

Cisco XDR을 사용하여 엔드포인트 격리 자동화 워크플로 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[Cisco 보안 엔드포인트의 초기 컨피그레이션](#)

[1.1단계: 정책에서 격리 기능 활성화](#)

[Cisco Secure Endpoint와의 통합 확인](#)

[2.1단계: 통합 확인](#)

[Cisco XDR Exchange에서 워크플로 설치](#)

[3.1단계: 엔드포인트 격리 워크플로 설치](#)

[자동화 규칙 만들기](#)

[4.1단계: 자동화 규칙 구성](#)

[워크플로 기능 검증](#)

[5.1단계: 워크플로 실행 확인](#)

[5.2단계: 엔드포인트 격리 확인](#)

[일반적인 문제](#)

[격리 기능이 Cisco Secure Endpoint에서 활성화되지 않았습니다.](#)

소개

이 문서에서는 새 인시던트에 대한 엔드포인트를 격리하기 위해 자동화 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 장애 발생 시 엔드포인트를 자동으로 격리하도록 워크플로를 구성하고 활성화하는 데 필요한 단계에 대해 자세히 설명합니다. 이 통합은 Cisco Secure Endpoint 및 워크플로 자동화 기능과 함께 수행됩니다. 단계는 다음과 같이 요약되어 있습니다.

Cisco 보안 엔드포인트의 초기 컨피그레이션

1.1단계: 정책에서 격리 기능 활성화

1. Cisco Secure Endpoint 포털에 로그인합니다.
2. Management > Policies 섹션으로 이동합니다.
3. 격리할 엔드포인트에 적용할 정책을 선택합니다.
4. Device Isolation(디바이스 격리) 옵션이 정책 설정 내에서 활성화되어 있는지 확인합니다. 

보안 엔드포인트 정책에서 엔드포인트 격리 허용

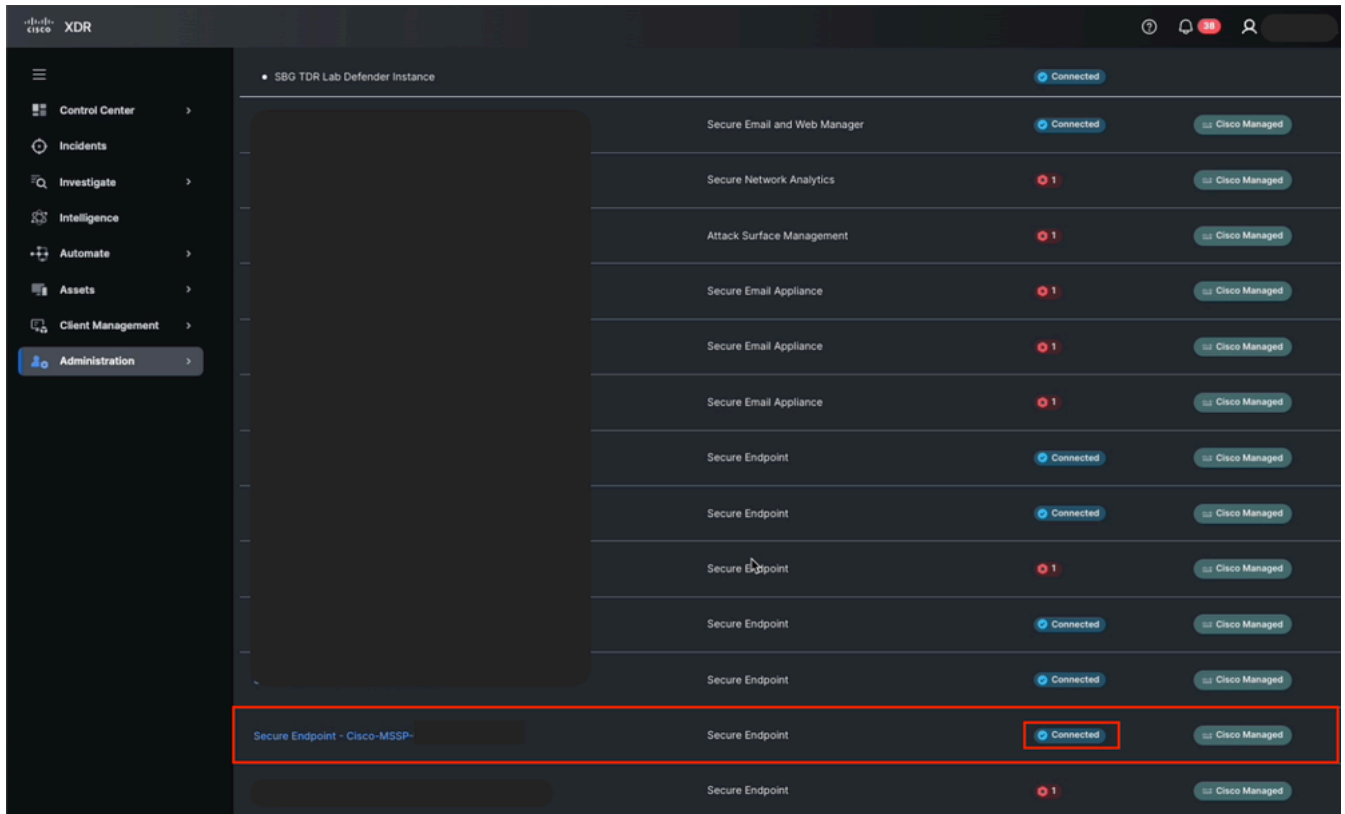
5. 변경 사항을 저장하고 필요한 경우 정책을 배포합니다.

