Hoe moet u een bestand in Threat Grid vanuit het AMP for Endpoints Portal indienen?

Inhoud

Inleiding

Dit document beschrijft het proces voor het verzenden van monsters naar de Threat Grid-cloud (TG) van de Advanced Malware Protection (AMP) voor Endpoints.

Bijgedragen door Yeraldin Sánchez, Cisco TAC Engineer.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Advanced Malware Protection voor endpoints
- TG Cloud

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Advanced Malware Protection voor endpoints, versie 5.4.2019.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

Dit zijn de eisen voor het scenario dat in dit document wordt beschreven:

- Toegang tot de Cisco Advanced Malware Protection voor endpoints
- Bestandsgrootte maximaal 20 MB
- Minder dan 100 inzendingen per dag

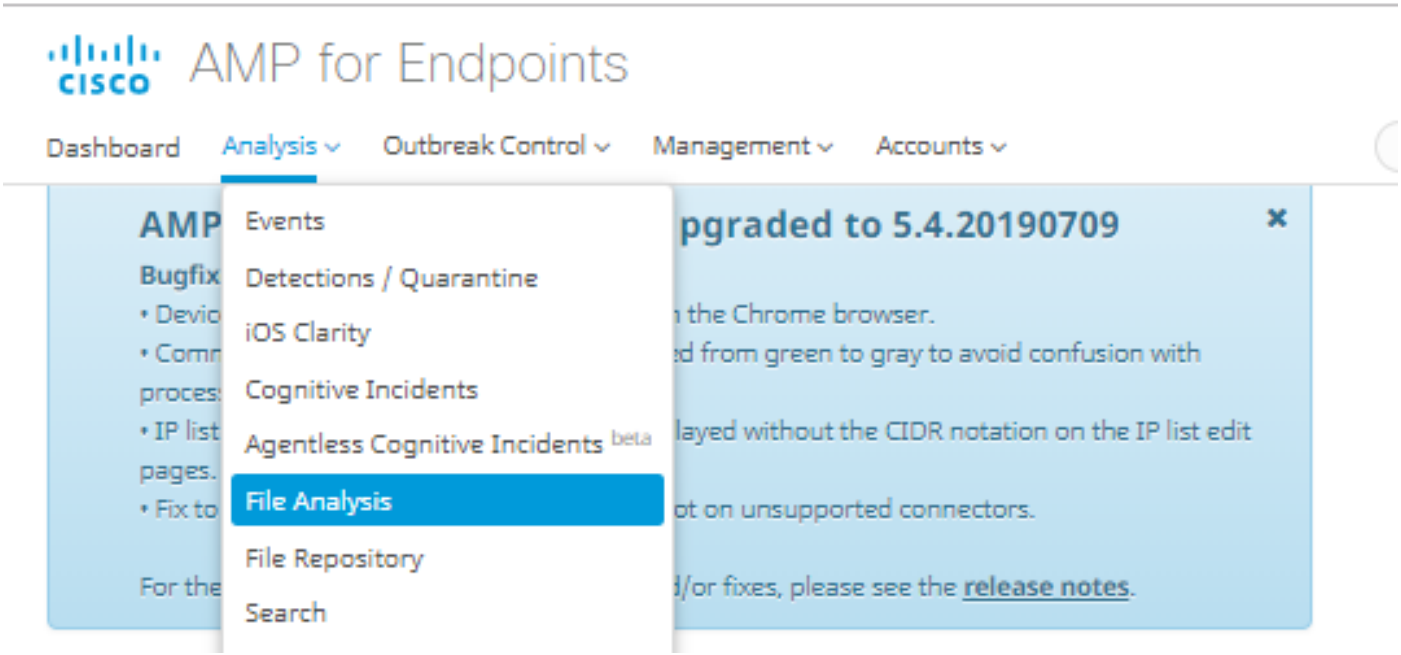
Beperkingen voor bestandsanalyse:

- Bestandsnaam is beperkt tot 59 Unicode-tekens.
- Bestanden mogen niet kleiner zijn dan 16 bytes of groter dan 20 MB
- Ondersteunde bestandstypen: **.exe, .dll, .jar, .swf, .pdf, .rtf, .doc(x), .xls(x), .ppt(x), .zip, .vbn en .sep**

