排除Cisco XDR和安全恶意软件分析云集成故障

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[背景信息](#)
[故障排除](#)
[许可证](#)
[模块磁贴](#)
[管理员角色](#)
[时间段](#)
[重新创建模块](#)

简介

本文档介绍如何使用Cisco XDR对安全恶意软件分析云模块进行故障排除。

作者：Javi Martinez，思科TAC工程师。

先决条件

要求

Cisco 建议您了解以下主题：

- 安全恶意软件分析云
- 思科XDR

使用的组件

本文档中的信息基于以下软件版本：

- 安全恶意软件分析云控制台（具有管理员权限的用户帐户）
- Cisco XDR控制台（具有管理员权限的用户帐户）

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。

背景信息

Cisco Secure Malware Analytics Cloud是一个高级且自动化的恶意软件分析和恶意软件威胁情报平台，可在其中触发可疑文件或Web目标，而不会影响用户环境。

在与Cisco XDR的集成中，安全恶意软件分析是一个参考模块，它提供了向安全恶意软件分析门户进行透视的能力，从而在安全恶意软件分析云（SMA云）知识库中收集有关文件散列、IP、域和URL的额外情报。

请参阅最新的安全恶意软件分析云集成指南，

- NAM云。
- EU云。

故障排除

许可证

- 验证您拥有适当的SMA许可证，以便访问安全恶意软件分析云控制台

模块磁贴

- 验证您为安全恶意软件分析云模块选择了正确的磁贴
  导航到Cisco XDR门户>控制面板>自定义按钮>选择SMA云模块>添加适当的磁贴

管理员角色

- 验证您在安全恶意软件分析门户中是否拥有具有管理员角色的安全恶意软件分析帐户
  导航到Cisco XDR门户>管理>您的帐户
- 验证您在SecureX门户中具有管理员权限的SecureX帐户
  导航到Malware Analytics门户> My Malware Analytics帐户

注意：如果您在安全恶意软件分析控制台和Cisco XDR控制台中没有管理员角色，则您的管理员可以直接从有问题的门户更改帐户角色

时间段

- 验证在Cisco XDR门户上正确设置了时间戳。
  导航到Cisco XDR门户>控制面板>时间范围选项>根据SMA活动选择适当的时间范围

重新创建模块

- 删除旧的SMA模块并创建新的SMA模块。
  导航到Secure Malware Analytics Cloud console > My Malware Analytics account > API Key > Copy the API key

导航到Cisco XDR门户>集成模块>选择SMA云模块>添加API密钥和URL（选择SMA云）>创建控制面板

注意：只有具有“组织管理员”(Org Admin)或“用户”(Users)角色的用户可以获取在Cisco XDR中启用安全恶意软件分析集成模块的API密钥。

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）。