

Règles de taille de fichier DLP à accès sécurisé sans classification des données Ne pas générer d'événements de surveillance pour les fichiers texte

Table des matières

Problème

Une stratégie Cisco Secure Access Web DLP configurée avec des critères de taille de fichier uniquement (sans classification des données) ne génère pas d'événements de surveillance DLP pour les téléchargements de fichiers .txt, alors que la même stratégie déclenche correctement des événements de surveillance pour d'autres types de fichiers tels que les fichiers .xlsx, .png et .pdf. La politique concernée Politique de la haute direction - Web est configurée avec :

- Contrôle de fichier avec taille de fichier personnalisée comprise entre 1 Ko et 49 Mo
- Aucun critère de classification des données
- Action définie sur Surveillance

Les tests ont révélé que :

- Les téléchargements de fichiers TXT n'apparaissent pas dans les événements DLP lorsque Action = Surveillance.
- Les mêmes fichiers TXT génèrent correctement des événements DLP lorsque Action = Block.
- Les journaux d'activité affichent tous les téléchargements de fichiers, y compris les fichiers TXT.
- D'autres formats de fichier (PNG, PDF, XLSX) génèrent des événements DLP comme prévu avec l'action Surveiller.

En outre, lorsqu'aucune classification des données n'est configurée dans les règles DLP, les

événements DLP enregistrés affichent toujours un niveau de gravité moyen, quel que soit le paramètre de gravité de règle configuré.

Environnement

- Cisco Secure Access (anciennement Cisco Umbrella)
- Stratégies Web DLP (Data Loss Prevention)
- Politiques d'accès Internet avec déchiffrement HTTPS activé
- Tests de téléchargement de fichiers effectués via des applications Web

Résolution

Ce comportement n'est pas documenté mais est attendu dès la conception. Les types MIME tels que text/plain sont ignorés de la surveillance DLP lors de l'utilisation de critères de taille de fichier uniquement avec l'action Surveillance pour empêcher la surcharge du journal. L'équipe de développement a confirmé qu'il s'agit d'un comportement intentionnel qui n'est pas documenté en externe.

Options de contournement

Option 1 (recommandée) : Ajouter une classification de données

Ajoutez des critères généraux de classification des données à la règle DLP tout en conservant Action = Surveillance.

Cette opération restaure :

- Génération d'événements DLP de fichier TXT

- Traitement de gravité correct en fonction de la configuration des règles

Option 2: Modifier l'action en blocage

Modifiez l'action de la règle de Moniteur à Bloquer. Cela génère des événements DLP pour les fichiers TXT, mais impose également le blocage qui ne peut pas être souhaité pour les cas d'utilisation de surveillance uniquement.

Résultats des tests en laboratoire

Des tests de laboratoire complets ont confirmé les comportements.

Scénario de test 1 : Règle DLP avec classification des données et taille de fichier (1 Ko-49 Mo),
Action = Bloquer

- Fichier TXT avec PII : Bloqué et consigné
- Fichier PDF : Bloqué et consigné
- Fichier TXT sans PII : Autorisé (attendu)
- PNG avec PII : Autorisé (attendu en fonction de la classification)

Scénario de test 2 : Règle DLP avec taille de fichier uniquement (sans classification des données),
Action = Bloquer

- Tous les types de fichiers (TXT, PDF, PNG) : Bloqué et consigné
- La gravité affiche Moyen malgré la règle configurée sur Faible

Scénario de test 3 : Règle DLP avec taille de fichier uniquement (sans classification des données),

Action = Surveillance

- Fichiers TXT : Événements DLP autorisés mais NON connectés
- Fichiers PDF et PNG : Événements DLP autorisés et connectés
- Les journaux d'activité affichent tous les téléchargements, y compris les fichiers TXT

Motif

Ce comportement est intentionnel mais non documenté dans Cisco Secure Access DLP. Le système ignore la journalisation des événements DLP pour les types MIME texte/clair lorsqu'il utilise des règles de taille de fichier uniquement avec l'action Surveiller pour empêcher la génération excessive de journaux. Le comportement dépend de l'action et est spécifique au type MIME :

- Surveiller l'action avec des critères de taille de fichier uniquement : Fichiers TXT ignorés de la journalisation
- Action de blocage avec des critères de taille de fichier uniquement : Fichiers TXT enregistrés normalement
- Toute action associée à la classification des données présente : Fichiers TXT enregistrés normalement

Le problème de gravité se produit parce que les événements DLP dérivent la gravité des métadonnées de classification des données plutôt que des paramètres de règle lorsqu'ils fonctionnent en mode de reconnaissance du contenu. Sans la classification des données, le système prend par défaut la valeur « Moyen », quel que soit le niveau de gravité de la règle configurée.

Autres informations utiles

- [Configuration de la taille du fichier DLP Cisco Secure Access](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.