SUSE Security Deployment and Operations (SEC201V5)

ID SEC201V5 **Price** CHF 1,450.—(excl. VAT) **Duration** 2 days

Who should attend

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 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

Course Content

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

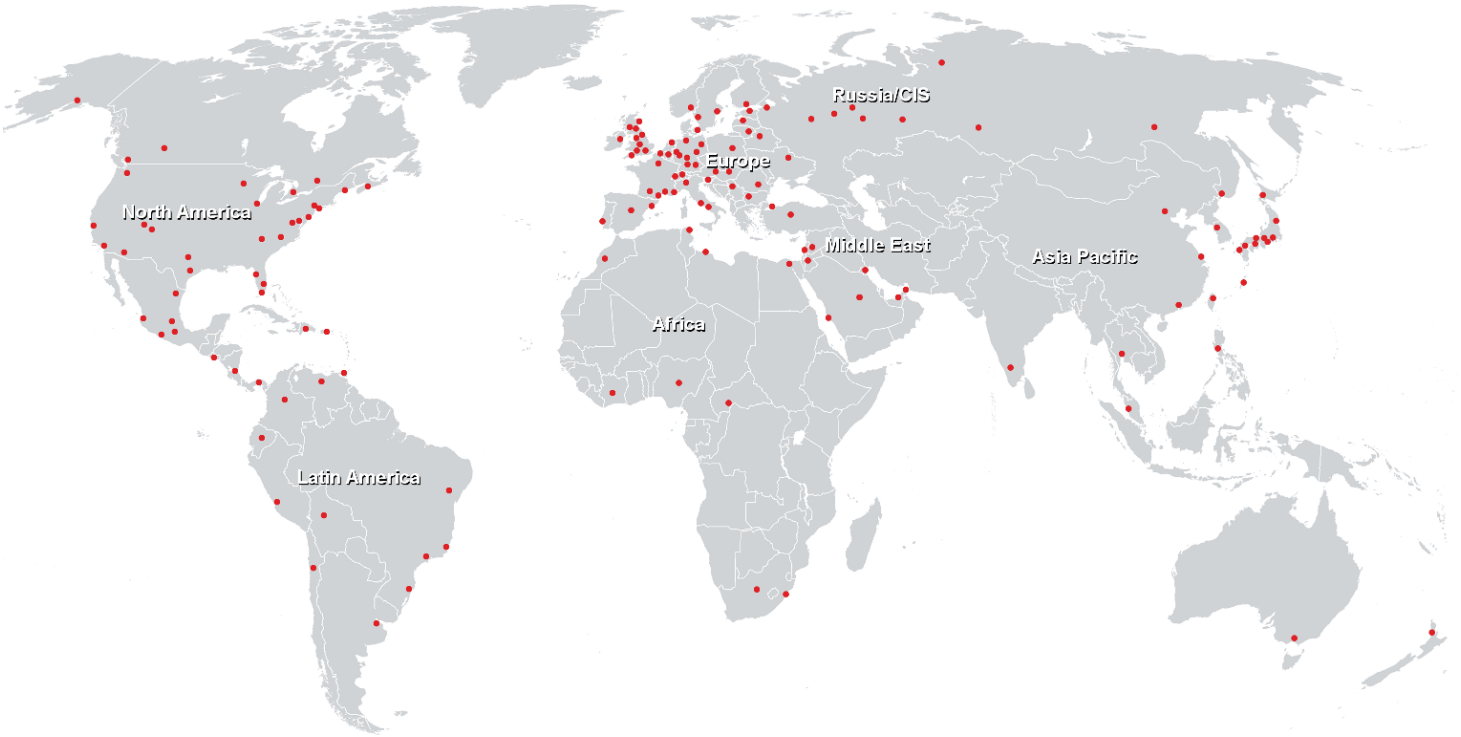
- REST API
- SUSE Security Management CLI

Section 10: Logging and Reporting

- External Logging Services
- SUSE Security Reports

SUSE Security Deployment and Operations (SEC201V5)

Training Centres worldwide



Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch