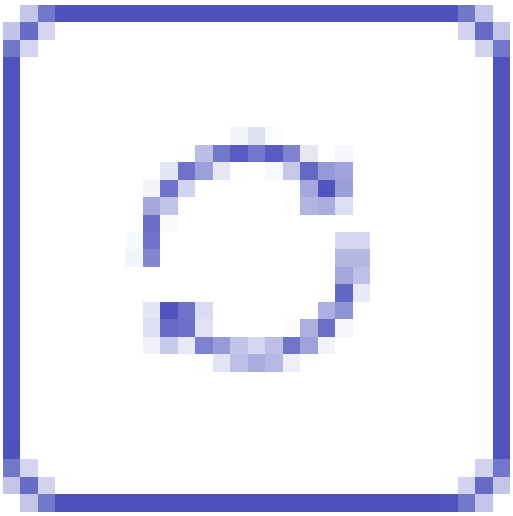
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모든 통합 뷰에 대한 작업

작업	설명
	이 작업을 사용하여 카드 형태로 모든 통합을 봅니다.
	이 작업을 사용하여 목록 형식으로 모든 통합을 볼 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모든 통합 뷰에 대한 작업

작업	설명
	이 작업을 사용하여 모든 통합 페이지를 새로 고침합니다.
	이 작업을 사용하여 다음을 기준으로 모든 통합을 정렬합니다. • 마지막으로 수정한 날짜(최신순) • 마지막으로 수정한 날짜(오래된 순) • 이름**(A-Z)** • 이름**(Z~A)**
카탈로그에서 검색	이 작업을 사용하여 카탈로그 내의 이름 및 설명을 기반으로 구성된 통합을 검색할 수 있습니다.

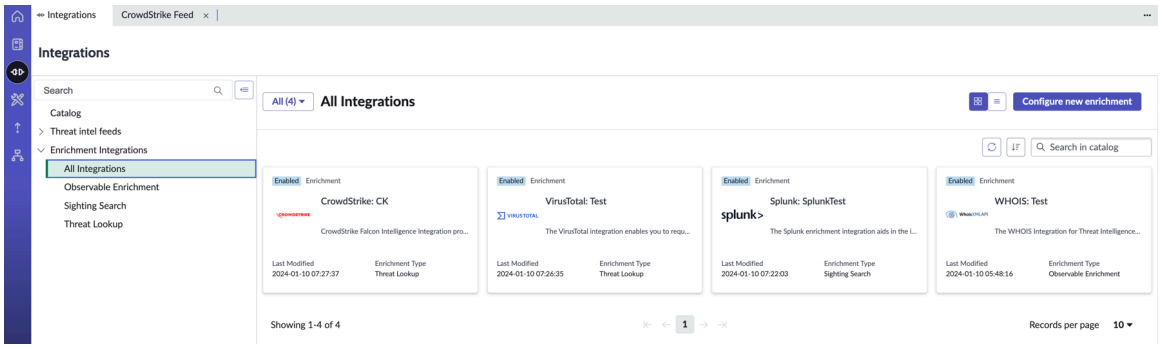
모든 통합 뷰에서 새 보강 구성

모든 통합 뷰에서 또는 옵저버블 보강, 사이팅 검색 또는 위협 조회 섹션에서 각각 새 보강을 구성할 수 있습니다. 모든 통합 보기에서 새 보강을 구성하려면 다음 단계를 수행합니다.

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.

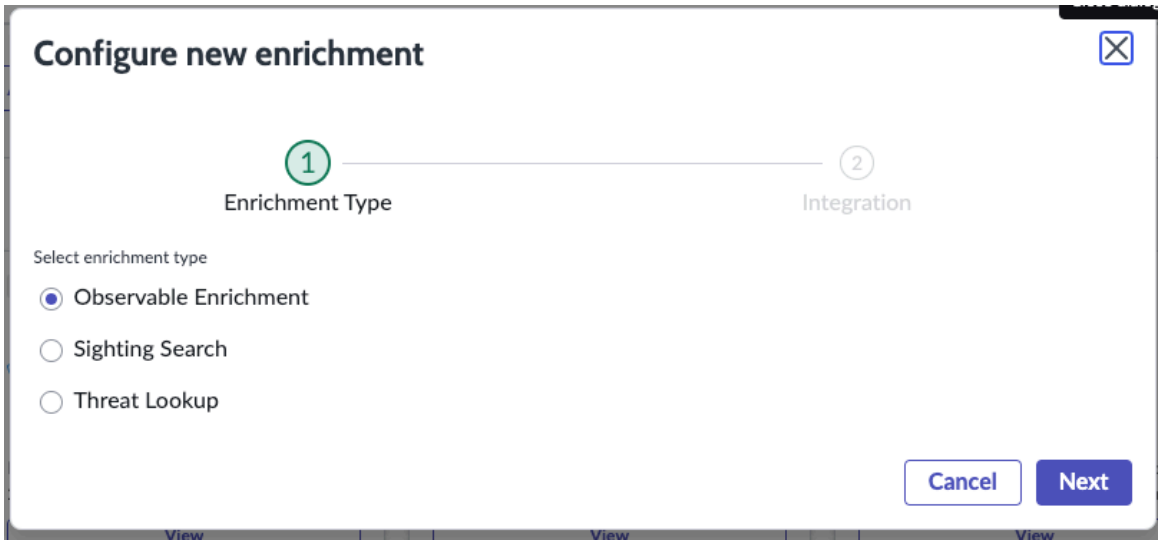
2. 통합 아이콘을 클릭하고 모든 통합 섹션을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



3. 새 보강 구성 작업을 클릭합니다.

새 보강 구성 팝업이 옵저버블 보강, 사이팅 검색 또는 위협 조회의 세 가지 보강 유형과 함께 나타납니다. 구성할 보강 유형을 선택해야 합니다.



4. 보강 유형을 선택하고 다음을 클릭합니다.

그러면 사용 가능한 통합을 표시하는 팝업으로 이동합니다. 구성할 통합을 선택해야 합니다.

5. 사용 가능한 통합 목록에서 통합을 선택하고 선택을 클릭합니다.

그러면 선택한 통합의 새 보강 통합 생성 페이지로 이동합니다. 이 페이지에는 기본적으로 선택한 통합에 대한 상세 정보가 미리 채워져 있습니다. WHOIS 통합을 예로 들 수 있습니다.

6. 새 통합 생성 양식의 필드에 내용을 입력합니다.

새 보강 통합 양식 구성

필드	설명
이름	새 보강 통합의 이름을 입력합니다. 예: WHOIS1.
벤더 이름	벤더의 이름입니다. 선택한 벤더의 상세 정보는 기본적으로 미리 채워져 있습니다. 예: WHOIS.
통합 유형	선택한 통합 유형입니다. 예를 들어 옵저버블 보강입니다. 선택한 통합 유형의 상세 정보는 기본적으로 미리 채워져 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	지원되는 통합 유형은 다음과 같습니다. ○ 관찰 대상 보강 ○ 검색 찾기 ○ 위협 조회
설명	새 보강 통합에 대한 고유한 설명을 입력합니다.

7. 통합 구성 섹션에서 요구 사항에 따라 통합 상세 정보를 구성합니다.

   통합 구성 섹션에는 API 키, API 클라이언트 ID 또는 비밀, 사용자 이름, 암호 등과 같은 구성 상세 정보를 입력해야 합니다. 이러한 구성 상세 정보는 통합에 따라 다릅니다.

8. 저장 작업을 클릭하여 보강 통합 구성을 저장하고 생성합니다.

   제공된 상세 정보가 확인되고 기본적으로 보강 통합의 상태는 사용 안 함입니다.

9. (선택 사항) 통합 구성을 초안으로만 저장하려면 초안으로 저장 작업을 클릭합니다. 초안 상태로 저장되면 사용자는 통합을 활성화할 수 없습니다.

   구성 상세 정보가 확실하지 않은 경우 초안으로 저장 옵션을 사용할 수 있습니다. 구성 상세 정보를 얻은 후 초안 버전에 나머지 정보를 채우고 생성할 수 있습니다.

10. 보강 통합을 활성화하려면 활성화를 클릭합니다.

    보강 통합이 활성화되었습니다.

11. 카탈로그 페이지 또는 보강 통합 페이지에서 필요한 통합 타일의 작업 메뉴를 사용하여 특정 보강 통합을 활성화, 비활성화 또는 삭제할 수도 있습니다.

옵저버블 보강 구성

하나 이상의 옵저버블에 대해 위협 인텔리전스 보강을 수행하여 알려진 보안 위협과 연관이 있는지 여부를 확인할 수 있습니다. 실행되는 구현은 활성화한 구현에 따라 다릅니다.

시작하기 전에

필요한 역할: sn_sec_tisc.admin

는 위협 인텔리전스 보안 센터 현재 WHOIS 통합에 대해서만 옵저버블 보강을 지원합니다. 자세한 내용은 Whois 통합 구성 및 사용 문서를 참조하십시오.

> **주:**
> 보강 통합 모듈은 기능을 지원하는 통합 중 하나 이상이 애플리케이션에 설치된 경우에만 표시됩니다.

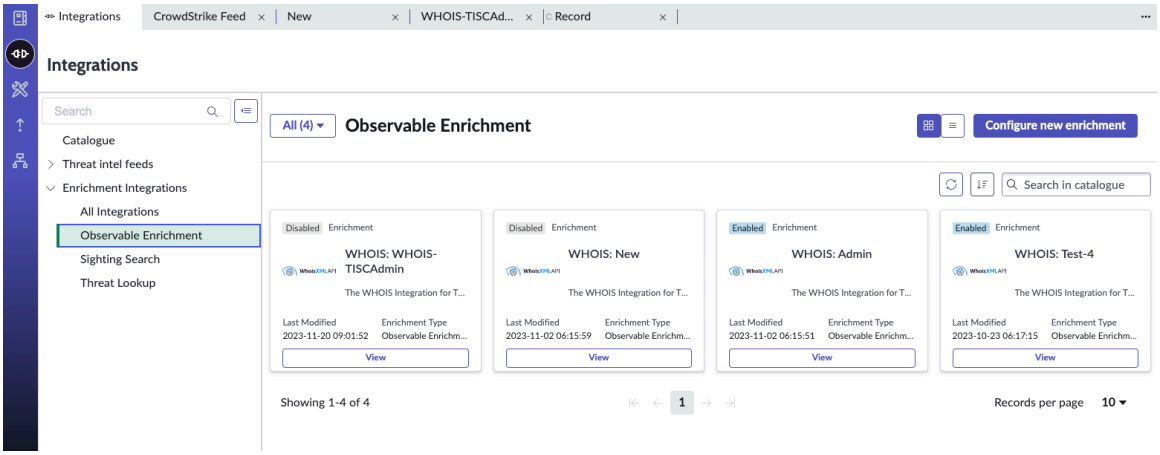
이 태스크 정보

옵저버블 보강 섹션에는 통합 유형이 옵저버블 보강인 통합만 포함됩니다. 이 섹션에는 활성화하고 사용할 수 있는 구성된 각 통합 구현에 대한 카드가 표시됩니다.

프로시저

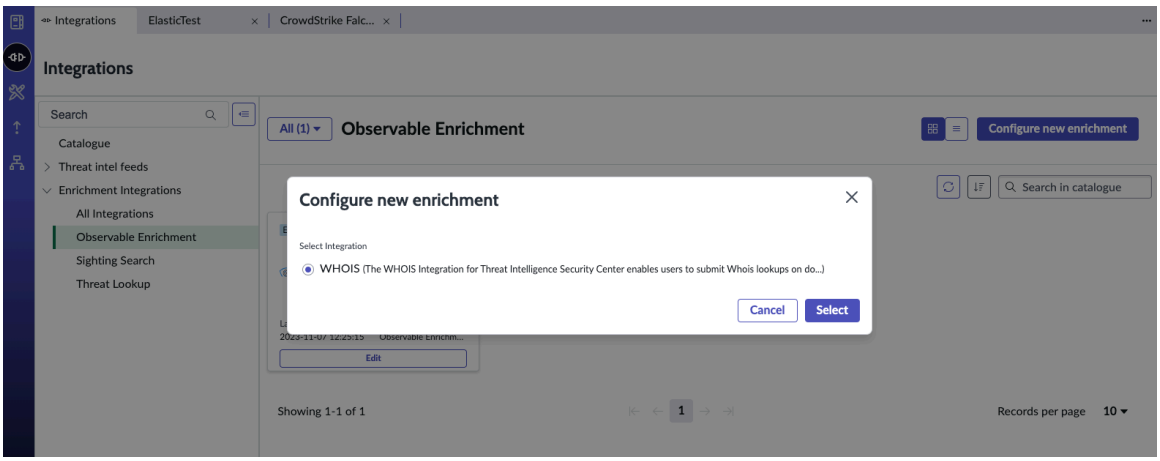
1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 통합 아이콘을 클릭하고 옵저버블 보강 섹션을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

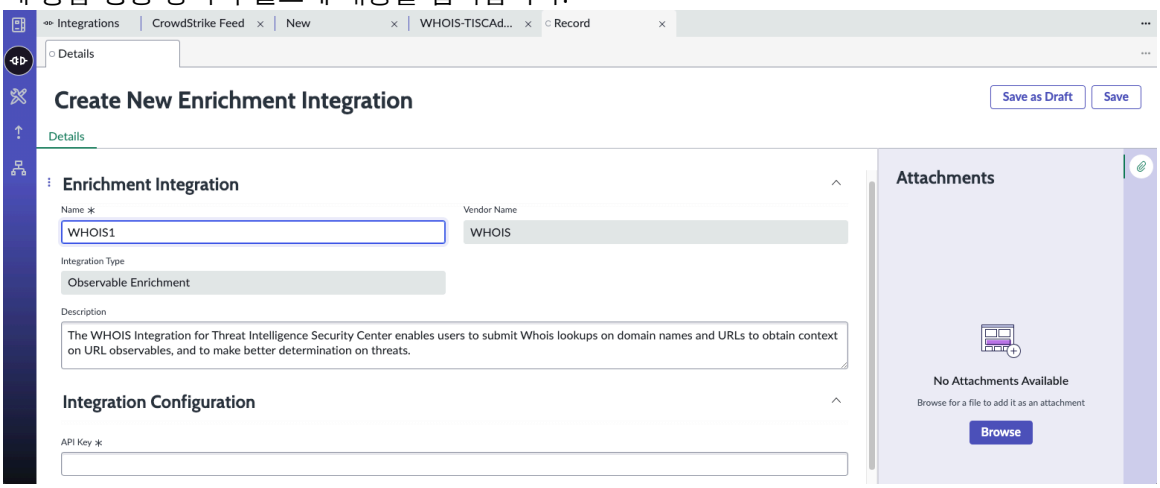


3. 새 보강 구성 작업을 클릭합니다.
그러면 사용 가능한 통합을 표시하는 팝업으로 이동합니다. 구성해야 하는 통합을 선택해야 합니다.

4. 사용 가능한 통합 목록에서 통합을 선택하고 선택을 클릭합니다.
그러면 선택한 통합의 새 보강 통합 생성 페이지로 이동합니다. 이 페이지에는 기본적으로 선택한 통합에 대한 상세 정보가 미리 채워져 있습니다. WHOIS 통합을 예로 들 수 있습니다.



5. 새 통합 생성 양식의 필드에 내용을 입력합니다.



6. 통합 구성 섹션에서 요구 사항에 따라 통합 상세 정보를 구성합니다.
통합 구성 섹션에는 API 키, API 클라이언트 ID 또는 비밀, 사용자 이름, 암호 등과 같은 구성 상세 정보를 입력해야 합니다. 이러한 구성 세부정보는 앱마다 다릅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

7. 저장 작업을 클릭하여 새 보강 통합 구성을 저장하고 생성합니다.
   저장 또는 사용 작업을 클릭하면 제공된 통합 구성을 사용하여 통합의 유효성이 확인됩니다. 기본적으로 보강 통합의 상태는 사용 안 함으로 설정됩니다.
8. 초안으로 저장 작업을 클릭하여 보강 구성에 대한 업데이트만 저장하고 생성하지 않습니다.
   구성 상세 정보가 확실하지 않은 경우 초안으로 저장 옵션을 사용할 수 있습니다. 구성 상세 정보를 얻은 후 초안 버전에 나머지 정보를 채우고 생성할 수 있습니다.
9. 보강 통합을 활성화하려면 활성화를 클릭합니다.
   보강 통합이 활성화되었습니다. 카탈로그 페이지 또는 보강 통합 페이지에서 필요한 통합 타일의 작업 메뉴를 사용하여 특정 보강 통합을 활성화, 비활성화 또는 삭제할 수도 있습니다.

Sighting 검색 구성

하나 이상의 옵저버블에 대해 사이팅 검색을 수행하여 조직 로그에서 옵저버블이 관찰된 횟수를 확인할 수 있습니다. 선택한 일 수 또는 날짜 범위 내에서 옵저버블에 대해 사이팅 검색을 수행할 수 있습니다.

시작하기 전에

필요한 역할: sn_sec_tisc.admin

> **주:**
> 보강 통합 모듈은 기능을 지원하는 통합 중 하나 이상이 애플리케이션에 설치된 경우에만 표시됩니다.

에서는 위협 인텔리전스 보안 센터 다음 통합에 대해서만 사이팅 검색을 지원합니다.

- Splunk 검색
- Elasticsearch

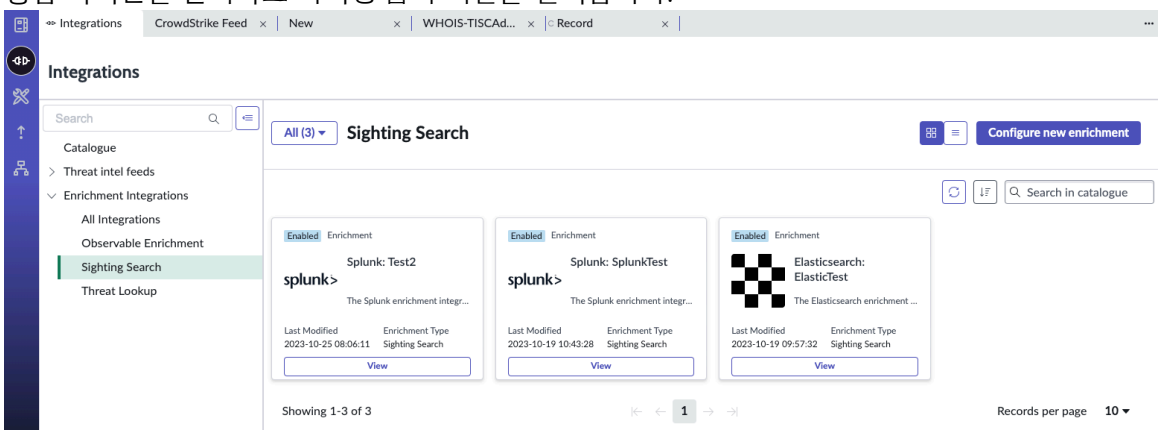
이 태스크 정보

사이팅 검색 섹션에는 통합 유형이 사이팅 검색인 통합만 포함됩니다.

이 섹션에는 활성화하고 사용할 수 있는 구성된 각 통합 구현에 대한 카드가 표시됩니다.

프로시저

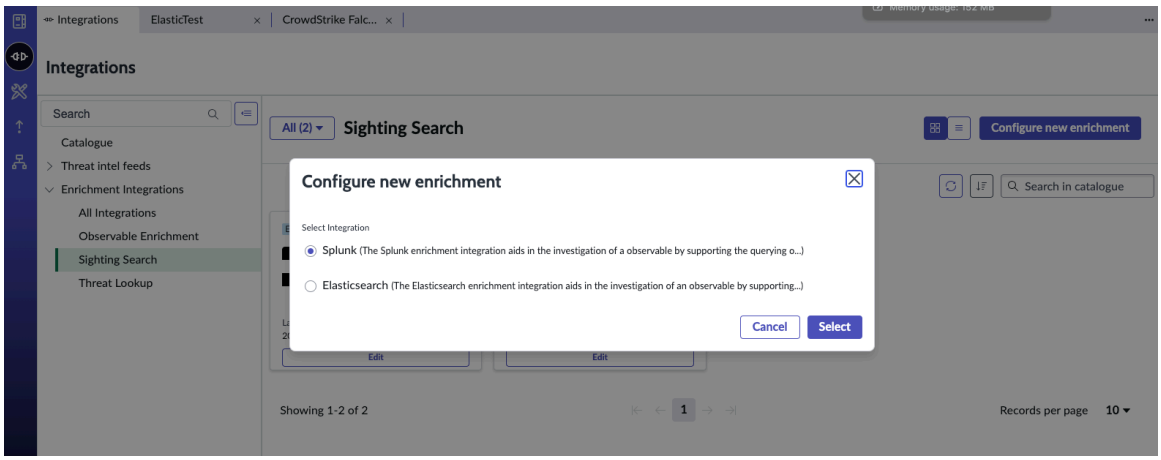
1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 통합 아이콘을 클릭하고 사이팅 검색 섹션을 선택합니다.



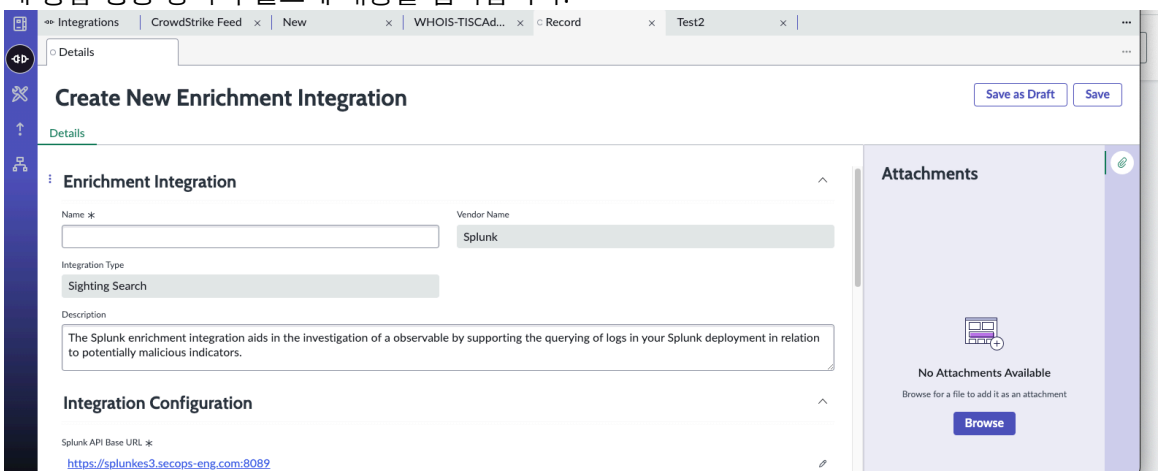
3. 새 보강 구성 작업을 클릭합니다.
   그러면 사용 가능한 통합을 표시하는 팝업으로 이동합니다. 구성해야 하는 통합을 선택해야 합니다.
4. 사용 가능한 통합 목록에서 통합을 선택하고 선택을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

그러면 선택한 통합의 새 보강 통합 생성 페이지로 이동합니다. 이 페이지에는 기본적으로 선택한 통합에 대한 상세 정보가 미리 채워져 있습니다. 예를 들어 Splunk 통합입니다.



5. 새 통합 생성 양식의 필드에 내용을 입력합니다.



6. 통합 구성 섹션에서 요구 사항에 따라 통합 상세 정보를 구성합니다.
통합 구성 섹션에는 API 키, API 클라이언트 ID 또는 비밀, 사용자 이름, 암호 등과 같은 구성 상세 정보를 입력해야 합니다. 이러한 구성 세부정보는 앱마다 다릅니다.
7. 저장 작업을 클릭하여 새 보강 통합 구성을 저장하고 생성합니다.
제공된 상세 정보가 확인되고 기본적으로 보강 통합의 상태는 사용 안 함입니다.
8. 초안으로 저장 작업을 클릭하여 보강 구성에 대한 업데이트만 저장하고 생성하지 않습니다.
구성 상세 정보가 확실하지 않은 경우 초안으로 저장 옵션을 사용할 수 있습니다. 구성 상세 정보를 얻은 후 초안 버전에 나머지 정보를 채우고 생성할 수 있습니다.
9. 보강 통합을 활성화하려면 활성화를 클릭합니다.
보강 통합이 활성화되었습니다. 카탈로그 페이지 또는 모든 통합 페이지에서 필요한 통합 타일의 작업 메뉴를 사용하여 특정 보강 통합을 활성화할 수도 있습니다.

사이팅 검색에 대한 쿼리 정의

관찰 대상 조사의 일환으로 사용자 환경에서 옵저버블의 보급을 찾는 데 사용되는 쿼리를 정의하기 위해 사이팅 검색 구성을 사용할 수 있습니다.

사이팅 검색에 대한 쿼리 보기

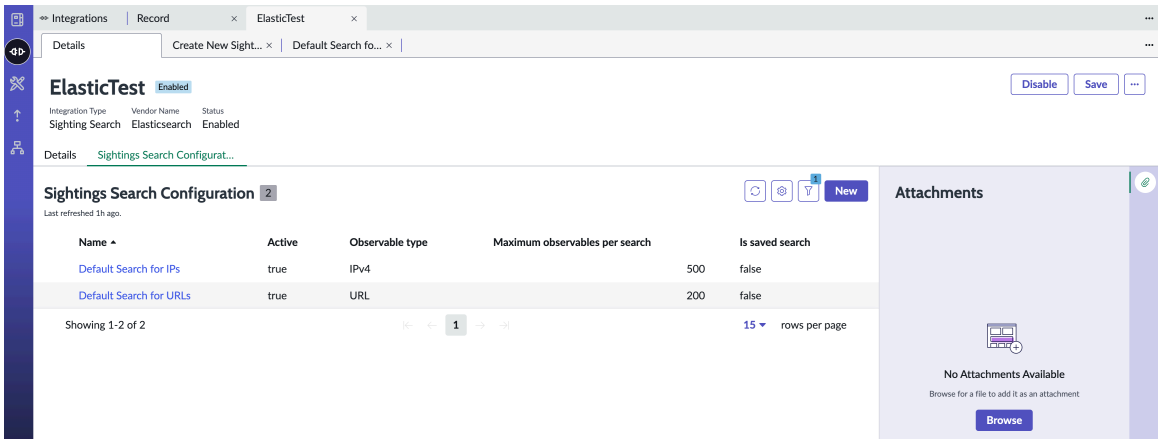
필요한 역할: sn_sec_tisc.admin

목격 검색 구성을 보려면 다음 단계를 수행하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터 〉 통합.
2. 통합 페이지에서 다음으로 이동합니다. 보강 통합 〉 검색 찾기.
3. 사이팅 검색 구성을 보려는 통합을 찾고 편집을 클릭합니다.
4. 사이팅 검색 구성 탭을 선택합니다.

   사이팅 검색 구성 목록을 볼 수 있습니다.



5. 구성의 상세 정보를 보려면 필요한 사이팅 검색 구성을 클릭합니다.
6. 테스트 사이팅 검색 쿼리를 생성하려면 테스트 사이팅 검색 쿼리 생성 작업을 클릭합니다.

   주:
   테스트 사이팅 검색 쿼리 생성 작업은 사이팅 검색 쿼리 매개변수를 구성한 경우에만 작동합니다. 자세한 내용은 사이팅 검색 매개변수 사용 문서를 참조하십시오.

7. 테스트 사이팅 검색 쿼리 생성 팝업에서 쉼표, 줄 바꿈, 탭 또는 파이프 구분 기호를 사용하여 여러 옵저버블을 입력하거나 붙여넣어 테스트 쿼리를 생성합니다.
8. 생성을 클릭하여 테스트 사이팅 검색 쿼리를 생성합니다.
9. 사이팅 검색 구성 탭에서 다음 작업을 수행할 수도 있습니다.
   a. 사이팅 검색 구성 목록을 새로 고치려면 아이콘을 클릭합니다.
   b. 사이팅 검색 구성에서 목록 작업을 수행하려면 아이콘을 클릭합니다.

      다음 두 목록 작업을 수행할 수 있습니다.
      - 열 편집: 이 작업을 사용하여 기존 열을 추가 또는 제거하고 요구 사항에 따라 순서를 수정할 수 있습니다.
      - 너비 재설정: 이 작업을 사용하여 열의 너비를 재설정할 수 있습니다.

   c. 조건에 따라 목격 검색 구성을 필터링하려면 아이콘을 클릭합니다.

      값 1은 필터링에 하나의 조건이 사용됨을 나타냅니다.

한숨 쉬는 검색 구성 작성

필요한 역할: sn_sec_tisc.admin

Maximum observables per search = "maximum number of observables that can be substituted in a single search query"

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

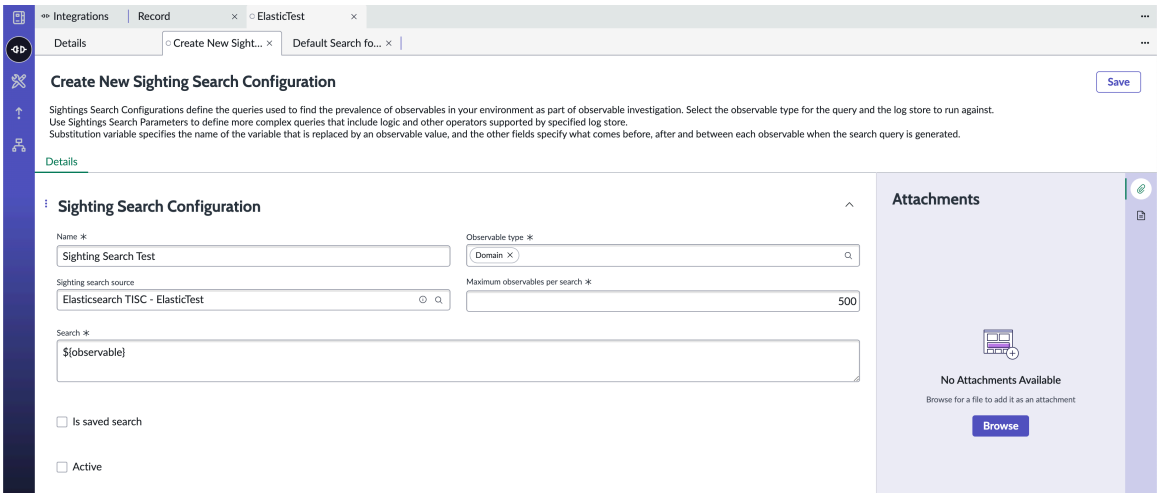
Search = "Search query that should be executed in sighting search source.
Search query can contain substitution variables that would be substituted with observables of specific type as configured in sighting search parameters when sighting search query is formed"

사이팅 검색 구성을 만들려면 다음 단계를 수행합니다.

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터 〉 통합.
2. 통합 페이지에서 다음으로 이동합니다. 보강 통합 〉 검색 찾기.
3. 사이팅 검색 구성을 보려는 통합을 찾고 편집을 클릭합니다.
4. 사이팅 검색 구성 탭을 선택합니다.

   사이팅 검색 구성 목록을 볼 수 있습니다.

5. 사이팅 검색 구성을 만들려면 새로 만들기를 클릭합니다.



6. 양식에서 필드를 채웁니다.

사이팅 검색 구성 생성

필드	설명
이름	목격 검색 구성의 이름입니다.
옵저버블 유형	옵저버블 범주의 유형을 정의합니다.
관찰 검색 소스	통합을 위해 구성된 소스를 정의합니다.
검색당 최대 옵저버블	검색 쿼리가 여러 쿼리로 분할되기 전의 옵저버블 수입니다. 이 통합에 대해 이 값을 500으로 설정합니다.
검색	네이티브 검색 문자열을 추가하여 쿼리를 만듭니다. 예: ${observable}.
저장된 검색 여부	저장된 검색을 실행합니다. 즉, 이름 필드는 저장된 검색의 이름과 일치해야 합니다.
활성	쿼리는 활성 옵션이 선택된 경우에만 실행됩니다.

7. 저장을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사이팅 검색 매개변수 사용

지정된 로그 저장소에서 지원하는 논리 및 기타 연산자를 포함하는 보다 복잡한 쿼리를 정의하는 사이팅 검색 매개변수를 사용할 수 있습니다.

사이팅 검색 매개변수 보기

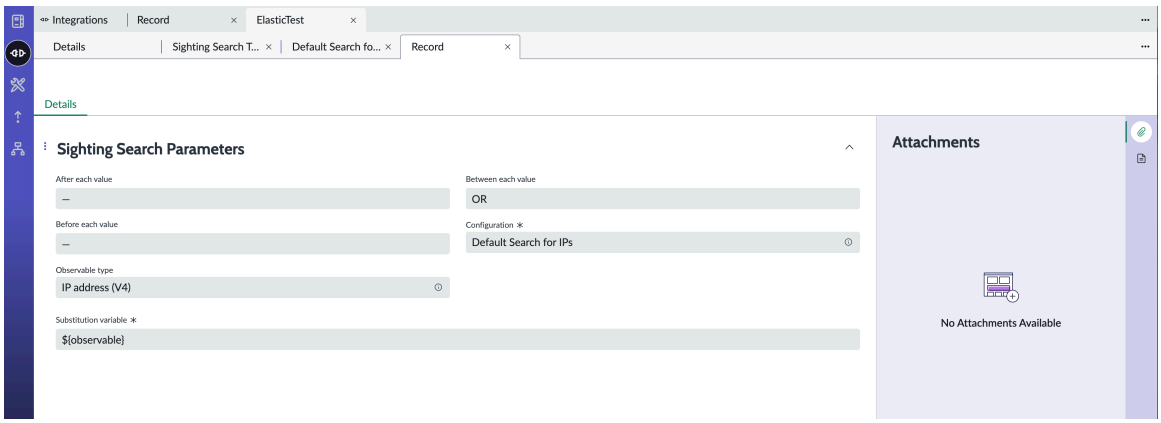
필요한 역할: sn_sec_tisc.admin

사이팅 검색 매개변수를 보려면 다음 단계를 수행하십시오.

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터 〉 통합.
2. 통합 페이지에서 다음으로 이동합니다. 보강 통합 〉 검색 찾기.
3. 사이팅 검색 구성을 보려는 통합을 찾고 편집을 클릭합니다.
4. 사이팅 검색 구성 탭을 선택합니다.

   사이팅 검색 구성 목록을 볼 수 있습니다.

5. 구성의 상세 정보를 보려면 필요한 사이팅 검색 구성을 클릭합니다.



6. 사이팅 검색 매개변수 탭을 선택합니다.

   사이팅 검색 매개변수 목록을 볼 수 있습니다.

7. 매개변수의 상세 정보를 보려면 필요한 사이팅 검색 매개변수를 클릭하십시오.
8. 사이팅 검색 매개변수 탭에서 다음 작업을 수행할 수도 있습니다.
   a. 사이팅 검색 매개변수 목록을 새로 고치려면 아이콘을 클릭합니다.
   b. 사이팅 검색 매개변수에 대한 목록 작업을 수행하려면 아이콘을 클릭합니다.

      열 편집: 이 작업을 사용하여 기존 열을 추가 또는 제거하고 요구 사항에 따라 순서를 수정할 수 있습니다.

   c. 조건을 기준으로 목격 검색 매개변수를 필터링하려면 아이콘을 클릭합니다.

      값 1은 필터링에 하나의 조건이 사용됨을 나타냅니다.

Sighting 검색 매개변수 작성

###

```
Configured Query: ${Observable}
```


© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Observables Substitutes for Sightings search: Obs1 , Obs2

Query: {Before each Value}Obs1{After each Value}{Between each value}{Before each Value}Obs2{After each Value}

Let observables are: 172.32.31.41 & 192.168.10.12

Query Formed with below configuration will be: “ip_address = 172.32.31.41 OR ip_address = 192.168.10.12”

사이팅 검색 매개변수를 생성하려면 다음 단계를 수행합니다.

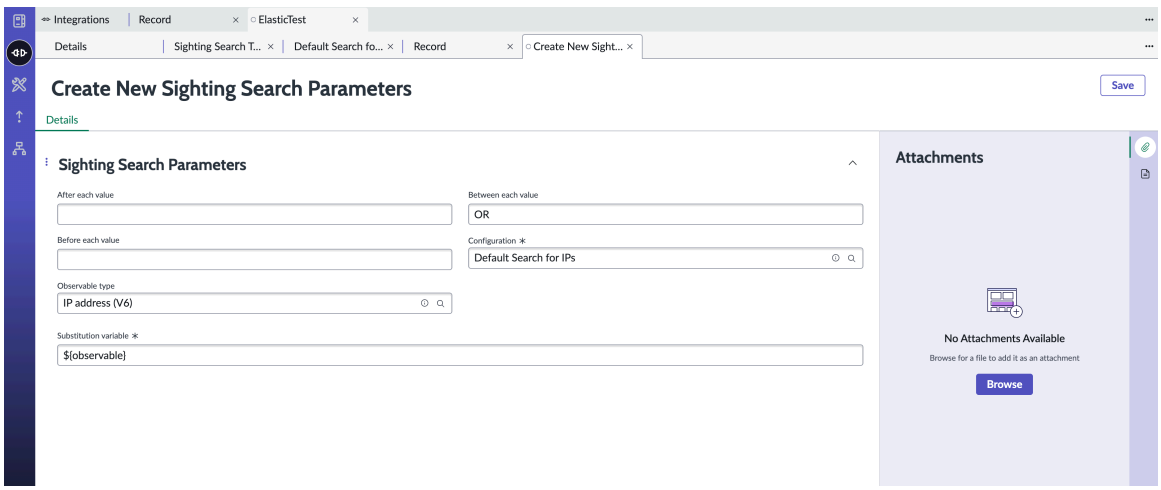
1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터 〉 통합.
2. 통합 페이지에서 다음으로 이동합니다. 보강 통합 〉 검색 찾기.
3. 사이팅 검색 구성을 보려는 통합을 찾고 편집을 클릭합니다.
4. 사이팅 검색 구성 탭을 선택합니다.

   사이팅 검색 구성 목록을 볼 수 있습니다.

5. 구성의 상세 정보를 보려면 필요한 사이팅 검색 구성을 클릭합니다.
6. 사이팅 검색 매개변수 탭을 선택합니다.

   사이팅 검색 매개변수 목록을 볼 수 있습니다.

7. 사이팅 검색 매개변수를 생성하려면 새로 만들기를 클릭합니다.



8. 양식에서 필드를 채웁니다.

사이팅 검색 매개변수 생성

필드	설명
각 값 뒤	검색 쿼리가 생성될 때 각 옵저버블 뒤의 사이팅 검색 매개변수입니다.
각 값 사이	검색 쿼리가 생성될 때 각 옵저버블 간의 사이팅 검색 매개변수입니다. 예: OR.
각 값 앞	검색 쿼리가 생성될 때 각 옵저버블 앞에 있는 사이팅 검색 매개변수입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
구성	검색 매개변수의 구성 상세 정보입니다.
옵저버블 유형	옵저버블 범주의 유형을 정의합니다.
대체 변수	옵저버블 값으로 대체되는 변수의 이름을 지정합니다.

9. 저장을 클릭합니다.

위협 조회 구성

선택한 옵저버블에 대한 조회를 수행하도록 위협 조회를 구성할 수 있습니다. 옵저버블이 Threat Intelligence에서 인식하는 유형인 경우 옵저버블에 맬웨어가 있는지 검사되고 결과가 반환됩니다. 하나 이상의 옵저버블에 대해 위협 조회를 수행하여 옵저버블의 악성여부를 확인할 수 있습니다.

시작하기 전에
필요한 역할: sn_sec_tisc.admin

> **주:**
> 보강 통합 모듈은 기능을 지원하는 통합 중 하나 이상이 애플리케이션에 설치된 경우에만 표시됩니다.

는 위협 인텔리전스 보안 센터 다음 통합에 대해서만 위협 조회를 지원합니다.

- VirusTotal
- CrowdStrike 인텔리전스

자세한 내용은 위협 조회 문서를 참조하십시오.

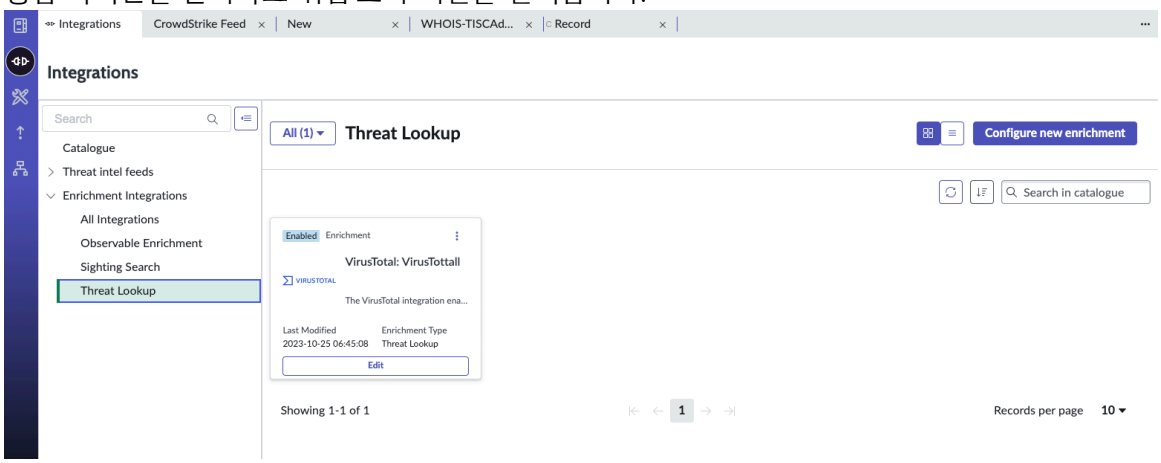
이 태스크 정보
위협 조회 섹션에는 통합 유형이 위협 조회인 통합만 포함됩니다.

이 섹션에는 활성화하고 사용할 수 있는 구성된 각 통합 구현에 대한 카드가 표시됩니다.

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.

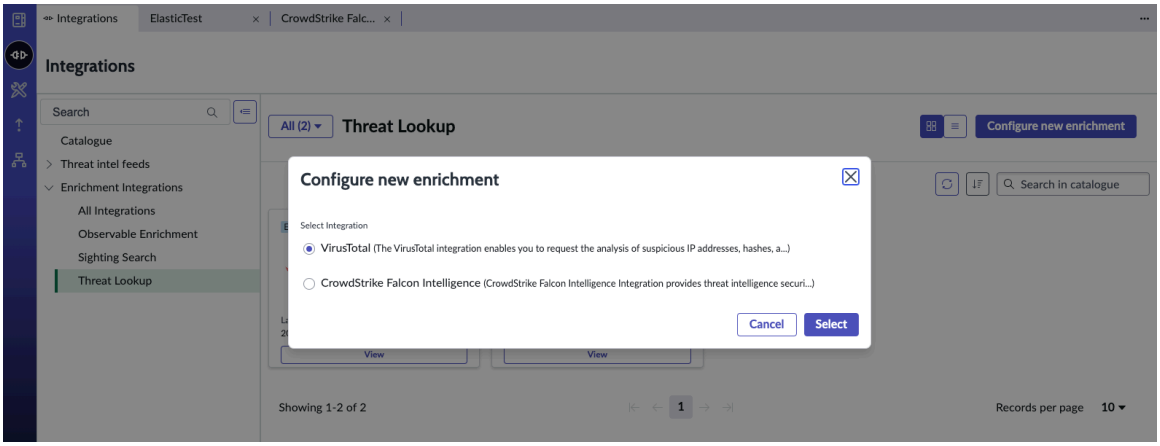
2. 통합 아이콘을 클릭하고 위협 조회 섹션을 선택합니다.



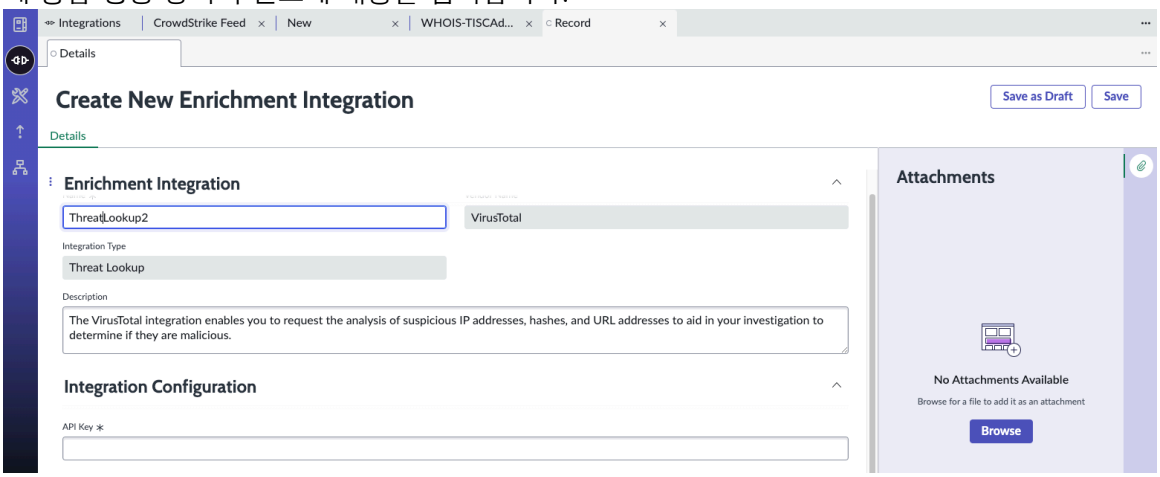
3. 새 보강 구성 작업을 클릭합니다.
그러면 사용 가능한 통합을 표시하는 팝업으로 이동합니다. 구성해야 하는 통합을 선택해야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 사용 가능한 통합 목록에서 통합을 선택하고 선택을 클릭합니다.
그러면 선택한 통합의 새 보강 통합 생성 페이지로 이동합니다. 이 페이지에는 기본적으로 선택한 통합에 대한 상세 정보가 미리 채워져 있습니다. 예를 들어 VirusTotal 통합입니다.



5. 새 통합 생성 양식의 필드에 내용을 입력합니다.



6. 통합 구성 섹션에서 요구 사항에 따라 통합 상세 정보를 구성합니다.
통합 구성 섹션에는 API 키, API 클라이언트 ID 또는 비밀, 사용자 이름, 암호 등과 같은 구성 상세 정보를 입력해야 합니다. 이러한 구성 세부정보는 앱마다 다릅니다.
7. 저장 작업을 클릭하여 새 보강 통합 구성을 저장하고 생성합니다.
제공된 상세 정보가 확인되고 기본적으로 보강 통합의 상태는 사용 안 함입니다.
8. 초안으로 저장 작업을 클릭하여 보강 구성에 대한 업데이트만 저장하고 생성하지 않습니다.
구성 상세 정보가 확실하지 않은 경우 초안으로 저장 옵션을 사용할 수 있습니다. 구성 상세 정보를 얻은 후 초안 버전에 나머지 정보를 채우고 생성할 수 있습니다.
9. 보강 통합을 활성화하려면 활성화를 클릭합니다.
보강 통합이 활성화되었습니다. 카탈로그 페이지 또는 보강 통합 페이지에서 필요한 통합 타일의 작업 메뉴를 사용하여 특정 보강 통합을 활성화, 비활성화 또는 삭제할 수도 있습니다.

위협 조회 평판 계산기 보기

위협 조회 찾기 계산기를 보고 통합에 대한 옵저버블 결과를 계산할 수 있습니다.

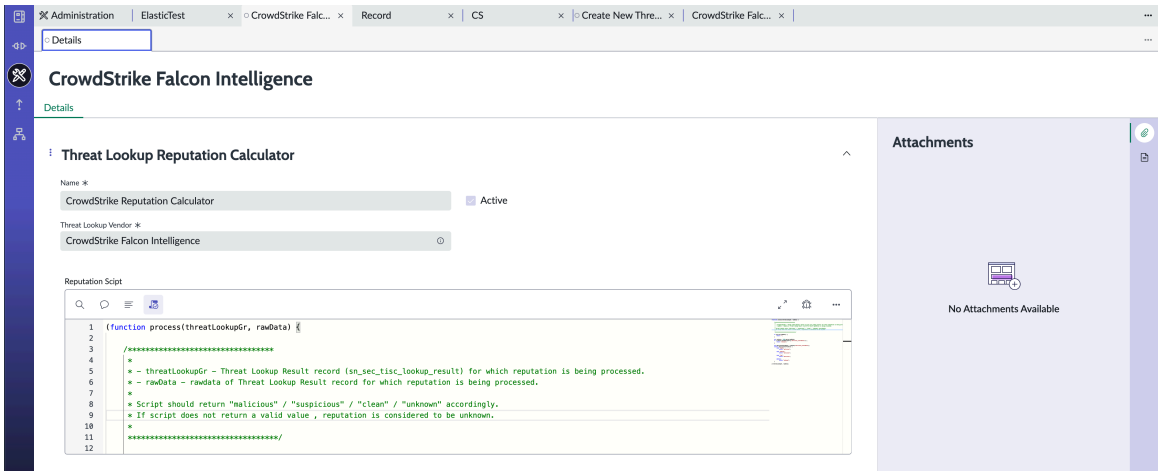
시작하기 전에
필요한 역할: sn_sec_tisc.admin

위협 조회 평판 계산기에 대한 자세한 내용은 문서를 참조하십시오 위협 조회 평판 계산기 관리.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터 〉 관리.
2. 위협 조회 평판 계산기 섹션을 선택합니다.
   위협 조회 평판 계산기 목록을 볼 수 있습니다.
3. 계산기의 세부 정보를 보려면 필요한 위협 조회 평판 계산기를 클릭하십시오.



4. 위협 조회 평판 계산기 섹션에서 다음 작업을 수행할 수도 있습니다.

   a. 위협 조회 평판 계산기 목록을 새로 고치려면 아이콘을 클릭합니다.

   b. 위협 조회 평판 계산기에서 목록 작업을 수행하려면 아이콘을 클릭합니다.

      다음 두 목록 작업을 수행할 수 있습니다.

      - 열 편집: 이 작업을 사용하여 기존 열을 추가 또는 제거하고 요구 사항에 따라 순서를 수정할 수 있습니다.
      - 너비 재설정: 이 작업을 사용하여 열의 너비를 재설정할 수 있습니다.

   c. 조건에 따라 위협 조회 평판 계산기를 필터링하려면 아이콘을 클릭합니다.

      값 1은 필터링에 하나의 조건이 사용됨을 나타냅니다.

TISC API 참조

다음 표에서는 보강에 도움이 되는 API 엔드포인트 참조를 제공합니다.

TISC API

API	설명
TISC API - POST /sn_sec_tisc/threat_intel_data/observables	이 API는 옵저버블과 기타 연관된 위협 인텔리전스 데이터 간의 관계를 포함하여 옵저버블 데이터를 검색합니다.
TISC API - POST /sn_sec_tisc/threat_intel_data/add_observables	이 API는 옵저버블 소스 기록을 생성하여 TISC(위협 인텔리전스 보안 센터) 애플리케이션에 유효한 옵저버블을 추가합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

TISC API 엔드포인트에 대한 자세한 내용은 API 구현에 대한 REST API 참조 섹션 및 servicenow.com/docs 에 대한 참조에서 TISC API 를 참조하십시오.

TISC 통합

이 섹션에서는 Threat Intelligence 통합을 구성하고 활성화하기 위한 지침을 제공합니다.

관찰 대상 보강

옵저버블 보강 WhoIs 워크플로우는 선택한 옵저버블에 대해 보강을 수행합니다. 옵저버블이 WhoisXML API 통합에서 인식되는 유형인 경우 옵저버블이 보강됩니다.

> **주:**
> 위협 인텔리전스 보안 센터는 WHOIS 통합에 대해서만 옵저버블 보강을 지원합니다.

Whois 통합

Whois 통합을 사용하면 도메인 이름 및 URL에 대한 Whois 조회를 제출하여 URL 옵저버블에 대한 컨텍스트를 얻고 위협에 대한 더 나은 결정을 내릴 수 있습니다.

Whois 통합 구성 및 사용

Whois 통합을 사용하려면 먼저 ServiceNow Store에서 다운로드해야 하며 Whois의 유효한 계정이 있어야 합니다.

시작하기 전에

필요한 역할: sn_sec_tisc.admin

위협 인텔리전스 보안 센터 및 Whois 옵저버블 통합 플러그인이 필요합니다.

프로시저

1. 인스턴스를 사용하여 **Threat Intelligence Security Center**에 액세스합니다.
2. 에서 통합을 다운로드합니다. ServiceNow Store.
3. 설치가 완료되면 작업 공간 〉 위협 인텔리전스 보안 센터.
4. 선택 통합 〉 보강 통합 〉 모든 통합.
5. 또는 다음으로 이동할 수 있습니다. 통합 〉 보강 통합 〉 모든 통합 〉 관찰 대상 보강.
6. **WHOIS** 카드에서 새 보강 구성을 클릭하여 **WHOIS** 통합을 구성합니다.
7. 새 보강 구성 양식의 필드에 내용을 입력합니다.

보강 통합

필드	설명
이름	새 보강 통합의 이름을 입력합니다. 예: WHOIS.
벤더 이름	벤더의 이름입니다. 선택한 벤더의 상세 정보가 기본적으로 채워집니다. 예: WHOIS.
통합 유형	선택한 통합 유형입니다. 예를 들어 위협 조회입니다.
설명	새 보강 통합에 대한 설명을 입력합니다. 예를 들어 WHOIS 통합에 대한 설명은 다음과 같습니다. 위협 인텔리전스 보안 센터용 WHOIS 통합을 통해 사용자는 도메인 이름 및 URL에 대한 Whois 조회를 제출하여 URL 옵저버블에

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	대한 컨텍스트를 얻고 위협에 대한 더 나은 결정을 내릴 수 있습니다.

8. 통합 구성 섹션으로 드릴다운합니다.
9. WHOIS 사이트에서 취득한 **API** 키를 입력하거나 붙여넣습니다.
10. 저장을 클릭합니다.
    통합 상세 정보가 확인되고 기본적으로 WHOIS 통합의 상태는 비활성화됩니다.
11. 활성화를 클릭하여 WHOIS 통합을 활성화합니다.

결과
구성된 후에는 위협 인텔리전스 보안 센터의 옵저버블에 대한 보강을 수행하기 위해 WHOIS를 선택할 수 있습니다.

Shodan 통합

Shodan은 전 세계 연결된 장치의 서비스 배너 정보를 분석하는 검색 엔진입니다.

Shodan 통합은 다음 옵저버블에 대해 보강을 수행합니다.

- IP 주소
- URL
- 도메인

Shodan 통합 구성 및 사용

Shodan 통합을 사용하려면 먼저 스토어에서 다운로드 ServiceNow 해야 합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.admin

프로시저

1. 인스턴스를 사용하여 **Threat Intelligence Security Center**에 액세스합니다.
2. 에서 통합을 다운로드합니다. ServiceNow Store.
3. 설치가 완료되면 작업 공간 〉 위협 인텔리전스 보안 센터.
4. 선택 통합 〉 보강 통합 〉 모든 통합.
5. 또는 다음으로 이동할 수 있습니다. 통합 〉 보강 통합 〉 모든 통합 〉 관찰 대상 보강.
6. **Shodan** 카드에서 새 보강 구성을 클릭하여 통합을 구성합니다.
7. 새 보강 구성 양식의 필드에 내용을 입력합니다.

보강 통합

필드	설명
이름	새 보강 통합의 이름을 입력합니다. 예를 들어, Shodan입니다.
벤더 이름	벤더의 이름입니다. 선택한 벤더의 상세 정보가 자동으로 채워지며 기본적으로 이 필드는 읽기 전용입니다. 예를 들어, Shodan입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
통합 유형	선택한 통합 유형입니다. 예를 들어 옵저버블 보강입니다.
설명	새 보강 통합에 대한 설명을 입력합니다. 예를 들어 Shodan 통합에 대한 설명은 다음과 같습니다. Shodan은 전 세계 연결된 장치의 배너 정보를 분석하는 데 도움이 됩니다.

8. 통합 구성 섹션으로 드릴다운합니다.
9. Shodan 포털에서 획득한 **API** 키를 입력하거나 붙여넣습니다.
10. 저장을 클릭합니다.
    통합 상세 정보가 확인되고 기본적으로 상태는 사용 안 함입니다.
11. 통합을 사용하려면 활성화를 클릭하십시오.

검색 찾기

이 섹션에서는 TISC 사이팅 검색 및 탄력적 검색 통합에 대해 설명합니다.

Elasticsearch 통합 시작하기

Elasticsearch 보강 통합은 로그를 검색하고 관련 사이팅 정보를 옵저버블에 추가합니다.

Elasticsearch 통합 구성 및 활성화

Elasticsearch는 Security Operations와 쉽게 통합되는 분산형 RESTful 검색 및 분석 엔진입니다.

시작하기 전에
Elasticsearch를 사용하려면 먼저 ServiceNow Store에서 다운로드해야 합니다.

필요한 역할: sn_sec_tisc.admin

- Elasticsearch 통합을 사용하려면 먼저 위협 인텔리전스 보안 센터 플러그인을 설치하고 활성화해야 합니다.
- Elasticsearch 프로필에서 Elasticsearch API 기본 URL, Kibana 기본 URL, 사용자 이름 및 암호를 가져옵니다.

프로시저

1. 인스턴스를 사용하여 **Threat Intelligence Security Center**에 액세스합니다.
2. 에서 통합을 다운로드합니다. ServiceNow Store.
3. 설치가 완료되면 작업 공간 〉 위협 인텔리전스 보안 센터.
4. 선택 통합 〉 보강 통합 〉 모든 통합.
5. 또는 다음으로 이동할 수 있습니다. 통합 〉 보강 통합 〉 모든 통합 〉 검색 찾기

   주:
   구성된 통합은 일련의 카드로 나타납니다.

6. **Elasticsearch** 카드에서 새 보강 구성을 클릭하여 **Elasticsearch** 통합을 구성합니다.
7. 새 보강 구성 양식의 필드에 내용을 입력합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보강 통합

필드	설명
이름	사이팅 검색 구성의 이름을 입력합니다.
벤더 이름	벤더의 이름입니다. 선택한 벤더의 상세 정보가 기본적으로 채워집니다. 예를 들어 Elasticsearch입니다.
통합 유형	선택한 통합 유형입니다. 예를 들어 위협 조회입니다.
설명	Elasticsearch 통합에 대한 설명을 입력합니다. 예를 들어, Elasticsearch 보강 통합은 Elasticsearch 배포에서 로그 쿼리를 지원하여 옵저버블을 조사하는 데 도움이 됩니다.
통합 구성	
Elasticsearch API 기준 URL	Elasticsearch 사이트에서 가져온 기본 URL입니다.
Kibana 기본 URL	Kibana 기본 URL입니다. 〔선택사항〕 사용 가능한 경우, Kibana 인스턴스에 대한 링크입니다.
사용자 이름	인텔 Elasticsearch 사용자 이름입니다.
암호	인텔 Elasticsearch 암호입니다.
Elasticsearch 인덱스	Elasticsearch 인덱스입니다. 여기에는 각 인덱스에 고유한 문서가 저장됩니다. 인덱스는 수행된 작업(예: 검색 및 삭제)을 나타내는 소문자 이름으로 식별됩니다.
날짜 범위 필드	구성의 타임스탬프입니다.
최대 행 수	검색할 행의 최대 수입니다.
가장 빠른 결과(일)	일수 단위로 보려는 가장 빠른 결과입니다.
검색 결과에 원시 데이터 샘플 포함	사이팅 검색 결과에 원시 데이터 샘플을 포함하려면 이 옵션을 선택합니다. 반환되는 데이터의 양은 보안 인시던트 응답 속성의 원시 데이터 속성 행 수의 설정에 따라 달라집니다.
MID 서버	활성 MID 서버를 사용하려면 임의를 선택하고, 특정 MID 서버 이름을 선택합니다.

주:
이 통합을 구성하면 워크플로우가 활성화됩니다. 워크플로우를 관리하려면 워크플로우 편집기로 이동합니다.

8. 저장을 클릭합니다.
   통합 세부 사항이 확인되고, 기본적으로 Elasticsearch 통합의 상태는 비활성화입니다.
9. 활성화를 클릭하여 Elasticsearch 통합을 활성화합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

결과
구성된 후에는 위협 인텔리전스 보안 센터의 옵저버블에 대한 사이팅 검색을 수행하기 위해 Elasticsearch를 선택할 수 있습니다.

Splunk 검색 통합 시작하기

Splunk 소프트웨어는 시스템에서 생성된 빅데이터를 검색, 모니터링 및 분석하고 Security Operations와 쉽게 통합됩니다. Splunk 사이팅 검색 통합을 사용하려면 먼저 ServiceNow Store에서 다운로드해야 합니다.

Splunk 통합 구성 및 활성화

Splunk 보강 통합은 로그를 검색하고 관련 사이팅 정보를 추가합니다.

시작하기 전에
Splunk 검색을 사용하려면 먼저 ServiceNow Store에서 다운로드해야 합니다.

필요한 역할: sn_sec_tisc.admin

- Splunk 검색 통합을 사용하려면 먼저 위협 인텔리전스 보안 센터 플러그인을 설치하고 활성화해야 합니다.
- Splunk와 Splunk 검색을 가져오고 Splunk 인스턴스에서 API 기준 URL, 링크 URL, 사용자 이름 및 암호를 가져옵니다.

프로시저

1. 인스턴스를 사용하여 **Threat Intelligence Security Center**에 액세스합니다.
2. 에서 통합을 다운로드합니다. ServiceNow Store.
3. 설치가 완료되면 작업 공간 〉 위협 인텔리전스 보안 센터.
4. 선택 통합 〉 보강 통합 〉 모든 통합.
5. 또는 다음으로 이동할 수 있습니다. 통합 〉 보강 통합 〉 모든 통합 〉 검색 찾기
   구성된 통합은 일련의 카드로 나타납니다.
6. **Splunk** 검색 카드에서 새 보강 구성을 클릭하여 **Splunk** 검색 통합을 구성합니다.
7. 새 보강 구성 양식의 필드에 내용을 입력합니다.

보강 통합

필드	설명
이름	사이팅 검색 구성의 이름을 입력합니다.
벤더 이름	벤더의 이름입니다. 선택한 벤더의 상세 정보가 기본적으로 채워집니다. 예를 들면 Splunk입니다.
통합 유형	선택한 통합 유형입니다. 예를 들어 위협 조회입니다.
설명	Splunk 통합에 대한 설명을 입력합니다. 예를 들어 Splunk 보강 통합은 Splunk 배포에서 잠재적으로 악의적인 표시기와 관련된 로그 쿼리를 지원함으로써 옵저버블을 조사하는 데 도움이 됩니다.
통합 구성	
Splunk API 기준 URL	Splunk 사이트에서 얻은 기본 URL입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
링크 URL	〔선택사항〕 Splunk 웹 인터페이스로 연결되는 링크 URL입니다(사용 가능한 경우).
사용자 이름	인텔 Elasticsearch 사용자 이름입니다.
암호	인텔 Elasticsearch 암호입니다.
최대 행 수	검색할 행의 최대 수입니다.
가장 빠른 결과(일)	일수 단위로 보려는 가장 빠른 결과입니다.
검색 결과에 원시 데이터 샘플 포함	사이팅 검색 결과에 원시 데이터 샘플을 포함하려면 이 옵션을 선택합니다. 반환되는 데이터의 양은 보안 인시던트 응답 속성의 원시 데이터 속성 행 수의 설정에 따라 달라집니다.
직접 배포	온 프레미스 배포 환경.
MID 서버	활성 MID 서버를 사용하려면 임의를 선택하고, 특정 MID 서버 이름을 선택합니다.

주:
이 통합을 구성하면 워크플로우가 활성화됩니다. 워크플로우를 관리하려면 워크플로우 편집기로 이동합니다.

8. 저장을 클릭합니다.
   통합 상세 정보가 확인되고 기본적으로 Splunk 통합의 상태는 사용 안 함입니다.
9. 활성화를 클릭하여 Splunk 통합을 활성화합니다.

결과
구성된 후에는 위협 인텔리전스 보안 센터의 옵저버블에 대해 사이팅 검색을 수행하기 위해 Splunk를 선택할 수 있습니다.

위협 조회

위협 조회 - VirusTotal 및 CrowdStrike Falcon 인텔리전스 워크플로우는 선택한 옵저버블에 대해 조회를 수행합니다. 옵저버블이 VirusTotal 및 CrowdStrike에서 인식하는 유형인 경우 옵저버블에 맬웨어가 있는지 검사되고 결과가 반환됩니다.

TISC VirusTotal 통합

TISC VirusTotal 통합을 사용하면 의심스러운 IP 주소, 파일 해시 및 URL 주소 분석을 요청하여 해당 주소 및 파일 해시가 악성인지 여부를 확인하는 데 도움이 될 수 있습니다.

VirusTotal 통합 구성 및 사용

VirusTotal 통합을 사용하려면 먼저 ServiceNow Store.

시작하기 전에
필요한 역할: sn_sec_tisc.admin

VirusTotal 통합을 활성화하려면 Threat Intelligence Security Center 플러그인이 필요합니다.

프로시저

1. 인스턴스를 사용하여 **Threat Intelligence Security Center**에 액세스합니다.
2. 에서 통합을 다운로드합니다. ServiceNow Store.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 설치가 완료되면 VirusTotal에 액세스하여 VirusTotal 프로필에서 API 키를 가져옵니다.
4. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
5. 선택 통합 〉 보강 통합 〉 모든 통합.
6. 또는 다음으로 이동할 수 있습니다. 통합 〉 보강 통합 〉 모든 통합 〉 위협 조회
7. 새 보강 구성을 클릭하여 **VirusTotal** 통합을 구성합니다.
8. 새 보강 구성 양식의 필드에 내용을 입력합니다.

보강 통합

필드	설명
이름	새 보강 통합의 이름을 입력합니다. 예: VirusTotal
벤더 이름	벤더의 이름입니다. 선택한 벤더의 상세 정보가 기본적으로 채워집니다. 예: VirusTotal
통합 유형	선택한 통합 유형입니다. 예를 들어 위협 조회입니다.
설명	새 보강 통합에 대한 설명을 입력합니다.

9. 통합 구성 섹션으로 드릴다운합니다.
10. VirusTotal 사이트에서 취득한 **API** 키를 입력하거나 붙여넣습니다.
11. 저장을 클릭합니다.
    통합 상세 정보가 확인되고 기본적으로 VirusTotal 통합의 상태는 사용 안 함입니다.
12. 사용을 클릭하여 VirusTotal 통합을 사용하도록 설정합니다.

결과
구성된 후에는 위협 인텔리전스 보안 센터에서 옵저버블에 대한 조회를 수행하기 위해 VirusTotal을 선택할 수 있습니다.

TISC CrowdStrike Falcon Intelligence 통합

CrowdStrike Falcon Intelligence는 Security Operations와 쉽게 통합되는 사이버 보안 인텔리전스를 제공합니다.

주:

CrowdStrike Falcon 인텔리전스 통합을 구현하려면 위협 인텔리전스 보안 센터 플러그인이 필요합니다.

CrowdStrike Falcon Intelligence 통합 구성 및 활성화

CrowdStrike Falcon Intelligence를 사용하려면 먼저 ServiceNow Store에서 다운로드하여 적절한 클라이언트 ID 및 클라이언트 비밀을 추가해야 합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 위협 인텔리전스 보안 센터 애플리케이션을 설치하고 활성화해야 합니다.
- CrowdStrike Falcon Intelligence 프로파일에서 API 클라이언트 ID 및 API 클라이언트 비밀을 가져옵니다.
- CrowdStrike Falcon Intelligence 포털 API 범위에서 표시기(Falcon Intelligence)에 대한 읽기 설정을 활성화합니다.

프로시저

1. 인스턴스를 사용하여 **Threat Intelligence Security Center**에 액세스합니다.
2. 에서 통합을 다운로드합니다. ServiceNow Store.
3. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
4. 선택 통합 〉 보강 통합 〉 모든 통합.
5. 또는 다음으로 이동할 수 있습니다. 통합 〉 보강 통합 〉 모든 통합 〉 위협 조회.
6. 새 보강 구성을 클릭하여 **CrowdStrike Falcon** 인텔리전스 통합을 구성합니다.
7. 새 보강 구성 양식의 필드에 내용을 입력합니다.

보강 통합

필드	설명
이름	새 보강 통합의 이름을 입력합니다. 예를 들면 CrowdStrike Falcon Intelligence입니다.
벤더 이름	벤더의 이름입니다. 선택한 벤더의 상세 정보가 기본적으로 채워집니다. 예를 들면 CrowdStrike Falcon Intelligence입니다.
통합 유형	선택한 통합 유형입니다. 예를 들어 위협 조회입니다.
설명	새 보강 통합에 대한 설명을 입력합니다.
통합 구성	
클라이언트 ID	CrowdStrike에서 얻은 클라이언트 ID입니다.
클라이언트 비밀	CrowdStrike에서 얻은 클라이언트 비밀 키입니다.

8. 저장을 클릭합니다.
   통합 상세 정보가 확인되고 기본적으로 CrowdStrike Falcon Intelligence 통합의 상태는 사용 안 함입니다.
9. 활성화를 클릭하여 CrowdStrike Falcon Intelligence 통합을 활성화합니다.

결과
구성된 후에는 Threat Intelligence Security Center에서 옵저버블에 대한 조회를 수행하기 위해 CrowdStrike Falcon Intelligence를 선택할 수 있습니다.

TISC 보안 도구 - EDR

TISC Endpoint Detection and Response(EDR) 통합은 엔드포인트 수준에서 보안 위협을 식별하고 해결하는 데 중점을 둡니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

EDR 네트워크 솔루션은 새로운 위협을 예측 및 선제적으로 차단하고 전반적인 조직의 보안 태세를 강화하는 데 도움이 됩니다.

TISC는 EDR과 같은 다른 보안 도구와 통합함으로써 엔드포인트에 대한 사전 예방적 위협 모니터링을 가능하게 하여 진화하는 위협에 대한 전반적인 보안 태세와 복원력을 향상시킵니다.

관련 정보

CrowdStrike Falcon EDR 통합

CrowdStrike Falcon EDR 통합

Falcon EDR과의 CrowdStrike 통합은 TISC의 인텔리전스를 기반으로 지속적인 모니터링 및 실시간 경고를 가능하게 합니다.

이러한 통합은 보안 운영을 간소화하고 조직의 비즈니스에 대한 잠재적 위험을 줄이는 데 도움이 될 수 있습니다.

Crowdstrike Falcon EDR 통합 구성

Falcon EDR 통합을 사용하려면 CrowdStrike 먼저 스토어에서 다운로드하여 ServiceNow Store 적절한 클라이언트 ID 및 클라이언트 비밀을 추가해야 합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.admin

- 위협 인텔리전스 보안 센터 애플리케이션을 설치하고 활성화해야 합니다.
- Falcon 콘솔에서 API 클라이언트 ID 및 API 클라이언트 비밀 CrowdStrike 을 가져옵니다.
- CrowdStrike Falcon 포털 API 범위에서 **IOC** 관리: 읽기 및 쓰기 권한을 활성화합니다.

프로시저

1. 인스턴스를 사용하여 **Threat Intelligence Security Center**에 액세스합니다.
2. 에서 통합을 다운로드합니다. ServiceNow Store.
3. 선택 통합 〉 보안 도구 〉 **EDR**.
4. 새 보안 도구 구성을 클릭하여 Falcon EDR 통합을 구성합니다CrowdStrike.
5. **CrowdStrike Falcon EDR** 옵션을 선택합니다.
6. 새 보안 도구 구성 양식의 필드에 내용을 입력합니다.

새 보강 통합 작성

필드	설명
이름	새 보안 도구 통합의 이름을 입력합니다. 예를 들어 Falcon EDR입니다 CrowdStrike .
벤더 이름	벤더의 이름입니다. 선택한 벤더의 상세 정보가 기본적으로 채워집니다. 예를 들어 Falcon EDR입니다 CrowdStrike .
설명	새 보안 도구 통합에 대한 설명을 입력합니다.
통합 유형	통합 유형을 표시하는 옵션입니다.
통합 범주	통합 범주를 표시하는 옵션입니다.
통합 구성	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
기본 URL	기본 URL은 CrowdStrike API 기본 URL입니다. 기본값은 입니다 https://api.crowdstrike.com. 자세한 내용은 https://falcon.crowdstrike.com/documentation/page/a2a7fc0e/crowdstrike-oauth2-based-apis#k9578c40 문서를 참조하십시오.
클라이언트 ID	에서 가져온 CrowdStrike클라이언트 ID입니다. 자세한 내용은 https://falcon.crowdstrike.com/documentation/page/a2a7fc0e/crowdstrike-oauth2-based-apis 문서를 참조하십시오.
클라이언트 비밀	에서 CrowdStrike가져온 클라이언트 비밀 키입니다. 자세한 내용은 https://falcon.crowdstrike.com/documentation/page/a2a7fc0e/crowdstrike-oauth2-based-apis 문서를 참조하십시오.
모든 유형의 옵저버블에 대한 만료 기간(일)	EDR로 CrowdStrike 전송될 때 모든 유형의 옵저버블에 적용되는 만료 기간(일)입니다. 주: 이 옵션은 만료 시간이 특정 옵저버블 유형에 대해 설정되지 않은 경우 만료 기간을 대체하는 것입니다.
IP 옵저버블 만료 시간	옵저버블의 IP 유형이 EDR로 CrowdStrike 전송될 때 적용되는 만료 기간(일)입니다.
도메인 옵저버블 만료 시간	옵저버블이 EDR로 CrowdStrike 전송될 때 옵저버블의 도메인 유형에 적용되는 만료 기간(일)입니다.
해시 옵저버블 만료 시간	옵저버블이 EDR로 CrowdStrike 전송될 때 옵저버블의 해시 유형에 적용되는 만료 기간(일)입니다.

7. 저장을 클릭합니다.
   통합 상세 정보가 확인되고 기본적으로 EDR 통합의 CrowdStrike 상태가 비활성화됩니다.
8. **EDR** 통합을 활성화하려면 활성화를 CrowdStrike 클릭하십시오.

주:
Falcon EDR 통합에는 CrowdStrike 여러 구성이 허용됩니다.

EDR에 옵저버블 전송

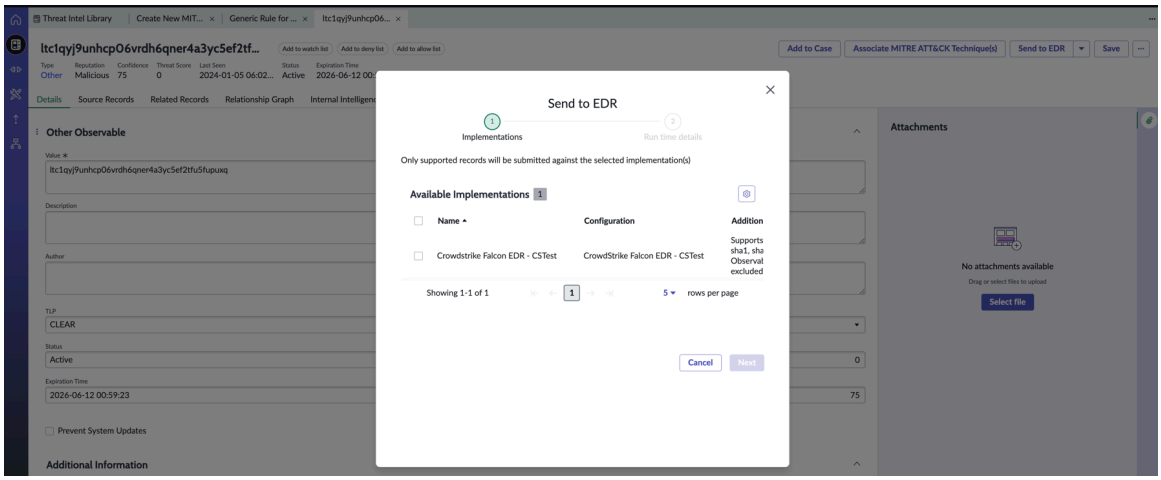
관찰 대상을 EDR 보안 도구로 보냅니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

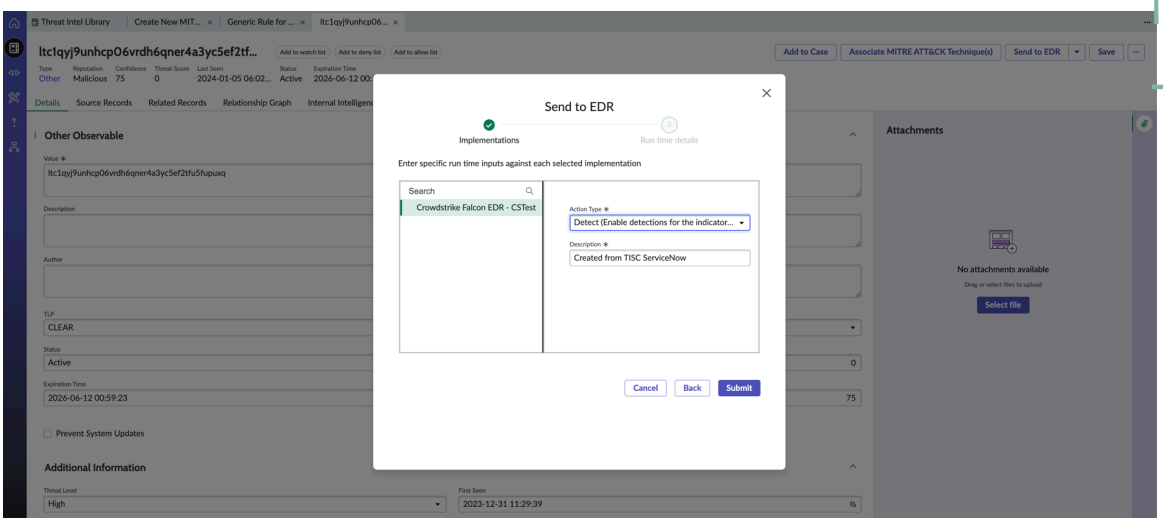
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 위협 인텔 라이브러리 아이콘을 클릭합니다.
3. 이동 옵저버블 〉 모든 옵저버블.
4. 옵저버블 기록을 엽니다.
5. EDR에 보내기를 선택합니다.
   EDR 구현 에 전송 모달 화면이 표시됩니다.
6. 목록에서 필요한 구현을 선택합니다.



7. 다음을 클릭합니다.
8. 작업 유형 및 구현 설명과 같은 실행 시간 상세 정보를 선택합니다.



구현 실행 시간 중 상세 정보에 사용할 수 있는 옵션은 다음과 같습니다.CrowdStrike

- 작업 없음(나중에 사용할 수 있도록 표시기를 저장하지만 아무 작업도 수행하지 않음): 옵저버블 양식 보기에서 옵저버블의 위협 심각도는 Falcon EDR에 대한 CrowdStrike 선택 사항입니다.
- 탐지(기록의 위협 심각도에서 표시기에 대한 탐지 활성화): 옵저버블 양식 뷰에서 위협 심각도는 Falcon EDR에 필수 CrowdStrike 입니다. 선택한 옵저버블에 대해 옵저버블의 위협 심각도가 비어 있으면 안 됩니다.

9. 제출을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

선택한 액션이 실행되고, EDR에 옵저버블 전송 실행이 시작되었다는 정보 메시지가 표시됩니다.

주:

- 실행이 시작되거나 완료되면 작업 메모가 양식 뷰의 활동 스트림에 게시됩니다.
- EDR에 보내기 작업은 케이스 기록에 대한 아티팩트 탭의 옵저버블 목록에서도 사용할 수 있습니다. 자세한 내용은 케이스 또는 케이스 작업에 아티팩트 추가 문서를 참조하십시오.

Microsoft Defender for EDR 통합

Microsoft Defender for EDR과의 통합을 통해 CTI(사이버 위협 인텔리전스) 분석가는 악의적이거나 의심스러운 IP 주소, 도메인, 파일 해시 및 URL을 Microsoft Defender에 자동으로 푸시하여 지속적인 모니터링 및 실시간 경고를 수행할 수 있습니다.

포털에서 **Microsoft Defender Microsoft Azure** 등록 및 구성

포털에 Microsoft Defender EDR Microsoft Azure 을 등록하고 애플리케이션에 대한 읽기 및 쓰기 액세스 권한을 부여합니다.

시작하기 전에
필요한 역할: 애플리케이션 개발자, 테넌트 관리자.

프로시저

1. Microsoft Azure 포털에 로그인합니다.
2. 검색 상자에 App registrations# 입력하고 **New** registration을 클릭합니다.
3. 애플리케이션의 이름과 리디렉션 URI를 입력하고 등록을 클릭합니다.
   예제 이름은 ###### Microsoft Defender입니다. 리디렉션 URI는 애플리케이션에 대한 관리자 동의를 제공하는 동안 사용됩니다.
4. 앱 등록 페이지에서 3단계에서 등록한 애플리케이션을 선택합니다.
5. 관리에서 인증서 및 비밀을 선택합니다.
6. 클라이언트 암호를 만들려면 새 클라이언트 암호를 선택합니다.
7. 클라이언트 비밀을 복사하여 저장합니다.

   클라이언트 비밀을 잊어버린 경우 새 클라이언트 비밀을 생성할 수 있습니다.
8. 다음으로 이동 관리 〉 **API** 권한.
9. 권한 추가를 클릭합니다.
10. API 권한 요청 창에서 조직에서 사용하는 **API** 탭을 클릭합니다.
11. **WindowsDefenderATP**를 검색하여 선택합니다.
12. WindowsDefenderATP 권한에서 애플리케이션 권한을 선택합니다.
    이 권한을 사용하도록 설정하면 애플리케이션이 로그인한 사용자 없이 백그라운드 서비스 또는 디먼으로 실행됩니다.
13. 다음 애플리케이션 수준 권한을 추가하고 새로 추가된 API 권한에 대한 관리자 동의를 부여합니다.

권한	권한 표시 이름
Ti.ReadWrite.All	읽기 및 쓰기 표시기

Microsoft Defender for EDR 통합 설치 및 구성

ServiceNow Store에서 Microsoft Defender for EDR 통합을 설치하고 구성합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_sec_tisc.admin

- 위협 인텔리전스 보안 센터 ServiceNow Store에서 애플리케이션을 설치하고 활성화해야 합니다.
- Microsoft Defender for EDR 콘솔에서 API 테넌트 ID, 클라이언트 ID 및 클라이언트 비밀을 가져옵니다.

프로시저

1. ServiceNow Store에서 Microsoft Defender for EDR 통합을 다운로드하여 설치합니다.
2. 인스턴스를 사용하여 .## ##### ## ##
3. 에서 통합을 다운로드합니다. ServiceNow Store.
4. 선택 통합 〉 보안 도구 〉 **EDR**.
5. 새 소스 도구 통합 구성을 클릭합니다.
6. **Microsoft Defender for EDR** 옵션을 선택합니다.
7. 선택을 클릭합니다.
8. 양식의 다음 필드에 내용을 입력합니다.

Microsoft Defender for EDR 통합 구성

필드	설명
이름	새 보안 도구 통합 구성의 이름입니다. 예를 들어 Microsoft Defender for EDR 통합이 있습니다.
통합 범주	통합 범주를 표시하는 옵션입니다.
벤더 이름	벤더의 이름입니다. 선택한 벤더의 상세 정보가 기본적으로 채워집니다.
통합 유형	통합 유형을 표시하는 옵션입니다.
설명	새 보안 도구 통합 구성에 대한 설명을 입력합니다.
통합 구성	
기본 URL	기본 URL은 Microsoft Defender for EDR API 기본 URL입니다. 기본값은 입니다 https://api.securitycenter.microsoft.com/ .
테넌트 ID	Microsoft Defender에서 가져온 테넌트 ID입니다.
클라이언트 ID	Microsoft Defender에서 가져온 클라이언트 ID입니다.
클라이언트 비밀	Microsoft Defender에서 가져온 클라이언트 비밀 키입니다.
미리 채워진 제목(제출 시 사용됨)	미리 채워진 제목은 Microsoft Defender에 옵저버블을 제출하는 동안 사용되는 기본 제목을 정의합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	이러한 세부 정보는 기본적으로 표시되므로 EDR에 제출하는 동안 매번 다시 입력할 필요가 없습니다.
미리 채워진 설명(제출 시 사용됨)	미리 채워진 설명은 Microsoft Defender에 옵저버블을 제출하는 동안 사용되는 기본 제목을 정의합니다. 이러한 세부 정보는 기본적으로 표시되므로 EDR에 제출하는 동안 매번 다시 입력할 필요가 없습니다.
모든 유형의 옵저버블에 대한 만료 기간(일)	옵저버블이 Microsoft Defender EDR로 전송될 때 옵저버블에 적용되는 만료 기간(일)입니다. 주: 이 옵션은 만료 시간이 특정 옵저버블 유형에 대해 설정되지 않은 경우 만료 기간을 대체하는 것입니다.
옵저버블의 IP 유형에 대한 만료 기간(일)	옵저버블의 IP 유형이 Microsoft Defender EDR로 전송될 때 적용되는 만료 기간(일)입니다.
옵저버블의 도메인 유형에 대한 만료 기간(일)	옵저버블이 Microsoft Defender EDR로 전송될 때 옵저버블의 도메인 유형에 적용되는 만료 기간(일)입니다.
해시 옵저버블 유형의 만료 기간(일)	옵저버블이 Microsoft Defender EDR로 전송될 때 옵저버블의 해시 유형에 적용되는 만료 기간(일)입니다.

9. 필요한 구성 정보를 추가한 후 저장을 클릭합니다.
10. 새 Microsoft Defender EDR 통합을 저장한 후 사용을 클릭하여 구성을 사용하도록 설정합니다. 보강 통합이 성공적으로 활성화되었다는 확인 메시지가 표시됩니다.

결과
통합이 구성되면 위협 인텔 라이브러리에서 Microsoft Defender EDR을 지원하는 모든 유형의 옵저버블을 선택한 다음 옵저버블을 EDR로 보낼 수 있습니다. 자세한 내용은 EDR에 옵저버블 전송 문서를 참조하십시오.

Microsoft Defender EDR에 대한 시스템 속성

다음은 Microsoft Defender EDR에 대한 시스템 속성을 자세히 설명합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.admin

프로시저

1. 다음으로 이동 모두 〉 **Glide** 속성 카탈로그 〉 **Glide** 속성.
2. Microsoft Defender 속성을 검색합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
sn_tisc_defender.rate_limiter.minute	이를 통해 사용자는 MS Defender에 EDR을 보내는 속도를 분 단위로 제한할 수 있습니다. ○ 유형: 정수 ○ 값: 100
sn_tisc_defender.rate_limiter.hour	이를 통해 사용자는 시간 단위로 MS Defender에 EDR을 보내는 속도를 제한할 수 있습니다. ○ 유형: 정수 ○ 값: 1500

EDR에 옵저버블 전송

관찰 대상을 EDR 보안 도구로 보냅니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 위협 인텔 라이브러리 아이콘을 클릭합니다.
3. 이동 옵저버블 〉 모든 옵저버블.
4. 옵저버블 기록을 엽니다.
5. EDR에 보내기를 선택합니다.
   EDR 구현 에 전송 모달 화면이 표시됩니다.
6. 목록에서 필요한 구현을 선택합니다.
   예를 들어 Microsoft Defender EDR과 연결된 구현을 선택합니다.
7. 다음을 클릭합니다.
8. 구현 제목 및 설명과 같은 실행 시간 상세 정보를 선택합니다.
9. 제출을 클릭합니다.
   선택한 작업이 실행되고, EDR에 옵저버블 전송 실행이 시작되었다는 정보 메시지가 표시되며, 실행이 완료된 후 이 실행의 결과를 활동 스트림에서 확인할 수 있습니다.

   주:
   실행이 시작되거나 완료되면 작업 메모가 양식 뷰의 활동 스트림에 게시되고 그에 따라 실행 진행률을 확인할 수 있습니다.

TISC 보안 도구 - 방화벽

TISC 보안 도구 - 방화벽은 네트워크에 대한 무단 액세스를 방지합니다. Palo Alto와 TISC의 통합은 위협 인텔리전스 데이터와 함께 ServiceNow EDL(External Dynamic List) 기능을 사용하여 악성 IP 주소, URL 및 도메인을 차단하는 데 도움이 됩니다.

TISC 내에서 다음과 같은 Palo Alto Networks 다른 보안 도구와 통합하여 전체 조직의 네트워크 보안을 강화합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Palo Alto Networks 통합

Palo Alto Networks 통합이 구성되면 위협 분석가가 악성 IP 주소, URL 및 도메인을 EDL(External Dynamic List)에 추가하거나, 비악성 또는 정상으로 확인되면 EDL에서 이러한 항목을 제거할 수 있습니다.

EDL은 외부 웹 서버에서 호스팅되는 텍스트 파일입니다. 이 통합의 경우 이 웹 서버가 Palo Alto Networks 방화벽이 ServiceNow AI Platform 목록, IP 주소, URL 및 도메인에 포함된 객체를 임포트할 수 있도록 허용하는 인스턴스입니다.

Palo Alto Networks를 위한 새 EDL 생성

Palo Alto Networks에 대한 새 EDL(외부 동적 목록)을 작성합니다. EDL을 작성한 후에는 해당 EDL에 대한 항목 작성을 시작할 수 있습니다.

시작하기 전에
필요한 역할: sn_sec_tisc.admin

프로시저

1. 새로 구성된 Palo Alto NGFW 컨피그레이션을 저장한 후 **EDL** 섹션으로 이동합니다.
2. 새로 만들기를 클릭하여 새 EDL(External Dynamic List)을 작성합니다.
3. 양식에서 필드를 채웁니다.

Palo Alto Networks 방화벽 외부 동적 목록 양식

필드	설명
이름	Palo Alto Networks 방화벽 동적 목록 이름입니다.
관찰 대상 유형	선택 목록에서 이 EDL이 허용하는 옵저버블 유형(IP(CIDR 포함), URL 또는 도메인)을 선택합니다.
만료 기간(일)	EDL의 만료 기간입니다. 0(기본값)은 EDL 항목이 만료되지 않음을 나타냅니다. 이 값을 변경하면 입력한 일수 동안 이 항목이 활성화됩니다. 최솟값은 1로 입력할 수 있으며 최댓값은 없습니다. 예를 들어, 11월 1일 오후 2:01에 30 일을 입력하면 EDL은 11월 30일 오후 2:01에 만료됩니다. 그러면 개별 항목을 기준으로 값을 재정의하지 않는 한 이 EDL의 모든 항목은 기본적으로 이 값을 상속합니다.
변경 요청 작성	이 확인란은 EDL 기록에 첨부된 변경 요청 및 변경 작업을 ServiceNow AI Platform 인스턴스에 자동으로 생성하기 위해 기본적으로 선택되어 있습니다. 변경 요청은 Palo Alto Networks Next-Generation Firewall 서버에서 EDL 목록 검색 URL을 구성하는 데 사용됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	방화벽 관리자가 방화벽 정책 또는 규칙 변경에도 사용하는 ServiceNow AI Platform 경우 이 옵션을 사용하는 것이 좋습니다. 요청을 생성한 경우 요청이 종결되면 EDL 목록이 자동으로 활성화됩니다.
설명	Palo Alto Networks 방화벽 동적 목록에 대한 설명입니다. 이름에는 일반적으로 이 EDL에 있을 것으로 예상되는 사이트 및 옵저버블 유형이 포함되며 이 필드를 사용하여 자세한 내용을 확인할 수 있습니다.
변경 요청	변경 요청 생성 확인란을 선택한 경우 EDL이 저장되면 인스턴스에 변경 요청 번호가 표시됩니다 ServiceNow AI Platform . 변경 요청 생성 확인란의 선택을 취소하면 이 필드가 표시되지 않습니다.
IP 주소와 서브넷 주소를 단일 항목으로 결합	IP 주소와 서브넷 주소를 단일 항목으로 결합하는 옵션입니다. 이 확인란을 선택하고 CIDR 유형의 IP가 추가되면 CIDR 범위에 속하는 기존 항목이 자동으로 제거됩니다. 예를 들어, 값이 192.168.1.1인 EDL에 항목이 있고 CIDR 값이 192.168.1.0/24가 동일한 EDL에 추가되면 새 항목의 CIDR 범위 내에 속하므로 초기 IP 주소 항목이 제거됩니다. 주: 이 옵션은 옵저버블 유형을 IP로 선택한 경우에만 표시됩니다.
EDL 검색 URL	Palo Alto Networks 방화벽 관리자가 Palo Alto Networks 방화벽의 구성에 사용하는 URL 링크가 자동으로 생성되어 표시됩니다.

4. 필요에 따라 EDL을 더 생성하고 추가합니다.
   EDL은 Palo Alto Networks 외부 동적 목록 목록에 표시됩니다.

관련 정보

Palo Alto EDL 승인 규칙

Palo Alto EDL 승인 규칙

승인 규칙을 사용하면 사용자가 EDL 항목을 승인하거나 거부하는 데 필요한 승인 작업 플로우를 활성화할 수 있습니다.

시작하기 전에
필요한 역할: sn_sec_tisc.admin

이 태스크 정보
TISC 관리자는 이러한 승인 규칙을 정의하여 승인 요청에 대한 동의를 부여합니다. TISC 관리자는 여기에서 여러 수준의 승인을 정의할 수도 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 새로 구성된 Palo Alto NGFW 구성을 저장한 후 **EDL** 승인 규칙 섹션으로 이동합니다.
2. 새로 만들기를 클릭하여 새 승인 규칙을 만듭니다.
   다음 규칙은 Palo Alto NGFW 통합을 위해 기본 시스템에 미리 구성된 규칙입니다.

미리 구성된 **EDL** 승인 규칙

이름	설명	**EDL** 작업
EDL에 추가하기 위한 승인 규칙	이 승인 규칙을 사용하면 사용자가 EDL에 항목을 추가하기 위한 승인 작업 플로우를 활성화할 수 있습니다.	EDL에 추가
EDL에서 제거하기 위한 승인 규칙	이 승인 규칙을 사용하면 사용자가 EDL에서 항목을 제거하기 위한 승인 작업 플로우를 활성화할 수 있습니다.	EDL에서 제거

3. 양식에 있는 필드를 적절하게 채웁니다.

새 **EDL** 승인 규칙 작성

필드	설명
이름	승인 규칙의 이름입니다.
EDL 작업	EDL 항목을 추가하거나 제거하는 옵션입니다.
EDL	승인이 필요한 EDL을 선택합니다. 이 항목을 비워 두면 모든 EDL이 포함됩니다.
설명	승인 규칙에 대한 설명을 입력합니다.
승인이 필요한 사용자 또는 그룹 선택	
사용자	승인이 필요한 사용자를 선택합니다.
그룹	승인이 필요한 그룹을 선택합니다.
승인자 선택	
사용자	승인할 사용자를 선택합니다.
그룹	승인할 그룹을 선택합니다.
알림	
승인 시 요청자에게 알림	EDL 승인을 요청자에게 알리려면 이 확인란을 선택합니다.
거부 시 요청자에게 알림	EDL 거부를 요청자에게 알리려면 이 확인란을 선택합니다.

4. 저장을 클릭하여 승인 규칙을 확인하고 저장합니다.
5. Enable(활성화)을 클릭하여 승인 규칙을 활성화합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

EDL에 옵저버블 추가

IP, 도메인 및 해시와 같은 옵저버블을 EDL(외부 동적 목록)에 추가합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 위협 분석가 워크벤치 아이콘을 클릭합니다.
3. 이동 옵저버블 〉 모든 옵저버블.
4. 옵저버블 기록을 엽니다.
5. EDL에 추가를 클릭합니다.
   EDL에 추가 모달 화면이 표시됩니다.

EDL에서 옵저버블 제거

EDL에서 옵저버블을 제거합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 위협 분석가 워크벤치 아이콘을 클릭합니다.
3. 이동 옵저버블 〉 모든 옵저버블.
4. 옵저버블 기록을 엽니다.
5. EDL에서 제거를 클릭합니다.
   EDL에서 제거 모달 화면이 표시됩니다.

Palo Alto Networks에 대한 **EDL** 항목 승인

EDL(External Dynamic List) 항목 승인은 사전 구성의 일부입니다. 방화벽이 항목을 검색하고 보안 정책을 적용하려면 EDL에서 항목을 활성화하기 전에 EDL 항목을 승인해야 합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.admin

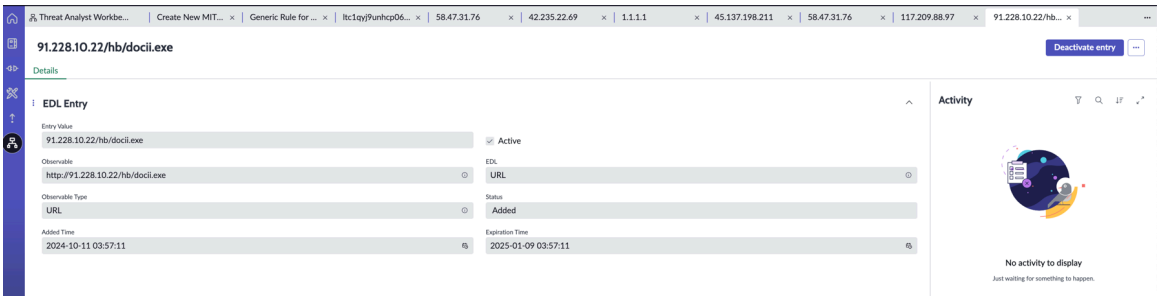
이 태스크 정보
승인 프로세스를 사용하는 경우 EDL 항목은 승인될 때까지 EDL에서 활성화되거나 비활성화되지 않습니다.

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터 〉 위협 분석가 워크벤치.
2. **PAN NGFW** 섹션으로 드릴다운하고 승인할 EDL 레코드를 선택합니다.
3. 내 승인으로 이동합니다.
4. 승인할 EDL 기록을 선택합니다.
5. 승인을 클릭합니다.
6. 내 승인 요청 아래의 상태 열에서 항목을 클릭하여 엽니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

7. EDL 항목을 승인하는 옵션을 선택합니다.
   EDL 항목을 승인하고 활성화되면 Palo Alto Networks는 다음 검색 간격 후에 EDL 항목을 검색합니다. 항목이 검색되면 해당 시점부터 옵저버블이 차단됩니다. 다음 그림에서는 활성 확인란이 선택되어 있고 상태가 추가됨이며 작업 메모에 요청이 승인되었음을 나타냅니다.



Splunk용 **TISC** 추가 기능 개요

앱용 Splunk 위협 인텔리전스 보안 센터(TISC)는 TISC 간의 통합을 제공하여 사용자가 TISC Splunk에서 최신 위협 인텔리전스를 원활하게 임포트하여 Splunk 경보를 모니터링하고 보강할 수 있도록 합니다. 사용자는 표시기 컬렉션을 구성하고, 검색을 수행하고, 대시보드를 활용하여 검색 일치 및 표시기 컬렉션을 효과적으로 분석할 수 있습니다.

와 **TISC** 통합 **Splunk**

와 (TISC)의 Splunk 통합을 위협 인텔리전스 보안 센터 통해 사용자는 관련 위협 인텔리전스 옵저버블 데이터를 필터링하고 로 가져올 수 Splunk있습니다. Splunk내에서 사용자는 이 데이터를 사용하여 보안 경고를 생성할 수 있습니다.

필요한 역할: Splunk 관리자

TISC 추가 기능 애플리케이션을 사용하여 인스턴스에서 옵저버블 ServiceNow TISC 을 끌어올 수 있는 간격을 구성할 수 있습니다.

이 간격은 애플리케이션이 옵저버블 데이터를 요청 ServiceNow 하고 검색할 수 있는 빈도를 결정합니다. 또한 필터를 정의하고 적용하여 인스턴스에서 끌어올 옵저버블을 지정할 수 있습니다 ServiceNow TISC .

옵저버블을 끌어오 ServiceNow면 옵저버블 데이터가 KV 저장소(키-값 저장소)에 Splunk 저장되고 끌어온 옵저버블 집합에 대한 상관관계 규칙을 추가로 작성할 수 있습니다.

ServiceNow TISC 인스턴스에서 사용자 생성

인스턴스에서 유효한 사용자 역할(sn_sec_tisc.api_obs_read_access)을 사용하여 사용자를 ServiceNow TISC 생성할 수 있습니다.

Splunk에 애드온 앱 설치 **TISC**

자세한 내용은 사용자에게 역할 할당 을 참조하십시오.

필요한 역할: Splunk admin

1. 에 *Splunk*로그인합니다.
2. 다음으로 이동 앱 〉 앱 관리 또는 관리 톱니바퀴 아이콘을 클릭합니다.
3. *## ##### ## ##* 해당 *Splunk* 앱을 검색하여 설치합니다.
4. 설치가 완료되면 응용 프로그램이 앱 목록 아래에 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

에서 추가 기능 구성 **TISCSplunk**

아래 절차에 따라 애플리케이션을 구성합니다.

시작하기 전에
필요한 역할: Splunk 관리자

이 태스크 정보
아래 절차에서는 의 TISC 추가 기능 Splunk구성에 대해 설명합니다.

프로시저

1. 왼쪽 탐색 창에서 **Threat Intelligence Security Center for Splunk** 앱을 검색합니다.
2. 작업 열 아래에서 설정을 클릭합니다.
   구성 페이지가 표시되고 계정을 설정할 수 있습니다ServiceNow TISC.
3. 추가를 선택합니다.
4. 양식에서 필드를 채웁니다.

필드	설명
계정 추가	
이름	계정의 고유한 이름입니다.
사용자 이름	계정 ServiceNow 사용자 이름을 입력합니다. 위 단계에서 역할 생성 중에 생성된 사용자에 사용되는 것과 동일한 사용자 이름을 사용할 수 sn_sec_tisc.api_obs_read_access .
암호	계정 암호를 제공하십시오 ServiceNow .
인스턴스 URL	ServiceNow 인스턴스 URL 주소를 제공합니다.

5. 추가를 클릭합니다.
   ServiceNow 인스턴스 계정이 Splunk.
6. 입력 페이지로 이동하여 컬렉션을 생성하고 계정에 대한 ServiceNow 데이터 입력을 관리합니다.
7. 새 입력 생성을 클릭합니다.
   계정에 입력을 ServiceNow 추가할 수 있는 입력 추가 대화 상자가 표시됩니다.

   입력 세트가 정의되면 애플리케이션은 조건을 충족하는 특정 수의 옵저버블을 검색하기 위해 정보를 인스턴스로 TISC 보냅니다.
8. 입력 상세 정보를 적절하게 입력합니다.

필드	설명
이름	입력의 고유 이름입니다. 예를 들어 악성 IP 목록입니다.
계정	계정 ServiceNow 사용자 이름을 입력합니다. 위 단계에서 sn_sec_tisc.api_obs_read_access 역할로 만든 사용자에게 사용되는 것과 동일한 사용자 이름을 사용할 수 있습니다.
간격	에서 데이터를 TISC검색할 시간 간격(초)을 설정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
만료 기간(일)	만료 기간을 일 단위로 설정하는 옵션입니다. **주:** 샘플 만료는 30일로 설정됩니다. 예를 들어 특정 날짜에 데이터를 끌어오면 10,000개의 기록 세트를 검색할 수 있습니다. 이러한 레코드는 내의 KV(키-값) 저장소에 Splunk저장됩니다. 수집된 날짜로부터 기록은 30일 동안 보존됩니다. 31일째 되는 날에는 KV 저장소에서 자동으로 삭제됩니다.
만료되지 않음	수집된 기록을 만료하지 않으려면 이 옵션을 선택합니다.
추가 속성	KV 저장소에 포함할 권장 옵션 목록에서 추가 속성을 추가할 수 있습니다. 속성은 쉼표로 구분해야 합니다. 허용되는 속성 목록은 필수 속성 테이블 다음 테이블에 제공됩니다.
필터	임포트할 조건을 정의하면 데이터가 필터링됩니다. 필터 조건을 설정하기 위해 위협 점수, 신뢰도 수준 및 유형과 같은 필드를 기반으로 기준을 정의할 수 있습니다. 단순 필터 조건의 경우 이 필터링 옵션을 사용할 수 있습니다. 그러나 필터 조건이 더 복잡하고 고급 필터링의 경우 JSON 필터를 추가하도록 선택할 수 있습니다. ○ 허용되는 정수 연산자는 다음과 같습니다. "=", "!=", ">", "<", ">=", "<=" ○ 허용되는 문자열 연산자는 다음과 같습니다. "=", "!=", "IN" 다음은 간단한 필터의 예입니다. {Sample filter format: Allowed Tokens: "threat_score", "confidence", "reputation", "type", "value". Allowed Integer Operators: "=", "!=", ">", "<", ">=", "<=". Allowed String Operators: "=", "!=", "IN". Example: reputation IN ("clean","suspicious","malicious") AND threat_score > 90 AND confidence > 90 AND type = "ip_v4_address"}
JSON	JSON 기반 필터를 사용하면 보다 복잡한 조건을 정의할 수 있습니다. JSON 객체의 상태는 활성 상태여야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	JSON을 사용하여 필터 조건을 적용할 수 있는 고급 필터로 전환하려면 JSON 필터 확인란을 선택합니다.

샘플 고급 필터:

```
{"boolean_operator":"AND","filters":[{"field_name":"reputation","operator":"IN","field_value":"clean,suspicious,malicious"},{"field_name":"threat_score","operator":">","field_value":"90"},{"field_name":"confidence","operator":">","field_value":"90"},{"field_name":"type","operator":"=","field_value":"ip_v4_address"}]}
```

주:
계정은 기본적으로 활성 상태이지만 입력은 기본적으로 비활성 상태입니다. 데이터 임포트를 시작하려면 계정을 활성화해야 합니다. 가능한 필터는 위협 인텔리전스 보안 센터(TISC) 애플리케이션에 옵저버블 소스 기록 추가 의 Observable_filters 섹션을 참조하십시오.

9. 추가를 클릭하여 입력을 추가합니다.
10. 클론 또는 복사를 클릭하여 기존 계정을 기반으로 새 계정을 복사하고 생성합니다.
동일한 기준을 사용하여 데이터를 임포트할 때 중복 항목이 작성되지 않도록 복제하기 전에 입력이 비활성화되었는지 확인하십시오.
11. 데이터를 가져오면 다음 정보가 검색되어 TISC에서 가져온 기록과 함께 KV Splunk 저장소에 저장됩니다.

필드	설명
신뢰도	위협 점수의 정확도와 연결된 신뢰도 수준을 나타냅니다.
kvlookup_created_time	키 값 저장소의 기록 생성 시간을 나타냅니다.
kvlookup_days_till_expiry	KV 저장소에서 기록이 삭제되기까지의 일 수를 나타냅니다.
instance_url	ServiceNow 인스턴스 URL 주소를 나타냅니다.
평판	관련된 엔터티의 평판을 나타냅니다.
source_reported_score	에서 TISC보고된 소스 점수입니다.
sys_id	수신 TISC되는 기록의 시스템 ID입니다.
threat_level	위협의 심각도 수준을 나타냅니다.
threat_score	기록과 연결된 위협 수준을 나타내는 점수입니다.
threat_severity	옵저버블의 위협 심각도를 나타냅니다.
유형	옵저버블 유형을 나타냅니다.
updated_by	기록을 마지막으로 업데이트한 사람에 대한 정보를 제공합니다.
kvlookup_updated_time	키 값 저장소에서 기록이 마지막으로 업데이트된 타임 스탬프를 나타냅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
값	기록의 값입니다. 예를 들어 IP, 해시 등이 있습니다.

추가 속성

필드	설명
additional_context	필요에 따라 추가 컨텍스트를 제공합니다.
attack_phases	LM, MITRE ATT&CK와 같은 킬 체인의 공격 단계를 나타냅니다.
저자	작성자 이름을 입력합니다.
설명	필요에 따라 주석을 추가합니다.
작성됨	옵저버블이 생성된 시기를 나타냅니다.
설명	설명을 입력합니다.
expiration_time	옵저버블 기록의 만료 시간을 지정합니다.
확장명	옵저버블의 확장을 나타냅니다.
first_observed	데이터를 처음으로 관찰한 시간입니다.
first_seen	처음으로 악의적인 활동을 수행하는 이 기록이 발견되었습니다.
historically_significant	옵저버블이 역사적으로 중요한 것으로 간주되는지 여부를 나타냅니다. 이 TISC 시스템 플래그는 보관에서 옵저버블을 제외하는 데 사용됩니다.
ID	TISC 시스템에서 옵저버블에 할당한 고유 식별자입니다.
is_defanged	옵저버블 값이 제거되었는지 여부를 나타내는 플래그입니다.
is_false_positive	옵저버블이 긍정 오류로 식별되는지 여부를 나타내는 부울 플래그입니다.
언어	이 객체의 텍스트 내용 언어를 나타냅니다.
last_observed	데이터를 마지막으로 관찰한 시간입니다.
last_seen	이 객체가 악의적인 활동을 수행하는 것이 마지막으로 목격된 시간입니다.
메모	옵저버블 기록에 대한 추가 메모를 추가합니다.
번호	TISC에서 옵저버블에 할당한 시스템 생성 번호입니다.
security_type	옵저버블이 허용 목록 또는 거부 목록에 속하는지 여부를 지정합니다.
no_of_sources	옵저버블에 기여한 고유 소스의 개수를 나타냅니다.
sources	이 기록이 생성되는 위협 소스를 지정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
상태	활성 또는 비활성인 경우 옵저버블의 상태를 입력합니다.
tisc_tags	옵저버블과 연결된 TISC 태그를 선택합니다.
분류	옵저버블과 연결된 분류를 선택합니다.
TLP	TLP별 데이터 민감도 설정을 나타내는 고유 값입니다.
업데이트됨	옵저버블 기록이 마지막으로 업데이트된 시기를 나타냄
usage_categories	옵저버블이 속하는 범주(예: 봇넷 또는 피싱)입니다.
watch_list	옵저버블이 감시 목록에 포함되는지 여부를 지정하는 플래그입니다.

이러한 필드는 기준에 정의된 다른 필드와 함께 검색 탭에서 Splunk 사용할 수 있으며 검색 탭을 통해 보고, 검색하고, 분석할 수 있습니다.

데이터 저장소 위치 **Splunk**

이 섹션에서는 데이터 저장을 위해 Splunk의 키-값 저장소 내에서 통합하는 동안 조회를 활용하는 방법을 TISC 간략하게 설명합니다. 이러한 조회가 내에서 구성되고 검색 Splunk되는 방법을 자세히 설명합니다.

조회	조회 설명
`tisc_store_lookup`	수신 기록을 검색하는 데 사용할 KV 조회의 이름입니다.
`tisc_kv_store`	데이터가 있는 KV 저장소의 이름입니다.
`inputlookup <lookup_name>" example : | inputlookup tisc_store_lookup`	KV 저장소에서 기록을 조회하는 쿼리입니다.

TISC - Microsoft Sentinel 통합

위협 인텔리전스 보안 센터 Microsoft Sentinel은 Sentinel에서 TISC Sentinel로 옵저버블 가져오기, 관련 옵저버블의 세부 정보로 Sentinel 인시던트 보강, Sentinel TISC에서 .

주:
Microsoft Sentinel에서 옵저버블을 엔터티라고 합니다.

필수 구성요소

의존성

Microsoft Sentinel 콘텐츠 허브의 위협 인텔리전스 솔루션을 설치해야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

역할 및 권한

애플리케이션	역할 및 권한	설명
Microsoft Sentinel 관련 역할	**1.** 논리 앱 기여자 **2.** Microsoft Sentinel 기여자	**1.** 자원 그룹 수준에서 필요한 플레이북을 설치합니다. **2.** Microsoft Sentinel 플레이북과 상호 작용합니다. 자세한 내용은 Microsoft Sentinel의 역할 및 권한을 참조하세요.
위협 인텔리전스 보안 센터	sn_sec_tisc.api_azure_sentinel_solution	TISC 사용자 지정 커넥터에 구성된 사용자에게 TISC API에 대한 액세스를 허용하려면 이 역할이 있어야 합니다.

TISC 플레이북 템플릿

이 섹션에서는 TISC Sentinel 솔루션과 함께 제공되는 플레이북 템플릿에 대해 설명합니다.

플레이북 사용 사례

다음 테이블에서는 다양한 플레이북 사용 사례를 설명합니다.

사용 케이스	플레이북	설명
TISC에서 Sentinel로 옵저버블 임포트	Batch_Indicator_Uploader	Microsoft Sentinel에서 제공하는 업로드 표시기 API를 사용하여 TISC에서 옵저버블을 내보내기 위한 일괄 처리 메커니즘을 제공합니다.
	Import_Observables_Batch	TISC에서 옵저버블의 예약된 익스포트를 활성화합니다.
Sentinel에서 TISC로 엔터티 익스포트	Export_Incident_Entities	Sentinel 인시던트의 모든 엔터티를 익스포트합니다.
	Export_Hash_Entity	Sentinel 인시던트의 파일 해시 엔터티를 익스포트합니다.
	Export_Domain_Entity 엔터티	Sentinel 인시던트의 도메인 엔터티를 익스포트합니다.
	Export_IP_Entity	Sentinel 인시던트의 IP 엔터티를 익스포트합니다.
	Export_URL_Entity	Sentinel 인시던트의 URL 엔터티를 익스포트합니다.
Sentinel 인시던트 보강	Incident_Enrichment	Sentinel과 연결된 엔터티와 관련된 상세 정보를 가져오고 인시던트에 대한 설명 형식으로 정보를 게시하여 Sentinel 인시던트를 보강할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
모든 플레이북은 내부적으로 TISC 사용자 지정 커넥터를 사용하여 TISC API를 사용합니다.

템플릿에서 플레이북 생성

1. **Sentinel** 작업 공간의 콘텐츠 허브에서 **TISC** 솔루션 콘텐츠 페이지로 이동합니다.
2. 컨텐츠 페이지에 표시된 각 플레이북에 대해 다음을 수행합니다.
   a. 플레이북 템플릿을 선택하면 화면 오른쪽에 컨텍스트 창이 표시되면 구성을 클릭합니다.
   b. 플레이북 템플릿에 대한 설명을 읽고 설명에 언급된 필요 조건 및 배포 후 단계를 진행합니다.
   c. 사용자 지정 커넥터 배포를 클릭합니다(사용자 지정 커넥터를 아직 배포하지 않은 경우).

      배포 구성 페이지에서 **ServiceNow** 인스턴스 **URL**을 추가합니다.

   d. 플레이북 생성을 클릭하면 배포 구성 화면으로 이동합니다.
   e. 플레이북 구성 생성 화면에서 다음을 수행합니다.
      - 적절한 자원 그룹을 선택합니다.
      - 플레이북 이름을 수정하거나 기본 이름을 사용합니다.
      - 매개변수 섹션에 사용자 지정 커넥터 이름을제공합니다(이전 단계에서 배포한 커넥터의 이름과 일치하는지 확인).
      - 검토 및 생성을 클릭합니다.

Import_Observables_Batch Playbook 구성

Import_Observables_Batch 플레이북Batch_Indicator_Uploader 생성하기 전에 플레이북을 생성해야 합니다.

1. 다음으로 이동 논리 앱 디자이너 플레이북을 편집합니다.
2. 필요에 따라 반복 시간(시간)을 업데이트합니다.
3. 플레이북 내의 TISC 사용자 지정 커넥터 구성요소에서 TISC API로 전송되는 매개변수를 업데이트합니다.

매개변수 이름	설명
관찰 대상 유형	지원되는 유형은 다음과 같습니다. 하나 이상을 선택하십시오. ○ IP ○ 파일 해시 ○ 도메인 ○ URL
위협 점수	옵저버블에 대한 위협 점수를 입력합니다. 위협 점수 값은 0-100 범위의 숫자여야 합니다(MUST).
신뢰도	옵저버블에 대한 신뢰도를 입력합니다. 신뢰도 값은 0-100 범위의 숫자여야 합니다(MUST).

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

매개변수 이름	설명
평판	지원되는 값은 다음과 같습니다. 하나 이상을 선택하십시오. ○ 정리 ○ 악성 ○ 의심스러움 ○ 알 수 없음
위협 심각성	지원되는 심각도 수준은 다음과 같습니다. 하나 이상을 선택하십시오. ○ 중요 ○ 높음 ○ 보통 ○ 낮음
위협 수준	지원되는 위협 수준은 다음과 같습니다. 하나 이상을 선택하십시오. ○ 높음 ○ 보통 ○ 낮음
마지막으로 업데이트된 델타(시간)	옵저버블에 대한 마지막 업데이트 시간(시간)입니다.

Export_Incident_Entities Playbook 구성

이 플레이북에서는 TISC 옵저버블 추가 API를 사용합니다. 논리 앱 디자이너를 사용하여 플레이북에서 API로 전송되는 매개 변수를 편집할 수 있습니다. 자세한 내용은 TISC API - POST /sn_sec_tisc/threat_intel_data/add_observables 를 참조하십시오.

다양한 유형의 엔터티를 익스포트하는 아래 나열된 모든 플레이북에 대해 동일한 절차를 따를 수 있습니다.

- Export_Hash_Entity
- Export_Domain_Entity
- Export_IP_Entity
- Export_URL_Entity

Incident_Enrichment Playbook 구성

이 플레이북에서는 TISC 옵저버블 API를 사용합니다. 논리 앱 디자이너를 사용하여 플레이북에서 API로 전송되는 매개 변수를 편집할 수 있습니다. 자세한 내용은 TISC API - POST /sn_sec_tisc/threat_intel_data/observables 를 참조하십시오.

Playbook 실행

다음 테이블에서는 다음 플레이북을 실행할 수 있는 방법을 설명합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

플레이북	작업
Import_Observables_Batch	이 플레이북은 반복 트리거에 언급된 예약된 시간을 기준으로 자동으로 실행됩니다.
Export_Incident_Entities	Sentinel 인시던트에서 인시던트 작업 〉 플레이북 실행 실행을 위해.
Export_Hash_Entity	Sentinel 인시던트에서 파일 해시 엔터티 〉 플레이북 실행 실행을 위해.
Export_Domain_Entity	Sentinel 인시던트에서 도메인 엔터티 〉 플레이북 실행 실행을 위해.
Export_IP_Entity	Sentinel 인시던트에서 **IP** 엔터티 〉 플레이북 실행 실행을 위해.
Export_URL_Entity	Sentinel 인시던트에서 **URL** 엔터티 〉 플레이북 실행 실행을 위해.
Incident_Enrichment	Sentinel 인시던트에서 인시던트 작업 〉 플레이북 실행 실행을 위해.

위협 인텔리전스 보안 센터 관리

왼쪽 탐색을 사용하여 다음 위협 인텔리전스 보안 센터 데이터 관리 모듈의 TISC 관리 모듈로 이동하여 필터링 규칙 및 승인 규칙을 추가로 설정하고, 위협 점수를 정의하고, 알림을 관리합니다.

데이터 관리

모듈	설명
규칙 엔진	이 섹션은 데이터 관리 중에 필요한 다음 규칙으로 구성됩니다. **1.** 데이터 임포트 승인 규칙: 승인 규칙을 정의하고 데이터 임포트를 제출한 후 인텔리전스 임포트 섹션 내에서 승인 플로우를 통합합니다. **2.** 인바운드 필터링 규칙: 들어오는 소스 기록 데이터를 필터링하기 위해 필터 규칙을 생성합니다. **3.** 위협 점수 규칙: 옵저버블에 위협 점수를 할당하는 위협 점수 계산기를 사용자 지정합니다.
보안 통제 목록	이 모듈은 보안 제어에 도움이 됩니다. **1. AllowList** **2. DenyList** **3.** 감시 목록
분류	이 모듈은 데이터 소스 기록에 대한 분류를 생성하는 데 도움이 됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈	설명
알림	이 모듈은 이메일 알림을 관리하는 방법을 정의합니다.
템플릿	이 모듈에서는 디자인 타임 및 런타임 환경에서 보고서 템플릿을 만드는 방법에 대해 간략하게 설명합니다.

데이터 임포트 정의 승인 규칙

이 섹션을 사용하여 승인 규칙을 정의하고 데이터 임포트를 제출한 후 인텔리전스 임포트 섹션 내에서 승인 플로우를 통합합니다.

시작하기 전에

필요한 역할: sn_sec_tisc.admin

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 작업 공간에서 관리 아이콘을 클릭합니다.
3. 이동 규칙 엔진 〉 데이터 임포트 승인 규칙.
4. 데이터 임포트에 대한 승인 규칙을 선택합니다.

   기본 시스템 내에서 데이터 임포트에 대한 승인 규칙은 사용자가 승인 워크플로우를 활성화할 수 있도록 프로비저닝된 기본 승인 규칙입니다.
5. 승인이 필요한 사용자 또는 그룹 선택 및 승인자 선택 섹션 각각에 대해 하나 이상의 사용자 이름 또는 사용자 그룹을 입력합니다.
6. 데이터 임포트에 대한 승인 플로우를 활성화하려면 활성화 버튼을 클릭하십시오.

   이 옵션을 사용하면 승인자가 데이터 처리를 승인하거나 거부할 수 있도록 데이터 임포트가 승인 큐에 있게 됩니다. 승인자는 분석가가 변경한 내용을 검토한 다음 데이터 임포트 요청을 승인하거나 거부합니다.

   주:
   임포트 작업이 처리되고 승인 또는 거부된다는 이메일 알림이 사용자 또는 사용자 그룹에 전송됩니다.

만료 규칙 정의

TISC에서 생성된 다양한 옵저버블 또는 다양한 소스 객체 또는 표시기 소스의 조합에 대한 만료 규칙을 정의합니다.

시작하기 전에

애플리케이션에서 생성된 모든 소스에는 만료 기간이 있습니다. 데이터 피드는 시간 기반 만료 기간과 같은 기술을 사용하여 데이터 수집을 향상시킵니다. TISC에서 만료 규칙은 특정 데이터 소스 세트 또는 객체 유형 세트 또는 옵저버블 유형의 만료 시간을 정의합니다.

필요한 역할: sn_sec_tisc.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 보안 센터 〉 관리.
2. 선택 만료 규칙.
   만료 규칙 페이지가 표시됩니다.
3. 새로 만들기를 클릭합니다.
4. 새 규칙을 생성한 후 만료 규칙을 활성화하려면 활성화 를 클릭하십시오.
   만료 규칙을 활성화하지 않으면 규칙이 소스 기록에 적용되지 않습니다.

   주:

   - 만료 규칙을 활성화할 때마다 백그라운드에서 중복 검사가 수행되어 시스템에 데이터 소스와 기록 유형의 조합이 동일한 중복 규칙이 있는지 확인합니다. 이 경우 응용 프로그램은 규칙에 이미 동일한 데이터 소스와 개체 범주 조합이 포함되어 있으며 규칙을 사용하려면 기존 조합을 수정해야 한다는 정보 메시지를 표시합니다.
   - 샘플 만료 규칙은 기본 시스템의 사용자에 대해 프로비저닝되어 있으며 옵저버블에 대한 이 샘플 만료 규칙은 기본적으로 비활성화된 상태이므로 규칙을 활성화하고 활성화해야 합니다.

5. 저장을 클릭합니다.
6. 만료 규칙을 삭제하려면 삭제를 클릭합니다.

소스 기록에 대한 만료 규칙

만료 규칙은 기본적으로 원본 기록의 만료 시간을 설정하는 데 유용합니다. 집계 기록은 해당 소스 기록에서 가장 높은 만료 시간을 상속합니다.

규칙 적용 방법

Example: 수신 소스 기록 유형은 데이터 소스 유형에서 CrowdStrike로 하는 맬웨어입니다.

소스 기록에 만료 시간을 적용하기 위해 제공된 규칙을 기반으로 하는 규칙 평가 프로세스:

1. 활성화된 모든 규칙을 가져옵니다. 애플리케이션은 현재 사용하도록 설정된 모든 규칙을 확인하여 시작합니다.
2. 특정 규칙 조합을 확인합니다.

   다음의 조합과 구체적으로 일치하는 규칙을 찾습니다.

   - 데이터 소스 유형: CrowdStrike
   - 기록 유형: 맬웨어

3. 일치 규칙 조합에 따른 우선순위:

   데이터 소스 유형이 **CrowdStrike** 이고 기록 유형이 맬웨어인 규칙이 있는 경우 이 규칙이 우선합니다. 이 규칙에 지정된 만료 시간이 적용됩니다.

4. 대체 규칙:

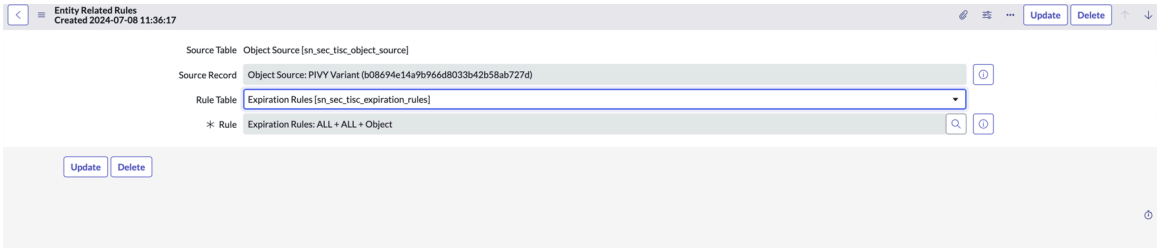
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. **CrowdStrike** 및 맬웨어 조합과 일치하는 규칙이 없으면 시스템은 데이터 소스 유형이 **CrowdStrike**이고 기록 유형이 모두인 규칙을 확인합니다.

b. 그래도 규칙이 발견되지 않으면 데이터 소스 유형이 모두 이고 레코드 유형이 맬웨어인 규칙을 찾습니다.

c. 마지막으로, 위의 규칙 중 어느 것도 존재하지 않는 경우, 데이터 소스 유형과 기록 유형이 모두 모두인 규칙으로 기본 설정됩니다.

5. 이러한 규칙이 시스템에 없으면 소스 기록에 만료 규칙이 적용되지 않습니다. 이 경우 아래 표(스크린샷 참조)로 이동하여 객체에 적용된 규칙의 조합을 확인합니다.



6. 데이터 소스 삭제:

   연결된 만료 규칙이 있는 데이터 소스가 삭제되면 이러한 규칙이 해결될 때까지 삭제가 제한되거나 허용되지 않을 수 있다고 가정합니다. 이렇게 하면 만료 정책 적용에 불일치가 발생하지 않습니다.

인바운드 데이터 제외 규칙 생성

모든 유형의 데이터 또는 모든 종류의 수신 소스 기록 데이터를 필터링하려면 인바운드 데이터 제외 규칙을 생성합니다.

시작하기 전에

이 애플리케이션은 STIX 데이터 소스를 포함하여 여러 위협 인텔리전스 피드의 통합을 지원합니다. 관련 데이터만 수집되도록 하려면 사용자 지정 가능한 제외 규칙을 적용해야 합니다.

필요한 역할: sn_sec_tisc.admin

이 태스크 정보

제외 규칙이 생성되고 소스 기록에 적용되어 추가 단계를 처리합니다. 기본 시스템은 수집된 옵저버블, 표시기 데이터 또는 엔터티/객체를 필터링하는 미리 정의된 규칙을 사용하여 사용자에게 샘플 필터링 규칙을 제공합니다.

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터 〉 관리.
2. 까지 드릴다운 규칙 엔진 〉 인바운드 데이터 제외 규칙.
3. 신규를 클릭하여 제외 규칙을 정의합니다.
   새 인바운드 데이터 제외 규칙 생성 페이지가 표시됩니다.
4. 양식에서 필드를 채웁니다.

제외 규칙 정의

필드	설명
이름	새 제외 규칙의 이름입니다.
설명	제외 규칙에 대한 간단한 설명입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
순서	제외 규칙 우선순위입니다. 이 필드는 둘 이상의 규칙이 트리거 조건을 공유할 때 제외 규칙이 실행되는 순서를 나타냅니다. 숫자가 가장 낮은 제외 규칙의 우선순위가 가장 높습니다. 작업 순서를 설정하려면 값을 입력합니다. 예를 들어 100, 200, 300 등의 값을 입력합니다. 기본 시스템 제외 규칙의 기본값은 100입니다.
데이터 소스	제외 규칙을 적용할 피드를 선택합니다.
테이블	필터를 적용할 테이블 유형을 선택합니다. 예를 들어 옵저버블 소스, 표시기 소스 및 객체 소스가 있습니다.
필터 유형(선택한 테이블이 옵저버블 소스인 경우에만)	필터 유형에는 필터를 적용할 수 있는 두 가지 옵션이 있습니다. ○ 조건을 기준으로 필터링 ○ 목록을 기준으로 필터링
필터 유형(조건에 따른 필터)	조건 작성기의 필터 조건. 이러한 조건은 소스 테이블을 기반으로 합니다. 예를 들어 표시기 소스와 객체 소스에는 필터 유형(조건에 따른 필터)만 있습니다. 조건을 더 추가하려면 **AND** 또는 **OR**을 클릭합니다. **AND**를 선택하면 모든 조건이 일치해야 합니다. **OR**을 선택하면 두 조건을 일치시킬 수 있습니다. 두 번째 필터 조건을 설정하려면 새 조건 집합을 클릭합니다.
필터 유형(목록을 기준으로 한 필터)	인바운드 옵저버블이 목록의 항목과 일치하는 경우 선택한 항목이 필터링됩니다. 주: 이러한 제외 규칙은 인텔리전스 임포트를 사용하는 데이터 임포트에는 적용되지 않으며 사용 가능한 옵션은 허용 목록, 거부 목록 및 감시 목록입니다.

제외 규칙에 의해 제외된 기록은 다음 섹션에서 볼 수 있습니다.

a. 필터링된 옵저버블 기록: 옵저버블 기록을 필터링하고 나열합니다.

b. 필터링된 표시기 기록: 표시기 기록을 필터링하고 나열합니다.

c. 필터링된 객체 기록: 객체 기록을 필터링하고 나열합니다.

주:
소스 기록에 추가된 태그를 기반으로 제외 규칙을 적용하려면 필터 조건 작성기에서 *TISC* 태그 옵션을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

TISC의 사용자 지정 위협 점수 계산기

사용자 지정 위협 점수 계산기를 사용하면 사용자 정의 기준에 따라 옵저버블의 위협 심각도 점수를 정의하고 계산할 수 있어 옵저버블에 대한 투명한 인텔리전스 점수 산정을 제공할 수 있습니다. 위협 점수는 옵저버블 기록에 대해 자동으로 계산됩니다.

위협 점수 계산기 정의

사용자 정의 매개변수를 기반으로 생성된 옵저버블 기록에 대한 위협 점수를 정의합니다. 기본 시스템에는 하나의 위협 점수 산정 규칙이 프로비저닝되며, 이에 따라 사용자 지정하고 활성화할 수 있습니다.

시작하기 전에

필요한 역할: sn_sec_tisc.admin

주:
기본적으로 위협 점수 규칙은 비활성 상태입니다. 옵저버블 점수를 보려면 규칙을 활성화해야 합니다.

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터 〉 관리.
2. 이동 위협 점수 산정 규칙.
   위협 점수 계산기 페이지가 표시됩니다.

중요사항:

- 애플리케이션의 기본 시스템 내에는 사용자가 위협 점수를 보거나, 편집하거나, 수정할 수 있도록 프로비저닝된 하나의 점수 규칙이 있지만, 사용자는 새 규칙을 생성하거나 미리 정의된 위협 점수 규칙을 삭제할 수 없습니다.
- 변경 사항은 해당 시점부터 새 옵저버블 또는 옵저버블에 대한 업데이트에 적용됩니다. 과거 점수를 다시 표시하려면 다시 계산 옵션을 사용해야 합니다.

3. 양식에서 다음 필드에는 미리 정의된 값이 포함되어 있습니다.

위협 점수 계산기

필드	설명
이름	위협 점수 산정 값의 이름입니다. 예를 들어 위협 점수 계산기입니다.
설명	위협 점수 기록에 대한 설명입니다. 예를 들어 미리 정의된 기준 점수의 가중치 합계를 기준으로 위협 점수를 계산합니다.
전체 가중치(기준 작성기에서 적용 가능)	이 필드는 편집할 수 없으며 활성화된 기준에 해당하는 가중치를 기준으로 시스템에서 계산한 전체 가중치를 표시합니다.
채점 기준	옵저버블에 대한 점수 산정 기준을 나타냅니다. 다음은 위협 점수 산정 기준을 정의하는 데 사용할 수 있는 두 가지 옵션입니다. ○ 기준 작성기: 위협 점수 계산에 기여하는 기준을 추가, 편집 또는 제거하고 활성화 및 비활성화하고 총

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	집계 가중치가 100%가 되도록 하려면 이 옵션을 사용합니다. ○ 스크립트 사용(고급): 스크립팅 기능은 0-100 범위 내에서 위협 점수를 반환해야 하는 사용자 지정 스크립트를 작성하는 고급 기능입니다.

다음은 점수 산정 기준을 정의하는 데 사용할 수 있는 옵션입니다.

○ 기준 작성기

○ 스크립트 사용(고급)

다음은 기준 작성기의 절차입니다.

주:
기존 기준을 편집 또는 수정하거나 새 기준을 추가할 수 있습니다.

a. 기준 유형을 선택합니다.
예를 들어, 새 기준을 추가합니다.

b. 기준이 구성되는 테이블을 선택합니다.
드롭다운 목록의 값 목록에는 옵저버블, 위협 액터, 캠페인, 위치, ID, 취약성, 위협 이벤트, 보안 인시던트 및 집계가 있습니다. 드롭다운 목록에서 이러한 옵션 중 하나를 선택하면 조건이 적용됩니다. 이 조건을 사용하면 선택한 값과 관련된 기록만 표시되거나 계산됩니다.

주:

- 옵저버블을 선택한 경우 위협 점수가 계산되는 옵저버블 기록에 조건이 적용됩니다. 선택한 테이블이 옵저버블이 아닌 경우 기록이 위협 점수가 계산되는 옵저버블과 관련된 경우에만 조건이 적용됩니다.
- 옵저버블과 연결된 관계 수를 기반으로 점수를 정의하기 위해 추가 집계 테이블이 추가됩니다. 예를 들어 테이블: 집계 및 필드 값: 위협 액터를 선택한 다음, 옵저버블의 경우 위협 액터가 3개 이상인 경우 점수를 설정하고 적절한 조건을 적용합니다.
- 예를 들어 옵저버블과 연결된 하나 이상의 위협 액터에 대한 점수를 설정하려면 필드를 위협 액터 없음으로 선택하고 원하는 점수를 설정한 다음 적절한 조건을 적용합니다.

c. 위에서 선택한 테이블에서 필드를 선택합니다.

d. 0-100 사이의 기준 가중치 를 입력합니다.
모든 기준의 전체 가중치는 100%여야 합니다.

e. 기준의 이름과 간단한 설명을 입력합니다.

f. 점수 산정 기준을 사용하려면 점수 산정 기준 사용 확인란을 선택합니다.

g. 조건을 정의하고 조건에 대한 점수를 설정합니다.

h. 새 조건 버튼을 사용하여 새 조건을 추가하고 기준 삭제 아이콘을 사용하여 조건을 삭제할 수도 있습니다.

i. 추가를 클릭하여 구성된 기준을 추가합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

위협 점수에 대한 조건을 정의하는 예는 다음과 같습니다.

```
Table: Vulnerability

Field: CVSS2.0

Weightage: 30%

Condition-1: CVSS2.0 > 7, Score = 80

Condition-2: CVSS2.0 > 4 AND CVSS2.0 < 7, Score = 50

Condition-3: CVSS2.0 < 4, Score = 10
```

4. **Re-Calculate** History(기록 재계산) 버튼을 클릭하여 위협 점수를 다시 계산합니다.
위협 점수 산정 규칙이 변경된 경우 과거에 이미 계산된 위협 점수가 있는 옵저버블에 점수 산정 규칙을 다시 적용해야 하며, 이력 재계산 버튼을 사용하여 재계산 작업을 트리거해야 합니다.

   주:

   - 작업을 수행할지 묻는 확인 메시지가 표시됩니다. ## ####### #### ## ## #######. ##### ### ### ### # ####. # ### ########?
   - 이력 재계산의 일부로 옵저버블에 대해 생성되는 업데이트 이벤트의 경우 웹후크 처리가 비활성화되며, 활성화하려면 이 시스템 속성 webhook_ignore_threat_score_reapply 수정합니다.

5. 확인을 클릭합니다.

   중요사항:
   이 작업은 장기 실행 작업을 트리거하고 시스템이 작업이 완료될 때까지 위협 점수 규칙을 더 이상 변경하는 것을 허용하지 않습니다. 백그라운드 작업 구성이 구성되는 방식에 대한 자세한 정보는 취약성 대응 백그라운드 작업 프레임워크 구성의 내용을 참조하십시오.

다음은 스크립트 사용(고급) 스크립트입니다. 이 스크립트를 사용하여 0-100 범위 내의 위협 점수를 반환해야 하는 사용자 지정 스크립트를 빌드합니다.

고급 스크립트 필드는 현재 및 집계 매개변수를 사용하는 함수로 자동으로 채워지며 이 함수는 0-100 범위의 위협 점수를 반환해야 합니다.

여기서 현재 매개변수는 위협 점수가 계산되는 엔터티(옵저버블)의 GlideRecord 객체입니다. 옵저버블의 경우 sn_sec_tisc_observable 테이블의 GlideRecord에 해당합니다. aggregates 매개변수는 메인 엔터티(옵저버블)에 연결된 다양한 기록 유형(예: 캠페인 또는 ID)의 기록 수에 접근하는 데 사용되는 sn_sec_tisc_aggregates 테이블 기록의 GlideRecord 객체입니다.

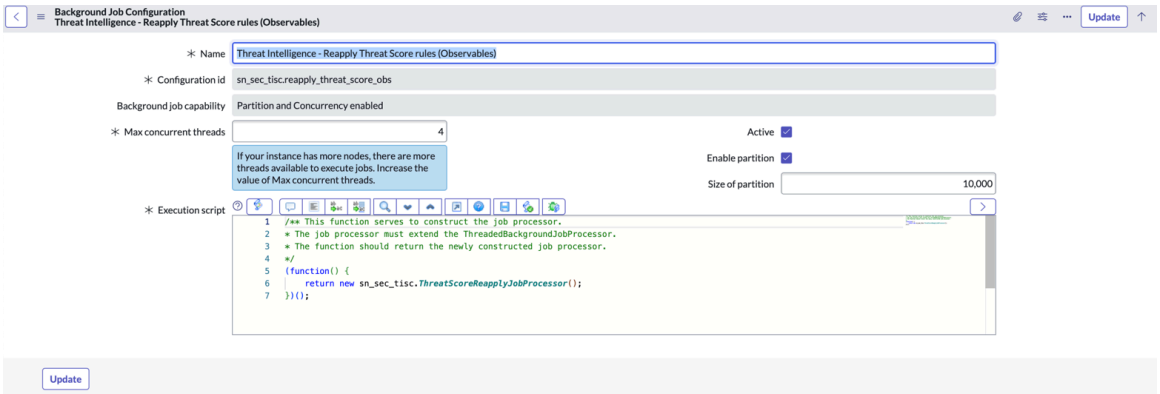
고급 옵션에 있는 스크립트의 샘플 예시:

```
answer = (function threatScoreCalculator(current, aggregates) {

  // return the threat score in the range of 0-100
  var threatSeverity = current.getValue("threat_severity");
  if(threatSeverity == "high")
   return 80;
  else {
     let associatedCampaigns = aggregates.getValue("num_of_campaigns");
     if(associatedCampaigns > 0)
        return 50;
  }
```


© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
    return 0;

})(current, aggregates);
```

참고로 아래는 위협 점수 백그라운드 작업 구성 프로세스를 보여주는 스크린샷입니다.



MITRE ATT&CK 기술 추출 규칙

다양한 데이터 소스에서 수집된 옵저버블 또는 객체에서 MITRE 기술을 자동으로 추출하고 옵저버블 기록의 위협 조회 결과에서 MITRE 기술도 추출합니다.

시작하기 전에

필요한 역할: sn_sec_tisc.admin

> **주:**
> 사용 중인 인스턴스에서 MITRE ATT&CK 리포지토리 데이터를 사용할 수 있는지 확인하십시오. 데이터를 사용할 수 없는 경우 애플리케이션은 추출을 수행하지 않습니다.

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 보안 센터 〉 관리.
2. 이동 규칙 엔진 〉 **MITRE ATT&CK** 기술 추출 규칙.
   MITRE ATT&CK 기술 추출 규칙 페이지가 표시됩니다.
3. 새로 만들기를 클릭합니다.
4. 새 규칙을 생성한 후 활성화 를 클릭하여 MITRE ATT&CK 기술 추출 규칙을 활성화합니다.
   MITRE ATT&CK 기술 추출 규칙을 사용하도록 설정하지 않으면 규칙이 기록에 적용되지 않습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

a. 데이터 소스: 추출 규칙을 활성화할 때마다 데이터 소스와 통합 유형의 조합은 기존에 활성화된 추출 규칙과 일치하지 않아야 하며, 일치하지 않을 경우 애플리케이션에 기존 조합을 수정하고 규칙을 다시 활성화하라는 오류 메시지가 표시됩니다.

b. 위협 조회: 추출 규칙을 활성화할 때마다 벤더 이름은 기존에 활성화된 추출 규칙과 일치하지 않아야 하며, 일치하지 않는 경우 애플리케이션은 벤더 이름을 수정하고 규칙을 다시 활성화하라는 오류 메시지를 표시합니다.

c. 샘플 MITRE ATT&CK 기술 추출 규칙은 기본 시스템의 사용자에 대해 프로비저닝되며, 이러한 규칙은 기본적으로 비활성화된 상태이므로 규칙을 활성화하고 활성화해야 합니다.

필드	설명
데이터 소스 수집에 대한 일반 규칙	인텔리전스 임포트 및 수동 생성을 포함한 모든 유형의 데이터 소스에서 수집하기 위한 일반 규칙입니다.
위협 조회를 위한 일반 규칙	이는 모든 위협 조회 통합에 대한 일반 규칙입니다.
옵저버블 보강 통합에 대한 일반 규칙	이는 모든 옵저버블 보강 통합에 대한 일반 규칙입니다.

5. 복제를 클릭하여 추출 규칙의 복사본을 만듭니다.
6. 추출 규칙을 사용하지 않으려면 사용 안 함을 클릭하십시오.

주:
비활성화되면 MITRE 데이터 추출에 더 이상 규칙이 고려되지 않습니다.

7. 저장을 클릭합니다.
8. MITRE ATT&CK 기술 추출 규칙을 삭제하려면 삭제를 클릭합니다.

MITRE ATT&CK 기법 추출 방법

MITRE ATT&CK 기법 추출 방법은 추출 방법을 수행하고 관련 기술을 검증하는 방법을 설명합니다.

1. 데이터 소스에 대한 추출 규칙(위협 조회는 적용되지 않음)은 엔터티(예: 옵저버블 소스 또는 객체 소스) 소스 기록이 생성될 때마다 처리됩니다.
2. 규칙은 엔터티 소스 기록 내의 모든 필드에 적용할 수 있습니다(날짜, 숫자 필드, 사용 범주 및 공격 단계 제외).
3. 추출된 MITRE 기술은 해당 엔터티 기록에 연결되며 관련 기록 탭의 MITRE 기술 관련 목록에서 기록을 볼 수 있습니다.

주:
MITRE 기술은 먼저 추출되어 엔터티 소스 기록에 연결된 다음 기술 연결이 중복 제거되고 상위 엔터티 기록으로 집계됩니다.

MITRE 기술 보기

1. 다음으로 이동 위협 인텔 라이브러리를 사용하는 모든 엔터티(옵저버블 또는 객체) 기록입니다.
2. 관련 기록 탭을 클릭합니다.
3. **MITRE** 기술을 선택하고 추출된 관련 기술을 봅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. MITRE 기술 연결 기록을 보고 액세스하려면 MITRE 기술 ID를 클릭합니다. 소스 열에는 MITRE 추출이 수행되는 엔터티 소스 기록에 연결된 모든 소스(소스가 하나 이상 있는 경우 쉼표로 구분됨)가 표시됩니다.

   주:
   여러 소스에서 동일한 방법 및 기술 ID를 추출하면 하나의 방법 및 기술 연결 기록만 표시되고 소스 열에는 추출된 모든 소스가 표시됩니다.

5. 문제 해결을 위해 기술 소스 관계로 이동하여 방법 및 기술 연결 추출을 담당한 MITRE 추출 규칙을 볼 수 있습니다.

   주:
   추출 규칙 열이 표시되지 않는 경우 목록 작업 아이콘을 사용하여 추출 규칙 열을 추가해야 합니다.

위협 조회 실행 작업이 트리거되는 옵저버블에 대해 위협 조회 결과 기록이 생성될 때마다 위협 조회를 위한 추출 규칙이 처리되며, 위협 조회 결과 기록에서 사용할 수 있는 원시 데이터(raw_data 필드) 페이로드에서만 추출이 수행됩니다.

주:

- 추출된 엔터티(옵저버블 또는 객체) 소스 또는 MITRE ATT&CK 기술에 대한 위협 조회 결과에 전술 ID가 없는 경우 MITRE 리포지토리의 해당 기술과 연결된 모든 전술에 대해 기술 연결이 생성됩니다.
- 추출된 엔터티(옵저버블 또는 객체) 소스 또는 MITRE ATT&CK 기술에 대한 위협 조회 결과에 전술 ID가 있는 경우 기술 연결은 MITRE 리포지토리의 해당 기술과 연결된 추출된 모든 전술에 대해서만 특별히 생성됩니다.

보안 제어 목록 정의

이 기능을 사용하여 옵저버블을 대량으로 추가하거나 제거합니다.

시작하기 전에

필요한 역할: sn_sec_tisc.admin

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터 〉 관리.
2. 이동 보안 통제 목록.
   예를 들어 허용 목록에 옵저버블을 추가한 다음 허용 목록 옵션으로 이동합니다.
3. 허용 목록을 선택합니다.
4. 허용 목록에 추가할 옵저버블 유형(예: IP 주소, 파일 등)을 선택합니다.
5. 추가를 클릭합니다.
   허용할 옵저버블 선택 목록이 표시됩니다.
6. 허용 목록에 추가해야 하는 모든 옵저버블을 선택합니다.
7. **Add to Allow** List(허용 목록에 추가)를 클릭합니다.
   선택한 옵저버블이 추가됩니다.
8. 마찬가지로 거부 목록에 추가를 선택하여 제거된 목록에 옵저버블을 추가합니다.
9. 감시 목록에 옵저버블을 추가하려면 감시 목록에 추가를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
양식 배너 위에 있는 옵저버블 양식 뷰 페이지에서 직접 허용 목록, 거부 목록 또는 감시 목록에 옵저버블을 직접 추가할 수 있습니다.

10. 확인하려면 위협 인텔 라이브러리로 이동합니다.
11. 허용 목록에 추가된 옵저버블 유형을 선택합니다.
옵저버블이 허용 목록에 추가된 것으로 표시됩니다.

주:
허용 목록과 거부 목록은 함께 사용할 수 없으며 시스템은 허용 목록의 옵저버블이 거부 목록에 포함되지 않도록 하며 그 반대의 경우도 마찬가지입니다.

분류 생성

데이터 소스 기록에 대한 분류를 생성합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.admin

프로시저
1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터 〉 관리 〉 분류.
2. 새로 만들기를 클릭합니다.
3. 이름을 입력합니다.
4. 활성화 또는 비활성화 양식 작업 활성화 또는 비활성화를 사용하여 분류 상태를 활성화 또는 비활성화합니다.

주:
비활성화된 분류는 분류를 적용할 수 있는 기록을 선택할 수 없습니다.

5. 분류 값 섹션으로 이동하여 분류 값을 추가합니다.
6. 새로 만들기를 클릭하여 새 분류 값 양식 뷰를 열고 분류 및 값을 입력합니다.
7. 저장을 클릭합니다.
8. 예를 들어 위협 인텔 라이브러리 〉 옵저버블 옵저버블 기록에 대한 분류를 확인하기 위해
9. 옵저버블 양식 페이지에서 태그 및 분류 섹션으로 이동하여 새로 만든 분류를 선택합니다.

주:
위협 인텔리전스 라이브러리의 목록 보기에서 태그와 분류를 추가할 수도 있습니다.

분류 벌크 임포트

분류 기록을 임포트합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.admin

이 태스크 정보
스프레드시트의 데이터를 사용하여 분류를 임포트할 수 있습니다. 이렇게 하면 여러 기록을 대량으로 임포트할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터 〉 관리 〉 분류.
2. 임포트 버튼을 선택합니다.
   이 작업은 XLSX 또는 CSV 형식의 데이터 파일을 임포트하는 작업을 엽니다. 샘플 파일을 다운로드하여 임포트할 형식을 이해할 수도 있습니다. 파일 형식에는 분류 및 분류 값을 포함하는 두 개의 값이 있습니다.
3. 파일 링크 추가를 클릭합니다.
4. 파일을 선택하고 업로드합니다.
5. 완료를 클릭합니다.
   첨부된 파일의 데이터를 성공적으로 가져왔는지 확인하는 메시지가 표시됩니다. 링크를 클릭하면 임포트 요약을 볼 수 있습니다. 링크를 클릭하면 기록이 새 탭에서 열립니다. 생성된 분류 및 분류 값 수를 볼 수 있으며 기록된 오류가 있는 경우 임포트 오류 섹션에 기록됩니다.

   주:
   기본적으로 이러한 모든 분류 및 분류 값은 사용 상태로 생성됩니다. 비활성화하려면 항상 목록 보기에서 비활성화할 수 있습니다.

6. 분류 페이지에서 기록을 클릭하면 분류 값이 별도의 탭으로 표시되고 성공적으로 임포트된 두 분류 값을 볼 수 있으며, 이러한 분류 값은 사용 가능한 상태가 됩니다.
7. 또한 분류 임포트를 보려면 언제든지 임포트 섹션으로 이동할 수 있습니다. 임포트한 분류는 분류 임포트 섹션 아래에 표시됩니다.
8. 모든 임포트를 클릭하면 애플리케이션에서 다른 사용자가 작성한 모든 분류 임포트를 볼 수 있습니다.
9. 내 임포트를 클릭하여 현재 로그인한 사용자에 대한 분류 임포트를 확인합니다.

위협 조회 평판 계산기 관리

위협 조회 찾기 계산기를 사용하여 위협 조회 벤더에서 받은 응답에 따라 옵저버블 결과를 계산할 수 있습니다.

통합에 대한 위협 조회 찾기 계산기를 생성하고 스크립트를 사용하여 다양한 옵저버블 결과를 식별하는 방법을 결정할 수 있습니다. 위협 조회 찾기 계산기에는 기본 시스템과 함께 제공되는 샘플 스크립트가 포함되어 있으며, 이 스크립트를 사용하여 옵저버블 찾기를 식별하거나 요구 사항에 따라 이 스크립트를 수정할 수 있습니다.

계산된 결과를 제공하는 외부 공급업체 통합의 경우 위협 조회 찾기 계산기는 결과를 기본 시스템에서 지원되는 결과에 매핑합니다.

위협 조회 결과 롤업

다양한 통합 벤더의 옵저버블에 대한 위협 조회 결과가 여러 개 있는 경우 모든 벤더의 최근 위협 조회 결과가 고려되고 전체 옵저버블 결과가 다음과 같이 표시됩니다.

위협 조회 결과 롤업

최신 옵저버블 찾기	전체 옵저버블 찾기
악성	통합 벤더 중 하나가 옵저버블을 악성으로 보고하면 전체 옵저버블 결과가 악성으로 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

위협 조회 결과 롤업

최신 옵저버블 찾기	전체 옵저버블 찾기
의심스러움	통합 벤더 중 옵저버블을 악성으로 보고한 벤더가 없는 경우, 그 중 한 벤더가 이를 의심스러움으로 보고하면 전체 옵저버블 발견 사항이 의심스러움으로 표시됩니다.
정리	모든 통합 벤더가 옵저버블을 정상으로 보고하면 전체 옵저버블 결과가 정상으로 표시됩니다.
알 수 없음	통합 벤더 중 옵저버블을 악성 또는 의심스러움으로 보고한 벤더가 없고 그 중 하나가 알 수 없음으로 보고하는 경우, 전체 옵저버블 발견 사항은 알 수 없음으로 표시됩니다.

위협 조회 평판 계산기 보기

위협 조회 찾기 계산기를 보고 특정 위협 조회 벤더의 응답에 따라 옵저버블의 평판을 계산하는 방법을 결정할 수 있습니다.

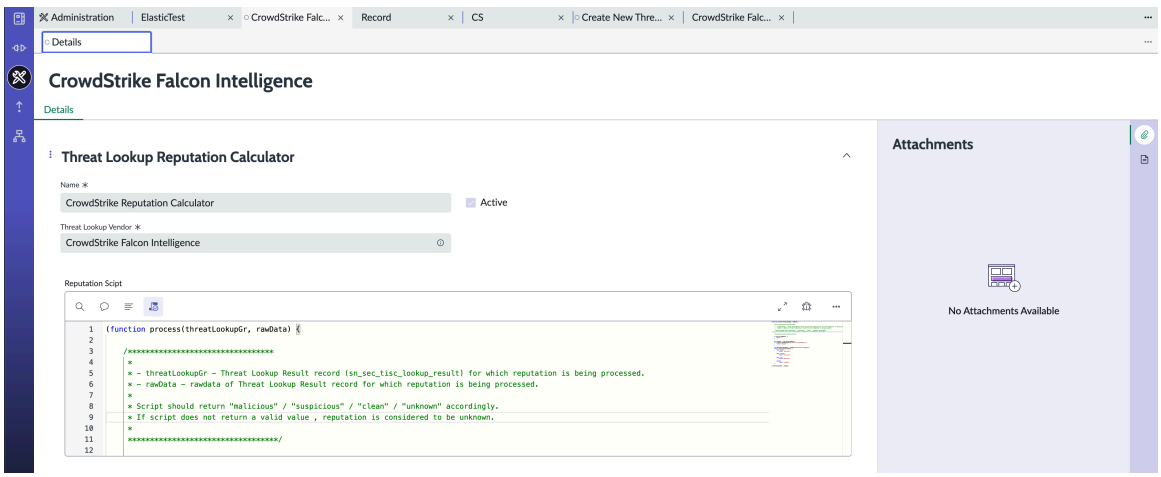
필요한 역할: sn_sec_tisc.admin

위협 조회 평판 계산기를 보려면 다음 단계를 수행하십시오.

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터 〉 관리.
2. 위협 조회 평판 계산기 섹션을 선택합니다.

   위협 조회 평판 계산기 목록을 볼 수 있습니다.

3. 계산기의 세부 정보를 보려면 필요한 위협 조회 평판 계산기를 클릭하십시오.



위협 조회 생성 평판 계산기

필요한 역할: sn_sec_tisc.admin

> **주:**
> 위협 조회 벤더마다 특정 시점에 하나의 위협 조회 계산기만 활성화할 수 있습니다.

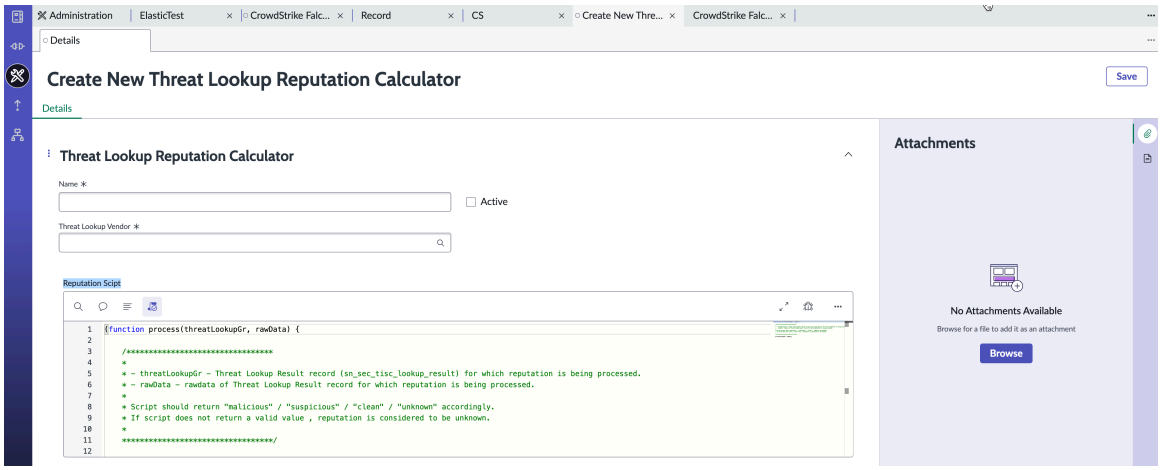
위협 조회 평판 계산기를 생성하려면 다음 단계를 수행하십시오.

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터 〉 관리.
2. 위협 조회 평판 계산기 섹션을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

위협 조회 평판 계산기 목록을 볼 수 있습니다.

3. 위협 조회 평판 계산기를 생성하려면 새로 만들기를 클릭합니다.



4. 양식에서 필드를 채웁니다.

위협 조회 평판 계산기 생성

필드	설명
이름	위협 조회 평판 계산기의 이름입니다.
활성	위협 조회 계산은 활성 옵션이 선택된 경우에만 실행됩니다.
위협 조회 벤더	위협 조회 벤더의 이름입니다. 예를 들면 CrowdStrike Falcon Intelligence입니다.
평판 스크립트	다양한 옵저버블 결과를 식별하는 방법을 결정하는 스크립트 편집기입니다. 모든 위협 조회 통합에는 위협 조회 평판을 계산하기 위한 기본 스크립트가 함께 제공됩니다.

5. 저장을 클릭합니다.

이메일 알림 관리

알림을 사용하여 ServiceNow 시스템 이메일 알림을 생성 및 관리하고, 이메일 로그를 봅니다.

이메일 알림

이메일 알림을 사용하여 선택한 사용자에게 옵저버블/표시기/기타 다양한 객체에 대한 업데이트와 같은 애플리케이션 내의 특정 작업에 대한 이메일 알림을 보냅니다.

필요한 역할: 관리자

주:
시스템 관리자는 애플리케이션의 클래식 뷰에서 이메일 알림 규칙 상세 정보를 보거나 작성하거나 편집할 수 있습니다.

위협 인텔리전스 보안 센터 개별 이메일 주소 또는 이메일 주소 목록으로 전송되는 규칙 기반 이메일 알림을 제공합니다. 일반적으로 내부 사용자에게 위협 인텔리전스 정보를 보급하는 것은 일반적으로 이메일 형식으로 전송됩니다. 이 프로세스에는 지정된 형식과 타임라인에 따라 사용자에게 위협 인텔리전스 데이터를 제공하는 작업이 포함됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이메일 알림을 통해 관리자는 다음을 지정할 수 있습니다.

- 알림 전송 시기
- 알림을 받는 사람
- 알림의 컨텐츠

주:
변경하려면 요구 사항에 따라 기본 시스템 규칙을 수정하여 이메일을 보낼 대상을 구성해야 합니다.

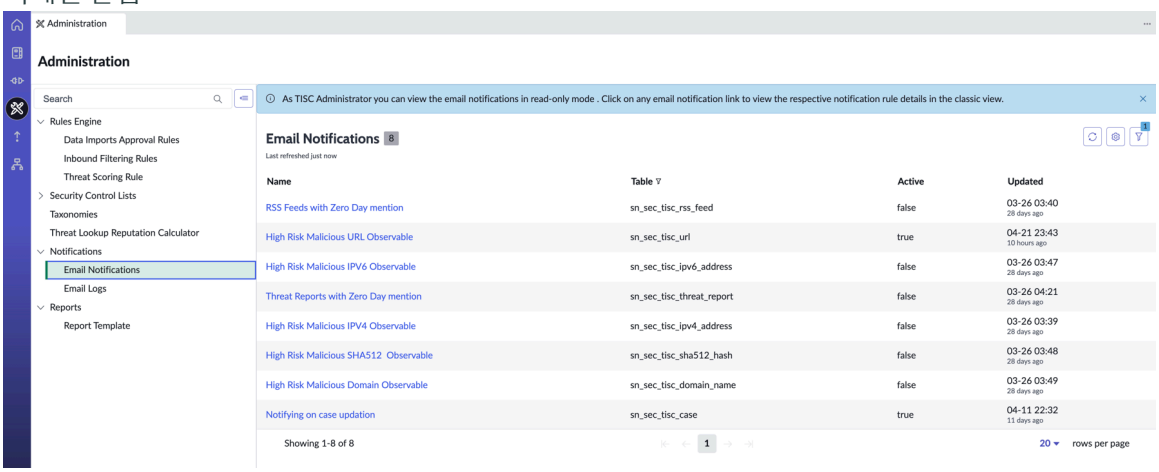
자세한 내용은 설명서의 이메일 알림 만들기 섹션을 ServiceNow AI Platform 관리 참조하십시오.

다음 테이블에서는 기본 시스템에서 프로비저닝되는 이메일 알림 규칙에 대해 자세히 설명합니다.

이메일 알림

이름	테이블
제로 데이 언급이 있는 RSS 피드	sn_sec_tisc_rss_feed
높은 위험 악성 URL 옵저버블	sn_sec_tisc_url
고위험 악성 IPV6 옵저버블	sn_sec_tisc_ipv6_address
제로 데이 멘션이 포함된 위협 보고서	sn_sec_tisc_threat_report
고위험 악성 IPV4 옵저버블	sn_sec_tisc_ipv4_address
높은 위험 악성 SHA512 옵저버블	sn_sec_tisc_sha512_hash
높은 위험 악성 도메인 옵저버블	sn_sec_tisc_domain_name
케이스 업데이트 시 알림	sn_sec_tisc_case

이메일 알림



주:
각 이메일 알림을 클릭하면 알림 보기, 편집 또는 만들기와 같은 필요한 작업을 수행할 수 있는 클래식 UI로 이동합니다.

이메일 로그

이 섹션에서는 구성된 이메일 알림 규칙을 사용하여 전송되는 이메일에 대해 TISC 관리자에게 명확한 가시성을 제공합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이메일 알림 및 로그 개요

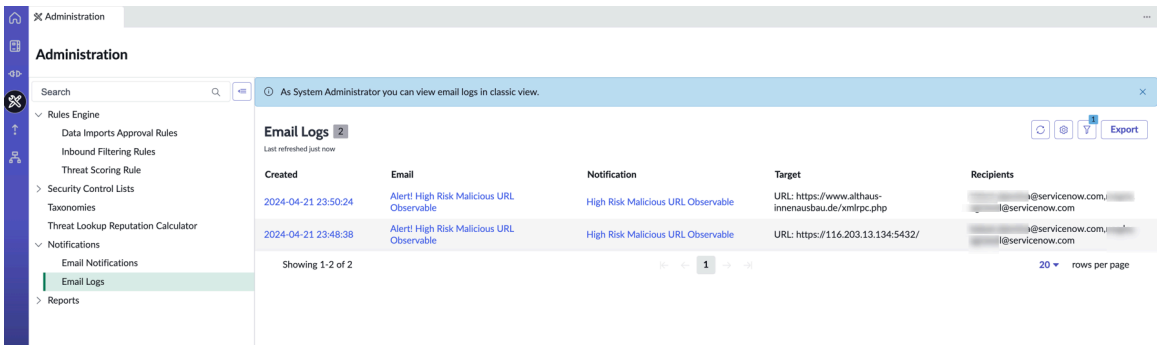
TISC는 다양한 가상 사용자에 따라 이메일 알림과 로그에 액세스, 확인 또는 수정할 수 있는 다양한 범위를 제공합니다.

주:

가상 사용자	접근 수준
TISC 관리자(sn_sec_tisc.admin)	sn_sec_tisc.admin은 TISC에 대해 구성된 이메일 알림만 볼 수 있습니다. 주: 이러한 알림을 보려면 이메일 로그 하이퍼링크를 클릭하여 클래식 UI로 이동합니다.
시스템 관리자(admin)	관리자는 클래식 UI에서 알림을 만들고, 보고, 편집할 수 있습니다. 주: 이메일 로그 하이퍼링크를 클릭하여 클래식 UI로 이동하면 이러한 알림을 보고 생성할 수 있습니다.

주:
TISC 관리자와 시스템 관리자 모두 필터를 사용하고 이메일 로그를 검색할 수 있습니다.

이메일 로그



보고서 템플릿

사용자 그룹 내에서 공유할 수 있는 보고서 템플릿을 재사용하여 보고서를 빠르고 일관되게 생성하는 기능을 정의합니다.

이 기능을 사용하여 조직에 대한 위협과 관련하여 진행 중인 조사의 상태를 제공하고 동일한 유형의 보고서를 생성하는 데 도움이 되는 케이스에 적용할 수 있는 다양한 유형의 보고서 템플릿을 생성합니다.

이 섹션에서는 케이스 수준에서 CTI 보고를 구현하는 방법을 설명하고 관리(템플릿 설계) 및 분석가(런타임) 경험을 모두 제공합니다.

사용자 지정 케이스 작업 양식 필드 또는 관련 목록을 닷워킹이 가능한 보고서 템플릿에 추가할 수 있습니다. 또한 다양한 보고서 요소를 사용하여 요구 사항에 따라 보고서의 형식을 지정하고 구성할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필요한 역할: sn_sec_tisc.admin

다음 표에서는 기본 시스템 내에서 제공되는 몇 가지 보고서 템플릿에 대해 설명합니다.

보고서 템플릿

이름	설명
케이스 상태 보고서 - 위협 액터 프로파일	이 보고서는 조직에 대한 위협의 맥락과 관련성, 적의 행동 및 잠재적 목표, IOC 보강, 관련 맬웨어 및 도구, 관찰된 TTP, 기존 TTP와의 차이점(완전히 새로운 기능, 약간의 수정 등)을 이해하려고 시도하는 위협 행위자와 관련된 진행 중인 사례 조사에 대한 상태를 제공하도록 설계되었습니다.
실무 요약	이 보고서는 고위 의사 결정권자에게 특정 위험에 대해 알리기 위해 고안되었습니다. 초점은 경영진 청중과 무엇을, 언제가 아니라 왜, 그리고 어떻게를 설명하는 전략적 문제를 지원하는 것입니다. 긴 형식의 서술적 글쓰기를 뒷받침하는 기술적 세부 사항 및 부록은 이 보고서에 포함되지 않습니다.
사후 조사 요약 - 위협 액터 프로파일	이 보고서는 조직에 대한 위협의 맥락과 관련성을 제공하도록 설계되었습니다. 적의 행동 및 잠재적 목표; IOC 강화; 관련 맬웨어 및 도구 관찰된 TTP; 기존 TTP와의 차이점 – 완전히 새로운 기능, 약간의 수정 등.

주:
기본적으로 이러한 보고서는 게시됨 상태이며 읽기 전용 모드입니다. 보고서 템플릿은 읽기 전용 모드이므로 사용자는 템플릿을 편집할 수 없으며 분석가는 보고서 템플릿이 비활성화되므로 보고서를 생성할 수 없습니다.

새 보고서 템플릿 생성

조직의 비즈니스 요구에 따라 새 케이스 보고서 템플릿을 생성합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.admin

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 보안 센터 〉 관리.
2. 선택 보고서 〉 보고서 템플릿.
   이 섹션에는 기본 시스템에서 사용할 수 있는 템플릿과 게시된 템플릿이 표시됩니다. 원하는 템플릿을 선택하여 보고서 작업에 사용할 수 있습니다.

   주:
   필요한 경우 이 섹션에서 템플릿을 삭제할 수도 있습니다.

3. 새로 만들기를 클릭합니다.
4. 템플릿의 이름 및 설명을 입력합니다.
5. 저장을 클릭합니다.
   템플릿 콘텐츠 섹션이 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
새 보고서 템플릿을 만들 때마다 템플릿은 초안 상태가 되며, 이는 템플릿 생성이 진행 중이고 완료될 때까지 다른 사용자는 보고서 템플릿을 볼 수 없음을 의미합니다.

6. 템플릿 컨텐츠를 확장하여 템플릿 본문에 원하는 필드를 삽입합니다.

주:

- 편집 중인 템플릿을 사용하면 템플릿 본문을 정의하고 템플릿 편집기 섹션에 추가할 필수 변수를 선택할 수 있습니다. 템플릿은 서식 있는 텍스트 편집기(RTE)에서 지원되므로 들여쓰기, 글꼴 크기, 표 작성, 이미지 추가 및 기타 다양한 서식 기능과 같은 사용 가능한 다양한 기능을 제어할 수 있습니다.
- 보고서 템플릿에 이미지를 삽입할 수도 있으므로 이미지를 복사하여 템플릿에 직접 붙여넣어야 합니다. 이미지를 추가하면 해당 이미지가 첨부 파일로 업로드됩니다.
- 최대 698픽셀의 이미지를 업로드하거나 첨부할 수 있으며, 이미지가 정의된 크기보다 크면 원래 크기로 자동 조정됩니다. 이러한 픽셀 크기 제한은 PDF 보고서 생성이 적절한 형식으로 표시되고 보고서에서 이미지가 잘리지 않도록 하는 데 도움이 됩니다.

7. 케이스에 필요한 요소를 추가합니다.
8. 내용 저장을 클릭하여 새 보고서 템플릿의 내용을 저장합니다.
9. 미리 보기를 클릭하여 보고서 형식을 미리 보고 케이스 보고서를 생성할 때 보고서가 어떻게 생성되는지 확인합니다.

주:

- 케이스 필드: 보고서 템플릿을 수정할 때마다 템플릿에 추가된 내용을 미리 봅니다. 예를 들어 케이스 보고서를 생성하는 경우 간단한 설명이라는 필드를 추가하려는 경우 케이스 필드에서 해당 필드를 선택하면 해당 필드가 보고서 템플릿에 변수로 추가됩니다. 분석가에 대한 보고서가 생성되면 해당 설명에 대한 짧은 설명이 보고서에 표시됩니다.
- 기록: 보고서 템플릿 내에서 케이스의 아티팩트로 표시되는 특정 케이스의 관련 기록을 추가할 수도 있습니다. 예를 들어 옵저버블 관련 목록의 보고서에 악의적인 옵저버블을 표시하려면 보고서 템플릿에 추가할 수 있습니다. 이러한 관련 기록은 테이블 형식으로 표시됩니다
- 스크립트: 보고서의 날짜 및 시간을보고 싶을 때마다 보고서 템플릿에 현재 날짜 시간 스크립트를 추가 할 수 있으며 보고서 작성 날짜 및 시간이 추가됩니다.
- **MITRE ATT&CK:** 보고서에 MITRE 카드 관련 기술이 표시됩니다.

필요한 모든 케이스 관련 필드를 보고서 템플릿에 추가한 후에는 보고서 템플릿을 게시해야 합니다.

10. 게시를 클릭하여 템플릿을 게시합니다.
보고서 템플릿을 게시할 것인지 여부를 확인하는 메시지가 표시됩니다.

주:
보고서 템플릿을 게시하면 모든 사용자에 대해 이 템플릿을 사용할 수 있습니다. 오래된 경우 사용자에 대한 보고서 보기를 제한하려는 경우 게시된 보고서를 비활성화할 수 있으며, 이는 보고서 템플릿이 사용자에게 숨겨짐을 의미합니다. 게시된 보고서를 사용자가 보고 사용할 수 있도록 다시 활성화해야 해당 보고서가 숨겨집니다.

11. 보고서 템플릿을 원하지 않는 경우 삭제를 클릭하여 보고서 템플릿을 삭제합니다.
보고서 템플릿의 이름을 바꾸려면 편집을 클릭하고 원하는 필드를 수정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보고서의 시스템 속성

보고서의 시스템 속성은 아래에 설명되어 있습니다.

속성	설명	값
sn_sec_reporting.max_list_columns_allowed	보고서 PDF에서 목록을 렌더링할 때 추가할 수 있는 열 수를 제한합니다. 이렇게 하면 뷰의 시작부터 허용된 제한까지의 열이 사용됩니다.	5
sn_sec_reporting.report_default_style_object	CSS를 사용하여 자유 양식 필드, 왼쪽 패널, 보고서 목록의 CSS를 제어합니다.	(JSON 객체)
sn_sec_reporting.load_all_records	템플릿에서 만든 보고서의 목록에 대한 모든 기록을 로드합니다. true - 모든 기록을 로드합니다. false - sn_sec_reporting.reporting_list_records_count 속성으로 정의된 특정 수의 기록을 로드합니다.	아니오
sn_sec_reporting.reporting_list_records_count	보고서 편집기에 특정 수의 기록을 로드합니다.	20
sn_sec_tisc.sn_sec_tisc_case.default_record_urls	목록에서 URL을 제거할지 여부를 제어합니다.	예
sn_sec_tisc.show_all_tactics_reporting	예인 경우 보고서에 렌더링된 MITRE 목록의 모든 전술(케이스와 연결된 기술이 없는 전술 포함)이 표시됩니다.	아니오
sn_sec_tisc.reporting_email_template_sn_sec_tisc_case	모든 보고서 유형 케이스(sn_sec_tisc_case) 테이블에 대한 이메일 클라이언트 템플릿의 시스템 ID입니다.	b55e22c54324021060eee0ea78b8f2df
sn_sec_tisc.sn_sec_tisc_case.excluded_ctx_fields	필드를 매체하기 위한 보고서/템플릿 메뉴 옵션에서 케이스의 제외된 필드입니다.	(모든 제외된 케이스 필드 목록
sn_sec_tisc.sn_sec_tisc_case.ctx_menu_field_header	이 속성은 보고서/템플릿 메뉴 옵션에서 케이스 필드 레이블에 해당하는 UI 메시지 기록을 가져오는 데 사용됩니다.	sn_sec_tisc_case_reporting_ctx_menu_field_head

게시된 보고서 템플릿 편집

이 섹션을 사용하여 게시된 보고서 템플릿을 편집합니다.

시작하기 전에

필요한 역할: sn_sec_tisc.admin

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터 〉 관리.
2. 선택 보고서 〉 보고서 템플릿.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

기계번역

3. 필요한 보고서 템플릿을 선택합니다.
4. 보고서 템플릿에 표시되는 편집 버튼을 선택합니다.

   주:

   게시된 템플릿을 편집하고 있으며 케이스 보고서에서 사용할 수 있도록 하려면 템플릿을 다시 게시해야 함을 나타내는 확인 메시지가 표시됩니다. 편집을 계속하시겠습니까? 즉, 필요한 변경 작업을 수행한 후 편집된 템플릿을 다시 게시해야 합니다.

5. 확인 대화 상자에서 편집을 선택합니다.
6. 필수 컨텐츠 필드 또는 관련 목록을 추가하여 필요한 사항을 변경합니다.
7. 내용 저장을 선택합니다.
8. 게시 버튼을 선택하여 변경 내용을 게시합니다.
   보고서 템플릿을 게시하면 보고서 템플릿이 성공적으로 게시되었음을 나타내는 확인 메시지가 표시됩니다.

   주:

   - 보고서 템플릿을 게시하기 전에 보고서 템플릿 내용을 미리 볼 수도 있습니다.
   - 보고서 템플릿을 삭제하려는 경우 삭제를 선택하여 보고서 템플릿을 삭제할 수 있습니다.

보고서 템플릿 복제

보고서 템플릿 복제 증분 업데이트를 추가하려면 보고서 템플릿의 사본을 만들 수 있습니다.

시작하기 전에
필요한 역할: sn_sec_tisc.admin

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 보안 센터 〉 〉 관리.
2. 선택 보고서 〉 보고서 템플릿.
3. 템플릿을 선택합니다.
4. 중복을 클릭합니다.
   선택한 템플릿의 내용이 복제되고 해당 템플릿의 복사본이 표시됩니다. 템플릿은 다시 초안 상태가 되고, 내용을 사용자 지정한 다음 필요에 따라 템플릿 이름을 바꿀 수 있습니다.
5. 복사한 템플릿의 컨텐츠를 편집하거나 수정합니다.

   주:
   더 이상 필요하지 않은 경우 보고서 템플릿을 삭제하고 새 템플릿을 만들 수도 있습니다.

웹후크 작업

웹후크는 소스 시스템(TISC)의 이벤트에 의해 트리거되고 이벤트 데이터의 페이로드와 함께 대상 시스템(엔드포인트 URL이 있는 곳)으로 전송되는 HTTP 요청입니다.

의 위협 인텔리전스 보안 센터 이러한 웹후크는 이벤트가 발생할 때마다 대상 애플리케이션에 알리는 데 유용합니다.

TISC에서는 다음을 수행할 수 있습니다.

- 웹후크 구성
- 트리거 관리

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 재시도 메커니즘
- 확인 수행
- 구독 관리

웹후크에 대한 시스템 속성

웹후크의 시스템 속성은 아래에 설명되어 있습니다.

속성 이름	설명	유형	값
sn_sec_tisc.webhook_ignore_threat_score_reapply	위협 점수에 의해 트리거된 웹후크 이벤트를 무시합니다. 이력 다시 계산.	true/false	예
sn_sec_tisc.webhook_max_event_batch_size	하나의 웹후크 요청의 일부로 전송할 최대 이벤트 수입니다. 이 속성에 더 높은 값이 설정되어 있더라도 배치 크기는 2,000으로 제한됩니다.	정수	1000
sn_sec_tisc.webhook_retry_count	실패한 요청을 오류로 표시하고 다음 이벤트 배치로 이동하기 전에 다시 시도할 횟수입니다. 이 속성에 더 높은 숫자가 설정되어 있더라도 재시도 횟수는 10으로 제한됩니다.	정수	5
sn_sec_tisc.webhook_retry_interval	실패한 배치를 재시도하기 전에 대기할 시간(초)입니다. 이는 재시도 횟수에 따라 기하급수적으로 증가합니다. 예를 들어 retry_count 3이고 retry_interval 30이면 30, 60, 120초 후에 다시 시도가 실행됩니다. 이 속성에 더 높은 값이 설정되어 있더라도 초기 재시도 간격은 300초로 제한됩니다.	정수	30

웹후크 구성

위협 인텔리전스 보안 센터의 이벤트를 구독하도록 웹후크를 구성합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_sec_tisc.admin

이 태스크 정보
TISC 웹후크는 SIEM과 같은 보안 도구와 통합할 수 있는 기능을 제공합니다. 그런 다음 사용자는 옵저버블 또는 표시기 또는 맬웨어 또는 위협 행위자와 같은 다양한 아티팩트와 관련된 다양한 이벤트를 구독할 수 있습니다. TISC는 새로운 위협 인텔리전스를 사용할 수 있거나 TISC에서 기존 위협 인텔리전스 데이터가 업데이트 또는 삭제될 때 보안 도구(예: SIEM)에 알립니다.

예를 들어 위협 인텔리전스에 새 옵저버블이 추가될 때마다 페이로드 요청이 웹후크 URL 구성으로 전송됩니다. 이 페이로드 요청은 일반적으로 옵저버블 정보를 수집하고 보안 도구(예: SIEM)에 추가 정보로 제공합니다.

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 보안 센터 〉 관리.
2. 선택 웹후크 구성 〉 웹후크.
   웹후크 페이지가 표시됩니다.
3. 새로 만들기를 클릭합니다.

4. 확인 및 저장을 클릭합니다.
   구성 상세 정보가 잘못된 경우 구성 상세 정보가 변경되면 시스템에서 자동으로 연결을 확인한 다음 애플리케이션에 웹후크 확인에 실패했으며 구성 상세 정보를 확인하고 그에 따라 수정해야 한다는 경고 메시지가 표시됩니다.

   주:
   - 웹후크 확인을 위해 빈 요청 페이로드가 엔드포인트로 전송되며, 사용자는 빈 요청이 구성된 웹후크 엔드포인트에 전달될 때 엔드포인트가 성공적인 응답 코드(200)를 전송하는지 확인해야 합니다.
   - 기본적으로 생성된 모든 웹후크는 비활성화됨 상태이므로 웹후크를 활성화하고 활성화해야 합니다. 샘플 웹후크는 사용자에 대한 참조로 기본 시스템에 프로비저닝되어 있습니다.

트리거 구독

현재 웹후크에 대해 구독된 모든 웹후크 트리거 목록을 봅니다.

시작하기 전에
필요한 역할: sn_sec_tisc.admin

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 보안 센터 〉 관리.
2. 선택 웹후크 구성 〉 웹후크.
   웹후크 페이지가 표시됩니다.
3. 웹후크를 선택합니다.
   구독한 트리거 섹션이 표시됩니다.
4. 구독한 트리거 섹션에서 구독 버튼을 클릭합니다.
   목록 뷰에는 인스턴스에서 활성화된 모든 웹후크 트리거가 표시됩니다.
5. 원하는 웹후크 트리거를 선택하고 웹후크 트리거 대화 상자에서 구독을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

웹후크가 선택한 트리거를 성공적으로 구독했다는 확인 메시지가 표시됩니다. 여기에서 직접 새 트리거를 생성하고 웹후크를 구독할 수도 있습니다.

> **주:**
> 선택한 트리거에서 웹후크 구독을 취소할 수도 있습니다.

웹후크 오류 로그 보기

이 오류 로그 섹션을 사용하여 특정 웹후크의 상태에서 오류로 표시된 모든 감사 항목을 볼 수 있습니다.

시작하기 전에
필요한 역할: sn_sec_tisc.admin

이 태스크 정보
감사 로그를 통해 사용자는 실행을 자세히 조사하고 디버그하며 실행 실패의 근본 원인을 식별할 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 보안 센터 〉 관리.
2. 선택 웹후크 구성 〉 웹후크.
   웹후크 페이지가 표시됩니다.
3. 웹후크를 선택합니다.
4. 오류 로그로 이동합니다.
5. 오류 로그를 봅니다.
   목록 뷰에는 특정 웹후크의 모든 오류 로그가 표시됩니다.
6. 배치 열로 이동합니다.
7. 배치 **ID**를 클릭합니다.

   > **주:**
   > 각 오류 로그는 배치에 연결되며 배치 ID(배치 열)를 사용하여 연결된 배치 기록을 볼 수 있습니다. 배치 ID 중 하나를 클릭하면 별도의 탭에서 열립니다. 각 배치 ID에는 웹후크 배치 번호, 오류 메시지, 응답 상태 코드, 재시도 횟수, 실제 페이로드 데이터 및 웹후크로 전송될 이벤트 목록이 포함되어 있습니다.

8. 배치 재시도를 클릭하여 실패한 배치를 다시 시도합니다.
   이 버튼을 클릭하면 구성된 웹후크 엔드포인트에 요청 페이로드(특정 배치 정보)가 전송됩니다.

   > **주:**
   > 이 작업은 실행 오류가 있거나 성공적으로 완료된 배치 기록에만 사용할 수 있으며 재시도 상태의 기록은 자동으로 재시도됩니다.

웹후크 배치 보기

각 웹후크 실행에 대해 웹후크 배치 기록이 생성됩니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
웹후크 엔드포인트로 전송되는 API 호출 수를 줄이기 위해 이벤트 배치가 웹후크에서 구현됩니다. 각 웹후크에 대해 거의 동시에 트리거된 이벤트가 여러 개 있는 경우 이러한 모든 이벤트는 웹후크 엔드포인트에 동일한 요청의 일부로 전송됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 보안 센터 〉 관리.
2. 선택 웹후크 구성 〉 웹후크.
   웹후크 페이지가 표시됩니다.
3. 웹후크를 선택합니다.
4. 오류 로그로 이동합니다.
5. 오류 로그를 봅니다.
   목록 뷰에는 특정 웹후크의 모든 오류 로그가 표시됩니다.
6. 배치 열로 이동합니다.
7. 배치 **ID**를 클릭합니다.
   웹후크 배치 페이지가 표시됩니다.

주:
모든 일괄 처리는 ### sn_sec_tisc_webhook_batch에 저장됩니다.

다음은 웹후크 엔드포인트가 수신하는 샘플 페이로드 형식입니다.


```
{
   "batch_id": "06eeb3693b6bca10f6f82a60c5e45a7b",
   "events": [
      {
         "record": "Observable",
         "record_fields": {
            "is_false_positive": "false",
            "reputation": "malicious",
            "sys_updated_on": "2024-07-22T14:31:26.000Z",
            "type": "url",
            "sys_updated_by": "admin",
            "sys_created_on": "2024-07-04T06:45:20.000Z",
            "id": "url--1e77adb7eb8b06107750fa86cad0cd70",
            "is_defanged": "false",
            "sys_created_by": "SecCommon.System",
            "tags": "Enriched",
            "taxonomies": "T1: V1",
            "domain": "urlhaus.abuse.ch",
            "status": "active",
            "source_count": "1",
            "threat_score": "20",
            "sys_id": "da77adb7eb8b06107750fa86cad0cd70",
            "value": "https://urlhaus.abuse.ch/url/2578255/",
            "confidence": "89",
            "expiration_time": "2025-10-07T07:13:18.000Z",
            "tlp": "CLEAR"
         },
         "trigger": {
            "name": "Observable Update",
            "type": "UPDATE",
            "trigger_time": "2024-07-22T14:31:26.000Z",
            "trigger_fields": [
               {
                  "field_name": "reputation",
                  "previous_value": null,
                  "current_value": "malicious"
```


© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
            }
          ]
        }
      },
      {
        "record": "Observable",
        "record_fields": {
          "is_false_positive": "false",
          "reputation": "malicious",
          "sys_updated_on": "2024-07-22T14:31:19.000Z",
          "type": "url",
          "sys_updated_by": "admin",
          "sys_created_on": "2024-07-04T06:45:20.000Z",
          "id": "url--9a77adb7eb8b06107750fa86cad0cd6f",
          "is_defanged": "false",
          "sys_created_by": "SecCommon.System",
          "tags": "Enriched",
          "taxonomies": "T1: V1",
          "domain": "urlhaus.abuse.ch",
          "status": "active",
          "source_count": "1",
          "threat_score": "20",
          "sys_id": "5a77adb7eb8b06107750fa86cad0cd6f",
          "value": "https://urlhaus.abuse.ch/url/2578264/",
          "confidence": "89",
          "expiration_time": "2025-10-07T07:13:18.000Z",
          "tlp": "CLEAR"
        },
        "trigger": {
          "name": "Observable Update",
          "type": "UPDATE",
          "trigger_time": "2024-07-22T14:31:19.000Z",
          "trigger_fields": [
            {
              "field_name": "reputation",
              "previous_value": null,
              "current_value": "malicious"
            }
          ]
        }
      }
    ]
}
```


다음 표에는 웹후크 페이로드로 사용자에게 전송될 배치 페이로드 구조와 해당 속성이 나열되어 있습니다.

배치 페이로드의 매개변수	유형	설명
batch_id	문자열	배치의 고유 식별자를 지정합니다.
이벤트	객체 배열	해당 웹후크의 일부로 트리거되는 이벤트 배열을 포함합니다. 각 이벤트는 이벤트 생성 시 필드 값의

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

배치 페이로드의 매개변수	유형	설명
		스냅샷을 포함하며 트리거 정보도 포함합니다. 주: 이벤트 객체의 매개변수를 보는 방법에 대한 자세한 내용은 을 참조하십시오 웹후크 트리거.

주:

8. 배치 재시도 버튼을 클릭하여 실패한 배치를 재시도합니다.

주:
완료된 일괄 처리에 대해 일괄 처리 재시도를 트리거할 수도 있습니다.

웹후크 트리거

웹후크 트리거는 생성, 업데이트 및 삭제와 같은 이벤트 변경 사항을 추적해야 하는 위협 인텔리전스 엔터티를 필터링하는 데 사용됩니다.

시작하기 전에
필요한 역할: sn_sec_tisc.admin

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 보안 센터 〉 관리.
2. 선택 웹후크 구성 〉 트리거.
   웹후크 트리거 페이지가 표시됩니다.
3. 새로 만들기를 클릭합니다.
4. 저장을 클릭합니다.
   기본적으로 트리거는 비활성화된 상태로 생성됩니다.
5. 활성화를 클릭하여 트리거를 활성화하면 이 트리거를 웹후크가 구독할 수 있게 됩니다.

주:
활성화된 트리거를 비활성화하려면 비활성화 를 클릭하고, 비활성화하면 이 트리거에서 연결된 모든 웹후크가 구독 취소됩니다.

6. 샘플 페이로드 보기를 클릭하여 기록을 선택합니다.
   해당 특정 웹후크 트리거의 샘플 페이로드를 봅니다. 선택한 테이블에 따라 지정된 테이블의 해당 기록이 기록 선택 드롭다운 목록에 채워집니다. 샘플 페이로드를 보려면 기록을 선택합니다. 샘플 페이로드는 JSON 형식으로 표시됩니다. 페이로드의 필드는 다음과 같습니다.
7. 드롭다운 목록에서 기록 유형을 선택합니다.
   선택한 기록에 따라 페이로드가 자동으로 변경됩니다.

```
{
   "record": "Observable",
   "record_fields": {
      "additional_context": "This could be a potential malicious IP. ",
```


© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
      "attack_phases": "Lockheed Martin: Command and Control",
      "author": "Anomali",
      "confidence": "50",
      "description": "This could be a potential malicious IP. ",
      "expiration_time": "2024-12-01T00:00:00.000Z",
      "first_observed": "2024-01-01T00:00:00.000Z",
      "first_seen": "2024-01-01T00:00:00.000Z",
      "id": "ipv4-addr--70526b0a436a02102164e0ea78b8f210",
      "is_defanged": "false",
      "is_false_positive": "false",
      "last_observed": "2024-01-01T00:00:00.000Z",
      "last_seen": "2024-01-01T00:00:00.000Z",
      "reputation": "suspicious",
      "source_count": "1",
      "status": "active",
      "sys_created_by": "SecCommon.System",
      "sys_created_on": "2024-06-04T00:00:00.000Z",
      "sys_id": "30526b0a436a02102164e0ea78b8f210",
      "sys_updated_by": "system",
      "sys_updated_on": "2024-06-15T00:00:00.000Z",
      "tags": "critical",
      "taxonomies": "MITRE: T121",
      "threat_level": "medium",
      "threat_score": "24",
      "threat_severity": "medium",
      "tlp": "CLEAR",
      "type": "ip_v4_address",
      "usage_categories": "APT",
      "value": "116.98.170.70"
   },
   "trigger": {
      "name": "Observable Update",
      "type": "UPDATE",
      "trigger_time": "2024-07-26T07:27:29.000Z",
      "trigger_fields": [
         {
            "field_name": "confidence",
            "previous_value": "30",
            "current_value": "50"
         }
      ]
   }
}
```


트리거 페이로드의 매개변수 목록

트리거 페이로드의 매개변수	유형	설명
기록	문자열	옵저버블 또는 표시기와 같은 기록 유형을 지정합니다.
record_fields	객체	이벤트가 생성될 때 기록 필드 스냅샷을 지정합니다. 지원되는 필드 목록은 아래 섹션의 테이블을 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

트리거 페이로드의 매개변수	유형	설명
트리거	객체	일치하는 트리거 정보를 지정합니다.
trigger.name	문자열	트리거의 이름을 지정합니다.
trigger.type	문자열	트리거의 유형을 지정합니다. 유효한 값은 CREATE, UPDATE, DELETE입니다.
trigger.trigger_time	날짜(UTC 시간대의 ISO 형식)	기록에서 이벤트가 발생한 시간을 지정합니다.
trigger_fields	객체 배열	UPDATE 트리거 유형에만 사용할 수 있습니다. 발생한 이벤트의 일부로 변경된 트리거 필드 목록을 지정합니다. **trigger_fields** 내부의 매개변수는 다음과 같습니다. ○ **field_name**: 변경된 필드 이름 제공 ○ **previous_value**: 필드의 이전 값을 제공합니다. ○ **current_value**: 필드의 현재 값을 제공합니다.

트리거 생성 및 업데이트에 대해 지원되는 필드 목록

테이블	열 이름	열 레이블
캠페인	별칭	별칭
캠페인	설명	설명
캠페인	first_seen	처음으로 발견됨
캠페인	last_seen	마지막으로 발견됨
캠페인	이름	이름
캠페인	목표	목표
표시기	additional_context	추가 컨텍스트
표시기	attack_phases	공격 단계
표시기	저자	작성자
표시기	신뢰도	신뢰도
표시기	설명	설명
표시기	expiration_time	만료 시간
표시기	first_detected	처음 탐지됨
표시기	first_observed	처음으로 관찰됨
표시기	first_seen	처음으로 발견됨
표시기	ID	ID
표시기	indicator_types	표시기 유형

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테이블	열 이름	열 레이블
표시기	ioc_classification	IOC 분류
표시기	last_observed	마지막으로 관찰됨
표시기	last_seen	마지막으로 발견됨
표시기	이름	이름
표시기	pattern	패턴
표시기	pattern_type	패턴 유형
표시기	pattern_version	패턴 버전
표시기	플랫폼	플랫폼
표시기	해지됨	해지함
표시기	source_count	소스 수
표시기	spec_version	사양 버전
표시기	상태	상태
표시기	태그	TISC 태그
표시기	분류	분류
표시기	threat_level	위협 수준
표시기	threat_severity	위협 심각성
표시기	TLP	TLP
표시기	usage_categories	사용 범주
표시기	valid_from	유효 기간(시작)
표시기	valid_until	유효 기간
맬웨어	별칭	별칭
맬웨어	attack_phases	공격 단계
맬웨어	설명	설명
맬웨어	executable_process_architectures	프로세스 아키텍처
맬웨어	first_seen	처음으로 발견됨
맬웨어	implementation_languages	구현 언어
맬웨어	is_family	제품군임
맬웨어	last_seen	마지막으로 발견됨
맬웨어	malware_capabilities	맬웨어 역량
맬웨어	malware_types	맬웨어 유형
맬웨어	이름	이름
객체(공통 객체 필드)	additional_context	추가 컨텍스트
객체(공통 객체 필드)	신뢰도	신뢰도
객체(공통 객체 필드)	expiration_time	만료 시간
객체(공통 객체 필드)	ID	ID

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테이블	열 이름	열 레이블
객체(공통 객체 필드)	해지됨	해지함
객체(공통 객체 필드)	source_count	소스 수
객체(공통 객체 필드)	spec_version	사양 버전
객체(공통 객체 필드)	상태	상태
객체(공통 객체 필드)	태그	TISC 태그
객체(공통 객체 필드)	분류	분류
객체(공통 객체 필드)	threat_level	위협 수준
객체(공통 객체 필드)	threat_severity	위협 심각성
객체(공통 객체 필드)	TLP	TLP
옵저버블	additional_context	추가 컨텍스트
옵저버블	attack_phases	공격 단계
옵저버블	저자	작성자
옵저버블	신뢰도	신뢰도
옵저버블	설명	설명
옵저버블	expiration_time	만료 시간
옵저버블	first_observed	처음으로 관찰됨
옵저버블	first_seen	처음으로 발견됨
옵저버블	ID	ID
옵저버블	is_defanged	제거됨 여부
옵저버블	is_false_positive	긍정 오류 여부
옵저버블	last_observed	마지막으로 관찰됨
옵저버블	last_seen	마지막으로 발견됨
옵저버블	평판	평판
옵저버블	source_count	소스 수
옵저버블	상태	상태
옵저버블	태그	TISC 태그
옵저버블	분류	분류
옵저버블	threat_level	위협 수준
옵저버블	threat_score	위협 점수
옵저버블	threat_severity	위협 심각성
옵저버블	TLP	TLP
옵저버블	유형	유형
옵저버블	usage_categories	사용 범주
옵저버블	값	값
위협 액터	별칭	별칭

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테이블	열 이름	열 레이블
위협 액터	설명	설명
위협 액터	first_seen	처음으로 발견됨
위협 액터	목표	목표
위협 액터	last_seen	마지막으로 발견됨
위협 액터	이름	이름
위협 액터	personal_motivations	개인적인 동기
위협 액터	primary_motivation	기본 동기
위협 액터	resource_level	자원 수준
위협 액터	secondary_motivations	보조 동기
위협 액터	세련	전문성
위협 액터	threat_actor_roles	위협 액터 역할
위협 액터	threat_actor_types	위협 액터 유형
위협 보고서	설명	설명
위협 보고서	이름	이름
위협 보고서	게시됨	게시 날짜:
위협 보고서	report_types	보고서 유형
취약성	affected_software	영향을 받는 소프트웨어
취약성	설명	설명
취약성	exploitation_status	취약점 공격 상태
취약성	exploit_exists	악용 존재
취약성	이름	이름
취약성	게시됨	게시 날짜:
취약성	record_last_modified	마지막으로 수정된 기록
취약성	severity	심각도

다음은 모든 엔터티에 공통적으로 적용되는 적용 가능한 시스템 필드 목록이며, 이는 생성 및 업데이트 트리거에 대한 웹후크 트리거 페이로드에서 지원됩니다.

- sys_id(시스템 ID)
- sys_created_on(생성됨)
- sys_created_by(작성자)
- sys_updated_on(업데이트됨)
- sys_updated_by(업데이트한 사람)

주:
삭제의 경우 sys_id(시스템 ID)만 페이로드의 일부로 웹후크 엔드포인트 URL로 전송되며 다른 시스템 필드는 지원되지 않습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

트리거 삭제에 대해 지원되는 필드 목록

테이블	열 이름	열 레이블
옵저버블	유형	유형
옵저버블	값	값
표시기	이름	이름
표시기	pattern	패턴
표시기	pattern_type	패턴 유형
표시기	valid_from	유효 기간(시작)
캠페인	이름	이름
맬웨어	is_family	제품군임
맬웨어	이름	이름
위협 액터	이름	이름
위협 보고서	이름	이름
위협 보고서	게시됨	게시 날짜:
취약성	이름	이름
취약성	severity	심각도

노드맵에 대한 도구 설명 구성

이 섹션을 사용하여 조사 캔버스의 노드 맵 관계에 대한 도구 설명을 구성합니다.

시작하기 전에

필요한 역할: sn_sec_tisc.admin

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터 〉 관리 〉 노드맵 통제 〉 도구 설명 구성.
2. 목록에서 원하는 객체를 선택합니다.
   기본적으로 다음 세 개의 기록이 기본 시스템에 프로비저닝됩니다.
   a. 옵저버블
   b. 표시기
   c. 객체
3. 예제 기록으로 옵저버블 을 선택합니다.
4. 필요한 경우 옵저버블 기록에 하나 이상의 값을 추가합니다.
   마찬가지로 표시기 및 기타 개체에 값을 추가합니다.

   주:
   각 객체는 최대 6개의 값을 지원합니다.

5. 저장을 선택하여 변경 내용을 적용합니다.
6. 조사 캔버스 섹션으로 이동하여 새로 고침 아이콘을 선택합니다.
   도구 설명 구성 페이지에서 구성한 것과 동일한 값이 각 노드 맵에 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

자동화된 플로우 작업

이러한 정의된 단계를 사용하여 TISC에서 자동화된 플로우를 사용하는 방법과 해당 기능을 알아봅니다.

TISC 역할로 실행되는 플로우를 생성합니다. TISC에서 플로우는 다음에 대해 생성됩니다.

- 자동화된 IOC 보강
- 위협과 관련된 IoC를 분석, 평가 및 전파합니다.
- 위협과 관련된 IoC를 분석 및 평가하고 인시던트를 생성합니다.
- 취약성 관리 지원.
- 제로 데이 취약성 추적.

주:
모든 플로우는 사용자가 필요에 따라 사용자 지정하거나 복사할 수 있도록 초안 상태로 제공되는 템플릿입니다.

재사용 가능한 작업

플로우 작업	설명
엔터티에 태그 추가	이를 지원하는 엔터티(옵저버블/표시기/객체)에 태그를 추가합니다.
엔터티에서 태그 제거	태그를 지원하는 엔터티 (옵저버블/표시기/객체)에 대한 태그를 제거합니다.
IP 주소가 CIDR 범위에 있는지 확인	IP 주소가 CIDR 범위 내에 있는지 확인합니다.
IP 주소가 범위에 있는지 확인	IP 주소가 시작 및 종료 범위 사이에 있는지 확인합니다.

자동화된 IOC 보강

특정 기준과 일치할 때 플로우를 사용하여 IOC의 보강을 자동화하는 방법을 알아봅니다.

시작하기 전에

필요한 역할:

- 시스템 관리자(보기, 만들기 또는 편집)
- sn_sec_tisc.admin(보기)

이 태스크 정보

다음과 같은 경우에만 IOC 트리거 보강을 자동화합니다.

- 옵저버블의 유형은 도메인 이름, IPv4 주소 또는 IPv6 주소입니다.
- 옵저버블이 처리된 상태입니다.
- 옵저버블에 보강 또는 보강 건너뛰기 태그가 없습니다.

프로시저

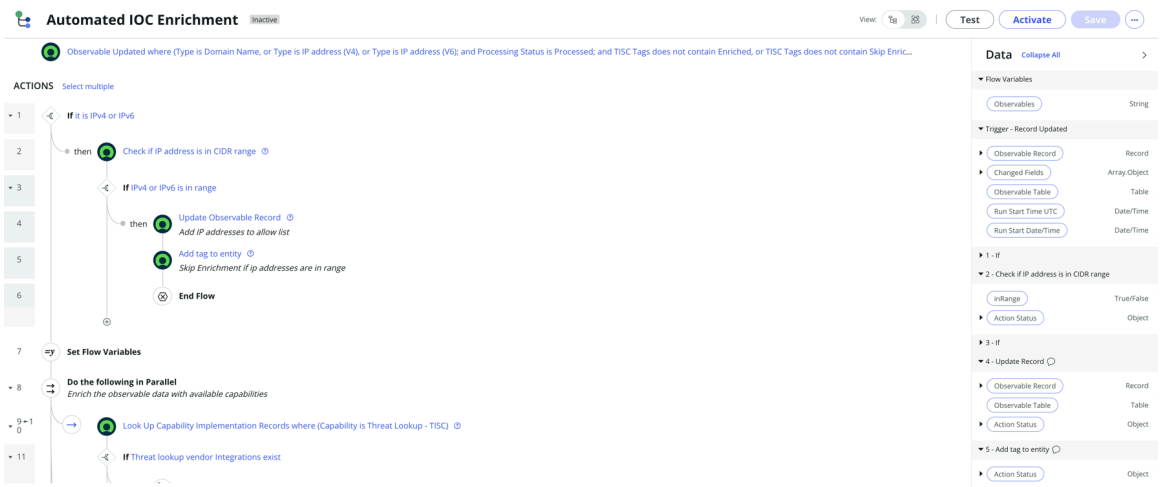
1. 다음으로 이동 모두 〉 위협 인텔리전스 보안 센터 〉 관리.
2. 선택 자동화된 플로우.
3. 플로우 디자이너에서 해당 규칙 상세 정보를 보려면 자동화된 **IOC** 보강 작업 링크를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 다음 트리거에 대한 플로우 디자이너 작업을 봅니다.

   Observable Updated where (Type is Domain Name, or Type is IP address (V4), or Type is IP address (V6); and Processing Status is Processed; and TISC Tags does not contain Enriched, or TISC Tags does not contain Skip Enrichment, or TISC Tags does not contain Potential New Threat)

5. 옵저버블이 **IPv4** 또는 **IPv6** 주소이고 허용된 **CIDR** 범위 내에 속하는 경우 다음을 수행합니다.
   a. 허용 목록에 옵저버블을 추가합니다.
   b. 옵저버블 태그를 Skip Enrichment(보강 건너뛰기)로 업데이트합니다.
   c. 이 옵저버블에 대한 플로우를 종료합니다.
6. 그렇지 않으면 사용 가능한 기능으로 옵저버블 데이터를 보강합니다.
   a. 위협 조회 및 사이팅 검색을 수행하여 옵저버블에 대한 추가 정보를 수집합니다.
   b. 보강된 데이터로 옵저버블을 업데이트합니다.
   c. IOC가 처리되었음을 나타내기 위해 보강됨 태그를 추가합니다.
7. 또한 옵저버블의 평판이 깨끗한 경우 다음을 수행합니다.
   a. 옵저버블을 긍정 오류 및 비활성화로 표시합니다.
8. 그 외에는 옵저버블 평판을 알 수 없는 경우
   a. 잠재적 위협 아님 및 보강됨 태그를 추가하여 위협이 아님을 나타냅니다.



신뢰할 수 있는 파트너와 고위험 IOC의 공유 자동화

신뢰할 수 있는 파트너와 고위험 IOC를 자동으로 공유하는 방법을 알아보세요.

시작하기 전에

필요한 역할:

- 시스템 관리자(보기, 만들기 또는 편집)
- sn_sec_tisc.admin(보기)

이 태스크 정보

신뢰할 수 있는 파트너와 고위험 IOC를 자동으로 공유하는 것은 다음과 같은 경우에만 트리거됩니다.

- 옵저버블의 유형은 도메인 이름, IPv4 주소 또는 IPv6 주소입니다.
- 옵저버블이 처리된 상태입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 보안 센터 〉 관리.
2. 선택 자동화된 플로우.
3. 플로우 디자이너에서 해당 규칙 상세 정보를 보려면 신뢰할 수 있는 파트너와 고위험 IOC의 자동화된 공유 작업 링크를 선택합니다.
4. 다음 트리거에 대한 플로우 디자이너 작업을 봅니다.

   ```
   Daily at 12.00.00
   Run every day once
   ```

5. 작업:

   a. 시스템 속성 기록 조회 및 찾아보기 아웃바운드 인텔리전스 임계치 한도:

   ```
   Look Up System Property Record where (Name is
    sn_sec_tisc.shared_intelligence_entity_threshold).
   ```

   b. IOC 유형 = IP, 도메인, 해시; 평판 = 악의적 ; 신뢰도 〉= 80 또는 위협 점수 〉=80.

   ```
   Look Up Observable Records where (Type is IP address (V4), or Type is IP address (V6),
    or Type is Domain Name, or Type is MD5 hash; and Confidence greater than 80, and
    Reputation is Malicious, and Processing Status is Processed, and Updated on Yesterday)
    IOC type = IP, Domain, Hash; Reputation = Malicious ; confidence >= 80 or Threat Score
    >=80.
   ```

6. 아웃바운드 인텔리전스 기록에 추가할 수 있는 기록의 임계치가 충족되면 다음을 수행합니다.

   a. 시스템은 처리를 위해 기록을 자동화된 아웃바운드 인텔리전스 작업에 자동으로 전달합니다.

   b. 신뢰할 수 있는 파트너와 고위험 IOC를 공유하는 흐름을 종료합니다.

7. 기록 카운트가 0보다 크면 시스템이 나머지 기록을 처리합니다.
   예제:

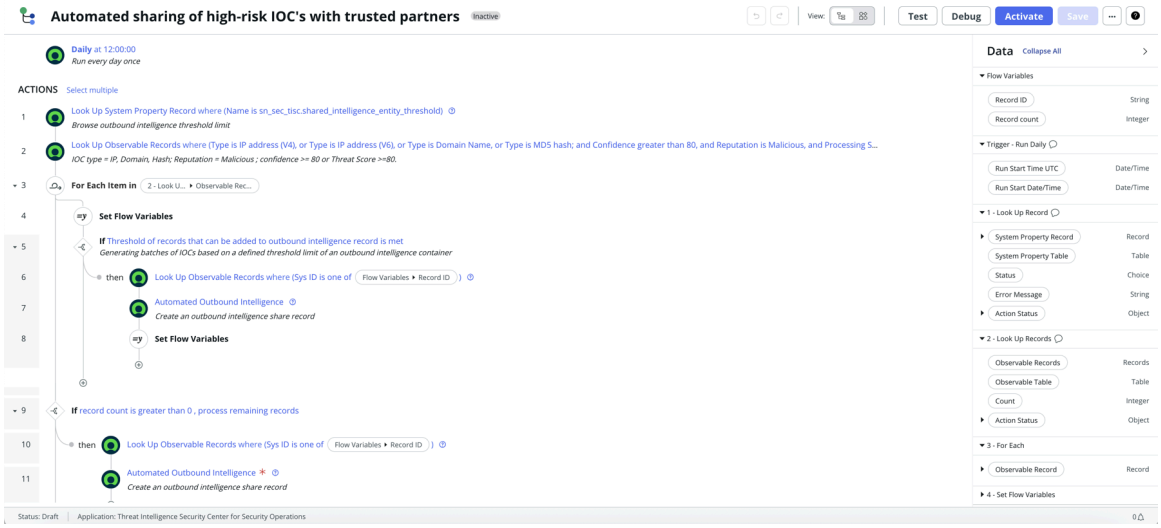
   정의된 임계치 한도가 1,000이고 총 2,030개의 기록이 처리되어야 하는 경우:

   - 아웃바운드 인텔리전스 기록 #1은 처음 1,000개 기록으로 생성됩니다.
   - 다음 1,000개 기록으로 아웃바운드 인텔리전스 기록 #2가 생성됩니다.
   - 나머지 30개 기록으로 아웃바운드 인텔리전스 기록 #3이 생성됩니다.

   이 일괄 처리 프로세스는 모든 인텔리전스 기록을 효율적으로 처리하면서 임계치 한계가 준수되도록 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

8. 신뢰할 수 있는 파트너와 고위험 IOC를 공유하는 흐름을 종료합니다.



관련 정보

아웃바운드 인텔리전스 기록 공유 자동화

GUI에서 아웃바운드 인텔리전스 기록 공유

TAXII 컬렉션에 위협 인텔리전스 자동 추가

위협 인텔리전스를 TAXII 서버 컬렉션에 자동으로 추가하는 방법을 알아봅니다.

시작하기 전에

필요한 역할:

- 시스템 관리자(보기, 만들기 또는 편집)
- sn_sec_tisc.admin(보기)

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 보안 센터 〉 관리.
2. 선택 자동화된 플로우.
3. 플로우 디자이너에서 해당 규칙 상세 정보를 보려면 **TAXII** 수집 작업 링크에 위협 인텔리전스 자동 추가를 선택합니다.
4. 다음 트리거에 대한 플로우 디자이너 작업을 봅니다.

   Observable Created or Updated where (Type is IP address (V4), or Type is IP address (V6), or Type is Domain Name; and TISC Tags contains Add to: Sample Collection, and Reputation is Malicious, and Threat Score greater than or is 60

5. 작업

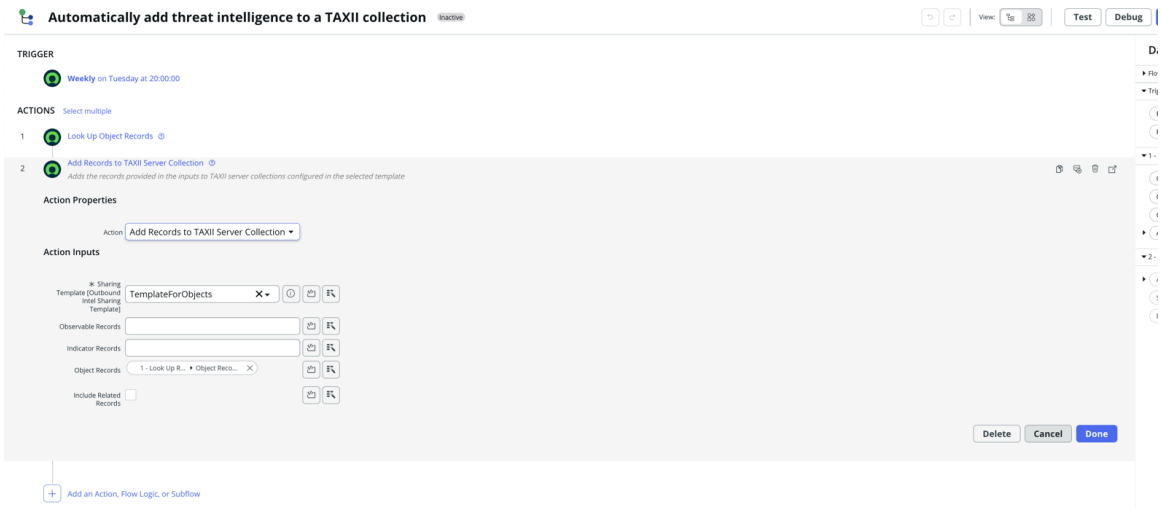
   입력에 제공된 기록을 선택한 템플릿에 구성된 TAXII 서버 컬렉션에 추가합니다.

   a. **TAXII** 서버 컬렉션에 기록 추가

   b. **TAXII** 서버 컬렉션에 기록 추가

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

6. TAXII 컬렉션에 위협 인텔리전스를 추가하는 플로우를 종료합니다.



옵저버블 분석, 평가 및 배포

위협과 관련된 옵저버블을 분석하고 배포하는 방법을 알아봅니다.

시작하기 전에

필요한 역할:

- 시스템 관리자(보기, 만들기 또는 편집)
- sn_sec_tisc.admin(보기)

이 태스크 정보

사이팅 검색 보강이 요청될 때마다 사이팅 없이 반환됩니다.

프로시저

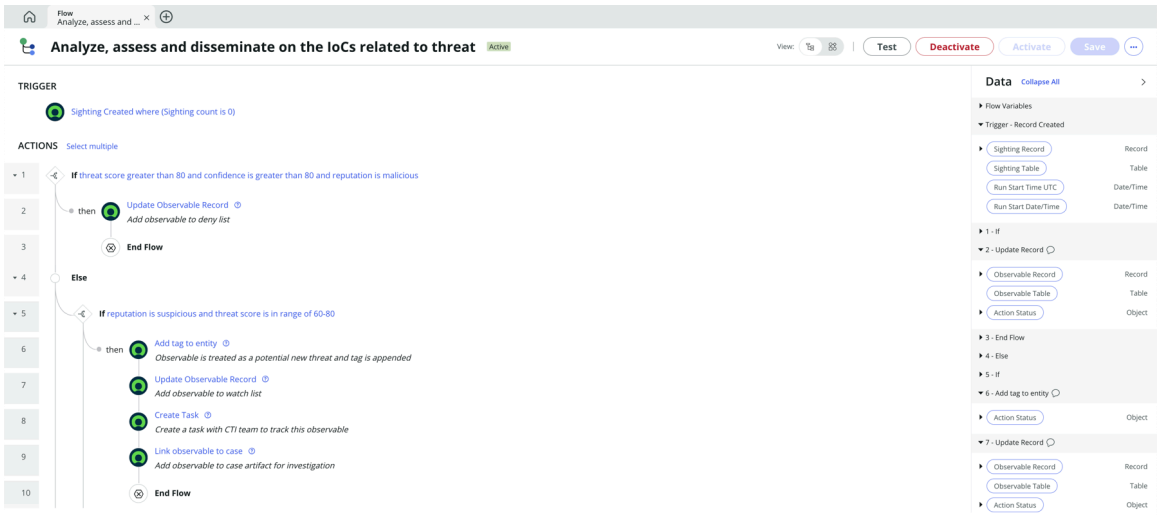
1. 다음으로 이동 모두 〉 위협 인텔리전스 보안 센터 〉 관리.
2. 선택 자동화된 플로우.
3. 위협 작업과 관련된 **IoC** 링크에서 분석, 평가 및 배포를 선택하여 플로우 디자이너에서 해당 규칙 상세 정보를 봅니다.
4. 다음 트리거에 대한 플로우 디자이너 작업을 봅니다.

   Sighting Created where (Sighting count is 0)

5. 옵저버블의 위협 점수가 80보다 크고 신뢰도가 80보다 크며 평판이 악성입니다.
   a. 거부 목록에 옵저버블을 추가합니다.
   b. 이 옵저버블에 대한 플로우를 종료합니다.
6. 그렇지 않으면 옵저버블 평판이 의심스럽고 위협 점수가 **60-80** 범위에 있습니다.
   a. 잠재적인 새로운 위협이라는 태그를 추가합니다.
   b. 감시 목록에 옵저버블을 추가합니다.
   c. CTI 팀과 함께 케이스 작업을 생성하여 이 옵저버블을 추적하고 추가로 분석합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

d. 조사를 위해 옵저버블을 케이스에 연결합니다.



위협 IoC 분석 및 평가

위협이 되는 IOC를 분석하고 보안 인시던트 팀에 알리는 방법을 알아봅니다.

시작하기 전에

필요한 역할:

- 시스템 관리자(보기, 만들기 또는 편집)
- sn_sec_tisc.admin(보기)

이 태스크 정보

사이팅 검색 보강이 요청될 때마다:

- 옵저버블이 발견된 경우(카운트 > 0) 및
- 옵저버블 평판이 악성이며
- 옵저버블 위협 점수는 > 80이며
- 옵저버블 신뢰도 > 80

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 보안 센터 〉 관리.
2. 선택 자동화된 플로우.
3. 분석을 선택하고, 위협과 관련된 IoC를 평가하고, 인시던트 작업 링크 생성을 선택하여 플로우 디자이너에서 해당 규칙 상세 정보를 확인합니다.
4. 다음 트리거에 대한 플로우 디자이너 작업을 봅니다.

   Sighting Created where (Sighting count greater than 0, and Observable. Reputation is Malicious, and Observable. Threat Score greater than 80, and Observable. Confidence greater than 80)

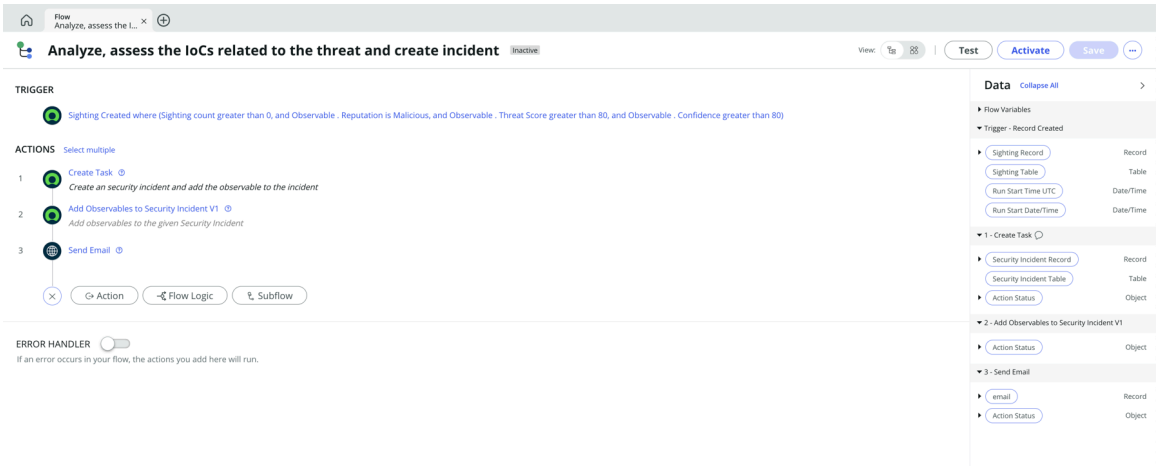
5. 사이팅이 작성된 경우(관찰 카운트가 0보다 크고 옵저버블. 평판은 악의적이며 관찰 가능합니다. 위협 점수가 80보다 크고 옵저버블입니다. 신뢰도가 80보다 크면, 다음과 같습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 보안 인시던트를 생성하고 인시던트에 옵저버블을 추가합니다.

b. 보안 인시던트 V1에 옵저버블을 추가합니다.

c. 이메일 커뮤니케이션을 보냅니다.



취약성 관리 지원

VR의 관련 취약성과 함께 TISC에서 새로운 취약성이 생성되는 방법에 대해 알아봅니다.

시작하기 전에

필요한 역할:

- 시스템 관리자(보기, 만들기 또는 편집)
- sn_sec_tisc.admin(보기)

이 태스크 정보

TISC에서 새로운 취약성이 생성되고 VR에 관련 취약성이 있는 경우.

- VR 취약점(v2) 점수가 > 8이거나 VR 취약점(v3) 점수가 > 8인 경우.
- 관련된 총 VI가 0보다 큽니다.

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 보안 센터 〉 관리.

2. 선택 자동화된 플로우.

3. 플로우 디자이너에서 해당 규칙 상세 정보를 보려면 취약성 관리 지원 작업 링크를 선택합니다.

4. 다음 트리거에 대한 플로우 디자이너 작업을 봅니다.

When new vulnerability is created in TISC and there is a related vulnerability in VR.

5. 해당 취약성과 관련된 정정된 총 VI의 백분율이 100%이면

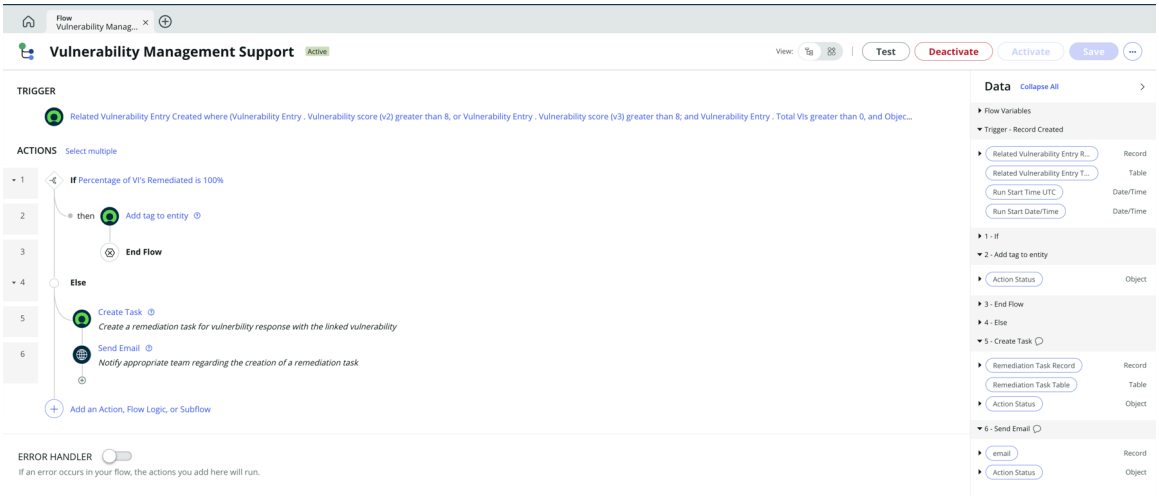
a. 정정됨이라는 태그를 옵저버블에 추가합니다.

6. 그렇지 않으면 사용 가능한 기능으로 옵저버블 데이터를 보강합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. VR에 대한 정정 작업을 생성합니다.

b. 관련 VR 팀에 알립니다.



제로 데이 취약성 추적

시스템에 들어오는 RSS 피드를 분석하는 방법에 대해 알아봅니다.

시작하기 전에

필요한 역할:

- 시스템 관리자(보기, 만들기 또는 편집)
- sn_sec_tisc.admin(보기)

이 태스크 정보

새 RSS 피드가 시스템에 생성되고 제목이나 설명에 'Zero Day'에 대한 언급이 있을 때마다.

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 보안 센터 〉 관리.

2. 선택 자동화된 플로우.

3. 플로우 디자이너에서 해당 규칙 상세 정보를 보려면 제로 데이 취약성 추적 링크를 선택합니다.

4. 다음 트리거에 대한 플로우 디자이너 작업을 봅니다.

RSS Feed Created where (Title contains zero day, or Description contains zero day, or Title contains zero_day, or Description contains zero_day, or Title contains zero-day, or Description contains zero-day)

5. 옵저버블이 **IPv4** 또는 **IPv6** 주소이고 허용된 **CIDR** 범위 내에 속하는 경우 다음을 수행합니다.

a. VR 팀에 대한 정정 작업과 함께 TISC 팀에 대한 케이스를 생성합니다.

b. 관련 TISC 팀 및 VR 팀에 알립니다.

자동화된 플로우 테이블

다음 테이블은 자동화된 플로우에 사용되는 엔터티와 보강 테이블 간의 관계 테이블을 이해하는 데 도움이 됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

엔터티 간 관계 테이블

테이블	엔터티
관련 표시기 옵저버블	sn_sec_tisc_m2m_indicator_observable
관련 표시기	sn_sec_tisc_m2m_indicator
관련 옵저버블	sn_sec_tisc_m2m_observable
객체-객체 관계	sn_sec_tisc_m2m_object
관련 표시기 객체	sn_sec_tisc_m2m_object_indicator
객체-옵저버블 관계	sn_sec_tisc_m2m_object_observable

보강 테이블

테이블	엔터티
위협 조회 결과	sn_sec_tisc_lookup_result
사이팅	sn_sec_tisc_sighting
옵저버블 보강 결과	sn_sec_tisc_observable_enrichment_result

위협 인텔리전스 보안 센터 참조

참조 주제는 에 위협 인텔리전스 보안 센터대한 추가 정보를 제공합니다.

참조 정보	주제에 대한 링크
도메인 분리 및 위협 인텔리전스 보안 센터	도메인 분리 및 Threat Intelligence Security Center
애플리케이션과 함께 위협 인텔리전스 보안 센터 설치되는 구성요소	위협 인텔리전스 보안 센터와 함께 설치되는 구성요소

도메인 분리 및 **Threat Intelligence Security Center**

위협 인텔리전스 보안 센터에서는 도메인 분리가 지원됩니다. 도메인 분리를 사용하여 데이터, 프로세스 및 관리 작업을 도메인이라는 논리적 그룹으로 분할할 수 있습니다. 어떤 사용자가 데이터를 보고 액세스할 수 있는지를 포함하여 이러한 분리의 여러 측면을 제어할 수 있습니다.

지원 수준: 표준

- 기본 수준 지원의 모든 측면을 포함합니다.
- 애플리케이션 속성이 필요에 따라 도메인을 인식합니다.
- 비즈니스 논리: 서비스 제공자(SP)가 고객별로 프로세스를 만들거나 수정합니다. 사용 사례는 여러 SP 고객이 단일 인스턴스에서 애플리케이션을 올바르게 사용하는 것을 반영합니다.
- 인스턴스 소유자는 특정 애플리케이션에 필요한 대로 테넌트별 최소 실행 가능한 제품(MVP) 비즈니스 논리 및 데이터 매개변수를 구성해야 합니다.

샘플 사용 사례: 관리자가 한 테넌트에 대해서는 기록이 닫히지만 다른 테넌트에 대해서는 기록이 닫히지 않는 경우 설명이 필요하도록 설정할 수 있어야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

지원 수준에 대한 자세한 내용은 도메인 분리를 위한 애플리케이션 지원 을 참조하십시오.

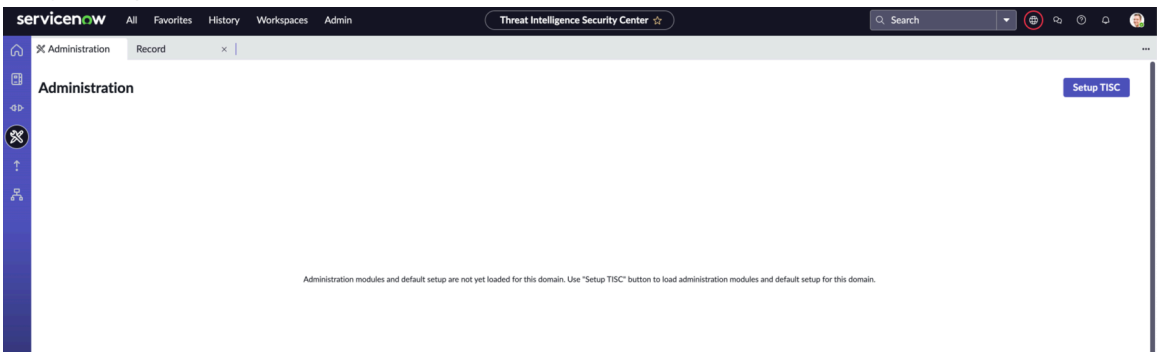
개요

의 모든 기능에 위협 인텔리전스 보안 센터대해 도메인 분리가 활성화됩니다.

위협 인텔리전스 보안 센터에서 도메인 분리가 작동하는 방식

- 기본 시스템에 프로비저닝된 모든 구성 관련 기록은 전역 도메인으로 제공됩니다. 인스턴스가 도메인으로 구분된 경우 TISC 작업 공간의 관리 모듈에서 사용자에게 **TISC** 설정 명시적 버튼이 표시됩니다. 기본 시스템이 프로비저닝된 전역 도메인 구성을 해당 도메인에 복제하려면 이 버튼을 클릭합니다.

  도메인 분리

  주:
  사용자는 도메인별 구성 기록만 활성화 또는 수정해야 하며 전역 도메인에서 구성 기록을 활성화하거나 수정해서는 안 됩니다.

- 기본 시스템에 몇 가지 플랫폼 알림 규칙(sysevent_email_action)이 프로비저닝되어 있으며, 이러한 알림 규칙은 필수 도메인에 복제되어야 하며 도메인별 알림 규칙만 사용하도록 설정해야 합니다.

  주:
  규칙 알림에 대한 자세한 내용은 다음으로 이동하십시오. 시스템 통보 〉 알림 사용자가 기본 시스템에서 프로비저닝된 기본 알림 규칙을 식별할 수 있는 방법을 이해하기 위해 이름 `sn_sec_tisc` 부터 시작하여 테이블에 정의된 모든 전역 도메인 알림 규칙을 필터링합니다.

- 수집된 모든 구성 및 데이터는 각 도메인별로 다르므로 한 도메인의 사용자는 다른 도메인의 데이터에 액세스할 수 없습니다.
- Domain Support - Domain Extensions Installer 플러그인을 설치하여 이 애플리케이션으로 도메인 분리 환경을 구성합니다.
- 모든 기본 시스템 애플리케이션 테이블에 대해 도메인 열이 추가됩니다.
- 테넌트 도메인은 플랫폼 제공 기능을 사용하여 자체 애플리케이션 데이터를 관리합니다.
- 인스턴스 소유자가 도메인 분리할 수 있는 비즈니스 로직 및 프로세스는 플랫폼이 지원하는 것과 동일합니다.
- 테넌트 도메인에서 관리할 수 있는 비즈니스 논리 및 프로세스는 플랫폼이 지원하는 것과 동일합니다.
- 관리 섹션에서 설정 페이지에 액세스할 수 있습니다. 도메인 분리 뷰를 보려면 관리 섹션 아래에 제공된 링크를 클릭합니다.
- TISC 홈 대시보드에서 PA(퍼포먼스 분석) 표시기를 사용하여 위젯에 대한 도메인 분리를 지원하려면 자세한 절차는 KB 문서 KB1647990 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

도메인 분리 테이블

모든 테이블은 도메인으로 분리됩니다.

사용 사례

이 애플리케이션의 모든 기능은 도메인으로 분리되어 있습니다.

관련 정보

서비스 제공자용 도메인 분리

위협 인텔리전스 보안 센터와 함께 설치되는 구성요소

애플리케이션을 다운로드하고 활성화하면 위협 인텔리전스 보안 센터 사용자 역할 및 속성을 포함한 여러 유형의 구성요소가 설치됩니다.

설치되는 속성

필요한 역할: sn_sec_tisc.admin

보안 관리자 [sn_sec_tisc.admin] 역할이 있는 사용자는 이를 수정할 수 있습니다.

속성	사용량
위협 인텔리전스 보안 센터에 대한 속성	
이렇게 하면 모든 상관관계 규칙이 비활성화됩니다. 선택한 상관 관계 규칙을 비활성화해야 하는 경우 상관 관계 규칙의 "활성" 필드를 대신 사용합니다. sn_sec_tisc.disable_correlation_rules	• 유형: true | false • 기본값: false
이 속성은 위협 점수 계산기 기능에서 집계 처리를 활성화/비활성화하는 데 사용됩니다. sn_sec_tisc.aggregates_for_calculator	• 유형: true | false • 기본값: True
사이팅 검색이 수행될 때 저장될 원시 데이터의 행 수입니다. 범위 0 - 100 sn_sec_tisc.sighting_search_raw_data_rows	• 유형: 정수 • 기본값: 50
사이팅 검색 결과를 CMDB의 CI와 연결합니다. sn_sec_tisc.associate_ci_with_sighting_search	• 유형: true | false • 기본값: True
목록에서 URL을 제거할지 여부를 제어합니다. sn_sec_tisc.sn_sec_tisc_case.defang_record_list_urls	• 유형: true | false • 기본값: false
이 속성을 사용하면 MITRE 기술을 연결된 개체 또는 보안 인시던트에서 케이스로 자동 롤업할 수 있습니다. sn_sec_tisc.auto_rollup_mitre_data	• 유형: true | false • 기본값: True

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	사용량
예인 경우 보고서에 렌더링된 MITRE 목록의 모든 전술(케이스와 연결된 기술이 없는 전술 포함)이 표시됩니다. sn_sec_tisc.show_all_tactics_reporting	• 유형: true | false • 기본값: True
공유 보고서에 사용할 케이스(sn_sec_tisc_case) 테이블에 대한 이메일 클라이언트 템플릿의 시스템 ID입니다. sn_sec_tisc.reporting_email_template_sn_sec_tisc_case	• 유형: 문자열 • 기본값: b55e22c54324021060eee0ea78b8f2df
새 기록을 만들 때 기본 TLP 수준이 적용됩니다. 양식에서 수동으로 설정하지 않으면 이 값이 사용됩니다. sn_sec_tisc.tlp_default_value	• 유형: 선택 목록 • 기본값: 955c9e5543d35110baf06e434ab8f2fb
로깅 수준 디버그,정보,경고,오류 sn_sec_tisc.logging.verbosity	• 유형: 선택 목록 • 기본값: 정보
위협 인텔리전스 피드에 대한 속성	
TAXII 수집 데이터를 가져오기 위해 대기 하는 아웃 바운드 HTTP 연결의 최대 시간 (초) sn_sec_tisc.taxii.http.max_timeout	• 유형: 정수 • 기본값: 300
TAXII 서버에서 하나의 REST 호출로 검색된 최대 객체 수 (TAXII 버전 2.0 및 2.1에만 적용) sn_sec_tisc.taxii.max_page_size	• 유형: 정수 • 기본값: 5000
실패한 TAXII2에 대한 최대 재시도 횟수입니다. X REST 호출 sn_sec_tisc.taxii2.retry_count	• 유형: 정수 • 기본값: 3
Cyware TAXII 서버에서 하나의 REST 호출로 검색되는 최대 객체 수 sn_sec_tisc.cyware_taxii.max_page_size	• 유형: 정수 • 기본값: 1000 주: Cyware TAXII 피드와 관련된 TAXII 컬렉션에서 데이터를 가져올 때 사용되는 페이지 크기를 지정합니다. 다른 모든 TAXII 컬렉션의 경우 컬렉션에서 TAXII 검색된 페이지 크기는 기본적으로 해당 속성 sn_sec_tisc.taxii.max_page_size에 정의된 값으로 설정됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	사용량
CrowdStrike에서 한 번에 가져올 기록의 수입니다. 숫자가 높을수록 페이로드를 처리하는 데 더 많은 메모리가 사용됩니다. sn_sec_tisc.crowdstrike_api_limit	• 유형: 정수 • 기본값: 1000
단일 API 호출에서 끌어올 표시기 수를 나타냅니다. 주: 이는 통합에서 시스템에 필요한 것을 찾지 못하는 경우에만 적용할 수 있습니다. sn_sec_tisc.crowdstrike_indicator_batch_size	• 유형: 정수 • 기본값: 1000
단일 API 호출에서 끌어올 액터 수를 나타냅니다. 주: 이는 통합에서 시스템에 필요한 것을 찾지 못하는 경우에만 적용할 수 있습니다. sn_sec_tisc.crowdstrike_actor_batch_size	• 유형: 정수 • 기본값: 1000
단일 API 호출에서 끌어올 보고서 수를 나타냅니다. 주: 이는 통합에서 시스템에 필요한 것을 찾지 못하는 경우에만 적용할 수 있습니다. sn_sec_tisc.crowdstrike_report_batch_size	• 유형: 정수 • 기본값: 50
CrowdStrike API에서 허용된 오프셋 및 한도의 총계입니다. sn_sec_tisc.crowdstrike_offset_limit_total	• 유형: 정수 • 기본값: 50000
REST API에 대한 속성	
옵저버블 가져오기 API에 대한 최대 페이지 크기(응답의 일부로 반환되는 옵저버블의 최대 수)를 정의합니다. API 응답시간에 영향을 줄 수 있으므로 높은 값으로 늘리지 않는 것이 좋습니다. sn_sec_tisc.api_maximum_page_size_limit	• 유형: 정수 • 기본값: 1000
옵저버블 추가 API에 대한 요청 본문에서 보낼 수 있는 최대 옵저버블 수를 정의합니다. API 응답시간에 영향을 줄 수 있으므로 높은 값으로 늘리지 않는 것이 좋습니다. sn_sec_tisc.add_obs_api_max_records	• 유형: 정수 • 기본값: 100
웹후크에 대한 속성	
하나의 웹후크 요청의 일부로 전송할 최대 이벤트 수입니다. 이 속성에 더 높은 값이 설정되어 있더라도 배치 크기는 2,000으로 제한됩니다. sn_sec_tisc.webhook_max_event_batch_size	• 유형: 정수 • 기본값: 100

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	사용량
실패한 요청을 오류로 표시하고 다음 이벤트 배치로 이동하기 전에 다시 시도할 횟수입니다. 이 속성에 더 높은 숫자가 설정되어 있더라도 재시도 횟수는 10으로 제한됩니다. sn_sec_tisc.webhook_retry_count	• 유형: 정수 • 기본값: 100
실패한 배치를 재시도하기 전에 대기할 시간(초)입니다. 이는 재시도 횟수에 따라 기하급수적으로 증가합니다. 예를 들어 retry_count 3이고 retry_interval 30이면 30, 60, 120초 후에 재시도가 실행됩니다. 이 속성에 더 높은 값이 설정되어 있더라도 초기 재시도 간격은 300초로 제한됩니다. sn_sec_tisc.webhook_retry_interval	• 유형: 정수 • 기본값: 30
위협 점수를 다시 적용하여 트리거된 웹후크 이벤트를 무시합니다. sn_sec_tisc.webhook_ignore_threat_score_reapply	• 유형: true | false • 기본값: True
조사 캔버스에 대한 속성	
값을 예로 설정하면 왼쪽 상단에 새 노드가 추가됩니다. 아니요인 경우 캔버스 중앙에 새 노드가 추가됩니다. sn_sec_tisc.canvas_suspend_reLayout	• 유형: true | false • 기본값: True
CTI 형식으로 익스포트하기 위한 속성	
STIX 2.1 파일로 익스포트할 수 있는 최대 행 수 sn_sec_tisc.stix_export_limit	• 유형: 정수 • 기본값: 10000
익스포트 파일에 저널 유형 필드를 포함합니다. sn_sec_tisc.export_journal_fields	• 유형: true | false • 기본값: True

예약된 작업

다음 표에서는 예약된 작업에 대해 설명합니다.

작업	설명
표시기 소스 기록 집계	표시기 소스 기록을 집계합니다.
집계 객체 소스 기록	객체 소스 기록을 집계합니다.
옵저버블 소스 기록 집계	옵저버블 소스 기록을 집계합니다.
부실 임포트 정리	부실 임포트 작업 기록을 정리합니다.
캔버스의 사용되지 않는 새 노드 정리	사용하지 않는 새 캔버스 노드를 정리합니다.
보안 파일 다운로드 기록 정리	보안 파일 다운로드 기록을 정리합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업	설명
표시기 소스 기록 중복 제거	표시기 소스 기록의 중복을 제거합니다.
중복 제거 객체 소스 기록	객체 소스 기록을 중복 제거합니다.
옵저버블 소스 기록 중복 제거	옵저버블 소스 기록을 중복 제거합니다.
비활성화 만료된 표시기	만료된 표시기 기록을 비활성화합니다.
만료된 객체 비활성화	만료된 객체 기록을 비활성화합니다.
비활성화된 만료된 옵저버블	만료된 옵저버블 기록 비활성화
TI에서 TISC로 데이터 마이그레이션	마이그레이션 작업 실행 기록이 보류 중인 프로세스
표시기 소스 기록에 대한 집계된 기록 채우기	새로 생성된 표시기 소스 기록에 대한 상위 집계 기록을 식별합니다.
객체 소스 기록에 대한 집계된 기록 채우기	새로 생성된 객체 소스 기록에 대한 상위 집계 기록을 식별합니다.
옵저버블 소스 기록에 대한 집계 기록 채우기	새로 작성된 옵저버블 소스 기록에 대한 상위 집계 기록을 식별합니다.
TI에서 TISC 참조 채우기	TI 옵저버블 기록에서 TISC 집계 옵저버블의 참조를 채웁니다.
승인된 임포트 처리	승인된 임포트 작업을 처리합니다.
임포트된 MISP DSM 큐 기록 처리	처리된 준비된 MISP 피드 수집 큐 기록입니다.
임포트된 MISP 표시기 임포트 큐 기록 처리	임포트 인텔리전스에서 수집된 준비된 MISP 데이터 처리
임포트된 STIX 임포트 큐 기록 처리	임포트 인텔리전스에서 수집된 준비된 STIX 데이터 처리
임포트된 STIX 임포트 큐 기록 처리 - 수집	위협 피드에서 수집된 스테이징된 STIX 데이터를 처리합니다.
보류 중인 케이스 아티팩트 마이그레이션 처리	위협 인텔리전스 애플리케이션에서 위협 인텔리전스 보안 센터로 케이스 아티팩트를 마이그레이션합니다.
보류 중인 위협 소스 수집 큐 기록 처리	보류 중인 소스 수집 큐 기록을 처리합니다.
위협 점수 계산기의 대기 중인 엔터티 처리	보류 중인 위협 계산기 큐 항목 처리
프로세스 큐에 대기 중인 MISP DSM 큐 기록	위협 피드에서 수집된 큐에 대기 중인 MISP 데이터 처리
프로세스 큐에 대기 MISP 표시기 임포트 큐 기록	임포트 인텔리전스에서 수집된 큐에 대기 중인 MISP 데이터 처리
프로세스 큐에 대기 STIX 임포트 큐 기록 - 수집	위협 피드에서 수집된, 큐에 대기 중인 STIX 데이터를 처리합니다.
프로세스 큐에 있는 STIX 표시기 임포트 큐 기록	임포트 인텔리전스에서 수집된 큐에 대기 중인 STIX 데이터 처리
프로세스 웹후크 큐	보류 중인 웹후크 큐 기록을 처리합니다.
소스 기록 재집계	집계된 기록이 삭제되는 소스 기록을 다시 집계합니다.
필터링된 소스 기록 제거	필터링된 소스 기록 정리

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업	설명
CrowdStrike 통합 프로세스 검사기 재개/CrowdStrike 소스 기록 다시 처리	요율 제한 대기 중인 CrowdStrike 피드 통합 실행을 재개/관계 집계를 위한 소스 기록 요청
긍정 오류 옵저버블 수 동기화	소스당 옵저버블 긍정 오류 개수를 flase 긍정 수와 동기화
TISC 웹후크 배치 생성	처리를 위해 대기 중인 웹후크 대기열 항목에 대한 배치를 생성함
TISC Fire 웹후크	보류 중인 웹후크 배치 실행
관계 보관 열 업데이트 중	관계 소스 및 대상 기록 보관 상태 업데이트

위협 인텔리전스 보안 센터 사용

위협 인텔리전스 라이브러리 기록을 관리하고, 외부 위협 데이터를 임포트하고, 케이스 관리를 간소화하는 데 사용합니다 위협 인텔리전스 보안 센터 . 이를 통해 보안 팀은 관련 정보를 진행 중인 조사에 통합하여 인텔리전스 데이터를 중앙 집중화하고, 분석을 개선하고, 위협에 보다 효과적으로 대응할 수 있습니다.

SIR 작업 공간과 **TISC** 통합

SIR과 TISC의 통합은 보안 분석가를 위해 보안 인시던트 작업 공간 내의 옵저버블에 대한 컨텍스트를 자동으로 연결합니다. SIR의 새로운 옵저버블은 화면에 제공되는 UI 작업을 사용하여 CTI 팀에서 추가 분석을 위해 TISC로 보낼 수 있습니다.

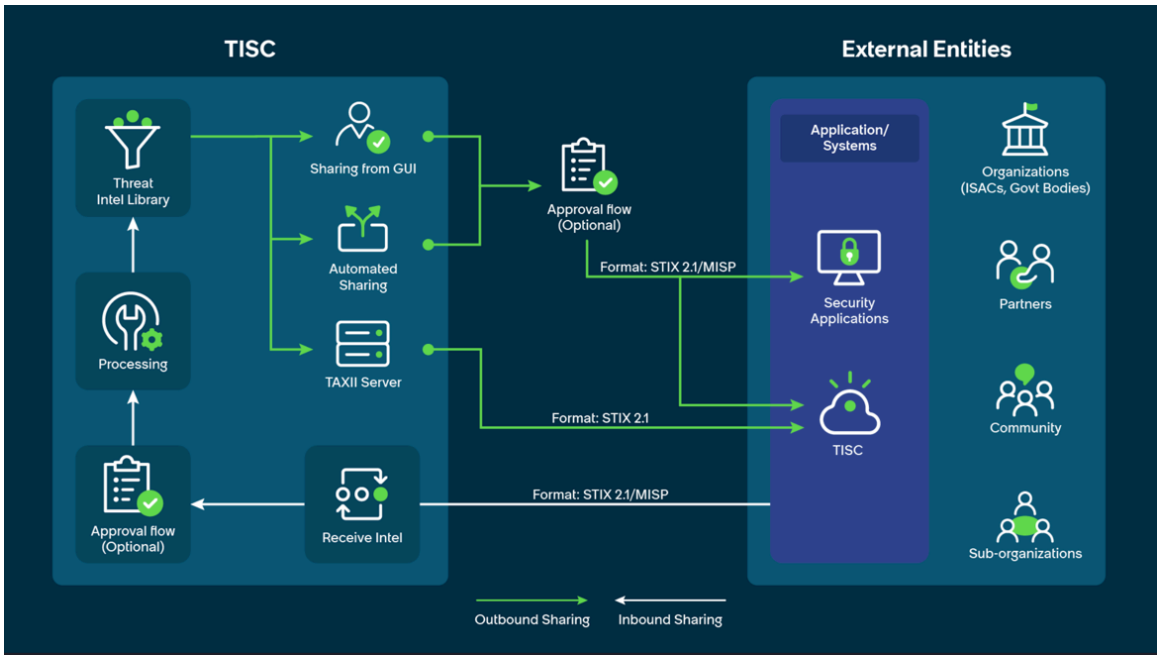
또한 SIR에서만 사용할 수 있는 통합에서 생성된 모든 보강 결과를 작업 공간에 제공된 UI 작업을 사용하여 푸시할 수도 있습니다.

Threat Intelligence 외부 공유 구성

의 TISC 위협 인텔리전스 외부 공유에서는 조직 내부 및 조직 전체에서 위협 인텔리전스의 자동화 및 GUI에서 공유하기 위한 지침과 기능을 간략하게 설명합니다. 이 기능은 제외 규칙 공유, 승인, 데이터 보존 및 감사와 같은 주요 영역에 중점을 두어 안전하고 규정을 준수하며 효율적인 인텔리전스 공유를 확인합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

위협 인텔리전스 보안 센터(TISC)와 위협 인텔리전스의 외부 공유



TISC를 통한 위협 인텔리전스의 외부 공유의 주요 기능

- 템플릿 공유: 템플릿을 사용하면 공유 인텔리전스에 포함되는 엔터티 및 필드를 제어할 수 있으므로 관련 데이터만 배포됩니다.
- 공유를 위한 승인 규칙: 관리자는 아웃바운드 및 인바운드 인텔리전스 모두에 대한 승인 규칙을 구성하여 승인 워크플로우를 강력하게 관리할 수 있습니다.
- 수정 기능: 분석가는 공유 인텔리전스에서 민감한 정보를 수정할 수 있으며, 수정을 켜거나 끌 수 있는 쉬운 옵션이 있습니다.
- 감사 기능: 모든 인텔리전스 공유 작업이 감사되어 발신자, 수신자, 타임스탬프 및 공유 콘텐츠를 포함한 세부 정보를 캡처하여 완전한 규정 준수 및 추적 가능성을 보장합니다.
- 데이터 보존 정책: 공유 인텔리전스 및 관련 감사 로그는 다양한 기록 유형의 보관 및 파기에 대해 정의된 규칙과 함께 규정 준수 요구 사항에 따라 유지됩니다.
- TISC에서 **TISC** 교환: (TISC) 인스턴스 간의 위협 인텔리전스 보안 센터 효율적인 양방향 정보 교환을 위한 메커니즘입니다.
- TAXII에 대한 사용자 및 그룹 관리: 컬렉션에 대한 액세스를 관리하고 보안 데이터 교환 프로토콜을 유지 관리하여 TAXII 사용자 및 그룹을 정의합니다.

아웃바운드 인텔 공유 탐색

아웃바운드 공유 인텔리전스를 사용하면 외부 및 내부에서 공유할 수 있는 위협 인텔리전스 엔터티 및 속성, 제외 규칙, 프로파일 및 그룹, 승인 규칙을 정의하고 공유할 수 있습니다.

아웃바운드 인텔 공유 통제 구성

이 섹션을 사용하여 외부 시스템에서 인텔리전스를 공유할 TISC 수 있는 엔터티를 결정하는 아웃바운드 공유 통제를 구성합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터 〉 관리 〉 아웃바운드 인텔 공유.
2. 아웃바운드 인텔 공유 통제를 선택합니다.
   아웃바운드 인텔 공유 통제는 기본 시스템에 프로비저닝된 기본 공유 통제입니다. 기본적으로 이 컨트롤은 게시됨 상태로 설정됩니다.

   주:
   - 이는 나중에 인텔리전스 공유 템플릿 내에서 사용할 수 있는 상위 수준 공유 통제입니다.
   - 아웃바운드 공유 통제에서 수행된 모든 작업이 기록되고 생성, 수정 또는 삭제된 각 엔터티에 대한 작업 메모가 활동 스트림에 게시됩니다.

공유 제어 편집:

3. 기본 공유 제어 기록을 변경하려면 편집을 선택하여 필수 필드를 수정합니다.

   공유 통제 기록을 편집할 때마다 계속하기 전에 모든 템플릿을 비활성화하고 보류 중인 아웃바운드 인텔리전스 공유 기록이 없는지 확인하라는 확인 메시지가 표시됩니다.

   위의 확인이 성공하면 먼저 비활성화하지 않고 계속 진행하면 이러한 설정을 기반으로 하는 자동화 플로우가 실패할 수 있음을 나타내는 다른 경고 메시지가 표시됩니다.

   경고:
   연결된 자동화 플로우를 먼저 비활성화하지 않고 이러한 설정을 편집하면 오류가 발생할 수 있습니다. 계속하시겠습니까?

   이 위험을 인지하고 계속 진행하려면 공유 제어를 수정할 수 있습니다.

엔터티 수준 공유 통제 관리:

4. 공유 통제 섹션으로 이동하여 엔터티에 사용할 수 있는 모든 공유 통제를 봅니다.
   기본적으로 옵저버블, 표시기, 객체 등 애플리케이션에 있는 모든 위협 인텔리전스 라이브러리 엔터티가 포함됩니다.
5. 필수 및 선택적 속성을 보려면 엔터티를 선택합니다.
   엔터티 및 속성 편집 대화 상자가 표시됩니다.

엔터티 추가 또는 제거:

6. 엔터티를 제거하려면 엔터티 제거 를 선택합니다.
   엔터티 제거는 엔터티를 제거하고 아웃바운드 인텔리전스 공유에서 자동으로 제외합니다. 제거된 엔터티는 내부 TISC 공유에 사용할 수 없으며 제거하면 이 엔터티가 공유 제어의 일부로 있는 모든 템플릿에서 엔터티가 자동으로 제거됩니다.

   또한 모든 특성 제거 (대화 상자 아래쪽에 있는 휴지통 아이콘)를 선택하여 모든 선택적 특성을 제거합니다. 이러한 속성을 제거하면 해당 인텔리전스 공유 템플릿에 직접적인 영향을 줍니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

- 선택한 엔터티를 포함하는 아웃바운드 공유 템플릿이 있는 경우 선택한 엔터티 또는 해당 속성을 제거하면 현재 포함된 {#total 수의 템플릿} 아웃바운드 인텔리전스 공유 템플릿에서 자동으로 제외됨을 나타내는 경고 메시지가 엔터티 및 속성 편집 대화 상자에 표시됩니다. 영향을 받는 템플릿은 엔터티 및 속성 편집 대화 상자 자체에 나열됩니다.
- 영향을 받는 템플릿 목록(예: 검토를 위해 IOC 공유 템플릿)이 표시됩니다.
- 외부 시스템과 공유하지 않으려는 특정 엔터티가 있는 경우 공유 제어에서 제거할 수 있습니다.
- 인텔리전스 아웃바운드 공유 템플릿을 생성하거나 수정할 때는 공유 통제 내에 구성된 엔터티만 선택할 수 있습니다.

7. 선택한 엔터티의 모든 선택적 속성을 아웃바운드 인텔리전스 공유에 포함하려면 모든 선택적 속성 추가를 선택합니다.
8. 공유 컨트롤을 필요에 따라 변경한 후 게시 를 선택하여 공유 컨트롤을 게시합니다.
   공유 통제가 게시되면 인텔리전스 아웃바운드 공유 템플릿 내에서 사용할 수 있습니다. 자세한 내용은 아웃바운드 인텔 공유 템플릿 구성 문서를 참조하십시오.

다음에 수행할 작업
GUI 및 자동 절차를 모두 사용하는 외부 인텔리전스 공유에 대한 지침은 다음 섹션을 참조하십시오.

- GUI에서 아웃바운드 인텔리전스 기록 공유
- 신뢰할 수 있는 파트너와 고위험 IOC의 공유 자동화아웃바운드 인텔 공유 템플릿 구성

아웃바운드 인텔 데이터 제외 규칙 구성

이 섹션을 사용하여 관리자가 정의된 기준과 일치하는 기록의 공유를 제한하도록 구성할 TISC 수 있는 제외 규칙을 생성합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.admin

이 태스크 정보
특정 엔터티를 공유하고 해당 엔터티 내의 특정 기록을 제외할 수 있습니다. 민감도에 따라 특정 기록을 제외하고 특정 유형의 엔터티를 공유할 수 있습니다. 예를 들어 도메인 이름은 공유하되 공유를 제한하는 TLP(Traffic Light Protocol) 등급의 도메인 이름은 제외할 수 있습니다. 이 방법은 중요한 도메인 이름이 조직 내에서 또는 외부 조직과 공유되는 것을 방지하는 데 도움이 됩니다.

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터 〉 관리 〉 아웃바운드 인텔 공유.
2. 아웃바운드 인텔 데이터 제외 규칙을 선택합니다.
   데이터 제외 규칙은 기본 시스템 내에서 프로비저닝된 아웃바운드 공유에 대한 기본 아웃바운드 인텔 데이터 제외 규칙입니다.

아웃바운드 인텔 데이터 제외 규칙 편집:

3. 제외 규칙 탭에서 각 테이블에 대해 정의된 제외 규칙을 수정하려면 편집 버튼을 선택합니다.
   이러한 설정을 먼저 비활성화하지 않고 진행할 경우 이러한 설정을 기반으로 하는 자동화 플로우가 실패할 수 있음을 나타내는 경고 메시지가 표시됩니다.

   이 위험을 인지하고 계속하려면 편집 버튼을 선택하여 제외 규칙을 수정할 수 있습니다.

아웃바운드 인텔 데이터 제외 규칙 수정:

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 제외 규칙 섹션으로 이동합니다.
   제외 규칙 목록에는 기본 시스템 내에서 프로비저닝된 모든 규칙이 표시됩니다. 이 목록은 엔터티, 엔터티 유형 및 특정 제외 조건을 포함하여 각 제외 규칙의 상세 정보를 제공합니다.

   조건이 일치하면 이러한 지정된 기준을 충족하는 기록은 공유되지 않습니다.

5. 조건을 수정하거나 추가하려는 제외 규칙을 선택하고 규칙을 저장합니다 .
6. 전역 데이터 제외 규칙을 필요에 따라 변경한 후 게시 버튼을 선택하여 업데이트된 제외 규칙을 적용합니다.

   제외 규칙에 대해 수행된 모든 작업이 기록되고 각 조건의 이전 및 현재 값을 보여 주는 작업 메모가 활동 스트림에 게시됩니다.

   주:

   - 아웃바운드 인텔리전스 데이터 제외 규칙이 편집 모드에 있는 동안에는 GUI에서 템플릿을 활성화하거나 공유할 수 없습니다.
   - 제외 규칙이 편집 모드로 유지되는 동안에는 TAXII 컬렉션에 대한 기록의 자동 공유 및 자동 추가도 실패합니다.

아웃바운드 인텔 공유 프로파일 구성

이 섹션을 사용하여 새 아웃바운드 인텔리전스 프로파일을 생성합니다. 아웃바운드 인텔리전스 프로파일은 위협 인텔리전스 데이터가 전송되는 엔드포인트 상세 정보를 지정합니다.

시작하기 전에

필요한 역할: sn_sec_tisc.admin

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터 〉 관리 〉 아웃바운드 인텔 공유.
2. 아웃바운드 인텔 공유 프로파일을 선택합니다.
3. 새로 만들기를 선택하여 아웃바운드 인텔리전스 프로파일을 작성합니다.
4. 양식에서 필드를 채웁니다.

새 아웃바운드 인텔리전스 프로파일 생성

필드	설명
이름	아웃바운드 인텔리전스 프로파일의 이름입니다.
산업	아웃바운드 인텔리전스 프로파일을 적용할 수 있는 항공 우주, 농업과 같은 산업 범주를 선택합니다.
설명	아웃바운드 인텔리전스 프로파일에 대한 설명입니다.
아웃바운드 인텔리전스 설정	
데이터 형식	아웃바운드 인텔리전스 공유 프로파일에 지원되는 데이터 형식입니다. 현재 아웃바운드 인텔리전스 공유에 대해 다음 두 가지 데이터 형식이 지원됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	○ **STIX 2.1**: 기본 인증 엔드포인트 및 오픈 소스 엔드포인트를 비롯한 다양한 엔드포인트 유형을 지원합니다. 이를 수용하기 위해 STIX 2.1에 대해 두 가지 인증 유형을 사용할 수 있습니다. ○ **MISP: MISP**의 경우 인증은 API 키를 통해서만 처리됩니다. ▪ MISP를 형식으로 선택하면 인증 필요 옵션이 자동으로 활성화됩니다. ▪ 인증 유형은 API 키로 고정되며 사용자는 MISP 인스턴스에 연결하려면 유효한 API 키를 제공해야 합니다.
API 엔드포인트 URL	데이터를 보내야 하는 API 엔드포인트 URL을 입력합니다.
인증 필요	인증이 필요한 경우 이 확인란을 선택합니다.
인증 유형	인증이 필요한 경우 드롭다운 목록에서 필요한 옵션을 선택합니다. 사용 가능한 옵션은 다음과 같습니다. 기본: 사용자 이름과 암호를 제공하려면 이 옵션을 선택합니다.
요청과 함께 전달할 헤더	요청과 함께 전달될 모든 헤더는 아웃바운드 인텔리전스 프로파일에 제공될 수 있습니다. 헤더는 콜론(":")으로 구분된 키-값 쌍으로 제공되어야 합니다. 각 헤더 키 값 쌍은 새 줄에 제공되어야 합니다. 인증 매개변수를 헤더 값으로 제공하려면 필수 인증을 "${" 및 "}$"로 묶습니다. (예: username:${Username}$)

5. 프로필 및 인증 세부 정보가 제공되면 저장을 클릭합니다.
6. 연결 확인을 선택하여 인텔리전스 아웃바운드 공유에 구성된 엔드포인트 URL을 테스트하여 설정을 확인합니다.

   이 옵션을 사용하면 프로필 섹션에 정의된 특정 엔드포인트의 유효성을 검사하는 요청 본문을 제공할 수 있습니다.

   > **주:**
   > 샘플 요청 본문은 선택한 형식에 따라 표시되며 필요에 따라 수정할 수 있습니다.

   요청 본문을 필요에 따라 변경하고 저장 및 유효성 검사 버튼을 클릭합니다. 원래 샘플 요청 본문으로 재설정하려는 경우 재설정 버튼을 선택하여 원래 요청 본문으로 다시 재설정할 수 있습니다.

   엔드포인트에 대한 연결이 성공했음을 나타내는 확인 메시지가 표시됩니다.

   엔드포인트에 대한 연결에 실패한 경우 오류 로그를 확인하고 문제를 해결한 후 다시 시도하십시오.
7. 아웃바운드 인텔리전스 공유 프로파일을 활성화하려면 사용 버튼을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
Enable(활성화) 버튼을 선택하면 엔드포인트 검사에 대한 유효성 검사가 자동으로 수행됩니다.

공유 프로파일을 만들 때마다 연결이 성공적으로 확인된 경우에만 사용 버튼이 나타나며, 그렇지 않으면 엔드포인트에 대한 연결이 성공할 때까지 이 버튼이 표시되지 않습니다.
공유 프로필이 성공적으로 활성화되었음을 나타내는 확인 메시지가 표시됩니다.

주:
공유 프로파일을 인텔리전스 공유에 사용하려면 해당 공유 프로파일을 활성화해야 합니다.

8. 또한 정보 공유에 필요하지 않은 경우 사용 안 함을 선택하여 프로파일을 비활성화합니다.

아웃바운드 인텔 공유 그룹 구성

아웃바운드 인텔 공유 그룹을 사용하면 여러 프로파일을 결합하여 데이터를 공유할 때 함께 사용할 수 있습니다.

시작하기 전에
필요한 역할: sn_sec_tisc.admin

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터 〉 관리 〉 아웃바운드 인텔 공유.
2. 아웃바운드 인텔 공유 그룹을 선택합니다.
3. 새로 만들기를 선택하여 아웃바운드 인텔리전스 공유 그룹을 만듭니다.
4. 양식에서 필드를 채웁니다.

필드	설명
이름	아웃바운드 인텔 공유 그룹의 이름입니다.
설명	아웃바운드 인텔 공유 그룹에 대한 설명입니다.
유형	그룹이 내부 조직에 속하는지 또는 외부 조직에 속하는지 여부를 지정합니다.

5. 저장을 클릭하여 인텔 공유 그룹을 저장합니다.

그룹 구성원 추가:

이 섹션을 사용하여 여러 프로파일을 그룹에 연결할 수 있습니다.

6. 그룹 구성원 섹션으로 이동합니다.
7. 추가를 클릭합니다.
아웃바운드 인텔리전스 프로파일 추가 대화 상자가 표시됩니다. 활성화된 모든 아웃바운드 인텔리전스 공유 프로파일이 나열됩니다.
8. 하나 이상의 프로파일을 선택합니다.
9. 추가를 클릭합니다.
10. 또한 제거 를 클릭하여 그룹에서 프로파일을 제거합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

그룹을 필요에 따라 변경한 후 인텔리전스 공유에서 그룹을 활성화하고 사용할 수 있도록 설정할 수 있습니다. 그렇지 않으면 더 이상 사용하지 않아야 하는 경우 비활성화할 수 있습니다.

주:
선택한 아웃바운드 인텔리전스 프로파일이 이 그룹에 추가 또는 제거되었음을 나타내는 정보 메시지가 표시됩니다. 이 메시지는 선택한 추가 또는 제거 작업과 관련하여 표시됩니다.

아웃바운드 인텔에 대한 승인 규칙 정의

특정 사용자가 공유 인텔리전스를 공유하기 전에 승인이 필요한지 여부를 제어하는 승인 규칙을 정의합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.admin

아웃바운드 인텔 기록에 대한 승인 규칙을 구성할 수 있습니다. 이러한 규칙은 사용자 역할 또는 기타 기준에 따라 공유에 승인이 필요한지 여부를 결정합니다.

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 작업 공간에서 관리 아이콘을 클릭합니다.
3. 아웃바운드 **Intel** 공유로 이동합니다.
4. 아웃바운드 인텔에 대한 승인 규칙을 선택합니다.

   주:
   기본 시스템 내에서 아웃바운드 인텔리전스에 대한 승인 규칙은 승인 워크플로우를 활성화하기 위해 기본 시스템 내에서 프로비저닝된 기본 규칙입니다.

   승인 규칙은 요청 시 아웃바운드 인텔리전스 공유에만 적용할 수 있습니다. 온디맨드 아웃바운드 인텔리전스에 대한 자세한 내용은 단원을 참조하십시오. 아웃바운드 인텔 공유 템플릿 구성입니다.
5. 승인 규칙 양식의 다음 각 섹션에 하나 이상의 사용자 또는 사용자 그룹을 입력합니다.
   a. 승인이 필요한 사용자 또는 그룹 선택
   b. 승인자 선택
6. 사용 버튼을 클릭하여 인바운드 인텔리전스에 대한 승인 플로우를 활성화합니다.

   주:
   - 활성화되면 적용 가능한 모든 아웃바운드 인텔 기록이 승인 큐로 라우팅됩니다.
   - 할당된 승인자는 분석가가 변경한 내용을 검토하고 요청을 승인하거나 거부합니다.
   - 결정이 내려지면 사용자 또는 사용자 그룹에 기록이 승인 또는 거부되었는지 여부를 나타내는 이메일 알림이 전송됩니다.

아웃바운드 인텔 공유 템플릿 구성

아웃바운드 인텔 공유 템플릿을 사용하면 ()TISC에서 외부로 공유되는 데이터를 정의하고 제어할 수 있습니다 위협 인텔리전스 보안 센터 .

시작하기 전에
필요한 역할: sn_sec_tisc.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보

공유 템플릿의 주요 목적은 공유 기록 이름, 설명, 아웃바운드 인텔리전스 프로파일 또는 그룹과 같은 공유 기록 세부 정보를 미리 채우는 것입니다. 자세한 내용은 GUI에서 아웃바운드 인텔리전스 기록 공유 문서를 참조하십시오.

이러한 템플릿은 포함되는 엔터티 및 속성과 공유를 위한 시스템 설정을 지정합니다.

이러한 템플릿을 구성하면 조직은 내부 및 외부 협업 노력 전반에 걸쳐 보안 및 규정 준수를 유지하여 관련성 있고 승인된 인텔리전스 데이터만 공유되도록 할 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 작업 공간에서 관리 아이콘을 선택합니다.
3. 아웃바운드 **Intel** 공유로 이동합니다.
4. 아웃바운드 인텔 공유 템플릿을 선택합니다.
5. 새로 만들기를 선택합니다.
6. 양식에서 필드를 채웁니다.

새 아웃바운드 인텔 공유 템플릿 작성

필드	설명
템플릿 이름	아웃바운드 인텔리전스 공유 템플릿의 이름입니다.
템플릿 설명	아웃바운드 인텔리전스 공유 템플릿에 대한 설명입니다.
사용 모드	공유 템플릿이 사용되는 방식을 나타냅니다. 아웃바운드 인텔리전스 공유 모듈의 템플릿은 다목적이며 요구 사항에 따라 여러 공유 시나리오에 적용할 수 있습니다. 사용 가능한 공유 옵션은 다음과 같습니다. **a.** 요청 시 공유: GUI에서 데이터를 공유하는 데 사용됩니다. **b.** 자동화된 공유: 자동화 플로우를 통해 예약 또는 트리거 기반 공유를 활성화합니다. **c.** 요청 시 공유와 자동화된 공유 모두: 템플릿을 요청 시 또는 자동화된 공유에서 사용할 수 있으므로 유연성이 극대화됩니다. **d. TAXII** 컬렉션에 자동 추가: 신뢰할 수 있는 외부 파트너에게 배포하기 위해 TAXII 컬렉션에 공유 데이터를 자동으로 추가합니다.
수정 활성화(자동 모드에만 해당)	정보 공유 중에 기밀성을 보호하기 위해 공유 데이터에서 중요한 정보를 대체하는 프로세스인 수정을 사용하려면 이 확인란을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	주: 이 옵션은 자동 공유뿐만 아니라 요청 시 공유 및 자동화된 공유 옵션 둘 다에 적용할 수 있으며, **TAXII** 컬렉션에 자동으로 추가 되고 요청 시 공유에는 적용되지 않습니다.
요청 시 공유에 대한 접근 제어	
중요사항: 이러한 템플릿은 특정 개체 또는 옵저버블에 대한 인텔리전스를 공유할 때와 같이 관리되는 공유 모델 내에서 사용되므로 템플릿에 액세스할 수 있는 사용자 또는 그룹을 제어할 수 있습니다. 이를 관리하기 위해 특정 템플릿에 대한 가시성이 있어야 하는 사용자 및 그룹을 지정할 수 있는 아웃바운드 인텔리전스 공유 권한이 있는 모든 사용자 또는 그룹에 대한 액세스 허용이라는 전용 섹션이 있습니다. 개별 사용자 또는 그룹을 지정하여 액세스를 제한하고 선택한 사용자 또는 그룹만 템플릿을 사용할 수 있도록 할 수 있습니다.	
아웃바운드 인텔 공유 권한이 있는 모든 사용자 또는 그룹에 대한 액세스 허용	아웃바운드 인텔 공유 권한이 있는 모든 사용자 또는 그룹에 액세스 권한을 부여하려면 이 확인란을 선택합니다.
사용자("sn_sec_tisc.int_exch_write" 역할이 있어야 함)	인텔리전스를 공유하기 위한 템플릿에 액세스할 사용자를 선택합니다. 아웃바운드 인텔리전스 공유를 수행하려면 sn_sec_tisc.int_exch_write 역할이 있어야 합니다.
그룹("sn_sec_tisc.int_exch_write" 역할이 있어야 함)	인텔리전스를 공유하기 위한 템플릿에 액세스하기 위한 그룹을 선택합니다. 아웃바운드 인텔리전스 공유를 수행하려면 ### sn_sec_tisc.int_exch_write 역할이 있어야 합니다.
미리 입력된 입력	
이름(공유 기록 이름)	공유 기록의 이름입니다. 이 값은 아웃바운드 인텔리전스 공유 기록 내에 미리 채워집니다.
설명(공유 기록 설명)	공유 기록에 대한 설명입니다. 이 값은 아웃바운드 인텔리전스 공유 기록 내에 미리 채워집니다.
아웃바운드 인텔 공유 프로파일	아웃바운드 인텔 공유 프로파일을 나타냅니다. 이 값은 아웃바운드 인텔리전스 공유 기록 내에 미리 채워집니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	자세한 내용은 아웃바운드 인텔 공유 프로파일 구성 문서를 참조하십시오.
아웃바운드 인텔 공유 그룹	아웃바운드 인텔 공유 그룹을 나타냅니다. 이 값은 아웃바운드 인텔리전스 공유 기록 내에 미리 채워집니다. 자세한 내용은 아웃바운드 인텔 공유 그룹 구성 문서를 참조하십시오.
TAXII 컬렉션	TAXII 컬렉션을 나타냅니다. 이 옵션은 사용 모드를 **TAXII** 컬렉션에 자동 추가로 선택한 경우에만 표시됩니다.
기본 신뢰도(0 - 100)	공유 기록 내의 인텔리전스 기록에서 신뢰도 값을 지정하지 않는 경우에만 적용되는 기본 신뢰도 값을 나타냅니다. 이 값은 아웃바운드 인텔리전스 공유 기록 내에 미리 채워집니다.
TLP 재정의	공유 통제 내의 모든 기록에 특정 TLP를 적용하여 TLP(Traffic Light Protocol)를 재정의하려면 이 확인란을 선택합니다. 이 TLP는 페이로드 생성 중에 사용되며 개별 기록 수준에서 할당된 TLP를 재정의합니다. 이 값은 아웃바운드 인텔리전스 공유 기록 내에 미리 채워집니다.
TLP	공유 템플릿의 TLP(Traffic Light Protocol)를 나타냅니다. 이 옵션은 **TLP** 재정의 확인란을 선택한 경우에만 표시됩니다.
공유를 위한 시스템 설정	
아웃바운드 인텔리전스 공유 통제	아웃바운드 인텔리전스 공유 통제를 나타냅니다. 기본적으로 이 필드의 값은 아웃바운드 인텔 공유 통제 입니다. 기본 시스템 내에서 제공되는 유일한 공유 통제이기 때문입니다.
아웃바운드 인텔리전스 제외 규칙	아웃바운드 인텔리전스 제외 규칙을 나타냅니다. 기본적으로 이 필드의 값은 기본 시스템 내에서 프로비저닝되는 유일한 제외 규칙이므로 아웃바운드 데이터 제외 규칙 입니다.

7. 저장을 선택하여 공유 템플릿을 저장합니다.
   모든 아웃바운드 인텔리전스 공유 통제가 이 템플릿에 자동으로 복사되고 몇 초 내에 템플릿 공유 통제 섹션에 표시됨을 나타내는 확인 메시지가 표시됩니다.

템플릿 공유 통제:

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

8. 템플릿 공유 통제 섹션으로 이동합니다.
   템플릿 공유 통제는 선택한 템플릿에 대해 정의된 모든 공유 통제를 표시하며, 이러한 공유 통제는 아웃바운드 인텔리전스 공유 통제로 알려진 주요 수준의 공유 통제에 따라 달라집니다. 자세한 내용은 아웃바운드 인텔 공유 통제 구성 문서를 참조하십시오.
9. 템플릿 공유 통제 섹션에서 추가를 선택합니다.
   엔티티 및 속성 추가(Add Entities and Attributes) 대화 상자가 표시됩니다.

   기본 공유 제어에 정의된 엔터티만 표시됩니다. 기본적으로 모든 엔터티는 기본 시스템에 포함되고 프로비저닝되므로 처음에는 모든 공유 통제가 표시됩니다. 그러나 메인 공유 통제에서 엔터티를 제거하면 템플릿의 공유 통제 내에서 해당 엔터티를 더 이상 선택할 수 없습니다.

   중요사항:
   이러한 템플릿은 STIX 내에서도 사용되므로 STIX에 대한 유효성 검사 규칙이 도입되었습니다. 이러한 규칙을 위반하면 페이로드 생성에 실패할 수 있습니다. 정의된 STIX 준수 규칙이 충족되지 않으면 페이로드가 구성된 엔드포인트로 전송되지 않을 수 있으며 공유 프로세스가 완전히 중지될 수 있습니다.

   STIX 검증 경고를 나타내는 오류 메시지가 표시됩니다. 이 엔터티에 필요한 속성 중 하나 이상을 포함해야 합니다.

10. 공유 템플릿에 선택적 속성을 포함하려면 모든 선택적 속성 추가를 선택합니다.
11. 또한모든 속성 제거 (대화 상자 아래쪽에 있는 휴지통 아이콘)를 클릭하여 모든 선택적 속성을 제거하거나 엔터티 및 속성 편집 대화 상자에서 엔터티 제거 버튼을 선택하여 템플릿에서 엔터티를 완전히 제거합니다.
12. 공유 컨트롤을 필요에 따라 변경한 후 게시 를 클릭하여 템플릿 공유 컨트롤을 게시합니다.
    템플릿 공유 통제가 게시되면 인텔리전스 아웃바운드 공유 템플릿 내에서 사용할 수 있게 됩니다.

    중요사항:
    이러한 템플릿은 GUI 설정에서 데이터를 공유하는 동안에도 적용할 수 있으며 위협 인텔리전스 라이브러리에서 액세스할 수 있습니다. 자세한 내용은 GUI에서 아웃바운드 인텔리전스 기록 공유 문서를 참조하십시오.

13. 옵션: 편집 버튼을 선택하여 템플릿을 필요에 따라 변경합니다.

    주:
    템플릿을 변경하는 경우 공유 템플릿에 종속된 보류 중인 아웃바운드 인텔리전스 공유 기록이 있음을 나타내는 경고 메시지가 표시됩니다. 이 템플릿을 편집하기 전에 보류 중인 아웃바운드 인텔리전스 공유 기록이 없는지 확인합니다.

    (Optional) 공유 템플릿을 편집하는 동안 종속 자동화 플로우를 먼저 비활성화하지 않고 이 템플릿을 편집하면 오류가 발생할 수 있으며 계속하시겠습니까를 나타내는 확인 메시지가 표시됩니다. 계속하려면 편집 버튼을 선택하여 변경합니다.

14. 또한 템플릿의 복제본을 생성하려면 **Duplicate** 버튼을 선택한 다음 현재 템플릿을 복제합니다.
    이 작업은 연결된 모든 공유 통제를 포함하여 전체 구성을 복제합니다.

공유 템플릿을 활성화하기 위한 확인:

애플리케이션은 아웃바운드 인텔리전스 공유 템플릿을 활성화하기 전에 다양한 유효성 검사를 검사하며, 필요한 모든 구성이 완료되면 활성화됩니다.

a. 공유 통제 누락: 템플릿에 공유 통제가 추가되지 않은 경우 사용자가 게시를 시도하면 애플리케이션에서 템플릿을 저장 및 게시할 수 있지만 활성화되지는 않습니다.

   템플릿이 활발하게 사용되지 않도록 도와주는 확인 메시지가 나타납니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

b. 기본 수준에서 초안 공유 통제: 기본 아웃바운드 인텔 공유 통제가 여전히 편집(초안) 모드인 경우 템플릿을 활성화할 수 없습니다. 이 경우 공유 컨트롤이 초안 상태이며 계속하기 전에 게시해야 한다는 경고 메시지가 표시됩니다.

이러한 확인은 모든 관련 구성요소가 게시 되고 활성화된 상태인 경우에만 공유를 위해 템플릿이 활성화되도록 하기 위해 적용됩니다. 이렇게 하면 불완전하거나 잘못된 구성이 운영 공유 프로세스에서 사용되는 것을 방지할 수 있습니다.

주:

- 게시를 선택하고 언급된 기준 중 하나라도 충족되지 않으면 템플릿이 계속 게시되지만 사용하도록 설정되지는 않습니다.
- 사용을 선택하고 언급된 기준 중 하나라도 충족되지 않으면 템플릿이 활성화되지 않습니다.
- 사용 및 사용 안 함 버튼은 게시된 템플릿에 대해서만 표시됩니다.

15. 옵션: 공유 템플릿을 비활성화하려면 아웃바운드 인텔 공유 템플릿 페이지에서 직접 비활성화를 선택합니다.

주:
아웃바운드 인텔 공유 템플릿 페이지 목록 보기에서 하나 이상의 템플릿을 선택하여 복제, 사용 또는 사용 안 함과 같은 다양한 작업을 수행할 수도 있습니다.

관련 정보

GUI에서 아웃바운드 인텔리전스 기록 공유

아웃바운드 인텔리전스 기록 공유 자동화

TAXII 컬렉션의 자동화된 공유

교정 라이브러리 작업

수정은 정보 공유 중에 기밀성을 보호하기 위해 공유 데이터에서 민감한 정보를 대체하는 프로세스입니다.

시작하기 전에
필요한 역할: sn_sec_tisc.admin

이 태스크 정보
이 기능을 사용하면 민감하거나 개인화된 정보를 특정 값으로 수정하거나 바꿀 수 있습니다.

아웃바운드 인텔리전스 공유 기록 내에서 수정 라이브러리를 적용하여 페이로드가 작성되기 전에 특정 속성이나 컨텐츠를 자동으로 필터링할 수 있습니다.

위협 인텔리전스 공유에서 수정 범주 값으로 정의되고 해당 수정 범주로 대체되는 중요한 정보입니다.

이는 관련 정보와 중요하지 않은 정보만 공개해야 하는 외부 조직과 데이터를 공유할 때 특히 유용합니다.

교정 라이브러리 기능을 활용하여 TISC 관리자와 분석가는 재사용 가능한 교정 구성을 정의하고 여러 공유 템플릿에 일관되게 적용할 수 있습니다.

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.

2. 작업 공간에서 관리 아이콘을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 아웃바운드 **Intel** 공유로 이동합니다.
4. 교정 라이브러리를 선택합니다.
   교정 라이브러리 목록 보기가 표시됩니다.
5. 새로 만들기를 선택합니다.
6. 양식의 필드에 내용을 입력합니다.

필드	설명
수정 범주	아웃바운드 인텔리전스 공유 기록에 대한 수정 범주를 지정합니다.
상태	수정 범주의 상태입니다. 기본적으로 모든 수정 범주가 활성화되어 있습니다. 그러나 특정 수정 범주를 비활성화하도록 선택할 수 있습니다.

7. 저장을 클릭합니다.
8. 수정 범주 값 섹션으로 이동합니다.
9. 새로 만들기를 선택하여 수정 범주 값 기록을 작성합니다.

수정 라이브러리의 시스템 속성:

이름	설명
sn_sec_tisc.case_sensitive_for_redaction	이 속성은 공유 인텔리전스에 수정을 적용할 때 대소문자 구분을 활성화하거나 비활성화합니다. 기본값: 비활성화됨(false), 이는 수정이 기본적으로 대/소문자를 구분하지 않음을 의미합니다. 주: 기본적으로 이 속성은 비활성화되어 있어 수정을 대/소문자를 구분하지 않습니다. 예를 들어 Service_Now과 service_now 모두 동일하게 수정됩니다. 이 기능을 활성화하면(#) 케이스가 정확히 일치하는 경우에만 수정이 적용됩니다.

10. 저장을 선택합니다.

수정 범주 및 값의 대량 임포트

수정 범주를 임포트합니다. 수정 범주 및 관련 값을 대량 임포트합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.admin

이 태스크 정보
CSV 또는 XLSX 형식의 샘플 파일을 다운로드하고 수정 범주와 해당 값으로 채운 다음 다시 애플리케이션으로 임포트할 수 있습니다. 이 대량 임포트 기능을 사용하면 여러 수정 규칙을 효율적으로 추가할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 작업 공간에서 관리 아이콘을 선택합니다.
3. 아웃바운드 **Intel** 공유로 이동합니다.
4. 교정 라이브러리를 선택합니다.
5. 임포트를 클릭합니다.
6. 샘플 파일을 다운로드합니다.
   임포트 파일에는 다음 두 개의 열이 포함됩니다.
   - 수정 범주
   - 값

   임포트 오류가 발생할 수 있으므로 샘플 파일의 헤더를 수정하지 마십시오.
7. 파일을 업로드하고 완료를 클릭합니다.
   수정 행을 성공적으로 가져왔다는 확인 메시지가 표시됩니다. 링크를 클릭하여 임포트 요약을 볼 수도 있습니다.

   주:
   파일 크기는 5MB를 초과할 수 없으며 행 수는 1000개를 초과할 수 없습니다.

   확인 규칙:

   a. 모든 수정 범주와 해당 범주 값이 고유한지 확인합니다.
   b. 하나의 수정 범주 값을 둘 이상의 수정 범주에 연결할 수 없습니다. 예를 들어, 범주 값이 이미 하나의 수정 범주와 연결되어 있는 경우 다른 범주에 할당할 수 없습니다.

   수정 범주 및 값의 대량 임포트를 위한 시스템 속성:

이름	설명
sn_sec_tisc.max_redaction_rows_import	이 속성은 데이터를 수정 라이브러리로 대량으로 임포트할 때 허용되는 최대 행 수를 설정합니다. 기본 최대값은 1000입니다.

인바운드 인텔 공유 탐색

에서 TISC 인바운드 인텔리전스 공유를 사용하면 인텔리전스를 제출할 수 있는 외부 시스템 또는 장치의 프로필을 생성할 수 있습니다.

인바운드 인텔 공유 프로파일 구성

이 섹션에서는 외부 조직 TISC으로부터 정보를 수신하는 데 사용되는 인바운드 인텔리전스 공유 프로파일에 대해 설명합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.admin

주:

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터 〉 관리 〉 인바운드 인텔 공유.
2. 인바운드 인텔 공유 프로파일을 선택합니다.
3. 새로 만들기를 선택하여 인바운드 인텔리전스 프로파일을 작성합니다.
4. 양식에서 필드를 채웁니다.

새 인바운드 인텔리전스 프로파일 생성

필드	설명
이름	인바운드 인텔리전스 프로파일의 이름입니다.
산업	인바운드 인텔리전스 프로파일을 적용할 수 있는 항공 우주, 농업과 같은 산업 범주를 선택합니다.
설명	인바운드 인텔리전스 프로파일에 대한 설명입니다.
인바운드 인텔리전스 설정	
데이터 형식	인바운드 인텔리전스 공유 프로파일에 지원되는 데이터 형식입니다. 현재 인바운드 인텔리전스 공유에는 두 가지 데이터 형식이 지원됩니다. ○ STIX 2.1 ○ MISP 데이터 형식 설명에 대한 자세한 내용은 문서를 참조하십시오 아웃바운드 인텔 공유 프로파일 구성.
인증을 위한 사용자(sn_sec_tisc.api_post_intel 역할이 있어야 함)	외부 시스템이 이 프로파일에 대한 인텔리전스를 공유할 TISC 때 인증에 자격 증명을 사용해야 하는 사용자를 선택합니다. 주: sn_sec_tisc.api_post_intel 역할을 가진 사용자는 드롭다운 목록에서만 사용할 수 있습니다.
기본 신뢰도	소스가 신뢰도 값을 제공하지 않는 경우 이 프로파일에서 받은 모든 인텔리전스 기록에 적용되는 기본 신뢰도를 나타냅니다.
만료 기간(일)	공유 프로파일에서 받은 인텔리전스 기록이 만료되는 일 수를 지정합니다. 일단 만료되면 정보 기록은 더 이상 공개, 공유 또는 유효한 것으로 간주되지 않을 수 있다.
기본 TLP	소스에서 TLP 값을 제공하지 않을 때 이 프로파일에서 받은 모든 인텔리전스 기록에 적용되는 기본 TLP를 지정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
알림 사용	인바운드 인텔리전스 기록의 승인 또는 거부 시 보낸 사람에게 알림을 보내려면 이 검사를 선택합니다.
다음 경우에 알림	이 옵션을 사용하여 구성된 이메일 받는 사람에게 알릴 시기(예: 기록의 승인이나 거부 또는 둘 다)를 선택합니다. **주:** 이 옵션은 알림 사용이 선택된 경우에만 나타납니다.
이메일 받는 사람	알림 대상 필드에 구성된 기준에 따라 알림을 받을 사용자의 이메일 주소를 입력합니다. **주:** 이 필드는 알림 사용이 선택된 경우에만 표시됩니다. 여러 이메일 주소를 쉼표로 구분하여 입력할 수 있습니다.
TISC 태그	외부 시스템에서 받은 모든 인바운드 인텔리전스에 추가할 태그를 지정합니다.

5. 저장을 선택합니다.

프로파일 **ID** 복사:

외부 조직에서 정보를 공유하려면 이 프로파일 ID가 필요합니다.

6. 공유할 프로필 ID를 복사하려면 프로필 **ID** 복사 버튼을 선택합니다.
7. 또한 이메일 프로필 **ID** 를 선택하여 공유 프로필 세부 정보를 이메일로 보냅니다.
   이 옵션을 선택하면 이메일 작성기 대화 상자가 표시됩니다. 프로파일을 공유할 이메일 세부 정보를 입력합니다.
8. 보내기를 선택하여 외부 사용자에게 세부 정보를 보냅니다.

관련 정보

인바운드 인텔 공유 그룹 구성

인바운드 인텔에 대한 승인 규칙 정의

인바운드 인텔 공유 그룹 구성

인바운드 인텔 공유 그룹을 사용하면 관리자가 유사한 인바운드 인텔리전스 공유 프로파일을 함께 그룹화할 수 있습니다. 이러한 그룹을 사용하여 그룹 내의 모든 프로필에 적용되는 승인 규칙을 정의할 수 있습니다.

시작하기 전에
필요한 역할: sn_sec_tisc.admin

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터 〉 관리 〉 인바운드 인텔 공유.
2. 인바운드 인텔 공유 그룹을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 새로 만들기를 선택하여 인바운드 인텔리전스 그룹을 생성합니다.
4. 양식에서 필드를 채웁니다.

필드	설명
이름	인바운드 인텔 공유 그룹의 이름입니다.
설명	인바운드 인텔 공유 그룹에 대한 설명입니다.
유형	그룹이 내부 조직에 속하는지 또는 외부 조직에 속하는지 여부를 지정합니다.

5. 저장을 선택하여 인텔리전스 공유 그룹을 저장합니다.
   또한 요구 사항에 따라 그룹을 사용하거나 사용하지 않도록 설정할 수 있습니다.

그룹 구성원 추가:

이 섹션을 사용하여 여러 프로파일을 그룹에 연결할 수 있습니다.

6. 그룹 구성원 섹션으로 이동합니다.
7. 추가를 선택합니다.
   인바운드 인텔리전스 프로파일 추가 대화 상자가 표시됩니다. 활성화된 모든 인바운드 인텔리전스 공유 프로파일이 나열됩니다.
8. 하나 이상의 프로파일을 선택합니다.
9. 옵션: 선택한 인바운드 인텔리전스 프로파일을 그룹에 추가하는 이유를 제공합니다.
10. 추가를 선택합니다.
    선택한 프로파일이 그룹에 추가됩니다.
11. 또한 제거 를 선택하여 그룹에서 프로파일을 제거합니다.

> **주:**
> 제거 사유를 추가해야 합니다.

관련 정보

인바운드 인텔 공유 프로파일 구성

인바운드 인텔에 대한 승인 규칙 정의

인바운드 인텔에 대한 승인 규칙 정의

승인 규칙을 정의하여 인바운드 인텔리전스를 처리하기 전에 특정 프로파일 또는 그룹에 승인이 필요한지 여부를 제어합니다.

시작하기 전에

필요한 역할: sn_sec_tisc.admin

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 작업 공간에서 관리 아이콘을 선택합니다.
3. 인바운드 인텔 공유로 이동합니다.
4. 인바운드 인텔리전스에 대한 승인 규칙을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
기본 시스템 내에서 인바운드 인텔리전스에 대한 승인 규칙은 승인 워크플로우를 활성화하기 위해 프로비저닝된 기본 규칙입니다.

5. 승인 규칙 양식의 다음 각 섹션에 하나 이상의 사용자 또는 사용자 그룹을 입력합니다.
   a. 승인할 프로파일 또는 그룹 선택: 이 섹션에서 인바운드 인텔리전스 데이터를 처리하기 위한 승인이 필요한 인바운드 인텔 공유 프로파일 또는 인바운드 인텔리전스 공유 그룹을 선택합니다.
   b. 승인자 선택: 이 섹션에서는 이전에 구성한 프로파일/그룹에서 받은 인바운드 인텔리전스 기록을 승인하는 데 필요한 사용자 또는 그룹을 선택합니다.
6. 인바운드 인텔에 대한 승인 규칙을 활성화하려면 활성화 버튼을 선택합니다.

주:
- 활성화되면 적용 가능한 모든 인바운드 인텔 기록이 승인 큐로 라우팅됩니다.
- 한 명 이상의 배정된 승인자가 분석가가 변경한 내용을 검토하고 요청을 승인하거나 거부합니다.
- 결정이 내려지면 해당 인바운드 인텔리전스 공유 프로필에 구성된 이메일 주소로 기록이 승인 또는 거부되었는지 나타내는 이메일 알림이 전송됩니다.

TAXII 아웃바운드 서버 탐색

TAXII 컬렉션은 위협 인텔리전스 데이터의 논리적 그룹입니다.

TAXII 컬렉션 작성

이 섹션에서는 인텔리전스 공유를 위해 TAXII 컬렉션을 구성하고 정의하는 방법을 알아봅니다.

시작하기 전에
필요한 역할: sn_sec_tisc.admin

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터 〉 관리 〉 **TAXII** 아웃바운드 서버.
2. **TAXII** 컬렉션을 선택합니다.
3. 새로 만들기를 선택하여 TAXII 컬렉션을 생성합니다.
4. 양식에서 필드를 채웁니다.

새 인바운드 인텔리전스 프로파일 생성

필드	설명
이름	TAXII 컬렉션의 이름입니다.
설명	TAXII 컬렉션에 대한 설명입니다.
사양 버전	데이터 형식 지정 및 교환에 사용되는 TAXII의 버전을 지정합니다. 주: 데이터 형식에 대해 지원되는 유일한 사양 버전은 2.1입니다.
만료 기간(일)	TAXII 컬렉션에 추가된 기록이 만료될 때까지 남은 일 수를 지정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	주: 만료 후 기록은 비활성으로 표시되고 컬렉션에서 제거됩니다.
버전 관리 사용	TAXII 컬렉션에 추가되는 기록에 대한 버전 관리를 사용하려면 이 확인란을 선택합니다. 주: 기록이 컬렉션에 TAXII 추가되고 이전 버전과 다른 경우 애플리케이션은 버전 관리가 활성화된 경우에만 새 버전을 추가합니다. 버전 관리를 사용하지 않으면 기존 기록을 업데이트된 데이터로 덮어씁니다.
모든 TAXII API 사용자에 대한 접근 권한	TAXII 사용자에 대한 액세스를 지정합니다. 선택하면 TAXII 서버 API 역할이 할당된 모든 사용자에게 이 컬렉션에서 데이터를 검색할 수 있는 권한이 부여됩니다. 주: 모든 **TAXII API** 사용자에 대한 액세스 필드를 선택하지 않으면 이 필드에 지정된 사용자만 TAXII 컬렉션 기록에 액세스할 수 있습니다.
읽기 권한	모든 **TAXII API** 사용자에 대한 액세스 필드를 선택하지 않으면 이 필드에 지정된 사용자만 TAXII 컬렉션 기록에 액세스할 수 있습니다.

5. 저장을 선택합니다.

기록을 추가하는 시스템 속성

TAXII 컬렉션에 대한 시스템 속성은 TAXII 컬렉션에 추가할 수 있는 기록 수를 제한합니다.

다음은 TAXII 컬렉션 구성에 대한 시스템 속성입니다.

이름	설명
sn_sec_tisc.taxii_server_collection_record_limit	아웃바운드 TAXII 서버 컬렉션에 추가할 수 있는 최대 기록 수입니다. 기본값은 10000입니다.

6. TAXII 컬렉션에 기록을 추가하기 위한 시스템 속성 정보를 봅니다.

7. 다음으로 이동합니다. 플로우 디자이너 〉 플로우.
이 탐색에는 TAXII 컬렉션을 추가하기 위한 템플릿 플로우가 표시됩니다.

8. TAXII 컬렉션에 위협 인텔리전스 자동 추가 플로우를 선택합니다.

9. 다음으로 이동합니다. 플로우 디자이너 〉 작업.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

TAXII 컬렉션에 기록 추가

현재 TAXII 서버 컬렉션에 레코드를 추가하는 유일한 방법은 자동화된 프로세스를 사용하는 것입니다. 다음은 기본 시스템에서 프로비저닝되는 두 가지 작업입니다.

a. TAXII 서버 컬렉션에 기록 추가

b. TAXII 서버 컬렉션에 기록 추가

10. 각 TAXII 서버 수집 작업을 봅니다.

관련 정보

TAXII 컬렉션의 자동화된 공유

아웃바운드 인텔 공유 템플릿 구성

TAXII 컬렉션의 자동화된 공유

자동화된 TAXII 컬렉션은 신뢰할 수 있는 외부 파트너에게 원활하게 배포할 수 있도록 인텔리전스 레코드를 TAXII 서버 컬렉션에 자동으로 추가합니다.

시작하기 전에
필요한 역할:

- 시스템 관리자(보기, 만들기 또는 편집)
- sn_sec_tisc.admin(보기)

이 태스크 정보
자동화된 플로우 작업은 입력에 제공된 기록을 선택한 템플릿에 구성된 TAXII 서버 컬렉션에 추가합니다. 자세한 내용은 아웃바운드 인텔 공유 템플릿 구성 문서를 참조하십시오.

자동화된 프로세스를 통해 TAXII 서버 컬렉션에 기록 추가:

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 보안 센터 〉 관리.

2. 선택 자동화된 플로우.

3. 플로우 디자이너에서 해당 규칙 상세 정보를 보려면 **TAXII** 수집 작업 링크에 위협 인텔리전스 자동 추가를 선택합니다.

4. 다음 트리거에 대한 플로우 디자이너 작업을 봅니다.

Observable Created or Updated where (Type is IP address (V4), or Type is IP address (V6), or Type is Domain Name; and TISC Tags contains Add to: Sample Collection, and Reputation is Malicious, and Threat Score greater than or is 60) Actions Select multiple

5. 동작으로 이동

6. 완료를 선택합니다.

다음에 수행할 작업
플로우를 활성화합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관련 정보

TAXII 컬렉션 작성

아웃바운드 인텔 공유 통제 구성

아웃바운드 인텔 공유 템플릿 구성

TAXII 컬렉션 기록 보기

TAXII 컬렉션에 추가된 기록을 봅니다.

시작하기 전에
필요한 역할:

- sn_sec_tisc.admin
- sn_sec_tisc.분석가

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터 〉 관리 〉 **TAXII** 아웃바운드 서버.
2. **TAXII** 컬렉션을 선택합니다.
3. 새 TAXII 컬렉션을 저장한 후 **TAXII** 컬렉션 기록 섹션으로 이동합니다.
   TAXII 컬렉션에 추가된 모든 기록이 이 섹션 아래에 표시됩니다.
4. 제거 버튼을 선택하여 TAXII 컬렉션에서 기록을 제거합니다.
   sn_sec_tisc.analyst 역할을 가진 사용자는 TAXII 컬렉션에서만 기록을 제거할 수 있습니다.
5. 제거할 기록을 선택하고 제거를 선택합니다.

View Threat Intelligence 외부 공유

위협 인텔리전스 공유는 다양한 위협 데이터 공유 소스에 대한 중앙 집중식 뷰를 제공합니다. 이 기능을 사용하면 인텔리전스 공유를 위해 처리 중인 위협 레코드를 모니터링하고 다양한 유형의 인텔리전스 데이터에 대한 승인 워크플로우를 관리할 수 있습니다.

이 섹션에서는 다음 사항에 대해 설명합니다.

1. 아웃바운드 인텔리전스
2. 인바운드 인텔리전스
3. TAXII 컬렉션

아웃바운드 인텔리전스

아웃바운드 인텔리전스는 조직이 외부 엔터티와 공유하는 위협 인텔리전스 데이터를 말합니다.

TISC 분석가는 템플릿, 프로파일, 그룹, 공유 엔터티 속성, 제외 규칙과 같은 관련 상세 정보를 검토하고 조직의 인텔리전스 시스템에 입력하기 전에 승인하거나 거부할 수 있습니다. 자세한 내용은 아웃바운드 인텔 공유 탐색 문서를 참조하십시오.

인바운드 인텔리전스

인바운드 인텔리전스는 외부 소스에서 받은 위협 데이터와 관련이 있습니다. 이 섹션에서는 외부 시스템에서 받은 인바운드 인텔리전스 데이터를 관리할 수 있습니다.

인바운드 인텔리전스는 위협 인텔리전스 옵저버블, 표시기 및 인바운드 인텔리전스 기록으로 알려진 기타 위협 객체를 포함하는 컬렉션 그룹입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

TISC 분석가는 조직의 인텔리전스 시스템에 수집되기 전에 검토하고 승인하거나 거부할 수 있습니다. 자세한 내용은 인바운드 인텔 공유 탐색 문서를 참조하십시오.

TAXII 컬렉션

TAXII(Trusted Automated Exchange of Intelligence Information)는 위협 인텔리전스 공유에 사용되는 프로토콜입니다. 자세한 내용은 TAXII 아웃바운드 서버 탐색 문서를 참조하십시오.

아웃바운드 인텔리전스 보기

이 섹션을 사용하여 모든 아웃바운드 인텔리전스 공유 기록을 봅니다. 인텔리전스 데이터를 검토하고 승인 또는 거부하는 데 필요한 조치를 취합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터 〉 **Threat Intelligence** 공유.
   위협 인텔리전스 공유 페이지는 적절한 조치가 필요한 다음과 같은 인텔리전스 공유 섹션과 함께 표시됩니다.
   - 아웃바운드 인텔리전스
   - 인바운드 인텔리전스
   - TAXII 아웃바운드 서버
2. 선택 아웃바운드 인텔리전스 〉 모두
   아웃바운드 인텔리전스 페이지에는 인텔리전스 공유 프로세스에 있는 기록이 표시됩니다. 다음과 같은 하위 섹션이 표시됩니다.
   - 모두: 모든 아웃바운드 인텔리전스 공유 기록을 표시합니다.
   - 내가 생성함: 사용자가 생성한 아웃바운드 인텔리전스 공유 기록을 표시합니다.
   - 승인 보류 중: 승인 보류 중인 아웃바운드 인텔리전스 기록을 표시합니다.
   - 내 승인: 승인을 기다리고 있는 아웃바운드 인텔리전스 기록을 표시합니다.
3. 기록을 열어 공유 기록의 상태를 봅니다.
   승인 또는 거부를 기다리고 있는 공유 인텔리전스 기록을 확인합니다.
4. 검토 섹션을 선택하여 아웃바운드 인텔리전스 데이터를 검토합니다.
5. 아웃바운드 인텔리전스 데이터와 연결된 게시된 작업을 확인합니다.
6. 승인을 선택하여 공유 기록을 승인합니다.
   아웃바운드 인텔리전스 승인이 표시됩니다.
7. 필요한 경우 주석을 추가합니다.
8. 승인 버튼을 선택하여 공유 인텔리전스 기록을 승인합니다.
   아웃바운드 인텔리전스 기록이 승인되었음을 나타내는 확인 메시지가 표시됩니다.
9. 또한 아웃바운드 공유 인텔리전스를 거부해야 하는 경우 거부 버튼을 선택합니다.

인바운드 인텔리전스 보기

이 섹션을 사용하여 모든 인바운드 인텔리전스 공유 기록을 봅니다. 인텔리전스 데이터를 검토하고 승인 또는 거부하는 데 필요한 조치를 취합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터 〉 **Threat Intelligence** 공유.
2. 선택 인바운드 인텔리전스 〉 모두
   인바운드 인텔리전스 페이지에는 인텔리전스 공유 프로세스에 있는 외부 당사자로부터 시스템이 받은 인바운드 인텔리전스 기록이 표시됩니다. 다음과 같은 하위 섹션이 표시됩니다.
   - 모두: 여러 프로파일에서 시스템에 수신된 모든 인바운드 인텔리전스 공유 기록을 표시합니다.
   - 승인 보류 중: 승인 보류 중인 인바운드 인텔리전스 기록을 표시합니다.
   - 내 승인: 승인을 기다리고 있는 인바운드 인텔리전스 기록을 표시합니다.

   주:
   내 승인 섹션 목록 뷰에서 직접 승인 또는 거부할 수 있습니다. 분할 버튼 뷰에서 원하는 옵션을 선택하고 이유를 제공하여 승인하거나 거부합니다.

   적절한 섹션을 선택하고 각 인바운드 인텔리전스 기록에 필요한 작업을 수행하는 것이 좋습니다.
3. 상세 정보를 보려면 인바운드 인텔리전스 기록을 선택합니다.
   인텔리전스 레코드의 일부로 수신된 모든 레코드는 인바운드 인텔리전스 레코드 섹션에서 사용할 수 있습니다.
4. 승인을 선택하여 공유 기록을 승인합니다.
   인바운드 인텔리전스 승인이 표시됩니다.
5. 필요한 경우 주석을 추가합니다.
6. 검토를 대기 중인 기록을 엽니다.

   a. 승인 버튼을 선택하여 인바운드 인텔리전스 기록을 승인합니다.
   인바운드 인텔리전스 기록이 승인되었음을 나타내는 확인 메시지가 표시됩니다.

   주:

   알림은 각 프로파일 내에서 구성된 규칙에 따라 트리거됩니다. 공유 기록을 승인하거나 거부하면 프로파일에 대한 이메일 알림이 활성화된 경우 이메일이 전송됩니다. 이메일을 구성하지 않으면 알림이 전송되지 않습니다.
7. 또한 인바운드 인텔리전스 기록을 거부하려면 거부 버튼을 선택합니다.

   주:

   공유 기록의 승인 및 거부를 위한 이메일 샘플:
   - 승인 시 이메일 알림: 인바운드 인텔리전스 데이터에 대한 요청이 승인되었습니다.
   - 거부 시 이메일 알림: 인바운드 인텔리전스 데이터에 대한 요청: {기록 번호 공유}이(가) 거부되었습니다. 지정된 링크를 사용하여 거부된 공유 기록을 볼 수 있습니다.

TAXII 컬렉션 보기

이 섹션을 사용하여 TAXII 아웃바운드 서버의 일부로 구성된 TAXII 컬렉션을 볼 수 있습니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터 〉 **Threat Intelligence** 공유.
2. 선택 **TAXII** 아웃바운드 서버 〉 **TAXII** 컬렉션.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 원하는 TAXII 컬렉션 기록을 선택하여 TAXII 컬렉션에 추가된 기록을 봅니다.
4. **TAXII** 컬렉션 기록 섹션으로 이동합니다.
   TAXII 컬렉션에 추가된 모든 기록이 TAXII 컬렉션 기록 섹션 아래에 표시됩니다.
5. 제거 버튼을 선택하여 TAXII 컬렉션에서 기록을 제거합니다.
   sn_sec_tisc.analyst 역할을 가진 사용자는 TAXII 컬렉션에서만 기록을 제거할 수 있습니다.
6. 제거할 기록을 선택하고 제거를 선택합니다.
   TAXII 수집 기록 제거를 시작하면 인텔리전스 공유에서 하나 이상의 기록을 제거할 수 있는지 확인하는 확인 메시지가 표시됩니다. 확인 시 기록이 제거되고 제거된 기록의 세부 정보를 제공하는 작업 메모 활동이 활동 스트림에 자동으로 게시됩니다.

수정 임포트 보기

수정 임포트를 사용하면 현재 임포트 작업에서 처리 중인 모든 기록과 승인 보류 중인 임포트 작업을 볼 수 있습니다.

모든 수정 임포트 보기

이 섹션을 사용하여 교정으로 임포트한 모든 기록을 봅니다.

시작하기 전에
필요한 역할: sn_sec_tisc.admin

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터 〉 임포트.
2. 선택 수정 임포트 〉 모든 임포트
   이 페이지에는 임포트 작업에 대해 처리 중인 모든 기록이 표시됩니다.
3. 임포트 프로세스의 상태를 보려면 기록을 엽니다.

> 주:
> 새 임포트를 클릭하여 새 임포트 기록을 만들 수도 있습니다. 이 버튼을 클릭하면 애플리케이션이 인텔리전스 임포트 페이지로 안내합니다. 새 기록 생성에 대한 자세한 내용은 섹션을 참조 에서 인텔리전스 임포트 TISC 하고 각 임포트 유형을 계속 진행합니다.

내 수정 임포트 보기

이 섹션을 사용하여 현재 로그인한 사용자가 만든 임포트 기록을 봅니다.

시작하기 전에
필요한 역할: sn_sec_tisc.admin

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터 〉 임포트.
2. 선택 수정 임포트 〉 내 임포트
   이 페이지에는 임포트 작업의 추가 프로세스를 위해 분류된 모든 기록 및 해당 임포트 기록이 표시됩니다.
3. 임포트 프로세스의 상태를 보려면 기록을 엽니다.
4. 로그인한 사용자가 임포트한 임포트 기록의 요약을 봅니다.

GUI에서 아웃바운드 인텔리전스 기록 공유

이 섹션에서는 사용자가 애플리케이션 내의 TI(Threat Intelligence) 라이브러리에서 직접 인텔리전스 레코드를 공유할 수 있는 기능을 간략하게 설명합니다 TISC .

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할:

- sn_sec_tisc.분석가
- sn_sec_tisc.admin

이 태스크 정보
공유 템플릿에 대한 액세스는 각 템플릿 내에 정의된 여러 제한 사항의 영향을 받습니다. 이러한 제한은 템플릿을 모든 사용자가 사용할 수 있는지 또는 특정 사용자 또는 사용자 그룹으로 제한되는지를 지정합니다. 따라서 사용자가 인텔리전스 공유 프로세스를 시작할 때 이러한 설정에서 허용하는 템플릿만 표시됩니다.

분석가 역할을 가진 사용자만 GUI에서 외부 시스템으로 인텔리전스 데이터를 공유할 수 있습니다. 인텔리전스 공유 기능은 옵저버블, 표시기 및 객체(예: 공격 패턴, 위협 액터 등)를 포함한 다양한 기타 위협 인텔리전스 라이브러리 엔터티에도 적용됩니다.

다음은 옵저버블 기록의 양식 뷰에서 인텔리전스를 공유하는 절차입니다.

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터 〉 위협 인텔 라이브러리 〉 옵저버블 〉 모든 옵저버블.
2. 옵저버블 기록을 엽니다.
3. 인텔리전스 공유 버튼을 클릭합니다.
   아웃바운드 인텔리전스 템플릿 선택 대화 상자가 표시됩니다.
4. 조회에서 필요한 아웃바운드 인텔리전스 템플릿을 선택합니다.

   주:
   기본 템플릿 포함(테이블 및 속성) 보기 하이퍼링크를 사용하면 포함된 모든 속성을 볼 수 있습니다.

5. 선택한 인텔리전스의 관련 기록을 자동으로 연결하고 관련 기록을 공유 기록에 자동으로 연결하고 세부 정보를 저장하려면 확인란을 선택합니다.
6. 제출을 선택합니다.
   인텔리전스 공유를 위해 기록을 제출한 후에는 액세스 가능한 템플릿만 표시됩니다.
   a. 데이터 제외 규칙 구성: 기록은 데이터 제외 규칙에 정의된 기준과 일치하는 경우 제외됩니다. 자세한 내용은 아웃바운드 인텔 데이터 제외 규칙 구성 문서를 참조하십시오.
   b. 선택한 공유 템플릿 통제: 선택한 공유 템플릿에 정의된 통제에 따라 기록이 필터링됩니다. 자세한 내용은 아웃바운드 인텔 공유 템플릿 구성 문서를 참조하십시오.

   이러한 구성 기준에 따라 관련 기록은 공유에서 제외됩니다.
7. 선택을 클릭하여 아웃바운드 인텔리전스 공유 기록을 작성합니다.
   필요한 경우 필요한 사항을 변경합니다.
8. 저장을 클릭하여 아웃바운드 인텔리전스 데이터 양식에 수정된 값을 저장합니다.
9. 제출을 선택하여 제출할 공유 기록을 제출합니다.
   공유 기록의 상세 정보 섹션에서 응용 프로그램은 아웃바운드 인텔 공유 템플릿 페이지의 미리 채워진 입력 에서 구성된 값을 자동으로 채웁니다. 자세한 내용은 아웃바운드 인텔 공유 템플릿 구성 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
다음은 아웃바운드 인텔리전스 기록에 대한 시스템 속성입니다.

이름	설명
shared_intelligence_entity_threshold	기록 임계치 제한: 이 속성은 단일 아웃바운드 인텔리전스 기록에 포함할 수 있는 개별 기록의 최대 수를 제어합니다. ○ 기본 제한은 1,000개입니다. ○ 최대 한도는 10,000개 기록입니다.
shared_intelligence_exclusion_work_notes_count	제외된 기록 제한: 이 속성은 활동 스트림에서 작업 메모당 표시되는 행 수를 제어합니다. ○ 기본값: 작업 메모당 10행. ○ 최대: 작업 메모당 100개 행. 행 수가 지정된 한도를 초과하면 가독성과 사용자 경험을 보장하기 위해 기록이 여러 작업 메모로 분할됩니다.

10. 인텔리전스 기록 섹션으로 이동합니다.
이 섹션에는 선택한 공유 기록의 일부인 모든 인텔리전스 기록이 표시됩니다.

인텔리전스 기록 보기 섹션:

주:
인텔리전스 공유 기록 섹션은 공유 기록이 초안 상태인 경우에만 표시되며 공유 기록이 처리됨, 승인 대기 중 등의 다른 상태인 경우에는 표시되지 않습니다.

기록의 일부로 그룹화되고 공유되는 옵저버블, 객체 및 관련 엔터티의 전체 목록을 볼 수 있습니다.

인텔리전스 공유 기록 섹션에 액세스하면 해당 기록과 연결된 모든 인텔리전스 엔터티의 구조화된 보기가 페이지의 왼쪽 패널에 표시됩니다.

- 템플릿 구성: 이 뷰에 표시되는 엔터티 테이블은 공유 기록과 연결된 공유 템플릿에 정의된 공유 제어를 기반으로 합니다.
- 엔터티 그룹화: 첫 번째 상위 수준 그룹은 옵저버블입니다. 또한 파일, IP 주소 및 기타 관련 유형과 같은 하위 수준 옵저버블도 볼 수 있습니다. 표시기와 객체는 옵저버블 뒤에도 나열됩니다.
- 관계: 공유 엔터티 간의 관계를 표시합니다. 6가지 유형의 관계가 표현되며, 각 유형은 명확성과 구조를 위해 해당 관계 테이블로 구성됩니다.

주:
하나 이상의 기록이 있는 목록 표시 는 데이터가 포함된 엔터티 테이블만 빠르게 필터링하고 표시할 수 있는 토글입니다.

11. 열 편집을 클릭하여 목록 뷰 열을 수정합니다.
열 선택 대화 상자가 표시되어 목록 뷰에 표시할 열을 구성할 수 있습니다.

12. 또한 기록의 상세 정보를 수정하려면 기록 수정을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

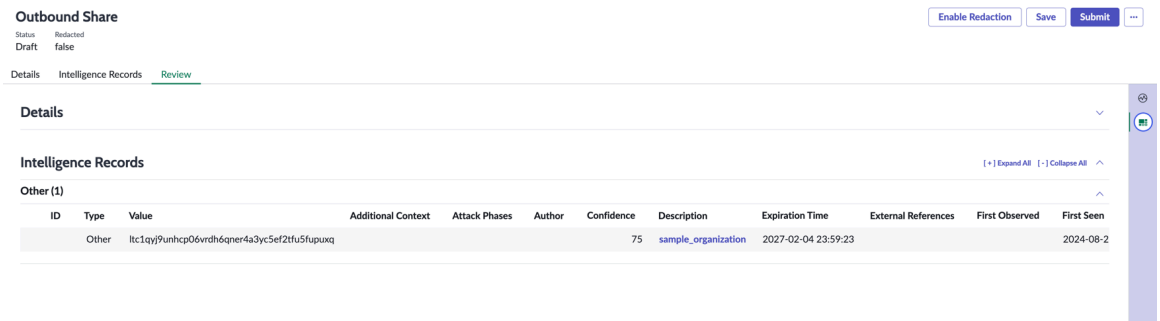
이 작업을 선택하면 하나 이상의 기록을 수정할 수 있습니다. 하나 이상의 기록을 수정하거나 대량 편집을 수행하는 경우 기록의 선택적 필드만 수정할 수 있다고 가정합니다. 대량 편집 옵션을 선택하면 필드의 모든 값이 지워지고 값을 제공하고 저장 하면 해당 값을 선택한 모든 기록에 적용할 수 있습니다.

주:
정보 기록 섹션에 있는 개체 기록에 대한 수정 사항은 해당 라이브러리 기록에 적용되지 않습니다. 예를 들어 공격 패턴에 대한 설명을 수정하는 경우 이 변경 내용은 위협 인텔리전스 라이브러리의 해당 공격 패턴에 영향을 미칠 수 있습니다.

13. 추가를 클릭하여 공유 기록에 기록을 추가하면 선택한 기록이 성공적으로 추가되었다는 확인이 표시됩니다.

주:
기록 공유에 대해 제외 규칙이 구성된 경우 제외 규칙 기준을 충족하는 선택한 기록은 자동으로 건너뜁니다. 이러한 기록은 정보 기록에 추가되지 않습니다. 사용자에게 알리기 위한 적절한 오류 메시지가 표시되고, 제외된 기록에 대한 자세한 정보가 활동 스트림에 기록됩니다.

14. 제거를 클릭하여 공유 기록에서 기록을 제거합니다.
15. 수정 사용 버튼을 선택하여 공유 기록에 대한 수정을 활성화합니다.



주:
수정 라이브러리를 사용하려면 수정 라이브러리를 구성해야 합니다. 자세한 내용은 교정 라이브러리 작업 문서를 참조하십시오.

수정 활성화 옵션을 사용하면 인텔리전스 기록을 공유하기 전에 중요한 콘텐츠를 수정하여 중요한 정보를 자동으로 제거하거나 마스킹할 수 있습니다. 수정을 사용하면 기밀 데이터가 보호되고 인텔리전스 공유 중에 노출되지 않습니다.

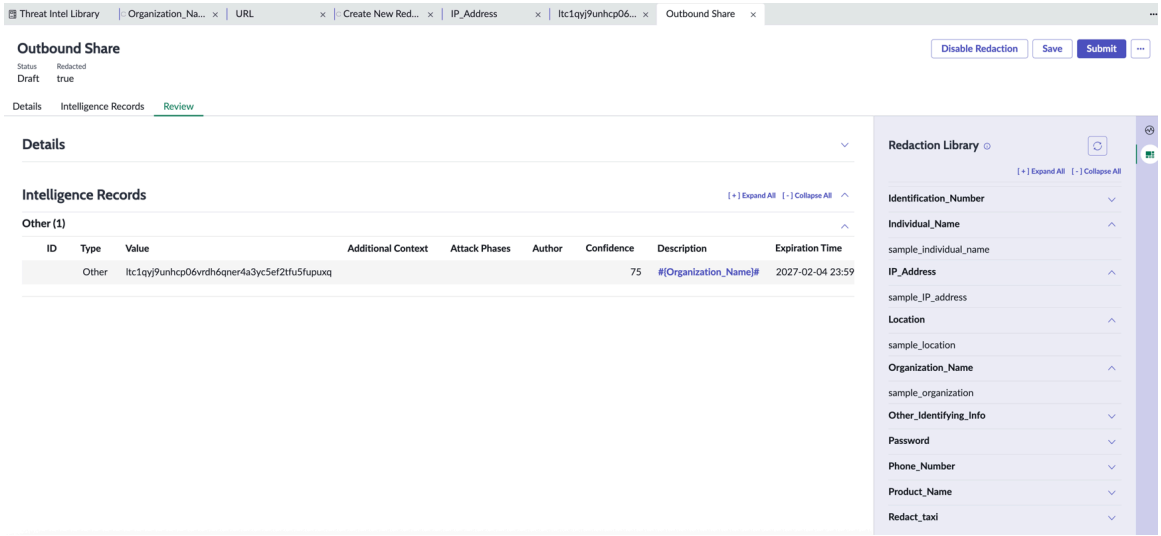
이 옵션을 활성화하면 오른쪽 상황별 메뉴에 수정 라이브러리 아이콘이 나타나 관리 섹션의 수정 라이브러리에 정의된 사용 가능한 모든 수정 범주 및 수정 범주 값 목록에 액세스할 수 있습니다.

본보기:**Service_Now**와 같은 조직 이름을 수정하는 경우 **Service_Now Organization_Name** 범주 아래에 수정 범주 값으로 추가되면 모든 **Service_Now** 항목이 다음 형식을 사용하여 대체됩니다.

#{Organization_Name}#.

수정 옵션을 활성화하면 시스템에서 공유하기 전에 조직 이름을 자동으로 수정합니다. 다음 스크린샷은 수정된 범주 값을 보여줍니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



16. 검토 섹션으로 이동하여 선택한 공유 기록의 인텔리전스 기록을 검토합니다.
17. 옵션: 필요한 경우 공유 기록에 대한 수정을 비활성화하려면 수정 사용 안 함을 선택합니다.

인텔리전스 기록 검토

18. 검토 섹션으로 이동하여 공유 기록의 기록을 검토합니다.
검토 섹션에서는 인텔리전스 공유에 포함된 모든 엔터티를 요약하는 스냅샷 보기를 제공합니다. 기록에는 다음에 대한 간략한 요약이 표시됩니다.
    - 상세 정보: 공유 기록의 상세 정보를 읽기 전용 모드로 표시합니다.
    - 공유 엔터티 속성: 공유 기록과 연결된 공유 템플릿에 정의된 공유 제어를 표시합니다.
    - 제외 규칙: 구성된 제외 규칙을 표시합니다.
    - 수정 라이브러리: 관리 섹션에 구성된 수정 라이브러리를 표시합니다. 자세한 내용은 교정 라이브러리 작업 문서를 참조하십시오.
19. 검토 섹션에서 필요한 사항을 변경하고 제출을 위해 제출을 클릭합니다.
처리를 위해 기록을 제출할 것인지 묻는 확인 메시지가 표시됩니다. 계속 진행하려면 제출을 선택합니다.

    제출하면 아웃바운드 인텔리전스 공유 기록의 상태가초안 에서 승인 대기 중으로 변경됩니다. 아웃바운드 인텔리전스에 대한 승인 규칙이 구성된 경우에만 상태가 승인 대기 중으로 변경됩니다. 자세한 내용은 아웃바운드 인텔에 대한 승인 규칙 정의 문서를 참조하십시오.

20. 승인 버튼을 선택하여 아웃바운드 인텔리전스 기록을 승인합니다.
21. 필요한 경우 주석을 추가하고 아웃바운드 인텔리전스 승인 대화 상자에서 승인을 선택합니다.
22. 또한 거부 버튼을 선택하여 아웃바운드 인텔리전스 기록을 거부합니다.
23. 이유를 입력하고 아웃바운드 인텔리전스 거부 대화 상자에서 거부를 선택합니다.

    거부하면 아웃바운드 인텔리전스 공유 기록의 상태가거부됨으로 변경됩니다.

    주:
    편집 버튼을 선택하고 거부 설명에 따라 필요한 사항을 변경합니다. 기록을 편집하고 다시 제출하도록 선택하면 상태가초안 으로 다시 이동합니다.

    승인 규칙이 정의되지 않았거나 기록이 이미 승인된 경우 아웃바운드 인텔리전스 공유 기록은 처리 대기 중 상태로 이동됩니다. 이 단계에서 인텔리전스 데이터는 외부와 공유된 후 상태가

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

처리됨으로 업데이트됩니다. 자세한 내용은 아웃바운드 인텔에 대한 승인 규칙 정의 문서를 참조하십시오.

24. 게시된 작업으로 이동하여 공유 기록에 대한 게시된 작업을 봅니다.
각 아웃바운드 인텔리전스 프로파일에는 게시된 작업이 있으며 이러한 게시된 작업을 통해 상태를 추적할 수 있습니다.

    자세한 내용은 게시된 작업을 클릭하면 페이로드, 상태 등과 같은 작업 세부 정보가 표시됩니다.

    해당 엔드포인트로 데이터를 보내는 동안 수신자 쪽에서 문제가 발생하면 애플리케이션은 기본적으로 최대 5회까지 자동으로 다시 시도합니다. 재시도 횟수를 변경하려면 다음 시스템 속성을 사용하여 값을 수정할 수 있습니다.

    sn_sec_tisc.shared_intelligence_retry_count

관련 정보

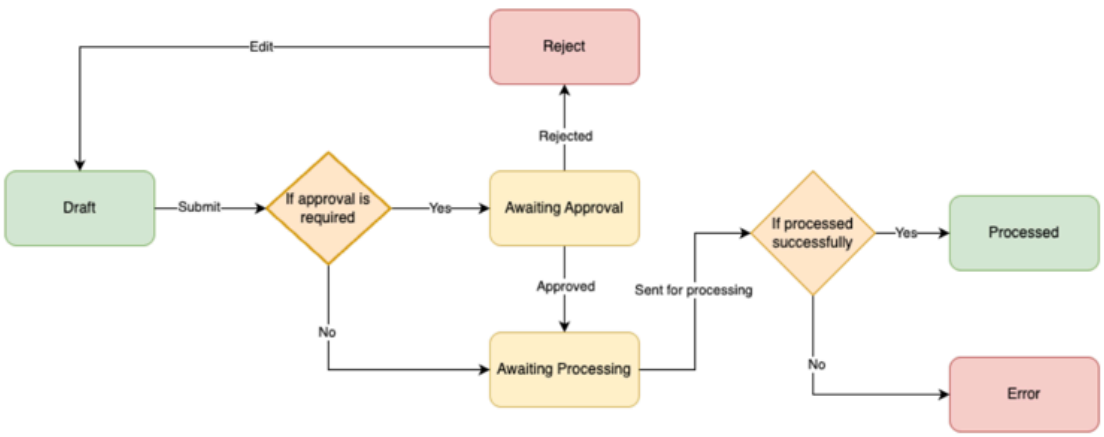
아웃바운드 인텔 공유 통제 구성

아웃바운드 인텔리전스 기록 공유 자동화

Threat Intelligence 공유 승인 워크플로우

이 섹션에서는 인텔리전스 데이터를 외부 조직과 공유할 때 필요한 다양한 승인 수준에 대해 간략하게 설명합니다.

아래 워크플로우는 외부 데이터 공유와 관련된 다양한 승인 수준을 보여줍니다. 승인 수준에 대한 자세한 내용은 다음 문서를 GUI에서 아웃바운드 인텔리전스 기록 공유참조하십시오.



아웃바운드 인텔리전스 기록 공유 자동화

자동화된 아웃바운드 인텔리전스 공유를 통해 인텔리전스 레코드를 외부 시스템에 원활하게 자동으로 배포할 수 있습니다.

시작하기 전에
필요한 역할:

- 시스템 관리자(보기, 만들기 또는 편집)
- sn_sec_tisc.admin(보기)

이 태스크 정보
자동화된 플로우 작업은 지정된 기록으로 아웃바운드 인텔리전스 공유 기록을 생성하고 그에 따라 처리합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

자동화된 프로세스를 통해 아웃바운드 인텔리전스 공유 기록 생성:

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 보안 센터 〉 관리.
2. 선택 자동화된 플로우.
3. 플로우 디자이너에서 해당 규칙 상세 정보를 보려면 신뢰할 수 있는 파트너와 고위험 IOC의 자동화된 공유 작업 링크를 선택합니다.
4. 다음 트리거에 대한 플로우 디자이너 작업을 봅니다.

   ```
   Daily at 12.00.00
   Run every day once
   ```

5. 동작으로 이동
6. 완료를 선택합니다.

다음에 수행할 작업

플로우를 활성화합니다. 자동화된 플로우에 대한 자세한 내용은 다음 문서를 참조하십시오 신뢰할 수 있는 파트너와 고위험 IOC의 공유 자동화.

관련 정보

아웃바운드 인텔 공유 통제 구성

GUI에서 아웃바운드 인텔리전스 기록 공유

데이터 임포트 작업

데이터 임포트를 사용하면 임포트 작업을 위해 처리 중인 모든 기록을 볼 수 있으며 승인을 기다리고 있는 임포트 작업도 나열할 수 있습니다.

모든 임포트 보기

이 섹션을 사용하여 모든 사용자에 대해 목록 뷰에 표시되는 임포트한 모든 기록을 봅니다.

시작하기 전에

필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터 〉 임포트.
2. 선택 데이터 임포트 〉 모든 임포트
   이 페이지에는 임포트 작업에 대해 처리 중인 모든 기록이 표시됩니다.
3. 임포트 프로세스의 상태를 보려면 기록을 엽니다.

   주:
   새 임포트를 클릭하여 새 임포트 기록을 만들 수도 있습니다. 이 버튼을 클릭하면 애플리케이션이 인텔리전스 임포트 페이지로 안내합니다. 새 기록 생성에 대한 자세한 내용은 섹션을 참조 에서 인텔리전스 임포트 TISC 하고 각 임포트 유형을 계속 진행합니다.

내 임포트 보기

이 섹션을 사용하여 로그인한 사용자가 생성한 임포트 기록을 봅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터 〉 임포트.
2. 선택 데이터 임포트 〉 내 임포트
   이 페이지에는 임포트 작업의 추가 프로세스를 위해 분류된 모든 기록 및 해당 임포트 기록이 표시됩니다.
3. 임포트 프로세스의 상태를 보려면 기록을 엽니다.

   주:
   새 임포트를 클릭하여 새 임포트 기록을 만들 수도 있습니다. 이 버튼을 클릭하면 애플리케이션이 인텔리전스 임포트 페이지로 안내합니다. 새 기록 생성에 대한 자세한 내용은 섹션을 참조 에서 인텔리전스 임포트 TISC 하고 각 임포트 유형을 계속 진행합니다.

4. 임포트 기록의 요약을 봅니다.

   주:
   임포트 작업이 제출되지 않은 경우 추가 처리를 위해 기록을 제출 하고 승인을 위해 보낼 수 있습니다. 해당 특정 임포트 작업에 승인이 필요하지 않은 경우 해당 기록이 자동으로 처리됩니다.

내 승인 보기

이 섹션을 사용하여 임포트 작업 기록을 검토하고 승인합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터 〉 임포트.
2. 선택 데이터 임포트 〉 내 승인
   이 페이지에는 로그인한 사용자의 승인을 기다리고 있는 모든 임포트 기록이 표시됩니다.
3. 기록을 열어 임포트 기록을 승인하거나 거부합니다.
4. 승인을 클릭하여 임포트 작업 기록을 승인합니다.
   임포트 승인 대화 상자가 표시되고 선택한 임포트를 승인할지 여부를 확인하는 메시지가 표시됩니다.

   주:
   처리 중이던 임포트 작업이 이제 승인되었다는 이메일 알림이 각 사용자에게 전송됩니다. 규칙 승인에 대한 자세한 내용은 다음 문서를 참조하십시오 데이터 임포트 정의 승인 규칙.

5. 대화 상자에서 승인을 선택합니다.
   임포트 작업을 생성한 사용자에게 이메일 알림이 전송되고 처리 중이던 임포트 작업이 이제 승인되었습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

6. 레코드를 거부하려면 거부 를 클릭합니다.

주:

- 거부된 임포트 작업을 검토하고 다시 제출할 수 있습니다. 거부에 대한 의견을 추가하십시오.
- 처리 중인 임포트 작업이 거부되면 임포트 작업 임포트 작업을 생성한 사용자에게 이메일 알림이 전송됩니다.
- 승인을 요청하는 이메일 알림이 승인자에게 전송됩니다.

에서 인텔리전스 임포트 TISC

이 기능을 사용하면 위협 인텔리전스 데이터를 리포지토리로 수동 임포트하여 분석가가 필요에 따라 외부 소스에서 관련 정보를 수집할 수 있습니다.

위협 인텔리전스 데이터를 임포트하는 데 지원되는 형식은 다음과 같습니다.

임포트 형식	설명	지원되는 기록
구조화된 파일에서 임포트	미리보기 링크를 사용하여 샘플 파일을 다운로드하고 구조화된 데이터를 CSV, XLS 또는 XLSX와 같은 호환 가능한 형식으로 업로드합니다.	• 옵저버블 • 표시기
표준 형식에서 임포트	지원되는 파일 형식에는 STIX 2.x JSON 및 MISP JSON 형식이 포함됩니다.	• **STIX 2.1**: 옵저버블, 표시기 • **MISP**: 옵저버블
원시 텍스트에서 임포트	입력을 원시 텍스트로 구문 분석하여 옵저버블을 임포트합니다. 입력의 최대 문자 제한은 10,000자입니다.	옵저버블
파일(구조화되지 않음)에서 임포트	애플리케이션은 업로드된 파일을 자동으로 구문 분석하여 옵저버블을 추출합니다. 지원되는 파일 형식: TXT, CSV, JSON, XLS 및 XLSX.	옵저버블

각 임포트 형식과 지원되는 기록 유형을 더 잘 이해하려면 관련 정보 섹션을 참조하십시오.

관련 정보

구조화된 파일을 사용하여 데이터 임포트

표준 형식을 사용하여 데이터 임포트

원시 텍스트를 사용하여 데이터 임포트

비정형 파일 형식을 사용하여 데이터 임포트

구조화된 파일을 사용하여 데이터 임포트

구조화된 데이터를 지원되는 파일 형식(예: CSV, XLSX, XLS)으로 업로드합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
   위협 인텔 라이브러리 페이지가 표시됩니다.
2. 인텔리전스 임포트를 클릭합니다.
3. 구조화된 파일 카드에서 임포트를 클릭합니다.

> **중요사항:**
> 위협 인텔리전스 데이터를 TXT, CSV, STIX 2.x JSON, MISP JSON 또는 구조적 파일과 같은 지원되는 파일 형식으로 임포트하는 동안 파일 크기는 5MB로 제한됩니다. 원시 텍스트에 대한 문자 제한은 10,000자로 제한됩니다.

4. 양식에서 필드를 채웁니다.

필드	설명
옵션 선택	드롭다운 목록에서 옵저버블 또는 표시기 같은 필수 옵션을 선택합니다. ○ 옵저버블: 임포트할 옵저버블 데이터를 선택합니다. **주:** 옵저버블 데이터를 임포트하는 경우 이 옵션을 선택합니다. 또한 파일의 열 헤더는 수정하지 마십시오. 필수 필드는 값과 유형이며 다른 필드는 선택 사항입니다. 또한 날짜/시간을 YYYY-MM-DDThh:mm:ssZ 형식으로 입력합니다. ○ 표시기: 임포트할 표시기 데이터를 선택합니다. **주:** 표시기 데이터를 임포트하는 경우 이 옵션을 선택합니다. 또한 파일의 열 헤더는 수정하지 마십시오. 표시기의 필수 필드는 패턴, 패턴 유형 및 유효 기간(시작)이며 다른 필드는 선택 사항입니다. 또한 날짜/시간을 YYYY-MM-DDThh:mm:ssZ 형식으로 입력합니다.
표시기에 대한 샘플 파일 미리 보기 및 다운로드	이 링크를 사용하여 미리 보기 링크를 통해 샘플 파일을 다운로드하고 구조화된 데이터를 호환 가능한 파일 형식(예: CSV, XLS 또는 XLSX)으로 업로드합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	주: 열 헤더는 헤더와 정확히 일치해야 합니다. 값, 유형 필드는 파일의 각 옵저버블에 필요합니다. 나머지 필드는 선택 사항이며, 처음 발견됨, 마지막으로 발견됨은 숫자이고 에포크 시간(밀리초)이어야 합니다.
파일 업로드	이 링크를 클릭하여 권장되는 구조 파일 형식으로 파일 데이터를 업로드합니다. 주: 한 번에 하나의 파일만 업로드할 수 있습니다. 새 파일을 추가하려면 기존 파일을 제거하고 새 파일을 추가해야 합니다.
정의 설정	
TLP	드롭다운 목록에서 TLP(Traffic Light Protocol) 표시기를 선택하여 임포트한 기록에 적용합니다. TLP는 TISC에 있으며 민감한 데이터가 의도한 사용자와 공유되도록 다양한 색상으로 레이블이 지정됩니다. ○ CLEAR: 정보를 제한 없이 공유할 수 있습니다. ○ 적색 ○ 호박색+엄격 ○ 호박색 ○ 녹색
신뢰도(0~100)	임포트한 기록에 대해 0-100 사이의 신뢰도 값을 설정합니다.
만료 기간(일)	임포트한 기록의 만료 기간을 입력합니다. 주: 필수 필드입니다.
보안 통제 목록에 옵저버블 추가	적절한 보안 제어 목록에 옵저버블을 추가하려면 이 옵션을 선택합니다. 이 옵션을 사용하면 임포트하는 동안 옵저버블을 보안 제어 목록에 직접 추가할 수 있습니다. 드롭다운 목록에서 사용할 수 있는 옵션은 다음과 같습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	○ 허용 목록 ○ 거부 목록 ○ 안 함 기본 옵션은 없음입니다.
태그	
태그 추가	태그를 사용하여 이 소스에서 시스템으로 수집된 기록에 주석을 달거나 이어마크합니다. 검색 창에 태그 이름을 입력하여 시스템에서 사용 가능한 태그를 선택하거나, 새 태그 이름을 입력하고 추가를 클릭하여 소스에 할당합니다.
분류	
분류 선택	임포트한 데이터의 분류를 선택합니다. 분류를 사용하여 위협 인텔리전스 기록에 할당된 분류로 사용할 수 있는 사전을 정의합니다. 예를 들어, CAPEC 명명법입니다. 자세한 내용은 분류 생성 문서를 참조하십시오. 주: 선택한 분류에 따라 분류 값 옵션이 변경됩니다.
소스 값 재정의	TLP, 신뢰도, 만료, 태그 및 분류에 대한 소스 값을 구성된 값으로 재정의하려면 이 확인란을 선택합니다. 이 확인란을 선택하지 않으면 구성된 값이 비어 있지 않은 경우 적용됩니다.

5. 다음을 클릭합니다.
6. 처리를 위해 제출하기 전에 데이터를 검토합니다.

   주:
   임포트한 기록 검토는 STIX 옵션에 대해 지원되지 않습니다.

   다음을 클릭하면 위 섹션에서 사용자가 제공한 모든 정보의 요약을 볼 수 있으며 아래 섹션에서는 임포트해야 하는 모든 기록을 제공합니다.

   사용자는 모든 유형의 활동을 수행할 수 있으며 오른쪽 상황별 메뉴에서 사용할 수 있는 설명 섹션을 사용하여 여러 사용자가 공동 작업할 수 있습니다. 전체 파일 또는 원시 텍스트가 처리되면 임포트된 기록 목록이 렌더링됩니다. 큰 파일의 임포트 처리에는 더 많은 시간이 소요되며, 처리하는 동안 임포트 기록 페이지에서도 상태를 확인하고 검토하며 제출할 수 있습니다.

   주:
   확인에 실패한 기록은 임포트 프로세스에서 건너뛰고 해당 기록은 추가 처리를 위해 검토 및 제출 페이지에 표시되지 않습니다.

7. 업데이트 유형을 클릭하고 임포트한 기록 중 모든 유형을 업데이트할 유형을 선택합니다.
8. 삭제를 클릭하여 임포트한 기록 중 모든 유형을 삭제합니다.
9. 제출을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

> **주:**
> 임포트 기록을 제출하면 사용자는 구성된 승인 규칙에 따라 해당 임포트 기록을 승인하도록 승인자에게 리디렉션됩니다. 기록을 생성하는 현재 사용자에게 승인 프로세스가 필요하지 않은 경우 기록은 자동 승인 프로세스를 거치며 요청을 제출하는 동안 임포트 작업이 자동으로 승인됩니다.

10. 상태 보기를 클릭하여 임포트 기록의 상태를 보거나 완료를 클릭합니다.
    처리를 위해 데이터를 임포트하면 기록에 처리된 상태가 표시됩니다.
11. 취소(**Cancel**)를 클릭하여 임포트 프로세스를 중단합니다.
12. 필요한 경우 뒤로 이동을 클릭하여 이전 페이지로 돌아가 기록을 검토합니다.

표준 형식을 사용하여 데이터 임포트

STIX 2.x JSON, MISP JSON과 같은 지원되는 파일 형식으로 표준 데이터를 업로드합니다.

시작하기 전에

필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
   위협 인텔 라이브러리 페이지가 표시됩니다.
2. 인텔리전스 임포트를 클릭합니다.
3. 표준 파일 카드에서 임포트를 클릭합니다.

> **중요사항:**
> 위협 인텔리전스 데이터를 TXT, CSV, STIX 2.x JSON, MISP JSON 또는 구조적 파일과 같은 지원되는 파일 형식으로 임포트하는 동안 파일 크기는 5MB로 제한됩니다. 원시 텍스트에 대한 문자 제한은 10,000자로 제한됩니다.

4. 양식에서 필드를 채웁니다.

필드	설명
파일 형식	드롭다운 목록에서 필요한 옵션(예: STIX 2.x JSON 또는 MISP JSON)을 선택합니다. ○ **STIX 2.x JSON: STIX 2.x JSON**에서 임포트할 형식을 선택합니다. **주:** 업로드된 STIX 파일에서 옵저버블 및 표시기만 임포트됩니다. 다른 모든 객체 유형은 가져오기 프로세스 중에 무시됩니다. ○ **MISP JSON:** MISP JSON 형식으로 임포트할 형식을 선택합니다.
파일 업로드	표준 파일 형식으로 데이터를 업로드하려면 이 링크를 클릭합니다.
정의 설정	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
TLP	드롭다운 목록에서 임포트한 기록에 적용할 TLP 표시기를 선택합니다.
신뢰도(0~100)	신뢰도 값을 정의합니다.
만료 기간(일)	임포트한 기록의 만료 기간을 입력합니다. 주: 필수 필드입니다.
태그 추가	태그를 사용하여 이 소스에서 시스템으로 수집된 기록에 주석을 달거나 이어마크합니다. 검색 창에 태그 이름을 입력하여 시스템에서 사용 가능한 태그를 선택하거나, 새 태그 이름을 입력하고 추가를 클릭하여 소스에 할당합니다.
보안 통제 목록에 옵저버블 추가	적절한 보안 제어 목록에 옵저버블을 추가하려면 이 옵션을 선택합니다. 이 옵션을 사용하면 임포트하는 동안 옵저버블을 보안 제어 목록에 직접 추가할 수 있습니다. 드롭다운 목록에서 사용할 수 있는 옵션은 다음과 같습니다. ○ 허용 목록 ○ 거부 목록 ○ 안 함 기본 옵션은 없음입니다.
분류	
분류 선택	임포트한 데이터의 분류를 선택합니다. 분류를 사용하여 위협 인텔리전스 기록에 할당된 분류로 사용할 수 있는 사전을 정의합니다. 예를 들어, CAPEC 명명법입니다. 자세한 내용은 분류 생성 문서를 참조하십시오.
분류 값 선택	분류와 연결된 분류 값을 나타냅니다.
소스 값 재정의	구성된 값에서 TLP, 신뢰도, 만료, 태그 및 분류에 대한 소스 값을 재정의하려면 이 확인란을 선택합니다. 이 확인란을 선택하지 않으면 기본값이 적용됩니다.

5. 다음을 클릭합니다.
6. 처리를 위해 제출하기 전에 데이터를 검토합니다.

주:
임포트한 기록 검토는 STIX 옵션에 대해 지원되지 않습니다.

다음을 클릭하면 위 섹션에서 사용자가 제공한 모든 정보의 요약을 볼 수 있으며 아래 섹션에서는 임포트해야 하는 모든 기록을 제공합니다.

사용자는 모든 유형의 활동을 수행할 수 있으며 오른쪽 상황별 메뉴에서 사용할 수 있는 설명 섹션을 사용하여 여러 사용자가 공동 작업할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
확인에 실패한 기록은 임포트 프로세스에서 건너뛰고 해당 기록은 추가 처리를 위해 검토 및 제출 페이지에 표시되지 않습니다.

7. 업데이트 유형을 클릭하고 임포트한 기록 중 모든 유형을 업데이트할 유형을 선택합니다.
8. 삭제를 클릭하여 임포트한 기록 중 모든 유형을 삭제합니다.
9. 제출을 클릭합니다.

주:

임포트 기록을 제출하면 사용자는 구성된 승인 규칙에 따라 해당 임포트 기록을 승인하도록 승인자에게 리디렉션됩니다. 기록을 생성하는 현재 사용자에게 승인 프로세스가 필요하지 않은 경우 기록은 자동 승인 프로세스를 거치며 요청을 제출하는 동안 임포트 작업이 자동으로 승인됩니다.

10. 상태 보기를 클릭하여 기록의 상태를 보거나 완료를 클릭합니다.
    기록은 처리되면 처리된 상태를 표시합니다.
11. 취소(**Cancel**)를 클릭하여 임포트 프로세스를 중단합니다.
12. 필요한 경우 뒤로 이동을 클릭하여 이전 페이지로 돌아가 기록을 검토합니다.

원시 텍스트를 사용하여 데이터 임포트

원시 텍스트를 복사하여 붙여넣거나 자유 텍스트를 입력하여 옵저버블 데이터를 임포트합니다.

시작하기 전에

필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
   위협 인텔 라이브러리 페이지가 표시됩니다.
2. 인텔리전스 임포트를 클릭합니다.

중요사항:
- 모든 제거 문자는 옵저버블의 구문 분석 및 추출의 일부로 정리됩니다.
- 이 붙여넣은 텍스트 옵션의 경우 URL, 도메인, 파일 이름, 해시 및 IP 주소만 추출되고 데이터 임포트에 대해 다른 옵저버블 유형은 추출되지 않으며, 레지스트리, 디렉터리 유형과 같은 옵저버블 유형의 경우 임포트에서 건너뜁니다.

3. 원시 텍스트 카드에서 임포트를 클릭합니다.

중요사항:
위협 인텔리전스 데이터를 원시 텍스트 형식으로 가져오는 동안 문자는 10,000자로 제한됩니다. 원시 텍스트 옵션을 임시 해결책으로 사용하여 PDF에서 옵저버블을 추출할 수 있습니다.

4. 양식에서 필드를 채웁니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
원시 데이터 텍스트 상자	이 텍스트 상자에 원시 텍스트를 입력하거나, 복사하여 여기에 붙여 넣습니다. 주: 원시 텍스트는 10,000자까지만 입력하거나 붙여넣을 수 있습니다.
정의 설정	
TLP	드롭다운 목록에서 임포트한 기록에 적용할 TLP 표시기를 선택합니다.
신뢰도(0~100)	신뢰도 값을 정의합니다.
만료 기간(일)	임포트한 기록의 만료 기간을 입력합니다. 주: 필수 필드입니다.
보안 통제 목록에 옵저버블 추가	적절한 보안 제어 목록에 옵저버블을 추가하려면 이 옵션을 선택합니다. 이 옵션을 사용하면 임포트하는 동안 옵저버블을 보안 제어 목록에 직접 추가할 수 있습니다. 드롭다운 목록에서 사용할 수 있는 옵션은 다음과 같습니다. ○ 허용 목록 ○ 거부 목록 ○ 안 함 기본 옵션은 없음입니다.
태그 추가	태그를 사용하여 이 소스에서 시스템으로 수집된 기록에 주석을 달거나 이어마크합니다. Staart 검색 창에 태그 이름을 입력하여 시스템에서 사용 가능한 태그를 선택하거나 새 태그 이름을 입력하고 추가를 클릭하여 소스에 할당합니다.
분류	
분류 선택	임포트한 데이터의 분류를 선택합니다. 분류를 사용하여 위협 인텔리전스 기록에 할당된 분류로 사용할 수 있는 사전을 정의합니다. 예를 들어, CAPEC 명명법입니다. 자세한 내용은 분류 생성 문서를 참조하십시오.

5. 다음을 클릭합니다.
6. 처리를 위해 제출하기 전에 데이터를 검토합니다.

   다음을 클릭하면 위 섹션에서 사용자가 제공한 모든 정보의 요약을 볼 수 있으며 아래 섹션에서는 임포트해야 하는 모든 기록을 제공합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용자는 모든 유형의 활동을 수행할 수 있으며 오른쪽 상황별 메뉴에서 사용할 수 있는 설명 섹션을 사용하여 여러 사용자가 공동 작업할 수 있습니다.

주:
확인에 실패한 기록은 임포트 프로세스에서 건너뛰고 해당 기록은 추가 처리를 위해 검토 및 제출 페이지에 표시되지 않습니다.

7. 업데이트 유형을 클릭하고 임포트한 기록 중 모든 유형을 업데이트할 유형을 선택합니다.
8. 삭제를 클릭하여 임포트한 기록 중 모든 유형을 삭제합니다.
9. 제출을 클릭합니다.

주:
임포트 기록을 제출하면 사용자는 구성된 승인 규칙에 따라 해당 임포트 기록을 승인하도록 승인자에게 리디렉션됩니다. 기록을 생성하는 현재 사용자에게 승인 프로세스가 필요하지 않은 경우 기록은 자동 승인 프로세스를 거치며 요청을 제출하는 동안 임포트 작업이 자동으로 승인됩니다.

10. 상태 보기를 클릭하여 기록의 상태를 보거나 완료를 클릭합니다.
    기록은 처리되면 처리된 상태를 표시합니다.
11. 취소(**Cancel**)를 클릭하여 임포트 프로세스를 중단합니다.
12. 필요한 경우 뒤로 이동을 클릭하여 이전 페이지로 돌아가 기록을 검토합니다.

비정형 파일 형식을 사용하여 데이터 임포트

TXT, CSV, JSON, XLS, XLSX와 같은 파일 형식을 사용하여 지원되는 구조화되지 않은 형식으로 데이터를 업로드합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
   위협 인텔 라이브러리 페이지가 표시됩니다.
2. 인텔리전스 임포트를 클릭합니다.

중요사항:
- 모든 제거 문자는 옵저버블의 구문 분석 및 추출의 일부로 정리됩니다.
- 이 비정형 파일 형식 옵션의 경우 URL, 도메인, 파일 이름, 해시 및 IP 주소만 추출되고 데이터 임포트에 대한 다른 옵저버블 유형은 추출되지 않으며, 레지스트리, 디렉터리 유형과 같은 옵저버블 유형의 경우 임포트를 건너뜁니다.

3. 파일(구조화되지 않은) 카드에서 임포트를 클릭합니다.

주:
위협 인텔리전스 데이터를 TXT, CSV, STIX 2.x JSON, MISP JSON 또는 구조적 파일과 같은 지원되는 파일 형식으로 임포트하는 동안 파일 크기는 5MB로 제한됩니다.

4. 양식에서 필드를 채웁니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
파일 업로드	표준 파일 형식으로 데이터를 업로드하려면 이 링크를 클릭합니다.
정의 설정	
TLP	드롭다운 목록에서 임포트한 기록에 적용할 TLP 표시기를 선택합니다.
신뢰도(0~100)	신뢰도 값을 정의합니다.
만료 기간(일)	연결된 옵저버블의 만료 기간을 입력합니다. 주: 필수 필드입니다.
보안 통제 목록에 옵저버블 추가	적절한 보안 제어 목록에 옵저버블을 추가하려면 이 옵션을 선택합니다. 이 옵션을 사용하면 임포트하는 동안 옵저버블을 보안 제어 목록에 직접 추가할 수 있습니다. 드롭다운 목록에서 사용할 수 있는 옵션은 다음과 같습니다. ○ 허용 목록 ○ 거부 목록 ○ 안 함 기본 옵션은 없음입니다.
태그 추가	태그를 사용하여 이 소스에서 시스템으로 수집된 기록에 주석을 달거나 이어마크합니다. 검색 창에 태그 이름을 입력하여 시스템에서 사용 가능한 태그를 선택하거나, 새 태그 이름을 입력하고 추가를 클릭하여 소스에 할당합니다.
분류	
분류 선택	임포트한 데이터의 분류를 선택합니다. 분류를 사용하여 위협 인텔리전스 기록에 할당된 분류로 사용할 수 있는 사전을 정의합니다. 예를 들어, CAPEC 명명법입니다. 자세한 내용은 분류 생성 문서를 참조하십시오.

5. 처리를 위해 제출하기 전에 데이터를 검토합니다.

   다음을 클릭하면 위 섹션에서 사용자가 제공한 모든 정보의 요약을 볼 수 있으며 아래 섹션에서는 임포트해야 하는 모든 기록을 제공합니다.

   사용자는 모든 유형의 활동을 수행할 수 있으며 오른쪽 상황별 메뉴에서 사용할 수 있는 설명 섹션을 사용하여 여러 사용자가 공동 작업할 수 있습니다.

   주:
   지원되는 데이터 임포트 형식은 TXT, CSV, JSON, XLS이며 확인에 실패한 기록은 임포트 프로세스에서 건너뛰고 이러한 기록은 처리를 위해 검토 및 제출 페이지에 표시되지 않습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

6. 업데이트 유형을 클릭하고 임포트한 기록 중 모든 유형을 업데이트할 유형을 선택합니다.
7. 삭제를 클릭하여 임포트한 기록 중 모든 유형을 삭제합니다.
8. 제출을 클릭합니다.

> 주:
> 임포트 기록을 제출하면 사용자는 구성된 승인 규칙에 따라 해당 임포트 기록을 승인하도록 승인자에게 리디렉션됩니다. 기록을 생성하는 현재 사용자에게 승인 프로세스가 필요하지 않은 경우 기록은 자동 승인 프로세스를 거치며 요청을 제출하는 동안 임포트 작업이 자동으로 승인됩니다.

9. 상태 보기를 클릭하여 기록의 상태를 보거나 완료를 클릭합니다.
   제출이 성공하면 기록에 처리 상태가 표시됩니다.
10. 취소(**Cancel**)를 클릭하여 임포트 프로세스를 중단합니다.
11. 필요한 경우 뒤로 이동을 클릭하여 이전 페이지로 돌아가 기록을 검토합니다.

위협 분석가 워크벤치

위협 분석가 워크벤치 페이지는 위협 분석가와 해당 팀에 속한 케이스 및 케이스 작업으로 구성됩니다.

케이스 관리 기능을 사용하여 위협 조사 및 분석 활동을 생성하고 추적합니다.

위협 조사 중에 분석가는 옵저버블, 위협 행위자, 캠페인 등과 같은 내부 인텔리전스 기록에서 데이터를 수집합니다.

워크벤치 개요

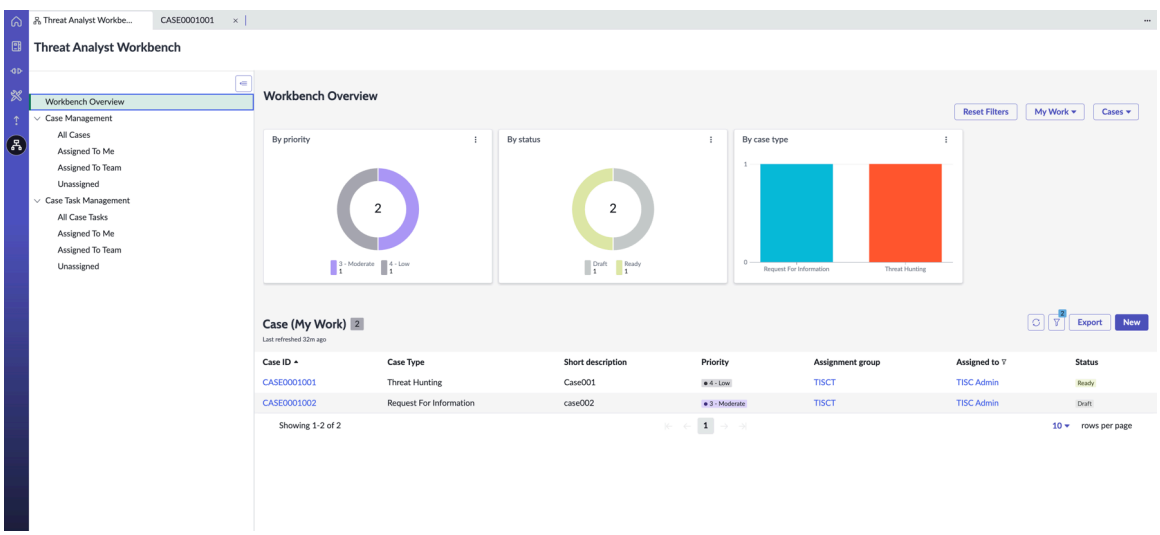
워크벤치 개요 페이지는 위협 분석가와 해당 팀 아래에 있는 케이스 작업 및 케이스로 구성됩니다.

개요에는 분석가가 작업 부하를 관리하고 조사 우선순위를 지정하는 데 도움이 되는 모든 오픈 케이스와 해당 상태가 나열됩니다.

필요한 역할: sn_sec_tisc.analyst, sn_sec_tisc.admin

케이스가 생성되면 분석가는 추가 조사를 위해 다른 분석가나 팀에 케이스 작업을 할당하고 이들과 공동 작업하여 정보와 인사이트를 공유합니다.

각 필터 아래에는 위협 분석가의 큐와 위협 분석가 팀의 큐에 있는 우선순위, 상태 및 케이스 유형별로 그룹화된 다양한 위젯이 있습니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

위젯에 필터를 적용하면 개요 페이지의 아래쪽 절반이 목록 항목으로 표시되는 해당 케이스 또는 케이스 작업으로 채워집니다. 적용된 필터를 제거하려면 **Reset** Filters(필터 재설정)를 클릭하여 원래 보기로 재설정합니다.

위협 분석가와 관리자는 이 페이지를 사용하여 자신의 작업, 팀 작업 및 할당되지 않은 작업을 볼 수 있습니다. 드롭다운 목록으로 이동할 수 있습니다. 사용 가능한 옵션은 다음과 같습니다.

- 내 작업: 할당된 작업을 보려면 이 옵션을 선택합니다.
- 내 팀의 작업: 내가 속한 모든 그룹에 할당된 팀의 작업을 보려면 이 옵션을 선택합니다.
- 미할당 작업: 할당되지 않은 케이스 또는 케이스 작업을 보려면 이 옵션을 선택합니다. 케이스 또는 케이스 작업을 할당하려면 양식 뷰로 이동하여 케이스 및 케이스 작업에 사용자 또는 사용자 그룹을 할당해야 합니다.

또한 본인에게 할당된 워크벤치 개요에서 케이스 및 케이스 작업을 직접 볼 수 있습니다. 기본적으로 케이스 뷰가 표시되며, 우선순위 및 상태별로 케이스 작업을 보려면 드롭다운을 사용하여 케이스 작업을 선택할 수 있습니다.

위협 분석가 워크벤치를 사용하여 케이스 생성

케이스는 조직을 위협하는 캠페인 또는 위협 행위자에 대한 정보를 추적하는 데 사용됩니다. 케이스를 만든 후에는 아티팩트를 추가하여 단일 케이스 또는 케이스 작업에서 모든 관련 정보를 검토하고 분석할 수 있습니다.

시작하기 전에

필요한 역할: sn_sec_tisc.analyst, sn_sec_tisc.admin

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 위협 분석가 워크벤치 아이콘을 클릭합니다.
3. 이동 케이스 관리 〉 모든 케이스.
   모든 케이스가 표시됩니다.
4. 새로 만들기를 클릭합니다.
5. 필드에 적절하게 입력합니다.

새 케이스 작성

필드	설명
케이스 ID	케이스의 고유 식별자입니다. 시스템에서 생성된 ID입니다.
간단한 설명	조사 중인 요청이나 문제 또는 간단한 설명에 대한 요약입니다.
설명	배경, 필요한 분석, 예상되는 결과 등 케이스에 대한 관련 정보를 포함한 자세한 설명입니다.
케이스 유형	조사 중인 케이스의 유형을 선택합니다. 조사에 사용할 수 있는 옵션은 다음과 같습니다. ○ 위협 헌팅 ○ 정보 요청 ○ 취약성 관리 케이스 ○ 규정 준수 케이스

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	○ 인시던트 응답 케이스 ○ 공동 작업 케이스 ○ 기타
우선순위	요청 또는 문제의 심각도에 대한 평가입니다.
할당 그룹	케이스 작업을 담당하는 할당된 그룹입니다.
상태	케이스의 현재 상태입니다.
담당자	케이스 작업을 담당하는 분석가입니다.
기한	작업을 완료하거나 종결해야 하는 날짜 및 시간입니다.
기고자	작업에서 롤업된 담당자 목록이며 그 위에 추가할 수 있어야 합니다.
TLP	TLP별 데이터 민감도 설정을 나타내는 고유 값입니다.
관찰 목록	사용자가 감시 목록에 추가되면 해당 사용자는 상태 및 우선 순위 변경에 대한 이메일 알림을 받게 됩니다.
제한 강화	허용된 그룹 및 허용된 구성원의 구성원을 수정하려면 이 확인란을 선택합니다. 자세한 내용은 케이스에 적용된 제한 사항 문서를 참조하십시오.

6. 인사이트 섹션의 필드에 적절히 입력합니다.

인사이트

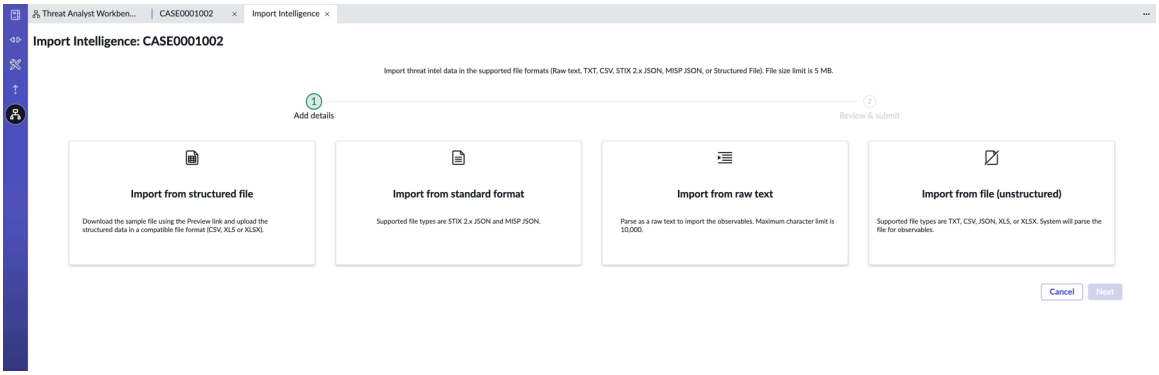
필드	설명
메모	위협 조사와 관련된 추가 메모입니다.
권장 사항 또는 작업	위협 조사와 관련된 권장 사항 또는 작업입니다.
분석 및 결과	위협 조사와 관련된 분석 및 결과를 입력합니다.
종결 요약	결과의 종결 요약을 추가합니다.

7. 저장을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

기록이 저장되면 인텔리전스 임포트 탭을 클릭하여 인텔리전스 임포트 기능을 사용하여 위협 인텔리전스 데이터를 임포트할 수 있습니다.

주:
케이스 관리에서 데이터를 임포트하고 처리하는 경우 고유 항목이 임포트 기록과 연결됩니다.



케이스에 적용된 제한 사항

이 기능을 사용하여 케이스를 제한하고 이에 액세스할 수 있는 그룹 및 사용자 목록을 제공합니다.

필요한 역할:

- sn_sec_tisc.분석가
- sn_sec_tisc_admin
- sn_sec_tisc.restriction_access_manager

주요 고려 사항

1. 케이스를 제한하고 이에 접근할 수 있는 그룹/사용자 목록을 제공합니다.
2. 케이스 양식 페이지에서 제한 적용 필드를 활성화합니다.
3. 허용된 그룹 및 허용된 구성원의 구성원을 수정합니다.
4. 케이스가 제한됨으로 표시되면 허용된 그룹의 구성원, 허용된 사용자 목록의 구성원 및 sn_sec_tisc.admin 역할을 가진 사용자만 이 케이스에 액세스할 수 있습니다.
5. 제한 적용 필드에 액세스해야 하는 분석가(이 역할을 가진 sn_sec_tisc.restriction_access_manager)에게 액세스 권한을 부여합니다.
6. 제한됨으로 표시한 기존 assigned_to 분석가와 분석가도 허용된 그룹이나 구성원에 추가되지 않으면 액세스 권한을 잃게 됩니다.
7. CTI 팀 내 케이스에 대한 제한은 케이스별로 구현됩니다. 허용된 구성원은 허용 목록에 있는 경우 제한된 케이스에 접근할 수 있습니다. 케이스 허용 목록 중 하나에 배치한다고 해서 다른 모든 제한된 케이스에 액세스할 수 있는 것은 아닙니다.
8. 케이스가 제한되고 허용된 구성원으로 표시되거나 허용된 그룹이 비어 있는 경우 sn_sec_tisc.admin만 이러한 제한된 케이스에 액세스할 수 있습니다.
9. 분석가(sn_sec_tisc.analyst) 역할이 할당된 그룹만 허용된 구성원 및 허용된 그룹 목록에 허용됩니다.

주:
케이스가 제한된 것으로 표시되면 작업 메모가 게시됩니다.

케이스에 대한 액세스 제어

케이스에 특정한 접근 제어를 허용합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음 표에서는 역할 및 액세스 제어에 대해 설명합니다.

역할	접근	설명
sn_sec_tisc.restriction_access_manager	읽기 액세스	여기에 추가된 외부 사용자는 케이스 양식을 볼 수 있는 접근 권한을 얻지만 케이스의 필드를 편집하거나 작업을 수행할 수는 없습니다.
	권한 있는 액세스	여기에 추가된 외부 사용자는 케이스 양식의 모든 필드를 편집할 수 있지만 오케스트레이션을 실행할 수는 없습니다.
sn_sec_tisc.special_access_read_manager	읽기 액세스	여기에 추가된 외부 사용자는 케이스 양식을 볼 수 있는 접근 권한을 얻지만 케이스의 필드를 편집하거나 작업을 수행할 수는 없습니다.
sn_sec_tisc.special_access_write_manager	권한 있는 액세스	여기에 추가된 외부 사용자는 케이스 양식의 모든 필드를 편집할 수 있지만 오케스트레이션을 실행할 수는 없습니다.

케이스 작업에 대한 외부 사용자 액세스

이 섹션에서는 케이스 작업에 대한 외부 사용자 액세스에 대해 설명합니다.

외부 사용자에게 케이스 작업 할당

케이스 작업은 sn_sec_tisc.analyst 역할에 접근할 수 없더라도 외부 역할을 가진 사용자에게 할당됩니다.

1. 케이스 작업에 할당된 모든 외부 사용자는 케이스 작업 모듈을 볼 수만 있으며 케이스 작업을 편집할 수 있는 권한을 갖습니다.
2. 외부 사용자는 해당 특정 사용자 또는 사용자가 속한 그룹에만 할당된 케이스 작업을 볼 수 있습니다.
3. 외부 사용자는 사용자가 속한 그룹 내에서 작업을 재할당할 수 있어야 합니다.

MITRE 기술을 케이스에 연결

하나 이상의 MITRE 기술을 케이스에 연결합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 위협 분석가 워크벤치 아이콘을 클릭합니다.
3. 이동 케이스 관리 〉 모든 케이스.
   모든 케이스가 표시됩니다.
4. 케이스를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. **MITRE** 기술 연결 버튼을 클릭합니다.
6. 매트릭스 추가를 클릭하여 MITRE 기술을 연결합니다.
   MITRE 기술을 케이스에 연결 대화 상자가 표시됩니다.
7. 매트릭스를 선택합니다.
   매트릭스를 선택할 수 있도록 활성화된 모든 매트릭스가 표시됩니다.
8. 드롭다운 목록에서 전술을 선택합니다.
   매트릭스와 관련된 모든 전술이 표시됩니다.

   주:
   전술을 더 추가하려면 전술 추가를 클릭하십시오. 새 전술을 추가하는 경우 이전에 선택한 전술은 더 이상 드롭다운 목록에 표시되지 않습니다.

9. 기술을 선택합니다.
   선택한 전술과 관련된 모든 기술이 표시됩니다. 전술을 더 추가하는 경우 선택한 전술에 연결된 기술을 선택할 수 있습니다.
10. 저장을 클릭합니다.
    전체 매트릭스 관련 데이터를 삭제하려면 매트릭스 삭제를 클릭합니다. 이 작업은 연결된 매트릭스 데이터만 제거하지만 매트릭스는 MITRE ATT&CK 리포지토리에 남아 있습니다.

    연결된 매트릭스 데이터 기록은 MITRE ATT&CK 카드 섹션 아래에 표시됩니다. 카드 뷰에서 다음을 수행합니다.

    주:
    매트릭스 드롭다운 목록에서 여러 매트릭스 간에 전환할 수 있습니다.

    a. 카드 뷰의 첫 번째 행에는 현재 선택한 매트릭스와 관련된 모든 전술이 표시됩니다.
    b. 각 방법 카드에는 현재 케이스 기록에 매핑된 해당 전술의 전술 이름과 기술 수가 표시됩니다.
    c. 해당 사례와 관련된 모든 기술은 각 전술 아래에 수직으로 표시됩니다. 기술을 클릭하면 기술 양식 뷰를 볼 수 있습니다.
11. **ID** 표시를 클릭하면 관련된 모든 기술에 대한 ID가 표시됩니다.

    주:
    각 기술 카드에는 **Show ID** 가 활성화된 경우에만 기술 이름과 기술 ID가 표시됩니다.

12. 새로 고침을 클릭하여 카드 뷰를 새로 고칩니다.
    선택한 매트릭스에 대한 마지막 새로 고침의 시간소인을 볼 수 있습니다.

    주:
    새 탭에서 보려는 연결된 매트릭스 카드를 팝업하려면 팝 아웃 아이콘을 클릭합니다.

MITRE 기술 연결 롤업

케이스 기록에서 연결되거나 연결 해제된 옵저버블, 표시기, 객체 및 보안 인시던트의 MITRE 기술 연결을 롤업합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에

주:

- 보안 인시던트에 대한 MITRE 기술 연결의 롤업은 보안 인시던트의 MITRE 기술 관련 데이터를 TISC의 케이스 관리로 롤업합니다.
- 기본적으로 이 속성 sn_sec_tisc.auto_rollup_mitre_data는 연결된 객체 또는 보안 인시던트에서 케이스로 자동 롤업되는 MITRE 기술에 대해 활성화됩니다.
- MITRE 기술 연결의 요청 시 롤업을 수행하려면 케이스 양식 뷰 내에서 추가 작업으로 이동하여 **MITRE** 기술 롤업 옵션을 선택합니다. 이 작업은 비동기식으로 발생하며 롤업 활동의 업데이트에 대한 활동 스트림 섹션을 확인할 수 있습니다.

필요한 역할: sn_sec_tisc.analyst

이 태스크 정보

- 옵저버블 또는 표시기와 같은 엔터티가 케이스에 연결될 때마다 해당 엔터티에 대해 존재하는 모든 MITRE 기술 연결이 케이스로 자동 롤업됩니다.
- 옵저버블 또는 표시기와 같은 엔터티가 연결 해제되고 케이스에서 제거될 때마다 해당 엔터티에 대해 존재하는 케이스에서 롤업된 모든 MITRE 기술 연결이 자동으로 제거되고 케이스로 롤업됩니다.

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 위협 분석가 워크벤치 아이콘을 클릭합니다.
3. 이동 케이스 관리 〉 모든 케이스.
   모든 케이스가 표시됩니다.
4. 아무 케이스나 엽니다.
5. 아티팩트 탭으로 이동합니다.
6. 아티팩트 관련 목록에서 옵저버블 을 선택합니다.
7. 링크 단추를 선택합니다.
8. 케이스에 연결할 수 있는 옵저버블을 선택합니다.
9. 링크를 클릭하여 옵저버블을 연결합니다.
   옵저버블을 케이스에 연결하면 해당 특정 옵저버블과 연결된 MITRE 기술이 자동으로 롤업되고 아티팩트 섹션 아래의 MITRE 기술 목록 수가 자동으로 업데이트됩니다.
10. 케이스에서 옵저버블의 연결을 해제하려면 연결 해제 를 클릭합니다.
    옵저버블을 케이스에 연결 해제하면 해당 특정 옵저버블과 연결된 MITRE 기술이 자동으로 제거되고 아티팩트 섹션 아래의 MITRE 기술 목록 수가 자동으로 업데이트됩니다.

위협 분석가 워크벤치를 사용하여 케이스 작업 생성

케이스와 연결할 케이스 작업을 생성합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst, sn_sec_tisc.admin

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 위협 분석가 워크벤치 아이콘을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 이동 케이스 작업 관리 〉 모든 케이스 작업.
   모든 케이스 작업이 표시됩니다.
4. 새로 만들기를 클릭합니다.
5. 필드에 적절하게 입력합니다.

새로운 케이스 작업 생성

필드	설명
작업 ID	케이스 작업에 대한 고유 식별자입니다. 시스템에서 생성된 ID입니다.
간단한 설명	조사 중인 요청이나 문제 또는 간단한 설명에 대한 요약입니다.
설명	백그라운드, 필요한 분석, 예상되는 결과 등 케이스 작업에 대한 관련 정보를 포함한 자세한 설명입니다.
상위 케이스 ID	조회에서 상위 케이스 ID를 선택합니다.
우선순위	요청 또는 문제의 심각도에 대한 평가입니다.
할당 그룹	케이스 작업 수행을 담당하는 할당된 그룹입니다.
상태	케이스 작업의 현재 상태입니다.
담당자	케이스 작업 수행을 담당하는 분석가입니다.
기한	케이스 작업이 완료되거나 종결되어야 하는 날짜 및 시간입니다.
TLP	TLP별 데이터 민감도 설정을 나타내는 고유 값입니다.
제한 강화	sn_sec_tisc_admin로, 허용된 그룹 및 허용된 구성원의 구성원을 수정하려면 이 확인란을 선택합니다. 자세한 내용은 케이스에 적용된 제한 사항 문서를 참조하십시오.

6. 인사이트 섹션의 필드에 적절히 입력합니다.

인사이트

필드	설명
메모	위협 조사와 관련된 추가 메모입니다.
종결	결과의 종결 요약을 추가합니다.

7. 저장을 클릭합니다.
   케이스 작업이 케이스와 연결됩니다.

주:
케이스 작업을 저장한 후 작업에 태그와 분류를 추가할 수 있습니다. 자세한 내용은 분류 생성 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

조사 캔버스 작업

조사 캔버스는 TI(위협 인텔리전스) 분석가에게 보다 귀중한 정보를 제공하는 중요한 핵심 기능입니다. 일대일 또는 일대다 관계를 매핑하고 옵저버블, 침해지표(IOC) 또는 엔터티와 관련된 정보를 시각화하여 구조화된 프레임워크를 제공합니다.

위협 분석가는 조사 캔버스를 사용하여 다음을 효과적으로 수행할 수 있습니다.

- 관계 매핑: 옵저버블, IOC(침해 표시기), 위협 행위자, 공격 패턴, 영향을 받는 자산 등과 같은 다양한 엔터티 간의 노드 연결을 시각화합니다. 조사 캔버스의 각 객체는 객체 유형, 노드 유형 및 상태와 함께 특정 색상으로 표시됩니다. 상태는 옵저버블 및 기타 객체 유형에 대해 의심스러움, 낮음 또는 중요 와 같은 객체의 평판을 반영합니다. 지표는 분석의 우선순위를 지정하는 데 도움이 되도록 관련 위협 심각도와 함께 표시됩니다.
- 케이스 또는 캔버스 연결: 케이스 또는 캔버스를 연결하여 분석을 개선하고 케이스 관리 내에서 위협 환경에 대한 보다 포괄적인 뷰를 제공합니다.
  - 링크 기능을 사용하면 분석가가 노드를 동적으로 추가하거나 제거할 수 있습니다. 이렇게 하면 노드 간의 기존 관계도 캔버스에 채워집니다.
  - 조사 캔버스의 컨텍스트 내에서 관계를 별도로 저장하여 임시 관계 그래프를 만듭니다.
- **MITRE** 기술 연결: 캔버스에서 직접 노드와 MITRE 기술을 연결하거나 제거하고 MITRE 킬 체인 카드에 대한 분석을 제공합니다.

조사 캔버스의 엔트리포인트

1. 첫 번째 진입점: 새 빈 캔버스: 이 진입점을 통해 분석가는 노드나 링크 없이 새롭고 빈 캔버스를 열 수 있습니다.
2. 두 번째 진입점: 케이스 조사에서 캔버스 열기:
   a. 이 엔트리포인트는 기존 조사 케이스를 열고 캔버스를 편집, 수정, 이름 변경할 수 있도록 합니다.
   b. 기존 아티팩트가 노드로 있는 새 캔버스입니다.

조사 캔버스에서 작업

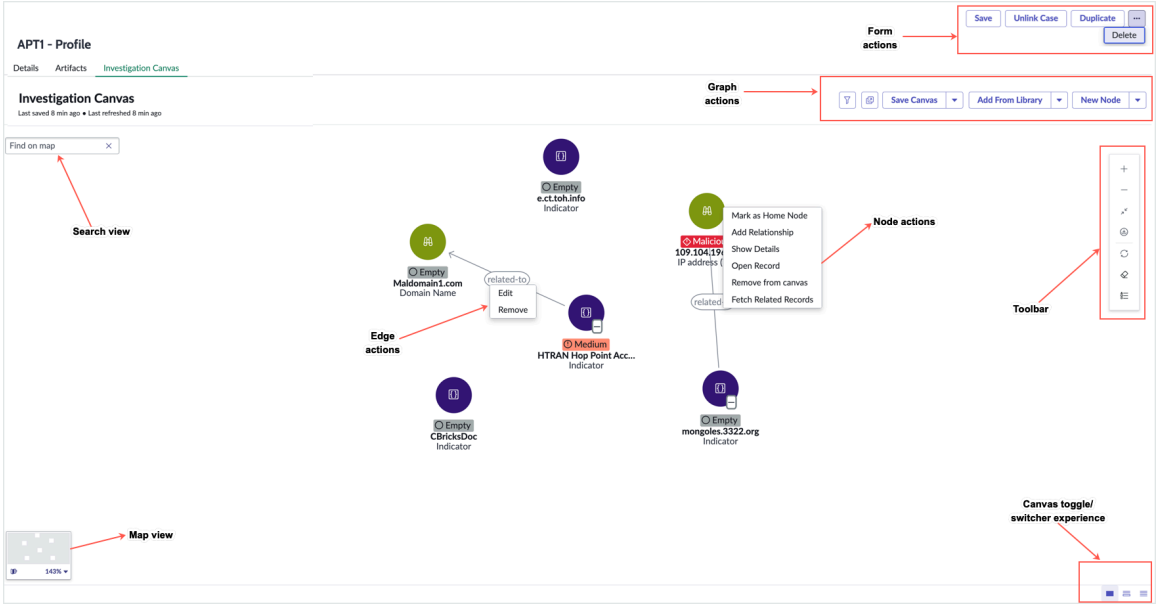
이 섹션에서는 조사 캔버스에서 수행할 수 있는 다양한 작업에 대해 설명합니다.

조사 캔버스에는 다음이 포함됩니다.

1. 양식 작업
2. 그래프 작업
3. 노드 작업
4. 에지 작업
5. 도구 모음 작업

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

조사 캔버스



조사 캔버스 양식 작업

작업	운영
케이스 연결	조사 캔버스에서 케이스를 연결할 수 있습니다.
케이스 연결 해제	조사 캔버스에서 케이스의 연결을 해제할 수 있습니다.
저장	케이스 기록을 저장하는 옵션입니다.
복제	조사 캔버스의 노드를 복제하는 옵션입니다.
삭제	캔버스를 삭제하는 옵션입니다.

조사 캔버스 그래프 작업

작업	운영
맵에서 찾기	여러 노드와 에지를 검색할 수 있습니다.
캔버스 필터	필터 기능을 사용하면 조사 캔버스에서 뷰를 구체화할 수 있습니다. 예를 들어 캠페인과 같은 기록 유형을 필터링하면 캔버스 표시에서 일시적으로 제거됩니다. 필터를 적용하여 맵에 표시되는 엔터티 또는 기록 유형을 통제하여 보다 깔끔하고 집중적인 조사 경험을 제공할 수 있습니다. **주:** 필터를 사용하여 옵저버블 또는 위협 행위자와 같이 가장 관련성이 높은 노드만 강조 표시하고 캔버스에서 덜 중요한 정보를 일시적으로 숨깁니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

조사 캔버스 그래프 작업

작업	운영
캔버스 저장	조사 캔버스를 저장할 수 있습니다.
라이브러리에 데이터 추가	이 옵션을 사용하면 조사 캔버스에서 서로 다른 두 노드 간에 새 관계를 설정할 수 있습니다. 새 노드, 노드 간의 새 링크, 편집되거나 수정된 에지 레이블을 포함하여 캔버스에서 수행된 모든 변경 사항이 라이브러리에 저장됩니다. 현재 캔버스에 있는 모든 노드는 연결된 케이스에 아티팩트로 추가됩니다. 데이터가 라이브러리에 성공적으로 저장되면 확인 메시지가 표시됩니다.
라이브러리에서 추가	이 작업은 위협 인텔리전스 라이브러리 데이터를 추가하고 위협 인텔리전스 라이브러리에서 임포트한 새 노드와 조사 캔버스의 기존 노드 간의 관계를 설정합니다.
케이스 아티팩트에서 추가	캔버스에 연결된 해당 케이스 아티팩트에서 데이터를 추가할 수 있습니다.

조사 캔버스 노드 작업

작업	운영
홈 노드로 표시	이 옵션을 사용하면 특정 노드를 조사 캔버스의 홈 노드로 표시할 수 있습니다. 분석 중에 피벗할 때 애플리케이션은 홈 노드를 자동으로 강조 표시하고 중앙에 배치하여 캔버스 중앙에 초점을 맞춥니다. 포커스를 맞춘 노드는 다음을 통해 시각적으로 강조됩니다. • 뚜렷한 테두리 • 강조 • 미묘한 원형 모션 애니메이션 이렇게 하면 조사의 주요 초점과 관련된 캔버스 데이터를 더 쉽게 식별하고 탐색할 수 있습니다.
관계 추가	이 옵션을 사용하면 조사 캔버스의 노드 간에 맞춤 관계를 추가할 수 있습니다. 다음과 같은 관계 유형을 정의할 수 있습니다. • 일대다 • 다대일 • 다대다 이는 엔터티 간의 복잡한 연결을 나타내는 데 도움이 됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

조사 캔버스 노드 작업

작업	운영
상세 정보 표시	이 옵션을 사용하면 조사 캔버스에서 선택된 노드에 대한 자세한 정보(해당 속성 및 관련 옵저버블 또는 관계 포함)를 볼 수 있습니다.
기록 오픈	이 옵션을 사용하면 보다 쉽게 참조하고 멀티태스킹할 수 있도록 선택한 기록을 새 브라우저 탭에서 열 수 있습니다.
캔버스에서 제거	이 옵션을 사용하면 조사 캔버스에서 선택한 노드를 제거하여 현재 뷰에서 효과적으로 삭제할 수 있습니다.
관련 기록 가져오기	이 옵션을 사용하면 특정 노드에 대한 관련 레코드를 가져오고 **Select Entity** Types 대화 상자를 사용하여 조사 캔버스에 직접 추가할 수 있습니다. 모든 객체 관련 기록 유형을 지정된 선택 상자에 자동으로 포함하려면 모두 추가 옵션을 선택합니다. 예를 들어, 관련 기록의 유형이 5개에서 10개인 경우 각 개체 유형을 수동으로 선택해야 합니다. 모두 추가 기능은 모든 관련 기록을 한 번에 채워 이 프로세스를 간소화함으로써 사용자 경험을 개선합니다. 기록을 추가한 후에는 레코드를 제거하거나 확장 옵션을 선택하여 관련 노드를 볼 수 있습니다. 그러나 사용성을 향상시키기 위해 이제 기록을 수동으로 추가하거나 확장하는 대신 모두 확장을 선택하여 노드에 연결된 모든 관련 기록을 즉시 확장할 수 있습니다.

조사 캔버스 에지 작업

작업	운영
편집	이 옵션을 사용하면 조사 캔버스에서 엣지의 레이블을 편집하고 수정하여 노드 간의 관계를 보다 명확하게 표현할 수 있습니다.
제거	이 옵션을 사용하면 조사 캔버스에서 에지를 제거하여 두 노드 간의 시각적 연결을 효과적으로 삭제할 수 있습니다.

조사 캔버스 도구 모음 아이콘

작업	운영
확대	조사 캔버스를 확대하여 캔버스의 특정 영역에 쉽게 초점을 맞추는 옵션입니다.

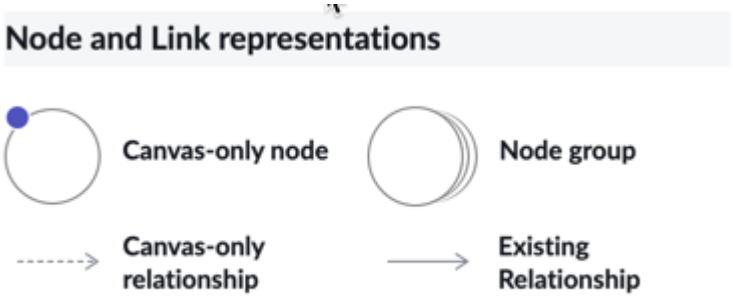
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

조사 캔버스 도구 모음 아이콘

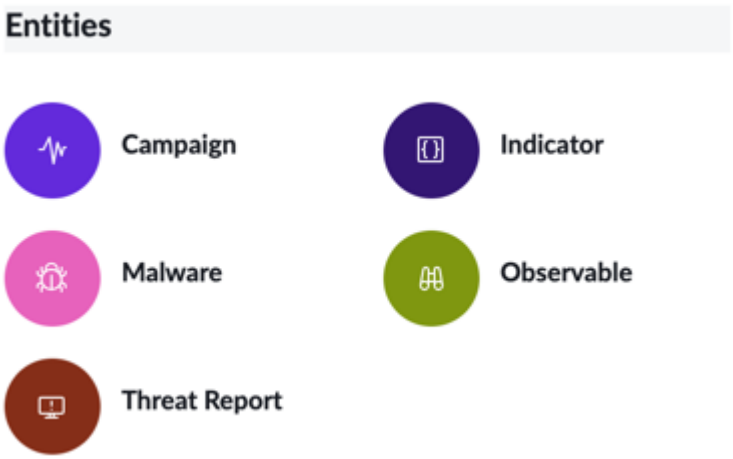
작업	운영
축소	조사 캔버스를 축소하여 캔버스의 특정 영역에 쉽게 초점을 맞추는 옵션입니다.
화면에 맞춤	조사 캔버스를 화면 크기에 맞추는 옵션입니다.
익스포트 맵	더 잘 볼 수 있도록 조사 캔버스를 PDF로 익스포트하는 옵션입니다.
새로 고침	새로 고침 옵션을 사용하면 라이브러리에서 조사 캔버스로 데이터를 새로 고치고 다시 로드할 수 있습니다. 주: 저장하지 않고 새로고침하면 캔버스에 저장되지 않은 변경 내용이 손실됩니다. 데이터 손실을 방지하기 위해 새로 고침하기 전에 캔버스를 저장하는 것이 좋습니다.
캔버스 지우기	캔버스를 지울 수 있습니다. 이 선택은 조사 캔버스에서 노드를 일시적으로 제거합니다. 캔버스를 지울지 여부를 확인하는 확인 메시지가 표시됩니다. 계속하려면 메시지를 확인하십시오. 주: 조사 캔버스를 변경한 후에는 캔버스를 저장 해야 합니다. 변경 사항이 저장되지 않고 캔버스를 새로 고치면 이전 상태로 돌아가고 저장되지 않은 노드 또는 수정 사항은 손실됩니다.
범례	이 옵션은 현재 조사 캔버스에 표시된 노드와 개체를 시각적으로 나타냅니다. 범례에는 두 가지 주요 뷰가 포함됩니다. • 노드 및 링크 표현: 다양한 노드 유형이 캔버스에 표시되는 방식과 에지를 통해 연결되는 방식을 표시합니다. 이를 통해 조사의 다양한 요소 간의 구조와 관계를 빠르게 이해할 수 있습니다. • 엔터티 표현: 현재 캔버스에 있는 엔터티 유형(옵저버블, 표시기 및 객체)을 표시합니다. 다음은 노드, 링크 및 엔터티 표현에 대한 범례를 보여줍니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

노드 및 링크 표현



엔터티 표현



조사 캔버스에서 기록 그룹화 또는 그룹 해제

그룹 기능을 사용하면 노드를 그룹화하여 더 쉽게 분석할 수 있습니다. 그룹화할 수 있는 노드 옆에 그룹화 버튼이 추가되었습니다. 기본적으로 이 버튼은 캔버스에 연결된 노드를 축소하거나 그룹화할 수 있음을 나타내는 빼기(–) 아이콘을 표시합니다.

모든 outdegree 노드는 그룹에 대해 고려됩니다.

주:
캔버스의 혼란을 줄이고 중요한 조사 중에 탐색을 단순화하기 위해 그룹 아이콘이 도입되었습니다. 추가 에지(연결)가 없는 노드의 경우 그룹화할 수 있는 관련 노드가 없으므로 그룹화 버튼이 표시되지 않습니다.

다음 표에서는 노드를 그룹화하거나 그룹을 해제하는 동안의 지침을 설명합니다.

작업	결과
노드 그룹화	• 부모가 하나뿐인 모든 하위 노드(여러 수준에 걸쳐 있더라도)는 그룹 내에서 숨겨집니다. • 상위 항목이 여러 개인 노드는 계속 표시되지만 그룹에서 해당 노드로의 연결은 숨겨집니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업	결과
노드 그룹 해제	• 한 상위 노드와 해당 연결이 있는 이전에 숨겨진 모든 노드를 표시합니다. • 여러 상위 항목이 있는 노드가 이미 표시된 경우 숨겨진 연결도 복원됩니다.
노드 임포트/관련 기록 가져오기	새 노드가 그룹 내의 숨겨진 노드에 연결되면 축소된 그룹을 자동으로 확장합니다.
허용된 작업	그룹화된 노드는 상위 노드의 상세 정보를 표시하는 상세 정보 표시 작업만 지원합니다. 다른 작업은 사용할 수 없습니다.
필터	그룹화되지 않은 노드를 필터링하는 것은 그룹화 규칙을 준수하면서 표준 필터링 동작을 따릅니다. 그룹화된 노드를 필터링하면 전체 그룹과 해당 하위 노드가 숨겨집니다.
기타 작업	노드 제거 또는 에지 수정과 같은 작업은 모든 그룹화 규칙 및 동작을 따릅니다.

조사 캔버스에서 기존 케이스 연결

이 섹션을 사용하여 조사 캔버스에서 기존 케이스를 연결합니다.

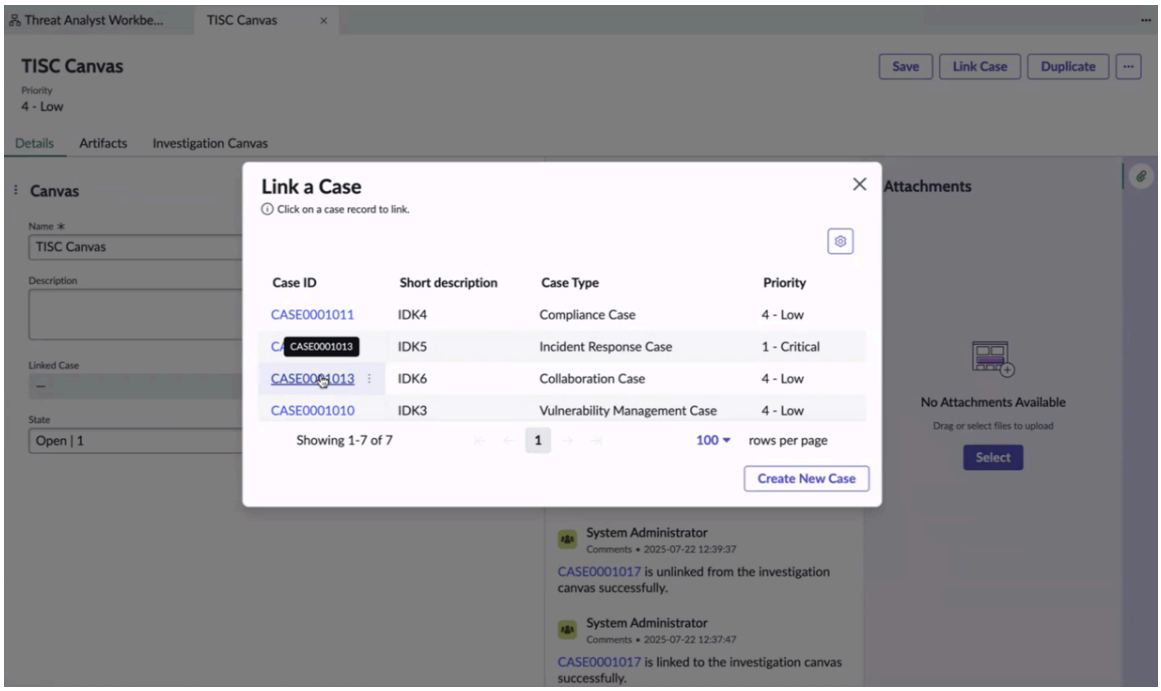
시작하기 전에

필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 위협 분석가 워크벤치 아이콘을 선택합니다.
3. 이동 케이스 관리 〉 모든 케이스.
   모든 케이스가 표시됩니다.
4. 선택 케이스 관리 〉 모든 케이스
5. 목록 뷰에서 케이스 기록을 엽니다.
6. 세부 정보 섹션에서 케이스 연결을 선택합니다.
   케이스 연결 대화 상자가 나타납니다.
7. 목록에서 케이스 ID를 선택하여 케이스를 조사 캔버스에 연결합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



케이스가 성공적으로 연결되었음을 확인하는 확인 메시지가 표시됩니다.

주:
조사 캔버스에 연결할 수 있는 케이스가 없는 경우 새 케이스를 생성하여 조사 컨텍스트를 시작하고 구성할 수 있습니다. 새 케이스를 만드는 방법에 대한 자세한 내용은 다음을 참조하십시오. 케이스 생성 및 조사 캔버스에서 연결

.

8. 연결된 케이스를 제거하려면 연결 해제 단추를 선택합니다.

관련 정보

조사 캔버스 생성

케이스 생성 및 조사 캔버스에서 연결

이 섹션을 사용하여 조사 캔버스에서 케이스를 생성하고 연결합니다.

시작하기 전에

필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 위협 분석가 워크벤치 아이콘을 선택합니다.
3. 이동 케이스 관리 〉 모든 케이스.
   모든 케이스가 표시됩니다.
4. 목록에서 케이스 기록을 엽니다.
5. 세부 정보 섹션에서 케이스 연결을 선택합니다.
   케이스 생성 및 연결 대화 상자가 나타납니다.
6. 목록에서 케이스를 선택하여 조사 캔버스에 케이스를 연결합니다.
7. 새 캔버스 만들기를 선택합니다.
   새 케이스 생성 대화 상자가 나타납니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

8. 적절하게 양식 필드를 채웁니다.

필드	설명
케이스 ID	케이스의 고유 식별자입니다. 시스템에서 생성된 ID입니다.
간단한 설명	조사 중인 요청이나 문제 또는 간단한 설명에 대한 요약입니다.
케이스 유형	조사 중인 케이스의 유형을 선택합니다. 조사에 사용할 수 있는 옵션은 다음과 같습니다. ○ 위협 헌팅 ○ 정보 요청 ○ 취약성 관리 케이스 ○ 규정 준수 케이스 ○ 인시던트 응답 케이스 ○ 공동 작업 케이스 ○ 기타
우선순위	케이스의 우선순위를 나타냅니다.
할당 그룹	케이스 작업을 담당하는 할당된 그룹입니다.
상태	케이스의 현재 상태입니다.
담당자	케이스 작업을 담당하는 분석가입니다.

9. 생성 및 연결을 선택하여 새 케이스를 만들고 조사 캔버스에 직접 연결합니다.

   케이스가 생성되어 조사 캔버스에 성공적으로 연결되었음을 확인하는 확인이 표시됩니다.

   주:
   이 옵션은 조사 캔버스와 연결된 기존 케이스가 없는 경우에 유용합니다.

10. 연결된 케이스를 제거하려면 연결 해제 단추를 선택합니다.
    기존 케이스를 조사 캔버스에 직접 연결하는 방법에 대한 자세한 내용은 문서를 참조하십시오 조사 캔버스에서 기존 케이스 연결.

관련 정보

조사 캔버스 생성

케이스에서 캔버스 연결

이 섹션을 사용하여 케이스에서 캔버스를 연결합니다.

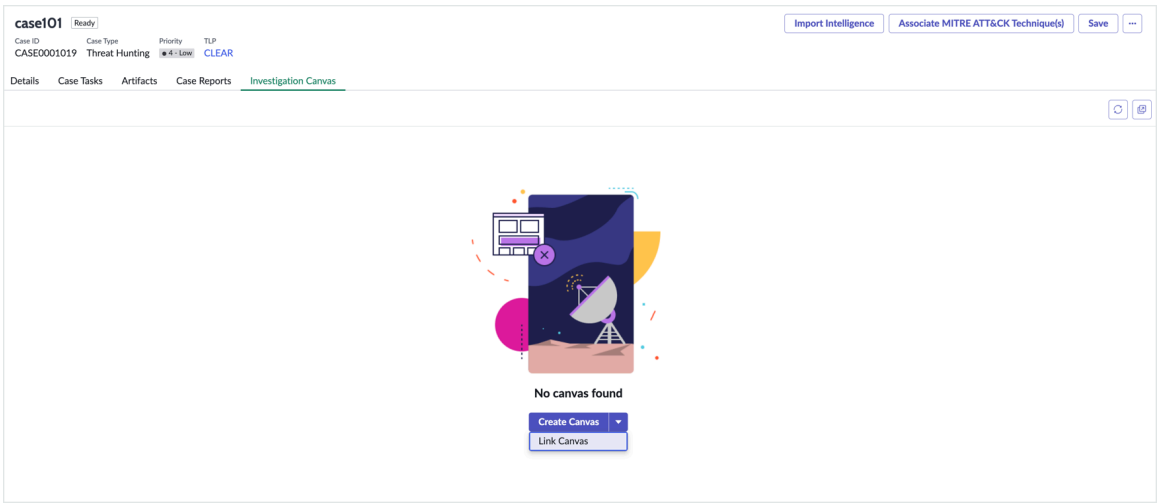
시작하기 전에
필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 위협 분석가 워크벤치 아이콘을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 이동 조사 캔버스 〉 모든 캔버스.
4. 모든 케이스 목록 뷰에서 캔버스에 연결되지 않은 케이스를 선택합니다.
5. 조사 캔버스 섹션으로 이동합니다.
6. 빈 캔버스 페이지의 드롭다운 목록에서 케이스 연결 을 선택합니다(옵션은 다음 스크린샷에 표시됨).



7. 캔버스를 선택합니다.
8. 링크 버튼을 선택하여 캔버스를 케이스에 연결합니다.

   캔버스 데이터가 성공적으로 새로 고침되었음을 나타내는 정보 메시지가 표시됩니다.

조사 캔버스 생성

위협 인텔리전스 라이브러리에서 옵저버블을 추가할 캔버스를 생성합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 위협 분석가 워크벤치 아이콘을 클릭합니다.
3. 이동 조사 캔버스 〉 모든 캔버스.
4. 새로 만들기를 클릭합니다.
5. 필드에 적절하게 입력합니다.

   새 캔버스 작성

필드	설명
이름	캔버스의 이름을 입력합니다.
설명	캔버스에 대한 설명을 추가합니다.
연결된 케이스	이 옵션은 연결된 캔버스가 없는 케이스 목록을 표시합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	이 필드는 각 케이스에 대해 연결된 캔버스가 있는지에 따라 동적으로 채워지므로 사용자가 생성 또는 연결된 조사 컨텍스트가 필요한 케이스를 쉽게 식별할 수 있습니다.
우선순위	캔버스의 우선순위를 선택합니다.
상태	캔버스의 상태를 선택합니다.

6. 저장을 클릭합니다.
   두 개의 새 섹션인 아티팩트 및 조사 캔버스가 표시됩니다. 새 캔버스를 만들 때 캔버스에는 노드가 포함되지 않습니다. 라이브러리에서 추가 옵션을 통해 위협 인텔리전스 라이브러리 또는 아티팩트에서 노드를 추가해야 합니다.
7. 조사 캔버스로 이동합니다.
8. 라이브러리에서 추가를 클릭합니다.

   주:
   노드를 추가하는 데 사용할 수 있는 두 가지 옵션이 있습니다. 임포트를 선택하여 모든 옵저버블을 임포트하거나 라이브러리에서 추가 옵션을 선택하여 위협 인텔리전스 라이브러리에서 옵저버블을 추가할 수 있습니다.

   Import node from Library 대화 상자가 표시됩니다.
9. 드롭다운 목록에서 노드 유형을 선택합니다.
   예를 들어 조사 캔버스에 옵저버블을 추가하는 경우 유형을 옵저버블로 선택합니다.
10. 필요한 옵저버블 수를 선택합니다.
11. 임포트를 클릭합니다.
    옵저버블을 임포트하면 노드가 조사 캔버스에 추가됩니다. 캔버스에 추가된 노드가 무엇이든 현재 캔버스에 일시적으로 추가되며 캔버스에 유지되지 않습니다.
12. 캔버스 저장을 선택합니다.
    노드 데이터를 캔버스로 처리하려면 데이터를 저장하여 영구적으로 보관해야 합니다.

    주:
    캔버스 저장 옵션을 수행하지 않으면 캔버스를 새로 고칠 때마다 데이터가 손실될 수 있습니다.

13. 라이브러리에 데이터 추가를 선택하여 서로 다른 두 노드 간에 새 관계를 생성합니다.
    두 노드 간의 관계는 노드가 일시적임을 의미하는 점선으로 표시됩니다. 노드 데이터를 관계로 이동하려면 라이브러리에 데이터 저장 및 라이브러리에 데이터 추가를 선택합니다. 이 작업을 수행하면 점선이 실선 모서리선으로 바뀌어 노드가 이제 라이브러리의 일부임을 나타냅니다.
14. 필터 아이콘을 사용하여 캔버스에 있는 옵저버블 및 객체 유형을 확인하고 조사 캔버스에 표시할 데이터 유형을 선택적으로 선택할 수 있습니다.
15. 또한 팝업 아이콘을 선택하여 더 큰 공간에 있는 조사 캔버스 노드에서 작업을 보거나 수행합니다.
16. 케이스 연결을 선택하여 조사 캔버스에 케이스를 연결합니다.
    a. 케이스 **ID**를 선택합니다.
    b. 링크 버튼을 클릭합니다.
17. 복제를 클릭하여 캔버스 내에서 캔버스 데이터와 노드를 복제합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관련 정보

조사 캔버스에서 작업

케이스에서 캔버스 연결

케이스 생성 및 조사 캔버스에서 연결

캔버스에 새 노드 추가

이 섹션을 사용하여 조사 캔버스에서 직접 옵저버블 또는 객체를 포함한 새 엔터티를 생성하고 추가합니다.

시작하기 전에
이 기능을 사용하면 현재 뷰에서 벗어날 필요 없이 캔버스를 빠르게 보강할 수 있습니다.

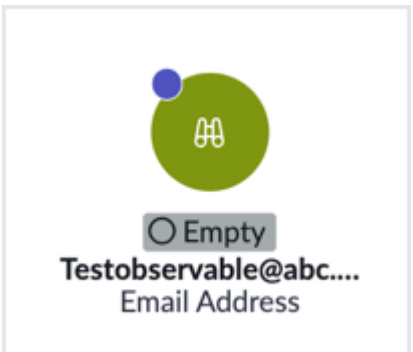
필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 위협 분석가 워크벤치 아이콘을 선택합니다.
3. 이동 케이스 관리 〉 모든 케이스.
4. 케이스 기록을 엽니다.

   주:
   케이스를 만들 때 캔버스를 만들거나 기존 캔버스를 연결해야 합니다. 연결 후에는 새 노드를 추가하는 옵션을 포함한 캔버스 작업을 사용자 인터페이스에서 자동으로 사용할 수 있습니다.

5. 선택 조사 캔버스 〉 새 노드.
   - 케이스의 빈조사 캔버스 섹션 드롭다운 목록에서 새 노드 기능을 볼 수도 있습니다.
   - 새 노드 기능을 보는 또 다른 옵션은 조사 캔버스 페이지에서 직접 보는 것입니다.
6. 노드를 생성하려면 적절한 엔터티 범주 및 엔터티 유형을 선택합니다.
7. 이름, 설명과 같은 필요한 객체 상세 정보를 입력합니다.
8. 추가를 선택하여 새 노드를 추가합니다.
   이 프로세스는 조사 캔버스에 노드를 자동으로 추가합니다.



새로 추가된 노드는 노드의 점 으로 시각적으로 구분되며, 라이브러리 또는 케이스 아티팩트를 통해 임포트된 노드와 구분됩니다.

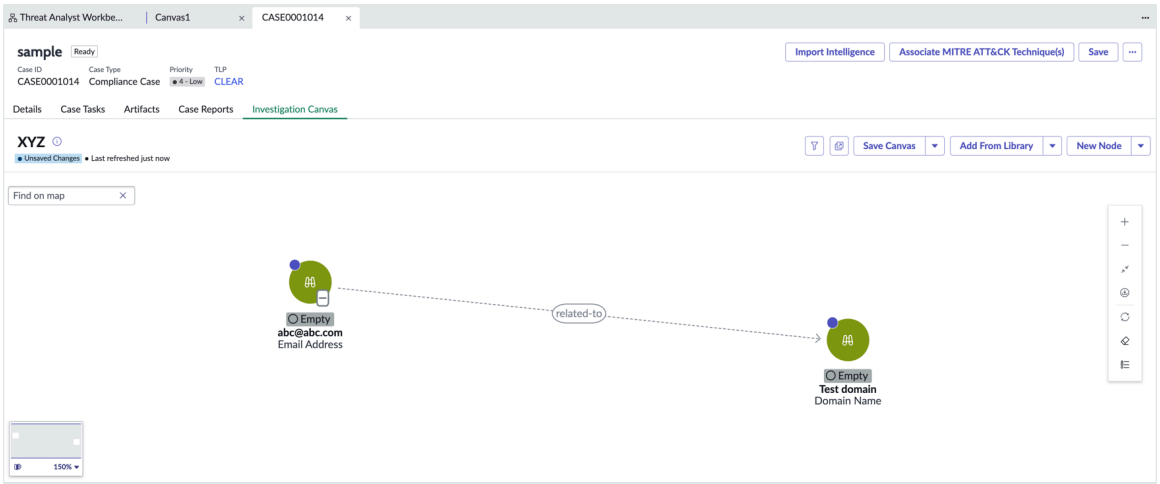
중요사항:
새로 추가된 노드는 일시적이며 위협 인텔리전스 라이브러리 또는 캔버스에 저장되지 않습니다. 저장하기 전에 캔버스를 새로 고치면 이러한 노드가 손실됩니다. 변경 사항을 유지하려면 새 노드를 추가한 후 캔버스를 저장해야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

9. 새 노드를 마우스 오른쪽 버튼으로 클릭하고 관계 추가 옵션을 선택하여 노드 간에 관계를 생성합니다.

   주:

   - 새 관계를 만들 때 에지는 점선으로 표시되어 임시 노드이며 위협 인텔리전스 라이브러리에 저장되지 않음을 나타냅니다.
   - 새로 추가된 에지는 일시적이며 위협 인텔리전스 라이브러리 또는 캔버스에 저장되지 않습니다. 저장하기 전에 캔버스를 새로 고치면 이러한 가장자리가 손실됩니다. 변경 사항을 유지하려면 새 모서리를 추가한 후 캔버스를 저장해야 합니다.



10. 마우스 오른쪽 버튼을 클릭하고 세부 정보 표시를 선택하여 선택한 엔터티와 관련된 세부 정보를 봅니다.

    주:
    데이터를 추가하려면 상세 정보 창 내의 하이퍼링크를 클릭하거나 기록 열기 옵션을 선택하고 필요한 노드 관련 데이터를 추가할 수 있습니다.

11. 라이브러리에 데이터 추가 옵션을 선택하여 조사 중에 일시적으로 추가된 모든 노드와 에지를 저장합니다.
    이 작업을 수행하면 임시 기록이 위협 인텔리전스 라이브러리 내의 영구 집계 기록으로 변환됩니다.

조사 캔버스 및 MITRE ATT&CK

조사 캔버스에서는 현재 캔버스에 있는 모든 노드와 관련된 MITRE ATT&CK 기술 및 하위 기술을 볼 수 있습니다.

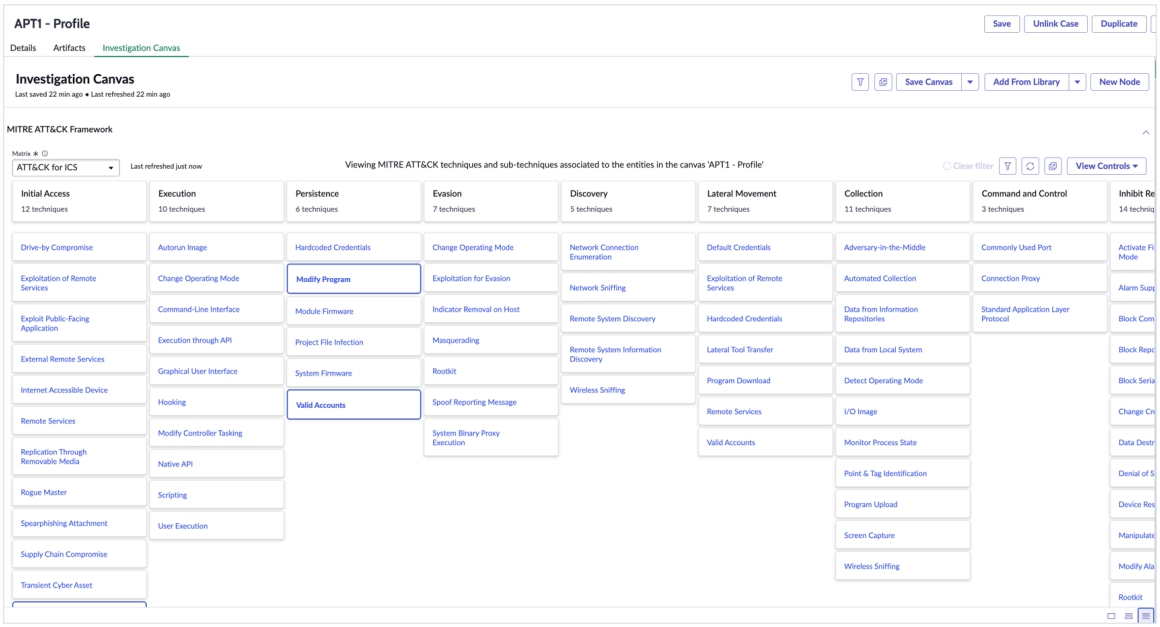
시작하기 전에
필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 위협 분석가 워크벤치 아이콘을 선택합니다.
3. 이동 케이스 관리 〉 모든 케이스.
4. 아무 케이스나 엽니다.
5. 조사 캔버스 탭으로 이동합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

6. 조사 캔버스에서 크기 조정 가능한 패널 구분선 핸들을 사용하여 끌어서 MITRE ATT&CK 프레임워크를 봅니다.
7. 매트릭스 드롭다운 목록에서 필요한 MITRE ATT&CK 매트릭스를 선택합니다.



MITRE ATT&CK 프레임워크는 다양한 수준의 전술 및 기술 연관성을 보여줍니다.

a. 맨 위 행에는 선택한 MITRE ATT&CK 매트릭스에 있는 모든 전술이 표시됩니다.

b. 기본적으로 각 방법에는 연결된 전체 기술 및 하위 기술의 수가 표시됩니다.

c. 새로 고침 아이콘을 사용하여 MITRE ATT&CK 프레임워크를 다시 로드하고 최신 기술-방법 연결을 봅니다.

d. 캔버스의 모든 노드(엔터티)와 관련된 MITRE ATT&CK 기술 및 하위 기술을 봅니다.

e. 하나 이상의 노드를 클릭하면 캔버스에서 선택한 노드와 관련된 관련 MITRE ATT&CK 기술 및 하위 기술을 볼 수 있습니다.

> **중요사항:**
> 프레임워크에서는 캔버스의 노드와 연결된 기술과 하위 기술이 강조 표시됩니다.

8. 필터를 선택하면 특정 악의적 사용자 및 기타 MITRE 기술 속성과 연결된 TTP에 대한 필터를 생성하고 저장할 수 있습니다.
MITRE 필터링 옵션에 대한 자세한 내용은 다음 문서를 참조하십시오 조사 캔버스 MITRE 필터.
9. 고급 필터링 옵션을 위해 뷰 컨트롤을 사용합니다.
적절한 필터를 선택하면 선택한 노드와 연결된 MITRE ATT&CK 기술 및 하위 기술만 표시됩니다.
통제 보기 목록의 옵션은 다음과 같습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- **ID** 표시: 고유한 기술 ID(예: T1059)를 쉽게 참조할 수 있도록 각 카드에 표시합니다.
- 하위 기술 표시: 하위 기술을 표시합니다. 이 옵션은 수동으로 확장할 필요 없이 상위 기술 카드를 자동으로 확장하여 하위 기술을 표시합니다.
- 연결된 기술만 표시 선택: 현재 조사 캔버스의 노드에 연결된 기술만 표시하며, 필터 기준을 충족하는 경우에도 관련 없는 기술을 숨깁니다. 이 옵션을 선택하면 각 방법에 현재 캔버스에 연결된 관련 기술 및 하위 기술의 총 수가 표시됩니다.

10. 팝업 아이콘을 클릭하면 더 넓은 공간에서 MITRE ATT&CK 프레임워크를 볼 수 있습니다.

중요사항:

- 노드를 추가하거나 제거할 때마다 MITRE ATT&CK 프레임워크가 자동으로 새로 고쳐집니다. 새로 고침 아이콘을 사용하여 언제든지 수동 새로 고침을 수행할 수도 있습니다.
- 특정 유형의 노드를 필터링할 때마다 MITRE ATT&CK 프레임워크가 자동으로 새로 고쳐져 변경 내용이 반영됩니다.

조사 캔버스 **MITRE** 필터

MITRE 필터를 사용하면 특정 악의적 사용자 및 기타 MITRE 기술 속성과 연결된 전술, 기술 및 절차(TTP)에 대한 필터를 생성하고 저장할 수 있습니다.

시작하기 전에

필요한 역할: sn_sec_tisc.analyst

이 태스크 정보

분석가는 MITRE 카드에서 사용할 수 있는 필터를 사용하여 조사에 관련된 악의적 사용자와 관련된 특정 액터 TTP를 필터링할 수 있습니다.

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.

2. 위협 분석가 워크벤치 아이콘을 선택합니다.

3. 이동 케이스 관리 〉 모든 케이스.

4. 아무 케이스나 엽니다.

5. 조사 캔버스 탭으로 이동합니다.

6. 필터를 선택하여 특정 악의적 및 기타 MITRE 기술 속성과 연결된 전술, 기술 및 절차(TTP)에 대한 필터를 생성합니다.

7. 필터 패널에 필요한 값을 입력하여 원하는 필터를 적용합니다.
MITRE 필터 패널을 사용하면 그룹, 맬웨어, 도구, 태그 및 우선 순위와 같은 선택한 기준에 따라 MITRE ATT&CK 기술을 필터링하고 시각화할 수 있습니다.

필드	설명
저장된 필터	분석가는 특정 기준을 저장된 필터 로 저장하여 재사용할 수 있습니다. 분석가가 저장한 필터는 사용자별로 다릅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

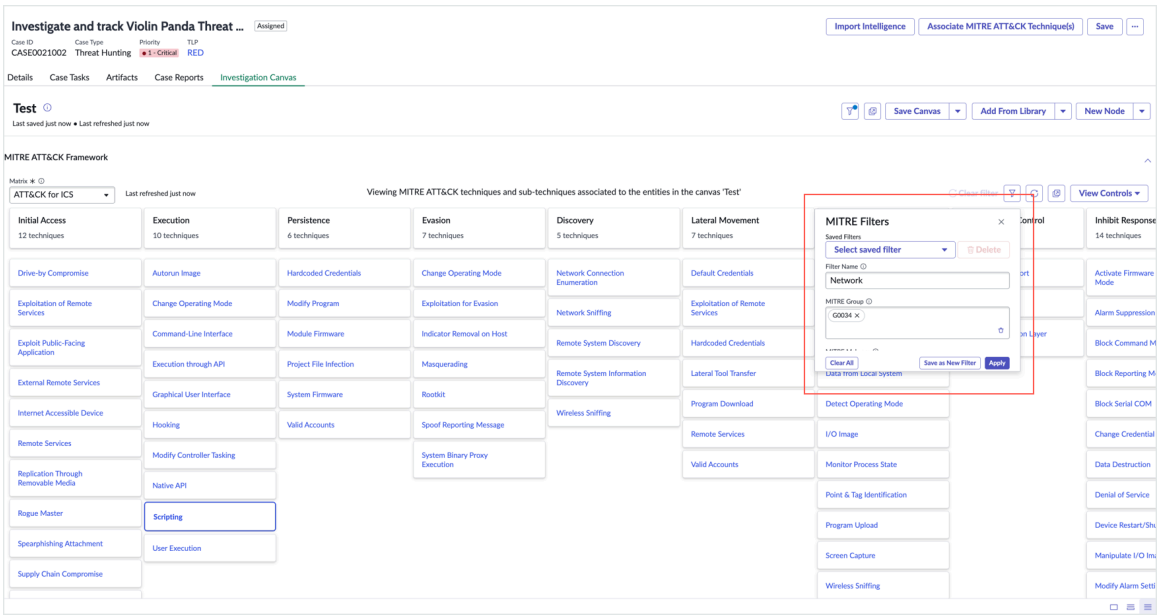
필드	설명
	주: 예를 들어 분석가 X가 필터 구성을 저장하면 분석가 X에게만 표시됩니다. 다른 분석가가 로그인하여 필터 드롭다운을 볼 때 다른 분석가가 저장한 필터는 볼 수 없습니다. 이렇게 하면 각 사용자가 다른 사용자의 필터 기본 설정에 영향을 주거나 영향을 받지 않고 개인화된 뷰를 만들고 관리할 수 있습니다.
필터 이름	필터의 이름입니다.
MITRE 그룹	MITRE 그룹을 나타냅니다. 하나 이상의 그룹을 선택하여 관련된 기술을 필터링합니다.
MITRE 맬웨어	MITRE 맬웨어를 나타냅니다. 하나 이상의 맬웨어 항목을 선택하여 관련된 기술을 필터링합니다.
MITRE 도구	MITRE 도구를 나타냅니다. 하나 이상의 도구를 선택하여 관련된 기술을 필터링합니다.
TISC 태그	태그를 TISC 나타냅니다. 하나 이상의 태그를 선택하여 분류에 따라 기술을 필터링합니다.
기술 우선순위	기술의 우선순위 수준을 나타냅니다. 하나 이상의 옵션을 선택하여 할당된 우선순위에 따라 기술을 필터링할 수 있습니다.
모두 지우기	필터 패널에 입력한 내용을 지울 수 있습니다.
새 필터로 저장	필터 패널에 입력된 기준을 새 저장된 필터로 저장합니다. 주: 저장된 필터 이름은 고유해야 합니다.
현재 필터 저장	기준에 대한 변경 사항을 현재 선택된 저장된 필터에 저장합니다. 이 옵션을 사용하여 필터 이름을 바꿀 수도 있습니다. 주: 저장된 필터 이름은 고유해야 합니다.
적용	이 옵션을 사용하면 MITRE 카드의 필터에 변경 내용을 적용할 수 있습니다.
삭제	선택한 저장된 필터를 제거하려면 이 옵션을 선택합니다. 저장된 필터 옆에 있는 삭제 버튼을 클릭하면 이 필터를 삭제할 것인지 확인하는 메시지가 나타납니다. 이 작업을 확인하면 저장된 필터가 영구적으로 제거됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	필터 패널 내에서 개별 필드 값을 제거하려면 해당 특정 필드 옆에 있는 삭제(휴지통) 아이콘을 클릭합니다.

이러한 값을 사용하여 필터를 적용하면 선택한 속성과 연결된 기술만 표시하도록 MITRE 매트릭스가 동적으로 업데이트됩니다. 이 집중적인 관점을 통해 분석가는 조사 중에 가장 관련성이 높은 전술, 기술 및 절차(TTP)에 더 집중할 수 있습니다.

또한 분석가는 멀웨어, 도구, 태그 및 우선순위 수준에 대한 필터를 사용하여 TTP의 범위를 더 좁힐 수 있습니다.

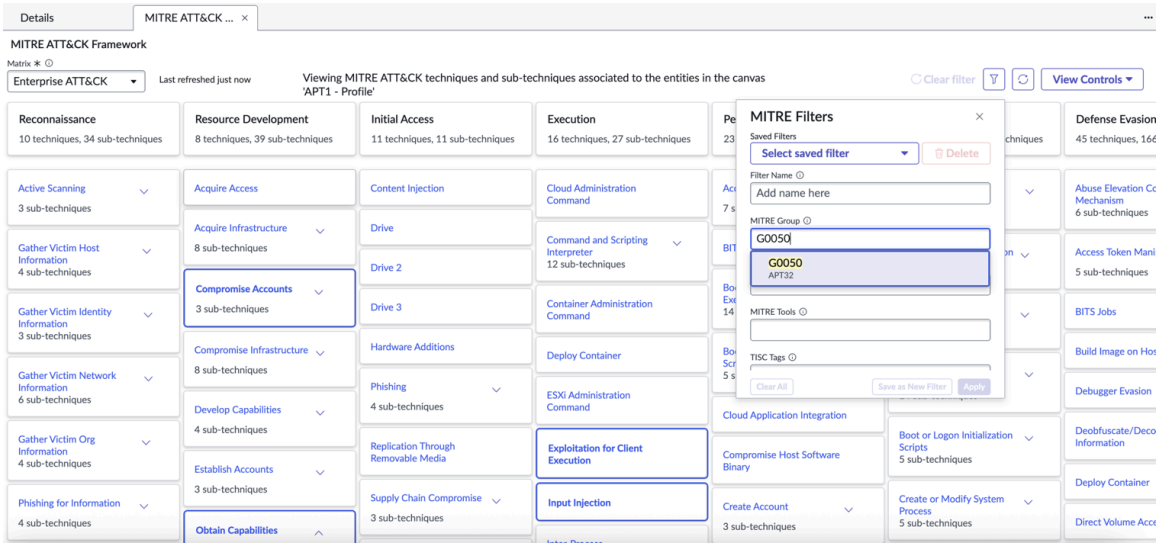


8. 옵션: 새 필터로 저장을 선택하여 필터 기준을 저장합니다.
9. 적용을 선택하여 변경 내용을 적용합니다.

Example: MITRE 그룹을 기준으로 필터링

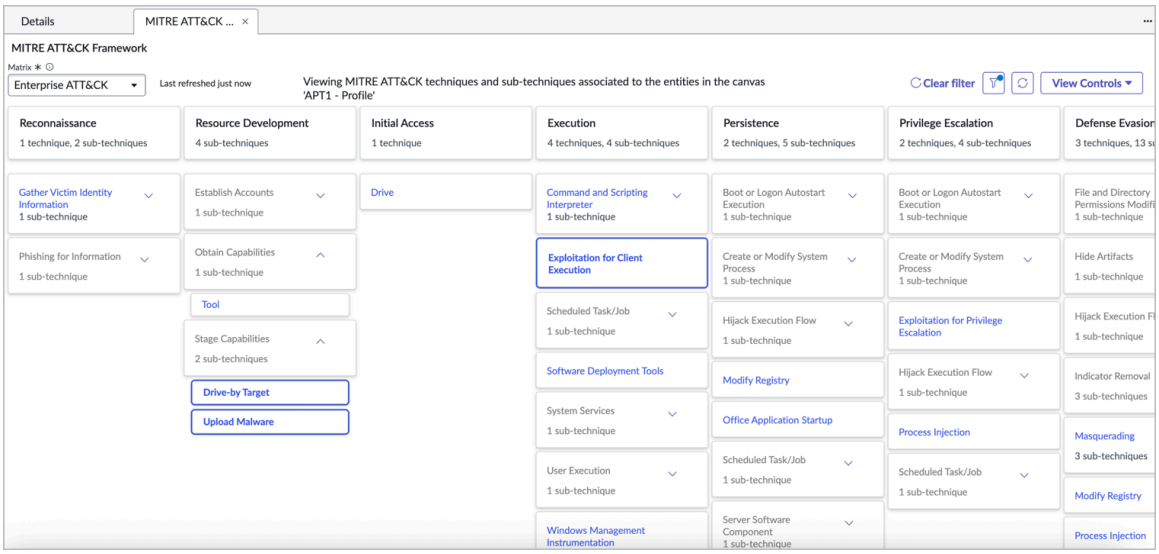
MITRE 그룹을 APT32로 선택합니다(G1001, 다음 스크린샷 참조). 이 필터를 적용하면 선택한 그룹에 직접 연결된 기술만 표시하도록 MITRE 매트릭스가 업데이트됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



이 포커스형 보기는 분석가가 선택한 위협 그룹과 관련된 전술, 기술 및 절차(TTP)에 특히 집중할 수 있도록 도와줍니다.

필터를 적용하면 매트릭스의 일부 기술은 파란색 텍스트로 표시되고 다른 기술은 회색으로 표시됩니다.



MITRE 프레임워크의 시각적 표현은 기술 및 하위 기술이 적용된 필터 및 조사 컨텍스트와 어떻게 관련되어 있는지를 나타냅니다.

- 파란색 텍스트: 파란색 텍스트로 표시된 기술 또는 하위 기술은 필터 기준과 일치하는 기술을 나타냅니다.
- 파란색 테두리가 있는 파란색 굵은 글씨: 파란색 테두리가 있는 굵은 파란색 텍스트로 표시되는 기술 또는 하위 기술은 필터 조건과 일치하고 캔버스에 있는 하나 이상의 노드와 연결된 기술 또는 하위 기술을 나타냅니다.
- 회색 카드: 상위 기술은 필터 기준과 직접 일치하지 않지만(선택한 그룹에 연결되지 않았음을 의미) 필터 조건과 일치하는 연결된 하위 기술과의 상위 관계를 나타내는 것으로 표시되는 경우 회색으로 표시됩니다.

케이스 또는 케이스 작업에 아티팩트 추가

케이스를 생성한 후에는 보안 인시던트, CI 및 손상 표시기와 같은 아티팩트를 보거나 케이스에 추가할 수 있습니다. 이러한 유물은 사건을 해결하는 데 단서 역할을 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: 관리자

주:
아티팩트는 기존 케이스에만 사용할 수 있습니다. 옵저버블 및 표시기의 경우 인텔리전스 임포트 버튼을 사용하여 임포트 작업에서 아티팩트를 추가하거나 케이스에 연결할 수도 있습니다. 임포트하는 방법에 대한 자세한 내용은 다음을 참조하십시오. 에서 인텔리전스 임포트 TISC

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 위협 분석가 워크벤치 아이콘을 클릭합니다.
3. 이동 케이스 관리 〉 모든 케이스.
   모든 케이스가 표시됩니다.
4. 케이스 또는 케이스 작업을 선택합니다.
5. 아티팩트 탭으로 이동합니다.
   연결된 아티팩트는 해당 특정 케이스 또는 케이스 작업에 대한 관련 목록으로 표시됩니다.
6. 케이스 또는 케이스 작업에서 기록을 연결하거나 연결 해제합니다.

주:
자세한 내용은 위협 인텔리전스 관련 기록 연결 문서를 참조하십시오.

다음 표에는 케이스 또는 케이스 작업과 관련된 아티팩트 관련 목록이 나열되어 있습니다.

관련 기록

관련 목록	설명
MITRE 기술	케이스와 관련된 MITRE 기술을 나열합니다. MITRE 기술은 케이스에 연결된 모든 기술도 표시합니다.
옵저버블	이 케이스 또는 케이스 작업과 관련된 옵저버블 목록입니다.
표시기	이 케이스 또는 케이스 작업과 관련된 표시기의 목록입니다.
공격 패턴	이 케이스 또는 케이스 작업과 관련된 공격 패턴의 목록입니다.
캠페인	이 케이스 또는 케이스 작업과 관련된 캠페인을 나열합니다.
작업 방침	이 케이스 또는 케이스 작업과 관련된 작업 과정을 나열합니다.
데이터 구성요소	이 케이스 또는 케이스 작업과 관련된 데이터 구성요소의 목록입니다.
위협 그룹화	이 케이스 또는 케이스 작업과 관련된 위협 그룹을 나열합니다.
ID	이 케이스 또는 케이스 작업과 관련된 ID를 나열합니다.
인프라	시스템, 소프트웨어 서비스 및 이 케이스 또는 케이스 작업과 관련된 관련된 물리적 또는 가상 자원과 같은 인프라를 나열합니다.
침입 세트	이 케이스 또는 케이스 작업과 관련된 공통 속성을 가진 일련의 적대적 행동 및 자원과 같은 침입 세트를 나열합니다.
위치	이 케이스 또는 케이스 작업과 관련된 위치 기록을 나열합니다.
맬웨어	이 케이스 또는 케이스 작업과 관련된 맬웨어 소스 기록을 나열합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관련 목록	설명
표시 정의	이 케이스 또는 케이스 작업과 관련된 표시 정의 기록을 나열합니다.
위협 메모	이 케이스 또는 케이스 작업과 관련된 표시 정의 기록을 나열합니다.
관찰 데이터	이 케이스 또는 케이스 작업과 관련된 관찰된 데이터를 나열합니다.
위협 의견	이 케이스 또는 케이스 작업과 관련된 위협 의견을 나열합니다.
위협 보고서	이 케이스 또는 케이스 작업과 관련된 위협 보고서를 나열합니다.
사이팅	이 케이스 또는 케이스 작업과 관련된 사이팅의 목록입니다.
위협 액터	이 케이스 또는 케이스 작업과 관련된 위협 행위자를 나열합니다.
도구	이 케이스 또는 케이스 작업과 관련된 도구를 나열합니다.
취약성	옵저버블이 IP 주소인 경우 이 목록에는 이 케이스 또는 케이스 작업과 관련된 일치하는 IP 주소가 있는 모든 자원(구성 항목)이 표시됩니다.
관련 케이스	관련 케이스를 나열합니다.
관련 케이스 작업	관련 케이스 작업을 나열합니다.
보안 인시던트	이 케이스 또는 케이스 작업과 관련된 보안 인시던트를 나열합니다.
영향을 받는 구성 항목	이 케이스 또는 케이스 작업과 관련된 영향을 받는 구성 항목을 나열합니다.
영향을 받는 서비스	이 케이스 또는 케이스 작업과 관련된 영향을 받는 서비스를 나열합니다.
영향을 받는 자산	이 케이스 또는 케이스 작업과 관련된 영향을 받는 자산을 나열합니다.
취약성 항목	이 케이스 또는 케이스 작업과 관련된 취약성 항목을 나열합니다.

아티팩트에서 케이스로 **MITRE** 기술 롤업

인텔리전스 기록이 케이스에 추가되면 연결된 모든 MITRE 기술이 케이스 수준으로 자동 롤업됩니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 위협 분석가 워크벤치 아이콘을 클릭합니다.
3. 이동 케이스 관리 〉 모든 케이스.
   모든 케이스가 표시됩니다.
4. 케이스를 선택합니다.
5. 아티팩트 탭으로 이동합니다.
   연결된 아티팩트가 해당 특정 케이스에 대한 관련 목록으로 표시됩니다.

케이스에 대한 **MITRE ATT&CK** 프레임워크 표시

MITRE ATT&CK 프레임워크에 케이스의 모든 관련 기술을 표시합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

이 태스크 정보
매트릭스 드롭다운 목록에서 필요한 MITRE ATT&CK 매트릭스를 선택합니다. MITRE ATT&CK 프레임워크는 다양한 수준의 전술 및 기술 연관성을 보여줍니다.

1. 맨 위 행에는 선택한 매트릭스에 있는 모든 전술이 표시됩니다. 기본적으로 모든 전술은 해당 전술에 대해 존재하는 전체 기술 및 하위 기술의 수를 표시합니다. 새로 고침 아이콘을 사용하여 MITRE ATT&CK 프레임워크를 다시 로드하고 최신 연결을 볼 수 있습니다.
2. 각 전술 아래에서 프레임워크는 해당 전술에 대한 관계로 존재하는 모든 기술을 표시합니다.
3. 프레임워크는 각 기술 아래에 있는 하위 기술을 표시합니다. 각 기술을 확장하여 하위 기술을 봅니다.

> **중요사항:**
> 프레임워크에서 케이스와 연결된 기술과 하위 기술이 강조 표시됩니다.

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 위협 분석가 워크벤치 아이콘을 클릭합니다.
3. 이동 케이스 관리 〉 모든 케이스.
   모든 케이스가 표시됩니다.
4. 케이스를 선택합니다.
5. 아티팩트 탭으로 이동합니다.
   연결된 아티팩트가 해당 특정 케이스에 대한 관련 목록으로 표시됩니다.
6. **MITRE ATT&CK** 프레임워크 표시 버튼 선택
   이 버튼을 선택하면 프레임워크가 MITRE ATT&CK에 케이스와 아티팩트의 모든 관련 기술을 표시합니다.
7. 확인하기로 선택한 MITRE 기술에서 케이스와 관련된 MITRE ATT&CK 기술 및 하위 기술을 봅니다.
8. 케이스와 관련된 MITRE ATT&CK 기술 및 하위 기술을 보려면 기록을 선택하십시오.
9. **View** Controls(보기 컨트롤)를 사용하여 view MITRE ATT&CK 기술 및 하위 기술을 원하는 대로 사용할 수 있습니다.
   통제 목록에서:
   - 기술 및 하위 기술 MITRE ID를 보려면 **ID** 표시를 선택합니다.
   - 모든 하위 기술을 보려면 하위 기술 표시를 선택합니다. 이 옵션을 선택하면 모든 기술이 확장된 보기에 표시됩니다. 기술의 확장된 보기에는 해당 기술에 대해 존재하는 모든 하위 기술이 표시됩니다.
   - 케이스와 연결된 MITRE 기술만 보려면 연결된 기술만 표시를 선택합니다. 이 옵션을 선택하면 각 방법에 연결된 기술 및 하위 기술의 총 수가 표시됩니다.

케이스 내에서 보강 작업 실행

이 섹션을 사용하여 케이스에서 강화 작업이 수행되는 방식을 이해합니다.

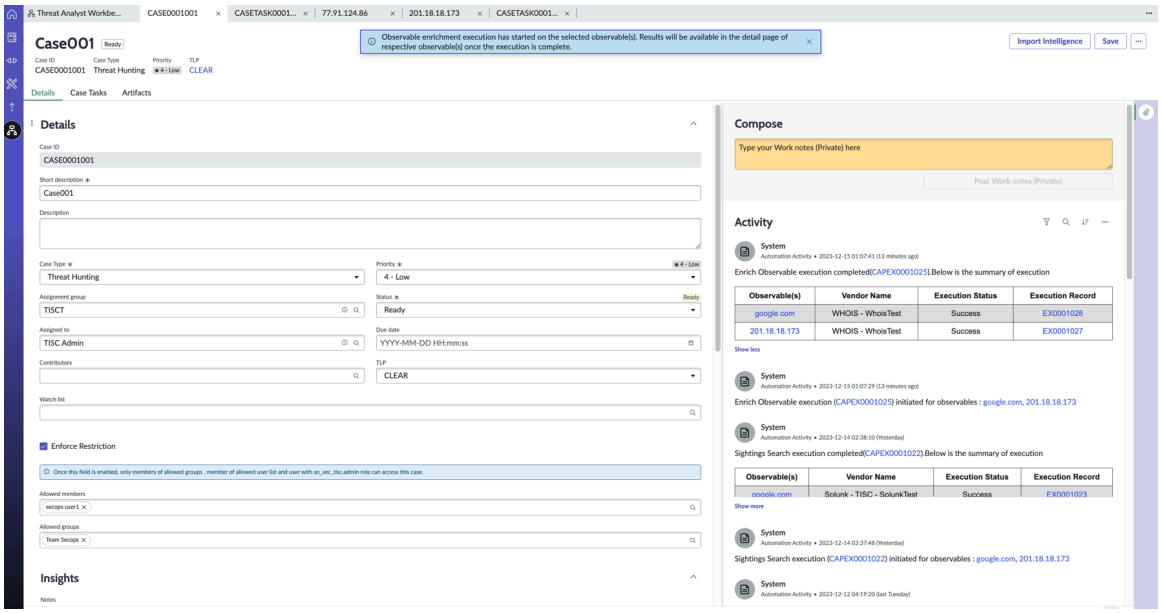
시작하기 전에
필요한 역할: sn_sec_tisc.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 위협 분석가 워크벤치 아이콘을 클릭합니다.
3. 이동 케이스 관리 〉 모든 케이스.
   모든 케이스가 표시됩니다.
4. 케이스 또는 케이스 작업을 선택합니다.
5. 아티팩트 탭으로 이동합니다.
6. 옵저버블 관련 목록을 선택합니다.
7. 옵저버블을 하나 더 선택하십시오.
8. 드롭다운 목록에서 보강 작업을 클릭합니다.
9. 사용 가능한 구현을 선택합니다.
10. 제출을 클릭합니다.
    예를 들어 위협 조회 실행입니다. 선택한 보강 작업이 실행되고 선택한 옵저버블에서 옵저버블 보강 실행이 시작되었다는 정보 메시지가 표시됩니다 . 실행이 완료되면 각 옵저버블의 상세 페이지에서 결과를 확인할 수 있습니다.

    주:
    실행이 시작되거나 완료되면 작업 메모가 양식 뷰의 활동 스트림에 게시됩니다.



케이스 보고서 보기

케이스 보고서 기능을 사용하여 케이스와 관련된 보고서를 생성합니다. 이러한 보고서에는 사후 조사 보고서 또는 핵심 요약 보고서가 포함됩니다.

시작하기 전에

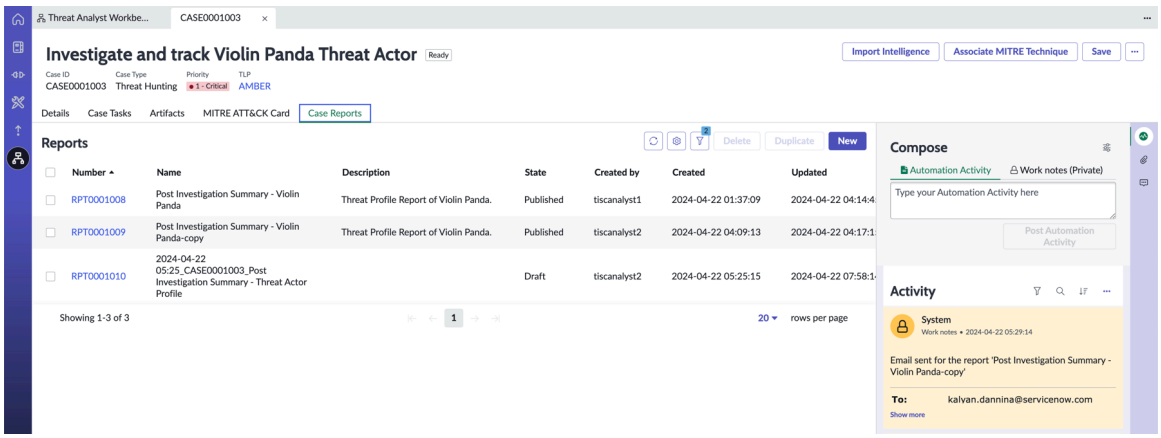
필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 위협 분석가 워크벤치 아이콘을 클릭합니다.

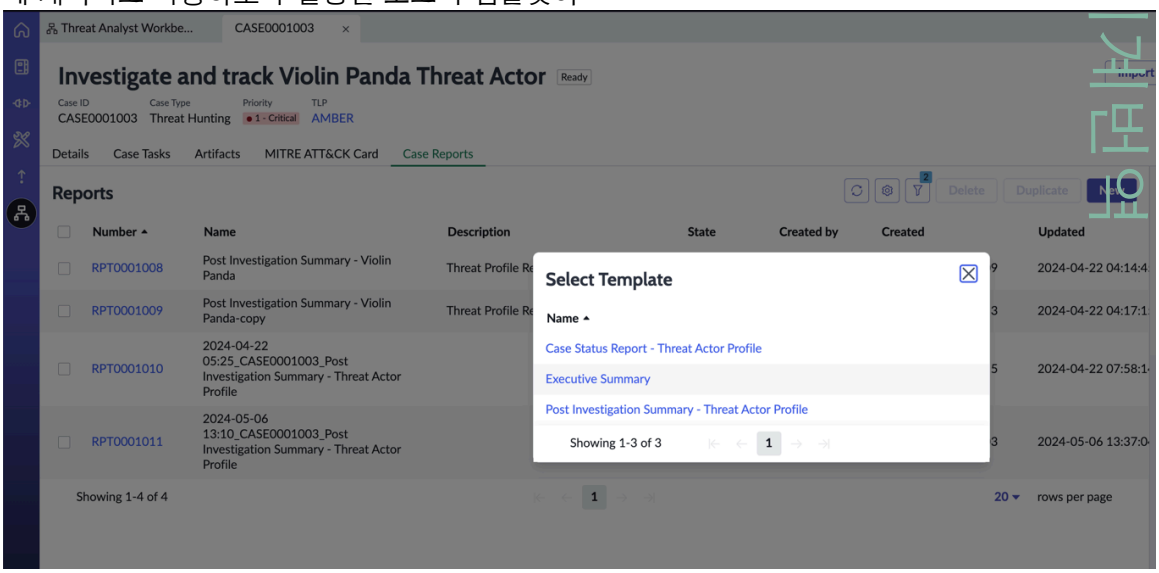
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 이동 케이스 관리 〉 모든 케이스.
   모든 케이스가 표시됩니다.
4. 케이스를 선택합니다.
5. 케이스 보고서로 이동합니다.



> 주:
> 목록에서 보고서를 삭제하고, 기존 보고서의 사본을 만들고, 고유한 보고서를 사용자 지정할 수 있습니다.

6. 새로 만들기를 클릭합니다.
   기본 시스템에 게시되고 사용하도록 설정된 보고서 템플릿이 표시됩니다.



7. 원하는 보고서 템플릿을 선택합니다.
   보고서 유형에 대해 선택한 보고서 템플릿이 생성됩니다. 또한 보고서가 게시되면 더 많은 사용자 그룹이 보고서를 볼 수 있지만 보고서가 초안 상태인 경우 해당 보고서가 사용자에게 숨겨집니다. 분석가는 게시된 보고서만 볼 수 있고 초안 상태의 보고서는 볼 수 없습니다.

> 주:
>
> - 필드를 더 추가하려면 필드를 선택하고 케이스 보고서 내에서 직접 추가하십시오.
> - 관련 목록(예: 옵저버블 목록)을 추가하려면 옵저버블을 선택합니다. 해당 케이스와 관련된 모든 옵저버블이 나열됩니다. 하나 이상의 옵저버블을 선택하고 추가를 클릭합니다. 필요한 옵저버블을 필터링하여 케이스에 추가할 수도 있습니다.

8. 내용 저장을 클릭하여 보고서의 내용을 저장합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

9. 미리 보기를 클릭하여 보고서를 미리 봅니다.

   주:
   다음과 같은 작업을 수행할 수 있습니다.
   - 보고서 창을 최대화합니다.
   - 다운로드 아이콘을 사용하여 보고서를 다운로드합니다.
   - 보고서의 높이나 크기가 더 나은 보기 환경을 제공하는 경우 새 탭에 보고서를 팝아웃합니다.
   - 보고서 이름 및 보고서 설명을 편집합니다.
   - 보고서를 게시합니다.

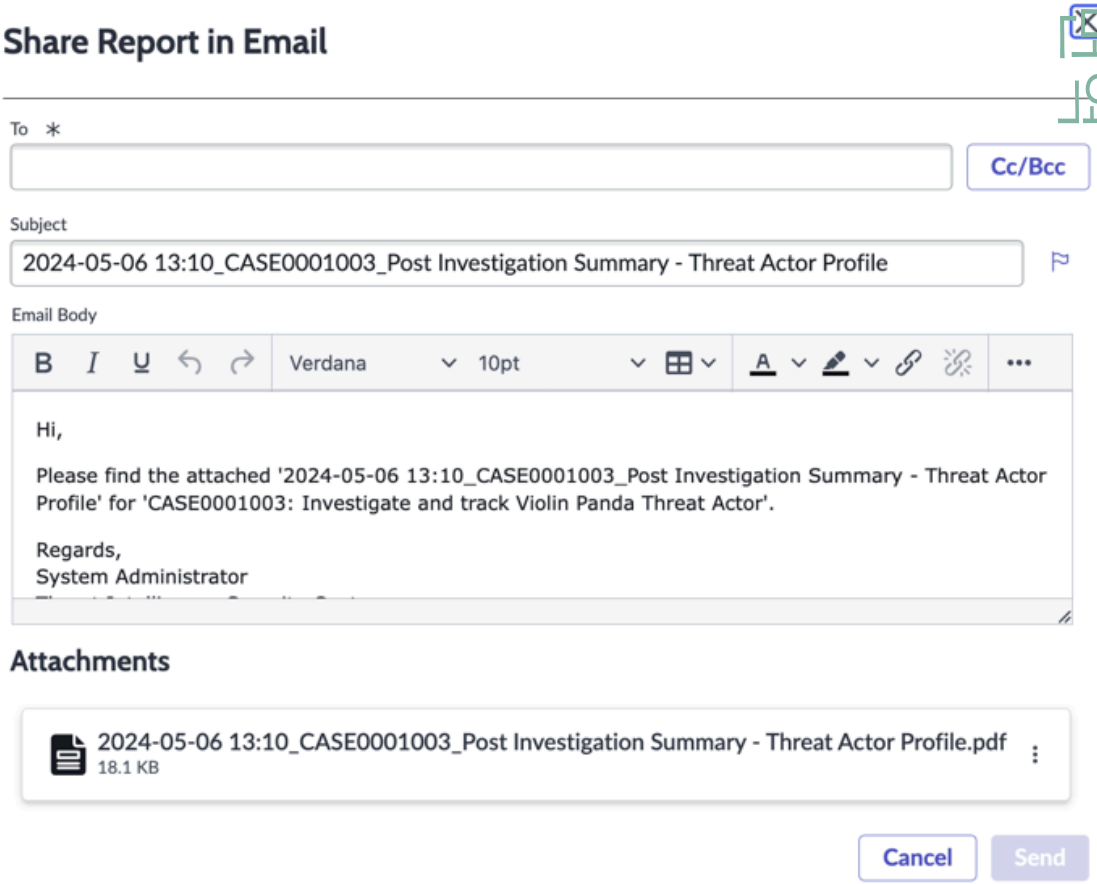
10. 보고서를 다시 게시하려면 컨텐츠 편집 버튼을 클릭합니다.

    주:
    보고서를 공유하라는 경고 메시지가 표시됩니다.

    보고서를 다운로드하거나 공유하려면 변경한 후 보고서를 다시 게시해야 합니다. 계속 편집하시겠습니까?

11. 편집을 클릭합니다.
    보고서를 편집하려면 설명된 대로 보고서 편집을 계속하거나 보고서를 게시할 수 있습니다. 일단 게시되면 보고서는 읽기 전용이 됩니다.

12. 이메일로 보고서 공유를 클릭하여 보고서를 공유합니다.
    보고서를 공유하는 동안 생성된 PDF 보고서는 이메일에 첨부 파일로



첨부됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

13. 받는 사람(보고서를 공유할 대상), 참조, 숨은 참조와 같은 필수 이메일 필드를 추가합니다.
14. 필요한 경우 이메일을 중요한 것으로 표시합니다.
15. 보내기를 클릭합니다.
    이 보고서는 더 많은 사용자 그룹과 공유됩니다.

케이스에서 TISC 보안 인시던트 만들기

보안 인시던트를 생성하고 옵저버블을 케이스의 TISC 보안 인시던트에 연결합니다.

시작하기 전에

필요한 역할: sn_si_basic

프로시저

1. 다음으로 이동 모두 〉 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 위협 분석가 워크벤치 아이콘을 클릭합니다.
3. 이동 케이스 관리 〉 모든 케이스.
   모든 케이스가 표시됩니다.
4. 아무 케이스나 엽니다.
5. 보안 인시던트 생성 버튼을 클릭합니다.

   주:
   케이스 관리 워크벤치에서 보안 인시던트 생성 버튼은 오픈 케이스 기록에 대해서만 활성화되고 종결된 케이스 기록에 대해서는 비활성화됩니다.

   보안 인시던트 생성 대화 상자가 표시됩니다.
6. 적절한 인시던트 상세 정보로 폼을 작성합니다.

   자세한 내용 추가

필드	설명
간단한 설명	보안 인시던트에 대한 간단한 설명을 입력합니다.
설명	보안 인시던트에 대한 설명을 입력합니다.
범주	보안 인시던트의 분류를 정의합니다.
우선순위	보안 인시던트의 우선순위를 정의합니다.
하위 범주	범주에 따라 보안 인시던트의 하위 분류를 정의합니다.
할당 그룹	보안 인시던트를 할당할 할당 그룹을 지정합니다.
상위	이 작업이 트리거되는 케이스인 TISC 상위 보안 인시던트를 나타냅니다.

7. 다음을 클릭하여 계속합니다.

   주:
   모든 필수 필드를 입력해야 합니다. 모든 필수 필드를 입력할 때까지 다음 버튼은 비활성화된 상태로 유지됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

8. 케이스와 연결된 옵저버블을 TISC 선택하여 보안 인시던트에 연결한 후 다음을 클릭하여 계속 진행합니다
9. 새로 생성된 보안 인시던트와 연결될 보안 인시던트 상세 정보 및 옵저버블을 검토한 다음 생성을 클릭하여 계속 진행하고 보안 인시던트를 생성합니다.

   주:
   보안 인시던트가 생성되었음을 나타내는 확인 메시지가 보안 인시던트에 대한 링크와 함께 표시됩니다. 이 링크를 클릭하면 의 보안 인시던트 보안 인시던트 응답 작업 공간로 이동합니다.

   보안 인시던트가 생성되면 케이스의 TISC 아티팩트 탭으로 리디렉션됩니다.
10. TISC 아티팩트 탭 아래의 보안 인시던트 섹션으로 이동하여 인시던트를 확인합니다.

    주:
    또한 케이스 활동 스트림에는 TISC 옵저버블과 TISC 연결된 보안 인시던트(보안 인시던트 번호)가 생성되었음을 나타내는 작업 메모가 게시됩니다. 이 작업 메모에는 옵저버블 유형 및 옵저버블 값과 같은 상세 정보가 포함됩니다.

    보안 인시던트 양식에서 보안 인시던트 응답 작업 공간다음을 수행합니다.

    - 보안 인시던트가 케이스에서 TISC 성공적으로 생성되었음을 나타내는 작업 메모가 활동 스트림에 게시됩니다. 이 작업 메모에는 선택한 옵저버블이 보안 인시던트와 연결되었음을 확인하는 케이스에 대한 TISC 링크도 포함되어 있습니다.
    - 또한 의 관련 기록 탭에 액세스하고 아래의 옵저버블 항목을 검토하여 이를 확인할 수도 있습니다.보안 인시던트 응답 작업 공간 위협 인텔리전스 〉 연결된 옵저버블. **TISC** 컨텍스트 섹션에서 연결된 옵저버블을 볼 수도 있습니다. 이러한 옵저버블이 에서 직접 연결 TISC되었음을 알 수 있습니다.

보안 첨부 파일 업로드

이 섹션을 사용하여 보안 첨부 파일을 케이스에 업로드하는 방법에 대해 알아봅니다.

시작하기 전에

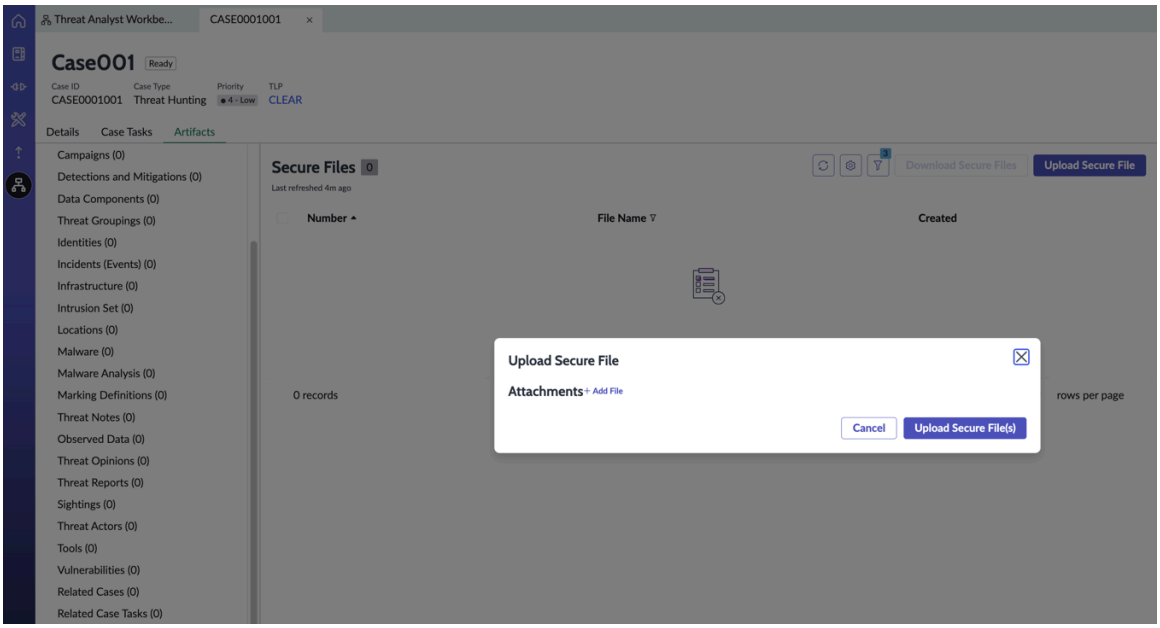
필요한 역할: sn_sec_tisc_secure_file_access, sn_sec_tiscadmin

주:
보안 파일 관련 목록은 사용자 역할 sn_sec_tisc.secure_file_access가 있는 경우에만 표시됩니다.

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 위협 분석가 워크벤치 아이콘을 클릭합니다.
3. 이동 케이스 관리 〉 모든 케이스.
   모든 케이스가 표시됩니다.
4. 케이스를 선택합니다.
5. 이동 아티팩트 〉 보안 파일 관련 목록.
6. **Upload Secure** File(보안 파일 업로드) 버튼을 클릭합니다.
7. 파일 추가를 클릭하여 첨부 파일을 추가합니다.
8. 파일을 선택하고 **Upload Secure File(s)**(보안 파일 업로드) 버튼을 클릭합니다.
   파일 첨부 파일이 업로드됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



9. 보안 파일 다운로드를 클릭하여 첨부 파일을 다운로드합니다.
   첨부 파일은 zip 형식으로 제공됩니다.
10. 또는 보안 파일 기록의 상세 페이지로 이동하여 파일을 다운로드할 수 있습니다.

주:

- 모든 보안 첨부 파일은 키 관리 프레임워크(KMF)를 사용하여 암호화되어 시스템에 저장됩니다. 자세한 내용은 첨부 파일 암호화를 참조하십시오.
- *ServiceNow ## ##* 사용자가 **Professional Pack Installer**를 구독하는 경우 보안 파일이 zip 형식으로 압축되고 암호화되어 저장됩니다

위협 인텔리전스 보안 센터 도서관

위협 라이브러리는 구조화된 보안 위협 정보와 구조화되지 않은 보안 위협 정보를 조직에 제공하는 조직화된 개체 및 엔터티의 그룹으로 정의됩니다.

위협 정보는 피드 형태로 제공됩니다. 피드는 위협 인텔리전스 엔터티를 나열하는 STIX, MISP 등의 소스에서 귀중한 위협 데이터를 제공합니다.

위협 인텔리전스 보안 센터 라이브러리에서는 기본 및 고급 검색을 수행하고 규칙을 필터링하고, 임포트 도우미를 호출하고, 위협 인텔리전스 기록을 수동으로 추가하고, 허용 목록, 거부 목록 및 감시 목록에 추가하는 등 필요한 작업을 수행하여 데이터를 탐색하는 방법을 설명합니다.

상세 정보 뷰는 인텔리전스 기록에 대한 인사이트를 제공하며 목록 뷰에서 하나 이상의 기록에 대해 빠른 작업을 수행할 수 있습니다.

데이터 모델 이해

위협 인텔리전스 보안 센터 모듈의 데이터 모델 및 아키텍처는 위협 인텔리전스 플랫폼 기능과 위협 분석가에게 자세한 데이터를 제공하는 다양한 보안 뷰를 지원하도록 설계되었습니다.

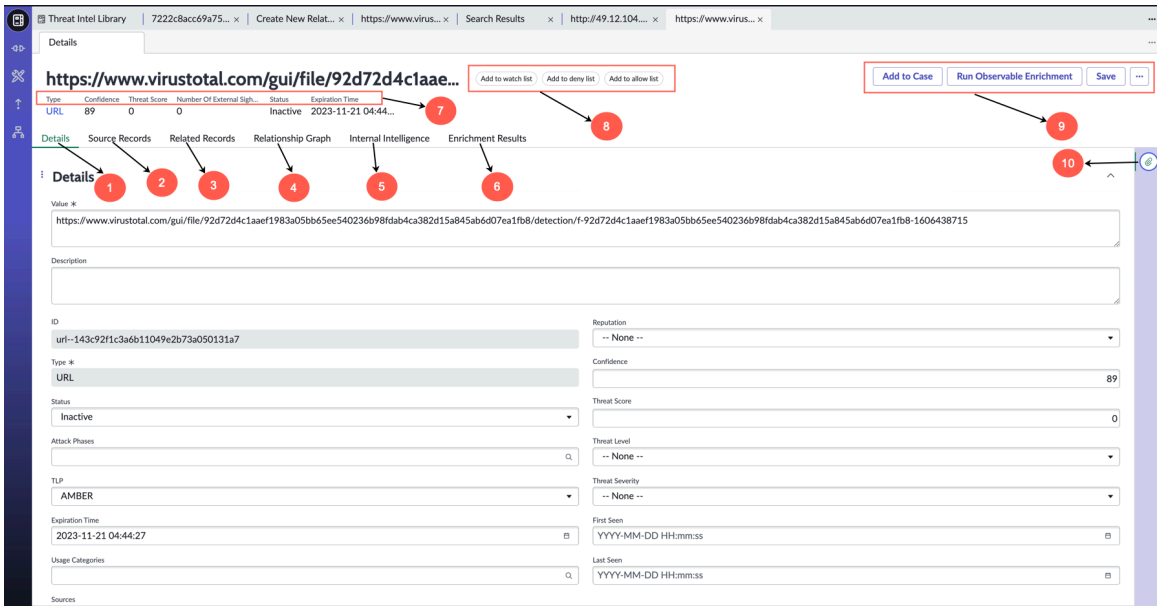
데이터 모델에는 위협 인텔리전스 리포지토리에서 객체로 표현되는 데이터 구조가 있습니다.

TISC 라이브러리 객체 양식 뷰

개체 홈페이지는 위협 인텔리전스 보안 센터 다음 기능으로 구성됩니다.

다음 섹션을 사용하거나 탐색하고 각 SDO에 대해 자세히 알아보십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



TISC 라이브러리 객체 양식 뷰

순서	메뉴/탭	설명
1	상세 정보 탭	이 섹션을 사용하여 양식 뷰에서 SDO를 보거나 편집합니다.
2	소스 기록 탭	소스 기록은 양식 뷰에 표시된 대로 집계된 기록에 기여합니다. 이러한 소스 기록은 피드에서 자동으로 생성되거나 사용자가 수동으로 생성합니다.
3	관련 기록 탭	SDO와 연관된 모든 관련 기록을 나열합니다.
4	관계 그래프 탭	관련 객체의 시각적 표현입니다.
5	내부 인텔리전스 탭	관련 객체의 내부 인텔리전스 기록을 나열합니다.
6	보강 결과 탭	개체와 연결된 보강 통합을 나열합니다.
7	양식 배너	유형, 신뢰도, 위협 점수, 사이팅 수, 상태 및 만료 시간과 같은 주요 필드가 포함된 읽기 전용 섹션입니다.
8	양식 배너 **UI** 작업	허용 목록에 추가하거나, 허용 목록(거부 목록)에서 제거하거나, 옵저버블에 따라 감시 목록에 추가해야 하는 경우 클릭할 수 있는 보안 제어 목록입니다. 클릭하여 다음을 수행합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

TISC 라이브러리 객체 양식 뷰

순서	메뉴/탭	설명
		• 감시 목록에 추가 • 거부 목록에 추가 • 허용 목록에 추가 주: 양식 작업은 옵저버블에만 적용할 수 있습니다.
9	양식 **UI** 작업	사용 가능한 양식 UI 작업은 다음과 같습니다. **1.** 케이스에 추가: 케이스에 개체를 추가합니다. **2.** 옵저버블 보강 실행: 선택한 개체에 대한 보강을 실행합니다. **3.** 저장: 기록을 저장합니다. **4.** 삭제: 기록을 삭제합니다.
10	오른쪽 상황별 메뉴	해당 객체와 연결된 작업에 따라 첨부 파일, 메모 등과 같은 빠른 제어에 쉽게 액세스할 수 있습니다. 이 옵션은 위협 분석가가 필요할 때마다 액세스할 수 있도록 나머지 두 탭에서 사용할 수 있습니다. 상황별 메뉴를 사용하면 다음 작업을 쉽게 탐색할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

TISC 라이브러리 객체 양식 뷰

순서	메뉴/탭	설명
		1. 첨부 파일: 개체와 관련된 모든 파일을 첨부합니다. 주: 새 옵저버블, 표시기 또는 객체를 만들거나 기존 객체를 볼 때마다 첨부 파일 창이 기본적으로 해당 양식 뷰에 표시됩니다. 오른쪽 상황별 메뉴에서 첨부 파일 아이콘을 클릭하거나 기본 설정 〉 작업 공간 을 클릭하고 사이드바 표시를 비활성화합니다. 자세한 내용은 Next Experience Workspace 기본 설정 구성을 참조하십시오. **2.** 인사이트: 해당 객체와 연결된 옵저버블 또는 표시기와 관련된 추가 정보를 추가합니다.
해당 사항 없음	탐색기에서 검색	이 검색 기능을 사용하여 TI(Threat Intel) 라이브러리 내에서 다양한 객체를 검색합니다. 예를 들어 TI 라이브러리 모듈 내에서 모든 옵저버블 기록을 검색할 수 있습니다.
해당 사항 없음	위협 인텔 라이브러리에서 검색	이 검색 기능을 사용하여 검색 기준에 따라 여러 소스에서 소스 기록을 검색합니다. 결과는 별도의 검색 결과 탭에 표시됩니다. 예를 들어 IP 주소 104.227.137.35의 경우 104.*를 입력하여 레코드를 검색하면 레코드 범위가 좁아지고 별도의 검색 결과 탭에 104로 시작하는 IP 주소가 포함된 레코드가 표시됩니다. • 위협 라이브러리 페이지로 돌아가지 않고 동일한 검색 결과 페이지의 검색 기준에서 기존 검색 키워드를 수정할 수도 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

TISC 라이브러리 객체 양식 뷰

순서	메뉴/탭	설명
		• 마찬가지로 특정 기록의 이름과 설명을 기준으로 검색할 수도 있습니다. • 기록이 필터링되고 나열되면 목록 뷰를 클릭하면 새 탭에서 해당 기록으로 이동합니다.

TISC 라이브러리 리포지토리

IoC 저장소에는 STIX 개체가 포함되어 있으며 이러한 각 개체에는 특정 정보가 포함되어 있습니다.

옵저버블

옵저버블은 컴퓨터 및 네트워크 작동과 관련된 상태 저장 속성(예: 파일의 MD5 해시 또는 레지스트리 키 값) 또는 측정 가능한 이벤트(예: 레지스트리 키 만들기 또는 파일 삭제)를 나타냅니다.

애플리케이션에서 사용할 수 있는 옵저버블의 유형은 다음과 같습니다.

- 아티팩트
- AS 번호
- 디렉터리
- 도메인 이름
- 이메일 주소
- 이메일 메시지
- 이메일 제목
- 파일
- IPv4 주소
- IPv4 CIDR
- IPv6 주소
- IPv6 CIDR
- MAC 주소
- MD5 해시
- 뮤텍스 이름
- 네트워크
- 기타 옵저버블
- 프로세스
- SHA1 해시
- SHA256 해시
- SHA512 해시
- 소프트웨어

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- URL
- 사용자 계정
- Windows 레지스트리 키
- X.509 인증서

옵저버블 정의

옵저버블은 예약된 피드 수집 또는 임포트 도우미에서 검색할 수 있습니다. 그러나 필요한 경우 옵저버블을 생성할 수 있습니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터 〉 위협 인텔 라이브러리 〉 옵저버블 〉 모든 옵저버블.
2. 새로 만들기를 클릭합니다.
3. 옵저버블 유형을 선택합니다.
   새 옵저버블 기록 생성 양식이 표시됩니다.

   주:
   옵저버블, 표시기, 엔터티 또는 객체에 대한 새 객체 기록을 생성할 때마다 소스 기록이 생성되고, 새 객체 기록이 생성된 다음 사용자가 집계된 기록으로 리디렉션된다는 프롬프트 메시지가 표시됩니다.

4. 양식에서 필드를 채웁니다.

   주:
   새 옵저버블을 만들거나 기존 옵저버블을 볼 때마다 첨부 파일 창이 기본적으로 양식 뷰에 표시됩니다. 오른쪽 상황별 메뉴에서 첨부 파일 아이콘을 클릭하거나 기본 설정 〉 작업 공간을 클릭하고 사이드바 표시를 비활성화합니다. 자세한 내용은 Next Experience Workspace 기본 설정 구성을 참조하십시오.

상세 정보 섹션

필드	설명
값	옵저버블과 연결된 값(예: IP 주소 또는 해시)입니다.
설명	옵저버블 기록에 대한 설명입니다.
작성자	이름을 입력합니다.
유형	IP 주소, 도메인 이름, 아티팩트, 디렉터리, 파일 또는 해시와 같은 옵저버블 분류 유형입니다. 기본적으로 새 기록을 선택하면 표시됩니다.
상태	옵저버블의 활성 또는 비활성 상태입니다.
공격 단계	LM, MITRE ATT&CK와 같은 킬 체인의 공격 단계를 나타냅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
TLP	TLP별 데이터 민감도 설정을 나타내는 고유 값입니다.
평판	옵저버블의 악의적인 평판을 지정합니다.
상태	활성 또는 비활성인 경우 옵저버블의 상태를 입력합니다.
위협 점수	해당 옵저버블에 대한 위협 점수를 나타냅니다.
만료 시간	옵저버블 기록의 만료 시간을 지정합니다.
소스	이 기록이 생성되는 위협 소스를 지정합니다.
신뢰도	이 옵저버블 기록에 대한 신뢰도를 입력합니다. confidence 속성은 작성자가 데이터의 정확성에 대해 가지고 있는 신뢰도를 식별합니다. 신뢰도 값은 0-100 범위의 숫자여야 합니다(MUST).
시스템 업데이트 방지	이 플래그를 예로 설정하면 시스템이 기록의 필드 값을 재정의할 수 없습니다.
긍정 오류 여부	옵저버블이 긍정 오류로 식별되는지 여부를 나타내는 부울 플래그입니다.

속성

필드	설명
해결 대상	도메인 이름이 확인되는 하나 이상의 IP 주소 또는 도메인 이름에 대한 참조 목록을 지정합니다.
FQDN 여부	FQDN(정규화된 도메인 이름)은 인터넷 호스트 또는 컴퓨터의 전체 주소입니다. 호스트 이름, 도메인 이름 및 TLD(최상위 도메인)를 지정하여 DNS(Domain Name System) 내의 정확한 위치를 제공합니다.

추가 정보

필드	설명
위협 수준	옵저버블 기록의 위협 수준을 나타냅니다.
처음으로 발견됨	이 옵저버블 기록이 악의적인 활동을 수행하는 것이 처음 목격된 시간입니다.
위협 심각성	옵저버블 기록의 위협 심각도를 나타냅니다.
마지막으로 발견됨	이 옵저버블 기록이 악의적인 활동을 수행하는 것이 마지막으로 목격된 시간입니다.
사용 범주	옵저버블이 속하는 범주(예: 봇넷 또는 피싱)입니다.
공격 단계	LM, MITRE ATT&CK와 같은 킬 체인의 공격 단계를 나타냅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
추가 컨텍스트	추가 컨텍스트를 추가합니다.
소스	이 기록이 생성되는 위협 소스를 지정합니다.

중요사항:
소스 보고된 점수: 이 필드에는 옵저버블이 수집되는 소스에서 보고한 위협 점수의 집계 값이 포함됩니다. 옵저버블 기록 양식에서 이 필드를 보려면 기본적으로 사용할 수 없으므로 수동으로 추가해야 합니다.

속성

필드	설명
해결 대상	도메인 이름이 확인되는 하나 이상의 IP 주소 또는 도메인 이름에 대한 참조 목록을 지정합니다.
FQDN 여부	FQDN(정규화된 도메인 이름)은 인터넷 호스트 또는 컴퓨터의 전체 주소입니다. 호스트 이름, 도메인 이름 및 TLD(최상위 도메인)를 지정하여 DNS(Domain Name System) 내의 정확한 위치를 제공합니다.

주:
Resolves To 및 **Is FQDN** 속성은 옵저버블의 도메인 이름 유형에만 적용할 수 있습니다.

옵저버블 유형 속성

특성 이름	속성 유형
아티팩트	○ 복호화 키 ○ 암호화 알고리즘 ○ MD5 해시 ○ MIME 형식 ○ SHA1 해시 ○ SHA256 해시 ○ SHA512 해시 ○ URL
AS 번호	○ 이름 ○ RIR
디렉터리	○ 디렉터리 생성 시간 ○ 디렉터리에 마지막으로 접근한 시간 ○ 디렉터리를 마지막으로 수정한 시간 ○ 인코딩된 경로
도메인 이름	○ FQDN 여부 ○ 해결 대상

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

특성 이름	속성 유형
이메일 주소	○ 표시 이름 ○ 이메일 본문 ○ 이메일 받는 사람 Bcc ○ 이메일 받는 사람 Cc ○ 이메일 받는 사람 To ○ 이메일 발신자 ○ 이메일 제목 ○ 보낸 날짜
파일	○ 추가 정보 ○ 인코딩된 파일 이름 ○ 파일 생성 시간 ○ 파일에 마지막으로 접근한 시간 ○ 파일을 마지막으로 수정한 시간 ○ 파일 이름 마법수 ○ MD5 해시 ○ MIME 형식 ○ SHA1 해시 ○ SHA256 해시 ○ SHA512 해시
IPv4 주소	○ AS 번호 ○ MAC 주소
IPv4 CIDR	○ AS 번호 ○ MAC 주소
IPv6 주소	○ AS 번호 ○ MAC 주소
IPv6 CIDR	○ AS 번호 ○ MAC 주소
네트워크	○ 대상 바이트 ○ 카운트 대상 패킷 카운트 ○ 대상 포트 ○ 종료 시간 ○ HTTP 메시지 본문 길이 ○ HTTP 요청 헤더 ○ HTTP 요청 메서드

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

특성 이름	속성 유형
	○ HTTP 요청 값 ○ HTTP 요청 버전 ○ ICMP 코드 바이트 ○ ICMP 유형 바이트 ○ 네트워크 활성 여부 ○ 소켓 블로킹 여부 ○ 소켓 리스닝 여부 ○ 네트워크 프로토콜 ○ 소켓 주소 체계 ○ 소켓 기술자 ○ 소켓 핸들 ○ 소켓 옵션 ○ 소켓 유형 소스 바이트 카운트 ○ 소스 패킷 카운트 ○ 소스 포트 ○ 시작 시간 ○ TCP 대상 플래그 ○ TCP 소스 플래그
프로세스	○ ASLR 사용 설정 ○ 명령줄 ○ 현재 작업 디렉터리(CWD) ○ DEP 사용 설정 ○ 환경 변수 ○ 숨겨짐 여부 ○ 소유자 SID ○ 프로세스 ID ○ 우선순위 ○ 프로세스 생성 시간 ○ 서비스 설명 ○ 서비스 표시 이름 ○ 서비스 그룹 이름 ○ 서비스 이름 ○ 서비스 시작 유형 ○ 서비스 상태 서비스 유형 ○ 시작 정보

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

특성 이름	속성 유형
	○ Windows 무결성 수준 ○ 창 제목
소프트웨어	○ CPE(공통 플랫폼 열거형) ○ 지원되는 언어 ○ 소프트웨어 식별(SWID) ○ 벤더 버전
사용자 계정	○ 계정 생성 시간 ○ 계정 만료 시간 ○ 계정 로그인 ○ 계정 유형 ○ 추가 정보 ○ 권한 에스컬레이션 가능 ○ 자격 증명이 마지막으로 변경된 시간 ○ 표시 이름 ○ 첫 번째 로그인 시간 ○ 계정 비활성화됨 여부 ○ 권한 있음 여부 ○ 서비스 계정 예부 ○ 마지막 로그인 시간 ○ 사용자 ID
Windows 레지스트리 키	○ 키 수정됨 ○ 시간 레지스트리 값 ○ 하위 키 수
X.509 인증서	○ 추가 정보 ○ 인증 키 식별자 ○ 기본 제약 조건 ○ 인증서 정책 ○ CRL 배포 지점 ○ 확장된 키 사용 ○ 모든 정책 금지 ○ 발급자 ○ 발급자 대체 이름 ○ 자체 서명됨 여부 ○ 주요 사용량

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

특성 이름	속성 유형
	○ 이름 제약 조건 ○ 정책 제약 조건 ○ 정책 매핑 ○ 개인 키 사용 유효 기간(시작) ○ 개인 키 사용 유효 기간(끝) ○ 서명 알고리즘 ○ 제목 ○ 제목 대체 이름 ○ 제목 디렉터리 속성 ○ 주체 키 식별자 ○ 주체 공개 키 알고리즘 ○ 주체 공개 키 지수 ○ 주체 공개 키 계수 ○ 유효 기간(시작) ○ 유효 기간 ○ 버전

인사이트

필드	설명
메모	옵저버블 기록에 대한 추가 메모를 추가합니다.

5. 저장을 클릭합니다.
   저장하면 새 옵저버블 기록이 생성되었음을 나타내는 프롬프트 메시지가 표시됩니다. 기록을 편집하고 새 관계를 생성하려면 "계속 "을 클릭하십시오.
6. 계속을 클릭합니다.

> **중요사항:**
> 새 옵저버블 기록을 생성하면 시스템 업데이트 방지 확인란이 표시됩니다.
>
> 옵저버블, 표시기 또는 STIX 객체 기록이 생성된 후 시스템에서 업데이트를 방지하려면 이 확인란을 선택합니다.

태그&분류

필드	설명
태그	
태그 선택	옵저버블과 연결된 태그를 선택합니다.
태그 추가	새 태그를 추가합니다.
분류	
분류 선택	옵저버블과 연결된 분류를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
분류 값 추가	옵저버블과 연결된 분류 값을 추가합니다.

소스 기록

필드	설명
옵저버블에 대한 소스 기록 상세 정보가 표시됩니다(있는 경우).	

다음에 수행할 작업

다음 표에는 옵저버블과 관련된 관련 기록이 나열되어 있습니다.

관련 기록

관련 목록	설명
옵저버블	이 옵저버블과 관련된 옵저버블 목록입니다. 주: 이 섹션에는 두 옵저버블 간의 잠재적 관계도 포함되어 있습니다. 자세한 내용은 두 옵저버블 간의 확인된 관계를 참조하십시오옵저버블-옵저버블 잠재성 관계 확인옵저버블-옵저버블 관계 정의.
표시기	이 옵저버블과 관련된 표시기 목록입니다.
공격 패턴	이 옵저버블과 관련된 공격 패턴의 목록입니다.
캠페인	이 옵저버블과 관련된 캠페인을 나열합니다.
인프라	시스템, 소프트웨어 서비스 및 이 옵저버블과 관련된 모든 연관된 물리적 또는 가상 자원과 같은 인프라를 나열합니다.
침입 세트	이 옵저버블과 관련된 공통 속성을 가진 일련의 적대적 행동 및 자원과 같은 침입 세트를 나열합니다.
맬웨어	이 옵저버블과 관련된 맬웨어 소스 기록을 나열합니다.
위협 액터	이 옵저버블과 관련된 위협 액터를 나열합니다.
위협 이벤트	이 옵저버블과 관련된 위협 이벤트를 나열합니다.
취약성	옵저버블이 IP 주소인 경우 이 목록에는 이 옵저버블과 관련된 일치하는 IP 주소가 있는 모든 자원(구성 항목)이 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

1. 이 객체와 연결된 관련 기록을 연결하거나 연결 해제할 수 있습니다. 자세한 내용은 위협 인텔리전스 관련 기록 연결 문서를 참조하십시오.
2. 또한 관련 기록 섹션에서 옵저버블 양식 뷰에 사용할 수 있는 잠재성 관계 섹션을 사용하여 두 옵저버블 간의 관계를 확인할 수 있습니다. 에 대한 자세한 내용은 관련 기록에서 잠재성 관계 확인를 참조하십시오.
3. 케이스에 옵저버블을 추가할 수 있습니다. 자세한 내용은 케이스에 추가 문서를 참조하십시오.
4. 옵저버블에 대한 보강 작업을 실행할 수도 있습니다. 자세한 내용은 케이스 내에서 보강 작업 실행 문서를 참조하십시오.

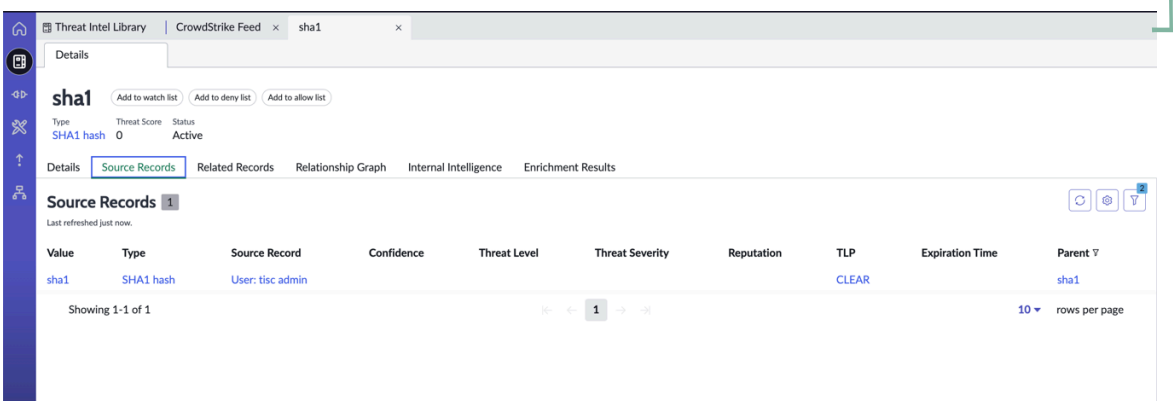
옵저버블 소스 기록

소스 기록은 양식 뷰에 표시된 것처럼 집계된 기록에 기여합니다. 이러한 소스 기록은 피드에서 자동으로 생성되거나 사용자가 수동으로 생성합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 위협 분석가 워크벤치 아이콘을 클릭합니다.
3. 이동 옵저버블 〉 모든 옵저버블.
4. 옵저버블을 하나 이상 선택합니다.
5. 소스 기록으로 이동합니다.
   집계된 기록에 대한 소스 기록이 표시됩니다.



6. 기록을 봅니다.

위협 인텔리전스 관련 기록 연결

해당 위협 인텔리전스 개체와 관련된 기록을 연결합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터 〉 위협 인텔 라이브러리 〉 옵저버블 〉 모든 옵저버블.
2. 예를 들어 옵저버블 기록을 선택합니다.
3. 관련 기록 섹션으로 이동합니다.
4. 관련 기록을 선택합니다.
5. 링크를 클릭합니다.
   개체 연결 대화 상자가 표시됩니다.
6. 목록에서 객체를 선택하고 링크 버튼을 클릭합니다.
   옵저버블 기록과 연결된 객체가 연결되어 관련 기록 목록 뷰에 표시됩니다.
7. 저장을 클릭합니다.
   연결 해제 버튼을 클릭하여 객체 연결을 해제합니다.

옵저버블 데이터 가져오기

옵저버블 관련 기록 데이터를 가져옵니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 작업 공간에서 위협 인텔 라이브러리 아이콘을 클릭합니다.
3. 옵저버블로 이동합니다.
   선택한 객체와 연결된 관련 옵저버블이 표시됩니다.
4. 옵저버블 기록을 선택합니다.
   지정된 옵저버블에 연결된 CVE가 있는 경우 제공된 버튼을 사용하여 취약한 관련 데이터를 자동으로 가져올 수 있으며 이러한 관련 기록은 취약성의 비즈니스 컨텍스트 섹션에 표시됩니다.
5. 이동 내부 인텔리전스 〉 취약한 항목.
   옵저버블에 대한 연결된 CVE 기록이 표시됩니다.
6. CVE를 선택하고 취약성 관련 데이터 가져오기 버튼을 클릭합니다.

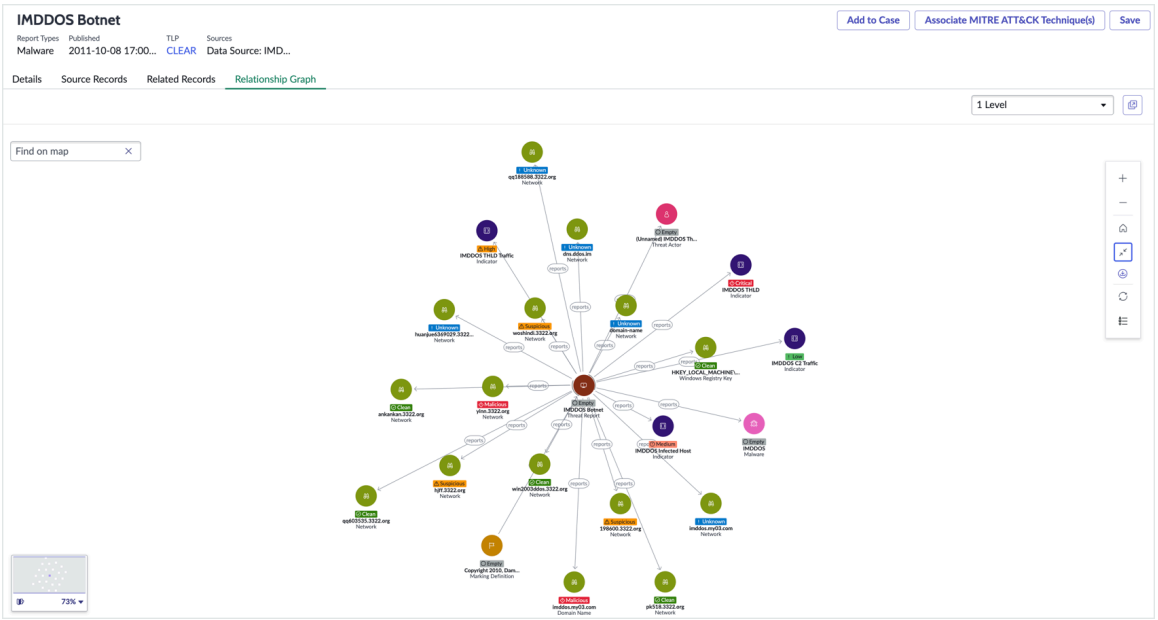
주:

- 다음과 같은 정보 메시지가 표시됩니다. 이 특정 취약성 객체에는 연결된 취약 항목이 없습니다. 데이터를 가져오려면 개체를 취약한 항목과 연결해야 합니다. 기록을 연결하고 데이터를 가져오기 위해 예약된 작업을 수행하는 방법에 대한 자세한 내용은 을 참조하십시오 취약성 데이터 가져오기 . 예약된 작업에 대한 자세한 내용은 예약된 작업을 참조하십시오.
- 이 버튼을 누르면 백그라운드 예약 작업이 트리거되고 작업 시작 및 실행 상세 정보가 활동 스트림 섹션에 표시됩니다. 예를 들어 작업이 트리거되면 활동 스트림에 취약 항목과 연결된 데이터 가져오기 시작 활동이 표시됩니다. 백그라운드 예약 작업은 옵저버블과 연결된 취약한 항목이 있는 옵저버블을 지속적으로 확인하고 자동으로 실행하며 이 예약된 작업은 1시간마다 실행됩니다. 기록을 가져오지 않은 경우 수동으로 기록을 연결하고 데이터를 가져올 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시각화 도구에서 상세 정보 보기

시각화 도우미를 사용하면 객체, 옵저버블 및 표시기 간의 관계를 볼 수 있으며, 이는 추가 조사에 필요한 컨텍스트를 제공합니다. 시각화 도우미는 색상과 아이콘을 사용하여 개체에 대한 다양한 정보를 나타냅니다.



다음과 같은 작업을 수행할 수 있습니다.

- 개체를 확대하거나, 화면에 맞추거나, 노드를 끌거나, 고정하여 특정 관계에 초점을 맞춥니다.
- 개체를 클릭하여 세부 정보 창을 엽니다. 상세 정보 창에서 객체와 관련된 자세한 정보를 확인할 수 있습니다. 객체, 객체 이름, 설명 및 소스와 같은 노드 속성을 볼 수 있습니다. 기본적으로 각 그래프 노드의 세부 정보 섹션은 표시되지 않으며 선택한 노드의 세부 정보를 보려면 그래프의 각 노드를 클릭해야 합니다.

  주:
  비주얼라이저는 관찰 데이터 객체를 제외한 모든 STIX 도메인 객체(SDO)에 사용할 수 있습니다. 새로 고침 버튼을 클릭하여 시각화 도우미를 새로 고칩니다.

- 팝업 아이콘을 클릭하면 훨씬 더 큰 창에서 그래프를 볼 수도 있습니다.

관계 그래프의 링크 노드 작업

새 관련 기록을 추가하여 노드를 연결합니다.

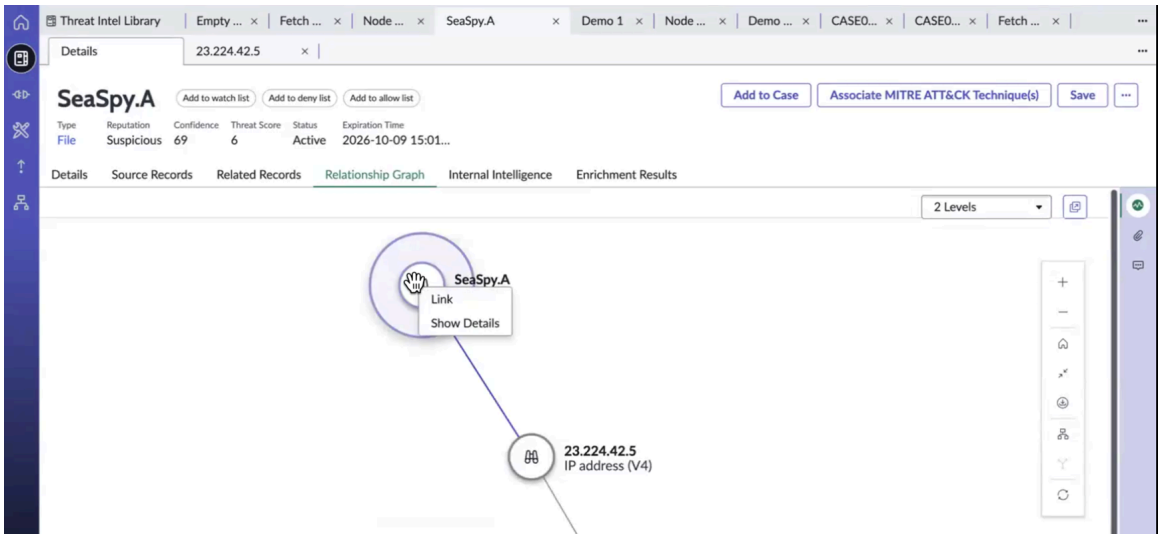
시작하기 전에
필요한 역할: sn_sec_tisc.analyst

프로시저

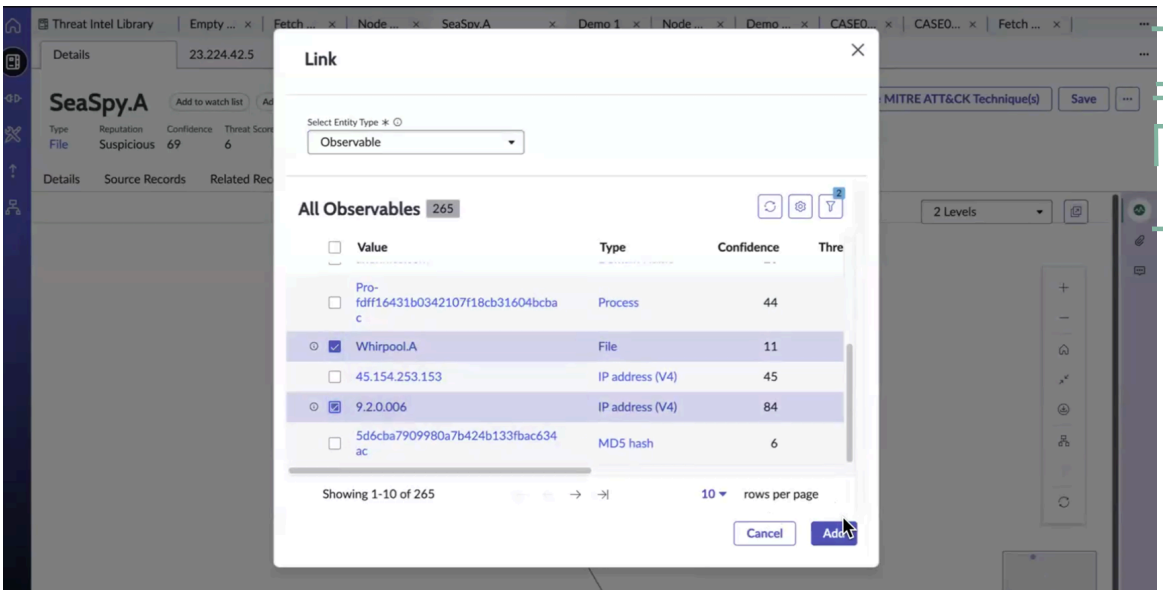
1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터 〉 위협 인텔 라이브러리 〉 옵저버블 〉 모든 옵저버블.
2. 예를 들어 옵저버블 기록을 선택합니다.
3. 관계 그래프 섹션으로 이동합니다.
4. 노드를 클릭합니다.
5. 링크를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
이 작업은 홈 노드 수준에서만 사용할 수 있습니다.



6. 옵저버블과 같은 엔터티 유형을 선택합니다.
7. 상위 노드에 대한 옵저버블을 하나 이상 선택합니다.
8. 추가를 클릭합니다.
   옵저버블이 상위 노드에 추가됩니다.



9. 노드에서 관련 기록의 연결을 해제하려면 연결 해제 를 선택합니다.

주:
관련 기록 데이터는 연결 해제되지만 홈 노드와 옵저버블 간의 관계는 위협 인텔리전스 라이브러리에 계속 남아 있습니다.

10. 상세 정보 표시를 선택하여 연결된 옵저버블 데이터를 봅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

내부 인텔리전스 기록 작업

이 기능을 사용하여 구성 데이터베이스 관리 시스템(CMDB)에서 위협 인텔리전스 보안 센터로 수집된 내부 인텔리전스 데이터로 작업합니다.

내부 인텔리전스 기록 조회

CMDB, SIR(보안 인시던트 대응), VR(취약성 대응) 기록에서 수집한 내부 인텔리전스 기록을 봅니다.

시작하기 전에

내부 인텔리전스 섹션에서는 SIR, VR 및 CMDB와 같은 플랫폼의 다른 애플리케이션의 컨텍스트를 제공하여 분석가에게 위협에 대한 보다 넓은 관점을 제공합니다.

필요한 역할: sn_sec_tisc.analyst

> **주:**
> 내부 인텔리전스 탭은 옵저버블 및 취약성 객체에 대해서만 표시됩니다.

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터 〉 위협 인텔 라이브러리 〉 옵저버블 〉 모든 옵저버블.
2. 옵저버블 기록을 선택합니다.
3. 내부 인텔리전스 탭으로 이동합니다.
   내부 인텔리전스 섹션은 보안 인시던트 응답, 비즈니스 컨텍스트, 취약성 대응과 같은 세 개의 하위 섹션으로 구성됩니다.

   > **주:**
   > 내부 인텔리전스 탭에 이 섹션을 나열하려면 인스턴스에 해당 애플리케이션이 설치되어 있어야 합니다.

   a. 보안 인시던트 응답: 연결된 옵저버블 및 취약성 항목과 연결된 모든 인시던트를 표시합니다.

   > **주:**
   > 옵저버블 값은 SIR 인시던트와 TISC 내에서만 일치해야 하며, 그런 다음에만 연결된 옵저버블 또는 표시기가 보안 인시던트 응답 섹션 아래에 나열됩니다. 소스 시스템 내에서 기록을 검색하여 기록을 연결 및 연결 해제할 수도 있습니다. 자세한 내용은 위협 인텔리전스 관련 기록 연결 문서를 참조하십시오.

   - 기록을 선택하여 소스 시스템에서 상세 정보를 탐색하고 봅니다. 예를 들어, 연결된 옵저버블 기록을 가져오기 위한 보안 인시던트 응답의 연결된 옵저버블입니다.
   - 최신 릴리스의 일부로 소스(SIR) 기록에서 가져올 수 있는 인텔리전스 데이터는 다음과 같습니다.
     - 연결된 옵저버블
     - 취약성 항목

   b. 비즈니스 컨텍스트: 영향을 받는 사용자 및 기타 구성 항목을 표시합니다. 현재 릴리스의 일부로 소스(비즈니스 컨텍스트) 기록에서 가져올 수 있는 인텔리전스 데이터는 다음과 같습니다.
   - 구성 항목
   - 영향을 받는 서비스
   - 영향을 받는 자산

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

c. 취약성 대응: 취약성 인텔리전스 데이터를 표시합니다.

취약성 항목: 이 옵션은 취약성을 일치시키고 관련 레코드를 가져옵니다.

옵저버블에서 보강 작업 실행

이 섹션을 사용하여 옵저버블 및 기타 객체에서 보강 작업이 수행되는 방식을 이해합니다.

시작하기 전에

필요한 역할: sn_sec_tisc.admin

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 위협 분석가 워크벤치 아이콘을 클릭합니다.
3. 이동 옵저버블 〉 모든 옵저버블.
4. 분할 버튼에서 보강 작업을 클릭합니다.
5. 사용 가능한 구현을 선택합니다.
6. 제출을 클릭합니다.
   예를 들어 위협 조회 실행입니다. 선택한 보강 작업이 실행되고 선택한 옵저버블에서 옵저버블 보강 실행이 시작되었다는 정보 메시지가 표시됩니다 . 실행이 완료되면 각 옵저버블의 상세 페이지에서 결과를 확인할 수 있습니다.

   주:
   실행이 시작되거나 완료되면 작업 메모가 양식 뷰의 활동 스트림에 게시됩니다.

케이스에 추가

케이스에 옵저버블, 표시기 또는 기타 객체를 추가합니다.

시작하기 전에

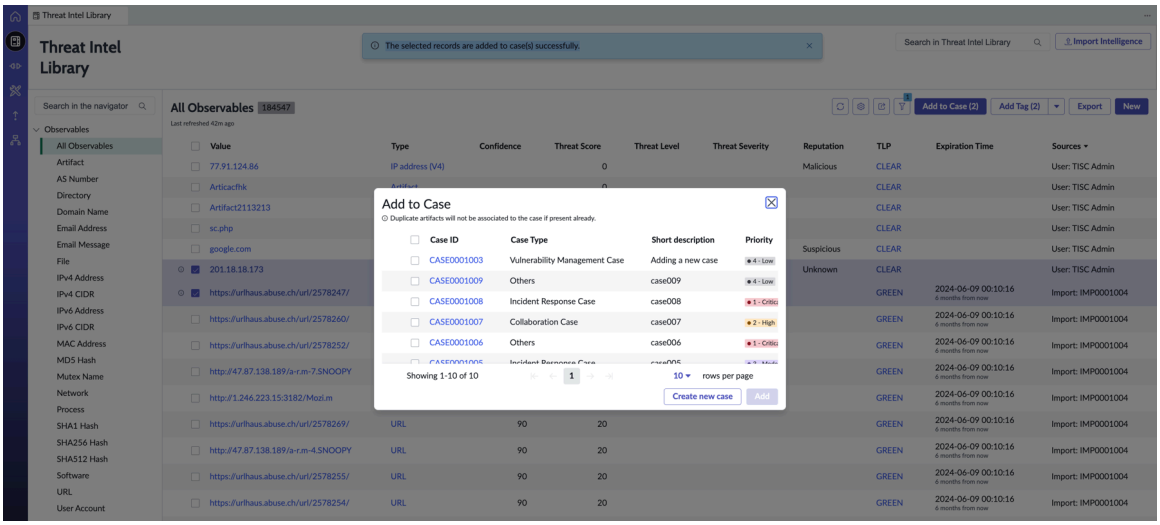
필요한 역할: sn_sec_tisc.analyst

다음은 옵저버블 기록에 케이스를 추가하는 방법을 보여주는 절차입니다.

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터 〉 위협 인텔 라이브러리 〉 옵저버블 〉 모든 옵저버블.
2. 옵저버블을 선택합니다.
3. **Add to Case** 버튼을 클릭합니다.
   기록이 아직 연결되지 않은 케이스만 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 기존 케이스에 기록을 추가할지 확인하고, 추가할 경우 기존 케이스를 선택하고, 추가할 경우 기존 케이스를 선택하고, 그렇지 않으면 새 케이스 생성을 클릭합니다.
다음 정보를 입력하여 새 케이스를 만듭니다.

새 케이스 작성

필드	설명
케이스 ID	케이스의 고유 식별자입니다. 시스템에서 생성된 ID입니다.
간단한 설명	조사 중인 요청이나 문제 또는 간단한 설명에 대한 요약입니다.
케이스 유형	조사 중인 케이스의 유형을 선택합니다. 조사에 사용할 수 있는 옵션은 다음과 같습니다. ○ 위협 헌팅 ○ 정보 요청 ○ 취약성 관리 케이스 ○ 규정 준수 케이스 ○ 인시던트 응답 케이스 ○ 공동 작업 케이스 ○ 기타
우선순위	요청 또는 문제의 심각도에 대한 평가입니다.
담당 그룹	케이스 작업을 담당하는 할당된 그룹입니다.
담당자	케이스 작업을 담당하는 분석가입니다.

5. 새 케이스를 만들려면 만들기를 클릭합니다.

주:
새 케이스가 기존 케이스 목록에 추가됩니다.

6. 새로 추가된 케이스를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

7. 추가를 클릭합니다.
   선택한 기록이 케이스에 성공적으로 추가되었다는 정보 메시지가 표시됩니다.

TISC에서 보강 작업 실행

아래 표에서는 TISC에서 다양한 보강 작업을 실행하는 것과 관련된 상호 작용에 대해 설명합니다.

TISC 모달 화면

역량	UX 프레임워크 상호작용	지원되는 통합
위협 조회 실행	화면 1 – 구현을 선택하고 제출합니다. 위협 조회 실행에 적용할 수 있는 공통 입력 또는 구현 특정 입력이 없습니다.	• Virus Total • Crowd Strike Falcon Intelligence
사이팅 검색 실행	화면 1 – 구현 선택 및 화면 2 – 공통 입력을 적용할 수 있습니다. 사이팅 검색은 Splunk 및 기타 통합의 여러 구현에서 날짜 및 시간 빈도를 공통 입력으로 사용합니다.	• 탄력적 검색 • Splunk 사이팅
옵저버블 보강 실행	화면 1 전용만 - 구현을 선택합니다. 옵저버블 보강 실행에 적용할 수 있는 공통 입력 또는 구현별 입력이 없습니다.	• 후이즈 • Shodan

위협 조회 실행

해당하는 구현을 하나 이상 선택하여 옵저버블에 대한 위협 조회를 실행합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.admin

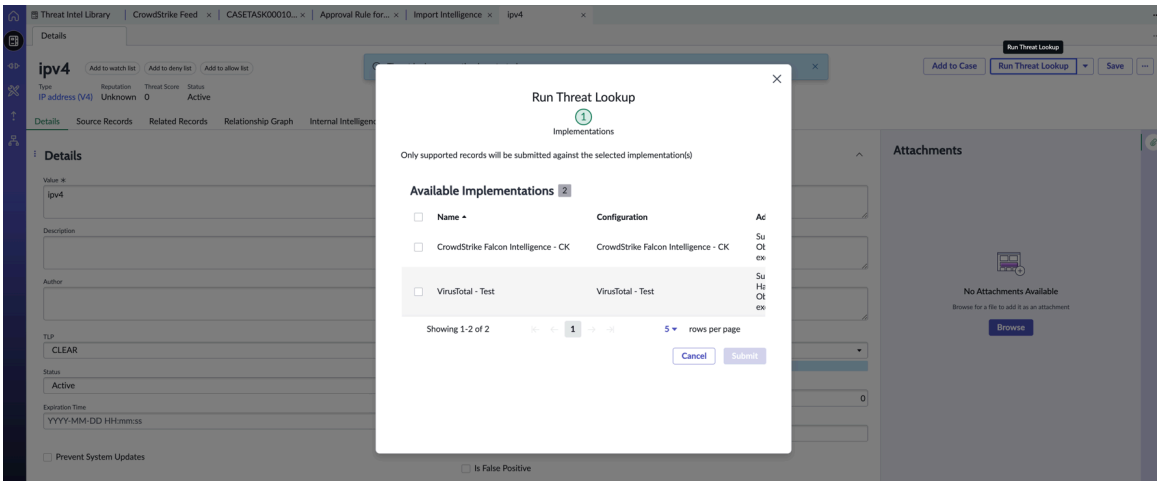
프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 위협 분석가 워크벤치 아이콘을 클릭합니다.
3. 이동 옵저버블 〉 모든 옵저버블.
4. 옵저버블 기록을 엽니다.
5. 위협 조회 실행을 클릭합니다.
   위협 조회 실행 구현 선택 모달 화면이 표시됩니다.

   주:
   위협 조회 실행은 위협 인텔리전스 조회를 수행하여 옵저버블이 알려진 위협과 연결되어 있는지 여부를 확인합니다.

6. 목록에서 필요한 구현을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



7. 제출을 클릭합니다.
선택한 보강 작업이 실행되고 위협 조회 실행이 시작되었다는 정보 메시지가 표시됩니다.

주:

- 실행이 시작되거나 완료되면 작업 메모가 양식 뷰의 활동 스트림에 게시됩니다.
- SIR 작업 공간에서 푸시된 보강 결과는 TISC 작업 공간의 해당 옵저버블 상세 정보 페이지에 있는 보강 결과 탭에서 찾을 수 있습니다.
- SIR 작업 공간에서 푸시된 향상된 결과는 보강 결과 테이블의 소스 필드를 사용하여 식별할 수 있습니다.

사이팅 검색 실행

사이팅 검색 관련 통합 실행을 수행합니다.

시작하기 전에

필요한 역할: sn_sec_tisc.admin

이 작업을 수행하려면 구현을 선택하고 해당하는 경우 선택한 모든 구현에 적용되는 공통 실행 시간 입력을 추가합니다.

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.

2. 위협 분석가 워크벤치 아이콘을 클릭합니다.

3. 이동 옵저버블 〉 모든 옵저버블.

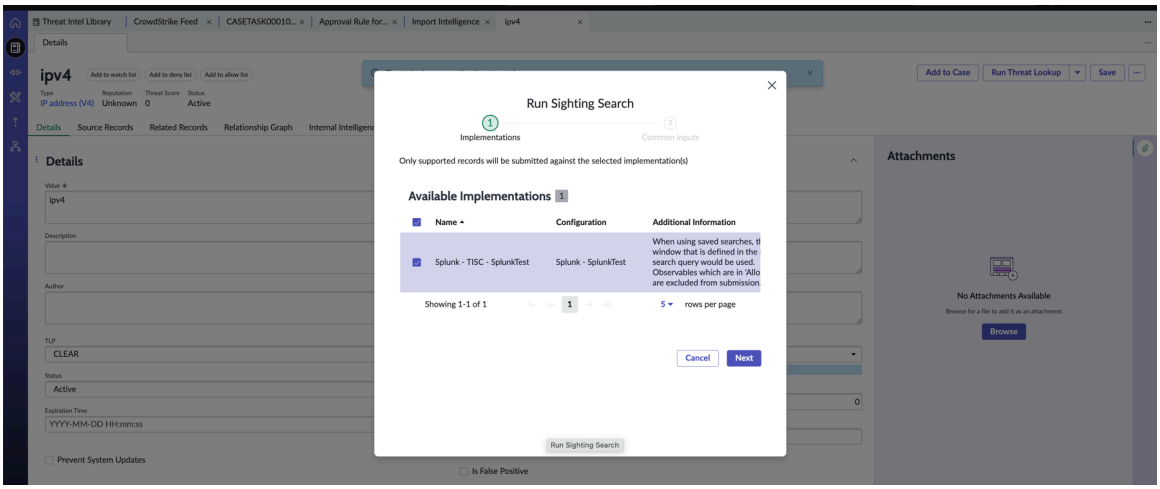
4. 옵저버블 기록을 엽니다.

5. 사이팅 검색 실행을 클릭합니다.
사이팅 검색 실행 구현 선택 모달 화면이 표시됩니다.

주:
사이팅 검색 실행은 위협 인텔리전스 조회를 수행하여 옵저버블이 알려진 위협과 연결되어 있는지 여부를 확인합니다.

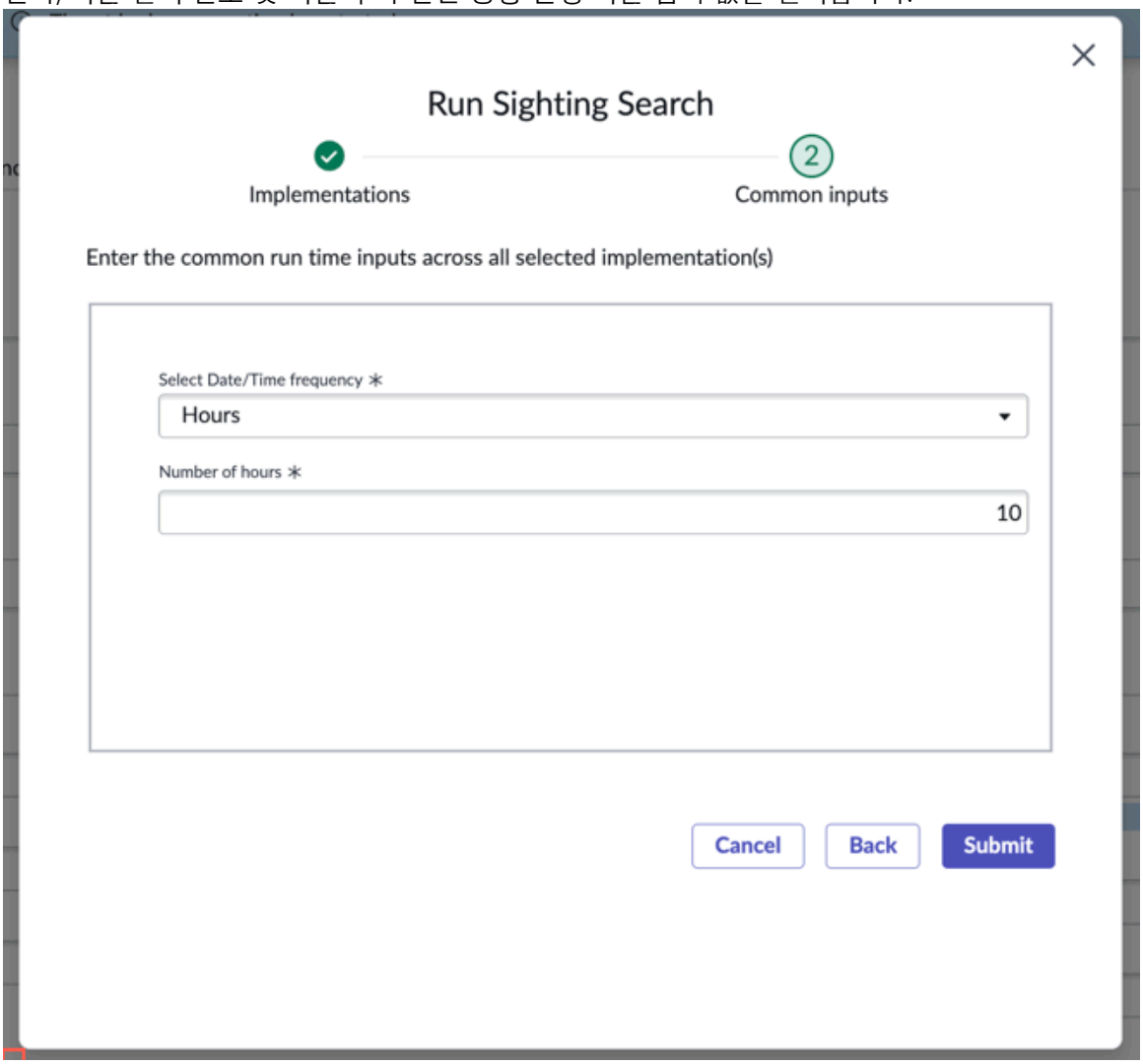
6. 목록에서 필요한 구현을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



7. 다음을 클릭합니다.

8. 날짜/시간 선택 빈도 및 시간 수와 같은 공통 실행 시간 입력 값을 선택합니다.



9. 제출을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

선택한 보강 작업이 실행되고 사이팅 검색 실행 실행이 시작되었다는 정보 메시지가 표시됩니다.

주:

- 실행이 시작되거나 완료되면 작업 메모가 양식 뷰의 활동 스트림에 게시됩니다.
- SIR 작업 공간에서 푸시된 보강 결과는 TISC 작업 공간의 해당 옵저버블 상세 정보 페이지에 있는 보강 결과 탭에서 찾을 수 있습니다.
- SIR 작업 공간에서 푸시된 향상된 결과는 보강 결과 테이블의 소스 필드를 사용하여 식별할 수 있습니다.

옵저버블 보강 실행

해당하는 구현을 하나 이상 선택하여 옵저버블에 대한 위협 조회를 실행합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.admin

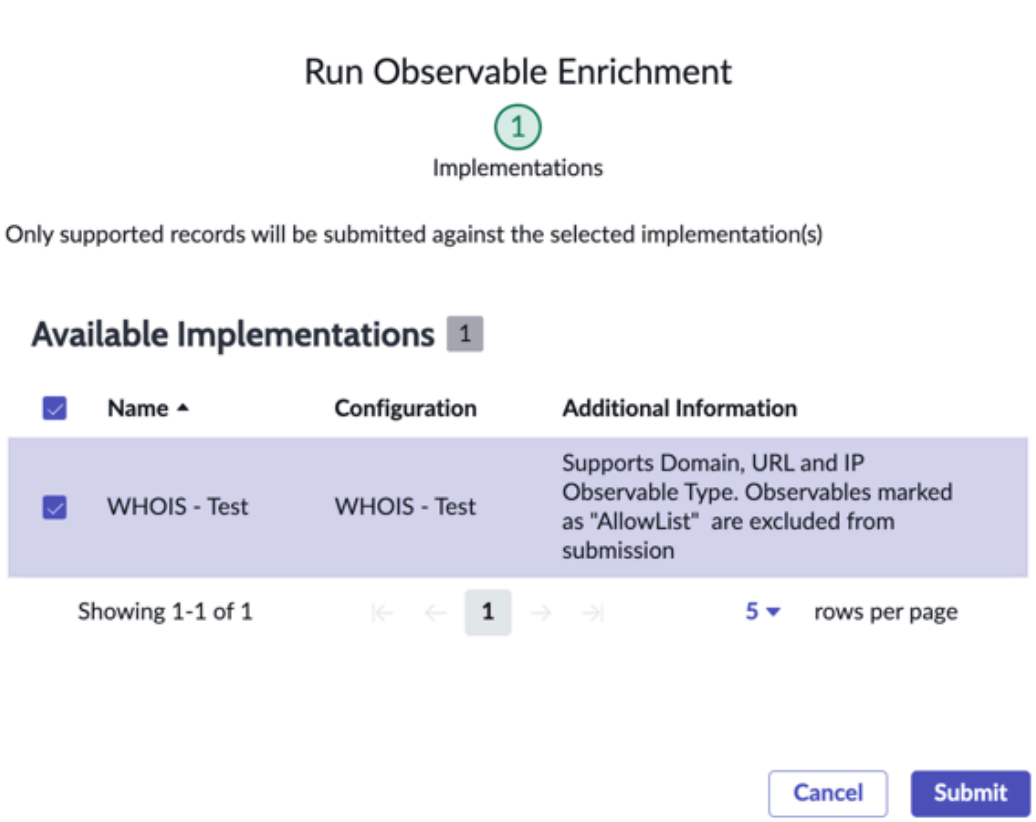
프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 위협 분석가 워크벤치 아이콘을 클릭합니다.
3. 이동 옵저버블 〉 모든 옵저버블.
4. 옵저버블 기록을 엽니다.
5. 옵저버블 보강 실행을 클릭합니다.
   옵저버블 보강 구현 선택 실행 모달 화면이 표시됩니다.

   주:
   선택한 구현에 대해 지원되는 기록만 제출됩니다.

6. 목록에서 필요한 구현(예: WHOIS)을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



7. 제출을 클릭합니다.
선택한 보강 작업이 실행되고 위협 조회 실행이 시작되었다는 정보 메시지가 표시됩니다.

주:

- 실행이 시작되거나 완료되면 작업 메모가 양식 뷰의 활동 스트림에 게시됩니다.
- SIR 작업 공간에서 푸시된 보강 결과는 TISC 작업 공간의 해당 옵저버블 상세 정보 페이지에 있는 보강 결과 탭에서 찾을 수 있습니다.
- SIR 작업 공간에서 푸시된 향상된 결과는 보강 결과 테이블의 소스 필드를 사용하여 식별할 수 있습니다.

보강 결과 보기

옵저버블, 표시기 및 다양한 객체 보강 결과를 봅니다.

시작하기 전에

필요한 역할: sn_sec_tisc.admin

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터 〉 위협 인텔 라이브러리 〉 옵저버블 〉 모든 옵저버블.

2. 옵저버블 기록을 선택합니다.

3. 보강 결과 탭으로 이동합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보강 결과에는 TISC 통합 보강 결과가 표시됩니다.

보강 이름	설명
위협 조회 결과	옵저버블에 대한 모든 관련 위협 조회 결과를 나열합니다.
사이팅	옵저버블에 대한 모든 관련 사이팅을 나열합니다.
옵저버블 보강 결과	옵저버블에 대해 연결된 모든 옵저버블 보강 결과를 나열합니다.

표시기

표시기는 침입을 나타낼 수 있는 네트워크 또는 운영 체제에서 관찰되는 아티팩트입니다. 일반적인 IoC는 바이러스 서명 및 IP 주소, 맬웨어 파일 또는 URL의 MD5 해시 또는 도메인 이름입니다.

표시기 정의

표시기를 정의합니다.

시작하기 전에

필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터 〉 위협 인텔 라이브러리 〉 표시기.
2. 표시기를 선택합니다.
3. 새로 만들기를 클릭합니다.

   주:
   옵저버블, 표시기, 엔터티 또는 객체에 대한 새 객체 기록을 생성할 때마다 소스 기록이 생성되고, 새 객체 기록이 생성된 다음 사용자가 집계된 기록으로 리디렉션된다는 프롬프트 메시지가 표시됩니다.

4. 양식에서 필드를 채웁니다.

   상세 정보 섹션

필드	설명
ID	표시기의 고유 ID입니다.
설명	표시기에 대한 설명입니다.
이름	표시기 이름입니다.
패턴	이 지표에 대한 검출 패턴은 STIX 패턴으로 표현될 수 있다.
패턴 유형	이 표시기에 사용되는 패턴 언어입니다.
패턴 버전	패턴 속성의 데이터에 사용되는 패턴 언어의 버전으로, 패턴 속성에 포함된 패턴 데이터의 유형과 일치해야 합니다.
유효 기간(시작)	이 표시기가 관련되거나 나타내는 동작의 유효한 표시기로 간주되는 시간입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
유효 기간	이 표시기가 더 이상 관련되거나 나타내는 동작의 유효한 표시기로 간주되어서는 안 되는 시간입니다.
IOC 분류	지표의 IOC 분류입니다.
표시기 유형	표시기의 다양한 범주를 나타냅니다.
상태	표시기의 상태를 나타냅니다.
플랫폼	이 표시기를 적용할 수 있는 플랫폼을 정의합니다.
TLP	TLP별 데이터 민감도 설정을 나타내는 고유 값입니다.
공격 단계	LM, MITRE ATT&CK와 같은 킬 체인의 공격 단계를 나타냅니다.
신뢰도	이 표시기 기록에 대한 신뢰도를 입력합니다. confidence 속성은 작성자가 데이터의 정확성에 대해 가지고 있는 신뢰도를 식별합니다. 신뢰도 값은 0-100 범위의 숫자여야 합니다(MUST).
위협 수준	표시기 기록의 위협 수준을 나타냅니다.
만료 시간	표시기 기록의 만료 시간을 지정합니다.
위협 심각성	표시기 기록의 위협 심각도를 나타냅니다.
사용 범주	옵저버블이 속하는 범주(예: 봇넷 또는 피싱)입니다.
처음으로 발견됨	이 표시기 기록이 악의적인 활동을 수행하는 것이 처음 목격된 시간입니다.
마지막으로 발견됨	이 표시기 기록이 마지막으로 악의적인 활동을 수행하는 것이 목격된 시간입니다.
소스	이 기록이 생성되는 위협 소스를 지정합니다.
해지함	해지된 개체가 개체 작성자에 의해 더 이상 유효한 것으로 간주되지 않음을 나타냅니다.

인사이트

필드	설명
메모	표시기에 대한 추가 메모를 추가합니다.

추가 정보

필드	설명
추가 컨텍스트	이 표시기에 대한 추가 컨텍스트를 추가합니다.
사양 버전	표시기를 나타내는 데 사용되는 STIX 사양의 버전입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	이 특성에 대한 값은 이 사양에 따라 정의된 STIX 객체에 대해 2.1이어야 합니다.
언어	이 속성은 이 객체의 텍스트 컨텐츠 언어를 식별합니다.
작성됨	시스템에서 표시기가 만들어지는 시간을 지정합니다.
업데이트됨	시스템에서 표시기가 업데이트되는 시간을 지정합니다.
확장명	표시기의 확장을 나타냅니다.
처리 상태	이 표시기의 처리 상태를 나타냅니다.

5. 저장을 클릭합니다.
저장하면 새 옵저버블 기록이 생성되었음을 나타내는 프롬프트 메시지가 표시됩니다. 기록을 편집하고 새 관계를 생성하려면 "계속 "을 클릭하십시오.
6. 계속을 클릭합니다.

중요사항:
새 옵저버블 기록을 생성하면 시스템 업데이트 방지 확인란이 표시됩니다.

옵저버블, 표시기 또는 STIX 객체 기록이 생성된 후 시스템에서 업데이트를 방지하려면 이 확인란을 선택합니다.

태그&분류

필드	설명
태그	
태그 선택	표시기와 연결된 태그를 선택합니다.
태그 추가	새 태그를 추가합니다.
분류	
분류 선택	표시기와 연관된 분류를 선택합니다.
분류 값 추가	표시기와 연결된 분류 값을 추가합니다.

소스 기록

필드	설명
표시기에 대한 소스 기록 상세 정보가 표시됩니다(있는 경우).	

다음에 수행할 작업
이제 다음 관련 목록 중 하나를 클릭하여 표시기와 연관된 객체에 대한 추가 정보를 볼 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관련 기록

관련 목록	설명
MITRE 기술	이 표시기와 관련된 MITRE 기술을 나열합니다.
공격 패턴	악의적 사용자가 이 표시기와 관련된 대상을 손상시키려고 시도하는 방법을 설명하는 공격 패턴 소스를 나열합니다.
캠페인	이 표시기와 관련된 특정 대상 집합에 대해 시간 경과에 따라 발생하는 일련의 악의적인 활동 또는 공격을 설명하는 캠페인 소스를 나열합니다.
작업 과정	이 표시기와 관련된 작업 과정을 나열합니다.
데이터 소스	이 표시기와 관련된 데이터 소스를 나열합니다.
데이터 구성요소	이 표시기와 관련된 데이터 구성요소를 나열합니다.
ID	이 표시기와 관련된 ID를 나열합니다.
표시기	이 표시기와 관련된 표시기를 나열합니다. 주: 이 섹션에는 두 표시기 간의 잠재적 관계도 포함되어 있습니다. 자세한 내용은 두 옵저버블 간의 확인된 관계를 참조하십시오표시기-표시기 잠재성 관계 확인표시기-표시기 관계 정의.
인프라	이 표시기와 관련된 공격의 특정 목적을 지원하기 위한 시스템, 소프트웨어 서비스 및 관련된 물리적 또는 가상 자원을 설명하는 인프라 소스를 나열합니다.
침입 세트	이 표시기와 관련된 공통 속성이 있는 일련의 적대적 행동 및 자원을 나열합니다.
위치	객체와 연결된 지리적 위치를 나열합니다.
맬웨어	이 표시기와 관련된 맬웨어 소스 기록을 나열합니다.
표시 정의	이 객체와 연결된 표시 정의를 나열합니다.
맬웨어 분석	이 표시기와 연결된 맬웨어 인스턴스에서 수행된 특정 정적 또는 동적 분석의 메타데이터와 결과를 나열합니다.
옵저버블	이 표시기와 관련된 관련 옵저버블 기록을 나열합니다.
관찰 데이터	파일, 시스템, 네트워크 등의 사이버 보안 관련 엔터티이고 이 표시기와 관련된 관찰 데이터를 나열합니다.
사이팅	이 객체와 연결된 사이팅 소스 기록을 나열합니다.
위협 액터	옵저버블과 연결된 변경 내용을 나열합니다.
위협 이벤트	표시기와 관련된 바람직하지 않은 결과나 영향을 초래할 가능성이 있는 이벤트 또는 상황을 나열합니다.
위협 그룹화	위협 그룹화를 공유 컨텍스트가 있는 개체로 나열합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관련 기록

관련 목록	설명
위협 메모	표시기와 연결된 추가 컨텍스트 또는 분석을 제공하기 위해 정보를 전달하는 위협 메모를 나열합니다.
위협 의견	표시기와 연결된 정보의 정확성에 대한 평가로 위협 의견을 나열합니다.
위협 보고서	이 표시기와 연결된 위협 보고서를 나열합니다.
도구	이 개체와 연결된 도구를 나열합니다.
취약성	옵저버블이 IP 주소인 경우 이 목록에는 일치하는 IP 주소가 있는 모든 리소스(구성 항목)가 표시됩니다.
관련 케이스	이 표시기와 연결된 관련 케이스를 나열합니다.
관련 케이스 작업	이 표시기와 연결된 관련 케이스 작업을 나열합니다.
관련 캔버스	이 표시기와 연결된 관련 캔버스를 나열합니다.
표시기 참조	이 표시기를 설명하는 외부 참조 목록입니다.

주:

1. 이 객체와 연결된 관련 기록을 연결하거나 연결 해제할 수 있습니다. 자세한 내용은 위협 인텔리전스 관련 기록 연결 문서를 참조하십시오.
2. 또한 관련 기록 섹션에서 표시기 양식 뷰에 사용할 수 있는 잠재성 관계 섹션을 사용하여 두 옵저버블 간의 관계를 확인할 수 있습니다. 에 대한 자세한 내용은 관련 기록에서 잠재성 관계 확인를 참조하십시오.
3. 케이스에 표시기를 추가할 수 있습니다. 자세한 내용은 케이스에 추가 문서를 참조하십시오.

공격 패턴

공격 패턴은 공격자가 대상을 손상시키려고 시도하는 방법을 설명하는 전술, 기술 및 절차(TTP)의 한 유형입니다.

공격 패턴은 공격을 분류하는 데 사용됩니다. 특정 공격을 따르는 패턴으로 일반화하고 공격이 수행되는 방식에 대한 자세한 정보를 제공합니다.

예를 들어 스피어 피싱은 공격자가 링크를 클릭하거나 첨부 파일을 열어 맬웨어를 전달하도록 하기 위해 신중하게 제작된 전자 메일 메시지를 당사자에게 보내는 일반적인 공격 유형입니다. 공격 패턴은 특정 위협 행위자에 의한 스피어 피싱(예: 대상이 콘테스트에서 우승한 경우)과 같이 보다 구체적입니다.

공격 패턴 정의

위협 분석가가 공격을 분류할 수 있도록 공격 패턴을 정의합니다.

시작하기 전에

필요한 역할: sn_sec_tisc.analyst

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 작업 공간에서 위협 인텔 라이브러리 아이콘을 클릭합니다.
3. 공격 패턴으로 이동합니다.
4. 새로 만들기를 클릭합니다.

   주:
   옵저버블, 표시기, 엔터티 또는 객체에 대한 새 객체 기록을 생성할 때마다 소스 기록이 생성되고, 새 객체 기록이 생성된 다음 사용자가 집계된 기록으로 리디렉션된다는 프롬프트 메시지가 표시됩니다.

5. 양식에서 필드를 채웁니다.

공격 패턴 세부 정보 뷰

필드	설명
ID	공격 패턴의 고유 ID입니다.
이름	이 공격 패턴의 이름을 입력합니다.
설명	공격 패턴에 대한 설명을 입력합니다.
별칭	이 공격 패턴을 식별하는 대체 이름입니다. 주: 애플리케이션에 없는 새 별칭을 추가하려면 별칭 필드 자체에 있는 새 별칭 추가 아이콘을 클릭합니다.
공격 단계	LM, MITRE ATT&CK와 같은 킬 체인의 공격 단계를 나타냅니다.
권한 필요	이 공격 패턴에 필요한 권한을 선택합니다.
TLP	TLP는 민감한 정보가 적절한 대상과 공유되도록 하는 데 사용됩니다. 4가지 색상(흰색, 녹색, 호박색, 빨간색)을 사용하여 다양한 민감도를 나타냅니다.
신뢰도	이 공격 패턴 모드에 대한 신뢰도를 입력합니다. confidence 속성은 작성자가 데이터의 정확성에 대해 가지고 있는 신뢰도를 식별합니다. 신뢰도 값은 0-100 범위의 숫자여야 합니다(MUST).
소스	이 개체 기록이 생성되는 위협 소스를 지정합니다.
해지함	해지된 개체가 개체 작성자에 의해 더 이상 유효한 것으로 간주되지 않음을 나타냅니다.
시스템 업데이트 방지	이 플래그를 예로 설정하면 시스템이 기록의 필드 값을 재정의할 수 없습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

중요사항:
새 개체 레코드를 만들면 시스템 업데이트 방지 확인란이 표시됩니다.

옵저버블, 표시기 또는 STIX 객체 기록이 생성된 후 시스템에서 업데이트를 방지하려면 이 확인란을 선택합니다.

인사이트

필드	설명
메모	공격 패턴에 대한 추가 메모를 추가합니다.

추가 정보

필드	설명
추가 컨텍스트	이 공격 패턴에 대한 추가 컨텍스트를 추가합니다.
사양 버전	이 객체, 공격 패턴을 나타내는 데 사용되는 STIX 사양의 버전입니다. 이 특성에 대한 값은 이 사양에 따라 정의된 STIX 객체에 대해 2.1이어야 합니다.
언어	이 속성은 이 객체의 텍스트 컨텐츠 언어를 식별합니다.
작성됨	시스템에서 기록이 생성되는 시간을 지정합니다.
업데이트됨	시스템에서 기록이 수정되는 시간을 지정합니다.
확장명	공격 패턴의 확장을 나타냅니다.
처리 상태	이 개체의 처리 상태, 공격 패턴을 나타냅니다.

6. 저장을 클릭합니다.
저장하면 새 옵저버블 기록이 생성되었음을 나타내는 프롬프트 메시지가 표시됩니다. 기록을 편집하고 새 관계를 생성하려면 "계속 "을 클릭하십시오.
7. 계속을 클릭합니다.

중요사항:
새 옵저버블 기록을 생성하면 시스템 업데이트 방지 확인란이 표시됩니다.

옵저버블, 표시기 또는 STIX 객체 기록이 생성된 후 시스템에서 업데이트를 방지하려면 이 확인란을 선택합니다.

태그&분류

필드	설명
태그	
태그 선택	옵저버블과 연결된 태그를 선택합니다.
태그 추가	새 태그를 추가합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
분류	
분류 선택	공격 패턴과 연결된 분류를 선택합니다.
분류 값 추가	공격 패턴과 연결된 분류 값을 추가합니다.

다음에 수행할 작업
이제 다음 관련 목록 중 하나를 클릭하여 공격 패턴과 관련된 객체에 대한 추가 정보를 볼 수 있습니다.

관련 기록

필드	설명
외부 참조	STIX가 아닌 정보를 참조하는 외부 참조를 나열합니다. 이 속성은 하나 이상의 외부 객체 식별자를 제공하는 데 사용됩니다.
캠페인	이 객체와 연관된 캠페인을 나열합니다.
ID	이 객체와 연결된 ID 목록입니다.
표시기	이 개체와 연결된 위협 소스에서 식별한 관련 IoC(침해 표시기)를 나열합니다.
침입 세트	이 객체와 관련된 공통 속성이 있는 일련의 적대적 동작 및 자원을 나열합니다.
위치	이 객체에 지리적 컨텍스트를 제공하는 위치를 나열합니다.
맬웨어	이 객체와 연결된 악성 코드를 나열합니다.
위협 액터	이 객체와 관련하여 악의적인 의도를 가지고 행동하는 개인, 그룹 또는 조직을 나열합니다.
도구	위협 행위자가 이 개체와 관련된 공격을 수행하는 데 사용하는 합법적인 소프트웨어를 나열합니다.
취약성	공격자가 악용하는 소프트웨어 또는 하드웨어의 약점 또는 결함을 나열합니다. 이 개체와 관련되어 있습니다.

주:

1. 이 객체와 연결된 관련 기록을 연결하거나 연결 해제할 수 있습니다. 자세한 내용은 위협 인텔리전스 관련 기록 연결 문서를 참조하십시오.
2. TI 라이브러리 내의 다양한 SDO에는 잠재적인 관계도 포함됩니다. 두 개체 간의 관계를 설정하려면 위협 인텔리전스 라이브러리의 **Potential** Relationships(잠재적 관계) 링크를 사용하여 개체 간의 관계를 확인합니다. 자세한 내용은 객체-객체 잠재성 관계 확인 문서를 참조하십시오.
3. 또한 객체 양식 뷰에서 관련 기록 섹션을 사용하면 양식 뷰에서 사용할 수 있는 잠재성 관계 섹션을 통해 두 객체 간의 관계를 확인할 수 있습니다. 에 대한 자세한 내용은 관련 기록에서 잠재성 관계 확인를 참조하십시오.
4. 케이스에 개체를 추가할 수 있습니다. 자세한 내용은 케이스에 추가 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

캠페인

캠페인은 일련의 악의적인 활동 또는 공격을 설명하는 적대적 행동의 그룹화로 정의되며, 특정 대상 집합에 대해 일정 기간 동안 발생하는 웨이브라고도합니다.

캠페인 정의

캠페인을 정의하여 적대적 행동을 그룹화합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 작업 공간에서 위협 인텔 라이브러리 아이콘을 클릭합니다.
3. 캠페인 객체로 이동합니다.
4. 새로 만들기를 클릭합니다.

   주:
   옵저버블, 표시기, 엔터티 또는 객체에 대한 새 객체 기록을 생성할 때마다 소스 기록이 생성되고, 새 객체 기록이 생성된 다음 사용자가 집계된 기록으로 리디렉션된다는 프롬프트 메시지가 표시됩니다.

5. 양식에서 필드를 채웁니다.

캠페인 뷰

필드	설명
ID	적대적 동작에 대한 고유 ID입니다.
이름	적대적 동작의 이름을 입력합니다.
설명	이 캠페인에 대한 설명을 입력합니다.
목표	캠페인의 기본 목표, 목적, 원하는 결과 또는 의도된 효과입니다. 위협 행위자 또는 침입 세트가 이 캠페인을 통해 달성하고자 하는 것입니다.
별칭	이 캠페인에 대해 식별할 대체 이름입니다. 주: 애플리케이션에 없는 새 별칭을 추가하려면 별칭 필드 자체에 있는 새 별칭 추가 아이콘을 클릭합니다.
TLP	TLP(Traffic Light Protocol)는 올바른 대상과 공유되는 중요한 정보를 나타냅니다. 4가지 색상(흰색, 녹색, 호박색 및 빨간색)을 사용하여 이 공격 패턴에 대한 다양한 민감도를 나타냅니다.
신뢰도	이 캠페인에 대한 신뢰도를 입력합니다.
소스	이 개체 기록이 생성되는 위협 소스를 지정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
해지함	해지된 개체가 개체 작성자에 의해 더 이상 유효한 것으로 간주되지 않음을 나타냅니다.

인사이트

필드	설명
메모	캠페인에 대한 메모를 추가합니다.

추가 정보

필드	설명
추가 컨텍스트	이 캠페인에 대한 추가 컨텍스트를 추가합니다.
처음으로 발견됨	이 객체가 적대적 행동을 수행하는 것을 처음 본 시간입니다.
마지막으로 발견됨	이 객체가 적대적 동작을 수행하는 것이 마지막으로 목격된 시간입니다.
사양 버전	이 객체를 나타내는 데 사용되는 STIX 사양의 버전입니다. 이 특성에 대한 값은 이 사양에 따라 정의된 STIX 객체에 대해 2.1이어야 합니다.
언어	이 속성은 이 객체의 텍스트 컨텐츠 언어를 식별합니다.
작성됨	원본에서 객체가 만들어진 날짜 및 시간을 지정합니다.
확장명	공격 패턴의 확장을 나타냅니다.
업데이트됨	원본에서 객체가 업데이트된 날짜 및 시간을 지정합니다.
처리 상태	캠페인인 이 개체의 처리 상태를 나타냅니다.

6. 저장을 클릭합니다.
   저장하면 새 옵저버블 기록이 생성되었음을 나타내는 프롬프트 메시지가 표시됩니다. 기록을 편집하고 새 관계를 생성하려면 "계속 "을 클릭하십시오.
7. 계속을 클릭합니다.

> **중요사항:**
> 새 옵저버블 기록을 생성하면 시스템 업데이트 방지 확인란이 표시됩니다.
>
> 옵저버블, 표시기 또는 STIX 객체 기록이 생성된 후 시스템에서 업데이트를 방지하려면 이 확인란을 선택합니다.

태그&분류

필드	설명
태그	
태그 선택	캠페인과 연결된 태그를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
태그 추가	새 태그를 추가합니다.
분류	
분류 선택	캠페인과 연관된 분류를 선택합니다.
분류 값 추가	캠페인과 연결된 분류 값을 추가합니다.

다음에 수행할 작업
이제 다음 관련 목록 중 하나를 클릭하여 캠페인과 연관된 객체에 대한 추가 정보를 볼 수 있습니다.

관련 기록

필드	설명
외부 참조	STIX가 아닌 정보를 참조하는 외부 참조를 나열합니다. 이 속성은 하나 이상의 외부 객체 식별자를 제공하는 데 사용됩니다.
공격 패턴	이 객체와 관련된 공격을 분류하는 데 도움이 되는 공격 패턴을 나열합니다.
ID	이 객체와 연결된 ID 목록입니다.
표시기	이 개체와 연결된 위협 소스에서 식별한 관련 IoC(침해 표시기)를 나열합니다.
인프라	시스템, 소프트웨어 서비스 및 이 객체와 연결된 연결된 모든 물리적 또는 가상 자원을 나열합니다.
침입 세트	이 객체와 관련된 공통 속성이 있는 일련의 적대적 동작 및 자원을 나열합니다.
위치	이 객체에 지리적 컨텍스트를 제공하는 위치를 나열합니다.
맬웨어	이 객체와 연결된 악성 코드를 나열합니다.
마케팅 정의	이 객체와 연결된 마케팅 정의를 나열합니다.
사이팅	이 객체와 연결된 사이팅을 나열합니다.
위협 액터	이 객체와 관련하여 악의적인 의도를 가지고 행동하는 개인, 그룹 또는 조직을 나열합니다.
도구	위협 행위자가 이 개체와 관련된 공격을 수행하는 데 사용하는 합법적인 소프트웨어를 나열합니다.
취약성	공격자가 악용하는 소프트웨어 또는 하드웨어의 약점 또는 결함을 나열합니다. 이 개체와 관련되어 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

1. 이 객체와 연결된 관련 기록을 연결하거나 연결 해제할 수 있습니다. 자세한 내용은 위협 인텔리전스 관련 기록 연결 문서를 참조하십시오.
2. TI 라이브러리 내의 다양한 SDO에는 잠재적인 관계도 포함됩니다. 두 개체 간의 관계를 설정하려면 위협 인텔리전스 라이브러리의 **Potential** Relationships(잠재적 관계) 링크를 사용하여 개체 간의 관계를 확인합니다. 자세한 내용은 객체-객체 잠재성 관계 확인 문서를 참조하십시오.
3. 또한 객체 양식 뷰에서 관련 기록 섹션을 사용하면 양식 뷰에서 사용할 수 있는 잠재성 관계 섹션을 통해 두 객체 간의 관계를 확인할 수 있습니다. 에 대한 자세한 내용은 관련 기록에서 잠재성 관계 확인를 참조하십시오.
4. 케이스에 개체를 추가할 수 있습니다. 자세한 내용은 케이스에 추가 문서를 참조하십시오.

작업 과정

동작 방침은 공격을 방지하거나 진행 중인 공격에 대응하기 위해 취하는 동작입니다.

동작 방침에서는 패치 적용, 방화벽 재구성 등의 기술적 또는 자동화된 대응을 설명합니다. 또한 직원 교육 또는 정책 변경과 같은 상위 수준의 작업을 설명할 수도 있습니다.

예를 들어, 취약성을 완화하기 위한 동작 방침은 취약성을 수정하는 패치를 적용하는 것을 설명할 수 있습니다.

동작 방침 정의

공격을 방지하거나 진행 중인 공격에 대응하기 위한 작업 방침을 정의합니다.

시작하기 전에

필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 작업 공간에서 위협 인텔 라이브러리 아이콘을 클릭합니다.
3. 동작 과정 객체로 이동합니다.
4. 새로 만들기를 클릭합니다.

   주:
   옵저버블, 표시기, 엔터티 또는 객체에 대한 새 객체 기록을 생성할 때마다 소스 기록이 생성되고, 새 객체 기록이 생성된 다음 사용자가 집계된 기록으로 리디렉션된다는 프롬프트 메시지가 표시됩니다.

5. 양식에서 필드를 채웁니다.

작업 방침 상세 정보 뷰

필드	설명
ID	공격을 방지하기 위한 작업 과정의 고유 ID입니다.
이름	이 작업 과정을 설명하는 이름을 입력합니다.
설명	목적과 주요 특성을 포함하여 작업 과정에 대한 자세한 내용과 컨텍스트를 제공하는 설명입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
작업	구조화되거나 자동화된 작업 과정을 캡처합니다.
TLP	TLP(Traffic Light Protocol)는 올바른 대상과 공유되는 중요한 정보를 나타냅니다. 4가지 색상(흰색, 녹색, 호박색 및 빨간색)을 사용하여 이 공격 패턴에 대한 다양한 민감도를 나타냅니다.
신뢰도	이 작업 과정에 대한 신뢰도를 입력합니다.
소스	이 개체 기록이 생성되는 위협 소스를 지정합니다.
해지함	해지된 개체가 개체 작성자에 의해 더 이상 유효한 것으로 간주되지 않음을 나타냅니다.

인사이트

필드	설명
메모	작업 과정에 대한 추가 메모를 추가합니다.

추가 정보

필드	설명
추가 컨텍스트	이 공격 패턴에 대한 추가 컨텍스트를 추가합니다.
사양 버전	이 객체를 나타내는 데 사용되는 STIX 사양의 버전입니다. 이 특성에 대한 값은 이 사양에 따라 정의된 STIX 객체에 대해 2.1이어야 합니다.
언어	이 속성은 이 객체의 텍스트 컨텐츠 언어를 식별합니다.
소스에서 생성된 시간	원본에서 개체가 만들어지는 시간을 지정합니다.
확장명	공격 패턴의 확장을 나타냅니다.
소스에서 수정된 시간	원본에서 개체가 수정되는 시간을 지정합니다.
처리 상태	이 객체의 처리 상태, 작업 과정을 나타냅니다.
작성됨	원본에서 객체가 만들어진 날짜 및 시간을 지정합니다.
업데이트됨	원본에서 객체가 업데이트된 날짜 및 시간을 지정합니다.
참조에 의해 생성됨	

6. 저장을 클릭합니다.
   저장하면 새 옵저버블 기록이 생성되었음을 나타내는 프롬프트 메시지가 표시됩니다. 기록을 편집하고 새 관계를 생성하려면 "계속 "을 클릭하십시오.
7. 계속을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

중요사항:
새 옵저버블 기록을 생성하면 시스템 업데이트 방지 확인란이 표시됩니다.

옵저버블, 표시기 또는 STIX 객체 기록이 생성된 후 시스템에서 업데이트를 방지하려면 이 확인란을 선택합니다.

태그&분류

필드	설명
태그	
태그 선택	옵저버블과 연결된 태그를 선택합니다.
태그 추가	새 태그를 추가합니다.
분류	
분류 선택	공격 패턴과 연결된 분류를 선택합니다.
분류 값 추가	공격 패턴과 연결된 분류 값을 추가합니다.

다음에 수행할 작업

작업 과정과 연결된 객체에 대한 추가 정보를 보려면 다음 관련 목록 중 하나를 클릭하십시오.

관련 기록

필드	설명
외부 참조	STIX가 아닌 정보를 참조하는 외부 참조를 나열합니다. 이 속성은 하나 이상의 외부 객체 식별자를 제공하는 데 사용됩니다.
공격 패턴	이 객체와 관련된 공격을 분류하는 데 도움이 되는 공격 패턴을 나열합니다.
표시기	이 개체와 연결된 위협 소스에서 식별한 관련 IoC(침해 표시기)를 나열합니다.
맬웨어	이 객체와 연결된 악성 코드를 나열합니다.
마케팅 정의	이 객체와 연결된 마케팅 정의를 나열합니다.
옵저버블	이 객체와 연결된 옵저버블을 나열합니다.
사이팅	이 객체와 연결된 사이팅을 나열합니다.
도구	위협 행위자가 이 개체와 관련된 공격을 수행하는 데 사용하는 합법적인 소프트웨어를 나열합니다.
취약성	공격자가 악용하는 소프트웨어 또는 하드웨어의 약점 또는 결함을 나열합니다. 이 개체와 관련되어 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

1. 이 객체와 연결된 관련 기록을 연결하거나 연결 해제할 수 있습니다. 자세한 내용은 위협 인텔리전스 관련 기록 연결 문서를 참조하십시오.
2. TI 라이브러리 내의 다양한 SDO에는 잠재적인 관계도 포함됩니다. 두 개체 간의 관계를 설정하려면 위협 인텔리전스 라이브러리의 **Potential** Relationships(잠재적 관계) 링크를 사용하여 개체 간의 관계를 확인합니다. 자세한 내용은 객체-객체 잠재성 관계 확인 문서를 참조하십시오.
3. 또한 객체 양식 뷰에서 관련 기록 섹션을 사용하면 양식 뷰에서 사용할 수 있는 잠재성 관계 섹션을 통해 두 객체 간의 관계를 확인할 수 있습니다. 에 대한 자세한 내용은 관련 기록에서 잠재성 관계 확인를 참조하십시오.
4. 케이스에 개체를 추가할 수 있습니다. 자세한 내용은 케이스에 추가 문서를 참조하십시오.

ID

ID는 실제 개인, 조직 또는 그룹 및 개인, 시스템 또는 그룹의 클래스를 나타냅니다. ID는 STIX 2.x에 적용됩니다.

ID SDO는 기본 식별 정보, 연락처 정보 및 ID가 속한 섹터를 캡처할 수 있습니다. ID는 공격의 대상, 정보 소스, 개체 생성자 및 위협 행위자 ID를 나타냅니다.

ID 정의

실제 개인, 조직 또는 그룹을 나타내는 ID를 정의합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 작업 공간에서 위협 인텔 라이브러리 아이콘을 클릭합니다.
3. **ID** 개체로 이동합니다.
4. 새로 만들기를 클릭합니다.

   주:
   옵저버블, 표시기, 엔터티 또는 객체에 대한 새 객체 기록을 생성할 때마다 소스 기록이 생성되고, 새 객체 기록이 생성된 다음 사용자가 집계된 기록으로 리디렉션된다는 프롬프트 메시지가 표시됩니다.

5. 양식에서 필드를 채웁니다.

ID 상세 정보 뷰

필드	설명
ID	ID의 고유 ID입니다.
이름	이 ID를 설명하는 이름을 입력합니다. 특정 엔터티(개인 또는 조직)를 참조할 때 이 속성에는 특정 엔터티의 정식 이름이 포함되어야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
설명	목적과 주요 특성을 포함하여 작업 과정에 대한 자세한 내용과 컨텍스트를 제공하는 설명입니다.
역할	이 ID가 수행하는 역할 목록입니다.
신원 클래스	이 ID가 설명하는 엔터티 유형입니다. 예를 들어 개인 또는 조직입니다.
섹터	이 ID가 속한 산업 부문 목록입니다.
연락처 정보	이 ID의 이메일 및 전화번호 등의 연락처 정보입니다.
TLP	TLP는 민감한 정보가 적절한 대상과 공유되도록 하는 데 사용됩니다. 4가지 색상(흰색, 녹색, 호박색, 빨간색)을 사용하여 다양한 민감도를 나타냅니다.
신뢰도	이 ID에 대한 신뢰도를 입력합니다.
소스	이 개체 기록이 생성되는 위협 소스를 지정합니다.
해지함	해지된 개체가 개체 작성자에 의해 더 이상 유효한 것으로 간주되지 않음을 나타냅니다.

인사이트

필드	설명
메모	ID에 대한 추가 메모를 추가합니다.

추가 정보

필드	설명
추가 컨텍스트	이 ID와 관련된 추가 컨텍스트를 추가합니다.
사양 버전	이 객체를 나타내는 데 사용되는 STIX 사양의 버전입니다. 이 특성에 대한 값은 이 사양에 따라 정의된 STIX 객체에 대해 2.1이어야 합니다.
언어	이 속성은 이 객체의 텍스트 컨텐츠 언어를 식별합니다.
소스에서 생성된 시간	원본에서 개체가 만들어지는 시간을 지정합니다.
확장명	공격 패턴의 확장을 나타냅니다.
소스에서 수정된 시간	원본에서 개체가 수정되는 시간을 지정합니다.
처리 상태	이 객체의 처리 상태, 작업 과정을 나타냅니다.
작성됨	원본에서 객체가 만들어진 날짜 및 시간을 지정합니다.
업데이트됨	원본에서 객체가 업데이트된 날짜 및 시간을 지정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
참조에 의해 생성됨	이 속성은 엔터티를 설명하는 ID 개체가 이 개체를 만들었음을 지정합니다.

6. 저장을 클릭합니다.
   저장하면 새 옵저버블 기록이 생성되었음을 나타내는 프롬프트 메시지가 표시됩니다. 기록을 편집하고 새 관계를 생성하려면 "계속 "을 클릭하십시오.
7. 계속을 클릭합니다.

> **중요사항:**
> 새 옵저버블 기록을 생성하면 시스템 업데이트 방지 확인란이 표시됩니다.
>
> 옵저버블, 표시기 또는 STIX 객체 기록이 생성된 후 시스템에서 업데이트를 방지하려면 이 확인란을 선택합니다.

태그&분류

필드	설명
태그	
태그 선택	자격 증명과 연결된 태그를 선택합니다.
태그 추가	새 태그를 추가합니다.
분류	
분류 선택	ID와 연결된 분류를 선택합니다.
분류 값 추가	ID와 연결된 분류 값을 추가합니다.

다음에 수행할 작업

ID와 연결된 객체에 대한 추가 정보를 보려면 다음 관련 목록 중 하나를 클릭하십시오.

관련 기록

필드	설명
외부 참조	STIX가 아닌 정보를 참조하는 외부 참조를 나열합니다. 이 속성은 하나 이상의 외부 객체 식별자를 제공하는 데 사용됩니다.
공격 패턴	이 객체와 관련된 공격을 분류하는 데 도움이 되는 공격 패턴을 나열합니다.
캠페인	이 개체와 연결된 위협 소스에서 식별한 관련 IoC(침해 표시기)를 나열합니다.
침입 세트	이 객체와 관련된 공통 속성이 있는 일련의 적대적 동작 및 자원을 나열합니다.
위치	이 객체에 지리적 컨텍스트를 제공하는 위치를 나열합니다.
맬웨어	이 객체와 연결된 악성 코드를 나열합니다.
마케팅 정의	이 객체와 연결된 마케팅 정의를 나열합니다.
사이팅	이 객체와 연결된 사이팅을 나열합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관련 기록

필드	설명
위협 액터	이 객체와 관련하여 악의적인 의도를 가지고 행동하는 개인, 그룹 또는 조직을 나열합니다.
도구	위협 행위자가 이 개체와 관련된 공격을 수행하는 데 사용하는 합법적인 소프트웨어를 나열합니다.

주:

1. 이 객체와 연결된 관련 기록을 연결하거나 연결 해제할 수 있습니다. 자세한 내용은 위협 인텔리전스 관련 기록 연결 문서를 참조하십시오.
2. TI 라이브러리 내의 다양한 SDO에는 잠재적인 관계도 포함됩니다. 두 개체 간의 관계를 설정하려면 위협 인텔리전스 라이브러리의 **Potential** Relationships(잠재적 관계) 링크를 사용하여 개체 간의 관계를 확인합니다. 자세한 내용은 객체-객체 잠재성 관계 확인 문서를 참조하십시오.
3. 또한 객체 양식 뷰에서 관련 기록 섹션을 사용하면 양식 뷰에서 사용할 수 있는 잠재성 관계 섹션을 통해 두 객체 간의 관계를 확인할 수 있습니다. 에 대한 자세한 내용은 관련 기록에서 잠재성 관계 확인를 참조하십시오.
4. 케이스에 개체를 추가할 수 있습니다. 자세한 내용은 케이스에 추가 문서를 참조하십시오.

인프라

인프라 SDO는 전술, 기술 및 절차(TTP)의 한 유형을 나타냅니다. 공격의 특정 목적을 지원하기 위한 모든 시스템, 소프트웨어 서비스 및 관련된 물리적 또는 가상 자원을 설명합니다. 인프라는 STIX 2.x에 적용됩니다.

공격 요소는 다른 SDO 또는 SCO로 표시됩니다. 그러나 인프라 SDO는 인프라를 구성하는 명명된 데이터 그룹을 나타냅니다.

인프라의 예로는 공격에 사용되는 C2 서버, 장치 또는 방어의 일부인 서버 또는 공격의 대상이 되는 데이터베이스 서버가 있습니다.

인프라 정의

인프라스트럭처, 즉 공격의 특정 목적을 지원하기 위한 시스템, 소프트웨어 서비스 및 관련된 물리적 또는 가상 자원을 정의합니다.

시작하기 전에

필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 작업 공간에서 위협 인텔 라이브러리 아이콘을 클릭합니다.
3. 인프라 개체로 이동합니다.
4. 새로 만들기를 클릭합니다.

주:
옵저버블, 표시기, 엔터티 또는 객체에 대한 새 객체 기록을 생성할 때마다 소스 기록이 생성되고, 새 객체 기록이 생성된 다음 사용자가 집계된 기록으로 리디렉션된다는 프롬프트 메시지가 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. 양식에서 필드를 채웁니다.

인프라 상세 정보 뷰

필드	설명
ID	공격을 방지하기 위한 작업 과정의 고유 ID입니다.
이름	이 작업 과정에 대한 설명이 포함된 이름을 입력합니다. 특정 엔터티(개인 또는 조직)를 참조할 때 이 속성에는 특정 엔터티의 정식 이름이 포함되어야 합니다.
설명	인프라의 목적, 사용 방법, 관련 개체에서 캡처한 다른 인텔리전스 활동과의 관련성 및 주요 특성을 포함하여 인프라에 대한 자세한 내용과 컨텍스트를 제공하는 설명입니다.
인프라 유형	인프라 분류에 대해 설명합니다.
별칭	이 인프라를 식별하는 대체 이름입니다. **주:** 애플리케이션에 없는 새 별칭을 추가하려면 별칭 필드 자체에 있는 새 별칭 추가 아이콘을 클릭합니다.
공격 단계	LM, MITRE ATT&CK와 같은 킬 체인의 공격 단계를 나타냅니다.
TLP	TLP는 민감한 정보가 적절한 대상과 공유되도록 하는 데 사용됩니다. 4가지 색상(흰색, 녹색, 호박색, 빨간색)을 사용하여 다양한 민감도를 나타냅니다.
처음으로 발견됨	이 인프라가 악의적인 활동을 수행하는 것이 처음 목격된 시간입니다.
마지막으로 발견됨	이 인프라가 악의적인 활동을 수행하는 것이 마지막으로 목격된 시간입니다.
신뢰도	이 작업 과정에 대한 신뢰도를 입력합니다.
소스	이 개체 기록이 생성되는 위협 소스를 지정합니다.
해지함	해지된 개체가 개체 작성자에 의해 더 이상 유효한 것으로 간주되지 않음을 나타냅니다.

인사이트

필드	설명
메모	이 인프라에 대한 추가 메모를 추가합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

추가 정보

필드	설명
추가 컨텍스트	이 인프라에 대한 추가 컨텍스트를 추가합니다.
사양 버전	이 객체를 나타내는 데 사용되는 STIX 사양의 버전입니다. 이 특성에 대한 값은 이 사양에 따라 정의된 STIX 객체에 대해 2.1이어야 합니다.
언어	이 속성은 이 객체의 텍스트 컨텐츠 언어를 식별합니다.
소스에서 생성된 시간	원본에서 개체가 만들어지는 시간을 지정합니다.
확장명	공격 패턴의 확장을 나타냅니다.
소스에서 수정된 시간	원본에서 개체가 수정되는 시간을 지정합니다.
처리 상태	이 객체의 처리 상태, 작업 과정을 나타냅니다.
작성됨	소스에서 기록이 생성되는 시간을 지정합니다.
업데이트됨	소스에서 기록이 수정되는 시간을 지정합니다.
참조에 의해 생성됨	이 속성은 엔터티를 설명하는 ID 개체가 이 개체를 만들었음을 지정합니다.

6. 저장을 클릭합니다.
   저장하면 새 옵저버블 기록이 생성되었음을 나타내는 프롬프트 메시지가 표시됩니다. 기록을 편집하고 새 관계를 생성하려면 "계속 "을 클릭하십시오.
7. 계속을 클릭합니다.

중요사항:
새 옵저버블 기록을 생성하면 시스템 업데이트 방지 확인란이 표시됩니다.

옵저버블, 표시기 또는 STIX 객체 기록이 생성된 후 시스템에서 업데이트를 방지하려면 이 확인란을 선택합니다.

태그&분류

필드	설명
태그	
태그 선택	인프라와 연결된 태그를 선택합니다.
태그 추가	새 태그를 추가합니다.
분류	
분류 선택	이 인프라와 연결된 분류를 선택합니다.
분류 값 추가	이 인프라와 연결된 분류 값을 추가합니다.

다음에 수행할 작업

ID와 연결된 객체에 대한 추가 정보를 보려면 다음 관련 목록 중 하나를 클릭하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관련 기록

필드	설명
외부 참조	STIX가 아닌 정보를 참조하는 외부 참조를 나열합니다. 이 속성은 하나 이상의 외부 객체 식별자를 제공하는 데 사용됩니다.
캠페인	이 객체와 연결된 캠페인을 나열합니다.
표시기	이 개체와 연결된 위협 소스에서 식별한 관련 IoC(침해 표시기)를 나열합니다.
인프라	시스템, 소프트웨어 서비스 및 이 객체와 연결된 연결된 모든 물리적 또는 가상 자원을 나열합니다.
침입 세트	이 객체와 관련된 공통 속성이 있는 일련의 적대적 동작 및 자원을 나열합니다.
위치	이 객체에 지리적 컨텍스트를 제공하는 위치를 나열합니다.
맬웨어	이 객체와 관련된 악성 코드를 나열합니다.
마케팅 정의	이 객체와 연결된 마케팅 정의를 나열합니다.
사이팅	이 객체와 연결된 사이팅을 나열합니다.
옵저버블	이 객체와 연결된 옵저버블을 나열합니다.
관찰 데이터	이 객체와 연결된 관찰 데이터를 나열합니다.
위협 액터	이 객체와 관련하여 악의적인 의도를 가지고 행동하는 개인, 그룹 또는 조직을 나열합니다.
도구	위협 행위자가 이 개체와 관련된 공격을 수행하는 데 사용하는 합법적인 소프트웨어를 나열합니다.
취약성	공격자가 악용하는 소프트웨어 또는 하드웨어의 약점 또는 결함을 나열합니다. 이 개체와 관련되어 있습니다.

주:

1. 이 객체와 연결된 관련 기록을 연결하거나 연결 해제할 수 있습니다. 자세한 내용은 위협 인텔리전스 관련 기록 연결 문서를 참조하십시오.
2. TI 라이브러리 내의 다양한 SDO에는 잠재적인 관계도 포함됩니다. 두 개체 간의 관계를 설정하려면 위협 인텔리전스 라이브러리의 **Potential** Relationships(잠재적 관계) 링크를 사용하여 개체 간의 관계를 확인합니다. 자세한 내용은 객체-객체 잠재성 관계 확인 문서를 참조하십시오.
3. 또한 객체 양식 뷰에서 관련 기록 섹션을 사용하면 양식 뷰에서 사용할 수 있는 잠재성 관계 섹션을 통해 두 객체 간의 관계를 확인할 수 있습니다. 에 대한 자세한 내용은 관련 기록에서 잠재성 관계 확인를 참조하십시오.
4. 케이스에 개체를 추가할 수 있습니다. 자세한 내용은 케이스에 추가 문서를 참조하십시오.

침입 세트

침입 세트는 공통 속성을 가진 적대적 행동 및 자원의 그룹화된 집합입니다. 침입 세트에는 일반적으로 단일 조직이 포함됩니다. 침입 세트는 STIX 2.x에 적용됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

침입 세트는 여러 캠페인 또는 기타 활동을 캡처할 수 있습니다. 이러한 활동은 일반적으로 알려지거나 알려지지 않은 위협 액터를 나타내는 속성을 공유합니다.

새로운 활동은 공격 배후의 위협 액터를 알지 못하는 경우에도 침입 세트에 기인할 수 있습니다. 위협 액터는 하나의 침입 세트 지원에서 다른 침입 세트 지원으로 이동하거나 여러 침입 세트를 지원할 수 있습니다.

침입 세트는 전체 공격 패키지이며 잠재적으로 여러 목적을 달성하기 위해 여러 캠페인에서 장기간에 걸쳐 사용될 수 있습니다.

침입 세트 정의

공통 속성을 가진 적대적 행동 및 자원의 그룹화된 집합인 침입 집합을 정의합니다.

시작하기 전에

필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 작업 공간에서 위협 인텔 라이브러리 아이콘을 클릭합니다.
3. 침입 세트로 이동합니다.
4. 새로 만들기를 클릭합니다.

   주:
   옵저버블, 표시기, 엔터티 또는 객체에 대한 새 객체 기록을 생성할 때마다 소스 기록이 생성되고, 새 객체 기록이 생성된 다음 사용자가 집계된 기록으로 리디렉션된다는 프롬프트 메시지가 표시됩니다.

5. 양식에서 필드를 채웁니다.

   침입 세트 세부 정보 보기

필드	설명
ID	침입 집합의 고유 ID입니다.
이름	이 침입 집합에 대한 설명이 포함된 이름을 입력합니다. 특정 엔터티(개인 또는 조직)를 참조할 때 이 속성에는 특정 엔터티의 정식 이름이 포함되어야 합니다.
설명	침입 세트의 목적과 주요 특성을 포함하여 침입 집합에 대한 자세한 내용과 컨텍스트를 제공하는 설명입니다.
별칭	이 침입 세트를 식별하는 대체 이름입니다. **주:** 애플리케이션에 없는 새 별칭을 추가하려면 별칭 필드 자체에 있는 새 별칭 추가 아이콘을 클릭합니다.
목표	이 침입 세트의 개략적인 목표, 즉 무엇을 하려고 하는가.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	예를 들어, 그들은 개인적인 이익을 위해 동기를 부여받을 수 있지만 목표는 신용 카드 번호를 훔치는 것입니다. 이를 위해 대형 소매업체의 POS 시스템을 손상시키는 것과 같은 자세한 목표가 있는 특정 캠페인을 실행할 수 있습니다.
처음으로 발견됨	이 침입 세트가 악의적인 활동을 수행하는 것이 처음 목격된 시간입니다.
마지막으로 발견됨	이 침입 세트가 악의적인 활동을 수행하는 것이 마지막으로 목격된 시간입니다.
기본 동기	이 침입 세트의 기본 이유, 동기 또는 목적입니다. 동기는 침입 세트가 목표(달성하려는 것)를 달성하고자 하는 이유입니다.
보조 동기	이 침입 세트의 이차적인 이유, 동기 또는 목적입니다. 이러한 동기는 일차적 동기와 동등하거나 거의 동등한 원인으로 존재할 수 있다. 그러나 주요 동기를 대체하거나 반드시 확대하지는 않지만 추가 컨텍스트를 나타낼 수 있습니다. 목록의 위치는 중요하지 않습니다.
자원 수준	이 속성은 이 침입 집합이 일반적으로 작동하는 조직 수준을 지정하며, 이에 따라 공격에 사용하기 위해 이 침입 집합에 사용할 수 있는 자원이 결정됩니다.
TLP	TLP는 민감한 정보가 적절한 대상과 공유되도록 하는 데 사용됩니다. 4가지 색상(흰색, 녹색, 호박색, 빨간색)을 사용하여 다양한 민감도를 나타냅니다.
신뢰도	이 침입 집합에 대한 신뢰도를 입력합니다.
소스	이 개체 기록이 생성되는 위협 소스를 지정합니다.
해지함	해지된 개체가 개체 작성자에 의해 더 이상 유효한 것으로 간주되지 않음을 나타냅니다.

인사이트

필드	설명
메모	이 침입 집합에 대한 추가 메모를 추가합니다.

추가 정보

필드	설명
추가 컨텍스트	이 침입 집합에 대한 추가 컨텍스트를 추가합니다.
사양 버전	이 객체를 나타내는 데 사용되는 STIX 사양의 버전입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	이 특성에 대한 값은 이 사양에 따라 정의된 STIX 객체에 대해 2.1이어야 합니다.
언어	이 속성은 이 객체의 텍스트 컨텐츠 언어를 식별합니다.
소스에서 생성된 시간	소스에서 기록이 생성되는 시간을 지정합니다.
확장명	공격 패턴의 확장을 나타냅니다.
소스에서 수정된 시간	원본에서 개체가 수정되는 시간을 지정합니다.
처리 상태	이 객체의 처리 상태, 작업 과정을 나타냅니다.
작성됨	소스에서 기록이 생성되는 시간을 지정합니다.
업데이트됨	소스에서 기록이 수정되는 시간을 지정합니다.
참조에 의해 생성됨	이 속성은 엔터티를 설명하는 ID 개체가 이 개체를 만들었음을 지정합니다.

6. 저장을 클릭합니다.
   저장하면 새 옵저버블 기록이 생성되었음을 나타내는 프롬프트 메시지가 표시됩니다. 기록을 편집하고 새 관계를 생성하려면 "계속 "을 클릭하십시오.
7. 계속을 클릭합니다.

중요사항:
새 옵저버블 기록을 생성하면 시스템 업데이트 방지 확인란이 표시됩니다.

옵저버블, 표시기 또는 STIX 객체 기록이 생성된 후 시스템에서 업데이트를 방지하려면 이 확인란을 선택합니다.

태그&분류

필드	설명
태그	
태그 선택	침입 집합과 연결된 태그를 선택합니다.
태그 추가	새 태그를 추가합니다.
분류	
분류 선택	이 침입 집합과 연결된 분류를 선택합니다.
분류 값 추가	이 침입 집합과 연결된 분류 값을 추가합니다.

다음에 수행할 작업

침입 집합과 연결된 개체에 대한 추가 정보를 보려면 다음 관련 목록 중 하나를 클릭합니다.

관련 기록

필드	설명
외부 참조	STIX가 아닌 정보를 참조하는 외부 참조를 나열합니다. 이 속성은 하나 이상의 외부 객체 식별자를 제공하는 데 사용됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관련 기록

필드	설명
공격 패턴	이 객체와 관련된 공격을 분류하는 데 도움이 되는 공격 패턴을 나열합니다.
캠페인	이 객체와 연결된 캠페인을 나열합니다.
ID	이 객체와 연결된 ID 목록입니다.
표시기	이 개체와 연결된 위협 소스에서 식별한 관련 IoC(침해 표시기)를 나열합니다.
인프라	시스템, 소프트웨어 서비스 및 이 객체와 연결된 연결된 모든 물리적 또는 가상 자원을 나열합니다.
위치	이 객체에 지리적 컨텍스트를 제공하는 위치를 나열합니다.
맬웨어	이 객체와 관련된 악성 코드를 나열합니다.
마케팅 정의	이 객체와 연결된 마케팅 정의를 나열합니다.
사이팅	이 객체와 연결된 사이팅을 나열합니다.
위협 액터	이 객체와 관련하여 악의적인 의도를 가지고 행동하는 개인, 그룹 또는 조직을 나열합니다.
도구	위협 행위자가 이 개체와 관련된 공격을 수행하는 데 사용하는 합법적인 소프트웨어를 나열합니다.
취약성	공격자가 악용하는 소프트웨어 또는 하드웨어의 약점 또는 결함을 나열합니다. 이 개체와 관련되어 있습니다.

주:

1. 이 객체와 연결된 관련 기록을 연결하거나 연결 해제할 수 있습니다. 자세한 내용은 위협 인텔리전스 관련 기록 연결 문서를 참조하십시오.
2. TI 라이브러리 내의 다양한 SDO에는 잠재적인 관계도 포함됩니다. 두 개체 간의 관계를 설정하려면 위협 인텔리전스 라이브러리의 **Potential** Relationships(잠재적 관계) 링크를 사용하여 개체 간의 관계를 확인합니다. 자세한 내용은 객체-객체 잠재성 관계 확인 문서를 참조하십시오.
3. 또한 객체 양식 뷰에서 관련 기록 섹션을 사용하면 양식 뷰에서 사용할 수 있는 잠재성 관계 섹션을 통해 두 객체 간의 관계를 확인할 수 있습니다. 에 대한 자세한 내용은 관련 기록에서 잠재성 관계 확인를 참조하십시오.
4. 케이스에 개체를 추가할 수 있습니다. 자세한 내용은 케이스에 추가 문서를 참조하십시오.

위치

위치는 지리적 위치를 나타냅니다. 위치는 주로 다른 SDO에 컨텍스트를 제공하는 데 사용됩니다. 위치는 STIX 2.x를 신청합니다.

위치에는 지역(북미), 시민 주소(뉴욕, 미국), 위도 및 경도의 일부 또는 전부가 포함될 수 있습니다.

위치 SDO는 ID 또는 침입 집합이 해당 위치에 있음을 나타내기 위해 ID 또는 침입 집합과 관련될 수 있습니다. 또한 맬웨어 또는 공격 패턴과 관련되어 대상 피해자가 특정 위치에 있음을 나타낼 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예를 들어, 위치는 부르주아 제비 침입 집합이 동유럽에서 유래했음을 설명하기 위해 관계에서 사용될 수 있습니다.

다음 속성 또는 속성 집합 중 하나 이상을 제공해야 합니다.

- 지역
- 국가
- 위도 및 경도

위치 정의

다른 SDO에 더 많은 컨텍스트를 제공하기 위해 지리적 위치를 정의하십시오.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 작업 공간에서 위협 인텔 라이브러리 아이콘을 클릭합니다.
3. 위치 객체로 이동합니다.
4. 새로 만들기를 클릭합니다.

   주:
   옵저버블, 표시기, 엔터티 또는 객체에 대한 새 객체 기록을 생성할 때마다 소스 기록이 생성되고, 새 객체 기록이 생성된 다음 사용자가 집계된 기록으로 리디렉션된다는 프롬프트 메시지가 표시됩니다.

5. 폼의 필드에 내용을 입력합니다.

ID 상세 정보 뷰

필드	설명
ID	위치의 고유 ID입니다.
이름	위치를 식별하기 위한 설명이 포함된 이름을 입력합니다.
설명	침입 세트의 목적과 주요 특성을 포함하여 침입 집합에 대한 자세한 내용과 컨텍스트를 제공하는 설명입니다.
위도	위치의 위도(십진수)입니다. 양수는 적도 북쪽의 위도를 나타내고 음수는 적도 남쪽의 위도를 나타냅니다. 이 속성의 값은 각각 -90.0에서 90.0 사이여야 합니다.
경도	위치의 경도(십진수)입니다. 양수는 본초 자오선 동쪽의 경도를 나타내고 음수는 본초 자오선 서쪽의 경도를 나타냅니다. 이 속성의 값은 -180.0에서 180.0 사이여야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
정확도	latitude 및 longitude 속성으로 지정된 좌표의 정밀도를 정의합니다. 이것은 미터 단위로 측정됩니다. 실제 위치는 정의된 지점에서 최대 정밀도 미터까지 어디에나 있을 수 있습니다. 이 속성이 없으면 정밀도가 지정되지 않습니다. 이 속성이 있는 경우 latitude 및 longitude 속성이 있어야 합니다.
지역	이 위치가 있는 지역입니다.
국가	이 위치가 위치한 국가입니다.
관리 영역	이 위치가 위치한 시,도 또는 기타 하위 국가 행정 구역입니다.
구/군/시	이 위치가 위치한 도시입니다.
거리 주소	이 위치가 설명하는 도로명 주소입니다. 이 숙박 시설에는 도로명 주소의 모든 측면 또는 일부가 포함됩니다.
우편 번호	이 위치가 위치한 우편 번호입니다.
신뢰도	이 작업 과정에 대한 신뢰도를 입력합니다.
TLP	TLP는 민감한 정보가 적절한 대상과 공유되도록 하는 데 사용됩니다. 4가지 색상(흰색, 녹색, 호박색, 빨간색)을 사용하여 다양한 민감도를 나타냅니다.
소스	이 개체 기록이 생성되는 위협 소스를 지정합니다.
해지함	해지된 개체가 개체 작성자에 의해 더 이상 유효한 것으로 간주되지 않음을 나타냅니다.

인사이트

필드	설명
메모	이 위치에 대한 추가 메모를 추가합니다.

추가 정보

필드	설명
추가 컨텍스트	이 위치에 대한 추가 컨텍스트를 추가합니다.
사양 버전	이 객체를 나타내는 데 사용되는 STIX 사양의 버전입니다. 이 특성에 대한 값은 이 사양에 따라 정의된 STIX 객체에 대해 2.1이어야 합니다.
언어	이 속성은 이 객체의 텍스트 컨텐츠 언어를 식별합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
소스에서 생성된 시간	원본에서 개체가 만들어지는 시간을 지정합니다.
확장명	이 위치의 확장명을 나타냅니다.
소스에서 수정된 시간	원본에서 개체가 수정되는 시간을 지정합니다.
처리 상태	이 객체의 처리 상태, 작업 과정을 나타냅니다.
작성됨	소스에서 기록이 생성되는 시간을 지정합니다.
업데이트됨	소스에서 기록이 수정되는 시간을 지정합니다.
참조에 의해 생성됨	이 속성은 엔터티를 설명하는 ID 개체가 이 개체를 만들었음을 지정합니다.

6. 저장을 클릭합니다.
   저장하면 새 옵저버블 기록이 생성되었음을 나타내는 프롬프트 메시지가 표시됩니다. 기록을 편집하고 새 관계를 생성하려면 "계속 "을 클릭하십시오.
7. 계속을 클릭합니다.

중요사항:
새 옵저버블 기록을 생성하면 시스템 업데이트 방지 확인란이 표시됩니다.

옵저버블, 표시기 또는 STIX 객체 기록이 생성된 후 시스템에서 업데이트를 방지하려면 이 확인란을 선택합니다.

태그&분류

필드	설명
태그	
태그 선택	위치와 연결된 태그를 선택합니다.
태그 추가	새 태그를 추가합니다.
분류	
분류 선택	이 위치와 연관된 분류를 선택합니다.
분류 값 추가	이 위치와 연결된 분류 값을 추가합니다.

다음에 수행할 작업

다음 관련 목록 중 하나를 클릭하면 해당 위치와 연관된 객체에 대한 추가 정보를 볼 수 있습니다.

관련 기록

필드	설명
외부 참조	STIX가 아닌 정보를 참조하는 외부 참조를 나열합니다. 이 속성은 하나 이상의 외부 객체 식별자를 제공하는 데 사용됩니다.
공격 패턴	이 객체와 관련된 공격을 분류하는 데 도움이 되는 공격 패턴을 나열합니다.
캠페인	이 객체와 연결된 캠페인을 나열합니다.
ID	이 객체와 연결된 ID 목록입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관련 기록

필드	설명
인프라	시스템, 소프트웨어 서비스 및 이 객체와 연결된 연결된 모든 물리적 또는 가상 자원을 나열합니다.
침입 세트	이 객체와 관련된 공통 속성이 있는 일련의 적대적 동작 및 자원을 나열합니다.
맬웨어	이 객체와 관련된 악성 코드를 나열합니다.
마케팅 정의	이 객체와 연결된 마케팅 정의를 나열합니다.
옵저버블	이 객체와 연결된 옵저버블을 나열합니다.
사이팅	이 객체와 연결된 사이팅을 나열합니다.
위협 액터	이 객체와 관련하여 악의적인 의도를 가지고 행동하는 개인, 그룹 또는 조직을 나열합니다.
도구	위협 행위자가 이 개체와 관련된 공격을 수행하는 데 사용하는 합법적인 소프트웨어를 나열합니다.

주:

1. 이 객체와 연결된 관련 기록을 연결하거나 연결 해제할 수 있습니다. 자세한 내용은 위협 인텔리전스 관련 기록 연결 문서를 참조하십시오.
2. TI 라이브러리 내의 다양한 SDO에는 잠재적인 관계도 포함됩니다. 두 개체 간의 관계를 설정하려면 위협 인텔리전스 라이브러리의 **Potential** Relationships(잠재적 관계) 링크를 사용하여 개체 간의 관계를 확인합니다. 자세한 내용은 객체-객체 잠재성 관계 확인 문서를 참조하십시오.
3. 또한 객체 양식 뷰에서 관련 기록 섹션을 사용하면 양식 뷰에서 사용할 수 있는 잠재성 관계 섹션을 통해 두 객체 간의 관계를 확인할 수 있습니다. 에 대한 자세한 내용은 관련 기록에서 잠재성 관계 확인를 참조하십시오.
4. 케이스에 개체를 추가할 수 있습니다. 자세한 내용은 케이스에 추가 문서를 참조하십시오.

맬웨어

멀웨어는 악성 코드를 나타내는 TTP의 일종입니다. 시스템에 은밀하게 삽입되는 프로그램을 말합니다. 맬웨어는 STIX 2.x에 적용됩니다.

멀웨어의 목적은 피해자의 데이터, 애플리케이션 또는 운영 체제(OS)의 기밀성, 무결성 또는 가용성을 손상시키는 것입니다.

맬웨어 SDO는 분석에서 파생된 데이터에서 맬웨어 인스턴스와 제품군을 특성화, 식별 및 분류합니다. 이 SDO는 멀웨어의 작동 방식과 기능에 대한 자세한 정보를 캡처합니다.

맬웨어 정의

악성 코드를 나타내는 맬웨어를 정의합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 작업 공간에서 위협 인텔 라이브러리 아이콘을 클릭합니다.
3. 맬웨어 위협 인텔리전스 개체로 이동합니다.
4. 새로 만들기를 클릭합니다.

   주:
   옵저버블, 표시기, 엔터티 또는 객체에 대한 새 객체 기록을 생성할 때마다 소스 기록이 생성되고, 새 객체 기록이 생성된 다음 사용자가 집계된 기록으로 리디렉션된다는 프롬프트 메시지가 표시됩니다.

5. 양식에서 필드를 채웁니다.

맬웨어 상세 정보 뷰

필드	설명
ID	맬웨어 인스턴스를 식별하는 고유 ID입니다.
이름	SDO 생성자가 지정한 대로 맬웨어 인스턴스 또는 제품군을 식별하는 이름을 입력합니다. 맬웨어 제품군의 경우 이름을 정의해야 합니다.
설명	맬웨어 인스턴스 또는 제품군에 대한 자세한 내용과 컨텍스트를 제공하며, 그 목적과 주요 특성을 포함할 수 있는 설명입니다.
맬웨어 유형	맬웨어의 다양한 범주를 나타냅니다.
제품군임	개체가 맬웨어 제품군 또는 맬웨어 인스턴스를 나타내는지 지정하려면 이 확인란을 선택합니다.
별칭	이 맬웨어 또는 맬웨어 제품군을 식별하는 데 사용되는 대체 이름입니다. 주: 애플리케이션에 없는 새 별칭을 추가하려면 별칭 필드 자체에 있는 새 별칭 추가 아이콘을 클릭합니다.
공격 단계	LM, MITRE ATT&CK와 같은 킬 체인의 공격 단계를 나타냅니다.
처음으로 발견됨	이 맬웨어 인스턴스 또는 제품군이 악의적인 활동을 수행하는 것이 처음 목격된 시간입니다.
마지막으로 발견됨	이 맬웨어 인스턴스 또는 제품군이 악성 활동을 수행하는 것이 마지막으로 목격된 시간
프로세스 아키텍처	이 맬웨어의 프로세스 아키텍처를 나타냅니다.
구현 언어	이 맬웨어의 구현 언어를 나타냅니다.
맬웨어 역량	맬웨어 인스턴스 또는 제품군에서 나타날 수 있는 기능입니다.
TLP	TLP는 민감한 정보가 적절한 대상과 공유되도록 하는 데 사용됩니다. 4가지 색상

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	(흰색, 녹색, 호박색, 빨간색)을 사용하여 다양한 민감도를 나타냅니다.
신뢰도	이 맬웨어에 대한 신뢰도를 입력합니다.
소스	이 개체 기록이 생성되는 위협 소스를 지정합니다.
해지함	해지된 개체가 개체 작성자에 의해 더 이상 유효한 것으로 간주되지 않음을 나타냅니다.

인사이트

필드	설명
메모	맬웨어 기록에 대한 추가 메모를 추가합니다.

추가 정보

필드	설명
추가 컨텍스트	이 맬웨어 기록에 대한 추가 컨텍스트를 추가합니다.
사양 버전	이 객체를 나타내는 데 사용되는 STIX 사양의 버전입니다. 이 특성에 대한 값은 이 사양에 따라 정의된 STIX 객체에 대해 2.1이어야 합니다.
언어	이 속성은 이 객체의 텍스트 컨텐츠 언어를 식별합니다.
소스에서 생성된 시간	원본에서 개체가 만들어지는 시간을 지정합니다.
확장명	공격 패턴의 확장을 나타냅니다.
소스에서 수정된 시간	원본에서 개체가 수정되는 시간을 지정합니다.
처리 상태	이 개체의 처리 상태인 맬웨어를 나타냅니다.
작성됨	원본에서 객체가 만들어진 날짜 및 시간을 지정합니다.
업데이트됨	원본에서 객체가 업데이트된 날짜 및 시간을 지정합니다.
참조에 의해 생성됨	이 속성은 엔터티를 설명하는 ID 개체가 이 개체를 만들었음을 지정합니다.

6. 저장을 클릭합니다.
   저장하면 새 옵저버블 기록이 생성되었음을 나타내는 프롬프트 메시지가 표시됩니다. 기록을 편집하고 새 관계를 생성하려면 "계속 "을 클릭하십시오.
7. 계속을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

중요사항:
새 옵저버블 기록을 생성하면 시스템 업데이트 방지 확인란이 표시됩니다.

옵저버블, 표시기 또는 STIX 객체 기록이 생성된 후 시스템에서 업데이트를 방지하려면 이 확인란을 선택합니다.

태그&분류

필드	설명
태그	
태그 선택	맬웨어와 연결된 태그를 선택합니다.
태그 추가	새 태그를 추가합니다.
분류	
분류 선택	맬웨어와 관련된 분류를 선택합니다.
분류 값 추가	맬웨어와 관련된 분류 값을 추가합니다.

다음에 수행할 작업
다음 관련 목록 중 하나를 클릭하면 맬웨어와 관련된 객체에 대한 추가 정보를 볼 수 있습니다.

필드	설명
외부 참조	STIX가 아닌 정보를 참조하는 외부 참조를 나열합니다. 이 속성은 하나 이상의 외부 객체 식별자를 제공하는 데 사용됩니다.
공격 패턴	이 객체와 관련된 공격을 분류하는 데 도움이 되는 공격 패턴을 나열합니다.
캠페인	이 객체와 연결된 캠페인을 나열합니다.
탐지 및 완화	이 맬웨어와 관련된 탐지 및 완화 방법을 나열합니다.
ID	이 객체와 연결된 ID 목록입니다.
표시기	이 개체와 연결된 위협 소스에서 식별한 관련 IoC(침해 표시기)를 나열합니다.
인프라	시스템, 소프트웨어 서비스 및 이 객체와 연결된 연결된 모든 물리적 또는 가상 자원을 나열합니다.
침입 세트	이 객체와 관련된 공통 속성이 있는 일련의 적대적 동작 및 자원을 나열합니다.
위치	이 객체에 지리적 컨텍스트를 제공하는 위치를 나열합니다.
맬웨어 분석	이 객체와 연결된 맬웨어 분석 기록을 나열합니다.
맬웨어	이 객체와 연결된 맬웨어 기록을 나열합니다.
마케팅 정의	이 객체와 연결된 마케팅 정의를 나열합니다.
옵저버블	이 객체와 연결된 옵저버블을 나열합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
사이팅	이 객체와 연결된 사이팅을 나열합니다.
위협 액터	이 객체와 관련하여 악의적인 의도를 가지고 행동하는 개인, 그룹 또는 조직을 나열합니다.
도구	위협 행위자가 이 개체와 관련된 공격을 수행하는 데 사용하는 합법적인 소프트웨어를 나열합니다.

주:

1. 이 객체와 연결된 관련 기록을 연결하거나 연결 해제할 수 있습니다. 자세한 내용은 위협 인텔리전스 관련 기록 연결 문서를 참조하십시오.
2. TI 라이브러리 내의 다양한 SDO에는 잠재적인 관계도 포함됩니다. 두 개체 간의 관계를 설정하려면 위협 인텔리전스 라이브러리의 **Potential** Relationships(잠재적 관계) 링크를 사용하여 개체 간의 관계를 확인합니다. 자세한 내용은 객체-객체 잠재성 관계 확인 문서를 참조하십시오.
3. 또한 객체 양식 뷰에서 관련 기록 섹션을 사용하면 양식 뷰에서 사용할 수 있는 잠재성 관계 섹션을 통해 두 객체 간의 관계를 확인할 수 있습니다. 에 대한 자세한 내용은 관련 기록에서 잠재성 관계 확인를 참조하십시오.
4. 케이스에 개체를 추가할 수 있습니다. 자세한 내용은 케이스에 추가 문서를 참조하십시오.

맬웨어 분석

맬웨어 분석은 맬웨어의 메타데이터와 결과를 캡처합니다. 맬웨어 분석은 STIX 2.x에 적용됩니다.

맬웨어 분석에는 맬웨어 인스턴스 또는 제품군에서 수행되는 정적 또는 동적 분석이 포함됩니다.

맬웨어 분석 정의

멀웨어 인스턴스 또는 패밀리에서 수행된 특정 정적 또는 동적 분석의 메타데이터와 결과를 캡처하는 멀웨어 분석을 정의합니다.

시작하기 전에

필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 작업 공간에서 위협 인텔 라이브러리 아이콘을 클릭합니다.
3. **Malware Analysis** object(맬웨어 분석 개체)로 이동합니다.
4. 새로 만들기를 클릭합니다.

   주:
   옵저버블, 표시기, 엔터티 또는 객체에 대한 새 객체 기록을 생성할 때마다 소스 기록이 생성되고, 새 객체 기록이 생성된 다음 사용자가 집계된 기록으로 리디렉션된다는 프롬프트 메시지가 표시됩니다.

5. 양식에서 필드를 채웁니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

맬웨어 분석 상세 정보 뷰

필드	설명
ID	맬웨어 분석을 식별하는 고유 ID입니다.
제품	사용된 분석 엔진 또는 제품의 이름입니다. 제품 이름은 모두 소문자여야 하며 단어는 대시 '-'로 구분되어야 합니다(SHOULD). 제품 이름을 지정할 수 없는 경우 anonymized 값을 사용해야 합니다.
버전	분석을 수행하는 데 사용된 분석 제품의 버전입니다.
호스트 VM	맬웨어 인스턴스 또는 제품군의 동적 분석에 사용된 게스트 운영 체제를 호스팅하는 데 사용된 가상 머신 환경에 대한 설명입니다(해당하는 경우). 이 값이 operating_system_ref 속성과 함께 포함되지 않은 경우 동적 분석이 베어메탈(즉, 가상화 없음)에서 수행되었거나 정보가 삭제되었을 수 있음을 의미합니다. 이 속성의 값은 SCO 소프트웨어 객체의 식별자여야 합니다(MUST).
운영 체제	맬웨어 인스턴스 또는 제품군의 동적 분석에 사용되는 운영 체제입니다. 이는 가상화된 운영 체제뿐만 아니라 베어 메탈에서 실행되는 운영 체제에도 적용됩니다. 이 속성의 값은 SCO 소프트웨어 객체의 식별자여야 합니다(MUST).
구성 버전	이 맬웨어 또는 맬웨어 제품군을 식별하는 데 사용되는 대체 이름입니다.
모듈	이 분석 실행 중에 제품에서 사용되고 구성된 특정 분석 모듈입니다.
분석 엔진 버전	분석을 수행하는 데 사용된 분석 엔진 또는 제품(AV 엔진 포함)의 버전입니다.
분석 정의 버전	AV 도구를 포함한 분석 도구에서 사용하는 분석 정의의 버전입니다.
분석 시작됨	맬웨어 분석이 시작된 날짜 및 시간입니다.
분석 종료됨	맬웨어 분석이 종료된 날짜 및 시간입니다.
결과	스캐너 또는 도구 분석 프로세스에 의해 결정된 분류 결과입니다.
결과 이름	스캐너 도구에서 맬웨어 인스턴스에 할당한 분류 결과 또는 이름입니다.
제출됨	멀웨어가 검사 또는 분석을 위해 처음 제출된 날짜 및 시간입니다. 스캔한 날짜가 변경될 수

