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

Duration: 4 Days Course Code: RH415

Overview:

The "Red Hat Security: Linux in Physical, Virtual, and Cloud" (RH415) course is designed for security and system administration personnel who manage the secure operation of computer systems running Red Hat Enterprise Linux on physical hardware, as virtual machines, or as cloud instances both in private data centers and on public cloud platforms.
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.
- Following course completion, you will receive a 45-day extended access to hands-on labs for any course that includes a virtual environment.
- **Note:** This course is offered as a five day virtual class or self-paced. Durations may vary based on the delivery. For full course details, scheduling, and pricing, select your location then “get started” on the right hand menu.

Target Audience:

System Administrator- responsible for supporting the companys 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 companys automation development and

Objectives:

- 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.

Prerequisites:

Recommended training

- Red Hat Certified Engineer (EX294 / RHCE) certification or equivalent Red Hat Enterprise Linux knowledge and experience.

Technology considerations

- If the instructor intends to demonstrate Red Hat Insights, internet access and appropriate entitlements are required.

Testing and Certification

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

Content:

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.

Additional Information:

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 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.

Further Information:

For More information, or to book your course, please call us on Head Office Tel.: +974 40316639

training@globalknowledge.qa

www.globalknowledge.com/en-qa/

Global Knowledge, Qatar Financial Center, Burj Doha,Level 21, P.O.Box 27110, West Bay, Doha, Qatar