Come inviare un file in Threat Grid dal portale AMP for Endpoints?

Sommario

Introduzione

In questo documento viene descritto il processo di invio di esempi al cloud TG (Threat Grid) da Advanced Malware Protection (AMP) for Endpoints Portal.

Contributo di Yeraldin Sánchez, Cisco TAC Engineer.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco AMP for Endpoints
- TG Cloud

Componenti usati

Il riferimento delle informazioni contenute in questo documento è la console Cisco AMP for Endpoints versione 5.4.20190709.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Di seguito sono riportati i requisiti per lo scenario descritto nel presente documento:

- Accesso al portale Cisco AMP for Endpoints
- Dimensioni del file non superiori a 20 MB
- Meno di 100 invii al giorno

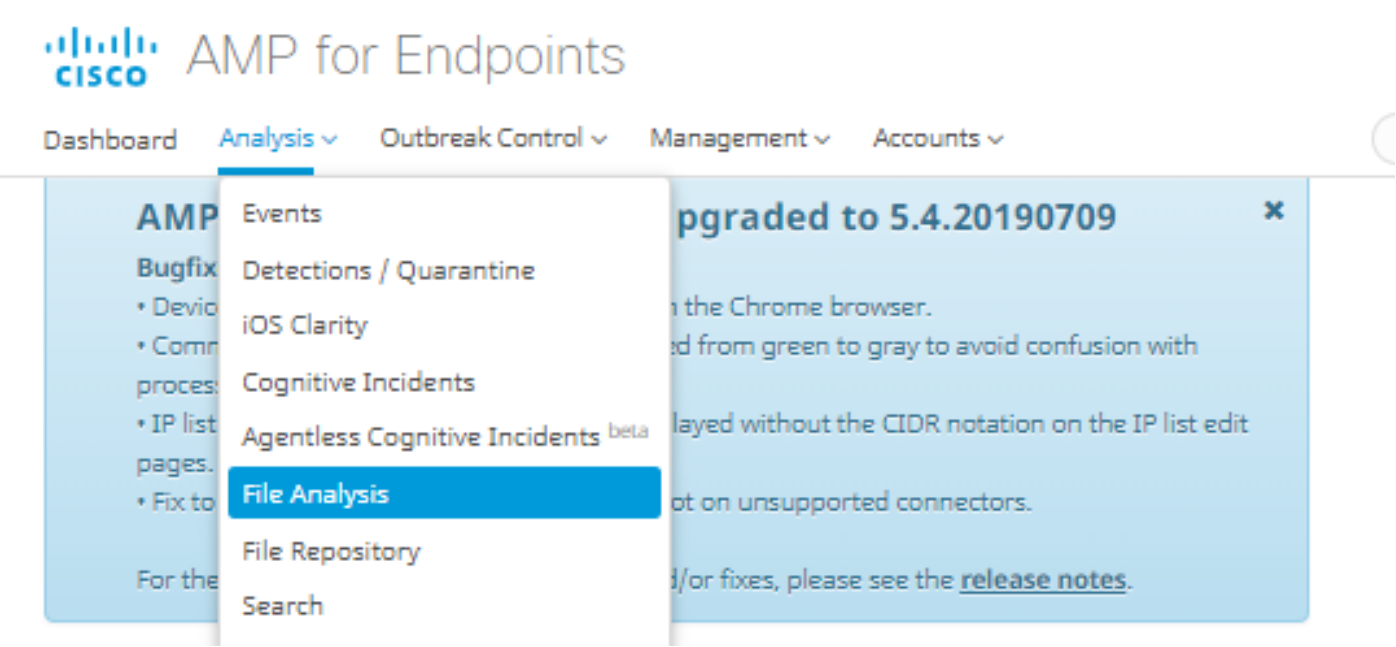
Limitazioni dell'analisi dei file:

- I nomi di file possono contenere un massimo di 59 caratteri Unicode.
- I file non possono essere inferiori a 16 byte o superiori a 20 MB
- Tipi di file supportati: **exe, dll, jar, swf, pdf, rtf, doc(x), xls(x), ppt(x), zip, vbn e sep**

