Configurar e gerenciar exclusões no Cisco Secure Endpoint Connector

Contents

Introdução

Este documento descreve como criar a exclusão para os diferentes mecanismos no console do Cisco Secure Endpoint.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Modificar e aplicar uma lista de exclusão a uma política no console do Secure Endpoint
- convenção CSIDL do Windows

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Console Cisco Secure Endpoint 5.4.20211013
- Guia do usuário do Secure Endpoint revisão 15 de outubro de 2021

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer

comando.

Fluxo de trabalho de endpoint seguro

Em um alto nível de operações, o Cisco Secure Endpoint processa um arquivo Secure Hash Algorithm (SHA) nesta ordem através dos principais componentes do conector:

- Exclusões
- Mecanismo Tetra
- Controle de aplicativos (Lista de permissões/Lista de bloqueio)
- Mecanismo SHA
- Prevenção de exploração (Exprev) / Proteção contra atividades mal-intencionadas (MAP) / Proteção de processos do sistema / Mecanismo de rede (Correlação de fluxo de dispositivos)

> **Observação**: a exclusão ou a criação de Permitir/Bloquear lista depende de qual mecanismo detectou o arquivo.

Exclusões Mantidas da Cisco

As Exclusões Mantidas pela Cisco são criadas e mantidas pela Cisco para fornecer melhor compatibilidade entre o Secure Endpoint Connector e o antivírus, e produtos de segurança ou outros softwares.

Esses conjuntos de exclusões contêm diferentes tipos de exclusões para garantir o funcionamento adequado.

Você pode acompanhar as alterações executadas nessas exclusões no artigo Cisco-Mainheld Exclusion List Changes for Cisco Secure Endpoint Console.

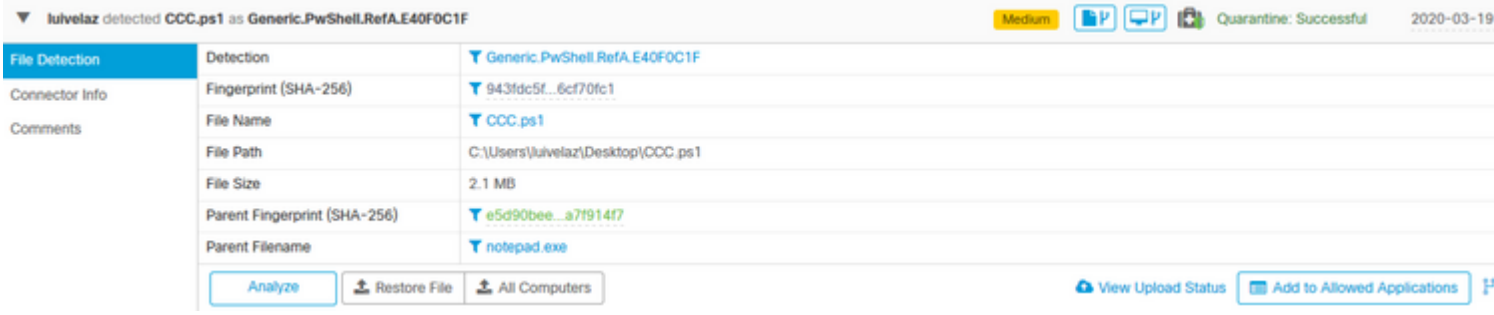
Exclusões personalizadas

Mecanismo de endpoint seguro

Verificação de arquivos (uso da CPU / detecções de arquivos) pelo mecanismo Tetra & SHA:

Use esses tipos de exclusões para evitar a detecção/quarentena de um arquivo ou para mitigar a alta utilização da CPU do Secure Endpoint.

O evento no console do Secure Endpoint é como mostrado na imagem.



> **Observação**: o CSIDL pode ser usado para exclusões. Consulte este documento da Microsoft para obter mais informações sobre o CSIDL.

