Configurazione e gestione delle esclusioni in Cisco Secure Endpoint Connector

Sommario

Introduzione

In questo documento viene descritto come creare l'esclusione per i diversi motori sulla console Cisco Secure Endpoint.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Modificare e applicare un elenco di esclusione a un criterio nella console dell'endpoint sicuro
- Convenzione CSIDL di Windows

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Secure Endpoint console 5.4.20211013
- Secure Endpoint User Guide - revisione 15 ott 2021

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei

comandi.

Flusso di lavoro Secure Endpoint

In caso di operazioni di alto livello, Cisco Secure Endpoint elabora un file SHA (Secure Hash Algorithm) in questo ordine tramite i componenti principali del connettore:

- Esclusioni
- Motore Tetra
- Controllo applicazione (elenco Consenti/elenco Blocca)
- Motore SHA
- Prevenzione degli attacchi (Exprev) / Protezione dalle attività dannose (MAP) / Protezione dei processi di sistema / Motore di rete (correlazione flusso dispositivo)

> **Nota**: l'esclusione o la creazione di un elenco indirizzi consentiti/bloccati dipende dal motore che ha rilevato il file.

Esclusioni gestite da Cisco

Le esclusioni gestite da Cisco sono create e gestite da Cisco per fornire una migliore compatibilità tra Secure Endpoint Connector e l'antivirus, e i prodotti di sicurezza, o altri software.

Questi set di esclusione contengono diversi tipi di esclusioni per garantire il corretto funzionamento.

Per tenere traccia delle modifiche apportate a queste esclusioni, vedere l'articolo Cisco-Managed Exclusion List Changes for Cisco Secure Endpoint Console.

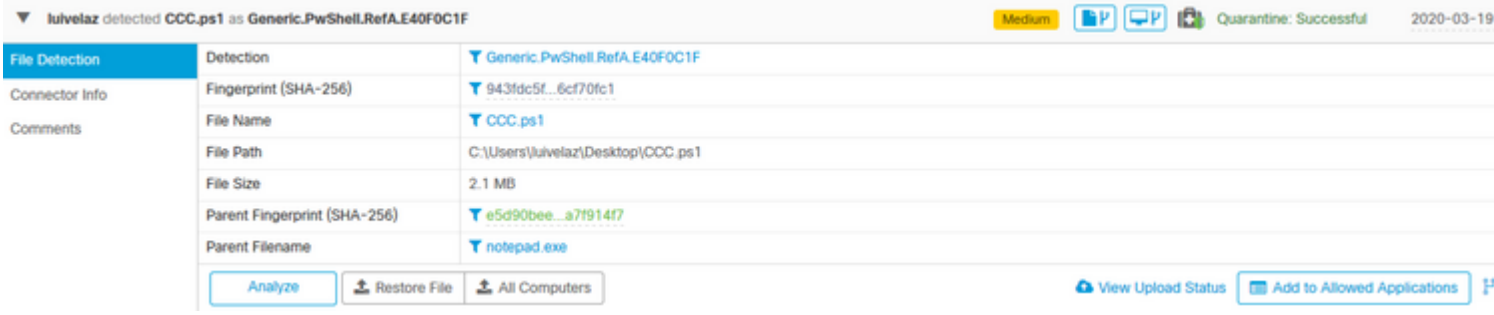
Esclusioni personalizzate

Secure Endpoint Engine

Scansione dei file (utilizzo CPU/rilevamento file) da parte del motore Tetra & SHA:

Utilizzare questi tipi di esclusioni per evitare il rilevamento/la quarantena di un file o per ridurre il numero di CPU elevato dell'endpoint sicuro.

L'evento sulla console di Secure Endpoint è come mostrato nell'immagine.



> **Nota**: CSIDL può essere utilizzato per le esclusioni. Per ulteriori informazioni su CSIDL, consultare questo documento Microsoft.

