تكوين استبعادات نقاط النهاية الآمنة وتحديدها

المحتويات

المقدمة

يصف هذا المستند ما هي الاستبعادات، وكيفية تحديد الاستبعادات، وأفضل الممارسات لإنشاء الاستبعادات على نقطة نهاية Cisco الآمنة.

إخلاء المسؤولية

أسست المعلومة في هذا وثيقة على Windows، Linux و MacOS.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

نظرة عامة

بعد قراءة هذا المستند، يجب أن تفهم ما يلي:

- ما هو الاستثناء والأنواع المختلفة من الاستباعادات المتاحة لنقطة النهاية الآمنة من Cisco.
- كيفية إعداد الموصل الخاص بك لمعايرة الاستباعاد.
- كيفية تحديد الاستباعادات المحتملة القوية.
- كيفية إنشاء إستثناءات جديدة في وحدة تحكم نقطة النهاية الآمنة من Cisco.
- ما هي أفضل الممارسات لإنشاء الاستباعادات.

ما هي الاستباعادات؟

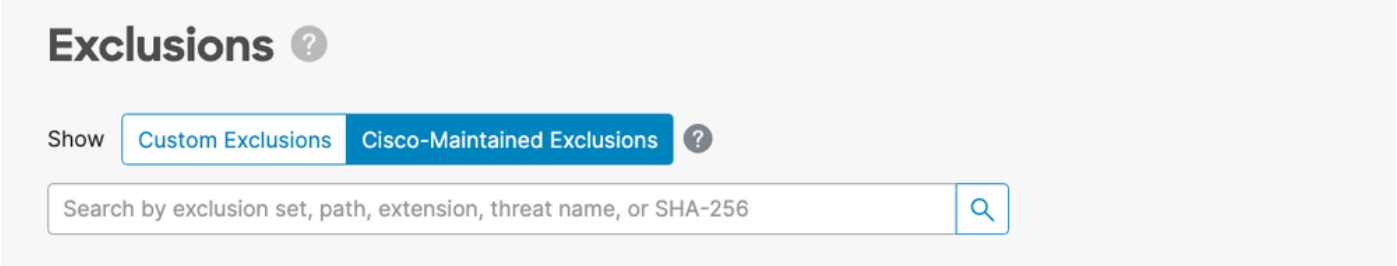
مجموعة الاستثناء هي قائمة من الأدلة، امتدادات الملفات، مسارات الملفات، العمليات، أسماء التهديدات، التطبيقات، أو مؤشرات التسوية التي لا تريد من الموصل مسحها أو إدانتها. يجب صياغة الاستباعادات بعناية لضمان تحقيق التوازن بين الأداء والأمان على الجهاز عند تمكين حماية نقطة النهاية مثل نقطة النهاية الآمنة. تصف هذه المقالة إستثناءات لسحابة نقطة النهاية الآمنة و TETRA و SPP و MAP.

وكل بيئة فريدة من نوعها، فضلا عن الكيان الذي يسيطر عليها، وهي تتنوع من السياسات الصارمة إلى السياسات المفتوحة. وعلى هذا النحو، يجب أن تكون الاستباعادات مصممة بشكل فريد لكل حالة.

يمكن تصنيف الاستباعادات بطريقتين، الاستباعادات والاستباعادات المخصصة التي تحافظ عليها Cisco.

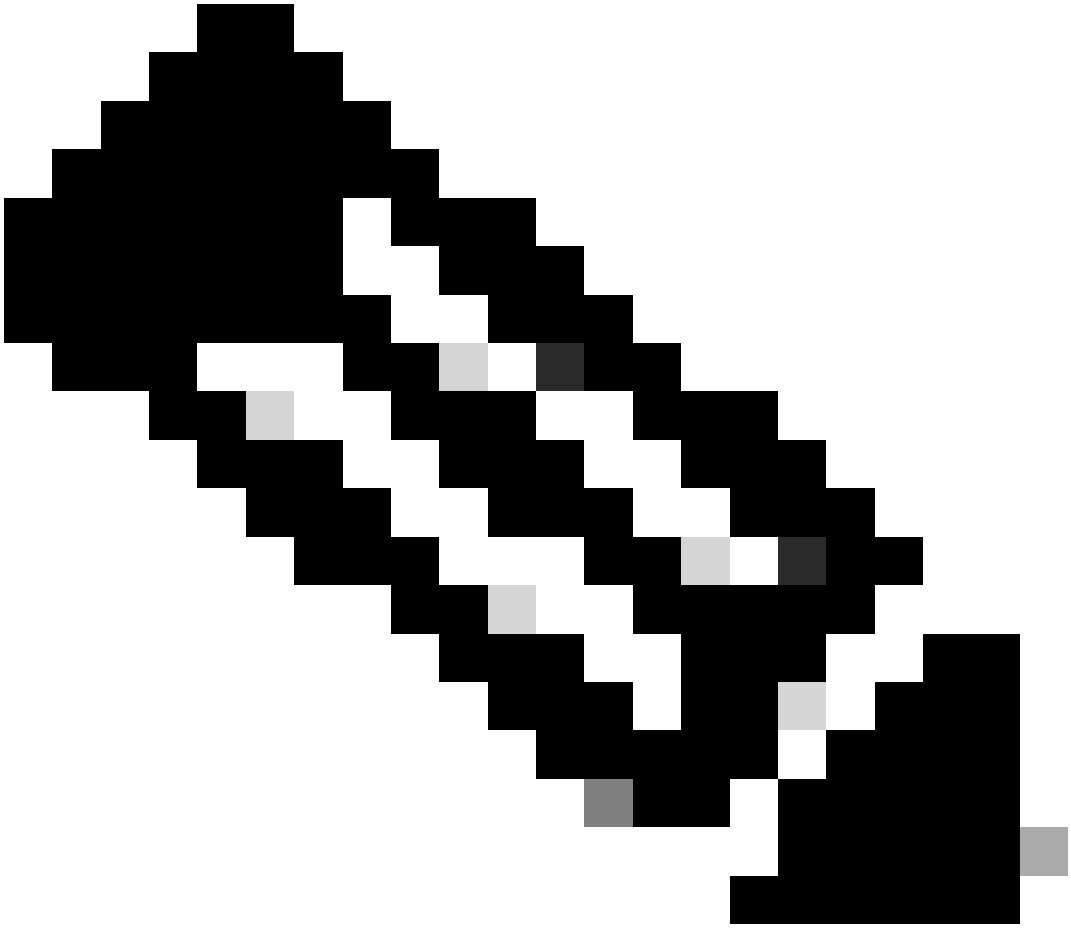
الاستثناءات التي قامت Cisco بصيانتها

الاستثناءات التي يتم صيانتها من Cisco هي استباعادات تم إنشاؤها بناء على أبحاث وخضعت لاختبار دقيق على أنظمة التشغيل والبرامج وبرامج الأمان الأخرى الشائعة الاستخدام. يمكن عرض هذه الاستباعادات من خلال تحديد الاستباعادات التي يتم صيانتها من قبل Cisco في وحدة تحكم نقطة النهاية الآمنة على صفحة الاستباعادات.



ترافق Cisco قوائم الاستباعاد الموصى بها التي ينشرها مورد برامج مكافحة الفيروسات

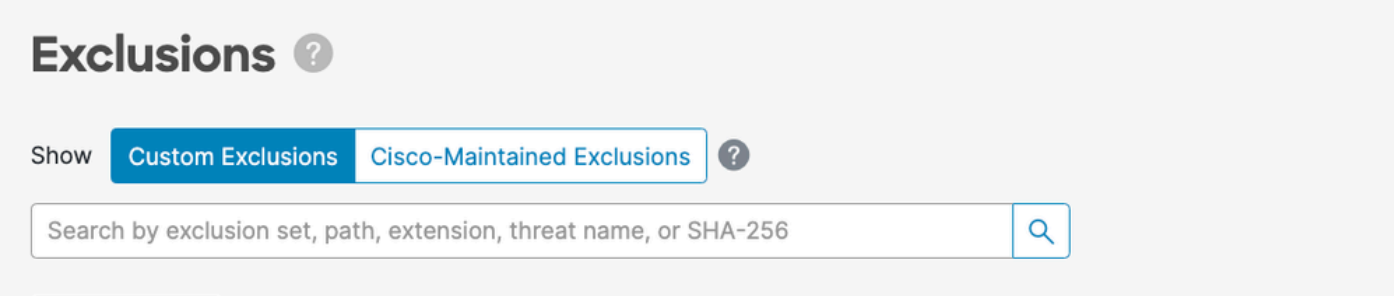
(AV) وتقوم بتحديث الاستثناءات التي يتم صيانتها من Cisco لتضمين الاستثناءات الموصى بها.



ملاحظة: قد لا ينشر بعض بائعي الصوت والفيديو استباعاتهم الموصى بها. في هذه الحالة، قد يحتاج العميل إلى الوصول إلى مورد الصوت والفيديو (AV) لطلب قائمة بالاستباعات الموصى بها ثم فتح حالة دعم للحصول على تحديث الاستثناءات التي يتم صيانتها من Cisco.

استباعات مخصصة

الاستباعات المخصصة هي استباعات تم إنشاؤها بواسطة مستخدم لحالة إستخدام مخصص على نقطة نهاية. يمكن عرض هذه الاستباعات من خلال تحديد استباعات مخصصة في وحدة تحكم نقطة النهاية الآمنة في صفحة الاستباعات.



أنواع الاستبعادات

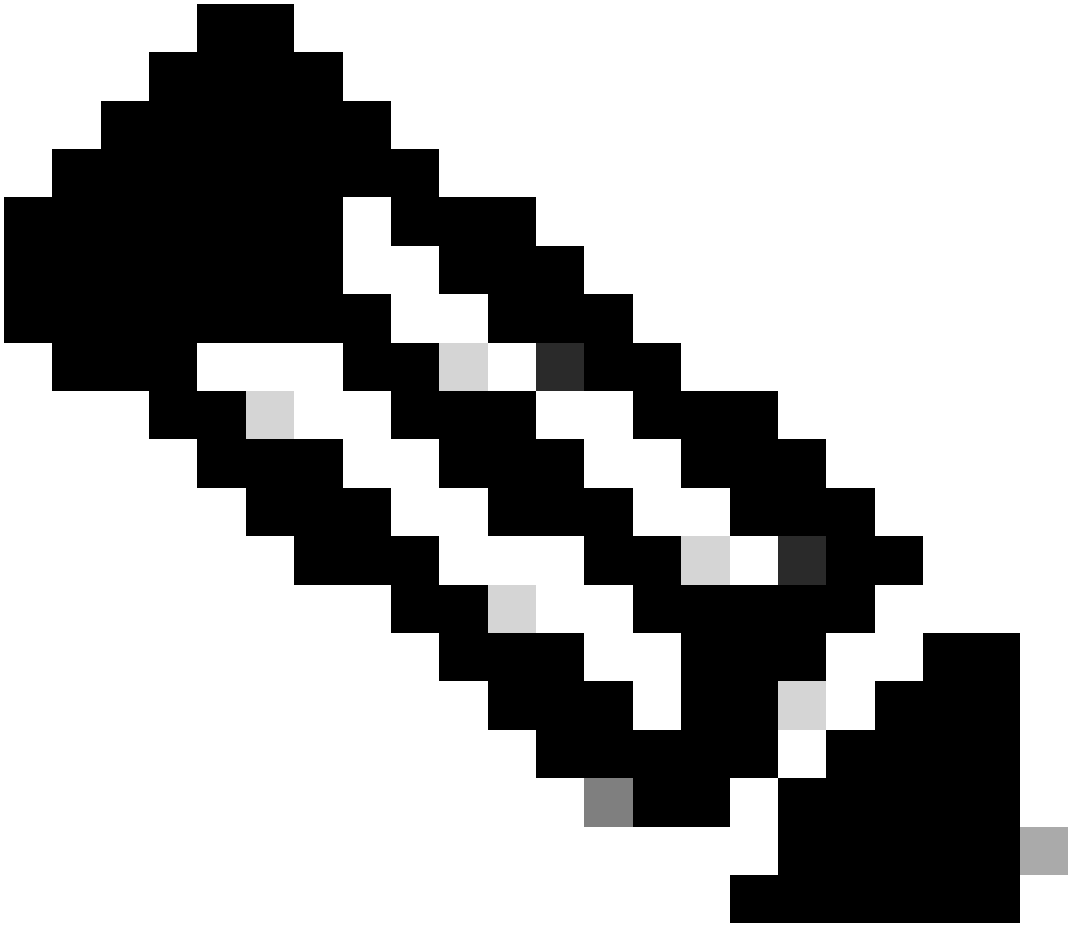
معالجة الاستبعادات

تسمح إستثناءات العملية للمسؤولين باستبعاد العمليات من المحركات المدعومة. يتم توضيح المحركات التي تدعم استبعادات العملية على كل منصة في الجدول التالي:

نظام تشغيل	محرك			
	فحص الملف	حماية عملية النظام	حماية الأنشطة الضارة	الحماية السلوكية
Windows	✓	✓	✓	✓
لينكس	✓	✗	✗	✓
ماك أو إس	✓	✗	✗	✓

MacOS و Linux

يجب عليك توفير مسار مطلق عند إنشاء إستثناء Process، كما يمكنك توفير مستخدم إختياري. إذا قمت بتحديد كل من المسار والمستخدم، فيجب استيفاء كلا الشرطين لاستبعاد العملية. إذا لم تقم بتحديد مستخدم، فسيتم تطبيق إستثناء العملية على كافة المستخدمين.



