Akamai 체크리스트

AI 애플리케이션을 위협으로부터 보호하는 4가지 방법

Forrester Consulting이 Akamai 의뢰로 2025년에 진행한 **엔터프라이즈 AI 현황: 경험 축적과 리스크 관리**에 따르면 AI는 기업이 추진하는 3대 핵심 비즈니스 영역 개선 목표의 핵심입니다.

76%
고객 경험

71%
고객 유지율

76%
운영 효율성

그러나 기업들이 LLM(Large Language Model)을 기반으로 구축하거나 구동하는 AI 애플리케이션 개발을 서두르는 가운데, 다음 4가지 공격 방식이 이러한 목표를 위협할 수 있습니다.

1. **AI DoS(Denial-of-Service) 공격:** 리소스를 많이 소모하는 AI 프로세스는 시스템을 마비시키는 DoS 공격에 특히 취약합니다. 이러한 공격은 애플리케이션 다운타임으로 사용자의 불만을 야기해 고객 경험을 악화시킬 수 있습니다.
2. **데이터 유출 및 모델 도용:** 공격자는 정상적으로 보이는 악성 쿼리를 생성해 AI를 속여 민감한 데이터를 노출시킬 수 있습니다. 문제 조사에 소요되는 시간은 운영 효율성을 저해할 수 있습니다.
3. **유해한 아웃풋:** 공격자는 챗봇과 같은 고객 상호작용에서 AI가 유해한 콘텐츠를 생성하도록 조작할 수 있습니다. 부적절한 답변부터 사용자를 겁먹게 하고 유지율을 떨어뜨리는 공격적인 응답까지 다양하게 조작할 수 있습니다.
4. **프롬프트 인젝션 및 탈옥:** AI 앱은 보안 제어가 트리거되지 않도록 설계된 프롬프트에 속아 민감한 정보를 노출시킬 수 있습니다. 고객 신뢰는 브랜드의 데이터 보호 능력에 달려 있습니다.

방대한 데이터를 처리하는 AI 애플리케이션은 복잡한 알고리즘을 통해 의사결정을 내리는데, 공격자는 기존 툴로는 탐지하거나 방어할 수 없는 방식으로 이를 조작합니다.

AI 특화 공격에 어떻게 대응할 수 있을까요? 이 체크리스트를 활용해 사이버 보안 제어부터 프로세스까지 강화할 수 있는 영역을 확인하세요.

AI 애플리케이션 보안 체크리스트

데이터는 안전합니까?

- 기밀 데이터 노출 여부를 확인하기 위해 AI 애플리케이션의 쿼리와 응답을 분석하고 있습니까?
- 데이터 처리 방식에 체계적인 문제가 있음을 나타내는 패턴을 확인하고 있습니까?

AI 리소스 사용량을 어떻게 추적합니까?

- 리소스 할당 관리를 위해 지능형 비율 제한 툴을 사용하고 있습니까?
- 쿼리 복잡성을 분석하는 툴을 보유하고 있습니까?
- 리소스 할당을 보호하기 위해 엣지 네트워크와 같은 유연한 배포 옵션을 사용하고 있습니까?

Akamai

AI 애플리케이션 보안 체크리스트 – 계속

AI에 대한 위협을 탐지할 수 있습니까?

AI 애플리케이션에 대한 일반적인 공격 패턴을 인식하도록 팀원을 교육했습니까?

2025년 LLM 애플리케이션용 OWASP 상위 10대 취약점을 막을 수 있는 보안 기능을 사용하고 있습니까?

프롬프트와 응답을 차단하거나 수정할 수 있습니까?

악성 프롬프트를 차단하고 의심스러운 프롬프트를 수정(유해한 언어는 제거하되 핵심 질문은 통과)하는 보안 기능을 갖추고 있습니까?

AI 앱이 민감한 정보를 응답에 포함하지 못하도록 차단할 수 있습니까?

유해한 언어를 제거하면서도 응답의 유효한 부분이 사용자에게 전달되도록 응답을 수정할 수 있습니까?

AI 툴이 규정을 준수하고 있습니까?

LLM에 컴플라이언스 및 규제 요구 사항을 위한 문서와 제어 기능을 제공했습니까?

민감한 데이터를 교환하는 LLM 연계 API(Application Programming Interface)를 식별하고 문서화할 수 있습니까?

써드파티 공급업체를 검증했습니까?

써드파티 클라우드, 엣지, 분산 컴퓨팅 공급업체가 AI 안전 장치 및 인시던트 대응 절차를 갖추고 있습니까?

콘텐츠 필터링을 사용합니까?

부적절한 응답, 허위 정보 또는 혐오 발언을 실시간으로 검사하는 필터가 있습니까?

교육 데이터의 무결성을 지속적으로 확인하고 있습니까?

Akamai가 AI 비즈니스를 보호하는 방법

기업의 AI 애플리케이션은 이 체크리스트에서 논의된 4가지 위협에 대한 멀티레이어 보안이 필요하며 AI 개발 및 배포 라이프사이클의 특정 취약점을 해결해야 합니다. Akamai Firewall for AI는 다음과 같은 포괄적인 기능 세트로 AI 기반 비즈니스를 보호하기 위해 특별히 설계되었습니다.

- 데이터 보호 분석
- AI 위협 탐지
- 지능형 콘텐츠 필터링
- 규제 컴플라이언스
- 리소스 소비 추적
- 지속적인 AI 행동 분석

Akamai Firewall for AI로 AI 애플리케이션을 보호하는 방법에 대해 문의하세요.

맞춤형 데모 요청하기

© 2025 Akamai Technologies | 지원 |
| 2025년 10월 발행