Configuration et identification des exclusions de terminaux sécurisés Cisco

Table des matières

Introduction

Ce document décrit les meilleures pratiques pour localiser et créer des exclusions sur le point d'extrémité sécurisé.

Contribution des ingénieurs Cisco.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Accès à la console Secure Endpoint
- Compte disposant de privilèges Administrateur

- Une connaissance pratique de l'environnement du client.

Composants utilisés

Les informations contenues dans ce document sont basées sur les systèmes d'exploitation Windows, Linux et MacOS.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre lâ€™incidence possible des commandes.

Informations générales

Comment comprendre les exclusions

Un jeu d'exclusions est une liste de répertoires, d'extensions de fichiers ou de noms de menaces que vous ne souhaitez pas que le connecteur Secure Endpoint Connector analyse ou déclare coupable. Les exclusions sont nécessaires pour garantir un équilibre entre performances et sécurité sur une machine lorsque la protection des terminaux, telle que Secure Endpoint, est activée. Cet article décrit les exclusions pour Secure Endpoint Cloud, TETRA, SPP et MAP.

Chaque environnement est unique, ainsi que l'entité qui le contrôle, variant des politiques strictes aux politiques ouvertes, où ces dernières seraient classées comme un pot de miel. Comme de telles exclusions sont définies, elles doivent être adaptées de façon unique à chaque situation.

Les exclusions peuvent être classées de deux façons : les **exclusions évidentes** et les **exclusions indistinctes**.

Exclusions évidentes

Les exclusions évidentes sont des exclusions qui ont été créées sur la base de recherches et de tests pour des systèmes d'exploitation, des programmes et d'autres logiciels de sécurité couramment utilisés. Ces exclusions se trouvent dans la liste d'exclusions gérée par Cisco sur votre console.

> **Remarque** : il est recommandé de contacter d'autres fournisseurs d'antivirus et de demander l'ajout de leurs exclusions recommandées, afin de garantir que le terminal sécurisé et l'antivirus fonctionnent en tandem et de minimiser l'impact sur les performances.

Exclusions indistinctes

Il est recommandé de créer une stratégie en double pour éviter les problèmes de sécurité et les interruptions de l'activité, afin d'identifier les ordinateurs présentant des indicateurs de problèmes de performances et de les séparer en un groupe pour utiliser cette stratégie en double.

> **Attention** : les modifications apportées à la configuration sur le tableau de bord nécessitent du temps pour permettre aux connecteurs de synchroniser la stratégie. Autorisez une mise à jour de pulsation ou synchronisez manuellement les stratégies sur les connecteurs.

Création de politiques

1. **Secure Endpoint Console > Onglet Management > Policies**
2. Cliquez sur **+ Nouvelle politique...**
3. **Sélectionnez** le système d'exploitation dans le menu déroulant.
4. Fournissez-lui un nom significatif pour vous permettre de distinguer cette stratégie de sa description (*facultatif*).
5. Sélectionnez les actions de stratégie correspondant à vos besoins, utilisez les exclusions par défaut pour l'instant.
6. ***Important*** Dans **Advanced Settings > Administrative Features,** définissez le niveau du journal du connecteur sur **Debug**.
7. Cliquez sur **Enregistrer** pour terminer la création de la stratégie.

Création de groupe

1. **Console Secure Endpoint > Onglet Management > Groups**
2. Cliquez sur **Créer un groupe**
3. Fournissez-lui un nom significatif pour vous permettre de distinguer ce groupe et sa description (*facultatif*).
4. **Sélectionnez** la stratégie dupliquée que vous avez créée.
5. Cliquez sur **Enregistrer** pour terminer la création du groupe.

Comment identifier les exclusions

Après la création de la stratégie et du groupe en double, avec le **niveau de journal de débogage sur les connecteurs** exécutez les *ordinateurs* selon les opérations normales de l'entreprise. Laissez le temps d'obtenir des données de journal de connecteur suffisantes pendant que les programmes et les processus ont été accédés, générez un bundle de diagnostic de support pour examiner et identifier les exclusions.

