XDR을 사용하여 전자 메일 알림 자동화 워크플로 구성

목차

소개

이 문서에서는 새 인시던트에 대한 이메일 알림을 전송하기 위해 자동화된 워크플로를 만드는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

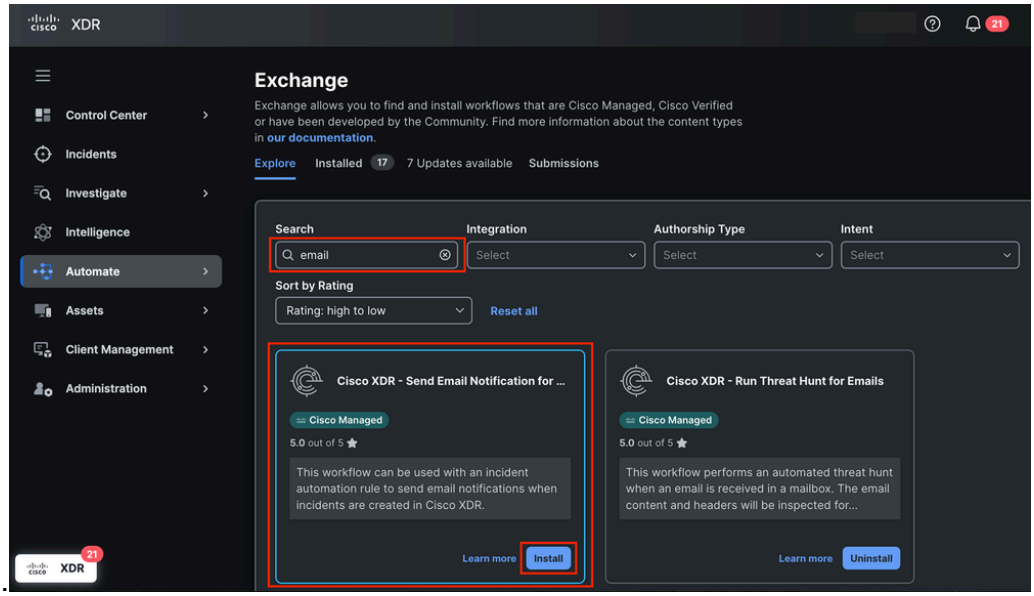
구성

이 가이드에서는 인시던트 발생 시 이메일 알림을 자동으로 전송하도록 워크플로를 구성하고 활성화하는 데 필요한 단계에 대해 자세히 설명합니다. 자세한 단계는 다음과 같습니다.

Cisco XDR Exchange에서 워크플로 설치

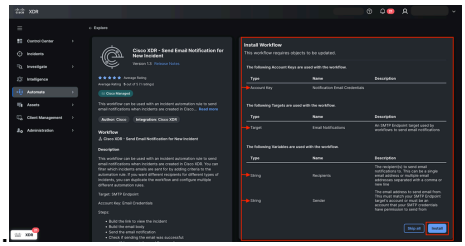
1단계. 엔드포인트 격리 워크플로 설치

1. Cisco XDR에 로그인하고 Automate(자동화) > Exchange로 이동합니다.
2. Cisco XDR - Send Email Notification for New Incident라는 이름의 워크플로를 검색하고 Install을 클릭합니다.



