보안 엔드포인트로 격리된 파일 복구

목차

소개

이 문서에서는 Secure Endpoint Connector에서 격리된 파일을 Secure Endpoint 콘솔에서 복원하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Secure Endpoint 콘솔

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Secure Endpoint Console v5.4.2025030619

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.

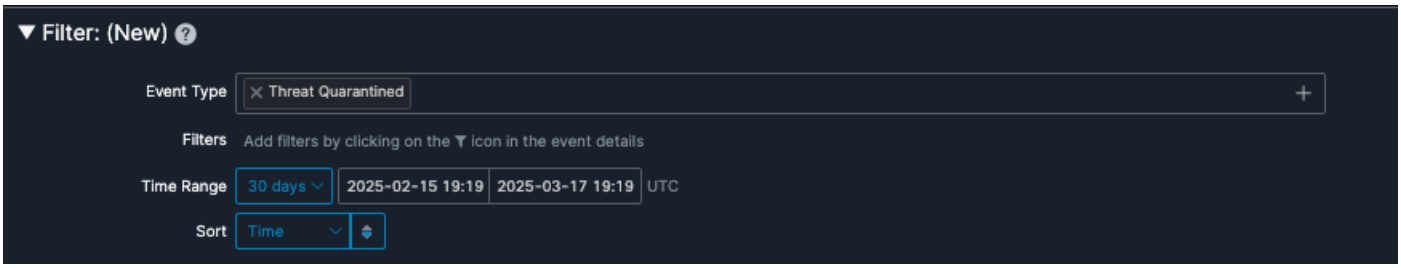
문제

SE(Secure Endpoint) 커넥터에 의해 격리된 파일은 안전한 것으로 알려진 경우 파일 분석, 오탐 제출 또는 복원을 위해 검색될 수 있습니다. 관리자는 Secure Endpoint Console에서 직접 이 작업을 수행할 수 있습니다.

솔루션

1. SE 콘솔에서 이벤트 페이지로 이동합니다.

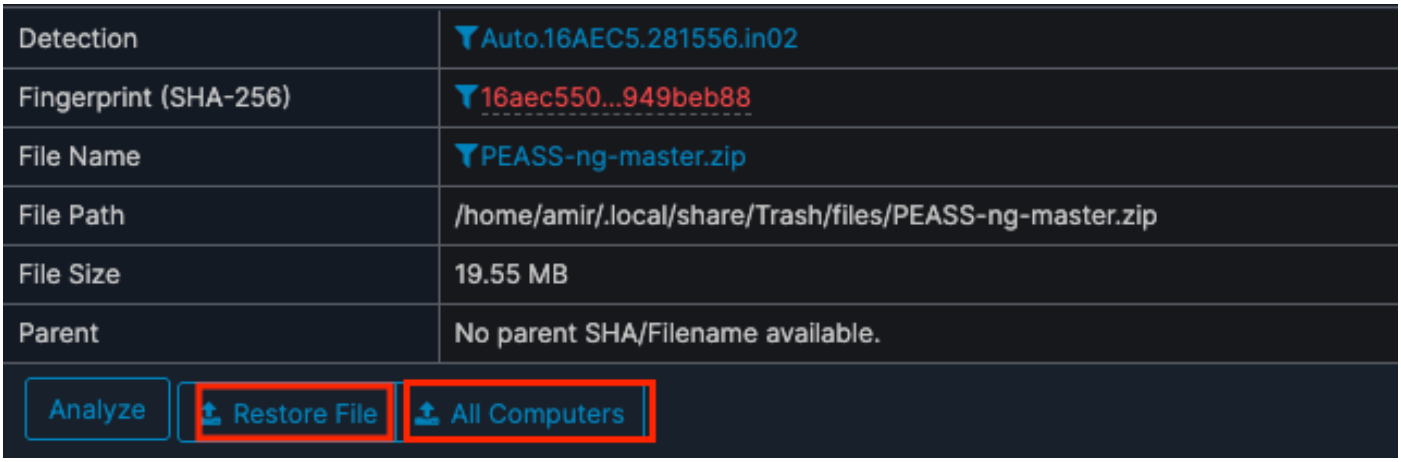
2. 이벤트 유형 = 위협 격리 필터를 선택하여 모든 성공적인 격리를 표시하도록 이벤트를 필터링합니다.



위협 격리 이벤트 유형

3. 복원해야 하는 파일과 관련된 탐지 이벤트를 식별합니다.