Cisco Secure Endpoint와의 통합 확인

2.1단계: 통합 확인

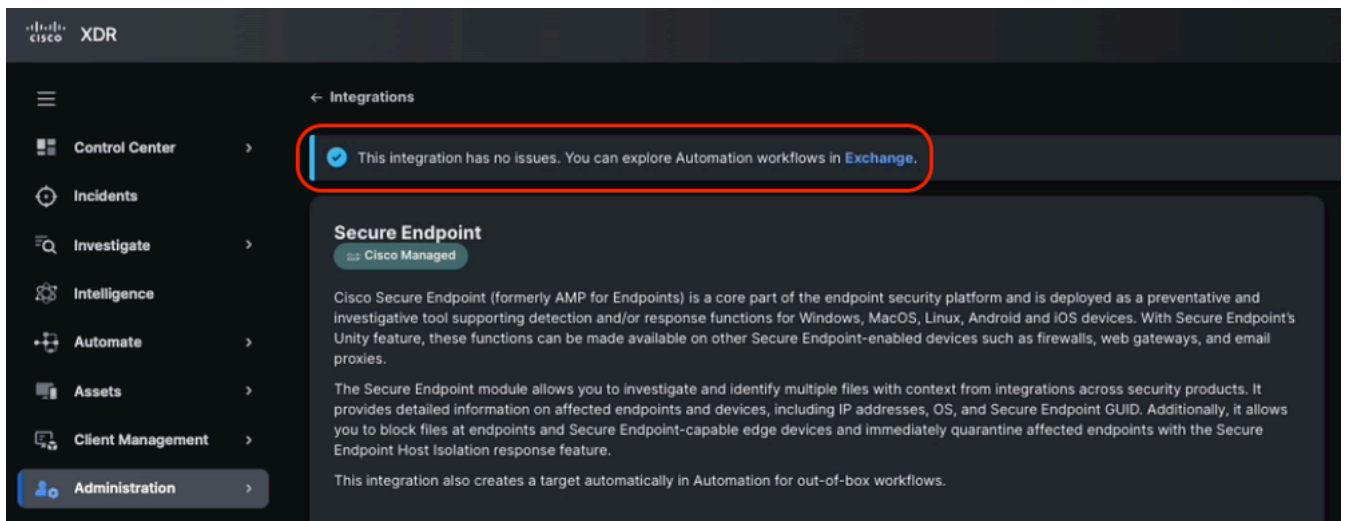
1. Cisco XDR에 로그인
2. Administration(관리) > Integrations(통합) > My Integrations(내 통합) 섹션으로 이동합니다.
3. Cisco Secure Endpoint와의 통합이 올바르게 구성되었는지 확인합니다.

Connected(연결됨)에서 통합 상태를 확인합니다.



Cisco XDR에서 보안 엔드포인트 통합 상태

API 컨피그레이션에 오류가 없는지 확인합니다.

