Configuración y administración de exclusiones en Cisco Secure Endpoint Connector

Contenido

Introducción

Este documento describe cómo crear la exclusión para los diferentes motores en la consola de Cisco Secure Endpoint.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Modificar y aplicar una lista de exclusión a una directiva de la consola de Secure Endpoint
- Convención CSIDL de Windows

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Secure Endpoint console 5.4.20211013
- Secure Endpoint User Guide, revisión, 15 de octubre de 2021

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de

entender el posible impacto de cualquier comando.

Flujo de trabajo de terminales seguros

En un alto nivel de operaciones, Cisco Secure Endpoint procesa un archivo de algoritmo hash seguro (SHA) en este orden a través de los componentes principales del conector:

- Exclusiones
- Motor Tetra
- Control de aplicaciones (lista de permitidos / lista de bloqueo)
- Motor SHA
- Prevención de vulnerabilidades (Exprev)/protección contra actividades maliciosas (MAP)/protección de procesos del sistema/motor de red (correlación de flujo de dispositivos)

> **Nota**: La creación de una exclusión o de una lista de permitidos/bloqueados depende del motor que haya detectado el archivo.

Exclusiones mantenidas por Cisco

Cisco crea y mantiene las exclusiones mantenidas por Cisco para proporcionar una mejor compatibilidad entre Secure Endpoint Connector y los antivirus, los productos de seguridad u otro software.

Estos conjuntos de exclusiones contienen distintos tipos de exclusiones para garantizar un funcionamiento correcto.

Puede realizar un seguimiento de los cambios realizados en estas exclusiones en el artículo Cambios en la lista de exclusiones mantenida por Cisco para Cisco Secure Endpoint Console.

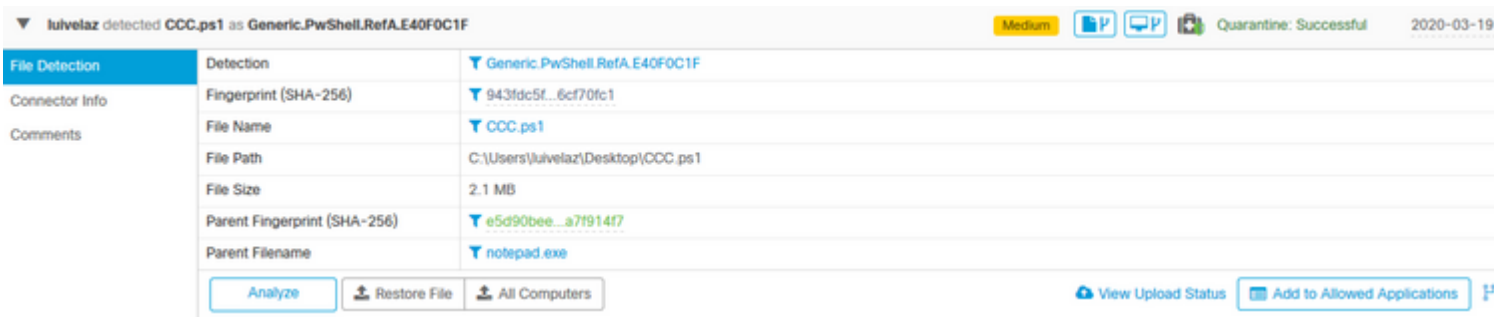
Exclusiones personalizadas

Motor de terminales seguros

Análisis de archivos (uso de CPU / detecciones de archivos) por motor Tetra y SHA:

Utilice estos tipos de exclusiones para evitar la detección/cuarentena de un archivo o para mitigar el uso elevado de la CPU del terminal seguro.

El evento de la consola de Secure Endpoint es el que se muestra en la imagen.



> **Nota**: CSIDL se puede utilizar para exclusiones; consulte este documento de Microsoft para obtener más información sobre CSIDL.

