Dépannage des événements d'analyse de fichiers faux positifs dans Secure Endpoint

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Dépannage de l'analyse des fichiers faux positifs dans Secure Endpoint
  - Fichier SHA 256 Hash
  - Exemple de copie de fichier
  - Capture d'événements d'alerte depuis Secure Endpoint Console
  - Détails de l'événement JSON depuis Secure Endpoint Console
  - Informations sur le fichier
  - Explication
  - Fournir des informations

Introduction

Ce document décrit comment collecter une analyse de fichier de faux positif dans Cisco Secure Endpoint.

Conditions préalables

Exigences

Cisco recommande que vous connaissiez le tableau de bord de la console Secure Endpoint.

Composants utilisés

Les informations contenues dans ce document sont basées sur Secure Endpoint version 8.x.x et ultérieures.

Remarque : Un compte doté de privilèges d'administrateur est nécessaire.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Les terminaux sécurisés peuvent générer des alertes excessives sur un certain fichier/processus/script/algorithme de hachage sécurisé (SHA) 256. Si vous suspectez des détections de faux positifs sur votre réseau, vous pouvez contacter le centre d'assistance technique Cisco et l'équipe de diagnostic poursuit l'analyse approfondie des fichiers. Lorsque vous contactez le centre d'assistance technique Cisco, vous devez fournir les informations suivantes :

· Fichier SHA 256 hash
· Exemple de copie de fichier
· Capture des événements d'alerte depuis Secure Endpoint Console

· Détails des événements JSON capturés à partir de la console Secure Endpoint
· Information sur le dossier (d'où il provient et pourquoi il doit être dans l'environnement)
· Expliquez pourquoi vous croyez que le dossier ou le processus peut être un faux positif

Cisco s'efforce toujours d'améliorer et de développer les informations sur les menaces pour la technologie Secure Endpoint. Toutefois, si votre solution Secure Endpoint déclenche une alerte par erreur, vous pouvez prendre des mesures pour empêcher tout impact supplémentaire sur votre environnement. Ce document fournit des directives pour obtenir tous les détails nécessaires afin d'ouvrir un dossier auprès du TAC de Cisco concernant un problème de faux positif. D'après l'analyse des fichiers de l'équipe de diagnostic, la disposition des fichiers peut être modifiée pour arrêter les événements d'alerte déclenchés sur Secure Endpoint Console ou Cisco TAC peut fournir le correctif approprié pour permettre l'exécution du fichier/processus sans problème dans votre environnement.

Dépannage de l'analyse des fichiers faux positifs dans Secure Endpoint

Cette section fournit les informations que vous pouvez utiliser pour obtenir tous les détails nécessaires à l'ouverture d'un ticket False Positive auprès du TAC Cisco.

Fichier SHA 256 Hash

Étape 1. Pour obtenir le hachage SHA 256, accédez à Secure Endpoint Console > Dashboard > Events.

Étape 2. Choisissez l'événement Alert and Cliquez sur le SHA256 et choisissez Copy comme indiqué dans l'image.

