Configuration et identification des exclusions de terminaux sécurisés

Table des matières

- Introduction
- Avertissement
- Aperçu
- Que sont les exclusions
  - Exclusions maintenues par Cisco
  - Exclusions personnalisées
- Types d'exclusions
  - Exclusions de processus
    - MacOS et Linux
    - Fenêtres
  - Exclusions des menaces
  - Exclusions de chemin
    - Correspondances de chemins partiels (Windows uniquement)
  - Exclusions d'extensions de fichier
  - Exclusions de caractères génériques
    - Fenêtres
  - Exclusions d'exécutables (Windows uniquement)
  - Exclusions IOC (Windows uniquement)
- CSIDL et KNOWNFOLDERID (Windows uniquement)
- Préparer le connecteur pour le réglage d'exclusion
- Identifier les exclusions
  - MacOS et Linux
    - Création d'exclusions de processus
    - Création d'exclusions de chemin d'accès, d'extension de fichier et de caractères génériques
    - moteur de protection comportementale
  - Fenêtres
- Création de règles d'exclusion dans la console Secure Endpoint
- Meilleures pratiques
  - Exclusions non recommandées
- Informations connexes

Introduction

Ce document décrit les exclusions, comment identifier les exclusions et les meilleures pratiques pour créer des exclusions sur Cisco Secure Endpoint.

Avertissement

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 l’incidence possible des commandes.

Aperçu

Après avoir lu ce document, vous devez comprendre :

- Qu'est-ce qu'une exclusion et les différents types d'exclusions disponibles pour Cisco Secure Endpoint.
- Comment préparer votre connecteur pour le réglage d'exclusion.
- Comment identifier les exclusions potentiellement fortes.
- Comment créer de nouvelles exclusions dans Cisco Secure Endpoint Console.
- Quelles sont les meilleures pratiques pour créer des exclusions ?

Que sont les exclusions

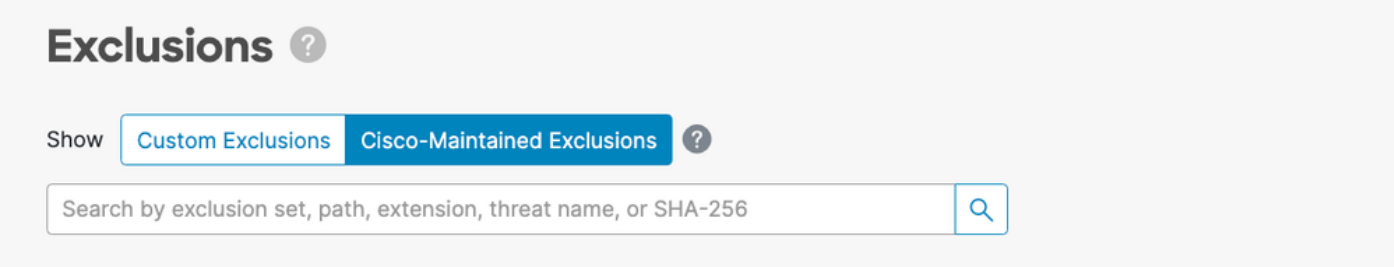
Un jeu d'exclusions est une liste de répertoires, d'extensions de fichiers, de chemins d'accès aux fichiers, de processus, de noms de menaces, d'applications ou d'indicateurs de compromission que vous ne souhaitez pas que le connecteur analyse ou détecte. Les exclusions doivent être conçues avec soin 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, de même que l'entité qui le contrôle, et va des politiques strictes aux politiques ouvertes. Par conséquent, les exclusions doivent être adaptées à chaque situation.

Les exclusions peuvent être classées de deux manières : les exclusions maintenues par Cisco et les exclusions personnalisées.

Exclusions maintenues par Cisco

Les exclusions maintenues par Cisco sont des exclusions qui ont été créées sur la base de recherches et qui ont fait l'objet de tests rigoureux sur les systèmes d'exploitation, programmes et autres logiciels de sécurité couramment utilisés. Ces exclusions peuvent être affichées en sélectionnant Exclusions gérées par Cisco dans la console Secure Endpoint sur la page Exclusions :

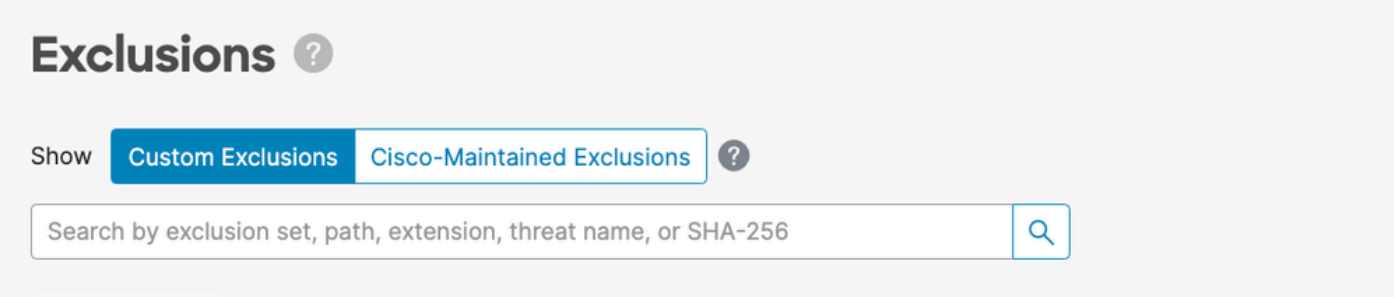


Cisco surveille les listes d'exclusions recommandées publiées par les fournisseurs d'antivirus et met à jour les exclusions maintenues par Cisco pour inclure les exclusions recommandées.

