

Configurazione e gestione delle esclusioni in Cisco Secure Endpoint Connector

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Flusso di lavoro Secure Endpoint](#)

[Esclusioni gestite da Cisco](#)

[Esclusioni personalizzate](#)

[Secure Endpoint Engine](#)

[Esclusione percorso](#)

[Esclusione caratteri jolly](#)

[Esclusione estensione file](#)

[Processo: Esclusione analisi file](#)

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

[Esclusione SPP](#)

[Protezione dalle attività dannose \(MAP\)](#)

[Esclusione MAP](#)

[Exprev \(Exploit Prevention\)](#)

[Protezione comportamentale \(BP\)](#)

[Informazioni correlate](#)

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

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

Esclusione caratteri jolly

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

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

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

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

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	

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.

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"/>		

Esclusione SPP

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 conditions must 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 conditions must be met for the process to be excluded.	
<input checked="" type="checkbox"/> Apply to child processes		

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.

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
<div style="display: flex; justify-content: space-between; align-items: center;"> Analyze Restore File All Computers </div>		

Esclusione MAP

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		

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.

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		

Esclusione espressione

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

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.

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).