Cisco Secure Endpoint Connector에서 제외 구성 및 관리

목차

소개

이 문서에서는 Cisco Secure Endpoint Console에서 여러 엔진에 대한 제외 항목을 만드는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Secure Endpoint 콘솔의 정책에 제외 목록 수정 및 적용
- Windows CSIDL 규칙

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Secure Endpoint Console 5.4.20211013
- 보안 엔드포인트 사용 설명서 2021년 10월 15일 개정판

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.

보안 엔드포인트 워크플로

상위 레벨의 작업에서 Cisco Secure Endpoint는 커넥터의 주요 구성 요소를 통해 파일 SHA(Secure Hash Algorithm)를 이 순서로 처리합니다.

- 제외
- 테트라 엔진
- 애플리케이션 제어(허용 목록/차단 목록)
- SHA 엔진
- 익스플로잇 방지(Exprev)/악의적 활동 방지(MAP)/시스템 프로세스 보호/네트워크 엔진(Device Flow Correlation)

참고: 제외 또는 허용/차단 목록 생성은 파일을 탐지한 엔진에 따라 달라집니다.

Cisco에서 유지 관리하는 제외 항목

Cisco-Maintained Exclusions는 Secure Endpoint Connector와 안티바이러스, 보안 제품 또는 기타 소프트웨어 간의 호환성을 개선하기 위해 Cisco에서 생성하고 유지 관리합니다.

이러한 제외 세트에는 올바른 작동을 보장하기 위해 다양한 유형의 제외가 포함되어 있습니다.

Cisco Secure Endpoint Console용 Cisco-Maintained Exclusion List Changes(Cisco 유지 제외 목록 변경) 문서에서 이러한 제외에 대해 수행된 변경 사항을 추적할 수 있습니다.

사용자 지정 제외

보안 엔드포인트 엔진

Tetra 및 SHA 엔진의 파일 스캔(CPU 사용량/파일 탐지):

파일의 탐지/격리를 방지하거나 Secure Endpoint의 높은 CPU를 완화하려면 이러한 제외 유형을 사용합니다.

Secure Endpoint 콘솔의 이벤트는 이미지에 표시된 것과 같습니다.

참고: CSIDL은 제외에 사용할 수 있습니다. CSIDL에 대한 자세한 내용은 이 Microsoft 문서를 참조하십시오.

경로 제외

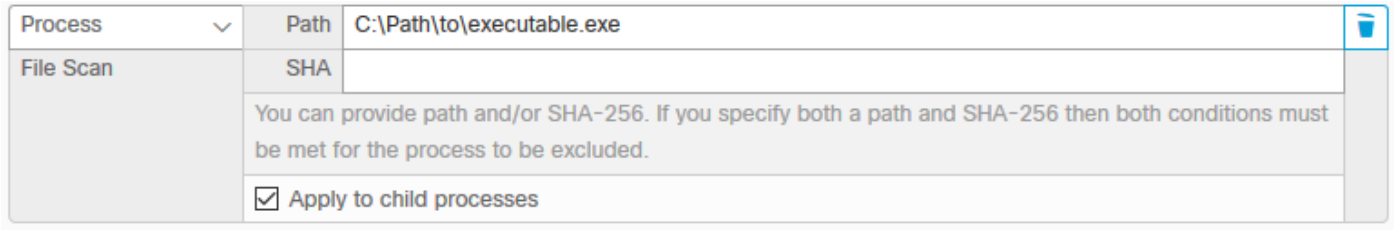
와일드카드 제외

참고: Option Apply to all drive letters(모든 드라이브 문자에 적용) 옵션은 시스템에 연결된 드라이브 [A-Z]에 제외 사항을 적용하는 데에도 사용됩니다.

파일 확장명 제외

주의: 경로 위치에 관계없이 파일 확장명을 가진 모든 파일을 검사에서 제외하므로 이 제외 유형을 신중하게 사용하십시오.

