

Akamai 与 Apiiro 携手合作， 从代码编写到运行时提供全方位保护

API 可为现代应用程序提供支持，推动创新并实现无缝的数字体验。然而，API 同时也成为了日益多见的攻击媒介，如果未被妥善保护，将使企业面临重大的安全风险。Akamai 和 Apiiro 携手合作，将 Akamai API Security 与 Apiiro 的应用程序安全态势管理 (ASPM) 平台相集成，以应对这一挑战。该联合解决方案使企业能够从代码编写到运行时全方位保护 API，从而降低风险、简化修复流程并加快创新步伐，同时不损害安全性。

监测能力对于有效管理基于 API 的风险至关重要。快速识别和应对漏洞尤为关键——一旦检测到问题，安全团队必须与开发团队合作，尽快修复高风险漏洞。然而，大多数解决方案无法将已识别的风险与源代码联系起来，这迫使安全和开发团队忙乱应对。Akamai 与 Apiiro 的集成通过提供端到端监测能力和上下文，解决了这一脱节问题。

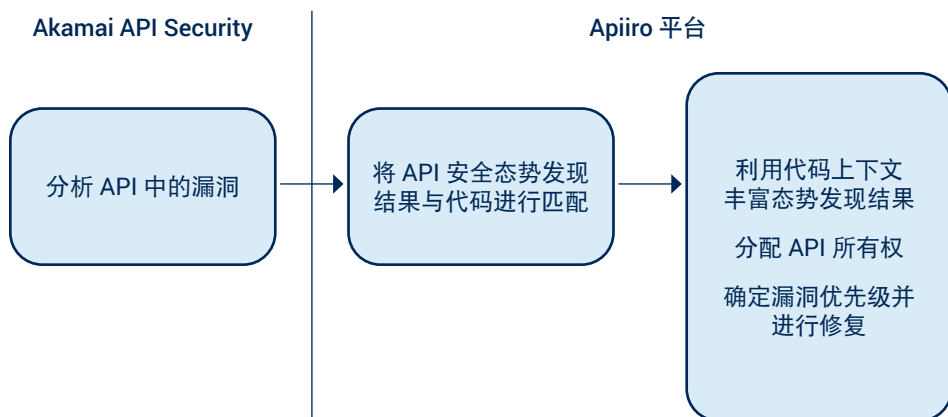
Akamai API Security 能够发现流量中的 API，并分析 API 中可能导致攻击的错误配置和漏洞。对于每个漏洞，Akamai API Security 可为开发人员提供详细见解，包括发生了什么、为何它构成风险以及如何复现该问题。这些可行信息被传递给 Apiiro 平台，该平台维护着通过深度代码分析发现的全面 API 清单。Apiiro 平台会自动将 Akamai 识别的 API 和漏洞与其现有的 API 库进行匹配，并将每个漏洞映射到相关的存储库、特定的代码行以及代码负责人。

这一无缝集成确保了 Akamai API Security 检测到的 API 风险能够动态追溯到其根本原因。开发人员可以利用所有必要信息，快速修复漏洞，提高解决过程的速度和效率。此外，这种方法促进了安全团队与开发团队之间更好的沟通与协作，弥补了 API 安全工作流中的关键差距。

为贵企业带来的好处

-  **提高监测能力**
使用 API 漏洞上下文增强代码分析。
-  **加快修复速度**
自动将 API 漏洞映射到源代码，并分配给开发团队负责人。
-  **降低风险状况**
通过将 API 流量与代码关联，简化漏洞调查，并根据潜在影响优先级排列漏洞。

工作原理



关键应用场景

- 自动化风险评估：持续全面地分析 API 及相关代码，以识别潜在风险。
- 加快风险抵御速度：优先处理 API 漏洞，将漏洞映射到源代码，并分配负责人，从而缩短平均解决时间 (MTTR)。
- 生产前防护：将安全措施集成到开发工作流中，主动监控和管理 API 变更。

结论

Akamai-Apiiro 解决方案通过提供端到端监测能力和切实可行的见解，为 API 安全提供了一种独特的方法。通过这一集成，Apiiro 客户可以将保护范围从代码编写扩展到运行时，从而确保全面的 API 安全。同时，Akamai 客户可以通过追踪 API 风险的代码来源并将其分配给相应的团队来提高修复效率。Akamai 和 Apiiro 携手合作，赋能企业在日益复杂的 API 环境中安全、自信地进行创新。