Remarque : Certains fournisseurs d'antivirus ne publient pas leurs exclusions recommandées. Dans ce cas, vous devez contacter le fournisseur AV pour demander une liste des exclusions recommandées, puis ouvrir un dossier d'assistance pour mettre à jour les exclusions maintenues par Cisco.

Exclusions personnalisées

Les exclusions personnalisées sont des exclusions qui ont été créées par un utilisateur pour un exemple d'utilisation personnalisé sur un point de terminaison. Ces exclusions peuvent être affichées en sélectionnant Exclusions personnalisées dans la console Secure Endpoint sur la page Exclusions.



Types d'exclusions

Exclusions de processus

Les exclusions de processus permettent aux administrateurs d'exclure des processus des moteurs pris en charge. Les moteurs qui prennent en charge les exclusions de processus sur chaque plate-forme sont décrits dans ce tableau :

Système d'exploitation	Moteur			
	Analyse de fichiers	Protection des processus système	Protection contre les activités malveillantes	Protection Comportementale
Fenêtres	✓	✓	✓	✓
Linux	✓	✗	✗	✓
macOS	✓	✗	✗	✓

MacOS et Linux

Vous devez fournir un chemin d'accès absolu lors de la création d'une exclusion de processus. Vous pouvez également fournir un utilisateur facultatif. Si vous spécifiez à la fois un chemin et un utilisateur, les deux conditions doivent être remplies pour que le processus soit exclu. Si vous ne spécifiez pas d'utilisateur, l'exclusion de processus s'applique à tous les utilisateurs.



Remarque : Sur macOS et Linux, les exclusions de processus s'appliquent à tous les moteurs.

Caractères génériques de processus :

Les connecteurs Secure Endpoint Linux et macOS prennent en charge l'utilisation d'un caractère générique dans l'exclusion de processus. Cela permet une couverture plus large avec moins d'exclusions, mais peut également être dangereux si trop est laissé indéfini.



Mise en garde : Vous ne devez utiliser le caractère générique que pour couvrir le nombre minimum de caractères requis pour fournir l'exclusion requise.

Utilisation du masque générique de processus pour macOS et Linux :

- Le caractère générique est représenté par un seul astérisque (*).
- Le caractère générique peut être utilisé à la place d'un caractère unique ou d'un répertoire complet.
- Le placement du caractère générique au début du chemin est considéré comme non valide.
- Le caractère générique fonctionne entre deux caractères définis, barres obliques ou caractères alphanumériques.

Exemples:

Exclusion	Résultat prévu
/Library/Java/JavaVirtualMachines/*/java	Exclut Java dans tous les sous-dossiers de JavaVirtualMachines
/Bibliothèque/Jibber/j*bber	Exclut le processus pour jabber, jibber, jobber, etc

Fenêtres

Vous pouvez fournir un chemin d'accès absolu et/ou un SHA-256 de l'exécutable de processus lors de la création d'une exclusion de processus. Si vous spécifiez à la fois un chemin et SHA-256, alors les deux conditions doivent être remplies pour que le processus soit exclu.

Sous Windows, vous pouvez également utiliser CSIDL ou KNOWNFOLDERID dans le chemin pour créer des exclusions de processus.

⚠ Mise en garde : Les processus enfants créés par un processus exclu ne sont pas exclus par défaut. Pour exclure d'autres processus lors de la création d'une exclusion de processus, sélectionnez Appliquer aux processus enfants.

Limites:

- Si la taille de fichier du processus est supérieure à la taille maximale de fichier d'analyse définie dans votre stratégie, le SHA-256 du processus n'est pas calculé et l'exclusion ne fonctionne pas. Utilisez une exclusion de processus basée sur le chemin pour les fichiers dont la taille est supérieure à la taille maximale du fichier à analyser.
- Le connecteur Windows impose une limite de 500 exclusions de processus pour tous les types d'exclusion de processus.
    - Les exclusions de processus ne sont respectées que jusqu'à la limite, en commençant par le haut de la liste des exclusions de processus dans policy.xml.
    - Chaque stratégie Windows a une exclusion de processus pour sfc.exe, qui compte par rapport à la limite d'exclusions de processus :

      ```
      <item>3|0||CSIDL_Secure Endpoint_VERSION\sfc.exe|48|</item>
      ```

✎ Remarque : Sous Windows, les exclusions de processus sont appliquées par moteur. Si la même exclusion doit être appliquée à plusieurs moteurs, alors l'exclusion de processus doit être dupliquée dans ce cas pour chaque moteur applicable.

Caractères génériques de processus :

Les connecteurs Windows de point de terminaison sécurisé prennent en charge l'utilisation d'un caractère générique dans l'exclusion de processus. Cela permet une couverture plus large avec moins d'exclusions, mais peut également être dangereux si trop est laissé indéfini.

⚠ Mise en garde : 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 de processus pour Windows :

- Le caractère générique est représenté par un seul astérisque (*) ou un double astérisque (**)
- Caractère générique astérisque unique (*) :
    - Le caractère générique peut être utilisé à la place d'un caractère unique ou d'un

répertoire complet.
    - Le placement du caractère générique au début du chemin est considéré comme non valide.
    - Le caractère générique fonctionne entre deux caractères définis, barres obliques ou caractères alphanumériques.
    - Le placement du caractère générique à la fin d'un chemin d'accès exclut tous les processus de ce répertoire, mais pas les sous-répertoires.
- Caractère générique double astérisque (**) :
    - Ne peut être placé qu'à la fin d'un tracé.
    - Le fait de placer le caractère générique à la fin d'un chemin d'accès exclut tous les processus de ce répertoire et tous les processus des 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:

