AMP for Endpoints 포털에서 Threat Grid의 파일을 제출하는 방법

목차

소개

이 문서에서는 AMP(Advance Malware Protection) for Endpoints 포털에서 TG(Threat Grid) 클라우드에 샘플을 제출하는 프로세스에 대해 설명합니다.

기고자: Yeraldin Sánchez, Cisco TAC 엔지니어

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco AMP for Endpoints
- TG 클라우드

사용되는 구성 요소

이 문서의 정보는 Cisco AMP for Endpoints 콘솔 버전 5.4.20190709을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

배경 정보

다음은 이 문서에 설명된 시나리오의 요구 사항입니다.

- Cisco AMP for Endpoints 포털 액세스

- 파일 크기는 20MB 이하여야 합니다.
- 하루에 100건 미만

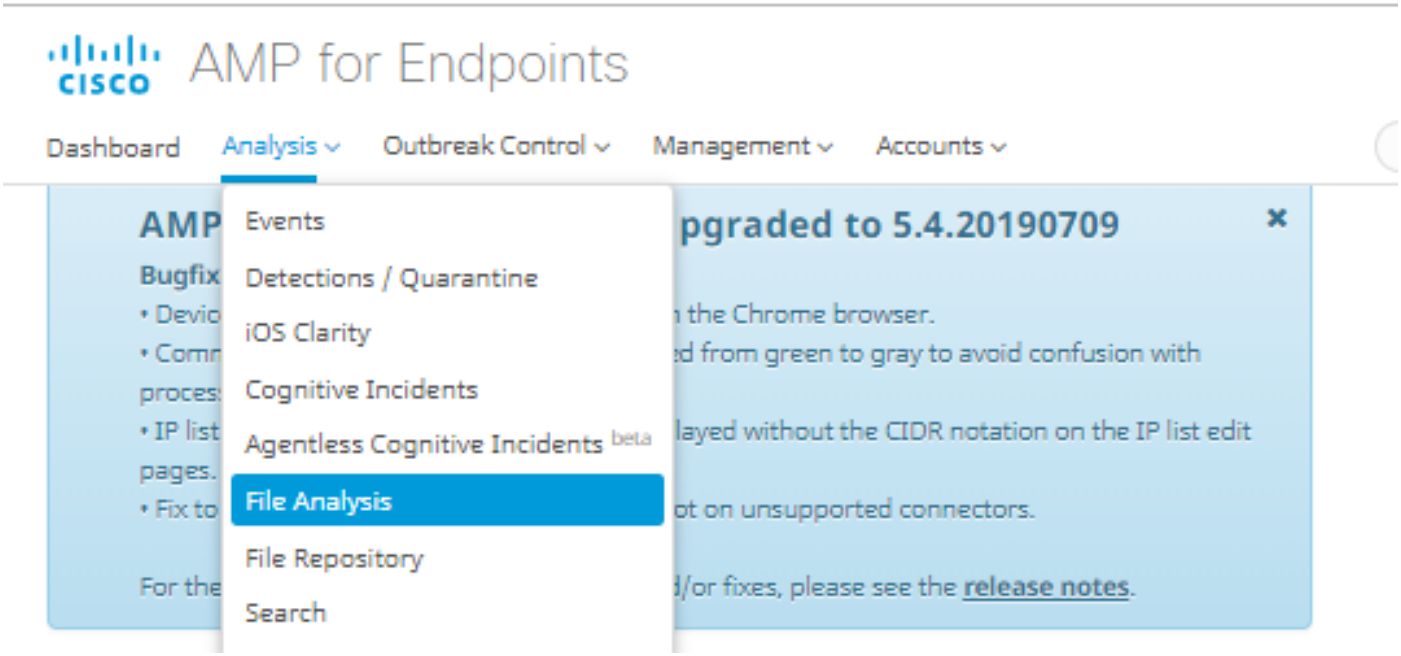
파일 분석 제한:

- 파일 이름은 유니코드 문자 59자로 제한됩니다.
- 파일은 16바이트보다 작거나 20MB보다 클 수 없습니다.
- 지원되는 파일 형식:**.exe, .dll, .jar, .swf, .pdf, .rtf, .doc(x), .xls(x), .ppt(x), .zip, .vbn 및 .sep**