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	있는 동안에도 이 값은 일정하게 유지됩니다. 예를 들어 맬웨어가 바이러스 분석 도구에 제출된 경우입니다.
분석된 옵저버블	분석된 옵저버블을 선택합니다.
TLP	TLP는 민감한 정보가 적절한 대상과 공유되도록 하는 데 사용됩니다. 4가지 색상(흰색, 녹색, 호박색, 빨간색)을 사용하여 다양한 민감도를 나타냅니다.
신뢰도	이 맬웨어 분석에 대한 신뢰도를 입력합니다.
소스	이 개체 기록이 생성되는 위협 소스를 지정합니다.
해지함	해지된 개체가 개체 작성자에 의해 더 이상 유효한 것으로 간주되지 않음을 나타냅니다.

인사이트

필드	설명
메모	맬웨어 제품군 기록에 대한 추가 메모를 추가합니다.

추가 정보

필드	설명
추가 컨텍스트	이 맬웨어 기록에 대한 추가 컨텍스트를 추가합니다.
사양 버전	이 객체를 나타내는 데 사용되는 STIX 사양의 버전입니다. 이 특성에 대한 값은 이 사양에 따라 정의된 STIX 객체에 대해 2.1이어야 합니다.
언어	이 속성은 이 객체의 텍스트 컨텐츠 언어를 식별합니다.
소스에서 생성된 시간	원본에서 개체가 만들어지는 시간을 지정합니다.
확장명	공격 패턴의 확장을 나타냅니다.
소스에서 수정된 시간	원본에서 개체가 수정되는 시간을 지정합니다.
처리 상태	이 개체의 처리 상태인 맬웨어를 나타냅니다.
작성됨	원본에서 객체가 만들어진 날짜 및 시간을 지정합니다.
업데이트됨	원본에서 객체가 업데이트된 날짜 및 시간을 지정합니다.
참조에 의해 생성됨	이 속성은 엔터티를 설명하는 ID 개체가 이 개체를 만들었음을 지정합니다.

6. 저장을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

저장하면 새 옵저버블 기록이 생성되었음을 나타내는 프롬프트 메시지가 표시됩니다. 기록을 편집하고 새 관계를 생성하려면 "계속 "을 클릭하십시오.

7. 계속을 클릭합니다.

> **중요사항:**
> 새 옵저버블 기록을 생성하면 시스템 업데이트 방지 확인란이 표시됩니다.
>
> 옵저버블, 표시기 또는 STIX 객체 기록이 생성된 후 시스템에서 업데이트를 방지하려면 이 확인란을 선택합니다.

태그&분류

필드	설명
태그	
태그 선택	맬웨어와 연결된 태그를 선택합니다.
태그 추가	새 태그를 추가합니다.
분류	
분류 선택	맬웨어와 관련된 분류를 선택합니다.
분류 값 추가	맬웨어와 관련된 분류 값을 추가합니다.

다음에 수행할 작업

다음 관련 목록 중 하나를 클릭하면 맬웨어와 관련된 객체에 대한 추가 정보를 볼 수 있습니다.

관련 기록

필드	설명
외부 참조	STIX가 아닌 정보를 참조하는 외부 참조를 나열합니다. 이 속성은 하나 이상의 외부 객체 식별자를 제공하는 데 사용됩니다.
맬웨어	이 객체와 연결된 맬웨어 기록을 나열합니다.
마케팅 정의	이 객체와 연결된 마케팅 정의를 나열합니다.
옵저버블	이 객체와 연결된 옵저버블을 나열합니다.
사이팅	이 객체와 연결된 사이팅을 나열합니다.

> **주:**

1. 이 객체와 연결된 관련 기록을 연결하거나 연결 해제할 수 있습니다. 자세한 내용은 위협 인텔리전스 관련 기록 연결 문서를 참조하십시오.
2. TI 라이브러리 내의 다양한 SDO에는 잠재적인 관계도 포함됩니다. 두 개체 간의 관계를 설정하려면 위협 인텔리전스 라이브러리의 **Potential** Relationships(잠재적 관계) 링크를 사용하여 개체 간의 관계를 확인합니다. 자세한 내용은 객체-객체 잠재성 관계 확인 문서를 참조하십시오.
3. 또한 객체 양식 뷰에서 관련 기록 섹션을 사용하면 양식 뷰에서 사용할 수 있는 잠재성 관계 섹션을 통해 두 객체 간의 관계를 확인할 수 있습니다. 에 대한 자세한 내용은 관련 기록에서 잠재성 관계 확인를 참조하십시오.
4. 케이스에 개체를 추가할 수 있습니다. 자세한 내용은 케이스에 추가 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

객체 사이팅

목격은 물체가 목격되었음을 나타냅니다. 개체는 맬웨어, 도구, 위협 액터 등일 수 있습니다.

목격은 표적이 누구이고 무엇인지, 공격이 어떻게 수행되는지를 추적하고 공격 행동의 추세를 추적합니다.

사이팅 관계 객체에는 일반 관계 객체에 없는 추가 속성이 포함되어 있습니다. 이러한 추가 속성은 사이팅 관계와 관련된 데이터를 나타냅니다.

객체 사이팅 정의

개체(맬웨어, 도구, 위협 액터 등)가 보임을 설명하는 개체 사이팅을 정의합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 작업 공간에서 위협 인텔 라이브러리 아이콘을 클릭합니다.
3. **Object Sighting** object로 이동합니다.
4. 새로 만들기를 클릭합니다.

   주:
   옵저버블, 표시기, 엔터티 또는 객체에 대한 새 객체 기록을 생성할 때마다 소스 기록이 생성되고, 새 객체 기록이 생성된 다음 사용자가 집계된 기록으로 리디렉션된다는 프롬프트 메시지가 표시됩니다.

5. 양식에서 필드를 채웁니다.

엔터티&값 선택

필드	설명
엔터티	엔터티 객체 사이팅 기록을 선택합니다. 주: 새 객체 사이팅 기록을 생성하는 동안 집계를 위해 연결된 관계 기록이 필요합니다.
다음의 사이팅	잠재적 위협에 대한 지표가 될 수 있는 환경에서 특정 엔터티 또는 표시기가 관찰되었음을 나타냅니다. 주: 이제 관련 기록을 생성하고 사이팅 기록을 집계할 수 있도록 엔터티 필드에서 선택한 객체와 연결된 사이팅 관련 기록을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

객체 사이팅 상세 정보 뷰

필드	설명
ID	공격을 방지하기 위한 작업 과정의 고유 ID입니다.
설명	사이팅에 대한 자세한 내용과 컨텍스트를 제공하는 설명입니다.
처음으로 발견됨	속성이 관찰된 SDO가 참조하는 기간의 시작 부분입니다.
마지막으로 발견됨	속성이 관찰된 SDO가 참조하는 기간의 끝입니다.
카운트	있는 경우 0에서 999,999,999 사이의 정수여야 하며 속성이 발견된 SDO가 참조하는 횟수를 나타냅니다.
요약임	사이팅을 요약 데이터로 간주해야 하는지 여부를 나타냅니다. 요약 데이터는 이전 사이팅 보고서의 집계이며 기본 소스 데이터로 간주되어서는 안 됩니다.
내부 항목 여부	Sighting이 내부인지 여부를 나타냅니다.
TLP	TLP는 민감한 정보가 적절한 대상과 공유되도록 하는 데 사용됩니다. 4가지 색상(흰색, 녹색, 호박색, 빨간색)을 사용하여 다양한 민감도를 나타냅니다.
신뢰도	이 작업 과정에 대한 신뢰도를 입력합니다.
소스	이 개체 기록이 생성되는 위협 소스를 지정합니다.
해지함	해지된 개체가 개체 작성자에 의해 더 이상 유효한 것으로 간주되지 않음을 나타냅니다.

인사이트

필드	설명
메모	이 침입 집합에 대한 추가 메모를 추가합니다.

추가 정보

필드	설명
추가 컨텍스트	이 공격 패턴에 대한 추가 컨텍스트를 추가합니다.
사양 버전	이 객체를 나타내는 데 사용되는 STIX 사양의 버전입니다. 이 특성에 대한 값은 이 사양에 따라 정의된 STIX 객체에 대해 2.1이어야 합니다.
언어	이 속성은 이 객체의 텍스트 컨텐츠 언어를 식별합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
소스에서 생성된 시간	원본에서 개체가 만들어지는 시간을 지정합니다.
확장명	공격 패턴의 확장을 나타냅니다.
소스에서 수정된 시간	원본에서 개체가 수정되는 시간을 지정합니다.
처리 상태	이 객체의 처리 상태, 작업 과정을 나타냅니다.
작성됨	원본에서 객체가 만들어진 날짜 및 시간을 지정합니다.
업데이트됨	원본에서 객체가 업데이트된 날짜 및 시간을 지정합니다.
참조에 의해 생성됨	이 속성은 엔터티를 설명하는 ID 개체가 이 개체를 만들었음을 지정합니다.

6. 저장을 클릭합니다.
   저장하면 새 옵저버블 기록이 생성되었음을 나타내는 프롬프트 메시지가 표시됩니다. 기록을 편집하고 새 관계를 생성하려면 "계속 "을 클릭하십시오.
7. 계속을 클릭합니다.

중요사항:
새 옵저버블 기록을 생성하면 시스템 업데이트 방지 확인란이 표시됩니다.

옵저버블, 표시기 또는 STIX 객체 기록이 생성된 후 시스템에서 업데이트를 방지하려면 이 확인란을 선택합니다.

태그&분류

필드	설명
태그	
태그 선택	자격 증명과 연결된 태그를 선택합니다.
태그 추가	새 태그를 추가합니다.
분류	
분류 선택	이 인프라와 연결된 분류를 선택합니다.
분류 값 추가	이 인프라와 연결된 분류 값을 추가합니다.

다음에 수행할 작업

다음 관련 목록 중 하나를 클릭하면 객체 사이팅과 연관된 객체에 대한 추가 정보를 볼 수 있습니다.

관련 기록

필드	설명
외부 참조	STIX가 아닌 정보를 참조하는 외부 참조를 나열합니다. 이 속성은 하나 이상의 외부 객체 식별자를 제공하는 데 사용됩니다.
객체	사이팅과 연결된 객체를 나열합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관련 기록

필드	설명
표시기	이 개체와 연결된 위협 소스에서 식별한 관련 IoC(침해 표시기)를 나열합니다.

주:

1. 이 객체와 연결된 관련 기록을 연결하거나 연결 해제할 수 있습니다. 자세한 내용은 위협 인텔리전스 관련 기록 연결 문서를 참조하십시오.
2. TI 라이브러리 내의 다양한 SDO에는 잠재적인 관계도 포함됩니다. 두 개체 간의 관계를 설정하려면 위협 인텔리전스 라이브러리의 **Potential** Relationships(잠재적 관계) 링크를 사용하여 개체 간의 관계를 확인합니다. 자세한 내용은 객체-객체 잠재성 관계 확인 문서를 참조하십시오.
3. 또한 객체 양식 뷰에서 관련 기록 섹션을 사용하면 양식 뷰에서 사용할 수 있는 잠재성 관계 섹션을 통해 두 객체 간의 관계를 확인할 수 있습니다. 에 대한 자세한 내용은 관련 기록에서 잠재성 관계 확인를 참조하십시오.
4. 케이스에 개체를 추가할 수 있습니다. 자세한 내용은 케이스에 추가 문서를 참조하십시오.

관찰 데이터

관찰 데이터는 STIX SCO(Cyber-Observable Objects)를 사용하여 파일, 시스템 및 네트워크와 같은 사이버 보안 관련 엔터티에 대한 정보를 전달합니다. 관찰 데이터는 STIX 2.x에 적용됩니다.

관찰 데이터는 단일 엔터티(파일, 네트워크 연결)에 대한 단일 관찰과 엔터티에 대한 여러 관찰 집계를 모두 캡처합니다.

관찰 데이터 단독으로(관계 없이) 사용하여 모든 소스에서 수집된 원시 데이터를 전달할 수 있습니다. 소스에는 분석 보고서, 샌드박스, 네트워크 및 호스트 기반 탐지 도구가 포함됩니다.

예를 들어 관찰 데이터는 IP 주소, 네트워크 연결, 파일 또는 레지스트리 키에 대한 정보를 캡처할 수 있습니다. 관찰 데이터는 정보 주장이 아니며, 그것이 의미하는 바에 대한 맥락이 없는 원시 정보일 뿐입니다.

관찰 데이터 정의

STIX SCO(Cyber-Observable Objects)를 사용하여 파일, 시스템 및 네트워크와 같은 사이버 보안 관련 엔터티에 대한 정보를 전달합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 작업 공간에서 위협 인텔 라이브러리 아이콘을 클릭합니다.
3. 관찰 데이터 객체로 이동합니다.
4. 새로 만들기를 클릭합니다.

주:
옵저버블, 표시기, 엔터티 또는 객체에 대한 새 객체 기록을 생성할 때마다 소스 기록이 생성되고, 새 객체 기록이 생성된 다음 사용자가 집계된 기록으로 리디렉션된다는 프롬프트 메시지가 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. 양식에서 필드를 채웁니다.

관찰 데이터 상세 정보 뷰

필드	설명
ID	관찰된 데이터를 식별하는 고유 ID입니다.
처음으로 관찰됨	데이터를 처음 본 시간입니다.
마지막으로 관찰됨	데이터를 마지막으로 본 시간입니다.
관찰 카운트	각 사이버 옵저버블 객체를 본 횟수입니다. 값은 1에서 999,999,999 사이의 정수여야 합니다.
TLP	TLP는 민감한 정보가 적절한 대상과 공유되도록 하는 데 사용됩니다. 4가지 색상(흰색, 녹색, 호박색, 빨간색)을 사용하여 다양한 민감도를 나타냅니다.
신뢰도	관찰된 데이터에 대한 신뢰도 입력
소스	이 개체 기록이 생성되는 위협 소스를 지정합니다.
해지함	해지된 개체가 개체 작성자에 의해 더 이상 유효한 것으로 간주되지 않음을 나타냅니다.

인사이트

필드	설명
메모	이 관찰 데이터에 대한 추가 메모를 추가합니다.

추가 정보

필드	설명
추가 컨텍스트	이 관찰된 데이터에 대한 추가 컨텍스트를 추가합니다.
사양 버전	이 객체를 나타내는 데 사용되는 STIX 사양의 버전입니다. 이 특성에 대한 값은 이 사양에 따라 정의된 STIX 객체에 대해 2.1이어야 합니다.
언어	이 속성은 이 객체의 텍스트 컨텐츠 언어를 식별합니다.
작성됨	원본에서 객체가 만들어진 날짜 및 시간을 지정합니다.
확장명	공격 패턴의 확장을 나타냅니다.
업데이트됨	원본에서 객체가 업데이트된 날짜 및 시간을 지정합니다.
처리 상태	이 객체의 처리 상태, 작업 과정을 나타냅니다.

6. 저장을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

저장하면 새 옵저버블 기록이 생성되었음을 나타내는 프롬프트 메시지가 표시됩니다. 기록을 편집하고 새 관계를 생성하려면 "계속 "을 클릭하십시오.

7. 계속을 클릭합니다.

> **중요사항:**
> 새 옵저버블 기록을 생성하면 시스템 업데이트 방지 확인란이 표시됩니다.
>
> 옵저버블, 표시기 또는 STIX 객체 기록이 생성된 후 시스템에서 업데이트를 방지하려면 이 확인란을 선택합니다.

태그&분류

필드	설명
태그	
태그 선택	관찰 데이터와 연결된 태그를 선택합니다.
태그 추가	새 태그를 추가합니다.
분류	
분류 선택	이 관찰 데이터와 연결된 분류를 선택합니다.
분류 값 추가	이 관찰 데이터와 연결된 분류 값을 추가합니다.

다음에 수행할 작업

관찰 데이터와 연결된 객체에 대한 추가 정보를 보려면 다음 관련 목록 중 하나를 클릭합니다.

관련 기록

필드	설명
외부 참조	STIX가 아닌 정보를 참조하는 외부 참조를 나열합니다. 이 속성은 하나 이상의 외부 객체 식별자를 제공하는 데 사용됩니다.
표시기	이 개체와 연결된 위협 소스에서 식별한 관련 IoC(침해 표시기)를 나열합니다.
인프라	시스템, 소프트웨어 서비스 및 이 객체와 연결된 연결된 모든 물리적 또는 가상 자원을 나열합니다.
마케팅 정의	이 객체와 연결된 마케팅 정의를 나열합니다.
사이팅	이 객체와 연결된 사이팅을 나열합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

1. 이 객체와 연결된 관련 기록을 연결하거나 연결 해제할 수 있습니다. 자세한 내용은 위협 인텔리전스 관련 기록 연결 문서를 참조하십시오.
2. TI 라이브러리 내의 다양한 SDO에는 잠재적인 관계도 포함됩니다. 두 개체 간의 관계를 설정하려면 위협 인텔리전스 라이브러리의 **Potential** Relationships(잠재적 관계) 링크를 사용하여 개체 간의 관계를 확인합니다. 자세한 내용은 객체-객체 잠재성 관계 확인 문서를 참조하십시오.
3. 또한 객체 양식 뷰에서 관련 기록 섹션을 사용하면 양식 뷰에서 사용할 수 있는 잠재성 관계 섹션을 통해 두 객체 간의 관계를 확인할 수 있습니다. 에 대한 자세한 내용은 관련 기록에서 잠재성 관계 확인를 참조하십시오.
4. 케이스에 개체를 추가할 수 있습니다. 자세한 내용은 케이스에 추가 문서를 참조하십시오.

위협 액터

위협 액터는 악의적인 의도로 행동하는 개인, 그룹 또는 조직입니다. 위협 액터는 STIX 2.x에 적용됩니다.

위협 액터는 침입 세트가 아니지만 시간이 지남에 따라 다양한 침입 세트, 그룹 또는 조직을 지원하거나 소속될 수 있습니다.

위협 액터는 자신의 리소스와 침입 세트의 리소스를 사용하여 공격을 수행하고 대상에 대해 캠페인을 실행합니다.

동기, 역량, 목표, 정교함 수준, 과거 활동, 액세스할 수 있는 자원 및 조직에서의 역할을 기준으로 위협 액터를 식별할 수 있습니다.

위협 액터 정의

악의적인 의도로 행동하는 개인, 그룹 또는 조직인 위협 행위자를 정의합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 작업 공간에서 위협 인텔 라이브러리 아이콘을 클릭합니다.
3. 위협 액터 오브젝트로 이동합니다.
4. 새로 만들기를 클릭합니다.

   주:
   옵저버블, 표시기, 엔터티 또는 객체에 대한 새 객체 기록을 생성할 때마다 소스 기록이 생성되고, 새 객체 기록이 생성된 다음 사용자가 집계된 기록으로 리디렉션된다는 프롬프트 메시지가 표시됩니다.

5. 양식에서 필드를 채웁니다.

위협 액터 상세 정보 뷰

필드	설명
ID	공격을 방지하기 위한 작업 과정의 고유 ID입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
이름	위치를 식별하기 위한 설명이 포함된 이름을 입력합니다.
설명	침입 세트의 목적과 주요 특성을 포함하여 침입 집합에 대한 자세한 내용과 컨텍스트를 제공하는 설명입니다.
별칭	이 위협 액터를 식별할 다른 이름의 목록입니다. 주: 애플리케이션에 없는 새 별칭을 추가하려면 별칭 필드 자체에 있는 새 별칭 추가 아이콘을 클릭합니다.
목표	이 위협 행위자의 개략적인 목표, 즉 그들이 하려는 일. 예를 들어, 그들은 개인적인 이익을 위해 동기를 부여받을 수 있지만 목표는 신용 카드 번호를 훔치는 것입니다.
위협 액터 유형	이 위협 액터의 유형입니다.
위협 액터 역할	이 개체에 대한 다양한 위협 액터 역할입니다.
처음으로 발견됨	이 위협 액터가 처음 나타난 시간입니다. 이 속성은 STIX에서 사용할 수 있거나 사용할 수 없는 사이팅 및 기타 데이터의 데이터의 요약 속성입니다. 처음 발견된 타임스탬프보다 이른 새로운 목격이 수신되면, 객체는 새로운 데이터를 설명하기 위해 업데이트될 수 있다.
마지막으로 발견됨	이 위협 액터가 마지막으로 목격된 시간입니다.
기본 동기	이 위협 액터의 기본 이유, 동기 또는 목적입니다. 동기는 위협 액터가 목표(달성하려는 것)를 달성하고자 하는 이유입니다. 예를 들어, 한 국가의 금융 부문을 붕괴시키려는 목표를 가진 위협 행위자는 자본주의에 대한 이데올로기적 증오에서 동기를 부여받을 수 있다.
전문성	위협 액터가 공격을 수행하는 데 필요한 기술, 특정 지식, 특수 교육 또는 전문 지식입니다.
보조 동기	이 속성은 이 위협 액터의 이차적인 이유, 동기 또는 목적을 지정합니다. 이러한 동기는 일차적 동기와 동등하거나 거의 동등한 원인으로 존재할 수 있다. 그러나 주요 동기를 대체하거나 반드시 확대하지는 않지만 추가 컨텍스트를 나타낼 수 있습니다. 목록의 위치는 중요하지 않습니다.
자원 수준	이 위협 액터가 일반적으로 작동하는 조직 수준으로, 이에 따라 이 위협 액터가 공격에 사용할 수 있는 리소스가 결정됩니다. 이 속성은

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	sophistication 프로퍼티와 연결되어 있으며, 특정 리소스 레벨은 위협 액터가 최소한 특정 정교함 레벨에 액세스할 수 있음을 의미합니다.
신뢰도	이 작업 과정에 대한 신뢰도를 입력합니다.
TLP	TLP는 민감한 정보가 적절한 대상과 공유되도록 하는 데 사용됩니다. 4가지 색상(흰색, 녹색, 호박색, 빨간색)을 사용하여 다양한 민감도를 나타냅니다.
소스	이 개체 기록이 생성되는 위협 소스를 지정합니다.
해지함	해지된 개체가 개체 작성자에 의해 더 이상 유효한 것으로 간주되지 않음을 나타냅니다.

인사이트

필드	설명
메모	이 위협 액터에 대한 추가 메모를 추가합니다.

추가 정보

필드	설명
추가 컨텍스트	이 공격 패턴에 대한 추가 컨텍스트를 추가합니다.
사양 버전	이 객체를 나타내는 데 사용되는 STIX 사양의 버전입니다. 이 특성에 대한 값은 이 사양에 따라 정의된 STIX 객체에 대해 2.1이어야 합니다.
언어	이 속성은 이 객체의 텍스트 컨텐츠 언어를 식별합니다.
소스에서 생성된 시간	원본에서 개체가 만들어지는 시간을 지정합니다.
확장명	공격 패턴의 확장을 나타냅니다.
소스에서 수정된 시간	원본에서 개체가 수정되는 시간을 지정합니다.
처리 상태	이 객체의 처리 상태, 작업 과정을 나타냅니다.
작성됨	원본에서 객체가 만들어진 날짜 및 시간을 지정합니다.
업데이트됨	원본에서 객체가 업데이트된 날짜 및 시간을 지정합니다.
참조에 의해 생성됨	이 속성은 엔터티를 설명하는 ID 개체가 이 개체를 만들었음을 지정합니다.

6. 저장을 클릭합니다.
   저장하면 새 옵저버블 기록이 생성되었음을 나타내는 프롬프트 메시지가 표시됩니다. 기록을 편집하고 새 관계를 생성하려면 "계속"을 클릭하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

7. 계속을 클릭합니다.

> **중요사항:**
> 새 옵저버블 기록을 생성하면 시스템 업데이트 방지 확인란이 표시됩니다.
>
> 옵저버블, 표시기 또는 STIX 객체 기록이 생성된 후 시스템에서 업데이트를 방지하려면 이 확인란을 선택합니다.

태그&분류

필드	설명
태그	
태그 선택	위협 액터와 연결된 태그를 선택합니다.
태그 추가	새 태그를 추가합니다.
분류	
분류 선택	이 위협 액터와 연결된 분류를 선택합니다.
분류 값 추가	이 위협 액터와 연결된 분류 값을 추가합니다.

다음에 수행할 작업

다음 관련 목록 중 하나를 클릭하여 위협 액터와 연결된 객체에 대한 추가 정보를 봅니다.

관련 기록

필드	설명
외부 참조	STIX가 아닌 정보를 참조하는 외부 참조를 나열합니다. 이 속성은 하나 이상의 외부 객체 식별자를 제공하는 데 사용됩니다.
공격 패턴	이 객체와 관련된 공격을 분류하는 데 도움이 되는 공격 패턴을 나열합니다.
캠페인	이 객체와 연결된 캠페인을 나열합니다.
ID	이 객체와 연결된 ID 목록입니다.
인프라	시스템, 소프트웨어 서비스 및 이 객체와 연결된 연결된 모든 물리적 또는 가상 자원을 나열합니다.
침입 세트	이 객체와 관련된 공통 속성이 있는 일련의 적대적 동작 및 자원을 나열합니다.
위치	이 객체와 연결된 위치의 목록입니다.
맬웨어	이 객체와 관련된 악성 코드를 나열합니다.
마케팅 정의	이 객체와 연결된 마케팅 정의를 나열합니다.
옵저버블	이 객체와 연결된 옵저버블을 나열합니다.
사이팅	이 객체와 연결된 사이팅을 나열합니다.
도구	위협 행위자가 이 개체와 관련된 공격을 수행하는 데 사용하는 합법적인 소프트웨어를 나열합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

1. 이 객체와 연결된 관련 기록을 연결하거나 연결 해제할 수 있습니다. 자세한 내용은 위협 인텔리전스 관련 기록 연결 문서를 참조하십시오.
2. TI 라이브러리 내의 다양한 SDO에는 잠재적인 관계도 포함됩니다. 두 개체 간의 관계를 설정하려면 위협 인텔리전스 라이브러리의 **Potential** Relationships(잠재적 관계) 링크를 사용하여 개체 간의 관계를 확인합니다. 자세한 내용은 객체-객체 잠재성 관계 확인 문서를 참조하십시오.
3. 또한 객체 양식 뷰에서 관련 기록 섹션을 사용하면 양식 뷰에서 사용할 수 있는 잠재성 관계 섹션을 통해 두 객체 간의 관계를 확인할 수 있습니다. 에 대한 자세한 내용은 관련 기록에서 잠재성 관계 확인를 참조하십시오.
4. 케이스에 개체를 추가할 수 있습니다. 자세한 내용은 케이스에 추가 문서를 참조하십시오.

위협 이벤트

바람직하지 않은 결과나 영향을 미칠 가능성이 있는 이벤트 또는 상황입니다.

웹 사이트를 공격하는 해커는 위협 이벤트입니다. 해커가 웹 사이트를 손상시키거나 정보를 훔치는 경우 위협 이벤트로 정의됩니다.

위협 이벤트 정의

비공개 정보에 대한 무단 액세스 및 획득 또는 정보시스템의 중단 또는 오용을 초래하는 이벤트 시 위협 이벤트를 정의합니다.

시작하기 전에

필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 작업 공간에서 위협 인텔 라이브러리 아이콘을 클릭합니다.
3. 위협 이벤트 개체로 이동합니다.
4. 새로 만들기를 클릭합니다.

주:
옵저버블, 표시기, 엔터티 또는 객체에 대한 새 객체 기록을 생성할 때마다 소스 기록이 생성되고, 새 객체 기록이 생성된 다음 사용자가 집계된 기록으로 리디렉션된다는 프롬프트 메시지가 표시됩니다.

5. 양식에서 필드를 채웁니다.

위협 액터 상세 정보 뷰

필드	설명
ID	위협 이벤트를 방지하기 위한 작업 과정의 고유 ID입니다.
이름	위협 이벤트를 식별하는 설명이 포함된 이름을 입력합니다.
설명	위협 이벤트의 목적과 주요 특성을 포함하여 위협 이벤트에 대한 자세한 내용과 컨텍스트를 제공하는 설명입니다.
신뢰도	이 작업 과정에 대한 신뢰도를 입력합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
TLP	TLP는 민감한 정보가 적절한 대상과 공유되도록 하는 데 사용됩니다. 4가지 색상(흰색, 녹색, 호박색, 빨간색)을 사용하여 다양한 민감도를 나타냅니다.
소스	이 개체 기록이 생성되는 위협 소스를 지정합니다.
해지함	해지된 개체가 개체 작성자에 의해 더 이상 유효한 것으로 간주되지 않음을 나타냅니다.

인사이트

필드	설명
메모	이 위협 액터에 대한 추가 메모를 추가합니다.

추가 정보

필드	설명
추가 컨텍스트	이 공격 패턴에 대한 추가 컨텍스트를 추가합니다.
사양 버전	이 객체를 나타내는 데 사용되는 STIX 사양의 버전입니다. 이 특성에 대한 값은 이 사양에 따라 정의된 STIX 객체에 대해 2.1이어야 합니다.
언어	이 속성은 이 객체의 텍스트 컨텐츠 언어를 식별합니다.
소스에서 생성된 시간	원본에서 개체가 만들어지는 시간을 지정합니다.
확장명	공격 패턴의 확장을 나타냅니다.
소스에서 수정된 시간	원본에서 개체가 수정되는 시간을 지정합니다.
처리 상태	이 객체의 처리 상태, 작업 과정을 나타냅니다.
작성됨	원본에서 객체가 만들어진 날짜 및 시간을 지정합니다.
업데이트됨	원본에서 객체가 업데이트된 날짜 및 시간을 지정합니다.
참조에 의해 생성됨	이 속성은 엔터티를 설명하는 ID 개체가 이 개체를 만들었음을 지정합니다.

6. 저장을 클릭합니다.
   저장하면 새 옵저버블 기록이 생성되었음을 나타내는 프롬프트 메시지가 표시됩니다. 기록을 편집하고 새 관계를 생성하려면 "계속 "을 클릭하십시오.
7. 계속을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

중요사항:
새 옵저버블 기록을 생성하면 시스템 업데이트 방지 확인란이 표시됩니다.

옵저버블, 표시기 또는 STIX 객체 기록이 생성된 후 시스템에서 업데이트를 방지하려면 이 확인란을 선택합니다.

태그&분류

필드	설명
태그	
태그 선택	위협 이벤트와 연결된 태그를 선택합니다.
태그 추가	새 태그를 추가합니다.
분류	
분류 선택	이 위협 이벤트와 관련된 분류를 선택합니다.
분류 값 추가	이 위협 이벤트와 연결된 분류 값을 추가합니다.

다음에 수행할 작업

위협 이벤트와 연결된 개체에 대한 추가 정보를 보려면 다음 관련 목록 중 하나를 클릭합니다.

관련 기록

필드	설명
외부 참조	STIX가 아닌 정보를 참조하는 외부 참조를 나열합니다. 이 속성은 하나 이상의 외부 객체 식별자를 제공하는 데 사용됩니다.
캠페인	이 객체와 연결된 캠페인을 나열합니다.
표시기	이 개체와 연결된 위협 소스에서 식별한 관련 IoC(침해 표시기)를 나열합니다.
인프라	시스템, 소프트웨어 서비스 및 이 객체와 연결된 연결된 모든 물리적 또는 가상 자원을 나열합니다.
침입 세트	이 객체와 관련된 공통 속성이 있는 일련의 적대적 동작 및 자원을 나열합니다.
위치	이 객체에 지리적 컨텍스트를 제공하는 위치를 나열합니다.
맬웨어	이 객체와 관련된 악성 코드를 나열합니다.
마케팅 정의	이 객체와 연결된 마케팅 정의를 나열합니다.
사이팅	이 객체와 연결된 사이팅을 나열합니다.
옵저버블	이 객체와 연결된 옵저버블을 나열합니다.
관찰 데이터	이 객체와 연결된 관찰 데이터를 나열합니다.
위협 액터	이 객체와 관련하여 악의적인 의도를 가지고 행동하는 개인, 그룹 또는 조직을 나열합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관련 기록

필드	설명
도구	위협 행위자가 이 개체와 관련된 공격을 수행하는 데 사용하는 합법적인 소프트웨어를 나열합니다.
취약성	공격자가 악용하는 소프트웨어 또는 하드웨어의 약점 또는 결함을 나열합니다. 이 개체와 관련되어 있습니다.

주:

1. 이 객체와 연결된 관련 기록을 연결하거나 연결 해제할 수 있습니다. 자세한 내용은 위협 인텔리전스 관련 기록 연결 문서를 참조하십시오.
2. TI 라이브러리 내의 다양한 SDO에는 잠재적인 관계도 포함됩니다. 두 개체 간의 관계를 설정하려면 위협 인텔리전스 라이브러리의 **Potential** Relationships(잠재적 관계) 링크를 사용하여 개체 간의 관계를 확인합니다. 자세한 내용은 객체-객체 잠재성 관계 확인 문서를 참조하십시오.
3. 또한 객체 양식 뷰에서 관련 기록 섹션을 사용하면 양식 뷰에서 사용할 수 있는 잠재성 관계 섹션을 통해 두 객체 간의 관계를 확인할 수 있습니다. 에 대한 자세한 내용은 관련 기록에서 잠재성 관계 확인를 참조하십시오.
4. 케이스에 개체를 추가할 수 있습니다. 자세한 내용은 케이스에 추가 문서를 참조하십시오.

위협 그룹화

위협 그룹화 개체는 참조된 STIX 개체에 공유 컨텍스트가 있음을 명시적으로 어설션합니다. 위협 그룹화는 STIX 2.x에 적용됩니다.

위협 그룹화 개체는 충분한 분석이 주어지면 인시던트 또는 위협 보고서를 STIX 보고서 개체로 전달하기 위해 성숙한 데이터 집합을 나타냅니다. 예를 들어, 그룹화는 보안 이벤트 또는 인시던트에 대해 진행 중인 조사의 특성을 나타내는 데 사용할 수 있습니다.

위협 그룹화 개체를 사용하여 참조된 STIX 개체가 진행 중인 분석 프로세스와 관련이 있는지 어설션할 수도 있습니다. 예를 들어 위협 분석가는 신뢰 커뮤니티의 다른 사용자와 협력하여 일련의 캠페인 및 표시기를 검사할 수 있습니다.

위협 그룹화 SDO에는 콘텐츠에서 공유하는 컨텍스트에 대한 명시적 설명, 텍스트 설명 및 그룹화 이름과 함께 SDO, SCO 및 SRO에 대한 참조 목록이 포함되어 있습니다.

위협 그룹화 정의

위협 그룹화를 공유 컨텍스트가 있는 개체로 정의합니다.

시작하기 전에

필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 작업 공간에서 위협 인텔 라이브러리 아이콘을 클릭합니다.
3. 위협 그룹화 개체로 이동합니다.
4. 새로 만들기를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
옵저버블, 표시기, 엔터티 또는 객체에 대한 새 객체 기록을 생성할 때마다 소스 기록이 생성되고, 새 객체 기록이 생성된 다음 사용자가 집계된 기록으로 리디렉션된다는 프롬프트 메시지가 표시됩니다.

5. 양식에서 필드를 채웁니다.

위협 그룹화 상세 정보 뷰

필드	설명
ID	위협 그룹 유형의 공격이 발생하지 않도록 방지하기 위한 작업 과정의 고유 ID입니다.
이름	위협 그룹을 식별하는 설명이 포함된 이름을 입력합니다.
설명	위협 이벤트의 목적과 주요 특성을 포함하여 위협 이벤트에 대한 자세한 내용과 컨텍스트를 제공하는 설명입니다.
신뢰도	이 작업 과정에 대한 신뢰도를 입력합니다.
TLP	TLP는 민감한 정보가 적절한 대상과 공유되도록 하는 데 사용됩니다. 4가지 색상(흰색, 녹색, 호박색, 빨간색)을 사용하여 다양한 민감도를 나타냅니다.
소스	이 개체 기록이 생성되는 위협 소스를 지정합니다.
해지함	해지된 개체가 개체 작성자에 의해 더 이상 유효한 것으로 간주되지 않음을 나타냅니다.

인사이트

필드	설명
메모	이 위협 그룹화에 대한 추가 메모를 추가합니다.

추가 정보

필드	설명
추가 컨텍스트	이 공격 패턴에 대한 추가 컨텍스트를 추가합니다.
사양 버전	이 객체를 나타내는 데 사용되는 STIX 사양의 버전입니다. 이 특성에 대한 값은 이 사양에 따라 정의된 STIX 객체에 대해 2.1이어야 합니다.
언어	이 속성은 이 객체의 텍스트 컨텐츠 언어를 식별합니다.
소스에서 생성된 시간	원본에서 개체가 만들어지는 시간을 지정합니다.
확장명	공격 패턴의 확장을 나타냅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
소스에서 수정된 시간	원본에서 개체가 수정되는 시간을 지정합니다.
처리 상태	이 객체의 처리 상태, 작업 과정을 나타냅니다.
작성됨	원본에서 객체가 만들어진 날짜 및 시간을 지정합니다.
업데이트됨	원본에서 객체가 업데이트된 날짜 및 시간을 지정합니다.
참조에 의해 생성됨	이 속성은 엔터티를 설명하는 ID 개체가 이 개체를 만들었음을 지정합니다.

6. 저장을 클릭합니다.
   저장하면 새 옵저버블 기록이 생성되었음을 나타내는 프롬프트 메시지가 표시됩니다. 기록을 편집하고 새 관계를 생성하려면 "계속 "을 클릭하십시오.
7. 계속을 클릭합니다.

중요사항:
새 옵저버블 기록을 생성하면 시스템 업데이트 방지 확인란이 표시됩니다.

옵저버블, 표시기 또는 STIX 객체 기록이 생성된 후 시스템에서 업데이트를 방지하려면 이 확인란을 선택합니다.

태그&분류

필드	설명
태그	
태그 선택	위협 그룹화와 연결된 태그를 선택합니다.
태그 추가	새 태그를 추가합니다.
분류	
분류 선택	이 위협 그룹화와 연결된 분류를 선택합니다.
분류 값 추가	이 위협 그룹화와 연결된 분류 값을 추가합니다.

다음에 수행할 작업
위협 그룹화와 연결된 개체에 대한 추가 정보를 보려면 다음 관련 목록 중 하나를 클릭합니다.

필드	설명
외부 참조	STIX가 아닌 정보를 참조하는 외부 참조를 나열합니다. 이 속성은 하나 이상의 외부 객체 식별자를 제공하는 데 사용됩니다.
캠페인	이 객체와 연결된 캠페인을 나열합니다.
표시기	이 개체와 연결된 위협 소스에서 식별한 관련 IoC(침해 표시기)를 나열합니다.
인프라	시스템, 소프트웨어 서비스 및 이 객체와 연결된 연결된 모든 물리적 또는 가상 자원을 나열합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
침입 세트	이 객체와 관련된 공통 속성이 있는 일련의 적대적 동작 및 자원을 나열합니다.
위치	이 객체에 지리적 컨텍스트를 제공하는 위치를 나열합니다.
맬웨어	이 객체와 관련된 악성 코드를 나열합니다.
마케팅 정의	이 객체와 연결된 마케팅 정의를 나열합니다.
사이팅	이 객체와 연결된 사이팅을 나열합니다.
옵저버블	이 객체와 연결된 옵저버블을 나열합니다.
관찰 데이터	이 객체와 연결된 관찰 데이터를 나열합니다.
위협 액터	이 객체와 관련하여 악의적인 의도를 가지고 행동하는 개인, 그룹 또는 조직을 나열합니다.
위협 이벤트	이 개체와 연결된 위협 이벤트를 나열합니다.
도구	위협 행위자가 이 개체와 관련된 공격을 수행하는 데 사용하는 합법적인 소프트웨어를 나열합니다.
취약성	공격자가 악용하는 소프트웨어 또는 하드웨어의 약점 또는 결함을 나열합니다. 이 개체와 관련되어 있습니다.

주:

1. 이 객체와 연결된 관련 기록을 연결하거나 연결 해제할 수 있습니다. 자세한 내용은 위협 인텔리전스 관련 기록 연결 문서를 참조하십시오.
2. TI 라이브러리 내의 다양한 SDO에는 잠재적인 관계도 포함됩니다. 두 개체 간의 관계를 설정하려면 위협 인텔리전스 라이브러리의 **Potential** Relationships(잠재적 관계) 링크를 사용하여 개체 간의 관계를 확인합니다. 자세한 내용은 객체-객체 잠재성 관계 확인 문서를 참조하십시오.
3. 또한 객체 양식 뷰에서 관련 기록 섹션을 사용하면 양식 뷰에서 사용할 수 있는 잠재성 관계 섹션을 통해 두 객체 간의 관계를 확인할 수 있습니다. 에 대한 자세한 내용은 관련 기록에서 잠재성 관계 확인를 참조하십시오.
4. 케이스에 개체를 추가할 수 있습니다. 자세한 내용은 케이스에 추가 문서를 참조하십시오.

위협 메모

위협 메모는 메모와 관련된 STIX 개체, 표시 정의 개체 또는 언어 콘텐츠 개체에 포함되지 않은 추가 분석을 제공하기 위해 정보 텍스트를 전달합니다. 위협 메모는 STIX 2.x에 적용됩니다.

예를 들어 분석가는 다른 조직에서 만든 캠페인 객체에 메모를 추가할 수 있습니다. 메모는 해커 포럼에서 해당 캠페인과 관련된 게시물을 보았음을 나타낼 수 있습니다.

메모는 일반적으로 인간 분석가가 작성하고 인간 중심의 텍스트로 구성되며 메모를 작성한 작성자를 캡처하는 추가 속성을 포함합니다.

위협 메모 정의

기존 객체에서 사용할 수 없는 추가 컨텍스트 또는 분석을 제공하기 위해 정보를 전달하는 위협 메모를 정의합니다.

시작하기 전에

필요한 역할: sn_sec_tisc.analyst

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 작업 공간에서 위협 인텔 라이브러리 아이콘을 클릭합니다.
3. 위협 메모로 이동합니다.
4. 새로 만들기를 클릭합니다.

   주:
   옵저버블, 표시기, 엔터티 또는 객체에 대한 새 객체 기록을 생성할 때마다 소스 기록이 생성되고, 새 객체 기록이 생성된 다음 사용자가 집계된 기록으로 리디렉션된다는 프롬프트 메시지가 표시됩니다.

5. 양식에서 필드를 채웁니다.

위협 메모 상세 정보 뷰

필드	설명
ID	위협 메모의 고유 ID입니다.
추상	메모 내용에 대한 간략한 요약을 지정합니다.
컨텐츠	메모의 내용을 지정합니다.
작성자	작성자의 이름(예: 분석가)을 지정합니다.
신뢰도	이 작업 과정에 대한 신뢰도를 입력합니다.
TLP	TLP는 민감한 정보가 적절한 대상과 공유되도록 하는 데 사용됩니다. 4가지 색상(흰색, 녹색, 호박색, 빨간색)을 사용하여 다양한 민감도를 나타냅니다.
소스	이 개체 기록이 생성되는 위협 소스를 지정합니다.
해지함	해지된 개체가 개체 작성자에 의해 더 이상 유효한 것으로 간주되지 않음을 나타냅니다.

인사이트

필드	설명
메모	이 위협 메모에 대한 추가 메모를 추가합니다.

추가 정보

필드	설명
추가 컨텍스트	이 공격 패턴에 대한 추가 컨텍스트를 추가합니다.
사양 버전	이 객체를 나타내는 데 사용되는 STIX 사양의 버전입니다. 이 특성에 대한 값은 이 사양에 따라 정의된 STIX 객체에 대해 2.1이어야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
언어	이 속성은 이 객체의 텍스트 컨텐츠 언어를 식별합니다.
소스에서 생성된 시간	원본에서 개체가 만들어지는 시간을 지정합니다.
확장명	공격 패턴의 확장을 나타냅니다.
소스에서 수정된 시간	원본에서 개체가 수정되는 시간을 지정합니다.
처리 상태	이 객체의 처리 상태, 작업 과정을 나타냅니다.
작성됨	원본에서 객체가 만들어진 날짜 및 시간을 지정합니다.
업데이트됨	원본에서 객체가 업데이트된 날짜 및 시간을 지정합니다.
참조에 의해 생성됨	이 속성은 엔터티를 설명하는 ID 개체가 이 개체를 만들었음을 지정합니다.

6. 저장을 클릭합니다.
   저장하면 새 옵저버블 기록이 생성되었음을 나타내는 프롬프트 메시지가 표시됩니다. 기록을 편집하고 새 관계를 생성하려면 "계속 "을 클릭하십시오.
7. 계속을 클릭합니다.

중요사항:
새 옵저버블 기록을 생성하면 시스템 업데이트 방지 확인란이 표시됩니다.

옵저버블, 표시기 또는 STIX 객체 기록이 생성된 후 시스템에서 업데이트를 방지하려면 이 확인란을 선택합니다.

태그&분류

필드	설명
태그	
태그 선택	위협 그룹화와 연결된 태그를 선택합니다.
태그 추가	새 태그를 추가합니다.
분류	
분류 선택	이 위협 그룹화와 연결된 분류를 선택합니다.
분류 값 추가	이 위협 그룹화와 연결된 분류 값을 추가합니다.

다음에 수행할 작업

위협 메모와 연결된 개체에 대한 추가 정보를 보려면 다음 관련 목록 중 하나를 클릭합니다.

관련 기록

필드	설명
외부 참조	STIX가 아닌 정보를 참조하는 외부 참조를 나열합니다. 이 속성은 하나 이상의 외부 객체 식별자를 제공하는 데 사용됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관련 기록

필드	설명
캠페인	이 객체와 연결된 캠페인을 나열합니다.
표시기	이 개체와 연결된 위협 소스에서 식별한 관련 IoC(침해 표시기)를 나열합니다.
인프라	시스템, 소프트웨어 서비스 및 이 객체와 연결된 연결된 모든 물리적 또는 가상 자원을 나열합니다.
침입 세트	이 객체와 관련된 공통 속성이 있는 일련의 적대적 동작 및 자원을 나열합니다.
위치	이 객체에 지리적 컨텍스트를 제공하는 위치를 나열합니다.
맬웨어	이 객체와 관련된 악성 코드를 나열합니다.
마케팅 정의	이 객체와 연결된 마케팅 정의를 나열합니다.
사이팅	이 객체와 연결된 사이팅을 나열합니다.
옵저버블	이 객체와 연결된 옵저버블을 나열합니다.
관찰 데이터	이 객체와 연결된 관찰 데이터를 나열합니다.
위협 액터	이 객체와 관련하여 악의적인 의도를 가지고 행동하는 개인, 그룹 또는 조직을 나열합니다.
위협 이벤트	이 개체와 연결된 위협 이벤트를 나열합니다.
도구	위협 행위자가 이 개체와 관련된 공격을 수행하는 데 사용하는 합법적인 소프트웨어를 나열합니다.
취약성	공격자가 악용하는 소프트웨어 또는 하드웨어의 약점 또는 결함을 나열합니다. 이 개체와 관련되어 있습니다.

주:

1. 이 객체와 연결된 관련 기록을 연결하거나 연결 해제할 수 있습니다. 자세한 내용은 위협 인텔리전스 관련 기록 연결 문서를 참조하십시오.
2. TI 라이브러리 내의 다양한 SDO에는 잠재적인 관계도 포함됩니다. 두 개체 간의 관계를 설정하려면 위협 인텔리전스 라이브러리의 **Potential** Relationships(잠재적 관계) 링크를 사용하여 개체 간의 관계를 확인합니다. 자세한 내용은 객체-객체 잠재성 관계 확인 문서를 참조하십시오.
3. 또한 객체 양식 뷰에서 관련 기록 섹션을 사용하면 양식 뷰에서 사용할 수 있는 잠재성 관계 섹션을 통해 두 객체 간의 관계를 확인할 수 있습니다. 에 대한 자세한 내용은 관련 기록에서 잠재성 관계 확인를 참조하십시오.
4. 케이스에 개체를 추가할 수 있습니다. 자세한 내용은 케이스에 추가 문서를 참조하십시오.

위협 의견

의견은 다른 엔터티에서 생성한 STIX 개체에 있는 정보의 정확성에 대한 평가입니다. 위협 의견은 STIX 2.x에 적용됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

의견 속성은 고정 척도를 사용하여 동의 또는 불일치 수준을 캡처합니다. 또한 고정 척도는 의견 간에 일관된 통계 연산을 가능하게 하는 숫자 매핑을 지원합니다.

예를 들어, 소비 조직의 분석가는 캠페인 개체에 "매우 동의하지 않는다"고 말하고 그 이유에 대한 설명을 제공할 수 있습니다.

의견은 주관적이며 사양은 이를 가장 잘 해석하는 방법을 다루지 않습니다.

인간 분석가는 의견을 만들고 인간 중심의 텍스트로 구성되며, 의견을 작성한 저자를 포착하기 위한 추가 속성을 포함합니다.

위협 의견 정의

위협 의견을 STIX 객체에 있는 정보의 정확성에 대한 평가로 정의합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 작업 공간에서 위협 인텔 라이브러리 아이콘을 클릭합니다.
3. 위협 의견 개체로 이동합니다.
4. 새로 만들기를 클릭합니다.

   주:
   옵저버블, 표시기, 엔터티 또는 객체에 대한 새 객체 기록을 생성할 때마다 소스 기록이 생성되고, 새 객체 기록이 생성된 다음 사용자가 집계된 기록으로 리디렉션된다는 프롬프트 메시지가 표시됩니다.

5. 양식에서 필드를 채웁니다.

위협 의견 상세 정보 뷰

필드	설명
ID	위협 의견의 고유 ID입니다.
의견	STIX 객체에 대한 생산자의 의견입니다.
설명	의견의 내용을 지정합니다.
작성자	작성자의 이름(예: 분석가)을 지정합니다.
TLP	TLP는 민감한 정보가 적절한 대상과 공유되도록 하는 데 사용됩니다. 4가지 색상(흰색, 녹색, 호박색, 빨간색)을 사용하여 다양한 민감도를 나타냅니다.
신뢰도	이 작업 과정에 대한 신뢰도를 입력합니다.
소스	이 개체 기록이 생성되는 위협 소스를 지정합니다.
해지함	해지된 개체가 개체 작성자에 의해 더 이상 유효한 것으로 간주되지 않음을 나타냅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

인사이트

필드	설명
메모	이 위협 의견에 대한 추가 메모를 추가합니다.

추가 정보

필드	설명
추가 컨텍스트	이 위협 의견에 대한 추가 컨텍스트를 추가합니다.
사양 버전	이 객체를 나타내는 데 사용되는 STIX 사양의 버전입니다. 이 특성에 대한 값은 이 사양에 따라 정의된 STIX 객체에 대해 2.1이어야 합니다.
언어	이 속성은 이 객체의 텍스트 컨텐츠 언어를 식별합니다.
소스에서 생성된 시간	원본에서 개체가 만들어지는 시간을 지정합니다.
확장명	공격 패턴의 확장을 나타냅니다.
소스에서 수정된 시간	원본에서 개체가 수정되는 시간을 지정합니다.
처리 상태	이 객체의 처리 상태, 작업 과정을 나타냅니다.
작성됨	소스에서 기록이 생성되는 시간을 지정합니다.
업데이트됨	소스에서 기록이 수정되는 시간을 지정합니다.
참조에 의해 생성됨	이 속성은 엔터티를 설명하는 ID 개체가 이 개체를 만들었음을 지정합니다.

6. 저장을 클릭합니다.
   저장하면 새 옵저버블 기록이 생성되었음을 나타내는 프롬프트 메시지가 표시됩니다. 기록을 편집하고 새 관계를 생성하려면 "계속 "을 클릭하십시오.
7. 계속을 클릭합니다.

> **중요사항:**
> 새 옵저버블 기록을 생성하면 시스템 업데이트 방지 확인란이 표시됩니다.
>
> 옵저버블, 표시기 또는 STIX 객체 기록이 생성된 후 시스템에서 업데이트를 방지하려면 이 확인란을 선택합니다.

태그&분류

필드	설명
태그	
태그 선택	위협 의견과 연결된 태그를 선택합니다.
태그 추가	새 태그를 추가합니다.
분류	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
분류 선택	이 위협 의견과 연결된 분류를 선택합니다.
분류 값 추가	이 위협 의견과 연결된 분류 값을 추가합니다.

다음에 수행할 작업

위협 의견과 연결된 개체에 대한 추가 정보를 보려면 다음 관련 목록 중 하나를 클릭합니다.

관련 기록

필드	설명
외부 참조	STIX가 아닌 정보를 참조하는 외부 참조를 나열합니다. 이 속성은 하나 이상의 외부 객체 식별자를 제공하는 데 사용됩니다.
캠페인	이 객체와 연결된 캠페인을 나열합니다.
표시기	이 개체와 연결된 위협 소스에서 식별한 관련 IoC(침해 표시기)를 나열합니다.
인프라	시스템, 소프트웨어 서비스 및 이 객체와 연결된 연결된 모든 물리적 또는 가상 자원을 나열합니다.
침입 세트	이 객체와 관련된 공통 속성이 있는 일련의 적대적 동작 및 자원을 나열합니다.
위치	이 객체에 지리적 컨텍스트를 제공하는 위치를 나열합니다.
맬웨어	이 객체와 관련된 악성 코드를 나열합니다.
마케팅 정의	이 객체와 연결된 마케팅 정의를 나열합니다.
사이팅	이 객체와 연결된 사이팅을 나열합니다.
옵저버블	이 객체와 연결된 옵저버블을 나열합니다.
관찰 데이터	이 객체와 연결된 관찰 데이터를 나열합니다.
위협 액터	이 객체와 관련하여 악의적인 의도를 가지고 행동하는 개인, 그룹 또는 조직을 나열합니다.
위협 이벤트	이 개체와 연결된 위협 이벤트를 나열합니다.
도구	위협 행위자가 이 개체와 관련된 공격을 수행하는 데 사용하는 합법적인 소프트웨어를 나열합니다.
취약성	공격자가 악용하는 소프트웨어 또는 하드웨어의 약점 또는 결함을 나열합니다. 이 개체와 관련되어 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

1. 이 객체와 연결된 관련 기록을 연결하거나 연결 해제할 수 있습니다. 자세한 내용은 위협 인텔리전스 관련 기록 연결 문서를 참조하십시오.
2. TI 라이브러리 내의 다양한 SDO에는 잠재적인 관계도 포함됩니다. 두 개체 간의 관계를 설정하려면 위협 인텔리전스 라이브러리의 **Potential** Relationships(잠재적 관계) 링크를 사용하여 개체 간의 관계를 확인합니다. 자세한 내용은 객체-객체 잠재성 관계 확인 문서를 참조하십시오.
3. 또한 객체 양식 뷰에서 관련 기록 섹션을 사용하면 양식 뷰에서 사용할 수 있는 잠재성 관계 섹션을 통해 두 객체 간의 관계를 확인할 수 있습니다. 에 대한 자세한 내용은 관련 기록에서 잠재성 관계 확인를 참조하십시오.
4. 케이스에 개체를 추가할 수 있습니다. 자세한 내용은 케이스에 추가 문서를 참조하십시오.

위협 보고서

위협 보고서는 하나 이상의 주제에 초점을 맞춘 위협 인텔리전스 모음입니다. 위협 보고서는 STIX 2.x에 적용됩니다.

위협 보고서에는 위협 행위자, 맬웨어, 공격 기술에 대한 설명(컨텍스트 및 관련 세부 정보 포함)이 포함됩니다. 관련 위협 인텔리전스를 그룹화하여 포괄적인 사이버 위협 스토리로 게시하는 데 사용됩니다.

위협 보고서 SDO에는 텍스트 설명 및 보고서 이름과 함께 STIX 개체에 대한 참조 목록이 포함되어 있습니다.

위협 보고서 정의

컨텍스트 및 관련 상세 정보를 포함하여 위협 행위자, 맬웨어, 공격 기술을 설명하는 위협 보고서를 정의합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 작업 공간에서 위협 인텔 라이브러리 아이콘을 클릭합니다.
3. 위협 보고서 개체로 이동합니다.
4. 새로 만들기를 클릭합니다.

   주:
   옵저버블, 표시기, 엔터티 또는 객체에 대한 새 객체 기록을 생성할 때마다 소스 기록이 생성되고, 새 객체 기록이 생성된 다음 사용자가 집계된 기록으로 리디렉션된다는 프롬프트 메시지가 표시됩니다.

5. 양식에서 필드를 채웁니다.

위협 보고서 상세 정보 뷰

필드	설명
ID	위협 보고서를 식별하는 이름을 지정합니다.
이름	메모 내용에 대한 간략한 요약을 지정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
설명	보고서에 대한 추가 인사이트와 컨텍스트를 제공하는 설명입니다.
보고서 유형	작성자의 이름(예: 분석가)을 지정합니다.
게시 날짜:	보고서 작성자가 이 보고서를 공식적으로 게시한 날짜입니다.
TLP	TLP는 민감한 정보가 적절한 대상과 공유되도록 하는 데 사용됩니다. 4가지 색상(흰색, 녹색, 호박색, 빨간색)을 사용하여 다양한 민감도를 나타냅니다.
소스	이 개체 기록이 생성되는 위협 소스를 지정합니다.
해지함	해지된 개체가 개체 작성자에 의해 더 이상 유효한 것으로 간주되지 않음을 나타냅니다.

인사이트

필드	설명
메모	이 위협 메모에 대한 추가 메모를 추가합니다.

추가 정보

필드	설명
추가 컨텍스트	이 공격 패턴에 대한 추가 컨텍스트를 추가합니다.
사양 버전	이 객체를 나타내는 데 사용되는 STIX 사양의 버전입니다. 이 특성에 대한 값은 이 사양에 따라 정의된 STIX 객체에 대해 2.1이어야 합니다.
언어	이 속성은 이 객체의 텍스트 컨텐츠 언어를 식별합니다.
소스에서 생성된 시간	원본에서 개체가 만들어지는 시간을 지정합니다.
확장명	공격 패턴의 확장을 나타냅니다.
소스에서 수정된 시간	원본에서 개체가 수정되는 시간을 지정합니다.
처리 상태	이 객체의 처리 상태, 작업 과정을 나타냅니다.
작성됨	원본에서 객체가 만들어진 날짜 및 시간을 지정합니다.
업데이트됨	원본에서 객체가 업데이트된 날짜 및 시간을 지정합니다.
참조에 의해 생성됨	이 속성은 엔터티를 설명하는 ID 개체가 이 개체를 만들었음을 지정합니다.

6. 저장을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

저장하면 새 옵저버블 기록이 생성되었음을 나타내는 프롬프트 메시지가 표시됩니다. 기록을 편집하고 새 관계를 생성하려면 "계속 "을 클릭하십시오.

7. 계속을 클릭합니다.

> **중요사항:**
> 새 옵저버블 기록을 생성하면 시스템 업데이트 방지 확인란이 표시됩니다.
>
> 옵저버블, 표시기 또는 STIX 객체 기록이 생성된 후 시스템에서 업데이트를 방지하려면 이 확인란을 선택합니다.

태그&분류

필드	설명
태그	
태그 선택	위협 그룹화와 연결된 태그를 선택합니다.
태그 추가	새 태그를 추가합니다.
분류	
분류 선택	이 위협 그룹화와 연결된 분류를 선택합니다.
분류 값 추가	이 위협 그룹화와 연결된 분류 값을 추가합니다.

다음에 수행할 작업

위협 보고서와 연결된 개체에 대한 추가 정보를 보려면 다음 관련 목록 중 하나를 클릭합니다.

관련 기록

필드	설명
외부 참조	STIX가 아닌 정보를 참조하는 외부 참조를 나열합니다. 이 속성은 하나 이상의 외부 객체 식별자를 제공하는 데 사용됩니다.
캠페인	이 객체와 연결된 캠페인을 나열합니다.
표시기	이 개체와 연결된 위협 소스에서 식별한 관련 IoC(침해 표시기)를 나열합니다.
인프라	시스템, 소프트웨어 서비스 및 이 객체와 연결된 연결된 모든 물리적 또는 가상 자원을 나열합니다.
침입 세트	이 객체와 관련된 공통 속성이 있는 일련의 적대적 동작 및 자원을 나열합니다.
위치	이 객체에 지리적 컨텍스트를 제공하는 위치를 나열합니다.
맬웨어	이 객체와 관련된 악성 코드를 나열합니다.
마케팅 정의	이 객체와 연결된 마케팅 정의를 나열합니다.
사이팅	이 객체와 연결된 사이팅을 나열합니다.
옵저버블	이 객체와 연결된 옵저버블을 나열합니다.
관찰 데이터	이 객체와 연결된 관찰 데이터를 나열합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관련 기록

필드	설명
위협 액터	이 객체와 관련하여 악의적인 의도를 가지고 행동하는 개인, 그룹 또는 조직을 나열합니다.
위협 이벤트	이 개체와 연결된 위협 이벤트를 나열합니다.
위협 그룹화	이 개체와 연결된 위협 그룹을 나열합니다.
위협 보고서	이 개체와 연결된 위협 보고서를 나열합니다.
도구	위협 행위자가 이 개체와 관련된 공격을 수행하는 데 사용하는 합법적인 소프트웨어를 나열합니다.
취약성	공격자가 악용하는 소프트웨어 또는 하드웨어의 약점 또는 결함을 나열합니다. 이 개체와 관련되어 있습니다.

주:

1. 이 객체와 연결된 관련 기록을 연결하거나 연결 해제할 수 있습니다. 자세한 내용은 위협 인텔리전스 관련 기록 연결 문서를 참조하십시오.
2. TI 라이브러리 내의 다양한 SDO에는 잠재적인 관계도 포함됩니다. 두 개체 간의 관계를 설정하려면 위협 인텔리전스 라이브러리의 **Potential** Relationships(잠재적 관계) 링크를 사용하여 개체 간의 관계를 확인합니다. 자세한 내용은 객체-객체 잠재성 관계 확인 문서를 참조하십시오.
3. 또한 객체 양식 뷰에서 관련 기록 섹션을 사용하면 양식 뷰에서 사용할 수 있는 잠재성 관계 섹션을 통해 두 객체 간의 관계를 확인할 수 있습니다. 에 대한 자세한 내용은 관련 기록에서 잠재성 관계 확인를 참조하십시오.
4. 케이스에 개체를 추가할 수 있습니다. 자세한 내용은 케이스에 추가 문서를 참조하십시오.

도구

도구는 위협 행위자가 공격을 수행하는 데 사용하는 합법적인 소프트웨어입니다. 도구는 STIX 2.x에 적용됩니다.

도구를 사용하면 위협 행위자가 캠페인을 실행하기 위해 도구를 사용하는 방법과 시기를 알 수 있습니다. 맬웨어와 달리 이러한 도구 또는 소프트웨어 패키지는 종종 시스템에서 발견되며 고급 사용자, 관리자, 네트워크 관리자 또는 일반 사용자를 위한 합법적인 목적을 가지고 있습니다.

예를 들어 원격 액세스 도구(RDP) 및 네트워크 검색 도구(Nmap)는 위협 행위자가 공격 중에 사용하는 도구입니다.

도구 정의

도구를 공격을 수행하는 데 사용되는 합법적인 소프트웨어로 정의합니다.

시작하기 전에

필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 작업 공간에서 위협 인텔 라이브러리 아이콘을 클릭합니다.
3. 도구 개체로 이동합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 새로 만들기를 클릭합니다.

   주:
   옵저버블, 표시기, 엔터티 또는 객체에 대한 새 객체 기록을 생성할 때마다 소스 기록이 생성되고, 새 객체 기록이 생성된 다음 사용자가 집계된 기록으로 리디렉션된다는 프롬프트 메시지가 표시됩니다.

5. 양식에서 필드를 채웁니다.

도구 상세 정보 뷰

필드	설명
ID	도구를 식별하는 고유 ID입니다.
이름	도구를 식별하는 설명이 포함된 이름을 입력합니다.
설명	도구의 목적과 주요 특성을 포함하여 도구에 대한 자세한 내용과 컨텍스트를 제공하는 설명입니다.
도구 유형	설명 중인 도구의 종류입니다.
별칭	이 도구를 식별하는 데 사용되는 대체 이름입니다. 주: 애플리케이션에 없는 새 별칭을 추가하려면 별칭 필드 자체에 있는 새 별칭 추가 아이콘을 클릭합니다.
도구 버전	도구와 연결된 버전 식별자입니다.
공격 단계	LM, MITRE ATT&CK와 같은 킬 체인의 공격 단계를 나타냅니다.
TLP	TLP는 민감한 정보가 적절한 대상과 공유되도록 하는 데 사용됩니다. 4가지 색상(흰색, 녹색, 호박색, 빨간색)을 사용하여 다양한 민감도를 나타냅니다.
소스	이 개체 기록이 생성되는 위협 소스를 지정합니다.
해지함	해지된 개체가 개체 작성자에 의해 더 이상 유효한 것으로 간주되지 않음을 나타냅니다.

인사이트

필드	설명
메모	이 도구에 대한 추가 참고 사항을 추가합니다.

추가 정보

필드	설명
추가 컨텍스트	이 도구에 대한 추가 컨텍스트를 추가합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
사양 버전	이 객체를 나타내는 데 사용되는 STIX 사양의 버전입니다. 이 특성에 대한 값은 이 사양에 따라 정의된 STIX 객체에 대해 2.1이어야 합니다.
언어	이 속성은 이 객체의 텍스트 컨텐츠 언어를 식별합니다.
소스에서 생성된 시간	원본에서 개체가 만들어지는 시간을 지정합니다.
확장명	공격 패턴의 확장을 나타냅니다.
소스에서 수정된 시간	원본에서 개체가 수정되는 시간을 지정합니다.
처리 상태	이 객체의 처리 상태, 작업 과정을 나타냅니다.
작성됨	원본에서 객체가 만들어진 날짜 및 시간을 지정합니다.
업데이트됨	원본에서 객체가 업데이트된 날짜 및 시간을 지정합니다.
참조에 의해 생성됨	이 속성은 엔터티를 설명하는 ID 개체가 이 개체를 만들었음을 지정합니다.

6. 저장을 클릭합니다.
   저장하면 새 옵저버블 기록이 생성되었음을 나타내는 프롬프트 메시지가 표시됩니다. 기록을 편집하고 새 관계를 생성하려면 "계속 "을 클릭하십시오.
7. 계속을 클릭합니다.

> **중요사항:**
> 새 옵저버블 기록을 생성하면 시스템 업데이트 방지 확인란이 표시됩니다.
>
> 옵저버블, 표시기 또는 STIX 객체 기록이 생성된 후 시스템에서 업데이트를 방지하려면 이 확인란을 선택합니다.

태그&분류

필드	설명
태그	
태그 선택	위협 그룹화와 연결된 태그를 선택합니다.
태그 추가	새 태그를 추가합니다.
분류	
분류 선택	이 위협 그룹화와 연결된 분류를 선택합니다.
분류 값 추가	이 위협 그룹화와 연결된 분류 값을 추가합니다.

다음에 수행할 작업

다음 관련 목록 중 하나를 클릭하면 도구와 연관된 객체에 대한 추가 정보를 볼 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관련 기록

필드	설명
외부 참조	STIX가 아닌 정보를 참조하는 외부 참조를 나열합니다. 이 속성은 하나 이상의 외부 객체 식별자를 제공하는 데 사용됩니다.
캠페인	이 객체와 연결된 캠페인을 나열합니다.
탐지 및 완화	이 객체와 관련된 탐지 및 완화 기능을 나열합니다.
표시기	이 개체와 연결된 위협 소스에서 식별한 관련 IoC(침해 표시기)를 나열합니다.
인프라	시스템, 소프트웨어 서비스 및 이 객체와 연결된 연결된 모든 물리적 또는 가상 자원을 나열합니다.
침입 세트	이 객체와 관련된 공통 속성이 있는 일련의 적대적 동작 및 자원을 나열합니다.
위치	이 객체에 지리적 컨텍스트를 제공하는 위치를 나열합니다.
맬웨어	이 객체와 관련된 악성 코드를 나열합니다.
마케팅 정의	이 객체와 연결된 마케팅 정의를 나열합니다.
사이팅	이 객체와 연결된 사이팅을 나열합니다.
옵저버블	이 객체와 연결된 옵저버블을 나열합니다.
관찰 데이터	이 객체와 연결된 관찰 데이터를 나열합니다.
위협 액터	이 객체와 관련하여 악의적인 의도를 가지고 행동하는 개인, 그룹 또는 조직을 나열합니다.
취약성	공격자가 악용하는 소프트웨어 또는 하드웨어의 약점 또는 결함을 나열합니다. 이 개체와 관련되어 있습니다.

주:

1. 이 객체와 연결된 관련 기록을 연결하거나 연결 해제할 수 있습니다. 자세한 내용은 위협 인텔리전스 관련 기록 연결 문서를 참조하십시오.
2. TI 라이브러리 내의 다양한 SDO에는 잠재적인 관계도 포함됩니다. 두 개체 간의 관계를 설정하려면 위협 인텔리전스 라이브러리의 **Potential** Relationships(잠재적 관계) 링크를 사용하여 개체 간의 관계를 확인합니다. 자세한 내용은 객체-객체 잠재성 관계 확인 문서를 참조하십시오.
3. 또한 객체 양식 뷰에서 관련 기록 섹션을 사용하면 양식 뷰에서 사용할 수 있는 잠재성 관계 섹션을 통해 두 객체 간의 관계를 확인할 수 있습니다. 에 대한 자세한 내용은 관련 기록에서 잠재성 관계 확인를 참조하십시오.
4. 케이스에 개체를 추가할 수 있습니다. 자세한 내용은 케이스에 추가 문서를 참조하십시오.

취약성

취약성은 공격자가 악용하는 소프트웨어 또는 하드웨어 구성요소의 약점 또는 결함입니다. STIX 2.x에 적용되는 취약성입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

약점 또는 결함은 소프트웨어 또는 하드웨어 구성요소에 있는 코드의 요구 사항, 디자인 또는 구현에 있습니다. 이 약점은 해당 시스템의 기밀성, 무결성 또는 가용성에 부정적인 영향을 미치기 위해 직접 악용됩니다.

CVE는 공개적으로 알려진 문제(CVE)에 대한 일반적인 이름을 제공하는 정보 보안 취약성 및 노출 목록입니다.

예를 들어 맬웨어가 CVE-2015-12345를 악용하는 경우 맬웨어 개체가 CVE-2015-12345를 참조하는 취약성 개체에 연결될 수 있습니다.

취약성 정의

취약성을 공격자가 악용하는 소프트웨어 또는 하드웨어 구성요소의 약점 또는 결함으로 정의합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 작업 공간에서 위협 인텔 라이브러리 아이콘을 클릭합니다.
3. 취약성 객체로 이동합니다.
4. 새로 만들기를 클릭합니다.

   주:
   옵저버블, 표시기, 엔터티 또는 객체에 대한 새 객체 기록을 생성할 때마다 소스 기록이 생성되고, 새 객체 기록이 생성된 다음 사용자가 집계된 기록으로 리디렉션된다는 프롬프트 메시지가 표시됩니다.

5. 양식에서 필드를 채웁니다.

취약성 상세 정보 뷰

필드	설명
ID	취약성을 식별하기 위한 고유 ID입니다.
이름	취약성을 식별하는 데 사용되는 이름입니다.
설명	취약성의 목적과 주요 특성을 포함하여 취약성에 대한 자세한 내용과 컨텍스트를 제공하는 설명입니다.
심각도	이 취약성의 표준화된 심각도 수준을 나타냅니다.
CVSS3.0	이 취약성에 대한 CVSS v3을 나타냅니다.
CVSS2.0	이 취약성에 대한 CVSS v2를 나타냅니다.
취약점 공격 상태	이 취약성과 연관된 악용 상태를 나타냅니다.
게시 날짜:	취약성이 게시된 시기를 나타냅니다.
마지막으로 수정된 기록	기록이 마지막으로 수정된 시기를 나타냅니다.
영향을 받는 소프트웨어	취약성과 연관된 영향을 받는 소프트웨어를 나열합니다.
TLP	TLP는 민감한 정보가 적절한 대상과 공유되도록 하는 데 사용됩니다. 4가지 색상

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	(흰색, 녹색, 호박색, 빨간색)을 사용하여 다양한 민감도를 나타냅니다.
소스	이 개체 기록이 생성되는 위협 소스를 지정합니다.
해지함	해지된 개체가 개체 작성자에 의해 더 이상 유효한 것으로 간주되지 않음을 나타냅니다.

인사이트

필드	설명
메모	이 취약성에 대한 추가 참고 사항을 추가하십시오.

추가 정보

필드	설명
추가 컨텍스트	이 취약성에 대한 추가 컨텍스트를 추가합니다.
사양 버전	이 객체를 나타내는 데 사용되는 STIX 사양의 버전입니다. 이 특성에 대한 값은 이 사양에 따라 정의된 STIX 객체에 대해 2.1이어야 합니다.
언어	이 속성은 이 객체의 텍스트 컨텐츠 언어를 식별합니다.
소스에서 생성된 시간	원본에서 개체가 만들어지는 시간을 지정합니다.
확장명	공격 패턴의 확장을 나타냅니다.
소스에서 수정된 시간	원본에서 개체가 수정되는 시간을 지정합니다.
처리 상태	이 객체의 처리 상태, 작업 과정을 나타냅니다.
작성됨	원본에서 객체가 만들어진 날짜 및 시간을 지정합니다.
업데이트됨	원본에서 객체가 업데이트된 날짜 및 시간을 지정합니다.
참조에 의해 생성됨	이 속성은 엔터티를 설명하는 ID 개체가 이 개체를 만들었음을 지정합니다.

6. 저장을 클릭합니다.
   저장하면 새 옵저버블 기록이 생성되었음을 나타내는 프롬프트 메시지가 표시됩니다. 기록을 편집하고 새 관계를 생성하려면 "계속 "을 클릭하십시오.
7. 계속을 클릭합니다.

중요사항:
새 옵저버블 기록을 생성하면 시스템 업데이트 방지 확인란이 표시됩니다.

옵저버블, 표시기 또는 STIX 객체 기록이 생성된 후 시스템에서 업데이트를 방지하려면 이 확인란을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

태그&분류

필드	설명
태그	
태그 선택	취약성과 관련된 태그를 선택합니다.
태그 추가	새 태그를 추가합니다.
분류	
분류 선택	이 취약성과 관련된 분류를 선택합니다.
분류 값 추가	이 취약성과 연관된 분류 값을 추가합니다.

다음에 수행할 작업
취약성과 관련된 개체에 대한 추가 정보를 보려면 다음 관련 목록 중 하나를 클릭하십시오.

관련 기록

필드	설명
외부 참조	STIX가 아닌 정보를 참조하는 외부 참조를 나열합니다. 이 속성은 하나 이상의 외부 객체 식별자를 제공하는 데 사용됩니다.
캠페인	이 객체와 연결된 캠페인을 나열합니다.
탐지 및 완화	이 객체와 관련된 탐지 및 완화 기능을 나열합니다.
표시기	이 개체와 연결된 위협 소스에서 식별한 관련 IoC(침해 표시기)를 나열합니다.
인프라	시스템, 소프트웨어 서비스 및 이 객체와 연결된 연결된 모든 물리적 또는 가상 자원을 나열합니다.
침입 세트	이 객체와 관련된 공통 속성이 있는 일련의 적대적 동작 및 자원을 나열합니다.
위치	이 객체에 지리적 컨텍스트를 제공하는 위치를 나열합니다.
맬웨어	이 객체와 관련된 악성 코드를 나열합니다.
마케팅 정의	이 객체와 연결된 마케팅 정의를 나열합니다.
사이팅	이 객체와 연결된 사이팅을 나열합니다.
옵저버블	이 객체와 연결된 옵저버블을 나열합니다.
관찰 데이터	이 객체와 연결된 관찰 데이터를 나열합니다.
위협 액터	이 객체와 관련하여 악의적인 의도를 가지고 행동하는 개인, 그룹 또는 조직을 나열합니다.
취약성	공격자가 악용하는 소프트웨어 또는 하드웨어의 약점 또는 결함을 나열합니다. 이 개체와 관련되어 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

1. 이 객체와 연결된 관련 기록을 연결하거나 연결 해제할 수 있습니다. 자세한 내용은 위협 인텔리전스 관련 기록 연결 문서를 참조하십시오.
2. TI 라이브러리 내의 다양한 SDO에는 잠재적인 관계도 포함됩니다. 두 개체 간의 관계를 설정하려면 위협 인텔리전스 라이브러리의 **Potential** Relationships(잠재적 관계) 링크를 사용하여 개체 간의 관계를 확인합니다. 자세한 내용은 객체-객체 잠재성 관계 확인 문서를 참조하십시오.
3. 또한 객체 양식 뷰에서 관련 기록 섹션을 사용하면 양식 뷰에서 사용할 수 있는 잠재성 관계 섹션을 통해 두 객체 간의 관계를 확인할 수 있습니다. 에 대한 자세한 내용은 관련 기록에서 잠재성 관계 확인를 참조하십시오.
4. 케이스에 개체를 추가할 수 있습니다. 자세한 내용은 케이스에 추가 문서를 참조하십시오.

취약성 데이터 가져오기

구성 항목, 취약 항목 및 비즈니스 컨텍스트와 같은 취약성 관련 데이터를 가져옵니다.

시작하기 전에

필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 작업 공간에서 위협 인텔 라이브러리 아이콘을 클릭합니다.
3. 취약성 객체로 이동합니다.
   이 개체와 연결된 관련 취약성이 표시됩니다.
4. 해당 취약성 레코드를 선택합니다.
   관련된 CVE가 있는 경우 제공된 버튼을 사용하여 취약한 관련 데이터를 자동으로 가져올 수 있으며 이러한 관련 기록은 취약성의 비즈니스 컨텍스트 섹션에 표시됩니다.
5. 이동 내부 인텔리전스 〉 취약한 항목.
   연결된 CVE 기록이 표시됩니다.
6. CVE를 선택하고 취약성 관련 데이터 가져오기 버튼을 클릭합니다.

   주:

   - 이 링크는 자동으로 기록을 연결하고 기록의 특정 비즈니스 컨텍스트를 가져옵니다.
   - 연결된 기록이 없는 경우 다음과 같은 정보 메시지가 표시됩니다. 이 특정 취약성 객체에는 연결된 취약 항목이 없습니다. 데이터를 가져오려면 개체를 취약한 항목에 수동으로 연결해야 합니다.
   - 이 버튼을 누르면 백그라운드 예약 작업이 트리거되고 작업 시작 및 실행 상세 정보가 활동 스트림 섹션에 표시됩니다. 예를 들어 작업이 트리거되면 활동 스트림에 취약 항목과 연결된 데이터 가져오기 시작 활동이 표시됩니다. 데이터를 가져오기 위해 예약된 작업을 실행하는 방법에 대한 자세한 내용은 예약된 작업을 참조하십시오.

7. 링크를 클릭하여 개체를 수동으로 연결합니다.
8. 연결할 기록을 선택하고 취약성 관련 데이터 가져오기 버튼을 사용하여 취약성 관련 데이터를 가져옵니다.
   이 버튼을 클릭하면 백그라운드 작업이 트리거되고 데이터를 해당 섹션으로 자동으로 가져옵니다. 취약 항목과 관련된 데이터를 가져오는 작업이 시작되었다는 메시지가 표시됩니다. 활동 스트림에서 상태를 추적하고 작업이 완료되면 목록을 새로 고쳐 결과를 확인할 수 있습니다. 예를

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

들어, 데이터가 구성 항목과 관련된 경우 구성 항목 섹션에서 결과를 확인합니다. CVE 추가에 대한 자세한 내용은 타사 항목에 CVE 추가를 참조하십시오.

> **주:**
> 마찬가지로 옵저버블 기록 데이터를 가져올 수 있습니다. 자세한 내용은 취약성 데이터 가져오기 문서를 참조하십시오.

표시 정의

마킹 정의 개체는 특정 마킹을 나타냅니다. 데이터 표시는 일반적으로 데이터에 대한 처리 또는 공유 요구 사항을 나타냅니다.

표시 정의 정의

데이터에 대한 요구 사항을 처리하고 공유하기 위한 표시 정의를 정의합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 작업 공간에서 위협 인텔 라이브러리 아이콘을 클릭합니다.
3. 표시 정의 개체로 이동합니다.
4. 새로 만들기를 클릭합니다.

> **주:**
> 옵저버블, 표시기, 엔터티 또는 객체에 대한 새 객체 기록을 생성할 때마다 소스 기록이 생성되고, 새 객체 기록이 생성된 다음 사용자가 집계된 기록으로 리디렉션된다는 프롬프트 메시지가 표시됩니다.

5. 양식에서 필드를 채웁니다.

표시 정의 소스 상세 정보 뷰

필드	설명
ID	표시 정의를 식별하는 고유 ID입니다.
이름	표시 정의를 식별하는 데 사용되는 이름입니다.
정의 유형	type 속성은 객체의 유형을 식별합니다. definition_type 속성은 표시 정의의 유형을 식별합니다.
정의	정의 속성에는 표시 개체 자체(예: TLP)가 포함됩니다.
TLP	TLP는 민감한 정보가 적절한 대상과 공유되도록 하는 데 사용됩니다. 4가지 색상(흰색, 녹색, 호박색, 빨간색)을 사용하여 다양한 민감도를 나타냅니다.
신뢰도	이 객체에 대한 신뢰도를 입력합니다. confidence 속성은 작성자가 데이터의 정확성에 대해 가지고 있는 신뢰도를

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	식별합니다. 신뢰도 값은 0-100 범위의 숫자여야 합니다(MUST).

인사이트

필드	설명
메모	이 표시 정의에 대한 추가 참고 사항을 추가합니다.

추가 정보

필드	설명
추가 컨텍스트	이 표시 정의에 대한 추가 컨텍스트를 추가합니다.
사양 버전	이 객체를 나타내는 데 사용되는 STIX 사양의 버전입니다. 이 특성에 대한 값은 이 사양에 따라 정의된 STIX 객체에 대해 2.1이어야 합니다.
언어	이 속성은 이 객체의 텍스트 컨텐츠 언어를 식별합니다.
소스에서 생성된 시간	원본에서 개체가 만들어지는 시간을 지정합니다.
확장명	공격 패턴의 확장을 나타냅니다.
소스에서 수정된 시간	원본에서 개체가 수정되는 시간을 지정합니다.
처리 상태	이 객체의 처리 상태, 작업 과정을 나타냅니다.
작성됨	원본에서 객체가 만들어진 날짜 및 시간을 지정합니다.
업데이트됨	원본에서 객체가 업데이트된 날짜 및 시간을 지정합니다.
참조에 의해 생성됨	이 속성은 엔터티를 설명하는 ID 개체가 이 개체를 만들었음을 지정합니다.

6. 저장을 클릭합니다.
저장하면 새 옵저버블 기록이 생성되었음을 나타내는 프롬프트 메시지가 표시됩니다. 기록을 편집하고 새 관계를 생성하려면 "계속 "을 클릭하십시오.
7. 계속을 클릭합니다.

중요사항:
새 옵저버블 기록을 생성하면 시스템 업데이트 방지 확인란이 표시됩니다.

옵저버블, 표시기 또는 STIX 객체 기록이 생성된 후 시스템에서 업데이트를 방지하려면 이 확인란을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

태그&분류

필드	설명
태그	
태그 선택	취약성과 관련된 태그를 선택합니다.
태그 추가	새 태그를 추가합니다.
분류	
분류 선택	이 취약성과 관련된 분류를 선택합니다.
분류 값 추가	이 취약성과 연관된 분류 값을 추가합니다.

다음에 수행할 작업
취약성과 관련된 개체에 대한 추가 정보를 보려면 다음 관련 목록 중 하나를 클릭하십시오.

관련 기록

필드	설명
외부 참조	STIX가 아닌 정보를 참조하는 외부 참조를 나열합니다. 이 속성은 하나 이상의 외부 객체 식별자를 제공하는 데 사용됩니다.
공격 패턴	이 객체와 관련된 공격 패턴을 나열합니다.
캠페인	이 객체와 연결된 캠페인을 나열합니다.
탐지 및 완화	이 객체와 관련된 탐지 및 완화 기능을 나열합니다.
ID	이 객체와 연결된 ID를 나열합니다.
표시기	이 개체와 연결된 위협 소스에서 식별한 관련 IoC(침해 표시기)를 나열합니다.
인프라	시스템, 소프트웨어 서비스 및 이 객체와 연결된 연결된 모든 물리적 또는 가상 자원을 나열합니다.
침입 세트	이 객체와 관련된 공통 속성이 있는 일련의 적대적 동작 및 자원을 나열합니다.
위치	이 객체에 지리적 컨텍스트를 제공하는 위치를 나열합니다.
맬웨어	이 객체와 관련된 악성 코드를 나열합니다.
맬웨어 분석	이 개체와 관련된 악성 분석을 나열합니다.
옵저버블	이 객체와 연결된 옵저버블을 나열합니다.
관찰 데이터	이 객체와 연결된 관찰 데이터를 나열합니다.
위협 액터	이 객체와 관련하여 악의적인 의도를 가지고 행동하는 개인, 그룹 또는 조직을 나열합니다.
위협 이벤트	이 객체와 연결된 위협 이벤트를 나열합니다.
위협 그룹화	이 개체와 연결된 위협 그룹을 나열합니다.
위협 메모	이 객체와 연관된 위협 메모를 나열합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관련 기록

필드	설명
위협 의견	이 객체와 연관된 위협 의견을 나열합니다.
도구	이 객체와 연결된 도구를 나열합니다.
취약성	이 개체와 관련된 취약성을 나열합니다.

주:

1. 이 객체와 연결된 관련 기록을 연결하거나 연결 해제할 수 있습니다. 자세한 내용은 위협 인텔리전스 관련 기록 연결 문서를 참조하십시오.
2. TI 라이브러리 내의 다양한 SDO에는 잠재적인 관계도 포함됩니다. 두 개체 간의 관계를 설정하려면 위협 인텔리전스 라이브러리의 **Potential** Relationships(잠재적 관계) 링크를 사용하여 개체 간의 관계를 확인합니다. 자세한 내용은 객체-객체 잠재성 관계 확인 문서를 참조하십시오.
3. 또한 객체 양식 뷰에서 관련 기록 섹션을 사용하면 양식 뷰에서 사용할 수 있는 잠재성 관계 섹션을 통해 두 객체 간의 관계를 확인할 수 있습니다. 에 대한 자세한 내용은 관련 기록에서 잠재성 관계 확인를 참조하십시오.
4. 케이스에 개체를 추가할 수 있습니다. 자세한 내용은 케이스에 추가 문서를 참조하십시오.

데이터 구성요소

데이터 구성요소는 데이터 소스의 특정 속성 또는 값을 식별하는 데 사용됩니다.

데이터 구성요소 정의

데이터 소스의 속성 또는 값을 식별하는 데이터 구성요소 정의

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 작업 공간에서 위협 인텔 라이브러리 아이콘을 클릭합니다.
3. 데이터 구성요소 객체로 이동합니다.
4. 새로 만들기를 클릭합니다.

주:
옵저버블, 표시기, 엔터티 또는 객체에 대한 새 객체 기록을 생성할 때마다 소스 기록이 생성되고, 새 객체 기록이 생성된 다음 사용자가 집계된 기록으로 리디렉션된다는 프롬프트 메시지가 표시됩니다.

5. 양식에서 필드를 채웁니다.

데이터 구성요소 상세 정보 뷰

필드	설명
ID	데이터 구성요소를 식별하는 고유 ID입니다.
이름	데이터 구성요소를 식별하는 데 사용되는 이름입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
설명	취약성의 목적과 주요 특성을 포함하여 취약성에 대한 자세한 내용과 컨텍스트를 제공하는 설명입니다.
데이터 소스	이 취약성의 표준화된 심각도 수준을 나타냅니다.
TLP	TLP는 민감한 정보가 적절한 대상과 공유되도록 하는 데 사용됩니다. 4가지 색상(흰색, 녹색, 호박색, 빨간색)을 사용하여 다양한 민감도를 나타냅니다.
소스	이 개체 기록이 생성되는 위협 소스를 지정합니다.
신뢰도	이 객체에 대한 신뢰도를 나타냅니다. 신뢰도는 0-100 사이여야 합니다.
해지함	해지된 개체가 개체 작성자에 의해 더 이상 유효한 것으로 간주되지 않음을 나타냅니다.

인사이트

필드	설명
메모	이 데이터 구성요소에 대한 추가 메모를 추가합니다.

추가 정보

필드	설명
추가 컨텍스트	이 데이터 구성요소에 대한 추가 컨텍스트를 추가합니다.
사양 버전	이 객체를 나타내는 데 사용되는 STIX 사양의 버전입니다. 이 특성에 대한 값은 이 사양에 따라 정의된 STIX 객체에 대해 2.1이어야 합니다.
언어	이 속성은 이 객체의 텍스트 컨텐츠 언어를 식별합니다.
소스에서 생성된 시간	원본에서 개체가 만들어지는 시간을 지정합니다.
확장명	데이터 구성요소의 확장을 나타냅니다.
소스에서 수정된 시간	원본에서 개체가 수정되는 시간을 지정합니다.
처리 상태	이 객체의 처리 상태, 작업 과정을 나타냅니다.
작성됨	원본에서 객체가 만들어진 날짜 및 시간을 지정합니다.
업데이트됨	원본에서 객체가 업데이트된 날짜 및 시간을 지정합니다.
참조에 의해 생성됨	이 속성은 엔터티를 설명하는 ID 개체가 이 개체를 만들었음을 지정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

6. 저장을 클릭합니다.
   저장하면 새 옵저버블 기록이 생성되었음을 나타내는 프롬프트 메시지가 표시됩니다. 기록을 편집하고 새 관계를 생성하려면 "계속 "을 클릭하십시오.
7. 계속을 클릭합니다.

> **중요사항:**
> 새 옵저버블 기록을 생성하면 시스템 업데이트 방지 확인란이 표시됩니다.
>
> 옵저버블, 표시기 또는 STIX 객체 기록이 생성된 후 시스템에서 업데이트를 방지하려면 이 확인란을 선택합니다.

태그&분류

필드	설명
태그	
태그 선택	취약성과 관련된 태그를 선택합니다.
태그 추가	새 태그를 추가합니다.
분류	
분류 선택	이 취약성과 관련된 분류를 선택합니다.
분류 값 추가	이 취약성과 연관된 분류 값을 추가합니다.

다음에 수행할 작업
데이터 구성요소와 연관된 객체에 대한 추가 정보를 보려면 다음 관련 목록 중 하나를 클릭하십시오.

관련 기록

필드	설명
공격 패턴	이 객체와 관련된 공격 패턴을 나열합니다.

> **주:**

1. 이 객체와 연결된 관련 기록을 연결하거나 연결 해제할 수 있습니다. 자세한 내용은 위협 인텔리전스 관련 기록 연결 문서를 참조하십시오.
2. TI 라이브러리 내의 다양한 SDO에는 잠재적인 관계도 포함됩니다. 두 개체 간의 관계를 설정하려면 위협 인텔리전스 라이브러리의 **Potential** Relationships(잠재적 관계) 링크를 사용하여 개체 간의 관계를 확인합니다. 자세한 내용은 객체-객체 잠재성 관계 확인 문서를 참조하십시오.
3. 또한 객체 양식 뷰에서 관련 기록 섹션을 사용하면 양식 뷰에서 사용할 수 있는 잠재성 관계 섹션을 통해 두 객체 간의 관계를 확인할 수 있습니다. 에 대한 자세한 내용은 관련 기록에서 잠재성 관계 확인를 참조하십시오.
4. 케이스에 개체를 추가할 수 있습니다. 자세한 내용은 케이스에 추가 문서를 참조하십시오.

데이터 소스

데이터 소스는 센서/로그로 수집할 수 있는 다양한 정보 주제/주제를 나타냅니다. 데이터 소스에는 데이터 소스의 특정 속성/값을 식별하는 데이터 구성요소도 포함됩니다.

데이터 소스 정의

정보의 다양한 주제 또는 주제를 나타내는 데이터 소스를 정의합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 작업 공간에서 위협 인텔 라이브러리 아이콘을 클릭합니다.
3. 데이터 소스 개체로 이동합니다.
4. 새로 만들기를 클릭합니다.

   주:
   옵저버블, 표시기, 엔터티 또는 객체에 대한 새 객체 기록을 생성할 때마다 소스 기록이 생성되고, 새 객체 기록이 생성된 다음 사용자가 집계된 기록으로 리디렉션된다는 프롬프트 메시지가 표시됩니다.

5. 양식에서 필드를 채웁니다.

취약성 상세 정보 뷰

필드	설명
ID	데이터 소스를 식별하는 고유 ID입니다.
이름	데이터 소스를 식별하는 데 사용되는 이름입니다.
설명	목적 및 주요 특성을 포함하여 데이터 소스에 대한 자세한 내용과 컨텍스트를 제공하는 설명입니다.
컬렉션 계층	호스트, 네트워크, 클라우드 컨트롤 플레인 등과 같이 데이터 소스를 물리적으로 수집할 수 있는 위치에 대한 설명을 나타냅니다.
플랫폼	악의적 사용자가 작동 중인 시스템이 운영 체제 또는 애플리케이션일 수 있음을 나타냅니다.
기고자	이 데이터 소스의 기고자를 나타냅니다.
TLP	TLP는 민감한 정보가 적절한 대상과 공유되도록 하는 데 사용됩니다. 4가지 색상(흰색, 녹색, 호박색, 빨간색)을 사용하여 다양한 민감도를 나타냅니다.
소스	이 개체 기록이 생성되는 위협 소스를 지정합니다.
해지함	해지된 개체가 개체 작성자에 의해 더 이상 유효한 것으로 간주되지 않음을 나타냅니다.

인사이트

필드	설명
메모	이 데이터 소스에 대한 추가 메모를 추가합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

추가 정보

필드	설명
추가 컨텍스트	이 데이터 소스에 대한 추가 컨텍스트를 추가합니다.
사양 버전	이 객체를 나타내는 데 사용되는 STIX 사양의 버전입니다. 이 특성에 대한 값은 이 사양에 따라 정의된 STIX 객체에 대해 2.1이어야 합니다.
언어	이 속성은 이 객체의 텍스트 컨텐츠 언어를 식별합니다.
소스에서 생성된 시간	원본에서 개체가 만들어지는 시간을 지정합니다.
확장명	공격 패턴의 확장을 나타냅니다.
소스에서 수정된 시간	원본에서 개체가 수정되는 시간을 지정합니다.
처리 상태	이 객체의 처리 상태, 작업 과정을 나타냅니다.
작성됨	원본에서 객체가 만들어진 날짜 및 시간을 지정합니다.
업데이트됨	원본에서 객체가 업데이트된 날짜 및 시간을 지정합니다.
참조에 의해 생성됨	이 속성은 엔터티를 설명하는 ID 개체가 이 개체를 만들었음을 지정합니다.

6. 저장을 클릭합니다.
저장하면 새 옵저버블 기록이 생성되었음을 나타내는 프롬프트 메시지가 표시됩니다. 기록을 편집하고 새 관계를 생성하려면 "계속 "을 클릭하십시오.
7. 계속을 클릭합니다.

중요사항:
새 옵저버블 기록을 생성하면 시스템 업데이트 방지 확인란이 표시됩니다.

옵저버블, 표시기 또는 STIX 객체 기록이 생성된 후 시스템에서 업데이트를 방지하려면 이 확인란을 선택합니다.

태그&분류

필드	설명
태그	
태그 선택	데이터 소스와 연결된 태그를 선택합니다.
태그 추가	새 태그를 추가합니다.
분류	
분류 선택	이 데이터 소스와 연결된 분류를 선택합니다.
분류 값 추가	이 데이터 소스와 연결된 분류 값을 추가합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 수행할 작업
다음 관련 목록 중 하나를 클릭하면 데이터 소스와 연결된 객체에 대한 추가 정보를 볼 수 있습니다.

관련 기록

필드	설명
외부 참조	STIX가 아닌 정보를 참조하는 외부 참조를 나열합니다. 이 속성은 하나 이상의 외부 객체 식별자를 제공하는 데 사용됩니다.

주:

1. 이 객체와 연결된 관련 기록을 연결하거나 연결 해제할 수 있습니다. 자세한 내용은 위협 인텔리전스 관련 기록 연결 문서를 참조하십시오.
2. TI 라이브러리 내의 다양한 SDO에는 잠재적인 관계도 포함됩니다. 두 개체 간의 관계를 설정하려면 위협 인텔리전스 라이브러리의 **Potential** Relationships(잠재적 관계) 링크를 사용하여 개체 간의 관계를 확인합니다. 자세한 내용은 객체-객체 잠재성 관계 확인 문서를 참조하십시오.
3. 또한 객체 양식 뷰에서 관련 기록 섹션을 사용하면 양식 뷰에서 사용할 수 있는 잠재성 관계 섹션을 통해 두 객체 간의 관계를 확인할 수 있습니다. 에 대한 자세한 내용은 관련 기록에서 잠재성 관계 확인를 참조하십시오.
4. 케이스에 개체를 추가할 수 있습니다. 자세한 내용은 케이스에 추가 문서를 참조하십시오.

RSS 피드 정의

위협 인텔리전스 피드는 사이버 위험 또는 위협과 관련된 정보를 수집하는 실시간의 지속적인 데이터 스트림입니다. RSS 피드를 사용하면 블로그나 최신 사이버 보안 뉴스와 같이 즐겨 찾는 웹 사이트를 쉽게 최신 상태로 유지할 수 있습니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 작업 공간에서 위협 인텔 라이브러리 아이콘을 클릭합니다.
3. **RSS** 피드 개체로 이동합니다.

   주:
   이 섹션을 사용하여 수집된 피드를 찾아볼 수 있지만 새 기록을 만들 수는 없습니다.

4. 양식에서 다음 필드가 자동으로 채워집니다.

RSS 피드 세부 정보 뷰

필드	설명
직위	RSS 피드의 제목입니다.
설명	RSS 피드의 목적과 주요 특성을 포함하여 RSS 피드에 대한 자세한 내용과 컨텍스트를 제공하는 설명입니다.
링크	RSS 피드에 추가된 링크를 나타냅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
소스	이 개체 레코드가 만들어지는 RSS 피드 소스를 지정합니다.
게시된 날짜	RSS 피드가 게시되는 시기를 나타냅니다.
작성자	RSS 피드의 작성자를 나타냅니다.

5. 저장을 클릭합니다.

인사이트

필드	설명
메모	이 피드에 대한 메모를 추가합니다.

추가 정보

필드	설명
미디어 URL	미디어 URL을 나타냅니다.
피드백 설명	피드백에 대한 추가 피드백 코멘트입니다.

관계 객체

관계 객체를 사용하여 두 옵저버블 또는 옵저버블과 SDO를 함께 연결하여 서로 어떻게 관련되어 있는지 설명할 수 있습니다.

STIX 관계 객체(SRO)는 다양한 STIX 객체 간의 관계 유형을 나타냅니다. 다음과 같은 관계 객체를 사용할 수 있습니다.

- 옵저버블-옵저버블 관계: 이 객체는 옵저버블 간의 관계를 정의합니다.
- 객체-객체 관계: 이 객체는 표시기 객체를 제외한 SDO 간의 관계를 정의합니다. 개체-개체 정의 관계의 예는 공격 패턴이 맬웨어를 전달하는 것입니다.
- 객체-옵저버블 관계: 이 객체는 SDO와 옵저버블 객체(SCO) 간의 관계를 정의합니다. 객체-옵저버블 정의 관계의 예는 인프라가 잠재적인 공격에 대한 정보를 제공하는 사이버 옵저버블 객체로 구성된다는 것입니다.
- 객체-표시기 관계: 이 객체는 SDO와 표시기 객체 간의 관계를 정의합니다.
- 표시기-표시기 관계: 이 개체는 표시기 개체 간의 관계를 정의합니다.
- 표시기-옵저버블 관계: 이 개체는 표시기 개체와 다른 SDO 간의 관계를 정의합니다. 객체-표시기 정의 관계의 예로는 표시기가 캠페인의 증거를 감지하는 경우를 들 수 있습니다.

객체 관계

관계 객체	예시 소스	예제 대상	예시 설명
옵저버블-옵저버블 관계	IP 주소, 도메인 이름		이 관계는 옵저버블 간에 대해 설명합니다.
객체-객체 관계	공격 패턴	맬웨어	이 관계는 이 공격 패턴이 이 맬웨어 인스턴스(또는 제품군)를

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

객체 관계

관계 객체	예시 소스	예제 대상	예시 설명
			전달하는 데 사용됨을 설명합니다.
객체-옵저버블 관계			이 관계는 객체와 옵저버블 간에 대해 설명합니다.
객체-표시기 관계	표시기	공격 패턴, 캠페인, 인프라, 침입 세트, 멀웨어, 위협 액터, 도구	이 관계는 표시기가 관련 공격 패턴, 캠페인, 인프라, 침입 세트, 멀웨어, 위협 액터 또는 도구의 증거를 탐지할 수 있음을 설명합니다. 증거가 직접적이지 않을 수 있습니다. 예를 들어, 표시기는 특정 캠페인에서 일반적으로 사용되는 맬웨어와 같은 캠페인의 2차 증거를 감지할 수 있습니다.
표시기 - 표시기 관계	인프라	관찰 데이터	이 관계는 표시기가 관찰된 데이터 객체의 정보를 기반으로 생성됨을 설명합니다. 객체-옵저버블 정의 관계의 예는 인프라가 잠재적인 공격에 대한 정보를 제공하는 사이버 옵저버블 객체로 구성된다는 것입니다.
표시기-옵저버블			이 관계는 표시기와 옵저버블을 설명합니다.

옵저버블-옵저버블 관계 정의

옵저버블 간의 관계를 정의합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 작업 공간에서 위협 인텔 라이브러리 아이콘을 클릭합니다.
3. 이동 관계 〉 옵저버블-옵저버블.
4. 새로 만들기를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. 양식에 있는 필드를 적절하게 작성합니다.

6. 제출을 클릭합니다.

객체-객체 관계 정의

표시기 객체를 제외한 SDO 간의 관계를 정의합니다.

시작하기 전에

필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 작업 공간에서 위협 인텔 라이브러리 아이콘을 클릭합니다.
3. 이동 관계 〉 객체-객체.
4. 새로 만들기를 클릭합니다.
5. 양식에 있는 필드를 적절하게 작성합니다.

6. 제출을 클릭합니다.

객체-옵저버블 관계 정의

SDO와 옵저버블 객체(SCO) 간의 관계를 정의합니다.

시작하기 전에

필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 작업 공간에서 위협 인텔 라이브러리 아이콘을 클릭합니다.
3. 이동 관계 〉 객체-옵저버블.
4. 새로 만들기를 클릭합니다.
5. 양식에 있는 필드를 적절하게 작성합니다.

6. 제출을 클릭합니다.

객체-표시기 관계 정의

표시기 객체와 다른 SDO 간의 관계를 정의합니다.

시작하기 전에

필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 작업 공간에서 위협 인텔 라이브러리 아이콘을 클릭합니다.
3. 이동 관계 〉 객체-표시기.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 새로 만들기를 클릭합니다.
5. 양식에 있는 필드를 적절하게 작성합니다.
6. 제출을 클릭합니다.

표시기-표시기 관계 정의

표시기 객체와 다른 객체 간의 관계 정의 관계 객체를 사용하여 두 옵저버블 또는 옵저버블과 SDO를 함께 연결하여 서로 어떤 관계가 있는지 설명합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

프로시저
1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 작업 공간에서 위협 인텔 라이브러리 아이콘을 클릭합니다.
3. 이동 관계 〉 표시기-표시기.
4. 새로 만들기를 클릭합니다.
5. 양식에 있는 필드를 적절하게 작성합니다.
6. 제출을 클릭합니다.

표시기-옵저버블 관계 정의

표시기 객체와 다른 SDO 간의 관계를 정의합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

프로시저
1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 작업 공간에서 위협 인텔 라이브러리 아이콘을 클릭합니다.
3. 이동 관계 〉 표시기-옵저버블.
4. 새로 만들기를 클릭합니다.
5. 양식에 있는 필드를 적절하게 작성합니다.
6. 제출을 클릭합니다.

잠재성 관계

애플리케이션은 자동화된 상관 관계를 사용하여 두 개의 SDO, 두 개의 옵저버블 또는 옵저버블과 SDO 간에 잠재적으로 가능한 관계를 설정합니다.

1. 하나 이상의 잠재적으로 관련된 기록을 선택하고 UI에 이 작업을 적용하면 기록이 확인된 관계로 추가적으로 변경되고 관련 기록 섹션에 표시됩니다.
2. 분석가가 수집하거나 수동으로 생성한 확인된 상관 관계는 자동 상관 관계에 의해 생성된 잠재적 관계를 재정의합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵저버블-옵저버블 잠재성 관계 확인

이 섹션을 사용하여 옵저버블 간의 관계를 확인합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 작업 공간에서 위협 인텔 라이브러리 아이콘을 클릭합니다.
3. 이동 잠재성 관계 〉 옵저버블-옵저버블.
4. 옵저버블 기록을 선택합니다.
5. 관계 확인**(Confirm Relation)**을 클릭합니다.
   상관관계 규칙을 기반으로 식별되는 잠재성 관계 기록이 이상적으로 생성됩니다. 관계를 확인하면 옵저버블 기록이 관계 섹션으로 이동하며, 이는 옵저버블과 옵저버블 간의 관계가 확인되었음을 의미합니다. 기록은 상관관계 규칙이 일치하는 경우에만 확인된 관계를 보여줍니다. 예를 들어 URL 유형의 옵저버블 2개가 동일한 도메인 이름을 가질 때 잠재적 관계를 만들 수 있습니다.

   또는 옵저버블 목록에서 옵저버블을 연결하여 새 옵저버블 기록을 생성하고 각 옵저버블의 관련 기록 탭에서 관계를 확인할 수도 있습니다.

   a. 옵저버블 기록을 엽니다.

   b. 관련 기록 탭으로 이동합니다.

   c. 링크 버튼을 클릭합니다.

   d. 옵저버블을 하나 이상 선택합니다.

   e. 링크를 클릭합니다.
      이렇게 하면 선택한 옵저버블 기록과 새로 연결된 옵저버블 간에 새 관계가 생성됩니다.
6. 삭제를 클릭하여 관계를 삭제합니다.

객체-객체 잠재성 관계 확인

개체 간의 잠재적 관계를 정의합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 작업 공간에서 위협 인텔 라이브러리 아이콘을 클릭합니다.
3. 이동 잠재성 관계 〉 객체-객체.
4. 옵저버블 기록을 선택합니다.
5. 관계 확인**(Confirm Relation)**을 클릭합니다.
   상관관계 규칙을 기반으로 식별되는 잠재성 관계 기록이 이상적으로 생성됩니다. 이 섹션에서 관계를 확인하면 옵저버블 기록이 관계 섹션으로 이동하며, 이는 옵저버블과 옵저버블 간의 관계가 확인되었음을 의미합니다. 기록은 상관관계 규칙이 일치하는 경우에만 확인된 관계를 보여줍니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예를 들어 URL 유형의 옵저버블 2개가 동일한 도메인 이름을 가질 때 잠재적 관계를 만들 수 있습니다.

또는 옵저버블 목록에서 옵저버블을 연결하여 새 옵저버블 기록을 생성하고 각 옵저버블의 관련 기록 탭에서 관계를 확인할 수도 있습니다.

a. 옵저버블 기록을 엽니다.

b. 관련 기록 탭으로 이동합니다.

c. 링크 버튼을 클릭합니다.

d. 옵저버블을 하나 이상 선택합니다.

e. 링크를 클릭합니다.
이렇게 하면 선택한 옵저버블 기록과 새로 연결된 옵저버블 간에 새 관계가 생성됩니다.

6. 삭제를 클릭하여 관계를 삭제합니다.

표시기-표시기 잠재성 관계 확인

개체 간의 잠재적 관계를 정의합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.

2. 작업 공간에서 위협 인텔 라이브러리 아이콘을 클릭합니다.

3. 이동 잠재성 관계 〉 표시기-표시기.

4. 옵저버블 기록을 선택합니다.

5. 관계 확인**(Confirm Relation)**을 클릭합니다.
잠재적 관계 기록은 자동화된 상관관계 규칙을 기반으로 확인하는 것이 이상적입니다. 관계를 확인하면 옵저버블 기록이 관계 섹션으로 이동하며, 이는 옵저버블과 옵저버블 간의 관계가 확인되었음을 의미합니다.

기록은 상관관계 규칙이 일치하는 경우에만 확인된 관계를 보여줍니다. 예를 들어 URL 유형의 옵저버블 2개가 동일한 도메인 이름을 가질 때 잠재적 관계가 확인됩니다.

또는 옵저버블 목록에서 옵저버블을 연결하여 새 옵저버블 기록을 생성하고 각 옵저버블의 관련 기록 탭에서 관계를 확인할 수도 있습니다.

a. 옵저버블 기록을 엽니다.

b. 관련 기록 탭으로 이동합니다.

c. 링크 버튼을 클릭합니다.

d. 옵저버블을 하나 이상 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

e. 링크를 클릭합니다.
이렇게 하면 선택한 옵저버블 기록과 새로 연결된 옵저버블 간에 새 관계가 생성됩니다.

6. 삭제를 클릭하여 관계를 삭제합니다.

인텔리전스 데이터 익스포트

익스포트 기능을 사용하여 인텔리전스 데이터를 다양한 형식으로 수동으로 익스포트합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

이 태스크 정보
현재 익스포트 기능은 옵저버블, 표시기 및 케이스 관리로 제한됩니다. 다음 절차에서는 옵저버블 데이터를 익스포트하고 동일한 절차에 따라 표시기 데이터를 익스포트하는 방법을 설명합니다.

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터 〉 위협 인텔 라이브러리 〉 옵저버블 〉 모든 옵저버블.
2. 옵저버블을 선택합니다.
3. 내보내기 버튼을 클릭합니다.

   주:
   익스포트 버튼은 익스포트를 위해 옵저버블을 선택한 경우에만 활성화됩니다. 옵저버블을 선택하지 않으면 버튼이 비활성화된 상태로 유지됩니다.

4. 익스포트할 파일 형식을 선택합니다.
   현재 지원되는 내보내기 형식은 Excel, CSV 및 STIX 2.1 JSON입니다. 익스포트 유형이 Excel인 경우 선택한 형식 유형에 관계없이 한 번에 익스포트할 수 있는 레코드 수가 10,000개로 제한된다고 가정합니다.

   선택 레코드가 10,000개를 초과하면 선택한 형식 유형에 대한 최대 한도를 초과했음을 나타내는 오류 메시지가 표시되고 처음 10,000개의 레코드만 익스포트됩니다.

   익스포트 형식이 CSV이고 기록 한도가 초과되면 익스포트 상태를 볼 수 있는 링크와 함께 익스포트가 진행 중 상태임을 나타내는 경고 메시지가 표시됩니다. 링크를 클릭하여 상태를 보고, 기록을 새로 고치고, 새로 고친 후 처리됨 상태로 이동하면 첨부 파일을 다운로드할 수 있습니다.

5. 익스포트를 클릭합니다.

   주:
   임포트/익스포트 모듈에서 익스포트 데이터를 볼 수도 있습니다.

   익스포트가 성공하고 다운로드가 완료되었음을 나타내는 확인 메시지가 표시됩니다.

관련 기록에서 잠재성 관계 확인

두 SDO 간의 관계를 확인합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

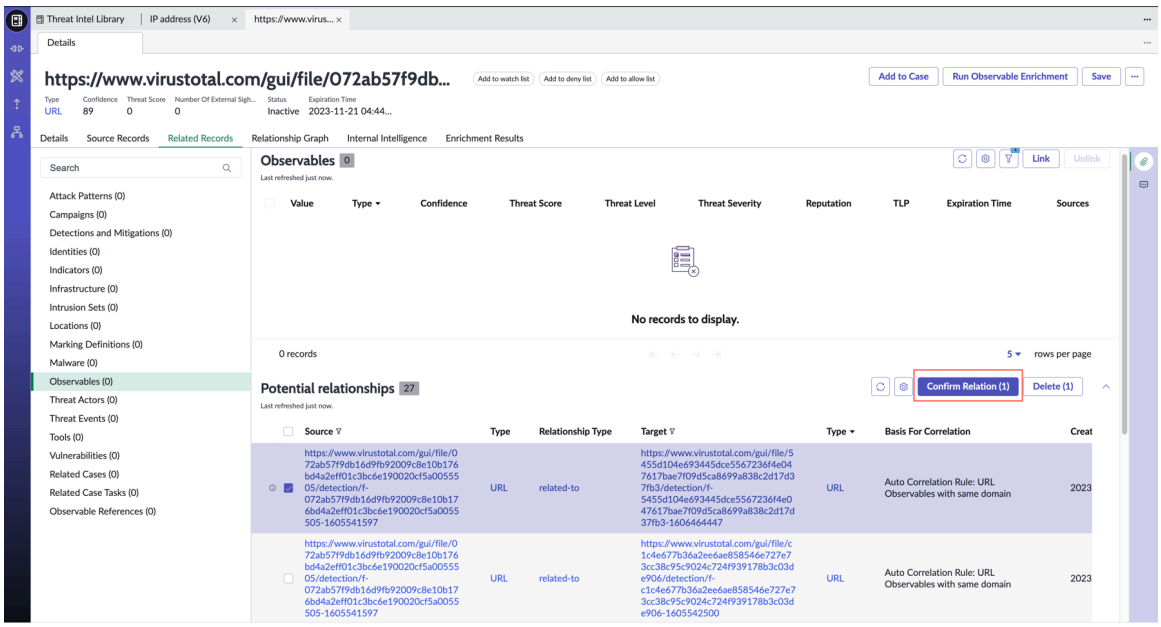
프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 작업 공간에서 위협 인텔 라이브러리 아이콘을 클릭합니다.
3. 관련 기록 섹션으로 이동합니다.
4. 잠재적 관계를 확장합니다.
5. 옵저버블, 표시기 또는 두 SDO 간의 관계를 확인하려는 기타 객체와 같은 기록을 엽니다.
6. 예를 들어 여기서는 왼쪽 탐색에서 옵저버블을 선택합니다.
7. 목록에서 옵저버블 기록을 선택합니다.

   주:
   목록 섹션에는 연결된 옵저버블의 연결된 모든 옵저버블 기록이 표시됩니다.

8. 관계 확인 버튼을 클릭하여 객체 간의 관계를 확인합니다.

   주:
   자세한 내용은관계 객체 및 잠재성 관계.



9. 삭제를 클릭하여 연결된 옵저버블을 삭제합니다.
   SDO들 사이에 잠재적인 관계와 관계가 어떻게 설정되는지에 대한 정보는 를 참조 잠재성 관계 하라 관계 객체.

자동화된 상관 관계

자동화된 상관관계는 옵저버블, 표시기 및 객체 간의 관계를 식별하는 데 도움이 됩니다.

상관 관계 프로세스를 통해 애플리케이션은 미리 정의된 규칙에 따라 위협 인텔리전스 기록 간의 상관 관계를 자동으로 설정합니다. 적용된 규칙의 유형에 따라 관계는 확인된 관계 또는 잠재적 관계가 될 수 있습니다. 객체 간의 관계가 확인되면 관련 기록 섹션 아래에 있는 해당 객체의 상세 정보 뷰에 해당 객체가 자동으로 표시됩니다.

다음은 관계와 잠재적 관계에 대한 설명입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 관계: 관계 객체를 사용하여 두 옵저버블 또는 옵저버블과 SDO를 함께 연결하여 서로 어떻게 관련되어 있는지 설명합니다.
- 잠재적 관계: 잠재적 관계를 사용하여 자동화된 상관 관계를 사용하여 두 개의 SDO, 두 개의 옵저버블 또는 옵저버블과 SDO 간에 잠재적으로 가능한 관계를 설정합니다.

다음은 기본 시스템 내에 프로비저닝된 미리 정의된 상관관계 규칙입니다.

상관관계 규칙

규칙 이름	규칙 설명	규칙 정의	규칙 작업
파일 해시가 동일한 옵저버블	이 규칙은 옵저버블의 해시 값(동일한 유형)을 비교하고 동일한 해시를 공유하는지 식별합니다.	이 규칙은 표시기의 해시 값(동일한 유형)을 비교하고 동일한 해시를 공유하는지 식별합니다.	관계 생성
동일한 도메인을 사용하는 URL 옵저버블	이 규칙은 URL 구조의 공통성을 검사하여 동일한 기본 도메인을 공유하는지 확인합니다.	이 규칙은 URL 구조의 공통성을 검사합니다. - 동일한 기본 도메인을 공유하고 유사한 하위 디렉터리 구조를 가지고 있는지 식별합니다.	잠재적 관계를 생성합니다.
네트워크 객체에서 소스로 찾은 옵저버블	이 규칙은 네트워크 소스 속성 값을 시스템의 IPV4, IPV6 또는 도메인 이름 옵저버블과 일치시키고 트래픽 소스로 연결합니다.	이 규칙은 소스 속성 값을 시스템의 IPV4, IPV6 또는 도메인 이름 옵저버블과 일치시키고 트래픽 소스로 연결합니다.	관계 생성
네트워크 객체에서 대상으로 찾은 옵저버블	이 규칙은 네트워크 대상 속성 값을 시스템의 IPV4, IPV6 또는 도메인 이름 옵저버블과 일치시키고 트래픽을 대상으로 링크합니다.	규칙은 소스 속성 값을 시스템의 IPV4, IPV6 또는 도메인 이름 옵저버블과 일치시키고 트래픽 대상으로 링크합니다.	관계 생성
커뮤니케이션을 기반으로 옵저버블 연결	이 규칙은 네트워크 객체를 기반으로 동일한 대상(IPV4, IPV6 또는 도메인 이름)과 통신한 모든 옵저버블(IPV4, IPV6 및 도메인 이름)을 식별하고 이러한 옵저버블 간의 관계를 설정합니다. 또한 대상과 통신하는 소스와 동일한 네트워크 객체와 관련된 경우 관련 옵저버블(IPV4, IPV6	네트워크 개체의 베이스에서 규칙은 동일한 대상(IPV4, IPV6, mac-addr 또는 domain-name)과 통신한 모든 표시기를 식별하고 동일한 C2 인프라에 연결된 이러한 표시기 간의 관계를 설정합니다.	관계 생성

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

상관관계 규칙

규칙 이름	규칙 설명	규칙 정의	규칙 작업
	및 도메인 이름)도 포함됩니다.		
하위 도메인에 대한 관련 루트 도메인 옵저버블	이 규칙은 루트 도메인을 하위 도메인과 연결하고 그 반대로 옵저버블의 도메인 유형을 연결합니다.	이 규칙은 루트 도메인과 하위 도메인을 함께 연결합니다.	관계 생성
DNS 확인에 기반한 IP에 대한 관련 도메인	규칙은 도메인 옵저버블의 domain-ipv4 또는 domain-ipv6 속성을 사용하여 도메인과 IP 간의 관계를 설정합니다.	domain-ipv4 또는 domain-ipv6 속성을 사용합니다. 이 규칙은 동일한 IP 주소로 확인되는 모든 도메인 또는 하위 도메인을 식별하고 표시기 간의 관계를 설정하여 동일한 C2 인프라에 대한 연결을 나타냅니다.	관계 생성
SSL 인증서와 도메인 일치	이 규칙은 도메인 옵저버블과 연결된 SSL 인증서 정보를 분석하고 둘 사이의 관계를 설정합니다.	이 규칙은 표시기와 연결된 SSL 인증서 정보를 분석하고 두 인증서가 동일한 인증 기관에서 발급되고 동일한 만료 날짜를 공유한다는 것을 식별하고, 표시기 간의 관계를 설정하여 동일한 C2 인프라 또는 위협 캠페인에 대한 연결을 나타냅니다.	관계 생성
공통 옵저버블을 기반으로 엔터티 연결	이 규칙은 동일한 옵저버블이 서로 다른 두 엔터티와 관련되어 있는지 비교하고 서로 연관시킵니다.	이 규칙은 동일한 옵저버블이 서로 다른 두 엔터티와 관련되어 있는지 비교하고 서로 관련된 것으로 식별합니다.	잠재적 관계를 생성합니다.
공통 옵저버블을 기반으로 표시기 연결	이 규칙은 동일한 옵저버블이 두 개의 서로 다른 표시기와 관련되어 있는지 비교하고 서로 연관시킵니다.	이 규칙은 동일한 옵저버블이 두 개의 서로 다른 표시기와 관련되어 있는지 비교하고 서로 관련된 것으로 식별합니다.	잠재적 관계를 생성합니다.
공통 옵저버블을 기반으로 표시기와 객체 관계 지정	이 규칙은 동일한 옵저버블이 표시기 및 객체와 관련되어 있는지 비교하고 서로 연관시킵니다.	이 규칙은 동일한 옵저버블이 두 개의 서로 다른 표시기 및 객체와 관련되어 있는지 비교하고 서로	잠재적 관계를 생성합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

상관관계 규칙

규칙 이름	규칙 설명	규칙 정의	규칙 작업
		관련되어 있는 것으로 식별합니다.	

데이터 익스포트 작업

위협 인텔리전스 보안 센터 권장 형식으로 옵저버블, 표시기 및 케이스의 수동 익스포트를 지원합니다.

이 기능을 사용하면 추가 분석을 위해 데이터를 쉽게 추출할 수 있습니다. 핵심 기능은 다음과 같습니다.

- 옵저버블, 표시기 및 케이스를 개별적으로 또는 대량으로 익스포트합니다.
- 원활한 통합을 위해 CSV, STIX 2.1과 같은 권장 형식으로 출력합니다.

주:
데이터 익스포트 기능은 현재 옵저버블, 표시기 및 케이스 관리에 대해서만 지원됩니다. 케이스 관리 내에서 익스포트는 케이스 아티팩트 아래의 옵저버블 및 표시기 목록으로 제한됩니다.

모든 익스포트 보기

이 섹션을 사용하여 수동으로 익스포트한 모든 기록을 봅니다.

시작하기 전에
필요한 역할: sn_sec_tisc.export

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터 〉 임포트/익스포트.
2. 선택 익스포트 〉 모든 익스포트
   이 페이지에는 익스포트 기록이 표시됩니다.
3. 익스포트 프로세스의 상태를 보려면 기록을 엽니다.

내 익스포트 보기

액세스 권한이 있는 익스포트를 보고 다운로드합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.export

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터 〉 임포트/익스포트.
2. 선택 익스포트 〉 내 익스포트
   이 페이지에는 익스포트 기록이 표시됩니다.
3. 익스포트 프로세스의 상태를 보려면 기록을 엽니다.

인텔리전스 시스템 속성 익스포트

이 섹션에서는 데이터를 익스포트하는 동안의 레코드 제한 사항과 해당 속성에 대해 설명합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
TISC 는 데이터 익스포트에 대해 다음과 같은 제한을 제공합니다. 다음 속성을 설정하려면 다음으로 이동합니다. 시스템 속성 〉 임포트 익스포트.

필요한 역할: sn_sec_tisc.export

형식	속성	설명
STIX 2.1 JSON	sn_sec_tisc.stix_export_limit	STIX 2.1 파일로 익스포트할 수 있는 최대 행 수입니다. 기본 e는 10000입니다.
STIX 2.1 JSON	sn_sec_tisc.stix_export_payload_streaming_attachment_min_objects_size	STIX 익스포트 페이로드의 "객체" 배열에 있는 객체 수가 이 속성에 지정된 수보다 크면 첨부 파일을 작성하는 데 JSONStreamingAPI가 사용됩니다. 기본 익스포트 제한은 4000입니다.
STIX 2.1 JSON	sn_sec_tisc.stix_json_from_json_streaming_api_action_timeout	JSON 스트리밍 API를 사용하여 STIX JSON 첨부 파일을 생성하기 위한 플로우 디자이너 작업을 트리거할 때 사용되는 시간 제한(초)입니다. 기본 익스포트 제한은 900입니다.

주:
다른 형식 유형의 내보내기 제한에 대한 더 나은 이해는 내보내기 제한을 참조하세요.

MITRE-ATT&CK™ 저장소

리포지토리는 MITRE-ATT&CK MITRE 소스의 데이터가 수집되는 인텔리전스 라이브러리에서 사용할 수 있습니다.

리포지토리로 오는 MITRE 데이터는 위협 인텔 라이브러리 데이터와 별도의 MITRE 리포지토리에 저장되며, 여기서 MITRE 데이터는 집계 또는 중복 제거 플로우를 위해 롤업되지 않고 독립적입니다.

애플리케이션 내에서 사용할 수 있는 데이터 소스는 다음과 같습니다.

1. MITRE - 엔터프라이즈 ATT&CK
2. MITRE - 모바일 ATT&CK
3. MITRE - ICS ATT&CK

이러한 소스의 데이터는 기본 시스템의 TI 라이브러리 아래에 있는 별도의 MITRE 리포지토리에 저장됩니다. 새 MITRE 소스를 생성하려면 사용자 지정 소스를 구성합니다. 자세한 내용은 사용자 지정 피드 보기 양식 뷰에서 고급 확인란을 클릭하고 보고서 프로세서를**MITRECollectionDataProcessor**로 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

매트릭스 관리

MITRE TAXII 컬렉션에서 임포트한 매트릭스를 관리합니다. 매트릭스는 전술과 기술의 모음입니다. 매트릭스를 보고 MITRE-ATT&CK 리포지토리에서 컬렉션을 사용할 수 있는지 검토할 수 있습니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

프로시저

1. 기본 시스템에서 사용할 수 있는 MITRE ATT&CK 관련 피드 데이터 소스를 활성화한 후 지금 실행을 클릭하여 통합을 실행하고 MITRE 관련 정보를 가져옵니다.
   통합 활성화에 대한 자세한 내용은 다음을 참조하십시오.
2. MITRE ATT&CK 리포지토리 데이터를 보려면 다음으로 이동하십시오. 작업 공간 〉 위협 인텔리전스 보안 센터 〉 위협 인텔 라이브러리 〉 **MITRE ATT&CK**.
   MITRE ATT&CK 관련 기록이 표시됩니다. 기본적으로 모든 기록은 사용 가능한 상태입니다.

   주:
   조직과 관련된 매트릭스만 활성화할 수 있습니다.

3. 매트릭스 기록을 선택하고 특정 기록을 사용 중지하려면 사용 안 함을 클릭합니다.
4. 또는 새로 만들기를 클릭하여 새 매트릭스 기록을 생성하고 수동으로 MITRE ATT&CK 매트릭스를 생성할 수 있습니다.
5. 필드를 적절하게 채웁니다.

새 **MITRE** 완화 생성 **-** 상세 정보

필드	설명
이름	매트릭스의 이름을 입력합니다.
소스	이 기록이 생성되는 위협 소스를 지정합니다.
활성	매트릭스 기록을 활성화하려면 이 확인란을 선택합니다.
소스에서 생성된 시간	원본에서 개체가 만들어지는 시간을 지정합니다.
소스에서 수정된 시간	원본에서 개체가 수정되는 시간을 지정합니다.
설명	침입 세트의 목적과 주요 특성을 포함하여 침입 집합에 대한 자세한 내용과 컨텍스트를 제공하는 설명입니다.
인사이트	
메모	완화와 관련된 추가 정보입니다.
추가 정보	
추가 컨텍스트	이 객체 유형에 대한 추가 컨텍스트를 추가합니다.
설명	추가적으로 작성할 수 있는 주석을 추가합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

기술 관리

MITRE TAXII 컬렉션에서 임포트한 기술을 관리합니다. 이 기술에는 공격자가 주어진 전술을 사용하기 위해 개발한 다양한 방법이 포함되어 있습니다. 조직과 관련이 없는 기술을 검토하고 비활성화할 수 있습니다. STIX에서는 기술을 공격 패턴이라고 합니다.

시작하기 전에

필요한 역할: sn_sec_tisc.analyst

기술은 악의적 사용자가 작업을 수행하여 전술적 목표를 달성하는 방법을 나타냅니다.

프로시저

1. 기본 시스템에서 사용할 수 있는 MITRE ATT&CK 관련 피드 데이터 소스를 활성화한 후 지금 실행을 클릭하여 통합을 실행하고 MITRE 관련 정보를 가져옵니다.
   통합 활성화에 대한 자세한 내용은 다음을 참조하십시오.
2. MITRE ATT&CK 리포지토리 데이터를 보려면 다음으로 이동하십시오. 작업 공간 〉 위협 인텔리전스 보안 센터 〉 위협 인텔 라이브러리 〉 **MITRE ATT&CK** 〉 기술.
   MITRE ATT&CK 기술 기록이 표시됩니다. 기본적으로 모든 기록은 사용 가능한 상태입니다.
3. 기술 기록을 선택하고 특정 기록을 비활성화하려면 사용 안 함을 클릭합니다.
4. 또는 새로 만들기를 클릭하여 새 기술 기록을 생성하고 MITRE ATT&CK 기술을 수동으로 생성할 수 있습니다.
5. 필드를 적절하게 채웁니다.

새 **MITRE** 완화 생성 **-** 상세 정보

필드	설명
ID	기술의 고유 ID입니다.
이름	기술의 이름을 입력합니다.
소스	이 기록이 생성되는 위협 소스를 지정합니다.
플랫폼	필요한 플랫폼을 추가합니다.
권한 필요	필요한 권한을 추가합니다.
소스에서 생성된 시간	원본에서 개체가 만들어지는 시간을 지정합니다.
소스에서 수정된 시간	원본에서 개체가 수정되는 시간을 지정합니다.
우선순위	MITRE 기술에 할당된 우선순위 수준(예: 낮음, 보통, 높음 또는 중요)을 나타냅니다. **주:** 기술에 우선순위를 할당하여 조직에 관련성을 추가할 수 있습니다.
설명	침입 세트의 목적과 주요 특성을 포함하여 침입 집합에 대한 자세한 내용과 컨텍스트를 제공하는 설명입니다.
탐지	탐지 기술은 컴퓨터 네트워크에 대한 악의적 액세스 또는 무단 활동을 식별하는 데 사용됩니다.
인사이트	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
메모	완화와 관련된 추가 정보입니다.
추가 정보	
추가 컨텍스트	이 객체 유형에 대한 추가 컨텍스트를 추가합니다.
설명	추가적으로 작성할 수 있는 주석을 추가합니다.
TISC 태그	
TISC 태그 선택	이 소스에서 시스템으로 수집된 기록에 주석을 달거나 할당할 태그를 선택합니다. 주: 기술에 태그를 할당하여 조직에 관련성을 추가할 수 있습니다.

완화 관리

MITRE TAXII 컬렉션에서 임포트한 완화를 관리합니다. 완화를 사용하면 악의적 사용자가 조직에 대해 기술 또는 하위 기술을 성공적으로 실행하지 못하도록 방지할 수 있습니다. STIX에서는 완화를 동작 방침이라고 합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

프로시저

1. 기본 시스템에서 사용할 수 있는 MITRE ATT&CK 관련 피드 데이터 소스를 활성화한 후 지금 실행을 클릭하여 통합을 실행하고 MITRE 관련 정보를 가져옵니다.
   통합 활성화에 대한 자세한 내용은 다음을 참조하십시오.
2. MITRE ATT&CK 리포지토리 데이터를 보려면 다음으로 이동하십시오. 작업 공간 〉 위협 인텔리전스 보안 센터 〉 위협 인텔 라이브러리 〉 **MITRE ATT&CK** 〉 완화.
   연관된 모든 정보를 보려면 완화를 클릭하십시오.
3. 새로 만들기를 클릭하여 MITRE ATT&CK 완화를 수동으로 생성합니다.
4. 필드를 적절하게 채웁니다.

새 **MITRE** 도구 생성 **-** 상세 정보

필드	설명
ID	공격을 방지하기 위한 작업 과정의 고유 ID입니다.
해지함	해지된 개체가 개체 작성자에 의해 더 이상 유효한 것으로 간주되지 않음을 나타냅니다.
이름	객체를 식별하는 설명이 포함된 이름을 입력합니다.
소스	이 개체 기록이 생성되는 위협 소스를 지정합니다.
별칭	이 객체를 식별하는 다른 이름의 목록입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
소스에서 생성된 시간	원본에서 개체가 만들어지는 시간을 지정합니다.
소스에서 수정된 시간	원본에서 개체가 수정되는 시간을 지정합니다.
설명	목적과 주요 특성을 포함하여 객체에 대한 자세한 내용과 컨텍스트를 제공하는 설명입니다.
기고자	기고자를 지정합니다.
인사이트	
메모	완화와 관련된 추가 정보입니다.
추가 정보	
추가 컨텍스트	이 객체에 대한 추가 컨텍스트를 추가합니다.
설명	이 객체에 대한 주석을 추가합니다.

5. 저장을 클릭합니다.

그룹 관리

MITRE TAXII 컬렉션에서 임포트한 그룹을 관리합니다. 그룹은 보안 커뮤니티에서 공통 이름으로 추적되는 관련 침입 활동의 집합입니다. 분석가는 위협 그룹, 활동 그룹, 위협 행위자, 침입 세트 및 캠페인과 같은 다양한 용어를 사용하여 활동 클러스터를 추적합니다. STIX에서는 그룹을 침입 세트라고 합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

프로시저

1. MITRE ATT&CK 리포지토리 데이터를 보려면 다음으로 이동하십시오. 작업 공간 〉 위협 인텔리전스 보안 센터 〉 위협 인텔 라이브러리 〉 **MITRE ATT&CK** 〉 그룹.
나열된 그룹을 볼 수 있습니다.

2. 새로 만들기를 클릭하여 MITRE ATT&CK 그룹을 수동으로 만듭니다.

3. 필드를 적절하게 채웁니다.

새 **MITRE** 그룹 생성 **-** 상세 정보

필드	설명
ID	공격을 방지하기 위한 작업 과정의 고유 ID입니다.
해지함	해지된 개체가 개체 작성자에 의해 더 이상 유효한 것으로 간주되지 않음을 나타냅니다.
이름	객체를 식별하는 설명이 포함된 이름을 입력합니다.
소스	이 개체 기록이 생성되는 위협 소스를 지정합니다.
별칭	이 객체를 식별하는 다른 이름의 목록입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
소스에서 생성된 시간	원본에서 개체가 만들어지는 시간을 지정합니다.
소스에서 수정된 시간	원본에서 개체가 수정되는 시간을 지정합니다.
설명	목적과 주요 특성을 포함하여 객체에 대한 자세한 내용과 컨텍스트를 제공하는 설명입니다.
인사이트	
메모	완화와 관련된 추가 정보입니다.
추가 정보	
추가 컨텍스트	이 객체에 대한 추가 컨텍스트를 추가합니다.
설명	이 객체에 대한 주석을 추가합니다.

4. 저장을 클릭합니다.
5. 이러한 객체의 관계를 보려면 관계를 클릭합니다.

맬웨어 관리

MITRE TAXII 컬렉션에서 임포트한 맬웨어 정보를 관리합니다. 악성 코드를 나타내는 TTP의 한 유형입니다.

시작하기 전에
시스템에 은밀하게 삽입되는 프로그램을 말합니다. 멀웨어의 목적은 피해자의 데이터, 애플리케이션 또는 운영 체제(OS)의 기밀성, 무결성 또는 가용성을 손상시키는 것입니다.

필요한 역할: sn_sec_tisc.analyst

프로시저

1. MITRE ATT&CK 리포지토리 데이터를 보려면 다음으로 이동하십시오. 작업 공간 〉 위협 인텔리전스 보안 센터 〉 위협 인텔 라이브러리 〉 **MITRE ATT&CK** 〉 그룹.
   나열된 맬웨어를 볼 수 있습니다.
2. 모든 관련 정보를 보려면 맬웨어를 클릭하십시오.
3. 새로 만들기를 클릭하여 MITRE ATT&CK 맬웨어를 수동으로 생성합니다.
4. 필드를 적절하게 채웁니다.

새 **MITRE** 맬웨어 생성 **-** 상세 정보

필드	설명
ID	공격을 방지하기 위한 작업 과정의 고유 ID입니다.
해지함	해지된 개체가 개체 작성자에 의해 더 이상 유효한 것으로 간주되지 않음을 나타냅니다.
이름	객체를 식별하는 설명이 포함된 이름을 입력합니다.
소스	이 개체 기록이 생성되는 위협 소스를 지정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
별칭	이 객체를 식별하는 다른 이름의 목록입니다.
소스에서 생성된 시간	원본에서 개체가 만들어지는 시간을 지정합니다.
소스에서 수정된 시간	원본에서 개체가 수정되는 시간을 지정합니다.
설명	목적과 주요 특성을 포함하여 객체에 대한 자세한 내용과 컨텍스트를 제공하는 설명입니다.
기고자	기고자를 지정합니다.
인사이트	
메모	완화와 관련된 추가 정보입니다.
추가 정보	
추가 컨텍스트	이 객체에 대한 추가 컨텍스트를 추가합니다.
설명	이 객체에 대한 주석을 추가합니다.

5. 저장을 클릭합니다.
6. 이러한 객체의 관계를 보려면 관계를 클릭합니다.

도구 관리

MITRE TAXII 컬렉션에서 임포트한 도구 정보를 관리합니다. 도구는 위협 행위자가 공격을 수행하는 데 사용하는 합법적인 소프트웨어입니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

이 태스크 정보
도구를 사용하면 위협 행위자가 캠페인을 실행하기 위해 도구를 사용하는 방법과 시기를 알 수 있습니다. 맬웨어와 달리 이러한 도구 또는 소프트웨어 패키지는 종종 시스템에서 발견되며 고급 사용자, 관리자, 네트워크 관리자 또는 일반 사용자를 위한 합법적인 목적을 가지고 있습니다.

프로시저

1. MITRE ATT&CK 리포지토리 데이터를 보려면 다음으로 이동하십시오. 작업 공간 〉 위협 인텔리전스 보안 센터 〉 위협 인텔 라이브러리 〉 **MITRE ATT&CK** 〉 도구.
   나열된 도구를 볼 수 있습니다.
2. 도구를 클릭하면 관련된 모든 정보를 볼 수 있습니다.
3. 새로 만들기를 클릭하여 MITRE ATT&CK 도구를 수동으로 생성합니다.
4. 필드를 적절하게 채웁니다.

새 **MITRE** 도구 생성 **-** 상세 정보

필드	설명
ID	공격을 방지하기 위한 작업 과정의 고유 ID입니다.
해지함	해지된 개체가 개체 작성자에 의해 더 이상 유효한 것으로 간주되지 않음을 나타냅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
이름	객체를 식별하는 설명이 포함된 이름을 입력합니다.
소스	이 개체 기록이 생성되는 위협 소스를 지정합니다.
별칭	이 객체를 식별하는 다른 이름의 목록입니다.
소스에서 생성된 시간	원본에서 개체가 만들어지는 시간을 지정합니다.
소스에서 수정된 시간	원본에서 개체가 수정되는 시간을 지정합니다.
설명	목적과 주요 특성을 포함하여 객체에 대한 자세한 내용과 컨텍스트를 제공하는 설명입니다.
기고자	기고자를 지정합니다.
인사이트	
메모	완화와 관련된 추가 정보입니다.
추가 정보	
추가 컨텍스트	이 객체에 대한 추가 컨텍스트를 추가합니다.
설명	이 객체에 대한 주석을 추가합니다.

5. 저장을 클릭합니다.
6. 이러한 객체의 관계를 보려면 관계를 클릭합니다.

MITRE 관계 관리

MITRE TAXII 컬렉션에서 임포트한 MITRE 관계 정보를 관리합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.analyst

프로시저

1. MITRE ATT&CK 리포지토리 데이터를 보려면 다음으로 이동하십시오. 작업 공간 〉 위협 인텔리전스 보안 센터 〉 위협 인텔 라이브러리 〉 **MITRE ATT&CK** 〉 관계.
   나열된 관계를 볼 수 있습니다.
2. 연관된 모든 정보를 보려면 아무 소스 객체나 클릭합니다.
3. 새로 만들기를 클릭하여 MITRE ATT&CK 관계를 수동으로 만듭니다.
4. 필드를 적절하게 채웁니다.

새 **MITRE** 도구 생성 **-** 상세 정보

필드	설명
소스 MITRE 객체	소스 MITRE 객체를 추가합니다.
대상 MITRE 객체	대상 MITRE 객체를 추가합니다.
소스 MITRE 유형	소스 MITRE 유형을 입력합니다.
대상 MITRE 유형	대상 MITRE 유형을 입력합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
관계 유형	개체 간의 관계를 정의합니다. 관계 유형에 대한 자세한 내용과 컨텍스트를 제공하는 설명입니다. 사용 가능한 옵션은 다음과 같습니다. 관계 방향이 직접인지 역인지 정의합니다. ○ 역 - 옵저버블과 객체 간의 관계 유형입니다. ○ 직접 - 객체와 옵저버블 간의 관계 유형입니다.
소스	원본 개체를 선택하고 정의합니다.
관계 ID	관계 ID를 정의합니다.

5. 저장을 클릭합니다.
6. 이러한 객체의 관계를 보려면 관계를 클릭합니다.

에서 데이터 마이그레이션 **TISC**

데이터 마이그레이션은 모든 데이터를 클래식 UI TISC에서 로 이동하는 프로세스입니다.

이 마이그레이션의 목적은 사용자가 기존 위협 인텔리전스 데이터에서 로 데이터를 마이그레이션할 수 TISC있도록 하는 것입니다. 이 프로세스를 실행하기 위해 다음 섹션에서 설명하는 새로운 프레임워크가 도입되었습니다 TISC .

SIR TI에서 **TISC**

의 TISC 데이터 마이그레이션 작업 구성을 사용하면 기존 위협 인텔리전스 플러그인 데이터를 플러그인 데이터로 직접 이동할 수 있습니다 TISC .

시작하기 전에

필요한 역할: sn_sec_tisc.admin

이 태스크 정보

- 선택적 기록 마이그레이션: 선택한 테이블 중 지정된 조건을 충족하는 기록만 마이그레이션됩니다.
- 관계 포함: 관계 포함 확인란이 선택된 경우에만 관련 기록이 마이그레이션됩니다.
- 엔터티 마이그레이션 상태: 엔터티(옵저버블 또는 객체)가 마이그레이션되면 관련 기록으로 마이그레이션되지 않는 한 추가 마이그레이션에 포함되지 않습니다.

  주:
  마이그레이션 유틸리티에 대한 기록 제외 기준

  마이그레이션 유틸리티는 다음 기준에 따라 특정 기록을 제외합니다.

  ○ 옵저버블: 보안 첨부 파일을 포함하는 파일 유형의 옵저버블은 마이그레이션되지 않습니다.
  ○ 표시기: 패턴 또는 패턴 유형 필드에 빈 값이 있는 표시기는 마이그레이션되지 않습니다.
  ○ 개체: 위협 인텔리전스 데이터 내의 MITRE TAXII 프로필에서 수집된 개체는 위협 인텔리전스 보안 센터로 마이그레이션되지 않습니다.

- 케이스 기록: 종결된 케이스 포함 확인란을 선택하지 않으면 기본적으로 활성 기록만 마이그레이션됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 보안 센터 〉 데이터 마이그레이션 작업 구성.
2. 새로 만들기를 클릭합니다.
3. 양식의 필드에 적절한 정보를 입력합니다.

데이터 마이그레이션 작업 구성

필드	설명
이름	데이터 마이그레이션의 이름입니다.
테이블	기록을 마이그레이션할 테이블을 TISC선택합니다. TISC 마이그레이션을 위한 테이블 옵션은 다음과 같습니다. ○ 옵저버블(sn_ti_observable) ○ 영향 표시기(sn_ti_indicator) ○ 보안 케이스(sn_ti_case) ○ STIX V2 개체(sn_ti_stix2_object) (공격 패턴, 캠페인, 작업 과정과 같은 옵션) 주: ○ STIX V2 옵션을 선택하면 TISC에는 MITRE ATT&CK를 마이그레이션하는 다른 프레임워크가 있으므로 MITRE ATT&CK를 제외한 모든 STIX 객체가 마이그레이션됩니다. ○ 보안 케이스 마이그레이션을 선택하면 종결된 케이스는 마이그레이션되지 않고 활성 케이스만 마이그레이션됩니다. 예를 들어 옵저버블 마이그레이션 테이블을 선택합니다.
활성	데이터 마이그레이션 프로세스가 활성 상태인 경우 이 확인란을 선택합니다.
관계 포함	위협 인텔리전스 기록의 관계를 기록으로 TISC 마이그레이션하려면 이 확인란을 선택합니다. 주: 이 확인란을 선택하면 모든 관련 엔터티가 옵저버블과 함께 마이그레이션되며, 이 확인란을 선택하지 않으면 관련 엔터티 없이 단일 옵저버블만 마이그레이션됩니다.
종결된 케이스 포함	종결된 케이스를 케이스 기록 마이그레이션의 일부로 포함하려면 이 확인란을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
보안 인시던트와 관련된 옵저버블만 마이그레이션	보안 인시던트와 연결된 옵저버블을 마이그레이션하려면 확인란을 선택합니다. 이 확인란을 선택하지 않으면 보안 인시던트와의 연관성에 관계없이 모든 옵저버블이 마이그레이션됩니다.
조건	마이그레이션 중인 데이터를 필터링하는 데 사용할 수 있는 조건을 선택하는 옵션입니다.
추가 구성	
신뢰도	마이그레이션된 TISC 엔터티(옵저버블 또는 객체 또는 표시기)에 대한 신뢰도를 입력합니다. 신뢰도는 0-100 범위 사이여야 합니다.
만료 기간(일)	마이그레이션된 TISC 엔터티의 만료 기간입니다.

주:
시스템은 다시 가져올 때 이미 마이그레이션 TISC 된 기록을 무시하거나 건너뜁니다.

4. 제출을 클릭합니다.
5. 지금 실행을 클릭하여 데이터 마이그레이션을 실행합니다.
   데이터 마이그레이션을 실행하면 백그라운드 작업이 실행되고 마이그레이션 작업이 생성됩니다. 이 작업은 마이그레이션 프로세스를 생성하며 이러한 마이그레이션 기록의 배치 크기는 5,000입니다.
6. 마이그레이션 작업 실행 섹션에서 마이그레이션 작업 상태를 확인합니다.
   작업 상태가 큐에 대기 중이며 배치 크기의 최대 한도는 5,000개 기록을 초과할 수 없습니다. 해당 특정 엔터티에 대해 모두 마이그레이션된 객체를 보려면 기록을 클릭합니다.
7. 마이그레이션 작업 실행 관련 목록에서 마이그레이션 작업 상태를 확인합니다.
8. 기록을 클릭하여 처리 상태를 확인합니다.
9. 마이그레이션 작업 실행 기록의 마이그레이션 처리 큐 기록 관련 목록 섹션에서 일괄 마이그레이션 상태를 확인합니다.
   기록 마이그레이션을 위한 배치 크기는 5000입니다.
10. 마이그레이션 처리 큐 기록의 각 관련 목록에서 배치 마이그레이션의 일부로 생성된 TISC 엔터티를 확인합니다.

TISC 데이터 처리 기능 플로우

TISC(Threat Intelligence Security Center)는 데이터 수집 및 처리를 자동화하는 솔루션을 제공하여 관련된 수동 단계를 방지함으로써 위협 인텔리전스 분석가의 부담을 줄이는 데 도움이 됩니다.

TISC(위협 인텔리전스 보안 센터)는 다음 방법 중 하나를 사용하여 인텔리전스를 수집합니다.

1. 미리 구성되어 일정에 따라 실행되는 데이터 소스에서 수집합니다.
2. 인텔리전스 임포트 기능을 사용하여 데이터를 임포트하는 위협 인텔리전스 분석가.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 애플리케이션 내에서 개별 기록을 수동으로 생성합니다.

   주:
   애플리케이션에서 수집된 데이터는 위협 인텔 라이브러리에 로드하기 전에 정보를 정규화, 중복 제거 및 집계하기 위해 처리됩니다.

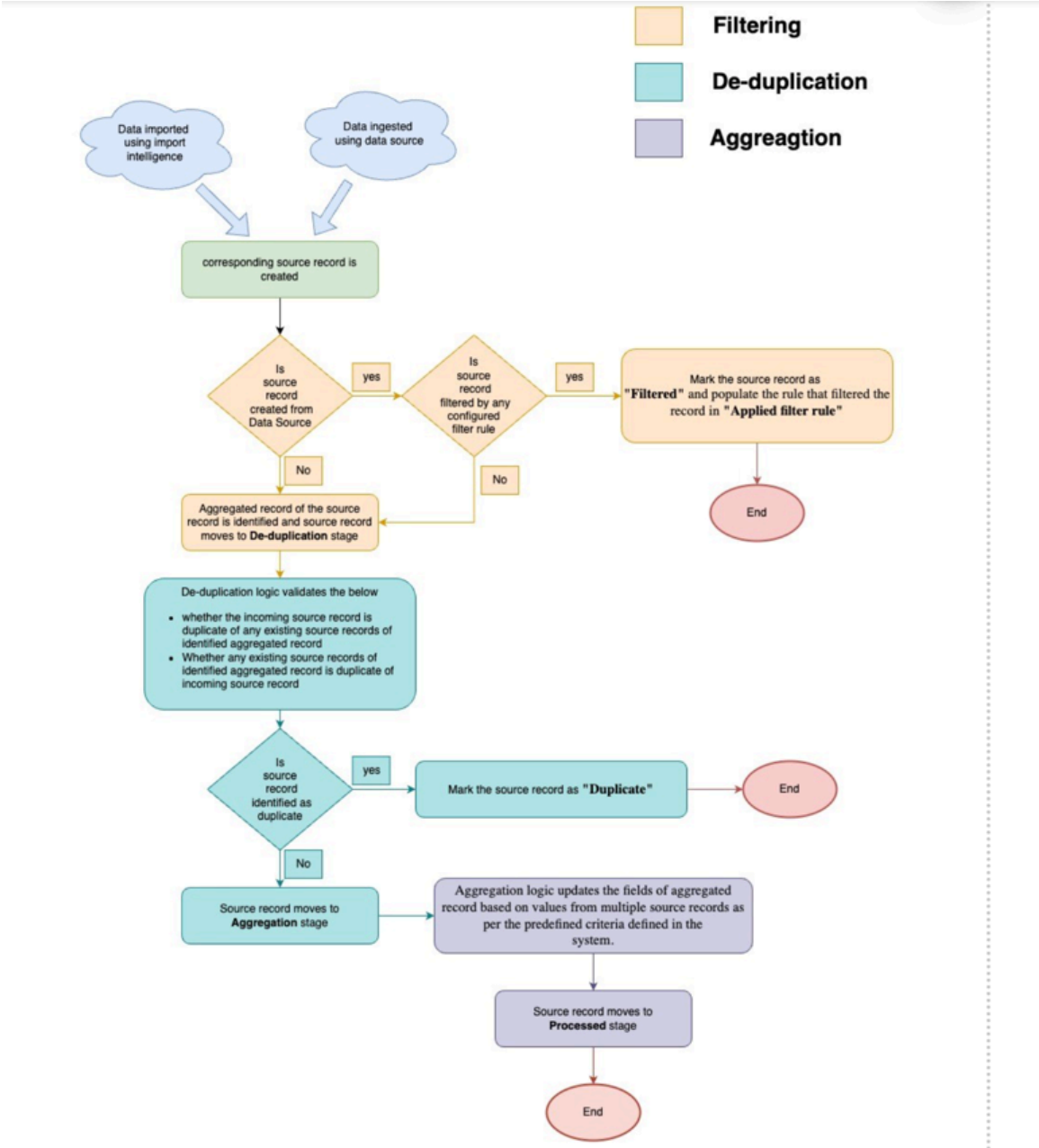
데이터 처리에 사용되는 기본 용어

1. 소스 테이블: 소스 테이블에는 여러 소스에서 가져온 엔터티와 관련된 데이터가 포함되어 있으며 각 소스에 의해 기록이 생성됩니다.
2. 집계된 기록: 집계된 기록 테이블에는 특정 엔터티의 모든 소스 기록에서 데이터를 집계하여 특정 엔터티와 관련된 데이터가 포함됩니다.

TISC 데이터 플로우

1. 인텔리전스/데이터 소스 임포트가 성공적으로 실행되면 해당 소스 테이블에 기록이 생성됩니다.
2. 데이터가 소스 테이블에 들어오면 데이터는 필터링 논리를 거쳐 구성된 인바운드 필터링 규칙을 기반으로 기록을 필터링해야 하는지 확인합니다. (설명을 위한 소스 레코드로 SourceRecord1을 고려해 보겠습니다.)
3. 구성된 인바운드 필터링 규칙 중 하나에 따라 기록이 필터링되면 해당 소스 기록 (SourceRecord1)이 필터링 됨으로 표시되고 기록을 필터링한 규칙은 적용된 필터 규칙에서 찾을 수 있습니다.
4. 소스 기록(SourceRecord1)이 AggregateRecord1로 집계된다고 가정해 보겠습니다.
5. 기록이 필터링되지 않은 경우 처리 상태를 중복 제거 준비 완료로 설정하여 기록이 중복 제거를 위해 표시됩니다.
6. 중복 제거 논리는 다음 사항을 확인합니다.
   a. 수신 소스 기록(SourceRecord1)이 AggregateRecord1에 대한 기존 소스 기록과 중복되는지 여부입니다.
   b. AggregateRecord1에 대한 기존 소스 기록은 수신 소스 기록(SourceRecord1)과 중복됩니다.
7. 모든 엔터티에는 소스 기록의 중복 여부를 확인하는 데 사용하는 특정 필드와 관계가 있습니다.
8. 수신 소스 기록(SourceRecord1)이 AggregateRecord1의 기존 소스 기록과 중복되는 경우, 수신 소스 기록(SourceRecord1)은 중복으로 표시됩니다.
9. AggregateRecord1의 기존 소스 기록(기존 소스 기록1) 중 하나라도 수신 소스 기록 (SourceRecord1)과 중복으로 식별되는 경우, 처리 상태를 집계 준비 완료로 설정하여 기존 소스 기록(기존 소스 기록1)이 중복으로 표시되고 수신 소스 기록(SourceRecord1)이 집계되도록 표시됩니다.
10. 집계의 일부로 집계된 기록 AggregateRecord1의 필드는 시스템에 정의된 미리 정의된 기준에 따라 여러 소스 기록의 값을 기반으로 업데이트됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



TISC 데이터 보관

플랫폼 채택이 증가함에 따라 테이블의 데이터가 빠르게 증가합니다. 일부 테이블은 다양한 데이터 관리 정책을 통해 기본 시스템 내에 제공되지만 다른 사용자는 직접 구현해야 합니다.

의 데이터 관리 TISC

데이터는 관리자가 조직의 필요에 따라 보고 구성할 수 있도록 라이브러리 객체 구조에 TISC 따라 인스턴스에 저장되고 관리 TISC 됩니다.

데이터 보관 및 복원은 나중에 사용할 수 있도록 기록을 보호하는 핵심 기능 중 하나입니다. 다음 섹션에서는 방대한 양의 데이터와 기록이 위협 인텔리전스 포함된 보관 프로세스 및 기록 보존에 TISC 대해 설명합니다.

사용자가 테이블에서 데이터를 관리할 수 있는 몇 가지 방법이 있습니다.

- 데이터 보관
- 데이터 삭제

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
사용자가 데이터를 효과적으로 관리하기 위한 방법을 채택하지 않으면 시간이 지남에 따라 사용량이 증가하고 데이터가 훨씬 커지는 경향이 있어 애플리케이션 인스턴스 성능과 스토리지에 큰 영향을 미칩니다.

TISC 데이터 보관

위협 인텔리전스 보안 센터 는 테이블에 대한 기본 시스템의 보관 규칙과 함께 프로비저닝됩니다TISC. 관련 기록도 기본 시스템의 보관 규칙에 추가됩니다 TISC .

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 〉 시스템 보관 〉 보관 규칙.
   적용할 수 TISC 있는 보관 규칙 목록이 표시됩니다. 이러한 보관 규칙은 객체 유형마다 다르며 독립적으로 적용할 수 있습니다.
2. sn_sec_tisc로 시작하는 테이블 이름을 필터링합니다.
3. TISC 관련 기록을 봅니다.

Threat Intelligence 기록	참조 테이블
아카이브 공격 패턴	sn_sec_tisc_attack_pattern
캠페인 보관	sn_sec_tisc_campaign
작업 방침 보관	sn_sec_tisc_course_of_action
보관 데이터 구성요소	sn_sec_tisc_aggregated_data_component
데이터 소스 보관	sn_sec_tisc_aggregated_data_source
보관 ID	sn_sec_tisc_identity
인프라 보관	sn_sec_tisc_infrastructure
침입 세트 보관	sn_sec_tisc_intrusion_set
맬웨어 보관	sn_sec_tisc_malware
아카이브 맬웨어 분석	sn_sec_tisc_malware_analysis
보관 표시 정의	sn_sec_tisc_marking_definition
객체 사이팅 보관	sn_sec_tisc_object_sighting
관찰 데이터 보관	sn_sec_tisc_observed_data
위협 액터 보관	sn_sec_tisc_threat_actor
위협 이벤트 보관	sn_sec_tisc_threat_event
보관 위협 그룹화	sn_sec_tisc_threat_grouping
위협 메모 보관	sn_sec_tisc_threat_note
위협 의견 보관	sn_sec_tisc_threat_opinion
위협 보고서 보관	sn_sec_tisc_threat_report
보관 도구	sn_sec_tisc_tool
취약성 보관	sn_sec_tisc_vulnerability

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Threat Intelligence 기록	참조 테이블
아티팩트	sn_sec_tisc_artifact
AS 번호	sn_sec_tisc_as_number
디렉터리	sn_sec_tisc_directory
이메일 주소	sn_sec_tisc_email_address
이메일 메시지	sn_sec_tisc_email_message
이메일 제목	sn_sec_tisc_email_subject
파일	sn_sec_tisc_file
표시기 보관 규칙	sn_sec_tisc_indicator
IPv4 주소	sn_sec_tisc_ipv4_address
IPv4 CIDR	sn_sec_tisc_ipv4_cidr
IPv6 주소	sn_sec_tisc_ipv6_address
위치	sn_sec_tisc_location
MAC 주소	sn_sec_tisc_mac_address
MD5 해시	sn_sec_tisc_md5_hash
뮤텍스 이름	sn_sec_tisc_mutex_name
기타 옵저버블	sn_sec_tisc_other_observable
프로세스	sn_sec_tisc_process
SHA1 해시	sn_sec_tisc_sha1_hash
SHA256 해시	sn_sec_tisc_sha256_hash
SHA512 해시	sn_sec_tisc_sha512_hash
URL	sn_sec_tisc_url
사용자 계정	sn_sec_tisc_user_account
Windows 레지스트리 키	sn_sec_tisc_windows_registry_key
X.509 인증서	sn_sec_tisc_x_509_certificate
객체-객체 관계 보관 규칙	sn_sec_tisc_m2m_object
객체-옵저버블 관계 보관 규칙	sn_sec_tisc_m2m_object_observable
관련 표시기 보관 규칙	sn_sec_tisc_m2m_indicator
RSS 피드 보관 규칙	sn_sec_tisc_m2m_object_indicator
임포트 보관 규칙	sn_sec_tisc_m2m_indicator_observable

주:

보관 규칙이 생성되는 방법에 대한 자세한 내용은 을 참조하십시오 Create an archive rule.

4. 보관 규칙을 선택합니다.
   예를 들어 기본 시스템 보관 규칙을 보려면 디렉터리 옵저버블 기록을 선택합니다.
5. 필요한 경우 규칙을 업데이트합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관련 기록 보관 TISC

관련 기록을 보관 규칙에 추가하려면 보관 관련 기록 관련 TISC 목록을 사용합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 〉 시스템 보관 〉 보관 규칙.
2. sn_sec_tisc로 시작하는 테이블 이름을 필터링합니다.
3. 관련 기록을 보려면 TISC보관 관련 기록 관련 목록 섹션으로 이동합니다.

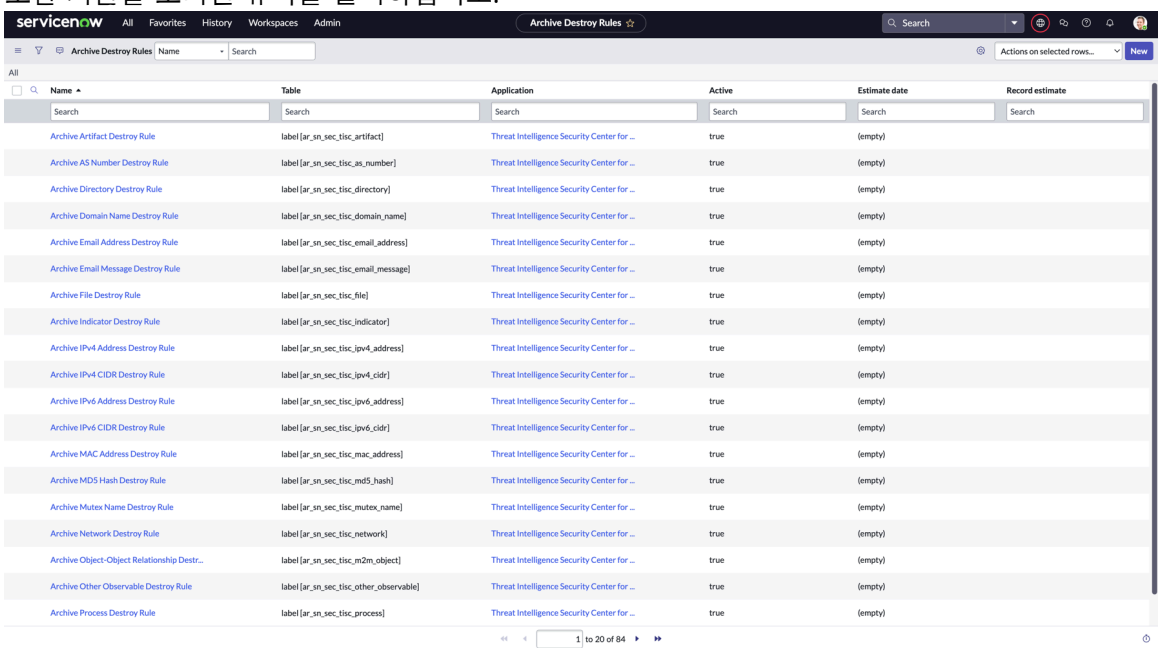
의 삭제 규칙 TISC

기본 시스템에 프로비저닝된 삭제 규칙을 봅니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 〉 시스템 보관 〉 보관 삭제 규칙.
   적용할 수 TISC 있는 삭제 규칙 목록이 표시됩니다. 이러한 삭제 규칙은 객체 유형마다 다르며 독립적으로 적용할 수 있습니다.
2. 에 적용 TISC가능한 삭제 규칙을 봅니다.
3. 보관 기간을 보려면 규칙을 클릭하십시오.



인텔리전스 기록 삭제

라이브러리에서 위협 인텔리전스 기록을 삭제합니다.

시작하기 전에
필요한 역할: sn_sec_tisc.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 작업 공간 〉 위협 인텔리전스 보안 센터.
2. 작업 공간에서 위협 인텔 라이브러리 아이콘을 클릭합니다.
3. 기록을 엽니다.
4. 소스 기록 섹션으로 이동합니다.
5. 삭제를 선택하여 소스 기록을 삭제합니다.
6. 라이브러리 기록을 삭제합니다.

주:

a. 연결된 소스 기록이 있는 라이브러리 기록이 삭제되면 소스 기록이 다시 처리되고, 소스 기록에서 필드 값을 집계하여 새 라이브러리 기록이 생성됩니다.

b. 위협 인텔리전스 라이브러리에서 데이터를 영구적으로 삭제하려면 라이브러리 기록을 삭제하는 대신 보관 규칙을 사용합니다. 자세한 내용은 TISC 데이터 보관 문서를 참조하십시오.

Data Loss Prevention Incident Response

Data Loss Prevention Incident Response (DLP IR) 애플리케이션을 사용하면 엔드포인트, 네트워크, 이메일 및 클라우드와 같은 여러 소스에서 DLP 인시던트 정정 워크플로우를 검토하고 관리할 수 있습니다.

스토어에서 앱 요청

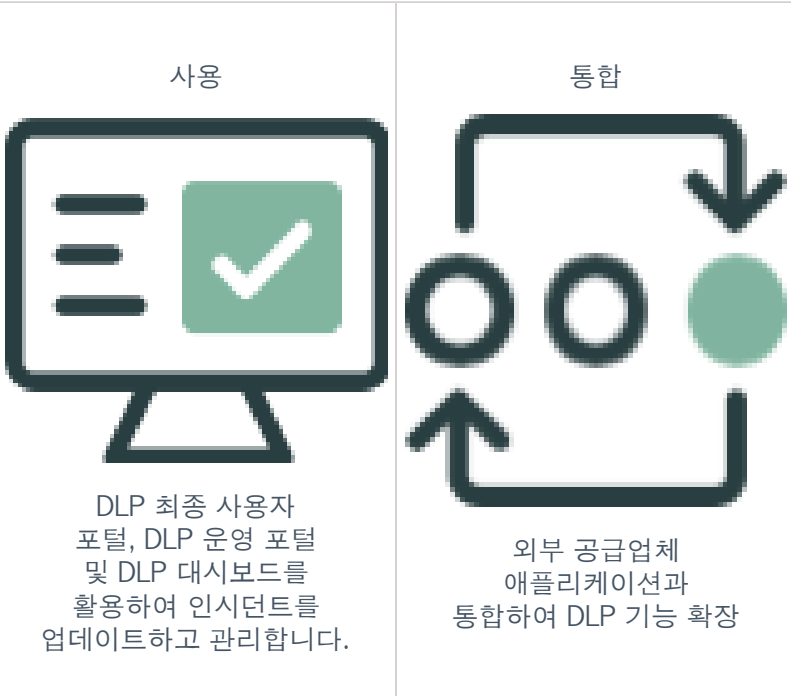
ServiceNow Store 웹 사이트를 방문하면 사용 가능한 모든 앱을 확인하고 스토어에 요청을 제출하는 방법에 대한 정보를 참조할 수 있습니다. 출시된 모든 앱의 누적 릴리스 정보는 ServiceNow Store 버전 기록 릴리스 정보를 참조하십시오.

Data Loss Prevention Incident Response

탐색	설치 및 구성	관리자
분석가 및 관리자가 DLP Incident Response를 사용하는 방법 알아보기	DLP 인시던트 응답 애플리케이션 설치 및 구성	에서 DLP 인시던트를 관리하는 방법에 대한 관리 작업 ServiceNow AI Platform

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Data Loss Prevention Incident Response



문제 해결 및 도움 받기

- Security Operations 리소스 라이브러리
- Security Operations 커뮤니티
- 알려진 오류 포털에서 알려진 오류 문서 검색
- 연락처 고객 서비스 및 지원

Data Loss Prevention Incident Response 탐색

애플리케이션을 탐색 Data Loss Prevention Incident Response 하여 금융 및 소유 데이터, 건강 기록 또는 주민 등록 번호와 같은 고객의 중요한 정보를 관리하는 방법을 알아봅니다.

데이터 손실은 무단 통신의 결과로 기밀 또는 민감한 정보가 엔터프라이즈 네트워크를 떠날 때 발생합니다. DLP 애플리케이션을 사용하여 데이터 손실 채널을 식별, 응답 및 보호할 수 있습니다.

애플리케이션을 사용 Data Loss Prevention Incident Response 함으로써 조직은 다음과 같은 주요 이점을 얻을 수 있습니다.

- 여러 외부 공급업체 DLP 솔루션과 통합하여 의 ServiceNow AI Platform인시던트를 종합적으로 볼 수 있습니다.
- DLP 인시던트 관리를 간소화할 수 있도록 인시던트를 모니터링하고 최종 사용자에게 할당합니다.
- 각 인시던트에 대해 전송되는 사용자 지정 이메일 템플릿과 알림, 그리고 다이제스트 형태로 직원을 코칭합니다.
- 기한이 지난 DLP 인시던트를 최종 사용자에게서 관리자로 에스컬레이션합니다.
- 정책, 심각도, 상위 공격자 등에 따른 미해결 인시던트의 요약 보고서를 봅니다.
- DLP 인시던트 추세, 가양성 추세 및 정정 추세를 추적합니다.

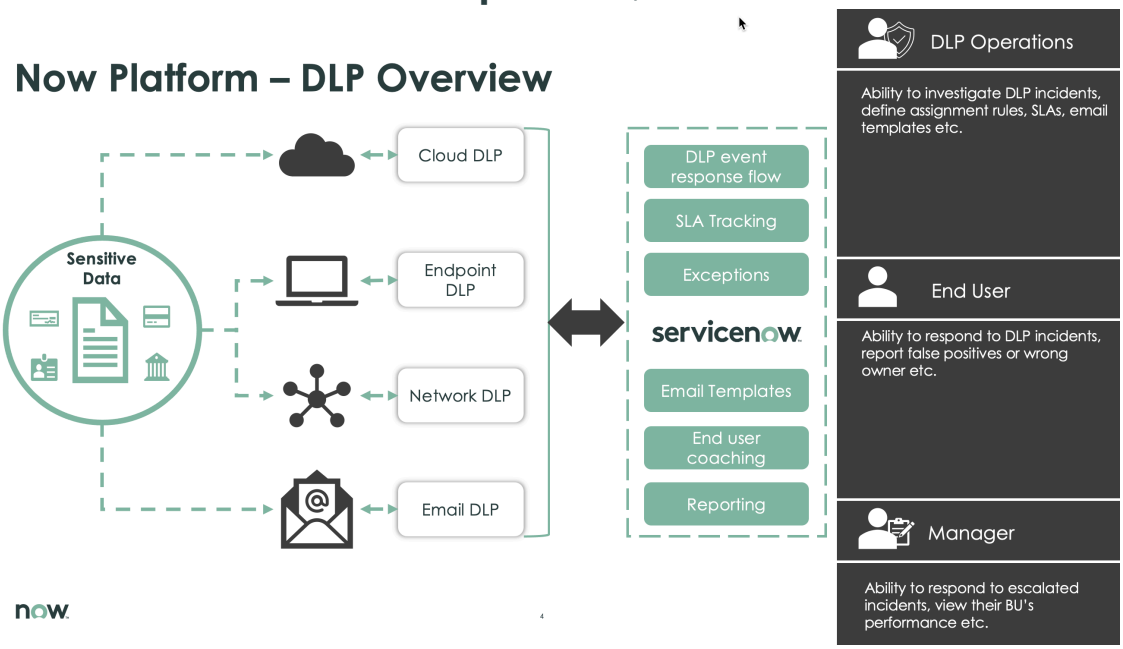
이 섹션에서는 DLP 인시던트 작업과 관련된 주요 기능, 다양한 역할에 대해 알아봅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

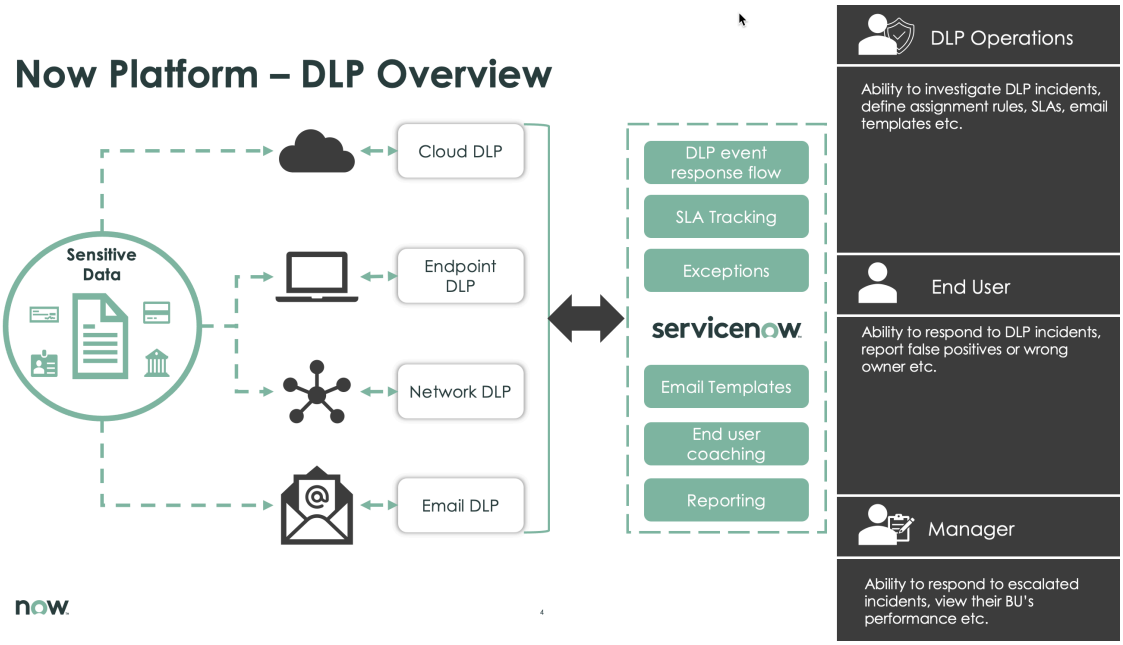
DLP 인시던트 응답 개요

및 Data Loss Prevention Incident Response (DLP IR) 애플리케이션을 사용하는 ServiceNow AI Platform 방법에 대해 알아봅니다. 금융 및 소유 데이터, 건강 기록 또는 주민등록번호와 같은 고객의 민감한 정보를 관리합니다. DLP 인시던트 응답 애플리케이션으로 정정 워크플로우를 자동화합니다.

Data Loss Prevention Incident Response 그리고 ServiceNow AI Platform



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



1. 이것은 클릭할 수 있는 이미지이므로 다른 섹션을 클릭하여 DLP에 대해 자세히 알아볼 수 있습니다
2. DLP 관리자 작업 - 클릭할 수 있는 이미지이므로 다른 섹션을 클릭하여 DLP에 대해 자세히 알아볼 수 있습니다.
3. DLP 최종 사용자 포털 사용 - 클릭할 수 있는 이미지이므로 다른 섹션을 클릭하여 DLP에 대해 자세히 알아볼 수 있습니다.
4. DLP 운영 포털 사용 - 클릭할 수 있는 이미지이므로 다른 섹션을 클릭하여 DLP에 대해 자세히 알아볼 수 있습니다.
5. DLP 대시 보드 사용 - 이것은 클릭 가능한 이미지이므로 다른 섹션을 클릭하여 DLP에 대해 자세히 알아볼 수 있습니다.

이 애플리케이션에는 Data Loss Prevention Incident Response 다음과 같은 기능이 포함됩니다.

- 최종 사용자 또는 직원이 할당된 DLP 인시던트를 검토하고 응답할 수 있는 최종 사용자 작업 공간입니다.
- 관리자가 에스컬레이션된 DLP 인시던트를 검토하고 적절한 조치를 취할 수 있는 관리자 작업 공간입니다.
- DLP 운영 팀이 스캔 소스별로 오픈 인시던트, 상위 공격자, 인시던트에 대한 추세를 추적하고 여러 소스(엔드포인트, 네트워크 및 이메일)에서 DLP 인시던트를 보고, 편집하고, 할당하고, 종결할 수 있는 통합 작업 공간입니다.
- 최종 사용자 코칭 및 커뮤니케이션을 위한 이메일 템플릿, 인시던트 자동 할당을 위한 할당 규칙, 자동 에스컬레이션 규칙 및 인시던트 응답에 대한 위임을 정의하는 관리 제어.

DLP 인시던트 응답 시작하기

(DLP IR) 애플리케이션 설정을 Data Loss Prevention Incident Response 시작하기 전에 다음 정보를 검토합니다.

검사 목록

설정 작업	설명
필수 ServiceNow AI Platform 역할과 DLP 역할을 할당했는지 확인합니다.	DLP 인시던트 응답은 다음 역할을 지원합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

검사 목록

설정 작업	설명
	• 관리자(admin)는 에서 애플리케이션을 ServiceNow Store 설치하고 DLP 관리자(sn_dlir.admin)를 할당합니다. • sn_dlir.admin • sn_dlir.분석가
ServiceNow 애플리케이션을 지원하는 Data Loss Prevention Incident Response 데 필요한 핵심 애플리케이션이 설치되고 활성화되었는지 확인합니다.	Data Loss Prevention Incident Response 제품을 지원하려면 플러그인(com.snc.data_loss_incident)이 Data Loss Prevention Incident Response 필요합니다. 에서 ServiceNow Store다음 보안 운영 애플리케이션이 설치되고 활성화되는지 확인합니다. 설치되지 않은 경우 원활한 설치를 위해 다음 순서로 한 번에 하나의 애플리케이션을 설치하고 활성화합니다. • 데이터 손실 방지 인시던트 응답(com.snc.data_loss_incident) • Security Support Common 통합을 위한 인스턴스 설정에 ServiceNow AI Platform 대한 자세한 내용은 보안 운영 제품 또는 애플리케이션에 대한 권리 얻기 또는 ServiceNow Store 애플리케이션 활성화를 참조하십시오.
도메인 분리	도메인 분리 및 DLP Incident Response 데이터, 프로세스 및 관리 작업을 분리하려면 주제를 확인합니다.

Incident Response 설치 및 구성 DLP IR

Data Loss Prevention Incident Response 에서 ServiceNow Store (DLP IR) 애플리케이션을 다운로드하여 인스턴스에 설치합니다.

통합을 위한 워크플로우를 호출하기 전에 인스턴스에서 애플리케이션을 ServiceNow StoreServiceNow AI Platform 설치하고 구성합니다Data Loss Prevention Incident Response.

DLP 인시던트 응답 애플리케이션 설치 및 구성

인스턴스에서 (DLP IR) 애플리케이션을 ServiceNow AI Platform 사용하여 중요한 정보를 관리하고 정정 워크플로우를 Data Loss Prevention Incident Response 자동화합니다.

시작하기 전에
구성 단계를 완료하려면 먼저 에서 ServiceNow Store 애플리케이션을 다운로드하여 인스턴스에 설치해야 합니다.

필요한 역할: admin 및 sn_dlir.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. ServiceNow Store에서 애플리케이션 다운로드에 대한 지침을 따르십시오.
2. **DLP** 인시던트 응답 애플리케이션과 모든 종속성 애플리케이션을 다운로드한 후 모두 〉 **DLP** 관리 〉 기본 구성 나머지 애플리케이션 구성을 완료합니다.

도메인 분리 및 **DLP Incident Response**

DLP 인시던트 응답과 함께 도메인 분리를 사용하여 데이터, 프로세스 및 관리 작업을 도메인이라는 논리적 그룹으로 구분할 수 있습니다. 그런 다음 사용자가 데이터를 보고 액세스할 수 있는 것을 포함하여 이러한 분리의 여러 가지 측면을 제어할 수 있습니다.

지원 수준: 표준

- 기본 수준 지원의 모든 측면을 포함합니다.
- 애플리케이션 속성이 필요에 따라 도메인을 인식합니다.
- 비즈니스 논리: 서비스 제공자(SP)가 고객별로 프로세스를 만들거나 수정합니다. 사용 사례는 여러 SP 고객이 단일 인스턴스에서 애플리케이션을 올바르게 사용하는 것을 반영합니다.
- 인스턴스 소유자는 특정 애플리케이션에 필요한 대로 테넌트별 최소 실행 가능한 제품(MVP) 비즈니스 논리 및 데이터 매개변수를 구성해야 합니다.

샘플 사용 사례: 관리자가 한 테넌트에 대해서는 기록이 닫히지만 다른 테넌트에 대해서는 기록이 닫히지 않는 경우 설명이 필요하도록 설정할 수 있어야 합니다.

지원 수준에 대한 자세한 내용은 도메인 분리를 위한 애플리케이션 지원 을 참조하십시오.

DLP 인시던트 응답에서 도메인 분리가 작동하는 방식

- 해당 도메인에서 필요한 sn_dlir.admin 및 sn_dlir.analyst 역할을 가진 사용자를 생성합니다.
- 적절한 도메인에서 DLP 인시던트 응답 구성을 수행합니다.

DLP 인시던트 응답 관리

규칙을 설정 및 할당하고, 기한 규칙을 구성하고, 이메일 템플릿을 사용하고, 최종 사용자 응답 동작을 구성하는 등 에서 (DLP IR) 인시던트를 Data Loss Prevention Incident Response 관리할 수 있습니다 ServiceNow AI Platform.

이 Data Loss Prevention Incident Response 애플리케이션을 사용하면 다음 구성을 수행할 수 있습니다.

DLP 기본 구성 설정

(DLP IR) 인시던트의 Data Loss Prevention Incident Response 기본 구성 설정을 정의하여 최종 사용자의 인시던트 알림 및 인시던트 할당 기본 설정을 식별하고 설정합니다.

시작하기 전에
필요한 역할:

- sn_dlir.admin - 작성, 편집 및 삭제.
- sn_dlir.analyst 및 sn_dlir.analyst_read - 뷰(읽기 전용).

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보

이 모듈을 사용하면 핵심 담당 규칙 및 식별자 규칙이 소진되어 조건 또는 사용자와 일치시킬 수 없는 경우 기본 구성 설정을 정의할 수 있습니다. 최종 사용자 조회 규칙 및 담당 규칙을 정의하고 기존 활성 DLP 인시던트에 다시 적용할 수도 있습니다.

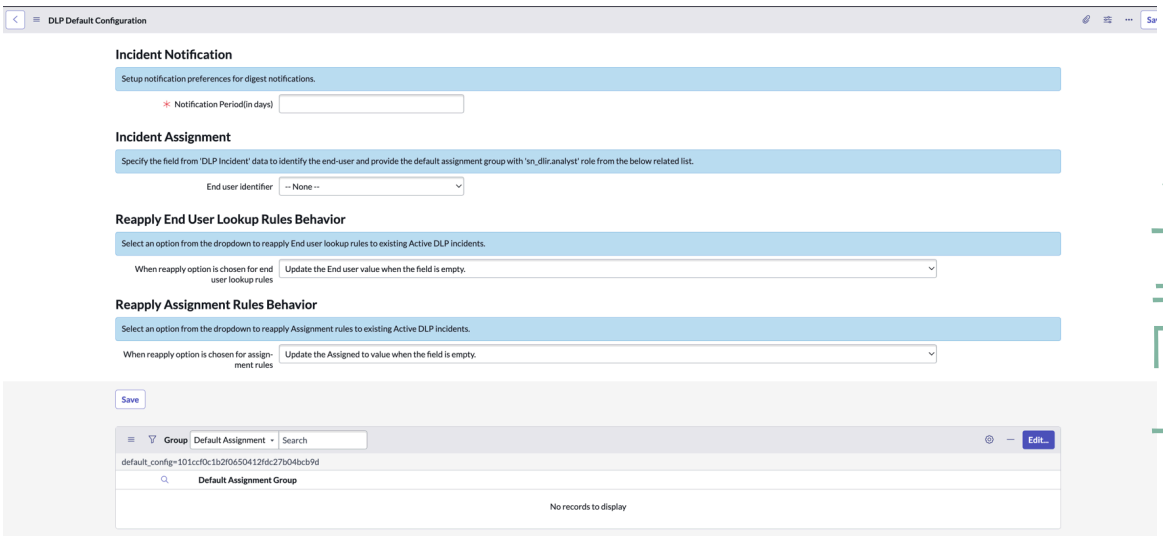
최종 사용자 인시던트 알림을 사용하면 최종 사용자에게 이메일 알림을 보내는 빈도를 지정할 수 있습니다. 예를 들어 인시던트를 누적하고 일주일에 한 번 이메일 다이제스트를 보내도록 알림 기본 설정을 지정할 수 있습니다. 인시던트를 할당하여 DLP 인시던트를 처음에 할당할 그룹을 지정할 수 있습니다. DLP 운영 팀에서 최종 사용자를 추가로 식별하는 방법을 지정할 수도 있습니다.

예를 들어 사용자가 네트워크의 파일에 신용 카드 정보를 저장했다고 가정해 보겠습니다. 타사 DLP 통합 제품이 민감한 데이터 정책 위반에 대한 인시던트를 생성하는 경우 DLP가 ServiceNow AI Platform 수집하는 인시던트 데이터에는 최종 사용자에 대한 정보가 포함됩니다. 그러면 인시던트를 올바른 최종 사용자에게 할당할 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 **DLP** 관리 〉 기본 구성.

DLP 정책 구성



2. 양식에서 필드를 채웁니다.

DLP 기본 구성 양식

구성 이름	필드	설명
최종 사용자 인시던트 알림	알림 기간(일)	최종 사용자에게 이메일 알림을 보내야 하는 일 수를 정의합니다. 일 수는 1일에서 60일 사이여야 합니다.
	복제된/하위 인시던트에 따라 상위 상태 자동 업데이트	복제된 인시던트 또는 하위 인시던트를 기반으로 상위 상태 인시던트를 자동으로 업데이트하는 옵션입니다.
인시던트 할당	최종 사용자 식별자	최종 사용자를 식별하기 위해 인시던트 데이터에서 사용할 필드를 지정합니다. 가능한 값은 다음과 같습니다. ○ 데이터 소유자 이메일 ○ 대상

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

구성 이름	필드	설명
		○ 파일을 생성한 사람 ○ 파일을 수정한 사람 ○ 파일 소유자 ○ **FTP** 사용자 이름 ○ 보낸 사람
최종 사용자 조회 규칙 동작 다시 적용	최종 사용자 조회 규칙에 재적용 옵션을 선택한 경우	최종 사용자 조회 규칙을 기존 활성 DLP 인시던트에 다시 적용하는 옵션입니다. 다음 옵션 중 하나를 선택하여 다시 적용할 수 있습니다. ○ 필드가 비어 있으면 최종 사용자 값 업데이트: 해당 필드가 비어 있는 경우 기존 활성 DLP 인시던트의 최종 사용자 값을 업데이트합니다. ○ 최종 사용자 값 업데이트: 기존 활성 DLP 인시던트의 최종 사용자 값을 업데이트합니다. ○ 최종 사용자와 할당 대상 값이 모두 비어 있으면 업데이트합니다. 기존 활성 DLP 인시던트의 최종 사용자 및 할당 대상 값이 모두 비어 있는 경우 두 필드를 모두 업데이트합니다. **주:** 이 옵션을 선택하면 필드가 비어 있을 때 할당 대상 값 업데이트 옵션이 할당 규칙 재적용 동작 섹션에서 자동으로 비활성화됩니다. ○ 모든 활성 **DLP** 인시던트에 대한 최종 사용자 및 할당 대상 값을 업데이트합니다. 모든 활성 DLP 인시던트에 대한 최종 사용자 및 할당 대상 값을 업데이트합니다. **주:** 이 옵션을 선택하면 모든 활성 **DLP** 인시던트에 대한 할당 대상 값 업데이트 옵션이 할당 규칙 다시 적용 동작 섹션에서 자동으로 비활성화됩니다.
할당 규칙 동작 다시 적용	할당 규칙에 재적용 옵션을 선택한 경우	할당 규칙을 기존 활성 DLP 인시던트에 다시 적용하는 옵션입니다. 다음 옵션 중 하나를 선택하여 다시 적용할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

구성 이름	필드	설명
		○ 필드가 비어 있으면 할당 대상 값을 업데이트합니다. ○ 모든 활성 **DLP** 인시던트에 대해 할당 대상 값을 업데이트합니다.

3. 모든 DLP 인시던트가 할당된 관련 목록 섹션에서 기본 할당 그룹을 선택합니다.
편집을 클릭하여 사용자 그룹을 추가합니다. 관련 목록 섹션에서 편집을 클릭하고 컬렉션 열에서 항목을 선택한 다음 선택한 담당자를 구성원 편집 페이지의 그룹 열에 추가하고 목록을 저장합니다.

   주:
   관련 목록에서 sn_dlir.analyst 역할이 할당된 그룹만 보고 선택할 수 있습니다. 하나의 그룹만 선택할 수 있습니다.

4. 저장을 클릭합니다.

최종 사용자 조회 규칙 생성

최종 사용자 조회 규칙을 생성 및 구성하고 해당 규칙에 따라 각 최종 사용자에게 DLP 인시던트를 할당할 수 있습니다.

시작하기 전에

필요한 역할:

- sn_dlir.admin - 작성, 편집 및 삭제.
- sn_dlir.analyst 및 sn_dlir.analyst_read - 뷰(읽기 전용).

이 태스크 정보

DLP 관리자는 이러한 최종 사용자 조회 규칙을 정의하여 최종 사용자 필드만 사용하여 최종 사용자를 DLP 인시던트에 자동으로 할당합니다. DLP 최종 사용자 조회 규칙을 사용하면 최종 사용자 식별자, 사용자 지정 속성 또는 스크립트를 기반으로 DLP 인시던트에 최종 사용자를 할당할 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 **DLP** 관리 〉 **DLP** 최종 사용자 조회 규칙.
2. 새로 만들기를 클릭합니다.
3. 양식에서 필드를 채웁니다.

DLP 최종 사용자 조회 규칙 양식

필드	설명
이름	최종 사용자 조회 규칙의 이름입니다.
활성	최종 사용자 조회 규칙이 활성 상태인지 여부를 나타내는 옵션입니다.
실행 순서	최종 사용자 조회 규칙 우선순위입니다. 이 필드는 둘 이상의 규칙이 트리거 조건을 공유할 때 최종 사용자 조회 규칙이 실행되는 순서를 나타냅니다. 가장 낮은 수의 최종 사용자 조회 규칙이 가장 높은 우선순위를 갖습니다. 작업 순서를

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

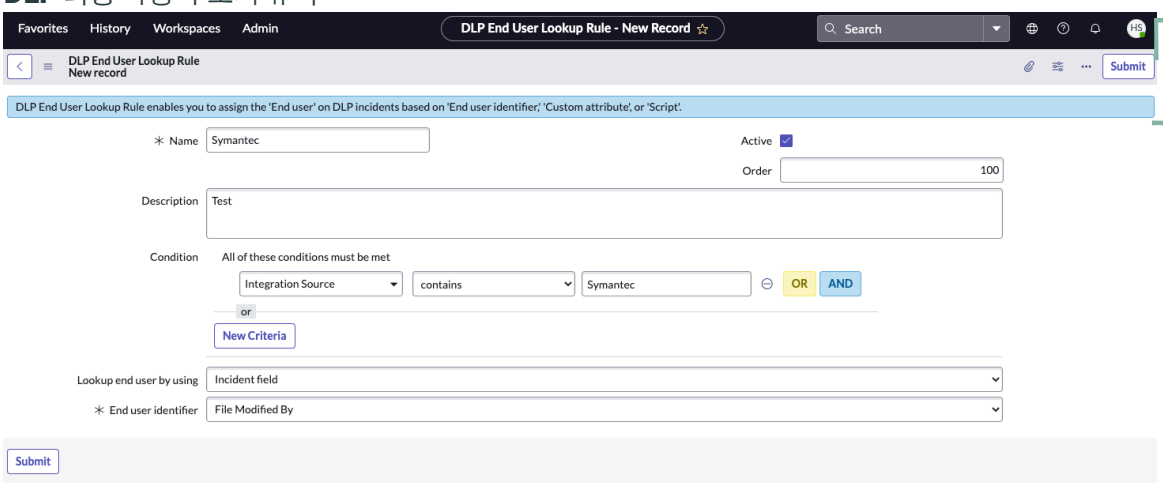
필드	설명
	설정하려면 값을 입력합니다. 예를 들어 100, 200, 300 등의 값을 입력합니다. 기본값은 100입니다.
설명	최종 사용자 조회 규칙에 대한 고유 설명입니다.
조건	조건 작성기의 조건입니다. 이러한 조건은 DLP 인시던트 테이블을 기반으로 합니다. 최종 사용자 조회 규칙에 대한 조건을 작성하려면 인시던트 필드를 선택합니다. 조건 작성기의 목록과 필드를 사용하여 첫 번째 행에 대한 필터를 설정합니다. 조건을 더 추가하려면 **AND** 또는 **OR**을 클릭합니다. ○ **AND**를 선택하면 모든 조건이 일치해야 합니다. ○ **OR**을 선택하면 두 조건을 일치시킬 수 있습니다. 두 번째 필터 조건을 설정하려면 새 기준을 클릭합니다. 예를 들어 조건을 통합 소스, 포함, 시만텍으로 선택하여 이 최종 사용자 조회 규칙의 조건을 설정할 수 있습니다. **주:** 조건 작성기의 조건은 대/소문자를 구분합니다.
다음을 사용하여 최종 사용자 조회	인시던트 필드 또는 스크립트를 사용하여 최종 사용자를 조회하는 옵션입니다.
최종 사용자 식별자	DLP 인시던트의 최종 사용자 식별자입니다. 이 필드는 '다음을 사용하여 최종 사용자 조회' 필드에서 인시던트 필드를 선택한 경우에 나타납니다. 다음 중에서 최종 사용자 식별자를 선택할 수 있습니다. ○ 데이터 소유자 이메일 ○ 대상 ○ 파일을 생성한 사람 ○ 파일을 수정한 사람 ○ 파일 소유자 ○ **FTP** 사용자 이름 ○ 보낸 사람

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	주: 위에 나열된 최종 사용자 식별자는 ### ## sn_dlir.assignment.fields를 사용하여 구성할 수 있습니다. 자세한 내용은 고급 설정 구성 문서를 참조하십시오. ○ 인시던트의 사용자 지정 사용자
사용자 지정 속성	사용자에 대한 참조가 있는 인시던트에서 사용자 지정 속성을 지정하는 옵션입니다. 이 필드는 최종 사용자 식별자 필드에서 **a**를 선택한 경우에만 나타납니다.
스크립트	스크립트 편집기를 사용하여 최종 사용자 조회 규칙을 생성하는 동안 필드 값을 사용자 지정하고 서식을 지정할 수 있습니다. 예를 들어 이메일 주소 필드를 사용하여 최종 사용자를 식별할 수 있습니다.

Example
다음 예는 이름이 'Symantec'인 최종 사용자 조회 규칙을 보여줍니다. 조건 작성기에는 "통합 소스"가 "Symantec"으로 필요합니다. 최종 사용자 조회 기준 옵션은 '인시던트 필드'로 설정되고 최종 사용자 식별자 옵션은 '파일을 수정한 사람'으로 설정됩니다.

DLP 최종 사용자 조회 규칙



4. 제출을 클릭합니다.
   하나 이상의 최종 사용자 조회 규칙을 선택하고 기존의 모든 DLP 인시던트에 다시 적용할 수도 있습니다.
5. 기존의 모든 DLP 인시던트에 최종 사용자 조회 규칙을 다시 적용하려면 다시 적용을 클릭합니다.

담당 규칙 생성

이 섹션을 사용하여 담당 규칙을 생성합니다. 그런 다음, 사용자 그룹, 최종 사용자, 관리자 또는 인시던트의 사용자에게 (DLP IR) 인시던트를 할당합니다 Data Loss Prevention Incident Response .

시작하기 전에
필요한 역할:

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- sn_dlir.admin - 작성, 편집 및 삭제.
- sn_dlir.analyst 및 sn_dlir.analyst_read - 뷰(읽기 전용).

이 태스크 정보

담당 규칙을 사용하여 사용자 그룹, 최종 사용자 또는 관리자에게 DLP IR 인시던트를 할당할 수 있습니다. DLP 인시던트 할당은 할당 규칙의 조건이 충족될 때 발생합니다.

프로시저

1. 다음으로 이동 모두 〉 **DLP** 관리 〉 담당 규칙.
2. 새로 만들기를 클릭합니다.
3. 양식에서 필드를 채웁니다.

DLP 할당 규칙 양식

필드	설명
이름	할당 규칙의 이름입니다.
활성	할당 규칙이 활성 상태인지 여부를 나타내는 옵션입니다.
실행 순서	할당 규칙 우선순위입니다. 이 필드는 둘 이상의 규칙이 트리거 조건을 공유할 때 담당 규칙이 실행되는 순서를 나타냅니다. 가장 낮은 수의 할당 규칙이 가장 높은 우선순위를 갖습니다. 작업 순서를 설정하려면 값을 입력합니다. 예를 들어 100, 200, 300 등의 값을 입력합니다. 기본값은 100입니다.
설명	이 할당 규칙에 대한 고유한 설명입니다.
조건	조건 작성기의 조건입니다. 이러한 조건은 DLP 인시던트 테이블을 기반으로 합니다. 할당 규칙에 대한 조건을 작성하려면 인시던트 필드를 선택합니다. 조건 작성기의 목록과 필드를 사용하여 첫 번째 행에 대한 필터를 설정합니다. 조건을 더 추가하려면 **AND** 또는 **OR**을 클릭합니다. ○ **AND**를 선택하면 모든 조건이 일치해야 합니다. ○ **OR**을 선택하면 두 조건을 일치시킬 수 있습니다. 두 번째 필터 조건을 설정하려면 새 기준을 클릭합니다. 예를 들어 엔드포인트에 대한 DLP 할당 규칙을 생성한다고 가정합니다. 조건 검사 소스가 인시던트를 할당하기 전에 충족되어야

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	하는 엔드포인트 파일 시스템임을 지정할 수 있습니다. **주:** 조건 작성기의 조건은 대/소문자를 구분합니다.
담당자	다음 중 하나에 할당: ○ 사용자 그룹 ○ 최종 사용자 ○ 관리자 ○ 인시던트의 사용자 조건 작성기의 조건이 충족될 때 할당이 수행됩니다.
사용자 그룹	DLP 인시던트를 할당할 사용자 그룹을 검색하고 선택하는 옵션입니다. 이 필드는 할당 대상 필드에서 사용자 그룹을 선택할 때 나타납니다. **주:** sn_dlir.analyst 역할이 할당된 그룹만 보고 선택할 수 있습니다.
최종 사용자	최종 사용자에게 DLP 인시던트를 할당하는 옵션입니다. 조건 작성기의 조건이 충족될 때 할당이 수행됩니다.
관리자 필드를 사용하여 할당	최종 사용자의 관리자입니다. 이 필드는 담당자 필드에서 관리자를 선택한 경우에 나타납니다. 관리자 필드 중 하나(예: 성, 이메일, 도시, 직원 번호)를 선택하여 특정 관리자에게 DLP 인시던트를 할당할 수 있습니다.
사용자 식별자	인시던트의 사용자 식별자입니다. 이 필드는 할당 대상 필드에서 인시던트의 사용자를 선택할 때 나타납니다. 다음 중에서 사용자 식별자를 선택할 수 있습니다. ○ 데이터 소유자 이메일 ○ 대상 ○ 파일을 생성한 사람 ○ 파일을 수정한 사람 ○ 파일 소유자 ○ **FTP** 사용자 이름 ○ 보낸 사람 ○ 인시던트의 사용자 지정 사용자

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

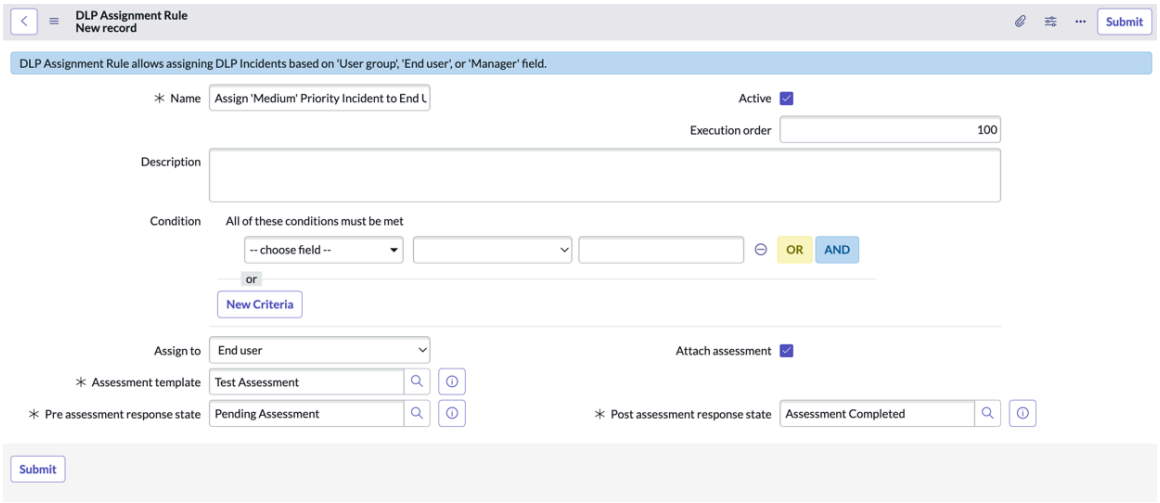
필드	설명
사용자 지정 속성	사용자에 대한 참조가 있는 인시던트에서 사용자 지정 속성을 지정하는 옵션입니다. 이 필드는 사용자 식별자 필드에서 인시던트의 사용자 지정 사용자를 선택한 경우에만 나타납니다.
평가 첨부	인시던트에 평가를 첨부할지 여부를 나타내는 옵션입니다.
사전 평가 응답 상태	최종 사용자가 응답하기 전에 인시던트가 있어야 하는 상태를 선택하는 옵션입니다. 사용자 지정 상태일 수도 있습니다. 기본값은 평가 보류 중입니다.
사후 평가 응답 상태	사용자가 응답한 후 DLP 인시던트가 있어야 하는 상태를 선택하는 옵션입니다. 기본값은 평가 완료됨입니다.
고급	최종 사용자를 식별하는 고급 옵션입니다. 이 필드는 사용자 식별자 필드에서 인시던트의 사용자 지정 사용자를 선택한 경우에만 나타납니다. 스크립트 편집기를 사용하면 할당 규칙을 생성하는 동안 최종 사용자를 식별하기 위해 필드 값을 사용자 지정하고 형식을 지정할 수 있습니다. 그런 다음 DLP 인시던트를 할당할 대상(최종 사용자 또는 최종 사용자의 관리자)을 선택합니다. 예를 들어 이메일 주소 필드를 사용하여 최종 사용자를 식별할 수 있습니다.

Example

다음 예에서는 '##' #### ##### ## ##### ##이라는 이름의 할당 규칙을 보여줍니다. 조건 작성기를 사용하려면 스캔 소스가 ## ##### "##" #### #### ##이어야 하며 ### 필드가 ## #### 설정되어 있어야 합니다. 그러면 최종 사용자의 '이메일'을 조회할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

DLP 할당 규칙



4. 모든 DLP 인시던트가 할당된 관련 목록 섹션에서 할당 대상 필드를 선택합니다.
편집을 클릭하여 사용자 그룹을 추가합니다. 관련 목록 섹션에서 편집을 클릭하고 컬렉션 열에서 항목을 선택한 다음 선택한 담당자를 구성원 편집 페이지의 그룹 열에 추가하고 목록을 저장합니다.

   주:
   관련 목록에서 sn_dlir.analyst 역할이 할당된 그룹만 보고 선택할 수 있습니다. 하나의 그룹만 선택할 수 있습니다.

5. 제출을 클릭합니다.
하나 이상의 할당 규칙을 선택하고 기존의 모든 DLP 인시던트에 다시 적용할 수도 있습니다.
6. 기존의 모든 DLP 인시던트에 할당 규칙을 다시 적용하려면 다시 적용을 클릭합니다.

인시던트 통합 규칙 생성

인시던트 통합 규칙을 생성하여 성격이 유사한 여러 인시던트를 하나의 상위 인시던트 아래에 통합합니다.

시작하기 전에
필요한 역할:

- sn_dlir.admin - 생성, 편집 및 삭제
- sn_dlir.analyst 및 sn_dlir.analyst_read - 보기(읽기 전용)

이 태스크 정보
DLP 관리자는 이러한 인시던트 통합 규칙을 정의하여 동일한 특성의 DLP 인시던트를 하나의 상위 인시던트 아래에 자동으로 통합합니다. DLP 인시던트 통합 규칙을 사용하면 통합 기간 및 통합 식별에 제공된 구성에 따라 DLP 인시던트를 통합할 수 있습니다.

주:

통합된 인시던트가 생성되면 상위 DLP 인시던트의 하위 인시던트가 됩니다. 통합된 인시던트의 심각도가 상위 인시던트의 심각도보다 높으면 상위 인시던트 심각도가 하위 인시던트와 일치하도록 업데이트됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 **DLP** 관리 〉 **DLP** 인시던트 통합 규칙.
2. 새로 만들기를 클릭합니다.
3. 양식에서 필드를 채웁니다.

DLP 할당 규칙 양식

필드	설명
이름	인시던트 통합 규칙의 이름입니다.
활성	인시던트 통합 규칙이 활성 상태인지 여부를 나타내는 옵션입니다.
실행 순서	인시던트 통합 규칙 우선순위입니다. 이 필드는 두 개 이상의 규칙이 트리거 조건을 공유할 때 인시던트 통합 규칙이 실행되는 순서를 나타냅니다. 가장 낮은 수의 인시던트 통합 규칙이 가장 높은 우선순위를 갖습니다. 작업 순서를 설정하려면 값을 입력합니다. 예를 들어 100, 200, 300 등의 값을 입력합니다. 기본값은 100입니다.
설명	인시던트 통합 규칙에 대한 고유한 설명입니다.
조건	조건 작성기의 조건입니다. 이러한 조건은 DLP 인시던트 테이블을 기반으로 합니다. 인시던트 통합 규칙에 대한 조건을 작성하려면 인시던트 필드를 선택합니다. 조건 작성기의 목록과 필드를 사용하여 첫 번째 행에 대한 필터를 설정합니다. 조건을 더 추가하려면 **AND** 또는 **OR**을 클릭합니다. ○ **AND**를 선택하면 모든 조건이 일치해야 합니다. ○ **OR**을 선택하면 두 조건을 일치시킬 수 있습니다. 두 번째 필터 조건을 설정하려면 새 기준을 클릭합니다. 예를 들어 조건을 통합 소스, 포함, **Symantec**으로 선택하여 이 인시던트 통합 규칙의 조건을 설정할 수 있습니다. 주: 조건 작성기의 조건은 대/소문자를 구분합니다.
통합 기간	인시던트 통합 기간을 설정하는 옵션입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	선택한 필드에 대해 동일한 값이 있는 이 기간의 인시던트는 첫 번째 인시던트 아래에 통합됩니다. 이 규칙과 일치하는 첫 번째 인시던트가 상위 인시던트가 되고 나머지 인시던트는 하위 인시던트가 됩니다.
인시던트 통합 기준	여러 인시던트에 대해 선택한 필드에 동일한 값이 있는 경우 DLP 인시던트 필드를 선택하여 인시던트를 통합합니다. 하나 이상의 필드를 선택합니다. 하나 이상의 필드를 선택합니다.

다음 예는 Symantec 통합을 위한 인시던트 통합이라는 이름의 인시던트 통합 규칙을 보여줍니다. 조건 작성기에는 통합 소스가 Symantec이어야 합니다. 조건 기간 옵션이 1시간으로 설정되고 인시던트 통합 기준에 대해 정책 이름 옵션이 선택됩니다.

Symantec DLP 인시던트 수집 시 이 규칙이 실행되며, 여러 인시던트의 정책 이름이 동일한 경우 이 규칙과 일치하는 첫 번째로 수집된 인시던트 아래에 인시던트가 통합됩니다.

4. 제출을 클릭합니다.
통합 규칙에 따라 통합된 인시던트는 DLP 분석가 작업 공간의 하위 인시던트 목록에서 사용할 수 있습니다.

응답 기한 날짜 규칙 생성

최종 사용자에게 할당 Data Loss Prevention Incident Response 된(DLP IR) 인시던트에 응답할 시간을 결정할 응답 기한 날짜 규칙을 설정합니다.

시작하기 전에
필요한 역할:

- sn_dlir.admin - 작성, 편집 및 삭제.
- sn_dlir.analyst 및 sn_dlir.analyst_read - 뷰(읽기 전용).

이 태스크 정보
이 모듈을 사용하여 다양한 유형의 DLP 인시던트에 대한 응답 기한 날짜 규칙과 기한 계산을 시작하는 규칙을 정의할 수 있습니다. 기한이 만료되면 사용자는 기한이 지난 인시던트에 대한 알림을 받습니다. 기한이 지난 인시던트를 다음 중 하나로 에스컬레이션하는 옵션도 제공됩니다.

- 관리자
- 인시던트의 사용자 지정 사용자
- 사용자 그룹

예를 들어 지연된 인시던트를 관리자에게 에스컬레이션하고 최대 3개의 에스컬레이션 수준을 지정한 경우입니다. 관리자의 첫 번째 수준이 먼저 알림을 받습니다. 인시던트 기한이 다시 지나면 관리자의 두 번째 수준에 알림이 전송되고, 인시던트가 아직 지연된 경우 세 번째 수준에 알림이 전송됩니다. 관리자에게 대리인이 있는 경우 관리자는 에스컬레이션 또는 지연된 인시던트를 대리인에게 할당할 수 있습니다.

또한 여러 응답 기한 규칙을 생성할 수 있는 기능도 제공됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 **DLP** 관리 〉 응답 기한 날짜 규칙.
2. 새로 만들기를 클릭합니다.
3. 양식에서 필드를 채웁니다.

응답 기한 날짜 규칙 양식

필드	설명
이름	응답 기한 날짜 규칙의 이름입니다.
활성	응답 기한 날짜 규칙이 활성 상태인지 여부를 나타내는 옵션입니다.
기한(일)	기한 수입니다.
기한 계산 출처	기한을 계산하는 데 사용되는 시작 날짜입니다. 기한은 사용자가 인시던트에 대해 처음 알림을 받았을 때 또는 인시던트 할당 날짜로부터 계산할 수 있습니다.
기한 전에 알림	기한 전에 DLP 인시던트에 대해 최종 사용자에게 알리는 옵션입니다.
다음에 알림(기한 전 날짜)	규칙이 최종 사용자에게 알림을 트리거하는 기한 전 일 수입니다.
설명	이 응답 기한 날짜 규칙에 대한 고유한 설명입니다.
조건	조건 작성기의 조건입니다. 이러한 조건은 DLP 인시던트 테이블을 기반으로 합니다. 응답 기한 날짜 규칙에 대한 조건을 작성하려면 인시던트 필드를 선택합니다. 조건 작성기의 목록과 필드를 사용하여 첫 번째 행에 대한 필터를 설정합니다. 조건을 더 추가하려면 **AND** 또는 **OR**을 클릭합니다. ○ **AND**를 선택하면 모든 조건이 일치해야 합니다. ○ **OR**을 선택하면 두 조건을 일치시킬 수 있습니다. 두 번째 필터 조건을 설정하려면 새 기준을 클릭합니다. 주: 조건 작성기의 조건은 대/소문자를 구분합니다.
에스컬레이션	응답 기한 날짜를 위반한 경우 DLP 인시던트를 다른 사람에게 에스컬레이션하는 옵션입니다. 자세한 내용은 DLP 인시던트에 액세스하기 위해 여러 사용자 추가 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

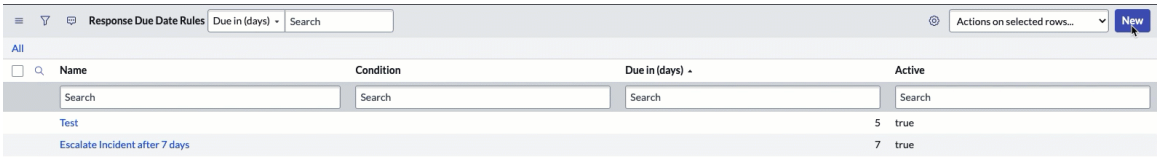
필드	설명
기한이 지난 인시던트를 다음으로 에스컬레이션	인시던트를 관리자, 사용자 지정 사용자 또는 사용자 그룹으로 에스컬레이션해야 하는지 지정하는 옵션입니다. 이 필드는 에스컬레이션 옵션이 활성화된 경우에만 나타납니다.
할당 사용	관리자 식별 방법을 지정합니다. 이 필드는 기한이 지난 인시던트를 다음으로 에스컬레이션 필드에서관리자를 선택한 경우에만 표시됩니다.
최대 에스컬레이션 수준	관리자와 사용자 지정 사용자에 대한 에스컬레이션 수준의 최대 수를 정의하는 옵션입니다. 관리자 또는 사용자 지정 사용자는 원하는 수만큼 에스컬레이션 수준을 정의할 수 있습니다. 기본적으로 세 가지 수준의 에스컬레이션이 제공됩니다. ○ 관리자는 이 필드의 값을 업데이트하여 원하는 만큼 에스컬레이션 수준을 정의할 수 있습니다. ○ 사용자 지정 사용자는 + 아이콘을 사용하여 원하는 수의 에스컬레이션 수준을 정의할 수 있습니다.
사용자 지정 속성	사용자에 대한 참조가 있는 인시던트에서 사용자 지정 속성을 지정하는 옵션입니다. 이 필드는 기한이 지난 인시던트를 다음으로 에스컬레이션 필드에서 인시던트의 사용자 지정 사용자를 선택한 경우에만 표시됩니다.
사용자 그룹	DLP 인시던트를 에스컬레이션할 사용자 그룹을 검색하고 선택하는 옵션입니다. 이 필드는 기한이 지난 인시던트를 다음으로 에스컬레이션 필드에서 사용자 그룹을 선택한 경우에만 표시됩니다. **주:** sn_dlir.analyst 역할이 할당된 그룹만 보고 선택할 수 있습니다.

Example

다음 예는 최종 사용자가 할당 Data Loss Prevention Incident Response 된(DLP) 인시던트에 응답할 시간을 결정하는 응답 기한 날짜 규칙을 보여줍니다. 최종 사용자에게 처음 알림을 받은 후 응답 기한은 2일입니다. 조건 작성기는 응답 기한 날짜 생성을 진행하려면 스캔 소스가 엔드포인트 파일 시스템과 일치해야 함을 보여줍니다. 에스컬레이션 옵션이 선택됩니다. 응답 기한 날짜를 위반하면 인시던트가 관리자에게 에스컬레이션됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

응답 기한 날짜 규칙 설정



4. 제출을 클릭합니다.

DLP 인시던트에 액세스하기 위해 여러 사용자 추가

에스컬레이션 체인 기능을 사용하면 인시던트가 다른 사용자에게 할당되어 있더라도 인시던트에 관련된 모든 사용자가 목록 뷰에서 DLP 인시던트에 액세스할 수 있습니다.

시작하기 전에

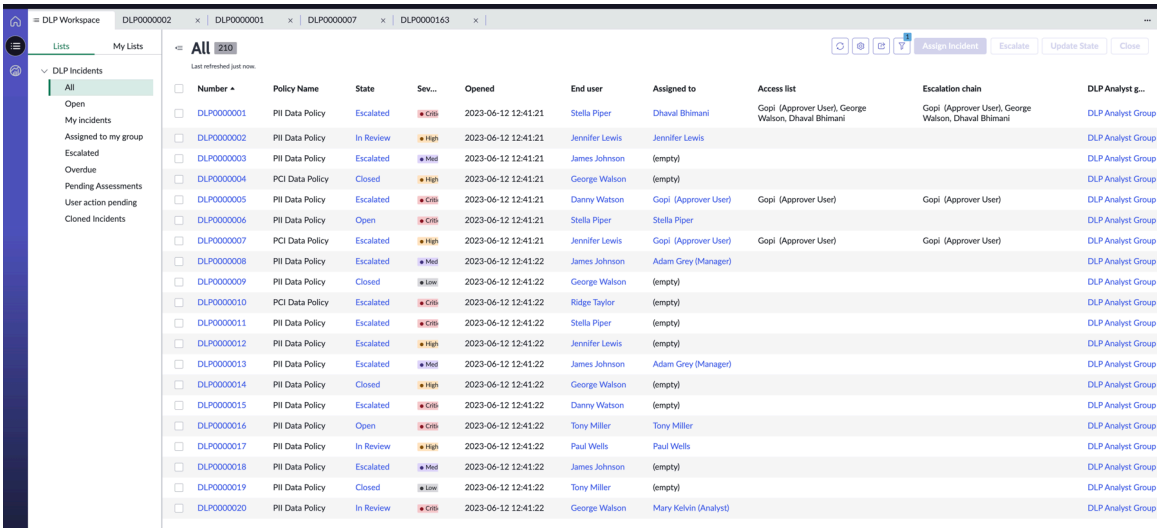
필요한 역할:

- sn_dlir.admin - 작성, 편집 및 삭제.
- sn_dlir.read, sn_dlir.analyst 및 sn_dlir.analyst_read - 뷰(읽기 전용).

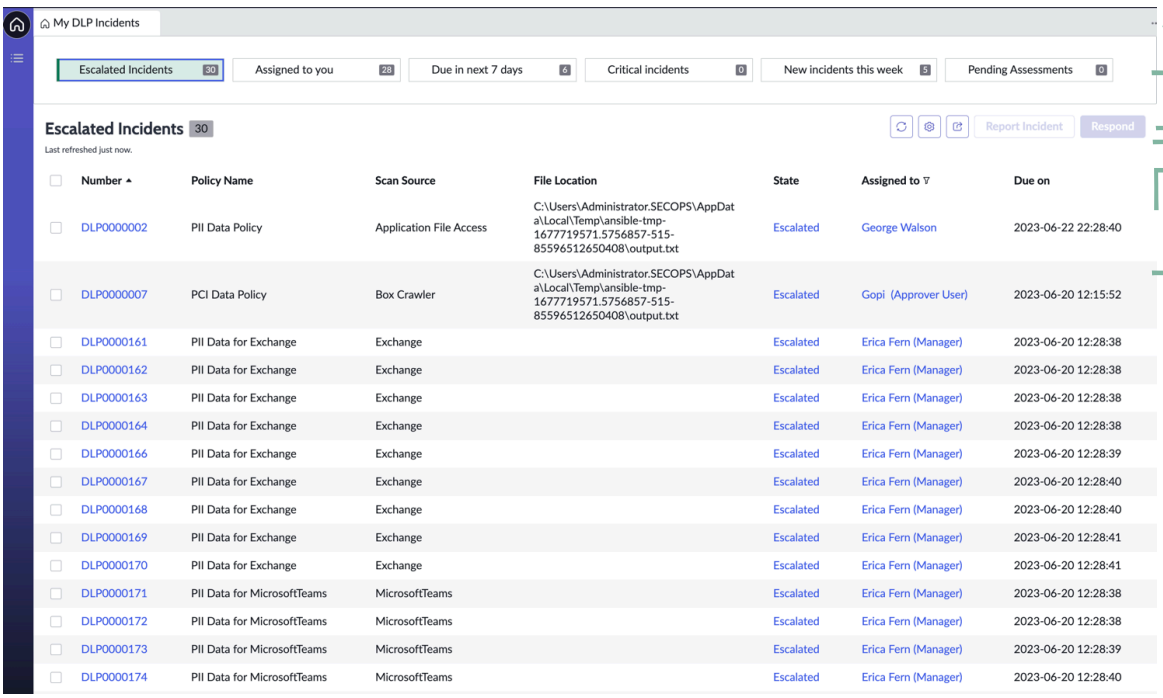
프로시저

1. 다음으로 이동 **DLP** 〉 **DLP** 분석가 작업 공간.
   목록 뷰에서 사용자와 해당 대리인은 최종 사용자 포털의 에스컬레이션된 인시던트 탭에서 DLP 인시던트를 볼 수 있어야 합니다.
2. 인시던트를 엽니다.
3. 인시던트를 에스컬레이션하려면 에스컬레이션 버튼을 클릭합니다.
4. 드롭다운 목록에서 사용자 또는 사용자 그룹을 선택합니다.
   에스컬레이션 체인에 여러 사용자를 추가할 수 있으며, 접근 권한이 있는 모든 사용자는 양식 뷰의 상세 정보 섹션과 모든 인시던트 탭 아래에 나열됩니다. 구성 설정에 따라 에스컬레이션 체인이 표시됩니다. 자세한 내용은 고급 설정 구성 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



5. 제출을 클릭합니다.
   제출하면 인시던트가 관리자에게 할당되지만 최종 사용자는 여전히 인시던트를 볼 수 있습니다.
6. 이를 확인하려면 최종 사용자로 **DLP** 사용자 작업 영역으로 이동합니다.
   최종 사용자에게 할당된 모든 인시던트가 표시됩니다.
7. 에스컬레이션된 인시던트 섹션에서 에스컬레이션된 인시던트 목록을 봅니다.



목록 뷰의 에스컬레이션 체인열에서 사용자 액세스 목록을 볼 수도 있습니다.

8. 인시던트를 엽니다.
9. 인시던트 응답을 제출하려면 응답 버튼을 클릭하십시오.
10. 드롭다운 목록에서 응답을 선택합니다.
11. 제출을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

승인 규칙 생성

고급 유형의 응답 옵션을 선택할 때마다 다양한 수준의 승인자 사용자로부터 승인을 받는 승인 규칙을 생성합니다.

시작하기 전에

필요한 역할:

- sn_dlir.admin - 작성, 편집 및 삭제.
- sn_dlir.analyst 및 sn_dlir.analyst_read - 뷰(읽기 전용).

이 태스크 정보

DLP 관리자는 이러한 승인 규칙을 정의하여 최종 사용자가 고급 유형의 응답 옵션을 승인하기 위해 제기한 요청에 대한 동의를 부여합니다. DLP 관리자는 여기에서 여러 수준의 승인을 정의할 수도 있습니다.

프로시저

1. 다음으로 이동 모두 〉 **DLP** 관리 〉 **DLP** 승인 규칙.
2. 새로 만들기를 클릭합니다.
3. 양식의 필드에 내용을 입력합니다.

DLP 할당 규칙 양식

필드	설명
이름	승인 규칙의 이름입니다.
활성	승인 규칙이 활성 상태인지 여부를 나타내는 옵션입니다.
실행 순서	승인 규칙 우선순위입니다. 이 필드는 둘 이상의 규칙이 트리거 조건을 공유할 때 승인 규칙이 실행되는 순서를 나타냅니다. 숫자가 가장 낮은 승인 규칙의 우선순위가 가장 높습니다. 작업 순서를 설정하려면 값을 입력합니다. 예를 들어 100, 200, 300 등의 값을 입력합니다. 기본값은 100입니다.
설명	승인 규칙에 대한 고유한 설명입니다.
조건	조건 작성기의 조건입니다. 이러한 조건은 DLP 인시던트 테이블을 기반으로 합니다. 승인 규칙에 대한 조건을 작성하려면 인시던트 필드를 선택합니다. 조건 작성기의 목록과 필드를 사용하여 첫 번째 행에 대한 필터를 설정합니다. 조건을 더 추가하려면 **AND** 또는 **OR**을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	○ **AND**를 선택하면 모든 조건이 일치해야 합니다. ○ **OR**을 선택하면 두 조건을 일치시킬 수 있습니다. 두 번째 필터 조건을 설정하려면 새 기준을 클릭합니다. 예를 들어 조건을 통합 소스, 포함, **Microsoft**로 선택하여 이 인시던트 통합 규칙의 조건을 설정할 수 있습니다.
응답 옵션에 적용 가능	고급 유형의 응답 옵션을 선택하는 옵션입니다. 복수 응답 옵션을 선택할 수 있습니다.
승인자	설정할 승인자 사용자 유형을 선택합니다. ○ 사용자 테이블: 사용자(sys_user) 테이블에서 승인자 사용자를 선택하려면 이 옵션을 선택합니다. ○ 사용자 지정 승인 목록: 단일 요청에 대해 여러 수준의 사용자 지정 승인자를 구성하려면 이 옵션을 선택합니다
승인자 식별자	이 필드는 승인자 옵션에 대해 사용자 테이블이 선택된 경우에 표시됩니다. 사용자(sys_user) 테이블에서 승인자의 식별자를 지정하는 필드를 선택합니다.
레벨 수	이 필드는 승인자 옵션에 대해 사용자 테이블이 선택된 경우에 표시됩니다. 승인 수준을 정의하는 이 필드의 종료 번호입니다. 예를 들어 수준 수 필드에 3이 추가되고 승인자 식별자 필드에 관리자가 선택된 경우 승인 요청은 세 가지 승인 수준으로 이동합니다.

다음 예는 고급 응답 옵션 중 하나에 대해 생성된 승인 규칙을 보여줍니다. 조건에는 이 구성을 트리거하는 Microsoft 키워드가 포함된 통합 소스 이름이 필요합니다.

4. 승인자 옵션으로 사용자 지정 승인 목록을 선택합니다.
5. 제출을 클릭합니다.
6. 승인 수준 관련 목록이 양식 뷰에 채워집니다.
7. 승인 수준 섹션에서 새로 만들기를 클릭합니다.
8. 양식에서 필드를 채웁니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

승인 수준 양식

필드	설명
이름	승인 수준에 대한 이름입니다.
활성	승인 수준이 활성 상태인지 여부를 나타내는 옵션입니다.
수준	승인 규칙의 수준입니다. 이 필드는 둘 이상의 수준이 구성된 경우 승인 수준이 실행되는 순서를 나타냅니다. 가장 낮은 숫자의 승인 수준이 가장 높은 우선순위를 갖습니다. 작업 수준을 설정하려면 값을 입력합니다. 예를 들어 100, 200, 300 등의 값을 입력합니다. 기본값은 100입니다.
승인 규칙	이 구성을 정의할 승인 규칙입니다. 이 필드는 읽기 전용이 됩니다.
설명	승인 규칙에 대한 고유한 설명입니다.
승인 필요	구성된 모든 사용자/그룹의 승인이 필요한지 또는 한 사용자에게만 승인이 필요한지 정의하는 옵션을 선택합니다.
승인자	승인자를 선택하는 옵션입니다. **a.** 사용자 및 그룹: **i.** 사용자: 목록에서 특정 사용자를 추가하려면 아이콘을 클릭합니다. 이메일 주소나 검색 옵션을 사용하여 사용자를 추가할 수도 있습니다. DLP 조건을 적용할 수 있는 사용자로 자신을 추가하려면 을 클릭합니다. **ii.** 그룹: 목록에서 특정 그룹을 추가하려면 <add_icon> 아이콘을 클릭합니다. 검색 옵션을 사용하여 그룹을 추가할 수도 있습니다. **b.** 스크립트를 사용하여 찾기: 스크립트 편집기를 사용하여 승인 수준을 생성하는 동안 필드 값을 사용자 지정하고 서식을 지정할 수 있습니다. 예를 들어 이메일 주소 필드를 사용하여 승인자 사용자를 식별할 수 있습니다.

9. 제출을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용자 지침 템플릿 생성

DLP 인시던트에 대한 사용자 지침 템플릿을 만들고 관리하여 사용자가 인시던트 해결과 관련된 지침 및 해결 프로세스와 관련된 다음 단계를 이해하는 데 도움을 줍니다.

시작하기 전에

사용자 지침 카드 템플릿에는 양식 뷰의 특정 인시던트에 대한 자세한 정보를 제공하는 두 개의 서로 다른 헤더가 표시됩니다.

필요한 역할:

- sn_dlir.admin - 작성, 편집 및 삭제.
- sn_dlir.analyst 및 sn_dlir.analyst_read - 뷰(읽기 전용).

이 태스크 정보

인시던트가 최종 사용자에게 할당되면 사용자는 인시던트에 대응하는 방법에 대한 추가 지침을 알고 사용자에게 용어를 소개하고 인시던트에 대한 추가 정보를 제공해야 할 수 있습니다. 이러한 템플릿은 사용자가 DLP 인시던트에 정확한 응답을 제공하도록 안내할 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 **DLP** 관리 〉 사용자 지침 템플릿.
2. 새로 만들기를 클릭합니다.
3. 양식에서 필드를 채웁니다.

DLP 인시던트 평가

필드	설명
이름	사용자 지침 템플릿의 이름입니다.
간단한 설명	이 사용자 지침 템플릿의 고유한 설명입니다.
활성	사용자 지침 템플릿이 활성 상태인지 여부를 나타내는 옵션입니다.
실행 순서	인시던트 사용자 지침 템플릿의 우선순위입니다. 이 필드는 인시던트가 생성될 때 사용자 지침 템플릿을 평가하기 위해 순서가 실행되는 순서를 나타냅니다. 숫자가 가장 낮은 옵션의 우선순위가 가장 높습니다. 작업 순서를 설정하려면 값을 입력합니다. 예를 들어 100, 200 또는 기타 숫자입니다. 기본값은 100입니다.
일치하는 인시던트 조건	조건 작성기에 정의된 조건과 일치하는 인시던트가 표시됩니다. 이러한 조건은 DLP 인시던트 데이터를 기반으로 합니다. 사용자 지침에 대한 조건을 작성하려면 인시던트 필드를 선택합니다. 조건 작성기의 목록과 필드를 사용하여 첫 번째 행에 대한 필터를 설정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	조건을 더 추가하려면 AND 또는 OR을 클릭합니다. AND를 선택하면 모든 조건이 일치해야 합니다. OR을 선택하면 두 조건을 일치시킬 수 있습니다. 두 번째 필터 조건을 설정하려면 새 기준을 클릭합니다. 주: 조건 작성기의 조건은 대/소문자를 구분합니다.
적용 대상	템플릿을 적용할 수 있는 사용자 또는 사용자 그룹을 선택합니다. 사용 가능한 다른 옵션은 다음과 같습니다. ○ 모든 최종 사용자: 지침 템플릿이 모든 사용자에게 적용되는 경우 이 확인란을 선택합니다. ○ 에스컬레이션된 인시던트의 모든 검토자: 템플릿이 에스컬레이션된 인시던트의 모든 검토자에게 적용되는 경우 이 확인란을 선택합니다. ○ 특정 사용자: DLP 인시던트 조건을 적용할 수 있는 특정 사용자를 목록에서 추가하려면 아이콘을 클릭합니다. 이메일 주소나 검색 옵션을 사용하여 사용자를 추가할 수도 있습니다. 예: 법무 관리자 DLP 조건을 적용할 수 있는 사용자로 자신을 추가하려면 본인 추가 아이콘을 클릭합니다. ○ 특정 사용자 그룹: DLP 인시던트 조건을 적용할 수 있는 특정 그룹을 목록에서 추가하려면 아이콘을 클릭합니다. 검색 옵션을 사용하여 그룹을 추가할 수도 있습니다. 예를 들어 설문 조사 작성자입니다.
지침 템플릿: 지침	인시던트 수준에서 사용할 수 있는 변수를 사용하여 서식 있는 텍스트 편집기에 지침을 추가합니다.

4. 지침 템플릿 섹션으로 드릴다운하고 템플릿 지침을 입력한 후 필요한 경우 이 섹션 아래에 인시던트 수준 정보를 추가합니다.
5. 특정 필드를 동적으로 표시하는 데 필요한 변수를 끌어서 놓습니다.
6. 제출을 클릭합니다.
   이제 사용자 지침 템플릿이 생성되었으며 사용자 지침 헤더를 클릭하여 DLP 인시던트의 추가 세부 정보를 확인할 수 있습니다.

   자세한 내용은 Data Loss Prevention Incident Response 사용자 작업 공간 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

DLP UI 사용자 지침 구성

필요에 따라 자세한 사용자 지침 헤더를 추가하도록 시스템 UI 메시지를 구성합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 〉 시스템 **UI** 〉 메시지.
2. **user_instruction_card_heading** 검색합니다.

   기본적으로 user_instruction_card_heading 및 user_instruction_modal_window_heading 는 사용자에게 프로비저닝된 두 가지 UI 메시지 구성입니다.
3. 업데이트하거나 수정할 사용자 지침을 클릭합니다.

이메일 템플릿 만들기

최종 사용자, 사용자 그룹 또는 관리자에게 알림을 보내기 위해 미리 구성된 이메일 템플릿을 만들고 관리합니다. 이러한 템플릿을 사용하면 (DLP IR) 인시던트에 대해 최종 사용자를 코칭하고 이에 대해 소통할 Data Loss Prevention Incident Response 수 있습니다.

시작하기 전에
필요한 역할:

- sn_dlir.admin - 작성, 편집 및 삭제.
- sn_dlir.analyst 및 sn_dlir.analyst_read - 뷰(읽기 전용).

> **중요사항:**
> 분석가가 활동 스트림에서 DLP 인시던트의 이메일 커뮤니케이션을 볼 수 있도록 하려면 전역 시스템 속성 glide.ui.activity.email_roles에 "sn_dlir.analyst" 역할을 추가하거나 추가해야 합니다.

이 태스크 정보
이메일 알림은 최종 사용자에게 전송되는 인시던트 알림, 관리자에게 전송되는 에스컬레이션 알림 또는 기한 알림으로 분류됩니다. DLP 인시던트의 기한에 대한 이메일 알림을 보내거나 이메일 조건 필터에서 특정 조건이 충족될 때 수행할 작업에 대해 최종 사용자를 코칭할 수도 있습니다. DLP 이메일 템플릿을 사용하면 최종 사용자, 관리자 및 분석가를 위한 이메일 알림을 보낼 수 있습니다. 인시던트별로 또는 다이제스트로 보낼 템플릿을 구성할 수 있습니다. 이메일 제목과 본문에는 기존 콘텐츠를 다시 사용할 수 있도록 변수가 포함될 수 있습니다.

DLP는 범주에 따라 다음과 같이 미리 구성된 전자 메일 템플릿을 제공합니다.

- **DLP** 이메일 템플릿 **-** 인시던트별 승인 알림: 사용자에게 요청 승인에 대해 알립니다.
- **DLP** 이메일 템플릿 **-** 에스컬레이션 알림: 다이제스트 형태로 관리자에게 에스컬레이션 알림을 보냅니다.
- **DLP** 이메일 템플릿 **-** 보류 중인 승인 알림: 보류 중인 항목에 대해 승인자에게 알립니다.
- **DLP** 이메일 템플릿 **-** 인시던트별 승인 요청 취소 알림:DLP 분석가 팀이 취소한 승인 요청에 대해 사용자에게 알립니다.
- **DLP** 이메일 템플릿 **-** 사용자 응답 완료 알림: 사용자가 제출한 응답에 대해 DLP 분석가 팀에 알립니다.
- **DLP** 이메일 템플릿 **-** 사용자 인시던트 알림:사용자 다이제스트 알림의 기본 템플릿입니다. 새 인시던트가 없는 경우에도 며칠마다 최종 사용자에게 다이제스트 형식으로 인시던트 알림을 보내 특정 사용자의 이름에 대한 총 인시던트 수를 사용자에게 알립니다. 또한 다이제스트 알림을

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

전송하여 심각도가 중요, 높음, 중간 또는 낮음인 DLP 인시던트의 가장 가까운 기한에 대해 사용자에게 알릴 수 있습니다.

- **DLP** 이메일 템플릿 **-** 인시던트당 승인 보류 중 알림: 승인자에게 보류 중인 승인에 대해 알립니다.
- **DLP** 이메일 템플릿 **-** 거부 알림: 요청자에게 거부 알림을 보냅니다.
- **DLP** 이메일 템플릿 **-** 기한 알림: 인시던트 기한 알림을 보냅니다. DLP 인시던트가 최종 사용자에게 할당되고 최종 사용자가 기한 전까지 아무 조치도 취하지 않은 경우 최종 사용자에게 이메일 알림이 전송됩니다. 응답 기한을 위반한 경우 DLP 인시던트를 관리자, 사용자 지정 사용자 또는 사용자 그룹으로 에스컬레이션할 수 있는 옵션도 있습니다.

  주:
  기한 알림은 다이제스트 형식이어야 합니다.

- **DLP** 이메일 템플릿 **-** 인시던트당 사용자 응답 알림: 인시던트당 사용자에게 제출된 응답에 대해 분석가에게 알립니다.
- **DLP** 이메일 템플릿 **-** 인시던트별 에스컬레이션 알림: 관리자에게 인시던트별 에스컬레이션에 대해 알립니다.
- **DLP** 이메일 템플릿 **-** 인시던트당 사용자 알림: 사용자에게 인시던트별 할당에 대해 알립니다.

프로시저

1. 다음으로 이동 모두 〉 **DLP** 관리 〉 이메일 템플릿.
2. 새로 만들기를 클릭합니다.
3. 양식에서 필드를 채웁니다.

DLP 이메일 템플릿 양식

필드	설명
이름	이메일 템플릿의 이름입니다.
활성	DLP 이메일 템플릿이 활성 상태인지 여부를 나타내는 옵션입니다. 이 옵션을 사용하지 않으면 이 이메일 템플릿에 대한 알림이 전송되지 않습니다.
범주	이메일 알림 범주입니다. DLP는 다음 옵션을 지원합니다. ○ 최종 사용자에게 인시던트 알림: 인시던트가 최종 사용자에게 할당될 때 전송됩니다. ○ 관리자에게 에스컬레이션 알림: 응답 기한을 위반하거나 DLP 운영 포털을 통해 관리자에게 수동으로 할당된 경우에 전송됩니다. ○ 기한 알림: 응답 기한이 위반된 경우에 전송됩니다. ○ 분석가에게 사용자 응답 알림: 최종 사용자가 DLP 인시던트에 대해 조치를 취할 때 전송됩니다. ○ 보류 중인 승인 알림: 보류 중인 항목에 대해 승인자에게 알립니다. ○ 요청자에게 승인 알림: 사용자에게 요청 승인에 대해 알립니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	○ 요청자에게 알림 거부: 사용자에게 요청 거부에 대해 알립니다. ○ 요청자에게 알림 취소: 사용자에게 요청 취소에 대해 알립니다.
유형	이메일을 인시던트별로 전송할지 또는 다이제스트로 전송할지를 나타내는 옵션입니다. 주: 범주 필드에서 기한 알림을 선택한 경우 다이제스트만 사용할 수 있습니다. 이 옵션을 선택합니다.
설명	이 이메일 템플릿에 대한 고유한 설명입니다.
실행 순서	이메일 템플릿 우선순위입니다. 이 필드는 둘 이상의 이메일 템플릿이 트리거 조건을 공유할 때 이메일 템플릿이 실행되는 순서를 나타냅니다. 가장 낮은 수의 이메일 템플릿이 가장 높은 우선순위를 갖습니다. 작업 순서를 설정하려면 값을 입력합니다. 예를 들어 100, 200 또는 기타 숫자입니다. 기본값은 100입니다.
템플릿 조건	DLP 인시던트 테이블을 기반으로 하는 템플릿 조건의 옵션입니다. 이메일 템플릿 트리거 조건을 빌드하기 위한 인시던트 필드를 선택할 수 있습니다. 조건 작성기의 목록과 필드를 사용하여 첫 번째 행에 대한 필터를 설정합니다. 조건을 더 추가하려면 **AND** 또는 **OR**을 클릭합니다. ○ **AND**를 선택하면 모든 조건이 일치해야 합니다. ○ **OR**을 선택하면 두 조건을 일치시킬 수 있습니다. 두 번째 필터 조건을 설정하려면 새 기준을 클릭합니다. 주: 조건 작성기의 조건은 대/소문자를 구분합니다.
대상 사용자	조건이 충족될 때 템플릿의 대상 사용자입니다. 대상 사용자는 다음 중 하나일 수 있습니다. ○ 모든 수신자: 대상 사용자에게 이메일을 보냅니다. ○ 그룹의 수신자: 필터 옵션을 사용하여 특정 그룹 내의 수신자에게만 이메일을 보냅니다. ○ 기준과 일치하는 수신자: 기준과 일치하는 대상 사용자에게 이메일을 보냅니다. 필터를 사용하여 조건에 따라 대상 사용자를 드릴다운할 수 있습니다. 예를 들어 city입니다.
이메일 템플릿	선택할 수 있는 이메일 템플릿입니다. 기존 컨텐츠를 재사용하여 이메일 알림에 추가할 변수를 정의할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명

	범주 및 유형 필드에 따라 선택할 수 있는 변수가 결정됩니다. 예를 들어 이메일 범주가 인시던트 알림으로 설정되고 이메일 유형이 다이제스트인 경우, 여러 DLP 인시던트의 누적을 수용하기 위한 다이제스트 필드는 선택 변수라고 가정해 보겠습니다.
	
	다음은 각 이메일 템플릿의 이메일 본문 HTML 예입니다.
	○ 인시던트별 승인 알림의 기본 템플릿:
	`Dear ${respondent.first_name},`
	
	`Your request "${end_user_response}" on the incident ${number} has been approved.`
	
	`- Date protection team`
	○ 인시던트 승인 요청별 취소 알림
	`Dear ${respondent.first_name},`
	
	`Your request "${end_user_response}" on the DLP incident ${number} has been cancelled.`
	
	`No action is required from you at this point. Data protection team will contact you for any further information required.`
	
	`- Data protection team`
	○ 기한 알림의 기본 템플릿:
	`Dear ${target_user.name},`
	
	`Following incidents require your response.`
	
	`${due_days_table}`
	
	`- Data protection team`
	○ 인시던트별 사용자 알림의 기본 템플릿:
	`Dear ${assigned_to.name},`
	
	`DLP Incident ${number} is assigned to you.`
	
	`Please review and submit your response.`
	
	`- Data protection team`
	○ 사용자 인시던트 알림의 기본 템플릿:
	`Hello ${target_user.name},`
	
	`You have ${total_number_of_incidents} incidents assigned to you currently that require your response.`

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	${new_incidents_in_period} new incidents got assigned to you since the last email communication. Nearest upcoming due date for responding to a critical incident is ${nearest_due_date_for_critical_severity_incidents}. Please log in to the ${link_to_dlp_portal} and submit your response. - Data protection team ○ 에스컬레이션 - 다이제스트에 대한 기본 템플릿: Hi ${target_user.name}, The following data security incidents have been escalated to you due to lack of response from the assignees. Please login to the incident response workspace to review the incidents and submit your response. ${overdue_table} - Data protection team ○ 에스컬레이션 기본 템플릿 - 인시던트당: Dear ${assigned_to.name}, Data security incident ${number} has been escalated to you. Please review and submit your response or assign the incident back to the user. - Data protection team ○ 보류 중인 승인 알림의 기본 템플릿: Dear ${approver.first_name}, Your approval is required for a few requests on data security incidents. Please login to the workspace here and review the requests. - Data protection team ○ 승인 알림이 보류 중인 인시던트별 기본 템플릿: Dear ${Approver},

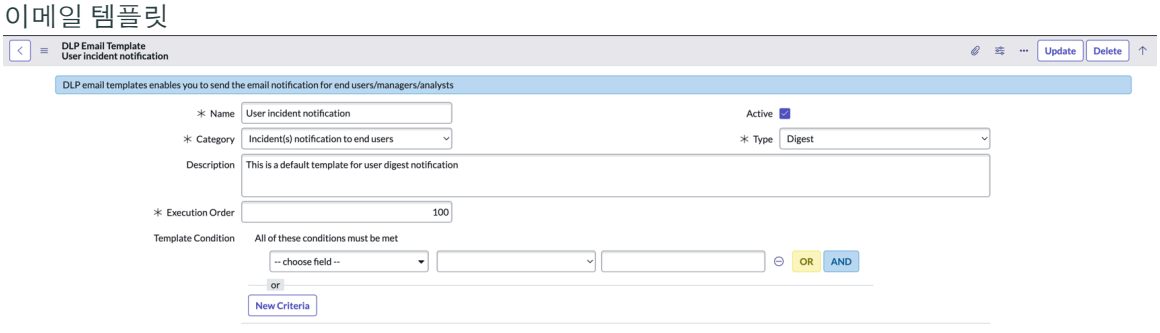
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	Your approval is required for the incident ${number} requested by the user ${respondent.first_name} ${respondent.last_name}. Please visit this here to approve or reject the request. - Data Protection Team ○ 인시던트별 거부 알림의 기본 템플릿: Dear ${respondent.first_name} ${respondent.last_name}, This is to inform you that your request "${end_user_response}" for the DLP incident ${number} has been rejected. Please review the incident here. - Data protection team ○ 인시던트당 사용자 응답 알림의 기본 템플릿: Hi ${assigned_to.name}, This is to inform you that a response has been submitted for the DLP Incident ${number}. ○ 사용자 응답 완료 알림의 기본 템플릿: Hello ${target_user.name}, This email is to inform you that users have submitted their response for ${new_incidents_in_period_user_response_completed} new incidents since the last email communication. Please review the response for these incidents ${link_to_incidents_in_period_user_response_completed}.

Example

다음 예제에서는 대상 사용자가 모든 받는 사람으로 정의된 DLP 전자 메일 템플릿을 보여 줍니다.

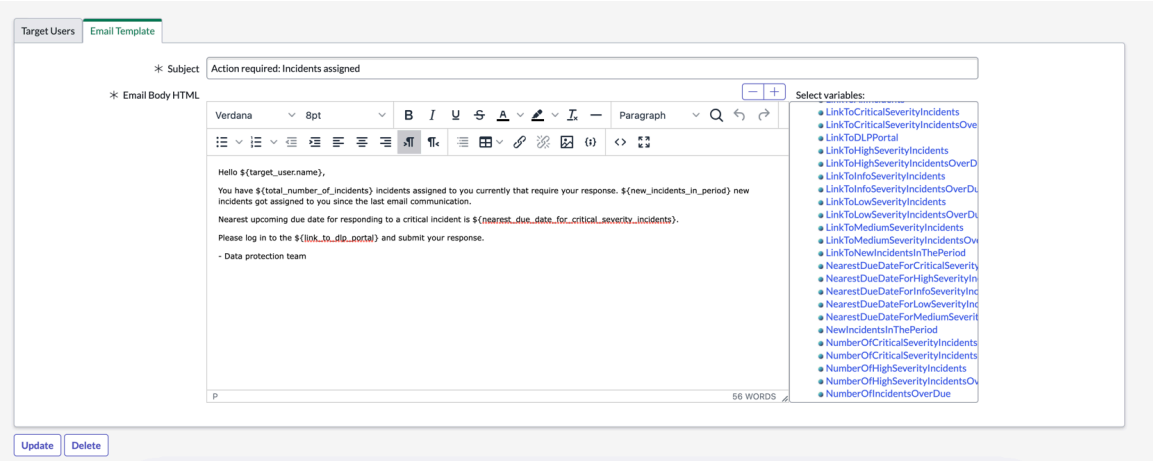
이메일 템플릿



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음 예는 "사용자 인시던트 알림"이라는 제목과 변수 *new_incidents_in_period*이 있는 이메일 템플릿을 보여줍니다. 이메일 본문에는 변수 선택 열에서 추가되는 여러 변수가 포함되어 있습니다.

이메일 템플릿 변수



4. 제출을 클릭합니다.

결과
최종 사용자는 템플릿에서 선택한 모든 변수 필드가 포함된 다이제스트 알림 이메일을 받습니다.

Data Loss Prevention Incident Response SLA 트리거 생성

Data Loss Prevention Incident Response 트리거될 때 인시던트에 신속하고 효율적인 응답을 가능하게 하는 SLA 트리거 조건을 생성합니다.

시작하기 전에
필요한 역할:

- sn_dlir.admin - DLP SLA 트리거 만들기, 업데이트 및 삭제
- sn_dlir.analyst.read - 트리거 테이블을 읽습니다.

프로시저

1. 다음으로 이동 모두 〉 **DLP** 관리 〉 **SLA** 트리거.
2. 새로 만들기를 선택하여 SLA 트리거를 만듭니다.

필드	설명
이름	트리거의 이름
순서	트리거가 고려되는 순서입니다.
활성	SLA 트리거를 평가하는 옵션입니다.
DLP 인시던트가 업데이트될 때 트리거	DLP 인시던트의 각 업데이트에서 트리거 조건을 평가하는 옵션입니다.

3. 규칙 기록을 선택하고 트리거 조건 필드에서 조건을 정의하여 조건을 구성합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예를 들어 이메일 스캔 소스에서 DLP 인시던트에 SLA를 설정하는 트리거 조건은 **[Scan Source] [is][Email SMTP]**일 것입니다.

4. 제출을 선택합니다.

결과
인시던트에 대한 Data Loss Prevention Incident Response 작업 SLA 기록이 생성되면 작업 공간에서 해당 특정 인시던트에 대한 SLA 기록 탭이 표시됩니다. 이 탭을 사용하면 조직의 작업에 SLA 시스템을 사용할 수 있습니다.

Data Loss Prevention Incident Response SLA 정의 생성

Data Loss Prevention Incident Response 데이터 위반에 대응하기 위한 조건 및 기간을 개략적으로 설명하는 SLA 정의를 생성합니다. 명확한 기대치와 프로토콜을 설정하면 사고에 신속하게 대응하여 잠재적 피해를 최소화하고 전반적인 데이터 보호 전략을 강화하는 데 도움이 됩니다.

시작하기 전에
필요한 역할:

- sn_dlir.admin - DLP SLA 정의를 생성, 업데이트 및 삭제합니다.
- sn_dlir.analyst.read - DLP SLA 정의를 읽습니다.

프로시저

1. 다음으로 이동 모두 〉 **DLP** 관리 〉 **SLA** 정의.
2. SLA 정의를 생성합니다.
   필드 값에 대한 설명은 DLP SLA 정의 양식 문서를 참조하십시오.
3. 제출을 선택합니다.

> **주:**
> 기한 규칙, 에스컬레이션 및 SLA 정의는 함께 사용할 수 없습니다. SLA 정의는 주로 특정 SLA가 발효, 중지, 일시 중지 또는 트리거되기 시작하는 시기를 결정합니다.

평가 생성

최종 사용자가 DLP 인시던트에 대응할 수 있도록 평가를 생성하고 관리합니다. 평가를 사용하여 DLP 인시던트에서 노출되거나 유출된 중요한 데이터에 대한 정보를 수집할 수 있습니다.

DLP 인시던트에 대한 평가 생성 및 관리

시작하기 전에
필요한 역할:

- sn_dlir.admin - 작성, 편집 및 삭제.
- sn_dlir.analyst 및 sn_dlir.analyst_read - 뷰(읽기 전용).

이 태스크 정보
DLP 인시던트 평가는 최종 사용자 응답을 기반으로 데이터에 대한 잠재적 위협 및 취약성을 식별하는 데 도움이 됩니다. 이 정보를 사용하여 최종 사용자의 기존 격차, 우려 사항 및 기대치를 확인할 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 **DLP** 관리 〉 평가.
2. 새로 만들기를 클릭합니다.
3. 양식에서 필드를 채웁니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

DLP 인시던트 평가

필드	설명
이름	DLP 인시던트 평가의 이름입니다.
활성	DLP 인시던트 평가가 활성 상태인지 여부를 나타내는 옵션입니다.
설명	이 DLP 인시던트 평가에 대한 고유 설명입니다.
평가 소개	평가에 대한 소개 또는 컨텍스트를 제공합니다. 변수 선택 섹션의 변수를 사용하여 특정 필드를 동적으로 표시할 수도 있습니다.

4. 제출을 클릭합니다.
5. 평가를 생성한 후 평가를 열고 평가 디자이너를 클릭합니다.
6. 새 평가 섹션의 통제 섹션에서 평가 질문 유형을 선택합니다.
7. 새 평가 섹션 아래에 필요한 평가 질문 유형을 끌어서 놓습니다.
   예를 들어 새 평가 또는 새 범주 섹션에서 선택 컨트롤을 끌어서 놓을 수 있습니다.
8. 평가에 대한 범주를 더 추가하려면 아이콘을 클릭합니다.
9. 기존 범주를 수정하려면 아이콘을 클릭합니다.
10. 다른 평가 질문을 처음 생성한 후 저장을 클릭한 다음 게시를 클릭합니다.

인시던트 응답 옵션 규칙 생성

최종 사용자 또는 분석가가 인시던트에 응답하는 동안 사용할 수 있는 인시던트 응답 옵션 규칙을 만듭니다.

시작하기 전에

필요한 역할:

- sn_dlir.admin - 작성, 편집 및 삭제.
- sn_dlir.analyst 및 sn_dlir.analyst_read - 뷰(읽기 전용).

이 태스크 정보

DLP 인시던트 유형에 따라 최종 사용자가 수행해야 하는 응답 유형을 구성할 수 있습니다. 기본 시스템 DLP 인시던트 응답 애플리케이션은 사용자에게 다음과 같은 응답 옵션을 제공합니다.

- 평가 완료
- 삭제된 컨텐츠
- 삭제된 파일
- 암호화된 파일
- 마스킹된 콘텐츠
- 오탐지 보고
- 잘못된 소유자 보고
- 비즈니스 프로세스에 필요
- 검토된 권리

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예를 들어 최종 사용자가 DLP 인시던트를 가양성으로 보고한다고 가정해 보겠습니다. 사용자가 구성한 대상 상태가 종결이므로 이 인시던트의 상태가 자동으로 종결됨으로 표시됩니다.

프로시저

1. 다음으로 이동 모두 〉 **DLP** 관리 〉 인시던트 응답 옵션 규칙.
2. 새로 만들기를 클릭합니다.
3. 양식에서 필드를 채웁니다.

인시던트 응답 옵션 규칙 양식

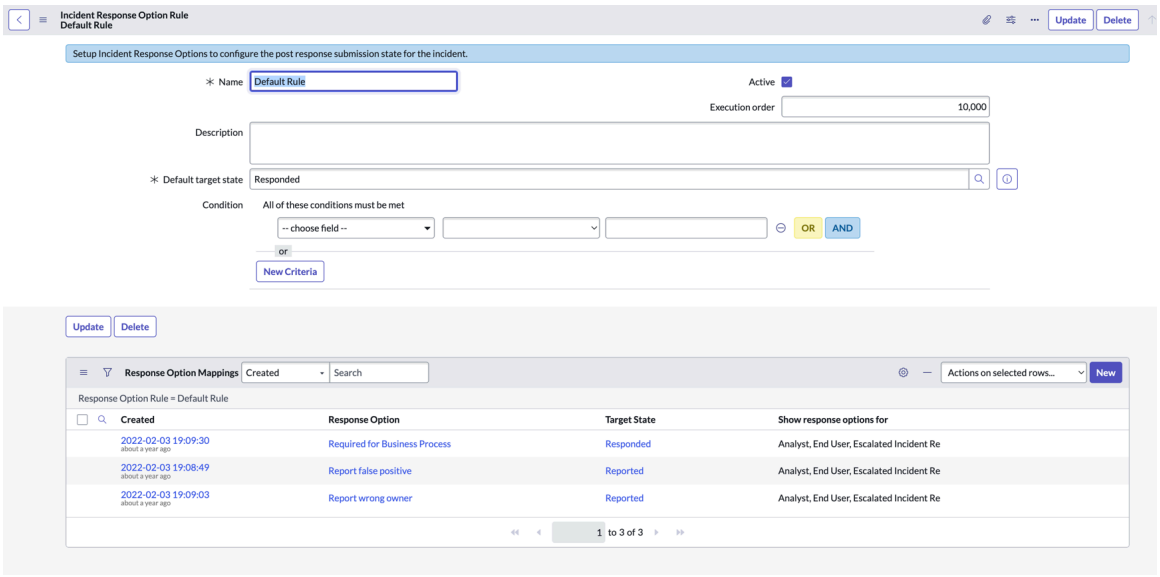
필드	설명
이름	인시던트 응답 옵션의 이름입니다.
활성	인시던트 응답 옵션이 활성 상태인지 여부를 나타내는 옵션입니다.
실행 순서	인시던트 응답 옵션의 우선순위입니다. 이 필드는 둘 이상의 인시던트 응답 옵션이 트리거 조건을 공유하는 경우 인시던트 응답 옵션이 실행되는 순서를 나타냅니다. 가장 낮은 수의 인시던트 응답 옵션이 가장 높은 우선순위를 갖습니다. 작업 순서를 설정하려면 값을 입력합니다. 예를 들어 100, 200 또는 기타 숫자입니다. 기본값은 100입니다.
설명	이 인시던트 응답 옵션에 대한 고유한 설명입니다.
기본 대상 상태	구성한 기본 대상 상태입니다.
조건	조건 작성기의 조건입니다. 이러한 조건은 DLP 인시던트 테이블을 기반으로 합니다. 인시던트 응답 옵션에 대한 조건을 작성하려면 인시던트 필드를 선택합니다. 조건 작성기의 목록과 필드를 사용하여 첫 번째 행에 대한 필터를 설정합니다. 조건을 더 추가하려면 **AND** 또는 **OR**을 클릭합니다. ○ **AND**를 선택하면 모든 조건이 일치해야 합니다. ○ **OR**을 선택하면 두 조건을 일치시킬 수 있습니다. 두 번째 필터 조건을 설정하려면 새 기준을 클릭합니다. 주: 조건 작성기의 조건은 대/소문자를 구분합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Example

다음 예는 엔드포인트에 대한 최종 사용자 작업 구성을 보여줍니다. 이 조건에 따라 스캔 소스가 이 최종 사용자 작업 구성을 트리거하는 엔드포인트 파일 시스템이어야 합니다. 매핑은 보고서 잘못된 소유자, 보고서 가양성 및 삭제된 파일이 최종 사용자가 사용할 수 있는 응답 옵션임을 보여줍니다.

인시던트 응답 옵션 규칙



4. 응답 옵션 매핑 섹션에서 새로 만들기를 클릭합니다.
5. 양식에서 필드를 채웁니다.

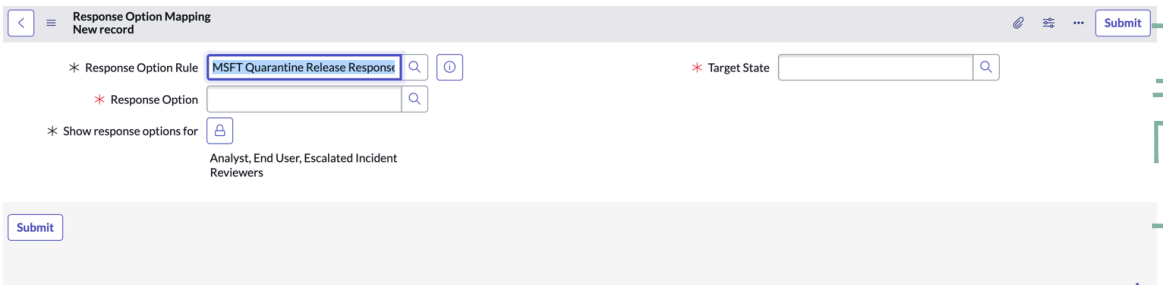
응답 옵션 매핑 양식

응답 옵션 규칙	인시던트 응답 옵션 규칙의 이름입니다. 예를 들어 SharePoint 는 스캔 소스가 SharePoint임을 암시합니다. 인시던트 응답의 이름을 입력하거나 검색을 사용하여 조회할 수 있습니다.
응답 옵션	응답 옵션을 선택하는 옵션입니다. 응답 옵션을 입력하거나 검색을 사용하여 조회할 수 있습니다.
대상 상태	최종 사용자가 적절한 작업을 선택한 후 DLP 인시던트의 대상 상태입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

	주: **a.** 대상 상태 필드는 유형: 기본의 응답 옵션을 선택한 경우에만 표시됩니다. 대상 상태 유형을 구성하는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 DLP 인시던트에 대한 응답 옵션 구성. **b.** 유형: 고급 응답 옵션을 선택하면 대상 상태를 설정할 수 없으며 숨겨집니다. 대상 상태는 Flow Designer 하위 플로우에서 구성된 사용자 지정 상태에 따라 할당됩니다.
다음에 대한 응답 옵션 표시	응답 옵션을 표시할 사용자 역할을 결정하는 옵션입니다. 잠금 해제 옵션을 사용하여 분석가, 최종 사용자 및 에스컬레이션된 분석가 검토 자 중에서 선택할 수 있습니다. 하나 또는 모든 역할을 선택할 수 있습니다.

응답 옵션 매핑 작업



6. 제출을 클릭합니다.

DLP 인시던트에 대한 응답 옵션 구성

이 기능을 사용하여 최종 사용자 또는 분석가가 수행해야 하는 응답 유형을 구성합니다.

시작하기 전에

기본 시스템 DLP 인시던트 응답 애플리케이션은 다음과 같은 응답 옵션을 제공합니다.

1. 평가 완료
2. 삭제된 컨텐츠
3. 삭제된 파일
4. 암호화된 파일
5. 마스킹된 콘텐츠
6. 오탐지 보고
7. 잘못된 소유자 보고
8. 격리에서 이메일 릴리스 요청

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
이 옵션은 DLP Microsoft Exchange 레코드에 사용할 수 있습니다.

9. 비즈니스 프로세스에 필요
10. 검토된 권리

필요한 역할:

- sn_dlir.admin - 작성, 편집 및 삭제.
- sn_dlir.analyst 및 sn_dlir.analyst_read - 뷰(읽기 전용).

프로시저

1. 다음으로 이동 모두 〉 **DLP** 관리 〉 응답 옵션.

   기본적으로 기본 시스템에서는 다음 두 가지 유형의 응답 옵션을 제공합니다.

   a. 기본: 사용자가 제출한 수동 응답 옵션입니다.

   b. 고급: 자동 응답 옵션은 사용자가 응답 옵션을 제출할 때 플로우 디자이너 하위 플로우를 트리거합니다.

2. 새로 만들기를 클릭합니다.
3. 양식에서 필드를 채웁니다.

응답 옵션 양식 유형: 기본

필드	설명
이름	인시던트 응답 옵션의 이름을 입력합니다.
유형	응답 옵션 유형을 선택하는 옵션입니다.

유형의 응답 옵션 양식: 고급

필드	설명
이름	인시던트 응답 옵션의 이름을 입력합니다.
유형	응답 옵션을 선택하는 옵션입니다. 기본적으로 이 필드에는 다음과 같은 두 가지 유형의 옵션이 표시됩니다. ○ 기본: 새 응답 옵션을 생성하는 동안 이 옵션을 선택하면 응답 옵션 이름과 유형을 추가해야 할 수 있습니다. ○ 고급: 이 옵션을 선택하면 다음 필드를 사용할 수 있습니다. ▪ 플로우: Flow Designer 하위 플로우를 선택합니다. ▪ **MID** 서버 필요: 선택한 플로우가 MID 서버를 사용하는 경우 이 확인란을 선택합니다.
플로우	필요한 Flow Designer 플로우를 선택하여 MID 애플리케이션 및 MID 기능을 활성화합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	응답 옵션에 대한 하위 플로우를 생성할 때 다음 하위 플로우 입력을 추가합니다. **a.** 이름: ▪ dlp_incident ▪ mid_server_capability ▪ mid_server_application **b.** 유형: ▪ 참조(DLP 인시던트 테이블에 대해) ▪ MID 서버 애플리케이션 및 MID 서버 역량 모두에 대한 시스템 ID
MID 서버 필요	MID 서버 구성을 결정하는 옵션입니다. **MID** 서버 필요 확인란을 활성화하여 **MID** 서버 애플리케이션 및 **MID** 서버 기능 필드를 사용하여 MID 애플리케이션 및 MID 기능을 구성할 수 있습니다. 주: MID 서버 애플리케이션 및 MID 서버 역량 구성을 기반으로 하며, MID가 실행 중인 경우 응답 옵션만 작업 공간에 표시됩니다.
MID 서버 애플리케이션	드롭다운 목록에서 필요한 MID 서버 애플리케이션을 선택합니다.
MID 서버 역량	드롭다운 목록에서 필요한 MID 서버 역량을 선택합니다.

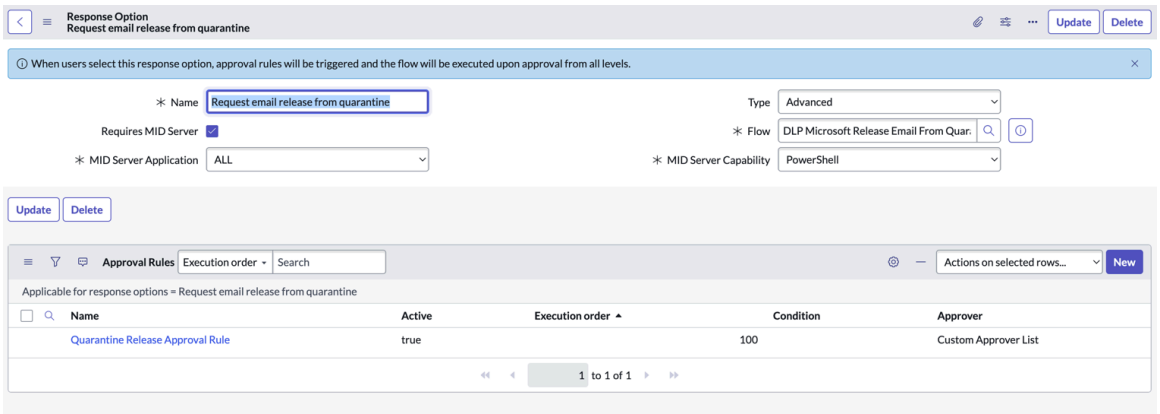
주:
선택한 MID 서버 역량에 사용할 수 있는 MID 서버가 없으면 응답 옵션이 표시되지 않습니다. 목록에서 특정 MID 서버를 사용하려면 MID 앱을 구성하여 목록에 표시해야 하며, 구성된 MID 서버가 선택한 MID 애플리케이션에서 하나 이상 실행되어야 하며 선택한 MID 서버 기능이 있어야 합니다.

4. 제출을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
고급 유형의 응답 옵션을 생성하는 경우 해당 새 응답 옵션에 대한 승인 규칙을 구성할 수 있도록 승인 규칙 관련 목록이 채워집니다. 자세한 내용은 승인 규칙 생성 문서를 참조하십시오.

유형의 응답 옵션 구성: 고급



연령 차트 구성 생성

(DLP IR) Ops 포털에 표시되는 Data Loss Prevention Incident Response 연령 차트를 구성합니다. 이 차트는 일 수에 따른 미해결 인시던트 수를 보여줍니다.

시작하기 전에

필요한 역할:

- sn_dlir.admin - 작성, 편집 및 삭제.
- sn_dlir.analyst 및 sn_dlir.analyst_read - 뷰(읽기 전용).

프로시저

1. 다음으로 이동 모두 〉 **DLP** 관리 〉 연령 차트 구성.
2. 다음 표의 연령 차트 항목을 검토하고 환경에 맞게 항목을 사용자 지정합니다.

DLP 연령 차트 구성 양식

이름	조건
0~30일	0일에서 30일 사이인 미해결 인시던트의 연령입니다.
31~60일	31일에서 60일 사이인 미해결 인시던트의 연령입니다.
61~90일	61일에서 90일 사이인 미해결 인시던트의 연령입니다.
90일 이상	90일이 지난 미해결 인시던트의 연령입니다.

3. 새로 만들기를 클릭하여 새 연령 차트 구성을 추가합니다.
4. 이름 필드에 DLP 연령 차트 구성의 이름을 입력합니다.
5. DLP 연령 차트 구성에 대한 조건을 설정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 조건을 추가하려면 **AND** 또는 **OR**을 클릭합니다.
   - **AND**를 선택하면 모든 조건이 일치해야 합니다.
   - **OR**을 선택하면 두 조건을 일치시킬 수 있습니다.

   주:
   조건 작성기의 조건은 대/소문자를 구분합니다.

b. 두 번째 필터 조건을 설정하려면 새 기준을 클릭합니다.

6. 제출을 클릭합니다.

사용자 위임 구성 작성

조직의 특정 임원이 자신에게 할당되거나 에스컬레이션된 인시던트에 대한 알림을 받지 못하도록 합니다.

시작하기 전에
필요한 역할:

- sn_dlir.admin - 작성, 편집 및 삭제.
- sn_dlir.analyst 및 sn_dlir.analyst_read - 뷰(읽기 전용).

이 태스크 정보
임원이 리더십 또는 임원 그룹에 속한 사용자인 시나리오를 생각해 보십시오. 임원에게 인시던트 할당 또는 에스컬레이션에 대한 이메일을 전송해서는 안 됩니다. 그러면 위임된 사용자가 임원을 대신하여 필요한 작업을 수행할 수 있습니다.

한 사용자가 특정 사람인 Henry를 대리인으로 할당하면 다른 사용자는 Henry를 다시 대리인으로 할당할 수 없습니다. 마찬가지로 대리인은 다른 사용자를 대리인으로 할당할 수 없습니다.

프로시저

1. 다음으로 이동 모두 〉 **DLP** 관리 〉 위임 구성.
2. 새로 만들기를 클릭합니다.
3. 양식에서 필드를 채웁니다.

위임 구성 양식

필드	설명
사용자	DLP 인시던트에 대한 대리인이 필요한 사용자의 이름입니다.
위임	원래 최종 사용자를 대신하여 DLP 인시던트에 응답할 수 있는 사용자의 이름입니다.

4. 제출을 클릭합니다.

반복 위반자 식별 규칙 생성

반복 위반자 식별 규칙을 생성하여 동일한 문제를 여러 번 반복하는 사용자를 식별합니다.

시작하기 전에
필요한 역할:

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- sn_dlir.admin - 작성, 편집 및 삭제.
- sn_dlir.analyst 및 sn_dlir.analyst_read - 뷰(읽기 전용).

이 태스크 정보

특정 규칙이나 기준을 사용하여 반복 위반자를 식별할 수 있습니다. Data Loss Prevention Incident Response 반복 위반자를 식별하는 데 사용할 수 있는 필드를 제공합니다.

프로시저

1. 다음으로 이동 모두 〉 **DLP** 관리 〉 반복 위반자 식별 규칙.
2. 새로 만들기를 클릭합니다.
3. 양식에서 필드를 채웁니다.

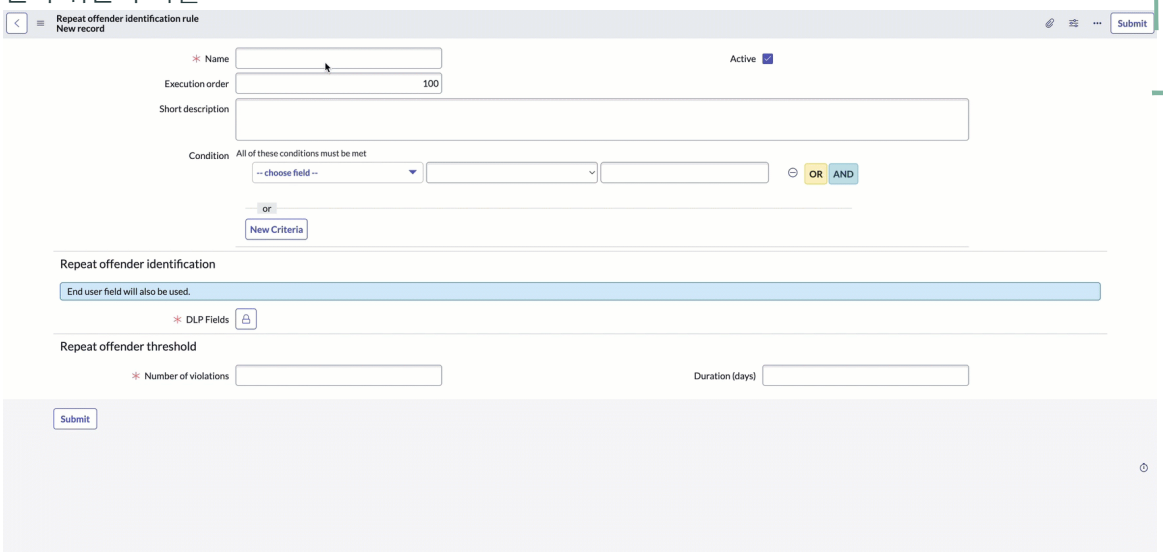
반복적인 범죄자 식별 규칙 양식

필드	설명
이름	반복 위반자 식별 규칙의 이름입니다.
실행 순서	반복 위반자 식별 규칙의 우선순위입니다. 이 필드는 둘 이상의 규칙이 트리거 조건을 공유할 때 반복 위반자 식별 규칙이 실행되는 순서를 나타냅니다. 가장 낮은 수의 반복 위반자 식별 규칙이 가장 높은 우선순위를 갖습니다. 작업 순서를 설정하려면 값을 입력합니다. 예를 들어 100, 200 또는 기타 숫자입니다. 기본값은 100입니다.
간단한 설명	이 반복 위반자 식별 규칙에 대한 고유 설명입니다.
조건	DLP 인시던트 테이블을 기반으로 하는 조건 작성기의 조건입니다. 인시던트 필드를 선택하여 반복 위반자 식별 규칙에 대한 트리거 조건을 작성할 수 있습니다. 조건 작성기의 목록과 필드를 사용하여 첫 번째 행에 대한 필터를 설정합니다. 조건을 더 추가하려면 **AND** 또는 **OR**을 클릭합니다. ○ **AND**를 선택하면 모든 조건이 일치해야 합니다. ○ **OR**을 선택하면 두 조건을 일치시킬 수 있습니다. 두 번째 필터 조건을 설정하려면 새 기준을 클릭합니다. 주: 조건 작성기의 조건은 대/소문자를 구분합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
DLP 필드	필수 DLP 필드를 기준으로 반복적인 위반자를 식별합니다. DLP 필드 옆에 있는 아이콘을 클릭하여 사용 가능한 DLP 필드 목록을 봅니다. 사용 가능 열에서 사용할 DLP 필드를 선택하고 선택됨 열로 이동합니다. 예를 들어 사용 가능 열에서파일 이름 및 파일 소유자 필드를 선택하고 선택됨 열로 이동할 수 있습니다. 그런 다음 파일 이름 및 파일 소유자 필드를 기반으로 반복 위반자를 식별할 수 있습니다. 따라서 사용자가 반복 위반자 임계치(위반 수 및 기간)를 위반하고 동일한 사용자가 DLP 필드와 일치하는 경우 해당 특정 사용자는 반복 위반자로 식별됩니다.
위반 건수	반복 위반자 임계치 제한 값을 정의합니다. 사용자가 동일한 작업을 반복하고 지정된 위반 횟수를 위반하면 사용자는 반복 위반자로 식별됩니다.
기간(일)	반복 위반자 임계치 한도를 일 형식으로 정의합니다. 사용자가 동일한 작업을 반복하고 임계치 기간을 위반하면 사용자는 반복 위반자로 식별됩니다.

반복 위반자 식별



4. 제출을 클릭합니다.

추가 인시던트 데이터 필드 생성

DLP 인시던트에 대한 추가 인시던트 데이터 필드를 생성합니다. 문자열, 숫자, 확인란, 선택, 날짜 및 시간 등 다양한 유형의 추가 인시던트 데이터 필드를 만들어 DLP 인시던트 양식에서 사용할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할:

- sn_dlir.admin - 작성, 편집 및 삭제.
- sn_dlir.analyst 및 sn_dlir.analyst_read - 뷰(읽기 전용).

중요사항:
DLP 인시던트에 대한 추가 인시던트 데이터 필드는 San Diego 버전 이상에서만 지원됩니다.

이 태스크 정보
추가 인시던트 데이터 필드는 필드 수준 제한과 연결되므로 필드 수준 제한이 있는 경우 DLP Ops 포털 및 최종 사용자 포털의 추가 인시던트 데이터 필드에 적용됩니다.

프로시저

1. 다음으로 이동 모두 〉 **DLP** 관리 〉 추가 인시던트 데이터 필드.
2. 새로 만들기를 클릭하여 추가 인시던트 데이터 필드를 만듭니다.
3. 양식에서 필드를 채웁니다.

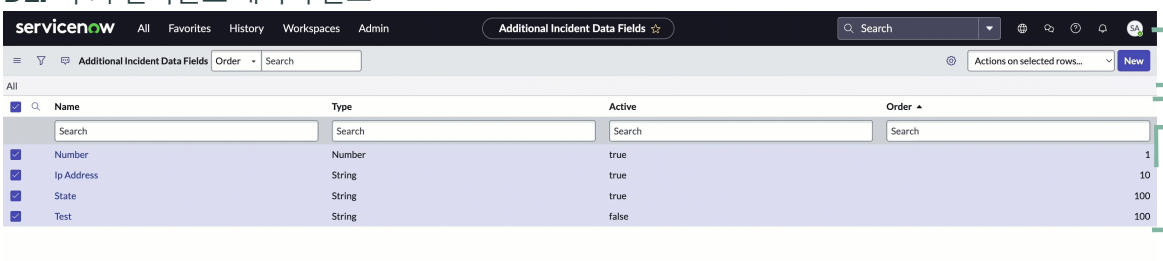
DLP 추가 인시던트 데이터 필드 양식

필드	설명
이름	추가 인시던트 데이터 필드의 이름입니다.
유형	추가 인시던트 데이터 필드의 유형을 선택하는 옵션입니다. 다음 유형 중 하나를 선택할 수 있습니다. ○ 문자열 ○ 번호 ○ 확인란 ○ 선택 추가 인시던트 데이터 필드 유형을 선택으로 선택한 경우, 추가 인시던트 데이터 필드를 생성한 후 추가 인시던트 데이터 필드 선택 옵션을 정의할 수 있습니다. 추가 인시던트 데이터 필드 선택 옵션을 작성하는 방법: **a.** 필요한 추가 인시던트 데이터 필드를 엽니다. **b.** Custom Choice Field Options(사용자 지정 선택 필드 옵션) 섹션에서 New(새로 만들기)를 클릭합니다. **c.** 옵션 이름 필드에서 필요한 옵션 이름을 정의합니다. **d.** 제출을 클릭합니다. ○ 날짜 ○ 날짜/시간

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	주: 새 추가 인시던트 데이터 필드의 유형을 선택한 후에는 수정할 수 없습니다. 유형을 수정하려면 필요한 유형으로 새 추가 인시던트 데이터 필드를 다시 만들어야 합니다.
순서	추가 인시던트 데이터 필드가 표시되는 순서를 선택하는 옵션입니다. 각 추가 인시던트 데이터 필드의 순서 값을 정의할 수 있습니다. 추가 인시던트 데이터 필드는 정의한 순서 값에 따라 정렬됩니다. 기본적으로 추가 인시던트 데이터 필드는 오름차순으로 정렬됩니다. 순서 열을 클릭하여 추가 인시던트 데이터 필드를 내림차순으로 정렬할 수 있습니다.
활성	추가 인시던트 데이터 필드가 활성 상태인지 여부를 나타내는 옵션입니다.
설명	생성한 추가 인시던트 데이터 필드에 대한 설명입니다.

DLP 추가 인시던트 데이터 필드



4. 제출을 클릭합니다.

DLP SLA 정의 양식

SLA 기록을 생성하는 데 사용되는 DLP SLA 정의 양식에 대한 필드 설명입니다.

필드	설명
이름	정의의 이름입니다.
유형	계약의 유형으로, 이 경우에는 SLA입니다.
대상	정의 중인 계약에 대한 필터링, 검색 및 보고에 사용되는 대상입니다. 사용 가능한 옵션은 다음과 같습니다. • 안 함 • 응답 • 해결

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
테이블	SLA에서 추적하는 기록을 판별하는 테이블로, DLP SLA 작업〔sn_dlir_incident_sla_task〕이어야 합니다.
플로우	SLA 정의가 작업 기록에 첨부될 때 실행할 플로우로, 기본 SLA 플로우여야 합니다.
기간 유형	SLA 기간을 계산하는 방법입니다. 사용 가능한 옵션은 다음과 같습니다. • 사용자 지정 기간 • 영업일 기준 2일 오후 4시까지 • 영업일 기준 3일 오후 4시까지 • 기한 위반 • 다음 영업일 종료 • 다음 영업일 오후 4시까지
지속 시간	위반됨으로 표시되기 전에 SLA가 실행되는 시간입니다. 이 필드는 기간 유형에서 사용자 지정 기간을 선택한 경우에만 사용할 수 있습니다.
일정 소스	작업 SLA를 생성하는 동안 사용할 일정입니다.
일정	SLA 타이머가 실행되는 시간입니다. 이 일정 집합은 핵심 구성에서 정의됩니다.
시간대소스	작업 SLA를 만들 때 사용할 시간대 소스입니다. 사용 가능한 옵션은 다음과 같습니다. • 호출자의 시간대 • SLA 정의의 시간대 • CI 위치의 시간대 • 작업 위치의 시간대 • 호출자 위치의 시간대
활성	시작 조건이 충족될 때 트리거를 유효하게 하는 옵션입니다.
탭	
시작 조건	SLA 타이머를 시작하고 SLA를 활성화하는 조건입니다.
일시 중지 조건	SLA가 일시 중단되는 조건으로, 총 경과 시간이 증가합니다.
조건 취소	SLA가 취소되는 조건입니다.
재설정 조건	작업 기록에 대한 필드 값이 기록의 특정 값으로 변경되거나, 특정 값에서 변경될 때 활성 SLA가 완료되고 새 SLA가 설정되는 조건입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	예를 들어, 작업 기록의 위치 필드 값이 101 Broadway East, Seattle, WA라고 가정해 보겠습니다. SLA 재설정 조건을 **[Location][changes from][101 Broadway East, Seattle, WA]**로 설정한 경우 위치 필드의 값을 변경하면 작업 기록의 SLA가 재설정됩니다.

관련 정보

Data Loss Prevention Incident Response SLA 정의 생성

고급 설정 구성

다른 기능 중에서 최종 사용자를 식별하기 위한 인시던트의 필드를 결정할 수 있도록 고급 설정을 구성합니다.

시작하기 전에

필요한 역할:

- sn_dlir.admin - 작성, 편집 및 삭제.
- sn_dlir.analyst 및 sn_dlir.analyst_read - 뷰(읽기 전용).

이 태스크 정보

에서 Data Loss Prevention Incident Response 고급 설정을 구성하는 것은 선택 사항입니다. 일부 고급 설정에는 다음이 포함됩니다.

- 다이제스트 이메일로 보낼 수 있는 최대 인시던트 수를 정의합니다.
- 빠른 모드를 활성화하여 이메일을 더 빠르게 보낼 수 있습니다.
- 애플리케이션의 로그 세부 정보를 결정합니다.

프로시저

1. 다음으로 이동 모두 〉 **DLP** 관리 〉 고급 설정.
2. 양식에서 필드를 채웁니다.

고급 설정 양식

필드	설명
위반을 일으킨 민감한 데이터를 인시던트에 표시해야 합니까?	위반을 일으킨 민감한 데이터를 DLP 인시던트에 표시할지 여부를 선택하는 옵션입니다. 기본적으로 이 옵션은 활성화되어 있습니다.
위반을 일으킨 민감한 데이터도 하위 인시던트에 표시되어야 합니까?	위반을 일으킨 민감한 데이터를 DLP 하위 인시던트에도 표시할지 여부를 선택하는 옵션입니다. 기본적으로 이 옵션은 꺼져 있습니다.
최종 사용자를 식별하는 데 사용되는 인시던트의 필드 목록	최종 사용자를 식별하는 데 사용되는 할당 규칙 모듈의 인시던트에 있는 필드 목록입니다. 최종

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	사용자를 식별하기 위해 고유한 사용자 지정 속성을 지정할 수도 있습니다.
다이제스트 이메일의 최대 인시던트 수	다이제스트 이메일로 보낼 수 있는 최대 인시던트 수입니다. 기본적으로 이 값은 100입니다.
반복 위반 최대 기간(일)	상습범을 식별할 수 있는 최대 기간입니다. 기본적으로 이 값은 90일입니다.
이메일을 보내기 위한 빠른 모드	이메일을 확인하고 문제를 식별하는 옵션입니다. Yes(예) 옵션을 활성화하여 확인을 수행할 수 있습니다. 기본적으로 이 옵션은 활성화되어 있습니다.
이 속성은 애플리케이션의 로그 세부 정보를 설정하는 데 사용됩니다.	애플리케이션의 로그 세부 정보 표시 수준으로, 정보 유형의 이름을 의미합니다. 값을 다음 옵션으로 업데이트할 수도 있습니다. ○ 오류 ○ 경고 ○ 정보 ○ **debug** 기본적으로 이 값은 정보입니다.
보고서에서 복제된 인시던트 및 하위 인시던트 제외	보고서에서 복제된 인시던트 및 하위 인시던트를 제외하는 옵션입니다. 기본적으로 이 옵션은 예입니다.
인시던트가 종결된 후 클라우드 스토리지에서 일치 컨텐츠가 삭제될 때까지 대기하는 일 수	특정 기간 동안 비활성 상태인 인시던트의 일치 콘텐츠를 정리하기 위한 대기 일수를 선택하는 옵션입니다. 기본적으로 이 값은 90입니다. 90일 후 DLP 인시던트가 비활성 상태인 경우 일치 콘텐츠가 클라우드 스토리지에서 정리됩니다.
마지막 에스컬레이션 수준 이후 DLP 분석가 그룹에 인시던트 할당	마지막 에스컬레이션 수준 후의 분석가에게 인시던트를 할당하려면 이 확인란을 선택합니다.
사용자가 에스컬레이션 후 인시던트에 액세스할 수 있도록 허용	할당된 사용자가 에스컬레이션 후 인시던트에 액세스할 수 있도록 하려면 이 확인란을 선택합니다. 이 옵션을 선택하면 에스컬레이션 체인 목록에 추가된 모든 사용자가 인시던트에 접근할 수 있습니다.
분석가가 완료된 평가를 편집하도록 허용	분석가가 완료된 평가를 편집할 수 있도록 하려면 이 확인란을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	이 옵션을 선택하면 분석가가 평가를 편집할 수 있으며, 선택하지 않으면 읽기 전용 모드에서 평가를 볼 수 있습니다.
증거 파일 미리 보기 속성	
이 시스템 속성을 활성화하면 DLP 분석가 작업 공간에서 증거 파일 미리 보기 기능이 활성화됩니다. sn_dlir.enable_evidence_file_preview	작업 공간에서 직접 증거 파일을 미리 볼지 여부를 선택하는 옵션입니다. 기본적으로 이 옵션은 예입니다.
이렇게 하면 DLP 사용자가 미리 본 증거 파일을 다운로드할 수 있습니다. 이 속성을 사용하도록 설정하면 문서 뷰어에 증거 파일을 다운로드할 수 있는 다운로드 버튼이 표시됩니다. sn_dlir.enable_download in_preview	미리 본 증거 파일을 다운로드할 수 있는 문서 뷰어에 다운로드 버튼을 표시할지 여부를 선택하는 옵션입니다. 기본적으로 이 옵션은 예입니다.
이 속성은 증거 파일 미리 보기를 위해 파일을 임시로 보존할 기간을 결정합니다. (분 단위) sn_dlir.preview_temp_files_cleanup_interval	증거 파일 미리 보기를 위해 파일을 임시로 저장하는 최대 기간입니다. 기본적으로 이 값은 10입니다. 10분 후 DLP 인시던트가 비활성 상태인 경우 증거 파일이 분석가 작업 공간에서 정리됩니다.
증거 파일이 사용 중인 경우 이 속성을 활성화하면 정리 간격이 연장됩니다. 이렇게 하면 시스템이 시스템 속성 "sn_dlir.preview_temp_files_cleanup_interval"에 설정된 값에 따라 증거 파일의 만료 시간을 연장할 수 있습니다. sn_dlir.extend_cleanup_interval_on_usage	증거 파일이 사용 중인 경우 삭제되기 전의 시간을 연장하는 옵션입니다. 기본적으로 이 옵션은 예입니다.
증거 파일의 정리 간격을 확장하는 최대 기간(분)입니다. sn_dlir.max_extension_duration_for_cleanup	증거 파일을 정리하기 전에 시스템에서 증거 파일을 보관하는 기간(분)을 선택하는 옵션입니다. 기본적으로 이 값은 60입니다.

3. 저장을 클릭합니다.

DLP 통합 실행 프로세스 모니터링

진행 중인 수집 또는 통합 실행 프로세스를 추적하고 모니터링합니다. 통합 실행 프로세스에는 처리된 데이터의 양과 통합 상태에 대한 통계가 포함됩니다.

필요한 역할: sn_dlir.admin.

통합 실행 프로세스에는 수집되는 기록 수에 대한 상세 정보가 나열됩니다. 예:

1. Symantec 통합에서 프로세스에는 하위 및 상위 통합 실행이 모두 포함됩니다. 상위 기록은 수집 데이터를 나타내고 하위 기록은 보강 호출 및 사용자 지정 속성 기록을 나타냅니다.
2. Microsoft 통합에서는 상위 기록 수집 프로세스만 실행할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

DLP 통합 실행 프로세스: 큐 항목, 큐 항목의 상태 및 가져온 기록이 표시됩니다.

통합 실행에는 통합 프로파일 및 통합 실행 기록이 생성되는 소스, 프로파일 폴링 간격, 수집 상태 및 하위 상태, 수집된 기록 수를 나타내는 인시던트 수가 포함됩니다.

1. 다음으로 이동 **DLP** 관리 〉 통합 실행.
2. 목록에서 통합 실행을 선택합니다.
3. **DLP** 통합 실행 프로세스로 이동합니다.
4. 기록의 큐 항목 상태를 봅니다.

DLP 인시던트 접근 제한

중요한 정보가 포함된 특정 DLP 인시던트의 가시성을 관리합니다. 인시던트 액세스 제한을 사용하여 특정 DLP 인시던트에 액세스할 수 있는 사용자를 정의하고 특정 사용자 또는 그룹이 해당 인시던트에 액세스하지 못하도록 제한할 수 있습니다.

필드 수준 제한 생성

DLP 인시던트에서 필드 수준 제한을 설정하여 중요한 정보가 노출되지 않도록 보호합니다. 필드 수준 제한을 사용하여 DLP 인시던트의 특정 필드에 액세스할 수 있는 사용자 또는 그룹을 제어할 수 있습니다.

시작하기 전에
필요한 역할:

- sn_dlir.admin - 작성, 편집 및 삭제.
- sn_dlir.analyst 및 sn_dlir.analyst_read - 뷰(읽기 전용).

이 태스크 정보
필드 수준 제한을 사용하면 특정 사용자 또는 그룹에 대해 특정 필드만 표시할 수 있으므로 사용자가 액세스할 수 있는 데이터를 보다 세부적으로 제어할 수 있습니다. DLP 인시던트 일치 조건을 정의하고, 이러한 조건이 적용되는 사용자 또는 그룹을 선택한 다음, 이러한 사용자 또는 그룹이 볼 수 있는 DLP 필드를 선택하여 필드 수준 제한을 만들 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 **DLP** 관리 〉 인시던트 접근 제한 〉 필드 수준 제한.
2. 새로 만들기를 클릭합니다.
3. 양식에서 필드를 채웁니다.

DLP 필드 수준 제한 양식

필드	설명
이름	필드 수준 제한의 이름입니다.
활성	필드 수준 제한이 활성 상태인지 여부를 나타내는 옵션입니다.
실행 순서	필드 수준 제한의 우선순위입니다. 이 필드는 둘 이상의 필드 수준 제한이 트리거 조건을 공유할 때 필드 수준 제한이 실행되는 순서를 나타냅니다. 숫자가 가장 낮은 필드 수준 제한이 가장 높은 우선순위를 갖습니다.

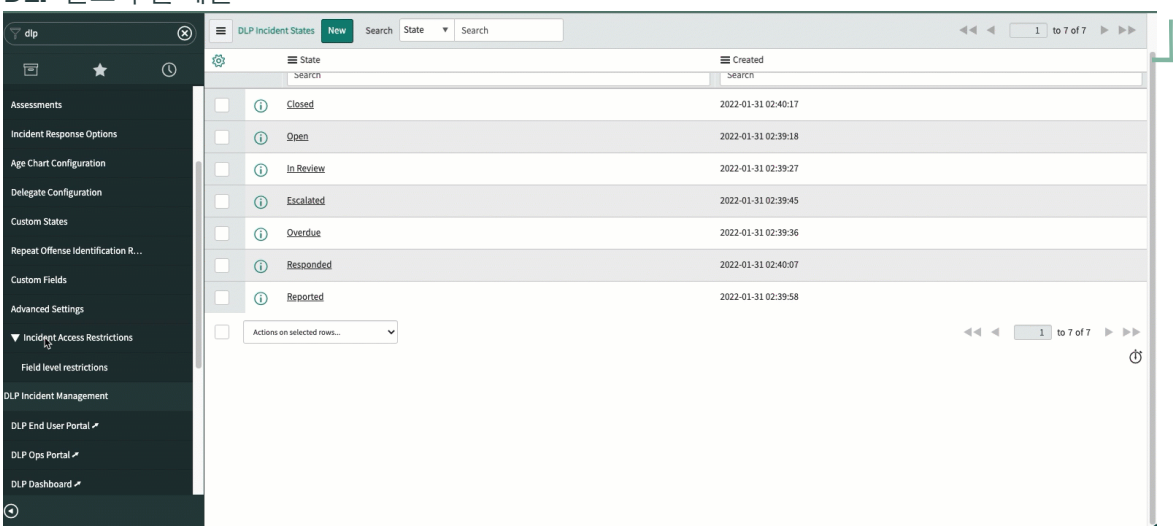
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	작업 순서를 설정하려면 값을 입력합니다. 예를 들어 100, 200 또는 기타 숫자입니다. 기본값은 100입니다.
간단한 설명	이 필드 수준 제한에 대한 고유한 설명입니다.
인시던트 일치 조건	정의된 조건과 일치하는 인시던트의 옵션입니다. 필드 수준 제한에 대한 트리거 조건을 정의하기 위해 인시던트 필드를 선택할 수 있습니다. 조건 작성기의 목록과 필드를 사용하여 첫 번째 행에 대한 필터를 설정합니다. 조건을 더 추가하려면 **AND** 또는 **OR**을 클릭합니다. ○ **AND**를 선택하면 모든 조건이 일치해야 합니다. ○ **OR**을 선택하면 두 조건을 일치시킬 수 있습니다. 두 번째 필터 조건을 설정하려면 새 기준을 클릭합니다. 예를 들어 필드를 ## ####선택하고 조건을 in 및 ## #### ### # ####. 주: 조건 작성기의 조건은 대/소문자를 구분합니다.
적용 대상	특정 사용자 또는 그룹에 인시던트 일치 조건을 적용하는 옵션입니다. 다음에 조건을 적용할 수 있습니다. ○ 모든 최종 사용자: DLP 인시던트 조건을 적용할 수 있는 모든 최종 사용자를 선택하는 옵션입니다. ○ 에스컬레이션된 인시던트의 모든 검토자: DLP 인시던트 조건을 적용할 수 있는 에스컬레이션된 인시던트의 모든 검토자를 선택하는 옵션입니다. Manager로 에스컬레이션된 모든 DLP 인시던트를 나타냅니다. ○ 사용자: 아이콘을 클릭하여 DLP 인시던트 조건을 적용할 수 있는 특정 사용자를 목록에서 추가합니다. 이메일 주소나 검색 옵션을 사용하여 사용자를 추가할 수도 있습니다. 예: 법무 관리자 DLP 조건을 적용할 수 있는 사용자로 자신을 추가하려면 ○ 그룹: 아이콘을 클릭하여 DLP 인시던트 조건을 적용할 수 있는 특정 그룹을 목록에서 추가합니다. 검색 옵션을 사용하여 그룹을 추가할 수도 있습니다. 예를 들어 설문 조사 작성자입니다.
다음 필드에만 접근 허용	○ **DLP** 필드: 선택한 사용자 또는 그룹에 대한 액세스를 허용할 DLP 필드를 정의하는 옵션입니다. 사용 가능 열에서 액세스를 허용할 DLP 필드를 선택하고 선택됨 열로 이동합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	주: 선택한 사용자 또는 그룹은 선택한 DLP 필드에만 액세스할 수 있습니다. 예를 들어 사용 가능 열에서할당 대상 및 오픈 필드를 선택하고 선택됨 열로 이동할 수 있습니다. 그러면 선택한 사용자 또는 그룹은 할당 대상 및 오픈됨 필드에만 액세스할 수 있습니다. ○ 첨부 파일 업로드: 선택한 사용자 또는 그룹이 첨부 파일을 업로드할 수 있도록 허용할지 여부를 나타내는 옵션입니다. ○ 사용자 지정 필드: 선택한 사용자 또는 그룹에 대한 액세스를 허용할 사용자 지정 필드를 정의하는 옵션입니다. 사용 가능 열에서 생성한 사용자 지정 필드를 볼 수 있습니다. 사용 가능 열에서 액세스를 허용할 사용자 지정 필드를 선택하고 선택됨 열로 이동합니다. 중요사항: ▪ DLP 인시던트에 대한 사용자 지정 필드는 San Diego 버전 이상에서만 지원됩니다. ▪ 선택한 사용자 또는 그룹은 선택한 사용자 지정 필드에만 액세스할 수 있습니다.

DLP 필드 수준 제한



4. 제출을 클릭합니다.

기록 수준 제한 생성

DLP 인시던트에서 기록 수준 제한을 설정하여 중요한 기록이 노출되지 않도록 보호합니다. 기록 수준 제한을 사용하여 DLP 인시던트의 특정 기록에 액세스할 수 있는 사용자 또는 그룹을 제어할 수 있습니다.

시작하기 전에
필요한 역할:

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- sn_dlir.admin - 작성, 편집 및 삭제.
- sn_dlir.analyst 및 sn_dlir.analyst_read - 뷰(읽기 전용).

이 태스크 정보

기록 수준 제한을 사용하면 특정 사용자 또는 그룹의 기록에 대한 액세스만 제공할 수 있으며, 사용자가 액세스할 수 있는 기록을 보다 세부적으로 제어할 수 있습니다. DLP 인시던트 일치 조건을 정의하고, 이러한 조건이 적용되는 사용자 또는 그룹을 선택한 다음, 이러한 사용자 또는 그룹이 볼 수 있는 DLP 기록을 선택하여 기록 수준 제한을 만들 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 **DLP** 관리 〉 인시던트 접근 제한 〉 기록 수준 제한.
2. 새로 만들기를 클릭합니다.
3. 양식에서 필드를 채웁니다.

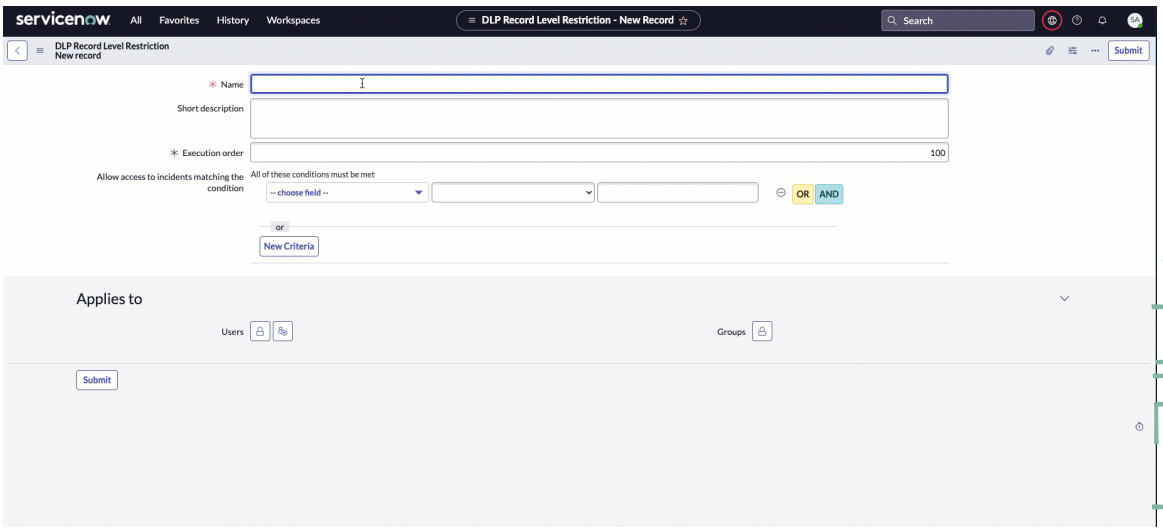
DLP 기록 수준 제한 양식

필드	설명
이름	기록 수준 제한의 이름입니다.
간단한 설명	이 기록 수준 제한에 대한 고유한 설명입니다.
실행 순서	기록 수준 제한의 우선순위입니다. 이 필드는 둘 이상의 기록 수준 제한이 트리거 조건을 공유할 때 기록 수준 제한이 실행되는 순서를 나타냅니다. 숫자가 가장 낮은 기록 수준 제한이 가장 높은 우선순위를 갖습니다. 작업 순서를 설정하려면 값을 입력합니다. 예를 들어 100, 200 또는 기타 숫자입니다. 기본값은 100입니다.
조건과 일치하는 인시던트에 대한 접근 허용	옵션을 사용하면 정의된 조건과 일치하는 인시던트에 액세스할 수 있습니다. 기록 수준 제한에 대한 트리거 조건을 정의하기 위한 인시던트 필드를 선택할 수 있습니다. 조건 작성기의 목록과 필드를 사용하여 첫 번째 행에 대한 필터를 설정합니다. 조건을 더 추가하려면 **AND** 또는 **OR**을 클릭합니다. ○ **AND**를 선택하면 모든 조건이 일치해야 합니다. ○ **OR**을 선택하면 두 조건을 일치시킬 수 있습니다. 두 번째 필터 조건을 설정하려면 새 기준을 클릭합니다. 주: 조건 작성기의 조건은 대/소문자를 구분합니다. 예를 들어 필드를 ##으로 선택하고 조건을 ## ### 및 #로 설정할 수 있습니다.
적용 대상	특정 사용자 또는 그룹에 기록 수준 제한을 적용하는 옵션입니다. 다음과 같이 조건을 적용할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	○ 사용자: 아이콘을 클릭하여 선택한 기록을 적용할 수 있는 특정 사용자를 목록에서 추가합니다. 이메일 주소나 검색 옵션을 사용하여 사용자를 추가할 수도 있습니다. 예: 법무 관리자 기록을 적용할 수 있는 사용자로 자신을 추가하려면 을 클릭합니다. 예: 시스템 관리자 ○ 그룹: 아이콘을 클릭하여 선택한 기록을 적용할 수 있는 목록에서 특정 그룹을 추가합니다. 검색 옵션을 사용하여 그룹을 추가할 수도 있습니다. 예를 들어 설문 조사 작성자입니다.

DLP 기록 수준 제한



4. 제출을 클릭합니다.

DLP 인시던트 보관

Data Loss Prevention Incident Response DLP 인시던트 테이블에 대한 기본 시스템에서 하나의 보관 규칙으로 프로비저닝됩니다. 관련 기록도 기본 시스템의 DLP 인시던트 보관 규칙에 추가됩니다.

시작하기 전에

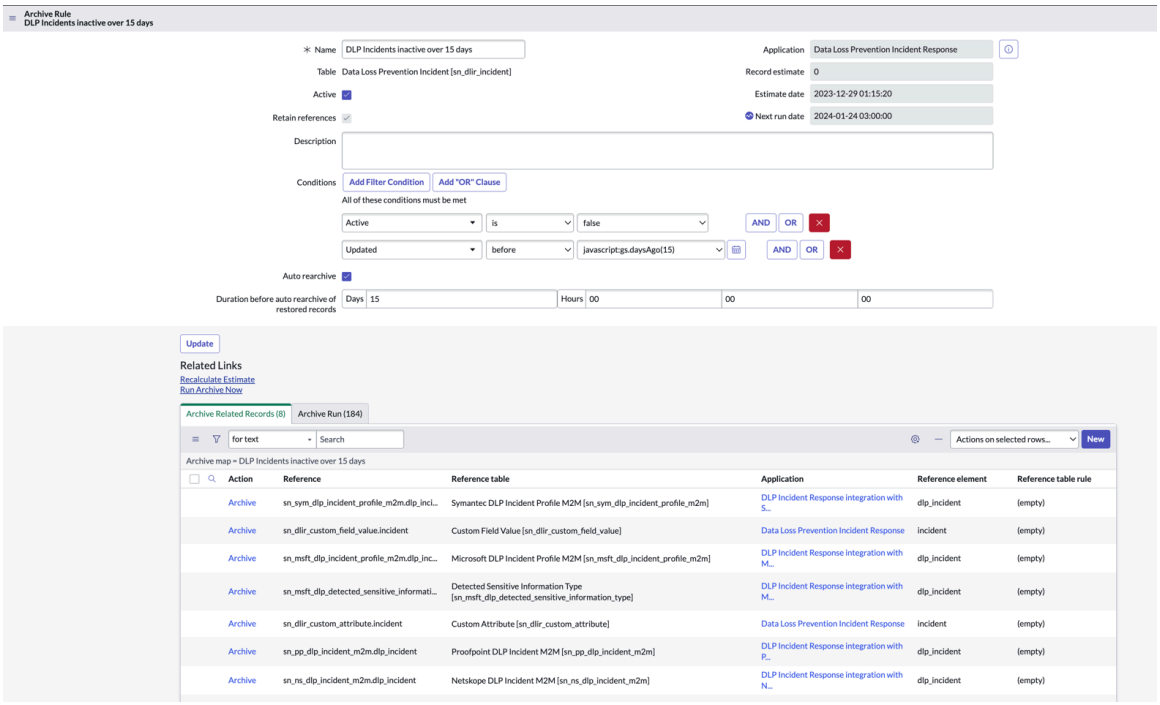
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 〉 시스템 보관 〉 보관 규칙.
   기본 시스템에 있는 시스템 보관 규칙이 표시됩니다.
2. DLP 보관 규칙을 봅니다.

> 주:
> 15일 동안 비활성 상태인 **DLP** 인시던트 는 DLP 인시던트에 대한 기본 시스템 보관 규칙입니다. 필요한 경우 보관 규칙을 수정할 수 있습니다. 이 규칙은 15일 이상 비활성 상태인 인시던트가 자동으로 보관됨을 나타냅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



주:
보관 규칙을 만드는 방법에 대한 자세한 내용은 보관 규칙 만들기를 참조하세요.

3. 필요한 경우 규칙을 업데이트합니다.

DLP 관련 기록 보관

DLP 인시던트에 대한 보관 관련 기록 관련 목록을 사용하여 보관 규칙에 관련 기록을 추가합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 〉 시스템 보관 〉 보관 규칙.

2. **DLP** 15일 이상 비활성 인시던트 보관 규칙을 선택합니다.

3. 보관 관련 기록 관련 목록으로 이동합니다.

4. DLP 관련 기록을 봅니다.

애플리케이션	참조 테이블
Symantec과의 DLP 인시던트 응답 통합	Symantec DLP 인시던트 프로파일 M2M (sn_sym_dlp_incident_profile_m2m)
데이터 손실 방지 인시던트 응답	사용자 지정 필드 값 (sn_dlir_custom_field_value)
Microsoft와의 DLP 인시던트 응답 통합	Microsoft DLP 인시던트 프로파일 M2M (sn_msft_dlp_incident_profile_m2m)
Microsoft와의 DLP 인시던트 응답 통합	탐지된 중요한 정보 유형 (sn_msft_dlp_detected_sensitive_information_type)
데이터 손실 방지 인시던트 응답	사용자 지정 속성 (sn_dlir_custom_attribute)

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

애플리케이션	참조 테이블
Proofpoint와의 DLP 인시던트 응답 통합	Proofpoint DLP 인시던트 M2M (sn_pp_dlp_incident_m2m)
Netskope와의 DLP 인시던트 응답 통합	Netskope DLP 인시던트 M2M (sn_ns_dlp_incident_m2m)
Symantec과의 DLP 인시던트 응답 통합	탐지된 중요한 정보 유형 (sn_sym_dlp_detected_sensitive_information_type)

주:
이메일, 평가, 첨부 파일과 같은 모든 시스템 테이블은 보관된 DLP 기록으로 자동으로 연결됩니다.

5. 보관할 보관 관련 기록 규칙을 선택합니다.

주:
관련 기록을 더 추가하는 방법에 대한 자세한 내용은 에서 DLP 관련 기록 보관 을 ServiceNow AI Platform참조하십시오.

Data Loss Prevention Incident Response 인시던트 관리

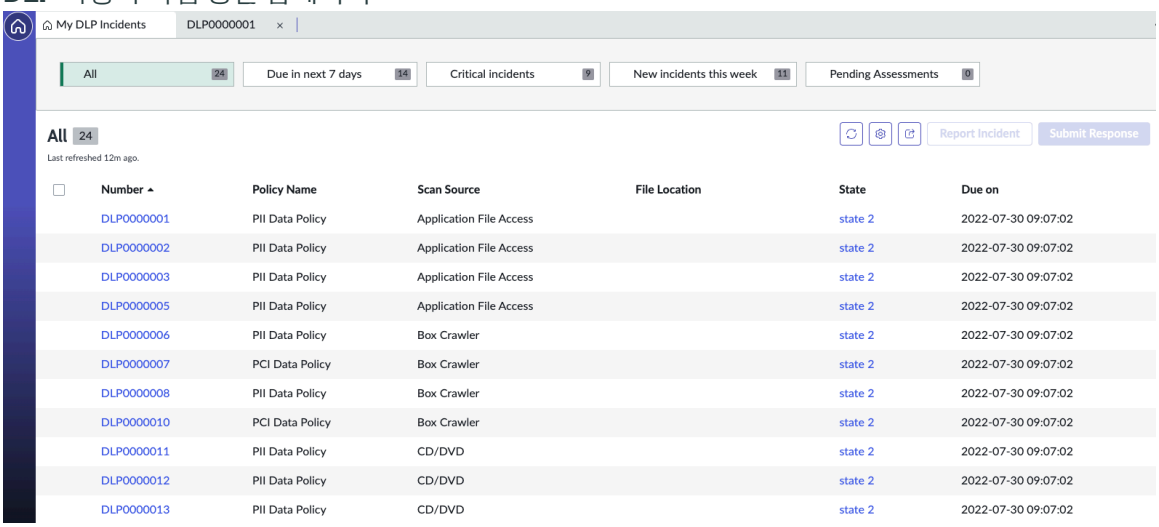
Data Loss Prevention Incident Response 인시던트 관리를 사용하면 DLP 사용자 작업 공간, DLP 분석가 작업 공간 및 DLP 대시보드를 활용하여 인시던트를 업데이트하고 관리할 수 있습니다.

Data Loss Prevention Incident Response 사용자 작업 공간

Data Loss Prevention Incident Response (DLP IR) 사용자 작업 공간은 최종 사용자, 관리자 및 승인자가 할당된 DLP 인시던트에 응답할 수 있는 작업 공간입니다. 그러면 최종 사용자, 관리자 및 승인자가 올바른 작업을 지정하여 인시던트에 대응할 수 있습니다.

최종 사용자가 DLP 인시던트에 대응할 수 있도록 평가를 만들고 관리할 수도 있습니다. 작업 공간은 할당된 DLP 인시던트를 볼 수 있는 방문 페이지와 목록 뷰로 구성됩니다.

DLP 사용자 작업 공간 홈페이지



DLP 인시던트 보고 또는 대응

Data Loss Prevention Incident Response (DLP) 사용자 작업 공간에 액세스하고, 할당된 DLP 인시던트를 검토하고, 인시던트를 보고하거나 대응합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할:

- 유효한 모든 사용자/직원

프로시저

1. 다음으로 이동 모두 〉 **DLP** 인시던트 관리 〉 **DLP** 사용자 작업 공간.
   내 DLP 인시던트 페이지가 새 탭에서 열립니다.
2. 목록 뷰를 클릭하여 자신에게 할당된 인시던트를 검토합니다.

목록 뷰	설명
모두	할당된 모든 인시던트를 봅니다.
7일 후 만료	다음 7일 내에 만료되는 모든 인시던트를 봅니다.
중요한 인시던트	심각도 레이블이 중요인 모든 인시던트를 봅니다.
이번 주 새 인시던트	이번 주에 할당된 모든 인시던트를 봅니다.
보류 중인 평가	아직 보류 중인 모든 평가를 봅니다.

3. 다음 두 가지 방법을 사용하여 DLP 인시던트를 검토할 수 있습니다.

   a. 첫 번째 방법은 검토하려는 DLP 인시던트를 하나 이상 찾아 선택하고 인시던트 옆에 있는 확인란을 클릭하는 것입니다.

   b. 자신에게 적합한 옵션을 선택합니다.

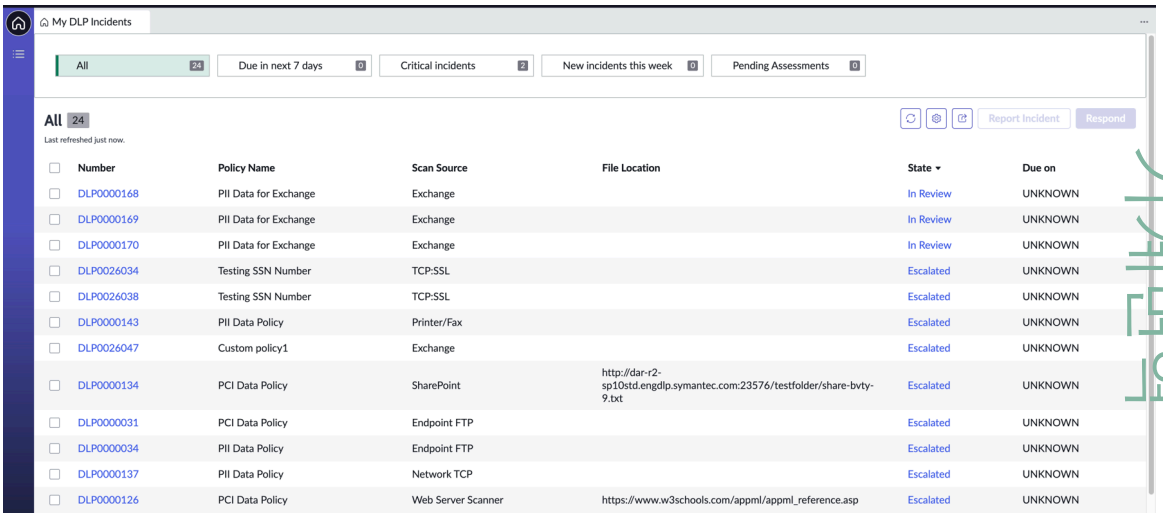
DLP 최종 사용자 포털 홈페이지

옵션	설명
목록 새로 고침	업데이트한 경우 DLP 인시던트 목록을 새로 고치는 옵션입니다.
목록 작업	수행할 수 있는 작업 목록입니다. 선택 항목은 다음과 같습니다. ▪ 다른 이름으로 저장 ▪ 열 편집 ▪ 너비 재설정 **주:** 내 목록 섹션 아래에 작업 공간에 대해 구성된 사용자 지정 목록이 있는 경우 아래의 추가 목록 작업도 수행할 수 있습니다. ▪ 이름 바꾸기 ▪ 저장 ▪ 삭제

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵션	설명
모두에 대한 URL 복사	모든 DLP 인시던트의 URL을 복사하는 옵션입니다.
인시던트 보고	인시던트를 가양성 또는 잘못된 소유자로 보고하는 작업입니다. 예를 들어 잘못된 소유자를 보고하고 다른 소유자를 제안하거나 인시던트를 긍정 오류로 보고할 수 있습니다.
응답	인시던트 응답 옵션을 선택하여 인시던트에 응답합니다. 예를 들어 사용자가 DLP 정책을 위반하는 파일을 삭제하는 경우 사용자는 삭제된 파일 옵션을 선택하여 파일이 삭제되었다는 수동 확인을 제출하고 의견을 제공할 수 있습니다. 여기에서 고급 응답 옵션을 선택할 수도 있습니다. (예: 격리에서 이메일 릴리스 요청)

DLP 사용자 포털 홈페이지



c. 두 번째 방법은 특정 DLP 인시던트를 클릭하여 여는 것입니다.
상세 정보 탭에는 다음 섹션이 표시됩니다.

- 상세 정보: 인시던트 번호, 심각도, 파일 이름 등 DLP 인시던트의 상세 정보를 볼 수 있습니다.
- 작성: 모든 사람에게 표시되는 DLP 인시던트에 대한 설명을 추가하려면 설명 탭에 설명을 입력합니다. 특정 사용자에게 표시되는 설명을 추가하려면 작업 메모(비공개) 탭에 설명을 입력합니다.
- 활동: DLP 인시던트에서 다양한 활동의 상세 정보를 볼 수 있습니다.
- 첨부 파일: DLP 인시던트와 관련된 첨부 파일이 있는 경우 찾아보기 를 클릭하고 로컬 드라이브에서 첨부 파일을 선택합니다.

  추가 상세 정보 탭에는 사용자 지정 필드를 포함하여 DLP 인시던트에 대한 모든 추가 정보가 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

중요사항:

- DLP 인시던트에 대한 사용자 지정 필드는 San Diego 버전 이상에서만 지원됩니다.
- 특정 DLP 인시던트에 사용할 수 있는 사용자 지정 필드 데이터가 있는 경우 추가 상세 정보 탭에서 볼 수 있습니다. DLP 인시던트에 대한 사용자 지정 필드가 없으면 빈 페이지가 표시됩니다.

- 탐지된 중요한 정보 유형: 인시던트에서 탐지된 중요한 정보를 표시합니다.

주:
이 관련 목록은 Microsoft 또는 Symantec 통합용으로 생성된 DLP 인시던트에 대해서만 표시됩니다. Microsoft 또는 Symantec 인시던트 기록 내에서 사용자가 탐지된 중요한 정보 유형 기록에 액세스할 때마다 해당 통합과 관련하여 강조 표시된 일치 컨텐츠가 표시됩니다.

d. 자신에게 적합한 옵션을 선택합니다.

옵션	설명
오탐지 보고	DLP 인시던트가 잘못 트리거되었거나 생성되었음을 보고하는 작업입니다. 인시던트를 긍정 오류로 표시한 이유에 대한 자세한 내용을 의견 필드에 언급할 수 있습니다.
잘못된 소유자 보고	DLP 인시던트가 잘못된 사용자에게 할당되었음을 보고하는 작업입니다. 인시던트의 올바른 소유자를 알고 있는 경우 소유자 제안 필드에서 소유자의 이름을 선택할 수 있습니다. 상세 정보를 추가하려면 의견 필드를 사용합니다.
응답	인시던트 응답 옵션을 선택하여 인시던트에 응답합니다. 예를 들어 사용자가 DLP 정책을 위반하는 파일을 삭제하는 경우 사용자는 삭제된 파일 옵션을 선택하여 파일이 삭제되었다는 수동 확인을 제출하고 의견을 제공할 수 있습니다. 여기에서 고급 응답 옵션을 선택할 수도 있습니다. (예: 격리에서 이메일 릴리스 요청)

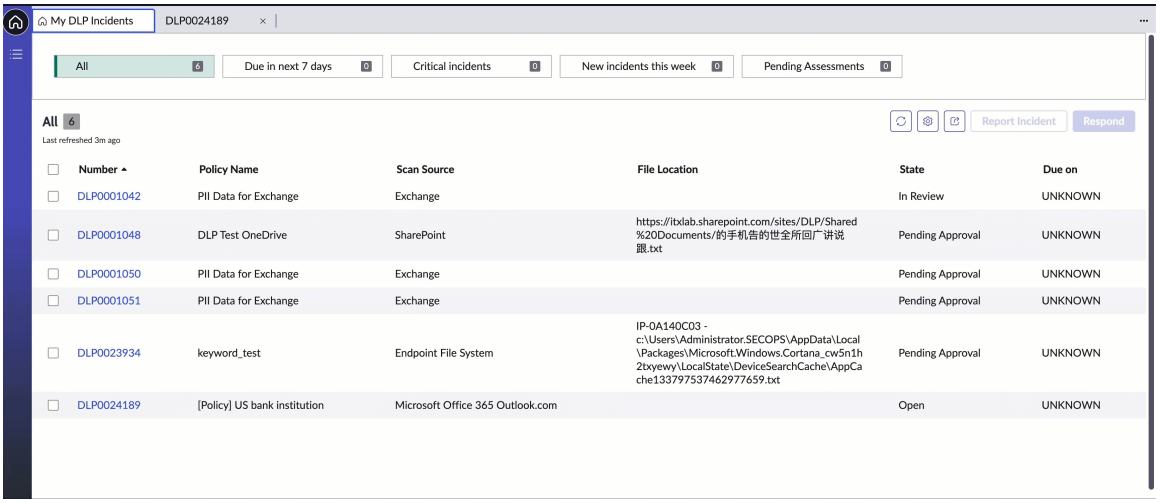
e. 분석가 쿼리에 응답한 후 응답 버튼을 선택합니다.
인시던트 응답을 제출하는 팝업이 나타납니다. 드롭다운 메뉴에서 응답을 선택하고 코멘트를 추가합니다.

f. 제출을 선택합니다.
응답이 성공적으로 제출되었음을 확인하는 배너가 나타납니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
인시던트가 해당 승인자 또는 분석가에게 할당되고 최종 사용자는 인시던트에 대한 액세스 권한을 잃게 됩니다.

DLP 인시던트 작업

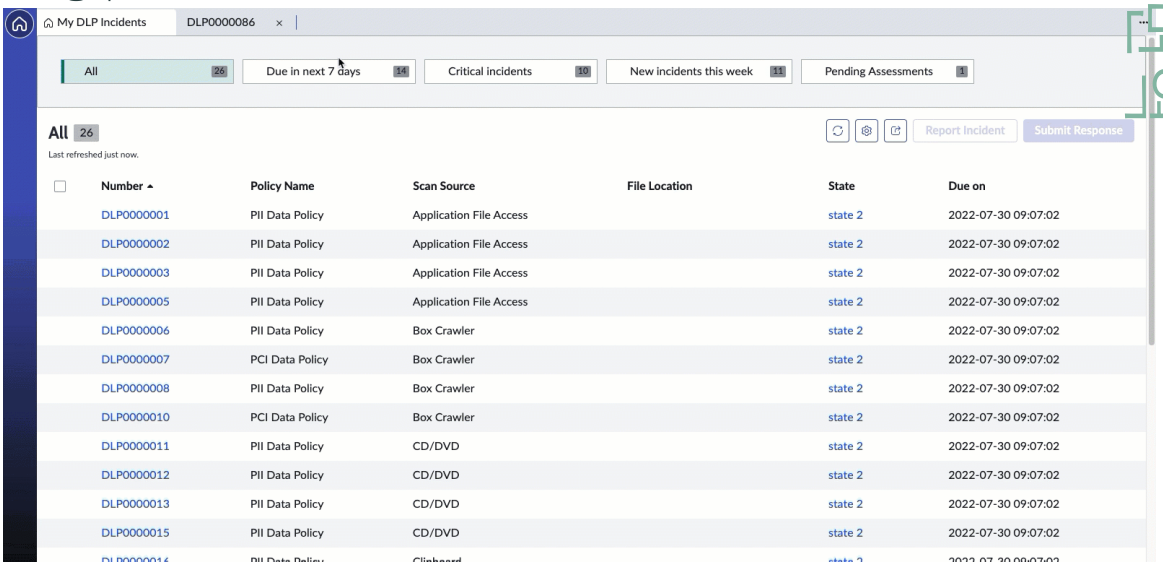


4. 평가를 수행하려면 보류 중인 평가 목록 뷰를 선택합니다.

a. 특정 평가 번호를 클릭하여 엽니다.

b. 평가 질문에 대답하고 요구 사항에 따라 저장 또는 제출 을 클릭합니다.

DLP 평가



5. 특정 인시던트에 대한 추가 정보를 보려면 DLP 인시던트 양식 뷰의 모든 필드 위에 표시되는 지침 카드 섹션을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
작업 공간의 이 섹션은 사용자에게 인시던트 해결의 다음 단계를 이해하는 데 도움이 되는 인시던트 정보를 안내합니다.

사용자 지침 카드에는 양식 뷰의 특정 인시던트에 대한 자세한 정보를 제공하는 두 개의 서로 다른 헤더가 표시됩니다. 추가 세부 정보를 보려면 사용자 지침 헤더를 클릭하십시오.

자세한 내용은 사용자 지침 템플릿 생성 및 DLP UI 사용자 지침 구성 문서를 참조하십시오.

내 승인 모듈로 작업하기

로그인한 사용자는 DLP 사용자 작업 공간에서 내 승인 모듈을 사용할 수 있습니다. 사용자는 여기에서 할당 승인 요청을 승인하거나 거부할 수 있습니다.

시작하기 전에

필요한 역할:

- 최종 사용자
- 관리자
- 승인자

프로시저

1. 다음으로 이동 모두 〉 **DLP** 인시던트 관리 〉 **DLP** 사용자 작업 공간.
   내 **DLP** 인시던트 페이지가 새 탭에 표시됩니다.
2. 내 **DLP** 인시던트 모듈 아래에 있는 내 승인 모듈을 클릭합니다.
   내 승인 목록 뷰가 표시됩니다.

   승인자는 내 승인 페이지의 목록 뷰에서 요청을 승인하거나 거부할 수 있습니다. 한 사람이 목록 뷰에서 여러 요청을 승인하거나 거부할 수 있습니다.

   승인자는 양식 뷰에서 할당된 요청의 상세 정보를 볼 수 있습니다. 양식 뷰에서 승인 또는 거부 작업을 클릭하여 개별 요청을 승인하거나 거부할 수 있습니다.

   주:
   DLP 인시던트 상세 정보를 보려면 승인 필드에 있는 정보 아이콘을 클릭합니다.

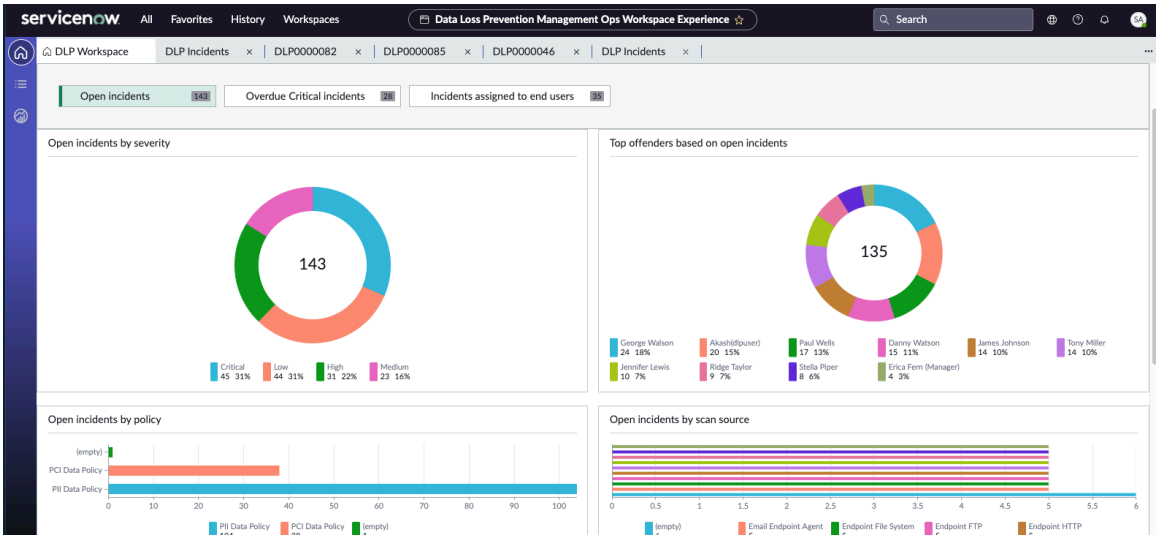
Data Loss Prevention Incident Response 분석가 작업 공간

Data Loss Prevention Incident Response (DLP IR) 분석가 작업 공간을 사용하여 DLP 인시던트를 봅니다. 해결 등을 위해 최종 사용자에게 인시던트를 할당합니다.

DLP 작업 영역은 대시보드, 목록 뷰 및 DLP 인시던트를 모니터링할 수 있는 양식 뷰가 있는 홈페이지로 구성됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

DLP 작업 공간 개요 페이지



DLP 인시던트 검토 및 할당

Data Loss Prevention Incident Response DLP 인시던트를 검토하고 할당하거나 해결할 수 있도록 (DLP IR) 분석가 작업 공간에 액세스합니다. 심각도별 인시던트, 상위 공격자, 검사 소스별 인시던트 및 정책별 인시던트에 대한 추세를 추적할 수 있습니다.

DLP 작업 공간 홈페이지

DLP 작업 공간 개요

시작하기 전에
필요한 역할:

- sn_dlir.analyst - DLP 인시던트를 편집하고 봅니다.
- sn_dlir.analyst_read 및 sn_dlir.read - DLP 인시던트를 봅니다.

프로시저

1. 다음으로 이동 모두 〉 **DLP** 인시던트 관리 〉 **DLP** 분석가 작업 공간.
   DLP 작업 공간 내 인시던트 운영 목록 페이지가 새 탭에서 열립니다.
2. **DLP** 작업 공간 홈 아이콘을 클릭하여 작업 공간 홈페이지 보기를 확인합니다.
3. 대시보드 위젯을 검토하여 심각도별 인시던트, 상위 공격자, 스캔 소스별 인시던트 및 정책별 인시던트별 추세를 식별합니다.
4. 홈페이지에서 적절한 필터를 클릭하여 다양한 범주별로 위젯을 봅니다.

필터	설명
오픈 인시던트	열려 있는 모든 인시던트를 봅니다.
지연된 중요 인시던트	중요 심각도 레이블이 있고 기한이 지난 인시던트를 봅니다.
최종 사용자에게 할당된 인시던트	최종 사용자에게 할당된 인시던트를 봅니다.

5. 다음 두 가지 방법을 사용하여 DLP 인시던트를 검토하고 할당할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 첫 번째 방법은 검토하려는 DLP 인시던트를 하나 이상 찾아 선택하고 인시던트 옆에 있는 확인란을 클릭하는 것입니다.

b. 자신에게 적합한 옵션을 선택합니다.

옵션	설명
목록 새로 고침	업데이트할 때 DLP 인시던트 목록을 새로 고치는 옵션입니다.
목록 작업	수행할 수 있는 작업 목록입니다. 선택 항목은 다음과 같습니다. ▪ 다른 이름으로 저장 ▪ 열 편집 ▪ 너비 재설정 주: 내 목록 섹션 아래에 작업 공간에 대해 구성된 사용자 지정 목록이 있는 경우 아래의 추가 목록 작업도 수행할 수 있습니다. ▪ 이름 바꾸기 ▪ 저장 ▪ 삭제
모두에 대한 URL 복사	모든 DLP 인시던트의 URL을 복사하는 옵션입니다.
필터 패널 표시	필터 옵션을 사용하여 필요한 인시던트를 드릴다운하는 옵션입니다. **i.** 페이지의 왼쪽 위에 있는 필터를 클릭하고 고급 보기를 선택합니다. **ii.** 기존 필터를 사용하거나 필드, 연산자 및 값이 포함된 조건을 추가하여 직접 빌드합니다. **iii.** 조건을 더 추가하려면 **AND** 또는 **OR**을 클릭합니다. ▪ **AND**를 선택하면 모든 조건이 일치해야 합니다. ▪ **OR**을 선택하면 두 조건을 일치시킬 수 있습니다. **iv.** 업데이트를 클릭합니다.
인시던트 할당	DLP 인시던트를 할당할 대상을 결정하는 작업입니다. 선택 항목은 다음과 같습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵션	설명

	▪ 인시던트 할당 대상: 분석가, 최종 사용자 또는 다른 사람에게 인시던트를 할당하는 옵션입니다.
	▪ 사용자: 인시던트를 할당해야 하는 사용자를 결정하는 옵션입니다.
	▪ 인시던트 상태 사전 사용자 응답: 사용자가 응답하기 전에 인시던트가 어느 상태에 있어야 하는지 결정하는 옵션입니다. 사용자 지정 상태일 수도 있습니다.
	▪ 평가 첨부: 인시던트에 평가를 첨부할지 여부를 나타내는 옵션입니다. 활성화하면 아래 옵션을 사용할 수 있습니다.
	  ▪ 평가 템플릿: DLP 인시던트에 대한 평가 템플릿을 선택하는 옵션입니다.
	  ▪ 인시던트 상태 사전 사용자 응답 사용자가 응답한 후 DLP 인시던트가 있어야 하는 상태를 선택하는 옵션입니다.

응답	인시던트 응답 옵션을 선택하여 인시던트에 응답합니다. 예를 들어 사용자가 DLP 정책을 위반하는 파일을 삭제하는 경우 사용자는 삭제된 파일 옵션을 선택하여 파일이 삭제되었다는 수동 확인을 제출하고 의견을 제공할 수 있습니다. 여기에서 고급 응답 옵션을 선택할 수도 있습니다. (예: 격리에서 이메일 릴리스 요청)
에스컬레이션	인시던트를 에스컬레이션하는 작업입니다. 인시던트를 에스컬레이션할 대상 사용자를 선택하여 인시던트를 에스컬레이션할 수 있습니다. 의견 필드에 추가 정보를 입력할 수도 있습니다.
상태 업데이트	인시던트의 상태를 업데이트하는 작업입니다. 드롭다운 옵션에서 상태 중 하나를 선택하여 인시던트의 상태를 업데이트할 수 있습니다. 사용자 지정 상태일 수도 있습니다.
닫기	인시던트를 종결하는 작업입니다. 드롭다운 목록에서 해당 종결 코드를 선택하고 종결 코멘트를 추가합니다. 의 Data Loss Prevention Incident Response닫기 기능은 목록 뷰에서 비동기 및 동기식으로 수행됩니다. **i.** 동기식 종결: 인시던트를 동기식으로 종결한다는 것은 종결 작업이 즉시 수행됨을 의미합니다. 종결할 인시던트를 여러 개 선택하고 인시던트 수가 100보다 작거나 같으면 DLP 인시던트 목록 뷰에서 인시던트가 전경으로 닫힙니다. 여기서 기본값은 100입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵션	설명
	ii. 비동기 종결: 선택한 인시던트 수가 100보다 큰 경우 종결 요청이 제출되고 애플리케이션이 백그라운드에서 요청을 실행함을 의미합니다. 업데이트된 인시던트 상태를 보려면 DLP 인시던트 목록 뷰를 새로 고쳐야 합니다. 주: ▪ 비동기 또는 동기 종결에 대해 선택한 인시던트 수는 ### ## *sn_dlir.closure_sync_count_limit*를 사용하여 구성됩니다. ▪ 기본적으로 인시던트 수는 100으로 설정됩니다.

c. 두 번째 방법은 특정 DLP 인시던트를 클릭하여 여는 것입니다.

- 상세 정보 탭: 다음 섹션이 표시됩니다.
  - 상세 정보: 인시던트 번호, 심각도, 파일 이름 등과 같은 DLP 인시던트의 상세 정보를 볼 수 있습니다. 심각도, 상태, 최종 사용자 및 DLP 분석가 그룹 필드를 각각 수정하고 저장할 수 있는 기능도 제공됩니다.
  - 작성: 모든 사람에게 표시되는 DLP 인시던트에 대한 설명을 추가하려면 설명 탭에 설명을 입력합니다. 특정 사용자에게 표시되는 설명을 추가하려면 작업 메모(비공개) 탭에 설명을 입력합니다.
  - 활동: DLP 인시던트에서 다양한 활동의 상세 정보를 볼 수 있습니다.
  - 첨부 파일: DLP 인시던트와 관련된 첨부 파일이 있는 경우 찾아보기 를 클릭하고 로컬 드라이브에서 첨부 파일을 선택합니다.
- 추가 상세 정보 탭: 사용자 지정 필드를 포함하여 DLP 인시던트에 대한 모든 추가 정보를 표시합니다.

  중요사항:
  - DLP 인시던트에 대한 사용자 지정 필드는 San Diego 버전 이상에서만 지원됩니다.
  - 추가 상세 정보 탭을 사용하여 특정 DLP 인시던트에 대해 사용자 지정 필드가 만들어졌는지 여부를 확인할 수 있습니다.

- 사용자 지정 속성 탭: DLP 인시던트와 관련된 사용자 지정 속성 목록을 표시합니다.
- 최종 사용자의 다른 인시던트: 동일한 최종 사용자의 인시던트를 표시합니다. 이 관련 목록에서 하위 인시던트로 추가 작업을 수행하여 인시던트를 통합할 수 있습니다.
- 탐지된 중요한 정보 유형: 인시던트에서 탐지된 중요한 정보를 표시합니다.

  주:
  이 관련 목록은 Microsoft 또는 Symantec 통합용으로 생성된 DLP 인시던트에 대해서만 표시됩니다. Microsoft 또는 Symantec 인시던트 기록 내에서 사용자가 탐지된 중요한 정보 유형 기록에 액세스할 때마다 해당 통합과 관련하여 강조 표시된 일치 컨텐츠가 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 하위 인시던트: 수동으로('하위 인시던트로 추가' 작업 수행) 또는 DLP 통합 규칙에서 생성된 하위 인시던트를 표시합니다. 이 관련 목록에서 '하위 인시던트 연결 해제'를 수행하여 하위 인시던트의 연결을 해제할 수 있습니다.
- 복제된 인시던트: 상위 인시던트에서 복제된 인시던트를 표시합니다. 양식 뷰의 인시던트 복제 작업을 클릭하여 새 복제된 인시던트를 만들 수 있습니다.
- 평가 탭: DLP 인시던트에 할당된 평가 목록을 표시합니다.

d. 자신에게 적합한 옵션을 선택합니다.

옵션	설명

인시던트 할당	DLP 인시던트를 할당할 대상을 결정하는 작업입니다. 선택 항목은 다음과 같습니다.
	▪ 인시던트 할당 대상: 분석가, 최종 사용자 또는 다른 사람에게 인시던트를 할당하는 옵션입니다.
	▪ 사용자: 인시던트를 할당할 사용자를 선택하는 옵션입니다.
	▪ 인시던트 상태 사전 사용자 응답: 사용자가 응답하기 전에 인시던트가 있어야 하는 상태를 선택하는 옵션입니다. 사용자 지정 상태일 수도 있습니다.
	▪ 평가 첨부: 인시던트에 평가를 첨부할지 여부를 나타내는 옵션입니다. 활성화하면 아래 옵션을 사용할 수 있습니다.
	  ▪ 평가 템플릿: DLP 인시던트에 대한 평가 템플릿을 선택하는 옵션입니다.
	  ▪ 사용자 응답 게시 인시던트 상태: 사용자가 응답한 후 DLP 인시던트가 있어야 하는 상태를 선택하는 옵션입니다.

승인 취소	승인 요청을 취소하는 작업입니다. 이 작업은 DLP 인시던트가 승인 보류 중 상태인 경우에만 양식 뷰에서 분석가에게 표시됩니다. 사용 가능한 옵션은 다음과 같습니다. ▪ 인시던트 할당 대상: 인시던트를 다른 사람, 분석가 또는 다른 사람에게 할당하지 않는 옵션입니다. ▪ 사용자: 인시던트를 할당할 사용자를 선택하는 옵션입니다. ▪ 취소 후 인시던트 상태: 요청을 취소한 후 인시던트가 있어야 하는 상태를 선택하는 옵션입니다. ▪ 의견: 취소에 대한 추가 세부 정보를 제공합니다.

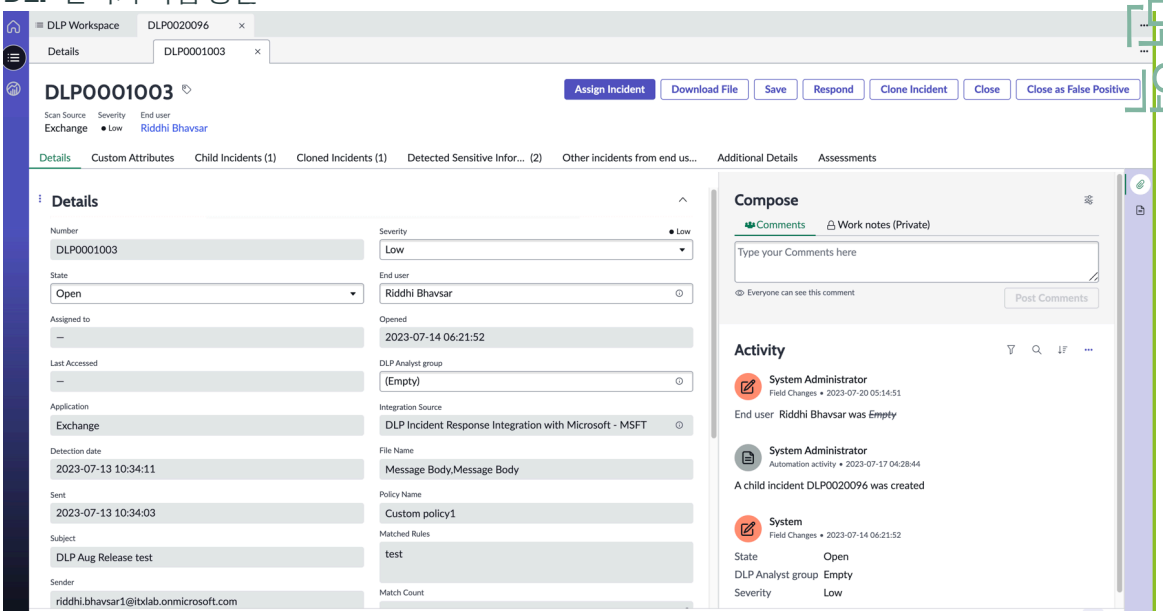
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵션	설명
평가 할당	인시던트를 할당하는 동안 평가를 첨부하는 작업입니다. 선택 항목은 다음과 같습니다. ▪ 평가 템플릿: DLP 인시던트에 대한 평가 템플릿을 선택하는 옵션입니다. ▪ 사용자 응답 게시 인시던트 상태: 사용자가 응답한 후 DLP 인시던트가 있어야 하는 상태를 선택하는 옵션입니다.
파일 다운로드	위반 컨텐츠가 있는 파일 또는 이메일을 다운로드하는 작업입니다. 이 작업은 Microsoft OneDrive, SharePoint Online 또는 Exchange Online용으로 생성된 인시던트에 대해 수행할 수 있습니다.
저장	변경한 내용을 저장하는 작업입니다. DLP 인시던트의 심각도, 상태 및 최종 사용자 필드를 수정하고 저장할 수 있는 옵션이 있습니다.
응답	인시던트 응답 옵션을 선택하여 인시던트에 응답합니다. 예를 들어 사용자가 DLP 정책을 위반하는 파일을 삭제하는 경우 사용자는 삭제된 파일 옵션을 선택하여 파일이 삭제되었다는 수동 확인을 제출하고 의견을 제공할 수 있습니다. 여기에서 고급 응답 옵션을 선택할 수도 있습니다. 예: 격리에서 이메일 릴리스를 요청합니다.
에스컬레이션	인시던트를 에스컬레이션하는 작업입니다. 인시던트를 에스컬레이션할 대상 사용자를 선택하여 인시던트를 에스컬레이션할 수 있습니다. 의견 필드에 추가 정보를 입력할 수도 있습니다.
인시던트 복제	인시던트 기록이 여러 사용자에게 영향을 주는 경우 복제 인시던트를 생성하는 작업입니다. 복제된 인시던트를 법무/IT 등 여러 이해 관계자에게 할당할 수 있습니다. 복제 인시던트 기록을 만들면 상위 DLP 인시던트 아래에 새 복제된 인시던트 탭이 생성되고 모든 복제된 인시던트가 이 뷰에 나열됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵션	설명
	주: ▪ 상위 DLP 인시던트 기록이 종결되면 복제된 모든 인시던트 기록이 자동으로 종결됩니다. ▪ DLP 인시던트 기록에 복제된 인시던트가 포함되어 있는 경우 최종 사용자에게 할당할 수 없습니다. 상위 DLP 인시던트 기록은 분석가 역할을 가진 사용자만 관리할 수 있습니다. ▪ 기본 구성 모듈에서 복제된 인시던트의 상태에 따라 상위 상태를 자동으로 업데이트하는 옵션도 있습니다. 예를 들어 복제된 모든 인시던트가 에스컬레이션됨 상태로 이동하면 상위 인시던트도 에스컬레이션됨 상태로 이동합니다.
닫기	인시던트를 종결하는 작업입니다. 드롭다운 목록에서 해당 종결 코드를 선택하고 필요한 경우 종결 코멘트를 추가해야 합니다.
긍정 오류로 종결	인시던트를 긍정 오류로 종결하는 작업입니다. 인시던트를 종결하기 전에 코멘트를 추가할 수도 있습니다.

DLP 분석가 작업 공간



6. 페이지 왼쪽 위로 이동하여 목록 탭을 클릭하면 홈페이지에서 목록 뷰를 볼 수 있습니다. 목록 범주는 DLP 인시던트에 대한 기본 목록 페이지와 사용자 지정된 목록 페이지로 구성됩니다.
   - 목록 탭: DLP 인시던트의 기본 목록입니다. 다음은 기본 목록입니다.
     - 모두
     - 오픈

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

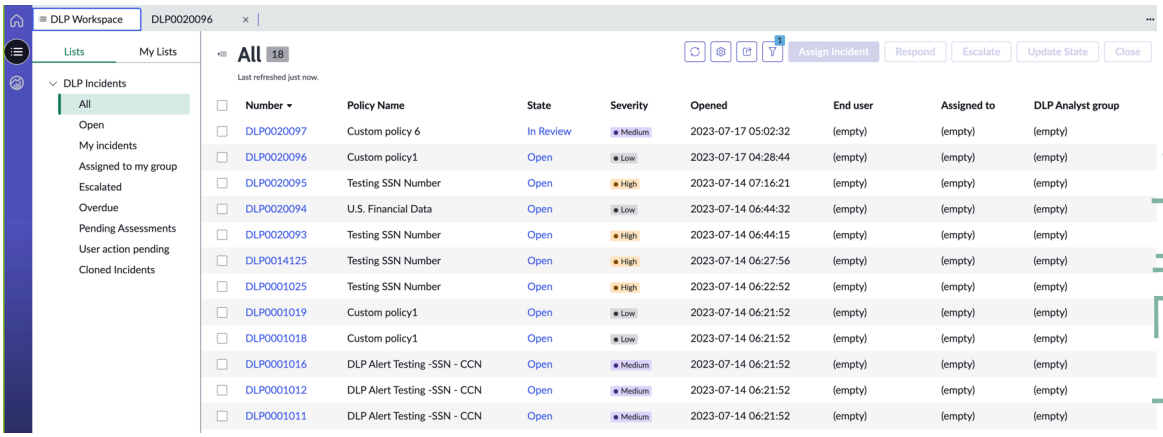
- 내 인시던트
- 내 그룹에 할당
- 에스컬레이션됨
- 지연
- 보류 중인 평가
- 사용자 작업 보류 중
- 복제된 인시던트
- 보관된 인시던트

○ 내 목록 탭: 이름을 변경한 모든 목록과 사용자가 만든 모든 목록을 표시합니다.

Example

다음 예제에서는 목록 보기 범주가 있는 DLP 작업 영역을 보여 줍니다. 모든 목록 뷰 옵션이 선택되어 있습니다.

DLP 분석가 작업 공간 목록 뷰



증거 파일 미리 보기

DLP IR 분석가 작업 공간에서 증거 파일을 미리 봅니다 Data Loss Prevention Incident Response .

시작하기 전에

중요사항:
DLP 분석가 작업 공간에서 증거 파일 작업을 사용하는 동안 증거 파일은 임시로 암호화되지 않은 형식으로 ServiceNow 데이터베이스에 저장됩니다. 증거 파일을 저장하지 않으려면 증거 파일 미리 보기 기능을 사용하지 않도록 설정합니다. 자세한 내용은 고급 설정 구성 문서를 참조하십시오.

필요한 역할: sn_dlir.analyst

프로시저

1. 다음으로 이동 모두 〉 **DLP** 인시던트 관리 〉 **DLP** 분석가 작업 공간.
2. DLP 인시던트 기록을 엽니다.
3. 상황별 사이드바에서 증거 파일 아이콘( )을 선택합니다.
4. 증거 파일 탭에서 증거 파일 카드를 선택하여 문서 뷰어에서 증거 파일을 미리 봅니다.

   미리 보기 기능은 다음 표에 나와 있는 것처럼 파일 형식마다 다릅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

파일 형식	파일 확장명
이미지	.bmp, .gif, .ico, .jpeg, .jpg, .png, .svg 및 .webp. 이미지 파일은 문서 뷰어 모드에서 열립니다.
Microsoft Office 파일	.doc, .docx, .ppt, .pptx, .xls, .xlsx Office 파일이 문서 뷰어 모드에서 열립니다.
텍스트 파일	.txt 텍스트 파일은 텍스트 편집기 모드에서 열립니다.
메일 파일	.eml 주: 파일 크기는 5MB 미만이어야 합니다. 콘텐츠를 미리 보려면 먼저 파일을 다운로드해야 합니다.
PDF 파일	.pdf ○ 키워드를 입력하여 문서를 검색합니다. ○ 확대 및 축소 기능으로 보기를 조정하여 가독성을 높입니다. ○ 페이지를 시계 방향 또는 시계 반대 방향으로 회전하면 내용을 더 선명하게 볼 수 있습니다.

주:

이진 파일은 렌더링되지 않으며 콘텐츠를 미리 보려면 다운로드해야 합니다. 증거 파일 미리 보기 기능은 보관된 인시던트에도 사용할 수 있습니다.

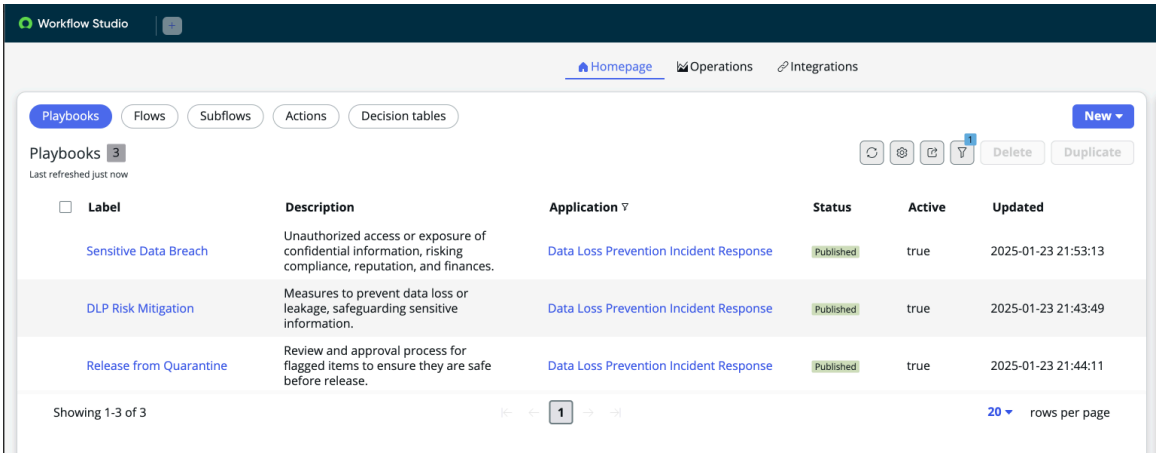
다음을 위한 플레이북 **Data Loss Prevention Incident Response**

Data Loss Prevention Incident Response Playbook은 조직의 보안을 손상시킬 수 있는 민감한 정보의 무단 노출, 유출 또는 침해를 포함할 수 있는 데이터 손실 인시던트를 해결하고 완화하기 위한 단계별 가이드입니다.

다음 이미지는 DLP IR에 사용할 수 있는 샘플 플레이북을 보여 줍니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

DLP Incident Response용 샘플 플레이북



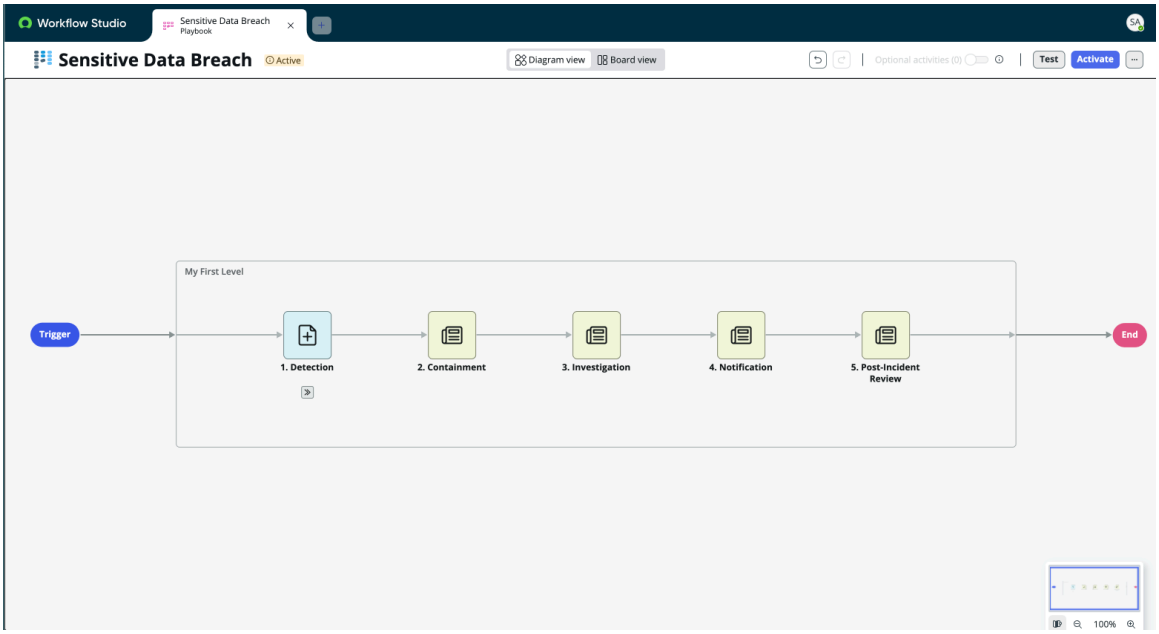
다음 표에는 DLP 플레이북을 만드는 데 사용할 수 있는 활동과 스테이지가 나와 있습니다. 자세한 내용은 다음을 참조하십시오 DLP 플레이북 추가.

활동	설명
탐지	민감한 데이터에 대한 무단 액세스 또는 노출을 식별하고 확인합니다.
방지	영향을 받는 시스템 또는 사용자를 격리하여 추가 데이터 유출 또는 무단 액세스를 방지합니다.
조사	위반을 조사하여 발생 경위, 영향을 받은 데이터, 잠재적 영향을 파악합니다.
알림	법률 또는 정책에서 요구하는 경우 내부 팀, 외부 이해 관계자 및 규제 기관에 알립니다.
정정	취약성을 해결하고, 정책을 업데이트하고, 향후 위반을 방지하기 위한 시정 조치를 적용합니다.
복구	보안 백업에서 시스템을 복원하고 인시던트 발생 후 데이터 무결성을 검증합니다.
사후 인시던트 검토	인시던트를 분석하여 근본 원인을 식별하고, 보안 제어를 개선하고, 정책을 강화합니다.

다음 그림은 중요한 데이터 위반 플레이북 생성과 관련된 활동 및 스테이지의 워크플로우를 보여줍니다. 플레이북 단계는 워크플로우에 따라 달라집니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

플레이북 설계 워크플로우



관련 정보

DLP 플레이북 추가

DLP 플레이북 취소

DLP 플레이북 추가

분석가 작업 공간에 조직의 보안을 손상시킬 수 있는 데이터 손실 인시던트를 해결하고 완화하기 위한 가이드 역할을 할 수 있는 플레이북 Data Loss Prevention Incident Response 을 추가합니다.

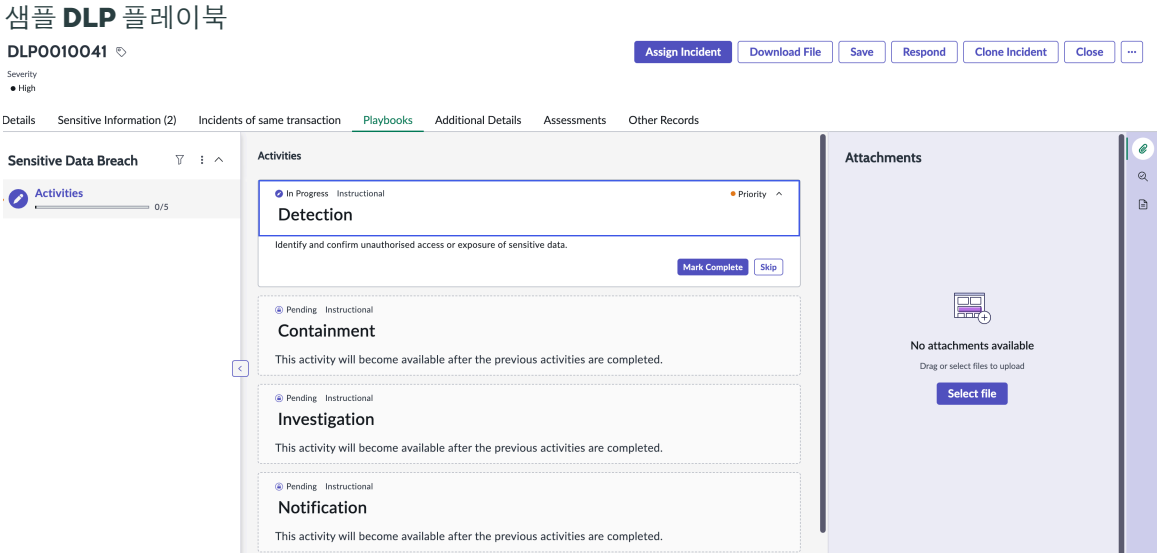
시작하기 전에
필요한 역할: sn_dlir.analyst - DLP 작업 공간에서 플레이북을 추가하거나 봅니다.

프로시저

1. 다음으로 이동 모두 〉 **DLP** 인시던트 관리 〉 **DLP** 분석가 작업 공간.
2. DLP 분석가 작업 공간 - 내 인시던트 페이지에서 DLP 인시던트를 엽니다.
3. 플레이북을 추가합니다.
   a. 플레이북 탭으로 이동합니다.
   b. UI 작업 메뉴에서 추가 작업 아이콘(.)을 선택하고 플레이북 추가를 선택합니다.
   c. 대화 상자의 드롭다운 메뉴에서 플레이북을 선택합니다.
   d. 플레이북 추가를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 각 레인을 선택하여 이 플레이북이 수행하는 작업을 탐색합니다.



DLP 플레이북 취소

더 이상 유효하지 않은 비즈니스 플로우를 중지하려면 플레이북을 취소합니다 Data Loss Prevention Incident Response .

시작하기 전에

> **주:**
> 연결된 DLP 인시던트가 종결되면 플레이북이 자동으로 취소됩니다.

필요한 역할: sn_dlir.admin.

프로시저

1. 다음으로 이동 모두 〉 **DLP** 인시던트 관리 〉 **DLP** 분석가 작업 공간.
2. DLP 인시던트를 엽니다.
3. 플레이북 탭으로 이동합니다.
4. 취소하려는 플레이북의 헤더에서 플레이북 작업 아이콘(⋮)을 선택한 다음 플레이북 취소를 선택합니다.
5. 플레이북 취소 이유를 제공합니다.
6. 플레이북 취소를 선택합니다.

결과

플레이북 헤더 아래에 플레이북이 취소되었음을 확인하는 배너가 나타납니다.

보관된 DLP 인시던트 보기

DLP 분석가 작업 공간을 사용하여 보관된 DLP 인시던트 보기

시작하기 전에

필요한 역할:

- sn_dlir.analyst - DLP 인시던트를 편집하고 봅니다.
- sn_dlir.analyst_read 및 sn_dlir.read - DLP 인시던트를 봅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 **DLP** 인시던트 관리 〉 **DLP** 분석가 작업 공간.
   기본적으로 내 인시던트 섹션이 표시됩니다.
2. 보관된 인시던트를 클릭합니다.
   보관된 DLP 인시던트 목록이 표시됩니다.
3. 보관된 인시던트 수를 보려면 인시던트 수 표시 버튼을 클릭합니다.

   주:

   - 기본적으로 보관된 인시던트 수는 목록 로드 시간을 개선하기 위해 숨겨집니다. 인시던트 수를 보려면 인시던트 수 표시 버튼을 클릭해야 합니다. 또한 인시던트 수를 보여주는 정보 메시지가 표시됩니다.
   - 보관된 인시던트에 대해 시스템 속성 glide.ui.list.seismic.omit.count가 기본 시스템에서 활성화되어 인시던트 목록 수를 숨깁니다.

4. 보려는 DLP 인시던트를 하나 이상 선택합니다.
   DLP 인시던트에 인시던트 상세 정보 섹션이 표시됩니다.

   주:

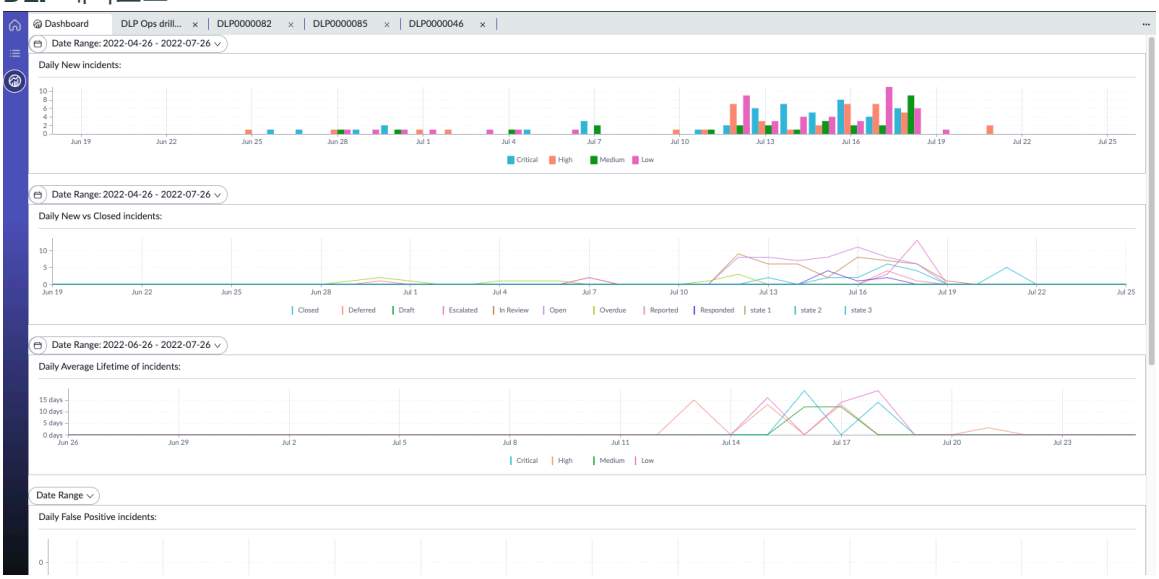
   - 최종 사용자의 기타 인시던트 탭에는 보관된 인시던트도 포함됩니다.
   - 컨텐츠 일치 는 보관된 모든 인시던트에 대해 지원되지만(모든 통합에서도 지원됨) 파일 다운로드 는 Microsoft 통합에 대해서만 지원됩니다.

Data Loss Prevention Incident Response 대시보드

(DLP IR) 대시보드는 Data Loss Prevention Incident Response 인스턴스의 DLP 인시던트 및 일일 인시던트 추세에 대한 개략적인 개요를 그래픽 차트 형식으로 제공합니다. 이러한 차트는 DLP 인시던트를 효과적으로 보고, 관리하고, 정정하는 데 도움이 됩니다.

대시보드는 Data Loss Prevention Incident Response 매일 DLP 인시던트에 대한 주요 인사이트를 제공합니다. 표시기를 설정하고 표시기 속성의 조건과 일치하는 인시던트의 데이터 스냅샷을 정기적으로 수집할 수 있습니다. 수집된 데이터는 대시보드의 위젯을 사용하여 시각화됩니다. DLP 인시던트를 서로 다른 시간 간격으로 분석하려면 서로 다른 날짜 범위를 적용할 수 있습니다.

DLP 대시보드



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

DLP 인시던트의 일일 인시던트 추세 분석

(DLP IR) 대시보드에 Data Loss Prevention Incident Response 액세스하여 DLP 인시던트의 일일 추세를 분석하고 효과적으로 정정합니다.

시작하기 전에

필요한 역할:

- sn_dlir.analyst - DLP 인시던트를 편집하고 봅니다.
- sn_dlir.analyst_read 및 sn_dlir.read - DLP 인시던트를 봅니다.

이 태스크 정보

DLP 대시보드에서 위젯을 사용하여 일일 추세를 시각화할 수 있습니다. DLP 인시던트의 일일 추세에 대한 데이터 또는 통계는 조직에서 정의한 일일 인시던트 표시기 속성에서 수집됩니다. 다음 차트에 대해 서로 다른 시간 간격으로 DLP 인시던트를 분석하기 위해 다양한 데이터 범위를 적용하여 주요 인사이트를 얻을 수 있습니다.

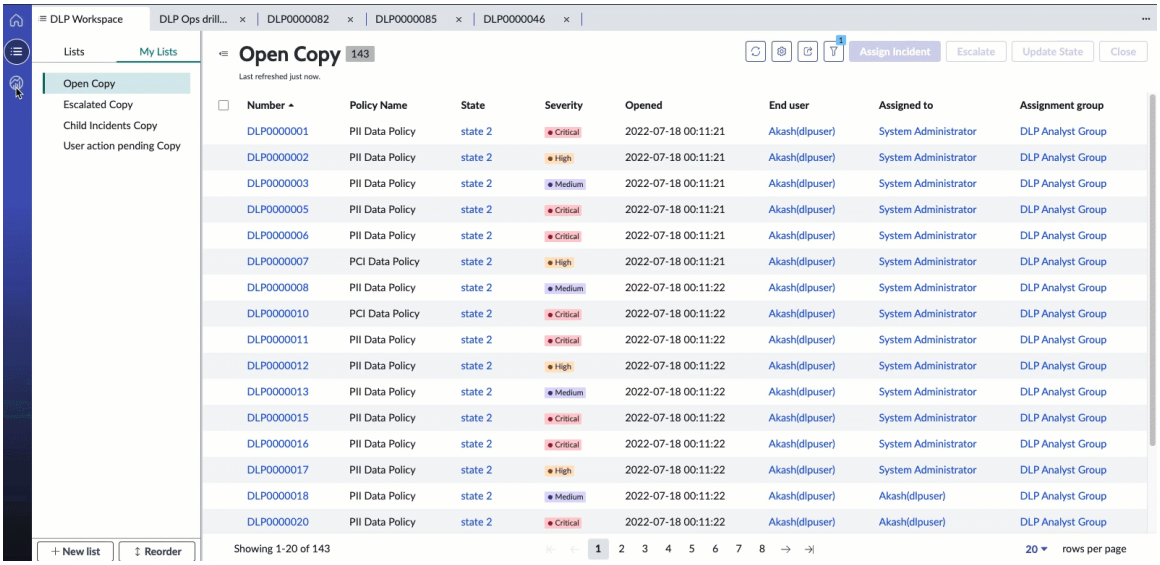
- 일일 신규 인시던트: 인시던트의 상태와 관계없이 매일 생성된 전체 DLP 인시던트에 대한 데이터입니다. DLP 인시던트는 중간, 중요, 높음 및 낮음 등의 심각도에 따라 분류됩니다. 각 DLP 인시던트 심각도는 차트에서 특정 색으로 표시됩니다.
- 일일 신규 인시던트 대 종결된 인시던트: DLP 인시던트의 다양한 상태와 일일 신규 인시던트와 일일 종결 인시던트 간의 비교입니다. 일일 신규 범주에는 오픈, 초안, 에스컬레이션됨, 검토 중, 기한 초과, 보고됨, 응답됨 또는 사용자 지정(있는 경우) 상태의 모든 DLP 인시던트가 포함됩니다. 종결된 인시던트 범주에는 종결된 DLP 인시던트가 포함됩니다. 각 DLP 인시던트 상태는 차트에서 특정 색으로 표시됩니다.
- 인시던트의 일일 평균 수명: 인시던트의 수명은 특정 DLP 인시던트의 시작과 종결 사이의 기간입니다. 일일 평균 수명은 종결된 DLP 인시던트에 대해서만 계산됩니다.
- 일일 가양성 인시던트: 일일 가양성으로 보고된 모든 DLP 인시던트의 데이터입니다. 일일 가양성 인시던트는 중간, 중요, 높음 및 낮음을 포함한 심각도에 따라 분류됩니다. 각 일일 가양성 인시던트 심각도는 차트에서 특정 색으로 표시됩니다.
- 인시던트의 경과 기간 대 심각도: 기간별로 분류되고 DLP 인시던트의 심각도로 구성된 모든 DLP 인시던트의 데이터 비교입니다. 연령 범주에는 조직에서 정의하는 연령 미만의 모든 DLP 인시던트가 포함됩니다. 연령 차트에 대한 자세한 내용은 을 참조하십시오 연령 차트 구성 생성. 인시던트 심각도에는 높음 또는 낮음 범주의 모든 DLP 인시던트가 포함됩니다. 각 심각도는 차트에서 특정 색으로 표시됩니다.
- 일별 에스컬레이션된 인시던트: 일별 에스컬레이션된 모든 DLP 인시던트의 데이터입니다. 일별 에스컬레이션된 인시던트는 중간, 중요, 높음 및 낮음을 포함한 심각도에 따라 분류됩니다. 매일 에스컬레이션되는 각 인시던트 심각도는 차트에서 특정 색으로 표시됩니다.

프로시저

1. 다음으로 이동 모두 〉 **DLP** 인시던트 관리 〉 **DLP** 대시보드.
   내 DLP 대시보드 페이지가 새 브라우저 탭에 표시됩니다.
2. 일일 추세 분석을 수행할 대시보드 위젯을 선택합니다.
   예를 들어 일일 신규 인시던트 차트가 있습니다.
3. 대시보드 위젯을 검토하여 추세를 식별합니다.
4. 날짜 범위를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

DLP 대시보드 개요



5. 달력에서 날짜 범위를 선택하고 적용을 클릭합니다.

Example
예를 들어 선택한 데이터 범위에 대해 일일 신규 인시던트 차트가 업데이트됩니다.

6. 차트 아래의 필터를 사용하여 드릴다운하고 더 심층적인 분석을 수행합니다.

를 위한 인바운드 통합 **Data Loss Prevention Incident Response**

인바운드 REST API를 사용하여 하나 또는 여러 개의 DLP 인시던트를 생성합니다.

단일 **DLP** 인시던트 만들기

필요한 역할: sn_dlir.api_integration_user

단일 DLP 인시던트를 만들려면 필요에 따라 다음 매개변수를 정의합니다.

필드	설명
HTTP 메서드	##
URL	https://{instance}/api/now/import/sn_dlir_incident_import
요청 헤더	받아들이다: *application/json* 콘텐츠 유형: *application/json*
샘플 페이로드	{ "application_window_title": "<value>", "assigned_to": "<value>", "attachments": "<value>", "data_owner_email": "<value>", "destination": "<value>", "dest_ip": "<value>", "dest_ip_port": "<value>",

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	"detection_date": "<value>", "endpoint_on_corporate_net": "<value>", "files": "", "file_created": "", "file_created_by": "", "file_location": "", "file_modified_by": "", "file_name": "", "file_owner": "", "file_permissions": "", "ftp_user_name": "", "last_modified": "", "machine_ip": "", "machine_name": "", "match_count": "", "policy_id": "", "policy_name": "", "printer_name": "", "printer_type": "", "print_job_name": "", "recipients": "", "scanned_machine": "", "scan_source": "", "seen_before": "", "sender":"", "source":"", "source_file":"", "source_ip":"", "source_ip_port":"", "subject":"", "url":"", "user_justification":"" }

샘플 응답	{
	"import_set": "ISET0010003",
	"staging_table": "sn_dlir_incident_import",
	"result": [
	{
	"transform_map": "",
	"table": "sn_dlir_incident",
	"display_name": "number",
	"display_value": "DLP0001012",
	"record_link":
	"https://{instance}/api/now/table/sn_dlir_incident/7cda322297c2411056a43d1e6253af1f",
	"status": "inserted",
	"sys_id": "7cda322297c2411056a43d1e6253af1f"
	}
	]
	}

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

여러 DLP 인시던트 만들기

필요한 역할: sn_dlir.api_integration_user

동일한 요청에서 여러 DLP 인시던트를 만들려면 필요에 따라 다음 매개변수를 정의합니다.

필드	설명
HTTP 메서드	##
URL	https://{instance}/api/now/import/sn_dlir_incident_import/insertMultiple
요청 헤더	받아들이다: *application/json* 콘텐츠 유형: *application/json*

샘플 페이로드	{
	"records": [
	{
	"file_name": "<value>",
	"file_modified_by": "<value>",
	"work_notes": "<value>",
	"url": "<value>",
	"scan_source": "<value>",
	"data_owner_email": "<value>",
	"file_created_by": "<value>",
	"file_owner": "<value>",
	"policy_name": "<value>"
	},
	{
	"dest_ip": "<value>",
	"dest_ip_port": "<value>",
	"detection_date": "<value>",
	"endpoint_on_corporate_net": "<value>",
	"files": "<value>",
	"file_created": "<value>",
	"file_created_by": "<value>",
	"file_location": "<value>",
	"file_modified_by": "<value>",
	"file_name": "<value>",
	"file_owner": "<value>",
	}
	]
	}

샘플 응답	{
	"import_set_id": "a38f69229734dd1056a43d1e6253af75",
	"multi_import_set_id":
	"e78f69229734dd1056a43d1e6253af75"
	}

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
기본적으로 변환은 비동기적입니다. 동기 변환을 설정하려면 REST Insert Multiples (sys_rest_insert_multiple) 테이블에 새 레코드를 만들고, 원본 테이블을 **sn_dlir_incident_import**으로 선택하고, 변환을 동기로 설정합니다.

DLP 통합

기본 시스템에는 Data Loss Prevention Incident Response 타사 데이터 손실 방지 소프트웨어 패키지에 대한 통합이 포함됩니다.

이 섹션에서는 플러그인을 활성화하고 타사 통합을 구성 ServiceNow 하기 위한 지침을 제공합니다. 또한 자체 통합을 개발하기 위한 몇 가지 기본 지침과 기본 시스템에 포함된 특정 통합에 대한 세부 정보가 포함되어 있습니다.

통합 구성

기본 시스템에는 활성화하고 사용할 수 있는 각 통합 구현에 대한 일련의 카드가 포함되어 있습니다. 또한 플러그인에 종속되어 보안 운영 있는 ServiceNow Store에 게시된 모든 통합에 대한 카드가 표시됩니다. 통합 카드는 선택하여 볼 수 있습니다. 보안 운영 〉 통합 구성.

Data Loss Prevention Incident Response 는 다음과 같은 타사 데이터 손실 방지 소프트웨어 패키지를 지원합니다.

Symantec 통합을 위한 Data Loss Prevention Incident Response

DLP 통합은 Symantec 배포 시 생성된 인시던트의 Data Loss Prevention Incident Response 수집을 Symantec Data Loss Prevention Incident Response 지원합니다. 수집 후 인시던트 관리 기능을 사용하여 DLP 인시던트를 정정할 수 있습니다.

스토어에서 앱 요청

ServiceNow Store 웹 사이트를 방문하면 사용 가능한 모든 앱을 확인하고 스토어에 요청을 제출하는 방법에 대한 정보를 참조할 수 있습니다. 출시된 모든 앱의 누적 릴리스 정보는 ServiceNow Store 버전 기록 릴리스 정보 를 참조하십시오.

개요 및 주요 기능

DLP 통합은 Symantec 기업이 다양한 플랫폼에서 민감한 데이터의 사용 및 이동을 추적하는 데 도움이 됩니다.

이 통합에는 다음과 같은 주요 기능이 포함됩니다.

- 서로 다른 Symantec API 엔드포인트에 대해 여러 통합 프로필을 생성하는 기능.
- 인스턴스에서 인스턴스 ServiceNow 로 DLP 인시던트의 Symantec 예약된 수집입니다.
- API 필터를 적용하여 필터 기준과 일치하는 인시던트를 검색하고 임포트해야 하는 DLP 인시던트에 대한 Symantec 필터도 지정하는 기능입니다.
- 인스턴스의 DLP 인시던트 상태를 ServiceNow 의 SymantecDLP 인시던트 상태에 매핑합니다.
- 인스턴스에서 상태가 변경될 ServiceNow 때 인시던트 상태를 Symantec 자동으로 업데이트합니다.
- Symantec DLP 인시던트와 ServiceNow 인시던트 간의 심각도 매핑을 사용자 지정하고 정의하는 능력.

통합에 대한 자세한 내용은 Symantec 제품 설명서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Data Loss Prevention을 Symantec 위한 DLP 통합 시작하기

통합을 사용하려면 먼저 다음 ServiceNow# Store에서 다운로드해야 합니다.

검사 목록

데이터 손실 방지를 위한 DLP 통합 설정을 Symantec 시작하기 전에 다음 정보를 검토합니다.

체크리스트

필드	설명
필요한 ServiceNow AI Platform데이터 손실 방지 애플리케이션, MID 애플리케이션 역할을 할당했는지 확인하십시오.	다음의 DLP 통합에서 Symantec 사용되는 역할은 다음과 같습니다.ServiceNow AI Platform • 관리자(admin)는 데이터 손실 방지 관리자(sn_dlir.admin)에서 ServiceNow# Store 애플리케이션을 설치하고 할당합니다. • sn_dlir.admin 역할을 가진 사용자는 통합을 구성하고 인시던트 프로파일을 설정할 수 있습니다. • sn_dlir.analyst 역할을 가진 사용자는 통합 전반에 걸쳐 읽기 역할을 갖게 됩니다.
필요한 Symantec DLP 사용자 역할을 할당합니다.	Symantec DLP 통합 역할 및 권한을 검토합니다.
DLP 15.8을 사용하고 Symantec 있는지 확인	Symantec Data Loss Prevention을 위한 DLP 통합은 15.8 버전의 Symantec Data Loss Prevention에서 테스트되었습니다. 주: DLP 15.8을 사용하고 Symantec 있는지 확인
ServiceNow# DLP 통합을 지원하는 Symantec 데 필요한 핵심 애플리케이션이 설치되고 활성화되었는지 확인합니다.	다음 DLP 애플리케이션 및 보안 지원 일반 애플리케이션이 ServiceNow Store에서 설치되고 활성화되었는지 확인합니다. 설치되지 않은 경우 애플리케이션에 설치하고 활성화합니다. • Security Support Common • 데이터 손실 방지 인시던트 응답

Data Loss Prevention용 Symantec DLP 통합 설치 및 구성

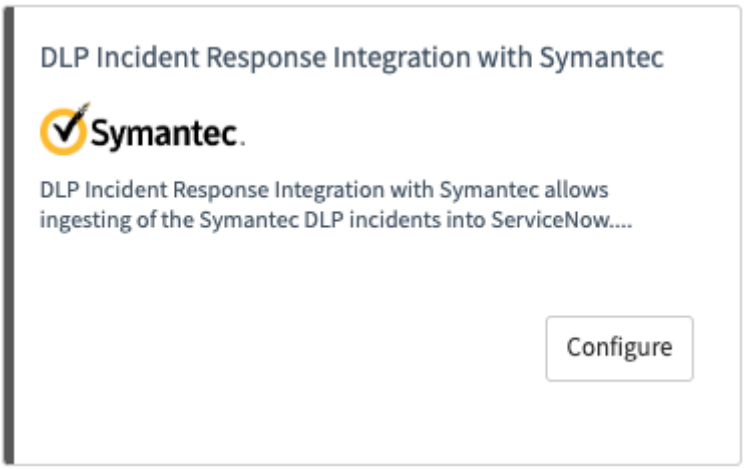
인스턴스에서 DLP 통합을 ServiceNow# StoreServiceNow AI Platform 설치하고 구성합니다Symantec. DLP 인시던트 데이터를 사용하여 Symantec DLP 인시던트 조사를 시작합니다.

시작하기 전에
필요한 역할: sn_dlir.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. Symantec 에서 ServiceNow# Store DLP 통합을 다운로드하여 설치합니다.
2. 다음으로 이동 보안 운영 〉 통합 〉 통합 구성.
3. 타일과 Symantec DLP 인시던트 응답 통합을 검색하고 구성을 클릭합니다.

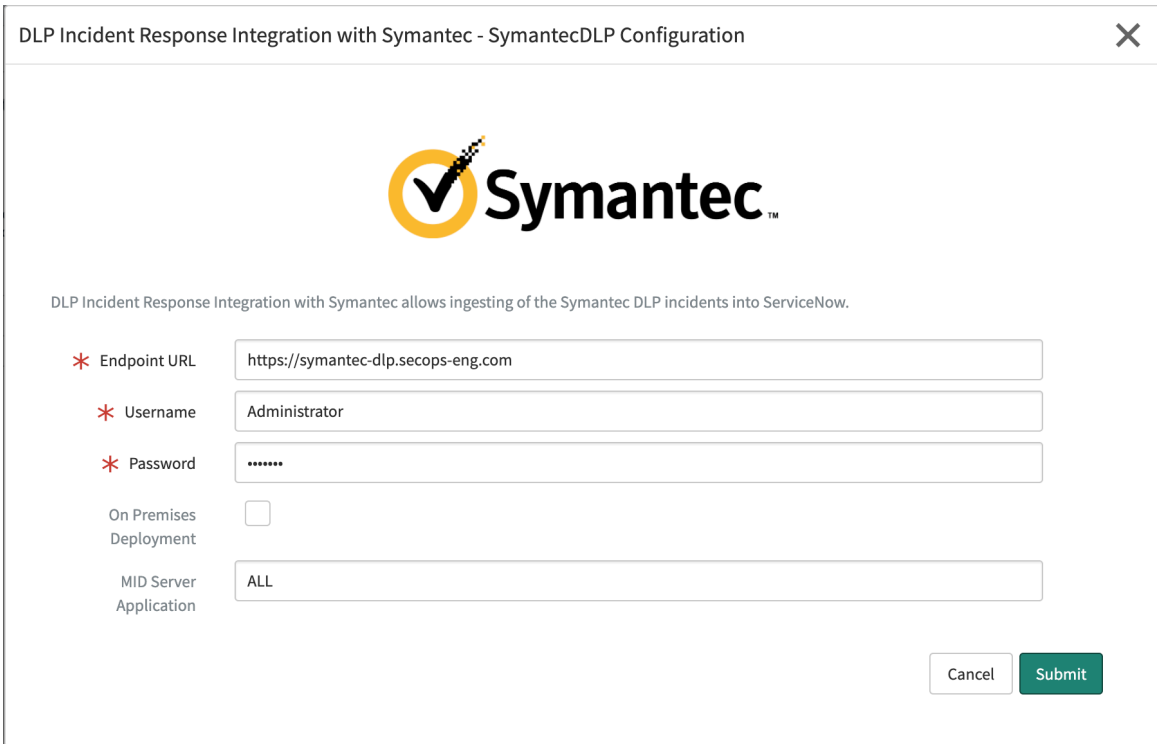


4. 양식에서 필드를 채웁니다.

Symantec DLP 통합 구성 양식

필드	설명
이름	Symantec DLP 통합 구성의 이름입니다.
엔드포인트 URL	Symantec REST API 엔드포인트입니다.
사용자 이름	Symantec 계정 이름입니다. 필요한 역할 및 권한에 대한 자세한 내용은 역할 및 권한을 참조하십시오.
암호	Symantec 계정 암호.
온프레미스 배포	사용자가 Symantec 온 프레미스 인스턴스에 배포되는 경우 선택할 수 있는 옵션입니다. 이 옵션을 선택하면 MID 서버를 사용하여 Symantec에 연결해야 합니다.
MID 서버 애플리케이션	에 Symantec통신하는 데 사용되는 MID 애플리케이션 이름입니다. 이 필드는 온프레미스 배포 옵션을 선택할 때 필요합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



5. 제출을 클릭합니다.

결과

주:
Symantec 하위 제품을 ServiceNow 하위 제품에 연결하십시오. 계정이 로그아웃되지 않도록 인스턴스 간에 모든 사용자 이름과 암호를 동기화된 상태로 유지합니다.

구성을 성공적으로 확인하고 제출하면 Symantec DLP 통합이 보안 통합 페이지에 타일로 저장됩니다.

DLP 통합을 위한 Symantec 프로파일 생성

인스턴스에 인시던트 프로파일을 ServiceNow AI Platform 생성합니다. DLP 인시던트를 Symantec 만드는 데 적합한 DLP 인시던트를 결정합니다.

시작하기 전에
필요한 역할: sn_dlir.admin

이 태스크 정보
엔드포인트에서 Symantec DLP 인시던트를 가져오도록 구성합니다ServiceNow AI Platform#.
이러한 인시던트를 ServiceNow# 인스턴스에 DLP 인시던트로 저장합니다.

프로시저

1. 다음으로 이동 **Symantec DLP** 통합 〉 인시던트 프로파일.

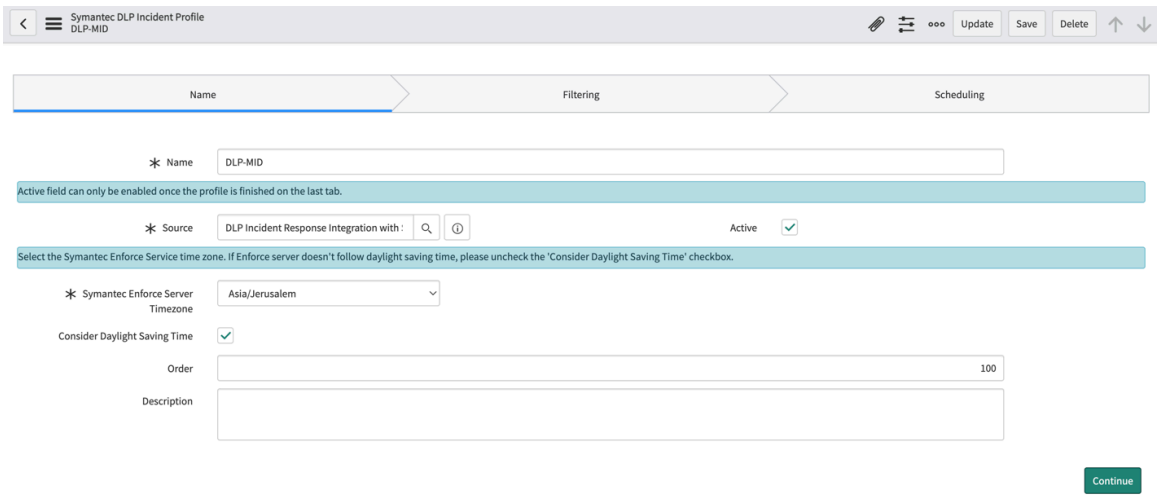
2. 새로 만들기를 클릭합니다.

3. 양식에서 이름 섹션의 필드에 내용을 입력합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로파일 생성

필드	설명
이름	프로필의 이름입니다. 이 필드는 프로파일을 식별하는 데 도움이 됩니다. **주:** 각 프로파일 이름은 고유해야 합니다.
소스	Symantec 인시던트를 수집하도록 구성한 DLP 인스턴스입니다. 여러 인스턴스가 구성된 경우 프로파일에 대해 수집하려는 인시던트 유형에 적합한 인스턴스를 선택합니다.
활성	프로파일이 활성 상태인지 여부를 나타내는 옵션입니다. 이 필드는 예약 섹션에서 마침 을 클릭한 후에만 활성화할 수 있습니다. 프로파일이 활성 상태이면 DLP 인시던트를 적극적으로 폴링 Symantec 하고 있음을 ServiceNow AI Platform 의미합니다. 필터링 조건이 제공한 일정 매개 변수에 따라 일치하면 해당 DLP 인시던트가 DLP에서 만들어집니다.
Symantec 서버 시간대 적용	시간대 문제로 인해 인시던트를 놓치지 않도록 프로파일에서 Symantec Enforce Server의 시간대를 선택하십시오.
일광 절약 시간제를 적용하는 것이 좋습니다.	적용 서버가 일광 절약 시간제를 따르는 경우 이 확인란을 선택합니다.
순서	프로파일 실행 순서입니다. 순서가 가장 낮은 프로파일이 가장 높은 우선 순위로 간주됩니다. 기본적으로 이 값은 100입니다.
설명	이 프로파일에 대한 고유 설명입니다.



다음에 수행할 작업
필터링 섹션으로 이동하려면 계속을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

인시던트 생성에 적용할 필터 정의

수신 Symantec DLP 인시던트를 드릴다운하도록 필터 조건을 정의하고 설정합니다. 에서 ServiceNow#DLP 인시던트로 생성할 인시던트를 결정합니다.

시작하기 전에

필요한 역할: sn_dlir.admin

이 태스크 정보

필터링을 사용하면 DLP 인시던트를 격리하고 생성하는 DLP 인시던트 수를 제한할 수 있습니다. 추가 필터링 기준이 설정되면 조건과 일치하는 인시던트만 만들어집니다.

프로시저

1. 인시던트 수집에 대한 **API** 기반 필터 확인란을 선택하여 API 필터를 적용하고 필터 기준과 일치하는 인시던트를 검색합니다.
2. API 필터를 추가합니다.
   다음은 API 필터를 보여주는 예시입니다.