Exclusión de ruta

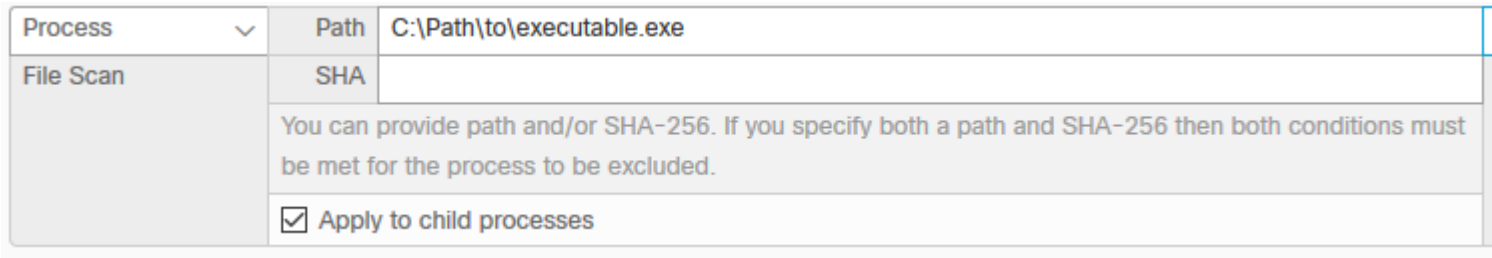
Exclusión de comodines

Nota: La opción **Aplicar a todas las letras de unidad** se utiliza para aplicar también la exclusión a las unidades [A-Z] conectadas al sistema.

Exclusión de extensión de archivo

Precaución: utilice este tipo de exclusión con precaución, ya que excluye todos los archivos con la extensión de archivo de los análisis independientemente de la ubicación de la ruta.

Proceso: Exclusión de análisis de archivos

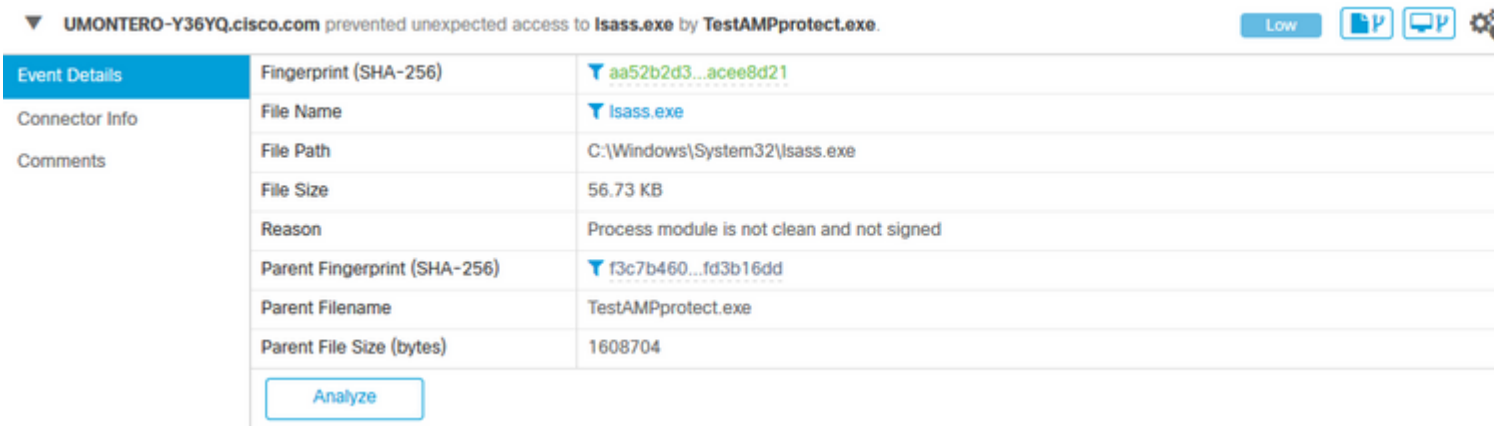


Protección de procesos del sistema (SPP)

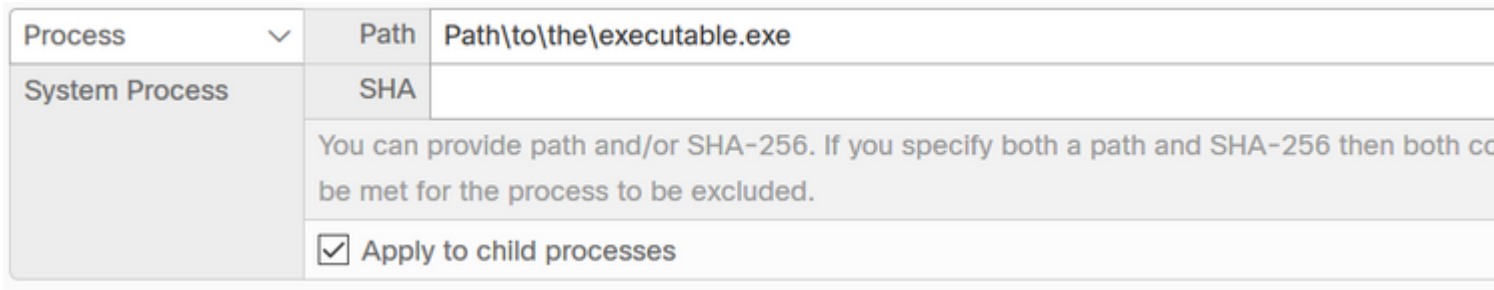
El motor System Process Protection está disponible en la versión 6.0.5 del conector y protege los siguientes procesos de Windows:

