+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 06/05/2026

Sign up

GitHub Advanced Security Training

2 days (14 hours)

Overview

GitHub Advanced Security (GHAS) helps secure the software development lifecycle directly within GitHub using Code Scanning, Secret Scanning, Dependabot, and security dashboards.

Our GitHub Advanced Security training will help you implement a practical DevSecOps approach to identify, prioritize, and fix vulnerabilities as early as possible in your software projects.

You will learn how to analyze your GitHub repositories, configure Code Scanning, use CodeQL, detect exposed secrets, handle dependency alerts, and reduce risks related to the software supply chain.

You will be able to strengthen the security of your repositories, structure a remediation process, configure governance best practices, and track security metrics with Security Overview.

By the end of this training, you will be able to leverage GitHub Advanced Security to secure your code, dependencies, secrets, and workflows within a DevOps organization.

Like all our training courses, this one will introduce you to **the latest stable version** of the technology and its new features.

Objectives

- Understand the role of GitHub Advanced Security in a DevSecOps approach.
- Configure code scanning and analyze application vulnerabilities.

- Use CodeQL to detect security vulnerabilities in code.
- Set up Secret Scanning and manage related alerts.
- Secure dependencies with Dependabot.
- Strengthen software supply chain security.
- Manage an organization’s security posture with GitHub dashboards.

Target Audience

- DevOps engineers
- DevSecOps engineers
- Developers
- Lead Developers
- Software architects
- Technical CISOs
- Application Security Managers
- Platform Engineers

Requirements

- Basic knowledge of Git and GitHub.
- Understanding of software development workflows.
- Familiarity with CI/CD is a plus.
- Basic knowledge of application security or DevSecOps is recommended.

Technical prerequisites

- Laptop with a stable internet connection.
- Active GitHub account.
- Access to a test GitHub organization or repository.
- Up-to-date web browser.
- Code editor installed, such as Visual Studio Code.

Agenda for our GitHub Advanced Security (GHAS) training

[Day 1 - Morning]

Introduction to GitHub Advanced Security and Code Security

- Overview of GitHub Advanced Security
- Security challenges in the software development lifecycle
- Integrating GHAS into a DevSecOps approach
- Understanding risks related to secrets, dependencies, and application vulnerabilities
- Overview of GitHub Advanced Security features

- Introduction to Code Scanning
- Understanding common application vulnerabilities
- Configuring and running a security scan
- Interpreting results and prioritizing fixes
- Hands-on workshop: Analyze a GitHub repository and implement an initial vulnerability detection strategy.

[Day 1 - Afternoon]

CodeQL and advanced vulnerability analysis

- Introduction to CodeQL
- Understanding the semantic code analysis model
- Configuring analysis rules
- Customizing CodeQL queries
- Identifying complex vulnerabilities
- Integrating CodeQL into CI/CD workflows

Secret scanning and secret protection

- Understanding the risks associated with secrets exposed in code
- How Secret Scanning Works
- Detecting sensitive keys, tokens, and credentials
- Alert management and remediation processes
- Best practices for secret management in GitHub
- Preventing secret leaks in collaborative projects
- Hands-on workshop: Detecting and fixing exposed secrets in a GitHub repository.

[Day 2 - Morning]

Dependabot and Securing Dependencies

- Understanding the risks associated with software dependencies
- Introduction to Dependabot Alerts
- Managing automatic updates
- Library vulnerability analysis
- Patch management and update validation
- Reducing Risks Associated with the Software Supply Chain
- Hands-on workshop: Configure Dependabot and address multiple detected vulnerabilities.

[Day 2 - Afternoon]

GitHub Supply Chain Security and Governance

- Understanding the Challenges of Software Supply Chain Security

- Identifying Risks Associated with Third-Party Components
- Implement security governance in GitHub
- Apply DevSecOps best practices
- Strengthen repository and workflow security

Security management and continuous improvement

- Security Overview and GitHub dashboards
- Monitor an organization’s security metrics
- Prioritizing remediation actions
- Measuring the effectiveness of DevSecOps practices
- Building a continuous improvement process
- Hands-on workshop: Build a security dashboard and present a project’s key metrics.

To learn more

Target Audience

This training is intended for both individuals and companies, large or small, seeking to train their teams in new advanced IT technologies or to acquire specific industry knowledge or modern methodologies.

Assessment upon enrollment

The pre-training assessment complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency in various types of technologies, as well as their expectations and personal goals regarding the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could pose challenges for monitoring and ensuring the smooth running of the training session.

Teaching Methods

Practical Course: 60% Practical, 40% Theory. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the trainer, supported by examples and reflection sessions, and group work.

Assessment

At the end of the session, a multiple-choice questionnaire is used to verify that the skills have been properly acquired.

Certification

A certificate will be issued to each trainee who has completed the entire training program.