Monitore os riscos de malware no AWS S3 e no armazenamento do Azure com malware na nuvem

Contents

Introdução

Este documento descreve como monitorar e lidar com os riscos de malware no AWS S3 e no Armazenamento do Azure com malware na nuvem.

Overview

Com esse recurso, agora você pode descobrir e monitorar os riscos de malware em seus ambientes AWS S3 e Armazenamento do Azure. Um caso de uso importante é a identificação de arquivos infectados com malware que podem roubar credenciais ou explorar vulnerabilidades, aumentando o risco de movimentação lateral dentro do seu ambiente ou para outros ambientes.

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 limitação evita a interrupção acidental de serviços de missão crítica e ainda permite monitorar a exposição de dados confidenciais e os riscos de malware.

Recursos relacionados

- Habilitar Proteção contra Malware na Nuvem para Locatários AWS
- Habilitar Proteção contra Malware na Nuvem para Locatários do Azure

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.