Comment envoyer un fichier dans Threat Grid à partir du portail AMP for Endpoints ?

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Components Used](#)
[Informations générales](#)
[Comment envoyer un fichier dans Threat Grid à partir du portail AMP for Endpoints ?](#)
[Vérification](#)
[Dépannage](#)
[Informations connexes](#)

Introduction

Ce document décrit le processus d'envoi d'échantillons au nuage Threat Grid (TG) à partir du portail Advanced Malware Protection (AMP) for Endpoints.

Contribution de Yeraldin Sánchez, ingénieur du TAC Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco AMP pour terminaux
- Cloud TG

Components Used

Les informations de ce document sont basées sur la console Cisco AMP for Endpoints version 5.4.20190709.

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

Voici les conditions requises pour le scénario décrit dans ce document :

- Accès au portail Cisco AMP for Endpoints
- Taille de fichier maximale de 20 Mo
- Moins de 100 envois par jour

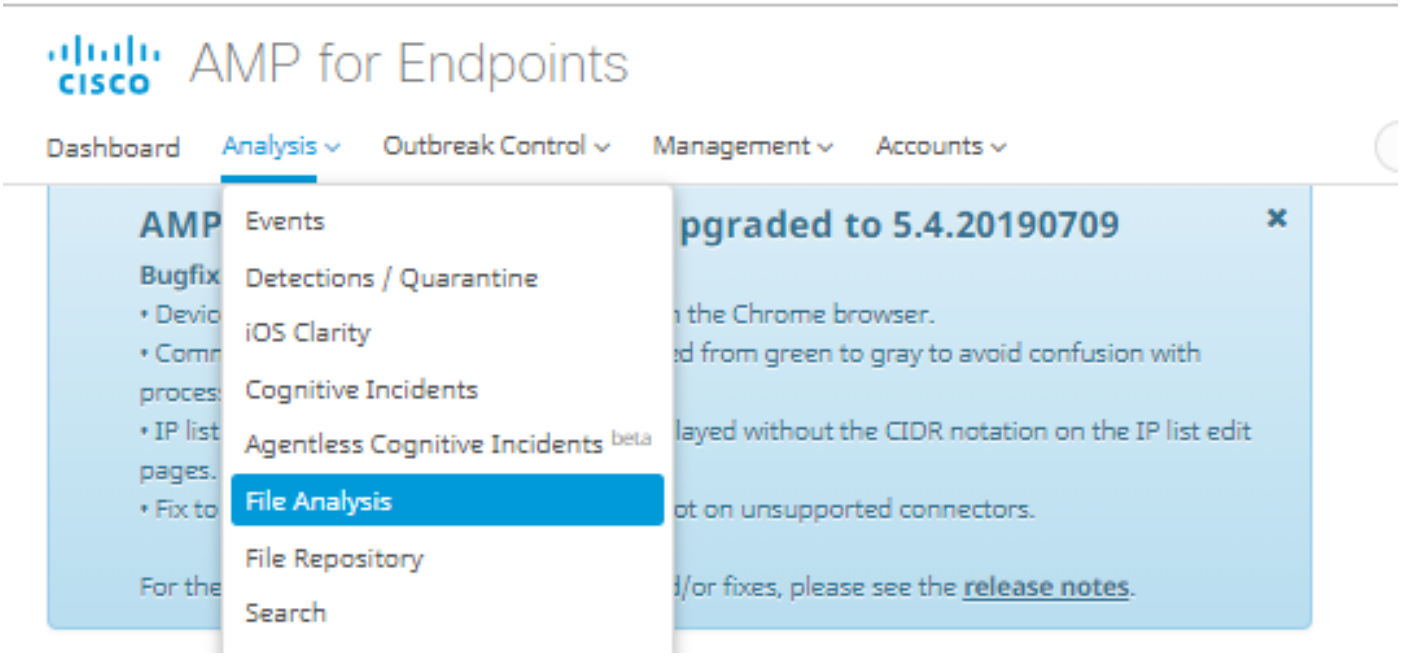
Limites de l'analyse des fichiers :

- Les noms de fichiers sont limités à 59 caractères Unicode.
- Les fichiers ne peuvent pas être inférieurs à 16 octets ou supérieurs à 20 Mo
- Types de fichiers pris en charge : **.exe, .dll, .jar, .swf, .pdf, .rtf, .doc(x), .xls(x), .ppt(x), .zip, .vbn et .sep**

