Umbrella Logs integreren met Azure Sentinel met REST API

Inhoud

Inleiding

In dit document wordt beschreven hoe u Umbrella-logs kunt invoegen in Azure Sentinel via REST API.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Umbrella.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Overzicht

Als u Azure Sentinel als SIEM gebruikt, kunt u Umbrella-logboeken invoegen. Dit artikel beschrijft het proces dat nodig is om de integratie te voltooien.

Procedure

Voer de volgende stappen uit om Umbrella-logs in te nemen in Azure Sentinel met behulp van de REST API:

1. Toegang tot de documentatie voor de integratie van Umbrella met Azure Sentinel.

2. Volg alle gedetailleerde instructies voor configuratie in de Microsoft-documentatie.

Lees meer in de Microsoft-integratiehandleiding.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.