ログエクスポートまたはレポートAPIを使用したデータ管理について

内容

[はじめに](#)

[前提条件](#)

- [要件](#)
- [使用するコンポーネント](#)

[概要](#)

[追加情報](#)

はじめに

このドキュメントでは、Cisco Umbrellaのログエクスポートまたはレポート API を使用してデータを管理する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

Umbrellaは、インターネットトラフィックに関するさまざまな情報を提供する強力なツールです。データを最大限に活用する方法を決定するのに役立つ簡単なガイドを次に示します。

使用例	粒度/タイプ	推奨事項	考慮事項
コンプライアンス/長期的なイベント保存	すべてのイベントのエクスポートと保存	S3：顧客所有バケット	Cisco Managed Bucketを使用することは可能ですが、情報は30日以内しか保持されません。
SIEM：イベント相関	すべてのイベントを	S3：シスコマ	情報は30日間までしか保持されま

	エクスポート	ネージドバケット	せん。オフロードは処理する必要があります。
ダッシュボードKPI/ウィジェット	アクティビティの検索/集約	レポートAPI	広範なクエリーによってタイムアウトが発生する可能性があるため、クエリーは十分に調整する必要があります。
レポートの生成	集約	レポートAPI	
SOARワークフロー：トリガー	アクティビティ検索	レポートAPI	広範なクエリーによってタイムアウトが発生する可能性があるため、クエリーは十分に調整する必要があります。

追加情報

- ログの管理方法に関する指示：Umbrellaドキュメント – ログの管理
- APIの管理手順：Cisco DevNet-Cisco Cloud Security API

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。