GitHub

GitHub Consultation

Advanced Security CodeQL Workshop

Learning Outcomes

Use CodeQL to find real vulnerabilities

Work as a team on CodeQL queries and libraries

Model your custom libraries and frameworks in CodeQL

Consultation Overview

After discovering a vulnerability in your code, how do you find other places where developers have made similar mistakes? Once the vulnerability is fixed, what are you doing to guard against it being reintroduced? CodeQL allows you to write queries that will search for other instances of the same problematic patterns within your code, which can then be built into the code review process using GitHub Advanced Security. During this three day workshop, your team will work with GitHub experts to perform Variant Analysis using CodeQL and find real vulnerabilities in your own code.

Key Features and Benefits

- Introductory training sessions
- Work on real world problems with a seasoned CodeQL writer
- Tweak existing community queries to understand your tech stack & threat model
- Build completely custom analyses from scratch

Syllabus

Prior to the workshop, your on-site expert will work with you to tailor the program to address your most important projects and objectives. This unique engagement is primarily free-form, prioritizing your team's progress on real projects and features:

Day 1

- Introduction to Variant Analysis with CodeQL: querying AST + dataflow
- Start work on projects

Days 2-3

- Advanced CodeQL (e.g. other analysis libraries, performance, testing)
- CodeQL in practice: testing, version control, creating libraries, etc
- Project work
- Lightweight sessions for any FAQ

Delivery Methods

Remote Prep:

3 days: 9:00am - 4:00pm

Onsite Consultation:

None

Prerequisites

- Advanced security rollout complete - all in scope projects analyzed
- Source/input vulnerabilities
- Team selected

Target Audience

Security Researcher

GitHub

Website **services.github.com** or email **services@github.com**