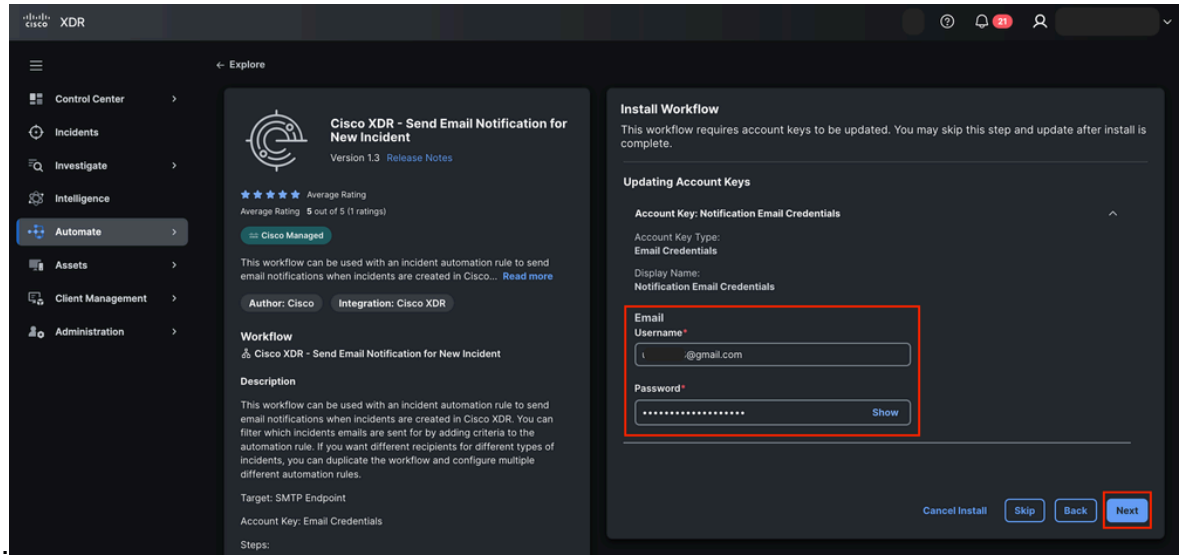
Exchange에서 전자 메일 알림 워크플로 보내기

3. 워크플로를 올바르게 구성하는 데 필요한 정보를 확인합니다.



