Document Generated: 09/12/2026

Learning Style: On Demand

Technology: Linux Foundation

Difficulty: Beginner

Course Duration: 40 Hours

Implementing DevSecOps (LFS262)

About This Course:

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.

Course Objectives:

- This course begins by laying the foundation of DevSecOps, explaining the principles, practices, cultural aspects and tooling landscape. It then goes on to show you how to incorporate various practices into the Continuous Delivery pipeline: perform Software Composition Analysis (SCA) and add it to the Continuous Integration pipeline, perform static code analysis and project gating using SAST tools, implement security best practices while writing Dockerfiles to build images, scan container images for vulnerability, perform Dynamic Application Software Testing (DAST) on a live environment, set up a centralized vulnerability management system to provide visibility and alerting, and build a cloud native DevSecOps pipeline. You will also use IaC effectively to enforce compliance, collect logs, analyze events to provide detection and monitoring of security issues, and learn to address cloud and container related risks. In order to make adoption of DevSecOps practices frictionless, this course focuses on usage of mostly open source software, at the same time providing enough flexibility to plug in a commercial alternative to match the implementation environment.

Audience:

- This course is designed for software developers, site reliability engineers, and DevOps practitioners looking to speed up delivery of more secure code. To make the most of this course, learners must have working knowledge of Linux operating systems and the command line interface, Git, Docker, and Kubernetes. They must also 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.

Prerequisites:

To make the most out of this course, you will need to:

- 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.

Course Outline:

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