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

**Length**: 4 Days

**Summary**: This course is ideal for security administrators and system administrators who need to manage the secure operation of servers running Red Hat® Enterprise Linux®, whether deployed on physical hardware, as virtual machines, or as cloud instances.

Maintaining security of computing systems is a process of managing risk through the implementation of processes and standards backed by technologies and tools. In this course, you will discover and understand the resources that can be used to help you implement and comply with your security requirements.

This course is based on Red Hat Enterprise Linux 7.5, Red Hat Satellite 6.3, Red Hat Ansible® Engine 2.5, Red Hat Ansible Tower 3.2, and Red Hat Insights.

**Learning Objectives**: Students that complete this course should be able to demonstrate these skills:

- Analyze and remediate system compliance using OpenSCAP and SCAP Workbench, employing and customizing baseline policy content 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 using 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 Tower.

**Target Audience**: System administrators, IT security administrators, IT security engineers, and other professionals responsible for designing, implementing, maintaining, and managing the security of Red Hat Enterprise Linux systems and ensuring their compliance with the organization's security policies.

**Prerequisites**: Be a Red Hat Certified Engineer (RHCE®), or demonstrate equivalent Red Hat Enterprise Linux knowledge and experience.

## COURSE CONTENT

### 1 - MANAGE SECURITY AND RISK

Define strategies to manage security on Red Hat Enterprise Linux servers.

### 2 - AUTOMATE CONFIGURATION AND REMEDIATION WITH ANSIBLE

Remediate configuration and security issues with Ansible Playbooks.

### 3 - PROTECT DATA WITH LUKS AND NBDE

Encrypt data on storage devices with LUKS and use NBDE to manage automatic decryption when servers are booted.

### 4 - RESTRICT USB DEVICE ACCESS

Protect system from rogue USB device access with USB Guard.

### 5 - CONTROL AUTHENTICATION WITH PAM

Manage authentication, authorization, session settings, and password controls by configuring pluggable authentication modules (PAMs).

### 6 - RECORD SYSTEM EVENTS WITH AUDIT

Record and inspect system events relevant to security, using the Linux kernel's audit subsystem and supporting tools.

### 7 - MONITOR FILE SYSTEM CHANGES

Detect and analyze changes to a server's file systems and their contents using AIDE.

### 8 - MITIGATE RISK WITH SELINUX

Improve security and confinement between processes by using SELinux and advanced SELinux techniques and analyses.

### 9 - MANAGE COMPLIANCE WITH OPENSCAP

Evaluate and remediate a server's compliance with security policies by using OpenSCAP.

### 10 - AUTOMATE COMPLIANCE WITH RED HAT SATELLITE

Automate and scale your ability to perform OpenSCAP checks and remediate compliance issues using Red Hat Satellite.

### 11 - ANALYZE AND REMEDIATE ISSUES WITH RED HAT INSIGHTS

Identify, detect, and correct common issues and security vulnerabilities with Red Hat Enterprise Linux systems by using Red Hat Insights.

### 12 - PERFORM A COMPREHENSIVE REVIEW

Review the content covered in this course by completing hands-on review exercises.