

Konfigurieren und Verwalten von Ausschlüssen in Cisco Secure Endpoint Connector

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Workflow für sichere Endgeräte](#)

[Von Cisco beibehaltene Ausschlüsse](#)

[Benutzerdefinierte Ausschlüsse](#)

[Secure Endpoint Engine](#)

[Pfadausschluss](#)

[Platzhalterausschluss](#)

[Dateierweiterungsausschluss](#)

[Prozess: Ausschluss der Dateisuche](#)

[System Process Protection \(SPP\)](#)

[SPP-Ausschluss](#)

[Schutz vor bösartigen Aktivitäten \(MAP\)](#)

[MAP-Ausschluss](#)

[Exploit-Schutz \(EXPERV\)](#)

[Verhaltensschutz \(BP\)](#)

[Zugehörige Informationen](#)

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 Ausschlüsselsätze 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](#).

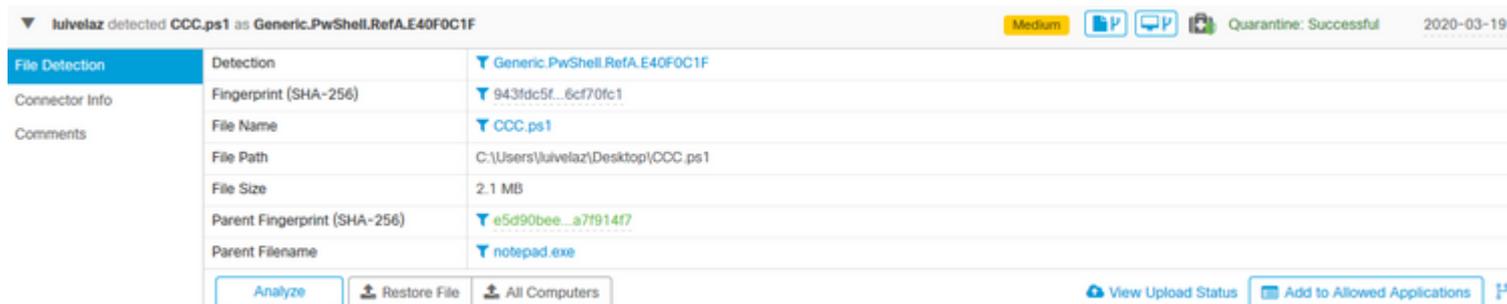
Benutzerdefinierte Ausschlüsse

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.



The screenshot shows a console event titled "luvelaz detected CCC.ps1 as Generic.PwShell.RefA.E40F0C1F". The event is categorized as "Medium" and has a status of "Quarantine: Successful" dated "2020-03-19". The event details are as follows:

Field	Value
Detection	Generic.PwShell.RefA.E40F0C1F
Fingerprint (SHA-256)	943fdc5f...6cf70fc1
File Name	CCC.ps1
File Path	C:\Users\luvelaz\Desktop\CCC.ps1
File Size	2.1 MB
Parent Fingerprint (SHA-256)	e5d90bee...a7f914f7
Parent Filename	notepad.exe

At the bottom of the event details, there are buttons for "Analyze", "Restore File", and "All Computers". On the right side, there are links for "View Upload Status" and "Add to Allowed Applications".

Hinweis: CSIDL kann für Ausschlüsse verwendet werden. Weitere Informationen zu CSIDL finden Sie in [diesem](#) Microsoft-Dokument.

Pfadausschluss

Path	C:\Users\luivelaz\Desktop\CCC.ps1
------	-----------------------------------

Platzhalterausschluss

Wildcard	C:\Users*\Desktop\CCC.ps1
	<input type="checkbox"/> Apply to all drive letters

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

Dateierweiterungsausschluss

File Extension	.ps1
----------------	------

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

Process	Path	C:\Path\to\executable.exe
File Scan	SHA	
	You can provide path and/or SHA-256. If you specify both a path and SHA-256 then both conditions must be met for the process to be excluded.	
	<input checked="" type="checkbox"/> Apply to child processes	

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.

