Slack 및 ServiceNow에서 SaaS API DLP에 대한 자동 교정 활성화 및 구성

목차

소개

이 문서에서는 Slack 및 ServiceNow 테넌트에서 SaaS API DLP에 대한 자동 교정을 활성화하고 구성하는 방법에 대해 설명합니다.

개요

이제 Slack 및 ServiceNow 테넌트에서 민감한 데이터 노출을 발견하고 자동으로 해결할 수 있습니다. 이를 통해 규정 준수를 유지하고 지적 재산권이나 다른 시스템의 자격 증명과 같은 중요한 데이터가 노출되지 않도록 할 수 있습니다.

지원되는 플랫폼에 대해 새 테넌트 인증

관리자는 Umbrella 대시보드의 SaaS API DLP(Data Loss Prevention) 기능을 사용하여 Slack 및 ServiceNow에 대한 새 테넌트를 인증할 수 있습니다.

1. Umbrella 대시보드에서 ADMIN > AUTHENTICATION > PLATFORMS로 이동합니다.
2. 프롬프트에 따라 새 테넌트를 인증합니다.

SaaS API DLP에서 지원되는 자동 교정

- ServiceNow:
  SaaS API DLP는 자동 격리를 지원합니다. 격리된 파일은 Cisco Quarantine(Cisco 격리) 테이블에 저장됩니다. 테넌트를 인증한 관리자만 이 테이블에 액세스할 수 있습니다.

- 슬랙:
  SaaS API DLP는 파일 및 메시지의 자동 삭제를 지원합니다.

감염된 파일에 대한 자동 교정 구성

관리자는 민감한 데이터 노출을 자동으로 치료하도록 SaaS API DLP를 구성할 수 있습니다.

SaaS API DLP 규칙에서 응답 작업을 설정합니다.

1. Umbrella 대시보드에서 POLICIES(정책) > MANAGEMENT(관리) > DATA LOSS PREVENTION POLICY(데이터 유출 방지 정책)로 이동합니다.

2. 규칙 추가를 클릭합니다.
3. SAAS API 규칙을 선택합니다.
4. 자동 교정을 활성화하려면 Response Action(응답 작업) 섹션에서 desiredACTION을 설정합니다.

추가 정보 찾기

자세한 지침은 Umbrella 설명서를 참조하십시오.

- 슬랙 테넌트를 위한 SaaS API 데이터 손실 방지 활성화
- ServiceNow 테넌트에 SaaS API 데이터 손실 방지 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.