

Dépannage de l'analyse de fichiers faux positifs dans AMP for Endpoints

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Dépannage de l'analyse de fichiers faux positifs dans AMP for Endpoints](#)

[Hachage du fichier SHA 256](#)

[Exemple de copie de fichier](#)

[Capture des événements d'alerte à partir de la console AMP](#)

[Capture des détails de l'événement à partir de la console AMP](#)

[Informations sur le fichier](#)

[Explication](#)

[Fournir des informations](#)

[Conclusion](#)

Introduction

Ce document décrit comment collecter une analyse de fichier False Positive dans Advanced Malware Protection (AMP) for Endpoints.

Contribué par Jesus Javier Martinez, ingénieur TAC Cisco.

Conditions préalables

Conditions requises

Cisco recommande de posséder des connaissances sur ces sujets :

- Tableau de bord de la console AMP
- Un compte avec des privilèges d'administrateur

Components Used

Les informations de ce document sont basées sur Cisco AMP for Endpoints version 6.X.X et ultérieure.

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. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

AMP for Endpoints peut générer des alertes excessives sur un fichier/processus/algorithmes de hachage sécurisé (SHA) spécifique 256. Si vous soupçonnez des détections de faux positifs sur votre réseau, vous pouvez contacter le centre d'assistance technique de Cisco (TAC), l'équipe de diagnostic procède à une analyse approfondie des fichiers. Lorsque vous contactez le TAC Cisco, vous devez fournir les informations suivantes :

Hachage du fichier · SHA 256

Copie d'exemple de fichier ·

Capture d'événements d'alerte · à partir de la console AMP

Capture des détails des événements · depuis AMP Console

Informations · sur le fichier (d'où il provient et pourquoi il doit être dans l'environnement)

· Expliquez pourquoi pensez-vous que le fichier/processus peut être un faux positif

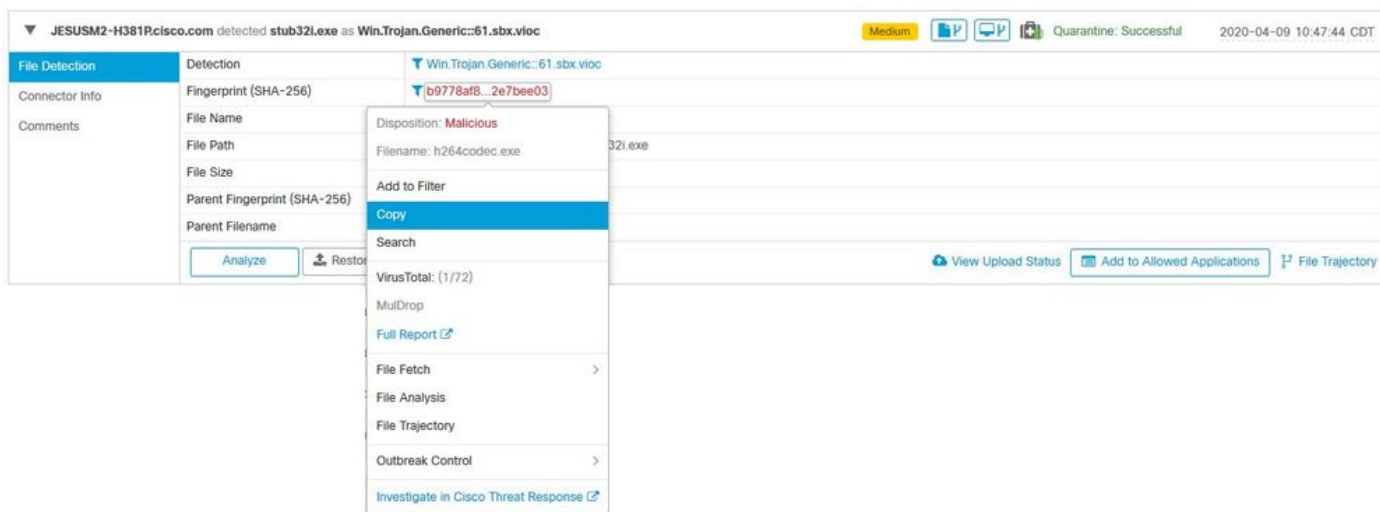
Dépanner l'analyse de fichiers faux positifs dans AMP for Endpoints

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

Hachage du fichier SHA 256

Étape 1. Pour obtenir le hachage SHA 256, accédez à **Console AMP > Tableau de bord > Événements**.

