# Uitsluitingen in Cisco Secure Endpoint Connector configureren en beheren

## Inhoud



## Inleiding

Dit document beschrijft hoe u de uitsluiting voor de verschillende motoren op de Cisco Secure Endpoint console kunt maken.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Een uitsluitingslijst wijzigen en toepassen op een beleid in de Secure Endpoint-console
- Windows CSIDL-conventie

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Secure Endpoint console 5.4.20211013
- Secure Endpoint Gebruikershandleiding revisie 15 okt 2021

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

# Secure Endpoint-workflow

Op een hoog niveau van bewerkingen verwerkt Cisco Secure Endpoint een bestand Secure Hash Algorithm (SHA) in deze volgorde door de belangrijkste onderdelen van de connector:

- Uitsluitingen
- Tetra Engine
- Toepassingscontrole (lijst toestaan / blokkeringslijst)
- SHA Engine
- Exploitpreventie (Exprev) / Kwaadaardige Activiteit Bescherming (MAP) / Systeemprocesbescherming / Netwerkmotor (Device Flow Correlatie)

---

> **Opmerking**: de optie Uitsluiten of Toestaan/Blocklist maken is afhankelijk van de door de engine gedetecteerde bestand.

---

# Door Cisco onderhouden uitsluitingen

Uitsluitingen voor Cisco-onderhoud worden gemaakt en onderhouden door Cisco om een betere compatibiliteit te bieden tussen de Secure Endpoint Connector en antivirus- en beveiligingsproducten of andere software.

Deze uitsluitingsstelsels bevatten verschillende soorten uitsluitingen om een goede werking te waarborgen.

U kunt de wijzigingen volgen die aan deze uitsluitingen zijn uitgevoerd in het artikel Wijzigingen in Cisco-lijst van ondergehouden uitsluitingen voor Cisco Secure Endpoint Console.

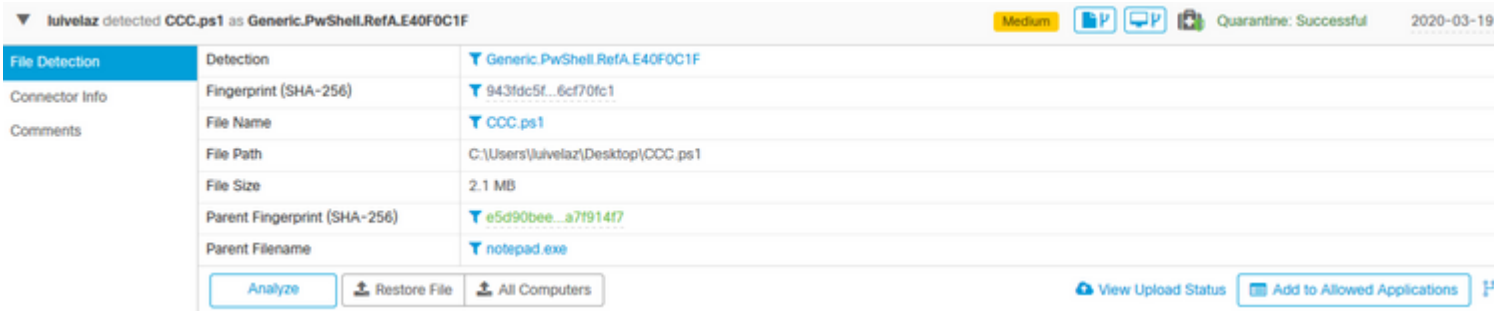
# Aangepaste uitsluitingen

## Secure Endpoint-engine

File Scan (CPU gebruik / bestandsdetectie) door Tetra & SHA engine:

Gebruik deze soorten uitsluitingen om detectie/quarantaine van een bestand te voorkomen of om Secure Endpoint hoge CPU te beperken.

De gebeurtenis op de Secure Endpoint console is zoals in de afbeelding.




---

> **Opmerking**: CSIDL kan worden gebruikt voor uitsluitingen. Raadpleeg dit Microsoft-document voor meer informatie over CSIDL.

---

**Uitsluiting pad**


**Uitsluiting jokerteken**


---

**Opmerking**: Optie **Toepassen op alle stationsaanduidingen** wordt ook gebruikt om de uitsluiting toe te passen op de schijven [A-Z] die aan het systeem zijn gekoppeld.

---

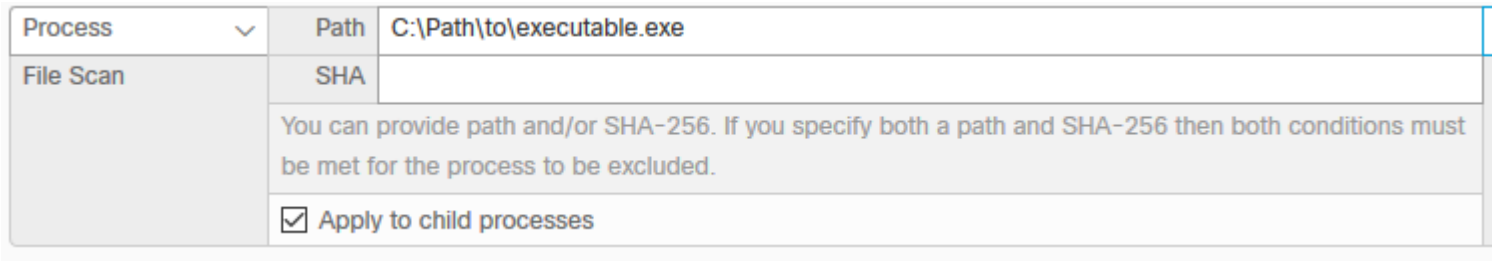
**Uitsluiting bestandsuitgang**


---

**Waarschuwing**: gebruik dit type uitsluiting met voorzichtigheid omdat het alle bestanden met de bestandsextensie uitsluit van scans, ongeacht de locatie van het pad.

