DevSecOps Bootcamp: Beginner Edition

Objective:

In today's world of continuous integration and continuous delivery, it has become imperative to involve security checks at every step of the process. Automation of build, deployment, setup preparation processes using DevOps process and automating code review, security scanning, security testing, vulnerability management using DevSecOps process improves the quality and security posture of the project while decreasing the chances of human error and overall delivery timeline. Hence, knowledge of DevSecOps has become an important skill for system administrators, security professionals and DevOps professionals.

In this bootcamp, we start with DevOps basics and cover building blocks/components used to create a DevOps pipeline. Then, learn about integration of security in different phases to convert a DevOps pipeline into a DevSecOps pipeline. The hands-on labs will be used to explore and practice all the tools individually. We will then learn to design and implement a DevOps pipeline end to end, using threat modelling to identify the threats and plan security measures, integrate security tools/scanners to the pipeline. In the last session, the attendees will learn to use publicly available CI/CD setups like GitLab for creating a DevSecOps pipeline. This bootcamp helps beginners learn essential concepts by encouraging them to try every activity/installation/configuration/integration hands-on in our purpose-built labs. As a result, at the end of this bootcamp, you will have job-ready skills to begin your journey as a DevSecOps Professional.

A non-exhaustive list of topics covered in this bootcamp includes:

Module I: Introduction to DevOps

Objective: Learn the basics of DevOps and SDLC processes, components required to implement a DevOps pipeline. Plan a pipeline for a web application and implement it for an on-premise setup involving virtual machines.

1. What is SDLC?
2. What is DevOps?
3. DevOps Building Blocks and Principles

4. Need of DevOps
5. What is Continuous Integration and Continuous Deployment?.
    a. Continuous Integration to Continuous Deployment to Continuous Delivery.
    b. Continuous Delivery vs Continuous Deployment.
    c. General workflow of CI/CD pipeline.
6. Phases of DevOps Pipeline
    a. Code Environment (IDE)
    b. Version Control System (VCS)
        i. Basics of Git VCS
        ii. Self Hosted VCS i.e. Gitlab, SCM
        iii. Publicly available VCS e.g. GitLab, GitHub, BitBucket
    c. Building the Project
        i. Manual Build vs Automated Build
        ii. Build Systems e.g. Maven, make, Dockerfile, Packer
    d. Testing
        i. Manual Testing vs Automated Testing
        ii. Automated Unit Testing e.g. JUnit, Pytest
        iii. Automated Functional Testing e.g. Selenium
    e. Deployment
        i. Manually creating the setup
        ii. Infrastructure as Code e.g. Ansible, Chef
    f. Continuous Integration (CI)
        i. Benefits of CI
        ii. CI solutions e.g. Jenkins, GitLab CI
            Lab : Continuous Integration lab for Django Webapp
    g. Monitoring
        i. Importance of Monitoring
        ii. Monitoring with NagiOS
            Concept and explanation what to monitor
    h. Maintenance
        i. Issue Tracking
        ii. Documentation
7. Case studies on DevOps Pipelines
8. Plan a DevOps Pipeline for a WebApp
9. Implement DevOps Pipeline for an On Premise model

Module II: DevSecOps: Adding Security to DevOps

This module is covered in Weeks 2 and 3 of the bootcamp.

Objective: Understand the secure SDLC and concept of integrating security in DevOps process, learn to perform threat modeling, identify the security components for the DevOps pipeline, install and configure the security tools to convert DevOps pipeline into DevSecOps pipeline.

1. What is Secure SDLC
2. Secure SDLC phases
3. DevSecOps Maturity Model (DSOMM)
4. Adding Security to DevOps
5. Phases of DevSecOps Pipeline
    a. Threat modelling
        i. What is Threat Modelling?
        ii. STRIDE vs DREAD approaches
        iii. Using ThreatSpec and BDD Security
    b. Automated Code Review
        i. What is Automated Code Review?
        ii. Using FindSecBugs, PMD, DevSkim tools
    c. Sensitive Information Scan
        i. What is Sensitive Information Scan?
        ii. Using Talisman, GitSecret,Trufflehog
    d. Static Code Analysis (SAST)
        i. What is SAST?
        ii. Using SonarQube, Graudit and Flawfinder
    e. Dynamic Code Analysis (DAST)
        i. What is DAST?
        ii. Using OWASP Zap, Arachini
    f. Software Component Analysis
        i. What is Software Component Analysis?
        ii. Using OWASP dependency check, Retire.js and Safety
    g. Vulnerability Management and Vulnerability Assessment
        i. What is Vulnerability Management and Vulnerability Assessment?
        ii. Using ArcherySec, DefectDojo, OpenVAS
    h. Compliance as Code
        i. What is Compliance as Code?
        ii. Using Inspec and Serverspec
    i. Secret Management
        i. Need for Secret Management
        ii. Using Hashicorp Vault, Torus
6. Case studies on DevSecOps Pipelines

7. Identify the security components for WebApp DevOps pipeline created in last session
8. Integrate the security components to form a DevSecOps pipeline

Module III: DevSecOps Pipelines on GitLab

Objective: Learn about GitLab CI fundamentals, configurations to create a DevSecOps pipeline on it. The GitLab can be hosted on-premise, in hosted service Gitlab.com and can also be installed on cloud infrastructure, making it a good choice for DevSecOps process.

1. Designing a DevOps Pipeline for a Django Web Application
2. Identifying the DevSecOps components to integrate
3. Introduction to GitLab CI
4. Writing gitlab-ci.yaml
5. Configuring Environment variables
6. Using secrets securely
7. Configuring Runners
8. Implementing Pipeline using GitLab CI
9. Integrating security tools