Datenmanagement mit Log-Exporten oder Reporting-API

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Daten mit Protokollexporten oder der Reporting-API in Cisco Umbrella verwaltet werden.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Umbrella.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Überblick

Umbrella ist ein mächtiges Werkzeug, das Ihnen eine Menge Informationen über Ihren Internet-Verkehr gibt. Hier finden Sie eine einfache Anleitung, die Ihnen hilft, zu entscheiden, wie Sie Ihre Daten am besten nutzen:

Anwendungsfall	Granularität/Typ	Empfehlung	Überlegungen
Compliance/Langfristige Ereignisaufbewahrung	Alle Ereignisse exportieren und speichern	S3: Eimer im Kundenbesitz	Sie können Cisco Managed Bucket

			verwenden. Die Informationen werden jedoch nur bis zu 30 Tage gespeichert.
SIEM: Ereigniskorrelation	Alle Veranstaltungen exportieren	S3: Von Cisco verwalteter Bucket	Die Informationen werden nur bis zu 30 Tage aufbewahrt. Abladung muss behandelt werden.
Dashboard-KPI/Widgets	Aktivitätssuche/Aggregationen	Reporting-API	Die Abfrage muss genau abgestimmt sein, da eine umfassende Abfrage zu Timeouts führen kann.
Berichte erstellen	Aggregationen	Reporting-API	
SOAR-Workflow: Auslöser	Aktivitätssuche	Reporting-API	Die Abfrage muss genau abgestimmt sein, da eine umfassende Abfrage zu Timeouts führen kann.

Zusätzliche Informationen

- Anweisungen zur Verwaltung Ihrer Protokolle: Umbrella-Dokumentation - Verwalten Sie Ihre Protokolle
- Anleitung zur Verwaltung Ihrer APIs: Cisco DevNet - Cisco Cloud Security API

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.