Exclusão de Caminho

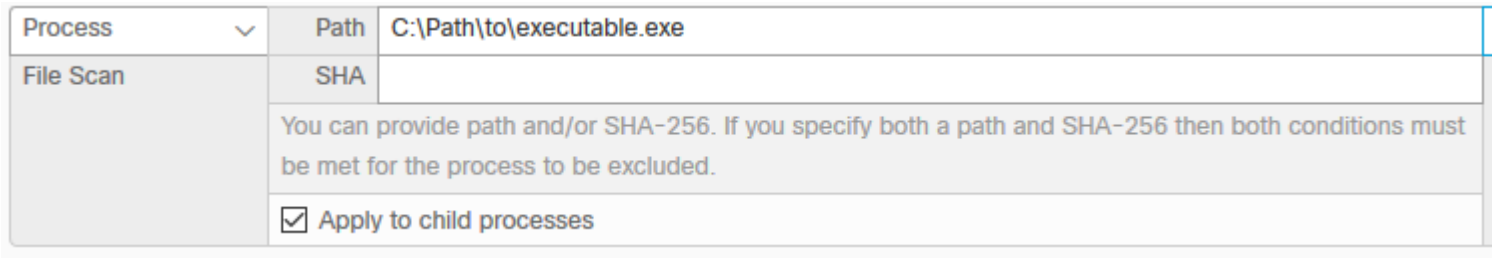
Exclusão de Curinga

Observação: a opção **Apply to all drive letters** é usada para aplicar também a exclusão a unidades [A-Z] conectadas ao sistema.

Exclusão de Extensão de Arquivo

Cuidado: use esse tipo de exclusão com cuidado, pois ele exclui todos os arquivos com a extensão de arquivo das varreduras, independentemente do local do caminho.

Processo: Exclusão de Verificação de Arquivo

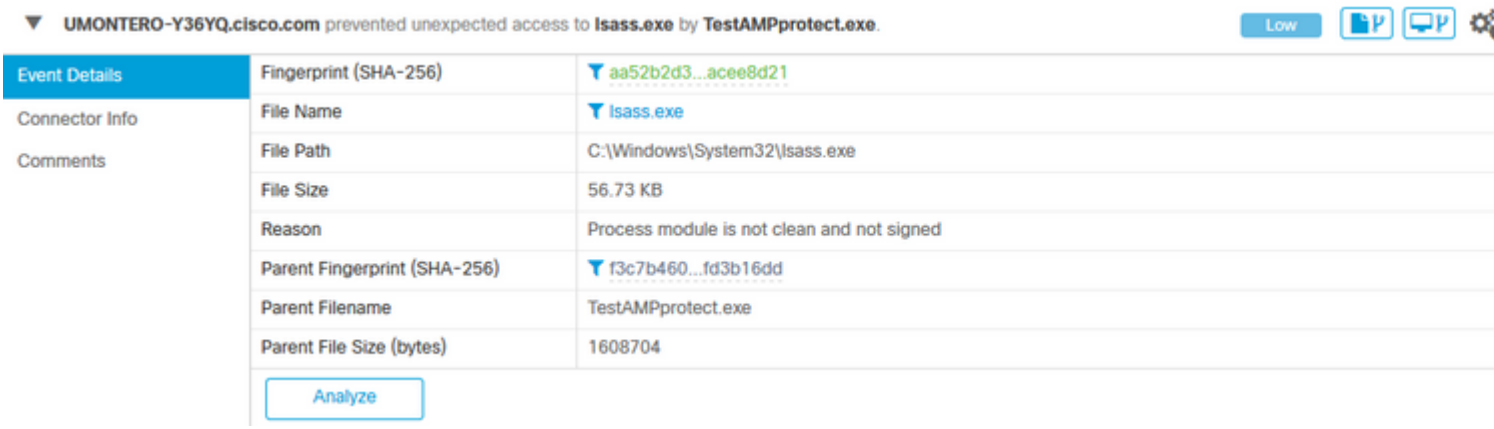


Proteção de processos do sistema (SPP)

