DLP를 사용하여 AWS S3 및 Azure Storage에서 민감한 데이터 노출 모니터링

목차

소개

이 문서에서는 DLP(데이터 손실 방지)를 사용하여 AWS S3 및 Azure Storage에서 민감한 데이터 노출을 모니터링하는 방법에 대해 설명합니다.

개요

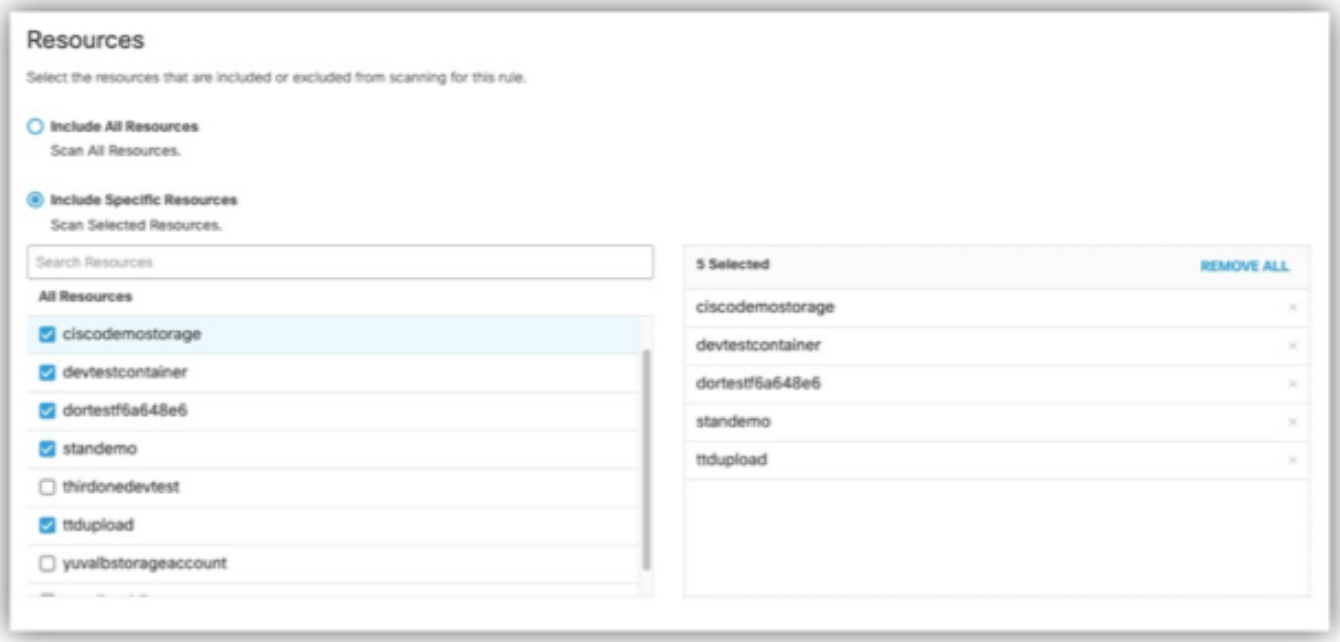
AWS S3 및 Azure Storage용 새 커넥터를 사용하면 클라우드 환경 내에서 민감한 데이터 노출을 검사할 수 있습니다. 이러한 기능을 통해 API 키, 비밀, 토큰과 같은 노출된 자격 증명은 물론 PII(Personally Identifiable Information), 재무 기록, 공개 웹에 노출될 수 있는 의료 정보를 비롯한 민감한 데이터를 검색하고 모니터링할 수 있습니다.

AWS S3 및 Azure File Storage에서 무엇이 스캔됩니까?

- AWS S3
  DLP는 기존의 민감한 데이터에 대한 초기 검색 검사와 새로운 파일 또는 업데이트된 파일에 대한 지속적인 모니터링을 모두 수행합니다. DLP 규칙에서 S3 버킷을 선택하여 스캔할 S3 버킷을 지정할 수 있습니다.

- Azure 파일 저장소:
  DLP는 신규 또는 업데이트된 파일에 대한 초기 검색 및 지속적인 모니터링을 지원합니다. DLP 규칙 내에서 스캔할 특정 Azure 컨테이너를 선택할 수 있습니다.

요구 사항과 우선 순위에 맞는 정확한 AWS S3 버킷 또는 Azure 컨테이너를 선택하여 DLP 검사를 맞춤화할 수 있습니다.



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 접근 방식을 통해 미션 크리티컬 IaaS 환경을 중단하는 위험을 방지하는 동시에 민감한 데이터 노출을 효과적으로 모니터링할 수 있습니다.

수동 교정을 위해 AWS S3 버킷 및 Azure Storage Blob 찾기

수동 교정을 지원하기 위해 DLP 보고서에는 다음과 같은 자세한 정보가 포함됩니다.

- 보고서에는 실제 S3 버킷 또는 blob 이름이 표시되므로 AWS 또는 Azure 콘솔에서 쉽게 검색할 수 있습니다.
- 각 DLP 위반 이벤트는 리소스 이름, 대상 URL, 사용 가능한 경우 리소스 ID를 제공합니다.
- 이 정보를 사용하여 AWS S3 버킷 및 Azure 저장소 blob 내에서 DLP 위반을 효율적으로 찾고 해결할 수 있습니다.

관련 리소스

자세한 지침은 Umbrella 설명서를 참조하십시오.

- AWS 테넌트를 위한 SaaS API 데이터 손실 방지 활성화
- Azure 테넌트에 대해 SaaS API 데이터 손실 방지 사용
- 데이터 손실 방지 정책에 SaaS API 규칙 추가
- 데이터 유출 방지 보고서

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.