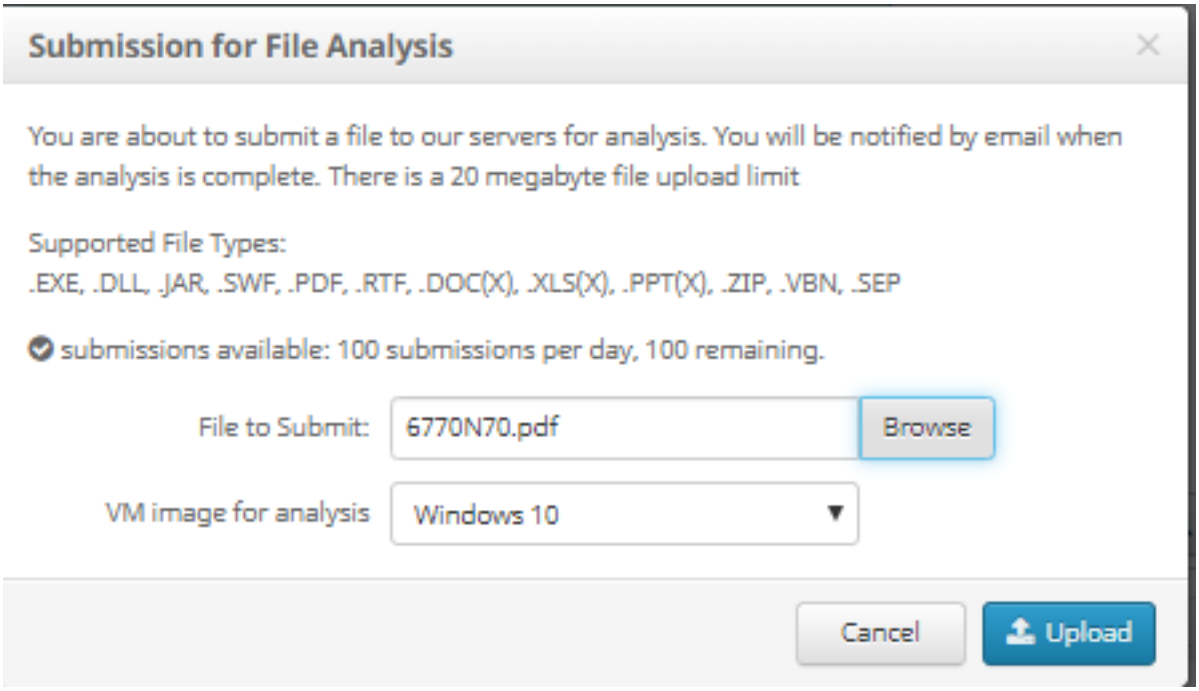
Come inviare un file in Threat Grid dal portale AMP for Endpoints?

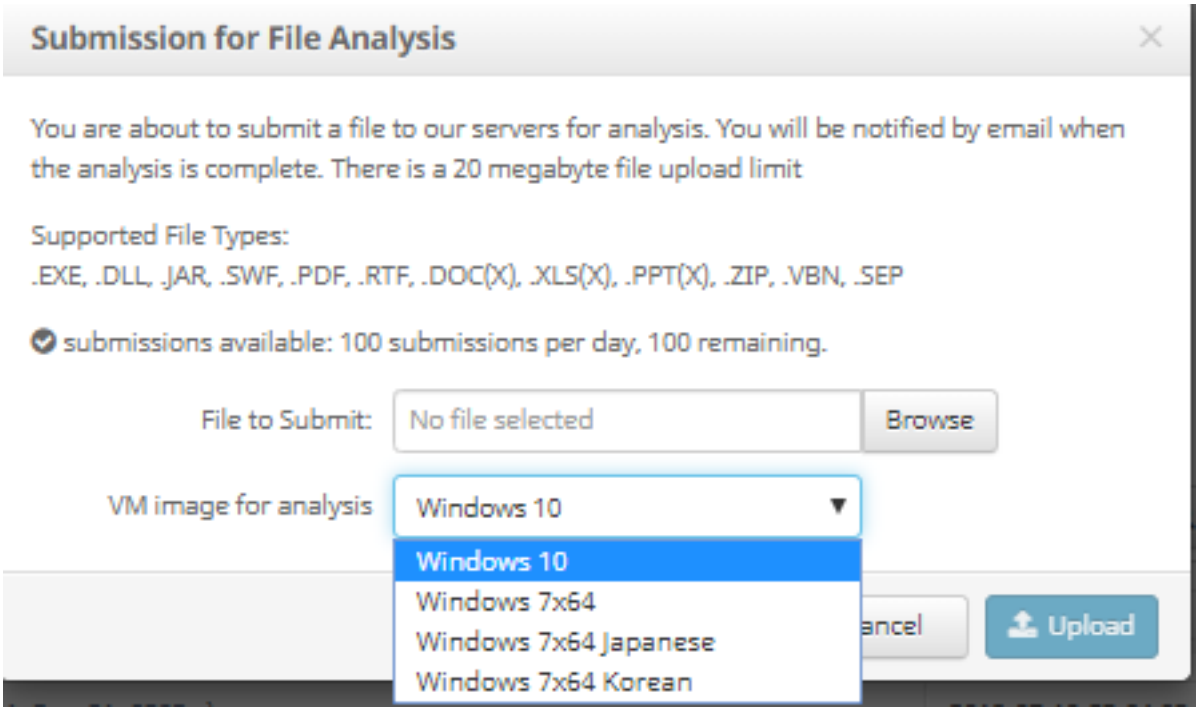
Di seguito sono riportati i passaggi da seguire per inviare un esempio a TG cloud dal portale AMP.