ملاحظة: في أنظمة التشغيل Linux و MacOS، تنطبق إستثناءات العملية على جميع المحركات.

معالجة أحرف البدل:

تدعم نقاط النهاية الآمنة Linux وموصلات MacOS إستخدام حرف بدل ضمن إستثناء العملية. وهذا يسمح بتغطية أوسع باستثناءات أقل، ولكنه قد يكون خطيرا أيضا إذا لم يتم تعريف الكثير جدا. يجب فقط إستخدام حرف البدل لتغطية الحد الأدنى لعدد الأحرف المطلوب لتوفير الاستثناء المطلوب.

إستخدام حرف البدل للعملية من أجل Linux و MacOS:

- يتم تمثيل أحرف البدل باستخدام حرف نجمي واحد (*)
- يمكن إستخدام أحرف البدل بدلا من حرف واحد أو دليل كامل.
- يعتبر وضع حرف البدل في بداية المسار غير صالح.
- تعمل أحرف البدل بين حرفين محددين، أو فواصل أو أبجدية رقمية.

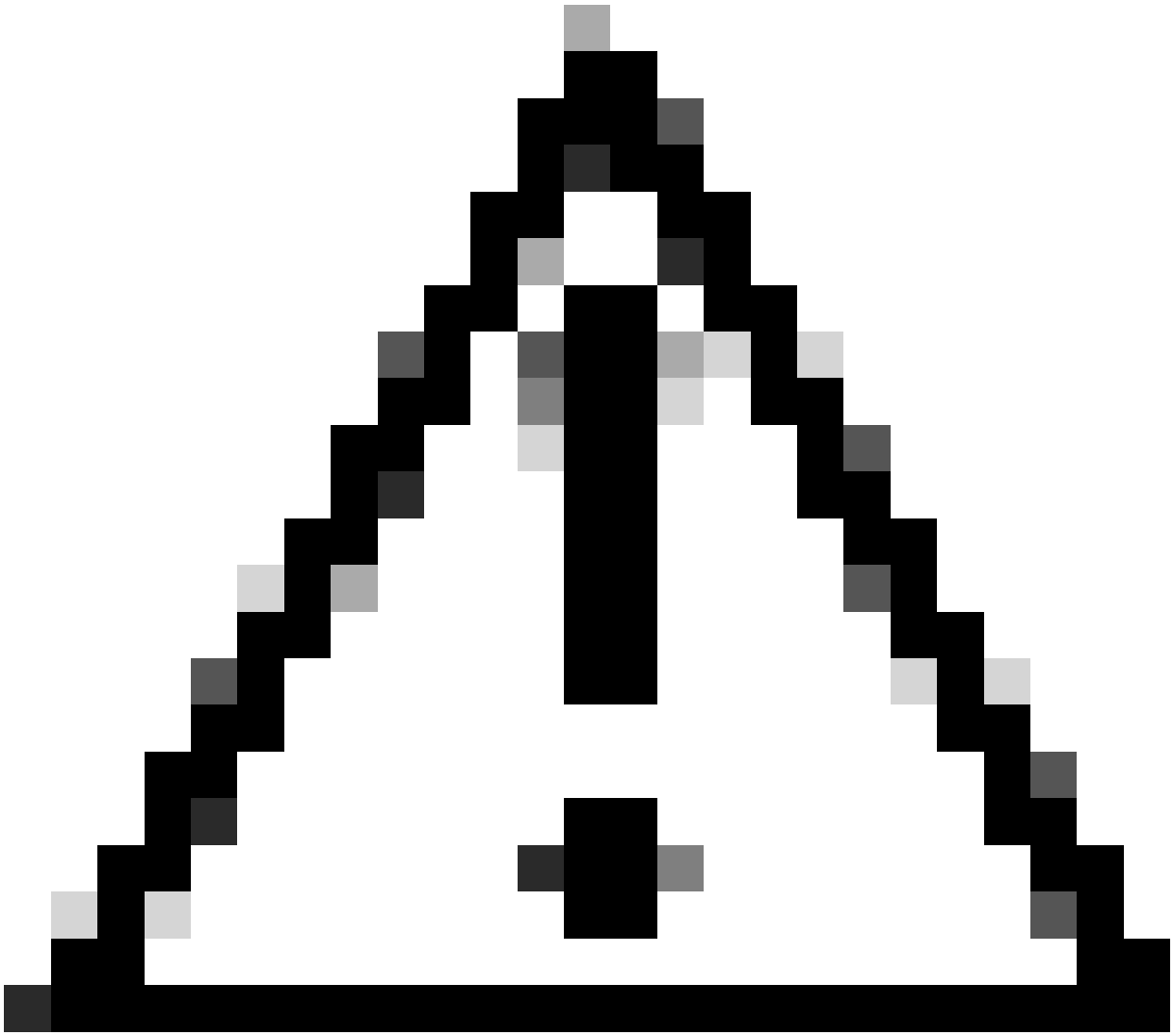
الأمثلة:

إستبعاد	النتيجة المتوقعة
`/Library/Java/JavaVirtualMachines/*/Java`	يستثني Java ضمن كل المجلدات الفرعية ل JavaVirtualMachine
`/المكتبة/Jibber/j*bber`	تستثني العملية ل Jabber وjibber وjobber، وما إلى ذلك

Windows

يمكنك توفير مسار مطلق و/أو SHA-256 للعمليات القابلة للتنفيذ عند إنشاء إستثناء العملية. إذا قمت بتحديد كل من المسار و SHA-256، فيجب استيفاء كلا الشرطين لاستبعاد العملية.

على Windows، يمكنك أيضا إستخدام CSIDL أو KNOWwFolderID ضمن المسار لإنشاء استبعادات العملية.

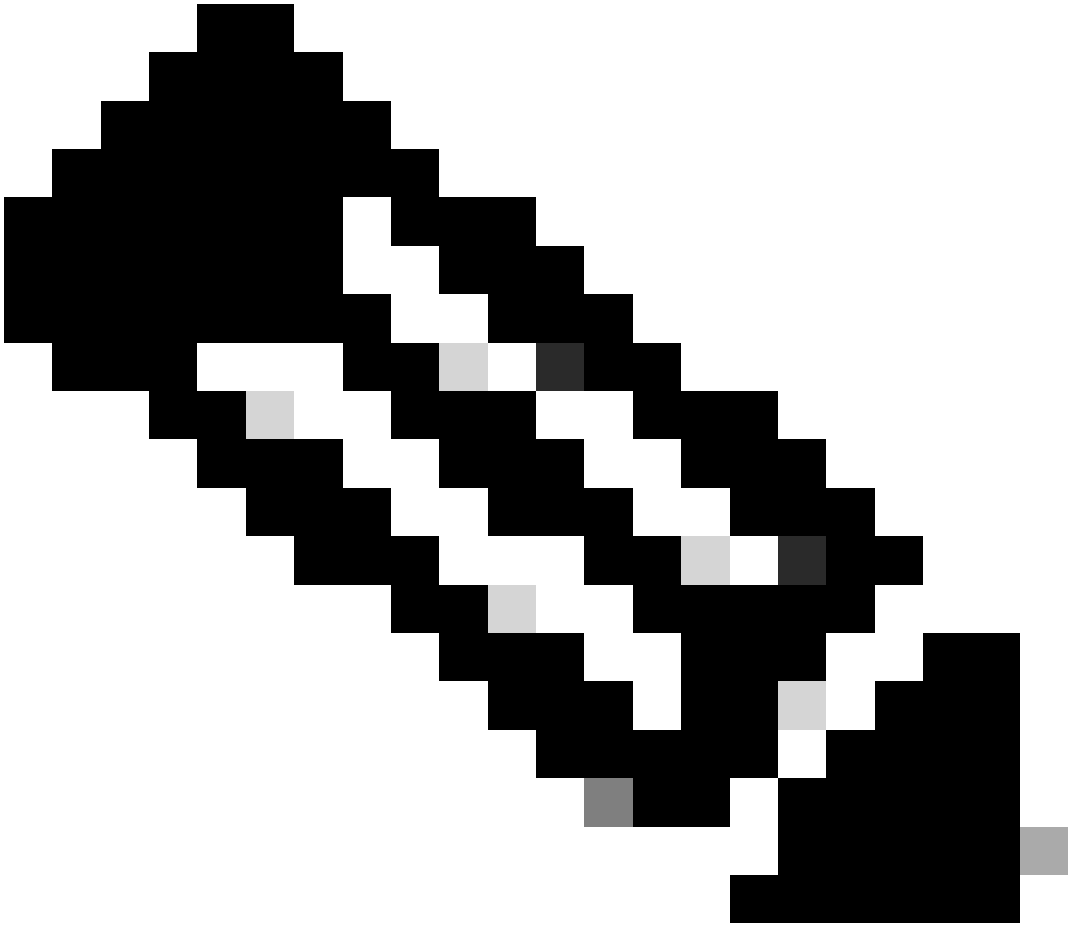


تحذير: لا يتم إستبعاد الإعداد الافتراضي للعمليات التابعة التي تم إنشاؤها بواسطة عملية مستبعدة. لاستبعاد عمليات إضافية عند إنشاء إستثناء عملية، حدد تطبيق على العملية التابعة.

القيود:

- إذا كان حجم ملف العملية أكبر من الحد الأقصى لحجم ملف المسح الضوئي المعين في النهج الخاص بك، فلن يتم حساب SHA-256 للعملية ولن يعمل الاستبعاد. أستخدم إستثناء عملية مبنية على المسار للملفات الأكبر من الحد الأقصى لحجم ملف المسح الضوئي.
- يفرض موصل Windows حد أقصى يبلغ 500 إستثناء عملية عبر كافة أنواع إستثناء العملية.
  - لا يتم إحترام إستثناءات العملية إلا إلى الحد الأقصى، بدءا من أعلى قائمة إستثناءات العملية في `policy.xml`.
  - يحتوي كل نهج Windows على إستثناء للعملية لـ `sfc.exe`، والذي يتم إحتسابه مقابل حد إستثناءات العملية:

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



ملاحظة: في Windows، يتم تطبيق إستثناءات العملية لكل محرك. إذا كان يجب تطبيق نفس الاستثناء على محركات متعددة، فيجب تكرار إستثناء العملية في

هذه الحالة لكل محرك قابل للتطبيق.

معالجة أحرف البدل:

دعم نقاط النهاية الآمنة لـ Windows Connectors باستخدام حرف بدل ضمن إستثناء العملية. وهذا يسمح بتغطية أوسع باستثناءات أقل، ولكنه قد يكون خطيرا أيضا إذا لم يتم تعريف الكثير جدا. يجب فقط إستخدام حرف البدل لتغطية الحد الأدنى لعدد الأحرف المطلوب لتوفير الاستثناء المطلوب.

إستخدام حرف البدل للعملية لـ Windows:

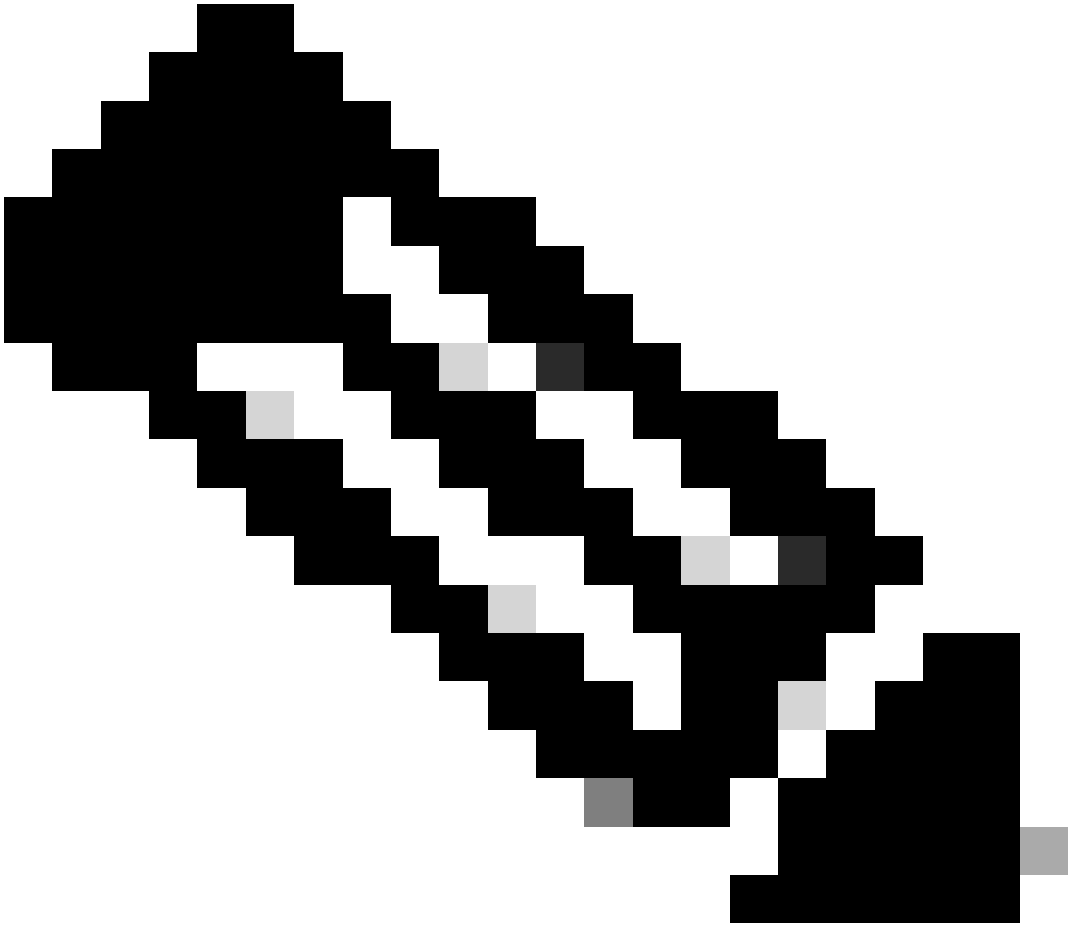
- يتم تمثيل أحرف البدل باستخدام حرف نجمي واحد (*) ونجمة مزدوجة (**)
- حرف بدل نجمة واحدة (*):
  - يمكن إستخدام أحرف البدل بدلا من حرف واحد أو دليل كامل.
  - يعتبر وضع حرف البدل في بداية المسار غير صالح.
  - تعمل أحرف البدل بين حرفين محددين، أو فواصل أو أبجدية رقمية.
  - يؤدي وضع حرف البدل في نهاية المسار إلى إستبعاد جميع العمليات في ذلك الدليل وليس الدلائل الفرعية.
- حرف بدل النجمة المزدوجة (**):
  - يمكن وضعها فقط في نهاية المسار.
  - يؤدي وضع حرف البدل في نهاية المسار إلى إستبعاد جميع العمليات في ذلك الدليل وجميع العمليات في الدلائل الفرعية.
  - يسمح ذلك بمجموعة إستثناء أكبر بكثير مع الحد الأدنى من المدخلات ولكن يترك أيضا ثغرة أمنية كبيرة جدا للرؤية. أستخدم هذه الميزة بحذر شديد.