Exclusion	Résultat attendu
C:\Windows*\Tiworker.exe	Exclut tous les processus Tiworker.exe trouvés dans les sous-répertoires de Windows
C:\Windows\P*t.exe	Exclut Pot.exe, Pat.exe, P1t.exe, etc
C:\Windows*poulets.exe	Exclut tous les processus du répertoire Windows se terminant par ickens.exe
C:*	Exclut tous les processus dans le C: mais pas dans les sous-répertoires
C:**	Exclut tous les processus sur le C: entraînement

Exclusions des menaces

Les exclusions de menaces vous permettent d'exclure un nom de menace particulier du déclenchement d'événements. Vous ne devez jamais utiliser une exclusion de menace que si vous êtes certain que les événements sont le résultat d'une détection de faux positifs. Dans ce cas, utilisez le nom de menace exact de l'événement comme votre exclusion de menace. Sachez que si vous utilisez ce type d'exclusion, même une détection positive du nom de la menace n'est pas détectée, mise en quarantaine ou générée.



Remarque : Les exclusions de menace ne respectent pas la casse. Exemple : W32.Zombies.NotAVirus et w32.zombies.notavirus correspondent tous deux au même nom de menace.



Avertissement : N'excluez pas les menaces à moins qu'une enquête approfondie n'ait confirmé que le nom de la menace était faux positif. Les menaces exclues ne renseignent

plus l'onglet Événements pour la révision et l'audit.

Exclusions de chemin

Les exclusions de chemin sont les plus fréquemment utilisées, car les conflits d'application impliquent généralement l'exclusion d'un répertoire. Vous pouvez créer une exclusion de chemin à l'aide d'un chemin absolu. Sous Windows, vous pouvez également utiliser CSIDIL ou KNOWNFOLDERID pour créer des exclusions de chemin.

Par exemple, pour exclure une application AV du répertoire Program Files sous Windows, le chemin d'exclusion peut être l'un des chemins suivants :

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



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

Correspondances de chemins partiels (Windows uniquement)

Si aucune barre oblique n'est fournie dans l'exclusion de chemin, le connecteur Windows effectue une correspondance partielle sur les chemins.



Remarque : Mac et Linux ne prennent pas en charge les correspondances de chemins partielles.

Par exemple, si vous appliquez les exclusions de chemin suivantes sous Windows :

```
C:\Program Files
C:\test
```

Ensuite, tous ces chemins sont exclus :

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

```
C:\test
C:\test123
```

Si vous remplacez l'exclusion C:\test par C:\test\, C:\test123 ne sera plus exclu.

Exclusions d'extensions de fichier

Les exclusions d'extension de fichier permettent l'exclusion de tous les fichiers portant une certaine extension.

Principaux points :

- L'entrée attendue dans la console Secure Endpoint est .extension
- La console Secure Endpoint ajoute automatiquement un point à l'extension de fichier si aucune extension n'a été ajoutée.
- Les extensions ne respectent pas la casse.

Par exemple, afin d'exclure tous les fichiers de base de données Microsoft Access, vous pouvez créer cette exclusion :

```
.MDB
```



Remarque : Les exclusions d'extension de fichier standard sont disponibles dans la liste par défaut. Il n'est pas recommandé de supprimer ces exclusions, ce qui peut entraîner des modifications de performances sur votre point de terminaison.

Exclusions de caractères génériques

Les exclusions avec caractère générique sont identiques aux exclusions avec chemin d'accès ou extension de fichier, à ceci près que vous pouvez utiliser un astérisque (*) pour représenter un caractère générique dans le chemin d'accès ou l'extension.

Par exemple, si vous souhaitez exclure de l'analyse vos machines virtuelles sur macOS, vous pouvez entrer cette exclusion de chemin :

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

Cependant, cette exclusion ne fonctionne que pour un seul utilisateur. Par conséquent, remplacez le nom d'utilisateur dans le chemin par un astérisque et créez une exclusion générique pour

exclure ce répertoire pour tous les utilisateurs :

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

⚠ Mise en garde : Les exclusions génériques ne s'arrêtent pas aux séparateurs de chemins, ce qui peut entraîner des exclusions non voulues. Par exemple, C:*\test exclut C:\sample\test ainsi que C:\1\test** ou C:\sample\test123.

⚠ Avertissement : Le fait de commencer une exclusion par un astérisque peut entraîner des problèmes de performances majeurs. Supprimez ou modifiez toutes les exclusions commençant par un astérisque pour limiter l'impact sur le processeur.

Fenêtres

Lors de la création d'exclusions génériques sous Windows, vous avez la possibilité d'appliquer à toutes les lettres de lecteur. La sélection de cette option applique l'exclusion générique à tous les lecteurs montés.



Si vous deviez créer manuellement la même exclusion, vous devriez la faire précéder de ^[A-Za-z], par exemple :

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

Dans les deux exemples, les adresses C:\testpath et D:\testpath sont exclues.

La console Secure Endpoint génère automatiquement le ^[A-Za-z] lorsque l'option Appliquer à toutes les lettres de lecteur est sélectionnée pour les exclusions génériques.

Exclusions d'exécutables (Windows uniquement)

Les exclusions exécutables s'appliquent uniquement aux connecteurs Windows avec la prévention des exploits activée. Une exclusion d'exécutable empêche certains exécutables d'être protégés par la prévention des exploits. Vous ne devez exclure un exécutable de la prévention des exploits que si vous rencontrez des problèmes ou de performances.

Vous pouvez vérifier la liste des processus protégés et exclure tout processus de la protection en spécifiant son nom d'exécutable dans le champ d'exclusion d'application. Les exclusions d'exécutable doivent correspondre exactement au nom de l'exécutable au format name.exe. Les caractères génériques ne sont pas pris en charge.

