Integra i log Umbrella con Azure Sentinel tramite l'API REST

Sommario

[Introduzione](#)

[Prerequisiti](#)

- [Requisiti](#)
- [Componenti usati](#)

[Panoramica](#)

[Procedura](#)

Introduzione

In questo documento viene descritto come caricare i log di Umbrella in Azure Sentinel tramite l'API REST.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano su Cisco Umbrella.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Panoramica

Se usi Azure Sentinel come SIEM, puoi acquisire i log di Umbrella in esso. In questo articolo viene descritto il processo necessario per completare l'integrazione.

Procedura

Per caricare i log di Umbrella in Azure Sentinel tramite l'API REST, completare la procedura seguente:

1. Accedere alla documentazione per l'integrazione di Umbrella con Azure Sentinel.

2. Attenersi a tutte le istruzioni dettagliate per la configurazione riportate nella documentazione Microsoft.

Ulteriori informazioni sono disponibili nella Guida all'integrazione di Microsoft.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).