الأمثلة:

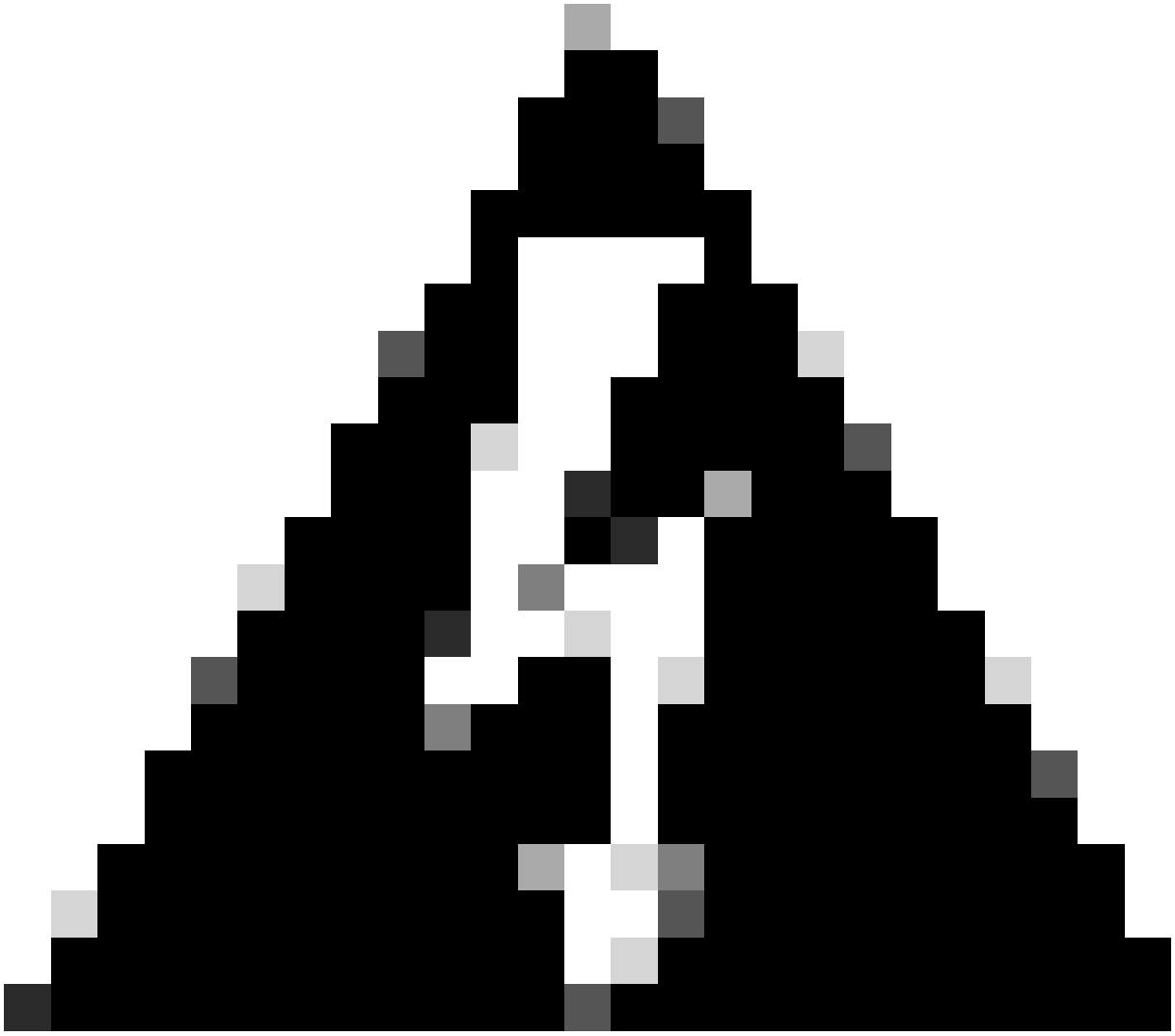
إستبعاد	النتيجة المتوقعة
`C:\Windows\*\Tiworker.exe`	يستثني كل عمليات `Tiworker.exe` الموجودة في الأدلة الفرعية لـ `Windows`
`C:\Windows\P*t.exe`	لا يشمل `Pot.exe` و`pat.exe` و`P1t.exe`، إلخ
`C:\Windows\*chickens.exe`	يستثني كافة العمليات في دليل `Windows` التي تنتهي بـ `chickens.exe`.
`C:\*`	يستثني كل العمليات في محرك الأقراص `C:` لكن ليس في المجلدات الفرعية
`C:\**`	يستثني كل عملية على محرك الأقراص `C:`

إستثناءات التهديد

تمكنك استبعادات التهديد من إستبعاد اسم تهديد معين من التسبب في وقوع الأحداث. يجب عليك إستخدام إستثناء التهديد في أي وقت فقط إذا كنت متأكدا من أن الأحداث هي نتيجة الاكتشاف الإيجابي الكاذب. في هذه الحالة، أستخدم اسم التهديد المحدد من الحدث على أنه إستثناء للتهديد الذي تمثله. كن على علم بأنه إذا كنت تستخدم هذا النوع من الاستثناء فإنه حتى الكشف الإيجابي الحقيقي لاسم التهديد لن يتم اكتشافه، أو وضعه في الحجر الصحي، أو إنشاء لحدث.



ملاحظة: تعتبر إستثناءات التهديد غير حساسة لحالة الأحرف.
مثال:W32.Zombies.NotAVviruses و32.zombies.notavirus كلاهما يطابق نفس اسم التهديد.



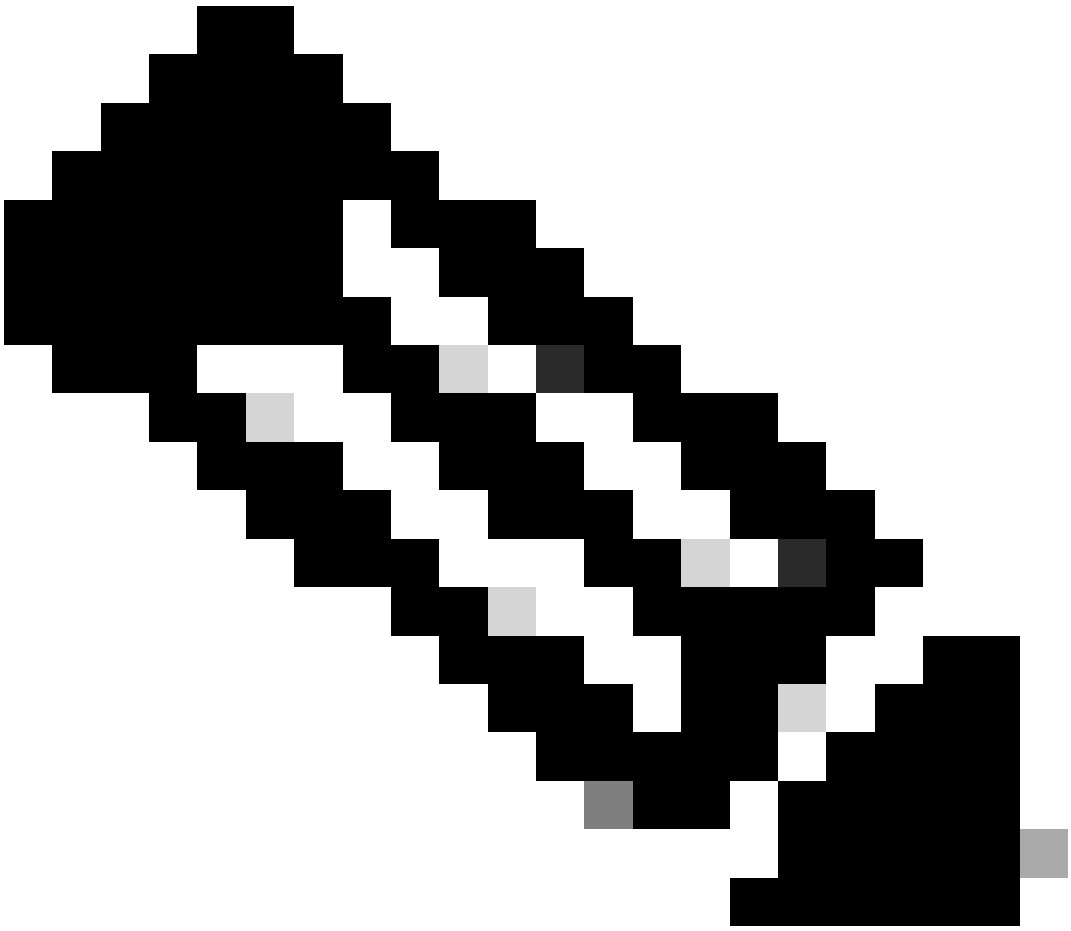
تحذير: لا تستبعدوا التهديدات إلا إذا أكد تحقيق شامل أن إسم التهديد إيجابي كاذب. لم تعد التهديدات المستبعدة تقوم بملء عالمة التبويب "الأحداث" للمراجعة والمراجعة.

إستثناءات المسار

استبعادات المسار هي الأكثر إستخدام، نظرا لأن تعارضات التطبيقات تتضمن عادة إستبعاد دليل. يمكنك إنشاء إستثناء مسار باستخدام مسار مطلق. على Windows، يمكنك أيضا إستخدام CSIDIL وأ KNOWwFolderId لإنشاء استبعادات للمسار.

على سبيل المثال، لاستبعاد تطبيق AV في دليل ملفات البرامج على Windows، يمكن أن يكون مسار الاستبعاد أي مما يلي:

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



ملاحظة: استبعادات المسار تكرارية وتستبعد كل الدلائل الفرعية أيضا.

تطابقات جزئية للمسار (في Windows فقط)

إذا لم يتم توفير شرطة مائلة في إستثناء المسار، يقوم موصل Windows بإجراء تطابق جزئي على المسارات. الا يدعم كل من Mac و Linux تطابقات جزئية للمسار.

على سبيل المثال، إذا قمت بتطبيق إستثناءات المسار التالية على Windows:

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

بعد ذلك سيتم إستبعاد كافة المسارات التالية:

```
C:\Program Files
C:\Program Files (x86)
C:\test
C:\test123
```

سيؤدي تغيير الاستثناء من "C:\test" إلى "C:\test\" إلى منع "C:\test123" من الاستبعاد.