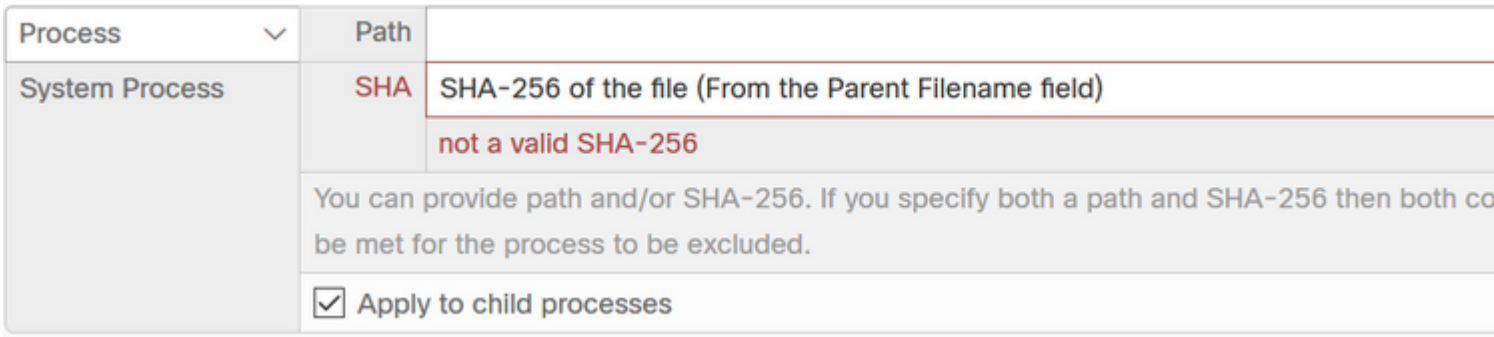
- Subsistema del Administrador de sesiones (smss.exe)
- Subsistema cliente/servidor en tiempo de ejecución (csrss.exe)
- Subsistema de autoridad de seguridad local (lsass.exe)
- Aplicación de inicio de sesión de Windows (winlogon.exe)
- Aplicación de inicio de Windows (wininit.exe)

Esta imagen muestra un evento SPP.



