

在Cisco Secure Endpoint Connector中配置和管理排除

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[安全終結點工作流](#)

[思科維護的排除項](#)

[自定義排除](#)

[安全終端引擎](#)

[路徑排除](#)

[萬用字元排除](#)

[副檔名排除](#)

[進程：檔案掃描排除](#)

[系統流程保護\(SPP\)](#)

[SPP排除](#)

[惡意活動保護\(MAP\)](#)

[MAP排除](#)

[防漏洞\(Exprev\)](#)

[行為保護\(BP\)](#)

[相關資訊](#)

簡介

本文檔介紹如何為思科安全終端控制檯上的不同引擎建立排除。

必要條件

需求

思科建議您瞭解以下主題：

- [修改排除清單並將其應用於安全終端控制檯中的策略](#)
- [Windows CSIDL慣例](#)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- [思科安全終端主控台5.4.20211013](#)


- 安全端點使用手冊修訂版2021年10月15日

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

安全終結點 workflow

在高級操作中，思科安全端點會透過連結器的主要元件，按以下順序處理檔案安全雜湊演算法 (SHA):

- 排除
- Tetra引擎
- 應用控制 (允許清單/阻止清單)
- SHA引擎
- 利用漏洞防護(ExpPrev)/惡意活動防護(MAP)/系統進程保護/網路引擎 (裝置流關聯)

 注意：排除或允許/阻止清單建立取決於哪個引擎檢測到檔案。

思科維護的排除項

思科維護的例外項由思科建立並維護，以便在安全終端連結器與防病毒、安全產品或其他軟體之間提供更好的相容性。

這些排除集包含不同型別的排除以確保正確操作。

您可以在[思科維護的思科安全端點控制檯的排除清單更改](#)文章中跟蹤對這些排除項執行的更改。

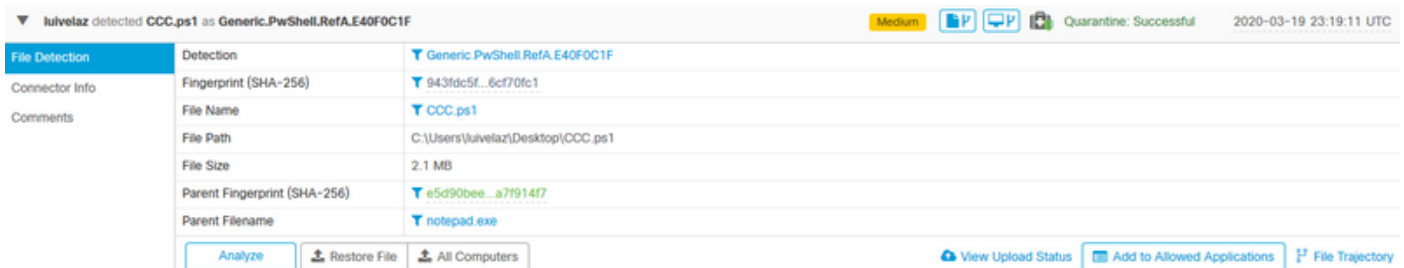
自定義排除

安全終端引擎

Tetra & SHA引擎的檔案掃描 (CPU使用率/檔案檢測) :

使用這些型別的排除可避免檢測/隔離檔案或減少安全端點高CPU。

安全端點控制檯上的事件如下圖所示。



The screenshot shows a file detection event in the Cisco Secure Endpoint console. The event details are as follows:

Field	Value
Detection	Generic.PwShell.RefA.E40F0C1F
Fingerprint (SHA-256)	943fde5f...6cf70fc1
File Name	CCC.ps1
File Path	C:\Users\luvelaz\Desktop\CCC.ps1
File Size	2.1 MB
Parent Fingerprint (SHA-256)	e5d90bee...a7f914f7
Parent Filename	notepad.exe

At the bottom of the console, there are buttons for "Analyze", "Restore File", and "All Computers". On the right side, there are links for "View Upload Status", "Add to Allowed Applications", and "File Trajectory".