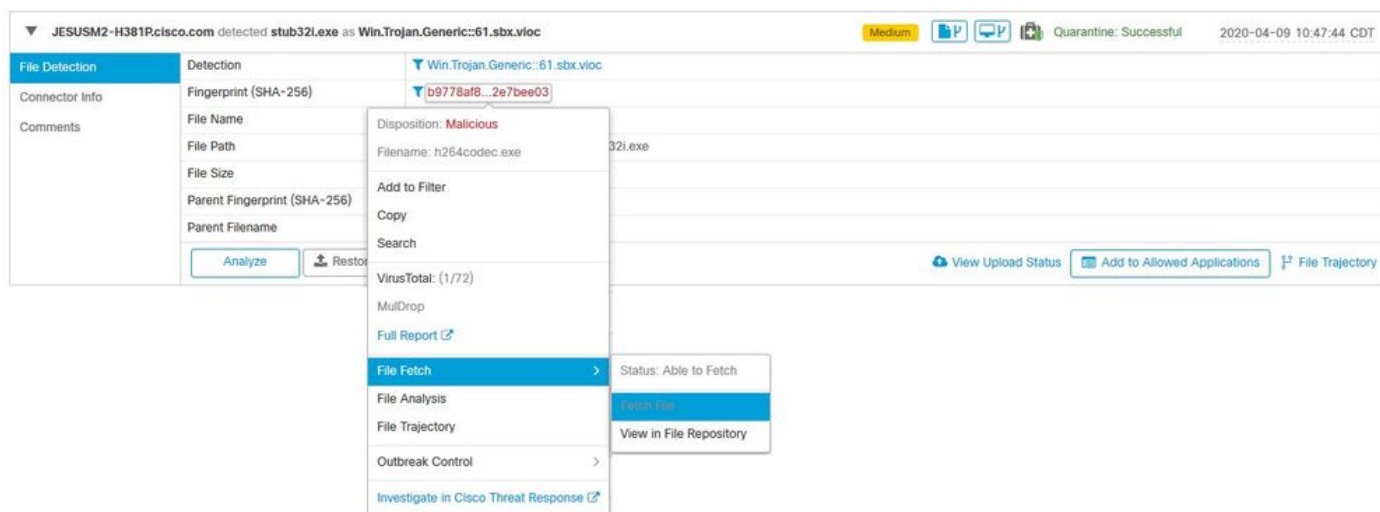
Étape 2. Sélectionnez l'événement d'alerte, cliquez sur le **SHA256** et sélectionnez **Copier** comme indiqué dans l'image.



