在安全终端中排除误报文件分析事件

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

在安全终端中排除误报文件分析故障

- 文件SHA 256哈希
- 文件示例副本
- 从安全终端控制台捕获警报事件
- 来自安全终端控制台的JSON事件详细信息
- 有关文件的信息
- 说明
- 提供信息

简介

本文档介绍如何在思科安全终端中收集误报文件分析。

先决条件

要求

思科建议您了解安全终端控制台控制面板。

使用的组件

本文档中的信息基于安全终端版本8.x.x及更高版本。

注意：需要具有管理员权限的帐户。

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。

背景信息

安全终端可能会生成有关特定文件/进程/脚本/安全哈希算法(SHA)256的过多警报。如果您怀疑网络中存在任何误报检测，您可以联系思科TAC，诊断团队会继续执行更深入的文件分析。当您联系思科TAC时，必须提供以下信息：

·文件SHA 256哈希
·文件示例副本
·从安全终端控制台捕获警报事件

·从安全终端控制台捕获的JSON事件详细信息
·有关文件的信息（文件来自何处，以及为何必须存在于环境中）
·解释为什么您认为文件/进程可能是误报

思科始终致力于改进和扩展安全终端技术的威胁情报，但是，如果您的安全终端解决方案错误地触发了警报，您可以采取一些措施以防止对您的环境造成任何进一步的影响。本文档提供了获取所有所需详细信息的指南，以便向思科TAC提交有关误报问题的支持请求。根据诊断组文件分析，文件性质可以更改以停止在安全终端控制台上触发的警报事件，或者Cisco TAC可提供适当的修复程序，让运行文件/进程时不会在您的环境中出现问题。

排除安全终端中的误报文件分析故障

此部分提供可用于获取通过Cisco TAC打开误报票证所需的所有详细信息。

文件SHA 256哈希

步骤1.要获取SHA 256哈希，请导航到安全终端控制台>控制面板>事件。

步骤2.选择Alertand事件单击SHA256，然后选择Copy，如图所示。

File Detection

Medium

Summary

[redacted] detected **eicar_com.zip** as **ZIP.INV.2546DCFF.CAE.Talos**.

Occurred at [redacted]

Hostname lenovo-laptop-amp >

Group Protect

User Not Available

MITRE

Detecti

Detecti AE.Talos

JSON

Descri

Relate

Medium

com.zip as **ZIP.INV.2546DCFF.CAE.Talos**.