Guide de création de bundles de diagnostic pour différents systèmes d'exploitation disponibles :

- Fenêtres
- Linux
- MAC

MacOS ou Linux

Extrayez le bundle de diagnostic de débogage compressé. Le fichier **fileops.txt** Le répertorie les chemins d'accès où les activités de création, de modification et de changement de nom des fichiers déclenchées par Secure Endpoint pour effectuer des analyses de fichiers. Chaque chemin est associé à un nombre qui indique le nombre de fois où il a été analysé et la liste est triée dans l'ordre décroissant. Bien qu'un nombre élevé ne signifie pas nécessairement que le chemin doit être exclu (p. ex., un répertoire qui stocke des courriels peut être analysé souvent, mais ne doit pas être exclu), la liste fournit un point de départ pour identifier les candidats à l'exclusion.

```
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
```

Fenêtres

Le système d'exploitation Windows est plus compliqué, plus d'options d'exclusion sont disponibles en raison des processus parent et enfant. Cela indique qu'un examen plus approfondi est nécessaire pour identifier les fichiers qui ont été consultés, mais aussi les programmes qui les ont générés. Reportez-vous à cet outil de réglage Windows de la page GitHub de Cisco Security pour obtenir plus de détails sur la façon d'analyser et d'optimiser les performances Windows avec Secure Endpoint.

Comment créer des exclusions

Cette section décrit les meilleures pratiques pour écrire des exclusions pour votre environnement.

> **Attention** : comprenez toujours les fichiers et les processus avant d'écrire une exclusion afin d'éviter des failles de sécurité sur l'ordinateur.

> **Remarque** : des détails supplémentaires sont disponibles dans le Guide de l'utilisateur, consultez le chapitre 3 ici. Ce chapitre présente les types d'exclusions, de mise en oeuvre et de navigation du portail Secure Endpoint.

Chemin et processus CSIDL

La LSIC est une façon acceptée et encouragée d'écrire des exclusions. CSIDL autorise les exclusions de processus qui peuvent être reconnues dans les environnements qui utilisent d'autres lettres de lecteur et qui peuvent contourner la nécessité d'utiliser un caractère générique lorsque ce chemin est spécifique à l'utilisateur (car les exclusions de processus ne permettent pas de caractère générique). Plus d'informations sur CSIDL . Il y a cependant des limites à prendre en considération lorsque la LCSII est utilisée. Si votre environnement installe des programmes sur plusieurs lettres de lecteur, le chemin CSIDL fait uniquement référence au lecteur marqué comme emplacement d'installation par défaut. Par exemple, si le système d'exploitation est installé sur C:\ mais que le chemin d'installation de Microsoft SQL a été modifié manuellement en D:\, l'exclusion basée sur CSIDL dans la liste d'exclusion mise à jour ne s'applique pas à ce chemin. Pour les exclusions de processus, cela signifie qu'une exclusion doit être entrée pour chaque processus qui ne se trouve pas sur le lecteur C:\ car l'utilisation de CSIDL ne le mappe pas.

Exclusions de chemin

Ces exclusions sont les plus fréquemment utilisées, les conflits d'application impliquent généralement l'exclusion d'un répertoire. Créez une exclusion de chemin à l'aide d'un chemin absolu ou du CSIDL.

Par exemple, pour exclure une application antivirus du répertoire Program Files, le chemin d'exclusion serait :

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

Sans barre oblique, le **connecteur Windows** fait une correspondance partielle sur les chemins, alors que **Mac et Linux ne font pas.**

Exemple si vous appliquez les exclusions de chemin suivantes "**C:\Program Files"** et comme **"C:\test" :**

Les fichiers C:\Program et les **fichiers C:\Program (x86)** sont exclus :

<#root>

C:\Program Files

C:\Program Files (x86)

C:\test est exclu, comme **C:\test123** :

<#root>

C:\test

C:\test123

Vous pouvez changer l'exclusion de "**C:\test"** à "**C:\test\"**, cela empêche "**C:\test123"** d'être exclu.

Remarque : les exclusions de chemin sont récursives et excluent également tous les sous-répertoires.

Extension de fichier

Ces exclusions permettent l'exclusion de tous les fichiers ayant une certaine extension.