Passaggio 1. Sul portale AMP, passare ad **Analisi > Analisi file**, come mostrato nell'immagine.



Passaggio 2. Selezionare il file e la versione dell'immagine Windows che si desidera inviare per l'analisi, come illustrato nelle immagini.

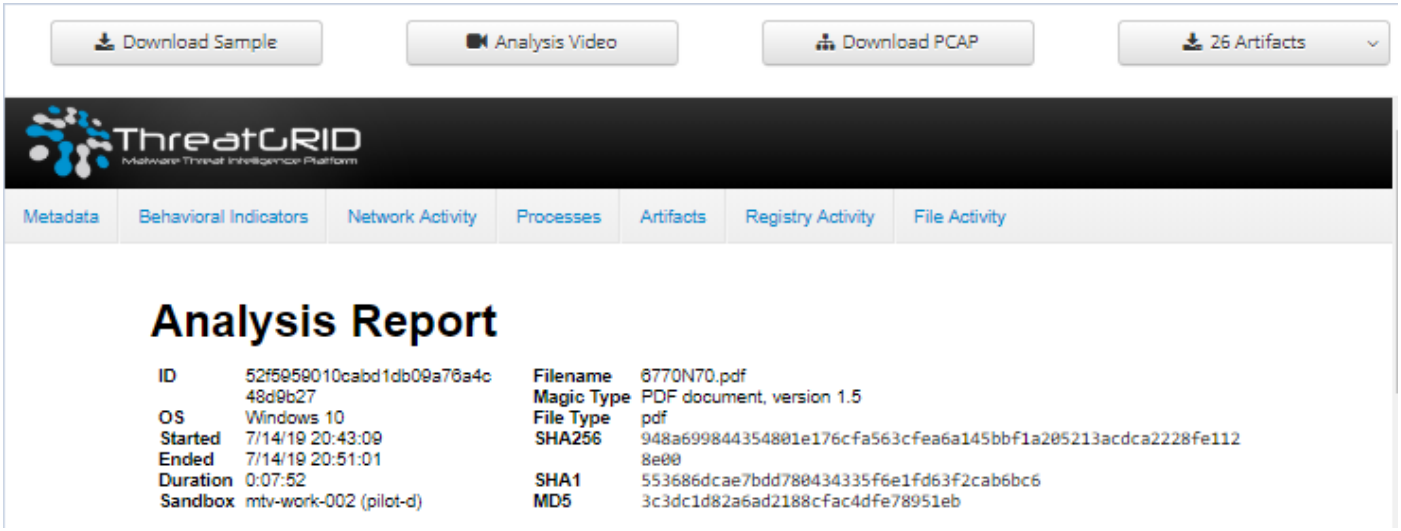




Passaggio 3. Una volta caricato il campione, l'analisi richiede circa 30-60 minuti per essere completata, dipende dal carico del sistema. Al termine di questo processo, viene inviata una notifica via e-mail all'utente.

Passaggio 4. Quando l'analisi del file è pronta, fare clic sul pulsante **Report** per ottenere informazioni dettagliate sul punteggio di minaccia ottenuto, come mostrato nelle immagini.

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	



Per ulteriori informazioni, sono disponibili ulteriori opzioni per l'analisi dei file:

Esempio di download: Questa opzione consente di scaricare l'esempio.

Video di analisi: Questa opzione fornisce il video campione ottenuto durante l'analisi.

Scarica PCAP: Questa opzione fornisce un'analisi della connettività di rete.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

> **Avviso:** I file scaricati dall'analisi dei file sono spesso malware in diretta e devono essere trattati con estrema cautela.

> **Nota:** L'analisi di un file specifico è suddivisa in più sezioni. Alcune sezioni non possono essere disponibili per tutti i tipi di file.

Informazioni correlate

- Cisco AMP for Endpoints - Guida per l'utente
- Documentazione e supporto tecnico – Cisco Systems