Medium

Obser

File

SHA-256 2546dcff...6e9eedad

File name eicar_com.zip

File path F:\Downloads\eicar_com.zip

File size 184 Bytes

Threat score 95

Parent

SHA-256 33453391...9e505168

File name curl.exe

File size 695.05 KB

Comments 0

Filename eicar_com.zip

Copy

Search

Filter

VirusTotal 62/77

Detected Eicar-test-file (not a

Full report

File Fetch

File Analysis

File Trajectory

Outbreak Control

Simple Detections

Allowed Applications

Blocked Applications

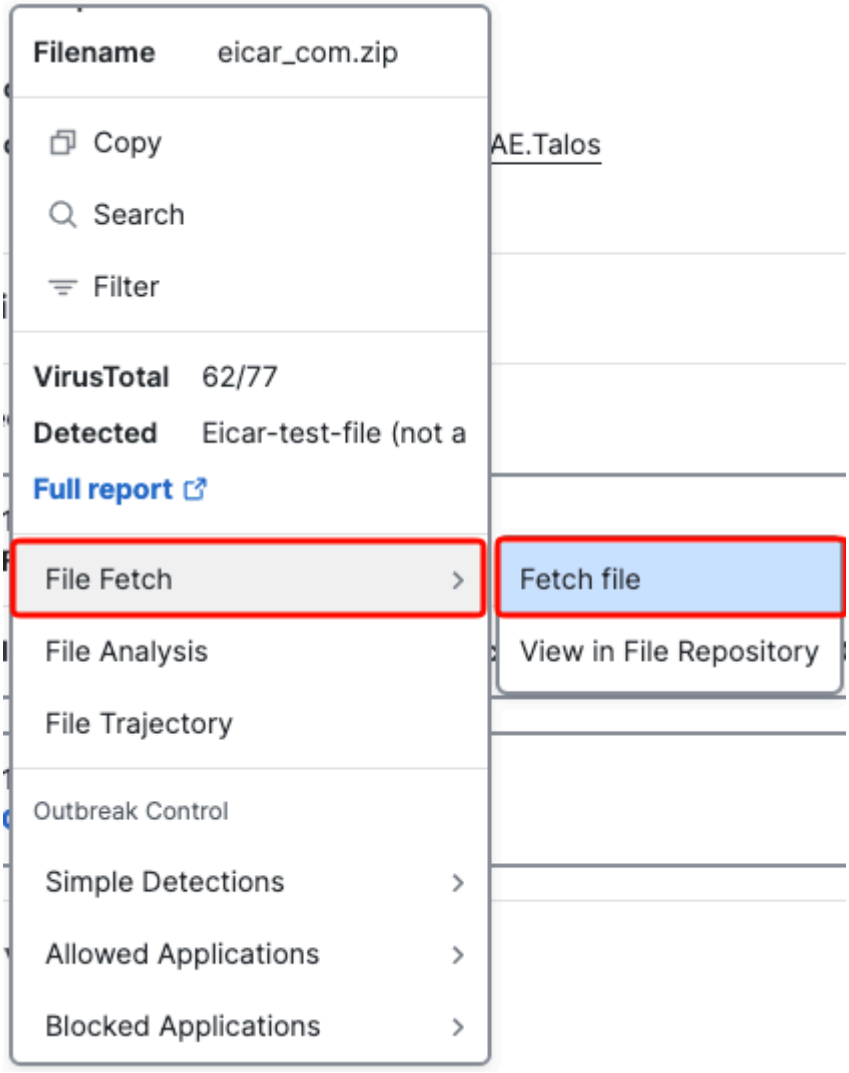
Device Trajectory

Scan | Move to group | More

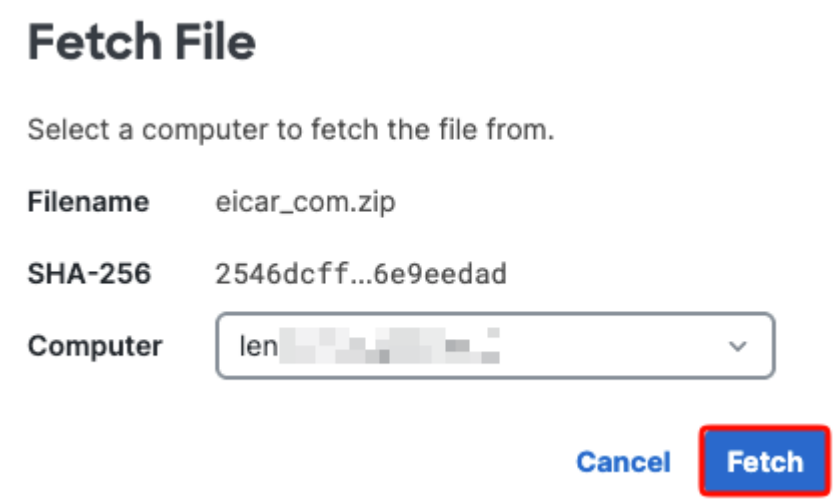
文件示例副本

步骤1.您可以从安全终端控制台获取文件示例，导航到安全终端控制台>控制面板>事件。