프로세스: 파일 스캔 제외

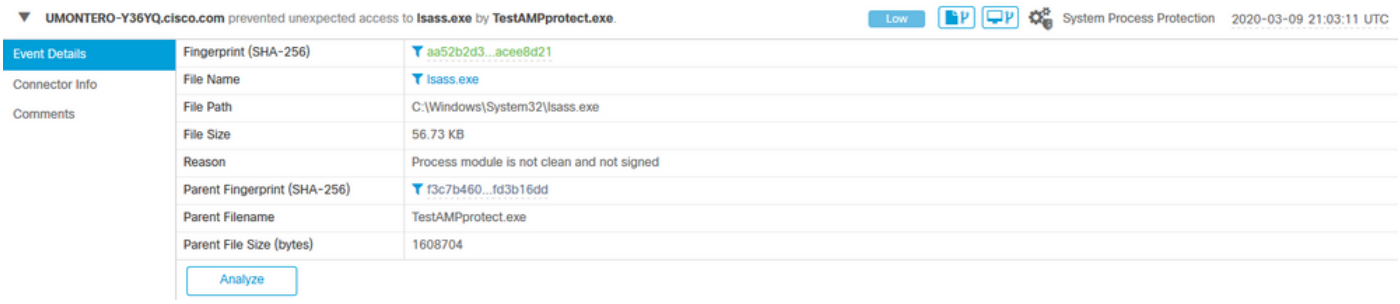


시스템 프로세스 보호(SPP)

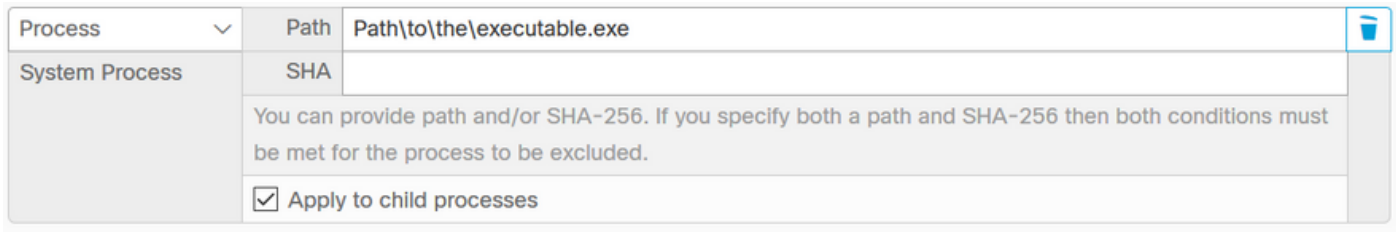
System Process Protection 엔진은 커넥터 버전 6.0.5에서 사용할 수 있으며 다음 Windows 프로세스를 보호합니다.

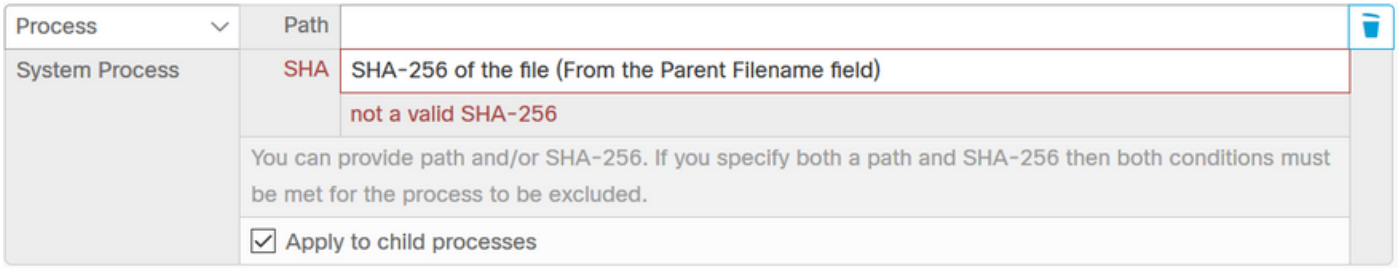
- 세션 관리자 하위 시스템(smss.exe)
- 클라이언트/서버 런타임 하위 시스템(csrss.exe)
- 로컬 보안 기관 하위 시스템(lsass.exe)
- Windows 로그온 응용 프로그램(winlogon.exe)
- Windows 시작 응용 프로그램(wininit.exe)

이 그림에서는 SPP 이벤트를 보여 줍니다.