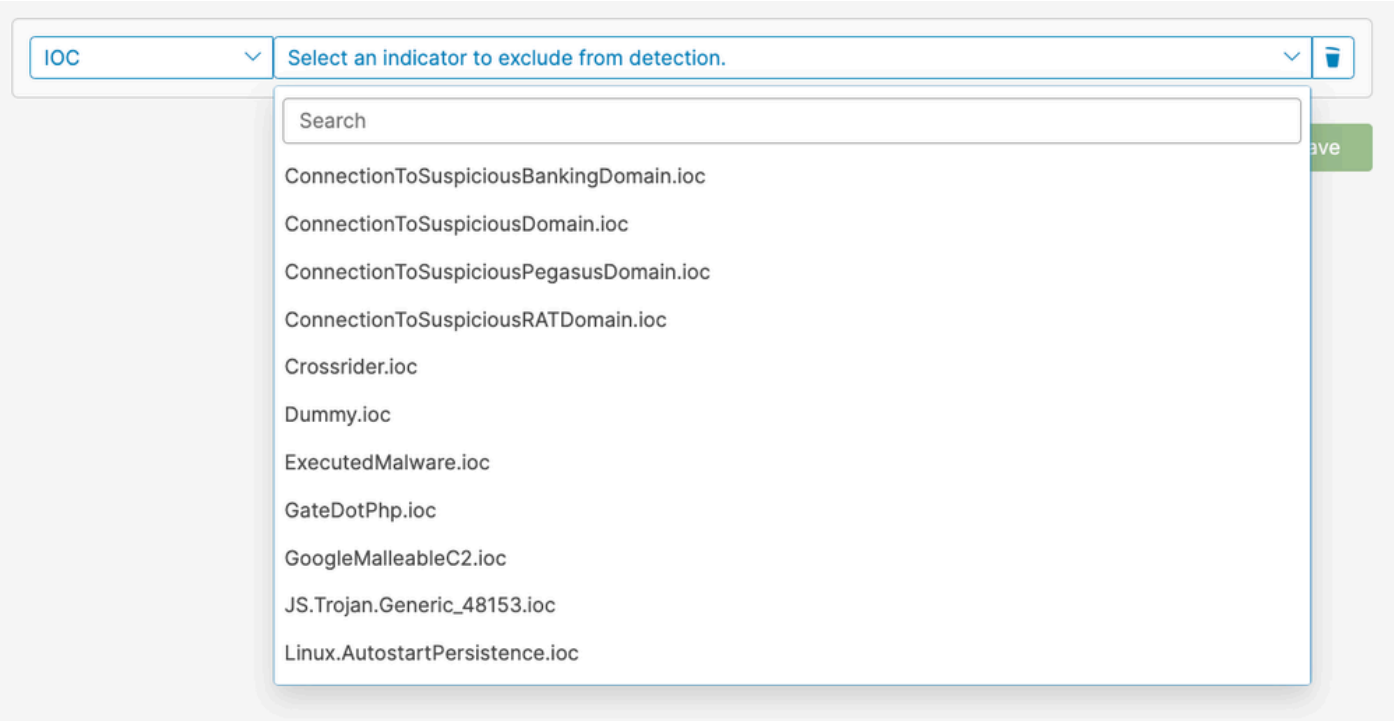
Remarque : Seules les applications peuvent être exclues à l'aide d'exclusions exécutables via Secure Endpoint Console. Toute exclusion liée aux DLL nécessite l'ouverture d'un dossier d'assistance pour la création d'une exclusion.

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.

Exclusions IOC (Windows uniquement)

Les exclusions IOC vous permettent d'exclure les indicateurs de compromission du cloud. Cela peut s'avérer utile si vous disposez d'une application personnalisée ou interne qui ne peut pas être signée et provoque le déclenchement fréquent de certains IOC. Secure Endpoint Console fournit une liste d'indicateurs parmi lesquels choisir pour les exclusions IOC.

Vous pouvez sélectionner les indicateurs à exclure via une liste déroulante :



Remarque : Si vous excluez un IOC de gravité élevée ou critique, vous perdez toute visibilité sur celui-ci et votre entreprise peut être exposée à un risque. Vous ne devez exclure ces indicateurs de compromission que si vous constatez un grand nombre de

---

détections de faux positifs.

CSIDL et KNOWNFOLDERID (Windows uniquement)

Les valeurs CSIDL et KNOWNFOLDERID sont acceptées et encouragées lors de l'écriture d'exclusions de chemin et de processus pour Windows. Les valeurs CSIDL/KNOWNFOLDERID sont utiles pour créer des exclusions de processus et de chemin pour les environnements qui utilisent des lettres de lecteur alternatives.

Il y a des limitations qui doivent être prises en compte lorsque CSIDL/KNOWNFOLDERID est utilisé. Si votre environnement installe des programmes sur plusieurs lettres de lecteur, la valeur CSIDL/KNOWNFOLDERID fait uniquement référence au lecteur marqué comme emplacement d'installation par défaut ou connu.

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/KNOWNFOLDERID dans la liste d'exclusion mise à jour ne s'applique pas à ce chemin. Cela signifie qu'une exclusion doit être entrée pour chaque chemin ou chaque exclusion de processus qui ne se trouve pas sur le lecteur C:\, car l'utilisation de CSIDL/KNOWNFOLDERID ne le mappe pas.

Reportez-vous à cette documentation Windows pour plus d'informations :

- CSIDL
- DOSSIER CONNU



Remarque : KNOWNFOLDERID est uniquement pris en charge dans le connecteur Windows 8.1.7 et versions ultérieures. Les versions antérieures du connecteur Windows utilisent des valeurs CSIDL.