Esclusione percorso

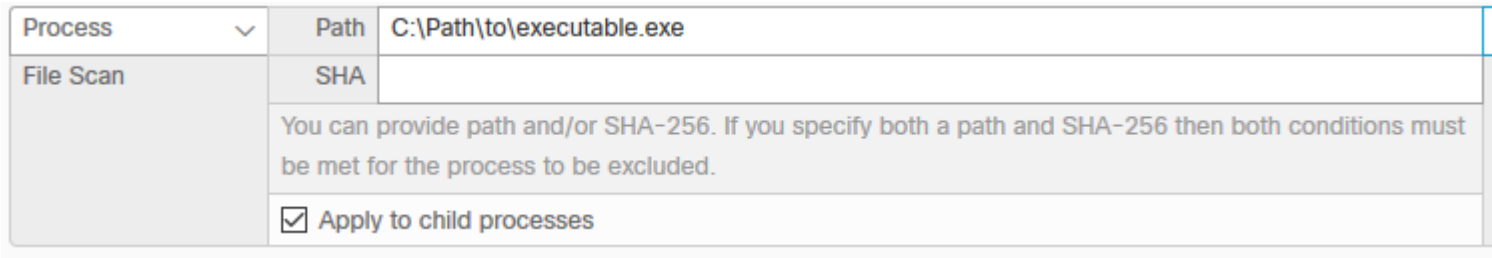
Esclusione caratteri jolly

Nota: l'opzione **Applica a tutte le lettere di unità** viene utilizzata anche per applicare l'esclusione alle unità [A-Z] collegate al sistema.

Esclusione estensione file

Attenzione: utilizzare questo tipo di esclusione con cautela in quanto esclude tutti i file con estensione dalle analisi indipendentemente dalla posizione del percorso.

Processo: Esclusione analisi file

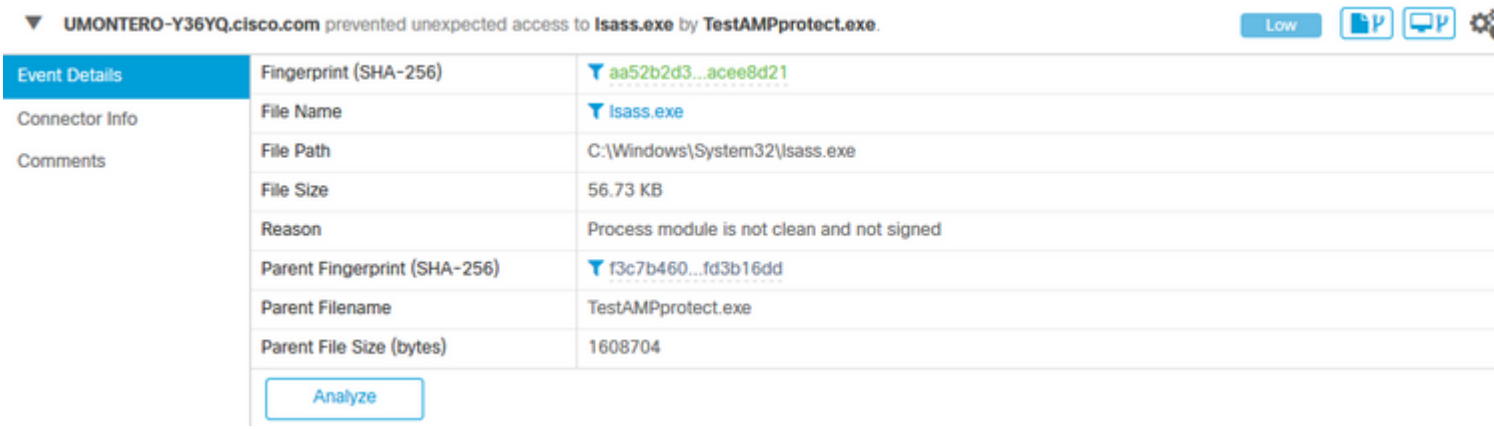


SPP (System Process Protection)

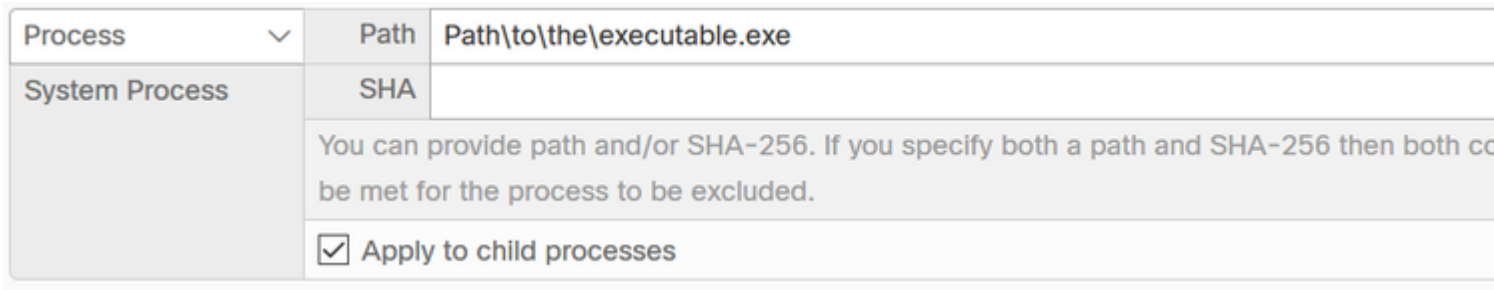
Il motore di protezione dei processi di sistema è disponibile dalla versione 6.0.5 del connettore e protegge i successivi processi Windows:

