Supervise los riesgos de malware en AWS S3 y Azure Storage con malware en la nube

Contenido

Introducción

Este documento describe cómo supervisar y abordar los riesgos de malware en AWS S3 y Azure Storage con malware en la nube.

Overview

Con esta función, ahora puede descubrir y supervisar los riesgos de malware en sus entornos de AWS S3 y Azure Storage. Un caso práctico clave es la identificación de archivos infectados con malware que pueden robar credenciales o aprovechar vulnerabilidades, lo que aumenta el riesgo de movimientos laterales dentro de su entorno o a otros entornos.

Acciones de respuesta admitidas para AWS y Azure

Actualmente, solo se admite la supervisión como acción de respuesta para AWS S3 y Azure Storage. Las acciones de remediación automáticas, como la eliminación de archivos o la cuarentena, no están disponibles. Esta limitación evita la interrupción accidental de servicios críticos al tiempo que le permite supervisar la exposición de datos confidenciales y los riesgos de malware.

Recursos relacionados

- Habilitar protección frente a malware en la nube para arrendatarios de AWS
- Habilitar Protección frente a malware en la nube para arrendatarios de Azure

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).