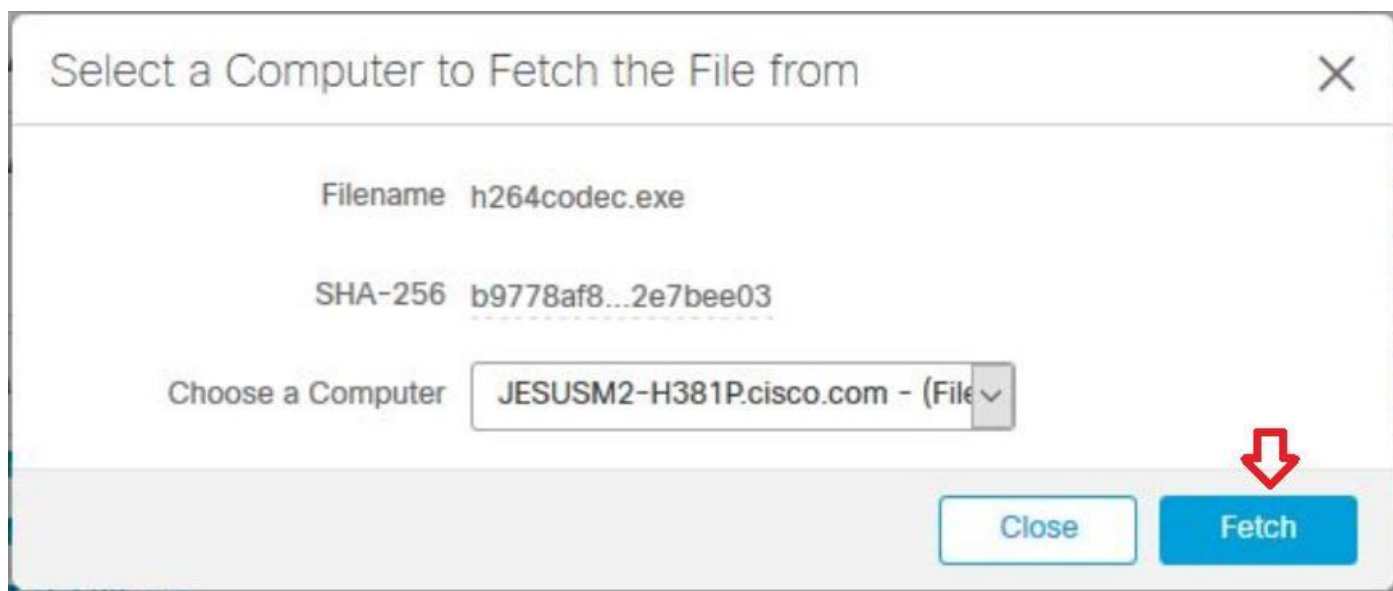
Exemple de copie de fichier

Étape 1. Vous pouvez obtenir l'exemple de fichier à partir de la console AMP, accéder à **la console AMP > Tableau de bord > Événements**.

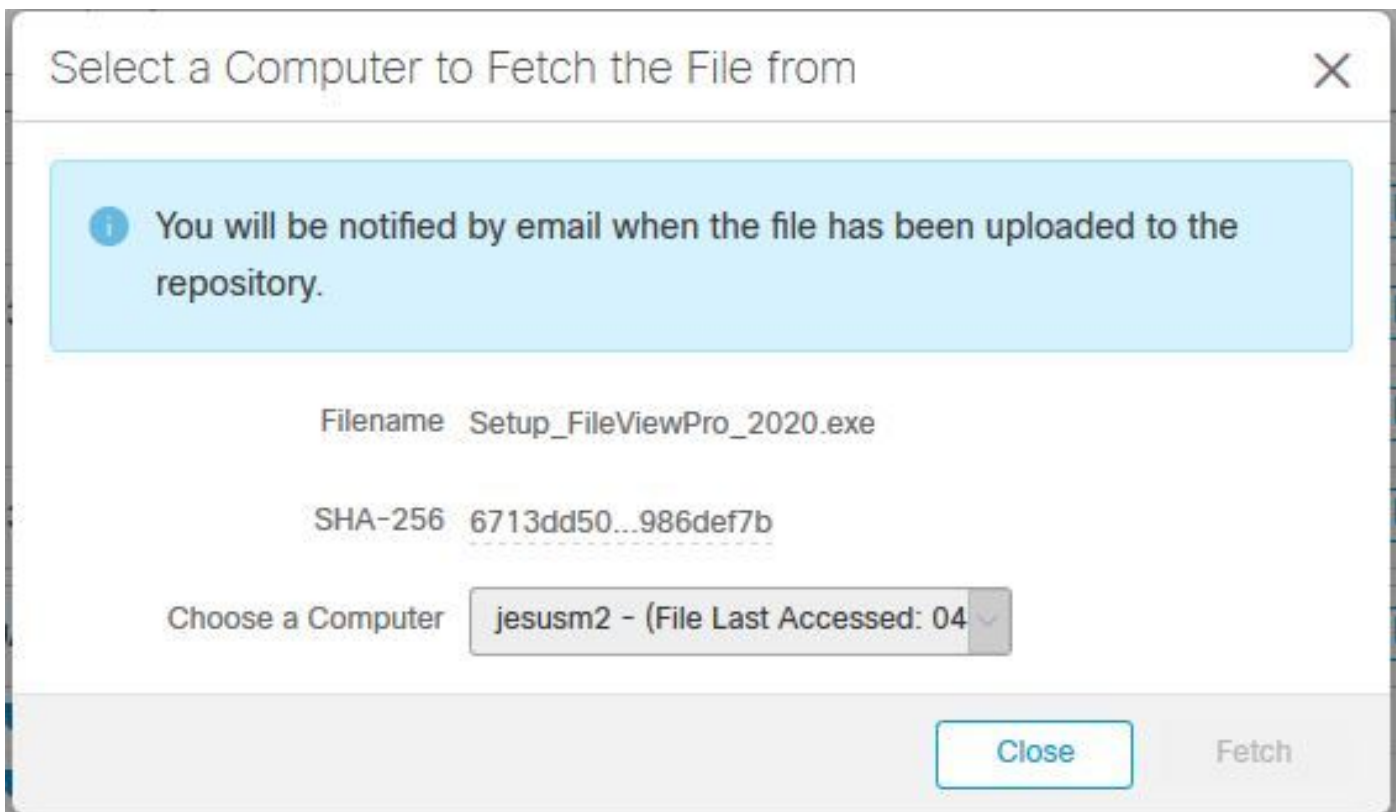
Étape 2. Sélectionnez l'événement d'alerte, cliquez sur le **SHA256** et naviguez jusqu'à **File Fetch** > **File Fetch** comme indiqué dans l'image.



