Konfigurieren und Verwalten von Ausschlüssen in Cisco Secure Endpoint Connector

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie den Ausschluss für die verschiedenen Engines auf der Cisco Secure Endpoint-Konsole erstellen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Ändern und Anwenden einer Ausschlussliste auf eine Richtlinie in der Konsole für sichere Endgeräte
- Windows CSIDL-Konvention

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Secure Endpoint-Konsole 5.4.20211013
- Secure Endpoint User Guide, Version vom 15. Oktober 2021

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die

möglichen Auswirkungen aller Befehle kennen.

Workflow für sichere Endgeräte

Auf hoher Betriebsebene verarbeitet Cisco Secure Endpoint eine Datei mit dem Secure Hash Algorithm (SHA) in dieser Reihenfolge über die Hauptkomponenten des Connectors:

- Ausschlüsse
- Tetra-Motor
- Anwendungskontrolle (Zulassungsliste/Sperrliste)
- SHA-Engine
- Exploit-Schutz (Exprev)/Schutz vor schädlichen Aktivitäten (MAP)/Schutz von Systemprozessen/Netzwerk-Engine (Device Flow Correlation)

Hinweis: Die Erstellung von Ausschlüssen oder Listen für Zulassen/Sperren hängt davon ab, von welcher Engine die Datei erkannt wurde.

Von Cisco beibehaltene Ausschlüsse

Von Cisco verwaltete Ausschlüsse werden von Cisco erstellt und verwaltet, um die Kompatibilität zwischen Secure Endpoint Connector und Antivirus-, Sicherheits- und anderer Software zu verbessern.

Diese Ausschlusssätze enthalten verschiedene Arten von Ausschlüssen, um einen ordnungsgemäßen Betrieb zu gewährleisten.

Sie können die an diesen Ausschlüssen vorgenommenen Änderungen im Artikel Cisco-Maintained Exclusion List Changes for Cisco Secure Endpoint Console nachverfolgen.

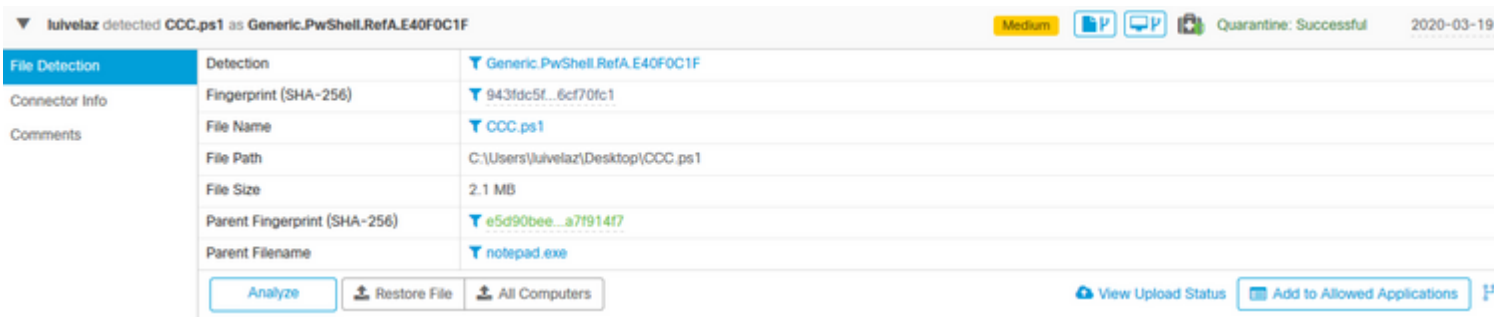
Benutzerdefinierte Ausschlüsse

Secure Endpoint Engine

Dateisuche (CPU-Auslastung/Dateierkennung) durch Tetra & SHA Engine:

Verwenden Sie diese Ausschlussarten, um die Erkennung/Quarantäne einer Datei zu vermeiden oder die hohe CPU-Auslastung für sichere Endgeräte zu minimieren.

