Práticas recomendadas para exclusões seguras de endpoints

Contents

Introduction

Este documento descreve as melhores práticas para localizar e criar exclusões nos conectores de ponto de extremidade seguro.

Contribuído por Caly Hess, Mathew Huynh e Matthew Franks, engenheiros da Cisco.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Acesso ao portal Secure Endpoint

- Conta com privilégios de administrador
- Um conhecimento funcional do ambiente do cliente.

Componentes Utilizados

As informações neste documento são baseadas em sistemas operacionais Windows, Linux e 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Como entender exclusões

Um conjunto de exclusões é uma lista de diretórios, extensões de arquivos ou nomes de ameaças que você não deseja que o conector de endpoint seguro verifique ou condene. As exclusões são uma necessidade de garantir um equilíbrio entre desempenho e segurança em uma máquina quando a proteção de endpoint, como Secure Endpoint, está habilitada. Este artigo descreve exclusões para Secure Endpoint Cloud, TETRA, SPP e MAP.

Cada ambiente é único, bem como a entidade que o controla, variando de políticas rigorosas a políticas abertas, em que estas últimas seriam classificadas como um depósito de mel. Como essas exclusões são definidas, devem ser adaptadas exclusivamente a cada situação.

Diferentes exclusões podem ser classificadas de duas formas, **exclusões óbvias** e **exclusões indistintas**.

Exclusões óbvias

As exclusões óbvias são exclusões que foram criadas com base em pesquisas e testes para sistemas operacionais, programas e outros softwares de segurança comumente usados. Essas exclusões podem ser encontradas na Lista de exclusões mantidas pela Cisco em seu console.

> **Note**: É recomendável entrar em contato com outros fornecedores de antivírus (AV) e solicitar que suas exclusões recomendadas sejam adicionadas, garantindo que o conector de ponto de extremidade seguro e o AV funcionem em conjunto e também minimizem o impacto no desempenho.

Exclusões Indistintas

Érecomendável criar uma política duplicada para evitar preocupações e interrupções na segurança da empresa para identificar computadores com indicadores de problemas de desempenho e separá-los em um grupo para usar essa política duplicada.

Caution: As alterações de configuração no painel requerem tempo para permitir que os conectores sincronizem a política. Permita uma atualização de pulsação ou sincronize manualmente as políticas nos conectores.

Criação de políticas

1. **Console de endpoint seguro > guia Gerenciamento > Políticas**
2. Clique em **+ Nova política...**
3. **Selecione** no menu suspenso do sistema operacional.
4. Forneça um nome significativo para permitir que você diferencie essa política e descrição (*opcional*).
5. Selecione as ações de política de acordo com seus requisitos, use as exclusões padrão por enquanto.
6. ***Importante*** em **Configurações avançadas > Recursos administrativos,** defina o nível de log do conector como **Depurar**.
7. Clique em **Salvar** para concluir a criação da diretiva.

Criação de grupo

1. **Console de endpoint seguro > guia Gerenciamento > Grupos**
2. Clique em **Criar grupo**
3. Forneça um nome significativo para permitir que você diferencie esse grupo e a descrição (*opcional*).
4. **Selecione** a política duplicada que criou.
5. Clique em **Salvar** para concluir a criação do grupo.

Como identificar exclusões

Após a política duplicada e a criação de grupos, com o **nível de log de depuração nos conectores,** execute os *Computadores* de acordo com as operações comerciais normais. Reserve um tempo para obter dados suficientes do registro de conectores enquanto programas e processos foram acessados, gere um pacote de diagnóstico de suporte para revisar e identificar exclusões.

Guia para criar pacotes de diagnóstico para diferentes sistemas operacionais disponíveis:

- Windows
- Linux
- MAC

MacOS ou Linux

Extraia o pacote de diagnóstico de depuração compactado. O arquivo **fileops.txt** A lista os caminhos onde os arquivos criam, modificam e renomeam atividades acionadas pelo Secure Endpoint para executar verificações de arquivos. Cada caminho tem uma contagem associada que indica quantas vezes ele foi digitalizado e a lista é classificada em ordem decrescente. Embora uma contagem alta não signifique necessariamente que o caminho deve ser excluído (por exemplo, um diretório que armazena e-mails pode ser digitalizado com frequência, mas não deve ser excluído), a lista fornece um ponto de partida para identificar os candidatos à exclusão.

```
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_session_resourceLog.p
list
3 /Library/Logs/Cisco/supporttool.log
2 /private/var/db/locationd/clients.plist
2 /Users/eugene/Desktop/.DS_Store
2 /Users/eugene/.dropbox/instance1/config.dbx
2 /Users/eugene/.DS_Store
2 /Library/Catacomb/DD94912/biolockout.cat
2 /.fseventsd/000000000029d66b
1 /private/var/db/locationd/.dat.nosync0063.arg4tq
```

Windows

O sistema operacional Windows é mais complicado, mais opções de exclusão estão disponíveis devido aos processos pai e filho. Isso indica que é necessária uma revisão mais profunda para identificar os arquivos que foram acessados, mas também os programas que os geraram. Consulte esta Ferramenta de Ajuste do Windows na página GitHub da Cisco Security para obter mais detalhes sobre como analisar e otimizar o desempenho do Windows com Endpoint Seguro.