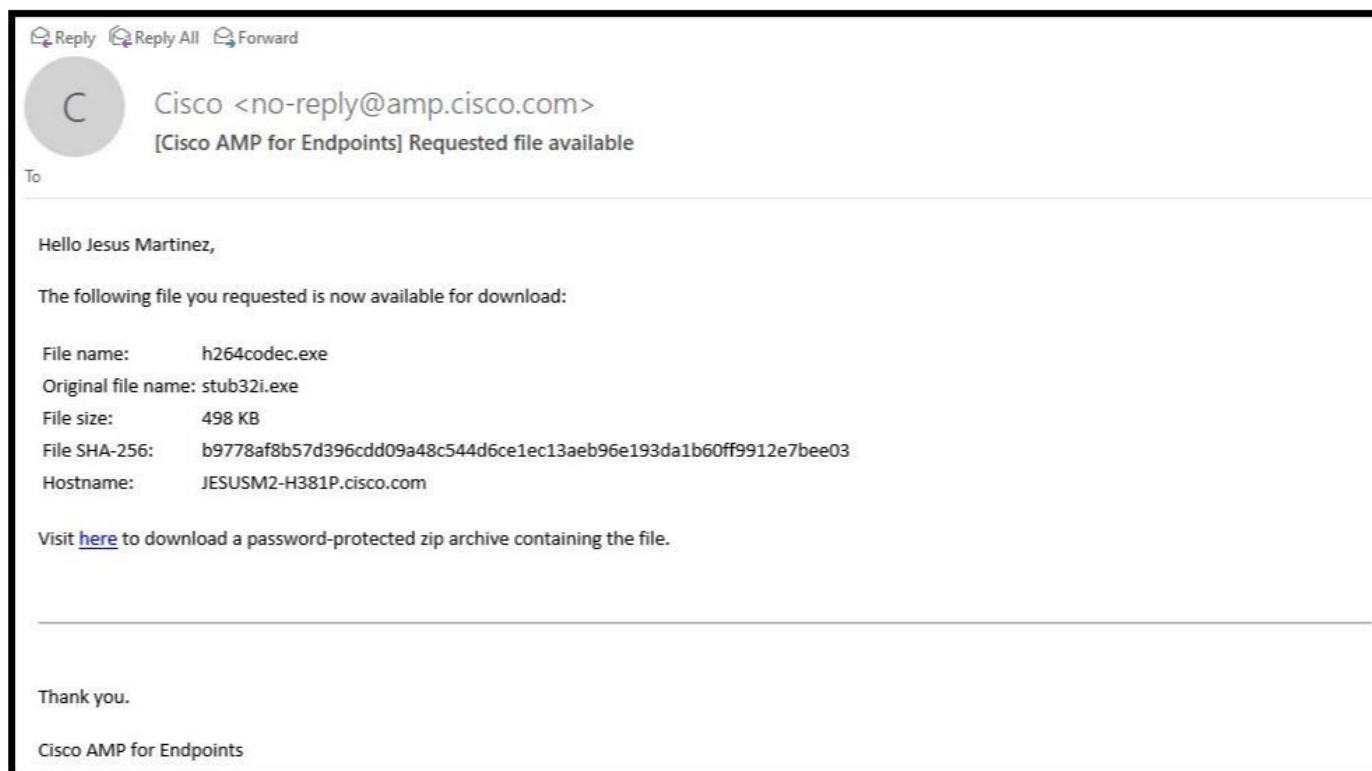
Étape 3. Sélectionnez le périphérique sur lequel le fichier a été détecté et cliquez sur **Récupérer** comme indiqué dans l'image (le périphérique doit être activé) comme indiqué dans l'image.



Étape 4. Vous recevez le message tel qu'il apparaît dans l'image.



