보안 엔드포인트에서 익스플로잇 방지 문제 해결

목차

소개

이 문서에서는 Secure Endpoint Console의 Exploit Prevention 엔진 컨피그레이션 및 기본 분석 수행 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 이러한 주제에 대해 알고 있는 것이 좋습니다.

- 보안 엔드포인트 콘솔에 대한 관리자 액세스
- 보안 엔드포인트 커넥터
- 익스플로잇 방지 기능 활성화

사용되는 구성 요소

이 문서의 정보는 이러한 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Connector 버전 7.3.15 이상
- Windows 10 버전 1709 이상 또는 Windows Server 2016 버전 1709 이상

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.

배경 정보

이 문서에 설명된 절차는 콘솔에서 트리거된 이벤트를 기반으로 하는 기본 분석을 수행하는 방법에 유용하며, 프로세스를 알고 사용자 환경에서 사용할 경우 Exploit Prevention(익스플로잇 방지) 제외를 제안합니다.

Exploit Prevention 엔진은 악성코드의 메모리 주입 공격 및 패치가 적용되지 않은 소프트웨어 취약점에 대한 기타 제로 데이 공격으로부터 엔드포인트를 방어하는 기능을 제공합니다. 보호된 프로세스에 대한 공격을 탐지하면 차단되고 이벤트를 생성하지만 격리되지는 않습니다.

보호된 프로세스

익스플로잇 방지 엔진은 이러한 32비트 및 64비트(Secure Endpoint Windows 커넥터 버전 6.2.1 이상) 프로세스와 하위 프로세스를 보호합니다.

- Microsoft Excel 응용 프로그램
- Microsoft Word 응용 프로그램
- Microsoft PowerPoint 애플리케이션
- Microsoft Outlook 응용 프로그램
- Internet Explorer 브라우저
- Mozilla Firefox 브라우저
- 구글 크롬 브라우저
- Microsoft Skype 애플리케이션
- TeamViewer 응용 프로그램
- VLC 미디어 플레이어 응용 프로그램
- Microsoft Windows 스크립트 호스트
- Microsoft Powershell 애플리케이션
- Adobe Acrobat Reader 응용 프로그램
- Microsoft 등록 서버
- Microsoft 작업 스케줄러 엔진
- Microsoft Run DLL 명령
- Microsoft HTML 애플리케이션 호스트
- Windows 스크립트 호스트
- Microsoft 어셈블리 등록 도구
- 확대/축소
- 한산해
- Cisco Webex 팀
- Microsoft Teams

제외된 프로세스

다음 프로세스는 호환성 문제로 인해 익스플로잇 방지 엔진에서 제외(모니터링되지 않음)됩니다.

- McAfee DLP 서비스
- McAfee 엔드포인트 보안 유틸리티

Exploit Prevention 버전 5(Connector 버전 7.5.1 이상)

Secure Endpoint Windows 커넥터 7.5.1에는 익스플로잇 방지에 대한 중요한 업데이트가 포함되어 있습니다. 이 버전의 새로운 기능은 다음과 같습니다.

- 네트워크 드라이브 보호: 네트워크 드라이브에서 실행되는 프로세스를 랜섬웨어 같은 위협으로부터 자동으로 보호
- 원격 프로세스 보호: 도메인 인증 사용자(admin)를 사용하는 보호된 컴퓨터에서 원격으로 실행되는 프로세스를 자동으로 보호합니다.
- rundll32를 통한 AppControl 우회: 해석된 명령을 실행할 수 있도록 특별히 만들어진 rundll32 명령줄을 중지합니다.
- UAC 바이패스: 악성 프로세스에 의한 권한 에스컬레이션을 차단하여 Windows 사용자 계정 컨트롤 메커니즘이 우회하는 것을 방지합니다.
- 브라우저/Mimikatz 자격 증명 모음: 활성화된 경우 Exploit Prevention은 Microsoft Internet Explorer 및 Edge 브라우저에서 자격 증명 도용을 방지합니다
- 섀도 복제본 삭제: 섀도 복사본의 삭제를 추적하고 Microsoft Volume Shadow Copy Service(vssvc.exe)에서 COM API를 인터셉트합니다.
- SAM 해시: Mimikatz에 의한 SAM 해시 자격 증명 도용을 방지하고, 레지스트리 하이브 Computer\HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users에 있는 모든 SAM 해시를 열거하고 해독하는 시도를 **가로챕니다.**

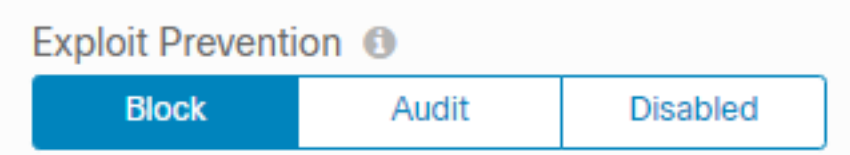
- 실행된 프로세스 보호: Exploit Prevention 인스턴스(explorer.exe, lsass.exe, spoolsv.exe, winlogon.exe) 전에 시작된 경우 실행되는 프로세스에 삽입합니다.