Como criar exclusões

Esta seção aborda as práticas recomendadas para criar exclusões para o seu ambiente.

> **Cuidado**: sempre entenda os arquivos e processos antes de gravar uma exclusão para evitar vulnerabilidades de segurança no computador.

> **Observação**: detalhes adicionais disponíveis no Guia do usuário, consulte o Capítulo 3 aqui. Este capítulo aborda os tipos de exclusões, implementação e navegação do portal Secure Endpoint.

Caminho e processo CSIDL

O CSIDL é uma forma aceita e incentivada de escrever exclusões. O CSIDL permite exclusões de processos que podem ser confirmadas em ambientes que usam letras de unidade alternativas e podem ignorar a necessidade de curinga quando esse caminho é específico do usuário (como exclusões de processos não permitem curinga). Mais informações sobre o CSIDL . Há limitações, no entanto, que precisam ser consideradas quando o CSIDL é usado. Se o ambiente instalar programas em mais de uma letra de unidade, o caminho CSIDL se refere somente à unidade marcada como o local de instalação padrão, por exemplo, se o SO estiver instalado em C:\ but the installation path for Microsoft SQL was manually changed to D:\, a exclusão baseada em CSIDL na lista de exclusão mantida não se aplica a esse caminho. Para exclusões de processos, isso significa que uma exclusão deve ser inserida para cada processo não localizado na pasta C:\ drive as the use of CSIDL does not map it.

Exclusões de caminho

Essas exclusões são as mais usadas, conflitos de aplicativos geralmente envolvem a exclusão de um diretório. Crie uma exclusão de caminho usando um caminho absoluto ou o CSIDL.

Por exemplo, para excluir um aplicativo antivírus no diretório Arquivos de programas, o caminho de exclusão seria:

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

Sem uma barra final, o **conector do Windows** faz uma correspondência parcial nos caminhos, enquanto **Mac e Linux não.**

Exemplo se você aplicar as seguintes exclusões de caminho"**C:\Program Files"** e como **"C:\test":**

C:\Program Files e **C:\Program Files (x86)** estão excluídos:

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

C:\test está excluído, como **C:\test123**:

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

Você pode alterar a exclusão de "**C:\test"** para "**C:\test\"**, isso impede que "**C:\test123"** seja excluído.

> **Observação**: as exclusões de caminho são recursivas e excluem todos os subdiretórios também.

Extensão de arquivo

Essas exclusões permitem a exclusão de todos os arquivos com uma certa extensão.

Pontos principais:

- A entrada esperada no lado do conector é **.extensão**
- O Painel prepara automaticamente um período para a extensão do arquivo se nenhum tiver sido adicionado.
- As extensões ***não*** diferenciam maiúsculas e minúsculas.

Por exemplo, para excluir todos os arquivos do banco de dados do Microsoft Access, você pode criar a seguinte exclusão:

```
.MDB
```

> **Observação**: as exclusões padrão estão disponíveis na lista padrão, **não** é recomendável excluir essas exclusões, pois isso pode causar alterações no desempenho em seus *computadores.*

Curinga

Essas exclusões são as mesmas que exclusões de caminho ou extensão, exceto o uso de um asterisco (*) como um caractere curinga.

> **Caution**: A exclusão de curinga não pára nos separadores de caminho, o que pode levar a exclusões não intencionais. Exemplo: **C:*\test exclui C:\sample\test e C:\1\2\3\4\5\6\test123.**

> **Aviso**: Começar uma exclusão com um asterisco(*) pode causar problemas maiores de desempenho e não é recomendado.

Por exemplo, exclua máquinas virtuais em um MAC de serem digitalizadas, insira esta exclusão de caminho:

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

Esta exclusão só funciona para *johndoe*, para permitir várias correspondências de usuário, substitua o nome de usuário no caminho por um asterisco(*) para uma exclusão curinga:

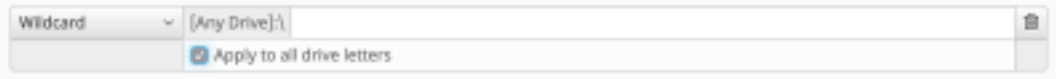
```
/Users/*/Documents/Virtual Machines/
```

Escreva uma exclusão para os caminhos que existem em unidades separadas.

