

Configurar e gerenciar exclusões no Cisco Secure Endpoint Connector

Contents

- [Introdução](#)
- [Pré-requisitos](#)
- [Requisitos](#)
- [Componentes Utilizados](#)
- [Fluxo de trabalho de endpoint seguro](#)
- [Exclusões Mantidas da Cisco](#)
- [Exclusões personalizadas](#)
- [Mecanismo de endpoint seguro](#)
- [Exclusão de Caminho](#)
- [Exclusão de Curinga](#)
- [Exclusão de Extensão de Arquivo](#)
- [Processo: Exclusão de Verificação de Arquivo](#)
- [Proteção de processos do sistema \(SPP\)](#)
- [Exclusão SPP](#)
- [Proteção contra atividades mal-intencionadas \(MAP\)](#)
- [Exclusão de MAP](#)
- [Prevenção de exploração \(Exprev\)](#)
- [Proteção comportamental \(BP\)](#)
- [Informações Relacionadas](#)

Introdução

Este documento descreve como criar a exclusão para os diferentes mecanismos no console do Cisco Secure Endpoint.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Modificar e aplicar uma lista de exclusão a uma política no console do Secure Endpoint
- convenção CSIDL do Windows

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Console Cisco Secure Endpoint 5.4.20211013
- Guia do usuário do Secure Endpoint revisão 15 de outubro de 2021

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer

comando.

Fluxo de trabalho de endpoint seguro

Em um alto nível de operações, o Cisco Secure Endpoint processa um arquivo Secure Hash Algorithm (SHA) nesta ordem através dos principais componentes do conector:

- Exclusões
- Mecanismo Tetra
- Controle de aplicativos (Lista de permissões/Lista de bloqueio)
- Mecanismo SHA
- Prevenção de exploração (Exprev) / Proteção contra atividades mal-intencionadas (MAP) / Proteção de processos do sistema / Mecanismo de rede (Correlação de fluxo de dispositivos)

Observação: a exclusão ou a criação de Permitir/Bloquear lista depende de qual mecanismo detectou o arquivo.

Exclusões Mantidas da Cisco

As Exclusões Mantidas pela Cisco são criadas e mantidas pela Cisco para fornecer melhor compatibilidade entre o Secure Endpoint Connector e o antivírus, e produtos de segurança ou outros softwares.

Esses conjuntos de exclusões contêm diferentes tipos de exclusões para garantir o funcionamento adequado.

Você pode acompanhar as alterações executadas nessas exclusões no artigo [Cisco-Mainheld Exclusion List Changes for Cisco Secure Endpoint Console](#).

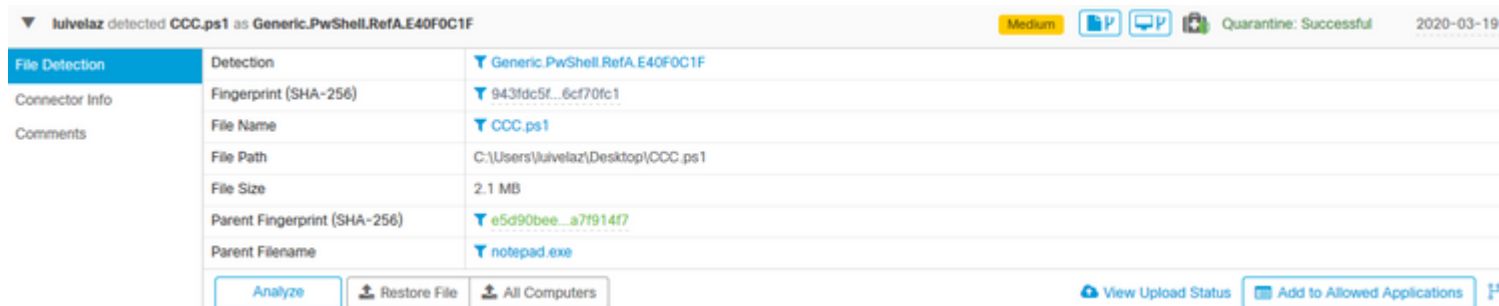
Exclusões personalizadas

Mecanismo de endpoint seguro

Verificação de arquivos (uso da CPU / detecções de arquivos) pelo mecanismo Tetra & SHA:

Use esses tipos de exclusões para evitar a detecção/quarentena de um arquivo ou para [mitigar a alta utilização da CPU do Secure Endpoint](#).