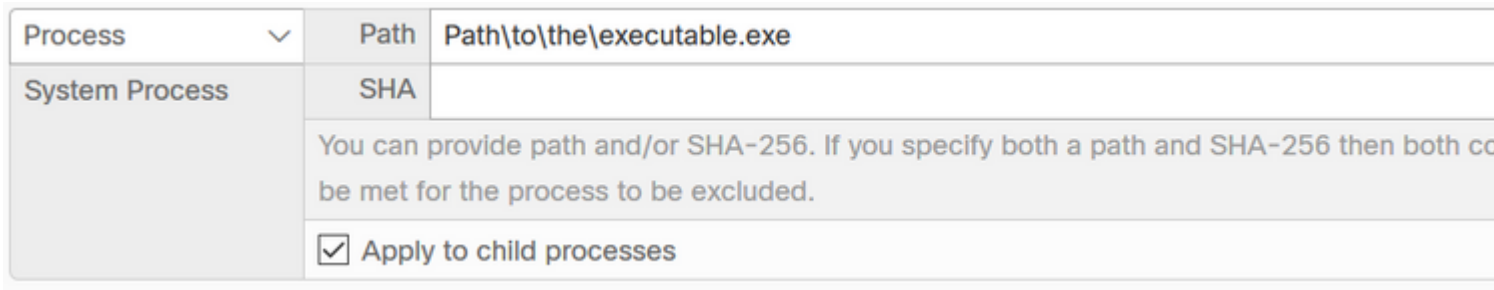
O mecanismo System Process Protection está disponível no conector versão 6.0.5 e protege os próximos processos do Windows:

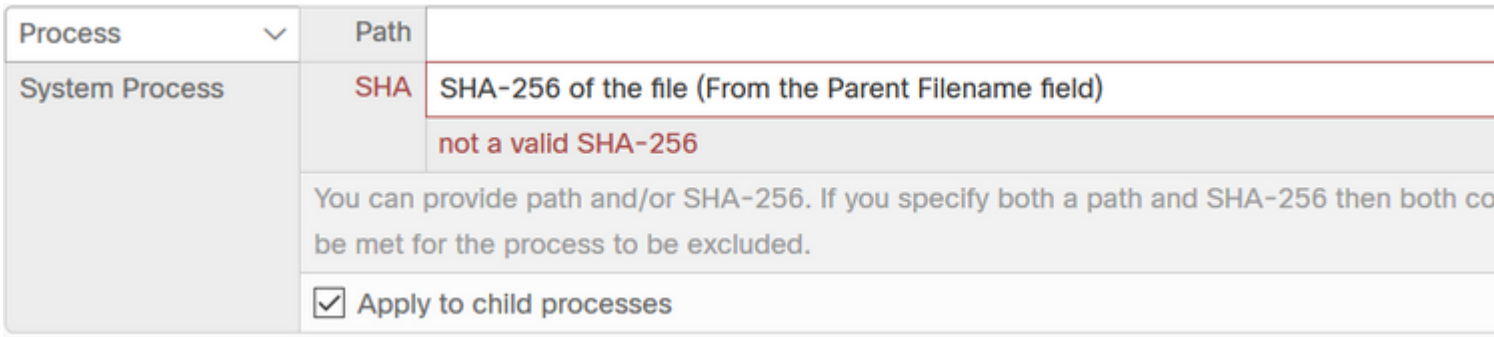
- Subsistema do Gerenciador de Sessões (smss.exe)
- Subsistema de Tempo de Execução Cliente/Servidor (csrss.exe)
- Subsistema de autoridade de segurança local (lsass.exe)
- Aplicativo de Logon do Windows (winlogon.exe)
- Aplicativo de Inicialização do Windows (wininit.exe)

Esta imagem mostra um evento SPP.



