보안 엔드포인트 제외 구성 및 식별

목차

소개

이 문서에서는 제외의 정의, 제외를 식별하는 방법 및 Cisco Secure Endpoint에서 제외를 생성하기 위한 모범 사례에 대해 설명합니다.

면책조항

이 문서의 정보는 Windows, Linux 및 macOS 운영 체제를 기반으로 합니다.

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.

개요

이 문서를 읽은 후에는 다음을 이해해야 합니다.

- 제외란 무엇이며 Cisco Secure Endpoint에서 사용할 수 있는 여러 유형의 제외입니다.
- 제외 조정을 위해 커넥터를 준비하는 방법.
- 잠재적으로 강력한 제외를 식별하는 방법.
- Cisco Secure Endpoint Console에서 새 제외를 생성하는 방법.
- 제외 항목을 만드는 모범 사례는 무엇입니까?

제외란 무엇입니까?

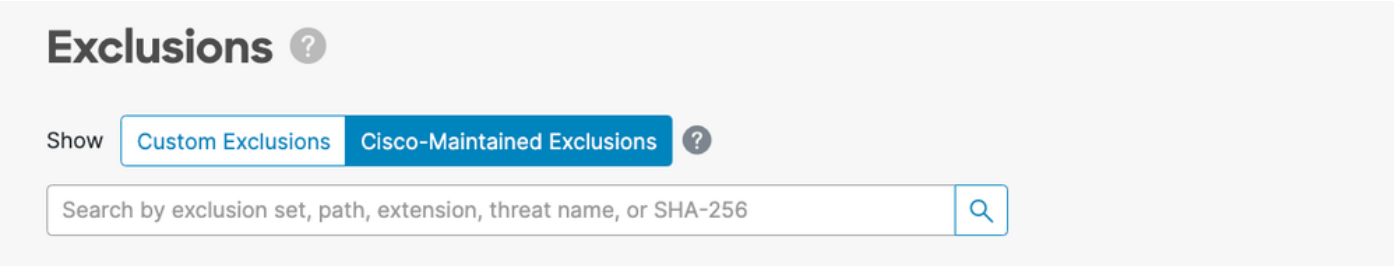
제외 세트는 커넥터가 검사하거나 확인하지 않도록 할 디렉토리, 파일 확장명, 파일 경로, 프로세스, 위협 이름, 애플리케이션 또는 보안 침해 지표의 목록입니다. 보안 엔드포인트와 같은 엔드포인트 보호가 활성화된 경우 컴퓨터에서 성능과 보안의 균형을 유지하기 위해 제외를 신중하게 만들어야 합니다. 이 문서에서는 Secure Endpoint Cloud, TETRA, SPP 및 MAP의 제외 사항에 대해 설명합니다.

모든 환경은 고유할 뿐만 아니라 이를 제어하는 엔티티가 있으며, 이는 엄격한 정책부터 개방형 정책까지 다양합니다. 이처럼 제외는 각 상황에 고유하게 맞춰져야 합니다.

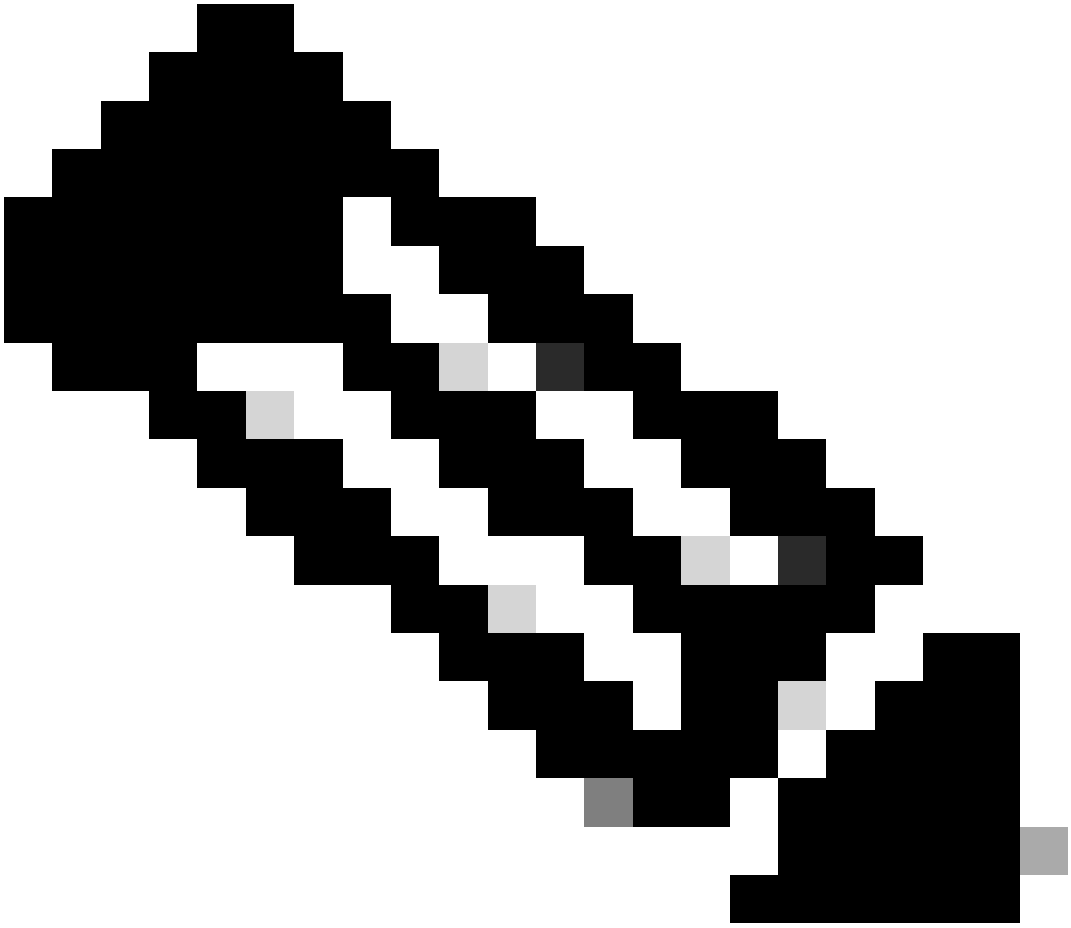
제외는 Cisco-Maintained Exclusions(Cisco-유지 제외) 및 Custom Exclusions(사용자 지정 제외)의 두 가지 방법으로 분류할 수 있습니다.

Cisco에서 유지 관리하는 제외

Cisco-Maintained Exclusions(Cisco 유지 관리 제외)는 연구를 기반으로 생성되었으며 일반적으로 사용되는 운영 체제, 프로그램 및 기타 보안 소프트웨어에 대한 엄격한 테스트를 거친 제외 항목입니다. 이러한 제외는 Exclusions(제외) 페이지의 Secure Endpoint Console에서 `Cisco-Maintained Exclusions`(`Cisco 유지 제외`)를 선택하여 `표시할` 수 있습니다.



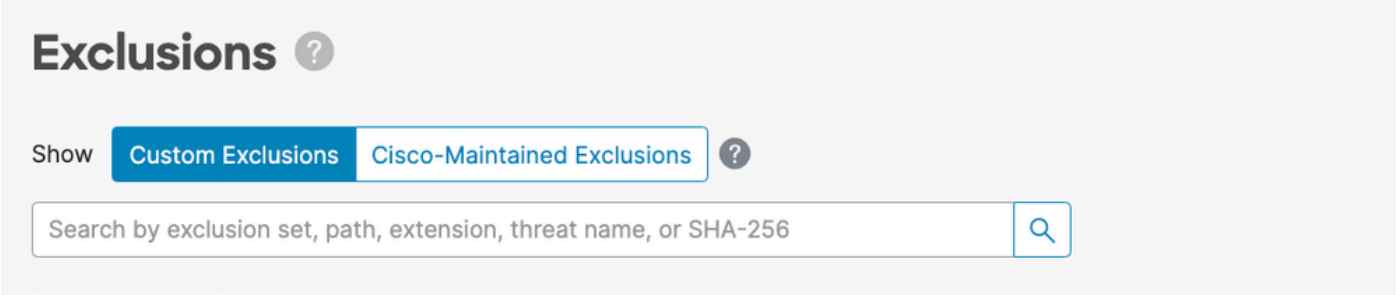
Cisco는 AV(Anti-Virus) 공급업체가 게시한 권장 제외 목록을 모니터링하고 Cisco-Maintained Exclusions에 권장 제외가 포함되도록 업데이트합니다.



참고: 일부 AV 벤더는 권장 제외 항목을 게시하지 않을 수 있습니다. 이 경우 고객은 AV 벤더에 연락하여 권장 제외 목록을 요청한 다음 지원 케이스를 열어 Cisco에서 관리하는 제외 항목을 업데이트해야 할 수 있습니다.

사용자 지정 제외

Custom Exclusions(맞춤형 제외)는 엔드포인트에서 맞춤형 활용 사례에 대해 사용자가 생성한 제외입니다. 이러한 제외는 Exclusions(제외) 페이지의 Secure Endpoint Console(보안 엔드포인트 콘솔)에서 Custom Exclusions(맞춤형 제외)를 선택하여 표시할 수 있습니다.



제외 유형

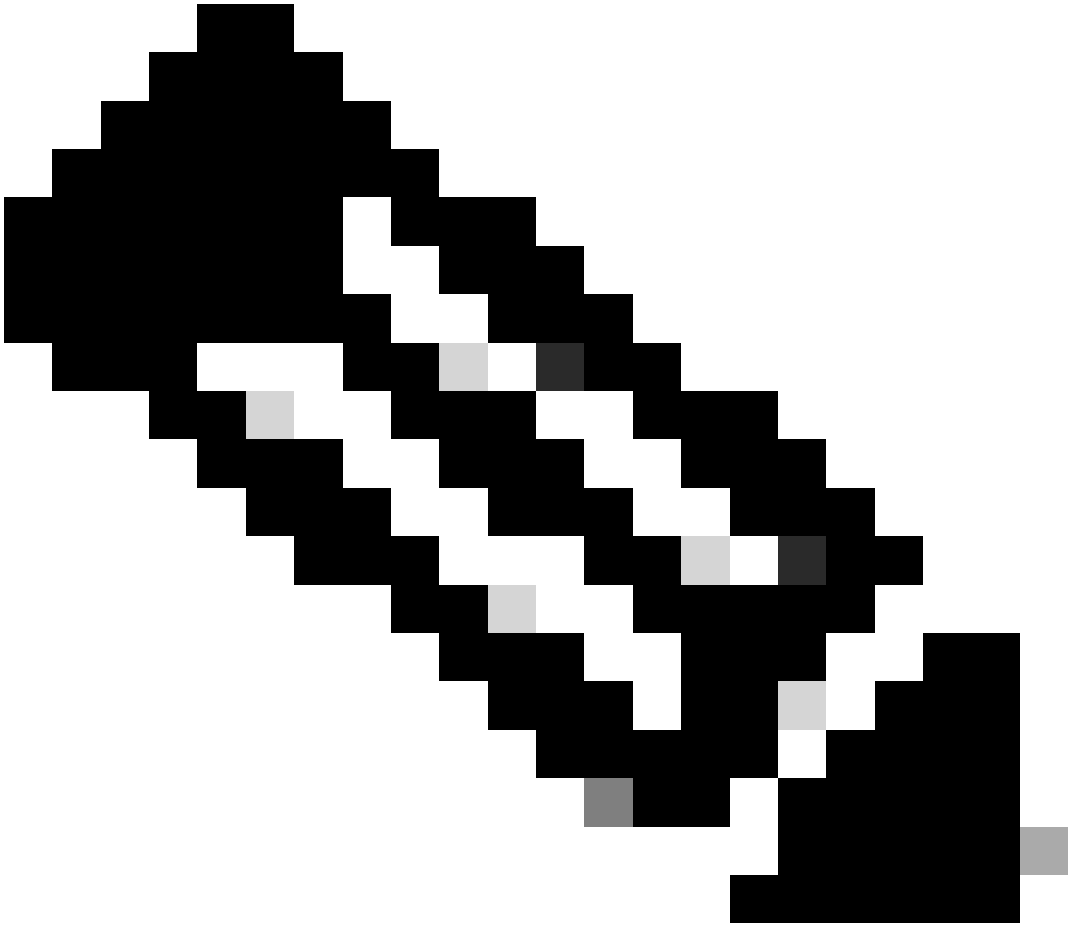
프로세스 제외

프로세스 제외를 통해 관리자는 지원되는 엔진에서 프로세스를 제외할 수 있습니다. 각 플랫폼에서 프로세스 제외를 지원하는 엔진은 다음 표에 요약되어 있습니다.

운영 체제	엔진			
	파일 스캔	시스템 프로세스 보호	악의적인 활동 보호	동작 보호
창	✓	✓	✓	✓
Linux	✓	✗	✗	✓
맥OS	✓	✗	✗	✓

MacOS 및 Linux

프로세스 제외를 생성할 때 절대 경로를 제공해야 하며, 선택 사항인 사용자도 제공할 수 있습니다. 경로와 사용자를 모두 지정하는 경우 프로세스를 제외하려면 두 조건이 모두 충족되어야 합니다. 사용자를 지정하지 않으면 프로세스 제외가 모든 사용자에게 적용됩니다.



참고: macOS 및 Linux에서는 프로세스 제외가 모든 엔진에 적용됩니다.