Principaux points :

- L'entrée attendue côté connecteur est **.extension**
- Le tableau de bord ajoute automatiquement un point à l'extension de fichier si aucune extension n'a été ajoutée.
- Les postes ***ne*** sont ***pas*** sensibles à la casse.

Par exemple, pour exclure tous les fichiers de base de données Microsoft Access, vous pouvez créer l'exclusion suivante :

```
.MDB
```

> **Remarque** : les exclusions standard sont disponibles dans la liste par défaut. Il n'est **pas** recommandé de supprimer ces exclusions, ce qui peut entraîner des modifications des performances sur vos *ordinateurs*.

Caractère Générique

Ces exclusions sont identiques aux exclusions de chemin d'accès ou d'extension, à l'exception de l'utilisation d'un astérisque (*) comme déclencheur générique.

> **Attention** : l'exclusion générique ne s'arrête pas aux séparateurs de chemins, ce qui peut entraîner des exclusions non souhaitées. Exemple : **C:*\test** exclut **C:\sample\test** ainsi que **C:\1\test** ou C:\sample\test123 .

> **Avertissement** : le début d'une exclusion avec un astérisque (*) peut entraîner des problèmes de performances majeurs. Avec la version **7.5.3+**, l'ajout d'exclusions de processus générique a causé des problèmes de performances supplémentaires avec des exclusions avec astérisque. Veuillez supprimer ou modifier toutes les exclusions dans ce format pour limiter l'impact sur le processeur.

Par exemple, excluez les ordinateurs virtuels sur un MAC de l'analyse, entrez cette exclusion de chemin :

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

Cette exclusion ne fonctionne que pour *johndoe*, pour permettre plusieurs correspondances d'utilisateurs, remplacez le nom d'utilisateur dans le chemin par un astérisque (*) pour une exclusion générique :

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

Écrivez une exclusion pour les chemins qui existent dans des lecteurs séparés.

Exemple : **C:\testpath** et **D:\testpath** sont :

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

Le système génère automatiquement le ^[A-Za-z] lorsque la case « Appliquer à toutes les lettres de lecteur » est cochée après que le caractère générique est sélectionné dans la liste déroulante Type d'exclusion, comme illustré dans l'image :

Process

Les exclusions de processus permettent aux administrateurs d'exclure les processus en cours d'exécution des analyses de fichiers normales (Connecteur Windows Secure Endpoint version 5.1.1 et ultérieure), Protection des processus système (Connecteur version 6.0.5 et ultérieure) ou Protection contre les activités malveillantes (Connecteur version 6.1.5 et ultérieure).

L'exclusion de processus se fait soit en spécifiant le chemin complet vers l'exécutable de processus, la valeur SHA-256 de l'exécutable de processus, soit à la fois le chemin et le SHA-256. Les chemins autorisent les deux chemins directs ou utilisent une valeur CSIDL.

> **Attention** : les processus enfants créés par un processus exclu **ne** sont **pas** inclus dans l'exclusion par défaut. Exemple : l'exclusion de processus pour MS Word n'exclurait pas par défaut les processus supplémentaires créés par Word.exe et serait analysée. Pour inclure d'autres processus, cochez la case **Appliquer aux processus enfants**. En outre, l'exclusion de Word.exe n'est pas suggérée car les programmes malveillants se cachent régulièrement dans les fichiers .docx modernes.

> **Remarque** : la spécification du chemin et du SHA-256 est requise pour que les deux conditions soient remplies afin d'exclure le processus.

Limites:

- Si la taille de fichier du processus est supérieure à la taille de fichier d'analyse maximale définie dans votre stratégie, le SHA-256 du processus n'est pas calculé et l'exclusion **ne fonctionne pas**. Utiliser une exclusion de processus basée sur le chemin pour les fichiers dont la taille est supérieure à la taille maximale du fichier à analyser
- Versions 5.x.x à 6.0.3 du connecteur : limite de 25 exclusions de processus pour tous les types d'exclusion de processus
- Versions 6.0.5+ du connecteur : limite de 100 exclusions de processus pour tous les types d'exclusion de processus.
- Connecteur versions 7.x.+ - limite de 500 exclusions de processus pour tous les types d'exclusion de processus.
- Le connecteur n'accepte que les exclusions de processus jusqu'à la limite, en haut de la liste des exclusions de processus dans policy.xml
- Chaque stratégie a une exclusion de processus pour sfc.exe, qui compte par rapport à la limite

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

Menace

Ces exclusions permettent d'exclure un nom de menace particulier du déclenchement d'événements. L'exclusion des menaces ne doit être utilisée que lorsque le résultat de l'analyse déclenche une détection de faux positifs et confirme qu'il ne s'agit pas d'une menace réelle.

