从面向终端的AMP门户向Threat Grid提交文件

目录

简介

问题

环境

文件分析限制

分辨率

简介

本文档介绍从面向终端的高级恶意软件防护(AMP)终端门户向Threat Grid(TG)云提交样本的过程。

问题

从面向终端的AMP门户向Threat Grid云提交文件进行分析。

环境

所需的知识包括：

- 面向终端的思科AMP
- Threat Grid云

本文档中引用的产品版本：面向终端的思科AMP思科AMP终端控制台版本5.4.20190709。

以下是本文档中描述的方案的条件和限制：

- 访问面向终端的思科AMP的终端门户
- 文件大小不超过20 MB
- 每天提交少于100次

文件分析限制

- 文件名限制为59个Unicode字符。
- 文件不能小于16字节或大于20 MB。
- 支持的文件类型：.exe、.dll、.jar、.swf、.pdf、.rtf、.doc(x)、.xls(x)、.ppt(x)、.zip、.vbn和.sep

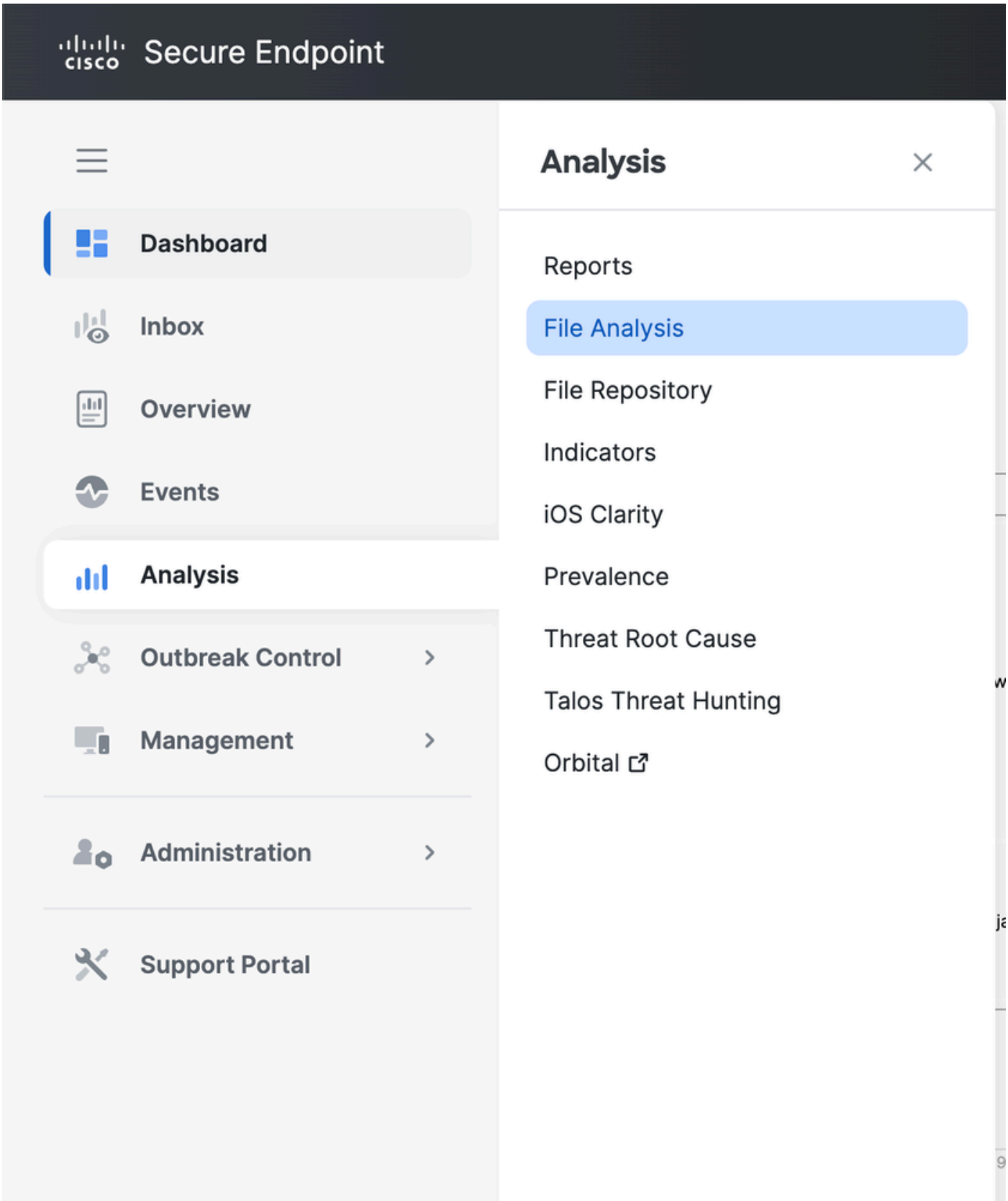
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