```
{
            "operandOne": {
               "name": "incidentStatusName"
            },
            "filterType": "string",
            "operator": "EQ",
            "operandTwoValues": [
               "incident.status.New"
            ]
         }
```

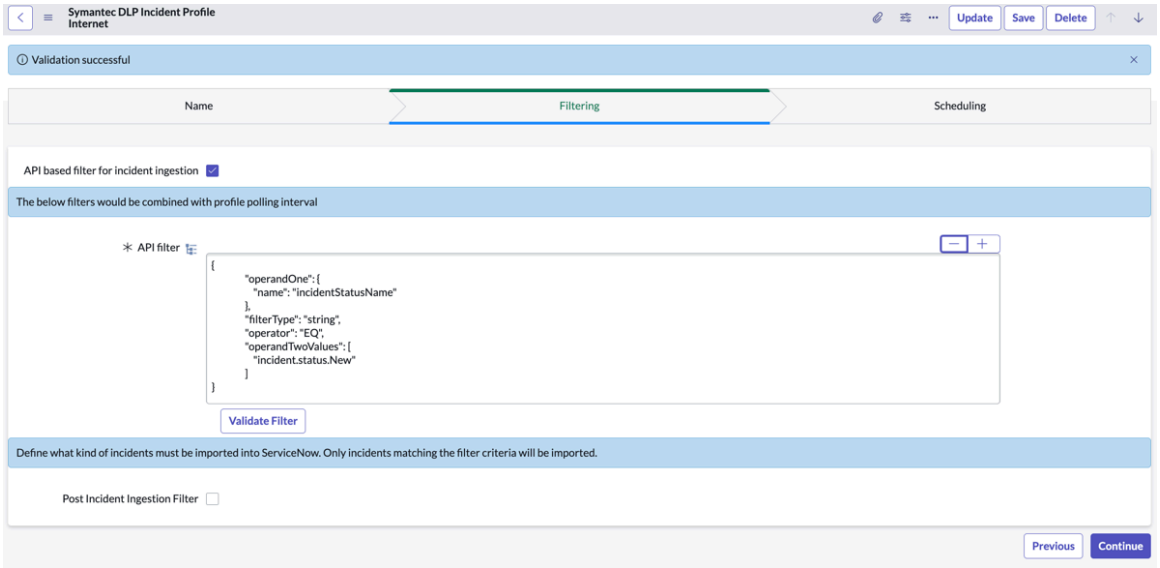
   주:
   Symantec 통합의 API 필터에 대한 자세한 내용은 인시던트 목록: 매개변수 - 요청 객체 상세 정보를 참조하십시오.

3. API 필터를 적용한 후 필터 확인을 클릭합니다.

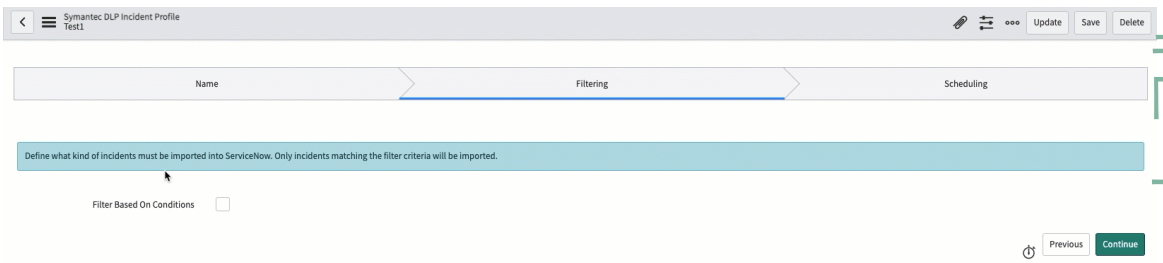
   주:
   유효성 검사에 실패하면 유효성 검사에 실패했다는 오류 메시지가 표시되며 이는 Symantec API에 따라 필터가 제대로 입력되지 않은 경우에 발생합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

API 필터 추가



4. DLP 인시던트가 생성되도록 수신 Symantec DLP 인시던트가 충족해야 하는 기준을 정의하려면 사후 인시던트 수집 필터 확인란을 선택합니다.
   필터 조건의 첫 번째 필드에 있는 옵션은 DLP 인시던트에서 사용할 수 있는 필드와 일치합니다. 입력하는 기준은 대/소문자를 구분합니다. 정의하는 기준이 인시던트의 값과 일치하는지 확인합니다.
5. 조건 작성기에서 필터 조건 필드의 필터를 설정합니다.



6. 조건을 더 추가하려면 **AND** 또는 **OR**을 클릭합니다.
   - **AND**를 선택하면 모든 조건이 일치해야 합니다.
   - **OR**을 선택하면 두 조건을 일치시킬 수 있습니다.

다음에 수행할 작업
일정을 구성하려면 계속을 클릭합니다.

증거 파일 스토리지 구성

DLP 인시던트에 대한 증거 파일을 안전하게 저장하도록 증거 파일 스토리지를 구성합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_dlir.admin

ServiceNow Symantec DLP 통합을 위해 구성 중인 Symantec 사용자가 Symantec DLP 포털의 역할 구성 페이지에서 본문, 첨부 파일 및 원본 메시지 옵션을 사용하도록 설정해야 함을 확인합니다. 자세한 내용은 역할 구성 문서에서 사용할 수 있는 속성 표시 섹션을 참조하십시오.

이 태스크 정보
파일을 안전하게 저장하도록 증거 파일 저장소를 구성할 수 있습니다. 이는 ServiceNow 인스턴스의 내부 저장소에 대한 옵션을 제공하여 파일이 ServiceNow의 필드 암호화. 자세한 내용은 NowPlatform의 필드 암호화 설명서를 참조하십시오.

DLP 분석가가 분석가 작업 공간에서 DLP 인시던트에 대한 증거 파일 다운로드 작업을 수행할 때 증거 파일 스토리지 옵션이 활성화된 경우 선택한 스토리지에서 파일이 다운로드됩니다. 그렇지 않으면 파일이 Symantec 소스에서 직접 다운로드되고 ServiceNow 인스턴스에 유지되지 않습니다.

> **주:**
> DLP 분석가가 분석가 작업 공간에서 DLP 인시던트에 대한 증거 파일 다운로드 작업을 수행할 때 증거 파일 스토리지 옵션이 활성화된 경우 선택한 스토리지에서 파일이 다운로드됩니다. 그렇지 않으면 파일이 Symantec 소스에서 직접 다운로드되고 ServiceNow 인스턴스에 유지되지 않습니다.

프로시저

1. 다음으로 이동 모두 〉 **Symantec DLP** 통합 〉 인시던트 프로파일.
2. 인시던트 프로파일 폼에서 증거 스토리지 섹션을 클릭합니다.
3. 증거 파일 저장소 확인란을 선택하여 파일 저장소를 활성화합니다.
4. 기본 스토리지 유형을 선택합니다.
5. 계속을 클릭하고 예약 섹션으로 이동합니다.

결과
증거 파일은 인시던트 수집이 완료된 후 구성에 따라 저장됩니다.

증거 파일 다운로드

시만텍에서 DLP 정책을 위반하는 DLP 인시던트 증거 파일을 다운로드합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
DLP IR 분석가 작업 영역 및 DLP IR 최종 사용자 작업 영역에서 이 파일을 로컬 컴퓨터로 다운로드합니다. 파일 다운로드 작업은 DLP IR 최종 사용자 작업 공간의 승인자만 사용할 수 있습니다.

필요한 역할:

- sn_dlir.분석가
- sn_dlir.secure_file_download(이 역할이 있는 모든 승인자)

프로시저

1. 다음으로 이동 모두 〉 **Symantec DLP** 통합 〉 설정.
2. 보고된 인시던트의 위반 파일 다운로드가 허용되어야 합니다.
   이 속성을 사용하도록 설정하면 이제 DLP 분석가 작업 공간에서 모든 Symantec DLP 인시던트에 대한 파일 다운로드 작업을 볼 수 있습니다.
3. 다음으로 이동 모두 〉 **DLP** 인시던트 관리 〉 **DLP** 분석가 작업 공간.
4. Symantec 소스에서 수집된 DLP 인시던트 기록을 엽니다.
5. 파일 다운로드를 클릭합니다.

   주:
   Symantec의 DLP 정책을 위반한 파일이 사용자의 로컬 컴퓨터에 다운로드됩니다.

   승인자가 파일 다운로드 작업을 볼 수 있도록 하려면 아래에 언급된 단계를 따르십시오.
6. 다음으로 이동 모두 〉 **DLP** 인시던트 관리 〉 **DLP** 사용자 작업 공간.
   내 DLP 인시던트 페이지가 새 탭에 표시됩니다.
7. 내 DLP 인시던트 모듈에서 사용 가능한 내 승인 모듈을 선택합니다.
   내 승인 목록 뷰가 표시됩니다.
8. Symantec DLP 인시던트에 대해 발생하는 승인 요청 기록을 엽니다.
9. 양식 뷰의 DLP 인시던트 필드에 있는 정보 아이콘(i)을 클릭합니다.
10. 파일 다운로드를 클릭합니다.

결과
이 작업을 수행하면 ZIP 형식의 증거 파일(인시던트가 여러 구성요소에 위반이 있거나 원본 메시지 데이터도 사용할 수 있는 경우) 또는 단일 파일(인시던트에 단일 구성요소에 위반이 있거나 원본 메시지 데이터만 사용할 수 있는 경우)이 사용자의 로컬 머신에 다운로드됩니다.

주:
DLP 관리자는 고급 설정 페이지에서 보고된 인시던트의 위반 파일 다운로드가 허용되어야 함옵션을 사용 중지하여 파일 다운로드 작업에 대한 액세스를 제어할 수 있습니다. 자세한 내용은 Data Loss Prevention Incident Response에 대한 고급 설정 구성을 참조하세요.

증거 파일 미리 보기

DLP IR 분석가 작업 공간에서 증거 파일을 미리 봅니다 Data Loss Prevention Incident Response .

시작하기 전에

중요사항:
DLP 분석가 작업 공간에서 증거 파일 작업을 사용하는 동안 증거 파일은 임시로 암호화되지 않은 형식으로 ServiceNow 데이터베이스에 저장됩니다. 증거 파일을 저장하지 않으려면 증거 파일 미리 보기 기능을 사용하지 않도록 설정합니다. 자세한 내용은 고급 설정 구성 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필요한 역할: sn_dlir.analyst

프로시저

1. 다음으로 이동 모두 〉 **DLP** 인시던트 관리 〉 **DLP** 분석가 작업 공간.
2. DLP 인시던트 기록을 엽니다.
3. 상황별 사이드바에서 증거 파일 아이콘( )을 선택합니다.
4. 증거 파일 탭에서 증거 파일 카드를 선택하여 문서 뷰어에서 증거 파일을 미리 봅니다.

   미리 보기 기능은 다음 표에 나와 있는 것처럼 파일 형식마다 다릅니다.

파일 형식	파일 확장명
이미지	.bmp, .gif, .ico, .jpeg, .jpg, .png, .svg 및 .webp. 이미지 파일은 문서 뷰어 모드에서 열립니다.
Microsoft Office 파일	.doc, .docx, .ppt, .pptx, .xls, .xlsx Office 파일이 문서 뷰어 모드에서 열립니다.
텍스트 파일	.txt 텍스트 파일은 텍스트 편집기 모드에서 열립니다.
메일 파일	.eml 주: 파일 크기는 5MB 미만이어야 합니다. 콘텐츠를 미리 보려면 먼저 파일을 다운로드해야 합니다.
PDF 파일	.pdf ○ 키워드를 입력하여 문서를 검색합니다. ○ 확대 및 축소 기능으로 보기를 조정하여 가독성을 높입니다. ○ 페이지를 시계 방향 또는 시계 반대 방향으로 회전하면 내용을 더 선명하게 볼 수 있습니다.

주:

이진 파일은 렌더링되지 않으며 콘텐츠를 미리 보려면 다운로드해야 합니다. 증거 파일 미리 보기 기능은 보관된 인시던트에도 사용할 수 있습니다.

Symantec DLP 인시던트 검색 예약

인시던트 데이터를 검색하고 프로파일의 기준과 일치하는 DLP 인시던트를 수집 Symantec 하도록 일정을 설정합니다. 에서 인시던트를 Symantec가져오는 방법과 시기를 정의하도록 일정을 구성합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_dlir.admin

이 태스크 정보
인시던트 프로파일 구성과 일치하는 향후 인시던트에 대해 폴링할 빈도를 계획할 수 있습니다. 자동 인시던트 수집을 사용하려면 프로파일을 활성화하기 전에 예약 및 인시던트 검색을 구성해야 합니다. 일회성 검색 확인란을 사용하여 일회성 검색을 수행하도록 프로파일을 구성할 수 있습니다. 이력 날짜는 현재 날짜로부터 최근 3개월까지입니다.

폴링 간격은 각 프로파일에 대해 개별적으로 구성됩니다. 폴링 간격이 다르면 DLP 인시던트 통합의 성능에 영향을 줄 수 있습니다 Symantec . 일정을 예약할 때 인시던트의 긴급도에 따라 시스템 부하의 균형을 맞추도록 계획합니다.

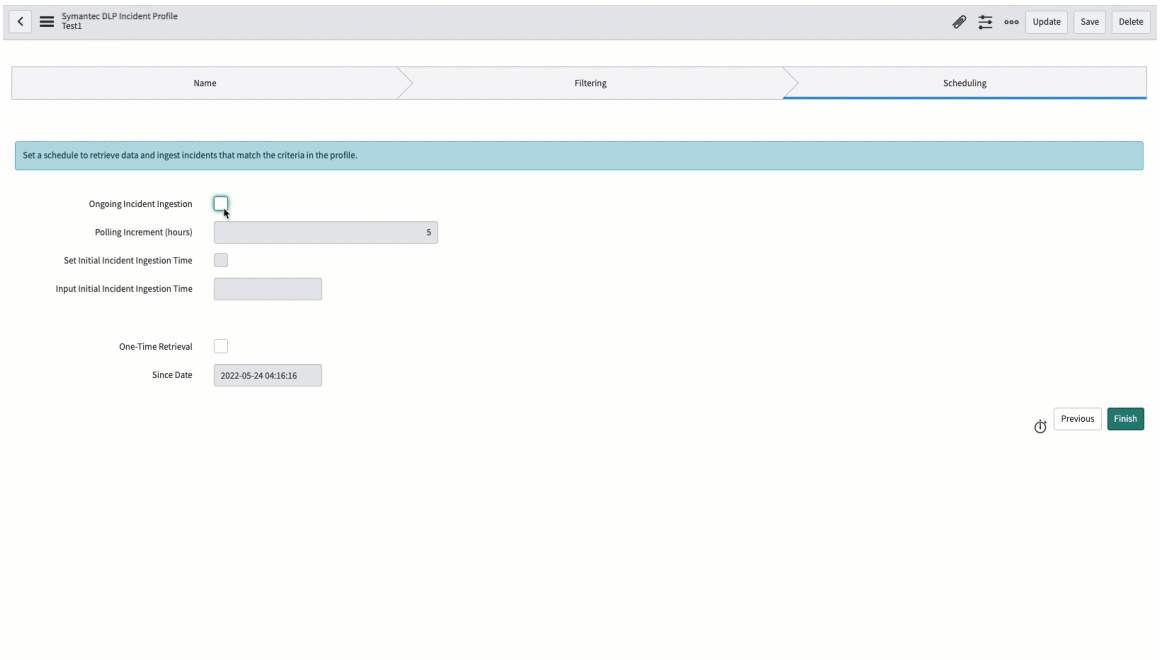
프로시저

1. 데이터를 검색하고 프로파일의 기준과 일치하는 인시던트를 수집하도록 일정을 설정합니다.
2. 양식에서 필드를 채웁니다.

DLP 인시던트 일정

필드	설명
지속적 인시던트 수집	새 인시던트에 대해 인스턴스가 Symantec에서 가져오는 진행 중인 인시던트 수집 ServiceNow AI Platform 입니다. DLP 인시던트는 트리거된 인시던트가 발견되고 인시던트 생성 필터링 기준이 일치하면 생성됩니다.
폴링 증분(분)	분 단위로 정의된 폴링 빈도입니다. 이 필드는 300분으로 자동 설정됩니다.
초기 인시던트 수집 시간 설정	초기 수집에 대한 날짜 및 시간을 정의하는 옵션입니다. 후속 수집은 폴링 간격 기간을 기반으로 합니다.
초기 인시던트 수집 시간 입력	인시던트 수집을 위해 지정하는 날짜 및 시간입니다.
초기 인시던트 수집 시간	데이터를 처음으로 수집합니다. 초기 인시던트 수집 시간이 설정되면 값이 표시되기 시작하는 것을 확인할 수 있습니다.
다음 인시던트 수집 시간(예상)	예상 인시던트 수집의 다음 기간입니다.
일회성 검색	일회성 기록 데이터 끌어오기를 활성화하는 옵션입니다. 이 필드를 선택하면 날짜 이후 필드에 추가된 날짜에 따라 Symantec DLP에서 이력 데이터를 끌어옵니다.
날짜 이후	Symantec에서 데이터를 검색해야 하는 시작 날짜입니다. 이 필드는 최대 3개월로 설정할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



3. 생성된 프로파일 구성을 저장하려면 팝업 창에서 마침 을 클릭합니다.

4. 프로파일을 활성화하려면 생성된 프로파일을 엽니다.

5. 활성 옵션을 활성화합니다.

6. 업데이트를 클릭합니다.

결과
프로파일을 성공적으로 만들고 활성화한 후에는 프로파일에 설정된 구성에 따라 인시던트가 주기적으로 검색되어 DLP 인시던트 테이블에 추가됩니다.

DLP 인시던트 상태를 인시던트 **ServiceNow** 상태와 매핑 **Symantec**

에서 ServiceNow 수집된 DLP 인시던트의 상태를 의 DLP 인시던트와 동기화합니다 Symantec. **ServiceNow** 인시던트 상태 필드를 **Symantec** 인시던트 상태 필드와 매핑합니다.

시작하기 전에
필요한 역할: sn_dlir.admin

이 태스크 정보
인시던트 상태는 매핑에 추가된 엔드포인트 소스에서 동적으로 Symantec 검색됩니다. 일대일 인시던트 상태 매핑을 수행해야 합니다.

프로시저

1. 다음으로 이동 **Symantec DLP** 통합 〉 인시던트 상태 매핑.

2. 매핑을 식별하는 이름을 제공합니다.

3. 상태를 가져올 소스 통합을 선택합니다.

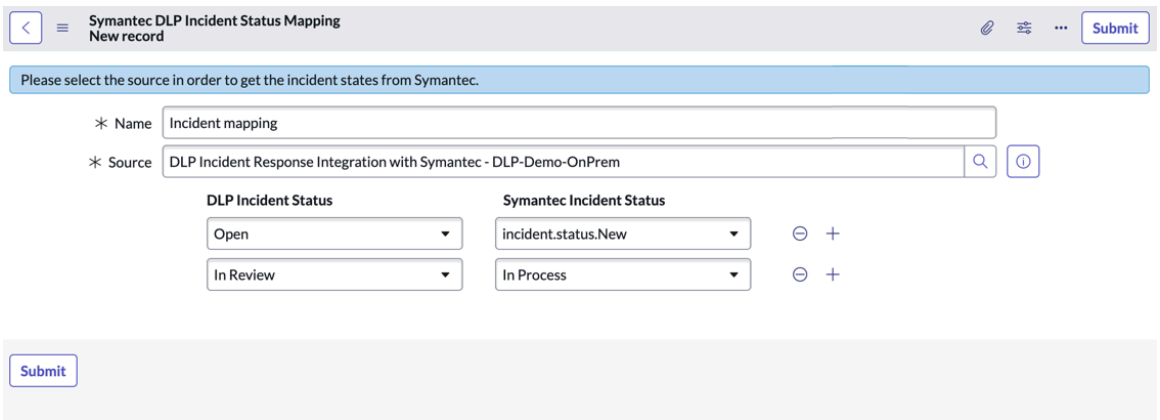
4. DLP 인시던트 상태를**Symantec** 인시던트 상태와 매핑합니다.

주:
모든 상태를 매핑할 필요는 없으며 필요한 상태만 매핑할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Symantec DLP 인시던트 상태 매핑

필드	설명
이름	매핑 기록의 이름입니다.
소스	인시던트 상태를 가져오려는 위치에서 구성된 Symantec 엔드포인트 소스입니다.
DLP 인시던트 상태	DLP 인시던트의 상태 목록입니다.
Symantec 인시던트 상태	소스(Symantec 엔드포인트)에서 가져온 상태 목록입니다.



5. 제출을 클릭합니다.

결과
인시던트 ServiceNow 의 매핑 상태에 ServiceNow 대한 기록을 성공적으로 만들면 인시던트 상태가 DLP 인시던트 상태와 동기화 Symantec 됩니다.

인스턴스에서 DLP 인시던트 ServiceNow 의 상태를 변경하면 연결된 Symantec DLP 인시던트의 상태가 기록에 설정된 매핑에 따라 소스 Symantec 플랫폼에서 변경됩니다.

Symantec DLP 인시던트와 **ServiceNow** 인시던트 간의 심각도 매핑

심각도 매핑 기능을 사용하여 인시던트와 ServiceNow AI Platform# 인시던트 간의 Symantec 매핑을 구성하고 동기화합니다.

시작하기 전에
필요한 역할: sn_dlir.admin

이 태스크 정보
DLP 심각도 매핑을 사용하면 소스 심각도를 DLP 인시던트 심각도와 매핑할 수 있습니다. 소스 심각도 값을 사용자 지정 및 정의하고 원하는 DLP 인시던트 심각도 값에 매핑할 수 있습니다.

프로시저

1. 다음으로 이동 **Symantec DLP** 통합 〉 인시던트 심각도 매핑.

2. 새로 만들기를 클릭합니다.

3. 양식에서 필드를 채웁니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

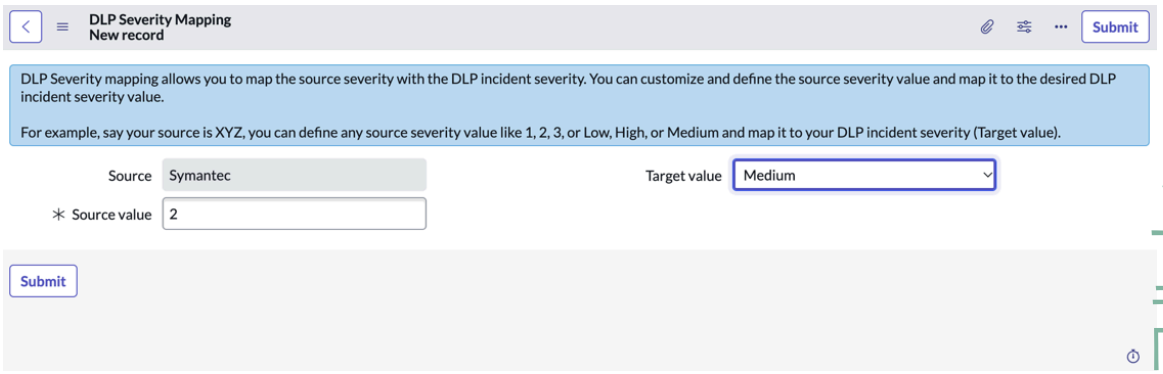
DLP 심각도 매핑

필드	설명
소스	인시던트를 가져올 위치에서 구성된 Symantec 엔드포인트 소스입니다.
대상 값	대상 값은 DLP 인시던트 심각도 ID입니다. 사용할 수 있는 값은 중요, 높음, 중간, 낮음 및 정보(Symantec에서 정보 심각도로 사용됨)입니다.
소스 값	소스 값은 Symantec 인시던트 심각도입니다.

주:
기본 시스템 내에는 DLP 사용자에게 제공되는 4개의 심각도 매핑이 있습니다.

4. 제출을 클릭합니다.

심각도 매핑



스마트 응답 규칙 구성

수집된 Symantec DLP 인시던트에 대한 응답 작업을 수행하도록 Symantec 스마트 응답 규칙을 구성합니다.

시작하기 전에
필요한 역할: sn_dlir.admin

이 태스크 정보
ServiceNow Symantec DLP 통합을 위해 구성 중인 Symantec 사용자가 역할 구성 페이지에서 해당 스마트 응답 규칙을 선택했는지 확인합니다. 자세한 내용은 역할 구성 문서에서 사용할 수 있는 작업 섹션을 참조하십시오.

가져온 스마트 응답 규칙의 경우 DLP 관리자는 인시던트 응답 옵션 규칙 및 응답 옵션 매핑을 생성하여 수집된 Symantec DLP 인시던트에서 수행할 응답 작업을 구성할 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 **Symantec DLP** 통합 〉 스마트 응답 규칙.
   구성된 각 통합 구성에 대해 사용 가능한 모든 스마트 응답 옵션을 볼 수 있습니다. 자세한 내용은 구성되지 않은 경우 Symantec 통합 구성 소스 구성을 참조 Data Loss Prevention용 Symantec DLP 통합 설치 및 구성 하고 설명된 절차를 따르십시오.)
2. 스마트 응답 규칙 중 하나를 클릭하여 양식 뷰를 엽니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

DLP 작업 공간의 응답 모달에 이 스마트 응답 규칙을 표시할 인시던트 응답 옵션 규칙 및 응답 옵션 매핑을 생성하려면 팔로우합니다 인시던트 응답 옵션 규칙 생성 .

3. 관련 목록의 승인 규칙 탭을 사용하거나 승인 규칙 구성 섹션에 설명된 절차에 따라 스마트 응답 규칙에 대한 승인 규칙을 생성합니다.
   각 스마트 응답 규칙에 대한 승인 규칙은 승인 규칙 관련 목록에 표시됩니다.
4. 인시던트 응답 옵션 규칙을 생성하면 스마트 응답 규칙 기록의 관련 목록에서 기록을 볼 수 있습니다.
5. 목록 뷰의 스마트 응답 규칙 새로 고침 버튼을 사용하여 소스를 수동으로 업데이트합니다.
   스마트 응답 규칙은 모든 소스에 대해 매일 자동으로 추가, 업데이트 또는 삭제됩니다.

스마트 응답 규칙 실행

이 기능을 사용하여 Symantec DLP 인시던트에 대한 스마트 응답 규칙을 실행합니다.

시작하기 전에

이 섹션에 스마트 응답 규칙 구성설명된 절차에 따라 스마트 응답 규칙을 구성해야 합니다.

필요한 역할: sn_dlir.admin

주:

작업 공간의 응답 옵션은 섹션에 DLP 인시던트에 대한 응답 옵션 구성언급된 구성에 따라 최종 사용자, 분석가 또는 관리자가 사용할 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 **DLP** 〉 **DLP** 사용자 작업 공간.
2. Symantec DLP 인시던트를 엽니다.
3. 응답을 클릭합니다.
4. 응답 드롭다운 목록에서 응답 옵션을 선택합니다.
   응답 옵션은 인시던트 응답 옵션 규칙 및 응답 옵션 매핑의 구성에 따라 표시됩니다.
5. 제출을 클릭합니다.

주:
섹션에 설명된 승인 규칙 생성 절차에 따라 응답 옵션에 대한 승인 규칙을 구성할 수도 있습니다. 스마트 응답 규칙에 대한 승인 규칙이 구성되면 승인 플로우가 먼저 트리거되고 모든 승인을 받은 후 스마트 응답 옵션 플로우가 트리거됩니다. DLP 인시던트의 상태는 응답 옵션을 성공적으로 실행한 후 응답 옵션 매핑의 대상 상태에 따라 업데이트됩니다.

Symantec DLP 통합 설정 구성

Symantec DLP 통합 기본 시스템 속성을 수정합니다.

시작하기 전에

필요한 역할: sn_dlir.admin

프로시저

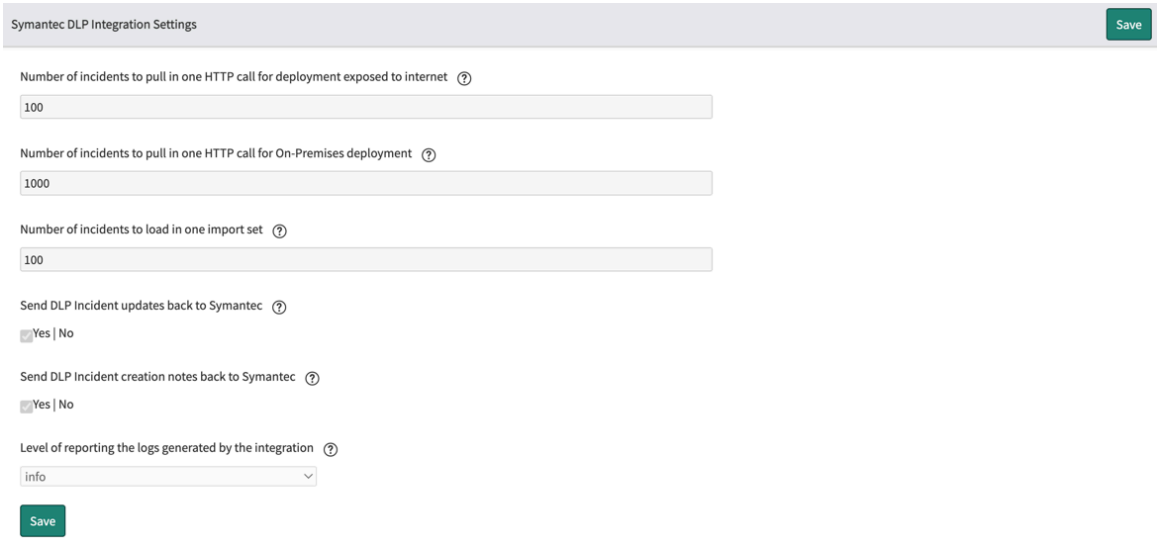
1. 다음으로 이동 **Symantec DLP** 통합 〉 설정.
2. 필요에 따라 다음 설정을 수정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설정

필드	설명
제한 적용 온프레미스 배포 sn_sym_dlp.page_size_on_prem에 대해 하나의 HTTP 호출을 끌어올 인시던트 수	의 Symantec온 프레미스 배포를 위해 하나의 HTTP 호출에서 가져올 최대 인시던트 수입니다. ○ 유형: 정수 ○ 기본값: 1000
제한 적용 인터넷에 노출된 배포에 대해 하나의 HTTP 호출을 끌어올 인시던트 수 sn_sym_dlp.page_size_on_internet	인터넷에 노출된 배포를 위해 Symantec 하나의 HTTP 호출에서 가져올 최대 인시던트 수입니다. ○ 유형: 정수 ○ 기본값: 100
하나의 임포트 세트에서 로드할 인시던트 수 sn_sym_dlp.incidents_per_attachment	처리를 위해 하나의 첨부 파일에 저장할 기록 수입니다. ○ 유형: 정수 ○ 기본값: 100
DLP 인시던트 업데이트를 Symantec sn_sym_dlp.incident_update로 다시 보내기	이 속성을 사용하면 DLP 인시던트와 Symantec 인시던트 간의 ServiceNow 상태 동기화를 제한할 수 있습니다. ○ 유형: 부울 ○ 기본값: **true**
DLP 인시던트 작성 메모를 Symantec sn_sym_dlp.incident_creation_notes로 다시 보내기	이 속성을 사용하면 에서 인시던트가 작성되는 즉시 Symantec에 메모를 다시 보낼 수 있습니다 ServiceNow. ○ 유형: 부울 ○ 기본값: **true**
통합에 의해 작성된 로그 보고 수준 sn_sym_dlp.logging.verbosity	통합으로 생성된 로그의 보고를 정의하는 속성입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



3. 저장을 클릭합니다.

DLP 통합의 Symantec 도메인 분리

도메인 분리를 사용하여 데이터, 프로세스 및 관리 작업을 도메인이라는 논리적 그룹으로 분할할 수 있습니다. 그런 다음 사용자가 데이터를 보고 액세스할 수 있는 것을 포함하여 이러한 분리의 여러 가지 측면을 제어할 수 있습니다.

지원 수준

지원: 기본.

DLP 통합에서 도메인 분리가 Symantec 작동하는 방식

도메인 분리를 수행하려면 다음 단계를 따르십시오.

- 해당 도메인에서 필요한 역할을 가진 사용자를 생성합니다.
- Symantec 해당 도메인에서 DLP 통합 절차를 수행합니다.

와 Data Loss Prevention Incident Response 통합 Proofpoint

DLP 통합은 Proofpoint 데이터 손실 방지 배포에서 생성된 데이터 손실 방지 인시던트의 수집을 Proofpoint 지원합니다. 수집 후 인시던트 관리 기능을 사용하여 DLP 인시던트를 정정할 수 있습니다.

스토어에서 앱 요청

ServiceNow Store 웹 사이트를 방문하면 사용 가능한 모든 앱을 확인하고 스토어에 요청을 제출하는 방법에 대한 정보를 참조할 수 있습니다. 출시된 모든 앱의 누적 릴리스 정보는 ServiceNow Store 버전 기록 릴리스 정보 를 참조하십시오.

개요 및 주요 기능

DLP 통합은 Proofpoint 기업이 다양한 플랫폼에서 민감한 데이터의 사용 및 이동을 추적하는 데 도움이 됩니다.

이 통합에는 다음과 같은 주요 기능이 포함됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 서로 다른 Proofpoint 엔드포인트에 대한 여러 프로파일 생성.
- DLP 인시던트 생성 자동화
- DLP 인시던트 상태 필드를 DLP 인시던트 상태 필드에 매핑 Proofpoint 합니다.
- DLP 인시던트 필터링 Proofpoint .
- DLP 테넌트에서 Proofpoint 인시던트가 생성되는 즉시 인스턴스에서 인시던트 ServiceNow 를 수집합니다.
- Proofpoint DLP 통합은 인시던트의 엔드포인트와 이메일 유형을 모두 지원합니다.
- DLP 인시던트 상태 및 코멘트, Proofpoint DLP 인시던트 생성, 측면 상태 변경 및 종결 ServiceNow 에 대한 자동 업데이트

이 통합에 대해 알아보기

문서 식별자	문서 제목
Proofpoint 제품 설명서 웹 사이트	Proofpoint 제품 설명서
ServiceNow# 제품 설명서 웹 사이트	ServiceNow 제품 설명서 웹 사이트

Data Loss Prevention을 **Proofpoint** 위한 통합 시작하기

DLP 통합은 Proofpoint 데이터 손실 방지 테넌트에서 생성된 데이터 손실 방지 인시던트의 수집을 Proofpoint 지원합니다. 수집 후에는 DLP 인시던트를 정정하는 인시던트 관리 기능이 사용됩니다.

검사 목록

Data Loss Prevention에 대한 DLP 통합 설정을 Proofpoint 시작하기 전에 다음 정보를 검토합니다.

체크리스트

필드	설명
필수 ServiceNow AI Platform 및 Data Loss Prevention Incident Response 애플리케이션 역할을 할당했는지 확인합니다.	다음의 DLP 통합에서 Proofpoint 사용되는 역할은 다음과 같습니다.ServiceNow AI Platform • 관리자(admin)는 에서 애플리케이션을 ServiceNow# Store 설치하고 데이터 손실 방지 관리자(sn_dlir.admin)를 할당합니다. • sn_dlir.admin 역할을 가진 사용자는 통합을 구성하고 인시던트 프로파일을 설정할 수 있습니다. • sn_dlir.analyst 역할을 가진 사용자는 통합 전반에 걸쳐 읽기 역할을 갖습니다.
필요한 Proofpoint DLP 사용자 역할을 할당합니다.	Proofpoint DLP 통합 역할 및 권한을 검토합니다.
DLP 1.0.1 이상을 사용하고 Proofpoint 있는지 확인합니다.	Proofpoint Data Loss Prevention에 대한 DLP 통합은 Data Loss Prevention 버전 1.0.1 이상에서 테스트되었습니다Proofpoint.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

체크리스트

필드	설명
DLP 통합을 지원하는 Proofpoint 데 필요한 최종 사용자 코어 애플리케이션이 설치되고 활성화되었는지 확인합니다.	다음 DLP 애플리케이션 및 보안 지원 공통 애플리케이션이 스토어에서 설치되고 활성화 ServiceNow 되었는지 확인합니다. 설치되지 않은 경우 애플리케이션에 설치하고 활성화합니다. • Security Support Common • 데이터 손실 방지 인시던트 응답

Data Loss Prevention을 위한 통합 설치 및 구성 **Proofpoint**

인스턴스에서 DLP 통합을 ServiceNow# StoreServiceNow AI Platform 설치하고 구성합니다Proofpoint. DLP 인시던트 데이터를 사용하여 Proofpoint DLP 인시던트 조사를 시작합니다.

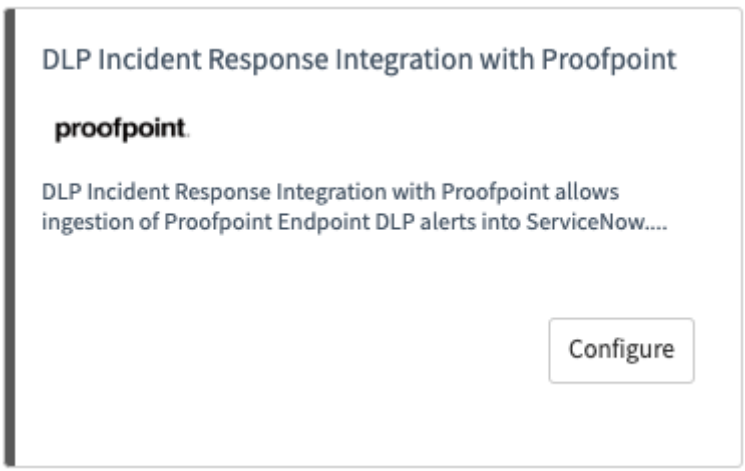
시작하기 전에
필요한 역할: sn_dlir.admin

프로시저

1. Proofpoint 에서 ServiceNow# Store DLP 통합을 다운로드하여 설치합니다.

2. 다음으로 이동 보안 운영 〉 통합 〉 통합 구성.

3. Proofpoint## DLP #### ## ## 타일을 검색하고 구성을 클릭합니다.

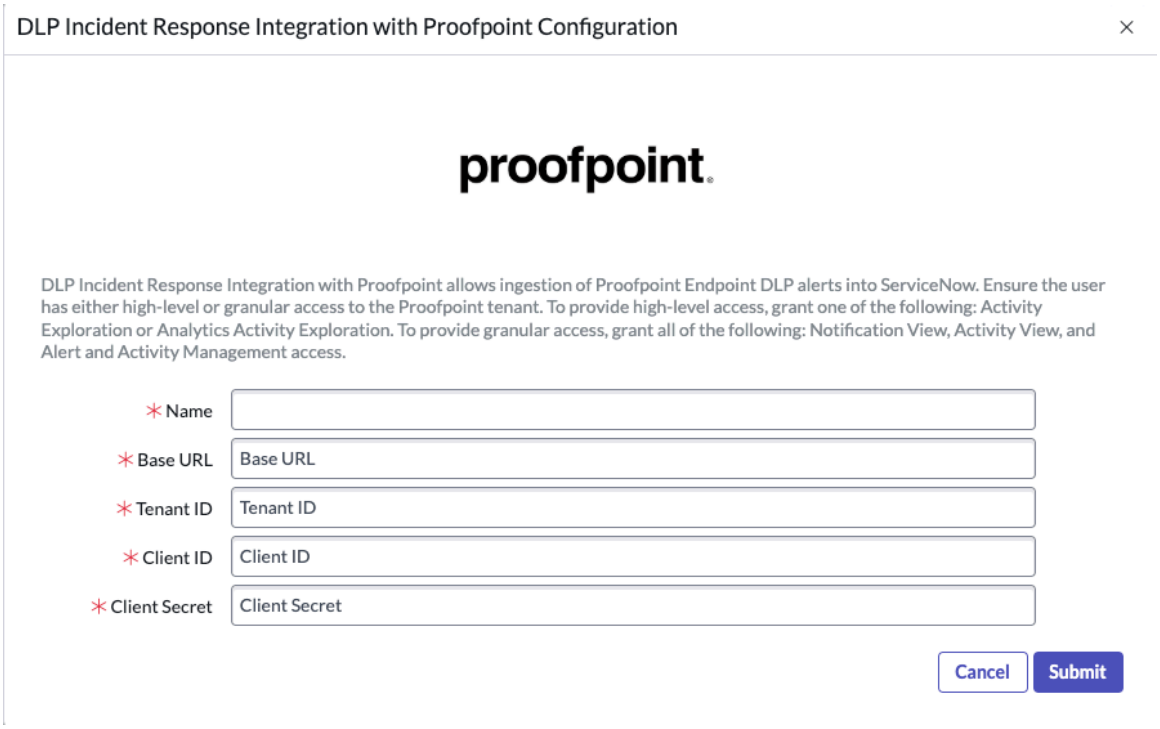


4. 양식에서 필드를 채웁니다.

Proofpoint DLP 통합 구성 양식

필드	설명
이름	Proofpoint DLP 통합 구성의 이름입니다.
기본 URL	Proofpoint REST 엔드포인트 역할을 하는 URL입니다.
클라이언트 ID	사용할 클라이언트의 ID Proofpoint 입니다.
클라이언트 비밀	의 Proofpoint사용자 계정에 대해 구성된 비밀입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



주:
기존 고객의 경우 기본 인증이 있는 기존 하위 타일이 예상대로 작동하는지 확인하기 위해 기본 인증을 계속 지원합니다. 그러나 고객이 하위 타일에 OAuth를 추가하려는 경우 기존 기본 인증 자격 증명(사용자 이름 및 암호)을 제거해서는 안 됩니다. 이러한 값을 더미 항목으로 바꿀 수 있지만 필드를 비워 두면 타일이 성공적으로 제출되지 않습니다.

5. 제출을 클릭합니다.

결과
구성을 성공적으로 확인하고 제출하면 Proofpoint DLP 통합이 보안 통합 페이지에 타일로 저장됩니다.

에 대한 경보 알림에 대한 **DLP** 테넌트에서 **Proofpoint** 웹후크 구성 **ServiceNow**

REST API 엔드포인트를 사용하여 웹후크 Proofpoint 를 구성하여 DLP 테넌트에서 경보 가져오기를 Proofpoint 시작합니다. 인스턴스는 ServiceNow 이러한 경보로부터 DLP 인시던트를 생성합니다. DLP 통합은 Proofpoint 최종 사용자가 웹후크를 구성할 수 있는 REST API 엔드포인트를 제공합니다.

시작하기 전에
필요한 역할: sn_pp_dlp.api_integration_user

프로시저

1. Proofpoint에 로그인합니다.

2. 다음으로 이동 **Proofpoint** 테넌트 〉 관리 애플리케이션 〉 통합 〉 알림 정책.

3. 적절한 이름으로 알림 정책을 생성합니다.

4. 알림 정책을 클릭하고 알림 정책에 구성된 웹후크를 관리합니다.

5. 웹후크 추가를 클릭하여 새 웹후크 구성을 생성합니다.

6. 웹후크 유형을 일반으로 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

7. URL 입력에 https://<Instance_Name>.service-now.com/api/sn_pp_dlp/proofpointalertapi/getalerts 형식을 사용하여 URL을 입력합니다.
8. 메서드를 **POST**로 유지합니다.
9. 웹후크에 다음 헤더를 추가합니다.
   - Name: Authorization
     Value: Basic <Base64Encoded Username and Password of the ServiceNow instance user>
   - Name: Content-Type
     Value: application/json
10. D는 다른 값을 변경하지 않습니다.
11. 저장을 클릭합니다.
12. 다음으로 이동 **Proofpoint** 테넌트 〉 관리 애플리케이션 〉 정책 〉 규칙.
13. 작업 섹션에서 웹후크 알림을 생성할 규칙을 선택합니다.
14. 웹후크가 구성된 새로 만든 알림 정책을 추가합니다.
15. 저장을 클릭합니다.

에서 **Proofpoint** 애플리케이션을 작성하고 클라이언트 자격 증명 가져오기

에서 Proofpoint 애플리케이션을 생성하고 클라이언트 자격 증명을 가져오는 데 필요한 설정을 구성합니다. 이러한 자격 증명을 통해 원활한 통합 및 자동화를 위해 Proofpoint의 API에 안전하게 액세스할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. Proofpoint 콘솔에 로그인합니다.
   Proofpoint 자격 증명을 사용하여 콘솔에 액세스합니다.
2. 새 애플리케이션을 생성합니다.
   a. 개발자 섹션에서 권한 부여를 선택합니다.
   b. 생성을 선택합니다.
   c. 애플리케이션 이름을 입력합니다.
   d. 허용된 범위에서 필요에 따라 애플리케이션에 범위를 추가합니다.
   e. 허용된 권한 부여에서 클라이언트 자격 증명을 선택합니다.
   f. 저장을 선택합니다.
      클라이언트 ID 및 클라이언트 비밀이 생성됩니다.
3. 애플리케이션 상세 정보를 구성합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 새로 생성된 애플리케이션을 선택합니다.

b. Access Policies(액세스 정책)에서 Edit(편집)를 선택합니다.

상위 수준 또는 세분화된 액세스 정책을 선택합니다.

c. 완료를 선택합니다.

결과
생성된 클라이언트 ID와 클라이언트 비밀을 사용하여 DLP Proofpoint (PPT) 애플리케이션에서 통합을 구성하고 사용을 시작합니다.

DLP 통합을 위한 **Proofpoint** 프로파일 생성

인스턴스에 인시던트 프로파일을 ServiceNow AI Platform 생성합니다. DLP 인시던트를 Proofpoint 만드는 데 적합한 DLP 인시던트를 결정합니다.

시작하기 전에
필요한 역할: sn_dlir.admin

이 태스크 정보
의 ProofpointDLP 경보를 ServiceNow AI Platform 채우도록 구성합니다. 경보를 인스턴스에 DLP 인시던트 ServiceNow 로 저장합니다.

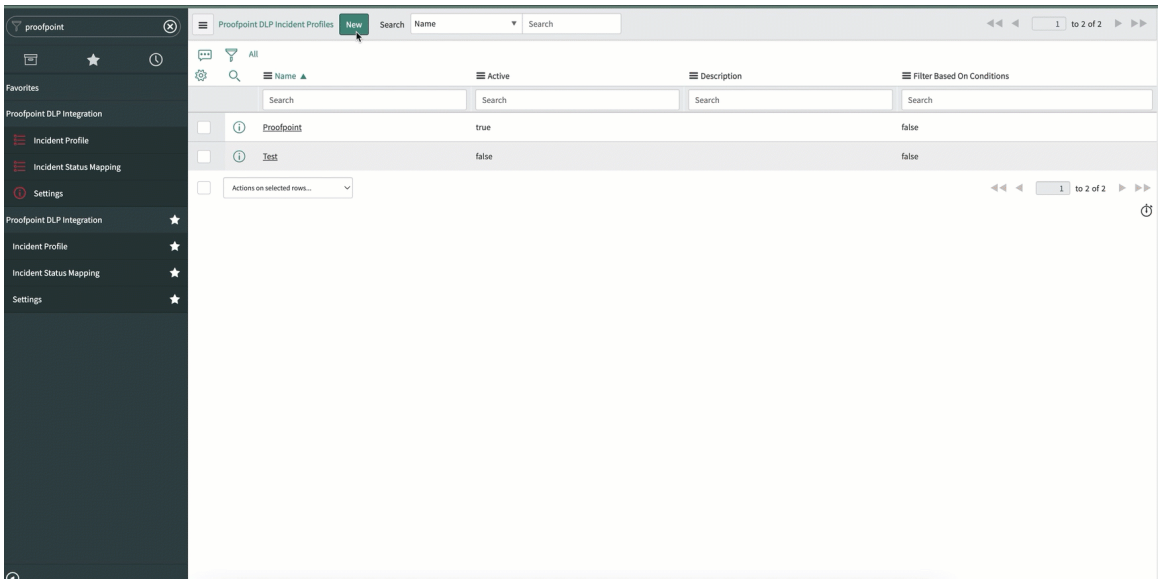
프로시저

1. 다음으로 이동 **Proofpoint DLP** 통합 〉 인시던트 프로파일.
2. 새로 만들기를 클릭합니다.
3. 양식에서 이름 섹션의 필드에 내용을 입력합니다.

DLP 통합 양식에 대한 **Proofpoint** 프로파일 생성

필드	설명
이름	프로필의 이름입니다. 이 이름은 프로파일을 식별하는 데 도움이 됩니다. 주: 각 프로파일 이름은 고유해야 합니다.
소스	Proofpoint 인시던트를 수집하도록 구성한 DLP 인스턴스입니다. 여러 인스턴스가 구성된 경우 프로파일에 대해 수집하려는 인시던트 유형에 적합한 인스턴스를 선택합니다.
활성	프로파일을 활성화하는 옵션입니다. 프로파일이 활성화되면 ServiceNow AI Platform 인스턴스가 로부터 Proofpoint인시던트를 받을 준비가 된 것입니다.
설명	이 프로파일을 다른 프로파일과 구별하는 데 도움이 되는 설명입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 계속을 클릭하고 필터링 섹션으로 이동합니다.

인시던트 생성에 적용할 필터 정의

수신 Proofpoint DLP 인시던트를 필터링하기 위한 필터 조건을 정의하고 설정합니다. 에서 생성할 ServiceNow#DLP 인시던트를 제어합니다.

시작하기 전에
필요한 역할: sn_dlir.admin

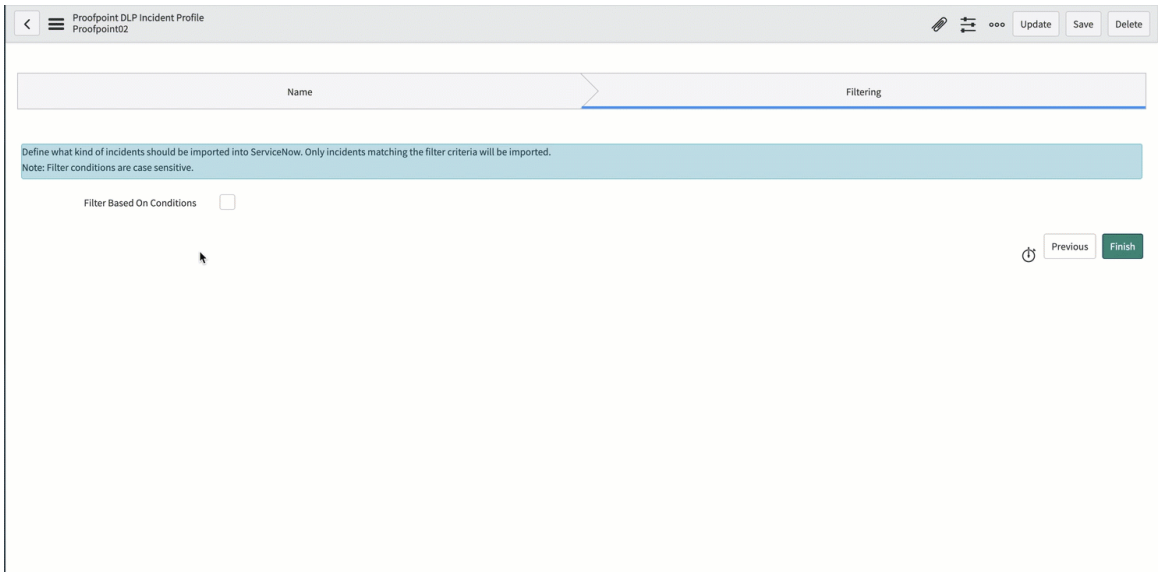
이 태스크 정보
이러한 유형의 필터링을 사용하면 DLP 인시던트를 격리하고 만드는 DLP 인시던트 수를 제한할 수 있습니다. 추가 필터링 기준이 설정되면 조건과 일치하는 인시던트만 만들어집니다.

프로시저

1. 조건에 따라 필터링 옵션을 선택하고 들어오는 DLP 인시던트가 보안 인시던트를 만들기 위해 충족해야 Proofpoint 하는 기준을 정의합니다.
2. 조건 작성기의 목록과 필드를 사용하여 필터 조건 필드에서 필터를 설정합니다.

   필터 조건의 첫 번째 필드에 있는 옵션은 DLP 인시던트에서 사용할 수 있는 필드와 일치합니다. 입력하는 기준은 대/소문자를 구분합니다. 정의하는 기준이 인시던트의 값과 일치하는지 확인합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



3. **AND** 또는 **OR**을 클릭하여 조건을 더 추가합니다.
   - **AND**를 선택하면 모든 조건이 일치해야 합니다.
   - **OR**을 선택하면 두 조건을 일치시킬 수 있습니다.
4. 마침을 클릭합니다.

증거 파일 미리 보기

DLP IR 분석가 작업 공간에서 증거 파일을 미리 봅니다 Data Loss Prevention Incident Response .

시작하기 전에

중요사항:
DLP 분석가 작업 공간에서 증거 파일 작업을 사용하는 동안 증거 파일은 임시로 암호화되지 않은 형식으로 ServiceNow 데이터베이스에 저장됩니다. 증거 파일을 저장하지 않으려면 증거 파일 미리 보기 기능을 사용하지 않도록 설정합니다. 자세한 내용은 고급 설정 구성 문서를 참조하십시오.

필요한 역할: sn_dlir.analyst

프로시저

1. 다음으로 이동 모두 〉 **DLP** 인시던트 관리 〉 **DLP** 분석가 작업 공간.
2. DLP 인시던트 기록을 엽니다.
3. 상황별 사이드바에서 증거 파일 아이콘( )을 선택합니다.
4. 증거 파일 탭에서 증거 파일 카드를 선택하여 문서 뷰어에서 증거 파일을 미리 봅니다.

   미리 보기 기능은 다음 표에 나와 있는 것처럼 파일 형식마다 다릅니다.

파일 형식	파일 확장명
이미지	.bmp, .gif, .ico, .jpeg, .jpg, .png, .svg 및 .webp. 이미지 파일은 문서 뷰어 모드에서 열립니다.
Microsoft Office 파일	.doc, .docx, .ppt, .pptx, .xls, .xlsx

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

파일 형식	파일 확장명
	Office 파일이 문서 뷰어 모드에서 열립니다.
텍스트 파일	.txt 텍스트 파일은 텍스트 편집기 모드에서 열립니다.
메일 파일	.eml 주: 파일 크기는 5MB 미만이어야 합니다. 콘텐츠를 미리 보려면 먼저 파일을 다운로드해야 합니다.
PDF 파일	.pdf ○ 키워드를 입력하여 문서를 검색합니다. ○ 확대 및 축소 기능으로 보기를 조정하여 가독성을 높입니다. ○ 페이지를 시계 방향 또는 시계 반대 방향으로 회전하면 내용을 더 선명하게 볼 수 있습니다.

주:

이진 파일은 렌더링되지 않으며 콘텐츠를 미리 보려면 다운로드해야 합니다. 증거 파일 미리 보기 기능은 보관된 인시던트에도 사용할 수 있습니다.

DLP 인시던트 상태를 인시던트 **ServiceNow** 상태와 매핑 **Proofpoint**

인스턴스에서 Proofpoint수집된 ServiceNow DLP 인시던트의 상태와 . ServiceNow 인시던트 상태를 Proofpoint 인시던트 상태와 매핑합니다.

시작하기 전에
필요한 역할: sn_dlir.admin

프로시저

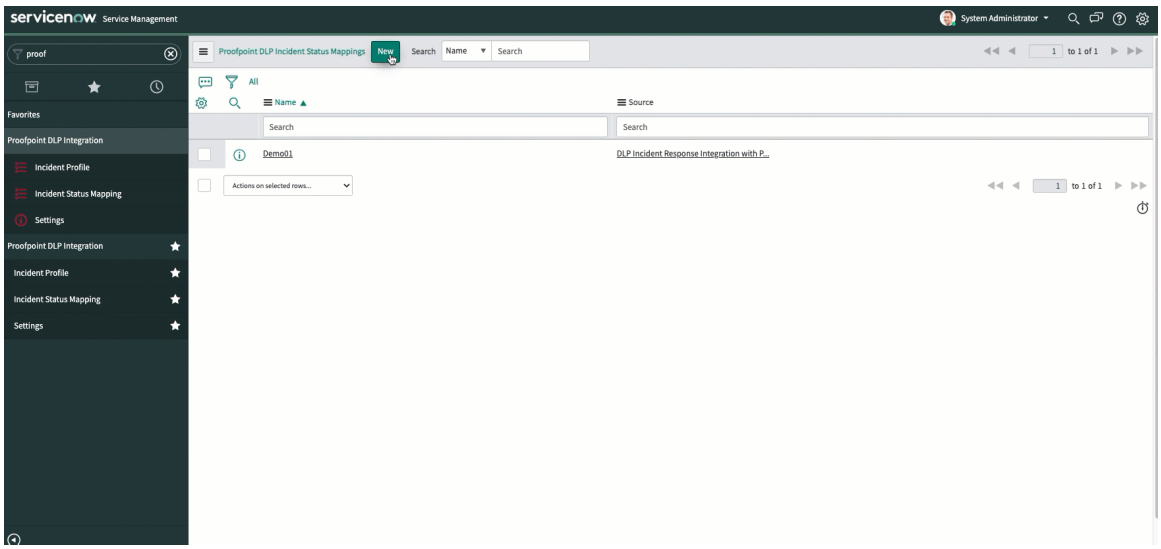
1. 다음으로 이동 **Proofpoint DLP** 통합 〉 인시던트 〉 인시던트 상태 매핑.
2. 매핑을 식별하는 이름을 제공합니다.
3. 상태 매핑을 적용할 소스(통합 구성) 타일을 선택합니다.
4. **ServiceNow DLP** 인시던트 상태를**Proofpoint** 인시던트 상태와 매핑합니다.

ServiceNow 인시던트 상태 양식과 **Proofpoint DLP** 인시던트 상태 매핑

필드	설명
이름	매핑 기록의 자리 표시자입니다.
소스	Proofpoint 인시던트 상태를 가져올 구성된 엔드포인트 소스입니다.
ServiceNow 인시던트 상태	DLP 인시던트의 상태 목록입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
Proofpoint 인시던트 상태	DLP 인시던트에서 사용할 수 있는 기본 상태에 대한 기본 매핑 값입니다. 사용자 지정 상태의 경우 기본 Proofpoint 상태는 신규입니다. 입력 필드에서 필요한 Proofpoint 상태를 수정하고 추가할 수 있습니다.



5. 제출을 클릭합니다.

결과
매핑에 대한 기록이 성공적으로 생성되었습니다. 인시던트의 ServiceNow 상태가 DLP 인시던트와 Proofpoint 동기화됩니다.

인스턴스에서 DLP 인시던트 ServiceNow 의 상태를 변경하면 연결된 Proofpoint DLP 인시던트의 상태가 기록에 설정된 매핑에 따라 소스 Proofpoint 플랫폼에서 변경됩니다.

DLP 통합 설정 구성 Proofpoint

Proofpoint DLP 통합 기본 시스템 속성을 수정합니다.

시작하기 전에
필요한 역할: sn_dlir.admin

프로시저

1. 다음으로 이동 **Proofpoint DLP** 통합 〉 설정.

2. 필요에 따라 다음 설정을 수정합니다.

3. 저장을 클릭합니다.

결과
수정된 통합 설정은 프로파일에 정의된 대로 다음 폴링 간격에 적용됩니다.

DLP 통합의 Proofpoint 도메인 분리

도메인 분리를 사용하여 데이터, 프로세스 및 관리 작업을 도메인이라는 논리적 그룹으로 분할할 수 있습니다. 그런 다음 사용자가 데이터를 보고 액세스할 수 있는 것을 포함하여 이러한 분리의 여러 가지 측면을 제어할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

지원 수준

지원: 기본.

DLP 통합에서 도메인 분리가 Proofpoint 작동하는 방식

도메인 분리를 수행하려면 다음 단계를 따르십시오.

- 해당 도메인에서 필요한 역할을 가진 사용자를 생성합니다.
- Proofpoint 해당 도메인에서 DLP 통합 절차를 수행합니다.

와 Data Loss Prevention Incident Response 통합 Netskope

DLP 통합은 Netskope 데이터 손실 방지 배포에서 생성된 데이터 손실 방지 인시던트의 수집을 Netskope 지원합니다. Netskope DLP는 기업이 다양한 플랫폼에서 민감한 데이터의 사용 및 이동을 추적하는 데 도움이 됩니다.

수집 후 인시던트 관리 기능을 사용하여 DLP 인시던트를 정정할 수 있습니다.

주요 기능

이 통합에는 다음과 같은 주요 기능이 포함됩니다.

- 여러 Netskope 테넌트에 대한 여러 프로필 생성.
- DLP 인시던트에서 ServiceNow DLP 인시던트 Netskope 생성을 자동화합니다.
- DLP 인시던트 필터링 Netskope .
- ServiceNow에서 DLP 인시던트를 생성하는 DLP 인시던트의 Netskope 예약된 수집입니다.
- ServiceNow 인스턴스에서 DLP 상태가 변경될 때 객체 상태를 Netskope 자동으로 업데이트합니다.
- DLP IR 분석가 작업 공간 및 DLP 최종 사용자 작업 공간에서 DLP 인시던트의 포렌식 상세 정보(위반 컨텐츠)를 봅니다.

  주:
  위반 컨텐츠가 ServiceNow에서 지속되지 않습니다. 인시던트가 작업 공간에서 열려 있을 때 컨텐츠를 끌어옵니다.

- 요청 시 Netskope 증거 파일을 직접 다운로드합니다.

  주:
  증거 파일이 ServiceNow에 남아 있지 않습니다. 분석가가 작업 공간에서 파일 다운로드를 클릭하면 증거 파일을 끌어옵니다.

- 토큰 만료 시 Netskope DLP 관리자 사용자에게 이메일을 통해 알림입니다.
- 인시던트 API 호출 실패에 대해 정의된 재시도 한도를 초과하는 경우 이메일을 통한 알림이 DLP 관리자 사용자에게 전송됩니다.
- Netskope 통합 실행 프로세스도 지원합니다. 자세한 내용은 DLP 통합 실행 프로세스 모니터링 문서를 참조하십시오.

Data Loss Prevention을 Netskope 위한 DLP 통합 시작하기

Data Loss Prevention에 대한 DLP 통합 설정을 Netskope 시작하기 전에 다음 정보를 검토합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설정 작업	설명
필요한 Now Platform, Data Loss Prevention 애플리케이션을 할당했는지 확인하십시오.	다음의 DLP 통합에서 Netskope 사용되는 역할은 다음과 같습니다.ServiceNow AI Platform • 관리자(admin)는 에서 애플리케이션을 ServiceNow Store 설치하고 데이터 손실 방지 관리자(sn_dlir.admin)를 할당합니다. • sn_dlir.admin 역할을 가진 사용자는 통합을 구성하고 인시던트 프로파일을 설정할 수 있습니다. • sn_dlir.analyst 역할을 가진 사용자는 통합 전반에 걸쳐 읽기 역할을 갖게 됩니다.
API v2 토큰에 Netskope 필요한 권한을 할당합니다.	다음 엔드포인트 권한은 API v2 토큰화에서 Netskope 사용됩니다. • 읽기: /api/v2/incidents/dlpincidents • 읽기: /api/v2/events/dataexport/events/incident • 읽기 + 쓰기: /api/v2/incidents/update
DLP 통합을 지원하는 Netskope 데 필요한 최종 사용자 코어 애플리케이션이 설치되고 활성화되었는지 확인합니다.	다음 DLP 애플리케이션 및 보안 지원 공통 애플리케이션이 스토어에서 설치되고 활성화 ServiceNow 되었는지 확인합니다. 설치되지 않은 경우 애플리케이션에 설치하고 활성화합니다. • Security Support Common • 데이터 손실 방지 인시던트 응답

Data Loss Prevention용 **Netskope DLP** 통합 설치 및 구성

인스턴스에서 DLP 통합을 ServiceNow StoreServiceNow AI Platform 설치하고 구성합니다Netskope. ☒ DLP인시던트 데이터를 사용하여 Netskope DLP 인시던트 조사를 시작할 수 있습니다.

시작하기 전에
필요한 역할: sn_dlir.admin

프로시저

1. Netskope 에서 ServiceNow Store DLP 통합을 다운로드하여 설치합니다.

2. 다음으로 이동합니다. 보안 운영 〉 통합 〉 통합 구성

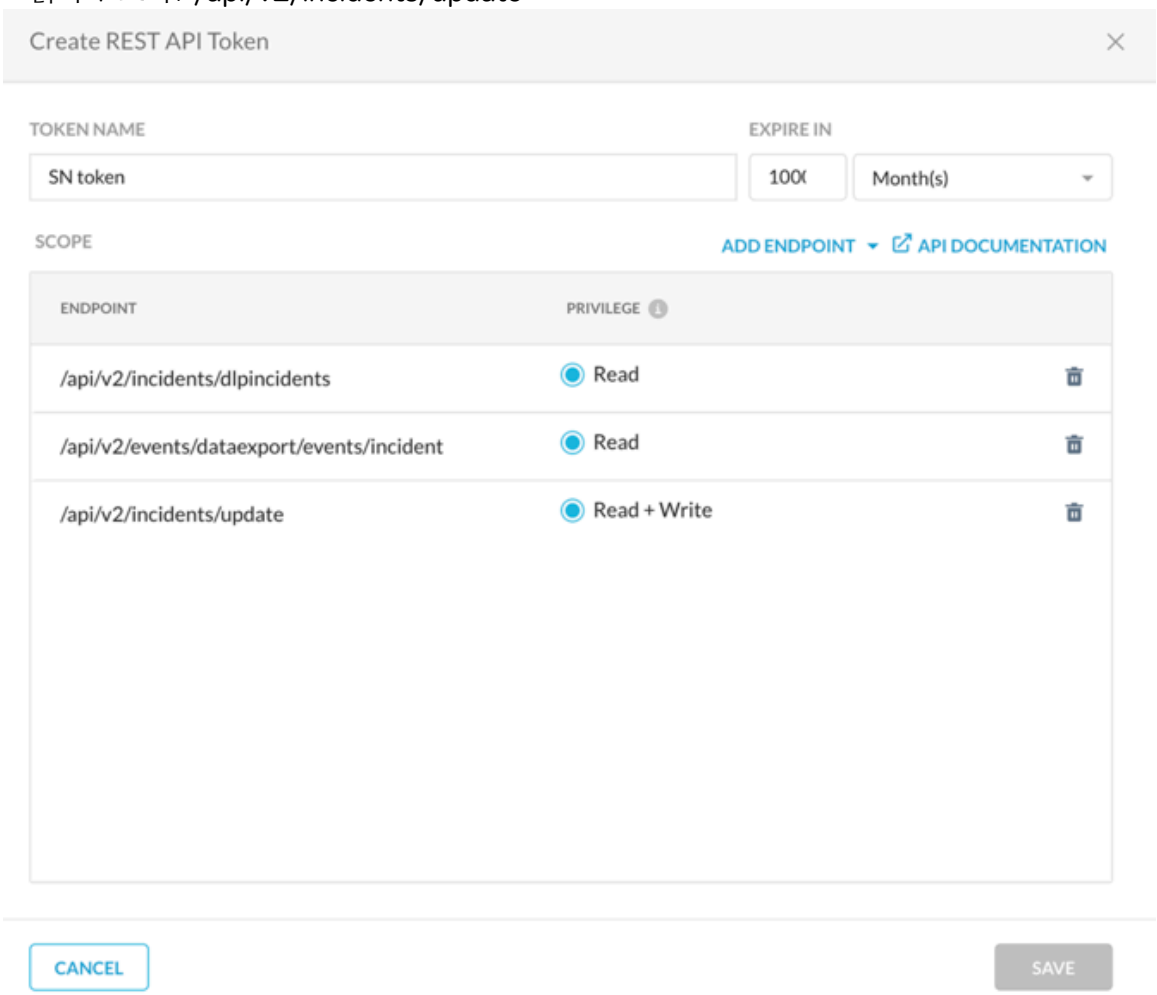
3. Netskope## DLP #### ## ## 타일을 검색하고 구성을 클릭합니다.

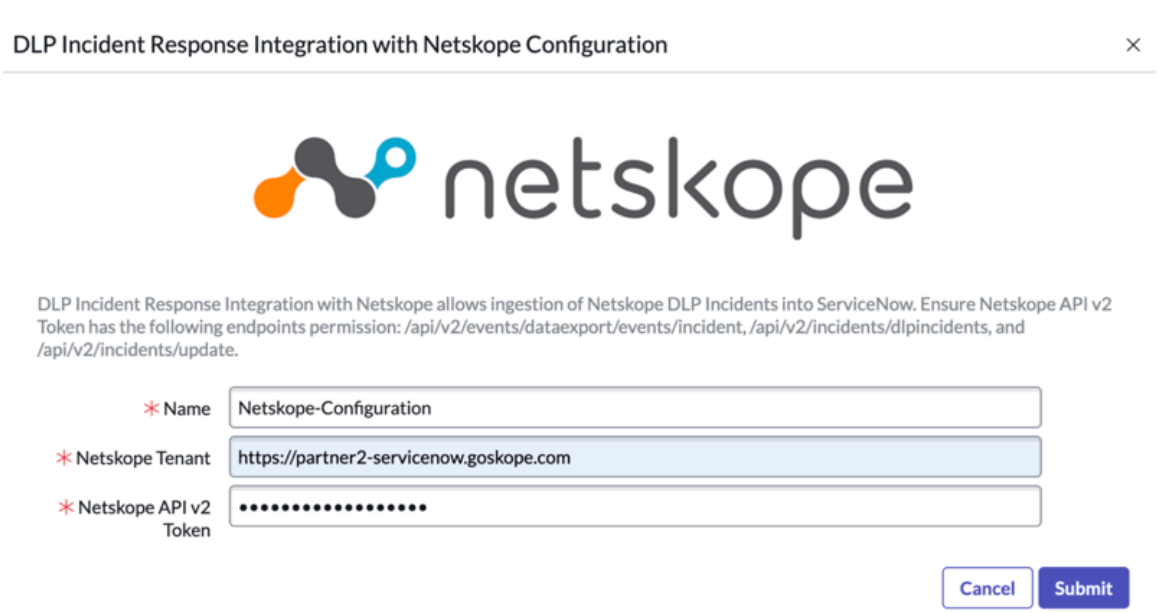
4. 양식에서 필드를 채웁니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
API v2 토큰에 아래 엔드포인트 권한이 있는지 확인합니다 Netskope .

- 읽기: /api/v2/incidents/dlpincidents
- 읽기: /api/v2/events/dataexport/events/incident
- 읽기 + 쓰기: /api/v2/incidents/update





작성

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
이름	Netskope DLP 통합 구성의 이름입니다.
Netskope 테넌트	테넌트 Netskope 의 기준 URL입니다 Netskope .
Netskope API v2 토큰	에서 사용자 계정의 REST API v2에 대해 구성된 토큰입니다 Netskope.

5. 제출을 클릭합니다.

결과

주:
Netskope 하위 프로덕션을 ServiceNow 하위 프로덕션에 연결하십시오. 계정이 로그아웃되지 않도록 인스턴스 간에 모든 사용자 이름과 암호를 동기화된 상태로 유지합니다.

구성을 성공적으로 확인하고 제출하면 Netskope DLP 통합이 보안 통합 페이지에 타일로 저장됩니다.

DLP 통합을 위한 Netskope 프로파일 생성

인스턴스에 인시던트 프로파일을 ServiceNow AI Platform 생성합니다.

시작하기 전에
필요한 역할: sn_dlir.admin

이 태스크 정보
엔드포인트에서 Netskope DLP 인시던트를 검색하도록 구성합니다ServiceNow AI Platform. 인시던트를 ServiceNow 인스턴스에 DLP 인시던트로 저장합니다.

프로시저

1. 다음으로 이동 **Netskope DLP** 통합 〉 인시던트 프로파일.
2. 새로 만들기를 클릭합니다.
3. 양식에서 필드를 채웁니다.

프로파일 생성

필드	설명
이름	프로필의 이름입니다. 각 프로파일 이름은 고유해야 합니다. 이 이름은 프로파일을 식별하는 데 도움이 됩니다.
소스	Netskope 인시던트를 수집하도록 구성한 DLP 인스턴스입니다. 여러 인스턴스가 구성된 경우 프로파일에 대해 수집하려는 인시던트 유형에 적합한 인스턴스를 선택합니다. 주: 소스당 하나의 활성 프로파일만 허용됩니다.
활성	프로파일이 활성 상태임을 나타내는 표시기입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	주: 이 필드는 마지막 예약 섹션에서 마침 을 클릭한 후에만 사용할 수 있습니다. 프로파일이 활성 상태이면 ServiceNow AI Platform 인스턴스가 DLP 인시던트를 적극적으로 폴링 Netskope 하고 있는 것입니다. 제공한 일정 매개변수에 따라 필터링 조건이 일치하면 해당 DLP 인시던트가 ServiceNow DLP 인시던트로 생성됩니다.
순서	프로파일 실행 순서입니다. 순서가 가장 낮은 프로파일이 가장 높은 우선 순위로 간주됩니다. 기본적으로 이 값은 100입니다.
설명	이 프로파일을 다른 프로파일과 구별하는 데 도움이 되는 설명입니다.

4. 계속을 클릭하고 필터링 섹션으로 이동합니다.

인시던트 작성에 적용할 필터 정의

수신 Netskope DLP 인시던트를 필터링하기 위한 필터 조건을 정의하고 설정합니다. 이러한 인시던트 중 인스턴스에서 DLP 인시던트 ServiceNow 로 생성할 인시던트를 제어합니다.

시작하기 전에
필요한 역할: sn_dlir.admin

이 태스크 정보
이러한 유형의 필터링을 사용하면 DLP 인시던트를 격리하고 만드는 DLP 인시던트 수를 제한할 수 있습니다. 추가 필터링 기준이 설정되면 조건과 일치하는 인시던트만 만들어집니다.

프로시저

1. 조건에 따라 필터링 옵션을 선택하고 DLP 인시던트가 생성되도록 수신 Netskope DLP 인시던트가 충족해야 하는 기준을 정의합니다.
2. 조건 작성기의 목록과 필드를 사용하여 필터 조건 필드에서 필터를 설정합니다.

   필터 조건의 첫 번째 필드에 있는 옵션은 **Netskope DLP** 인시던트 임포트 테이블에서 사용할 수 있는 필드와 일치합니다. 입력하는 기준은 대/소문자를 구분합니다. 정의하는 기준이 인시던트의 값과 일치하는지 확인합니다.

3. **AND** 또는 **OR**을 클릭하여 조건을 더 추가합니다.
   - **AND**를 선택하면 모든 조건이 일치해야 합니다.
   - **OR**을 선택하면 두 조건을 일치시킬 수 있습니다.
4. 계속을 클릭하고 예약 섹션으로 이동합니다.

Netskope DLP 인시던트 검색 예약

프로파일의 기준과 일치하는 DLP 인시던트를 검색 Netskope 하도록 일정을 설정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_dlir.admin

이 태스크 정보
인시던트 프로파일 구성과 일치하는 순 신규 Netskope 인시던트를 폴링하는 빈도를 계획할 수 있습니다. 자동 인시던트 수집을 사용하려면 프로파일을 활성화하기 전에 예약 및 인시던트 검색을 구성해야 합니다. 일회성 검색 확인란을 사용하여 일회성 검색을 수행하도록 프로파일을 구성할 수 있습니다. 이력 날짜는 과거로부터 최대 1개월이 될 수 있습니다.

프로시저

1. 에서 인시던트를 Netskope가져오는 방법과 시기를 정의하도록 일정을 구성합니다.
2. 양식에서 필드를 채웁니다.

Netskope DLP 인시던트 예약

필드	설명
지속적 인시던트 수집	인스턴스가 새 인시던트에 대해 가져오는 Netskope 지속적 인시던트 수집 ServiceNow AI Platform 입니다. 인시던트 필터링 기준과 일치하는 트리거된 인시던트가 발견되면 DLP 인시던트가 생성됩니다.
폴링 증분(분)	분 단위로 정의된 폴링 빈도입니다. 이 기본값은 **5**로 설정됩니다.
초기 인시던트 수집 시간 설정	구성된 날짜 및 시간을 기준으로 초기 인시던트 수집을 설정하는 옵션입니다. 이 옵션을 사용하여 초기 수집에 대한 특정 날짜 및 시간을 정의할 수 있습니다. 후속 수집은 폴링 간격 기간을 기반으로 합니다.
초기 인시던트 수집 시간 입력	인시던트 수집을 위해 지정하는 날짜 및 시간입니다.
초기 인시던트 수집 시간	데이터를 처음으로 수집할 때입니다. 주: 이 값은 초기 인시던트 수집 시간 설정 옵션을 선택한 경우에만 표시됩니다.
다음 인시던트 수집 시간(예상)	다음 예상 인시던트 수집 시간입니다.
일회성 검색	일회성 기록 데이터 끌어오기를 활성화하는 옵션입니다. 주: 이 옵션을 선택하면 날짜 이후에 추가된 날짜에 따라 DLP에서 Netskope 기록 데이터를 끌어옵니다.
날짜 이후	데이터를 가져온 Netskope시작 날짜입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	주: 기껏해야 최근 30일 동안의 데이터를 에서 가져올 Netskope수 있습니다.

3. 마침을 클릭합니다.
4. 팝업에서 마침을 클릭하여 생성된 프로파일 구성을 저장합니다.
5. 프로파일을 활성화합니다.
   a. 생성된 프로파일을 엽니다.
   b. 활성을**true**로 설정합니다.
   c. 업데이트를 클릭합니다.

결과
프로파일이 성공적으로 생성되면 프로파일의 구성에 따라 주기적으로 인시던트를 가져옵니다. 인시던트가 DLP 인시던트 테이블에 추가됩니다.

DLP 인시던트 상태 매핑 **Netskope**

인시던트 상태 매핑 섹션을 사용하면 사용자가 ServiceNow Netskope 의 DLP 인시던트 상태와 객체 상태 간의 매핑을 제공할 수 있습니다.

시작하기 전에
매핑은 ServiceNow에서 DLP 인시던트를 수집할 때 사용될 뿐만 아니라 ServiceNow에서 Netskope DLP 인시던트의 상태 변경을 에 다시 동기화하는 Netskope데 사용됩니다.

ServiceNow에서 수집된 DLP 인시던트의 상태를 Netskope의 DLP 인시던트와 동기화합니다. ServiceNow 인시던트 상태 필드를 객체 상태 필드와 Netskope 매핑합니다.

필요한 역할: sn_dlir.admin

이 태스크 정보
및 ServiceNow 상태의 Netskope 일대일 인시던트 상태 매핑을 생성해야 합니다.

프로시저

1. 다음으로 이동 **Netskope DLP** 통합 〉 인시던트 상태 매핑.
2. 매핑을 식별하는 이름을 제공합니다.
3. 소스 통합을 선택합니다.
4. DLP 인시던트 상태를 개체 상태와 매핑 Netskope 합니다(중복 Netskope 상태도 매핑할 수 있음). 매핑 기록을 생성하지 않으면 ServiceNow에서 다음으로 Netskope 상태 동기화가 비활성화됩니다.

   중요사항:
   모든 Netskope 객체 상태를 모든 ServiceNow 상태에 매핑해야 합니다. DLP 인시던트 상태를 객체에 다시 동기화하려면 Netskope 소스를 선택합니다.

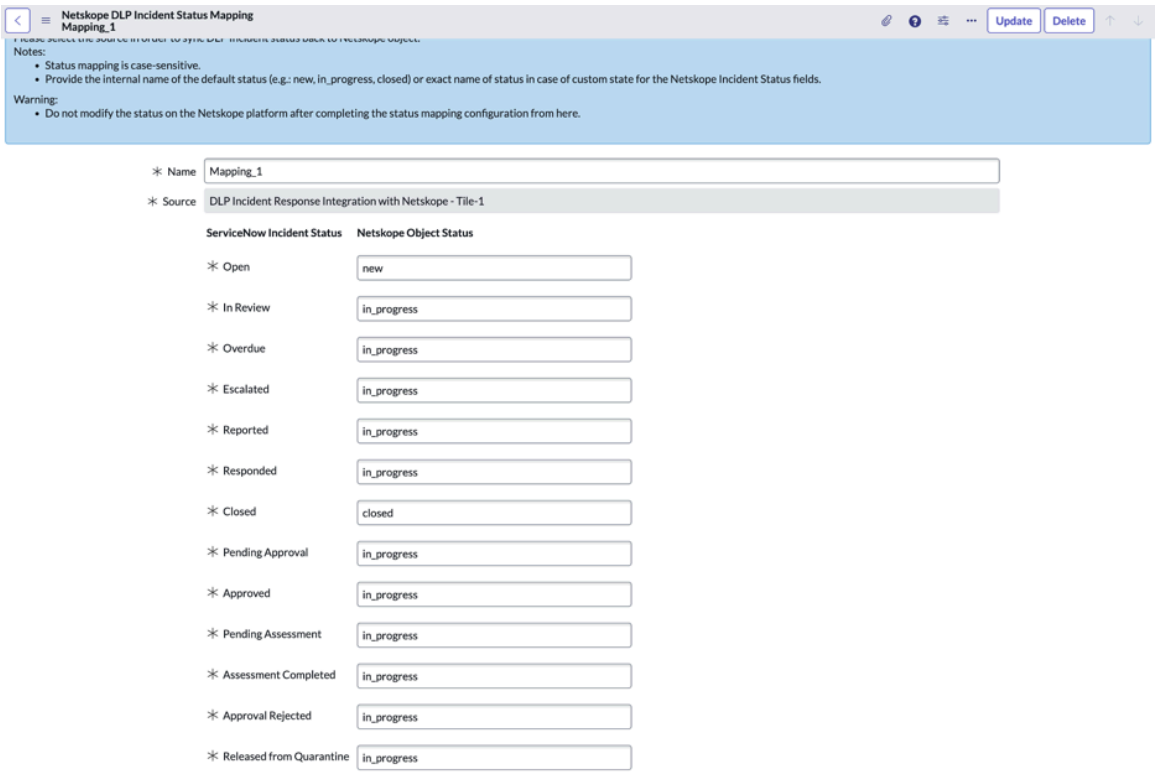
   인시던트 상태를 매핑하면 다음 정보와 경보 메시지가 표시되며, 메시지를 검토하고 계속 진행합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

- 상태 매핑은 대소문자를 구분합니다.
- 객체 상태 필드에 기본 상태의 내부 이름(예: 신규, in_progress, 종결) 또는 사용자 지정 상태인 Netskope 경우 정확한 상태 이름을 제공합니다.

> **경고:**
> 여기에서 상태 매핑 구성을 완료한 후에는 플랫폼에서 상태를 Netskope 수정하지 마십시오.



Netskope DLP 인시던트 상태 매핑

필드	설명
이름	매핑 기록의 이름입니다.
소스	인시던트 상태를 동기화하려는 구성된 Netskope 엔드포인트 소스입니다.
DLP 인시던트 상태	DLP 인시던트 상태 목록을 나타냅니다.
Netskope 객체 상태	개체 상태의 Netskope 목록을 나타냅니다.

5. 제출을 클릭합니다.

결과
상태 매핑에 대한 기록을 성공적으로 생성한 후에는 ServiceNow DLP 인시던트의 상태가 업데이트될 때마다 매핑에 따라 측면에 자동으로 반영 Netskope 됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
테넌트에서 Netskope DLP 인시던트의 상태를 직접 변경하는 경우 API 제한을 고려할 때 SN에서 SN으로의 Netskope 상태 동기화가 작동하지 않습니다. 모든 DLP 인시던트 상태를 Netskope 개체 상태와 신중하게 매핑해야 합니다.

DLP 통합 설정 구성 Netskope

Netskope DLP 통합 기본 시스템 속성을 수정합니다.

시작하기 전에
필요한 역할: sn_dlir.admin

프로시저

1. 다음으로 이동 **Netskope DLP** 통합 〉 설정.
2. 필요에 따라 다음 설정을 수정합니다.

DLP 통합 설정 구성 Netskope

필드	설명
보고된 인시던트의 위반 파일 다운로드가 허용되어야 합니다. sn_ns_dlp.enable_file_download.	파일 다운로드를 활성화할지 여부를 선택하는 옵션입니다. 기본적으로 이 옵션은 활성화되어 있습니다.
HTTP 호출의 최대 시간 제한(초) sn_ns_dlp.maximum_http_time_out.	HTTP 호출의 최대 시간 제한(초)입니다. 이 필드는 30으로 자동 설정됩니다.
API 실패에 대해 수행할 최대 재시도 횟수입니다. sn_ns_dlp.maximum_retry입니다.	API 실패에 대해 수행할 최대 재시도 횟수입니다. 기본값은 3으로 설정되어 있습니다.
통합 sn_ns_dlp.logging.verbosity에서 작성된 로그 보고 수준입니다.	통합에 의해 생성된 보고 로그의 수준을 정의합니다. 이 필드는 정보로 자동 설정됩니다.

3. 저장을 클릭합니다.

결과
수정된 통합 설정은 프로파일에 정의된 대로 다음 폴링 간격에 적용됩니다.

증거 파일 다운로드

에서 DLP 정책을 Netskope위반하는 파일을 다운로드합니다. 승인자용 DLP IR 분석가 작업 공간 및 DLP IR 최종 사용자 작업 공간에서 로컬 머신으로 이 파일을 다운로드합니다.

시작하기 전에
필요한 역할:

- sn_dlir.분석가
- sn_dlir.secure_file_download(이 역할이 있는 모든 승인자)

이 태스크 정보
진행하기 전에 에 대한 파일 다운로드를 Netskope 활성화해야 합니다.

프로시저

1. 다음으로 이동 모두 〉 **Netskope DLP** 통합 〉 설정.
2. 속성 활성화 보고된 인시던트의 위반 파일 다운로드가 허용되어야 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

DLP IR 분석가 작업 공간 및 DLP IR 최종 사용자 작업 공간에서 파일 다운로드 버튼을 볼 수 있습니다.

3. 다음으로 이동 모두 〉 **DLP** 인시던트 관리 〉 **DLP** 분석가 작업 공간.
4. 소스에서 수집된 Netskope DLP 인시던트 기록을 엽니다.
5. 파일 다운로드를 클릭합니다.
의 DLP 정책을 Netskope 위반하는 파일이 사용자의 로컬 컴퓨터에 다운로드됩니다.

> **주:**
> DLP 관리자는 DLP 관리의 고급 설정 페이지에서 보고된 인시던트의 위반 파일 다운로드가 허용되어야 함 옵션을 비활성화하여 모든 통합에 대한 파일 다운로드 작업의 액세스를 제어할 수 있습니다. 자세한 내용은 고급 설정 구성 문서를 참조하십시오.

증거 파일 미리 보기

DLP IR 분석가 작업 공간에서 DLP 인시던트 증거 파일을 미리 봅니다.

시작하기 전에

- 다음으로 이동 모두 〉 **DLP** 관리 〉 고급 설정.
- **sn_ns_dlp.enable_evidence_file_preview** 속성이 이미 활성화되어 있는지 확인합니다.

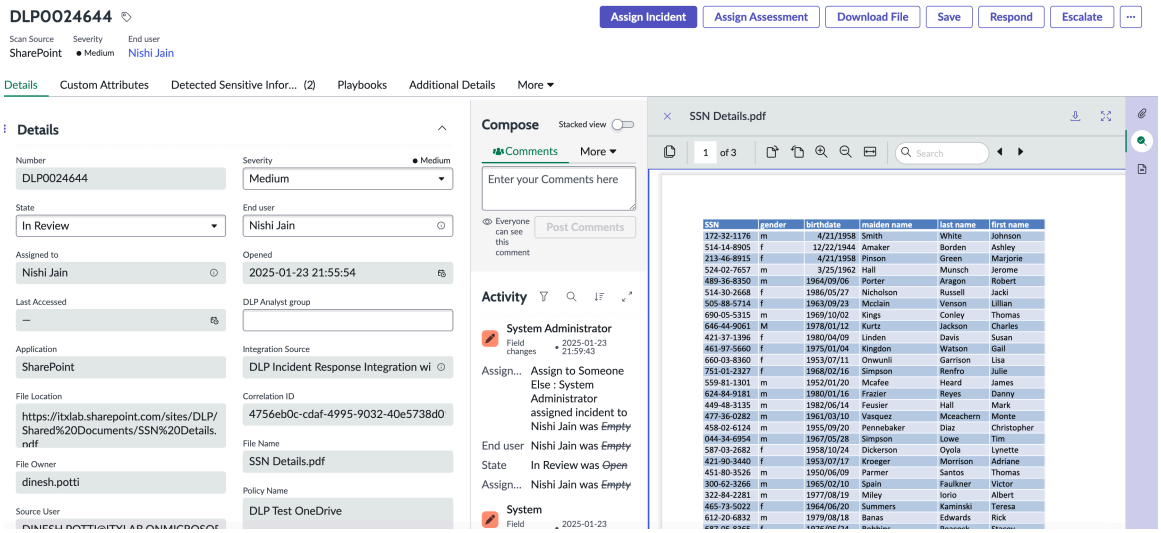
> **중요사항:**
> DLP 분석가 작업 공간에서 증거 파일 작업을 사용하는 동안 증거 파일은 고급 설정 페이지의 **sn_dlir.preview_temp_files_cleanup_interval** 속성을 사용하여 선택한 기간 동안 암호화되지 않은 형식으로 ServiceNow 데이터베이스에 임시로 저장됩니다. ServiceNow 데이터베이스에 데이터를 저장하지 않으려면 증거 파일 미리 보기 기능을 비활성화할 수 있습니다. 자세한 내용은 고급 설정 구성 문서를 참조하십시오.

필요한 역할: sn_dlir.analyst

프로시저

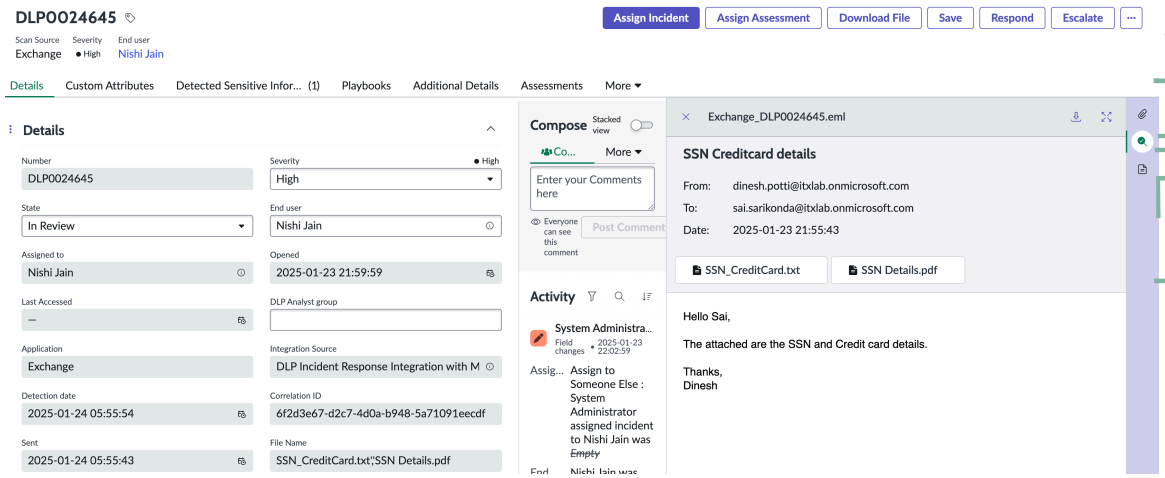
1. 다음으로 이동 모두 〉 **DLP** 인시던트 관리 〉 **DLP** 분석가 작업 공간.
2. DLP 인시던트 기록을 엽니다.
3. 상황별 메뉴에서 사용할 수 있는 증거 파일 아이콘을 선택합니다.
모든 증거 파일을 가져오는 탭이 열립니다. 다운로드가 완료되면 증거 파일 탭에서 모든 증거 파일을 볼 수 있습니다.
4. 미리 보려는 증거 파일 카드를 선택합니다.
미리 보기 기능은 파일 형식마다 다릅니다.
5. 증거 파일의 오른쪽 상단에 있는 확장 아이콘을 선택하여 문서 뷰어에서 PDF 및 Office 문서를 미리 보고 PDF를 전체 화면으로 엽니다.
문서 뷰어가 증거 파일을 여는 Office 확장에는 doc, docx, ppt, pptx, xls, xlsx가 포함됩니다.
   a. 검색 창을 찾아 찾고 있는 키워드를 입력합니다.
   b. 확대 및 축소 기능을 사용하여 뷰를 조정하여 가독성을 높입니다.
   c. 페이지를 시계 방향 또는 시계 반대 방향으로 회전하면 내용을 더 선명하게 볼 수 있습니다.
이러한 제어 옵션은 증거 파일을 포괄적으로 이해하는 능력을 향상시킵니다. PDF에만 머리글에 제어 옵션이 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

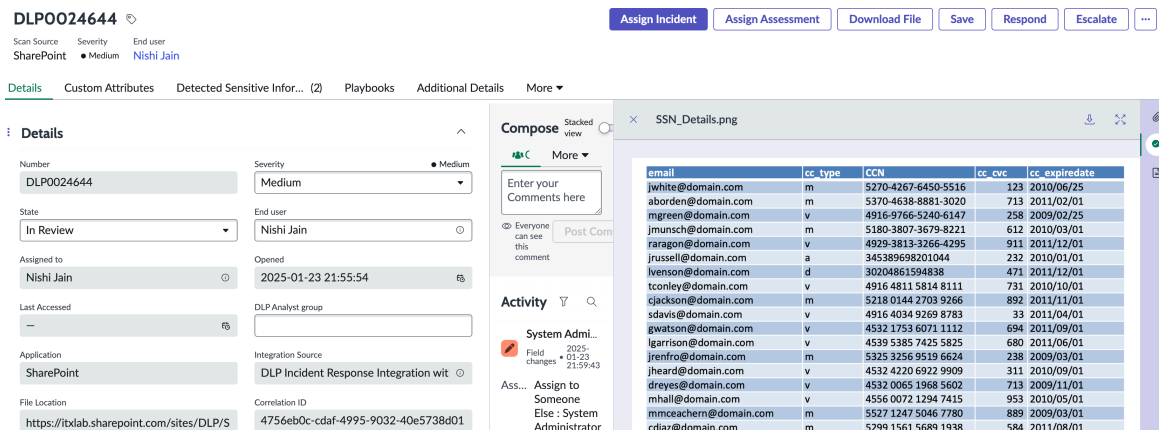


6. eml 파일을 미리 봅니다.
이메일에서 첨부 파일을 선택하고 미리 봅니다.

주:
선택한 증거 파일이 5MB 한도를 초과하는 경우 분석가 작업 공간에서 미리 볼 수 없습니다. 내용을 미리 보려면 파일을 다운로드해야 합니다. 이 제한은 .eml 파일에만 적용됩니다.

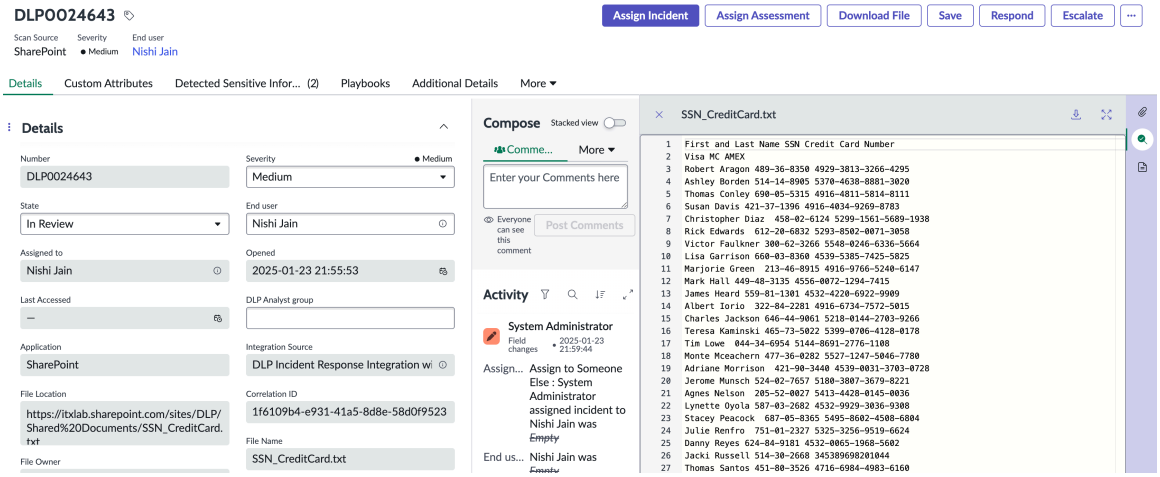


7. DLP 분석가 작업 공간에서 이미지를 미리 봅니다.
.bmp, .gif, .ico, .jpeg, .jpg, .png, .svg 및 .webp 확장자를 가진 이미지만 지원됩니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

8. 증거 파일의 오른쪽 위에 있는 확장 아이콘을 선택하여 텍스트 편집기에서 텍스트 파일을 미리 봅니다.



주:
Office 문서, eml 파일, 텍스트 및 이미지 확장명을 제외한 증거 파일은 미리 보기에 지원되지 않습니다. 이진 파일은 렌더링되지 않으며 콘텐츠를 미리 보려면 다운로드해야 합니다. 증거 파일 미리 보기 기능은 보관된 인시던트에도 사용할 수 있습니다.

재시도 메커니즘의 사용자에 대한 알림

Netskope 통합은 DLP 인시던트 수집 중에 API 오류가 발생할 경우 구성된 횟수를 다시 시도합니다.

최대 재시도 한도가 초과 Netskope 되면 통합에서 DLP 관리자(sn_dlir.admin) 역할이 있는 사용자에게 이메일 알림을 보냅니다.

통합 설정 및 구성을 완료한 후 최대 재시도 한도가 초과할 때 알림을 받을 사용자에게 DLP 관리자(sn_dlir.admin) 역할을 제공합니다.

최대 재시도 한도를 초과하면 프로필은 최대 1시간 동안 수집을 건너뜁니다. 최대 재시도 횟수는 API ### ## ### ## ### ## 속성을 사용하여 구성됩니다. 자세한 내용은 DLP 통합 설정 구성 Netskope 문서를 참조하십시오.

자격 증명 만료에 대한 이메일 알림

인스턴스에 사용된 ServiceNow 토큰이 만료 Netskope 되면 통합은 DLP 관리자(sn_dlir.admin) 역할을 가진 사용자에게 이메일 알림을 보냅니다.

통합 구성 설정이 완료되면 토큰이 만료된 경우 알림을 받을 사용자에게 DLP 관리자(sn_dlir.admin) 역할을 제공합니다.

토큰이 만료되면 Netskope 통합 구성이 유효한 토큰으로 업데이트될 때까지 연결된 프로파일에 대한 데이터 수집이 보류됩니다.

에서 토큰을 생성하거나 이전 토큰을 Netskope갱신한 다음 인스턴스에서 토큰을 ServiceNow 업데이트해야 합니다. 만료 시간을 Netskope 연장하여 토큰을 갱신하면 애플리케이션이 자동으로 갱신을 감지하고 데이터 수집을 계속합니다. 토큰을 만드는 경우 구성에서 토큰을 업데이트해야 합니다.

DLP 통합의 Netskope 도메인 분리

도메인 분리를 사용하여 데이터, 프로세스 및 관리 작업을 도메인이라는 논리적 그룹으로 분할할 수 있습니다. 그런 다음 사용자가 데이터를 보고 액세스할 수 있는 것을 포함하여 이러한 분리의 여러 가지 측면을 제어할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

지원 수준

지원: 기본.

DLP 통합에서 도메인 분리가 Netskope 작동하는 방식

도메인 분리를 수행하려면 다음 단계를 따르십시오.

- 해당 도메인에서 필요한 역할을 가진 사용자를 생성합니다.
- Netskope 해당 도메인에서 DLP 통합 절차를 수행합니다.

DLP IR을 위한 ICAP(Internet Content Adaption Protocol) 통합

ICAP(Internet Content Adaption Protocol) DLP 통합은 경보 수집 Data Loss Prevention Incident Response 을 지원하고, ICAP 지원 Data Loss Prevention Incident Response 배포에서 생성된 Amazon S3에서 일치 콘텐츠 및 증거 파일을 가져올 수 있도록 합니다.

경보를 수집한 후 DLP 작업 공간을 사용하여 일치 컨텐츠, 경보 심각도 및 다양한 인시던트 관리 기능과 같은 필요한 주요 정보를 확인하여 DLP 인시던트를 정정할 수 있습니다.

ServiceNow Store 웹 사이트를 방문하면 사용 가능한 모든 앱을 확인하고 스토어에 요청을 제출하는 방법에 대한 정보를 참조할 수 있습니다. 출시된 모든 앱의 누적 릴리스 정보는 ServiceNow Store 버전 기록 릴리스 정보 를 참조하십시오.

개요 및 주요 기능

ICAP(Internet Content Adaption Protocol) 통합은 다양한 플랫폼에서 중요한 데이터의 사용 및 이동을 추적하는 데 도움이 됩니다.

이 통합에는 다음과 같은 주요 기능이 포함됩니다.

- DLP 경보 수집: 사용자는 지정된 Amazon S3 버킷에서 DLP 경보 수집을 구성하고 예약할 수 있습니다. 여기에는 델타 임포트를 수행하여 새 데이터만 수집되도록 하는 기능이 포함됩니다.
- DLP 작업 영역에 수집된 경고 표시: 경고가 수집되면 DLP 작업 영역에 표시되어 일치 내용, 경고 심각도 및 관련 메타데이터와 같은 각 경고에 대한 주요 세부 정보를 제공해야 합니다.
- 일치 콘텐츠: 중요한 정보 기록은 수집 중에 생성되며, 기록이 열릴 때 일치 콘텐츠를 가져옵니다.
- 증거 파일 다운로드: 시스템을 사용하면 사용자가 추가 조사 또는 검토를 위해 DLP 작업 영역에서 직접 관련 증거 파일을 다운로드할 수 있습니다.
- ICAP DLP 인시던트와 ServiceNow 인시던트 간의 심각도 매핑을 사용자 지정하고 정의하는 능력.

데이터 손실 방지를 위한 ICAP DLP 통합 시작하기

통합을 사용하려면 먼저 다음에서 다운로드해야 합니다. ServiceNow# Store

검사 목록

데이터 손실 방지를 위한 제공자 ICAP DLP 통합 설정을 시작하기 전에 다음 정보를 검토합니다.

검사 목록

필드	설명
필요한 ServiceNow AI PlatformData Loss Prevention 애플리케이션 애플리케이션 역할을 할당했는지 확인합니다.	다음의 ICAP DLP 통합에서 사용되는 역할은 다음과 같습니다.ServiceNow AI Platform

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

검사 목록

필드	설명
	• 관리자(admin)는 Data Loss Prevention 관리자(sn_dlir.admin)에서 ServiceNow# Store 애플리케이션을 설치하고 할당합니다. • sn_dlir.admin 역할을 가진 사용자는 통합을 구성하고 인시던트 프로파일을 설정할 수 있습니다. • sn_dlir.analyst 역할을 가진 사용자는 통합 구성 전반에 걸쳐 읽기 역할을 갖게 됩니다.
필요한 Amazon S3 버킷 정책을 할당했는지 확인합니다.	다음 링크를 통해 IAM 사용자, 정책 및 권한을 생성하고 관리하는 방법에 대한 공식 AWS 설명서를 따를 수 있습니다. • IAM 사용자 생성 • IAM 정책 생성 • Amazon S3 권한 주: 위의 링크를 사용하여 AWS에서 IAM 사용자 및 S3 권한을 관리하기 위한 자세한 지침 및 추가 옵션, AWS 계정 - AWS Identity and Access Management에서 IAM 사용자를 생성하는 방법, AWS Identity and Access Management에서 IAM 사용자 및 자격 증명을 생성하는 데 사용되는 프로세스의 기본 개요에 대해 자세히 알아볼 수 있습니다.
ServiceNow# ICAP DLP 통합을 지원하는 데 필요한 핵심 애플리케이션이 설치되고 활성화되었는지 확인합니다.	다음 DLP 애플리케이션 및 보안 지원 일반 애플리케이션이 ServiceNow Store에서 설치되고 활성화되었는지 확인합니다. 설치되지 않은 경우 애플리케이션에 설치하고 활성화합니다. • Security Support Common • 보안 케이스 관리 공통 작업 공간 구성요소입니다. • 데이터 손실 방지 인시던트 응답

ICAP DLP 통합 설치 및 구성

인스턴스에서 제공자 ICAP DLP 통합을 ServiceNow# StoreServiceNow AI Platform 설치하고 구성합니다. 제공자 ICAP DLP 인시던트 데이터를 사용하여 DLP 인시던트 조사를 시작합니다.

시작하기 전에
필요한 역할: sn_dlir.admin

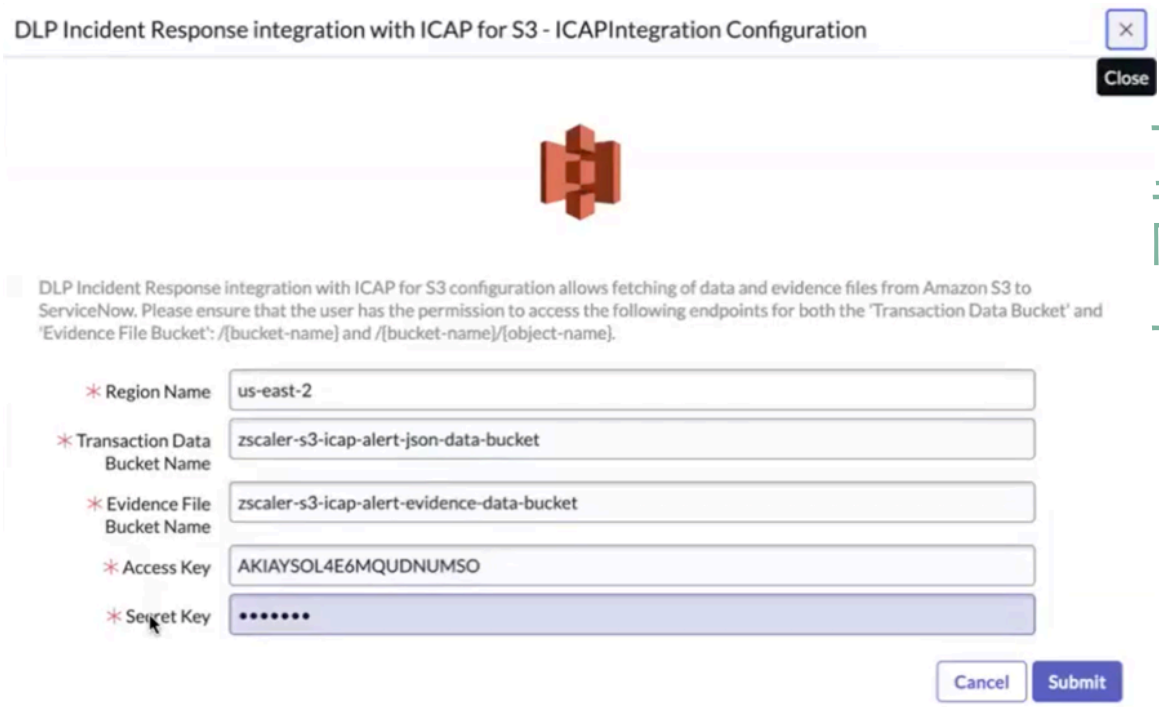
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 에서 ServiceNow# Store 제공자 ICAP DLP 통합을 다운로드하고 설치합니다.
2. 다음으로 이동 보안 운영 〉 통합 〉 통합 구성.
3. ICAP와의 DLP 인시던트 응답 통합 타일을 검색하고 구성을 클릭합니다.
4. 양식에서 필드를 채웁니다.

ICAP DLP 통합 구성 양식

필드	설명
지역 이름	Amazon S3 버킷 이름의 지역 이름입니다.
트랜잭션 데이터 버킷 이름	트랜잭션 데이터 버킷 이름은 DLP 위반 트랜잭션이 발생한 버킷입니다.
증거 파일 버킷 이름	증거 파일 버킷 이름은 위반을 일으킨 DLP 파일을 찾을 수 있는 버킷입니다.
접근 키	ICAP 구성을 위한 AWS IAM 접근 키입니다.
비밀 키	ICAP 구성에 대한 AWS IAM 비밀 키입니다.



5. 제출을 클릭합니다.

결과

주:
ICAP 하위 프로젝트를 ServiceNow 하위 제품에 연결하십시오. 계정이 로그아웃되지 않도록 인스턴스 간에 모든 사용자 이름과 암호를 동기화된 상태로 유지합니다.

구성을 성공적으로 확인하고 제출하면 ICAP DLP 통합 구성이 저장됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

ICAP DLP 통합을 위한 프로파일 생성

인스턴스에 인시던트 프로파일을 ServiceNow AI Platform 생성합니다. DLP 인시던트를 생성하는 데 적합한 ICAP DLP 경보를 결정합니다.

시작하기 전에

필요한 역할: sn_dlir.admin

이 태스크 정보

Amazon S3 구성에서 DLP 경보를 가져오도록 NowPlatform을 구성합니다. 이러한 경보를 ServiceNow 인스턴스에 DLP 인시던트로 저장합니다.

프로시저

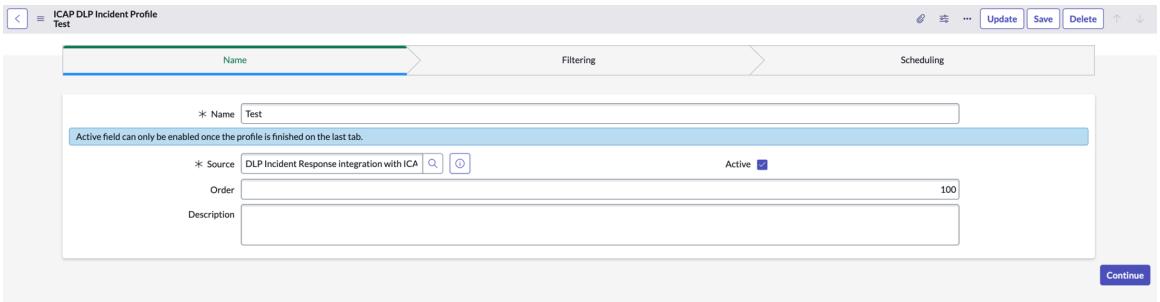
1. 다음으로 이동 모두 〉 **ICAP DLP** 통합 〉 인시던트 프로파일.
2. 새로 만들기를 클릭합니다.
3. 양식에서 이름 섹션의 필드에 내용을 입력합니다.

프로파일 생성

필드	설명
이름	프로필의 이름입니다. 이 필드는 프로파일을 식별하는 데 도움이 됩니다. 주: 각 프로파일 이름은 고유해야 합니다.
소스	인시던트를 수집하도록 구성한 Amazon S3 구성입니다. 여러 소스가 구성된 경우 프로파일에 대해 수집하려는 인시던트 유형에 적합한 소스를 선택합니다. 주: 활성 프로파일에는 단일 소스만 허용됩니다.
활성	프로파일이 활성 상태인지 여부를 나타내는 옵션입니다. 이 필드는 예약 섹션에서 마침 을 클릭한 후에만 활성화할 수 있습니다. 프로파일이 활성 상태이면 ICAP DLP 경고를 적극적으로 폴링하고 있음을 ServiceNow AI Platform 의미합니다. 필터링 조건이 제공한 일정 매개 변수에 따라 일치하면 해당 DLP 경고가 DLP에 만들어집니다.
순서	프로파일 실행 순서입니다. 순서가 가장 낮은 프로파일이 가장 높은 우선 순위로 간주됩니다. 기본적으로 이 값은 100입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
설명	이 프로파일에 대한 설명입니다.



다음에 수행할 작업
필터링 섹션으로 이동하려면 계속을 클릭합니다.

인시던트 생성에 적용할 필터 정의

수신 DLP 경보를 필터링하기 위한 필터 조건을 정의하고 설정합니다. ServiceNow에서 DLP 인시던트로 생성할 경보를 결정합니다.

시작하기 전에
필요한 역할: sn_dlir.admin

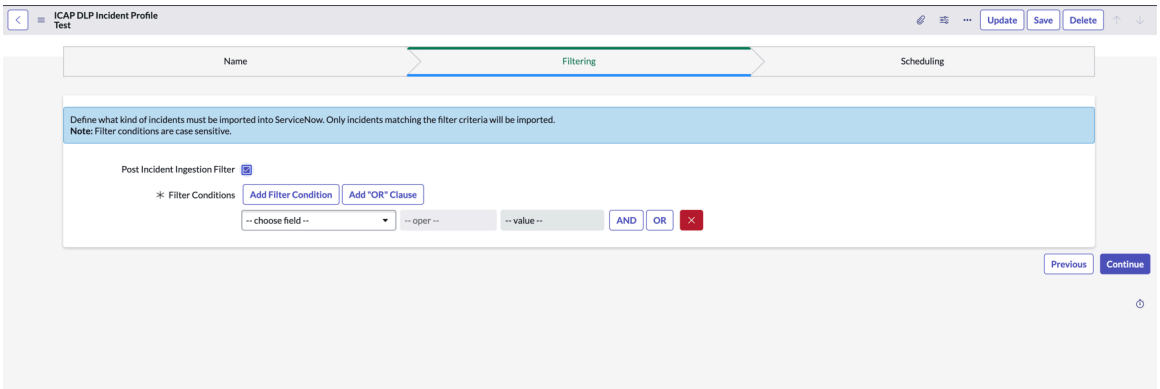
이 태스크 정보
필터링을 사용하면 DLP 경고를 격리하고 만드는 DLP 경고 수를 제한할 수 있습니다. 추가 필터링 기준이 설정되면 조건과 일치하는 경보만 생성됩니다.

프로시저

1. 사후 인시던트 수집 필터를 적용하고 필터 기준과 일치하는 인시던트를 검색하려면 사후 인시던트 수집 필터 확인란을 선택합니다.
2. 조건에 따라 필터링 옵션을 선택하고 DLP 인시던트가 생성되도록 수신 ICAP DLP 인시던트가 충족해야 하는 기준을 정의합니다.
3. 필터 조건 필드에서 필터를 설정합니다.

   드롭다운 필터 조건 의 옵션은 **ICAP DLP** 인시던트 임포트 테이블에서 사용할 수 있는 필드와 일치합니다. 입력하는 기준은 대/소문자를 구분합니다. 정의하는 기준이 인시던트의 값과 일치하는지 확인합니다.

4. **AND** 또는 **OR**을 클릭하여 조건을 더 추가합니다.
   - **AND**를 선택하면 모든 조건이 일치해야 합니다.
   - **OR**을 선택하면 두 조건을 일치시킬 수 있습니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 수행할 작업
일정을 구성하려면 계속을 클릭합니다.

ICAP DLP 인시던트 검색 예약

프로파일의 기준과 일치하는 ICAP DLP 경보를 검색하도록 일정을 설정합니다.

시작하기 전에
필요한 역할: sn_dlir.admin

이 태스크 정보
인시던트 프로파일 구성과 일치하는 순 신규 ICAP 인시던트를 폴링하는 빈도를 계획할 수 있습니다. 자동 인시던트 수집을 사용하려면 프로파일을 활성화하기 전에 예약 및 인시던트 검색을 구성해야 합니다. 일회성 검색 확인란을 사용하여 일회성 검색을 수행하도록 프로파일을 구성할 수 있습니다.

프로시저

1. ICAP에서 인시던트를 끌어오는 방법과 시기를 정의하도록 일정을 구성합니다.
2. 양식에서 필드를 채웁니다.

ICAP DLP 인시던트 예약

필드	설명
지속적 인시던트 수집	인스턴스가 새 인시던트에 대해 ICAP에서 끌어오는 지속적 인시던트 수집 ServiceNow AI Platform 입니다. 인시던트 필터링 기준과 일치하는 트리거된 인시던트가 발견되면 DLP 인시던트가 생성됩니다.
폴링 증분(분)	분 단위로 정의된 폴링 빈도입니다. 이 기본값은 **5**로 설정됩니다.
초기 인시던트 수집 시간 설정	구성된 날짜 및 시간을 기준으로 초기 인시던트 수집을 설정하는 옵션입니다. 이 옵션을 사용하여 초기 수집에 대한 특정 날짜 및 시간을 정의할 수 있습니다. 후속 수집은 폴링 간격 기간을 기반으로 합니다.
초기 인시던트 수집 시간 입력	인시던트 수집을 위해 지정하는 날짜 및 시간입니다.
초기 인시던트 수집 시간	데이터를 처음으로 수집할 때입니다. 주: 이 값은 초기 인시던트 수집 시간 설정 옵션을 선택한 경우에만 표시됩니다.
다음 인시던트 수집 시간(예상)	다음 예상 인시던트 수집 시간입니다.
일회성 검색	일회성 기록 데이터 끌어오기를 활성화하는 옵션입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	주: 이 옵션을 선택하면 날짜 이후에 추가된 날짜에 따라 ICAP DLP에서 기록 데이터를 끌어옵니다.
폴더 이름	데이터를 검색할 폴더의 이름입니다. 사전순으로 제공된 폴더 이름보다 이름이 큰 모든 폴더는 일회성 검색으로 수집됩니다.

3. 마침을 클릭합니다.
4. 팝업에서 마침을 클릭하여 생성된 프로파일 구성을 저장합니다.
5. 프로파일을 활성화합니다.
   a. 생성된 프로파일을 엽니다.
   b. 활성을**true**로 설정합니다.
   c. 업데이트를 클릭합니다.

결과
프로파일이 성공적으로 생성되면 프로파일의 구성에 따라 주기적으로 인시던트를 가져옵니다. 경보가 DLP 인시던트 테이블에 추가됩니다.

DLP 경보에 대한 중요한 정보 보기

DLP 경보에 대해 탐지된 중요한 정보를 봅니다.

시작하기 전에
각 통합에 구성된 특정 규칙과 정책이 있으며, 정의된 정책을 위반할 때마다 DLP 인시던트가 생성되고 해당 DLP 인시던트 기록의 중요한 정보 섹션 아래에 정보를 위반한 일치 컨텐츠가 표시됩니다.

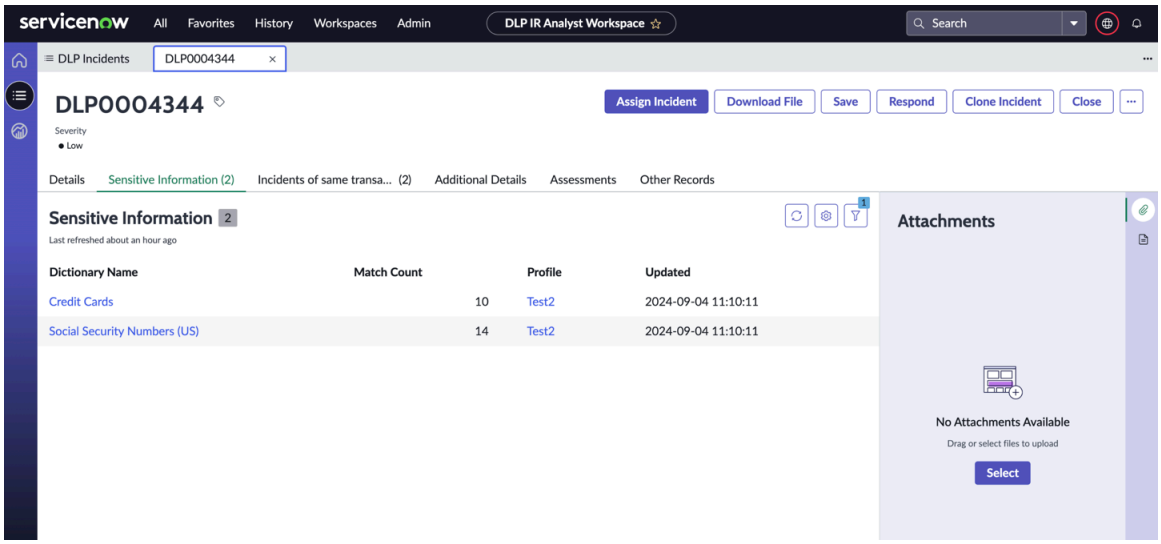
필요한 역할: sn_dlir.analyst

주:
최종 사용자는 DLP 사용자 작업 영역에 로그인하여 중요한 정보를 볼 수도 있습니다.

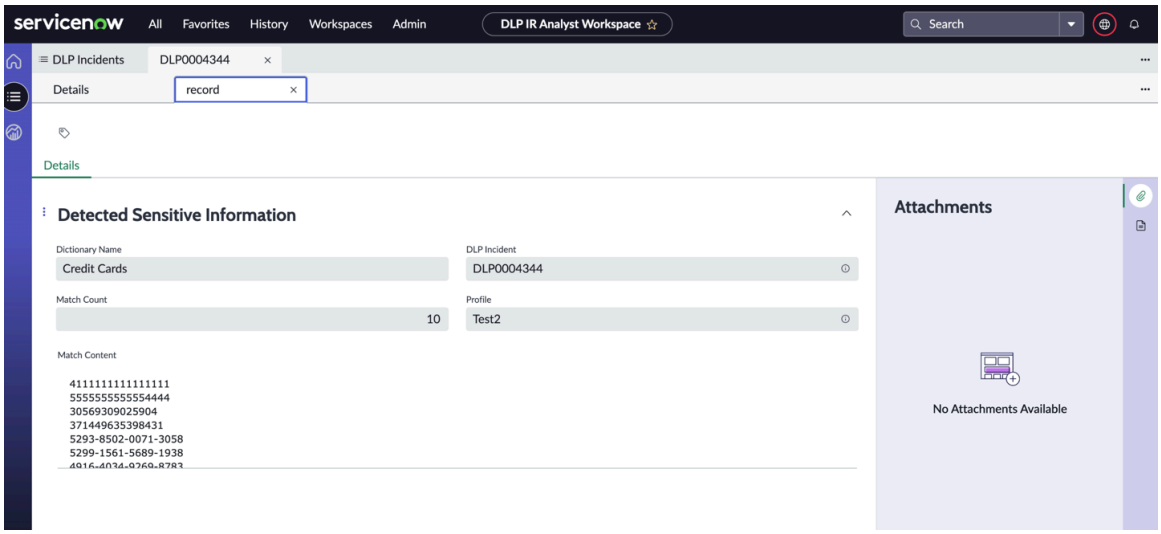
프로시저

1. 다음으로 이동 모두 〉 **DLP** 인시던트 관리 〉 **DLP** 분석가 작업 공간.
   분석가를 위해 DLP 분석가 작업 공간에 DLP 작업 공간 - 내 인시던트 페이지가 표시됩니다.
2. DLP 인시던트를 엽니다.
3. 중요한 정보 탭으로 이동합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 위반된 기록을 클릭합니다.
5. 경기 내용 정보를 보고 필요에 따라 각 조치를 취합니다.



DLP 경보에 대한 증거 파일 다운로드

ICAP를 지원하는 공급자에 대한 DLP 정책을 위반하는 파일을 다운로드합니다. 승인자용 DLP IR 분석가 작업 공간 및 DLP IR 최종 사용자 작업 공간에서 로컬 머신으로 이 파일을 다운로드합니다.

시작하기 전에

필요한 역할:

- sn_dlir.분석가 및 승인자는 다음을 다운로드할 수 있습니다.

이 태스크 정보

계속 진행하기 전에 ICAP에 대한 파일 다운로드를 사용하도록 설정해야 합니다.

프로시저

1. 다음으로 이동 모두 〉 **ICAP DLP** 통합 〉 설정.
2. 속성 sn_icap_dlp.enable_file_download를 활성화합니다. 이 속성을 활성화하면 보고된 **ICAP** 인시던트의 증거 파일을 다운로드할 수 있습니다.
   DLP IR 분석가 작업 공간 및 DLP IR 최종 사용자 작업 공간에서 파일 다운로드 버튼을 볼 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 다음으로 이동 모두 〉 **DLP** 인시던트 관리 〉 **DLP** 분석가 작업 공간.
4. ICAP 제공자 소스에서 수집된 DLP 인시던트 기록을 엽니다.
5. 파일 다운로드를 클릭합니다.

> **주:**
> DLP 관리자는 DLP 관리의 고급 설정 페이지에서 보고된 인시던트의 위반 파일 다운로드가 허용되어야 함 옵션을 비활성화하여 모든 통합에 대한 파일 다운로드 작업의 액세스를 제어할 수 있습니다. 자세한 내용은 고급 설정 구성 문서를 참조하십시오.

ICAP에 대한 증거 파일 미리 보기

DLP IR 분석가 작업 공간에서 DLP 인시던트 증거 파일을 미리 봅니다.

시작하기 전에

- 다음으로 이동 모두 〉 **DLP** 관리 〉 고급 설정.
- **sn_icap_dlp.enable_evidence_file_preview** 속성이 이미 활성화되어 있는지 확인합니다.

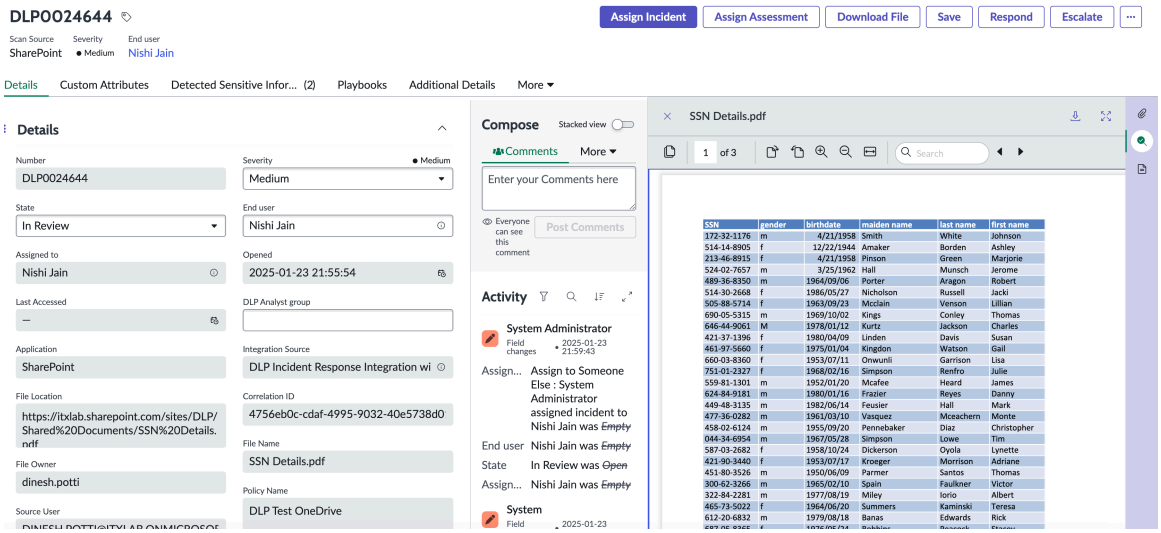
> **중요사항:**
> DLP 분석가 작업 공간에서 증거 파일 작업을 사용하는 동안 증거 파일은 고급 설정 페이지의 **sn_dlir.preview_temp_files_cleanup_interval** 속성을 사용하여 선택한 기간 동안 암호화되지 않은 형식으로 ServiceNow 데이터베이스에 임시로 저장됩니다. ServiceNow 데이터베이스에 데이터를 저장하지 않으려면 증거 파일 미리 보기 기능을 비활성화할 수 있습니다. 자세한 내용은 고급 설정 구성 문서를 참조하십시오.

필요한 역할: sn_dlir.analyst

프로시저

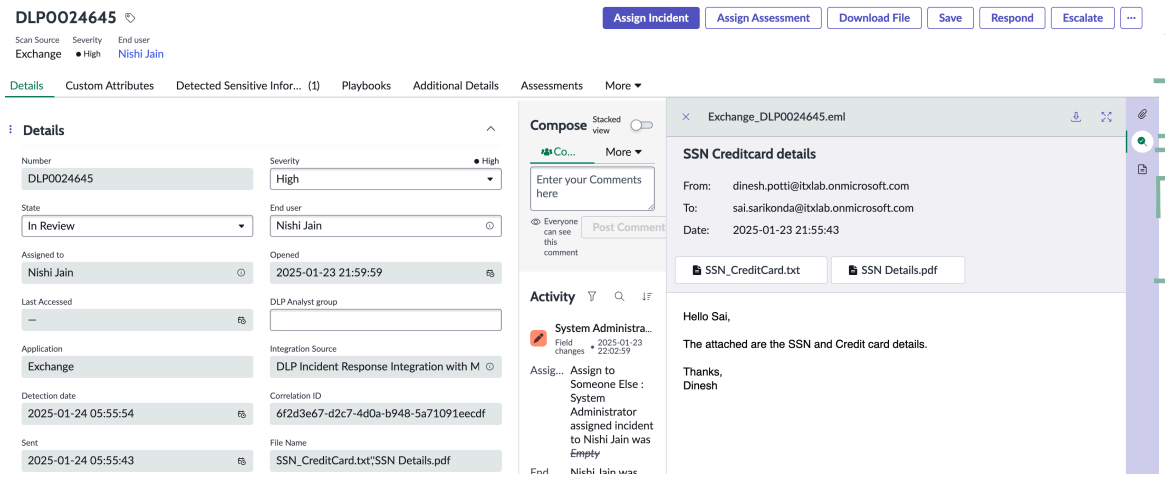
1. 다음으로 이동 모두 〉 **DLP** 인시던트 관리 〉 **DLP** 분석가 작업 공간.
2. DLP 인시던트 기록을 엽니다.
3. 상황별 메뉴에서 사용할 수 있는 증거 파일 아이콘을 선택합니다.
   모든 증거 파일을 가져오는 탭이 열립니다. 다운로드가 완료되면 증거 파일 탭에서 모든 증거 파일을 볼 수 있습니다.
4. 미리 보려는 증거 파일 카드를 선택합니다.
   미리 보기 기능은 파일 형식마다 다릅니다.
5. 증거 파일의 오른쪽 상단에 있는 확장 아이콘을 선택하여 문서 뷰어에서 PDF 및 Office 문서를 미리 보고 PDF를 전체 화면으로 엽니다.
   문서 뷰어가 증거 파일을 여는 Office 확장에는 doc, docx, ppt, pptx, xls, xlsx가 포함됩니다.
   a. 검색 창을 찾아 찾고 있는 키워드를 입력합니다.
   b. 확대 및 축소 기능을 사용하여 뷰를 조정하여 가독성을 높입니다.
   c. 페이지를 시계 방향 또는 시계 반대 방향으로 회전하면 내용을 더 선명하게 볼 수 있습니다.
   이러한 제어 옵션은 증거 파일을 포괄적으로 이해하는 능력을 향상시킵니다. PDF에만 머리글에 제어 옵션이 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

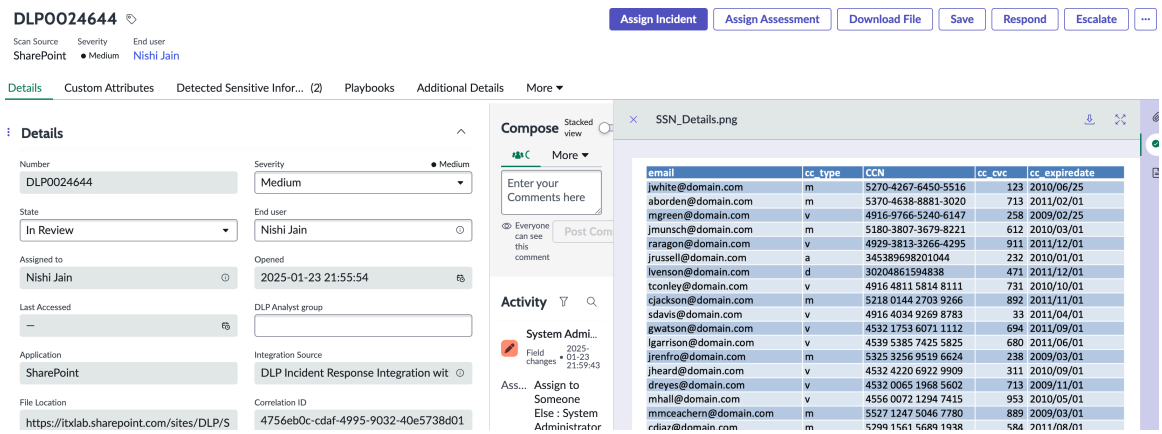


6. eml 파일을 미리 봅니다.
이메일에서 첨부 파일을 선택하고 미리 봅니다.

주:
선택한 증거 파일이 5MB 한도를 초과하는 경우 분석가 작업 공간에서 미리 볼 수 없습니다. 내용을 미리 보려면 파일을 다운로드해야 합니다. 이 제한은 .eml 파일에만 적용됩니다.

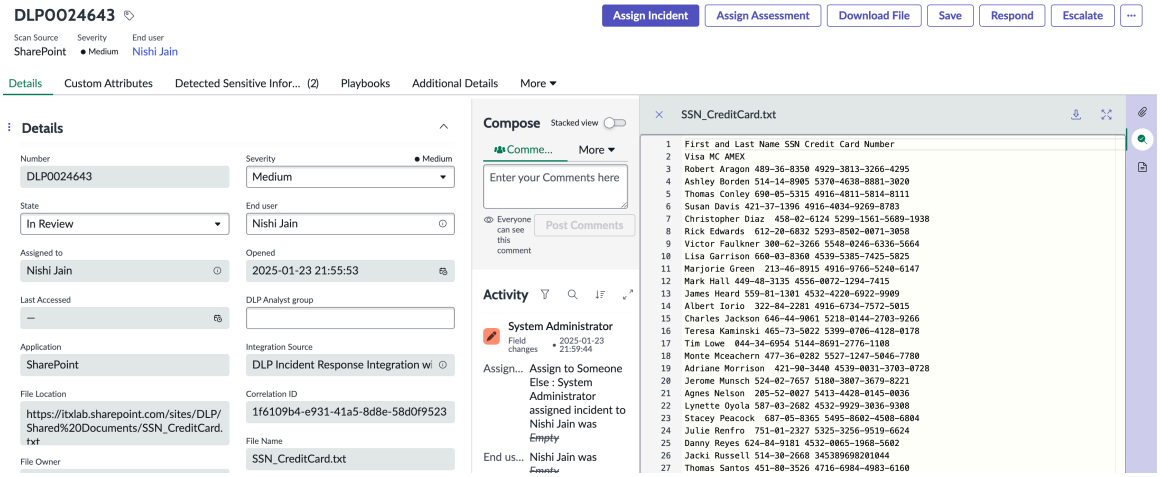


7. DLP 분석가 작업 공간에서 이미지를 미리 봅니다.
.bmp, .gif, .ico, .jpeg, .jpg, .png, .svg 및 .webp 확장자를 가진 이미지만 지원됩니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

8. 증거 파일의 오른쪽 위에 있는 확장 아이콘을 선택하여 텍스트 편집기에서 텍스트 파일을 미리 봅니다.



> **주:**
> Office 문서, eml 파일, 텍스트 및 이미지 확장명을 제외한 증거 파일은 미리 보기에 지원되지 않습니다. 이진 파일은 렌더링되지 않으며 콘텐츠를 미리 보려면 다운로드해야 합니다. 증거 파일 미리 보기 기능은 보관된 인시던트에도 사용할 수 있습니다.

ICAP DLP 통합 설정 검토

제공자 ICAP DLP 통합 설정을 검토하고 환경에 맞게 기본 시스템 속성을 수정합니다.

시작하기 전에
필요한 역할: sn_dlir.admin

프로시저

1. 다음으로 이동 모두 〉 **ICAP DLP** 통합 〉 설정.
2. 설정을 검토하고 수정해야 합니다.

Microsoft가 포함된 **Data Loss Prevention Incident Response**

with Microsoft 는 Data Loss Prevention Incident Response 미리 보기 앱(MicrosoftTeams, Exchange Online, SharePoint Online, 비즈니스용 OneDrive) 및 기타 이벤트 유형과 같은 Microsoft 여러 소스에서 DLP(데이터 손실 방지) 인시던트를 가져오는 핵심 프레임워크를 제공합니다. 엔드포인트 장치는 자동화된 인시던트 할당 및 에스컬레이션을 통해 최종 사용자, 관리자 및 DLP 운영 팀이 참여하는 정정 워크플로우를 활성화합니다.

스토어에서 앱 요청

ServiceNow Store 웹 사이트를 방문하면 사용 가능한 모든 앱을 확인하고 스토어에 요청을 제출하는 방법에 대한 정보를 참조할 수 있습니다. 출시된 모든 앱의 누적 릴리스 정보는 ServiceNow Store 버전 기록 릴리스 정보를 참조하십시오.

주요 기능

이 통합의 주요 기능을 사용하여 다음 작업을 수행합니다.

- 서로 다른 계정에 대해 여러 프로필을 생성합니다.
- 인시던트 생성을 DLP IR 자동화합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- Microsoft DLP IR 이벤트 필드를 DLP IR 인시던트 필드에 매핑합니다.
- 이벤트를 필터링합니다 Microsoft DLP IR .
- 주기적으로 인시던트를 생성하는 DLP IR 이벤트 수집 DLP IR 을 예약합니다.
- 각 Microsoft DLP 이벤트의 일치하는 컨텐츠를 외부 클라우드 저장소에 저장합니다.
- 에서 ServiceNow인시던트를 DLP IR 삭제할 때 외부 클라우드 저장소에서 일치하는 컨텐츠를 삭제합니다.
- Exchange, OneDrive 및 SharePoint 유형의 인시던트에 대한 DLP IR 파일을 다운로드합니다.

이 통합에 대해 알아보기

문서 식별자	문서 제목
Microsoft 제품 설명서 웹 사이트	Microsoft 제품 설명서 웹 사이트
ServiceNow 제품 설명서 웹 사이트	ServiceNow 제품 설명서 웹 사이트

데이터 손실 방지를 위한 **Microsoft DLP IR** 통합 시작

데이터 손실 방지를 위한 통합 설정을 Microsoft DLP IR 시작하기 전에 다음 정보를 검토합니다.

검사 목록

설정 작업	설명
이벤트 데이터를 가져오기 위한 Microsoft Purview 자격 증명과 일치 콘텐츠를 저장하기 위한 AWS/Azure Storage 계정 자격 증명을 가져옵니다. Microsoft ID 플랫폼에 애플리케이션 등록	여기에서 Microsoft Azure 플랫폼에 애플리케이션을 등록하여 클라이언트 ID, 클라이언트 비밀 및 테넌트 ID를 가져옵니다. 애플리케이션을 만드는 데 필요한 역할에 대한 자세한 내용은 필수 구성 요소를 참조하십시오. Microsoft DLP 통합에서 ServiceNow Microsoft Azure 애플리케이션을 구성하는 데 필요한 API 권한/역할에 대한 자세한 내용은 다음 테이블을 참조하십시오.
Azure 사용자가 Azure Storage에서 Blob 읽기/쓰기/삭제에 액세스하는 데 필요한 권한	Azure 사용자에게는 Azure Storage에서 Blob을 읽고, 쓰고, 삭제할 수 있는 **Storage Blob** 데이터 기여자 역할이 있어야 합니다.
AWS 사용자가 AWS 저장소에서 객체 읽기/쓰기/삭제에 액세스하는 데 필요한 권한	AWS S3 저장소의 객체에 대한 목록, 읽기, 쓰기 및 삭제 액세스 권한을 부여하는 정책을 생성해야 합니다.
데이터 손실 관리 역할에 필요한 ServiceNow AI Platform 역할이 있는지 할당하고 확인합니다.	예상 결과를 구성하고 검증하려면 다음 역할이 필요합니다. • 관리자 역할은 에서 ServiceNow Store 통합을 설치하고 sn_dlir.admin 역할을 할당합니다. • sn_dlir.admin 역할은 다음 작업을 수행합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

검사 목록

설정 작업	설명
	○ 통합을 구성합니다. ○ 인시던트 프로파일을 설정합니다.
ServiceNow 이 통합을 구성하기 전에 Microsoft DLP IR 통합을 지원하는 데 필요한 핵심 애플리케이션이 설치되고 활성화되었는지 확인합니다.	다음 DLP IR 애플리케이션 및 보안 지원 공통 애플리케이션이 스토어에서 설치되고 활성화 ServiceNow 되었는지 확인합니다. 설치되지 않은 경우 애플리케이션에 설치하고 활성화합니다. • Security Support Common • 데이터 손실 방지 인시던트 응답

Microsoft Azure 애플리케이션에 필요한 **API** 권한/역할

Microsoft DLP 통합에서 **ServiceNow** 구성하려면 ***Microsoft Azure*** 애플리케이션에서 다음 ***API*** 권한/역할이 필요합니다.

API	권한 이름	유형	설명	어떤 **ServiceNow** 기능에 필요합니까?	관리자 동의가 필요합니까?
Office 365 관리 API	ActivityFeed.ReadDlp	애플리케이션	검색된 중요한 데이터를 포함한 DLP 정책 이벤트를 읽습니다.	MSFT Purview ServiceNow에서 . 주: 이 권한은 MSFT 데이터를 ServiceNow로 가져오는 데 필수입니다.	예
Microsoft 그래프 API	파일.읽기.모두	애플리케이션	액세스할 수 있는 모든 사이트 모음의 파일을 읽습니다.	파일 다운로드: OneDrive 또는 SharePoint에서 DLP 이벤트를 발생시킨 ServiceNow 인스턴스의 첨부 파일을 다운로드합니다. 주: 선택 사항입니다. 분석가가 DLP 이벤트를 발생시킨 첨부 파일을 다운로드하지 못하도록 하려면 이 API 권한을 건너뛸 수 있습니다.	예

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Microsoft Azure 애플리케이션에 필요한 **API** 권한/역할

Microsoft DLP 통합에서 **ServiceNow** 구성하려면 ***Microsoft Azure*** 애플리케이션에서 다음 ***API*** 권한/역할이 필요합니다.

API	권한 이름	유형	설명	어떤 **ServiceNow** 기능에 필요합니까?	관리자 동의가 필요합니까?
	메일.읽기	애플리케이션	모든 메일함에서 메일을 읽습니다.	파일 다운로드: Exchange에서 DLP 이벤트를 발생시킨 ServiceNow 인스턴스의 이메일 콘텐츠 (본문 및 첨부 파일)를 다운로드합니다. **주:** 선택 사항입니다. 분석가가 DLP 이벤트를 발생시킨 이메일 콘텐츠(본문, 첨부 파일)를 다운로드하지 못하도록 하려면 이 API 권한을 건너뛸 수 있습니다.	예
	사용자.읽기	위임됨	로그인하고 사용자 프로파일을 읽습니다.	모든 새 애플리케이션에 사용할 수 있는 기본 권한입니다.	아니요

탐지된 중요한 정보(선택 사항)

일치 콘텐츠는 Azure Blob Storage 또는 Amazon S3 버킷에 외부에 저장되며 사용자가 인시던트를 볼 때 외부 스토리지에서 끌어옵니다.

사용자가 DLP Core 애플리케이션에서 컨텐츠/검색된 중요한 정보 일치를 보려면 다음 권한 중 하나가 필요합니다.

1. 사용자인 Microsoft Azure 경우 Azure Storage에서 Blob을 읽고, 쓰고, 삭제할 수 있는 Storage Blob 데이터 기여자 역할이 있어야 합니다.
2. Amazon S3 사용자인 경우 Amazon S3 스토리지의 객체에 대한 목록, 읽기, 쓰기 및 삭제 액세스 권한을 부여하는 정책을 생성해야 합니다.

Microsoft DLP 통합 설치 및 구성

인스턴스에서 DLP ServiceNow# StoreServiceNow AI Platform 와의 Microsoft DLP 인시던트 응답 통합을 설치하고 구성합니다. DLP 이벤트 데이터를 사용하여 Microsoft DLP 인시던트 조사를 시작합니다.

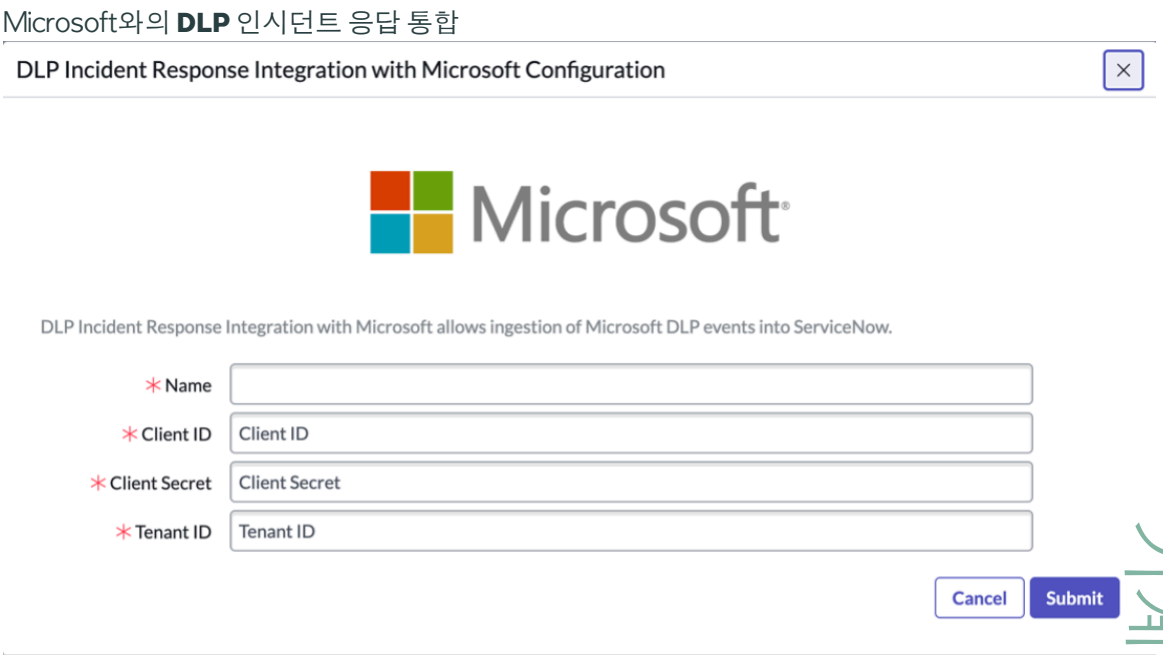
시작하기 전에
필요한 역할: sn_dlir.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. Microsoft 에서 ServiceNow# Store DLP 통합을 다운로드하여 설치합니다.
2. 다음으로 이동 보안 운영 〉 통합 〉 통합 구성.
3. Microsoft DLP 통합을 구성합니다.

   a. **DLP Incident Response Integration with Microsoft** 타일을 검색하고 구성을 클릭합니다.



   b. 양식에서 필드를 채웁니다.

Microsoft DLP 통합 구성 양식

필드	설명
이름	Microsoft DLP 통합 구성의 이름입니다.
클라이언트 ID	Microsoft Azure 포털에서 작성된 앱의 클라이언트 ID입니다.
클라이언트 비밀	Microsoft Azure 포털에서 작성된 앱의 클라이언트 비밀입니다.
테넌트 ID	사용자의 테넌트 ID입니다.

   c. 제출을 클릭합니다.

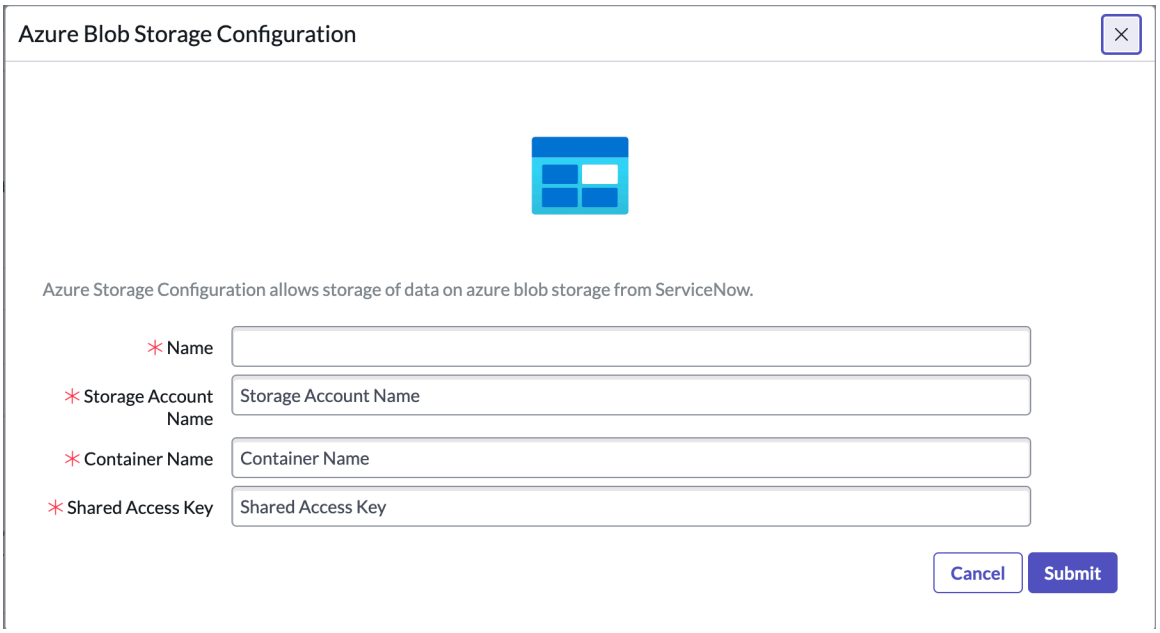
   구성을 성공적으로 확인하고 제출하면 Microsoft DLP 통합이 보안 통합 페이지에 타일로 저장됩니다.

4. Azure 저장소 구성을 업데이트합니다.

   a. 보안 통합 페이지에서 **Azure** 저장소 구성 타일을 검색합니다.

   b. Azure Storage 구성 타일에서 업데이트를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



c. 양식에서 필드를 채웁니다.

Azure 저장소 구성 양식

필드	설명
이름	Azure 저장소 구성의 이름입니다.
스토리지 계정 이름	Azure Portal에서 만든 스토리지 계정 이름
컨테이너 이름	Azure Portal의 스토리지 계정에서 만든 컨테이너 이름입니다.
공유 액세스 키	저장소 계정에 대한 공유 액세스 키입니다.

d. 제출을 클릭합니다.

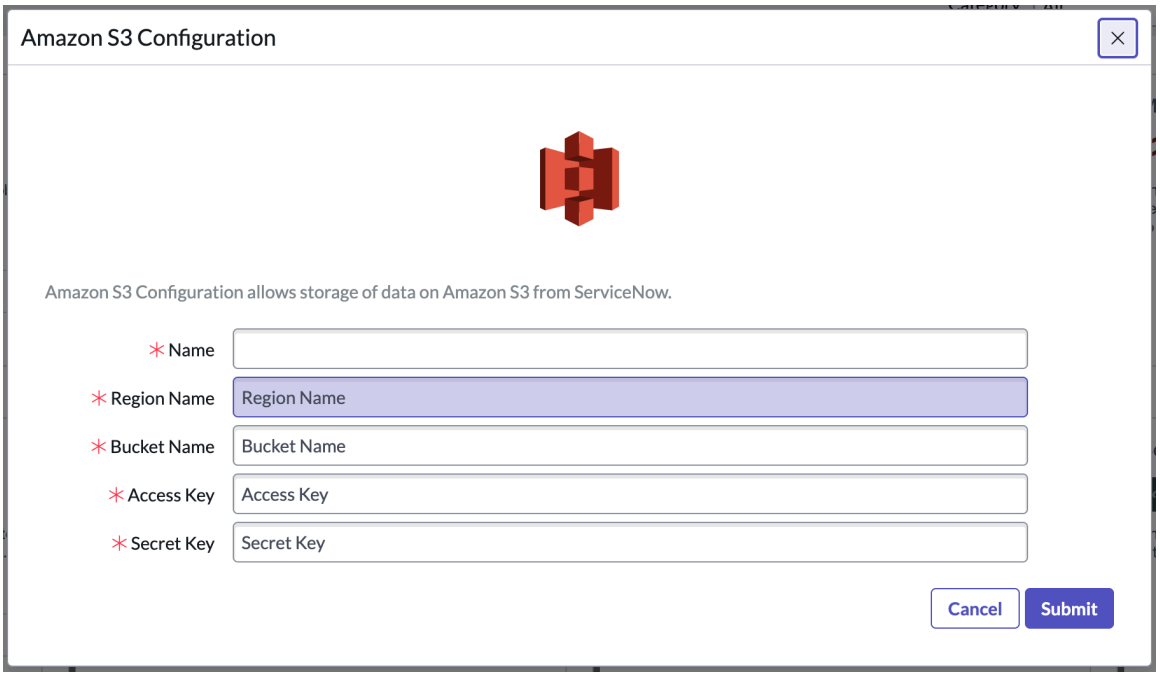
구성을 성공적으로 확인하고 제출하면 Azure 저장소 구성이 보안 통합 페이지에 타일로 저장됩니다.

5. AWS 저장소 구성을 업데이트합니다.

a. 보안 통합 페이지에서 **AWS** 저장소 구성 타일을 검색합니다.

b. AWS 저장소 구성 타일에서 업데이트를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



c. 양식에서 필드를 채웁니다.

AWS 저장소 구성 양식

필드	설명
이름	AWS 저장소 구성의 이름입니다.
지역 이름	AWS 저장소 계정의 지역 이름입니다.
버킷 이름	AWS 포털에서 생성된 버킷 이름입니다.
접근 키	읽기, 쓰기 및 삭제 권한이 있는 접근 키입니다.
비밀 키	읽기, 쓰기 및 삭제 권한이 있는 공유 키

d. 제출을 클릭합니다.

결과
구성을 성공적으로 확인하고 제출하면 AWS S3 구성이 보안 통합 페이지에 타일로 저장됩니다.

DLP 통합을 위한 **Microsoft** 새 인시던트 프로파일 생성

인스턴스에 인시던트 프로파일을 ServiceNow AI Platform 생성하여 Microsoft Purview에서 데이터를 검색하고 인시던트 테이블에 데이터를 ServiceNow DLP IR 추가합니다.

시작하기 전에
필요한 역할: sn_dlir.admin(만들기, 편집 및 삭제)

sn_dlir.analyst - 뷰(읽기 전용)

이 태스크 정보
Purview에서 Microsoft 이벤트를 검색하도록 구성합니다ServiceNow AI Platform#. 이러한 이벤트를 DLP IR 인스턴스의 인시던트 테이블에 ServiceNow# 저장합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 **Microsoft DLP** 통합 〉 인시던트 프로파일.
2. 새로 만들기를 클릭합니다.
3. 양식에서 이름 섹션의 필드에 내용을 입력합니다.

프로파일 양식 만들기

필드	설명
이름	프로필의 이름입니다. 이 필드는 프로파일을 식별하는 데 도움이 됩니다. 주: 각 프로파일 이름은 고유해야 합니다.
소스	Microsoft DLP IR 인시던트를 수집하도록 구성한 인스턴스입니다. 통합 구성이 여러 개인 경우 프로파일에 수집하려는 인시던트 유형에 적합한 통합 구성 기록을 선택합니다.
활성	프로파일이 활성 상태인지 여부를 나타내는 옵션입니다. 이 필드는 예약 섹션에서 마침 필드를 클릭한 후에만 활성화할 수 있습니다. 프로필이 활성 상태이면 프로필에 ServiceNow AI Platform 정의된 구성에 따라 이벤트를 적극적으로 폴링 Microsoft DLP IR 하고 있음을 의미합니다.
순서	프로파일 실행 순서입니다. 순서가 가장 낮은 프로파일이 가장 높은 우선 순위로 간주됩니다. 기본적으로 이 값은 100입니다.
설명	프로파일에 대한 고유 설명입니다.

다음에 수행할 작업
필터링 섹션으로 이동하려면 계속을 클릭합니다.

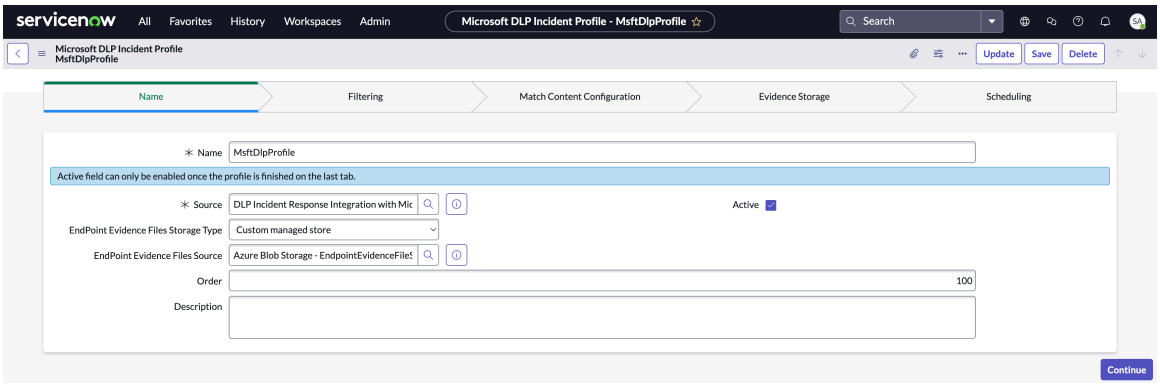
Microsoft Purview 엔드포인트 스토리지 구성

Microsoft Purview 엔드포인트 증거 파일 스토리지 구성은 Purview - 사용자 지정 관리 저장소 또는 Microsoft 관리형 스토리지 환경에서 엔드포인트 증거 파일이 저장되는 위치를 알려줍니다.

Microsoft 관리 저장소의 경우 Microsoft 자체에서 증거 파일을 일부 위치에 저장하고 사용자 지정 관리 저장소의 경우 경고가 생성될 때 purview에서 증거 파일을 저장할 컨테이너를 지정해야 합니다.

시스템의 미리 보기 끝에서 구성 중인 항목에 따라 두 스토리지 유형 중 하나를 선택하여 해당 엔드포인트 DLP 인시던트의 증거 파일을 가져옵니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



주:
Microsoft는 현재 Microsoft Managed Store에서 증거 파일을 검색하는 API를 제공하지 않으므로 사용자 지정 관리 저장소를 사용하는 것이 좋습니다. 따라서 Microsoft Managed Store 저장된 증거에 대해 미리 보기 및 다운로드 기능이 지원되지 않습니다. Microsoft는 이 제한과 관련하여 Microsoft에 소송을 제기했습니다.

인시던트 생성에 적용할 필터 정의

수신 Microsoft DLP 이벤트를 필터링하기 위한 필터 조건을 정의하고 설정합니다. 이러한 이벤트 중 어떤 이벤트를 인스턴스에서 인시던트 ServiceNow 로 DLP IR 생성할지 제어합니다.

시작하기 전에
필요한 역할: sn_dlir.admin(만들기, 편집 및 삭제)

sn_dlir.analyst - 뷰(읽기 전용)

이 태스크 정보
이러한 유형의 필터링을 사용하면 Microsoft DLP 이벤트를 격리하여 생성하는 인시던트 수를 DLP IR 제한할 수 있습니다. 필터링 기준이 설정되면 조건과 일치하는 이벤트만 DLP 인시던트로 생성됩니다.

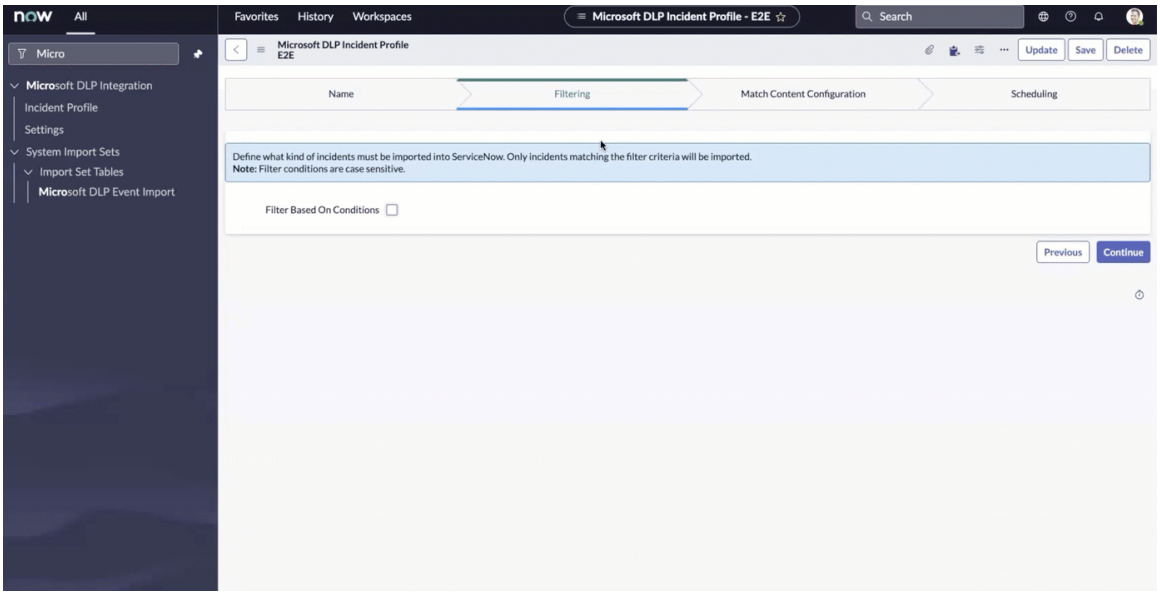
프로시저

1. 조건에 따라 필터링 옵션을 선택합니다.
2. 조건 작성기의 목록과 필드를 사용하여 필터 조건 필드에서 필터를 설정합니다.

   DLP 인시던트가 생성되도록 수신 Microsoft DLP 이벤트가 충족해야 하는 기준을 정의합니다.

   필터 조건의 첫 번째 필드에 있는 옵션은 Microsoft DLP 이벤트에서 사용할 수 있는 필드와 일치합니다. 입력하는 기준은 대/소문자를 구분합니다. 정의하는 기준이 이벤트의 값과 일치하는지 확인합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



3. **AND** 또는 **OR**을 클릭하여 조건을 더 추가합니다.
   - **AND**를 선택하면 모든 조건이 일치해야 합니다.
   - **OR**을 선택하면 두 조건을 일치시킬 수 있습니다.
4. 계속을 클릭하고 컨텐츠 구성 일치 섹션으로 이동합니다.
   이전에는 UserID가 원본 사용자 필드에만 매핑되었지만 UserID 필드는 현재 엔드포인트 이벤트를 비롯한 모든 Purview 이벤트에 대한 조회 특성으로 사용할 수 있습니다.

인시던트에 대한 일치 컨텐츠 구성

DLP IR 인시던트에 액세스하는 동안 부하에서 해당 콘텐츠를 검색하기 위해 Azure Storage 또는 AWS S3 버킷과 같은 외부 클라우드 스토리지에 중요한 정보를 저장하는 구성을 제공합니다.

시작하기 전에
필요한 역할: sn_dlir.admin(만들기, 편집 및 삭제)

sn_dlir.analyst - 뷰(읽기 전용)

프로시저

1. 진행률 표시줄에서 컨텐츠 일치 구성 단계를 클릭합니다.
2. 양식에서 필드를 채웁니다.

컨텐츠 구성 일치

필드	설명
일치 컨텐츠 저장	일치하는 컨텐츠를 클라우드 스토리지에 저장하는 옵션입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	중요사항: 이 옵션을 선택하지 않으면 DLP 작업 공간에서 DLP 인시던트에 대한 정책 일치 콘텐츠를 볼 수 없습니다. 이 옵션을 활성화하면 DLP 인시던트에 반환된 일치 콘텐츠가 외부 클라우드 스토리지(예: Azure, AWS)에 저장됩니다. 작업 공간에서 DLP 인시던트가 열릴 때마다 일치 콘텐츠를 검색하고 표시할 수도 있습니다. 외부 클라우드 저장소 구성에 대한 자세한 내용은 문서를 참조하십시오 Microsoft DLP 통합 설치 및 구성.
인시던트 삭제 시 일치 컨텐츠 삭제	외부 클라우드 저장소에서 인시던트 일치 컨텐츠를 삭제하는 옵션입니다. 이 옵션은 일치 컨텐츠 저장 필드를 선택한 경우에만 표시됩니다.
외부 클라우드 자격 증명	매치 콘텐츠가 저장되는 외부 클라우드 저장소입니다. 저장소 구성에 추가된 외부 클라우드 자격 증명을 참조할 수 있습니다. 이 옵션은 일치 컨텐츠 저장 필드를 선택한 경우에만 표시됩니다.

3. 계속을 클릭하고 예약 섹션으로 이동합니다.

DLP IR Microsoft 인시던트 검색 예약

인시던트 데이터를 검색하고 프로파일의 기준과 일치하는 인시던트를 수집 Microsoft DLP IR 하도록 일정을 설정합니다. 에서 인시던트를 Microsoft가져오는 방법과 시기를 정의하도록 일정을 구성합니다.

시작하기 전에
필요한 역할: sn_dlir.admin(만들기, 편집 및 삭제)

sn_dlir.analyst - 뷰(읽기 전용)

이 태스크 정보
인시던트 프로파일 구성과 일치하는 향후 인시던트를 폴링할 빈도를 계획할 수 있습니다. 자동 인시던트 수집을 사용하려면 프로파일을 활성화하기 전에 예약 및 인시던트 검색을 구성해야 합니다. 일회성 검색 확인란을 사용하여 일회성 검색을 수행하도록 프로파일을 구성할 수 있습니다. 이력 날짜는 현재 날짜로부터 최근 3개월까지입니다.

폴링 간격은 각 프로파일에 대해 개별적으로 구성됩니다. 다양한 폴링 간격은 인시던트 통합의 성능에 영향을 줄 수 있습니다 Microsoft DLP IR . 일정을 예약할 때 인시던트의 긴급도에 따라 시스템 부하의 균형을 맞추도록 계획합니다.

프로시저

1. 데이터를 검색하고 프로파일의 기준과 일치하는 인시던트를 수집하도록 일정을 설정합니다.
2. 양식에서 필드를 채웁니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

DLP 인시던트 양식에 대한 일정

필드	설명
지속적 인시던트 수집	인스턴스가 새 인시던트에 대해 Microsoft에서 가져오는 진행 중인 인시던트 수집 ServiceNow AI Platform 입니다. DLP IR 트리거된 인시던트가 발견되고 인시던트 생성 필터링 기준이 일치하면 인시던트가 생성됩니다.
폴링 증분(분)	Microsoft의 폴링 빈도입니다. 이 필드는 300분으로 자동 설정됩니다.
초기 인시던트 수집 시간 설정	초기 수집에 대한 날짜 및 시간을 정의하는 옵션입니다. 후속 수집은 폴링 간격 기간을 기반으로 합니다. 이 옵션은 진행 중인 인시던트 수집 필드를 선택한 경우에만 표시됩니다.
초기 인시던트 수집 시간 입력	인시던트 수집을 위해 지정하는 날짜 및 시간입니다. ○ 값이 설정되면 Microsoft에서 검색하는 데이터는 추가된 미래 날짜부터 시작됩니다. ○ 이 필드는 초기 수집 시간 설정을 선택한 경우에만 표시됩니다.
초기 인시던트 수집 시간	데이터를 처음으로 수집합니다. 초기 인시던트 수집 시간이 설정되면 값이 표시되기 시작하는 것을 확인할 수 있습니다.
다음 인시던트 수집 시간(예상)	예상되는 인시던트 수집의 다음 기간입니다.
일회성 검색	일회성 기록 데이터 끌어오기를 활성화하는 옵션입니다. 이 필드를 선택하면 날짜 이후 필드에 추가된 날짜에 따라 Microsoft DLP IR 에서 기록 데이터를 끌어옵니다.
날짜 이후	Microsoft에서 데이터를 검색해야 하는 시작 날짜입니다. 이 필드는 최대 7일로 설정할 수 있습니다.

3. 팝업 창에서 마침 을 클릭하여 생성된 프로파일 구성을 저장합니다.

4. 프로파일을 활성화합니다.

a. 생성된 프로파일을 엽니다.

b. 활성 옵션을 활성화합니다.

c. 업데이트를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

결과
프로파일을 성공적으로 만들고 활성화한 후에는 프로파일에 설정된 구성에 따라 인시던트가 주기적으로 검색되어 DLP 인시던트 테이블에 추가됩니다.

Microsoft DLP IR 통합 설정 구성

Microsoft DLP IR 통합 기본 시스템 속성을 수정합니다.

시작하기 전에
필요한 역할: sn_dlir.admin

프로시저

1. 다음으로 이동 **Microsoft DLP** 통합 〉 설정.
2. 필요에 따라 다음 속성을 수정합니다.

Microsoft DLP 통합 설정

필드	설명
HTTP 호출의 최대 시간 제한 (sn_pp_dlp.maximum_http_time_out)	HTTP 호출의 최대 시간 제한(초)입니다. ○ 유형: 정수 ○ 기본값: 30
통합으로 작성된 로그 보고 수준 (sn_pp_dlp.logging.verbosity)	통합에 의해 생성된 보고 로그의 수준으로, 정보 유형의 이름을 의미합니다. 값을 다음 옵션으로 업데이트할 수도 있습니다. ○ 오류 ○ 경고 ○ 정보 ○ **debug** ○ 끄기 기본적으로 이 값은 정보입니다.
통합에서 작성된 로그 보고 대상 (sn_pp_dlp.logging.destination)	통합으로 생성되는 로그의 대상입니다. 값을 다음 옵션으로 업데이트할 수도 있습니다. ○ **db** ○ **file** ○ 없음 기본적으로 이 값은 **db**입니다.

3. 저장을 클릭합니다.

결과
수정된 통합 설정은 프로파일에 정의된 대로 다음 폴링 간격에 적용됩니다.

격리에서 릴리스 이메일 요청

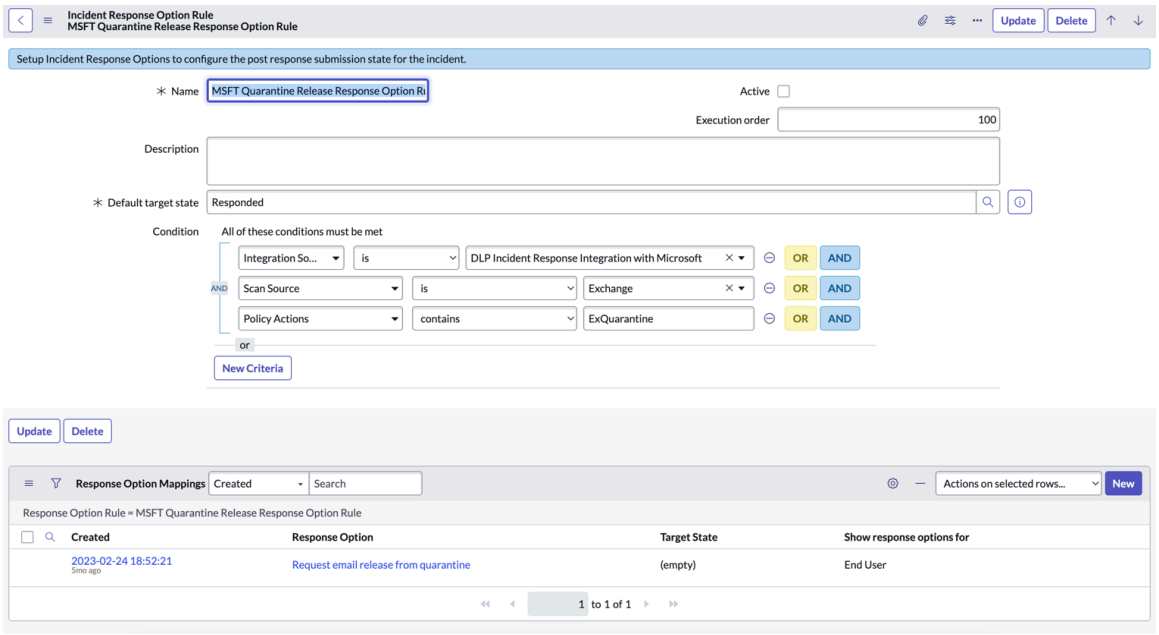
이 기능을 사용하여 Microsoft Purview 규정 준수 포털 격리된 전자 메일을 릴리스합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

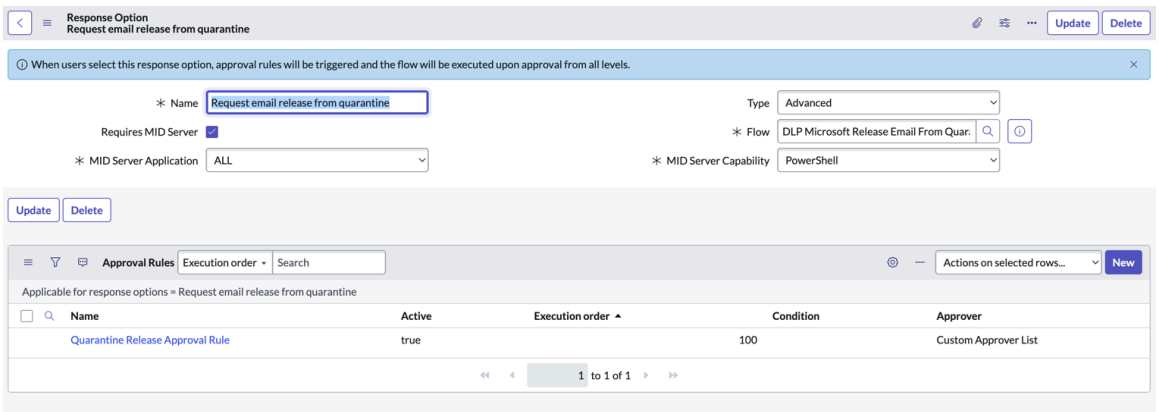
시작하기 전에

기본적으로 기본 시스템은 격리에서 이메일을 릴리스하는 격리 응답 에서 이메일 릴리스 요청 옵션 및 **MSFT** 격리 릴리스 응답 옵션 규칙을 제공합니다. 이 기본 기록에는 이 작업에 대한 승인 기능을 활용하도록 구성된 격리 릴리스 승인 규칙 도 있습니다. 자세한 내용은 인시던트 응답 옵션 규칙 생성, DLP 인시던트에 대한 응답 옵션 구성, 승인 규칙 생성 문서를 참조하십시오.

MSFT 격리 릴리스 응답 옵션 규칙



기본 **MSFT** 응답 옵션



전제 조건:

1. MID 서버에 Exchange Online PowerShell 모듈을 설치해야 합니다. 자세한 내용은 Exchange Online PowerShell 설치 및 유지 관리를 참조하세요.
2. MID 서버는 클라우드 서비스이기도 한 Exchange 서버와 통신해야 합니다. 따라서 MID 서버에는 지속적인 인터넷 액세스가 필요합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:
이 응답 옵션을 사용하는 경우 PowerShell 기능을 사용하여 MID 서버가 실행 중인지 확인하십시오. MID 서버가 실행 중이 아니고 PowerShell 기능이 없는 경우 최종 사용자는 DLP 사용자 작업 공간에서 격리 작업에서 이메일 릴리스 요청을 선택할 수 없습니다. 자세한 내용은 인시던트 응답 옵션 규칙 생성 및 DLP 인시던트에 대한 응답 옵션 구성 문서를 참조하십시오.

- 목록에서 특정 MID 서버를 원하는 경우 MID 앱을 구성하여 목록에 표시해야 하며, 구성된 MID 서버가 선택한 MID 애플리케이션에서 실행 중이어야 하며 전원 셸 기능이 있어야 합니다.
- 격리에서 해제 옵션을 사용하려면 API 권한이 필요합니다. Microsoft API 권한 페이지에서 다음을 확인합니다. **Office 365 Exchange Online** 〉 **Exchange.ManageAsApp** 이(가) 나열되며 다음 값을 포함합니다.
  - ▪ 유형: 응용 프로그램.
  - ▪ 관리자 동의 필요: 예.
  - ▪ 상태: 현재 잘못된 값은 **Office 365 Exchange Online** > **Exchange.ManageAsApp** 항목에 대한 〈조직〉에 부여되지 않으며 상태 값을 변경합니다. API 권한에 대한 자세한 단계는 Microsoft 설명서 사이트에서 애플리케이션에 API 권한 할당을 참조하십시오.

    주:
    이 단계는 서비스 주체를 사용하여 Exchange Online에 연결하는 데 필요합니다.

- 또한 서비스 주체에서 보안 관리자 역할이 필요합니다.
  - Microsoft Azure 포털에서 **Microsoft Entra ID** 역할 및 관리자를 검색하고, 등록된 앱(서비스 주체)에 할당을 추가한 다음, 역할을 할당 하는 방법에 대한 Microsoft 설명서에 설명된 절차를 따릅니다.
- 이 옵션은 인시던트 양식 뷰에 **ExQuarantine**으로 정책 작업 옵션이 있는 Microsoft Exchange 인시던트에만 적용할 수 있습니다.

필요한 역할: 최종 사용자

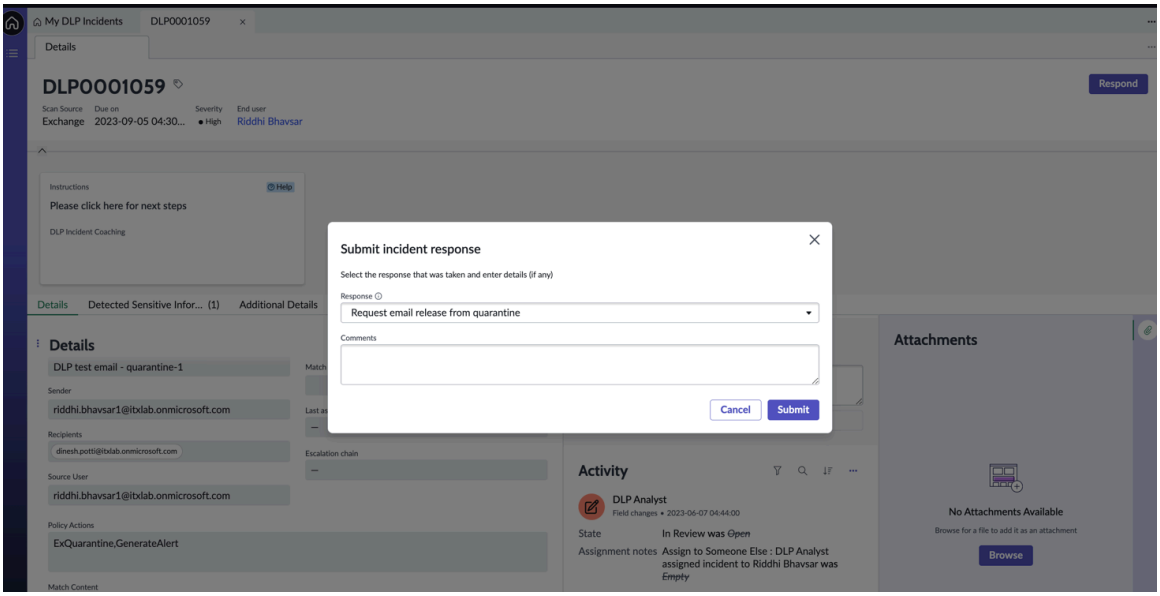
다음 절차에서는 DLP 사용자 작업 영역에서 이 작업을 제출하는 방법에 대해 설명합니다.

프로시저

1. 다음으로 이동 **DLP** 〉 **DLP** 사용자 작업 공간.
2. Microsoft Exchange DLP 인시던트를 엽니다.
   인시던트 정책 작업이 ExQuarantine으로 설정되어 있는지 확인합니다.
3. 응답을 클릭합니다.
4. 응답 드롭다운 목록에서 격리에서 메일 릴리스 요청 옵션을 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

인시던트 응답 제출 - 격리 옵션에서 이메일 릴리스 요청



5. 제출을 클릭합니다.

> **주:**
> 이 작업에 대해 승인 규칙이 구성되면 승인 플로우가 먼저 트리거되고 모든 승인을 받은 후 격리에서 이메일 릴리스 요청 플로우가 트리거되고 이메일이 격리에서 해제됩니다. DLP 인시던트의 상태는 성공적인 릴리스 후 격리에서 해제 됨으로 업데이트됩니다.

Exchange Online, OneDrive 및 **SharePoint** 유형의 **DLP** 인시던트에 대한 파일 다운로드

Microsoft Purview에서 DLP 정책을 위반하는 파일 또는 전자 메일을 다운로드합니다. 인시던트 뷰에서 DLP IR 이 파일 또는 이메일을 로컬 머신에 다운로드합니다. 스캔 소스 Exchange Online, OneDrive 및 SharePoint 유형의 인시던트에 대한 DLP IR 파일을 다운로드할 수 있습니다.

시작하기 전에
필요한 역할:

- sn_dlir.admin, sn_dlir.analyst
- 모든 유효한 승인자

프로시저

1. 다음으로 이동 모두 〉 **DLP** 인시던트 관리 〉 **DLP** 분석가 작업 공간.

2. Microsoft 소스에서 수집된 스캔 소스 Exchange Online, OneDrive 또는 SharePoint 유형의 DLP 인시던트 기록을 엽니다.

3. 파일 다운로드를 클릭합니다.
Microsoft Purview 쪽의 DLP 정책을 위반한 파일 또는 전자 메일이 사용자의 로컬 머신에 다운로드됩니다.

> **주:**
> DLP 관리자는 고급 설정 페이지에서 보고된 인시던트의 위반 파일 다운로드가 허용되어야 함 설정을 사용하지 않도록 설정하여 파일 다운로드 작업의 액세스를 제어할 수 있습니다. 자세한 내용은 고급 설정 구성 문서를 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Exchange Online, OneDrive 및 **SharePoint** 유형의 **DLP** 인시던트에 대한 증거 파일 미리 보기

DLP IR 분석가 작업 공간에서 증거 파일을 미리 봅니다 Data Loss Prevention Incident Response .

시작하기 전에

중요사항:
DLP 분석가 작업 공간에서 증거 파일 작업을 사용하는 동안 증거 파일은 임시로 암호화되지 않은 형식으로 ServiceNow 데이터베이스에 저장됩니다. 증거 파일을 저장하지 않으려면 증거 파일 미리 보기 기능을 사용하지 않도록 설정합니다. 자세한 내용은 고급 설정 구성 문서를 참조하십시오.

필요한 역할: sn_dlir.analyst

프로시저

1. 다음으로 이동 모두 〉 **DLP** 인시던트 관리 〉 **DLP** 분석가 작업 공간.
2. DLP 인시던트 기록을 엽니다.
3. 상황별 사이드바에서 증거 파일 아이콘( )을 선택합니다.
4. 증거 파일 탭에서 증거 파일 카드를 선택하여 문서 뷰어에서 증거 파일을 미리 봅니다.

   미리 보기 기능은 다음 표에 나와 있는 것처럼 파일 형식마다 다릅니다.

파일 형식	파일 확장명
이미지	.bmp, .gif, .ico, .jpeg, .jpg, .png, .svg 및 .webp. 이미지 파일은 문서 뷰어 모드에서 열립니다.
Microsoft Office 파일	.doc, .docx, .ppt, .pptx, .xls, .xlsx Office 파일이 문서 뷰어 모드에서 열립니다.
텍스트 파일	.txt 텍스트 파일은 텍스트 편집기 모드에서 열립니다.
메일 파일	.eml **주:** 파일 크기는 5MB 미만이어야 합니다. 콘텐츠를 미리 보려면 먼저 파일을 다운로드해야 합니다.
PDF 파일	.pdf

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

파일 형식	파일 확장명
	○ 키워드를 입력하여 문서를 검색합니다. ○ 확대 및 축소 기능으로 보기를 조정하여 가독성을 높입니다. ○ 페이지를 시계 방향 또는 시계 반대 방향으로 회전하면 내용을 더 선명하게 볼 수 있습니다.

주:

이진 파일은 렌더링되지 않으며 콘텐츠를 미리 보려면 다운로드해야 합니다. 증거 파일 미리 보기 기능은 보관된 인시던트에도 사용할 수 있습니다.

DLP 통합의 Microsoft 도메인 분리

도메인 분리를 사용하여 데이터, 프로세스 및 관리 작업을 도메인이라는 논리적 그룹으로 분할할 수 있습니다. 그런 다음 사용자가 데이터를 보고 액세스할 수 있는 것을 포함하여 이러한 분리의 여러 가지 측면을 제어할 수 있습니다.

지원 수준

지원: 기본.

DLP 통합에서 도메인 분리가 Microsoft 작동하는 방식

도메인 분리를 수행하려면 다음 단계를 따르십시오.

- 해당 도메인에서 필요한 역할을 가진 사용자를 생성합니다.
- Microsoft 해당 도메인에서 DLP 통합 절차를 수행합니다.

보안 운영 공통 기능

메인 보안 운영 애플리케이션(보안 인시던트 응답, 취약성 대응, 위협 인텔리전스또는 구성 준수)의 플러그인이 활성화될 때마다 플러그인이 Security Support Common 활성화됩니다. 이 플러그인은 모든 보안 운영 애플리케이션에서 공통적인 기능을 제공하는 다양한 모듈을 로드합니다.

주:
〔sn_sec_cmn.admin〕 역할을 가진 사용자만 모듈을 보고 사용할 보안 운영 수 있습니다. 이 역할은 애플리케이션에서 관리 역할이 보안 운영 할당될 때 상속됩니다.

보안 운영 모듈

기능	설명
Security Operations Integrations 참조, 위협 인텔리전스 통합, 취약성 대응 통합	애플리케이션(보안 인시던트 응답, 위협 인텔리전스, 및 취약성 대응)에는 여러 통합이 보안 운영 포함되어 있습니다. 이 섹션에서는 플러그인을 활성화하고 타사 통합을 구성 ServiceNow 하기 위한 지침을 제공합니다. 또한 자체 통합을 개발하기 위한 몇 가지 기본 지침과 기본 시스템에 포함된 특정 통합에 대한 세부 정보가 포함되어 있습니다.
보안 운영 이메일 처리	를 사용하여 이메일 처리외부 탐지 시스템의 정보 통합을 설정하고, 보안 운영 기록 처리 시 세밀성을

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

기능	설명
	제공하고, 일치하지 않는 이메일을 처리하고, 기록의 중복을 방지할 수 있습니다.
그룹	• 필터 그룹 필터 그룹을 생성하고 사용하여 인스턴스의 테이블에서 기록을 찾습니다. 예를 들어 동일한 제조업체별로 모든 컴퓨터 그룹을 만들 수 있습니다. 유사한 취약성이 있거나 특정 서브넷 IP 주소 범위에 속하는 구성 항목(CI)을 필터링할 수도 있습니다. • 에스컬레이션 주의 또는 전문 지식이 더 필요한 문제의 보안 인시던트에 대해 에스컬레이션 경로를 작성할 수 있습니다. 에스컬레이션 그룹이 있으면 해당 그룹의 모든 보안 인시던트에 버튼이 나타납니다.
보안 태그	태그: 보안 태그 규칙은 보안 태그 액세스에 대한 필터링을 제공합니다.
워크플로우	• 보안 워크플로우 보기 보안 운영 애플리케이션에 포함된 여러 워크플로우를 볼 수 있습니다. 워크플로우는 템플릿과 워크플로우 편집기에서 생성할 수 있습니다. • 워크플로우 트리거 보안 운영 워크플로우 트리거는 테이블에 조건을 포함합니다. 조건이 충족되면 워크플로우 트리거 기록에 첨부된 모든 워크플로우가 실행됩니다.
유틸리티	• 보강 데이터 매핑 보강 데이터 매핑 데이터를 XML, JSON 또는 속성 파일에서 기록으로 ServiceNow 변환합니다. 보안 운영 워크플로우는 향상된 데이터 맵을 사용하고 보안 인시던트에 출력 데이터를 제공합니다. • 필드 값 변환 고유한 고객 필드 값을 필드 맵을 사용하여 이메일 구문 분석, 데이터 강화 또는 테이블에서 인식하는 보안 운영 필드 값으로 변환합니다. 선택 필드, 참조를 지원하고 외부 데이터를 새 기록의 표준 용어 및 형식으로 정렬합니다. • 필드 매핑

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

기능	설명
	보안 운영 테이블은 다른 테이블과 매핑되어 보안 인시던트를 고객 서비스 케이스에 연결하거나 문제를 시스템의 다른 부분에 보안 운영 연결할 수 있습니다. 예를 들어, 플러그인을 작업에 통합할 수 있습니다 보안 인시던트 응답 . • 요청 시 오케스트레이션 분석 중에 보안 인시던트 응답 보안 분석가는 보안 인시던트 워크플로우에 기반한 작업을 수행하기를 원할 수 있습니다. 예를 들어, 특정 CI에서 프로세스 덤프를 실행합니다. 이는 주문형 오케스트레이션을 통해 수행할 수 있습니다. • 운영 체제 그룹 해당 사항 없음 • **SecOps** 애플리케이션 레지스트리 해당 사항 없음
CMDB	**CI** 식별자 규칙: CI 식별자는 타사 통합에서 일치하는 정보를 포함하는 CMDB의 CI(구성 항목)를 조회하는 데 사용되는 규칙입니다. 이러한 규칙은 일치하는 데이터를 포함하는 필드와 이러한 필드를 평가하는 우선순위를 정의합니다. 가장 낮은 순서 값이 먼저 평가됩니다.

Security Operations에서 필터 그룹 생성 및 정의

필터 그룹을 생성하고 사용하여 인스턴스의 테이블에서 기록을 찾습니다. 예를 들어 동일한 제조업체별로 모든 컴퓨터 그룹을 만들 수 있습니다. 유사한 취약성이 있거나 특정 서브넷 IP 주소 범위에 속하는 구성 항목(CI)을 필터링할 수도 있습니다.

시작하기 전에
필요한 역할: sn_sec_cmn.write

이 태스크 정보
필터 그룹에는 동적으로 업데이트되는 기록, 조건을 사용하여 필터링되지 않는 일련의 정적 기록 또는 동적으로 업데이트된 기록과 정적 기록의 조합이 포함될 수 있습니다. CI 제외 항목과 같은 일부 필터 그룹은 기본 시스템에 포함됩니다.

프로시저

1. 다음으로 이동 모두 〉 보안 운영 〉 그룹 〉 필터 그룹.

2. 새로 만들기를 클릭합니다.

3. 양식의 필드에 적절히 입력합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
이름	필터 그룹의 이름입니다.
활성	그룹을 활성화하는 상자입니다.
설명	필터 그룹에 대한 설명입니다.
네트워크 IP 주소	그룹에 추가할 CI의 IP 주소가 들어 있는 네트워크 IP 주소입니다. 이 필드는 구성 항목 [cmdb_ci] 또는 테이블 필드에서 구성 항목을 확장하는 테이블을 선택한 경우에만 나타납니다.
서브넷 마스크	그룹에 추가할 CI의 IP 주소를 포함하는 서브넷(예: 255.255.255.0)입니다. 이 필드는 구성 항목 [cmdb_ci] 또는 테이블 필드에서 구성 항목을 확장하는 테이블을 선택한 경우에만 나타납니다.
테이블	필터링할 테이블입니다.
조건	조건 작성기 를 사용하여 필터링할 기준을 정의합니다.

4. 양식 헤더를 마우스 오른쪽 버튼으로 클릭하고 저장을 선택합니다.
고급 조건 탭이 나타납니다.

   테이블 필드에서 지정한 테이블 유형에 따라 다음과 같이 더 많은 탭이 나타납니다.

테이블	표시된 탭
구성 항목 [cmdb_ci] 또는 구성 항목 테이블을 확장하는 테이블	수동으로 추가된 **CI** 및 일치하는 **CI**
작업 [task] 또는 작업 테이블을 확장하는 테이블	수동으로 추가된 작업 및 일치하는 작업
CI 또는 작업과 관련이 없는 테이블	수동으로 추가된 기록

5. 필터 그룹에 대한 추가 조건을 정의하는 방법:

   a. 고급 조건을 클릭합니다.

   b. 추가 필터 그룹 조건 포함된 목록에 새 행을 삽입하여 업데이트할 필터 그룹과 결합할 다른 미리 작성된 필터 그룹을 선택합니다.
   선택한 필터 그룹이 참조 필드를 기반으로 기록을 필터링하도록 하려면 현재 기록이 저장될 때 매핑된 필드가 자동으로 선택됩니다.

   > 주:
   > 매핑된 필드 값은 추가 필터 그룹 조건 포함된 목록에서 편집할 수 없습니다. 필드를 변경하려면 정보 아이콘 클릭하여 기록을 엽니다.

   c. 업데이트를 클릭합니다.

6. 필터 그룹에 CI 또는 작업을 수동으로 더 추가하려면 다음과 같이 하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 수동으로 추가된 **CI** 또는 수동으로 추가된 작업 탭을 클릭합니다.

b. 편집을 클릭합니다.

c. 추가할 CI 또는 작업을 선택합니다.

d. 저장을 클릭합니다.

7. 선택 기준과 일치하는 CI 또는 작업을 보려면 다음을 수행합니다.

a. 일치하는 **CI** 또는 일치하는 작업 탭을 클릭합니다.

b. 기준을 변경한 경우 양식 헤더를 마우스 오른쪽 버튼으로 클릭하고 목록 새로 고침을 선택하여 목록을 새로 고칩니다.

공유 데이터 변환

, 취약성 대응, 및 위협 인텔리전스 플러그인은 보안 인시던트 응답관계 데이터 및 중복 규칙에 대한 공통 기능을 공유하며, 외부 및 내부 정보를 로 임포트하는 보안 운영데 사용됩니다.

이메일 구문 분석, 중복 규칙및 필드 매핑 입력 데이터(이메일, JSON 또는 XML 파일 또는 기록)를 가져와 올바른 형식으로 변환하여 새 기록을 생성합니다. 이러한 각 기능은 고유한 방식으로 데이터를 가져오지만 동일한 여러 프로세스를 사용하여 새 기록으로 변환됩니다.

관계 데이터

관련 목록(예: 보안 인시던트의 연결된 옵저버블)에 정보를 추가하면 m2m 테이블로 구성된 관계 기록을 생성할 수 있습니다. 경우에 따라 해당 관계 기록에 설정할 추가 데이터가 있습니다. 예를 들어 옵저버블은 소스 IP(대상 IP와 반대)입니다. 해당 정보는 이메일 구문 분석 또는 필드 매핑 양식의 필드 매핑 필드 관련 목록에서 사용하는 필드 변환 양식의 관계 데이터 필드에 있습니다.

관계 데이터 필드는 일반적으로 비어 있습니다. 이메일 구문 분석에서 옵저버블의 IP 주소에 가장 일반적으로 사용됩니다.

필드 매핑 기능의 필드 매핑 필드를 사용하여 모든 ServiceNow 기록의 데이터를 다른 ServiceNow 기록으로 변환할 수 있습니다. 예를 들어 인시던트에서 보안 인시던트로 또는 보안 인시던트에서 PRB로 데이터를 변환할 수 있습니다.

보안 운영 중복 규칙

보안, 취약성, IoC 등에 대한 중복 기록을 처리하는 데 사용합니다 중복 규칙 .

중복 규칙에는 두 가지 목적이 있습니다. 너무 많은 중복 기록이 생성되는 것을 방지하고 중복이 감지되면 업데이트할 기록의 필드를 지정합니다. 활성 중복 항목만 검색됩니다. 기록이 활성화되어 있지 않으면(예: 인시던트가 종결되면 동일한 새 문제가 새 인시던트가 됩니다.)

중복 규칙은 이메일 구문 분석, 필드 매핑 및 보강 데이터 매핑에 사용됩니다.

관련 정보

보안 운영에서 이메일 파서 생성

보안 운영 필드 매핑을 사용하여 테이블을 테이블에 매핑

에서 중복 규칙 생성 보안 운영

를 사용하여 활성 중복 기록이 있는 새 이메일, 보강 데이터 또는 필드 맵을 식별하고 적절하게 처리할 수 있습니다 중복 규칙 .

시작하기 전에
필요한 역할: sn_sec_cmn.write

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 보안 운영 〉 중복 규칙.
2. 새로 만들기를 클릭합니다.
3. 양식의 필드에 적절한 정보를 입력합니다.

중복 규칙

필드	설명
이름	중복 규칙의 이름입니다.
테이블	기록이 작성되고 중복을 결정하는 데 사용되는 테이블입니다.
식별 필드	중복 보안 인시던트, 옵저버블, 취약성 등을 나타내는 필드 집합을 이러한 필드의 값이 동일한 경우 선택합니다.
중복 동작	중복 이메일을 처리하는 방법을 관리합니다. 선택 항목은 다음과 같습니다. 하위로 생성 기록을 원본의 하위 항목으로 생성합니다. 하위를 상위에 연결하는 필드는 상위필드입니다. 기록 생성 및 업데이트 금지 (기본값) 아무 작업도 수행하지 않습니다. 중복 항목은 무시합니다. 중복 기록 업데이트 중복 동작에 지정된 대로 기존 기록의 필드를 업데이트합니다. 주: 중복 기록 업데이트를 선택하면 중복 작업 관련 목록이 나타납니다.
활성	규칙을 활성화하려면 이 확인란을 선택합니다.
설명	이 중복 규칙의 목적과 적용에 대해 설명합니다. 예를 들어 IP 기반 옵저버블 또는 방화벽의 보안 인시던트를 위해 설계된 규칙과 같이 사용해야 하는 경우입니다.

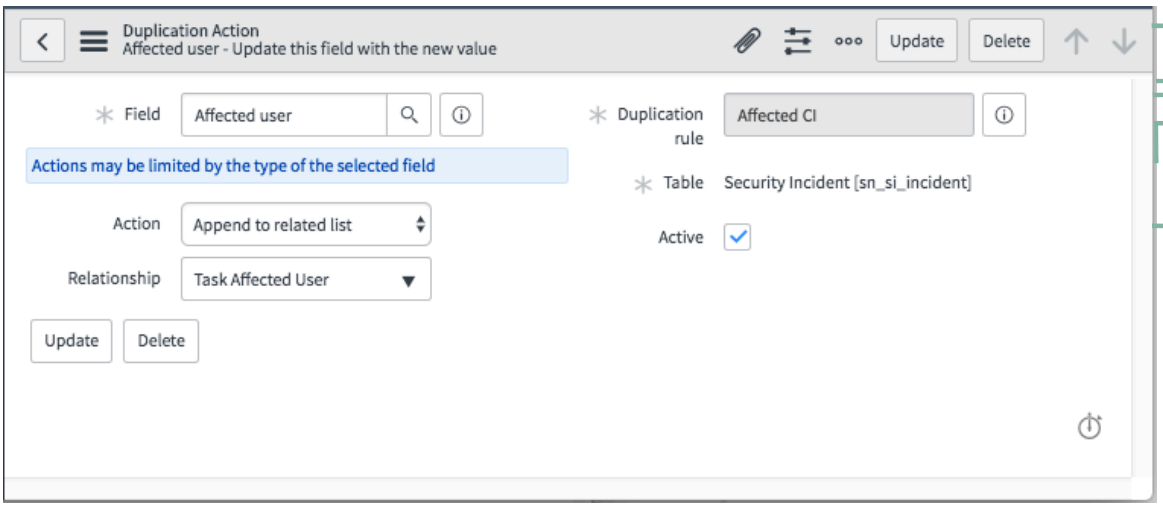
4. 기록 헤더를 마우스 오른쪽 버튼으로 클릭하고 저장을 선택하거나 업데이트를 클릭합니다.
5. 중복 작업을 설정하려면 중복 기록 업데이트를 선택한 경우 새로 만들기를 클릭하여 인시던트에서 업데이트하려는 각 필드에 대해 중복 작업을 생성합니다.
6. 양식의 필드를 입력하거나 편집하여 필드를 업데이트하는 방법을 설명합니다.

중복 동작

필드	설명
필드	중복 작업에 사용할 필드의 이름입니다.
작업	지원되는 작업은 필드 유형에 따라 다릅니다. 선택 항목은 다음과 같습니다. 새로운 값으로 이 필드를 업데이트 기존 기록의 이전 값을 이 값으로 바꿉니다. 새로운 값을 콤마 분리 목록에 추가(하나뿐인 경우) 값을 쉼표로 구분된 목록의 항목으로 처리하고 새 데이터(있는 경우)를 해당 목록의 새 항목으로 추가합니다. 데이터가 이미 목록에 있으면 두 번 추가되지 않습니다.

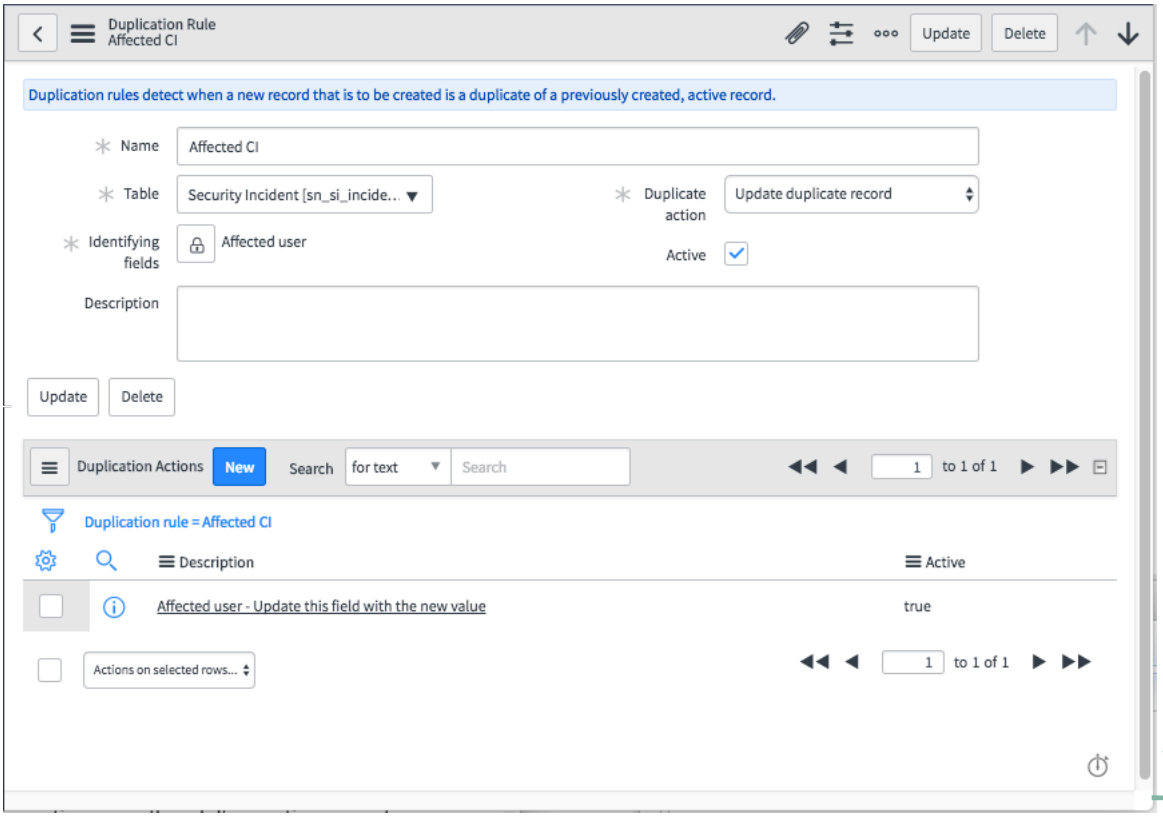
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	새로운 값을 이 필드에 추가 필드의 기존 텍스트 끝에 새 값을 추가합니다. 1을 카운터 필드에 추가 숫자 필드에 1을 더합니다. 필드를 오늘로 설정 필드를 현재 날짜 및 시간으로 설정합니다. 관련 목록에 추가 이 값이 있는 관련 기록을 현재 기록의 관련 목록에 추가합니다. 업데이트 중인 테이블에 연결된 동일한 형식의 열이 있는 다대다 테이블이 있을 때 나타납니다. 예를 들어 영향을 받는 **CI** 또는 영향을 받는 사용자입니다.
관계	〔선택사항〕 이 필드는 관련 목록에 추가 작업을 선택한 경우에만 나타납니다. 이 규칙과 연결할 관련 목록의 이름입니다.
중복 규칙	이 작업이 속한 규칙입니다.
테이블	기록이 생성되는 테이블입니다. 정보 전용으로 표시됩니다.
활성	작업을 활성화하려면 이 확인란을 선택합니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

7. 제출을 클릭합니다.



보안 운영 이메일 처리

를 사용하여 이메일 처리외부 탐지 시스템의 정보 통합을 설정하고, 보안 운영 기록 처리 시 세밀성을 제공하고, 일치하지 않는 이메일을 처리하고, 기록의 중복을 방지할 수 있습니다.

이메일 처리 는 다음 기능으로 구성됩니다.

기능	설명
이메일 구문 분석	외부 시스템 이메일에서 새 보안 운영 기록을 생성합니다.
중복 규칙	알려진 인시던트가 있는 새 이메일을 식별하고 적절하게 처리합니다.
속성	보안, 취약성 및 IoC에 대한 입력 이메일 구문 분석 으로 사용되는 계정을 지정합니다. 처리 보안 운영 기록의 세분성을 제공합니다.
일치하지 않는 이메일	기록과 보안 운영 일치하지 않는 이메일을 나열합니다.

보안 운영 이메일 속성

이메일 속성 은 외부 탐지 시스템에서 정보를 임포트하여 보안, 취약성 및 IoC에 대한 기록을 생성하기 위해 입력 이메일 구문 분석 으로 사용되는 받은 편지함을 지정합니다. 모든 외부 탐지 시스템에서 사용할 일반 계정을 설정하거나 , 위협 인텔리전스, 또는 에 대한 보안 인시던트 응답개별 이메일 계정을 설정할 수 있습니다취약성 대응.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이메일 속성 만들기 보안 운영

보고서에 대한 이메일 주소를 지정하고 이메일을 사용하여 자동 이메일 동작을 제어할 수 있습니다 속성.

시작하기 전에

필요한 역할: sn_sec_cmn.admin
이메일 구문 분석 받은 편지함으로 이메일을 보내도록 외부 탐지 도구를 설정합니다.

프로시저

1. 다음으로 이동 모두 〉 보안 운영 〉 이메일 처리 〉 속성.
2. 수신자 사서함을 적절하게 입력합니다.
   인바운드 작업이 아닌 이메일 구문 분석으로 처리되는 인바운드 이메일 주소입니다.

이메일 구문 분석 속성

필드	설명
도구용 보안 운영 받은 편지함	의 보안 운영전체 이메일 주소입니다. 예를 들어 secops_support@yourcompany.com.
보안 인시던트 도구용 받은 편지함	의 보안 인시던트 응답전체 이메일 주소입니다. 예: sir_support@your.company.com.
도구용 취약성 대응 받은 편지함	의 취약성 대응전체 이메일 주소입니다. 예: vuln_resp@yourcompany.com.
도구용 위협 인텔리전스 받은 편지함	의 위협 인텔리전스전체 이메일 주소입니다. 예를 들어 threat_intel@yourcompany.com.

3. 저장을 클릭합니다.

보안 운영 이메일 구문 분석

를 사용하여 이메일 구문 분석외부 탐지 시스템에서 새 보안 운영 기록 생성 . 이 기능은 맬웨어 탐지, 취약성 탐지, 방화벽, 위협 인텔리전스 등과 같은 외부 도구의 정보를 통합하는 방법을 제공합니다.

이메일 구문 분석 방법

이메일을 보낼 수 있는 모든 시스템은 보안 인시던트, 요청, 취약한 항목, 취약성, 보안 인시던트 옵저버블, 공격 방법 등과 같은 기록을 생성할 보안 운영 수 있습니다.

모든 보안 운영 플러그인(보안 인시던트 응답, 위협 인텔리전스및 취약성 대응)에는 이메일 구문 분석기로 구문 분석하기 위해 외부 통합에서 이메일을 보내야 하는 이메일 주소를 정의하는 속성 (**email_to**)이 있습니다. 참조 이메일 처리 〉 속성 자세한 내용은.

이메일 보안 운영 주소로 전송된 이메일은 이메일 이벤트 테이블에 저장됩니다. 이러한 이메일은 모든 이메일 파서와 일치하는지 확인하기 위해 처리됩니다.

일치하는 이메일에는 플래그가 지정되고 변환 및 중복 규칙이 기록을 생성하거나 업데이트합니다 보안 운영 . 이메일은 해당 기록에 연결되고 #### 것으로 플래그가 지정됩니다.

일치하지 않는 이메일은 기록으로 보안 운영 나열됩니다일치하지 않는 이메일. 이러한 이메일을 처리하기 위한 이메일 파서를 빌드하는 데 도움이 되도록 검토할 수 있습니다. 다시 처리 작업을 사용하면 파서를 통해 일치하지 않는 이메일을 다시 실행할 수 있습니다. 원본 이메일 로그가 해당 기록에 연결됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이메일 변환의 중복 규칙은 동일한 문제와 관련된 여러 이메일을 관리합니다. 이러한 규칙은 중복 기록의 원인을 정의하고 중복 기록이 생성되는 것을 방지할 수 있습니다. 중복이 감지되면 규칙은 수행할 작업을 지정합니다(작업 없음(새 기록을 생성하지 않음), 새 기록을 기존 기록의 하위 기록으로 생성, 기존 기록 업데이트 중복 규칙을 업데이트할 때 업데이트할 기존 기록의 필드를 지정합니다.

주:
보안 운영 이메일 파서는 플랫폼 인바운드 작업과 함께 작동하며 이를 대체하지 않습니다. **sys_journal_field** 항목과 같은 간접 필드에 대한 값 설정은 지원하지 않습니다.

기본적으로 이메일 이벤트는 30일 후에 삭제됩니다.

여러 기록

외부 탐지 시스템(맬웨어 탐지기, 취약성 등)은 한 번에 여러 항목에 대해 보고하는 이메일을 보낼 수 있습니다. 이메일 파서는 이메일 내의 구분 기호를 지원합니다.

예를 들어, 멀웨어 탐지기는 특정 멀웨어에 감염된 네트워크 내의 모든 시스템에 대한 이메일 보고서를 먼저 멀웨어에 대한 정보와 함께 보낸 다음 영향을 받는 시스템 목록을 보낼 수 있습니다.

샘플 악성 이메일