Exclusão SPP

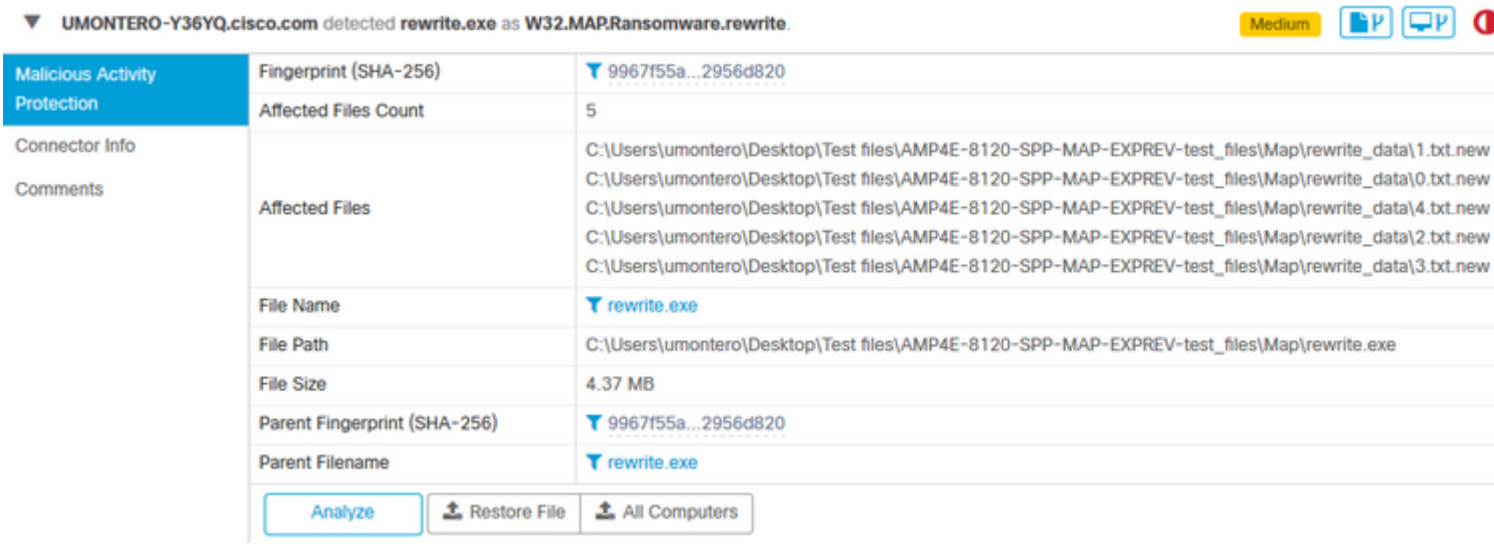




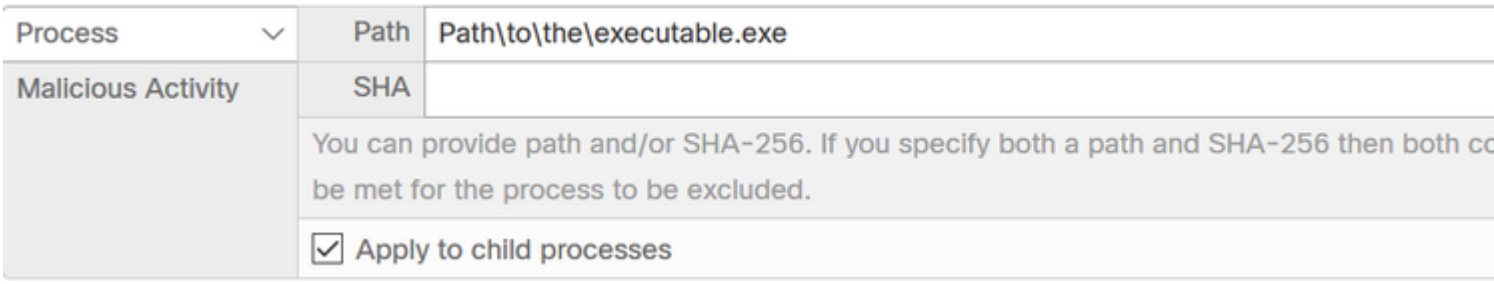
Proteção contra atividades mal-intencionadas (MAP)

