Configurazione e identificazione delle esclusioni di Cisco Secure Endpoint

Sommario

Introduzione

In questo documento vengono descritte le best practice per individuare e creare esclusioni sull'endpoint sicuro.

Contributo dei tecnici Cisco.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso alla console Secure Endpoint
- Account con privilegi di amministratore

- Una conoscenza operativa dell'ambiente del cliente.

Componenti usati

Le informazioni fornite in questo documento si basano sui sistemi operativi Windows, Linux e MacOS.

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.

Premesse

Come comprendere le esclusioni

Un set di esclusione è un elenco di directory, estensioni di file o nomi di minacce che non si desidera sottoporre a scansione o condannare in Secure Endpoint Connector. Le esclusioni sono necessarie per garantire l'equilibrio tra prestazioni e sicurezza in un computer quando è abilitata la protezione degli endpoint, ad esempio Secure Endpoint. In questo articolo vengono descritte le esclusioni per Secure Endpoint Cloud, TETRA, SPP e MAP.

Ogni ambiente è unico, così come l'entità che lo controlla, che varia da politiche rigorose a politiche aperte, dove queste ultime sarebbero classificate come un honeypot. Poiché tali esclusioni sono definite devono essere adattate in modo univoco a ogni situazione.

Le esclusioni diverse possono essere classificate in due modi, **esclusioni ovvie** ed **esclusioni indistinte**.

Esclusioni evidenti

Le esclusioni ovvie sono esclusioni create in base a ricerche e test per sistemi operativi, programmi e altri software di sicurezza di uso comune. Queste esclusioni sono disponibili nell'elenco di esclusione gestito da Cisco nella tua console.

> **Nota**: si consiglia di contattare altri fornitori di software antivirus e richiedere l'aggiunta delle esclusioni consigliate. In questo modo, il funzionamento dell'endpoint sicuro e dell'antivirus è garantito e l'impatto sulle prestazioni è ridotto al minimo.

Esclusioni indirette

È consigliabile creare un criterio duplicato per evitare problemi di sicurezza aziendale e interruzioni per identificare i computer con indicatori di problemi di prestazioni e separarli in un gruppo per utilizzare il criterio duplicato.

> **Attenzione**: le modifiche alla configurazione nel dashboard richiedono tempo per consentire ai connettori di sincronizzare il criterio. Consentire un aggiornamento heartbeat o sincronizzare manualmente i criteri sui connettori.

Creazione criteri

1. **Secure Endpoint Console > Scheda Gestione > Criteri**
2. Fare clic su **+ Nuovo criterio...**
3. **Selezionare** dal menu a discesa del sistema operativo.
4. Fornire un nome significativo che consenta di distinguere il criterio e la descrizione (*facoltativo*).
5. Selezionare le azioni dei criteri in base alle proprie esigenze, utilizzare le esclusioni predefinite per il momento.
6. ***Importante*** In **Advanced Settings > Administrative Features,** impostare il livello di log del connettore su **Debug**.
7. Fare clic su **Salva** per completare la creazione del criterio.

Creazione di gruppi

1. **Secure Endpoint Console > Scheda Gestione > Gruppi**
2. Fare clic su **Crea gruppo**
3. Fornire un nome significativo che consenta di distinguere il gruppo e la descrizione (*facoltativo*).
4. **Selezionare** il criterio duplicato creato.
5. Fate clic su **Salva (Save)** per completare la creazione del gruppo.

Come identificare le esclusioni

Dopo la creazione di criteri e gruppi duplicati, con il **livello di registro di debug sui connettori** eseguire i *computer* secondo le normali operazioni aziendali. Attendere il tempo necessario per ottenere dati di registro del connettore sufficienti durante l'accesso a programmi e processi, generare un pacchetto diagnostico di supporto per esaminare e identificare le esclusioni.