Au bout de quelques minutes, vous recevez une notification par e-mail lorsque le fichier est disponible pour téléchargement, comme l'illustre l'image.



Étape 5. Accédez à **AMP Console > Analysis > File Repository** et sélectionnez le fichier, puis cliquez sur **Download** comme indiqué dans l'image.

[Connector Diagnostics Feature Overview](#)

Search by SHA-256 or file name...

Status

Group

Type

▼ **h264codec.exe is Available** Requested by **Jesus Martinez** 2020-04-16 03:37:42 CDT

Original File Name	stub32i.exe
Fingerprint (SHA-256)	b9778af8...2e7bee03
File Size	498 KB
Computer	JESUSM2-H381P.cisco.com

Étape 6. La boîte de notification s'affiche, cliquez sur **Télécharger**, comme illustré dans l'image, et le fichier est téléchargé sur un fichier ZIP.



Capture des événements d'alerte à partir de la console AMP

Étape 1. Accédez à **Console AMP > Tableau de bord > Événements**.

Étape 2. Sélectionnez l'**événement d'alerte** et prenez la capture comme indiqué dans l'image.

▼ JESUSM2-H381P.cisco.com detected stub32i.exe as Win.Trojan.Generic::61.sbx.vloc Medium 2020-04-09 10:47:44 CDT

File Detection	Detection	▼ Win.Trojan.Generic::61.sbx.vloc
Connector Info	Fingerprint (SHA-256)	▼ b9778af8...2e7bee03
Comments	File Name	▼ stub32i.exe
	File Path	C:\Users\jesusm2\Downloads\stub32i.exe
	File Size	498.49 KB
	Parent Fingerprint (SHA-256)	▼ 2fb898ba...7bf74fef
	Parent Filename	▼ 7zG.exe

Capture des détails de l'événement à partir de la console AMP

Étape 1. Accédez à **Console AMP > Tableau de bord > Événements**.

Étape 2. Sélectionnez l'événement d'alerte et cliquez sur l'option **Trajectoire du périphérique** comme indiqué dans l'image.



File Detection	Detection	Win.Trojan.Generic:61.sbx.vioc
Connector Info	Fingerprint (SHA-256)	b9778af8...2e7bee03
Comments	File Name	stub32i.exe
	File Path	C:\Users\jesusm2\Downloads\stub32i.exe
	File Size	498.49 KB
	Parent Fingerprint (SHA-256)	2fb898ba...7bf74fef
	Parent Filename	7zG.exe

[Analyze](#) [Restore File](#) [All Computers](#) [View Upload Status](#) [Add to Allowed Applications](#) [File Trajectory](#)

Il redirige vers les détails de la trajectoire du périphérique comme indiqué dans l'image.

Device Trajectory

JESUSM2-H381P:cisco.com in group jesusm2 - Oscar Group

2 compromise events (spanning less than a ...)

Filters Search Device Trajectory

Event Details

2020-04-09 10:47:43 CDT

Detected **stub32i.exe**, n264codeic.4.1.0.0 (b9778af8...2e7bee03) [PE_Executable] as Win.Trojan.Generic:61.sbx.vioc.

Created by 7zG.exe, 7-Zip 19.00.0 (2fb898ba...7bf74fef) [Unknown] executing as.

The file was quarantined.

Process disposition benign.

File full path: C:\Users\jesusm2\Downloads\stub32i.exe

File SHA-1: 6e05e270e4136e44871b39e3e15e2137225

File MD5: ff4325a74006a686e37887e0d11102

File size: 510450 bytes.

Parent file SHA-1: af22812647d804d515688eae490349882505a

Parent file MD5: 6463ae79568bc333125972e907298

Parent file size: 581632 bytes.

Parent file age: 0 seconds.

Parent process id: 24064.

Detected by the SHA engines.

Étape 3. Prenez une capture de la zone **Détails de l'événement** comme illustré dans l'image.

Event Details ✕

Medium

2020-04-09 10:47:43 CDT

Detected **stub32i.exe**, h264codec 4.1.0.0 (b9778af8...2e7bee03)
[PE_Executable] as **Win.Trojan.Generic::61.sbx.vioc**.

Created by **7zG.exe**, 7-Zip 19.0.0.0 (2fb898ba...7bf74fef)
[Unknown] executing as .

The file was **quarantined**.

Process disposition Benign.

File full path: C:\Users\jesusm2\Downloads\stub32i.exe

File SHA-1: 6e055a270bdc13dcaa4871b39fac3d15a2137225.

