Bewaak gevoelige gegevens in AWS S3 en Azure Storage met DLP

Inhoud

Inleiding

In dit document wordt beschreven hoe u de blootstelling aan gevoelige gegevens in AWS S3 en Azure Storage kunt bewaken met behulp van Data Loss Prevention (DLP).

Overzicht

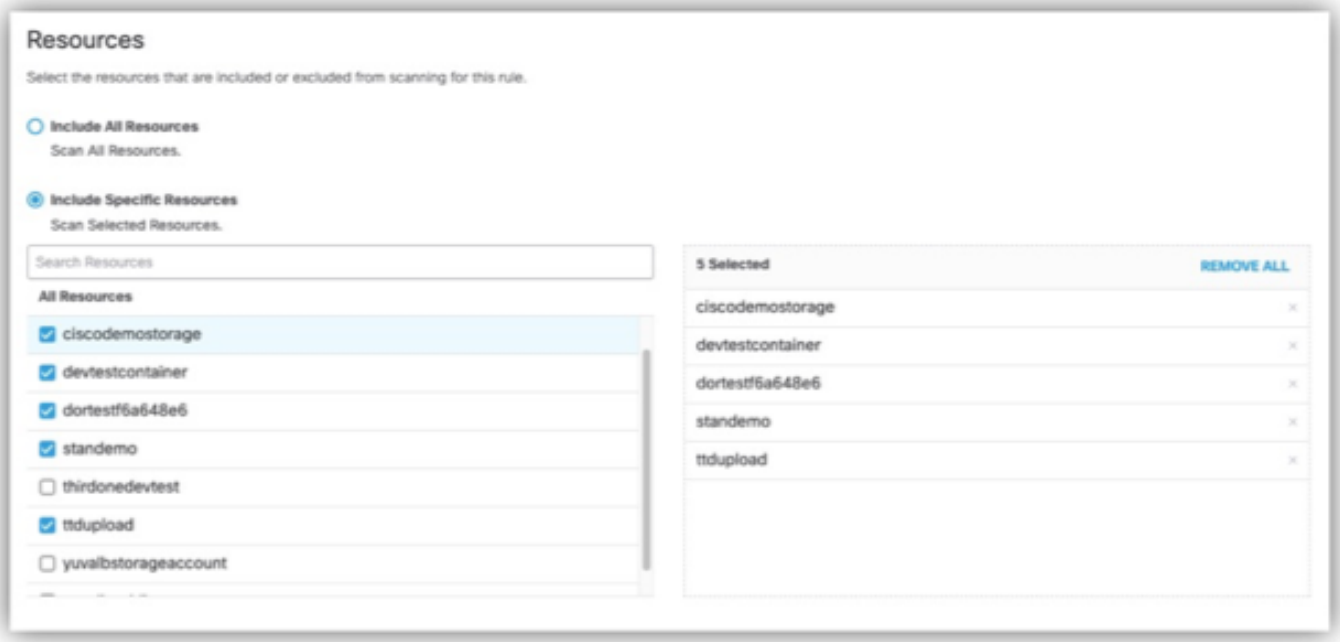
Met nieuwe connectors voor AWS S3 en Azure Storage kunt u nu scannen op gevoelige gegevensblootstelling in uw cloudomgevingen. Deze mogelijkheden helpen u blootgestelde referenties te ontdekken en te bewaken, zoals API-sleutels, geheimen en tokens, evenals gevoelige gegevens, waaronder persoonlijk identificeerbare informatie (PII), financiële gegevens en gezondheidsinformatie die kan worden blootgesteld aan het openbare web.

Wat wordt gescand in AWS S3 en Azure File Storage?

- AWS S3:
  DLP voert zowel een eerste detectiescan uit voor reeds bestaande gevoelige gegevens als continue monitoring voor nieuwe of bijgewerkte bestanden. U kunt opgeven welke S3-emmers u wilt scannen door ze te selecteren in uw DLP-regel.

- Azure File Storage:
  DLP ondersteunt de eerste detectie en doorlopende bewaking van nieuwe of bijgewerkte bestanden. U kunt de specifieke Azure-containers kiezen om te scannen binnen uw DLP-regel.

U kunt DLP-scanning aanpassen door de exacte AWS S3-emmers of Azure-containers te selecteren om aan uw behoeften en prioriteiten te voldoen.



Ondersteunde responsacties voor AWS en Azure

Momenteel wordt alleen bewaking ondersteund als een responsactie voor AWS S3 en Azure Storage. Automatische herstelacties, zoals het verwijderen van bestanden of quarantaine, zijn niet beschikbaar. Deze aanpak voorkomt het risico dat bedrijfskritieke IaaS-omgevingen worden verstoord, terwijl u toch de blootstelling aan gevoelige gegevens effectief kunt bewaken.

Zoek AWS S3-emmers en Azure Storage Blobs voor handmatig herstel

Voor hulp bij handmatige probleemoplossing bevat het DLP-rapport gedetailleerde informatie:

- Het rapport geeft de werkelijke S3-bucket of blob-naam weer, waardoor het gemakkelijk is om te zoeken in AWS- of Azure-consoles.
- Elke DLP-overtreding geeft de bronnaam, de bestemmings-URL en, indien beschikbaar, de bron-ID.
- Gebruik deze informatie om DLP-overtredingen efficiënt te lokaliseren en aan te pakken in uw AWS S3-emmers en Azure-opslagblobs.

Gerelateerde bronnen

Raadpleeg de documentatie van de paraplu voor gedetailleerde richtlijnen:

- SaaS API Data Loss Protection inschakelen voor AWS-huurders
- SaaS API Data Loss Protection voor Azure-huurders inschakelen
- Een SaaS API-regel toevoegen aan het beleid voor het voorkomen van gegevensverlies

- Rapport Preventie van gegevensverlies

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.