REST API를 사용하여 Umbrella 로그를 Azure Sentinel과 통합

목차

소개

이 문서에서는 REST API를 통해 Umbrella 로그를 Azure Sentinel에 가져오는 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

Azure Sentinel을 SIEM으로 사용하는 경우 Umbrella 로그를 가져올 수 있습니다. 이 문서에서는 통합을 완료하는 데 필요한 프로세스에 대해 설명합니다.

절차

REST API를 사용하여 Umbrella 로그를 Azure Sentinel에 가져오는 절차는 다음과 같습니다.

1. Umbrella와 Azure Sentinel의 통합을 위한 문서에 액세스합니다.

2. Microsoft 설명서의 구성에 대한 모든 세부 지침을 준수합니다.

자세한 내용은 Microsoft 통합 설명서를 참조하십시오.

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.