REST APIを使用してUmbrella口グをAzure Sentinelと統合する

内容

はじめに

このドキュメントでは、REST APIを使用してUmbrellaのログをAzure Sentinelに取り込む方法について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Cisco Umbrellaに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

概要

Azure SentinelをSIEMとして使用する場合は、Umbrellaの口グを取り込むことができます。この記事では、統合を完了するために必要なプロセスについて説明します。

手順

REST APIを使用してUmbrellaの口グをAzure Sentinelに取り込むには、次の手順を実行します。

1. UmbrellaとAzure Sentinelの統合に関するドキュメントにアクセスします。

2. Microsoftのドキュメントに記載されている設定に関する詳細な指示すべてに従います。

詳細については、『Microsoft統合ガイド』を参照してください。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。