

DevSecOps: Embedding Security in Application Development and Infrastructure

Duration: 1 day

Audience: Professionnel TI

Who is this training for?

People developing applications, people working in DevOps engineering, application security specialists

Training objectives

- Understand DevSecOps and shift-left principles
- Integrate security controls into CI/CD pipelines
- Automate code analysis and vulnerability detection
- Improve Dev-Sec-Ops collaboration

Summary

This course introduces the concept of DevSecOps, where security is integrated into DevOps pipelines and agile practices. You will learn how to equip and automate security from design to deployment.

Course outline

Module 1: Introduction to DevSecOps

- From DevOps to DevSecOps
- Shift-left Philosophy
- Organizational and Cultural Considerations

Module 2: Coding and Security Testing

- Static and Dynamic Analysis
- Automated Security Testing in CI/CD
- Code Review Best Practices

Module 3: Securing and Automating the Pipeline

- Tools for Integration (SonarQube, Snyk, GitHub Actions, etc.)
- Secrets Management and Secure Configuration
- Basics of Container Security and Kubernetes

Module 4: Case Study and Best Practices

- Hands-on Lab: Securing a CI/CD Pipeline
- Common Success Studies and Pitfalls
- Roadmap to DevSecOps Maturity

Approach and methodology

Practical, integrated and application lifecycle oriented approach. Participants learn how to integrate security into every stage of development, through hands-on workshops covering CI/CD, deployment, and operation. They are experimenting with integrating security mechanisms (code analysis, vulnerability management, access control) directly into DevOps pipelines and cloud infrastructures. The training emphasizes: Learning by doing with realistic DevSecOps scenarios Security integration scenarios (Shift Left) Demonstrations of security and automation tools Case analysis to understand risks and best practices

Prerequisites

- Knowledge of DevOps flows (CI/CD)
- Notions of secure coding

Recommendations

- Basics in software development (CI/CD, code management, pipelines)
- Understanding of DevOps concepts (automation, continuous integration, deployment)
- Knowledge of cybersecurity principles (vulnerabilities, access management, best practices)
- Notions of infrastructure (cloud, containers, networks)
-

Familiarity with version control tools (Git) Interest in integrating security from the development lifecycle (Shift Left)