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

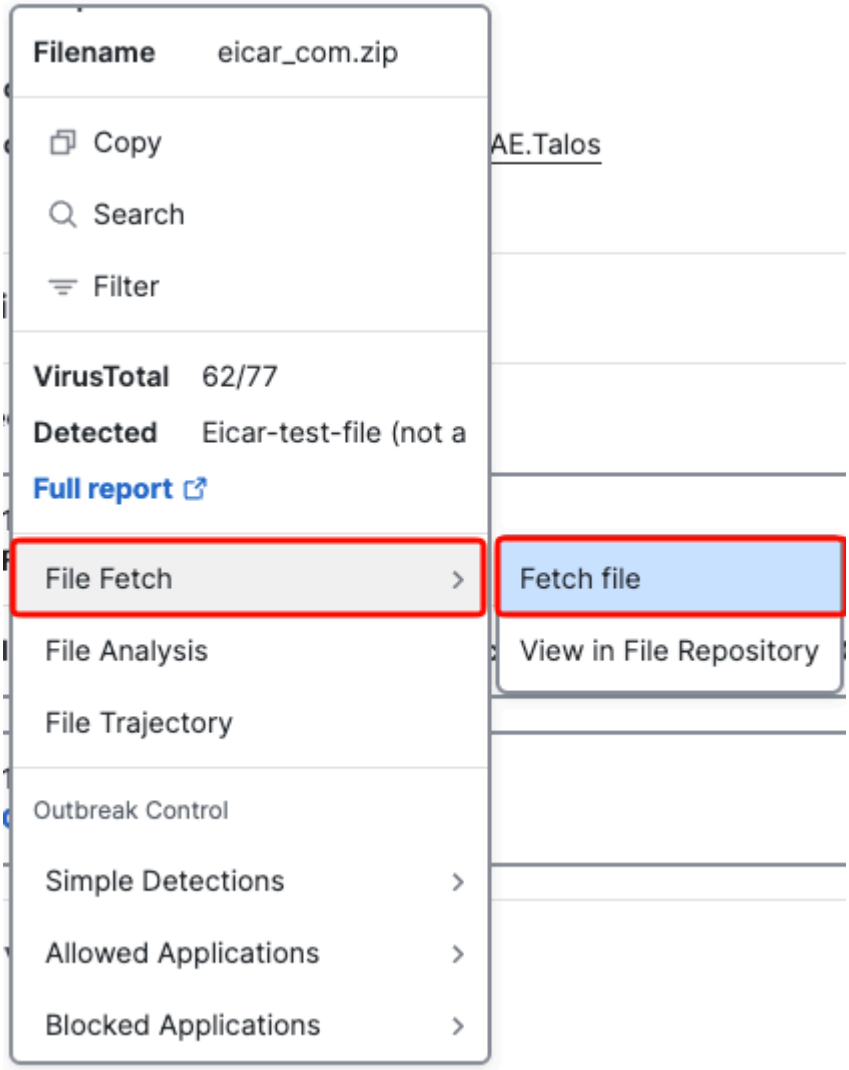
Device Trajectory

Scan | Move to group | More

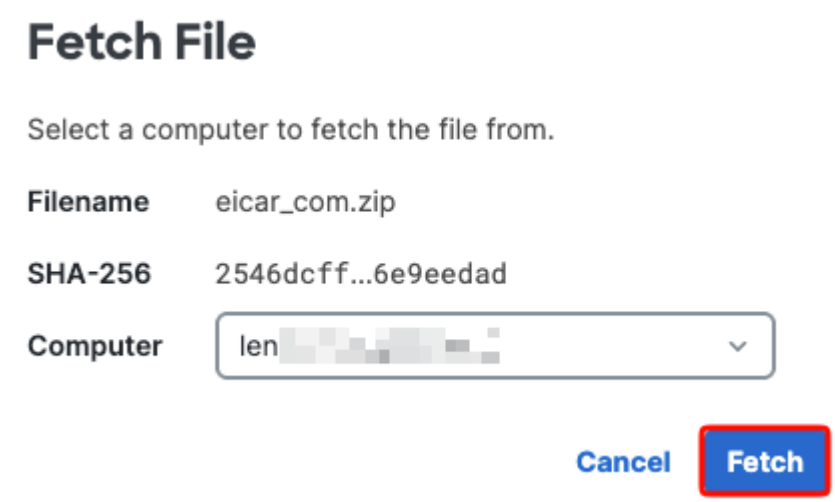
Exemple de copie de fichier

Étape 1. Vous pouvez obtenir l’exemple de fichier à partir de la console Secure Endpoint, naviguez jusqu’à la console Secure Endpoint > Dashboard > Events.

Étape 2. Choisissez l'événement d'alerte, cliquez sur le SHA256 et naviguez jusqu'à File Fetch > Fetch File comme indiqué dans l'image.

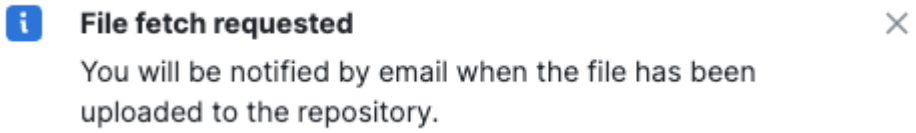


Étape 3. Choisissez le périphérique sur lequel le fichier a été détecté et cliquez sur Fetch comme indiqué dans l’image.

