

Las reglas de tamaño de archivo DLP de Secure Access sin clasificación de datos no generan eventos de supervisión para archivos de texto

Contenido

Problema

Una política de DLP web de Cisco Secure Access configurada sólo con criterios de tamaño de archivo (sin clasificación de datos) no genera eventos de supervisión de DLP para cargas de archivos .txt, mientras que la misma política activa correctamente eventos de supervisión para otros tipos de archivos como archivos .xlsx, .png y .pdf. La política afectada Senior Management Policy - Web está configurada con:

- Control de archivos con tamaño de archivo personalizado entre 1 KB y 49 MB
- Sin criterios de clasificación de datos
- Acción establecida en Monitor

Las pruebas revelaron que:

- Las cargas de archivos TXT no aparecen en los eventos DLP cuando Action = Monitor.
- Los mismos archivos TXT generan eventos DLP correctamente cuando Action = Block.
- Los registros de actividad muestran todas las cargas de archivos, incluidos los archivos TXT.
- Otros formatos de archivo (PNG, PDF, XLSX) generan eventos DLP según lo esperado con la acción Monitor.

Además, cuando no se configura ninguna clasificación de datos en las reglas DLP, los eventos DLP registrados siempre muestran una gravedad media, independientemente de la configuración de gravedad de la regla configurada.

Entorno

- Cisco Secure Access (anteriormente Cisco Umbrella)
- Políticas web de DLP (prevención de la pérdida de datos)
- Políticas de acceso a Internet con el descifrado HTTPS habilitado
- Pruebas de carga de archivos realizadas mediante aplicaciones web

Resolución

Este comportamiento es indocumentado, pero se espera por diseño. Los tipos MIME como texto/sin formato se omiten de la supervisión DLP cuando se utilizan criterios de sólo tamaño de archivo con la acción Supervisar para evitar la sobrecarga de registros. El equipo de desarrollo confirmó que se trata de un comportamiento intencional que no está documentado externamente.

Opciones de solución

Opción 1 (recomendada): Agregar clasificación de datos

Agregue cualquier criterio amplio de clasificación de datos a la regla DLP mientras mantiene Action = Monitor.

Esto restaura:

- Generación de eventos DLP del archivo TXT
- Control de gravedad correcto basado en la configuración de reglas

Opción 2: Cambiar acción a Bloquear

Cambie la acción de regla de Monitor a Block (Bloquear). Esto genera eventos DLP para archivos TXT, pero también aplica bloqueos que no pueden ser deseados para casos de uso solo de monitoreo.

Resultados de pruebas de laboratorio

Exhaustivas pruebas de laboratorio confirmaron los patrones de comportamiento.

Situación de prueba 1: Regla DLP con clasificación de datos y tamaño de archivo (1 KB-49 MB), acción = bloquear

- Archivo TXT con PII: Bloqueados y registrados
- Archivo PDF: Bloqueados y registrados
- Archivo TXT sin PII: Permitido (esperado)
- PNG con PII: Permitido (se espera según la clasificación)

Situación de prueba 2: Regla DLP sólo con tamaño de archivo (sin clasificación de datos), Acción = Bloquear

- Todos los tipos de archivo (TXT, PDF, PNG): Bloqueados y registrados
- La gravedad se muestra como Media a pesar de que la regla está configurada como Baja

Situación de prueba 3: Regla DLP sólo con tamaño de archivo (sin clasificación de datos), Acción = Monitor

- Archivos TXT: Eventos DLP permitidos pero NO conectados
- Archivos PDF y PNG: Eventos DLP permitidos y registrados
- Los registros de actividad muestran todas las cargas, incluidos los archivos TXT

Causa

Se trata de un comportamiento intencionado pero no documentado en Cisco Secure Access DLP. El sistema omite el registro de eventos DLP para los tipos MIME text/plain cuando utiliza reglas de sólo tamaño de archivo con la acción Supervisar para evitar la generación excesiva de registros. El comportamiento depende de la acción y es específico del tipo MIME:

- Supervisar la acción con criterios de sólo tamaño de archivo: Archivos TXT omitidos del registro
- Bloquear acción con criterios de sólo tamaño de archivo: Archivos TXT registrados normalmente
- Cualquier acción con la clasificación de datos presente: Archivos TXT registrados normalmente

El problema de gravedad se produce porque los eventos DLP derivan la gravedad de los metadatos de clasificación de datos en lugar de la configuración de reglas cuando funcionan en modo de reconocimiento de contenido. Sin la clasificación de datos, el sistema establece de forma predeterminada una gravedad "Media" independientemente de la gravedad de la regla configurada.

Contenido relacionado

- [Configuración del tamaño del archivo DLP de Cisco Secure Access](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).