---

**Proces: uitsluiting bestandsscan**

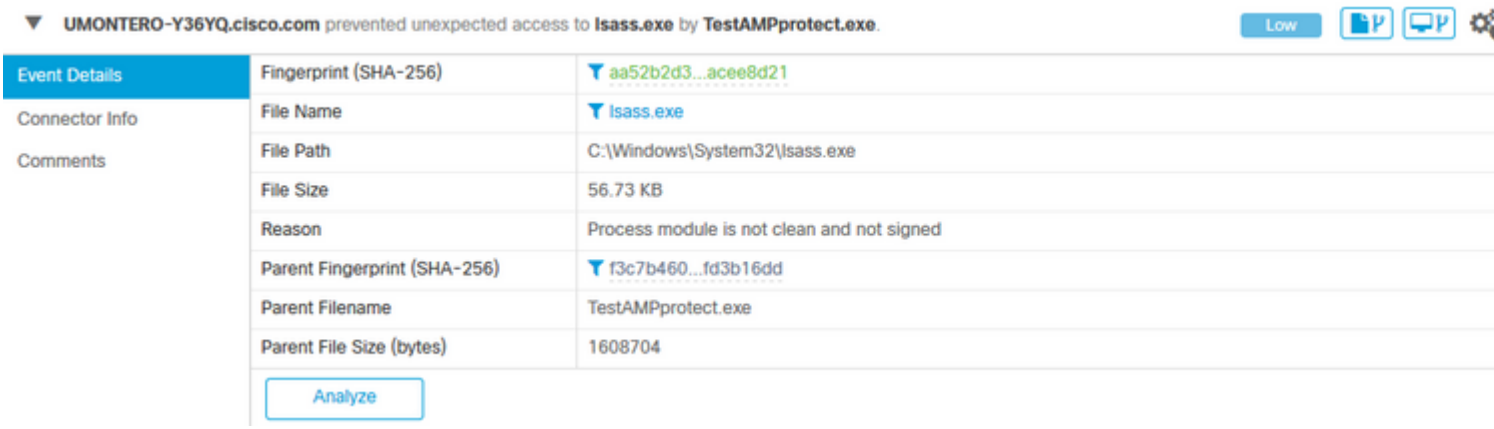



## System Process Protection (SPP)

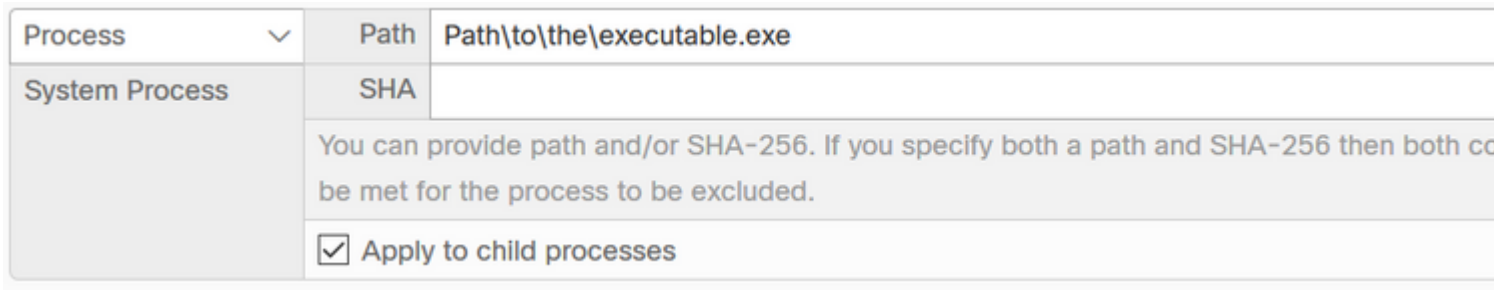
System Process Protection engine is beschikbaar via connector versie 6.0.5 en beschermt de volgende Windows processen:

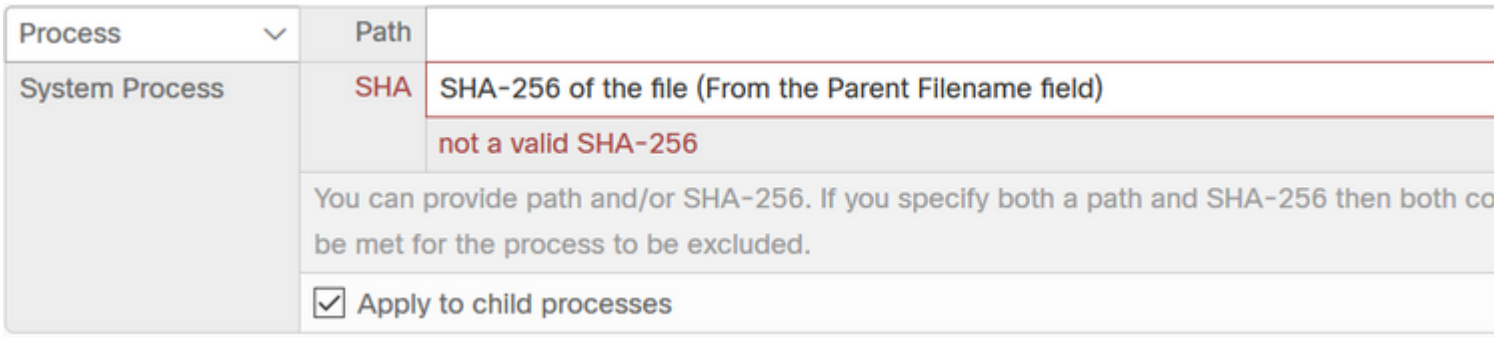
- Session Manager-subsysteem (smss.exe)
- Runtime-subsysteem client/server (csrss.exe)
- Subsysteem met lokale beveiligingsinstantie (lsass.exe)
- Windows Logon-toepassing (winlogon.exe)
- Windows Start-up-toepassing (wininit.exe)

Dit beeld toont een SPP-gebeurtenis.




