Surveiller les risques de programmes malveillants dans AWS S3 et Azure Storage avec les programmes malveillants cloud

Table des matières

Introduction

Ce document décrit comment surveiller et gérer les risques de programmes malveillants dans AWS S3 et Azure Storage avec les programmes malveillants du cloud.

Aperçu

Grâce à cette fonctionnalité, vous pouvez désormais détecter et surveiller les risques de programmes malveillants dans vos environnements AWS S3 et Azure Storage. Un exemple d'utilisation clé est l'identification des fichiers infectés par un programme malveillant qui peut voler des informations d'identification ou exploiter des vulnérabilités, augmentant ainsi le risque de déplacement latéral au sein de votre environnement ou vers d'autres environnements.

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 limitation empêche l'interruption accidentelle des services critiques tout en vous permettant de surveiller l'exposition aux données sensibles et les risques de programmes malveillants.

Ressources connexes

- Activer la protection contre les programmes malveillants cloud pour les locataires AWS
- Activer la protection contre les programmes malveillants cloud pour les locataires Azure

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.