Remarque : Les valeurs KNOWNFOLDERID sont sensibles à la casse. Par exemple, vous devez utiliser la valeur FOLDERID_ProgramFiles et non la valeurFolderID_programfiles non valide.

Préparer le connecteur pour le réglage d'exclusion

Pour préparer votre connecteur au réglage d'exclusion, vous devez :

1. Configurez une stratégie et un groupe à exécuter en mode Débogage.
2. Exécutez les ordinateurs du nouveau groupe de débogage conformément aux opérations

normales de l'entreprise, laissez le temps d'obtenir des données de journal de connecteur suffisantes.
3. Générez des données de diagnostic sur le connecteur à utiliser pour identifier les exclusions.

Reportez-vous à ces documents pour obtenir des instructions sur l'activation du mode de débogage et la collecte de données de diagnostic sur différents systèmes d'exploitation :

- Cisco Secure Endpoint Connector pour la collecte de données de diagnostic Mac
- Cisco Secure Endpoint Connector pour la collecte de données de diagnostic Linux
- Analyser l'offre groupée de diagnostics AMP pour CPU élevé (Windows)

Identifier les exclusions

MacOS et Linux

Les données de diagnostic générées en mode Débogage fournissent deux fichiers utiles pour créer des exclusions : fileops.txt et execs.txt. Le fichier fileops.txt est utile pour créer des exclusions de chemin d'accès/extension de fichier/caractères génériques et le fichier execs.txt est utile pour créer des exclusions de processus.

Création d'exclusions de processus

Le fichier execs.txt répertorie les chemins d'accès aux fichiers exécutables qui ont déclenché l'analyse du fichier Secure Endpoint. 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. Vous pouvez utiliser cette liste pour déterminer les processus avec un volume élevé d'événements d'exécution, puis utiliser le chemin du processus pour créer des exclusions. Cependant, il n'est pas recommandé d'exclure les programmes utilitaires généraux (tels que /usr/bin/grep) ou les interpréteurs (tels que /usr/bin/ruby).

Si un programme utilitaire général ou un interpréteur génère un volume important d'analyses de fichiers, vous pouvez effectuer des recherches supplémentaires pour essayer de créer des exclusions plus ciblées :

1. Exclure le processus parent : déterminez l'application qui exécute le processus (par exemple, recherchez le processus parent qui exécute grep) et excluez ce processus parent. Cela doit être fait, si et seulement si, le processus parent peut être transformé en une exclusion de processus en toute sécurité. Si l'exclusion de parent s'applique aux enfants, les appels à tous les enfants du processus parent sont également exclus.
2. Exclure le processus pour un utilisateur donné : déterminez l'utilisateur qui exécute le processus. Si le processus est exécuté à un volume élevé par un utilisateur spécifique, vous pouvez exclure le processus uniquement pour cet utilisateur spécifique (par exemple, si un processus est appelé à un volume élevé par la racine de l'utilisateur, vous pouvez exclure le processus, mais uniquement pour la racine de l'utilisateur spécifié, cela permet à Secure Endpoint de surveiller les exécutions d'un processus donné par tout utilisateur qui n'est pas la racine).

Exemple de sortie du fichier execs.txt :

```
33 /usr/bin/bash
23 /usr/bin/gawk
21 /usr/bin/wc
21 /usr/bin/sleep
21 /usr/bin/ls
19 /usr/bin/pidof
17 /usr/bin/sed
14 /usr/bin/date
13 /usr/libexec/gdb
13 /usr/bin/iconv
11 /usr/bin/cat
10 /usr/bin/systemctl
 9 /usr/bin/pgrep
 9 /usr/bin/kmod
 7 /usr/bin/rm
 6 /usr/lib/systemd/systemd-cgroups-agent
 6 /usr/bin/rpm
 4 /usr/bin/tr
 4 /usr/bin/sort
 4 /usr/bin/find
```

Création d'exclusions de chemin d'accès, d'extension de fichier et de caractères génériques

Le fichier fileops.txt répertorie les chemins d'accès où les activités de création, de modification et de renommage de fichiers ont déclenché l'analyse de fichiers par Secure Endpoint. 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. Une façon de commencer avec les exclusions de chemin est de trouver les chemins d'accès aux fichiers et dossiers les plus fréquemment analysés à partir de fileops.txt, puis d'envisager de créer des règles pour ces chemins d'accès. Bien qu'un nombre élevé ne signifie pas nécessairement que le chemin doit être exclu (par exemple, un répertoire qui stocke des courriels peut être analysé fréquemment, mais ne doit pas être exclu), la liste fournit un point de départ pour identifier les candidats à l'exclusion.

Exemple de sortie de fileops.txt :

```
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_browsing_sessio
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
```

En règle générale, tout élément doté d'une extension de journal ou de journal doit être considéré comme un candidat d'exclusion approprié.

moteur de protection comportementale

Le moteur de protection comportementale a été introduit dans la version 1.22.0 du connecteur Linux et dans la version 1.24.0 du connecteur macOS ; à partir de ces versions, le connecteur peut détecter une activité extrêmement élevée du système, puis déclencher le défaut 18.

Les exclusions de processus sont appliquées à tous les moteurs et à toutes les analyses de fichiers. Appliquez des exclusions de processus à des processus bénins très actifs afin de corriger cette erreur. Généré par les données de diagnostic du mode de débogage, le fichier top.txt peut être utilisé pour déterminer les processus les plus actifs sur le système. Reportez-vous aux conseils relatifs à la panne 18 du connecteur Mac/Linux du terminal sécurisé pour connaître les étapes de correction détaillées.