 注意:CSIDL可用於排除項，有關CSIDL的詳細信息，請參閱此Microsoft文檔。

路徑排除

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


萬用字元排除

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


 註：選項Apply to all drive letters（應用於所有驅動器碟符）也用於將排除項應用於連線到系統的驅動器[A-Z]。

副檔名排除

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

 注意：請謹慎使用此排除型別，因為它會排除所有具有副檔名的檔案，而不管其路徑位置如何。

進程：檔案掃描排除

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		

系統流程保護(SPP)

系統進程保護引擎可從連結器版本6.0.5中獲得，它可保護下一個Windows進程：

- 會話管理器子系統(smss.exe)
- 客戶端/伺服器運行時子系統(csrss.exe)
- 本地安全授權子系統(lsass.exe)
- Windows登入應用程式(winlogon.exe)
- Windows啟動應用程式(wininit.exe)

此圖顯示SPP事件。

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

SPP排除

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 conditions must 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 conditions must be met for the process to be excluded.		
<input checked="" type="checkbox"/> Apply to child processes		

惡意活動保護(MAP)

惡意活動保護(MAP)引擎可保護您的終端免受勒索軟體攻擊。它可以在惡意操作或進程執行時識別它們，並保護您的資料免遭加密。

MAP事件如本圖所示。

Malicious Activity Protection	Fingerprint (SHA-256)	9967f55a...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)	9967f55a...2956d820
	Parent Filename	rewrite.exe

Analyze Restore File All Computers

MAP排除

Process	Path	Path\to\the\executable.exe	
Malicious Activity	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			

注意：在確認檢測確實不是惡意程式後，請謹慎使用此型別的排除。

防漏洞(Exprev)

漏洞攻擊防禦引擎可保護您的終端免受惡意軟體常用記憶體注入攻擊以及其他針對未修補軟體的零日攻擊

漏洞。當檢測到對受保護進程的攻擊時，將被阻止並生成事件，但不會隔離該進程。

Exprev事件如圖所示。

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

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\lend...app_1dbe42229d1ba886_07e5.0402_a608579ft
	File Size	5.82 MB
	Parent Fingerprint (SHA-256)	375a7501...e8624659
	Parent Filename	dfsvc.exe
	Parent File Size	24.27 KB

Exprev排除

Executable	Name	CUDL.LOS.exe	
Exploit Prevention	Provide an executable name to be excluded from protection by the Exploit Prevention engine (Example: ValidExecutable.exe).		

注意：只要您信任受影響的模組/應用程式上的活動，即可使用此排除項。

行為保護(BP)

行為保護引擎增強了以行為方式檢測和阻止威脅的能力。它增強了檢測「陸地生活」攻擊的能力，並提供通過特徵碼更新更快地響應威脅形勢的變化。

BP事件如本圖所示。

Testing.machine2.amp detected Scheduled Task Containing Suspicious Target Tactics Medium Threat Detection 2022-10-20 17:07:41 UTC

Event Overview

Connector Details

Comments

Description	A suspicious scheduled task was created. This particular task stands out because it references a shortcut (.lnk) or a VB script file (.vba or .vbs). The schtasks command can create one-time only tasks, recurring tasks, and tasks that run based on specific system events, such as logon and startup. Malware can use scheduled tasks to establish persistence.		
Occured At	2022-10-20 17:07:40 UTC		
MITRE ATT&CK	Tactics	TA0002: Execution TA0003: Persistence	
	Techniques	T1053.005: Scheduled Task/Job: Scheduled Task	

Observables

▼ File: schtasks.exe ▼ 013c013e...b0ad28ef ▼

Analyze

BP排除

Process	Path	Path/to/the/executable/executable.exe	
Behavioral Protection	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 type="checkbox"/> Apply to child processes			

+ Add Exclusion + Add Multiple Exclusions... Save

相關資訊

- [有關策略配置的詳細資訊，請導航至《使用手冊》](#)
- [在Cisco Secure Endpoint Connector影片中建立排除項](#)
- [技術支援與文件 - Cisco Systems](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。