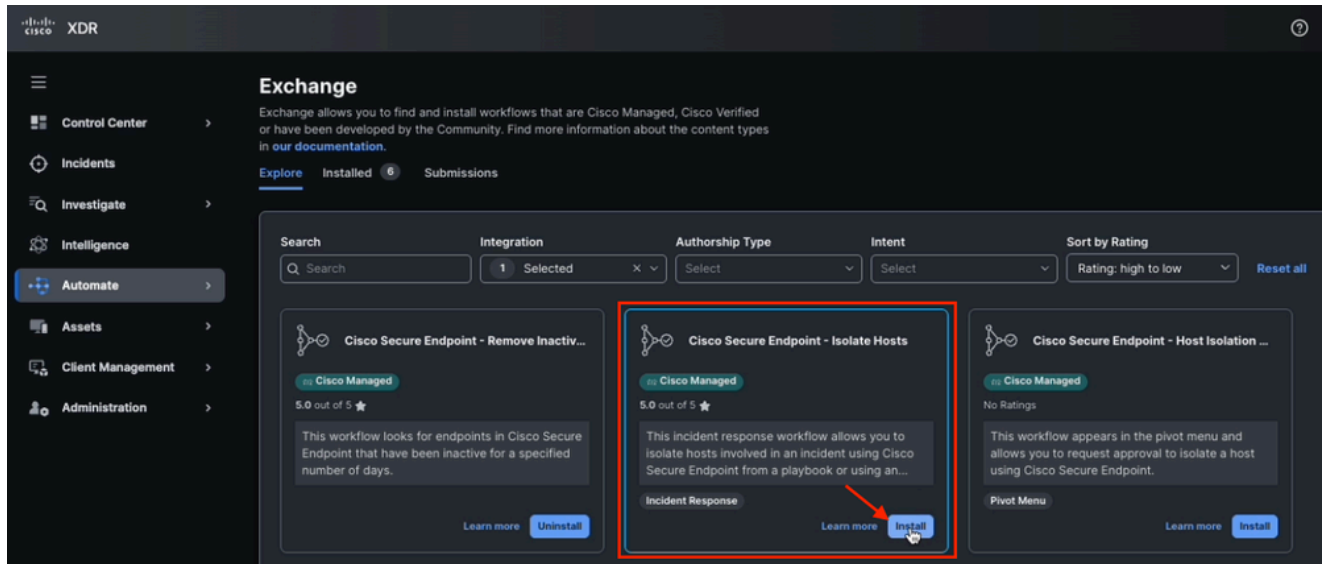


보안 엔드포인트 통합 상태 확인

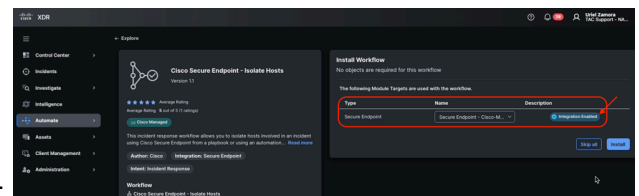
Cisco XDR Exchange에서 워크플로 설치

3.1단계: 엔드포인트 격리 워크플로 설치

1. Cisco XDR에 로그인하고 Automate(자동화) > Exchange로 이동합니다.
2. Cisco Secure Endpoint - Isolate Hosts(Cisco 보안 엔드포인트 - 호스트 격리)라는 워크플로를 검색하고 Install(설치)을 클릭합니다.



Exchange에서 호스트 워크플로 격리



3. 설치하기 전에 대상이 사용 가능한지 확인합니다.

워크플로에서 모듈 대상 사용

4. 자동화 시스템에 워크플로를 설치합니다.

자동화 규칙 만들기

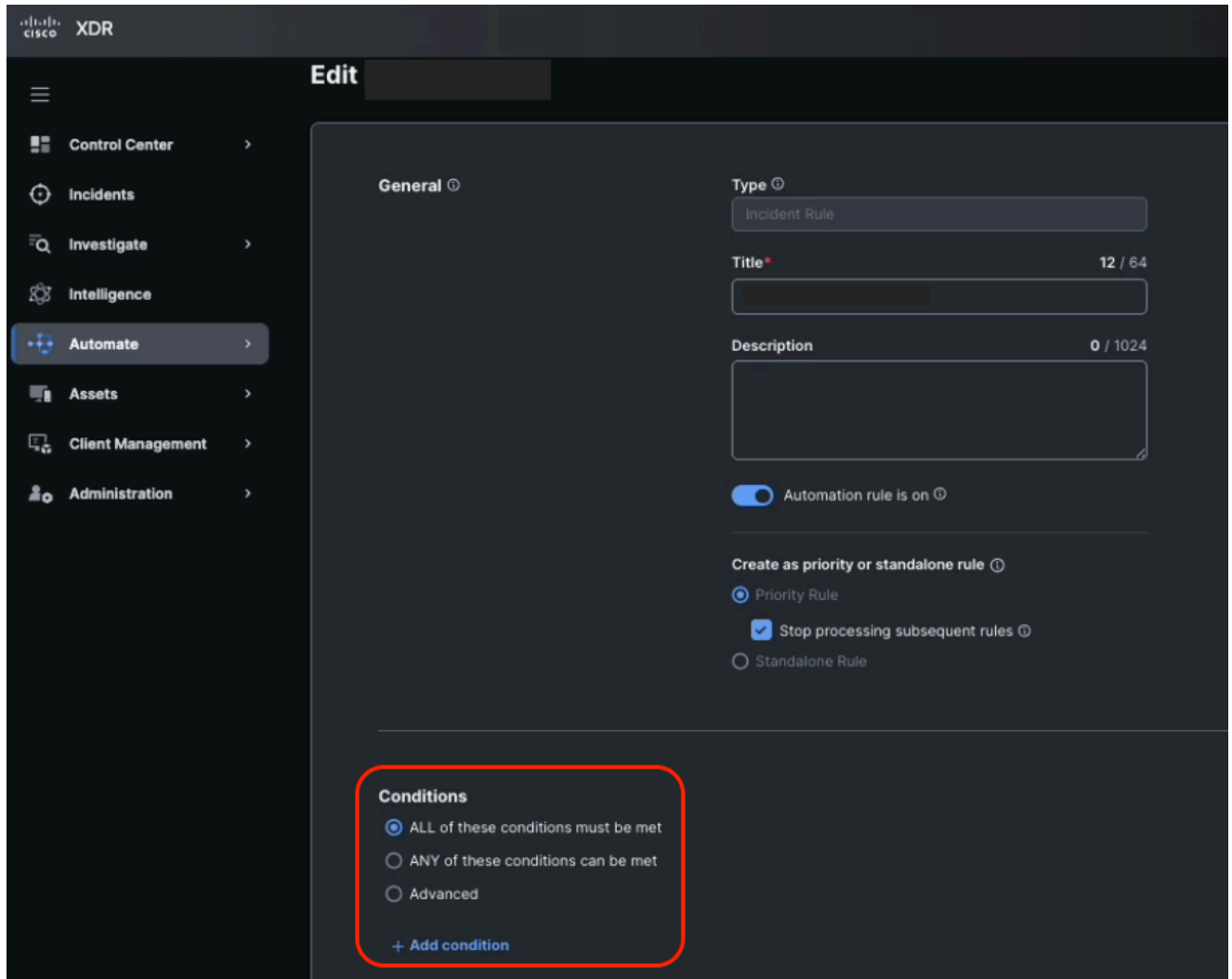
자동화 규칙은 특정 이벤트 또는 미리 정의된 일정을 기반으로 워크플로를 실행해야 하는 시기를 정의하는 구성입니다. 이러한 규칙에는 선택적 조건이 포함될 수 있으며, 그러한 조건이 충족되면 관련 워크플로가 자동으로 트리거됩니다.

