보고서의 핵심 인사이트

AI 기반 API가 그렇지 않은 API보다 보안에 더 취약합니다.

대부분의 AI(인공지능) 기반 API는 외부에서 접속할 수 있으며, 불충분한 인증 메커니즘에 의존하는 경우가 많습니다. 이러한 취약점은 해당 API를 노리는 AI 기반 공격 유형이 점점 다양해지고 있는 상황에서 더욱 심각해지고 있습니다.

AI가 공격자의 기술적 진보를 촉진합니다.

이에는 AI 기반 멀웨어, 취약점 스캔, AI 통합 시스템 공격, 고도화된 웹 스크레이핑 기능 등이 포함됩니다.

32%

OWASP API 보안 상위 10대 리스크 관련 인시던트의 증가율

API 보안 인시던트가 증가하고 있으며 OWASP(Open Worldwide Application Security Project) API 보안 상위 10대 문제에서 인증 및 권한 확인 취약점이 민감한 데이터와 기능을 노출시키는 것으로 드러났습니다.

30%

MITRE 보안 프레임워크 관련 보안 알림 증가율

공격자는 자동화 및 AI를 포함한 고급 기술을 활용해 API를 악용하고 있습니다. MITRE 프레임워크는 보안팀이 이러한 공격을 더 빠르게 정확히 식별하는 데 도움을 줄 수 있습니다.

33%

전 세계 웹 공격의 연간 증가율

공격 급증은 클라우드 서비스, 마이크로서비스, AI 애플리케이션의 빠른 도입과 직접적으로 연관되어 있으며 이에 따라 공격 표면이 확장되고 새로운 보안 과제가 등장하고 있습니다.

2300억 이상

커머스 기업을 표적으로 한 웹 공격 건수

영향을 가장 많이 받은 커머스는 첨단 기술(두 번째로 많은 공격을 받은 업계)의 약 3배에 달하는 공격을 받고 있습니다.