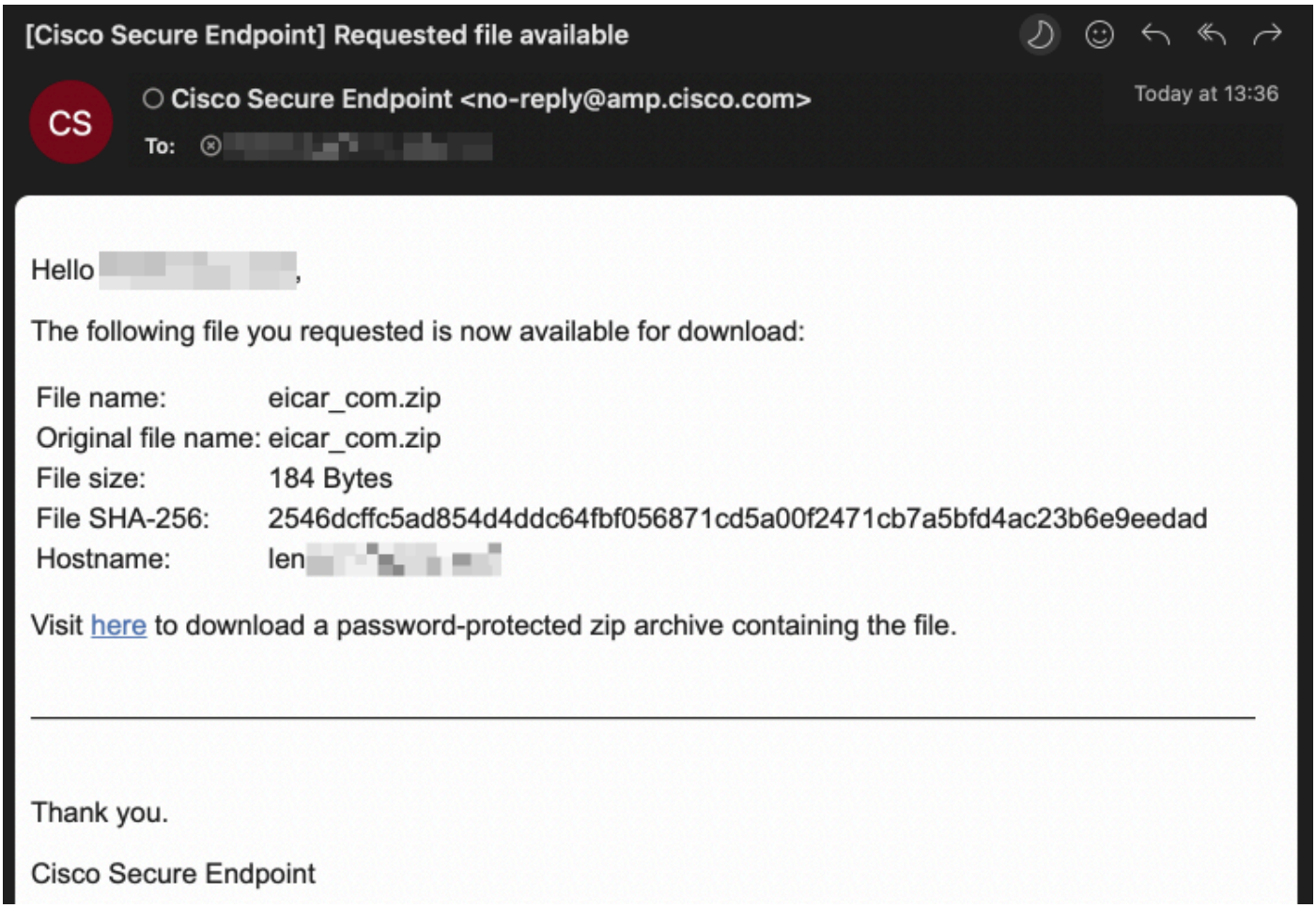


Remarque : Le périphérique doit être sous tension pour obtenir le fichier d'exemple.