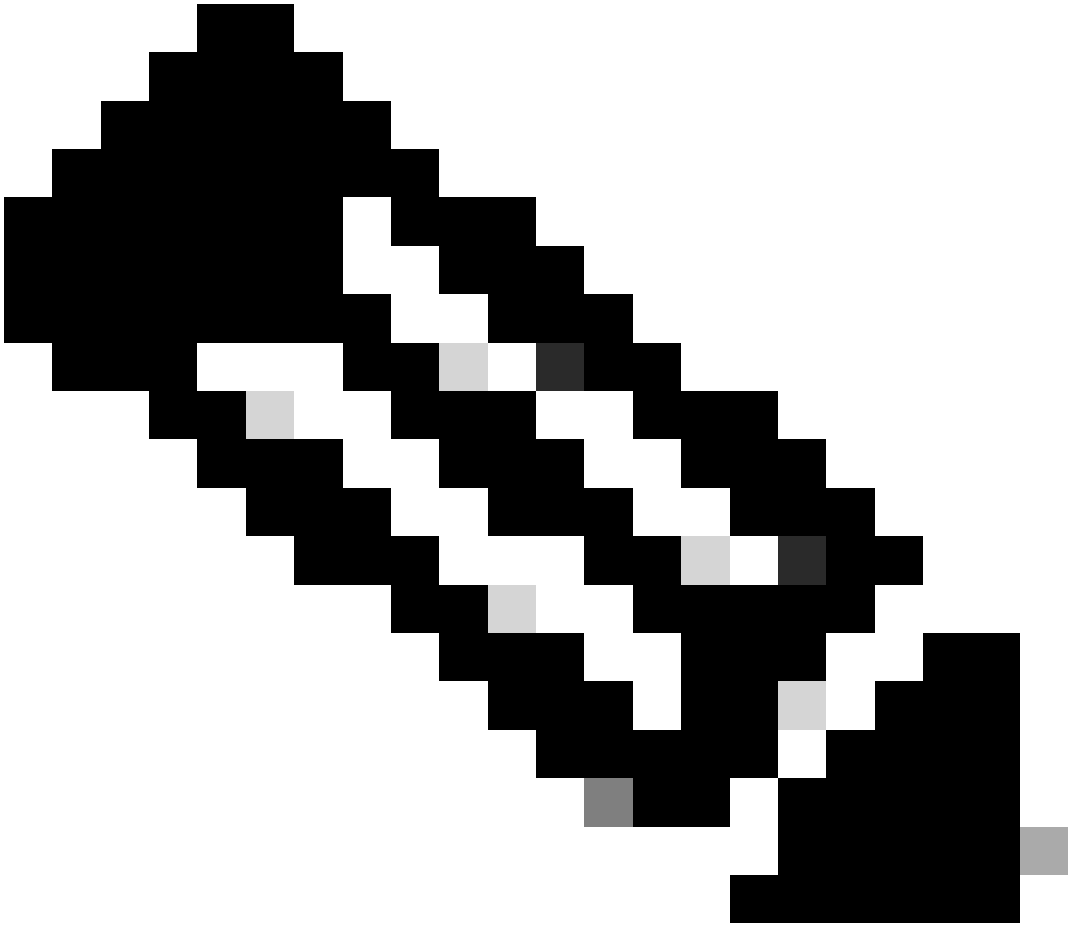
4. 이벤트 세부 정보를 확장하여 파일 복원 옵션에 액세스합니다. 파일 복원을 선택하면 영향을 받는 시스템에 파일이 복원됩니다. 모든 컴퓨터를 선택하면 파일이 격리된 모든 컴퓨터에서 파일이 복원됩니다.



복원 파일 옵션

5. 하트비트 간격은 관리자가 복원할 파일이 있는지 확인하기 위해 커넥터가 홈을 호출하는 빈도입니다. 영향을 받는 컴퓨터가 온라인 상태이거나 다음 하트비트 간격이 발생하면 파일이 복원됩니다.

6. 파일을 신뢰할 수 있는 경우 허용 목록에 추가하여 파일이 다시 격리되지 않도록 합니다.



참고: 파일은 30일 동안 또는 격리 폴더가 100MB에 도달하고 가장 오래된 파일이 삭제될 때 격리됩니다. 격리된 파일은 제거된 후 더 이상 복원할 수 없습니다.