分辨率

1.确认您可以登录到面向终端的思科AMP的终端门户。

2.确认示例符合文件分析限制（文件大小、支持的文件类型和每日提交限制）。

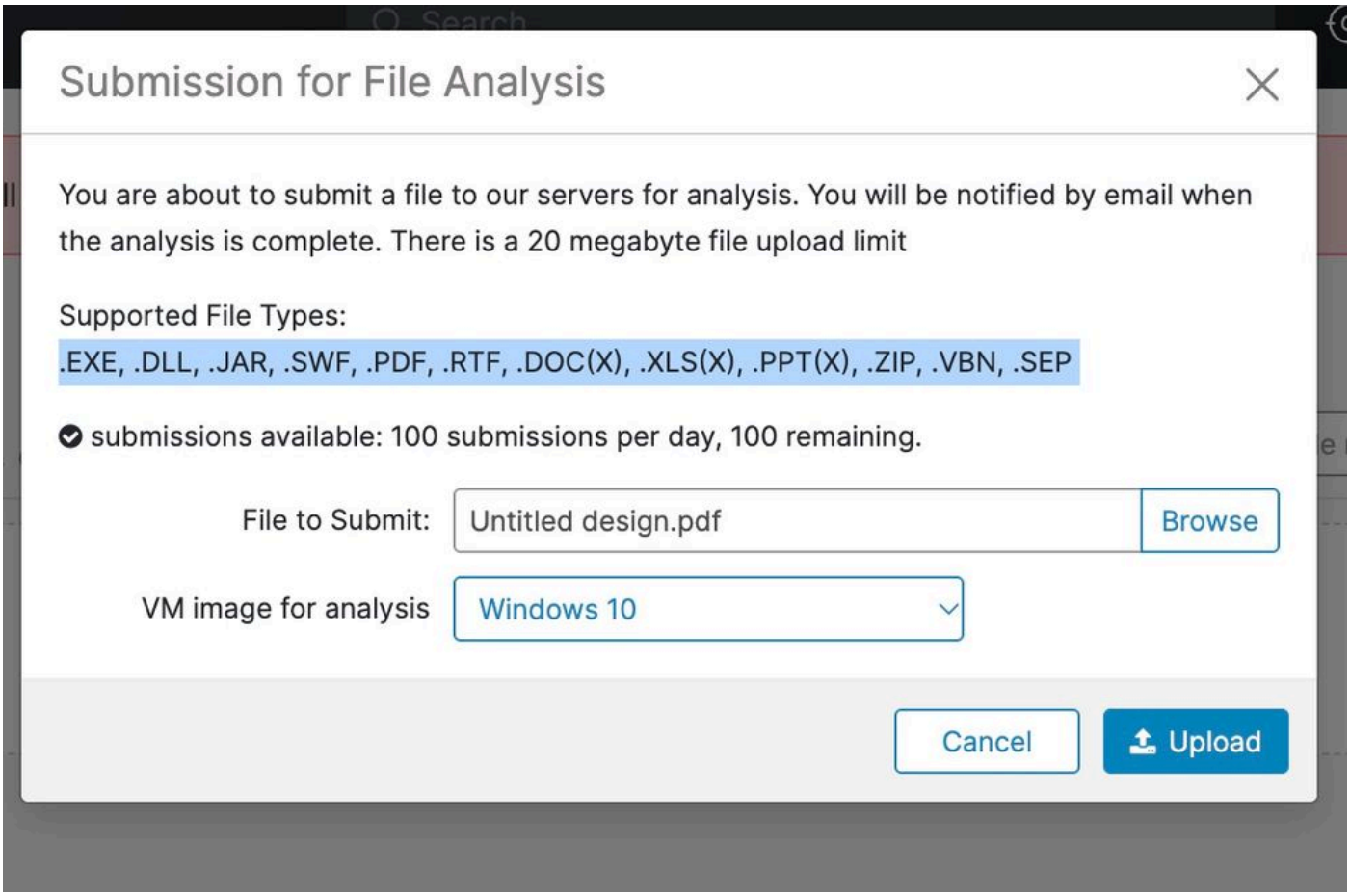
3.在AMP门户中，导航到分析>文件分析。



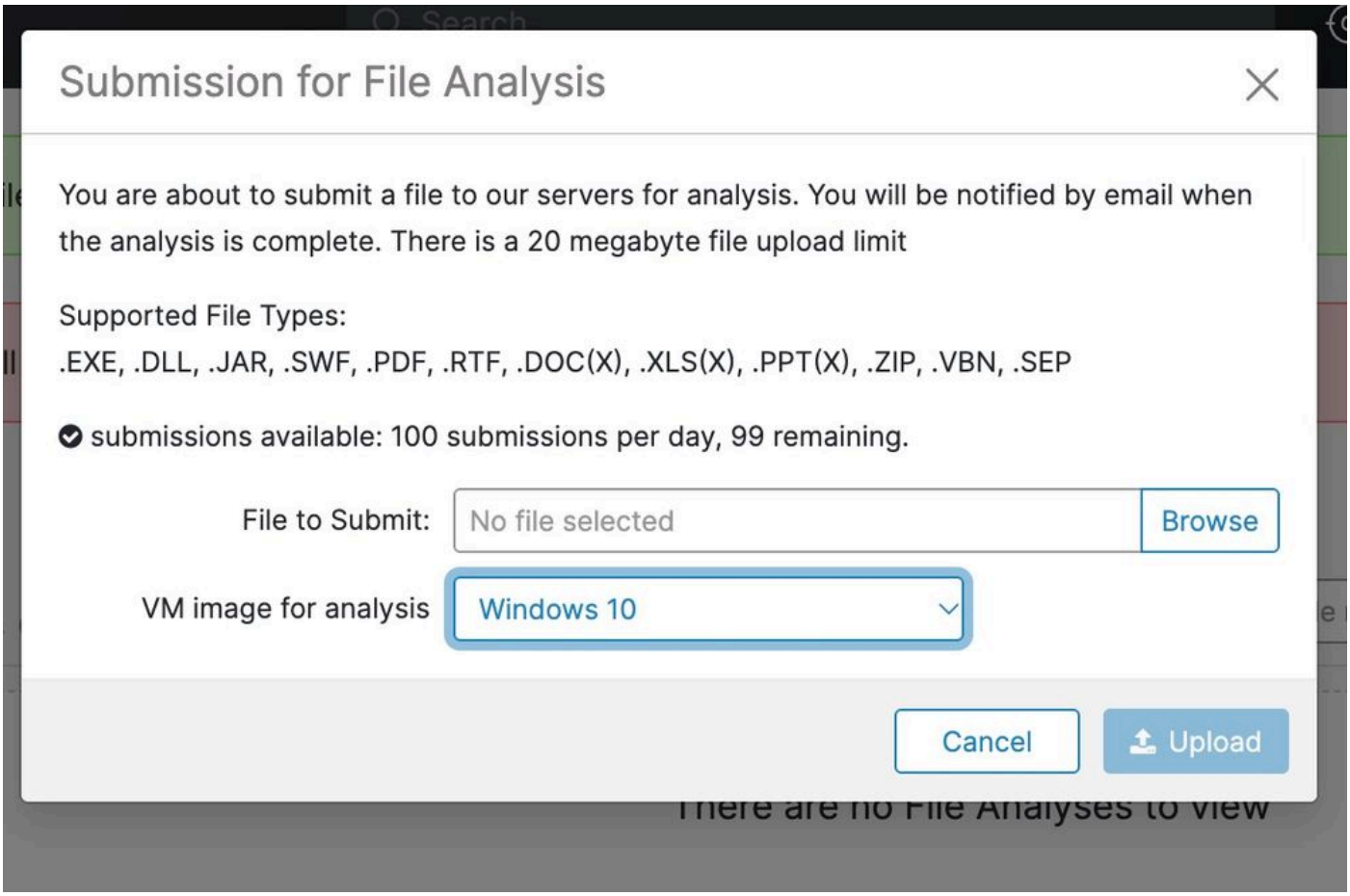
文件分析AMP page.png

4.单击Choose File（或上传控件），然后选择要提交的文件。

5.选择要用于分析的Windows映像版本。


Submission for File Analysis
You are about to submit a file to our servers for analysis. You will be notified by email when the analysis is complete. There is a 20 megabyte file upload limit
Supported File Types:
.EXE, .DLL, .JAR, .SWF, .PDF, .RTF, .DOC(X), .XLS(X), .PPT(X), .ZIP, .VBN, .SEP
submissions available: 100 submissions per day, 100 remaining.
File to Submit:
Untitled design.pdf
Browse
VM image for analysis
Windows 10
Cancel
Upload

提交file.jpeg


Submission for File Analysis
You are about to submit a file to our servers for analysis. You will be notified by email when the analysis is complete. There is a 20 megabyte file upload limit
Supported File Types:
.EXE, .DLL, .JAR, .SWF, .PDF, .RTF, .DOC(X), .XLS(X), .PPT(X), .ZIP, .VBN, .SEP
submissions available: 100 submissions per day, 99 remaining.
File to Submit:
No file selected
Browse
VM image for analysis
Windows 10
Cancel
Upload

