Monitore a exposição de dados confidenciais no AWS S3 e no Armazenamento do Azure com DLP

Contents

Introdução

Este documento descreve como monitorar a exposição de dados confidenciais no AWS S3 e no Armazenamento do Azure usando a Prevenção de Perda de Dados (DLP).

Overview

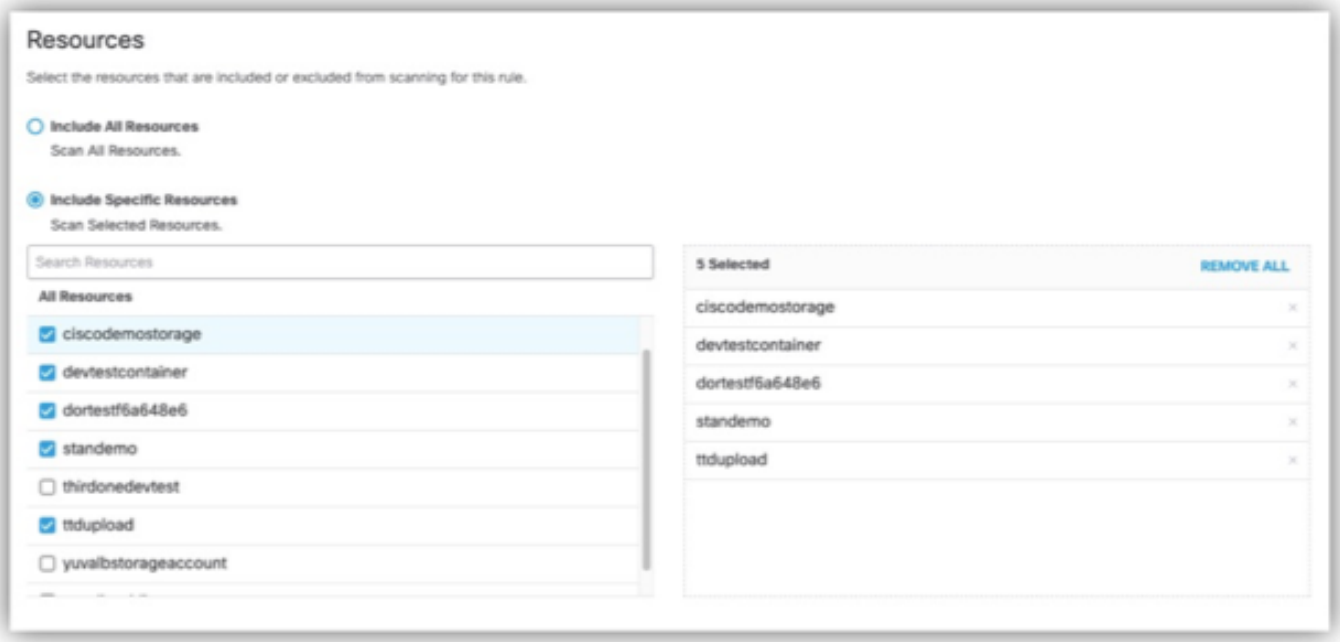
Com os novos conectores para o AWS S3 e o Armazenamento do Azure, agora você pode verificar a exposição de dados confidenciais em seus ambientes de nuvem. Esses recursos ajudam a descobrir e monitorar credenciais expostas, como chaves de API, segredos e tokens, bem como dados confidenciais, incluindo informações pessoais identificáveis (PII), registros financeiros e informações de saúde que possam ser expostas à Web pública.

O que é verificado no armazenamento de arquivos do AWS S3 e do Azure?

- AWS S3:
  O DLP executa uma verificação de detecção inicial para dados confidenciais preexistentes e monitoramento contínuo para arquivos novos ou atualizados. É possível especificar quais buckets S3 serão verificados selecionando-os em sua regra DLP.

- Armazenamento de Arquivos do Azure:
  O DLP oferece suporte à detecção inicial e ao monitoramento contínuo de arquivos novos ou atualizados. Você pode escolher os contêineres do Azure específicos para verificar dentro de sua regra PPD.

Você pode personalizar a verificação DLP selecionando os recipientes exatos do AWS S3 ou do Azure para atender às suas necessidades e prioridades.



Ações de Resposta com Suporte para AWS e Azure

Atualmente, somente o monitoramento tem suporte como uma ação de resposta para o AWS S3 e o Armazenamento do Azure. Ações de correção automática, como exclusão de arquivo ou quarentena, não estão disponíveis. Essa abordagem evita o risco de interromper ambientes de IaaS de missão crítica, permitindo ainda que você monitore a exposição de dados confidenciais com eficiência.

Localize os buckets do AWS S3 e os blobs de armazenamento do Azure para correção manual

Para auxiliar na correção manual, o relatório DLP inclui informações detalhadas:

- O relatório exibe o nome real do bucket ou blob do S3, facilitando a pesquisa nos consoles AWS ou Azure.
- Cada evento de violação de DLP fornece o nome do recurso, o URL de destino e, quando disponível, o ID do recurso.
- Use essas informações para localizar e resolver violações de DLP de forma eficiente em seus buckets AWS S3 e blobs de armazenamento do Azure.

Recursos relacionados

Consulte a documentação do Umbrella para obter orientações detalhadas:

- Habilitar proteção contra perda de dados da API SaaS para usuários AWS
- Habilitar Proteção contra Perda de Dados da API SaaS para Locatários do Azure

- Adicionar uma regra de API de SaaS à política de prevenção de perda de dados
- Relatório de Prevenção de Perda de Dados

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.