使用云恶意软件监控AWS S3和Azure存储中的恶意软件风险

目录

简介

本文档介绍如何监控和解决带有云恶意软件的AWS S3和Azure存储中的恶意软件风险。

概述

借助此功能，您现在可以在AWS S3和Azure存储环境中发现并监控恶意软件风险。一个关键使用案例是识别受恶意软件感染的文件，这些文件可能会窃取凭据或利用漏洞，从而增加在您的环境中横向移动或移动至其他环境的风险。

AWS和Azure支持的响应操作

目前，仅支持监控作为AWS S3和Azure存储的响应操作。自动补救操作（如文件删除或隔离）不可用。此限制可防止任务关键型服务意外中断，同时仍允许您监控敏感数据泄露和恶意软件风险。

相关资源

- 为AWS租户启用云恶意软件防护
- 为Azure租户启用云恶意软件保护

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。