4.1단계: 자동화 규칙 구성

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

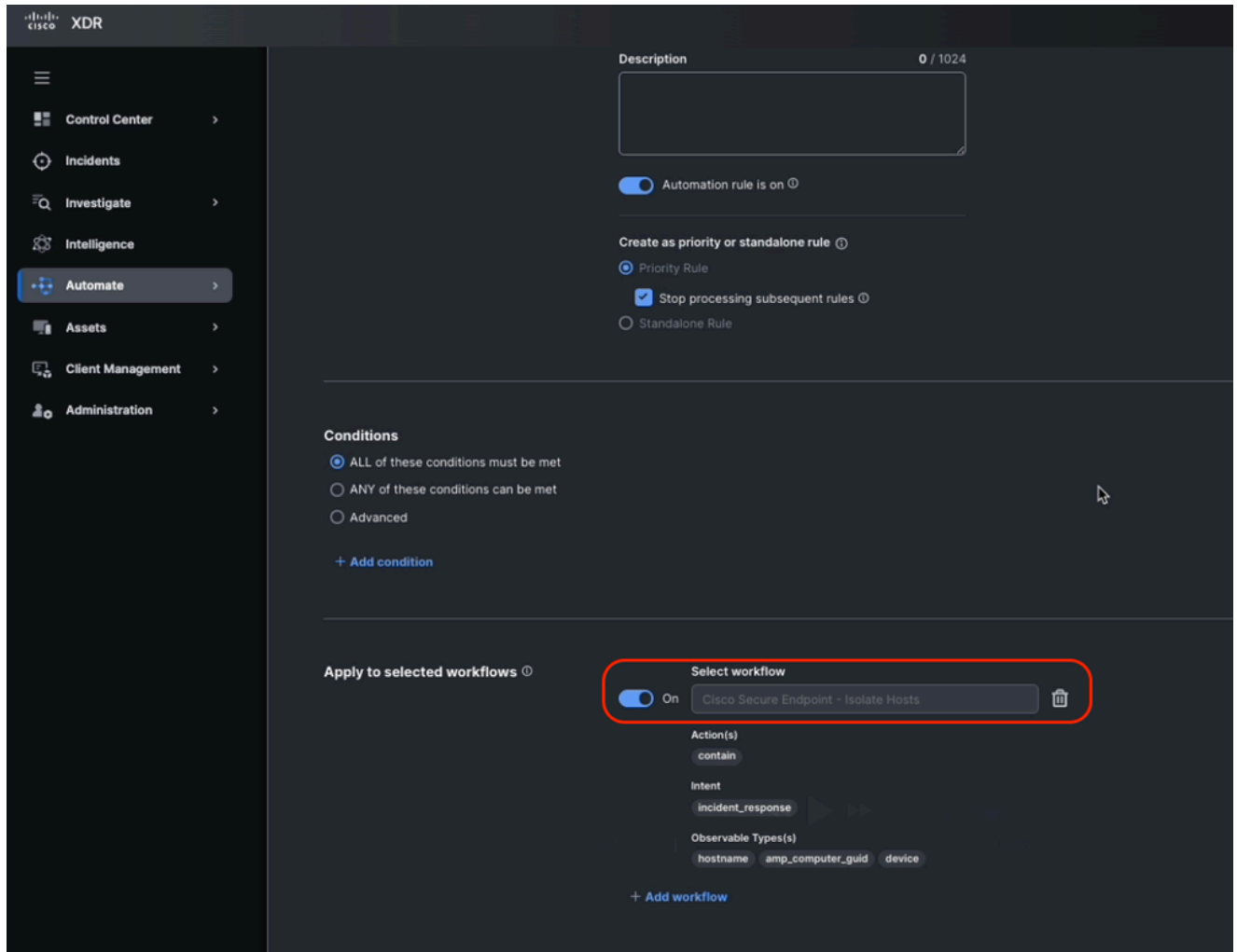
트리거에서 자동화 규칙 추가

3. 트리거 조건을 설정합니다. 조건을 비워 둘 수 있습니다. 그러면 모든 인시던트가 이 규칙을 활성화합니다. 필요한 경우 조건을 사용자 지정합니다.