**Uitsluiting SPP**

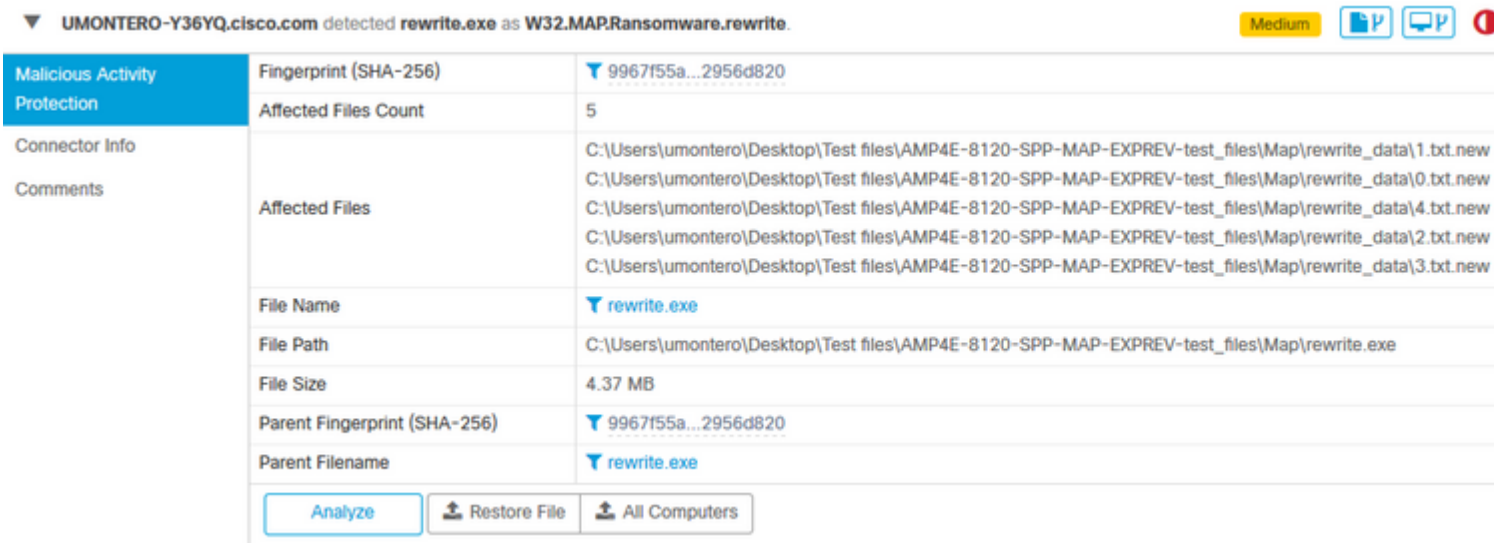


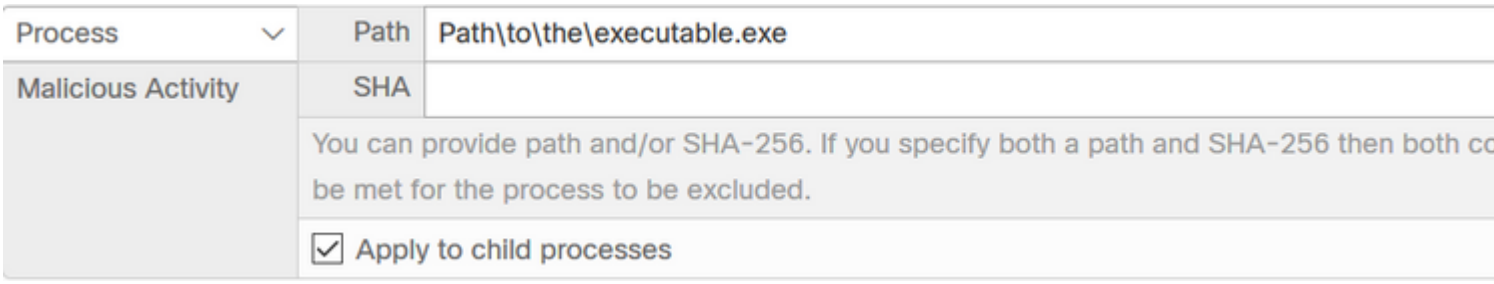

## Bescherming tegen kwaadaardige activiteiten (MAP)

Malicious Activity Protection (MAP) engine, verdedigt uw eindpunt tegen een ransomware aanval. Het identificeert kwaadwillige acties of processen wanneer zij