Wie wird eine Datei in Threat Grid vom AMP für Endgeräte-Portal gesendet?

Inhalt

[Einführung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Hintergrundinformationen](#)
[Wie wird eine Datei in Threat Grid vom AMP für Endgeräte-Portal gesendet?](#)
[Überprüfen](#)
[Fehlerbehebung](#)
[Zugehörige Informationen](#)

Einführung

Dieses Dokument beschreibt den Prozess zum Einsenden von Stichproben an die Threat Grid (TG) Cloud über das Advanced Malware Protection (AMP) for Endpoints-Portal.

Mitarbeiter: Yeraldin Sánchez, Cisco TAC Engineer.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco AMP für Endgeräte
- TG Cloud

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco AMP für Endgeräte Konsolenversion 5.4.20190709.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Dies sind die Anforderungen für das in diesem Dokument beschriebene Szenario:

- Zugriff auf das Cisco AMP für Endgeräte-Portal
- Dateigröße nicht mehr als 20 MB
- Weniger als 100 eingereichte Dateien pro Tag

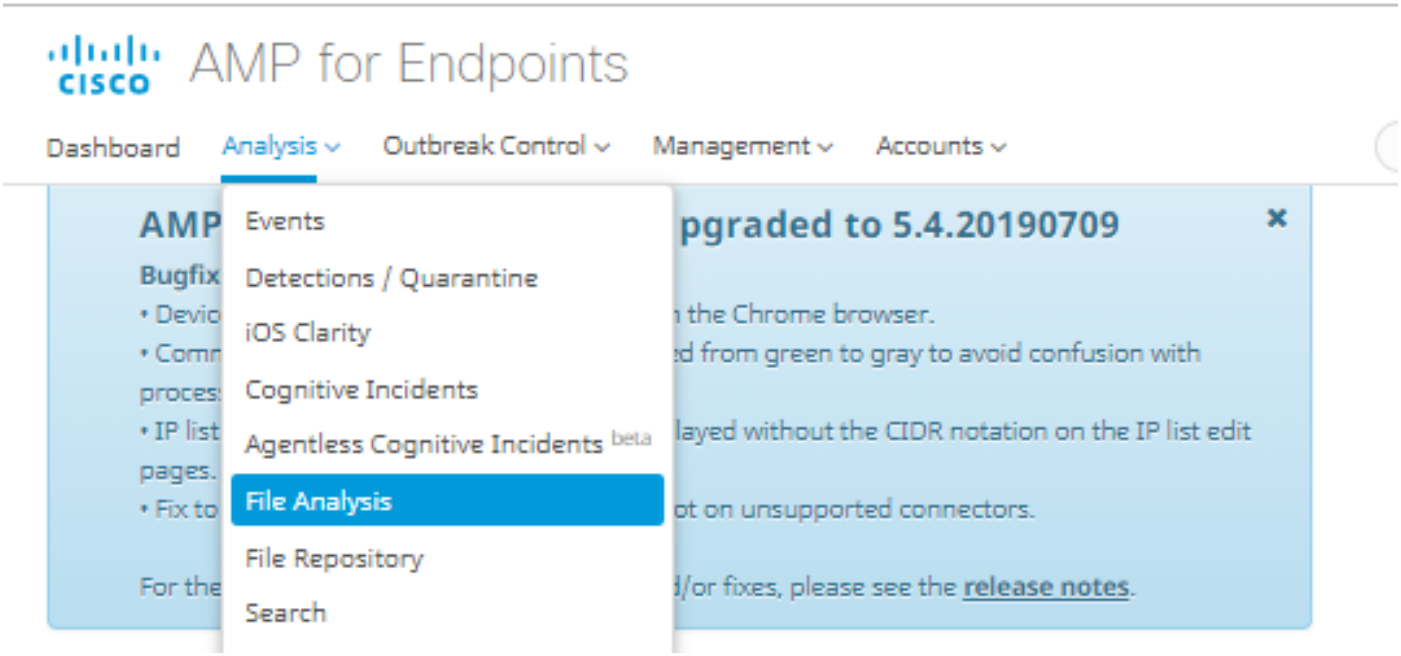
Dateianalyseeinschränkungen:

- Dateinamen sind auf 59 Unicode-Zeichen beschränkt.
- Dateien dürfen nicht kleiner als 16 Byte oder größer als 20 MB sein.
- Unterstützte Dateitypen: **.exe, .dll, .jar, .swf, .pdf, .rtf, .doc(x), .xls(x), .ppt(x), .zip, .vbn und .sep**

