Cloud Contraptions
TRAINING & CONSULTING

To discuss this course and customizations:
Call: 434-509-5680 or Email: sales@cloudcontraptions.com

Kubernetes for Programmers

Class Duration

7 hours of live training delivered over 1-2 days to accommodate your scheduling needs

Student Prerequisites

- Ability to read computer program code.
- Command line experience with a terminal or command prompt.
- Experience with a modern editor (ex. Visual Studio Code) or IDE (ex. Visual Studio or a JetBrains IDE).
- Experience using cloud-based services such as Azure, AWS, or Google Cloud Platform.
- This course focuses on using GitHub Advanced Security. Students write minimal code and all necessary programming code is provided.

Target Audience

Designed for senior software engineers, AppSec engineers, security champions, DevOps/platform teams, and engineering managers who own code quality and risk. Ideal for organizations standardizing on GitHub and seeking to operationalize “shift-left” AppSec practices across multiple services. Attendees should be comfortable with Git, pull requests, and basic CI/CD concepts. Suitable for live delivery online or in-person for distributed or co-located teams.

Description

This live, hands-on GHAS training equips software teams to embed security into everyday delivery without slowing velocity. Participants learn how to activate and govern GitHub Advanced Security at scale; integrate it into existing CI/CD; and apply developer-first controls including secret scanning, CodeQL code scanning, and Dependabot dependency management. Through practical labs and real-world workflows, your team will learn to detect issues earlier, reduce mean time to remediation, and harden your supply chain—turning AppSec from a late-stage blocker into a competitive advantage for shipping reliable, compliant software faster.

Cloud Contraptions
TRAINING & CONSULTING

To discuss this course and customizations:
Call: 434-509-5680 or Email: sales@cloudcontraptions.com

Learning Outcomes

- Articulate GHAS core capabilities and the AppSec “shift-left” philosophy to align engineering and business goals.
- Configure GHAS across repositories, permissions, and security policies; wire it into CI/CD, GitHub Actions, and Azure DevOps.
- Implement secret scanning and credential protection, including custom detectors, alerting, and rapid remediation workflows.
- Set up and tune CodeQL code scanning for monorepos and services, including PR gating and scheduled analyses.
- Interpret CodeQL findings to prioritize risk, suppress noise responsibly, and drive measurable defect reduction.
- Author and run custom CodeQL queries with the CLI; package, version, and maintain reusable query sets.
- Integrate GHAS code scanning with third-party tooling (e.g., Codacy) to streamline triage and reporting.
- Secure the software supply chain with Dependabot: dependency graph/review, automated updates, and policy-driven triage.

Training Materials

All students receive comprehensive courseware covering all topics in the course. Courseware is distributed via GitHub in the form of documentation and extensive code samples. Students practice the topics covered through challenging hands-on lab exercises.

Software Requirements

Students will need a free, personal GitHub account to access the courseware. Student will need permission to install the selected language platform (Node.js, .NET SDK, or Python) and Visual Studio Code on their computers. Also, students will need permission to install packages for the selected coding platform as well as Visual Studio Extensions.

Training Topics

GitHub Advanced Security (GHAS)

- What is GHAS? Core features and philosophy
- What is Application Security (AppSec)?
- State of AppSec in the industry
- What does it mean to shift security left?

To discuss this course and customizations:
Call: 434-509-5680 or Email: sales@cloudcontraptions.com

- Benefits of shifting security left in the development lifecycle
- The value of “developer-first” security
- SAST, DAST, SCA, and other security acronyms
- Supply Chain, Code, and Platform

Configure GHAS in Your Workflow

- Activating GHAS features in repositories
- Managing permissions and access controls
- Define a Security Policy
- CI/CD pipelines and GHAS
- Integrate GHAS with GitHub Actions (optional)
- Integrate GHAS with Azure DevOps (optional)

Secret Scanning and Credential Protection

- How secret scanning works
- Identifying exposed secrets in code
- Creating and managing custom secret patterns
- Remediation strategies and alerts handling

Code Scanning with CodeQL

- What is CodeQL and how it works
- Setting up CodeQL analysis in repositories
- Interpreting CodeQL results and findings
- Writing and running custom CodeQL queries
- Advanced Configuration
- Manual vs. automatic code scanning
- CodeQL CLI
- CodeQL Custom Queries
- Integrate with Third-Party Tools (optional)
- Integrate with Codacy (optional)

Dependency Scanning with Dependabot

- Understanding Dependency Graph and Dependency Review
- Automating updates with Dependabot
- Triage and remediation workflows
- Managing third-party packages securely