在Cisco Secure Endpoint Connector中配置和管理例外项

目录

简介

先决条件

- 要求
- 使用的组件

安全终端工作流程

思科维护的例外项

自定义排除

- 安全终端引擎
  - 路径排除
  - 通配符排除
  - 文件扩展名排除
  - 进程：文件扫描排除
- 系统进程保护(SPP)
  - SPP排除
- 恶意活动保护(MAP)
  - MAP排除
- 漏洞防御(Exprev)
- 行为保护(BP)

相关信息

简介

本文档介绍如何为思科安全终端控制台上的不同引擎创建例外项。

先决条件

要求

Cisco 建议您了解以下主题：

- 修改排除列表并将其应用于安全终端控制台中的策略
- Windows CSIDL约定

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科安全终端控制台5.4.20211013

- 安全终端用户指南修订版2021年10月15日

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

安全终端工作流程

在高级操作中，思科安全终端通过连接器的主要组件按以下顺序处理文件安全散列算法(SHA):

- 排除
- Tetra引擎
- 应用控制（允许列表/阻止列表）
- SHA引擎
- 漏洞防御(Exprev)/恶意活动保护(MAP)/系统进程保护/网络引擎（设备流关联）

注意：“排除”或“允许/阻止列表”创建取决于哪个引擎检测到文件。

思科维护的例外项

思科维护的例外项由思科创建并维护，以便在安全终端连接器与防病毒、安全产品或其他软件之间提供更好的兼容性。

这些排除集包含不同类型的排除以确保正确操作。

您可以在Cisco-Maintended Exclusion List Changes for Cisco Secure Endpoint Console文章中跟踪对这些例外项执行的更改。

自定义排除

安全终端引擎

Tetra和SHA引擎的文件扫描（CPU使用情况/文件检测）：

使用这些类型的例外可避免检测/隔离文件或减少安全终端CPU使用率较高。

安全终端控制台上的事件如图所示。

注意:CSIDL可用于排除项，有关CSIDL的详细信息，请参阅此Microsoft文档。

路径排除

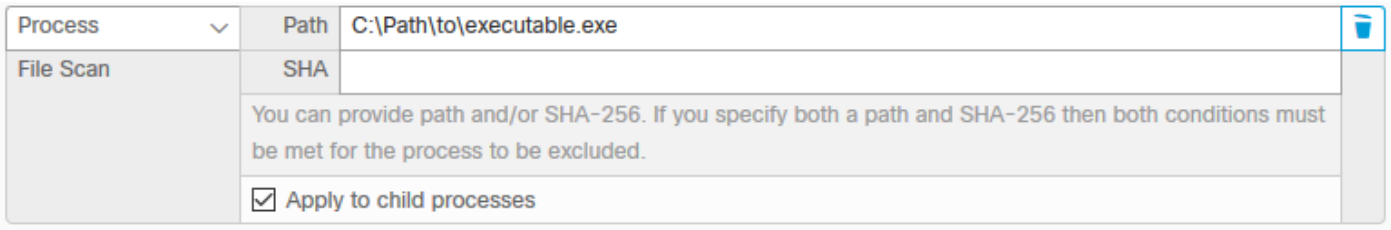
通配符排除

注意：选项Apply to all drive letters也用于将例外项应用于连接到系统的驱动器[A-Z]。

文件扩展名排除

注意：请谨慎使用此排除类型，因为它会排除所有具有文件扩展名的文件，而不考虑路径位置。

进程：文件扫描排除

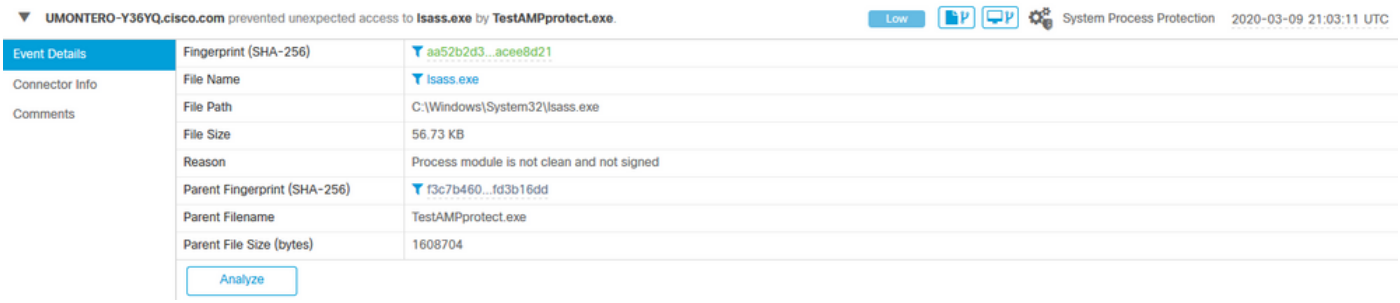


系统进程保护(SPP)