Das Ereignis auf der Konsole für sichere Endgeräte ist wie im Bild dargestellt.



Hinweis: CSIDL kann für Ausschlüsse verwendet werden. Weitere Informationen zu CSIDL finden Sie in diesem Microsoft-Dokument.

Pfadausschluss

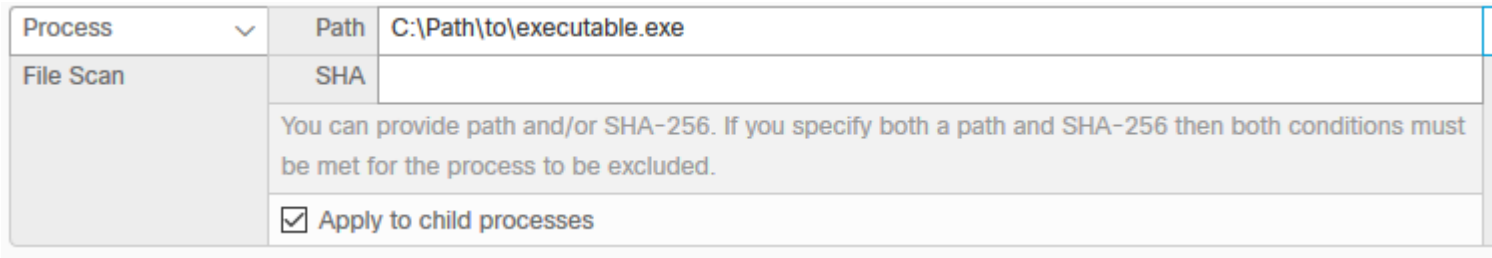
Platzhalterausschluss

Hinweis: Die Option **Auf alle Laufwerkbuchstaben anwenden** wird verwendet, um den Ausschluss auch auf Laufwerke [A-Z] anzuwenden, die an das System angeschlossen sind.

Dateierweiterungsausschluss

Achtung: Verwenden Sie diese Art des Ausschlusses mit Vorsicht, da alle Dateien mit der Dateierweiterung von der Suche unabhängig vom Pfad ausgeschlossen werden.

Prozess: Ausschluss der Dateisuche

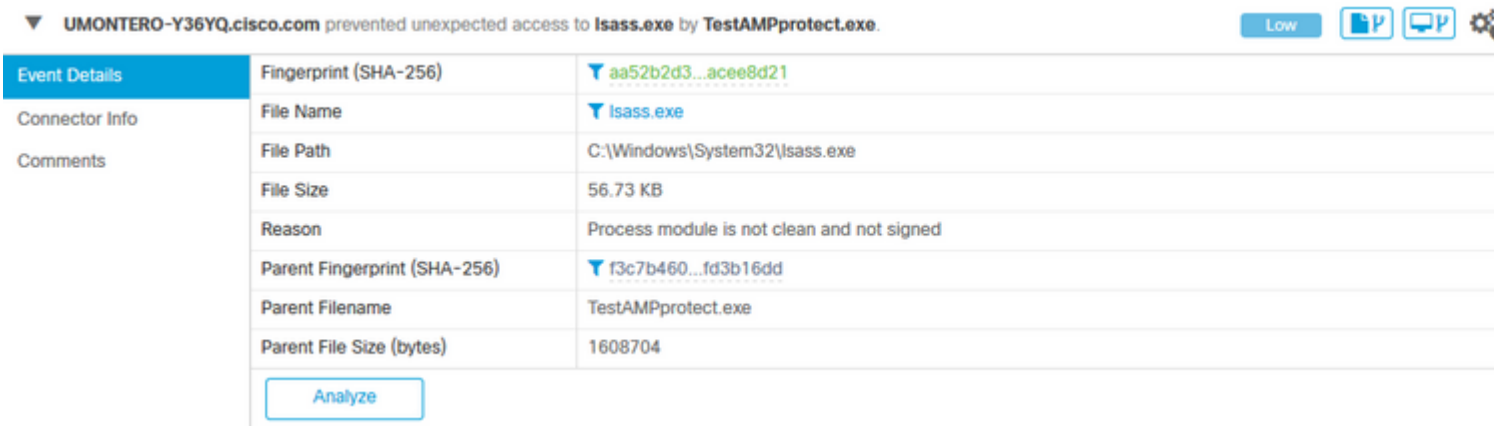


System Process Protection (SPP)