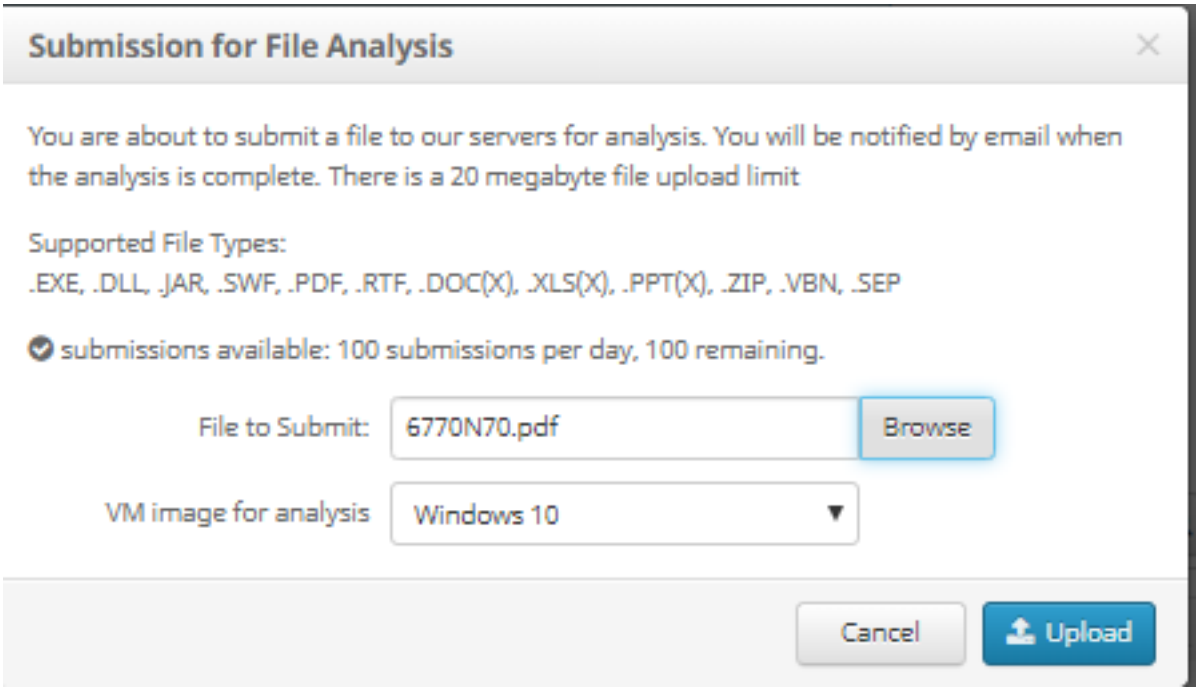
Comment envoyer un fichier dans Threat Grid à partir du portail AMP for Endpoints ?

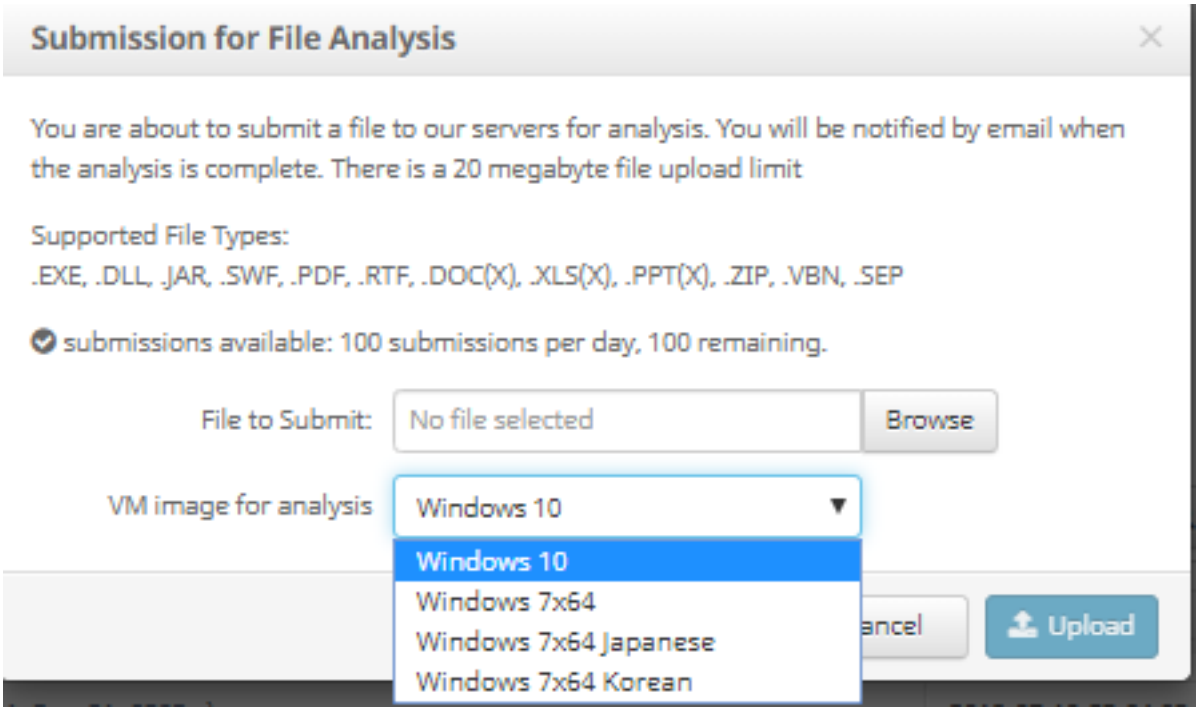
Voici les étapes à suivre pour soumettre un exemple au cloud TG à partir du portail AMP.