이러한 기능은 정책에서 Exploit Prevention이 활성화된 경우 기본적으로 모두 활성화됩니다.

설정

Exploit Prevention 엔진을 활성화하려면, 이미지에 표시된 것처럼 정책에서 **Modes and Engines(모드 및 엔진)**로 이동하여 Audit mode(감사 모드), Block mode(차단 모드) 또는 Disabled mode(비활성화 모드)를 선택합니다.

> **참고:** 감사 모드는 Secure Endpoint Windows 커넥터 7.3.1 이상에서만 사용할 수 있습니다. 이전 버전의 커넥터는 감사 모드를 차단 모드와 동일하게 취급합니다.

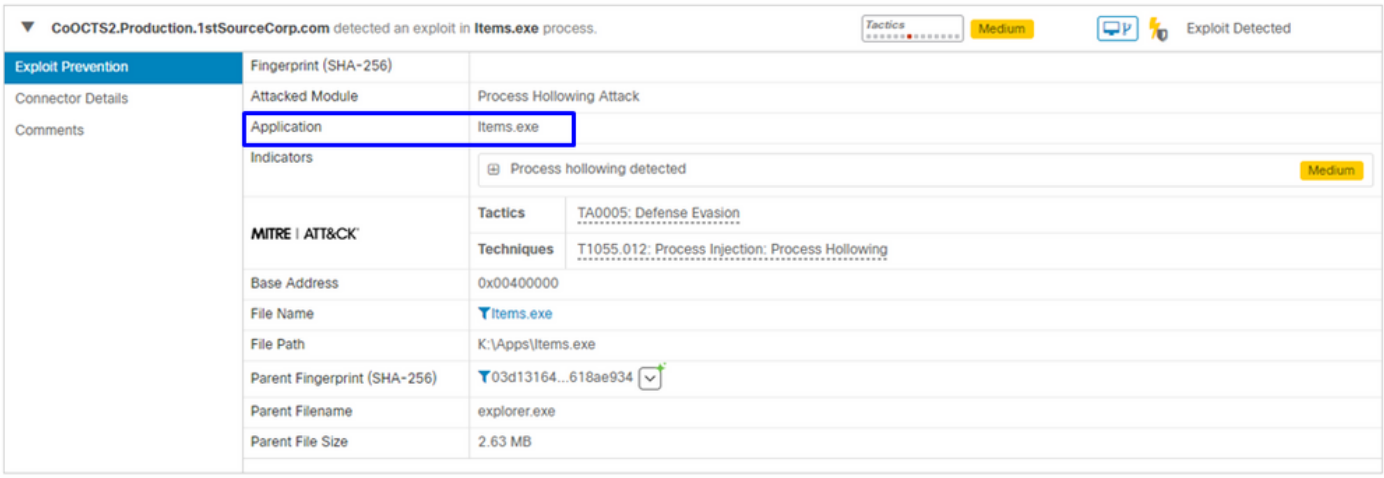


> **참고:** Windows 7 및 Windows Server 2008 R2에서는 커넥터를 설치하기 전에 Microsoft Security Advisory 3033929용 패치를 적용해야 합니다.

탐지

탐지가 트리거되면 이미지에 표시된 것처럼 엔드포인트에 팝업 알림이 표시됩니다.

콘솔은 이미지에 표시된 대로 익스플로잇 방지 이벤트를 표시합니다.