Guida alla creazione di pacchetti diagnostici per sistemi operativi diversi disponibili:

- Windows
- Linux
- MAC

MacOS o Linux

Estrarre il pacchetto di diagnostica di debug compresso. Il file **fileops.txt** elenca i percorsi in cui i file creano, modificano e rinominano le attività attivate da Secure Endpoint per eseguire le scansioni dei file. A ogni percorso è associato un conteggio che indica quante volte è stato digitalizzato e l'elenco è ordinato in ordine decrescente. Sebbene un conteggio elevato non significhi necessariamente che il percorso debba essere escluso (ad esempio, una directory in cui sono archiviati i messaggi di posta elettronica può essere analizzata spesso ma non deve essere esclusa), l'elenco costituisce un punto di partenza per identificare i candidati all'esclusione.

```
31 /Users/eugene/Library/Cookies/Cookies.binarycookies
24 /Users/eugene/.zhistory
9 /Users/eugene/.vim/.temp/viminfo
9 /Library/Application Support/Apple/ParentalControls/Users/eugene/2018/05/10-usage.data
5 /Users/eugene/Library/Cookies/HSTS.plist
5 /Users/eugene/.vim/.temp/viminfo.tmp
4 /Users/eugene/Library/Metadata/CoreSpotlight/index.spotlightV3/tmp.spotlight.state
3 /Users/eugene/Library/WebKit/com.apple.Safari/WebsiteData/ResourceLoadStatistics/full_browsir
3 /Library/Logs/Cisco/supporttool.log
2 /private/var/db/locationd/clients.plist
2 /Users/eugene/Desktop/.DS_Store
2 /Users/eugene/.dropbox/instance1/config.dbx
```

```
 2 /Users/eugene/.DS_Store
 2 /Library/Catacomb/DD94912/biolockout.cat
 2 /.fseventsd/000000000029d66b
 1 /private/var/db/locationd/.dat.nosync0063.arg4tq
```

Windows

Il sistema operativo Windows è più complesso, sono disponibili più opzioni di esclusione a causa dei processi padre e figlio. Ciò indica che è necessaria una revisione più approfondita per identificare i file a cui si è avuto accesso, ma anche i programmi che li hanno generati. Fare riferimento a questo Windows Tuning Tool dalla pagina GitHub di Cisco Security per ottenere ulteriori dettagli su come analizzare e ottimizzare le prestazioni di Windows con Secure Endpoint.

Come creare le esclusioni

In questa sezione vengono descritte le procedure ottimali per la scrittura delle esclusioni per l'ambiente in uso.

> **Attenzione**: comprendere sempre i file e i processi prima di scrivere un'esclusione per evitare vulnerabilità di protezione al computer.

> **Nota**: ulteriori informazioni sono disponibili nella Guida dell'utente. Vedere il Capitolo 3 qui. In questo capitolo vengono illustrati i tipi di esclusione, implementazione e navigazione del portale Secure Endpoint.

Percorso e processo CSIDL

Il CSIDL è un modo accettato e incoraggiato per scrivere esclusioni. CSIDL consente esclusioni di processo che possono essere riconosciute in ambienti che utilizzano lettere di unità alternative e che possono ignorare la necessità di caratteri jolly quando il percorso è specifico dell'utente (poiché le esclusioni di processo non consentono i caratteri jolly). Ulteriori informazioni su CSIDL. Esistono tuttavia limitazioni che è necessario considerare quando si utilizza CSIDL. Se nell'ambiente i programmi vengono installati in più di una lettera di unità, il percorso CSIDL si riferisce solo all'unità contrassegnata come percorso di installazione predefinito, ad esempio se il sistema operativo è installato in C:\ ma il percorso di installazione di Microsoft SQL è stato modificato manualmente in D:\, l'esclusione basata su CSIDL nell'elenco di esclusione mantenuto non si applica a tale percorso. Per le esclusioni di processo, questo significa che è necessario immettere un'esclusione per ogni processo non presente nell'unità C:\, in quanto l'utilizzo di CSIDL non ne esegue il mapping.

Esclusioni di percorsi

Queste esclusioni sono le più utilizzate, i conflitti tra applicazioni in genere comportano l'esclusione di una directory. Creare un'esclusione di percorso utilizzando un percorso assoluto o il CSIDL.