자동화 규칙 조건

4. 규칙의 작업에서 이전에 설치한 Cisco Secure Endpoint - Isolate Hosts 워크플로를 선택합니다.



워크플로에 자동화 규칙 할당

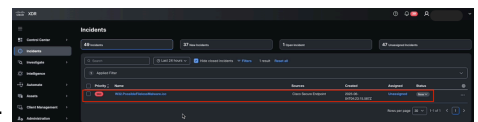
5. 저장을 클릭합니다.

워크플로 기능 검증

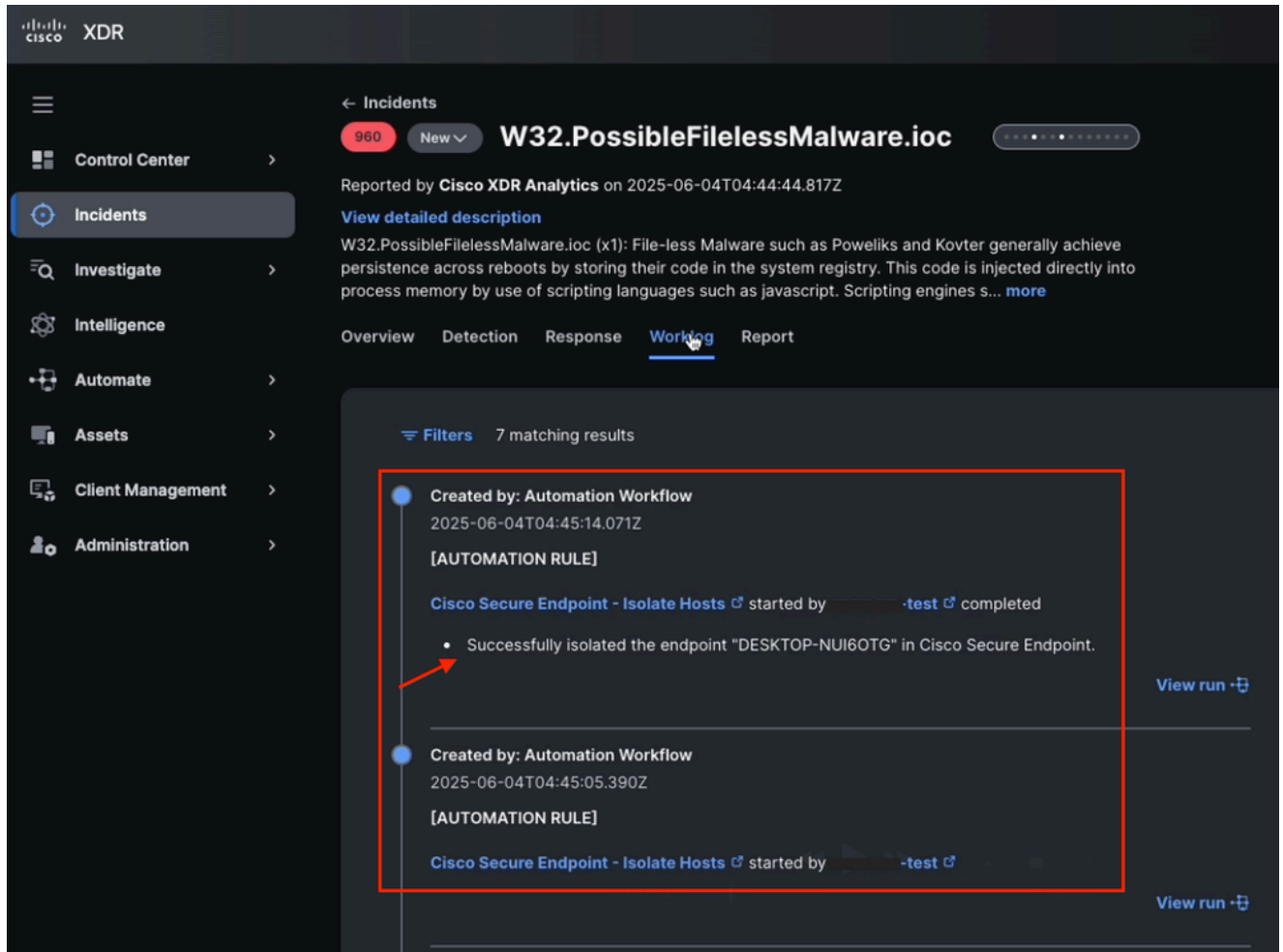
5.1단계: 워크플로 실행 확인

1. 규칙의 조건을 충족하는 인시던트를 생성하거나 기다립니다.

