为了解亚太地区 (APAC) 四大经济体的 API 安全现状，最新一期的《API 安全影响研究》收集了该地区 800 多名网络安全从业人员的反馈：中国、印度、日本和澳大利亚。此研究基于 Noname Security（现为 Akamai Technologies 的子公司）进行的一项年度调查，该调查旨在了解安全专业人员在过去三年里如何将 API 纳入其安全计划。结果一如既往，我们的研究发现，尽管人们对 API 漏洞的认识不断提高，但高层领导对 API 安全的重视程度并未相应地提升，因为首席信息安全官 (CISO) 和首席信息官 (CIO) 们都疲于应付日益增多且相互冲突的优先事项。

2024 年，**《API 安全影响研究》**将其传统的调研范围从美国和英国的企业扩大到了德国的企业。该研究发现：

- API 安全事件已连续第三年呈上升趋势。
- 据估计，应对这些事件的成本平均超过了 50 万美元（IT 和安全负责人表示，该成本已接近 100 万美元）。
- 大多数受访者认识到了这些事件给安全团队带来的压力和声誉损失。

这项调查的受访者包括以下八个行业的企业高管（CISO、CIO 和首席技术官）、资深安全人员以及应用安全团队成员：

- 汽车
- 保险
- 金融服务
- 政府/公共部门
- 零售/电子商务
- 制造
- 医疗保健
- 能源/公用事业

调查结果揭示了有关 API 安全实践和优先事项的宝贵见解，包括：

- API 安全事件的原因
- 整体网络安全优先事项
- 与 API 安全事件相关的成本，例如罚款和修复费用
- API 安全事件对安全团队的影响
- API 清点和测试实践的状态
- 对哪些 API 会返回敏感信息的认知
- API 安全在监管合规工作中的现状

什么是 API 安全事件?

安全事件可能包括 API 滥用、API 攻击、以 API 为中心的数据泄露，以及恶意攻击者破坏 API 的所有尝试。