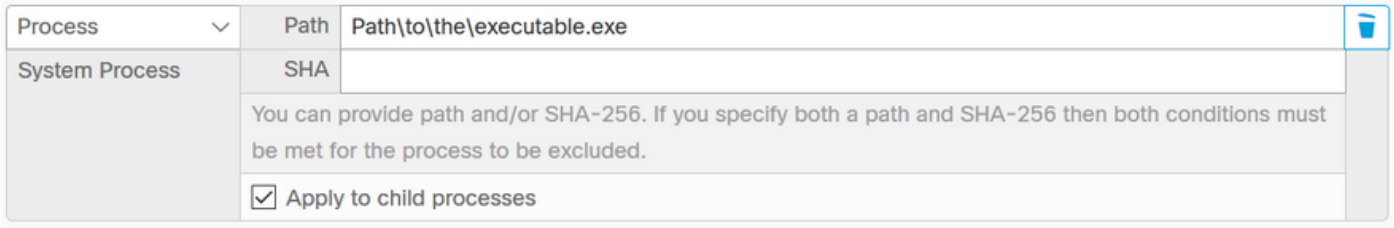
System Process Protection引擎可从连接器版本6.0.5中获得，它可保护下一个Windows进程：

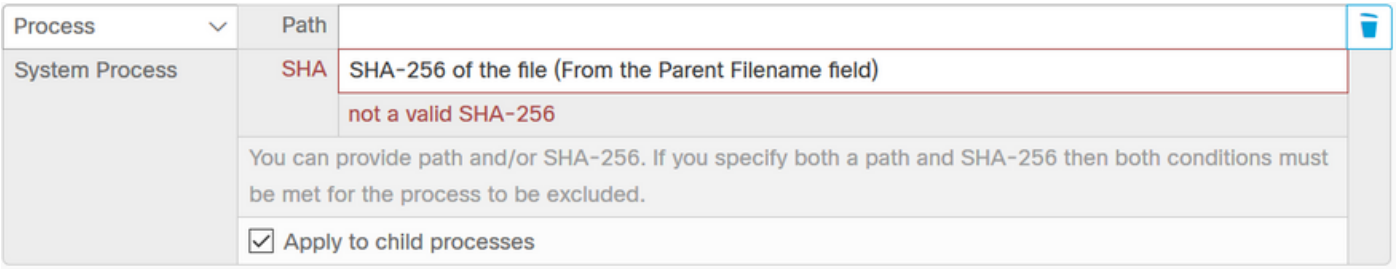
- 会话管理器子系统(smss.exe)
- 客户端/服务器运行时子系统(csrss.exe)
- 本地安全授权子系统(lsass.exe)
- Windows登录应用程序(winlogon.exe)
- Windows启动应用程序(wininit.exe)