Cisco XDR에서 새 인시던트가 검색됨



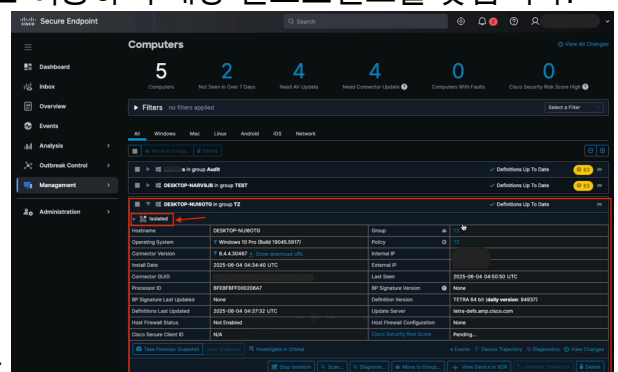
2. 인시던트가 생성되면 인시던트 내의 Worklog(작업 로그) 탭에서 워크플로가 성공적으로 실행되었는지 확인합니다.



인시던트 작업 로그 탭 정보

5.2단계: 엔드포인트 격리 확인

1. Cisco Secure Endpoint 포털에 로그인합니다.
2. Management(관리) > Computers(컴퓨터) 섹션으로 이동하여 대상 엔드포인트를 찾습니다.



3. 디바이스 상태가 Isolated(격리됨)인지 확인합니다.

보안 엔드포인트 컴퓨터로부터의 격리 상태

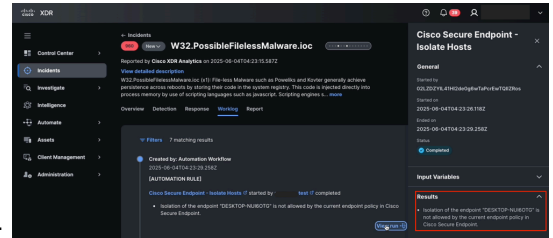
4. 엔드포인트가 격리되지 않은 경우 워크플로 로그 및 컨피그레이션을 검토하여 가능한 문제를 식별합니다.

일반적인 문제

격리 기능이 Cisco Secure Endpoint에서 활성화되지 않았습니다.

1. Cisco XDR에서 인시던트로 이동하고, 마지막 인시던트를 찾고, Worklog로 이동합니다.
2. 자동화 워크플로를 실행한 후 관련 오류가 있는지 확인합니다.

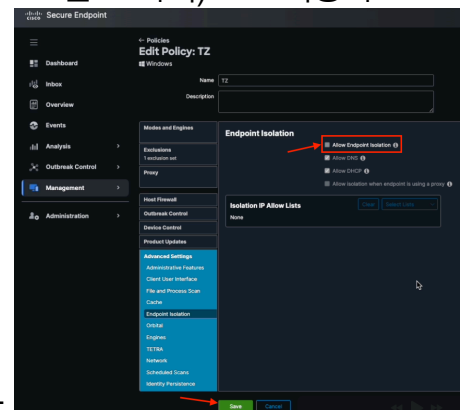
예를 들어, 보안 엔드포인트 정책에서 엔드포인트 격리가 활성화되지 않았기 때문에 엔드포인



트 격리가 호스트를 격리하는 것을 허용하지 않았습니다.

인시던트 워크로그에서 자동화 워크플로 결과

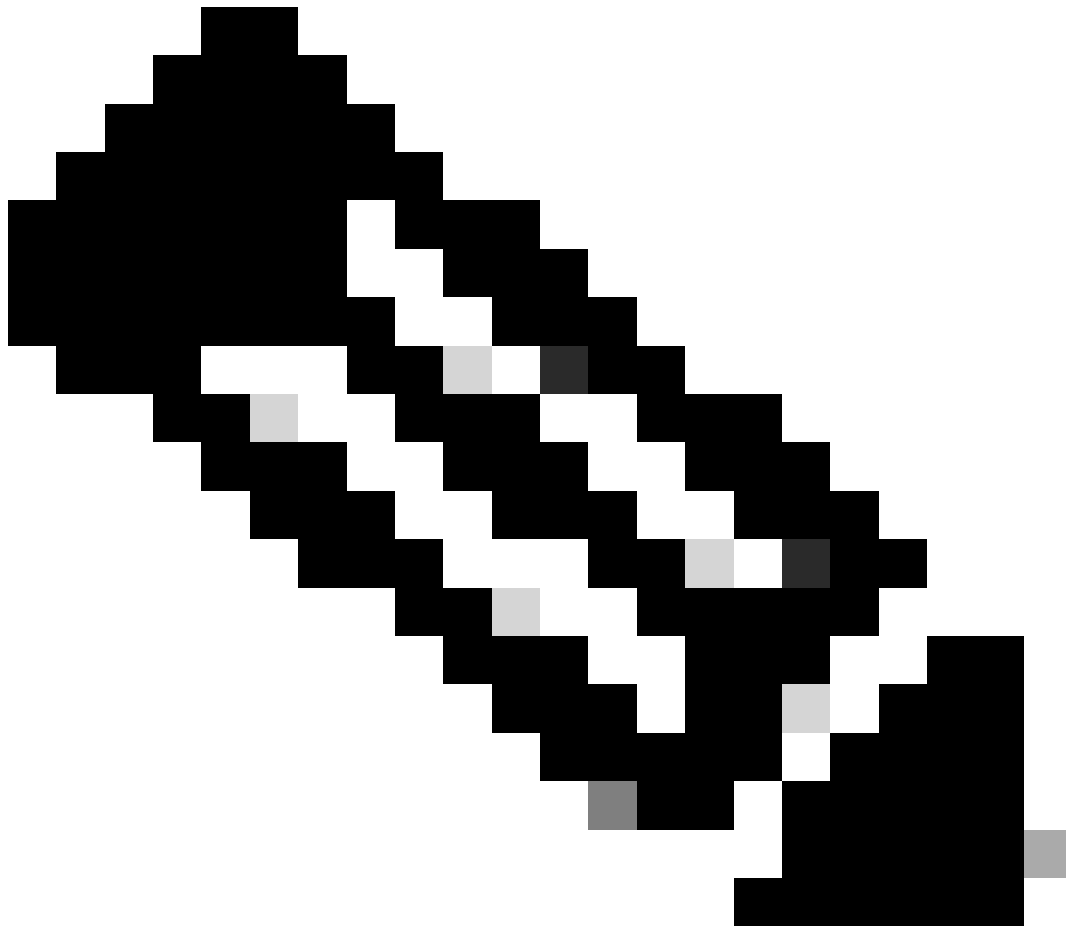
3. 보안 엔드포인트에서 관리 > 정책으로 이동하여 해당 정책을 선택합니다.
4. 정책에서 Advanced Settings(고급 설정) > Endpoint Isolation(엔드포인트 격리)으로 이동하고



