报告的关键见解

AI 驱动的 API 比传统 API 风险更高。

大多数人工智能 (AI) 驱动的 API 皆可通过外部访问，并且许多 API 依赖不完善的身份验证机制，这一漏洞随着 AI 驱动的 API 攻击量不断增加而加剧。

AI 为攻击者的技术进步推波助澜。

随着 AI 的发展，恶意软件、漏洞扫描、针对 AI 集成系统的攻击和先进的网络内容抓取功能等方面也出现了长足进步。

32%

OWASP 十大 API 安全风险相关事件的增幅

API 安全事件在不断增加，开放全球应用程序安全项目 (OWASP) 十大 API 安全问题揭示了会暴露敏感数据和功能的身份验证及授权漏洞。

30%

与 MITRE 安全框架相关的安全告警增幅

攻击者正在使用自动化和 AI 等先进技术来利用 API。MITRE 框架可以帮助防御者更快、更准确地识别这些攻击。

33%

全球 Web 攻击量的同比增幅

攻击量的激增与云服务、微服务以及 AI 应用程序的快速采用密切相关，这些服务和应用程序会扩大攻击面并带来新的安全挑战。

2300 多亿次

商业企业遭受的 Web 攻击量，这使得该行业成为受影响最大的行业，其遭受的攻击量几乎是高科技行业（遭受攻击第二多的行业）的三倍。