GitHub Advanced Security (GH-500T00)

Duration: 1 day
Audience: Professionnel TI

Who is this training for?

This course in intended for students who want to understand and implement advanced security practices with the help of GitHub Advanced Security (GHAS). They will learn how to significantly enhance software development processes and create a more resilient and secure development ecosystem using developer-first solutions to unlock the ability to keep code, supply chain, and secrets secure before you push to production. They will learn how GHAS gives security teams visibility into the cross-organizational security posture and supply chain and unparalleled access to curated security intelligence from millions of developers and security researchers around the world.

Training objectives

By the end of this course, students will be able to:

- Define GitHub Advanced Security (GHAS): Understand the importance of integral features such as

  Secret scanning, Code scanning, and Dependabot.
- Utilize GHAS: Learn how to maximize security impact using GHAS features.
- Understand GHAS in the Security Ecosystem: Recognize GHAS's role and its integration into the security workflow.
- Configure Dependabot: Learn to enable and configure Dependabot alerts and security updates.
- Implement Secret Scanning: Understand how to enable and use secret scanning to prevent secret leaks.
- Configure Code Scanning: Learn to implement and configure code scanning using CodeQL and other tools

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

Learning Path : GitHub Advanced Security

- Module 1: Introduction to GitHub Advanced Security
- Module 2: Configure Dependabot Security Updates on Your GitHub Repository
- Module 3: Configure and Use Secret Scanning in Your GitHub Repository
- Module 4: Configure Code Scanning on GitHub
- Module 5: Identify Security Vulnerabilities in Your Codebase by Using CodeQL
- Module 6: Code Scanning with GitHub CodeQL
- Module 7: GitHub Administration for GitHub Advanced Security
- Module 8: Manage Sensitive Data and Security Policies Within GitHub

Approach and methodology

Practical and structured approach combining focused theory and guided workshops. Participants gradually discover the fundamentals of GitHub Advanced Security through concrete exercises inspired by real-world software development scenarios, promoting immediate application of the learnings.

They learn how to identify vulnerabilities, secure code, protect secrets, and strengthen software supply chain security using GitHub’s integrated security features.

Led by a Microsoft Certified Trainer (MCT), the training focuses on interactivity and the development of directly transferable skills to help teams build and maintain secure software throughout the development lifecycle.

Prerequisites

Students should have the following knowledge and experience before attending this course:

- Experience in using and administering GitHub repositories.
- Experience of working with Microsoft Azure services.
- Technical skills in code scanning, dependency management, and secret scanning, and are familiar with tools like CodeQL and Dependabot.

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

Legal notices