O evento no console do Secure Endpoint é como mostrado na imagem.



Observação: o CSIDL pode ser usado para exclusões. Consulte [este](#) documento da Microsoft para obter mais informações sobre o CSIDL.

Exclusão de Caminho

Path	C:\Users\luivelaz\Desktop\CCC.ps1
------	-----------------------------------

Exclusão de Curinga

Wildcard	C:\Users*\Desktop\CCC.ps1
	<input type="checkbox"/> Apply to all drive letters

Observação: a opção **Apply to all drive letters** é usada para aplicar também a exclusão a unidades [A-Z] conectadas ao sistema.

Exclusão de Extensão de Arquivo

File Extension	.ps1
----------------	------

Cuidado: use esse tipo de exclusão com cuidado, pois ele exclui todos os arquivos com a extensão de arquivo das varreduras, independentemente do local do caminho.

Processo: Exclusão de Verificação de Arquivo

Process	Path	C:\Path\to\executable.exe
File Scan	SHA	
	You can provide path and/or SHA-256. If you specify both a path and SHA-256 then both conditions must be met for the process to be excluded.	
	<input checked="" type="checkbox"/> Apply to child processes	

Proteção de processos do sistema (SPP)

O mecanismo System Process Protection está disponível no conector versão 6.0.5 e protege os próximos processos do Windows:

- Subsistema do Gerenciador de Sessões (smss.exe)
- Subsistema de Tempo de Execução Cliente/Servidor (csrss.exe)
- Subsistema de autoridade de segurança local (lsass.exe)
- Aplicativo de Logon do Windows (winlogon.exe)
- Aplicativo de Inicialização do Windows (wininit.exe)

Esta imagem mostra um evento SPP.

Event Details	Fingerprint (SHA-256)	aa52b2d3...acee8d21
Connector Info	File Name	lsass.exe
Comments	File Path	C:\Windows\System32\lsass.exe
	File Size	56.73 KB
	Reason	Process module is not clean and not signed
	Parent Fingerprint (SHA-256)	f3c7b460...fd3b16dd
	Parent Filename	TestAMPprotect.exe
	Parent File Size (bytes)	1608704
Analyze		

Exclusão SPP

Process	Path	Path\to\the\executable.exe
System Process	SHA	
	You can provide path and/or SHA-256. If you specify both a path and SHA-256 then both can be met for the process to be excluded.	
	<input checked="" type="checkbox"/> Apply to child processes	

Process	Path	
System Process	SHA	SHA-256 of the file (From the Parent Filename field)
	not a valid SHA-256	
	You can provide path and/or SHA-256. If you specify both a path and SHA-256 then both can be met for the process to be excluded.	
<input checked="" type="checkbox"/> Apply to child processes		

Proteção contra atividades mal-intencionadas (MAP)

Mecanismo de proteção contra atividades mal-intencionadas (MAP), defende seu endpoint contra um ataque de ransomware. Ele identifica ações ou processos mal-intencionados quando são executados e protege seus dados contra criptografia.

Um evento MAP é mostrado nesta imagem.

Malicious Activity Protection	Fingerprint (SHA-256)	9967155a...2956d820
Connector Info	Affected Files Count	5
Comments	Affected Files	C:\Users\umontero\Desktop\Test files\AMP4E-8120-SPP-MAP-EXPREV-test_files\Map\rewrite_data\1.txt.new C:\Users\umontero\Desktop\Test files\AMP4E-8120-SPP-MAP-EXPREV-test_files\Map\rewrite_data\0.txt.new C:\Users\umontero\Desktop\Test files\AMP4E-8120-SPP-MAP-EXPREV-test_files\Map\rewrite_data\4.txt.new C:\Users\umontero\Desktop\Test files\AMP4E-8120-SPP-MAP-EXPREV-test_files\Map\rewrite_data\2.txt.new C:\Users\umontero\Desktop\Test files\AMP4E-8120-SPP-MAP-EXPREV-test_files\Map\rewrite_data\3.txt.new
	File Name	rewrite.exe
	File Path	C:\Users\umontero\Desktop\Test files\AMP4E-8120-SPP-MAP-EXPREV-test_files\Map\rewrite.exe
	File Size	4.37 MB
	Parent Fingerprint (SHA-256)	9967155a...2956d820
	Parent Filename	rewrite.exe
	<div style="display: flex; gap: 10px;"> Analyze Restore File All Computers </div>	