La zone de texte permettant d'ajouter une exclusion de menace ***ne respecte pas*** la casse. Exemple :

W32.Zombies.NotAVirus ou w32.zombies.notavirus correspondent tous deux au même nom de menace.

> **Avertissement** : n'excluez pas les menaces à moins que l'enquête et la confirmation du nom de la menace ne soient considérées comme des faux positifs. Les menaces exclues ne sont plus renseignées dans l'onglet Événements à des fins de révision et d'audit.

Caractère Générique De Processus

Fenêtres

Le point de terminaison 7.5.3+ permet des exclusions supplémentaires à l'aide de la fonctionnalité de caractères génériques dans les exclusions de processus. Cela permet une couverture plus large avec moins d'exclusions, mais peut également être dangereux si trop est laissé indéfini. **Vous ne devez utiliser le caractère générique que pour couvrir le nombre minimum de caractères requis pour fournir l'exclusion requise.**

Utilisation du caractère générique (*) dans le processus pour Windows :

- (*) Peut être utilisé à la place d'un caractère unique ou d'un répertoire complet. Il ne peut pas être placé au début du chemin, il sera déclaré non valide. Le caractère générique fonctionne entre deux caractères définis, barres obliques ou caractères alphanumériques. Le placer à la fin d'un chemin d'accès exclura les processus de ce répertoire mais pas les sous-répertoires.
- (**) Peut être utilisé à la fin d'un chemin d'accès pour exclure tous les processus dans ce répertoire et les processus dans les sous-répertoires. Cela permet un jeu d'exclusions beaucoup plus grand avec une entrée minimale, mais laisse également un très grand trou de sécurité pour la visibilité. **Utilisez cette fonction avec une extrême prudence**.