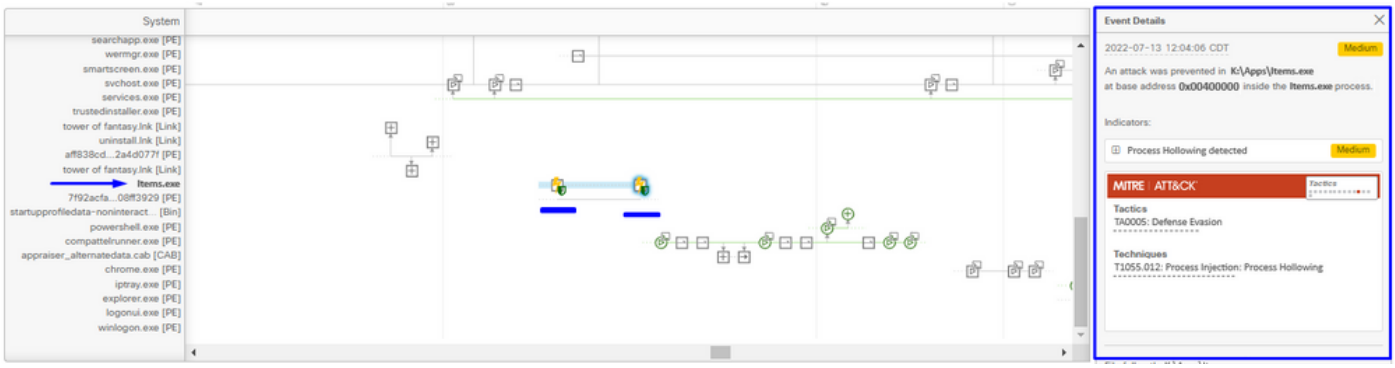


문제 해결

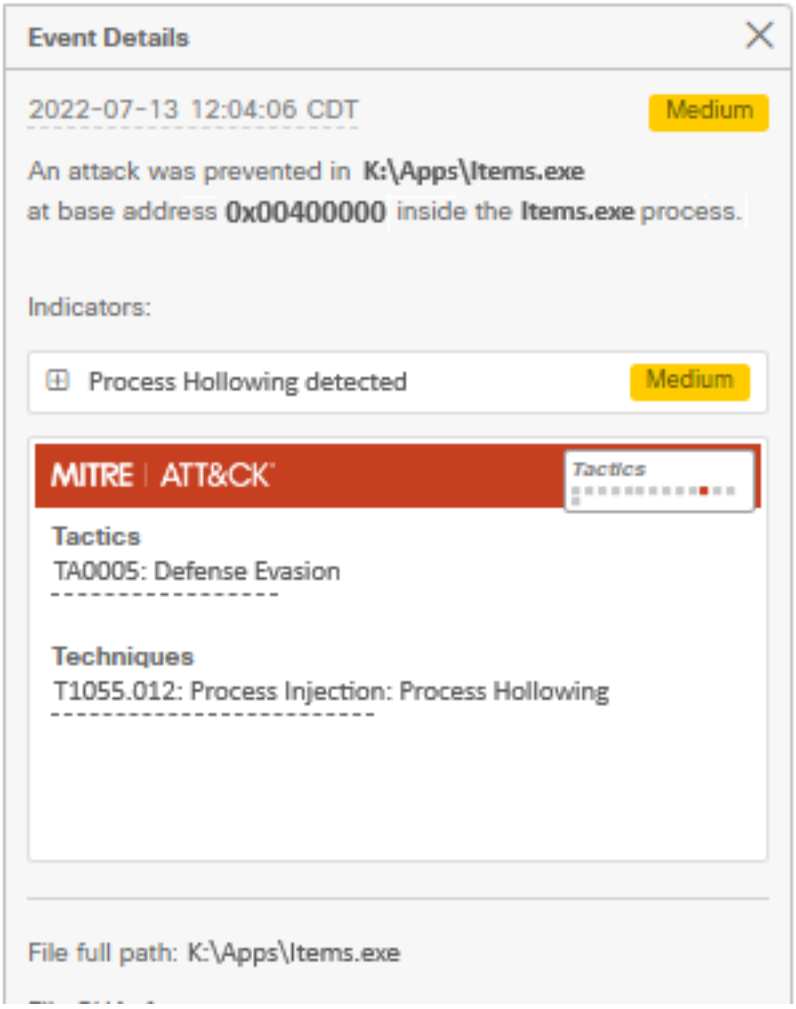
콘솔에서 Exploit Prevention(익스플로잇 방지) 이벤트가 트리거되면 탐지된 프로세스를 식별하는 방법은 애플리케이션 또는 프로세스가 실행되는 동안 발생한 이벤트에 대한 가시성을 제공하기 위한 세부 정보를 기반으로 하며, **Device Trajectory(디바이스 전파 흔적 분석)**로 이동할 수 있습니다.

1단계. 이미지에 표시된 대로 **Exploit** Prevention 이벤트에 나타나는 Device Trajectory(디바이스 전파 흔적 분석) 아이콘을 클릭합니다.

2단계. Event Details(**이벤트 세부** 정보) 섹션을 보려면 Device Trajectory(디바이스 전파 흔적 분석)의 타임라인에서 Exploit Prevention(익스플로잇 방지) 아이콘을 찾습니다(이미지 참조).



3단계. 이벤트의 세부사항을 확인하고 프로세스 또는 애플리케이션이 사용자 환경에서 신뢰/알려져 있는지 평가합니다.



