Maslak Mahallesi, Maslak Meydan Sk. No:5. Spring Giz Plaza. Maslak/İstanbul
+90 212 282 7700 - info@bilginc.com

Red Hat Security: Securing Containers and OpenShift

Learn via: **Classroom**

Duration: **4 Days**

Overview

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 content summary

- 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

Prerequisites

- 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

What You Will Learn

Impact on the organisation

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.

Red Hat has created this course in a way intended to benefit our customers, but each company and infrastructure is unique, and actual results or benefits may vary.

Impact on the individual

As a result of attending this course, you should be able to use security technologies included in Red Hat OpenShift Container Platform and Red Hat Enterprise Linux to manage security risk and help meet compliance requirements. You should be able to demonstrate these skills:

- Use recommend practices to ensure that images for container deployment come from trusted sources, including the use of secure registries, signed images, secure access protocols, and authorized access controls.
- Explain and implement advanced SELinux techniques to restrict access by users, processes, and virtual machines.
- Configure security context constraints to control the actions that pods can perform and to declare what a pod has the ability to access.
- Implement the Linux computer security (seccomp) and Linux capabilities features to control the vulnerability footprint of a containerized application.
- Implement and configure single sign-on for web applications, including the use of JWT for token sharing.
- Explain and implement network isolation and encryption techniques to segregate application traffic to allow only authorized access.
- Implement and explain storage management techniques to segregate volume storage I/O to allow only authorized access.
- Observe and explain how the build process can be extended to include automated security testing and vulnerability scanning to ensure that no exploits are introduced into the final container images to be deployed.
- Manage container deployment policies and configuration to control application placement, resource capacity, container affinity, and application demand scaling.
- Manage OpenShift project access and quotas to ensure private and authorized self-service access, as well as to limit exposure to rogue tokens and denial-of-service attempts.

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.