Principais insights do relatório

As APIs impulsionadas por IA apresentam maior risco de segurança do que suas equivalentes.

A maioria das APIs impulsionadas por IA é acessível externamente e muitas dependem de mecanismos de autenticação inadequados, o que aumenta a vulnerabilidade à crescente variedade de ataques orientados por IA.

A IA fomenta o avanço técnico dos agentes de ameaças.

Isso inclui avanços como malware orientado por IA, verificação de vulnerabilidades, ataques a sistemas integrados por IA e técnicas sofisticadas de web scraping.

32%

A porcentagem de aumento dos incidentes relacionados ao Top 10 em Segurança de APIs do OWASP

Os ataques à segurança de APIs estão se tornando mais frequentes e os principais problemas identificados pelo Top 10 em Segurança de APIs do OWASP evidenciam vulnerabilidades em autenticação e autorização, expondo dados e funcionalidades confidenciais.

30%

Expansão de alertas de segurança vinculados à estrutura de segurança da MITRE

Os invasores estão usando técnicas avançadas, incluindo automação e IA, para explorar APIs. A estrutura de segurança da MITRE pode ajudar os defensores a identificar esses ataques de forma mais rápida e precisa.

33%

A porcentagem de expansão dos ataques globais na web ano a ano

O aumento dos ataques está diretamente ligado à rápida implementação de serviços de nuvem, microsserviços e aplicações com tecnologia de IA, que ampliam as superfícies de ataque e trazem novos desafios de cibersegurança.

Mais de 230 bilhões

O número de ataques na web direcionados a organizações do setor de comércio,

o que tornou esse setor o mais impactado, com quase três vezes mais ataques do que o setor de alta tecnologia, que ocupa o segundo lugar em número de incidentes.