Exclusão de MAP

Process	Path	Path\to\the\executable.exe
Malicious Activity	SHA	
	<p>You can provide path and/or SHA-256. If you specify both a path and SHA-256 then both conditions must be met for the process to be excluded.</p>	
	<input checked="" type="checkbox"/> Apply to child processes	

Cuidado: use esse tipo de exclusão com cuidado e depois de confirmar que a detecção realmente não é mal-intencionada.

Prevenção de exploração (Exprev)

O mecanismo de prevenção de exploração defende seus endpoints contra ataques de injeção de memória comumente usados por malware e outros ataques de dia zero em software sem patches vulnerabilidades. Ao detectar um ataque contra um processo protegido, ele será bloqueado e gerará um evento, mas não haverá uma quarentena.

Um evento Exprev é mostrado nesta imagem.

Testing.machine1.amp.com prevented an exploit in CUDL.LOS.exe process.

Exploit Prevention	Fingerprint (SHA-256)	ab6b87b8...3e70e087
Connector Details	Attacked Module	c:\program files (x86)\adobe\acrobat dc\acrobat\bib.dll
Comments	Application	CUDL.LOS.exe
	Base Address	0x7C700000
	File Name	CUDL.LOS.exe
	File Path	C:\Users\mabat\AppData\Local\Apps\2.0\E9781GXN.CJV\80XQ3X5B.94H\len
	File Size	5.82 MB
	Parent Fingerprint (SHA-256)	375a7501...e8624659
	Parent Filename	dfsvc.exe
	Parent File Size	24.27 KB
Analyze		

Exclusão de Expre

Executable	Name	CUDL.LOS.exe
Exploit Prevention	Provide an executable name to be excluded from protection by the Exploit Prevention (ValidExecutable.exe).	
<input type="button" value="+ Add Exclusion"/> <input type="button" value="+ Add Multiple Exclusions..."/>		

Cuidado: use esta exclusão sempre que confiar na atividade no módulo/aplicativo afetado.

Proteção comportamental (BP)

O mecanismo de proteção comportamental aprimora a capacidade de detectar e interromper ameaças de forma comportamental. Ela aumenta a capacidade de detectar ataques "vivendo fora da terra" e oferece resposta mais rápida às mudanças no cenário de ameaças por meio de atualizações de assinaturas.

Um evento BP é mostrado nesta imagem.

Testing.machine2.amp detected Scheduled Task Containing Suspicious Target Tactics Medium

Event Overview	Description		A suspicious scheduled task was created. This particular task stands out because it references a shortcut (.lnk) file. .lnk files can create one-time only tasks, recurring tasks, and tasks that run based on specific system events, such as system startup, to establish persistence.
Connector Details	Occured At		2022-10-20 17:07:40 UTC
Comments	MITRE ATT&CK	Tactics	TA0002: Execution TA0003: Persistence
		Techniques	T1053.005: Scheduled Task/Job: Scheduled Task
Observables			
		File: schtasks.exe	013c013e...b0ad28ef <input type="checkbox"/>

Exclusão BP

Process <input type="text"/>	Path	Path/to/the/executable/executable.exe
Behavioral Protection	SHA	
<p>You can provide path and/or SHA-256. If you specify both a path and SHA-256, both must be met for the process to be excluded.</p> <p><input type="checkbox"/> Apply to child processes</p>		

+ Add Exclusion
+ Add Multiple Exclusions...

Informações Relacionadas

- [Para obter mais informações sobre a configuração de diretivas, navegue até o Guia do usuário](#)
- [Vídeo Create Exclusions in Cisco Secure Endpoint Connector \(Criar exclusões no Cisco Secure Endpoint Connector\)](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.