와일드카드 처리:

보안 엔드포인트 Linux 및 macOS 커넥터는 프로세스 제외 내에서 와일드카드 사용을 지원합니다. 이것은 더 적은 제외로 더 넓은 범위를 허용하지만 너무 많은 것이 정의되지 않은 채로 남아 있는 경우 위험할 수 있습니다. 필요한 제외를 제공하는 데 필요한 최소 문자 수를 포함하려면 와일드카드만 사용해야 합니다.

macOS 및 Linux용 프로세스 와일드카드 사용:

- 와일드카드는 단일 별표 문자(*)를 사용하여 표시됩니다
- 와일드카드는 단일 문자 또는 전체 디렉터리 대신 사용할 수 있습니다.
- 경로의 시작 부분에 와일드카드를 배치하는 것은 유효하지 않은 것으로 간주됩니다.
- 와일드카드는 두 정의된 문자(슬래시 또는 영숫자) 사이에서 작동합니다.

예:

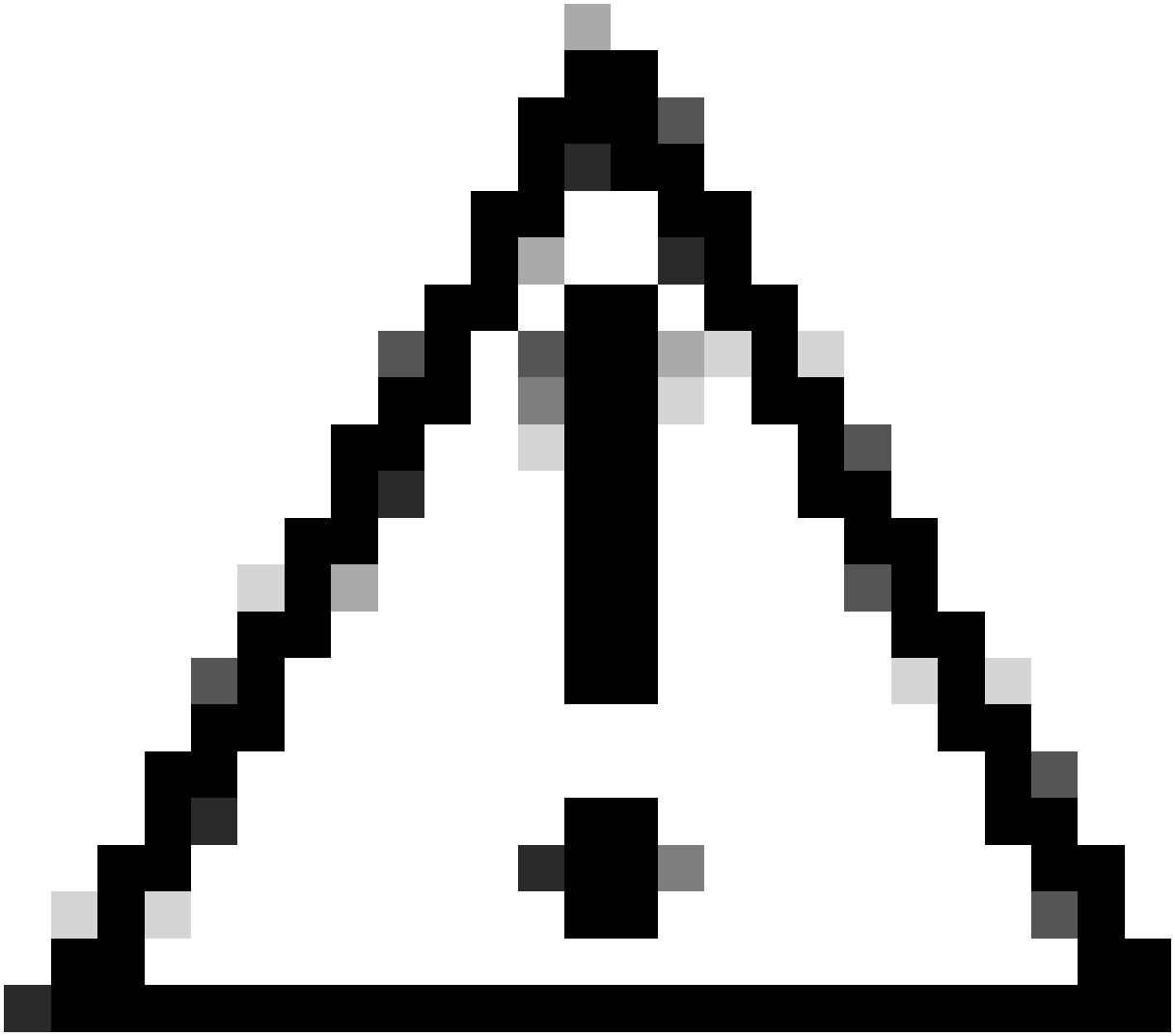
제외	예상 결과

`/Library/Java/JavaVirtualMachines/*/java`	JavaVirtualMachines의 모든 하위 폴더 내에서 `java` 제외
`/Library/Jibber/j*bber`	jabber, `jibber`, `jobber` 등의 프로세스를 제외합니다

창

프로세스 제외를 생성할 때 프로세스 실행 파일의 절대 경로 및/또는 SHA-256을 제공할 수 있습니다. 경로와 SHA-256을 모두 지정하는 경우 프로세스를 제외하려면 두 조건이 모두 충족되어야 합니다.

Windows에서는 경로 내에서 CSIDL 또는 KNOWNFOLDERID를 사용하여 프로세스 제외를 만들 수도 있습니다.

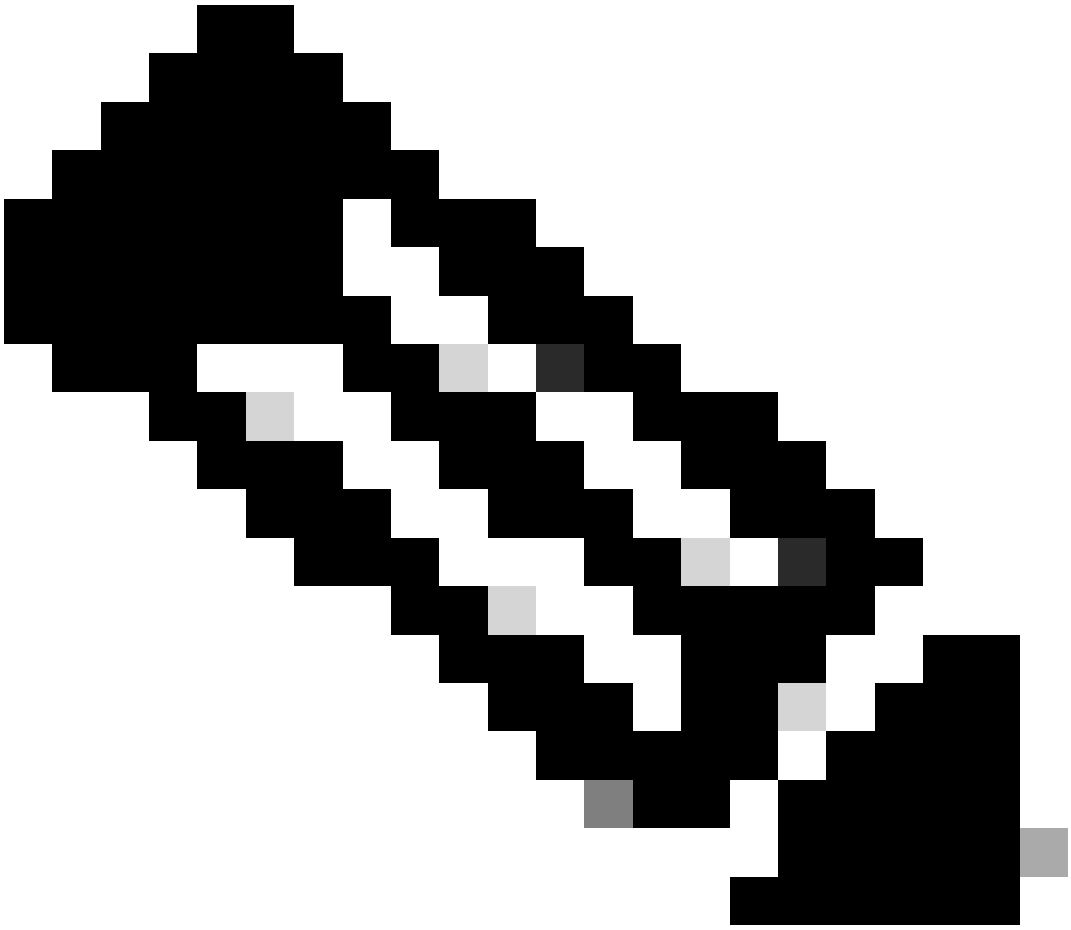


주의: 제외된 프로세스에 의해 생성된 하위 프로세스는 기본적으로 제외되지 않습니다. 프로세스 제외를 생성할 때 추가 프로세스를 제외하려면 하위 프로세스에 적용을 선택합니다.

제한 사항:

- 프로세스의 파일 크기가 정책에 설정된 최대 스캔 파일 크기보다 큰 경우 프로세스의 SHA-256이 계산되지 않으며 제외가 작동하지 않습니다. 최대 스캔 파일 크기보다 큰 파일에 대해서는 경로 기반 프로세스 제외를 사용합니다.
- Windows 커넥터에서는 모든 프로세스 제외 유형에 대해 500개의 프로세스 제외를 제한합니다.
    - 프로세스 제외는 policy.xml의 프로세스 제외 목록의 맨 위부터 최대 한도까지만 적용됩니다.
    - 모든 Windows 정책에는 sfc.exe에 대한 프로세스 제외가 있으며, 이는 프로세스 제외 제한에 대해 계산됩니다.

      ```
      <item>3|0||CSIDL_Secure Endpoint_VERSION\sfc.exe|48|</item>
      ```



참고: Windows에서는 엔진당 프로세스 제외가 적용됩니다. 동일한 제외를 여러 엔진에 적용해야 하는 경우 프로세스 제외는 적용 가능한 각 엔진에 대해 복제되어야 합니다.

와일드카드 처리:

보안 엔드포인트 Windows 커넥터는 프로세스 제외 내에서 와일드카드를 사용할 수 있습니다. 이것은 더 적은 제외로 더 넓은 범위를 허용하지만 너무 많은 것이 정의되지 않은 채로 남아 있는 경우 위험할 수 있습니다. 필요한 제외를 제공하는 데 필요한 최소 문자 수를 포함하려면 와일드카드만 사용해야 합니다.

Windows용 프로세스 와일드카드 사용:

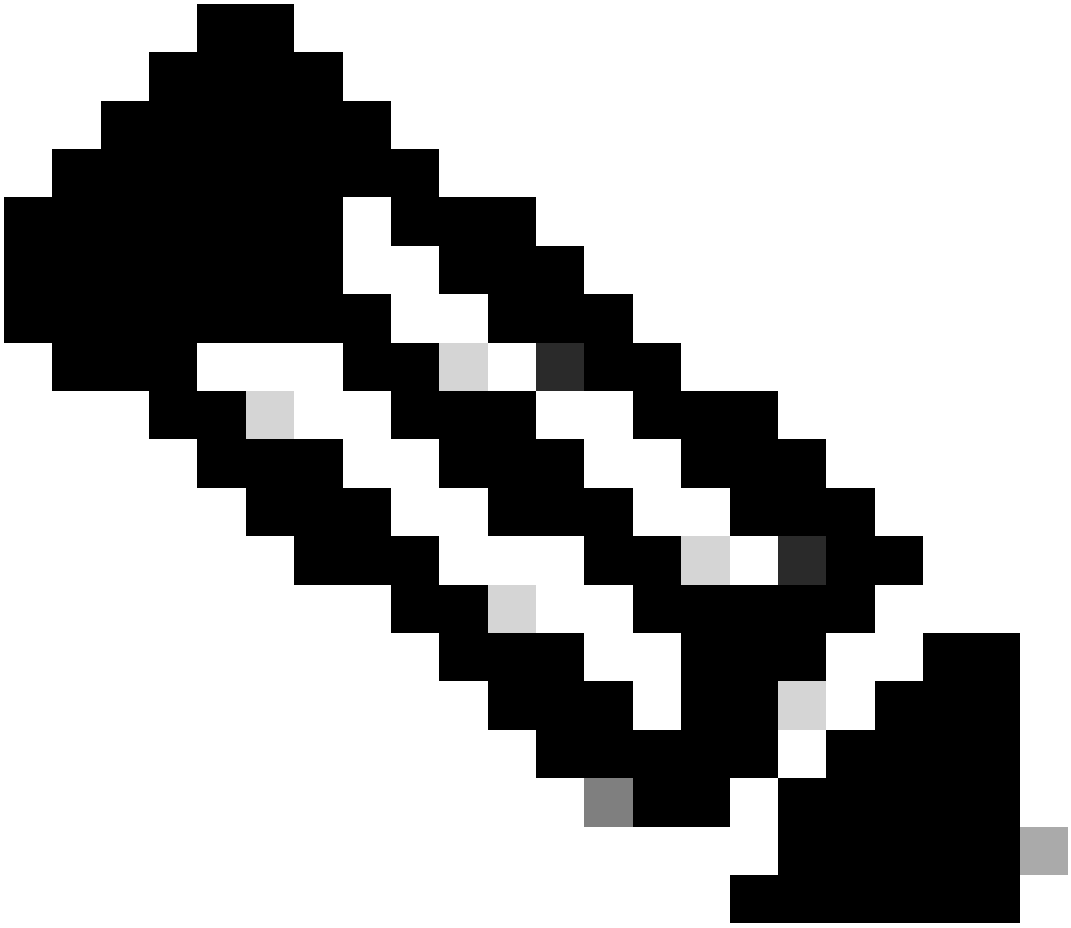
- 와일드카드는 단일 별표 문자()와 이중 별표(*)를 사용하여 표시됩니다
- 단일 별표 와일드카드(*):
  - 와일드카드는 단일 문자 또는 전체 디렉터리 대신 사용할 수 있습니다.
  - 경로의 시작 부분에 와일드카드를 배치하는 것은 유효하지 않은 것으로 간주됩니다.
  - 와일드카드는 두 정의된 문자(슬래시 또는 영숫자) 사이에서 작동합니다.
  - 경로 끝에 와일드카드를 배치하면 하위 디렉토리가 아닌 해당 디렉토리의 모든 프로세스가 제외됩니다.
- 이중 별표 와일드카드(**):
  - 패스의 끝에만 배치할 수 있습니다.
  - 경로 끝에 와일드카드를 배치하면 해당 디렉토리의 모든 프로세스와 하위 디렉토리의 모든 프로세스가 제외됩니다.
  - 이렇게 하면 최소한의 입력으로 훨씬 더 큰 제외 세트를 사용할 수 있지만, 가시성을 위해 매우 큰 보안 구멍을 남깁니다. 이 기능은 매우 신중하게 사용하십시오.