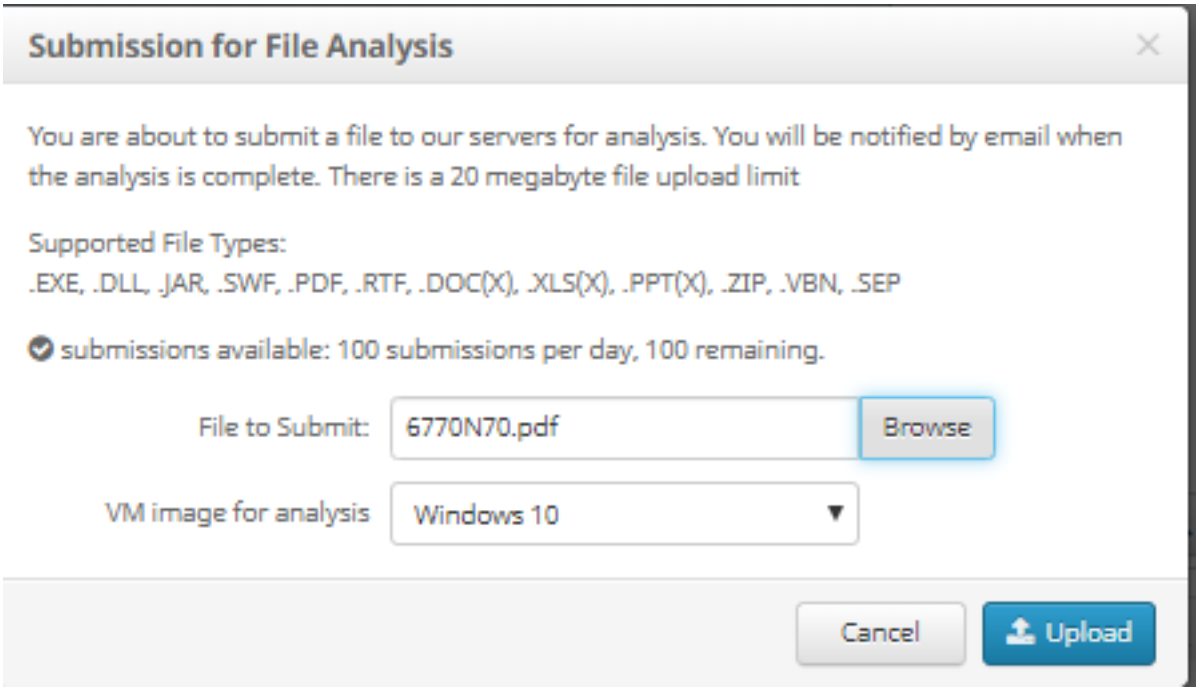
Wie wird eine Datei in Threat Grid vom AMP für Endgeräte-Portal gesendet?

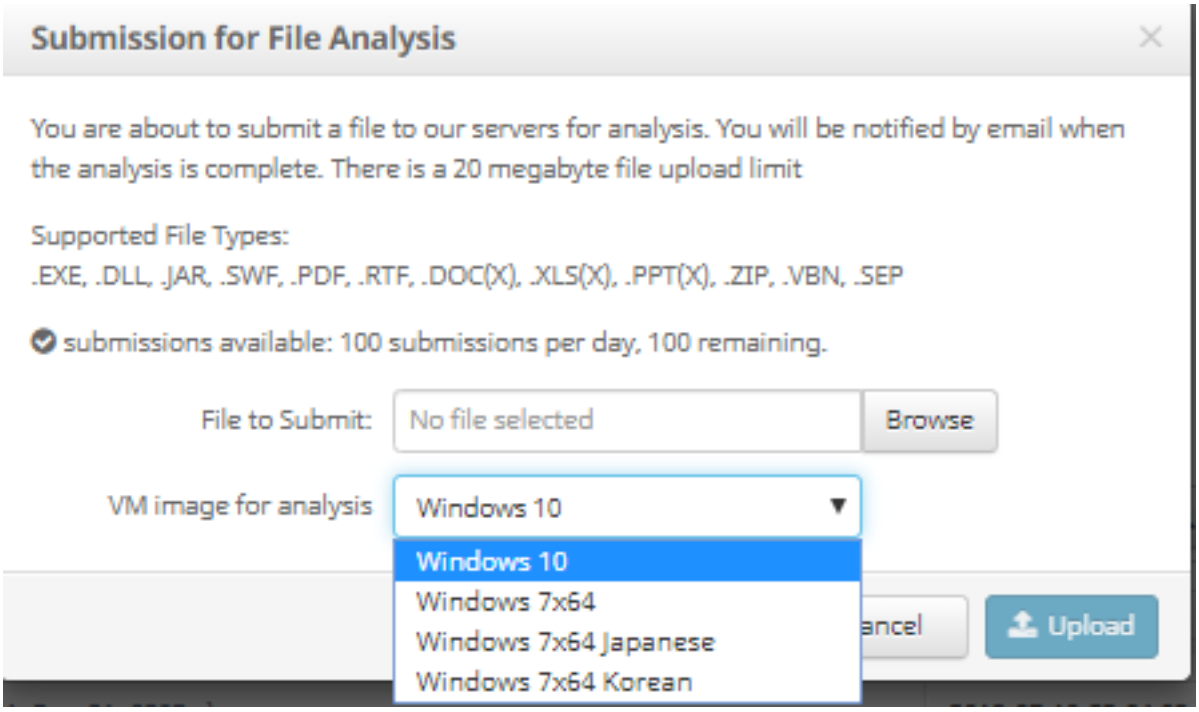
Im Folgenden finden Sie die erforderlichen Schritte, um ein Beispiel vom AMP-Portal an die TG-Cloud zu senden.