SPP 제외

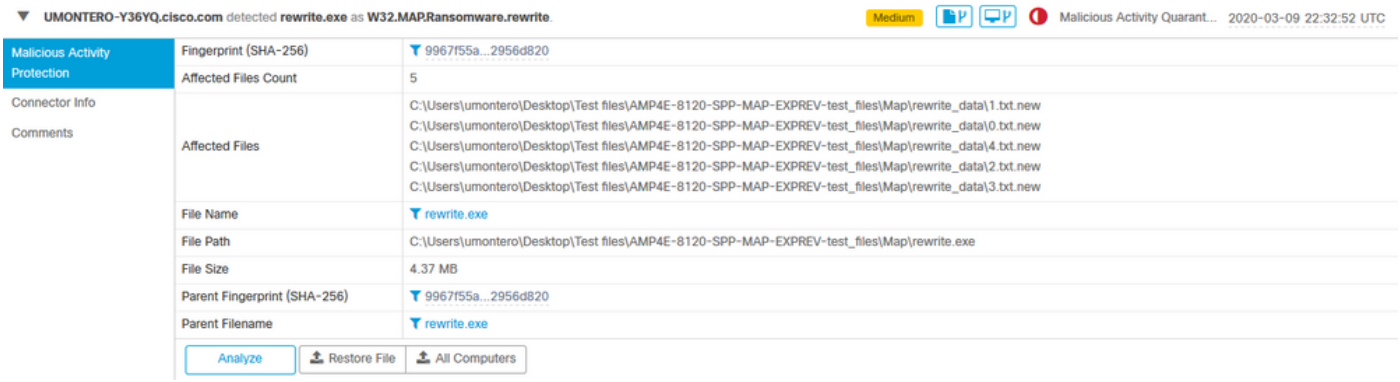




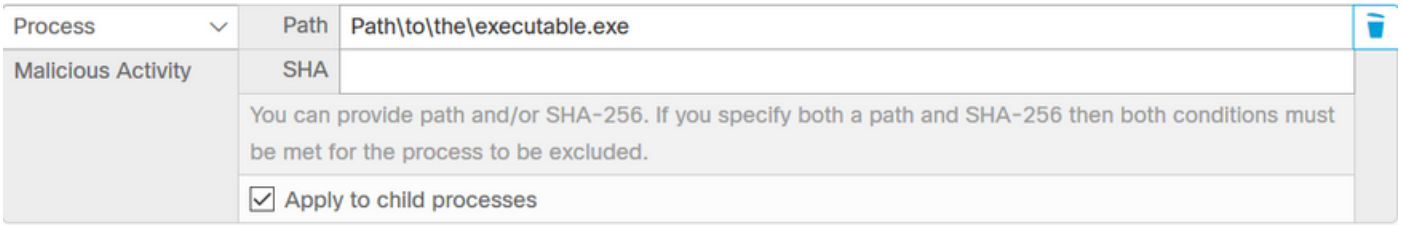
악의적인 활동 보호(MAP)

MAP(Malicious Activity Protection) 엔진을 통해 랜섬웨어 공격으로부터 엔드포인트를 보호합니다. 악의적인 작업 또는 프로세스가 실행될 때 이를 식별하고 암호화로부터 데이터를 보호합니다.

이 그림에는 MAP 이벤트가 표시되어 있습니다.