Event Details	Fingerprint (SHA-256)	aa52b2d3...acee8d21
Connector Info	File Name	lsass.exe
Comments	File Path	C:\Windows\System32\lsass.exe
	File Size	56.73 KB
	Reason	Process module is not clean and not signed
	Parent Fingerprint (SHA-256)	f3c7b460...fd3b16dd
	Parent Filename	TestAMPprotect.exe
	Parent File Size (bytes)	1608704
<input type="button" value="Analyze"/>		

SPP-Ausschluss

Process	Path	Path\to\the\executable.exe
System Process	SHA	
	You can provide path and/or SHA-256. If you specify both a path and SHA-256 then both can be met for the process to be excluded.	
	<input checked="" type="checkbox"/> Apply to child processes	

Process	Path	
System Process	SHA	SHA-256 of the file (From the Parent Filename field)
	not a valid SHA-256	
	You can provide path and/or SHA-256. If you specify both a path and SHA-256 then both can be met for the process to be excluded.	
<input checked="" type="checkbox"/> Apply to child processes		

Schutz vor böartigen 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.

Malicious Activity Protection	Fingerprint (SHA-256)	9967f55a...2956d820
Connector Info	Affected Files Count	5
Comments	Affected Files	C:\Users\umontero\Desktop\Test files\AMP4E-8120-SPP-MAP-EXPREV-test_files\Map\rewrite_data\1.txt.new C:\Users\umontero\Desktop\Test files\AMP4E-8120-SPP-MAP-EXPREV-test_files\Map\rewrite_data\0.txt.new C:\Users\umontero\Desktop\Test files\AMP4E-8120-SPP-MAP-EXPREV-test_files\Map\rewrite_data\4.txt.new C:\Users\umontero\Desktop\Test files\AMP4E-8120-SPP-MAP-EXPREV-test_files\Map\rewrite_data\2.txt.new C:\Users\umontero\Desktop\Test files\AMP4E-8120-SPP-MAP-EXPREV-test_files\Map\rewrite_data\3.txt.new
	File Name	rewrite.exe
	File Path	C:\Users\umontero\Desktop\Test files\AMP4E-8120-SPP-MAP-EXPREV-test_files\Map\rewrite.exe
	File Size	4.37 MB
	Parent Fingerprint (SHA-256)	9967f55a...2956d820
	Parent Filename	rewrite.exe

MAP-Ausschluss

Process	Path	Path\to\the\executable.exe
Malicious Activity	SHA	
<p>You can provide path and/or SHA-256. If you specify both a path and SHA-256 then both conditions must be met for the process to be excluded.</p>		
<input checked="" type="checkbox"/> Apply to child processes		

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 Speichereinjektionen, 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.

Testing.machine1.amp.com prevented an exploit in CUDL.LOS.exe process.

Exploit Prevention	Fingerprint (SHA-256)	ab6b87b8...3e70e087
Connector Details	Attacked Module	c:\program files (x86)\adobe\acrobat dc\acrobat\bib.dll
Comments	Application	CUDL.LOS.exe
	Base Address	0x7C700000
	File Name	CUDL.LOS.exe
	File Path	C:\Users\mabat\AppData\Local\Apps\2.0\E9781GXN.CJV\80XQ3X5B.94H\len
	File Size	5.82 MB
	Parent Fingerprint (SHA-256)	375a7501...e8624659
	Parent Filename	dfsvc.exe
	Parent File Size	24.27 KB

Analyze

Expev-Ausschluss

Executable	Name	CUDL.LOS.exe
Exploit Prevention	Provide an executable name to be excluded from protection by the Exploit Prevention (ValidExecutable.exe).	

+ Add Exclusion + Add Multiple Exclusions...

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.

Testing.machine2.amp detected Scheduled Task Containing Suspicious Target Tactics Medium

Event Overview	Description		A suspicious scheduled task was created. This particular task stands out because it references a shortcut (.lnk) file. .lnk files can create one-time only tasks, recurring tasks, and tasks that run based on specific system events, such as system startup, to establish persistence.
Connector Details	Occurred At		2022-10-20 17:07:40 UTC
Comments	MITRE ATT&CK	Tactics	TA0002: Execution TA0003: Persistence
		Techniques	T1053.005: Scheduled Task/Job: Scheduled Task

Observables

▼ File: schtasks.exe ▼ 013c013e...b0ad28ef ▼

BP-Ausschluss

Process ▼	Path	Path/to/the/executable/executable.exe
Behavioral Protection	SHA	
<p>You can provide path and/or SHA-256. If you specify both a path and SHA-256, both must be met for the process to be excluded.</p> <p><input type="checkbox"/> Apply to child processes</p>		

+ Add Exclusion
+ Add Multiple Exclusions...

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.