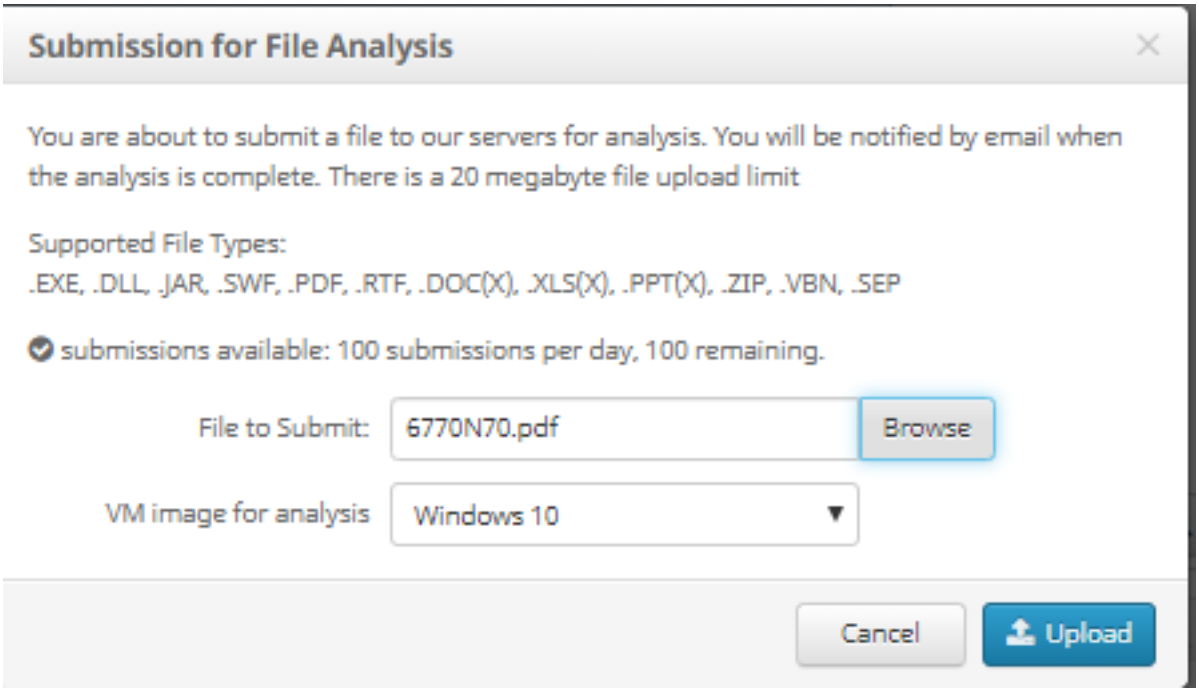
AMP for Endpoints 포털에서 Threat Grid의 파일을 제출하는 방법

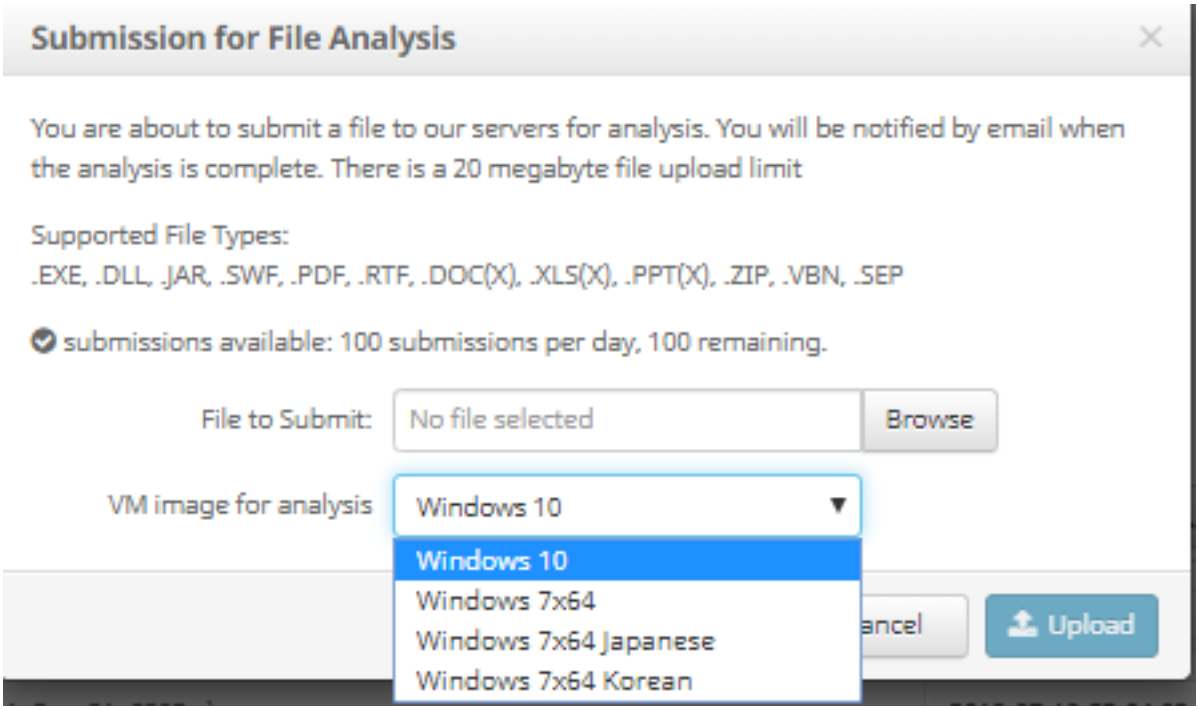
다음은 AMP 포털에서 TG 클라우드에 샘플을 제출하기 위해 따라야 할 단계입니다.