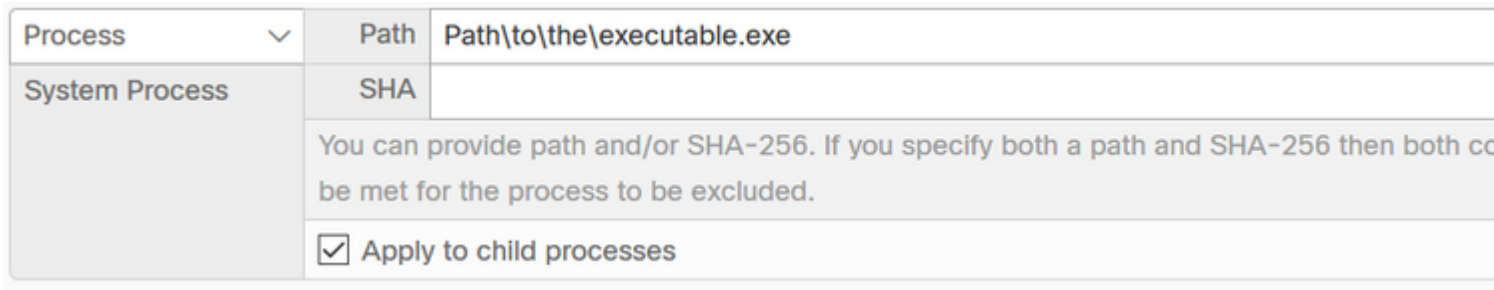
Das System Process Protection-Modul ist ab Connector-Version 6.0.5 verfügbar und schützt die nächsten Windows-Prozesse:

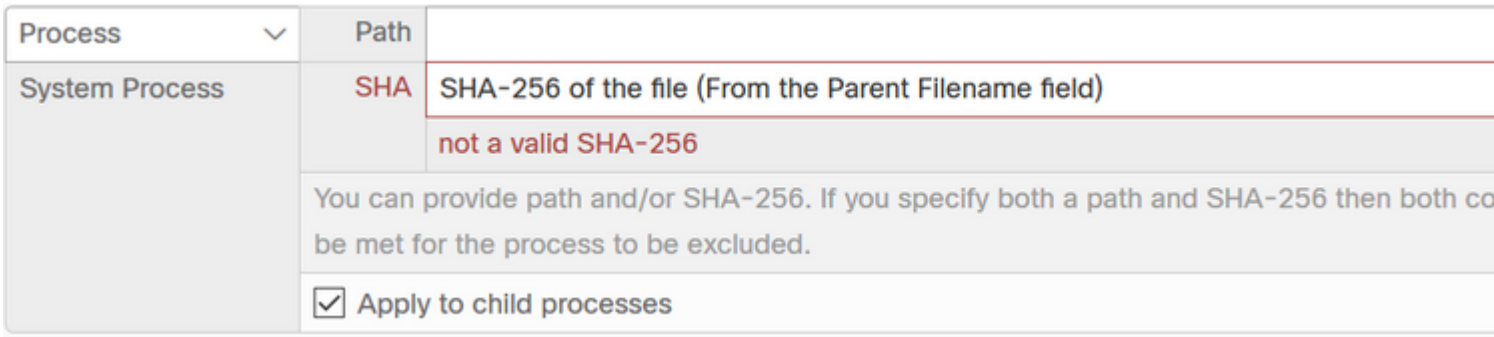
- Session Manager-Subsystem (smss.exe)
- Client/Server Runtime Subsystem (csrss.exe)
- Subsystem der lokalen Sicherheitsbehörde (lsass.exe)
- Windows-Anmeldeanwendung (winlogon.exe)
- Windows-Startanwendung (wininit.exe)

Dieses Bild zeigt ein SPP-Ereignis.