예:

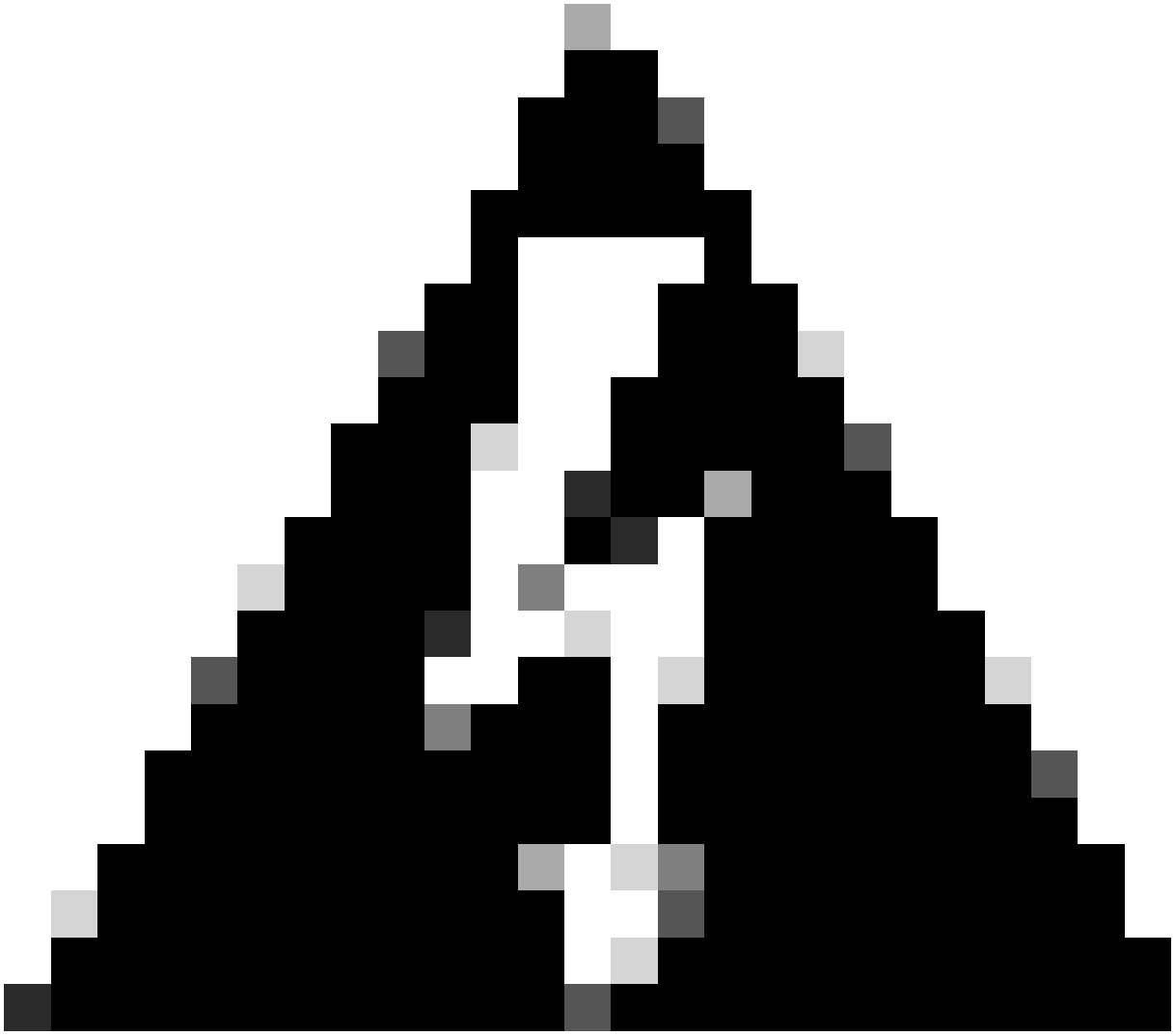
제외	예상 결과
`C:\Windows\*\Tiworker.exe`	`Windows`의 하위 디렉터리에 있는 모든 `Tiworker.exe` 프로세스를 제외합니다
`C:\Windows\P*t.exe`	`Pot.exe`, `Pat.exe`, `P1t.exe` 등을 제외합니다.
`C:\Windows\*chickes.exe`	`Windows` 디렉터리에서 `chickes.exe`로 끝나는 모든 프로세스를 제외합니다.
`C:\*`	`C:`드라이브의 모든 프로세스를 제외하지만 하위 디렉토리에는 제외하지 않습니다.
`C:\**`	`C:` 드라이브의 모든 프로세스 제외

위협 제외

위협 제외를 사용하면 이벤트 트리거에서 특정 위협 이름을 제외할 수 있습니다. 이벤트가 오탐 탐지의 결과라고 확신하는 경우에만 위협 제외를 사용해야 합니다. 이 경우 이벤트의 정확한 위협 이름을 위협 제외로 사용합니다. 이 제외 유형을 사용하는 경우 위협 이름의 true-positive 탐지도 탐지, 격리 또는 이벤트를 생성하지 않습니다.



참고: 위협 제외는 대/소문자를 구분하지 않습니다. 예: `W32.Zombies.NotAVirus` 및 `w32.zombies.notavirus` 둘 다 동일한 위협 이름과 일치합니다.



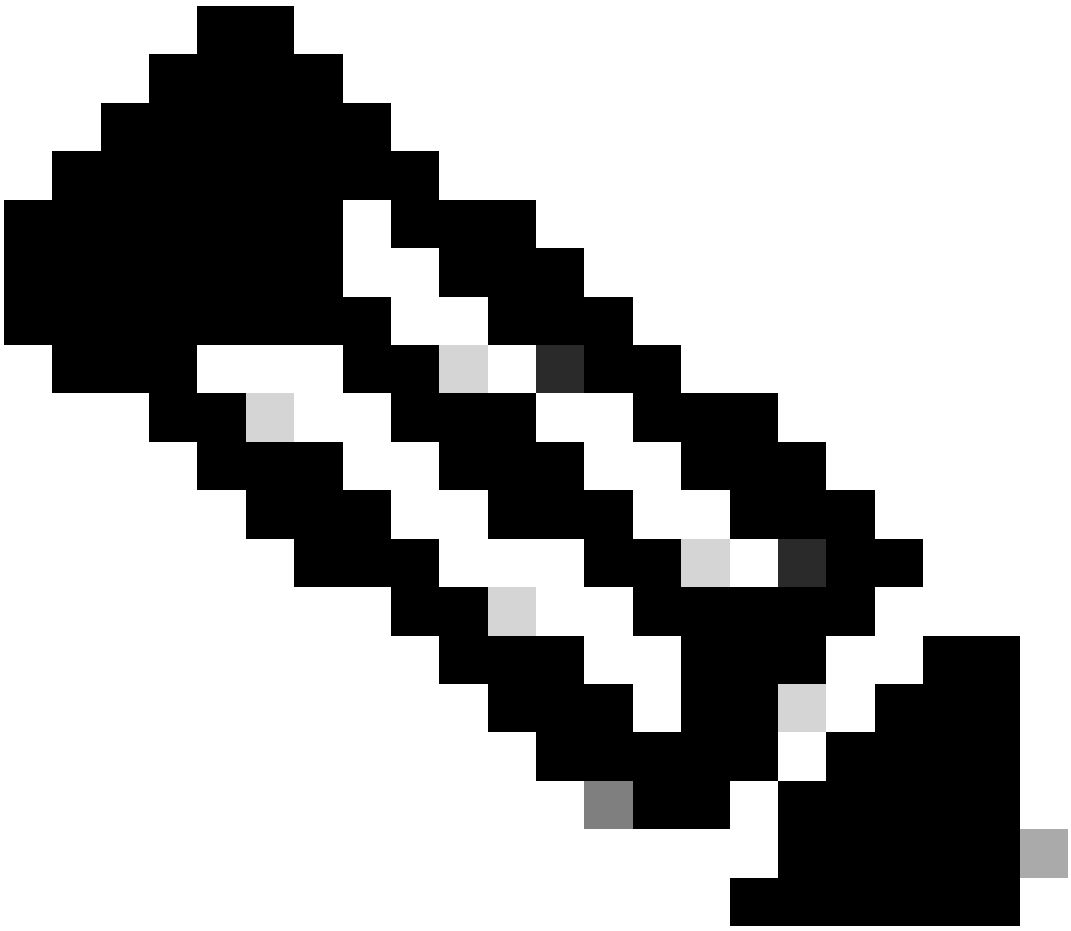
경고: 철저한 조사를 통해 위협 이름이 오탐으로 확인된 경우가 아니면 위협을 제외하지 마십시오. 제외된 위협은 더 이상 검토 및 감사를 위해 Events(이벤트) 탭에 채워지지 않습니다.

경로 제외

애플리케이션 충돌에는 일반적으로 디렉토리 제외가 포함되므로 경로 제외가 가장 자주 사용됩니다. 절대 경로를 사용하여 경로 제외를 생성할 수 있습니다. Windows에서는 CSIDIL 또는 KNOWNFOLDERID를 사용하여 경로 제외를 만들 수도 있습니다.

예를 들어 Windows의 `Program Files` 디렉토리에서 AV 애플리케이션을 제외하려면 제외 경로는 다음 중 하나가 될 수 있습니다.

```
C:\Program Files\MyAntivirusAppDirectory
CSIDL_PROGRAM_FILES\MyAntivirusAppDirectory
FOLDERID_ProgramFiles\MyAntivirusAppDirectory
```



참고: 경로 제외는 재귀적이며 모든 하위 디렉토리도 제외합니다.

부분 경로 일치(Windows 전용)

경로 제외에 후행 슬래시가 제공되지 않으면 Windows 커넥터가 경로에서 부분 일치를 수행합니다. Mac 및 Linux는 부분 경로 일치를 지원하지 않습니다.

예를 들어 Windows에서 다음 경로 제외를 적용하는 경우

```
C:\Program Files
C:\test
```

그러면 다음 경로가 모두 제외됩니다.

```
C:\Program Files
C:\Program Files (x86)
C:\test
C:\test123
```

"C:\test"에서 `"C:\test\"`로 제외를 변경하면 `"C:\test123"`이 제외되지 않습니다.