오탐 감지

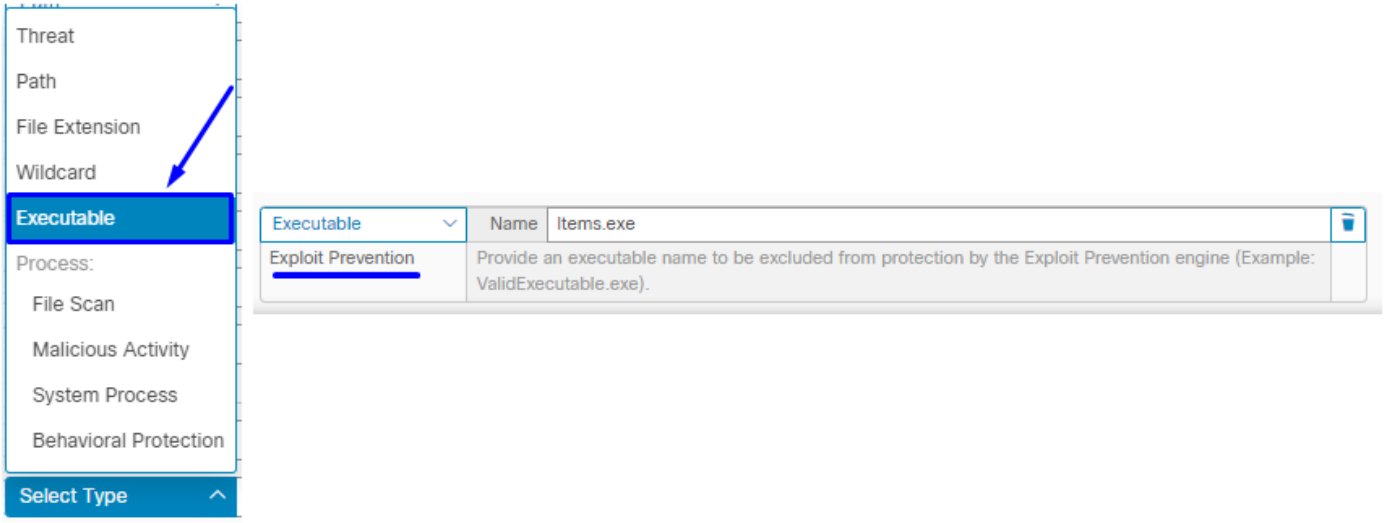
탐지가 식별되고 프로세스/실행 파일이 환경에 의해 신뢰되고 알려지면 제외로 추가할 수 있습니다. 커넥터가 스캔되는 것을 방지하기 위해서입니다.

실행 파일 제외는 익스플로잇 방지(커넥터 버전 6.0.5 이상)가 활성화된 커넥터에만 적용됩니다. 실행 파일 제외는 익스플로잇 방지 엔진에서 특정 실행 파일을 제외하는 데 사용됩니다.

> **주의**: exe 이외의 와일드카드 및 확장명은 지원되지 않습니다.

Protected Processes(보호된 프로세스) 목록을 확인하고 Exploit Prevention 엔진에서 any(모두)를 제외할 수 있습니다. application exclusion(애플리케이션 제외) 필드에 실행 파일 이름을 지정해야 합니다. 엔진에서 모든 애플리케이션을 제외할 수도 있습니다. 실행 파일 제외는 그림과 같이 name.**exe 형식**의 실행 파일 이름과 정확히 일치해야 합니다.

> **참고:** 익스플로잇 방지에서 제외하는 모든 실행 파일은 제외가 커넥터에 적용된 후 다시 시작해야 합니다. 또한 Exploit Prevention(익스플로잇 방지)을 비활성화하는 경우 활성 상태인 보호된 프로세스를 다시 시작해야 합니다.



참고: 제외 세트가 영향을 받는 커넥터에 적용된 정책에 추가되었는지 확인합니다.

마지막으로 동작을 모니터링할 수 있습니다.

익스플로잇 방지 탐지가 지속될 경우, 심층 분석을 수행하려면 TAC 지원에 문의하십시오. 여기에서 필요한 정보를 찾을 수 있습니다.

- 익스플로잇 방지 이벤트의 스크린샷
- 디바이스 전파 흔적 분석 및 이벤트 세부 정보 스크린샷
- 영향을 받는 애플리케이션/프로세스의 SHA256
- 익스플로잇 방지 기능이 비활성화된 상태에서 문제가 발생합니까?
- 보안 엔드포인트 커넥터 서비스가 비활성화된 상태에서 문제가 발생합니까?
- 엔드포인트에 다른 보안 또는 안티바이러스 소프트웨어가 있습니까?
- 영향을 받는 애플리케이션은 무엇입니까? 기능 설명
- 문제가 발생할 때 디버그 모드가 활성화된 진단 파일(디버그 번들 로그)(이 문서에서 진단 파일을 수집하는 방법을 찾을 수 있음)

관련 정보

- 보안 엔드포인트 사용 설명서
- 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.