KOENIG
step forward

redhat
CERTIFIED
TRAINING PARTNER

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

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.