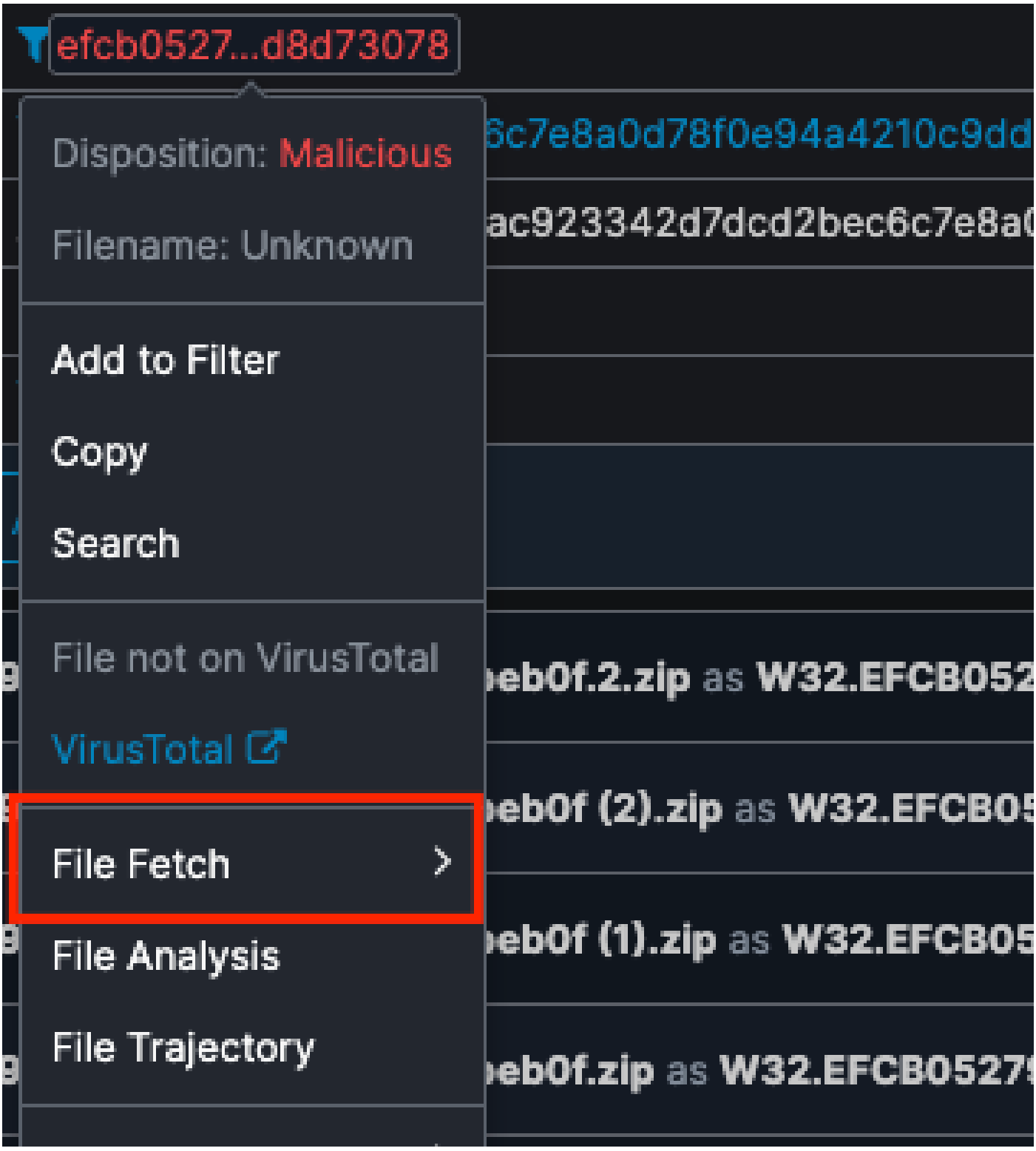
환경에 복원하지 않고 위협 분석 또는 오탐 제출을 위해 격리된 파일을 다운로드해야 하는 경우 파일 가져오기 기능을 사용할 수 있습니다. 격리된 파일 다운로드 단계:

1. SE 콘솔에서 이벤트 페이지로 이동합니다.

2. 이벤트 유형 = 위협 격리 필터를 선택하여 모든 성공적인 격리를 표시하도록 이벤트를 필터링합니다.

3. 다운로드할 파일과 관련된 탐지 이벤트를 식별합니다.

4. 격리된 파일의 SHA-256 값을 클릭하여 File Fetch(파일 가져오기) 옵션을 표시합니다.



파일 가져오기

파일 가져오기의 상태, 가져오기를 시작하는 옵션 및 파일 저장소에서 파일을 볼 수 있는 액세스 권한을 제공합니다.