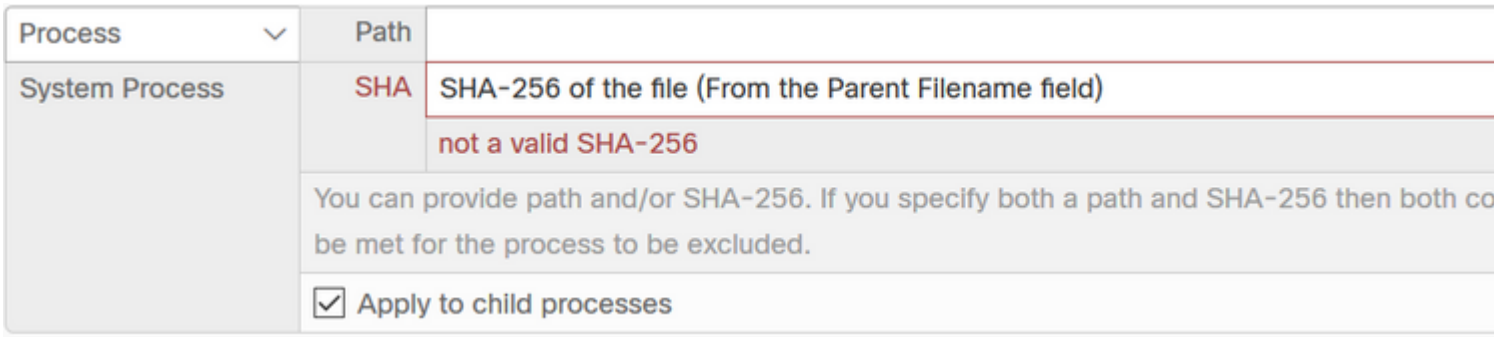
- Sottosistema di gestione delle sessioni (smss.exe)
- Sottosistema di runtime client/server (csrss.exe)
- Sottosistema autorità di sicurezza locale (lsass.exe)
- Applicazione di accesso a Windows (winlogon.exe)
- Applicazione di avvio di Windows (wininit.exe)

Nell'immagine è illustrato un evento SPP.