```
Subject: EvilChocolateBunny detected on multiple systems
Malware Hash: 20380285098260923490723
Malware Name: Evil Chocolate Bunny
Type: Keylogger
==========
System: WIN-GHARRISON
IP: 123.45.67.888
Status: File present, not infected
==========
System: WIN-ATUTER
IP: 123.45.67.889
Status: Infected
==========
System: WIN-BANGLIN
IP: 123.45.67.899
Status: File present, not infected
```

이 예에서 이메일 변환내에서 기록 구분 기호가 **==========**으로 설정되면 이메일이 별도로 평가되는 네 개의 섹션으로 분할됩니다. 이렇게 하면 영향을 받는 세 시스템 각각에 대해 보안 인시던트가 생성됩니다.

주:
헤더 섹션이 탐지되었지만 영향을 받는 시스템이 없으므로 세 기록 모두에 사용되며 네 번째 기록은 생성되지 않습니다.

필드 변환은 각 섹션에서 데이터를 끌어옵니다. 이메일의 머리글 또는 바닥글에 있는 내용이 이 예제의 맬웨어 해시, 맬웨어 이름 및 유형과 같은 모든 기록에 적용되는 경우 필드 변환은 값 검색을이메일 본문 내에서 이메일 본문의 줄 시작 또는 이메일 본문의 아무 곳이나 검색하는 값으로 설정해야 합니다.

필드변환은 시스템, IP 주소 또는 상태와 같이 각 섹션 내에 정의된 데이터를 기록 섹션 또는 초내의 줄 시작 부분에 검색하도록 설정되어야 합니다. 기록 섹션 옵션은 이메일 변환 내에 정의된 기록 구분 기호가 있는 경우에만 사용할 수 있습니다.

구분 기호가 정의된 이메일을 구문 분석할 때 하나 이상의 섹션별 데이터가 있는 섹션에 대해서만 기록이 생성됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 예에서는 4개의 섹션이 정의되어 있더라도 3개의 기록이 생성됩니다. 첫 번째 섹션은 헤더이며 하나의 시스템에만 특정한 것이 없습니다. 첫 번째 섹션(시스템, IP 또는 상태) 내의 필드가 채워지면 해당 섹션에 대한 기록도 생성됩니다.

관련 정보

보안 운영에서 이메일 파서 생성

보안 운영 보강 데이터 매핑

보안 운영 필드 매핑

보안 운영에서 이메일 파서 생성

이메일 구문 분석 보안, 취약성 및 옵저버블에 대한 이메일에서 기록을 생성하여 보안 운영 위협 대응 및 정정을 신속하게 처리합니다.

시작하기 전에

- 중앙 이메일 주소로 이메일을 보내도록 외부 탐지 도구를 설정합니다.
- 보안 운영 속성에서 이메일 주소를 설정합니다. 자세한 내용은 이메일 속성 만들기 보안 운영 문서를 참조하십시오.
- 이 이메일 주소에 사용자 계정을 할당하고 해당 사용자에게 이메일 이벤트 기록을 만들고 업데이트할 수 있는 보안 접근 제어를 제공합니다.
- 외부 탐지 도구의 관련 이메일 사본을 앞에 두십시오.
- 생성할 기록 유형, 보안 인시던트, 취약성 기록, 작업 등을 결정합니다. 이 선택에 따라 선택한 테이블이 결정됩니다.

필요한 역할: sn_sec_cmn.admin

프로시저

1. 다음으로 이동 모두 〉 보안 운영 〉 이메일 구문 분석.
2. 새로 만들기를 클릭합니다.
3. 양식의 필드에 적절히 입력합니다.

> **주:**
> 두 개 이상의 필드가 지정된 경우 기록을 생성하려면 모든 필드가 이메일과 일치해야 합니다.

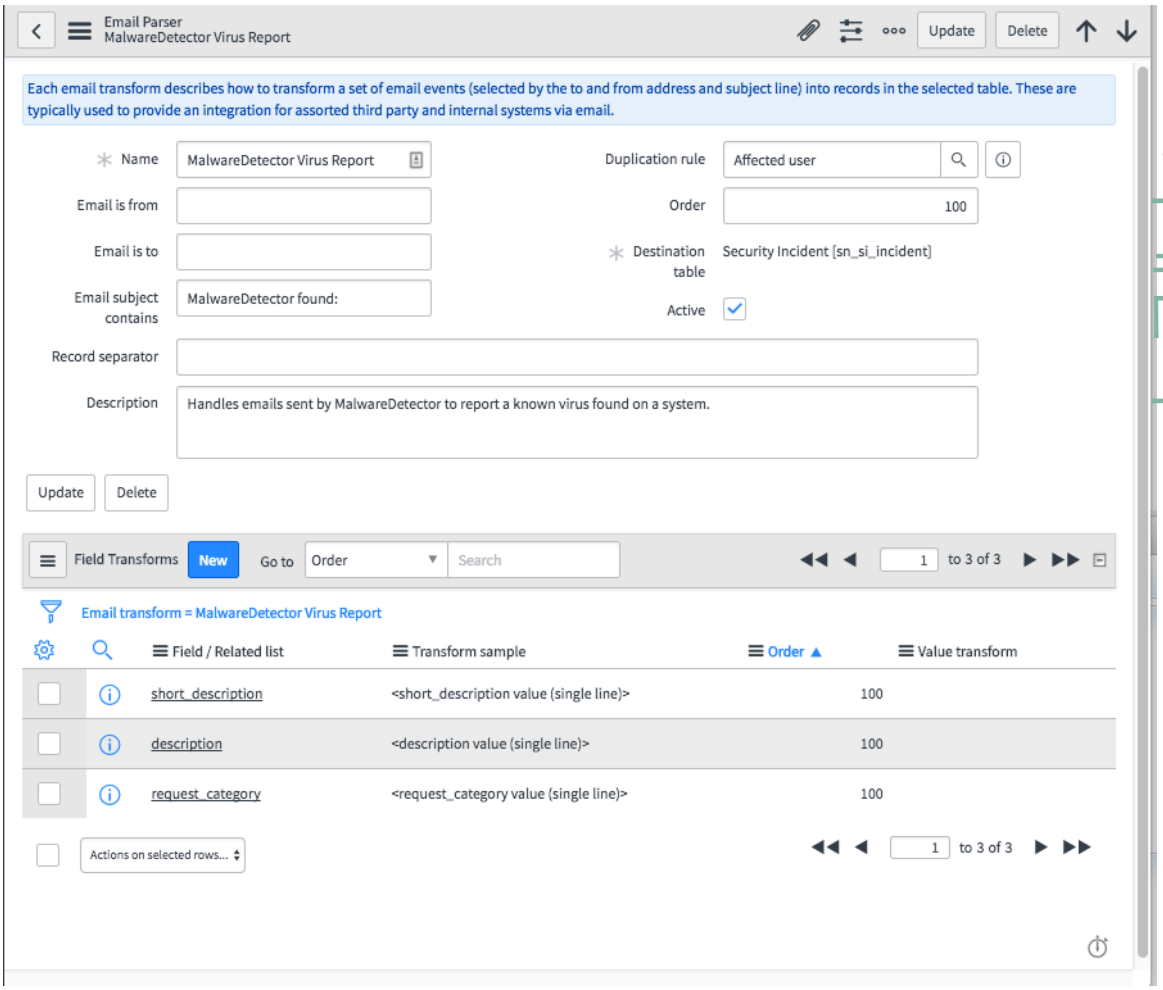
이메일 파서

필드	설명
이름	이메일 파서의 이름입니다.
이메일 송신	입력된 경우 이 주소의 이메일만 이 이메일 파서에 의해 변환됩니다.
이메일 수신	입력된 경우 이 주소의 이메일만 이 이메일 파서에 의해 변환됩니다.
이메일 제목에 포함	이 문구를 입력하면 제목에 이 문구가 포함된 이메일만 이 이메일 파서에 의해 변환됩니다.
중복 규칙	이 변환으로 처리되는 모든 이메일의 중복 이메일 처리 방법을 관리합니다. 자세한 내용은 공유 데이터 변환 문서를 참조하십시오.
순서	변환을 고려할 순서입니다. 첫 번째로 일치하는 이메일 변환이 사용됩니다. 일반적으로 낮은 숫자에 약간의 대체를 사용하여 가장 구체적인 이메일 파서를 설정하려고 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	다른 것이 일치하지 않으면 실행되도록 포괄적인 이메일 파서에 더 높은 순서 번호를 부여합니다. 기본값은 100입니다. 모든 항목이 일치하면 가장 구체적인 이메일 파서(보낸 사람, 받는 사람 및 제목과 일치)가 사용됩니다.
대상 테이블	기록을 생성하려는 테이블입니다.
활성	이 변환이 활성 상태인지, 사용 중인지, 비활성 상태인지 여부입니다. 이 옵션을 선택하지 않으면 이 코드로 이메일이 변환되지 않습니다.
기록 구분 기호	이 이메일 파서에서 처리하는 이메일이 여러 기록을 만들 때 이 필드에는 해당 기록에 대한 정보 사이의 구분 기호가 포함됩니다. 자세한 내용은 보안 운영 이메일 구문 분석 문서를 참조하십시오.
설명	이 이메일 파서에 대한 설명, 작동하는 도구, 목적 등입니다.

4. 입력을 완료했으면 양식 헤더를 마우스 오른쪽 버튼으로 클릭하고 저장을 선택합니다.
필드 변환 탭이 나타납니다. 이 탭은 대상 테이블 내의 개별 필드가 이메일 컨텐츠를 기반으로 설정되는 방식을 보여줍니다.



5. 필드 변환을 추가하려면 다음 단계를 수행합니다.

a. 필드 변환 탭에서 새로 만들기를 클릭합니다.

b. 양식의 필드에 적절히 입력합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵션	설명
필드	설명
필드 또는 관련 목록에 값 저장	값을 찾을 위치를 선택합니다. 선택 항목은 다음과 같습니다. ○ 새 기록의 필드에 값을 저장합니다. ○ 관련 목록에서 이 값에 연결 ○ 이 값에 연결, 일치하는 기록이 없는 경우 새 레코드 생성 주: 대상 테이블에 관련 목록이 없으면 이 필드가 표시되지 않습니다.
필드	이 값을 입력할 필드를 선택합니다. 주: 선택 필드의 경우 기본 선택 레이블 또는 값을 사용하여 기존 선택 사항과 일치시킵니다. 일치하는 항목이 없으면 필드가 설정되지만 새 항목이 선택 목록에 추가되지 않습니다. 자세한 내용은 다음을 참조하십시오. 선택 목록입니다. 참조 필드의 경우 기록의 표시 이름과 일치하는 값 또는 유효한 sys_id 있는 경우에만 항목이 설정됩니다. 자세한 내용은 다음을 참조하십시오. 참조 필드
관련 목록	필드 또는 관련 목록의 값 저장을관련 목록의 이 값에 연결 또는 이 값에 대한 연결로 설정하고 일치하는 기록이 없는 경우 새 기록을 생성하면 이 필드는 정보를 추가할 관련 목록을 지정합니다.
값 필드	필드 또는 관련 목록의 저장 값이관련 목록에서 이 값에 연결 또는 이 값에 연결로 설정되면 일치하는 기록이 없는 경우 새 레코드를 생성하며, 이 필드는 관련 목록에 표시되는 테이블 내의 필드를 지정합니다. 기존 기록을 조회하고 찾는 데 사용됩니다. 예를 들어, 관련 목록이 영향을 받는 **CI**인 경우 이 필드에는 이름 , 전체 주소 도메인 이름 또는 영향을 받는 **CI** 목록에 추가된 **CI** 를 조회하는 데 사용되는 CI 기록의 다른 필드가 포함될 수 있습니다.
관계 데이터	필드 또는 관련 목록의 값 저장을관련 목록의 이 값에 연결로 설정하면 해당 기록(예: 보안 인시던트)을 값(CI, 옵저버블 등)에 연결하기 위한 기록이 생성됩니다. 이 필드는 링크 기록에 추가해야 하는 추가 정보(필드 및

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵션	설명
	값 쌍)를 지정합니다. 예를 들어 소스 IP에 대한 옵저버블을 추가하는 경우 이 IP를 대상 IP가 아닌 소스로 지정합니다. 값이 여러 개인 경우 ^ 구분 기호(예: type= Source IP^Active=true)를 사용합니다.
새 기록 데이터	필드 또는 관련 목록의 값 저장을이 값에 연결로 설정하고 새 레코드를 만듭니다. 일치하는 레코드가 없으면 구문 분석된 값과 일치하는 관련 레코드가 없으면 레코드가 만들어집니다. 이 필드는 해당 기록에 추가할 정적 데이터를 지정합니다. 영향을 받는 **CI**의 경우 일치하는 CI가 없으면 CI 기록이 생성됩니다.) 이 경우 이메일에 있는 값이 CI 레코드의 값 필드로 설정됩니다. CI가 생성된 이유, 작업 중인 CI 유형에 대한 일부 정보 등을 나타내는 메모와 같은 추가 데이터를 설정할 수 있습니다. 샘플은 description=Created by Malware Scanner email parser^type=autodetect입니다.
값 검색	이메일에서 검색할 위치를 선택합니다. 선택 항목은 다음과 같습니다. ○ 이메일 본문의 줄 시작 부분에 ○ 이메일 본문의 모든 곳 ○ 이메일 제목 라인에 ○ 항상 정적 값 기록 구분 기호를 정의하면 추가 옵션(기록 섹션 내 아무 곳이나 및 기록 섹션 내 줄 시작 부분)을 사용하여 전체 이메일 본문 대신 현재 섹션 내에서만 검색할 수 있습니다(자세한 내용은 참조보안 운영 이메일 구문 분석). 모든 기록에 적용되는 머리글 또는 바닥글에 있는 정보는 전체 이메일 본문에서 검색됩니다. 기록마다 다른 정보는 섹션 내에서만 검색됩니다.
값 구분자	필드 또는 관련 목록의 저장 값이관련 목록에서 이 값에 연결 또는 이 값에 연결로 설정되면 일치하는 기록이 없는 경우 새 레코드를 생성하며, 이 필드는 항목 목록에 사용할 구분 기호를 지정합니다. 예를 들어 이메일의 데이터가 IP 주소 목록인 경우 쉼표 또는 세미콜론.
값 프리픽스	추출하기 위해 이 필드에 배치된 값보다 항상 선행하는 텍스트입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵션	설명
값의 끝	값의 끝을 표시하는 항목을 선택합니다. 선택 사항에는 줄의 끝, 이메일의 끝 (이메일에 남아 있는 모든 텍스트 가져오기) 또는 때까지 (지정된 텍스트를 찾으면 중지) 또는 때까지 (지정된 텍스트를 찾으면 중지)가 포함됩니다.
값 서픽스	값의 끝이 종료 기간으로 설정된 경우 이 필드는 이 필드에 배치된 값 뒤에 항상 오는 텍스트를 지정합니다. 예를 들어 "영향을 받는 컴퓨터는" 뒤와 "." 앞에 오는 값을 찾으면 "치매 토끼 바이러스가 발견되었습니다"에서 "AB123"이 구문 분석됩니다. 영향을 받는 컴퓨터는 AB123입니다. 감염 추정 시간은 오후 3시 45분이었다"고 이메일에서 밝혔다.
값 변환	적용할 필드 변환 항목을 선택합니다. 이메일에 있는 값을 다른 값으로 변환하여 선택 필드, 경우에 따라 참조 및 기타 필드를 채우는 데 사용됩니다.
순서	필드 변환이 실행되는 순서(가장 낮은 순서에서 가장 높은 순서)입니다. 주문 항목이 100인 필드 변환이 먼저 시도됩니다. 해당 필드 변환이 값을 찾지 못하는 경우에만 동일한 필드에서 더 높은 순서(200)의 필드 변환이 실행됩니다.
이메일 변환	이 필드 변환이 속한 변환입니다.
대상 테이블	이메일 변환의 대상 테이블입니다. 여기에는 이메일 변환의 정보 데이터가 포함되어 있습니다.
활성	기본값은 선택되어 있습니다. 선택하면 필드 변환이 활성화됩니다. 필드 변환을 비활성화하려면 이 확인란의 선택을 취소합니다.

a. 제출을 클릭합니다.
새 기록은 이메일의 정보를 새 기록으로 구문 분석하는 데 사용됩니다.

관련 정보

에서 중복 규칙 생성 보안 운영

필드 값 변환 생성 보안 운영

이메일 알림 정의 취약성 대응

에서 이메일 기록 편집 보안 운영

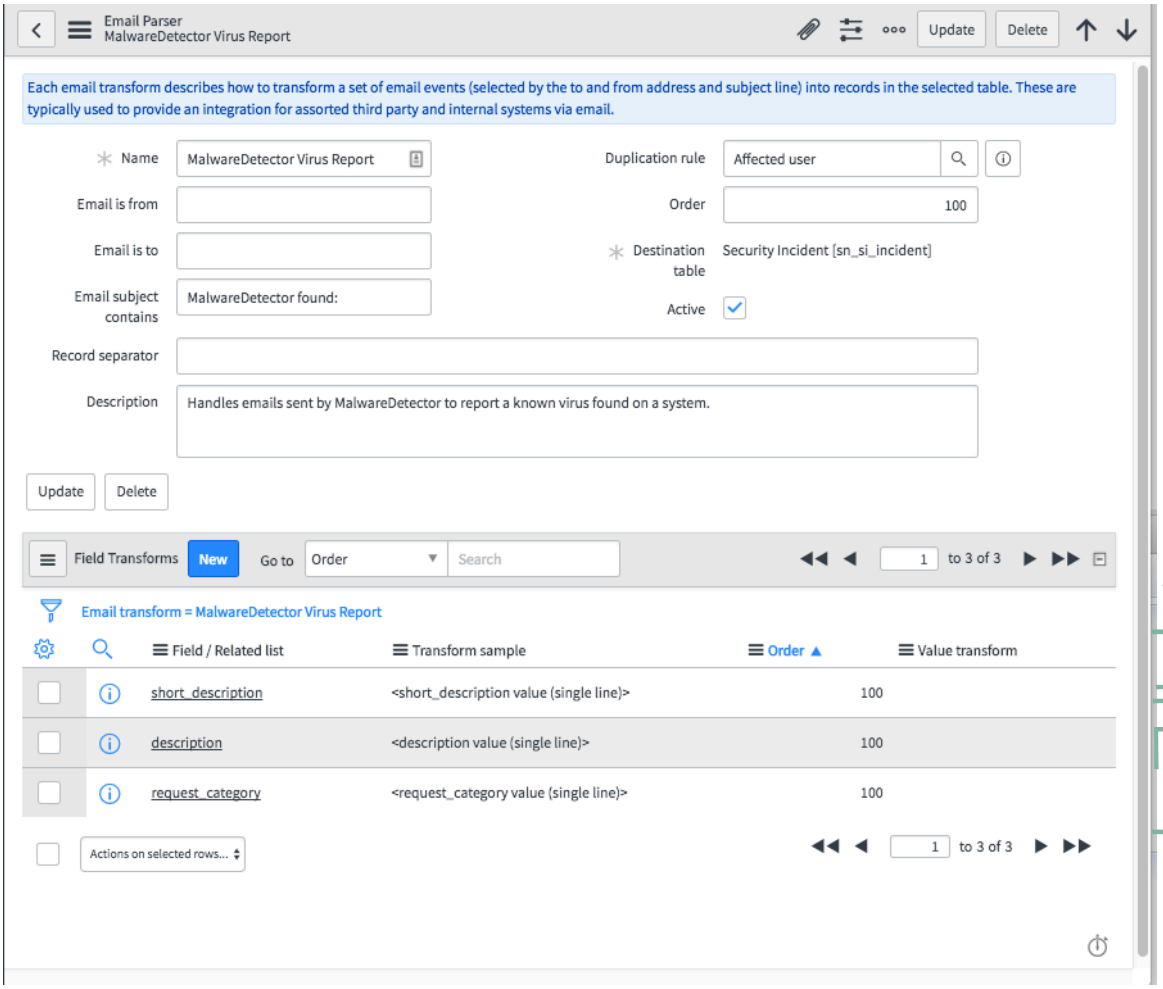
기존 이메일 이벤트 기록에 변환을 추가하거나 생성합니다.

시작하기 전에
필요한 역할: sn_sec_cmn.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 보안 운영 〉 이메일 구문 분석.
2. 편집할 이메일 파서를 클릭합니다.
   기록이 읽기 전용인 경우 헤더 메시지에서 여기 링크를 클릭합니다.
   변환의 편집 가능한 양식으로 이동합니다.



3. 필드를 적절하게 편집합니다.
4. 필드 변환을 편집하려면 필드를 클릭하고 적절하게 변경합니다.
5. 업데이트를 클릭합니다.

일치하지 보안 운영 않는 이메일 이벤트

이메일 파서와 일치하지 않는 이메일 이벤트에는 "matched" 플래그가 설정되지 않습니다. 목록에서 이러한 이메일 이벤트 기록을 일치하지 않는 이메일 보고 이메일이 아직 구문 분석되지 않은 외부 탐지 시스템을 표시할 수 있습니다.

이메일 파서를 만들 때 양식 또는 목록에서 이메일 이벤트를 다시 처리하여 새 이메일 파서의 유효성을 검사할 수 있습니다.

일치하지 않는 보안 운영 이메일 확인 및 재처리

중단된 필터를 검토 일치하지 않는 이메일 하거나 새 필터의 후보로 검토하여 이메일 위협을 탐지하는 속도를 유지하거나 개선할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_sec_cmn.read

프로시저

1. 다음으로 이동 모두 〉 보안 운영 〉 일치하지 않는 이메일.
   일치하지 않는 이메일이 발견되면 나열됩니다.
2. 양식의 필드는 다음과 같습니다.

보안 이메일 이벤트

필드	설명
시작일	보낸 사람의 이메일 주소입니다.
~	수신자의 이메일 주소입니다.
제목	이메일의 제목 줄입니다.
본문	이메일 본문의 내용입니다.
일치함	이 이메일 이벤트가 일치하는지 나타냅니다.

3. 이 이메일을 다시 처리하려면 이메일 기록을 생성하거나 이 이메일의 정보와 일치하도록 기존 이메일 기록을 편집합니다.
   보안 운영에서 이메일 파서 생성 문서를 참조하십시오.
4. (으)로 다시 이동 보안 운영 〉 일치하지 않는 이메일.
5. 이메일 이벤트 다시 처리를 클릭하여 이 이메일을 처리해 봅니다.
   기본 목록으로 돌아갑니다 일치하지 않는 이메일 . 새 이메일 기록이 일치하면 이메일 이벤트가 더 이상 목록에 없습니다. 메시지는 일치하는지 여부를 나타냅니다.

보안 운영 필드 매핑

보안 운영 테이블은 다른 테이블과 매핑되어 보안 인시던트를 고객 서비스 케이스에 연결하거나 문제를 시스템의 다른 부분에 보안 운영 연결할 수 있습니다.

필드 매핑 은 소스 테이블의 기록이 대상 테이블에서 새 기록을 생성하는 데 사용될 때 사용되는 매핑을 정의합니다. 일반적으로 다른 기록에서 보안 인시던트를 생성하는 데 사용되는 이러한 맵은 새 문제에 삽입되는 보안 인시던트의 필드 또는 기존 고객 인시던트의 어떤 필드가 새 보안 인시던트를 채우는지를 정의합니다.

보안 운영 필드 매핑을 사용하여 테이블을 테이블에 매핑

보안 운영 테이블을 다른 테이블에 매핑 보안 운영 할 수 있도록 더 세부적인 필드 매핑 세분성을 제공합니다.

시작하기 전에
필요한 역할: sec_cmn.write

프로시저

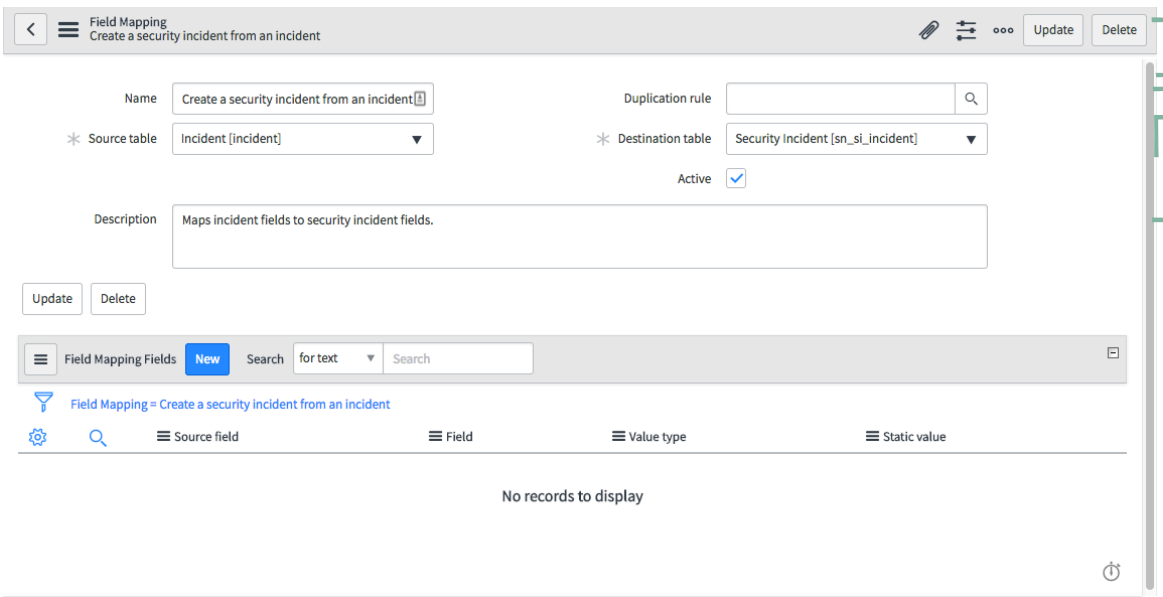
1. 다음으로 이동 모두 〉 보안 운영 〉 유틸리티 〉 필드 매핑.
2. 새로 만들기를 클릭합니다.
3. 양식의 필드에 적절히 입력합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드 매핑

필드	설명
이름	필드 맵의 이름입니다.
소스 테이블	대상 테이블에 기록을 생성하는 데 사용할 데이터를 제공하는 테이블입니다.
중복 규칙	중복 기록을 생성하는 소스 기록을 처리하는 방법을 제어합니다. 자세한 내용은 공유 데이터 변환 문서를 참조하십시오.
대상 테이블	새 기록이 생성되는 테이블입니다.
활성	매핑을 활성화하려면 이 확인란을 선택합니다. 주: 테이블 간의 매핑은 한 번에 하나만 활성화할 수 있습니다. 두 맵에 동일한 테이블이 포함되어 있으면 이전 버전이 자동으로 비활성화됩니다.
설명	필드 맵에 대한 설명입니다.

4. 입력을 완료했으면 양식 헤더를 마우스 오른쪽 버튼으로 클릭하고 저장을 선택합니다.
필드 매핑 필드 탭이 나타납니다. 이 기록은 이 필드 변환에 의해 생성된 기록에서 대상 필드에 배치되는 데이터를 정의합니다.



5. 새로 만들기를 클릭합니다.
6. 양식의 필드에 적절히 입력합니다.

옵션	설명
필드	설명
필드 또는 관련 목록에 값 저장	값을 찾을 위치를 선택합니다. 선택 항목은 다음과 같습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵션	설명
	○ 기록의 필드에 새 값 추가 ○ 관련 목록에서 이 값에 연결 ○ 이 값에 연결, 일치하는 기록이 없는 경우 레코드 생성 주: 대상 테이블에 관련 목록이 없으면 이 필드가 표시되지 않습니다.
필드	필드 또는 관련 목록의 값 저장을기록의 필드에 새 값 추가로 설정하면 이 필드는 채울 필드를 지정합니다. 주: 선택 필드의 경우 기본 선택 레이블 또는 값을 사용하여 기존 선택 사항과 일치시킵니다. 일치하는 항목이 없으면 필드가 설정되지만 새 항목이 선택 목록에 추가되지 않습니다. 자세한 내용은 다음을 참조하십시오. 선택 목록입니다. 참조 필드의 경우, 기록의 표시 이름과 일치하는 값이 있거나 유효한sys_id 있는 경우에만 항목이 설정됩니다. 자세한 내용은 다음을 참조하십시오. 참조 필드
관련 목록	필드 또는 관련 목록의 값 저장을관련 목록의 이 값에 연결 또는 이 값에 대한 연결로 설정하고 일치하는 기록이 없는 경우 새 기록을 생성하면 이 필드는 정보를 추가할 관련 목록을 지정합니다.
값 필드	필드 또는 관련 목록의 값 저장을관련 목록에서 이 값에 연결 또는 이 값에 연결하여 새 기록 생성(일치하는 기록이 없는 경우)으로 설정된 경우, 이 필드는 관련 목록에 표시되는 테이블 내의 필드를 지정하여 기존 기록을 조회하고 찾는 데 사용됩니다. 예를 들어, 관련 목록이 영향을 받는 **CI**인 경우 이 필드에는 이름 또는 전체 주소 도메인 이름이 포함될 수 있으며, CI를 조회하는 데 사용해야 하는 CI 기록의 다른 필드가 영향을 받는 **CI** 목록에 추가됩니다.
관계 데이터	필드 또는 관련 목록의 값 저장을관련 목록의 이 값에 연결로 설정하면 해당 기록(예: 보안 인시던트)을 값(CI, 옵저버블 등)에 연결하기 위한 새 기록이 생성됩니다. 이 필드는 해당 링크 기록에 추가해야 하는 추가 정보(필드 및 값 쌍)를 지정합니다. 예를 들어 소스 IP에 대한 옵저버블을 추가할 때 이 IP를 대상 IP가

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵션	설명
	아닌 소스로 지정할 수 있습니다. 값이 여러 개인 경우 ^ 구분 기호(예: type= Source IP^active=true)를 사용합니다.
새 기록 데이터	필드 또는 관련 목록의 값 저장을이 값에 연결로 설정하고 일치하는 기록이 없는 경우 새 레코드를 만들고 구문 분석된 값과 일치하는 관련 레코드를 찾을 수 없는 경우 새 레코드가 만들어집니다. 이 필드는 해당 기록에 추가할 정적 데이터를 지정합니다. 예를 들어 영향을 받는 CI의 경우 **CI**를 찾을 수 없으면 이 설정은 새 CI가 생성되었음을 나타냅니다.) 소스 기록에 있는 값이 CI 기록의 값 필드로 설정됩니다. 추가 데이터(이 CI가 생성된 이유, 작업 중인 CI 유형에 대한 일부 정보를 나타내는 메모)를 설정할 수 있습니다. 샘플은 다음과 같습니다. description=Created by malware Incident report^type=autodetect
값 구분자	필드 또는 관련 목록의 값 저장을관련 목록의 이 값에 연결 또는 이 값에 대한 연결로 설정하고 일치하는 기록이 없는 경우 새 기록을 생성하면 이 필드는 항목 목록에 사용할 구분 기호(일반적으로 쉼표 또는 세미콜론)를 지정합니다.
값 유형	필드 또는 관련 목록의 값 저장을기록의 필드에 새 값 추가로 설정하면 이 필드는 값의 유형을 지정합니다. 선택 항목은 다음과 같습니다. ○ 소스 필드 기록 ○ 새 라인으로 필드에 추가 ○ 정적 값 ○ 정적 값 더하기 소스 기록 필드 값
소스 필드	대상 필드 또는 선택한 관련 목록에 배치할 값이 포함된 소스 필드를 선택합니다.
정적 필드	필드에 대한 정적 값입니다.
값 변환	적용할 필드 값 변환 항목을 선택합니다. 이 옵션은 기록 간에 선택 필드를 매핑하는 데 사용됩니다. 예를 들어, 보안 인시던트에 대한 범주 선택 세트를 변경 요청의 적절한 유형 필드로 변환합니다.
대상 테이블	대상 테이블로 자동으로 채워집니다.
필드 매핑	상위 필드 맵으로 자동으로 채워집니다.
소스 테이블	소스 테이블로 자동으로 채워집니다.

7. 제출을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 운영 필드 값 변환

고유한 고객 필드 값을 필드 맵을 사용하여 이메일 구문 분석, 데이터 강화 또는 테이블에서 인식하는 보안 운영 필드 값으로 변환합니다. 선택 필드, 참조를 지원하고 외부 데이터를 새 기록의 표준 용어 및 형식으로 정렬합니다.

범주, 상태 또는 할당 그룹과 같은 필드의 데이터를 보안 운영 테이블 내에서 사용되는 값에 매핑할 수 있습니다. 예를 들어 "분석 중"을 "진행 중"에 매핑합니다.

필드 값 변환 생성 보안 운영

필드 값 변환은 제공된 소스 데이터와 사용할 대체 값 간의 하나의 변환을 정의합니다.

시작하기 전에

필요한 역할: sn_sec_cmn.basic 또는 sn_si.basic

이 태스크 정보

검색 값과 일치하는 경우 또는 검색 값이 제공된 소스 데이터에 포함되거나 일치하는 항목이 없을 때 적용할 각 변환 항목을 정의합니다. 일치하는 항목이 없는 경우의 기본값을 설정합니다. 기본값이 설정되지 않고 일치하는 항목이 없으면 원래 소스 데이터가 사용됩니다.

프로시저

1. 다음으로 이동 모두 〉 보안 운영 〉 유틸리티 〉 필드 값 변환.
2. 새로 만들기를 클릭합니다.
3. 양식의 필드에 적절히 입력합니다.

필드 값 변환

필드	설명
이름	필드 값 변환의 이름입니다.
설명	필드 맵에 대한 설명입니다.
필드 값 변환 항목	항목의 테이블 목록입니다. **a.** 데이터 바꾸기에서 '새 행 삽입'을 두 번 클릭합니다. **b.** 다음 중 하나를 선택합니다. 이 필드의 날짜가 일치하는 경우 이 필드의 데이터에 다음이 포함된 경우 데이터와 일치하는 다른 변환 항목이 없는 경우(기본값) **c.** 녹색 확인 표시를 클릭합니다. **d.** 검색 값 아래를 두 번 클릭하고 검색 값을 추가합니다. **e.** 녹색 확인 표시를 클릭합니다. **f.** 대체 값 아래를 두 번 클릭하고 해당 값을 추가합니다ServiceNow. **g.** 필요한 경우 반복합니다.
활성	변환을 활성화하려면 이 확인란을 선택합니다.
애플리케이션	애플리케이션의 범위입니다.

4. 제출을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 운영 보강 데이터 매핑

보강 데이터 매핑 데이터를 XML, JSON 또는 속성 파일에서 기록으로 ServiceNow 변환합니다. 보안 운영 워크플로우는 향상된 데이터 맵을 사용하고 보안 인시던트에 출력 데이터를 제공합니다.

보안 운영 에는 다양한 워크플로우에 의해 트리거되는 여러 보강 데이터 맵이 포함되어 있습니다. 예를 들어, 보안 운영 통합 - 네트워크 통계 플로우 가져오기보안 운영 시스템 명령 통합 - 실행 중인 프로세스 가져오기 플로우및 . 워크플로우의 보안 운영 보강 데이터 맵 출력이 보안 인시던트 양식의 보강 데이터 탭에 표시됩니다.

보안 운영 보강 데이터 맵 생성

향상된 데이터 맵을 사용하여 데이터를 JSON, XML 또는 속성 파일 형식에서 기록으로 ServiceNow 변환합니다.

시작하기 전에

필요한 역할: sn_sec_cmn.write

이 태스크 정보

기존 보강 데이터 맵은 내에서 보안 운영제공되는 워크플로우에서 사용됩니다. **Enrichment Data** Mapping(보강 데이터 매핑)에서 목록을 볼 수 있습니다. 맵을 사용하려면 트리거(비즈니스 규칙 또는 워크플로우)가 필요합니다.

프로시저

1. 다음으로 이동 모두 〉 보안 운영 〉 유틸리티 〉 보강 데이터 매핑.
2. 새로 만들기를 클릭합니다.
3. 필드에 적절한 정보를 입력합니다.

보강 데이터 맵 생성

필드	설명
이름	이 보강 데이터 맵의 이름입니다.
입력 형식	목록에서 형식을 선택합니다. JSON(기본값) XML 속성 파일 형식
프리픽스 키	입력 데이터 세트를 지정된 키로 제한하는 데 사용합니다. 입력 데이터 세트의 루트가 이 키로 설정됩니다. 이 예에서 file_info 입력한 경우 입력 값은 file_info 내의 해당 값으로 제한됩니다. <?xml version="1.0" encoding="UTF-8"?> <malware> <version>2.0</version> <file_info> <malware>yes</malware> <sha1>24c051142583e10451a53893fed3aa5d80bfb1f6</sha1> <filetype>PE</filetype>

기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	<sha256>be9bd96808173e2d967feef8c8c5b8c4d73b621584fb11eb68434da1e6a0a9300</sha256> <md5>ee8c91751b3010e38c479cf9ab09827a</md5> <size>546304</size> </file_info> </malware>
애플리케이션	애플리케이션의 범위입니다.
중복 규칙	기록이 중복으로 간주되는 경우와 중복 기록에 대해 수행할 작업을 정의하는 규칙입니다.
대상 테이블	목록에서 테이블을 선택합니다.
활성	맵을 활성화하려면 이 확인란을 선택합니다.
설명	보강 데이터 맵에 대한 설명을 입력합니다.

4. 제출을 클릭합니다.
   보강 데이터 매핑 필드 탭이 나타납니다.
5. 새로 만들기를 클릭합니다.
6. 양식의 필드에 적절히 입력합니다.

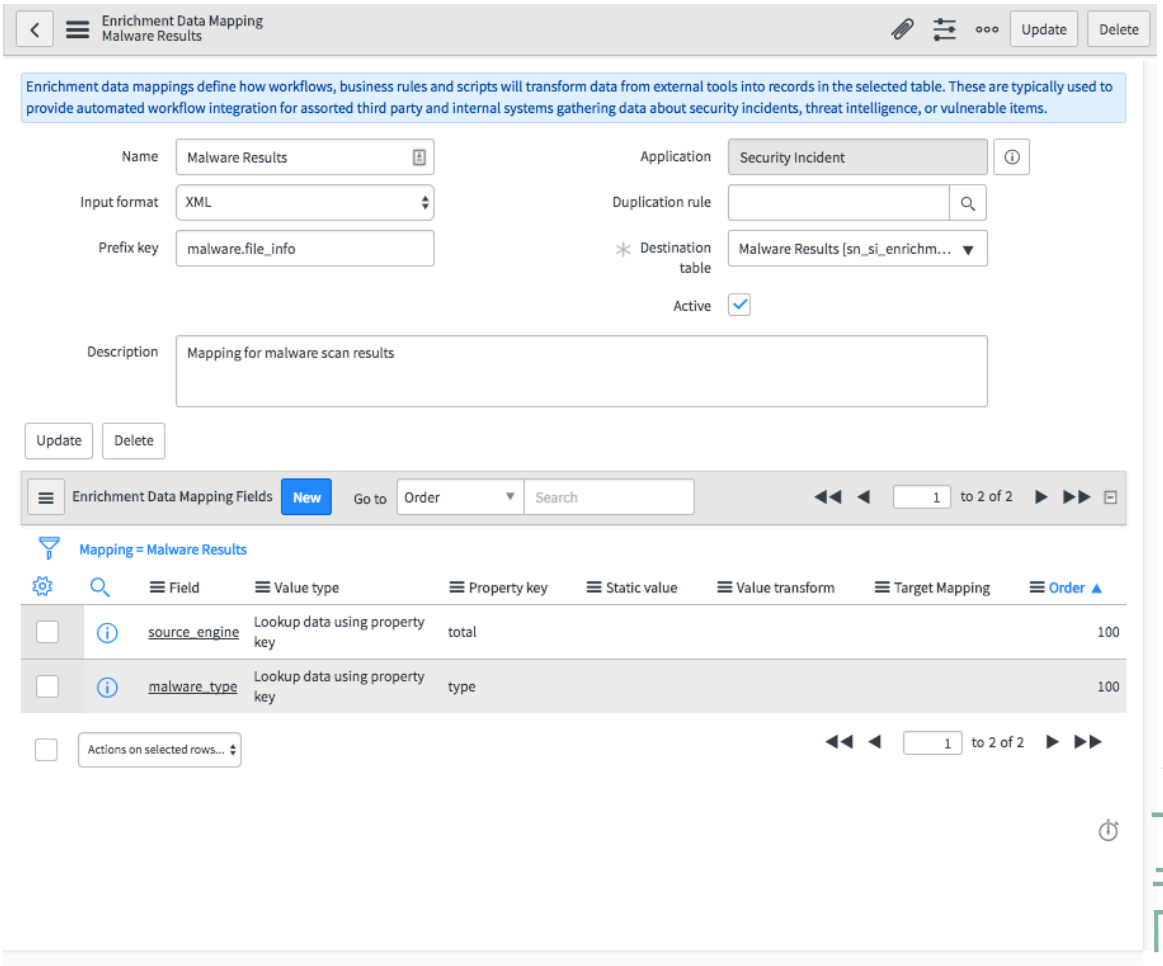
보강 데이터 매핑 필드

필드	설명
필드	보강 데이터 맵의 이름입니다.
값 유형	목록에서 선택합니다. 속성 키를 사용하여 데이터 조회 정적 값 정적 값 더하기 속성 키의 데이터 필드가 어레이 또는 객체(원시 데이터 네스팅) 각 선택 항목에는 다른 항목이 있습니다. 필드 값과 배열 또는 객체에는 Property 키가 필요합니다.
속성 키	입력 데이터 검색의 키와 대상 필드에 쓰여진 값을 결정합니다.
값 변환	한 값을 다른 값에 매핑하는 필드 값 변환입니다.
애플리케이션	애플리케이션의 범위입니다.
순서	매핑을 고려할 순서입니다. 첫 번째 일치가 사용됩니다. 기본값은 100입니다.
매핑	보강 데이터 맵의 이름입니다.
대상 테이블	매핑할 필드가 이동하는 테이블입니다.

7. 제출을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음은 보강 데이터 맵의 예입니다.



보안 운영 사용자 정의 에스컬레이션

주의 또는 전문 지식이 더 필요한 문제의 보안 인시던트에 대해 에스컬레이션 경로를 작성할 수 있습니다. 에스컬레이션 그룹이 있으면 해당 그룹의 모든 보안 인시던트에 버튼이 나타납니다.

보안 운영 사용자 정의 에스컬레이션 그룹 생성

에스컬레이션을 사용하여 보안 인시던트를 인시던트와 관련된 그룹으로 에스컬레이션합니다.

시작하기 전에
필요한 역할: sn_si.admin

프로시저

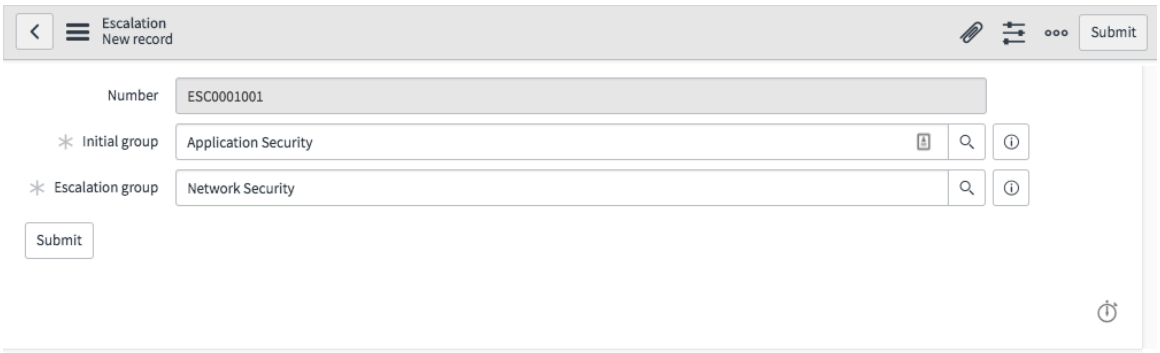
1. 다음으로 이동 모두 〉 보안 운영 〉 그룹 〉 에스컬레이션.
2. 새로 만들기를 클릭합니다.
3. 양식의 필드에 적절히 입력합니다.

에스컬레이션

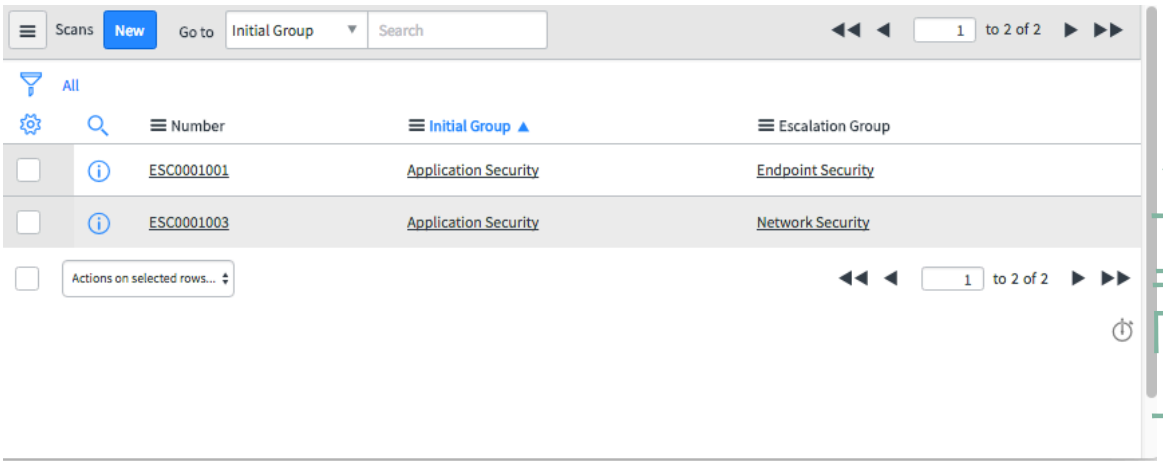
필드	설명
번호	에스컬레이션 인시던트 번호(필드는 자동 생성됨)입니다.
시작 그룹	이 보안 인시던트가 속한 그룹을 선택하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
에스컬레이션 그룹	보안 인시던트를 에스컬레이션할 대상 그룹을 선택합니다.



4. 제출을 클릭합니다.
   초기 그룹의 모든 보안 인시던트에 에스컬레이션 그룹을 사용할 수 있습니다. 여러 그룹을 생성할 수 있습니다.



도메인 분리 속성 재정의 생성

도메인 분리를 사용할 때 각 도메인에서 애플리케이션의 기능을 사용자 지정할 수 있는 기존 보안 운영 속성에 대한 재정의를 만들 수 있습니다.

시작하기 전에

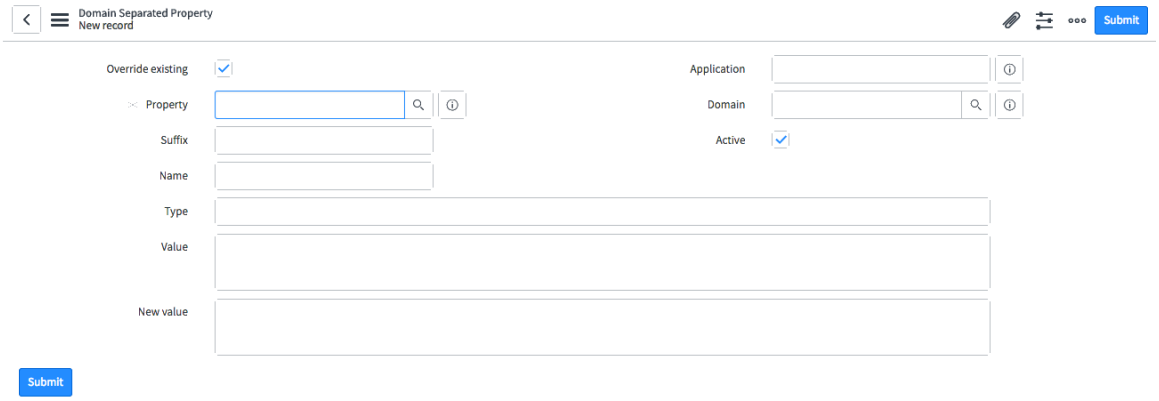
도메인 지원 - 도메인 확장을 활성화해야 합니다. 도메인 재정의 뷰어에 대해서도 알아볼 수 있습니다.

필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 〉 보안 운영 〉 유틸리티 〉 도메인으로 구분된 속성.
2. 새로 만들기를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



3. 양식에서 필드를 채웁니다.

도메인 분리 속성 양식

필드	설명
기존 재정의	기존 속성에 대해 도메인별 값을 생성하려면 이 확인란을 선택합니다.
애플리케이션	재정의할 속성이 포함된 애플리케이션을 선택합니다.
속성	도메인별 재정의를 만들 선택한 애플리케이션의 속성을 선택합니다.
도메인	이 속성 재정의를 생성할 도메인을 선택합니다.
활성	재정의를 켜거나 끕니다.
접미사	속성 접미사를 표시합니다.
이름	속성 이름을 표시합니다.
유형	속성 유형을 표시합니다.
값	속성에 대해 설정된 현재 값을 표시합니다.
새 값	이 도메인에 적용할 속성의 새 값을 입력합니다.

4. 제출을 클릭합니다.
속성 재정의가 지정된 도메인에서 선택한 속성에 적용됩니다. 이 속성에 대한 논리가 트리거되면 시스템은 도메인으로 구분된 속성 무효화를 확인합니다. 도메인에 대한 재정의가 발견되면 새 값이 사용됩니다. 그렇지 않으면 기본 도메인의 값이 사용됩니다.

관련 정보

도메인 분리 이해

운영 체제 그룹 작성

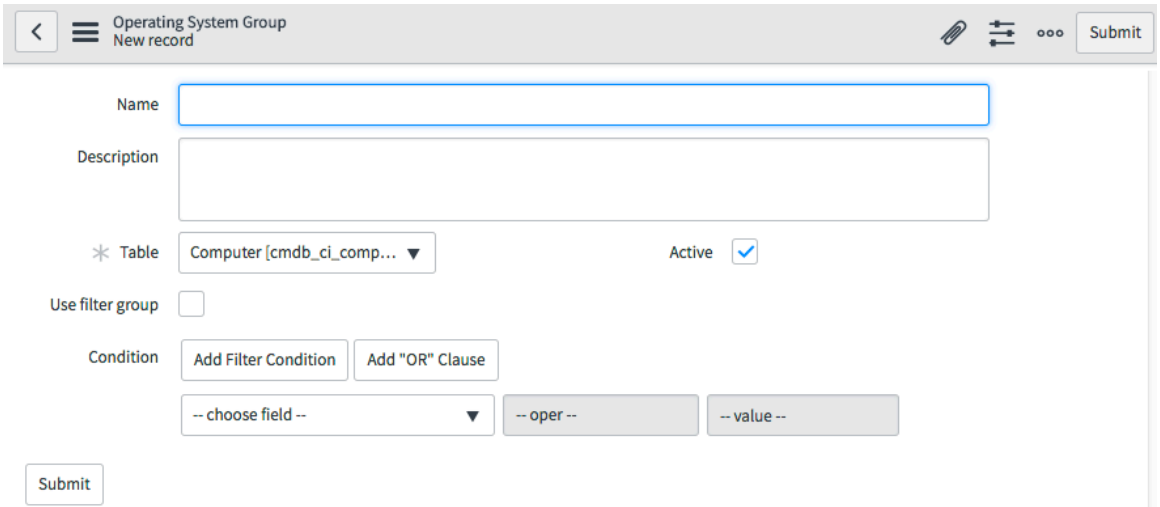
운영 체제 그룹은 운영 체제를 워크플로우의 보안 인시던트 응답 특정 프로세스 유형 및 스크립트에 매핑하는 데 사용됩니다. 스크립트는 정의된 운영 체제 그룹에 대해 실행 중인 프로세스를 검색하는 방법을 정의합니다. 필요에 따라 새 운영 체제를 추가할 수 있습니다.

시작하기 전에
필요한 역할: sn_sec_cmn.admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 보안 운영 〉 유틸리티 〉 운영 체제 그룹.
   기본 시스템에는 다음 세 가지 운영 체제에 대한 스크립트가 포함되어 있습니다.
   - BSD 기반 OS
   - POSIX 기반 OS
   - Windows OS
2. 새로 만들기를 클릭합니다.

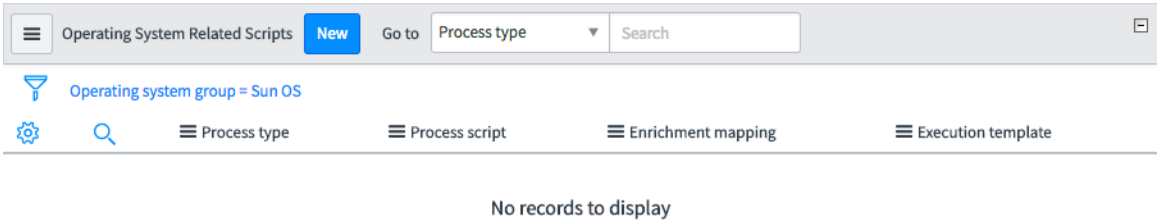


3. 필요에 따라, 필드를 채웁니다.

필드	설명
이름	운영 체제 그룹의 이름입니다.
설명	운영 체제 그룹에 대한 설명입니다.
테이블	영향을 받는 테이블입니다.
활성	운영 체제 그룹을 활성화하려면 이 확인란을 선택합니다.
필터 그룹 이용	선택한 테이블에서 일치하는 기록을 찾기 위해 필터 그룹을 사용하려면 이 확인란을 선택합니다.
필터 그룹	선택한 테이블에서 일치하는 기록을 찾으려면 필터 그룹을 선택합니다. 이 필드는 필터 그룹 사용 확인란을 선택한 경우에만 표시됩니다.
조건	는 조건 작성기 필드는 필터 그룹 사용 확인란을 선택하지 않은 경우에만 표시됩니다.

4. 양식 헤더를 마우스 오른쪽 버튼으로 클릭하고 저장을 선택합니다.
   운영 체제 관련 스크립트 관련 목록이 열립니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



5. 새로 만들기를 클릭합니다.
6. 사용 중인 워크플로우에 해당하는 스크립트를 선택하여 실행 중인 프로세스, 서비스 및/또는 네트워크 통계를 가져옵니다.
7. 제출을 클릭합니다.

관련 정보

동기화된 파일에 스크립트 파일 첨부 MID 서버

보안 태그 그룹 및 태그 설정

보안 인시던트, 응답 작업, 취약한 항목, 옵저버블, IoC 및 보안 케이스에 태그를 할당하여 응답 기록에 대한 메타데이터를 생성하고 특정 유형의 보안 콘텐츠에 액세스할 수 있는 사용자를 정의할 수 있습니다. 태그를 보안 그룹에 추가하여 구성할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.admin

프로시저

1. 다음으로 이동 모두 〉 보안 운영 〉 보안 태그 〉 그룹.
   기본 시스템에는 세 개의 기본 분류 그룹이 포함되어 있습니다.
   - 보강 허용 목록/거부 목록: 이 그룹은 기록을 허용 목록 또는 거부 목록 기록으로 처리할지 여부를 정의합니다. 허용 목록 기록은 일반적으로 중요도가 낮으므로 무시해도 됩니다. 거부 목록 기록은 일반적으로 관심이 더 높습니다.
   - 메타 태그: 이 그룹은 데모 데이터로 제공됩니다. 이를 사용하여 보안 운영 애플리케이션에서 사용하는 사용자 지정 분류 태그를 만들 수 있습니다.
   - 신호등 프로토콜: 이 그룹은 중요한 정보가 올바른 대상과 공유되도록 하는 데 사용됩니다. 4가지 색상(흰색, 녹색, 호박색, 빨간색)을 사용하여 다양한 민감도를 나타냅니다. 각 색상에 대해 적절한 읽기/쓰기 액세스 역할을 할당할 수 있습니다. 옵저버블을 신뢰할 수 있는 보안 서클에 공유할 때 신뢰할 수 있는 보안 서클 프로파일에 할당된 태그는 다음과 같이 서클에 공유할 수 있는 TLP 태그가 지정된 옵저버블을 결정합니다.
     - **TLP:** 흰색: TLP: WHITE가 있는 옵저버블만 TLP: WHITE 프로필에 공유할 수 있습니다.
     - **TLP:** 녹색: TLP: GREEN 및 TLP: WHITE가 있는 옵저버블은 TLP: GREEN 프로필에 공유할 수 있습니다.
     - **TLP:** 호박색: TLP: AMBER, TLP: GREEN 및 TLP: WHITE가 있는 옵저버블을 TLP: AMBER 프로파일에 공유할 수 있습니다.
     - **TLP:** 빨간색: TLP: RED가 가장 높은 순위의 TLP 태그이므로 TLP 태그에 관계없이 모든 옵저버블을 TLP: RED 프로필과 공유할 수 있습니다.

     주:
     다른 TLP 색상을 추가할 수 있지만 포함된 네 가지 색상 외에 다른 색상은 FIRST(인시던트 응답 및 보안 팀 포럼)에서 유효하지 않은 것으로 간주됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

2. 새로 만들기를 클릭합니다.
3. 양식의 필드에 적절히 입력합니다.

필드	설명
이름	보안 그룹의 이름을 입력합니다.
다중 선택 허용	그룹을 공유하는 기록에 여러 보안 태그를 할당하려면 이 확인란을 선택합니다.
활성	그룹을 사용 또는 사용 중지합니다.
설명	이 그룹에 대한 설명을 입력합니다.

4. 양식 헤더를 마우스 오른쪽 버튼으로 클릭하고 저장을 선택합니다.
보안 태그 관련 목록이 나타납니다.
5. 보안 태그 관련 목록에서 새로 만들기를 클릭합니다.
6. 양식의 필드에 적절히 입력합니다.

필드	설명
이름	분류 태그의 이름입니다.
보안 태그 그룹	그룹 관련 목록에서 새로 만들기 버튼을 사용하여 태그를 만든 경우 이 필드는 기본적으로 현재 그룹으로 지정됩니다. 필요한 경우 다른 그룹에 태그를 추가할 수 있지만 이는 선택 사항입니다.
순서	양식이나 목록 내에서 태그가 나타나는 순서를 지정합니다.
색상	이 태그의 색상을 선택합니다.
제한된 권한 실행	사용자가 이 보안 태그가 있는 레코드를 읽거나 쓰는 데 필요한 읽기 및/또는 쓰기 역할을 할당하려면 이 확인란을 선택합니다.
활성	태그를 사용 또는 사용 중지합니다.
설명	이 태그에 대한 설명입니다.
역할(읽기 권한)	보안 태그에 읽기 권한을 할당하려면 자물쇠 아이콘을 클릭하고 적절한 접근 역할을 선택한 다음 자물쇠 아이콘을 다시 클릭합니다. 이 필드는 제한된 접근 적용 확인란을 선택한 경우에만 나타납니다.
역할(쓰기 권한)	보안 태그에 쓰기 액세스 권한을 할당하려면 잠금 아이콘을 클릭하고 적절한 액세스 역할을 선택한 다음 잠금 아이콘을 다시 클릭합니다. 이 필드는 제한된 접근 적용 확인란을 선택한 경우에만 나타납니다.

7. 필요한 만큼 반복하여 더 많은 보안 태그를 생성합니다.
8. 업데이트를 클릭합니다.

> **주:**
> 다음으로 이동하여 새 태그를 생성할 수도 있습니다. 보안 운영 〉 보안 태그 〉 태그. 절차는 동일합니다.

보안 태그 규칙 생성

보안 태그 규칙은 보안 태그 액세스에 대한 필터링을 제공합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 〉 보안 운영 〉 보안 태그 〉 태그.
2. 보안 태그를 선택하거나 생성합니다.
3. 보안 태그 규칙 관련 탭에서 새로 만들기를 클릭합니다.
4. 양식의 필드에 적절히 입력합니다.

필드	설명
이름	보안 태그 규칙의 이름입니다.
보안 태그	규칙에 연결할 보안 태그입니다.
활성	보안 태그를 켜거나 끕니다.
설명	이 규칙에 대한 설명입니다.

5. 기록 필터링을 결정합니다.
6. 양식의 필드에 적절히 입력합니다.

필드	설명
필터 그룹 이용	필터 그룹을 규칙에 연결합니다.
테이블	규칙을 포함할 테이블입니다.
조건	하나 이상의 필터 조건을 추가합니다.

7. 제출을 클릭합니다.

보안 태그 규칙 임포트

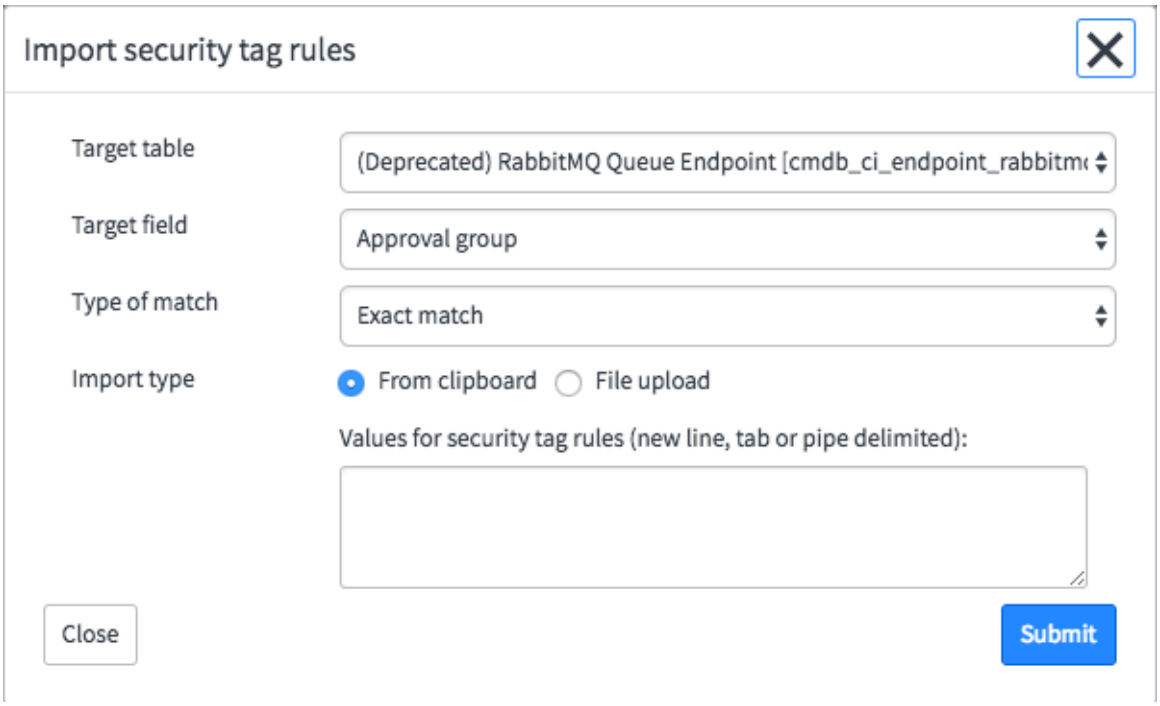
배포의 다른 테이블에서 보안 태그 규칙을 임포트할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 〉 보안 운영 〉 보안 태그 〉 태그.
2. 보안 태그를 선택하거나 생성합니다.
3. 보안 태그 규칙 임포트 관련 링크를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 양식의 필드에 적절히 입력합니다.

필드	설명
대상 테이블	규칙을 임포트하는 데 사용할 테이블을 선택합니다.
대상 필드	규칙을 임포트하는 데 사용할 필드를 선택합니다.
일치 유형	다음에서 임포트한 규칙을 보안 태그 와 일치시키는 방법을 선택합니다. 정확히 일치(기본값) 포함 다음으로 시작 다음으로 끝남 정규 표현식
임포트 유형	고르다: 클립보드에서 구분 값 목록을 텍스트 영역에 복사합니다. 이 값은 보안 태그로 구문 분석됩니다. 파일 업로드에서 구분 값으로 값을 포함한 파일을 업로드합니다. 이 값은 보안 태그로 구문 분석됩니다. 줄 바꿈 또는 파이프 구분 기호를 사용하여 보안 태그 규칙에 대한 값을 추가합니다.

5. 제출을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 주석

보안 주석은 구성 항목, 옵저버블 또는 보안 인시던트에 대한 사용에 추가되는 설명 또는 설명에 대한 메모입니다.

사용자 및 옵저버블에 대해 여러 보안 주석을 사용할 수 있습니다(플러그인 위협 인텔리전스 필요). 보안 주석에 대한 보고서도 사용할 수 있습니다.

CI에 대한 보안 주석 생성

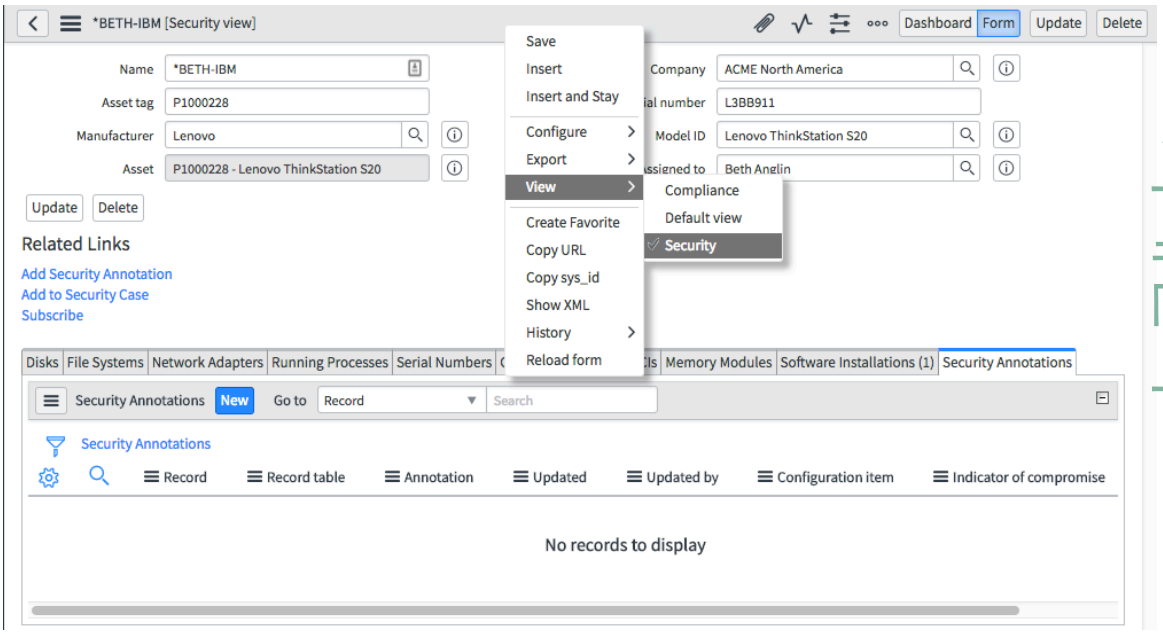
CI에 대한 주석을 사용하면 여러 인시던트의 활동을 추적할 수 있습니다. 하나 또는 여러 개의 CI에 주석을 추가할 수 있습니다.

시작하기 전에

필요한 역할: 관리자

프로시저

1. 보안 인시던트 또는 구성 항목 테이블에서 CI를 엽니다.
2. 헤더를 마우스 오른쪽 버튼으로 클릭하고 뷰 > 보안.



3. 보안 주석 관련 목록 탭에서 새로 만들기를 클릭합니다.
4. 주석을 입력합니다.
   주석은 모든 텍스트 형식이 될 수 있습니다.
5. 제출을 클릭합니다.

> **주:**
> 목록에서 CI를 선택하고, 보안 주석 추가를 선택하고, 텍스트 형식으로 주석을 입력하고, 제출을 클릭하여 여러 CI에 동일한 주석을 추가할 수 있습니다.

옵저버블에 대한 보안 주석 생성

하나 또는 여러 옵저버블을 선택하고 선택한 행에 대한 작업 선택 메뉴를 사용하여 보안 주석을 적용할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

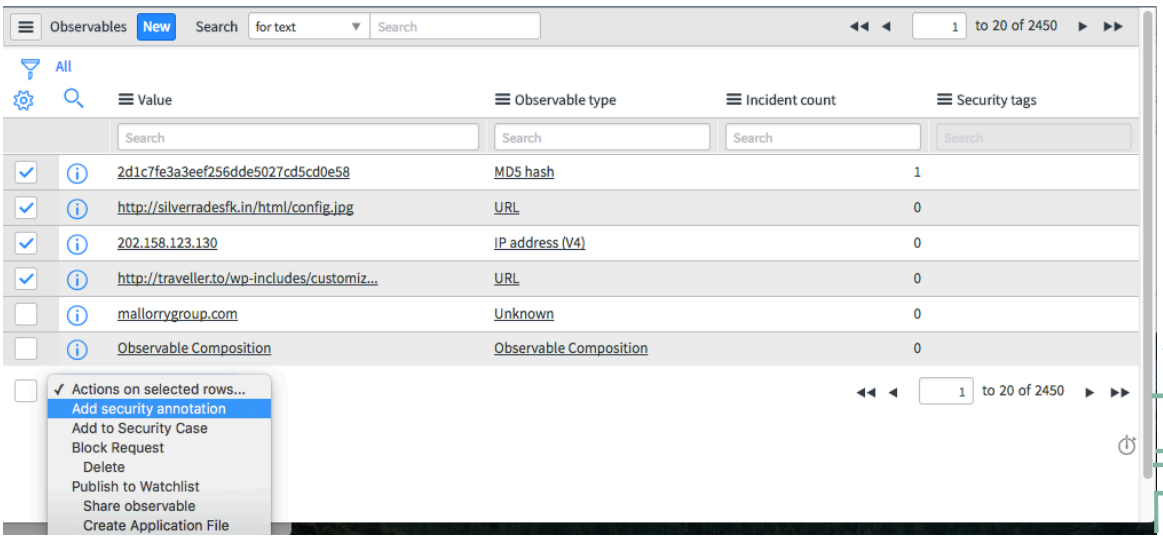
시작하기 전에

- 플러그인과 활성화가 위협 인텔리전스 필요합니다. 위협 인텔리전스 플러그인은 별도의 구독으로 제공됩니다.

필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 〉 위협 인텔리전스 〉 옵저버블
2. 목록에서 옵저버블을 하나 이상 선택합니다.
3. **Actions on selected** rows(선택한 행에 대한 작업) 드롭다운 메뉴에서 **Add security** annotation(보안 주석 추가)을 선택합니다.



4. 주석을 입력합니다.
   주석은 모든 텍스트 형식이 될 수 있습니다.
5. 제출을 클릭합니다.

사용자에 대한 보안 주석 작성

한 명 또는 여러 명의 사용자를 선택하고 선택한 행 선택 메뉴에 대한 작업을 사용하여 보안 주석을 적용할 수 있습니다.

시작하기 전에
플러그인과 활성화가 위협 인텔리전스 필요합니다. 위협 인텔리전스 플러그인은 별도의 구독으로 제공됩니다.

필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 〉 사용자 관리 〉 사용자
2. 목록에서 하나 이상의 사용자를 선택합니다.
3. **Actions on selected** rows(선택한 행에 대한 작업) 드롭다운 메뉴에서 **Add security** annotation(보안 주석 추가)을 선택합니다.
4. 주석을 입력합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주석은 모든 텍스트 형식이 될 수 있습니다.

5. 제출을 클릭합니다.

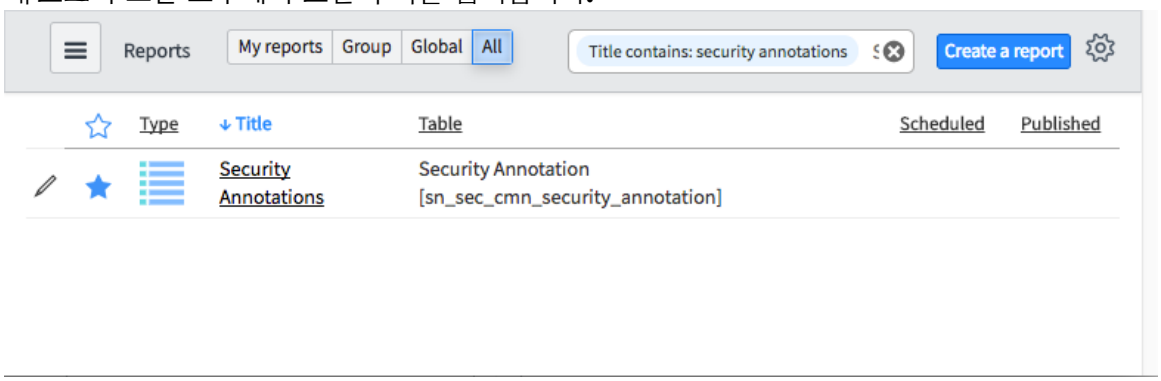
보안 주석 보고서 보기

보안 주석 보고서에는 보안 주석 [sn_sec_cmn_security_annotations] 테이블에 저장된 세부 정보가 표시됩니다. 보고서의 열을 사용자 지정하고 원하는 방식으로 데이터를 그룹화할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 〉 보고서 〉 보기/실행.
2. 내 보고서 또는 모두에서 보안 주석을 검색합니다.



관련 정보

보고서 목록 보기

Security Support Common 앱과 함께 설치되는 구성요소

Security Support Common 앱과 함께 여러 가지 유형의 구성요소가 설치됩니다. 와 같은 보안 인시던트 응답다양한 보안 애플리케이션에서 사용할 수 있는 공통 기능을 제공합니다.

설치된 구성요소 찾기 및 보기

설치된 구성요소를 찾아 보는 방법에 대한 자세한 내용을 참조하십시오 와 함께 설치되는 구성요소 뷰 Security Support Common .

와 함께 설치되는 구성요소 뷰 Security Support Common

플러그인을 활성화하면 Security Support Common 테이블, 사용자 역할, 모듈을 포함하되 이에 국한되지 않는 여러 유형의 구성요소가 설치됩니다.

구성요소 찾기

주:
애플리케이션 파일 테이블에는 이 애플리케이션과 함께 설치되는 구성요소가 나열됩니다. 이 테이블에 액세스하는 방법에 대한 지침은 애플리케이션과 함께 설치되는 구성요소 찾기 를 참조하십시오.

설치된 구성요소 목록을 보안 지원 공통 애플리케이션의 역할, 예약된 작업 및 테이블로 제한하려면 다음 단계를 수행하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

애플리케이션과 함께 설치된 구성요소에 대해 필터링된 목록 보기

애플리케이션과 함께 설치되는 역할, 예약된 작업 및 테이블만 표시되도록 애플리케이션 파일 테이블을 필터링합니다. 해당 파일이 인스턴스와 메타데이터 테이블에 로드되도록 이러한 구성요소를 보려는 애플리케이션을 설치해야 합니다. 다음 단계에 따라 애플리케이션 파일 테이블에서 필터링된 목록을 봅니다.

1. 필터 탐색기에서 **sys_metadata.list** 를 입력하여 메타데이터 테이블로 이동합니다.
2. 조건 작성기(필터 아이콘)를 선택하고 애플리케이션 〉 다음과 같음 다음에 애플리케이션 이름이 표시됩니다.
3. 조건 작성기에서 두 번째 필터를 추가하려면 **AND**를 클릭한 후 클래스 〉 다음 중 하나 을 클릭하고 목록에서 역할, 예약된 작업 또는 테이블 클래스 중 하나를 선택합니다.
4. 실행을 선택합니다.

선택한 클래스의 결과가 필터링된 목록에 표시됩니다.

〔store-future: BEGIN review〕

보안 운영 애플리케이션에 대한 역할별 모듈 액세스

각 애플리케이션에 대해 특정 역할로 액세스할 수 있는 메뉴 항목을 확인합니다.

〔End〕
〔store-future: BEGIN review〕

구성 준수를 위한 역할별 모듈 액세스

구성 준수에 대한 자세한 내용은 특정 역할로 액세스할 수 있는 메뉴 항목을 참조하십시오.

다음에 대한 모듈 액세스: **sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule**

다음에 대한 모듈 액세스: **sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule**

다른 역할에 대한 정보:

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

sn_vulc.remediation_owner

모듈	sn_vul_qualys.관리자	sn_vulc.관리자	**sn_vulc.exception_approver**	**sn_vulc.manage_approval_rules**	**sn_vul**
(메인 앱 그룹)					

기계번역

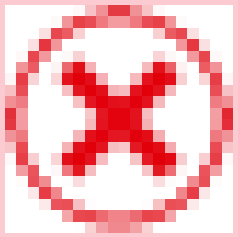
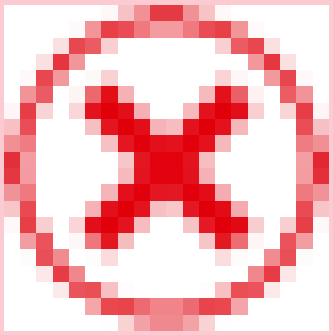
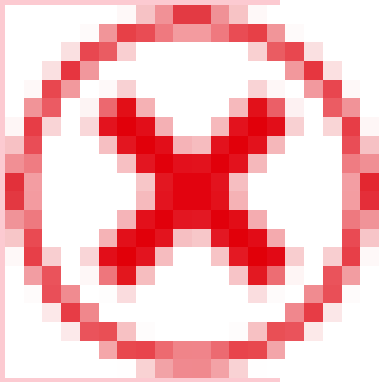
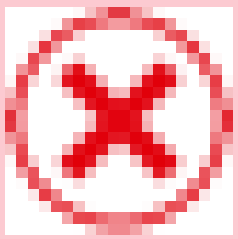
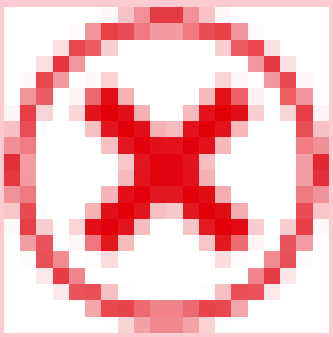
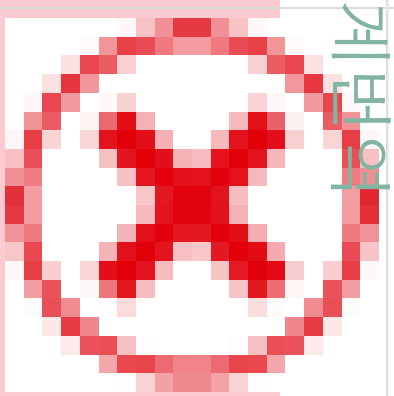
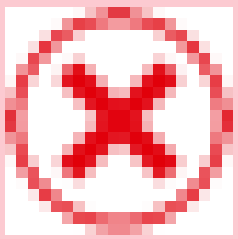
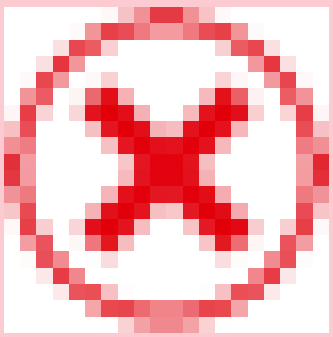
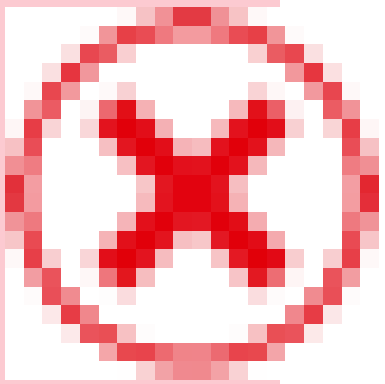
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule**

다른 역할에 대한 정보:

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

sn_vulc.remediation_owner

모듈	sn_vul_qualys.관리자	sn_vulc.관리자	sn_vulc.exception_approver	sn_vulc.manage_approval_rules	sn_vul
개요					
정책					
테스트					

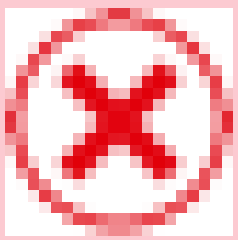
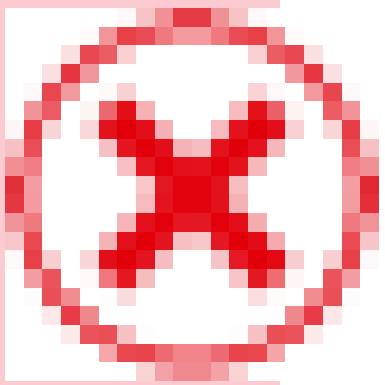
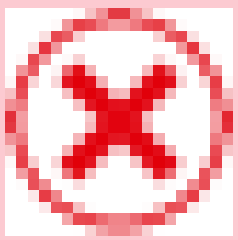
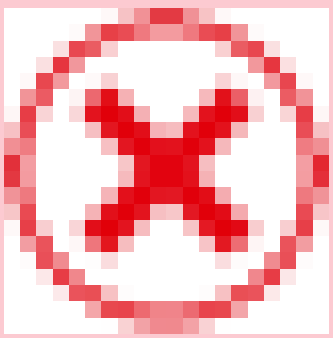
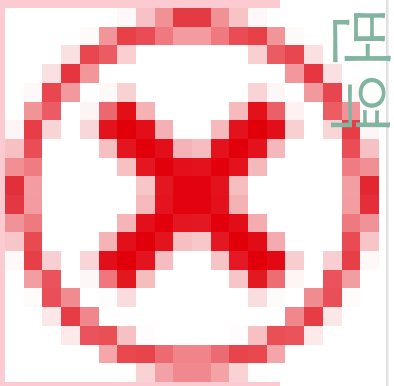
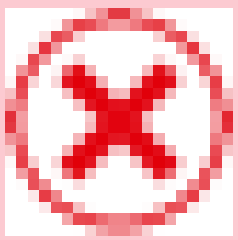
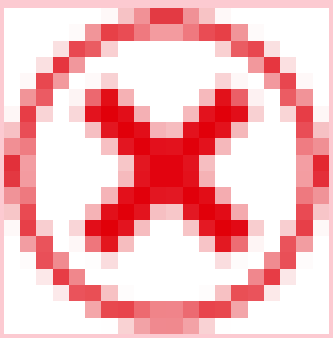
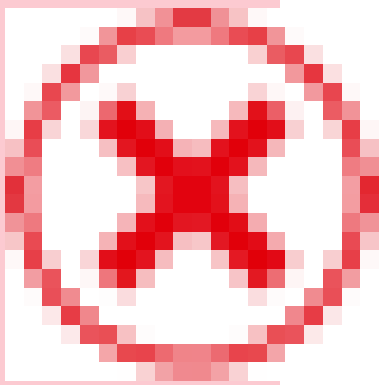
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule**

다른 역할에 대한 정보:

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

sn_vulc.remediation_owner

모듈	sn_vul_qualys.관리자	sn_vulc.관리자	sn_vulc.exception_approver	sn_vulc.manage_approval_rules	sn_vul
내 승인					
테스트 결과					
우선순위가 부여되지 않은 테스트 결과					
열린 사용자 테스트 결과					

기계번역

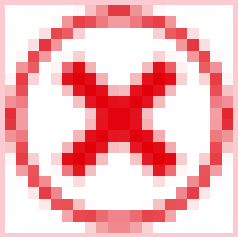
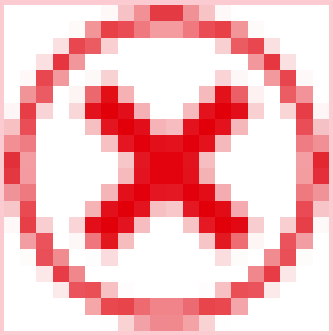
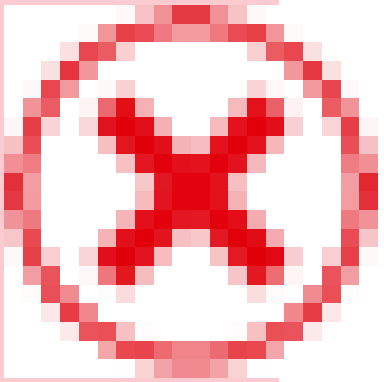
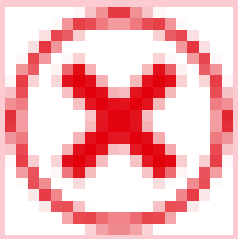
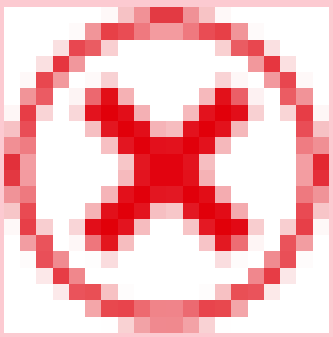
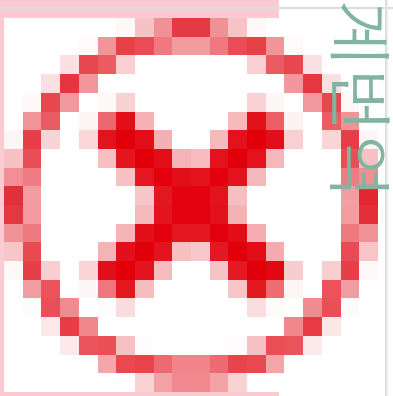
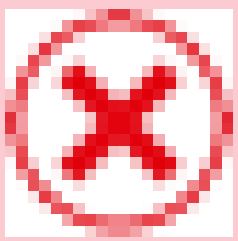
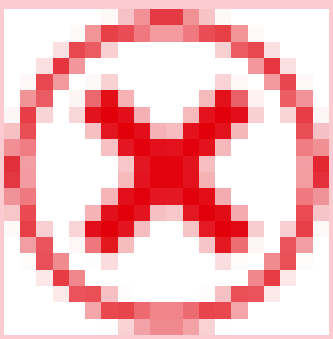
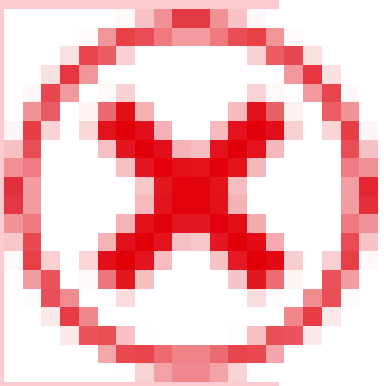
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule**

다른 역할에 대한 정보:

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

sn_vulc.remediation_owner

모듈	sn_vul_qualys.관리자	sn_vulc.관리자	sn_vulc.exception_approver	sn_vulc.manage_approval_rules	sn_vul
테스트 결과 오픈					
대상에 접근					
누락된 대상					

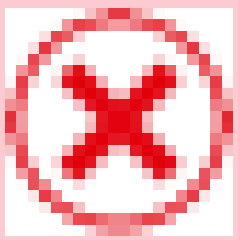
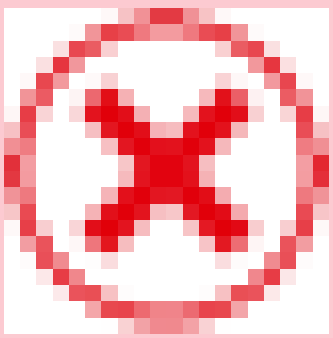
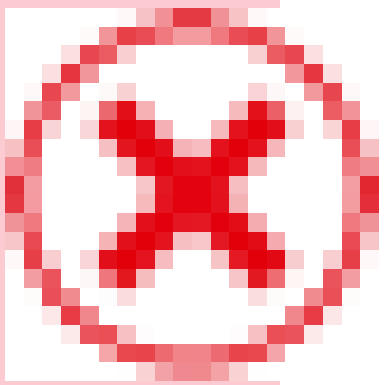
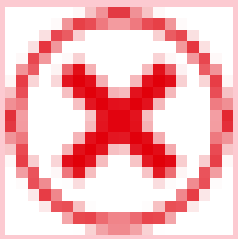
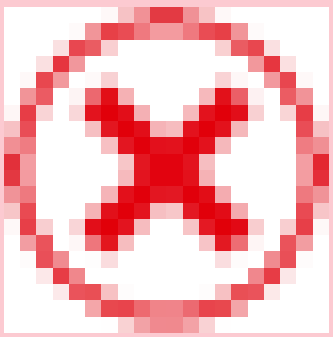
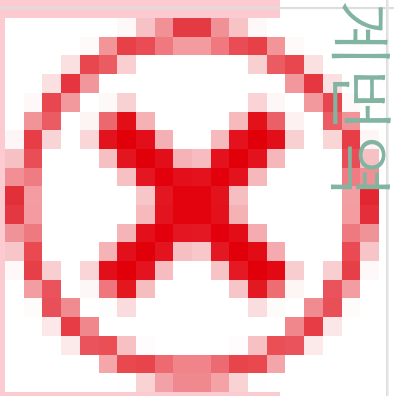
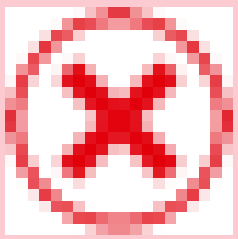
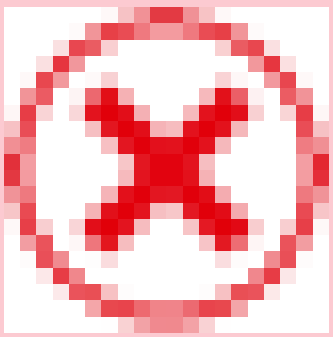
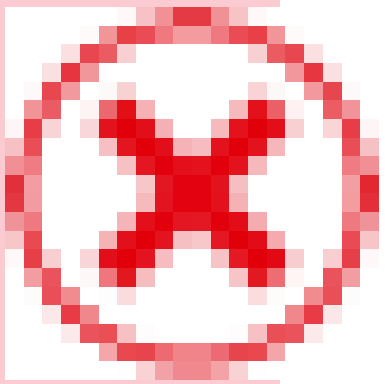
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule**

다른 역할에 대한 정보:

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

sn_vulc.remediation_owner

모듈	sn_vul_qualys.관리자	sn_vulc.관리자	sn_vulc.exception_approver	sn_vulc.manage_approval_rules	sn_vul
미할당					
여러 지연					
모두					

테스트 결과 그룹

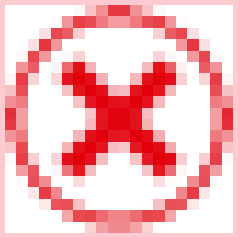
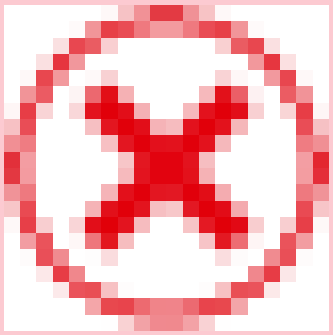
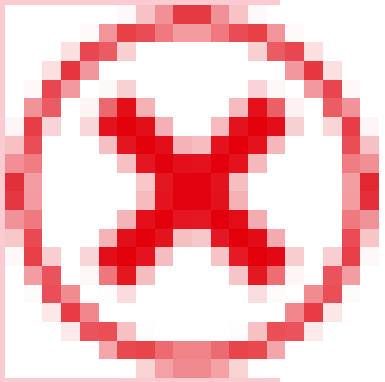
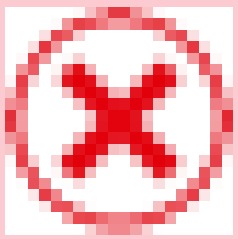
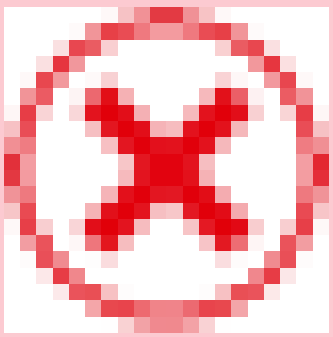
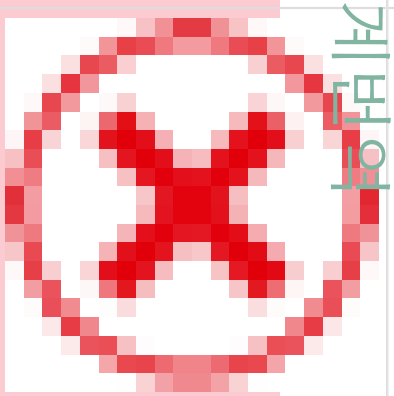
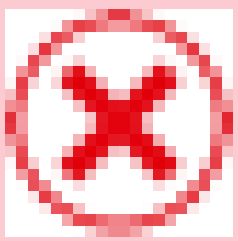
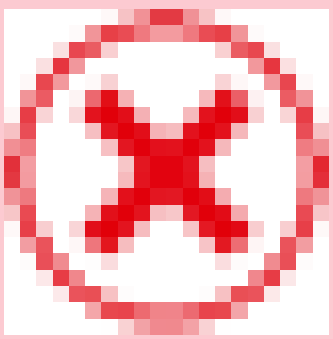
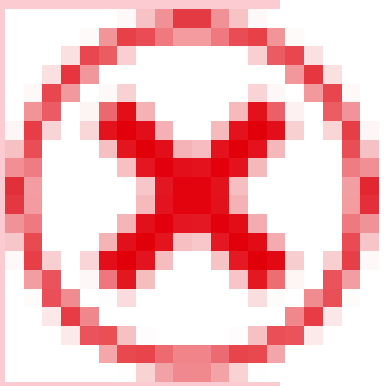
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule**

다른 역할에 대한 정보:

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

sn_vulc.remediation_owner

모듈	sn_vul_qualys.관리자	sn_vulc.관리자	sn_vulc.exception_approver	sn_vulc.manage_approval_rules	sn_vul
내 오픈 그룹					
모든 오픈 그룹					
여러 지연					

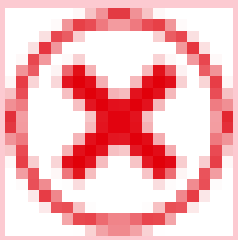
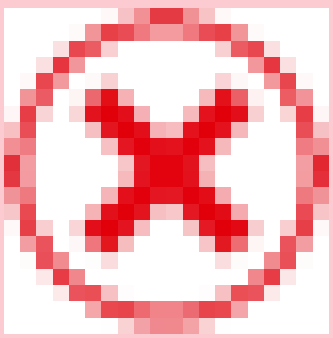
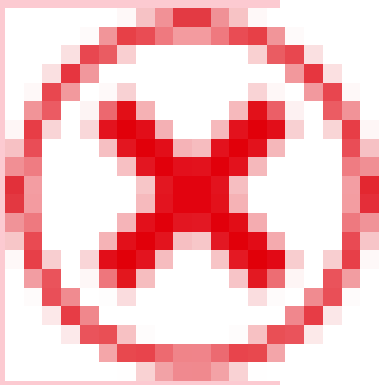
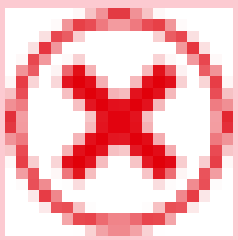
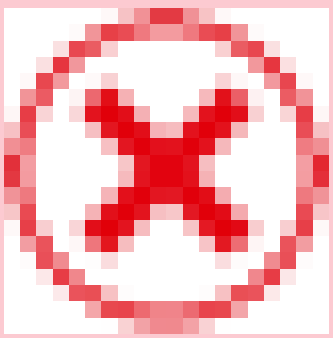
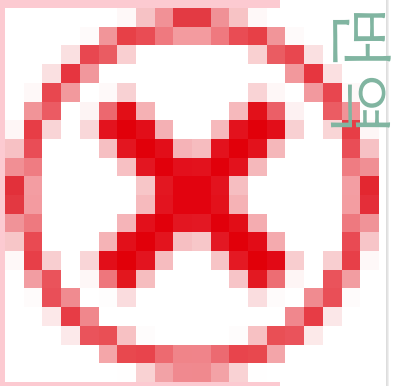
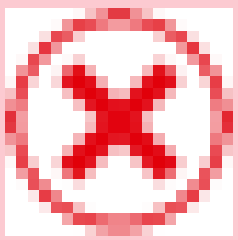
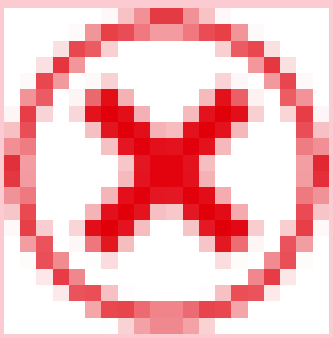
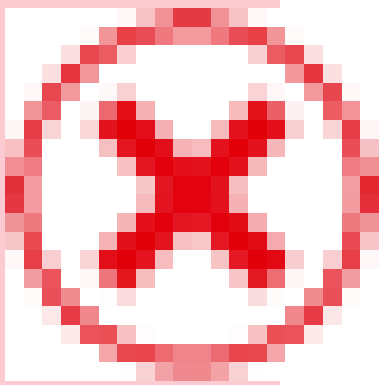
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule**

다른 역할에 대한 정보:

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

sn_vulc.remediation_owner

모듈	sn_vul_qualys.관리자	sn_vulc.관리자	sn_vulc.exception_approver	sn_vulc.manage_approval_rules	sn_vul
모든 그룹					
지원 데이터					
권한이 부여된 소스					
기술					

기계번역

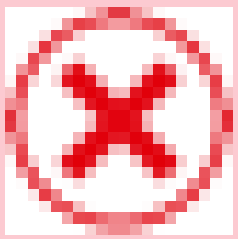
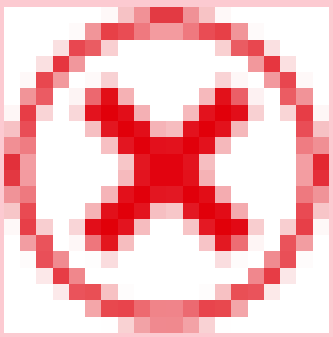
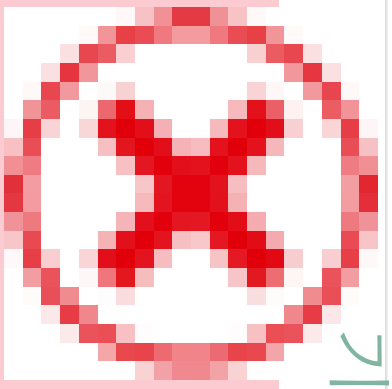
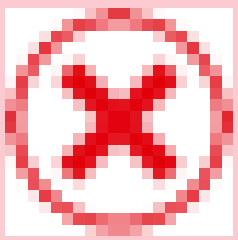
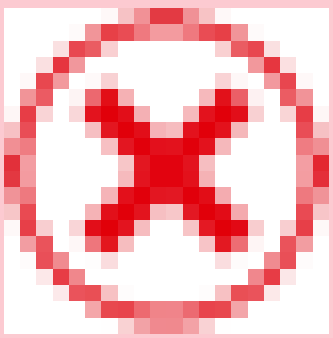
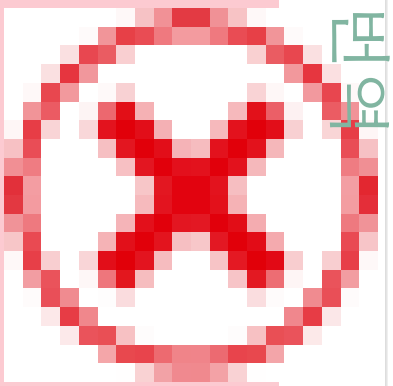
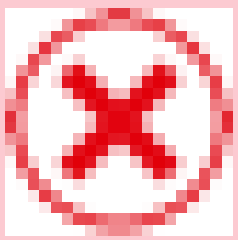
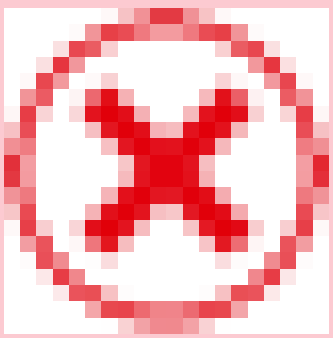
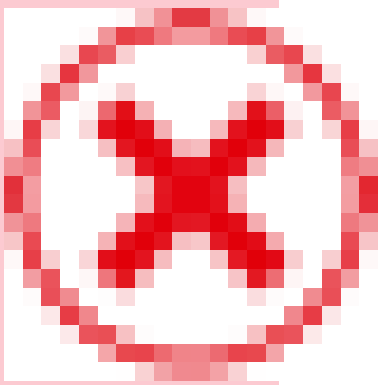
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule**

다른 역할에 대한 정보:

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

sn_vulc.remediation_owner

모듈	sn_vul_qualys.관리자	sn_vulc.관리자	sn_vulc.exception_approver	sn_vulc.manage_approval_rules	sn_vul
관리					
담당 규칙					
부실 테스트 결과 자동 닫기					
그룹 규칙					

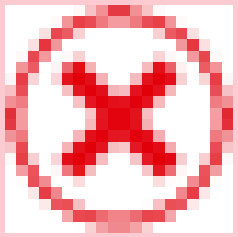
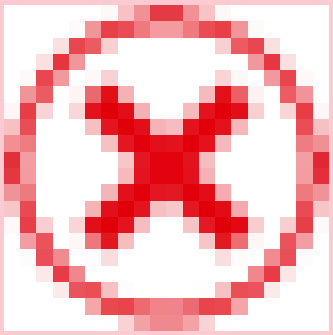
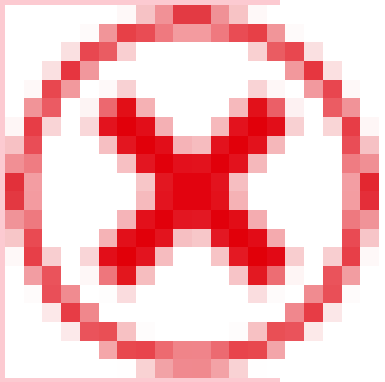
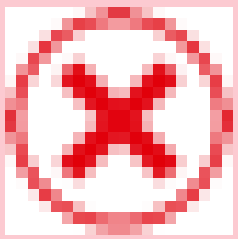
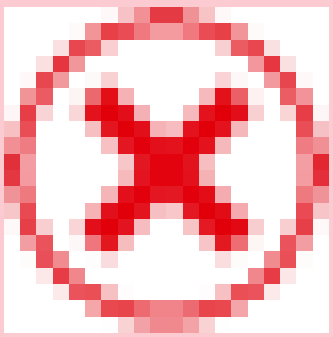
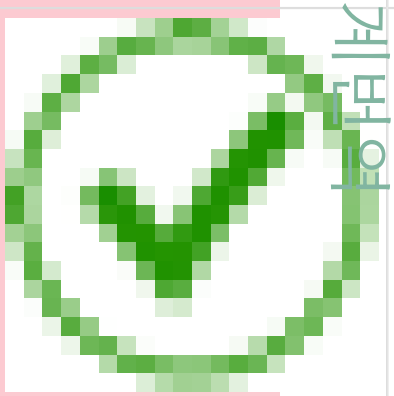
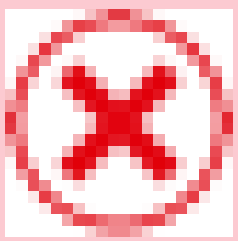
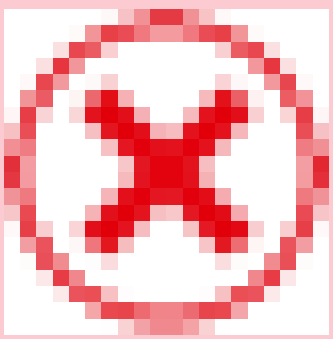
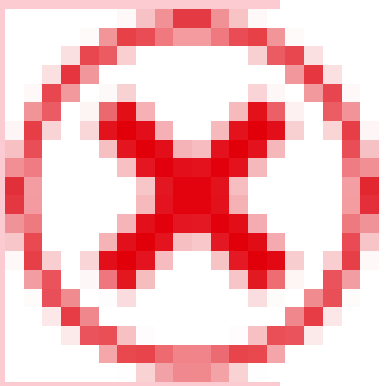
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule**

다른 역할에 대한 정보:

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

sn_vulc.remediation_owner

모듈	sn_vul_qualys.관리자	sn_vulc.관리자	sn_vulc.exception_approver	sn_vulc.manage_approval_rules	sn_vul
자동 예외 규칙					
승인 규칙					
위험 계산기					

기계 번역

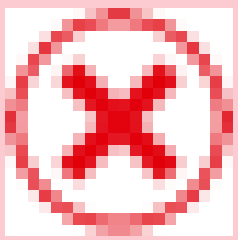
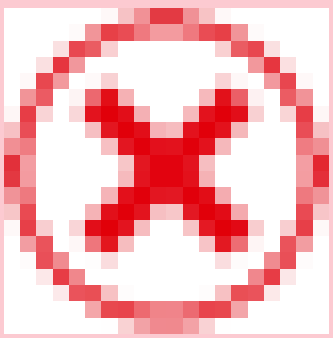
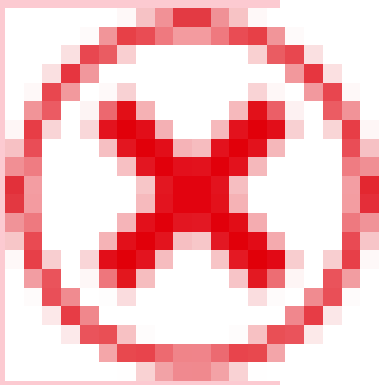
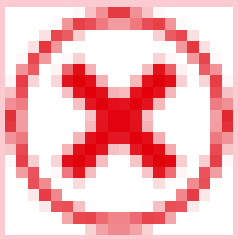
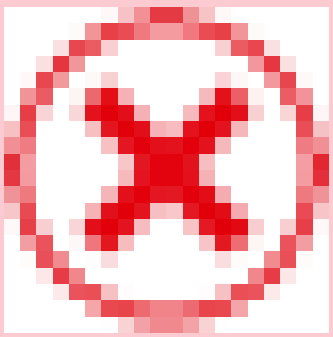
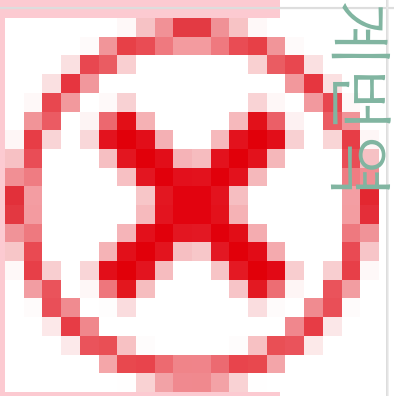
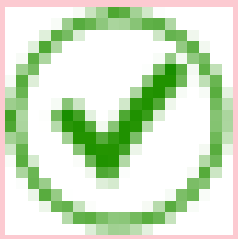
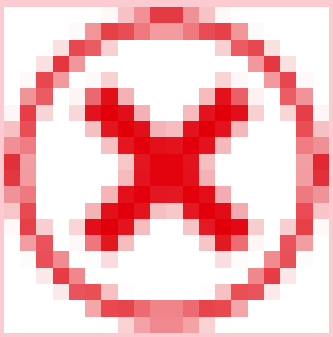
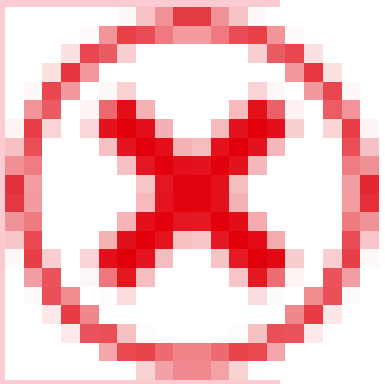
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule**

다른 역할에 대한 정보:

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

sn_vulc.remediation_owner

모듈	sn_vul_qualys.관리자	sn_vulc.관리자	sn_vulc.exception_approver	sn_vulc.manage_approval_rules	sn_vul
위험 점수 롤업 계산기					
정정 대상 규칙					
중요도 매핑					

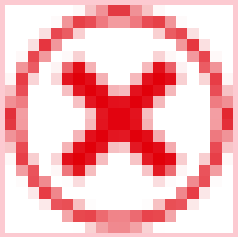
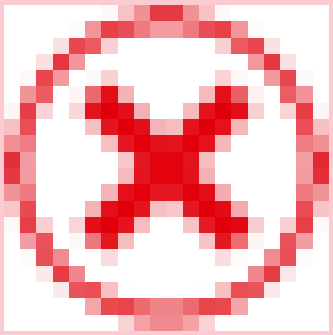
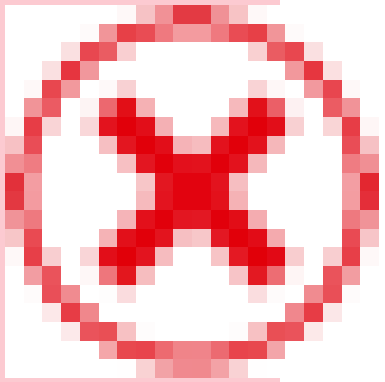
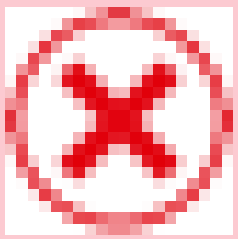
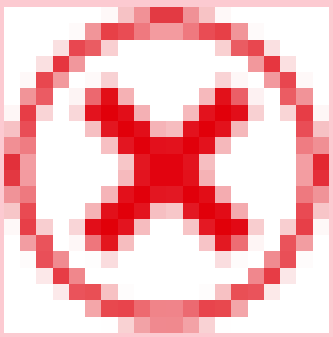
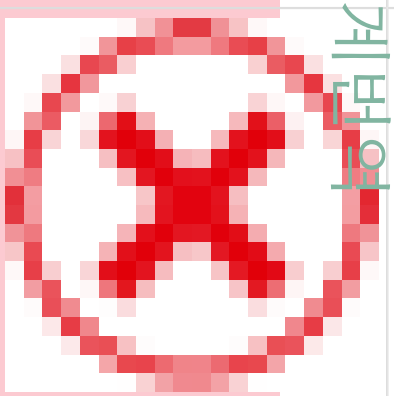
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule**

다른 역할에 대한 정보:

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

sn_vulc.remediation_owner

모듈	sn_vul_qualys.관리자	sn_vulc.관리자	**sn_vulc.exception_approver**	**sn_vulc.manage_approval_rules**	**sn_vul**
알림					
예외 관리					

기계 번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

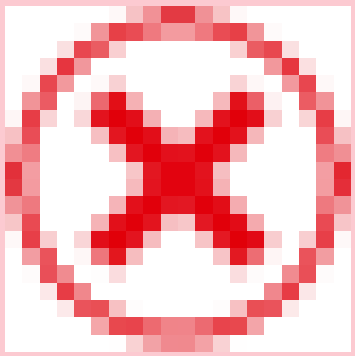
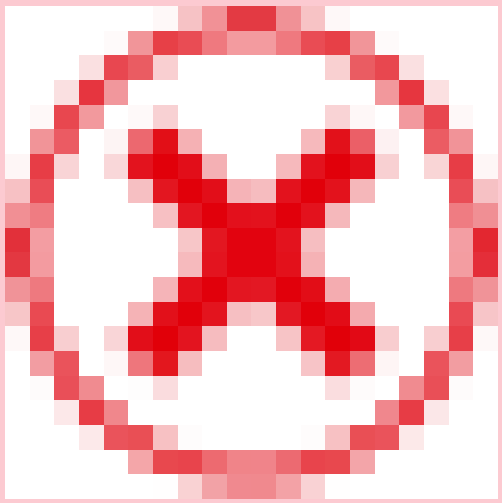
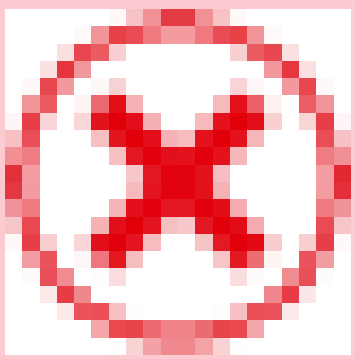
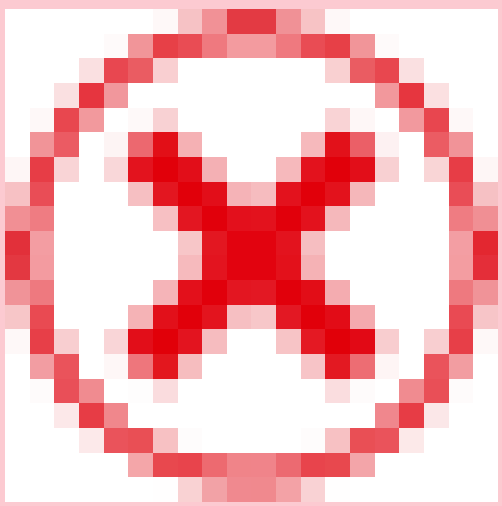
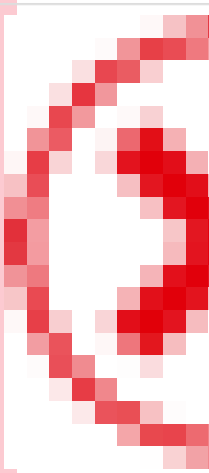
다음에 대한 모듈 액세스: **sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules**

다음에 대한 모듈 액세스: **sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules**

다른 역할에 대한 정보:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

모듈	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc. 읽다	sn_vulc.read_rem
(메인 앱 그룹)				
개요				
정책				

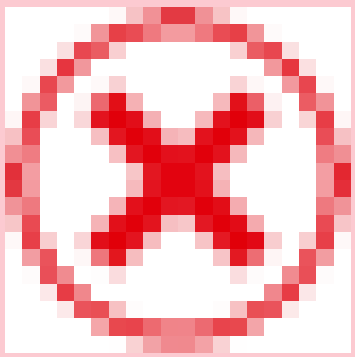
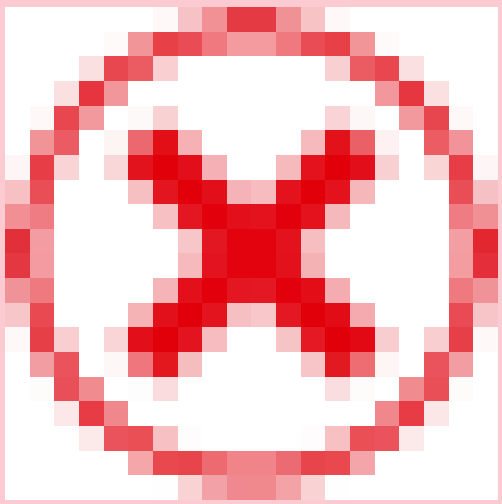
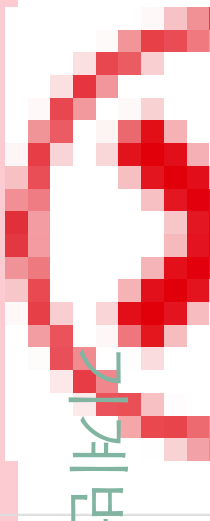
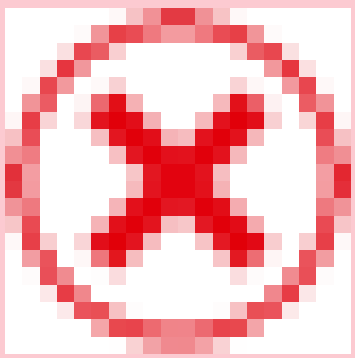
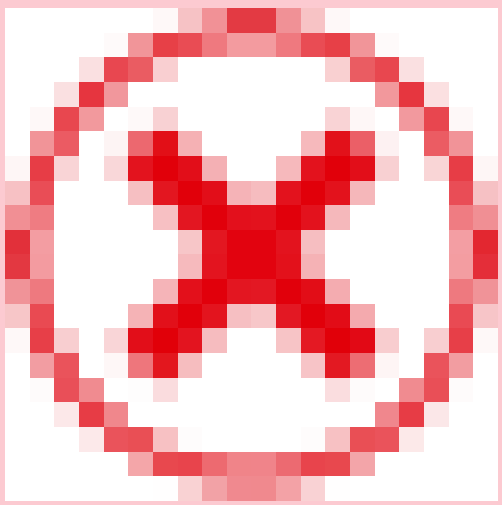
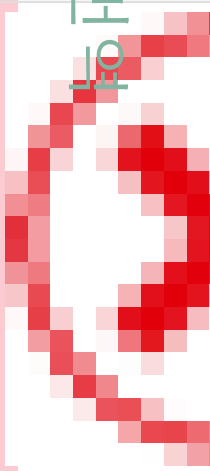
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules**

다른 역할에 대한 정보:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

모듈	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.읽다	sn_vulc.read_rem
테스트				
내 승인				
테스트 결과				

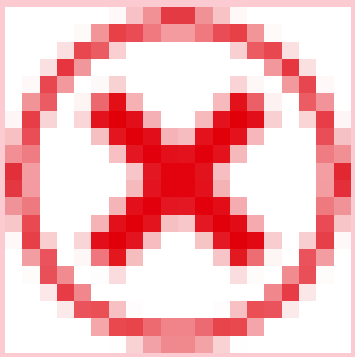
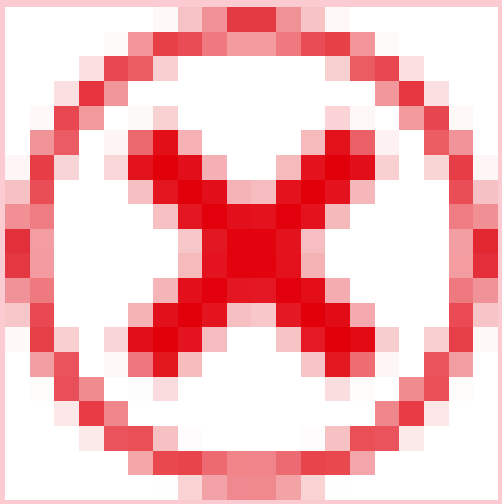
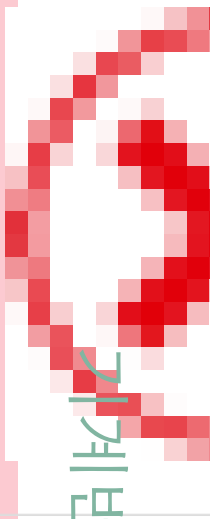
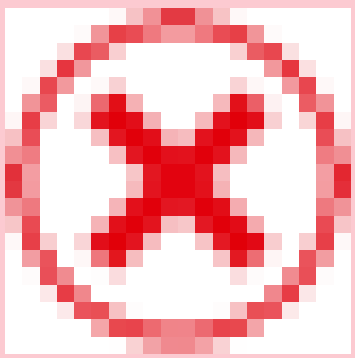
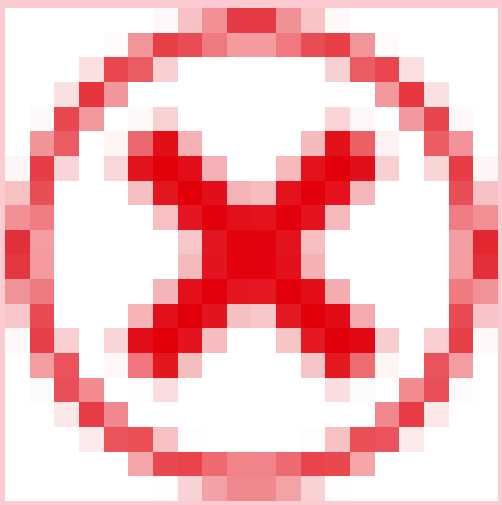
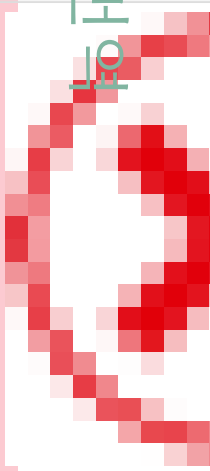
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules**

다른 역할에 대한 정보:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

모듈	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.읽다	sn_vulc.read_rem
우선순위가 부여되지 않은 테스트 결과				
열린 사용자 테스트 결과				

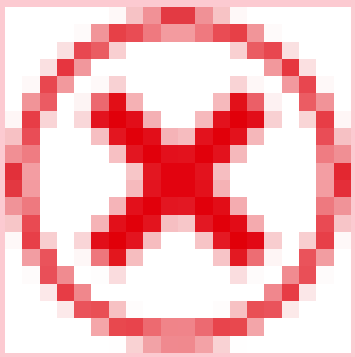
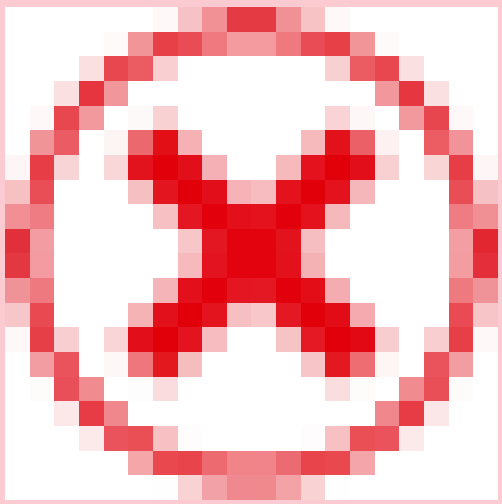
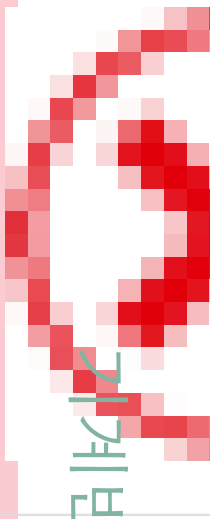
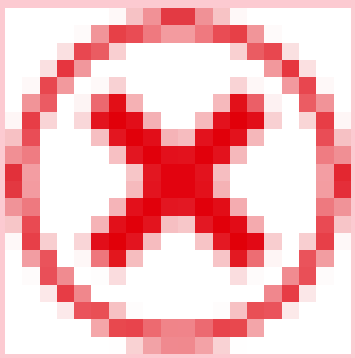
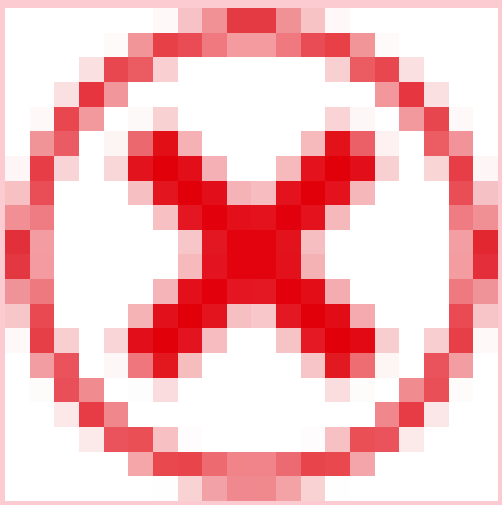
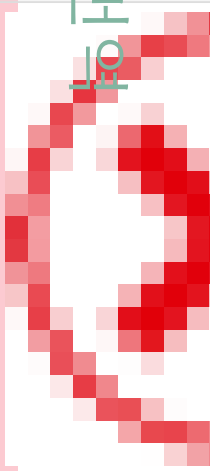
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules**

다른 역할에 대한 정보:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

모듈	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc. 읽다	sn_vulc.read_rem
테스트 결과 오픈				
대상에 접근				

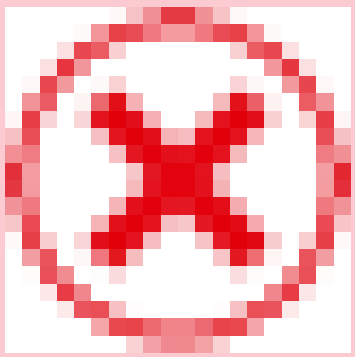
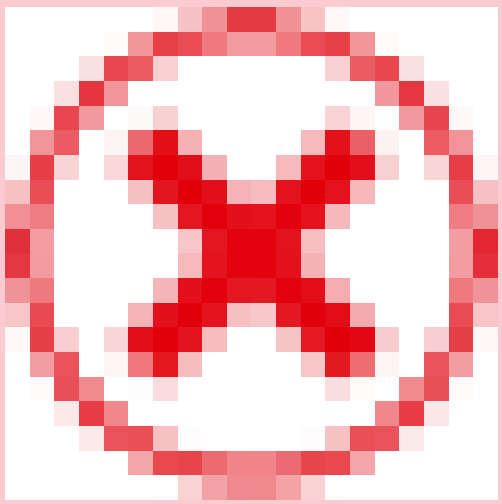
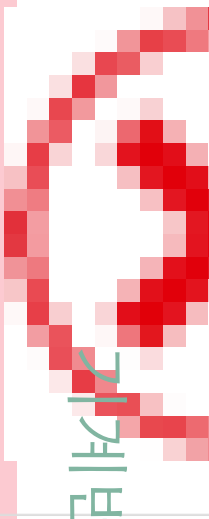
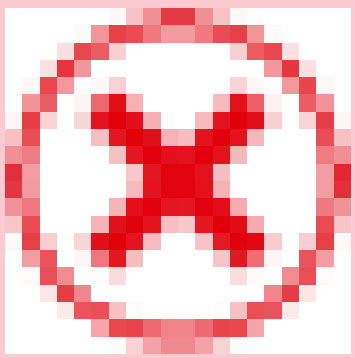
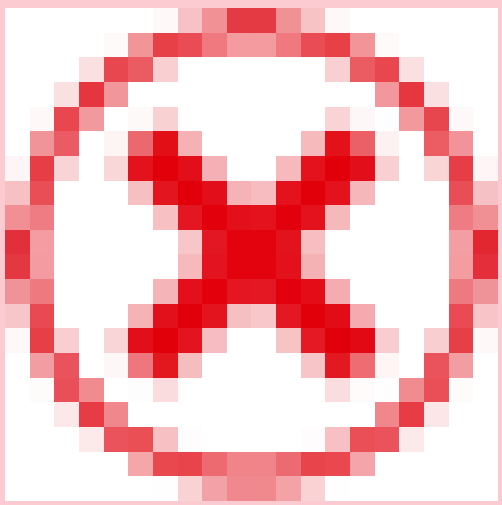
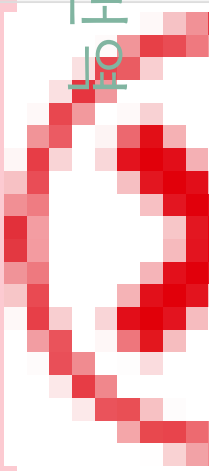
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules**

다른 역할에 대한 정보:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

모듈	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc. 읽다	sn_vulc.read_rem
누락된 대상				
미할당				

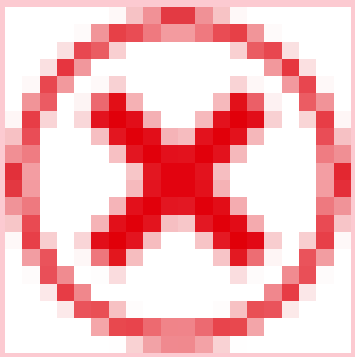
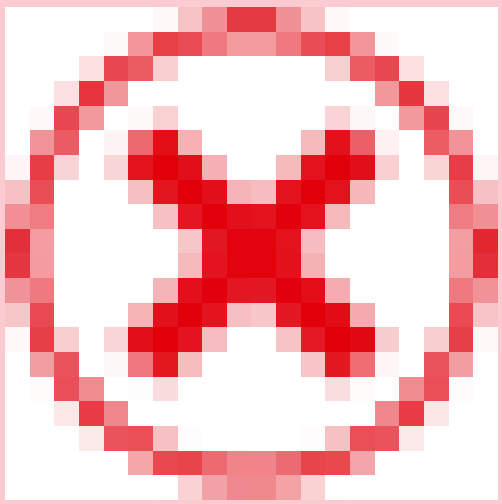
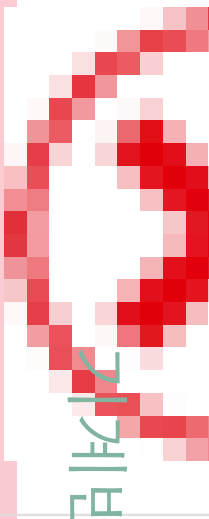
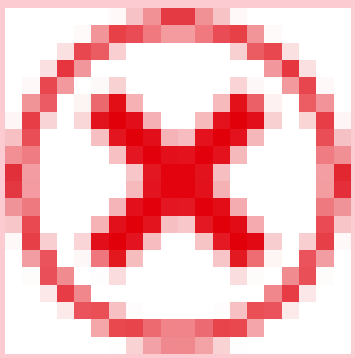
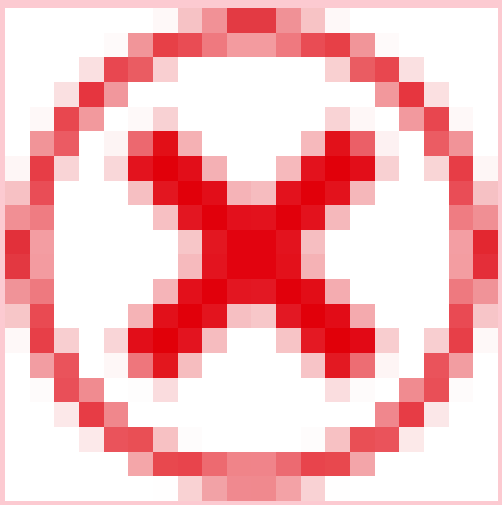
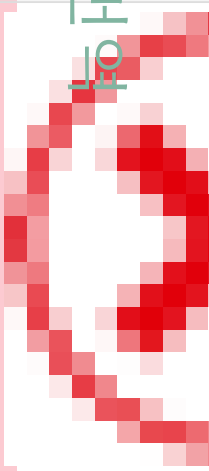
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules**

다른 역할에 대한 정보:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

모듈	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc. 읽다	sn_vulc.read_rem
여러 지연				
모두				
테스트 결과 그룹				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules**

다른 역할에 대한 정보:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

모듈	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.읽다	sn_vulc.read_rem
내 오픈 그룹	✗	✗	✓	✗
모든 오픈 그룹	✗	✗	✓	✗

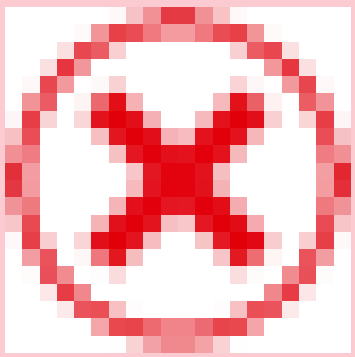
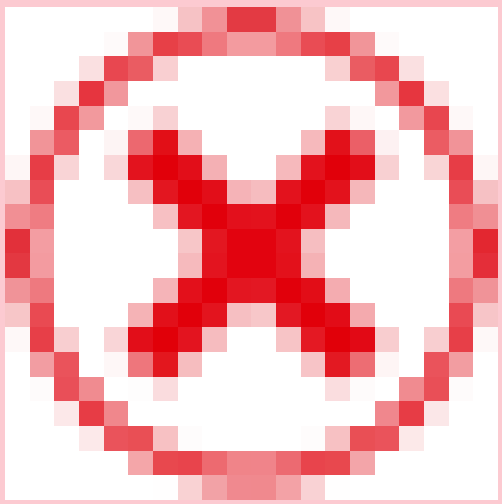
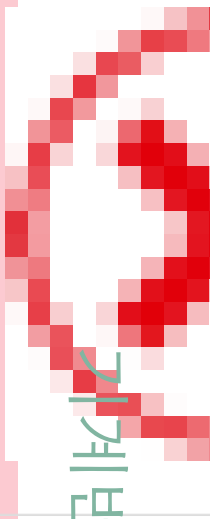
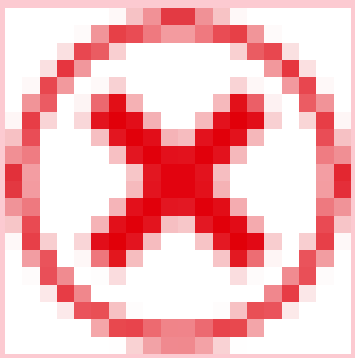
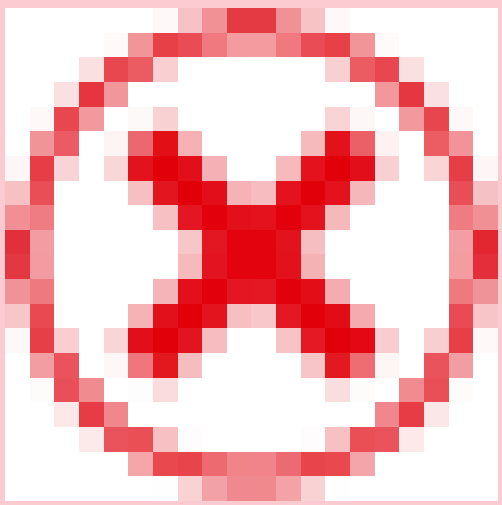
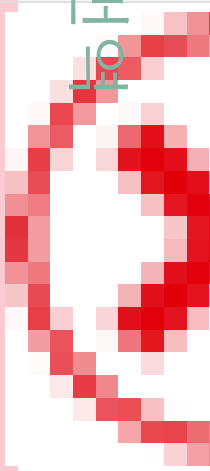
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules**

다른 역할에 대한 정보:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

모듈	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.읽다	sn_vulc.read_rem
여러 지연				
모든 그룹				
지원 데이터				

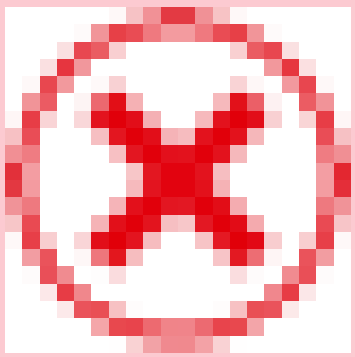
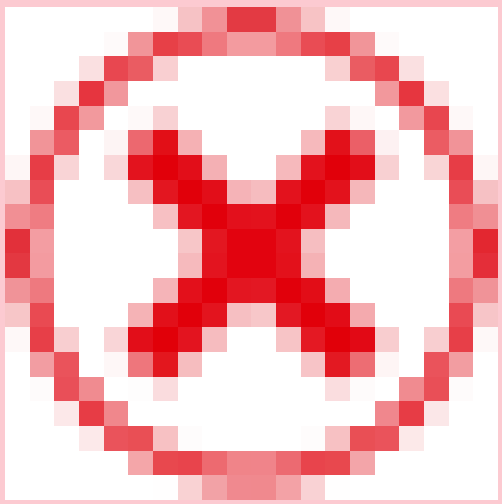
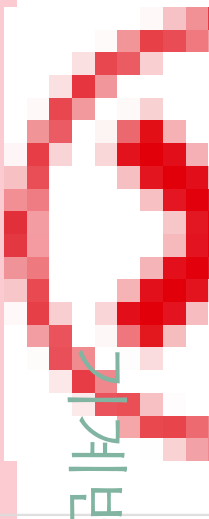
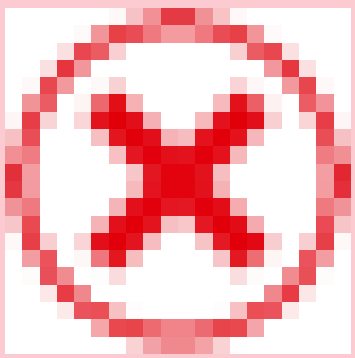
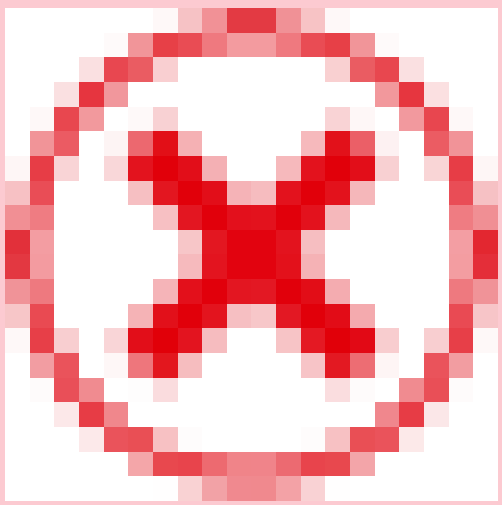
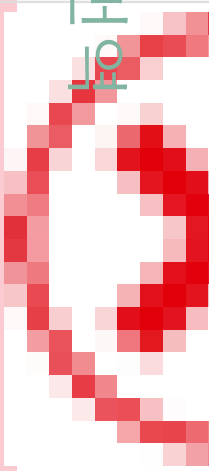
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules**

다른 역할에 대한 정보:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

모듈	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.읽다	sn_vulc.read_rem
권한이 부여된 소스				
기술				
관리				

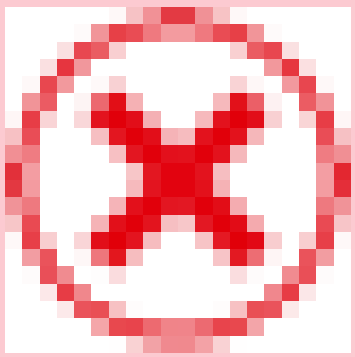
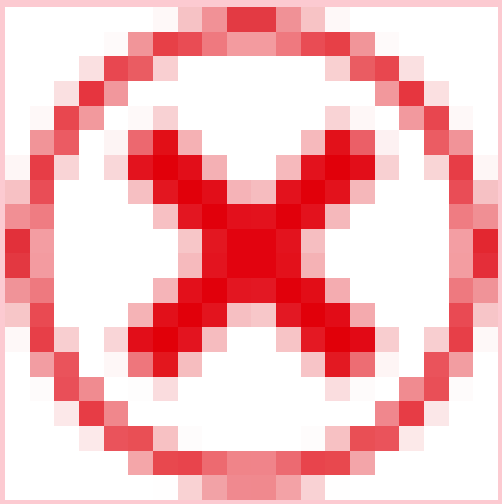
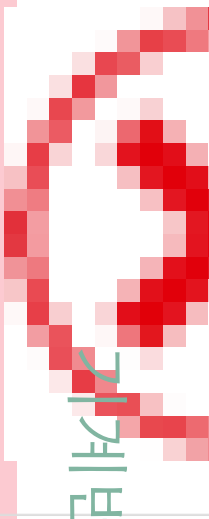
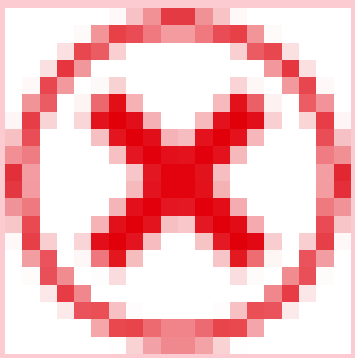
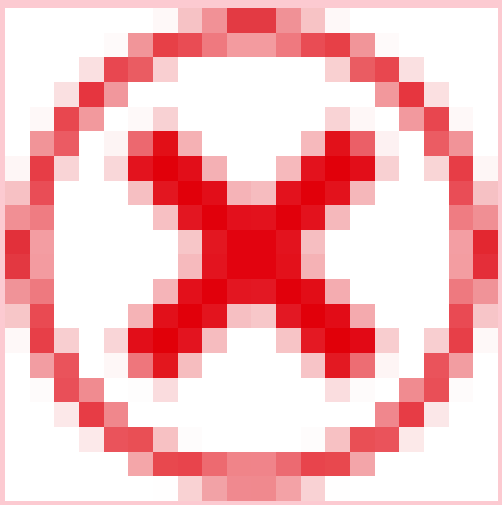
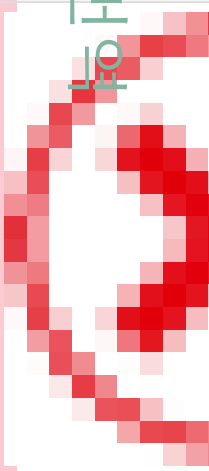
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules**

다른 역할에 대한 정보:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

모듈	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc. 읽다	sn_vulc.read_rem
담당 규칙				
부실 테스트 결과 자동 닫기				

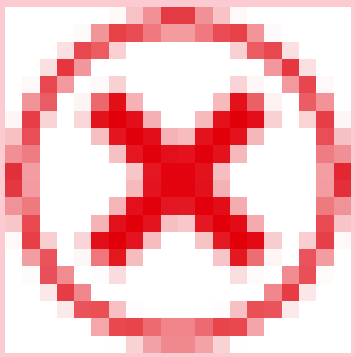
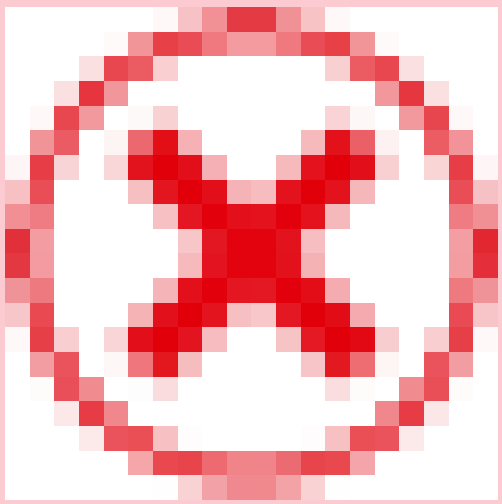
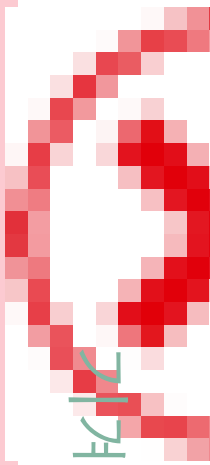
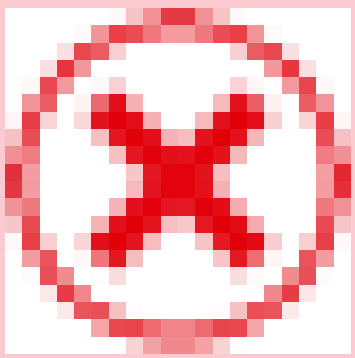
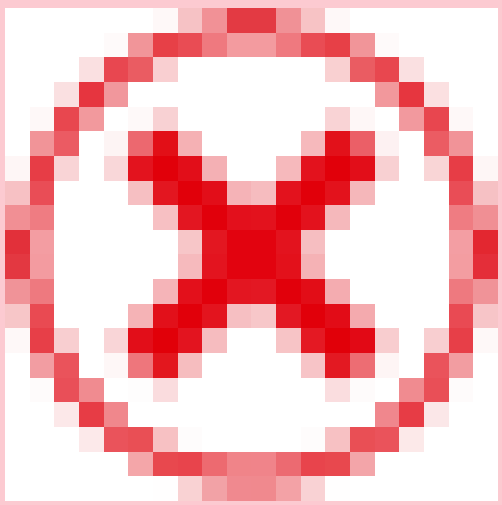
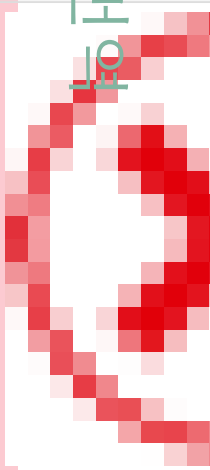
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules**

다른 역할에 대한 정보:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

모듈	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.읽다	sn_vulc.read_rem
그룹 규칙				
자동 예외 규칙				

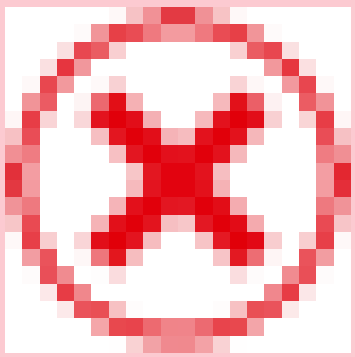
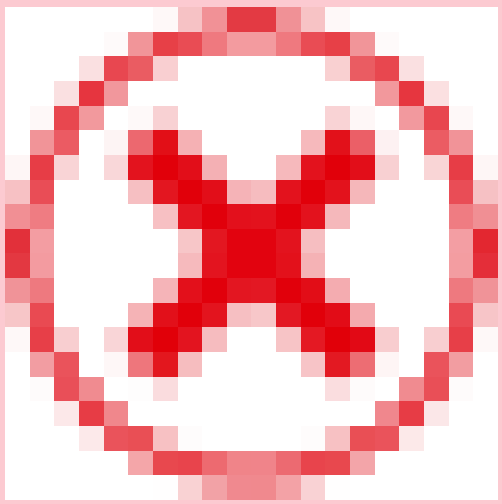
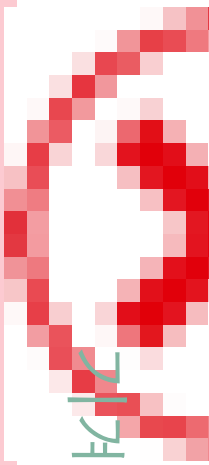
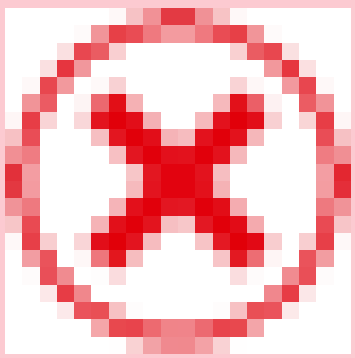
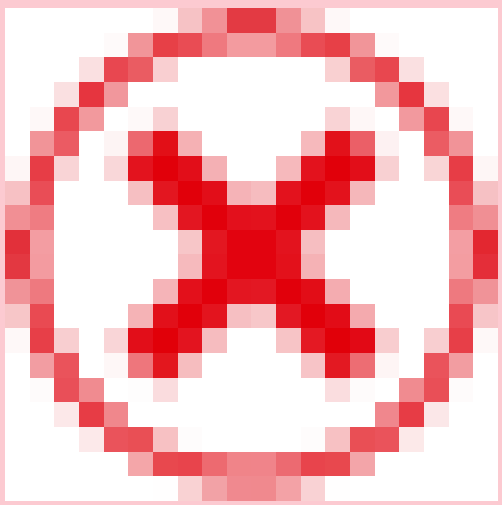
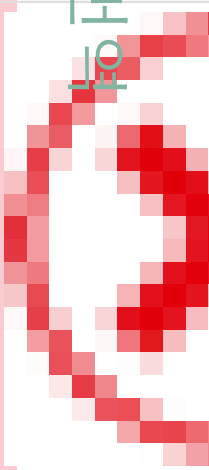
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules**

다른 역할에 대한 정보:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

모듈	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.읽다	sn_vulc.read_rem
승인 규칙				
위험 계산기				

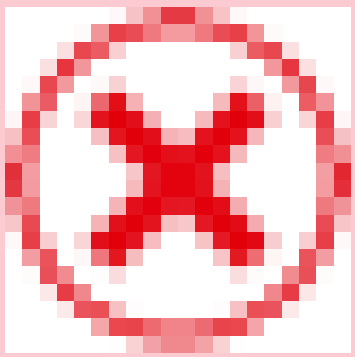
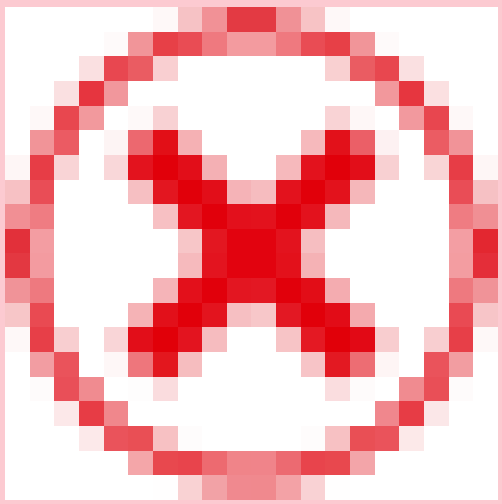
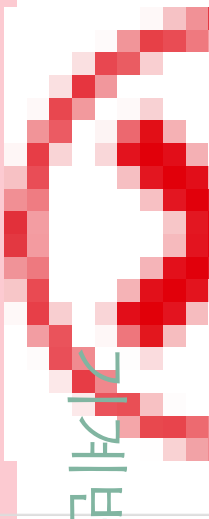
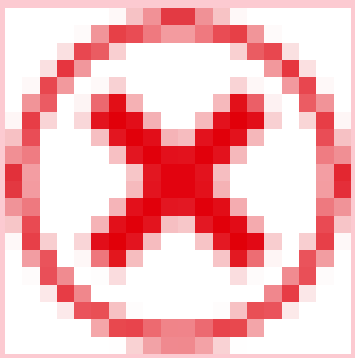
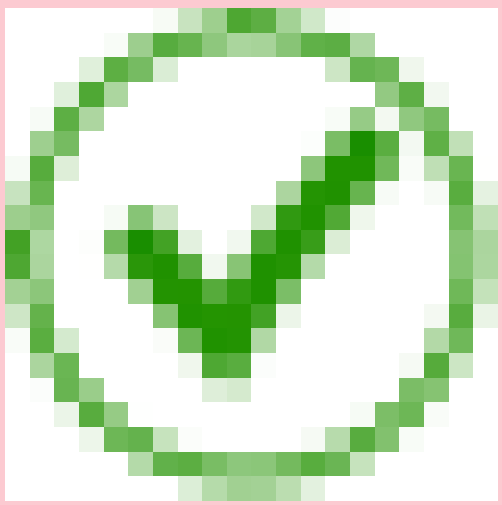
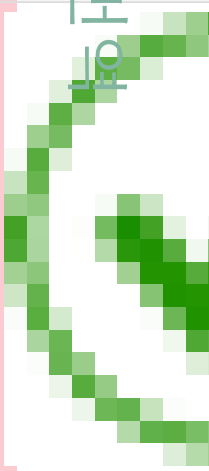
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules**

다른 역할에 대한 정보:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

모듈	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc. 읽다	sn_vulc.read_rem
위험 점수 롤업 계산기				
정정 대상 규칙				

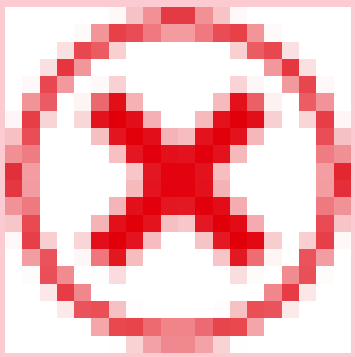
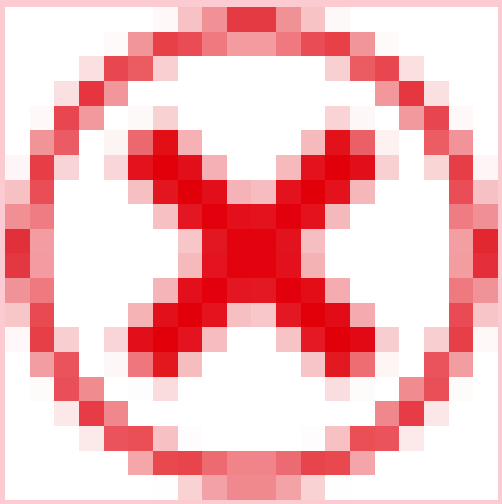
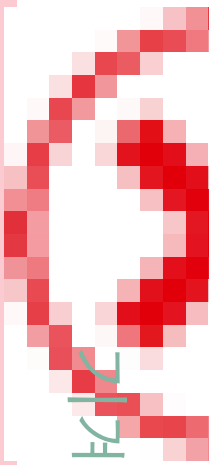
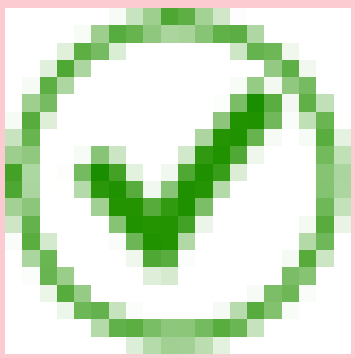
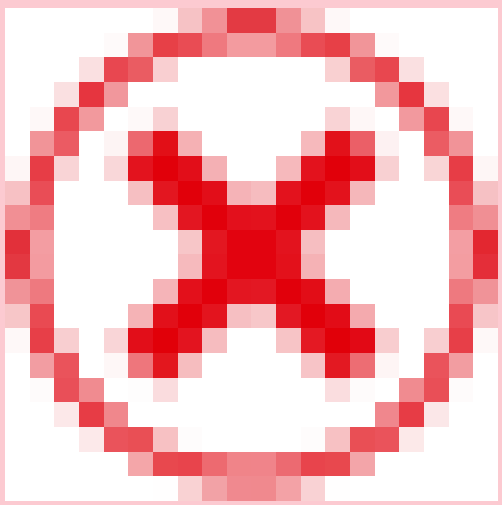
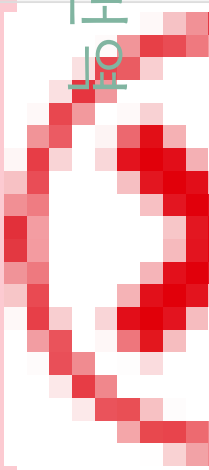
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules**

다른 역할에 대한 정보:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

모듈	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.읽다	sn_vulc.read_rem
중요도 매핑				
알림				

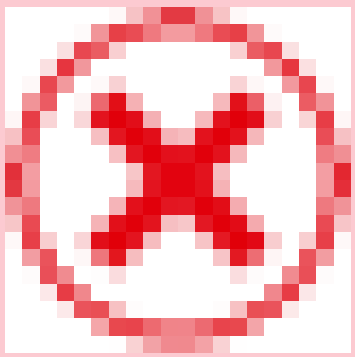
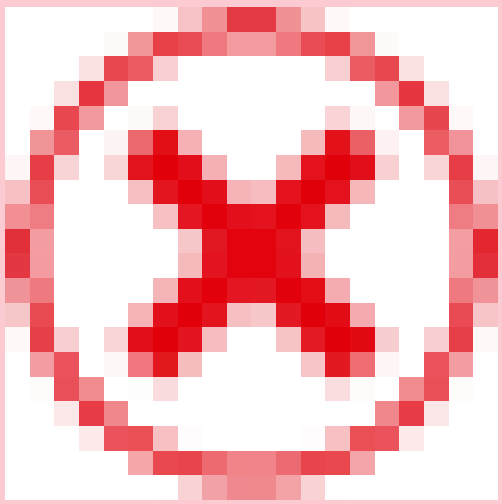
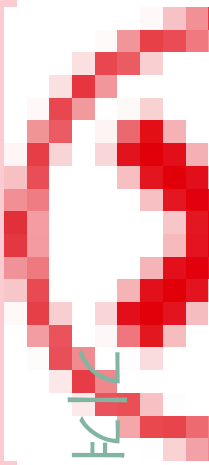
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules**

다른 역할에 대한 정보:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

모듈	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.읽다	sn_vulc.read_rem
예외 관리				

다음에 대한 모듈 액세스: **sn_vulc.remediation_owner**

다음에 대한 모듈 액세스: **sn_vulc.remediation_owner**

다른 역할에 대한 정보:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

모듈	sn_vulc.remediation_owner
(메인 앱 그룹)	

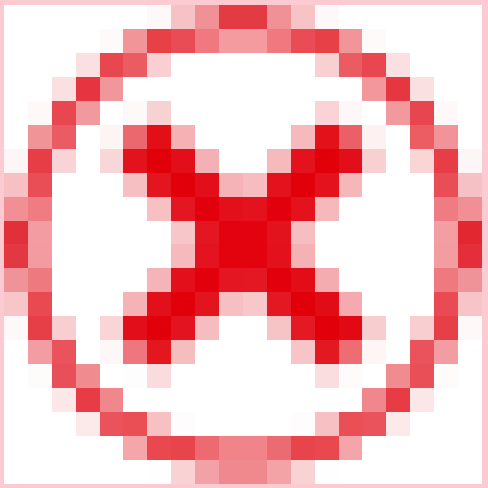
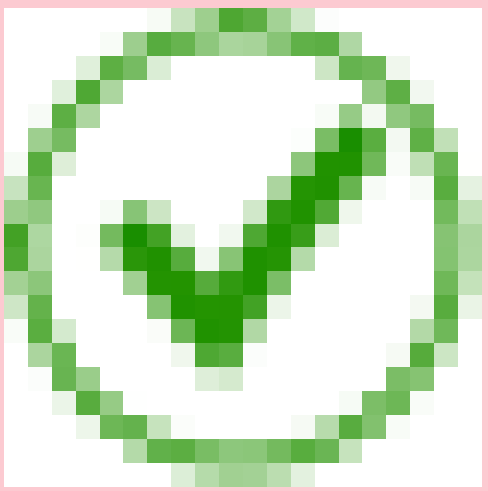
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vulc.remediation_owner**

다른 역할에 대한 정보:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

모듈	sn_vulc.remediation_owner
개요	
정책	

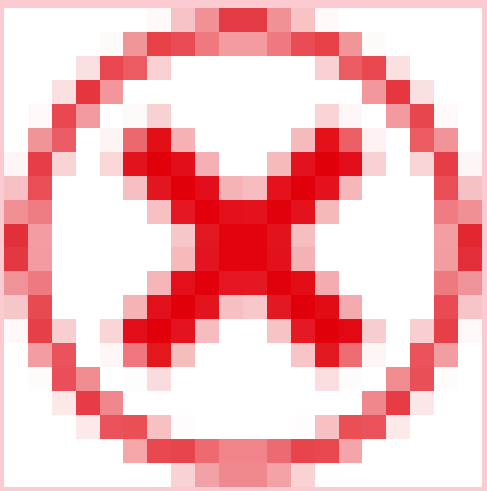
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vulc.remediation_owner**

다른 역할에 대한 정보:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

모듈	sn_vulc.remediation_owner
테스트	
내 승인	
테스트 결과	

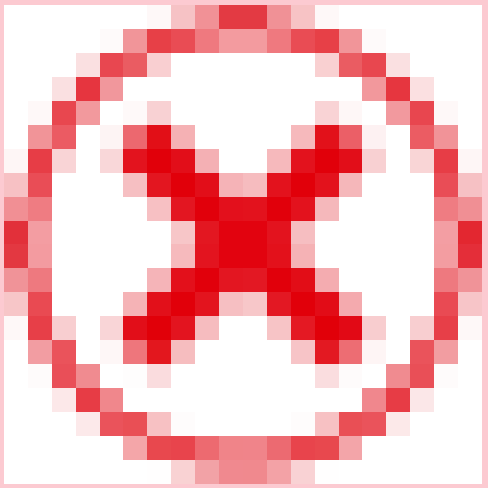
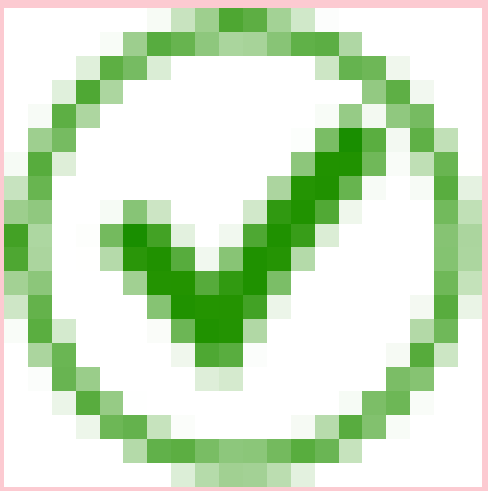
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vulc.remediation_owner**

다른 역할에 대한 정보:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

모듈	sn_vulc.remediation_owner
우선순위가 부여되지 않은 테스트 결과	
열린 사용자 테스트 결과	

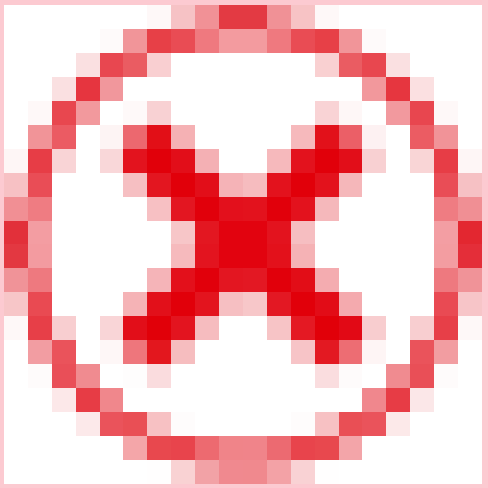
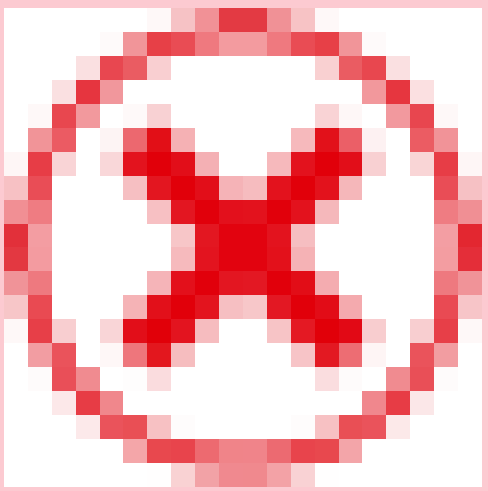
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vulc.remediation_owner**

다른 역할에 대한 정보:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

모듈	sn_vulc.remediation_owner
테스트 결과 오픈	
대상에 접근 중	

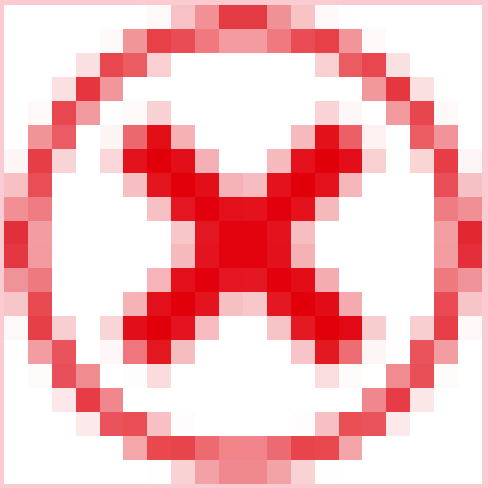
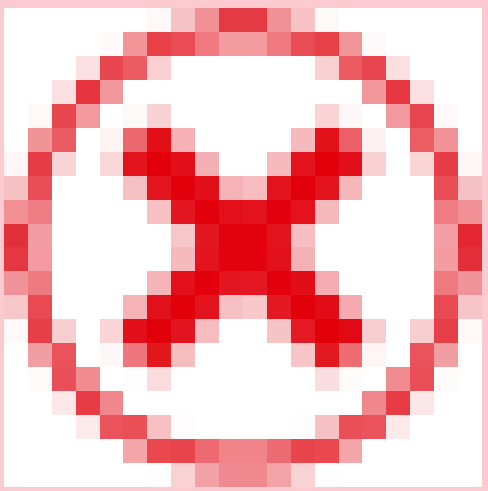
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vulc.remediation_owner**

다른 역할에 대한 정보:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

모듈	sn_vulc.remediation_owner
누락된 대상	
미할당	

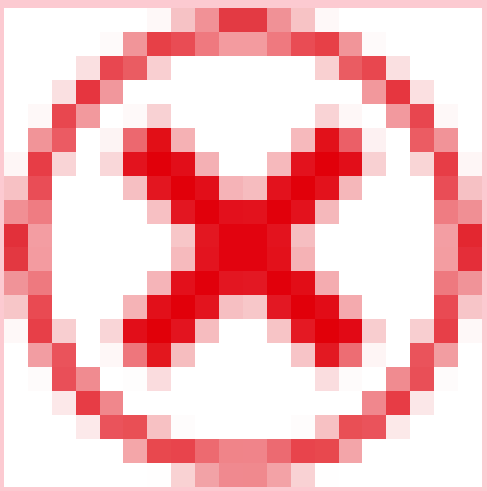
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vulc.remediation_owner**

다른 역할에 대한 정보:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

모듈	sn_vulc.remediation_owner
여러 지연	
모두	
테스트 결과 그룹	

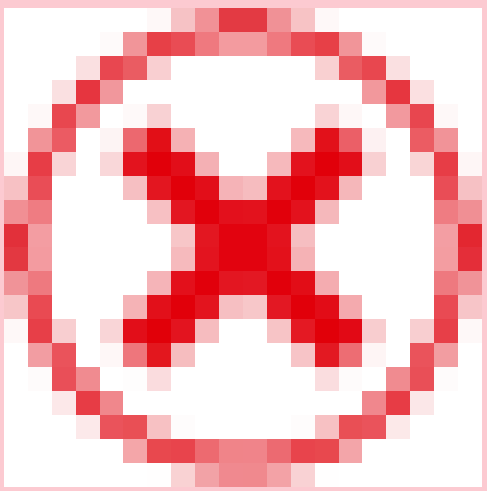
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vulc.remediation_owner**

다른 역할에 대한 정보:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

모듈	sn_vulc.remediation_owner
내 오픈 그룹	
모든 오픈 그룹	

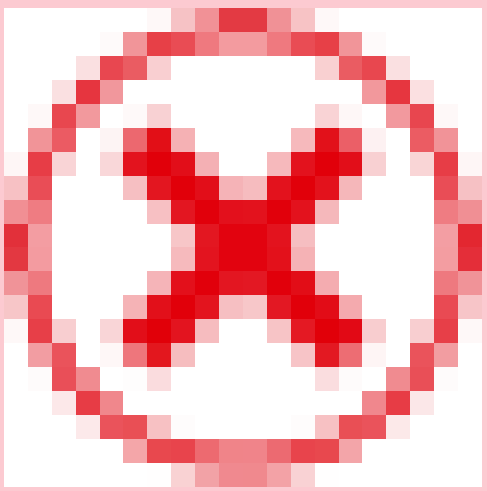
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vulc.remediation_owner**

다른 역할에 대한 정보:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

모듈	sn_vulc.remediation_owner
여러 지연	
모든 그룹	
지원 데이터	

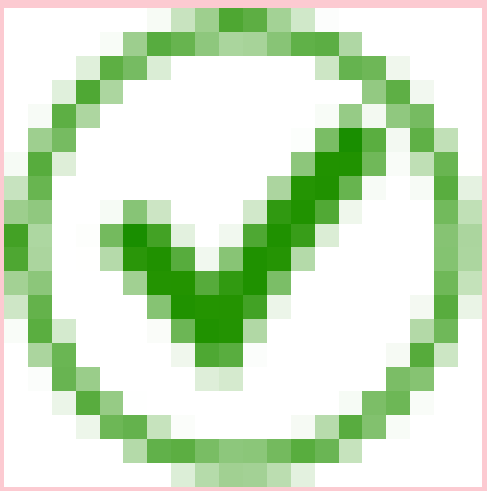
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vulc.remediation_owner**

다른 역할에 대한 정보:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

모듈	sn_vulc.remediation_owner
권한이 부여된 소스	
기술	
관리	

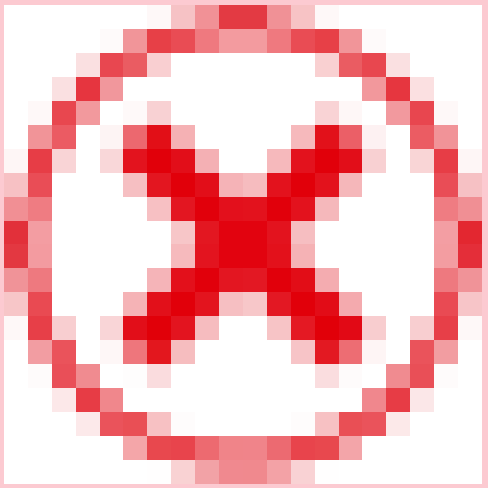
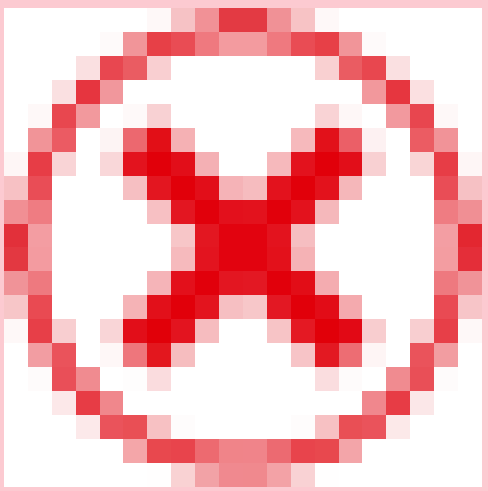
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vulc.remediation_owner**

다른 역할에 대한 정보:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

모듈	sn_vulc.remediation_owner
담당 규칙	
부실 테스트 결과 자동 닫기	

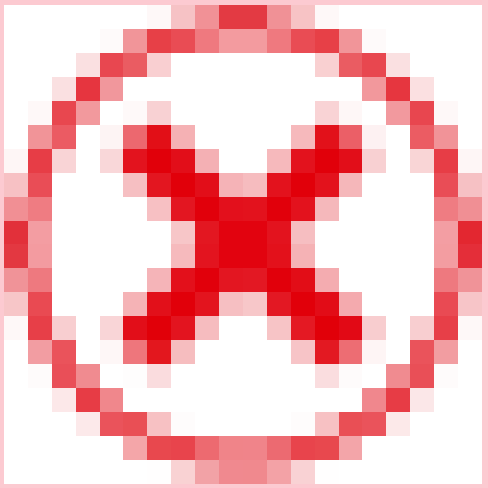
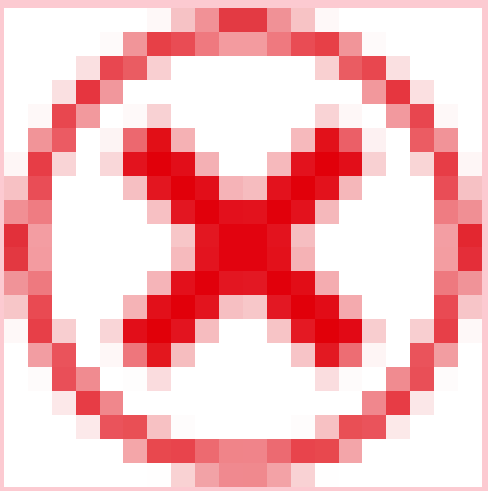
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vulc.remediation_owner**

다른 역할에 대한 정보:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

모듈	sn_vulc.remediation_owner
그룹 규칙	
자동 예외 규칙	

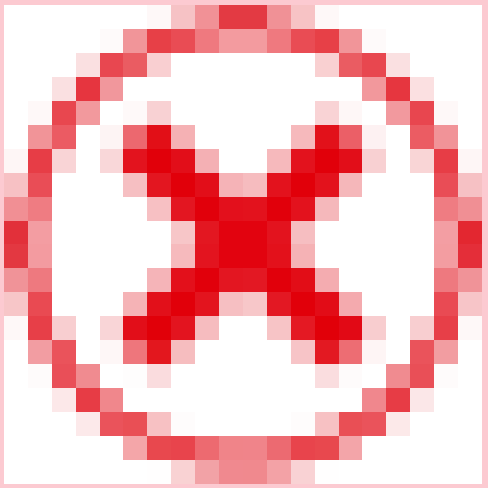
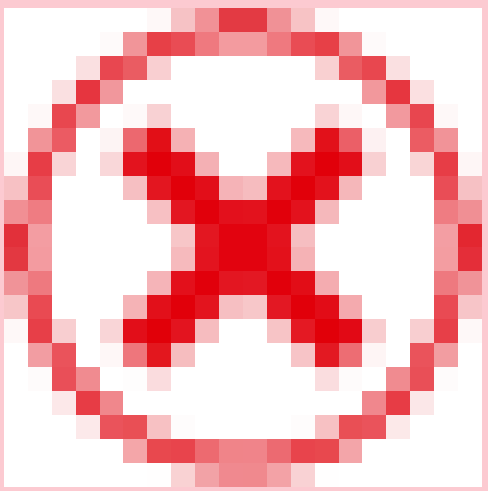
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vulc.remediation_owner**

다른 역할에 대한 정보:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

모듈	sn_vulc.remediation_owner
승인 규칙	
위험 계산기	

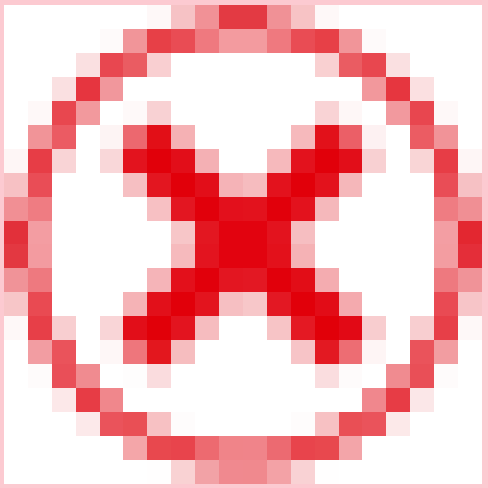
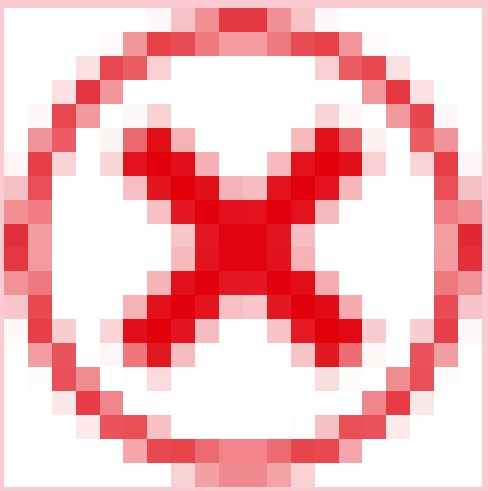
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vulc.remediation_owner**

다른 역할에 대한 정보:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

모듈	sn_vulc.remediation_owner
위험 점수 롤업 계산기	
정정 대상 규칙	

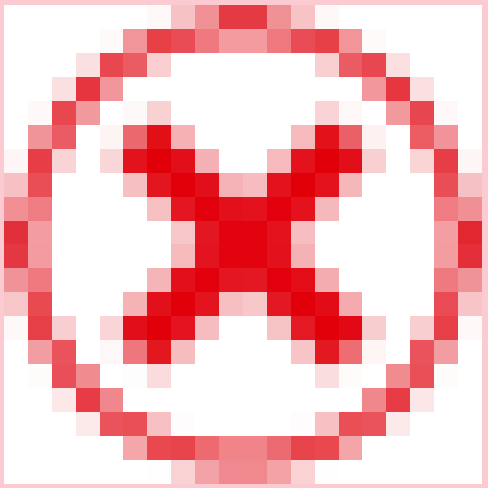
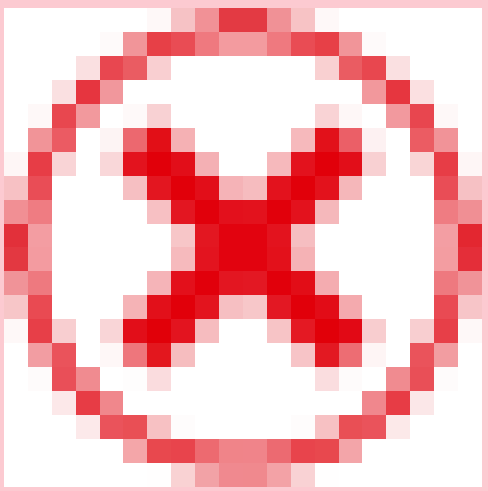
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vulc.remediation_owner**

다른 역할에 대한 정보:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

모듈	sn_vulc.remediation_owner
중요도 매핑	
알림	

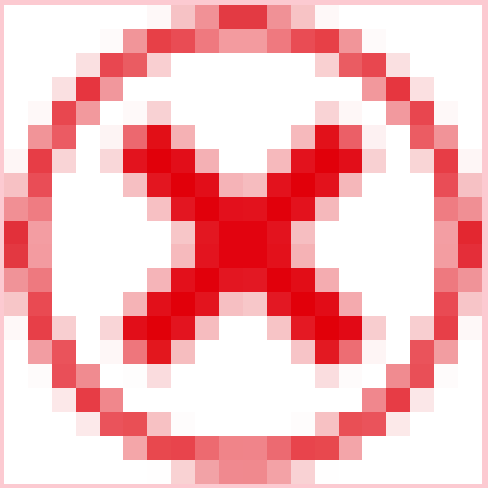
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vulc.remediation_owner**

다른 역할에 대한 정보:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

모듈	sn_vulc.remediation_owner
예외 관리	

〔End〕

〔store-future: BEGIN review〕

컨테이너 취약성 대응에 대한 역할별 모듈 액세스

컨테이너 취약성 대응의 경우 특정 역할이 액세스할 수 있는 메뉴 항목을 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity**

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity**

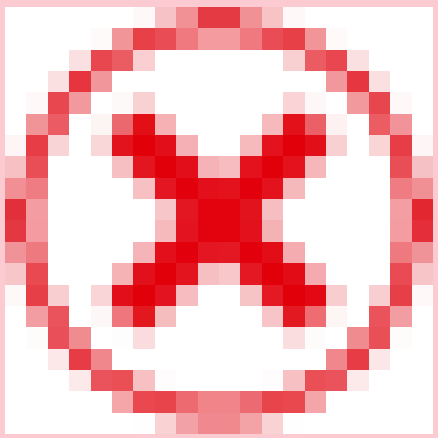
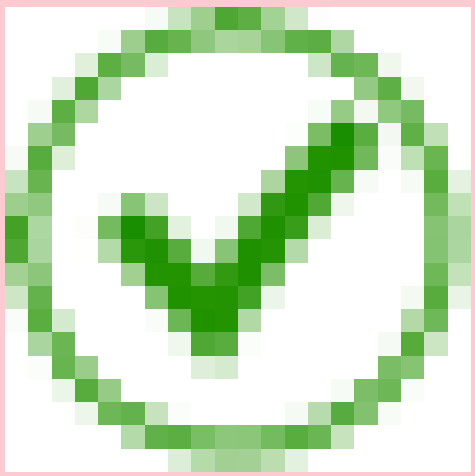
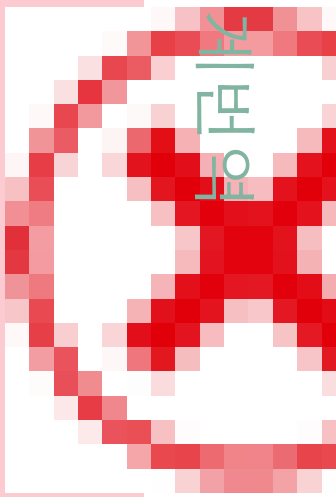
다른 역할에 대한 정보:

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

모듈	sn_sec_cmn.manage_approval_rules	sn_vul_container.configure_integrations	sn_vul_container.configure_v
(메인 앱 그룹)			
개요			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity**

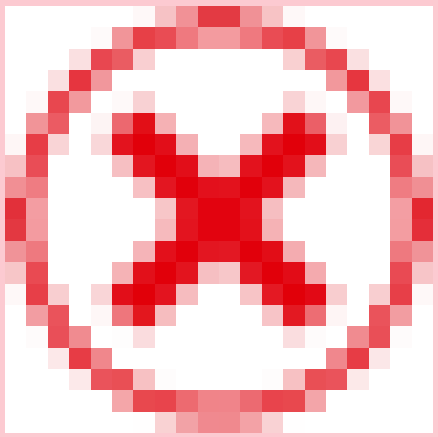
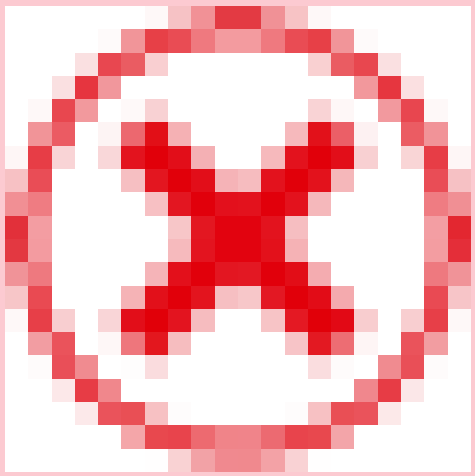
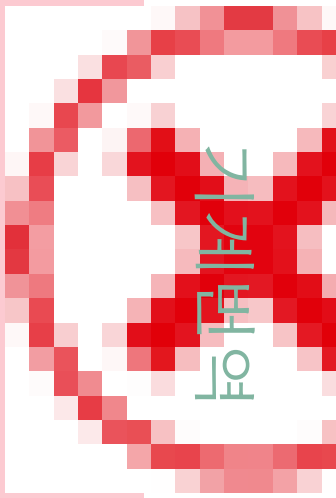
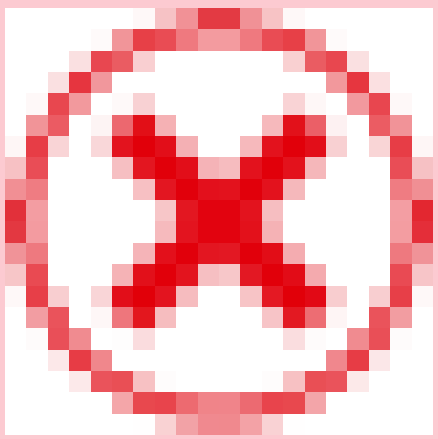
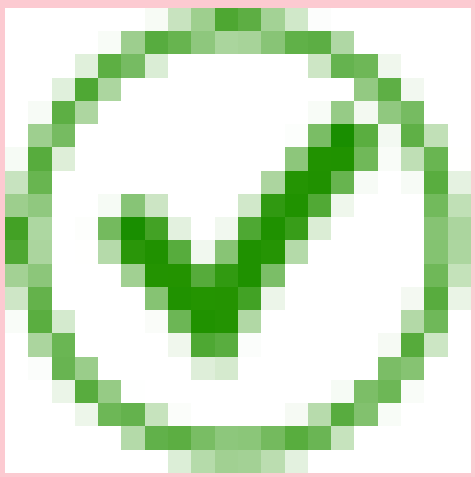
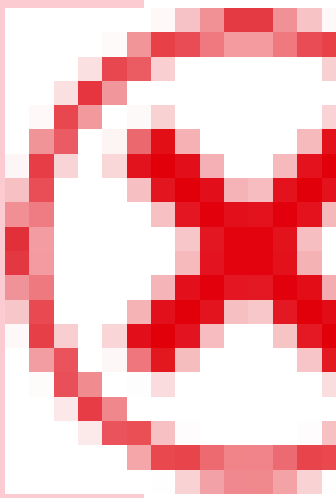
다른 역할에 대한 정보:

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

모듈	sn_sec_cmn.manage_approval_rules	sn_vul_container.configure_integrations	sn_vul_container.configure_v
내 승인			
컨테이너 취약한 항목			
나에게 할당됨			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity**

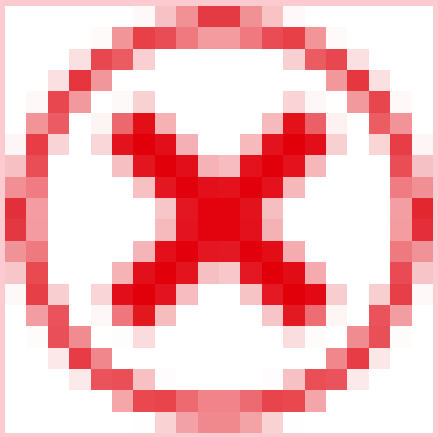
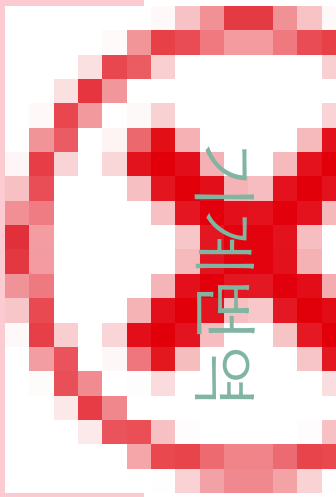
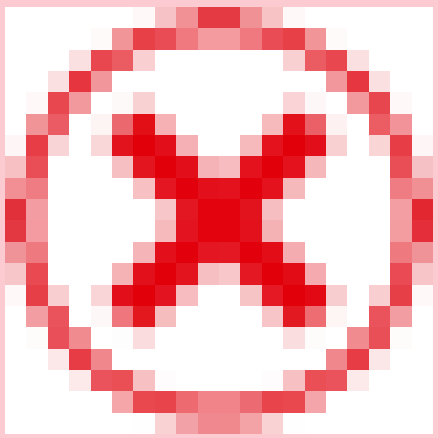
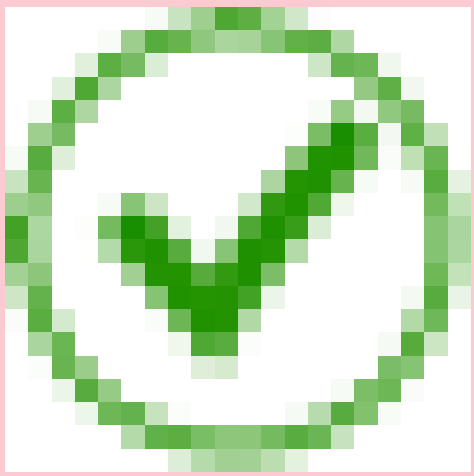
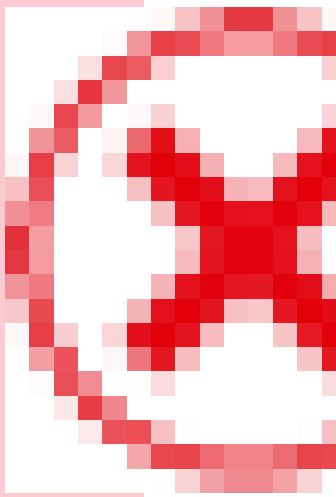
다른 역할에 대한 정보:

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

모듈	sn_sec_cmn.manage_approval_rules	sn_vul_container.configure_integrations	sn_vul_container.configure_v
사용자 그룹에 할당됨			
중요 및 높은 위험			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity**

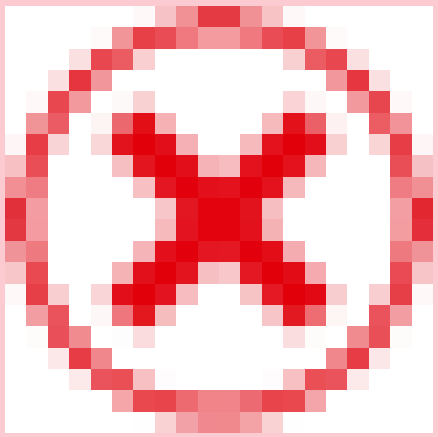
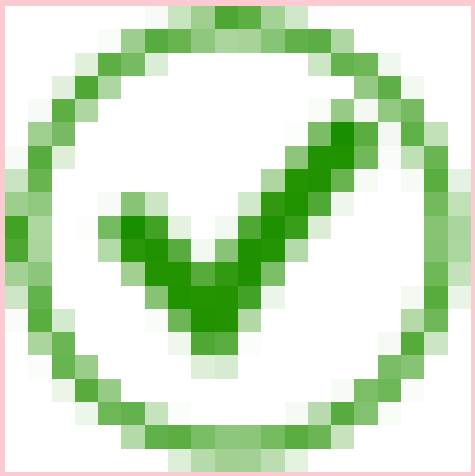
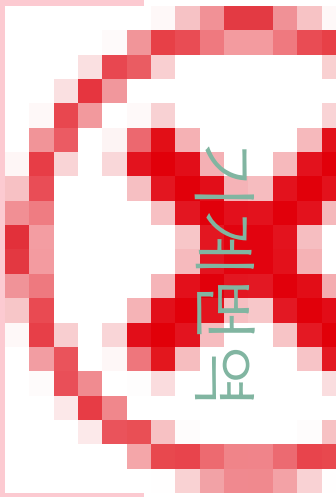
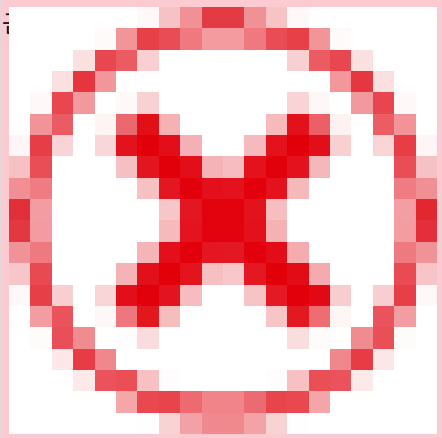
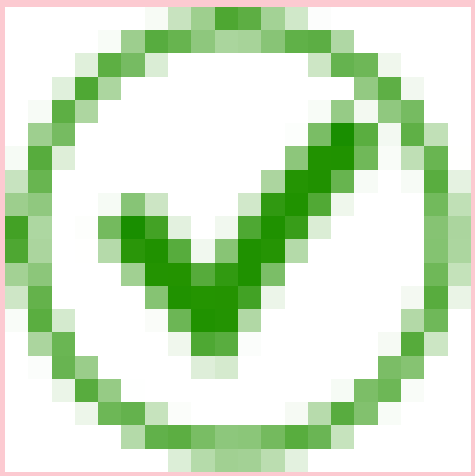
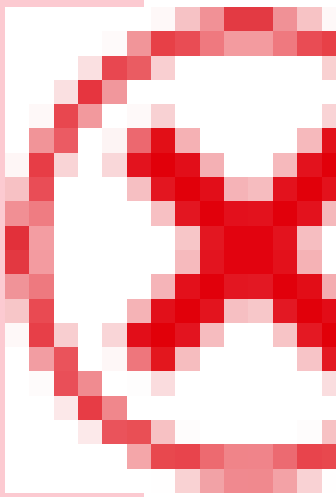
다른 역할에 대한 정보:

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

모듈	sn_sec_cmn.manage_approval_rules	sn_vul_container.configure_integrations	sn_vul_container.configure_v
악용 가능			
대상에 접			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity**

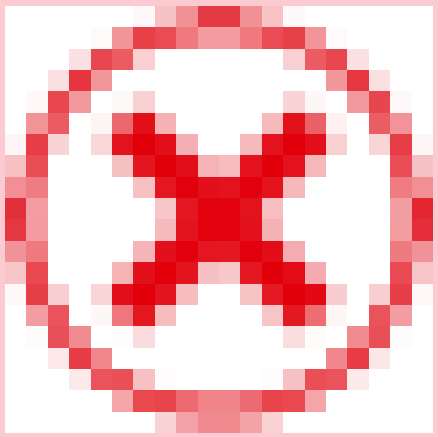
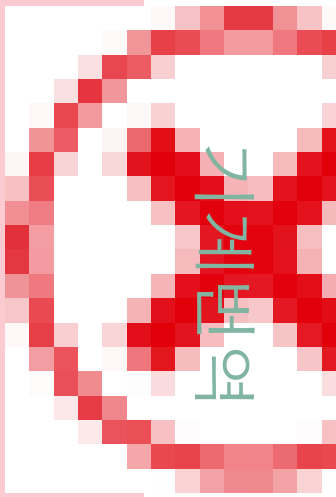
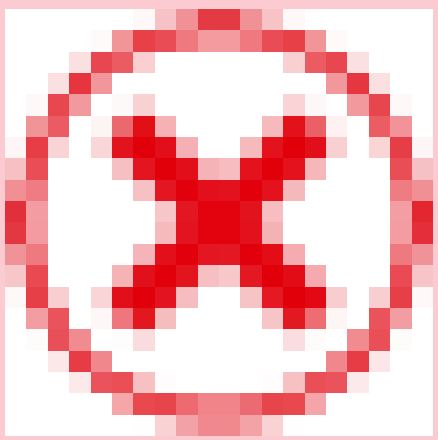
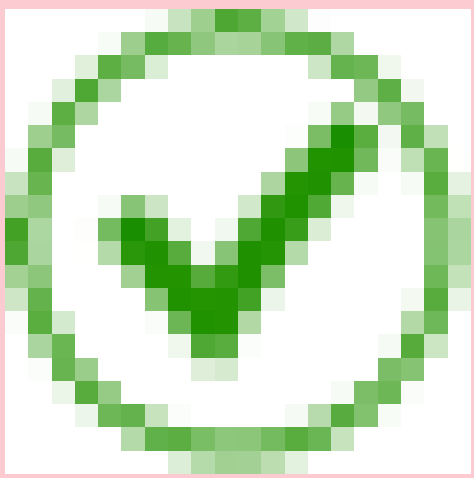
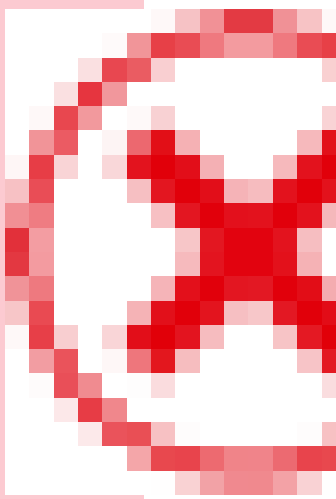
다른 역할에 대한 정보:

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

모듈	sn_sec_cmn.manage_approval_rules	sn_vul_container.configure_integrations	sn_vul_container.configure_v
누락된 대상			
모두			

라이브러리

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity**

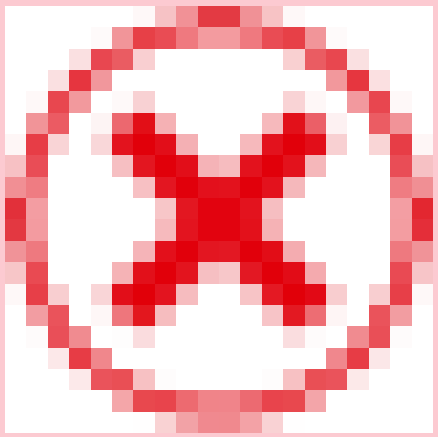
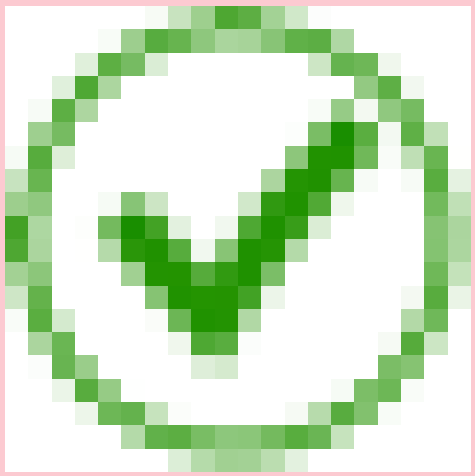
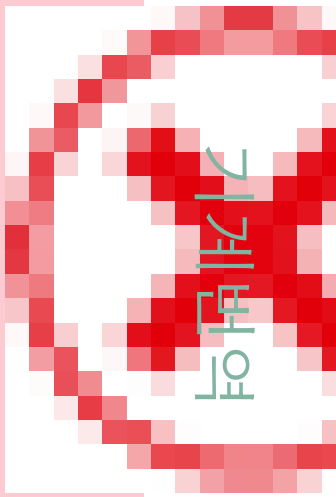
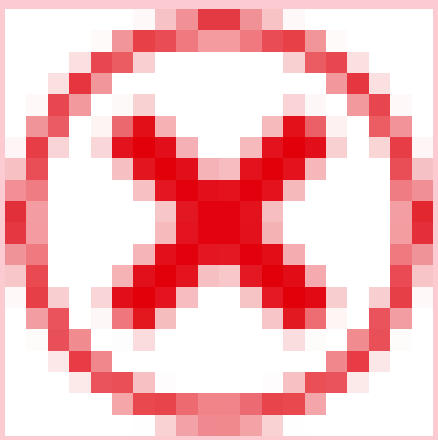
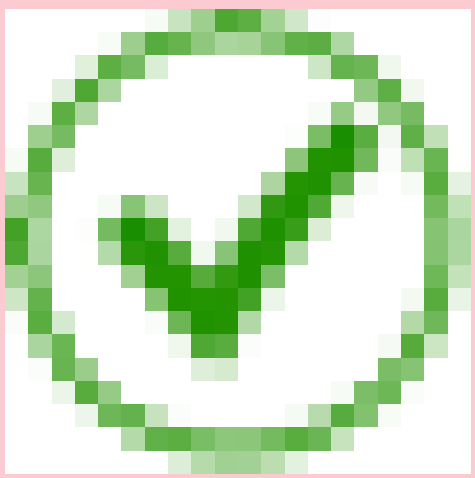
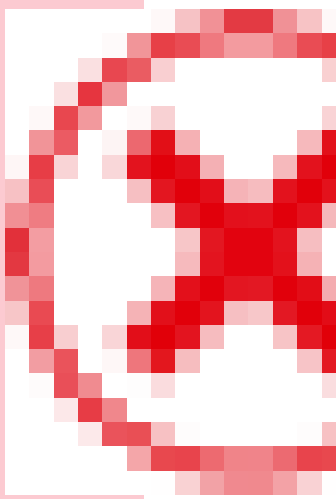
다른 역할에 대한 정보:

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

모듈	sn_sec_cmn.manage_approval_rules	sn_vul_container.configure_integrations	sn_vul_container.configure_v
NVD			
외부 공급업체			
관리			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity**

다른 역할에 대한 정보:

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

모듈	sn_sec_cmn.manage_approval_rules	sn_vul_container.configure_integrations	sn_vul_container.configure_v
담당 규칙	✗	✗	✗
취약성 계산기	✗	✗	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity**

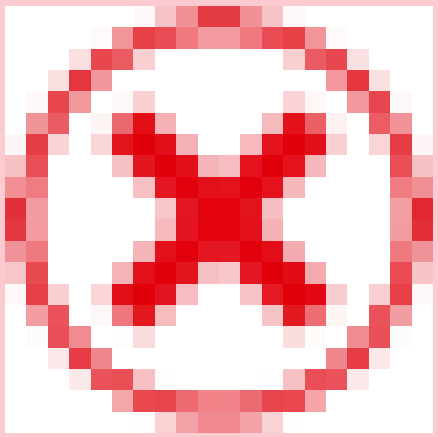
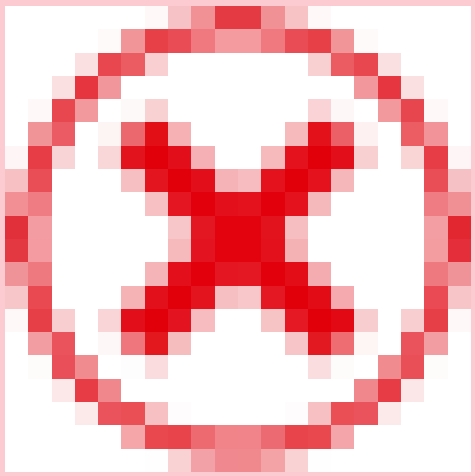
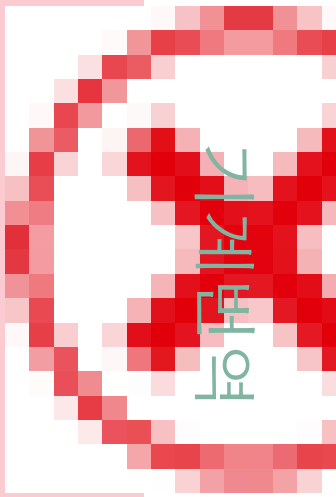
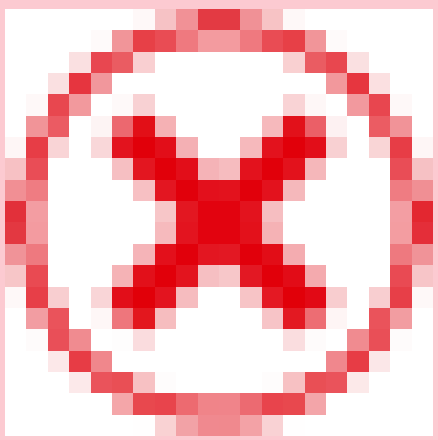
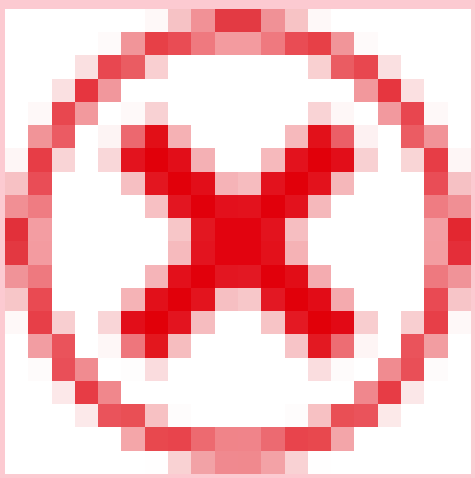
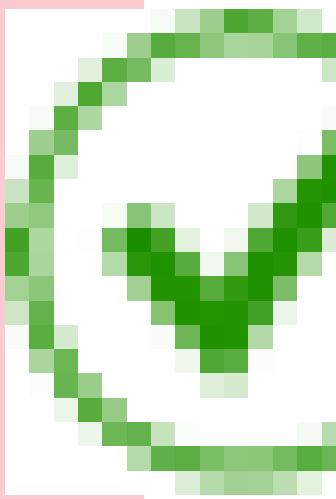
다른 역할에 대한 정보:

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

모듈	sn_sec_cmn.manage_approval_rules	sn_vul_container.configure_integrations	sn_vul_container.configure_v
정정 대상 규칙			
VI 세분성 구성			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity**

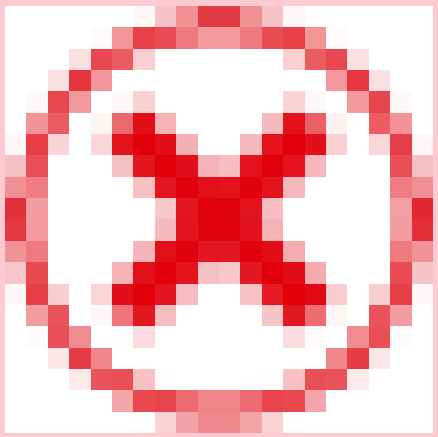
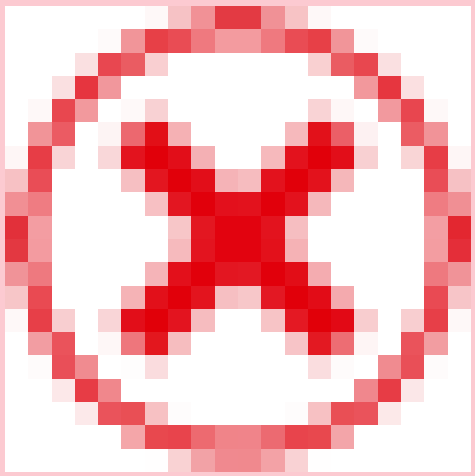
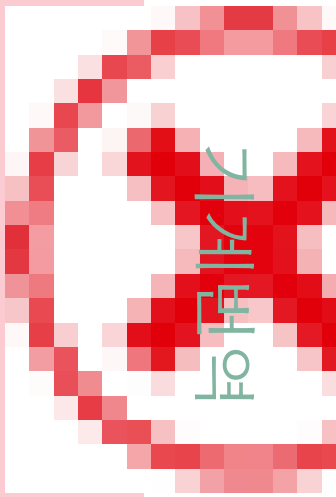
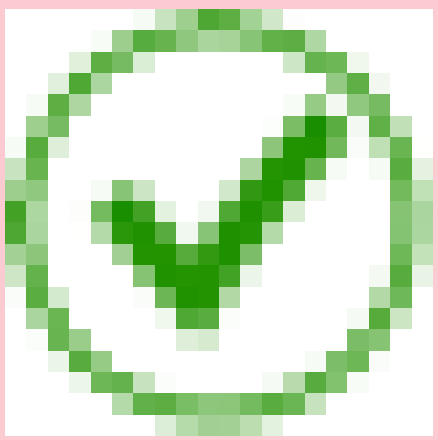
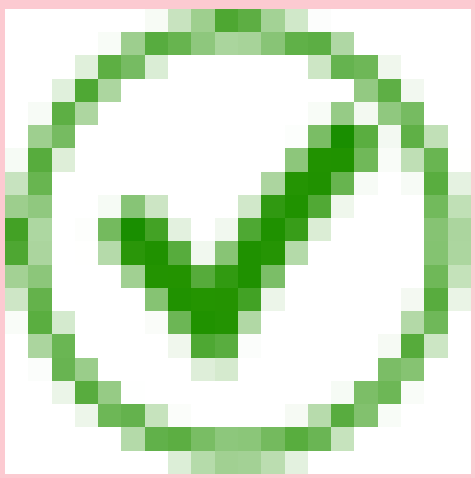
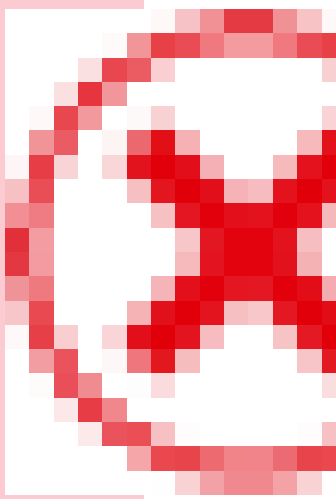
다른 역할에 대한 정보:

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

모듈	sn_sec_cmn.manage_approval_rules	sn_vul_container.configure_integrations	sn_vul_container.configure_v
예외 규칙			
승인 규칙			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity**

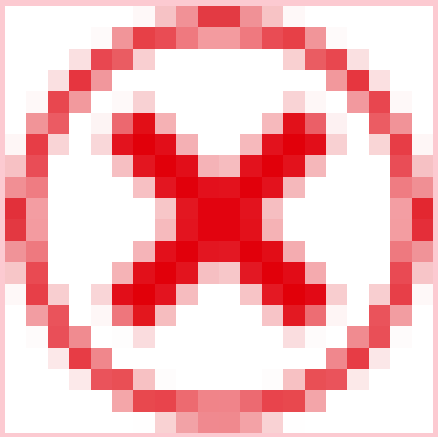
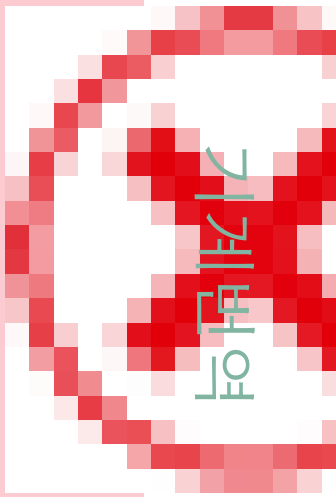
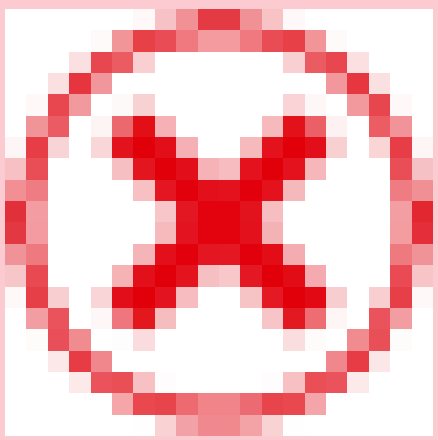
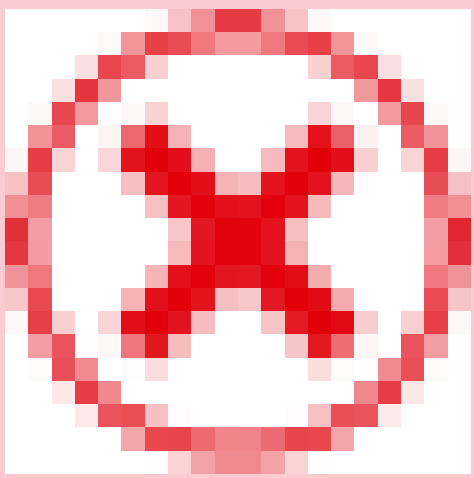
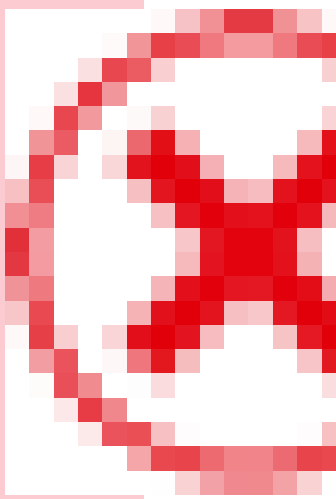
다른 역할에 대한 정보:

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

모듈	sn_sec_cmn.manage_approval_rules	sn_vul_container.configure_integrations	sn_vul_container.configure_v
컨테이너 보안 통합			
취약한 항목 자동 닫기			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity**

다른 역할에 대한 정보:

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

모듈	sn_sec_cmn.manage_approval_rules	sn_vul_container.configure_integrations	sn_vul_container.configure_v
표준화된 심각성 맵			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules**

다음에 대한 모듈 액세스: **sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules**

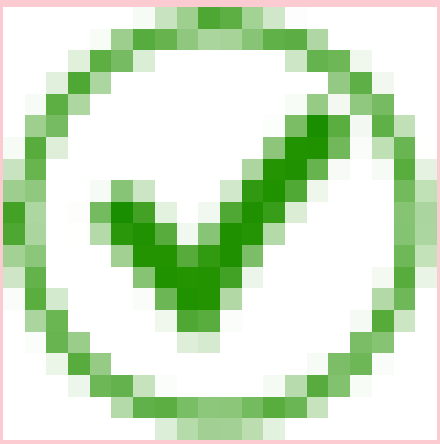
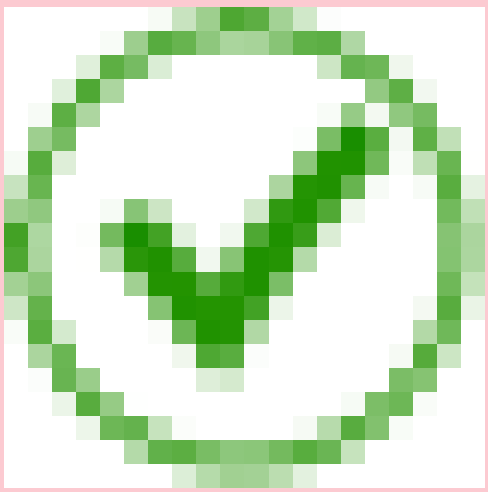
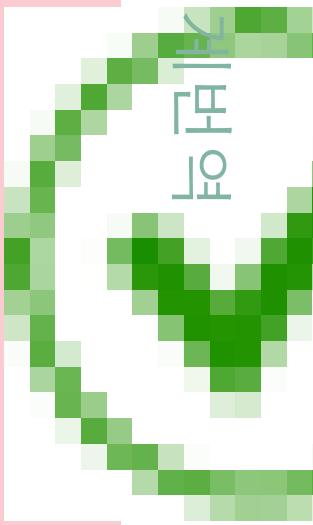
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.exception_approver	sn_vul_container.false_positive_approver	sn_vul_container.manage_
(메인 앱 그룹)			
개요			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules**

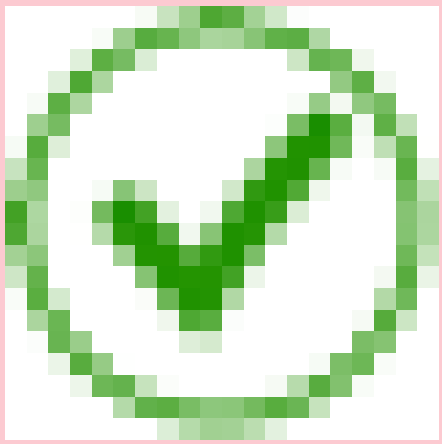
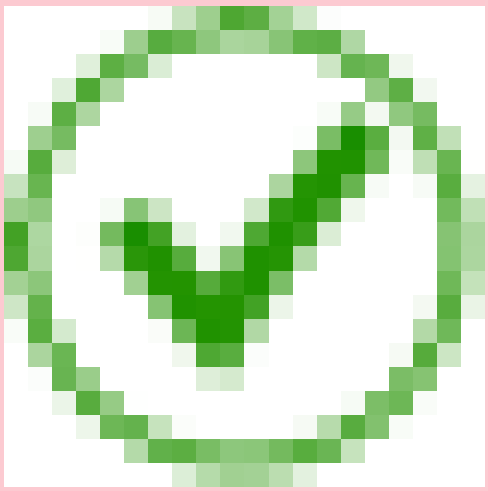
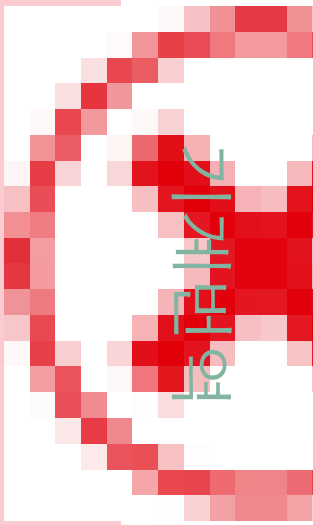
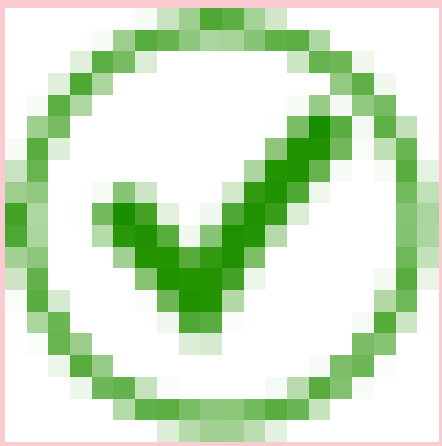
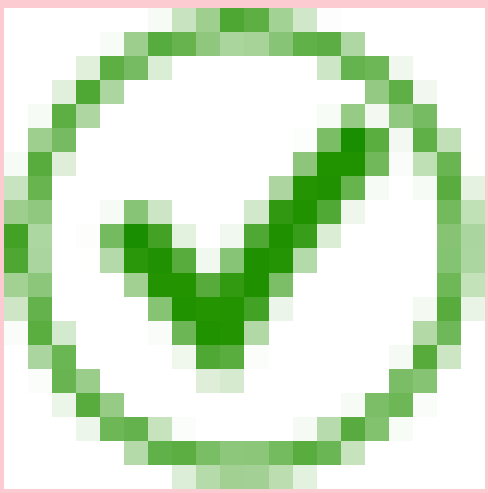
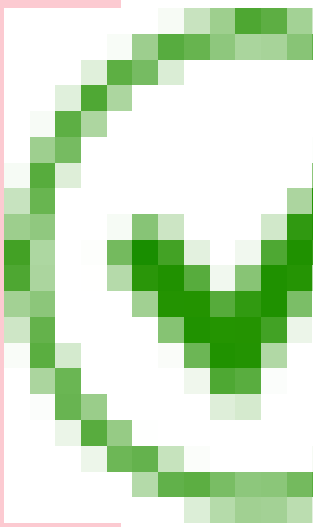
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.exception_approver	sn_vul_container.false_positive_approver	sn_vul_container.manage_
내 승인			
컨테이너 취약한 항목			
나에게 할당됨			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules**

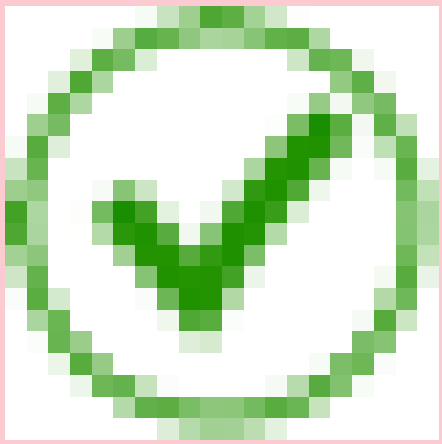
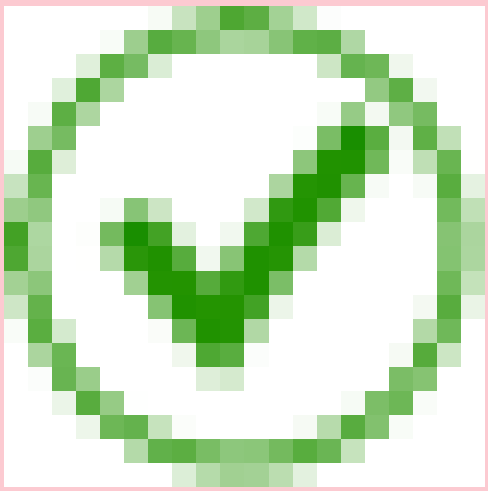
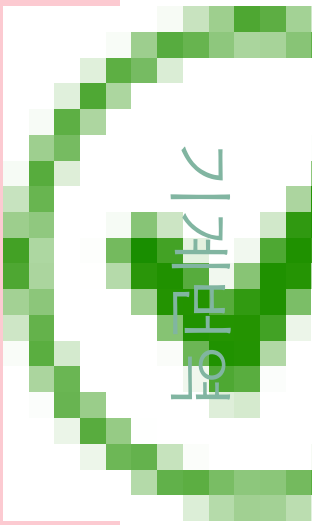
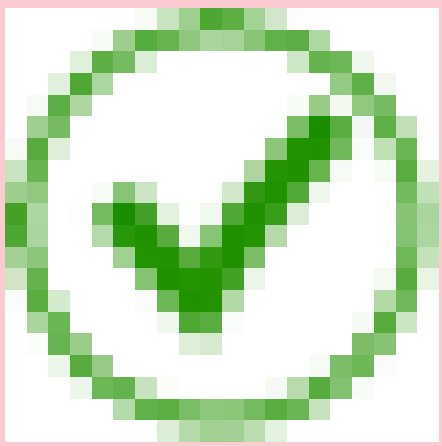
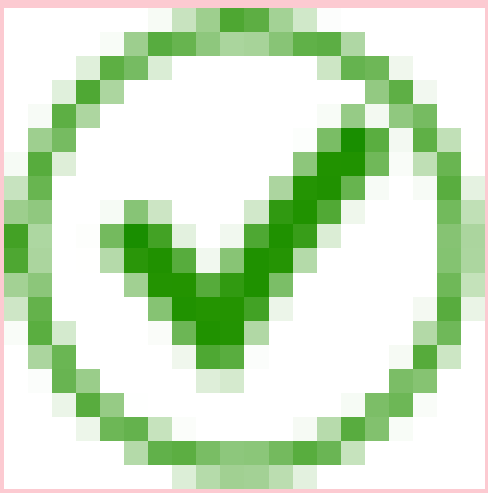
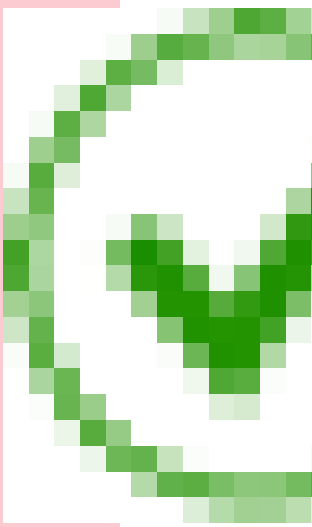
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.exception_approver	sn_vul_container.false_positive_approver	sn_vul_container.manage_
사용자 그룹에 할당됨			
중요 및 높은 위험			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules**

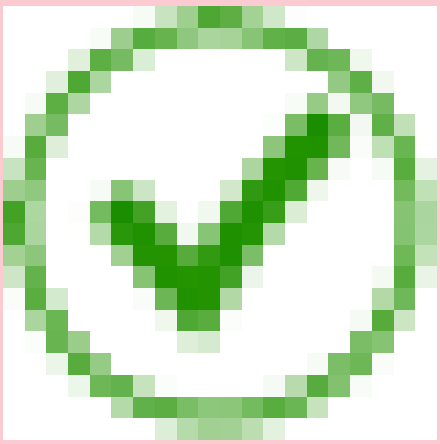
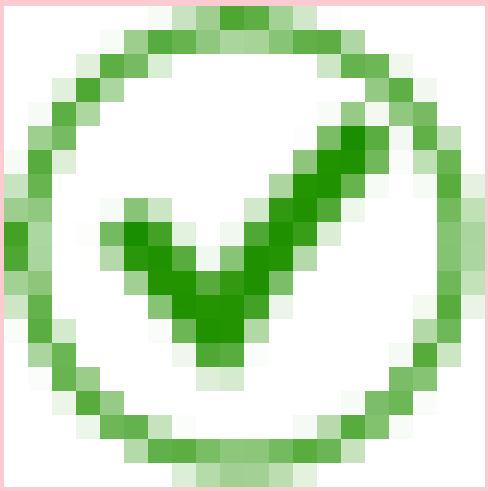
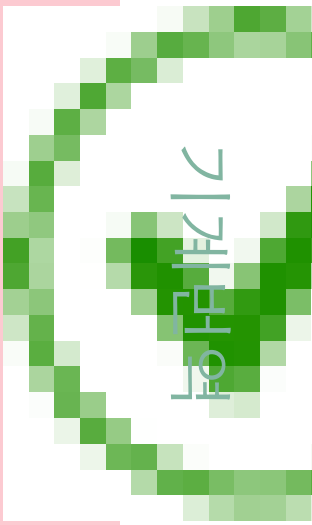
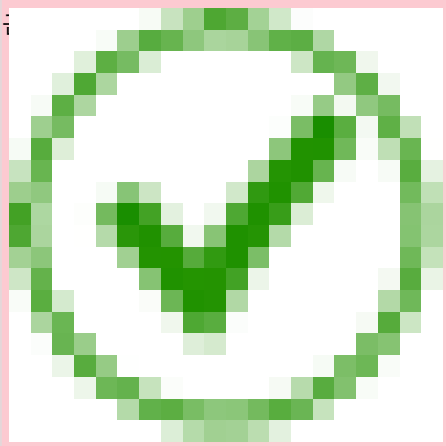
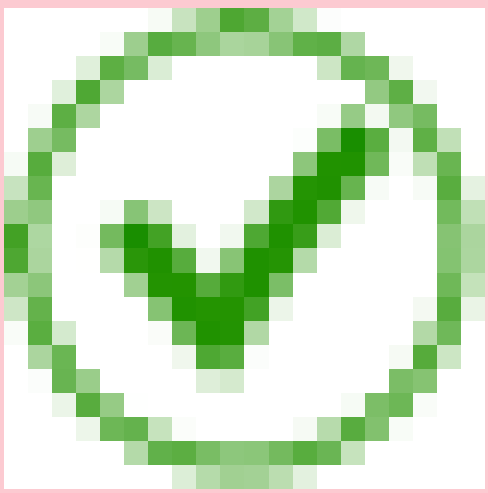
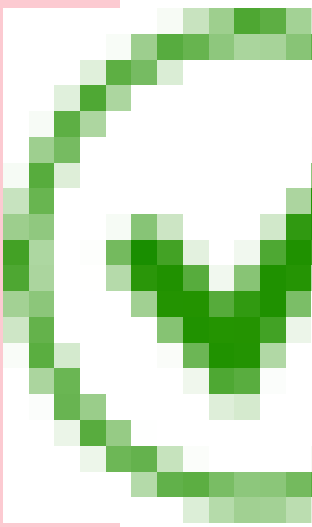
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.exception_approver	sn_vul_container.false_positive_approver	sn_vul_container.manage_
악용 가능			
대상에 접			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules**

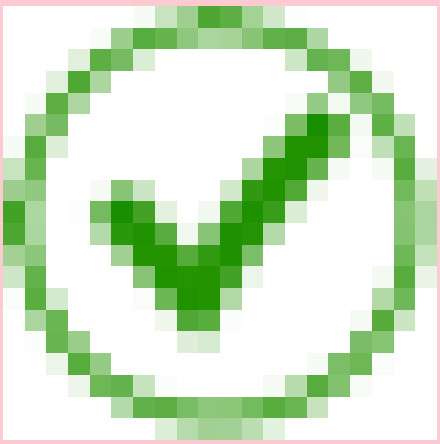
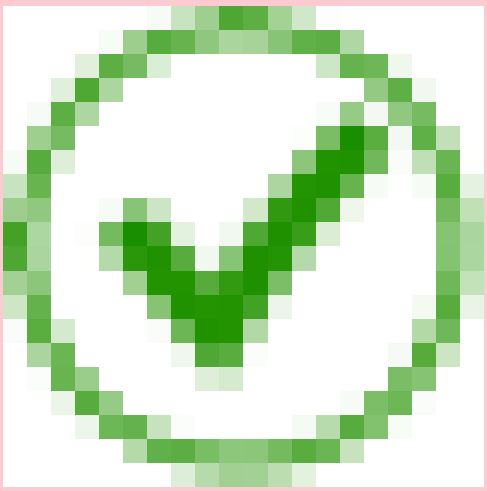
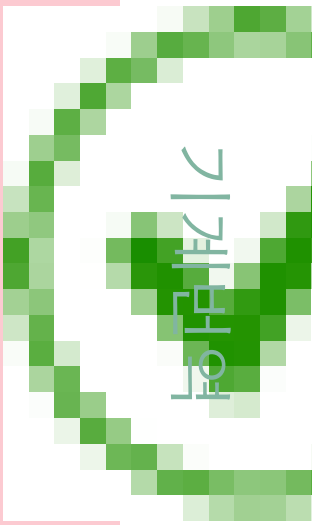
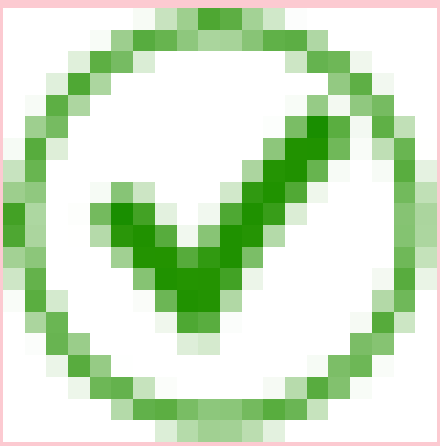
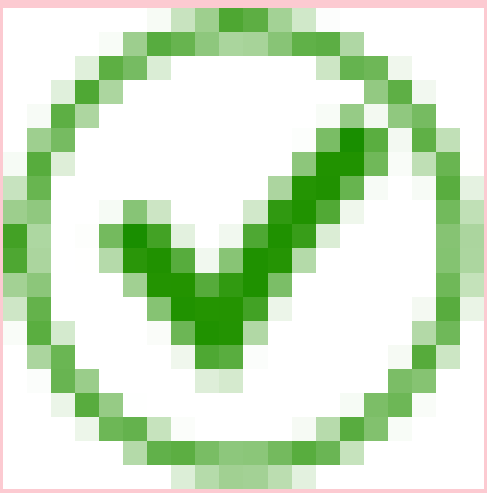
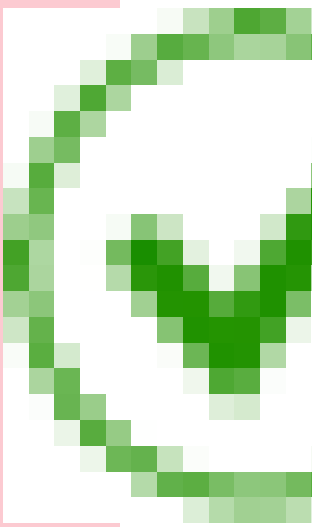
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.exception_approver	sn_vul_container.false_positive_approver	sn_vul_container.manage_
누락된 대상			
모두			

라이브러리

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules**

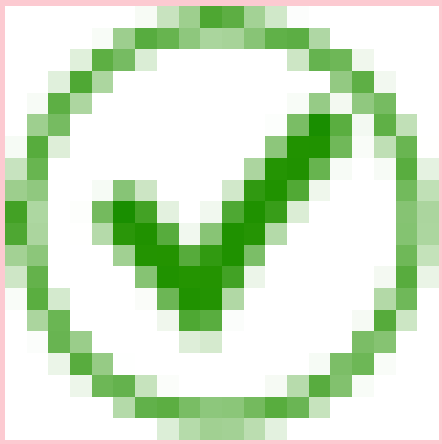
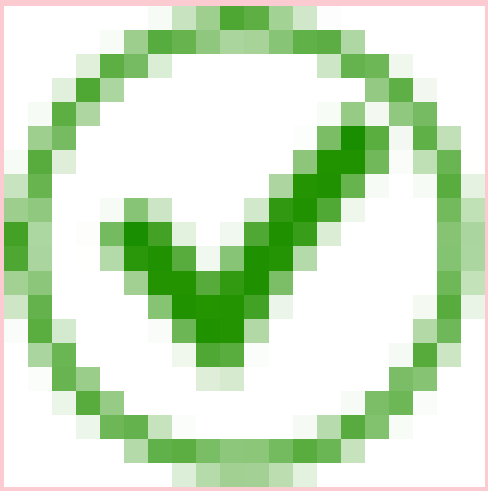
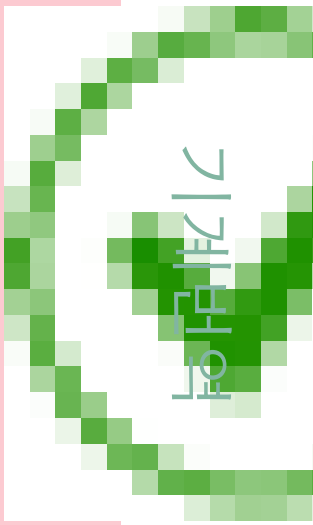
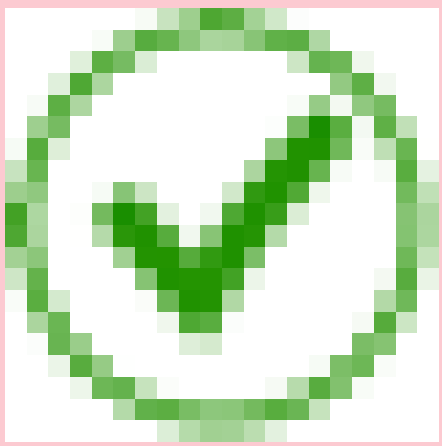
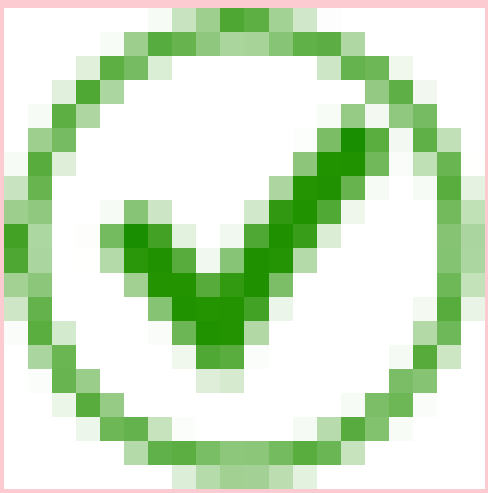
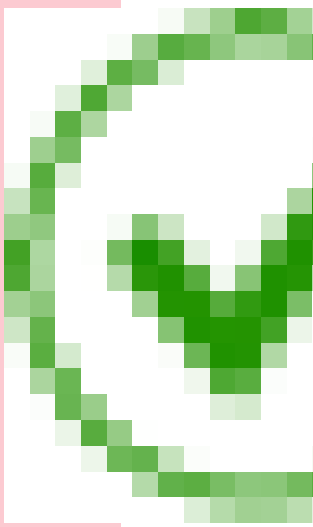
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.exception_approver	sn_vul_container.false_positive_approver	sn_vul_container.manage_
NVD			
외부 공급업체			
관리			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules**

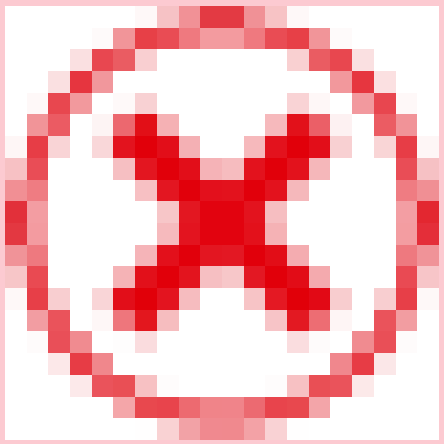
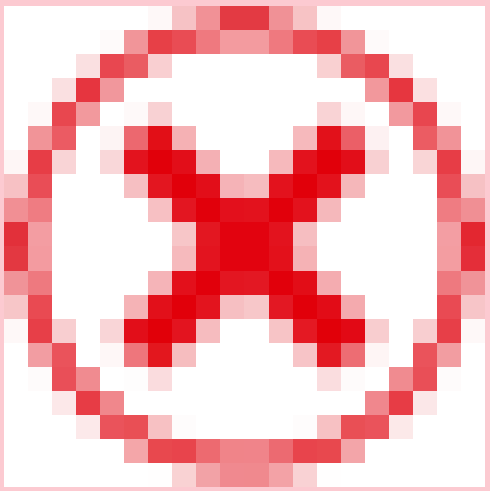
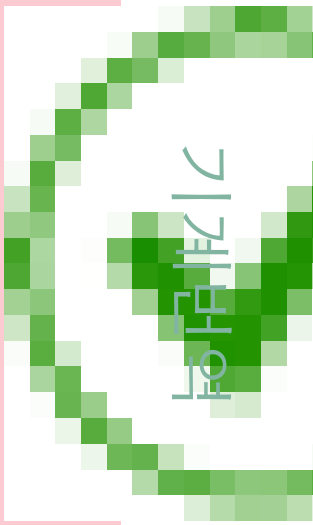
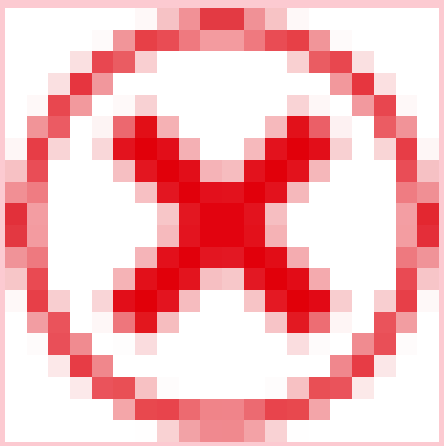
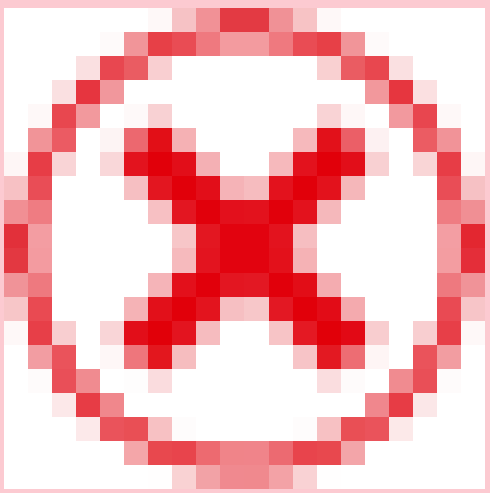
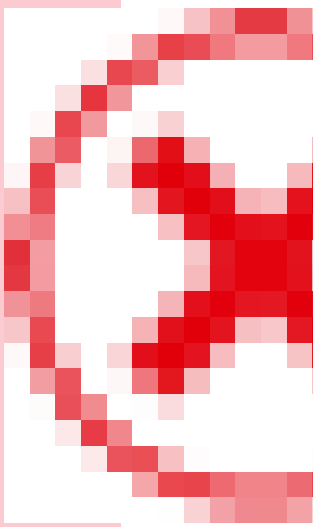
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.exception_approver	sn_vul_container.false_positive_approver	sn_vul_container.manage_
담당 규칙			
취약성 계산기			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules**

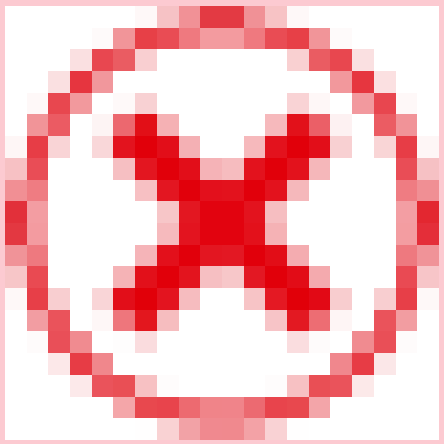
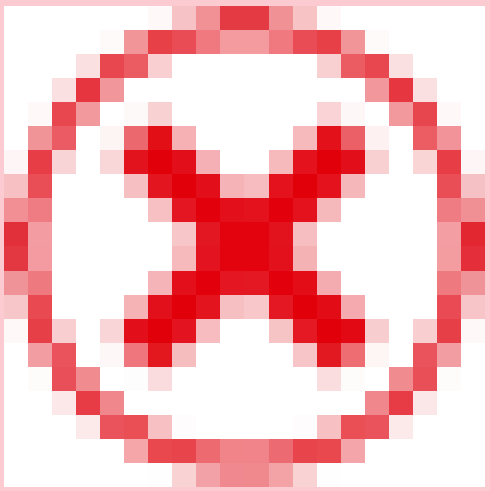
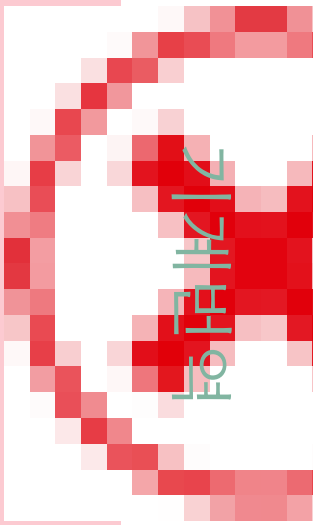
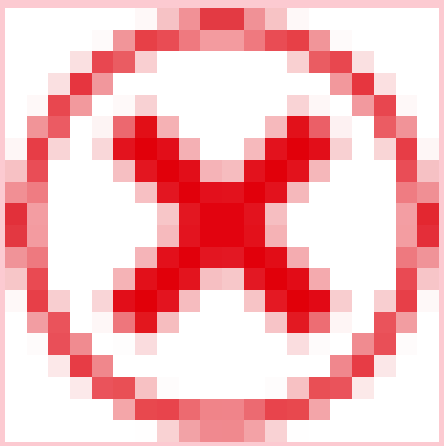
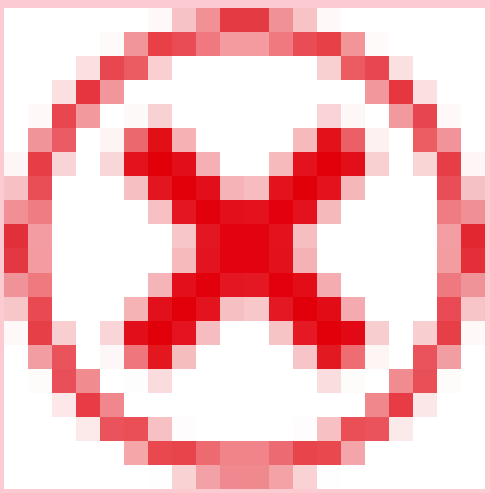
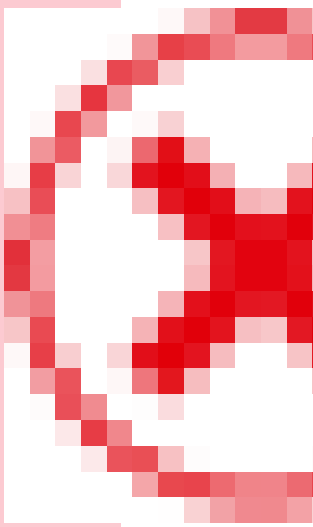
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.exception_approver	sn_vul_container.false_positive_approver	sn_vul_container.manage_
정정 대상 규칙			
VI 세분성 구성			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules**

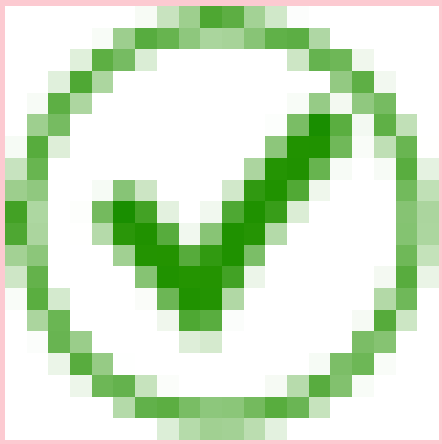
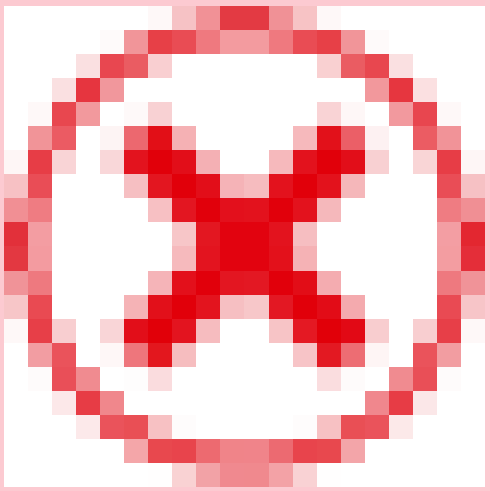
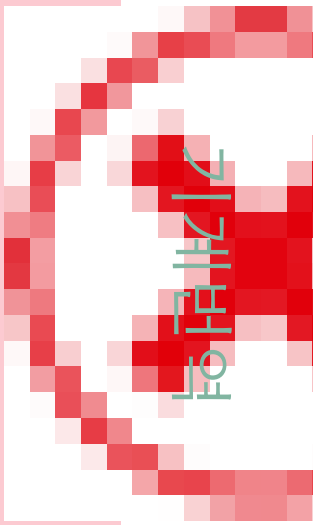
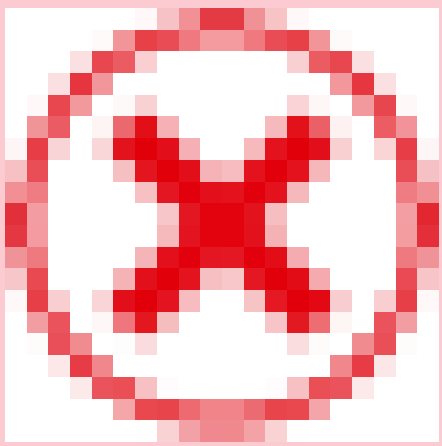
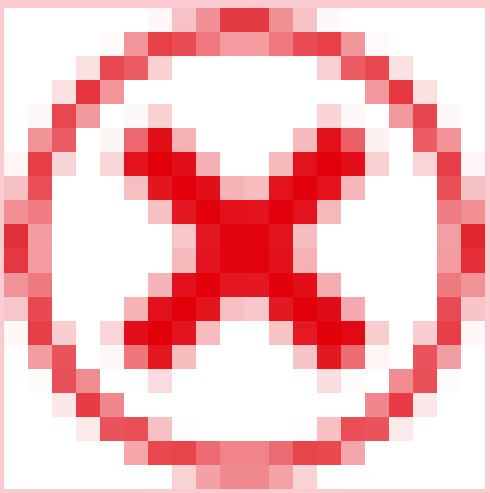
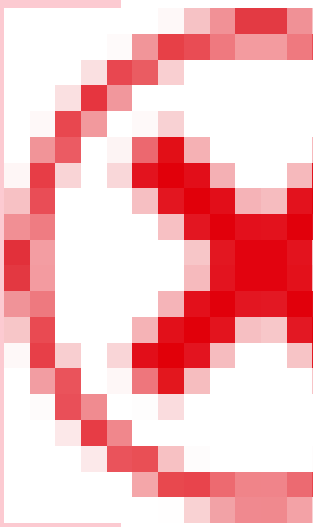
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.exception_approver	sn_vul_container.false_positive_approver	sn_vul_container.manage_
예외 규칙			
승인 규칙			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules**

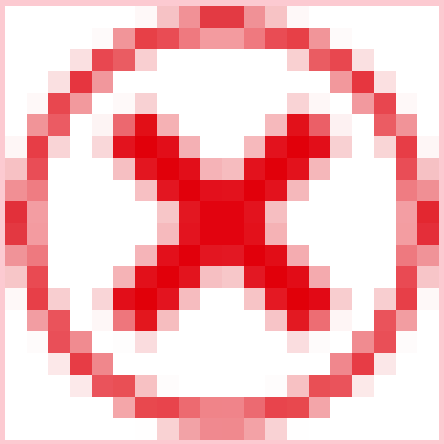
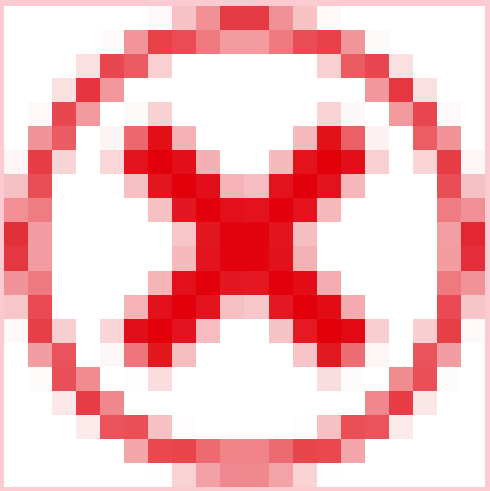
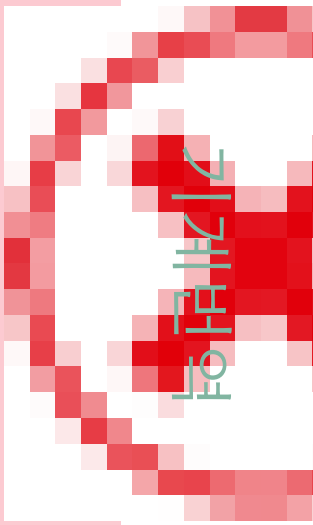
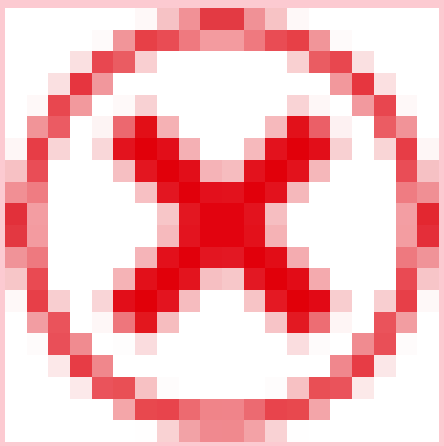
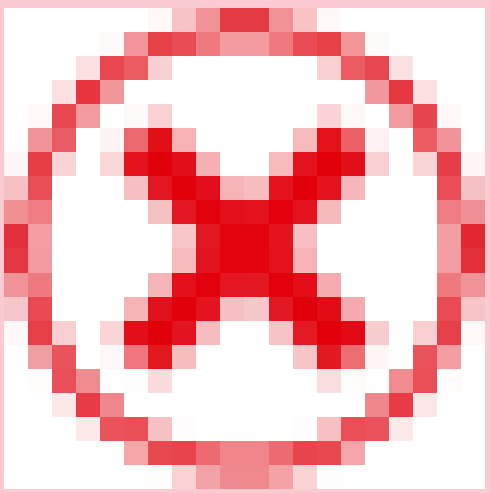
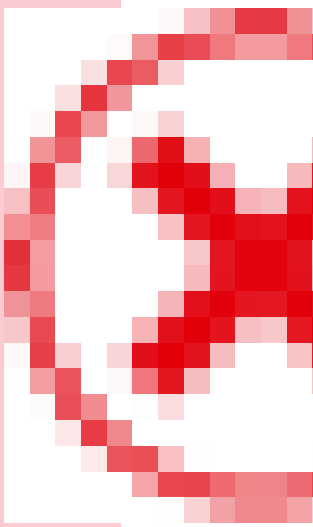
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.exception_approver	sn_vul_container.false_positive_approver	sn_vul_container.manage_
컨테이너 보안 통합			
취약한 항목 자동 닫기			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules**

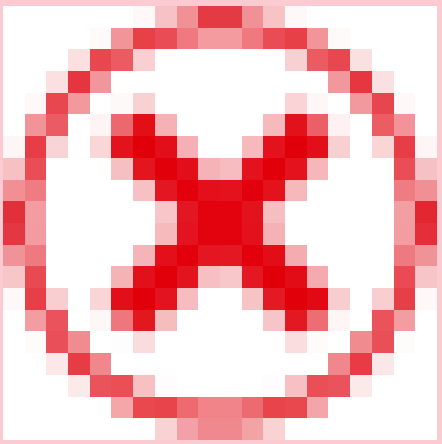
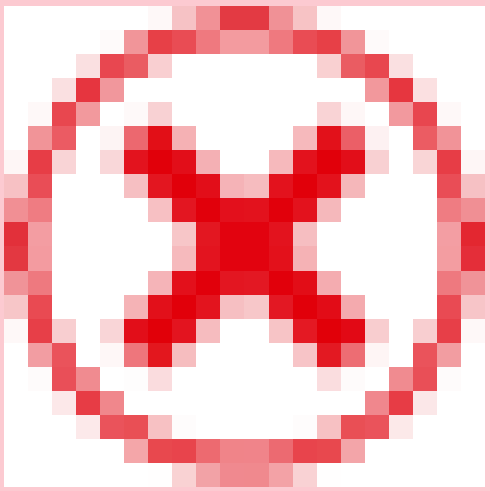
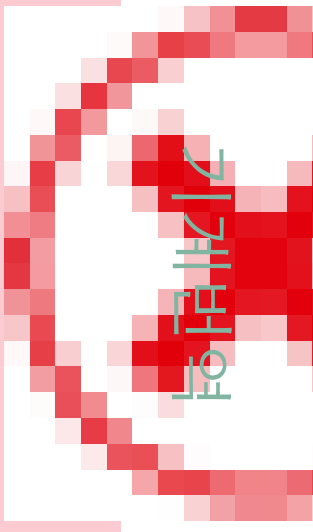
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.exception_approver	sn_vul_container.false_positive_approver	sn_vul_container.manage_
표준화된 심각성 맵			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules**

다음에 대한 모듈 액세스: **sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules**

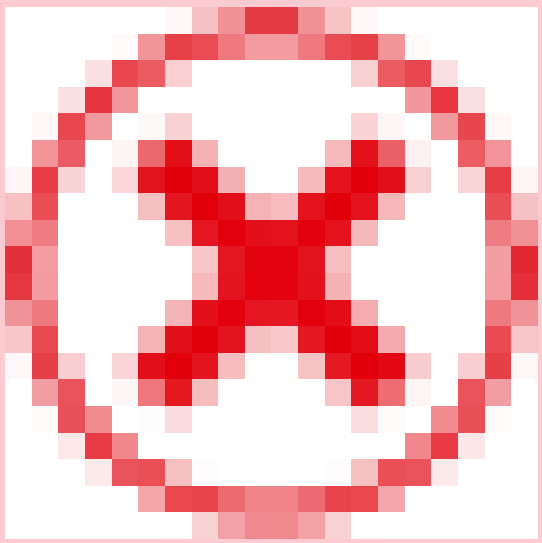
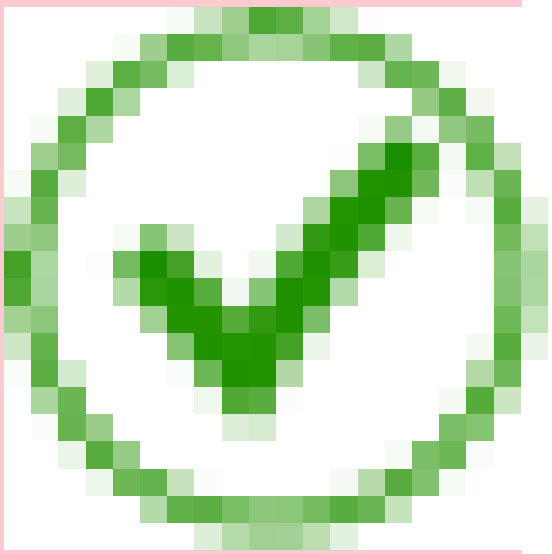
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul_conta
(메인 앱 그룹)			
개요			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul_conta
내 승인			
컨테이너 취약한 항목			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules**

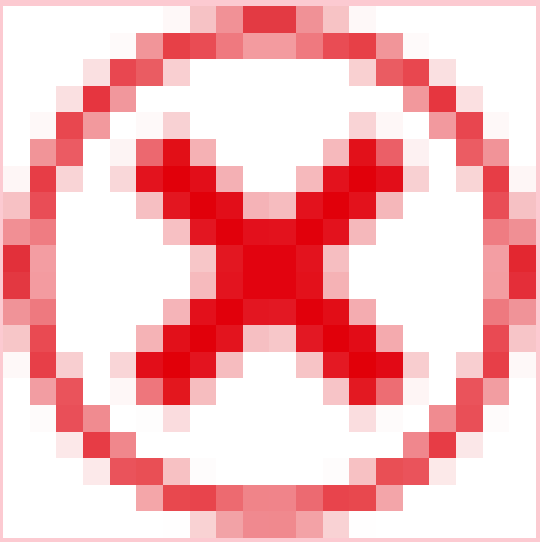
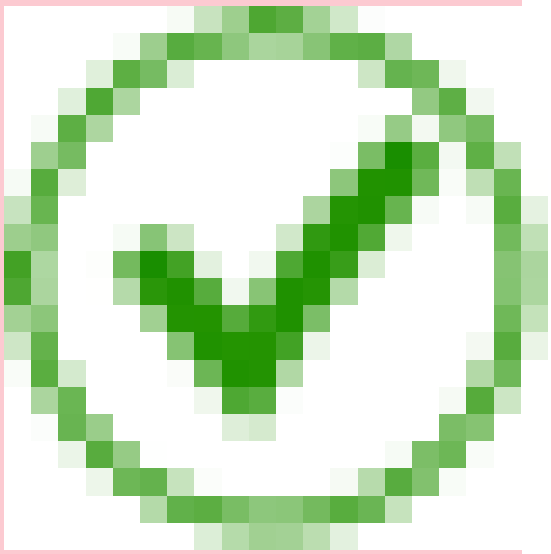
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul_conta
나에게 할당됨			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul_conta
사용자 그룹에 할당됨	✗	✓	✓

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules**

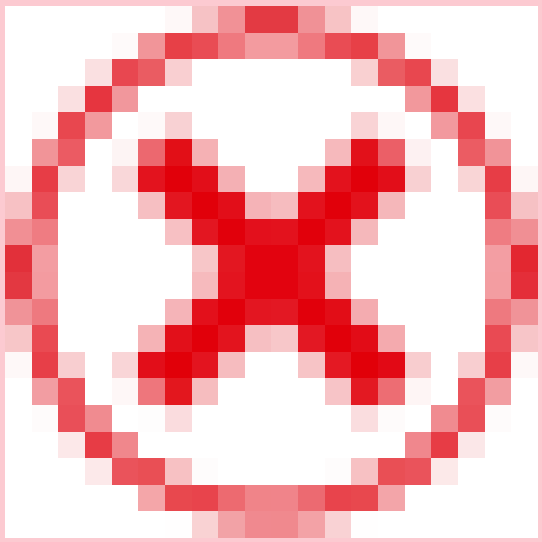
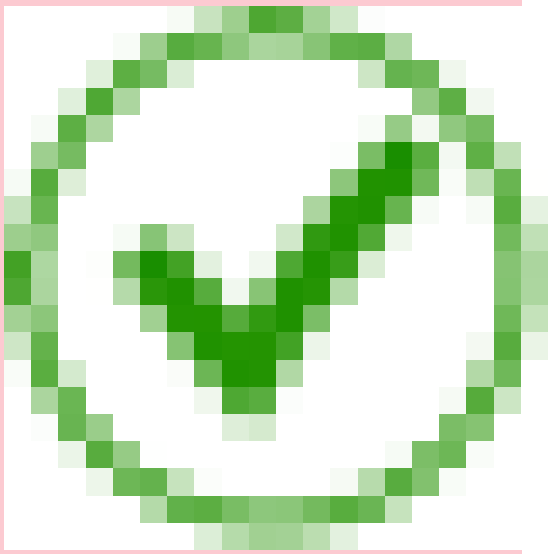
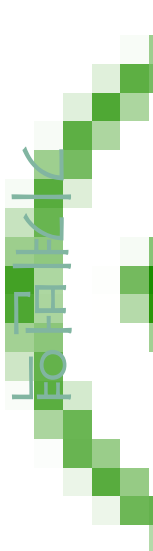
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul_conta
중요 및 높은 위험			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules**

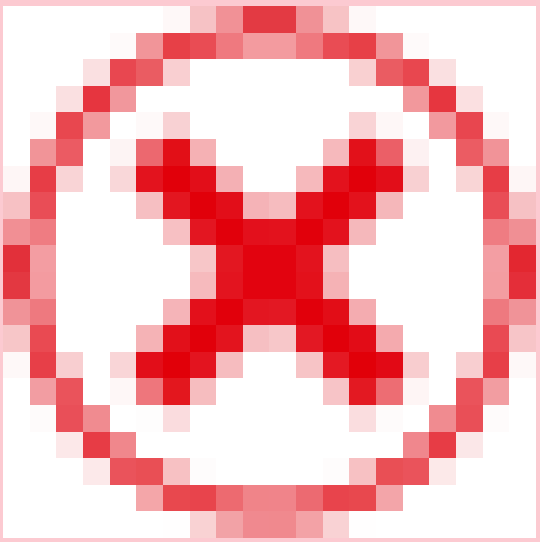
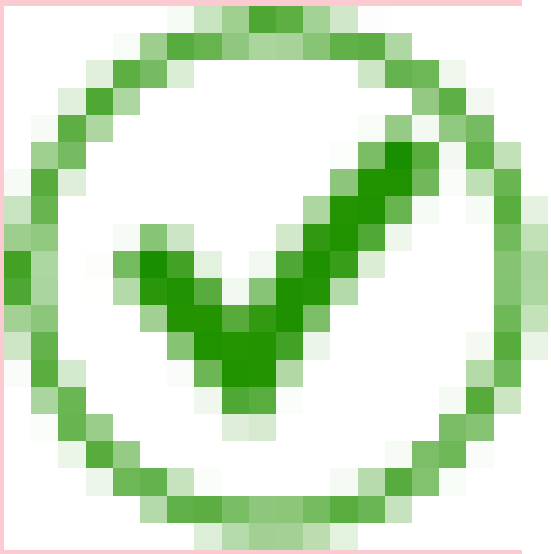
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul_conta
악용 가능			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules**

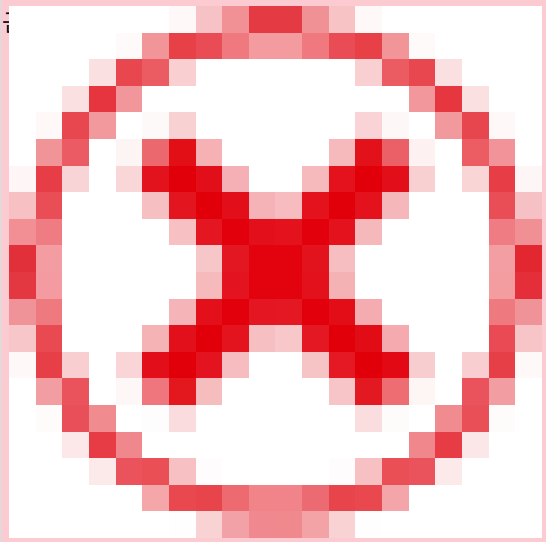
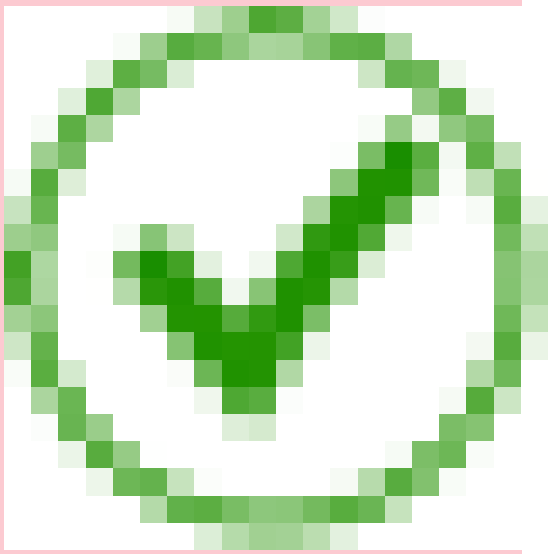
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul_conta
대상에 접			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules**

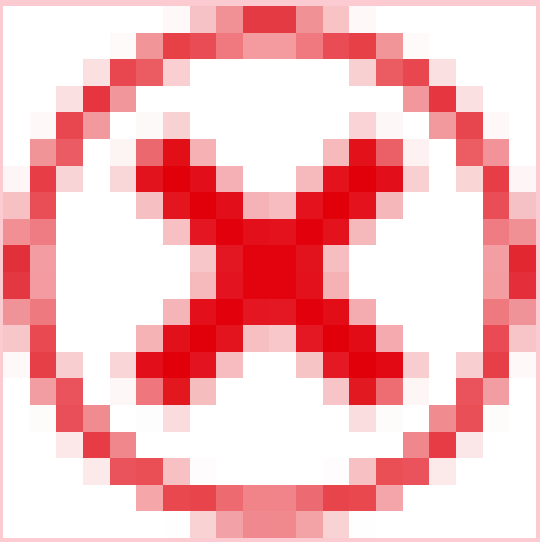
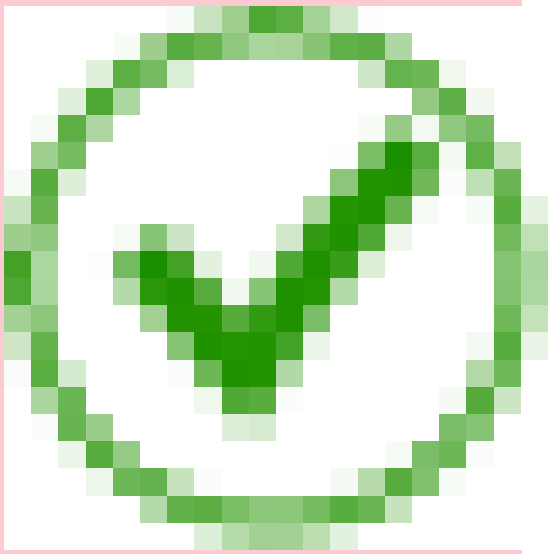
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul_conta
누락된 대상			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules**

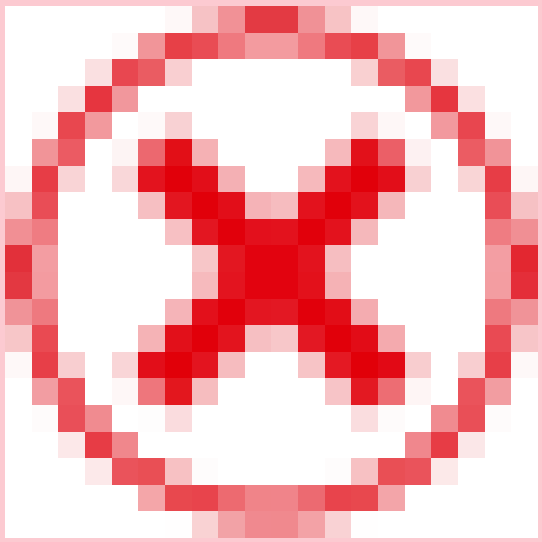
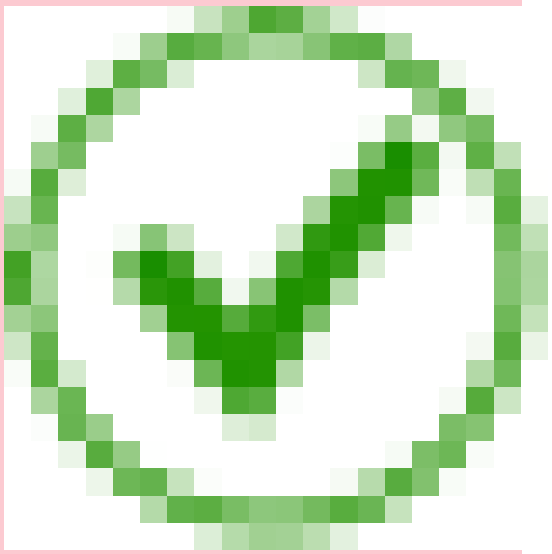
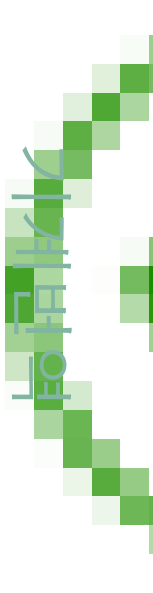
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul_conta
모두			
라이브러리			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules**

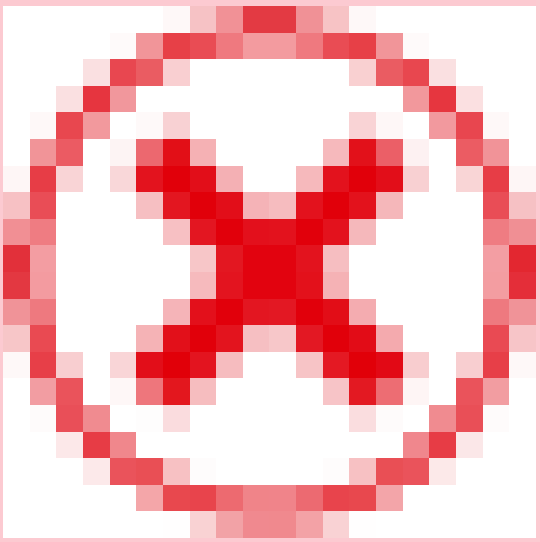
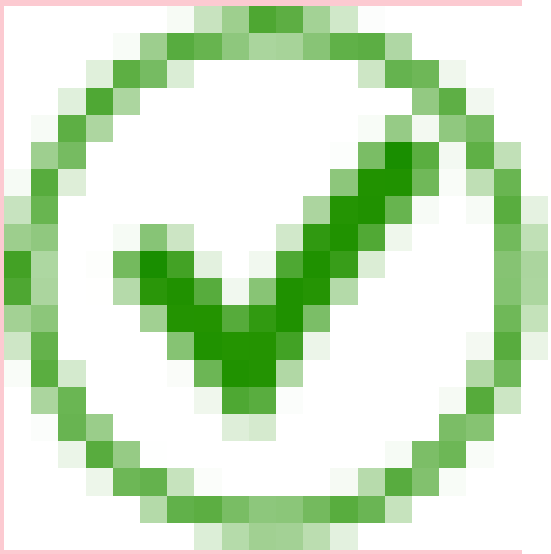
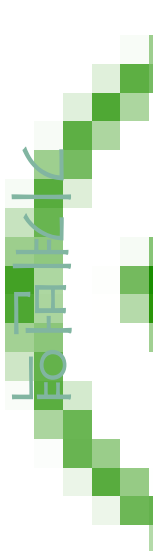
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul_conta
NVD			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules**

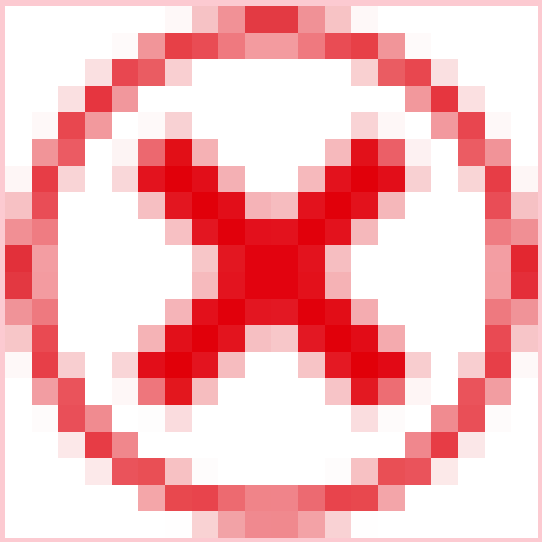
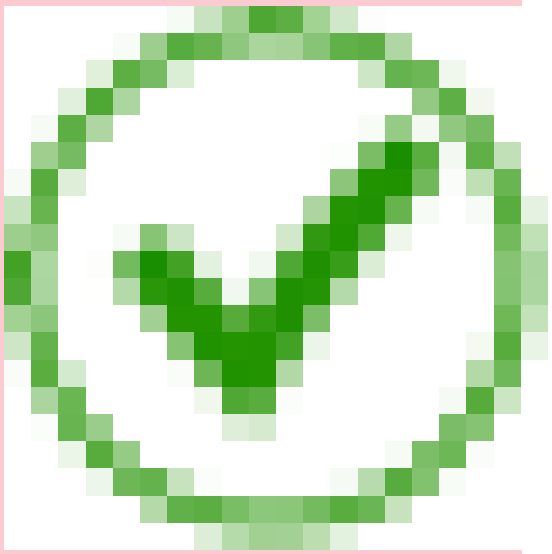
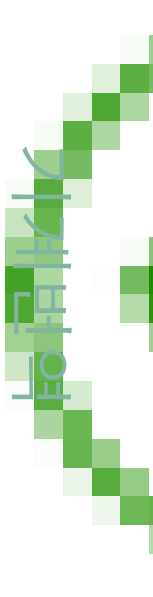
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul_conta
외부 공급업체			
관리			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul_conta
담당 규칙			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul_conta
취약성 계산기			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul_conta
정정 대상 규칙			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul_conta
VI 세분성 구성			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules**

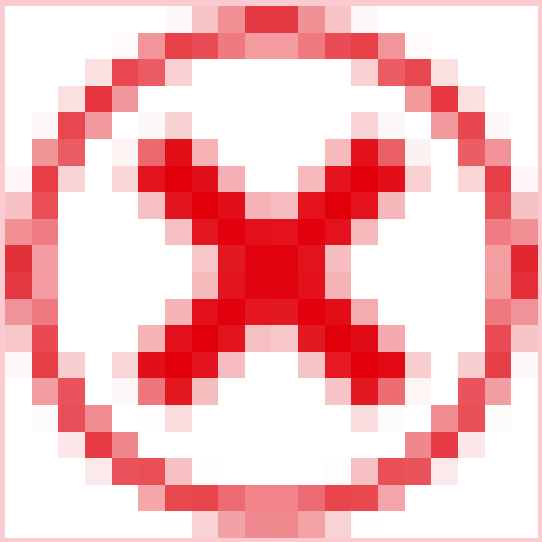
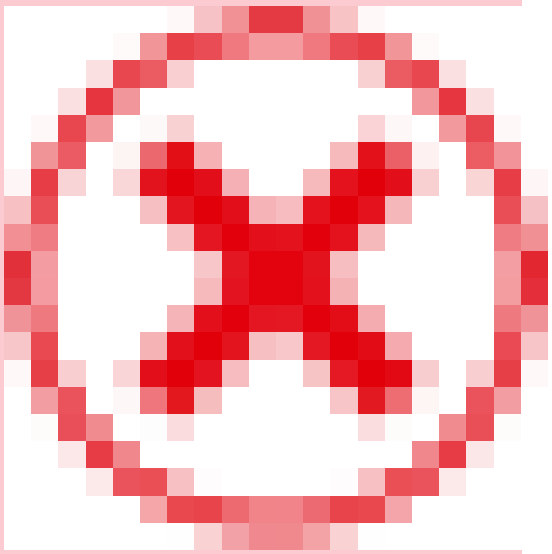
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul_conta
예외 규칙			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules**

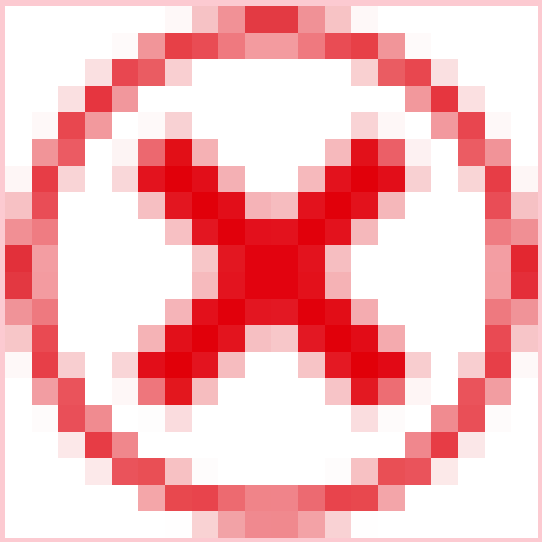
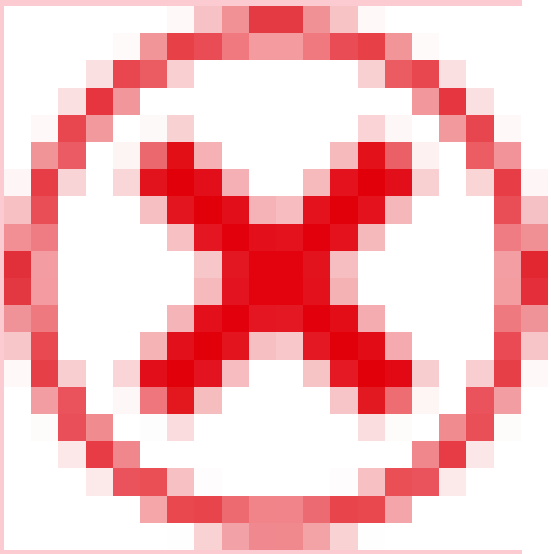
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul_conta
승인 규칙			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul_conta
컨테이너 보안 통합	✗	✗	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules**

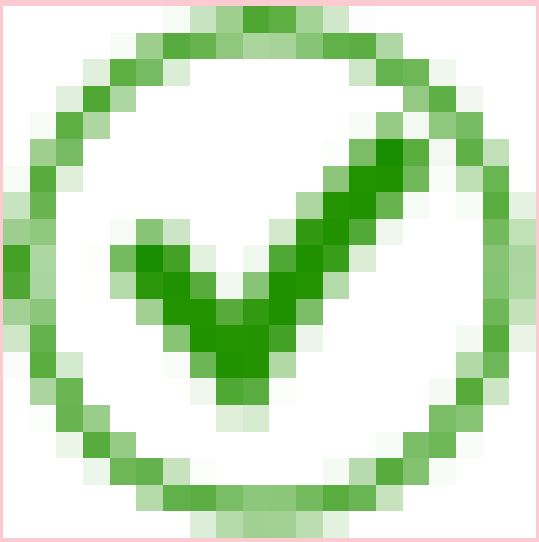
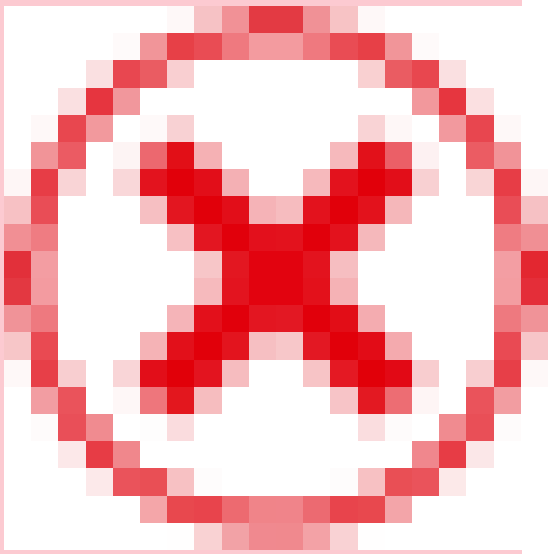
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul_conta
취약한 항목 자동 닫기			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules**

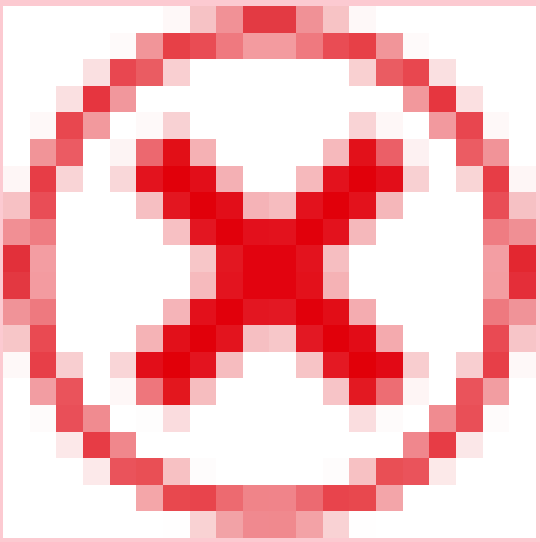
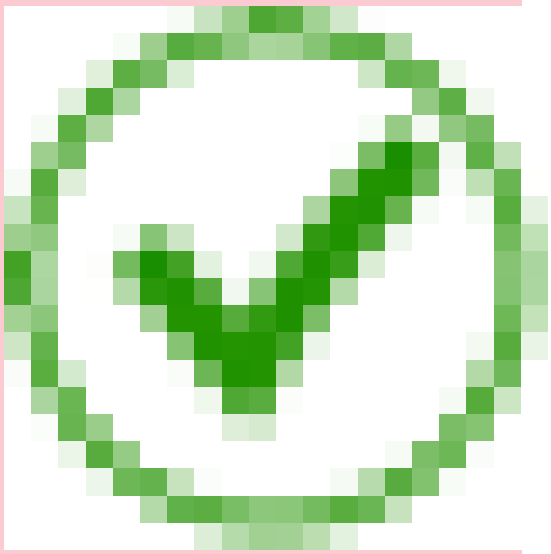
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul_conta
표준화된 심각성 맵			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned**

다음에 대한 모듈 액세스: **sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned**

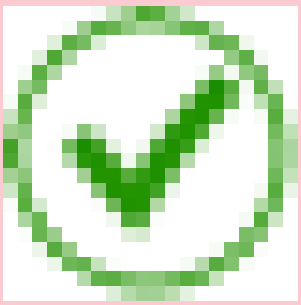
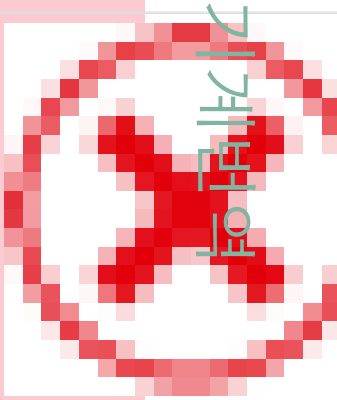
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_assig
(메인 앱 그룹)			
개요			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned**

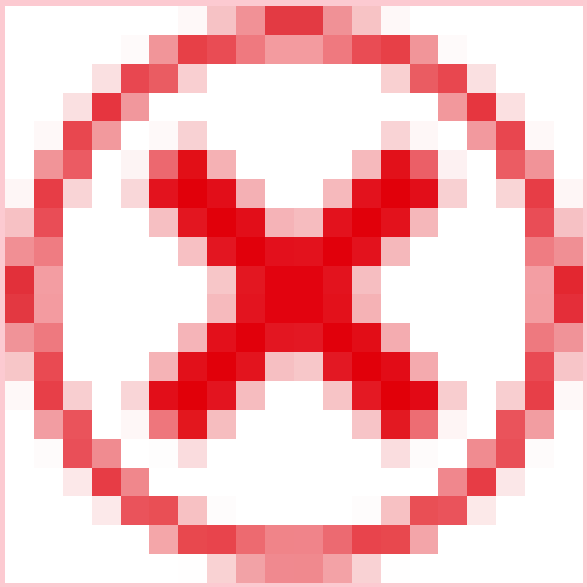
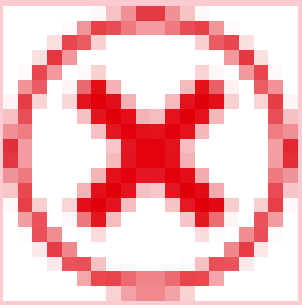
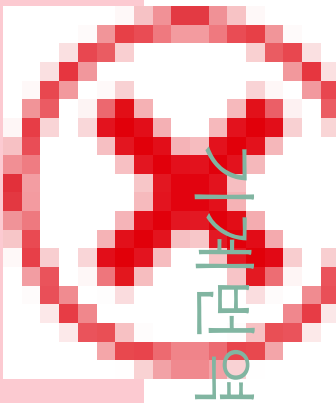
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_assig
내 승인			
컨테이너 취약한 항목			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_assig
나에게 할당됨			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_assig
사용자 그룹에 할당됨			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned**

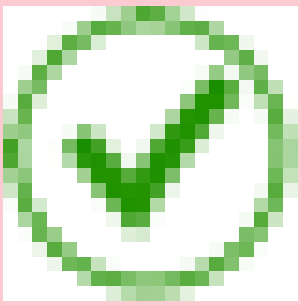
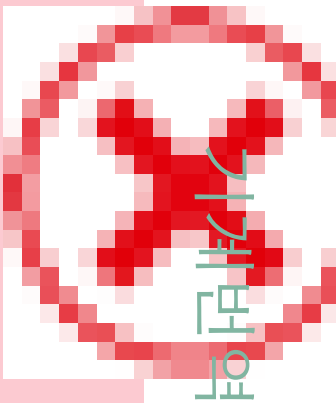
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_assig
중요 및 높은 위험			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned**

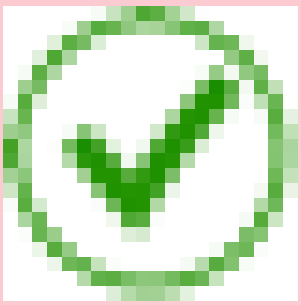
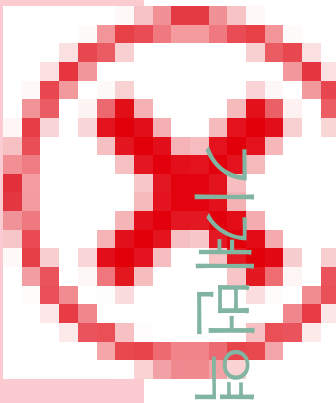
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_assig
악용 가능			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned**

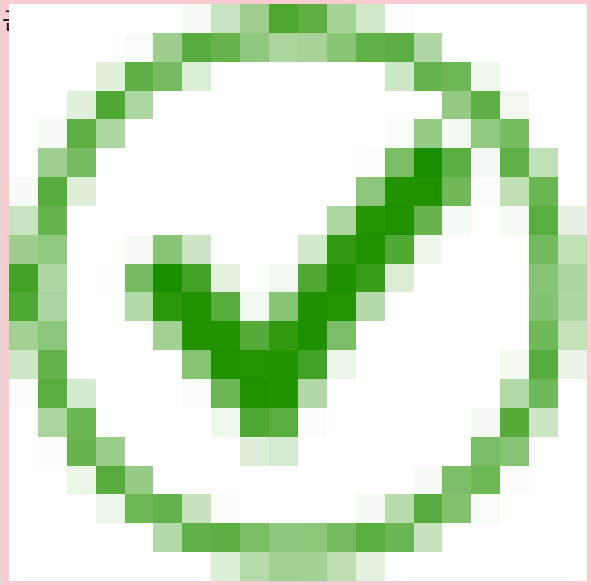
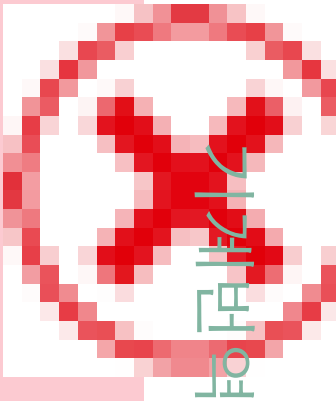
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_assig
대상에 접			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned**

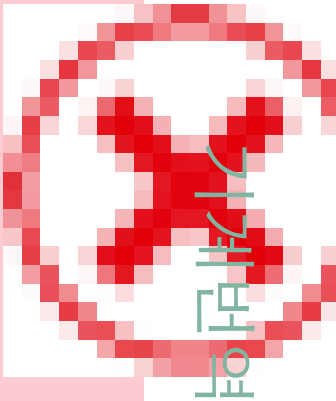
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_assig
누락된 대상			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned**

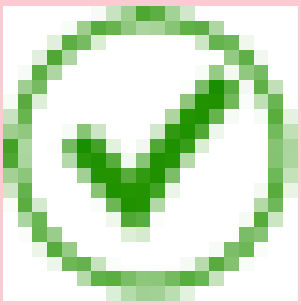
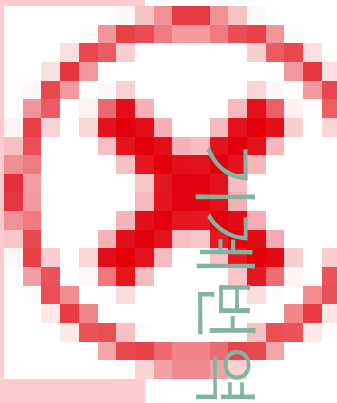
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_assig
모두			
라이브러리			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned**

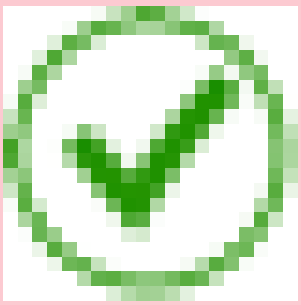
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_assig
NVD			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned**

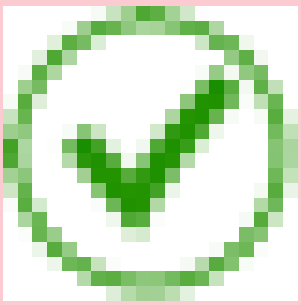
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_assig
외부 공급업체			
관리			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned**

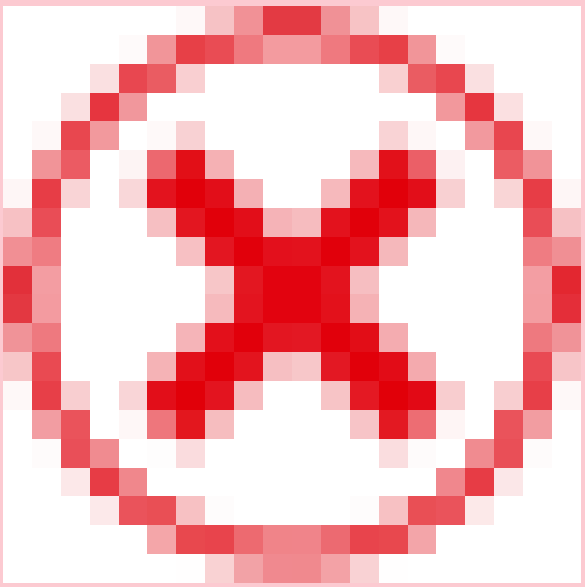
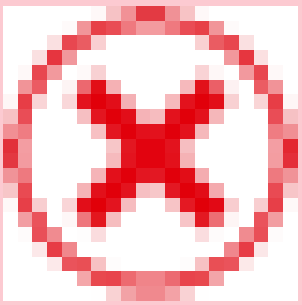
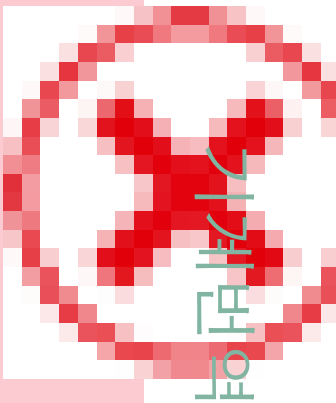
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_assig
담당 규칙			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned**

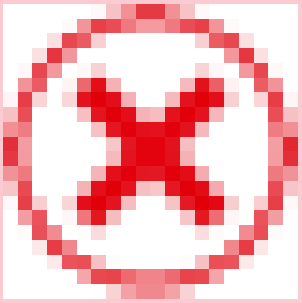
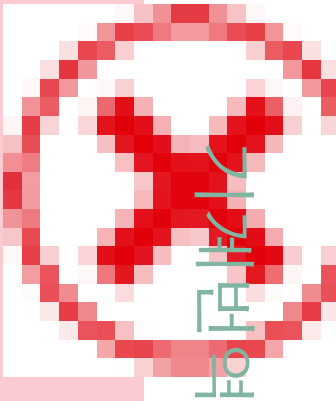
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_assig
취약성 계산기			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned**

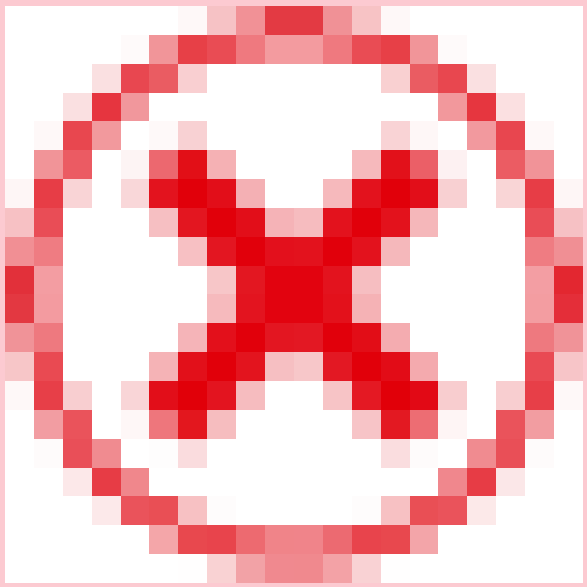
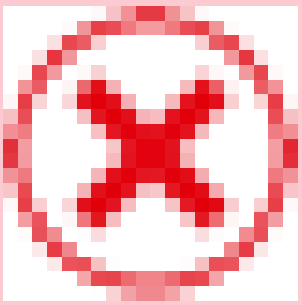
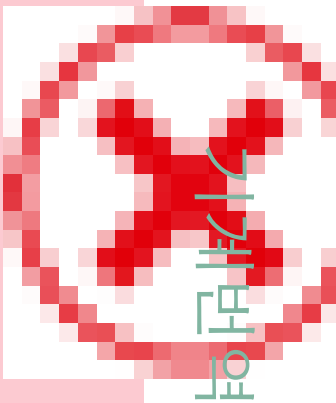
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_assig
정정 대상 규칙			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned**

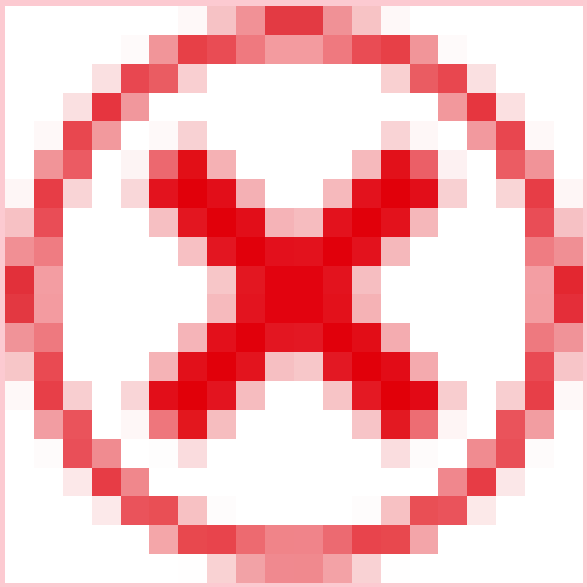
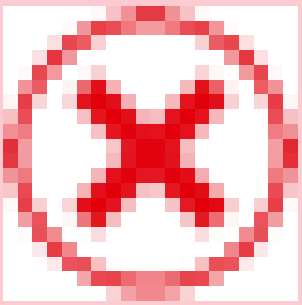
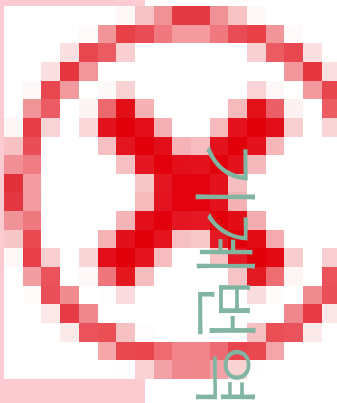
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_assig
VI 세분성 구성			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned**

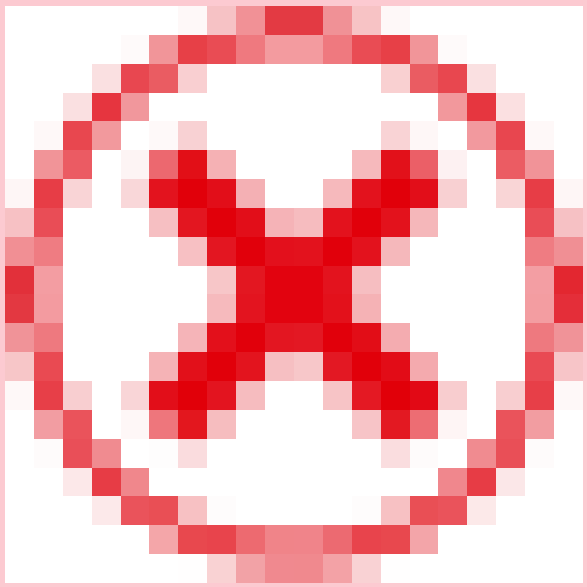
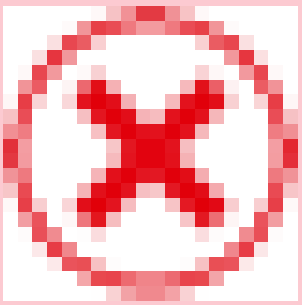
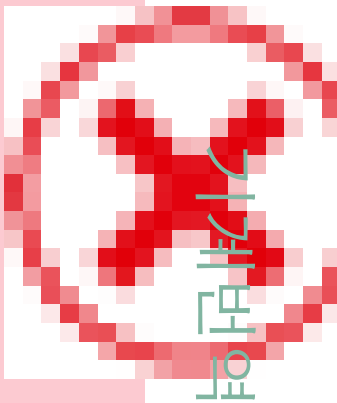
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_assig
예외 규칙			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned**

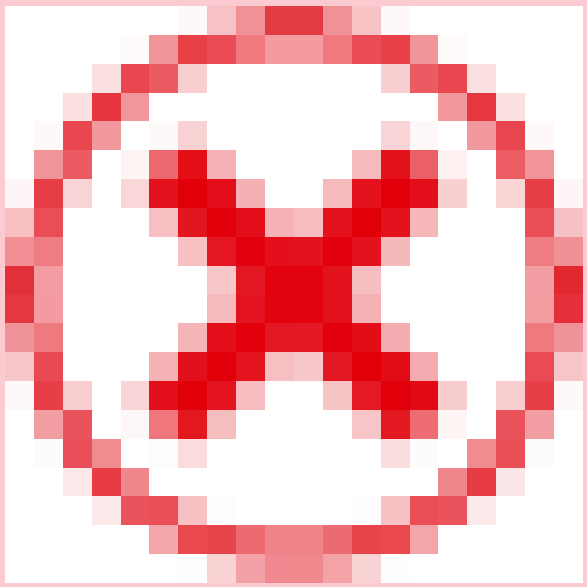
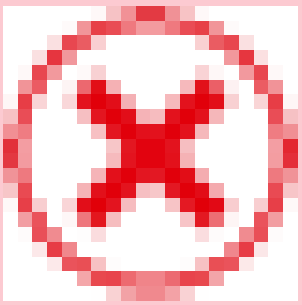
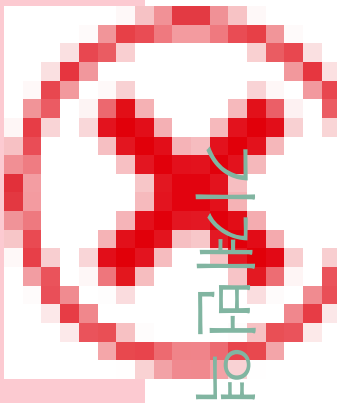
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_assig
승인 규칙			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned**

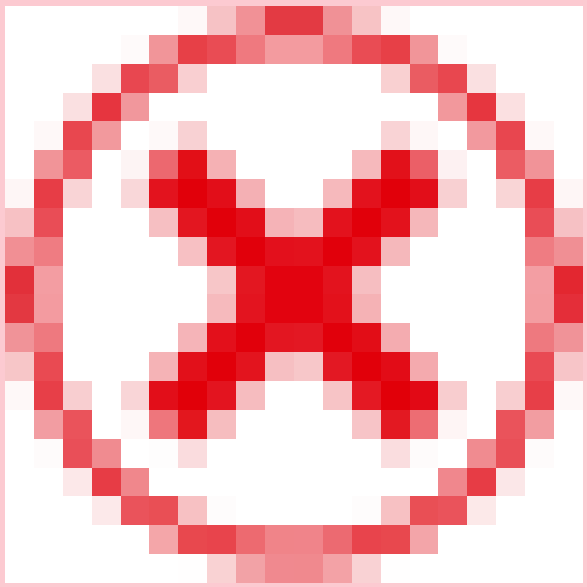
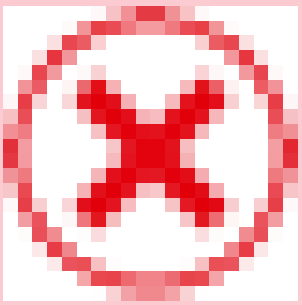
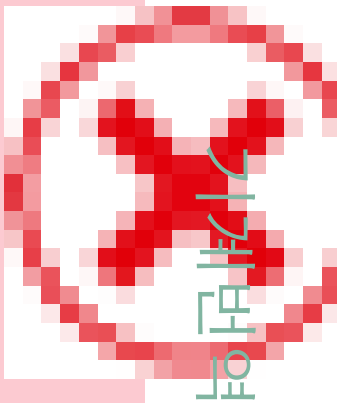
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_assig
컨테이너 보안 통합			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned**

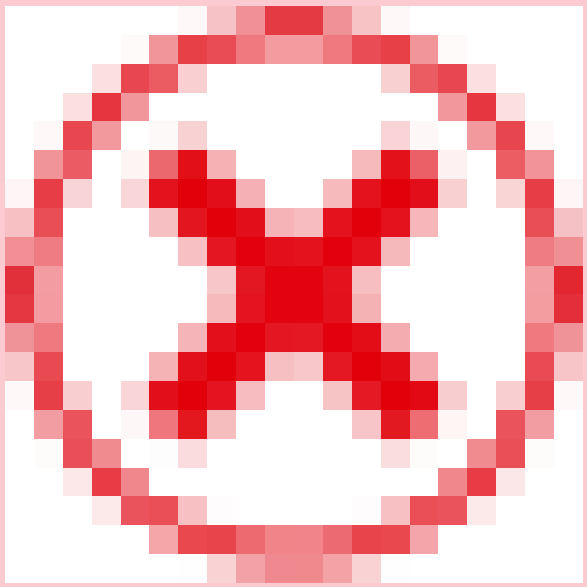
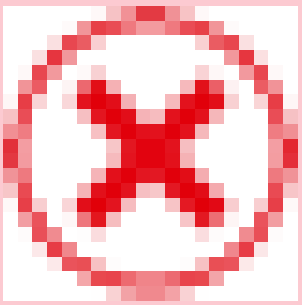
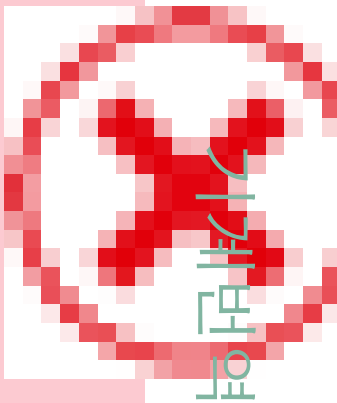
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_assig
취약한 항목 자동 닫기			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned**

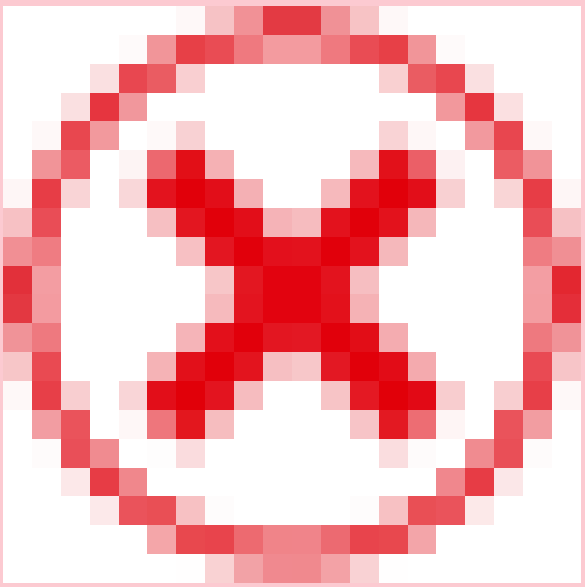
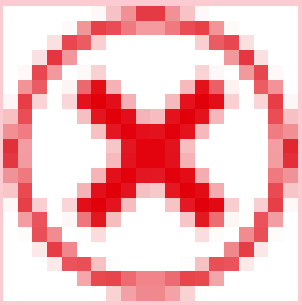
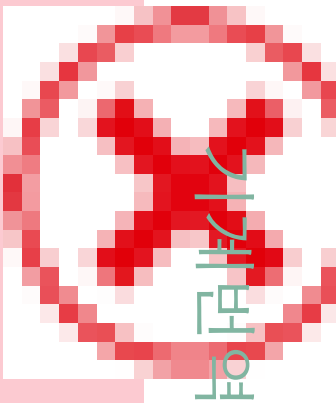
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

모듈	sn_vul_container.manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_assig
표준화된 심각성 맵			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.read_auto_exception_rule**

다음에 대한 모듈 액세스: **sn_vul_container.read_auto_exception_rule**

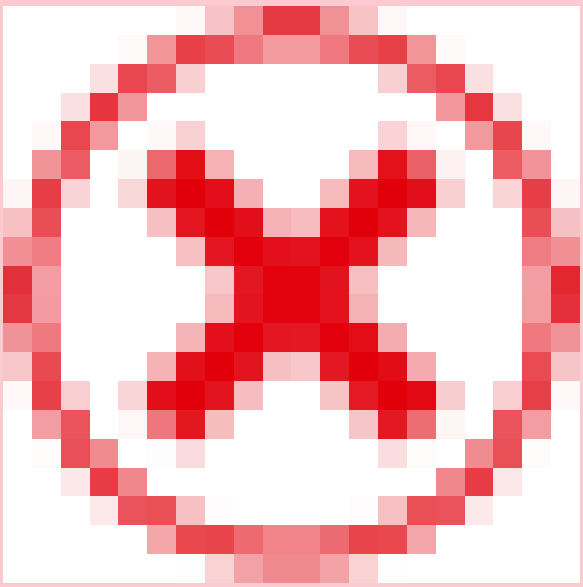
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

모듈	sn_vul_container.read_auto_exception_rule
(메인 앱 그룹)	
개요	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.read_auto_exception_rule**

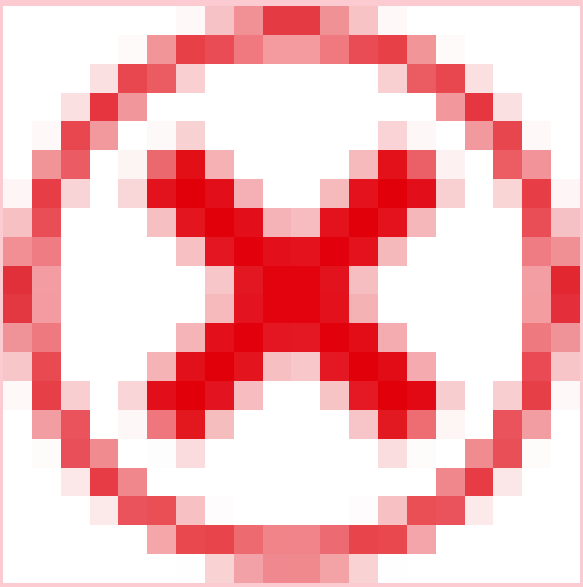
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

모듈	sn_vul_container.read_auto_exception_rule
내 승인	
컨테이너 취약한 항목	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.read_auto_exception_rule**

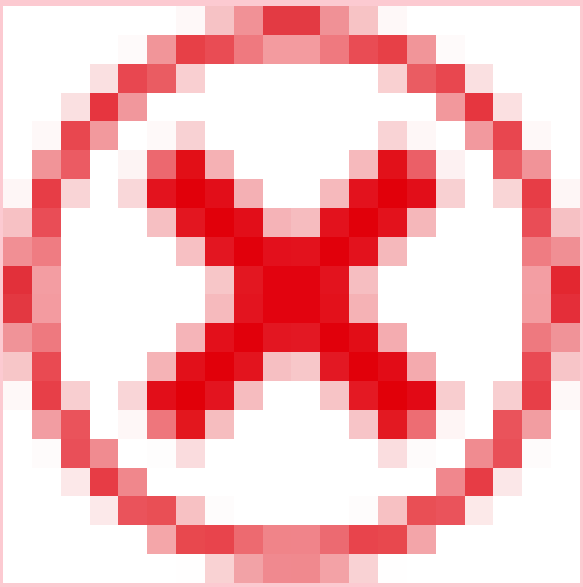
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

모듈	sn_vul_container.read_auto_exception_rule
나에게 할당됨	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.read_auto_exception_rule**

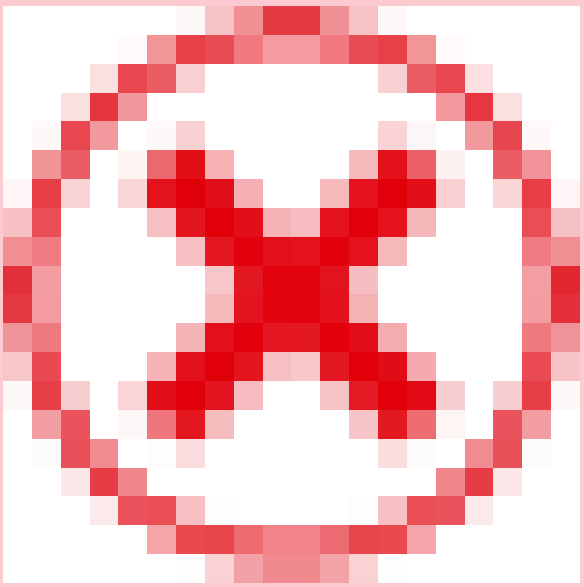
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

모듈	sn_vul_container.read_auto_exception_rule
사용자 그룹에 할당됨	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.read_auto_exception_rule**

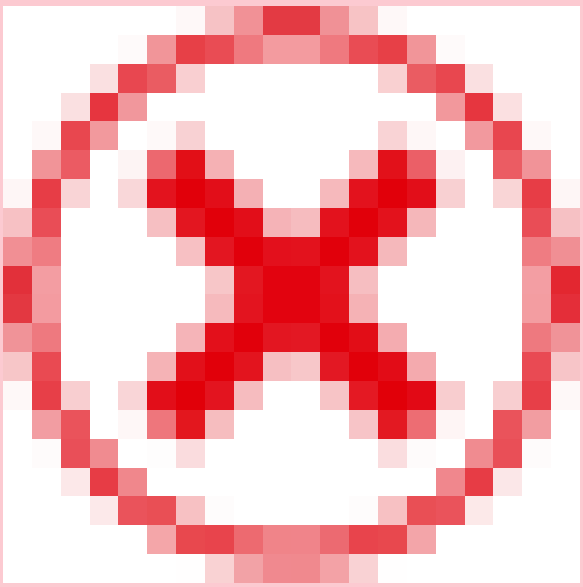
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

모듈	sn_vul_container.read_auto_exception_rule
중요 및 높은 위험	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.read_auto_exception_rule**

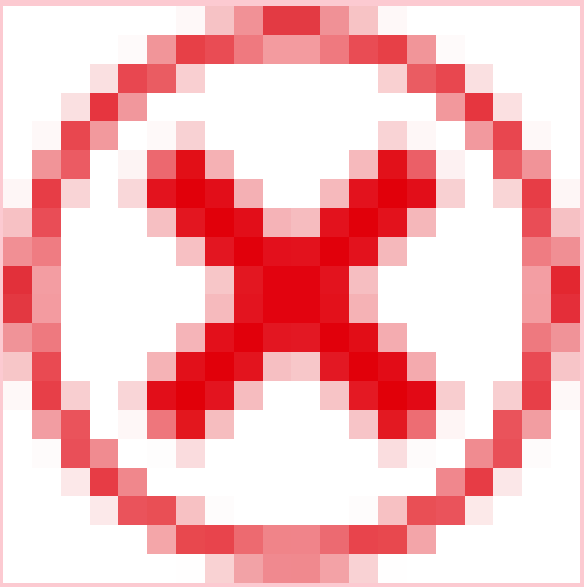
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

모듈	sn_vul_container.read_auto_exception_rule
악용 가능	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.read_auto_exception_rule**

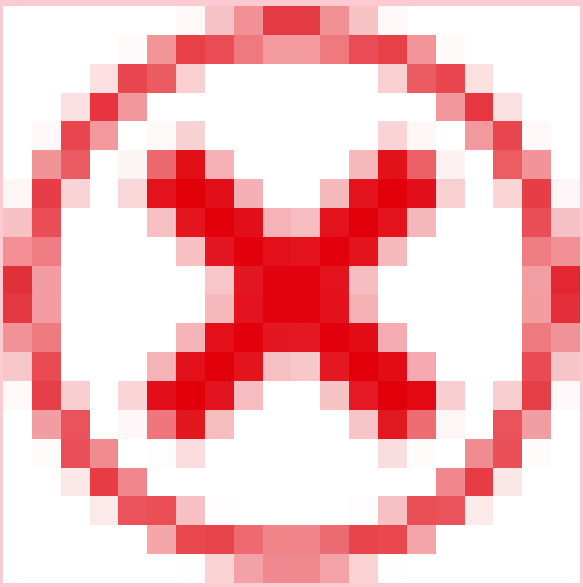
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

모듈	sn_vul_container.read_auto_exception_rule
대상에 접근 중	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.read_auto_exception_rule**

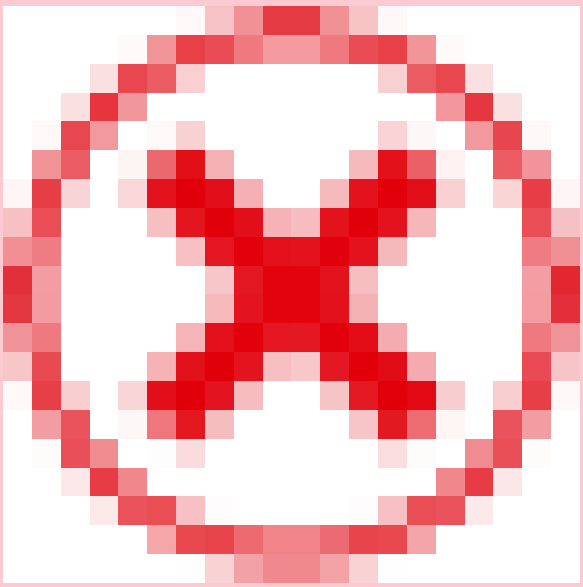
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

모듈	sn_vul_container.read_auto_exception_rule
누락된 대상	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.read_auto_exception_rule**

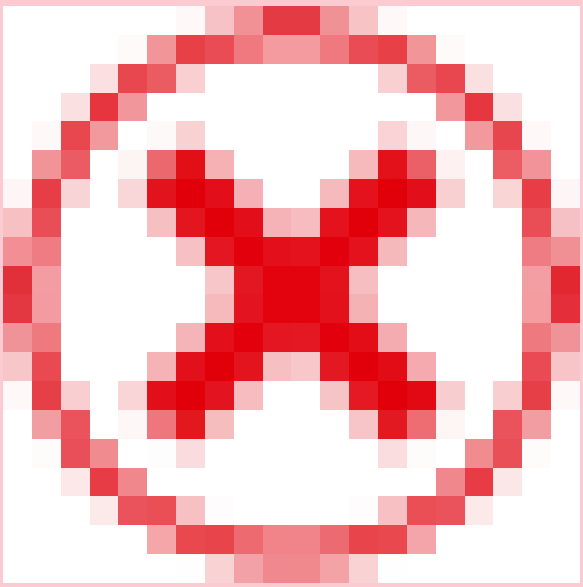
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

모듈	sn_vul_container.read_auto_exception_rule
모두	
라이브러리	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.read_auto_exception_rule**

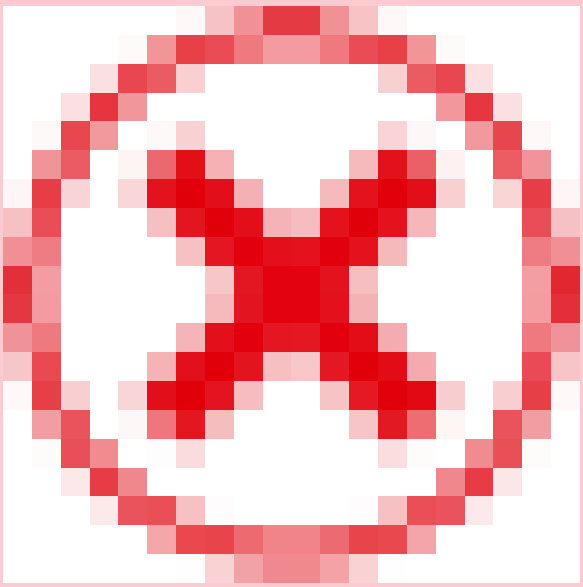
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

모듈	sn_vul_container.read_auto_exception_rule
NVD	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.read_auto_exception_rule**

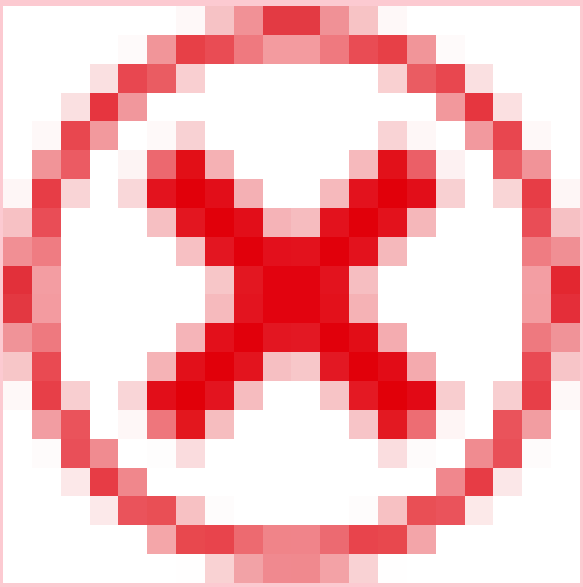
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

모듈	sn_vul_container.read_auto_exception_rule
외부 공급업체	
관리	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.read_auto_exception_rule**

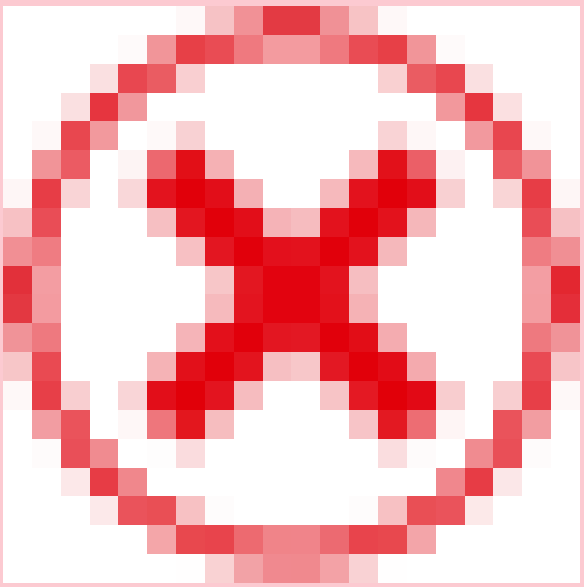
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

모듈	sn_vul_container.read_auto_exception_rule
담당 규칙	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.read_auto_exception_rule**

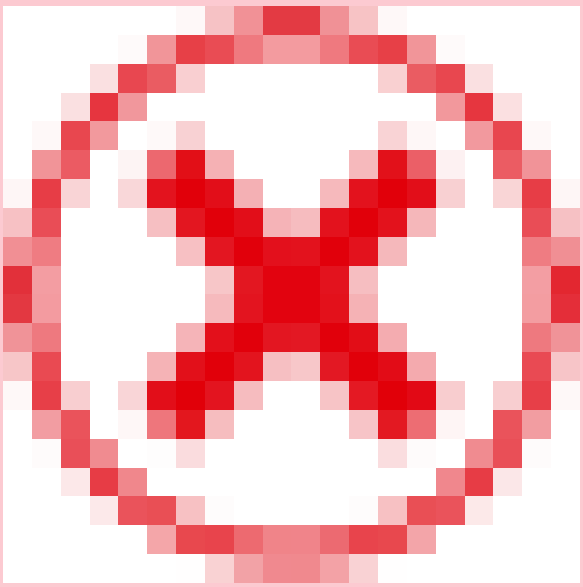
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

모듈	sn_vul_container.read_auto_exception_rule
취약성 계산기	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.read_auto_exception_rule**

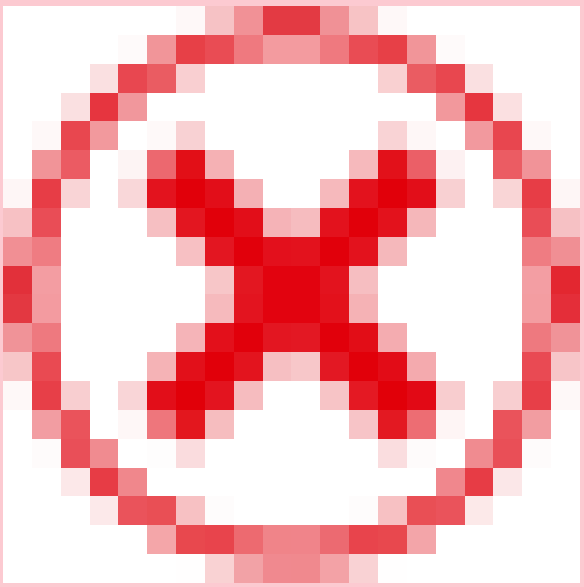
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

모듈	sn_vul_container.read_auto_exception_rule
정정 대상 규칙	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.read_auto_exception_rule**

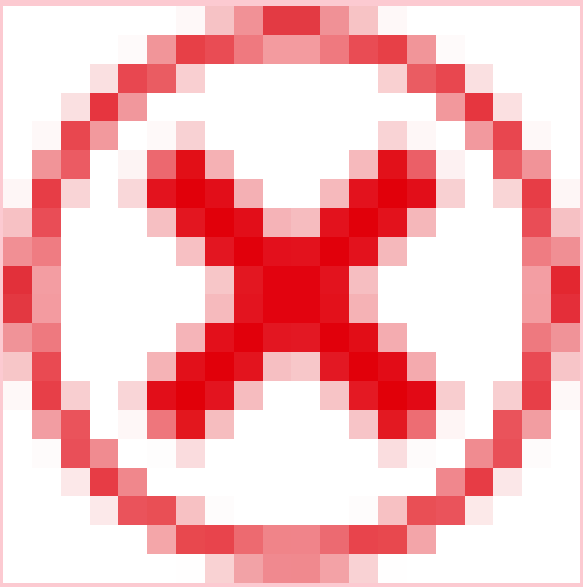
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

모듈	sn_vul_container.read_auto_exception_rule
VI 세분성 구성	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.read_auto_exception_rule**

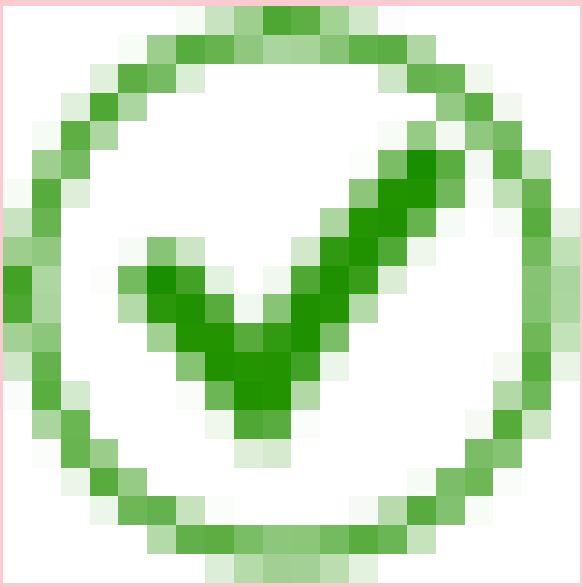
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

모듈	**sn_vul_container.read_auto_exception_rule**
예외 규칙	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.read_auto_exception_rule**

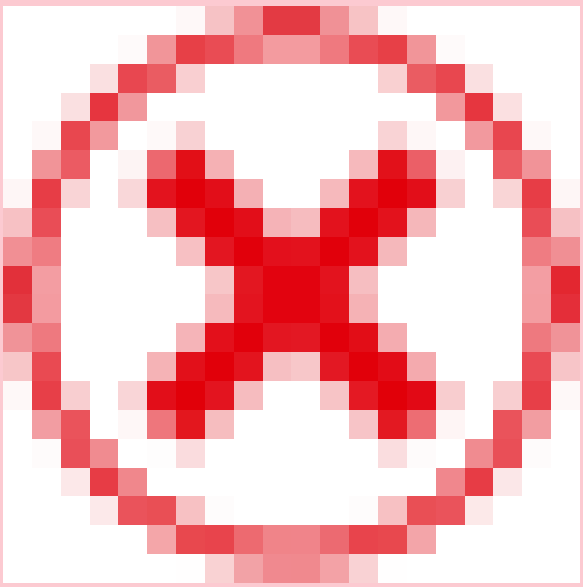
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

모듈	sn_vul_container.read_auto_exception_rule
승인 규칙	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.read_auto_exception_rule**

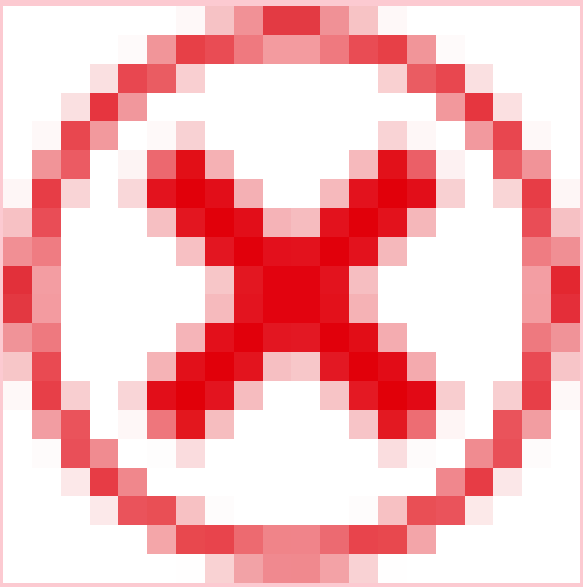
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

모듈	sn_vul_container.read_auto_exception_rule
컨테이너 보안 통합	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.read_auto_exception_rule**

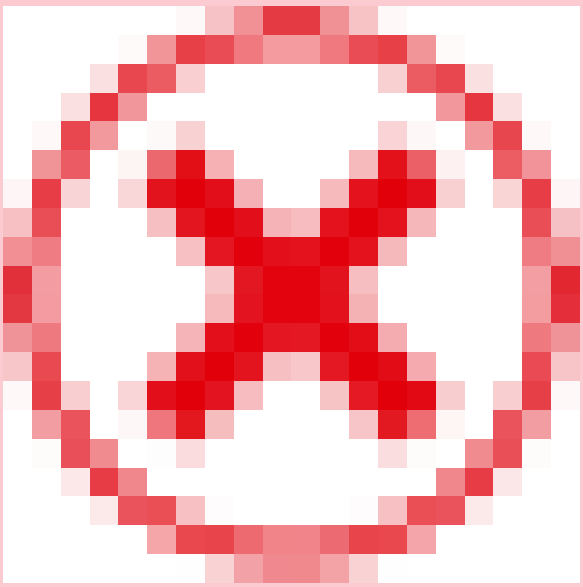
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

모듈	sn_vul_container.read_auto_exception_rule
취약한 항목 자동 닫기	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul_container.read_auto_exception_rule**

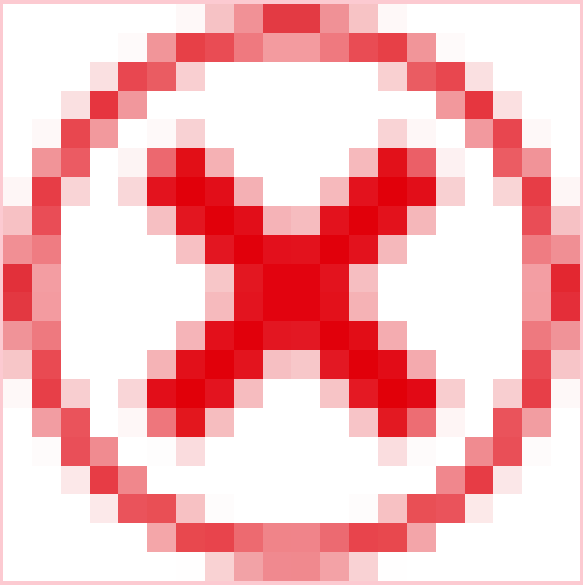
다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

모듈	**sn_vul_container.read_auto_exception_rule**
표준화된 심각성 맵	

〔End〕

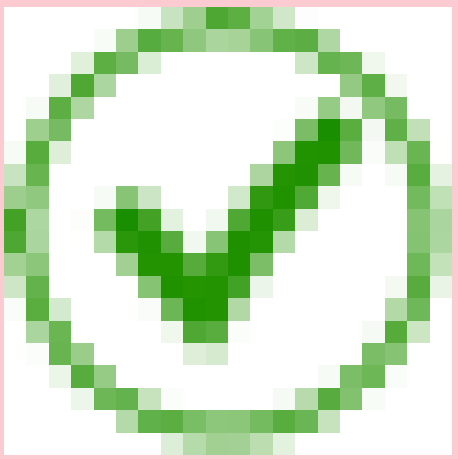
〔store-future: BEGIN review〕

DLP 관리를 위한 역할별 모듈 액세스

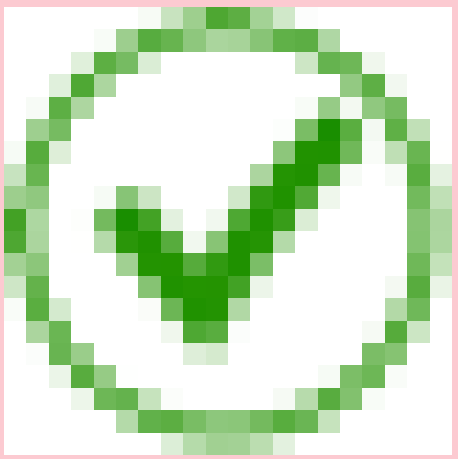
DLP 관리의 경우 특정 역할에서 액세스할 수 있는 메뉴 항목을 참조하십시오.

모듈	sn_dlir.분석자
(메인 앱 그룹)	

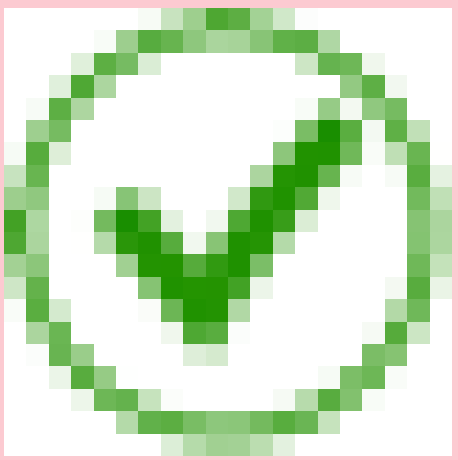
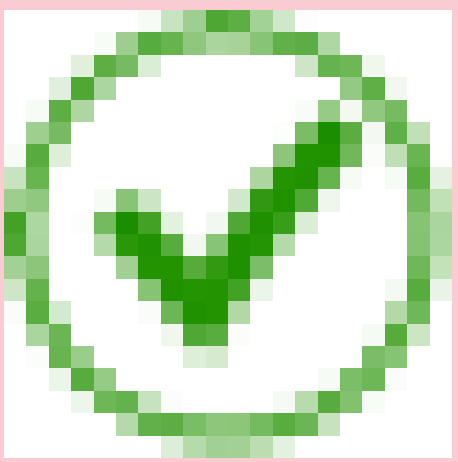
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈	sn_dlir.분석자
기본 구성	
담당 규칙	
응답 기한 날짜 규칙	

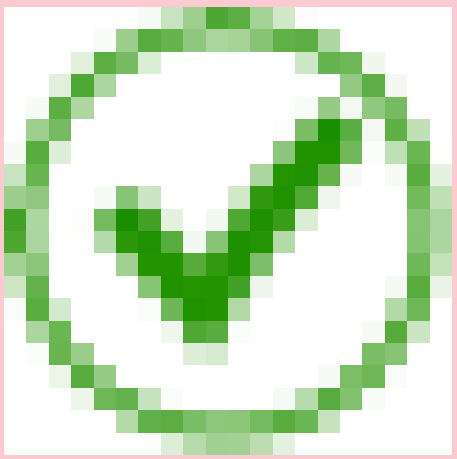
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈	sn_dlir.분석자
이메일 템플릿	
평가	
인시던트 응답 옵션	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈	sn_dlir.분석자
연령 차트 구성	
위임 구성	
사용자 지정 상태	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈	sn_dlir.분석자
반복 위반 식별 규칙	
사용자 지정 필드	
고급 설정	
인시던트 접근 제한	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

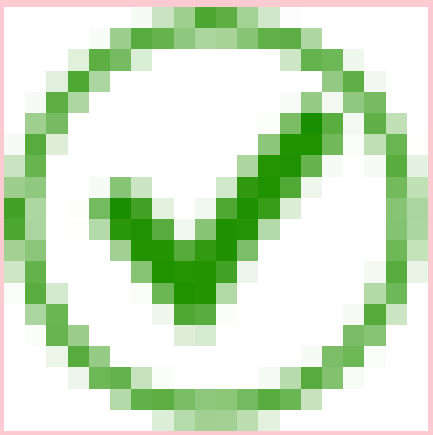
모듈	sn_dlir.분석자
기록 수준 제한	
필드 수준 제한	

〔End〕

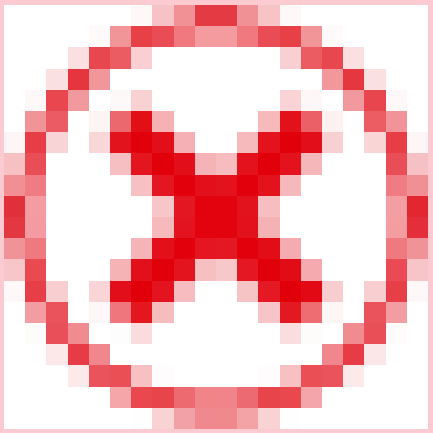
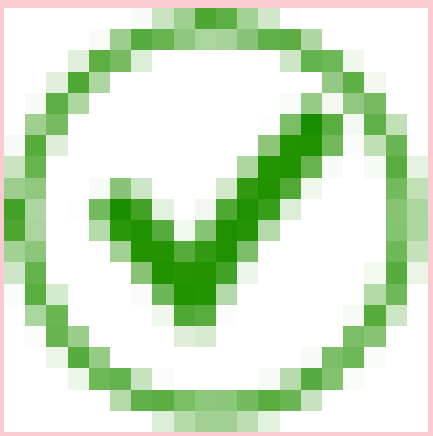
〔store-future: BEGIN review〕

DLP 인시던트 관리에 대한 역할별 모듈 액세스

DLP 인시던트 관리의 경우 특정 역할로 액세스할 수 있는 메뉴 항목을 참조하십시오.

모듈	sn_dlir.분석자
(메인 앱 그룹)	
DLP 운영 포털	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

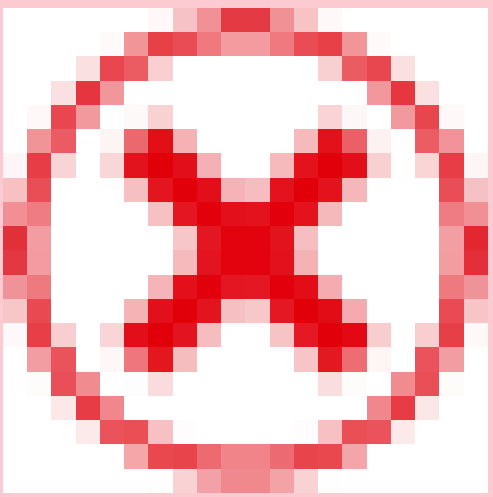
모듈	sn_dlir.분석자
DLP 최종 사용자 포털	
DLP 대시보드	

〔End〕

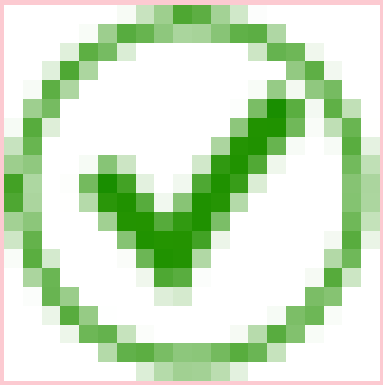
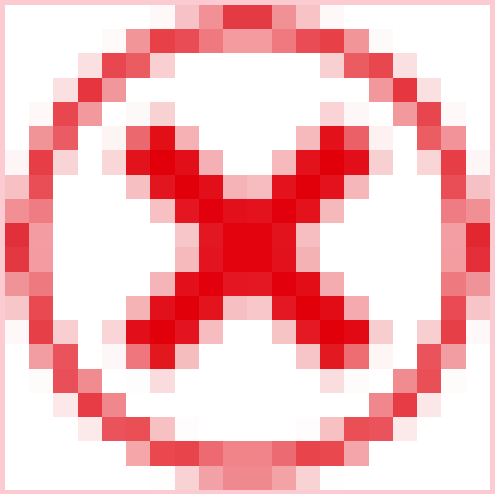
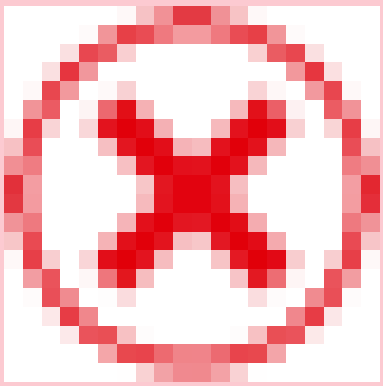
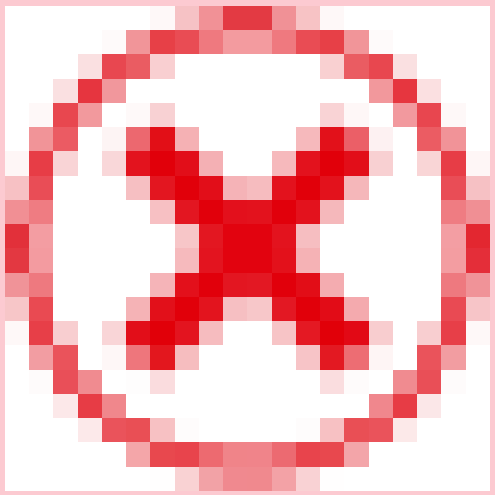
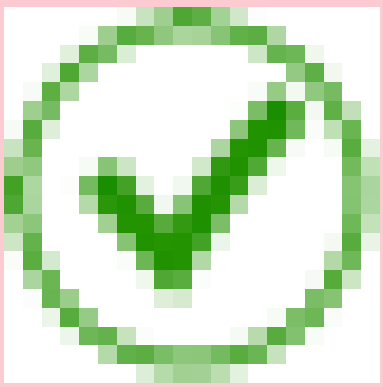
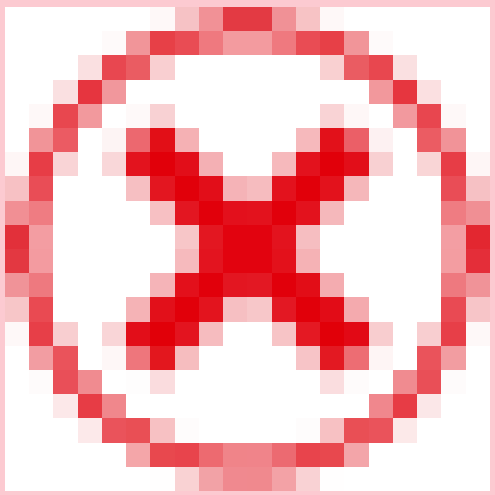
〔store-future: BEGIN review〕

데이터 인증을 위한 역할별 모듈 액세스

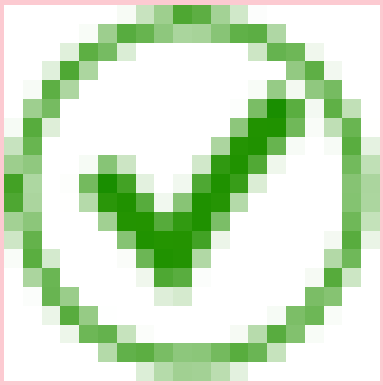
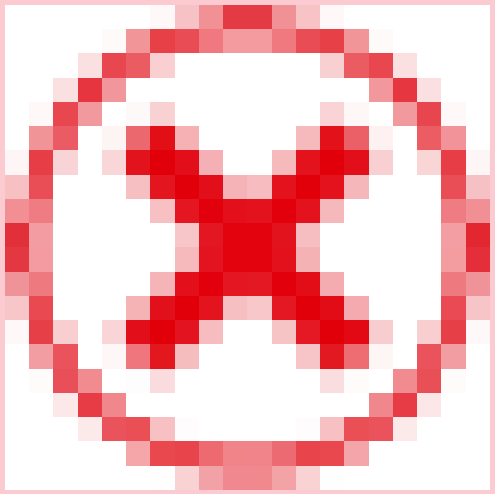
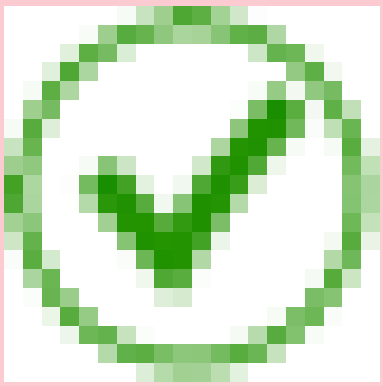
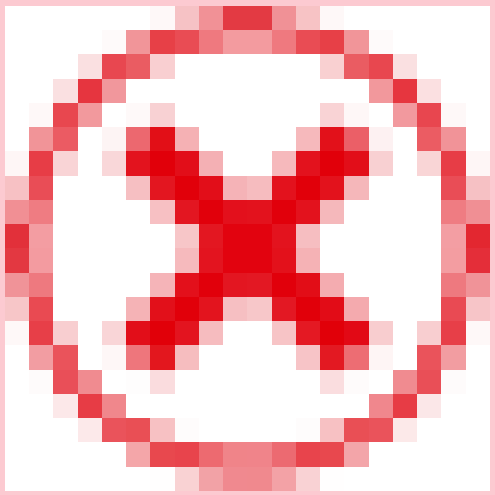
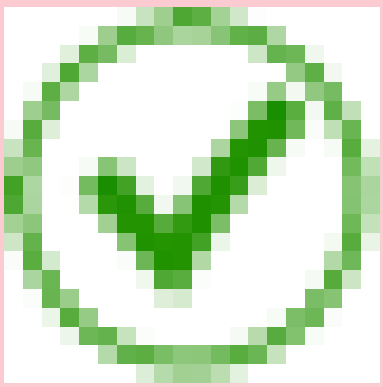
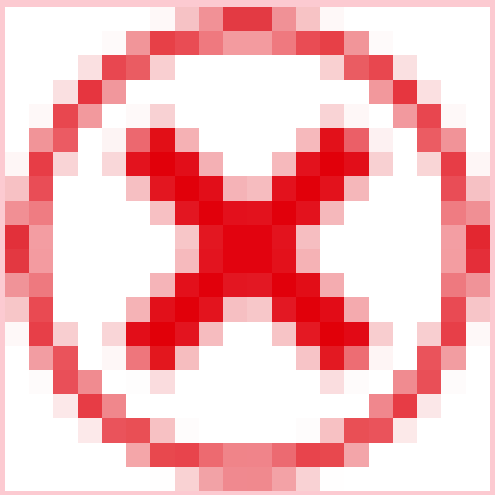
데이터 인증의 경우 특정 역할이 액세스할 수 있는 메뉴 항목을 참조하십시오.

모듈	certification_admin	certification_filter_admin
(메인 앱 그룹)		
개요		

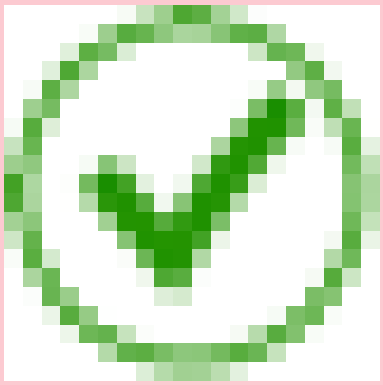
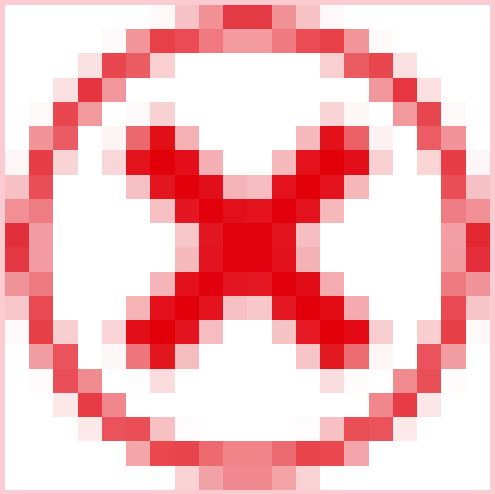
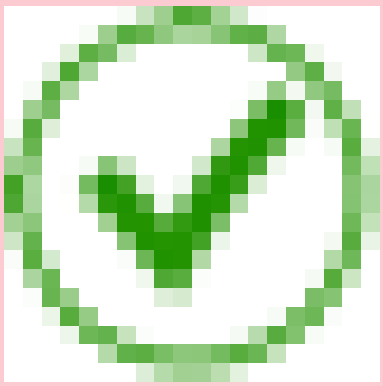
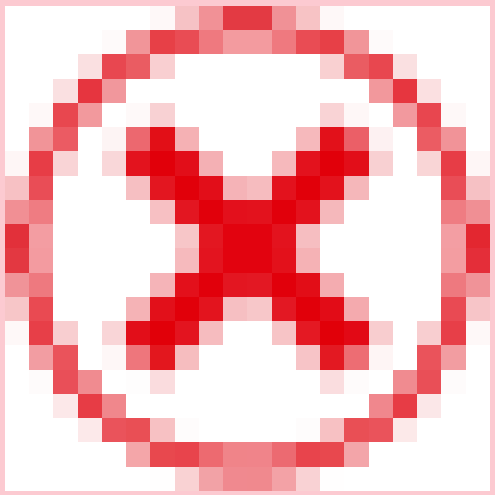
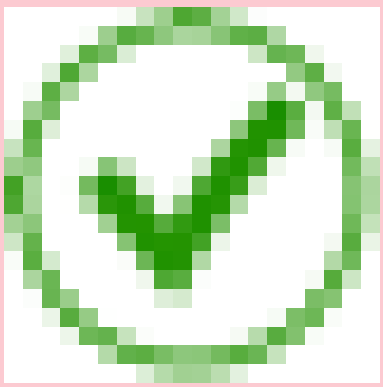
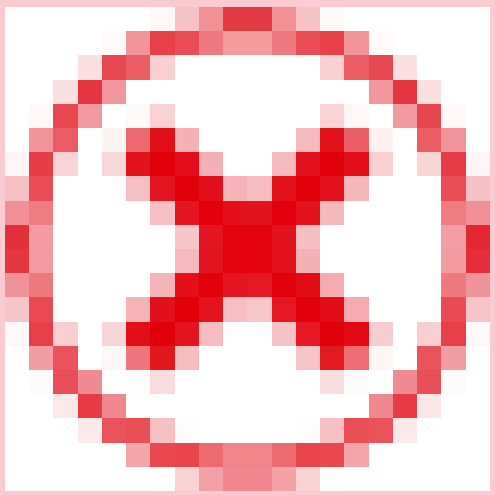
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈	certification_admin	certification_filter_admin
시작		
작업		
내 작업		
오픈		

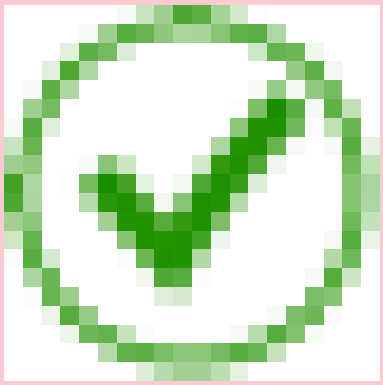
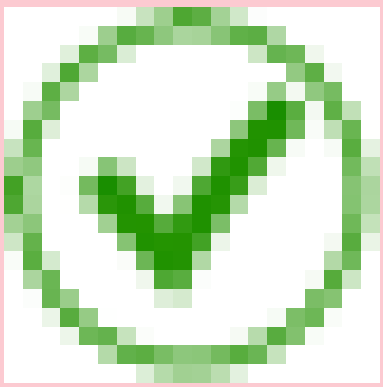
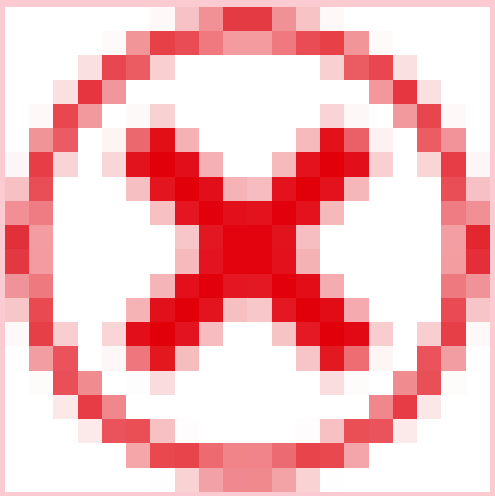
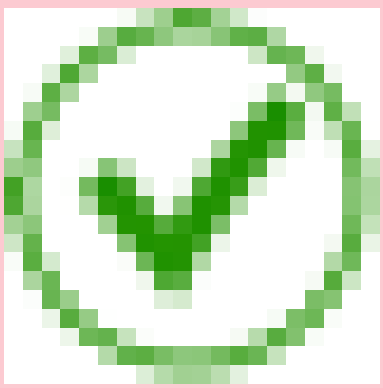
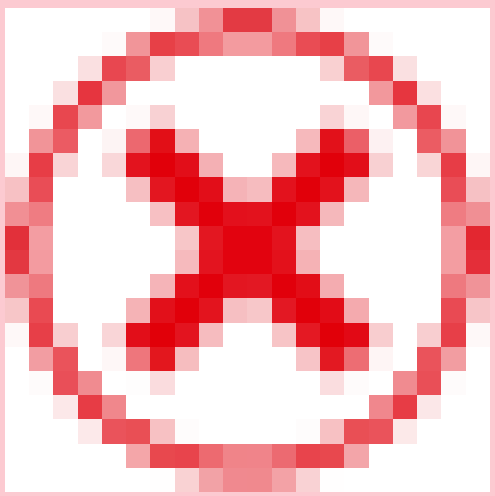
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈	certification_admin	certification_filter_admin
모든 작업		
인증		
인증됨		
보류 중		

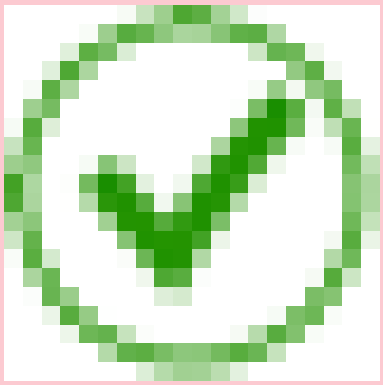
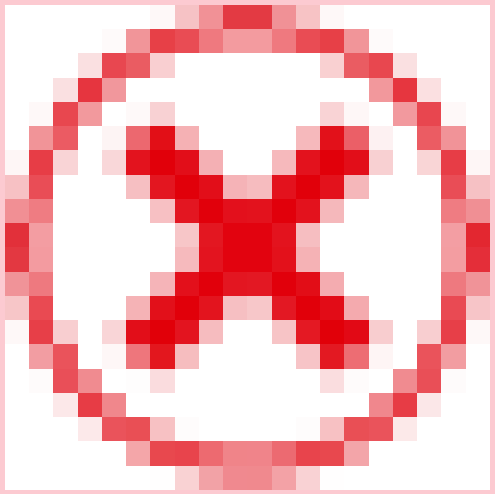
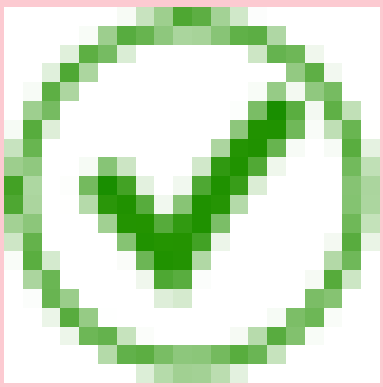
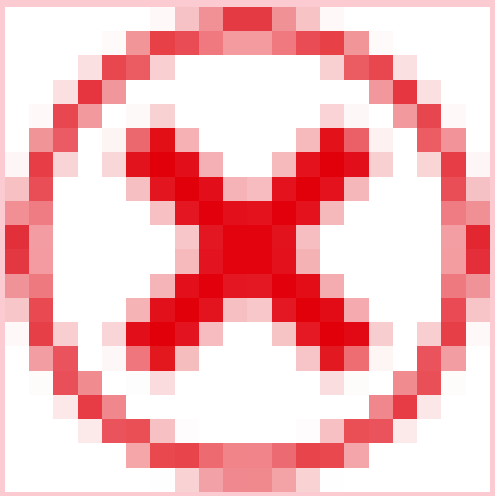
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈	certification_admin	certification_filter_admin
모두		
일정		
새로 작성		
일정 정의		

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈	certification_admin	certification_filter_admin
인증 필터		
인스턴스		
감사 결과		
감사		

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

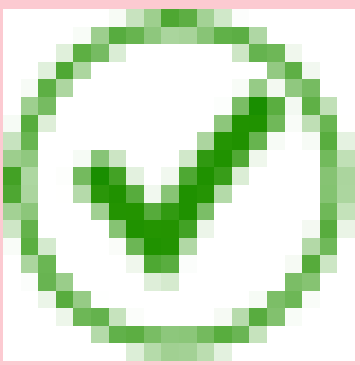
모듈	certification_admin	certification_filter_admin
감사 정의		
감사 인스턴스		

〔End〕

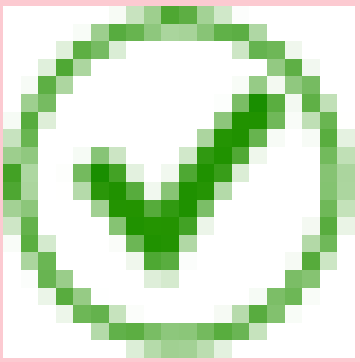
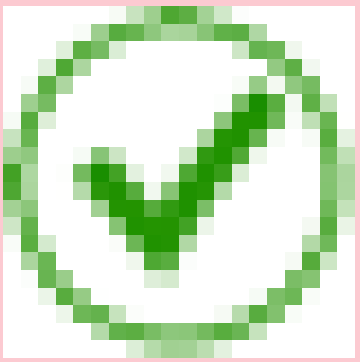
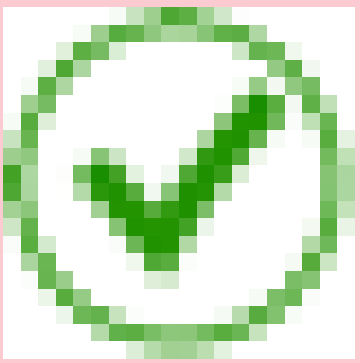
〔store-future: BEGIN review〕

IBM QRadar Integration에 대한 역할별 모듈 액세스

IBM QRadar Integration의 경우 특정 역할이 액세스할 수 있는 메뉴 항목을 참조하십시오.

모듈	sn_si.analyst
(메인 앱 그룹)	
IBM QRadar 프로파일	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈	sn_si.analyst
IBM QRadar Offense 임포트	
작업에 대한 IBM QRadar 위반	
IBM QRadar 필드 변환	
IBM QRadar 통합 설정	

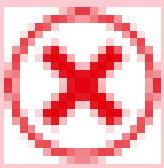
〔End〕

〔store-future: BEGIN review〕

MISP 통합을 위한 역할별 모듈 액세스

MISP 통합의 경우 특정 역할로 접근할 수 있는 메뉴 항목을 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈	sn_si.관리자	sn_si.분석자	sn_ti.관리자	sn_ti.읽다	sn_ti.쓰다
(메인 앱 그룹)					
통합 설정					
사이팅 검색 구성					
자동 이벤트 작성 프로파일					
자동 이벤트 작성 큐					
MISP 이벤트 데이터					
연결된 MISP 이벤트					
MISP 사용자 정보					

〔End〕

〔store-future: BEGIN review〕

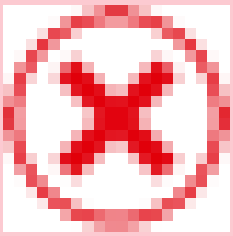
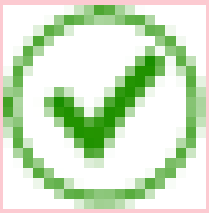
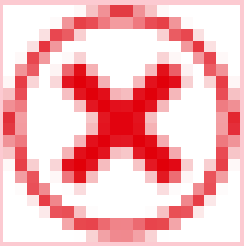
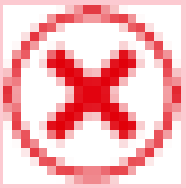
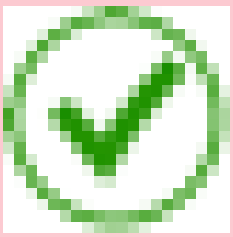
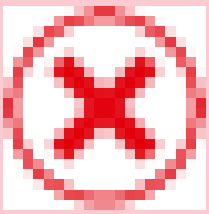
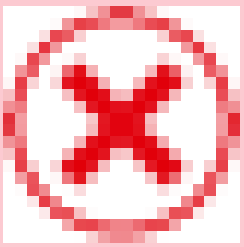
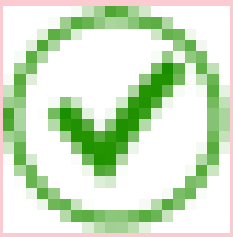
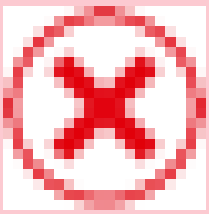
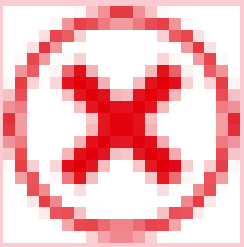
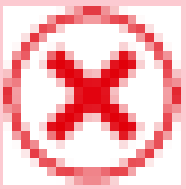
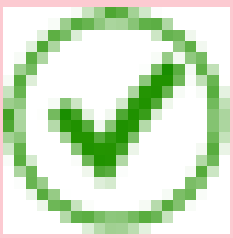
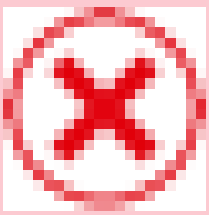
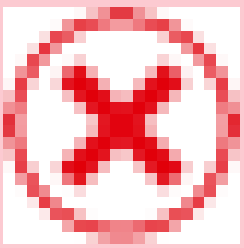
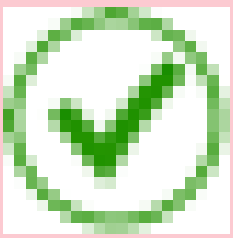
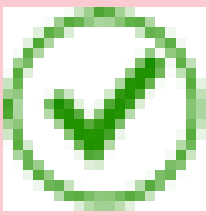
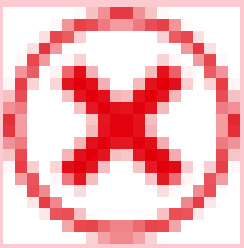
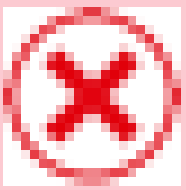
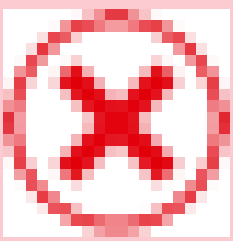
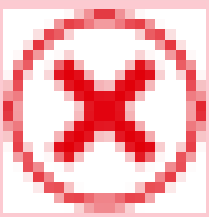
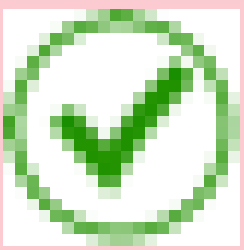
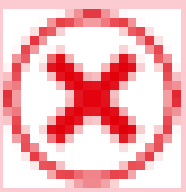
Microsoft Azure Defender for IoT에 대한 역할별 모듈 액세스

Microsoft Azure Defender for IoT의 경우 특정 역할에서 액세스할 수 있는 메뉴 항목을 참조하세요.

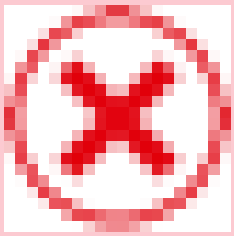
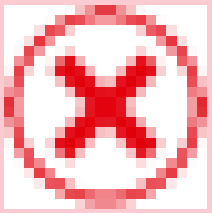
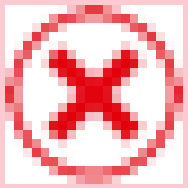
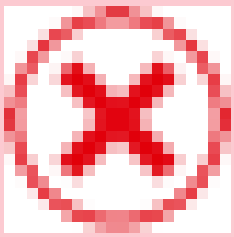
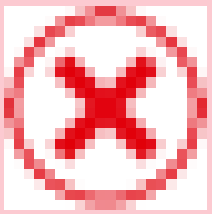
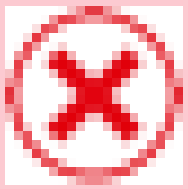
모듈	cmdb_inst_admin	cmdb_ot_admin	connection_admin	import_admin
(메인 앱 그룹)				

기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈	cmdb_inst_admin	cmdb_ot_admin	connection_admin	import_admin
설정				
데이터 소스				
통합 허브 ETL				
일정 임포트				
속성				
연결 및 자격 증명				
연결 자격 증명 별칭				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

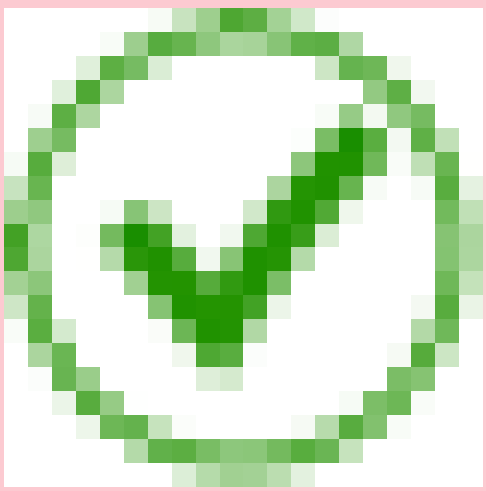
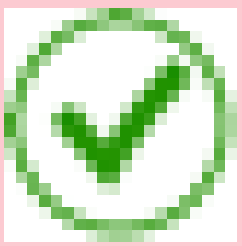
모듈	cmdb_inst_admin	cmdb_ot_admin	connection_admin	import_admin
자격 증명				
연결				

〔End〕

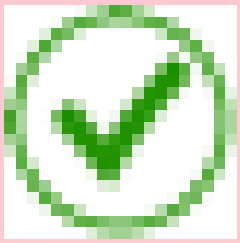
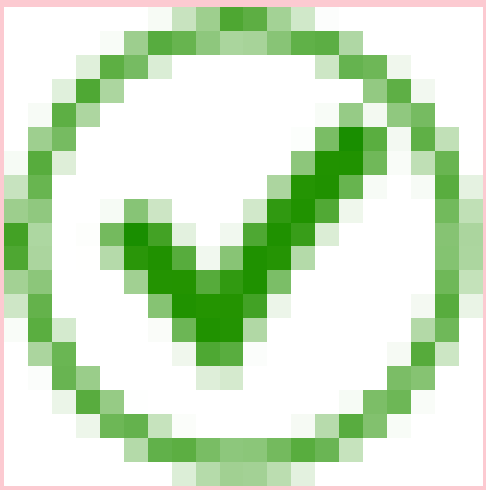
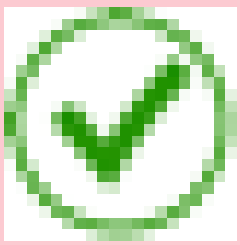
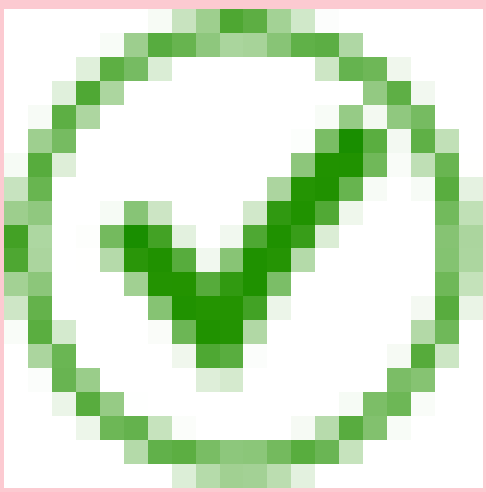
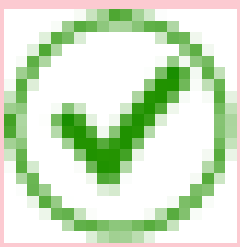
〔store-future: BEGIN review〕

Qualys 취약성 통합에 대한 역할별 모듈 액세스

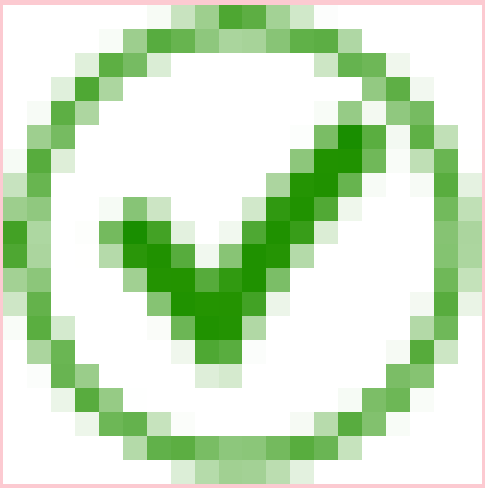
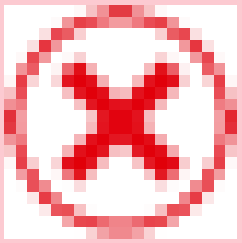
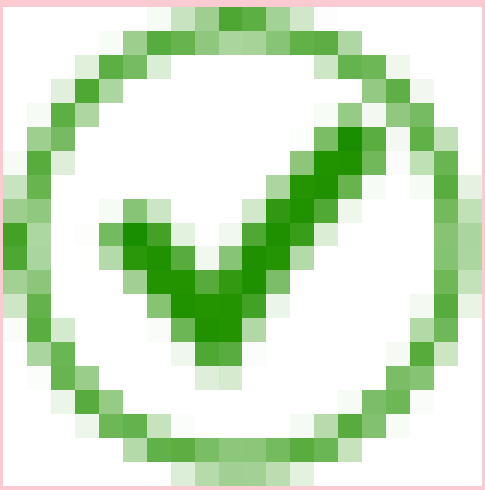
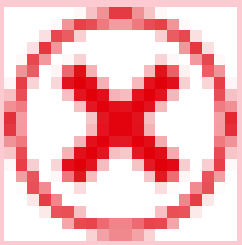
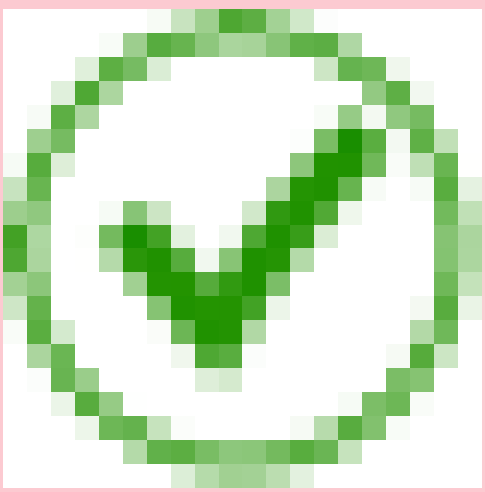
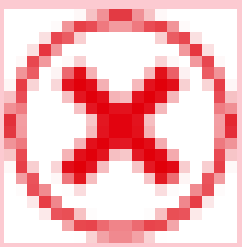
Qualys 취약성 통합의 경우 특정 역할로 액세스할 수 있는 메뉴 항목을 참조하십시오.

모듈	sn_vul.configure_qualys_integration	sn_vul_qualys.읽다
(메인 앱 그룹)		
개요		

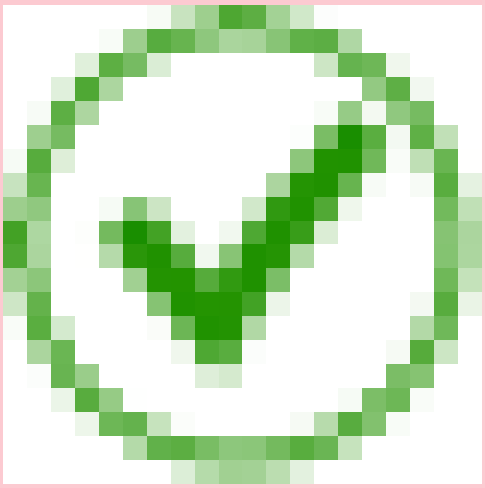
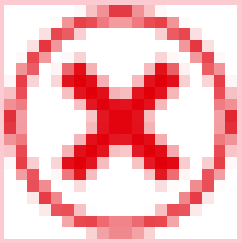
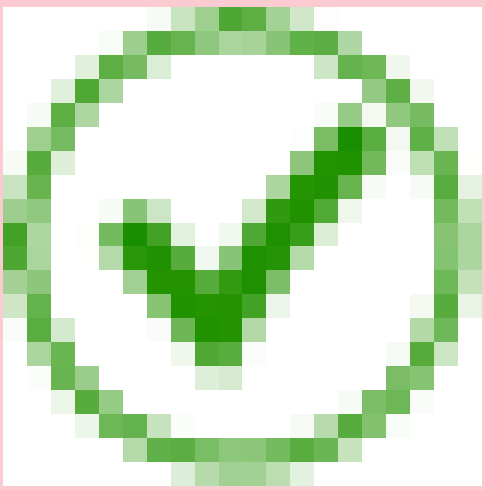
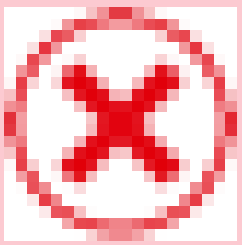
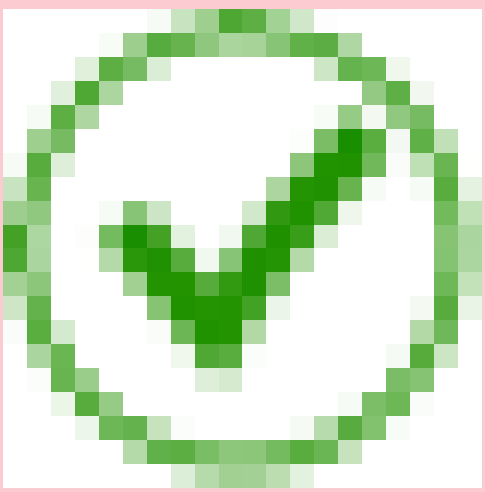
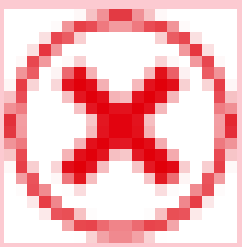
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈	sn_vul.configure_qualys_integration	sn_vul_qualys.읽다
통합 실행 상태		
스캐너 장치		
검색 목록		
관리		

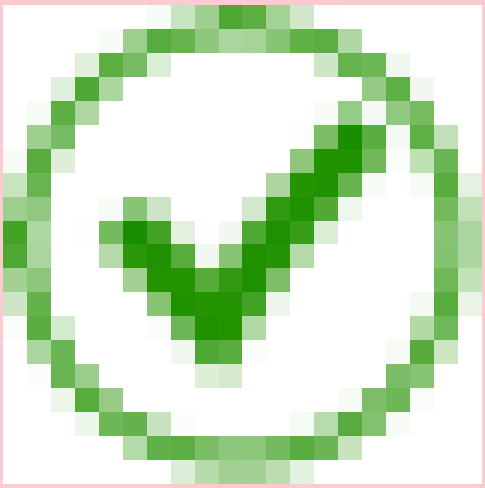
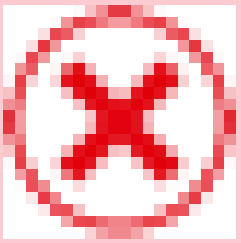
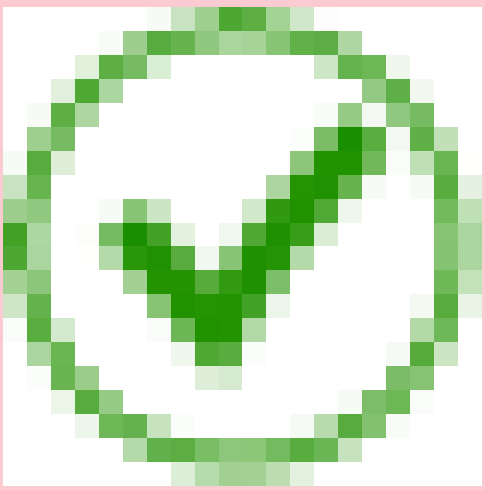
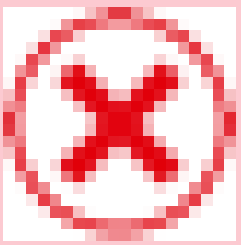
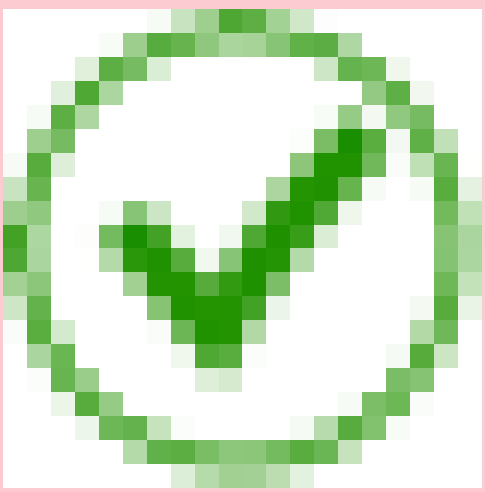
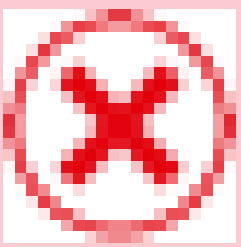
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈	sn_vul.configure_qualys_integration	sn_vul_qualys.읽다
통합 인스턴스		
기본 통합		
지원 통합		
임포트 세트 테이블		

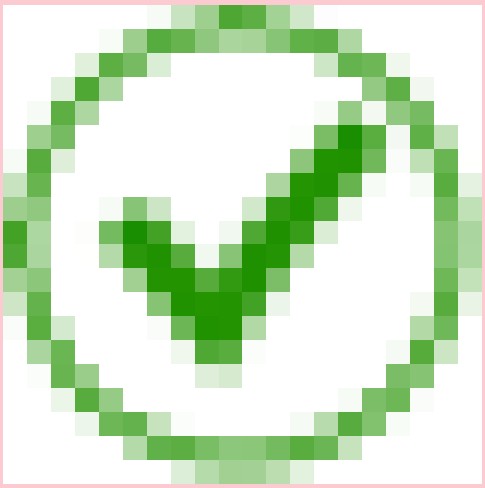
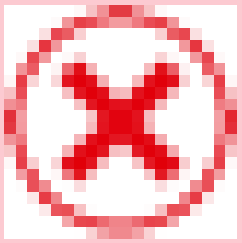
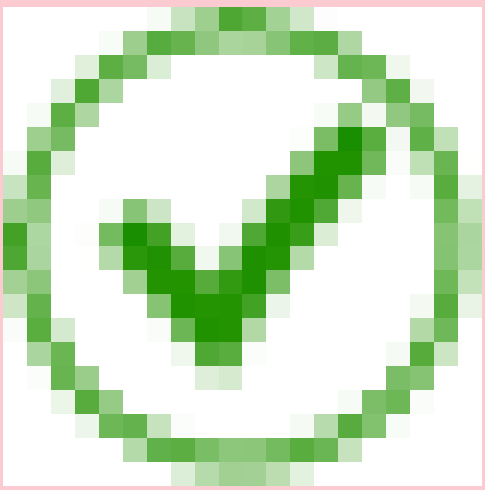
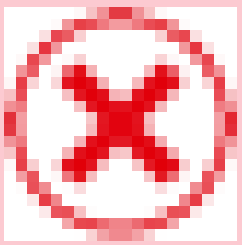
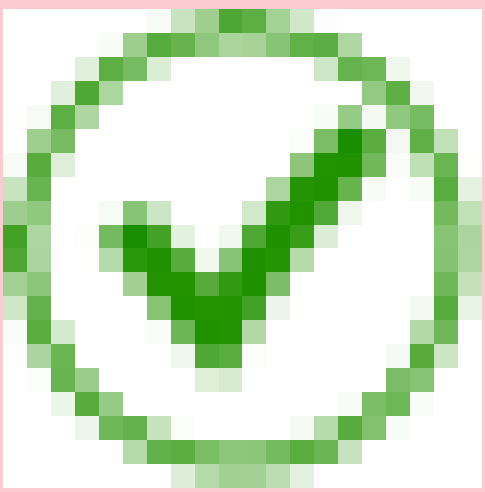
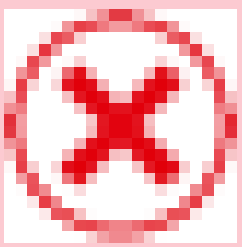
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈	sn_vul.configure_qualys_integration	sn_vul_qualys.읽다
호스트 임포트		
호스트 탐지 목록 임포트		
지식 임포트		

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈	**sn_vul.configure_qualys_integration**	sn_vul_qualys.읽다
티켓 목록 임포트		
동적 검색 목록 임포트		
정적 검색 목록 임포트		

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈	sn_vul.configure_qualys_integration	sn_vul_qualys.읽다
자산 그룹 임포트		
장치 임포트		
호스트 탐지 페이지 매김 임포트		

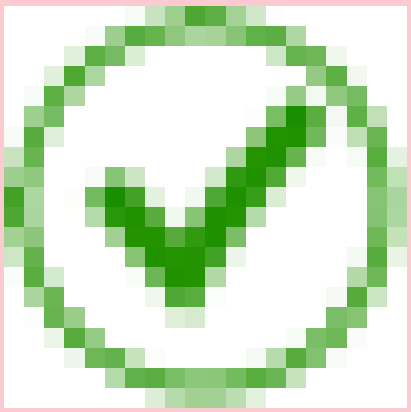
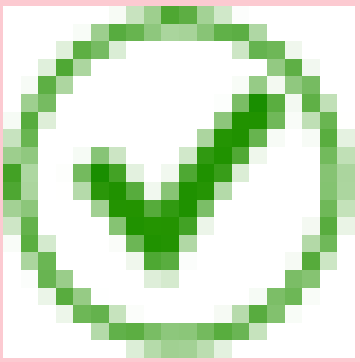
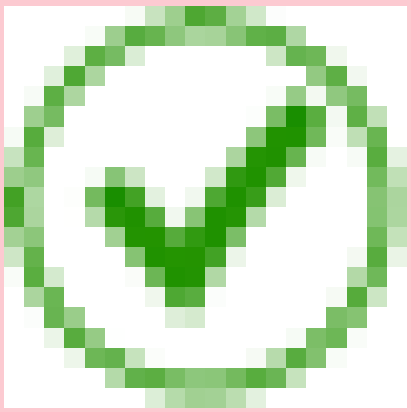
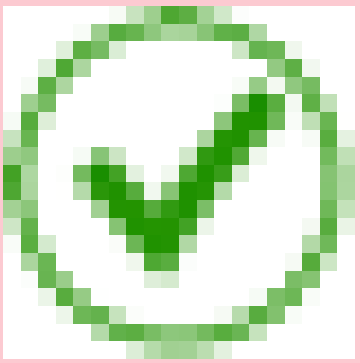
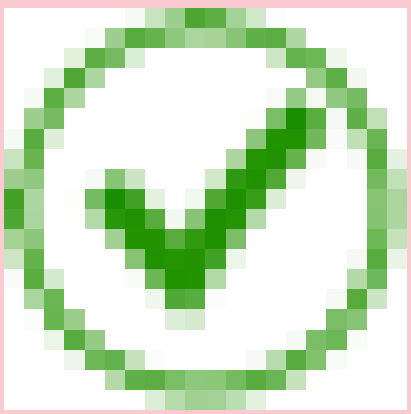
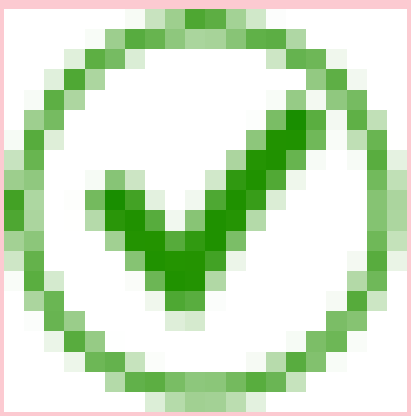
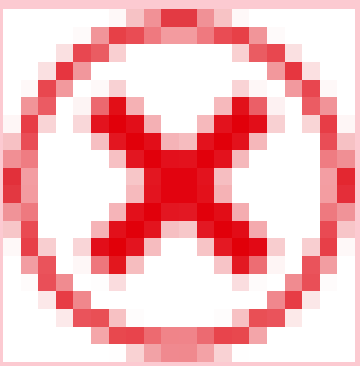
〔End〕

〔store-future: BEGIN review〕

Rapid7 취약성 통합에 대한 역할별 모듈 액세스

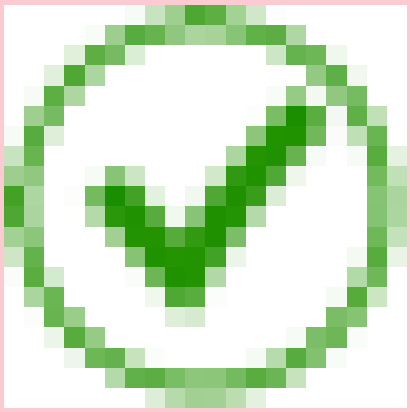
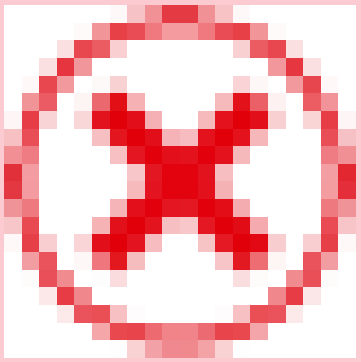
Rapid7 취약성 통합의 경우 특정 역할이 액세스할 수 있는 메뉴 항목을 참조하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈	sn_vul_r7.관리자	sn_vul_r7.읽다
(메인 앱 그룹)		
통합 실행 상태		
사이트		
솔루션		
관리		
통합		

기계 번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈	sn_vul_r7.관리자	sn_vul_r7.읽다
구성		

〔End〕

〔store-future: BEGIN review〕

보안 인시던트에 대한 역할별 모듈 액세스

보안 인시던트의 경우 특정 역할이 액세스할 수 있는 메뉴 항목을 참조하십시오.

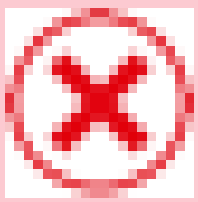
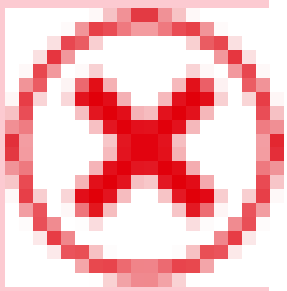
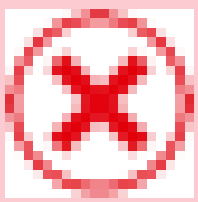
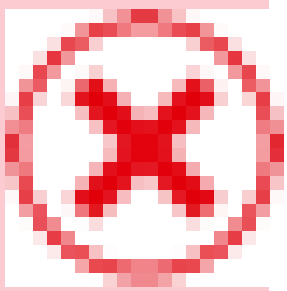
다음에 대한 모듈 액세스: **sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read**

다음에 대한 모듈 액세스: **sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read**

다른 역할에 대한 정보:

sn_si.special_access, sn_si_approver_user

기계번역

모듈	sn_sec_cmn.읽다	sn_si.관리자	sn_si.분석자	**sn_si.CISO**	sn_si.외부	**sn_si.knowledge_admin**	sn_si.매니저	s
(메인 앱 그룹)								
인시던트 새 UI								
서비스 영향도								

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read**

다른 역할에 대한 정보:

sn_si.special_access, sn_si_approver_user

모듈	sn_sec_cmn.읽다	sn_si.관리자	sn_si.분석자	**sn_si.CISO**	sn_si.외부	**sn_si.knowledge_admin**	sn_si.매니저	s
개요	✗	✓	✓	✓	✗	✗	✓	
실시간	✗	✓	✗	✗	✗	✗	✓	
인시던트								
나에게 표시	✗	✗	✗	✗	✗	✗	✗	
나에게 할당됨	✗	✓	✓	✓	✗	✓	✓	

기계 번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read**

다른 역할에 대한 정보:

sn_si.special_access, sn_si_approver_user

모듈	sn_sec_cmn.읽다	sn_si.관리자	sn_si.분석자	**sn_si.CISO**	sn_si.외부	**sn_si.knowledge_admin**	sn_si.매니저	s
내 작업	✗	✗	✗	✗	✓	✗	✗	
팀에 할당됨	✗	✓	✓	✓	✗	✓	✓	
열린 인시던트 표시	✗	✓	✓	✓	✗	✓	✓	
모든 인시던트 표시	✗	✓	✓	✓	✗	✓	✓	
미할당 인시던트	✗	✓	✓	✓	✗	✓	✓	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read**

다른 역할에 대한 정보:

sn_si.special_access, sn_si_approver_user

모듈	sn_sec_cmn.읽다	sn_si.관리자	sn_si.분석자	**sn_si.CISO**	sn_si.외부	**sn_si.knowledge_admin**	sn_si.매니저	s
응답 작업								
나에게 할당됨	✗	✓	✓	✓	✗	✓	✓	
팀에 할당됨	✗	✓	✓	✓	✗	✓	✓	
열린 작업 표시	✗	✓	✓	✓	✗	✓	✓	
모든 작업 표시	✗	✓	✓	✓	✗	✓	✓	

기계 번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read**

다른 역할에 대한 정보:

sn_si.special_access, sn_si_approver_user

모듈	sn_sec_cmn.읽다	sn_si.관리자	sn_si.분석자	**sn_si.CISO**	sn_si.외부	**sn_si.knowledge_admin**	sn_si.매니저	s
미할당 작업	✗	✓	✓	✓	✗	✓	✓	
인바운드 요청								
나에게 할당됨	✗	✓	✓	✓	✗	✓	✓	
팀에 할당됨	✗	✓	✓	✓	✗	✓	✓	
내 승인	✗	✗	✗	✗	✗	✗	✗	

기계 번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read**

다른 역할에 대한 정보:

sn_si.special_access, sn_si_approver_user

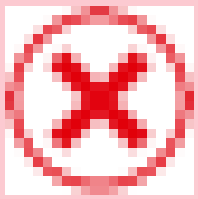
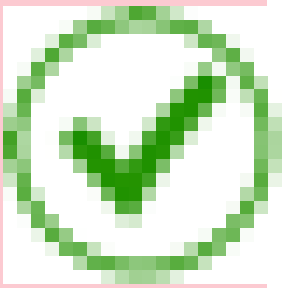
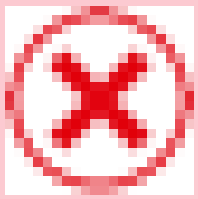
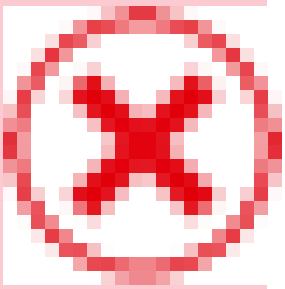
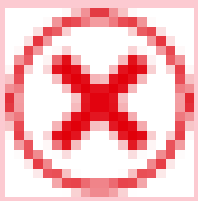
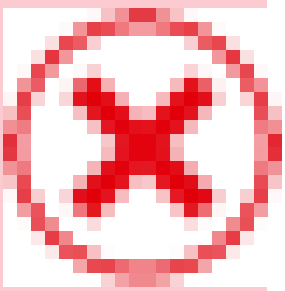
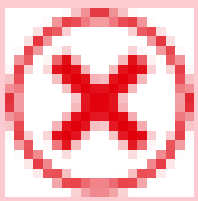
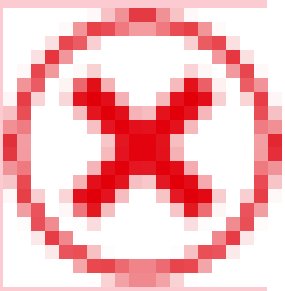
모듈	sn_sec_cmn.읽다	sn_si.관리자	sn_si.분석자	**sn_si.CISO**	sn_si.외부	**sn_si.knowledge_admin**	sn_si.매니저	s
미해결 요청 표시	✗	✓	✓	✓	✗	✓	✓	
모든 요청 표시	✗	✓	✓	✓	✗	✓	✓	
미할당 요청	✗	✓	✓	✓	✗	✓	✓	
내 맵	✗	✓	✓	✗	✗	✗	✗	
경보 및 이벤트								
게시 인시던트 검토								

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read**

다른 역할에 대한 정보:

sn_si.special_access, sn_si_approver_user

모듈	sn_sec_cmn.읽다	sn_si.관리자	sn_si.분석자	**sn_si.CISO**	sn_si.외부	**sn_si.knowledge_admin**	sn_si.매니저	s
보류 중인 사용자 검토								
팀에서 보류 중인 검토								
모든 완료되지 않은 검토								
설정								
보안 인시던트 계산기 그룹								

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read**

다른 역할에 대한 정보:

sn_si.special_access, sn_si_approver_user

모듈	sn_sec_cmn.읽다	sn_si.관리자	sn_si.분석자	**sn_si.CISO**	sn_si.외부	**sn_si.knowledge_admin**	sn_si.매니저	s
심각도 계산기	✗	✓	✗	✗	✗	✗	✓	
위험 점수 구성	✓	✓	✓	✓	✗	✓	✓	
뉴스 피드 구성	✗	✓	✓	✓	✗	✓	✓	
그룹	✗	✓	✗	✗	✗	✗	✗	
역할	✗	✓	✗	✗	✗	✗	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read**

다른 역할에 대한 정보:

sn_si.special_access, sn_si_approver_user

모듈	sn_sec_cmn.읽다	sn_si.관리자	sn_si.분석자	**sn_si.CISO**	sn_si.외부	**sn_si.knowledge_admin**	sn_si.매니저	s
SLA	✗	✓	✗	✗	✗	✗	✗	
분석가 작업 공간 설정(신규 UI)								
설정 도우미	✗	✓	✗	✗	✗	✗	✗	
방문 페이지 필터 구성	✗	✓	✗	✗	✗	✗	✗	
양식 UI 작업	✗	✓	✗	✗	✗	✗	✗	

기계 번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read**

다른 역할에 대한 정보:

sn_si.special_access, sn_si_approver_user

모듈	sn_sec_cmn.읽다	sn_si.관리자	sn_si.분석자	**sn_si.CISO**	sn_si.외부	**sn_si.knowledge_admin**	sn_si.매니저	s
관련 목록 구성	✗	✓	✗	✗	✗	✗	✗	
분석가 작업 공간 속성	✗	✓	✗	✗	✗	✗	✗	
카탈로그 및 지식베이스								
보안 인시던트 템플릿	✗	✓	✗	✗	✗	✗	✗	
카탈로그 항목 유지	✗	✓	✗	✗	✗	✗	✗	

기계 번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read**

다른 역할에 대한 정보:

sn_si.special_access, sn_si_approver_user

모듈	sn_sec_cmn.읽다	sn_si.관리자	sn_si.분석자	**sn_si.CISO**	sn_si.외부	**sn_si.knowledge_admin**	sn_si.매니저	s
지식	✗	✓	✗	✗	✗	✓	✗	
수동 Runbook								
새 Runbook 생성	✗	✓	✗	✗	✗	✓	✗	
Runbook 문서 보기	✗	✓	✗	✗	✗	✓	✗	
관리								
속성	✗	✓	✗	✗	✗	✗	✗	

기계 번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read**

다른 역할에 대한 정보:

sn_si.special_access, sn_si_approver_user

모듈	sn_sec_cmn.읽다	sn_si.관리자	sn_si.분석자	**sn_si.CISO**	sn_si.외부	**sn_si.knowledge_admin**	sn_si.매니저	s
구성	✗	✓	✗	✗	✗	✗	✗	
알림	✗	✓	✗	✗	✗	✗	✗	
서비스 중요도 보고 정의	✗	✓	✗	✗	✗	✗	✗	
서비스 중요도 정의	✗	✓	✗	✗	✗	✗	✗	
서비스 영향도 정의	✗	✓	✗	✗	✗	✗	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read**

다른 역할에 대한 정보:

sn_si.special_access, sn_si_approver_user

모듈	sn_sec_cmn.읽다	sn_si.관리자	sn_si.분석자	**sn_si.CISO**	sn_si.외부	**sn_si.knowledge_admin**	sn_si.매니저	s
사후 인시던트 검토 평가 설정	✗	✓	✗	✗	✗	✗	✗	
게시 인시던트 검토 보고서 설정	✗	✓	✗	✗	✗	✗	✗	
실시간 정의	✗	✓	✗	✗	✗	✗	✗	
프로세스 선택	✗	✓	✗	✗	✗	✗	✗	
프로세스 정의	✗	✓	✗	✗	✗	✗	✗	

기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read**

다른 역할에 대한 정보:

sn_si.special_access, sn_si_approver_user

모듈	sn_sec_cmn.읽다	sn_si.관리자	sn_si.분석자	**sn_si.CISO**	sn_si.외부	**sn_si.knowledge_admin**	sn_si.매니저	s
템플릿 워크플로우 결과 평가자	✗	✓	✗	✗	✗	✗	✗	
피싱 이메일								
라이센스 관리	✗	✓	✗	✗	✗	✗	✗	
피싱 메일 보고	✗	✓	✓	✗	✗	✗	✗	
모든 피싱 이메일 표시	✗	✓	✓	✗	✗	✗	✗	

기계 번역

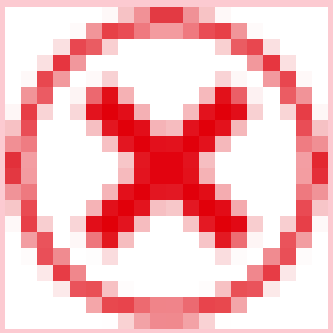
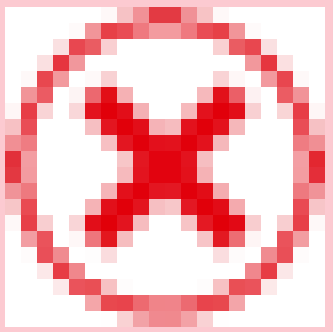
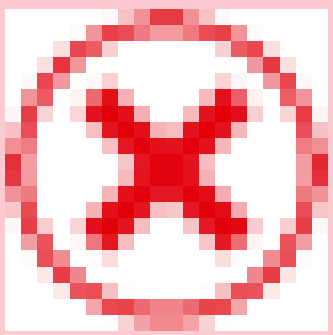
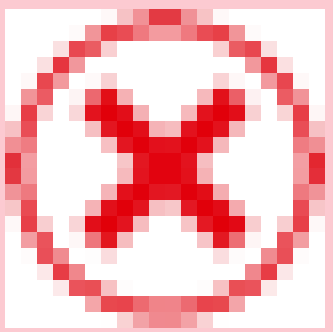
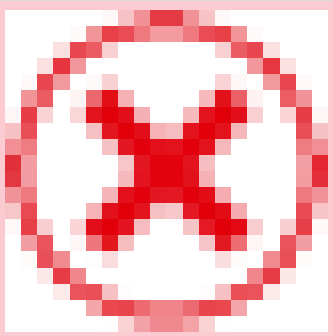
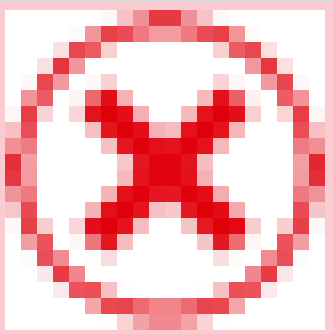
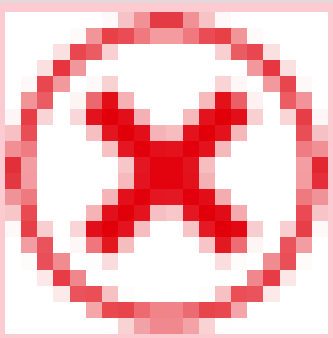
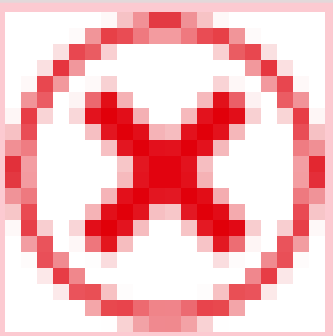
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 접근: **sn_si.special_access, sn_si_approver_user**

모듈 접근: **sn_si.special_access, sn_si_approver_user**

다른 역할에 대한 정보:

sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

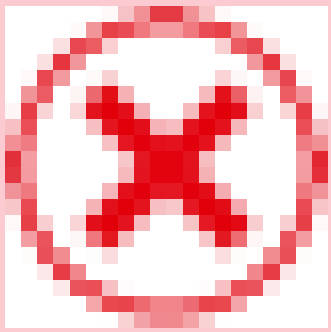
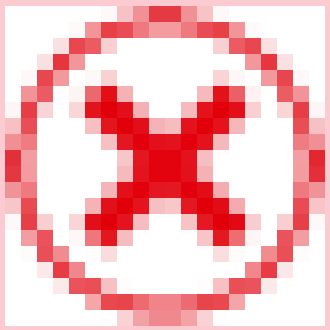
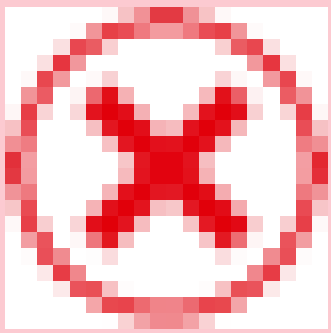
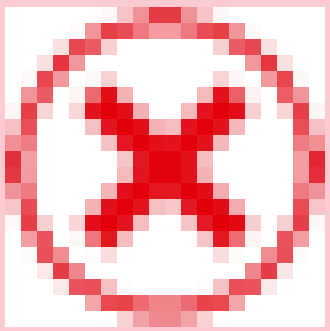
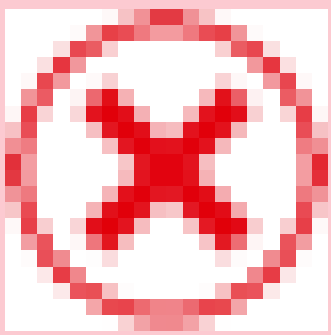
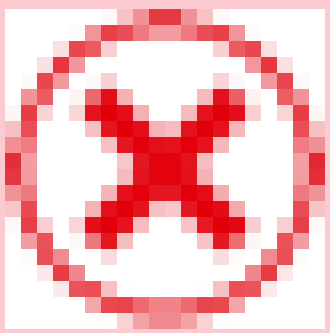
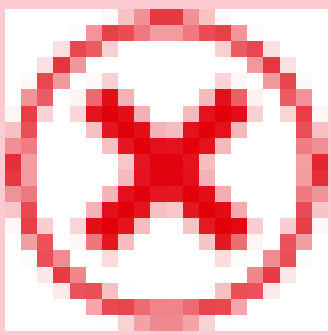
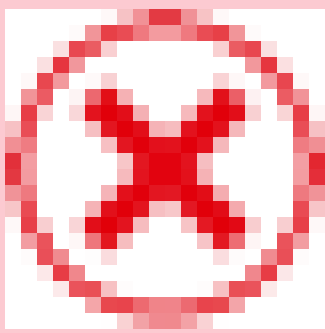
모듈	sn_si.special_access	sn_si_approver_user
(메인 앱 그룹)		
인시던트 새 UI		
서비스 영향도		
개요		
실시간		
인시던트		

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 접근: **sn_si.special_access, sn_si_approver_user**

다른 역할에 대한 정보:

sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

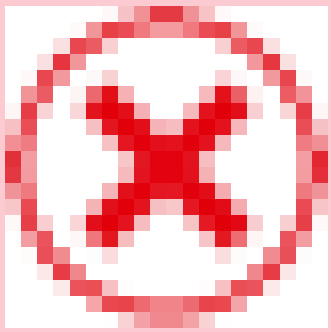
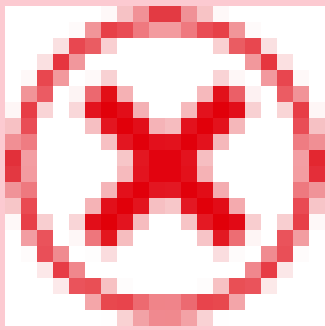
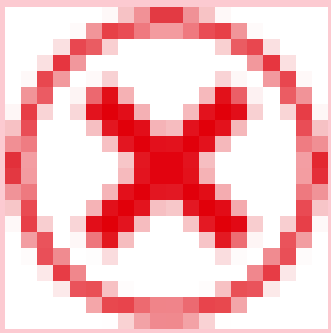
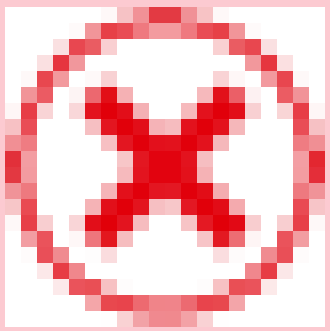
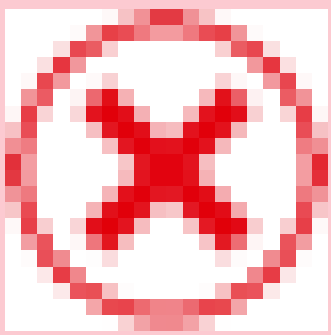
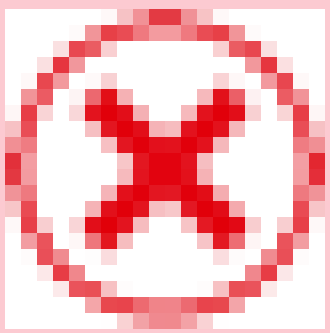
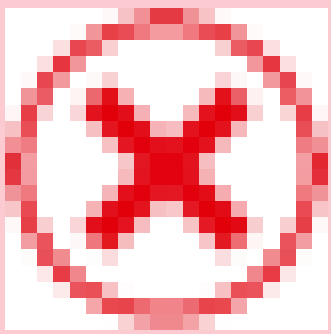
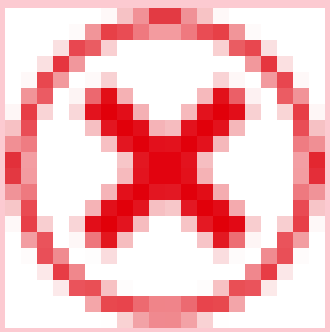
모듈	sn_si.special_access	sn_si_approver_user
나에게 표시		
나에게 할당됨		
내 작업		
팀에 할당됨		

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 접근: **sn_si.special_access, sn_si_approver_user**

다른 역할에 대한 정보:

sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

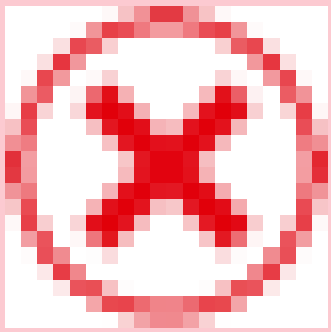
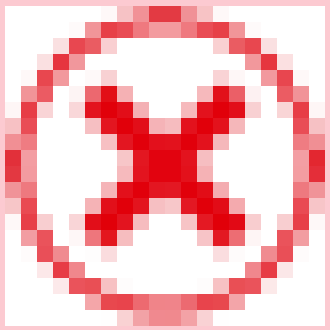
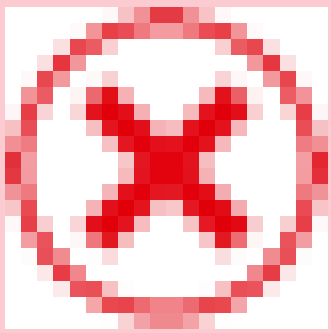
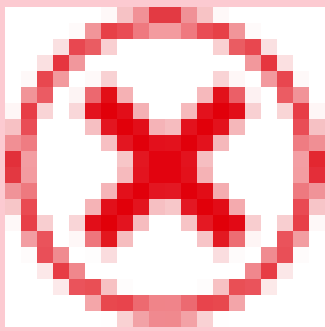
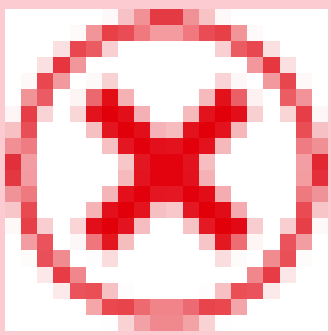
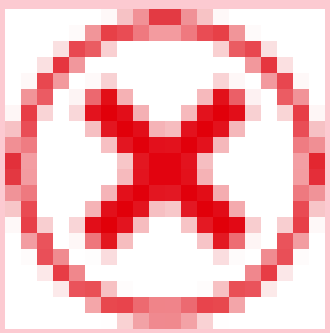
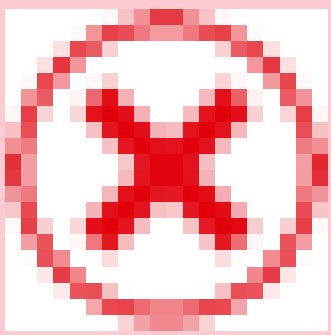
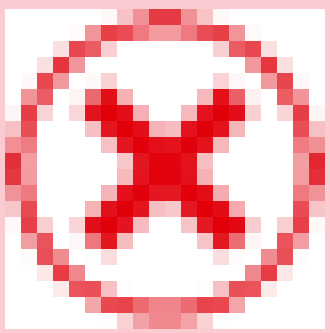
모듈	sn_si.special_access	sn_si_approver_user
열린 인시던트 표시		
모든 인시던트 표시		
미할당 인시던트		
응답 작업		
나에게 할당됨		

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 접근: **sn_si.special_access, sn_si_approver_user**

다른 역할에 대한 정보:

sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

모듈	sn_si.special_access	sn_si_approver_user
팀에 할당됨		
열린 작업 표시		
모든 작업 표시		
미할당 작업		
인바운드 요청		

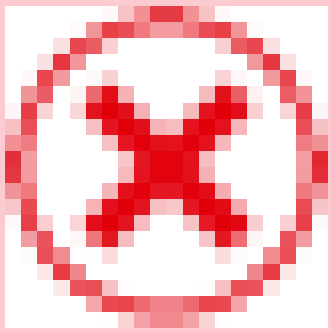
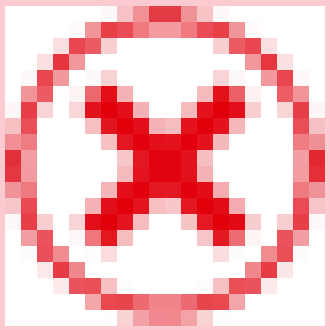
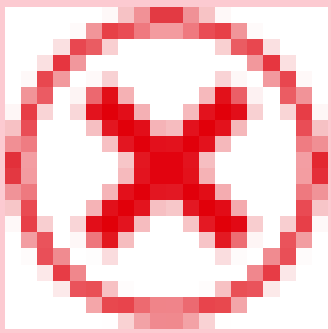
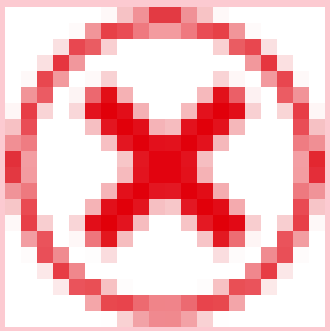
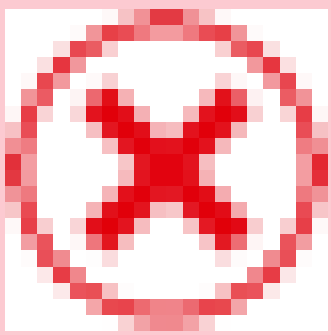
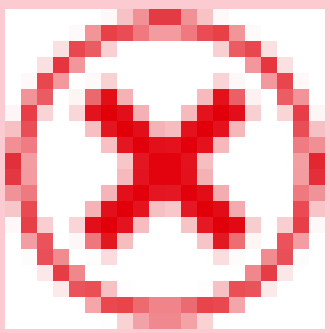
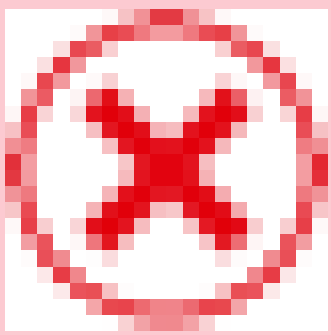
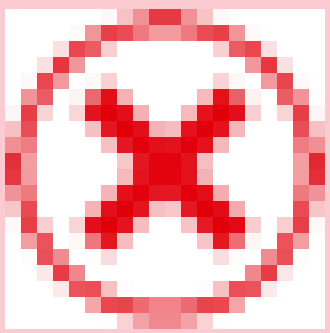
기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 접근: **sn_si.special_access, sn_si_approver_user**

다른 역할에 대한 정보:

sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

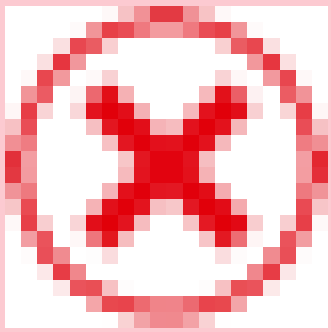
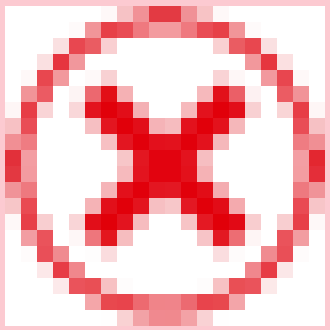
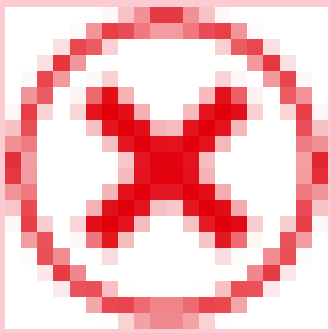
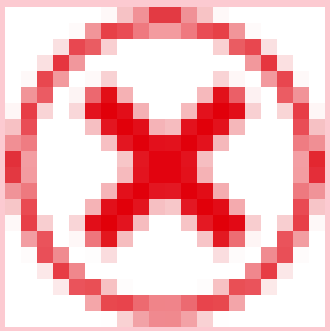
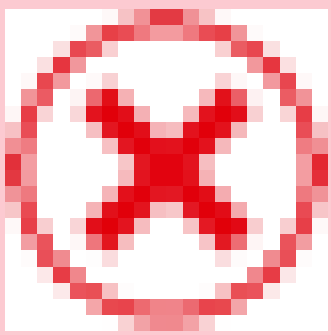
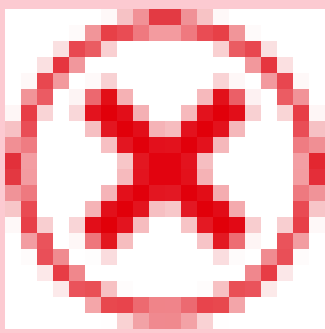
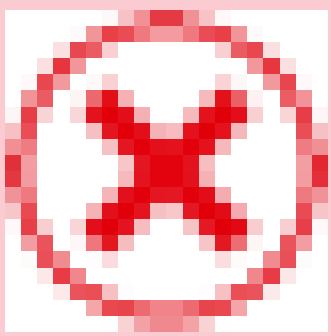
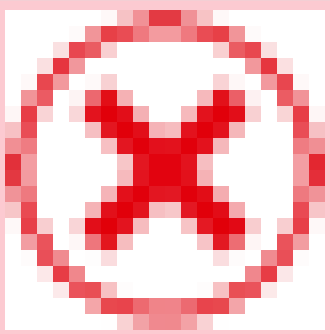
모듈	sn_si.special_access	sn_si_approver_user
나에게 할당됨		
팀에 할당됨		
내 승인		
미해결 요청 표시		

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 접근: **sn_si.special_access, sn_si_approver_user**

다른 역할에 대한 정보:

sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

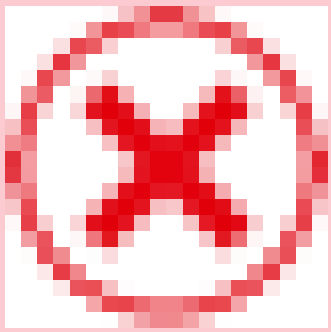
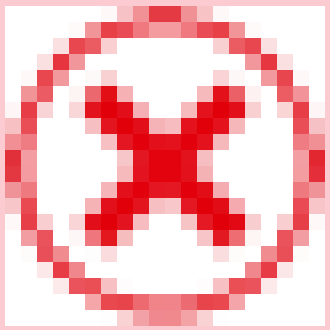
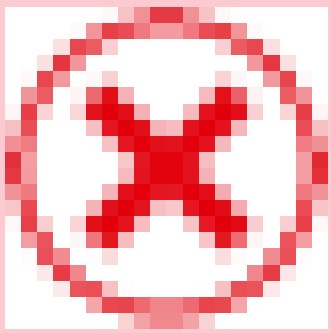
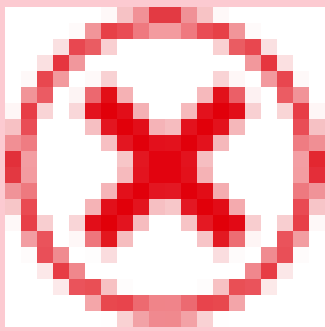
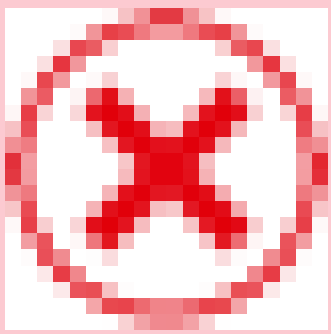
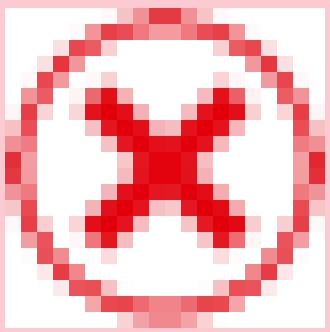
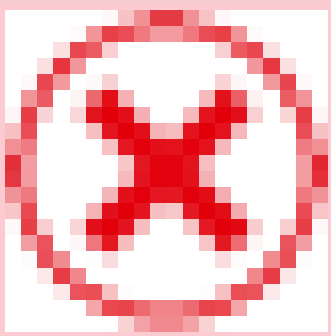
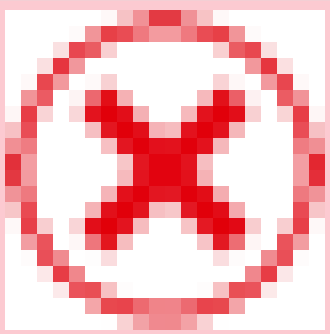
모듈	sn_si.special_access	sn_si_approver_user
모든 요청 표시		
미할당 요청		
내 맵		
경보 및 이벤트		
게시 인시던트 검토		
보류 중인 사용자 검토		

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 접근: **sn_si.special_access, sn_si_approver_user**

다른 역할에 대한 정보:

sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

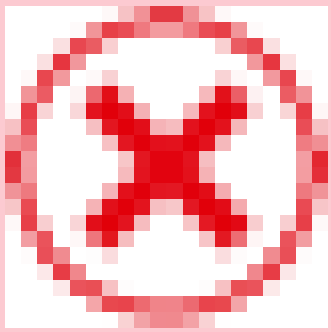
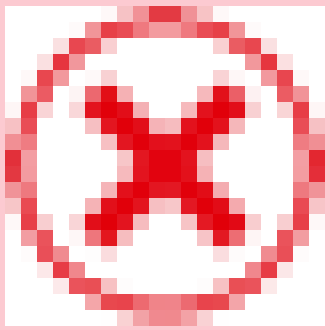
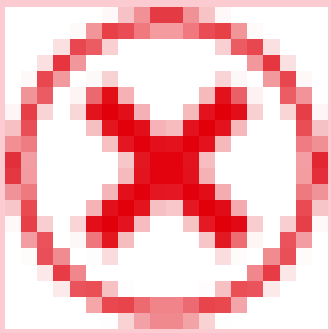
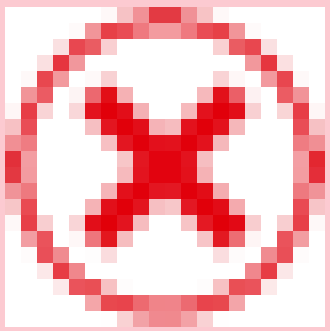
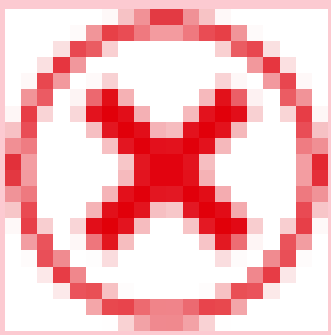
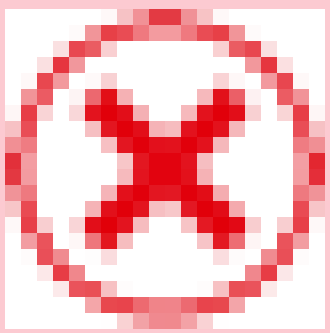
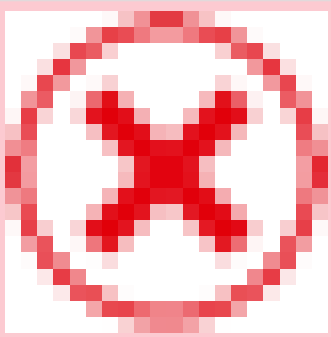
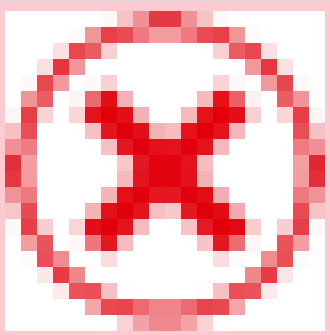
모듈	sn_si.special_access	sn_si_approver_user
팀에서 보류 중인 검토		
모든 완료되지 않은 검토		
설정		
보안 인시던트 계산기 그룹		
심각도 계산기		

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 접근: **sn_si.special_access, sn_si_approver_user**

다른 역할에 대한 정보:

sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

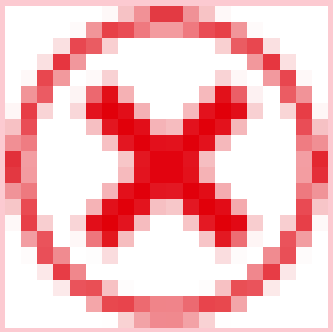
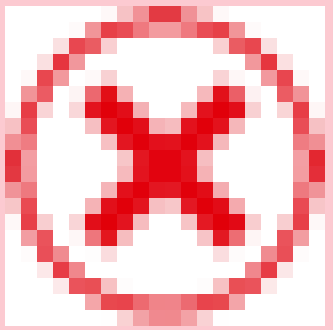
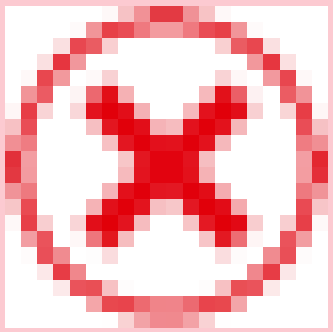
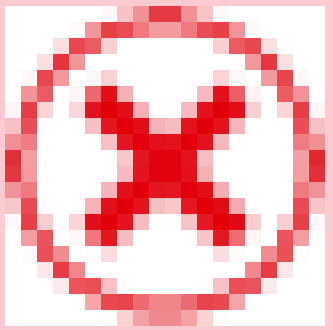
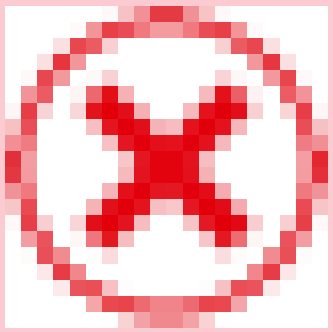
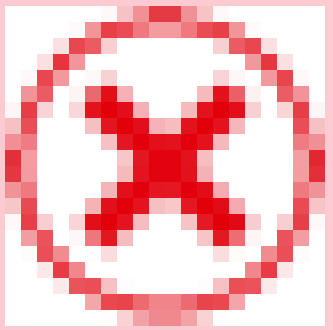
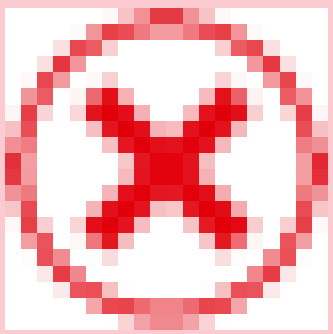
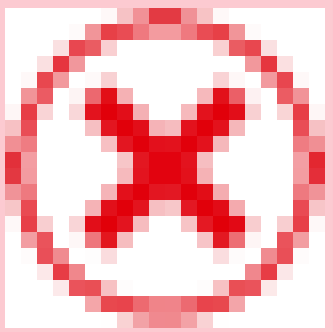
모듈	sn_si.special_access	sn_si_approver_user
위험 점수 구성		
뉴스 피드 구성		
그룹		
역할		

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 접근: **sn_si.special_access, sn_si_approver_user**

다른 역할에 대한 정보:

sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

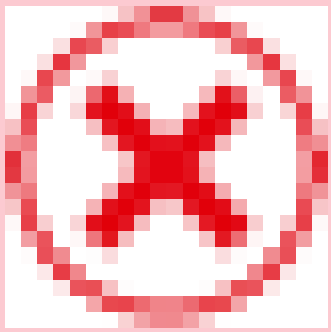
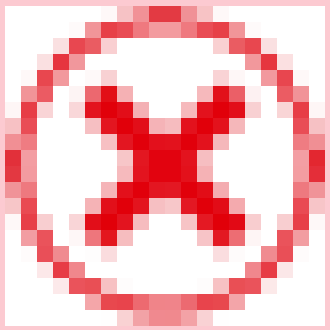
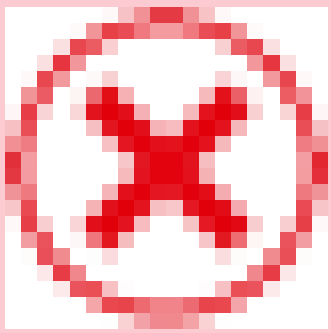
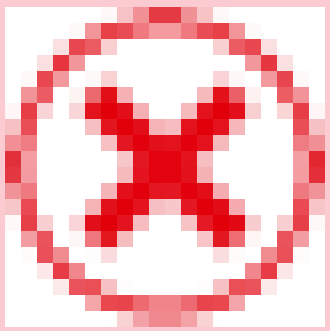
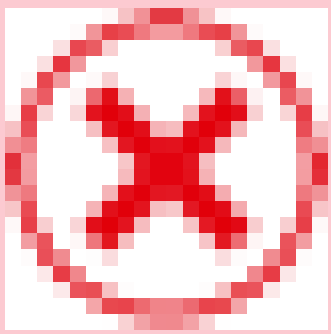
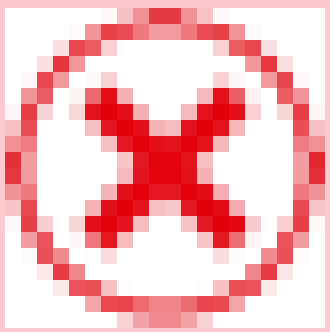
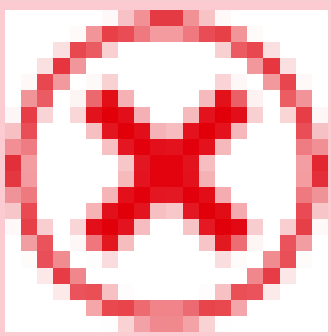
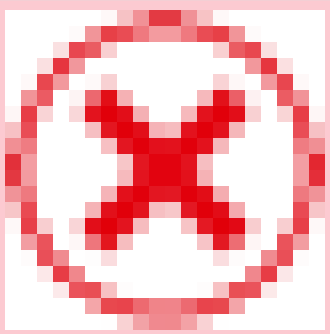
모듈	sn_si.special_access	sn_si_approver_user
SLA		
분석가 작업 공간 설정(신규 UI)		
설정 도우미		
방문 페이지 필터 구성		
양식 UI 작업		

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 접근: **sn_si.special_access, sn_si_approver_user**

다른 역할에 대한 정보:

sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

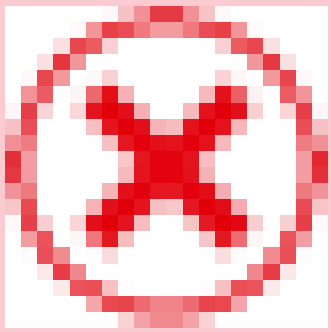
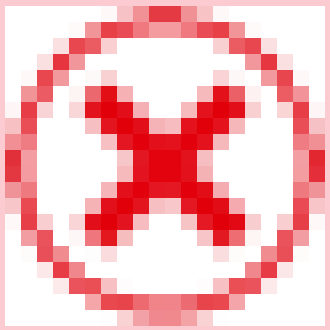
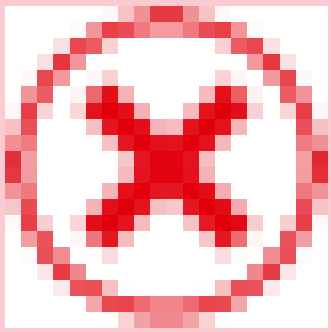
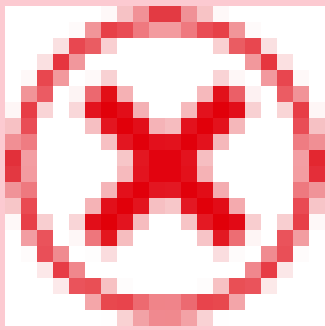
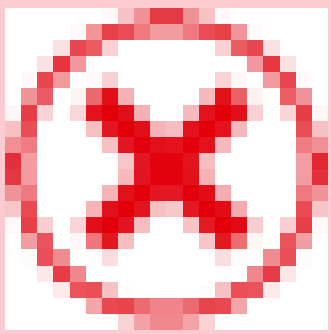
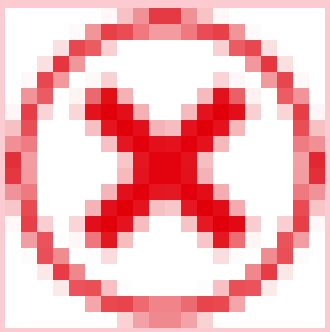
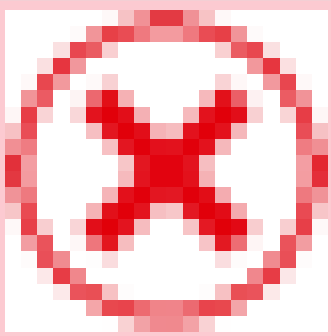
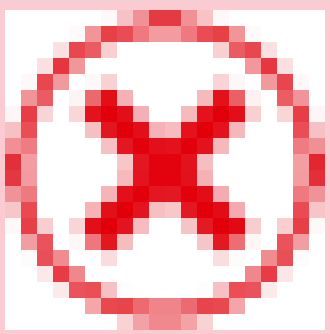
모듈	sn_si.special_access	sn_si_approver_user
관련 목록 구성		
분석가 작업 공간 속성		
카탈로그 및 지식베이스		
보안 인시던트 템플릿		
카탈로그 항목 유지		

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 접근: **sn_si.special_access, sn_si_approver_user**

다른 역할에 대한 정보:

sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

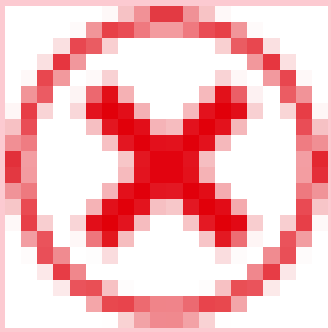
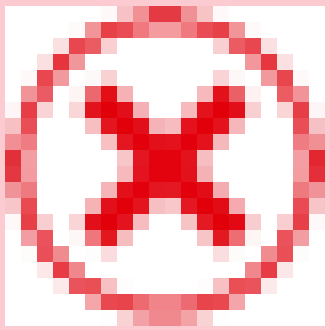
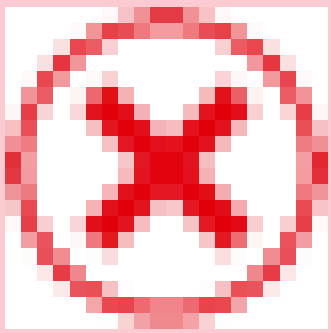
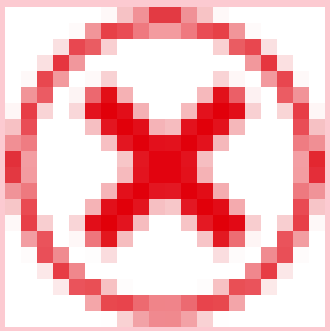
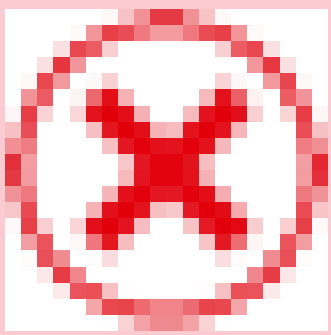
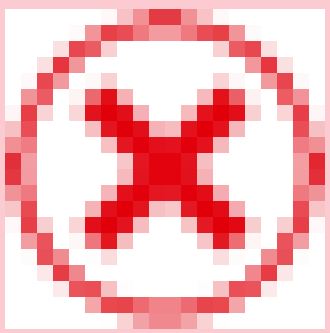
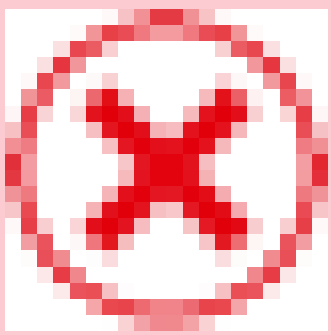
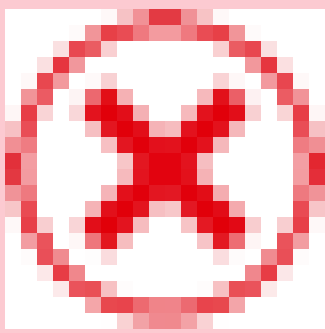
모듈	sn_si.special_access	sn_si_approver_user
지식		
수동 Runbook		
새 Runbook 생성		
Runbook 문서 보기		
관리		
속성		

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 접근: **sn_si.special_access, sn_si_approver_user**

다른 역할에 대한 정보:

sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

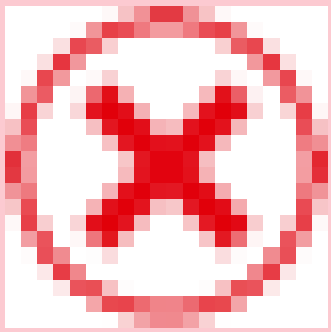
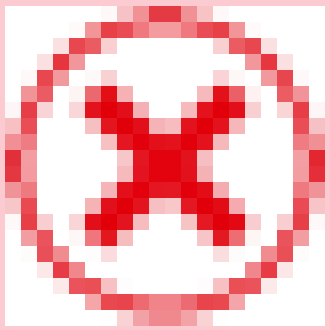
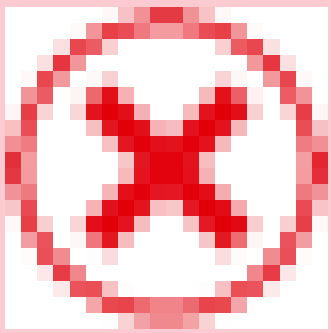
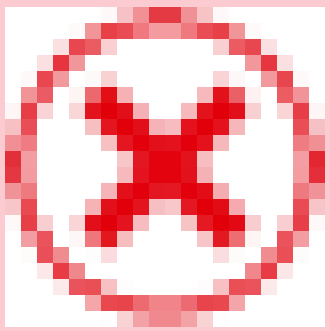
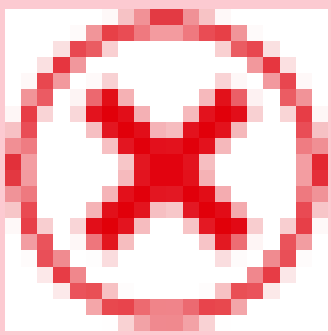
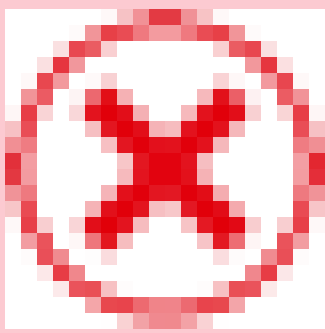
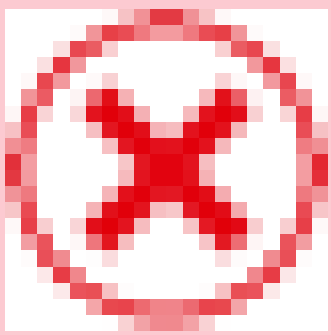
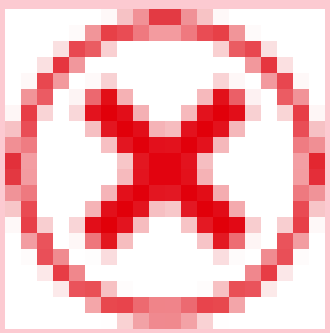
모듈	sn_si.special_access	sn_si_approver_user
구성		
알림		
서비스 중요도 보고 정의		
서비스 중요도 정의		

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 접근: **sn_si.special_access, sn_si_approver_user**

다른 역할에 대한 정보:

sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

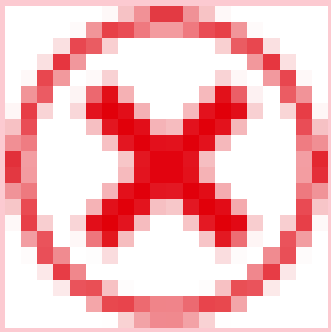
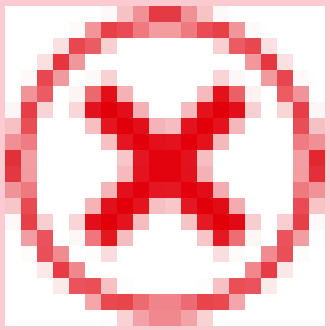
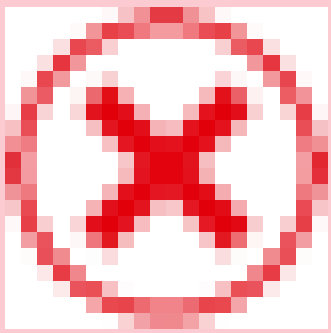
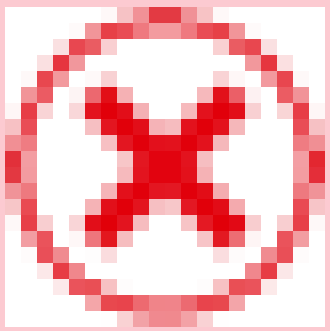
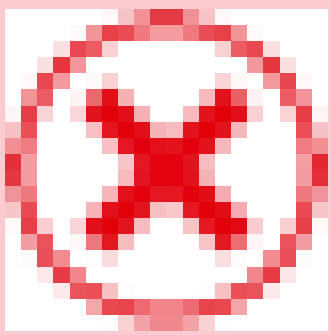
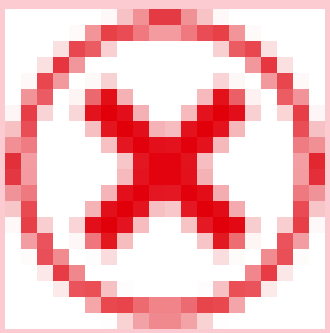
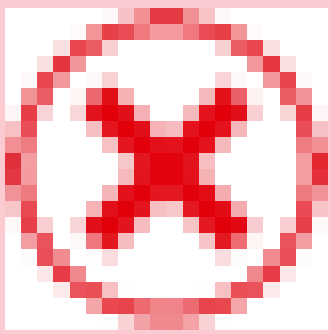
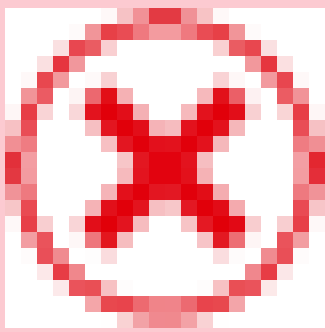
모듈	sn_si.special_access	sn_si_approver_user
서비스 영향도 정의		
사후 인시던트 검토 평가 설정		
게시 인시던트 검토 보고서 설정		
실시간 정의		

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 접근: **sn_si.special_access, sn_si_approver_user**

다른 역할에 대한 정보:

sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

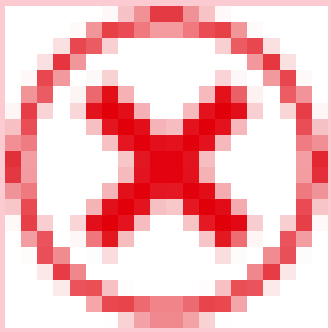
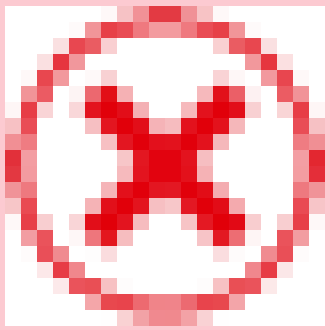
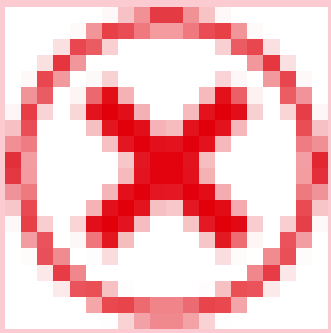
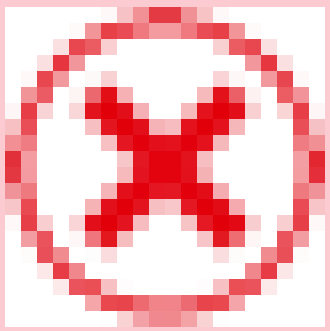
모듈	sn_si.special_access	sn_si_approver_user
프로세스 선택		
프로세스 정의		
템플릿 워크플로우 결과 평가자		
피싱 이메일		
라이센스 관리		

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 접근: **sn_si.special_access, sn_si_approver_user**

다른 역할에 대한 정보:

sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

모듈	sn_si.special_access	sn_si_approver_user
피싱 메일 보고		
모든 피싱 이메일 표시		

〔End〕

〔store-future: BEGIN review〕

보안 운영에 대한 역할별 모듈 액세스

보안 운영에 대한 자세한 내용은 특정 역할이 액세스할 수 있는 메뉴 항목을 참조하십시오.

다음에 대한 모듈 액세스: **admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job**

다음에 대한 모듈 액세스: **admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job**

다른 역할에 대한 정보:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

모듈	관리자	sn_sec_cmn.관리자	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_background_job	sn_sec_c
(메인 앱 그룹)					

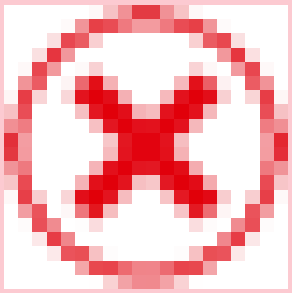
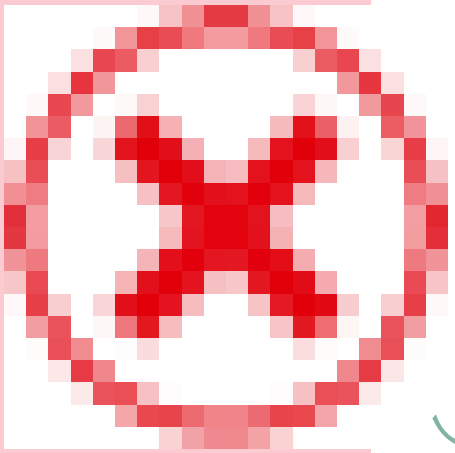
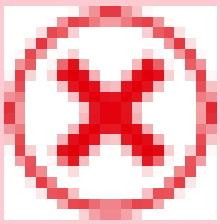
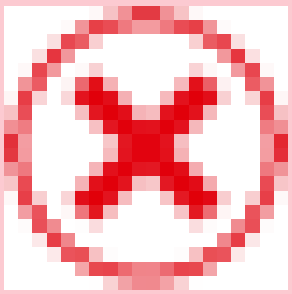
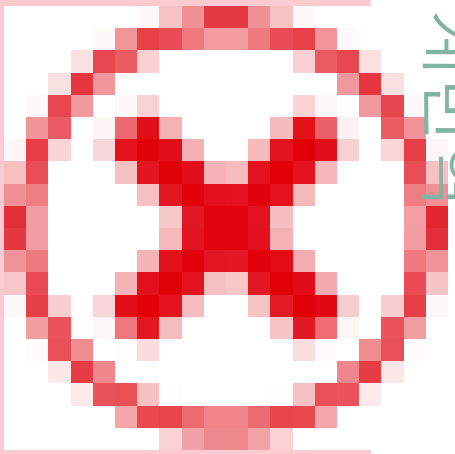
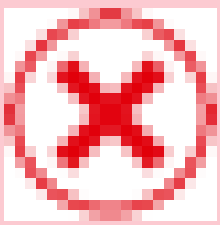
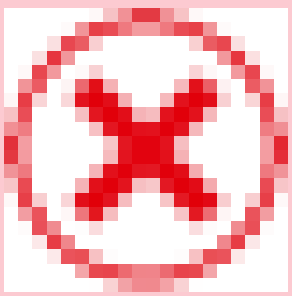
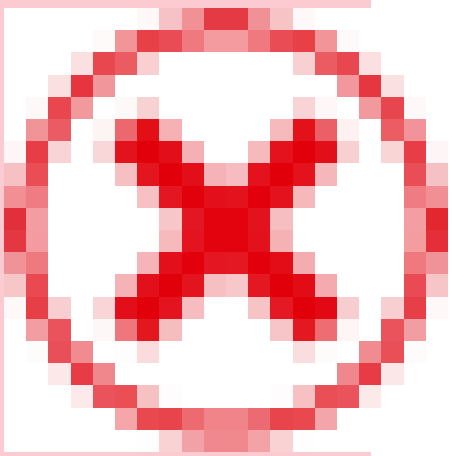
기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job**

다른 역할에 대한 정보:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

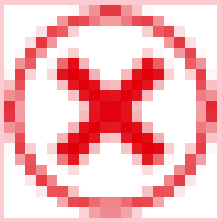
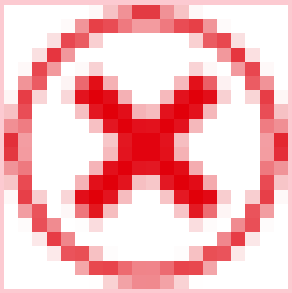
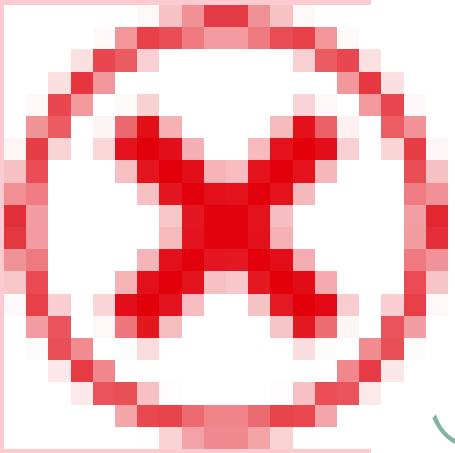
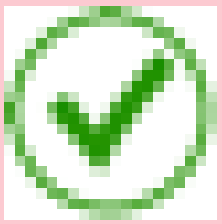
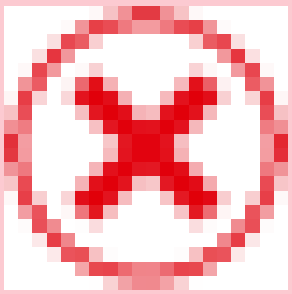
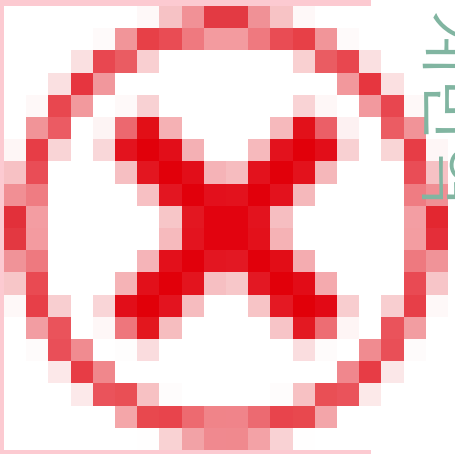
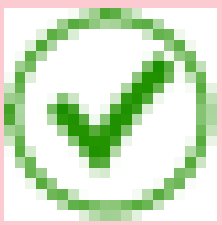
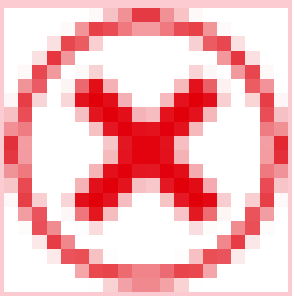
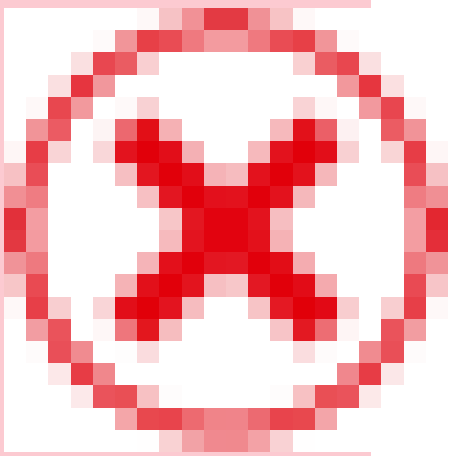
모듈	관리자	sn_sec_cmn.관리자	**sn_sec_cmn.ci_manager**	**sn_sec_cmn.manage_background_job**	sn_sec_c
통합					
통합 역량 플로우					
역량 실행					

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job**

다른 역할에 대한 정보:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

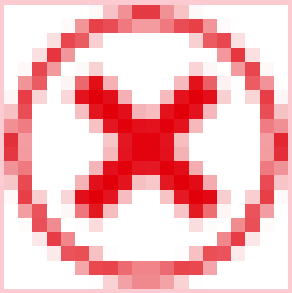
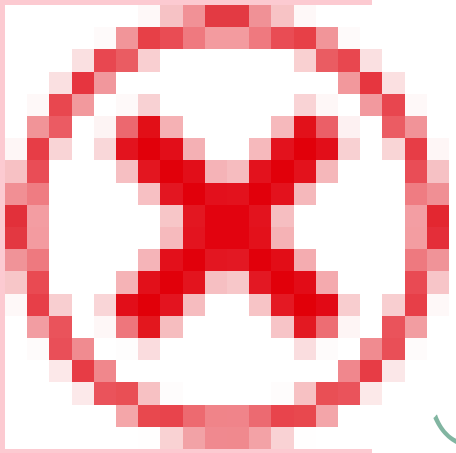
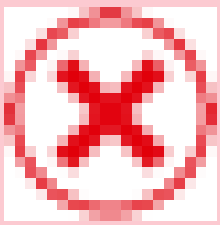
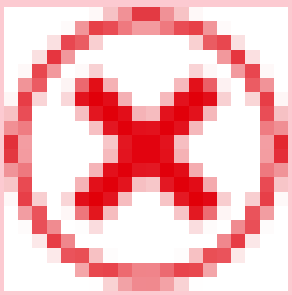
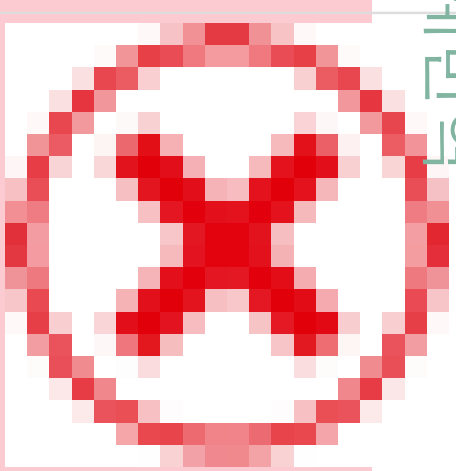
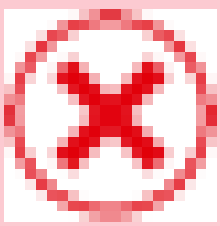
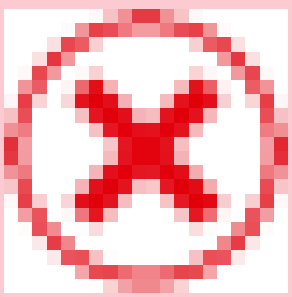
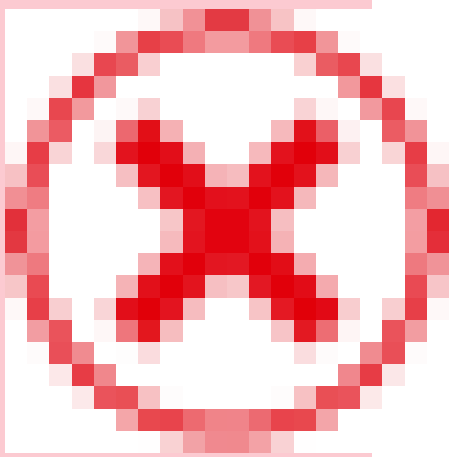
모듈	관리자	sn_sec_cmn.관리자	**sn_sec_cmn.ci_manager**	**sn_sec_cmn.manage_background_job**	sn_sec_c
역량 구현 비율 제한					
통합 구성					
사이팅 검색 구성					

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job**

다른 역할에 대한 정보:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

모듈	관리자	sn_sec_cmn.관리자	**sn_sec_cmn.ci_manager**	**sn_sec_cmn.manage_background_job**	sn_sec_c
통합 기능					
통합					
통합 역량 플로우					
역량 실행					

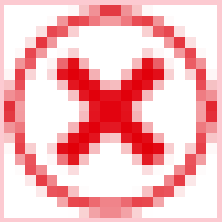
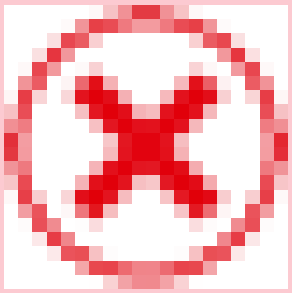
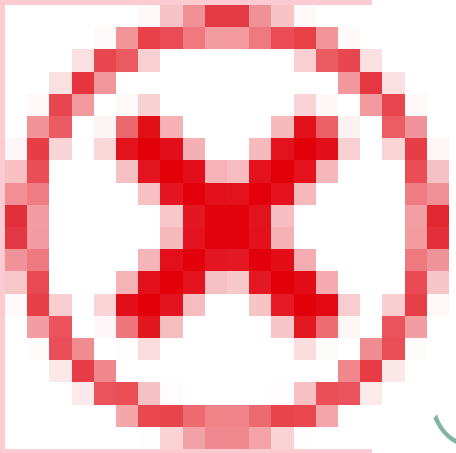
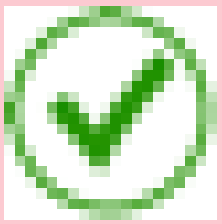
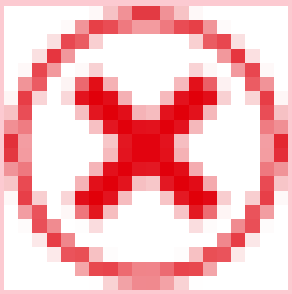
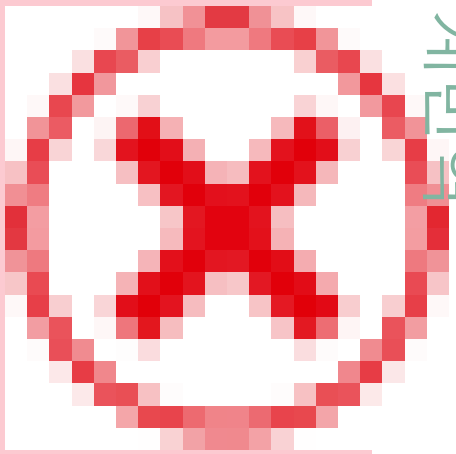
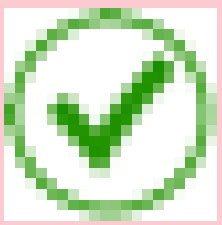
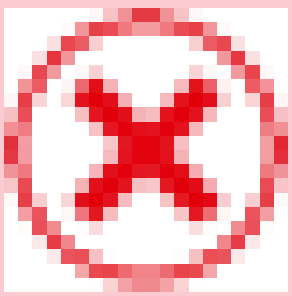
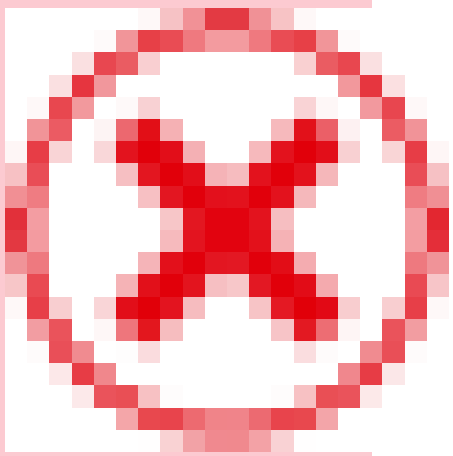
기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job**

다른 역할에 대한 정보:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

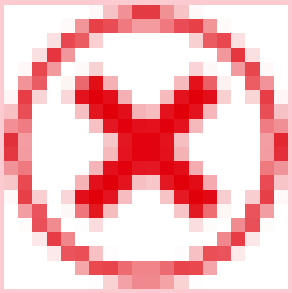
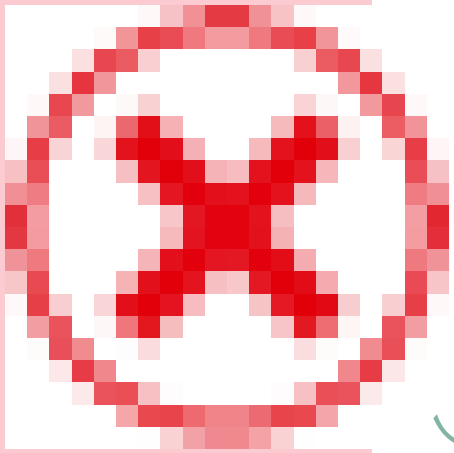
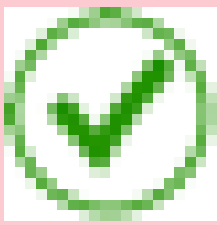
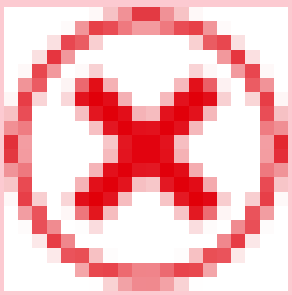
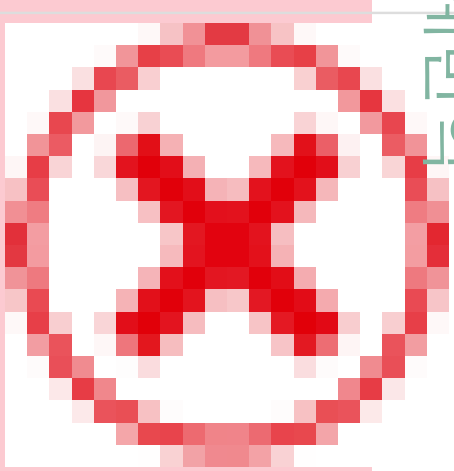
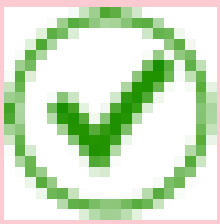
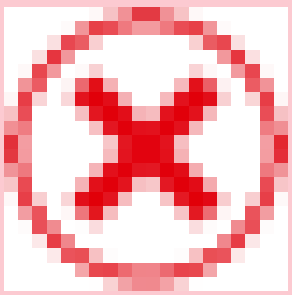
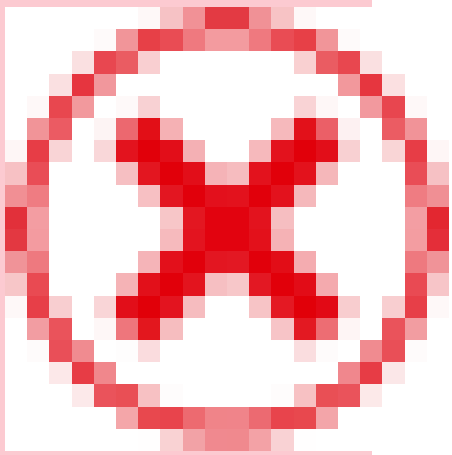
모듈	관리자	sn_sec_cmn.관리자	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_background_job	sn_sec_c
역량 구현 비율 제한					
통합 구성					
사이팅 검색 구성					

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job**

다른 역할에 대한 정보:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

모듈	관리자	sn_sec_cmn.관리자	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_background_job	sn_sec_c
통합 기능					
이메일 처리					
이메일 구문 분석					
중복 규칙					

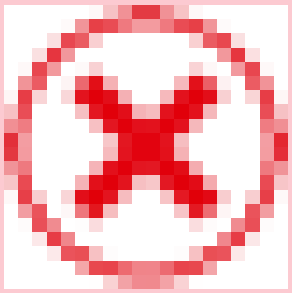
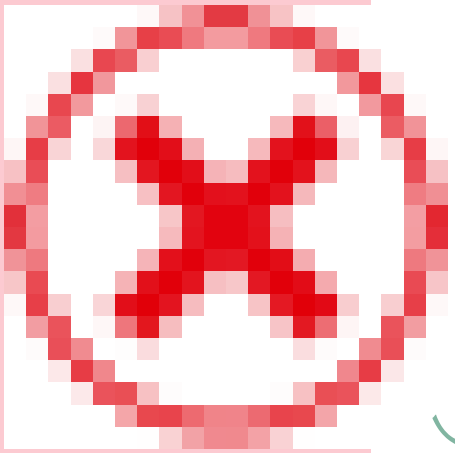
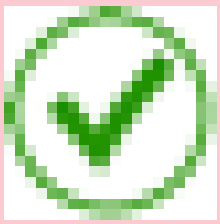
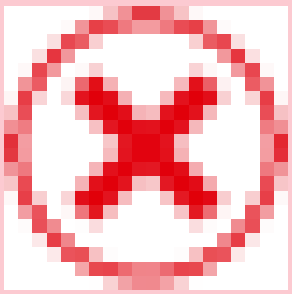
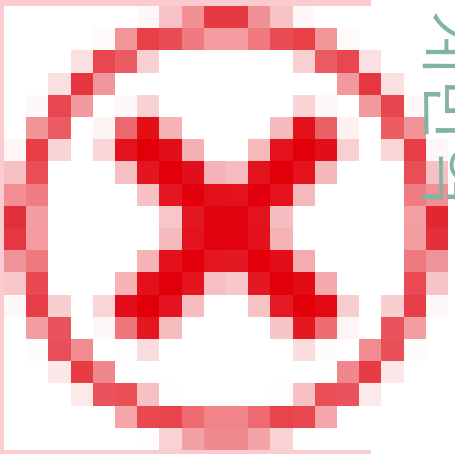
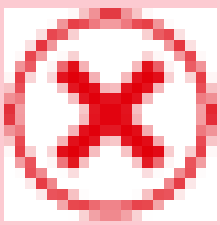
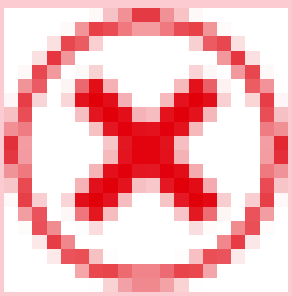
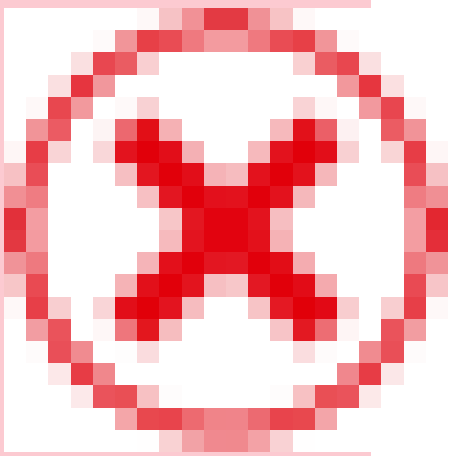
기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job**

다른 역할에 대한 정보:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

모듈	관리자	sn_sec_cmn.관리자	**sn_sec_cmn.ci_manager**	**sn_sec_cmn.manage_background_job**	sn_sec_c
속성					
일치하지 않는 이메일					
수집 규칙 사용자가 보고한 피싱					

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job**

다른 역할에 대한 정보:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

모듈	관리자	sn_sec_cmn.관리자	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_background_job	sn_sec_c
사용자가 보고한 피싱 속성	✓	✗	✗	✗	
그룹					
필터 그룹	✓	✓	✗	✗	
에스컬레이션	✓	✓	✗	✗	

기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job**

다른 역할에 대한 정보:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

모듈	관리자	sn_sec_cmn.관리자	**sn_sec_cmn.ci_manager**	**sn_sec_cmn.manage_background_job**	sn_sec_c
데이터 강화					
보안 태그					
그룹	✓	✓	✗	✗	✗
태그	✓	✓	✗	✗	✗
워크플로우					

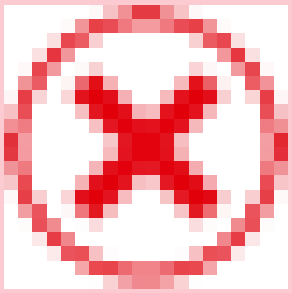
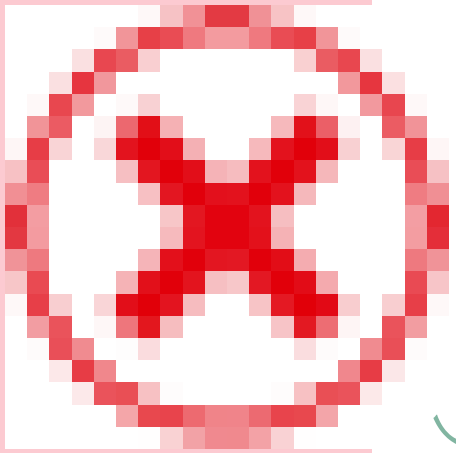
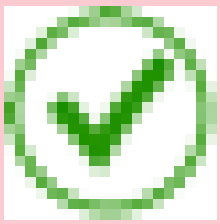
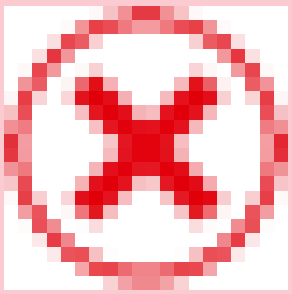
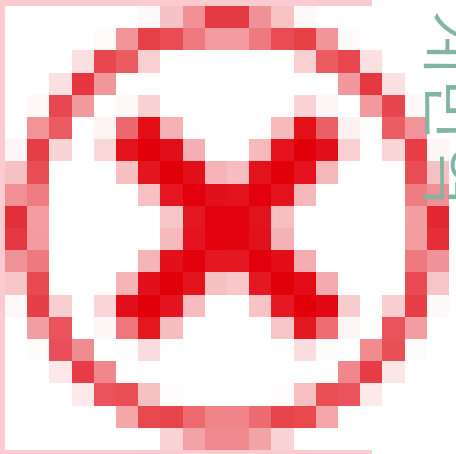
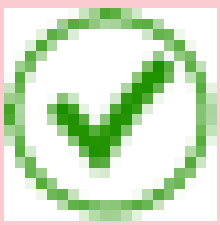
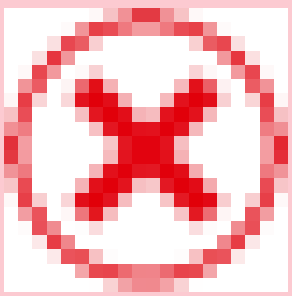
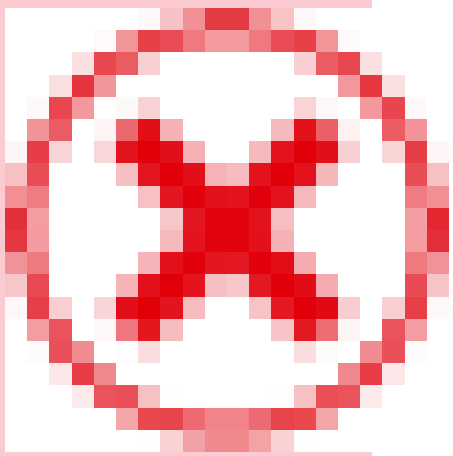
기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job**

다른 역할에 대한 정보:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

모듈	관리자	sn_sec_cmn.관리자	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_background_job	sn_sec_c
실행 추적					
보안 워크플로우 보기					
워크플로우 트리거					
유틸리티					

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job**

다른 역할에 대한 정보:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

모듈	관리자	sn_sec_cmn.관리자	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_background_job	sn_sec_c
보강 데이터 매핑	✓	✓	✗	✗	✗
필드 값 변환	✓	✓	✗	✗	✗
필드 매핑	✓	✓	✗	✗	✗

기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job**

다른 역할에 대한 정보:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

모듈	관리자	sn_sec_cmn.관리자	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_background_job	sn_sec_c
온디맨드 오케스트레이션	✓	✗	✗	✗	
운영 체제 그룹	✓	✓	✗	✗	
SecOps 애플리케이션 레지스트리	✓	✗	✗	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job**

다른 역할에 대한 정보:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

모듈	관리자	sn_sec_cmn.관리자	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_background_job	sn_sec_c
백그라운드 작업 구성	✓	✓	✗	✓	✓
CMDB					
CI 조회 규칙	✓	✓	✓	✗	✗
검색된 항목	✓	✓	✓	✗	✗

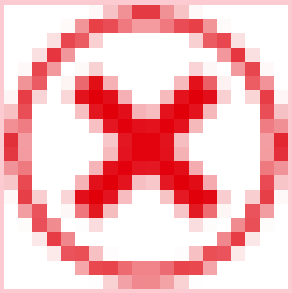
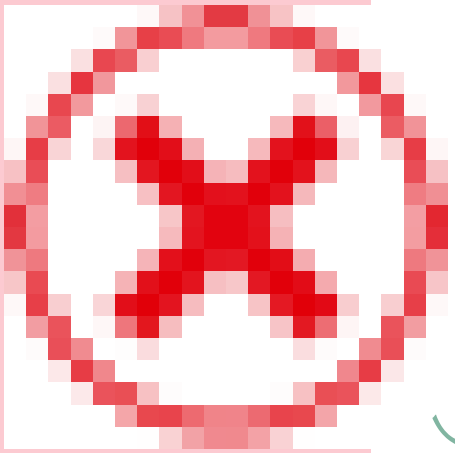
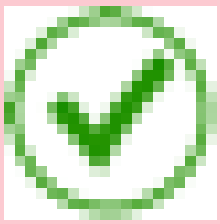
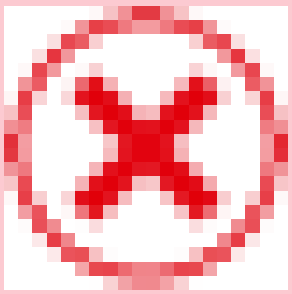
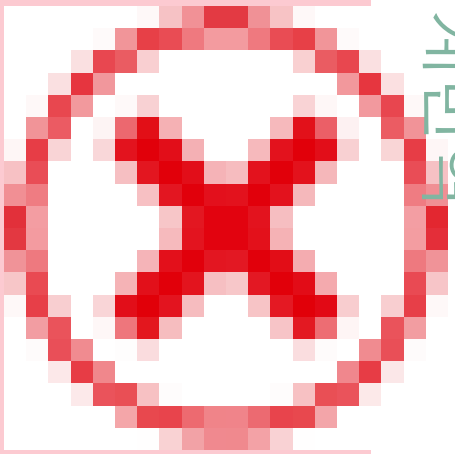
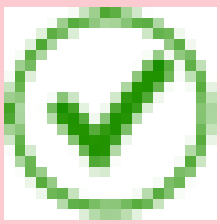
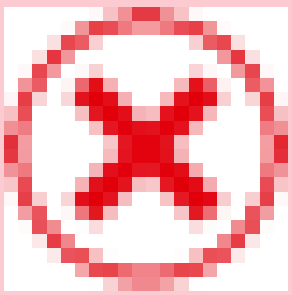
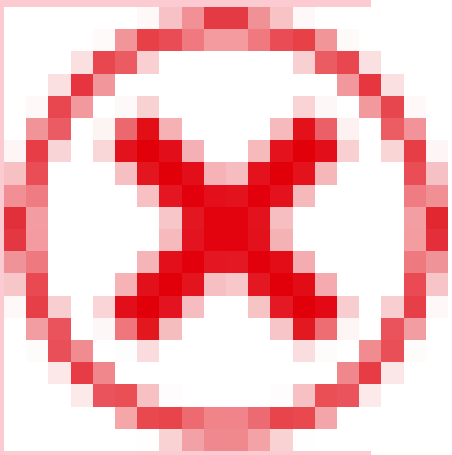
기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job**

다른 역할에 대한 정보:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

모듈	관리자	sn_sec_cmn.관리자	**sn_sec_cmn.ci_manager**	**sn_sec_cmn.manage_background_job**	sn_sec_c
불일치하는 검색된 항목을 일치시키기					
탐색한 컨테이너 이미지					
WatchDog					
구성					

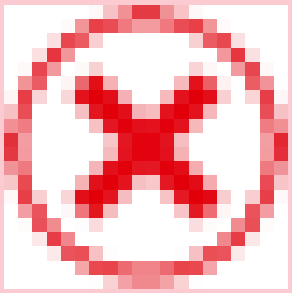
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

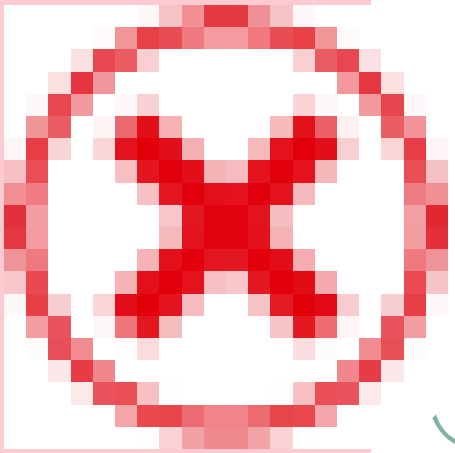
다음에 대한 모듈 액세스: **admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job**

다른 역할에 대한 정보:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

모듈	관리자	sn_sec_cmn.관리자	**sn_sec_cmn.ci_manager**	**sn_sec_cmn.manage_background_job**	sn_sec_c
개요	✓	✓	✗	✗	✓





다음에 대한 모듈 액세스: **sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image**

다음에 대한 모듈 액세스: **sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image**

다른 역할에 대한 정보:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

모듈	**sn_sec_cmn.reclassify_unmatch_ci**	sn_si.관리자	sn_si.기초의	**sn_vul.read_discovered_item**	**sn_vul_c**
(메인 앱 그룹)					

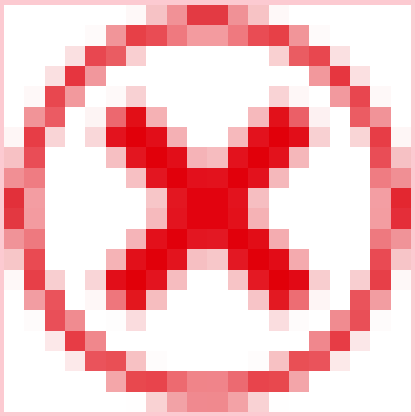
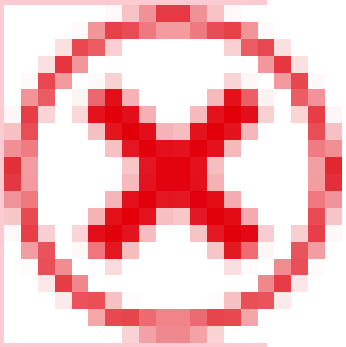
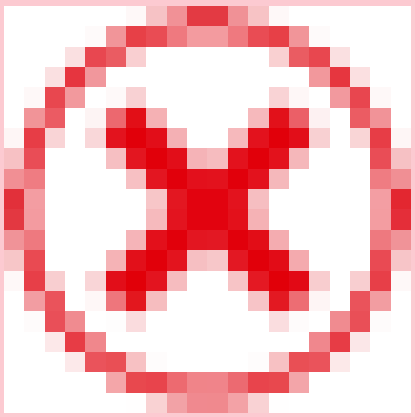
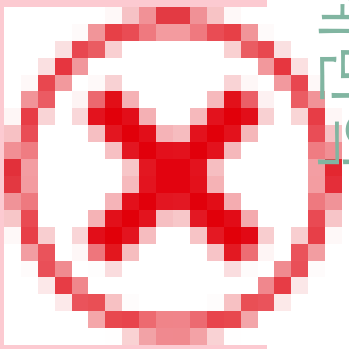
기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image**

다른 역할에 대한 정보:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

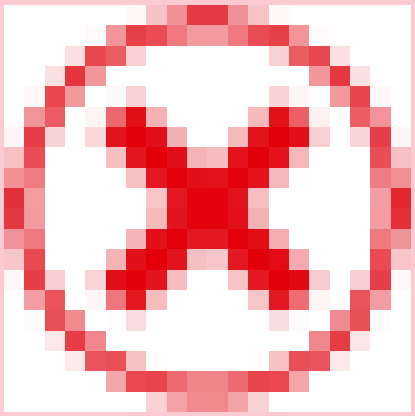
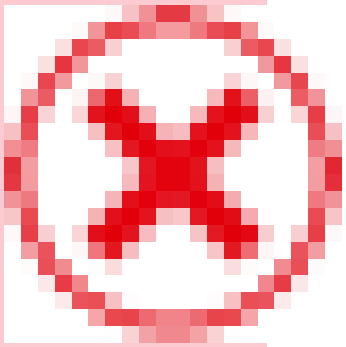
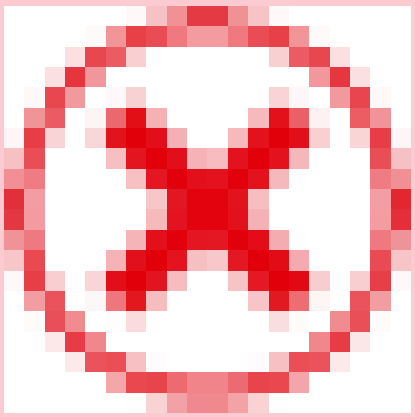
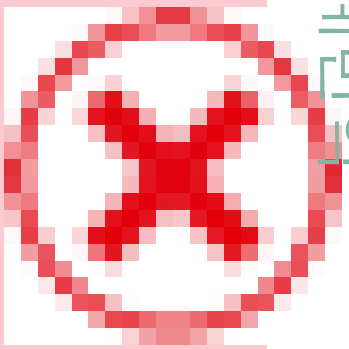
모듈	sn_sec_cmn.reclassify_unmatch_ci	sn_si.관리자	sn_si.기초의	sn_vul.read_discovered_item	sn_vul_c
통합					
통합 역량 플로우					

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image**

다른 역할에 대한 정보:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

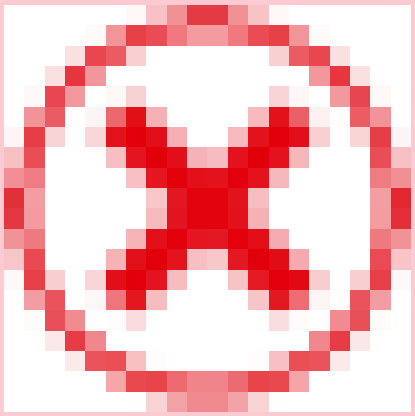
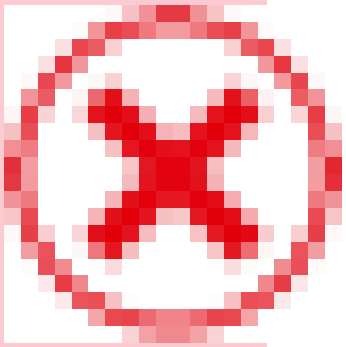
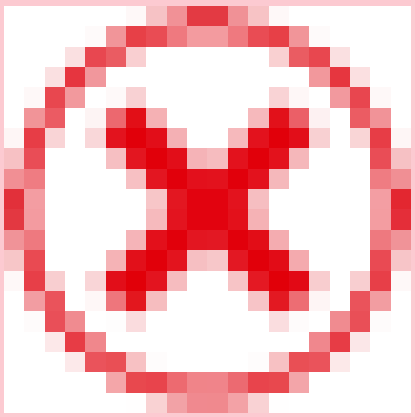
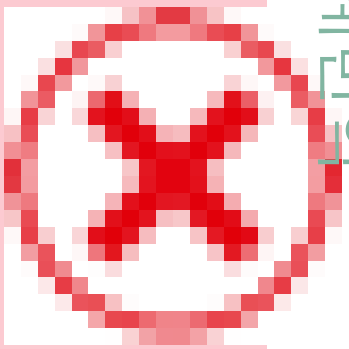
모듈	sn_sec_cmn.reclassify_unmatch_ci	sn_si.관리자	sn_si.기초의	sn_vul.read_discovered_item	sn_vul_c
역량 실행					
역량 구현 비율 제한					

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image**

다른 역할에 대한 정보:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

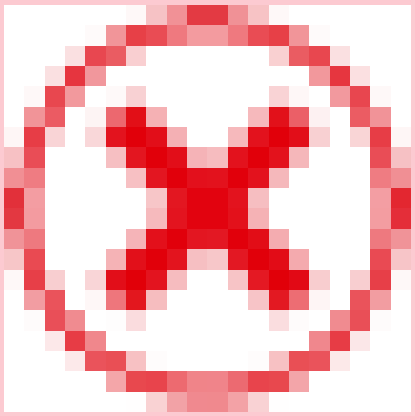
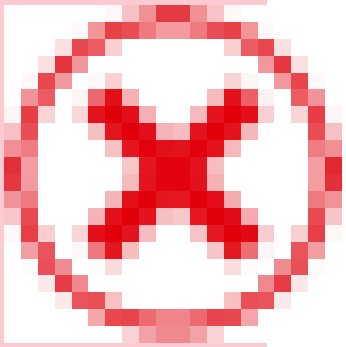
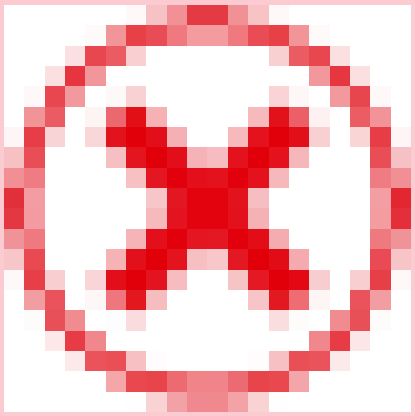
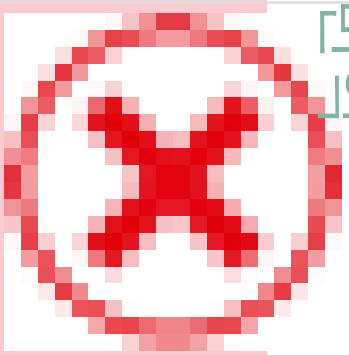
모듈	sn_sec_cmn.reclassify_unmatch_ci	sn_si.관리자	sn_si.기초의	sn_vul.read_discovered_item	sn_vul_c
통합 구성					
사이팅 검색 구성					

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image**

다른 역할에 대한 정보:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

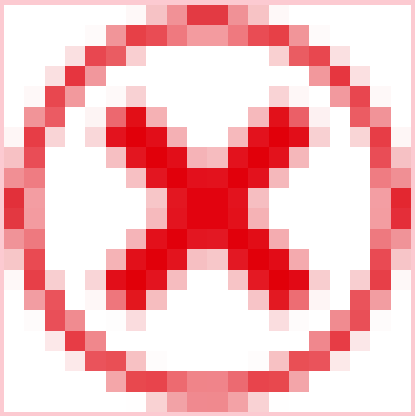
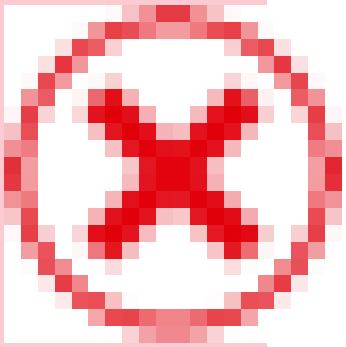
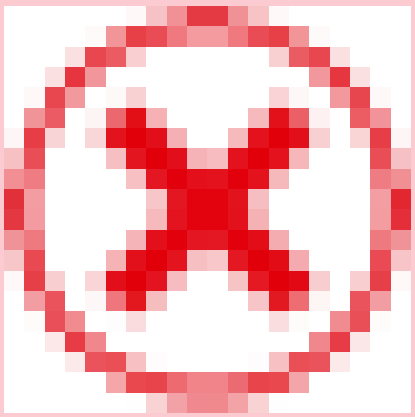
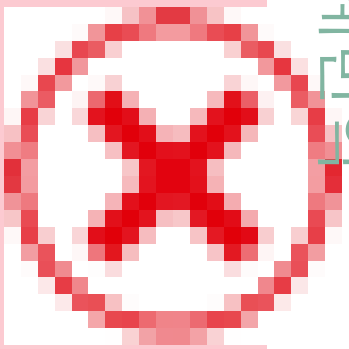
모듈	sn_sec_cmn.reclassify_unmatch_ci	sn_si.관리자	sn_si.기초의	sn_vul.read_discovered_item	sn_vul_c
통합 기능					
통합					
통합 역량 플로우					

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image**

다른 역할에 대한 정보:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

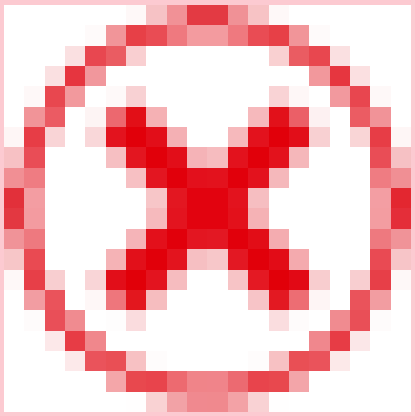
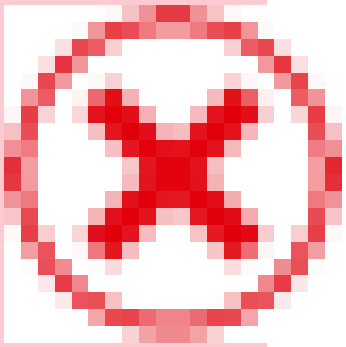
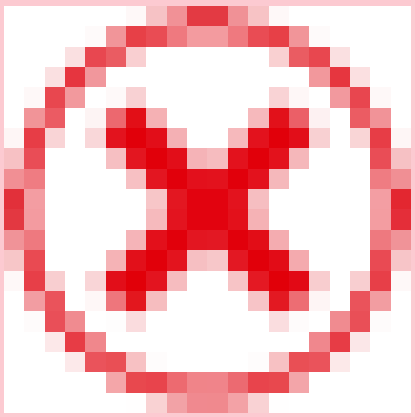
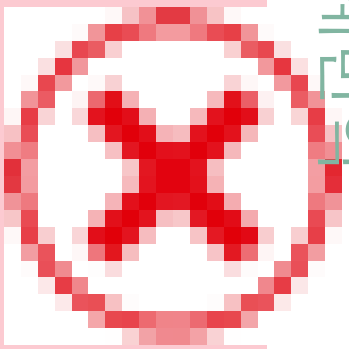
모듈	sn_sec_cmn.reclassify_unmatch_ci	sn_si.관리자	sn_si.기초의	sn_vul.read_discovered_item	sn_vul_c
역량 실행					
역량 구현 비율 제한					

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image**

다른 역할에 대한 정보:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

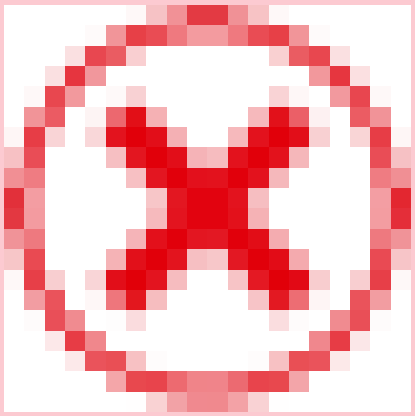
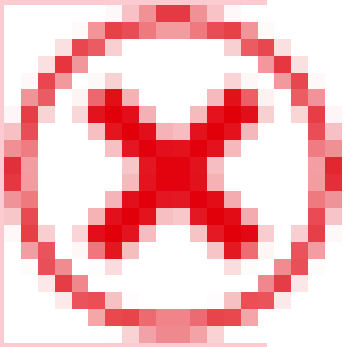
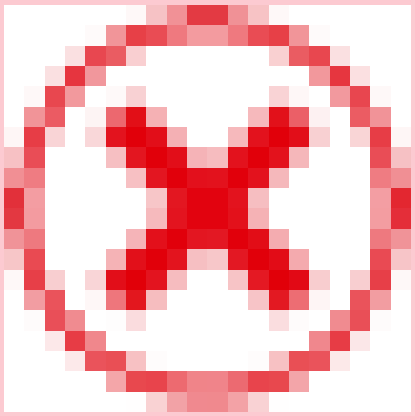
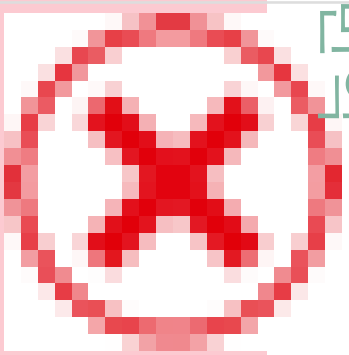
모듈	sn_sec_cmn.reclassify_unmatch_ci	sn_si.관리자	sn_si.기초의	sn_vul.read_discovered_item	sn_vul_c
통합 구성					
사이팅 검색 구성					

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image**

다른 역할에 대한 정보:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

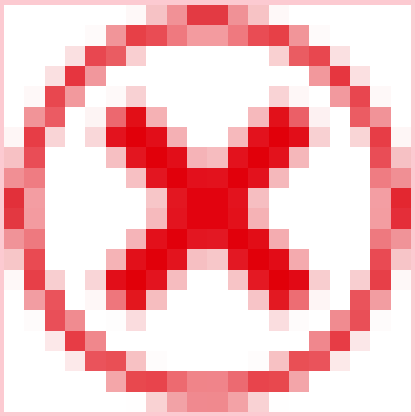
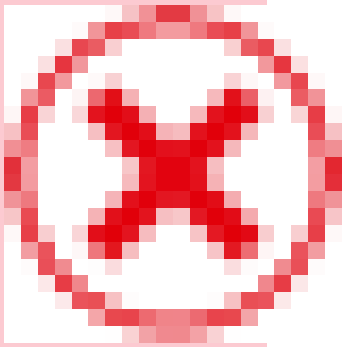
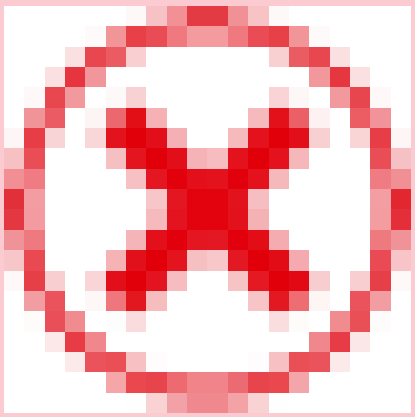
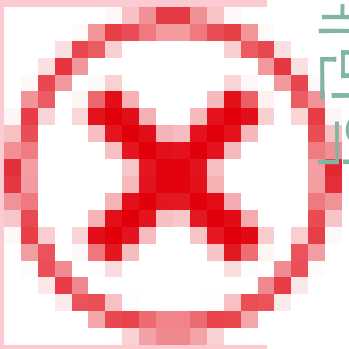
모듈	sn_sec_cmn.reclassify_unmatch_ci	sn_si.관리자	sn_si.기초의	sn_vul.read_discovered_item	sn_vul_c
통합 기능					
이메일 처리					
이메일 구문 분석					

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image**

다른 역할에 대한 정보:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

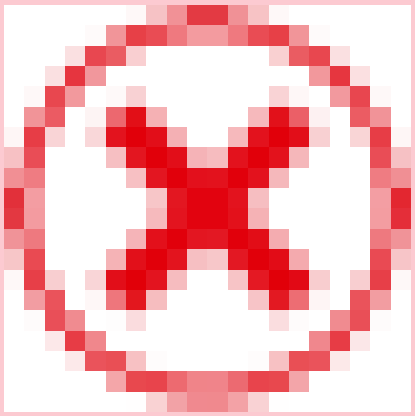
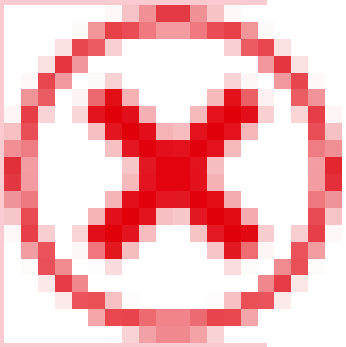
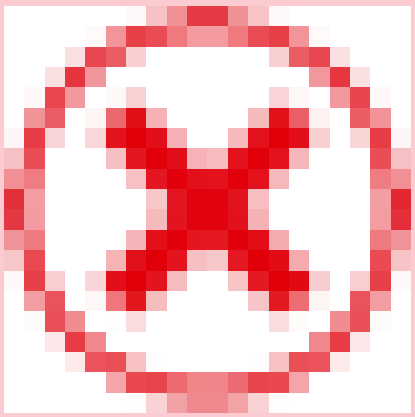
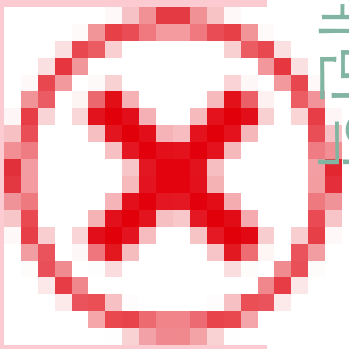
모듈	sn_sec_cmn.reclassify_unmatch_ci	sn_si.관리자	sn_si.기초의	sn_vul.read_discovered_item	sn_vul_c
중복 규칙					
속성					

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image**

다른 역할에 대한 정보:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

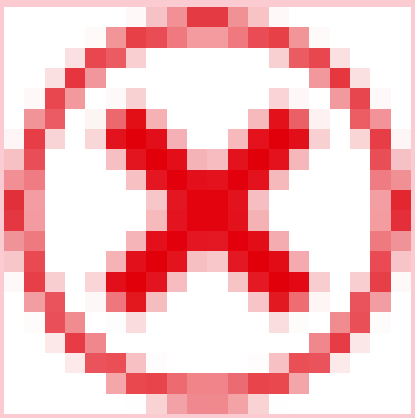
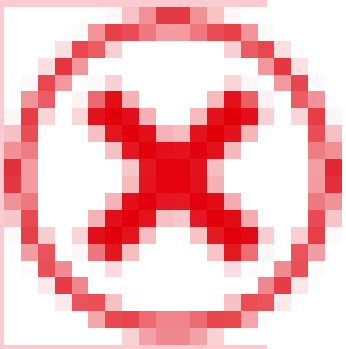
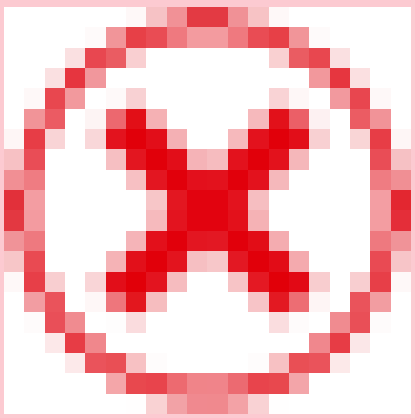
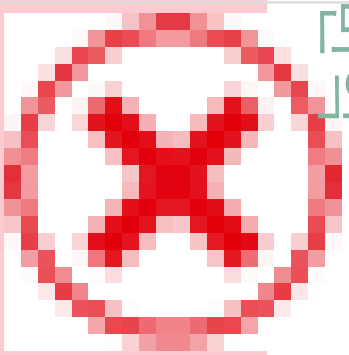
모듈	sn_sec_cmn.reclassify_unmatch_ci	sn_si.관리자	sn_si.기초의	sn_vul.read_discovered_item	sn_vul_c
일치하지 않는 이메일					
수집 규칙 사용자가 보고한 피싱					

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image**

다른 역할에 대한 정보:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

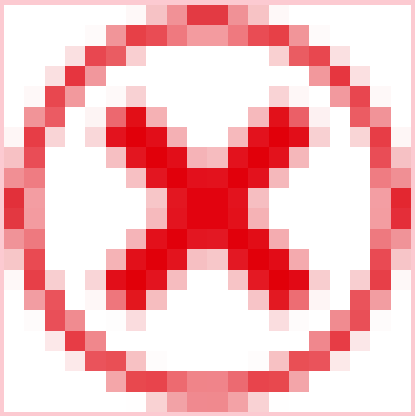
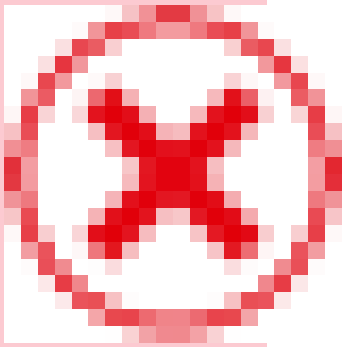
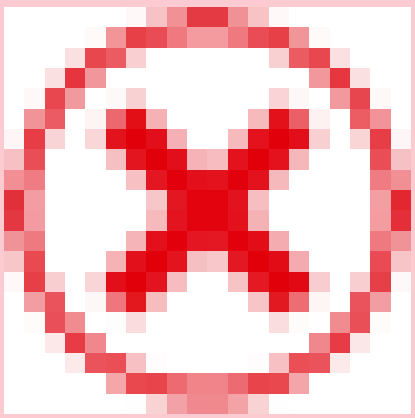
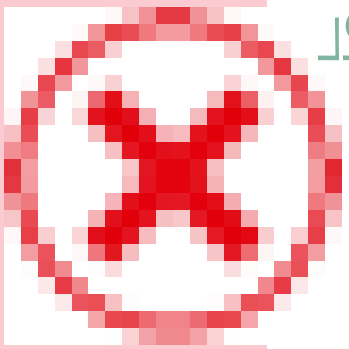
모듈	sn_sec_cmn.reclassify_unmatch_ci	sn_si.관리자	sn_si.기초의	sn_vul.read_discovered_item	sn_vul_c
사용자가 보고한 피싱 속성					
그룹					
필터 그룹					

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image**

다른 역할에 대한 정보:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

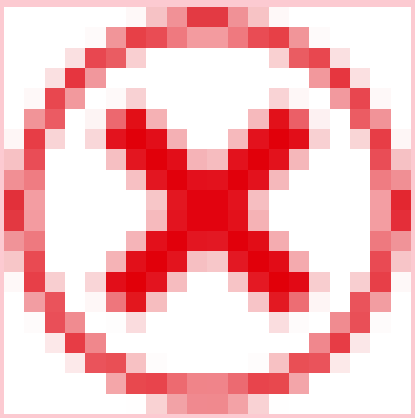
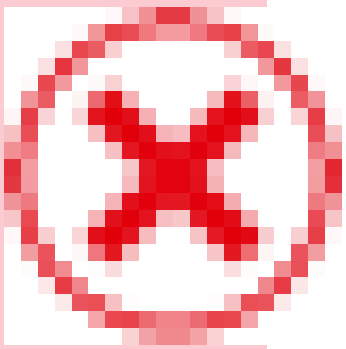
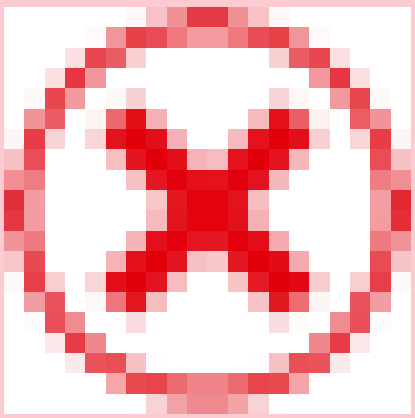
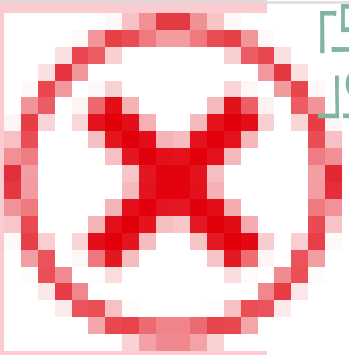
모듈	sn_sec_cmn.reclassify_unmatch_ci	sn_si.관리자	sn_si.기초의	sn_vul.read_discovered_item	sn_vul_c
에스컬레이션					
데이터 강화					
보안 태그					
그룹					

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image**

다른 역할에 대한 정보:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

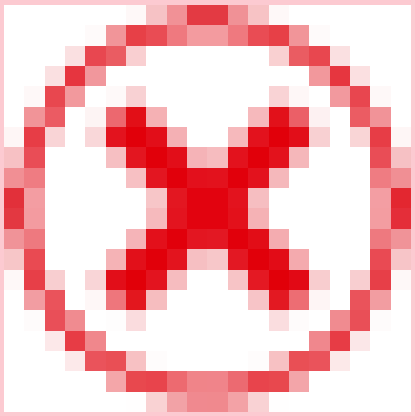
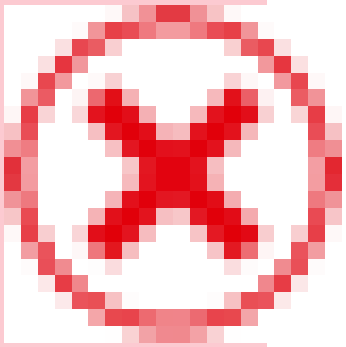
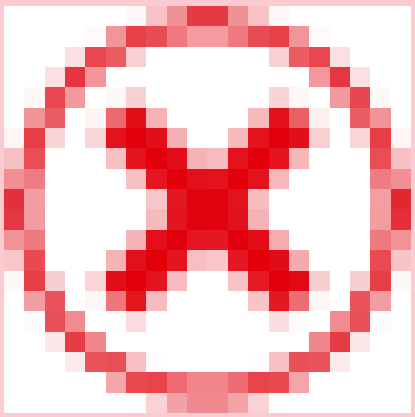
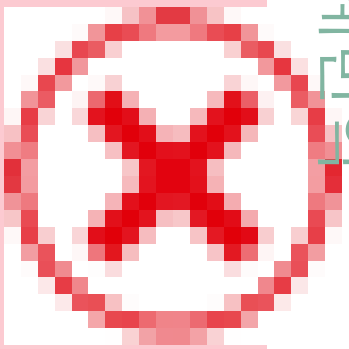
모듈	sn_sec_cmn.reclassify_unmatch_ci	sn_si.관리자	sn_si.기초의	sn_vul.read_discovered_item	sn_vul_c
태그					
워크플로우					
실행 추적					

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image**

다른 역할에 대한 정보:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

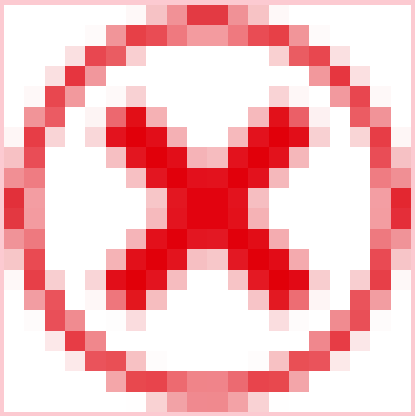
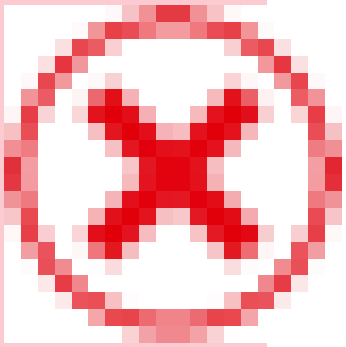
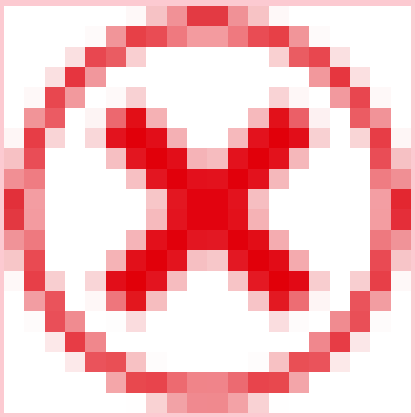
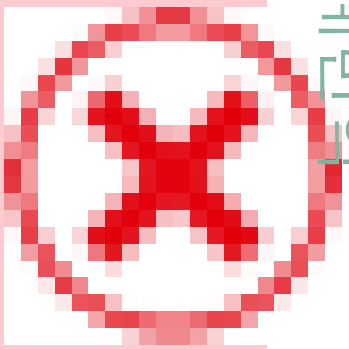
모듈	sn_sec_cmn.reclassify_unmatch_ci	sn_si.관리자	sn_si.기초의	sn_vul.read_discovered_item	sn_vul_c
보안 워크플로우 보기					
워크플로우 트리거					
유틸리티					

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image**

다른 역할에 대한 정보:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

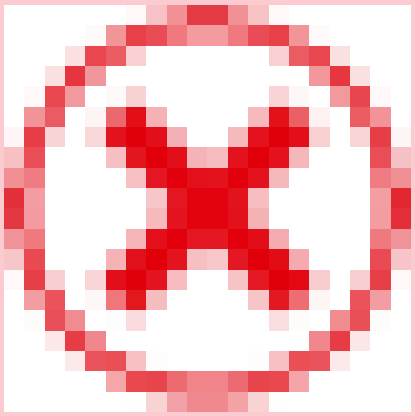
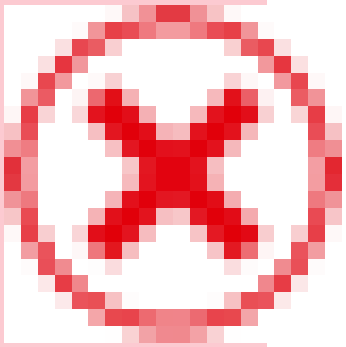
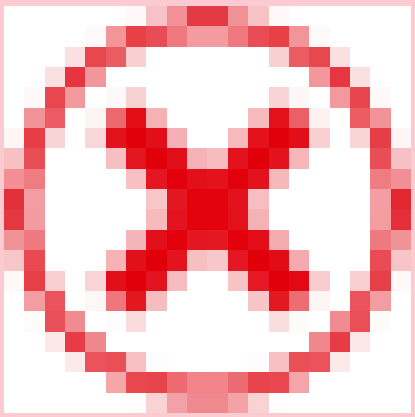
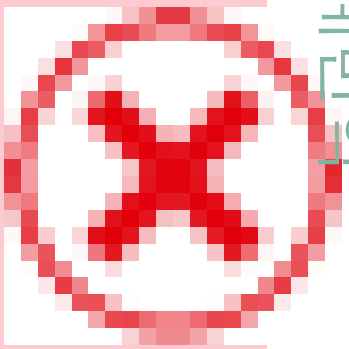
모듈	sn_sec_cmn.reclassify_unmatch_ci	sn_si.관리자	sn_si.기초의	sn_vul.read_discovered_item	sn_vul_c
보강 데이터 매핑					
필드 값 변환					

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image**

다른 역할에 대한 정보:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

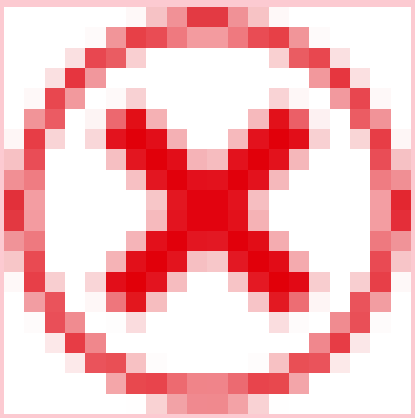
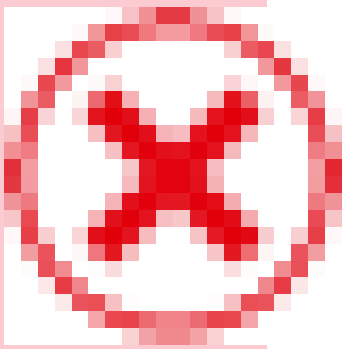
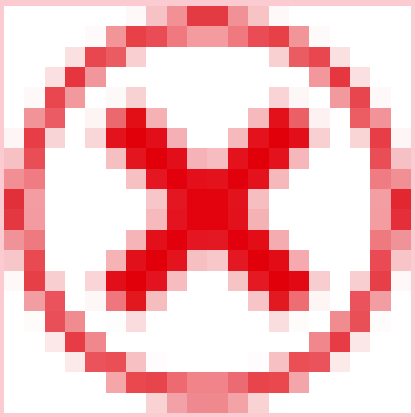
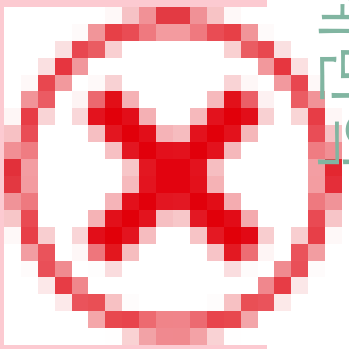
모듈	sn_sec_cmn.reclassify_unmatch_ci	sn_si.관리자	sn_si.기초의	sn_vul.read_discovered_item	sn_vul_c
필드 매핑					
온디맨드 오케스트레이션					

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image**

다른 역할에 대한 정보:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

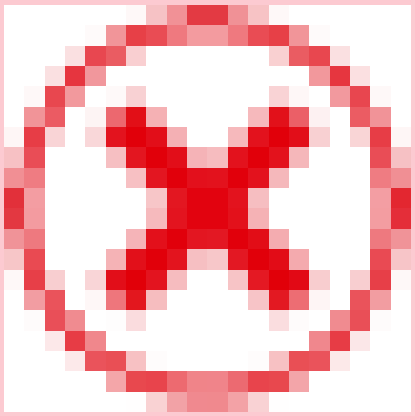
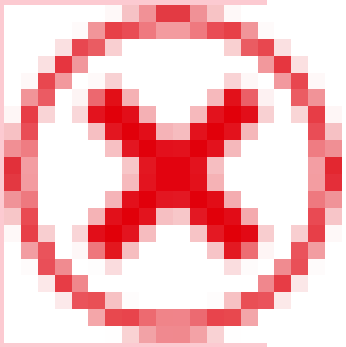
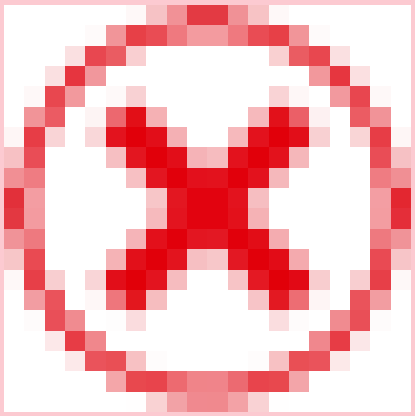
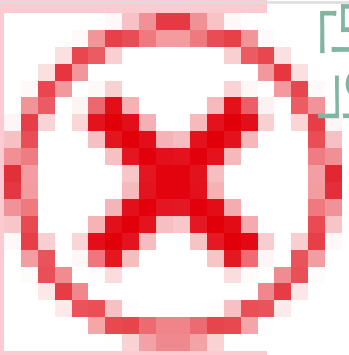
모듈	sn_sec_cmn.reclassify_unmatch_ci	sn_si.관리자	sn_si.기초의	sn_vul.read_discovered_item	sn_vul_c
운영 체제 그룹					
SecOps 애플리케이션 레지스트리					

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image**

다른 역할에 대한 정보:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

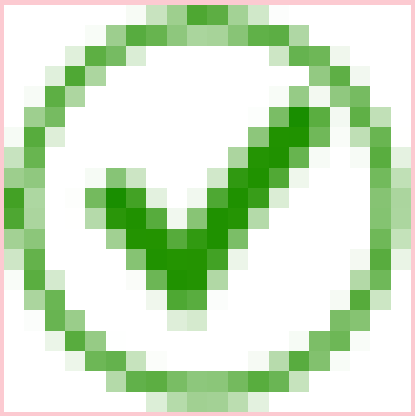
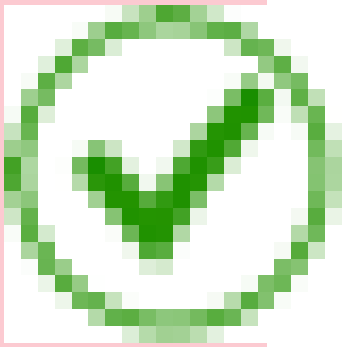
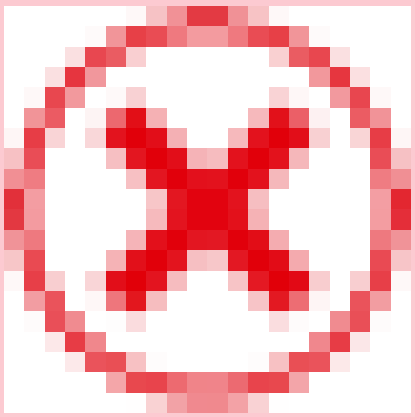
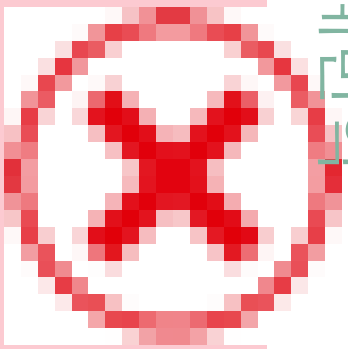
모듈	sn_sec_cmn.reclassify_unmatch_ci	sn_si.관리자	sn_si.기초의	sn_vul.read_discovered_item	sn_vul_c
백그라운드 작업 구성					
CMDB					
CI 조회 규칙					

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image**

다른 역할에 대한 정보:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

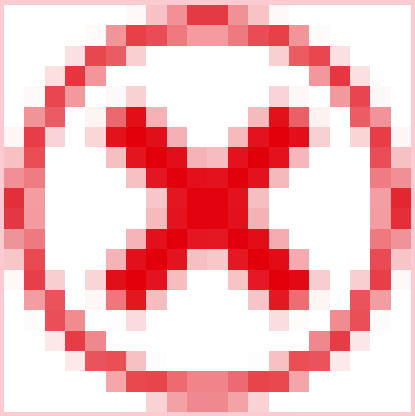
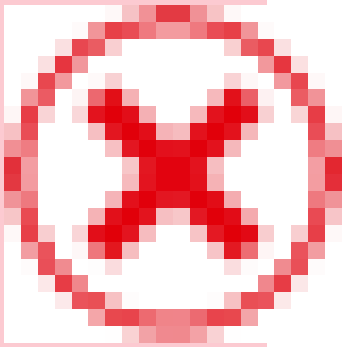
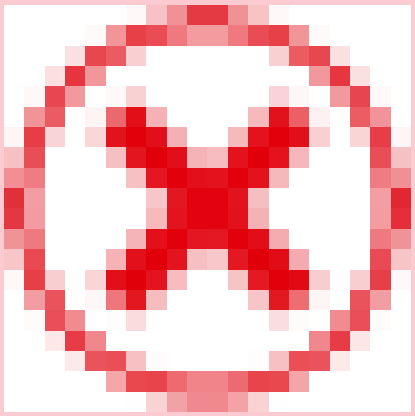
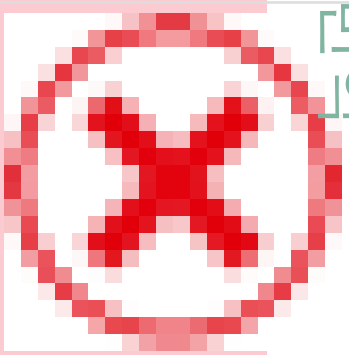
모듈	sn_sec_cmn.reclassify_unmatch_ci	sn_si.관리자	sn_si.기초의	sn_vul.read_discovered_item	sn_vul_c
검색된 항목					
불일치하는 검색된 항목을 일치시키기					

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image**

다른 역할에 대한 정보:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

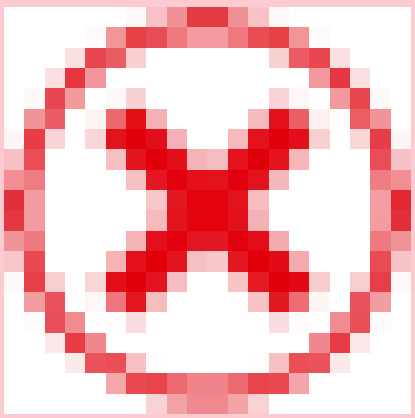
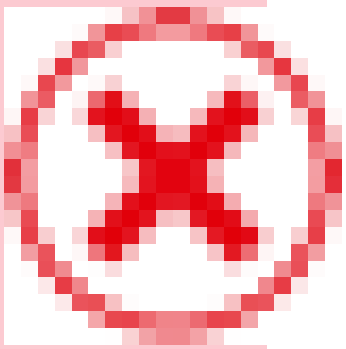
모듈	sn_sec_cmn.reclassify_unmatch_ci	sn_si.관리자	sn_si.기초의	sn_vul.read_discovered_item	sn_vul_c
탐색한 컨테이너 이미지					
WatchDog					
구성					

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image**

다른 역할에 대한 정보:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

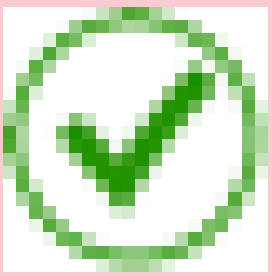
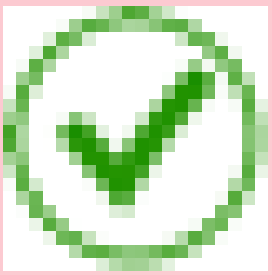
모듈	sn_sec_cmn.reclassify_unmatch_ci	sn_si.관리자	sn_si.기초의	sn_vul.read_discovered_item	sn_vul_c
개요					

〔End〕

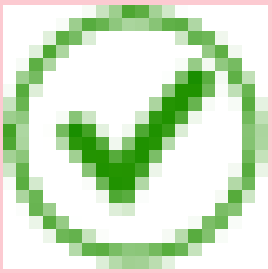
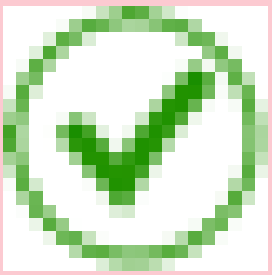
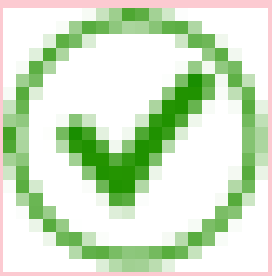
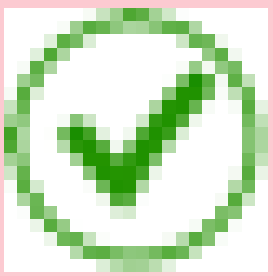
〔store-future: BEGIN review〕

Splunk 통합을 위한 역할별 모듈 액세스

Splunk 통합의 경우 특정 역할이 액세스할 수 있는 메뉴 항목을 참조하십시오.

모듈	sn_si.관리자	sn_si.분석자
(메인 앱 그룹)		
Splunk 이벤트 프로파일		
Splunk 필드 번역		

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

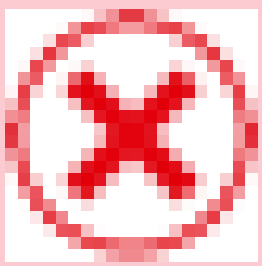
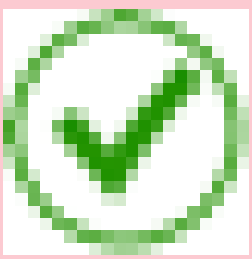
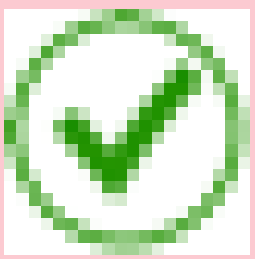
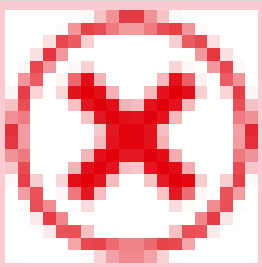
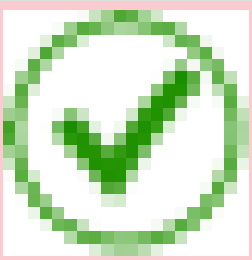
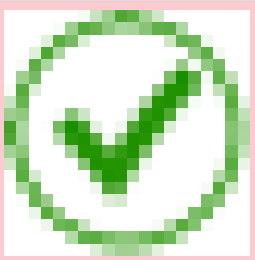
모듈	sn_si.관리자	sn_si.분석자
Splunk 작업에 대한 이벤트		
Splunk 이벤트 임포트		
Splunk Integration 설정		

〔End〕

〔store-future: BEGIN review〕

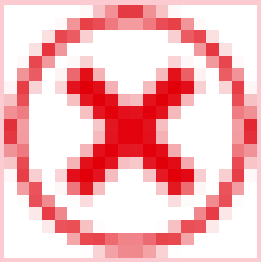
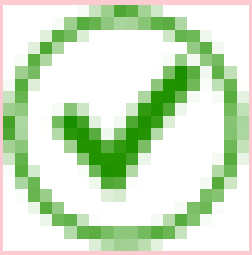
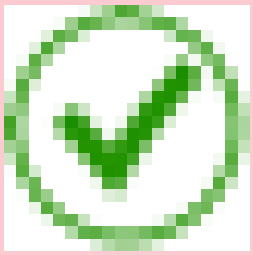
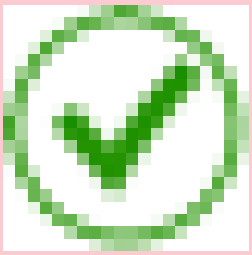
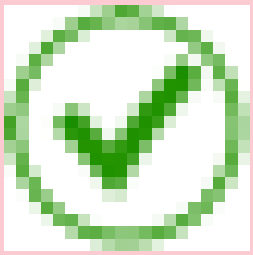
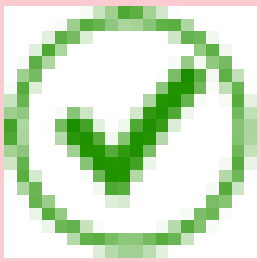
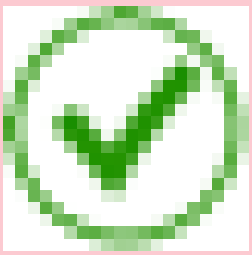
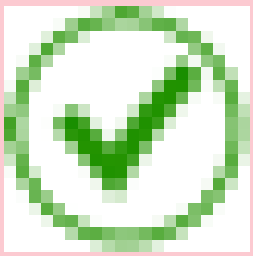
Symantec DLP 통합을 위한 역할별 모듈 액세스

Symantec DLP 통합의 경우 특정 역할로 액세스할 수 있는 메뉴 항목을 참조하십시오.

모듈	**agent_admin**	sn_dlir.관리자	sn_dlir.분석자
(메인 앱 그룹)			
인시던트 프로파일			
인시던트 상태 매핑			

기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

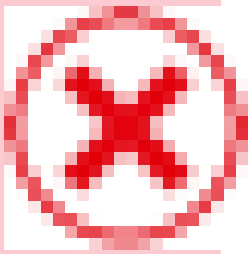
모듈	**agent_admin**	sn_dlir.관리자	sn_dlir.분석자
설정			
MID 애플리케이션			
MID 서버			

〔End〕

〔store-future: BEGIN review〕

Threat Intelligence에 대한 역할별 모듈 액세스

Threat Intelligence의 경우 특정 역할이 액세스할 수 있는 메뉴 항목을 참조하십시오.

모듈	sn_si.관리자	sn_si.분석자	**sn_si.CISO**	sn_si.매니저	sn_ti.관리자	**sn_ti.case_user_read**	sn_ti.읽다	sn
(메인 앱 그룹)								
객체								
객체								
IoC 리포지토리								

기계 번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈	sn_si.관리자	sn_si.분석자	**sn_si.CISO**	sn_si.매니저	sn_ti.관리자	**sn_ti.case_user_read**	sn_ti.읽다	sn
공격 모드메소드	✓	✓	✓	✓	✓	✓	✓	
표시기	✓	✓	✓	✓	✓	✓	✓	
옵저버블	✓	✓	✓	✓	✓	✓	✓	
