Red Hat Security: Linux in Physical, Virtual, and Cloud with Exam (EX415)

Durée: 5 Jours **Réf de cours: RH416** **Méthodes d'apprentissage: Virtual Learning**

Résumé:

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.

Public visé:

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.

Objectifs pédagogiques:

- 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.

Pré-requis:

Test et certification

EX415 - Red Hat Certified Specialist in Security: Linux exam.

By passing this exam, you become a Red Hat Certified Specialist: Linux, which also counts toward becoming a Red Hat Certified Architect (RHCA®).

This exam is based on Red Hat Enterprise Linux version 7.5.

Après cette formation, nous vous conseillons le(s) module(s) suivant(s):

Recommended next exam or courseRed Hat Satellite 6 Administration (RH403) Recommended for those interested in learning more about Red Hat Satellite

Automation with Ansible I (DO407) and Automation with Ansible II: Ansible Tower (DO409) Recommended for those who want to use DevOps practices to ensure security

Contenu:

- 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 reviewReview the content covered in this course by completing hands-on review exercises.

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• Modalités d'évaluation : le participant est invité à s’auto-évaluer par rapport aux objectifs énoncés.
• Chaque participant, à l'issue de la formation, répond à un questionnaire de satisfaction qui est ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d’inscription :

•Vous pouvez vous inscrire sur l’une de nos sessions planifiées en inter-entreprises jusqu’à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
•Votre place sera confirmée à la réception d'un devis ou ""booking form"" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
•Attention, si vous utilisez votre Compte Personnel de Formation pour financer votre inscription, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés.