Document Generated: 01/18/2025

Learning Style: Virtual Classroom

Provider: Linux Foundation

Difficulty: Intermediate

Course Duration: 4 Days

Kubernetes Security Fundamentals (LFS460)

About this course:

This course exposes you to knowledge and skills needed to maintain security in dynamic, multi-project environments. This course addresses security concerns for cloud production environments and covers topics related to the security container supply chain, discussing topics from before a cluster has been configured through deployment, and ongoing, as well as agile use, including where to find ongoing security and vulnerability information. The course includes hands-on labs to build and secure a Kubernetes cluster, as well as monitor and log security events.

Audience:

- This course is ideal for anyone holding a CKA certification and interested in or responsible for cloud security..

Course Outline:

Introduction

- Linux Foundation
- Linux Foundation Training
- Linux Foundation Certifications
- Linux Foundation Digital Badges
- Laboratory Exercises, Solutions and Resources
- Things Change in Linux and Open Source Projects
- ELearning Course: LFS260
- Platform Details

Cloud Security Overview

- Multiple Projects
- What is Security?
- Assessment
- Prevention
- Detection
- Reaction
- Classes of Attackers
- Types of Attacks
- Attack Surfaces
- Hardware and Firmware Considerations
- Security Agencies
- Manage External Access
- Labs

Preparing to Install

- Image Supply Chain
- Runtime Sandbox
- Verify Platform Binaries

- Minimize Access to GUI
- Policy Based Control
- Labs

Installing the Cluster

- Update Kubernetes
- Tools to Harden the Kernel
- Kernel Hardening Examples
- Mitigating Kernel Vulnerabilities
- Labs

Securing the kubeapiserver

- Restrict Access to API
- Enable Kubeapiserver Auditing
- Configuring RBAC
- Pod Security Policies
- Minimize IAM Roles
- Protecting etcd
- CIS Benchmark
- Using Service Accounts
- Labs

Networking

- Firewalling Basics
- Network Plugins
- Mitigate Brute Force Login Attempts
- Ingress Objects
- Pod to Pod Encryption
- Restrict Cluster Level Access
- Labs

Workload Considerations

- Minimize Base Image
- Static Analysis of Workloads
- Runtime Analysis of Workloads
- Container Immutability
- Mandatory Access Control
- SELinux
- AppArmor
- Generate AppArmor Profiles
- Labs

Issue Detection

- Understanding Phases of Attack
- Preparation

- Understanding an Attack Progression
- During an Incident
- Handling Incident Aftermath
- Intrusion Detection Systems
- Threat Detection
- Behavioral Analytics
- Labs

Domain Reviews

- Preparing for the Exam
- Labs

Credly Badge:

Display your Completion Badge And Get The Recognition You Deserve.

Add a completion and readiness badge to your Linkedin profile, Facebook page, or Twitter account to validate your professional and technical expertise. With badges issued and validated by Credly, you can:

- Let anyone verify your completion and achievement by clicking on the badge
- Display your hard work and validate your expertise
- Display each badge's details about specific skills you developed.

Badges are issued by QuickStart and verified through Credly.

Find Out More or See List Of Badges