Esclusione SPP

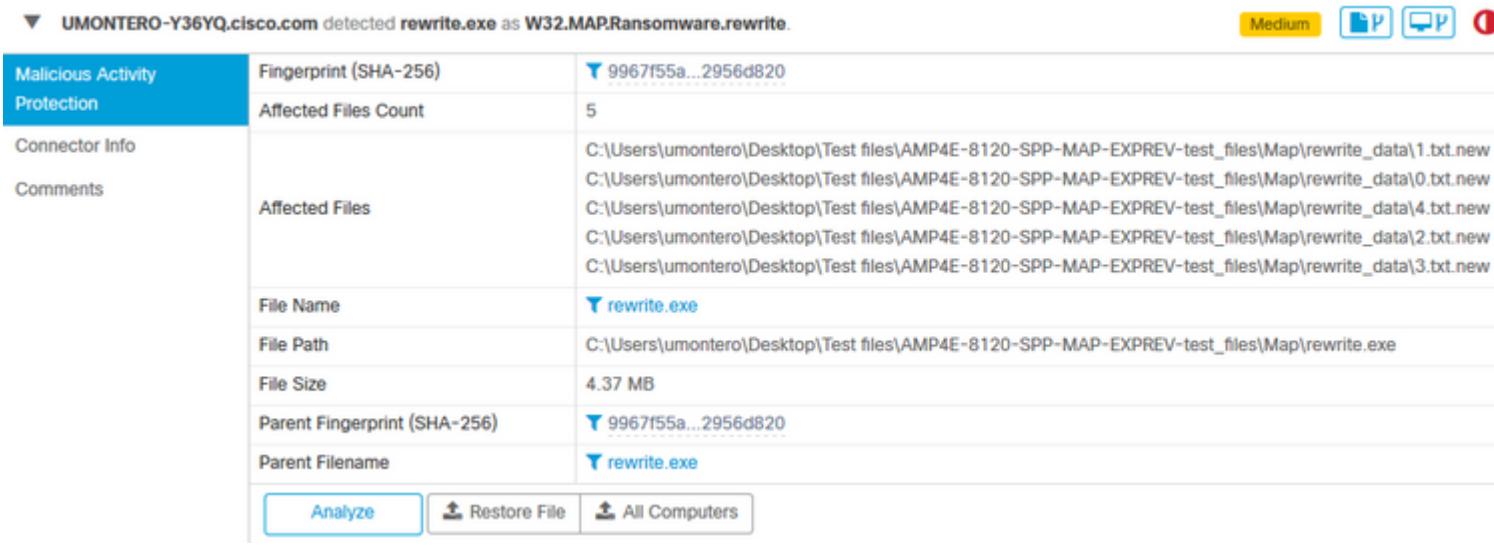




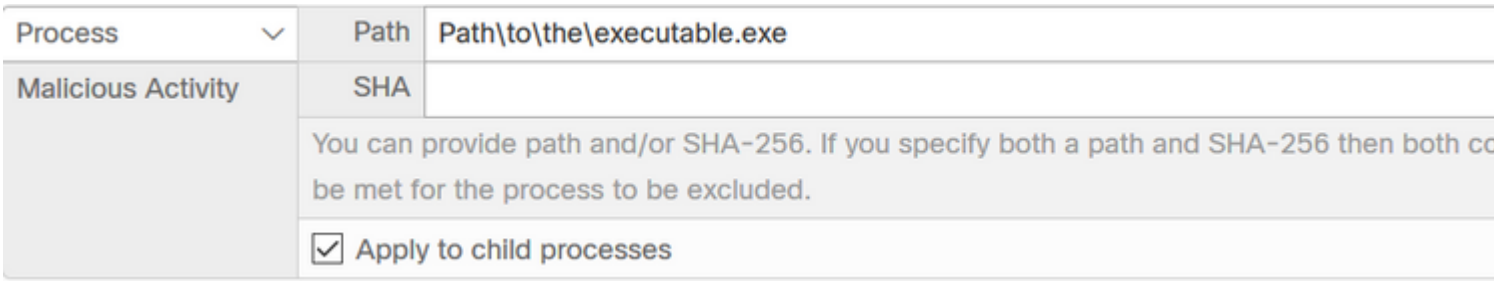
Protezione dalle attività dannose (MAP)

Malicious Activity Protection (MAP), difende l'endpoint da un attacco ransomware. Identifica azioni o processi dannosi durante l'esecuzione e protegge i dati dalla crittografia.

In questa immagine viene visualizzato un evento MAP.