Exclusión de SPP

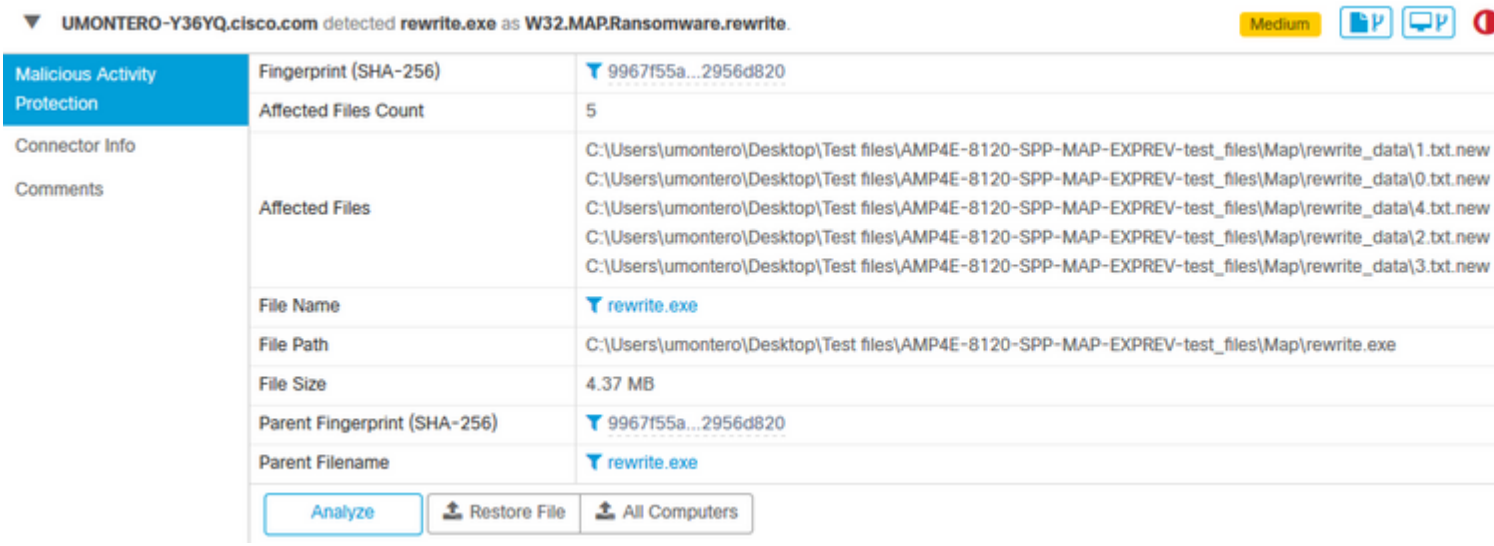




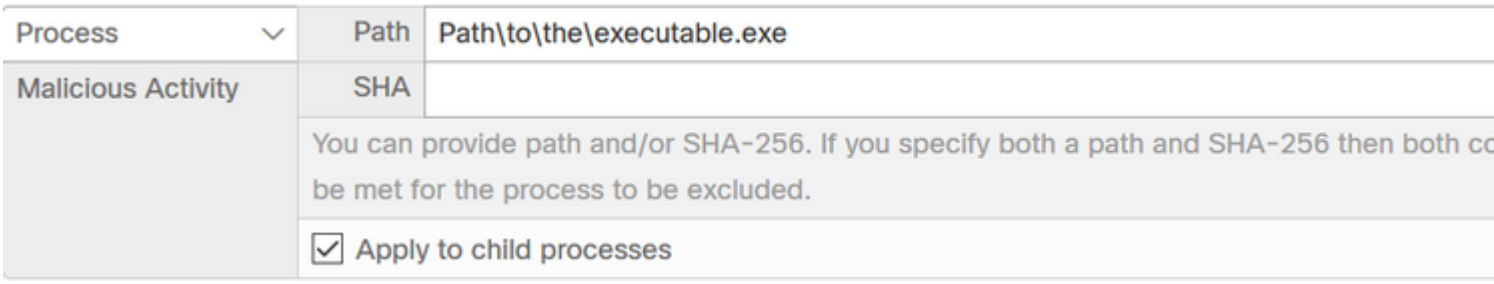
Protección frente a actividades maliciosas (MAP)

Motor de protección contra actividad maliciosa (MAP), que protege su terminal de un ataque de ransomware. Identifica acciones o procesos maliciosos cuando se ejecutan y protege sus datos contra el cifrado.

En esta imagen se muestra un evento MAP.