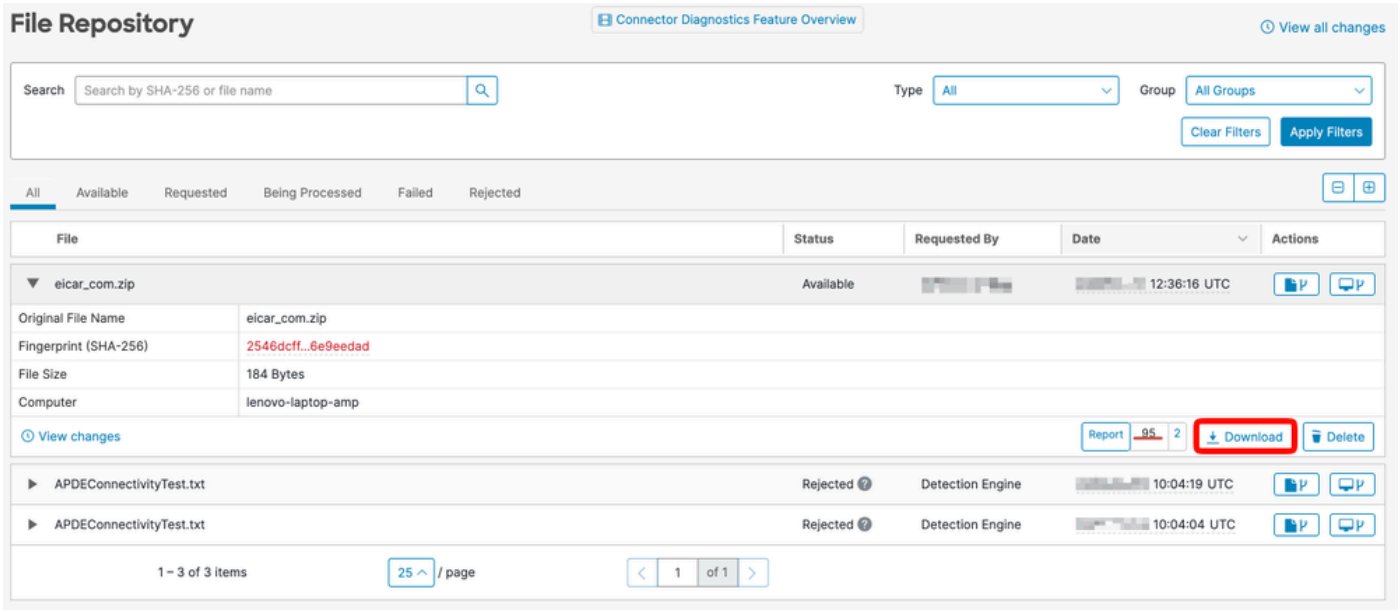
Étape 4. Vous recevez la notification comme indiqué dans l’image.



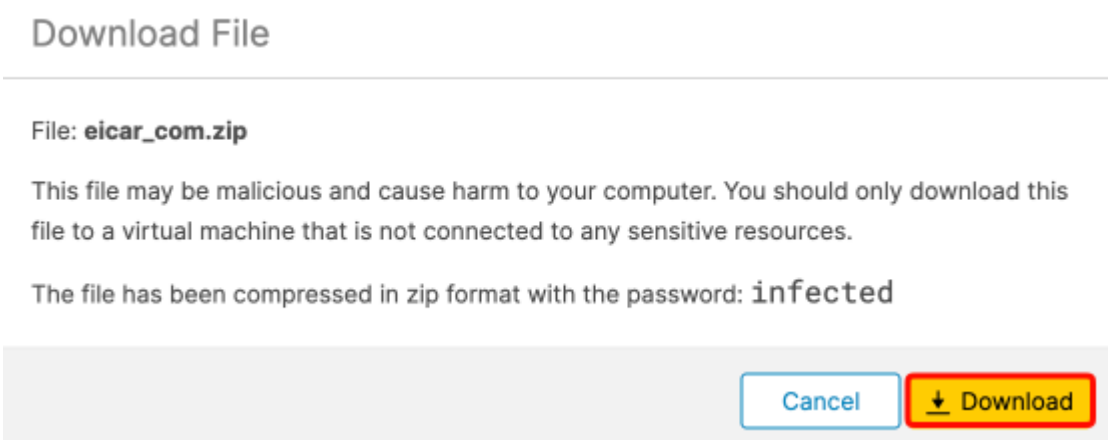
Après quelques minutes, vous recevez une notification par e-mail lorsque le fichier est disponible pour téléchargement, comme illustré dans l'image.



Étape 5. Accédez à Secure Endpoint Console > Analysis > File Repository et choisissez Download comme indiqué dans l'image.



Étape 6. Une boîte de notification apparaît, cliquez sur Download, comme indiqué dans l'image, et le fichier est téléchargé en tant que fichier ZIP.



Capture d'événements d'alerte depuis Secure Endpoint Console

Étape 1. Accédez à Secure Endpoint Console > Dashboard > Events.

Étape 2. Choisissez l'événement Alert et effectuez la capture comme indiqué dans l'image.

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

Détails de l'événement JSON depuis Secure Endpoint Console

Étape 1. Accédez à Secure Endpoint Console > Dashboard > Events.

Étape 2. Choisissez l'événement Alert et cliquez sur View, à côté de l'option JSON comme indiqué dans l'image.

