

---

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

Varighed: 4 Days    Kursus Kode: RH415

---

### Beskrivelse:

#### Manage security of Red Hat Enterprise Linux systems deployed in bare-metal, virtual, and cloud environments

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.

#### Course overview

Security of computing systems is a process of managing risk through the implementation of processes and standards backed by technologies and tools. You will learn about resources that can be used to help you implement and comply with your security requirements.

---

### Målgruppe:

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.

---

### Agenda:

- 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.
- 

### Forudsætninger:

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

---

## Indhold:

Manage security and risk	Control authentication with PAM	Manage compliance with OpenSCAP
Define strategies to manage security on Red Hat Enterprise Linux servers.	Manage authentication, authorization, session settings, and password controls by configuring pluggable authentication modules (PAMs).	Evaluate and remediate a server's compliance with security policies by using OpenSCAP.
Automate configuration and remediation with Ansible	Record system events with audit	Automate compliance with Red Hat Satellite
Remediate configuration and security issues with Ansible Playbooks.	Record and inspect system events relevant to security, using the Linux kernel's audit subsystem and supporting tools.	Automate and scale your ability to perform OpenSCAP checks and remediate compliance issues using Red Hat Satellite.
Protect data with LUKS and NBDE	Monitor file system changes	Analyze and remediate issues with Red Hat Insights
Encrypt data on storage devices with LUKS and use NBDE to manage automatic decryption when servers are booted.	Detect and analyze changes to a server's file systems and their contents using AIDE.	Identify, detect, and correct common issues and security vulnerabilities with Red Hat Enterprise Linux systems by using Red Hat Insights.
Restrict USB device access	Mitigate risk with SELinux	Perform a comprehensive review
Protect system from rogue USB device access with USBGuard.	Improve security and confinement between processes by using SELinux and advanced SELinux techniques and analysis.	Review the content covered in this course by completing hands-on review exercises.

---

## Flere Informationer:

For yderligere informationer eller booking af kursus, kontakt os på tlf.nr.: 44 88 18 00

[training@globalknowledge.dk](mailto:training@globalknowledge.dk)

[www.globalknowledge.com/da-dk/](http://www.globalknowledge.com/da-dk/)

Global Knowledge, Stamholmen 110, 2650 Hvidovre