Envoyer un fichier à Threat Grid à partir du portail AMP for Endpoints

Table des matières

Introduction

Problème

Environnement

- Limites de l'analyse de fichier

Résolution

Introduction

Ce document décrit la procédure à suivre pour envoyer des exemples au cloud Threat Grid (TG) à partir du portail Advanced Malware Protection (AMP) for Endpoints.

Problème

Envoyez un fichier du portail AMP for Endpoints au cloud Threat Grid pour analyse.

Environnement

Les connaissances requises incluent :

- Cisco AMP pour les terminaux
- Cloud Threat Grid

Version du produit mentionnée dans ce document : Console Cisco AMP for Endpoints version 5.4.20190709.

Voici les conditions et les limites du scénario décrit dans ce document :

- Accès au portail Cisco AMP for Endpoints
- Taille de fichier inférieure à 20 Mo
- Moins de 100 soumissions par jour

Limites de l'analyse de fichier

- Les noms de fichiers sont limités à 59 caractères Unicode.
- Les fichiers ne peuvent pas avoir une taille inférieure à 16 octets ou supérieure 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

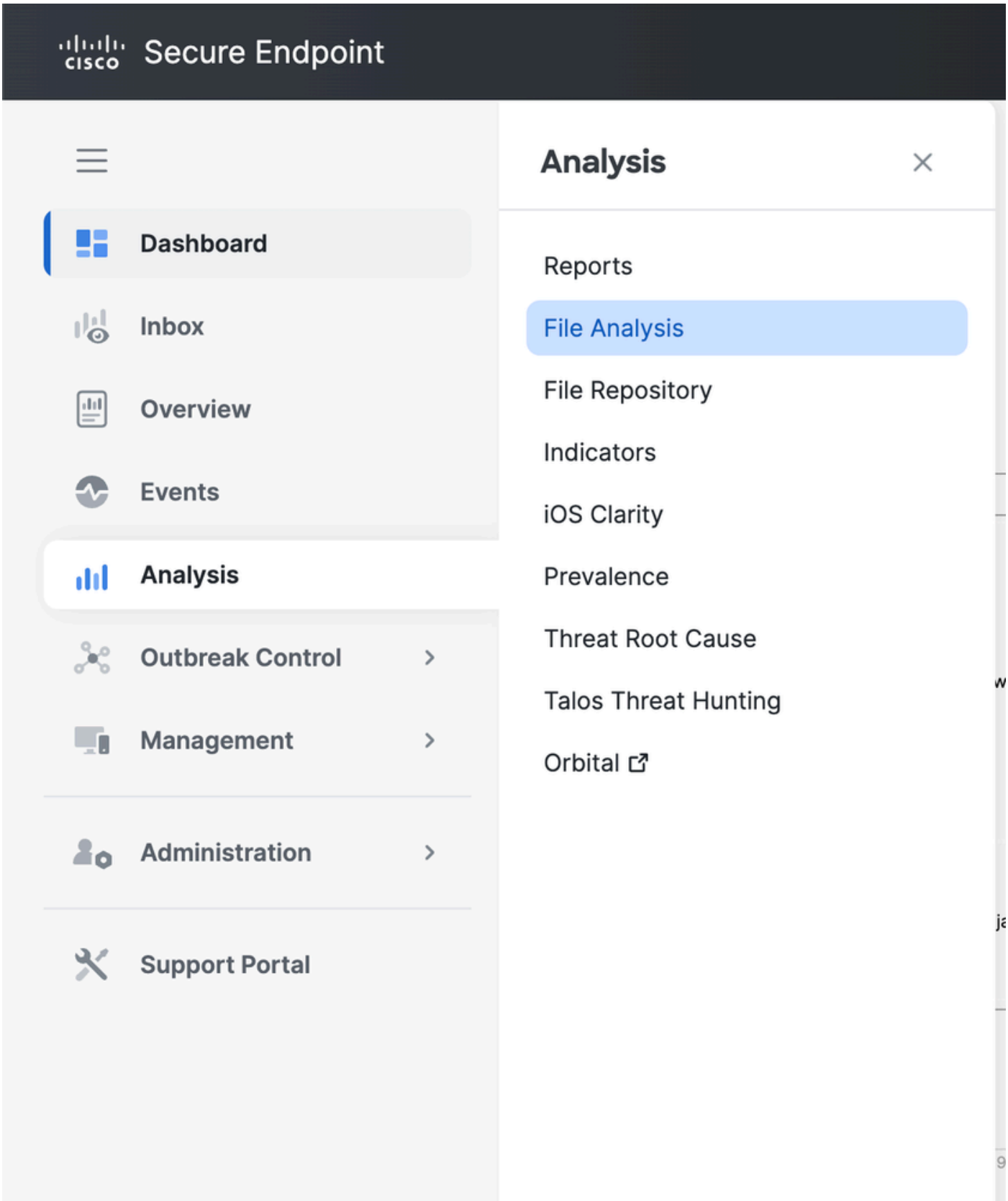
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Résolution

