Course Description

Course: SEC201v5
SUSE Security v5 Deployment and Operations

Training Level:
- ❏ Intermediate

Delivery Method
- ❏ ILT

Duration:
- ❏ 3 days

Course Overview
This course provides a substantial guide to implementing, managing, and automating end-to-end container security using SUSE Security. Designed for technical professionals, the training introduces the entire cloud-native lifecycle—from securing the supply chain and CI/CD pipelines to defending active workloads at runtime. Participants will learn to deploy SUSE Security via SUSE Rancher Prime, configure automated admission controls, enforce zero-trust runtime protection, and utilize Deep Packet Inspection (DPI) via Web Application Firewall (WAF) and Data Loss Prevention (DLP) sensors. Through hands-on labs, students will gain practical experience with multi-cluster management, automated log forwarding, and programmatic administration using the REST API and CLI.

This course prepares students for the SCA in the SUSE Security exam.

Key Objectives
Attendees will be taught how to:
- ❏ Differentiate container and microservice network vulnerabilities from traditional application attack surfaces
- ❏ Deploy and automate security profiles across single or multi-cluster environments using Fleet and Helm
- ❏ Shift security left by integrating automated vulnerability and compliance scanning into CI/CD build pipelines
- ❏ Enforce admission controls to validate and intercept resource creation based on critical risk criteria
- ❏ Implement zero-trust protection by auto-learning and locking down process profiles, network rules, and file paths
- ❏ Intercept advanced threats utilizing built-in network attack detection alongside custom DLP and WAF sensors
- ❏ Federate global security policies centrally from a primary cluster down to all managed downstream environments
- ❏ Manage programmatically using example REST API scripts and the containerized Management CLI
- ❏ Integrate SIEM operations by forwarding structured log notifications to Webhooks and external Syslog servers

Audience
This course is specifically targeted at container software developers, IT cloud operators, security administrators, and DevOps personnel responsible for managing, auditing, and improving security compliance postures for containerized microservices.

Prerequisites
Participants need a basic understanding of containerization principles, Kubernetes orchestrator operations, and fundamental container development processes. Additionally, practical comfort working inside a standard Linux terminal shell is required.

Course Outline

- ❏ Section 1: Course Overview
- ❏ Section 2: Introduction to Container Security
  - ❏ The Need for Container Security
  - ❏ Threat and Vulnerability Management
  - ❏ SUSE Security
- ❏ Section 3: Deploying SUSE Security
  - ❏ Deployment Methods
  - ❏ Deploying SUSE Security using SUSE Rancher Prime
  - ❏ Deploying SUSE Security using Fleet
- ❏ Section 4: SUSE Security Management Console User Interface
  - ❏ Navigation within the Management Console
  - ❏ Security Risk Score
  - ❏ Assets
  - ❏ Network Activity
- ❏ Section 5: SUSE Security Management Console Basic Configuration
  - ❏ Configure SUSE Security Management Console Settings
  - ❏ Manage Local Users and Roles
  - ❏ Enable Authentication from External Directories
- ❏ Section 6: Supply Chain Security with SUSE Security
  - ❏ Vulnerability Scanning
  - ❏ Compliance Scanning
  - ❏ Admission Controls
- ❏ Section 7: Runtime Security with SUSE Security
  - ❏ Runtime Scanning
  - ❏ Threat Based Controls
  - ❏ Zero-Trust Controls
  - ❏ Runtime Security Management with SUSE Security
- ❏ Section 8: Multi-Cluster Management with SUSE Security
  - ❏ Federation
  - ❏ Multi-Cluster Policies
- ❏ Section 9: SUSE Security API and Command Line Management
  - ❏ REST API
  - ❏ SUSE Security Management CLI
- ❏ Section 10: Logging and Reporting
  - ❏ External Logging Services
  - ❏ SUSE Security Reports

SUSE Training

Information about SUSE Training can be found at:

https://www.suse.com/training/

Contact suse-training@suse.com with any questions.