MAP 제외

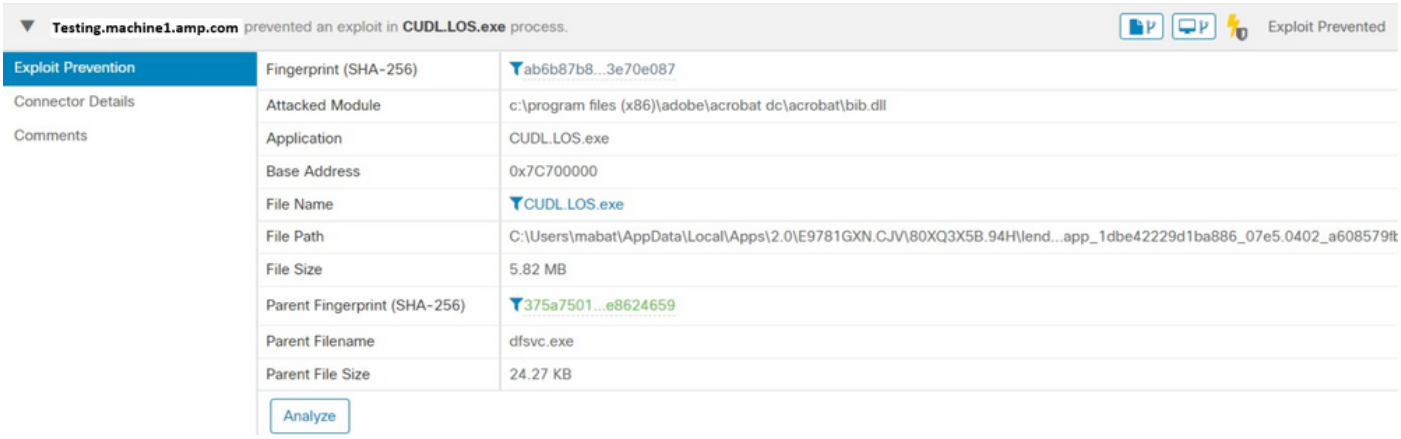


⚠ 주의: 탐지가 실제로 악성이 아님을 확인한 후에는 이 제외 유형을 신중하게 사용하십시오.

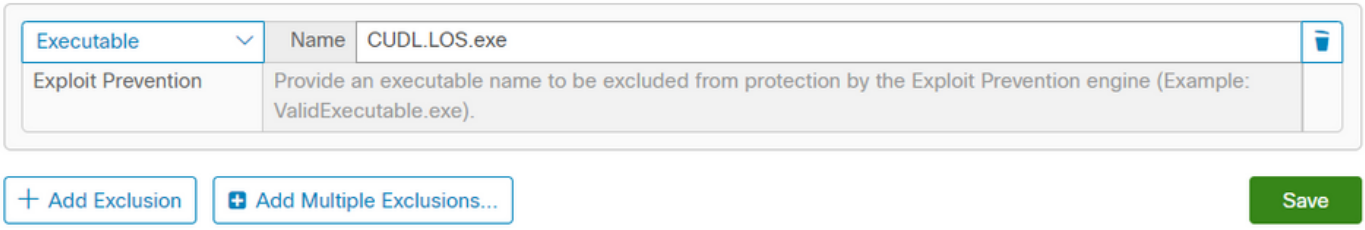
익스플로잇 방지(Exprev)

익스플로잇 방지 엔진은 악성코드가 일반적으로 사용하는 메모리 주입 공격과 패치가 적용되지 않은 소프트웨어에 대한 기타 제로 데이 공격으로부터 엔드포인트를 보호합니다
취약성. 보호된 프로세스에 대한 공격을 탐지하면 차단되고 이벤트가 생성되지만 격리는 없습니다.

이 그림에는 Exprev 이벤트가 표시되어 있습니다.



