Slack 및 ServiceNow에서 클라우드 악성코드에 대한 자동 교정 구성

목차

소개

이 문서에서는 Slack 및 ServiceNow 테넌트의 Cloud Malware에 대한 자동 교정을 활성화하고 구성하는 방법에 대해 설명합니다.

개요

이제 Slack 및 ServiceNow 테넌트에서 악성코드 위험을 발견하고 자동으로 치료할 수 있습니다. 이러한 기능은 감염된 파일을 제거하거나 격리하여 테넌트의 보안을 유지하는 데 도움이 됩니다.

지원되는 플랫폼에 대해 새 테넌트 인증

관리자는 Umbrella 대시보드를 통해 새로운 Slack 또는 ServiceNow 테넌트를 Cloud Malware Protection에 대해 인증할 수 있습니다.

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

클라우드 악성코드가 지원하는 자동 교정

- ServiceNow:
  Cloud Malware는 자동 격리를 지원합니다. 격리된 파일은 테넌트를 인증한 관리자만 액세스할 수 있는 Cisco 격리 테이블에 저장됩니다.

- 슬랙:
  Cloud Malware는 감염된 파일의 자동 삭제를 지원합니다.

감염된 파일에 대한 자동 교정 구성

관리자는 감염된 파일을 자동으로 치료하도록 클라우드 악성코드를 구성할 수 있습니다.

1. Umbrella 대시보드에서 ADMIN(관리) > AUTHENTICATION(인증) > PLATFORMS(플랫폼)로 이동합니다.
2. 테넌트에 대한 인증 마법사를 사용합니다. 3단계 중에 응답 작업을 설정합니다.
3. 선호하는 응답 작업(격리 또는 모니터링)을 선택합니다.
4. 필요에 따라 언제든지 응답 작업을 업데이트할 수 있습니다.

관련 리소스

- 슬랙 테넌트에 대해 클라우드 악성코드 차단 활성화
- ServiceNow 테넌트에 대해 클라우드 악성코드 차단 활성화

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.