Esclusione MAP

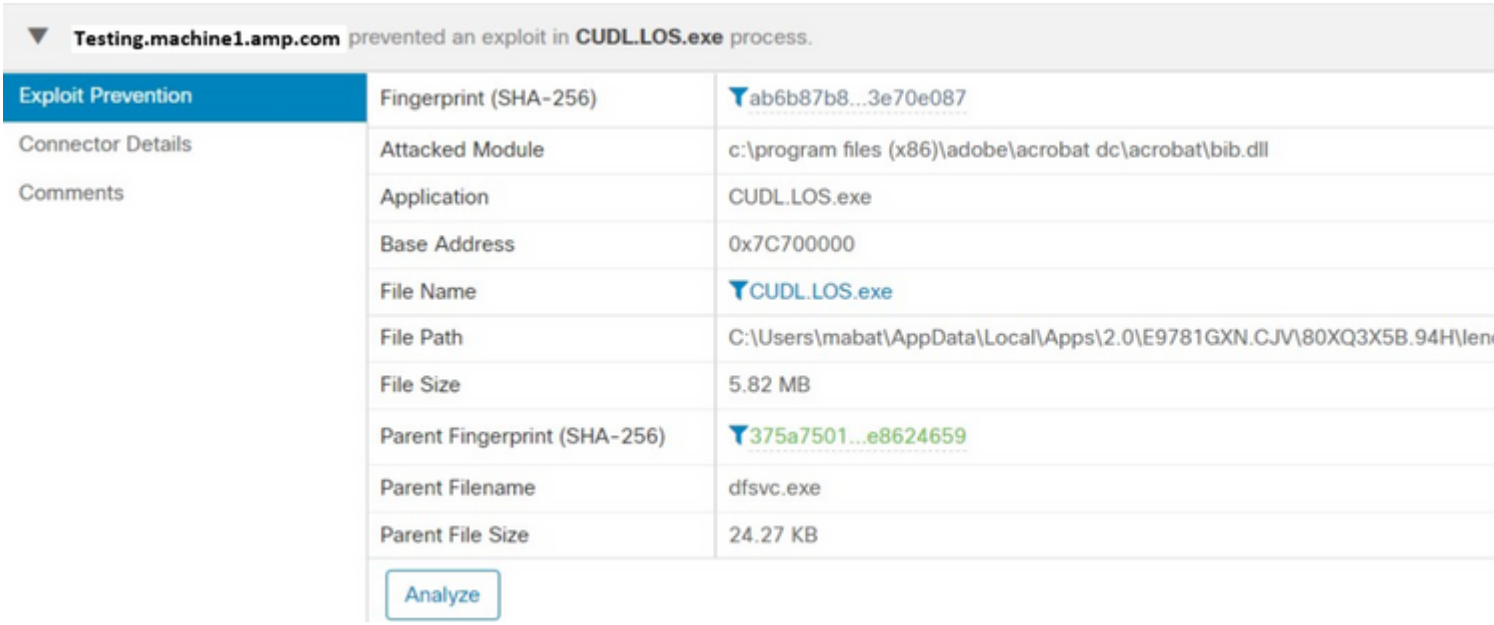


> **Attenzione**: utilizzare questo tipo di esclusione con cautela e dopo aver verificato che il rilevamento non è dannoso.

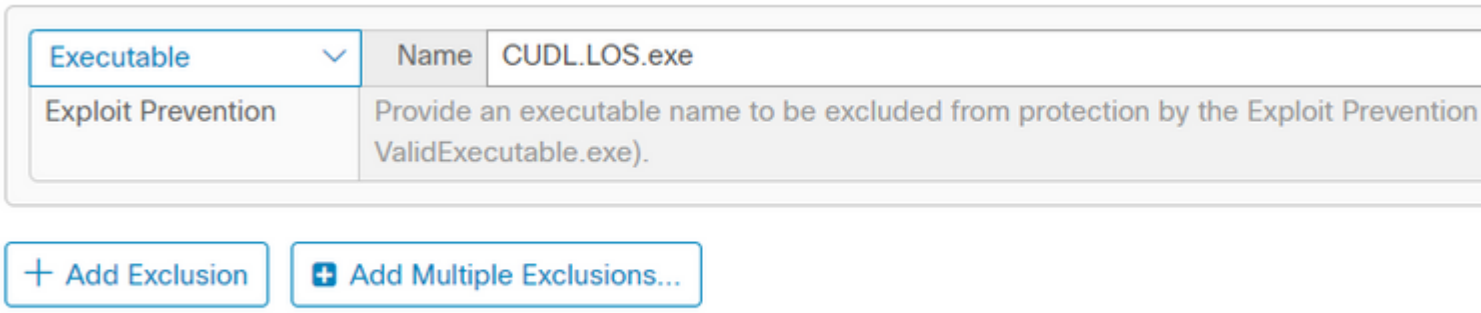
Exprev (Exploit Prevention)

Il motore di prevenzione degli attacchi difende gli endpoint dagli attacchi di aggiunta di memoria comunemente utilizzati dal malware e da altri attacchi a giorno zero su software senza patch vulnerabilità. Quando rileva un attacco contro un processo protetto, viene bloccato e generato un evento, ma non viene messa in quarantena.

Nell'immagine è visualizzato un evento Exprev.