1. Vérifiez que vous pouvez vous connecter au portail Cisco AMP for Endpoints.

2. Vérifiez que l'échantillon respecte les limites d'analyse de fichier (taille du fichier, type de fichier pris en charge et limite de soumission quotidienne).

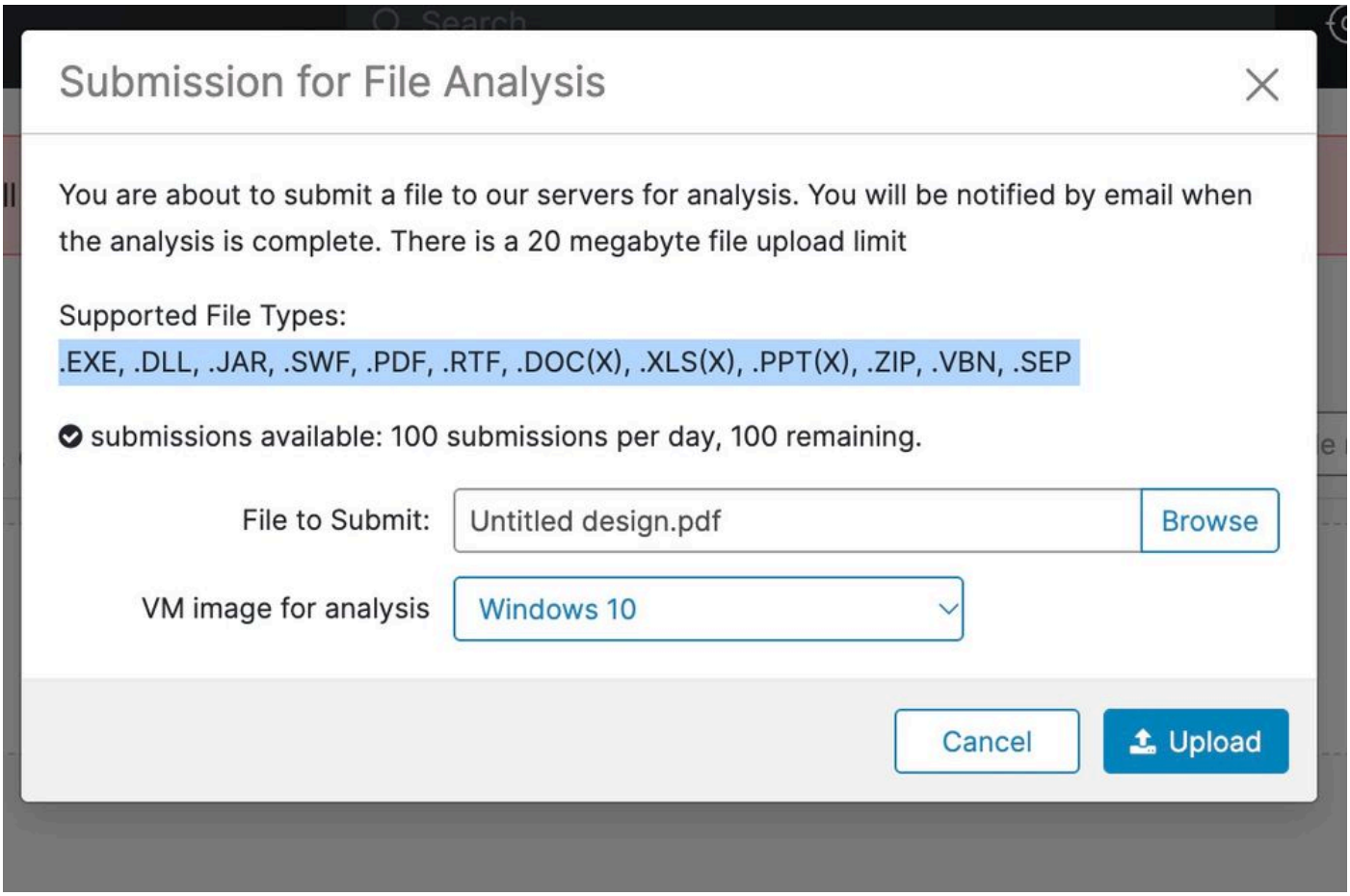
3. Dans le portail AMP, accédez à Analysis > File Analysis.



