Seguridad de Red Hat: Protección de Contenedores y OpenShift con Examen

Código: DO-426

Propuesta de Valor: REDHAT

Duración: 32 Horas

Aprenda a mitigar y gestionar las amenazas a la infraestructura basada en contenedores de OpenShift.
Red Hat Security: Asegurar contenedores y OpenShift con examen (DO426) ayuda a los administradores de infraestructura y a los profesionales de seguridad a aprender y validar cómo identificar y mitigar las amenazas a la infraestructura basada en contenedores de OpenShift. El plan de estudios también cubre cómo implementar y administrar arquitectura, políticas y procedimientos seguros para aplicaciones modernas en contenedores y redes definidas por software.

Más información: AQUÍ

Reserve su plaza: AQUÍ

AUDIENCIA

- Este curso está diseñado para profesionales responsables del diseño, implementación, mantenimiento y administración de la seguridad de aplicaciones en contenedores en sistemas Red Hat Enterprise Linux y en instalaciones de Red Hat OpenShift Container Platform

PRE REQUISITOS

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

OBJETIVOS

- Aprenda las tecnologías de privilegio mínimo y aislamiento multiusuario de Linux.
- Automatice las implementaciones basadas en políticas.

CERTIFICACIÓN DISPONIBLE

CONTENIDO

1. DESCRIBIR LAS TECNOLOGÍAS DE SEGURIDAD DEL HOST

1.1. COMPRENDA LAS TECNOLOGÍAS CENTRALES QUE HACEN DE RED HAT ENTERPRISE LINUX UN HOST DE CONTENEDOR SÓLIDO Y CONFIABLE

2. ESTABLECER IMÁGENES DE CONTENEDORES CONFIABLES

2.1. DESCRIBA LOS REGISTROS, SERVICIOS Y MÉTODOS QUE COMPONEN EL ECOSISTEMA DE IMÁGENES DE RED HAT

3. IMPLEMENTAR SEGURIDAD EN EL PROCESO DE CONSTRUCCIÓN

3.1. APRENDA MÉTODOS AUTOMATIZADOS PARA INTEGRAR CONTROLES DE SEGURIDAD EN LAS CANALIZACIONES DE CONSTRUCCIÓN E IMPLEMENTACIÓN

4. GESTIONAR EL CONTROL DE ACCESO DE LOS USUARIOS

4.1. APLICAR MÉTODOS DE INTEGRACIÓN Y GESTIÓN DE LA AUTENTICACIÓN DE USUARIOS PARA OPERADORES Y APLICACIONES WEB

5. CONTROLAR EL ENTORNO DE IMPLEMENTACIÓN

5.1. DETERMINE CÓMO UNA PLATAFORMA DE CONTENEDORES ASEGURA EL PROCESO DE IMPLEMENTACIÓN A TRAVÉS DE POLÍTICAS Y AUTOMATIZACIÓN

6. GESTIONAR LA ORQUESTACIÓN DE LA PLATAFORMA SEGURA

6.1. ESTUDIE CÓMO UNA PLATAFORMA DE CONTENEDORES ASEGURA EL PROCESO DE ORQUESTACIÓN A TRAVÉS DE POLÍTICAS E INFRAESTRUCTURA

7. PROPORCIONE E / S DE RED SEGURA

7.1. DESCUBRA LAS TECNOLOGÍAS Y LAS FUNCIONES DE CONTROL QUE PERMITEN LA TENENCIA MÚLTIPLE Y EL AISLAMIENTO DE PROYECTOS

8. OFREZCA E / S DE ALMACENAMIENTO SEGURO

8.1. HABILITE EL ACCESO AL ALMACENAMIENTO DE MÚLTIPLES INQUILINOS AUTORIZADO A TRAVÉS DE UNA SÓLIDA COMPRENSIÓN DE LAS TECNOLOGÍAS RELACIONADAS Y LAS FUNCIONES DE CONTROL

BENEFICIOS

Hat Enterprise Linux para gestionar los riesgos de seguridad y ayudar a cumplir con los requisitos de cumplimiento.