AMBIENT-IT

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

Updated 06/04/2025

Sign up

DevSecOps discovery training

1 day (7 hours)

PRESENTATION

Our SecOps Discovery course provides architects, developers and security experts with a shared vision of the issues at stake, enabling them to speak the same language and initiate a structured approach.

Our training program will familiarize you with the concepts and skills needed to effectively identify and address vulnerabilities, software design through to production operations.

Demonstrations and feedback will illustrate how a strong SecOps culture enables architects, developers and security teams to speak the same language and work together seamlessly.

At the end of this training course, you'll have a clear view of the possibilities offered by SecOps in your company.

OBJECTIVES

- Acquire a common base of knowledge on the key concepts of operational security (SecOps) and its links with DevOps (DevSecOps)
- Understand the challenges and constraints of security in the application and software lifecycle infrastructures
- Assess the opportunity and relevance of adopting a SecOps / DevSecOps approach within the organization

TARGET AUDIENCE

- Software architects
- Cybersecurity Team

- Lead developers
- Possibly Ops/System administrators interested in security aspects

Prerequisites

- Basic knowledge of software development and/or architecture
- Sensitivity to cybersecurity (no need to be an expert)

Program of our DevSecOps discovery training course

Introduction to Operational Safety (SecOps)

- Background and definitions
- From DevOps to SecOps: why is security now at the heart of operations?
- Differences and complementarities between SecOps and DevSecOps
- Current issues and trends
- Growing number of cyberthreats and increasingly complex systems
- Evolving responsibilities and the need for collaboration

Safety Fundamentals in the Value Chain

- Application lifecycle and checkpoints (from design to production)
- Main vulnerabilities (OWASP Top 10, configuration errors, etc.) and detection methodologies
- Infrastructure risks: configuration, network, containers, virtualization, cloud
- Regulatory constraints: RGPD, ISO 27001, etc. (depending on the organization's context)
- Understanding the main concepts of risk and vulnerability to create a common language

The pillars of SecOps

- Culture and organization
- Collaboration between teams: sharing responsibilities, breaking down silos
- Integration of Sec and Ops teams throughout the delivery cycle
- Automation and tools
- Security supervision and monitoring (SIEM, SOC, etc.)
- Vulnerability management
- Identity and Access Management (IAM)
- Incident management process
- Detection, reaction and remediation
- Feedback and continuous improvement
- Identify how to integrate safety into operations (processes, culture, tools)

DevSecOps Panorama

- What is DevSecOps?
- How and why to shift safety to the left
- Examples of safe pipelines
- Key practices and tools
- SAST, DAST, IAST, Container Security, IaC Security
- CI/CD tools with integrated security controls
- Feedback
- Case studies of companies that have implemented a DevSecOps approach (successes, failures, lessons learned)
- Continuity between SecOps and DevOps
- Importance of the "Shift Left

Case study / Summary

- Setting the scene: open discussion around a concrete use case (e.g. an existing in-house project)
- Q&A: open forum to clarify key points
- Synthesis: review of key concepts and advice on how to initiate the process internally

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

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

Organization

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

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.