此图显示SPP事件。



SPP排除

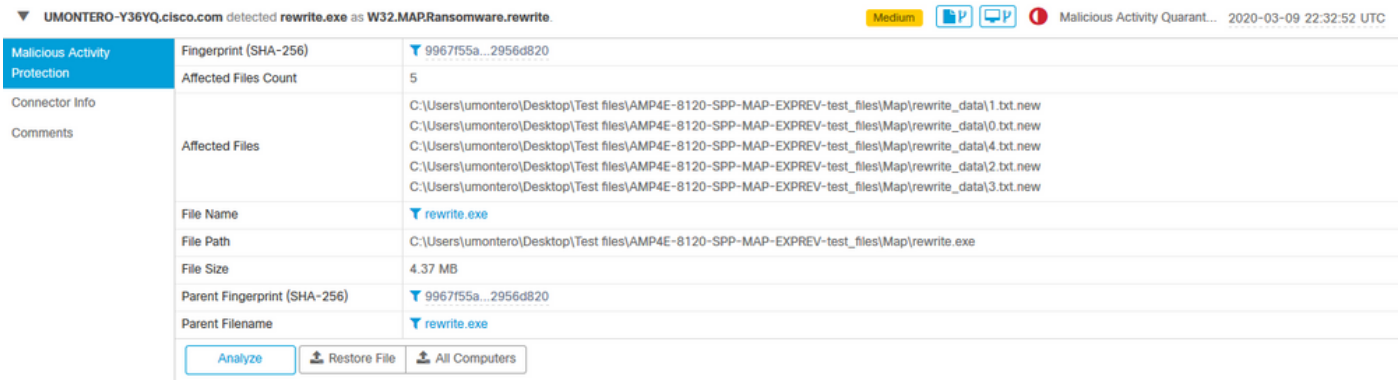




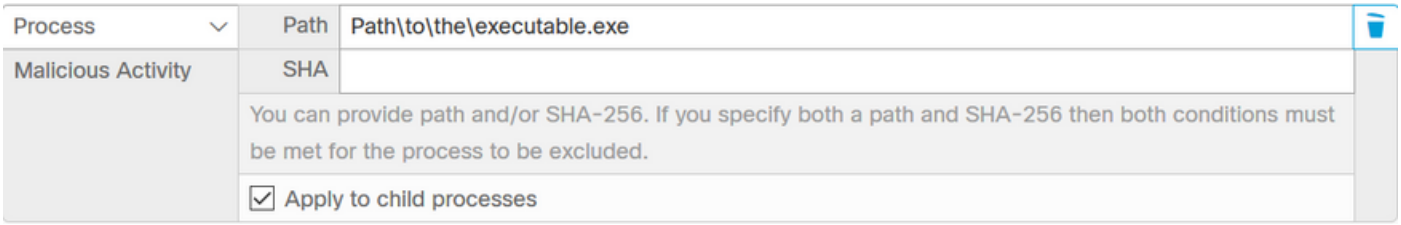
恶意活动保护(MAP)

恶意活动保护(MAP)引擎可保护您的终端免受勒索软件攻击。它可以在恶意操作或进程执行时识别它们，并保护您的数据免遭加密。

MAP事件显示在此图像中。



MAP排除

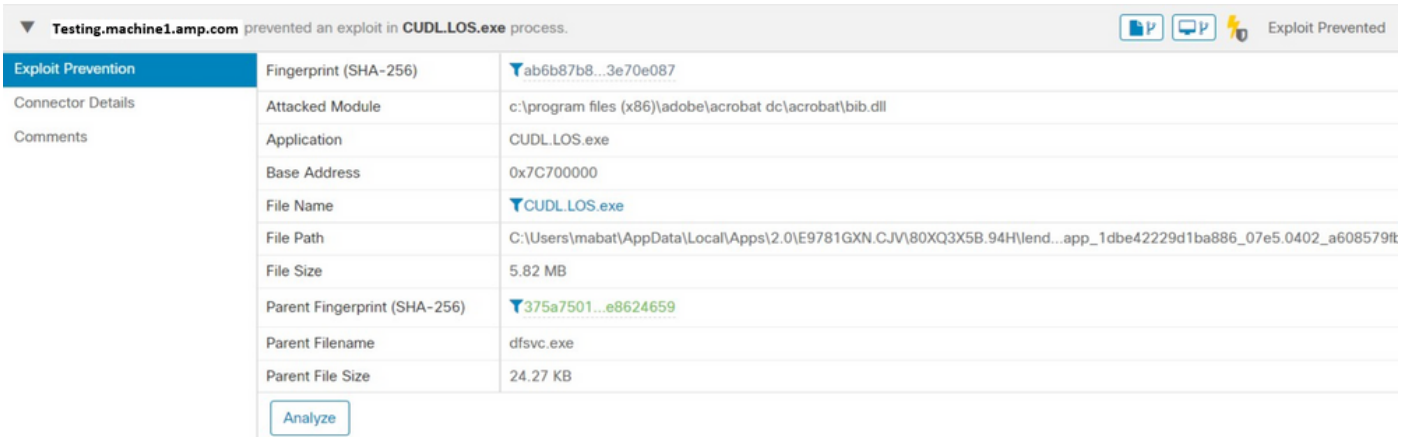


⚠ 注意：在确认检测确实不是恶意之后，请谨慎使用此类型的排除。

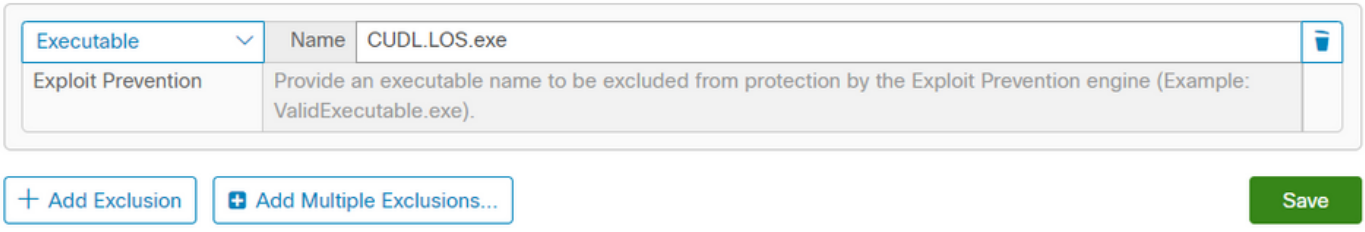
漏洞防御(Exprev)

