Seguridad de Red Hat: Linux en físico, Virtual y en la Nube

Código: RH-415

Propuesta de Valor: REDHAT

Duración: 32 Horas

Red Hat Security: Linux in Physical, Virtual, and Cloud (RH415) está diseñado para administradores de seguridad y administradores de sistemas que necesitan administrar el funcionamiento seguro de servidores que ejecutan Red Hat® Enterprise Linux® , ya sea implementados en hardware físico, como máquinas virtuales, o como instancias en la nube.

Este curso 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.

Mantener la seguridad de los sistemas informáticos es un proceso de gestión de riesgos mediante la implementación de procesos y estándares respaldados por tecnologías y herramientas. En este curso, aprenderá acerca de los recursos que se pueden utilizar para ayudarlo a implementar y cumplir con sus requisitos de seguridad.

Más información: AQUÍ

Reserve su plaza: AQUÍ

AUDIENCIA

- Administradores de sistemas, administradores de seguridad de TI, ingenieros de seguridad de TI y otros profesionales responsables de diseñar, implementar, mantener y administrar la seguridad de los sistemas Red Hat Enterprise Linux y garantizar su cumplimiento con las políticas de seguridad de la organización.

PRE REQUISITOS

- Sea un ingeniero certificado por Red Hat (RHCE®) o demuestre el conocimiento y la experiencia equivalentes de Red Hat Enterprise Linux.

OBJETIVOS

Adquirir conocimientos en:

- Gestionar el cumplimiento de OpenSCAP.
- Habilitar SELinux en un servidor desde un estado deshabilitado.
- Identificar y resolver problemas de forma proactiva con Red Hat Insights.

Copyright © Cognos 2020 Todos los derechos reservados.

- Gestionar los controles de autenticación con PAM.
- Aplicar manualmente los Playbooks de Ansible.
- Escale la gestión de OpenSCAP y Red Hat Insights con Red Hat Satellite y Red Hat Ansible Tower.

CERTIFICACIÓN DISPONIBLE

- Certificado de participación.
- Este curso lo prepara para el examen: **RED HAT CERTIFIED SPECIALIST IN SECURITY: LINUX**

CONTENIDO

1. GESTIONAR LA SEGURIDAD Y EL RIESGO

1.1. DEFINIR ESTRATEGIAS PARA ADMINISTRAR LA SEGURIDAD EN SERVIDORES RED HAT ENTERPRISE LINUX

2. AUTOMATIZAR LA CONFIGURACIÓN Y LA CORRECCIÓN CON ANSIBLE

2.1. SOLUCIONAR LOS PROBLEMAS DE CONFIGURACIÓN Y SEGURIDAD CON ANSIBLE PLAYBOOKS

3. PROTEJER LOS DATOS CON LUKS Y NBDE

3.1. CIFRAR LOS DATOS DE LOS DISPOSITIVOS DE ALMACENAMIENTO CON LUKS Y UTILICE NBDE PARA GESTIONAR EL DESCIFRADO AUTOMÁTICO CUANDO SE INICIAN LOS SERVIDORES

4. RESTRINGIR EL ACCESO A DISPOSITIVOS USB

4.1. PROTEJER EL SISTEMA DEL ACCESO ILEGAL A DISPOSITIVOS USB CON USBGUARD

5. CONTROLAR LA AUTENTICACIÓN CON PAM

5.1. ADMINISTRAR LA AUTENTICACIÓN, AUTORIZACIÓN, CONFIGURACIÓN DE SESIÓN Y CONTROLES DE CONTRASEÑA MEDIANTE LA CONFIGURACIÓN DE MÓDULOS DE AUTENTICACIÓN CONECTABLES (PAM)

6. REGISTRAR LOS EVENTOS DEL SISTEMA CON AUDITORÍA

6.1. REGISTRAR E INSPECCIONAR LOS EVENTOS DEL SISTEMA RELEVANTES PARA LA SEGURIDAD, UTILIZANDO EL SUBSISTEMA DE AUDITORÍA DEL KERNEL DE LINUX Y LAS HERRAMIENTAS DE SOPORTE

7. SUPERVISAR CAMBIOS EN EL SISTEMA DE ARCHIVOS

7.1. DETECTAR Y ANALIZAR CAMBIOS EN LOS SISTEMAS DE ARCHIVOS DE UN SERVIDOR Y SU CONTENIDO USANDO AIDE

8. MITIGAR EL RIESGO CON SELINUX

8.1. MEJORAR LA SEGURIDAD Y EL CONFINAMIENTO ENTRE PROCESOS MEDIANTE EL USO DE SELINUX Y TÉCNICAS Y ANÁLISIS AVANZADOS DE SELINUX

Copyright © Cognos 2020 Todos los derechos reservados.

9. GESTIONAR EL CUMPLIMIENTO DE OPENSCAP

9.1. EVALUAR Y REPARAR EL CUMPLIMIENTO DE LAS POLÍTICAS DE SEGURIDAD DE UN SERVIDOR MEDIANTE OPENSCAP

10. AUTOMATIZAR EL CUMPLIMIENTO CON RED HAT SATELLITE

10.1. AUTOMATIZAR Y ESCALAR SU CAPACIDAD PARA REALIZAR COMPROBACIONES DE OPENSCAP Y SOLUCIONAR PROBLEMAS DE CUMPLIMIENTO CON RED HAT SATELLITE

11. ANALIZAR Y SOLUCIONAR PROBLEMAS CON RED HAT INSIGHTS

11.1. IDENTIFICAR, DETECTAR Y CORRIJIR PROBLEMAS COMUNES Y VULNERABILIDADES DE SEGURIDAD CON LOS SISTEMAS RED HAT ENTERPRISE LINUX MEDIANTE RED HAT INSIGHTS

12. REALIZAR UNA REVISIÓN INTEGRAL

12.1. REVIZAR EL CONTENIDO CUBIERTO EN ESTE CURSO COMPLETANDO EJERCICIOS PRÁCTICOS DE REVISIÓN

BENEFICIOS

Al finalizar el curso, debería poder demostrar estas habilidades:

- Analice y repare el cumplimiento del sistema mediante OpenSCAP y SCAP Workbench.

Copyright © Cognos 2020 Todos los derechos reservados.