استبعادات امتداد الملف

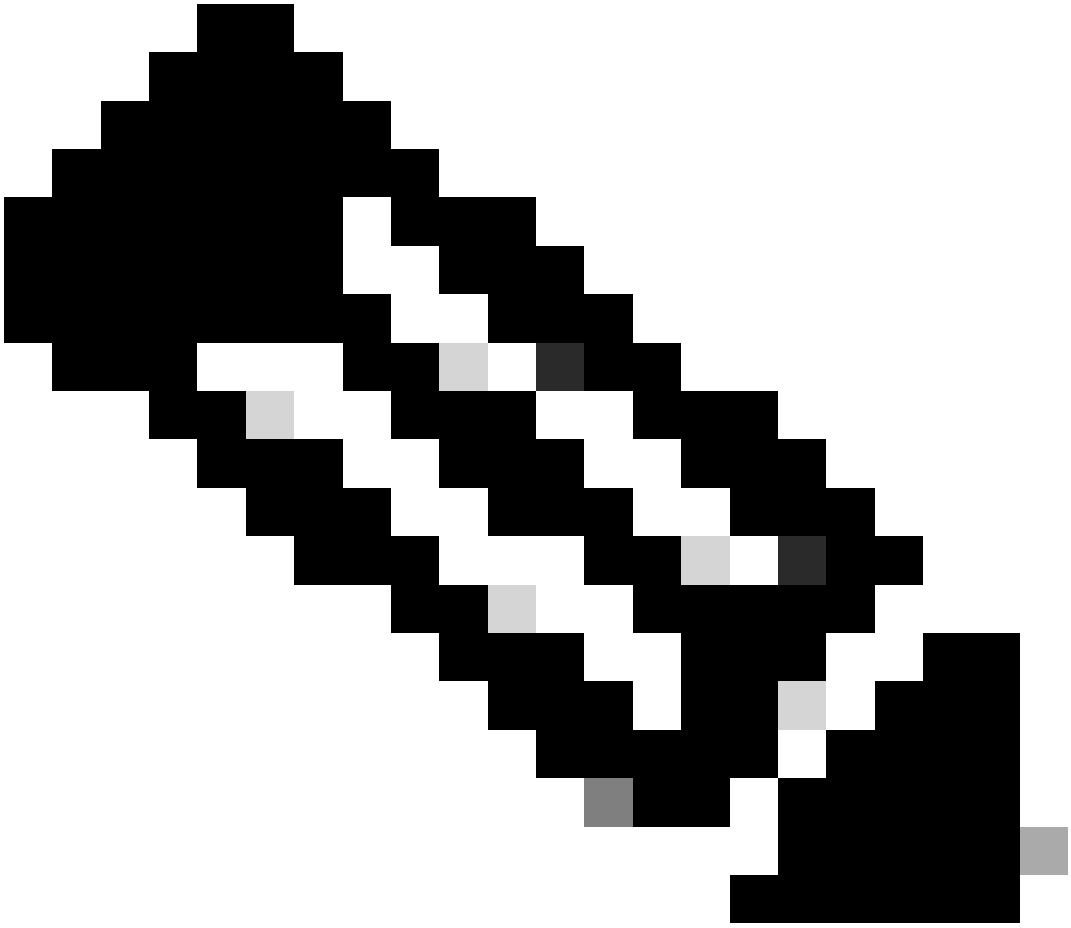
تسمح إستثناءات ملحق الملف باستبعاد كافة الملفات ذات الملحق المحدد.

النقاط الرئيسية:

- الإدخال الموقوع في وحدة تحكم نقطة النهاية الآمنة وه .extension
- تقوم "وحدة التحكم في النقطة الطرفية الآمنة" تلقائيا بتمديد فترة لملحق الملف إذا لم تتم إضافة أي شيء.
- الامتدادات غير حساسة لحالة الأحرف.

على سبيل المثال، لاستبعاد كافة ملفات قاعدة بيانات Microsoft Access، يمكنك إنشاء الاستثناء التالي:

.MDB



ملاحظة: تتوفر استبعادات امتداد الملف القياسية في القائمة الافتراضية، ولا يوصى بحذف هذه الاستبعادات، وقد يؤدي ذلك إلى تغييرات في الأداء على نقطة النهاية الخاصة بك.

إستثناءات Wildcard

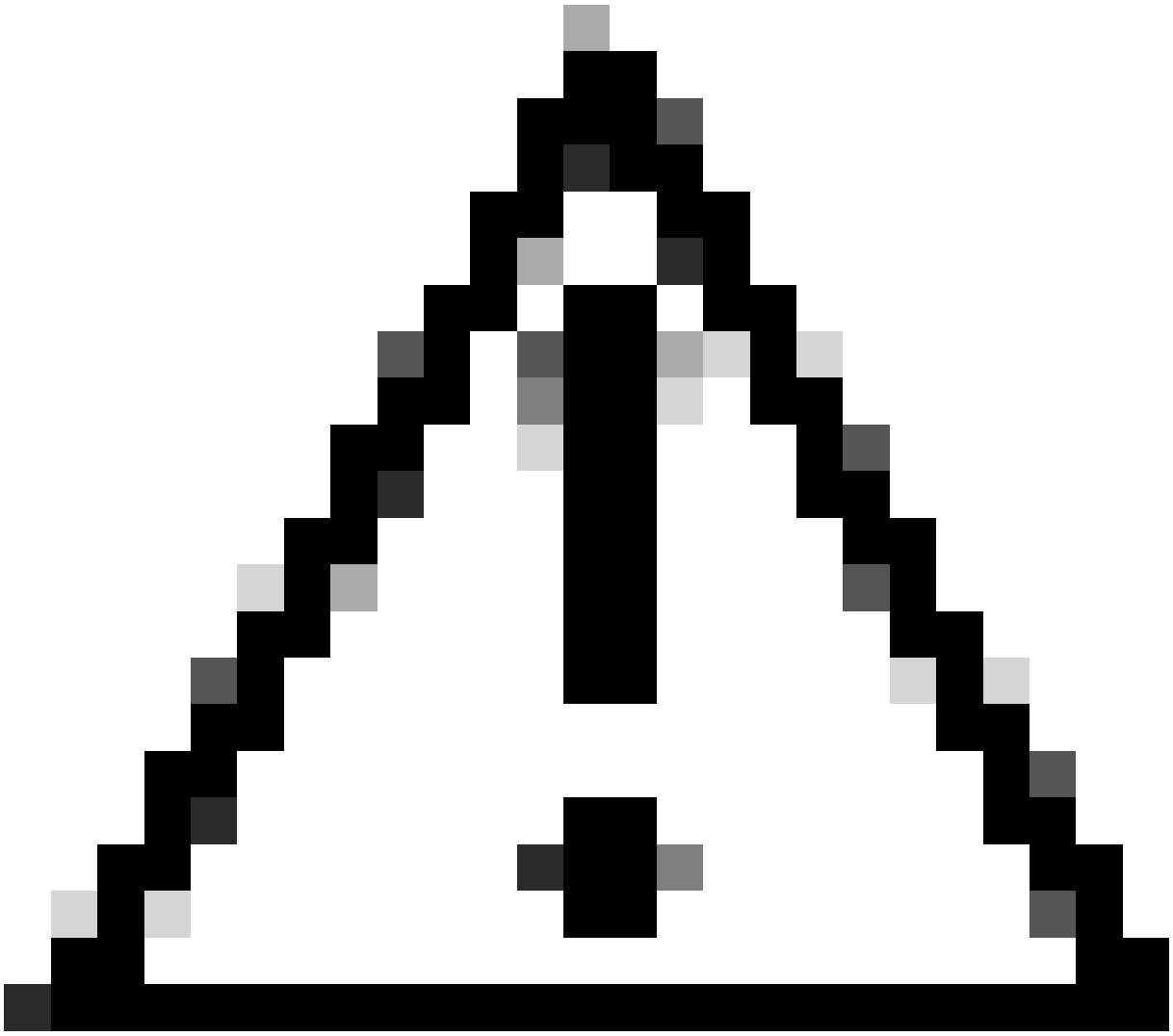
إستثناءات أحرف البدل هي نفسها إستثناءات المسار أو امتداد الملف باستثناء أنه يمكنك إستخدام حرف نجمي (*) لتمثيل حرف بدل داخل المسار أو الملحق.

على سبيل المثال، إذا كنت تريد إستبعاد الأجهزة الافتراضية على MacOS من أن يتم مسحها ضوئيا، فقد تقوم بإدخال إستثناء المسار:

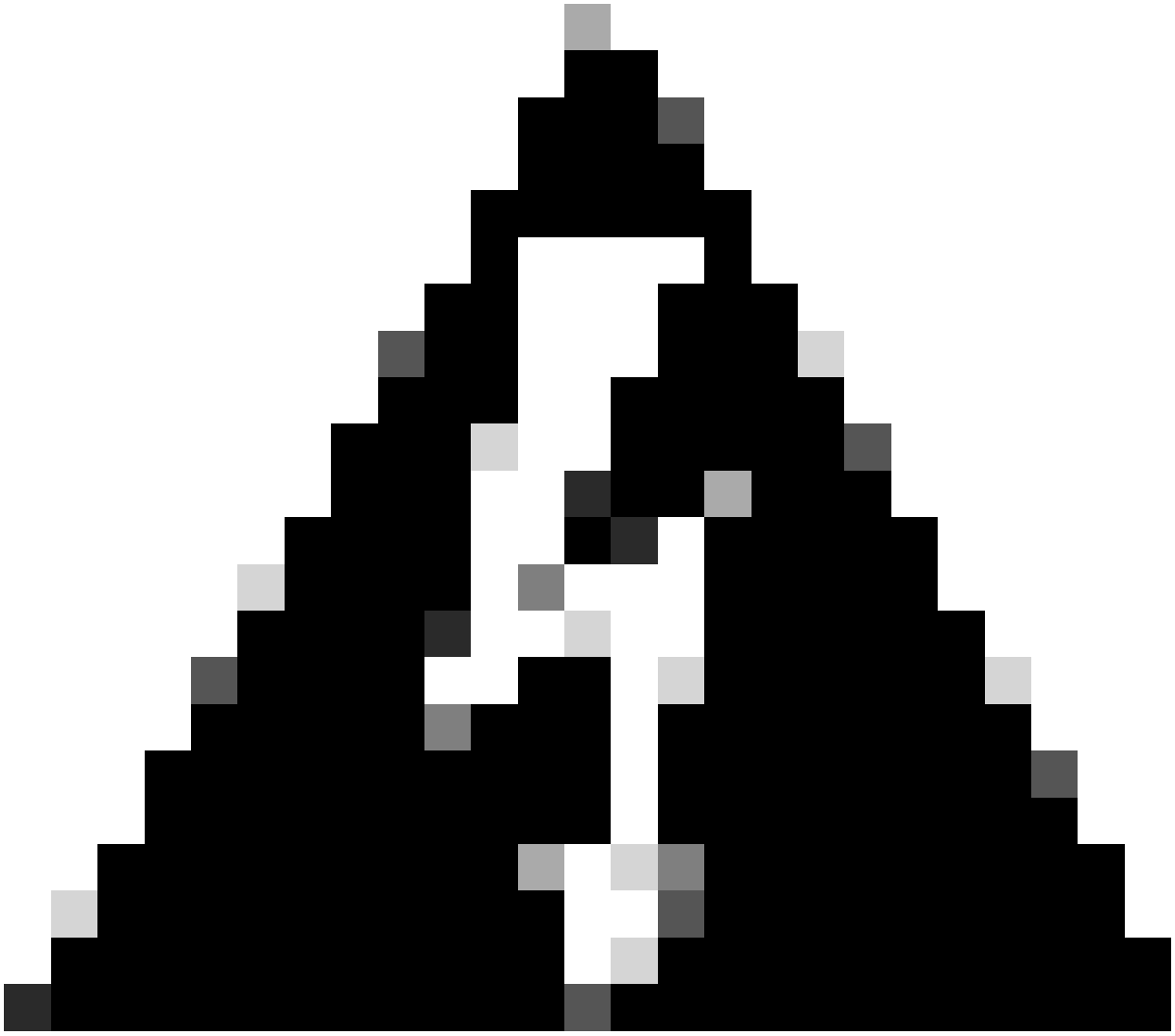
```
/Users/johndoe/Documents/Virtual Machines/
```

ومع ذلك، سيعمل هذا الاستبعاد فقط لمستخدم واحد، لذلك بدلاً من ذلك استبدل اسم المستخدم في المسار بنجمة وإنشاء إستثناء حرف بدل لاستبعاد هذا الدليل لجميع المستخدمين:

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



تحذير: لا تتوقف إستثناءات أحرف البدل عند فواصل المسار، قد يؤدي ذلك إلى إستثناءات غير مقصودة. على سبيل المثال `C:\*\test` يستثني `C:\sample\test` و `C:\sample\test123`. بالإضافة إلى `C:\1\test**` أ



تحذير: يمكن أن يؤدي بدء الاستباعاد بحرف نجمي إلى مشاكل كبيرة في الأداء. قم بإزالة جميع الاستثناءات التي تبدأ بحرف عالمة نجمية أو تغييرها لتقليل تأثير وحدة المعالجة المركزية (CPU).

Windows

عند إنشاء إستثناءات أحرف البدل على Windows، هناك خيار للتطبيق على كافة أحرف محرك الأقراص. تحديد هذا الخيار يطبق إستثناء حرف البدل على كل محركات الأقراص المحملة.