공격 패턴	✓	✓	✓	✓	✓	✓	기술 분석	
캠페인	✓	✓	✓	✓	✓	✓	✓	
작업 방침	✓	✓	✓	✓	✓	✓	✓	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈	sn_si.관리자	sn_si.분석자	**sn_si.CISO**	sn_si.매니저	sn_ti.관리자	**sn_ti.case_user_read**	sn_ti.읽다	sn
ID	✓	✓	✓	✓	✓	✓	✓	
인프라	✓	✓	✓	✓	✓	✓	✓	
위치	✓	✓	✓	✓	✓	✓	✓	
맬웨어	✓	✓	✓	✓	✓	✓	✓	
침입 세트	✓	✓	✓	✓	✓	✓	✓	
위협 액터	✓	✓	✓	✓	✓	✓	✓	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈	sn_si.관리자	sn_si.분석자	**sn_si.CISO**	sn_si.매니저	sn_ti.관리자	**sn_ti.case_user_read**	sn_ti.읽다	sn
맬웨어 분석	✓	✓	✓	✓	✓	✓	✓	
관찰 데이터	✓	✓	✓	✓	✓	✓	✓	
위협 그룹화	✓	✓	✓	✓	✓	✓	✓	
표시 정의	✓	✓	✓	✓	✓	✓	✓	
위협 메모	✓	✓	✓	✓	✓	✓	✓	
위협 의견	✓	✓	✓	✓	✓	✓	✓	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈	sn_si.관리자	sn_si.분석자	**sn_si.CISO**	sn_si.매니저	sn_ti.관리자	**sn_ti.case_user_read**	sn_ti.읽다	sn
위협 보고서	✓	✓	✓	✓	✓	✓	✓	
표시기 목격	✓	✓	✓	✓	✓	✓	✓	
객체 사이팅	✓	✓	✓	✓	✓	✓	✓	
취약성	✓	✓	✓	✓	✓	✓	✓	
도구	✓	✓	✓	✓	✓	✓	✓	
ObjectObject 관계	✓	✓	✓	✓	✓	✓	✓	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈	sn_si.관리자	sn_si.분석자	**sn_si.CISO**	sn_si.매니저	sn_ti.관리자	**sn_ti.case_user_read**	sn_ti.읽다	sn
ObjectIndicator 관계	✓	✓	✓	✓	✓	✓	✓	
ObjectObservable 관계	✓	✓	✓	✓	✓	✓	✓	
소스								
위협 소스	✗	✗	✗	✗	✓	✗	✗	
TAXII 프로파일	✗	✗	✗	✗	✓	✗	✗	
외부 인텔리전스								
데이터 위반 라이브러리	✓	✓	✓	✓	✓	✓	✓	
WHOIS 라이브러리	✓	✓	✓	✓	✓	✓	✓	
관리								

기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈	sn_si.관리자	sn_si.분석자	**sn_si.CISO**	sn_si.매니저	sn_ti.관리자	**sn_ti.case_user_read**	sn_ti.읽다	sn
속성	✗	✗	✗	✗	✓	✗	✗	
공격 메커니즘	✗	✗	✗	✗	✓	✗	✗	
공격 동기	✗	✗	✗	✗	✓	✗	✗	
디스커버리 방법	✗	✗	✗	✗	✓	✗	✗	
피드	✗	✗	✗	✗	✓	✗	✗	
표시기 유형	✗	✗	✗	✗	✓	✗	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈	sn_si.관리자	sn_si.분석자	**sn_si.CISO**	sn_si.매니저	sn_ti.관리자	**sn_ti.case_user_read**	sn_ti.읽다	sn
인프라 유형	✗	✗	✗	✗	✓	✗	✗	
의도된 효과	✗	✗	✗	✗	✓	✗	✗	
맬웨어 역량	✗	✗	✗	✗	✓	✗	✗	
맬웨어 유형	✗	✗	✗	✗	✓	✗	✗	
알림	✗	✗	✗	✗	✓	✗	✗	
관찰 대상 유형	✗	✗	✗	✗	✓	✗	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈	sn_si.관리자	sn_si.분석자	**sn_si.CISO**	sn_si.매니저	sn_ti.관리자	**sn_ti.case_user_read**	sn_ti.읽다	sn
속도 제한 정의	✗	✗	✗	✗	✓	✗	✗	
보고서 유형	✗	✗	✗	✗	✓	✗	✗	
위협 액터 역할	✗	✗	✗	✗	✓	✗	✗	
위협 액터 유형	✗	✗	✗	✗	✓	✗	✗	
도구 유형	✗	✗	✗	✗	✓	✗	✗	
케이스 관리								
모든 케이스	✗	✗	✗	✗	✗	✓	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈	sn_si.관리자	sn_si.분석자	**sn_si.CISO**	sn_si.매니저	sn_ti.관리자	**sn_ti.case_user_read**	sn_ti.읽다	sn
오픈 케이스	✗	✗	✗	✗	✗	✓	✗	
내 케이스	✗	✗	✗	✗	✗	✓	✗	
MITRE ATT&CK 리포지토리								
개요	✓	✓	✓	✓	✓	✓	✓	
매트릭스	✓	✓	✓	✓	✓	✓	✓	
기술	✓	✓	✓	✓	✓	✓	✓	
완화	✓	✓	✓	✓	✓	✓	✓	

기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈	sn_si.관리자	sn_si.분석자	**sn_si.CISO**	sn_si.매니저	sn_ti.관리자	**sn_ti.case_user_read**	sn_ti.읽다	sn
그룹	✓	✓	✓	✓	✓	✓	✓	
맬웨어	✓	✓	✓	✓	✓	✓	✓	
도구	✓	✓	✓	✓	✓	✓	✓	
MITRE 관계	✓	✓	✓	✓	✓	✓	✓	
히트맵 및 네비게이터	✓	✓	✓	✓	✓	✓	✓	
CVE 기술 매핑	✓	✓	✓	✓	✓	✓	✓	
MITRE ATT&CK 관리								

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈	sn_si.관리자	sn_si.분석자	**sn_si.CISO**	sn_si.매니저	sn_ti.관리자	**sn_ti.case_user_read**	sn_ti.읽다	sn
데이터 소스 매핑	✓	✓	✓	✓	✓	✓	✓	
데이터 구성요소 매핑	✓	✓	✓	✓	✓	✓	✓	
탐지 범위 정의	✓	✓	✓	✓	✓	✓	✓	
탐지 범위 매핑	✓	✓	✓	✓	✓	✓	기술 문서	
완화 범위 정의	✓	✓	✓	✓	✓	✓	✓	
완화 범위 계산기	✓	✓	✓	✓	✓	✓	✓	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈	sn_si.관리자	sn_si.분석자	**sn_si.CISO**	sn_si.매니저	sn_ti.관리자	**sn_ti.case_user_read**	sn_ti.읽다	sn
완화 범위 매핑	✓	✓	✓	✓	✓	✓	✓	
기술 추출 규칙	✓	✓	✓	✓	✓	✓	✓	
탐지 규칙 MITRE ATTCK 매핑	✓	✓	✓	✓	✓	✓	✓	
Threat GroupTechnique 히트맵 정의	✓	✓	✓	✓	✓	✓	✓	
위협 그룹MITRE ATTCK 기술 매핑	✓	✓	✓	✓	✓	✓	✓	
속성	✓	✗	✗	✗	✓	✗	✗	

〔End〕

〔store-future: BEGIN review〕

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Vulnerability Response에 대한 역할별 모듈 액세스

취약성 대응의 경우 특정 역할로 액세스할 수 있는 메뉴 항목을 참조하십시오.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

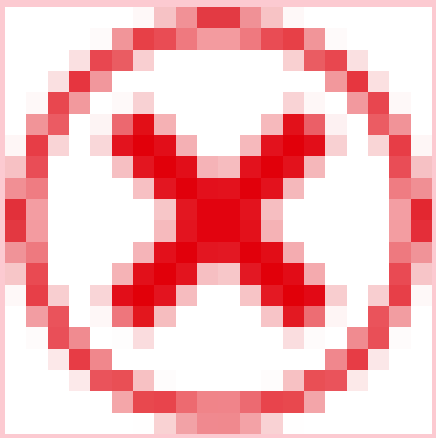
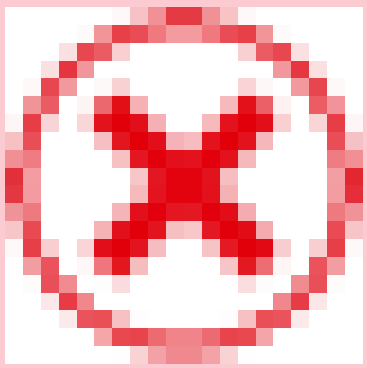
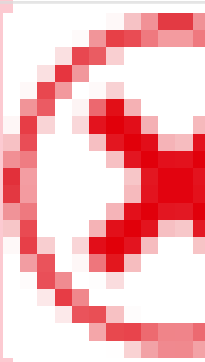
sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

기계번역

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
(메인 앱 그룹)				
CISO 대시보드				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
정정 개요	✗	✓	✗	✓

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
취약성 관리자 작업 공간	✗	✓	✗	✓

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
개요	✗	✓	✗	✓

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
IT 정정 작업 공간	✗	✗	✗	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
승인자 개요	✗	✓	✗	✓

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
개요	✗	✓	✗	✓

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
내 승인	✗	✓	✗	✓
정정 작업				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
활성	✗	✓	✗	✓

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
나에게 할당됨	✗	✓	✗	✓

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

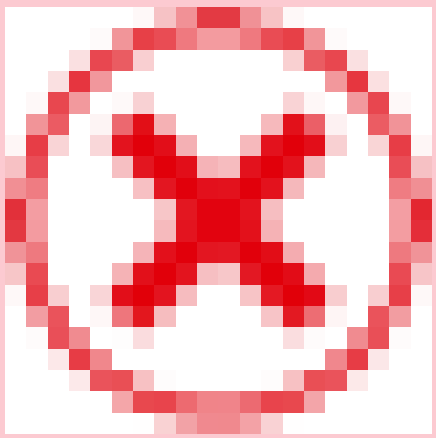
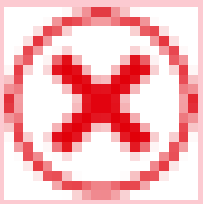
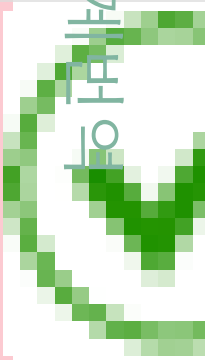
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
사용자 그룹에 할당됨				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

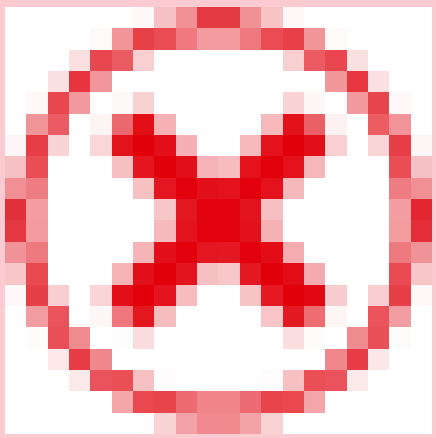
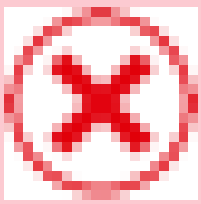
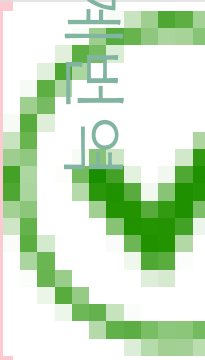
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
모두				

취약 항목

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

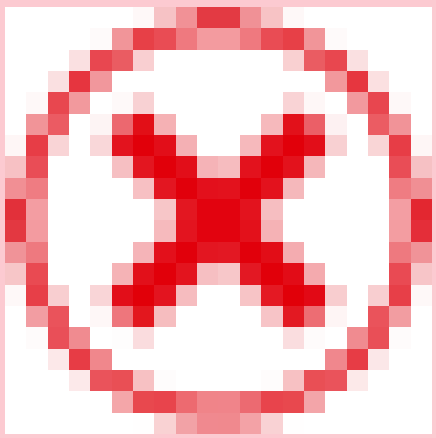
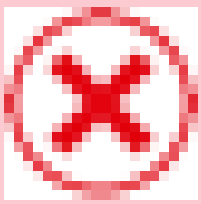
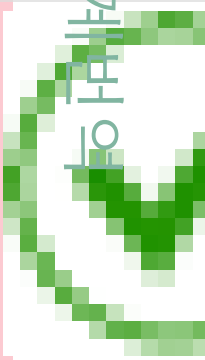
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
중요 위험				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

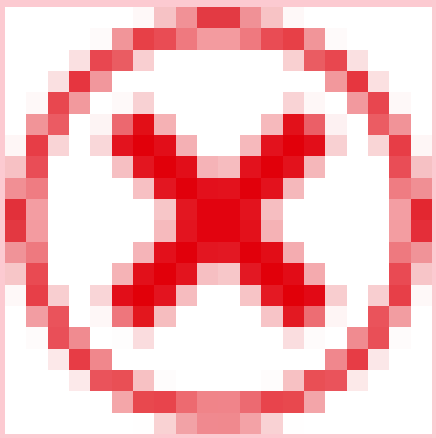
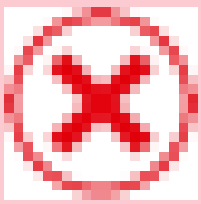
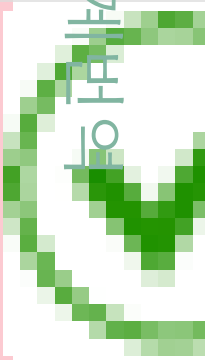
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
높은 위험				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
악용 가능	✗	✓	✗	✓

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
대상에 접근	✗	✓	✗	✓

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

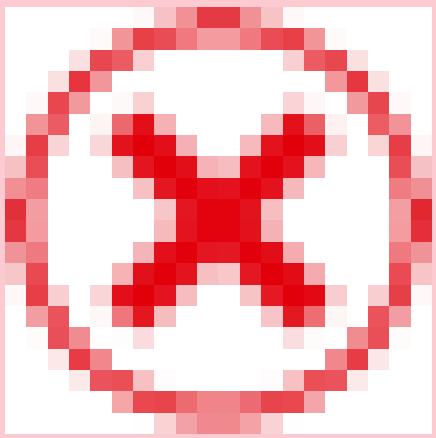
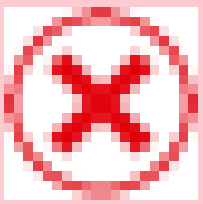
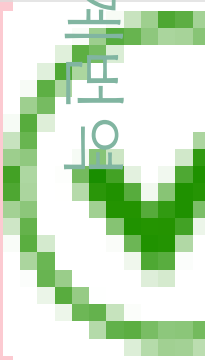
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
누락된 대상				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
지난 90일 이내	✗	✓	✗	✓

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

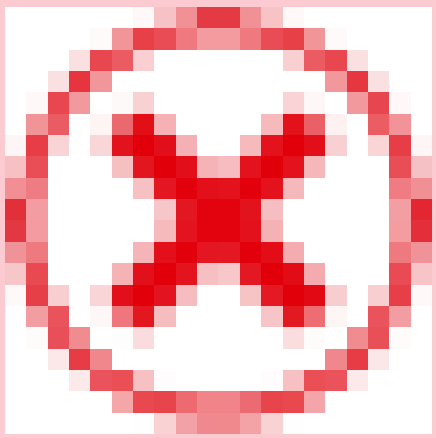
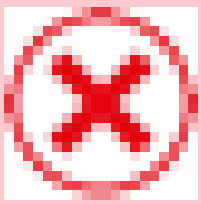
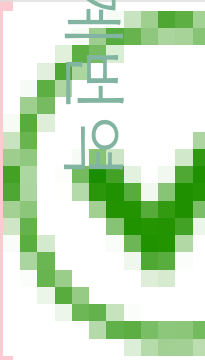
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
90일 경과				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
미할당	✗	✓	✗	✓

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
그룹 해제	✗	✓	✗	✓

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
해제됨	✗	✓	✗	✓

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
여러 지연	✗	✓	✗	✓

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
모두	✗	✓	✗	✓
솔루션				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
모두	✗	✓	✗	✓

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

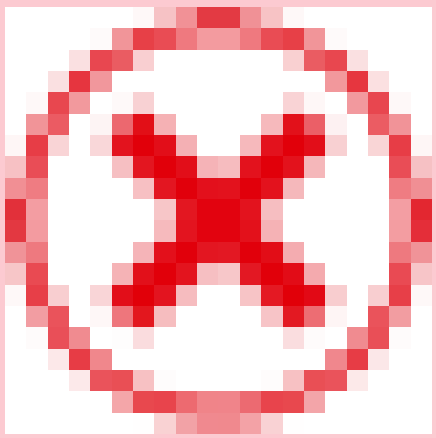
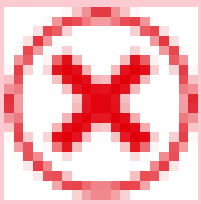
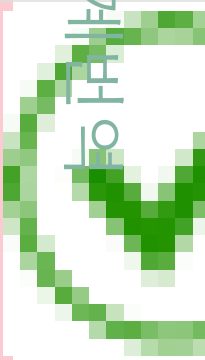
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
가장 높은 대체				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

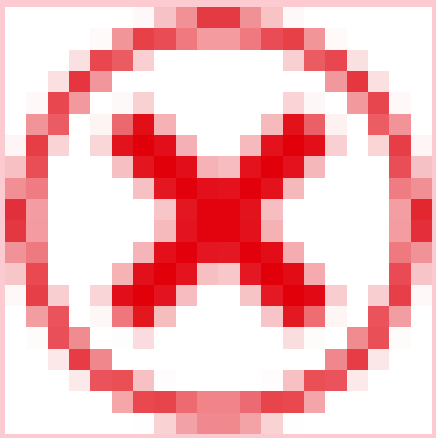
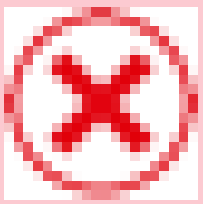
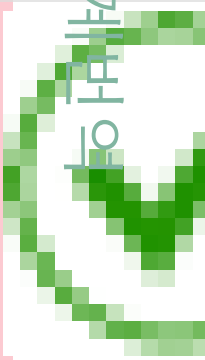
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
취약한 항목 포함				

라이브러리

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
NVD	✗	✓	✗	✓

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

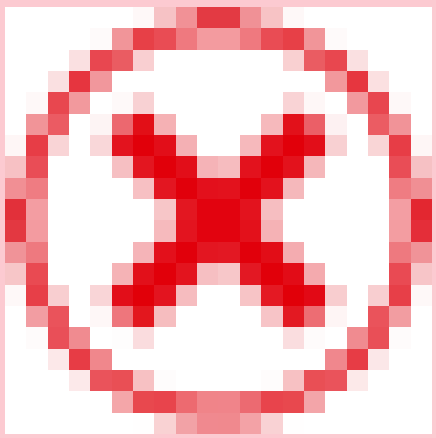
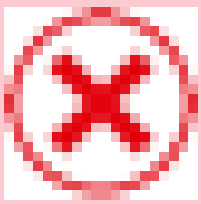
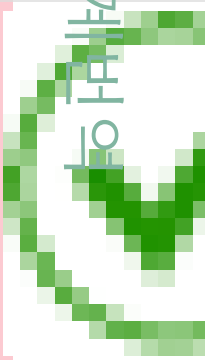
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
CWE				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

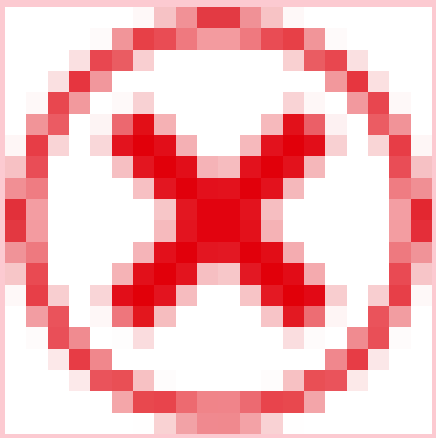
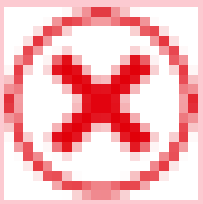
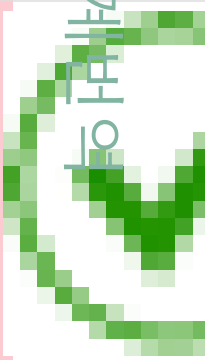
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
외부 공급업체				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

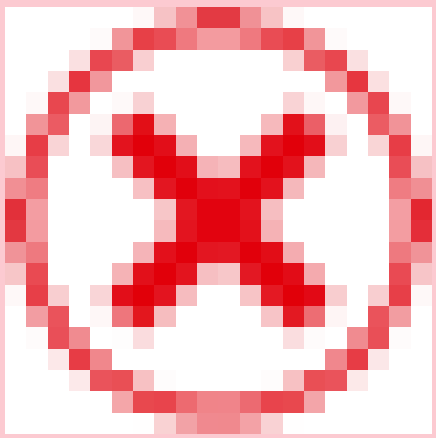
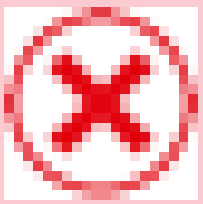
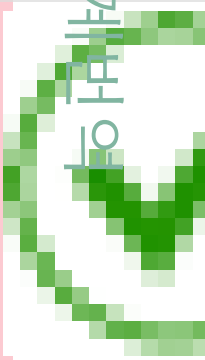
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
취약한 소프트웨어				

취약성 스캐닝

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
노출 평가	✗	✓	✗	✓

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
스캔	✗	✓	✗	✓

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
스캐너	✗	✓	✗	✓

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
스캔 큐	✗	✓	✗	✓

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

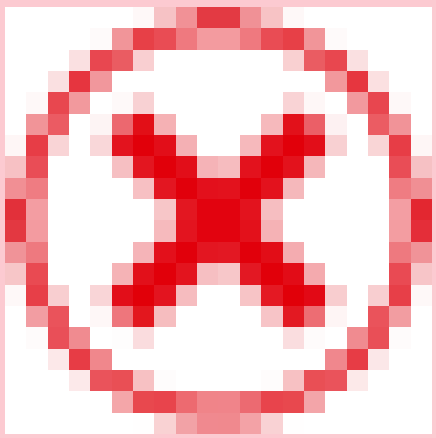
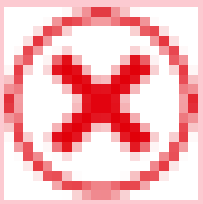
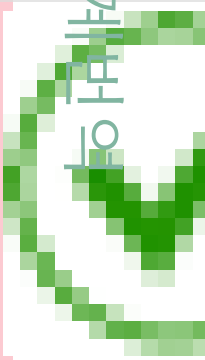
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
스캐너 속도 제한				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

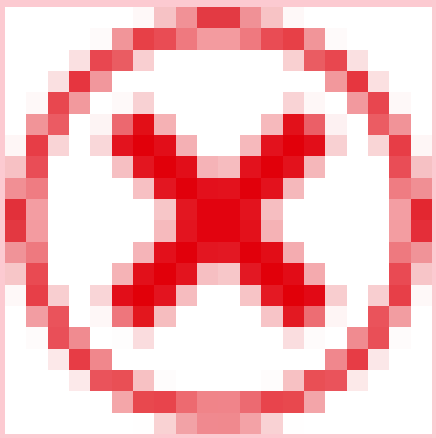
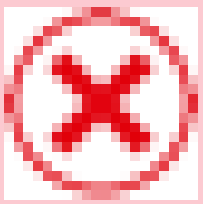
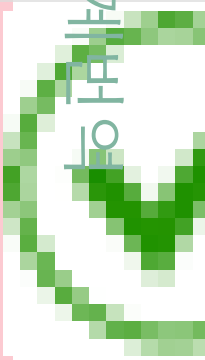
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
속도 제한 정의				

관리

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

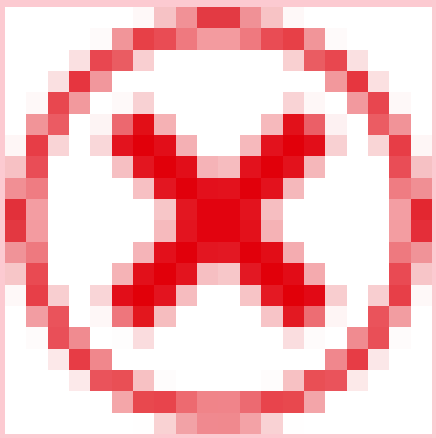
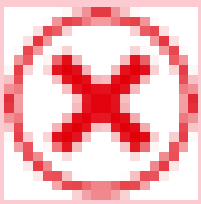
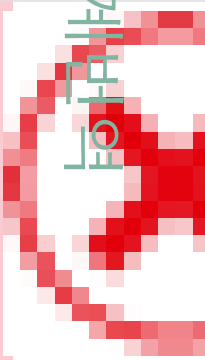
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
설정 도우미				

피드백

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
주시 주제	✗	✓	✗	✓

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
담당 규칙	✗	✓	✗	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

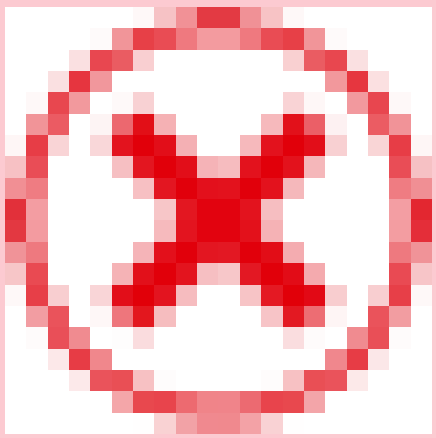
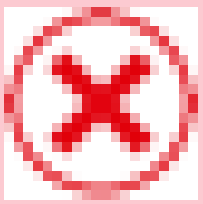
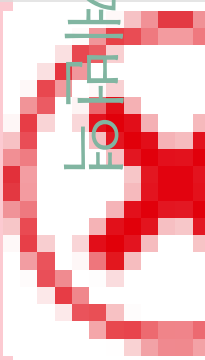
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
정정 작업 규칙				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
할당 권장 사항	✗	✗	✗	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
취약성 계산기	✗	✓	✗	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
취약성 롤업 계산기	✗	✓	✗	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

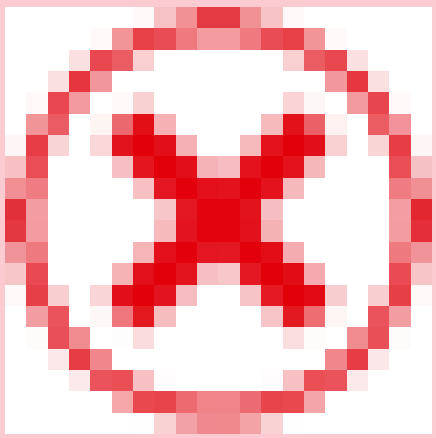
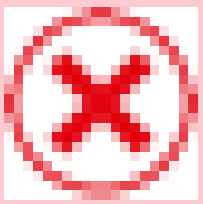
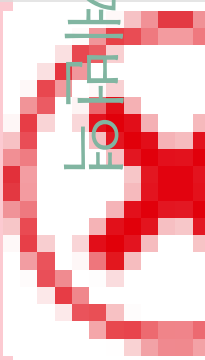
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
정정 대상 규칙				

고객 버전

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

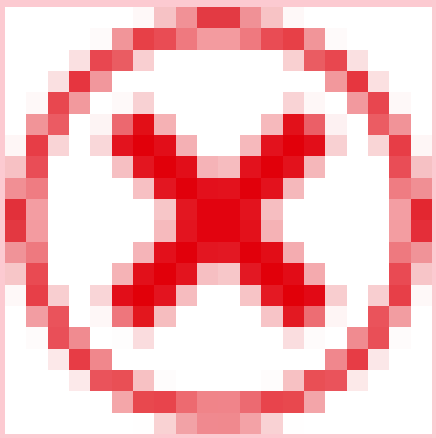
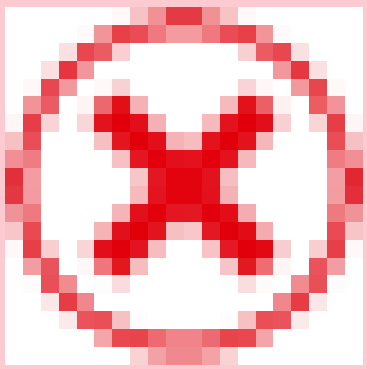
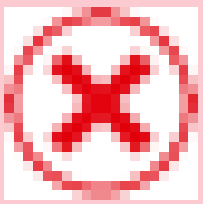
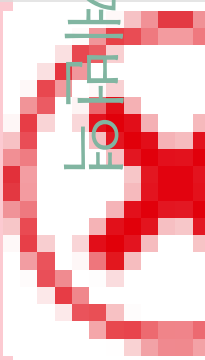
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
AutoClose 구성				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
자동 삭제 규칙	✗	✓	✗	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
예외 규칙	✗	✓	✗	✓

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

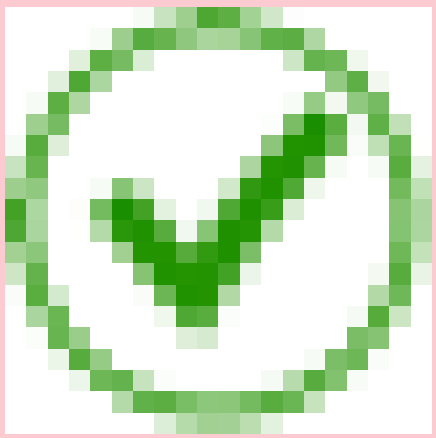
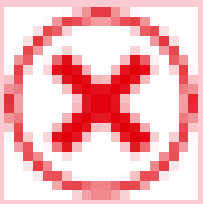
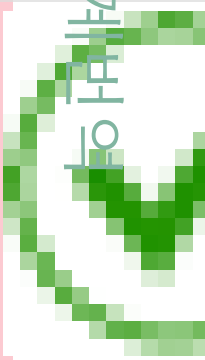
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
승인 규칙				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
분류 규칙				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

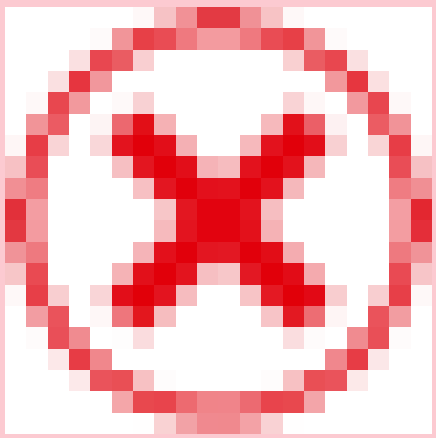
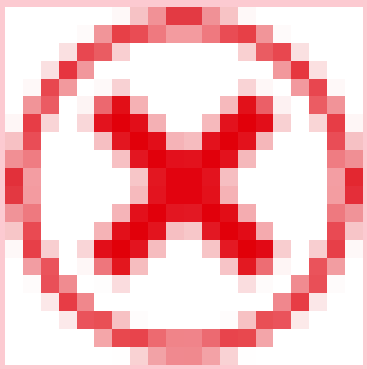
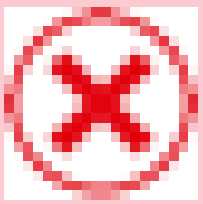
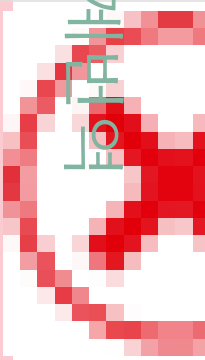
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
성과 구성				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

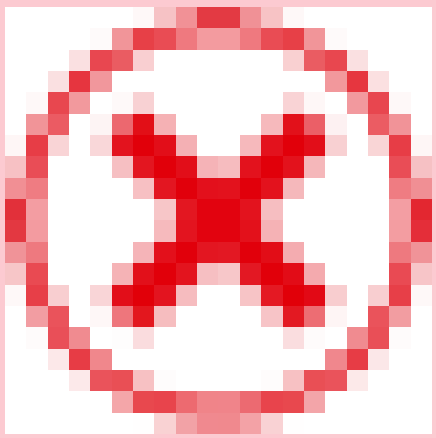
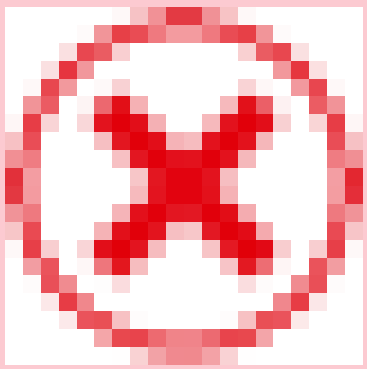
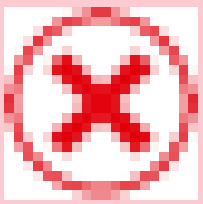
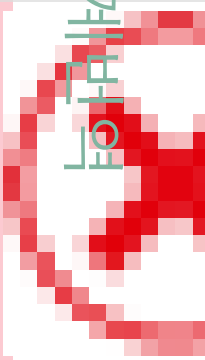
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
VI 세분성 구성				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

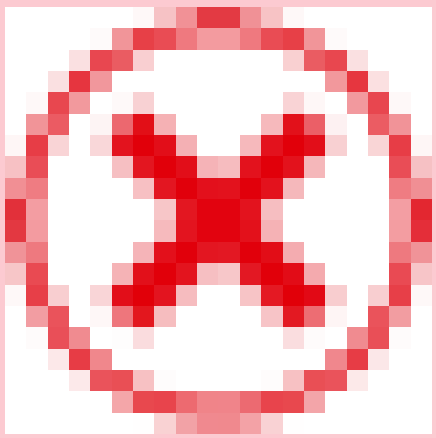
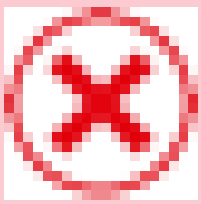
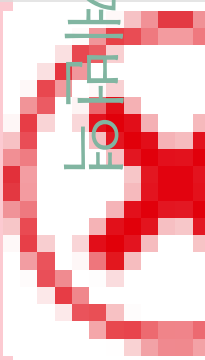
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
알림				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
이메일 템플릿	✗	✓	✗	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
임포트 큐	✗	✓	✗	✓

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

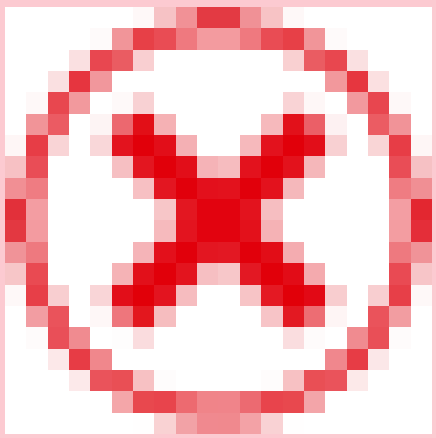
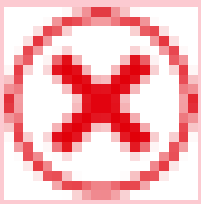
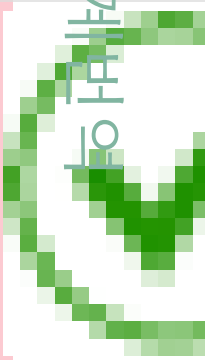
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
통합				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
SLA 정의	✗	✓	✗	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
SAM NVD 구성	✗	✓	✗	✓

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
표준화된 심각성 맵	✗	✓	✗	✓

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

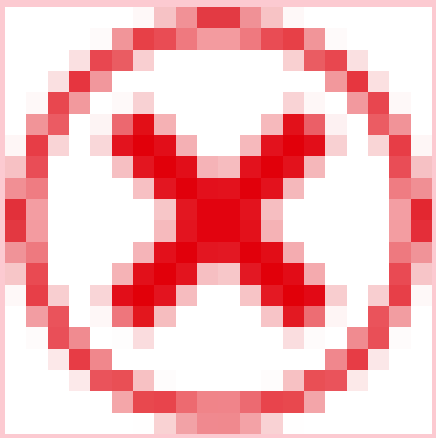
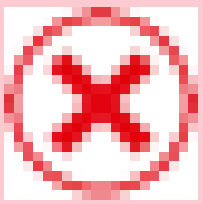
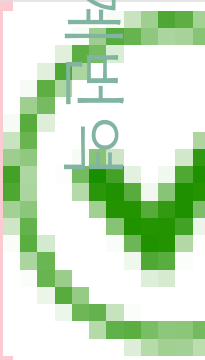
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
스캔 보장 범위 구성				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

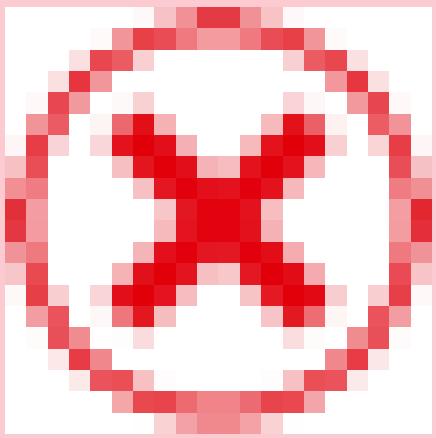
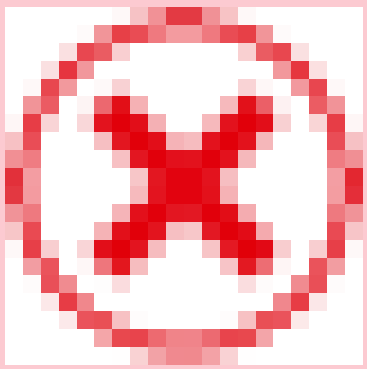
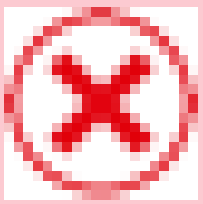
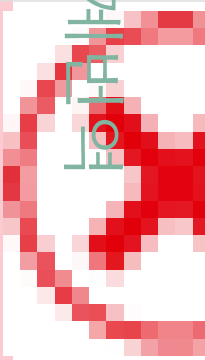
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
예외 관리				

고객 버전

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
사용량 보고서	✗	✗	✗	✗
진단				

고객 버전

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

다른 역할에 대한 정보:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

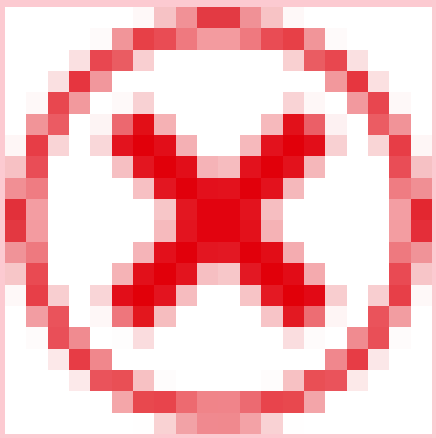
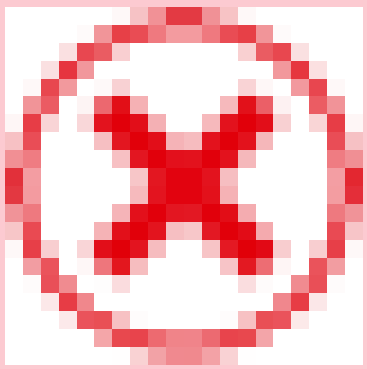
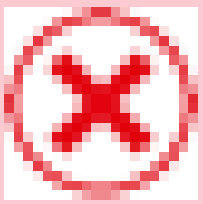
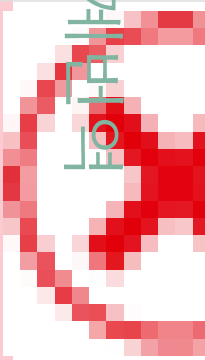
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configure_
검사				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

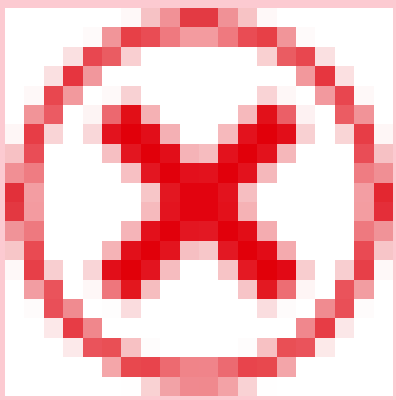
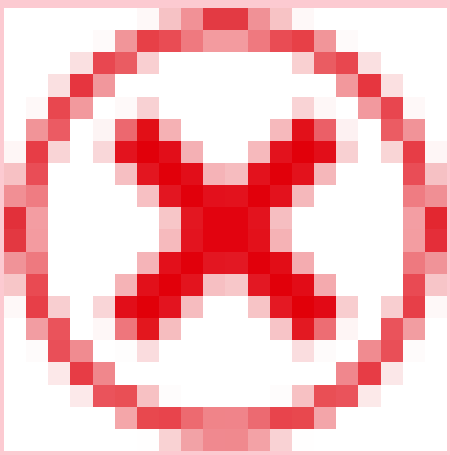
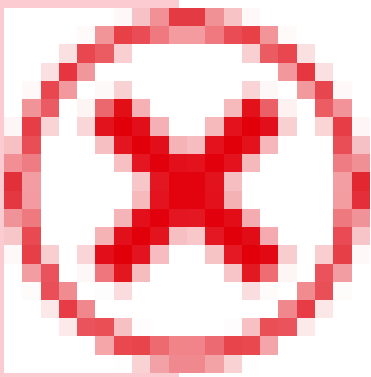
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
(메인 앱 그룹)			
CISO 대시보드			

기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

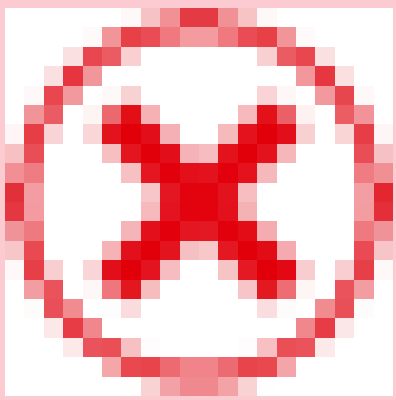
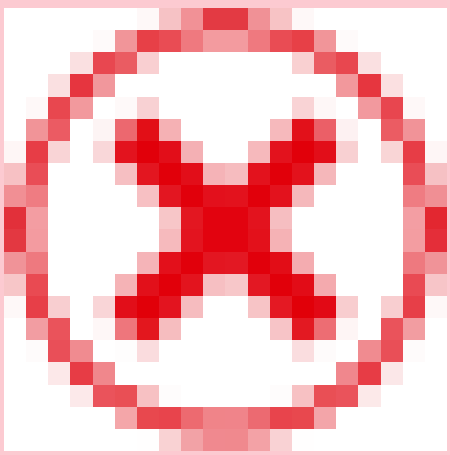
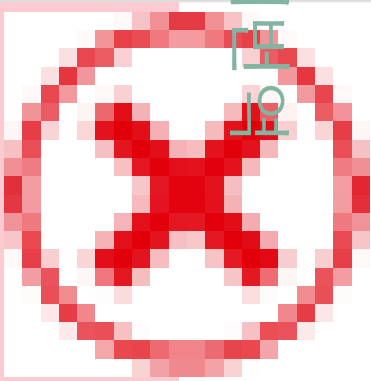
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
정정 개요			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

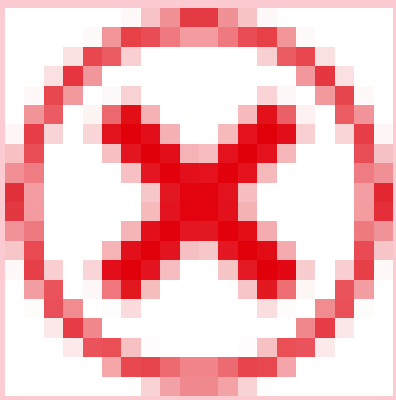
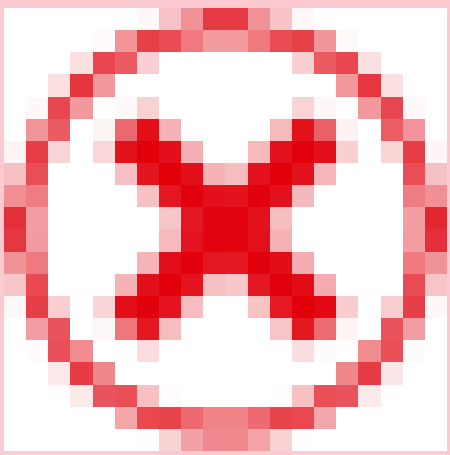
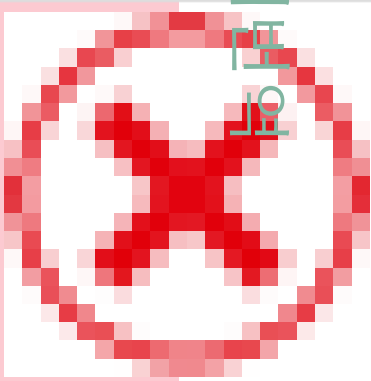
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
취약성 관리자 작업 공간			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
개요	✗	✗	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

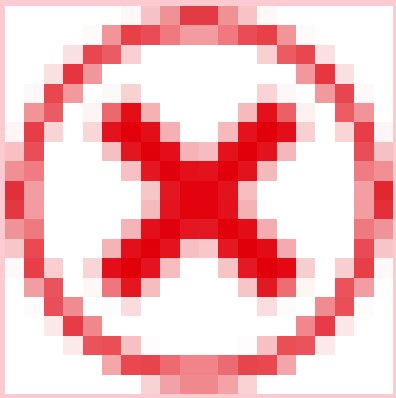
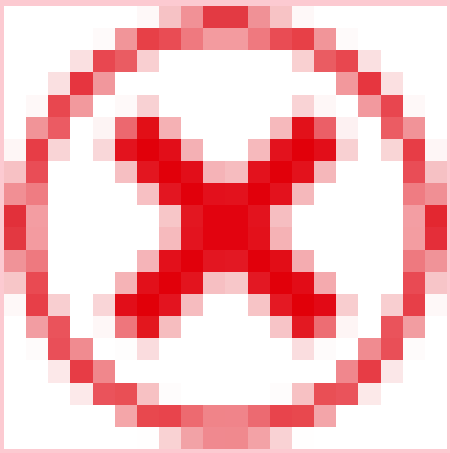
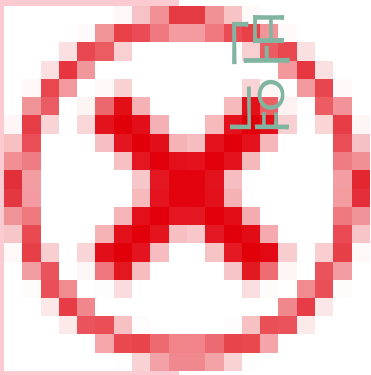
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
IT 정정 작업 공간			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
승인자 개요	✗	✗	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

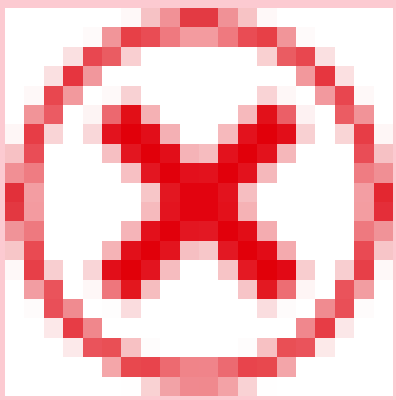
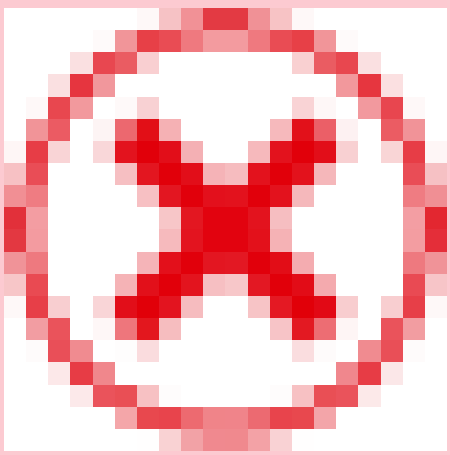
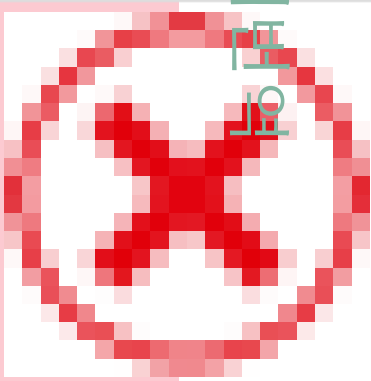
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
개요			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

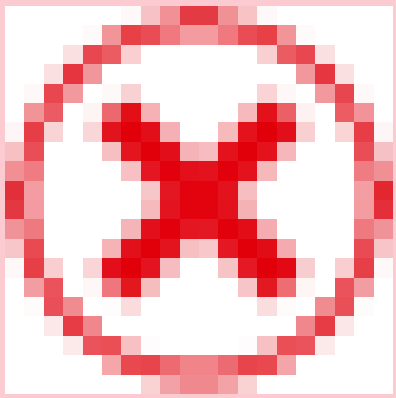
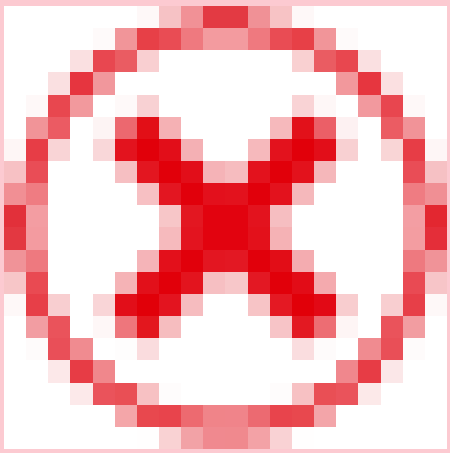
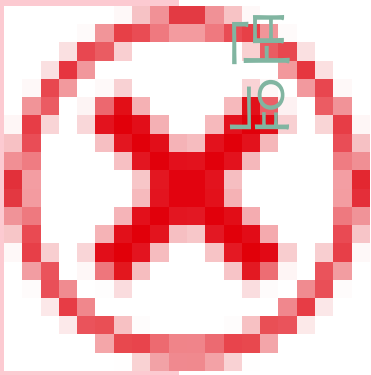
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
내 승인			
정정 작업			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

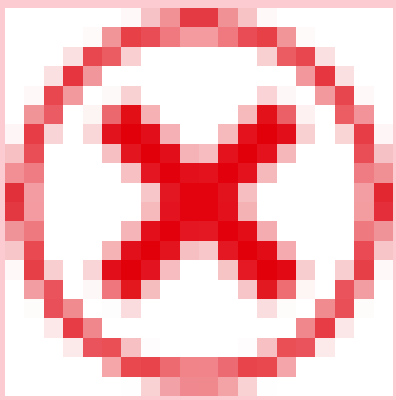
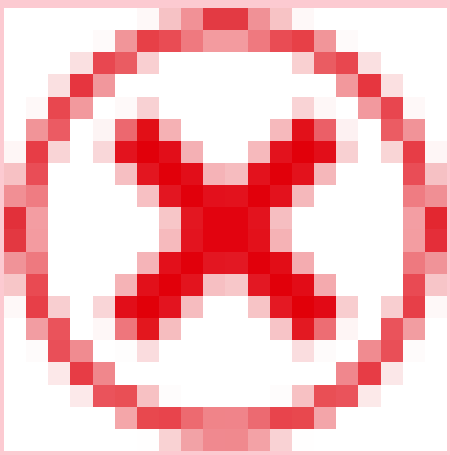
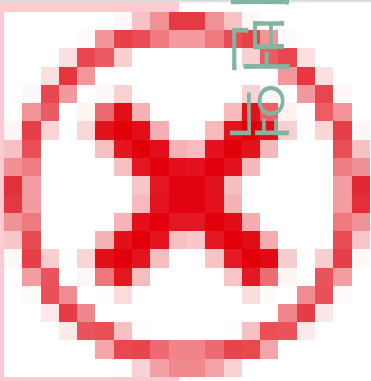
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
활성			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

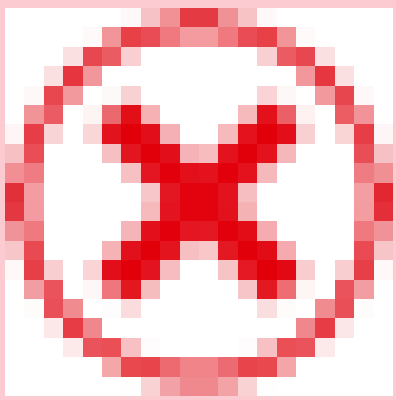
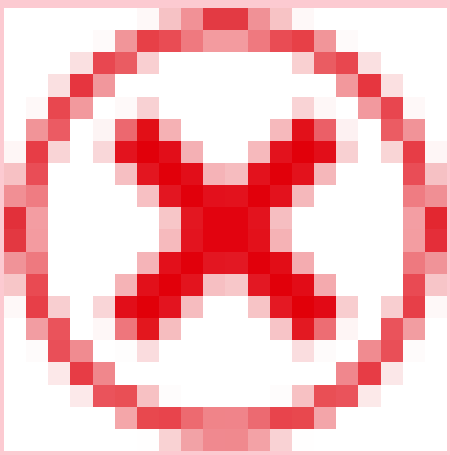
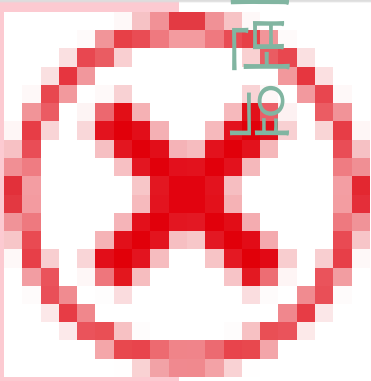
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
나에게 할당됨			

기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

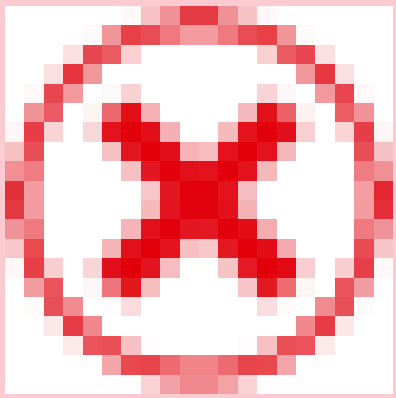
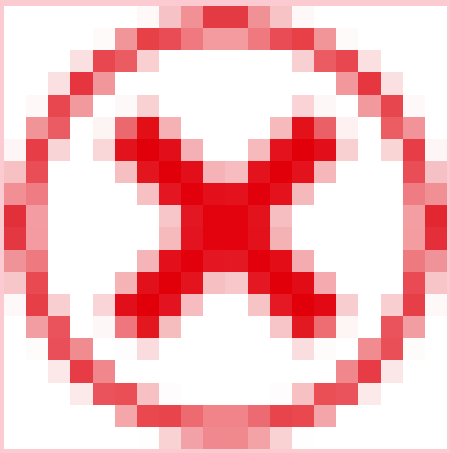
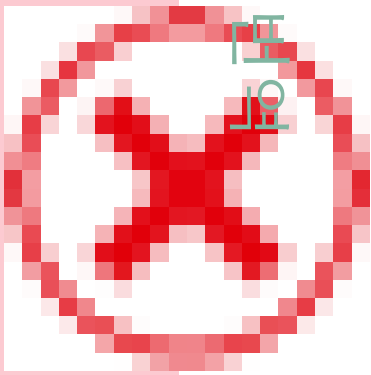
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
사용자 그룹에 할당됨			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

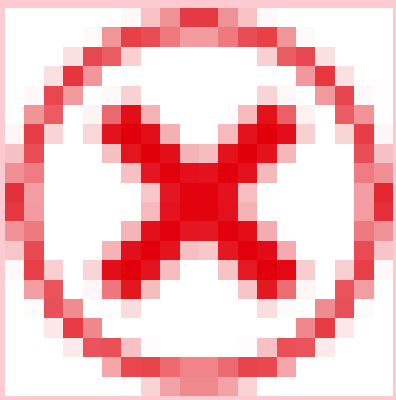
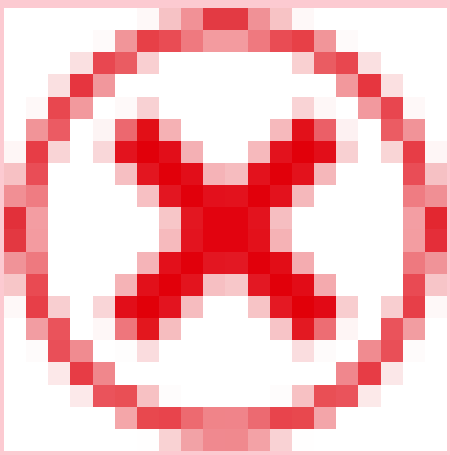
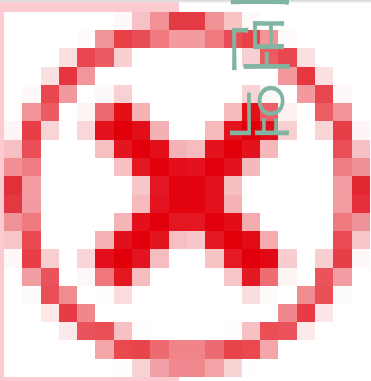
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
모두			
취약 항목			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

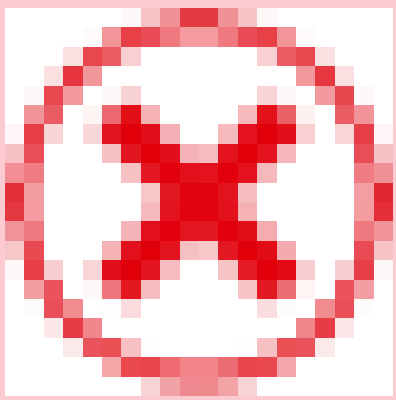
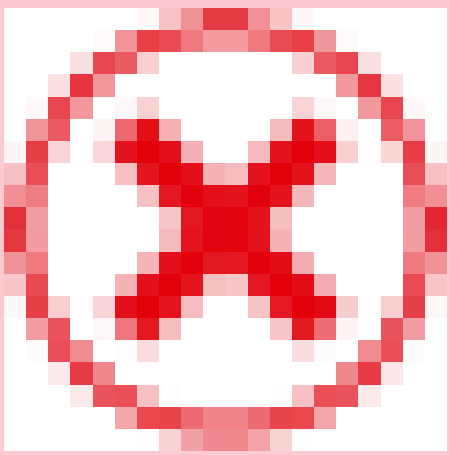
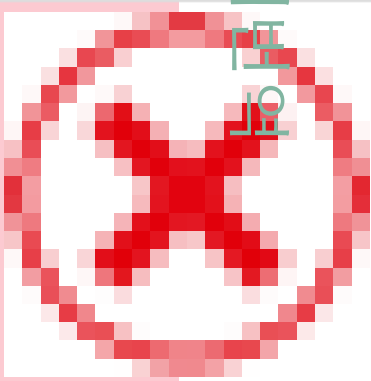
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
중요 위험			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

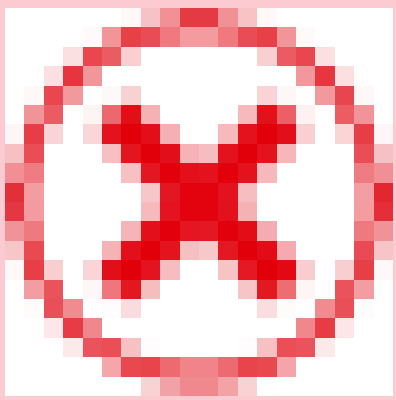
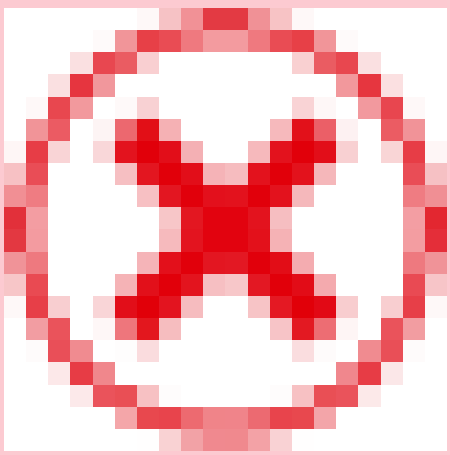
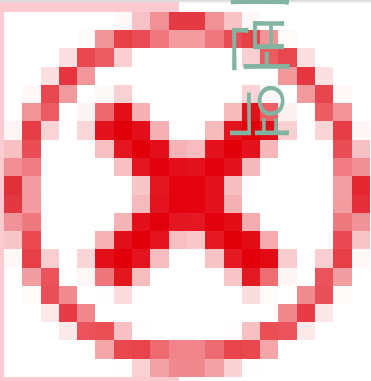
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
높은 위험			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

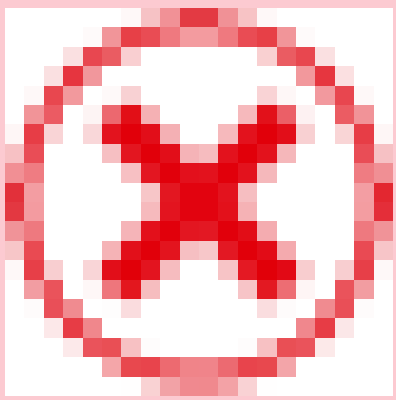
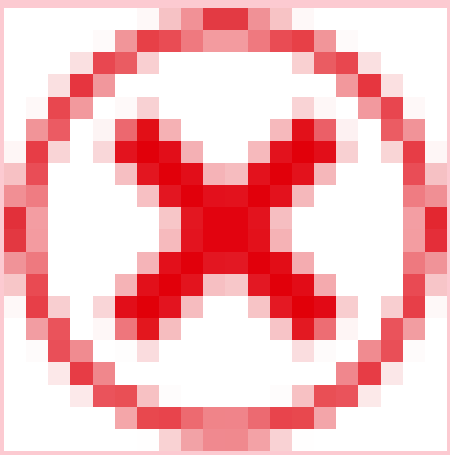
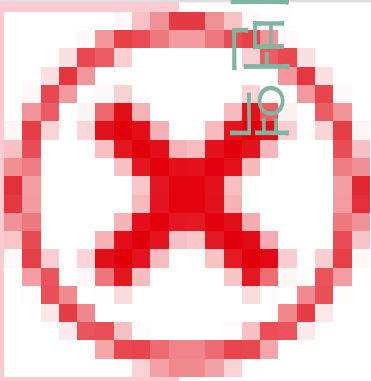
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
악용 가능			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

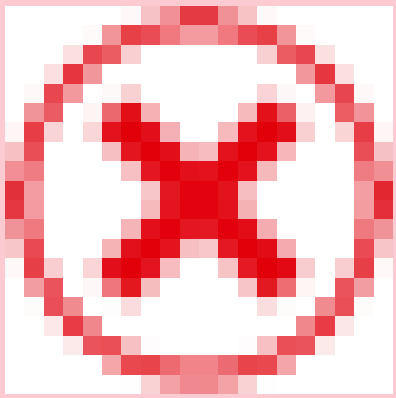
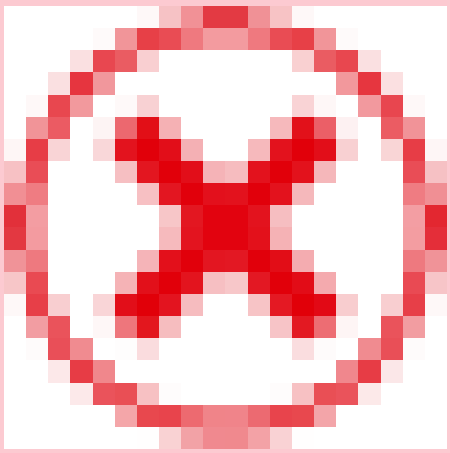
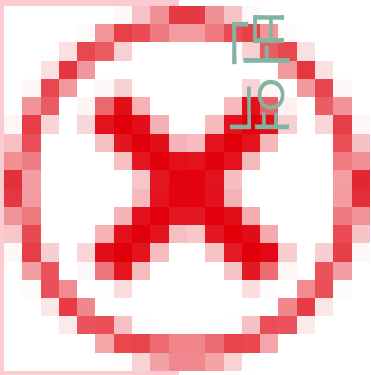
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
대상에 접근			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

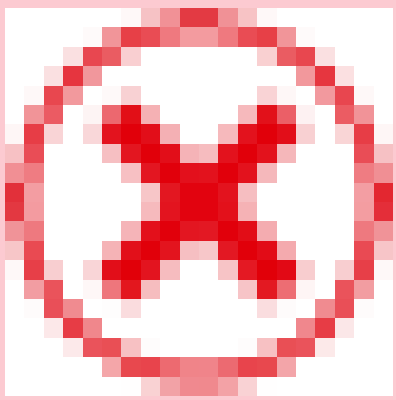
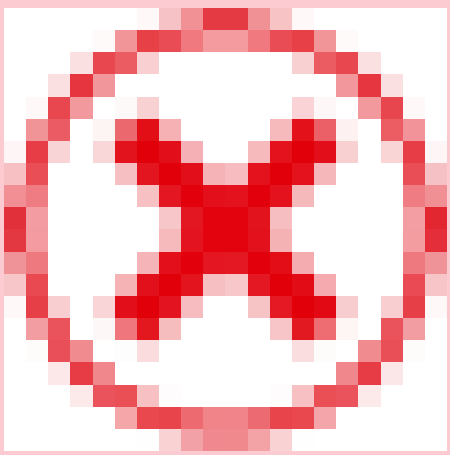
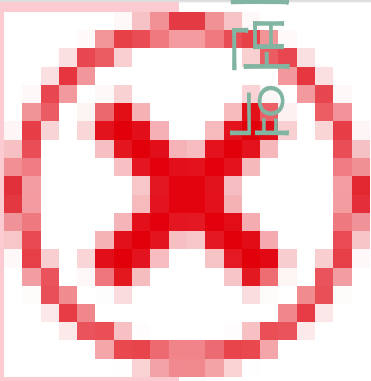
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
누락된 대상			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

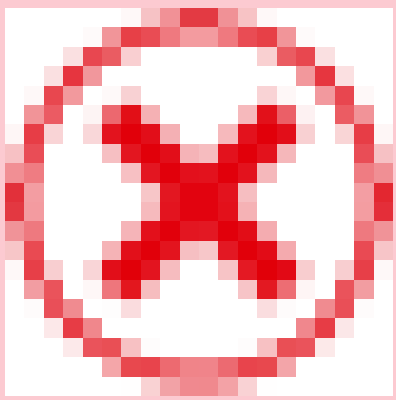
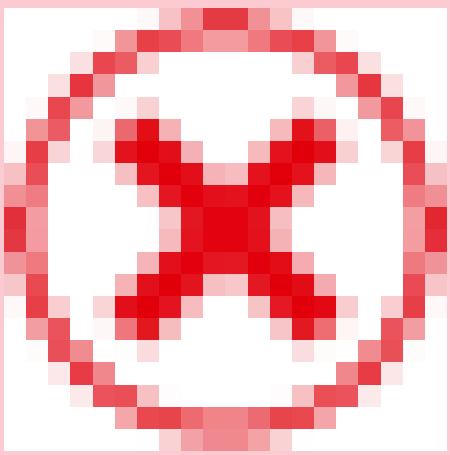
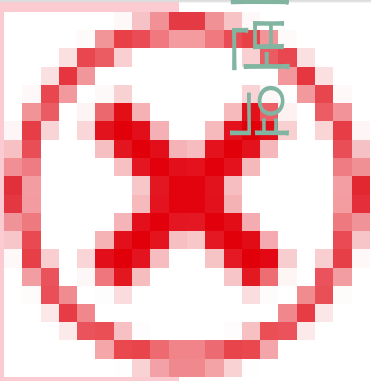
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
지난 90일 이내			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

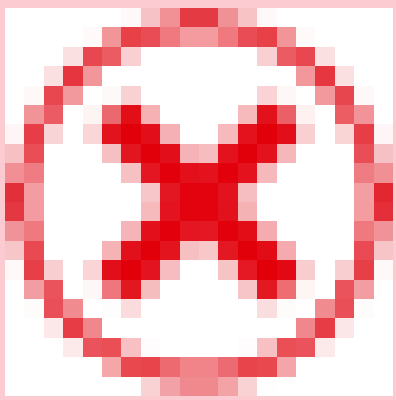
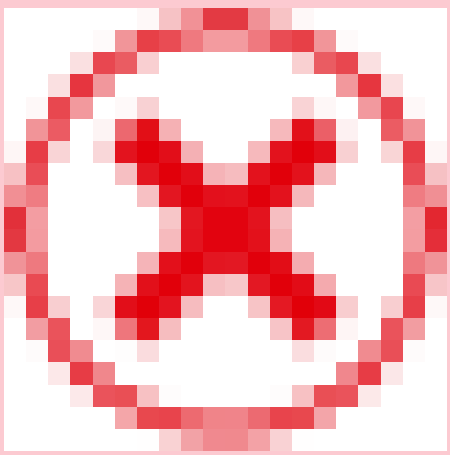
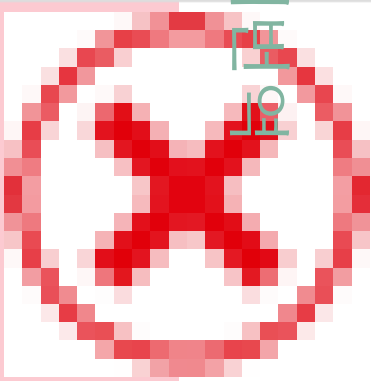
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
90일 경과			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

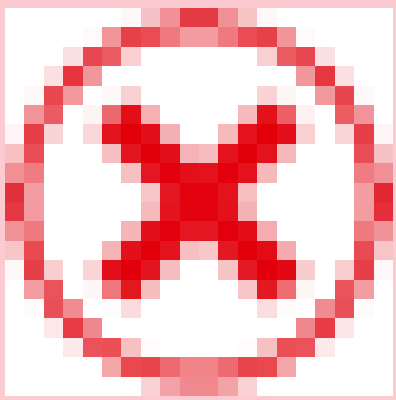
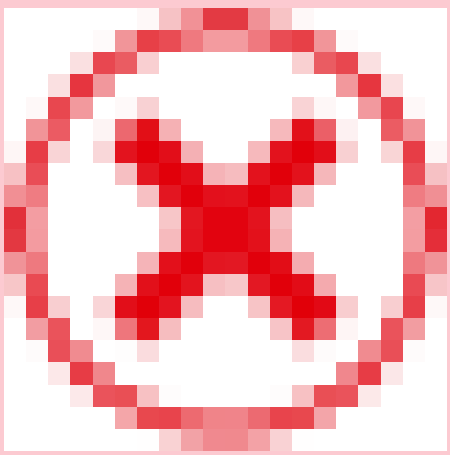
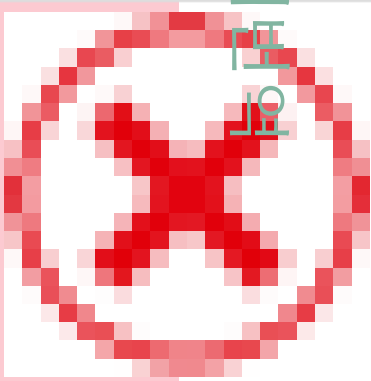
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
미할당			

기능 표

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

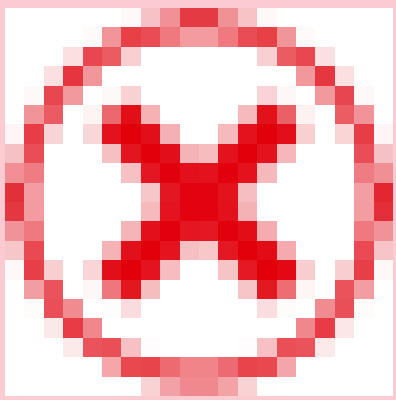
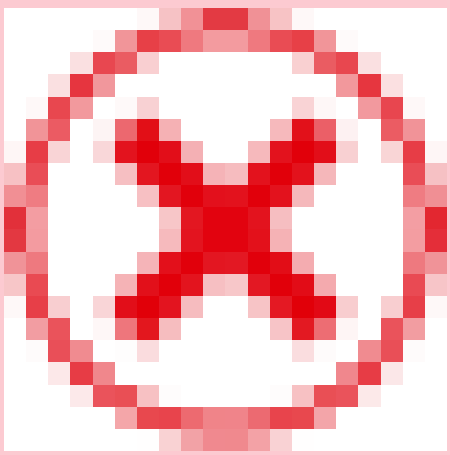
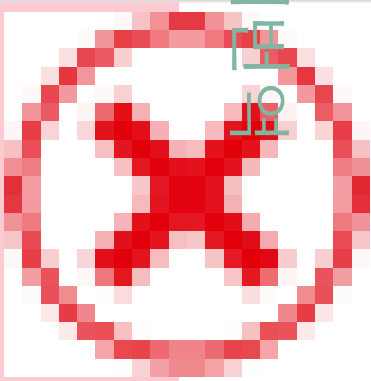
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
그룹 해제			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

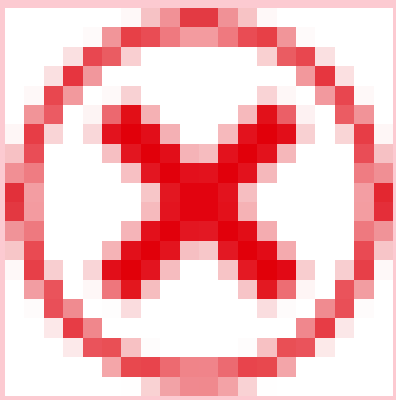
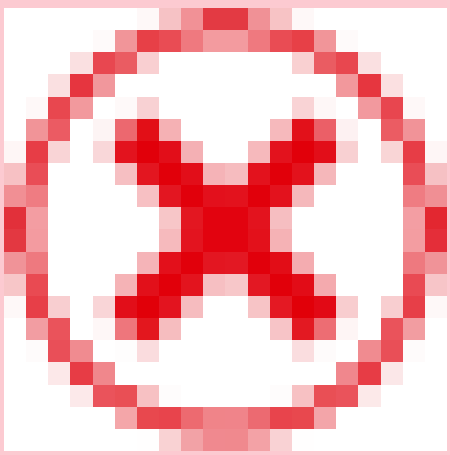
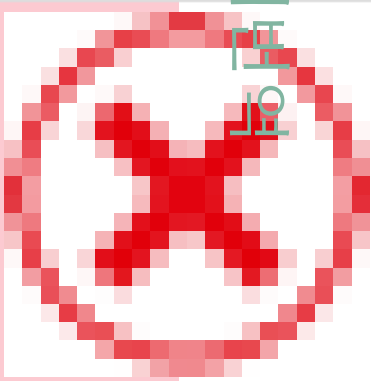
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
해제됨			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

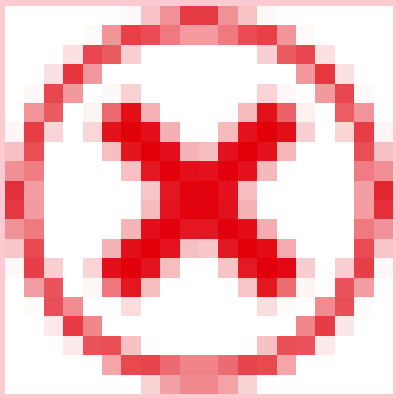
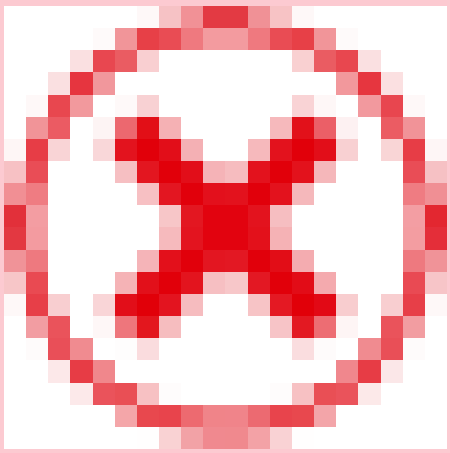
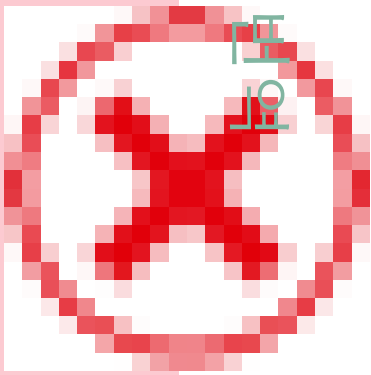
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
여러 지연			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

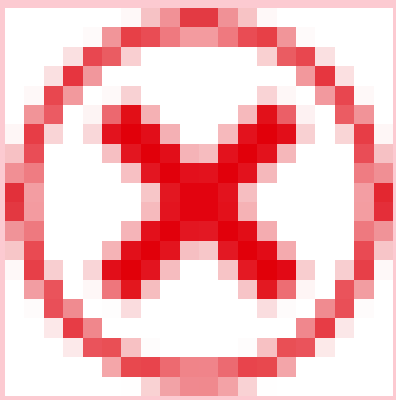
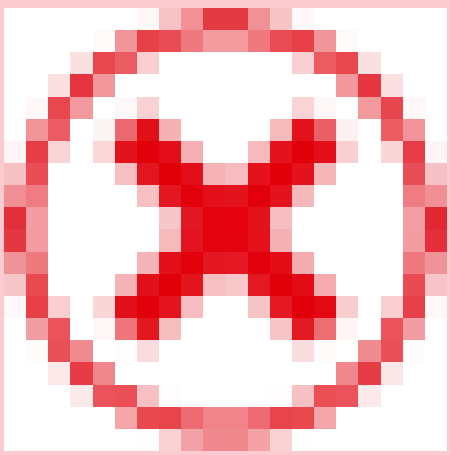
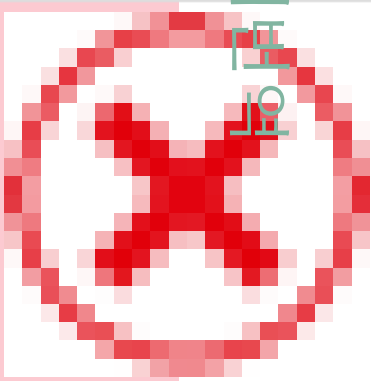
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
모두			
솔루션			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

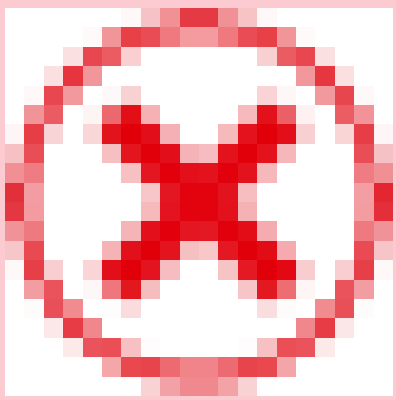
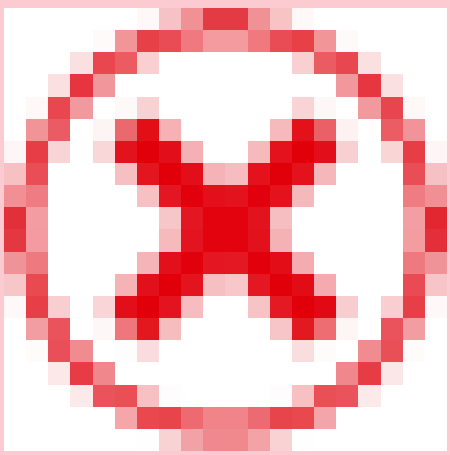
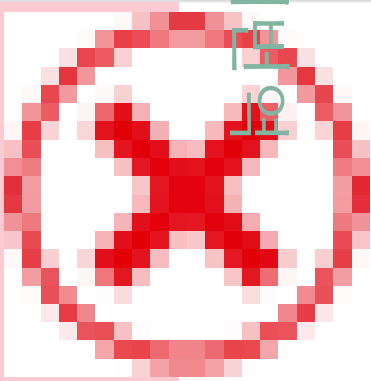
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
모두			

기술 표준 PDF

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
가장 높은 대체			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

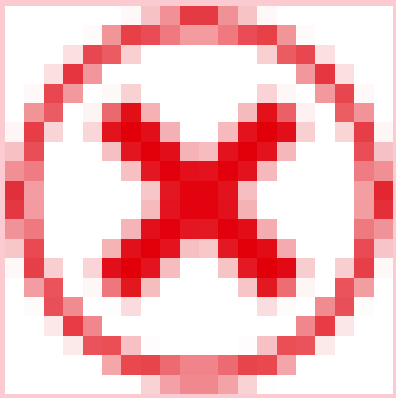
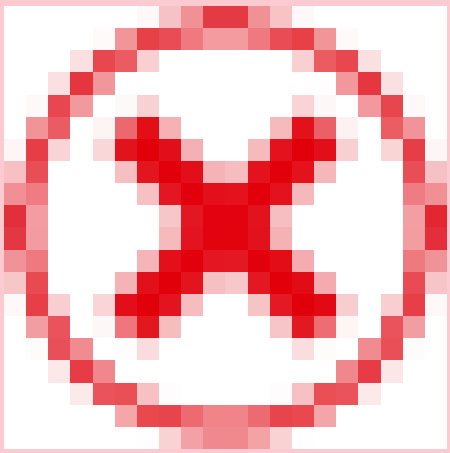
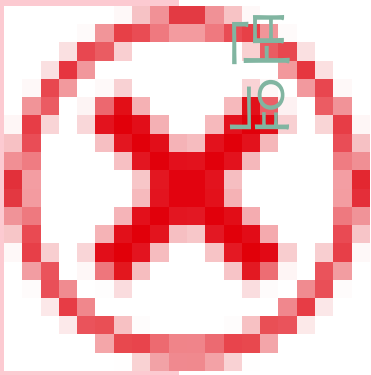
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
취약한 항목 포함			
라이브러리			

기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

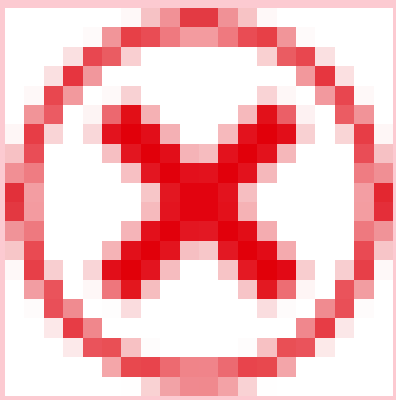
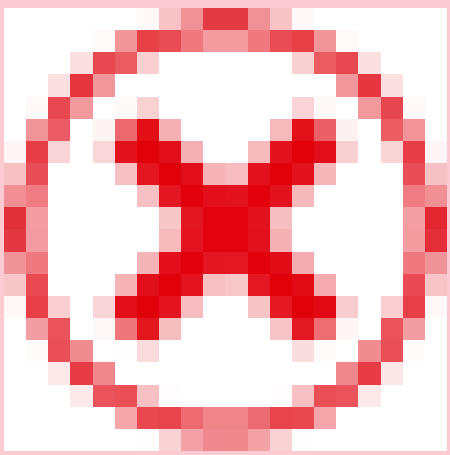
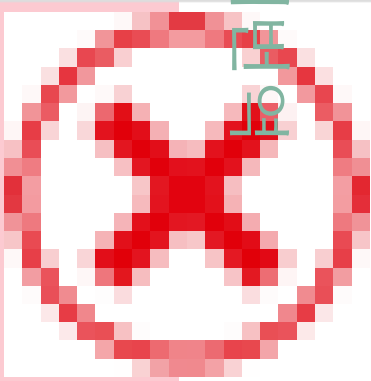
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
NVD			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

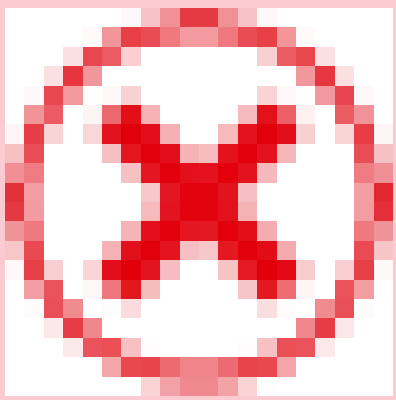
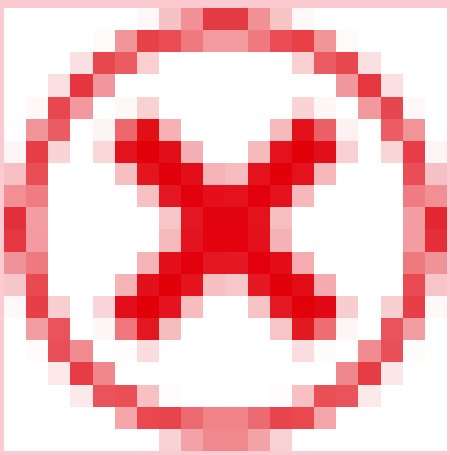
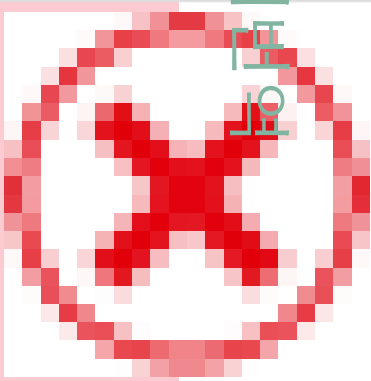
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
CWE			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

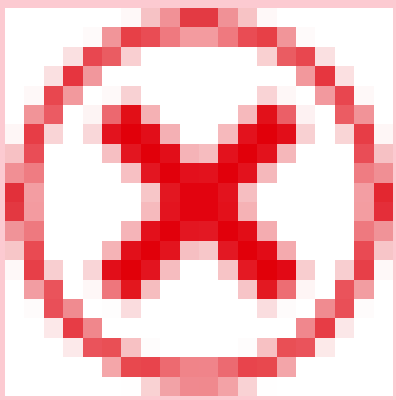
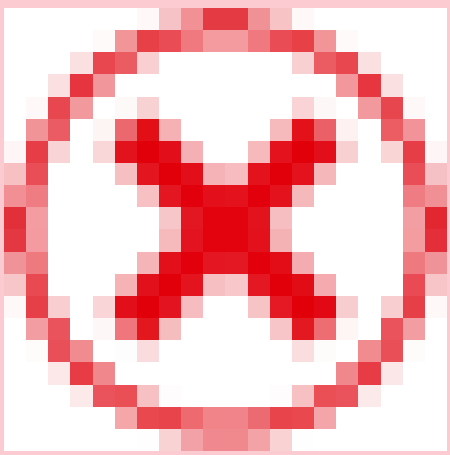
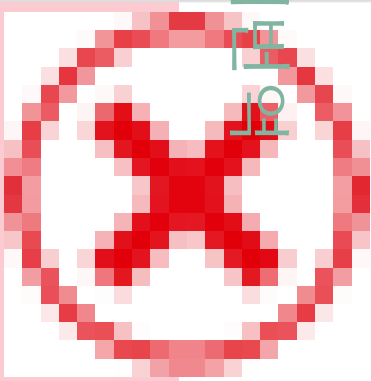
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
외부 공급업체			

기술 표준

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

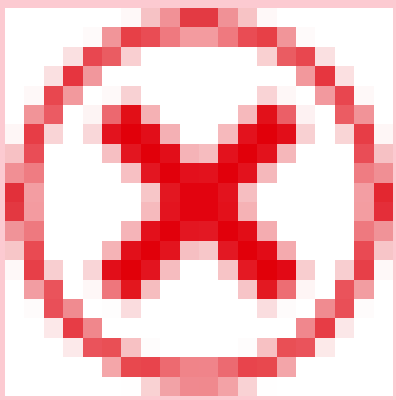
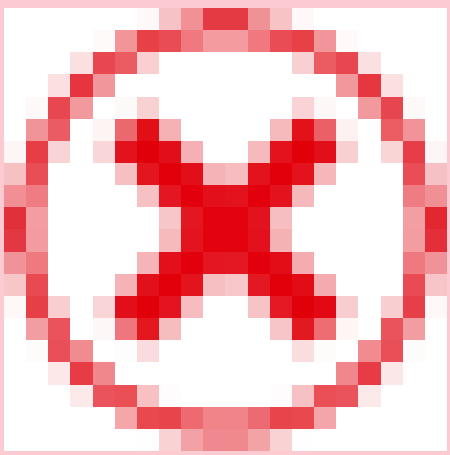
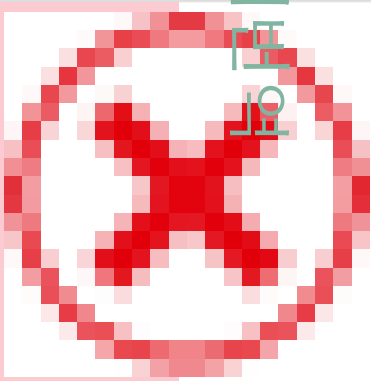
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
취약한 소프트웨어			

취약성 스캐닝

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

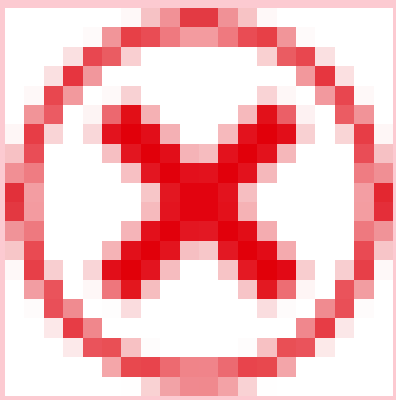
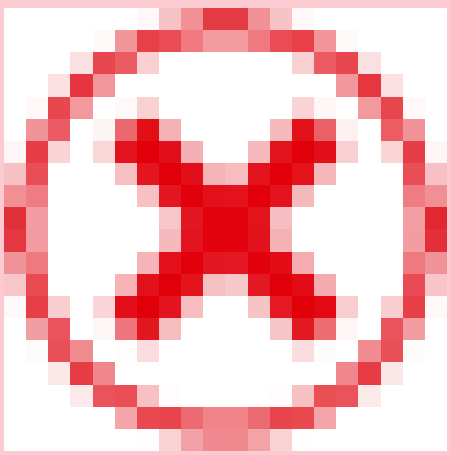
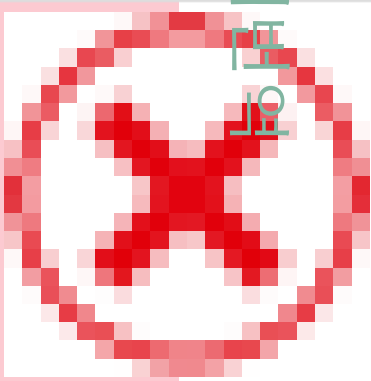
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
노출 평가			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

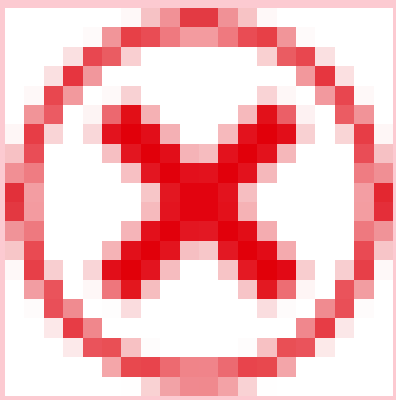
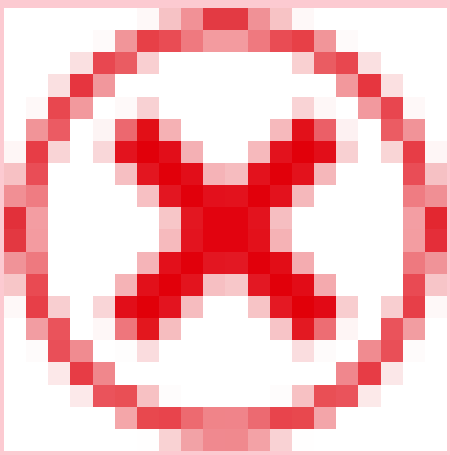
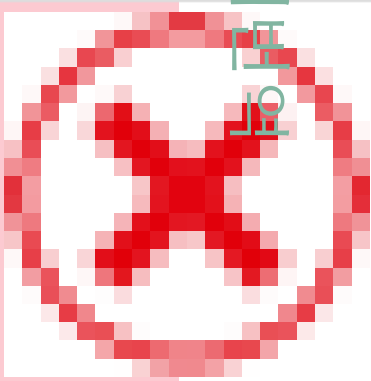
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
스캔			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

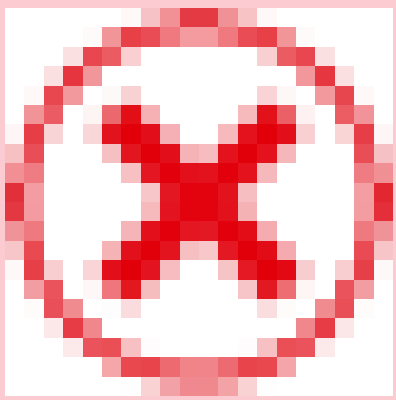
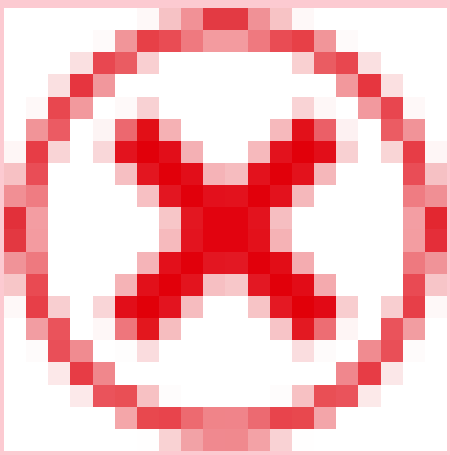
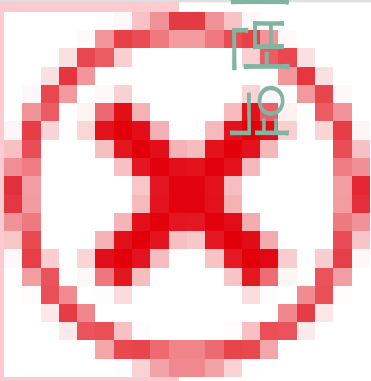
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
스캐너			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

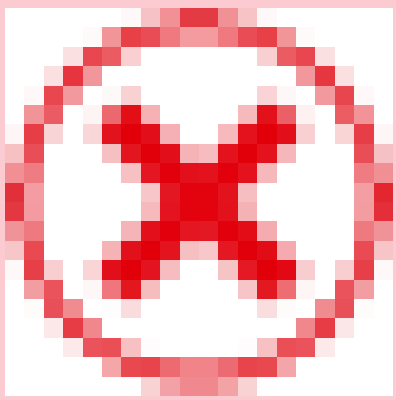
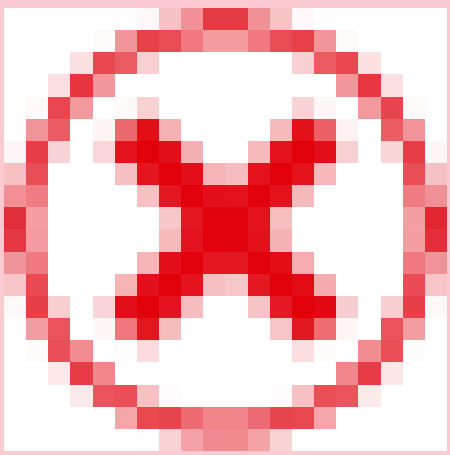
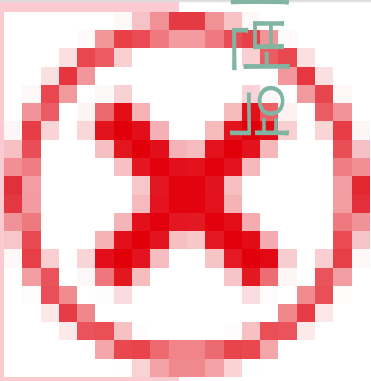
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
스캔 큐			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

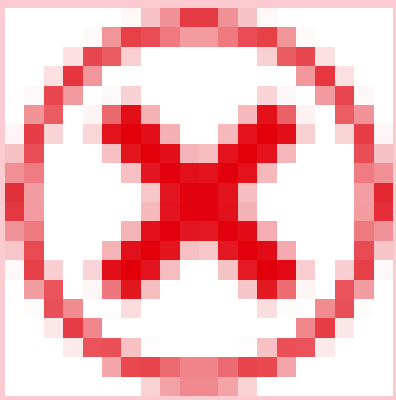
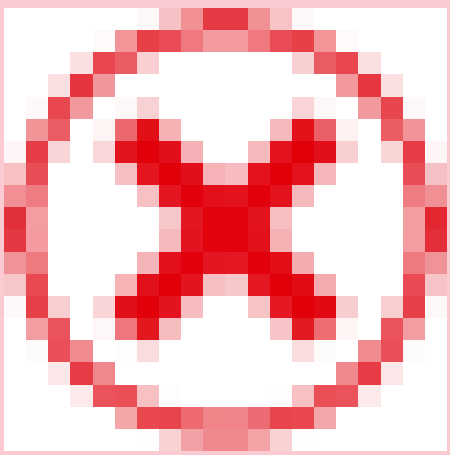
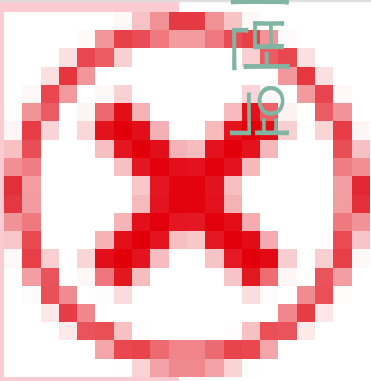
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
스캐너 속도 제한			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

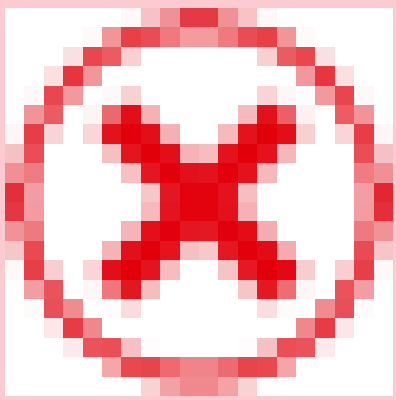
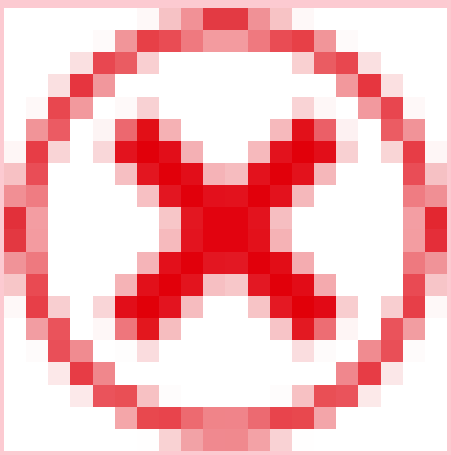
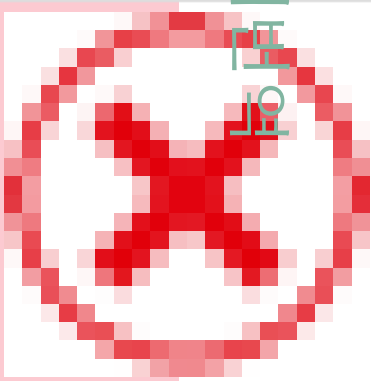
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
속도 제한 정의			
관리			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
설정 도우미			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
주시 주제	✗	✗	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

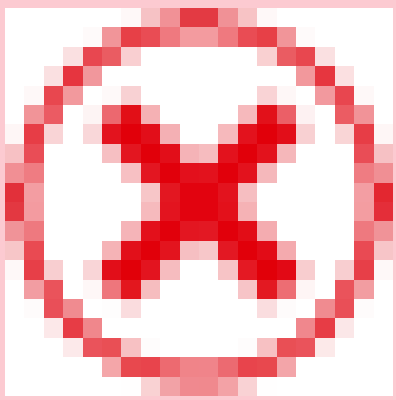
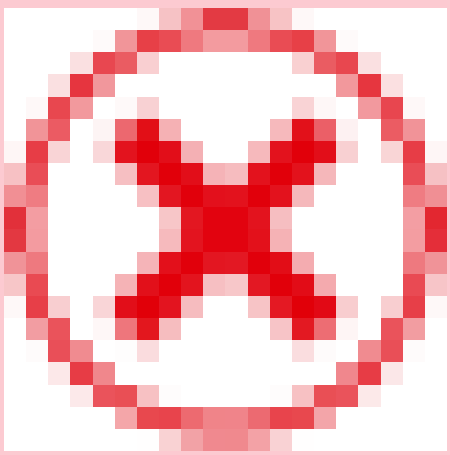
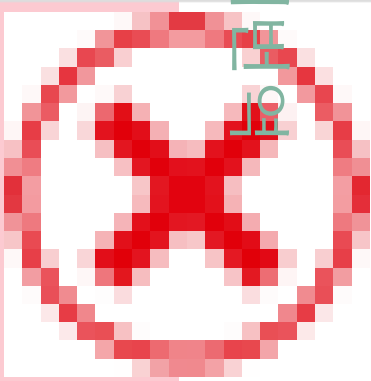
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
담당 규칙			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
정정 작업 규칙			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

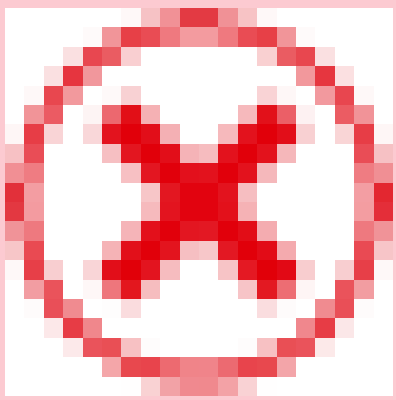
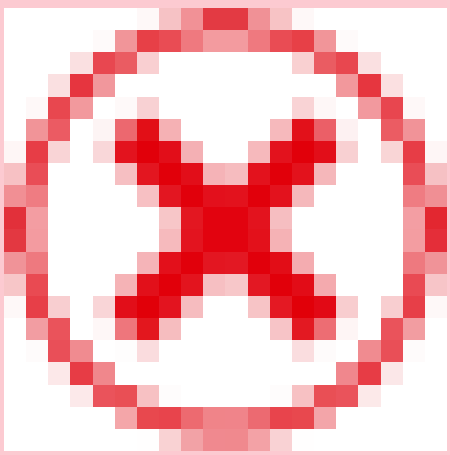
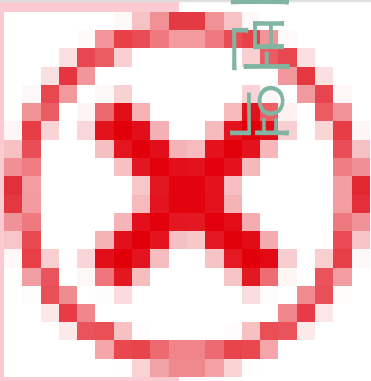
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
할당 권장 사항			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
취약성 계산기	✗	✗	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

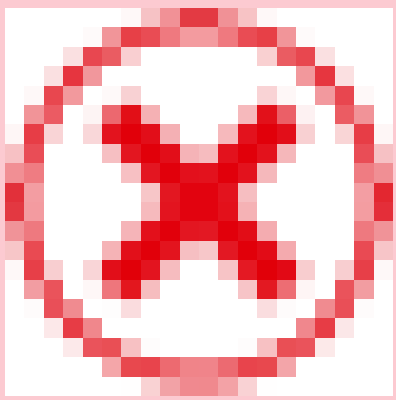
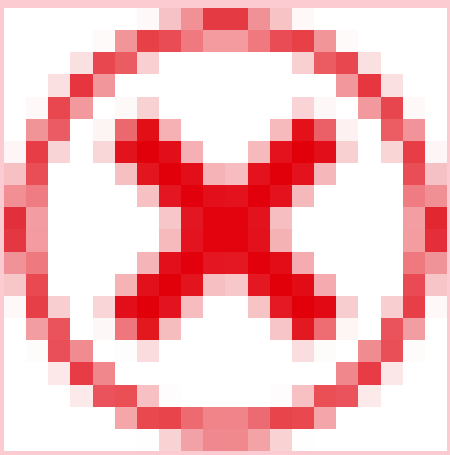
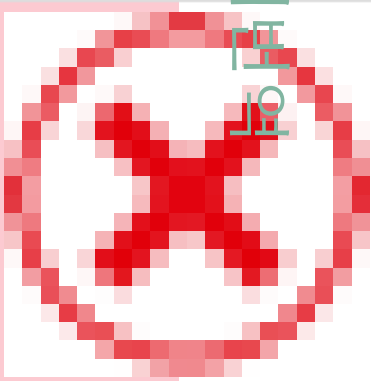
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
취약성 롤업 계산기			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

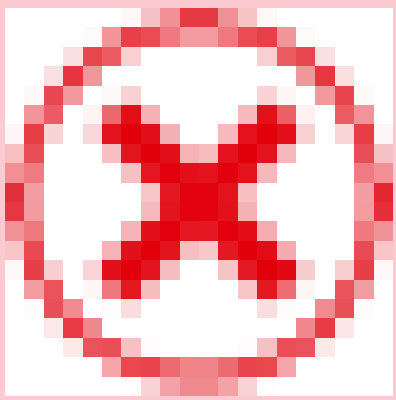
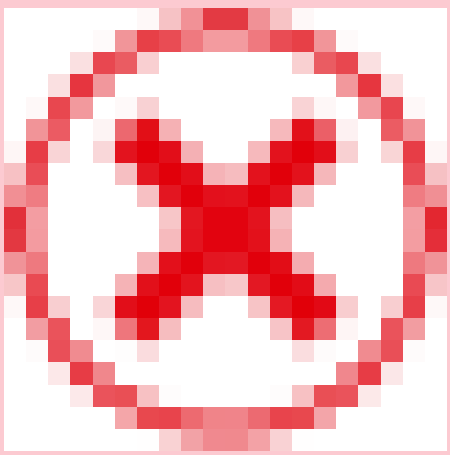
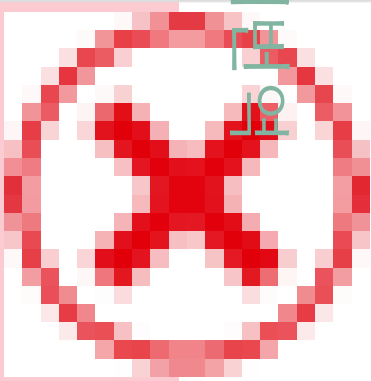
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
정정 대상 규칙			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

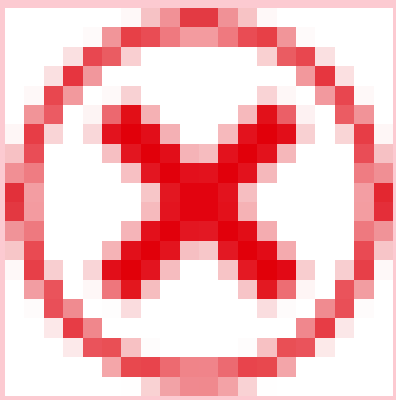
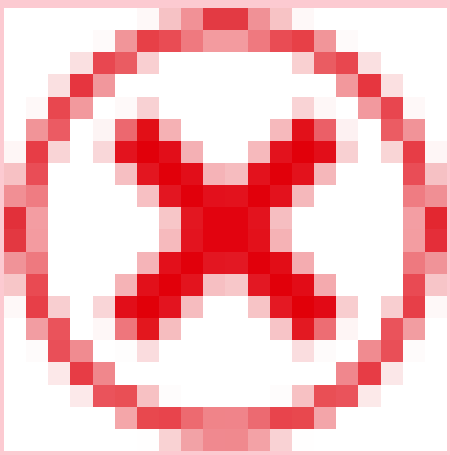
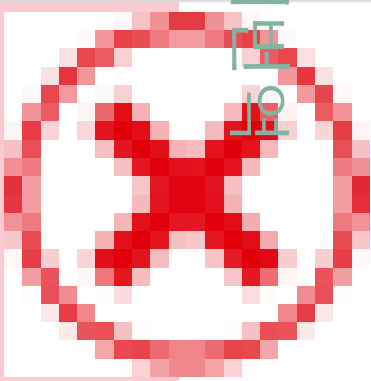
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
AutoClose 구성			

기밀 및 독점

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
자동 삭제 규칙	✗	✗	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

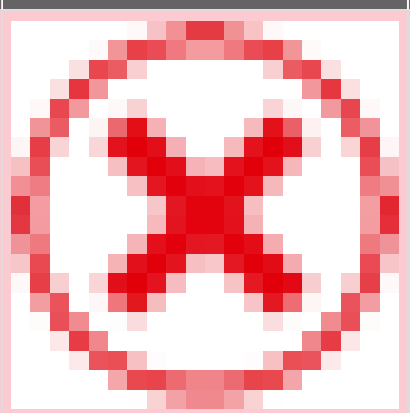
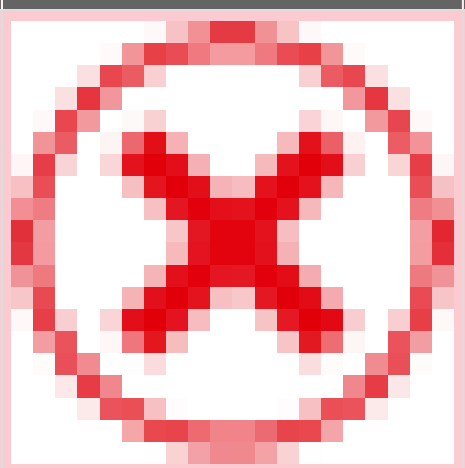
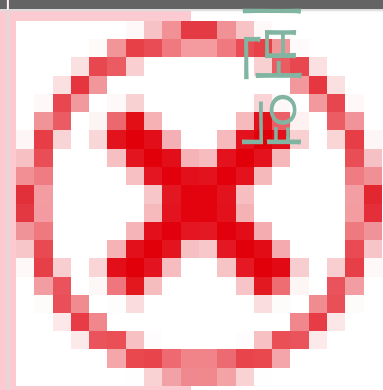
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
예외 규칙			

기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

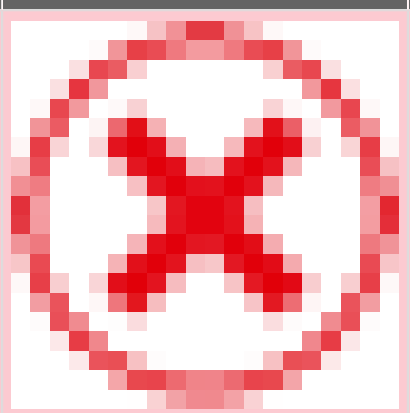
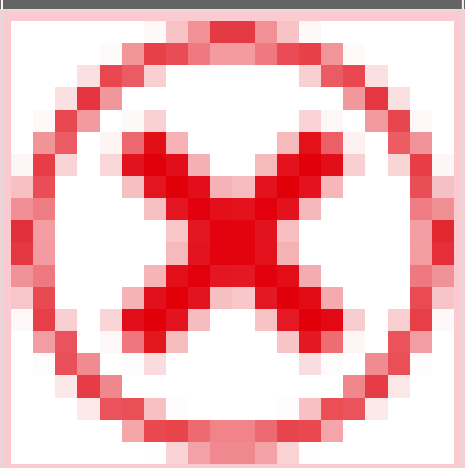
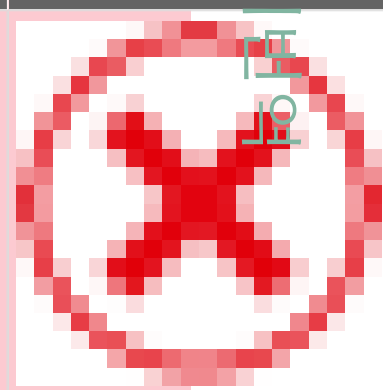
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
승인 규칙			

기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

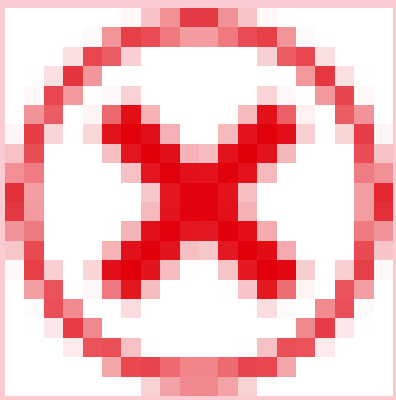
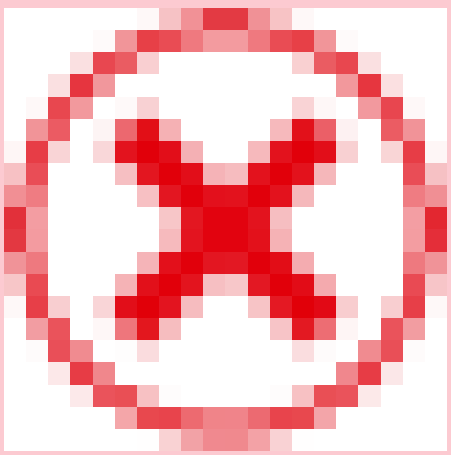
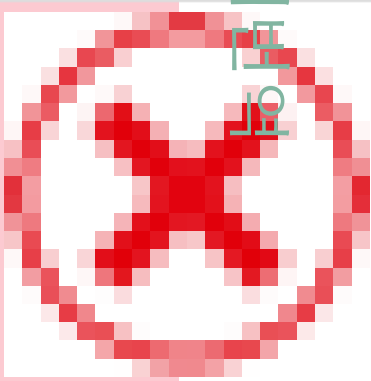
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
분류 규칙			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

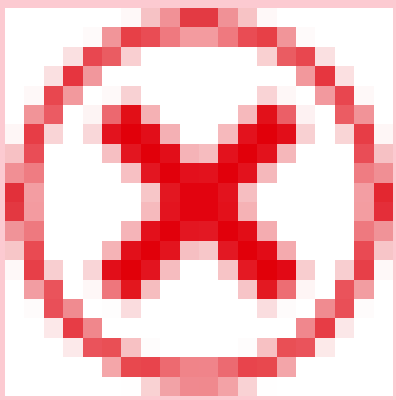
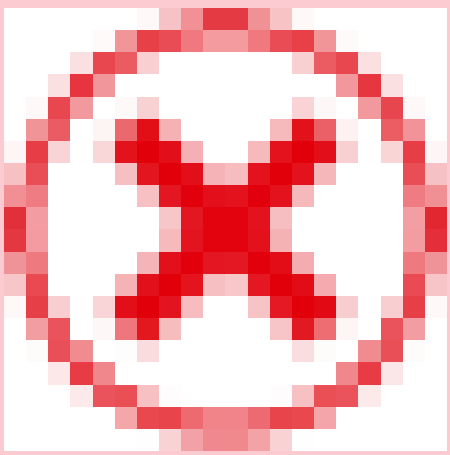
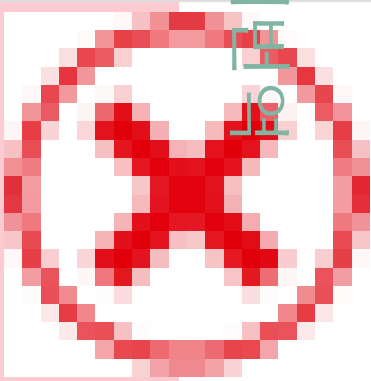
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
성과 구성			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
VI 세분성 구성	✗	✗	✓

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

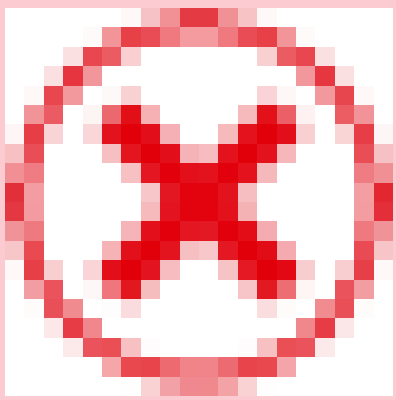
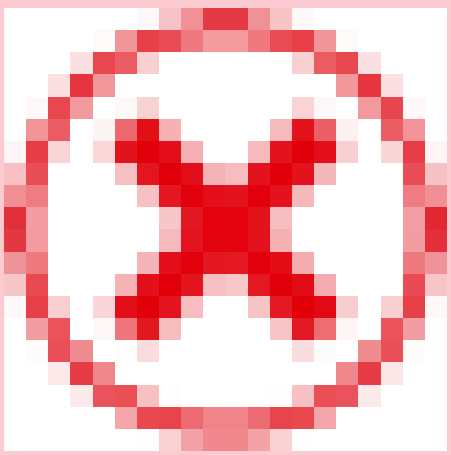
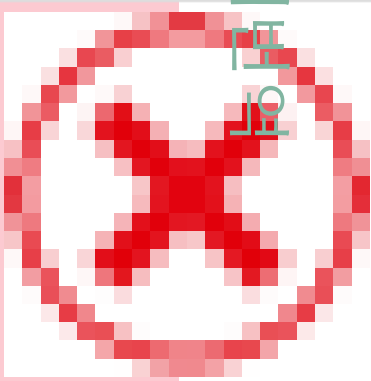
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
알림			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
이메일 템플릿			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
임포트 큐			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

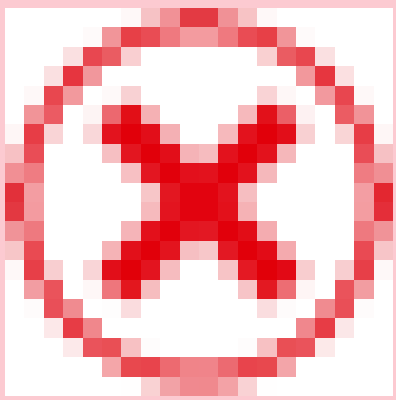
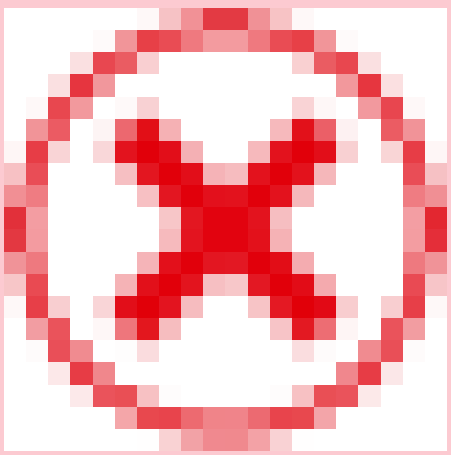
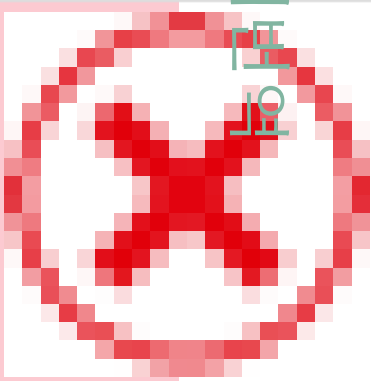
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
통합			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
SLA 정의			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

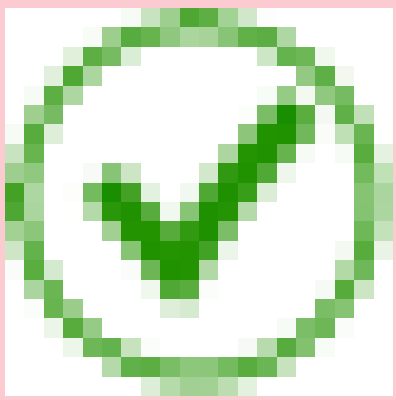
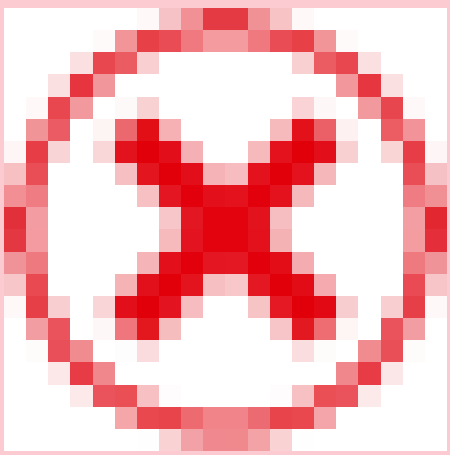
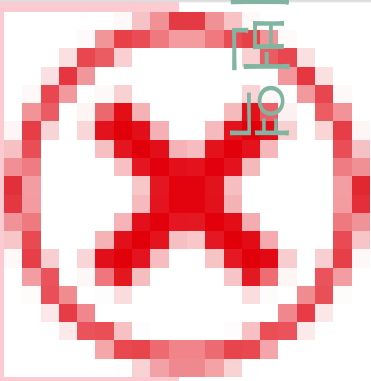
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
SAM NVD 구성			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
표준화된 심각성 맵			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

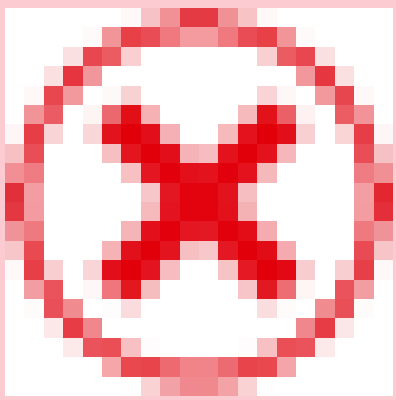
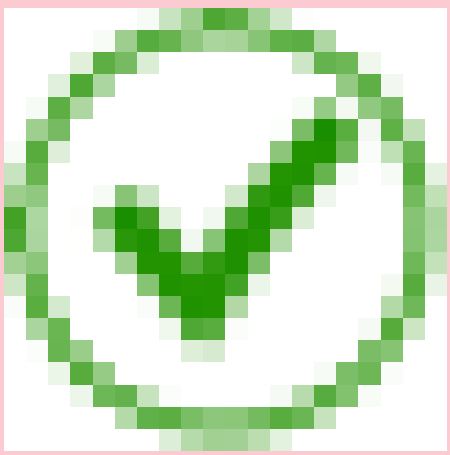
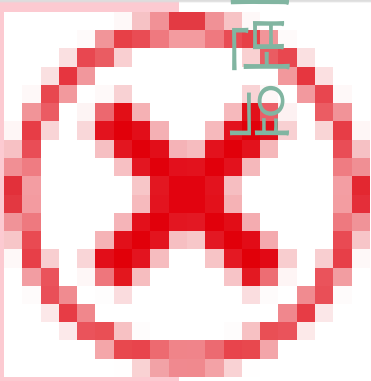
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
스캔 보장 범위 구성			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
예외 관리	✗	✗	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

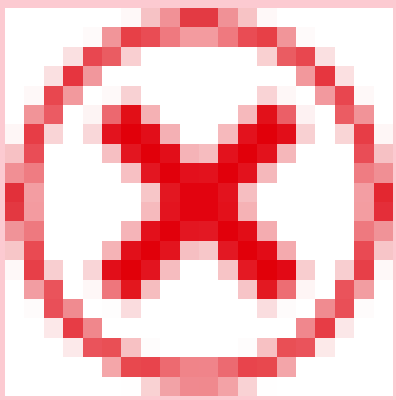
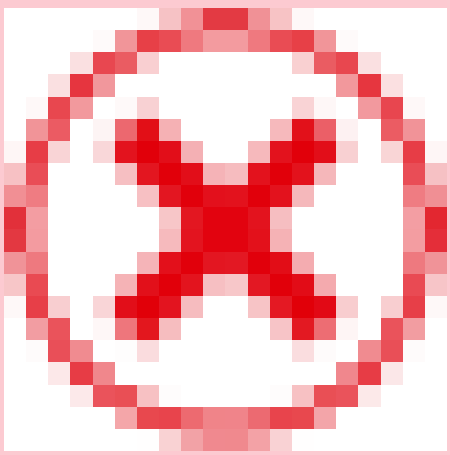
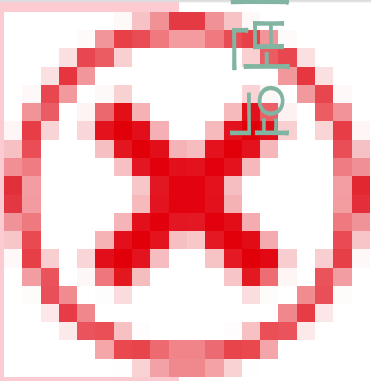
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
사용량 보고서			
진단			

PDF 기능 제한

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

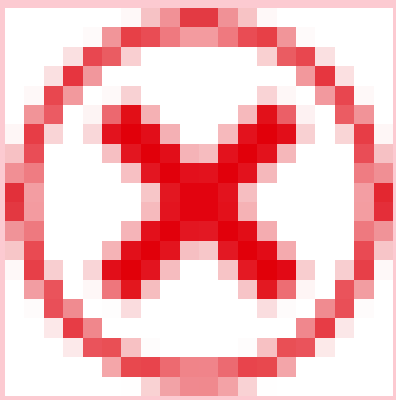
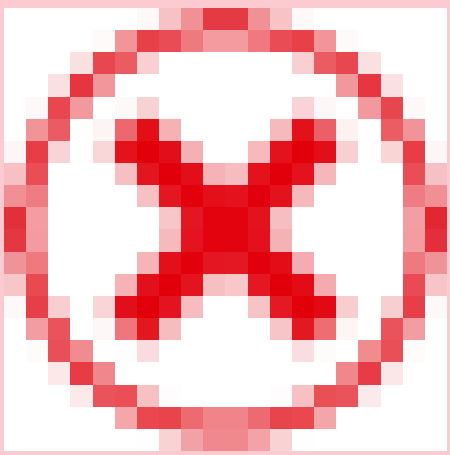
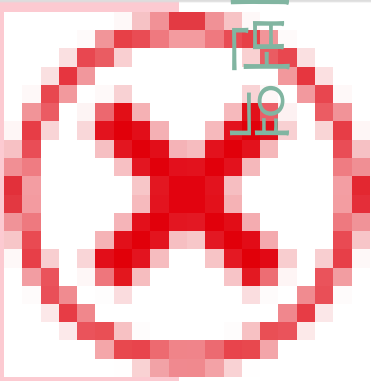
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granularity
검사			

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
(메인 앱 그룹)				
CISO 대시보드	✗	✗	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

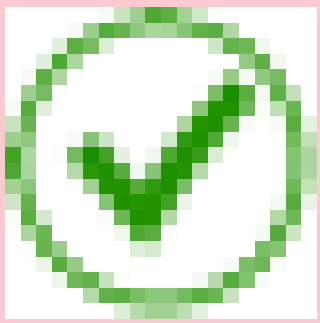
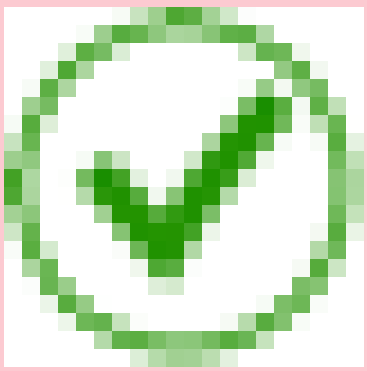
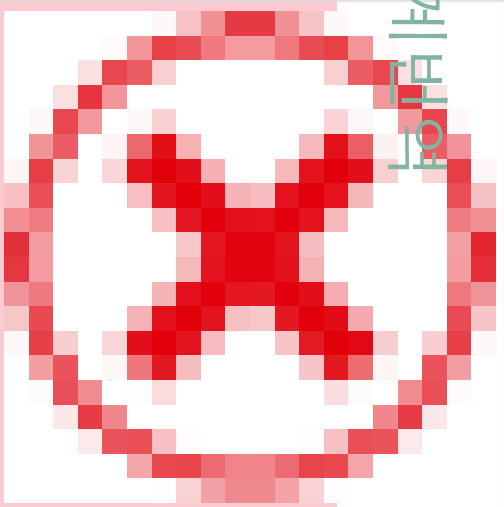
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
정정 개요				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

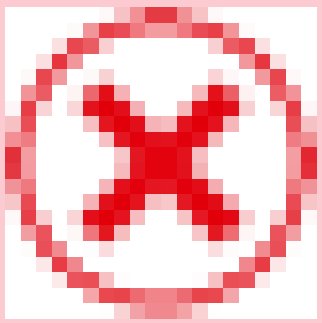
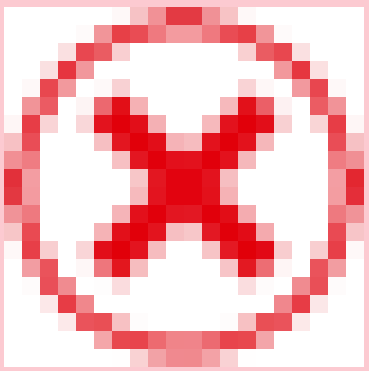
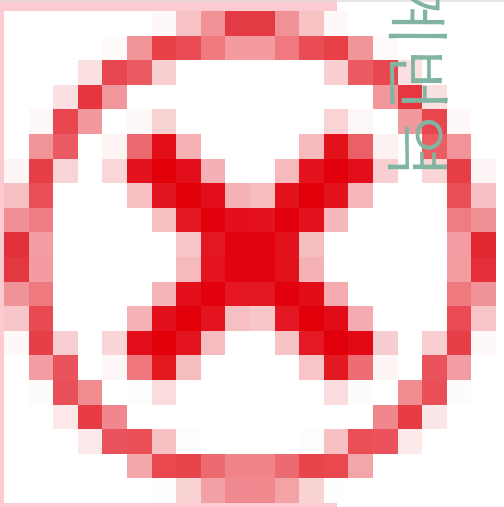
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
취약성 관리자 작업 공간				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

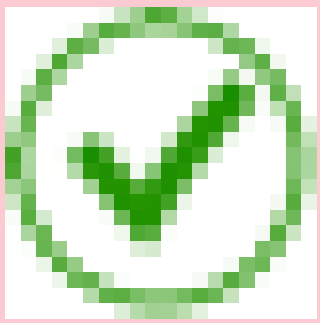
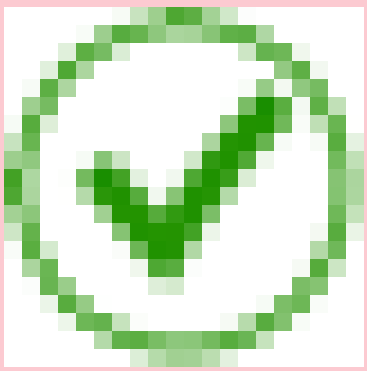
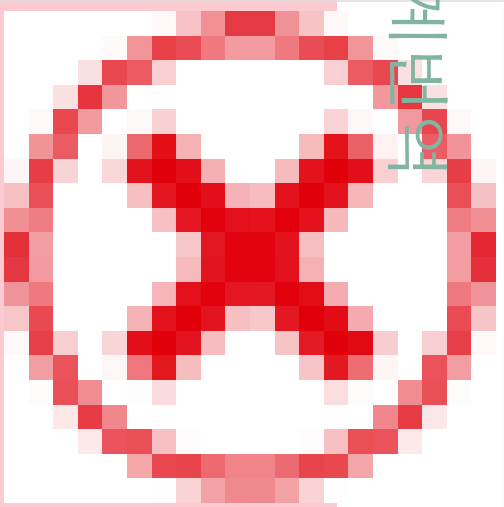
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
개요				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

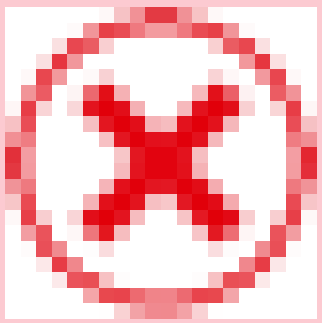
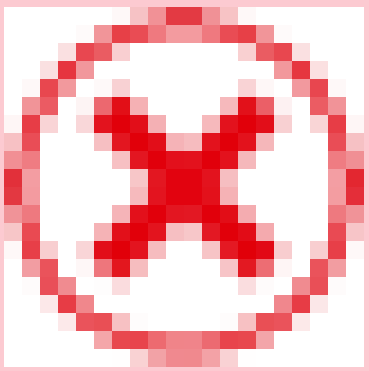
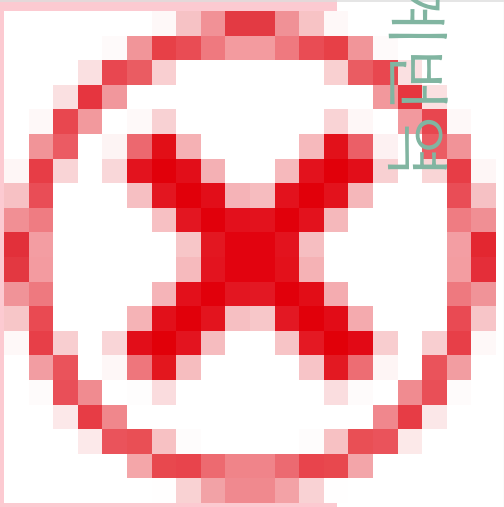
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
IT 정정 작업 공간				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

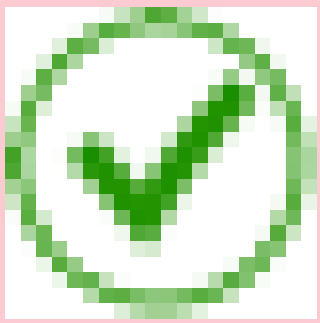
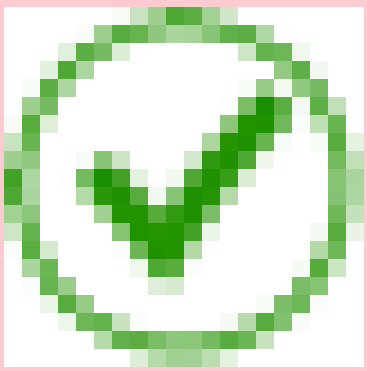
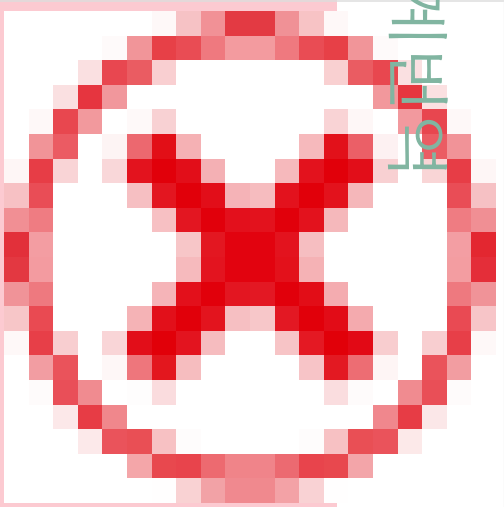
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
승인자 개요				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

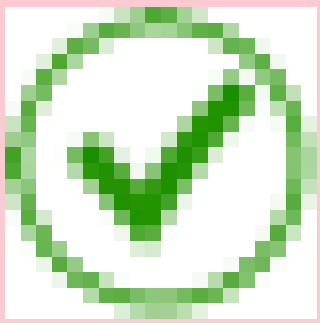
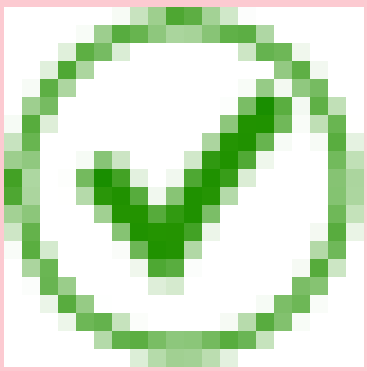
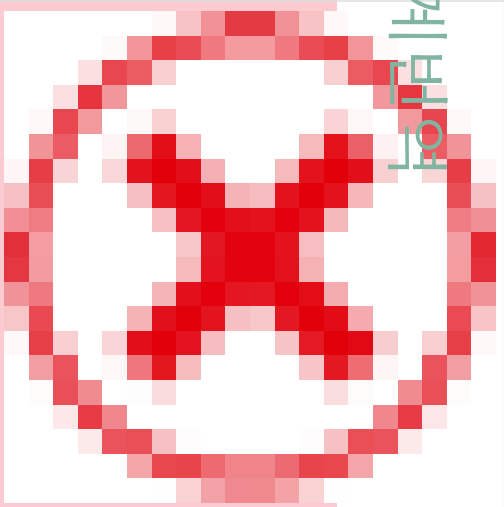
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
개요				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

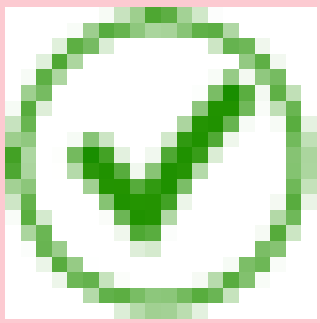
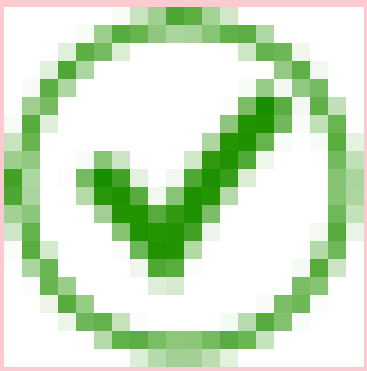
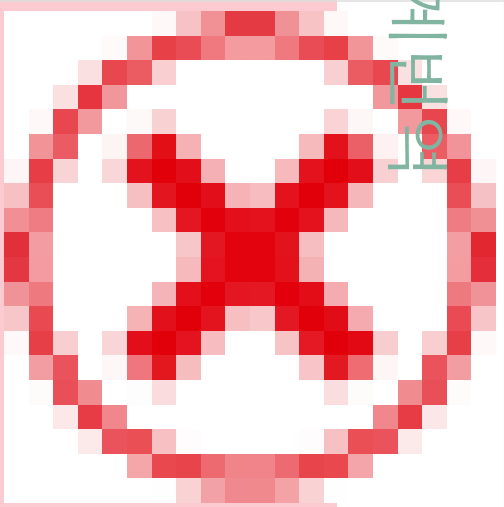
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
내 승인				

정정 작업

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

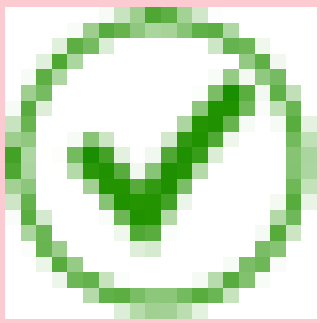
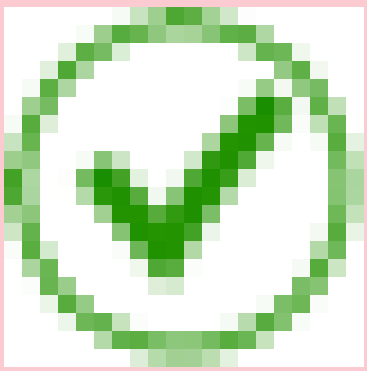
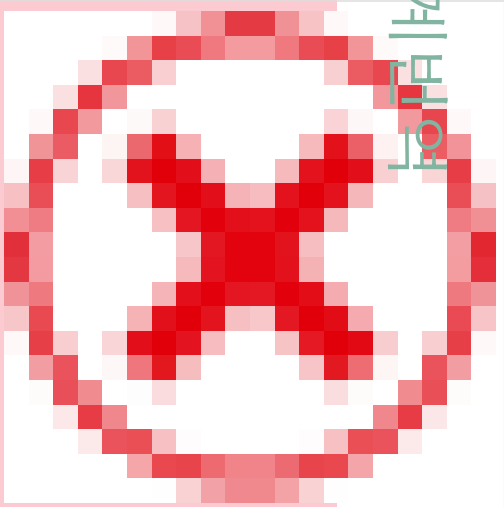
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
활성				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

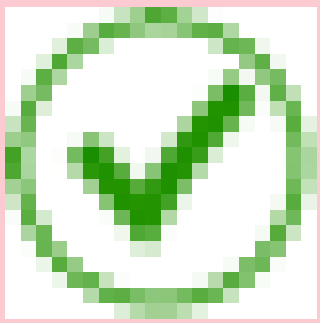
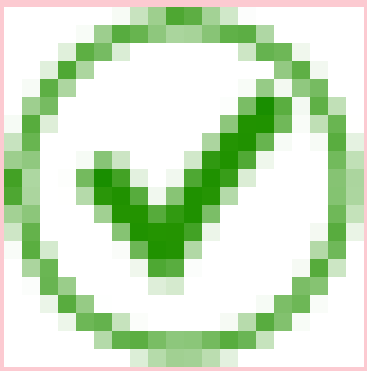
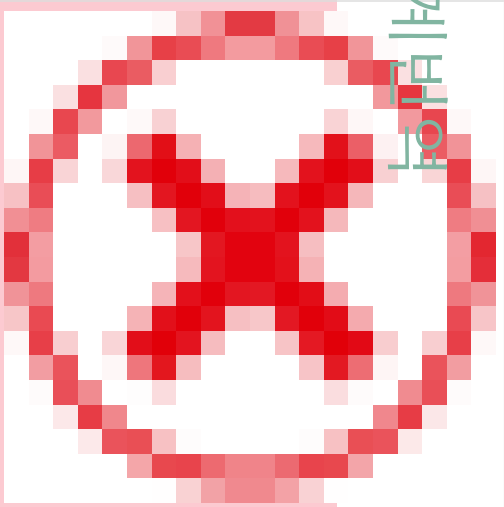
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
나에게 할당됨				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

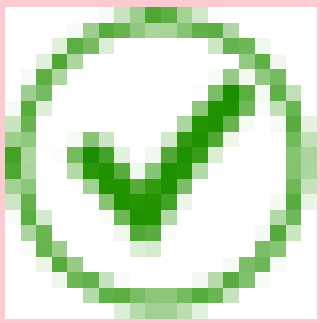
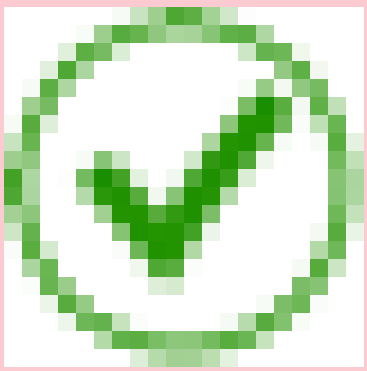
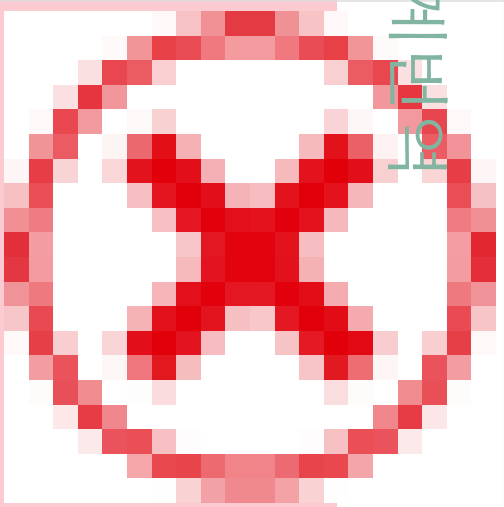
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
사용자 그룹에 할당됨				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

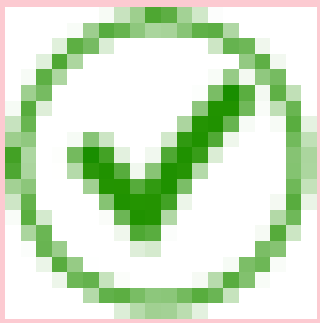
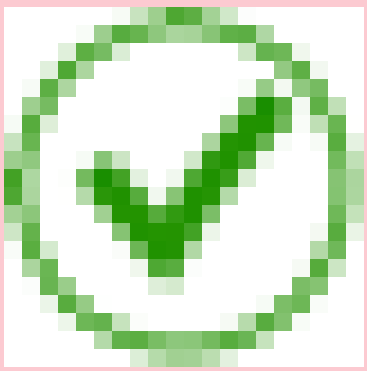
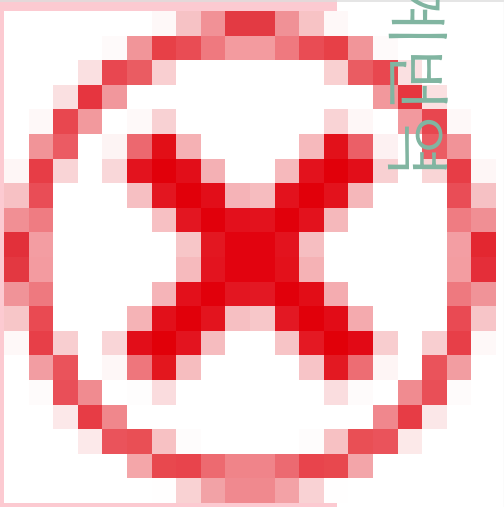
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
모두				

취약 항목

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

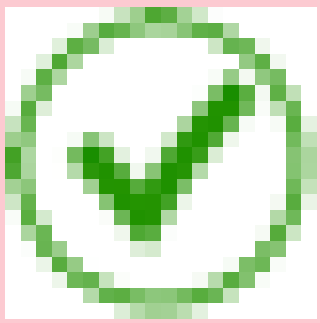
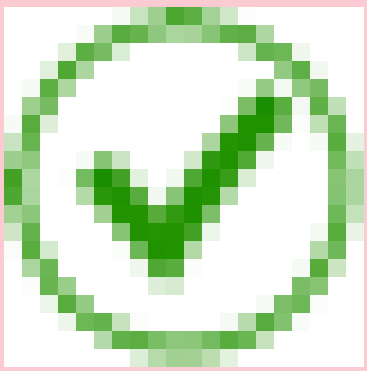
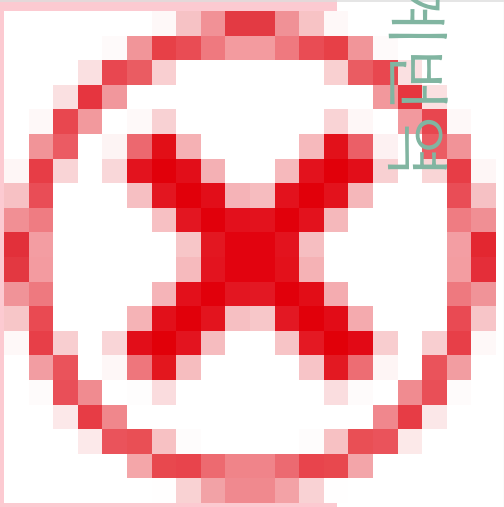
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
중요 위험				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

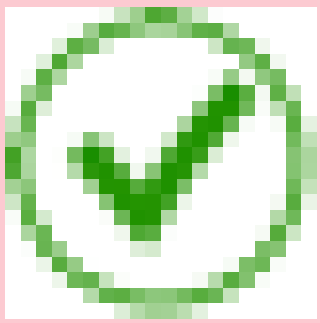
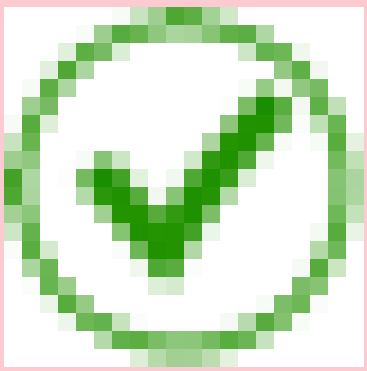
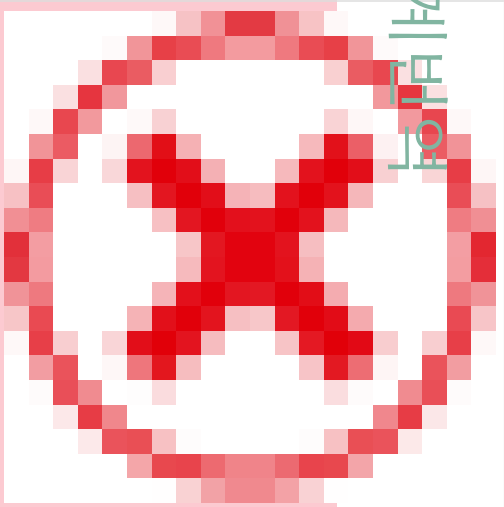
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
높은 위험				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

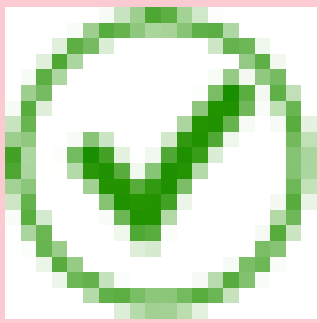
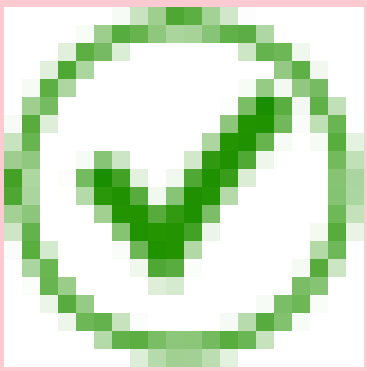
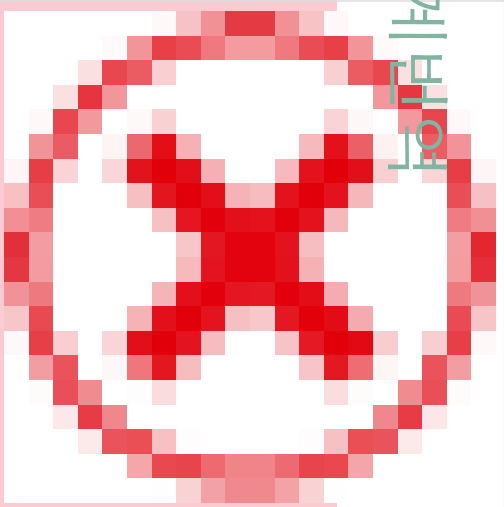
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
악용 가능				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

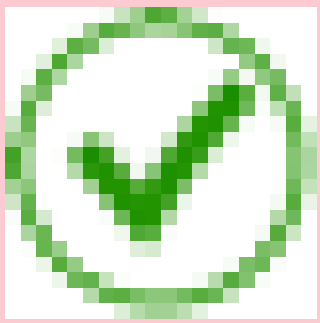
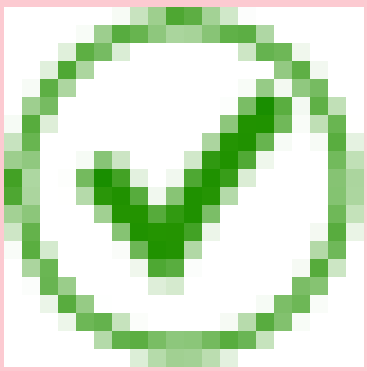
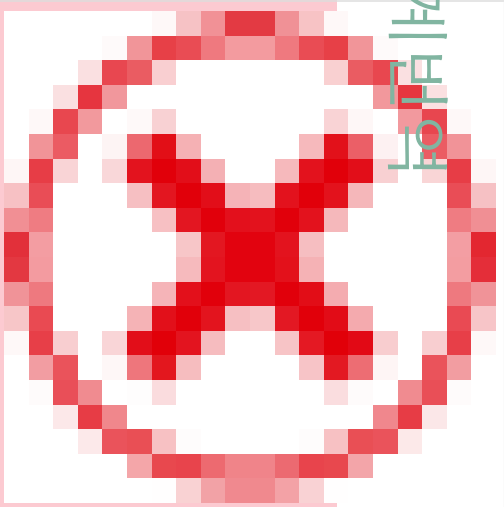
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
대상에 접근				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

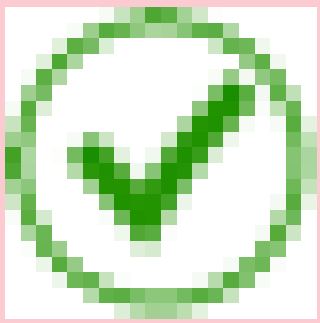
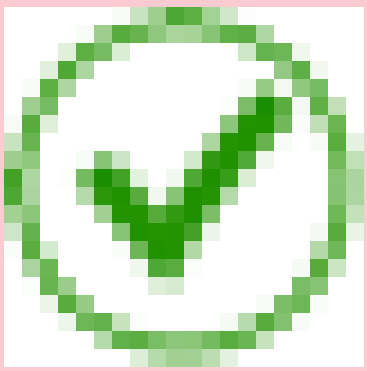
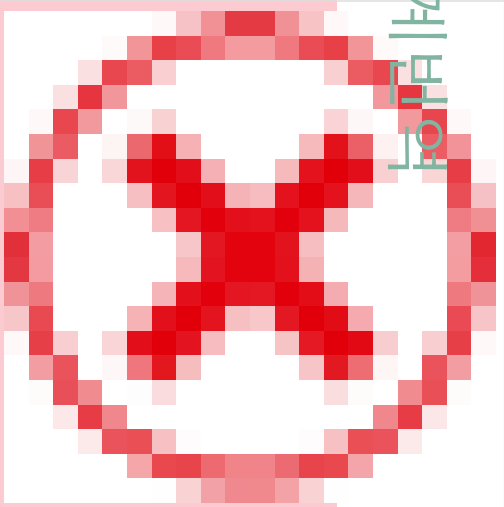
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
누락된 대상				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

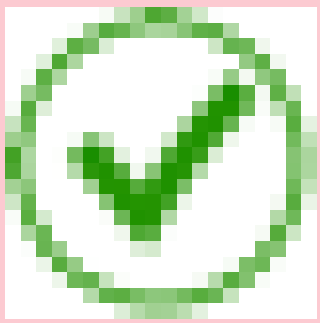
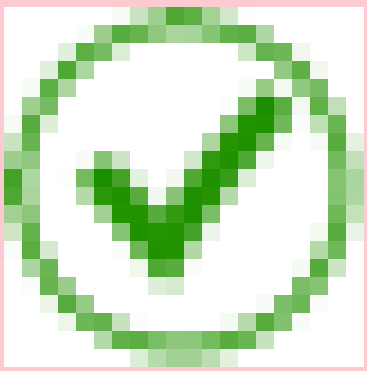
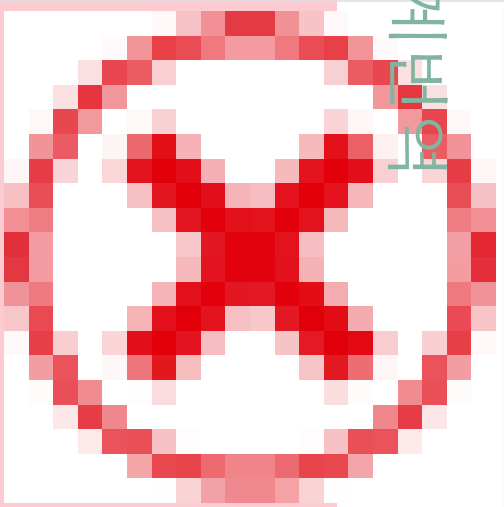
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
지난 90일 이내				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

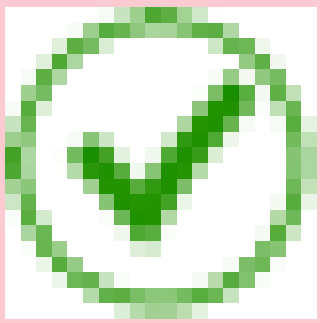
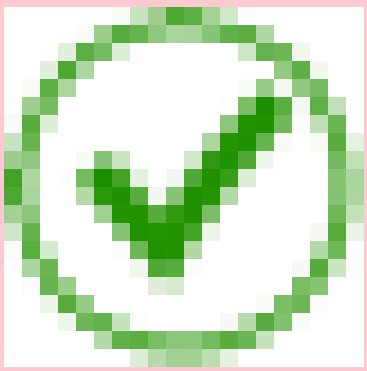
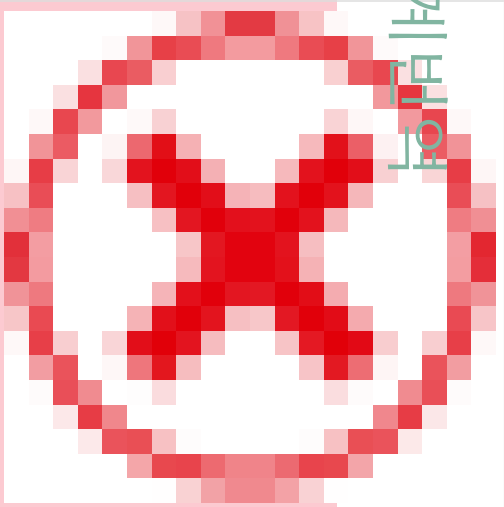
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
90일 경과				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

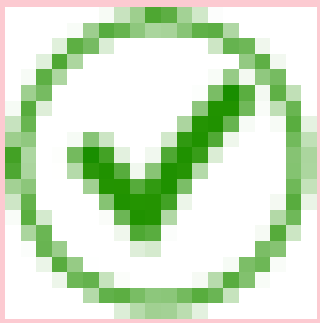
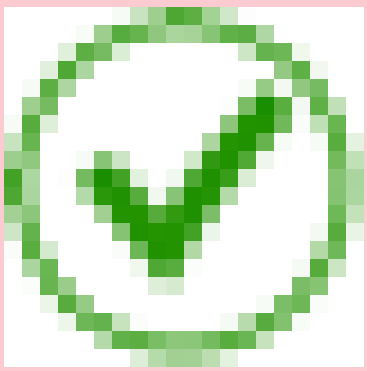
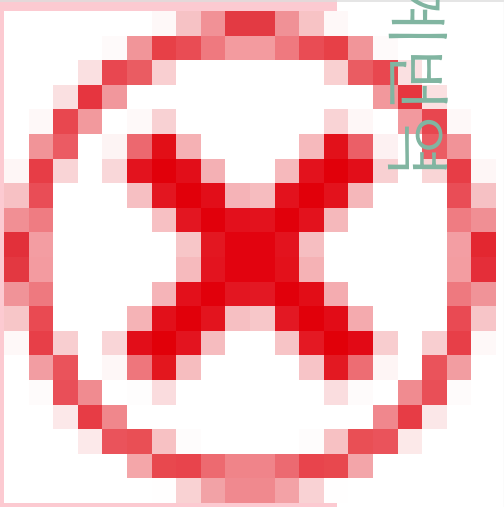
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
미할당				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

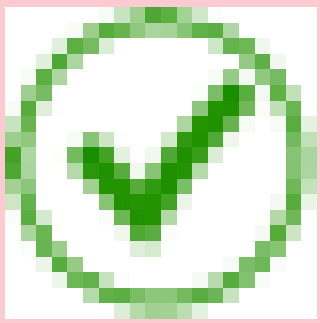
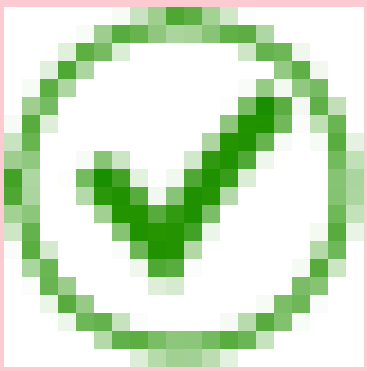
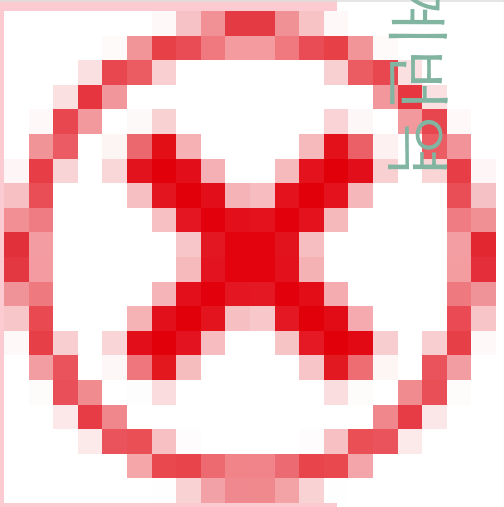
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
그룹 해제				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

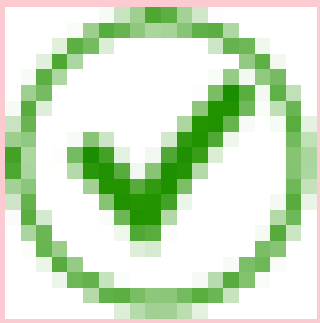
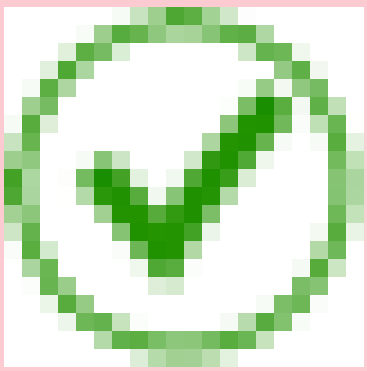
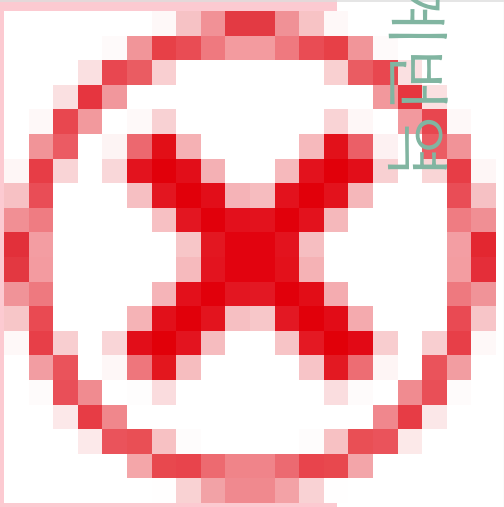
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
해제됨				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

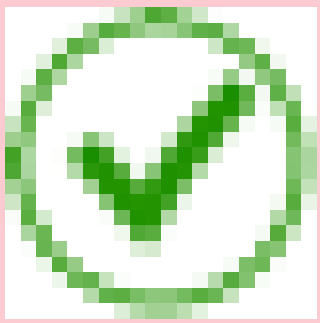
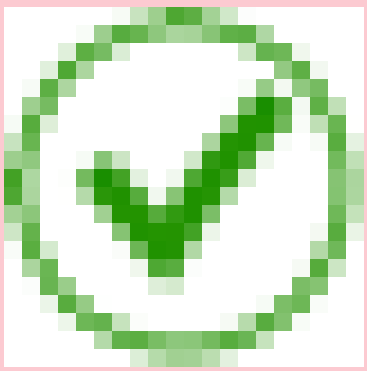
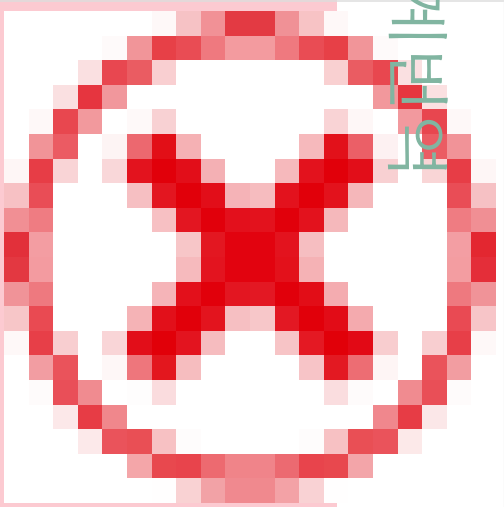
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
여러 지연				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

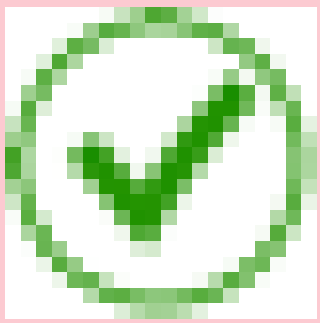
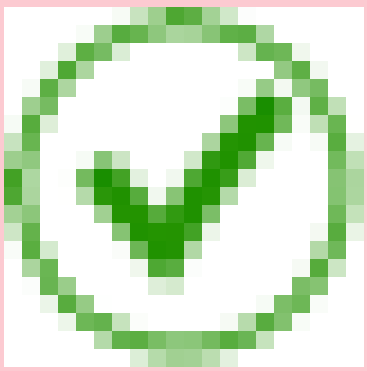
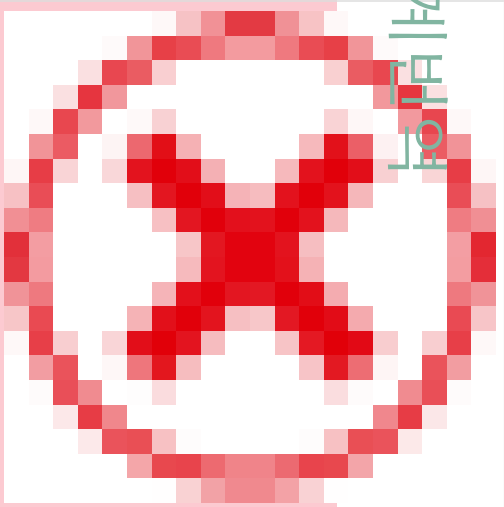
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
모두				

솔루션

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

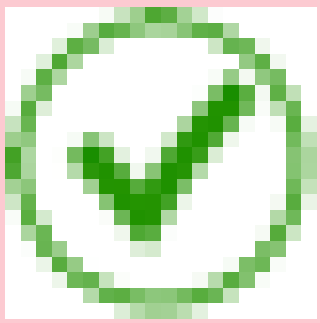
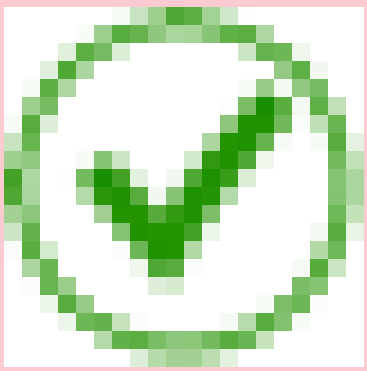
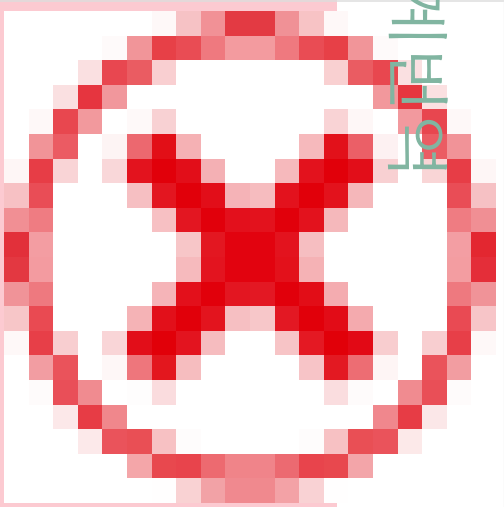
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
모두				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

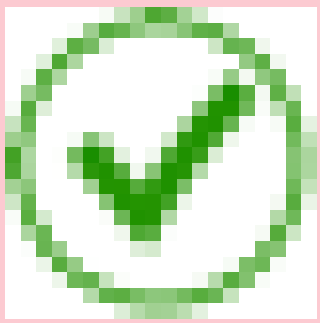
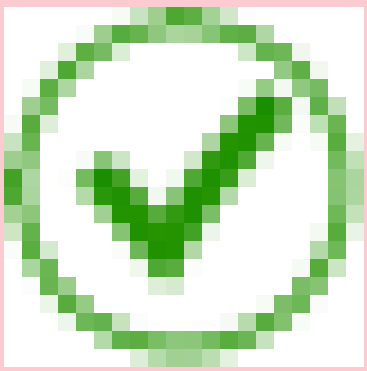
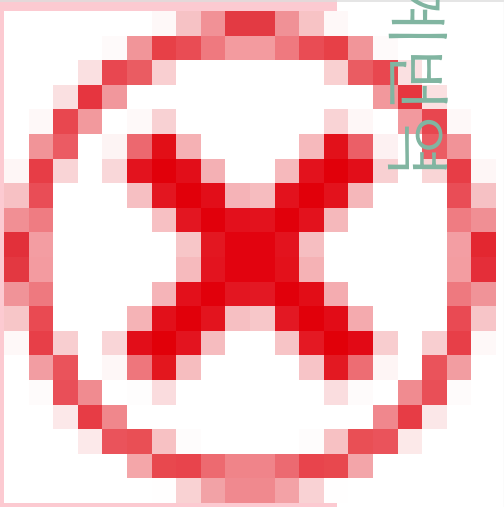
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
가장 높은 대체				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

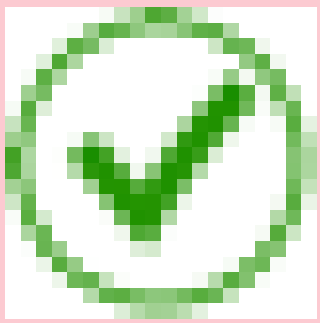
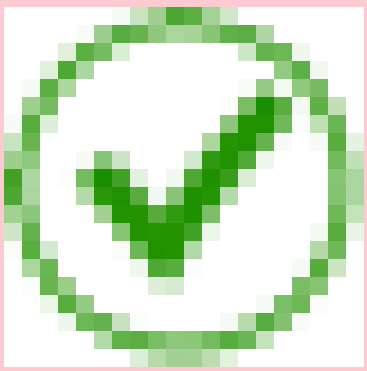
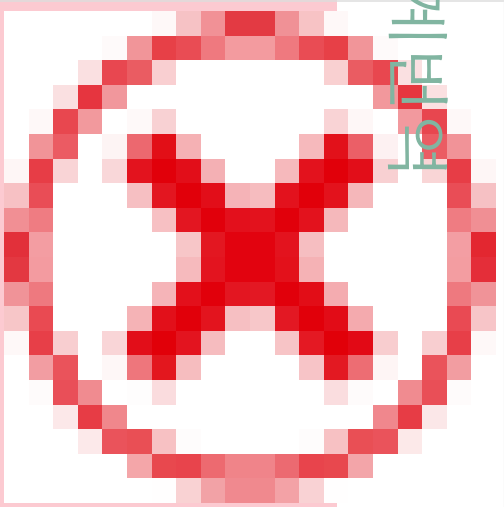
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
취약한 항목 포함				

라이브러리

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

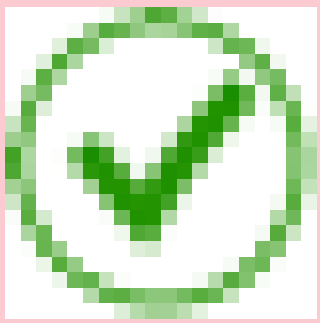
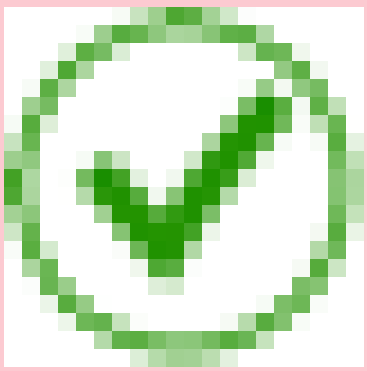
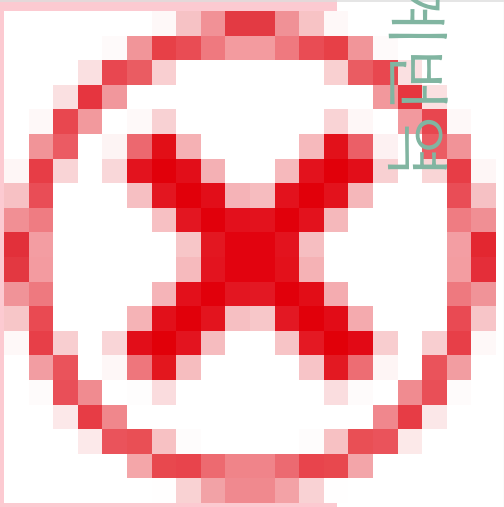
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
NVD				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

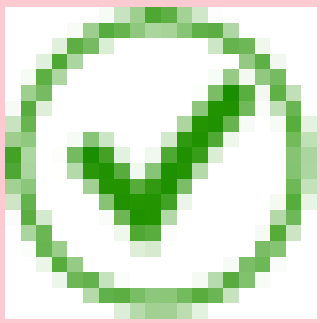
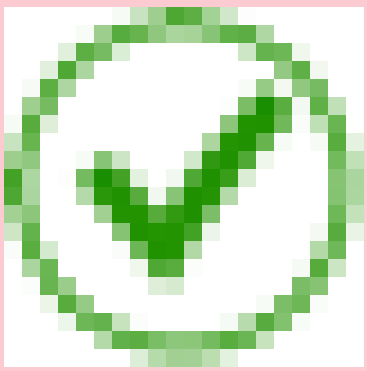
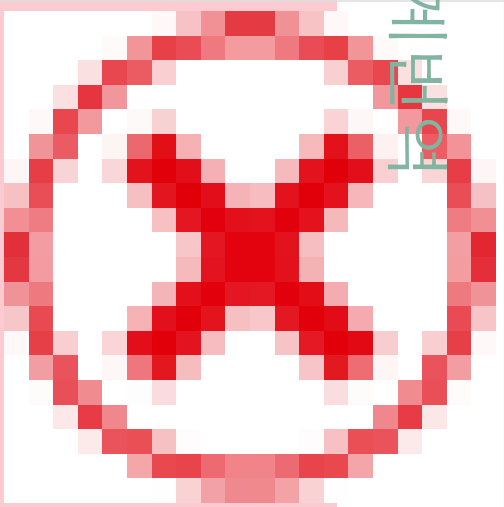
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
CWE				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

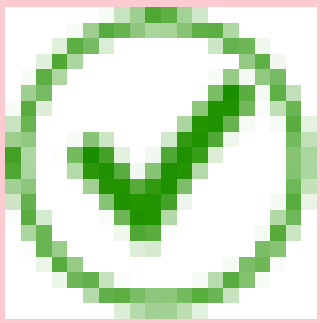
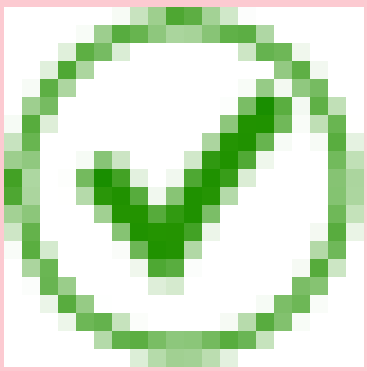
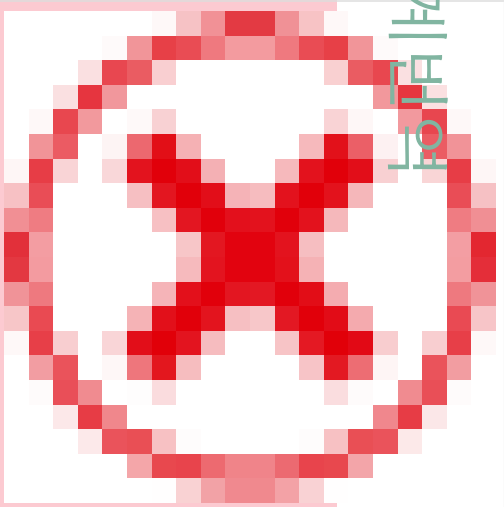
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
외부 공급업체				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

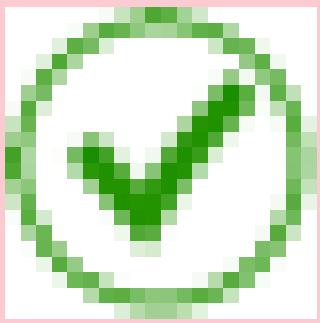
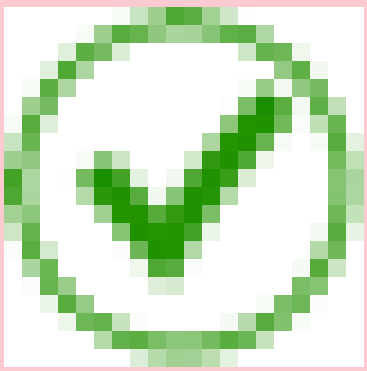
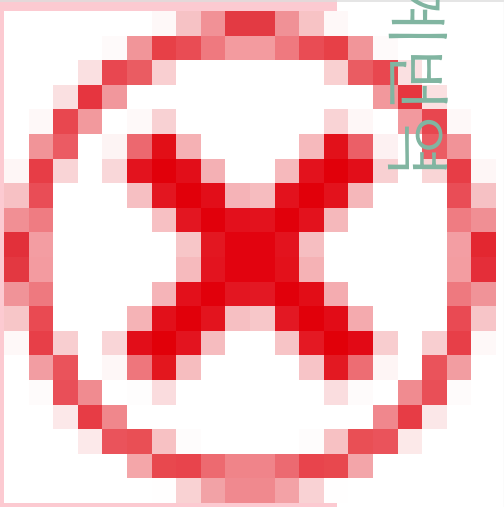
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
취약한 소프트웨어				

취약성 스캐닝

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

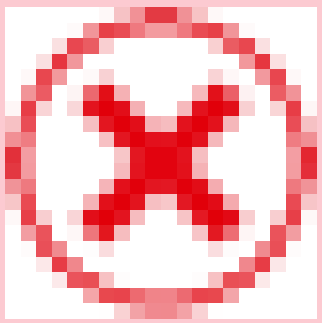
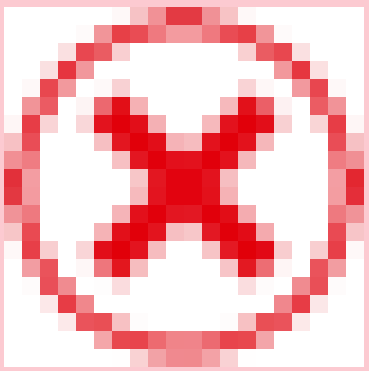
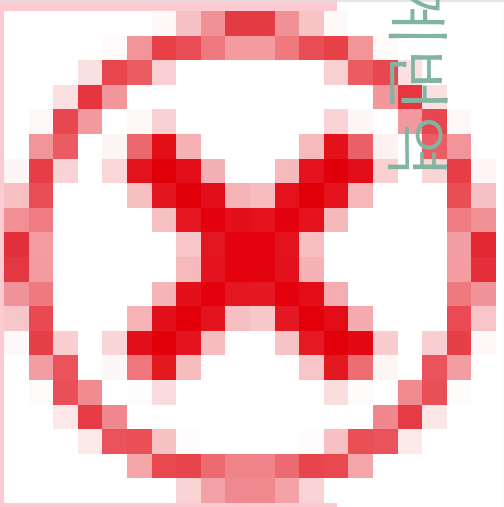
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
노출 평가				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

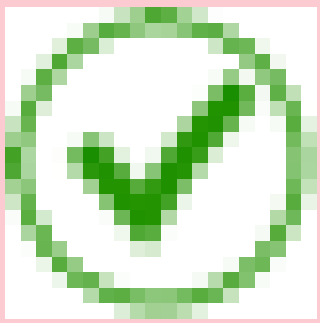
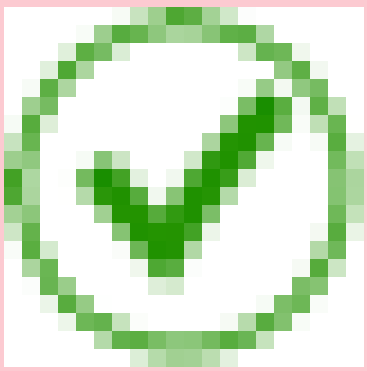
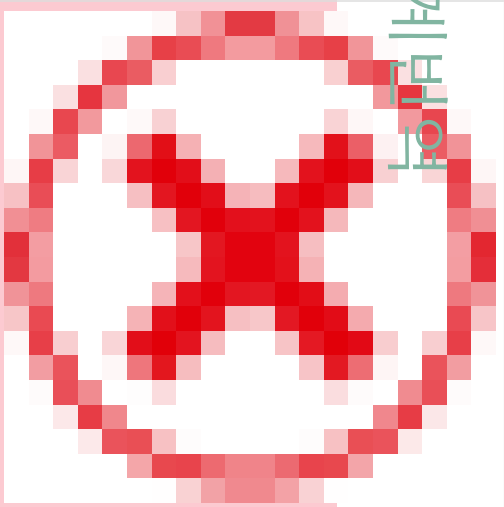
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
스캔				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

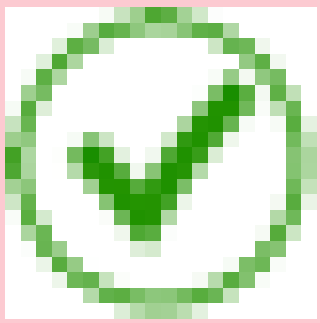
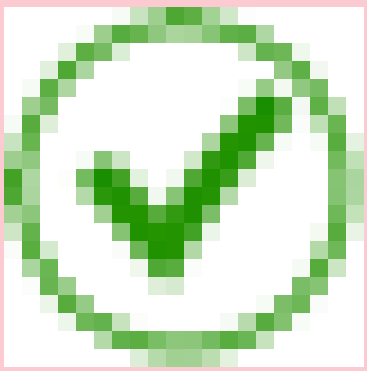
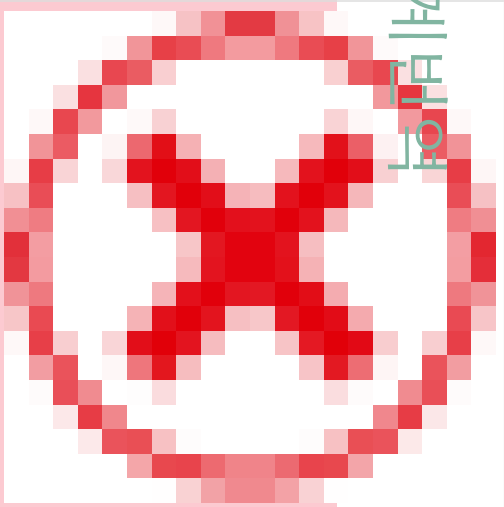
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
스캐너				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

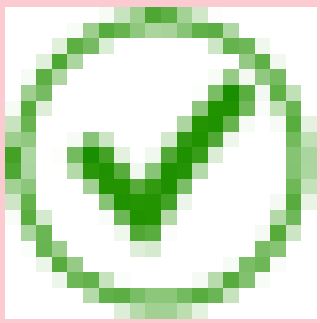
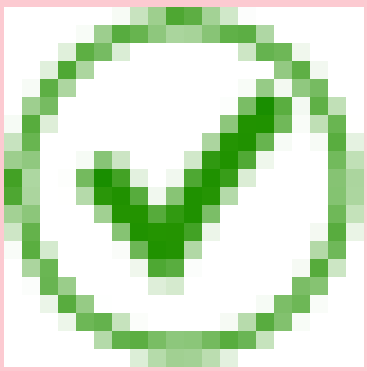
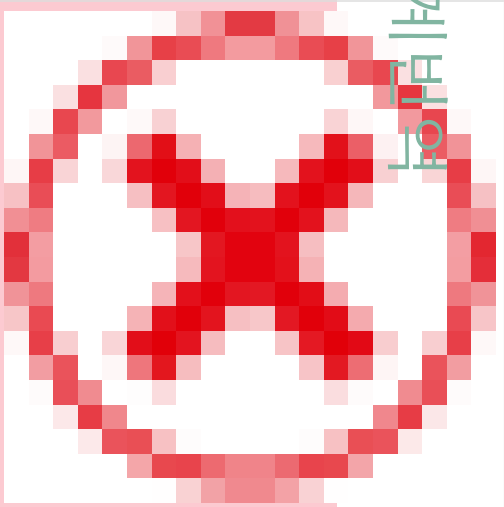
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
스캔 큐				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

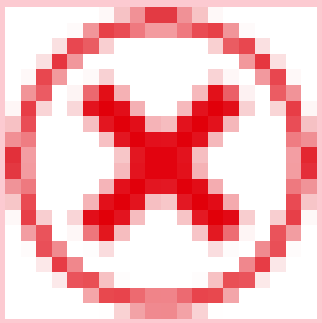
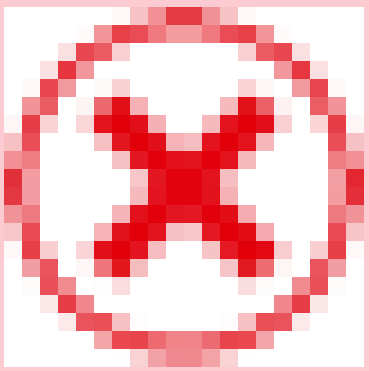
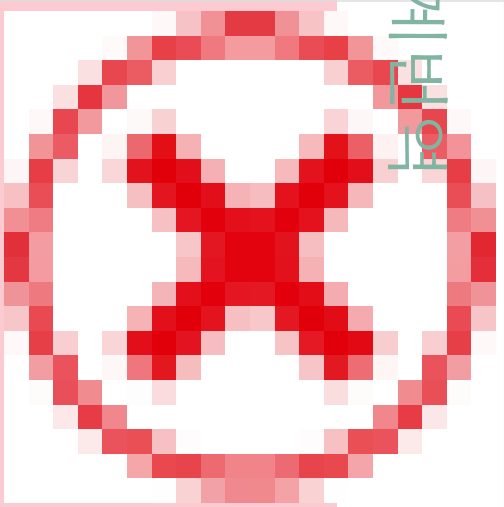
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
스캐너 속도 제한				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

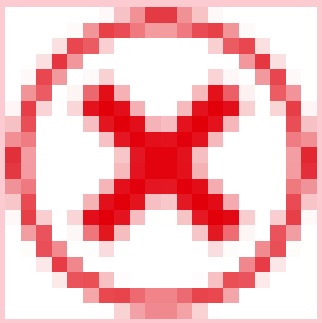
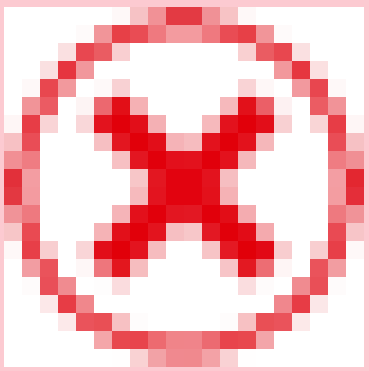
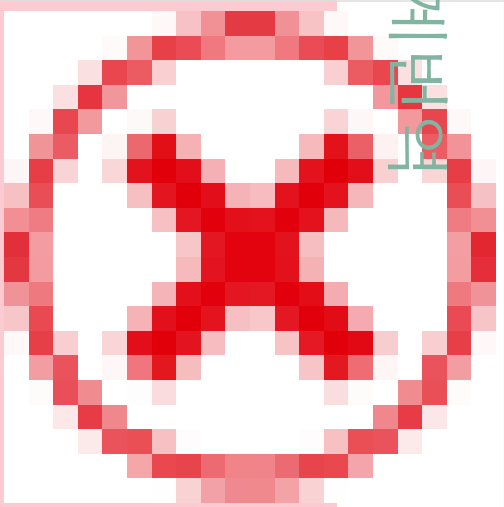
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
속도 제한 정의				

관리

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

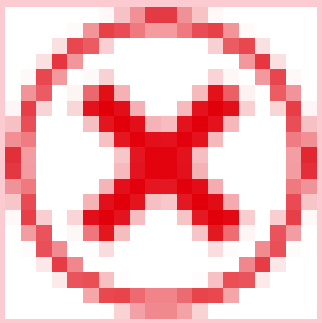
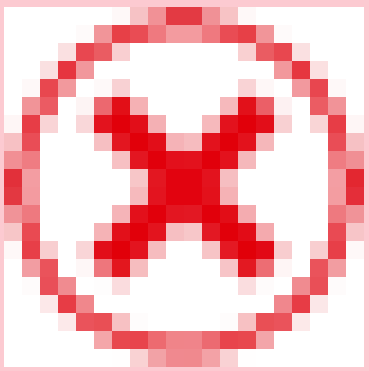
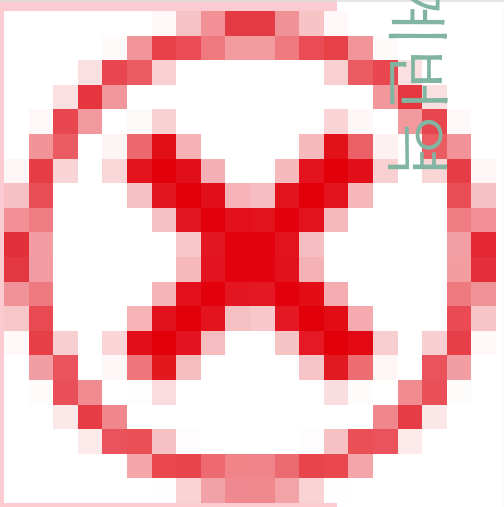
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
설정 도우미				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

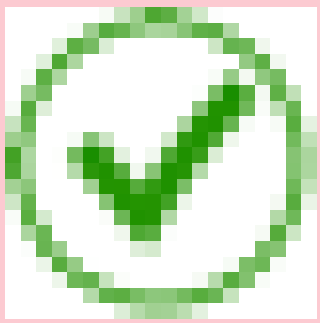
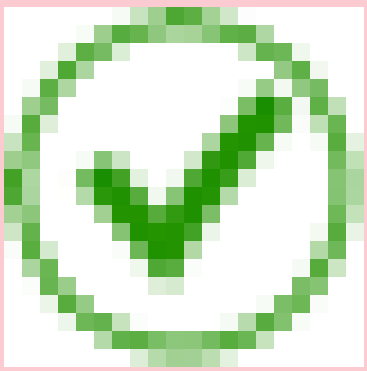
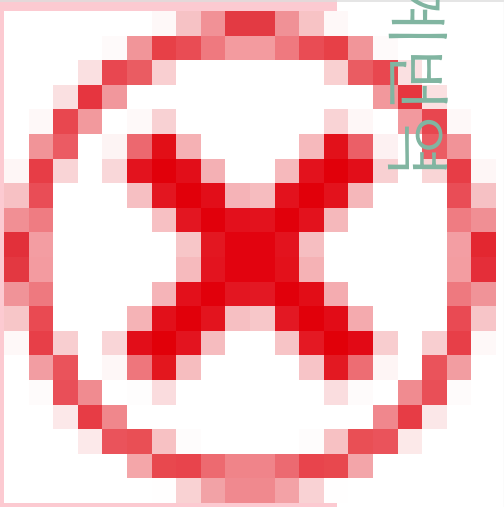
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
주시 주제				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

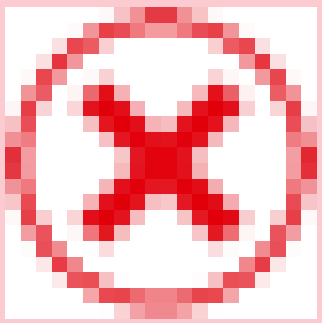
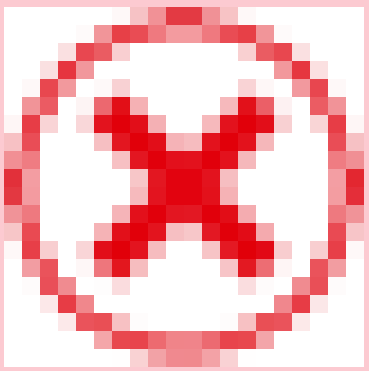
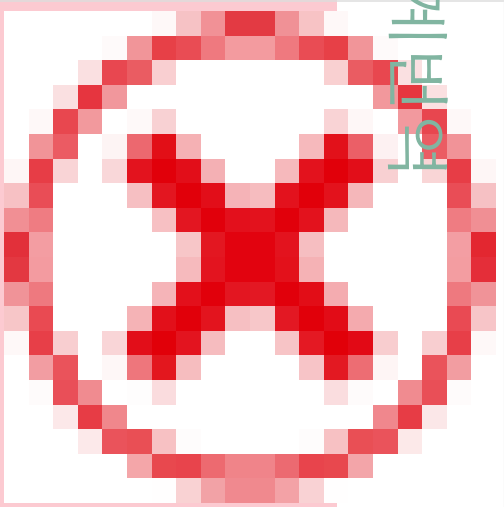
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
담당 규칙				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

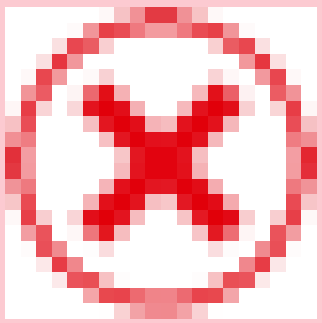
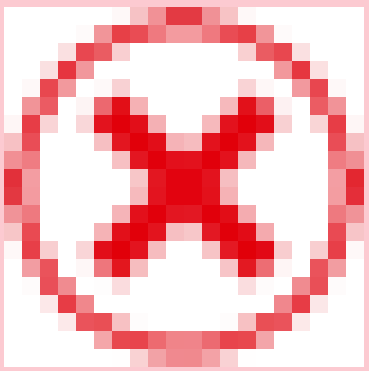
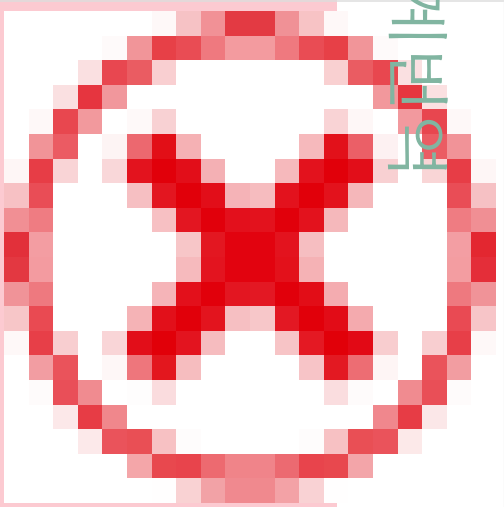
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
정정 작업 규칙				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

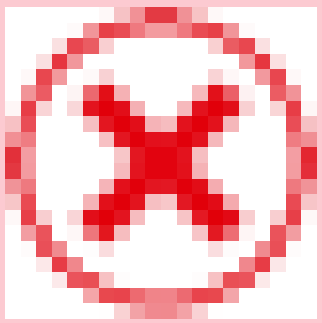
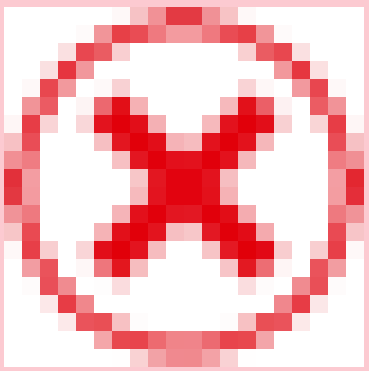
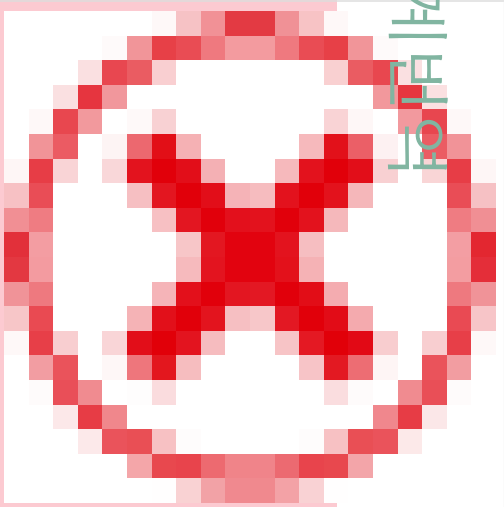
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
할당 권장 사항				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

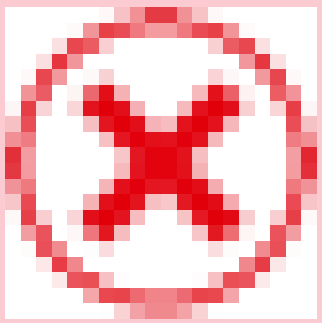
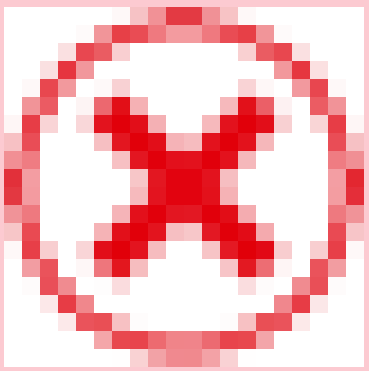
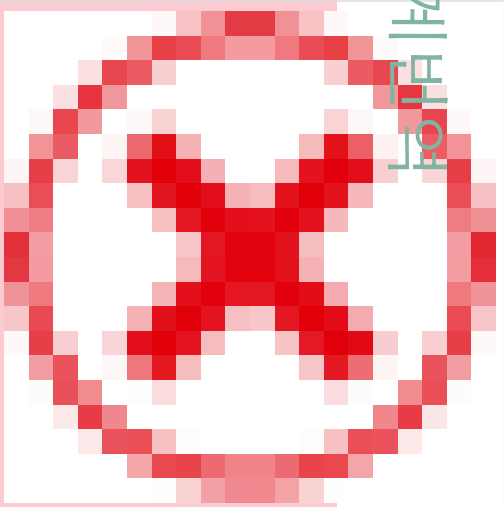
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
취약성 계산기				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

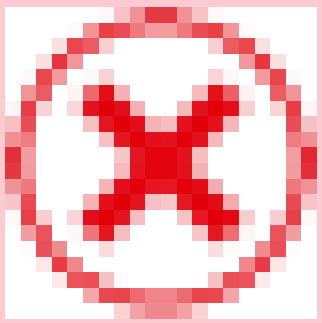
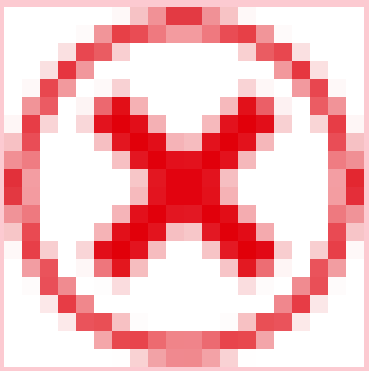
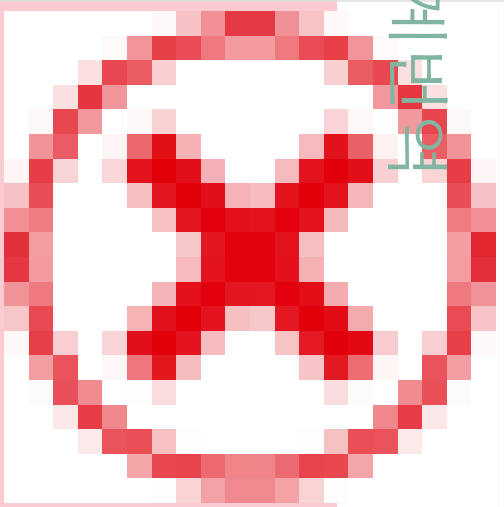
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
취약성 롤업 계산기				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

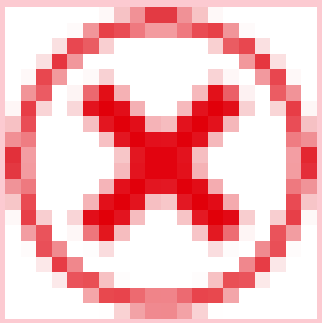
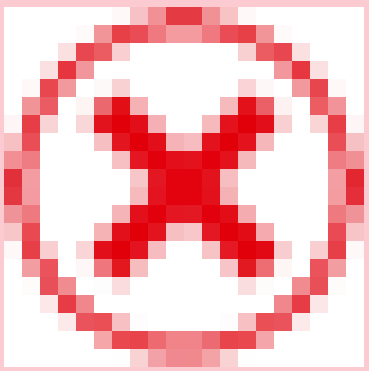
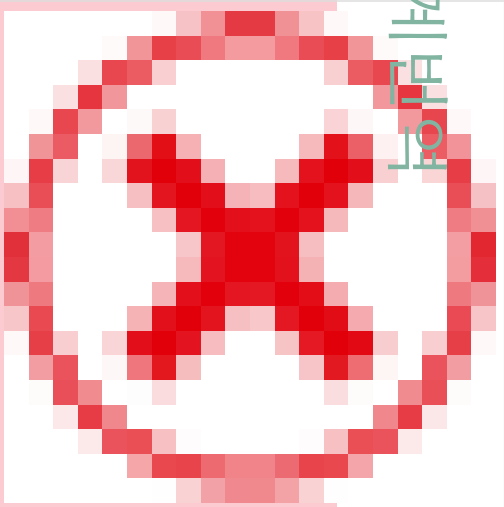
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
정정 대상 규칙				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

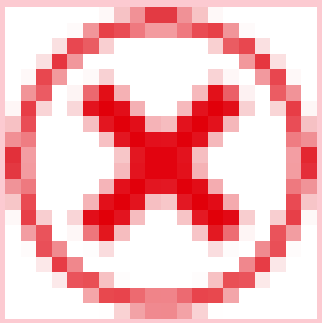
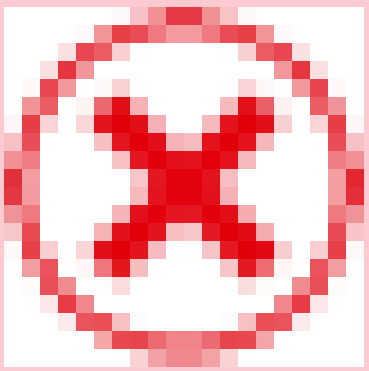
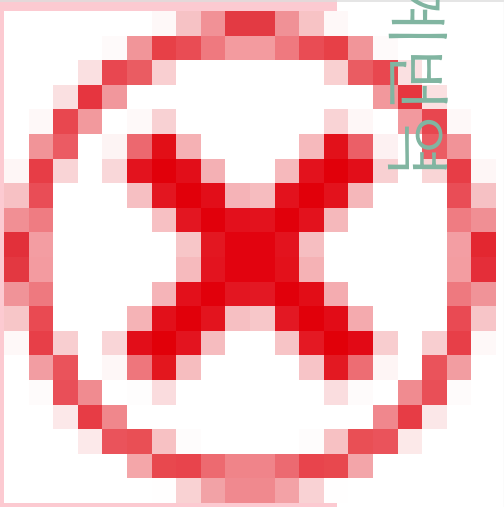
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
AutoClose 구성				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

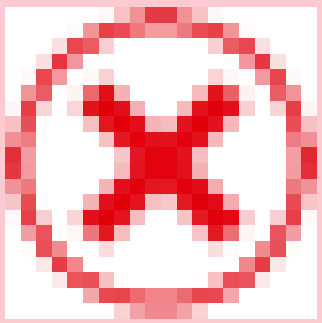
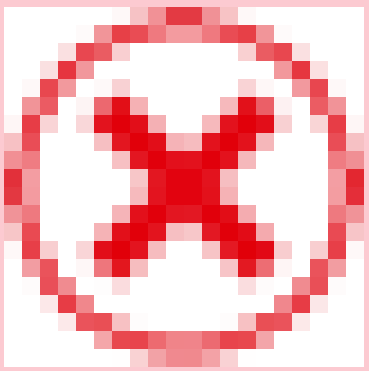
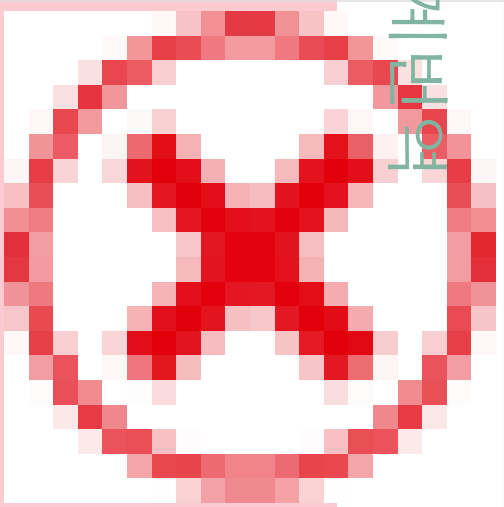
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
자동 삭제 규칙				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

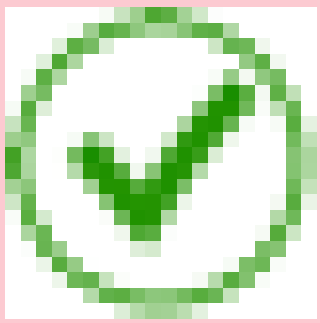
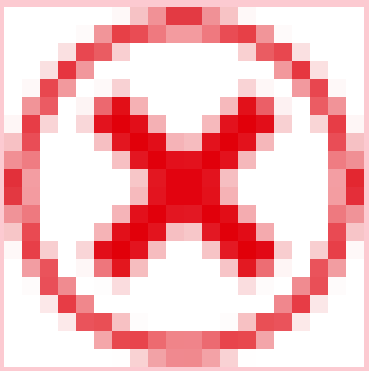
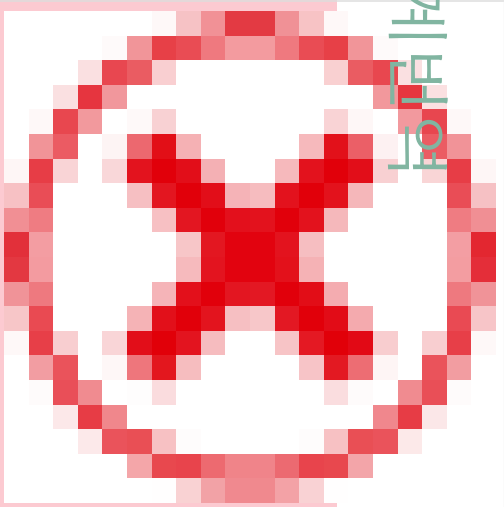
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
예외 규칙				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

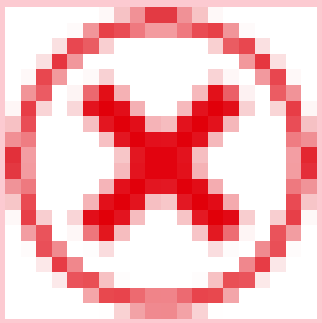
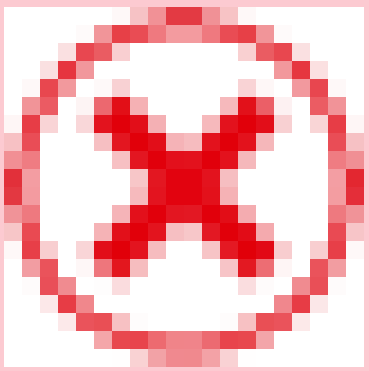
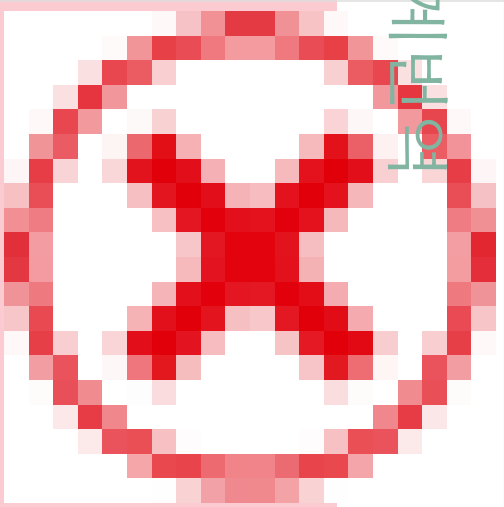
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
승인 규칙				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

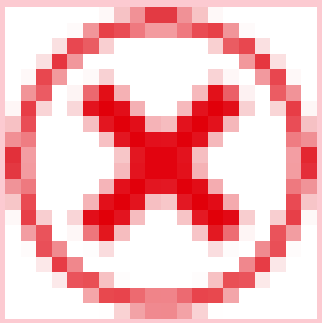
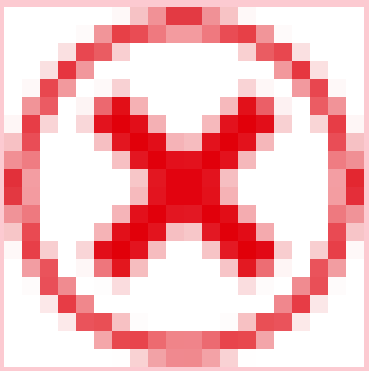
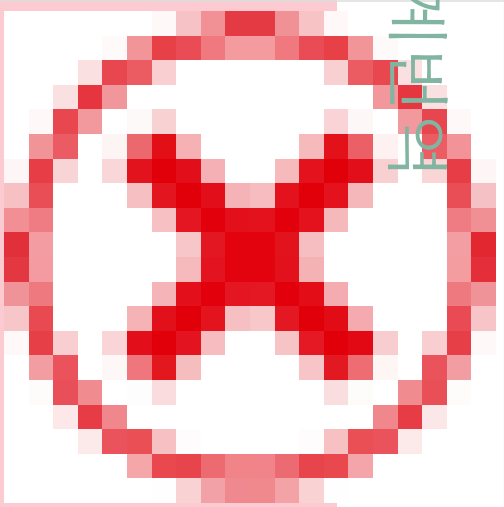
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
분류 규칙				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

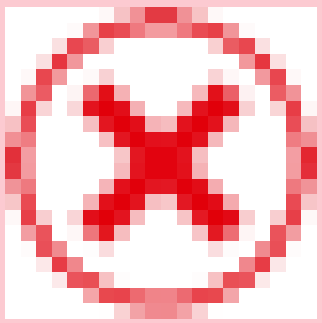
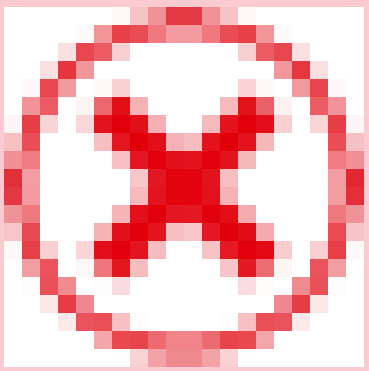
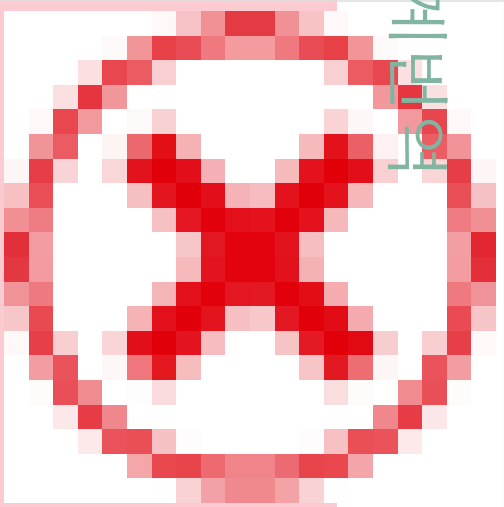
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
성과 구성				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

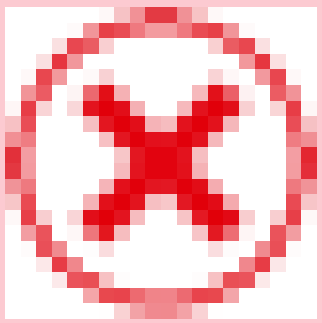
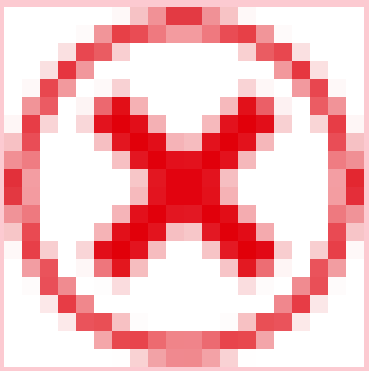
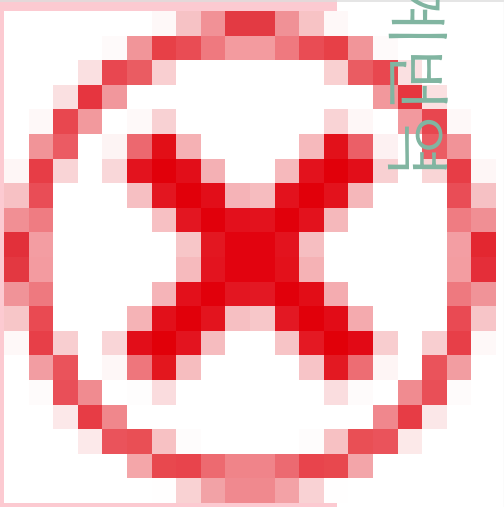
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
VI 세분성 구성				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

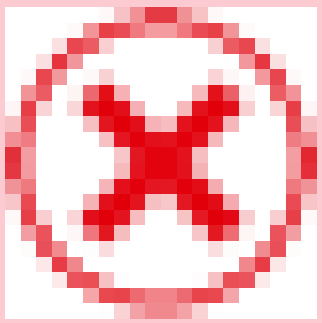
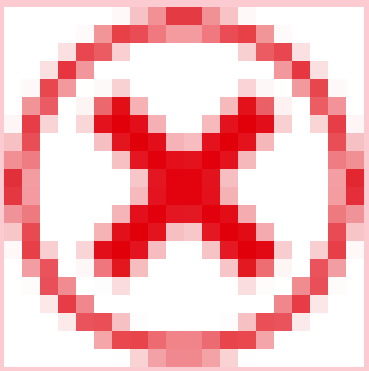
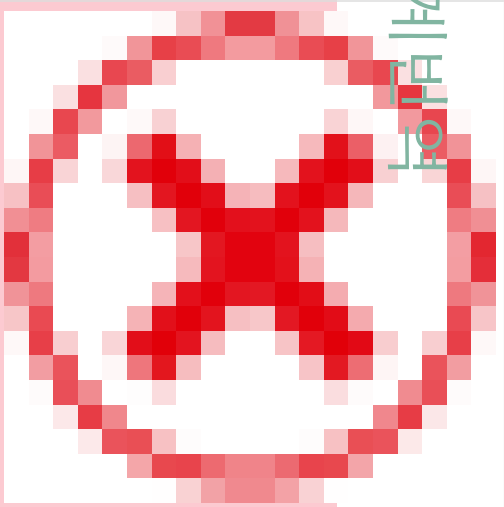
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
알림				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

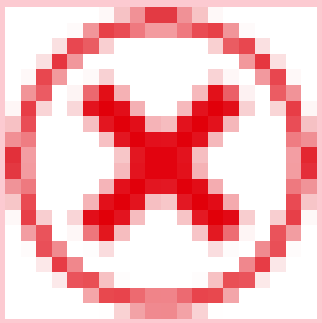
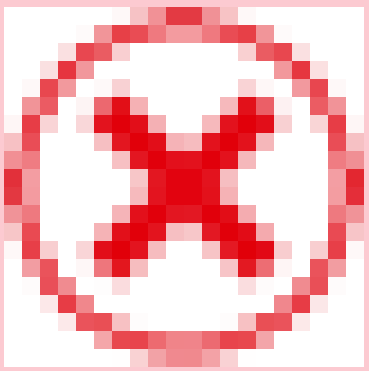
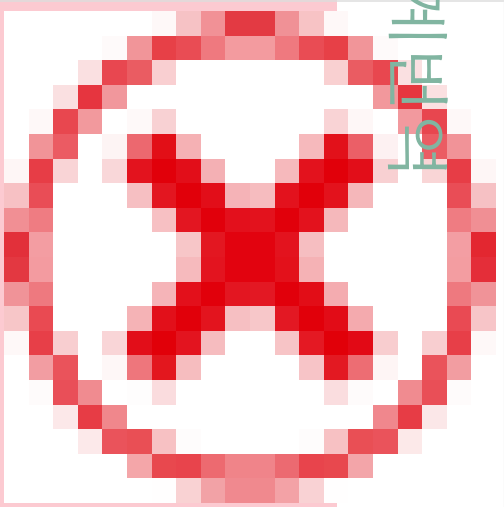
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
이메일 템플릿				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

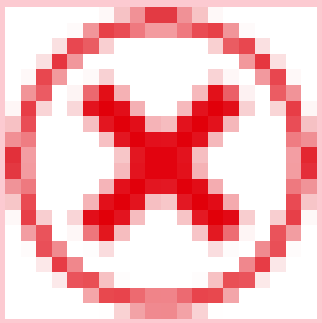
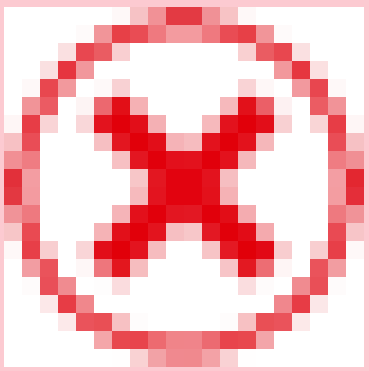
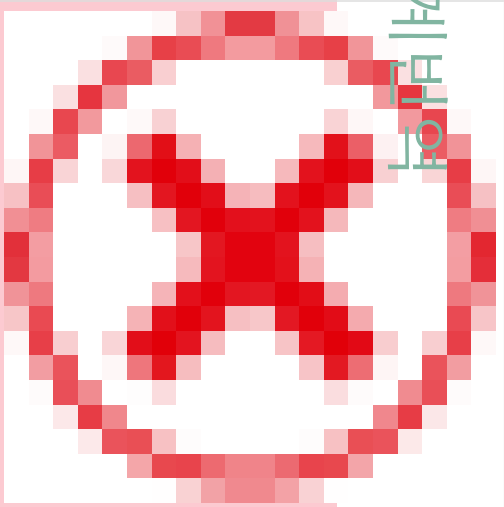
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
임포트 큐				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

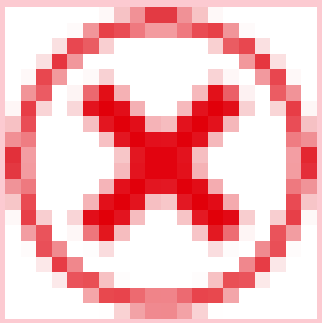
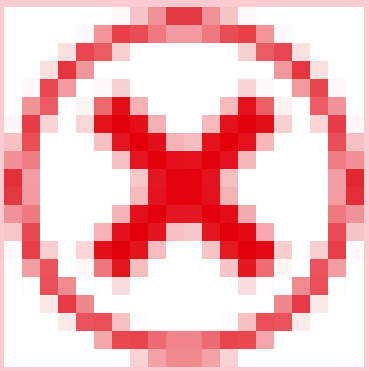
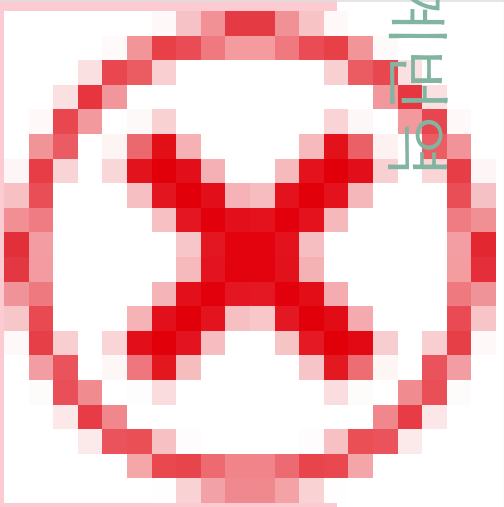
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
통합				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

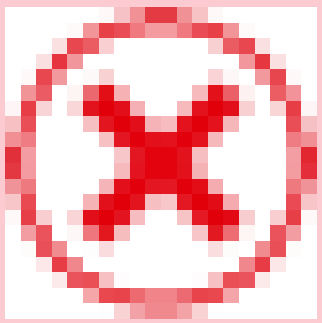
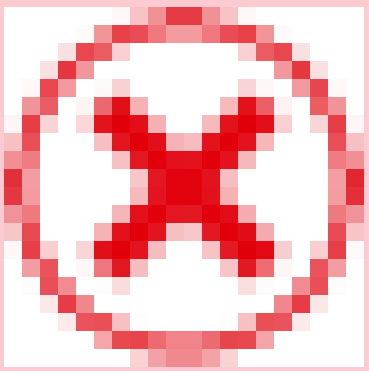
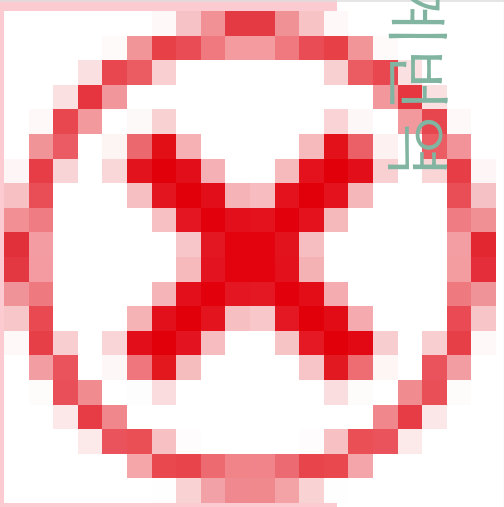
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
SLA 정의				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

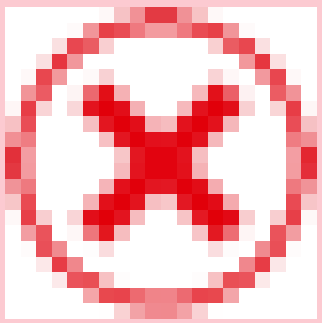
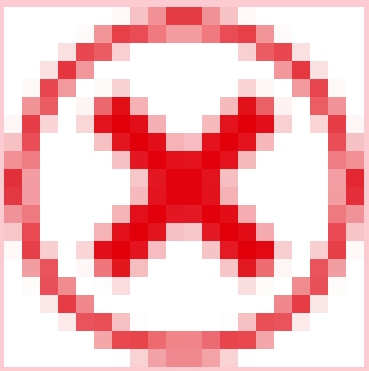
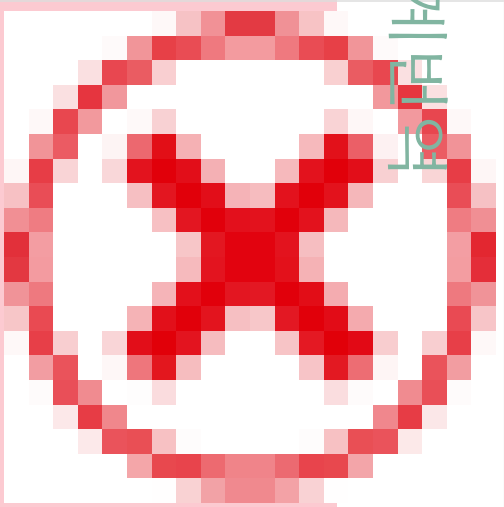
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
SAM NVD 구성				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

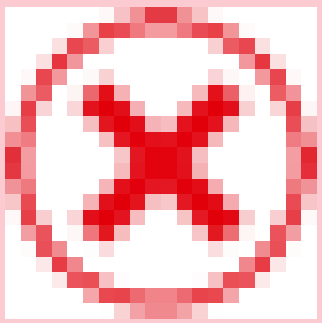
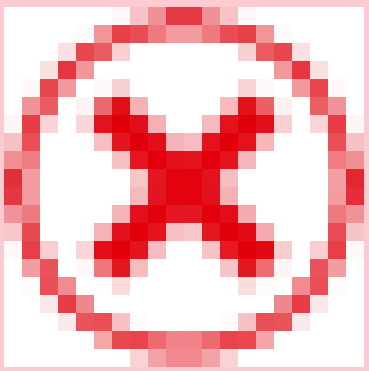
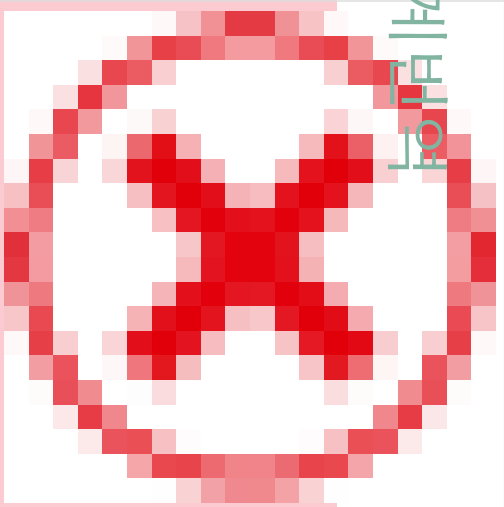
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
표준화된 심각성 맵				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

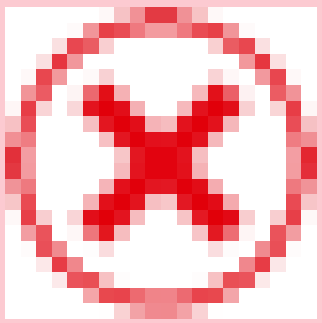
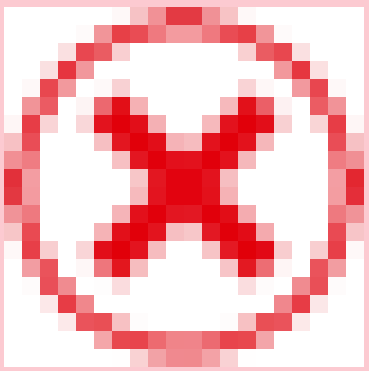
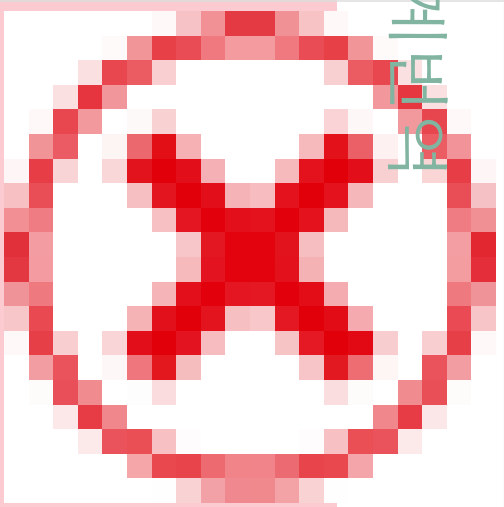
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
스캔 보장 범위 구성				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

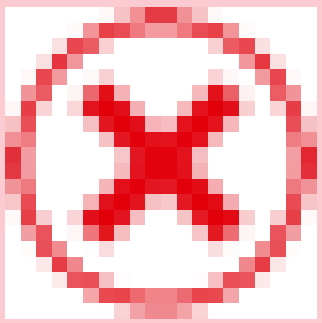
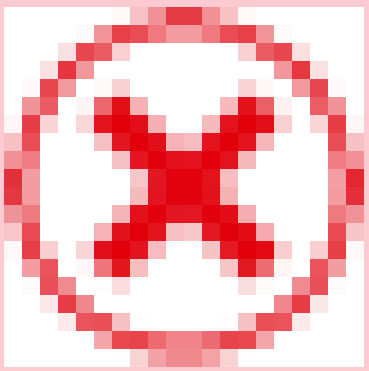
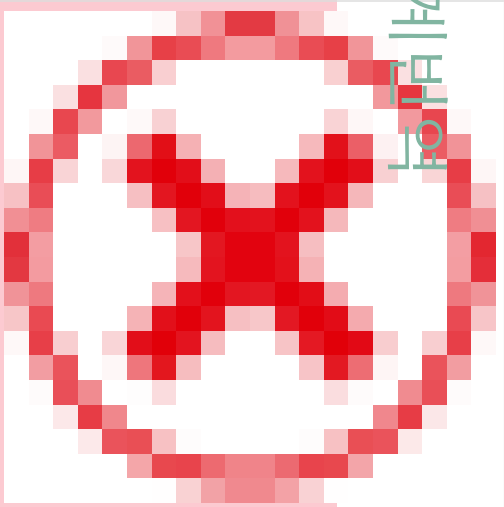
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
예외 관리				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

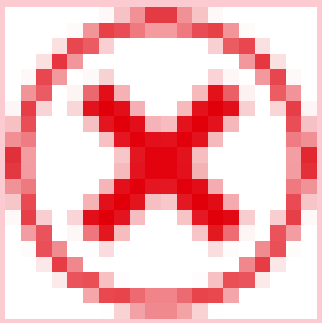
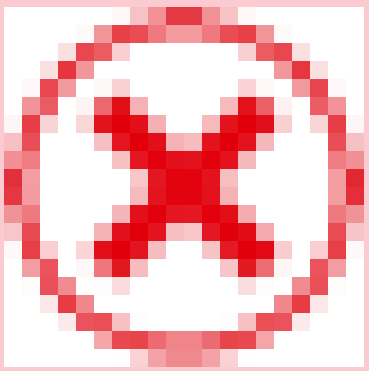
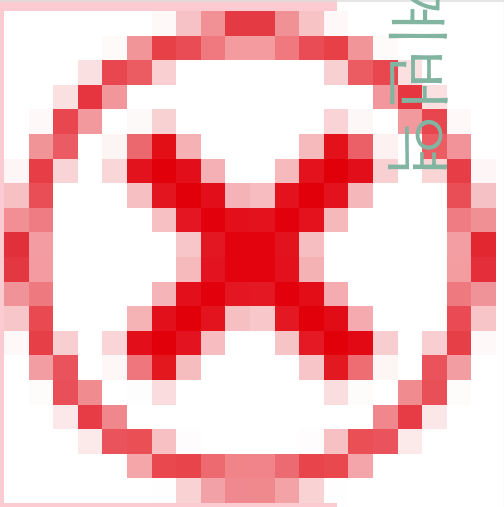
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
사용량 보고서				
진단				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

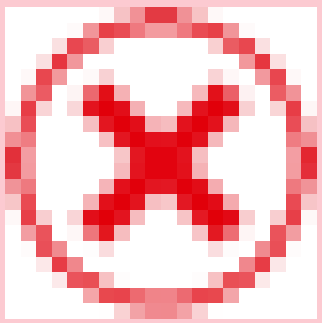
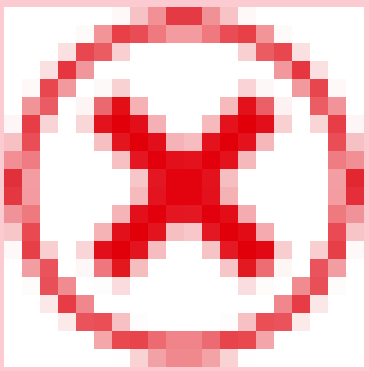
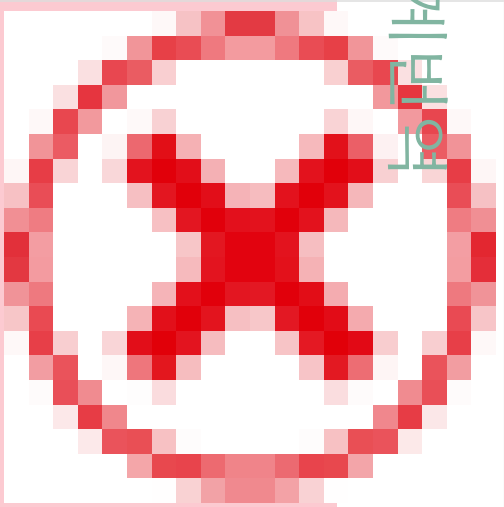
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_config	s
검사				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

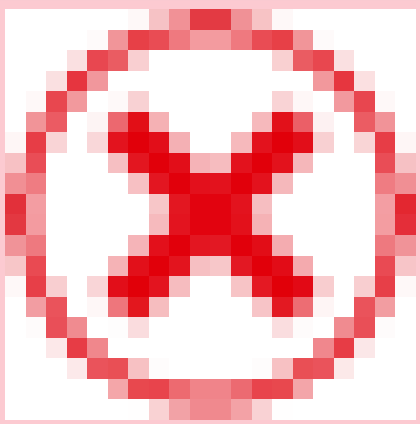
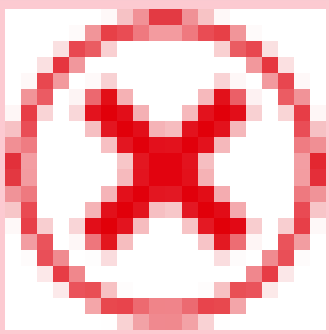
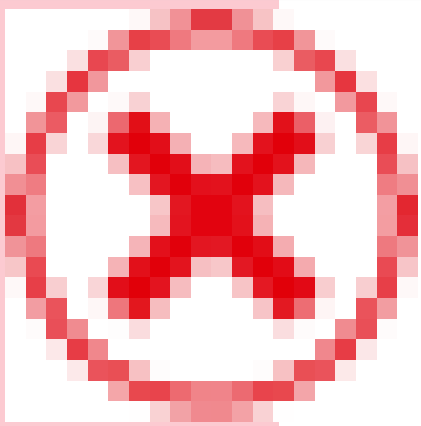
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
(메인 앱 그룹)				
CISO 대시보드				

기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

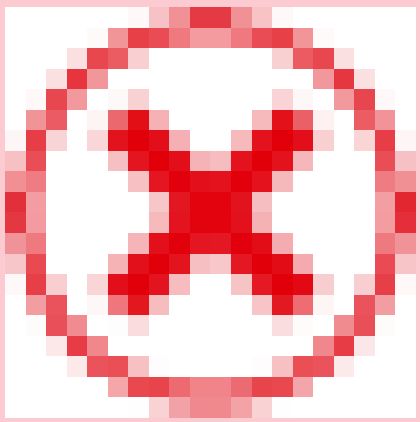
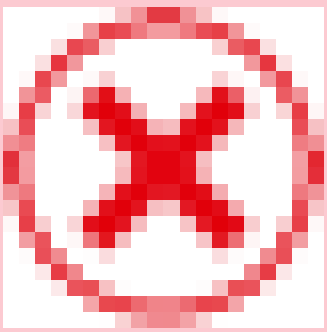
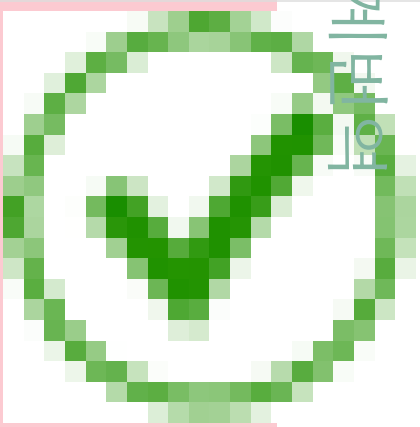
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
정정 개요				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

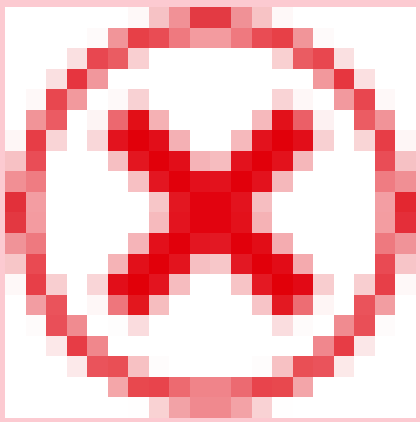
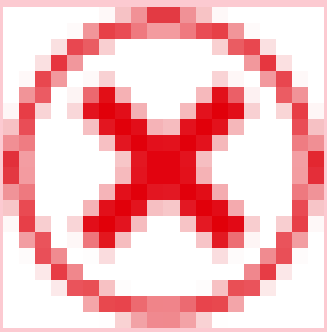
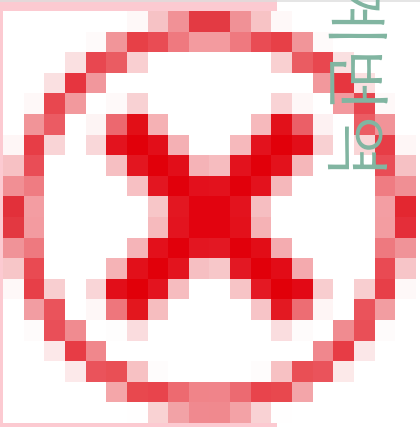
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
취약성 관리자 작업 공간				

고객 버전

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

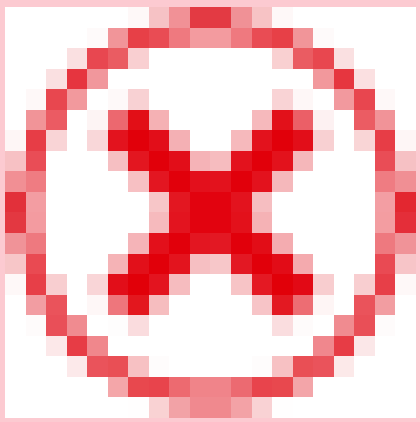
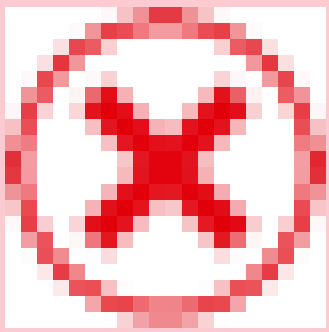
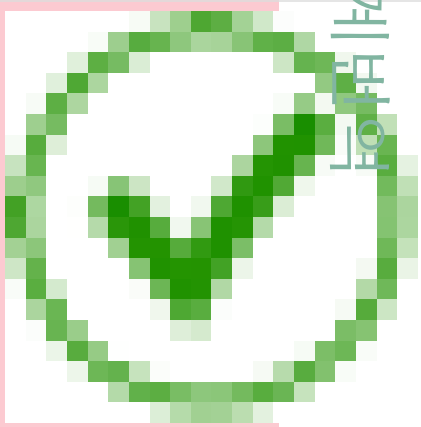
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
개요				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

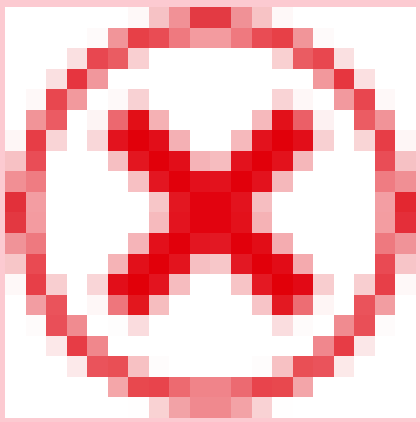
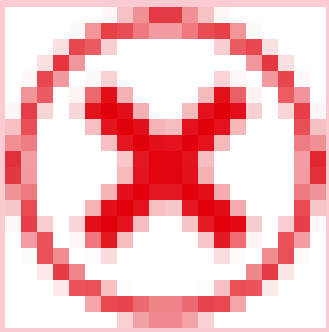
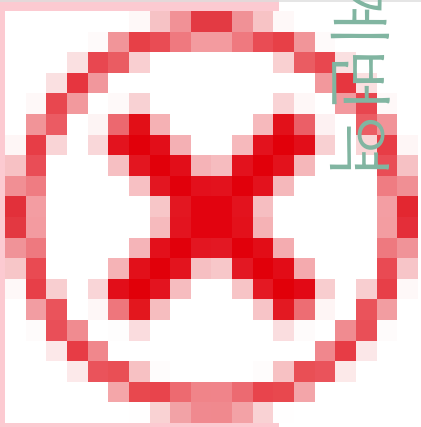
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
IT 정정 작업 공간				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

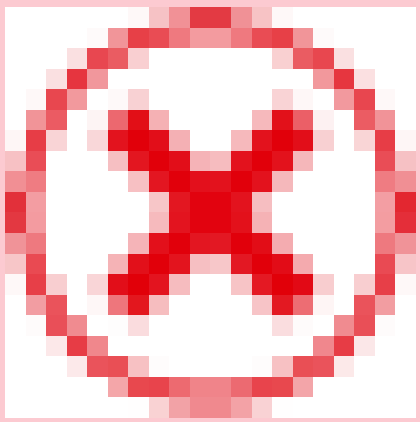
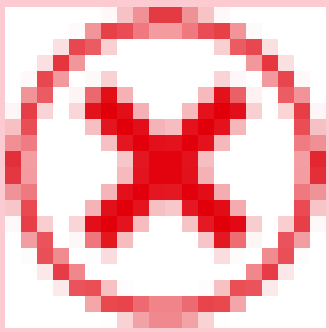
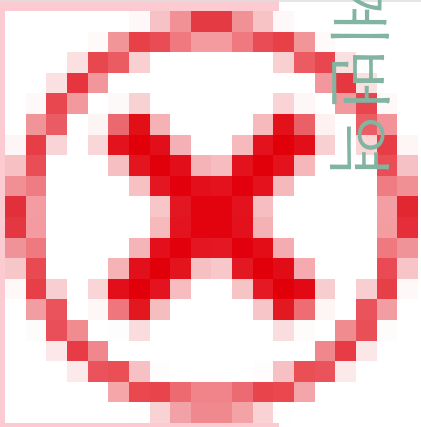
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
승인자 개요				

개발 버전

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

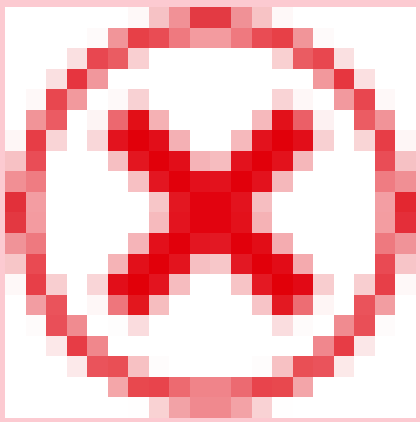
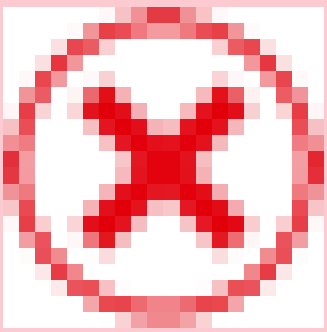
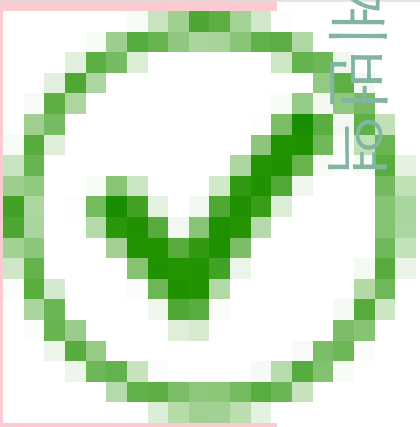
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
개요				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

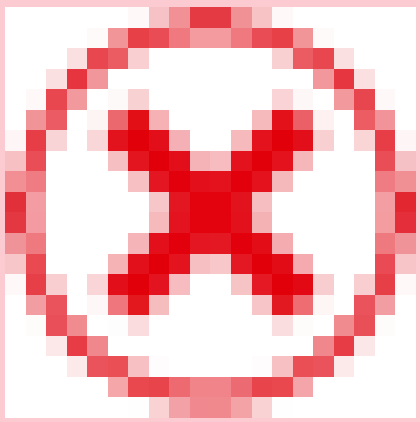
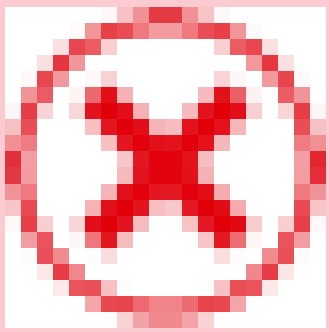
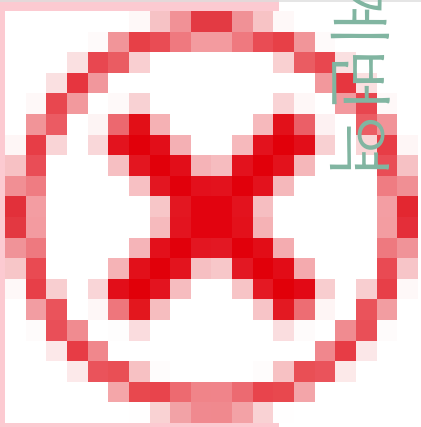
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
내 승인				
정정 작업				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

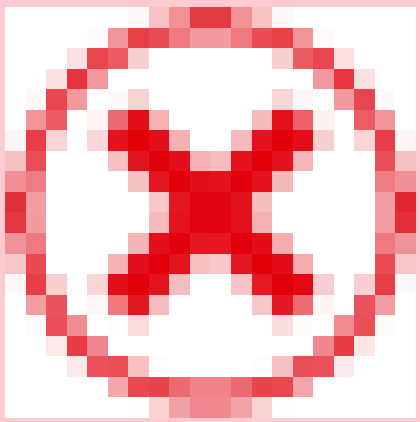
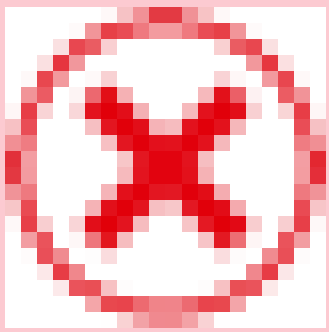
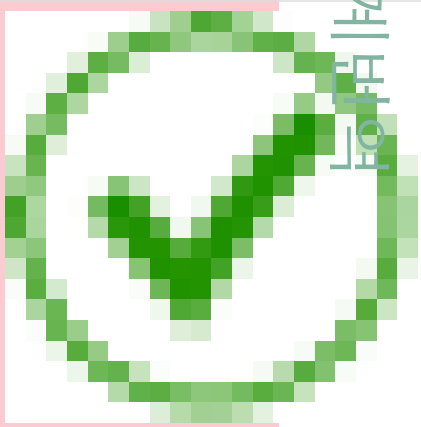
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
활성				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

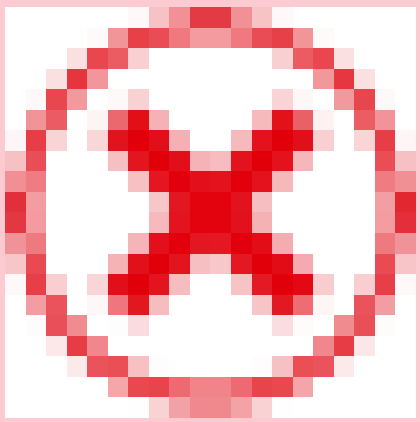
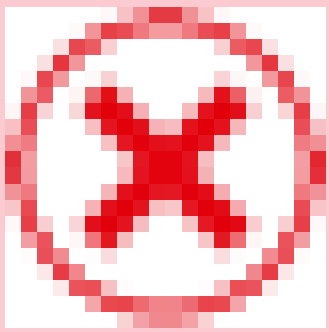
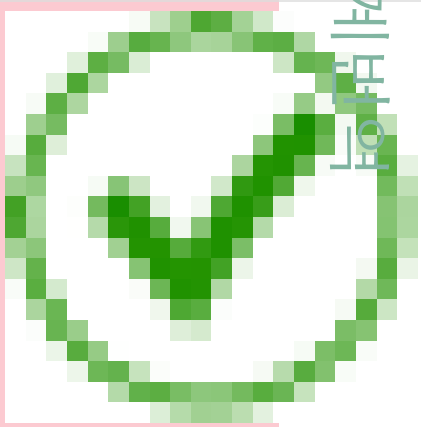
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
나에게 할당됨				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

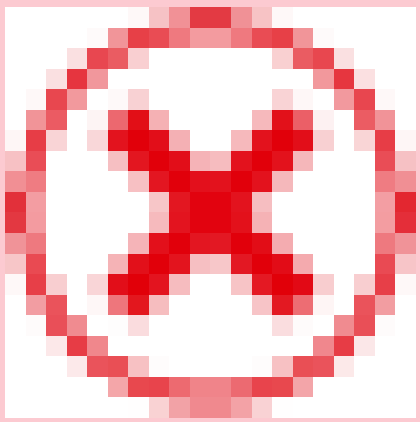
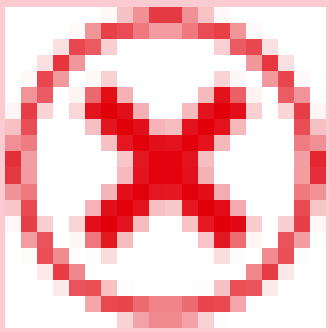
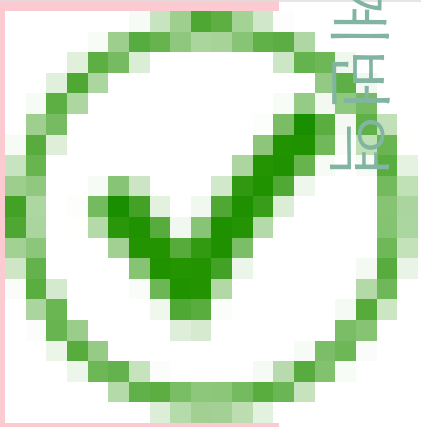
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
사용자 그룹에 할당됨				

PDF 버전

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

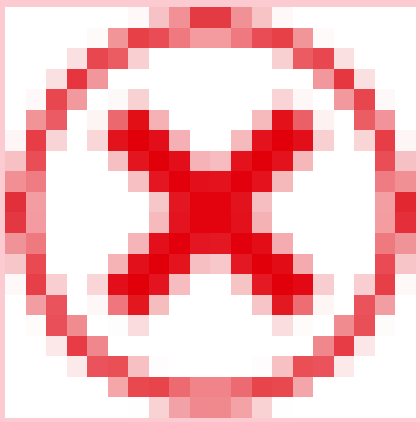
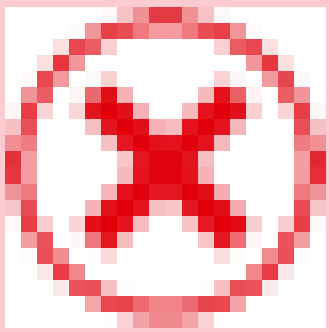
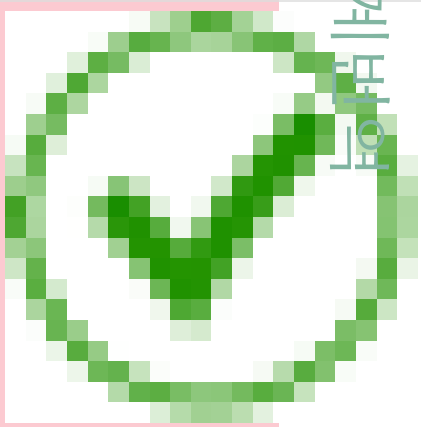
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
모두				
취약 항목				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

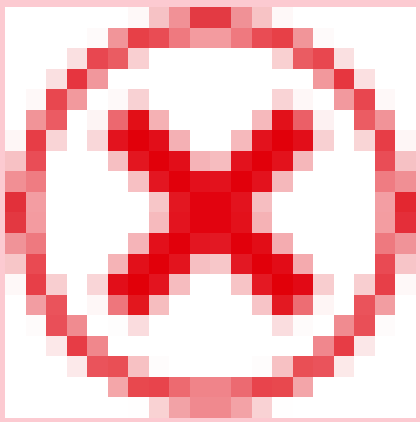
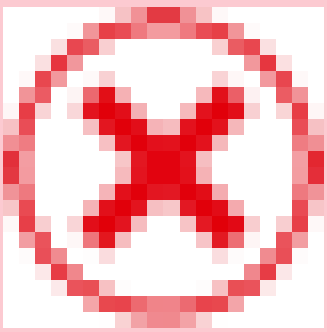
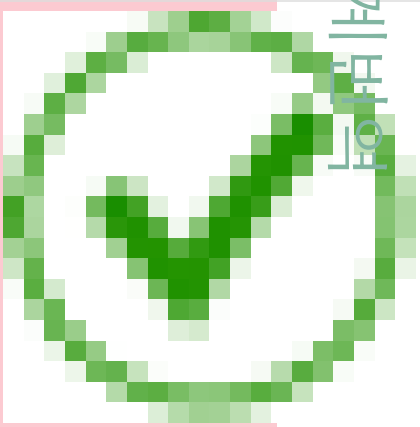
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
중요 위험				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

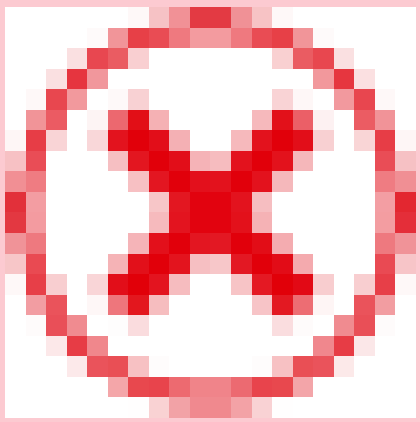
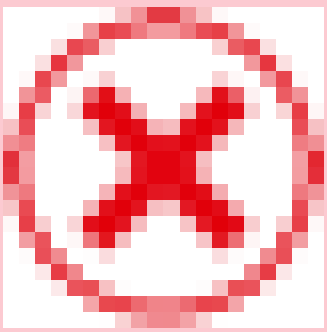
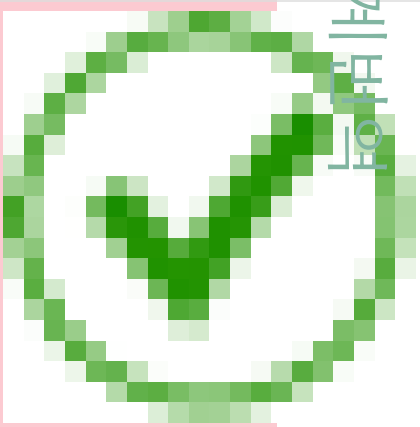
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
높은 위험				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

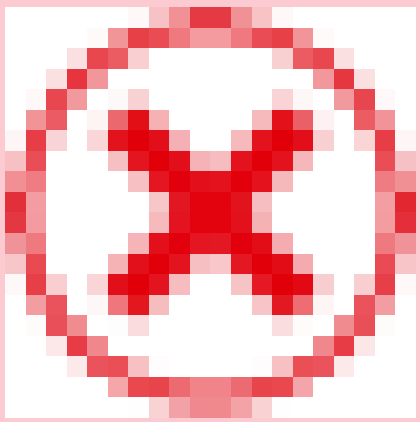
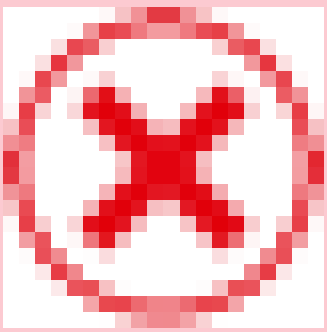
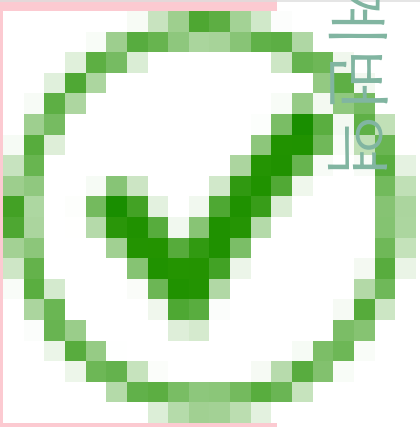
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
악용 가능				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

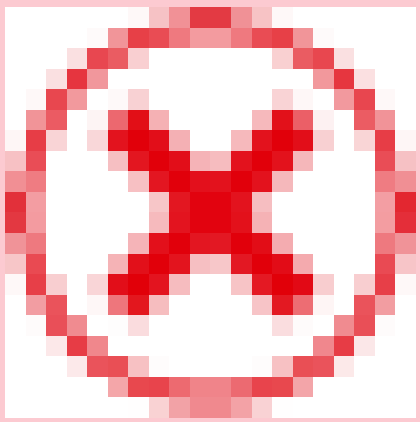
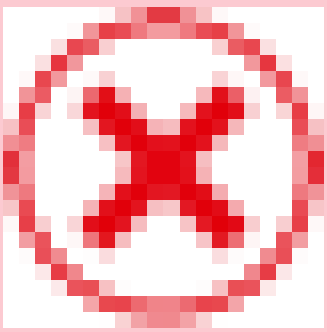
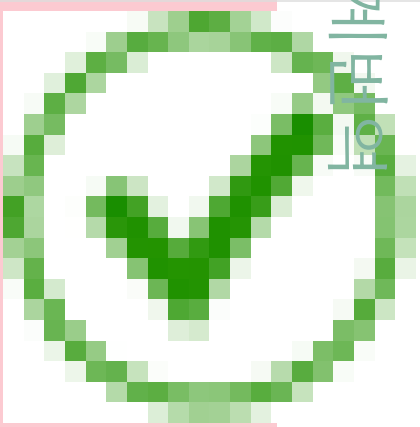
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
대상에 접근				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

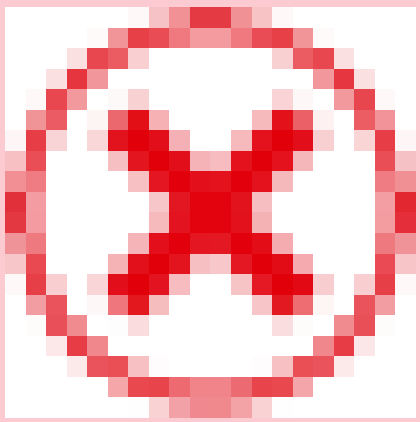
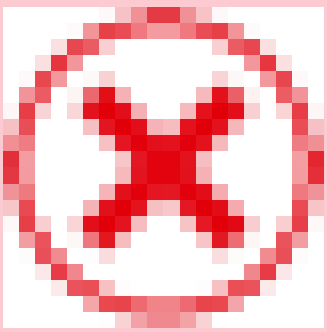
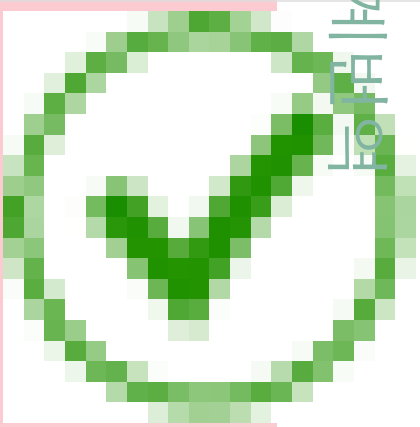
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
누락된 대상				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

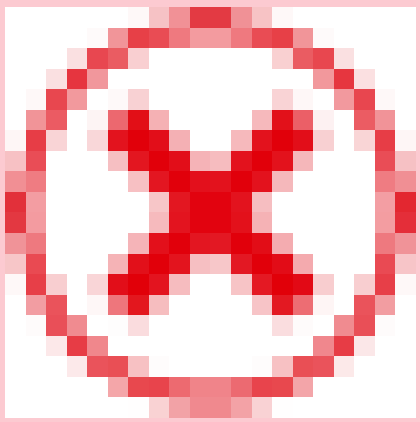
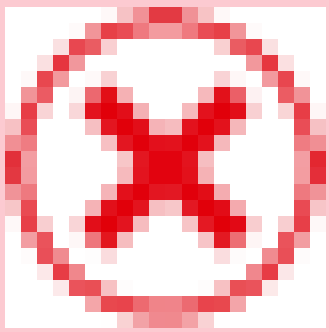
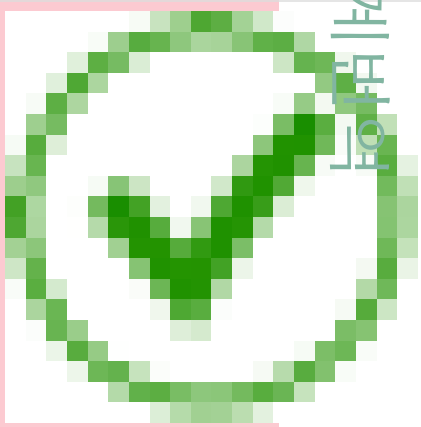
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
지난 90일 이내				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

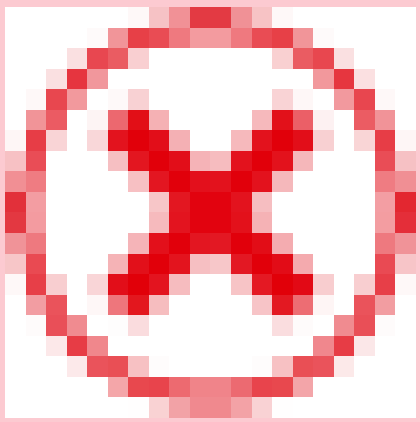
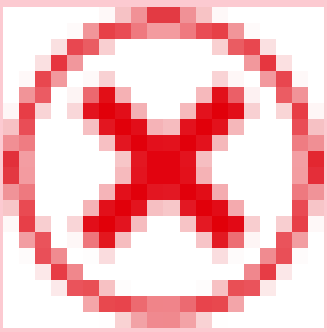
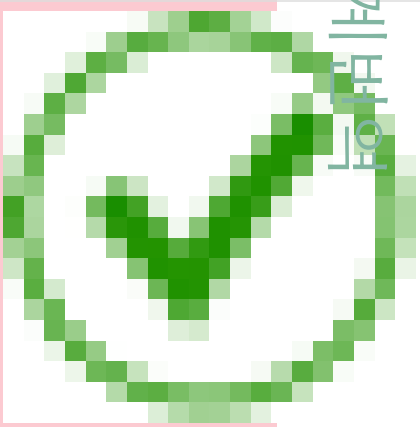
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
90일 경과				

고객 버전

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

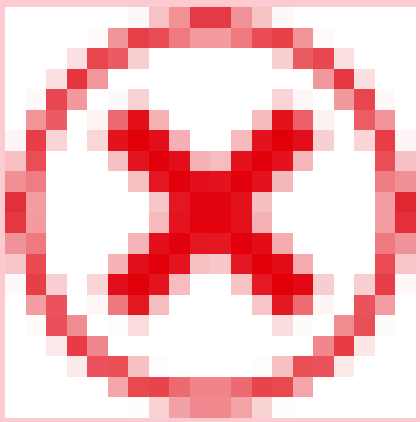
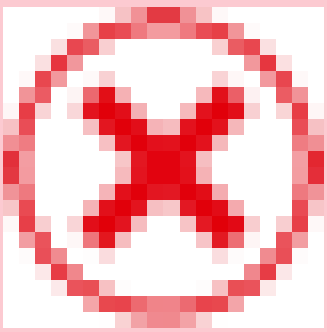
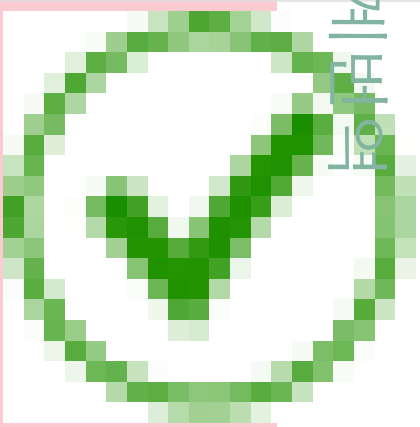
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
미할당				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

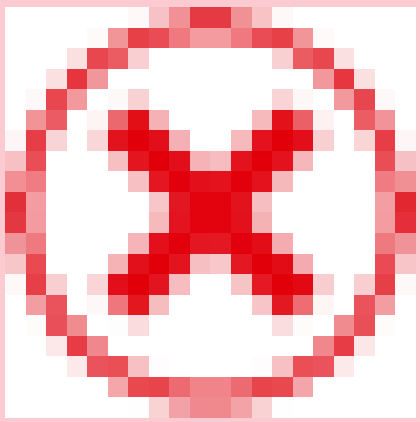
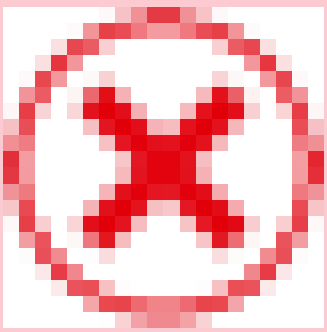
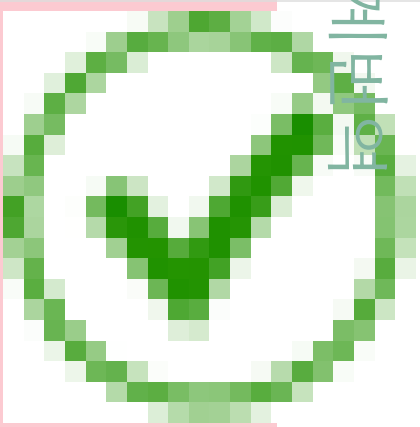
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
그룹 해제				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

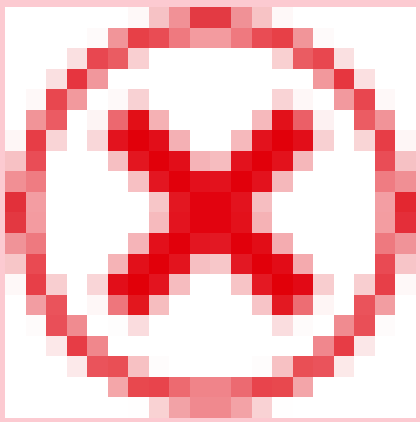
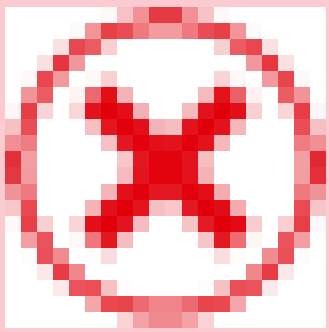
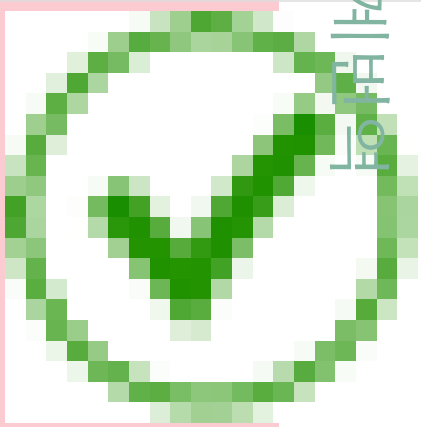
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
해제됨				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

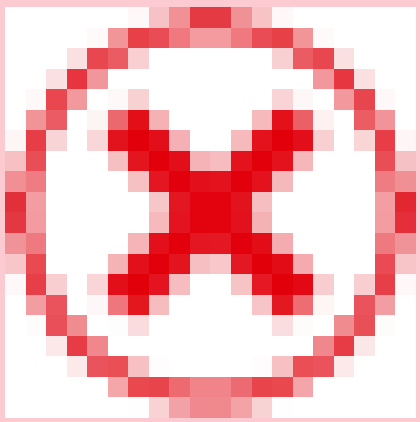
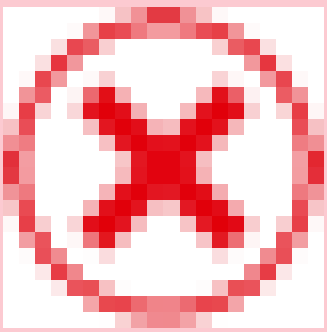
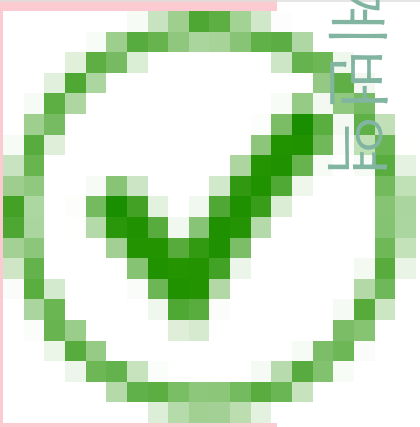
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
여러 지연				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

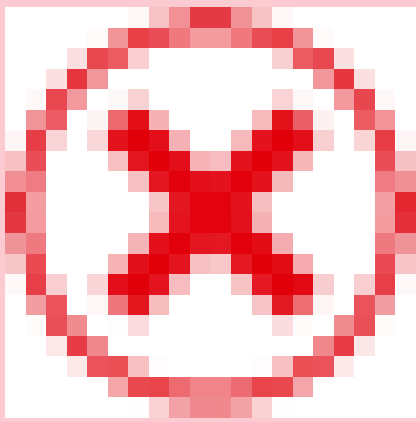
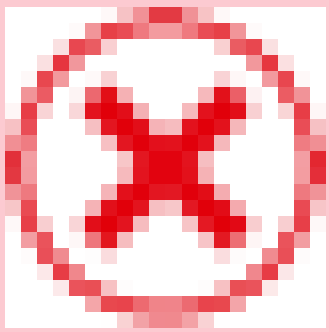
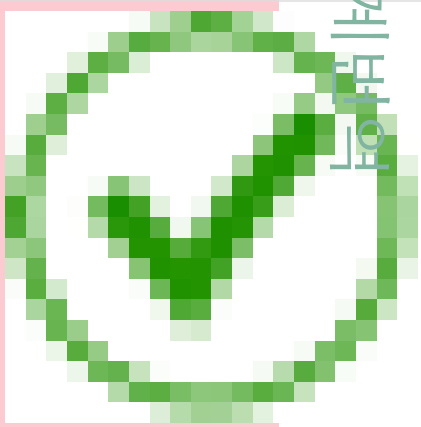
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
모두				
솔루션				

고객 버전

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

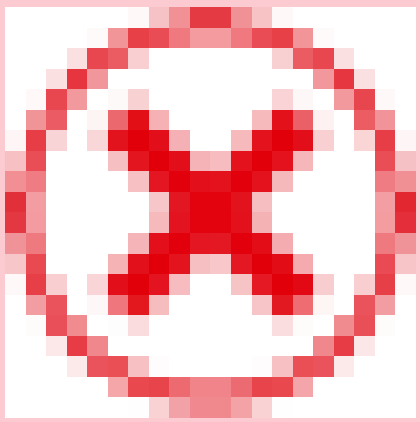
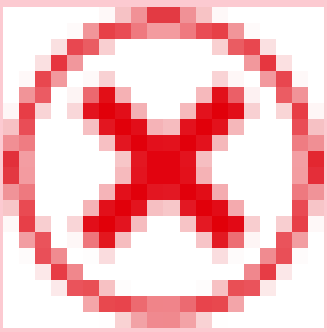
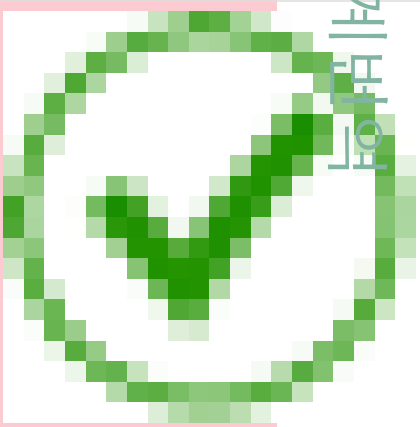
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
모두				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

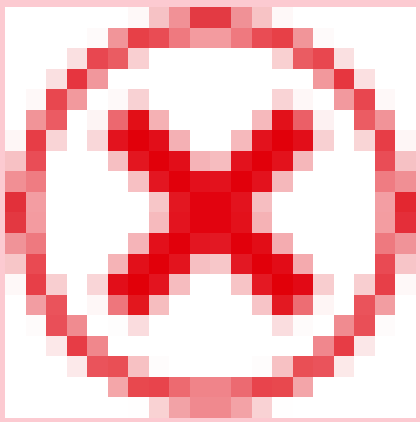
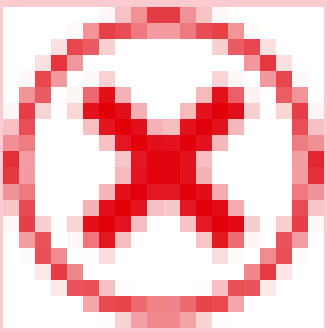
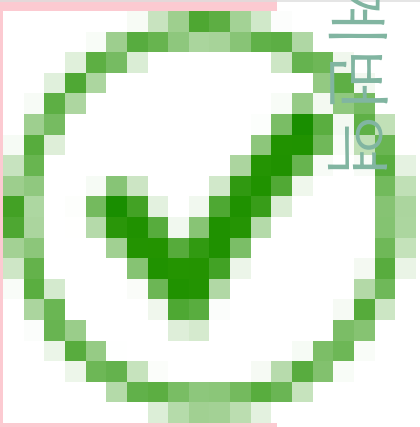
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
가장 높은 대체				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

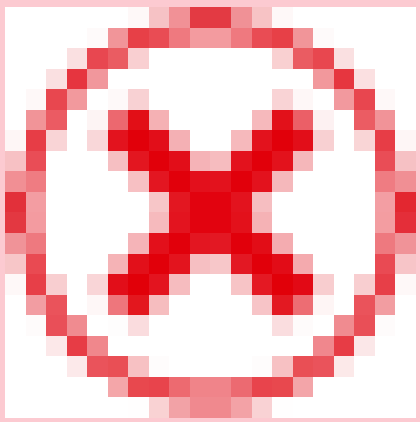
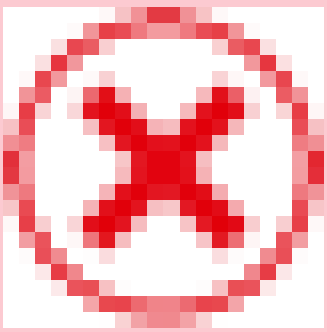
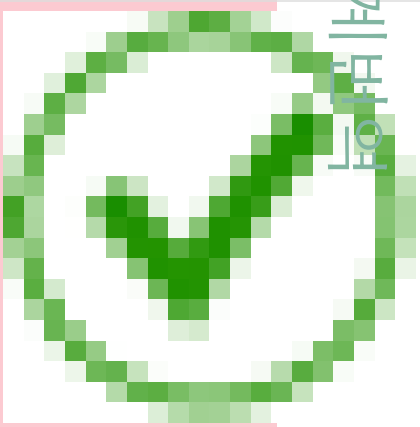
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
취약한 항목 포함				

라이브러리

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

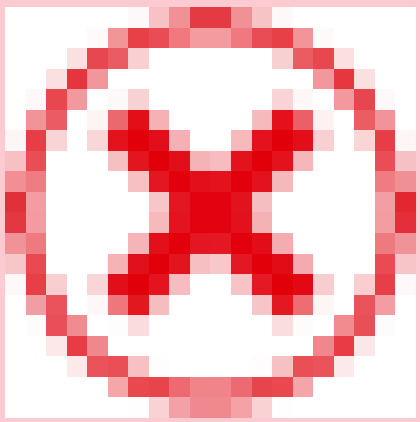
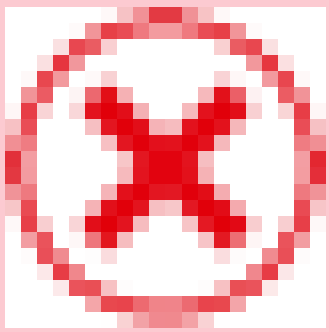
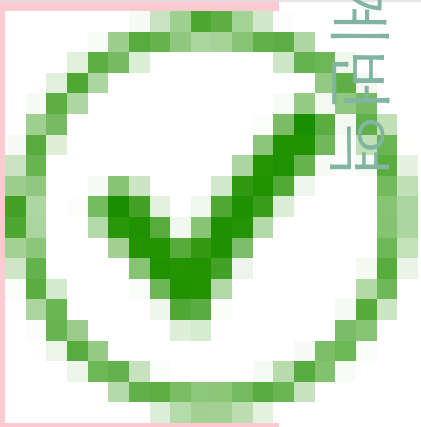
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
NVD				

고객 버전

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

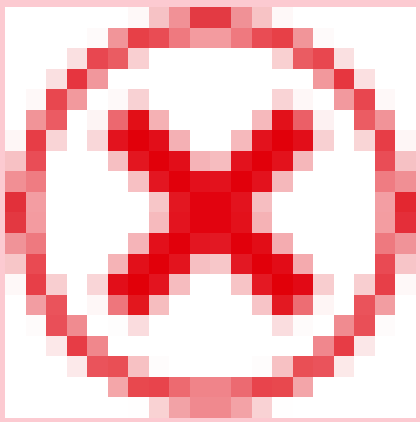
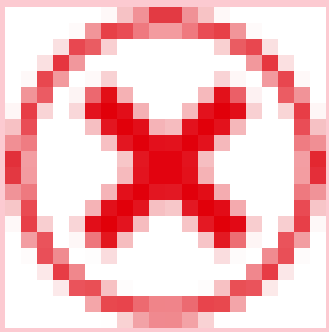
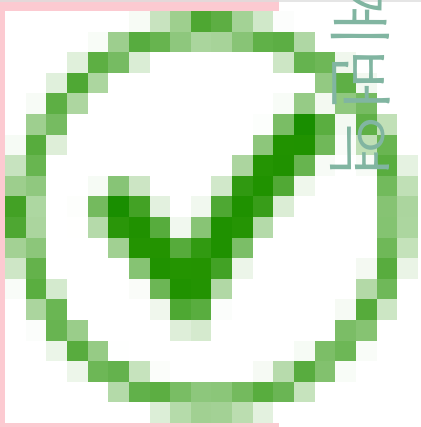
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
CWE				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

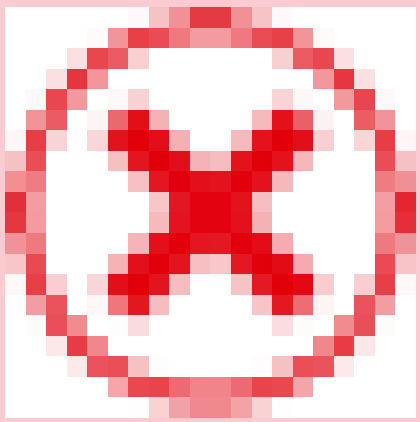
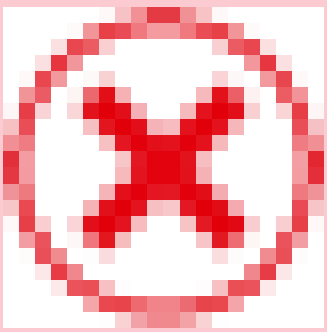
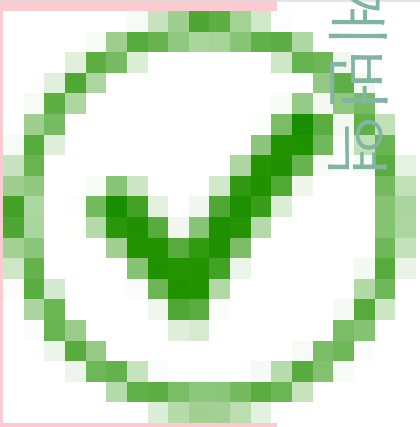
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
외부 공급업체				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

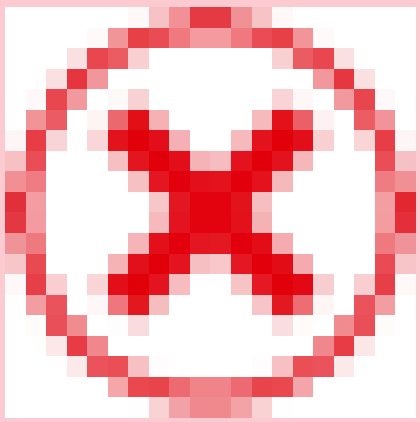
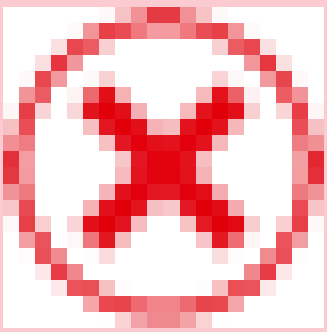
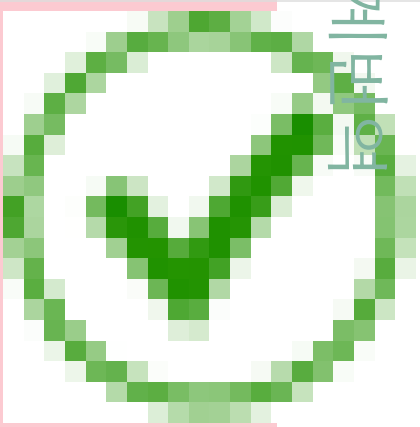
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
취약한 소프트웨어				
취약성 스캐닝				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

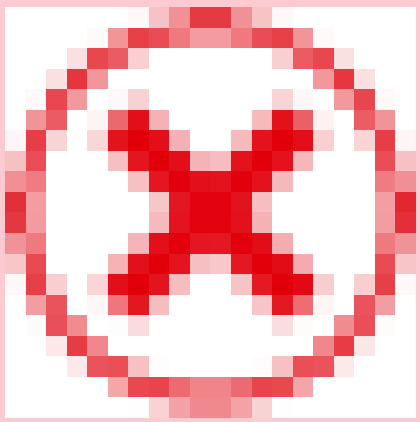
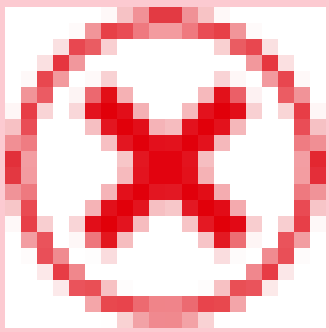
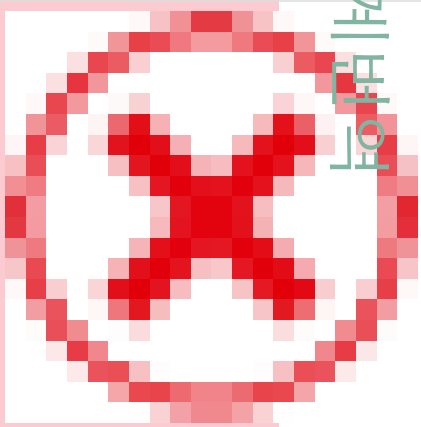
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
노출 평가				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

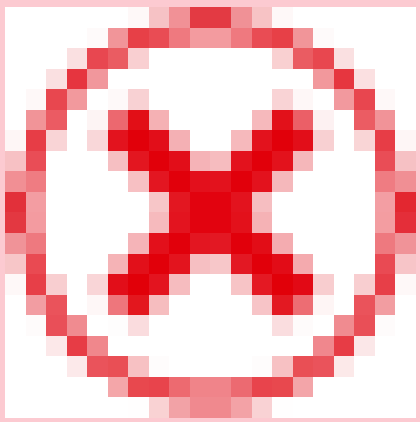
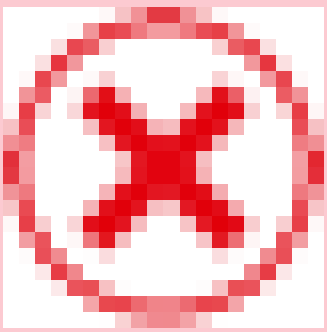
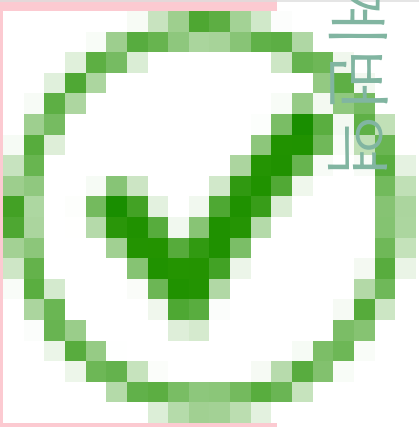
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
스캔				

고객 버전

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

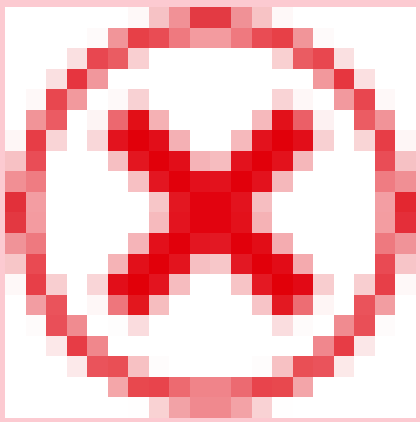
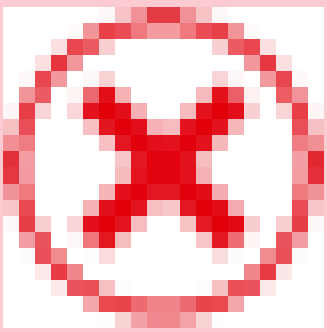
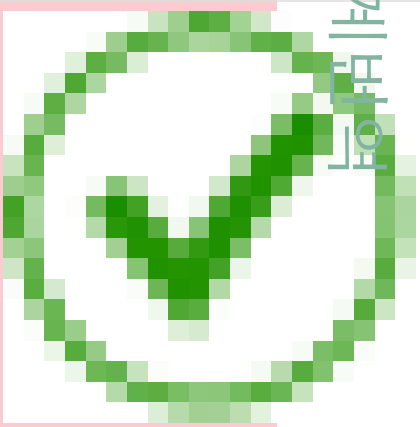
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
스캐너				

고객 버전

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

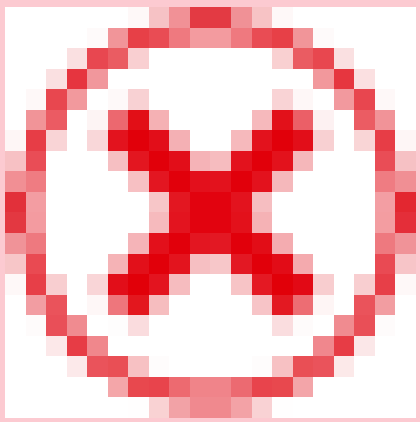
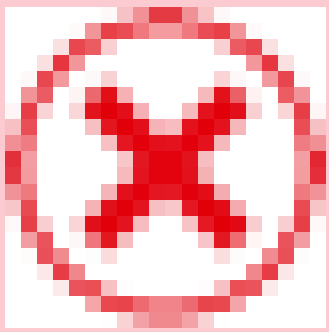
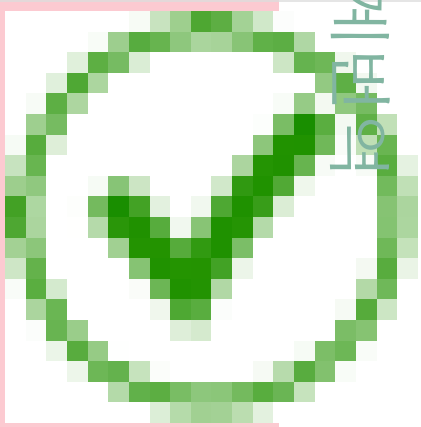
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
스캔 큐				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

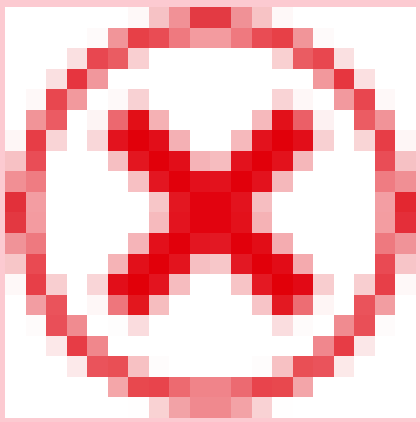
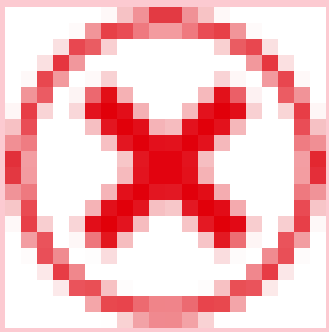
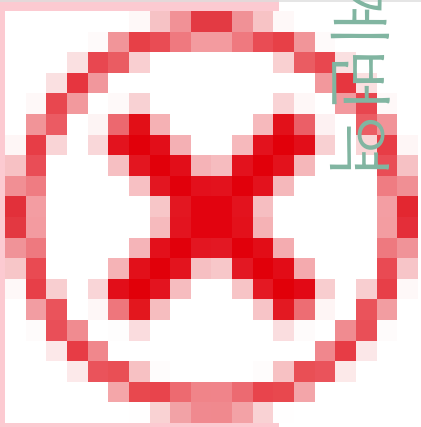
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
스캐너 속도 제한				

고객 버전

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
속도 제한 정의	✗	✗	✗	

관리

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
설정 도우미	✗	✗	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

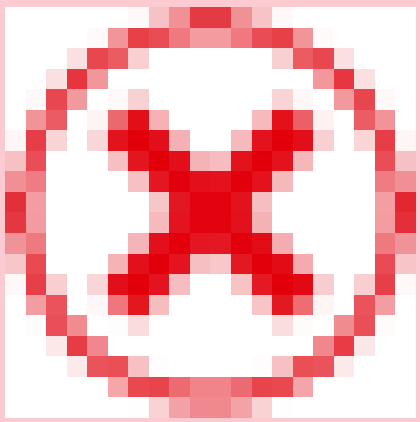
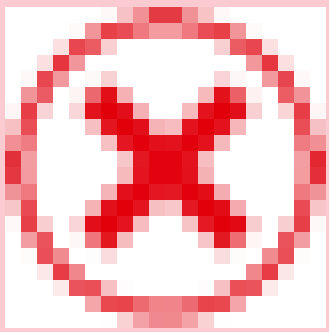
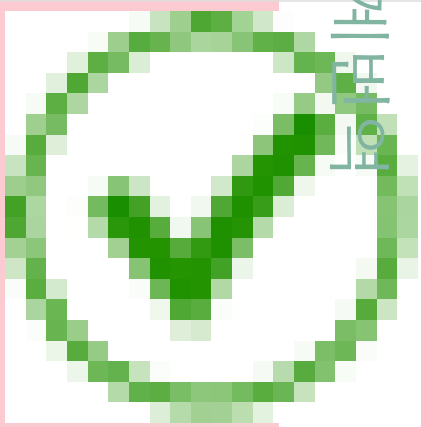
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
주시 주제				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

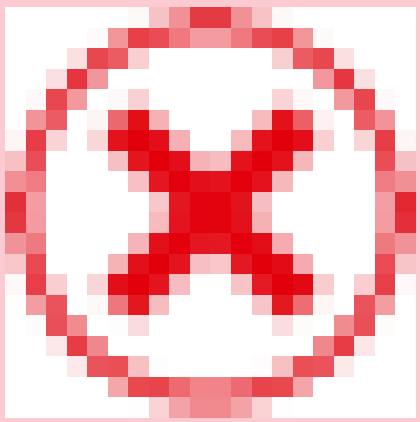
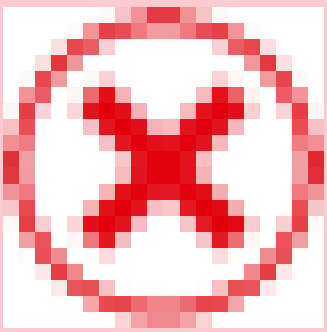
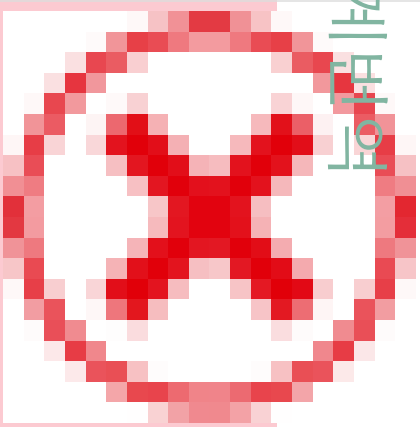
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
담당 규칙				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

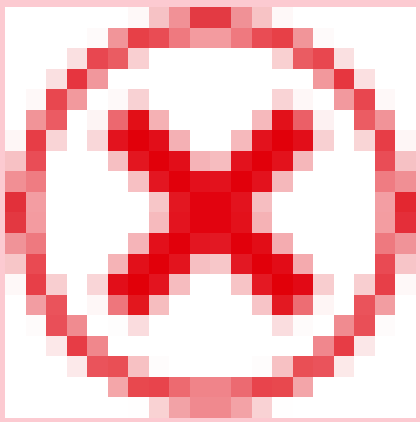
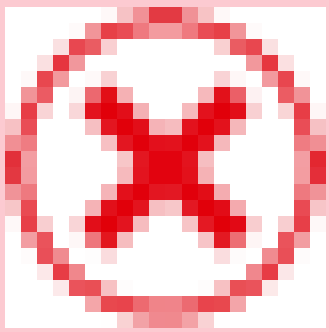
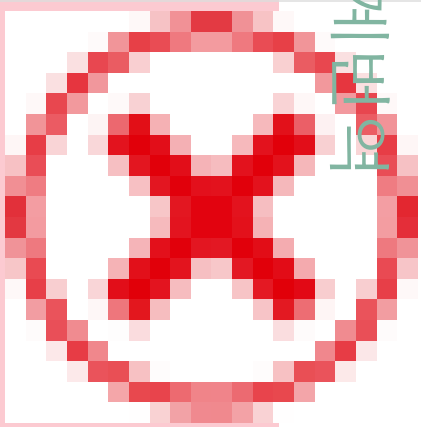
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
정정 작업 규칙				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

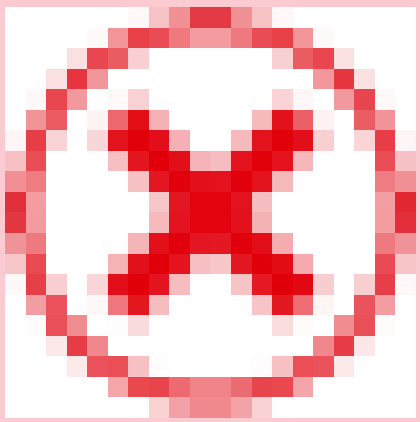
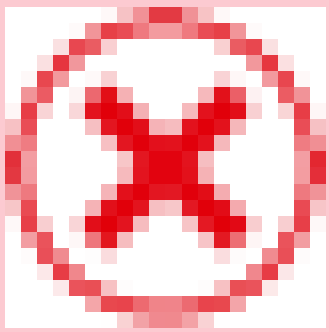
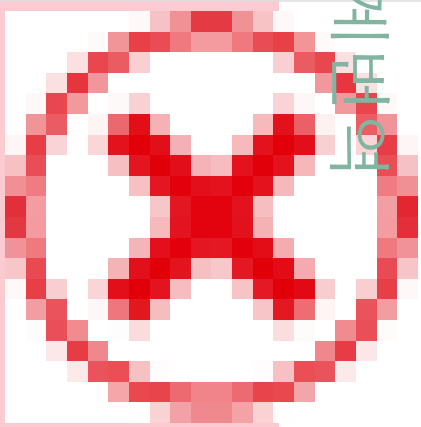
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
할당 권장 사항				

검토용

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

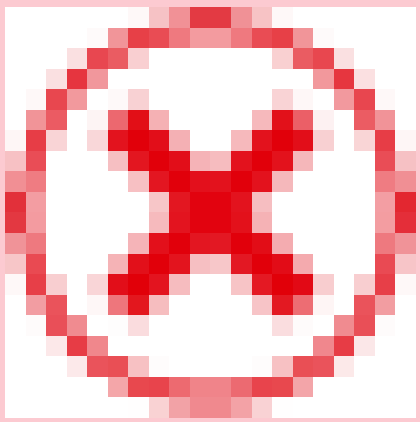
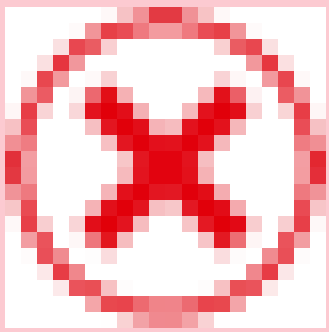
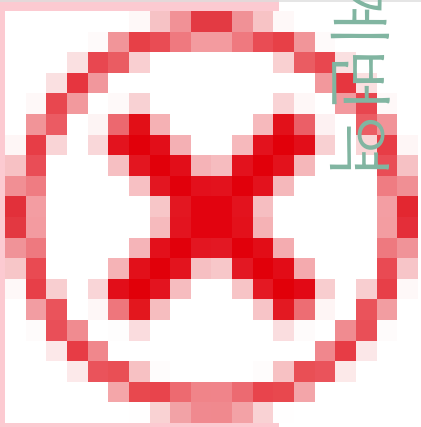
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
취약성 계산기				

기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

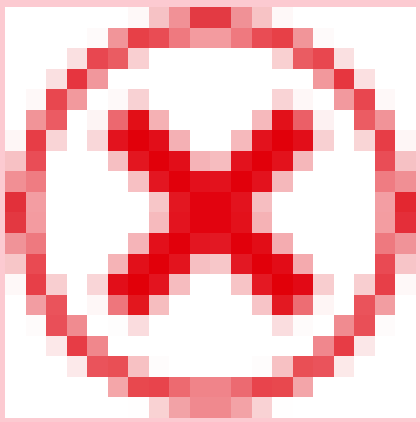
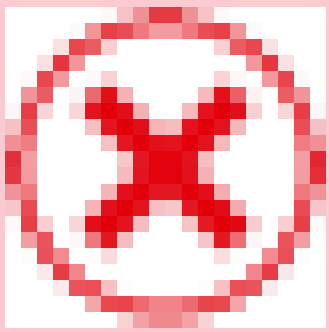
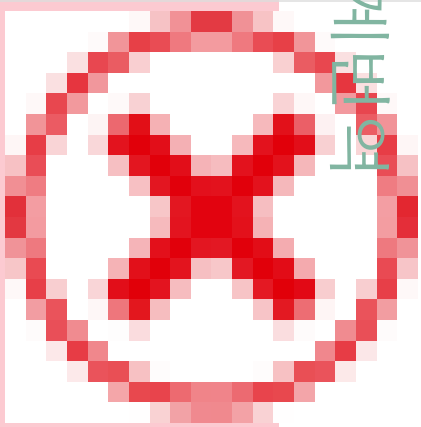
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
취약성 롤업 계산기				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

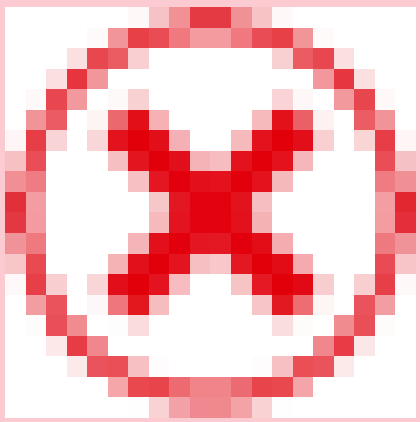
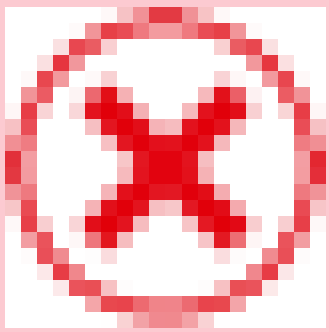
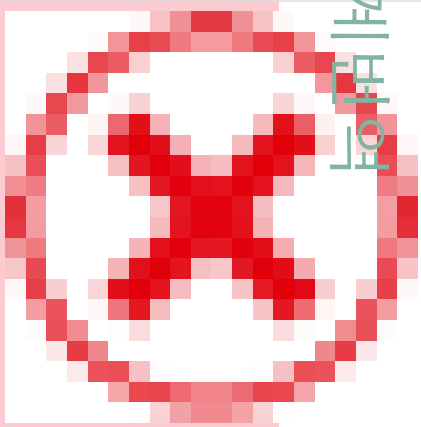
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
정정 대상 규칙				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

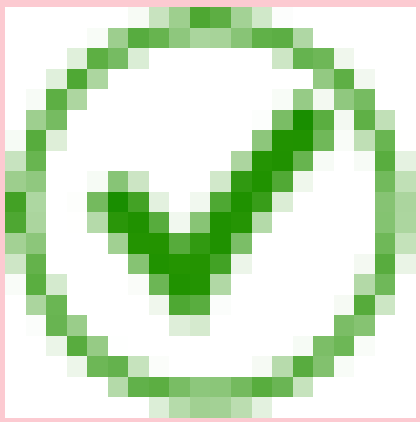
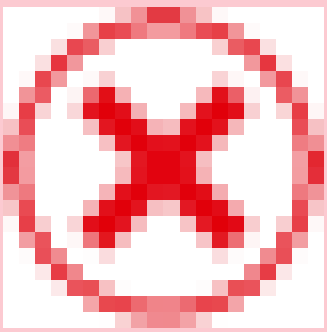
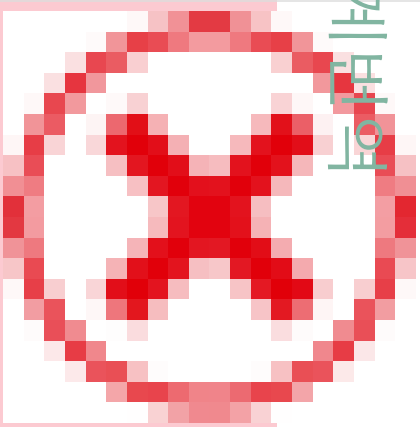
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
AutoClose 구성				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
자동 삭제 규칙	✗	✓	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

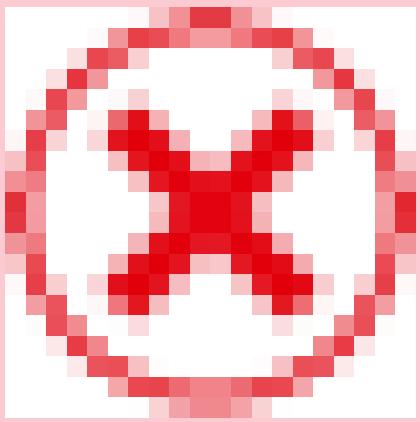
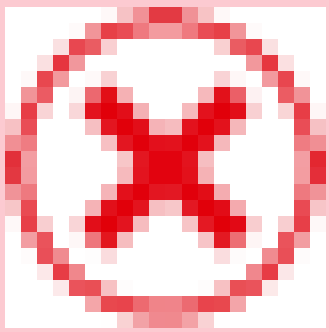
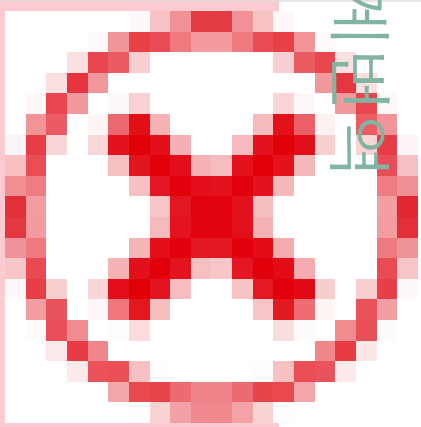
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
예외 규칙				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

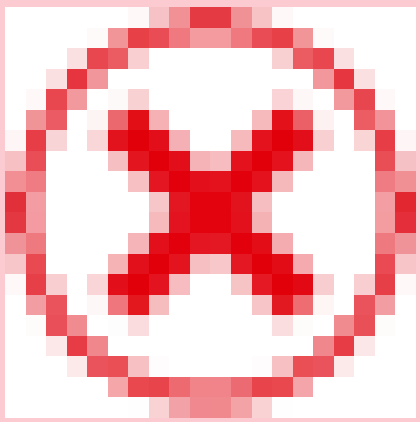
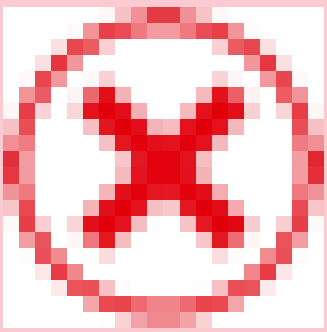
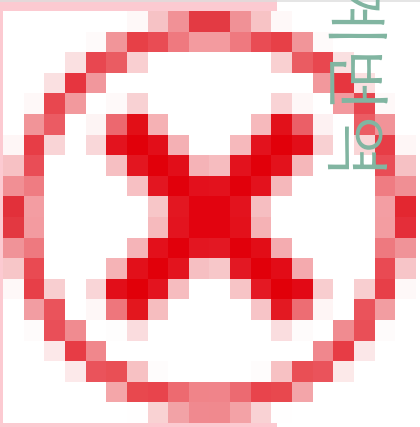
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
승인 규칙				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

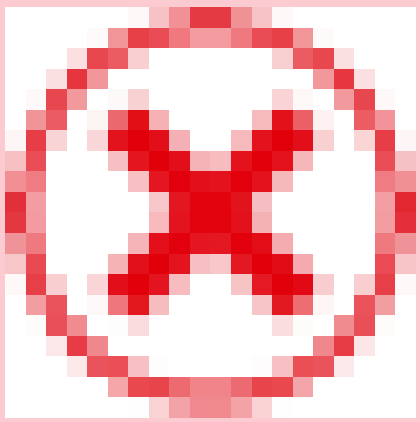
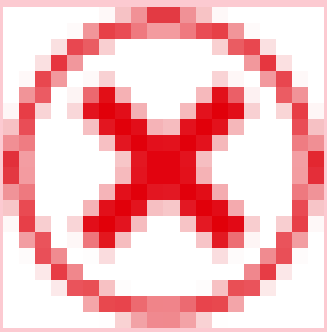
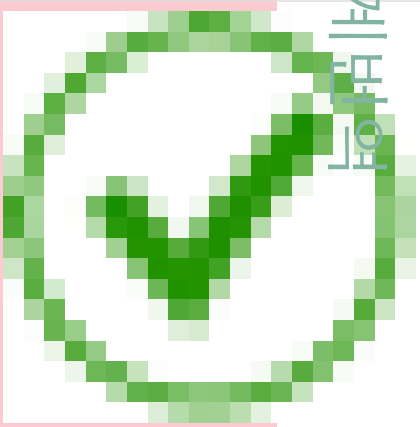
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
분류 규칙				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

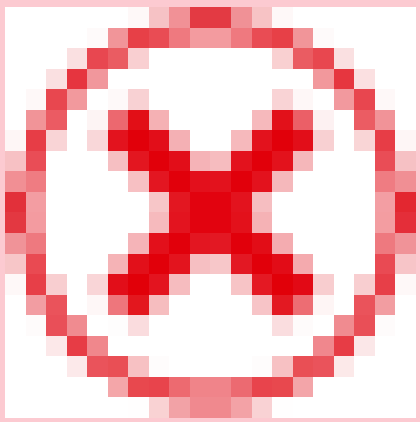
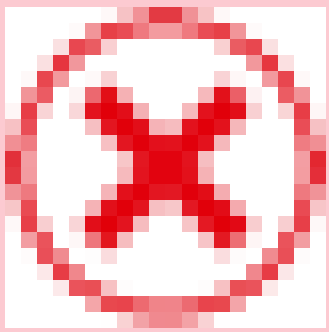
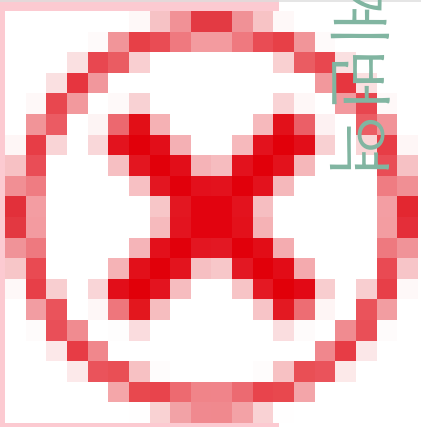
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
성과 구성				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

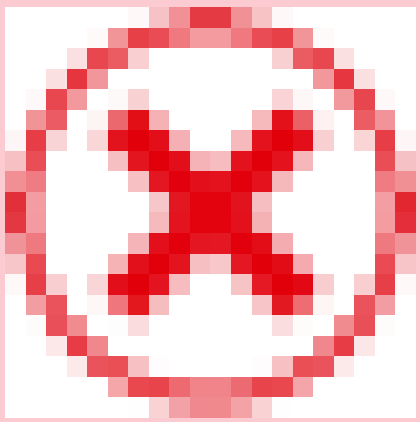
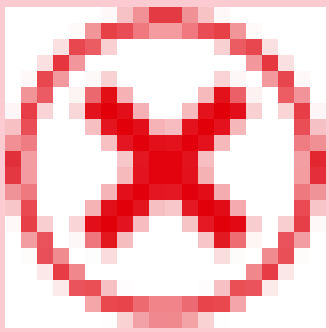
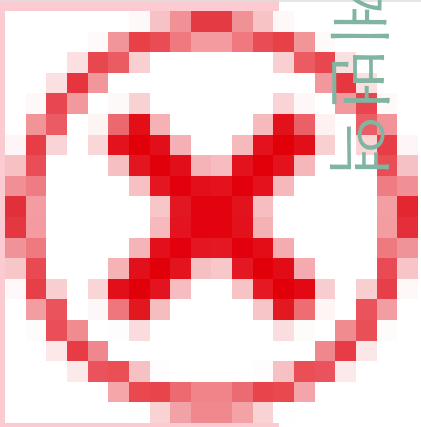
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
VI 세분성 구성				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

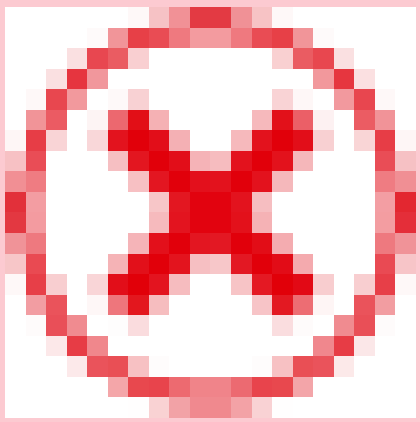
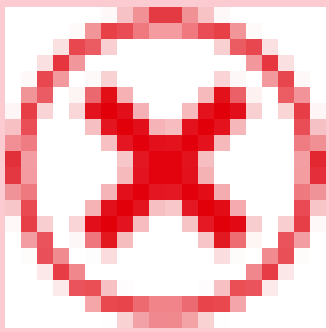
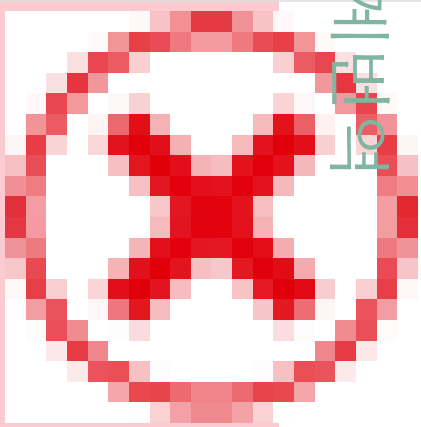
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
알림				

고객 버전

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

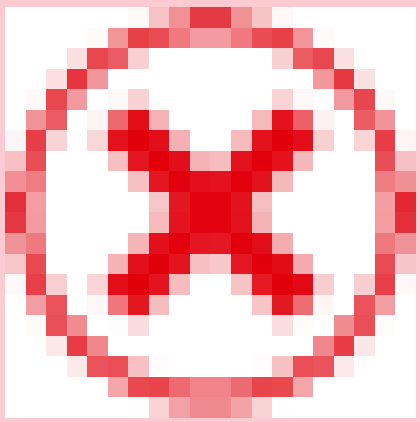
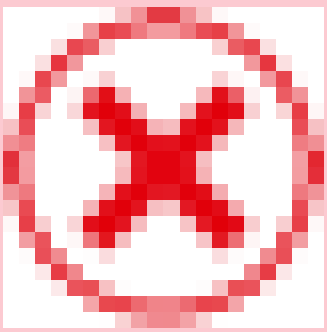
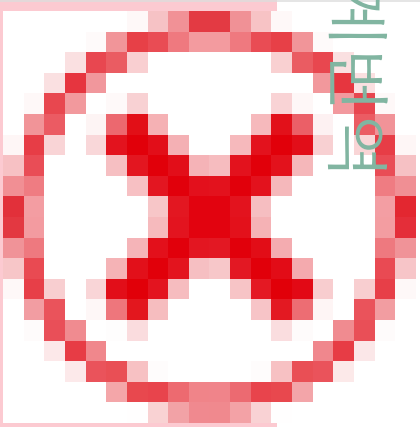
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
이메일 템플릿				

검토본

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

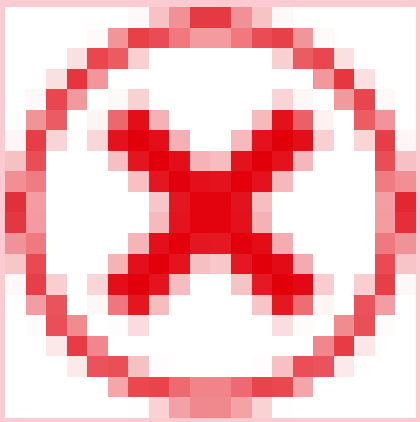
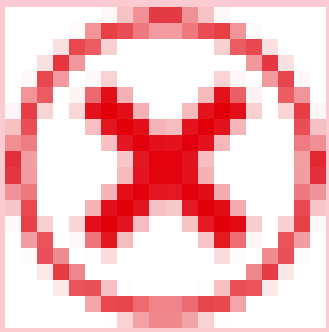
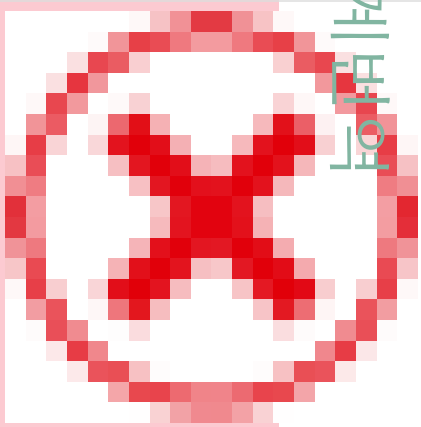
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
임포트 큐				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

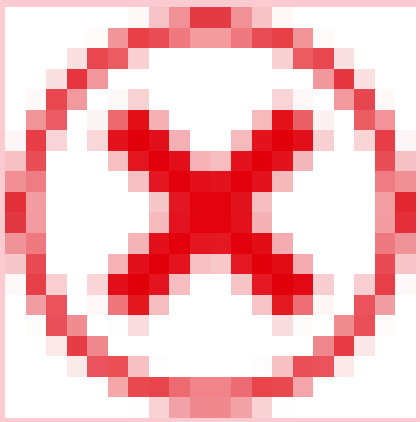
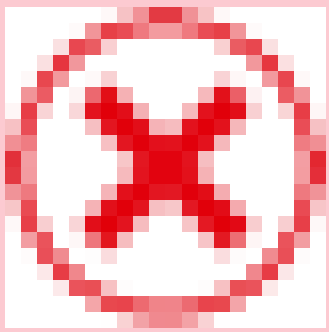
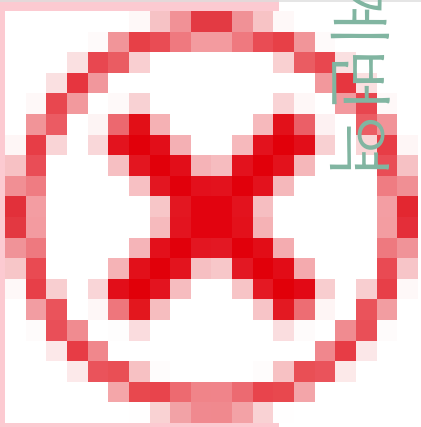
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
통합				

고객 버전

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

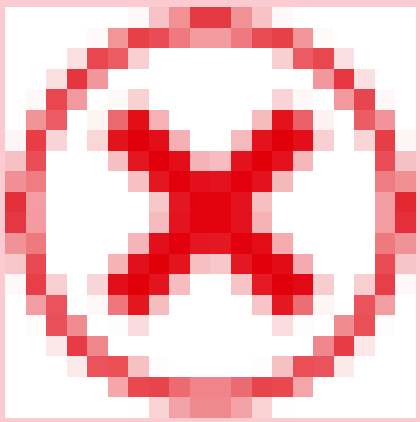
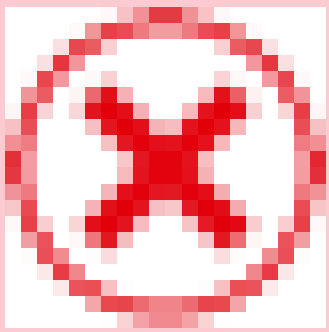
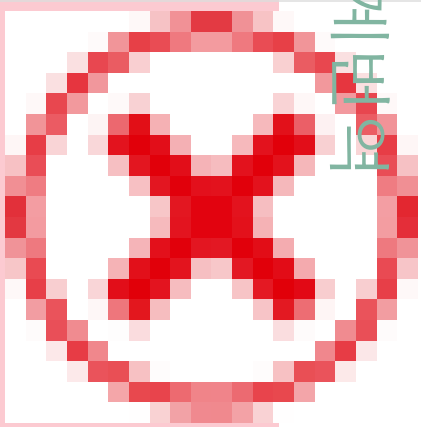
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
SLA 정의				

도움말 보기

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

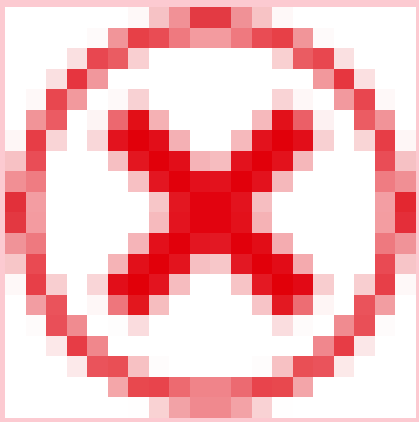
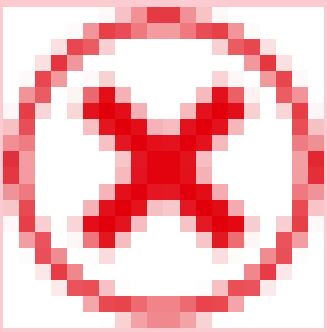
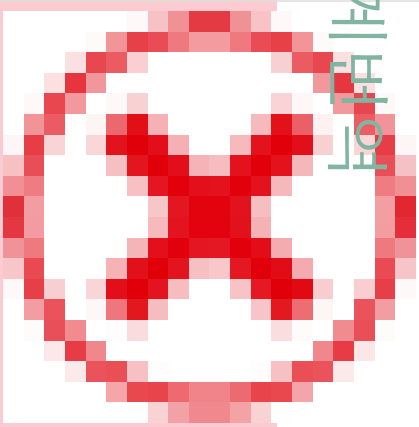
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
SAM NVD 구성				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

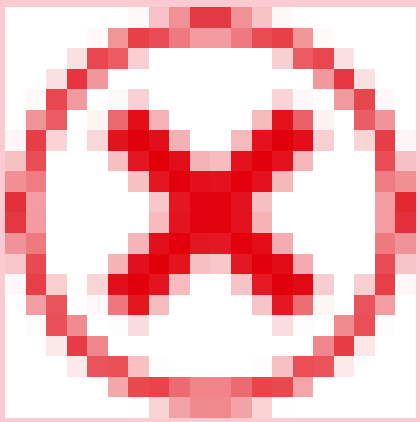
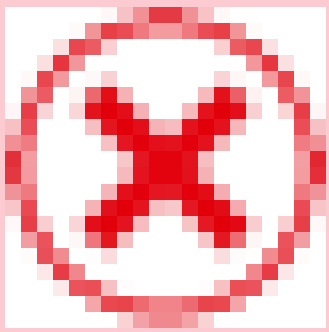
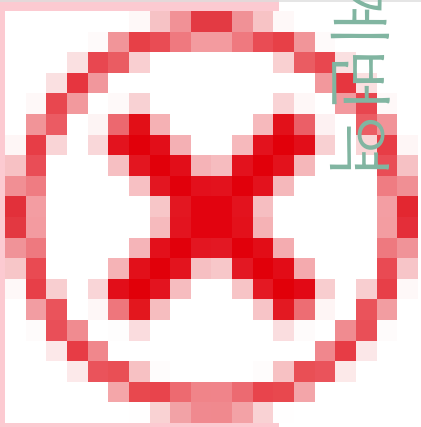
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
표준화된 심각성 맵				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

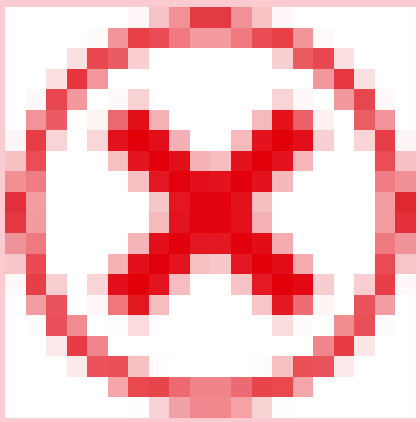
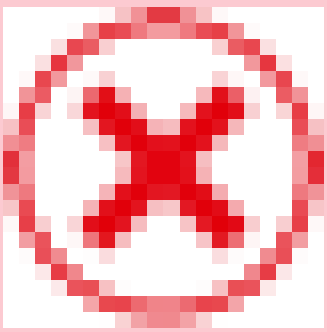
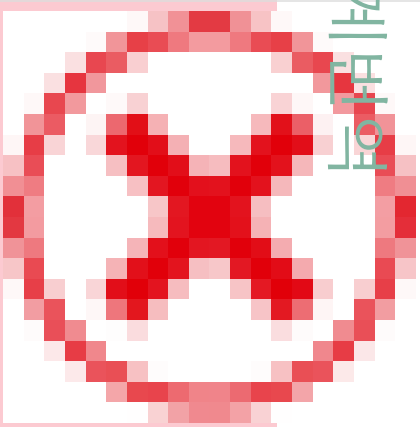
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
스캔 보장 범위 구성				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
예외 관리	✗	✗	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
사용량 보고서	✗	✗	✗	
진단				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

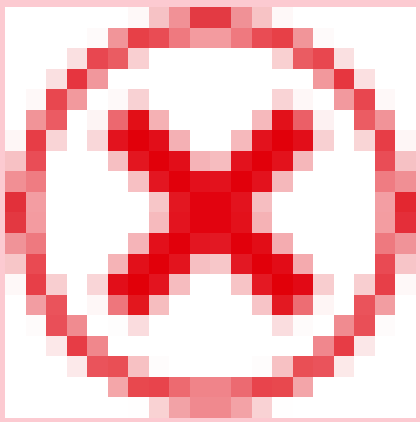
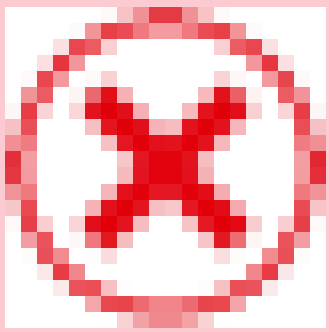
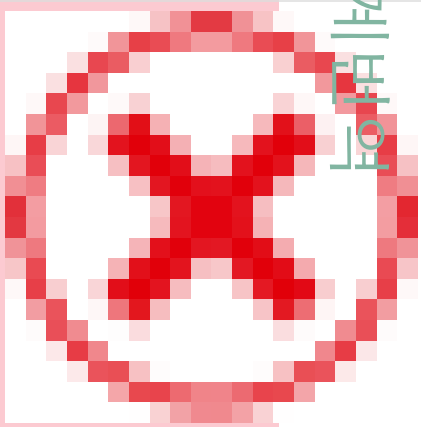
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules	sn_
검사				

피드백 보내기

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

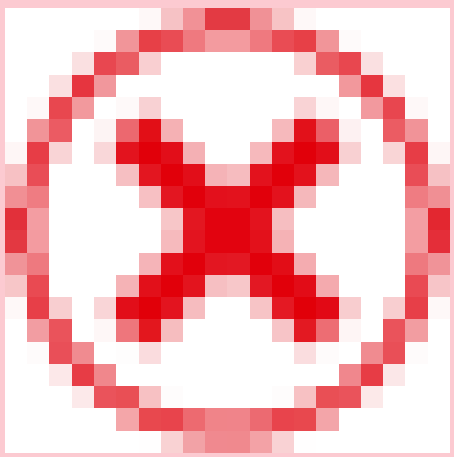
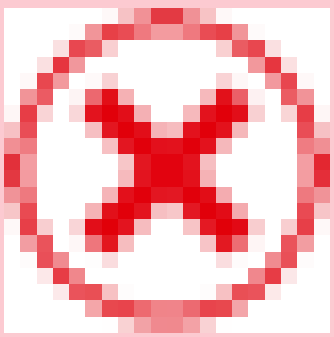
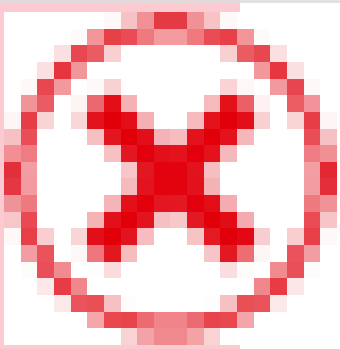
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
(메인 앱 그룹)				
CISO 대시보드				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
정정 개요	✗	✓	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
취약성 관리자 작업 공간	✗	✗	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
개요	✗	✓	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
IT 정정 작업 공간	✗	✗	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
승인자 개요	✗	✗	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
개요	✗	✓	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
내 승인	✗	✗	✗	
정정 작업				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
활성	✗	✓	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
나에게 할당됨	✗	✓	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
사용자 그룹에 할당됨	✗	✓	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
모두	✗	✓	✗	

취약 항목

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
중요 위험	✗	✓	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
높은 위험	✗	✓	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
악용 가능	✗	✓	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
대상에 접근	✗	✓	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
누락된 대상	✗	✓	✗	

기술 문서

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
지난 90일 이내	✗	✓	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
90일 경과	✗	✓	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
미할당	✗	✓	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
그룹 해제	✗	✓	✗	

기술 문서

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
해제됨	✗	✓	✗	

기술 문서

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
여러 지연	✗	✓	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
모두	✗	✓	✗	
솔루션				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
모두	✗	✓	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
가장 높은 대체	✗	✓	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
취약한 항목 포함	✗	✓	✗	

라이브러리

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
NVD	✗	✓	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
CWE	✗	✓	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
외부 공급업체	✗	✓	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
취약한 소프트웨어	✗	✓	✗	
취약성 스캐닝				

기술 문서

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
노출 평가	✓	✗	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
스캔	✗	✓	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
스캐너	✗	✓	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
스캔 큐	✗	✓	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
스캐너 속도 제한	✗	✗	✗	

기술 문서

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
속도 제한 정의	✗	✗	✗	
관리				

기술 문서

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
설정 도우미	✗	✗	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
주시 주제	✗	✓	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
담당 규칙				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
정정 작업 규칙	✗	✓	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
할당 권장 사항	✗	✗	✗	

기술 문서

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
취약성 계산기	✗	✗	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
취약성 롤업 계산기	✗	✗	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
정정 대상 규칙	✗	✗	✗	

기술 문서

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
AutoClose 구성	✗	✗	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
자동 삭제 규칙	✗	✗	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
예외 규칙	✗	✗	✗	

기술 문서

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
승인 규칙	✗	✗	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
분류 규칙	✗	✗	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
성과 구성	✗	✗	✗	

기술 문서

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
VI 세분성 구성	✗	✗	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
알림	✗	✗	✓	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
이메일 템플릿	✗	✗	✓	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
임포트 큐				

기술 문서

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
통합	✗	✗	✗	

기술 문서

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
SLA 정의	✗	✗	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
SAM NVD 구성	✗	✗	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
표준화된 심각성 맵	✗	✗	✗	

기술 문서

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
스캔 보장 범위 구성	✗	✗	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
예외 관리	✗	✗	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
사용량 보고서	✗	✗	✗	
진단				

기술 문서

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_vul
검사	✗	✗	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

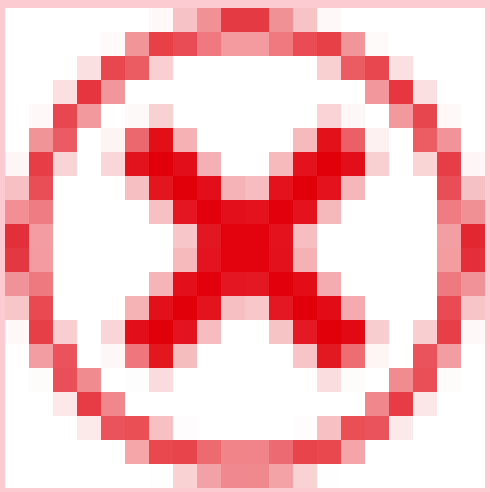
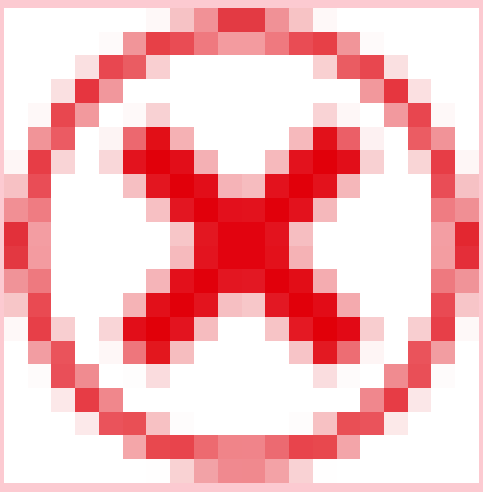
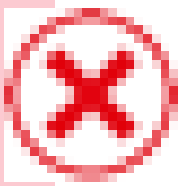
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
(메인 앱 그룹)				
CISO 대시보드				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

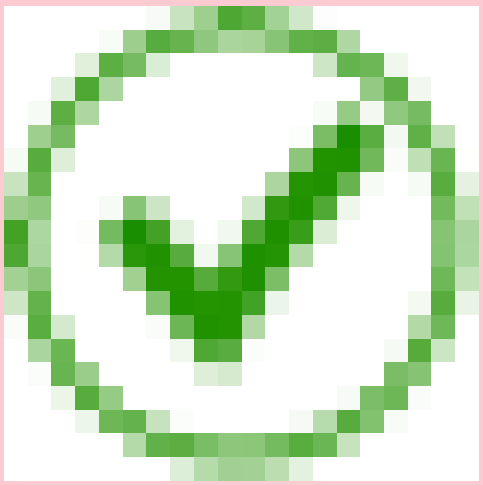
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
정정 개요				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

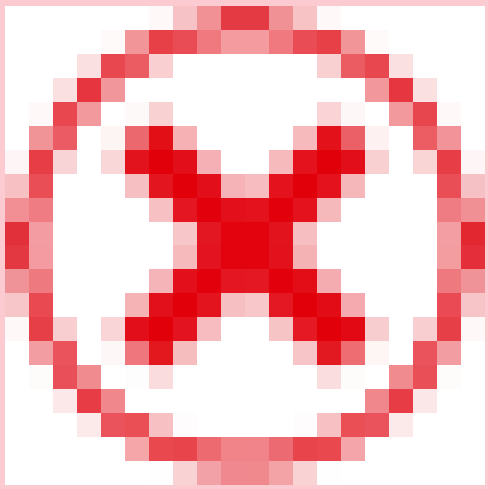
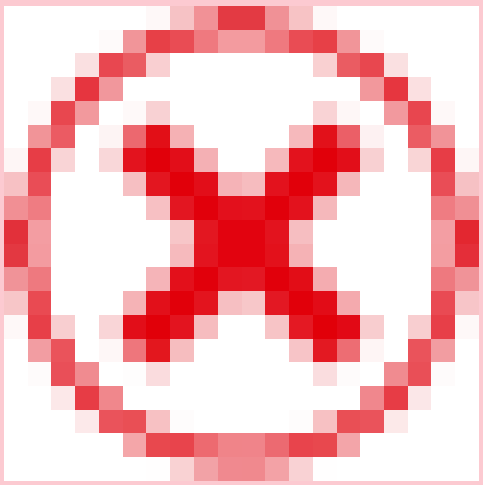
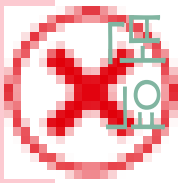
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
취약성 관리자 작업 공간				

기계 번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
개요	✓	✓	✓	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

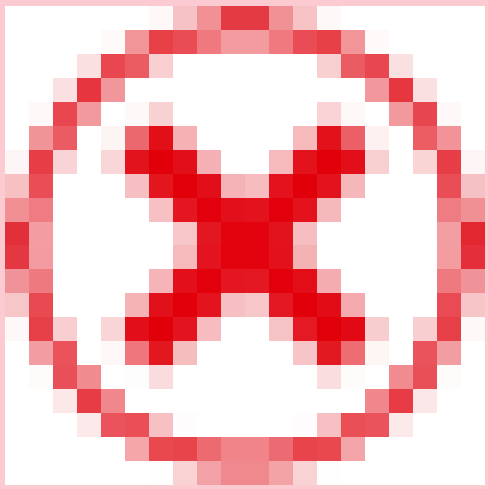
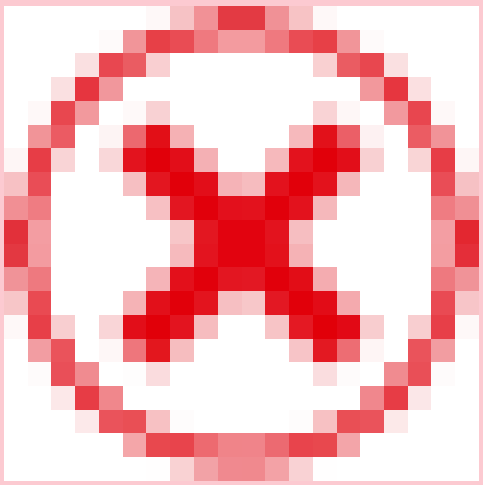
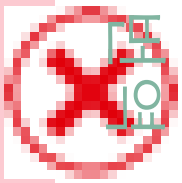
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
IT 정정 작업 공간				

기계 번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
승인자 개요	✗	✗	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
개요	✓	✓	✓	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

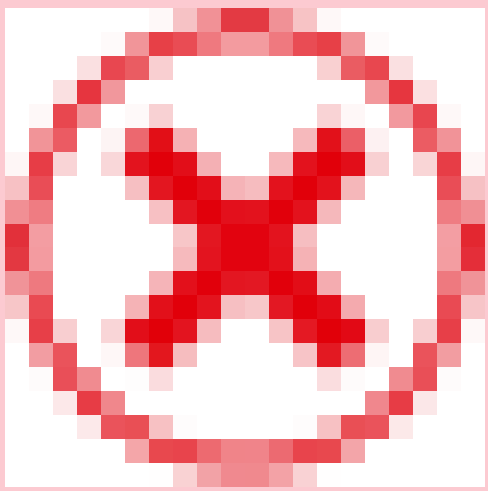
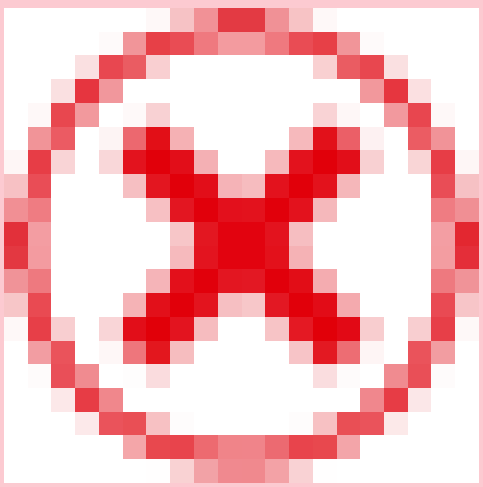
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
내 승인				
정정 작업				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
활성	✓	✓	✓	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

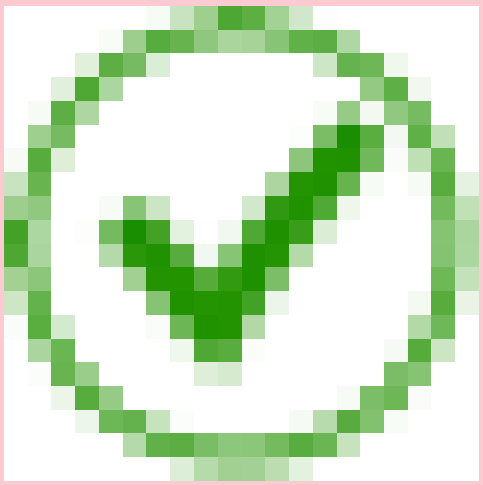
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
나에게 할당됨				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

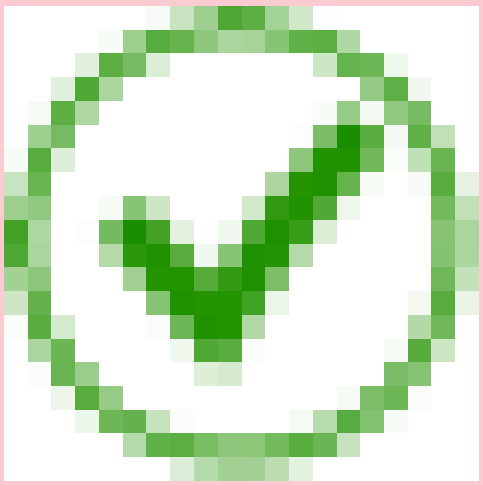
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
사용자 그룹에 할당됨				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
모두	✓	✓	✓	
취약 항목				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
중요 위험	✓	✓	✓	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
높은 위험	✓	✓	✓	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

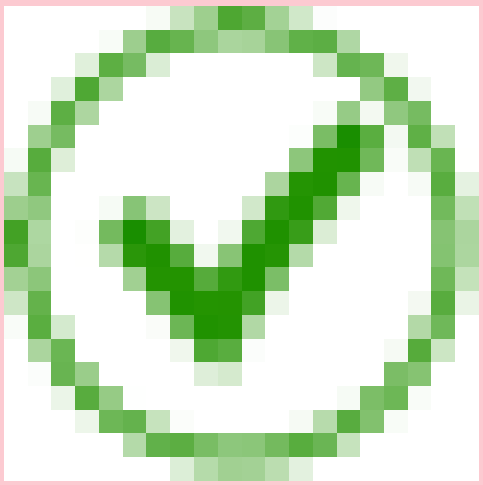
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
악용 가능				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
대상에 접근	✓	✓	✓	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

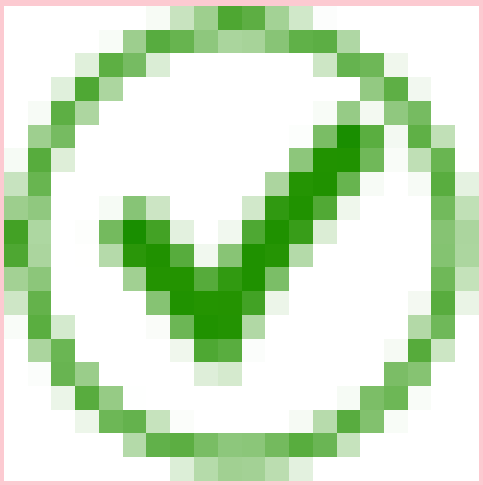
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
누락된 대상				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

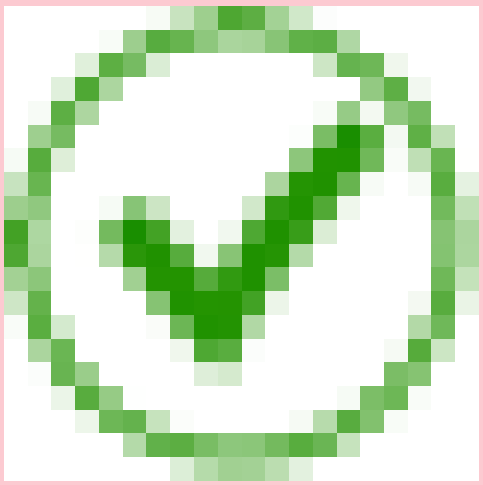
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
지난 90일 이내				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

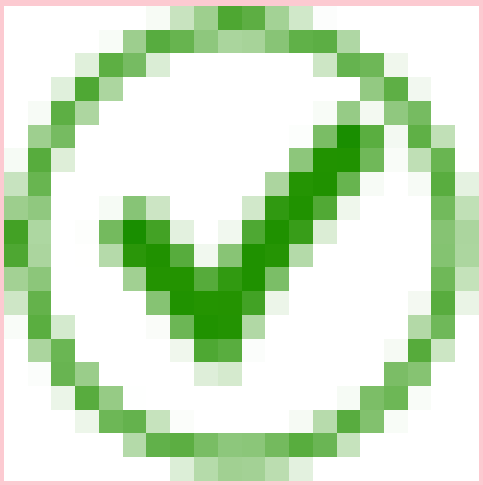
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
90일 경과				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
미할당	✓	✓	✓	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
그룹 해제	✓	✓	✓	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
해제됨	✓	✓	✓	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
여러 지연	✓	✓	✓	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
모두	✓	✓	✓	
솔루션				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

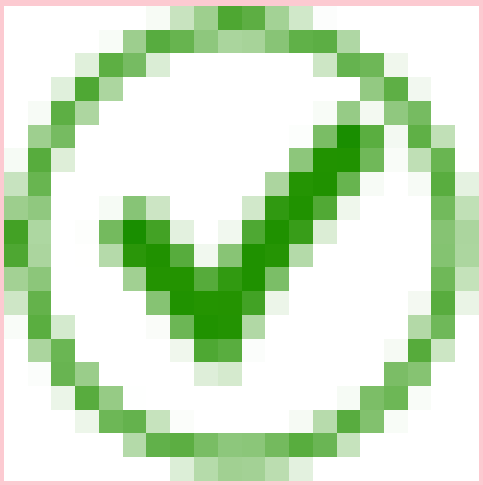
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
모두				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
가장 높은 대체	✓	✓	✓	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

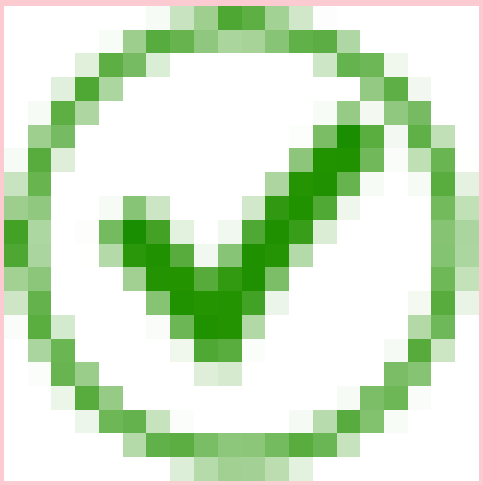
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
취약한 항목 포함				

라이브러리

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
NVD	✓	✓	✓	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
CWE	✓	✓	✓	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
외부 공급업체	✓	✓	✓	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

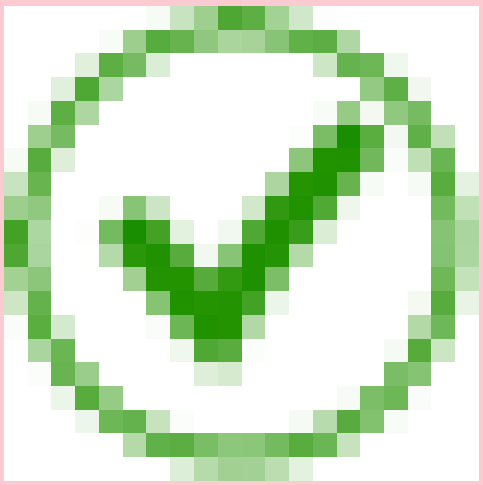
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
취약한 소프트웨어				
취약성 스캐닝				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
노출 평가	✗	✗	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

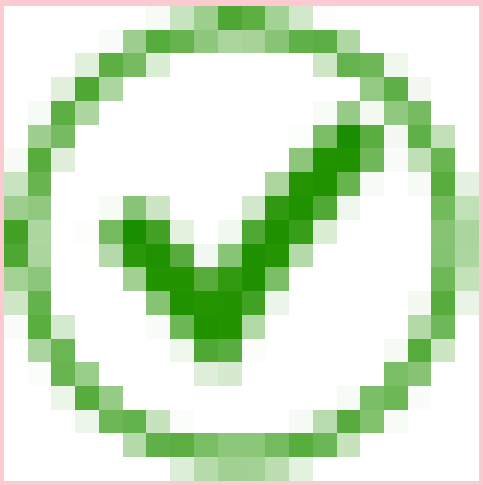
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
스캔				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
스캐너	✓	✓	✓	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
스캔 큐	✓	✓	✓	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

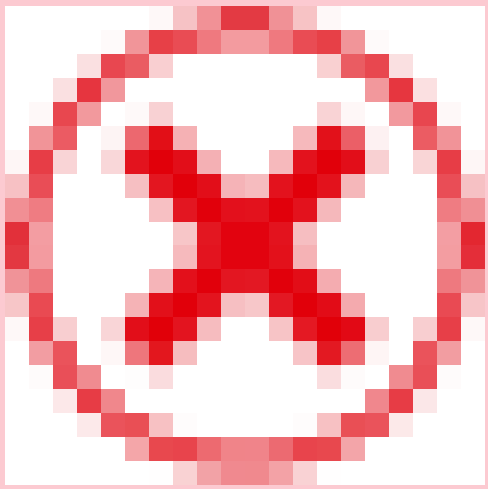
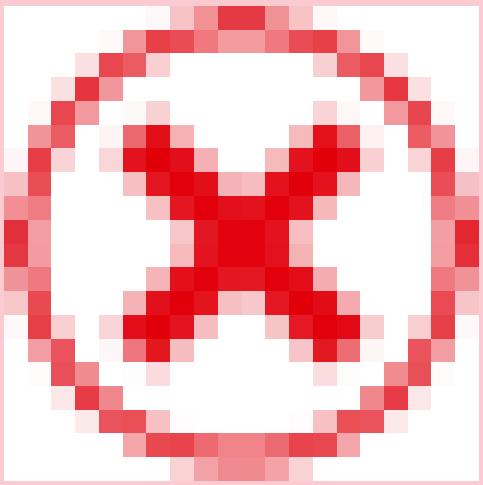
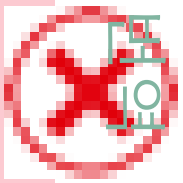
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
스캐너 속도 제한				

기계 번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

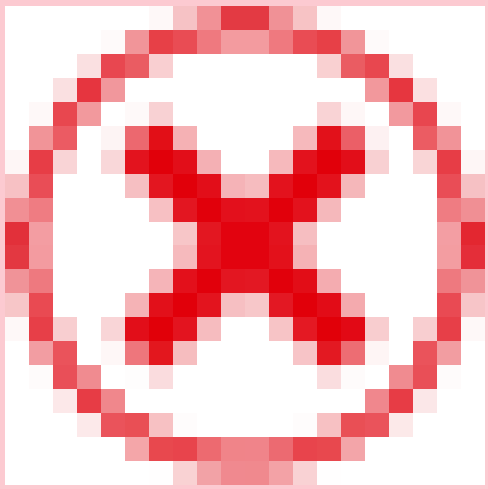
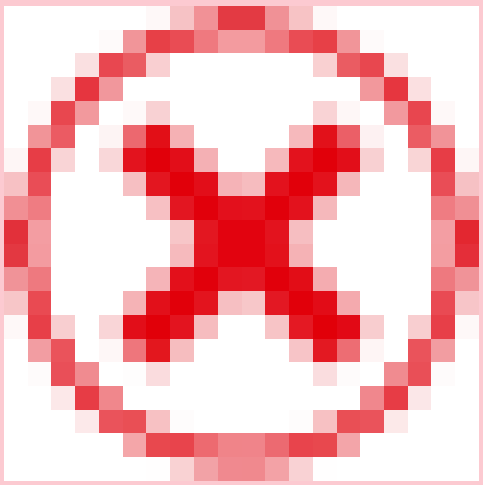
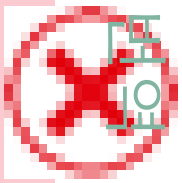
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
속도 제한 정의				
관리				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
설정 도우미	✗	✗	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
주시 주제	✓	✓	✓	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
담당 규칙				

기계 번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
정정 작업 규칙	✗	✗	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
할당 권장 사항	✗	✗	✗	

기계 번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
취약성 계산기	✗	✓	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

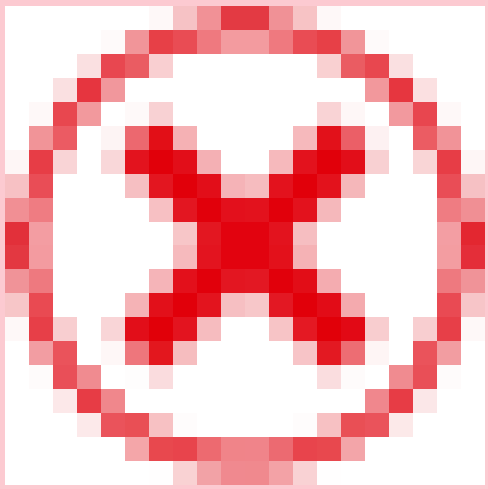
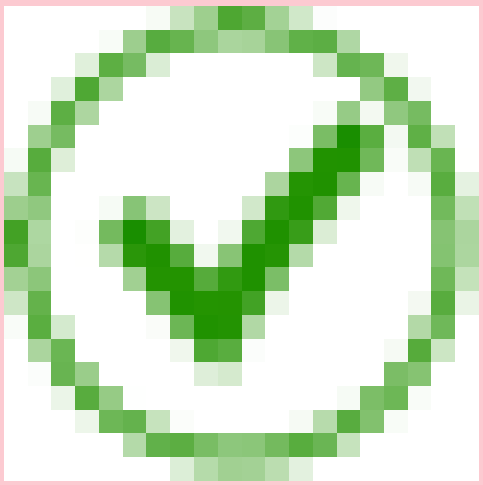
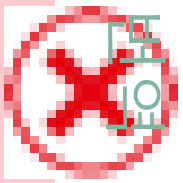
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
취약성 롤업 계산기				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

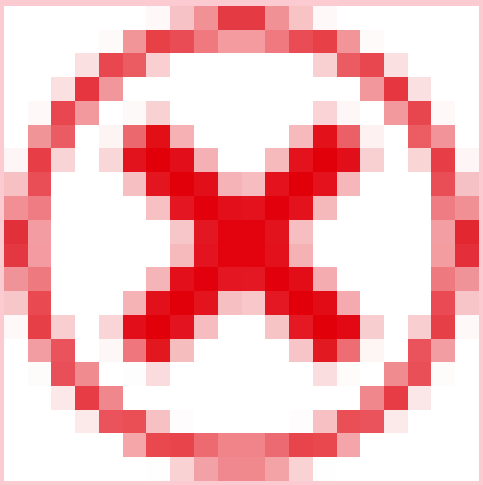
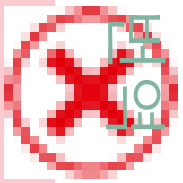
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
정정 대상 규칙				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
AutoClose 구성	✗	✗	✗	

기계 번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
자동 삭제 규칙	✗	✗	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
예외 규칙	✗	✗	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

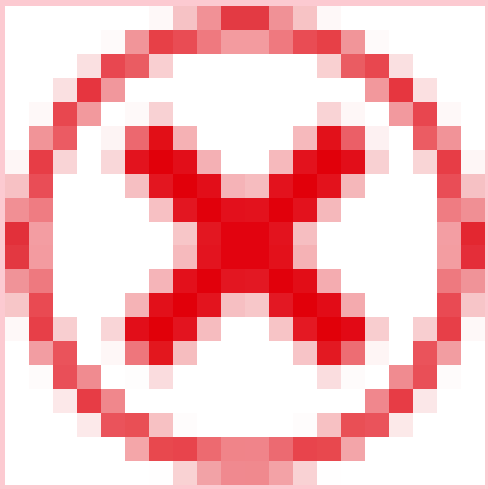
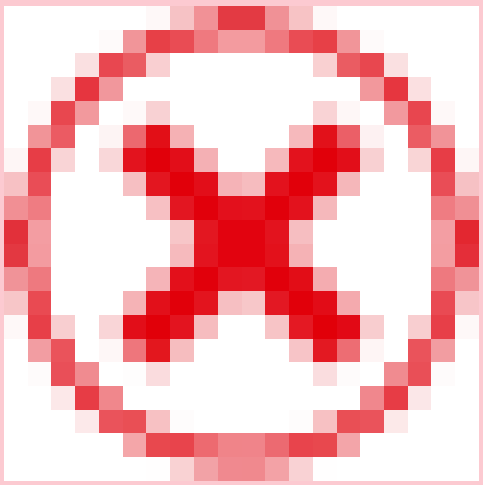
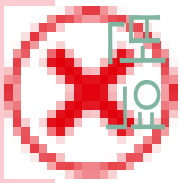
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
승인 규칙				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
분류 규칙				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
성과 구성	✗	✗	✗	

기계 번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
VI 세분성 구성	✗	✗	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
알림	✗	✗	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
이메일 템플릿	✗	✗	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
임포트 큐				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

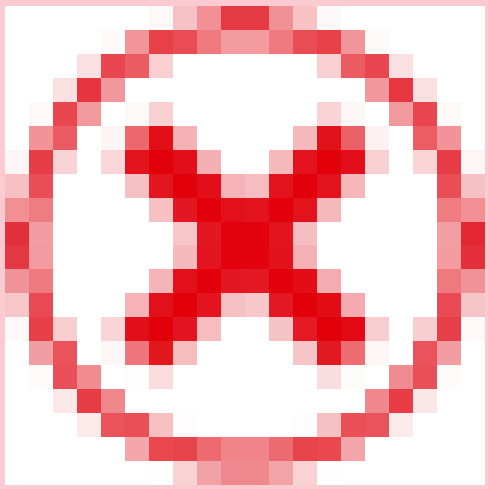
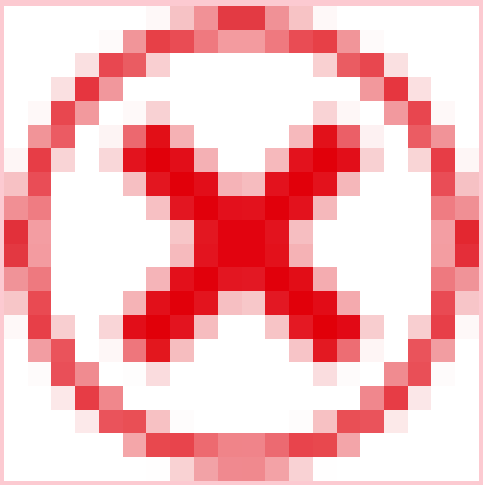
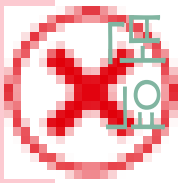
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
통합				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

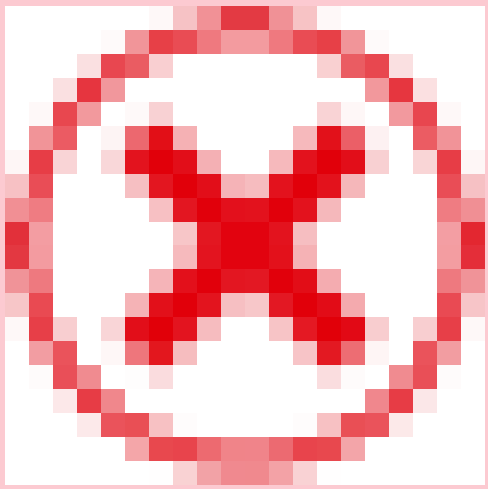
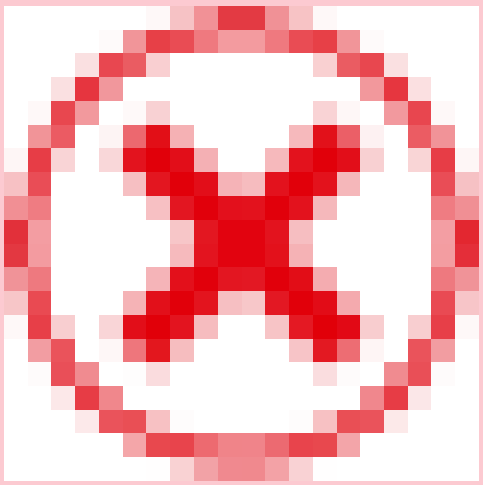
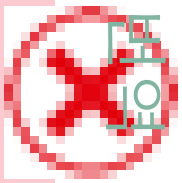
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
SLA 정의				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
SAM NVD 구성	✗	✗	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

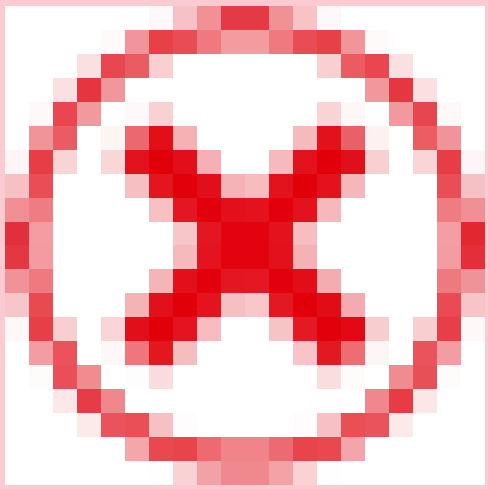
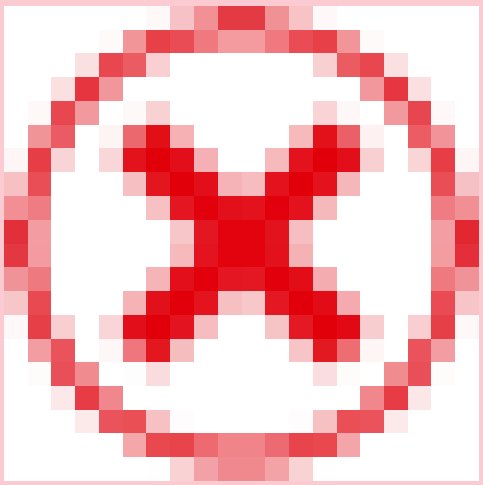
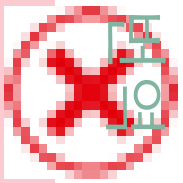
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
표준화된 심각성 맵				

기계 번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
스캔 보장 범위 구성	✗	✗	✗	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

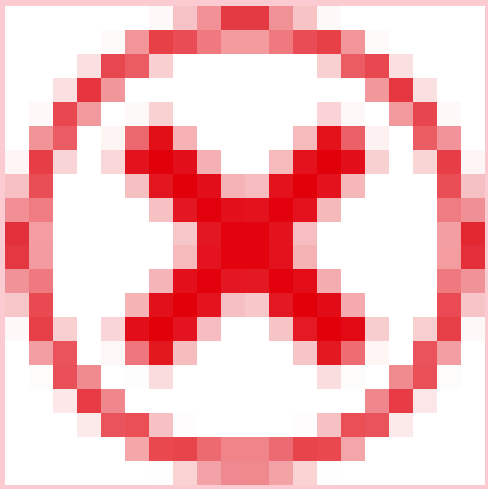
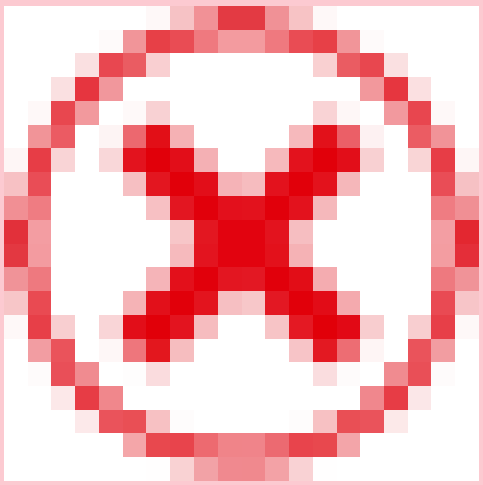
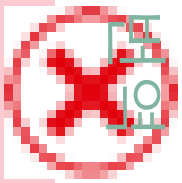
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
예외 관리				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

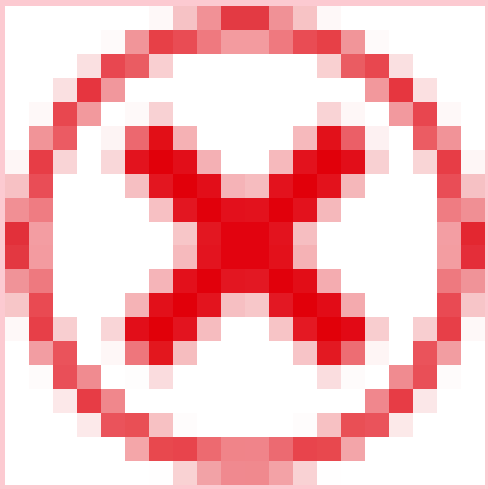
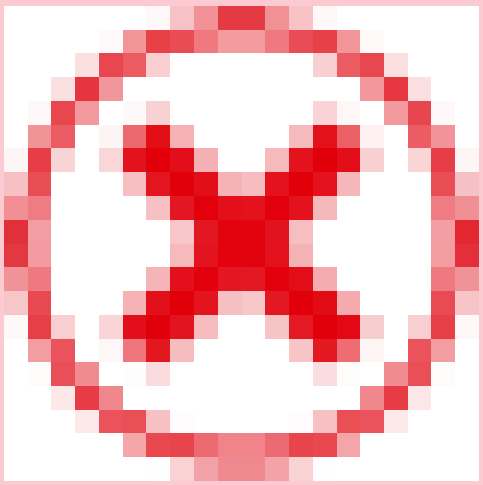
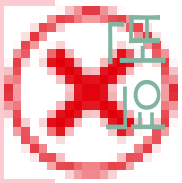
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
사용량 보고서				
진단				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

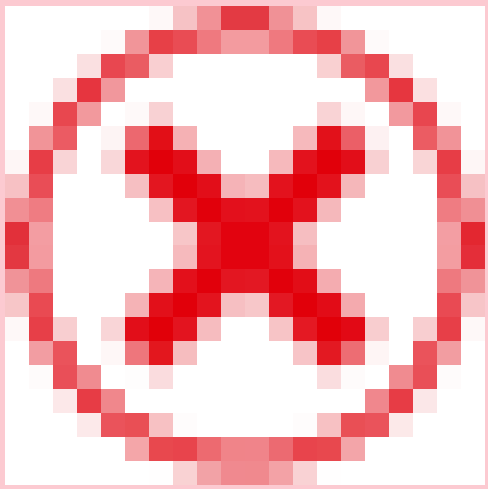
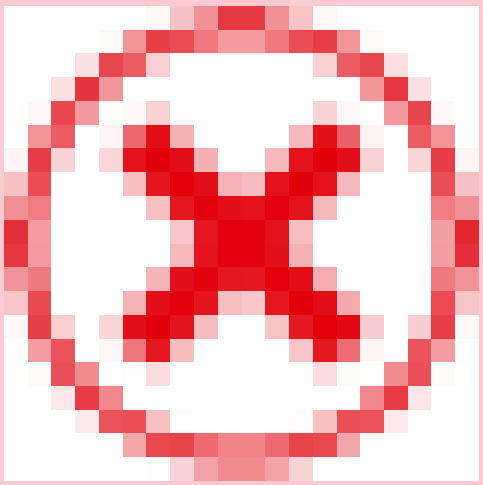
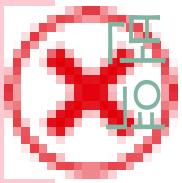
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	sn_v
검사				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats**

다음에 대한 모듈 액세스: **sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approver
(메인 앱 그룹)				
CISO 대시보드	✗	✗	✗	✗

기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approve
정정 개요	✗	✗	✓	✗
취약성 관리자 작업 공간	✗	✗	✗	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

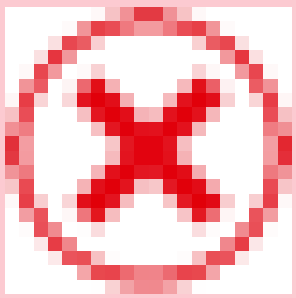
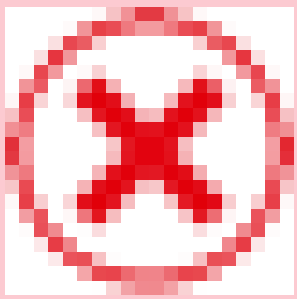
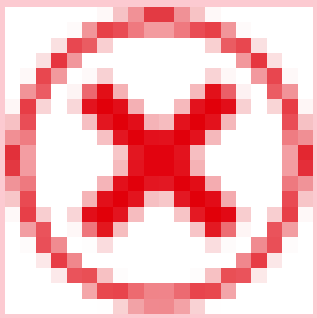
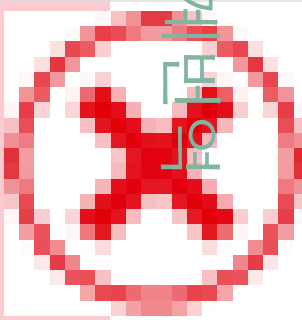
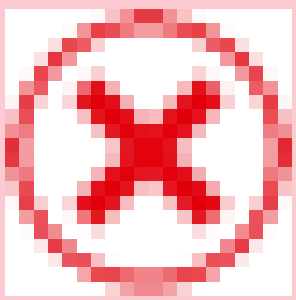
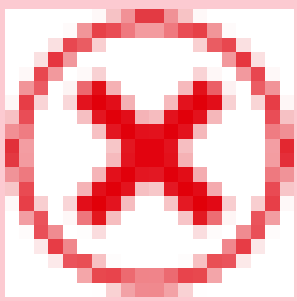
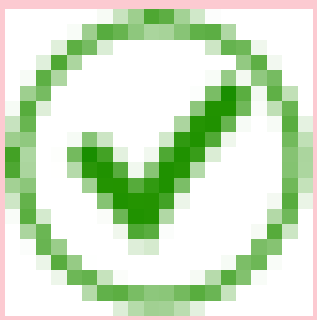
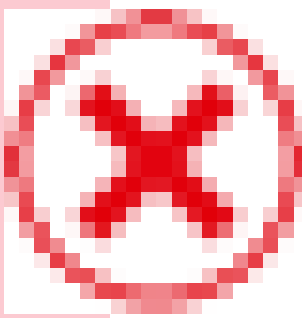
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approve
개요				
IT 정정 작업 공간				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approve
승인자 개요	✗	✗	✗	✗
개요	✗	✗	✗	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approve
내 승인	✗	✗	✗	✓
정정 작업				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approve
활성	✗	✗	✗	✗
나에게 할당됨	✗	✗	✓	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approve
사용자 그룹에 할당됨	✗	✗	✓	✗
모두	✗	✗	✗	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approve
취약 항목				
중요 위험	✗	✗	✗	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approve
높은 위험	✗	✗	✗	✗
악용 가능	✗	✗	✗	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approve
대상에 접근	✗	✗	✗	✗
누락된 대상	✗	✗	✗	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approve
지난 90일 이내	✗	✗	✗	✗
90일 경과	✗	✗	✗	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approve
미할당	✗	✗	✓	✗
그룹 해제	✗	✗	✗	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

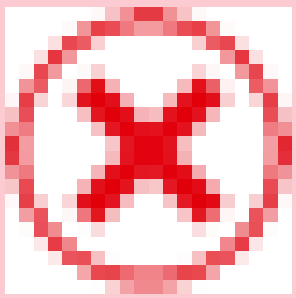
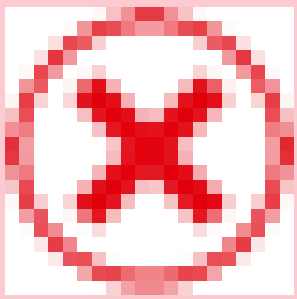
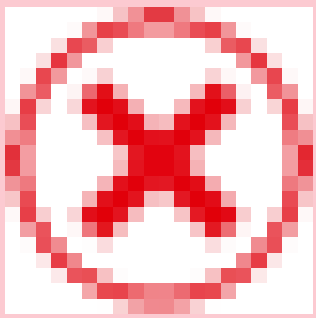
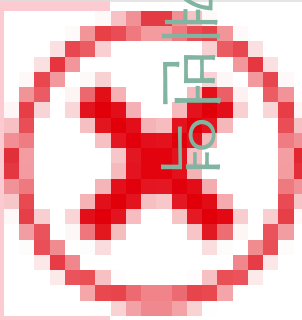
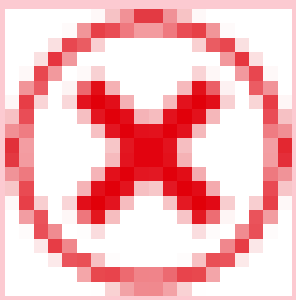
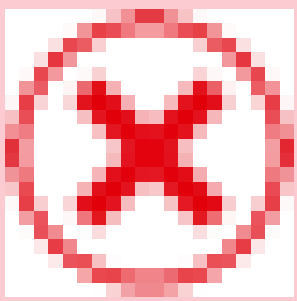
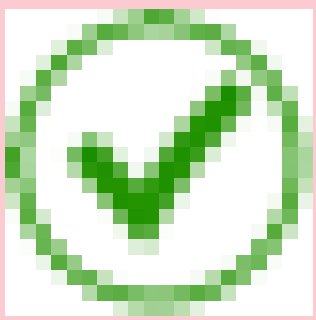
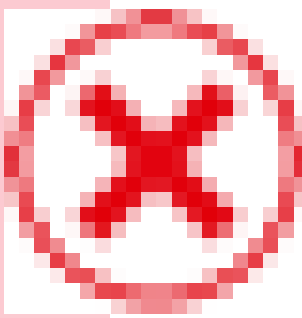
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approve
해제됨				
여러 지연				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

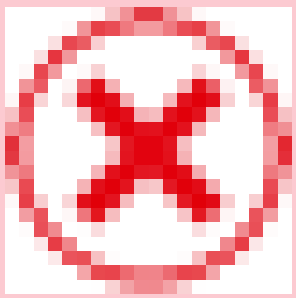
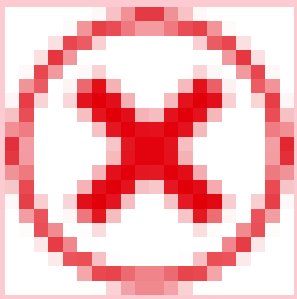
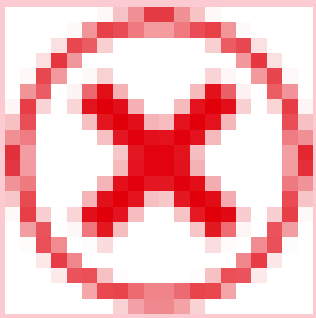
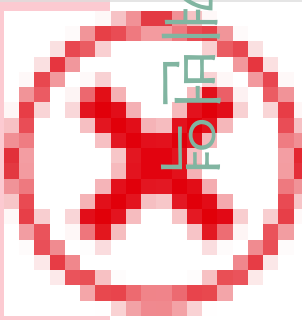
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approve
모두				
솔루션				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approve
모두	✗	✗	✓	✗
가장 높은 대체	✗	✗	✓	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approve
취약한 항목 포함	✗	✗	✗	✗

라이브러리

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approve
NVD	✗	✗	✓	✗
CWE	✗	✗	✗	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approve
외부 공급업체	✗	✗	✓	✗
취약한 소프트웨어	✗	✗	✗	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approve
취약성 스캐닝				
노출 평가	✗	✗	✗	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approve
스캔	✗	✗	✗	✗
스캐너	✗	✗	✗	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approve
스캔 큐	✓	✗	✗	✗
스캐너 속도 제한	✗	✗	✗	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approve
속도 제한 정의				
관리				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approve
설정 도우미	✗	✗	✗	✗
주시 주제	✗	✓	✗	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approve
담당 규칙	✗	✗	✗	✗
정정 작업 규칙	✗	✗	✗	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approve
할당 권장 사항	✗	✗	✗	✗
취약성 계산기	✗	✗	✗	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

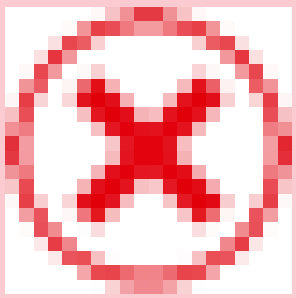
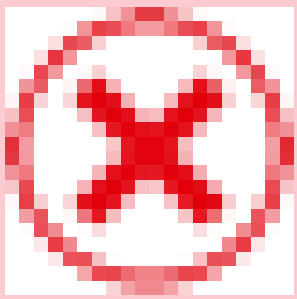
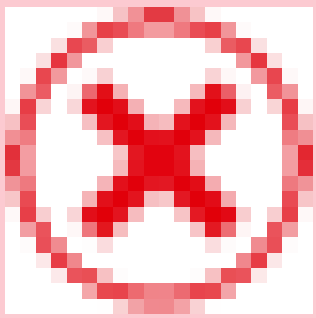
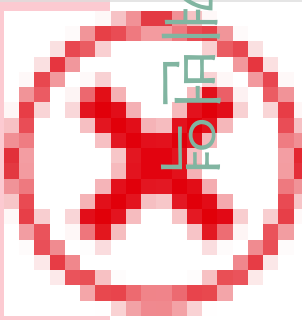
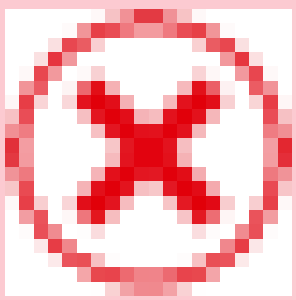
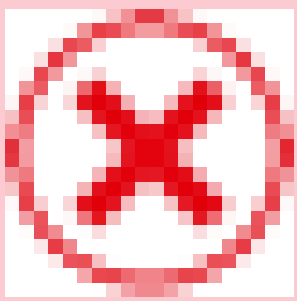
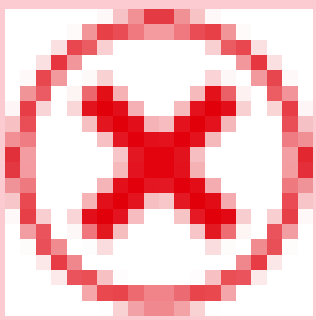
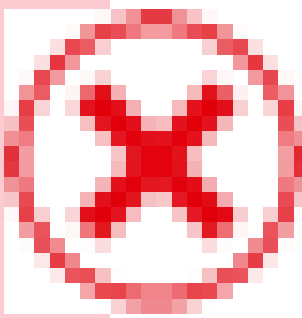
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approve
취약성 롤업 계산기				
정정 대상 규칙				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approve
AutoClose 구성	✗	✗	✗	✗
자동 삭제 규칙	✗	✗	✗	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approve
예외 규칙	✗	✗	✗	✗
승인 규칙	✗	✗	✗	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approve
분류 규칙	✗	✗	✗	✗
성과 구성	✗	✗	✗	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approve
VI 세분성 구성	✗	✗	✗	✗
알림	✗	✗	✗	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approve
이메일 템플릿	✗	✗	✗	✗
임포트 큐	✗	✗	✗	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

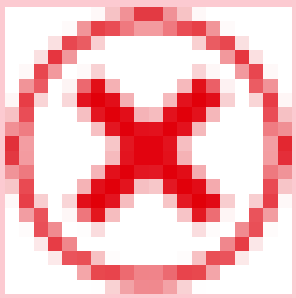
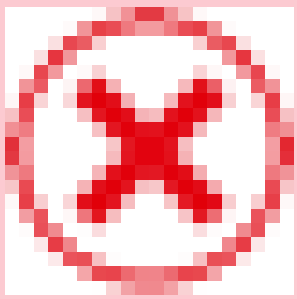
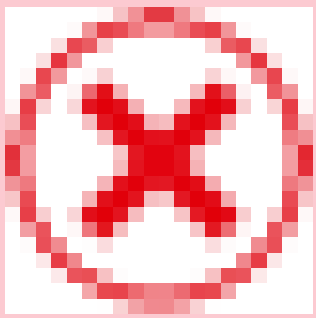
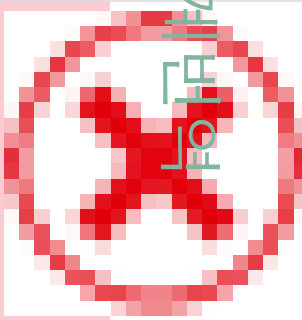
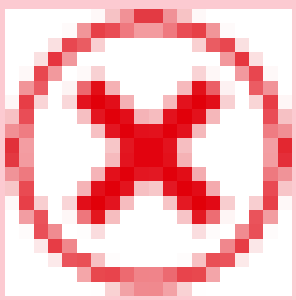
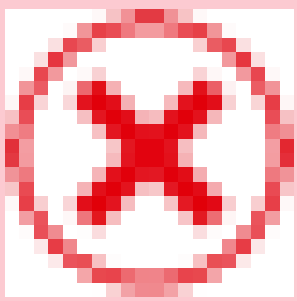
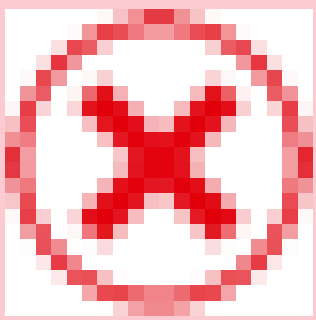
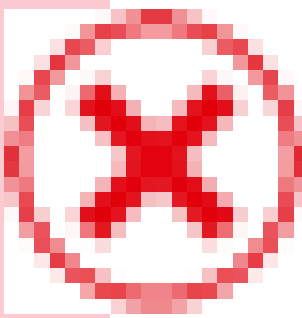
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approve
통합				
SLA 정의				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

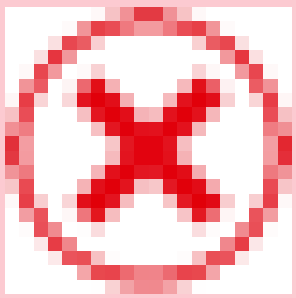
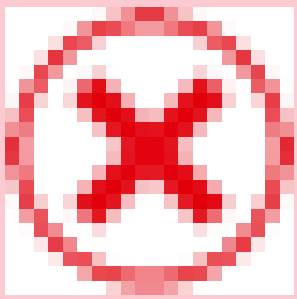
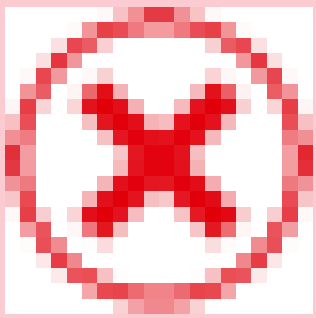
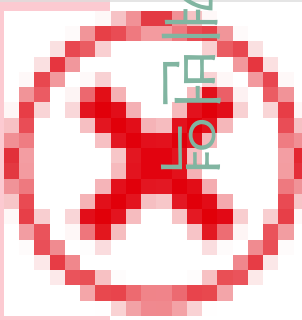
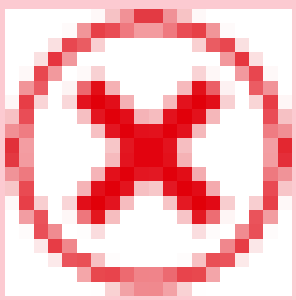
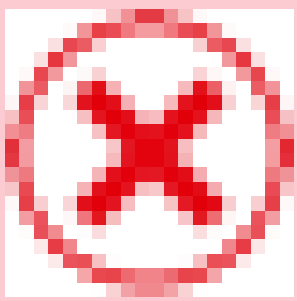
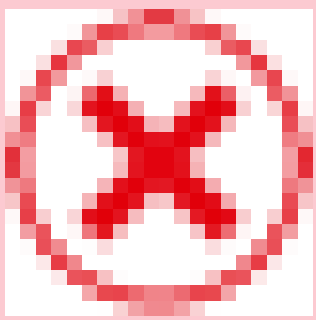
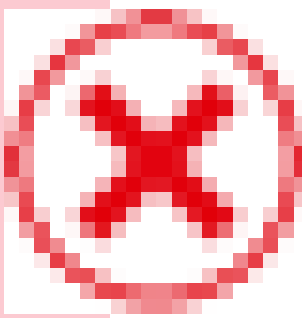
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approve
SAM NVD 구성				
표준화된 심각성 맵				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approve
스캔 보장 범위 구성	✗	✗	✗	✗
예외 관리	✗	✗	✗	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approve
사용량 보고서	✗	✗	✗	✗
진단				

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 대한 모듈 액세스: **sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

모듈	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_approve
검사	✗	✗	✗	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 액세스: **sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

모듈 액세스: **sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

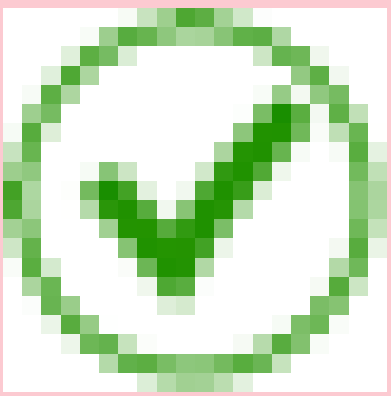
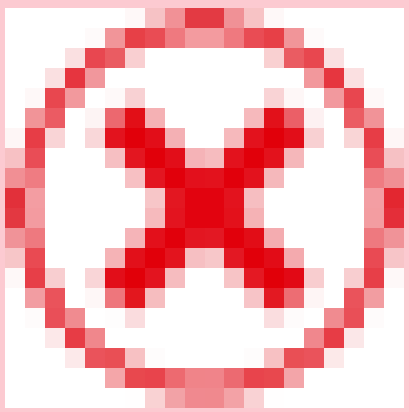
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

모듈	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
(메인 앱 그룹)		
CISO 대시보드		

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 액세스: **sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

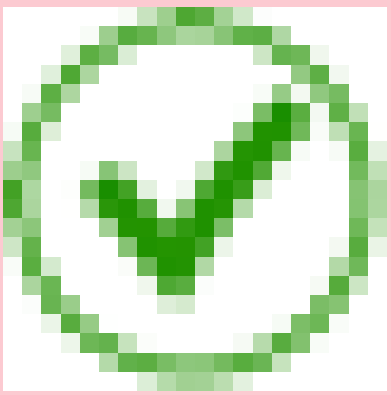
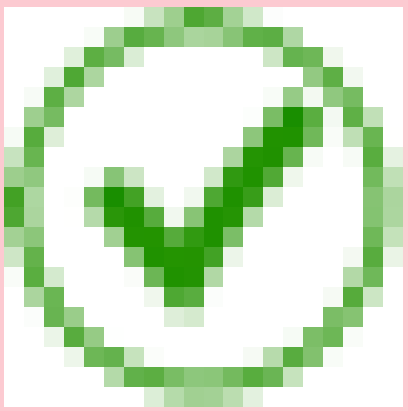
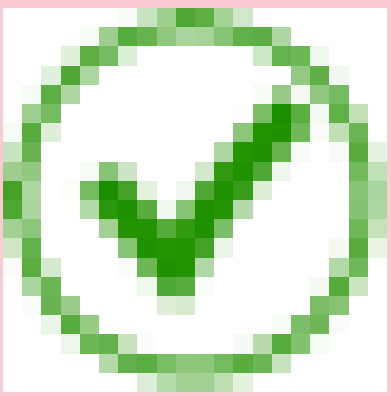
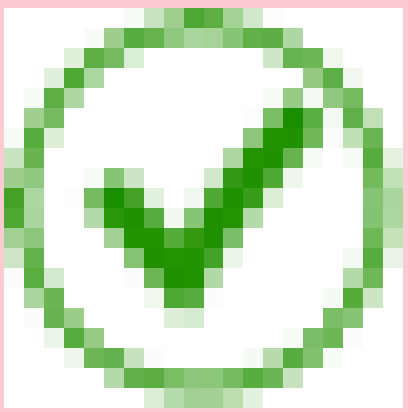
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

모듈	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
정정 개요		
취약성 관리자 작업 공간		

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 액세스: **sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

모듈	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
개요	✓	✓
IT 정정 작업 공간	✗	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 액세스: **sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

모듈	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
승인자 개요	✓	✓
개요	✓	✓

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 액세스: **sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

모듈	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
내 승인	✓	✓
정정 작업		
활성	✓	✓

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 액세스: **sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

모듈	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
나에게 할당됨	✓	✓
사용자 그룹에 할당됨	✓	✓

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 액세스: **sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

모듈	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
모두	✓	✓
취약 항목		
중요 위험	✓	✓

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 액세스: **sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

모듈	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
높은 위험	✓	✓
악용 가능	✓	✓

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 액세스: **sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

모듈	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
대상에 접근 중	✓	✓
누락된 대상	✓	✓

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 액세스: **sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

모듈	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
지난 90일 이내	✓	✓
90일 경과	✓	✓

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 액세스: **sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

모듈	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
미할당	✓	✓
그룹 해제	✓	✓

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 액세스: **sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

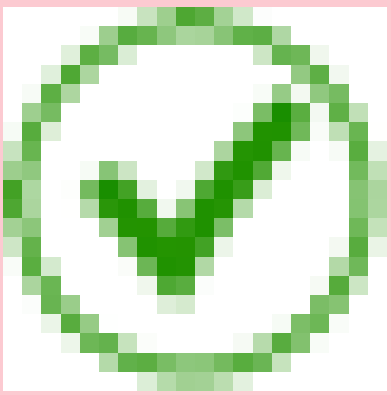
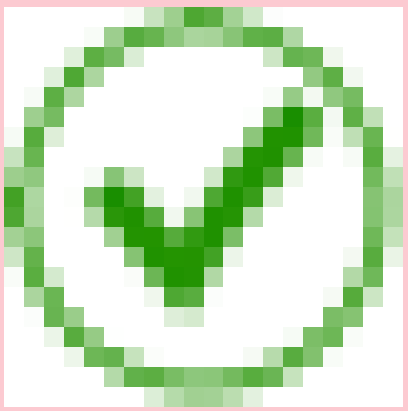
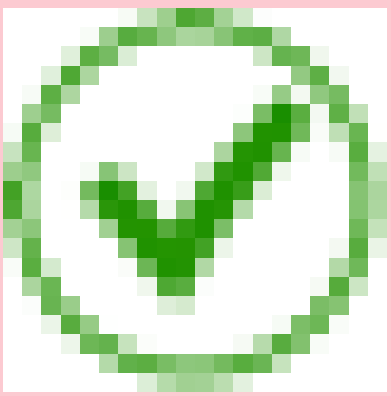
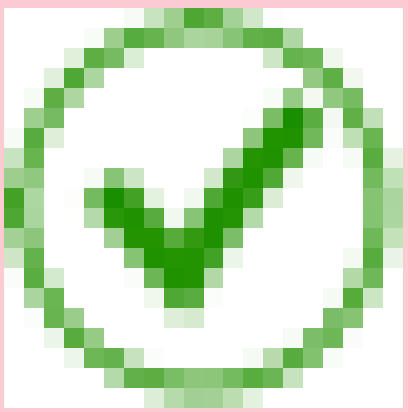
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

모듈	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
해제됨		
여러 지연		

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 액세스: **sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

모듈	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
모두	✓	✓
솔루션		
모두	✓	✓

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 액세스: **sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

모듈	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
가장 높은 대체	✓	✓
취약한 항목 포함	✓	✓
라이브러리		

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 액세스: **sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

모듈	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
NVD	✓	✓
CWE	✓	✓

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 액세스: **sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

모듈	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
외부 공급업체	✓	✓
취약한 소프트웨어	✓	✓
취약성 스캐닝		

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 액세스: **sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

모듈	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
노출 평가	✓	✓
스캔	✓	✓

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 액세스: **sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

모듈	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
스캐너	✓	✓
스캔 큐	✓	✓

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 액세스: **sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

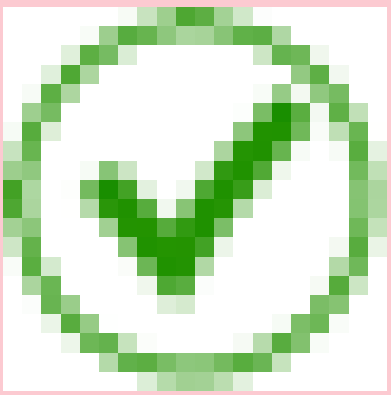
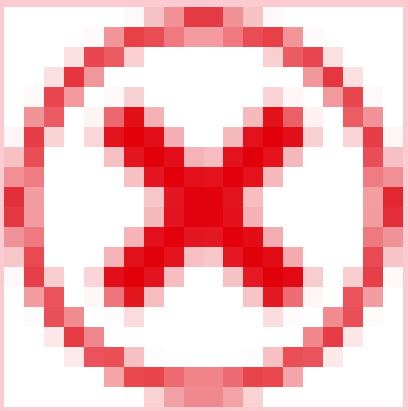
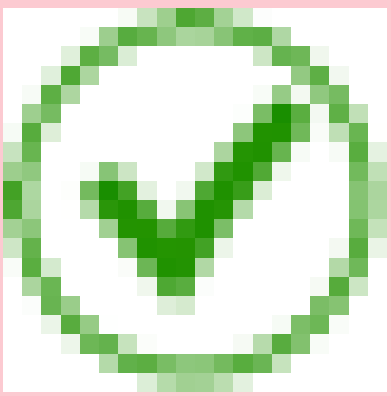
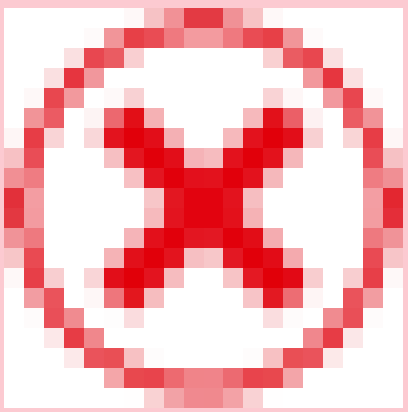
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

모듈	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
스캐너 속도 제한		
속도 제한 정의		
관리		

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 액세스: **sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

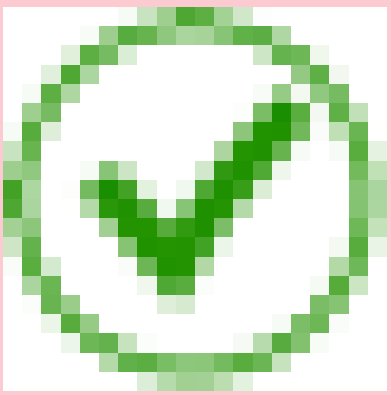
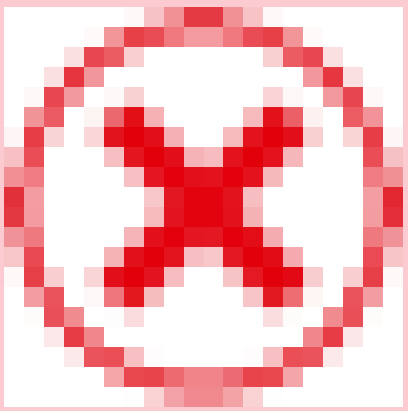
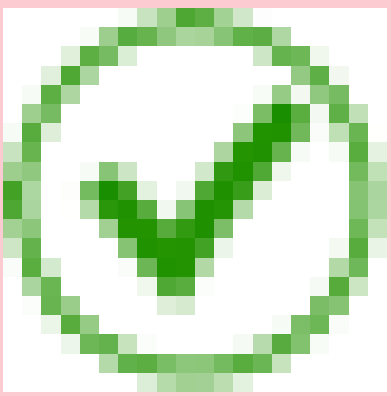
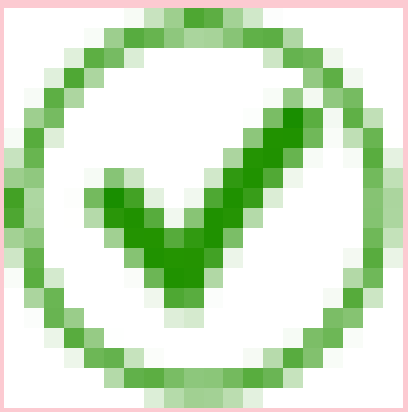
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

모듈	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
설정 도우미		
주시 주제		

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 액세스: **sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

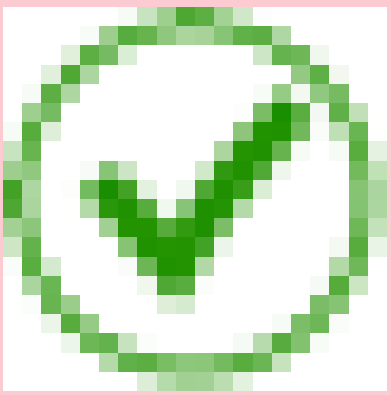
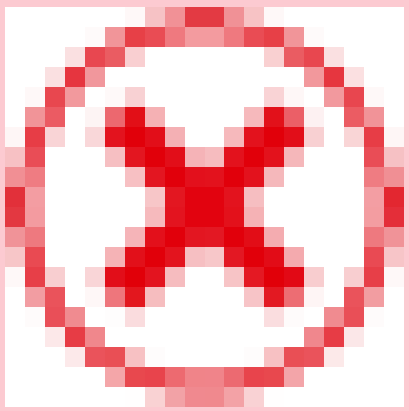
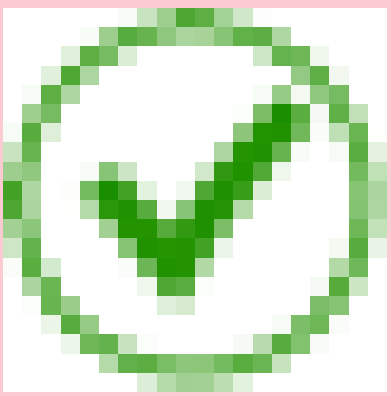
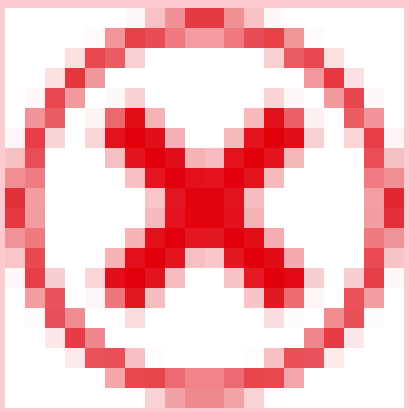
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

모듈	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
담당 규칙		
정정 작업 규칙		

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 액세스: **sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

모듈	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
할당 권장 사항	✗	✗
취약성 계산기	✓	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 액세스: **sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

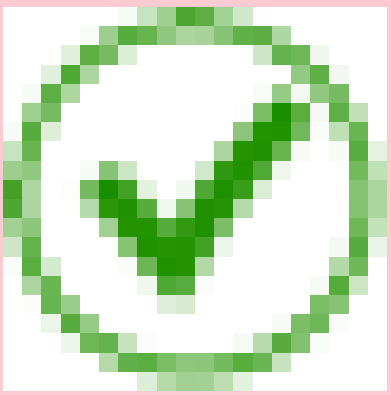
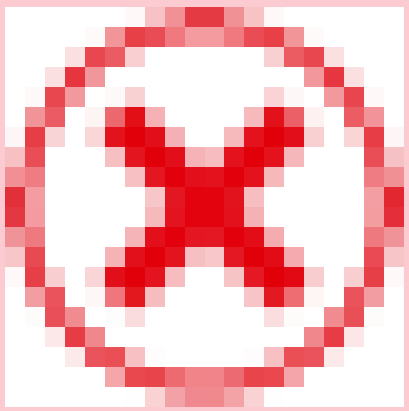
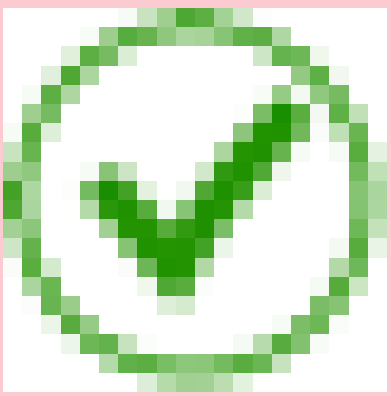
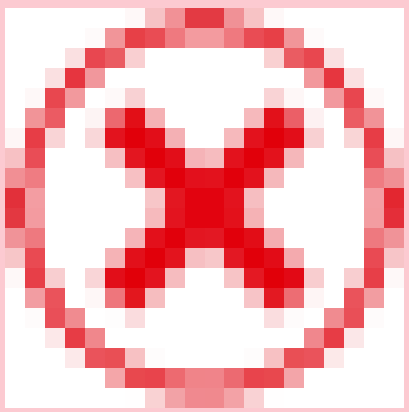
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

모듈	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
취약성 롤업 계산기		
정정 대상 규칙		

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 액세스: **sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

모듈	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
AutoClose 구성	✓	✗
자동 삭제 규칙	✓	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 액세스: **sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

모듈	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
예외 규칙	✓	✓
승인 규칙	✓	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 액세스: **sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

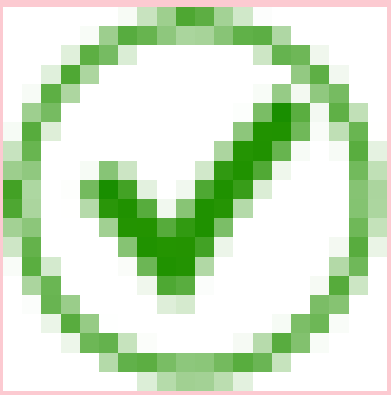
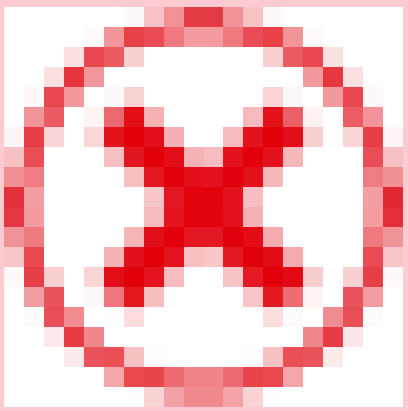
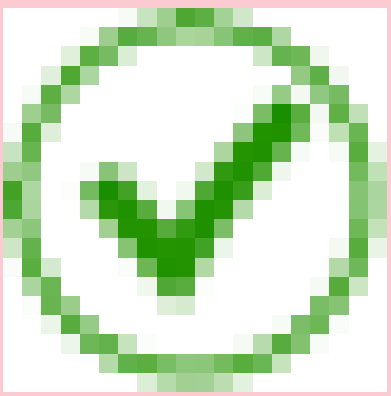
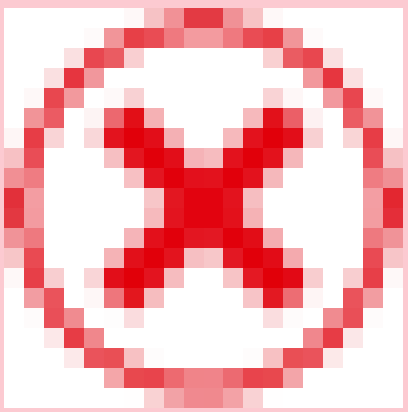
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

모듈	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
분류 규칙		
성과 구성		

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 액세스: **sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

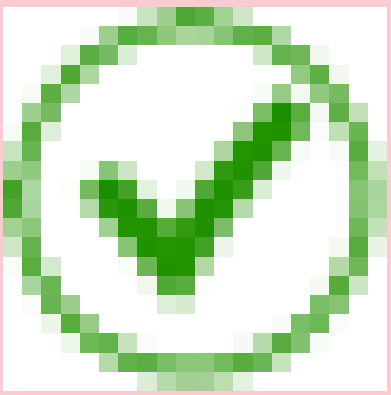
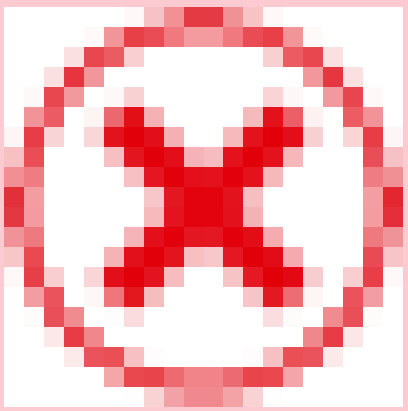
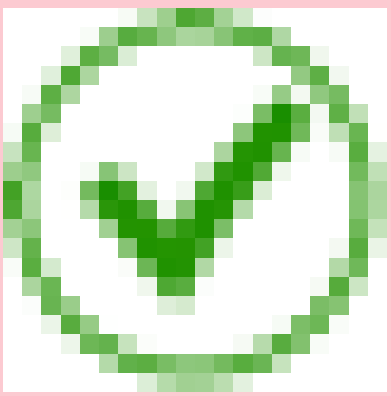
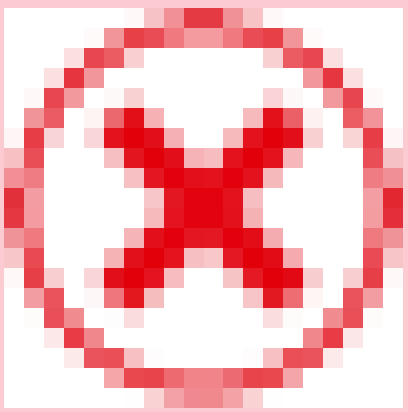
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

모듈	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
VI 세분성 구성		
알림		

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 액세스: **sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

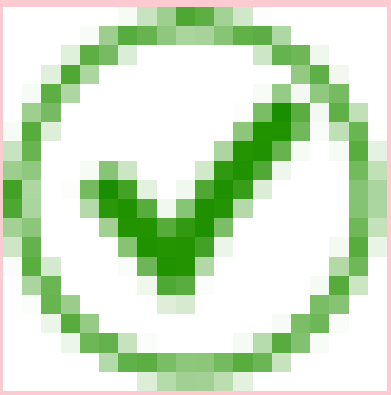
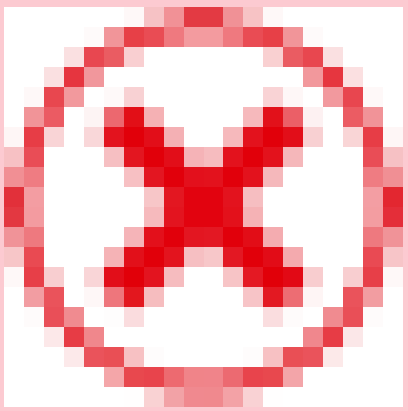
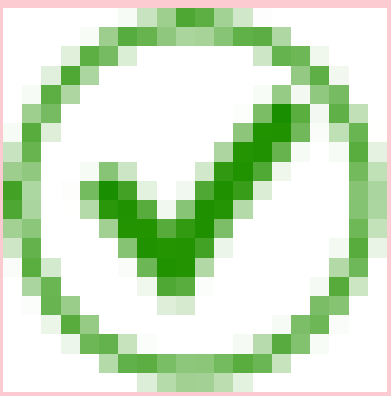
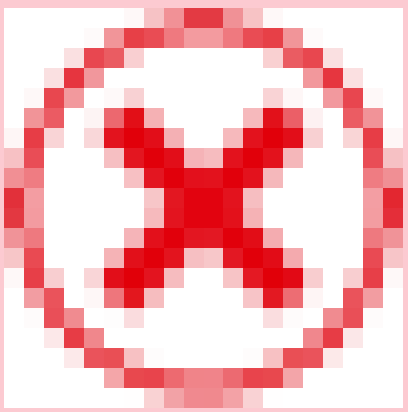
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

모듈	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
이메일 템플릿		
임포트 큐		

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 액세스: **sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

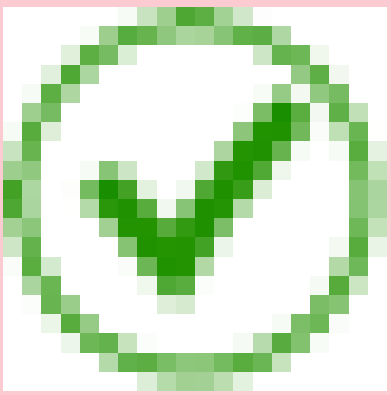
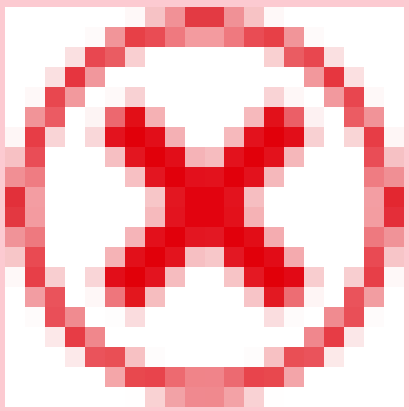
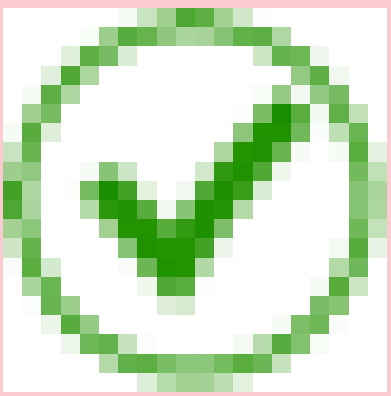
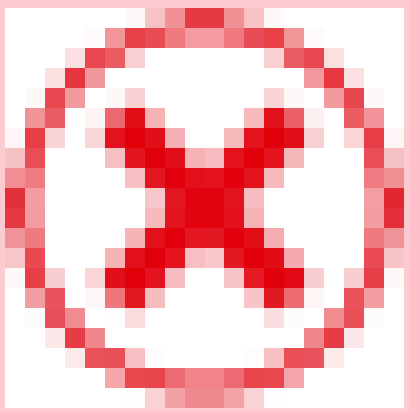
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

모듈	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
통합		
SLA 정의		

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 액세스: **sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

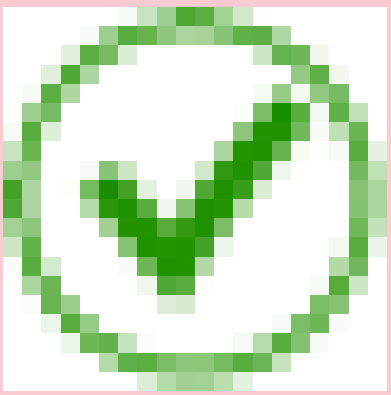
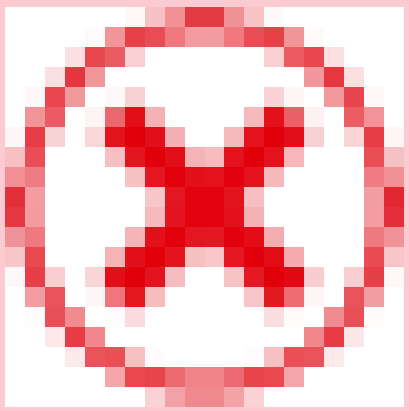
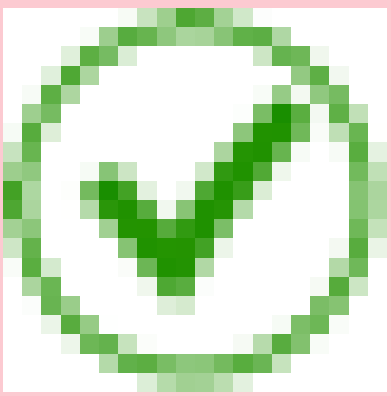
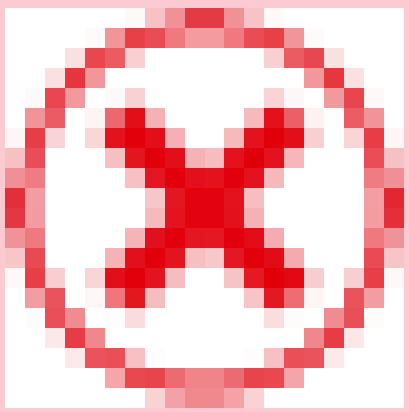
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

모듈	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
SAM NVD 구성		
표준화된 심각성 맵		

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 액세스: **sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

모듈	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
스캔 보장 범위 구성	✓	✓
예외 관리	✓	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 액세스: **sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

다른 역할에 대한 정보:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.노출_평가_관리, sn_vul.그룹_규칙관리, sn_vul.알림관리, sn_vul.관리_권한

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

모듈	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
사용량 보고서	✓	✗
진단		
검사	✗	✗

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

〔End〕

보안 운영 검색

화면 헤더의 검색 아이콘을 사용하여 모든 보안 운영 애플리케이션에서 정보를 빠르게 찾을 수 있습니다. Zing은 인스턴스에서 모든 텍스트 검색을 수행하는 텍스트 인덱싱 및 검색 엔진입니다.

시작하기 전에
필요한 역할: sn_si.read 이상

프로시저

1. 화면의 오른쪽 상단 모서리에 있는 검색 아이콘( )을 클릭합니다.
2. 검색할 기준을 입력하고 **Enter** 키를 누릅니다.
   플러그인이 보안 인시던트 응답 활성화되어 있으면 입력한 검색 기준에 보안 인시던트, 보안 인시던트 응답 작업 또는 보안 요청에 일치하는 짧은 설명 텍스트, CI, IP 주소 또는 URL이 표시됩니다. OR 위협 인텔리전스 플러그인이 취약성 대응 활성화된 경우 검색 결과에는 취약성, 취약한 항목, 취약한 항목, 옵저버블, IoC 및 공격 모드/방법이 포함됩니다.

관련 정보

검색 소개

Zing 텍스트 검색

Security Operations Integrations 참조

개발자와 ServiceNow 파트너는 이 섹션의 정보를 사용하여 개발 가이드라인, 통합 역량 및 워크플로우를 포함한 외부 공급업체 통합의 내부 기능에 대한 이해를 얻을 수 있습니다.

ServiceNow 보안 운영 통합 개발 가이드라인

플랫폼은 ServiceNow 외부 시스템과의 통합을 개발하기 위한 몇 가지 메커니즘을 제공합니다. 이 제품군은 ServiceNow 보안 운영 보안 중심의 외부 시스템과 통합하는 프로세스를 간소화하기 위한 통합 기능을 추가합니다.

이 가이드에 있는 대부분의 개념은 표준 ServiceNow 기능에 어느 정도 익숙하다고 가정합니다. 제품군과 보안 운영 통합하려면 최소한 다음 ServiceNow 개념에 대한 지식이 필요합니다.

- 스크립트 포함
- 인바운드/아웃바운드 웹 서비스
- 데이터 소스
- 임포트 세트
- 변환 맵

기술 파트너 프로그램

기술 파트너 프로그램 문헌에 제공된 애플리케이션 인증 또는 지침에 대한 모든 요구 사항은 이 가이드의 모든 정보를 대체합니다. 이 가이드는 기술 파트너 프로그램 자료를 대체하지 않으며 기존 설명서를 보완하는 용도로만 사용됩니다.

자세한 내용은 기술 파트너 프로그램 교육 과정 블로그 게시물을 참조하세요.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

제공되는 통합의 **ServiceNow** 유형

애플리케이션(보안 인시던트 응답, 위협 인텔리전스, 취약성 대응및)은 보안 운영 다른 ServiceNow 애플리케이션과 원활하게 통합되어 기능을 향상시킬 수 있습니다.

기본 시스템에서는 다음과 같은 통합이 보안 운영 제공됩니다.

Security Incident Response – Event Management 통합

애플리케이션의 기능은 이벤트 관리 를 지원하도록 보안 인시던트 응답확장되었습니다. 지원 플러그인은 보안 인시던트 응답 이벤트 관리 의 이벤트 관리 이벤트 내용을 자동으로 구문 분석하여 보안 인시던트의 필드를 채웁니다.

다루는 사용 사례:

보안 정보 및 이벤트 관리 (SIEM) 도구에서 시스템의 보안 이벤트 이벤트 관리 생성

유용한 기능이 제공됩니다.

- Event Management 기능 – 이벤트 상관관계, 이벤트 규칙 및 경보 규칙
- 결과 보안 인시던트에 additional_information 값을 자동으로 매핑

리소스:

보안 인시던트 이벤트 관리 지원 설명서

이벤트 관리 설명서

보안 인시던트 응답 **-** 임포트 세트 **API** 통합

이 보안 인시던트 응답 애플리케이션은 보안 관련 이벤트를 푸시하는 데 사용할 이벤트 관리 수 있을 뿐만 아니라 보안 인시던트를 직접 생성할 수 있는 임포트 세트 API를 제공합니다. 보안 인시던트 임포트 세트의 REST 엔드포인트는 http://localhost:8080/api/now/import/sn_si_incident_import 입니다.

이 통합 기술은 a) 이벤트 관리 설치되어 있지 않거나, b) 를 사용할 이벤트 관리때 필요한 이벤트 > 경보 > 보안 인시던트 플로우를 거치지 않고 단순히 보안 인시던트를 생성하려는 경우에 유용합니다.

다루는 사용 사례:

SIEM 도구에서 직접 보안 인시던트 생성

유용한 기능이 제공됩니다.

IP, NetBIOS 또는 정규화된 도메인 이름을 기반으로 보안 인시던트 생성 시 자동 CI 일치.

리소스:

플랫폼 임포트 세트 API 설명서

보안 인시던트 웹 서비스 임포트 세트 설명서

Threat Intelligence - 소스 통합 조회

조회 소스는 외부 조회 소스로 데이터를 보내 해당 데이터가 악성인지 여부를 확인하는 기능을 제공합니다. 일반적으로 해당 데이터는 IP 주소, URL, 파일 또는 파일 해시입니다.

다루는 사용 사례:

외부 조회 서비스를 사용하여 IP 주소, URL, 파일 또는 해시를 조회합니다.

유용한 기능이 제공됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 카탈로그 항목 및 보안 인시던트에서 조회를 요청하는 일관된 방법입니다.
- 코딩이 거의 또는 전혀 없이 제공되는 속도 제한 및 제한 기능입니다.
- 조회 소스에서 찾은 문제에 대한 IoC(침해 표시기) 옵저버블 항목 자동 생성.

Threat Intelligence - 위협 소스 통합

위협 소스는 외부 위협 인텔리전스 리포지토리에서 데이터를 가져오는 기능을 제공합니다. 그런 다음 이 데이터는 시스템 내에 있는 다양한 침해지표 테이블로 임포트됩니다. TAXII 컬렉션 및 단순 차단 목록은 기본적으로 지원됩니다. 새 TAXII 컬렉션(또는 검색 또는 컬렉션 관리 서비스를 기반으로 하는 프로파일)을 추가하려면 항목을 추가하는 것만큼 간단합니다. 마찬가지로, 새로운 간단한 단일 열 차단 목록을 추가하는 것은 새 레코드를 입력하고 차단 목록의 URL을 제공하는 문제입니다. 더 복잡한 데이터 세트의 경우 URL을 호출하고 응답을 구문 분석하는 사용자 지정 통합을 제공할 수 있습니다.

다루는 사용 사례:

위협 인텔리전스 소스에서 데이터를 검색하여 IoC 테이블에 로드합니다.

유용한 기능이 제공됩니다.

- 코딩 없이 간단한 차단 목록 및 TAXII 컬렉션을 지원합니다.
- 데이터 검색을 위해 REST 메시지를 실행하는 간단한 메커니즘입니다.
- 통합 구성요소 재사용성을 위해 데이터 검색/처리가 분리되었습니다.
- 데이터 소스(및 임포트 세트/변환 맵)로 반환되는 데이터 전달 처리를 기본 지원합니다.
- 후속 호출에 컨텍스트를 전달하는 기능으로 통합당 여러 데이터 요청(페이지 매김된 호출의 경우)을 지원합니다.

리소스:

위협 소스 정의

Vulnerability Response - 스캐너 호출 통합

취약성 스캐너 발동은 인스턴스에서 취약성 스캔 호출을 지원하는 간단한 통합 엔트리포인트입니다. 구성 항목 또는 IP 주소에 대한 검사를 예약하기 위해 타사 취약성 스캐너가 비동기적으로 호출됩니다.

다루는 사용 사례:

CI(CI에서 파생된 호스트 정보 사용) 또는 IP 주소를 스캔하기 위해 타사 스캐너에 요청합니다.

유용한 기능이 제공됩니다.

- 스캐너 구현을 정의하기 위한 간단한 프레임워크입니다.
- 카탈로그 항목, 보안 인시던트 및 취약한 항목에서 검사를 요청하는 일관된 방법입니다.
- 스캔 호출의 결과로 작업이 자동으로 업데이트됩니다.

취약성 대응 - 데이터 통합

취약성 데이터 통합은 외부 공급업체 취약성 시스템에서 취약성 데이터를 검색하기 위한 것입니다. 이러한 통합에서 예상되는 출력은 취약성 항목 및 취약한 항목입니다. 이 통합을 통해 외부 공급업체 취약성 스캐너가 독립적으로 작동할 수 있으며, 인스턴스 내에서 취약성을 처리하고 추적할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다루는 사용 사례:

- 취약성 라이브러리 검색
- 취약성/CI 쌍 검색
- CI와 취약성 관리 시스템 동기화

유용한 기능이 제공됩니다.

- 통합 구성요소 재사용성을 위해 데이터 검색/처리가 분리되었습니다.
- 데이터 소스(및 임포트 세트/변환 맵)로 반환되는 데이터 전달 처리를 기본 지원합니다.
- 후속 호출에 컨텍스트를 전달하는 기능을 사용하여 통합당 여러 데이터 요청(페이지 매김된 호출의 경우)을 지원합니다.

리소스:

취약성 데이터 통합 문서

보안 운영 통합 구성

기본 시스템에 포함된 대부분의 통합은 설정이 거의 또는 전혀 필요하지 않으며 동일한 방식으로 작동합니다. 그러나 와 같은 Qualys Cloud Platform특정 통합의 경우 통합을 설정하는 데 별도의 단계가 필요합니다. 다른 사람들은 다른 스캔 및 조회 유형 집합과 다른 속도 제한을 지원합니다.

이 섹션에서는 지원되는 통합 간의 차이점을 설명하고 필요에 따라 추가 설명서를 참조할 수 있습니다.

- Carbon Black 통합: Carbon Black API를 사용하여 보안 인시던트와 연관된 엔드포인트를 쿼리하고 상호작용함으로써 보안 인시던트를 조사하고 그에 대응할 수 있습니다.
- Check Point Anti-bot - Email Parser 통합: Check Point 안티 봇의 이메일 알림을 사용하는 이메일 파서를 사용하여 보안 인시던트를 생성합니다.
- Elasticsearch 인시던트 보강 통합: 로그를 검색하고 관련 사이팅 정보를 보안 인시던트에 추가합니다.
- Have I been pwned? 통합: 침해된 계정 목록(이메일 주소 및 사용자 이름)을 RESTful 서비스를 통해 빠르게 검색할 수 있습니다.
- HPE Security ArcSight ESM - 이메일 파서 통합: HPE ArcSight ESM의 이메일 알림을 사용하는 이메일 파서를 사용하여 보안 인시던트를 생성합니다.
- HPE ArcSight Logger - 인시던트 보강 통합: 로그를 검색하고 관련 사이팅 정보를 보안 인시던트에 추가합니다.
- IBM QRadar - 인시던트 보강 통합: 로그를 검색하고 관련 사이팅 정보를 보안 인시던트에 추가합니다.
- McAfee ESM - 이메일 파서 통합: McAfee ESM의 이메일 알림을 사용하는 이메일 파서를 사용하여 보안 인시던트를 생성합니다.
- McAfee ESM - 인시던트 보강 통합: 로그를 검색하고 관련 사이팅 정보를 보안 인시던트에 추가합니다.
- OPSWAT Metadefender 통합 개요: 외부 공급업체 Metadefender 스캐너에서 탐지된 위협 데이터를 추적, 우선순위 지정 및 해결을 위해 애플리케이션에 다운로드할 위협 인텔리전스 수 있습니다.
- Palo Alto Networks - AutoFocus 통합: 위협 인텔리전스 클라우드 서비스인 Palo Alto Networks AutoFocus를 사용하면 보안 인시던트 옵저버블과 관련된 세션 정보를 검색할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- Palo Alto Networks - Firewall 통합: Palo Alto Networks 방화벽을 사용하면 네트워크, 클라우드 및 엔드포인트 전반에서 알려지거나 알려지지 않은 위협을 방지하기 위한 방화벽을 설정하고 유지 관리할 수 있습니다.
- Palo Alto Networks - WildFire 통합: Wildfire 통합을 사용하면 Wildfire에서 프로그래밍 방식으로 분석 작업을 쿼리하고 간단한 XML API 인터페이스를 통해 기록 결과를 검색할 수 있습니다.
- Qualys Vulnerability Integration 이해: Qualys Cloud Platform 에서 취약성 대응사용됩니다.
- Splunk - Incident Enrichment 통합: 로그를 검색하고 관련 사이팅 정보를 보안 인시던트에 추가합니다.
- VirusTotal 통합: 에서 위협 인텔리전스사용됩니다. 이 조회 소스를 사용하려면 VirusTotal 통합 플러그인을 활성화해야 합니다.
- WhoisXML API 통합 설정: Whois 조회에서 일관되고 잘 구조화된 데이터를 제공합니다. 정확한 Whois 데이터에 24/7 액세스할 수 있도록 유지합니다.

외부 공급업체 통합 활성화 및 구성

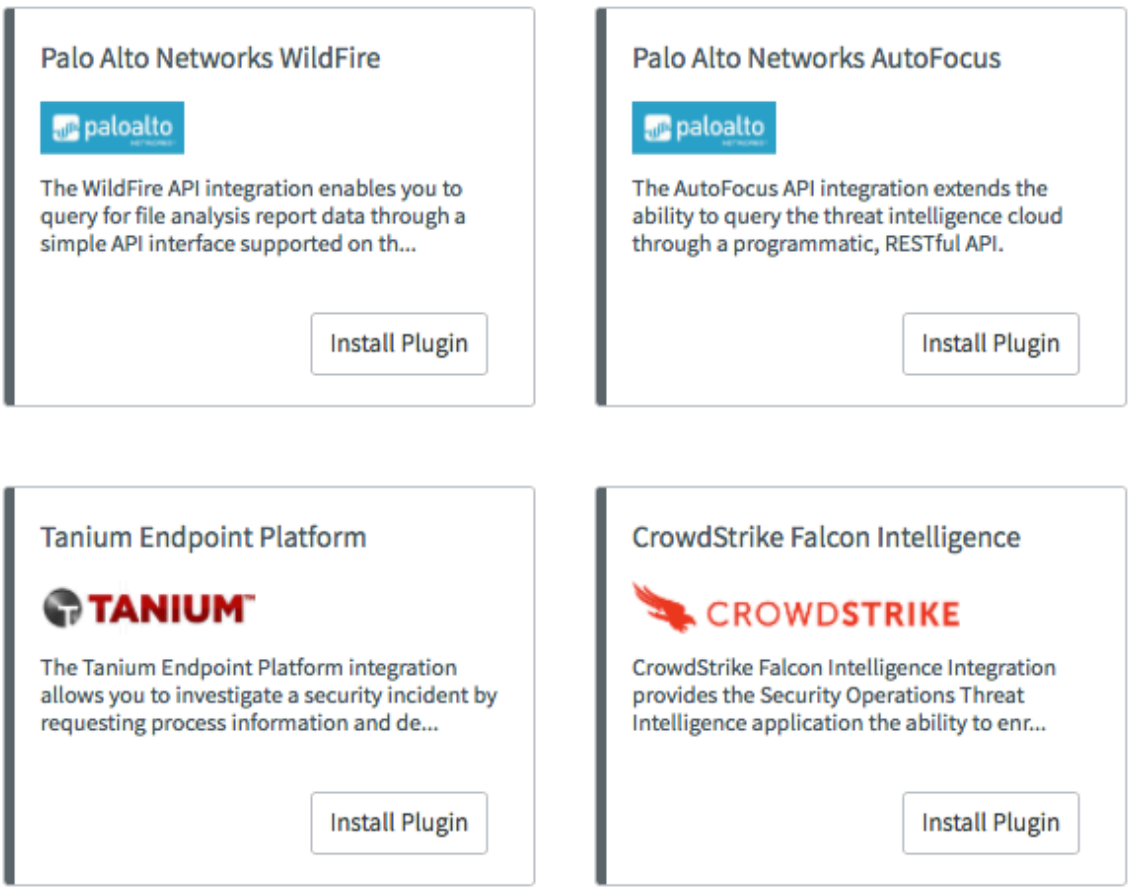
외부 공급업체 통합을 위한 플러그인을 활성화하고 동일한 화면에서 사용하도록 구성할 수 있습니다.

시작하기 전에

필요한 역할: sn_sec_cmn.admin

프로시저

1. 다음으로 이동 모두 〉 보안 운영 〉 통합 구성.
   사용 가능한 보안 통합은 다음 카드 그룹과 유사한 일련의 카드로 표시됩니다. 아무 카드나 가리키면 통합에 대한 설명을 얻을 수 있습니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

2. 지정된 통합에 대한 플러그인을 설치하려면 플러그인 설치를 클릭합니다.

   a. 시스템 플러그인 양식에서 플러그인 상세 정보를 검토하고 활성화/업그레이드 관련 링크를 클릭합니다.

   b. 활성화를 클릭합니다.
   활성화가 완료되면 보안 통합 화면이 다시 열리고 활성화한 통합 버튼에 구성 레이블이 지정됩니다.

3. 구성을 클릭합니다.

   주:
   를 Qualys Vulnerability Integration구성하는 경우 문서를 참조하십시오 취약성 대응 설치 및 지원되는 애플리케이션.

4. **API** 키를 입력합니다.
5. 제출을 클릭합니다.

통합 생성

통합을 생성하고 연결된 통합 카드를 보안 통합 화면에 추가할 수 있습니다. 이 절차는 외부 공급업체 통합을 생성하는 파트너를 위한 것입니다.

시작하기 전에
필요한 역할: sn_sec_cmn.admin

관객: 외부 공급업체 통합을 생성하는 파트너입니다.

프로시저

1. 탐색 필터에 sn_sec_core_integration_item.list를 입력하고 **Enter** 키를 누릅니다.
2. 새로 만들기를 클릭합니다.
3. 양식의 필드에 적절히 입력합니다.

필드	설명
이름	통합의 이름입니다.
플러그인 ID	통합을 사용하기 위해 활성화해야 하는 플러그인입니다.
순서	이 통합 카드가 나타나는 순서를 나타냅니다.
배너 텍스트	링크를 클릭하고 통합 카드에 표시할 이미지 또는 로고를 선택한 후 확인을 클릭합니다.
설치된	플러그인이 이미 설치되었는지 여부를 나타내는 읽기 전용 필드입니다.
구성 가능	통합을 구성할 수 있는지 여부를 나타냅니다.
범주	통합 카드를 필터링하는 데 사용됩니다.
간단한 설명	카드의 도구 설명 힌트에 나타나는 통합에 대한 설명입니다.
설명	통합에 대한 더 긴 설명입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 양식 헤더를 마우스 오른쪽 버튼으로 클릭하고 저장을 선택합니다.
   통합 및 구성 관련 목록이 나타납니다. 이 관련 목록을 사용하여 통합에 대한 구성 옵션을 정의할 수 있습니다. 이러한 옵션은 연결된 통합 카드에서 구성 버튼을 클릭할 때 나타납니다.
5. 새로 만들기를 클릭합니다.
6. 양식의 필드에 적절히 입력합니다.

필드	설명
레이블	통합 항목의 이름입니다.
이름	통합을 사용하기 위해 활성화해야 하는 플러그인입니다.
통합	통합 항목을 정의하는 통합을 표시합니다.
순서	이 통합 항목이 나타나는 순서를 나타냅니다.
유형	목록에서 필드 유형을 선택합니다. ○ 문자열 ○ 정수 ○ 10진수 ○ 날짜 ○ 부울 ○ 암호 ○ IPv4 ○ IPv6 ○ URL
값	선택한 유형과 연결된 값을 입력합니다. 선택한 유형에 대해 유효하지 않은 값을 입력하면 통합이 실행될 때 기록이 검색되지 않습니다. 예를 들어 URL 유형을 선택하고 12.32.23.10 값을 입력하면 기록이 검색되지 않습니다.

7. 제출을 클릭합니다.

통합 작성을 위한 팁

다음 가이드라인에 따라 자체 통합을 작성할 때 발생할 수 있는 몇 가지 함정을 방지하십시오.

가능할 때마다 **ServiceNow** 플랫폼 기능을 사용합니다.

대부분 애플리케이션(, , 및)에 보안 운영 내장된 통합 기능은 기존 ServiceNow 플랫폼 통합 기능을 개선하거나 간소화하기 위한 것입니다.취약성 대응위협 인텔리전스보안 인시던트 응답 통합을 작성할 때는 항상 플랫폼 기능이 있으면 해당 기능을 사용해야 합니다. 다음은 "직접 롤링"하는 대신 사용할 수 있는 몇 가지 일반적인 ServiceNow 기능입니다.

- 아웃바운드 웹 서비스 – 외부 공급업체 시스템과의 대부분의 상호 작용에서 통신은 웹 서비스를 통해 이루어집니다. 이러한 경우 플랫폼 아웃바운드 웹 서비스(REST 및 SOAP 지원)를 활용합니다.
- 데이터 소스/임포트 세트/변환 맵 – 데이터를 처리하고 테이블에 삽입 ServiceNow 하기 위해 선호되는 메커니즘은 데이터 소스와 관련 구성요소를 사용하는 것입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

가능할 때마다 보안 운영 통합 프레임워크를 사용합니다.

통합 메커니즘으로 많은 공통적인 문제가 해결되었기 때문에 보안 운영 모든 통합에 대해 기본 기능을 다시 구현할 필요는 없습니다. 예를 들어 취약성 데이터 및 위협 소스 프레임워크는 여러 페이지를 처리하고 해당 데이터를 데이터 소스/변환/임포트 세트로 전달하는 것을 지원합니다. 마찬가지로 스캔 또는 조회 소스 프레임워크는 구성 가능한 요율 제한 기능을 제공합니다. 일반적으로 기능 또는 기능 세트를 구현할 때 기존 보안 운영 통합 프레임워크가 사용 사례를 다루는지 확인합니다. 그렇다면 해당 프레임워크를 사용하십시오.

필요에 따라 기존 보안 운영 통합 프레임워크 확장

통합 프레임워크에서 보안 운영 사용하는 대부분의 테이블과 스크립트는 향후 요구 사항에 맞게 확장될 수 있습니다. 통합을 작성하는 동안 사용 사례가 발생하면 해당 사용 사례에 더 적합하도록 통합 테이블 또는 스크립트를 확장합니다.

통합 중에 발생한 문제에 대해 ServiceNow에 피드백 제공

통합이 개발되거나 테스트되는 동안 문제가 발생할 경우 피드백을 제공해야 합니다. 임시 해결책이 필요한 고객 서비스 및 지원 경우에도 담당자는 향후 릴리스에서 개선하여 향후 통합을 위해 문제를 완화할 수 있습니다.

적정 하중 하에서 시험

통합의 일반적인 문제는 현실적인 로드를 처리할 수 있는 장비가 없다는 것입니다. 각 통합은 범위가 지정된 애플리케이션이므로 시스템 안정성을 보장하기 위해 플랫폼에서 부과하는 더 많은 제한 사항이 있습니다. 이러한 제한으로 인해 장기 실행 작업 또는 API 호출이 종료될 수 있습니다. 각 호출 또는 프로세스에 걸리는 시간을 줄임으로써(일반적으로 API 요청을 페이지 매김하거나 큰 데이터 집합을 청크하는 방법을 제공하여) 장기 실행 프로세스 또는 많은 데이터를 처리하는 프로세스가 정상적으로 처리되도록 할 수 있습니다.

통합 문제 해결

이러한 문제 해결 제안은 통합을 설정하거나 실행할 때 발생할 수 있는 일반적인 문제를 해결하는 데 도움이 될 수 있습니다.

신뢰할 수 없거나 만료된 타사 **SSL** 인증서 교체

통합에 SSL 연결이 필요한 경우 외부 공급업체 벤더가 제공한 인증서를 아직 신뢰 ServiceNow 하지 않거나 만료된 경우가 있습니다. 인증서를 교체하거나 새 인증서를 추가할 수 있습니다.

시작하기 전에
필요한 역할: sn_ti.write

프로시저

1. 외부 공급업체 벤더로부터 SSL 인증서를 받습니다.
   예를 들어, 다음과 같이 Firefox 브라우저의 SSL 엔드포인트에서 X.509 인증서(PEM)를 임포트할 수 있습니다.

   a. 브라우저 주소 표시줄에 엔드포인트 URL을 입력합니다.
   예: https://<3rdparty>/.

   b. 주소란에서 자물쇠 아이콘을 클릭합니다.

   c. 추가 정보를 클릭하고 보안 탭을 클릭합니다.

   d. **View** Certificate(인증서 보기)를 클릭하고 Detail(세부 정보) 탭을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

e. 내보내기를 클릭하여 PEM을 로컬 파일 시스템에 저장합니다.

f. 저장된 파일을 텍스트 편집기 도구에서 열고 내용을 클립보드에 복사합니다.
-----BEGIN CERTIFICATE-----로 시작하고 -----END CERTIFICATE-----로 끝나야 합니다.

2. 다음으로 이동 시스템 정의 〉 인증서.
3. 새로 만들기를 클릭하고 통합에 대한 새 레코드를 생성합니다.
4. **PEM** 인증서에서 이전에 다운로드하여 클립보드에 복사한 인증서를 붙여넣습니다.
5. 저장을 클릭합니다.
기록의 다른 필드는 자동으로 생성됩니다.

통합 역량 프레임워크 2.0

새로운 Integration Capabilities Framework 2.0은 간단하고 일관된 방식으로 통합을 구현할 수 있도록 재설계되었습니다. 이를 통해 유사한 유형의 통합에 대해 일관된 환경이 보장됩니다(예: 옵저버블 평판 조회).

새 프레임워크에는 플로우를 사용하여 구현된 기능이 있습니다.

향상된 프레임워크 구현의 이점은 다음과 같습니다.

- 구현별 로직 없이 비즈니스 수준 구성요소만 포함하는 역량 플로우입니다.
- 이제 기능 플로우는 최대한의 유연성을 위해 광범위한 입력 및 형식 배열(예: 옵저버블 참조, CI 참조, 작업, 모든 테이블 또는 sys_id 조합)을 허용합니다.
- 이제 통합 실행에 대한 속도 제한 또는 제한을 쉽게 구성할 수 있습니다(사용자 지정 코드를 사용하거나 구현 워크플로우를 변경하여 이 작업을 수행할 필요가 없음).
- 향상된 감사 및 실행 추적 기능을 통해 이제 더 나은 보고와 더 쉬운 문제 해결이 가능합니다.
- 강력한 오류 처리 기능이 기능 흐름에 내장되어 구현 루틴의 중복을 방지합니다.
- 역량 또는 통합의 조건부 트리거를 구성하는 능력. 이를 통해 인시던트 범주에 따라 자동화를 자동으로 시작할 수 있는 유연성이 제공됩니다.
- 통합에 입력이 제공되기 전에 허용 목록에 있는 옵저버블을 필터링하는 기본 필터 조건이 모든 기능에 도입되었습니다.

주:
이 새로운 기능 프레임워크는 현재 기능 프레임워크를 업그레이드하지 않습니다. 두 프레임워크는 동시에 작동할 수 있습니다. 새 기능 프레임워크를 활용하는 방법에 대한 지침은 및 플로우에 새 역량 프레임워크 사용를 참조하십시오설치된 통합과 함께 새 기능 프레임워크 사용.

지원되는 통합 및 구성요소

보안 인시던트 응답 플러그인에는 통합 역량 프레임워크 2.0에 나열된 모든 역량 플로우와 요구 사항에 따라 사용하거나 사용하지 않도록 설정할 수 있는 상위 표준 필터가 포함되어 있습니다.

주:
New York 릴리스에서 새 역량 통합 프레임워크를 사용하려면 ServiceNow 통합 허브 Starter Pack Installer 플러그인을 설치해야 합니다. 설치에 대한 지원을 받으려면 고객 지원에 문의하십시오.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

지원되는 애플리케이션 버전

Security Incident Response 10.0부터 다음 통합이 지원됩니다.

애플리케이션	최소 버전 필요
보안 운영 하이브리드 분석 통합	10.0.0
보안 운영 PhishTank 통합	10.0.0
보안 운영 ThreatCrowd 통합	10.0.0
Security Operations CrowdStrike 인텔리전스 통합	10.0.0
보안 운영 '내가 pwned를 받았습니까?' 통합	10.0.0
보안 운영 Metadefender 통합	10.0.0
보안 운영 기록됨 향후 통합	10.0.0
보안 운영 VirusTotal 통합	10.0.0
보안 운영 WhoIs 통합 취소	10.0.0

Security Incident Response 10.4부터 다음 통합이 지원됩니다.

애플리케이션	최소 버전 필요
Security Operations RiskIQ 통합	10.0.0
보안 운영 Shodan 통합	10.0.0
보안 운영 WhoIs 통합	10.0.0
보안 운영 Carbon Black 통합	10.3.1
보안 운영 Splunk 검색 통합	10.3.0
보안 운영 ArcSight 로거 통합	10.3.0
보안 운영 McAfee ESM 통합	10.3.0
보안 운영 Elasticsearch 통합	10.3.0
보안 운영 IBM QRadar 통합	10.3.1
보안 운영 CrowdStrike Falcon 호스트	10.3.0

포함된 구성요소

새로운 역량 통합 프레임워크에는 다음 구성요소가 포함됩니다.

- 기능: 현재 워크플로우로 제품에 존재하는 다음 기능은 모두 플로우를 사용하여 재설계되었습니다.
  - 요청 차단: 방화벽, 웹 프록시 또는 기타 제어 지점의 보안 인시던트와 연관된 옵저버블을 차단하는 방법을 제공합니다. 이 역량은 식별된 위협이 포함되도록 인시던트 응답 조사 중에 사용됩니다.
  - 이메일 검색 및 삭제: 보안 조사 중에 이메일 서버를 검색하고 필요한 경우 서버에서 이메일을 삭제하는 방법을 제공합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 구성 항목 보강: 다양한 소스의 추가 정보로 구성 항목을 보강하는 일반적인 방법을 제공합니다. 이 기능은 인시던트 응답 조사 중에 보안 인시던트와 관련된 데이터를 보강하는 데 사용됩니다.
- 옵저버블 보강: 다양한 소스의 추가 정보로 옵저버블을 보강하는 일반적인 방법을 제공합니다. 이 역량은 식별된 위협이 포함되도록 인시던트 응답 조사 중에 사용됩니다.
- 이벤트 수집: 통합 소스의 이벤트를 보안 인시던트에 매핑하여 보안 인시던트를 생성하는 일반적인 방법을 제공합니다.
- 네트워크 통계 가져오기: 엔드포인트 또는 호스트에서 활성 네트워크 연결 목록을 검색합니다. 이 역량은 조사 중 인시던트 보강에 사용됩니다.
- 실행 중인 프로세스 가져오기: 엔드포인트 또는 호스트에서 실행 중인 프로세스 목록을 검색합니다. 이 역량은 조사 중 인시던트 보강에 사용됩니다.
- 호스트 격리: 보안 인시던트와 연관된 엔드포인트 또는 호스트를 격리하는 방법을 제공합니다. 호스트 격리는 CI(구성 항목)에 대해 실행됩니다.
- 감시 목록에 게시: 보안 이벤트를 모니터링하고 경보를 생성하는 감시 목록에 보안 인시던트와 연관된 옵저버블을 추가하는 방법을 제공합니다. 이 역량은 조사 중에 인시던트 응답의 일부로 사용됩니다.
- 사이팅 검색: 다양한 SIEM 또는 옵저버블의 인스턴스를 저장하는 다른 로그 저장소를 검색합니다. 이 기능은 사용자 환경에 악의적인 IoC가 있는지 확인하는 데 사용됩니다.
- 위협 조회: 위협 인텔리전스 조회를 수행하여 특정 옵저버블이 알려진 보안 위협과 연관이 있는지 여부를 확인합니다. 이 역량은 조사 중에 인시던트 응답의 일부로 사용됩니다.

- 새 테이블:
  - sn_sec_cmn_capability: 역량 및 역량을 구현하는 플로우입니다.
  - sn_sec_cmn_capability_implementation: 역량 서비스를 제공하는 실제 구현 플로우입니다.
  - sn_sec_cmn_capability_execution: 런타임 시 역량에 대한 실행 기록입니다.
  - sn_sec_cmn_capability_implementation_execution: 런타임 시 역량 구현에 대한 실행 기록입니다.
  - sn_sec_cmn_filter_condition: 런타임 시 기능 또는 기능 구현에 적용할 수 있는 필터 조건입니다.
- 스크립트 포함: CapabilityProcessor: 프레임워크에 대한 모든 처리 코드를 처리합니다.
- 요율 제한: 기간당 역량 최대 동시 요청: 병렬로 실행할 수 있는 통합 수를 정의합니다.
- 예약된 작업 프로세스 기능 구현: 15초마다 실행되며 보안 관리 속성 페이지(보안 인시던트 〉 관리 〉 속성.
  - 예약된 작업을 활성화 또는 비활성화합니다. 프로세스 역량 구현: 이 작업은 역량 구현 실행 플로우를 자동으로 예약하고 관리합니다.
  - 자동 조회 또는 보강 활성화 또는 비활성화: 현재 역량 프레임워크에서 옵저버블이 보안 인시던트에 추가될 때 옵저버블의 자동화된 위협 조회 또는 보강을 수행하는 예약된 작업을 활성화하거나 비활성화하는 설정입니다.
  - 예약된 작업인 보안 인시던트 옵저버블 조회를 활성화하거나 비활성화합니다. 이 작업은 옵저버블이 보안 인시던트에 추가될 때 위협 조회 또는 옵저버블 보강 작업을 자동으로 예약합니다.

새 역량 프레임워크의 구성

이 섹션에서는 새 프레임워크에서 사용할 수 있는 구성에 대해 설명합니다.

시작하기 전에

필요한 역할: sn_si.admin, flow_designer, action_designer

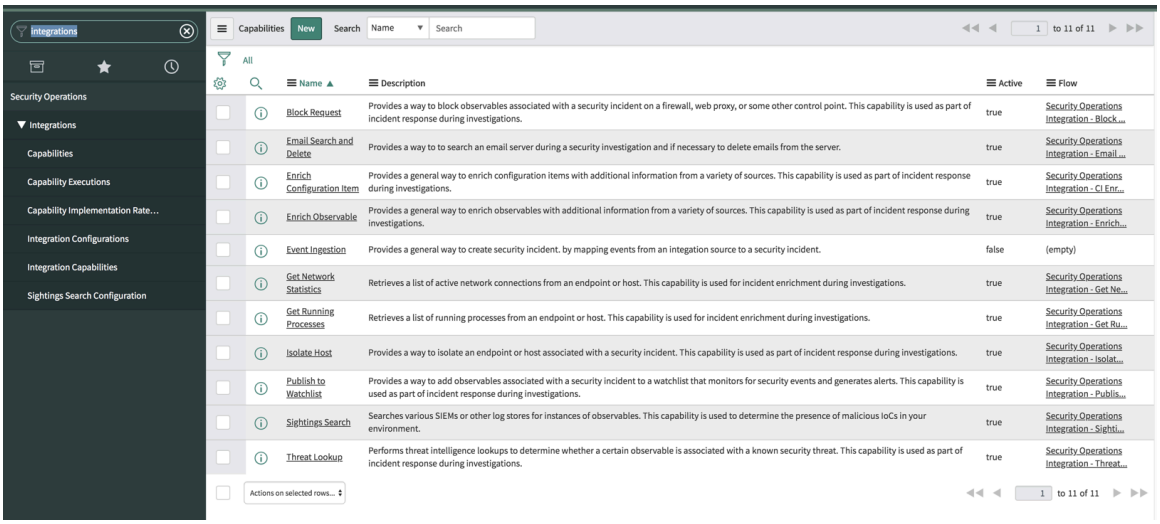
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 〉 보안 운영 〉 통합 〉 역량.

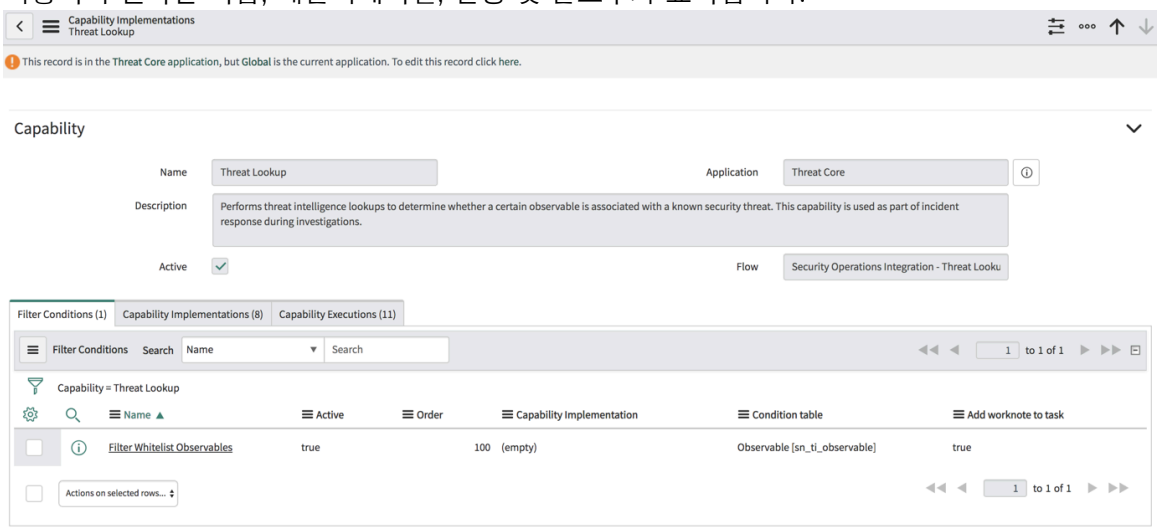
> 주:
> 버전 10.4: Security Incident Response 10.4부터 메뉴 이름이 통합 기능(플로우)으로 변경되었습니다.

2. 기본 시스템에서 사용할 수 있는 기능이 표시됩니다.



> 주:
>
> 기본 시스템과 함께 제공되는 기능입니다. 기능을 사용하거나 필요에 따라 사용자 지정할 수 있습니다. 다음 단계에서는 기능을 구성하는 방법과 기능에 대해 구현된 통합을 설명합니다.

3. 이름 열의 링크를 클릭하여 역량을 구성합니다.
역량이 구현하는 이름, 애플리케이션, 설명 및 플로우가 표시됩니다.

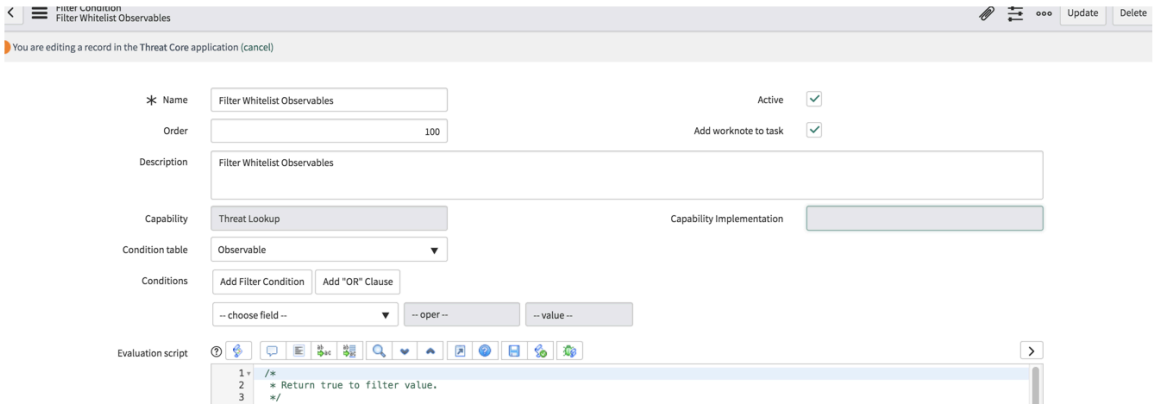


4. 활성 확인란을 선택하여 기능을 활성화합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 역량 수준의 필터 조건: 통합 역량이 플로우를 구현하면 역량 플로우가 시작되기 전에 플로우와 연결된 필터 조건이 실행됩니다. 예를 들어 위협 조회 기능에는 위와 같이 허용 목록에 추가된 옵저버블 필터링 조건이 포함됩니다. 이름 링크를 클릭하여 필터 조건을 편집합니다.

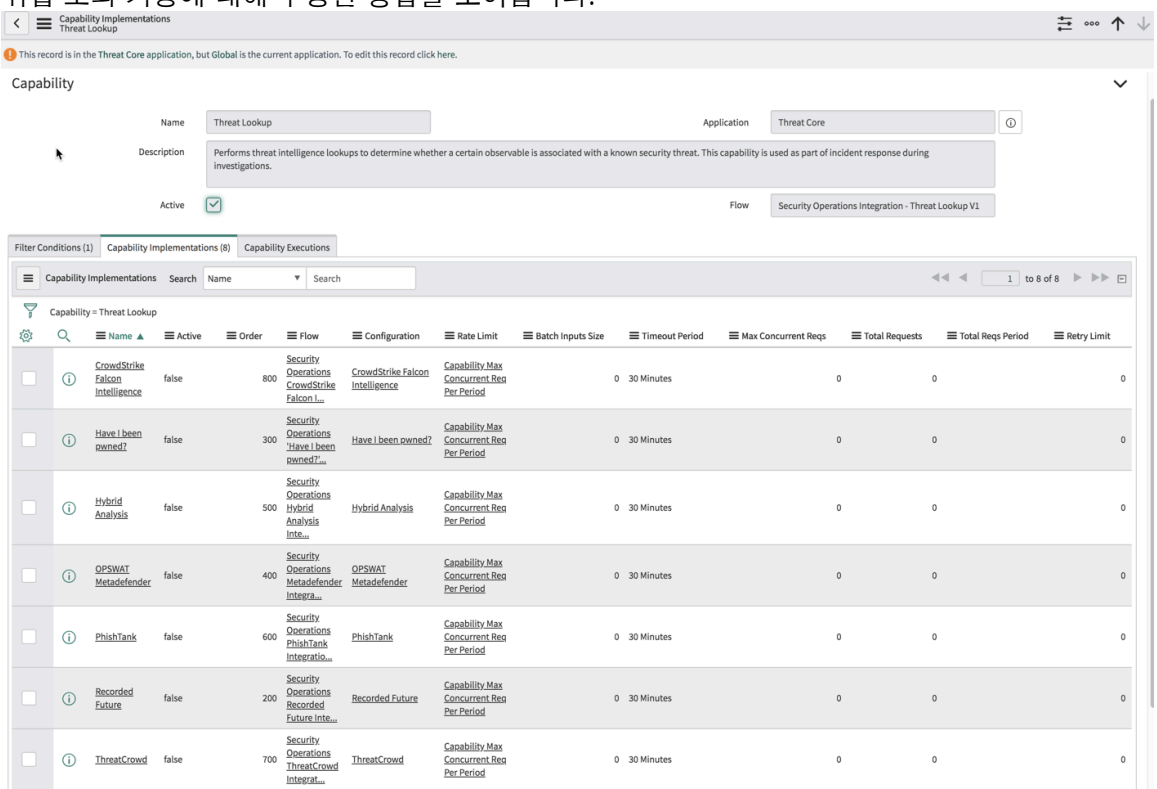
  주:
  작업에 작업 메모 추가 확인란을 선택하여 작업 메모를 추가하고 사용된 필터 조건에 대한 정보를 포함합니다.



필터 조건이나 스크립트 또는 둘의 조합을 정의할 수 있습니다. 위 예시에서는 스크립트를 사용하여 필터 조건을 정의합니다. 역량 플로우가 실행되면 스크립트는 허용 목록에 추가된 옵저버블을 검색하여 테이블에서 제거합니다.

  주:
  여기에 설정된 필터 조건은 역량 구현 탭에 정의된 모든 활성 통합에 적용할 수 있습니다.

- 역량 구현: 역량 구현 탭을 클릭합니다. 역량에 대해 구성된 구현(통합)이 표시됩니다. 아래 예는 위협 조회 기능에 대해 구성된 통합을 보여줍니다.

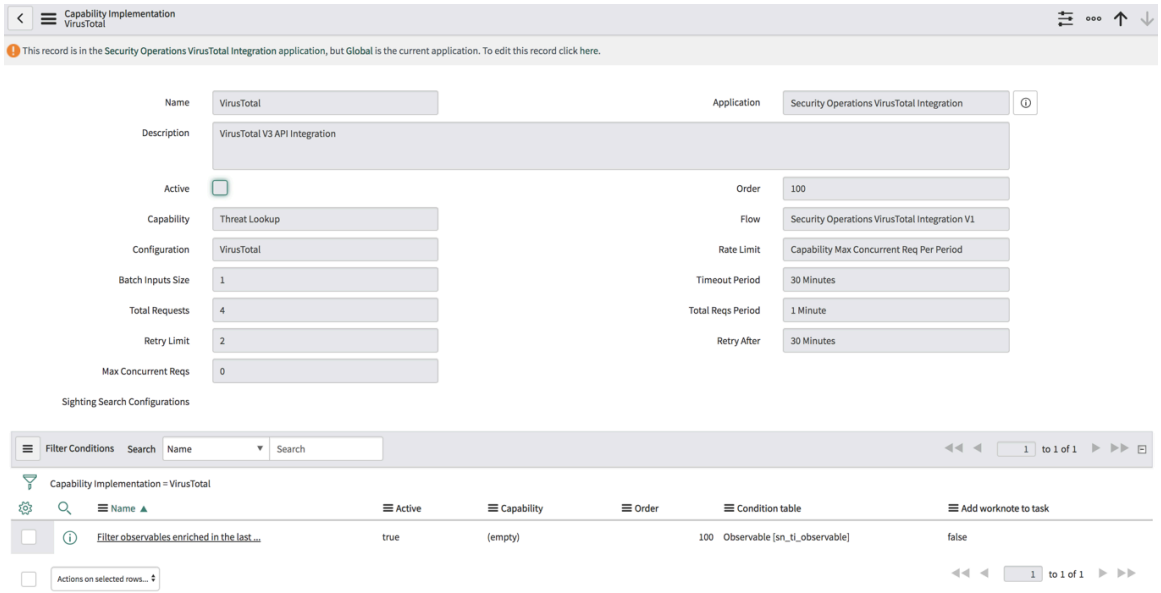


5. 이름 링크를 클릭하여 역량 구현을 봅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

역량이 구현하는 이름, 애플리케이션, 설명 및 플로우가 표시됩니다.

6. 활성 확인란을 클릭하여 기능을 활성화합니다.



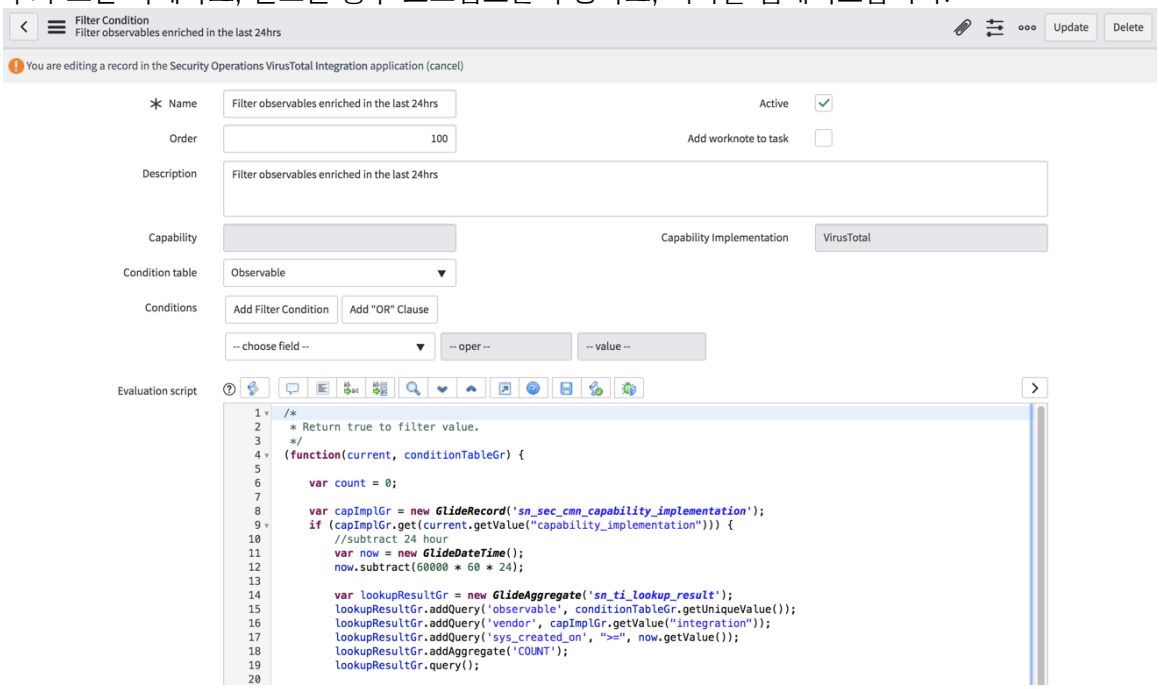
다음과 같은 상세 정보를 지정할 수 있습니다.

필드 이름	설명
활성	이 통합을 사용하지 않도록 설정하려면 이 확인란을 선택합니다. **주:** 의 통합 타일을 사용하여 이 통합을 구성하는 경우 보안 운영 〉 통합 〉 통합 구성페이지에서 이 플래그는 활성으로 자동 설정됩니다.
순서	통합이 실행되는 순서를 나타냅니다.
역량	이러한 통합을 통해 구현되는 역량입니다.
플로우	역량을 구현하는 하위 플로우입니다.
구성	이 역량에 대한 통합 구성입니다. **주:** 처음에는 기본 시스템에 제공된 기본 구성으로 설정됩니다. 통합 구성 페이지에서 통합 타일을 사용하여 통합을 구성하는 경우 이 값은 생성된 새 구성으로 자동으로 재설정됩니다.
속도 제한	런타임에 실행할 수 있는 통합 수(병렬 또는 시간 단위당)를 나타냅니다.
배치 입력 크기	각 실행에 대한 배치 입력 크기입니다. 예를 들어 사이팅 검색 통합의 경우 생성된 쿼리가 너무 커지지 않도록 옵저버블을 50개의 배치로 그룹화할 수 있습니다. 0은 제한이 없음을 나타냅니다.
시간 초과 기간	역량 구현 플로우가 취소되기 전의 최대 기간입니다. 0은 시간 초과 기간이 없음을 나타냅니다.
요청한 총 수	총 구현 실행 요청 수입니다. 이 필드는 총 요청 기간 필드와 함께 서비스에 대한 요청 수를 제한하는 데 사용할 수 있습니다. 예를 들어 분당 요청 수를 4개로 제한할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드 이름	설명
총 요청 기간	기간당 허용되는 총 실행 요청 수입니다.
재시도 제한	실패한 실행 요청에 허용되는 재시도 횟수입니다. 이 제한은 조건이 충족될 때 실행 요청을 재시도하도록 통합에 재시도 플래그가 설정된 경우에 적용할 수 있습니다. 예를 들어, 일정 기간 동안 해당 서비스에 대한 라이센스 한도를 초과했거나 서비스가 다운되면 재시도 요청이 수행됩니다.
다음 이후에 다시 시도	실패한 실행 요청을 다시 시도하기 위한 기간입니다.
최대 동시 요청	동시 구현 실행 요청의 최대 수입니다. 0은 제한이 없음을 나타냅니다.
사이팅 검색 구성	실행할 수 있는 기본 사이팅 검색 쿼리입니다.

필터 조건 섹션에서 이름 링크를 클릭하여 구현에 대해 정의된 조건을 구성합니다. 필터 조건을 추가 또는 삭제하고, 필요한 경우 스크립트를 수정하고, 기록을 업데이트합니다.



설치된 통합과 함께 새 기능 프레임워크 사용

이 섹션에서는 기존 통합에 새 기능 프레임워크를 사용하는 방법을 설명합니다.

아래 단계를 사용하여 이미 설치되고 구성된 통합을 활성화(지원되는 지원되는 통합 및 구성요소통합 목록 참조)하여 새 역량 프레임워크를 사용하십시오.

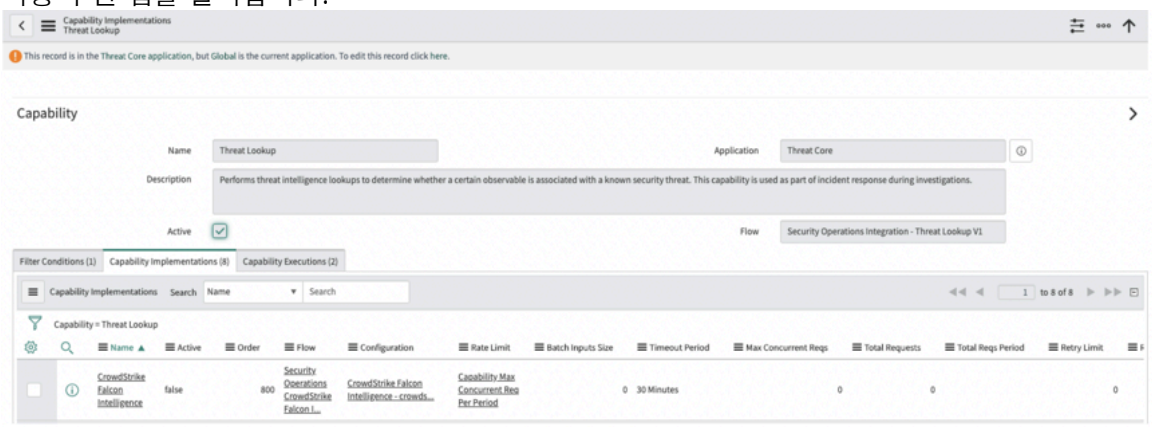
> **주:**
> Security Incident Response 10.0.2와 함께 사용할 수 있는 Integration Capability Framework 2.0은 위협 조회 및 옵저버블 보강 기능의 구현을 지원합니다. 다른 기능에 대한 구현은 향후 릴리스에서 제공될 예정입니다.

시작하기 전에

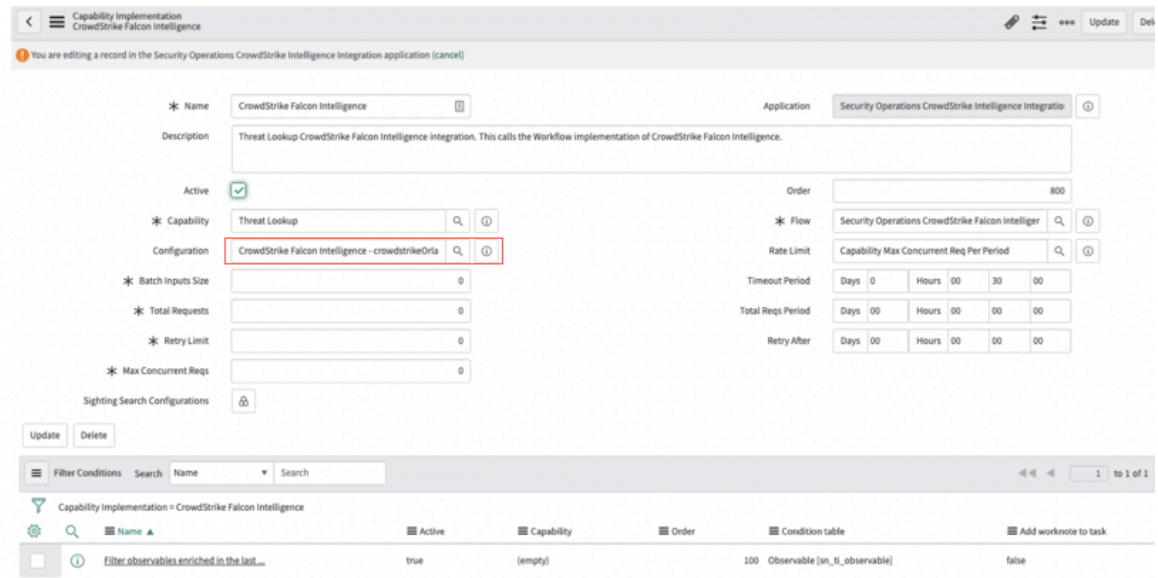
- 필요한 역할: sn_si.admin
- 보안 인시던트 응답 10.0.2

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

1. 다음으로 이동 보안 운영 〉 통합 〉 역량.
2. 위협 조회 기능을 클릭합니다.
3. 역량 구현 탭을 클릭합니다.

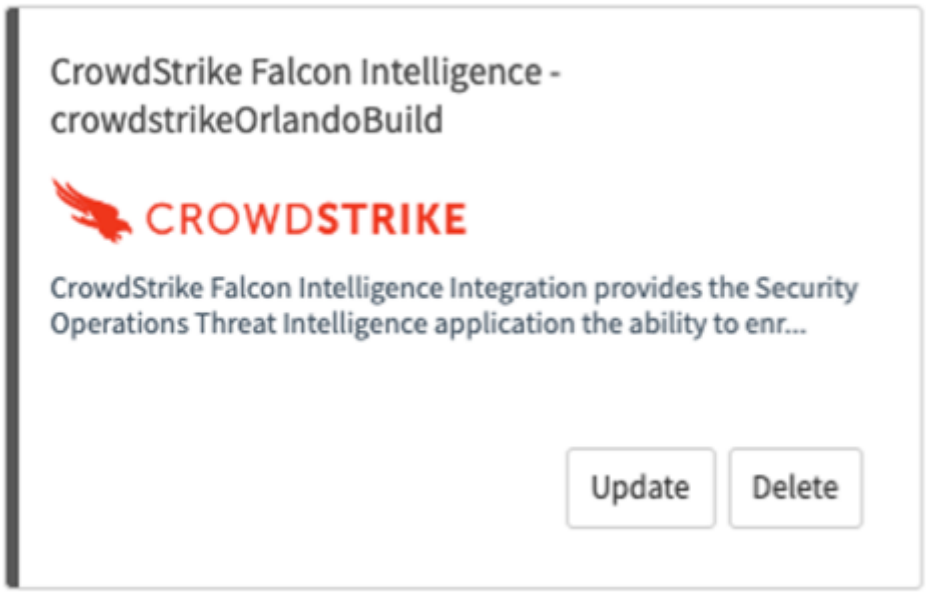


4. 4. 관심 통합에 대한 역량 구현 기록을 봅니다(예: Crowdstrike Falcon Intelligence). 활성 열의 값은 **False**여야 합니다.
5. 이름 링크를 클릭하여 구현 기록을 봅니다.



6. 활성 확인란을 선택합니다.
7. 구현 기록이 올바른 구성 기록(의 통합에 대한 타일 이름)을 가리키는지 확인하십시오. 통합 구성 〉 구성 표시(예)).

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



8. 새 프레임워크에서 사용할 수 있도록 구현이 활성화됩니다.

주:
Security Incident Response 10.0.2와 함께 설치되면 지원되는 모든 통합이 새 통합 기능 프레임워크에서 자동으로 활성화됩니다.

플로우에 새 역량 프레임워크 사용

아래 단계를 사용하여 플로우를 생성하고 새 역량 프레임워크에서 제공하는 하위 플로우를 호출합니다.

시작하기 전에

- 필요한 역할: sn_si.admin, flow_designer, action_designer
- 지원되는 통합 중 하나를 설치합니다(지원되는 통합 및 구성요소

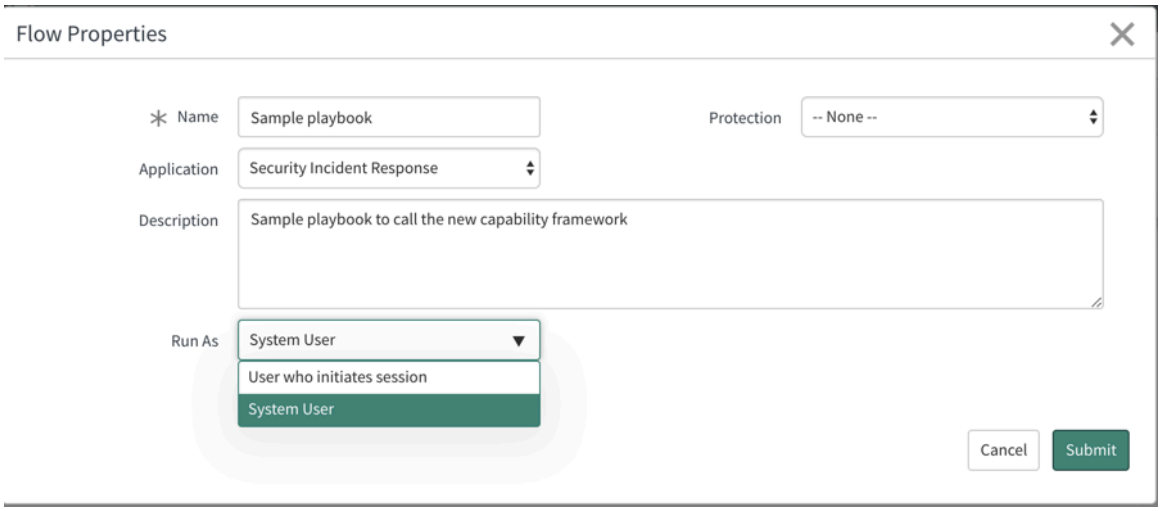
아래 단계에서는 샘플 플로우를 만들고 새 역량 프레임워크와 함께 제공되는 하위 플로우 중 하나를 호출하는 방법을 설명합니다.

프로시저

1. 다음으로 이동 모두 〉 플로우 디자이너 〉 디자이너.

2. 새로 만들기를 클릭하여 새 플로우를 만들고 속성에 필요한 정보를 제공합니다.

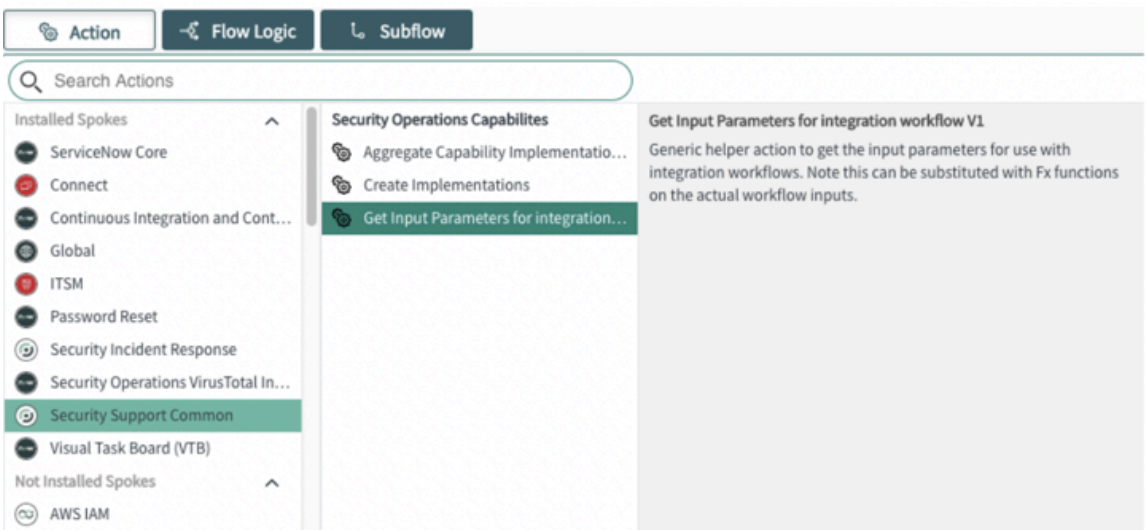
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



주:
위의 이미지에 표시된 대로 Run As 선택 목록에서 **System User** 를 선택합니다.

3. 플로우에 대한 트리거 조건을 선택합니다(일반적인 트리거는 특정 인시던트 범주에 대한 보안 인시던트 기록 생성).

4. 플로우의 1단계에서 보안 인시던트에서 입력을 가져오는 작업(예: 옵저버블)을 선택합니다. 보안 지원 공통 스포크가 있는 기본 시스템과 함께 제공되는 작업 중에서 작업을 선택할 수 있습니다.



5. 2단계에서 하위 플로우(예: 위협 조회)를 선택합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

6. 아래와 같이 선택한 하위 플로우를 구성합니다.

7. 플로우를 저장하고 게시합니다.

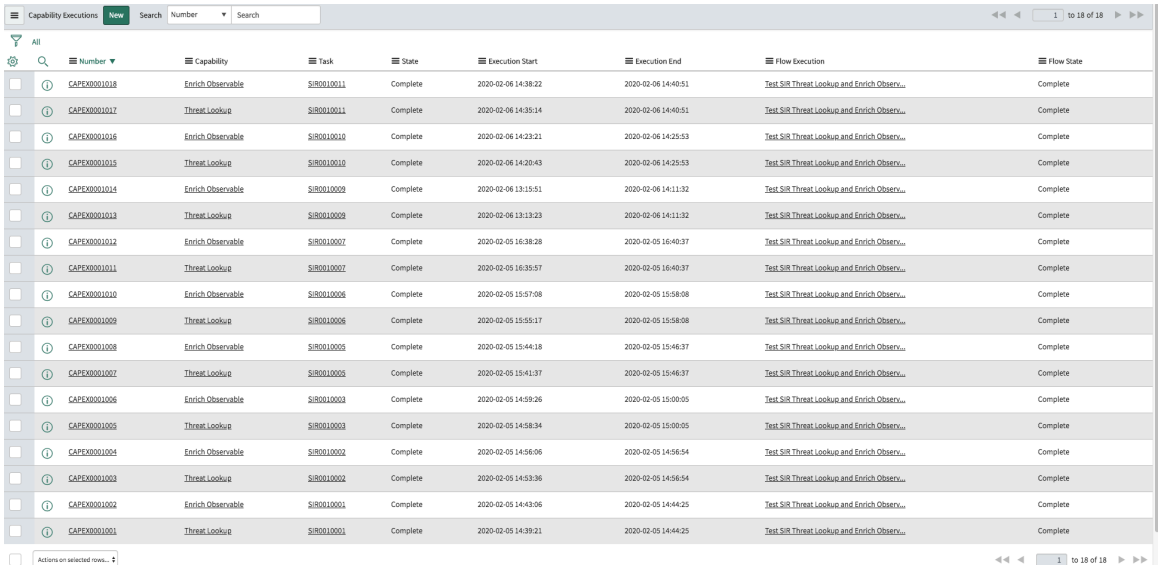
통합 역량 플로우 문제 해결

기능 실행 옵션은 실행된 각 기능에 대한 자세한 정보를 제공합니다.

주:
완료된 실행은 30일 후에 보관됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

1. 다음으로 이동 보안 운영 〉 통합 〉 역량 실행.



2. 역량 실행 링크를 클릭하여 추가 상세 정보를 봅니다.

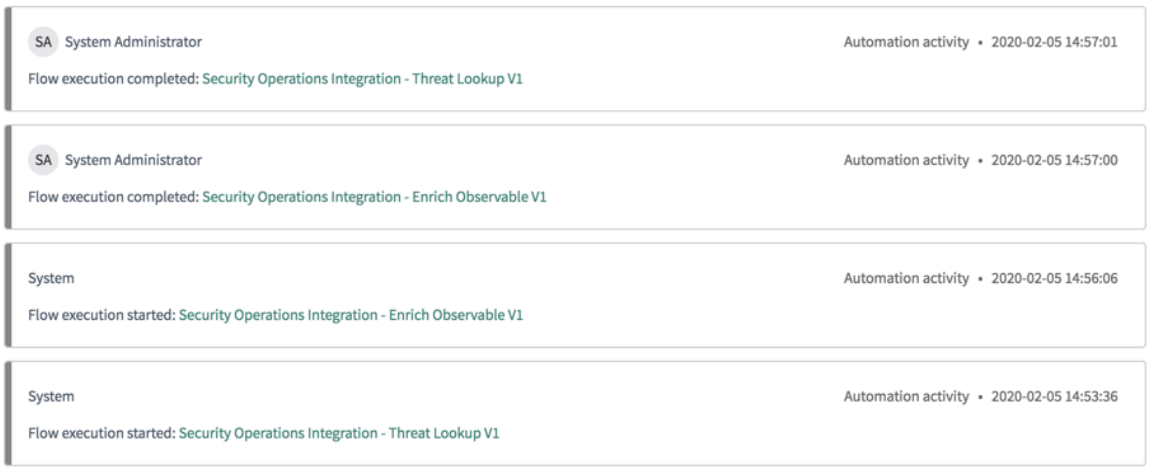
##

옵저버블이 보안 인시던트에 추가되고 플로우에 대한 트리거 조건이 충족되면 위협 조회 및 옵저버블 보강 하위 플로우가 시작되고 다음 작업 메모가 보안 인시던트에 추가됩니다.

- 플로우 실행 시작: 보안 운영 통합 - 옵저버블 보강 V1
- 플로우 실행 완료: 보안 운영 통합 - 옵저버블 보강 V1
- 플로우 실행 시작: 보안 운영 통합 – 위협 조회 V1
- 플로우 실행 완료: 보안 운영 통합 - 위협 조회 V1

이러한 작업 메모를 보려면 *sn_si.admin* 또는 *sn_si.analyst*, *flow_designer* 및 *action_designer* 역할을 가진 사용자로 로그인합니다.

보안 인시던트 기록 페이지로 이동하고 이러한 작업 메모를 클릭하여 플로우 실행 세부 정보를 봅니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 운영과 외부 공급업체 통합을 위한 **REST API**

기본 시스템에는 보안 운영 고객과 파트너가 기존 보안 운영 배포와 쉽게 통합할 수 있도록 하는 일련의 스크립팅된 REST API가 포함되어 있습니다. API를 사용하면 시스템 외부에서 데이터를 수집하고(예: Python 스크립트를 사용하여 VirusTotal에서 데이터를 수신함) 인스턴스로 다시 보낼 수 있습니다.

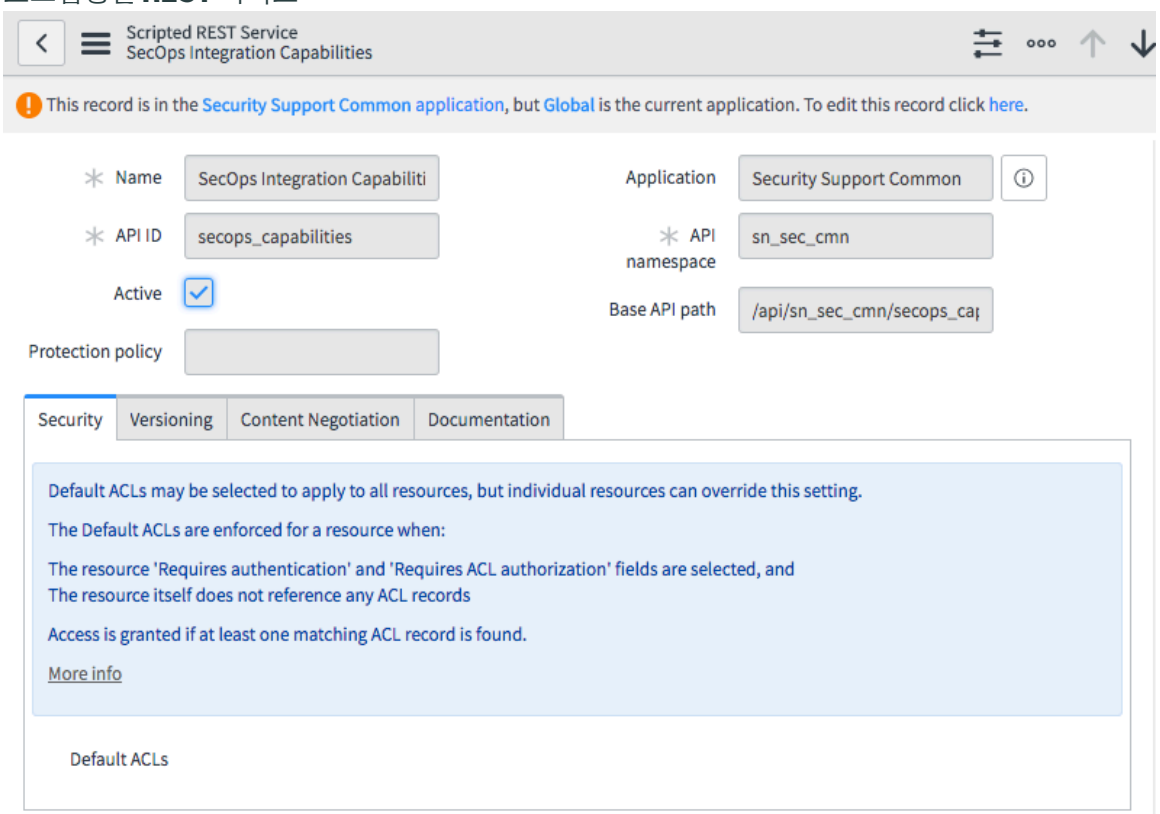
거의 모든 언어(예: Python)로 작성된 스크립트를 API와 함께 사용하여 고객별 프로세스를 수행할 수 있습니다. 스크립트는 외부 연결 HTTP Post 호출을 수행할 수 있는 언어로 작성되어야 합니다. 예를 들어 Java 애플리케이션이 있는 경우 java.net.HttpUrlConnection 패키지와 같은 라이브러리를 사용하여 HTTP 호출을 구성하고 JSON 문자열을 메시지의 본문으로 전달해야 합니다.

API는 시스템 외부에서 수집된 데이터를 추가하는 데만 사용됩니다. 예를 들어, VT python 스크립트를 입력하고 VT에서 데이터를 받은 경우 해당 데이터를 SN 인스턴스로 다시 보낼 수 있습니다.

인증

API 정의 내의 모든 작업은 에서 제공하는 플랫폼 인증을 사용합니다. 스크립팅된 REST API 작업 기능. 액세스하려면 다음으로 이동하십시오. 시스템 웹 서비스 〉 스크립트 기반 웹 서비스 〉 스크립트 기반 **REST API** 를 클릭하고 **SecOps** 통합 기능 API를 찾습니다.

스크립팅된 **REST** 서비스



사용자와 사용자의 도메인은 API의 컨텍스트 내에서 쉽게 사용할 수 있습니다. 기록을 사용자와 연결하고, 감사 경로를 설정하고, 도메인 분리를 수행할 수 있습니다. 또한 특정 사용자로 인증되었으므로 GlideRecordSecure를 사용하여 데이터에 대한 무단 액세스를 방지합니다.

권한 부여

애플리케이션 외부의 보안 운영 사용자로부터 레코드 생성 프로세스를 보호하려면 sn_sec_cmn.api_write 역할이 있어야 합니다. 이 역할을 가진 사용자만 API에 액세스할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

구성 요청 매개변수

다음과 같은 요청 매개변수를 사용할 수 있습니다.

이름	기본값	설명
ignore_mandatory_fields	아니오	true로 설정하면 필수 필드가 채워지지 않아도 기록이 유지됩니다.
include_wrap	아니오	true로 설정된 경우 응답에는 스크립팅된 REST API에 대한 인스턴스 제공 표준 래퍼가 포함됩니다.
simple_response	아니오	true로 설정하면 응답에 작업의 성공 여부만 포함됩니다.

오류 응답

다음과 같은 오류 응답이 발생할 수 있습니다.

오류 메시지	언제 발생합니까?	솔루션
접근 권한이 부족함	사용자에게 sn_sec_cmn.api_write 역할이 없습니다.	사용자에게 역할을 추가합니다.
잘못된 게시 본문	요청 본문이 비어 있거나 빈 객체입니다.	API 정의를 따릅니다.
제공된 필드 없음	유지하기 위해 제공된 데이터 필드가 비어 있습니다.	API 정의를 따릅니다.
필수 필드 누락됨: x,y,z	필수 필드가 누락되었습니다.	대상 테이블의 테이블 정의를 따르거나 **ignore_mandatory_fields** true로 설정합니다.
기록을 지속할 수 없음	구문 분석된 기록을 유지할 수 없습니다.	GlideRecord insert()가 실패했습니다. 추가 분석이 필요합니다.
알 수 없는 오류	알려진 오류 경로를 따르지 않은 경우 발생합니다.	추가 분석이 필요합니다.

CI 보강 사용 사례

타사 스크립트를 사용하여 CI 보강을 위해 구성 항목 보강[sn_sec_cmn_ci_enrichment_result] 테이블에 쓸 수 있습니다. 보강 기록은 외부 공급업체 소스의 기록에 대한 자세한 정보를 제공하는 기존 기능을 기반으로 합니다.

CI 보강 사용 사례에 대한 샘플 요청 및 응답이 여기에 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

생성-CI 보강 요청