步骤2.选择Alert Event，单击SHA256，然后导航到File Fetch > Fetch File，如图所示。

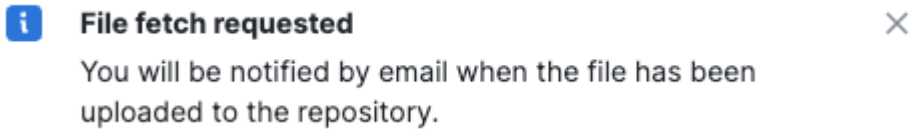


步骤3.选择检测到文件的设备，然后单击Fetch，如图所示。

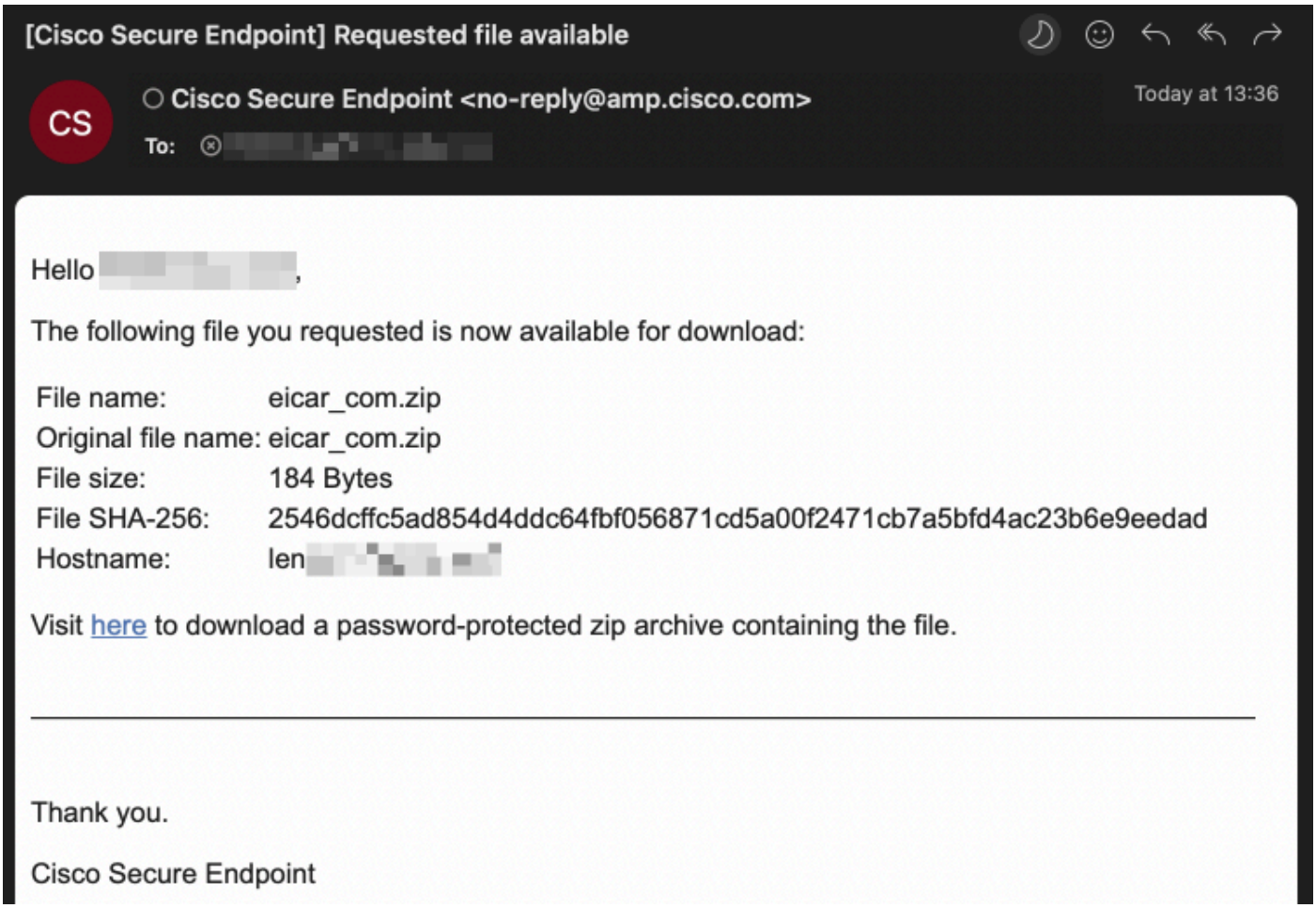


注意：必须打开设备才能成功获取示例文件。

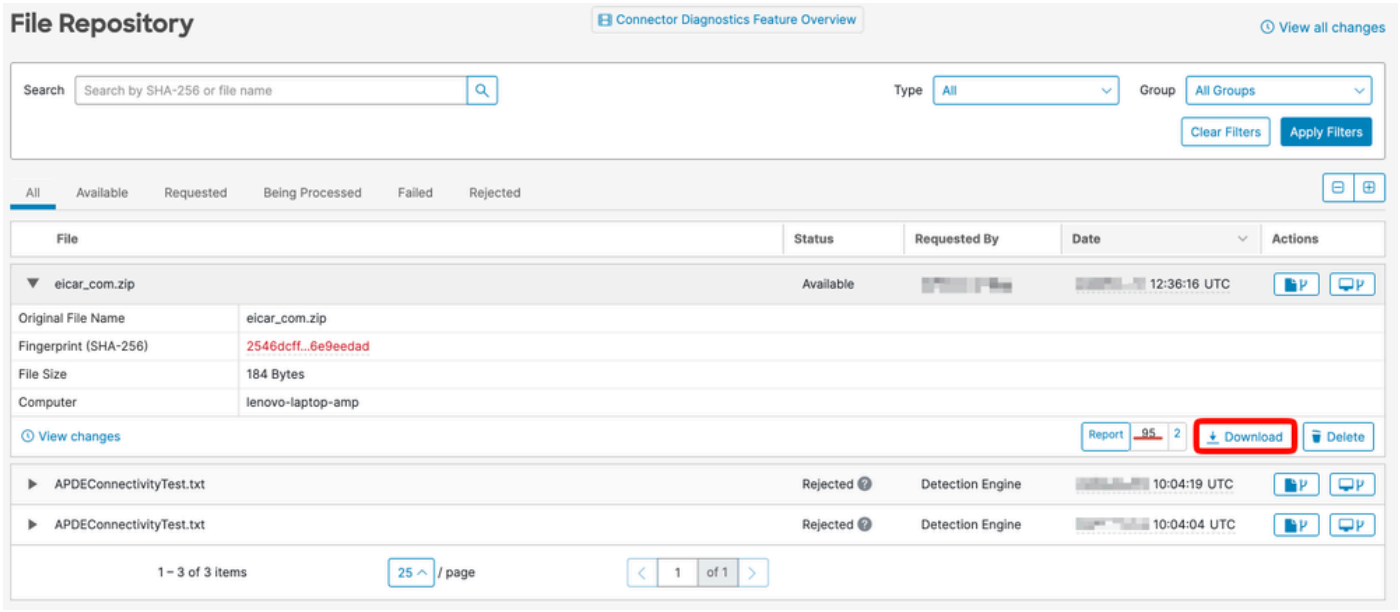
步骤4.您收到通知，如图所示。



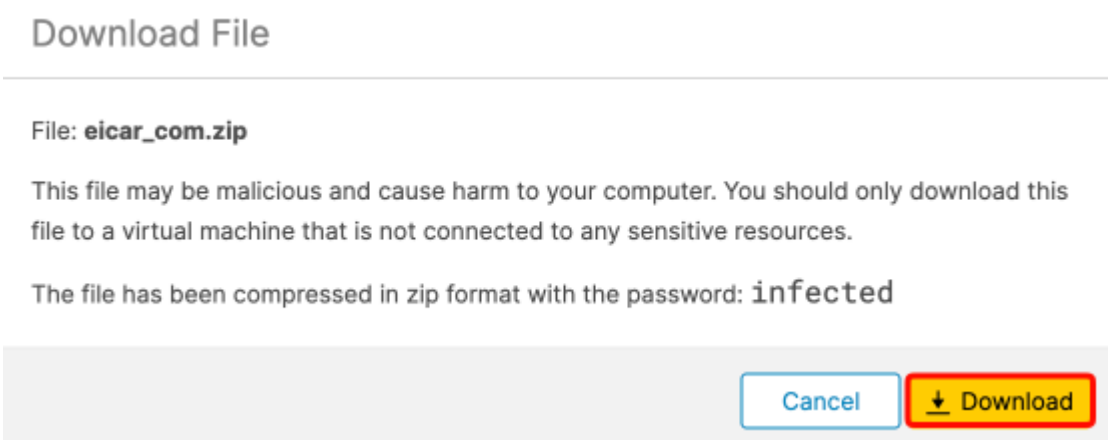
几分钟后，当文件可供下载时，您会收到电子邮件通知，如图所示。



步骤5.导航到Secure Endpoint Console > Analysis > File Repository，然后选择Download，如图所示。



步骤6.出现通知框，单击Download（如图所示），该文件将下载为ZIP文件。



从安全终端控制台捕获警报事件

步骤1.导航到安全终端控制台>控制面板>事件。

步骤2.选择Alert Event并捕获图像，如图所示。

File Detection

Medium

Summary

len[redacted] detected **eicar_com.zip** as **ZIP.INV.2546DCFF.CAE.Talos**.

Occurred at	[redacted] 12:22:10 UTC
