Risoluzione dei problemi di prevenzione della perdita dei dati in tempo reale con Cisco Secure Access

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi relativi alla prevenzione della perdita dei dati in linea o in tempo reale (DLP, Data Loss Prevention) all'interno dell'ambiente Secure Web Gateway (SWG).

Prerequisiti e avvisi

- Controllo HTTPS: Verificare che l'ispezione HTTPS sia abilitata. DLP non può analizzare il traffico crittografato. Verificare che il sito Web venga decrittografato con la CA radice di accesso sicuro Cisco o la CA personalizzata.
- Protocollo QUIC: Disattivare il protocollo QUIC in tutti i browser. QUIC utilizza UDP, che ignora il file SWG e impedisce la scansione DLP.
- IPv6: Disabilitare IPv6 se il traffico non colpisce il file SWG, in quanto la funzionalità dual-stack deve causare bypassaggi.
- Criterio di protezione: Verificare che per la regola di accesso non sia abilitato "Consenti - Ignora protezione" o "Isolamento".

Panoramica

Il DLP in linea è una funzione di scansione estesa del SWG. Controlla o blocca il caricamento di dati sensibili, riservati o identificabili personalmente nei file caricati tramite il proxy SWG. I clienti creano le classificazioni dei dati utilizzando identificatori definiti da Cisco (ad esempio, carte di credito o numeri di previdenza sociale) o parole chiave personalizzate. Queste classificazioni vengono applicate ai criteri di prevenzione della perdita dei dati assegnati a identità e destinazioni specifiche. Il motore DLP analizza solo i metodi HTTP POST, PUT e PATCH.

Elenco di controllo generale per la risoluzione dei problemi

Se il rilevamento della prevenzione della perdita dei dati non viene eseguito, verificare i passaggi descritti:

- Connettività: Confermare che il client sta utilizzando il file SWG visitando il sito http://policy.test.sse.cisco.com. Verificare che venga applicato il data center SWG corretto e che il risultato del test indichi che il data center è protetto da accesso protetto.
- Decrittografia: Verificare che la decrittografia SSL sia abilitata nel profilo di sicurezza. Verificare che non vi siano esclusioni dall'elenco Decrittografia selettiva o Non decrittografare.
- Traffic Steering: Verificare che non sia configurato alcun bypass del dominio esterno in Impostazioni Internet.
- Identità: Se i criteri di prevenzione della perdita dei dati si basano sui gruppi di Active Directory, verificare che l'utente sia membro del gruppo corretto.
- Impostazioni applicazione: Assicurarsi che le impostazioni di Office 365 Bypass o M365 Compatibility siano disabilitate se un dominio Microsoft viene utilizzato per DLP.
- Ricerca attività: Utilizzare Reporting > Ricerca attività per verificare che l'URL completo sia visibile (decrittografato) e che l'identità prevista sia associata al traffico. Selezionare Reporting > Prevenzione perdita dati per verificare se l'attività di monitoraggio o blocco è registrata.
- Configurazione criteri: Verificare che i criteri di prevenzione della perdita dei dati siano configurati per l'identità e l'applicazione di destinazione corrette.
- Test: Utilizzare una destinazione nota come valida (ad esempio, pastebin.com o dlptest.com) e una stringa di test di esempio nota come valida nella documentazione di Cisco.
- Dati di supporto: Raccogliere un file HAR dall'utente per verificare che il traffico sia instradato attraverso lo SWG e controllare le intestazioni SWG.

Risoluzione dei problemi relativi ai falsi negativi

Se il DLP è attivo ma un classificatore specifico non riesce ad attivarsi, esaminare le seguenti aree:

Classificatori, file e stringhe

- Stato file: Verificare che il file non sia crittografato o non possa essere analizzato. Eseguire il test con un file di testo semplice.
- Soglie: Verificare le impostazioni Soglia e Prossimità in Criterio > Classificazione dati. Il classificatore può richiedere un numero maggiore di accessi o la prossimità a una stringa personalizzata.
- Regex: Utilizzare uno strumento online (ad esempio, regexr.com) per visualizzare i modelli. Semplificate il pattern in modo da catturare una parte più piccola della stringa ed espandetelo gradualmente.

Etichette file

- Compatibilità: Il rilevamento dell'etichetta del file non funziona per Confluence o JIRA.
- Metadati: Aprire Proprietà documento in un'applicazione Microsoft. Il valore deve corrispondere esattamente all'etichetta del file Umbrella; distinzione tra maiuscole e minuscole.
- Crittografia: Il rilevamento dell'etichetta non funziona per i file protetti da password o crittografati.

Siti Web e destinazioni

- App supportate: Controllare l'elenco delle applicazioni supportate. Per le applicazioni non supportate o "Tutte le destinazioni", vengono analizzati solo tipi MIME specifici.
- Applicazioni controllate: Le applicazioni controllate (ad esempio, dlptest.com) vengono scansionate in modo più completo. I siti Web casuali possono essere analizzati solo per rilevare violazioni di file.
- Nomi file: Il sistema cerca i nomi dei file solo per alcune applicazioni controllate.

Risoluzione dei problemi relativi ai falsi positivi

Se il DLP corrisponde in modo imprevisto al contenuto, controllare il nome del classificatore e la regola DLP in Reporting > Prevenzione perdita dati. Se il rilevamento è legittimo ma indesiderato, modificare le impostazioni Soglie o Prossimità per definire meglio il criterio.

Supporto per applicazioni desktop

Il supporto per le applicazioni desktop (ad esempio, Outlook, Teams o Google Workspace) è fornito con la massima semplicità. L'efficacia dipende dal formato del messaggio utilizzato durante il caricamento dei file, che può variare a seconda della versione basata sul Web o della versione desktop. Per le applicazioni non sottoposte a controllo, non vi è alcuna garanzia che il caricamento dei file sarà supportato.

Vantaggi del classificatore DLP

- Numeri di carta di credito: Per la convalida viene utilizzato l'algoritmo Luhn. Verifica solo con numeri di carta di credito validi.
- Nomi persona: Richiede 2-3 parole e ogni parola deve essere in maiuscolo.
- Combinazioni di nomi: È necessaria una stringa di separazione tra il nome e altri dati (ad esempio, "Viagra - John Smith" corrisponde, ma "Viagra John Smith" non corrisponde).
- Data di nascita: Deve trovarsi vicino a una parola chiave o a un'intestazione, ad esempio "dob" o "data di nascita".
- Contenuto discutibile: Alcune stringhe di eccezione impediscono la generazione di questo classificatore se il testo è simile a un registro o a un report.
- CAP: Deve trovarsi in prossimità di parole chiave specifiche relative alla posizione.

Corrispondenza esatta dei dati (EDM)

Prima di esaminare l'EDM, verificare che la scansione DLP generale sia funzionale. Per problemi specifici di EDM, verificate che il campo "Ultima modifica" sia attivo nel quadro comandi e verificate l'output dello strumento di indicizzazione.

Sintassi comando:

Eseguire lo strumento di indicizzazione con l'opzione `-d` per generare un file di filtro BLOOM (.blm). Questo comando viene utilizzato per convalidare l'indice EDM e per risolvere i problemi relativi all'omissione dei record. Il flag `-d` indica allo strumento di generare l'output del file del filtro BLOM di diagnostica, che deve essere condiviso con il supporto insieme a un file di esempio o ai dati dello strumento di sviluppo HAR/Web.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).