파일 확장명 제외

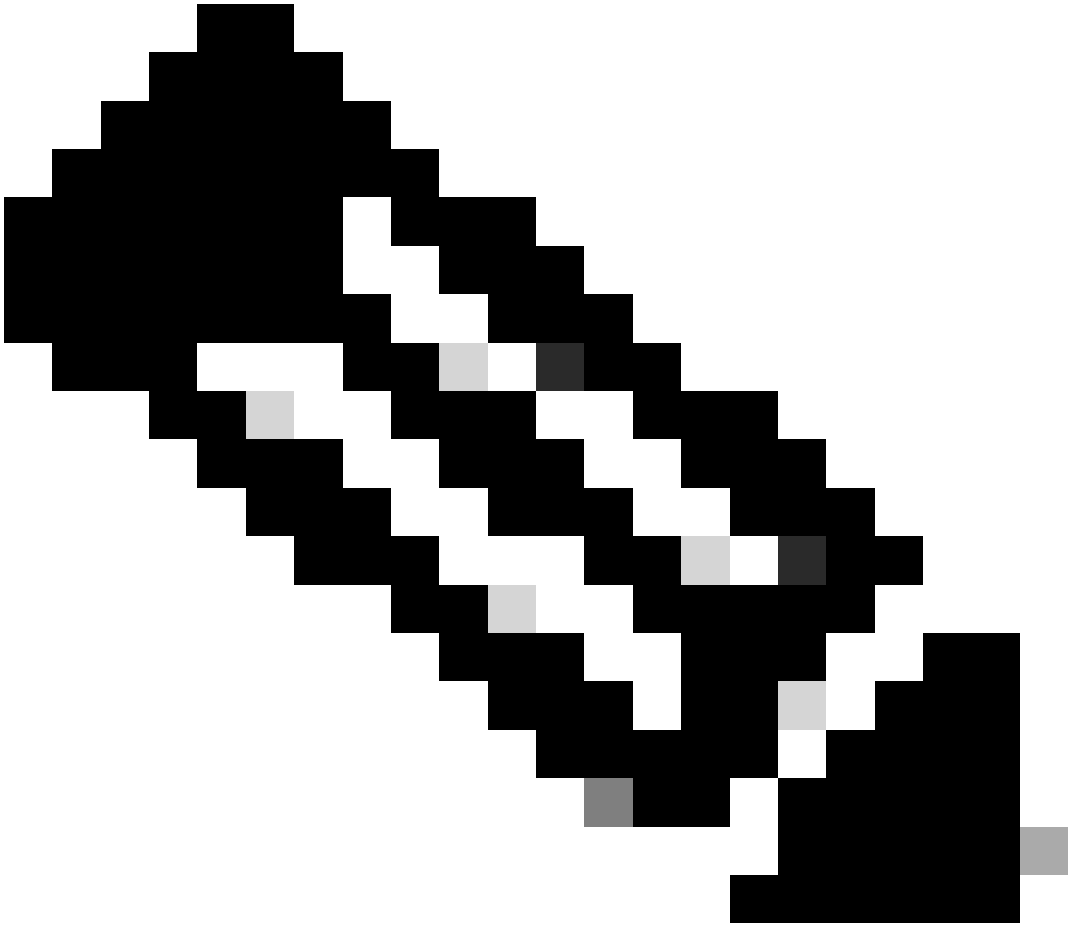
파일 확장자 제외를 사용하면 특정 확장자의 모든 파일을 제외할 수 있습니다.

요점:

- Secure Endpoint Console에 필요한 입력은 확장입니다.
- 추가된 항목이 없으면 Secure Endpoint Console에서 자동으로 파일 확장명 앞에 기간을 추가합니다.
- 확장명은 대/소문자를 구분하지 않습니다.

예를 들어, 모든 Microsoft Access 데이터베이스 파일을 제외하려면 다음 제외를 만들 수 있습니다.

```
.MDB
```



참고: 표준 파일 확장명 제외는 기본 목록에서 사용할 수 있습니다. 이러한 제외를 삭제하지 않는 것이 좋습니다. 이렇게 하면 엔드포인트에서 성능이 변경될 수 있습니다.

와일드카드 제외

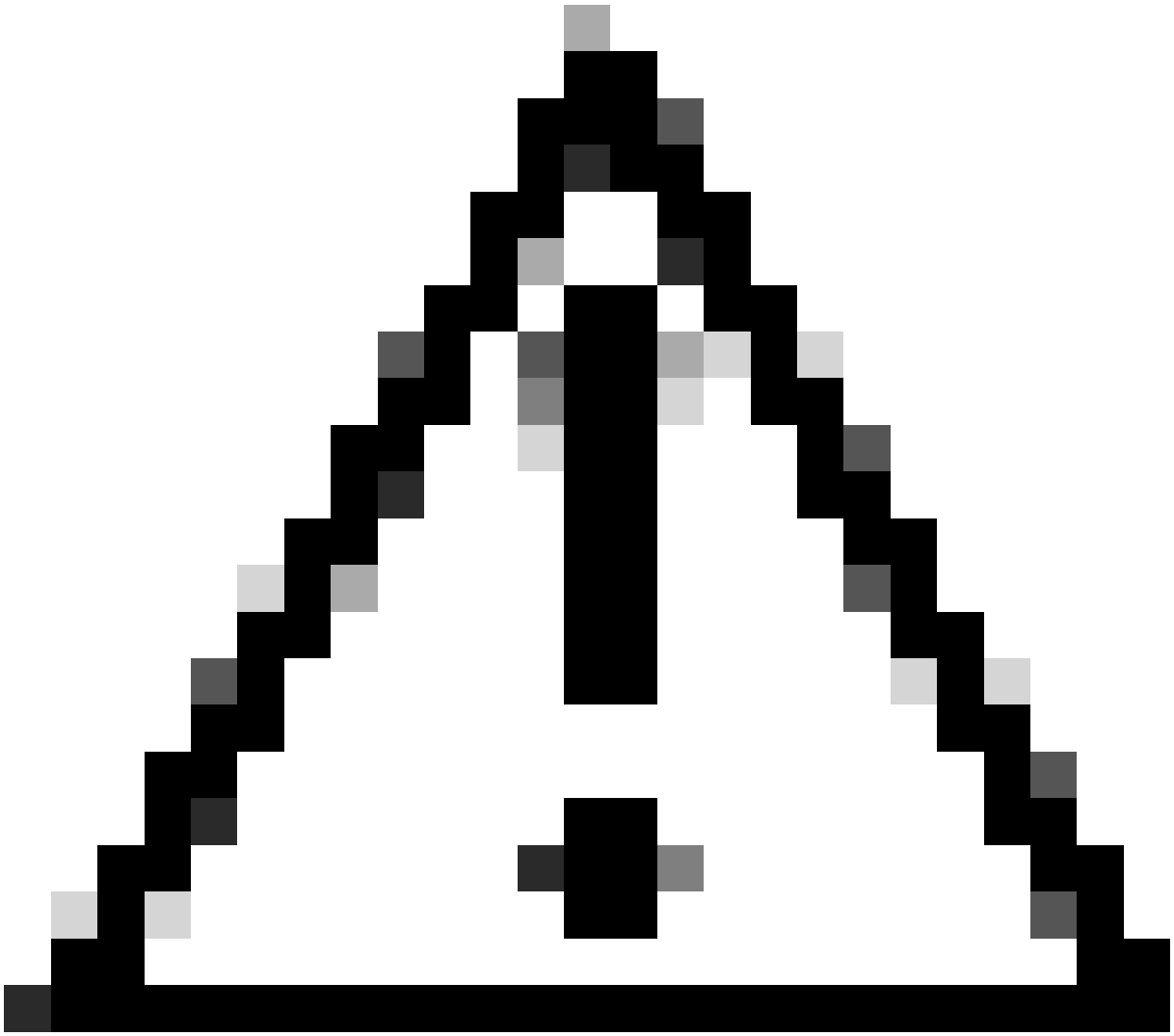
와일드카드 제외는 경로 또는 파일 확장명 제외와 동일하지만, 경로 또는 확장명 내에서 와일드카드를 나타내기 위해 별표 문자(*)를 사용할 수 있습니다.

예를 들어 macOS의 가상 머신을 검사에서 제외하려면 다음 경로 제외를 입력할 수 있습니다.

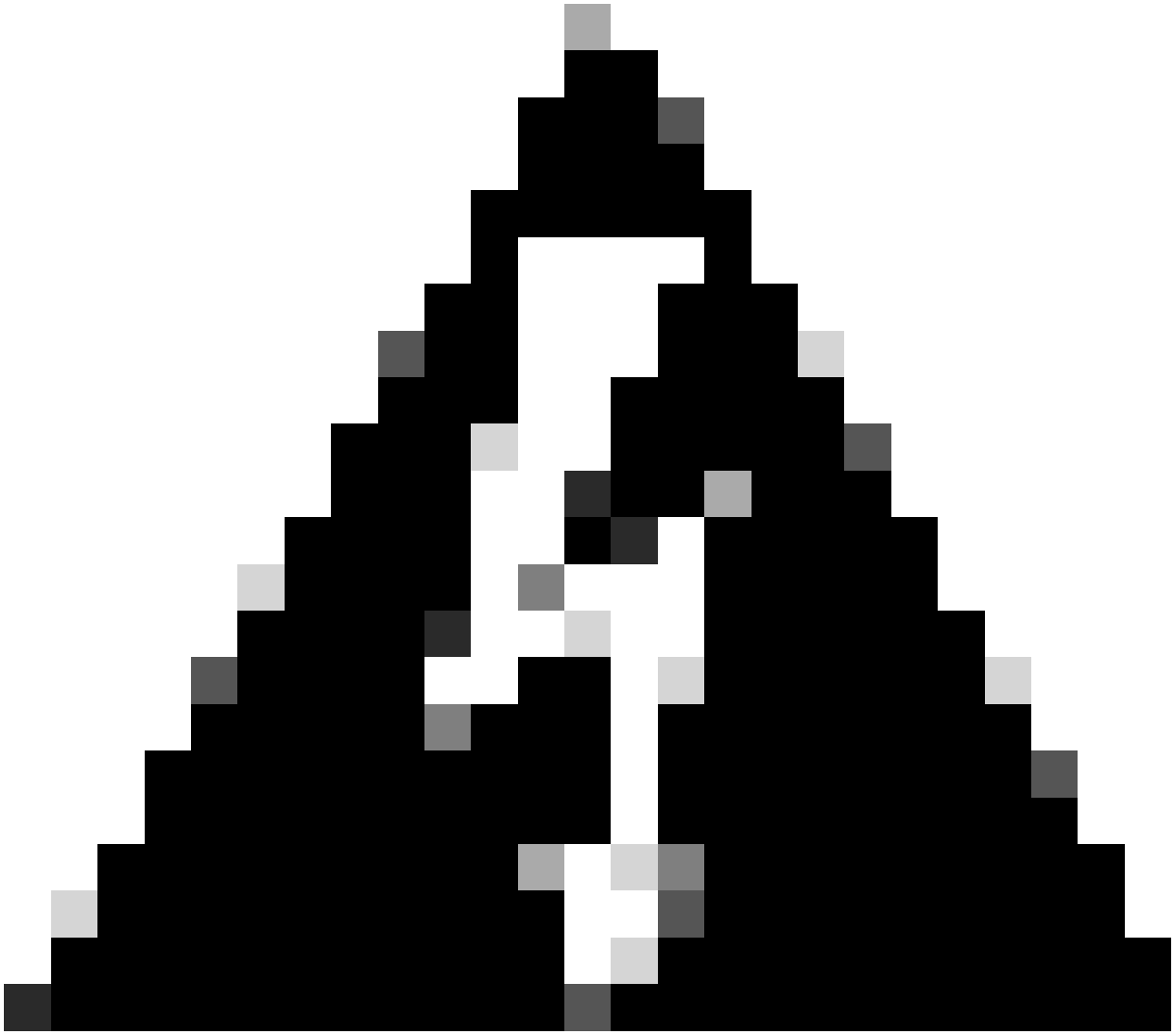
```
/Users/johndoe/Documents/Virtual Machines/
```

그러나 이 제외는 한 사용자에게만 적용되므로 대신 경로의 사용자 이름을 별표로 바꾸고 와일드카드 제외를 생성하여 모든 사용자에 대해 이 디렉토리를 제외합니다.

/Users/*/Documents/Virtual Machines/



주의: 와일드카드 제외는 경로 구분 기호에서 멈추지 않습니다. 이로 인해 의도하지 않은 제외가 발생할 수 있습니다. 예를 들어 `C:\*\test`는 `C:\sample\test` 및 C:\1\test** 또는 `C:\sample\test123`을 제외합니다.



경고: 별표 문자로 제외를 시작하면 성능에 큰 문제가 발생할 수 있습니다. 별표 문자로 시작하는 모든 제외를 제거하거나 변경하여 CPU 영향을 줄입니다.

창

Windows에서 와일드카드 제외를 만들 때 모든 드라이브 문자에 적용할 수 있는 옵션이 있습니다. 이 옵션을 선택하면 모든 마운트된 드라이브에 와일드카드 제외가 적용됩니다.

