SUSE Security Deployment and Operations (SEC201V5)

ID SEC201V5 **Preis** CHF 1'450.– (exkl. MwSt.) **Dauer** 2 Tage

Zielgruppe

Dieser Kurs richtet sich speziell an Entwickler von Container-Software, IT-Cloud-Betreiber, Sicherheitsadministratoren und DevOps-Mitarbeiter, die für die Verwaltung, Überprüfung und Verbesserung der Sicherheitskonformität bei containerisierten Microservices verantwortlich sind.

Voraussetzungen

Die Teilnehmer benötigen Grundkenntnisse über die Prinzipien der Containerisierung, den Betrieb des Kubernetes-Orchestrators sowie grundlegende Prozesse der Containerentwicklung. Darüber hinaus sind praktische Kenntnisse im Umgang mit einer Standard-Linux-Terminal-Shell erforderlich.

Kursziele

Den Teilnehmern wird vermittelt, wie sie:

- Unterscheiden Sie Schwachstellen in Container- und Microservice-Netzwerken von den Angriffsflächen herkömmlicher Anwendungen
- Sicherheitsprofile mithilfe von Fleet und Helm in Umgebungen mit einem oder mehreren Clustern bereitstellen und automatisieren
- Die Sicherheit nach vorne verlagern, indem automatisierte Schwachstellen- und Compliance-Scans in CI/CD-Build-Pipelines integriert werden
- Zugriffskontrollen durchsetzen, um die Erstellung von Ressourcen anhand kritischer Risikokriterien zu überprüfen und zu unterbinden
- Implementieren Sie einen Zero-Trust-Schutz durch automatisches Erlernen und Sperren von Prozessprofilen, Netzwerkregeln und Dateipfaden
- Abwehren Sie komplexe Bedrohungen mithilfe der integrierten Erkennung von Netzwerkangriffen sowie benutzerdefinierter DLP- und WAF-Sensoren
- Globale Sicherheitsrichtlinien zentral von einem primären Cluster aus auf alle verwalteten nachgelagerten Umgebungen anwenden
- Programmgesteuerte Verwaltung mithilfe von Beispielskripten für die REST-API und der containerisierten Management-CLI
- Integrieren Sie SIEM-Abläufe, indem Sie strukturierte Protokollmeldungen an Webhooks und externe Syslog-Server weiterleiten

Kursinhalt

Abschnitt 1: Kursübersicht

Abschnitt 2: Einführung in die Containersicherheit

- Die Notwendigkeit von Containersicherheit
- Bedrohungs- und Schwachstellenmanagement
- SUSE-Sicherheit

Abschnitt 3: Bereitstellung von SUSE Security

- Bereitstellungsmethoden
- Bereitstellung von SUSE Security mit SUSE Rancher Prime
- Bereitstellung von SUSE Security mit Fleet

Abschnitt 4: Benutzeroberfläche der SUSE Security Management Console

- Navigation innerhalb der Verwaltungskonsole
- Sicherheitsrisikobewertung
- Vermögenswerte
- Netzwerkaktivität

Abschnitt 5: Grundlegende Konfiguration der SUSE Security Management Console

- Einstellungen der SUSE Security Management Console konfigurieren
- Lokale Benutzer und Rollen verwalten
- Authentifizierung über externe Verzeichnisse aktivieren

Abschnitt 6: Sicherheit in der Lieferkette mit SUSE Security

- Schwachstellen-Scans
- Compliance-Prüfung
- Zugangskontrollen

Abschnitt 7: Sicherheit zur Laufzeit mit SUSE Security

- Scannen während der Laufzeit
- Auf Bedrohungen basierende Kontrollmassnahmen
- Zero-Trust-Kontrollen
- Sicherheitsmanagement zur Laufzeit mit SUSE Security