Exemplo: **C:\testpath** e **D:\testpath** são:

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

O sistema gera automaticamente o ^[A-Za-z] quando a opção "Aplicar a todas as letras da unidade" é marcada na caixa após a seleção do curinga no menu suspenso Tipo de exclusão, conforme mostrado na imagem:



Processo

As exclusões de processos permitem que os administradores excluam os processos em execução de verificações de arquivos normais (Secure Endpoint Windows Connector versão 5.1.1 e posterior), System Process Protection (Connector versão 6.0.5 e posterior) ou Malicious Activity Protection (Connector versão 6.1.5 e posterior).

A exclusão do processo é feita por: especificando o caminho completo para o executável do processo, o valor SHA-256 do executável do processo ou o caminho e o SHA-256. Os caminhos permitem caminhos diretos ou usam um valor CSIDL.

> **Cuidado**: os processos filho criados por um processo excluído **não** são incluídos na exclusão por padrão. Exemplo: A exclusão do processo do MS Word não excluiria por padrão nenhum processo adicional criado pelo Word.exe e seria verificado. Para incluir processos adicionais, clique na caixa de seleção **Aplicar processos filho**. Além disso, excluir o Word.exe não é sugerido, pois o malware se oculta regularmente em arquivos .docx modernos.

> **Observação**: a especificação de Path e SHA-256 é necessária para que ambas as

condições sejam atendidas para excluir o processo.

Limitações:

- Se o tamanho do arquivo do processo for maior que o tamanho máximo do arquivo de verificação definido na sua política, o SHA-256 do processo não será calculado e a exclusão **não funcionará**. Usar uma exclusão de processo baseada em caminho para arquivos maiores que o tamanho máximo do arquivo de verificação
- Conector versões 5.x.x a 6.0.3 - um limite de 25 exclusões de processo em todos os tipos de exclusão de processo
- Conector versões 6.0.5+ - limite de 100 exclusões de processo em todos os tipos de exclusão de processo.
- Versões 7.x.+ do conector - limite de 500 exclusões de processos em todos os tipos de exclusão de processos.
- O conector apenas honra as exclusões do processo até o limite, na parte superior da lista de exclusões do processo em policy.xml
- Cada política tem uma exclusão de processo para sfc.exe, que conta contra o limite

Ameaça

Essas exclusões permitem que um nome de ameaça específico seja excluído do desencadeamento de eventos. A exclusão de ameaças deve ser usada somente quando o resultado da verificação acionar a detecção de falsos positivos e confirmar que não são uma ameaça real.

A caixa de texto para adicionar uma exclusão de ameaça ***não*** diferencia maiúsculas de minúsculas. Exemplo: W32.Zombies.NotAVirus ou w32.zombies.notavirus ambos correspondem ao mesmo nome de ameaça.

> **Aviso**: não exclua ameaças, a menos que a investigação e a confirmação do nome da ameaça sejam consideradas falsas positivas. As ameaças excluídas não são mais preenchidas na guia Eventos para revisão e auditoria.

Curinga do processo

Windows

O Connector 7.5.3+ permite exclusões adicionais usando a funcionalidade Curinga nas exclusões do processo. Isso permite uma cobertura mais ampla com menos exclusões, mas também pode ser perigoso se muito for deixado indefinido. **Você só deve usar o curinga para cobrir o número mínimo de caracteres necessários para fornecer a exclusão necessária.**

Uso do (*) curinga em processamento para Windows:

- (*) Pode ser usado no lugar de um único caractere ou de um diretório completo. Ele não pode ser colocado no início do caminho, ele será considerado inválido. O curinga funcionará entre dois caracteres definidos, barras ou alfanuméricos. Colocá-lo no final de um caminho

excluirá os processos desse diretório, mas não os subdiretórios.
- (**) Pode ser usado no final de um caminho para excluir todos os processos nesse diretório e os processos nos subdiretórios. Isso permite um conjunto de exclusões muito maior com entrada mínima, mas também deixa uma grande brecha de segurança para visibilidade. **Use este recurso com extremo cuidado**.

Examples:

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

MacOS e Linux

O Connector 1.15.2+ permite exclusões adicionais usando a funcionalidade Curinga nas exclusões do processo. Isso permite uma cobertura mais ampla com menos exclusões, mas também pode ser perigoso se muito for deixado indefinido. **Você só deve usar o curinga para cobrir o número mínimo de caracteres necessários para fornecer a exclusão necessária.**

Uso de (*) curinga em processamento para Mac:

- (*) Pode ser usado no lugar de um único caractere ou de um diretório completo. Ele não pode ser colocado no início do caminho, ele será considerado inválido. O curinga funcionará entre dois caracteres definidos, barras ou alfanuméricos.

Examples:

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

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems
- Endpoint seguro da Cisco - Notas técnicas
- Cisco Secure Endpoint - Guia do usuário
- Endpoint seguro: Exclusões de processos em MacOS e Linux