DevSecOps Training

Duration: **2 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

This hands-on {*training} introduces participants to integrating**security within modern DevOps practices**, including CI/CD, Continuous Monitoring, and Infrastructure as Code (IaC).

Regulatory Note for Financial Institutions:
In compliance with the *Regulation on Banks' Information Systems and Electronic Banking Services* (Articles 16–25), DevSecOps pipelines in financial institutions must ensure **secure development**, **continuous vulnerability monitoring**, and **traceable audit mechanisms** for all deployments and code changes.

Participants will receive a fully functional **DevSecOps Lab VM** (Vagrant + Ansible) preloaded with open-source tools such as OWASP ZAP, HashiCorp Vault, and Semgrep to simulate real-world security automation pipelines.

Who Should Attend

Ideal for developers, DevOps engineers, and IT managers in**banks, financial institutions, and regulated enterprises**.

What You Will Learn

By the end of this {*training}, you will have gained knowledge and skills in the following areas:

- Automate security in CI/CD pipelines.
- Deploy and secure tools like Vault, ZAP, OpenVAS, and Semgrep.
- Align DevSecOps processes with **BDDK Article 23** compliance (secure software lifecycle and traceability).
- Build resilient, auditable, and regulation-ready DevOps environments.
- Act as **Security Champions** within agile teams.

By the end of this course, participants will confidently build**secure, compliant, and automated DevSecOps pipelines**
fully aligned with both **global best practices** and **BDDK banking regulations**.

Outline

DevSecOps Training

Duration: **2 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Day 1

Lab Setup

- Online Lab Setup
- Offline Lab Instructions

Introduction to DevOps

- What is DevOps?
- Lab : DevOps Pipeline

Introduction to DevSecOps

- Challenges for Security in DevOps
- DevOps Threat Model
- DevSecOps – Why, What and How?
- Vulnerability Management

Continuous Integration

Pre-Commit Hooks

- Introduction to Talisman
  - Lab : Running Talisman
  - Lab : Create your own regexes for Talisman

Secrets Management

- Introduction to HashiCorp Vault
- Demo : Vault Commands

Continuous Delivery

- Software Composition Analysis (SCA)
  - Introduction to Dependency-Check
  - Lab : Run Dependency-Check pipeline
  - Lab : Fix issues reported by Dependency-Check
- Static Analysis Security Testing (SAST)
  - Introduction to Semgrep
  - Lab : Run Semgrep pipeline
  - Lab : Create your own Semgrep Rules
  - Lab : Fix Issues reported by Semgrep
- Dynamic Analysis Security Testing (DAST)
  - Introduction to OWASP ZAP
  - Demo : Creating ZAP Context File
  - Lab : Run ZAP in pipeline

Day 2

Infrastructure As Code

- Vulnerability Assessment (VA)
  - Introduction to OpenVAS

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

    - Lab : Run OpenVAS pipeline
- Container Security (CS)
    - Introduction to Trivy
    - Lab : Run Trivy in Pipeline
    - Lab : Improvise Docker base image
- Compliance as Code (CaC)
    - Introduction to Inspec
    - Lab : Run Inspec in Pipeline
    - Lab : Improvise Docker compliancy controls

Continuous Monitoring

- Logging
    - Introduction to the ELK Stack
    - Lab : View Logs in Kibana
- Alerting
    - Introduction to ElastAlert and ModSecurity
    - Lab : View Alerts in Kibana
- Monitoring
    - Lab : Create Attack Dashboards in Kibana

DevSecOps in AWS

- DevOps on Cloud Native AWS
- AWS Threat Landscape
- DevSecOps in Cloud Native AWS

DevSecOps Challenges and Enablers

- Challenges with DevSecOps
- Building DevSecOps Culture
- Security Champions
- Case Studies
- Where do we Begin?
- DevSecOps Maturity Model