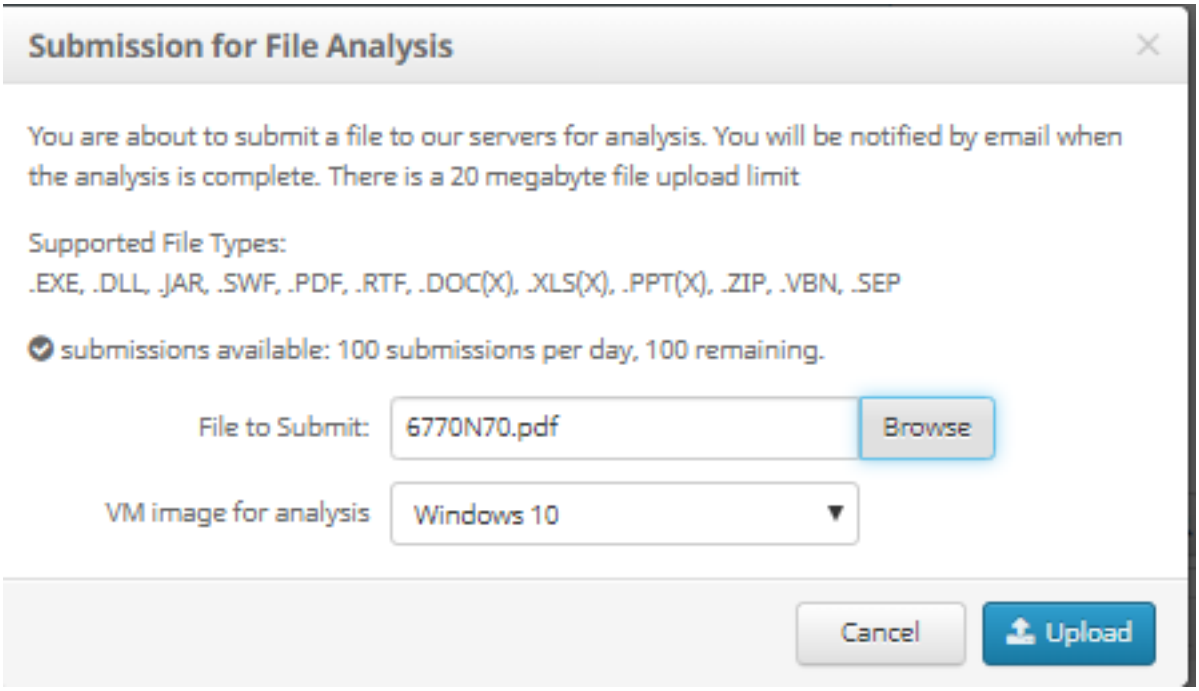
Hoe moet u een bestand in Threat Grid vanuit het AMP for Endpoints Portal indienen?

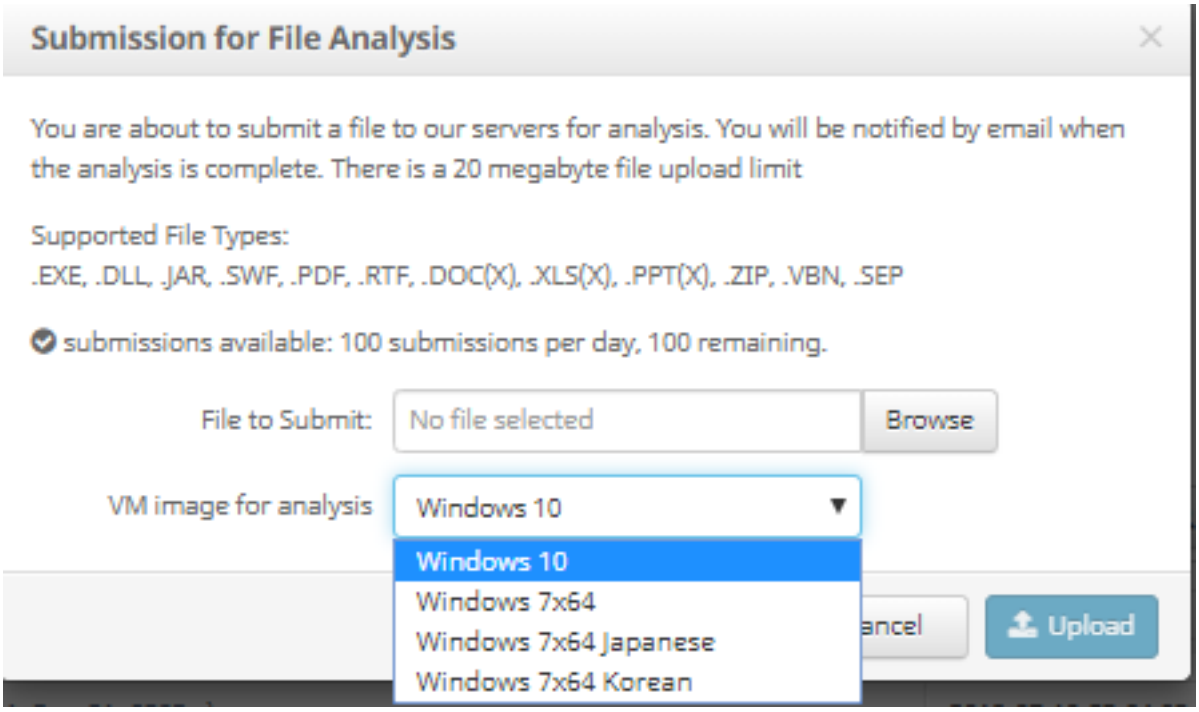
Hier volgen de stappen om een monster aan de TG-cloud van het AMP Portal te sturen.