En outre, les exclusions de processus peuvent réduire au silence les détections de protection comportementale faussement positives à partir d'un logiciel inoffensif. Pour les détections de faux positifs dans la console Secure Endpoint, le processus peut être exclu pour améliorer la création de rapports.

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.

Création de règles d'exclusion dans la console Secure Endpoint

---

⚠ Mise en garde : Comprenez toujours les fichiers et les processus avant d'écrire une exclusion pour éviter les failles de sécurité sur le terminal.

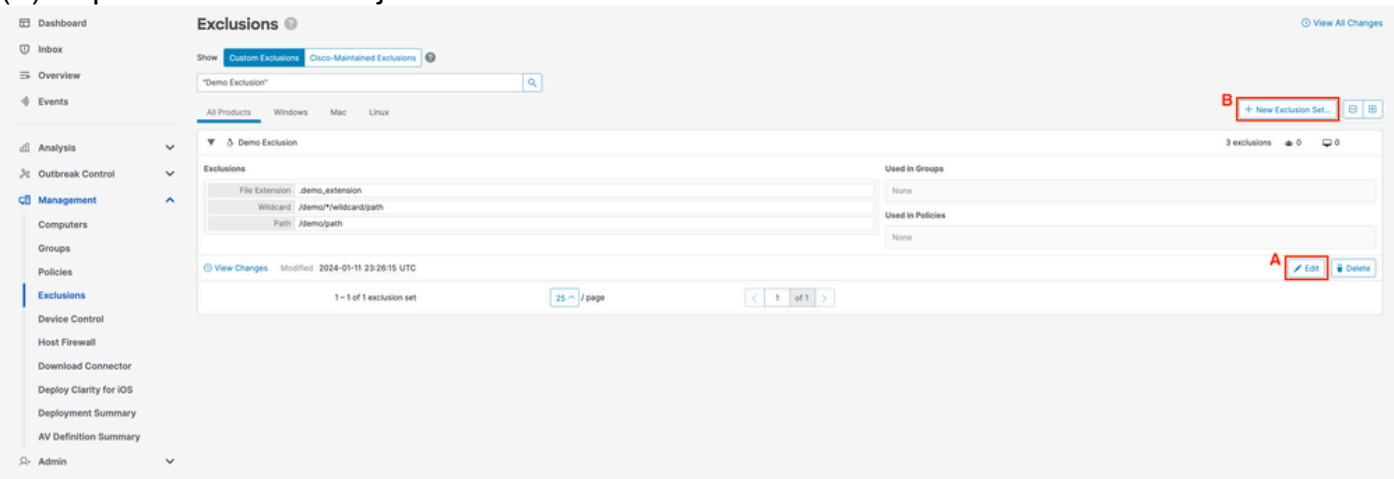
Suivez ces étapes pour créer une nouvelle règle d'exclusion à l'aide de la console Secure Endpoint :

1. Dans la console Secure Endpoint, accédez à la page Policies en sélectionnant Management

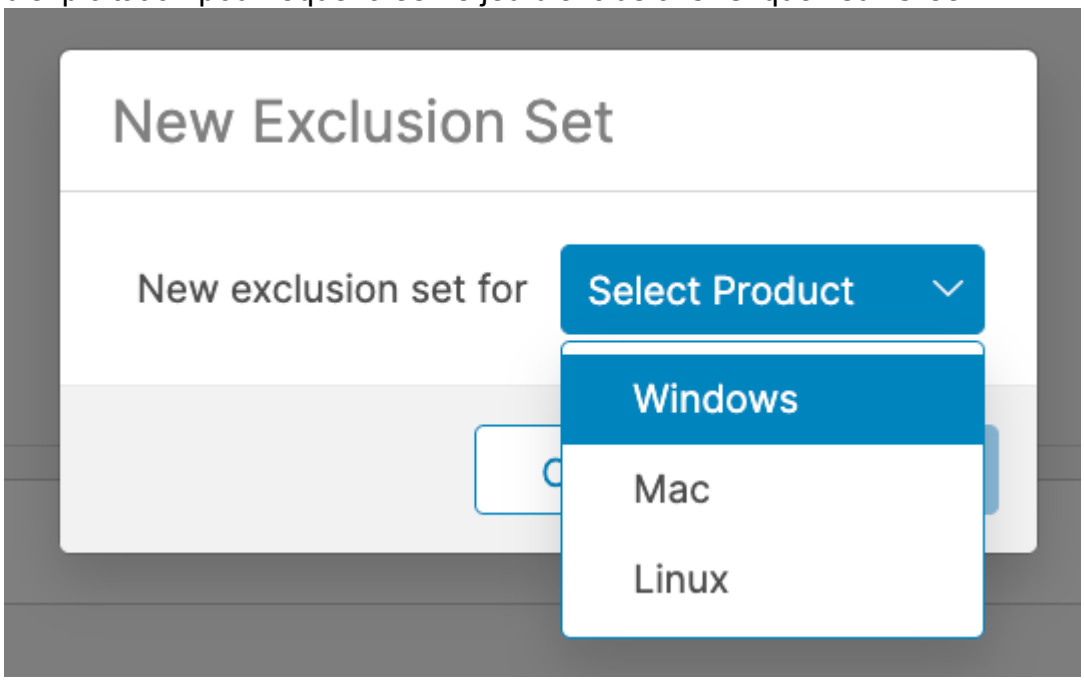
> Exclusions. Soit :

(A) recherchez le jeu d'exclusions que vous souhaitez modifier et cliquez sur Modifier, ou

(B) cliquez sur + Nouveau jeu d'exclusions....