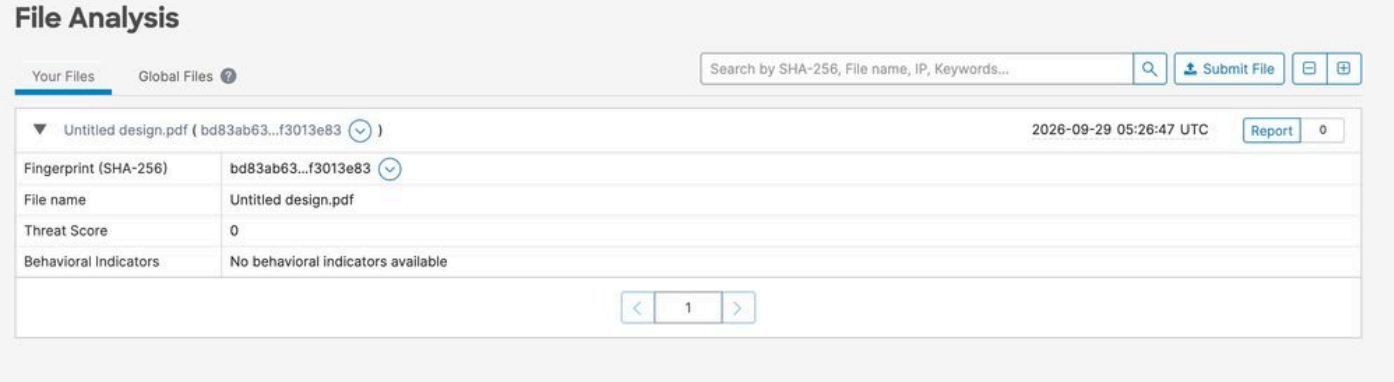
提交文件2.jpeg

6.等待分析完成。分析通常需要30到60分钟。

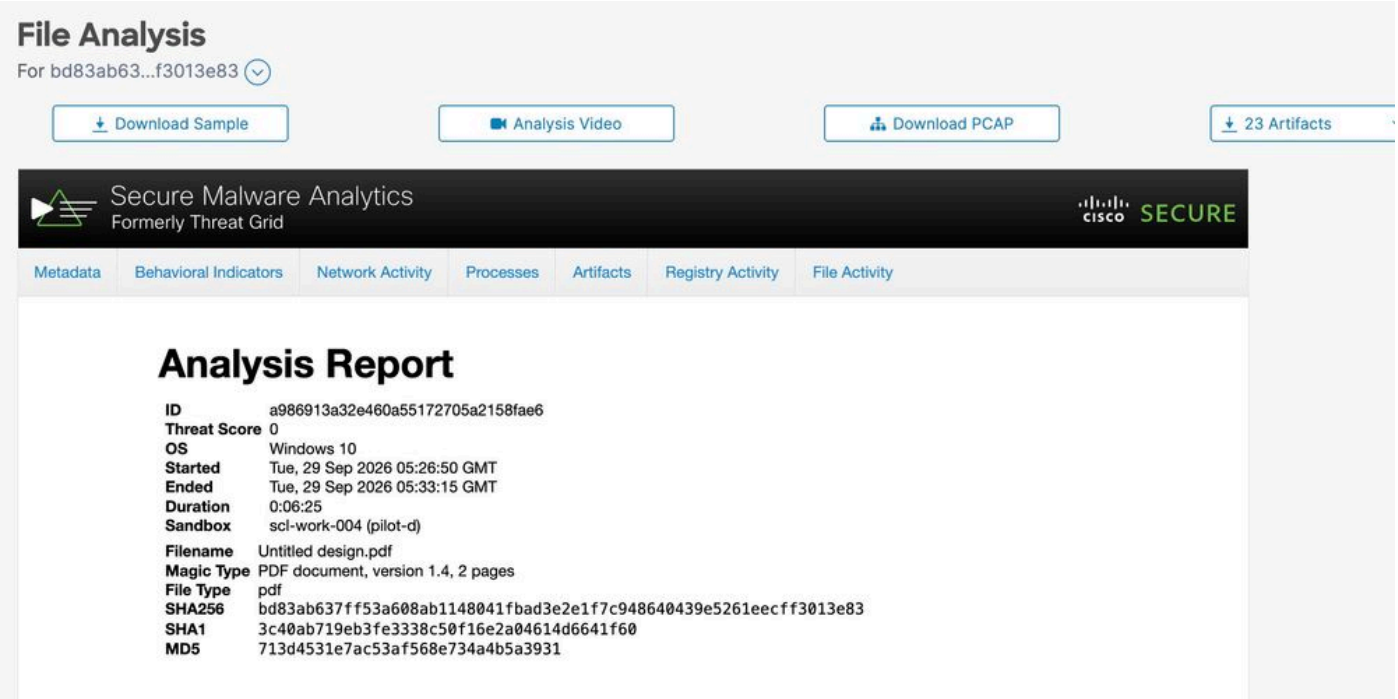
注意：持续时间取决于系统负载。

7.确认分析完成后收到电子邮件通知。

8.文件分析准备就绪后，单击Report查看威胁评分详细信息。



文件就绪.jpeg



Report.jpeg

可选对象（如果可用）包括：

- 下载示例:下载已提交的示例。
- 分析视频:此选项提供在分析期间生成的示例视频。
- 下载PCAP:从分析下载数据包捕获。

预期结果：分析状态更改为“已完成”(completed),Report视图打开，显示威胁评分详情和任何可用对象。

 警告：从文件分析下载的文件通常是实时恶意软件，必须谨慎处理。

 注意：特定文件的分析分为几个部分。某些部分可能并非适用于所有文件类型。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。