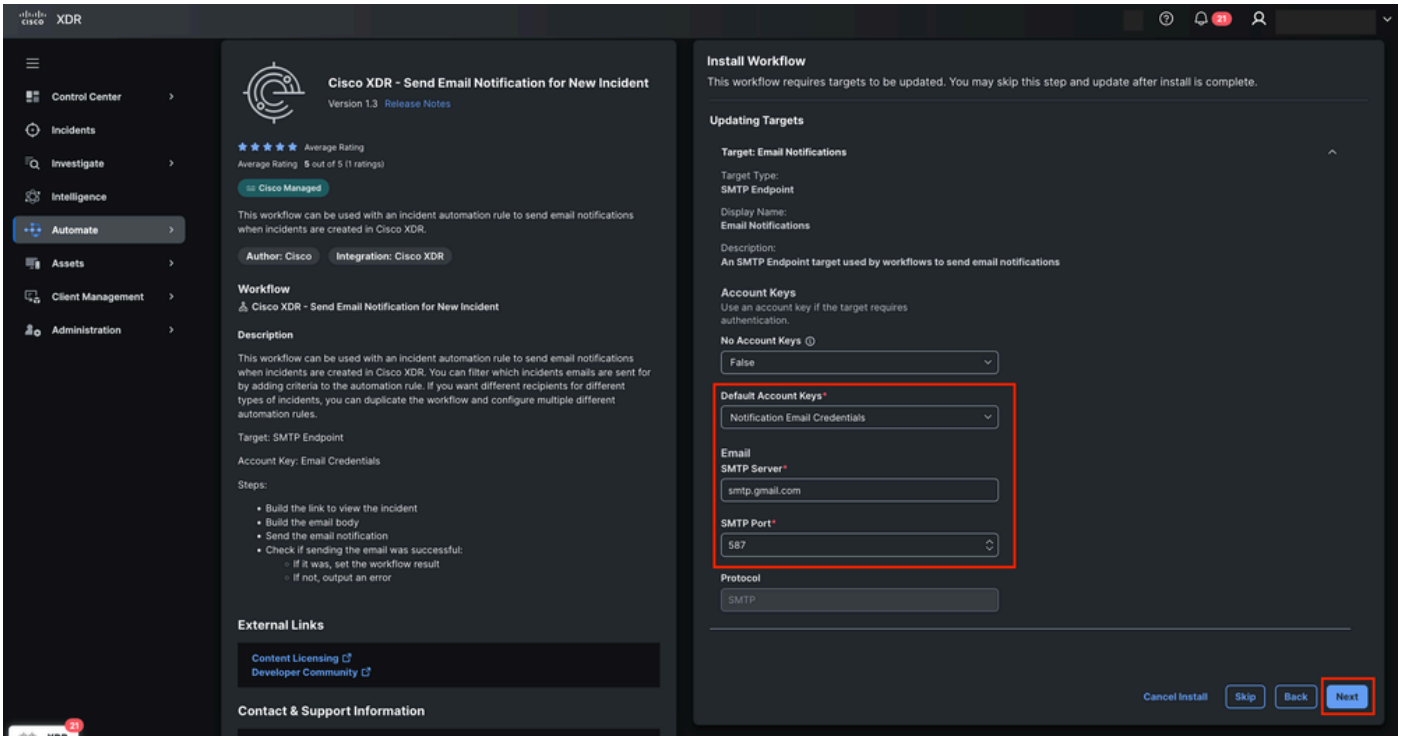
이메일 알림 전송 워크플로 개요

4. 계정 키 입력발신자를 설정할 이메일 자격 증명 표시되는 이름은 알림 이메일 자격 증명이며 다음 단계.