إذا كنت ستقوم بصنع نفس الاستباعاد يدويا ستحتاج إلى ترجيحه باستخدام ^[A-Za-z]، على سبيل المثال:

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

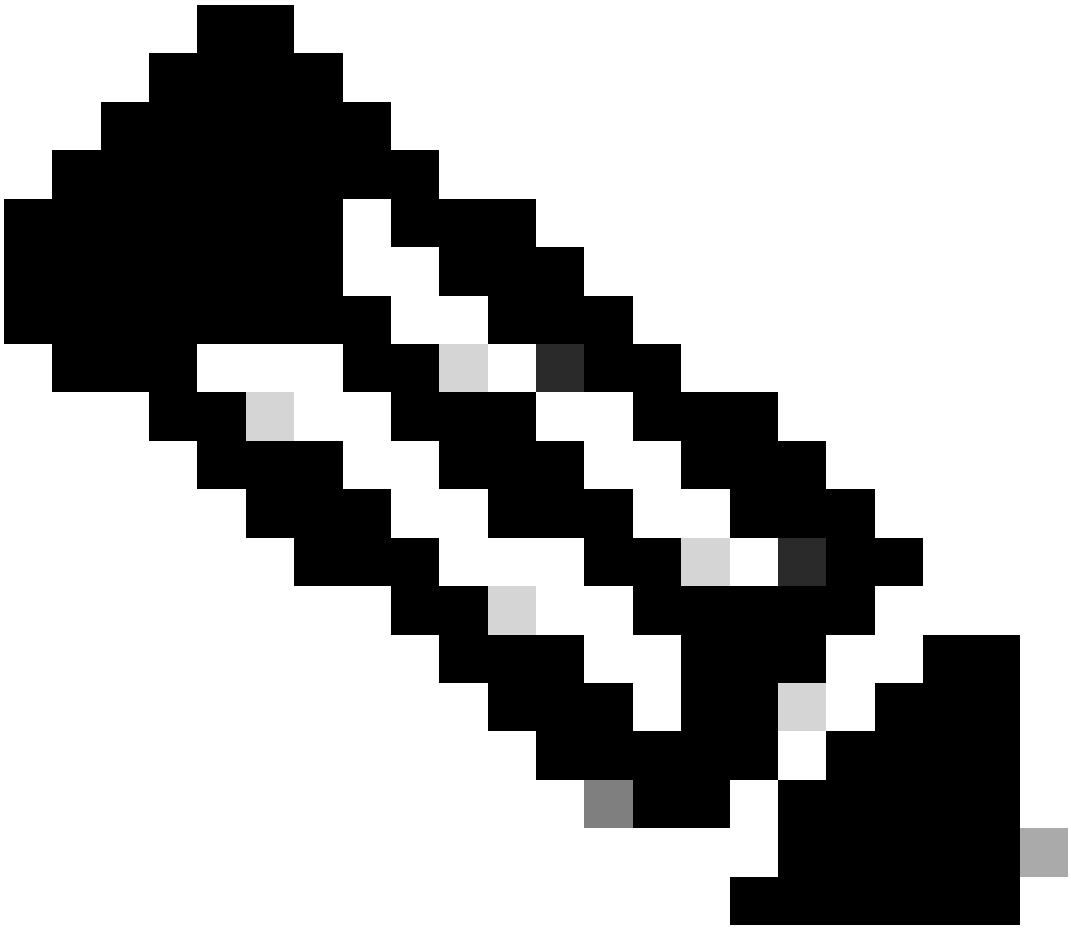
في كل الأمثلة، سيتم إستبعاد C:\testpath وD:\testpath.

تقوم وحدة التحكم في نقطة النهاية الآمنة تلقائيا بإنشاء ^[A-ZA-z] عند تحديد تطبيق على جميع أحرف الأقراص الاستثناءات أحرف البدل.

إستثناءات قابلة للتنفيذ (في Windows فقط)

تنطبق الاستثناءات القابلة للتنفيذ فقط على موصلات Windows مع تمكين منع الاستغلال. إستثناء قابل للتنفيذ يستبعد بعض الملفات التنفيذية من أن تكون محمية من خلال منع الاستغلال. يجب إستبعاد الملف التنفيذي من Exploit Prevention فقط إذا كنت تواجه مشاكل أو مشاكل في الأداء.

يمكنك التحقق من قائمة العمليات المحمية واستبعاد أي من الحماية بتحديد اسمها التنفيذي في حقل إستثناء التطبيق. يجب أن تتطابق الاستبعادات القابلة للتنفيذ مع اسم الملف التنفيذي تماما في اسم التنسيق.exe. أحرف البدل غير مدعومة.



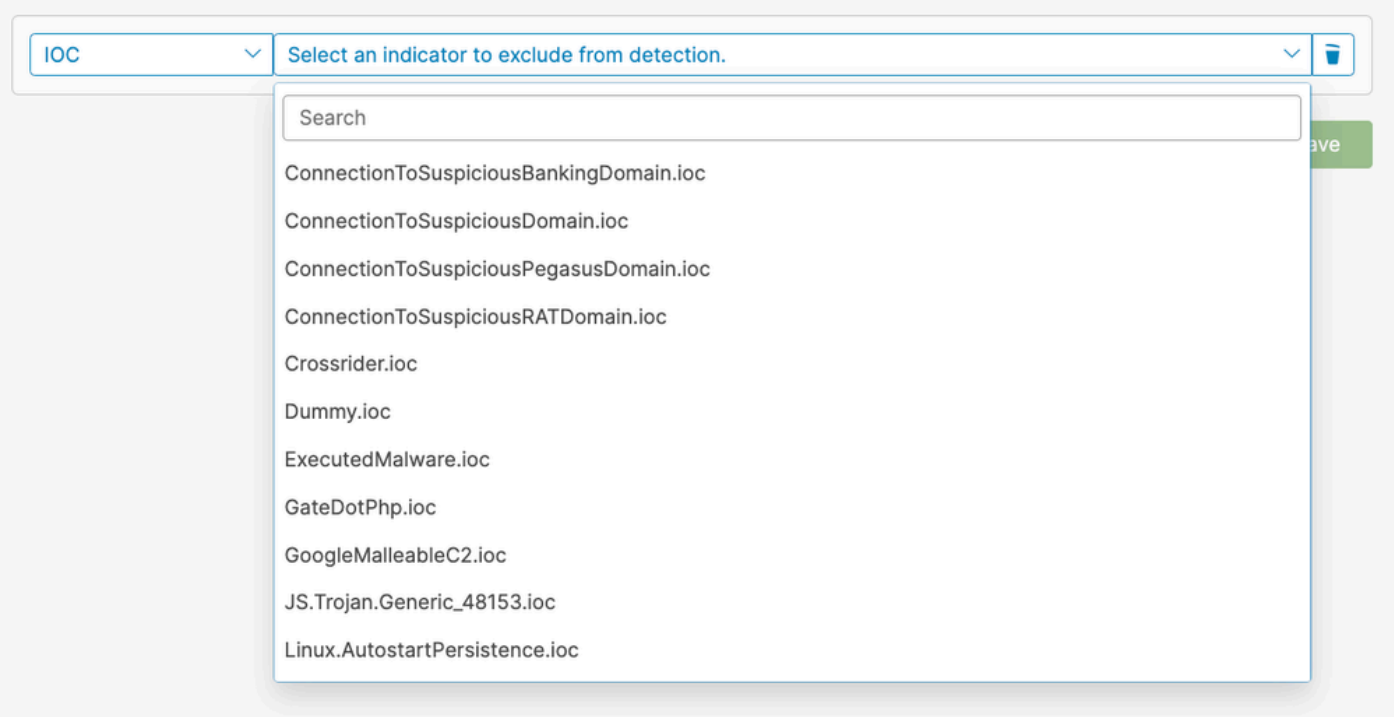
ملاحظة: يمكن إستبعاد التطبيقات فقط باستخدام إستثناءات قابلة للتنفيذ

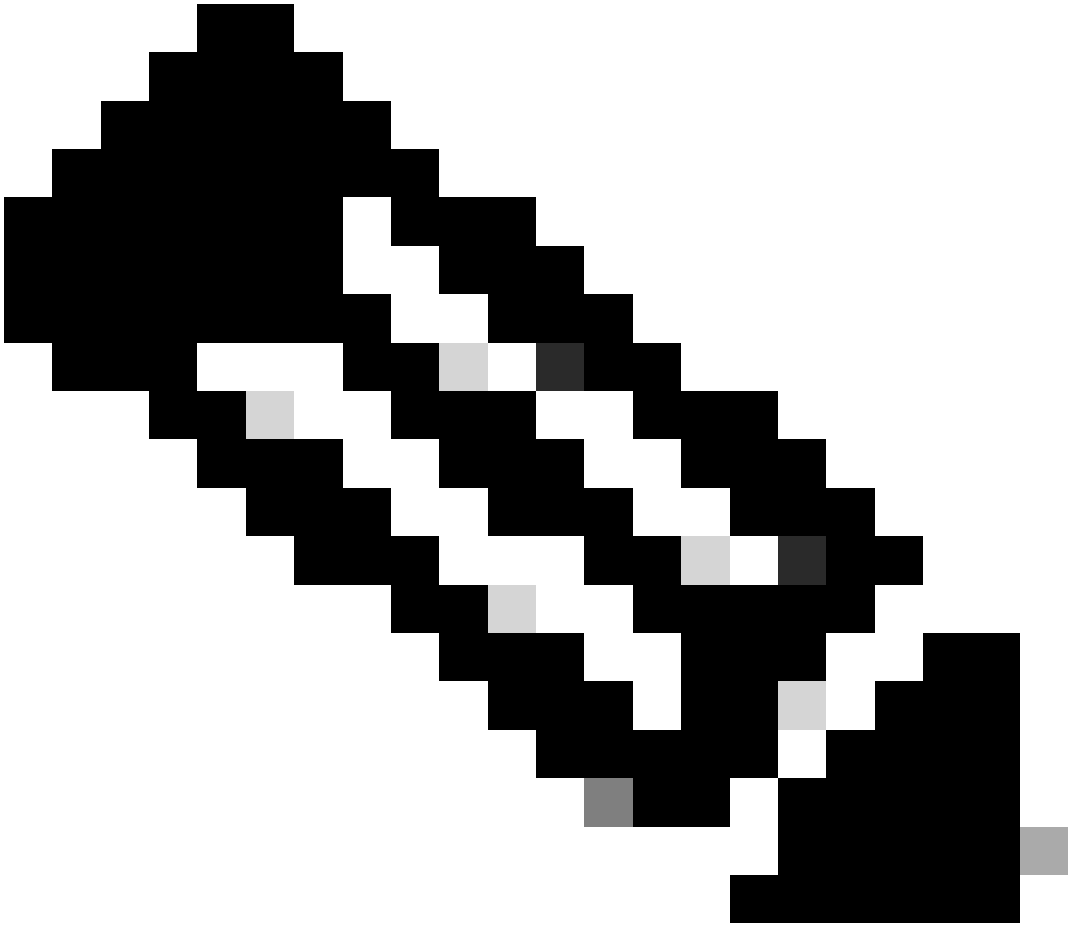
عبر وحدة تحكم نقطة النهاية الآمنة. تتطلب أي إستثناءات متعلقة بشبكات DLL فتح حالة دعم لإنشاء إستثناء.

يعتبر العثور على الاستثناءات الصحيحة لمنع الاستغلال عملية أكثر كثافة بكثير من أي نوع آخر من أنواع الاستباعد ويتطلب إختبارا مكثفا لتقليل أي ثغرات أمنية ضارة إلى الحد الأدنى.

استباعدات IOC (في Windows فقط)

تسمح لك استباعدات اللجنة الأوقيانوغرافية الحكومية الدولية باستباعد إشارات السحابة للتسوية. يمكن أن يكون هذا مفيدا إذا كان لديك تطبيق مخصص وأ داخلي قد ال يكون موقع ويتسبب في تشغيل بعض IOCs بشكل متكرر. توفر "وحدة التحكم في نقطة النهاية الآمنة" قائمة بالمؤشرات للاختيار من بين استثناءات IOC. يمكنك تحديد المؤشرات التي سيتم إستباعداها من خلال القائمة المنسدلة:





ملاحظة: إذا استبعدت اللجنة الأولمبية الدولية ذات الخطورة العالية أو الحرجة، ستفقد إمكانية الرؤية فيها وقد تترك مؤسستك في خطر. يجب إستبعاد هذه اللجنة الأولمبية الدولية فقط إذا واجهت عددا كبيرا من عمليات الكشف الإيجابي الكاذبة.

CSIDL و KNOWwFolderID (Windows فقط)

يتم قبول قيم CSIDL و KNOWwFolderID وتشجيعها عند كتابة إستثناءات المسار والمعالجة ل Windows. تكون قيم CSIDL/KNOWnfolderid مفيدة لإنشاء استبعادات للعملية والمسار للبيئات التي تستخدم أحرف محركات أقراص بديلة.

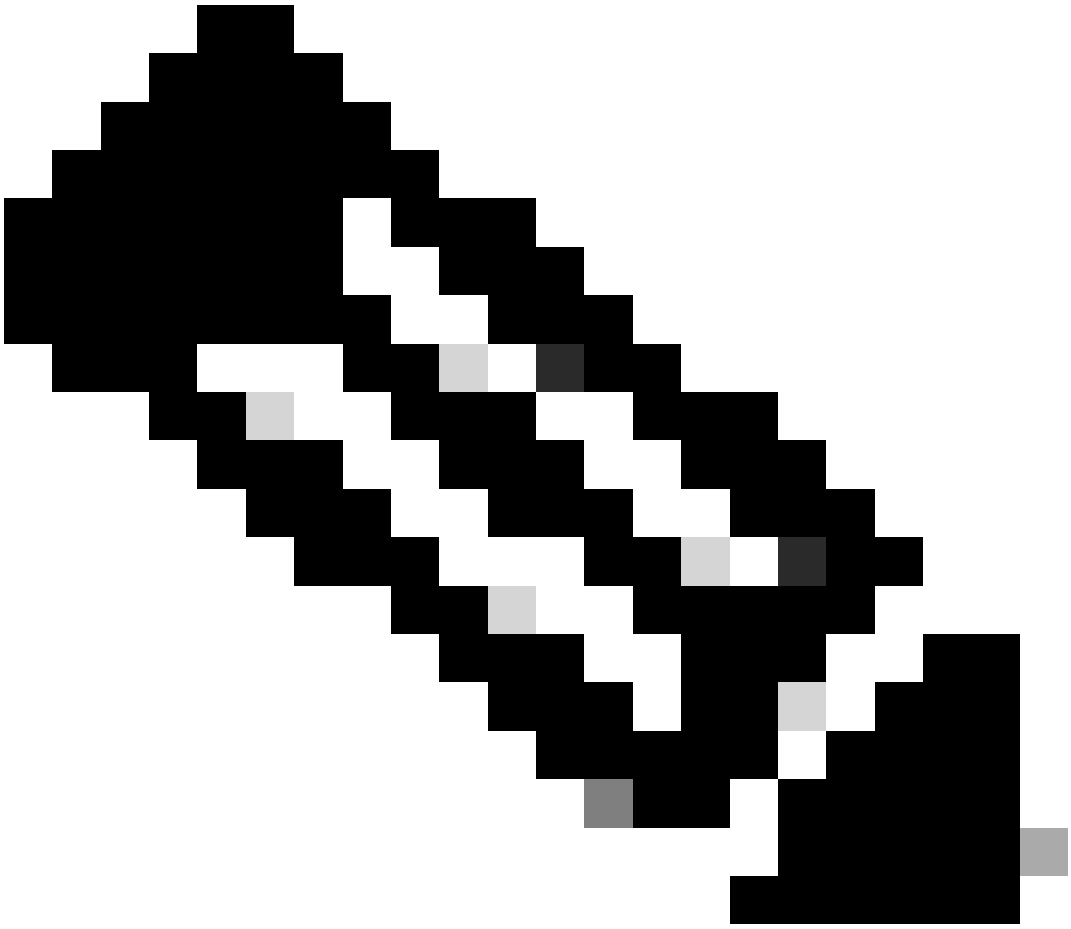
هناك قيود يجب مراعاتها عند إستخدام CSIDL/KNOWwFolderID. إذا قامت البيئة الخاصة بك بتثبيت البرامج على أكثر من حرف محرك أقراص، فإن قيمة CSIDL/KNOWNnfolderid تشير فقط إلى محرك الأقراص الذي تم وضع العلامة عليه كموقع التثبيت الافتراضي أو المعروف.

