클라우드 악성코드를 사용하여 AWS S3 및 Azure Storage에서 악성코드 위험 모니터링

목차

소개

이 문서에서는 AWS S3 및 Azure Storage에서 클라우드 악성코드를 사용하여 악성코드 위험을 모니터링하고 해결하는 방법에 대해 설명합니다.

개요

이제 이 기능을 사용하여 AWS S3 및 Azure Storage 환경 내에서 악성코드 위험을 검색하고 모니터링할 수 있습니다. 주요 활용 사례는 자격 증명을 훔치거나 취약점을 악용할 수 있는 악성코드에 감염된 파일을 식별하여 환경 내에서 또는 다른 환경으로 측면 이동할 위험을 높이는 것입니다.

AWS 및 Azure에 대해 지원되는 응답 작업

현재 AWS S3 및 Azure Storage에 대한 응답 작업으로 모니터링만 지원됩니다. 파일 삭제 또는 격리 같은 자동 교정 작업은 사용할 수 없습니다. 이러한 제한으로 인해 미션 크리티컬 서비스가 실수로 중단되는 것을 방지할 수 있으며, 민감한 데이터 노출 및 악성코드 위험을 모니터링할 수 있습니다.

관련 리소스

- AWS 테넌트를 위한 클라우드 악성코드 차단 활성화
- Azure 테넌트에 대해 클라우드 악성코드 차단 사용

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.