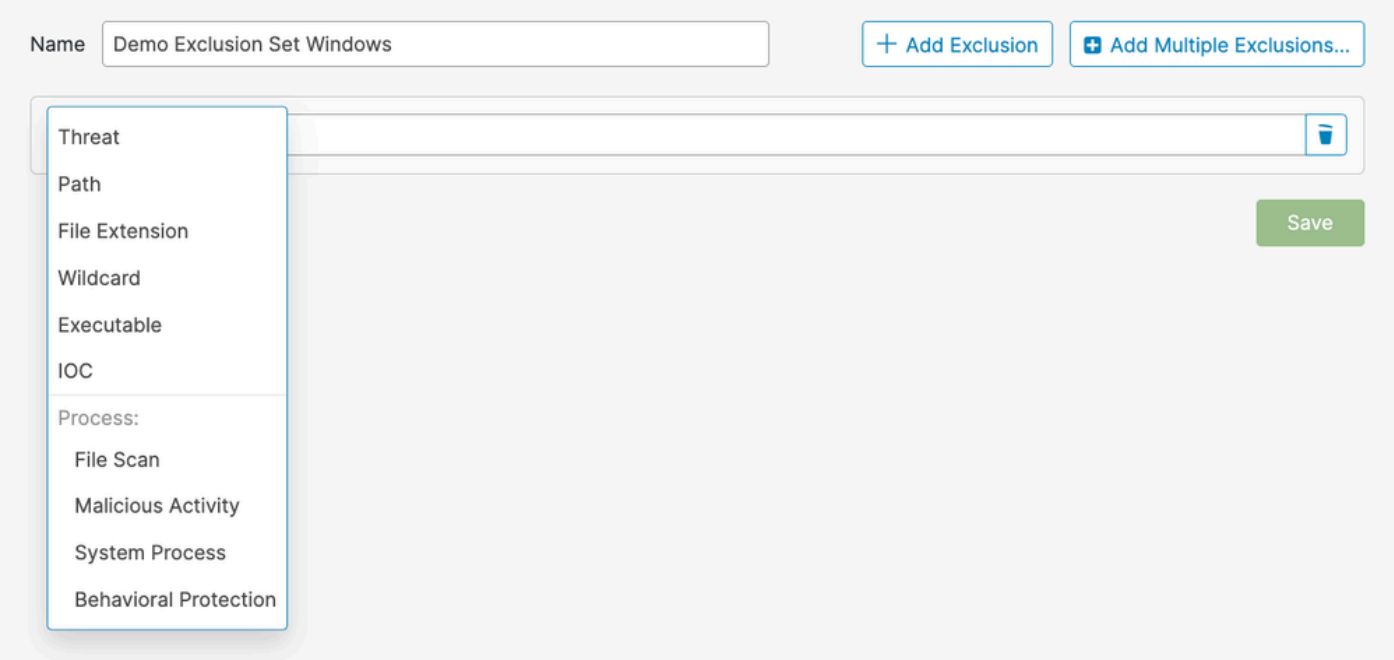


1. Dans la fenêtre contextuelle Nouveau jeu d'exclusions, sélectionnez un système d'exploitation pour lequel créer le jeu d'exclusions. Cliquez sur Créer.

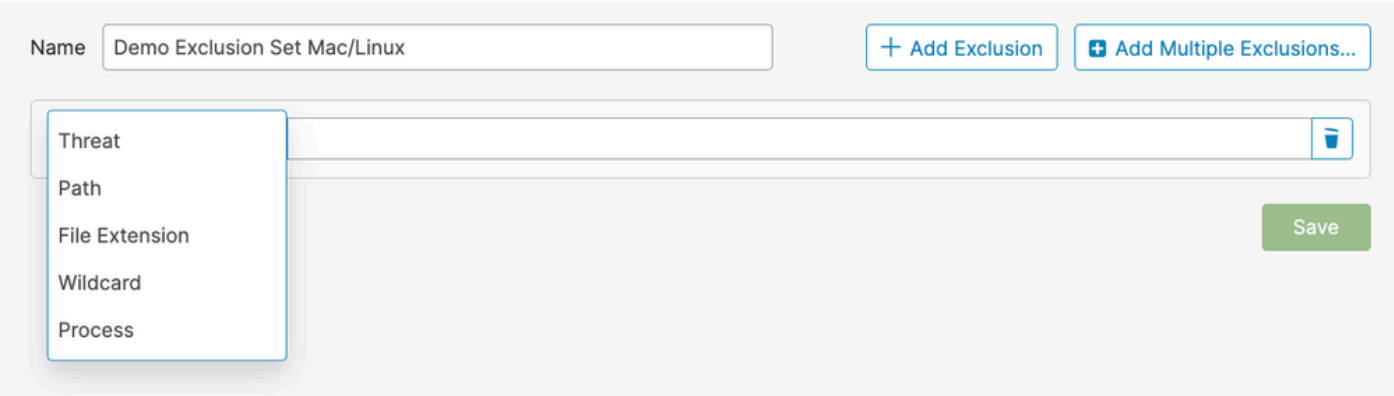


2. Vous êtes redirigé vers la page Nouveau jeu d'exclusions. Cliquez sur + Ajouter exclusion et sélectionnez le type d'exclusion dans la liste déroulante Sélectionner le type.

Fenêtres:



Mac/Linux :



1. Renseignez les champs obligatoires pour le type d'exclusion sélectionné.
2. Répétez les étapes 2 et 3 pour ajouter d'autres règles ou cliquez sur Enregistrer pour enregistrer le jeu d'exclusions.

Meilleures pratiques

⚠ Mise en garde : Soyez prudent lorsque vous créez des exclusions, car elles réduisent 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 peuvent être améliorés autrement.

