GH - 500T00 : GitHub Advanced Security

Course Outline

GitHub Advanced Security – Part 1 of 2

1. Introduction to GitHub Advanced Security (GHAS)

- Define GitHub Advanced Security (GHAS) and its core features: Secret Scanning, Code Scanning, and Dependabot
- Understand the role of GHAS in enhancing security in the development lifecycle
- Learn how to leverage GHAS to maximize security impact

2. Managing Vulnerable Dependencies with Dependabot

- Configure Dependabot security updates on a GitHub repository
- Explore tools for managing vulnerable dependencies
- Enable and configure Dependabot alerts and security updates
- Understand required permissions and roles for Dependabot
- Identify, review, and resolve vulnerable dependencies
- Use the GraphQL API to retrieve vulnerability information
- Configure notifications for vulnerable dependencies

Lab:

- Configure Dependabot Security Updates

3. Secret Scanning in GitHub

- Understand what secret scanning is and how it helps prevent sensitive data leaks
- Configure and enable secret scanning for a repository
- Utilize secret scanning results effectively

4. Code Scanning on GitHub

- Understand the concept and importance of code scanning
- Steps to enable code scanning in a repository
- Enable code scanning with both GitHub-native tools and third-party analysis tools
- Compare CodeQL implementation using GitHub Actions vs third-party CI tools
- Configure code scanning using various triggering events (scheduled or on-demand)

GitHub Advanced Security – Part 2 of 2

1. Identifying Security Vulnerabilities with CodeQL

- Use CodeQL to create a database representation of your codebase
- Run CodeQL queries to detect security vulnerabilities
- Interpret scan results using built-in and custom queries

2. Code Scanning with GitHub CodeQL

- Learn what CodeQL is and how it analyzes code
- Understand QL, the logic programming language behind CodeQL
- Set up CodeQL-based scanning in GitHub repositories
- Reference and use custom CodeQL queries

- Configure the language matrix in CodeQL workflows
- Use the CodeQL CLI to generate and upload results
- Implement custom build steps for effective analysis

Labs:

- Reference a CodeQL Query
- Configure a CodeQL Language Matrix

3. GitHub Administration for Advanced Security

- Understand how to apply GHAS in the software development lifecycle
- Identify features available for open-source and enterprise environments
- Enable GHAS features across different enterprise plans
- Assign correct access and permissions to users
- Set organization and repository-level security policies
- Respond effectively to security alerts
- Monitor security alerts using the Security Overview dashboard
- Use GitHub Advanced Security API endpoints for automation and management

4. Managing Sensitive Data and Policies

- Create clear documentation with security guidelines
- Set permissions and rules to protect data
- Automate security processes to prevent breaches
- Understand how to respond to and mitigate security incidents