Red Hat Certified Specialist in Security: Linux

Course Outline

1. Managing Security and Risk
Define and implement strategies to manage security on Red Hat Enterprise Linux systems.

2. Automating Configuration and Remediation with Ansible
Remediate configuration and security issues automatically with Ansible Playbooks.

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

4. Restricting USB Device Access
Protect systems from rogue USB device access with USBGuard.

5. Controlling Authentication with PAM
Manage authentication, authorization, session settings, and password controls by configuring Pluggable Authentication Modules (PAM).

6. Recording System Events with Audit
Record and inspect system events relevant to security by using the Linux kernel's Audit system and supporting tools.

7. Monitoring File System Changes
Detect and analyze changes to a server's file systems and their contents by using AIDE.

8. Mitigating Risk with SELinux
Improve security and confinement between processes by using SELinux and advanced SELinux techniques and analysis.

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

10. 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.

11. Automating Compliance with Red Hat Satellite
Automate and scale OpenSCAP compliance checks by using Red Hat Satellite.

12. Comprehensive Review
Review tasks from Red Hat Security: Linux in Physical, Virtual, and Cloud.