로그 내보내기 또는 보고 API를 통한 데이터 관리 이해

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[개요](#)

[추가 정보](#)

소개

이 문서에서는 Cisco Umbrella에서 로그 내보내기 또는 보고 API를 사용하여 데이터를 관리하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco Umbrella를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

개요

Umbrella는 인터넷 트래픽에 대한 많은 정보를 제공하는 강력한 도구입니다. 다음은 데이터를 가장 효과적으로 사용하는 방법을 결정하는 데 도움이 되는 간단한 가이드입니다.

사용 사례	세분성/유형	권장 사항	고려 사항
규정 준수/장기 이벤트 보존	모든 이벤트 내보내기 및 저장	S3: 고객 소유 버킷	Cisco Managed Bucket을 사용할 수 있지만 정보는 최대 30일까지만 보존됩니다.
SIEM: 이벤트 상관관계	모든 이벤트 내보내기	S3: Cisco 매니지드 버킷	정보는 최대 30일까지만 보존됩니다. 오프로드를 처리해야 합니다.

대시보드 KPI/위젯	활동 검색/집계	보고 API	광범위한 쿼리로 인해 시간이 초과될 수 있으므로 쿼리를 잘 조정해야 합니다.
보고서 생성	집계	보고 API	
SOAR 워크플로: 트리거	활동 검색	보고 API	광범위한 쿼리로 인해 시간이 초과될 수 있으므로 쿼리를 잘 조정해야 합니다.

추가 정보

- 로그 관리 방법에 대한 지침: [Umbrella 문서 - 로그 관리](#)
- API 관리 방법에 대한 지침: [Cisco DevNet-Cisco Cloud Security API](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.