Hostname	lenovo-laptop-amp ›
Group	Protect
User	Not Available
MITRE	[redacted]
Detection Engine	Tetra
Detection	ZIP.INV.2546DCFF.CAE.Talos
JSON	View ›

Description

Related events timeline

12:22:10 UTC — Medium
File Detection

len[redacted] detected **eicar_com.zip** as **ZIP.INV.2546DCFF.CAE.Talos**.

12:22:10 UTC — Medium
Quarantine Succeeded ›

Observables

File

SHA-256	2546dcff...6e9eedad
File name	eicar_com.zip
File path	F:\Downloads\eicar_com.zip
File size	184 Bytes
Threat score	95

Parent

SHA-256	33453391...9e505168
File name	curl.exe
File size	695.05 KB

Comments

0

Device Trajectory | Scan | Move to group | More

来自安全终端控制台的JSON事件详细信息

步骤1.导航到安全终端控制台>控制面板>事件。

步骤2.选择Alert Event，然后单击JSON选项旁边的View（如图所示）。

File Detection

Medium

Summary

len[redacted] detected **eicar_com.zip** as **ZIP.INV.2546DCFF.CAE.Talos**.

Occurred at	[redacted] 12:22:10 UTC
Hostname	lenovo-laptop-amp ›
Group	Protect
User	Not Available
MITRE	[redacted]
Detection Engine	Tetra
Detection	ZIP.INV.2546DCFF.CAE.Talos
JSON	View ›

Description

Related events timeline

12:22:10 UTC — Medium
File Detection

len[redacted] detected **eicar_com.zip** as **ZIP.INV.2546DCFF.CAE.Talos**.

12:22:10 UTC — Medium
Quarantine Succeeded ›

Observables

File

SHA-256	2546dcff...6e9eedad
File name	eicar_com.zip
File path	F:\Downloads\eicar_com.zip
File size	184 Bytes
Threat score	95

