Résolution des problèmes DLP en temps réel avec Cisco Secure Access

Table des matières

Introduction

Ce document décrit les étapes de dépannage pour les problèmes de prévention des pertes de données en ligne ou en temps réel (DLP) dans l'environnement Secure Web Gateway (SWG).

Conditions préalables et avertissements

- Inspection HTTPS : Assurez-vous que l'inspection HTTPS est activée. DLP ne peut pas analyser le trafic chiffré. Assurez-vous que le site Web est déchiffré avec l'autorité de certification racine Cisco Secure Access ou l'autorité de certification personnalisée.
- Protocole QUIC : Désactivez le protocole QUIC dans tous les navigateurs. QUIC utilise le protocole UDP, qui contourne le SWG et empêche l'analyse DLP.
- IPv6 : Désactivez IPv6 si le trafic n'atteint pas le SWG, car la fonctionnalité de double pile doit provoquer des contournements.
- Stratégie de sécurité : Assurez-vous que les options Autoriser - Remplacer la sécurité ou Isolation ne sont pas activées pour la règle d'accès.

Aperçu

La DLP en ligne est une fonction de numérisation étendue du SWG. Il surveille ou bloque le téléchargement de données sensibles, confidentielles ou personnellement identifiables dans des fichiers téléchargés via le proxy SWG. Les clients créent des classifications de données à l'aide d'identifiants définis par Cisco (par exemple, des cartes de crédit ou des numéros de sécurité sociale) ou de mots clés personnalisés. Ces classifications sont appliquées aux stratégies DLP affectées à des identités et destinations spécifiques. Le moteur DLP analyse uniquement les méthodes HTTP POST, PUT et PATCH.

Liste générale de dépannage

Si la détection DLP n'a pas lieu, vérifiez les étapes décrites ci-dessous :

- Connectivité : Vérifiez que le client utilise le SWG en visitant http://policy.test.sse.cisco.com. Vérifiez que le centre de données SWG correct est appliqué et que le résultat du test indique « protégé par un accès sécurisé ».
- Déchiffrement : Assurez-vous que le décodage SSL est activé dans le profil de sécurité. Vérifiez qu'il n'y a pas d'exclusions de la liste Déchiffrement sélectif ou Ne pas déchiffrer.
- Orientation du trafic : Assurez-vous qu'aucun contournement de domaine externe n'est configuré dans les paramètres Internet.
- Identité : Si les stratégies DLP reposent sur des groupes Active Directory, vérifiez que l'utilisateur est membre du groupe approprié.
- Paramètres d'application: Assurez-vous que les paramètres de contournement Office 365 ou de compatibilité M365 sont désactivés si un domaine Microsoft est utilisé pour DLP.
- Recherche d'activité : Utilisez Reporting > Activity Search pour vous assurer que l'URL complète est visible (décryptée) et que l'identité attendue est associée au trafic. Cochez Reporting > Data Loss Prevention pour confirmer si l'activité de surveillance ou de blocage est consignée.
- Configuration de la stratégie : Vérifiez que la stratégie DLP est configurée pour l'identité et l'application de destination correctes.
- Test : Utilisez une destination correcte connue (par exemple, pastebin.com ou dlptest.com) et une chaîne de test d'exemple valide connue provenant de la documentation Cisco.
- Données de support : Recueillez un fichier HAR auprès de l'utilisateur pour vérifier que le trafic est acheminé via le SWG et recherchez les en-têtes SWG.

Dépanner les faux négatifs

Si DLP est actif mais qu'un classifieur spécifique ne se déclenche pas, examinez les points suivants :

Classificateurs, fichiers et chaînes

- État du fichier : Assurez-vous que le fichier n'est pas chiffré ou ne peut pas être analysé. Testez avec un simple fichier texte.
- Seuils : Vérifiez les paramètres Seuil et proximité dans Politique > Classification des données. Le classificateur peut nécessiter un nombre plus élevé de résultats ou une proximité avec une chaîne personnalisée.
- Modèles Regex : Utilisez un outil en ligne (par exemple, regexr.com) pour visualiser des modèles. Simplifiez le motif pour attraper une partie plus petite de la chaîne et développez progressivement.

Étiquettes de fichier

- Compatibilité : La détection d'étiquette de fichier ne fonctionne pas pour Confluence ou JIRA.
- Métadonnées : Ouvrez Propriétés du document dans une application Microsoft. La valeur doit correspondre exactement à l'étiquette Fichier Umbrella ; cette option est sensible à la casse.
- Chiffrement : La détection d'étiquette ne fonctionne pas pour les fichiers protégés par mot de passe ou chiffrés.

Sites Web et destinations

- Applications prises en charge : Consultez la liste des applications prises en charge. Pour les applications non prises en charge ou « Toutes les destinations », seuls les types MIME spécifiques sont analysés.
- Applications vérifiées : Les applications vérifiées (par exemple, dlptest.com) sont analysées de manière plus complète. Les sites Web aléatoires ne peuvent être analysés que pour détecter les violations de fichiers.
- Noms des fichiers : Le système recherche les noms de fichiers uniquement pour certaines applications contrôlées.

Dépanner les faux positifs

Si DLP correspond au contenu de manière inattendue, vérifiez le nom du classifieur et la règle DLP dans Reporting > Data Loss Prevention. Si la détection est légitime mais indésirable, ajustez les paramètres Seuils ou Proximité pour affiner la stratégie.

Prise en charge des applications bureautiques

La prise en charge des applications de bureau (par exemple, Outlook, Teams ou Google Workspace) est assurée au mieux. L'efficacité dépend du format de message utilisé lors du téléchargement des fichiers, qui peut varier entre les versions Web et les versions de bureau. Pour les applications non approuvées, rien ne garantit que les téléchargements de fichiers seront pris en charge.

Objets récupérés du classificateur DLP

- Numéros de carte de crédit : L'algorithme de Luhn est utilisé pour la validation. Tester uniquement avec des numéros de carte de crédit valides.
- Noms des personnes : Nécessite de 2 à 3 mots et chaque mot doit être en majuscules.
- Combinaisons de noms : Une chaîne de séparation est requise entre le nom et les autres données (par exemple, « Viagra - John Smith » correspond, mais pas « Viagra John Smith »).
- Date de naissance : Doit se trouver à proximité d'un mot clé ou d'un en-tête tel que « dob » ou « date de naissance ».
- Contenu répréhensible : Certaines chaînes d'exception empêchent le déclenchement de ce classifieur si le texte ressemble à un livre ou à un état.
- Code postal : Doit se trouver à proximité de mots-clés spécifiques relatifs à l'emplacement.

Correspondance exacte des données (EDM)

Avant d'examiner l'EDM, vérifiez que l'analyse DLP générale est fonctionnelle. Pour les problèmes spécifiques à l'EDM, vérifiez que le champ "Dernière modification" est actif dans le tableau de bord et vérifiez la sortie de l'outil d'indexation.

Utilisation des commandes :

Exécutez l'outil d'indexation avec l'option `-d` pour générer un fichier de filtre de bloom (.blm). Cette commande permet de valider l'index EDM et de déterminer pourquoi les enregistrements doivent être ignorés. L'indicateur `-d` indique à l'outil de sortir le fichier de filtre de bloom de diagnostic, qui doit être partagé avec le support avec un fichier d'exemple ou des données d'outil de développement HAR/Web.

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.