SPP-Ausschluss

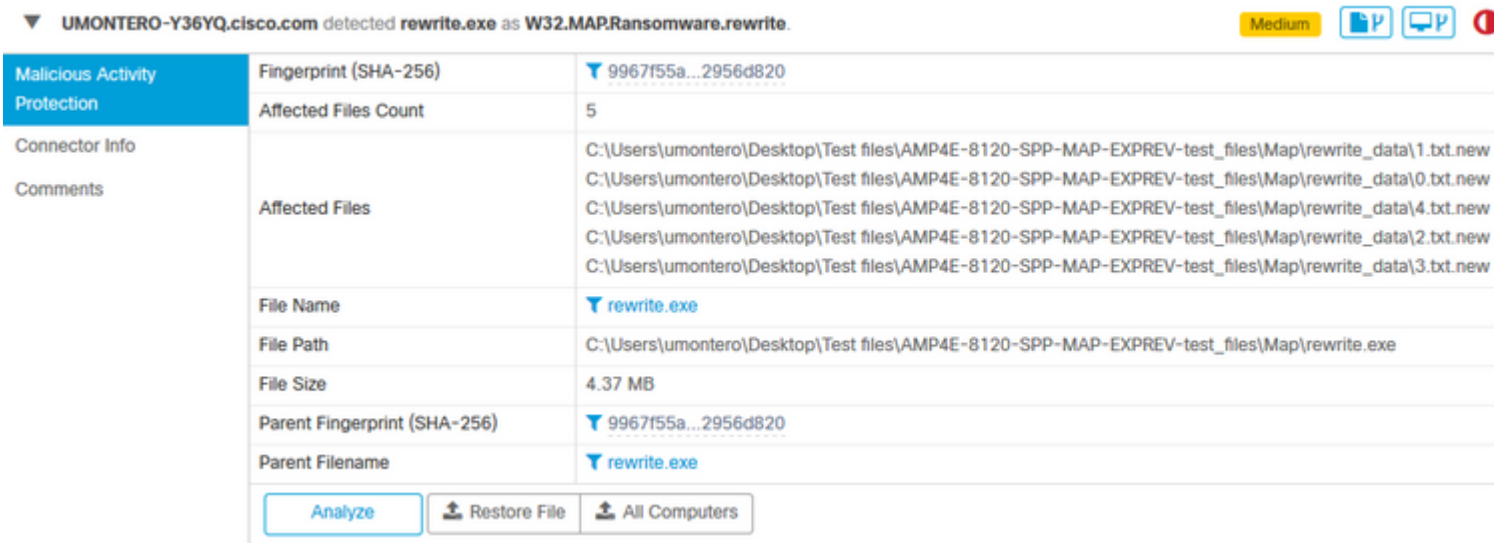




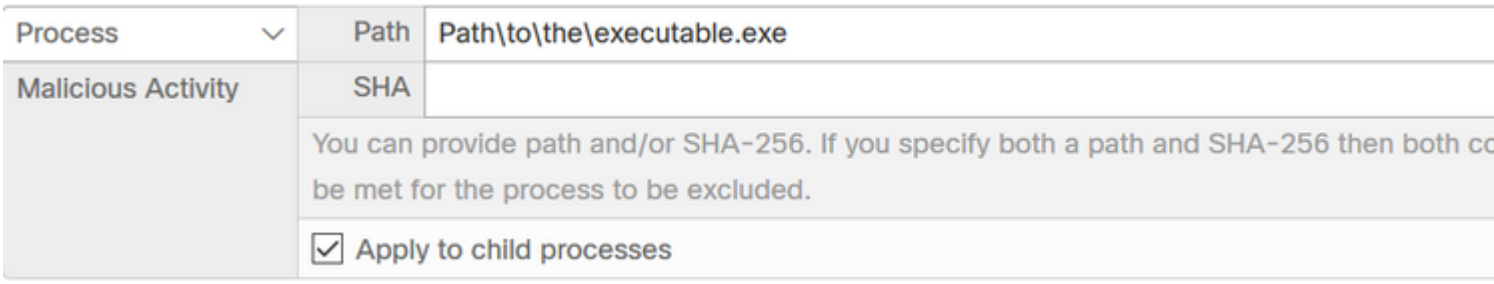
Schutz vor bösartigen Aktivitäten (MAP)

