Comprendre la gestion des données avec les exportations de journaux ou l'API de rapport

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Aperçu](#)

[Additional Information](#)

Introduction

Ce document décrit comment gérer les données avec les exportations de journaux ou l'API de rapport dans Cisco Umbrella.

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

Umbrella est un outil puissant qui vous donne beaucoup d'informations sur votre trafic Internet. Voici un guide simple pour vous aider à décider comment utiliser au mieux vos données :

Scénario	Granularité / Type	Recommandation	Considérations
Conformité/rétention à long terme des événements	Exporter et stocker tous les événements	S3 : Compartiment appartenant au client	Il est possible d'utiliser Cisco Managed Bucket, mais les informations ne sont conservées que jusqu'à 30 jours.
SIEM : Corrélation des événements	Exporter tous les événements	S3 : Compartiment	Les renseignements sont conservés pendant une période

		géré par Cisco	maximale de 30 jours; le déchargement doit être traité.
Indicateurs/Widgets du tableau de bord	Recherche d'activité/Agrégations	API de rapport	La requête doit être bien réglée, car une requête étendue peut entraîner des délais d'attente.
Générer des rapports	Agrégations	API de rapport	
Workflow SOAR : Déclencheur	Recherche d'activité	API de rapport	La requête doit être bien réglée, car une requête étendue peut entraîner des délais d'attente.

Additional Information

- Instructions relatives à la gestion de vos journaux : [Documentation Umbrella - Gérer vos journaux](#)
- Instructions relatives à la gestion de vos API : [API de sécurité cloud Cisco DevNet-Cisco](#)

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.