

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

ID RH415 Preis 3.320,- € (exkl. MwSt.) Dauer 4 Tage

Kursüberblick

Der Kurs Red Hat Security: Linux in Physical, Virtual, and Cloud (RH415) ist für Sicherheits- und Systemadministratoren gedacht, die für die sichere Ausführung von Servern mit Red Hat® Enterprise Linux® verantwortlich sind, und zwar egal, ob sie auf physischer Hardware, als virtuelle Rechner oder Cloud-Instanzen implementiert sind.

Dieser Kurs basiert auf Red Hat Enterprise Linux 7.5, Red Hat Satellite 6.3, Red Hat Ansible® Engine 2.5, Red Hat Ansible Tower 3.2 und Red Hat Insights.

Zielgruppe

System- und IT-Sicherheitsadministratoren, IT-Sicherheitsingenieure und andere Fachleute, die für das Design, die Implementierung, Wartung und Verwaltung der Sicherheit von Red Hat Enterprise Linux Systemen sowie ihre Compliance mit den Sicherheitsrichtlinien der Organisation verantwortlich sind.

Voraussetzungen

Qualifikation zum Red Hat Certified Engineer (RHCE®) oder nachweisliche vergleichbare Kenntnisse und Erfahrungen in Bezug auf Red Hat Enterprise Linux

Kursziele

Auswirkungen auf die Organisation

In diesem Kurs werden die Kenntnisse und Fertigkeiten zur Verringerung von Sicherheitsrisiken

bzw. für die effiziente Implementierung, Verwaltung und Behebung von Compliance- und Sicherheitsproblemen vermittelt. Mit den Tools und Techniken können Sie sicherstellen, dass Systeme auf eine Art und Weise konfiguriert und implementiert werden, die eine kontinuierliche Erfüllung von Sicherheits- und Compliance-Anforderungen gewährleistet und dass alle aktuellen Systeme geprüft und Korrekturen und Änderungen auch bei sich verändernden Anforderungen einheitlich angewandt werden. Mit dieser Flexibilität können Unternehmen Sicherheitsverletzungen effizient reduzieren, die eine geschäftliche Disruption, Markenerosion, einen Verlust des Kunden- und Aktionärsvertrauens sowie hohe Kosten für eine nachträgliche Problembehebung verursachen. Dazu können Sie die in diesem Kurs vorgestellten Tools dazu verwenden, um die Erfüllung der von Kunden, Prüfern oder anderen Stakeholdern festgelegten Compliance-Anforderungen nachzuweisen.

Red Hat hat diesen Kurs in erster Linie für seine Kunden entwickelt. Da aber jedes Unternehmen, jede Infrastruktur anders ist, kann es sein, dass die gezeigten Vorteile von Fall zu Fall variieren.

Auswirkungen auf den Einzelnen

Nach Abschluss dieses Kurses sollten Sie in der Lage sein, mit den in Red Hat Enterprise Linux integrierten Tools Sicherheitsrisiken zu verwalten und zur Erfüllung von Compliance-Anforderungen beizutragen.

Sie sollten in der Lage sein, folgende Aufgaben auszuführen:

- Analyse und Korrektur der System-

- Compliance mit OpenSCAP und SCAP Workbench unter Nutzung bzw. Anpassung von Basisrichtlinieninhalten in Red Hat Enterprise Linux
- Überwachung sicherheitsrelevanter Aktivitäten auf Ihren Systemen mit der Audit-Infrastruktur des Kernels
- Erläuterung und Implementierung fortschrittlicher SELinux-Techniken zur Beschränkung des Zugriffs durch Nutzer, Prozesse und VMs
- Bestätigung der Integrität von Dateien sowie ihrer Berechtigungen mit AIDE
- Unterbindung der Nutzung nicht autorisierter USB-Geräte mit USBGuard
- Schutz gespeicherter Daten bzw. Gewährleistung einer sicheren automatischen Entschlüsselung beim Systemstart mit NBDE
- Proaktive Identifizierung von Risiken und Fehlkonfigurationen von Systemen und ihre Behebung mit Red Hat Insights
- Analyse und Korrektur der Compliance im großen Maßstab mit OpenSCAP, Red Hat Insights, Red Hat Satellite und Red Hat Ansible Tower.

Kursinhalt

Die Verwaltung der Sicherheit von Computing-Systemen ist ein Prozess der Risikoverwaltung im Rahmen der Implementierung von Prozessen und Standards, der mit Technologien und Tools unterstützt wird. In diesem Kurs erfahren Sie alles zu den Ressourcen, die Sie bei der Implementierung und Einhaltung Ihrer Sicherheitsanforderungen unterstützen.

Überblick über den Kursinhalt

- Compliance-Verwaltung mit OpenSCAP
- Aktivierung von SELinux auf einem Server aus einem deaktivierten Zustand heraus, Durchführung einer grundlegenden Analyse der Systemrichtlinie und Risikominderung mit modernen SELinux-Techniken
- Proaktive Identifizierung und Behebung von Problemen mit Red Hat Insights
- Überwachung von Aktivitäten und Änderungen auf einem Server mit Linux Audit und AIDE

- Datenschutz mit USBGuard und Storage-Verschlüsselung
- Verwaltung von Authentifizierungs-Tools mit PAM
- Manuelle Anwendung bereitgestellter Playbooks zwecks Automatisierung der Behebung von Sicherheits- und Compliance-Problemen
- Skalierung von OpenSCAP und Red Hat Insights Management mit Red Hat Satellite und Red Hat Ansible Tower.

Detaillierter Kursinhalt

Verwaltung von Sicherheit und Risiken

Strategien zur Verwaltung der Sicherheit auf Red Hat Enterprise Linux Servern definieren

Automatisierung der Konfiguration und Fehlerbehebung mit Ansible

Konfigurations- und Sicherheitsprobleme mit Ansible Playbooks beheben

Datenschutz mit LUKS und NBDE

Storage-Geräte mit LUKS verschlüsseln und NBDE zur Verwaltung der automatischen Entschlüsselung beim Serverstart nutzen

Beschränkung des Zugriffs auf USB-Geräte

System mit USBGuard vor unkoordinierten Zugriffen mit USB-Geräten schützen

Kontrolle der Authentifizierung mit PAM

Authentifizierung, Autorisierung, Sitzungseinstellungen und Passwortkontrollen durch die Konfiguration von PAMs (Pluggable Authentication Modules) verwalten

Aufzeichnung von Systemereignissen bei Prüfungen

Sicherheitsrelevante Systemereignisse mit dem Audit-Subsystem und den unterstützenden Tools des Linux Kernels aufzeichnen und prüfen

Überwachung von Dateisystem-Änderungen

Änderungen an den Dateisystemen eines Servers und ihrer Inhalte mit AIDE erkennen und analysieren

Risikominderung mit SELinux

Sicherheit und Quarantäne zwischen Prozessen mit SELinux und modernen SELinux-Techniken und -Analysen verbessern

Compliance-Verwaltung mit OpenSCAP

Server-Compliance mit Sicherheitsrichtlinien durch Verwendung von OpenSCAP prüfen und beheben

Compliance-Automatisierung mit Red Hat Satellite

OpenSCAP-Prüfungen automatisieren und skalieren bzw. Compliance-Probleme mit Red Hat Satellite beheben

Problemanalyse und -behebung mit Red Hat Insights

Häufige Probleme und Schwachstellen bei Red Hat Enterprise Linux Systemen mit Red Hat Insights erkennen und korrigieren.

Ausführliche Überprüfung

Die in diesem Kurs abgedeckten Inhalte mit praktischen Übungen prüfen.