# GitHub Advanced Security (GH-500)

## Description

La sécurité dans le développement logiciel n'a jamais été aussi cruciale qu'aujourd'hui. C'est pourquoi comprendre et maîtriser GitHub devient essentiel pour toute équipe de développement ambitieuse. La formation "Sécurité avancée GitHub (GH-500)" est conçue pour vous donner toutes les compétences nécessaires pour intégrer la sécurité dès les premières étapes de vos projets. Grâce aux puissantes fonctionnalités de GitHub Advanced Security, vous saurez comment protéger votre code, votre chaîne d'approvisionnement et vos secrets avant même la mise en production.

Ce cours vous propose une approche concrète et progressive, adaptée aux développeurs, chefs de projet et responsables de la sécurité. À travers des modules pratiques et accessibles, vous apprendrez à configurer des analyses de code, à utiliser CodeQL pour détecter les vulnérabilités, et à déployer des stratégies de sécurité robustes au sein de votre organisation.

## Pourquoi choisir la formation Sécurité avancée GitHub ?

Grâce à une compréhension approfondie de l'écosystème de GitHub, vous deviendrez un acteur clé de la sécurisation de vos projets. Vous découvrirez comment sécuriser vos dépôts, analyser vos dépendances et prévenir les fuites d'informations sensibles. Cette formation vous prépare à anticiper les risques et à réagir efficacement face aux menaces.

**Course Content**
**Module 1: Introduction to GitHub Advanced Security**

- Define GHAS and the importance of its core features
- Use GHAS to maximize its impact
- Understand GHAS and its role in the security ecosystem

**Module 2: Configure Dependabot security updates on your GitHub repository**

- Manage your dependencies on GitHub
- Dependabot alerts
- Dependabot security updates
- Manage Dependabot notifications and reports
- Dependency review

**Module 3: Configure and use secret scanning in your GitHub repository**

- Understand secret scanning
- Configure secret scanning
- Use secret scanning

**Module 4: Configure code scanning on GitHub**

- Understand code scanning
- Enable code scanning with third-party tools
- Configure code scanning

**Module 5: Identify security vulnerabilities in your codebase using CodeQL**

- Prepare a database for CodeQL
- Run CodeQL in a database
- Understand CodeQL results
- Fix issues identified by CodeQL

**Module 6: Code analysis with GitHub CodeQL**

- Understand what CodeQL is
- Understand how CodeQL analyzes code
- Understand what QL is
- Connect code scanning and CodeQL
- Customize your code analysis workflow with CodeQL: Part 1
- Reference a CodeQL query
- Customize your code analysis workflow with CodeQL: Part 2
- Use the CodeQL CLI interface
- Customize languages and builds for code scanning
- Configure a CodeQL language matrix

**Module 7: GitHub administration for GitHub Advanced Security**

- Understand GitHub Advanced Security
- Enable GitHub Advanced Security
- Manage access to GitHub Advanced Security
- Manage alerts and features of GitHub Advanced Security

**Module 8: Manage sensitive data and security policies in GitHub**

- Define security policies
- Create and manage repository rule sets
- Generate reports and audit logs

**Module 9: Identify security vulnerabilities in your codebase using CodeQL**

- Prepare a database for CodeQL
- Run CodeQL in a database
- Understand CodeQL results
- Fix issues identified by CodeQL

**Module 10: Code scanning with GitHub CodeQL**

- Understand what CodeQL is
- Analyze how CodeQL processes code
- Understand the QL language
- Connect code analysis and CodeQL
- Customize a code scanning workflow with CodeQL: Part 1
- Reference a CodeQL query

- Customize a code scanning workflow with CodeQL: Part 2
- Use the CodeQL CLI interface
- Customize languages and builds for code scanning
- Configure a CodeQL language matrix

**Module 11: GitHub administration for GitHub Advanced Security**

- Understand where GitHub Advanced Security fits into your development lifecycle
- Enable GitHub Advanced Security
- Manage access and usage of GitHub Advanced Security
- Manage alerts and associated features

**Module 12: Manage sensitive data and security policies within GitHub**

- Understand GitHub's basic security tools
- Create and apply security policies to repositories
- Manage repository rule sets
- Generate reports and audit security actions

**Lab / Exercises**

- This course provides you with exclusive access to the official Microsoft lab, enabling you to practice your skills in a professional environment.

**Documentation**

- Access to Microsoft Learn, Microsoft's online learning platform, offering interactive resources and educational content to deepen your knowledge and develop your technical skills.

**Participant profiles**

- Software developers
- Software architects
- DevOps engineers
- Information security managers
- Technical project managers

**Prerequisites**

- Have an active GitHub account
- Understand the basics of using GitHub
- Understand the fundamental principles of software development

**Objectives**

- Understand the core features of GitHub Advanced Security
- Configure security updates with Dependabot
- Set up and use secret scanning on GitHub
- Implement code scanning with CodeQL
- Identify and fix security vulnerabilities in code
- Administer and manage access to GitHub Advanced Security
- Define and enforce security policies within repositories

**Description**
GitHub Advanced Security (GH-500)
**Niveau**

Intermédiaire
**Classroom Registration Price (CHF)**
900
**Virtual Classroom Registration Price (CHF)**
850
**Duration (in Days)**
1
**Reference**
GH-500