Exclusión de MAP

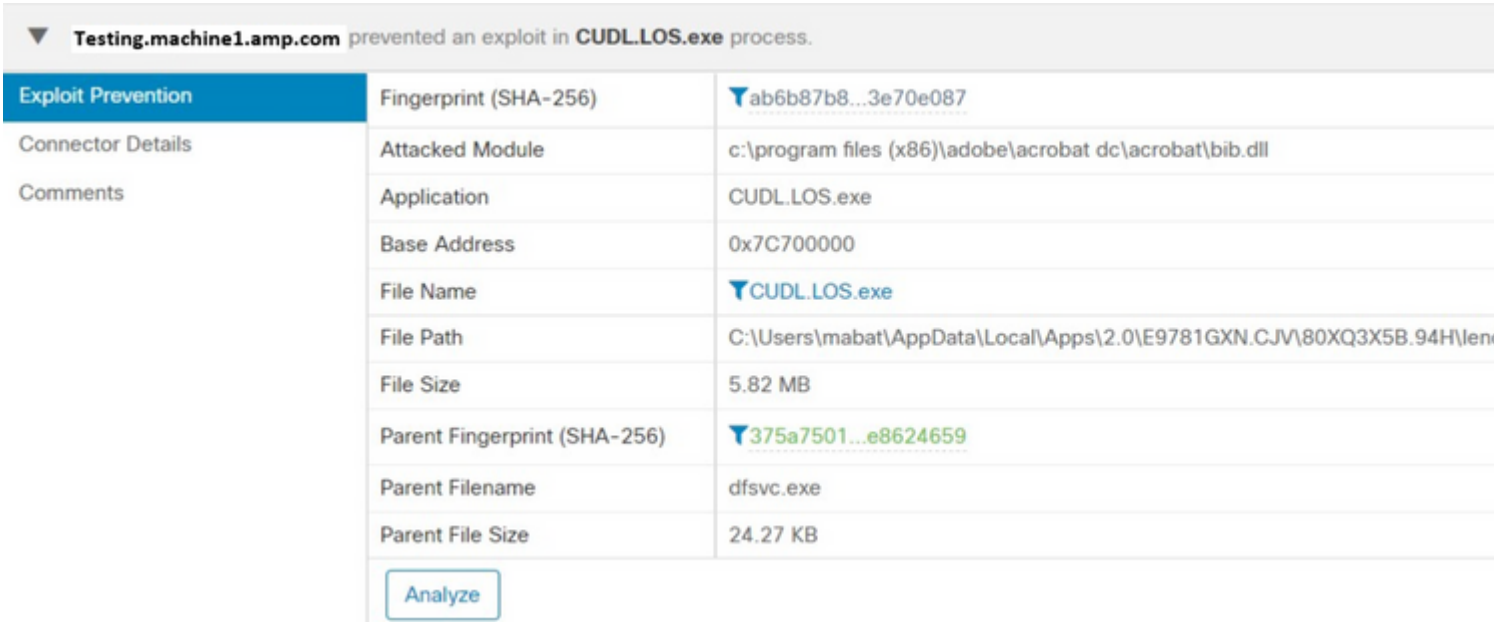


> **Precaución**: utilice este tipo de exclusión con precaución y después de confirmar que la detección no es maliciosa.

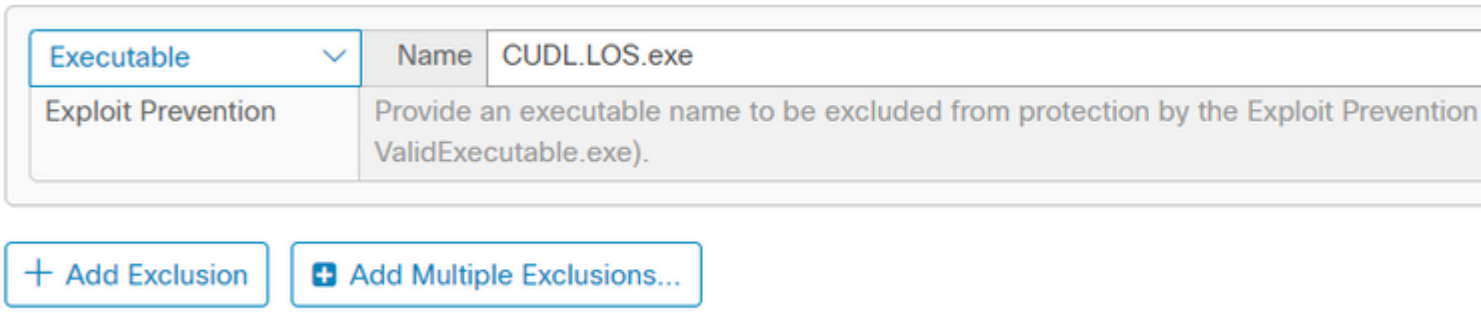
Prevención de vulnerabilidades (Exprev)

El motor de prevención de vulnerabilidades protege los terminales frente a los ataques de inyección de memoria que suelen utilizar el malware y otros ataques de día cero en software sin parches vulnerabilidades. Cuando detecte un ataque contra un proceso protegido, se bloqueará y generará un evento, pero no habrá una cuarentena.

En esta imagen se muestra un evento Exprev.



