graylog
API SECURITY

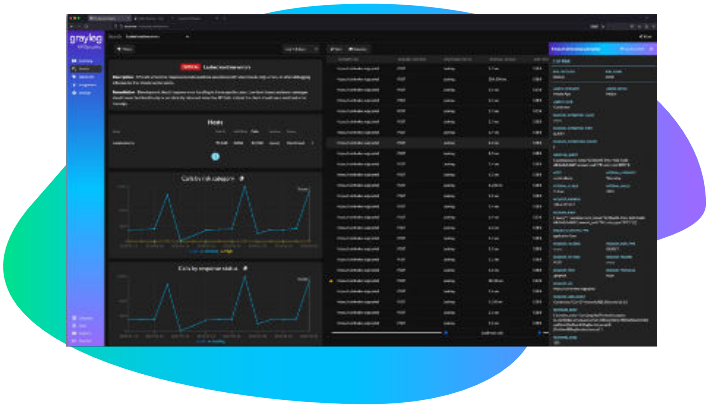
利用全面API发现、威胁检测和事件响应

获得对API攻击面的可见性和控制

Graylog API Security 安全是专门为安全团队提供对周边运行时API活动的完全可观察性的首个API安全解决方案。由于攻击者正在寻找创新方法来冒充有效用户以获得对关键生产API的不受限访问权限，因此您不能再仅仅依靠周边防御。您的安全团队现在可以使用Graylog API安全来加强您的周边后API安全态势并管理不断增长的API攻击面。Graylog API安全提供API发现、威胁检测和事件响应功能，可为您提供对环境的完整可见性、实时攻击监测以及对端到端API请求和响应数据的透彻分析。

咨询我们的专家并了解Graylog API安全的运行

眼见为实。在Graylog，我们希望您在购买之前就能得到所有问题的答案。我们提供定期产品演示，以展示产品功能并留出时间进行问答。立即安排您的Graylog API安全演示，亲眼见证我们的强大网络安全平台的运行。



Graylog API 安全优势

- **持续API发现** — 自动发现并分类所有API，确保没有API漏网
- **引导式威胁检测和响应** — 使用清晰、可操作的步骤获取警报以立即处理威胁
- **完整的请求和响应负载** — 超越标头数据，实现精确警报、追溯威胁搜寻和API特定补救
- **安全的自我管理解决方案** — 将敏感数据保留在公司内部，避免第三方干扰、PII问题以及SaaS安全审查的繁文缛节

graylog
API SECURITY

强大的功能集

API捕获
通过网络、网关和应用程序内捕获选项全面洞察您的API攻击面。

资产澄清
通过自动对流经任何API的数据进行分类来节省开发时间。

持续API 发现
消除开发和安全团队手动识别组织正在使用的API的负担。

无代码规则
轻松构建您自己的自定义威胁检测和警报规则。

OWASP前10
利用超越OWASP的Graylog威胁特征来立即降低风险。

实时威胁检测
监控运行时的安全问题，生成具有完整背景和定制补救指导的良好警报。

补救
警报包括详细、有针对性和可定制的指示，以便立即解决风险。

请求和响应捕获
自动捕获REST API和GraphQL查询的所有请求和响应的标头和正文数据。

风险评分
自动评估您的API的安全态势并获得有关当前API安全风险的可操作情报。

搜索
使用标准SQL和正则表达式查询快速查找所需信息。

独立数据湖
以经济高效的方式保存API交易用于调查和威胁搜寻，无需外部数据库。

SIEM/SOAR集成
自动向Graylog SIEM或您的SOAR解决方案发送关键安全警报以进行事件响应。

单点登录
使用OAuth或JWT安全访问Graylog API安全。

针对性警报
通过Slack、Teams、Gchat或Zapier将警报直接精确路由到安全和/或DevOps团队。• 将来自各地的日志