Red Hat Security: Securing Containers and OpenShift – Online

Calle de la Basílica, 19
28020 Madrid
(34) 915 53 61 62
www.cas-training.com

WE ARE CAS

Objetivos:

Después de realizar este curso, podrá utilizar las tecnologías de seguridad que se incluyen en Red Hat OpenShift Container Platform y Red Hat Enterprise Linux para gestionar los riesgos de seguridad y satisfacer los requisitos de cumplimiento. Podrá demostrar las siguientes habilidades:

- Utilizar prácticas recomendadas para garantizar que las imágenes para la implementación en contenedores provengan de fuentes confiables, lo cual incluye el uso de registros seguros, imágenes firmadas, protocolos de acceso seguros y controles de acceso autorizado.
- Explicar e implementar técnicas avanzadas de SELinux para restringir el acceso de usuarios, procesos y máquinas virtuales.
- Configurar las restricciones de seguridad para controlar las acciones que pueden realizar los pods y establecer a qué pueden acceder.
- Implementar la seguridad informática (seccomp) de Linux y las capacidades de Linux de controlar el tamaño de la vulnerabilidad de una aplicación en contenedores.
- Implementar y configurar el inicio de sesión único para aplicaciones web, lo cual incluye el uso de JWT para compartir un token.
- Explicar e implementar técnicas de cifrado y aislamiento de red para separar el tráfico de las aplicaciones, y así permitir el acceso autorizado únicamente.
- Implementar y explicar técnicas de gestión de almacenamiento para separar la E/S de almacenamiento de volumen para permitir el acceso autorizado únicamente.
- Observar y explicar cómo se puede extender el proceso de diseño para incluir el escaneo de las vulnerabilidades y las pruebas de seguridad automatizados, a fin de garantizar que no se presenten vulnerabilidades en las imágenes de contenedor definitivas que van a implementarse.
- Gestionar la configuración y las políticas de implementación de los contenedores para controlar la ubicación de las aplicaciones, la capacidad de los recursos, la afinidad de los contenedores y la escalabilidad de la demanda de aplicaciones.
- Gestionar las cuotas y el acceso al proyecto de Openshift para garantizar el acceso de autoservicio privado y autorizado, y limitar la exposición a los tokens maliciosos, así como los intentos de denegación de servicio.

Requisitos:

No es necesario cumplir con requisitos previos para acceder a este curso

Perfil del docente:

- Formador Certificado por Red Hat
- Más de 5 años de experiencia profesional
- Más de 4 años de experiencia docente
- Profesional activo en empresas del sector IT

Metodología:

- "Learning by doing" se centra en un contexto real y concreto, buscando un aprendizaje en equipo para la resolución de problemas en el sector empresarial.
- Aulas con grupos reducidos para que el profesional adquiera la mejor atención por parte de nuestros instructores profesionales.
- El programa de estudios como partners oficiales es confeccionado por nuestro equipo de formación y revisado por las marcas de referencia en el sector.
- La impartición de las clases podrá ser realizada tanto en modalidad Presencial como Virtual.

Contenidos:

- **Descripción de las tecnologías de seguridad de host**
  - Comprender las tecnologías esenciales que convierten a Red Hat Enterprise Linux en un host de contenedores sólido y de confianza.
- **Establecer imágenes de contenedores de confianzae**
  - Describir los registros, los servicios y los métodos que componen el ecosistema de imágenes de Red Hat
- **Implementar la seguridad en el proceso de diseño**
  - Aprender sobre los métodos automatizados para integrar las comprobaciones de seguridad en los canales de diseño e implementación.
- **Controlar el entorno de implementación**
  - Determinar la manera en que las políticas y la automatización de una plataforma de contenedores protegen el proceso de implementación.
- **Gestionar la organización de una plataforma segura**
  - Gestione el control de tareas, los gestores y los errores de tareas en los playbooks de Ansible.
- **Implementación de archivos en hosts gestionados**
  - Estudiar cómo una plataforma de contenedores protege el proceso de organización con políticas e infraestructura.
- **Proporcionar una E/S de red segura.**
  - Descubrir las tecnologías y las características de control que permiten la arquitectura multiempresa y el aislamiento del proyecto.
- **Suministrar una E/S de almacenamiento segura**
  - Permitir el acceso autorizado al almacenamiento multiempresa gracias a una comprensión firme de las tecnologías y las características de control relacionadas.

CAS TRAINING

UN ESPACIO PARA CRECER

cas-training.com