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

Duration: **4 Days**

Course Description:

Maintaining the security of computing systems is a process of managing risk through the implementation of processes and standards backed by technologies and tools. "Red Hat Security: Linux in Physical, Virtual, and Cloud" (RH415) is designed 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. You will learn about technologies and tools that can be used to help you implement and comply with your security requirements, including the kernel's Audit subsystem, AIDE, SELinux, OpenSCAP and SCAP Workbench, USBGuard, PAM authentication, and Network-Based Device Encryption. You will learn to monitor compliance and to proactively identify, prioritize, and resolve issues by using OpenSCAP, Red Hat Insights, Red Hat Satellite, and Red Hat Ansible Automation Platform. You will have a basic introduction to how Red Hat Ansible Automation Platform automates the deployment of remediation to systems, by using Ansible Playbooks from OpenSCAP or Red Hat Insights.

This course is based on RHEL 9.2, Ansible Core 2.14, Red Hat Ansible Automation Platform 2.4, Satellite 6.14, and OpenSCAP 1.3.7.

Maintaining the 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 learn about resources that can be used to help you implement and comply with your security requirements.

Intended Audience:

- 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.

Course Outlines:

Managing Security and Risk

- Define and implement strategies to manage security on Red Hat Enterprise Linux systems.

Automating Configuration and Remediation with Ansible

- Remediate configuration and security issues automatically with Ansible Playbooks.

Protecting Data with LUKS and NBDE

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

Restricting USB Device Access

- Protect systems from rogue USB device access with USBGuard.

Controlling Authentication with PAM

- Manage authentication, authorization, session settings, and password controls by configuring Pluggable Authentication Modules (PAM).

Recording System Events with Audit

- Record and inspect system events relevant to security by using the Linux kernel's Audit system and supporting tools.

Monitoring File System Changes

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

Mitigating Risk with SELinux

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

Managing Compliance with OpenSCAP

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

Analyzing and Remediating 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**.**

Automating Compliance with Red Hat Satellite

- Automate and scale OpenSCAP compliance checks by using Red Hat Satellite.

Comprehensive Review

- Review tasks from Red Hat Security: Linux in Physical, Virtual, and Cloud.