동일한 제외를 수동으로 작성하려면 `^[A-Za-z]\` 를 추가해야 합니다. 예를 들면 다음과 같습니다.

```
^[A-Za-z]\testpath
```

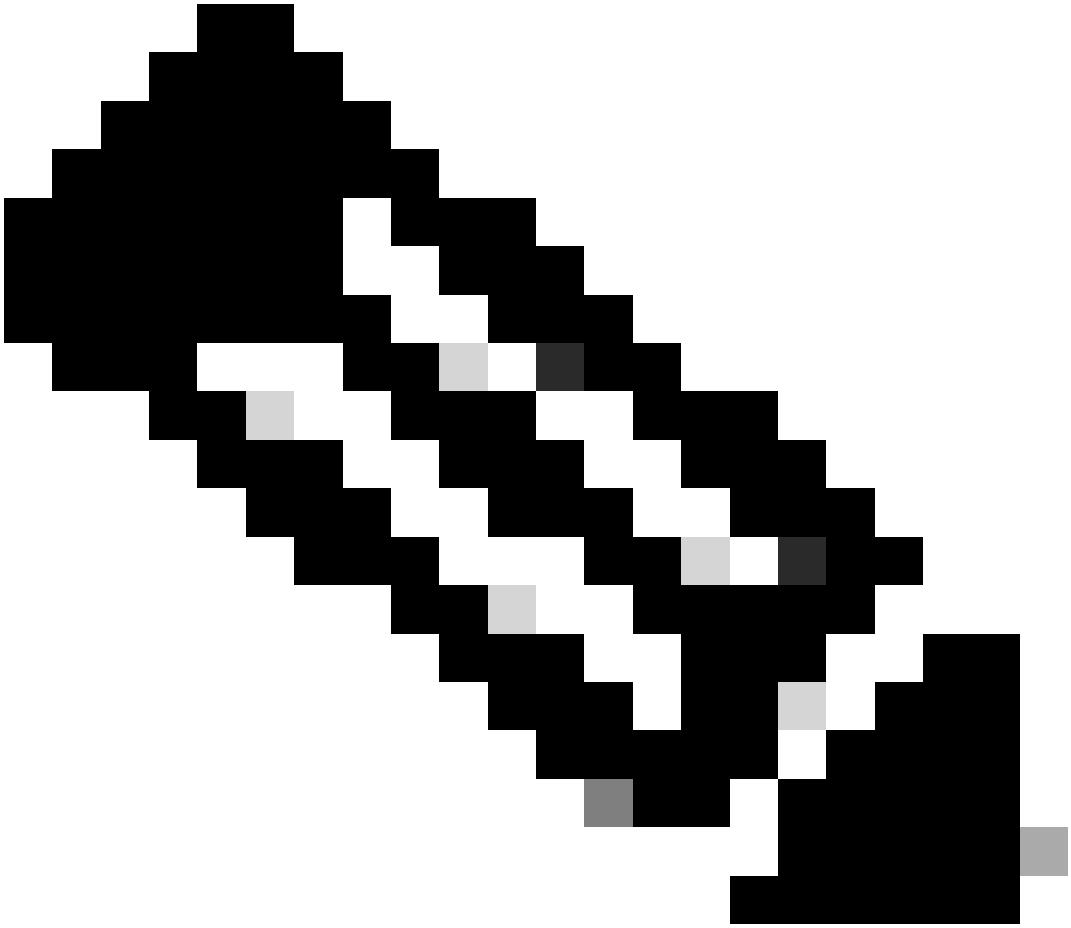
두 예에서 모두 C:\testpath 및 D:\testpath는 제외됩니다.

와일드카드 제외에 대해 모든 드라이브 문자에 적용을 선택한 경우 Secure Endpoint Console은^[A-Za-z]를 자동으로 생성합니다.

실행 파일 제외(Windows 전용)

실행 파일 제외는 Exploit Prevention이 활성화된 Windows 커넥터에만 적용됩니다. 실행 파일 제외는 특정 실행 파일이 익스플로잇 방지로 보호되지 않도록 제외합니다. 문제 또는 성능 문제가 발생하는 경우에만 실행 파일을 익스플로잇 방지에서 제외해야 합니다.

Application Exclusion(애플리케이션 제외) 필드에 실행 파일 이름을 지정하여 보호된 프로세스 목록을 확인하고 보호에서 를 제외할 수 있습니다. 실행 파일 제외는 name.exe 형식의 실행 파일 이름과 정확히 일치해야 합니다. 와일드카드는 지원되지 않습니다.

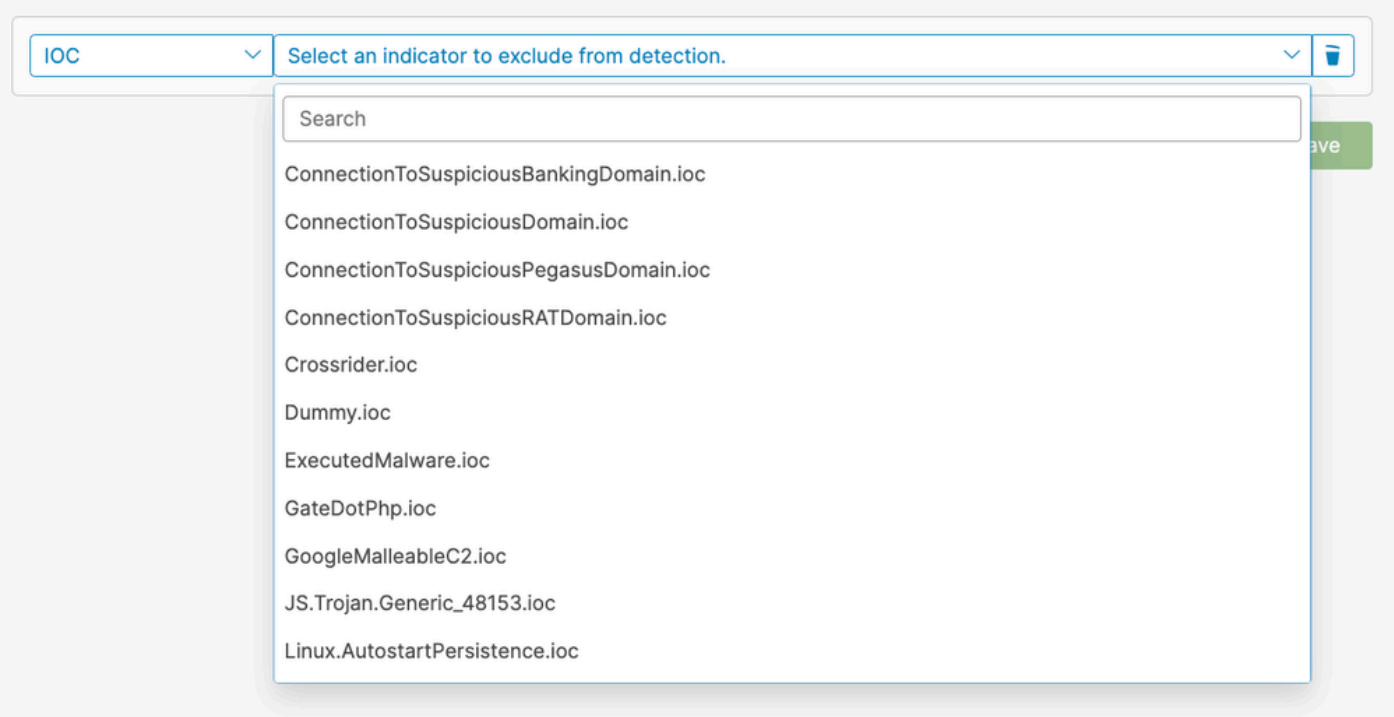


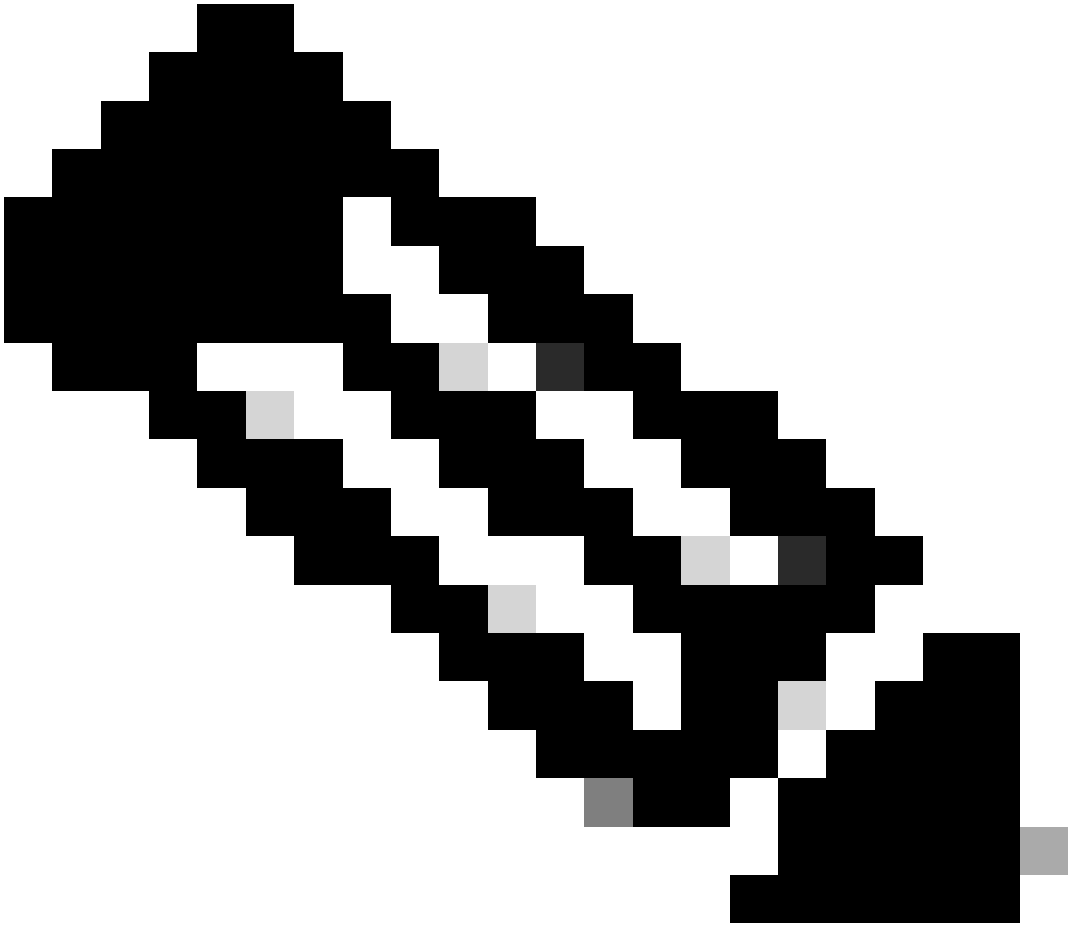
참고: Secure Endpoint Console에서 Executable 제외를 사용하여 애플리케이션만 제외할 수 있습니다. DLL과 관련된 제외는 제외를 만들 지원 케이스를 열어야 합니다.

익스플로잇 방지에 대한 올바른 제외 항목을 찾는 것은 다른 제외 유형보다 훨씬 더 집중적인 프로세스이며, 보안 취약점을 최소화하기 위해 광범위한 테스트가 필요합니다.

IOC 제외(Windows 전용)

IOC 제외를 사용하면 Cloud Indications of Compromise를 제외할 수 있습니다. 이는 서명되지 않은 사용자 지정 또는 내부 애플리케이션이 있고 특정 IOC가 자주 트리거되는 경우에 유용할 수 있습니다. Secure Endpoint Console은 IOC 제외에 대해 선택할 수 있는 표시기 목록을 제공합니다. 드롭다운을 통해 제외할 지표를 선택할 수 있습니다.





참고: 심각도가 높거나 심각한 IOC를 제외할 경우 IOC에 대한 가시성이 떨어지고 조직이 위험에 노출될 수 있습니다. 오탐이 많이 발생하는 경우에만 이러한 IOC를 제외해야 합니다.

CSIDL 및 KNOWNFOLDERID(Windows 전용)

CSIDL 및 KNOWNFOLDERID 값은 Windows용 경로 및 프로세스 제외를 작성할 때 허용되고 권장됩니다. CSIDL/KNOWNFOLDERID 값은 대체 드라이브 문자를 사용하는 환경에 대한 프로세스 및 경로 제외를 만드는 데 유용합니다.

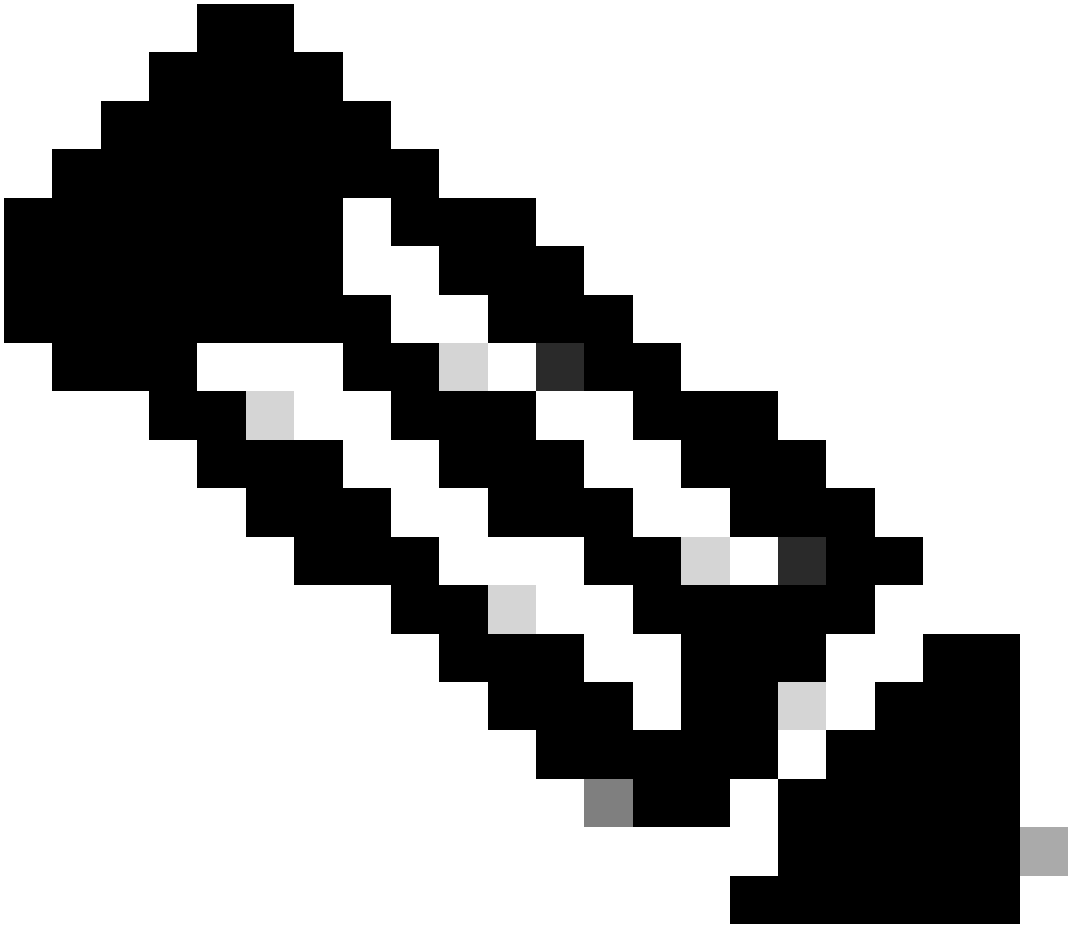
CSIDL/KNOWNFOLDERID를 사용할 경우 고려해야 할 제한이 있습니다. 사용자 환경에서 둘 이상의 드라이브 문자에 프로그램을 설치하는 경우 CSIDL/KNOWNFOLDERID 값은 기본 또는 알려진 설치 위치로 표시된 드라이브만 참조합니다.

