Umbrella 클라우드 악성코드 검사를 위해 Microsoft 365에서 감사 로깅 구성

목차

소개

이 문서에서는 Microsoft 365 for Umbrella Cloud Malware 스캐닝에서 감사 로깅을 활성화하는 방법에 대해 설명합니다.

개요

클라우드 악성코드 검사를 위해 Cisco Umbrella를 Microsoft 365(이전의 Office 365)와 통합하려면 Microsoft 365에서 사용자 이벤트 감사를 활성화해야 합니다(기본적으로 활성화되지 않을 수 있음). 이 문서에서는 Microsoft Purview 규정 준수 포털에서 감사 로깅을 활성화하는 방법에 대해 설명합니다.

클라우드 악성코드 기능에 대한 자세한 내용은 Cisco Umbrella 설명서를 참조하십시오.

감사 로깅 사용

Microsoft 365에서 감사 로깅을 사용하려면

1. Microsoft Purview 규정 준수 포털(https://compliance.microsoft.com)에서 솔루션 > 감사로 이동합니다.
    - 또는 Audit(감사) 페이지로 직접 이동하려면 https://compliance.microsoft.com/auditlogsearch을 사용합니다.
2. 조직에 대해 감사가 설정되어 있지 않으면 사용자 및 관리자 활동 기록을 시작하라는 배너가 표시됩니다.
3. 녹음 시작 사용자 및 관리자 활동 배너를 선택합니다.

감사 작업이 시작되는 데 약 24시간이 걸릴 수 있습니다. 감사 로깅에 대한 도움이 필요하면 Microsoft 설명서를 읽거나 MS 지원 파트너에게 문의하십시오.

Cloud Malware Report(클라우드 악성코드 보고서)가 Cisco Umbrella에서 작동하려면 사용자/파일 활동과 관련된 감사가 Microsoft 365의 Purview 규정 준수 포털의 Audit(감사) 페이지에 나타나야 합니다.

예를 들면 다음과 같습니다.

4404249123348

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.