Schritt 1: Navigieren Sie im AMP-Portal zu **Analyse > Dateianalyse**, wie im Bild gezeigt.



Schritt 2: Wählen Sie die Datei- und Windows-Image-Version aus, die Sie zur Analyse senden möchten, wie in den Bildern gezeigt.

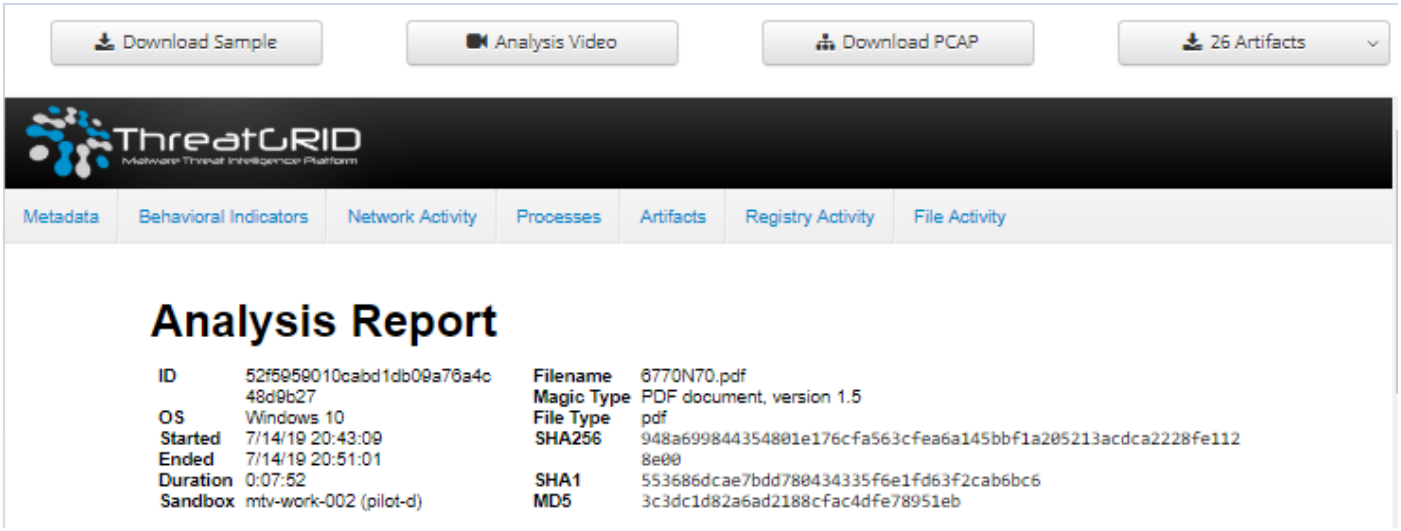




Schritt 3: Nach dem Hochladen des Beispiels dauert die Analyse ca. 30 bis 60 Minuten. Sie hängt vom System ab. Nach Abschluss dieses Vorgangs wird eine E-Mail-Benachrichtigung an Ihre E-Mail gesendet.

Schritt 4: Wenn die Dateianalyse abgeschlossen ist, klicken Sie auf die Schaltfläche **Report** (**Bericht**), um detaillierte Informationen zur erhaltenen Bedrohungsbewertung zu erhalten, wie in den Bildern gezeigt.

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	



Um weitere Informationen zu erhalten, können Sie weitere Optionen für die Dateianalyse finden:

Beispiel herunterladen: Mit dieser Option können Sie das Beispiel herunterladen.

Analyse-Video: Mit dieser Option erhalten Sie das in der Analyse erhaltene Beispielvideo.

PCAP herunterladen: Diese Option bietet eine Analyse der Netzwerkverbindungen.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

> **Warnung**: Dateien, die von der Dateianalyse heruntergeladen werden, sind häufig Live-Malware und müssen mit äußerster Vorsicht behandelt werden.

> **Hinweis**: Die Analyse einer bestimmten Datei ist in mehrere Abschnitte unterteilt. Einige Abschnitte können nicht für alle Dateitypen verfügbar sein.

Zugehörige Informationen

- Cisco AMP für Endgeräte - Benutzerhandbuch
- Technischer Support und Dokumentation - Cisco Systems