AMP for EndpointsポータルからThreat Gridのファイルを送信する方法

内容

概要

このドキュメントでは、Advance Malware Protection(AMP)for EndpointsポータルからThreat Grid(TG)クラウドにサンプルを送信するプロセスについて説明します。

著者：Cisco TACエンジニア、Yeraldin Sanchez

前提条件

要件

次の項目に関する知識があることが推奨されます。

- エンドポイント向けCisco AMP
- TGクラウド

使用するコンポーネント

このドキュメントの情報は、Cisco AMP for Endpointsコンソールバージョン5.4.20190709に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

このドキュメントで説明するシナリオの要件は次のとおりです。

- Cisco AMP for Endpointsポータルへのアクセス
- ファイルサイズは20 MB以下
- 1日あたり100件未満の提出物

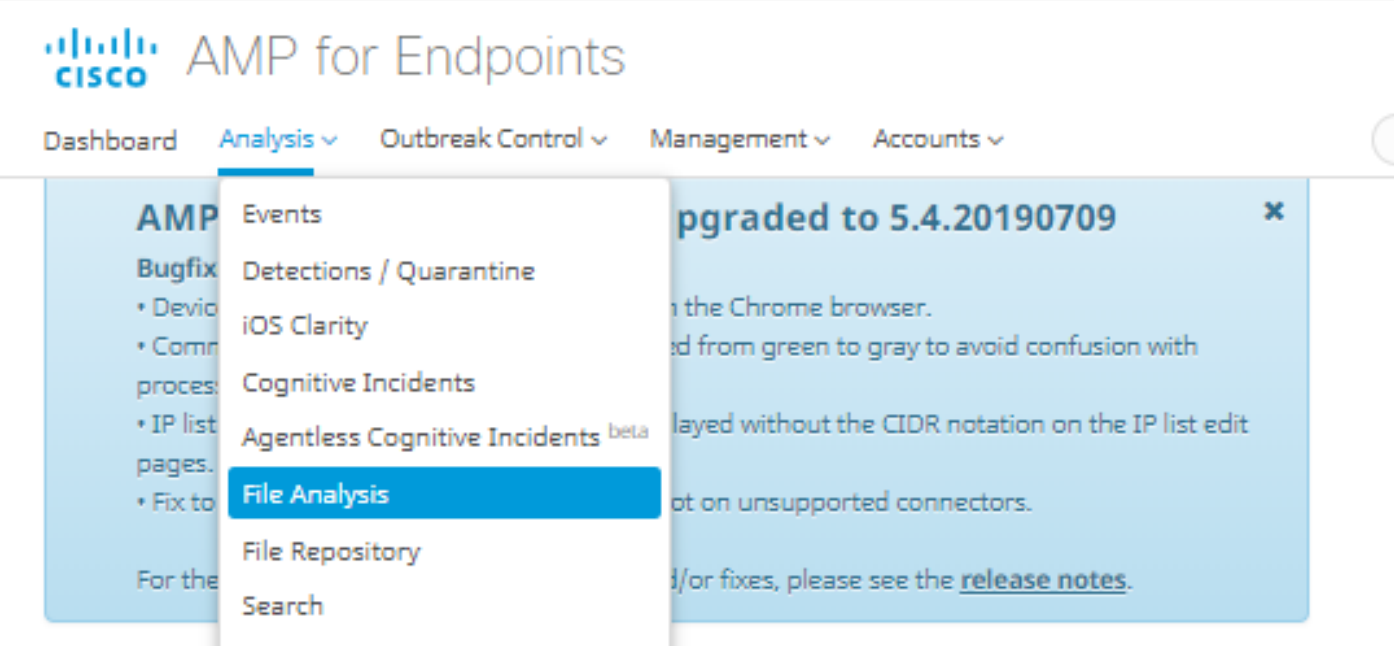
ファイル分析の制限事項：

- ファイル名は59文字のUnicode文字に制限されています。
- ファイルは16バイト以下または20 MBを超えることはできません
- サポートされるファイルの種類：**.exe、.dll、.jar、.swf、.pdf、.rtf、.doc(x)、.xls(x)、.ppt(x)、.zip、.vbnおよび.sep**