Parent

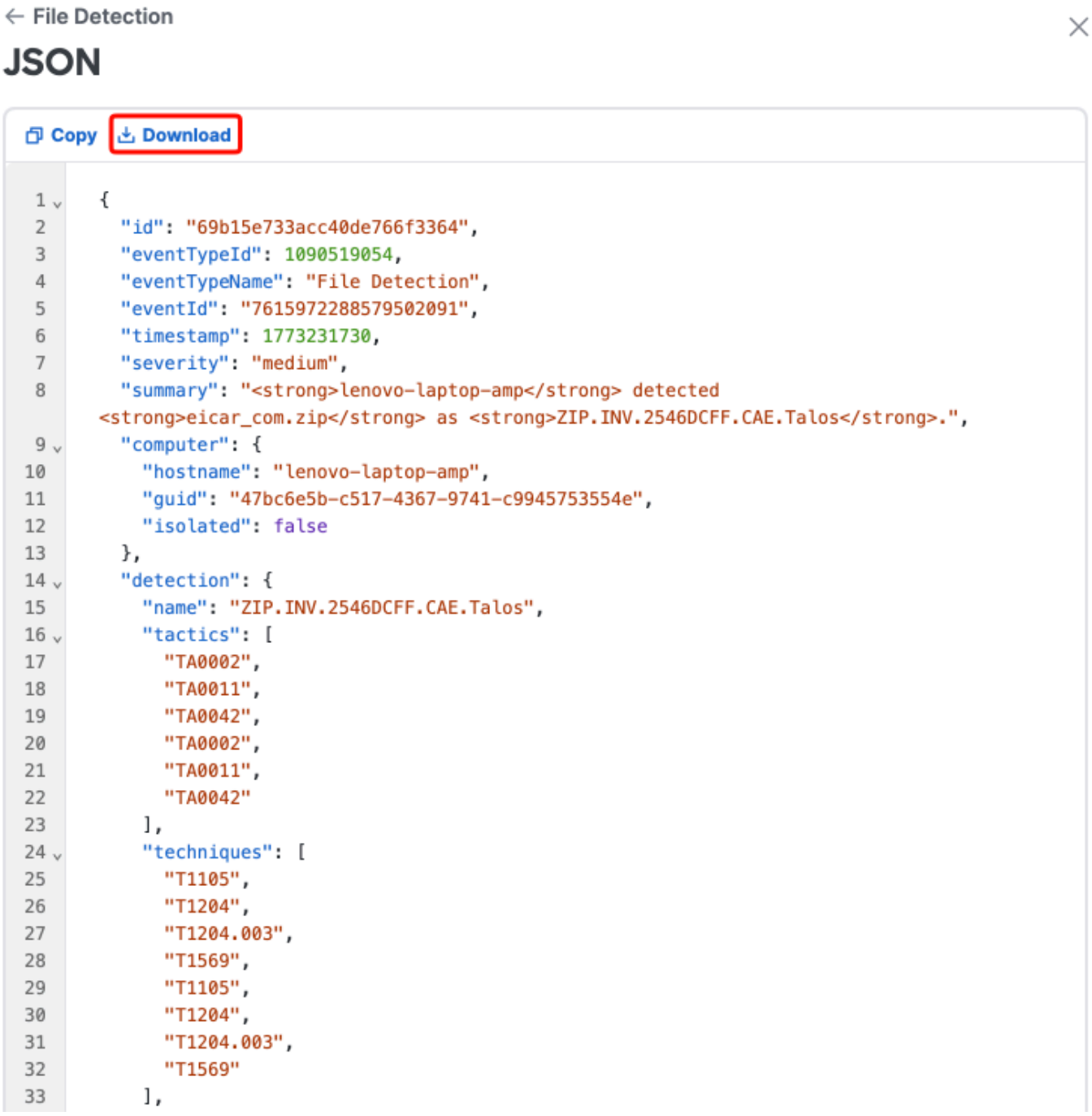
SHA-256	33453391...9e505168
File name	curl.exe
File size	695.05 KB

Comments

0

Device Trajectory | Scan | Move to group | More

它将打开JSON详细信息，如图所示。单击Download以保存内容。



有关文件的信息

- 有关文件来源的信息。
- 如果文件来自某个网站，请共享该Web URL。
- 共享一些文件说明并解释文件功能。

说明

- 为什么您认为文件进程可能是误报？
- 分享您信任文件的原因。

提供信息

- 收集所有详细信息后，请登录并将所有请求信息上传到您的思科案例。
- 确保您参考了服务请求(SR)编号。

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）。