Intégration des journaux Umbrella avec Azure Sentinel à l'aide de l'API REST

Table des matières

Introduction

Ce document décrit comment ingérer des journaux Umbrella dans Azure Sentinel via l'API REST.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur Cisco Umbrella.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Aperçu

Si vous utilisez Azure Sentinel en tant que SIEM, vous pouvez y ingérer des connexions Umbrella. Cet article décrit le processus requis pour terminer l'intégration.

Procédure

Pour ingérer les journaux Umbrella dans Azure Sentinel à l'aide de l'API REST, procédez comme suit :

1. Accédez à la documentation pour intégrer Umbrella à Azure Sentinel.

2. Suivez toutes les instructions détaillées de configuration fournies dans la documentation Microsoft.

Pour en savoir plus, consultez le guide d'intégration Microsoft.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.