Ad esempio, per escludere un'applicazione antivirus nella directory Programmi, il percorso di esclusione sarà:

```
C:\Program Files\MyAntivirusAppDirectory
CSIDL_PROGRAM_FILES\MyAntivirusAppDirectory
```

Senza una barra finale, **Windows connector** esegue una corrispondenza parziale sui percorsi, a differenza di **Mac e Linux.**

Esempio se si applicano le seguenti esclusioni di percorso "**C:\Program Files"** e come **"C:\test":**

C:\Program File e **C:\Program File (x86)** sono esclusi:

<#root>

```
C:\Program Files
```

```
C:\Program Files (x86)
```

C:\test è escluso, come **C:\test123**:

<#root>

```
C:\test
```

```
C:\test123
```

È possibile modificare l'esclusione da "**C:\test"** a "**C:\test\"**, in modo che "**C:\test123" non** venga escluso.

Nota: le esclusioni di percorso sono ricorsive ed escludono anche tutte le sottodirectory.

Estensione file

Tali esclusioni consentono l'esclusione di tutti i file con una determinata estensione.

Considerazioni principali:

- L'input previsto sul lato connettore è **.extension**
- Se non è stato aggiunto alcun punto, il dashboard lo precede automaticamente all'estensione del file.
- Nelle estensioni ***non*** viene fatta distinzione tra maiuscole e minuscole.

Ad esempio, per escludere tutti i file di database di Microsoft Access, è possibile creare l'esclusione seguente:

```
.MDB
```

Nota: le esclusioni standard sono disponibili nell'elenco predefinito. **Non** è consigliabile eliminare tali esclusioni, in quanto potrebbero causare modifiche alle prestazioni dei *computer*.

Carattere jolly

Queste esclusioni sono identiche alle esclusioni di percorso o di estensione, ad eccezione dell'utilizzo di un asterisco (*) come trigger di carattere jolly.

> **Attenzione**: l'esclusione dei caratteri jolly non si arresta ai separatori di percorso e può causare esclusioni non intenzionali. Esempio: **C:*\test** esclude **C:\sample\test** e **C:\1\test** o **C:\sample\test123 .**

> **Avviso**: l'impostazione di un'esclusione con un asterisco (*) può causare problemi di prestazioni importanti. Con **7.5.3+**, l'aggiunta delle esclusioni dei processi con caratteri jolly ha causato ulteriori problemi di prestazioni con esclusioni che precedono l'asterisco. Rimuovere o modificare tutte le esclusioni in questo formato per ridurre l'impatto sulla CPU.

Ad esempio, per escludere le macchine virtuali su un MAC dall'analisi, immettere questa esclusione di percorso:

```
/Users/johndoe/Documents/Virtual Machines/
```

Questa esclusione funziona solo per *johndoe,* per consentire più corrispondenze utente, sostituire il nome utente nel percorso con un asterisco (*) per un'esclusione con caratteri jolly:

```
/Users/*/Documents/Virtual Machines/
```

Scrivere un'esclusione per i percorsi presenti in unità separate.

Esempio: **C:\testpath** e **D:\testpath** sono:

```
^[A-Za-z]\testpath
```

Il sistema genera automaticamente ^[A-Za-z] quando la casella di controllo "Applica a tutte le lettere di unità" è selezionata dopo aver selezionato il carattere jolly nell'elenco a discesa Tipo di esclusione, come mostrato nell'immagine:

Processo

Le esclusioni di processo consentono agli amministratori di escludere i processi in esecuzione dalle normali analisi dei file (Secure Endpoint Windows Connector versione 5.1.1 e successive), Protezione processo di sistema (Connector versione 6.0.5 e successive) o Protezione attività dannosa (Connector versione 6.1.5 e successive).

L'esclusione dei processi viene eseguita specificando il percorso completo dell'eseguibile di processo, il valore SHA-256 dell'eseguibile di processo oppure sia il percorso che SHA-256. I percorsi consentono entrambi i percorsi diretti o utilizzano un valore CSIDL.

