Implementing DevSecOps (LFS262)

DevSecOps practices are an extension to standard DevOps practices, focusing on automating security and incorporating it as part of the process, which includes Continuous Delivery, Infrastructure-as-Code (IaC), and observability. Use of DevSecOps results not only in delivering safer code faster, but also facilitates early feedback to developers, helping them build more reliable software. This course explores implementing DevSecOps practices into the software delivery pipeline using open source software.

Duration: 5 Days

Prerequisites for this course

- Have working knowledge of Linux operating systems and the command line interface, Git, Docker, and Kubernetes.
- Know how to build CI/CD pipelines, write Infrastructure-as-Code (IaC), run Ansible Playbooks, and understand observability concepts such as log management and monitoring.

Outline for this course

Chapter 1 – Course Introduction

Chapter 2 – What Is DevSecOps?

Chapter 3 – Setting Up the Lab Environment

Chapter 4 – Building a DevOps Pipeline

Chapter 5 – Securing the Supply Chain with SCA

Chapter 6 – Static Application Security Testing (SAST)

Chapter 7 – Auditing Container Images

Chapter 8 – Secure Deployment and Dynamic Application Security Testing (DAST)

Chapter 9 – System Security Auditing with IAC

Chapter 10 – Securing Kubernetes Deployments

Chapter 11 – Secrets Management with Vault

Chapter 12 – Runtime Security Monitoring and Remediation