Étape 1. Sur le portail AMP, accédez à **Analysis > File Analysis**, comme illustré dans l'image.



Étape 2. Sélectionnez le fichier et la version de l'image Windows que vous souhaitez envoyer pour analyse, comme indiqué dans les images.

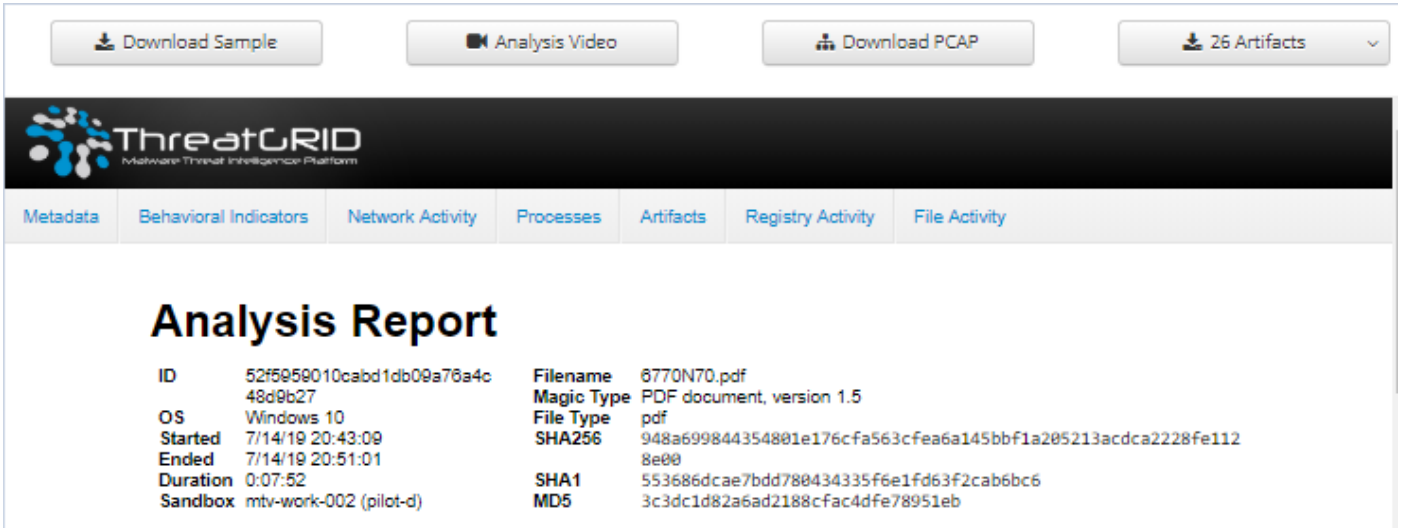




Étape 3. Une fois l'échantillon téléchargé, l'analyse prend environ 30 à 60 minutes pour se terminer, cela dépend de la charge du système, une fois ce processus terminé, une notification par e-mail est envoyée à votre e-mail.

Étape 4. Une fois l'analyse de fichier terminée, cliquez sur le bouton **Rapport** pour obtenir des informations détaillées sur le score de menace, comme le montrent les images.

6770N70.pdf (948a6998...e1128e00)		2019-07-14 20:43:04 UTC	Report 56
Fingerprint (SHA-256)	948a6998...e1128e00		
File name	6770N70.pdf		
Threat Score	56		
Behavioral Indicators	Name	Score	
	pdf-uri-action	56	
	pdf-contains-uris	25	



Pour plus d'informations, vous pouvez trouver des options supplémentaires pour l'analyse de fichiers :

Télécharger l'exemple : Cette option vous permet de télécharger l'exemple.

Vidéo d'analyse : Cette option vous fournit l'exemple de vidéo obtenu lors de l'analyse.

Télécharger PCAP : Cette option vous fournit une analyse de connectivité réseau.

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

> **Avertissement :** Les fichiers téléchargés à partir de l'analyse des fichiers sont souvent des programmes malveillants en direct et doivent être traités avec une extrême prudence.

> **Note**: L'analyse d'un fichier spécifique est divisée en plusieurs sections. Certaines sections ne peuvent pas être disponibles pour tous les types de fichiers.

Informations connexes

- Cisco AMP for Endpoints - Guide de l'utilisateur
- Support et documentation techniques - Cisco Systems