Entender o Gerenciamento de Dados com Exportações de Log ou API de Relatório

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Overview](#)

[Informações adicionais](#)

Introdução

Este documento descreve como gerenciar dados com exportações de log ou a API de relatório no Cisco Umbrella.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no Cisco Umbrella.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Overview

Umbrella é uma ferramenta poderosa que lhe dá muitas informações sobre o seu tráfego de Internet. Aqui está um guia simples para ajudá-lo a decidir como consumir melhor seus dados:

Caso de uso	Granularidade/tipo	Recomendação	Considerações
Conformidade/retenção de eventos a longo prazo	Exportar e armazenar todos os eventos	S3: Bucket de propriedade do cliente	É possível usar o Cisco Managed Bucket, mas as informações são retidas somente até 30 dias.
SIEM: Correlação de	Exportar todos os	S3: Balde	As informações são retidas apenas

Evento	eventos	gerenciado pela Cisco	até 30 dias; o descarregamento precisa ser tratado.
KPI/Widgets do Painel	Pesquisa/agregações de atividades	API de relatório	A consulta deve ser bem ajustada, pois uma consulta ampla pode resultar em tempos limite.
Gerar relatórios	Agregações	API de relatório	
Fluxo de trabalho do SOAR: Gatilho	Pesquisa de atividade	API de relatório	A consulta deve ser bem ajustada, pois uma consulta ampla pode resultar em tempos limite.

Informações adicionais

- Instruções sobre como gerenciar seus logs: [Documentação abrangente - Gerencie seus registros](#)
- Instruções sobre como gerenciar suas APIs: [API Cisco DevNet-Cisco Cloud Security](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.