Solución de problemas de DLP en tiempo real con Cisco Secure Access

Contenido

Introducción

En este documento se describen los pasos de solución de problemas de prevención de pérdida de datos (DLP) en línea o en tiempo real en el entorno de gateway web seguro (SWG).

Requisitos previos y advertencias

- Inspección de HTTPS: Asegúrese de que la inspección HTTPS está activada. DLP no puede analizar el tráfico cifrado. Asegúrese de que el sitio web se descifra con la CA raíz de Cisco Secure Access o la CA personalizada.
- Protocolo QUIC: Inhabilite el protocolo QUIC en todos los navegadores. QUIC utiliza UDP, que omite el SWG y evita el escaneo de DLP.
- IPv6: Desactive IPv6 si el tráfico no llega al SWG, ya que la funcionalidad de doble pila debe provocar desvíos.
- Política de seguridad: Asegúrese de que la regla de acceso no tenga habilitada la opción "Permitir: omitir seguridad" o "Aislamiento".

Overview

DLP en línea es una función de exploración ampliada del SWG. Supervisa o bloquea la carga de datos sensibles, confidenciales o personalmente identificables en archivos cargados a través del proxy SWG. Los clientes crean clasificaciones de datos mediante identificadores definidos por Cisco (por ejemplo, tarjetas de crédito o números de la seguridad social) o palabras clave personalizadas. Estas clasificaciones se aplican a las políticas DLP asignadas a identidades y destinos específicos. El motor DLP sólo explora los métodos HTTP POST, PUT y PATCH.

Lista de comprobación general de Troubleshooting

Si no se produce la detección de DLP, compruebe los pasos descritos:

- Conectividad: Confirme que el cliente está utilizando el SWG visitando http://policy.test.sse.cisco.com. Verifique que se haya aplicado el Data Center SWG correcto y que el resultado de la prueba muestre "protegido por Secure Access".
- Descifrado: Asegúrese de que el descifrado SSL está activado en el perfil de seguridad. Verifique que no haya exclusiones de la lista "No descifrar" o de descifrado selectivo.
- Dirección de tráfico: Asegúrese de que no haya ningún desvío de dominio externo configurado en Configuración de Internet.
- Identidad: Si las políticas DLP se basan en grupos de Active Directory, confirme que el usuario es miembro del grupo correcto.
- Configuraciones de la aplicación: Asegúrese de que la configuración de omisión de Office 365 o de compatibilidad con M365 esté deshabilitada si se está utilizando un dominio de Microsoft para DLP.
- Búsqueda de actividad: Utilice Reporting > Activity Search para asegurarse de que la URL completa esté visible (descifrada) y de que la identidad esperada esté asociada con el tráfico. Marque Reporting > Data Loss Prevention para confirmar si se registra la actividad de control o bloqueo.
- Configuración de políticas: Compruebe que la política DLP está configurada para la identidad y la aplicación de destino correctas.
- Prueba: Utilice un destino correcto conocido (por ejemplo, pastebin.com o dlptest.com) y una cadena de prueba de ejemplo válida conocida de la documentación de Cisco.
- Datos de asistencia: Recopile un archivo HAR del usuario para verificar que el tráfico se enruta a través del SWG y compruebe los encabezados SWG.

Solución de problemas de falsos negativos

Si DLP está activo pero no se activa un clasificador específico, investigue las siguientes áreas:

Clasificadores, archivos y cadenas

- Estado del archivo: Asegúrese de que el archivo no está cifrado ni no se puede analizar. Pruebe con un archivo de texto simple.
- Umbrales: Verifique los valores de Umbral y Proximidad en Política > Clasificación de datos. El clasificador puede requerir un número mayor de aciertos o proximidad a una cadena personalizada.
- Patrones de Regex: Utilice una herramienta en línea (por ejemplo, regexr.com) para visualizar patrones. Simplifique el patrón para capturar una parte más pequeña de la cadena y expandirla gradualmente.

Etiquetas de archivo

- Compatibilidad: La detección de etiquetas de archivo no funciona para Confluence o JIRA.
- Metadatos: Abra Propiedades del documento en una aplicación de Microsoft. El valor debe coincidir exactamente con la etiqueta de archivo de Umbrella; distingue entre mayúsculas y minúsculas.
- Cifrado: La detección de etiquetas no funciona para archivos cifrados o protegidos mediante contraseña.

Sitios web y destinos

- Aplicaciones compatibles: Revise la lista de aplicaciones compatibles. Para aplicaciones no compatibles o "Todos los destinos", solo se analizan tipos MIME específicos.
- Aplicaciones comprobadas: Las aplicaciones analizadas (por ejemplo, dlptest.com) se analizan de forma más exhaustiva. Los sitios web aleatorios solo se pueden analizar en busca de violaciones de archivos.
- Nombres de archivo: El sistema busca nombres de archivo sólo para determinadas aplicaciones comprobadas.

Solución de problemas de falsos positivos

Si DLP coincide con el contenido de forma inesperada, compruebe el nombre del clasificador y la regla DLP en Informes > Prevención de pérdida de datos. Si la detección es legítima pero no deseada, ajuste los valores de Umbrales o Proximidad para refinar la política.

Compatibilidad con aplicaciones de escritorio

La compatibilidad con las aplicaciones basadas en escritorio (por ejemplo, Outlook, Teams o Google Workspace) se proporciona en función del esfuerzo. La eficacia depende del formato del

mensaje utilizado durante la carga de archivos, que puede diferir entre las versiones basadas en Web y de escritorio. En el caso de las aplicaciones no analizadas, no hay garantía de que se admitan las cargas de archivos.

Gotchas clasificador DLP

- Números de tarjeta de crédito: Para la validación se utiliza el algoritmo Luhn. Realice la prueba solo con números de tarjeta de crédito válidos.
- Nombres de personas: Requiere de 2 a 3 palabras, y cada palabra debe ir en mayúsculas.
- Combinaciones de nombres: Se requiere una cadena de separación entre el nombre y otros datos (por ejemplo, "Viagra - Juan Pérez" coincide, pero "Viagra Juan Pérez" no).
- Fecha de nacimiento: Debe estar cerca de una palabra clave o encabezado como "dob" o "fecha de nacimiento".
- Contenido objetable: Ciertas cadenas de excepción impiden que se active este clasificador si el texto se asemeja a un libro o informe.
- Código postal: Debe estar cerca de palabras clave específicas relacionadas con la ubicación.

Coincidencia exacta de datos (EDM)

Antes de investigar la EDM, confirme que el análisis general de DLP funciona correctamente. Para problemas específicos de EDM, verifique que el campo "Última edición" esté actualizado en el panel y verifique la salida de la herramienta de indexación.

Uso de Comandos:

Ejecute la herramienta de indexación con la opción `-d` para generar un archivo de filtro de floración (.blm). Este comando se utiliza para validar el índice de EDM y resolver problemas por qué se deben omitir los registros. El indicador `-d` indica a la herramienta que genere el archivo de filtro de floración de diagnóstico, que debe compartirse con el soporte junto con un archivo de ejemplo o datos de la herramienta de desarrollo web/HAR.

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).