利用漏洞防御引擎可保护您的终端免受恶意软件通常使用的内存注入攻击，以及其他针对未修补软件的零日攻击
漏洞。当检测到对受保护进程的攻击时，将被阻止并生成事件，但不会隔离该进程。

Exprev事件如图所示。



Exprev排除

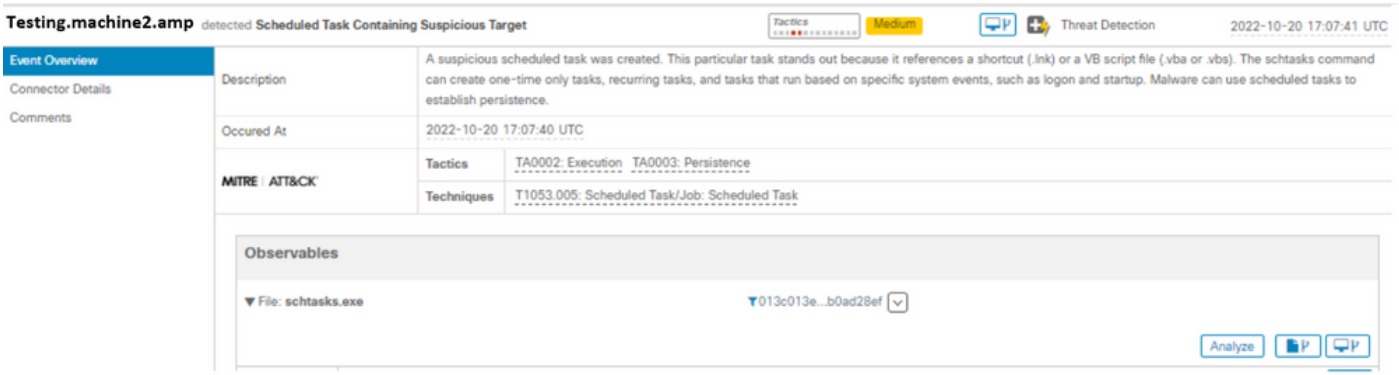


⚠ 注意：只要您信任受影响模块/应用程序上的活动，即可使用此排除项。

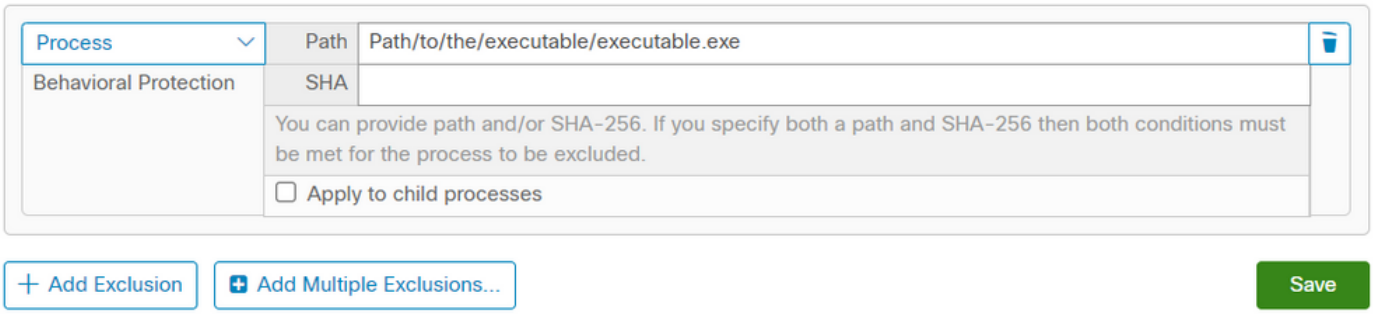
行为保护(BP)

行为保护引擎增强了以行为方式检测和阻止威胁的能力。它提高了检测“离家出走”攻击的能力，并提供
通过签名更新更快地响应威胁形势的变化。

BP事件如图所示。



BP排除



相关信息

- 有关策略配置的详细信息，请导航至《用户指南》
- 在Cisco Secure Endpoint Connector视频中创建例外项
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。