예를 들어, OS가 C:\에 설치되었지만 Microsoft SQL의 설치 경로가 수동으로 D:\으로 변경된 경우, 유지 관리되는 제외 목록의 CSIDL/KNOWNFOLDERID 기반 제외는 해당 경로에 적용되지 않습니다. 즉, CSIDL/KNOWNFOLDERID를 사용할 경우 매핑되지 않으므로 C:\ 드라이브에 없는 각 경로 또

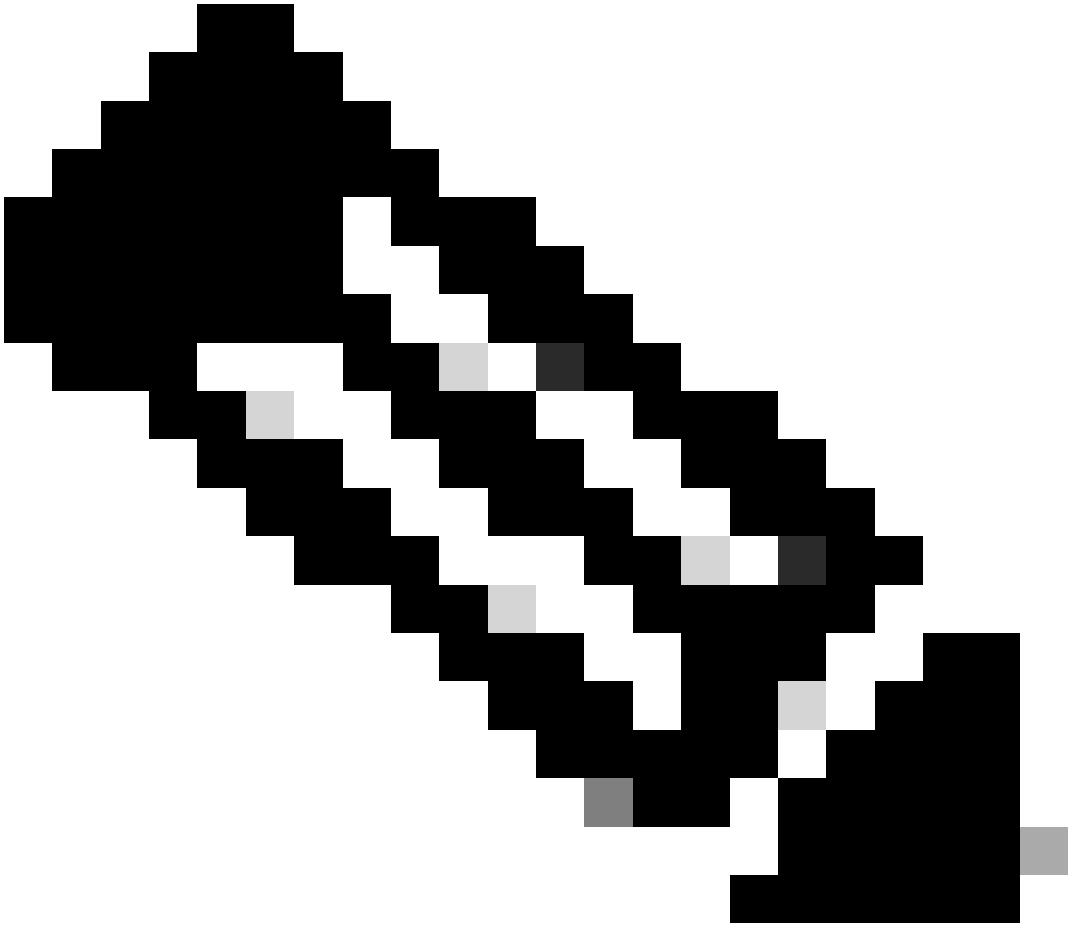
는 프로세스 제외에 대해 하나의 제외를 입력해야 합니다.

자세한 내용은 다음 Windows 설명서를 참조하십시오.

- CSIDL
- 알려진 폴더 ID



참고: KNOWNFOLDERID는 Windows 커넥터 8.1.7 이상에서만 지원됩니다. 이전 버전의 Windows 커넥터는 CSIDL 값을 사용합니다.



참고: KNOWNFOLDERID 값은 대/소문자를 구분합니다. 예를 들어, 잘못된 valueFolderID_programfiles가 아니라 valueFOLDERID_ProgramFiles를 사용해야 합니다.

제외 조정을 위한 커넥터 준비

제외 조정을 위해 커넥터를 준비하려면 다음을 수행해야 합니다.

1. 디버그 모드에서 실행할 정책 및 그룹을 설정합니다.
2. 정상적인 비즈니스 작업에 따라 새 디버그 그룹의 컴퓨터를 실행하여 충분한 커넥터 로그 데이터를 얻을 수 있습니다.
3. 제외를 식별하는 데 사용할 커넥터에 대한 진단 데이터를 생성합니다.

디버그 모드를 활성화하고 다른 운영 체제에서 진단 데이터를 수집하는 방법에 대한 지침은 다음 문서를 참조하십시오.

- Mac 진단 데이터 수집을 위한 Cisco Secure Endpoint Connector
- Cisco Secure Endpoint Connector for Linux 진단 데이터 수집

- 높은 CPU를 위한 AMP 진단 번들 분석(Windows)

제외 항목 식별

MacOS 및 Linux

디버그 모드에서 생성된 진단 데이터는 제외를 생성하는 데 유용한 파일인 fileops.txt와 execs.txt를 제공합니다. fileops.txt 파일은 경로/파일 확장명/와일드카드 제외를 만드는 데 유용하고, execs.txt 파일은 프로세스 제외를 만드는 데 유용합니다.

프로세스 제외 생성

execucs.txt 파일은 파일 검사를 수행하기 위해 보안 엔드포인트를 트리거한 실행 가능한 경로를 나열합니다. 각 경로에는 스캔한 횟수를 나타내는 연결된 카운트가 있으며 목록은 내림차순으로 정렬됩니다. 이 목록을 사용하여 실행 이벤트 볼륨이 많은 프로세스를 결정한 다음 프로세스 경로를 사용하여 제외를 지정할 수 있습니다. 그러나 일반 유틸리티 프로그램(예: /usr/bin/grep)이나 해석기(예: /usr/bin/ruby)는 제외하는 것이 좋습니다. 일반 유틸리티 프로그램 또는 인터프리터가 많은 양의 파일 스캔을 생성하는 경우 더 많은 대상 제외를 만들기 위해 더 많은 조사를 수행할 수 있습니다
.

1. 상위 프로세스 제외: 프로세스를 실행 중인 응용 프로그램을 결정하고(예: grep를 실행 중인 상위 프로세스 찾기) 이 상위 프로세스를 제외합니다. 이것은 부모 프로세스가 안전하게 프로세스 제외로 만들어질 수 있는 경우에만 행해져야 한다. 상위 제외가 1차 하위 구성요소에 적용되는 경우 상위 프로세스에서 1차 하위 구성요소에 대한 호출도 제외됩니다.
2. 지정된 사용자에 대한 프로세스 제외: 프로세스를 실행 중인 사용자를 결정합니다. 프로세스가 특정 사용자에 의해 높은 볼륨에서 실행 중인 경우 해당 사용자에 대한 프로세스만 제외할 수 있습니다. 예를 들어 프로세스가 사용자 "root"에 의해 높은 볼륨에서 호출되는 경우 프로세스를 제외할 수 있지만 지정된 사용자 'root"에 대해서만 보안 엔드포인트가 "root"가 아닌 모든 사용자에 의한 지정된 프로세스의 실행을 모니터링할 수 있습니다.

execs.txt의 출력 예:

```
33 /usr/bin/bash
23 /usr/bin/gawk
21 /usr/bin/wc
21 /usr/bin/sleep
21 /usr/bin/ls
19 /usr/bin/pidof
17 /usr/bin/sed
14 /usr/bin/date
13 /usr/libexec/gdb
13 /usr/bin/iconv
11 /usr/bin/cat
10 /usr/bin/systemctl
 9 /usr/bin/pgrep
 9 /usr/bin/kmod
 7 /usr/bin/rm
 6 /usr/lib/systemd/systemd-cgroups-agent
 6 /usr/bin/rpm
 4 /usr/bin/tr
```

```
 4 /usr/bin/sort
 4 /usr/bin/find
```

경로, 파일 확장자 및 와일드카드 제외 생성

fileops.txt 파일은 파일 생성, 수정 및 이름 바꾸기 작업이 보안 끝점을 트리거하여 파일 스캔을 수행하는 경로를 나열합니다. 각 경로에는 스캔한 횟수를 나타내는 연결된 카운트가 있으며 목록은 내림차순으로 정렬됩니다. 경로 제외를 시작하는 한 가지 방법은 fileops.txt에서 가장 자주 스캔되는 파일 및 폴더 경로를 찾은 다음 해당 경로에 대한 규칙을 생성하는 것입니다. 카운트가 높다고 해서 경로를 반드시 제외해야 하는 것은 아니지만(예: 이메일을 저장하는 디렉토리를 자주 스캔할 수 있지만 제외해서는 안 됨), 목록은 제외 후보를 식별할 수 있는 시작점을 제공합니다.

fileops.txt의 출력 예:

```
31 /Users/eugene/Library/Cookies/Cookies.binarycookies
24 /Users/eugene/.zhistory
9 /Users/eugene/.vim/.temp/viminfo
9 /Library/Application Support/Apple/ParentalControls/Users/eugene/2018/05/10-usage.data
5 /Users/eugene/Library/Cookies/HSTS.plist
5 /Users/eugene/.vim/.temp/viminfo.tmp
4 /Users/eugene/Library/Metadata/CoreSpotlight/index.spotlightV3/tmp.spotlight.state
3 /Users/eugene/Library/WebKit/com.apple.Safari/WebsiteData/ResourceLoadStatistics/full_browsing_sessio
3 /Library/Logs/Cisco/supporttool.log
2 /private/var/db/locationd/clients.plist
2 /Users/eugene/Desktop/.DS_Store
2 /Users/eugene/.dropbox/instance1/config.dbx
2 /Users/eugene/.DS_Store
2 /Library/Catacomb/DD94912/biolockout.cat
2 /.fseventsd/000000000029d66b
1 /private/var/db/locationd/.dat.nosync0063.arg4tq
```

좋은 경험의 규칙은 로그 또는 저널 파일 확장명을 가진 모든 것이 적합한 제외 후보로 간주되어야 한다는 것입니다.

동작 보호 엔진

동작 보호 엔진은 Linux 커넥터 버전 1.22.0 및 macOS 커넥터 버전 1.24.0에 도입되었습니다. 이러한 버전부터 커넥터는 압도적으로 높은 시스템 활동을 탐지한 다음 결함 18을 발생시킬 수 있습니다.

프로세스 제외는 모든 엔진 및 파일 스캔에 적용됩니다. 이 결함을 해결하기 위해 프로세스 제외를 매우 활동적인 무해한 프로세스에 적용합니다. 디버그 모드 진단 데이터에 의해 생성되는 top.txt 파일을 사용하여 시스템에서 가장 활성화된 프로세스를 확인할 수 있습니다. 자세한 교정 단계는 Secure Endpoint Mac/Linux Connector Fault 18 지침을 참조하십시오.

