Red Hat Security: Linux in Physical, Virtual, and Cloud («RH416»)

This course 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.

Duration: 5 days
Price: 4'050.–

Content

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 outline

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.

Key Learnings

- Managing compliance with OpenSCAP
- Enabling SELinux on a server from a disabled state, performing basic analysis of the system policy, and mitigating risk with advanced SELinux techniques
- Proactively identifying and resolving issues with Red Hat Insights
- Monitoring activity and changes on a server with Linux Audit and AIDE
- Protecting data from compromise with USBGuard and storage encryption
- Managing authentication controls with PAM
- Manually applying provided Ansible Playbooks to automate mitigation of security and compliance issues
- Scaling OpenSCAP and Red Hat Insights management with 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.

Any questions?

We are happy to advise you on +41 44 447 21 21 or info@digicomp.ch. You can find detailed information about dates on www.digicomp.ch/courses-it-provider/red-hat/red-hat-enterprise-linux/course-red-hat-security-linux-in-physical-virtual-and-cloud