Esclusione espressione

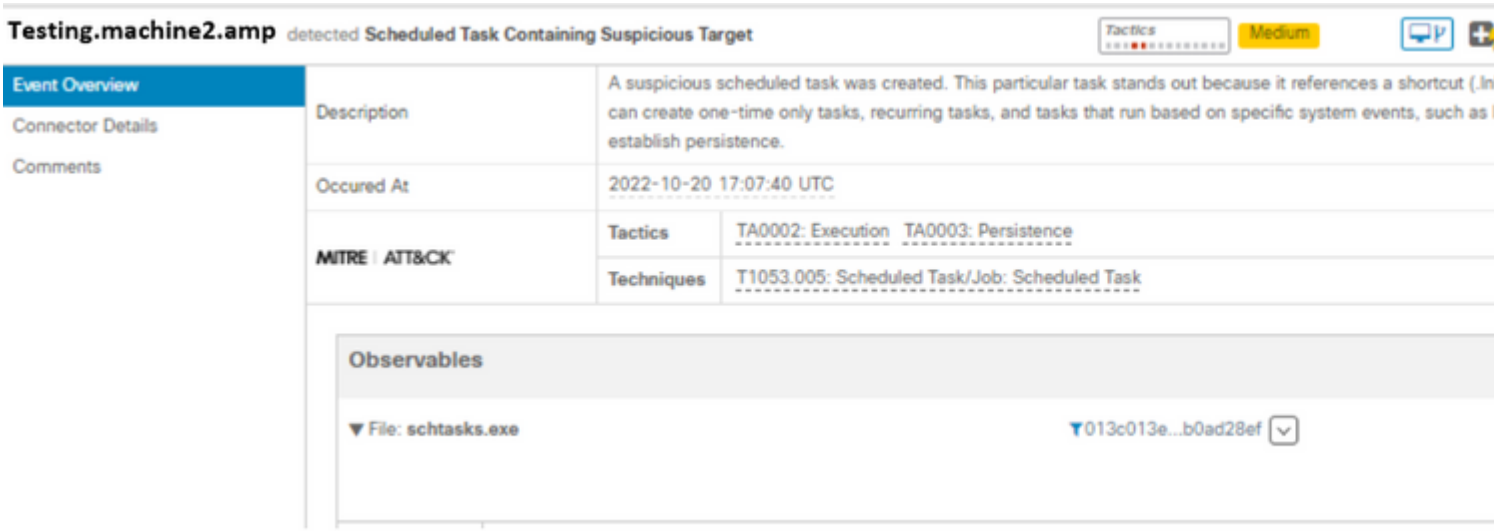


Attenzione: utilizzare questa esclusione ogni volta che si considera attendibile l'attività sul modulo/applicazione interessata.

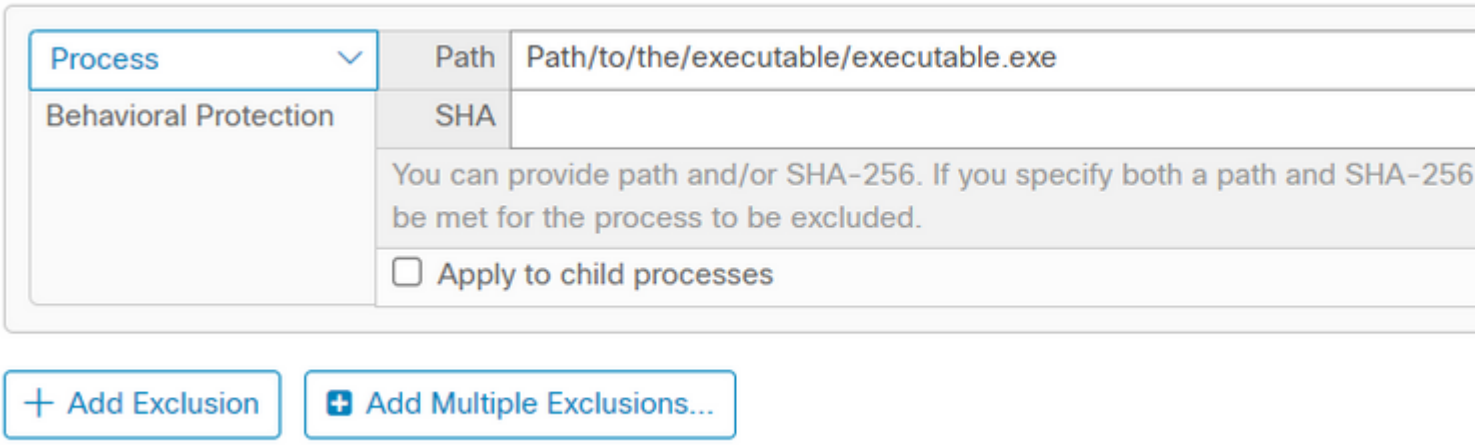
Protezione comportamentale (BP)

Il motore di protezione comportamentale migliora la capacità di rilevare e arrestare le minacce in modo comportamentale. Rafforza la capacità di rilevare gli attacchi "fuori terra" e fornisce tempi di risposta più rapidi ai cambiamenti nel panorama delle minacce tramite aggiornamenti delle firme.

In questa immagine viene mostrato un evento BP.



Esclusione BP



Informazioni correlate

- **Per ulteriori informazioni sulla configurazione dei criteri, consultare la Guida dell'utente**
- **Creare esclusioni nel video di Cisco Secure Endpoint Connector**
- **Documentazione e supporto tecnico â€“ Cisco Systems**

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).