AKAMAI 产品资料

API Security ShadowHunt

API Security ShadowHunt 是一款托管式威胁搜寻服务，有了擅长 API 威胁搜寻的专业分析师的加持，您的安全团队将如虎添翼。API Security ShadowHunt 是一种外包解决方案，可帮助您降低风险，非常适合人手不足或者缺乏 API 安全专业知识的团队。Akamai 威胁搜寻分析师能够帮助您的团队检测并报告 API 流量中藏匿最深且难以发现的攻击。

API Security ShadowHunt 如何运作

ShadowHunt 首先会分析 API Security 平台中的 API 活动数据。这些自动进行的分析操作能够检测行为偏差和漏洞利用，并将机器学习信号发送给 ShadowHunt 分析师进行调查。这时就需要分析师专业知识的介入了。

由于分析师熟悉客户的 API 资产，因而他们能够快速识别活跃威胁，然后生成并发送 ShadowHunt 告警。如果分析结果不明确，分析师会联系 ShadowHunt 用户进行说明。分析师和 API Security 研究团队分析威胁情报信息并向所有客户定期提供新兴威胁报告。

API Security 与分析师专业知识相结合

API Security 平台提供全面的 API 安全功能，其中包括：

- **API 发现：**广泛而持续的 API 发现
- **风险状况：**对 API 风险了如指掌
- **利用行为分析，进行威胁检测：**利用大数据和基于云的分析引擎，检查一段时间内的所有 API 活动，持续检测 API 滥用情况
- **预防和响应：**定制的条件响应手册，强化安全性和 API DevSecOps 流程
- **调查和威胁搜寻：**强大的调查能力，能够发现 API 流量中隐藏的威胁

威胁搜寻是 API Security 平台的一项高级功能。API Security ShadowHunt 服务非常适合缺乏工具、专业知识或时间来搜寻威胁的客户。

对企业的好处

- Akamai 专家负责检查 API 活动，让您安心无忧
- 能够检测出隐匿在 API 数据中更多的安全威胁
- 有了 Akamai 专门负责 API 安全，您的团队便能抽身忙于其他事务
- 获得有关软件开发和 IT 运营方面切实可行的见解
- 更为严格的审查，使您能够更好地监测 API 行为

值得信赖的 API Security ShadowHunt 服务

告警：*一旦发现您的 API 资产中存在威胁，会立即通知相关人员。*API Security ShadowHunt 服务最重要的功能就是告警，它会在确认发生事件后立即发出告警。告警包括：

- 事件调查结果和分析
- 与事件相关的威胁情报摘要
- 修复建议

威胁报告：*获得早期 API 安全情报。*API Security ShadowHunt 新兴威胁报告是基于团队所掌握的全球威胁情报、API Security 研究团队的建议以及持续的威胁搜寻活动。新兴威胁报告包含：

- 团队发现的新 API 漏洞、威胁或攻击的详细信息
- 对您 API 资产的影响
- 修复建议（如有必要）

月度总结：*全面监测您的 API 资产。*ShadowHunt 月度威胁报告会在每月的第一周发送给所有 API Security 客户。其中包含：

- 上月发送的 ShadowHunt 告警和新兴威胁报告的总结
- 您的 API 资产概览
- 过去两个月的 API 活动比较
- API 行业的安全新闻

咨询专家：用户可以就安全告警和新兴威胁报告的疑问咨询 API Security ShadowHunt 团队并寻求建议。

为何选择 API Security?

API Security 运用扩展检测和响应 (XDR) 的原则，来化解在防护 API 漏洞和避免 API 滥用中遇到的挑战。只有 API Security 会将 API 活动汇集到基于云的大数据环境中，然后进行复杂的数据扩充和数据组织。这种独特的架构可实现持续的 API 发现、风险评分和情境感知行为分析，从而能检测 API 滥用和威胁，并进行威胁搜寻。API Security 架构在设计上考虑了隐私性，任何发往数据湖的 API 活动都可以进行标记化。

专业的威胁搜寻服务，保护企业 API 安全

随着部署的 API 越来越多，这给企业的 IT 安全部门带来巨大压力。如今有了 API Security ShadowHunt 服务，您的团队便可如虎添翼。

咨询专家以了解更多信息。

扫码关注，获取最新CDN前沿资讯