Attenzione: i processi figlio creati da un processo escluso **non** vengono inclusi nell'esclusione per impostazione predefinita. Esempio: l'esclusione dei processi per MS Word non esclude per impostazione predefinita i processi aggiuntivi creati da Word.exe e verrebbero analizzati. Per includere processi aggiuntivi, selezionare la casella di controllo **Applica per processi figlio**. Inoltre, l'esclusione di Word.exe non è consigliata in quanto il malware si nasconde regolarmente nei file .docx moderni.

Nota: per escludere il processo, è necessario specificare sia Path che SHA-256.

Limitazioni:

- Se la dimensione del file del processo è maggiore della dimensione massima del file di analisi impostata nel criterio, il valore SHA-256 del processo non verrà calcolato e l'esclusione **non funzionerà**. Utilizza un'esclusione di processo basata su percorso per i file di dimensioni superiori alla dimensione massima del file di digitalizzazione
- Connector versioni da 5.x.x a 6.0.3: un limite di 25 esclusioni di processo per tutti i tipi di esclusione di processo
- Connector versioni 6.0.5+: limite di 100 esclusioni di processo per tutti i tipi di esclusione di processo.
- Connector versioni 7.x.+: limite di 500 esclusioni di processo per tutti i tipi di esclusione di processo.
- Il connettore rispetta solo le esclusioni di processo fino al limite, dall'inizio dell'elenco di esclusioni di processo in policy.xml
- A ogni criterio è associata un'esclusione di processo per sfc.exe, che viene conteggiata a fronte del limite

```
3|0||CSIDL_Secure Endpoint_VERSION\sfc.exe|48|
```

Minaccia

Queste esclusioni consentono di escludere un particolare nome di minaccia dagli eventi di attivazione. L'esclusione delle minacce deve essere utilizzata solo quando il risultato della scansione attiva il rilevamento di falsi positivi e conferma che non si tratta di una minaccia reale.

La casella di testo per l'aggiunta di un'esclusione di minaccia ***non fa*** distinzione tra maiuscole e minuscole. Esempio: W32.Zombies.NotAVirus o w32.zombies.notavirus corrispondono entrambi allo stesso nome di minaccia.

Avvertenza: non escludere minacce a meno che l'indagine e la conferma sul nome della minaccia non siano ritenute false positive. Le minacce escluse non vengono più inserite nella scheda Eventi per la revisione e il controllo.

Carattere jolly processo

Windows

L'endpoint 7.5.3+ consente ulteriori esclusioni utilizzando la funzionalità Wildcard all'interno delle esclusioni Process. Questo permette una copertura più ampia con meno esclusioni, ma può anche essere pericoloso se troppo viene lasciato indefinito. **È consigliabile utilizzare il carattere jolly solo per includere il numero minimo di caratteri necessario per l'esclusione.**

Utilizzo di (*) in Elabora carattere jolly per Windows:

- (*) Può essere utilizzato al posto di un singolo carattere o di una directory completa. Non può essere posizionato all'inizio del percorso. Verrà dichiarato non valido. Il carattere jolly funziona tra due caratteri definiti, barre o caratteri alfanumerici. Se lo si posiziona alla fine di un percorso, i processi in tale directory verranno esclusi, ma non le sottodirectory.
- (**) Può essere utilizzato alla fine di un percorso per escludere tutti i processi in tale directory e i processi nelle sottodirectory. Questo permette un set di esclusione molto più grande con input minimo, ma lascia anche un buco di sicurezza molto grande per la visibilità. **Utilizzare questa funzione con estrema cautela**.