Exclusión de Exprev

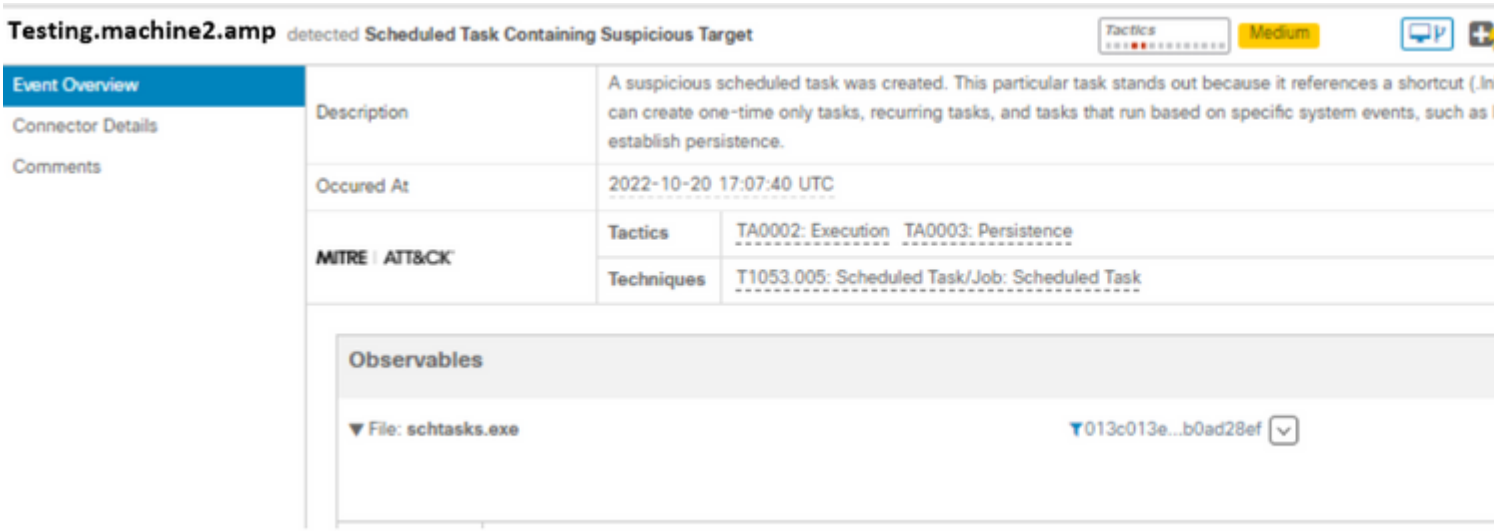


Precaución: utilice esta exclusión siempre que confíe en la actividad del módulo o la aplicación afectados.

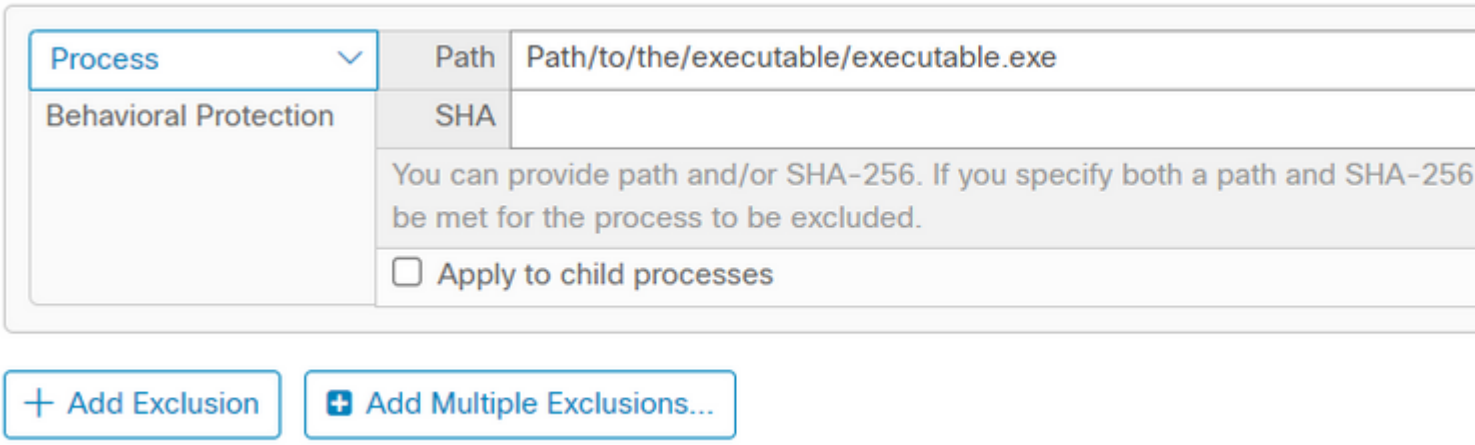
Protección del comportamiento (BP)

El motor de protección del comportamiento mejora la capacidad de detectar y detener amenazas de forma conductual. Aumenta la capacidad de detectar ataques que se producen "fuera de la tierra" y proporciona una respuesta más rápida a los cambios en el panorama de amenazas mediante actualizaciones de firmas.

En esta imagen se muestra un evento de PA.



exclusión de PA



Información Relacionada

- **Para obtener más información sobre la configuración de directivas, acceda a la guía del usuario**
- **Creación de exclusiones en vídeo de Cisco Secure Endpoint Connector**
- **Soporte Técnico y Documentación - Cisco Systems**

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).