또한 프로세스 제외는 안전한 소프트웨어에서 오탐(false-positive) 동작 보호 탐지를 잠재울 수 있습니다. Secure Endpoint Console에서 오탐이 발생한 경우, 보고 기능 향상을 위해 이 프로세스를 제

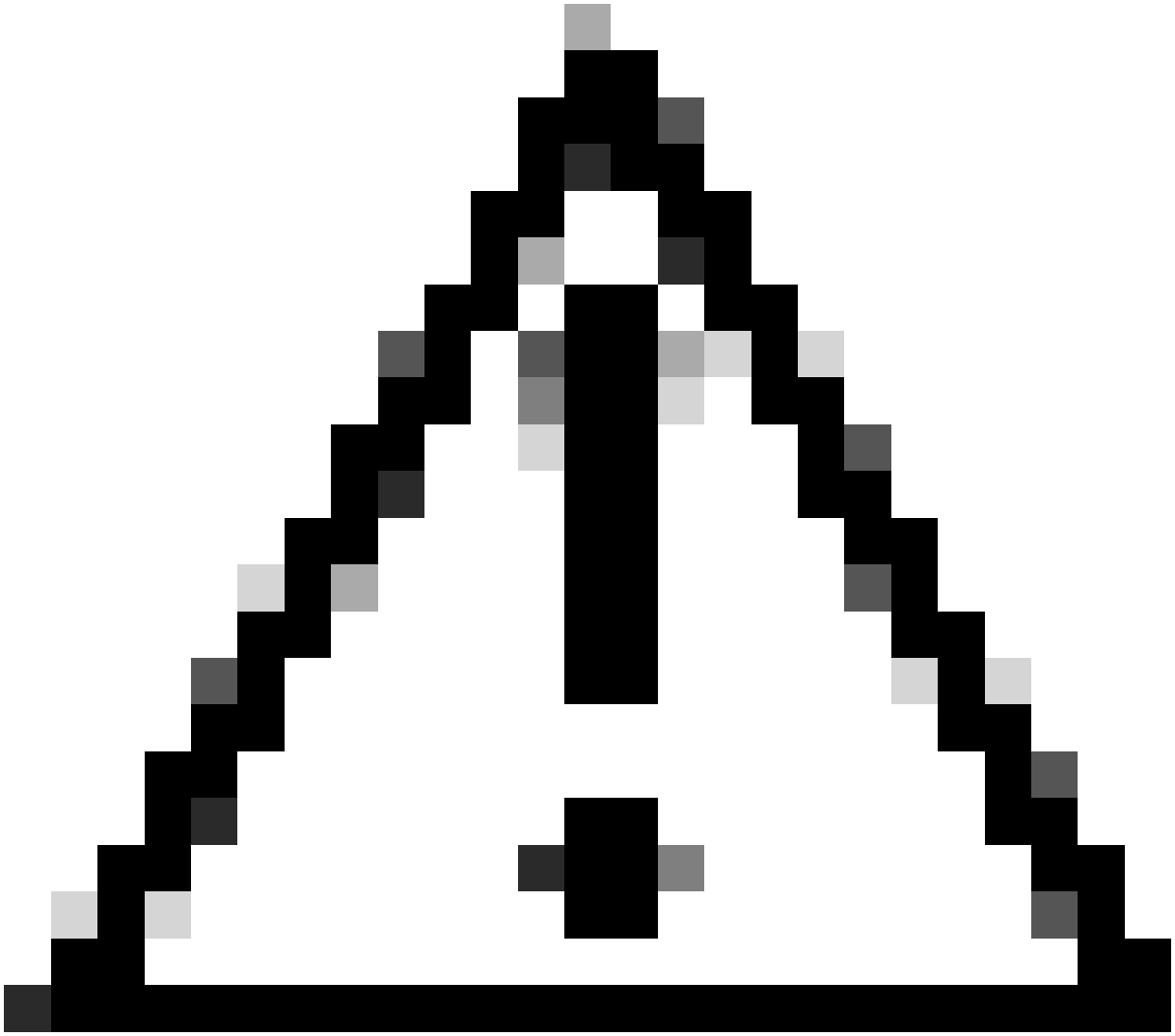
외할 수 있습니다.

창

Windows 운영 체제는 상위 및 하위 프로세스로 인해 더 복잡하고 더 많은 제외 옵션을 사용할 수 있습니다. 이는 액세스한 파일을 식별하려면 더 심층적인 검토가 필요하지만 파일을 생성한 프로그램도 확인해야 함을 나타냅니다.

Cisco Security의 GitHub 페이지에서 이 Windows 조정 도구를 참조하여 보안 엔드포인트로 Windows 성능을 분석하고 최적화하는 방법에 대한 자세한 내용을 확인하십시오.

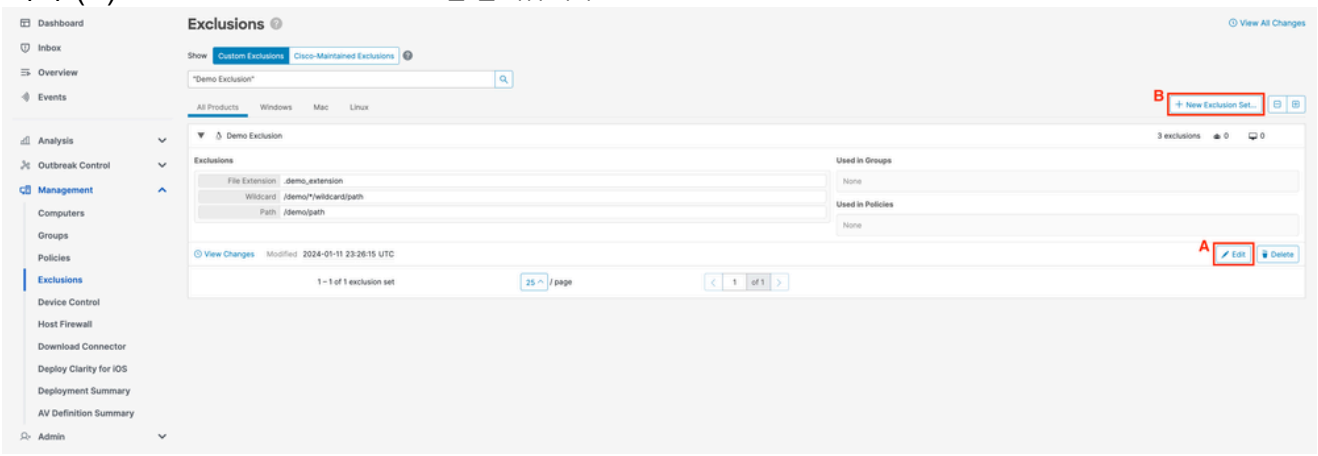
Secure Endpoint Console에서 제외 규칙 생성



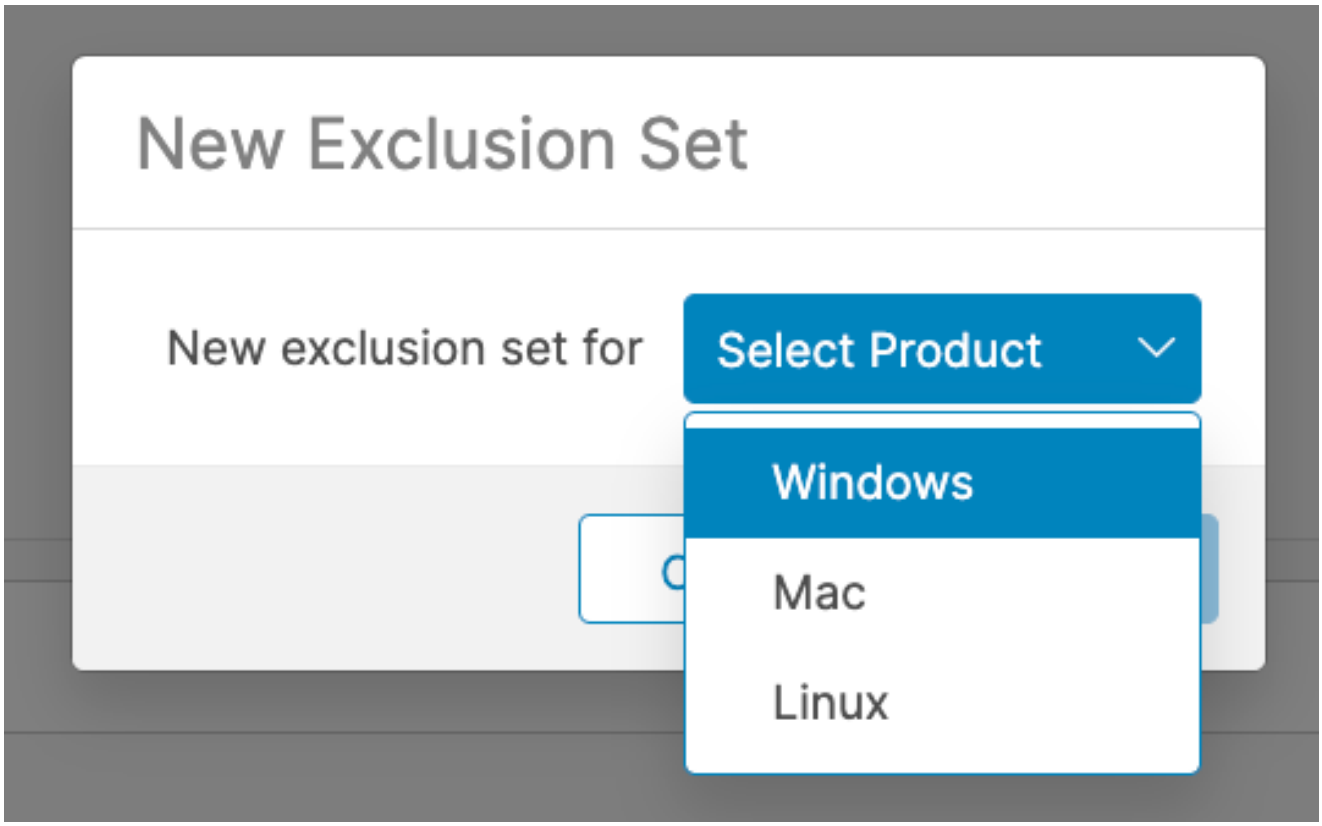
주의: 제외를 작성하기 전에 항상 파일 및 프로세스를 파악하여 엔드포인트의 보안 취약성을 방지하십시오.

Secure Endpoint Console을 사용하여 새 제외 규칙을 생성하려면 다음 단계를 완료합니다.

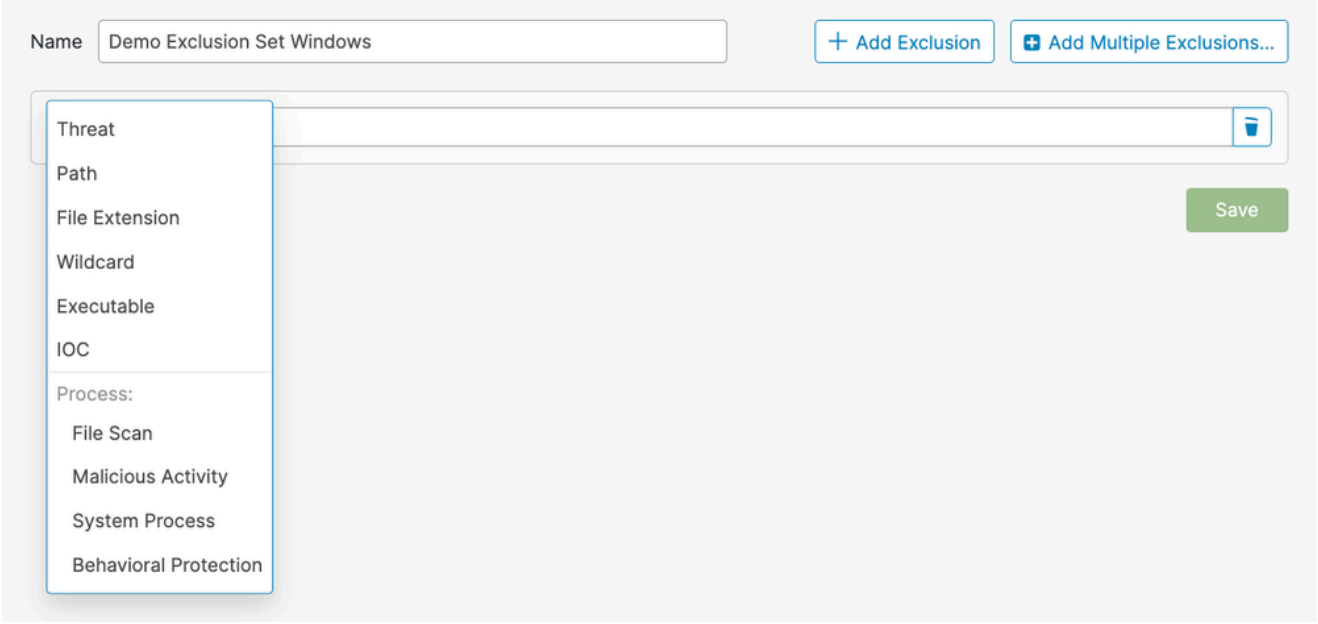
1. Secure Endpoint Console(보안 엔드포인트 콘솔)에서 Management(관리) -> Exclusions(제외)를 선택하여 Policies(정책) 페이지로 이동합니다. (A) 수정할 제외 세트를 찾아 Edit(편집)를 클릭하거나 (B) + New Exclusion Set...를 클릭합니다.



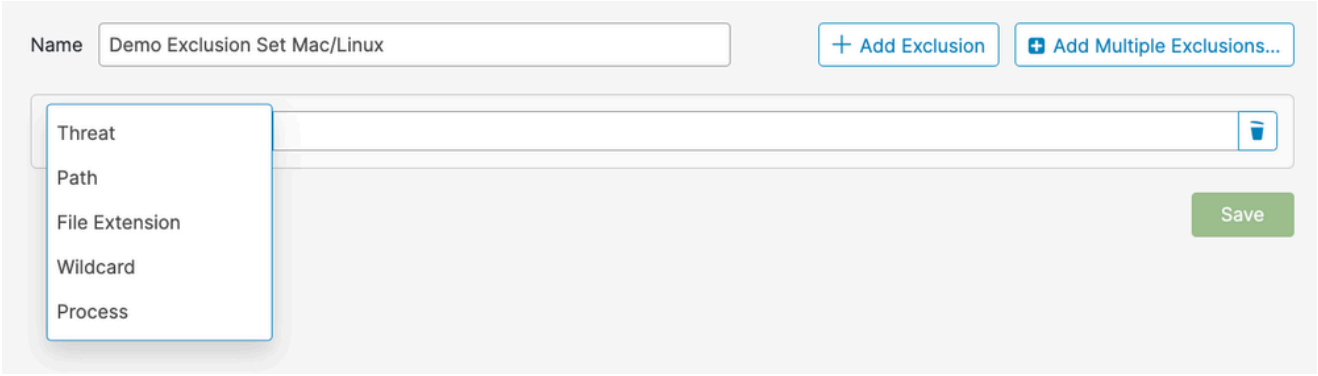
2. New Exclusion Set 팝업에서 제외 세트를 생성할 운영 체제를 선택합니다. Create(생성)를 클릭합니다.