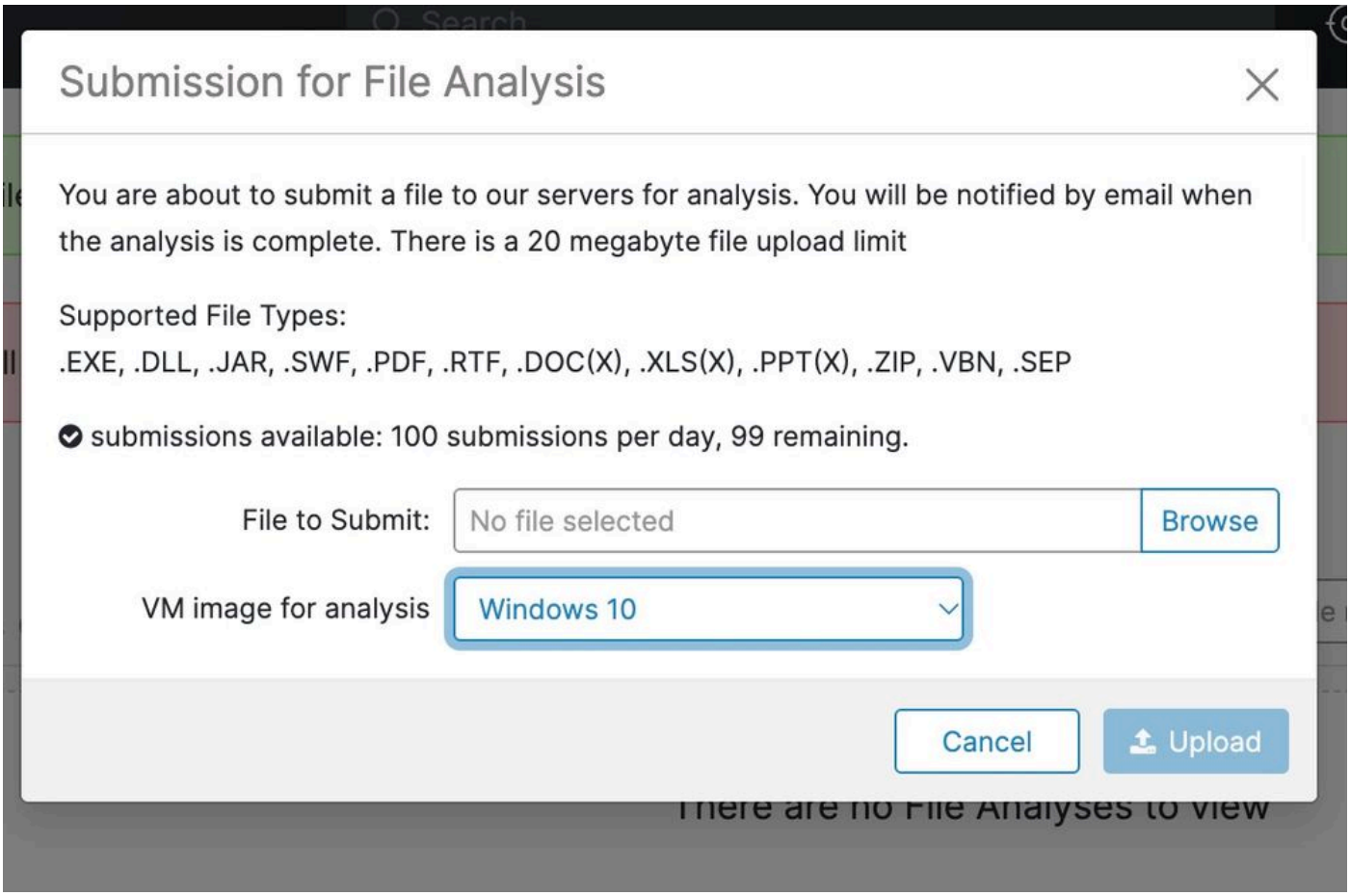
Analyse de fichiers AMP page.png

4. Cliquez sur Choisir un fichier (ou le contrôle de téléchargement), puis choisissez le fichier à soumettre.

5. Sélectionnez la version de l'image système Windows à utiliser pour l'analyse.