Mecanismo de proteção contra atividades mal-intencionadas (MAP), defende seu endpoint contra um ataque de ransomware. Ele identifica ações ou processos mal-intencionados quando são executados e protege seus dados contra criptografia.

Um evento MAP é mostrado nesta imagem.



Exclusão de MAP

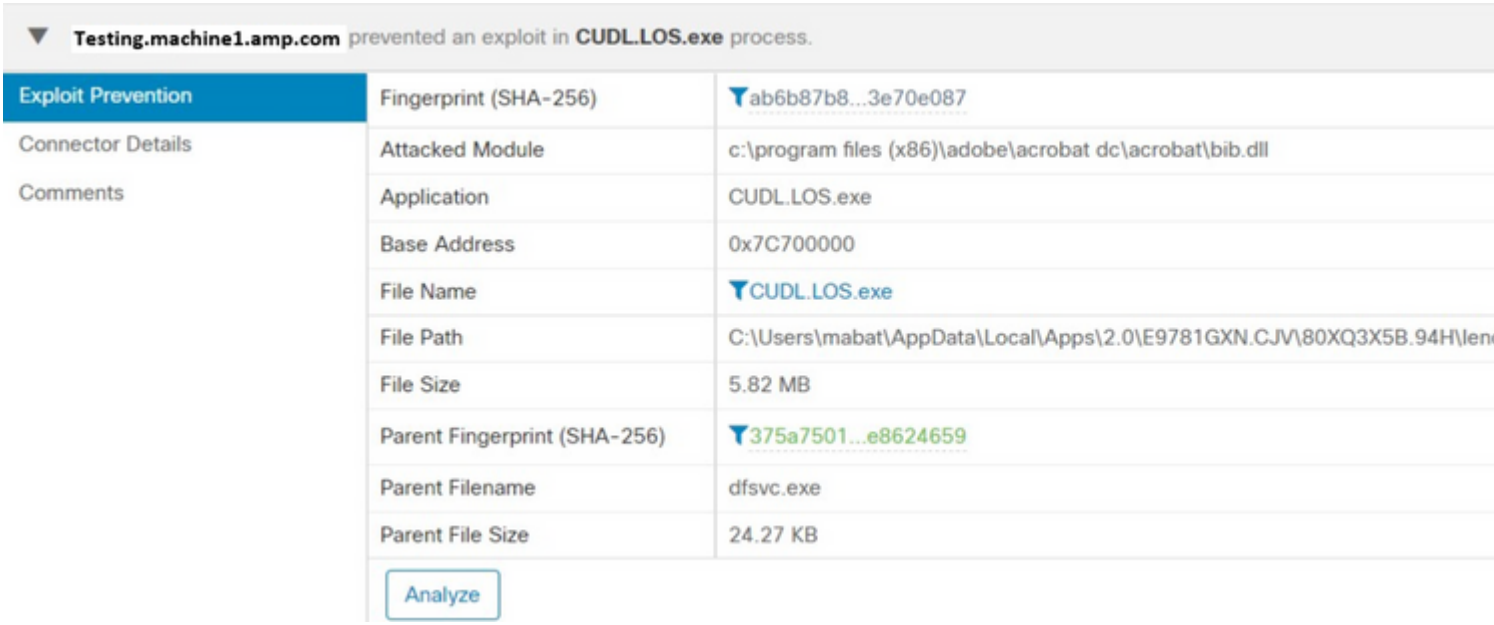


> **Cuidado**: use esse tipo de exclusão com cuidado e depois de confirmar que a detecção realmente não é mal-intencionada.