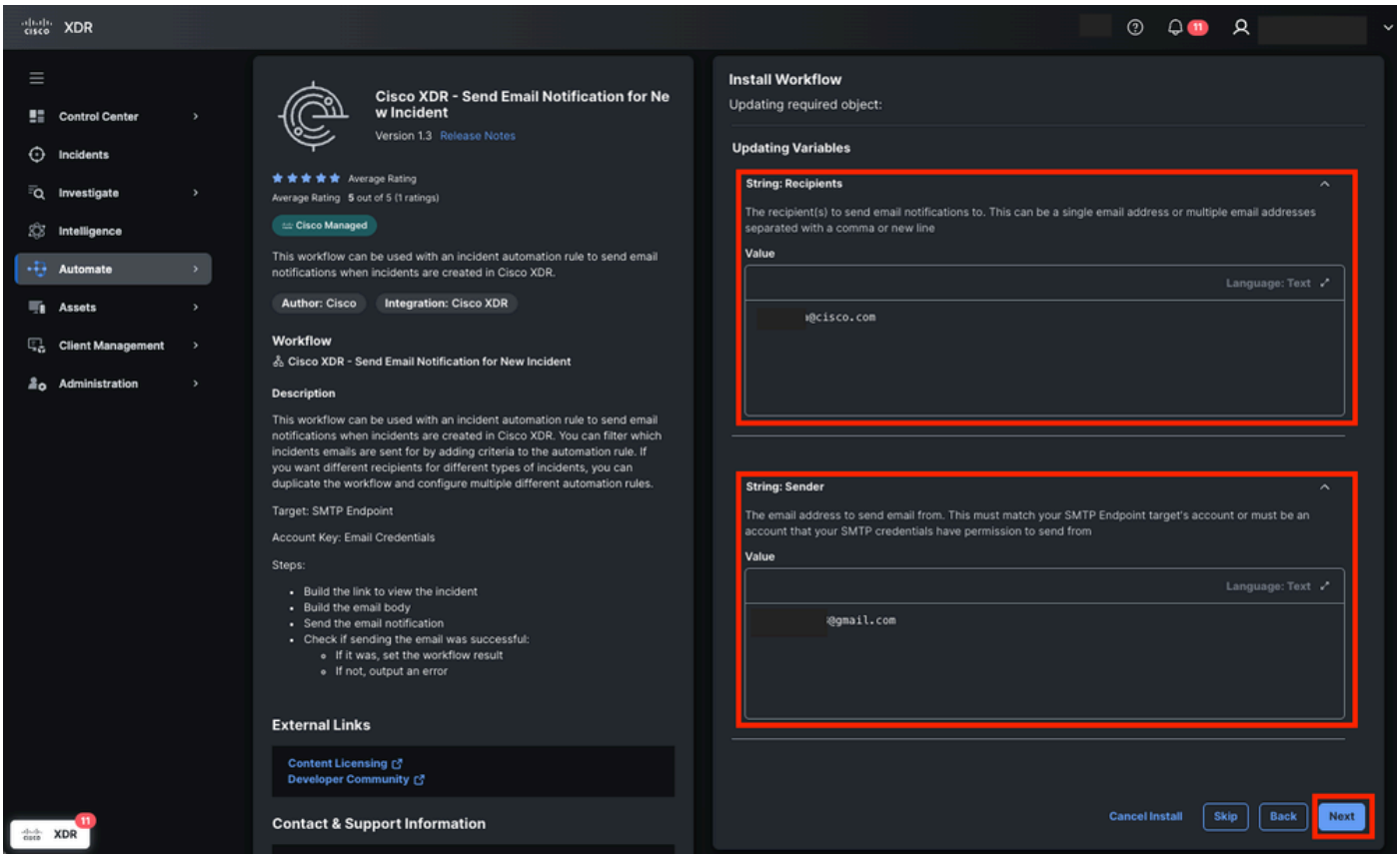
워크플로의 계정 키

5. 다음과 같이 대상 정보를 구성합니다.
    - 계정 키: 알림 이메일 자격 증명
    - Email
        - SMTP 서버: smtp.gmail.com
        - SMTP 포트: 587



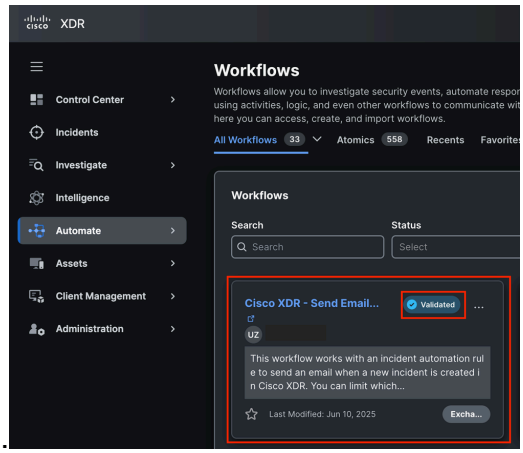
워크플로의 대상 구성

1. Next(다음)를 클릭합니다.
2. 다음에 대한 변수를 업데이트합니다.
    - 수신인
    - 발송인



워크플로에 대한 변수 할당

8. 다음을 클릭합니다.



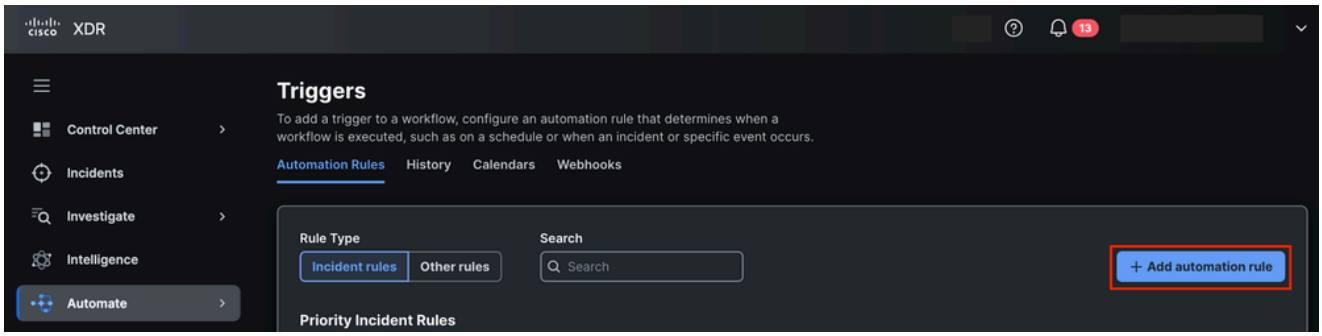
9. 자동화 > 워크플로우로 이동하여 검증됨 상태를 확인합니다.