على سبيل المثال، إذا تم تثبيت نظام التشغيل على `C:\` ولكن تم تغيير مسار التثبيت ل Microsoft SQL يدويا إلى `D:\`، فإن الاستثناء المستند إلى

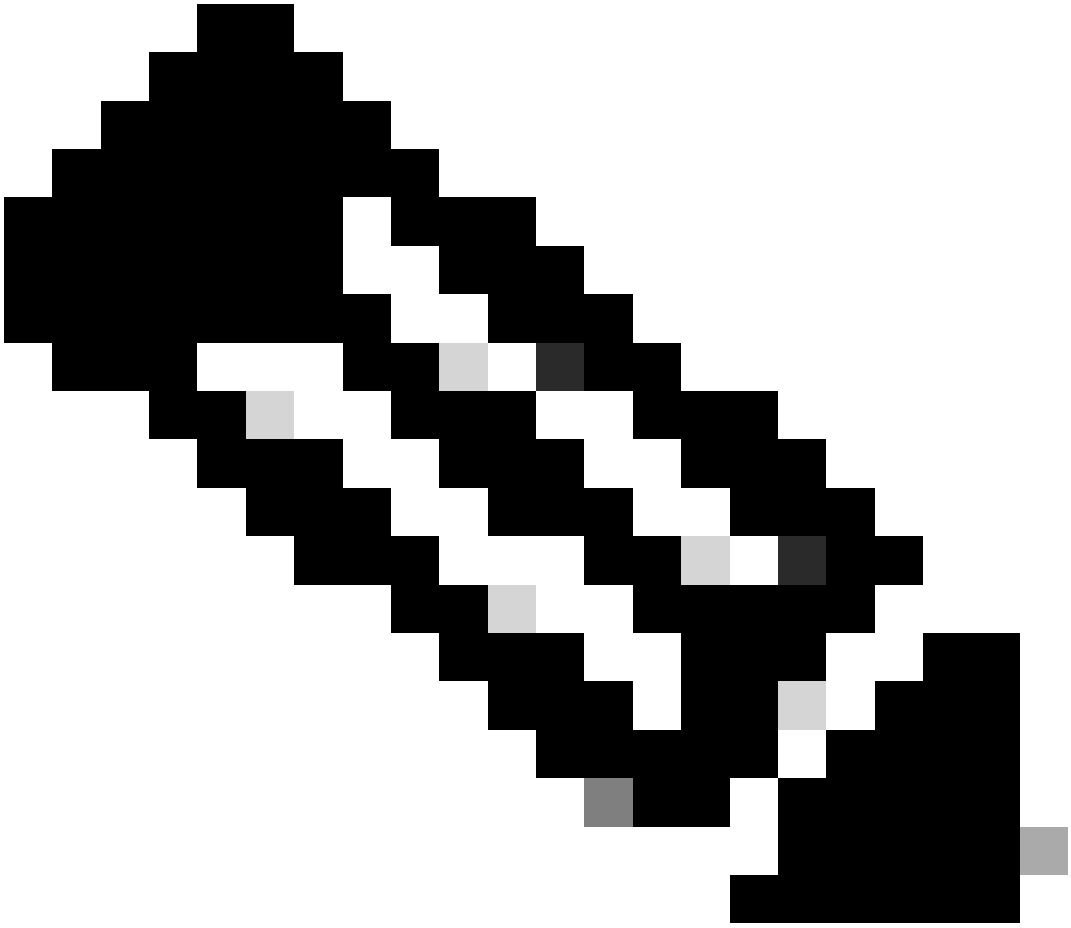
اذه قبطني على ال يتم الاحتفاظ بها في قائمة الاستبعاد التي تم الاحتفاظ بها في CSIDL/KNOWNwFolderID المسار. وهذا يعني أنه يجب إدخال إستثناء واحد لكل مسار أو إستثناء عملية غير موجود على محرك الأقراص C:\ حيث أن إستخدام CSIDL/KNOWwFolderID ال يرسمها.

راجع وثائق Windows التالية للحصول على مزيد من المعلومات:

- سيدل
- معرف معرف المجهر



ملاحظة: ال يتم دعم KNOWNnfolderid إلا في Windows Connector 8.1.7 والإصدارات اللاحقة. تستخدم الإصدارات السابقة من موصل Windows قيم CSIDL.



ملاحظة: تعد قيم KNOWNnfolderID حساسة لحالة الأحرف. على سبيل المثال، يجب إستخدام `valueFOLDERID_ProgramFiles` وليس `valueFolderID_ProgramFiles` غير الصحيح.

إعداد الموصل لمربع الاستباعاد

لإعداد الموصل الخاص بك لموالفة الاستباعاد، يجب:

1. إعداد نهج ومجموعة لتشغيلهما في وضع تصحيح الأخطاء.
2. قم بتشغيل أجهزة الكمبيوتر في مجموعة تصحيح الأخطاء الجديدة حسب عمليات العمل العادية، مما يتيح الوقت للحصول على بيانات كافية لسجل الموصلات.
3. قم بإنشاء بيانات تشخيصية على الموصل لاستخدامها في تحديد الاستثناءات.

ارجع إلى المستندات التالية للحصول على تعليمات حول تمكين وضع تصحيح الأخطاء وتجميع البيانات التشخيصية على أنظمة التشغيل المختلفة:

- Cisco Secure Endpoint Connector لجمع بيانات MAC التشخيصية
- Cisco Secure Endpoint Connector لتجميع البيانات التشخيصية ل Linux

- تحليل حزمة تشخيص AMP لوحدة المعالجة المركزية (Windows)

تحديد الاستبعادات

Linux و MacOS

توفر بيانات التشخيص التي تم إنشاؤها في وضع تصحيح الأخطاء ملفين مفيدين لإنشاء الاستثناءات: fileops.txt وexec.txt. يكون ملف fileops.txt مفيدًا لإنشاء إستثناءات المسار/الامتداد الملف/حرف البدل ويكون ملف execS.txt مفيدًا لإنشاء إستثناءات العملية.

إنشاء استبعادات العملية

يسرد الملف exs.txt المسارات القابلة للتنفيذ التي أدت إلى تشغيل نقطة النهاية الآمنة لإجراء فحص الملف. يحتوي كل مسار على عدد مرتبط يشير إلى عدد المرات التي تم مسحه فيها والقائمة التي تم فرزها بترتيب تنازلي. يمكنك إستخدام هذه القائمة لتحديد العمليات ذات الحجم الكبير لأحداث التنفيذ ثم إستخدام مسار العملية لصياغة الاستبعادات. غير أنه لا يوصى باستبعاد برامج المرافق العامة (مثل /usr/bin/grep) أو المترجمين الشفويين (مثل /usr/bin/ruby). إذا كان برنامج منفعة عامة أو مترجم شفوي يقوم بإنشاء حجم كبير من عمليات مسح الملفات، فيمكنك إجراء المزيد من التحقيقات لمحاولة صياغة استبعادات أكثر إستهدافا:

1. إستثناء العملية الأصلية: تحديد التطبيق الذي يقوم بتنفيذ العملية (على سبيل المثال، البحث عن العملية الأصلية التي تقوم بتنفيذ GREP) واستبعاد هذه العملية الأصلية. يجب تنفيذ هذا الإجراء، في حالة، وفقط في حالة، إمكانية تحويل العملية الأصلية بأمان إلى إستثناء للعملية. إذا كان الاستثناء الأصل ينطبق على العناصر التابعة، فسيتم إستبعاد الاستدعاءات لأي عناصر فرعية من العملية الأصلية أيضا.
2. إستبعاد العملية لمستخدم معين: تحديد المستخدم الذي يقوم بتنفيذ العملية. إذا تم تنفيذ العملية بواسطة مستخدم معين بكميات كبيرة، يمكنك إستبعاد العملية لذلك المستخدم المحدد فقط (على سبيل المثال، إذا تم إستدعاء عملية على مستوى كبير من قبل المستخدم "الجذر"، يمكنك إستبعاد العملية، ولكن فقط بالنسبة للمستخدم "الجذر" المحدد، فإن ذلك سيسمح لنقطة النهاية الآمنة بمراقبة عمليات تنفيذ عملية معينة من قبل أي مستخدم ليس "الجذر").

مثال إخراج exec.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
```

إنشاء استبعادات المسار وملحقات الملف وحرف البدل

يسرد الملف fileops.txt المسارات حيث يقوم الملف بإنشاء الأنشطة التي تم تشغيل نقطة النهاية الآمنة لها وتعديلها وإعادة تسميتها إجراء عمليات مسح الملفات. يحتوي كل مسار على عدد مرتبط يشير إلى عدد المرات التي تم مسحه فيها والقائمة التي تم فرزها بترتيب تنازلي. إحدى الطرق للبدء مع إستثناءات المسار هي العثور على مسارات الملفات والمجلد التي تم مسحها ضوئيا بشكل متكرر من fileops.txt ثم النظر في إنشاء قواعد لتلك المسارات. بينما لا يعني العدد المرتفع بالضرورة إستبعاد المسار (على سبيل المثال، الدليل الذي يخزن رسائل البريد الإلكتروني يمكن مسحه غالبا ولكن يجب عدم إستبعاده)، توفر القائمة نقطة بداية لتحديد المرشحين للاستبعاد.

مثال إخراج من 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
```

هناك قاعدة صحيحة للتجربة وهي أن أي شيء يحتوي على ملحق ملف سجل أو ملف دفتر يومية يجب اعتباره مرشح إستبعاد مناسب.

محرك الحماية السلوكية

تم إدخال محرك الحماية السلوكية في الإصدار 1.22.0 من موصل Linux والإصدار 1.24.0 من موصل MacOS، بدءا من هذه الإصدارات، يمكن للموصل اكتشاف نشاط النظام المرتفع بشكل كبير جدا مع رفع الخطأ 18.

يتم تطبيق استبعادات العملية على جميع المحركات والملفات الممسوحة. تطبيق

إستثناءات العملية على عمليات حميدة نشطة للغاية من أجل إصلاح هذا الخطأ. يمكن إستخدام الملف top.txt الذي تم إنشاؤه بواسطة بيانات تشخيص وضع التصحيح لتحديد العمليات الأكثر نشاطا على النظام. يرجى الرجوع إلى إرشادات خطأ موصل Mac/Linux لنقطة النهاية الآمنة 18 للحصول على خطوات الإصلاح التفصيلية.

