Ereignisprotokolle der Datei für sicheren Zugriff fehlen nach Lizenzänderung in SIEM

Inhalt

Problem

Die Dateiereignisprotokolle wurden vom SIEM nicht mehr vom AWS S3-Speicher empfangen, während die DNS-Protokolle weiterhin erfolgreich übermittelt wurden. Die Dateiereignis-Datenverbindungen zeigten ein Symbol für "Getrennt" in der SIEM-Schnittstelle an. Die nicht mehr angezeigten Protokolle wurden als DLP-/IPS-bezogene Datensätze für Dateiereignisse identifiziert. Die DNS-Layer-Protokolle waren während des gesamten Problemzeitraums funktionsfähig.

Während der Migration verwendete die Umgebung sowohl Umbrella als auch Secure Access. Die Protokolle wurden an denselben AWS-Bucket gesendet. Die Schlüssel wurden gedreht und es wurde bestätigt, dass sie ordnungsgemäß funktionieren. Die Schemaversion wurde als in Version 10 angegeben, während Version 16 verfügbar war.

Umwelt

- Cisco Secure Access-Organisation mit Umbrella- und Secure Access-Konfigurationen
- AWS S3-Speicherintegration für Protokollexport
- Microsoft Sentinel SIEM-Plattform
- Schemaversion 10 in Gebrauch (Version 16 verfügbar)
- Änderung der Secure Access-Lizenz von Advantage zu Essentials am 23. Juni 2026
- Dateiereignisprotokolle, die zuletzt am 24. Juni 2026 beobachtet wurden

Auflösung

Die Untersuchung ergab, dass die Dateiereignisprotokolle mit der DLP-/IPS-Funktionalität in Zusammenhang standen, für die spezielle Lizenzfunktionen erforderlich sind. Die Ursache wurde in der nächsten Analyse ermittelt.

Schritt 1: Datenverkehrsanalyse

Überprüfen Sie die Aktivitätssuche in Sicherer Zugriff, um die Datenverkehrsmuster zu bestätigen:

1.- Navigieren Sie zu Aktivitätssuche, und filtern Sie nach Web-Datenverkehr oder schädlichen Einstufungsereignissen. Die Analyse zeigte, dass DNS-Datenverkehr vorhanden war, aber in den letzten 30 Tagen keine Web-Datenverkehrsereignisse sichtbar waren und keine Regeln mit aktivierter Dateiinspektion identifiziert wurden.
2.- Traffic Flow > Logs on the CSA report > S3 bucket - SIEM.

Phase 2: Lizenz-Verlaufsbericht

1.- Überprüfen Sie den Lizenzverlauf in Secure Access, um alle Änderungen zu identifizieren, die mit dem Zeitpunkt des Anhaltens des Dateiereignisprotokolls übereinstimmen.

2.- Navigieren Sie zu Secure Access > Admin > Subscription, um die aktuelle Lizenzebene und die Funktionsübersicht anzuzeigen.

Die Untersuchung ergab, dass die Secure Access-Lizenz am 23. Juni 2026 von Secure Access Advantage in Secure Access Essentials geändert wurde. Dies entsprach dem Zeitpunkt, zu dem Dateiereignisprotokolle nicht mehr angezeigt wurden.

Schritt 3: Funktionsüberprüfung

Überprüfen Sie, welche Funktionen in der aktuellen Lizenzstufe enthalten sind. DLP- und IPS-Funktionen zum Generieren von Dateiereignisprotokollen sind nicht in der Secure Access Essentials-Lizenzstufe enthalten.

Schritt 4: Bestätigung und Ursache

Der Zeitpunkt der Lizenzänderung stimmte genau überein, als die Dateiereignisprotokolle nicht mehr angezeigt wurden. Da die DNS-Layer-Protokollierung weiterhin funktionierte und die primäre Anforderung war, wurde der Fall mit der Maßgabe gelöst, dass Dateiereignisprotokolle unter der aktuellen Essentials-Lizenz nicht verfügbar sind.

Ursache

Die Dateiereignisprotokolle wurden aufgrund einer Lizenzänderung von Secure Access Advantage in Secure Access Essentials am 23. Juni 2026 nicht mehr generiert. Dateiereignisprotokolle sind mit DLP- und IPS-Funktionen verknüpft, die nicht in der Essentials-Lizenzstufe enthalten sind. Durch das Lizenz-Downgrade wurde der Zugriff auf Dateiinspektionsfunktionen entfernt, die diese spezifischen Protokolltypen generieren.

Verwandte Inhalte

- Technischer Support und Downloads von Cisco

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.