Exemples:

```
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 et Linux

Le point de terminaison 1.15.2+ permet des exclusions supplémentaires à l'aide de la fonctionnalité de caractères génériques dans les exclusions de processus. Cela permet une couverture plus large avec moins d'exclusions, mais peut également être dangereux si trop est laissé indéfini. **Vous ne devez utiliser le caractère générique que pour couvrir le nombre minimum de caractères requis pour fournir l'exclusion requise.**

Utilisation du caractère générique (*) en cours pour Mac :

- (*) Peut être utilisé à la place d'un caractère unique ou d'un répertoire complet. Il ne peut pas être placé au début du chemin, il sera déclaré non valide. Le caractère générique fonctionne entre deux caractères définis, barres obliques ou caractères alphanumériques.

Exemples:

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

Exclusions de prévention des exploits (application)

Fenêtres

Secure Endpoint 7.5.1+ utilise la version V5 du moteur de prévention des exploits et la console permet désormais de configurer les exclusions d'application dans la fonctionnalité de liste d'exclusion actuelle. **Actuellement, cette procédure est limitée aux applications et toute exclusion relative aux DLL doit toujours être effectuée par le biais de l'ouverture d'un dossier auprès de l'assistance.**

La recherche des exclusions correctes pour la prévention des exploits est un processus beaucoup plus intensif que tout autre type d'exclusion et nécessite des tests approfondis afin de réduire les failles de sécurité.

Erreurs courantes à éviter

Soyez prudent lorsque vous créez des exclusions, car cela réduit le niveau de protection fourni par Cisco Secure Endpoint. Les fichiers exclus ne sont pas hachés, analysés ou disponibles dans le cache ou le cloud, l'activité n'est pas surveillée et des informations sont manquantes dans les moteurs principaux, la trajectoire des périphériques et l'analyse avancée.

Les exclusions *ne* doivent être utilisées *que* dans des cas ciblés, tels que des problèmes de compatibilité avec des applications spécifiques ou des problèmes de performances qui ne pourraient être améliorés autrement.

Voici quelques erreurs courantes à éviter lorsque vous travaillez avec des exclusions.

- **Exclusions proactives**
  - Ne supposez pas qu'une exclusion est nécessaire à moins qu'il ait été prouvé qu'il s'agissait d'un problème qui ne peut être résolu autrement. Les problèmes de performances, les faux positifs ou les problèmes de compatibilité des applications doivent faire l'objet d'une étude approfondie et d'une atténuation avant d'appliquer une exclusion

- **Une exclusion trop large.**
  - Exclusion de grandes parties du terminal, comme l'intégralité du lecteur C
  - Utiliser une exclusion générique lorsqu'une exclusion plus spécifique est possible
  - En utilisant uniquement le nom du fichier au lieu d'un chemin d'accès complet au fichier
  - Utiliser le package de diagnostics de la trajectoire du périphérique ou du terminal sécurisé et l'outil de réglage des performances pour étudier et déterminer l'exclusion spécifique nécessaire

- **Surutilisation des exclusions génériques**
  - Non seulement les exclusions génériques créent plus de failles de sécurité, mais elles nécessitent également plus de ressources système que tout autre type d'exclusion
  - Assurez-vous d'utiliser la quantité minimale de caractères génériques dans une exclusion ; seuls les dossiers qui sont vraiment variables doivent être rendus variables avec un caractère générique. Exemple :
    - Program Files\Software* exclut tout le contenu du dossier, mais pas les sous-dossiers
    - Program Files\Software** exclut tout le contenu du dossier, y compris les sous-dossiers

- **Exclusion des éléments utilisés dans les attaques**

    - Types de fichiers tels que .cmd, .zip, .jpg, etc
    - Processus tels que svchost.exe, bash.exe, powershell.exe, etc.
    - Emplacements de dossiers tels que C:\Users\, C:\Windows\Temp\, C:\Program Files\Java, etc

- **Exclusions en double**
    - Avant de créer une exclusion, vérifiez si l'exclusion existe déjà dans les exclusions personnalisées créées par l'utilisateur ou dans les exclusions gérées par Cisco.
    - La suppression des exclusions en double améliore non seulement les performances, mais réduit également la gestion opérationnelle des exclusions

- **Exclusions périmées**
    - Les exclusions créées il y a longtemps et qui ne sont peut-être pas encore nécessaires.
    - Vérifiez régulièrement votre liste d'exclusions et assurez-vous de conserver un enregistrement des raisons pour lesquelles une certaine exclusion a été ajoutée.

- **Ne pas supprimer les exclusions après l'infection**
    - Les exclusions doivent être supprimées une fois qu'une infection a été identifiée afin de retrouver une sécurité et une visibilité optimales
    - L'utilisation de la fonction d'actions automatisées « Déplacer l'ordinateur vers le groupe » à l'avance vous permettra d'appliquer rapidement une stratégie plus sécurisée après l'infection, y compris la configuration d'une stratégie sans exclusions

- **Manque de tactiques d'atténuation**
    - Lorsque des exclusions sont absolument nécessaires, réfléchissez aux tactiques d'atténuation qui peuvent être utilisées, comme l'activation de la protection en écriture pour ajouter des couches de protection pour les éléments exclus.

Pour plus d'informations sur les exclusions ou les terminaux sécurisés, consultez le Guide des meilleures pratiques

Exclusions non recommandées

Afin d'assurer une bonne sécurité et une bonne visibilité, les exclusions suivantes ne sont pas recommandées :

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
0,7 z
.bat
.bin
cabine
.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
.système
.tar
.tmp
URL
.vbe
.vbs
.wsf
.zip
coup
java
python
python3

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 Fichiers\<nom de la société>\
C:\Program Fichiers (x86)\<nom de la société>\
C:\Users\<NomProfilUtilisateur>\AppData\Local\Temp\
C:\Users\<NomProfilUtilisateur>\AppData\LocalLow\Temp\

Informations connexes

- **Assistance et documentation techniques - Cisco Systems**
- **Cisco Secure Endpoint - Notes techniques**
- **Cisco Secure Endpoint - Guide de l'utilisateur**
- **Secure Endpoint : exclusions de processus dans macOS et Linux**

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.