通过日志导出或报告API了解数据管理

目录

简介

本文档介绍如何使用Cisco Umbrella中的日志导出或报告API管理数据。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于Cisco Umbrella。

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。

概述

Umbrella是一个功能强大的工具，可为您提供大量有关互联网流量的信息。以下是一个简单的指南，可帮助您确定如何最好地使用数据：

使用案例	粒度/类型	建议	考虑事项
法规遵从性/长期事件保留	导出并存储所有事件	S3:客户拥有的存储桶	可以使用Cisco Managed Bucket，但信息最多只能保留30天。
SIEM:事件关联	导出所有事件	S3:思科管理的存储桶	信息的保留期最长为30天；需要处理分流。
控制面板KPI/构件	活动搜索/聚合	报告API	查询必须经过适当调整，因为广泛查询可能会导致超时。

生成报告	聚合	报告API	
SOAR工作流程：触发器	活动搜索	报告API	查询必须经过适当调整，因为广泛查询可能会导致超时。

Additional Information

- 有关如何管理日志的说明：Umbrella文档 — 管理您的日志
- 有关如何管理API的说明：Cisco DevNet — 思科云安全API

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）。