File MD5: f74325a740d0a9cf68e37887ce017102.

File size: 510450 bytes.

Parent file SHA-1: df22612647e9404a515d48ebad490349685250de.


Parent file MD5: 04fb3ae7f05c8bc333125972ba907398.

Parent file size: 581632 bytes.

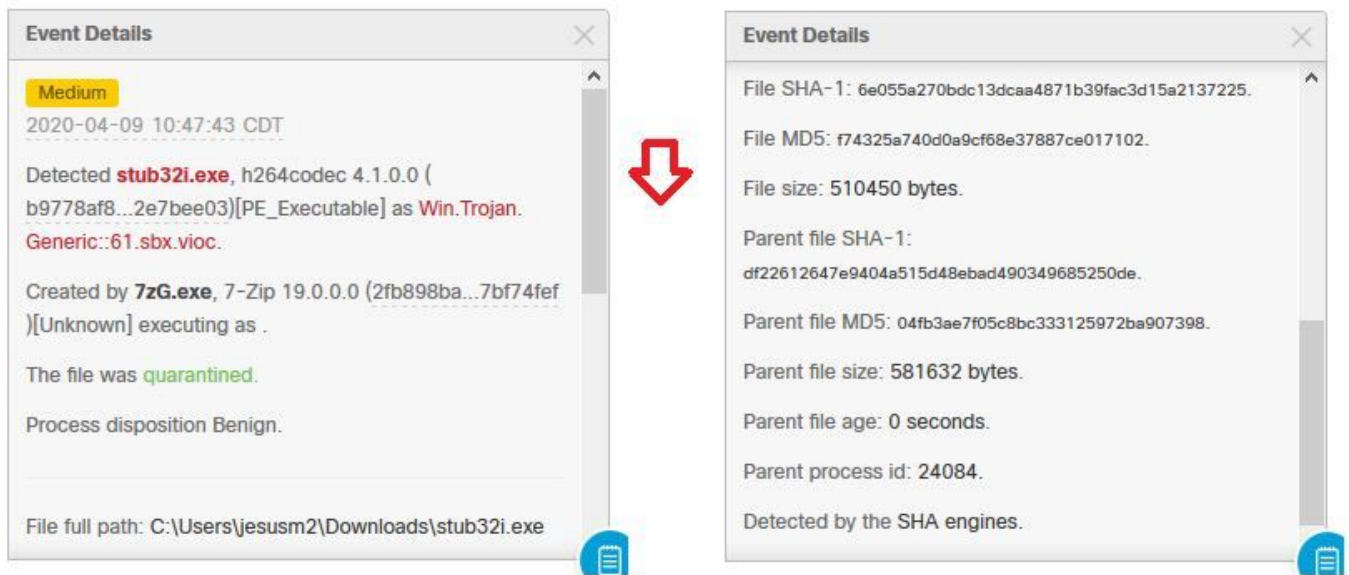
Parent file age: 0 seconds.

Parent process id: 24084.

Detected by the SHA engines.



Étape 4. Si nécessaire, faites défiler la page vers le bas et prenez quelques captures pour obtenir toutes les informations **Détails des événements** comme indiqué dans l'image.



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 de fichier et expliquez la fonction de fichier.

Explication

- Pourquoi pensez-vous que le processus de fichier peut être un faux positif ?
- Partagez les raisons de votre confiance dans le fichier.

Fournir des informations

- Une fois que vous avez recueilli tous les détails, téléchargez toutes les informations demandées à <https://cway.cisco.com/csc/>.
- Assurez-vous de référencer le numéro de demande de service.

Conclusion

Cisco s'efforce toujours d'améliorer et d'étendre l'intelligence des menaces pour la technologie AMP for Endpoints. Toutefois, si votre solution AMP for Endpoints déclenche une alerte par erreur, vous pouvez prendre certaines mesures afin d'éviter tout autre impact sur votre environnement. Ce document fournit des directives pour obtenir tous les détails nécessaires pour ouvrir un dossier auprès du TAC Cisco en ce qui concerne un problème de faux positif. En fonction de l'analyse des fichiers de l'équipe de diagnostic, la disposition des fichiers peut être modifiée pour arrêter les événements d'alerte déclenchés sur AMP Console ou le TAC Cisco peut fournir la correction appropriée pour permettre l'exécution du fichier/processus sans problème dans votre environnement.