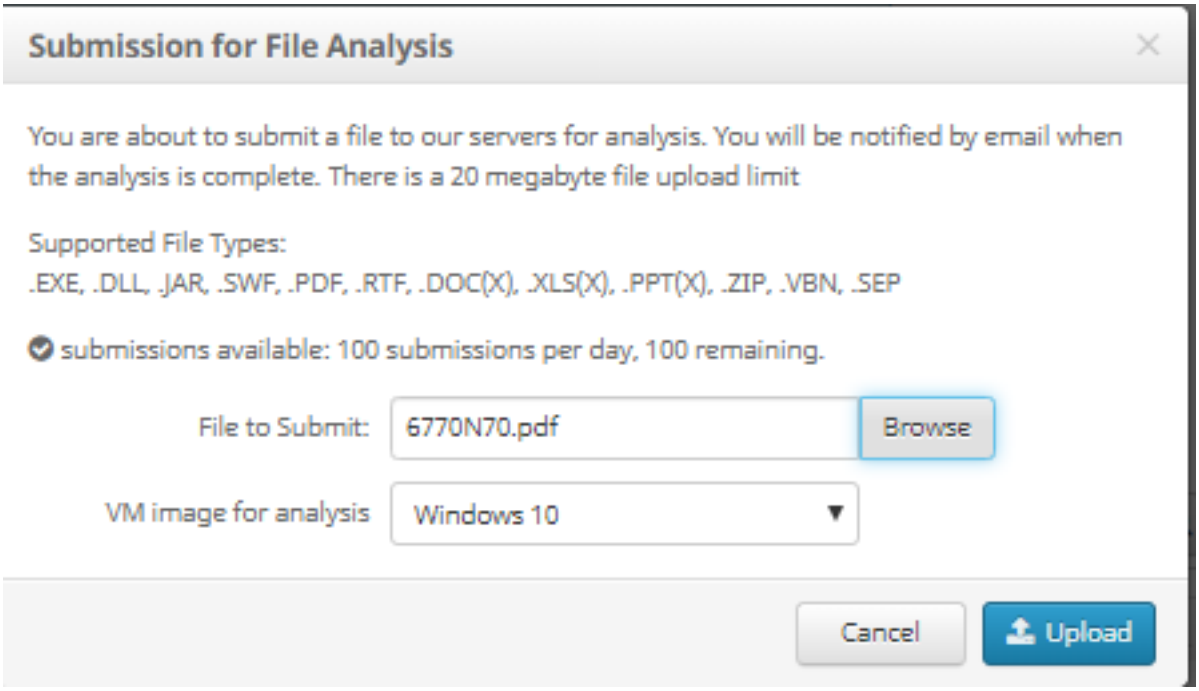
AMP for EndpointsポータルからThreat Gridのファイルを送信する方法