Malicious Activity Protection (MAP)-Engine, schützt Ihr Endgerät vor einem Ransomware-Angriff. Es identifiziert schädliche Aktionen oder Prozesse, wenn diese ausgeführt werden, und schützt Ihre Daten vor Verschlüsselung.

In diesem Bild wird ein MAP-Ereignis angezeigt.



MAP-Ausschluss

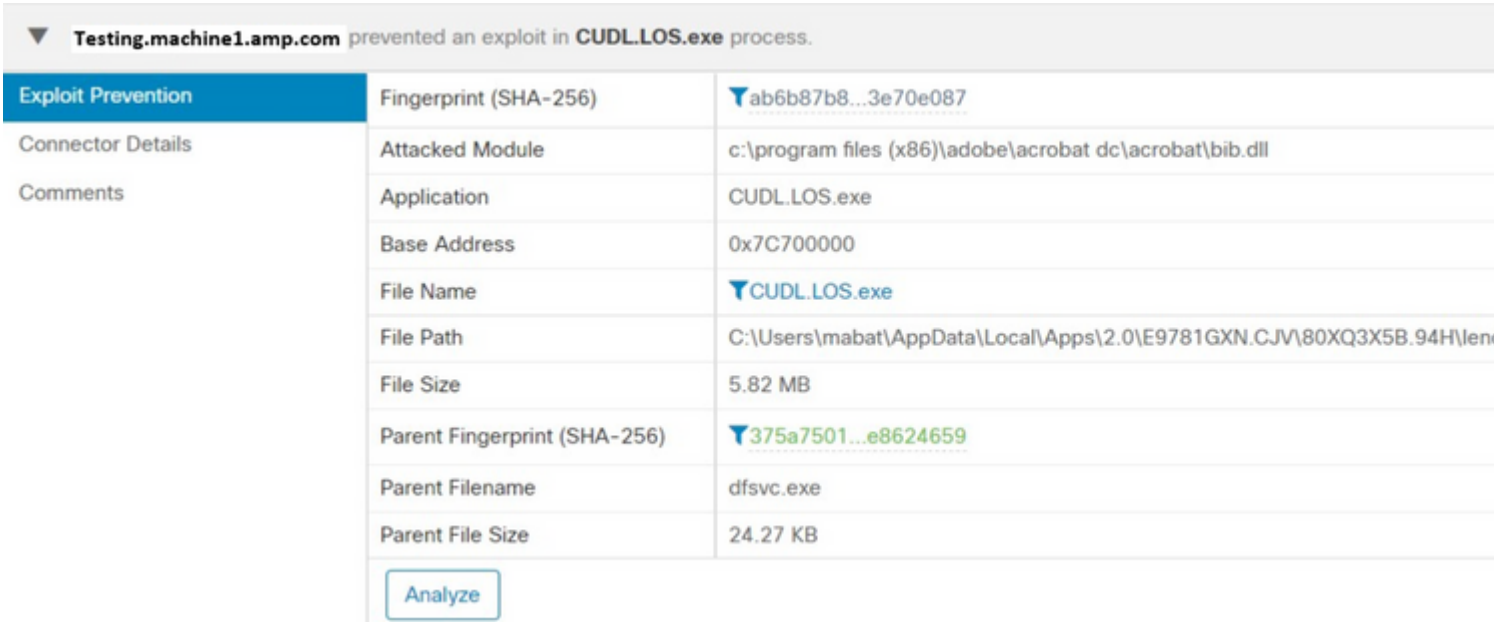


> **Vorsicht**: Verwenden Sie diese Art des Ausschlusses mit Vorsicht, nachdem Sie bestätigt haben, dass die Erkennung tatsächlich nicht schädlich ist.

