GitHub Advanced Security (GH-500T00)

Duration: 1 day
Audience: Professionnel TI

Who is this training for?

Individuals who want to understand and implement advanced security practices using GitHub Advanced Security (GHAS). They will learn how to significantly improve software development processes and create a more resilient and secure development ecosystem by using solutions focused on people developing applications, to ensure code, supply chain, and secrets are secure before release. They will learn how GHAS provides security teams with visibility into organizational and supply chain security posture, as well as unparalleled access to insights from millions of people developing applications and security seekers around the world.

Training objectives

- Understand the features and benefits of GitHub Advanced Security
- Enable and configure code analysis to identify vulnerabilities
- Use secret analysis to detect and prevent secret leaks
- Implement dependency analysis (Dependabot) for vulnerable dependencies
- Interpret and act on security alerts generated by GHAS • Integrate security flows into CI/CD pipelines
- Leverage advanced configuration options to
- Support compliance with organizational and regulatory security requirements

Summary

GitHub Advanced Security (GHAS) plays a crucial role in strengthening the security posture of software development projects on GitHub. It provides a comprehensive set of tools and features designed to identify and address security vulnerabilities throughout the development lifecycle. By integrating security directly into the development process with GHAS, your team can create more secure and reliable software. This course explores how to use GHAS to maximize security impact and understand the role of GHAS in the security ecosystem.

Course outline

Introduction to GitHub Advanced Security

- Define GHAS and the importance of its core features
- How to use GHAS for maximum impact
- Understand the role of GHAS in the security ecosystem
- Module evaluation

Configure Dependabot security updates on your GitHub repository

- Configure and use secret scanning in your GitHub repository
- Configure code analysis on GitHub Identify security vulnerabilities in your codebase using CodeQL
- Code Analysis with GitHub CodeQL GitHub
- Administration for GitHub Advanced Security
- Manage sensitive data and security policies in GitHub

Approach and methodology

Practical and structured approach combining focused theory and guided workshops. Participants gradually strengthen the security of GitHub environments through real-world exercises inspired by professional scenarios, promoting immediate application of learnings. They learn how to identify vulnerabilities, protect code, and implement advanced security practices using GitHub Advanced Security features. Led by a Microsoft-certified trainer, the training focuses on interactivity and the development of directly transferable technical skills to effectively secure development chains in a professional context.

Prerequisites

Before taking this course, participants should have:

- A basic knowledge of Git and GitHub (essential commands, branch management, merging, etc.)
- Experience with software development workflows (repositories, pull requests, code reviews)
- An understanding of fundamental security concepts

- Access to a GitHub account (ideally with admin or security rights on a test repository)

Recommendations

- Basics in GitHub and version control (Git)
- Knowledge of software development and CI/CD concepts
- Understanding of application security concepts (vulnerabilities, dependencies)
- Familiarity with DevSecOps principles
- Notions of identity and access management