3. 새 제외 세트 페이지로 리디렉션됩니다. + Add Exclusion(제외 추가)을 클릭하고 Select Type(유형 선택) 드롭다운에서 제외 유형을 선택합니다.
창:



Mac/Linux:



4. 선택한 제외 유형에 대한 필수 필드를 입력합니다.
5. 2단계와 3단계를 반복하여 규칙을 더 추가하거나, Save를 클릭하여 제외 세트를 저장합니다.

모범 사례

Cisco Secure Endpoint에서 제공하는 보호 수준이 감소하므로 제외를 생성할 때는 주의해야 합니다. 제외된 파일은 캐시나 클라우드에서 해시되거나 검사되거나 사용할 수 없으며, 활동이 모니터링되지 않으며, 백엔드 엔진, 디바이스 전파 흔적 분석 및 고급 분석에서 정보가 누락됩니다.

제외는 특정 응용 프로그램과의 호환성 문제 또는 달리 개선할 수 없는 성능 문제와 같은 대상 인스턴스에서만 사용해야 합니다.

제외를 생성할 때 따라야 할 몇 가지 모범 사례는 다음과 같습니다.

- 입증된 문제에 대한 제외 항목만 생성
  - 달리 해결할 수 없는 문제가 아닌 것으로 입증된 경우가 아니라면 제외할 필요가 없다고 가정하지 마십시오.
  - 제외를 적용하기 전에 성능 문제, 오탐 또는 애플리케이션 호환성 문제를 철저하게 조사하고 완화해야 합니다.
- 경로/파일 확장명/와일드카드 제외보다 프로세스 제외 선호
  - 프로세스 제외는 경로, 파일 확장자 및 와일드카드 제외를 조합하여 동일한 결과를 얻는 것보다 정상적인 소프트웨어 활동을 제외하는 더 직접적인 방법을 제공합니다.

    - 가능한 경우 프로그램 실행 파일을 대상으로 하는 경로, 파일 확장명 및 와일드카드 제외를 해당 프로세스 제외로 대체하는 것이 좋습니다.
- 광범위한 제외 사항 방지
    - 전체 C 드라이브와 같은 엔드포인트의 많은 부분을 제외하지 마십시오.
    - 파일 이름만 사용하는 대신 파일의 정규화된 경로를 사용합니다.
    - 장치 전파 흔적 분석, 보안 엔드포인트 진단 데이터, Windows 튜닝 도구를 사용하여 특정 제외를 조사하고 결정합니다.
- 와일드카드 제외 초과 사용 방지
    - 와일드카드로 제외를 만들 때는 주의하십시오. 가능한 경우 더 구체적인 제외 항목을 사용합니다.
    - 제외에 최소 와일드카드 수를 사용합니다. 실제로 변수가 있는 폴더만 와일드카드를 사용해야 합니다.
- 일반 유틸리티 프로그램 및 해석기를 제외하지 마십시오
    - 일반적인 유틸리티 프로그램이나 해석자를 배제하는 것은 권장되지 않는다.
    - 일반 유틸리티 프로그램 또는 해석기를 제외해야 하는 경우 프로세스 사용자(macOS/Linux에만 해당)를 제공합니다.
    - 예를 들어, python, `java`, ruby, `bash`, `sh` 등 제외 항목을 작성하지 마십시오.
- 중복 제외 방지
    - 제외를 생성하기 전에 Custom Exclusions(맞춤형 제외) 또는 Cisco-Maintained Exclusions(Cisco 유지 관리 제외)에 제외가 이미 있는지 확인합니다.
    - 중복 제외를 제거하면 성능이 향상되고 제외의 운영 관리가 줄어듭니다.
    - 프로세스 제외에 지정된 경로가 경로/파일 확장자/와일드카드 제외에 포함되지 않는지 확인합니다.
- 악성코드 공격에 일반적으로 사용되는 것으로 알려진 프로세스 제외 방지
    - 자세한 내용은 권장되지 않는 제외를 참조하십시오.
- 오래된 제외 제거
    - 정기적으로 제외 목록을 검토 및 감사하고 특정 제외가 추가된 이유를 기록합니다.
- 보안 침해에서 제외 항목 제거
    - 최적의 보안 및 가시성을 되찾기 위해 커넥터가 손상되면 제외를 제거해야 합니다.
    - 자동화된 작업을 사용하여 감염 후 커넥터에 더 안전한 정책을 적용할 수 있습니다. 커넥터가 손상된 경우, 최고 수준의 보호를 적용하려면 어떤 제외도 없는 정책이 포함된 그룹으로 이동해야 합니다.
    - "보안 침해 시 컴퓨터를 그룹으로 이동" 자동화된 작업을 사전 대응적으로 설정하는 방법에 대한 자세한 내용은 보안 엔드포인트에서 자동화된 작업을 트리거할 조건 식별을 참조하십시오.
- 제외된 항목에 대한 보호 강화
    - 제외가 절대적으로 필요한 경우, 제외된 항목에 대해 일부 보호 계층을 추가하는 쓰기 보호 기능을 활성화하는 등 취할 수 있는 완화 전술을 고려하십시오.
- 지능적으로 제외 항목 생성
    - 제외할 응용 프로그램을 고유하게 식별하는 최상위 레벨 상위 프로세스를 선택하고 하위 프로세스에 적용 옵션을 사용하여 규칙 수를 최소화하여 규칙을 최적화합니다.
- 시작 프로세스를 제외하지 않음
    - 시작 프로세스(macOS에서 `시작`, Linux에서 `init` 또는 `systemd`)는 시스템에서 다른 모든 프로세스를 시작하며 프로세스 계층 구조의 맨 위에 있습니다.
    - 시작 프로세스 및 모든 하위 프로세스를 제외하면 Secure Endpoint 모니터링을 효과적으로 비활성화할 수 있습니다.

- 가능한 경우 프로세스 사용자 지정(macOS/Linux에만 해당)
    - 사용자 필드가 비어 있으면 지정된 프로그램을 실행하는 모든 프로세스에 제외가 적용됩니다.
    - 모든 사용자에게 적용되는 제외는 더 유연하지만, 이러한 광범위한 범위는 모니터링해야 하는 활동을 의도치 않게 제외할 수 있습니다.
    - 런타임 엔진(예: `java`) 및 스크립트 해석기(예: `bash`, python)와 같은 공유 프로그램에 적용되는 규칙에는 사용자를 지정하는 것이 특히 중요합니다.
    - 사용자 범위를 지정 하고 다른 인스턴스를 모니터링 하는 동안 특정 인스턴스를 무시 하도록 보안 엔드 포인트를 지정 합니다.

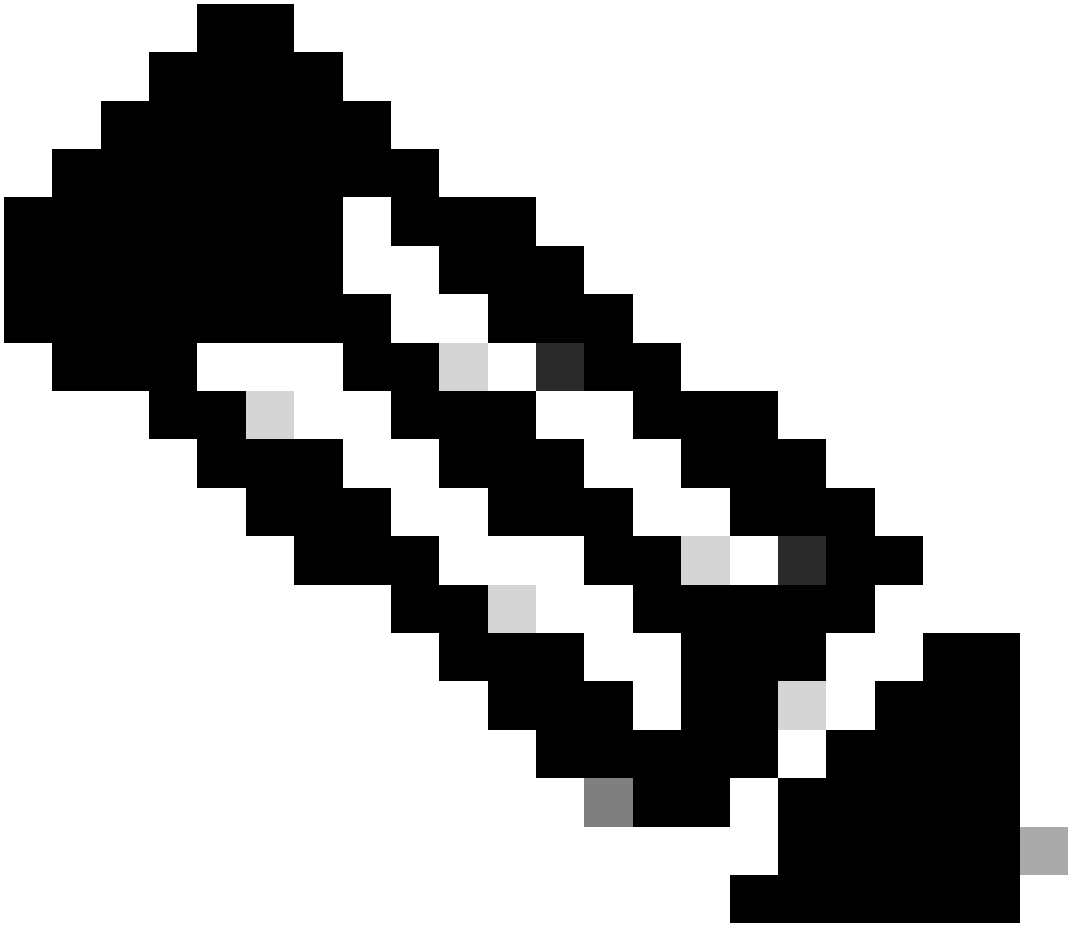
권장되지 않는 제외

공격자가 사용할 수 있는 모든 공격 벡터를 알 수는 없지만, 모니터링해야 할 몇 가지 핵심 공격 벡터가 있습니다. 양호한 보안 상태와 가시성을 유지하기 위해 다음 제외 항목은 권장되지 않습니다.

AcroRd32.exe
addinprocess.exe
addinprocess32.exe
addinutil.exe
bash.exe
bginfo.exe
bitsadmin.exe
cdb.exe
csi.exe
dbghost.exe
dbgsvc.exe
dnx.exe
dotnet.exe
excel.exe
fsi.exe
fsiAnyCpu.exe
iexplore.exe
java.exe
kd.exe
lxssmanager.dll
msbuild.exe
mshta.exe
ntkd.exe
ntsd.exe
outlook.exe
psexec.exe
powerpnt.exe
powershell.exe

rcsi.exe
svchost.exe
schtasks.exe
system.management.automation.dll
windbg.exe
winword.exe
wmic.exe
wuauclt.exe
0.7z
.bat
.bin
.cab
.cmd
.com
.cpl
.dll
.exe
.fla
.gif
.gz
.hta
.inf
.java
.jar
.작업
.jpeg
.jpg
.js
.ko
.ko.gz
.msi
.ocx
.png
.ps1
.py
.rar
.reg
.scr
.sys
.tar
.tmp
.url

.vbe
.vbs
.wsf
.zip
강타
자바
비단뱀
파이썬3
쉬
쾌활해
/
/bin
/sbin
/usr/lib
C:
C:\
C:*
D:\
D:*
C:\Program Files\Java
C:\Temp\
C:\Temp*
C:\Users\
C:\Users*
C:\Windows\Prefetch
C:\Windows\Prefetch\
C:\Windows\Prefetch*
C:\Windows\System32\Spool
C:\Windows\System32\CatRoot2
C:\Windows\Temp
C:\Windows\Temp\
C:\Windows\Temp*
C:\Program 파일\<회사 이름>\
C:\Program 파일(x86)\<회사 이름>\
C:\Users\<UserProfileName>\AppData\Local\Temp\
C:\Users\<UserProfileName>\AppData\LocalLow\Temp\



참고: 이 목록은 피해야 할 완전한 제외 목록이 아니라 핵심 공격 벡터에 대한 통찰력을 제공합니다. 이러한 경로, 파일 확장명 및 프로세스에 대한 가시성을 유지하는 것이 중요합니다.

관련 정보

- 기술 지원 및 문서 – Cisco Systems
- Cisco 보안 엔드포인트 - TechNotes
- Cisco Secure Endpoint - 사용 설명서
- 보안 엔드포인트에서 익스플로잇 방지 트러블슈팅
- 보안 엔드포인트에서 자동화된 작업을 트리거할 조건 식별

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.