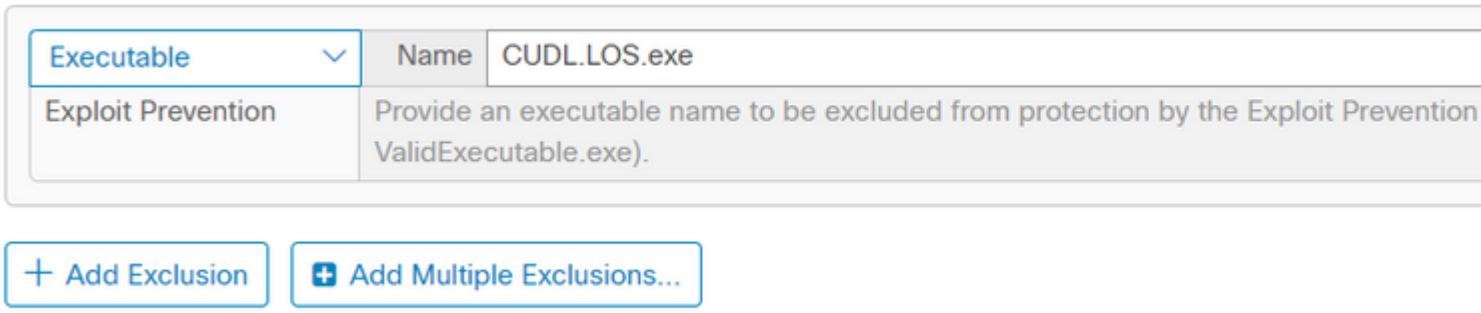
Exploit-Schutz (EXPERV)

Die Engine zum Schutz vor Exploits schützt Ihre Endgeräte vor Angriffen durch Speicherinjektionen, die häufig von Malware und anderen Zero-Day-Angriffen auf ungepatchte Software verwendet werden Sicherheitslücken. Wenn ein Angriff auf einen geschützten Prozess erkannt wird, wird er blockiert und löst ein Ereignis aus. Es findet jedoch keine Quarantäne statt.

In diesem Bild wird ein Exprev-Ereignis angezeigt.