Abschnitt 8: Verwaltung mehrerer Cluster mit SUSE Security

- Verband
- Richtlinien für mehrere Cluster

Abschnitt 9: SUSE-Sicherheits-API und Verwaltung über die Befehlszeile

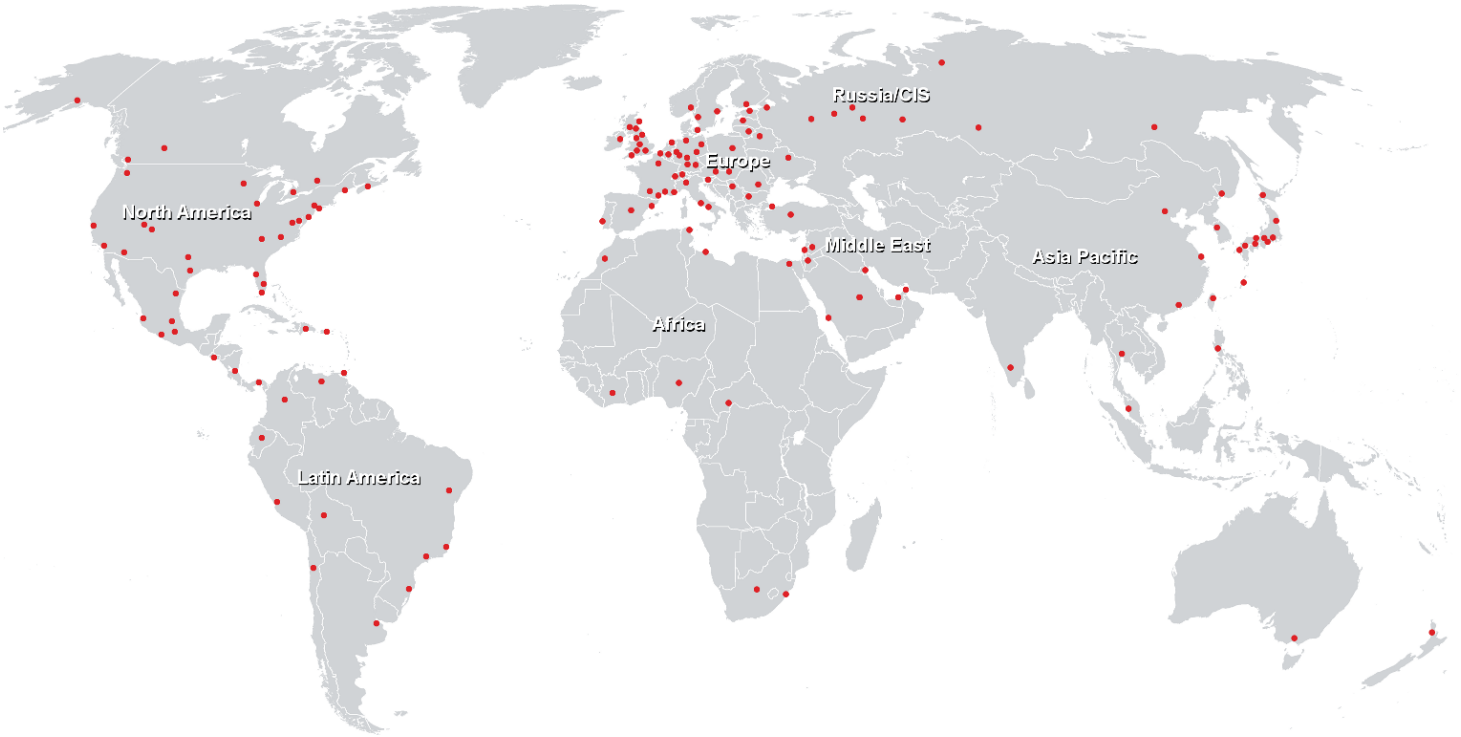
- REST-API
- SUSE Security Management-Befehlszeilenschnittstelle

Abschnitt 10: Protokollierung und Berichterstattung

- Externe Protokollierungsdienste
- SUSE-Sicherheitsberichte

SUSE Security Deployment and Operations (SEC201V5)

Weltweite Trainingscenter



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