Red Hat Security: Containers and OpenShift (DO425VT)

Modality: Virtual Classroom

Duration: 5 Days

About this course:

Learn to mitigate and manage threats to OpenShift container-based infrastructure

Red Hat Security: Securing Containers and OpenShift (DO425) is designed to help infrastructure administrators and security professionals learn to identity and mitigate threats to OpenShift container-based infrastructure. The curriculum also covers how to implement and manage secure architecture, policies, and procedures for modern containerized applications and software-defined networking.

This course is based on Red Hat®Enterprise Linux® 7.5, Red Hat® OpenShift® Container Platform 3.11, and Red Hat® Identity Manager 7.5.

You will learn about using secure and trusted container images, registries, and source code; managing network and storage isolation; implementing application single sign-on; and configuring appropriate security constraints and service role–based access control. You will also find out how existing core Linux technologies—such as namespaces, cgroups, seccomp, capabilities, and SELinux—provide a robust and mature host environment with strongly secure containers.

Course Objective:

- Learn Linux multitenancy isolation and least-privilege technologies.
- Investigate trusted repositories, as well as signing and scanning images.
- Implement security in a continuous integration and continuous development (CI/CD) pipeline.
- Integrate web application single sign-on.
- Automate policy-based deployments.
- Configure security context constraints (SCC).
- Manage API access control.
- Provide secure network I/O.
- Deliver secure storage I/O.

Audience:

This course is designed for professionals responsible for designing, implementing, maintaining, and managing the security of containerized applications on Red Hat Enterprise Linux systems and in Red Hat OpenShift Container Platform installations, including these roles:

- System administrators
- IT security administrators
- IT security engineers
- DevOps engineers
- Cloud developers

- Cloud architects

Prerequisite:

- Become a Red Hat Certified Engineer (RHCE®), or demonstrate equivalent Red Hat Enterprise Linux knowledge and experience
- Become a Red Hat Certified Specialist in OpenShift Administration, or demonstrate equivalent Red Hat OpenShift Container Platform knowledge and experience

Course Outline:

Describe host security technologies

Understand the core technologies that make Red Hat Enterprise Linux a robust and trusted container host.

Establish trusted container images

Describe the registries, services, and methods that comprise the Red Hat image ecosystem.

Implement security in the build process

Learn automated methods for integrating security checks into build and deployment pipelines.

Manage user access control

Apply methods for integrating and managing user authentication for operators and for web applications.

Control the deployment environment

Determine how a container platform secures the deployment process through policies and automation.

Manage secure platform orchestration

Study how a container platform secures the orchestration process through policies and infrastructure.

Provide secure network I/O

Discover the technologies and control features that enable multitenancy and project isolation.

Deliver secure storage I/O

Enable authorized, multitenant storage access through a firm understanding of related technologies and control features.