DevSecOps

Learn via: **Classroom**

Duration: **2 Day**

https://bilginc.com/en/training/devsecops-806-training/

Overview

Hands-on training to automate security into a fast-paced DevOps environment using various open-source tools and scripts.

Modern enterprises are implementing the technical and cultural changes required to embrace DevOps methodology by introducing practices such Continuous Integration (CI), Continuous Delivery (CD), Continuous Monitoring (CM) and Infrastructure as Code (IaC). DevSecOps extends DevOps by introducing security in each of these practices giving a certain level of security assurance in the final product. In this training, we will demonstrate using our state-of-the-art DevSecOps Lab as to how to inject security in CI, CD, CM and IaC.

This is a complete hands-on training with attendees requiring only a browser to complete the entire training. Attendees will receive the DevSecOps Lab built using Vagrant and Ansible comprising of various open-source tools and scripts to help the DevOps engineers in automating security within their CI/CD pipeline.

The attendees will receive a DevSecOps-Lab VM (designed by the NotSoSecure team) containing all the code, scripts and tools that are used for building the entire DevSecOps pipeline.

Prerequisites

Anybody with a background in IT or related to software development whether a developer or a manager can attend this course to get an insight about DevOps and DevSecOps.

What You Will Learn

Shift your organisation's security left, make it a less attractive target to attackers, and help it resist attacks by building a team that can develop resilient applications and systems using secure processes.

Trained delegates can:

- Implement security tools and build and automate secure processes within their DevOps pipelines
- Secure any DevOps environment, from development and staging to production
- Securely deploy all the latest DevSecOps technologies which are covered in the course
- Understand the business impact of DevSecOps principles and articulate this to key stakeholders
- Solve business and development problems with a security mindset
- Take on greater responsibility in the team and become an advocate of security in the wider business

Outline

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
    - 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