uitvoeren, en beschermt uw gegevens tegen encryptie.

In deze afbeelding is een MAP-gebeurtenis afgebeeld.




**MAP-uitsluiting**




---

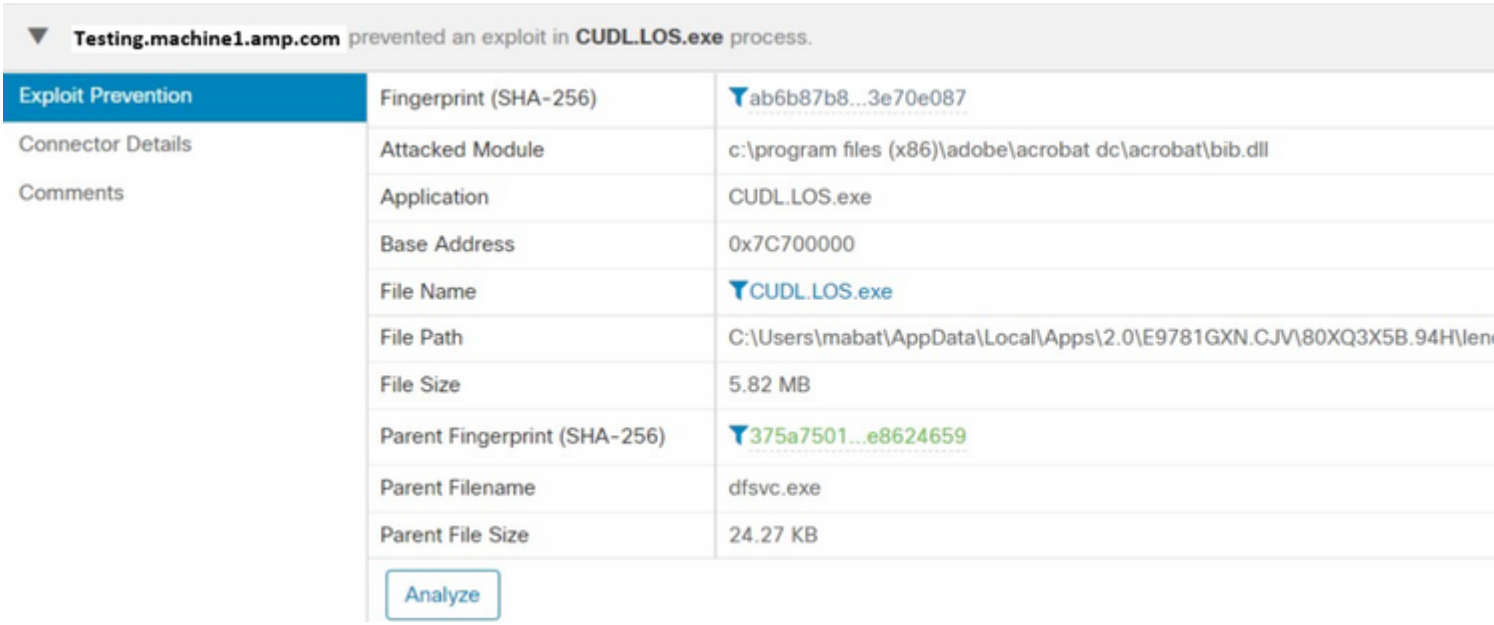
> **Waarschuwing**: gebruik dit soort uitsluiting voorzichtig en nadat u hebt bevestigd dat de detectie inderdaad niet kwaadaardig is.