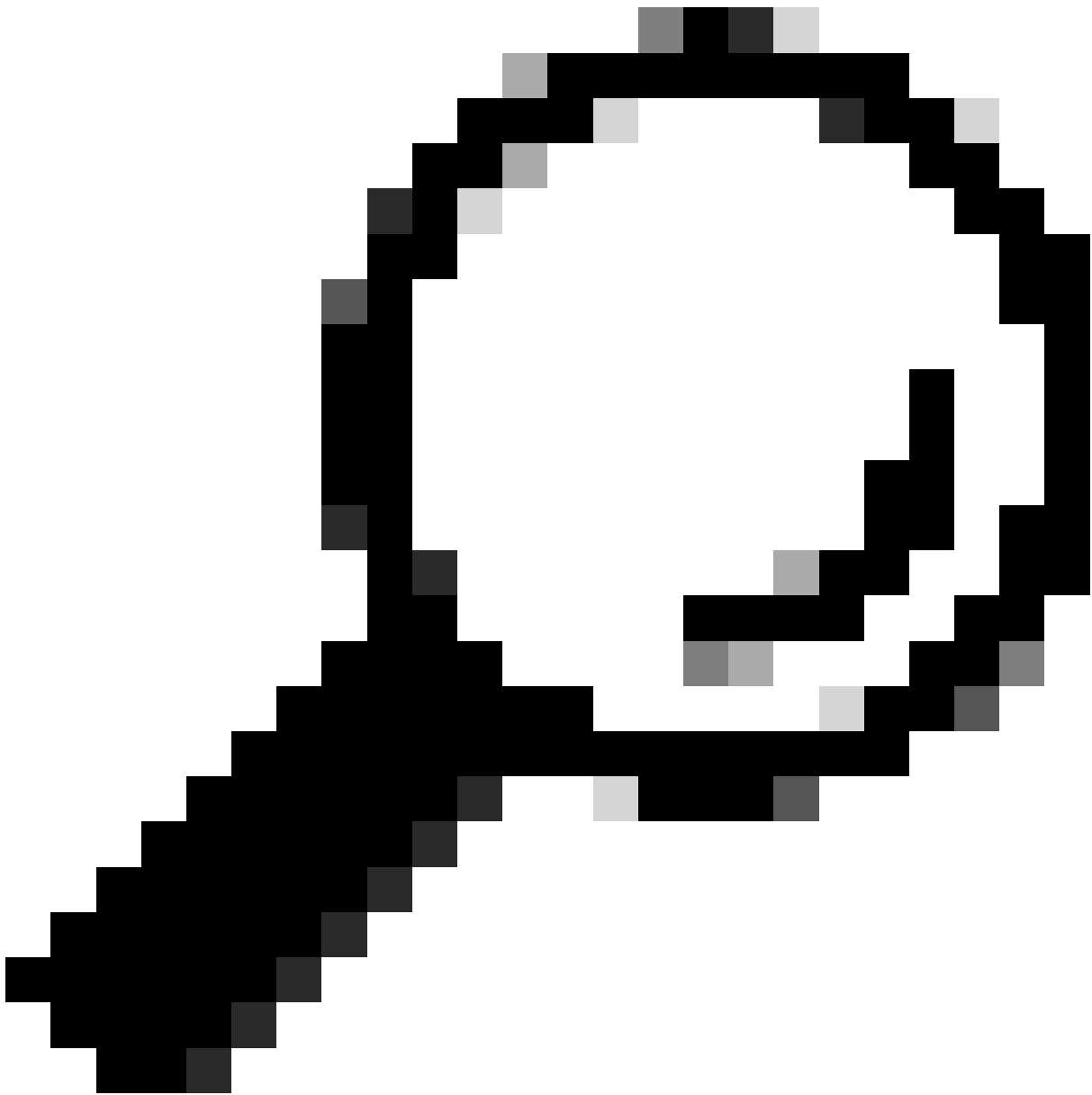
Allow Endpoint Isolation(엔드포인트 격리 허용) 상자를 선택합니다.

