Reference: 2B/EN/AZ2001

DevSecOps on Azure AZ-2001 Training Course

Integrated Security in CI/CD and DevOps Pipelines

Duration: 1 Day | Hours: 7 h

Remote · Sessions guaranteed from 1 registrant · 60% hands-on practice

DESCRIPTION

This DevSecOps on Azure training teaches you how to implement automated security controls directly inside your integration and deployment processes. You will learn how to shift security left in your pipelines, manage secrets, scan vulnerabilities and enforce compliance policies using Azure DevOps and GitHub Advanced Security tools.

The programme follows the Microsoft AZ-2001 reference and combines secure pipeline design, container security, secret management with Azure Key Vault and operational coverage with Microsoft Defender for Cloud / Defender for DevOps.

LEARNING OBJECTIVES

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

- Understand the fundamentals of DevSecOps and the benefits of integrating security directly into DevOps pipelines
- Design and configure secure CI/CD pipelines using Azure DevOps and GitHub Actions
- Implement code scanning (SAST), secret management and dependency analysis in your workflows
- Apply OWASP best practices and container security in a cloud environment
- Monitor and respond to security alerts using Microsoft Defender for Cloud and GitHub Advanced Security

PREREQUISITES

- Knowledge of Azure DevOps or GitHub Actions (CI/CD pipeline basics)
- Proficiency in Git and understanding of DevOps workflows
- Basic knowledge of application security and automated testing practices

> *Because each participant is unique, a personalised interview is systematically organised in advance with our expert to design a training programme perfectly aligned with their objectives, level and professional challenges.*

TARGET AUDIENCE

- Developers, DevOps engineers, cloud/IT engineers and security professionals wishing to integrate security into their pipelines

- System administrators, cloud architects and quality/production managers
- Any technical professional seeking to understand and implement DevSecOps practices

DETAILED PROGRAMME

> The training alternates between theoretical input and hands-on practice (approximately 60% of the time). Modules are built around practical exercises based on real-world business use cases.

Module 1 – Introduction to DevSecOps and shift-left security

- DevSecOps mindset and shared responsibility
- Why automated security gates beat manual reviews
- Mapping risks to pipeline stages

Module 2 – Securing CI/CD pipelines on Azure DevOps and GitHub

- Service connections with least-privilege
- Branch protection, signed commits and approval flows
- Audit logs and pipeline-level alerting

Module 3 – Secret management with Azure Key Vault

- Key Vault provisioning and access policies
- Managed identities and federated credentials
- Removing secrets from code and pipelines

Module 4 – SAST, DAST and dependency scanning

- Static analysis with SonarQube and CodeQL
- Dynamic application security testing (OWASP ZAP)
- Software Composition Analysis (Snyk, Trivy)

Module 5 – Container security

- Image scanning in Azure Container Registry
- Hardening Dockerfiles and base images
- Runtime protection patterns

Module 6 – Microsoft Defender for Cloud and Defender for DevOps

- Defender for Cloud overview: posture and threat protection
- Defender for DevOps: GitHub and Azure DevOps coverage
- Azure Policy for compliance enforcement

Module 7 – GitHub Advanced Security (GHAS) integration

- Code scanning and secret scanning at scale
- Dependency review and supply chain hygiene
- Triage workflow and security campaigns

TEACHING METHODS

Format and Delivery

The training is delivered remotely via an interactive virtual classroom. It can also be delivered on-site, with content customised to match the needs of your professional project. The theory/practice split is approximately 40%/60%.

MFE-IT Ultra-Personalised Format

Each session accommodates between 1 and 3 participants, ensuring highly individualised support. A preliminary interview allows us to tailor the content to each participant's profile. Inter-company sessions are guaranteed from just 1 registrant (except in cases of force majeure).

Skills Assessment

Throughout the training, the trainer assesses participant progress through multiple-choice questions, role-playing exercises and hands-on work. At the end, a certificate of achievement is issued to each participant.

Post-Training Support

For one month following the training, each participant can contact MFE-IT trainers with questions about implementing acquired knowledge. A response is provided by email or telephone within 48 working hours.

Accessibility

MFE-IT is committed to welcoming people with disabilities. Contact: contact@mfe-it.com.

PRACTICAL INFORMATION

Trainer Resources

- Structured demonstrations aligned with the detailed programme
- Exercise briefs and solutions throughout the training
- A ready-to-use technical environment for practical workshops
- Trainer validation of acquired knowledge at the end of each workshop
- Digital reference documents

Certification and Validation

At the end of the training, a certificate is sent by email specifying the objectives, nature, duration and assessment results. A completion certificate can also be provided on request.

Benefits for Participants

- Train from your workplace or home, with no travel required
- Benefit from an expert trainer-consultant on the subject
- Enjoy an ultra-personalised format (1 to 3 participants)
- Continue training even in the event of unforeseen circumstances

Benefits for the Organisation

- Optimise the training budget by reducing travel and accommodation costs
- Offer quality training to all employees, regardless of location
- Reduce absence time linked to travel
- Support team upskilling in all contexts