---

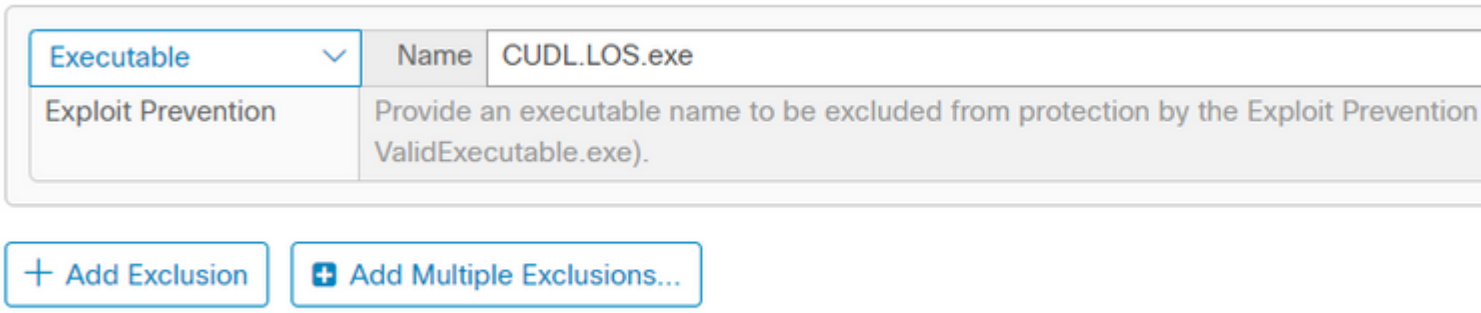
## Preventie van exploitatie (Exprev)

De exploit prevention engine verdedigt uw endpoints tegen geheugeninjecties die vaak worden gebruikt door malware en andere zero-day aanvallen op niet-gepatcheerde software kwetsbaarheden. Wanneer het een aanval tegen een beschermd proces ontdekt zal het worden geblokkeerd en een gebeurtenis genereren, maar er zal geen quarantaine zijn.

In deze afbeelding wordt een gebeurtenis Exprev weergegeven.




**Exprev-uitsluiting**




---

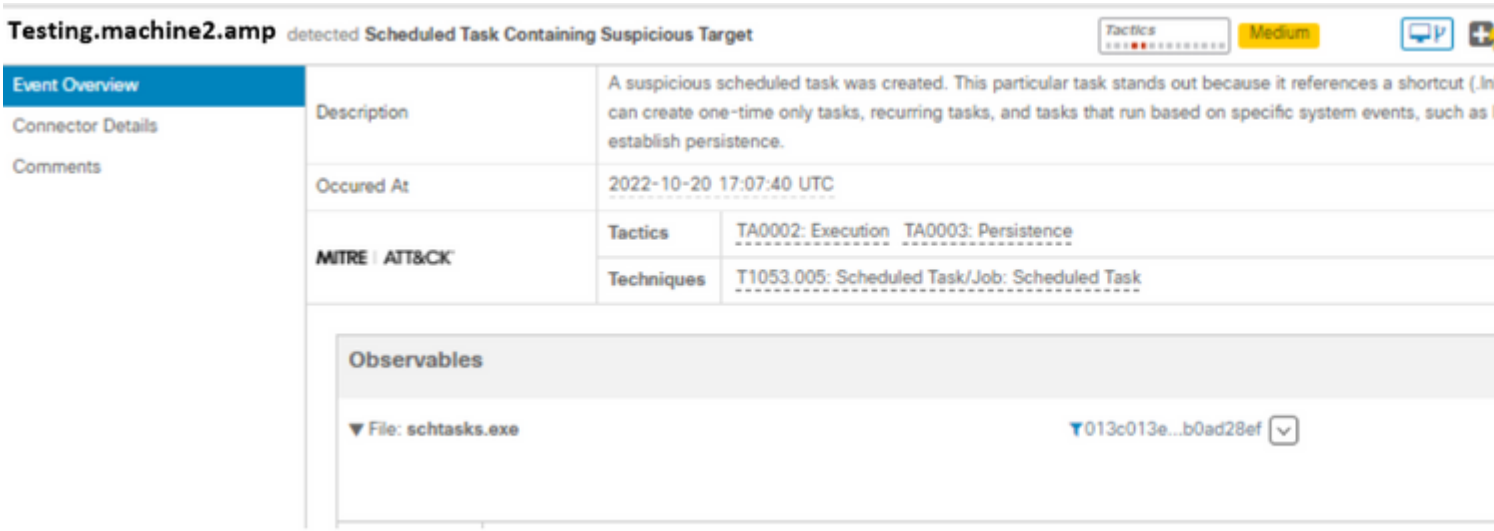
> **Waarschuwing**: gebruik deze uitsluiting wanneer u de activiteit op de betreffende module/toepassing vertrouwt.

