Red Hat Security: Linux in Physical, Virtual, and Cloud

Duration: 4 Days **Course Code: RH415**

Overview:

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.
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.

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.

Objectives:

- 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 learn about resources that can be used to help you implement and comply with your security requirements.
- Course content summary
- 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 Tower.

Prerequisites:

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

Follow-on-Courses:

• Red Hat Certified Specialist in Security: Linux exam (EX415)

• Red Hat Satellite 6 Administration (RH403)

• Recommended for those interested in learning more about Red Hat Satellite

• Automation with Ansible I (DO407) and Automation with Ansible II: Ansible Tower (DO409)

• Recommended for those who want to use DevOps practices to ensure security

Content:

Manage security and risk

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

Automate configuration and remediation with Ansible

Remediate configuration and security issues with Ansible Playbooks.

Protect data with LUKS and NBDE

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

Restrict USB device access

Protect system from rogue USB device access with USBGuard.

Control authentication with PAM

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

Record system events with audit

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

Monitor file system changes

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

Mitigate risk with SELinux

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

Manage compliance with OpenSCAP

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

Automate compliance with Red Hat Satellite

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

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.

Perform a comprehensive review

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

Note: Course outline is subject to change with technology advances and as the nature of the underlying job evolves. For questions or confirmation on a specific objective or topic, contact your Training Advisor or call us.

Additional Information:

Impact on the organization
This course is intended to develop the skills needed to reduce security risk and to implement, manage, and remediate compliance and security issues in an efficient way. The tools and techniques can be used 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 all existing systems can be audited and remediations and changes consistently applied as those requirements are revised. This flexibility may help the business to efficiently reduce 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 compliance requirements set by customers, auditors, or other stakeholders have been met.

Red Hat has created this course in a way intended to benefit our customers, but each company and infrastructure is unique, and actual results or benefits may vary.

Impact on the individual
As a result of attending this course, you should be able to use security technologies included in Red Hat Enterprise Linux to manage security risk and help meet compliance requirements.

You 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.

Further Information:

For More information, or to book your course, please call us on 00 971 4 446 4987

training@globalknowledge.ae

www.globalknowledge.com/en-ae/

Global Knowledge, Dubai Knowledge Village, Block 2A,First Floor, Office F68, Dubai, UAE