Stap 1. Ga op het AMP-portal naar **Analyse > Bestandsanalyse**, zoals in de afbeelding.



Stap 2. Selecteer het bestand en de Windows-afbeeldingsversie die u voor analyse wilt verzenden, zoals in de afbeeldingen.

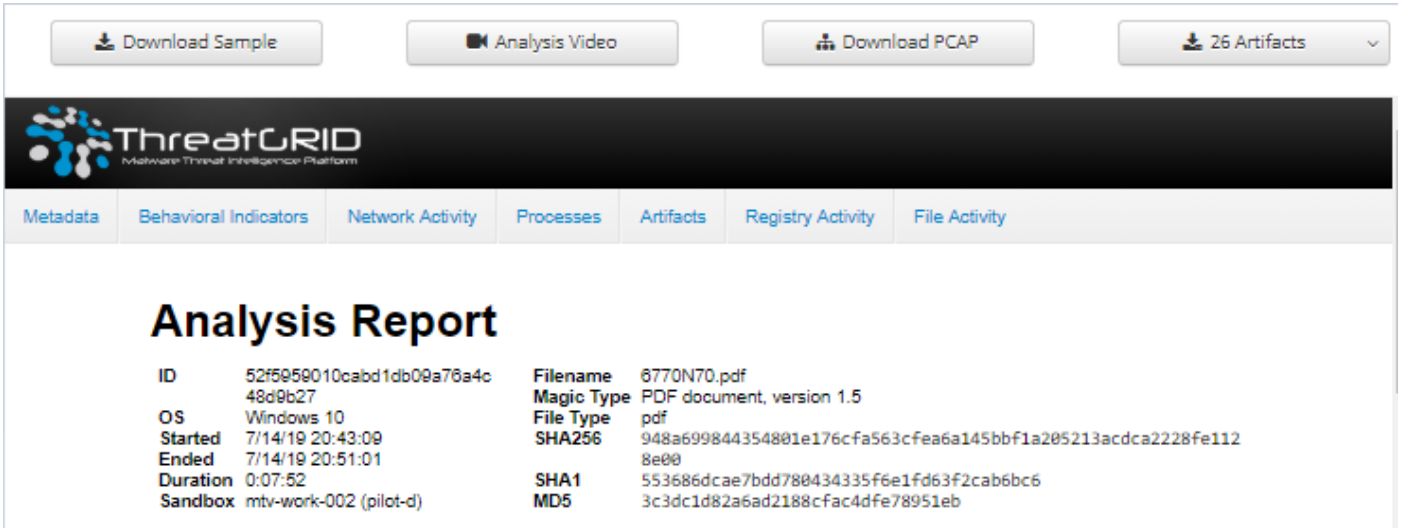




Stap 3. Zodra de steekproef is geüpload, duurt de analyse ongeveer 30 tot 60 minuten om te voltooien, afhankelijk van de systeemlading. Nadat dit proces is voltooid, wordt er een e-mailbericht naar uw e-mail verzonden.

Stap 4. Wanneer de bestandsanalyse klaar is, klikt u op de knop **Rapport** om gedetailleerde informatie te hebben over de verkregen Threat Score, zoals in de afbeeldingen wordt weergegeven.

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	



Meer informatie op de website zijn er ook opties voor de bestandsanalyse:

Monster downloaden: Met deze optie kunt u de steekproef downloaden.

Video analyse: Deze optie biedt de voorbeeldvideo die op de analyse is verkregen.

DownloadPCAP: Deze optie biedt u een analyse van de netwerkconnectiviteit.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

> **Waarschuwing**: Bestanden die zijn gedownload van de bestandsindeling worden vaak onderhandeld en moeten met uiterste voorzichtigheid worden behandeld.

> Opmerking: De analyse van een specifiek bestand wordt in verschillende delen opgesplitst. Sommige delen kunnen niet voor alle bestandstypen beschikbaar zijn.

Gerelateerde informatie

- Cisco Advanced Malware Protection voor endpoints - gebruikershandleiding
- Technische ondersteuning en documentatie – Cisco Systems