---

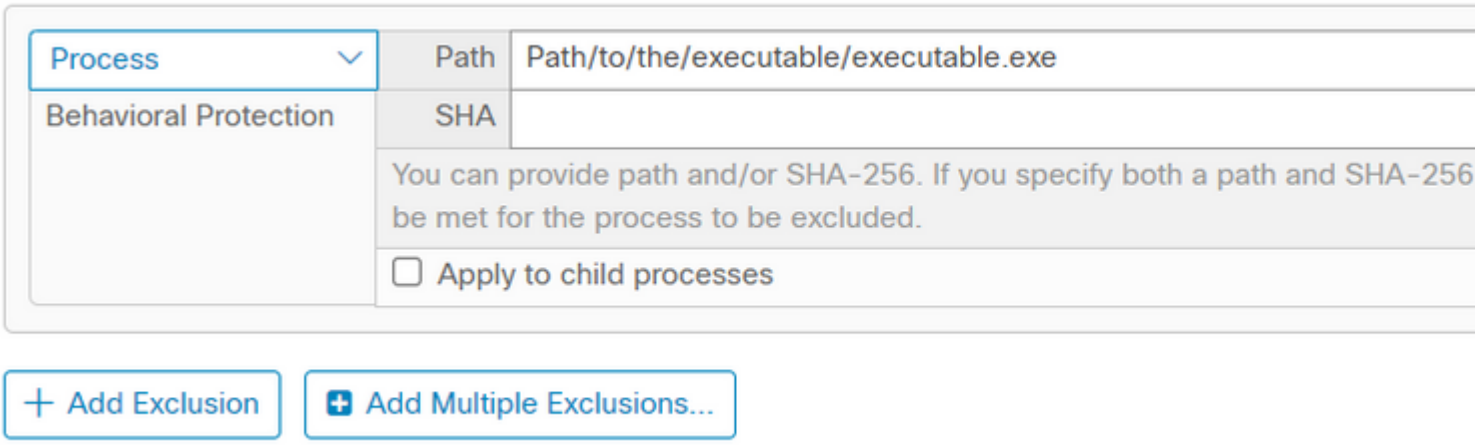
## Gedragsbescherming

De behavioral protection engine vergroot de mogelijkheid om bedreigingen op gedragswijze te detecteren en te stoppen. Het vergroot de mogelijkheid om aanvallen op andere gebieden dan het land te detecteren en biedt
snellere reactie op veranderingen in het bedreigingslandschap door handtekeningupdates.

In deze afbeelding wordt een bloeddrukgebeurtenis weergegeven.




**BGP-uitsluiting**




# Gerelateerde informatie

- **Voor meer informatie over de beleidsconfiguratie, navigeer naar de Gebruikersgids**
- **Uitsluitingen maken in video van Cisco Secure Endpoint Connector**
- **Technische ondersteuning en documentatie â€“ Cisco Systems**

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.