Expev-Ausschluss

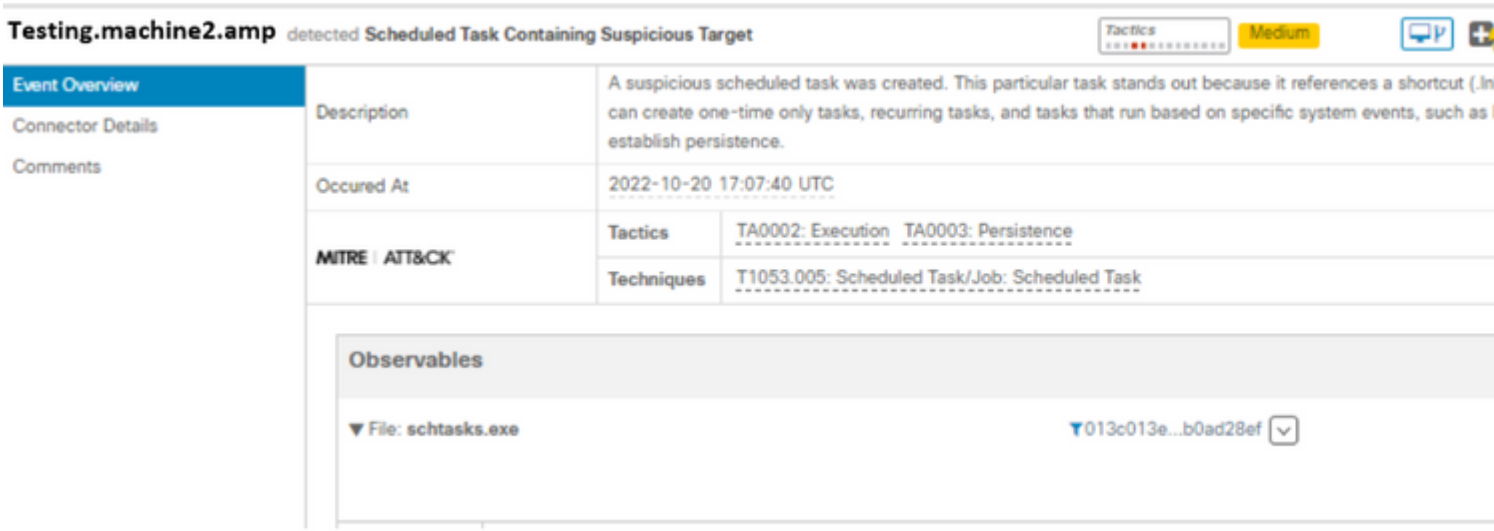


> **Vorsicht**: Verwenden Sie diesen Ausschluss immer dann, wenn Sie der Aktivität auf dem betroffenen Modul/der betroffenen Anwendung vertrauen.

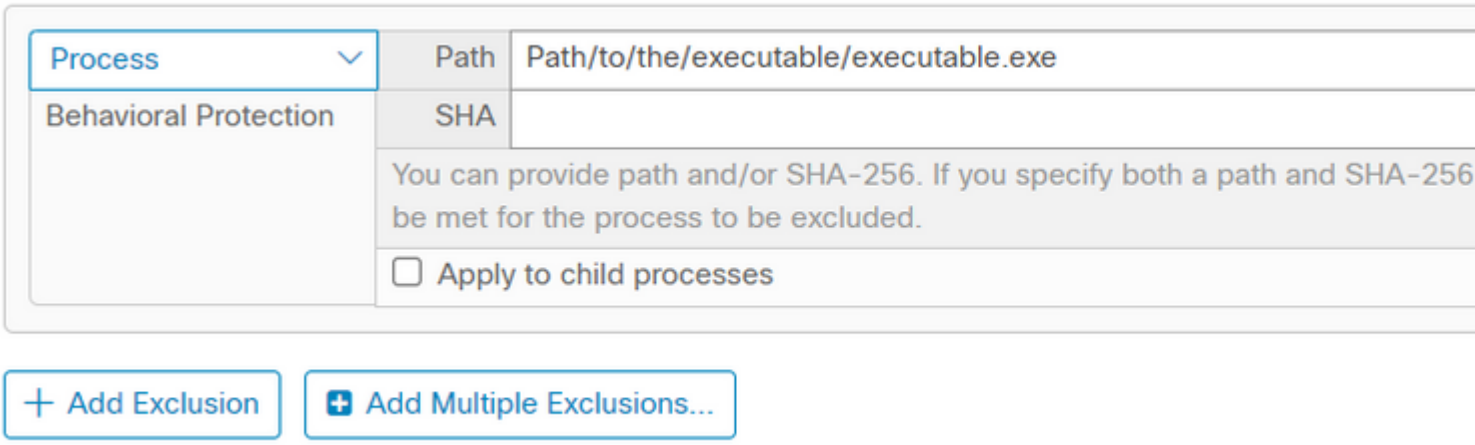
Verhaltensschutz (BP)

Die verhaltensbasierte Schutz-Engine verbessert die Fähigkeit, Bedrohungen auf verhaltensbasierte Weise zu erkennen und abzuwehren. Es vertieft die Fähigkeit zur Erkennung von "living-off-the-land"-Angriffen und bietet
schnellere Reaktion auf Änderungen in der Bedrohungslandschaft durch Signatur-Updates

In diesem Bild wird ein BP-Ereignis angezeigt.



BP-Ausschluss



Zugehörige Informationen

- **Weitere Informationen zur Richtlinienkonfiguration finden Sie im Benutzerhandbuch.**
- **Erstellen von Ausschlüssen im Video zu Cisco Secure Endpoint Connector**
- **Technischer Support und Dokumentation für Cisco Systeme**

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.