Envoyer le fichier.jpeg



Envoyer le fichier 2.jpeg

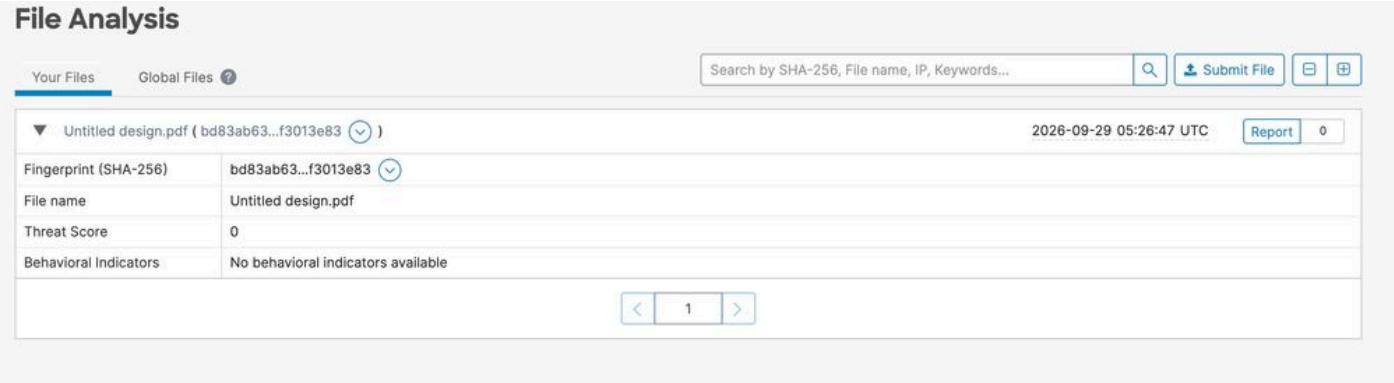
6. Attendez la fin de l'analyse. L'analyse prend généralement entre 30 et 60 minutes.

Remarque : La durée dépend de la charge du système.