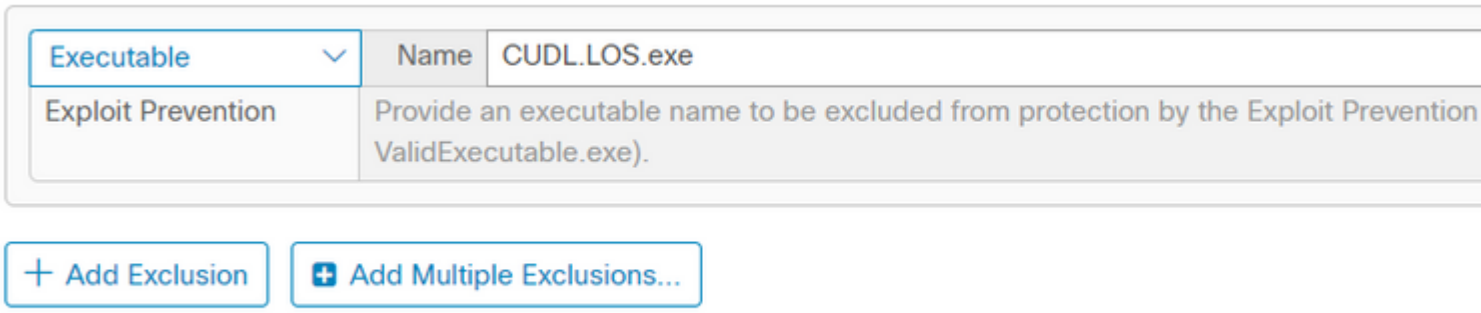
Prevenção de exploração (Exprev)

O mecanismo de prevenção de exploração defende seus endpoints contra ataques de injeção de memória comumente usados por malware e outros ataques de dia zero em software sem patches vulnerabilidades. Ao detectar um ataque contra um processo protegido, ele será bloqueado e gerará um evento, mas não haverá uma quarentena.

Um evento Exprev é mostrado nesta imagem.



