

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

Duración: 4 Días **Código del Curso: RH415** **Método de Impartición: Curso Remoto (Virtual)**

Temario:

El curso Red Hat Security: Linux in Physical, Virtual, and Cloud (RH415) está diseñado para los administradores de seguridad y de sistemas que necesiten gestionar la operación segura de los servidores que ejecutan Red Hat® Enterprise Linux®, ya sea que se encuentren implementados en el hardware físico, como máquinas virtuales o como instancias de nube.

Este se basa en Red Hat Enterprise Linux 7.5, Red Hat Satellite 6.3, Red Hat Ansible® Engine 2.5, Red Hat Ansible Tower 3.2 y Red Hat Insights.

El mantenimiento de la seguridad de los sistemas informáticos es un proceso de gestión de riesgos que implica implementar procesos y estándares con el respaldo de las tecnologías y las herramientas. En este curso, aprenderá sobre los recursos que se pueden utilizar para implementar requisitos de seguridad y cumplir con ellos.

Curso Remoto (Abierto)

Nuestra solución de formación remota o virtual, combina tecnologías de alta calidad y la experiencia de nuestros formadores, contenidos, ejercicios e interacción entre compañeros que estén atendiendo la formación, para garantizar una sesión formativa superior, independiente de la ubicación de los alumnos.

Dirigido a:

Administradores de sistemas, administradores de seguridad de TI, ingenieros de seguridad de TI y otros profesionales que se encarguen de diseñar, implementar, mantener y gestionar la seguridad de los sistemas Red Hat Enterprise Linux y de garantizar su adhesión a las políticas de seguridad de la empresa.

Objetivos:

- Gestionar el cumplimiento con OpenSCAP
- Habilitar SELinux en un servidor a partir de un estado deshabilitado, ejecutar un análisis básico de la política del sistema y mitigar los riesgos con técnicas avanzadas de SELinux
- Identificar y resolver problemas de manera proactiva con Red Hat Insights
- Supervisar la actividad y los cambios en un servidor con Linux Audit y AIDE
- Proteger los datos de posibles riesgos con USBGuard y el cifrado del almacenamiento
- Gestionar los controles de autenticación con PAM
- Aplicar manualmente los playbooks de Ansible proporcionados para automatizar la mitigación de los problemas de seguridad y cumplimiento
- Ampliar la gestión de OpenSCAP y Red Hat Insights con Red Hat Satellite y Red Hat Ansible Tower

Prerequisitos:

Tener la acreditación [Red Hat Certified Engineer \(RHCE®\)](#) o demostrar conocimientos y experiencia equivalentes en Red Hat Enterprise Linux

Exámenes y certificación

EX415 - Red Hat Certified Specialist in Security: Linux exam

Siguientes cursos recomendados:

- Red Hat Satellite 6 Administration (RH403) -
- Automation with Ansible I (DO407) and Automation with Ansible II: Ansible Tower (DO409) -

Contenido:

Gestión de la seguridad y los riesgos

- Defina las estrategias para gestionar la seguridad en los servidores de Red Hat Enterprise Linux.

Automatización de la configuración y las tareas de corrección con Ansible

- Corrija los problemas de configuración y seguridad con los playbooks de Ansible.

Protección de datos con LUKS y NBDE

- Cifre los datos en los dispositivos de almacenamiento con LUKS y utilice NBDE para gestionar el descifrado automático cuando se inician los servidores.

Restricción de acceso para dispositivos USB

- Utilice USBGuard para proteger el sistema del acceso de dispositivos USB fraudulentos.

Control de la autenticación con PAM

- Gestione la autenticación, la autorización, los ajustes de la sesión y los controles de contraseñas mediante la configuración de los módulos de autenticación conectables (PAM).

Registro de eventos del sistema con auditorías

- Registre e inspeccione los eventos del sistema relevantes para la seguridad con el subsistema de auditoría del kernel de Linux y las herramientas de soporte.

Supervisión de cambios en los sistemas de archivos

- Utilice AIDE para detectar y analizar los cambios en los sistemas de archivos de un servidor y su contenido.

Mitigación de riesgos con SELinux

- Mejore la seguridad y el confinamiento entre los procesos utilizando SELinux y las técnicas y los análisis avanzados de este sistema.

Gestión del cumplimiento con OpenSCAP

- Utilice OpenSCAP para evaluar la adhesión del servidor a las políticas de seguridad y aplicar las correcciones necesarias.

Automatización del cumplimiento con Red Hat Satellite

- Automatice y amplíe su capacidad para realizar verificaciones de OpenSCAP y solucionar los problemas de cumplimiento con Red Hat Satellite.

Análisis y resolución de problemas con Red Hat Insights

- Utilice Red Hat Insights para identificar, detectar y corregir puntos vulnerables en materia de seguridad y problemas comunes en los sistemas Red Hat Enterprise Linux.

Repaso completo

- Repase los contenidos del curso mediante ejercicios prácticos de revisión.

Más información:

Para más información o para reservar tu plaza llámanos al (34) 91 425 06 60

info.cursos@globalknowledge.es

www.globalknowledge.com/es-es/

Global Knowledge Network Spain, C/ Retama 7, 6ª planta, 28045 Madrid