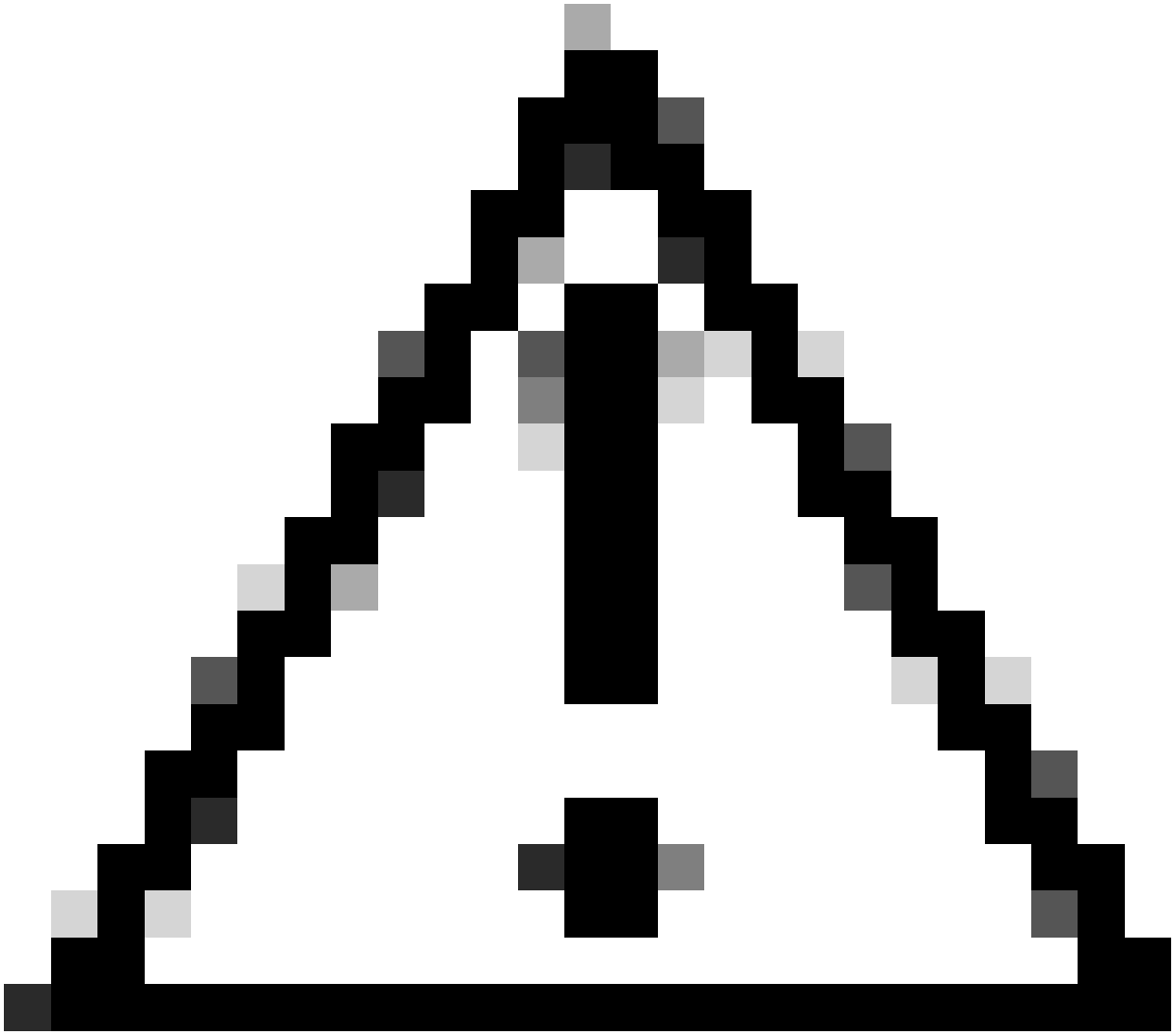
بالإضافة إلى ذلك، يمكن لاستثناءات العملية إسكات عمليات الكشف عن الحماية السلوكية الإيجابية الزائفة من البرامج الحميدة. بالنسبة لعمليات الكشف عن موجبة خاطئة في وحدة تحكم نقطة النهاية الآمنة، يمكن إستبعاد العملية لتحسين إعداد التقارير.

Windows

نظام تشغيل Windows أكثر تعقيدا، يتوفر المزيد من خيارات الاستبعاد بسبب العمليات الأصلية والتابعة. ويشير ذلك إلى أنه يلزم إجراء إستعراض أعمق لتحديد الملفات التي تم الوصول إليها، وكذلك البرامج التي تمخضت عنها.

الرجاء الرجوع إلى أداة ضبط Windows من هذه صفحة GitHub الخاصة بأمان Cisco للحصول على مزيد من التفاصيل حول كيفية تحليل أداء Windows وتحسينه باستخدام نقطة نهاية آمنة.

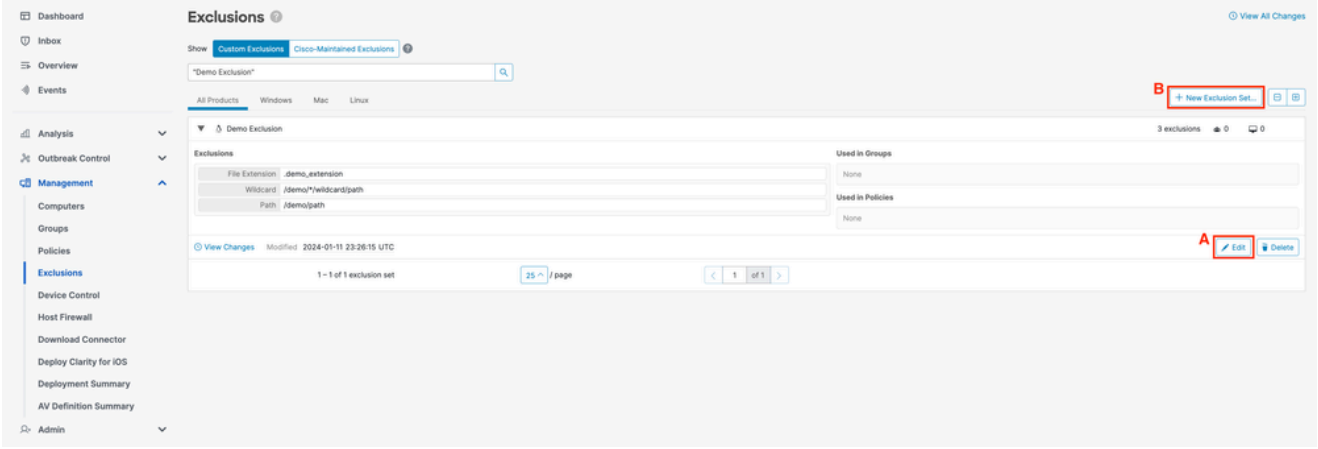
إنشاء قواعد إستثناء في وحدة تحكم نقطة النهاية الآمنة



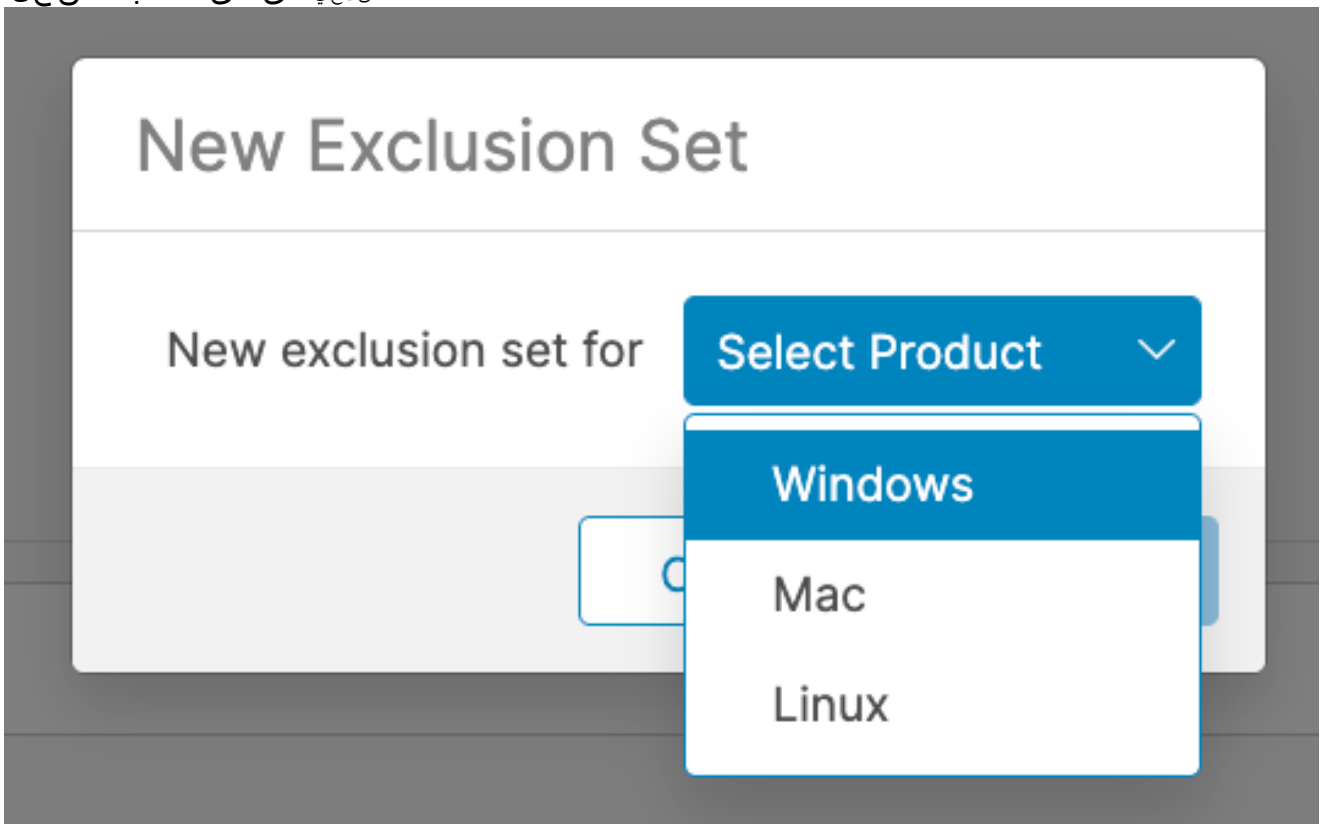
تحذير: فهم الملفات والعمليات دائما قبل كتابة إستثناء لتجنب نقاط ضعف الأمان على نقطة النهاية.

أكمل الخطوات التالية لإنشاء قاعدة إستثناء جديدة باستخدام وحدة تحكم نقطة النهاية الآمنة:

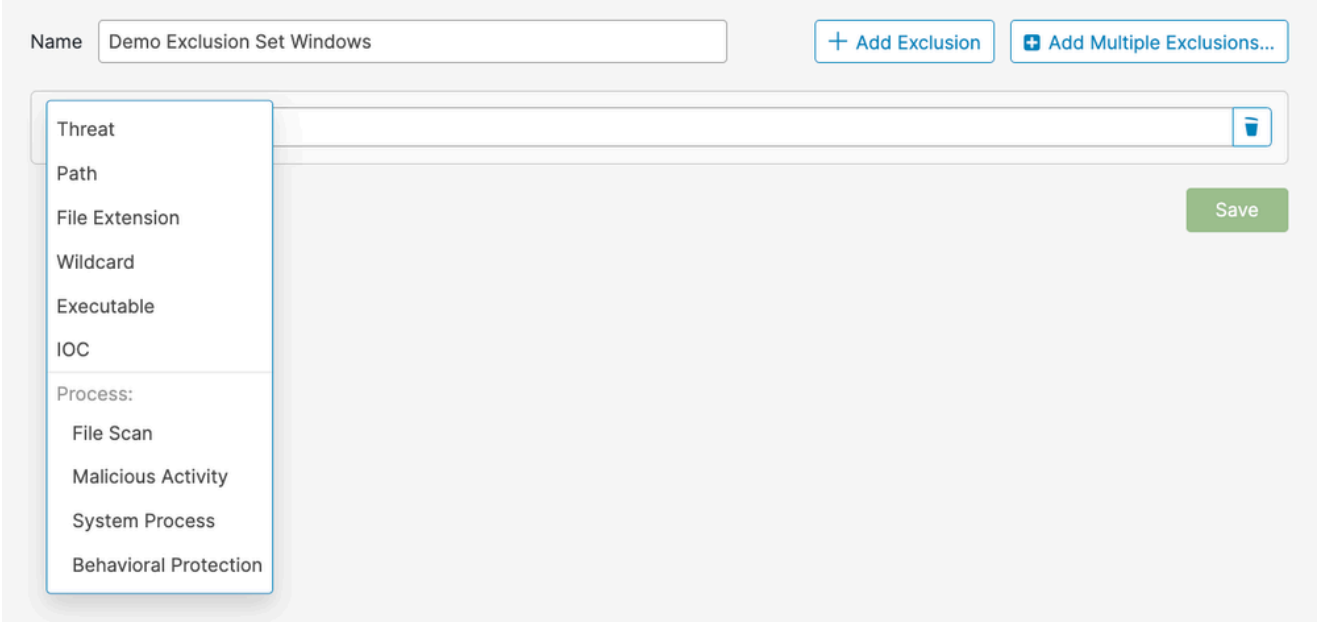
1. في "وحدة التحكم في نقطة النهاية الآمنة"، انتقل إلى صفحة "السياسات" من خلال تحديد Management -> الاستبعاد. إما (أ) حدد موقع مجموعة الاستثناء التي ترغب في تعديلها وانقر فوق تحرير، أو (ب) انقر + مجموعة إستبعاد جديدة....



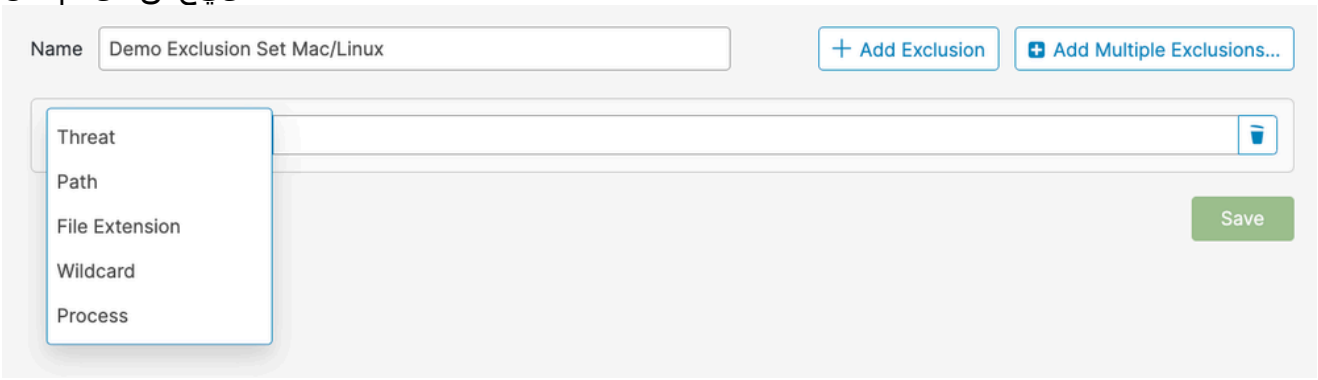
2. في منبثق مجموعة الاستثناء الجديدة، حدد نظام تشغيل لإنشاء مجموعة الاستثناء الخاصة به. طقطقة يخلق.



