Red Hat Security: Linux in Physical, Virtual, and Cloud (RH415)

ID RH415 **Price** CHF 3,690.—(excl. VAT) **Duration** 4 days

Who should attend

- System Administrator - responsible for supporting the company's physical and virtual infrastructure, systems, and servers
- IT Security Practitioner / Compliance & Auditor - responsible for ensuring the technology environment is protected from attacks and is in compliance with security/privacy rules and regulations.
- Automation Architect - Engineer or architect responsible for the company's automation development and optimizing cloud tools and infrastructure to achieve automation goals.

Prerequisites

- Take our free assessment to gauge whether this offering is the best fit for your skills.
- Red Hat Certified Engineer (EX294 / RHCE) certification or equivalent Red Hat Enterprise Linux knowledge and experience.

Course Objectives

- As a result of attending this course, students should be able to use security technologies included in Red Hat Enterprise Linux to manage security risk and help meet compliance requirements.
- Analyze and remediate system compliance by using OpenSCAP and SCAP Workbench, and using and customizing baseline policy content that is provided with Red Hat Enterprise Linux.
- Monitor security-relevant activity on your systems with the kernel's Audit infrastructure.
- Explain and implement advanced SELinux techniques to restrict access by users, processes, and virtual machines.
- Confirm the integrity of files and their permissions with AIDE.
- Prevent unauthorized USB devices from being used with USBGuard.
- Protect data at rest but provide secure automatic decryption at boot by using Network-Bound Device Encryption (NBDE).
- Proactively identify risks and misconfigurations of systems and remediate them with Red Hat Insights.
- Analyze and remediate compliance at scale with OpenSCAP, Red Hat Insights, Red Hat Satellite, and Red Hat Ansible Automation Platform.

Impact on the organization

This course is intended to develop the skills that are needed to reduce security risk and to implement, manage, and remediate compliance and security issues in an efficient way at scale. The tools and techniques can help to ensure that systems are configured and deployed in a way that meets security and compliance needs, that they continue to meet those requirements, and that as those requirements are revised, all existing systems can be audited, and remediations and changes consistently applied. This outcome may help the business to efficiently reduce the risk of security breaches, which have a high cost in business disruption, brand erosion, loss of customer and shareholder trust, and financial costs for post-incident remediation. In addition, the organization may be able to use the tools in this course to help demonstrate that the compliance requirements set by customers, auditors, or other stakeholders have been met.

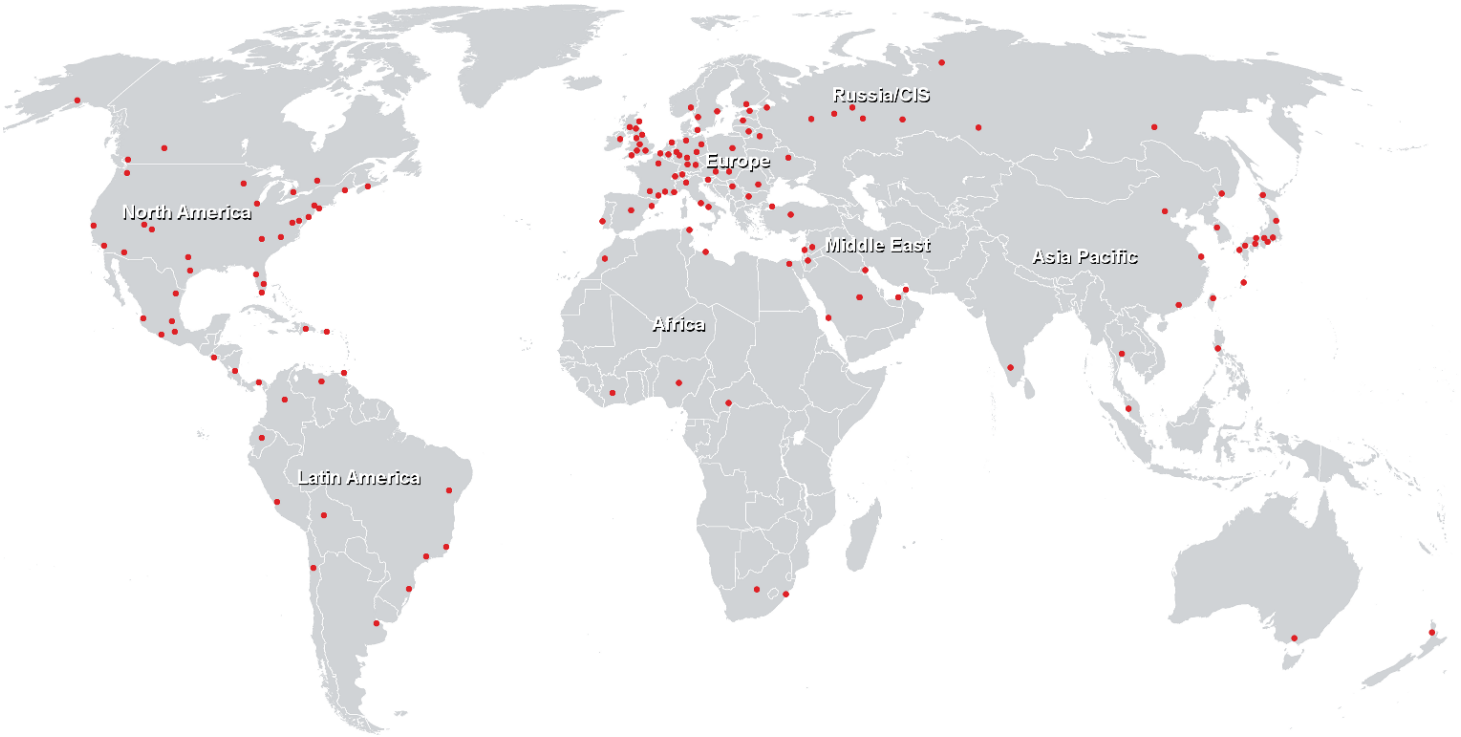
Impact on the individual

Course Content

- Manage compliance with OpenSCAP.
- Enable SELinux on a server from a disabled state, perform basic analysis of the system policy, and mitigate risk with advanced SELinux techniques.
- Proactively identify and resolve issues with Red Hat Insights.
- Monitor activity and changes on a server with Linux Audit and AIDE.
- Protect data from compromise with USBGuard and storage encryption.
- Manage authentication controls with PAM.
- Manually apply provided Ansible Playbooks to automate mitigation of security and compliance issues.
- Scale OpenSCAP and Red Hat Insights management with Red Hat Satellite and Red Hat Ansible Automation Platform.

Red Hat Security: Linux in Physical, Virtual, and Cloud (RH415)

Training Centres worldwide



Fast Lane Institute for Knowledge Transfer GmbH

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

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