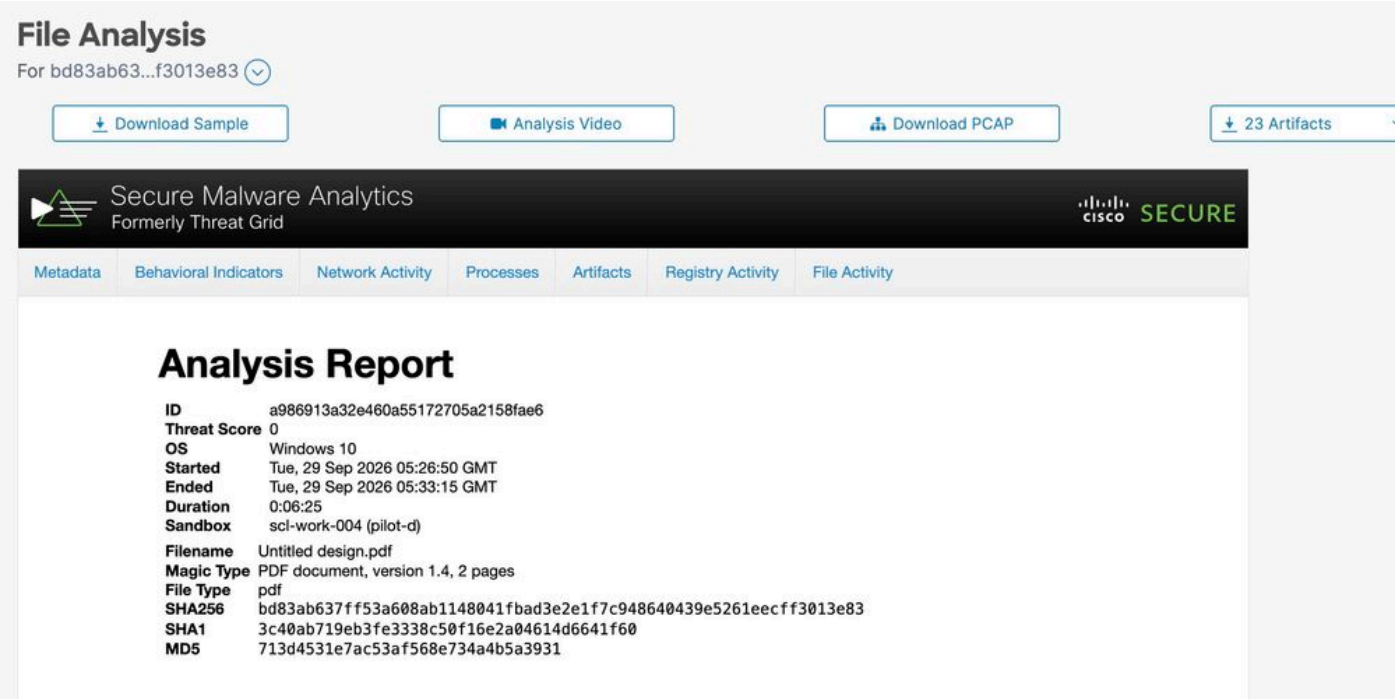
---

7. Confirmez que la notification par e-mail est reçue une fois l'analyse terminée.

8. Lorsque l'analyse de fichier est prête, cliquez sur Rapport pour afficher les détails du score de menace.



Prêt pour le fichier.jpeg



Report.jpeg

Les artefacts facultatifs (le cas échéant) sont :

- Télécharger l'exemple : Télécharge l'échantillon envoyé.
- Vidéo d'analyse : Cette option fournit l'exemple de vidéo généré pendant l'analyse.
- Télécharger PCAP : Télécharge une capture de paquets à partir de l’analyse.

Résultat attendu : L'état de l'analyse passe à Terminé et la vue Rapport s'ouvre avec les détails du score de menace et tous les artefacts disponibles.

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

 Remarque : L'analyse d'un fichier spécifique est divisée en plusieurs sections. Certaines sections ne sont peut-être pas disponibles pour tous les types de fichiers.

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.