워크플로 검증 상태

자동화 규칙 만들기

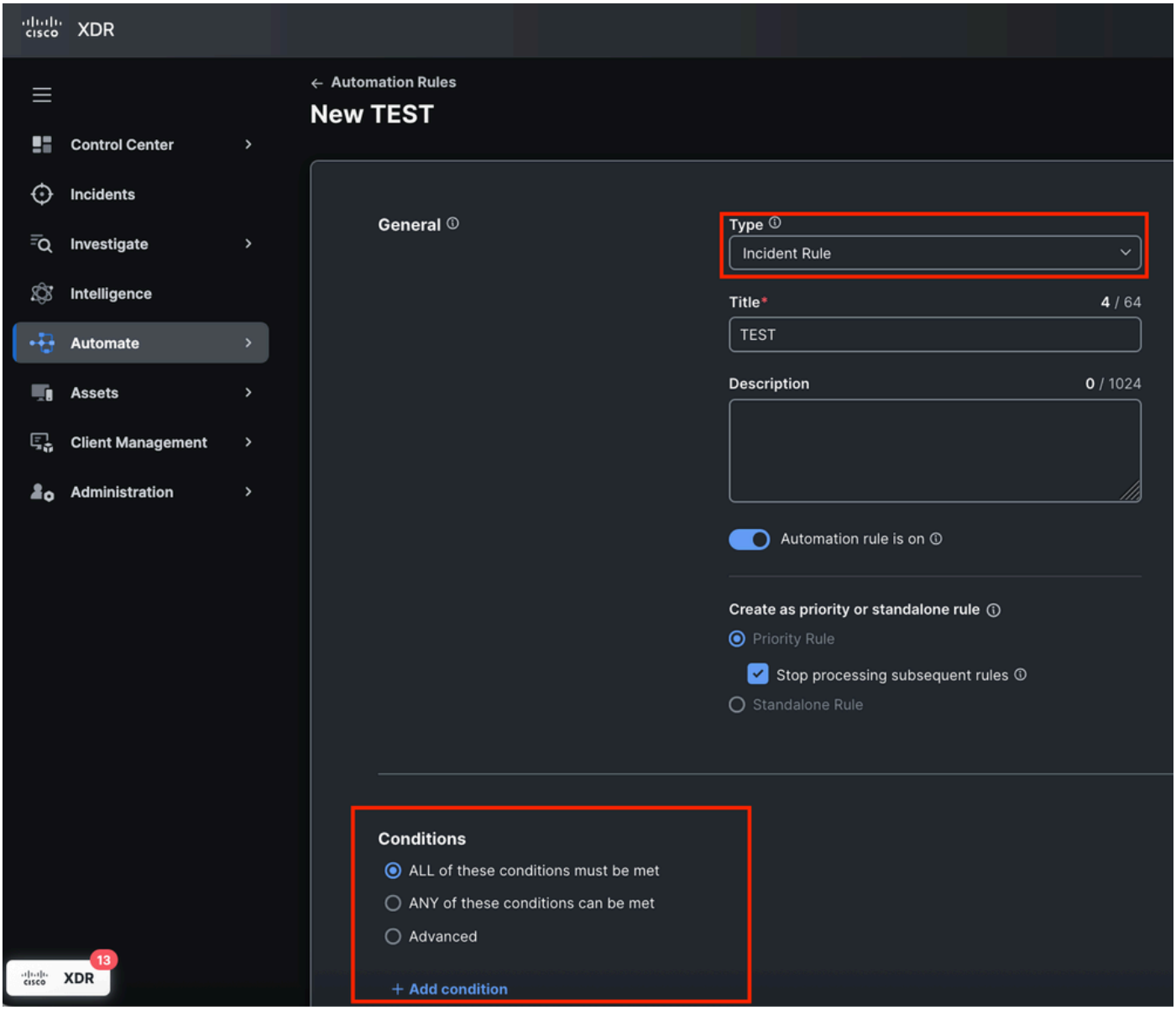
2단계. 자동화 규칙 구성

1. Automation > Triggers 섹션으로 이동합니다.
2. 새 규칙을 생성합니다. Add automation rule(자동화 규칙 추가)을 클릭하고 이름을 할당합니다.



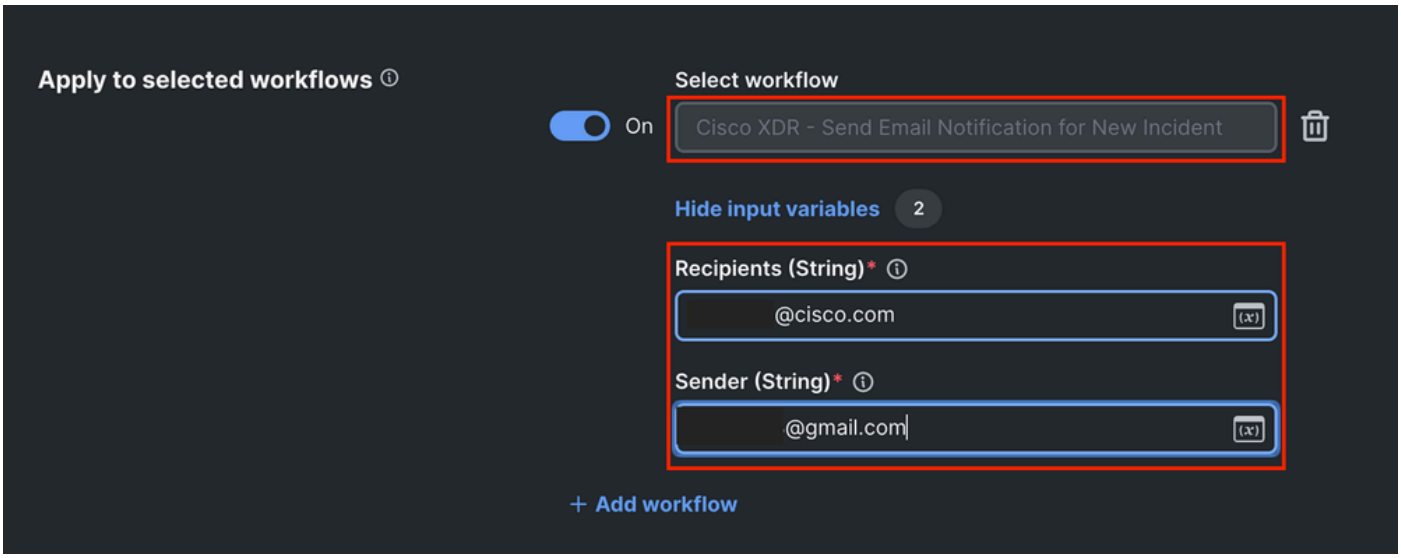
트리거에서 자동화 규칙 추가

3. Incident Rule Type을 선택하고 트리거 조건을 정의합니다. 규칙 조건을 추가하지 않고도 계속할 수 있으며, 그러면 인시던트가 이 규칙을 활성화하게 됩니다. 필요한 경우 조건을 사용자 지정합니다.



자동화 규칙 유형 및 조건

4. 이전에 설치한 Cisco XDR - Send Email Notification for New Incident 워크플로에 자동화 규칙을 적용합니다. 수신자 및 발신자 변수를 설정합니다.

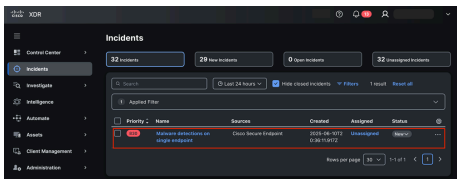


워크플로에 자동화 규칙 적용 및 변수 할당

5. 규칙을 저장합니다.

워크플로 기능 검증

3단계. 워크플로 실행 확인



1. 규칙의 조건을 충족하는 인시던트를 생성하거나 기다립니다.

   Cisco XDR에서 새 인시던트가 검색됨

2. Incident(인시던트)를 클릭한 다음 View Incident Detail(인시던트 세부사항 보기)을 클릭합니다.

Malware detections on single endpoint

Priority 830 Status New

Reported by
Cisco XDR Analytics

on 2025-06-10T20:36:11.917Z

Unassigned

MITRE

Priority score breakdown

830

83	10
Detection Risk	Asset Value at Risk

Sources

Cisco Secure Endpoint

View Incident Detail

초기 인시던트 이름은 첫 번째 탐지를 기반으로 생성됩니다. 그러나 추가 탐지가 발생하거나 새로운 정보가 사건을 가중시킬 경우 변경될 수 있습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.