Esempi:

```
C:\Windows\*\Tiworker.exe - Excludes all Tiworker.exe found in the subfolders of 'Windows'
C:\Windows\P*t.exe - Excludes Pot.exe, Pat.exe, P1t.exe Etc.
C:\Windows\*chickens.exe - Excludes all Processes in 'Windows' folder ending in chickens.exe
C:\* - Excludes all Processes in the C: drive in the top layer of folders but not the subfolders
C:\** - Excludes every Process on the C: drive.
```

MacOS e Linux

L'endpoint 1.15.2+ consente ulteriori esclusioni utilizzando la funzionalità Wildcard all'interno delle esclusioni Process. Questo permette una copertura più ampia con meno esclusioni, ma può anche essere pericoloso se troppo viene lasciato indefinito. **È consigliabile utilizzare il carattere jolly solo per includere il numero minimo di caratteri necessario per l'esclusione.**

Uso di (*) in Elabora carattere jolly per Mac:

- (*) Può essere utilizzato al posto di un singolo carattere o di una directory completa. Non può essere posizionato all'inizio del percorso. Verrà dichiarato non valido. Il carattere jolly funziona tra due caratteri definiti, barre o caratteri alfanumerici.

Esempi:

```
/Library/Java/JavaVirtualMachines/*/java - Excludes Java within all subfolders of JavaVirtualMac
/Library/Jibber/j*bber - Excludes the Process for jabber, jibber, jobber, etc.
```

Esclusioni dalla prevenzione degli attacchi (applicazione)

Windows

Secure Endpoint 7.5.1+ utilizza V5 di Exploit Prevention Engine e la console consente ora di configurare le esclusioni delle applicazioni all'interno della funzionalità dell'elenco di esclusioni corrente. **Questa operazione è attualmente limitata alle applicazioni e qualsiasi esclusione relativa alle DLL deve essere ancora eseguita aprendo una richiesta con il supporto.**

Trovare le esclusioni corrette per la prevenzione dell'utilizzo è un processo molto più intenso rispetto a qualsiasi altro tipo di esclusione e richiede test approfonditi per ridurre al minimo eventuali problemi di sicurezza.

Errori comuni da evitare

Prestare attenzione quando si creano esclusioni in quanto ciò riduce il livello di protezione fornito da Cisco Secure Endpoint. I file esclusi non vengono sottoposti a hashing, non vengono scansionati o non sono disponibili nella cache o nel cloud, l'attività non viene monitorata e mancano informazioni dai motori di back-end, dalla traiettoria del dispositivo e dall'analisi avanzata.

Le esclusioni devono essere utilizzate *solo* in modo limitato in casi mirati, ad esempio problemi di compatibilità con applicazioni specifiche o problemi di prestazioni che altrimenti non potrebbero essere migliorati.

Di seguito sono riportati alcuni errori comuni da evitare quando si utilizzano le esclusioni.

- **Esclusioni proattive**
  - Non presumere che un'esclusione sia necessaria a meno che non sia stato dimostrato che si è trattato di un problema che non può essere affrontato altrimenti. I problemi di prestazioni, i falsi positivi o i problemi di compatibilità delle applicazioni devono essere esaminati attentamente e risolti prima di applicare un'esclusione

- **Un'esclusione troppo ampia**
  - Esclusione di porzioni estese dell'endpoint, ad esempio l'intera unità C
  - Utilizzo di un'esclusione con caratteri jolly quando è possibile un'esclusione più specifica
  - Utilizzo del solo nome del file anziché di un percorso completo del file
  - Utilizzare Device Trajectory o Secure Endpoint Diagnostics Package e Performance Tuning Tool per analizzare e determinare l'esclusione specifica necessaria

- **Utilizzo eccessivo delle esclusioni dei caratteri jolly**
  - Le esclusioni dei caratteri jolly non solo creano più lacune nella sicurezza, ma richiedono anche più risorse di sistema rispetto a qualsiasi altro tipo di esclusione
  - Assicurarsi di utilizzare la quantità minima di caratteri jolly in un'esclusione; solo le cartelle che sono realmente variabili devono essere rese variabili con un carattere jolly. Ad esempio:
    - Programmi\Software* escluderà tutti gli elementi della cartella, ma non le sottocartelle
    - Programmi\Software** escluderà tutti gli elementi della cartella, incluse le sottocartelle

- **Esclusione degli elementi utilizzati negli attacchi**
  - Tipi di file quali cmd, zip, jpg e così via
  - Processi quali svchost.exe, bash.exe, powershell.exe e così via.
  - Posizioni delle cartelle, ad esempio C:\Users\, C:\Windows\Temp\, C:\Program Files\Java e così via

- **Esclusioni duplicate**
  - Prima di creare un'esclusione, verificare se l'esclusione esiste già nelle esclusioni personalizzate create dall'utente o nelle esclusioni gestite da Cisco.