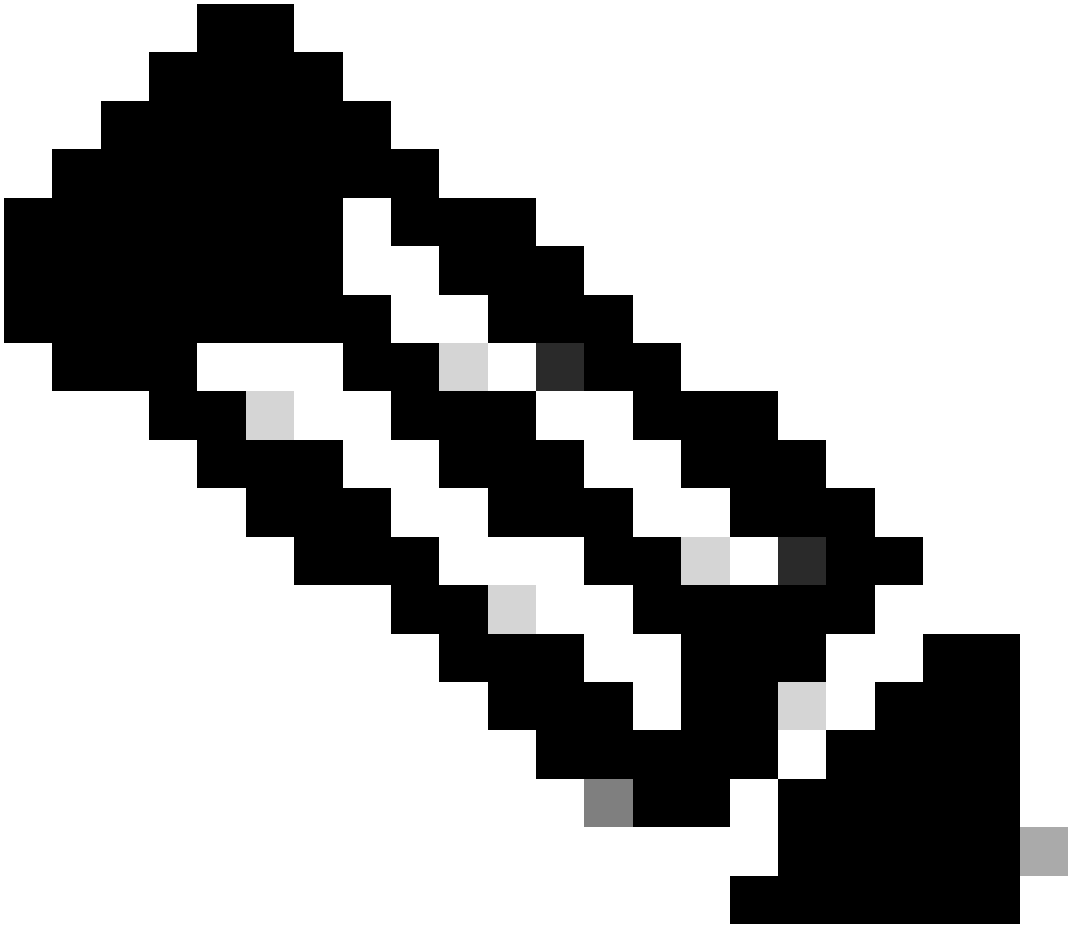
5. 파일 가져오기를 클릭하고 파일을 검색할 컴퓨터를 선택한 다음 가져오기를 클릭하여 확인합니다.

6. 파일이 파일 저장소에 업로드되면 전자 메일 알림이 전송됩니다.