3. ستتم إعادة توجيهك إلى صفحة مجموعة إستثناء جديدة. انقر فوق + إضافة إستثناء وحدد نوع الاستثناء من القائمة المنسدلة تحديد نوع.
Windows:



نظام التشغيل Mac/Linux:



4. قم بتعبئة الحقول المطلوبة لنوع الاستثناء المحدد.
5. كرر الخطوات 2 و 3 لإضافة المزيد من القواعد، أو انقر حفظ لحفظ مجموعة الاستثناء.

أفضل الممارسات

توخ الحذر عند إنشاء الاستبعاد لأنها تقلل مستوى الحماية الذي توفره نقطة النهاية الآمنة من Cisco. لا يتم تجزئة الملفات المستبعدة أو مسحها ضوئيا أو توفرها في ذاكرة التخزين المؤقت أو السحابة، ولا يتم مراقبة النشاط، ولا تتوفر المعلومات من محركات الخلفية ومسار الهجاز والتحليل المتقدم.

يجب إستخدام الاستثناءات فقط في الحالات المستهدفة مثل مشاكل التوافق مع تطبيقات محددة أو مشاكل الأداء التي لا يمكن تحسينها بطريقة أخرى.

بعض أفضل الممارسات التي يجب اتباعها عند إنشاء الاستبعاد هي:

- إنشاء استبعادات فقط للمشكلات التي أثبتت جدواها
  - لا تفترض أن الإستبعاد ضروري إلا إذا ثبت أنه كان مشكلة لا يمكن علاجها بطريقة أخرى.
  - يجب التحقيق في مشاكل الأداء أو الجوانب الإيجابية الخاطئة أو مشاكل توافق التطبيقات بشكل شامل وتخفيفها قبل تطبيق الاستثناء.
- تفضيل إستثناءات العملية على إستثناءات امتداد المسار/الملف/حرف البدل
  - توفر استبعادات العملية طريقة أكثر مباشرة لاستبعاد أنشطة البرامج

الحميدة من إستخدام مجموعة من إستثناءات المسار وامتداد الملف وحرف البدل للحصول على نفس النتيجة.
    - يوصى باستبدال إستثناءات المسار والملحق الملحق والبدل التي تستهدف عمليات تنفيذ البرنامج مع إستثناءات العملية المقابلة عند الإمكان.
- تجنب الاستبعادات الواسعة
    - لا تستثني أجزاء كبيرة من نقطة النهاية، مثل محرك الأقراص C بأكمله.
    - أستخدم المسار المؤهل بالكامل للملف بدلا من اسم الملف فقط.
    - أستخدم مسار الجهاز، [وبيانات تشخيصات نقاط النهاية الآمنة](#)، [وأداة ضبط Windows](#) للتحقق من الاستثناءات المحددة وتحديدها.
- تجنب الإفراط في إستخدام إستثناءات أحرف البدل
    - كن حذرا عند إنشاء استبعادات باستخدام أحرف البدل. أستخدم استبعادات أكثر تحديدا عندما يكون ذلك ممكنا.
    - أستخدم الحد الأدنى لمقدار أحرف البدل في الاستبعاد؛ يجب أن تستخدم أحرف البدل فقط المجلدات التي تكون متغيرة بالفعل.
- تجنب إستبعاد برامج المرافق العامة والمترجمين الشفويين
    - والا يوصى باستبعاد برامج المرافق العامة أو المترجمين الشفويين.
    - إذا كنت بحاجة لاستبعاد برامج المرافق العامة أو المترجمين فعليك توفير مستخدم للعملية (MacOS/Linux فقط).
    - على سبيل المثال، تجنب كتابة الاستبعاد التي تتضمن Python، `Java`، `Ruby`، `bash`، sh، وما إلى ذلك.
- تجنب الاستبعادات المكررة
    - قبل إنشاء إستثناء، تحقق مما إذا كان الاستبعاد موجودا بالفعل في الاستبعادات المخصصة أو الاستبعادات التي تحتفظ بها Cisco.
    - تؤدي إزالة الاستثناءات المتكررة إلى تحسين الأداء وتقليل الإدارة التشغيلية للاستبعادات.
    - تأكد من أن المسار المحدد في إستثناء العملية غير مغطى بإستثناء المسار/ملحق الملف/حرف البدل.
- تجنب إستبعاد العمليات المعروفة بأنها شائعة الاستخدام في هجمات البرامج الضارة
    - انظر [الاستبعادات غير الموصى بها](#) للحصول على مزيد من التفاصيل.
- إزالة الاستبعادات القديمة
    - مراجعة قائمة الاستبعاد ومراجعتها بانتظام والاحتفاظ بسجل يوضح سبب إضافة بعض الاستثناءات.
- إزالة الاستبعادات عند التسوية
    - يجب إزالة الاستبعادات، يتم أختراق موصل من أجل إستعادة المستوى الأمثل من الأمان وإمكانية الرؤية.
    - يمكن إستخدام الإجراءات المؤتمتة لتطبيق سياسات أكثر أمانا على الموصلات بعد الإصابة. إذا تم أختراق موصل، فيجب نقله إلى مجموعة تحتوي على سياسة دون أي إستثناءات لضمان تطبيق أعلى مستوى من الحماية.
    - ارجع إلى [تحديد الظروف لتشغيل الإجراءات التلقائية في نقطة النهاية الآمنة](#) للحصول على مزيد من التفاصيل حول كيفية الإعداد الاستباقي للإجراء التلقائي "نقل الكمبيوتر إلى مجموعة عند التسوية".
- زيادة الحماية للأصناف المستبعدة
    - عندما تكون الاستبعادات ضرورية للغاية، تذكر التكتيكات التي يمكن إتخاذها للتخفيف من حدة المشكلة مثل تمكين حماية الكتابة لإضافة بعض طبقات الحماية للأصناف المستبعدة.
- إنشاء عمليات الاستبعاد بذكاء

- تحسين القواعد باختيار أعلى مستوى للعملية الأصلية التي تعرف التطبيق على العملية الفرعية لتقليل عدد تطبيقات الاستبعاد واستخدام خيار بشكل فردي إلى الحد الأدنى.
- عدم إستثناء عملية بدء التشغيل أبدا
  - تعتبر عملية بدء التشغيل (بدء التشغيل على نظام التشغيل MacOS وأ Init وأ System على نظام التشغيل Linux) مسؤولة عن بدء جميع العمليات الأخرى على النظام وهي على قمة التسلسل الهرمي للعملية.
  - سيؤدي إستبعاد عملية بدء التشغيل وكافة العمليات التابعة لها إلى تعطيل مراقبة نقطة النهاية الآمنة بشكل فعال.
- حدد مستخدم العملية عندما يكون ممكنا (MacOS/Linux فقط)
  - في حالة ترك حقل المستخدم فارغا، يتم تطبيق الاستبعاد على أي عملية تشغل البرنامج المحدد.
  - وفي حين أن الاستثناء الذي ينطبق على أي مستخدم يكون أكثر مرونة، فإن هذا النطاق الواسع يمكن أن يستبعد عن غير قصد النشاط الذي يجب رصده.
  - يعتبر تحديد المستخدم مهما بشكل خاص للقواعد التي تنطبق على البرامج المشتركة مثل محركات وقت التشغيل (على سبيل المثال، Java) ومترجمي البرامج النصية (على سبيل المثال، Bash وPython).
  - تحديد المستخدم يحد النطاق ويوجه نقطة النهاية الآمنة لتجاهل مثيلات معينة أثناء مراقبة المثيلات الأخرى.

الاستبعادات غير الموصى بها

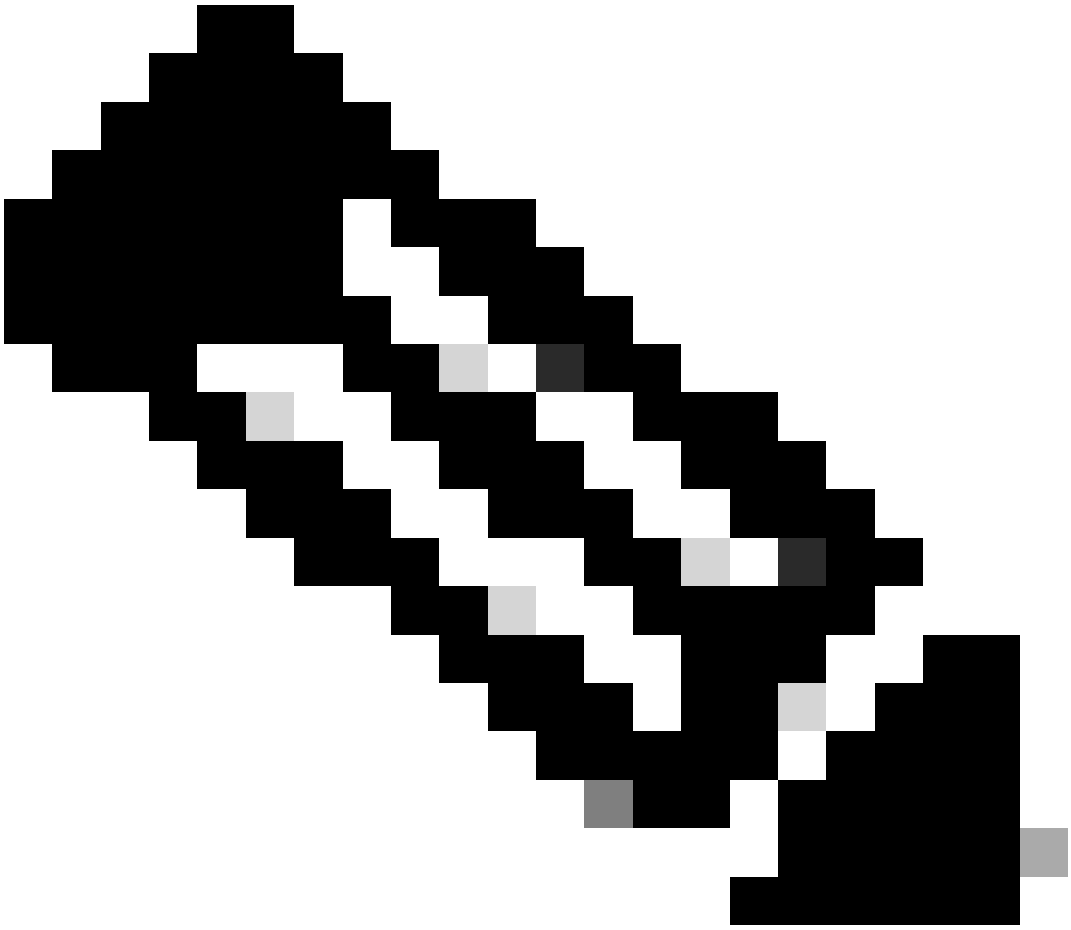
على الرغم من أنه من المستحيل معرفة أي متجه هجوم محتمل قد يستخدمه الخصم، إلا أن هناك بعض ناقل الهجوم الأساسية التي يجب مراقبتها. للحفاظ على وضعية أمان جيدة وإمكانية رؤية فائقة، لا يوصى بالاستثناءات التالية:

AcroRd32.exe
addinprocess.exe
addinprocess32.exe
addinutil.exe
base.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
chtasks.exe
system.management.automation.dll
windbg.exe
winword.exe
wmic.exe
wuauclt.exe
.7z
.bat
.bin
.CAB
.cmd
.com
.cpl
.dll
.exe
.fla
.gif
.gz
.hta
.inf
.Java
.ةرج
.ةفيظو
.jpeg
.jpg
.js
.وك
.ko.gz
.msi
.ocx

.png
.ps1
.يب
.rar
.reg
.scr
.sys
.tar
.tmp
.url
.vbe
.vbs
.wsf
.zip
شاب
Java
ناوثياب
ناوثياب 3
ش
شز
/
/bin
/sbin
/usr/lib
ج:
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 الملفات\<اسم الشركة>\
C:\Program ملفات (x86)\<اسم الشركة>\
C:\Users\<UserProfileName>\AppData\Local\Temp\
C:\Users\<UserProfileName>\AppData\LocalLow\Temp\



ملاحظة: هذه ليست قائمة شاملة للاستبعادات لتجنبها، ولكنها توفر رؤية متعمقة لمتجهات الهجمات الأساسية. يعد الحفاظ على إمكانية الرؤية في هذه المسارات وملحقات الملفات والعمليات أمرا بالغ الأهمية.

معلومات ذات صلة

- الدعم التقني والمستندات - Cisco Systems
- نقطة النهاية الآمنة من Cisco - TechNotes
- نقطة النهاية الآمنة من Cisco - دليل المستخدم
- أستكشاف أخطاء منع الاستغلال وإصلاحها في نقطة نهاية آمنة

- تحديد الشروط لتشغيل الإجراءات التلقائية في نقطة النهاية الآمنة

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).