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

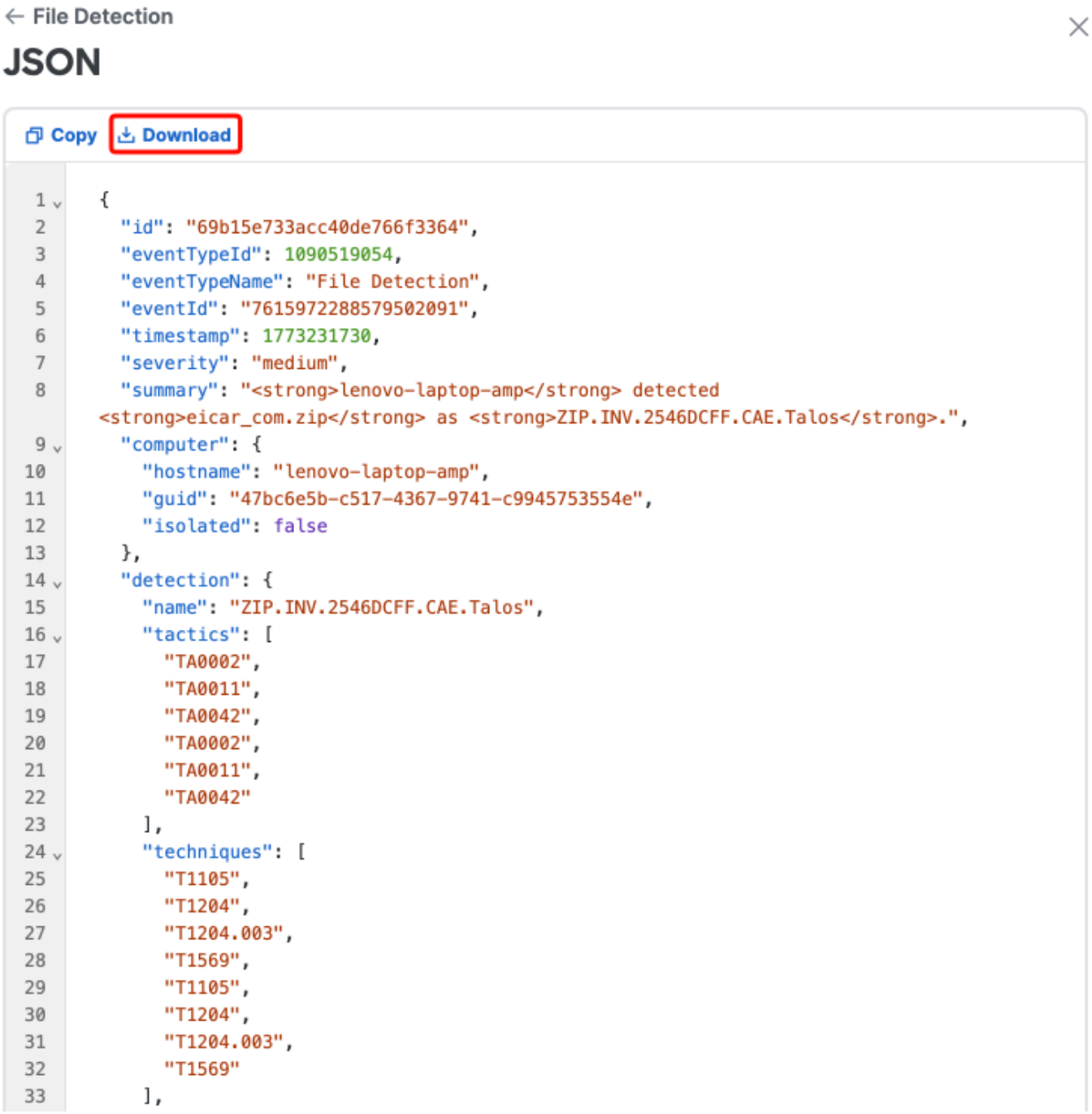
SHA-256	33453391...9e505168
File name	curl.exe
File size	695.05 KB

Comments

0

Device Trajectory | Scan | Move to group | More

Il ouvre les détails JSON comme indiqué dans l'image. Cliquez sur Download afin d'enregistrer le contenu.



Informations sur le fichier

- Informations sur l'origine du fichier.
- Si le fichier provient d'un site Web, partagez l'URL Web.
- Partagez une petite description du fichier et expliquez sa fonction.

Explication

- Pourquoi pensez-vous que le processus de traitement des fichiers peut être un faux positif ?
- Partagez les raisons pour lesquelles vous approuvez le fichier.

Fournir des informations

- Une fois que vous avez collecté tous les détails, connectez-vous et téléchargez toutes les informations demandées dans votre dossier Cisco.
- Veillez à faire référence au numéro de la demande de service (SR).

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.