

Regole per le dimensioni dei file DLP con accesso sicuro senza classificazione dei dati

Non generare eventi di monitoraggio per i file di testo

Sommario

Problema

I criteri di prevenzione della perdita dei dati di Cisco Secure Access Web configurati solo con i criteri relativi alle dimensioni dei file (senza classificazione dei dati) non generano eventi di monitoraggio di prevenzione della perdita dei dati per il caricamento di file con estensione txt, mentre gli stessi criteri attivano correttamente gli eventi di monitoraggio per altri tipi di file, ad esempio file con estensione xlsx, png e pdf. Il criterio interessato Criteri gestione avanzata - Web è configurato con:

- Controllo file con dimensioni personalizzate comprese tra 1 KB e 49 MB
- Nessun criterio di classificazione dei dati
- Set di azioni da monitorare

I test hanno rivelato che:

- I caricamenti di file TXT non vengono visualizzati negli eventi DLP quando Action = Monitor.
- Gli stessi file TXT generano correttamente gli eventi DLP quando Action = Block.
- Nei log attività vengono visualizzati tutti i file caricati, inclusi i file TXT.
- Altri formati di file (PNG, PDF, XLSX) generano eventi DLP come previsto con l'azione Monitor.

Inoltre, quando nelle regole di prevenzione della perdita dei dati non è configurata alcuna classificazione dei dati, gli eventi di prevenzione della perdita dei dati registrati mostrano sempre il livello di gravità Medio indipendentemente dall'impostazione di severità della regola configurata.

Ambiente

- Cisco Secure Access (in precedenza Cisco Umbrella)
- Criteri Web DLP (Data Loss Prevention)
- Criteri di accesso a Internet con decrittografia HTTPS abilitata
- Test di caricamento dei file eseguiti tramite applicazioni Web

Risoluzione

Questo comportamento non è documentato ma previsto dalla progettazione. I tipi MIME come text/plain vengono ignorati dal monitoraggio DLP quando si utilizzano criteri di sola dimensione file con l'azione Esegui monitoraggio per evitare l'overload del log. Il team di sviluppo ha confermato che si tratta di un comportamento intenzionale non documentato esternamente.

Opzioni per la soluzione

Opzione 1 (consigliata): Aggiungi classificazione dati

Aggiungere criteri di classificazione dati generali alla regola di prevenzione della perdita dei dati mantenendo Action = Monitor.

In questo modo viene ripristinato:

- Generazione di eventi DLP con file TXT
- Correggi la gestione della gravità in base alla configurazione della regola

Opzione 2: Blocca azione

Modificare l'azione della regola da Monitoraggio a Blocco. Questo genera eventi DLP per i file TXT, ma applica anche il blocco che non può essere desiderato per casi di solo monitoraggio.

Risultati dei test di laboratorio

Esaurienti test di laboratorio hanno confermato i modelli comportamentali.

Scenario di test 1: Regola di prevenzione della perdita dei dati con classificazione dei dati e dimensioni del file (1 KB-49 MB), azione = blocco

- File TXT con PII: Bloccato e registrato
- File PDF: Bloccato e registrato
- File TXT senza PII: Consentito (previsto)
- PNG con PII: Consentito (previsto in base alla classificazione)

Scenario di test 2: Regola di prevenzione della perdita dei dati solo con dimensioni file (senza classificazione dati), azione = blocco

- Tutti i tipi di file (TXT, PDF, PNG): Bloccato e registrato
- Il livello di gravità viene visualizzato come Medio nonostante la regola sia configurata come Basso

Scenario di test 3: Regola di prevenzione della perdita dei dati solo con le dimensioni del file (senza classificazione dei dati), azione = monitoraggio

- File TXT: Consentiti ma NON registrati negli eventi DLP
- File PDF e PNG: Eventi DLP consentiti e registrati
- I log attività mostrano tutti i caricamenti, inclusi i file TXT

Causa

Si tratta di un comportamento intenzionale ma non documentato in Cisco Secure Access DLP. Il sistema ignora la registrazione degli eventi DLP per i tipi MIME di testo/semplificato quando utilizza regole di sola dimensione file con l'azione Esegui monitoraggio per evitare un'eccessiva generazione di log. Il comportamento è dipendente dall'azione e specifico per il tipo MIME:

- Esegui monitoraggio azione con criteri di sola dimensione file: File TXT ignorati dalla registrazione
- Azione di blocco con criteri di sola dimensione file: File TXT registrati normalmente
- Qualsiasi azione con la classificazione dei dati presente: File TXT registrati normalmente

Il problema di gravità si verifica perché gli eventi DLP derivano la gravità dai metadati di classificazione dei dati anziché dalle impostazioni delle regole quando si opera in modalità di riconoscimento del contenuto. Senza la classificazione dei dati, per impostazione predefinita il sistema imposta la gravità "Media" indipendentemente dalla gravità della regola configurata.

Contenuto correlato

- [Configurazione delle dimensioni dei file DLP di Cisco Secure Access](#)

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).