    - La rimozione delle esclusioni duplicate non solo migliora le prestazioni, ma riduce la gestione operativa delle esclusioni

- **Esclusioni non aggiornate**
    - Le esclusioni create molto tempo fa potrebbero non essere ancora necessarie.
    - Controllare regolarmente l'elenco di esclusione e assicurarsi di tenere traccia del motivo per cui è stata aggiunta una determinata esclusione.

- **Non rimuovere le esclusioni post-infezione**
    - Le esclusioni devono essere rimosse una volta identificata un'infezione al fine di riottenere la massima sicurezza e visibilità
    - L'utilizzo anticipato della funzione Azioni automatizzate "Sposta il computer nel gruppo" consente di applicare rapidamente una policy più sicura dopo l'infezione, inclusa l'impostazione di una policy senza esclusioni

- **Mancanza di tattiche di mitigazione**
    - Quando le esclusioni sono assolutamente necessarie, prendere in considerazione quali tattiche di mitigazione possono essere adottate, ad esempio abilitando la protezione da scrittura per aggiungere alcuni livelli di protezione per gli elementi esclusi.

Per ulteriori procedure consigliate relative alle esclusioni o agli endpoint sicuri, vedere la Guida alle procedure consigliate

Esclusioni non consigliate

Ai fini di una buona postura di sicurezza e di una buona visibilità, non si raccomanda di escludere:

AcroRd32.exe
addinprocess.exe
addinprocess32.exe
addinutil.exe
bash.exe
bginfo.exe
bitsadmin.exe
cdb.exe

csi.exe
dbghost.exe
dbgsvc.exe
dnx.exe
dotnet.exe
excel.exe
fsi.exe
fsiAnyCpu.exe
iexplore.exe
java.exe
kd.exe
lxssmanager.dll
msbuild.exe
mshta.exe
ntkd.exe
ntsd.exe
outlook.exe
psexec.exe

powerpnt.exe
powershell.exe
rcsi.exe
svchost.exe
schtasks.exe
system.management.automation.dll
windbg.exe
winword.exe
wmic.exe
wuauclt.exe
0,7z
bat
bin
.cab
cmd
.com
cpl
DLL

exe
fla
gif
.gz
hta
inf
java
jar
job
.jpeg
.jpg
js
ko
.ko.gz
msi
ocx
png
ps1

py
.rar
reg
scr
sys
.tar
tmp
url
vbe
vbs
wsf
.zip
sbattere
java
pitone
pitone 3
sh
zsh

/
/bin
/sbin
/usr/lib
C:
C:\
C:*
D:\
D:*
C:\Program Files\Java
C:\Temp\
C:\Temp*
C:\Users\
C:\Users*
C:\Windows\Prefetch
C:\Windows\Prefetch\
C:\Windows\Prefetch*

C:\Windows\System32\Spool
C:\Windows\System32\CatRoot2
C:\Windows\Temp
C:\Windows\Temp\
C:\Windows\Temp*
C:\Program Files\<nome società>\
C:\Program Files (x86)\<nome società>\
C:\Users\<NomeProfiloUtente>\AppData\Local\Temp\
C:\Users\<NomeProfiloUtente>\AppData\LocalLow\Temp\

Informazioni correlate

- **Documentazione e supporto tecnico â€“ Cisco Systems**
- **Cisco Secure Endpoint - Note tecniche**
- **Cisco Secure Endpoint - Guida per l'utente**
- **Endpoint sicuro: esclusioni di processi in macOS e Linux**

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).