GitHub

基于LGTM的Advanced Security

从开源到DevOps，不同的组织都在寻找可加速软件交付的新方法，但仍然不得不依靠传统的安全工具。GitHub高级安全利用全球领先的代码分析引擎“LGTM”，帮助团队提升代码构建速度与安全性。

借由社区力量保护代码安全

超过1,600项查询可供选择

通过行业专家和LGTM社区贡献的查询，让顶尖安全研究人员成为您团队的一员。

共享最佳安全实践

通过每个人都能学习和使用的已编码、可执行和可共享的查询，提高整个组织的安全性。

从头至尾确保您工作流程的安全

运行开箱即用或自定义的查询

GitHub高级安全研究人员使用一种称为QL的语言对LGTM查询进行编码。然后，团队可以跨多个代码库运行和执行QL查询，大规模地发现安全漏洞。

查看安全警报与分步修复

在发现漏洞时，安全警报会直接显示在开发人员的pull请求中，同时还会显示安全专家提供的分步文档和建议修复方法。

找到并永久修复安全漏洞

每次发现新的安全漏洞时，系统都会编写更新的QL查询并将其添加到GitHub Advanced Security中，因此相同的漏洞不会出现两次。

随时改进和更新查询

在每次部署中，内部开发人员和安全团队能够持续修改查询以匹配您的代码，避免误报，并识别新的安全问题。

保护代码与客户的强大工具

代码即数据

通过识别您需要确定的漏洞，而非您不需要的修复，实现代码即数据特性。

减少误报

让安全和开发团队专注于对您的组织最重要的漏洞。

可扩展的安全性

快速分析代码，识别代码库中最复杂的语义模式。

面向对象的查询

快速完成针对自定义控制、数据流分析和污点跟踪的运行语义查询，只需数小时，而非数周。

> *“我们使用LGTM在整个组织内建立共享的知识和专业技能，使我们能够以团队形式展开协作，共同推动产品向前发展。”*

BlackLine软件开发总监**Gregory Burns**

端到端安全性

了to有关GitHub
和软件安全性的更多信息：
github.com/features/security

需要帮助开始吗?

联系我们的销售团队：
sales@github.com
github.com/enterprise