Voici quelques-unes des meilleures pratiques à suivre lors de la création d'exclusions :

- Ne créez d'exclusions que pour les problèmes éprouvés.
    - Ne présumez 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.
- Préférez les exclusions Processus aux exclusions Chemin/Extension de fichier/Caractères génériques.
    - Les exclusions de processus offrent un moyen plus direct d'exclure les activités logicielles bénignes que l'utilisation d'une combinaison d'exclusions de chemin, d'extension de fichier et de caractères génériques pour obtenir le même résultat.
    - Il est recommandé de remplacer les exclusions Path, File Extension et Wildcard qui ciblent les exécutables de programme par les exclusions Process correspondantes lorsque cela est possible.
- Éviter les exclusions générales.
    - N'excluez pas de grandes parties du point d'extrémité, comme l'intégralité du lecteur C.
    - Utilisez le chemin d'accès complet au fichier au lieu du nom du fichier.
    - Utilisez la fonctionnalité Device Trajectory, Secure Endpoint Diagnostics Data et l'outil de réglage de Windows pour étudier et déterminer les exclusions spécifiques.
- Évitez de surutiliser les exclusions génériques.
    - Soyez prudent lorsque vous créez des exclusions avec des caractères génériques. Utilisez des exclusions plus spécifiques lorsque cela est possible.
    - Utiliser le nombre minimal de caractères génériques dans une exclusion ; seuls les dossiers qui sont vraiment variables doivent utiliser un caractère générique.
- Évitez d'exclure les programmes d'utilitaires généraux et les interprètes.
    - Il n'est pas recommandé d'exclure les programmes d'utilité générale ou les interprètes.
    - Si vous devez exclure un programme utilitaire général ou des interpréteurs, fournissez un utilisateur de processus (macOS/Linux uniquement).
    - Par exemple, évitez d'écrire des exclusions qui incluent python, java, ruby, bash et sh.
- Évitez les exclusions en double.
    - Avant de créer une exclusion, vérifiez si celle-ci existe déjà dans les exclusions personnalisées ou dans les exclusions gérées par Cisco.
    - La suppression des exclusions en double améliore les performances et réduit la gestion opérationnelle des exclusions.
    - Assurez-vous que le chemin spécifié dans une exclusion de processus n'est pas couvert par une exclusion de chemin/extension de fichier/caractère générique.
- Évitez d'exclure les processus connus pour être utilisés couramment dans les attaques de programmes malveillants.
    - Voir Exclusions non recommandées pour plus de détails.
- .Supprimez les exclusions obsolètes.
    - Examinez et vérifiez régulièrement votre liste d'exclusions et notez pourquoi certaines exclusions ont été ajoutées.
- Supprimer les exclusions sur compromission.
    - Les exclusions doivent être supprimées si le connecteur est compromis afin de retrouver une sécurité et une visibilité optimales.
    - Les actions automatisées peuvent être utilisées pour appliquer des stratégies plus

sécurisées aux connecteurs après l'infection. Si un connecteur est compromis, il doit être déplacé vers un groupe qui contient une stratégie sans exclusions pour garantir l'application du niveau de protection le plus élevé.
    - Référez-vous à Identifier les conditions pour déclencher des actions automatisées dans Secure Endpoint pour plus de détails sur la façon de configurer de façon proactive l'action automatisée « Déplacer l'ordinateur vers le groupe en cas de compromission ».
- Augmenter la protection des éléments exclus.
    - 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.
- Créez des exclusions intelligemment.
    - Optimisez les règles en choisissant le processus parent de plus haut niveau qui identifie de manière unique l'application à exclure et utilisez l'option Appliquer au processus enfant pour réduire le nombre de règles.
- N'excluez jamais le processus de démarrage.
    - Le processus de démarrage (lancé sur macOS, init ou systemd sur Linux) est responsable du démarrage de tous les autres processus sur le système et se trouve au sommet de la hiérarchie des processus.
    - L'exclusion du processus de démarrage et de tous ses processus enfants désactiverait efficacement la surveillance Secure Endpoint.
- Spécifiez l'utilisateur du processus si possible (macOS/Linux uniquement).
    - Si le champ utilisateur est laissé vide, l'exclusion s'applique à tout processus exécutant le programme spécifié.
    - Bien qu'une exclusion qui s'applique à n'importe quel utilisateur soit plus flexible, cette large portée pourrait involontairement exclure une activité qui doit être surveillée.
    - La spécification de l'utilisateur est particulièrement importante pour les règles qui s'appliquent aux programmes partagés tels que les moteurs d'exécution (par exemple, java) et les interpréteurs de script (par exemple, bash, python).
    - La spécification de l'utilisateur limite l'étendue et indique à Secure Endpoint d'ignorer des instances spécifiques tout en surveillant d'autres instances.

Exclusions non recommandées

Bien qu'il soit impossible de connaître tous les vecteurs d'attaque possibles qu'un pirate peut utiliser, certains vecteurs d'attaque principaux doivent être surveillés. Pour garantir une bonne sécurité et une bonne visibilité, ces exclusions 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\



Remarque : Il ne s'agit pas d'une liste exhaustive d'exclusions à éviter, mais elle donne un aperçu des vecteurs d'attaque principaux. Il est essentiel de maintenir une visibilité sur ces chemins, extensions de fichiers et processus.

Informations connexes

- Assistance et documentation techniques - Cisco Systems
- Cisco Secure Endpoint - Notes techniques
- Cisco Secure Endpoint - Guide de l'utilisateur
- Dépannage de la prévention des exploits dans Secure Endpoint
- Identifier les conditions de déclenchement des actions automatisées sur les terminaux sécurisés

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.