1단계. AMP 포털에서 이미지에 표시된 대로 **Analysis > File Analysis**로 이동합니다.



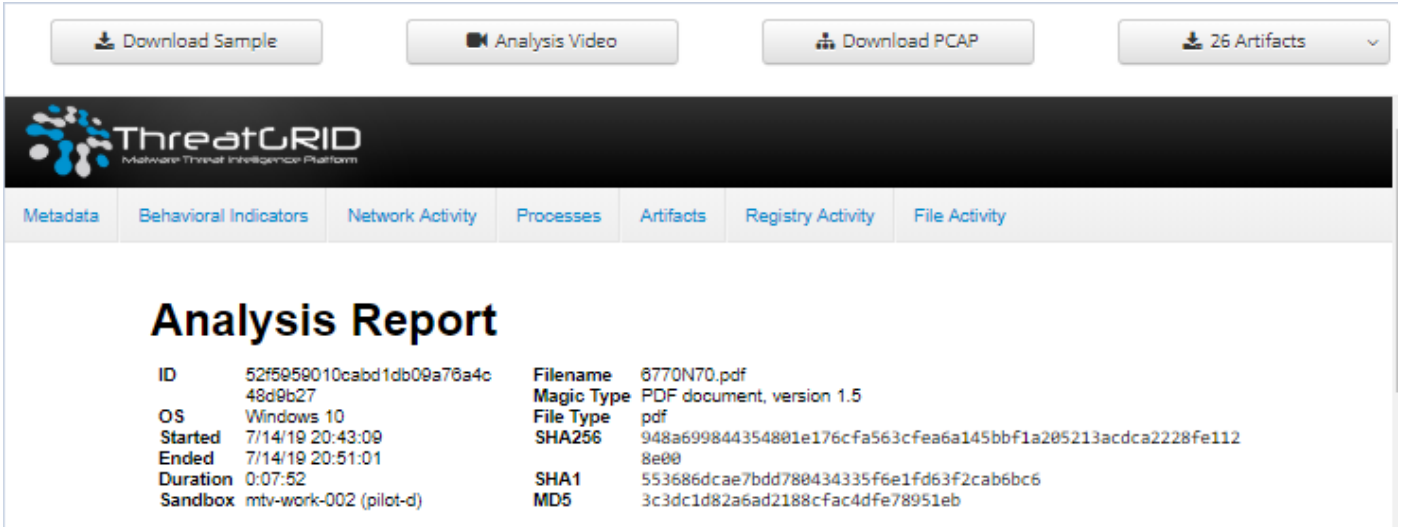
2단계. 이미지에 표시된 대로 분석을 위해 보낼 파일 및 Windows 이미지 버전을 선택합니다.





3단계. 샘플을 업로드한 후 분석을 완료하는 데 약 30~60분이 소요되며, 이 프로세스가 완료되면 이메일 알림이 이메일로 전송됩니다.

4단계. 파일 분석이 준비되면 **Report** 버튼을 클릭하여 이미지에 표시된 것처럼 가져온 위협 점수에 대한 자세한 정보를 확인합니다.



자세한 내용을 보려면 파일 분석을 위한 추가 옵션을 찾을 수 있습니다.

샘플 다운로드:이 옵션을 사용하면 샘플을 다운로드할 수 있습니다.

분석 비디오:이 옵션은 분석에서 얻은 샘플 비디오를 제공합니다.

PCAP 다운로드:이 옵션은 네트워크 연결 분석을 제공합니다.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

> **경고:**File Analysis(파일 분석)에서 다운로드한 파일은 종종 라이브 악성코드이며 매우 주의해야 합니다.

> **참고:**특정 파일의 분석은 여러 섹션으로 구분됩니다.일부 섹션은 모든 파일 유형에 사용할 수 없습니다.

관련 정보

- Cisco AMP for Endpoints - 사용 설명서
- 기술 지원 및 문서 – Cisco Systems