Red Hat Security: Securing Containers and OpenShift («DO425»)

This course is designed to help infrastructure administrators and security professionals identify and reduce threats to the container-based OpenShift infrastructure.

Duration: 4 days
Price: 3'400.–

Content

The curriculum also covers how to implement and manage secure architecture, policies, and procedures for modern containerized applications and software-defined networking.

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.

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.

Note: Course outline is subject to change with technology advances and as the nature of the underlying job evolves.

Key Learnings

- Learning Linux multitenancy isolation and least-privilege technologies
- Investigating trusted repositories, as well as signing and scanning images
- Implementing security in a continuous integration and continuous development (CI/CD) pipeline
- Integrating web application single sign-on
- Automating policy-based deployments
- Configuring security context constraints (SCC)
- Managing API access control
- Providing secure network I/O
- Delivering secure storage I/O

Methodology & didactics

Containers and container orchestration platforms, such as OpenShift and Kubernetes, have become pervasive in enterprise computing. Container environments have introduced new attack vectors, exploits, and vulnerabilities. Enterprises require strong security, and the migration to containerized microservices has upended traditional network-based security models. Developers must prove that their code, images, and deployments are trusted and secure.

This course is intended to develop the skills needed to maintain a high level of security in the evolving world of containerized applications and OpenShift installations. OpenShift is an enterprise-grade, container-based application platform that provides the mature security of Red Hat Enterprise Linux and additional mechanisms of security assurance for service role access control, build process hardening, source image layered trust, and controlled deployment management. These security features may help your organization efficiently reduce risk of security breaches, which have a high cost in business disruption, brand erosion, loss of customer and shareholder trust, and financial costs for post-incident remediation. In addition, your organization may be able to use the tools in this course to help demonstrate that compliance requirements set by customers, auditors, or other stakeholders have been met.

Target 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

Any questions?

We are happy to advise you on +41 44 447 21 21 or info@digicomp.ch. You can find detailed information about dates on www.digicomp.ch/courses-it-provider/red-hat/red-hat-open-shift/course-red-hat-security-securing-containers-and-openshift