使用REST API将Umbrella日志与Azure Sentinel集成

目录

简介

本文档介绍如何通过REST API将Umbrella日志导入Azure Sentinel。

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

如果将Azure Sentinel用作SIEM，则可以将Umbrella日志吸收入其中。本文描述了完成集成所需的过程。

步骤

要使用REST API将Umbrella登录导入Azure Sentinel，请完成以下步骤：

1.访问将Umbrella与Azure Sentinel集成的文档。

2.遵守Microsoft文档中有关配置的所有详细说明。

请阅读《Microsoft集成指南》中的更多内容。

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）。