```
{
   "ignore_mandatory_fields": true,
   "payload": [
      {
         "configuration_item_id": "2dfd7c8437201000deeabfc8bcbe5d56",
         "data": [
             {
               "external_link": "http://www.servicenow.com",
               "vendor": "aafbf46ad72212007a6de294de6103a2",
               "data_type": null,
               "source": null,
               "name": null,
               "parent": null,
               "summary": "Found 1000 open vulnerabilities on the specified
               configuration item",
               "retrieval_date": "2017-09-05 08:56:28"
             }
          ]
      }
   ]
}
```

생성-CI 보강을 위한 응답

```
{
   "success": true,
   "status": "success",
   "payload": {
        "results": [
            {
                "sys_id": "2dfd7c8437201000deeabfc8bcbe5d56",
                "reference_url":
                "http://10.0.214.15:8080/nav_to.do?uri=cmdb_ci.do?sys_id=2dfd7c8437201000
                deeabfc8bcbe5d56",
                    "results": [
                        {
                            "sys_id": "4a8b92fb0b410300263a089b37673a33",
                            "reference_url":
                            "http://10.0.214.15:8080/nav_to.do?uri=sn_sec_cmn_ci_
                        enrichment_result.do?sys_id=4a8b92fb0b410300263a089b37673a33"}
                    ]
                }
            ],
            "domain": "global",
            "configuration_item_ids": [
            "2dfd7c8437201000deeabfc8bcbe5d56"
        ]
    }
}
```

옵저버블 보강 사용 케이스

외부 공급업체 스크립트를 사용하여 옵저버블 보강을 위해 옵저버블 보강 결과 [sn_ti_observable_enrichment_result] 테이블에 쓸 수 있습니다. 보강 기록은 외부 공급업체 소스의 기록에 대한 자세한 정보를 제공하는 기존 기능을 기반으로 합니다.

옵저버블 보강 사용 사례에 대한 샘플 요청 및 응답이 여기에 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

생성-옵저버블 보강 요청