Exprev 제외

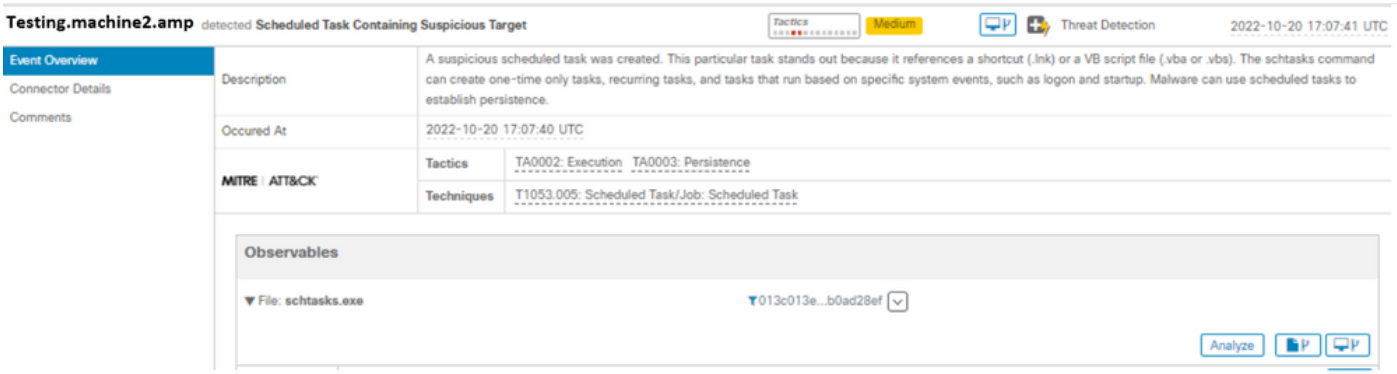


⚠ 주의: 영향을 받는 모듈/애플리케이션의 활동을 신뢰할 때마다 이 제외를 사용합니다.

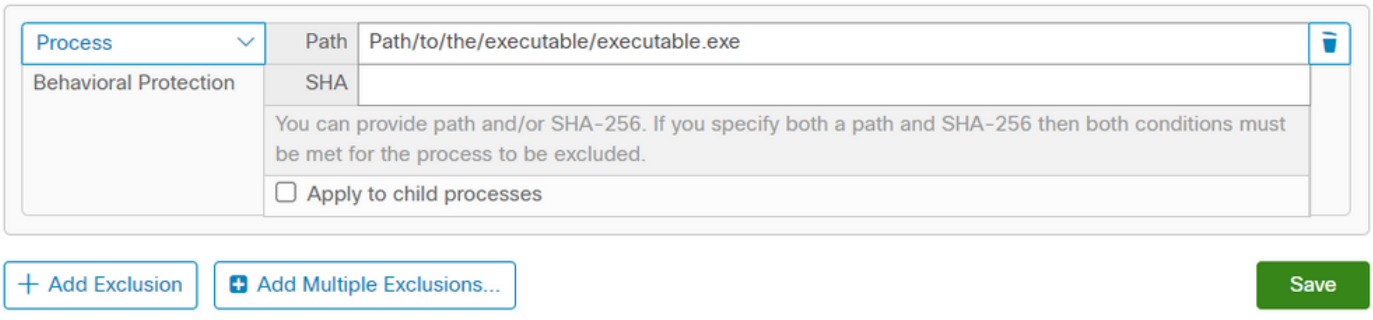
행동 보호(BP)

행동 보호 엔진은 행동 방식으로 위협을 탐지하고 차단하는 기능을 향상시킵니다. 이 솔루션은 "해외 거주" 공격을 탐지할 수 있는 기능을 강화하고
시그니처 업데이트를 통해 위협 환경의 변화에 신속하게 대응

이 그림에는 BP 이벤트가 표시되어 있습니다.



BP 제외



관련 정보

- 정책 컨피그레이션에 대한 자세한 내용은 사용 설명서로 이동합니다
- Cisco Secure Endpoint Connector 비디오에서 제외 항목 만들기
- 기술 지원 및 문서 – Cisco Systems

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.