Surveiller l'exposition des données sensibles dans AWS S3 et Azure Storage avec DLP

Table des matières

Introduction

Ce document décrit comment surveiller l'exposition des données sensibles dans AWS S3 et Azure Storage à l'aide de Data Loss Prevention (DLP).

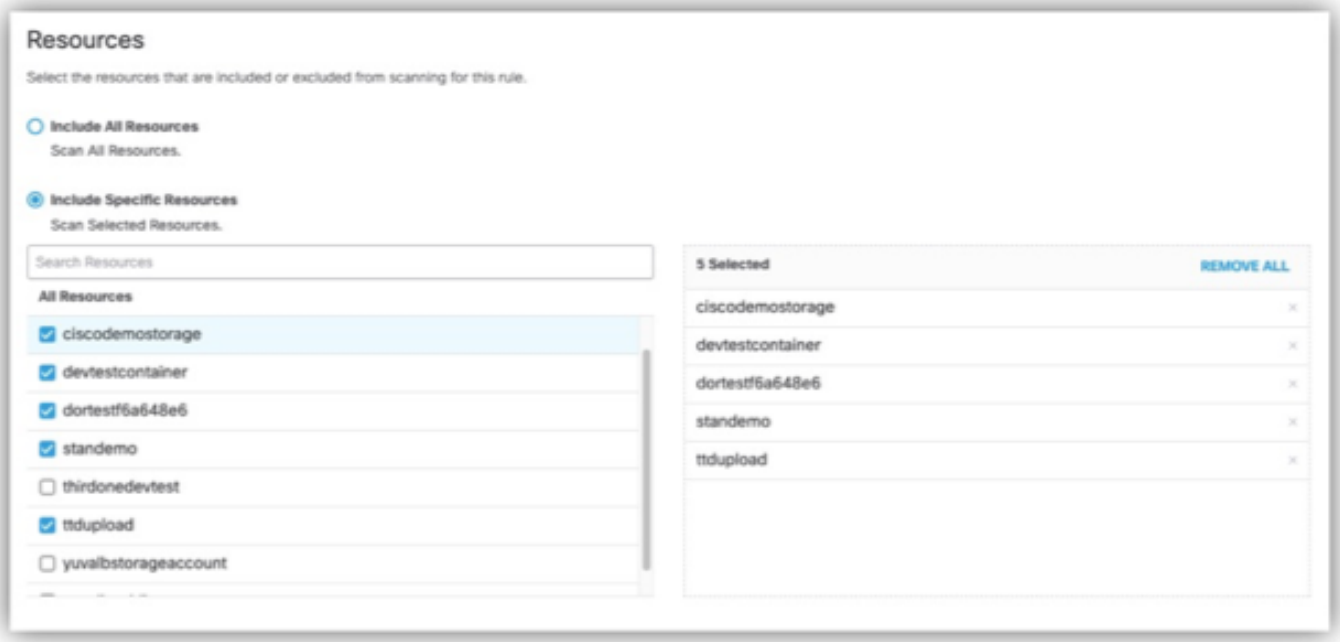
Aperçu

Avec les nouveaux connecteurs pour AWS S3 et Azure Storage, vous pouvez désormais rechercher l'exposition des données sensibles dans vos environnements cloud. Ces fonctionnalités vous aident à découvrir et à surveiller les informations d'identification exposées (clés API, secrets et jetons, par exemple), ainsi que les données sensibles, notamment les informations d'identification personnelle (PII), les dossiers financiers et les informations médicales susceptibles d'être exposées au Web public.

Qu'est-ce qui est analysé dans AWS S3 et Azure File Storage ?

- AWS S3 :
  DLP effectue à la fois une analyse de détection initiale pour les données sensibles préexistantes et une surveillance continue pour les fichiers nouveaux ou mis à jour. Vous pouvez spécifier les compartiments S3 à analyser en les sélectionnant dans votre règle DLP.
- Stockage de fichiers Azure :
  DLP prend en charge la détection initiale et la surveillance continue des fichiers nouveaux ou mis à jour. Vous pouvez choisir les conteneurs Azure spécifiques à analyser dans votre règle DLP.

Vous pouvez personnaliser l'analyse DLP en sélectionnant les compartiments AWS S3 ou les conteneurs Azure exacts en fonction de vos besoins et priorités.



Actions de réponse prises en charge pour AWS et Azure

Actuellement, seule la surveillance est prise en charge en tant qu'action de réponse pour AWS S3 et Azure Storage. Les actions correctives automatiques, telles que la suppression de fichiers ou la mise en quarantaine, ne sont pas disponibles. Cette approche évite le risque de perturber les environnements IaaS critiques tout en vous permettant de surveiller efficacement l'exposition des données sensibles.

Localisez les compartiments AWS S3 et les objets blob de stockage Azure pour une correction manuelle

Pour faciliter la correction manuelle, le rapport DLP inclut des informations détaillées :

- Le rapport affiche le nom réel du bucket S3 ou de l'objet blob, ce qui facilite la recherche dans les consoles AWS ou Azure.
- Chaque événement de violation DLP fournit le nom de la ressource, l'URL de destination et, le cas échéant, l'ID de la ressource.
- Utilisez ces informations pour localiser et traiter efficacement les violations DLP au sein de vos compartiments AWS S3 et des objets blob de stockage Azure.

Ressources connexes

Reportez-vous à la documentation Umbrella pour obtenir des instructions détaillées :

- Activer la protection contre la perte de données des API SaaS pour les locataires AWS
- Activer la protection contre la perte de données de l'API SaaS pour les locataires Azure

- Ajouter une règle d'API SaaS à la stratégie de prévention de perte de données
- Rapport Data Loss Prevention

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.