```
"ignore_mandatory_fields": true,
  "payload": [
    {
      "observable_value": "http://www.google.com",
      "security_incident_ids": [
        "9424d4e10b110300263a089b37673a21"
      ],
      "enrichment_mapping_id": "9fa7d4590b622200263a089b37673a1d",
      "data": [{
        "vendor": "f15a46140b622200263a089b37673a7e",
        "summary": "Registrar:MarkMonitor, Inc., Registration Date:1997-09-15,
            Expiration Date:2020-09-14, Registrant country:UNITED STATES",
        "data_type": "json",
        "retrieval_date": "2017-08-30 10:35:02",
        "raw_data": "{\"WhoisRecord\":{\"administrativeContact\":{\"city\":
            \"Mountain View\",\"country\":\"UNITED STATES\",\"email\":
            \"dns-admin@google.com\",\"fax\":\"16506188571\",\"name\":
            \"DNS Admin\",\"organization\":\"Google Inc.\"}"
      }]
    }
  ]
}
```

옵저버블 보강을 위한 **Create-Response**

```
{
    "success": true,
    "status": "success",
    "payload": {
        "results": [
            {
                "sys_id": "43bd3f210b510300263a089b37673ac6",
                "reference_url": "http://10.0.65.185:8080/sn_ti_observable.do?
                    sys_id=43bd3f210b510300263a089b37673ac6&sys_target=&XML",
                "results": [
                    {
                        "sys_id": "0bbd3f210b510300263a089b37673acc",
                        "reference_url": "http://10.0.65.185:8080/sn_ti_observable_
                            enrichment_result.do?sys_id=0bbd3f210b510300263a089b37673acc
                                &sys_target=&XML"
                    }
                ]
            }
        ],
        "domain": "global",
        "observable_ids": [
            "43bd3f210b510300263a089b37673ac6"
        ]
    }
}
```

주:
기존 기록을 보강하는 것 외에도 기존 보강 매핑에 대한 **enrichment_mapping_id**와 매핑 프로세스로 구문 분석할 수 있는 해당 **raw_data** 문자열을 전달하여 테이블에 새 기록을 추가하는 데 사용할 보안 운영 보강 데이터 매핑 수도 있습니다.

위협 조회 사용 케이스

타사 스크립트를 사용하여 위협 조회 결과에 대한 위협 조회 결과 [sn_ti_lookup_result] 테이블에 쓸 수 있습니다. 조회 기록은 외부 공급업체 소스의 기록에 대한 자세한 정보를 제공하는 기존 기능을 기반으로 합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

위협 조회 사용 사례에 대한 샘플 요청 및 응답은 다음과 같습니다.

생성-위협 조회 요청


```
{
"simple_response": false,
"include_wrapper": true,
  "ignore_mandatory_fields": false,
  "payload": [
    {
      "request_element_correlation_id": "1",
      "observable_value": "128.214.67.80",
      "data": [
        {
          "request_element_correlation_id": "2",
          "finding": "Malicious6",
          "source_engine": "VirusTotal API",
          "vendor": "aafbf46ad72212007a6de294de6103a2",
          "data_type": null,
          "source": null,
          "name": null,
          "parent": null,
          "retrieval_date": "2017-09-05 08:56:28",
          "external_link": "https://www.virustotal.com/en/ip-address/41.79.173.47/
            information/"
        },
        {
          "finding": "Malicious8",
          "source_engine": "VirusTotal API",
          "source_engine_version": "v2",
          "first_found": "2000-09-05 15:56:28",
          "parent": null,
          "retrieval_date": "2017-09-05 08:56:28",
          "external_link": "https://www.virustotal.com/en/ip-address/41.79.173.47/
            information/"
        }
      ]
    }
  ]
}
```


© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

위협 조회를 위한 **Create-Response**


```
{
    "success": true,
    "status": "success",
    "payload": {
        "results": [
            {
                "sys_id": "a0bddafb0b410300263a089b37673a93",
                "reference_url":
                    http://10.0.214.15:8080/nav_to.do?uri=sn_ti_observable.do?sys_id=
                        a0bddafb0b410300263a089b37673a93,
                    "request_element_correlation_id": "1",
                    "results": [
                        {
                            "sys_id": "24bddafb0b410300263a089b37673a95",
                    "reference_url":
                        http://10.0.214.15:8080/nav_to.do?uri=sn_ti_lookup_result.do?sys
                            _id=24bddafb0b410300263a089b37673a95,
                    "request_element_correlation_id": "2",
                },
                {
                    "sys_id": "e8bddafb0b410300263a089b37673a96",
                    "reference_url":
                        http://10.0.214.15:8080/nav_to.do?uri=sn_ti_lookup_result.do?
                            sys_id=e8bddafb0b410300263a089b37673a96
                            }
                        ]
                    }        ],
                "domain": "global",
                "observable_ids": [
                    "a0bddafb0b410300263a089b37673a93"        ]
    }
}
```


통합 역량

프레임워크는 통합 기능 외부 공급업체 통합과의 상호 운용성을 지원하는 일관된 아키텍처를 제공합니다. 이렇게 추상화된 인터페이스와 데이터 모델은 핵심 애플리케이션의 변경으로부터 통합을 격리하고 유사한 유형의 통합에 대해 일관된 환경을 보장합니다.

각 통합 기능은 통합 기능 [sn_sec_cmn_integration_capability] 테이블에 유지됩니다. 통합 역량 플로우는 단독으로 실행할 수 없으며 구현 플로우를 시작해야 합니다. 기능 구현을 제공하는 모든 플러그인은 하위 테이블인 통합 기능 구현 [sn_sec_cmn_integration_capability_implementation]에 구현을 추가합니다.

구현에서는 실행할 플로우, 관련 통합(플러그인 ID) 및 구현하는 기능을 지정합니다. 이러한 흐름은 병렬 흐름 시작 관리자를 사용하여 병렬로 실행할 수 있습니다. 그러나 순차 실행은 기본 시스템에서 기본값입니다. 필요한 경우 실행 순서를 변경할 수 있습니다.

주:
사용 가능한 구현이 없으면 역량 작업이 제품 메뉴에 표시되지 않습니다.

보안 운영 통합 - 차단 요청 기능

차단 작업 기능은 구현 플로우를 사용하여 방화벽, 웹 프록시 또는 기타 제어 지점의 보안 인시던트와 연관된 옵저버블을 차단합니다. 이 역량은 식별된 위협이 포함되도록 인시던트 응답 조사 중에 사용됩니다.

차단 요청 역량에는 차단 요청을 실행하는 플로우 Security Operations Integration - 요청 플로우 차단가 있습니다. 이 플로우는 옵저버블 목록을 수락하고, 구현 역량을 찾고, 구성된 플로우에 따라 요청을 실행합니다.

주:
사용 가능한 구현이 없으면 역량 작업이 제품 메뉴에 표시되지 않습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

차단 요청 실행

보안 인시던트와 관련된 옵저버블과의 통신을 차단합니다.

시작하기 전에

필요한 역할: sn_si.analyst

이 태스크 정보

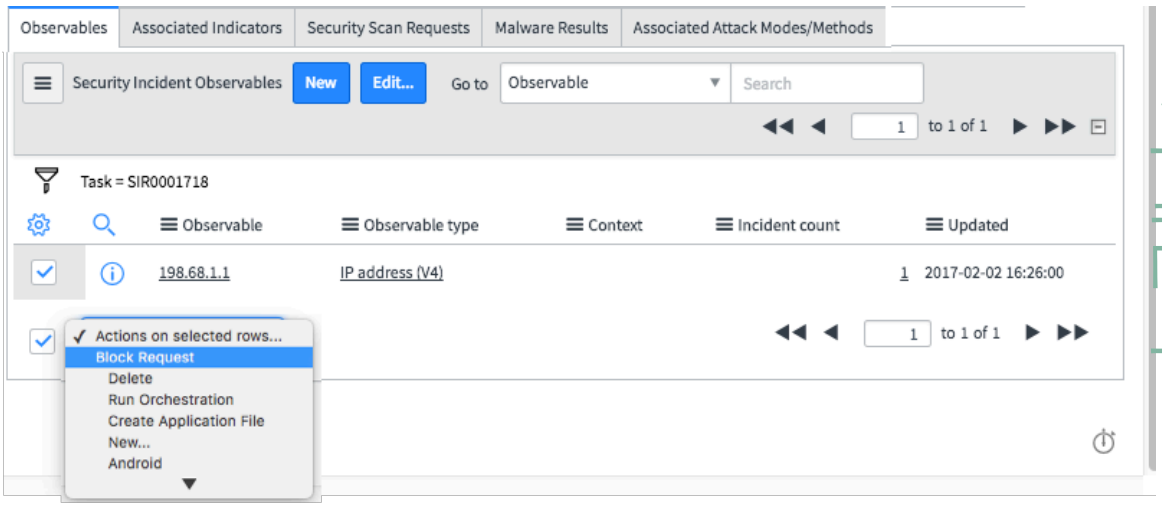
주:
사용 가능한 구현이 없으면 역량 작업이 제품 메뉴에 표시되지 않습니다.

보안 운영 통합 - 차단 요청 플로우는 옵저버블 양식 또는 보안 인시던트의 보안 인시던트 옵저버블 관련 목록에서 트리거될 수 있습니다.

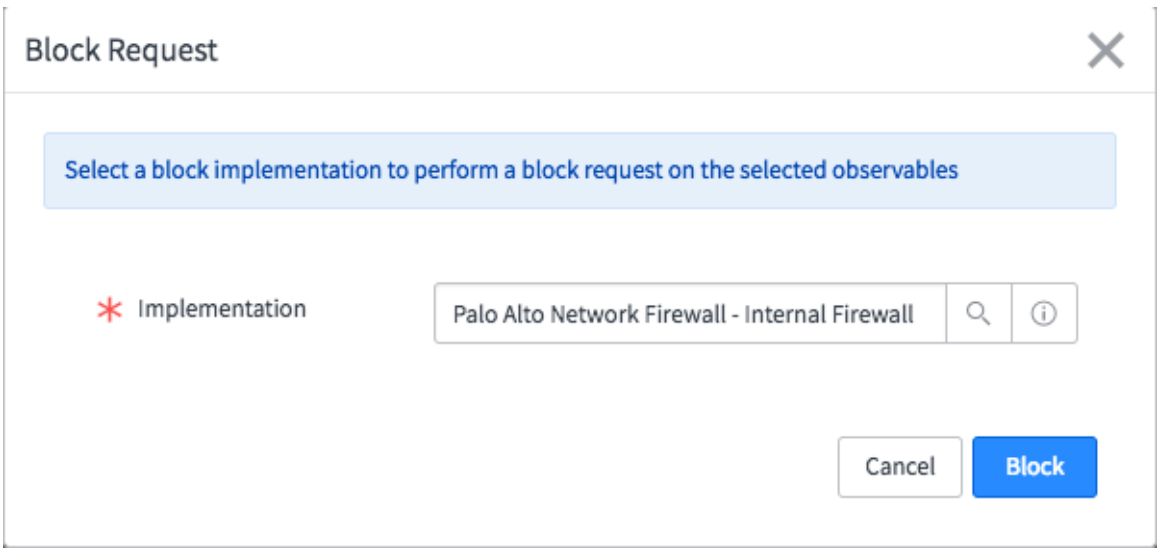
이 예시에서는 보안 인시던트의 차단 요청을 보여줍니다.

프로시저

1. 보안 인시던트로 이동합니다.
2. 관련 목록 탭에서 옵저버블을 선택합니다.
3. 선택한 행에 대해 수행할 작업... 드롭다운 메뉴에서 요청 차단을 클릭합니다.

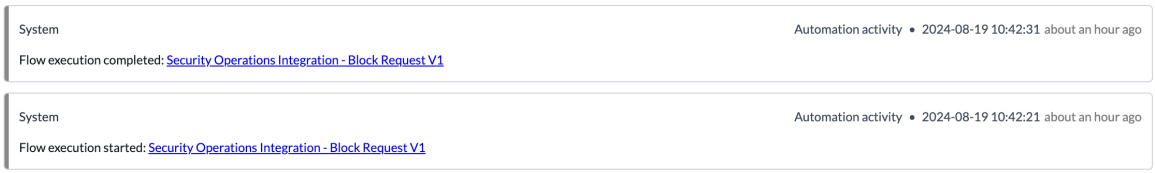


대화 상자가 나타납니다.



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 구현을 선택합니다.
5. 차단을 클릭합니다.
   플로우 실행 감사가 작업 메모 섹션에 표시됩니다.

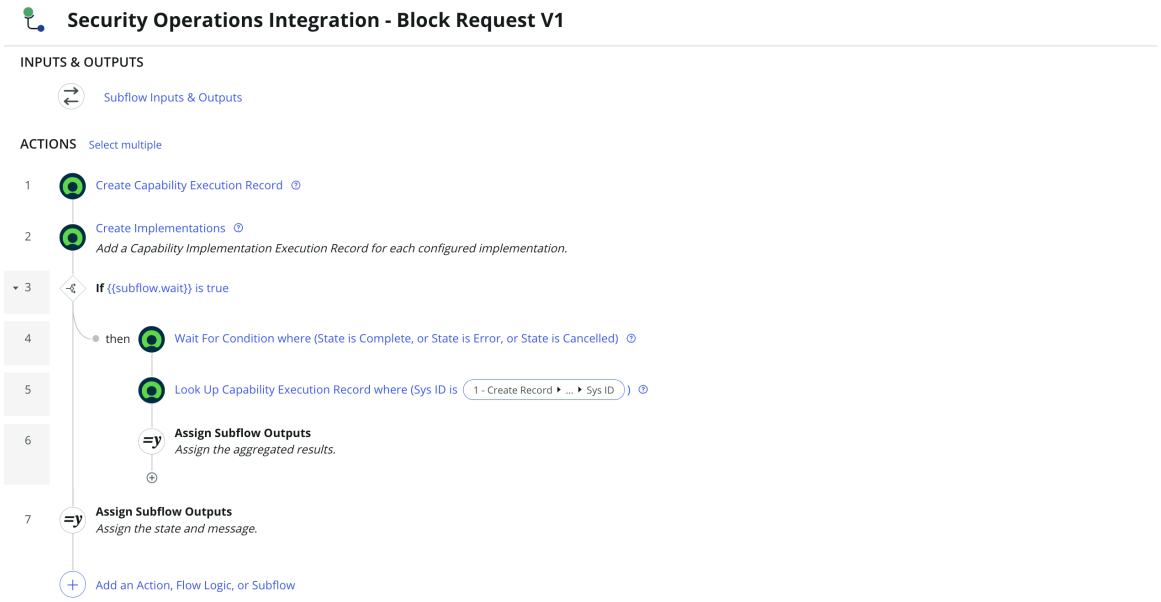


Security Operations Integration - 요청 플로우 차단

보안 운영 통합 - 차단 요청 플로우는 통합과 독립적인 상위 수준 플로우입니다. 보안 인시던트와 관련된 옵저버블을 차단합니다. 이를 사용하여 와 같은 Palo Alto Networks - Firewall통합을 수행합니다.

보안 운영 통합 **-** 차단 요청 플로우는 옵저버블 양식에서 트리거되거나 보안 인시던트의 보안 인시던트 옵저버블 관련 목록에서 트리거될 수 있습니다. 목록에서 드롭다운 작업 메뉴에 있습니다. 양식에서는 관련 링크입니다. 요청 차단은 요청 차단 기능에 대한 구현이 설치된 경우에만 사용할 수 있습니다.

요청 차단



이 플로우와 관련된 작업은 여기에 설명되어 있습니다. 다른 작업에 대한 자세한 내용은 다음 문서를 참조하십시오 일반 Security Operations 통합 플로우 및 오케스트레이션 활동.

보안 운영 통합 **-** 이메일 검색 및 삭제 기능

이메일 검색 및 삭제 기능은 이메일 서버 검색에서 위협 이메일 수를 반환하고, 필요에 따라 발견된 각 이메일에 대한 세부 정보를 반환합니다. 이메일 검색이 완료되면 이메일을 삭제할 수 있습니다.

이메일 검색 및 삭제 기능에는 이메일 검색 및 삭제 프로세스를 실행하는 플로우가 하나 있습니다.

주:
사용 가능한 구현이 없으면 역량 작업이 제품 메뉴에 표시되지 않습니다. 또한 활성화된 이메일 검색 및 삭제 역량 구현이 없으면 보안 인시던트의 이메일 검색 관련 링크가 표시되지 않습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Security Operations Integration - 이메일 검색 및 삭제 플로우

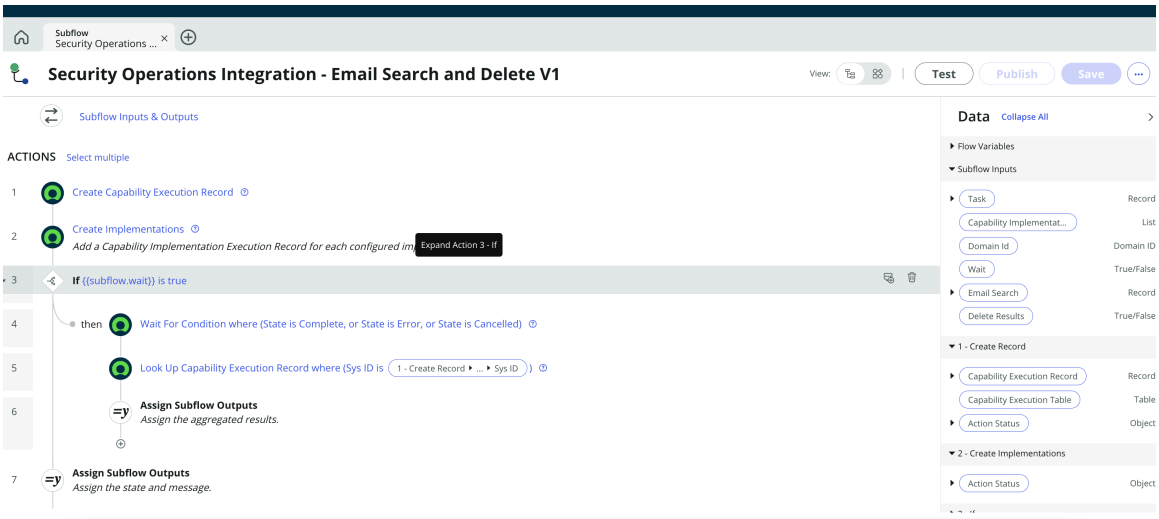
보안 운영 통합 - 이메일 검색 및 삭제 플로우는 이메일 서버 검색에서 위협 이메일 수를 반환하고, 선택적으로 찾은 각 이메일에 대한 상세 정보를 반환합니다. 이메일 검색이 완료되면 이메일을 삭제할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.analyst

이 태스크 정보
검색 쿼리를 완료하는 데 다소 시간이 걸릴 수 있습니다. 카운트를 받은 후 이메일 서버에서 이메일을 삭제하려면 승인이 필요합니다.

이 플로우는 보안 인시던트에서 이메일 검색 양식의 이메일 서버에서 삭제 및 이메일 서버에서 검색 버튼에 의해 트리거됩니다. 자세한 내용은 피싱 이메일 검색 및 삭제 문서를 참조하십시오.

이메일 검색 및 삭제



이 플로우와 관련된 활동은 여기에 설명되어 있습니다. 다른 활동에 대한 자세한 내용은 다음 문서를 참조하십시오 일반 Security Operations 통합 플로우 및 오케스트레이션 활동.

플로우 프로세스 활동에는 다음이 포함됩니다.

실행 추적 시작(메일 검색) 작업

실행 추적 - 시작(메일 검색) 역량 실행 작업은 실행 추적 기록을 생성하고 기록 상태를 시작됨으로 표시합니다. 이 작업은 모든 역량 및 구현 플로우에서 상태를 추적하는 데 사용됩니다.

결과

이 동작의 가능한 결과는 다음과 같습니다.

결과

결과	설명
성공	실행 추적 기록이 생성되었습니다.
실패	실행 추적 기록을 생성할 수 없습니다.

입력 변수

입력 변수는 작업의 초기 동작을 결정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

변수	설명
capabilityId	실행 중인 통합 역량의 시스템 식별자입니다.
구현 ID	실행 중인 통합 기능 구현의 시스템 식별자입니다.
taskId	플로우와 관련된 모든 작업의 시스템 식별자입니다.
flowContextId	연결된 플로우 컨텍스트 기록의 시스템 식별자입니다. 시스템에서 제공합니다.
플로우 이름	플로우의 이름입니다. 시스템에서 제공합니다.
parentCapabilityExcutionId	구현 플로우를 시작한 감사 기록의 시스템 식별자입니다. Splunk, Elasticsearch와 같은 통합 기능 구현 플로우에만 필요합니다.
이메일 검색 ID	이메일 검색 [sn_sec_cmn_email_search] 테이블의 이메일 검색 기록 sysid입니다.

출력 변수

출력 변수에는 후속 작업에서 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
capabilityExecutionId	실행 추적 기록의 시스템 식별자입니다.

- 지원되는 보안 역량 가져오기 작업
- 역량 실행 추적 - 구현 작업 없음

보안 운영 통합 - CI 기능 보강

CI 보강 기능을 사용하면 보안 인시던트와 관련된 구성 항목의 데이터를 보강할 수 있습니다.

CI 보강 역량에는 플로우(보안 운영 통합 - CI 보강 플로우. 역량 플로우가 실행되면 활성화된 구현을 위한 추가 플로우가 실행됩니다. 선택한 CI에서 보강을 수행하는 데 사용할 구현을 지정하거나 모든 구현을 사용하여 보강을 수행할 수 있습니다.

주:
이 보강된 데이터는 지정된 조사(예: CI에서 memdump 수행)와 관련된 포렌식 데이터이므로 CMDB에 저장하려는 데이터 유형이 아닙니다. 대신 데이터가 구성 항목 보강 [sn_sec_cmn_ci_enrichment_result] 테이블에 저장됩니다.

주:
사용 가능한 구현이 없으면 역량 작업이 제품 메뉴에 표시되지 않습니다.

보안 운영 통합 - CI 보강 플로우

보안 운영 통합 - CI 보강 플로우를 사용하면 보안 인시던트와 연관된 CI(구성 항목)의 데이터를 보강할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.analyst

이 태스크 정보
이 플로우는 두 가지 방법으로 트리거 보안 인시던트 응답 됩니다.

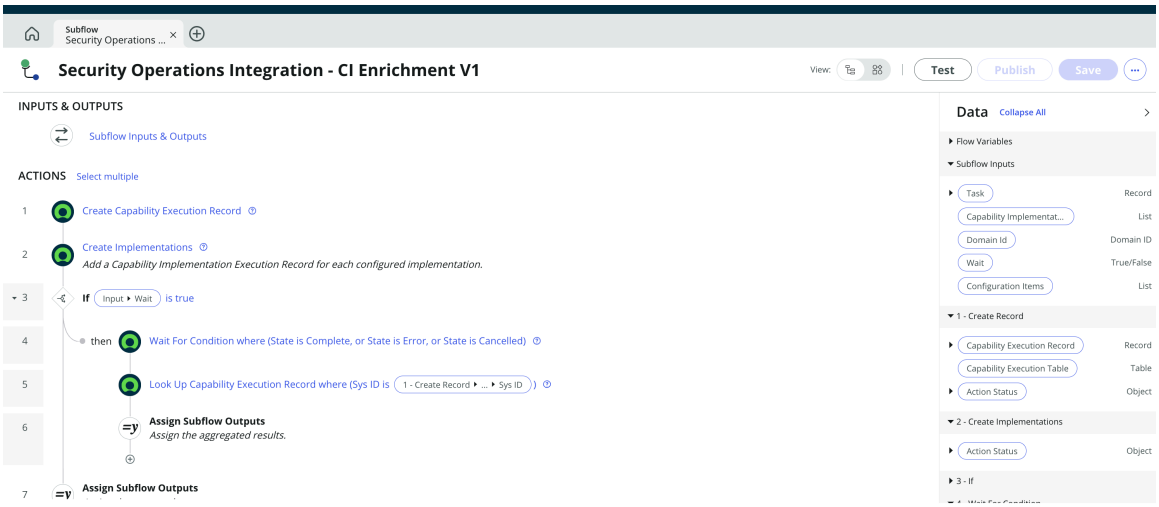
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 구성 항목 탭(영향을 받는 항목 관련 링크 아래에 있음)에서 하나 이상의 CI를 선택하고 선택한 행 선택 목록에 대한 작업에서**CI** 보강 실행을 선택합니다.
- CI 기록을 열고 **CI** 보강 실행 관련 링크를 클릭하면 됩니다.

그런 다음 두 방법 중 하나를 사용하여 선택한 CI를 보강하는 데 사용할 구현을 지정할 수 있습니다. 보강을 수행하기 위해 연결된 구현 플로우가 실행됩니다.

주:
기본 시스템에는 이 역량에 대한 구현 플로우가 포함되어 있지 않습니다. CI를 보강하려면 고유한 구현 플로우를 만들어야 합니다.

CI 보강



이 플로우와 관련된 작업은 여기에 설명되어 있습니다. 다른 작업에 대한 자세한 내용은 다음 문서를 참조하십시오 일반 Security Operations 통합 플로우 및 오케스트레이션 활동.

플로우 프로세스 작업에는 다음이 포함됩니다.

- 실행 추적 - 플로우 작업 시작
- 보안 운영 통합 - CI 보강 플로우
- 역량 실행 추적 - 구현 작업 없음
- 지원되는 보안 역량 가져오기 작업

보안 운영 통합 - 옵저버블 보강 기능

옵저버블 보강 기능을 사용하면 구현 플로우를 사용하여 다양한 소스의 추가 정보로 옵저버블을 보강할 수 있습니다. 이 역량은 식별된 위협이 포함되도록 인시던트 응답 조사 중에 사용됩니다.

옵저버블 보강 역량에는 플로우 가 Security Operations Integration - 옵저버블 보강 플로우있습니다. 역량 플로우가 실행되면 활성화된 구현을 위한 추가 플로우가 실행됩니다. 선택한 옵저버블에서 보강을 수행하는 데 사용할 구현을 지정하거나 지원되는 관찰 대상 유형과 일치하는 모든 구현을 사용하여 보강을 수행할 수 있습니다.

주:
사용 가능한 구현이 없으면 역량 작업이 제품 메뉴에 표시되지 않습니다.

Security Operations Integration - 옵저버블 보강 플로우

Security Operations Integration - 옵저버블 보강 하위 플로우를 사용하면 구현 플로우 디자이너를 사용하여 다양한 소스의 추가 정보로 옵저버블을 보강할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

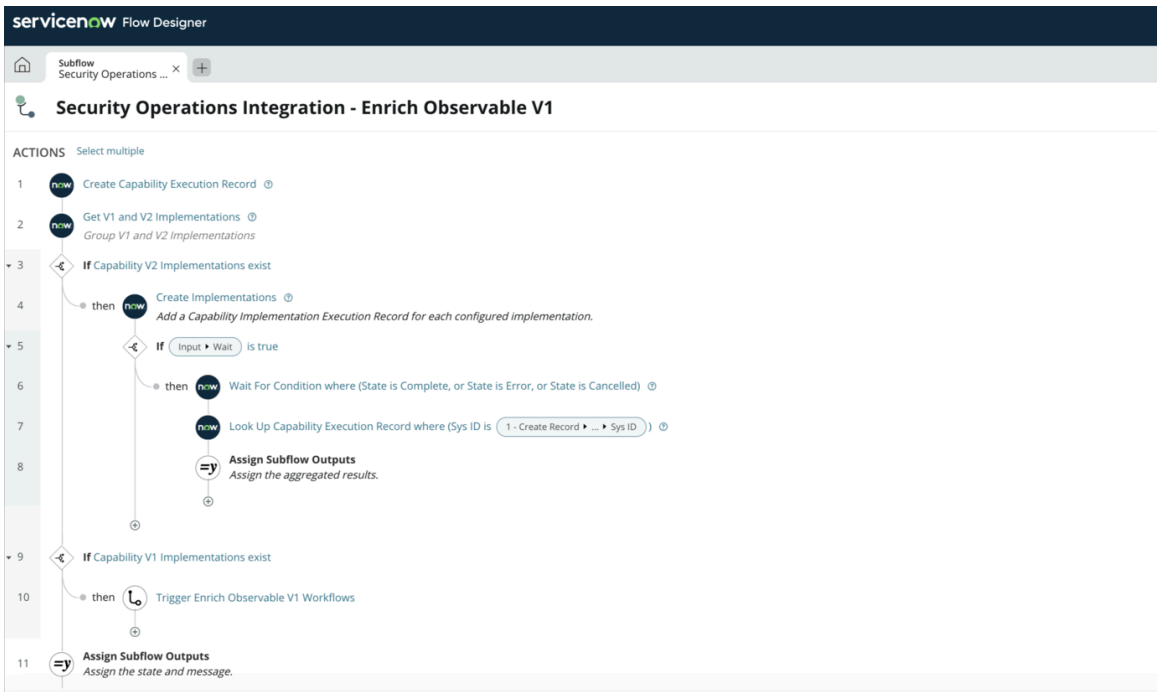
시작하기 전에
필요한 역할: sn_si.analyst

이 태스크 정보
이 플로우는 두 가지 방법 중 하나 보안 인시던트 응답 또는 위협 인텔리전스 두 가지 방법으로 트리거될 수 있습니다.

- 옵저버블 목록에서 하나 이상의 옵저버블을 선택하고 선택한 행 선택 목록에 대한 작업에서옵저버블 보강 실행을 선택합니다.
- 옵저버블 기록을 열고 옵저버블 보강 실행 관련 링크를 클릭하면 됩니다.

그런 다음 두 방법 모두 선택한 옵저버블을 보강하는 데 사용할 구현을 지정할 수 있습니다. 보강을 수행하기 위해 연결된 구현 플로우가 실행됩니다.

옵저버블 보강



이 플로우와 관련된 작업은 여기에 설명되어 있습니다. 다른 작업에 대한 자세한 내용은 다음 문서를 참조하십시오 일반 Security Operations 통합 플로우 및 오케스트레이션 활동.

플로우 프로세스 작업에는 다음이 포함됩니다.

- 역량 실행 추적 - 구현 작업 없음
- 지원되는 보안 역량 가져오기 작업역량 실행 추적 - 구현 작업 없음

보안 운영 통합 - 네트워크 통계 기능 가져오기

네트워크 통계 가져오기 기능은 호스트 또는 엔드포인트에서 활성 네트워크 연결 목록을 검색합니다. 조사 진행 중에 인시던트를 향상하는 데 사용할 수 있습니다. 이 기능은 구성 항목이 보안 인시던트에 추가될 때 자동으로 트리거됩니다.

네트워크 통계 가져오기 기능에는 하나 이상의 CI 및 작업을 허용하는 흐름 보안 운영 통합 - 네트워크 통계 플로우 가져오기 이 있습니다. 플로우는 각 구현과 각 CI에 대해 반복되고 구현 플로우를 다시 호출합니다.

주:
사용 가능한 구현이 없으면 역량 작업이 제품 메뉴에 표시되지 않습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

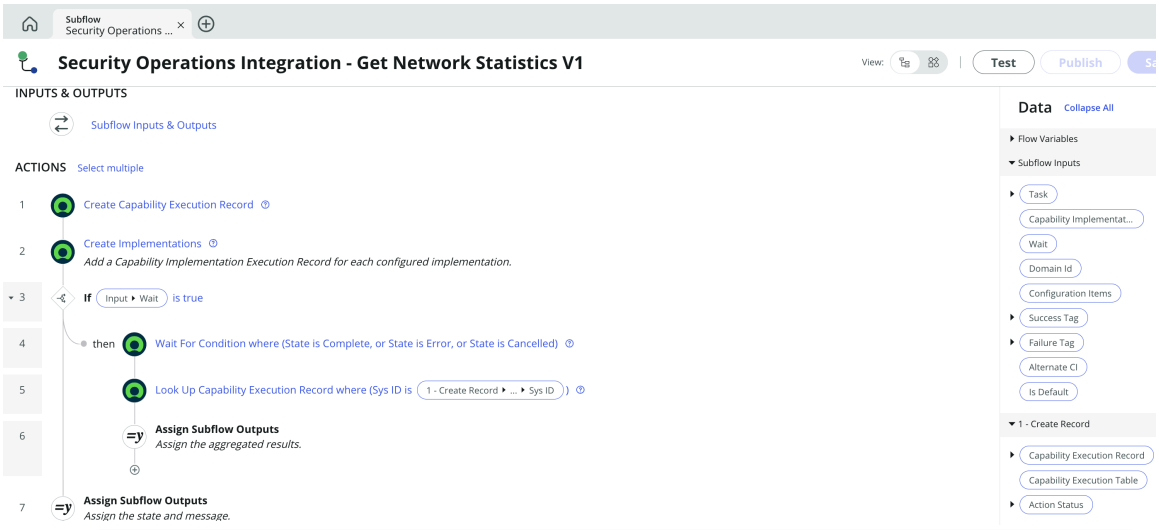
보안 운영 통합 - 네트워크 통계 플로우 가져오기

보안 운영 통합 - 네트워크 통계 가져오기 플로우는 호스트나 엔드포인트에서 활성 네트워크 연결 목록을 검색합니다.

시작하기 전에
필요한 역할: sn_si.analyst

이 태스크 정보
이 플로우는 구성 항목이 보안 인시던트에 추가되면 자동으로 실행됩니다.

네트워크 통계 가져오기



이 플로우와 관련된 작업은 여기에 설명되어 있습니다. 다른 작업에 대한 자세한 내용은 다음 문서를 참조하십시오 일반 Security Operations 통합 플로우 및 오케스트레이션 활동.

플로우 작업에는 다음이 포함됩니다.

- 역량 - CI 활동 결정
-

.

실행 추적 - 시작(CI) 플로우 작업

실행 추적 - 시작(CI) 플로우 작업은 CI(구성 항목)에서 작동하는 통합 플로우에 대한 보안 운영 감사 프로세스를 시작합니다.

실행 추적 - 시작(CI) 플로우 작업을 CI 플로우와 함께 사용하여 감사에서 플로우의 진행률을 기록하기 시작할 수 있습니다.

결과

이 플로우 작업의 가능한 결과는 다음과 같습니다.

결과

결과	설명
성공	감사 레코드가 생성됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

입력 변수

입력 변수는 플로우 작업의 초기 동작을 결정합니다.

변수	설명
capabilityId	실행 중인 통합 역량의 시스템 식별자입니다.
isImpl	통합 역량 플로우 또는 통합 역량 구현 플로우에 대해 감사가 수행되는지 여부를 지정하는 플래그입니다. 가능한 값: • false - 사이팅 검색과 같은 추상적인 통합 역량 플로우에 대한 감사를 나타냅니다. (기본값입니다.) • true - 통합 역량 구현 플로우에 대한 감사를 나타냅니다. 예를 들어 Splunk 또는 Elasticsearch입니다.
taskId	플로우와 관련된 모든 작업의 시스템 식별자입니다.

ci리스트	원하는 작업을 수행할 하나 이상의 CI(구성 항목)를 다음과 같은 형식으로 지정합니다.
	`["sysId", "sysId"]`
	또는
	`"sysId"`
	플로우 입력으로 사용됩니다.

flowContextId	연결된 플로우 컨텍스트 기록의 시스템 식별자입니다. 시스템에서 제공합니다.
플로우 이름	플로우의 이름입니다. 시스템에서 제공합니다.
parentCapabilityExcutionId	구현 플로우를 시작한 감사 기록의 시스템 식별자입니다. Splunk, Elasticsearch와 같은 통합 기능 구현 플로우에만 필요합니다.

출력 변수

출력 변수에는 후속 활동에 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
capabilityExecutionId	감사 기록의 시스템 식별자입니다.

플로우 프로세스 작업에는 다음이 포함됩니다.

- 지원되는 보안 역량 가져오기 작업
- 역량 실행 추적 - 구현 작업 없음

보안 인시던트 응답 - 네트워크 통계 플로우 가져오기

는 보안 인시던트 응답 〉 네트워크 통계 가져오기 플로우는 분석 상태의 보안 인시던트에 추가될 때 영향을 받는 Windows 기반 자원에 대한 네트워크 통계를 검색합니다.

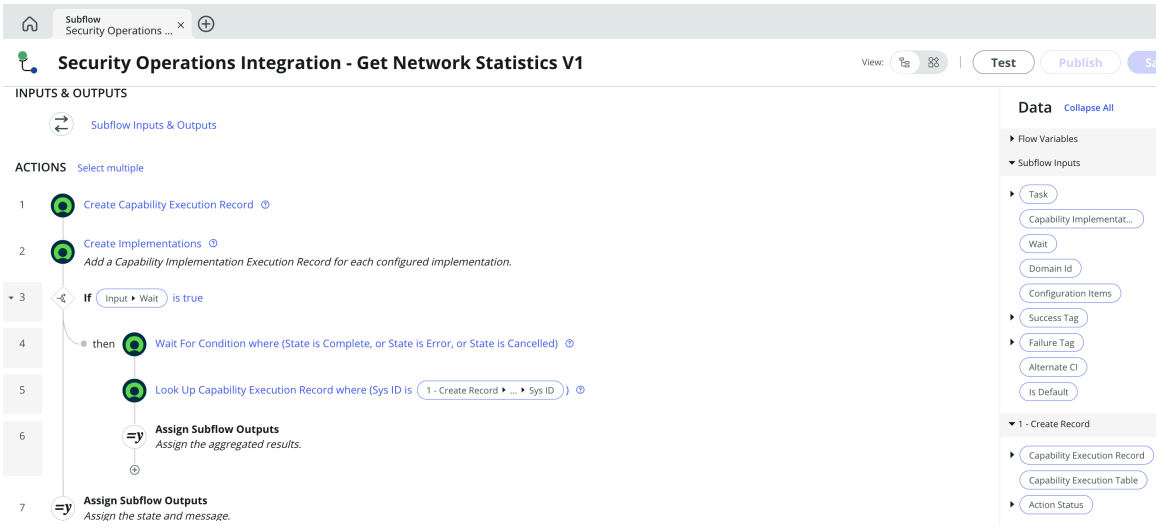
시작하기 전에
필요한 역할: sn_si.analyst

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보
구성 항목이 포함된 새 보안 인시던트의 경우 상태가 분석으로 변경되면 플로우가 자동으로 실행됩니다.

기존 보안 인시던트는 분석 상태에서 새 구성 항목을 추가하면 자동으로 업데이트됩니다.

네트워크 통계 가져오기



플로우 프로세스 작업에는 다음이 포함됩니다.

구성 항목 FQDN 가져오기 플로우 작업

OS별 셸 스크립트 결정

Powershell에서 문을 실행하는 경우

실행 추적 - 플로우 작업 시작

netstat 플로우 작업을 통해 네트워크 통계 가져오기

역량 실행 추적 - 실패 플로우 작업

보강 데이터 기록 플로우 작업 생성

역량 실행 추적 - 실패 플로우 작업 - 보강 ID를 반환합니다.

역량 실행 추적 - 플로우 작업 완료

프로시저

1. 보안 인시던트를 엽니다.
2. 필요한 경우 상태를분석으로 업데이트합니다.
3. 구성 항목(컴퓨터, 서버 또는 이와 유사한 항목)을 추가합니다.
4. 업데이트를 클릭합니다.
   보안 인시던트 응답 오케스트레이션 에서 네트워크 통계 정보를 제공합니다. 관련 링크 〉 보안 인시던트 보강 탭. 자세한 내용은 보안 운영 보강 데이터 매핑 문서를 참조하십시오.

   이 플로우와 관련된 작업은 여기에 설명되어 있습니다. 다른 작업에 대한 자세한 내용은 다음 문서를 참조하십시오 일반 Security Operations 통합 플로우 및 오케스트레이션 활동.

보안 운영 통합 - 실행 중인 프로세스 가져오기 기능

실행 중인 프로세스 가져오기 기능은 호스트 또는 엔드포인트에서 CI(구성 항목)의 실행 중인 프로세스 목록을 검색합니다. 이 역량은 조사 중 인시던트 보강에 사용됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

실행 중인 프로세스 가져오기 역량에는 두 가지 구현 플로우가 있습니다.

- 보안 운영 Carbon Black 통합 - 실행 중인 프로세스 플로우 가져오기
- 보안 운영 시스템 명령 통합 - 실행 중인 프로세스 가져오기 플로우

주:
사용 가능한 구현이 없으면 역량 작업이 제품 메뉴에 표시되지 않습니다.

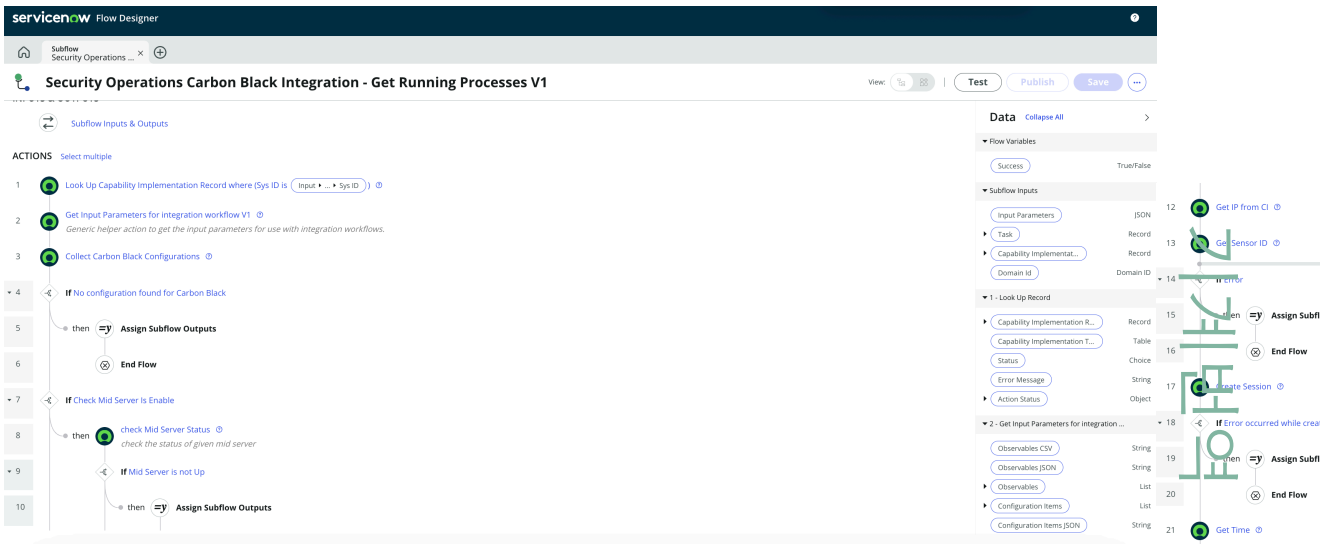
이 플로우와 관련된 작업은 여기에 설명되어 있습니다. 다른 작업에 대한 자세한 내용은 다음 문서를 참조하십시오 일반 Security Operations 통합 플로우 및 오케스트레이션 활동.

보안 운영 **Carbon Black** 통합 - 실행 중인 프로세스 플로우 가져오기

보안 운영 Carbon Black 통합 - 실행 중인 프로세스 가져오기는 보안 운영 통합 - 실행 중인 프로세스 가져오기 플로우에 의해 시작된 Carbon Black 통합을 위한 구현입니다.

필요한 역할: sn_si.analyst

카본 블랙이 실행 중인 프로세스 임포트



이 플로우와 관련된 작업은 여기에 설명되어 있습니다. 다른 작업에 대한 자세한 내용은 다음 문서를 참조하십시오 일반 Security Operations 통합 플로우 및 오케스트레이션 활동.

Carbon Black 구성 수집 플로우 작업

Carbon Black 구성 수집 플로우 작업은 플로우에서 사용할 구성 정보를 수집합니다.

Carbon Black 구성 수집 플로우 작업은 플로우에 사용할 Carbon Black 구성 정보를 수집합니다.

결과

이 플로우 작업의 가능한 결과는 다음과 같습니다.

결과

결과	설명
성공	구성에 성공했습니다.
실패	구성을 검증하는 동안 오류가 발생했습니다. 자세한 오류 정보는 활동 출력 오류에서 확인할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

입력 변수

이 플로우 작업에 대한 입력 변수가 없습니다.

출력 변수

출력 변수에는 후속 활동에 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
endpoint_base	외부 공급업체 통합 API의 기본 URL입니다.
use_mid_server	REST 활동이 MID 서버를 사용하여 Carbon Black과 상호작용하는지 여부를 결정합니다.
api_token	외부 공급업체 통합 API 키입니다.

MID Server 상태 확인

통합 구성의 **MID** 서버 호스트 필드에서 식별된 MID 서버가 실행 중인지 여부를 확인합니다. 필드가 임의로 설정된 경우 플로우 작업은 모든 MID 서버가 실행 중인지 확인합니다.

MID 서버 상태 확인 플로우 작업은 플로우 내에 실행 중인 MID 서버가 있는지 확인하기 위해 모든 플로우와 함께 사용할 수 있습니다.

결과

이 플로우 작업의 가능한 결과는 다음과 같습니다.

결과

결과	설명
성공	세션 상태가 반환됩니다.
실패	세션 상태 오류입니다. 더 많은 오류 정보는 플로우 작업 출력 오류에서 확인할 수 있습니다.

입력 변수

입력 변수는 플로우 작업의 초기 동작을 결정합니다.

변수	설명
capabilityExecutionId	실행 중인 역량의 ID입니다.
플로우 이름	실행 중인 플로우의 이름입니다.
mid_server_host	통합의 구성에서 식별된 MID 서버

출력 변수

출력 변수에는 후속 활동에 사용할 수 있는 데이터가 포함됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

출력 변수

변수	설명
mid_server_live	통합 구성의 **MID** 서버 호스트 필드에서 식별된 MID 서버가 실행 중인지 여부를 식별합니다. 필드가 임의로 설정된 경우 플로우 작업은 모든 MID 서버가 실행 중인지 확인합니다.

센서 **ID** 플로우 작업 가져오기

센서 ID 가져오기 플로우 작업은 플로우에 사용할 센서 식별자를 수집합니다.

센서 ID 가져오기 플로우 작업은 플로우에 사용할 센서 정보를 수집하기 위해 모든 플로우와 함께 사용할 수 있습니다.

결과

이 플로우 작업의 가능한 결과는 다음과 같습니다.

결과

결과	설명
성공	센서 식별자를 찾았습니다.
실패	센서를 찾을 수 없습니다. 더 많은 오류 정보는 플로우 작업 출력 오류에서 확인할 수 있습니다.

입력 변수

입력 변수는 플로우 작업의 초기 동작을 결정합니다.

변수	설명
api_token	Carbon Black API 키입니다.
use_mid_server	REST 활동이 MID 서버를 사용하여 Carbon Black과 상호작용하는지 여부를 결정합니다.
endpoint_base	Carbon Black API의 기본 URL입니다.
ci_ip_address	구성 항목 IP 주소입니다.

출력 변수

출력 변수에는 후속 활동에 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
status_code	요청이 성공했는지 여부를 결정합니다. 그렇지 않은 경우 HTTP 오류 코드 및 메시지를 표시합니다.
배열 요소 유형	API 변수를 사용합니다.
sensor_detail	JSON 형식으로 된 Carbon Black 센서에 대한 설명입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

세션 플로우 작업 생성

세션 생성 플로우 작업은 플로우에 사용할 Carbon Black 세션을 설정합니다.

세션 생성 플로우 작업은 플로우 내에 Carbon Black 세션을 생성하기 위해 모든 플로우와 함께 사용할 수 있습니다.

결과

이 플로우 작업의 가능한 결과는 다음과 같습니다.

결과

결과	설명
성공	세션이 작성되었습니다.
실패	세션이 작성되지 않았습니다. 더 많은 오류 정보는 플로우 작업 출력 오류에서 확인할 수 있습니다.

입력 변수

입력 변수는 플로우 작업의 초기 동작을 결정합니다.

변수	설명
api_token	Carbon Black API 키입니다.
endpoint_base	Carbon Black API의 기본 URL입니다.
sensor_id	센서 식별자입니다.
use_mid_server	REST 활동이 MID 서버를 사용하여 Carbon Black과 상호작용하는지 여부를 결정합니다.

출력 변수

출력 변수에는 후속 활동에 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
status_code	요청이 성공했는지 여부를 결정합니다. 그렇지 않은 경우 HTTP 오류 코드 및 메시지를 표시합니다.
출력	API 변수

세션 상태 플로우 작업 확인

플로우 내에서 Carbon Black 세션의 상태를 결정합니다.

세션 상태 확인 플로우 작업은 플로우 내의 Carbon Black 세션 상태를 확인하기 위해 모든 플로우와 함께 사용할 수 있습니다.

결과

이 플로우 작업의 가능한 결과는 다음과 같습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

결과

결과	설명
성공	세션 상태가 반환됩니다.
실패	세션 상태 오류입니다. 더 많은 오류 정보는 플로우 작업 출력 오류에서 확인할 수 있습니다.

입력 변수

입력 변수는 플로우 작업의 초기 동작을 결정합니다.

변수	설명
api_token	Carbon Black API 키입니다.
endpoint_base	Carbon Black API의 기본 URL입니다.
session_id	세션 식별자입니다.
use_mid_server	REST 활동이 MID 서버를 사용하여 Carbon Black과 상호작용하는지 여부를 결정합니다.

출력 변수

출력 변수에는 후속 활동에 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
status_code	요청이 성공했는지 여부를 결정합니다. 그렇지 않은 경우 HTTP 오류 코드 및 메시지를 표시합니다.
출력	Carbon Black 실행 프로세스에 대한 정보입니다.

명령 프로세스 플로우 작업 생성

명령 프로세스 작성 플로우 작업은 플로우에 사용할 Carbon Black 명령 프로세스를 작성합니다.

명령 프로세스 생성 플로우 작업은 플로우 내에 Carbon Black 명령 프로세스를 생성하기 위해 모든 플로우와 함께 사용할 수 있습니다.

결과

이 플로우 작업의 가능한 결과는 다음과 같습니다.

결과

결과	설명
성공	명령 프로세스가 작성되었습니다.
실패	명령 프로세스가 작성되지 않았습니다. 더 많은 오류 정보는 플로우 작업 출력 오류에서 확인할 수 있습니다.

입력 변수

입력 변수는 플로우 작업의 초기 동작을 결정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

변수	설명
api_token	Carbon Black API 키입니다.
endpoint_base	Carbon Black API의 기본 URL입니다.
session_id	세션 식별자입니다.
command_id	명령 식별자입니다.
use_mid_server	REST 활동이 MID 서버를 사용하여 Carbon Black과 상호작용하는지 여부를 결정합니다.

출력 변수

출력 변수에는 후속 활동에 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
status_code	요청이 성공했는지 여부를 결정합니다. 그렇지 않은 경우 HTTP 오류 코드 및 메시지를 표시합니다.
출력	API 변수

명령 상태 검사 및 프로세스 흐름 작업 가져오기

Carbon Black 명령 상태를 확인하고 플로우에서 사용할 프로세스를 검색합니다.

명령 상태 검사 및 프로세스 흐름 가져오기 작업을 모든 흐름과 함께 사용하여 Carbon Black 명령 상태를 확인하고 흐름 내의 프로세스를 가져올 수 있습니다.

결과

이 플로우 작업의 가능한 결과는 다음과 같습니다.

결과

결과	설명
성공	명령 상태가 반환되고 프로세스가 작성되었습니다.
실패	명령 상태 또는 프로세스 오류입니다. 더 많은 오류 정보는 플로우 작업 출력 오류에서 확인할 수 있습니다.

입력 변수

입력 변수는 플로우 작업의 초기 동작을 결정합니다.

변수	설명
api_token	Carbon Black API 키입니다.
endpoint_base	Carbon Black API의 기본 URL입니다.
session_id	세션 식별자입니다.
command_id	명령 식별자입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

변수	설명
use_mid_server	REST 활동이 MID 서버를 사용하여 Carbon Black과 상호작용하는지 여부를 결정합니다.

출력 변수

출력 변수에는 후속 활동에 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
status_code	요청이 성공했는지 여부를 결정합니다. 그렇지 않은 경우 HTTP 오류 코드 및 메시지를 표시합니다.
출력	API 변수

프로세스 매핑 데이터 플로우 작업

프로세스 데이터 매핑 플로우 작업은 Carbon Black 프로세스 데이터를 플로우 내에 매핑합니다.

프로세스 매핑 데이터 플로우 작업은 Carbon Black 프로세스를 매핑하기 위한 모든 플로우와 함께 사용할 수 있습니다.

결과

이 플로우 작업의 가능한 결과는 다음과 같습니다.

결과

결과	설명
성공	매핑된 프로세스
실패	프로세스가 매핑되지 않았습니다. 더 많은 오류 정보는 플로우 작업 출력 오류에서 확인할 수 있습니다.

입력 변수

입력 변수는 플로우 작업의 초기 동작을 결정합니다.

변수	설명
affected_ci	영향을 받는 구성 항목입니다.
implementation_id	구현 식별자입니다.

출력 변수

출력 변수에는 후속 활동에 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
출력	형식이 지정됨: 추상 워크플로우에서 사용하는 실행 중인 프로세스에 대한 데이터를 반환합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

출력 변수

변수	설명
processes	배열의 프로세스 목록입니다.

역량 실행 추적 - 플로우 작업 완료

역량 실행 추적 - 완료 플로우 작업은 플로우가 완료되면 감사 기록을 업데이트합니다.

역량 실행 추적 - 전체 플로우 작업은 플로우의 완료를 기록하기 위해 모든 플로우와 함께 사용할 수 있습니다.

주:
병렬 시작 관리자 코어 플로우 작업의 반환 값 배열에는 모든 통합 플로우 실행의 결과 배열이 포함되어 있으며 실행 추적을 성공적으로 완료하라는 메시지를 표시합니다.

결과

이 플로우 작업의 가능한 결과는 다음과 같습니다.

결과

결과	설명
성공	감사 기록 상태가 완료로 업데이트됩니다.

입력 변수

입력 변수는 플로우 작업의 초기 동작을 결정합니다.

변수	설명
capabilityExecutionId	감사 기록의 시스템 식별자입니다. 이 필드는 감사 시작 활동의 출력입니다.
플로우 이름	플로우의 이름입니다. 시스템에서 제공합니다.
메시지	완료 메시지.

출력 변수

출력 변수가 없습니다.

세션 닫기 플로우 작업

플로우 내에서 Carbon Black 세션을 닫습니다.

세션 닫기 활동은 Carbon Black 세션을 닫기 위한 모든 플로우와 함께 사용할 수 있습니다.

결과

이 플로우 작업의 가능한 결과는 다음과 같습니다.

결과

결과	설명
성공	세션이 닫혔습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

결과

결과	설명
실패	세션이 닫히지 않았습니다. 더 많은 오류 정보는 플로우 작업 출력 오류에서 확인할 수 있습니다.

입력 변수

입력 변수는 플로우 작업의 초기 동작을 결정합니다.

변수	설명
api_token	Carbon Black API 키입니다.
endpoint_base	Carbon Black API의 기본 URL입니다.
session_id	세션 식별자입니다.
use_mid_server	REST 활동이 MID 서버를 사용하여 Carbon Black과 상호작용하는지 여부를 결정합니다.

출력 변수

출력 변수에는 후속 활동에 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
status_code	요청이 성공했는지 여부를 결정합니다. 그렇지 않은 경우 HTTP 오류 코드 및 메시지를 표시합니다.
출력	API 변수

보안 운영 시스템 명령 통합 - 실행 중인 프로세스 가져오기 플로우

보안 운영 시스템 명령 통합 - 실행 중인 프로세스 가져오기 플로우는 분석 상태에서 Windows 또는 Unix 기반 보안 인시던트에 추가 또는 업데이트될 때 구성 항목의 실행 중인 프로세스를 검색합니다.

시작하기 전에
필요한 역할: sn_si.analyst

이 태스크 정보
새 보안 인시던트의 경우 선택한 구성 항목으로 인시던트를 제출하면 상태가 자동으로 분석으로 변경되어 플로우가 자동으로 실행됩니다. 초안 상태로 유지되면 실행되지 않습니다.

기존 보안 인시던트는 분석 상태에서 새 구성 항목을 추가하면 자동으로 업데이트됩니다.

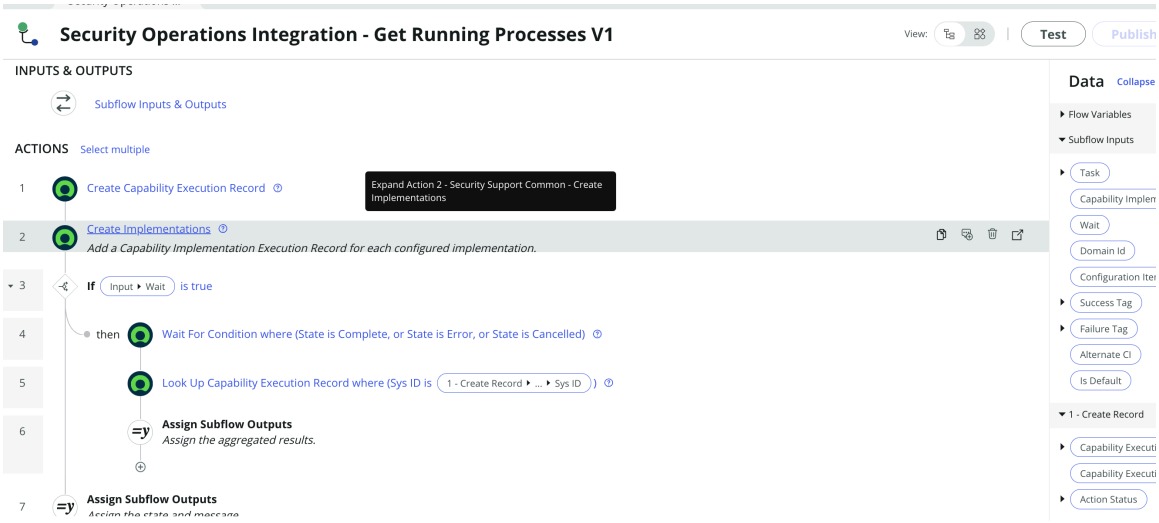
플로우 프로세스 작업에는 다음이 포함됩니다.

- 구성 항목 FQDN 가져오기 플로우 작업
- OS 활동별 셸 스크립트 결정
- 실행 추적 - 플로우 작업 시작
- PowerShell을 통해 실행 중인 프로세스 가져오기
- 셸 스크립트 실행 활동

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 역량 실행 추적 - 실패 플로우 작업
- MID 스크립트 활동에서 셸 스크립트 추출
- 결과 결합 과 배열의 값 반환
- 보강 데이터 기록 플로우 작업 생성
- 역량 실행 추적 - 플로우 작업 완료

실행 중인 프로세스 임포트



프로시저

1. 보안 인시던트를 엽니다.
2. 필요한 경우 상태를분석으로 업데이트합니다.
3. 구성 항목(컴퓨터, 서버 또는 이와 유사한 항목)을 추가합니다.
4. 업데이트를 클릭합니다.
   보안 인시던트 응답 오케스트레이션 에서 실행 중인 프로세스 정보를 제공합니다. 관련 링크 〉보안 인시던트 보강탭. 자세한 내용은 보안 운영 보강 데이터 매핑 문서를 참조하십시오.

   이 플로우와 관련된 작업은 여기에 설명되어 있습니다. 다른 작업에 대한 자세한 내용은 다음 문서를 참조하십시오 일반 Security Operations 통합 플로우 및 오케스트레이션 활동.

결과 결합 활동

결과 결합 워크플로우 활동은 워크플로우에서 사용할 외부 공급업체 통합의 결과를 병합합니다.

결과 결합 활동은 워크플로우에서 MID 서버 셸 스크립트를 실행하기 위해 모든 워크플로우와 함께 사용할 수 있습니다.

결과

이 활동의 가능한 결과는 다음과 같습니다.

결과

결과	설명
성공	결과를 결합했습니다.
실패	조합에 실패했습니다. 자세한 오류 정보는 활동 출력 오류에서 확인할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

입력 변수

입력 변수는 활동의 초기 동작을 결정합니다.

변수	설명
입력A	결과 세트 A
입력B	결과 세트 B
implementation_id	구현 식별자입니다.
affected_ci	구성 항목

출력 변수

출력 변수에는 후속 활동에 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
결과	채워진 결과에 따라 결과 세트 A 또는 결과 세트 B가 표시됩니다.

셸 스크립트 실행 활동

셸 스크립트 실행 워크플로우 활동은 워크플로우 내에서 MID 서버 셸 스크립트를 실행합니다.

셸 스크립트 실행 활동은 워크플로우에서 MID 서버 셸 스크립트를 실행하기 위한 모든 워크플로우와 함께 사용할 수 있습니다.

결과

이 활동의 가능한 결과는 다음과 같습니다.

결과

결과	설명
성공	셸 스크립트 찾음
실패	셸 스크립트를 찾을 수 없습니다. 자세한 오류 정보는 활동 출력 오류에서 확인할 수 있습니다.

입력 변수

입력 변수는 활동의 초기 동작을 결정합니다.

변수	설명
대상	대상 CI의 IP 또는 FQDN(정규화된 도메인 이름)입니다.
스크립트값	문자열 값으로 Unix 시스템에서 실행되는 스크립트입니다.

출력 변수

출력 변수에는 후속 활동에 사용할 수 있는 데이터가 포함됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

출력 변수

변수	설명
response	원시 출력입니다. 실행 중인 프로세스 데이터입니다.

MID 스크립트 활동에서 셸 스크립트 추출

MID 스크립트에서 셸 스크립트 추출 워크플로우 활동은 워크플로우에서 사용할 MID 서버 셸 스크립트를 끌어옵니다.

MID 스크립트에서 셸 스크립트 추출 활동은 워크플로우에 포함할 MID 서버 셸 스크립트를 추출하기 위해 모든 워크플로우와 함께 사용할 수 있습니다.

결과

이 활동의 가능한 결과는 다음과 같습니다.

결과

결과	설명
성공	셸 스크립트 찾음
실패	셸 스크립트를 찾을 수 없습니다. 자세한 오류 정보는 활동 출력 오류에서 확인할 수 있습니다.

입력 변수

입력 변수는 활동의 초기 동작을 결정합니다.

변수	설명
sysId	시스템 식별자

출력 변수

출력 변수에는 후속 활동에 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
스크립트값	문자열 값으로 Unix 시스템에서 실행되는 스크립트입니다.

PowerShell 작업을 통해 실행 중인 프로세스 가져오기

센서 ID 가져오기 워크플로우 활동은 워크플로우에서 사용할 PowerShell을 통해 실행 중인 프로세스를 수집합니다.

PowerShell을 통해 실행 중인 프로세스 가져오기 워크플로우 활동은 워크플로우에 포함할 프로세스를 검색하기 위해 모든 워크플로우와 함께 사용할 수 있습니다.

결과

이 활동의 가능한 결과는 다음과 같습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

결과

결과	설명
성공	찾은 프로세스
실패	프로세스를 찾을 수 없음. 자세한 오류 정보는 활동 출력 오류에서 확인할 수 있습니다.

입력 변수

입력 변수는 활동의 초기 동작을 결정합니다.

변수	설명
대상	대상 CI의 IP 또는 FQDN(정규화된 도메인 이름)입니다.
processing스크립트	ECC 스크립트는 Windows 기반 시스템에서 실행됩니다.

출력 변수

출력 변수에는 후속 활동에 사용할 수 있는 데이터가 포함됩니다.

출력 변수

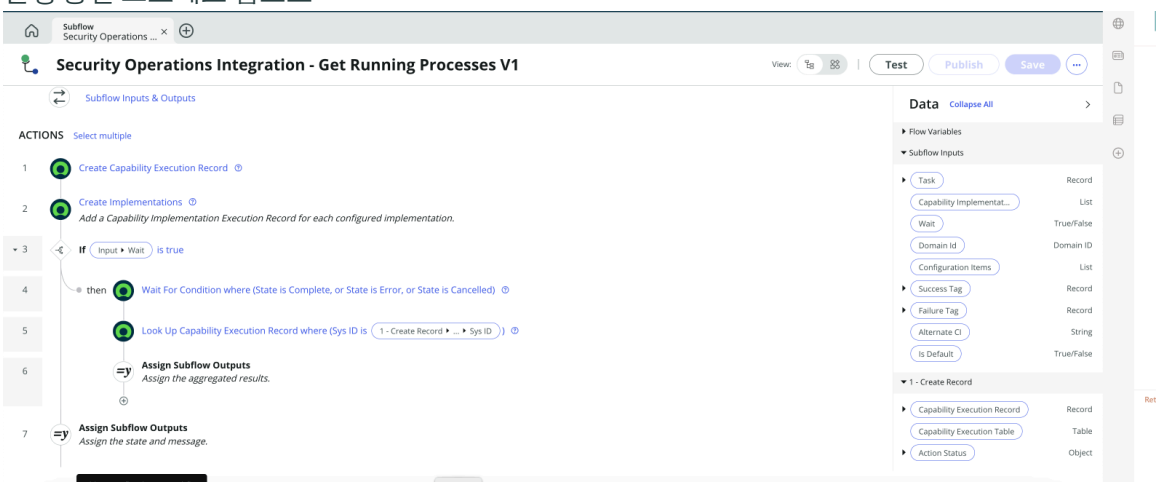
변수	설명
response	원시 출력입니다. 실행 중인 프로세스 데이터입니다.

보안 운영 - 실행 중인 프로세스 가져오기 플로우

보안 운영 - 실행 중인 프로세스 가져오기 플로우는 통합과 독립적인 상위 수준 플로우입니다. 호스트에서 CI(구성 항목)의 실행 중인 프로세스 목록을 검색합니다. Carbon Black과 같은 통합을 수행하거나 Windows 기반 보안 인시던트에 이를 사용합니다.

필요한 역할: sn_si.analyst

실행 중인 프로세스 임포트



이 플로우와 관련된 활동은 여기에 설명되어 있습니다. 다른 활동에 대한 자세한 내용은 다음 문서를 참조하십시오 일반 Security Operations 통합 플로우 및 오케스트레이션 활동.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 운영 통합 - 호스트 격리 기능

호스트 격리 기능은 다른 장치에 대한 시스템 연결을 제한합니다. 호스트 격리는 CI(구성 항목)에 대해 실행됩니다.

호스트 격리 역량에는 하나 이상의 CI를 수락하고 선택적으로 구현을 허용하는 플로우 보안 운영 - 호스트 격리 플로우 가 있습니다. 호스트를 격리하는 데 사용할 구현을 지정하거나 플로우에서 모든 구현을 사용하여 호스트 격리를 시도할 수 있습니다.

주:
기능과 통합되지는 않지만 오케스트레이션에서 격리된 호스트와의 통신을 복원하기 위해 플로우 보안 운영 Carbon Black 통합 - 호스트 격리 플로우 제거 를 사용할 수 있습니다.

주:
사용 가능한 구현이 없으면 역량 작업이 제품 메뉴에 표시되지 않습니다.

호스트 격리 실행

호스트 격리 는 다른 장치에 대한 시스템 연결을 제한합니다.

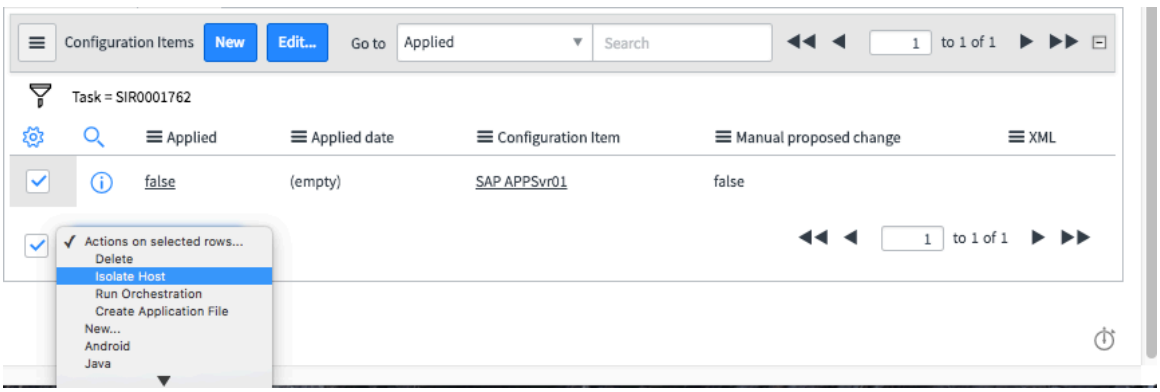
시작하기 전에
필요한 역할: sn_si.analyst

이 태스크 정보
주:
사용 가능한 구현이 없으면 역량 작업이 제품 메뉴에 표시되지 않습니다.

보안 인시던트의 관련 목록에서 **Security Operations Integration -** 호스트 또는 엔드포인트 격리 플로우를 트리거할 수 있습니다.

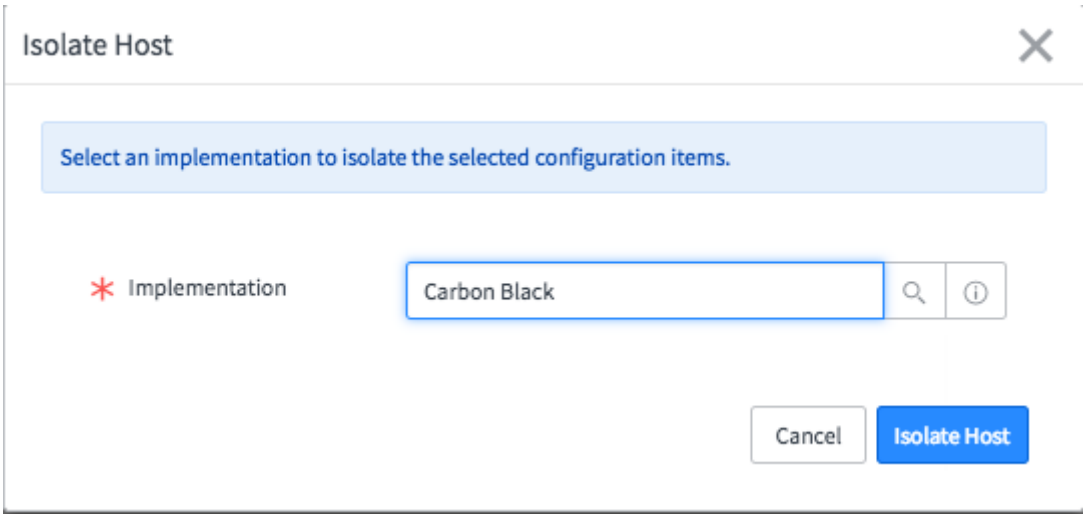
프로시저

1. 보안 인시던트로 이동합니다.
2. 관련 목록 탭에서 구성 항목을 선택합니다.
3. **Actions on selected rows...**(선택한 행에 대해 수행할 작업) 드롭다운 메뉴에서 **Isolate Host**(호스트 격리)를 클릭합니다.

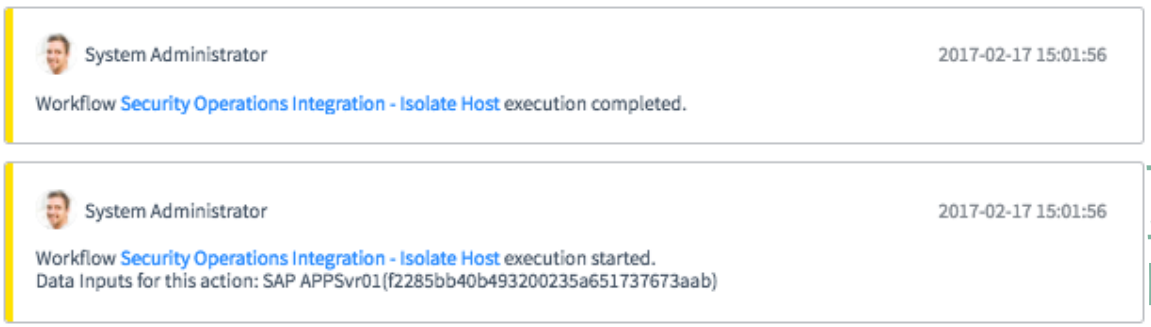


대화 상자가 나타납니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 구현을 선택합니다.
5. 호스트 격리를 클릭합니다.
   플로우 실행 감사가 작업 메모 섹션에 표시됩니다.



보안 운영 - 호스트 격리 플로우

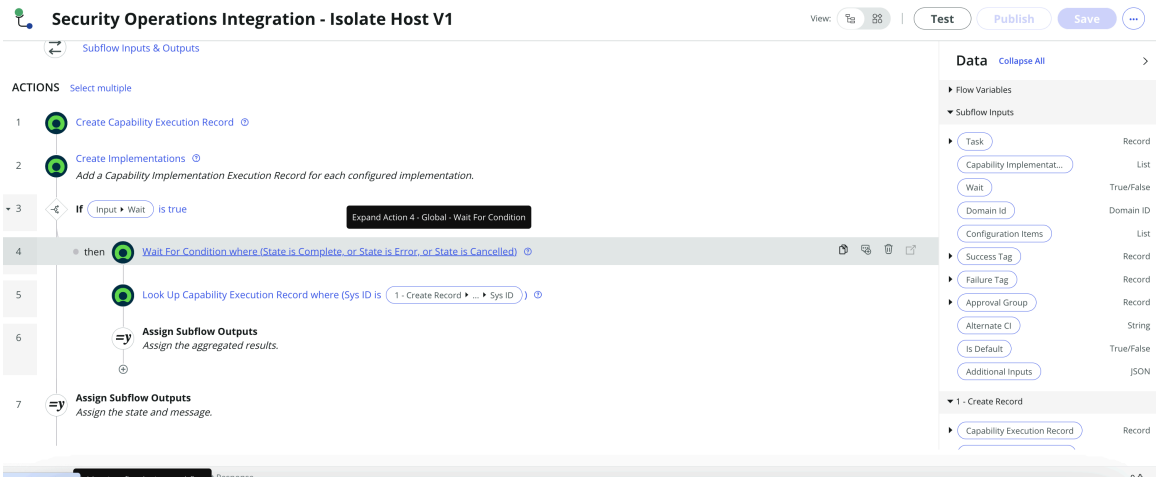
보안 운영 - 호스트 격리 플로우는 통합과 독립적인 상위 수준 플로우입니다. 구성된 쿼리를 사용하여 구성 항목 세트를 검색합니다. Carbon Black과 같은 통합을 이행하는 데 사용합니다.

시작하기 전에
필요한 역할: sn_si.analyst

이 태스크 정보
이 플로우는 보안 인시던트 관련 목록의 구성 항목 탭에서 트리거됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

호스트 격리



이 플로우와 관련된 활동은 여기에 설명되어 있습니다. 다른 활동에 대한 자세한 내용은 다음 문서를 참조하십시오 일반 Security Operations 통합 플로우 및 오케스트레이션 활동.

Security Operations Carbon Black 통합 - 호스트 분리 플로우

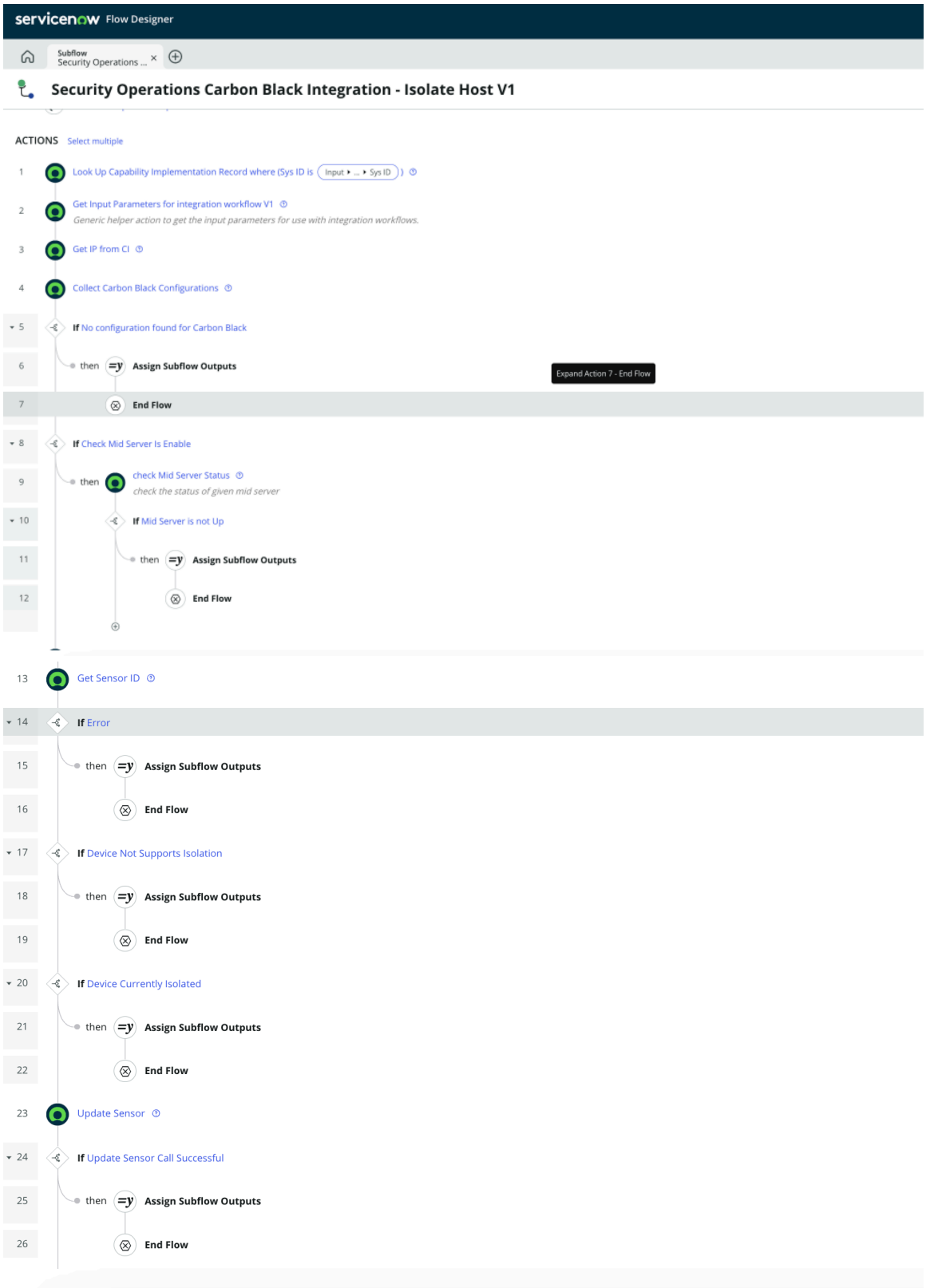
보안 운영 Carbon Black 통합 - 호스트 격리는 보안 운영 통합 - 호스트 격리 플로우로 시작된 Carbon Black 통합을 위한 구현입니다.

시작하기 전에
필요한 역할: sn_si.analyst

이 태스크 정보
플로우 프로세스 활동에는 다음이 포함됩니다.

- 실행 추적 - 시작(CI) 플로우 작업
- CI에서 IP 가져오기
- Carbon Black 구성 수집
- 역량 실행 추적 - 실패 플로우 작업
- 센서 ID 가져오기
- 네트워크 격리 설정 사용 작업
- 센서 업데이트 - 호스트 격리 결과를 반환합니다.
- 역량 실행 추적 - 플로우 작업 완료

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



이 플로우와 관련된 활동은 여기에 설명되어 있습니다. 다른 활동에 대한 자세한 내용은 다음 문서를 참조하십시오 일반 Security Operations 통합 플로우 및 오케스트레이션 활동.

센서 ID 플로우 작업 가져오기

센서 ID 가져오기 플로우 작업은 플로우에 사용할 센서 식별자를 수집합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

센서 ID 가져오기 플로우 작업은 플로우에 사용할 센서 정보를 수집하기 위해 모든 플로우와 함께 사용할 수 있습니다.

결과

이 플로우 작업의 가능한 결과는 다음과 같습니다.

결과

결과	설명
성공	센서 식별자를 찾았습니다.
실패	센서를 찾을 수 없습니다. 더 많은 오류 정보는 플로우 작업 출력 오류에서 확인할 수 있습니다.

입력 변수

입력 변수는 플로우 작업의 초기 동작을 결정합니다.

변수	설명
api_token	Carbon Black API 키입니다.
use_mid_server	REST 활동이 MID 서버를 사용하여 Carbon Black과 상호작용하는지 여부를 결정합니다.
endpoint_base	Carbon Black API의 기본 URL입니다.
ci_ip_address	구성 항목 IP 주소입니다.

출력 변수

출력 변수에는 후속 활동에 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
status_code	요청이 성공했는지 여부를 결정합니다. 그렇지 않은 경우 HTTP 오류 코드 및 메시지를 표시합니다.
배열 요소 유형	API 변수를 사용합니다.
sensor_detail	JSON 형식으로 된 Carbon Black 센서에 대한 설명입니다.

네트워크 격리 설정 사용 작업

네트워크 격리 사용 설정 워크플로우 활동은 네트워크 격리를 활성화합니다.

네트워크 격리 사용 설정 작업은 모든 워크플로와 함께 사용하여 네트워크 격리를 사용하도록 설정할 수 있습니다.

결과

이 활동의 가능한 결과는 다음과 같습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

결과

결과	설명
성공	네트워크 격리 사용.
실패	네트워크 격리를 사용할 수 없습니다. 자세한 오류 정보는 활동 출력 오류에서 확인할 수 있습니다.

입력 변수

입력 변수는 활동의 초기 동작을 결정합니다.

변수	설명
sensor_detail	JSON 형식으로 된 Carbon Black 센서에 대한 설명입니다.
사용 안 함	호스트를 격리할지 아니면 호스트 격리를 제거할지 여부를 결정합니다. True = 격리 사용 안 함 False = 격리가 활성화된 상태로 유지됨

출력 변수

출력 변수에는 후속 활동에 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
sensor_detail	JSON 형식으로 된 Carbon Black 센서에 대한 설명입니다.

센서 활동 업데이트

센서 업데이트 워크플로우 활동은 센서를 업데이트하여 호스트 또는 엔드포인트를 분리합니다.

센서 업데이트 활동은 호스트나 엔드포인트를 격리하기 위한 모든 워크플로우와 함께 사용할 수 있습니다.

결과

이 활동의 가능한 결과는 다음과 같습니다.

결과

결과	설명
성공	센서가 업데이트되었습니다.
실패	센서를 업데이트할 수 없습니다. 자세한 오류 정보는 활동 출력 오류에서 확인할 수 있습니다.

입력 변수

입력 변수는 활동의 초기 동작을 결정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

변수	설명
api_token	Carbon Black API 키입니다.
use_mid_server	REST 활동이 MID 서버를 사용하여 Carbon Black과 상호작용하는지 여부를 결정합니다.
endpoint_base	Carbon Black API의 기본 URL입니다.
sensor_id	센서 식별자입니다.
sensor_detail	JSON 형식으로 된 Carbon Black 센서에 대한 설명입니다.

출력 변수

출력 변수에는 후속 활동에 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
status_code	요청이 성공했는지 여부를 결정합니다. 그렇지 않은 경우 HTTP 오류 코드 및 메시지를 표시합니다.

보안 운영 **Carbon Black** 통합 **-** 호스트 격리 플로우 제거

보안 운영 **Carbon Black** 통합 **-** 호스트 격리 제거 플로우는 Carbon Black 시스템에서 지정된 호스트 또는 엔드포인트와의 통신 차단을 해제합니다.

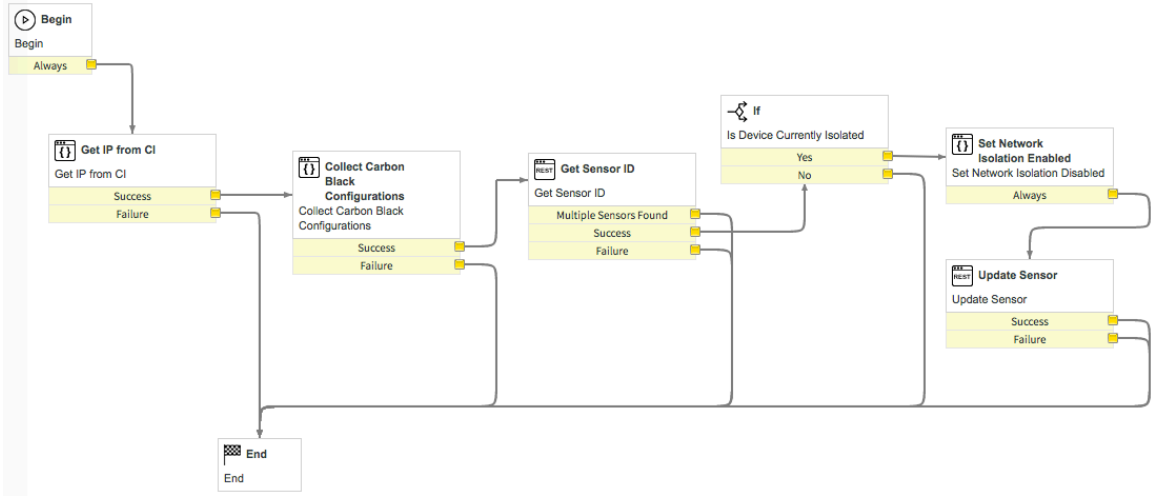
시작하기 전에
필요한 역할: sn_si.analyst

이 태스크 정보
이 플로우는 역량의 일부가 아니며 실행하려면 사용자 지정 오케스트레이션이 필요합니다.
플로우 프로세스 활동에는 다음이 포함됩니다.

- CI 활동에서 IP 가져오기
- 성공한 경우- Carbon Black 구성 수집 플로우 작업
- 센서 ID 플로우 작업 가져오기센서 ID 가져오기
- If - 디바이스가 격리를 지원하고 디바이스가 비활성화로 격리 되지 않습니다.
- 센서 활동 업데이트- 호스트 격리 결과를 반환합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Carbon Black 통합 - 호스트 격리 제거



보안 운영 통합 - 감시 목록에 게시 기능

감시 목록에 게시 기능은 보안 이벤트를 모니터링하고 경보를 생성하는 외부 공급업체 감시 목록에 보안 인시던트와 연관된 옵저버블 및 표시기를 추가합니다. 이 역량은 조사 중에 인시던트 응답의 일부로 사용됩니다.

주:
사용 가능한 구현이 없으면 역량 작업이 제품 메뉴에 표시되지 않습니다.

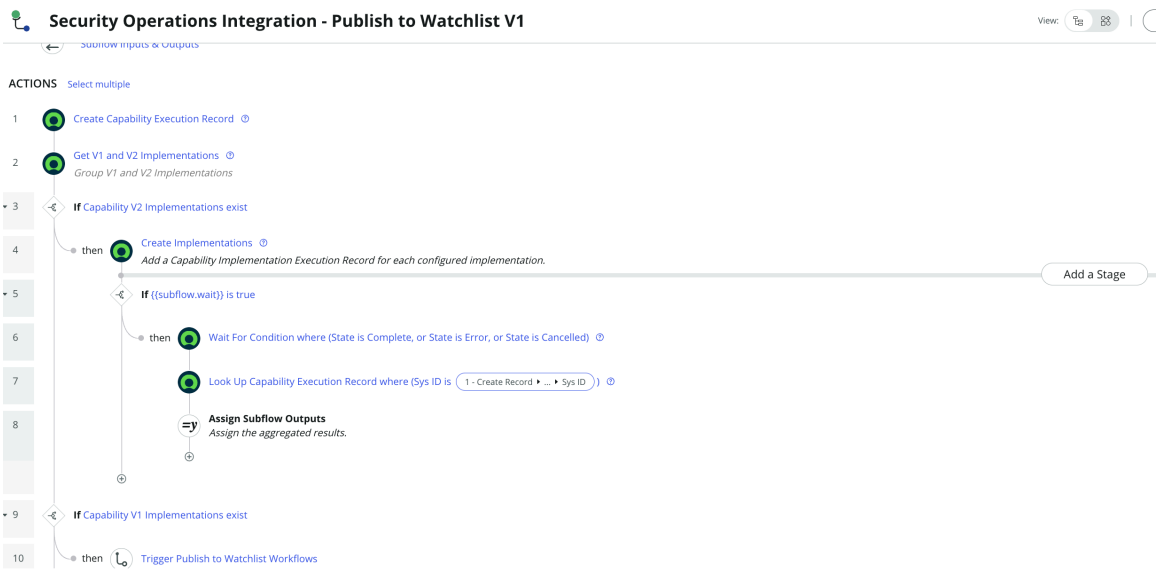
Security Operations Integration - 감시 목록에 게시 플로우

보안 운영 통합 - 감시 목록에 게시 플로우는 통합과 독립적인 상위 수준 플로우입니다. 역량을 지원하는 외부 공급업체 주시 목록에 옵저버블을 추가합니다. 이를 사용하여 통합을 수행합니다.

시작하기 전에
필요한 역할: sn_si.analyst

이 태스크 정보
이 플로우는 통합이 표시되는 경우에만 실행됩니다. 보안 인시던트의 옵저 버블 또는 관련 표시기 탭에서 트리거됩니다.

감시 목록에 게시



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 플로우와 관련된 활동은 여기에 설명되어 있습니다. 다른 활동에 대한 자세한 내용은 다음 문서를 참조하십시오 일반 Security Operations 통합 플로우 및 오케스트레이션 활동.

보안 운영 통합 - 사이팅 검색 역량

사이팅 검색 역량은 옵저버블 세트를 수락하고 사이팅 검색을 지원하는 통합을 찾은 다음 해당 검색을 실행합니다.

사이팅 검색 역량에는 사이팅 검색을 실행하는 워크플로우 Security Operations Integration - 사이팅 검색 플로우가 있습니다. 이 워크플로우는 옵저버블 목록을 수락하고, 구현 역량을 찾고, 사이팅 검색 구성을 기반으로 쿼리를 생성하고, 구성된 워크플로우를 기반으로 검색을 실행합니다. 검색이 완료되면 사이팅이 발견되었는지 여부와 발견되었다면 몇 개가 포함된 메모가 인시던트 작업 메모에 추가됩니다.

사이팅 검색 구성을 보려면 다음으로 이동하십시오. 보안 운영 〉 통합 〉 사이팅 검색 구성.

주:
사용 가능한 구현이 없으면 역량 작업이 제품 메뉴에 표시되지 않습니다.

사이팅 검색 구성 기록 생성

여러 사이팅 검색 구성 기록을 생성하여 여러 로그 저장소를 쿼리하거나 검색 매개변수를 변경하는 동안 사용합니다.

시작하기 전에
필요한 역할: sn_si.admin

- Splunk 인스턴스에 CIM 추가 기능을 설치해야 합니다.
- 저장된 검색 및 즉석 쿼리는 Splunk 통합에 대해서만 지원됩니다.

이 태스크 정보
사이팅 검색 구성 레코드를 생성하여 Splunk 엔터프라이즈 로그 저장소에 저장된 검색을 호출할 수도 있습니다.

주:
검색 구성 쿼리는 Splunk CIM(공통 정보 모델)을 준수하기 위해 Splunk 로그 데이터를 사용합니다.

저장된 검색 구성을 사용하여 다음을 수행할 수 있습니다.

- 여러 이벤트 기록을 결합하는 사용자 지정 검색을 생성합니다.
- 설계 효율적이고 효과적인 검색.
- Splunk 저장된 검색에서 매개변수화된 입력을 사용합니다.

기본 시스템에는 다음 이미지에 표시된 샘플 컨피그레이션이 포함되어 있습니다.

저장된 검색 구성

	Name	Observable type	Search	Is saved search
	Search	Search	Search	Search
	Default Proofpoint Inplace Search-Emails	Email	tag=email [| search tag="email" AND (sub...	false
	Default Saved Search - Emails	Email	args.email.subject=${email.subject}&args...	true
	Default PAN Inplace Search - URLs	URL	tag=network url=${observable} | table us...	false

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

저장된 검색 및 Inplace 구성 쿼리는 예제 쿼리이며 사용자 환경에 적합한 매개 변수로 대체할 수 있습니다. 필요에 따라 저장된 검색 구성을 추가로 생성합니다. 저장된 검색 구성을 정의할 때 검색 쿼리의 이름과 매개변수는 Splunk 인스턴스에 정의된 저장된 구성과 일치해야 합니다. 이름과 매개변수가 동일하지 않으면 사이팅 검색을 수행할 때 정확한 결과를 볼 수 없습니다.

주:
Splunk 인스턴스에서 검색, 보고서 및 경보 페이지로 이동하여 저장된 검색 쿼리를 찾습니다. 권한 링크를 눌러 권한 페이지로 이동합니다. 모든 앱 라디오 버튼을 선택하고 모든 사용자에 대해 읽기 권한 옵션을 활성화합니다. 이렇게 하면 저장된 검색 쿼리의 공유 열 값이 비공개에서 앱으로 변경됩니다. 이 항목이 설정되어 있지 않으면 저장된 검색 쿼리가 결과를 반환하지 않을 수 있습니다.

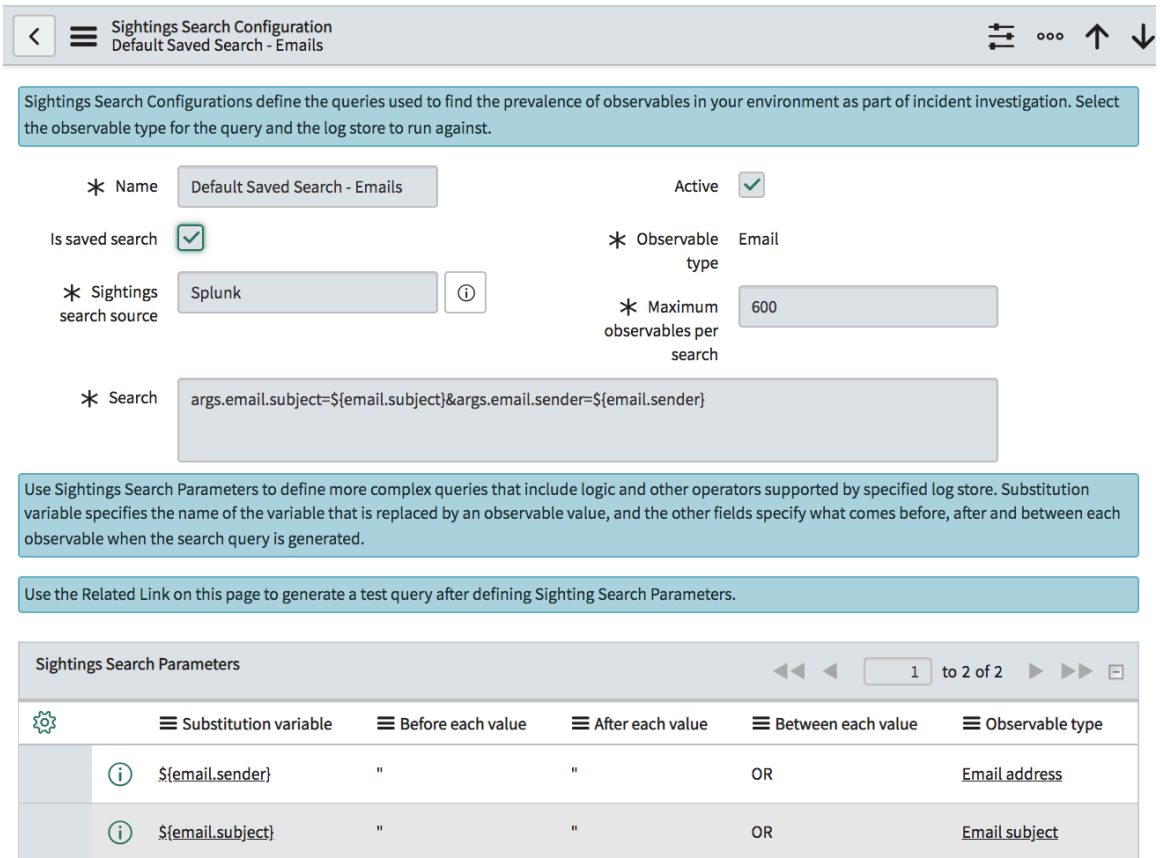
저장된 검색 구성이 Splunk 인스턴스에 정의된 구성과 일치하는지 확인하려면 다음을 수행합니다.

1. 다음으로 이동 설정 〉 검색, 보고서 및 경보.
2. 앱 컨텍스트를 모두로 변경합니다.

   검색 보고서 목록이 표시됩니다.
3. 저장된 검색 쿼리가 목록에 있는지 확인합니다.

예를 들어, 사이팅 검색 구성 양식에는 이메일 주소와 이메일 발신자가 검색 매개변수로 포함되어 있습니다.

사이팅 검색 구성 양식



Splunk 인스턴스에서 동일한 이름, 기본 저장된 검색 - 이메일, 이메일 주소 및 이메일 제목에 대한 동일한 검색 매개변수를 사용하여 저장된 검색을 정의합니다. 이름과 검색 매개변수가 동일하지 않으면 사이팅 검색이 정확한 결과를 생성하지 않습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 보안 운영 〉 통합 〉 사이팅 검색 구성 그런 다음 새 기록을 생성합니다(필드 설명은 표 참조).

사이팅 검색 구성 양식

필드	설명
이름	구성의 이름입니다.
저장된 검색 여부	이 옵션을 선택하면 저장된 검색 구성이 생성됩니다.
관찰 검색 소스	사이팅 검색의 소스입니다. Splunk 로그 저장소를 소스로 선택합니다.
활성	저장된 검색 상태에 대한 옵션입니다. 사이팅 검색을 수행하는 데는 활성 검색 구성만 사용할 수 있습니다.
옵저버블 유형	옵저버블 유형은 IP, 해시 값, URL, 도메인 이름 등과 같은 모든 옵저버블 유형일 수 있습니다.
검색당 최대 옵저버블	검색에서 반환될 최대 옵저버블 수입니다.
검색	기본 검색 문자열은 $(observable)이지만 Splunk 로그 저장소에서 지원하는 매개변수를 지정하여 사용자 고유의 검색 쿼리를 정의할 수 있습니다.

2. 제출을 클릭합니다.

결과
사이팅 검색 구성 기록을 생성했습니다.

다음에 수행할 작업
검색 쿼리를 정의한 후 사이팅 검색 테스트 쿼리 생성을 클릭하고 옵저버블 값 목록을 지정하여 이 저장된 검색 구성을 기반으로 테스트 쿼리를 생성합니다.

사이팅 검색 실행

시간 경과에 따른 위협의 확산을 확인하거나 정정 또는 근절 노력을 테스트합니다. 보안 인시던트에서 개별 또는 여러 옵저버블과 검색 날짜 범위를 선택할 수 있습니다. 결과는 보안 인시던트 옵저버블 관련 목록에 포함됩니다.

시작하기 전에
필요한 역할: sn_si.analyst

이 태스크 정보
사이팅 검색 역량에는 사이팅 검색을 실행하는 플로우 Security Operations Integration - 사이팅 검색 플로우가 있습니다. 이 플로우는 옵저버블 목록을 수락하고, 구현 역량을 찾고, 사이팅 검색 구성을 기반으로 쿼리를 생성하고, 구성된 플로우를 기반으로 검색을 실행합니다.

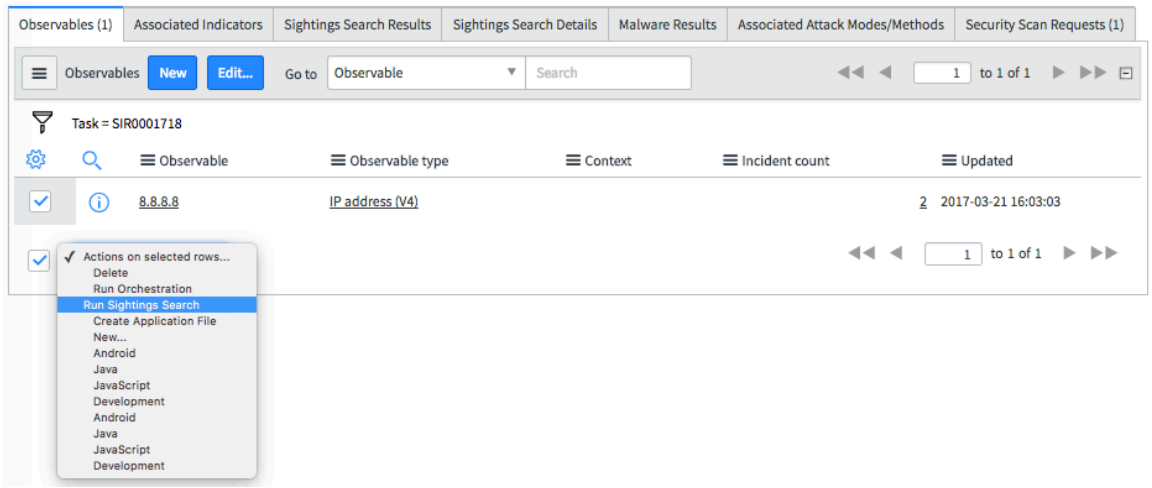
주:
활성 구현을 구성해야 합니다. Sightings Search는 Elasticsearch, Splunk, McAfee ESM, HPE ArcSight Logger 및 QRadar 인시던트 보강을 지원합니다. 사용 가능한 구현이 없으면 사이팅 검색 실행과 같은 역량 작업이 제품 메뉴에 표시되지 않습니다.

프로시저

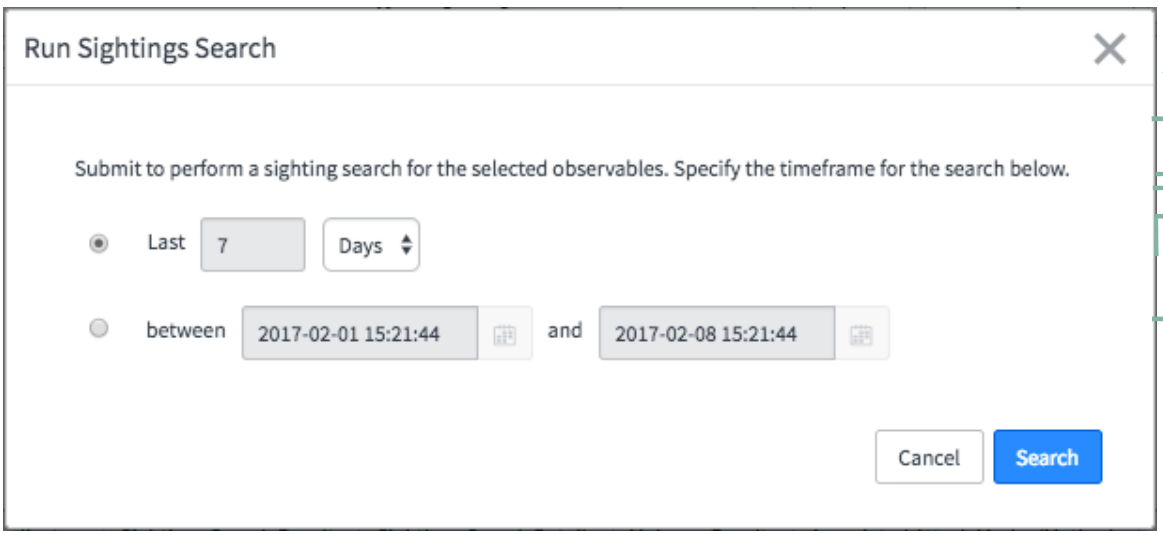
1. 보안 인시던트로 이동합니다.
2. **IoC** 표시 관련 링크를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 관련 목록 탭에서 옵저버블을 선택합니다.
4. 사이팅 검색을 수행할 옵저버블을 선택합니다.
5. 선택한 행에 대해 수행할 작업... 드롭다운 메뉴에서 사이팅 검색 실행을 클릭합니다.



사이팅 검색 실행 대화 상자가 열립니다.



주:
대화 상자에 입력한 값은 이 실행에 대한 역량 구성 값을 덮어씁니다.

6. 데이터를 검색할 일 수 또는 날짜 범위를 선택합니다.

옵션	설명
마지막	검색할 인시던트를 작성하기 전의 시간 또는 일수입니다. 기본값은 7일입니다. 한도는 99시간 또는 일입니다.
다음 날짜 사이	검색할 날짜 범위입니다. 기본 날짜는 다음과 같습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵션	설명
	인시던트가 열린 날짜 및 시간입니다. 인시던트가 열리기 7일 전의 날짜 및 시간입니다.

주:
마지막 은 검색할 인시던트가 생성되기 전의 시간 또는 일수입니다. 기본값은 7일입니다. 한도는 99시간 또는 일입니다.

7. 검색을 클릭합니다.
사이팅 검색 기록이 생성됩니다. 집계 및 연관된 사이팅 데이터는 사이팅 검색 결과 및 사이팅 검색 상세 정보 탭 아래의 보안 인시던트에 표시됩니다.

주:
사이팅 검색 결과 데이터는 원시 데이터를 포함하도록 구성된 구현의 경우 원시 데이터를 제외하고 와 공유할 Trusted Security Circle수 있습니다.

사이팅 검색 결과

결과	설명
번호	사이팅 검색의 식별자입니다.
옵저버블 수	쿼리로 검색된 옵저버블 수입니다.
내부 사이팅	내부 사이팅 수입니다.
외부 사이팅	외부 사이팅 수입니다. (위협 공유에서 수신)
일치하는 구성 항목	사용자 환경에서 발견된 각 옵저버블에 대해 CMDB의 기존 기록과 일치하는 구성 항목 수입니다.
시작 날짜 범위	목격을 찾기 시작할 시간입니다.
종료 날짜 범위	목격을 찾는 것을 멈출 시간입니다.
업데이트됨	마지막으로 수정한 날짜 및 시간입니다.

메모: 사이팅 검색에 사용되는 구현이 원시 데이터를 포함하도록 구성되어 있고 하나 이상의 사이팅이 발견되면 원시 데이터 샘플이 포함된 첨부 파일이 보안 인시던트의 맨 위에 나타납니다.

사이팅 검색 상세 정보

상세 정보	설명
사이팅 검색	사이팅 검색의 식별자입니다.
옵저버블	쿼리로 검색된 옵저버블입니다.
옵저버블 유형	쿼리로 검색되는 옵저버블의 유형입니다.
내부 사이팅	내부 사이팅의 집계 수입니다.
외부 사이팅	집계된 외부 사이팅 수입니다. (위협 공유에서 수신)
업데이트됨	마지막으로 수정한 날짜 및 시간입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

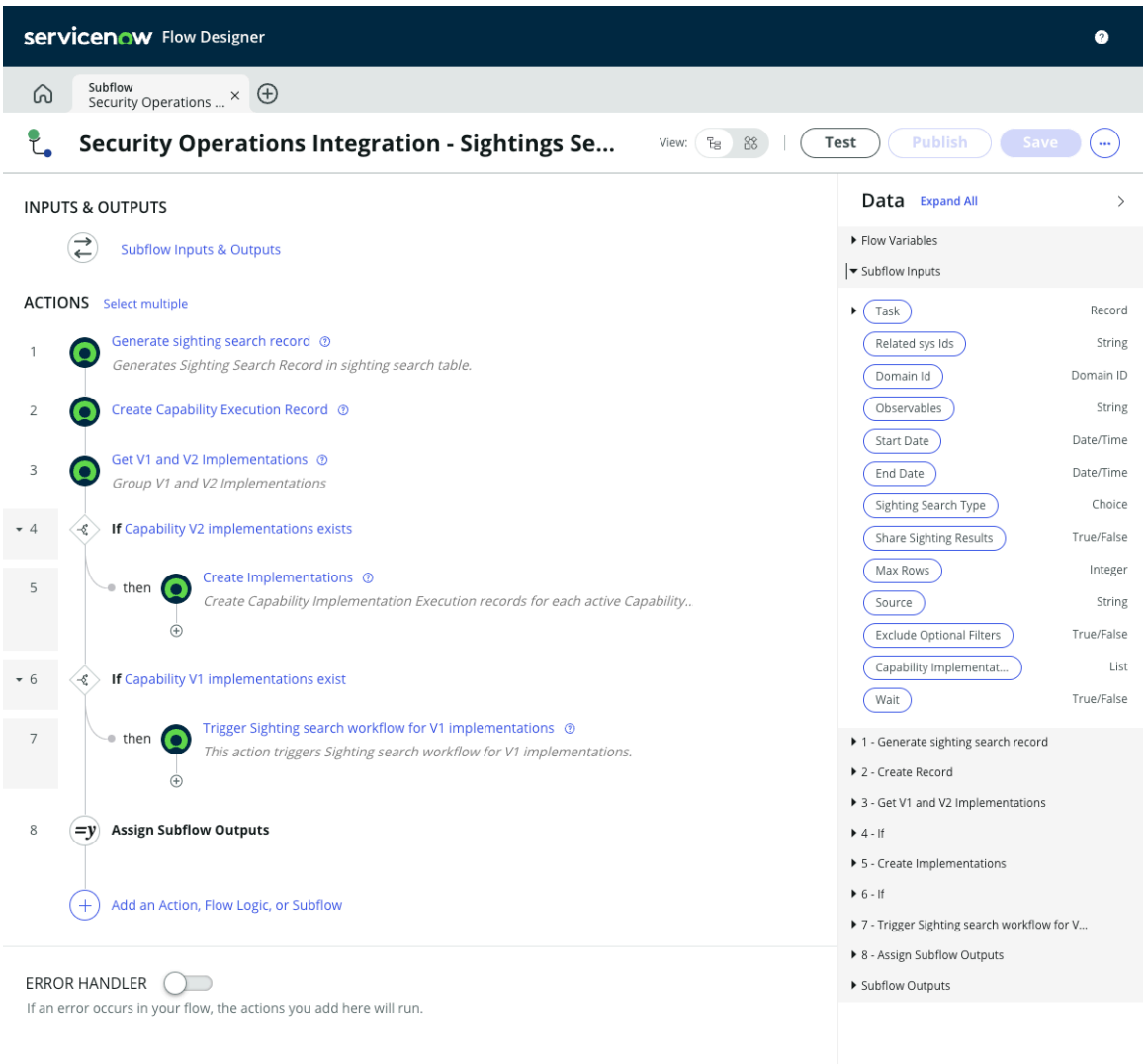
Security Operations Integration - 사이팅 검색 플로우

Security Operations Integration - 사이팅 검색 플로우는 통합과 독립적인 상위 수준 플로우입니다. 구성된 쿼리를 사용하여 기능을 지원하는 구성된 통합을 기반으로 옵저버블 집합을 검색합니다. 이를 사용하여 Splunk 또는 Elasticsearch와 같은 통합을 수행합니다.

시작하기 전에
필요한 역할: sn_si.analyst

이 태스크 정보
보안 인시던트에 옵저버블이 첨부되어 있는 경우 보안 인시던트 옵저버블 탭의 선택한 행에 대한 작업... 드롭다운 메뉴에서 사이팅 검색 실행을 클릭하면 이 플로우가 트리거됩니다.

사이팅 검색



이 플로우와 관련된 활동은 여기에 설명되어 있습니다. 다른 활동에 대한 자세한 내용은 다음 문서를 참조하십시오 일반 Security Operations 통합 플로우 및 오케스트레이션 활동.

사이팅 검색 - 옵저버블 활동 결정

사이팅 검색 - 옵저버블 결정 워크플로우 활동은 워크플로우에 포함할 옵저버블을 결정합니다.

사이팅 검색 - 옵저버블 결정 활동은 워크플로우에 포함할 옵저버블을 결정하기 위해 모든 워크플로우와 함께 사용할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

결과

이 활동의 가능한 결과는 다음과 같습니다.

결과

결과	설명
성공	옵저버블 찾음
실패	옵저버블을 찾을 수 없습니다. 자세한 오류 정보는 활동 출력 오류에서 확인할 수 있습니다.

입력 변수

입력 변수는 활동의 초기 동작을 결정합니다.

변수	설명
task_sys_id	작업 식별자(보안 인시던트를 옵저버블에 매핑)입니다.
옵저버블	IP 주소, 해시, URL, 도메인 이름
workflow_current_sys_id	현재 기록의 시스템 식별자입니다. (task_sys_id 옵저버블 입력을 사용할 수 없는 경우에만 사용됩니다.

출력 변수

출력 변수에는 후속 활동에 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
옵저버블	필터링된 옵저버블

지속 옵저버블 사이팅 활동

지속 옵저버블 사이팅 워크플로우 활동은 외부 공급업체 통합에서 옵저버블을 검색합니다.

지속 옵저버블 사이팅 활동은 외부 공급업체 통합에서 발견된 옵저버블을 기록하기 위해 모든 워크플로우와 함께 사용할 수 있습니다.

결과

이 활동의 가능한 결과는 다음과 같습니다.

결과

결과	설명
성공	검색된 옵저버블입니다.
실패	옵저버블을 수집하는 동안 오류가 발생했습니다. 자세한 오류 정보는 활동 출력 오류에서 확인할 수 있습니다.

입력 변수

입력 변수는 활동의 초기 동작을 결정합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

변수	설명
sightingsResponse	
taskId	작업 식별자입니다.

출력 변수

출력 변수에는 후속 활동에 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
response	

옵저버블 사이팅 쿼리 활동 가져오기

옵저버블 사이팅 쿼리 가져오기 워크플로우 활동은 통합 구성에서 쿼리를 검색합니다.

옵저버블 사이팅 쿼리 가져오기 활동은 병렬 흐름 시작 관리자를 사용하여 지정된 구현에 보낼 쿼리를 가져오기 위해 모든 워크플로우와 함께 사용할 수 있습니다.

결과

이 활동의 가능한 결과는 다음과 같습니다.

결과

결과	설명
성공	쿼리가 발견되었습니다.
실패	쿼리를 가져오는 동안 오류가 발생했습니다. 자세한 오류 정보는 활동 출력 오류에서 확인할 수 있습니다.

입력 변수

입력 변수는 활동의 초기 동작을 결정합니다.

변수	설명
옵저버블	필터링된 옵저버블의 목록입니다.
역량	지원되는 역량 목록입니다.

출력 변수

출력 변수에는 후속 활동에 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
쿼리	검색 문자열입니다.
쿼리 카운트	실행할 쿼리 수입니다.

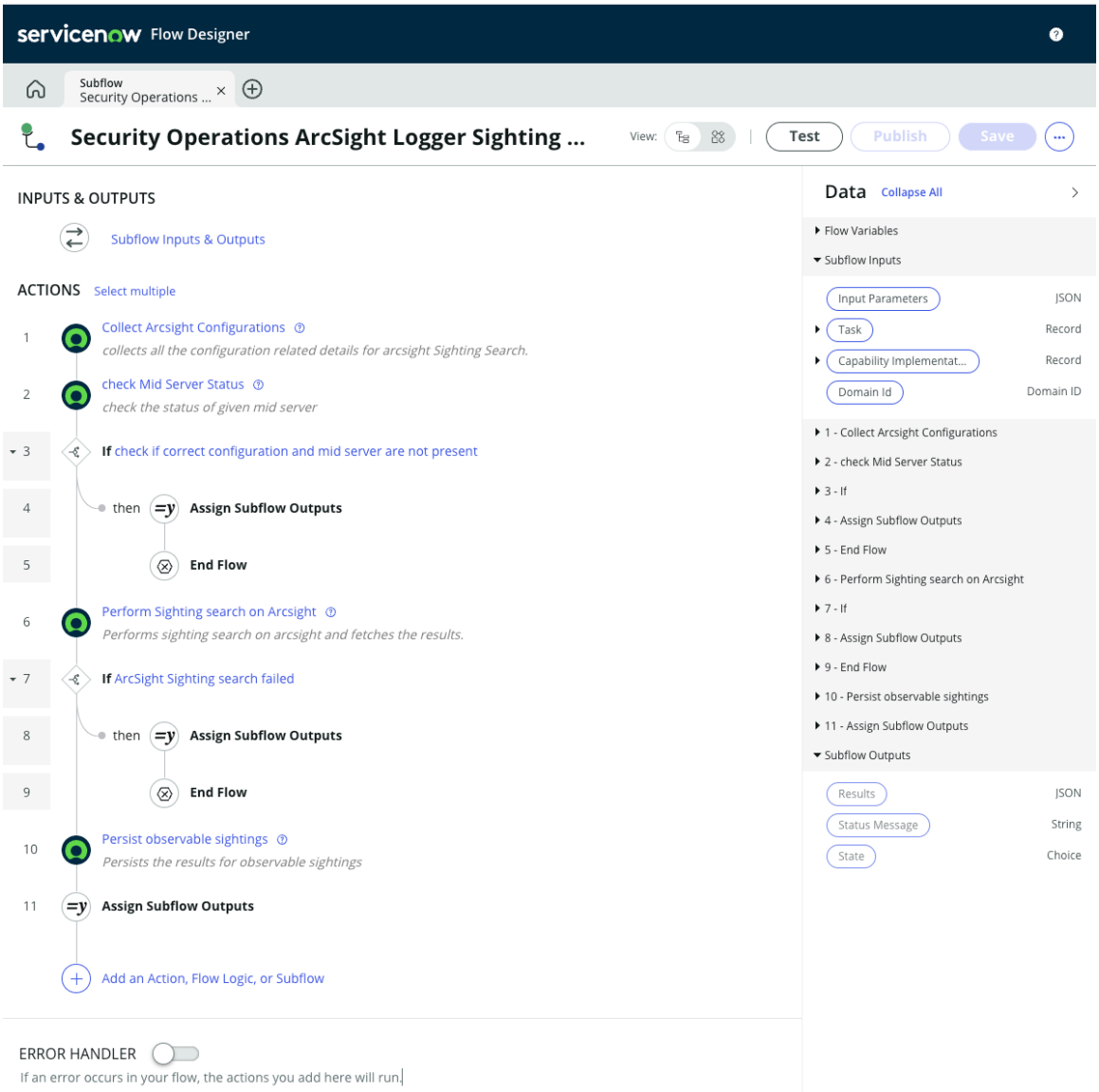
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 운영 - **Arcsight** 로거 사이팅 검색 플로우

보안 운영 - **ArcSight** 로거 사이팅 검색 플로우는 보안 운영 통합 - 사이팅 검색 플로우로 시작하는 Splunk 통합을 위한 구현입니다.

필요한 역할: sn_si_analyst

Arcsight 로거 사이팅 검색



이 플로우와 관련된 활동은 여기에 설명되어 있습니다. 다른 활동에 대한 자세한 내용은 다음 문서를 참조하십시오 일반 Security Operations 통합 플로우 및 오케스트레이션 활동.

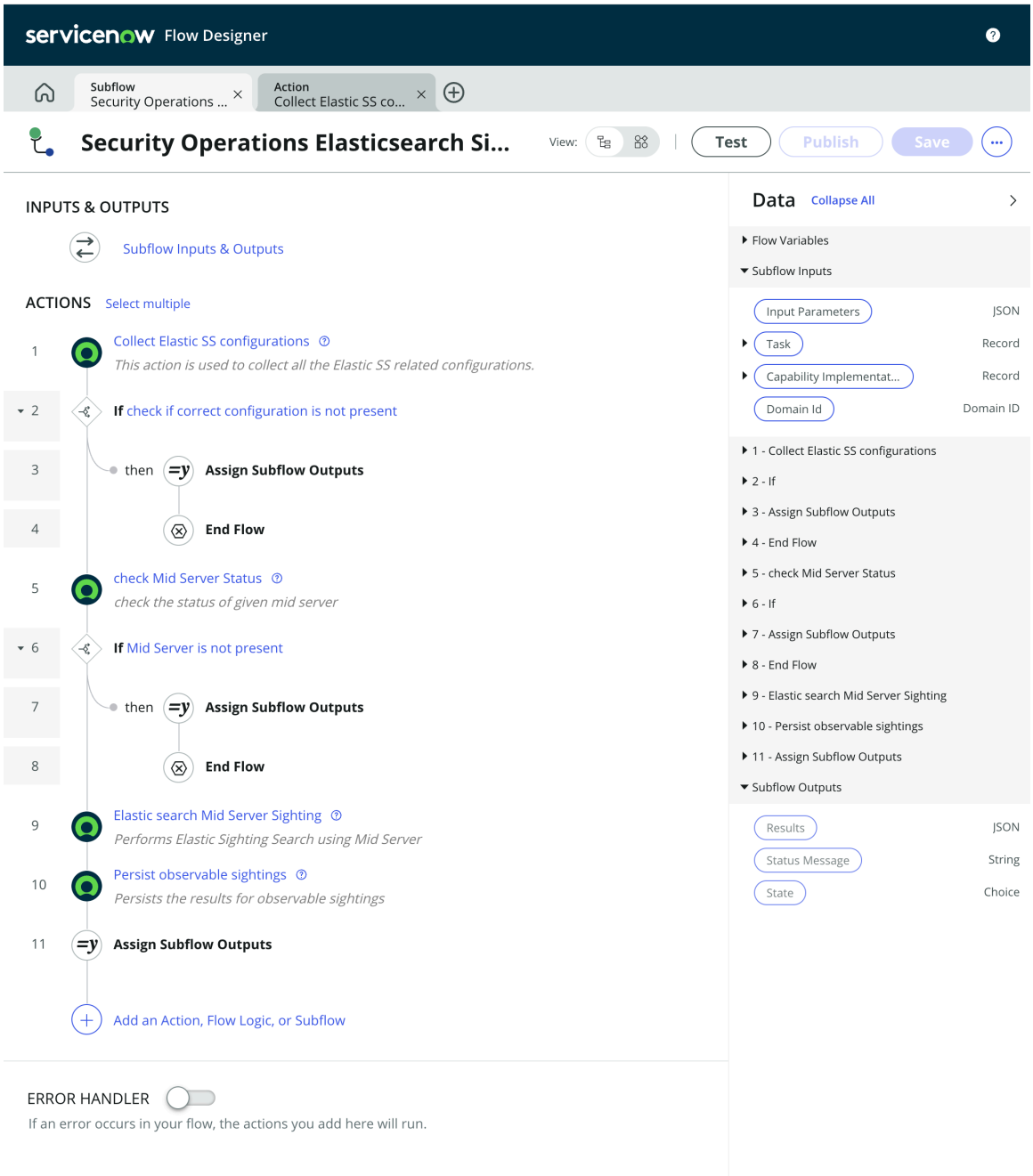
보안 운영 - **Elasticsearch** 사이팅 검색 플로우

보안 운영 - **Elasticsearch** 관찰 검색 플로우는 보안 운영 통합 - 관찰 검색 플로우로 시작되는 Elasticsearch 구현입니다.

필요한 역할: sn_si.analyst

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Elasticsearch 관찰 검색



이 플로우와 관련된 활동은 여기에 설명되어 있습니다. 다른 활동에 대한 자세한 내용은 다음 문서를 참조하십시오 일반 Security Operations 통합 플로우 및 오케스트레이션 활동.

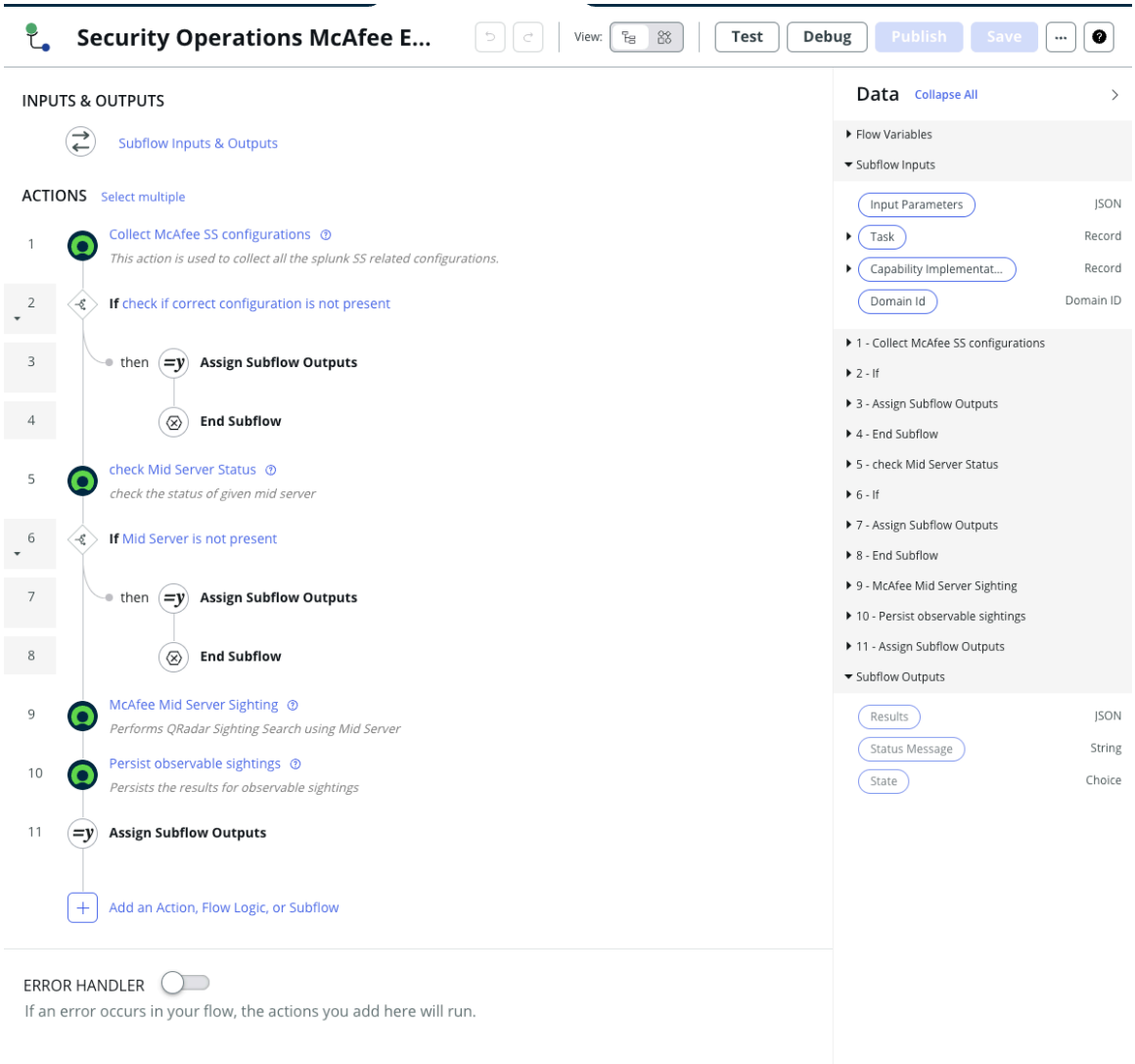
보안 운영 - McAfee ESM 사이팅 검색 플로우

보안 운영 - **McAfee ESM** 사이팅 검색 플로우는 보안 운영 통합 - 사이팅 검색 플로우에서 시작된 McAfee 사이팅 검색 구현을 위한 구현입니다.

필요한 역할: sn_si_analyst

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

McAfee ESM 사이팅 검색



이 플로우와 관련된 활동은 여기에 설명되어 있습니다. 다른 활동에 대한 자세한 내용은 다음 문서를 참조하십시오 일반 Security Operations 통합 플로우 및 오케스트레이션 활동.

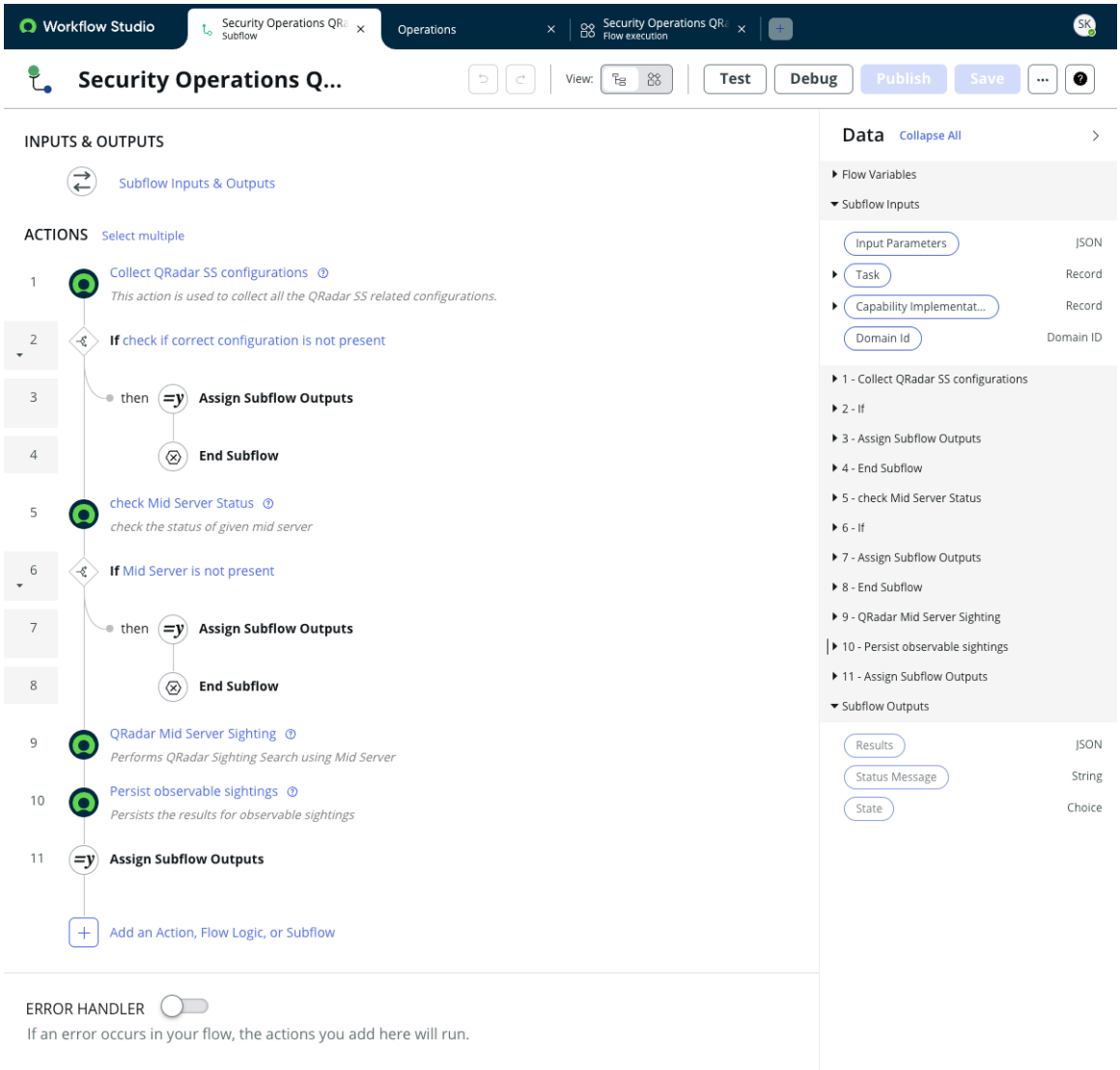
보안 운영 - QRadar 사이팅 검색 플로우

Security Operations - QRadar Sightings Search 플로우는 **Security Operations Integration - Sightings Search** 플로우에서 실행되는 IBM QRadar 통합을 위한 구현입니다.

필요한 역할: sn_si_analyst

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

QRadar 사이팅 검색



이 플로우와 관련된 활동은 여기에 설명되어 있습니다. 다른 활동에 대한 자세한 내용은 다음 문서를 참조하십시오 일반 Security Operations 통합 플로우 및 오케스트레이션 활동.

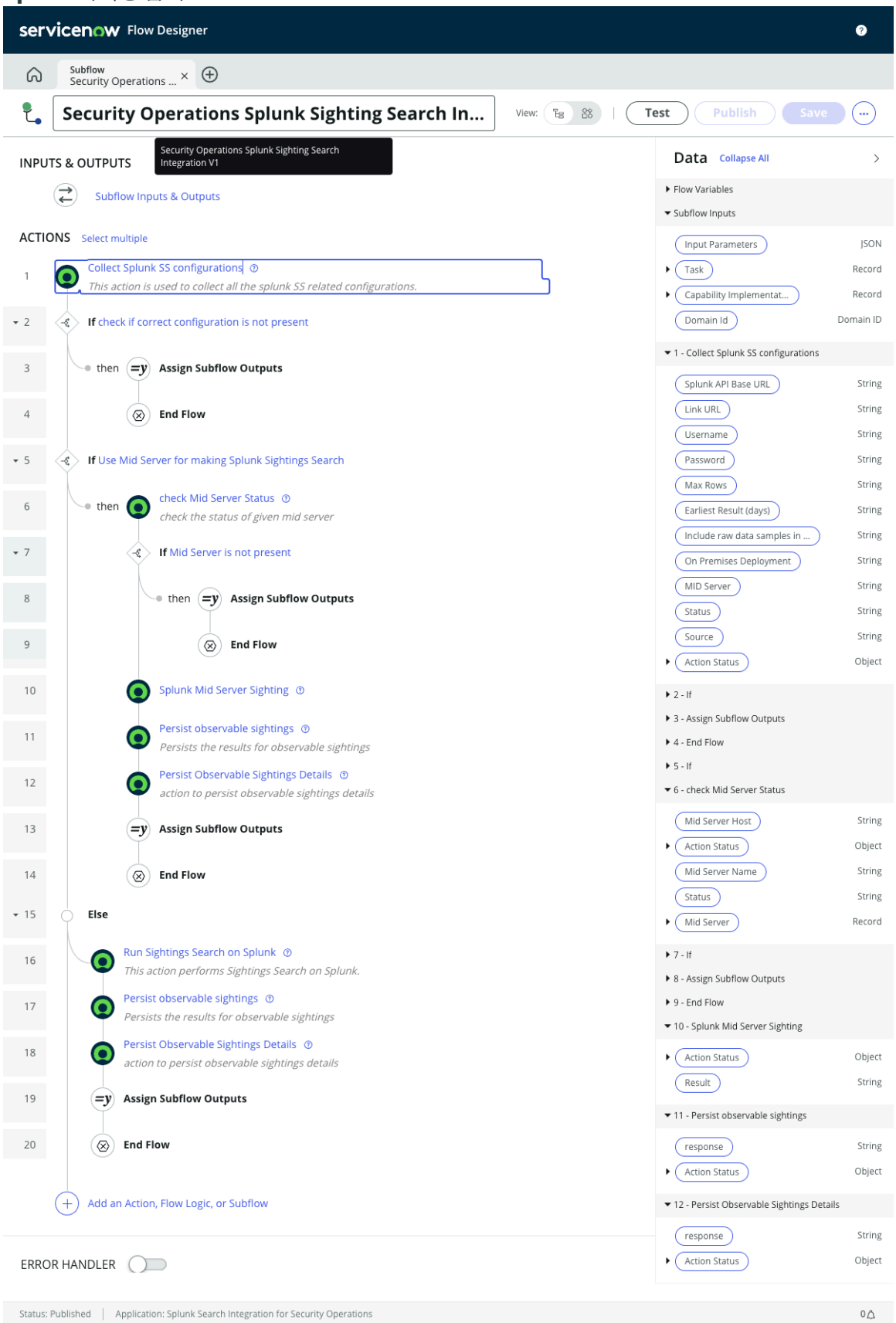
보안 운영 통합 **- Splunk** 사이팅 검색 플로우

보안 운영 **- Splunk** 사이팅 검색 플로우는 보안 운영 통합 **-** 사이팅 검색 플로우로 시작되는 Splunk 통합을 위한 구현입니다.

필요한 역할: sn_si_analyst

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Splunk 사이팅 검색



이 플로우와 관련된 활동은 여기에 설명되어 있습니다. 다른 활동에 대한 자세한 내용은 다음 문서를 참조하십시오 일반 Security Operations 통합 플로우 및 오케스트레이션 활동.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사이팅 검색 결과 보기

내부 및 외부 악성 표시기에 대한 사이팅 검색 결과를 검토할 수 있습니다.

시작하기 전에

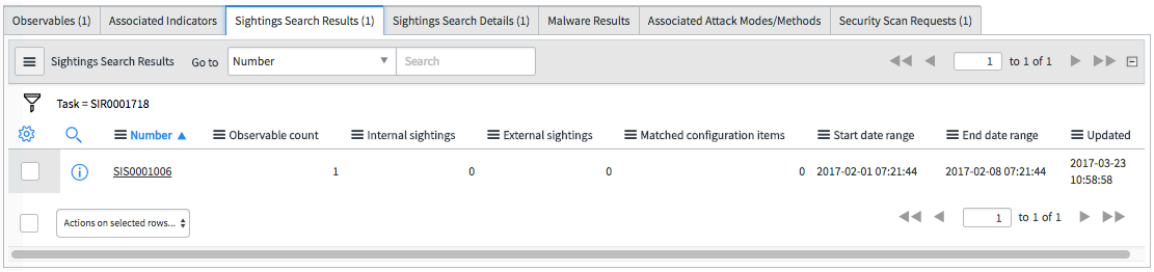
필요한 역할: sn_si.analyst

이 태스크 정보

.

프로시저

1. 보안 인시던트로 이동합니다.
2. 사이팅 검색 목록을 보려면 **IoC** 관련 목록 표시 그룹에서 사이팅 검색 결과 탭을 선택합니다.



주:
이 데이터는 와 공유할 Trusted Security Circle수 있습니다.

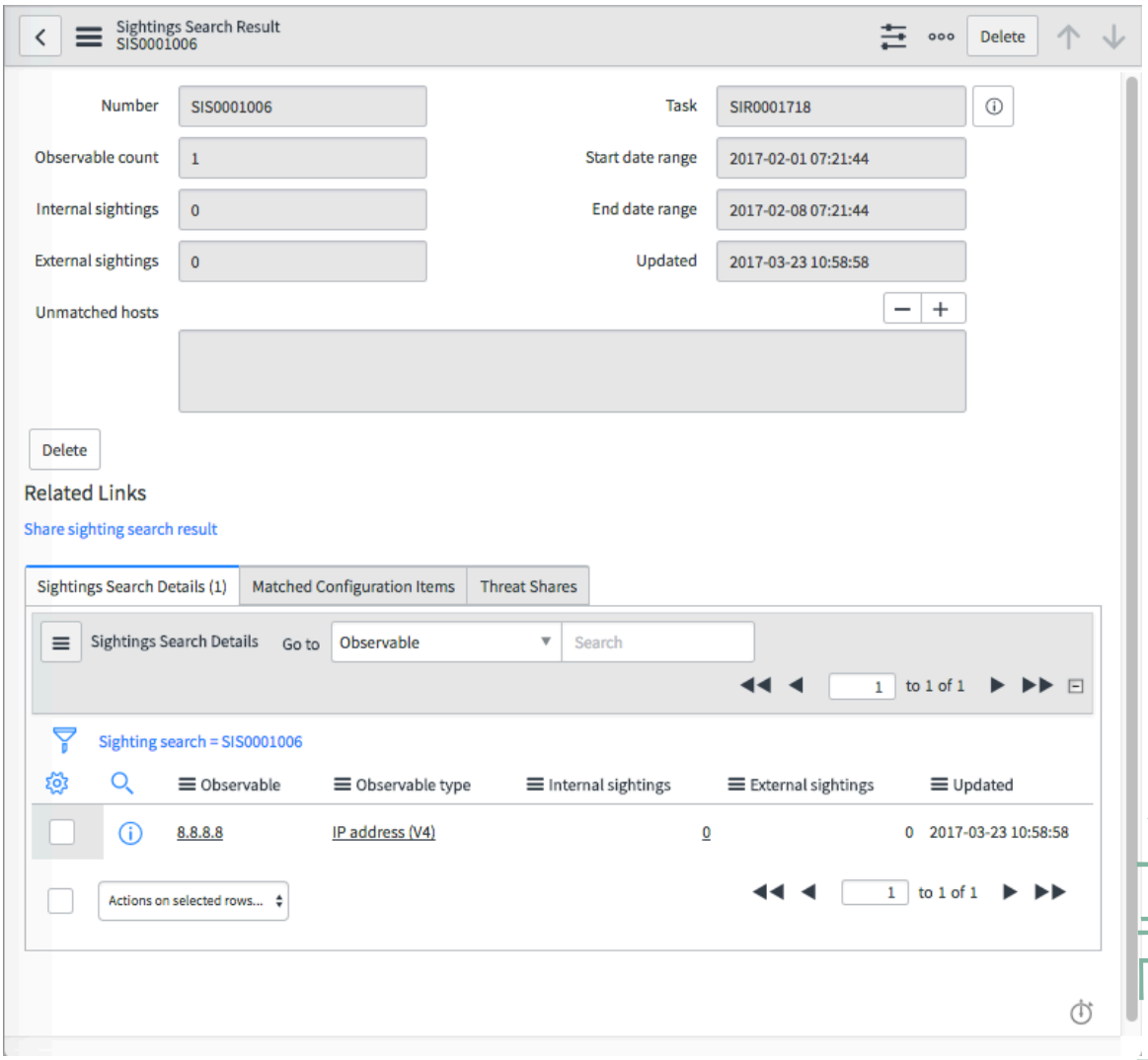
사이팅 검색 결과

결과	설명
번호	사이팅 검색 식별자입니다.
옵저버블 수	검색된 옵저버블 수입니다.
내부 Sightings	내부 사이팅의 집계 수입니다.
외부 관찰	집계된 외부 사이팅 수입니다. (위협 공유에서 수신)
일치하는 구성 항목	CMDB의 기존 기록과 일치하는 구성 항목의 집계 수입니다.
시작 날짜 범위	목격을 찾기 시작할 시간입니다.
종료 날짜 범위	목격을 찾는 것을 멈출 시간입니다.
업데이트됨	마지막으로 수정한 날짜 및 시간입니다.

단일 검색의 상세 정보를 보려면 다음을 수행합니다.

3. 사이팅 검색 결과 목록에서 사이팅 검색을 클릭합니다.
   사이팅 검색 결과 양식이 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



사이팅 검색 결과 양식

상세 정보	설명
번호	내부 사이팅 검색 식별자입니다.
옵저버블 수	이 쿼리에서 검색한 옵저버블 수입니다.
내부 사이팅	이 검색에 대한 내부 사이팅 수입니다.
외부 사이팅	이 검색에 대한 외부 사이팅 수입니다. (에서 Trusted Security Circle받음)
일치하지 않는 호스트	CMDB의 기록과 일치하지 않는 이 검색에 대한 잠재적 구성 항목 목록입니다.
작업	보안 인시던트 작업 식별자입니다.
시작 날짜 범위	사이팅 검색이 시작된 시간입니다.
종료 날짜 범위	사이팅 검색이 중지된 시간입니다.
업데이트됨	마지막으로 수정한 날짜 및 시간입니다.
사이팅 검색 정보	유형, 사이팅 수 및 수정 날짜.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

상세 정보	설명
일치하는 구성 항목	CMDB의 기존 기록과 일치하는 구성 항목 수입니다. CI 및 사이팅을 나열합니다.
위협 공유	와 공유된 Trusted Security Circle위협 목록입니다.

사이팅 검색 결과 공유

특정 검색과 연결된 로컬 사이팅, 세부 정보 또는 결과를 Trusted Security Circle과 공유할 수 있습니다.

시작하기 전에

필요한 역할: sn_si.analyst

이 태스크 정보

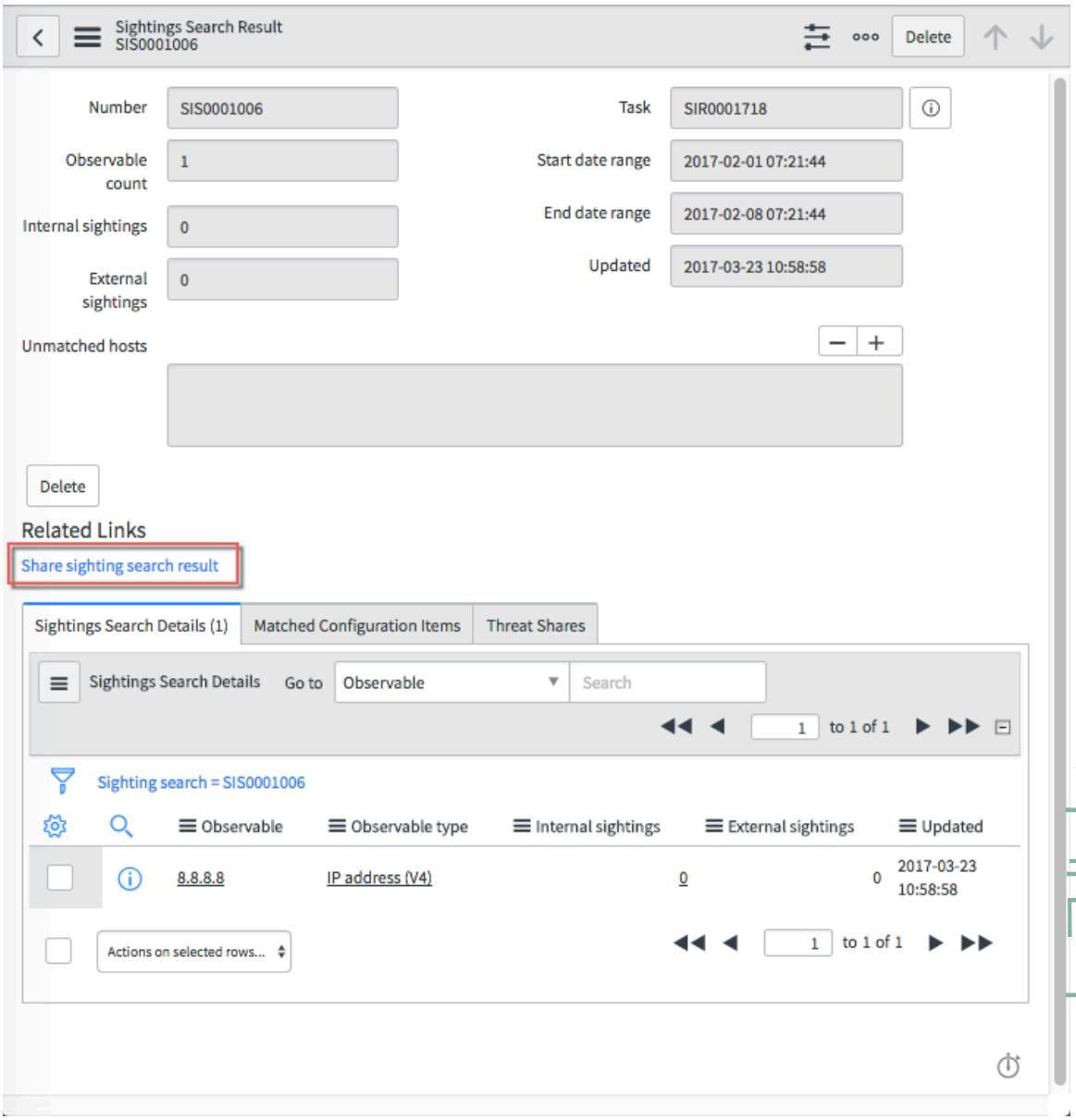
다음 보안 인시던트 응답 속성을 사용하여 공유를 자동화할 수 있습니다.

- 사이팅 검색 결과를 기본 ServiceNow 신뢰 원에 자동으로 공유
- 사이팅 검색 결과를 자동으로 공유할 때 로컬 사이팅이 없는 옵저버블 포함
- 신뢰할 수 있는 서클에서 위협 공유를 수신할 때마다 로컬 목격으로 대응

프로시저

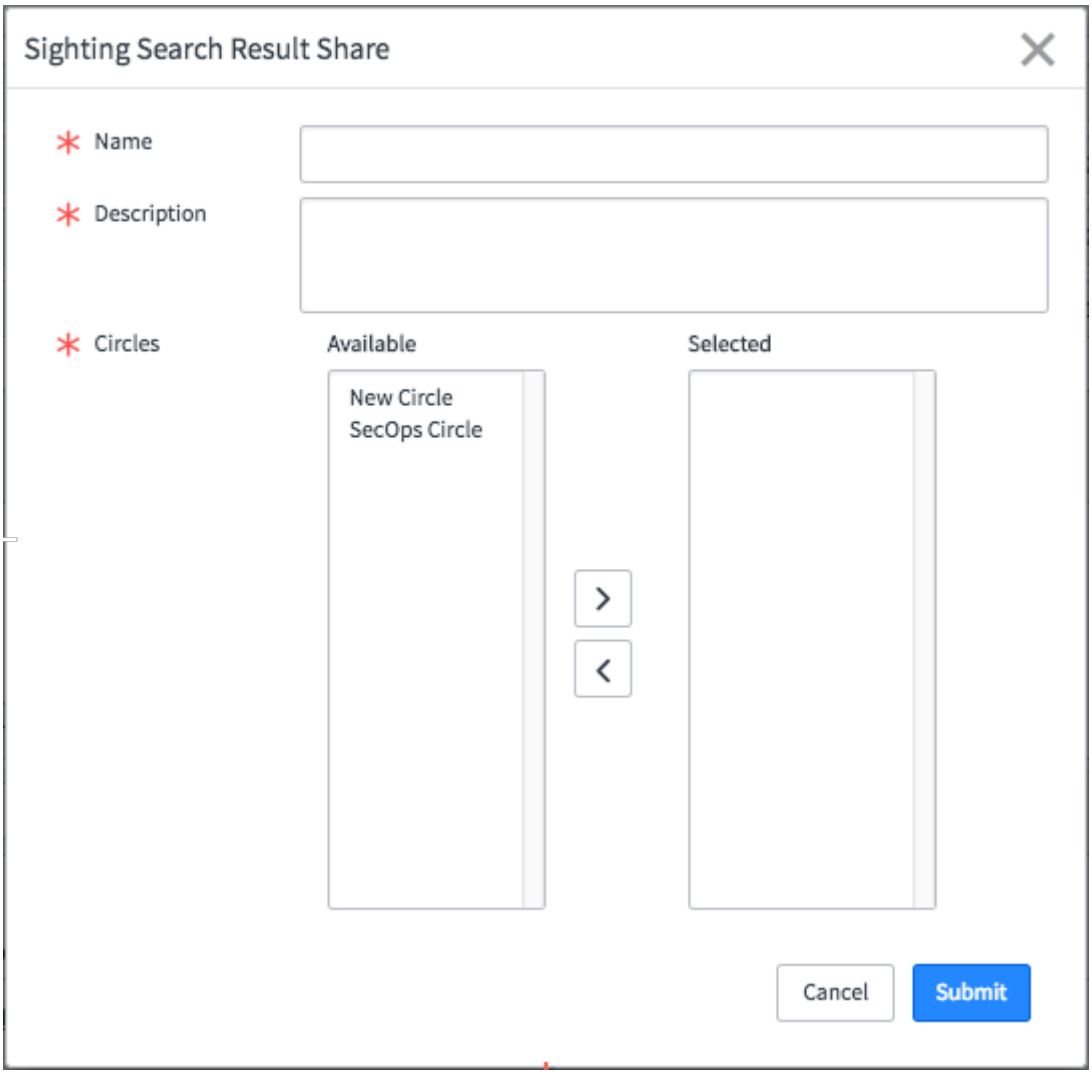
1. 보안 인시던트로 이동합니다.
2. **IoC** 관련 목록 표시를 클릭하고 사이팅 검색 결과 탭을 선택하여 사이팅 검색 목록을 봅니다.
3. 사이팅 검색 결과를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 사이팅 검색 결과양식에서 사이팅 검색 결과 공유 관련 링크를 클릭합니다.
사이팅 검색 결과 공유 대화 상자가 나타납니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



5. 이 옵저버블 공유 기록의 이름을 입력합니다.
6. 공유할 옵저버블에 대한 설명을입력합니다.
7. 옵저버블을 공유할 서클을 선택합니다.
8. 제출을 클릭합니다.
   옵저버블은 지정된 신뢰할 수 있는 서클과 공유됩니다.

보안 인시던트의 옵저버블 공유

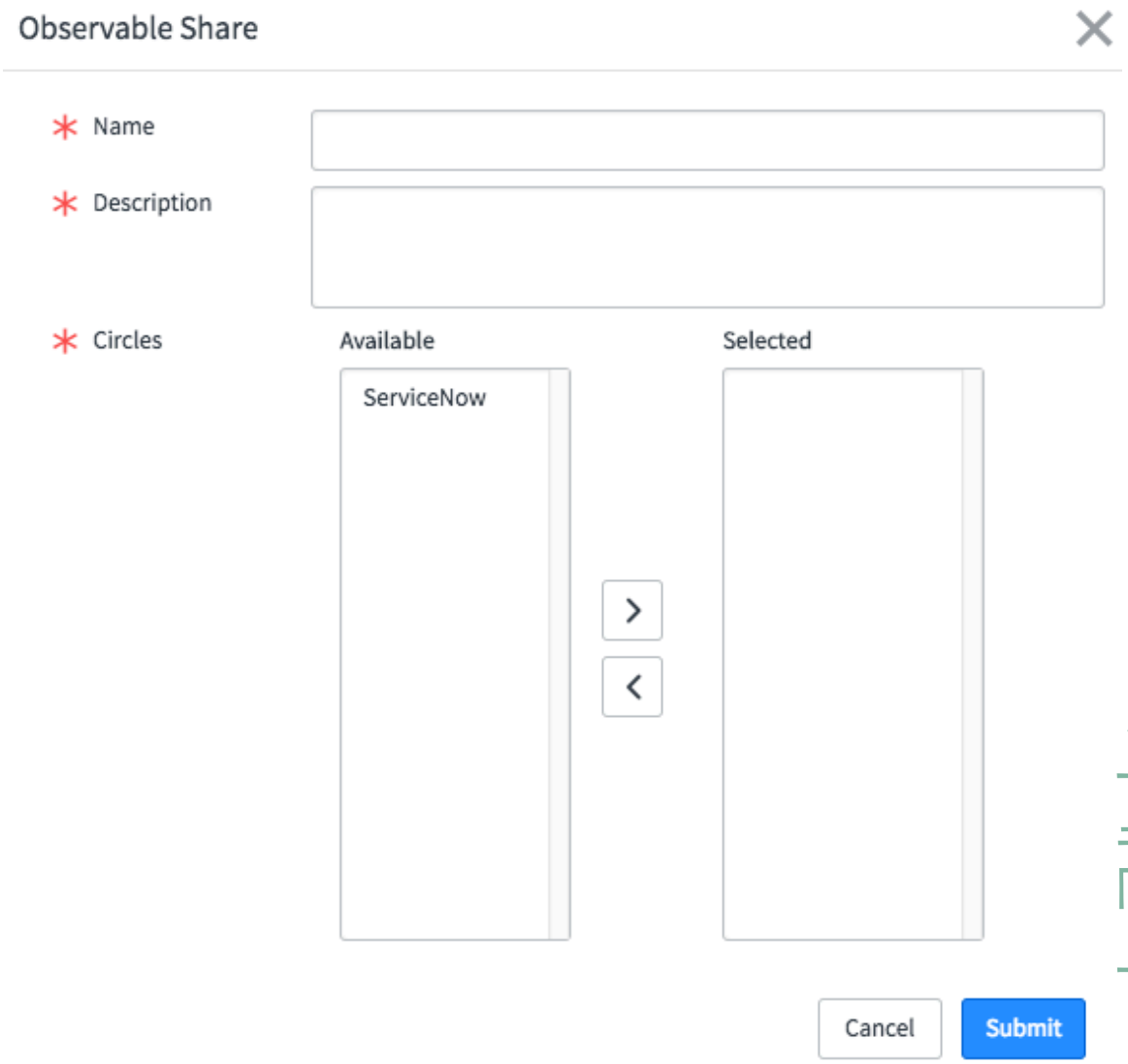
옵저버블은 보안 인시던트 보안 인시던트 응답 에서 신뢰할 수 있는 서클의 구성원과 공유할 수 있습니다.

시작하기 전에
필요한 역할: sn_si.analyst

프로시저
1. 보안 인시던트로 이동합니다.
2. **IoC** 관련 목록 표시 그룹에서 옵저버블 탭을 선택합니다.
3. 옵저버블을 클릭합니다.
4. 옵저버블 양식에서 옵저버블 공유 관련 링크를 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵저버블 공유 대화 상자가 나타납니다.



5. 이 위협 공유 기록의 이름을 입력합니다.
6. 선택한 옵저버블에 대한 설명을입력합니다.
7. 옵저버블을 공유할 서클을 선택합니다.
8. 제출을 클릭합니다.
   옵저버블은 지정된 신뢰할 수 있는 서클과 공유됩니다.
9. 위협 공유 탭을 클릭하여 위협 공유 기록을 볼 수 있습니다.
10. 공유된 옵저버블에 사이팅이 포함된 경우 사이팅도 공유되며 사이팅 탭을 클릭하여 볼 수 있습니다.

사이팅 검색 상세 정보 보기

모든 사이팅 검색의 집계 상세 정보를 검토합니다.

시작하기 전에
필요한 역할: sn_si.analyst

이 태스크 정보
.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 보안 인시던트로 이동합니다.
2. 사이팅 검색 목록을 보려면 **IoC** 관련 목록 표시 그룹에서 사이팅 검색 상세 정보 탭을 선택합니다.

> 주:
> 이 데이터는 와 공유할 Trusted Security Circle수 있습니다.

사이팅 검색 정보

상세 정보	설명
옵저버블	쿼리로 검색된 모든 옵저버블 목록입니다.
옵저버블 유형	
내부 사이팅	모든 검색에 대한 내부 사이팅 수입니다.
외부 사이팅	모든 검색에 대한 외부 사이팅 수입니다. (위협 공유에서 수신)
사이팅 검색	사이팅 검색 식별자입니다.
업데이트됨	마지막으로 수정한 날짜 및 시간입니다.

사이팅 검색 데이터 보기

모든 사이팅 검색의 집계 데이터를 검토합니다.

시작하기 전에
필요한 역할: sn_si.analyst

프로시저

1. 보안 인시던트로 이동합니다.
2. 사이팅 검색 목록을 보려면 모든 관련 목록 표시 관련 목록 그룹에서 사이팅 검색 데이터 탭을 선택합니다.

> 주:
> 이 데이터는 와 공유할 Trusted Security Circle수 있습니다.

사이팅 검색 데이터

결과	설명
종료 날짜 범위	목격을 찾는 것을 멈출 시간입니다.
외부 관찰	집계된 외부 사이팅 수입니다. (위협 공유에서 수신)
내부 Sightings	내부 사이팅의 집계 수입니다.
로컬 여부	사이팅이 현재 또는 공유 환경에서 왔는지 여부를 나타냅니다.
옵저버블	쿼리로 검색된 모든 옵저버블 목록입니다.
관찰 카운트	검색된 사이팅 수입니다.
사이팅 검색	사이팅 검색 식별자입니다.
사이팅 검색 상세 정보	사이팅 검색의 집계 상세 정보입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

결과	설명
사이팅 검색 링크	사이팅 검색 포털을 가리키는 링크입니다. 검색 쿼리는 사이팅 검색 링크를 클릭하면 자동으로 적용됩니다.
사이팅 검색 쿼리	인스턴스를 식별하는 쿼리입니다. 172.10.0.171은 대체 가능하며 선택한 옵저버블에서 대체됩니다. (검색 172.10.0.171 | 머리 10) 주: 일 선택은 저장된 검색에 적용되지 않습니다.

보안 운영 통합 - 위협 조회 기능

위협 조회 기능은 위협 인텔리전스 조회를 수행하여 하나 이상의 옵저버블이 알려진 보안 위협과 연결되어 있는지 여부를 확인합니다.

위협 조회 역량에는 워크플로우인 보안 운영 통합 - 위협 조회 플로우. 역량 워크플로우가 실행되면 활성화된 구현을 위한 추가 워크플로우가 실행됩니다. 선택한 옵저버블에 대한 조회를 수행하는 데 사용할 구현을 지정하거나 모든 구현을 사용하여 조회를 수행할 수 있습니다.

주:
사용 가능한 구현이 없으면 역량 작업이 제품 메뉴에 표시되지 않습니다.

보안 운영 통합 - 위협 조회 플로우

보안 운영 통합 - 위협 조회 역량 플로우는 사용 가능한 위협 조회 구현에 액세스하고 각 구현과 연관된 구현 플로우를 실행하여 선택한 옵저버블의 위협 조회를 수행합니다.

시작하기 전에
필요한 역할: sn_ti.write

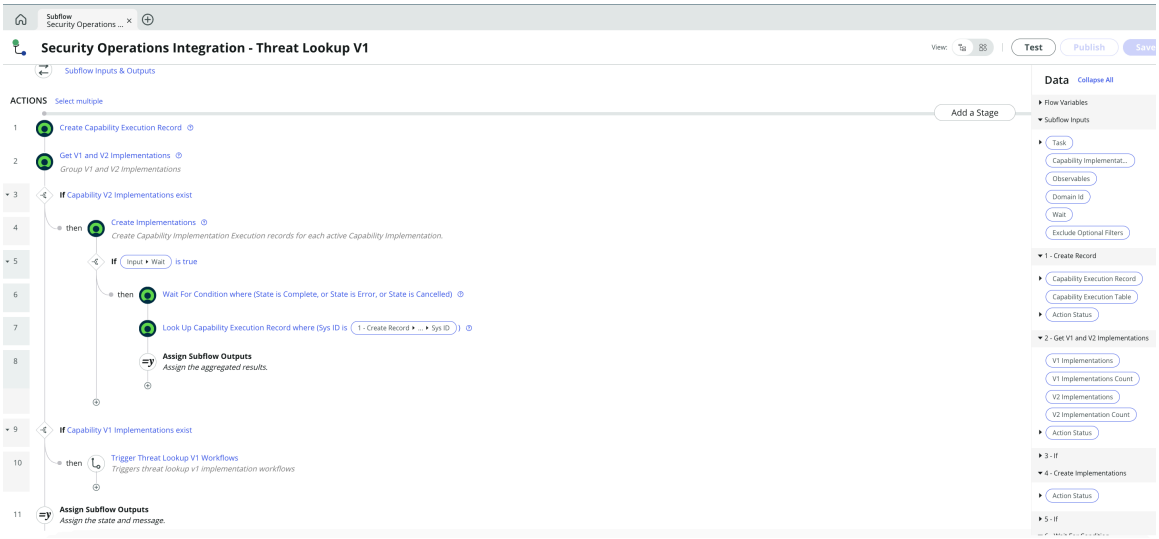
이 태스크 정보
이 플로우는 다음과 같은 방법으로 트리거될 수 있습니다.

- 옵저버블 목록에서 하나 이상의 옵저버블을 선택하고 선택한 행 선택 목록에 대한 작업에서위협 조회 실행을 선택합니다.
- 옵저버블 기록을 열고 위협 조회 실행 관련 링크를 클릭하면 됩니다.
- 보안 인시던트의 옵저버블 관련 목록에서

그런 다음 각 방법을 사용하면 선택한 옵저버블을 스캔하는 데 사용할 조회 구현을 지정할 수 있습니다. 조회를 수행하기 위해 연결된 구현 플로우가 실행됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

위협 조회



이 플로우와 관련된 작업은 여기에 설명되어 있습니다. 다른 작업에 대한 자세한 내용은 다음 문서를 참조하십시오 일반 Security Operations 통합 플로우 및 오케스트레이션 활동.

플로우 프로세스 작업에는 다음이 포함됩니다.

- 지원되는 보안 역량 가져오기 작업
- 역량 실행 추적 - 구현 작업 없음

플로우 실행 순서 변경

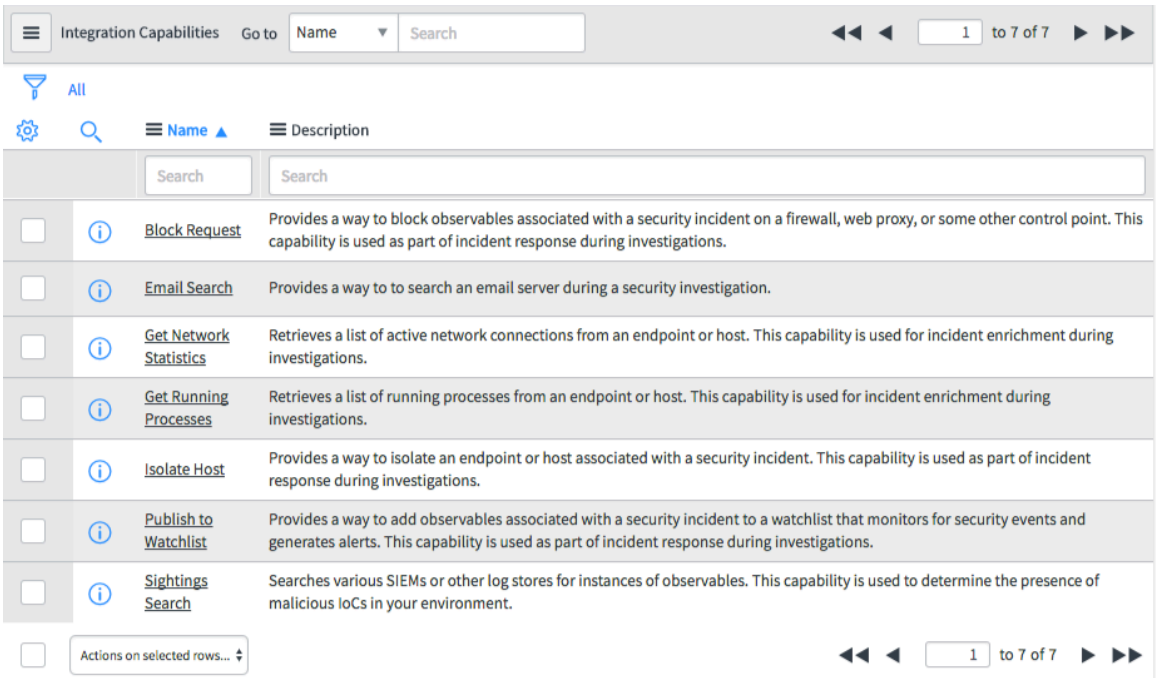
통합 기능 구현은 실행할 플로우를 지정합니다. 기본 시스템에서 플로우는 구현에 지정된 순서대로 실행됩니다. 필요에 따라 순서를 변경할 수 있습니다.

시작하기 전에
필요한 역할: sn_sec_cmn.write

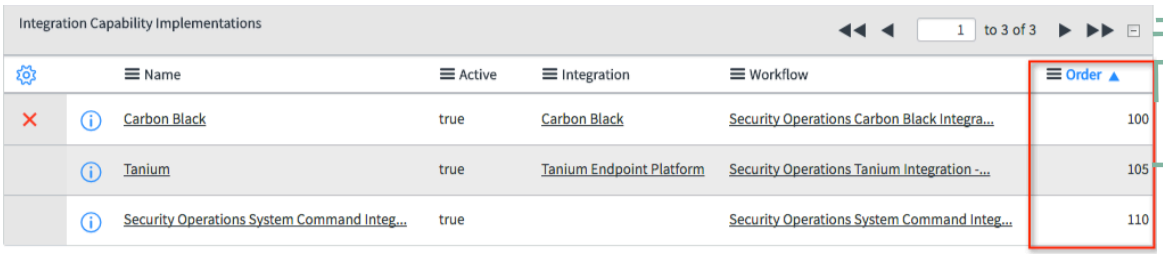
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

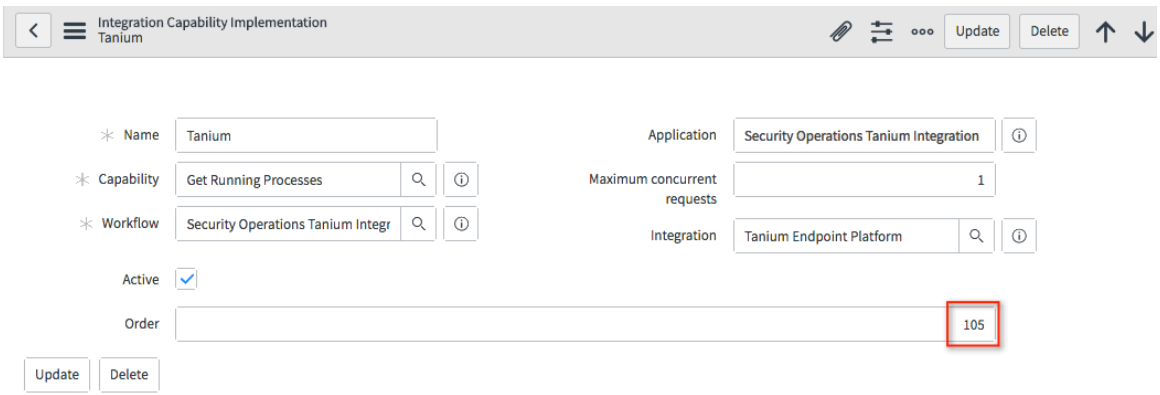
1. 다음으로 이동 모두 〉 보안 운영 〉 통합 〉 통합 기능.



2. 실행 순서를 변경할 통합 기능을 선택합니다.



3. 수정할 구현을 선택합니다.



4. 순서를 더 높거나 낮은 숫자로 변경합니다.
숫자가 작을수록 실행 우선순위가 높습니다.

5. 제출을 클릭합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

일반 **Security Operations** 통합 플로우 및 오케스트레이션 활동

외부 공급업체 통합과 연결된 많은 플로우에는 동일한 활동이 포함됩니다. 처리를 시작하고 완료하기 위한 활동을 예로 들 수 있습니다.

실행 추적 - 플로우 작업 시작

실행 추적 - 시작 플로우 작업은 옵저버블에서 작동하는 통합 플로우에 대한 보안 운영 감사 프로세스를 시작합니다.

실행 추적 - 플로우 시작 작업을 모든 플로우와 함께 사용하여 감사에서 플로우의 진행 상황을 기록할 수 있습니다.

결과

이 플로우 작업의 가능한 결과는 다음과 같습니다.

결과

결과	설명
성공	감사 레코드가 생성됩니다.

입력 변수

입력 변수는 플로우 작업의 초기 동작을 결정합니다.

변수	설명
capabilityId	실행 중인 통합 역량의 시스템 식별자입니다.
isImpl	통합 역량 플로우 또는 통합 역량 구현 플로우에 대해 감사가 수행되는지 여부를 지정하는 플래그입니다. 가능한 값: • false - 사이팅 검색과 같은 추상적인 통합 역량 플로우에 대한 감사를 나타냅니다. (기본값입니다.) • true - 통합 역량 구현 플로우에 대한 감사를 나타냅니다. 예를 들어 Splunk 또는 Elasticsearch입니다.
taskId	플로우와 관련된 모든 작업의 시스템 식별자입니다.
옵저버블 목록	원하는 작업을 수행하기 위한 하나 이상의 옵저버블 SysID입니다. 플로우 입력으로 사용됩니다.
flowContextId	연결된 플로우 컨텍스트 기록의 시스템 식별자입니다. 시스템에서 제공합니다.
플로우 이름	플로우의 이름입니다. 시스템에서 제공합니다.
parentCapabilityExcutionId	구현 플로우를 시작한 감사 기록의 시스템 식별자입니다. Splunk, Elasticsearch 및 VirusTotal과 같은 통합 기능 구현 플로우에만 필요합니다.

출력 변수

출력 변수에는 후속 작업에서 사용할 수 있는 데이터가 포함됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

출력 변수

변수	설명
capabilityExecutionId	감사 기록의 시스템 식별자입니다.

- 지원되는 보안 역량 가져오기 작업
- 역량 실행 추적 - 구현 작업 없음

역량 실행 추적 - 플로우 작업 완료

역량 실행 추적 - 완료 플로우 작업은 플로우가 완료되면 감사 기록을 업데이트합니다.

역량 실행 추적 - 전체 플로우 작업은 플로우의 완료를 기록하기 위해 모든 플로우와 함께 사용할 수 있습니다.

주:
병렬 시작 관리자 코어 플로우 작업의 반환 값 배열에는 모든 통합 플로우 실행의 결과 배열이 포함되어 있으며 실행 추적을 성공적으로 완료하라는 메시지를 표시합니다.

결과

이 플로우 작업의 가능한 결과는 다음과 같습니다.

결과

결과	설명
성공	감사 기록 상태가 완료로 업데이트됩니다.

입력 변수

입력 변수는 플로우 작업의 초기 동작을 결정합니다.

변수	설명
capabilityExecutionId	감사 기록의 시스템 식별자입니다. 이 필드는 감사 시작 활동의 출력입니다.
플로우 이름	플로우의 이름입니다. 시스템에서 제공합니다.
메시지	완료 메시지.

출력 변수

출력 변수가 없습니다.

역량 실행 추적 - 실패 플로우 작업

역량 실행 추적 - 실패 플로우 작업은 감사 기록에 실패를 기록합니다.

역량 실행 추적 - 실패 플로우 작업은 실패 조건을 기록하기 위한 모든 플로우와 함께 사용할 수 있습니다.

결과

이 플로우 작업의 가능한 결과는 다음과 같습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

결과

결과	설명
성공	감사 기록 상태가 오류로 설정되고 오류가 기록되었음을 나타내는 메시지가 표시됩니다.

입력 변수

입력 변수는 플로우 작업의 초기 동작을 결정합니다.

변수	설명
capabilityExecutionId	감사 기록의 시스템 식별자입니다. 감사 시작 활동의 출력입니다.
errorMessage	오류의 이유를 나타내는 메시지입니다.
플로우 이름	플로우의 이름입니다. 시스템에서 제공합니다.

출력 변수

출력 변수가 없습니다.

역량 - CI 활동 결정

역량 - CI 결정 워크플로우 활동은 워크플로우에 포함할 구성 항목(CI)을 결정합니다.

기능 - CI 결정 활동은 워크플로우에 포함할 CI를 결정하기 위해 모든 워크플로우와 함께 사용할 수 있습니다.

결과

이 활동의 가능한 결과는 다음과 같습니다.

결과

결과	설명
성공	구성 항목을 찾았습니다.
실패	CI를 찾을 수 없습니다. 자세한 오류 정보는 활동 출력 오류에서 확인할 수 있습니다.

입력 변수

입력 변수는 활동의 초기 동작을 결정합니다.

변수	설명
task_sys_id	작업 식별자(보안 인시던트를 CI에 매핑)입니다.
cis_affected	구성 항목입니다.

출력 변수

출력 변수에는 후속 활동에 사용할 수 있는 데이터가 포함됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

출력 변수

변수	설명
cis_affected	필터링된 CI
task_sys_id	작업 식별자(보안 인시던트를 CI에 매핑)입니다.

보강 데이터 기록 플로우 작업 생성

보강 데이터 기록 생성 플로우 작업은 플로우에서 사용할 보강 기록을 생성하거나 업데이트합니다.

보강 데이터 기록 생성 플로우 작업은 플로우의 보강 기록을 업데이트하기 위해 모든 플로우와 함께 사용할 수 있습니다.

결과

이 플로우 작업의 가능한 결과는 다음과 같습니다.

결과

결과	설명
성공	보강 기록이 업데이트되었습니다.
실패	보강 기록이 업데이트되지 않았습니다. 더 많은 오류 정보는 플로우 작업 출력 오류에서 확인할 수 있습니다.

입력 변수

입력 변수는 플로우 작업의 초기 동작을 결정합니다.

변수	설명
task_id	작업 식별자입니다.
컨텐츠	원시 콘텐츠(실행 중인 프로세스 데이터)입니다.
enrichment_mapping_id	보강 매핑 식별자입니다.
ci_id	구성 항목 식별자입니다.
reference_value	하지 않는.

출력 변수

출력 변수에는 후속 활동에 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
결과	enrichmentUtils 스크립트를 사용하여 작성된 GlideRecord입니다.

구성 항목 **FQDN** 가져오기 플로우 작업

는 보안 공통 오케스트레이션 〉 구성 항목 **FQDN** 가져오기 플로우 작업은 구성 항목의 FQDN(정규화된 도메인 이름)을 조회합니다. 이 플로우 작업을 통해 조사 및 정정 프로세스를 가속화할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

구성 항목 FQDN 가져오기 플로우 작업은 구성 항목의 FQDN(정규화된 도메인 이름)을 검색하기 위해 모든 플로우와 함께 사용할 수 있습니다.

입력 변수

입력 변수는 플로우 작업의 초기 동작을 결정합니다.

입력 변수

변수	설명
cmdb_ci.id [문자열]	구성 항목 기록의 시스템 식별자(sys_id)입니다.

출력 변수

출력 변수에는 후속 작업에서 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
fqdn [문자열]	구성 항목의 전체 주소 도메인 이름(FQDN)입니다.

추가 참고 사항

구성 항목의 fqdn 필드를 채워야 합니다.

옵저버블 활동 결정

옵저버블 결정 워크플로우 활동은 워크플로우에 포함할 옵저버블을 결정합니다

옵저버블 결정 활동은 워크플로우에 포함할 옵저버블을 결정하기 위해 모든 워크플로우와 함께 사용할 수 있습니다.

결과

이 활동의 가능한 결과는 다음과 같습니다.

결과

결과	설명
성공	옵저버블 찾음
실패	옵저버블을 찾을 수 없습니다. 자세한 오류 정보는 활동 출력 오류에서 확인할 수 있습니다.

입력 변수

입력 변수는 활동의 초기 동작을 결정합니다.

변수	설명
task_sys_id	작업 식별자(보안 인시던트를 옵저버블에 매핑)입니다.
옵저버블	IP 주소, 해시, URL, 도메인 이름

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

출력 변수

출력 변수에는 후속 활동에 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
옵저버블	필터링된 옵저버블

지원되는 보안 역량 가져오기 작업

지원되는 역량 가져오기 플로우 작업은 활성 상태이며 요청된 역량을 지원하는 통합의 이름과 수를 검색합니다.

지원되는 역량 가져오기 작업을 모든 플로우와 함께 사용하여 지원되는 역량을 결정할 수 있습니다.

결과

이 동작의 가능한 결과는 다음과 같습니다.

결과

결과	설명
성공	발견된 역량을 지원하는 통합입니다.
실패	역량을 지원하는 활성 통합을 찾는 동안 오류가 발생했습니다. 자세한 오류 정보는 작업 출력 오류에서 확인할 수 있습니다.

입력 변수

입력 변수는 작업의 초기 동작을 결정합니다.

변수	설명
capabilityName	역량의 이름입니다.
taskId	플로우와 관련된 모든 작업의 시스템 식별자입니다.
domainId	플로우와 연결된 모든 도메인의 시스템 식별자입니다.

출력 변수

출력 변수에는 후속 작업에서 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
지원 기능	역량을 지원하는 통합 목록입니다.
역량 카운트	역량을 지원하는 통합 수입니다.

역량 실행 추적 - 구현 작업 없음

통합 기능 구현을 찾을 수 없는 경우 기능 실행 추적 - 구현 없음 플로우 작업은 오류 기록을 생성합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

구성된 기능 구현을 사용할 수 없는 경우 오류 조건을 처리하기 위해 추상 통합 기능 플로우와 함께 기능 실행 추적 - 구현 없음 작업을 사용할 수 있습니다.

결과

이 동작의 가능한 결과는 다음과 같습니다.

결과

결과	설명
성공	실행 추적 기록 상태가 오류로 설정되고 오류가 기록되었음을 나타내는 메시지가 표시됩니다.

입력 변수

입력 변수는 작업의 초기 동작을 결정합니다.

변수	설명
capabilityExecutionId	감사 기록의 시스템 식별자입니다. 실행 추적을 시작하는 데 사용되는 작업의 출력입니다.
플로우 이름	플로우의 이름입니다. 시스템에서 제공합니다.

출력 변수

출력 변수가 없습니다.

준수 검색 작업 작성

준수 검색 만들기 작업은 정의된 검색 쿼리를 사용하여 지정된 Exchange 서버에서 이메일에 대한 준수 검색을 만들고 만들어진 준수 검색의 이름을 반환합니다.

입력 변수

입력 변수는 작업의 초기 동작을 결정합니다.

변수	설명
search_query	모든 사서함의 Exchange 서버에서 이메일을 찾는 데 사용되는 필수 검색 쿼리입니다.
교환 위치	정의된 위치에서 검색하는 데 사용되는 필수 위치 필드입니다. 값은 다음과 같습니다. • 모두 • 특정 사서함의 이름
targetId	Exchange 서버가 있는 필수 대상 호스트 식별자 필드입니다.

출력 변수

출력 변수에는 후속 작업에서 사용할 수 있는 데이터가 포함됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

출력 변수

변수	설명
response	생성된 준수 검색의 이름입니다.

종료 조건

이 작업에 대한 가능한 종료 조건은 다음과 같습니다.

종료 조건

변수	설명
검색 작성 실패	Exchange 서버의 예외로 인해 검색 생성에 실패한 경우.
검색이 성공적으로 생성됨	검색 생성에 성공한 경우입니다.
구문 분석 오류로 인해 검색을 작성하지 못했습니다.	구문 분석 문제로 인해 검색 생성에 실패한 경우.
오류	플로우 작업에서 예외가 발생한 경우.

CI 활동에서 IP 가져오기

이 워크플로우 활동은 CI(구성 항목)와 연결된 IPV4 주소를 결정합니다.

CI에서 **IP** 가져오기 활동은 CI의 IPv4 주소를 검색하는 모든 워크플로우와 함께 사용할 수 있습니다.

입력 변수

입력 변수는 활동의 초기 동작을 결정합니다.

입력 변수

변수	설명
ci_sys_id [string]	구성 항목 시스템 식별자

출력 변수

출력 변수에는 후속 활동에 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
ip_addr [string]	IPv4 주소입니다. IP 주소를 확인할 수 없는 경우 이 값은 비어 있습니다.

종료 조건

이 활동의 가능한 결과는 다음과 같습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

조건

조건	설명
성공	IPv4 주소가 반환되었습니다.
실패	IPv4 주소를 확인할 수 없습니다.

netstat 플로우 작업을 통해 네트워크 통계 가져오기

보안 일반 오케스트레이션 - netstat를 통해 네트워크 통계 가져오기 플로우 작업은 Windows 기반 시스템에서 영향을 받는 자원에 대한 네트워크 통계를 검색합니다. 이 플로우 작업을 통해 조사 및 정정 프로세스를 가속화할 수 있습니다.

netstat 흐름을 통해 네트워크 통계 가져오기 작업은 Windows 기반 시스템에서 네트워크 통계를 검색하기 위해 모든 흐름과 함께 사용할 수 있습니다. 머신은 **-a** 및 **-o** 매개변수를 포함하여 **netstat** 명령으로 쿼리됩니다. 출력 데이터를 향상시키기 위해 **get-process** 명령도 호출됩니다.

결과

이 플로우 작업의 가능한 결과는 다음과 같습니다.

결과

결과	설명
성공	네트워크 통계는 JSON 형식으로 검색되었습니다.
실패	네트워크 통계를 검색하는 동안 오류가 발생했습니다. 더 많은 오류 정보는 플로우 작업 출력 오류에서 확인할 수 있습니다.

입력 변수

변수	설명
대상 〔string〕	대상 시스템의 FQDN(정규화된 도메인 이름) 또는 IP 주소입니다.

출력 변수

출력 변수에는 후속 활동에 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
응답 〔string〕	대상 머신에서 현재 실행 중인 프로세스를 나타내는 JSON 문자열입니다. JSON 데이터에는 다음이 포함됩니다. pid 프로세스 식별자 로컬 _port 네트워크 트랜잭션을 위한 로컬 포트 상태 TCP 연결의 상태입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

출력 변수

변수	설명
	주: UDP 연결의 경우 이 필드는 null입니다. local_address 로컬 FQDN(정규화된 도메인 이름) 또는 IP 주소 remote_address 원격 FQDN(정규화된 도메인 이름) 또는 IP 주소 프로토콜 TCP 또는 UDP remote_port 네트워크 트랜잭션의 원격 포트 path 프로세스 실행 파일의 파일 경로 해시 실행 가능한 프로세스의 해시 값입니다. 해시는 PowerShell V4 이상의 SHA-256에 있습니다. 그렇지 않으면 해시는 MD5에 있습니다.

제한

MID Server에서 PowerShell을 지원해야 합니다.

SHA-256 해시에는 PowerShell V4가 필요합니다.

WMI 활동을 통해 실행 중인 프로세스 가져오기

실행 중인 프로세스 가져오기 워크플로우 활동은 Windows 기반 시스템에서 구성 항목의 실행 중인 프로세스를 검색합니다. 이 활동은 조사 및 정정 프로세스를 가속화할 수 있습니다.

WMI를 통해 실행 중인 프로세스 가져오기 작업은 Windows 기반 시스템에서 실행 중인 프로세스를 검색하기 위해 모든 워크플로와 함께 사용할 수 있습니다.

입력 변수

입력 변수는 활동의 초기 동작을 결정합니다.

입력 변수

변수	설명
대상 〔string〕	대상 시스템의 FQDN(정규화된 도메인 이름) 또는 IP 주소입니다.

출력 변수

출력 변수에는 후속 활동에 사용할 수 있는 데이터가 포함됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

출력 변수

변수	설명
응답 (string)	대상 시스템에서 현재 실행 중인 프로세스를 나타내는 JSON 문자열입니다. JSON 데이터에는 다음이 포함됩니다. pid 프로세스 식별자 이름 프로세스의 이름 또한 사용 가능한 경우 다음을 수행합니다. 소유자 프로세스 소유자의 이름 owner_sid 프로세스 소유자의 시스템 식별자 owner_domain 프로세스 소유자의 도메인 path 프로세스 실행 파일의 파일 경로 해시 실행 가능한 프로세스의 해시 값입니다. 해시는 PowerShell V4 이상의 SHA-256에 있습니다. 그렇지 않으면 해시는 MD5에 있습니다.

제한

MID Server에서 **PowerShell**을 지원해야 합니다.

SHA-256 해시에는 PowerShell V4가 필요합니다.

준수 검색 상태 확인 작업

준수 검색 상태 확인 작업은 Exchange 서버에서 생성된 준수 검색의 상태를 확인하고 상태가 완료됨이면 준수 검색에 대해 검색된 이메일 검색에 대한 정보를 반환합니다.

입력 변수

입력 변수는 작업의 초기 동작을 결정합니다.

변수	설명
targetId	Exchange 서버가 있는 필수 대상 호스트 식별자 필드입니다.
searchName	Exchange 서버에서 작성된 준수 검색의 필수 이름입니다.

출력 변수

출력 변수에는 후속 작업에서 사용할 수 있는 데이터가 포함됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

출력 변수

변수	설명
response	준수 검색의 상태와 준수 검색을 위해 Exchange 서버에서 찾은 이메일 수를 포함합니다.

종료 조건

이 작업에 대한 가능한 종료 조건은 다음과 같습니다.

종료 조건

변수	설명
검색 진행 중	준수 검색의 상태가 진행 중인 경우입니다.
검색 완료 - 위협 이메일을 찾을 수 없음	준수 검색 상태가 완료되고 준수 검색의 일부로 이메일을 찾을 수 없는 경우.
검색 완료 - 위협 이메일 찾음	준수 검색의 상태가 완료되고 준수 검색의 일부로 이메일이 발견되는 경우
상태 확인 중 오류 발생	Exchange 서버의 예외로 인해 상태 확인에 실패한 경우.
오류	플로우 작업에서 예외가 발생한 경우.

작업 작업 메모 활동 업데이트

보안 공통 오케스트레이션 - 작업 작업 메모 업데이트 워크플로우 활동은 작업 기록의 활동 섹션(작업 메모)을 업데이트합니다. 이는 정보를 로깅하는 데 유용합니다.

작업 작업 메모 업데이트 활동은 모든 워크플로우와 함께 사용하여 작업 기록의 작업 메모를 업데이트할 수 있습니다.

입력 변수

입력 변수는 활동의 초기 동작을 결정합니다.

입력 변수

변수	설명
task_id [string]	작업 기록의 시스템 식별자(sys_id)입니다.
콘텐츠 [string]	작업의 작업 메모에 기록된 데이터입니다.

출력 변수

출력 변수에는 후속 활동에 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
결과 [string]	업데이트가 성공적으로 완료되었는지 여부를 나타냅니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 인시던트 활동에 조회 정보 롤업

보안 인시던트에 정보 롤업 활동은 위협 조회에서 정보를 수집하고 작업 메모에 원래 보안 인시던트의 ID뿐만 아니라 내용 요약을 출력하는 데 워크플로우와 함께 사용할 수 있습니다.

결과

이 활동의 가능한 결과는 다음과 같습니다.

결과

결과	설명
성공	보안 인시던트로 롤업된 조회 보고서 요약입니다.
실패	원래 작업 및 조회 요약 보고서가 비어 있습니다.

입력 변수

변수	설명
scanID〔문자열〕	조회 식별자입니다.

출력 변수

출력 변수에는 후속 활동에 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
sild〔문자열〕	보안 인시던트 식별자입니다.
응답〔string〕	IoC 값, 결과, 실패 이유, 조회 참조 등을 포함한 조회 결과 요약입니다.

조회 결과로 보안 인시던트 업데이트 워크플로우

조회 결과로 보안 인시던트 업데이트 워크플로우는 기존 보안 인시던트를 조회 결과로 업데이트합니다.

시작하기 전에
필요한 역할: sn_si.basic

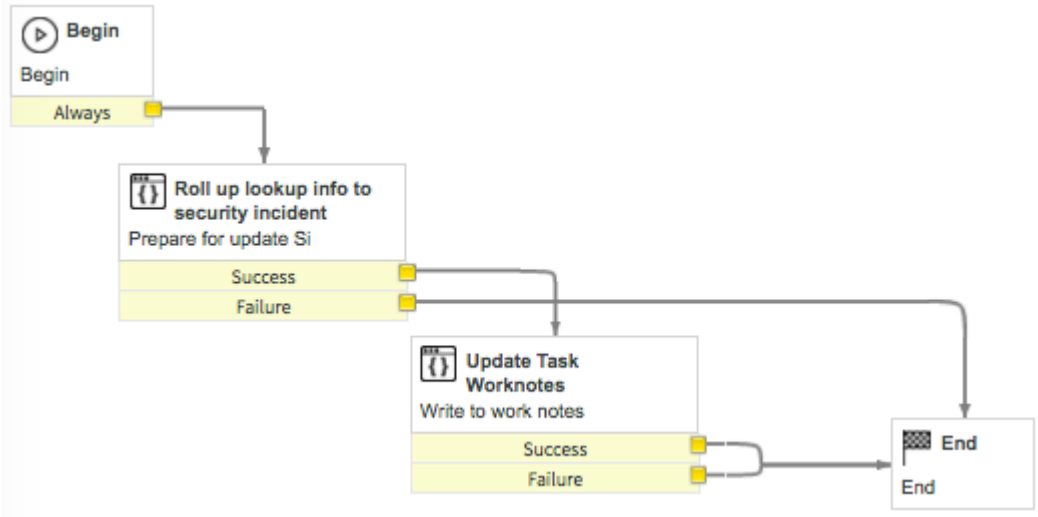
이 태스크 정보
이 워크플로우는 결과 필드가 실패로 변경되는 시기를 모니터링하는 조회 테이블의 비즈니스 규칙에 의해 트리거됩니다.

워크플로우 프로세스 활동에는 다음이 포함됩니다.

보안 인시던트 활동에 조회 정보 롤업

작업 작업 메모 활동 업데이트

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



허용 목록에 추가된 옵저버블 활동 필터링

필터링된 허용 목록에 추가된 옵저버블 워크플로우 활동은 옵저버블 목록에서 무시할 수 있는 옵저버블을 제거합니다. 이 활동은 조사 및 정정 프로세스를 가속화할 수 있습니다.

허용 목록에 추가된 옵저버블 필터 활동은 작업을 수행하기 전에 옵저버블을 필터링하는 워크플로우와 함께 사용할 수 있습니다.

결과

이 활동의 가능한 결과는 다음과 같습니다.

결과

결과	설명
성공	필터 목록이 작성되었습니다.
실패	옵저버블을 필터링하는 동안 오류가 발생했습니다. 자세한 오류 정보는 활동 출력 오류에서 확인할 수 있습니다.

입력 변수

입력 변수는 활동의 초기 동작을 결정합니다.

변수	설명
옵저버블	사용 가능한 옵저버블 목록입니다.

출력 변수

출력 변수에는 후속 활동에 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
filteredObservable	필터링된 옵저버블입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

첨부 파일 활동으로 기록할 컨텐츠 쓰기

이 활동은 입력에서 전달된 콘텐츠를 쓰고 지정된 기록에 지정된 첨부 파일을 만듭니다.

Write **content to record as attachment** 활동은 컨텐츠를 쓰고 기록에 첨부하는 워크플로우와 함께 사용할 수 있습니다.

입력 변수

입력 변수는 활동의 초기 동작을 결정합니다.

입력 변수

변수	설명
테이블 이름 [문자열]	기록의 테이블 이름입니다. 이 입력 필드는 필수입니다.
sysid [문자열]	작업 기록의 시스템 식별자(sys_id)입니다. 이 입력 필드는 필수입니다.
페이로드	첨부 파일로 작성할 일반 텍스트 컨텐츠입니다. 이 입력 필드는 필수입니다.
파일 이름	첨부 파일 이름입니다.

출력 변수

출력 변수에는 후속 활동에 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
결과 [string]	업데이트가 성공적으로 완료되었는지 여부를 나타냅니다.

CI 활동에서 IP 가져오기

CI에서 IP 가져오기 플로우 활동은 플로우에 사용할 CI(구성 항목)에서 IP 주소를 수집합니다.

CI에서 IP 가져오기 활동은 플로우에서 사용할 CI(구성 항목) IP 주소를 수집하기 위해 모든 플로우와 함께 사용할 수 있습니다.

결과

이 활동의 가능한 결과는 다음과 같습니다.

결과

결과	설명
성공	찾은 IP 주소.
실패	IP 주소를 찾을 수 없습니다. 자세한 오류 정보는 활동 출력 오류에서 확인할 수 있습니다.

입력 변수

입력 변수는 활동의 초기 동작을 결정합니다.

변수	설명
ci_sys_id	구성 항목 식별자입니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

출력 변수

출력 변수에는 후속 활동에 사용할 수 있는 데이터가 포함됩니다.

출력 변수

변수	설명
ip_addr	IP 주소입니다.

보안 운영 워크플로우 트리거

보안 운영 워크플로우 트리거는 테이블에 조건을 포함합니다. 조건이 충족되면 워크플로우 트리거 기록에 첨부된 모든 워크플로우가 실행됩니다.

워크플로우 트리거 생성 보안 운영

테이블에 대한 조건을 포함하는 워크플로우 트리거를 생성합니다.

시작하기 전에
보안 운영 에는 기본 시스템에 여러 워크플로우 트리거가 포함되어 있습니다.

활성 보안 인시던트의 구성 항목 변경 사항

구성 항목이 변경됨에 따라 통합을 사용하여 CI 관련 데이터를 보강합니다.

취약 그룹 다시 스캔

그룹을 종결/무시할 때 를 사용하여 취약성 스캔 워크플로우취약한 그룹을 재스캔합니다.

취약한 항목 다시 스캔

항목을 닫거나 무시할 때 를 사용하여 취약성 항목 검사 워크플로우 취약한 항목을 다시 스캔합니다.

필요한 역할:

- 읽으려면: sn_sec_cmn.read
- 생성 또는 업데이트: sn_sec_cmn.write
- 삭제 방법: sn_sec_cmn.admin

프로시저

1. 다음으로 이동 모두 〉 보안 운영 〉 유틸리티 〉 워크플로우 트리거.
2. 새로 만들기를 클릭합니다.
3. 양식의 필드에 적절히 입력합니다.

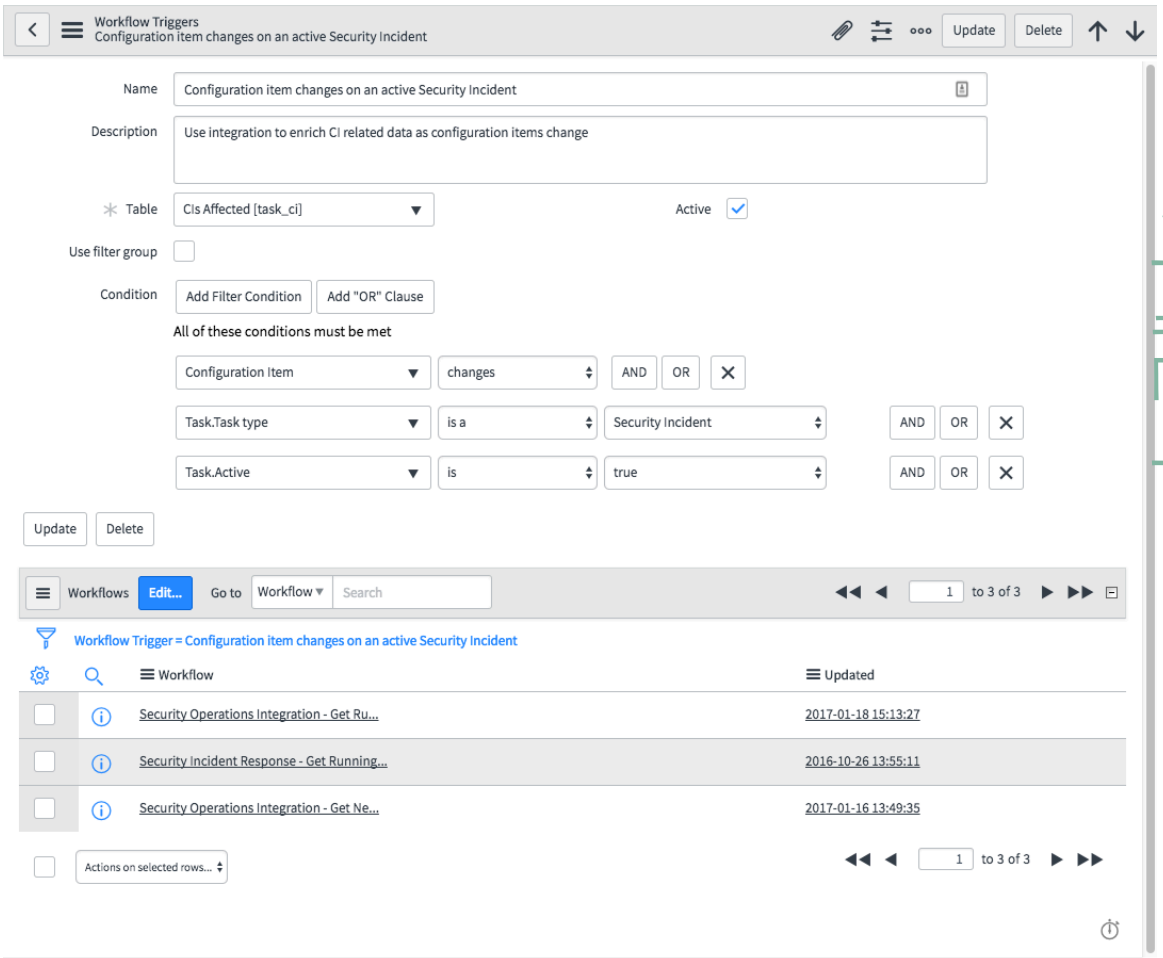
워크플로우 트리거

필드	설명
이름	워크플로우 트리거의 이름입니다.
설명	워크플로우 트리거에 대한 설명을 입력합니다.
테이블	워크플로우 트리거가 포함된 테이블입니다. 필터 그룹 사용 확인란을 선택하고 필터 그룹을 선택한 경우 이 필드는 기본적으로 선택한 필터 그룹과 연결된 테이블로 설정됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
조건	다음 사용 워크플로우 트리거의 기준을 정의하는 조건 작성기 입니다. 필터 그룹 사용 확인란을 선택하고 필터 그룹을 선택한 경우 조건 필드가 표시되지 않습니다.
활성	워크플로우 트리거를 활성화하려면 이 확인란을 선택합니다.
필터 그룹 이용	미리 정의된 필터 그룹을 사용하거나 워크플로우 트리거 기준을 정의하는 새 필터 그룹을 만들려면 이 확인란을 선택합니다.
필터 그룹	워크플로우 트리거를 정의하는 데 사용할 필터 그룹을 선택합니다. 이 필드는 필터 그룹 사용 확인란을 선택한 경우에만 나타납니다.

4. 입력을 완료했으면 양식 헤더를 마우스 오른쪽 버튼으로 클릭하고 저장을 선택합니다.



워크플로우 탭이 나타납니다. 여기에는 모든 필터 조건 또는 필터 그룹 조건이 충족될 때 실행되는 워크플로우가 포함되어 있습니다.

5. 워크플로우를 추가하려면 다음 단계를 수행합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 워크플로우 탭에서 편집을 클릭합니다.

b. 필요시 조건 작성기를 사용하여 선택하려는 워크플로우를 찾거나 슬러시버킷을 사용하여 워크플로우를 선택하고 워크플로우 목록으로 이동합니다.

c. 저장을 클릭합니다.
선택한 워크플로우가 추가됩니다.

6. 업데이트를 클릭합니다.

Security Operations 오케스트레이션

사용자는 의 보안 운영 오케스트레이션활동 팩과 워크플로우를 사용하여 Windows 또는 UNIX 기반 시스템 및 환경에서 데이터를 검색하고 상호작용할 수 있습니다.

보안 운영 오케스트레이션 수동 프로세스를 제거하고 상황별 정보를 확보하여 인시던트를 정정함으로써 시간을 절약합니다. 보안 운영 제품에는 각 플러그인에 포함되고 활성화되는 표준 활동 팩과 워크플로우가 있습니다.

표준 오퍼링 보안 운영 제품에서 사용할 수 없는 추가 오케스트레이션 활동을 생성하고 액세스하려면 전체 오케스트레이션 라이센스를 구매합니다.

- 보안 인시던트 응답 오케스트레이션 워크플로우:
  - 보안 인시던트 응답 - 네트워크 통계 플로우 가져오기
  - 보안 운영 시스템 명령 통합 - 실행 중인 프로세스 가져오기 플로우
  - IoC 변경에 대한 조회 요청 생성 워크플로우
  - Security Operations Integration - 이메일 검색 및 삭제 플로우
- 위협 인텔리전스 오케스트레이션 워크플로우:
  - 위협 인텔리전스 - IoC 조회 워크플로우 실행
  - 조회 결과로 보안 인시던트 업데이트 워크플로우
- 취약성 대응 오케스트레이션 워크플로우:
  - 취약성 스캔 워크플로우
  - 취약성 항목 검사 워크플로우

〔store-future: BEGIN review〕

보안 운영 시나리오 및 예시

ServiceNow# 보안 운영 몇 가지 시나리오를 연구하면 제품을 쉽게 이해할 수 있습니다. 이러한 시나리오는 제품을 사용하는 동안 사용할 수 있는 기능을 나타냅니다. 이러한 제품의 힘과 유연성에 대해 교육하기 위한 것입니다.

〔End〕
〔store-future: BEGIN review〕

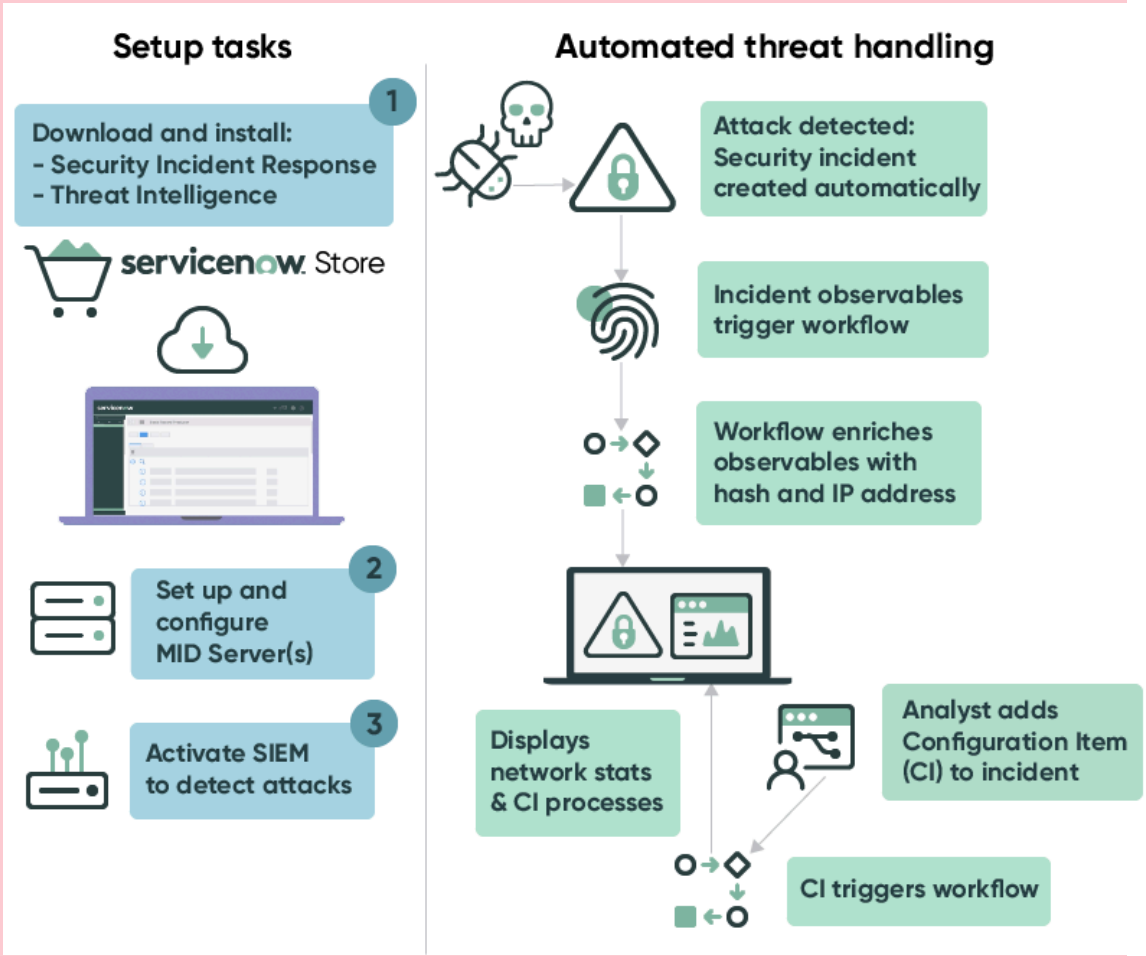
자동화를 사용하여 위협 분석 시간 단축

보안 인시던트 분류 및 분석은 위협 대응 프로세스 중에 가양성을 제거하고 보안 위협을 가장 잘 식별, 억제 및 제거할 수 있는 방법을 결정하는 데 필요한 단계입니다.

환자 분류에는 위협의 원인과 영향을 파악하는 수동 단계가 포함될 수 있습니다. 많은 단계를 자동화하여 위협을 분석하고 억제하는 데 필요한 시간과 노력을 크게 줄일 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

소프트웨어에서 ServiceNow# 보안 운영 자동화를 설정한 후 다양한 유형의 자동화를 수행할 수 있습니다. 예를 들어 옵저버블이 보안 인시던트에 추가될 때 옵저버블 데이터를 자동으로 보강할 수 있습니다. 또는 CMDB의 CI가 보안 인시던트에 추가될 때 실행 중인 프로세스를 보거나 네트워크 통계를 얻을 수 있습니다. 아래에 설명된 이러한 프로세스는 위협 분석 중에 귀중한 시간을 절약할 수 있습니다.



이 시나리오에서는 회사에서 위협 탐지에 사용하는 SIEM(보안 정보 및 이벤트 관리) 도구에 의해 악성 파일이 탐지되었습니다. 보안 운영 SIEM과의 통합을 통해 발생한 위협 유형에 따라 보안 인시던트가 자동으로 생성됩니다. 악성 파일에 옵저버블이 이미 포함되어 있거나 보안 분석가가 해당 사실 이후에 만료되지 않은 새 옵저버블을 추가한 경우 옵저버블 레코드를 보강하는 워크플로가 자동으로 트리거됩니다. 워크플로우로 인해 옵저버블이 검사되고 파일을 보낸 당사자의 해시 및 IP 주소가 보안 인시던트에 추가됩니다.

분류 과정에서 분석가는 회사의 CMDB에 포함된 CI(구성 항목)가 침입의 영향을 받았을 수 있음을 관찰할 수 있습니다. 따라서 분석가는 보안 인시던트에 CI를 추가합니다. 보안 인시던트가 저장되면 두 개의 다른 워크플로우가 실행되고 CI와 관련된 네트워크 통계 및 실행 중인 프로세스가 보안 인시던트에 즉시 추가됩니다.

〔End〕

자동화 준비 위협 인텔리전스

위협 응답 프로세스에서 자동화를 사용하려면 먼저 위협 인텔리전스 몇 가지 예비 설정 단계를 완료해야 합니다. 설정이 완료되면 사용자 지원이 거의 또는 전혀 없이 워크플로가 자동으로 실행됩니다.

시작하기 전에
필요한 역할: 관리자

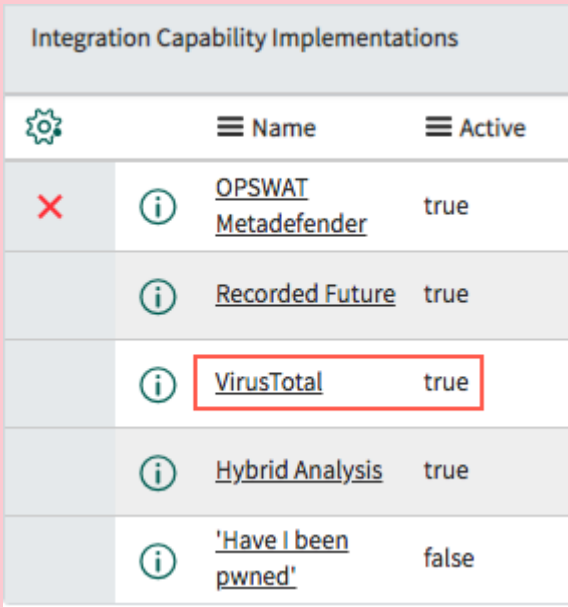
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다운로드 보안 인시던트 응답 및 위협 인텔리전스 애플리케이션의 ServiceNow Store.
2. 하나 이상의 MID Server를 설치하고 각 MID Server에 대한 서비스 자격 증명을 구성합니다.
3. MID Server가 실행 중이면 위협 조회 기능에 대해 사용 중인 통합 기능 구현(예: VirusTotal)이 활성 상태인지 확인합니다.
   위협 조회 기능은 하나 이상의 옵저버블이 알려진 보안 위협과 연결되어 있는지 여부를 확인하기 위해 조회를 수행합니다.

   a. 다음으로 이동 보안 운영 〉 통합 〉 통합 기능.

   b. 위협 조회를 클릭하고 통합 역량 구현 관련 목록을 찾아 아래로 스크롤합니다.



   c. 사용할 구현을 찾고 활성 열이 **true**로 표시되는지 확인합니다.

   d. 구현이 활성화되어 있지 않으면 구현 이름을 클릭하고 활성 확인란을 클릭하여 선택한 다음 업데이트를 클릭합니다.

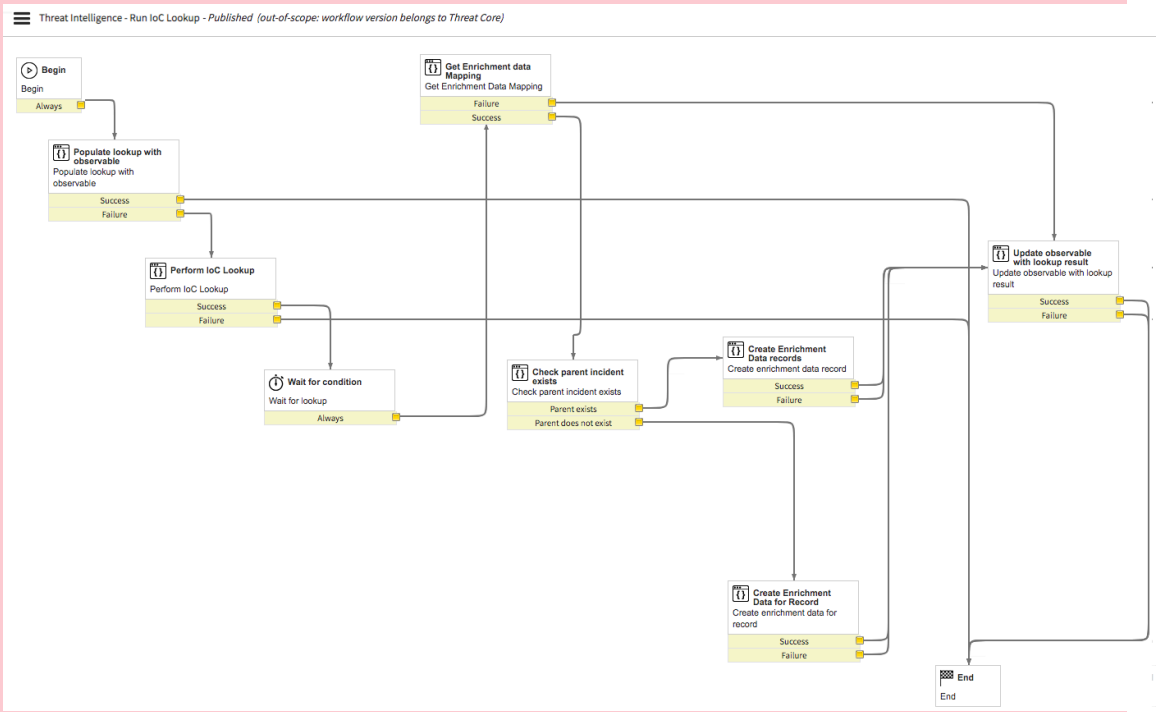
옵저버블 데이터 자동 보강

자동화를 준비하고 위협 인텔리전스 새 IoC(침해 표시기)를 보안 인시던트에 추가하면 위협 인텔리전스 - IoC 조회 실행 워크플로우가 자동으로 실행됩니다.

워크플로우 활동은 사용자 개입 없이 의심스러운 파일의 해시와 원래 IP 주소를 포함하여 IoC에서 정보를 추출합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵저버블 데이터 자동 보강



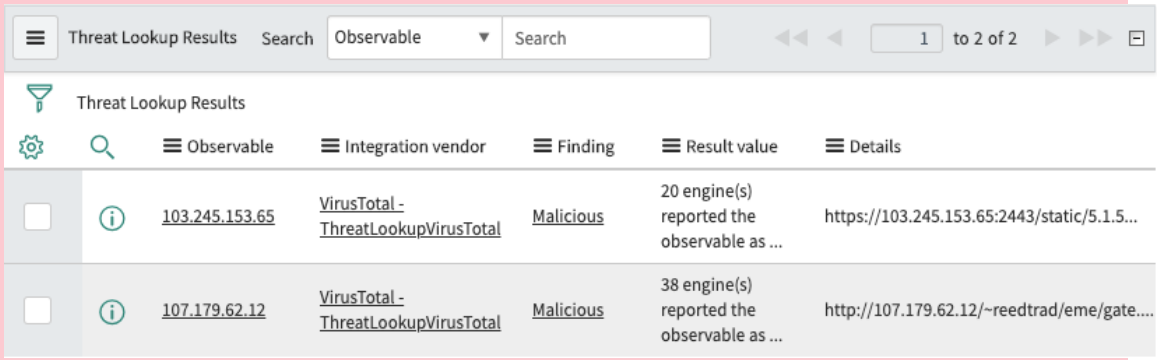
주:
보안 인시던트에 이미 연결된 하나 이상의 옵저버블을 선택하고 선택한 행에 대한 작업 선택 목록에서 위협 조회 실행을 선택하여 조회를 수동으로 실행할 수도 있습니다.

워크플로우는 다음과 같은 활동을 수행합니다.

1. 옵저버블로 조회 채우기 활동은 입력으로 활동에 제공된 조회의 값 및 유형과 일치하는 조회에 대한 기존 옵저버블을 찾으려고 시도합니다.
   a. 입력과 일치하는 옵저버블이 발견되면 **IoC** 조회 수행 활동으로 인해 기록의 ScanID에서 조회가 수행됩니다.
   b. 옵저버블이 발견되었지만 만료되지 않은 경우 조회가 수행되지 않고 보안 인시던트의 조회 결과가 옵저버블의 정보로 업데이트됩니다. 자세한 내용은 옵저버블 활동으로 조회 채우기 문서를 참조하십시오.
2. IoC 조회가 수행되면 다음 네 가지 활동이 먼저 보강 데이터 맵에서 정보를 검색합니다. 보강 데이터 매핑 은 XML, JSON 또는 속성 파일의 데이터를 ServiceNow 기록으로 변환합니다. 그런 다음 상위 보안 인시던트가 있는지 확인합니다. 그렇다면 옵저버블이 생성되고 보강됩니다. 그렇지 않은 경우 기존 옵저버블이 보강됩니다. 자세한 내용은 조회 결과 활동으로 옵저버블 업데이트 문서를 참조하십시오.
   - 보강 데이터 매핑 가져오기
   - 상위 인시던트 존재 확인
   - 보강 데이터 기록 작성
   - 기록에 대한 보강 데이터 작성
3. 데이터 보강이 완료되면 조회 결과로 옵저버블 업데이트 활동은 보안 인시던트에서 옵저버블을 업데이트하고 결과를 위협 조회 결과 관련 목록에 작성합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

위협 조회 결과



자동으로 네트워크 통계 및 실행 중인 프로세스 가져오기

CMDB에 있는 FQDM(정규화된 Windows 도메인 이름)을 가진 CI(구성 항목)를 보안 인시던트에 추가하면 추가 워크플로우가 실행되어 네트워크 통계 및 실행 중인 프로세스를 제공합니다.

시작하기 전에

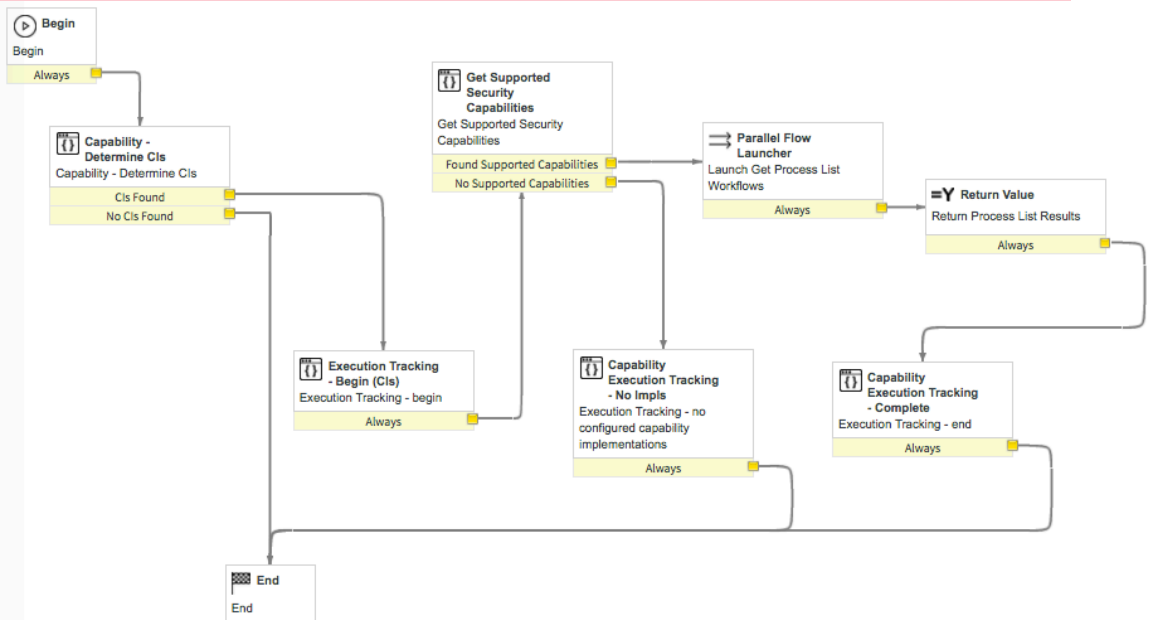
필요한 역할: 관리자

프로시저

1. Discovery 모듈을 사용하여 CMDB를 Windows 도메인 이름으로 채웁니다.

> **주:**
> ServiceNow 검색 모듈을 구독하지 않는 경우 CMDB를 수동으로 채우거나 타사 검색 유형 제품을 사용해야 합니다.

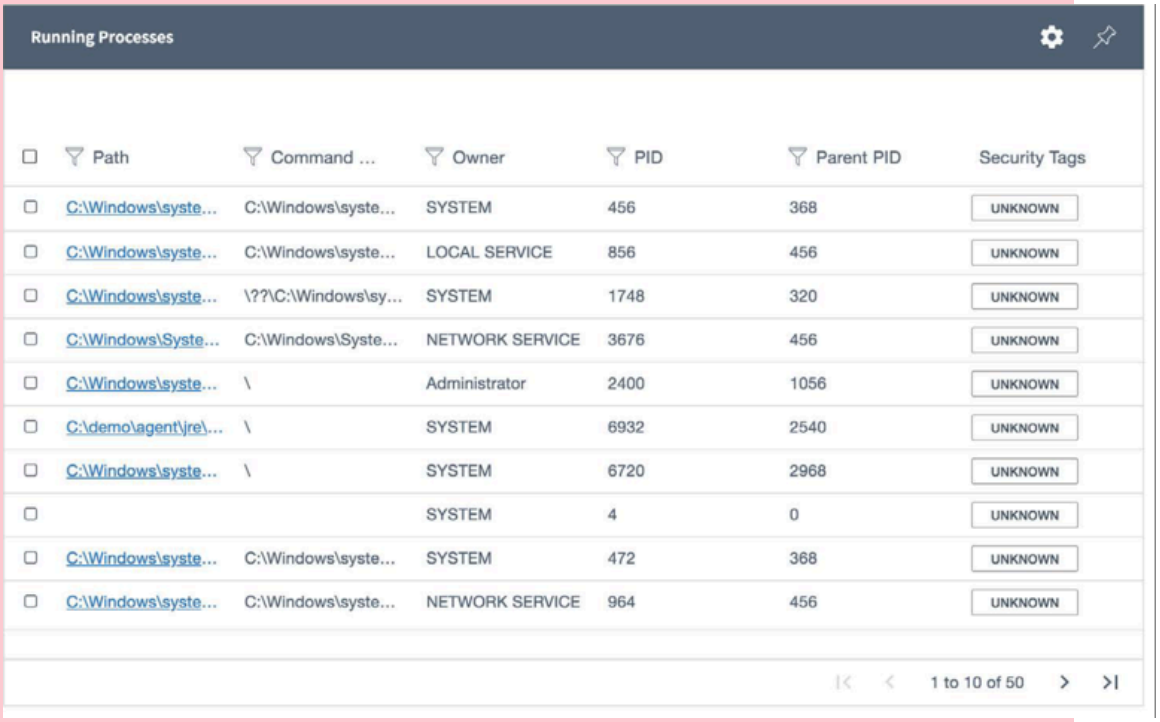
2. 보안 인시던트에 CI를 추가합니다.
   다음 두 워크플로우는 병렬로 실행됩니다.
   - 보안 운영 - 실행 중인 프로세스 가져오기 플로우: 이 워크플로우는 호스트에서 CI(구성 항목)의 실행 중인 프로세스 목록을 검색합니다. Carbon Black과 같은 통합을 수행하거나 Windows 기반 보안 인시던트에 이를 사용합니다.



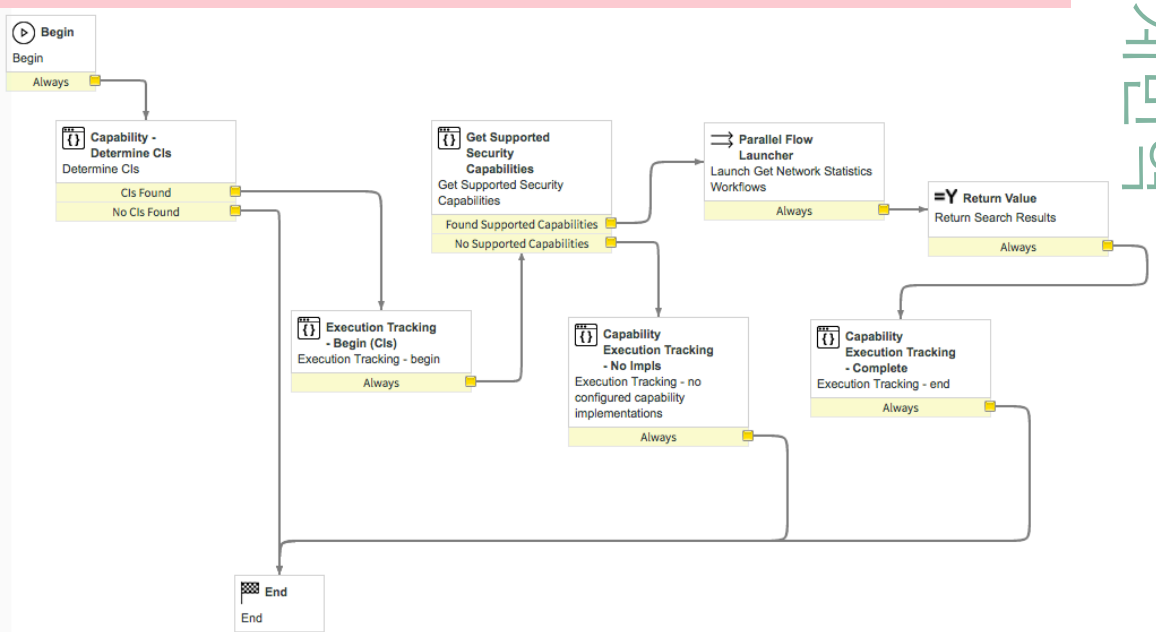
워크플로우가 완료되면 실행 중인 프로세스가 보안 인시던트의 실행 중인 프로세스 관련 목록에 표시됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

실행 중인 프로세스



- 보안 운영 통합 - 네트워크 통계 플로우 가져오기: 이 워크플로우는 호스트나 엔드포인트에서 활성 네트워크 연결 목록을 검색합니다. 시기



기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

워크플로우가 완료되면 네트워크 통계가 보안 인시던트의 네트워크 통계 관련 목록에 표시됩니다.

네트워크 통계

Workflow Activity History Search Started Search 1 to 8 of 8

Context = Security Operations Integration - Get Network Statistics

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

세간의 이목을 끄는 취약성 우선순위 지정

네트워크가 공격을 받으면 일반적으로 묻는 질문에는 "위험 노출을 어떻게 결정합니까?", 더 중요하게는 "어떤 시스템을 먼저 해결해야 하는지 어떻게 결정합니까?" 등이 있습니다.

2018년 초에 **Meltdown** 과 **Spectre**라는 두 가지 중요한 취약점이 공개되었습니다.

세간의 이목을 끄는 취약성 우선순위 지정

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

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

악성 프로그램은 Meltdown 및 Spectre를 악용하여 실행 중인 다른 프로그램의 메모리에 저장된 비밀에 액세스할 수 있습니다. 전 세계적으로 거의 30억 개의 시스템이 이 취약점의 영향을 받았을 가능성이 있으며, 하드웨어 및 소프트웨어 제공업체 모두 고객에게 패치를 제공하기 위해 분주히 움직였습니다.

에서 검사한 데이터를 사용하여 위협 순위 지정 취약성 대응

이 보안 운영 취약성 대응 애플리케이션을 사용하면 취약성 스캔을 수행하는 데 사용할 수 있는 다양한 방법을 사용할 수 있습니다. 보안 인시던트 응답 애플리케이션이 활성화된 경우 보안 인시던트 카탈로그, 보안 인시던트 기록 또는 보안 스캔 요청에서 스캔을 시작할 수도 있습니다.

사용하는 외부 공급업체 통합 에 따라 API를 사용하여 취약성 데이터를 스캔한 후 애플리케이션으로 취약성 대응 임포트합니다. 그런 다음 의 ServiceNow 구성 관리 데이터베이스(CMDB)자산과 일치합니다. 그 결과로 발생하는 취약한 항목에는 취약성의 심각도와 영향을 받는 자산의 중요도를 포함한 여러 요인에 따라 위험 점수 가 할당됩니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

위험 점수

All Open Incidents

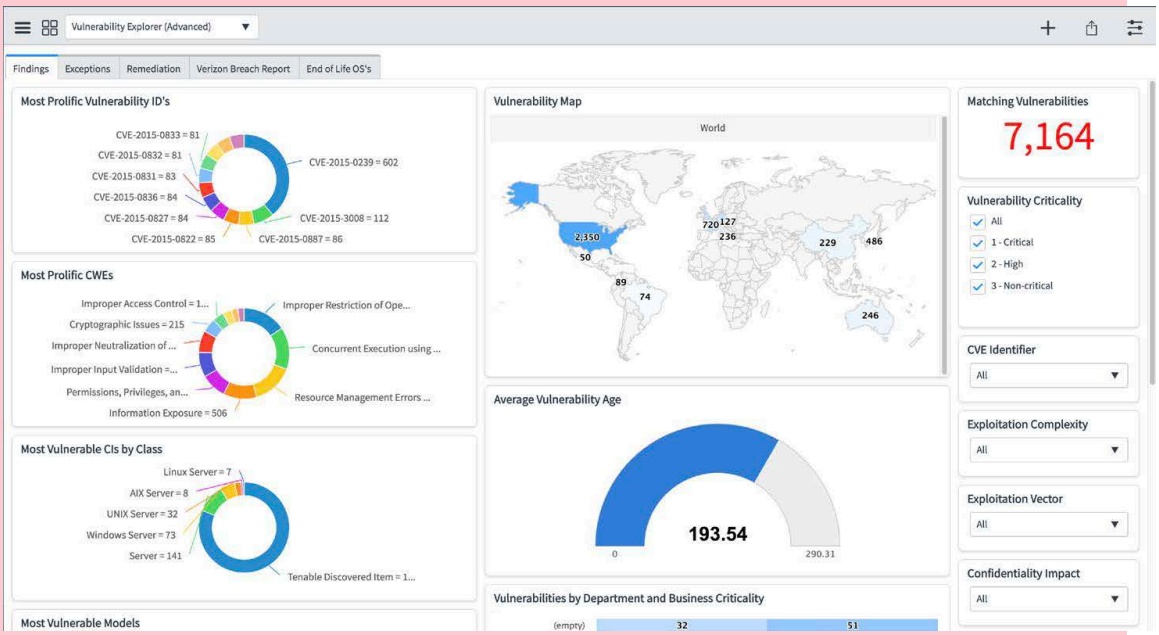
Search all incident columns

Create Incident

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

위험 점수는 구성 가능하며 빠른 우선순위 지정을 제공합니다. 취약성에 대한 모든 정보(예: 취약성의 정의, 악용 방법 및 위협 수정 방법)는 NVD(국가 취약성 데이터베이스)에서 자동으로 가져온 취약성 대응 므로 수동 조사가 필요하지 않습니다. 솔루션의 구성 가능한 대시보드는 조직의 전반적인 취약성 노출을 즉시 보여줍니다.

VR 대시보드

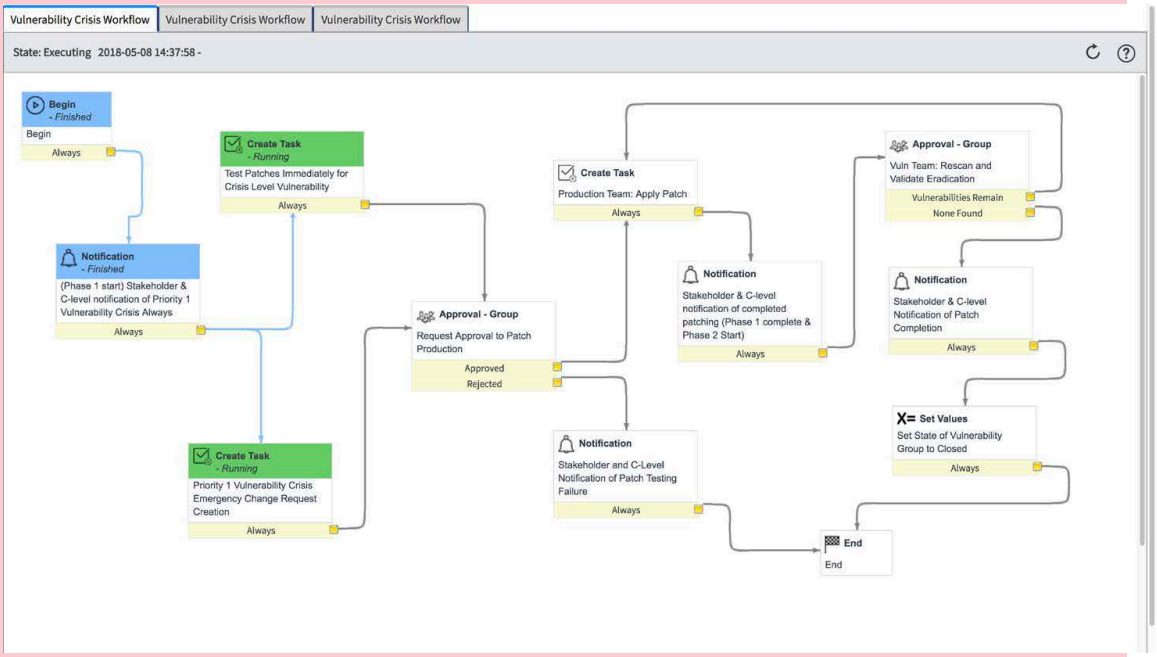


다음 단계 자동화

가장 중요한 취약한 항목을 보안 운영 식별하고 우선순위를 지정하면 워크플로우에서 다음 단계 중 몇 가지를 자동화합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

상태 인코딩 워크플로우



비즈니스에 중요한 취약한 항목의 경우 자동 패치 적용 승인 요청이 전송되고 적절한 소유자에게 알림이 전송됩니다. 따라서 당직 분석가를 검색하거나 "중요"로 간주되는 항목을 수동으로 결정할 필요가 없습니다.

패치가 승인되고 완료되면 수정 사항을 확인하기 위해 두 번째 검사가 자동으로 실행됩니다. 우선순위 지정, 워크플로우 및 자동화를 사용하여 가장 중요한 항목을 먼저 해결합니다.

보안 운영 그리고 **ServiceNow Store**

부터 Madrid모든 보안 운영 애플리케이션과 지원되는 통합은 에서 다운로드할 수 있습니다 ServiceNow Store. 이를 통해 새 기능과 업데이트된 기능을 더 빠르게 얻을 수 있습니다. 애플리케이션을 사용하려면 보안 운영 먼저 해당 애플리케이션에 대한 권리가 있는지(즉, 애플리케이션을 사용할 수 있는 유효한 라이센스가 있는지) 확인하고, 에서 다운로드한 ServiceNow Store후 활성화해야 합니다.

다운로드할 수 있는 애플리케이션 목록은 보안 운영 계속 증가하고 있습니다.

- 보안 인시던트 응답 (및 지원되는 통합)
- 취약성 대응 (및 지원되는 통합)
- 위협 인텔리전스 (및 지원되는 통합)
- 구성 준수
- Trusted Security Circle
- Data Loss Prevention Incident Response

5분 길이의 이 비디오를 통해 Security Operations 및 GRC 애플리케이션을 ServiceNow Store. 이 5분 길이의 비디오에서는 ServiceNow Store에서 보안 운영 및 GRC 애플리케이션을 다운로드하는 방법을 설명합니다.

애플리케이션 및 통합을 가져오는 보안 운영 데 사용하는 프로세스는 애플리케이션을 처음 다운로드하는지, 에서 이전에 다운로드한 ServiceNow Store애플리케이션을 업데이트하는지 또는 한 제품군 릴리스에서 다음 제품군 릴리스로 업그레이드하는지에 따라 달라집니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

에서 처음으로 애플리케이션 **ServiceNow Store** 다운로드

에서 응용 프로그램을 ServiceNow Store 처음 다운로드하려면 여러 가지 간단한 단계를 거쳐야 합니다. 일부 단계는 에서 ServiceNow Store 수행되고 일부 단계는 인스턴스에서 수행됩니다.

핵심 ServiceNow Store 제품과 애플리케이션을 다운로드할 수 있습니다. 제품에는 그룹으로 사용이 허가된 하나 이상의 애플리케이션이 포함되어 있습니다. 예를 들어, 보안 인시던트 응답 는 제품입니다. 프로세스에는 다음 단계가 포함됩니다.

필요한 역할: admin.

- ServiceNow Store에서 애플리케이션 및 해당 종속 애플리케이션에 대한 권리(또는 라이센스)가 있는지 확인해야 합니다.

  주:
  이 프로세스는 프로덕션 인스턴스에 다운로드된 애플리케이션에만 적용됩니다. 애플리케이션을 비프로덕션 또는 개발 인스턴스에 다운로드하는 경우에는 권리를 얻을 필요가 없습니다. 로 애플리케이션 활성화 ServiceNow Store계속 진행합니다.

- 마지막으로 애플리케이션을 활성화하고 인스턴스에서 실행할 수 있습니다.

주:
이전 버전 Rome 이상의 릴리스부터 핵심 애플리케이션을 활성화하면 종속성 플러그인이 자동으로 활성화됩니다. 예를 들어 애플리케이션을 취약성 대응 활성화하면 취약성 대응 Dependencies 플러그인도 활성화됩니다. 자세한 내용은 애플리케이션 활성화 ServiceNow Store 문서를 참조하십시오.

제품 또는 애플리케이션에 대한 보안 운영 권리 가져오기

애플리케이션을 설치하는 보안 운영 첫 번째 단계는 애플리케이션 또는 제품 및 관련 애플리케이션에 유효한 ServiceNow 권리가 있는지 확인하는 것입니다.

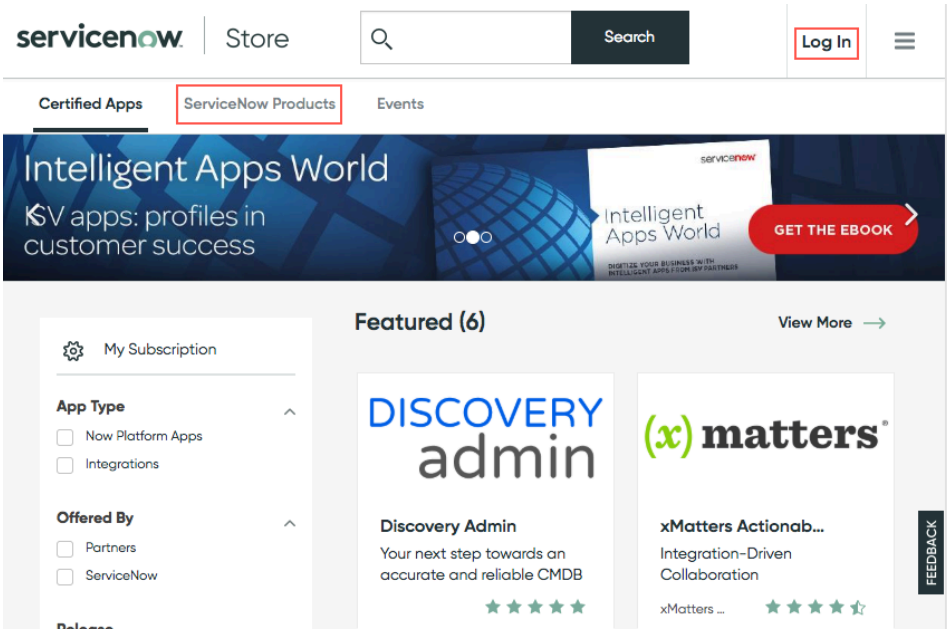
시작하기 전에
필요한 역할: 관리자
권리를 수행하는 개인은 Now Support 계정이 있어야 하며 고려 중인 인스턴스에 대한 애플리케이션을 요청할 수 있는 권한이 있어야 합니다.

주:
이 프로세스는 프로덕션 인스턴스에 다운로드된 애플리케이션에만 적용됩니다. 하위 프로덕션 또는 개발 인스턴스에 애플리케이션을 다운로드하는 경우에는 권리를 얻을 필요가 없습니다. 로 애플리케이션 활성화 ServiceNow Store계속 진행합니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

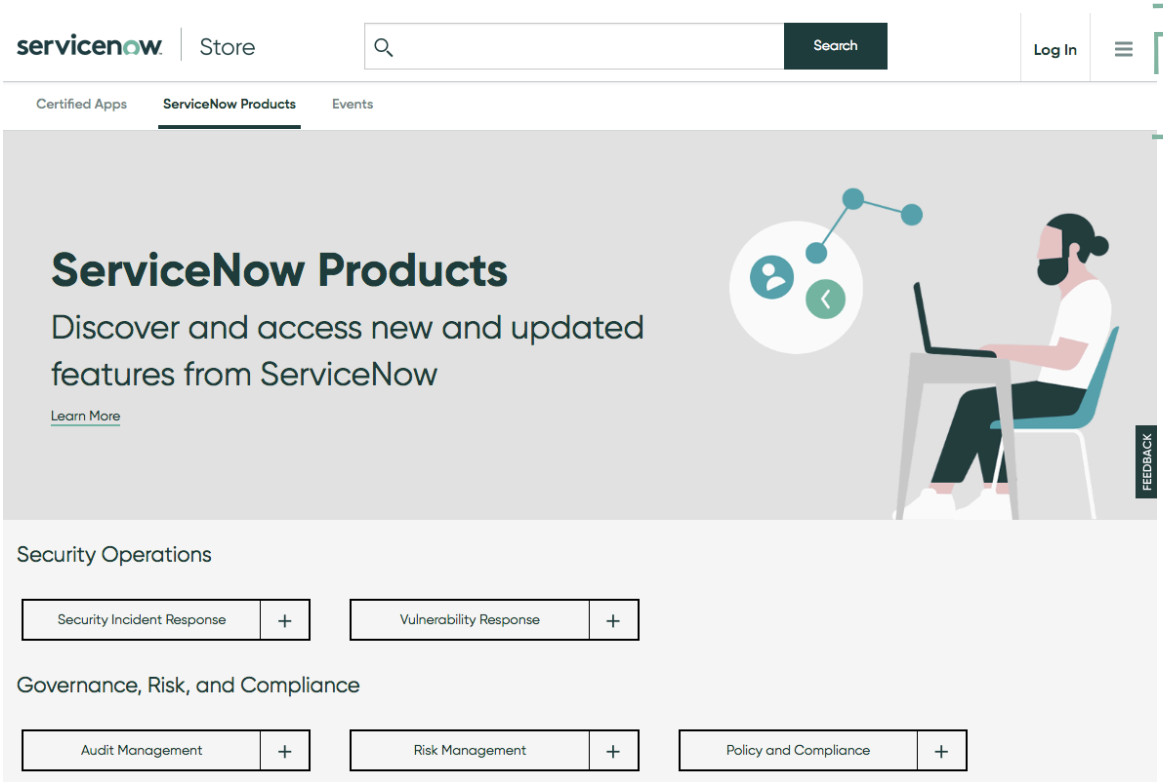
프로시저

1. 다음으로 이동합니다. ServiceNow Store .



2. 로그인을 클릭하고 자격 증명을 사용하여 HI 로그인합니다.

3. **ServiceNow** 제품 탭을 클릭하여 사용 가능한 ServiceNow 모든 제품을 확인합니다. 통합 및 기타 유형의 콘텐츠가 인증된 앱 탭에 표시됩니다.



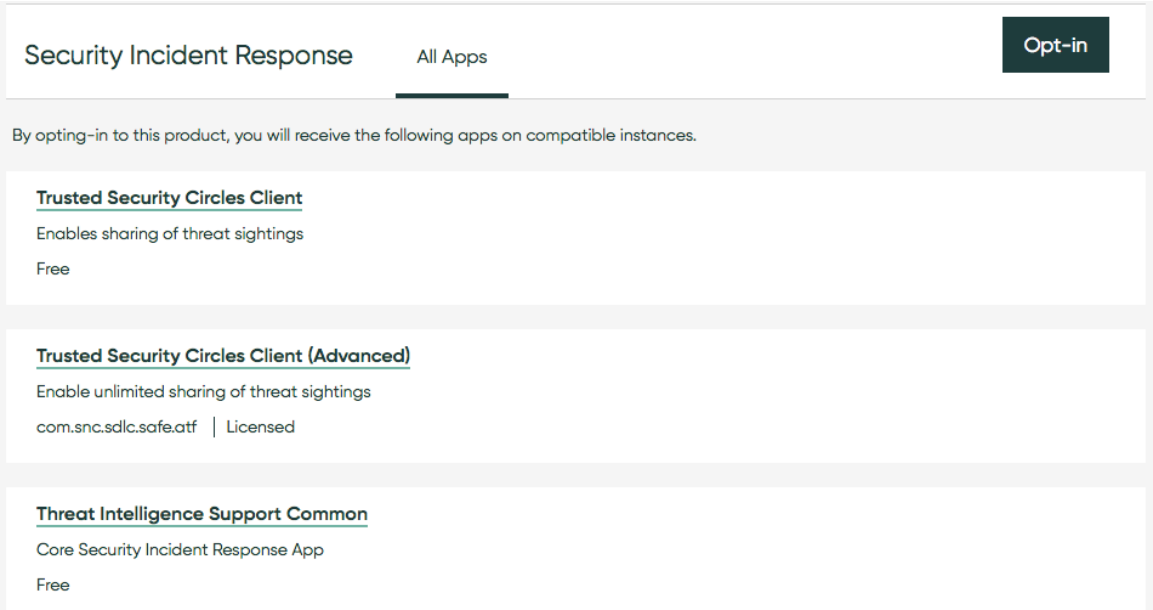
주:
이 예에서는 제품에 대한 보안 인시던트 응답 권리를 획득한다고 가정합니다.

4. 권리를 얻으려는 제품 이름 옆의 더하기(+) 기호를 클릭합니다.

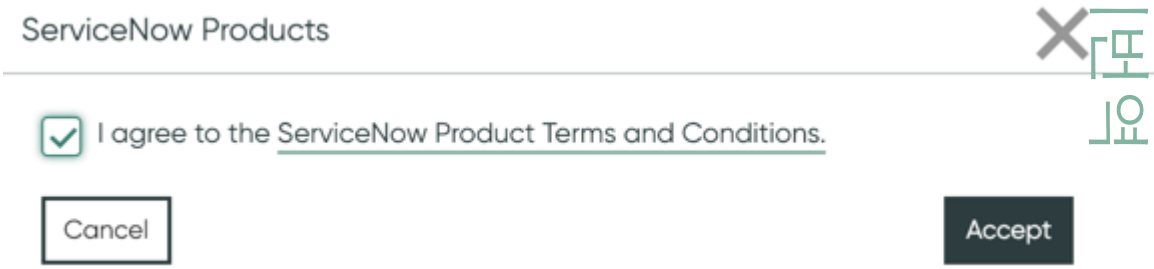
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

권한을 부여하는 제품과 연결된 모든 애플리케이션이 나열됩니다. 핵심 제품에 대한 권리를 획득하면 그 아래에 나열된 애플리케이션에도 자격이 부여됩니다.

주:
제품 이름을 클릭하여 제품 및 관련 애플리케이션에 대한 자세한 정보를 볼 수도 있습니다.



5. 옵트인을 클릭하여 나열된 제품 및 애플리케이션에 대한 권리가 있는지 확인합니다. 사용 약관을 읽고 동의 ServiceNow 하라는 메시지가



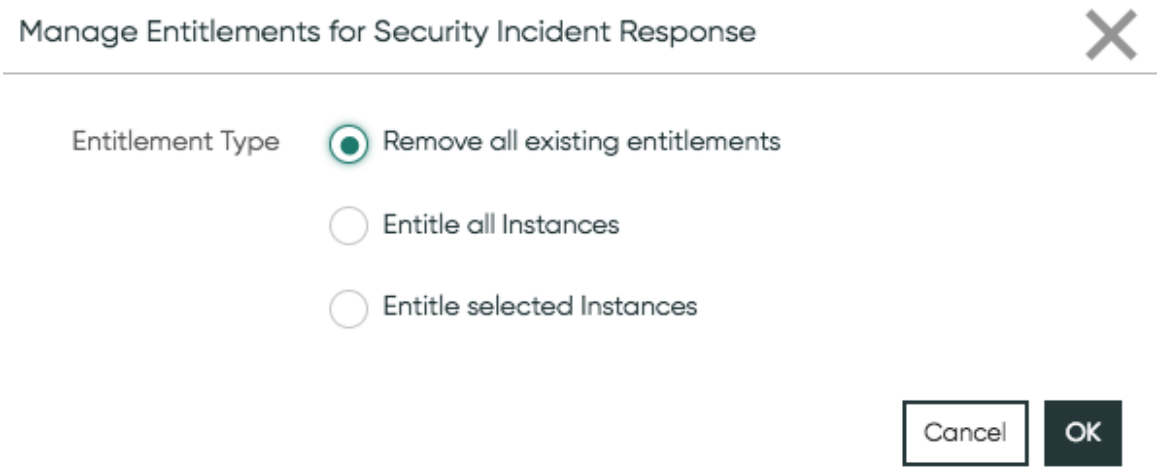
표시됩니다.

6. 확인란을 선택하고 수락을 클릭합니다.
7. 제품 이름 옆에 확인 표시가 나타나고 권리 관리 버튼이 나타납니다.

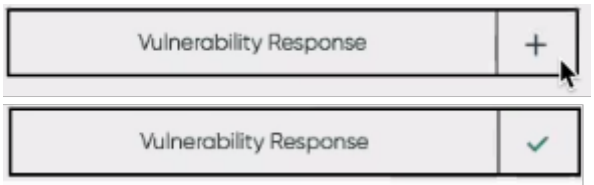
확인 표시는 제품 및 관련 애플리케이션을 구독했음을 나타냅니다. 이제 권리를 관리할 차례입니다. 이 프로세스는 이 제품과 나중에 설치하려는 다른 제품에 대한 일회성 프로세스입니다.

8. 옵션: 권리 관리를 클릭하여 권리가 부여된 애플리케이션의 영향을 받는 인스턴스를 변경할 수 있습니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



9. 사용 약관 및 관리되는 권리에 ServiceNow 동의한 후에는 클릭 한 번으로 다른 제품에 권한을 부여할 수 있습니다.



주:
제품을 활성화할 준비가 되었습니다.

애플리케이션 활성화 **ServiceNow Store**

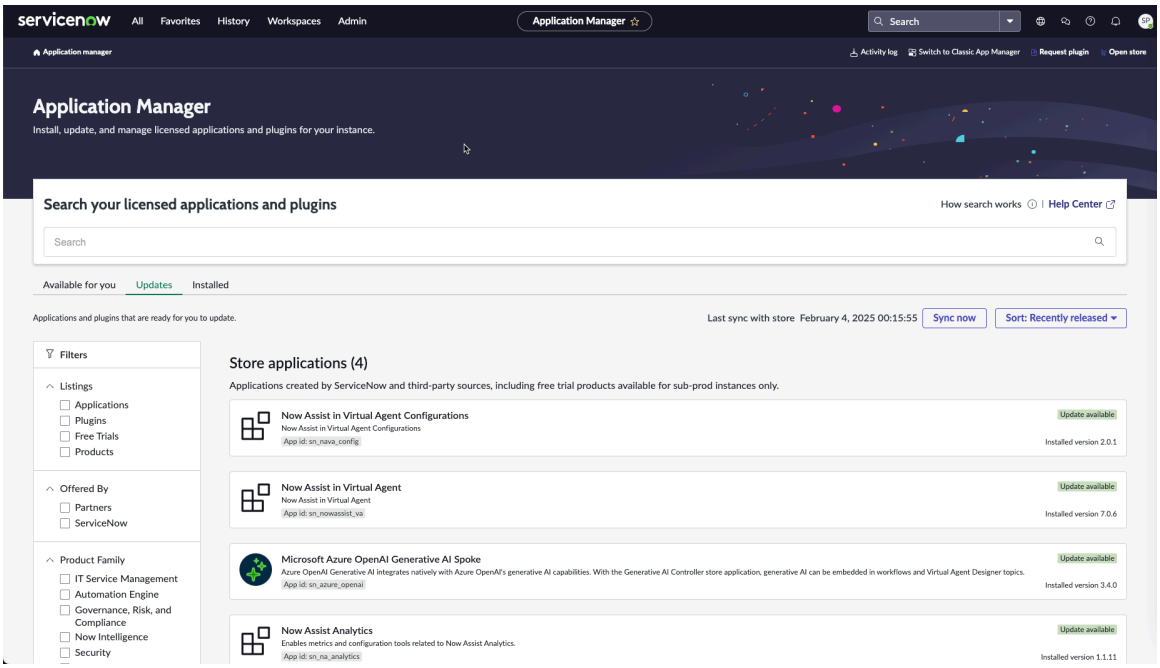
애플리케이션에 권리가 부여되면 해당 종속성 플러그인을 활성화하고 애플리케이션을 활성화해야 합니다. 이 프로세스는 하위 프로덕션 인스턴스에 다운로드된 애플리케이션에도 적용됩니다.

시작하기 전에
필요한 역할: admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

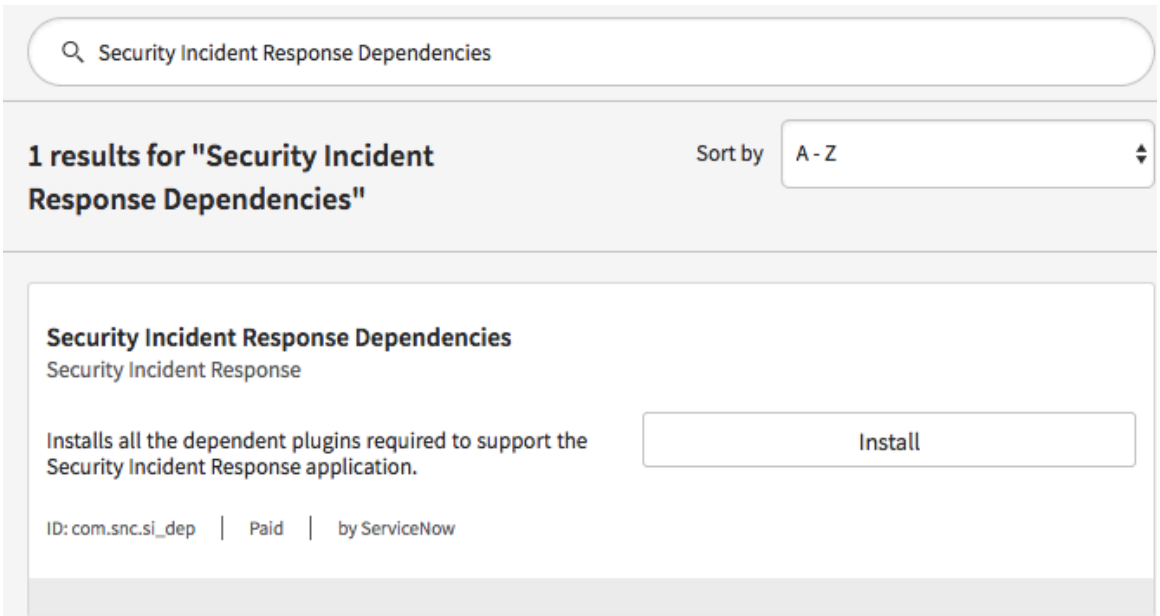
프로시저

1. 다음으로 이동 시스템 애플리케이션 〉 모든 사용 가능 애플리케이션 〉 모두.



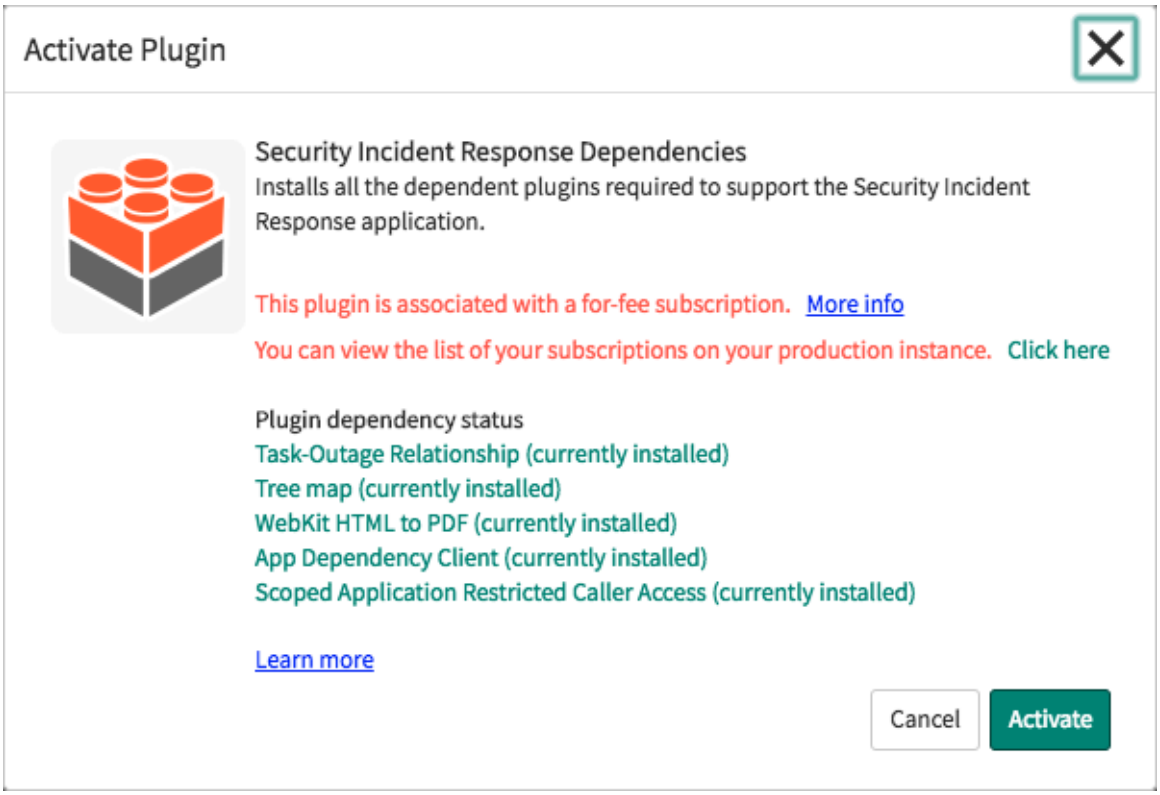
주:
Orlando부터는 핵심 애플리케이션을 활성화하면 의존성 플러그인이 자동으로 활성화됩니다. 예를 들어 애플리케이션을 취약성 대응 활성화하면 취약성 대응 Dependencies 플러그인도 활성화됩니다. 따라서 2-5단계는 선택 사항입니다.

2. 활성화하려는 애플리케이션의 dependencies 플러그인을 검색합니다.
예를 들어, 를 활성화하는 보안 인시던트 응답경우 종속성 플러그인을 찾습니다 보안 인시던트 응답 .



3. 설치를 클릭합니다.
플러그인 활성화 대화 상자가 나타납니다.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 플러그인 활성화**(Activate Plugin)** 대화 상자에서 활성화(**Activate**)를 클릭합니다.
5. 활성화가 완료되면 **Close & Reload Form**을 클릭합니다.
6. 이제 활성화 중인 핵심 제품을 찾고, 데모 데이터를 로드하려면 데모 데이터와 함께 설치 확인란을 클릭한 다음 설치를 클릭합니다.
   애플리케이션이 인스턴스에 자동으로 설치됩니다.

   주:
   데모 데이터와 함께 설치 확인란을 선택하지 않으면 나중에 애플리케이션 관리자에서 데모 데이터를 설치할 수 없습니다. 초기 설치 후 데모 데이터를 설치하거나 다시 설치하는 방법에 대한 자세한 내용은 기술 자료에서 애플리케이션이 이미 설치된 경우 데모 데이터를 설치하기 위한 해결 방법 (KB0722909) 문서를 HI 참조하십시오.

보안 운영 통합 설치

모든 ServiceNow 통합은 에서 사용할 수 있습니다 ServiceNow Store. Security Incident Response와 같은 핵심 애플리케이션은 스토어의 **ServiceNow** 제품 탭에서 볼 수 있습니다. 통합 추가 기능은 인증된 앱 탭에서 볼 수 있습니다.

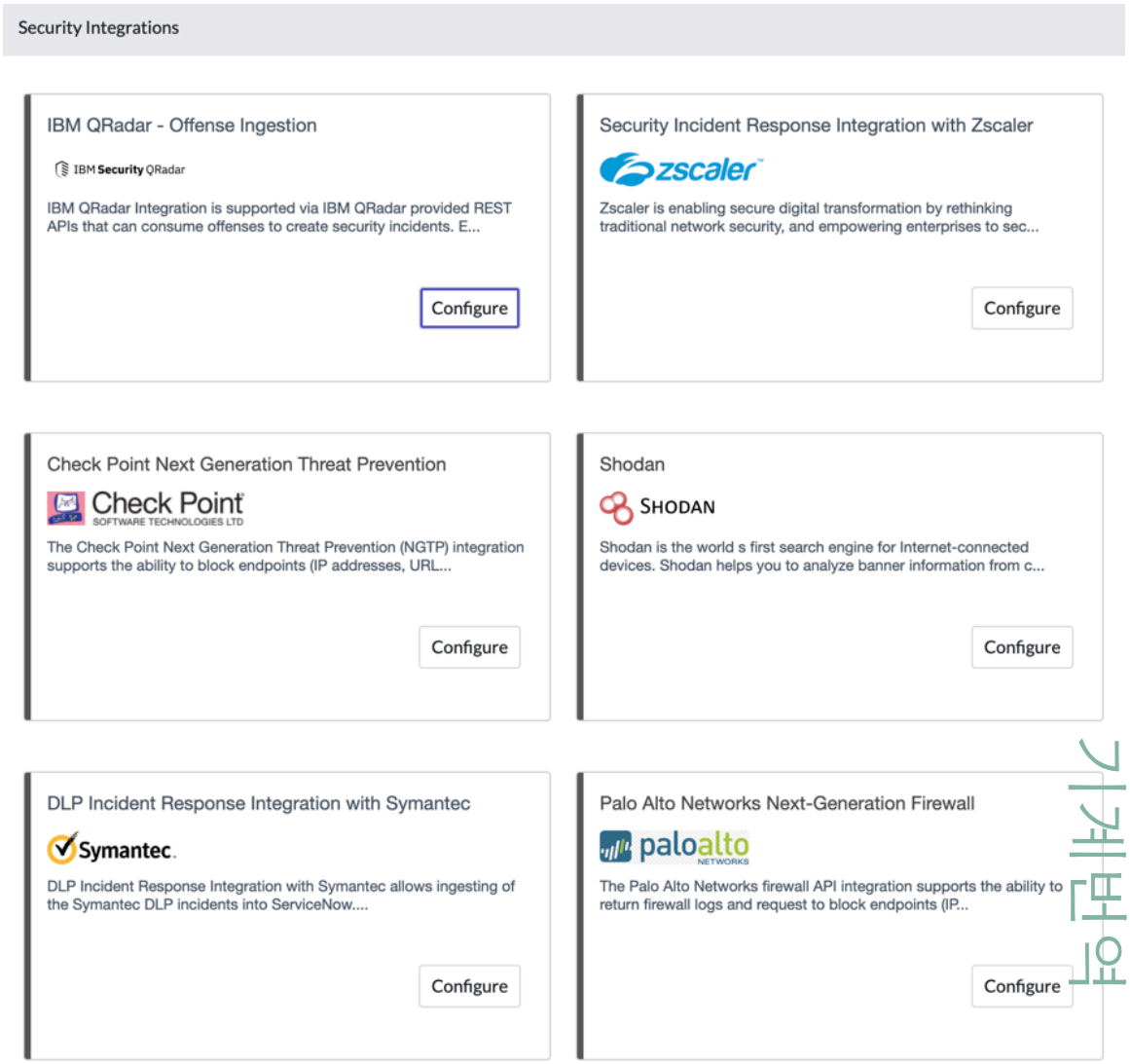
시작하기 전에
필요한 역할: 관리자
스토어 설치에는 Now Support 고려 중인 인스턴스에 대한 애플리케이션을 요청할 수 있는 계정 및 권한이 필요합니다.

프로시저

1. 다음으로 이동 보안 운영 〉 통합 〉 통합 구성 ServiceNow Store에서 애플리케이션을 설치한 후 통합에 대한 구성 타일이 나타납니다

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

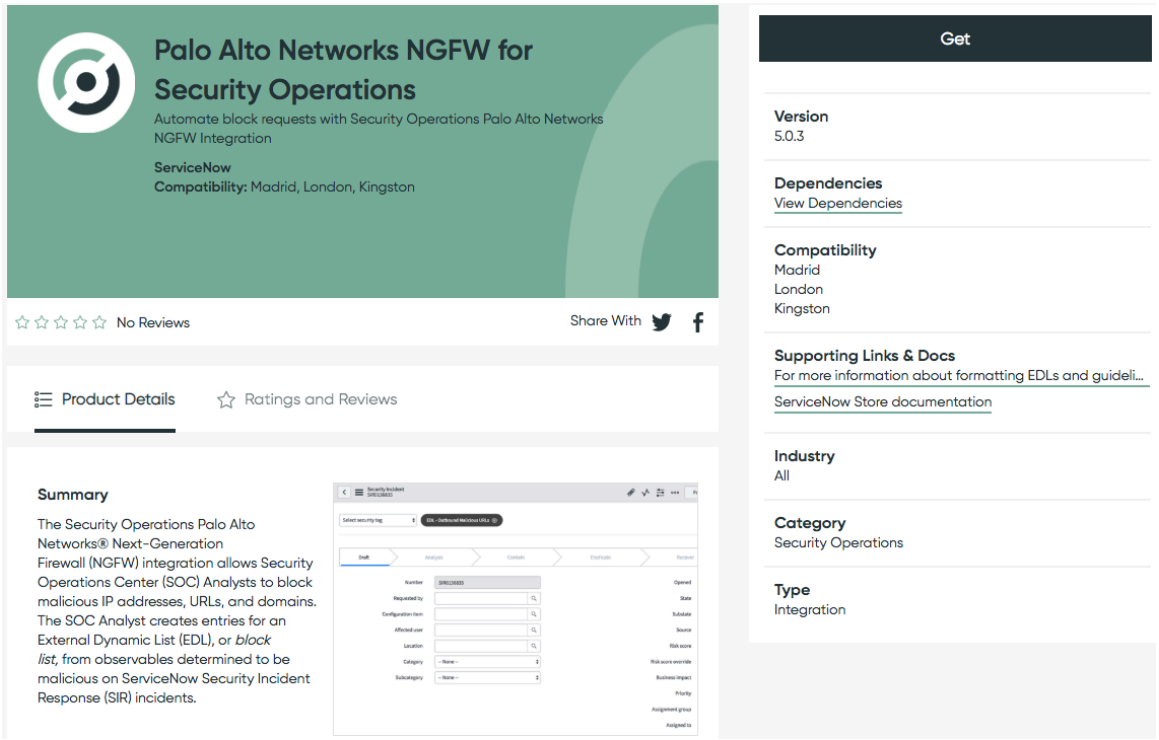
주:



2. 설치할 통합을 찾고 구성을 클릭합니다.
선택한 통합이 ServiceNow Store

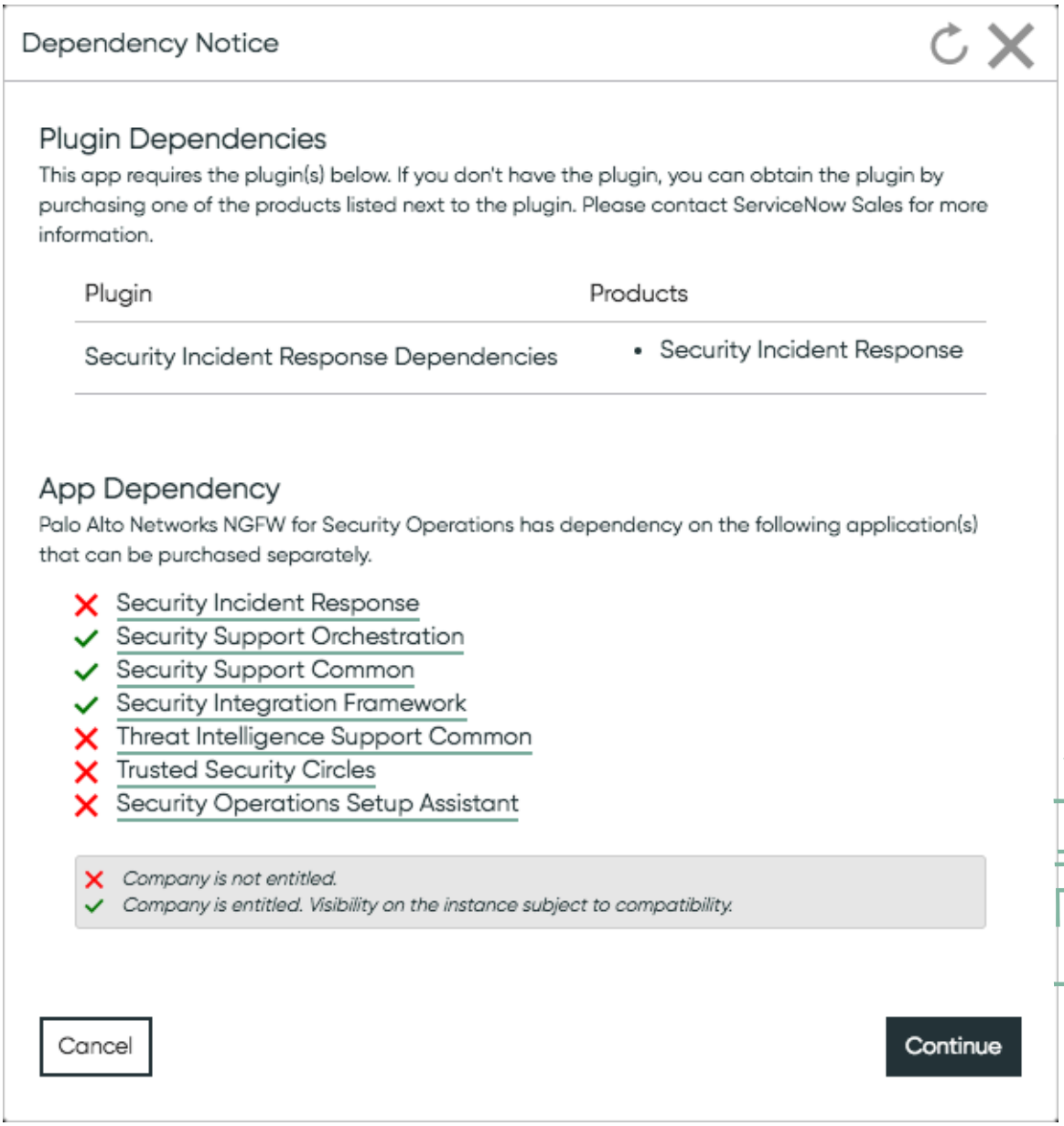
기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



3. 종속성 보기를 클릭하고 나열된 앱 종속성을 검토합니다.

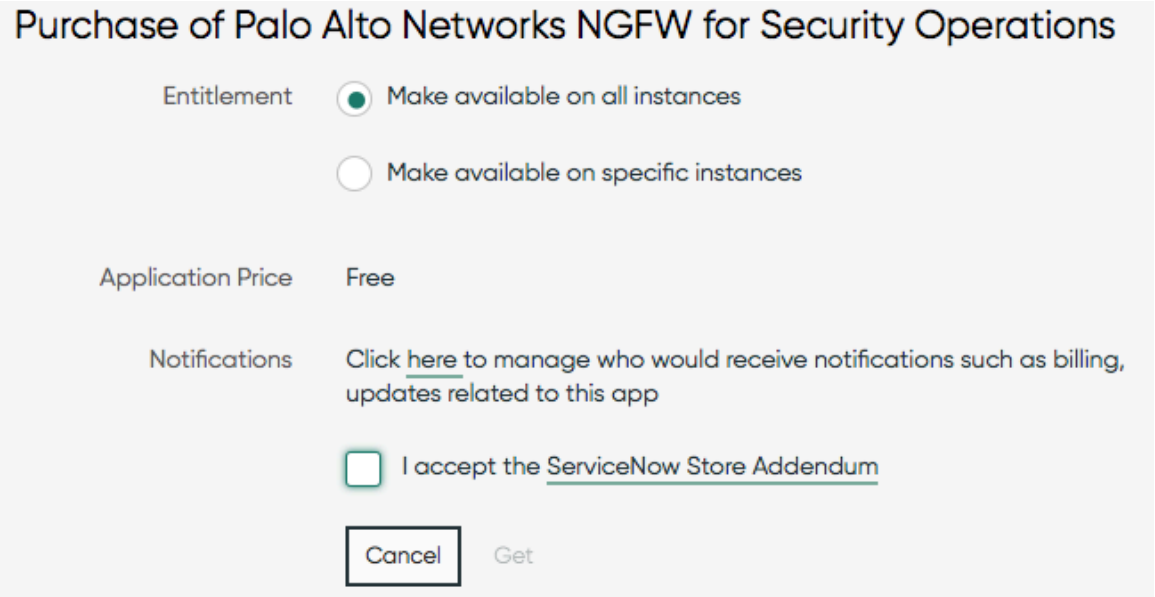
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 통합에 회사에 아직 권리가 부여되지 않은 핵심 애플리케이션 의존성(예: 보안 인시던트 응답)이 있는 경우
   a. 다음 지침에 따라 권리를 얻고, 종속성 플러그인을 다운로드하고, 애플리케이션을 활성화합니다.
   b. 이 절차로 돌아갑니다.
   c. 계속을 클릭합니다.
5. 가져오기를 클릭합니다.
   ServiceNow 사용 약관이 나타납니다.
6. 계속을 클릭합니다.
   다음과 유사한 구매 화면이 열립니다.

기계번역

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



7. 통합을 사용할 수 있는 인스턴스를 식별하고, 알림을 관리하고, **ServiceNow Store** 부록 확인란을 선택합니다.
8. 가져오기를 클릭합니다.

   주:
   구입을 위해 애플리케이션을 다운로드하는 경우 구입을 클릭합니다. 벤더의 사전 승인을 받아야 하는 애플리케이션을 다운로드하는 경우 애플리케이션 요청을 클릭합니다.

9. 인스턴스 이름과 요청 이유를 입력한 다음 요청을 클릭합니다.
   자세한 설치 지침이 포함된 이메일이 전송됩니다.
10. 다음으로 이동 시스템 애플리케이션 > 모든 사용 가능 애플리케이션 > 모두.
    설치할 수 있는 애플리케이션 목록이 표시됩니다.
11. 애플리케이션을 찾아서 선택한 다음 설치를 클릭합니다.
    통합이 인스턴스에 자동으로 설치됩니다.

에서 이전에 다운로드한 애플리케이션 업데이트 **ServiceNow Store**

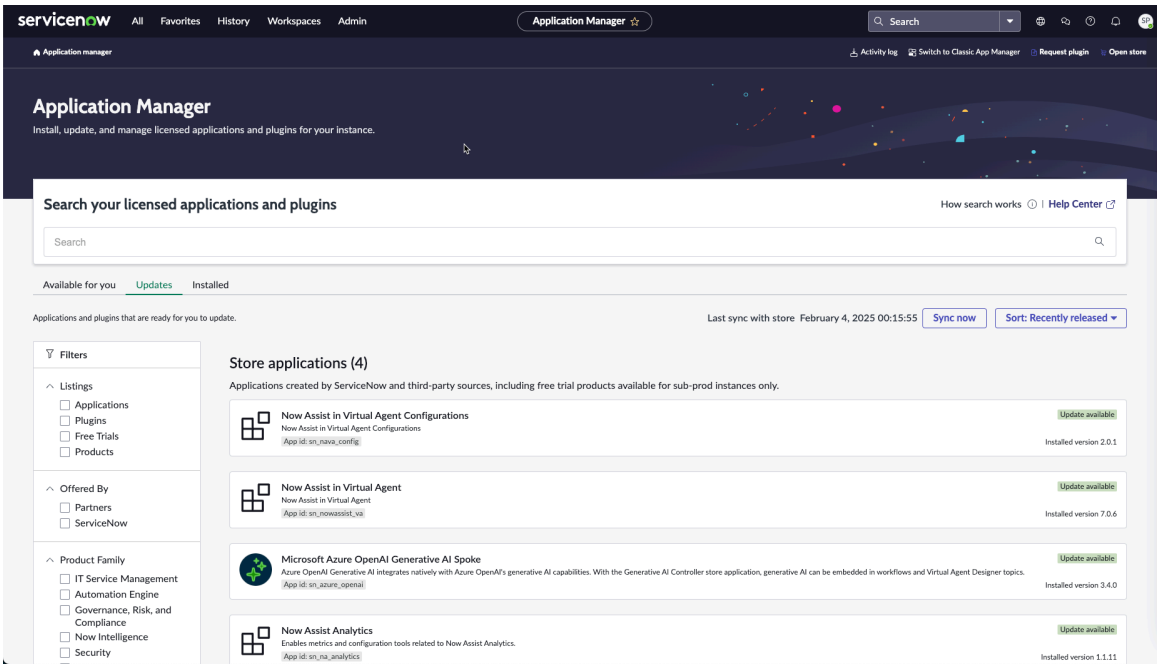
이전에 에서 ServiceNow Store 애플리케이션을 다운로드한 적이 있고 새 버전을 사용할 수 있는 경우, 인스턴스에서 업데이트할 수 있습니다.

시작하기 전에
필요한 역할: admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 시스템 애플리케이션 〉 모든 사용 가능 애플리케이션 〉 모두.



2. 업데이트하려는 애플리케이션을 검색합니다.
3. 업그레이드할 버전을 선택하고 업데이트를 클릭합니다.
   애플리케이션이 인스턴스에 자동으로 설치됩니다.

인스턴스를 다음 제품군 릴리스로 업그레이드

현재 제품군 릴리스를 실행 중이고 다음 릴리스로 업그레이드하려는 경우에는 에서 ServiceNow Store애플리케이션을 가져올 필요가 없습니다. 플랫폼이 필요한 최소 버전으로 업데이트되면 애플리케이션이 자동으로 업데이트됩니다.

필요한 역할: 관리자

자세한 내용은 다시 디자인된 릴리스 정보를 탐색하고 원하는 Learn about the Zurich release 정보와 새로운 기능을 찾는 방법을 참조하십시오Using the release notes .

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.