Exclusão de Exprev

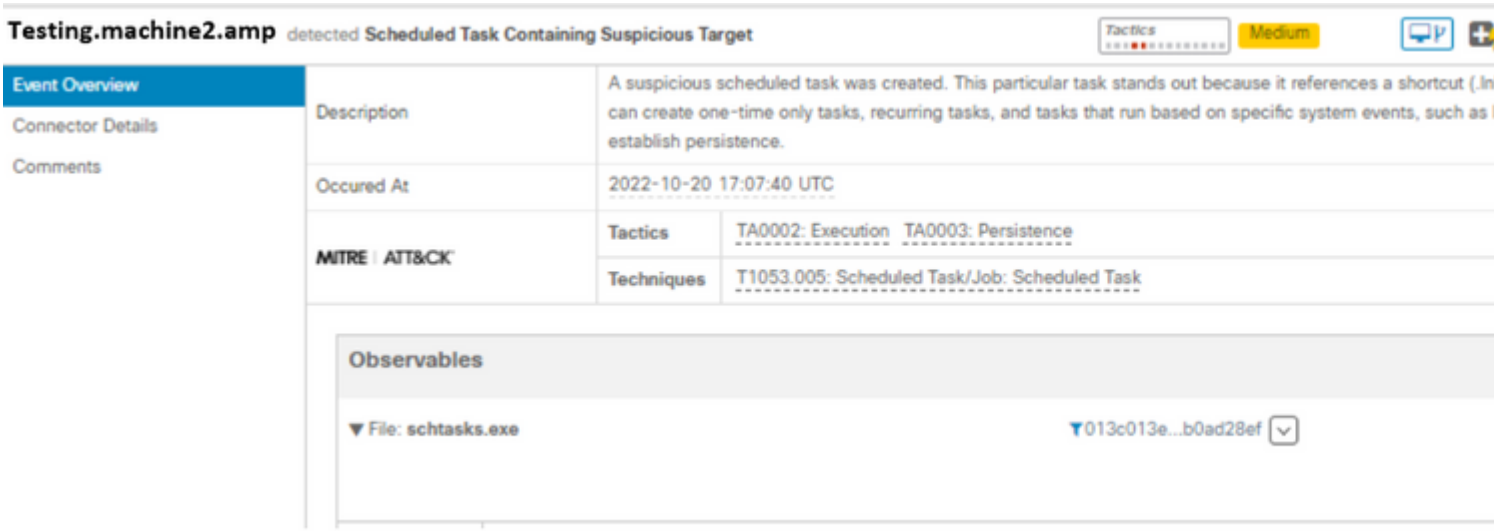


Cuidado: use esta exclusão sempre que confiar na atividade no módulo/aplicativo afetado.

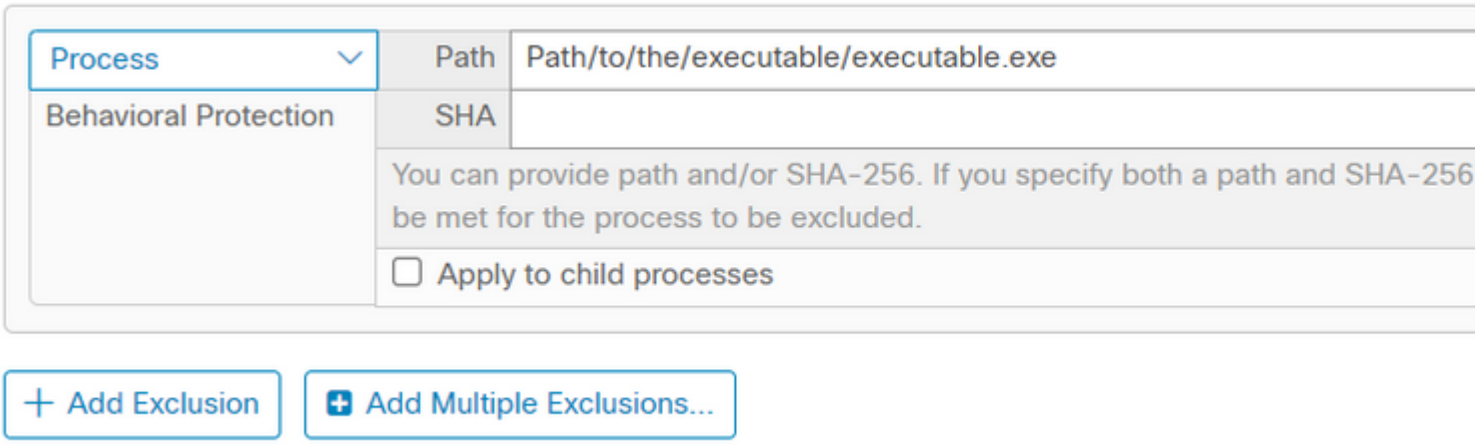
Proteção comportamental (BP)

O mecanismo de proteção comportamental aprimora a capacidade de detectar e interromper ameaças de forma comportamental. Ela aumenta a capacidade de detectar ataques "vivendo fora da terra" e oferece resposta mais rápida às mudanças no cenário de ameaças por meio de atualizações de assinaturas.

Um evento BP é mostrado nesta imagem.



Exclusão BP



Informações Relacionadas

- **Para obter mais informações sobre a configuração de diretivas, navegue até o Guia do usuário**
- **Vídeo Create Exclusions in Cisco Secure Endpoint Connector (Criar exclusões no Cisco Secure Endpoint Connector)**
- **Suporte Técnico e Documentação - Cisco Systems**

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.