민감한 데이터가 ChatGPT에 의해 사용되지 않도록 보호하도록 DLP 구성

목차

소개

이 문서에서는 DLP(Data Loss Prevention)를 사용하여 민감한 데이터가 ChatGPT에 의해 사용되지 않도록 보호하는 방법에 대해 설명합니다.

개요

오픈인공지능의 언어모델인 챗지피티와 같은 혁신이 충전을 주도하며 인공지능의 세계가 들썩이고 있다. 이 AI 강국은 스마트하고 상황 인식 가능한 대화로 수많은 산업을 혁신하며 무서운 속도로 성장하고 있습니다. 하지만 이러한 흥미로운 발전으로 인해 몇 가지 잠재적인 과제가 생기게 됩니다. 특히 데이터 손실 위험이 있습니다.

ChatGPT를 제공하는 내용을 기반으로 텍스트를 생성하는 매우 스마트한 대화 파트너라고 생각해 보십시오. 그러나 중요한 정보가 섞여 있어 제대로 처리되지 않을 경우 데이터 유출 위험이 있습니다. 따라서 포괄적인 DLP(Data Loss Prevention) 계획을 수립하는 것이 매우 중요한 이유를 강조합니다.

Umbrella DLP 솔루션은 이러한 위험으로부터 조직을 보호하도록 설계되었습니다. Cisco 솔루션으로 즉시 해결할 수 있는 3가지 긴급 활용 사례는 다음과 같습니다. 단 5분이면 구현할 수 있습니다.

A. GDPR, HIPPA, PCI-DSS 등의 데이터 프라이버시 규정 준수:

1. Umbrella 대시보드에서 Policies(정책) > Management(관리) > Data Loss Prevention Policy(데이터 손실 방지 정책)로 이동합니다.
2. 새 DLP 규칙 생성을 시작합니다. 오른쪽 상단에서 Add Rule(규칙 추가)을 클릭하고 Real Time Rule(실시간 규칙)을 선택합니다.
3. 'ChatGPT Protection(ChatGPT 보호)'과 같이 알기 쉬운 이름을 규칙에 지정하고, 요구 사항에 맞는 심각도 수준(낮음에서 중요까지)을 선택합니다.
4. Classifications(분류) 섹션에서 조직과 관련된 Built-In Compliance Classifications(기본 제공 규정 준수 분류) 중 하나 이상을 선택합니다. 예를 들어 '내장형 GDPR 분류' 또는 '내장형 PCI 분류'가 될 수 있습니다.
5. Identities 섹션에서 모니터링하고 보호할 모든 ID를 선택합니다. 가능하다면, 우리는 포괄적 보장을 위해 광범위한 선택을 추천한다.
6. Destinations(대상) 섹션으로 이동하여 Destination Lists(대상 목록) 및 Applications for Inclusion(포함할 응용 프로그램)을 선택한 다음 OpenAI ChatGPT를 선택합니다.
7. 이제 행동으로 옮길 때입니다. Action(작업) 섹션에서 Monitor(모니터링) 또는 Block(차

단) 중 하나를 선택할 수 있습니다. 이 기능을 처음 사용하는 경우 '모니터링' 작업부터 시작하는 것이 좋습니다. 이를 통해 사용 패턴을 관찰하고 잠재적 위험 및 혜택에 대해 보다 정확한 정보를 바탕으로 결정할 수 있습니다.

8. '모니터링' 작업을 선택한 경우 주 또는 한 달 후에 DLP 보고서를 확인하십시오. 이렇게 하면 ChatGPT와 중요한 정보를 공유하는 사용자가 표시되며, '차단' 작업이 필요한지 여부를 결정하는 데 도움이 되는 경우가 표시됩니다.

나. 개인식별정보(PII) 보호 조직의 PII를 ChatGPT 위험으로부터 보호하려면 위와 동일한 지침을 사용하되 4단계에서 규정준수 분류 대신 '기본 제공 PII 분류'를 선택합니다.

다. 소스코드 및 지식재산의 보호 조직에서 소스 코드 또는 기타 지적 재산과 관련된 활동에 ChatGPT를 사용하는 경우 다음 단계를 수행하십시오.

1. 먼저 새 소스 코드 데이터 분류를 만듭니다. Policies(정책) > Management(관리) > Policy Components(정책 구성 요소) > Data Classification(데이터 분류)으로 이동합니다. 오른쪽 상단의 Add(추가) 버튼을 클릭하고 데이터 분류에 'Source Code Classification(소스 코드 분류)'과 같이 인식 가능한 이름을 지정합니다.
2. 기본 제공 데이터 식별자 목록에서 소스 코드를 선택합니다.
3. 저장을 클릭합니다.
4. 저장 후 위의 '데이터 개인 정보 보호 규정 준수'에 대한 지침을 다시 참조하되, 4단계에서는 기본 제공 소스 코드 대신 새로 만든 소스 코드 데이터 분류를 선택합니다.

이 프로세스는 간단하며 몇 분 정도밖에 걸리지 않습니다. 하지만 조직의 보안 및 규정 준수에 대한 이점은 매우 중요합니다. 데이터 보호를 강화하기 위해 가능한 한 빨리 이러한 단계를 수행할 것을 촉구합니다.

Umbrella가 사용자를 보호하는 방법 및 발생 AI 위험에 대해 자세히 알아보려면 ChatGPT 사용에서 민감한 데이터를 보호하십시오 웹 세미나를 시청하십시오.

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.