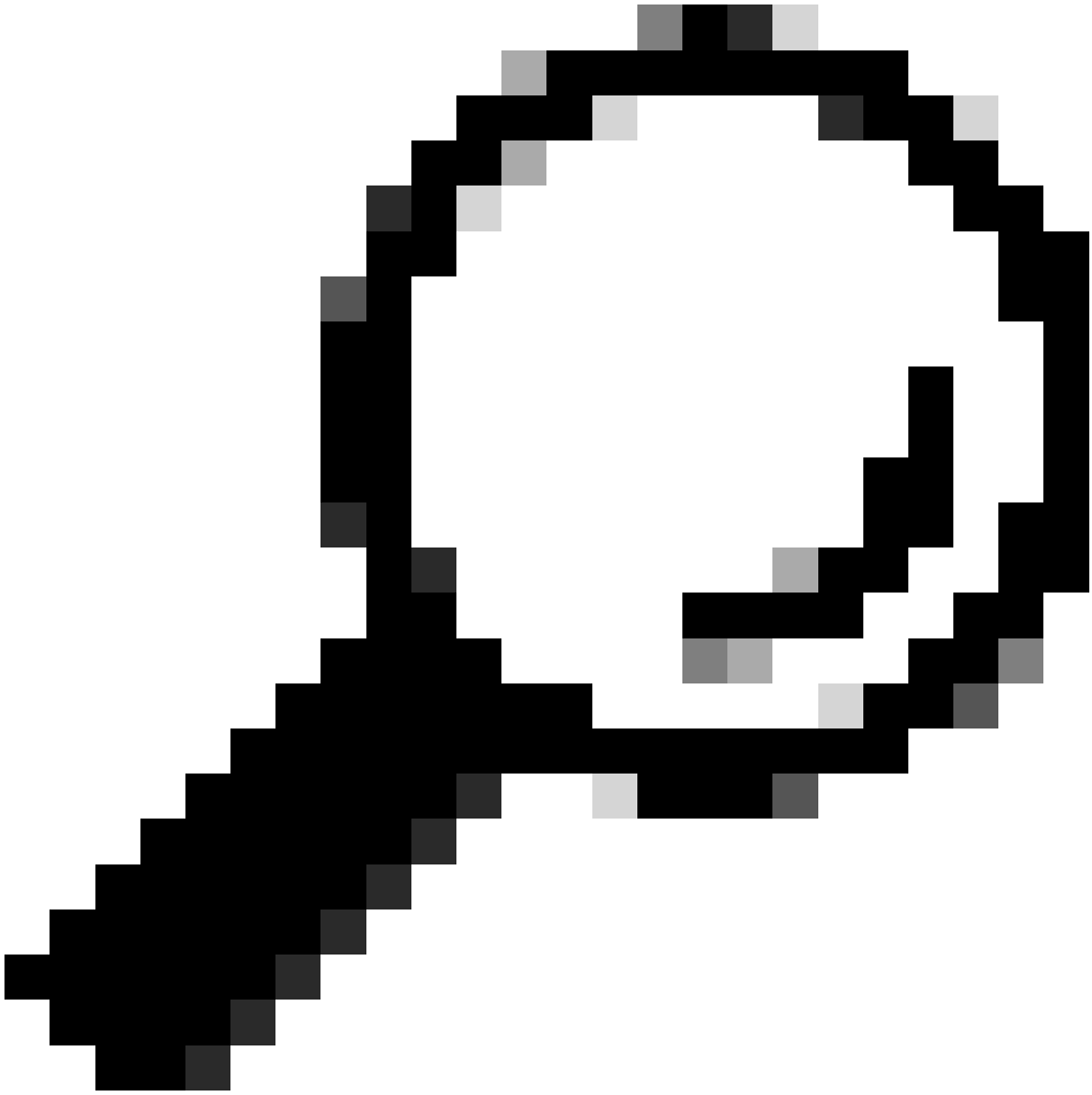
7. 파일을 사용할 수 있게 되면 Analysis> File Repository에서 파일 및 파일 다운로드 옵션을 볼 수 있습니다.

파일 다운로드

파일 저장소에서 다운로드한 모든 파일은 압축되며 비밀번호로 보호됩니다.



참고: File Fetch(파일 가져오기)가 제대로 작동하려면 클라우드 영역을 기반으로 적절한 File Fetch(파일 가져오기) 서버에 네트워크 트래픽을 허용해야 합니다. 유럽: rff.eu.amp.cisco.com 북미: rff.amp.cisco.com APJC: rff.apjc.amp.cisco.com을 참조하십시오. 또한 파일 가져오기 요청을 성공적으로 시작하는 데 필요한 경우 관리자 계정에 대해 2FA(Two-Factor Authentication)가 활성화되어 있는지 확인합니다.



팁: 이벤트 유형 = 격리된 복원 실패 및 이벤트 유형 = 파일 가져오기 실패를 사용하여 이벤트를 필터링하여 실패를 식별하고 복원 및 파일 가져오기 작업에 대한 해당 이유를 각각 검토할 수 있습니다.

설명된 단계를 사용하여 파일을 복원할 수 없는 경우 Cisco TAC에 문의하고 C:\Program Files\Cisco\AMP\Quarantine 디렉터리에 있는 .qrt 파일을 제공하십시오.

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.