보안 엔드포인트 정책의 엔드포인트 격리 허용 확인란

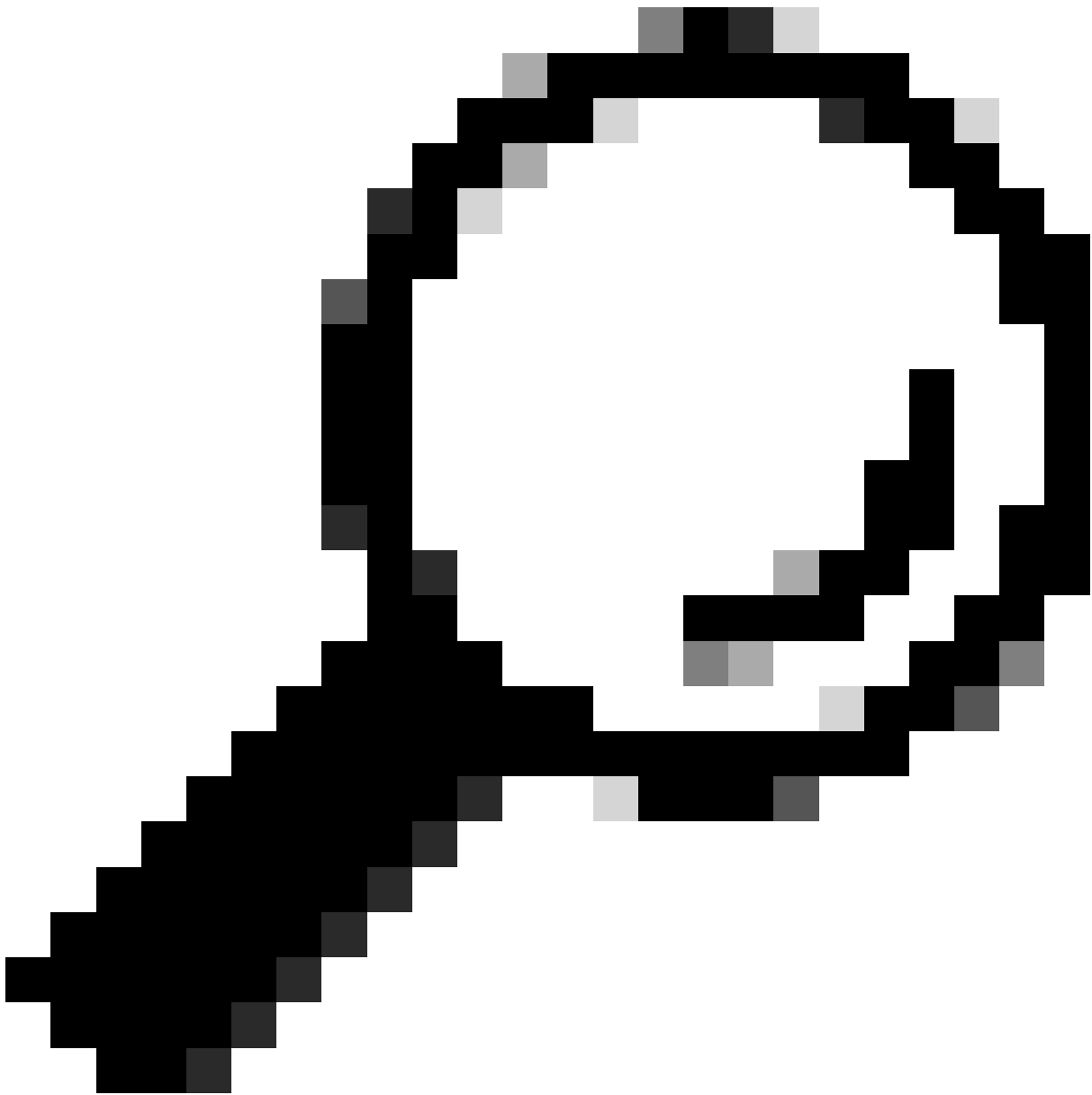
5. 저장을 클릭합니다.



참고: 통합 및 워크플로를 구성하는 데 필요한 관리 권한이 있어야 합니다.



팁: 프로덕션 환경에서 자동화를 구축하기 전에 제어된 환경에서 설정을 테스트합니다.



팁: 워크플로 또는 자동화 규칙에 대한 사용자 지정 조정을 문서화합니다.

이러한 단계가 완료되면 인시던트가 생성된 후 엔드포인트를 자동으로 격리하고 보안 위협에 신속하고 효과적으로 대응하는 워크플로를 성공적으로 구성하고 활성화할 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.