SvD-Dateigrößenregeln für sicheren Zugriff ohne DatenklassifizierungÜberwachungsereignisse für Textdateien nicht generieren

Inhalt

Problem

Eine mit Dateigrößenkriterien konfigurierte Cisco Secure Access Web-DLP-Richtlinie (keine Datenklassifizierung) generiert keine DLP-Überwachungsereignisse für Uploads von TXT-Dateien, während dieselbe Richtlinie Überwachungsereignisse für andere Dateitypen wie XLSX-, PNG- und PDF-Dateien korrekt auslöst. Die betroffene Richtlinie Senior Management Policy - Web ist wie folgt konfiguriert:

- Dateikontrolle mit benutzerdefinierter Dateigröße zwischen 1 KB und 49 MB
- Keine Datenklassifizierungskriterien
- Zu überwachende Aktion festgelegt

Die Tests ergaben Folgendes:

- TXT-Datei-Uploads werden nicht in SvD-Ereignissen angezeigt, wenn Aktion = Überwachen lautet.
- Dieselben TXT-Dateien generieren SvD-Ereignisse korrekt, wenn Aktion = Sperren festgelegt ist.
- In Aktivitätsprotokollen werden alle Datei-Uploads einschließlich TXT-Dateien angezeigt.
- Andere Dateiformate (PNG, PDF, XLSX) generieren DLP-Ereignisse wie erwartet mit der Überwachungsaktion.

Wenn in SvD-Regeln keine Datenklassifizierung konfiguriert ist, zeigen die protokollierten SvD-Ereignisse unabhängig von der konfigurierten Einstellung für den Schweregrad der Regel immer den Schweregrad Mittel an.

Umwelt

- Cisco Secure Access (ehemals Cisco Umbrella)
- SvD-Webrichtlinien (Schutz vor Datenverlust)
- Richtlinien für den Internetzugriff mit aktivierter HTTPS-Entschlüsselung
- Upload-Tests über Web-Anwendungen

Auflösung

Dieses Verhalten ist nicht dokumentiert, wird aber von der Planung erwartet. MIME-Typen wie text/plain werden von der SvD-Überwachung umgangen, wenn Dateigrößenkriterien mit Überwachungsaktion verwendet werden, um eine Protokollüberlastung zu verhindern. Das Entwicklungsteam bestätigte, dass es sich um ein vorsätzliches Verhalten handelt, das nicht extern dokumentiert ist.

Problemumgehungsoptionen

Option 1 (empfohlen): Datenklassifizierung hinzufügen

Fügen Sie der SvD-Regel allgemeine Datenklassifizierungskriterien hinzu, und behalten Sie dabei Action = Monitor bei.

Dadurch wird Folgendes wiederhergestellt:

- SvD-Ereignisgenerierung für TXT-Datei
- Korrekte Behandlung des Schweregrads basierend auf der Regelkonfiguration

Option 2: Aktion zu sperren ändern

Ändern Sie die Regelaktion von Überwachen in Blockieren. Dadurch werden DLP-Ereignisse für TXT-Dateien generiert, aber auch eine Blockierung erzwungen, die bei reinen Überwachungsfällen nicht erwünscht sein kann.

Ergebnisse der Labortests

Umfassende Labortests bestätigten die Verhaltensmuster.

Testszenario 1: SvD-Regel mit Datenklassifizierung und Dateigröße (1 KB - 49 MB), Aktion = Blockieren

- TXT-Datei mit PII: Gesperrt und protokolliert
- PDF-Datei: Gesperrt und protokolliert
- TXT-Datei ohne PII: Zulässig (erwartet)
- PNG mit PII: Zulässig (basierend auf Klassifizierung erwartet)

Testszenario 2: SvD-Regel nur mit Dateigröße (keine Datenklassifizierung), Aktion = Blockieren

- Alle Dateitypen (TXT, PDF, PNG): Gesperrt und protokolliert
- Schweregrad wird trotz niedriger Regel als Mittel angezeigt.

Testszenario 3: SvD-Regel nur mit Dateigröße (keine Datenklassifizierung), Aktion = Überwachen

- TXT-Dateien: Zulässige, aber NICHT angemeldete SvD-Ereignisse
- PDF- und PNG-Dateien: Zulässige und angemeldete SvD-Ereignisse
- Aktivitätsprotokolle zeigen alle Uploads einschließlich TXT-Dateien an

Ursache

Dies ist ein absichtliches Verhalten, das in Cisco Secure Access DLP jedoch nicht dokumentiert ist. Das System umgeht die SvD-Ereignisprotokollierung für Text-/Nur-MIME-Typen, wenn nur Dateigrößenregeln mit Überwachungsaktion verwendet werden, um eine übermäßige Protokollgenerierung zu verhindern. Das Verhalten ist aktionsabhängig und MIME-typspezifisch:

- Überwachungsaktion nur anhand von Kriterien für die Dateigröße: Vom Protokollieren umgangene TXT-Dateien
- Aktion blockieren mit Kriterien, die nur die Dateigröße betreffen: TXT-Dateien normal protokolliert
- Alle Aktionen mit vorhandener Datenklassifizierung: TXT-Dateien normal protokolliert

Das Schweregrad tritt auf, da SvD-Ereignisse den Schweregrad aus Datenklassifizierungsmetadaten und nicht aus Regeleinstellungen ableiten, wenn sie im inhaltsbezogenen Modus ausgeführt werden. Ohne die Datenklassifizierung lautet der Standardwert des Systems "Mittel", unabhängig vom konfigurierten Regelschweregrad.

Verwandte Inhalte

- Konfiguration der DLP-Dateigröße für Cisco Secure Access

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.