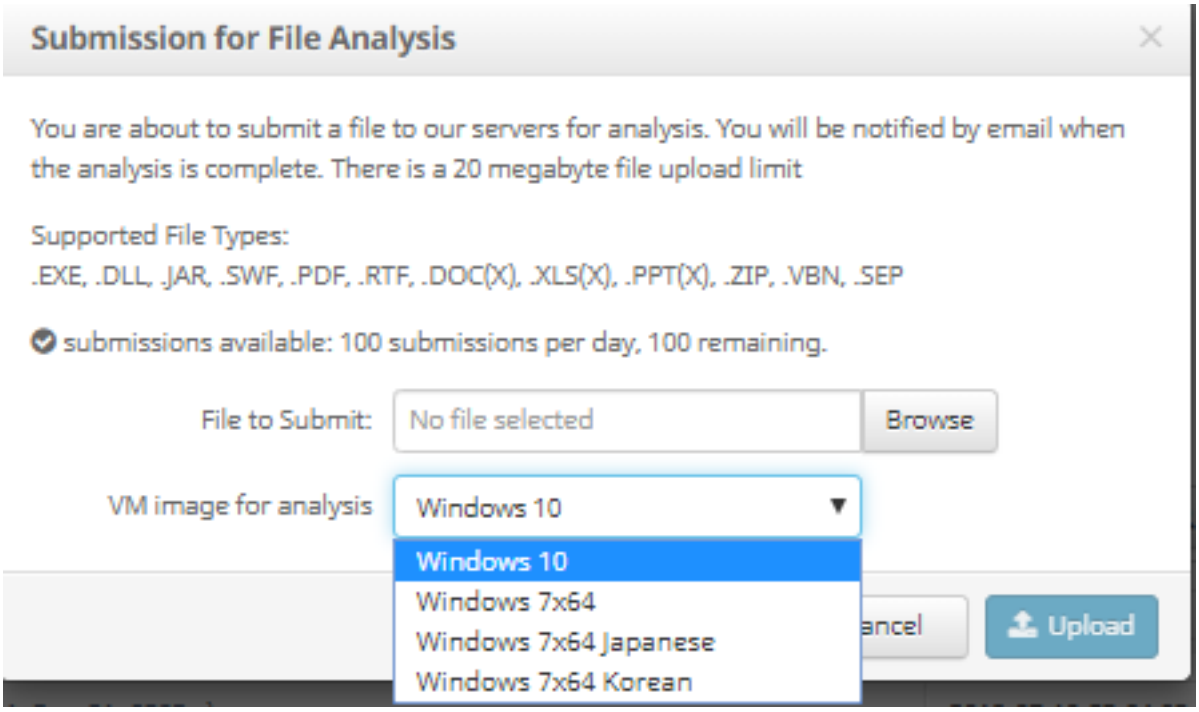
AMPポータルからサンプルをTGクラウドに送信する手順を次に示します。

ステップ1：図に示すように、AMPポータルで[**Analysis**] > [**File Analysis**]に移動します。



ステップ2：図に示すように、分析のために送信するファイルとWindowsイメージのバージョンを選択します。

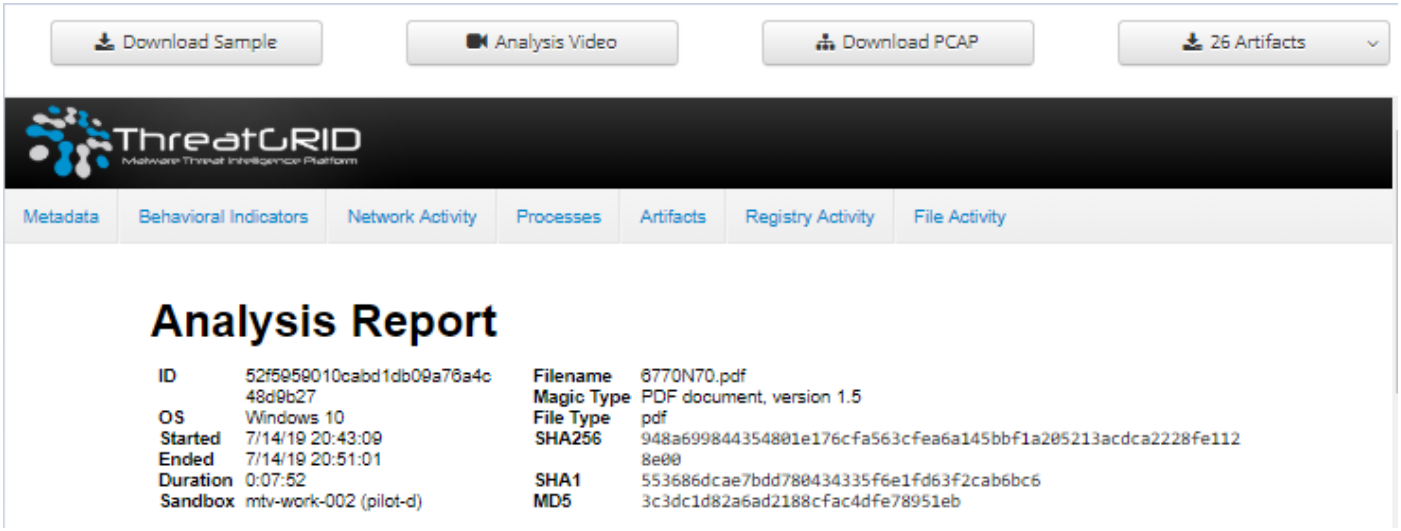




ステップ3：サンプルがアップロードされると、分析が完了するまでに約30 ~ 60分かかります。これはシステムの負荷によって異なります。このプロセスが終了すると、電子メール通知が電子メールに送信されます。

ステップ4：ファイル分析の準備が整ったら、[Report]ボタンをクリックして、図に示すように、取得した脅威スコアに関する詳細情報を取得します。

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	



詳細については、ファイル分析の追加オプションを参照してください。

ダウンロード例：このオプションを使用すると、サンプルをダウンロードできます。

分析ビデオ：このオプションを使用すると、解析時に取得したサンプルビデオを表示できます。

PCAPのダウンロード：このオプションを使用すると、ネットワーク接続の分析が可能になります。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

> **警告**：ファイル分析からダウンロードしたファイルは、多くの場合、ライブマルウェアであり、細心の注意を払って処理する必要があります。

> **注**：特定のファイルの分析は、いくつかのセクションに分かれています。一部のセクションは、すべてのファイルの種類で使用できません。

関連情報

- エンドポイント向けCisco AMP – ユーザガイド
- テクニカル サポートとドキュメント – Cisco Systems