CON101 - DEFENDING CONTAINERS

Course Learning Objectives

This course is designed for those interested in the best practices for defending their container implementation. By the end of this course, you'll discover the basics of what containers are and what their ecosystem is composed of, how to harden containers and secure access and key management, and, finally, manage container orchestration, network security, and logging and monitoring.

Description

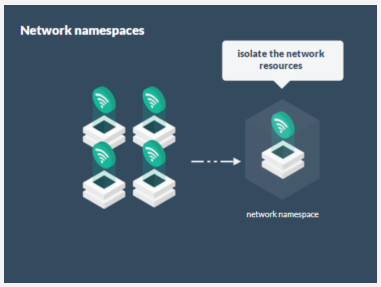
Defending Containers helps DevOps engineers understand and implement strategies to secure containers. This course covers fundamental concepts of containerization, what's required for hardening your build environment, operating system, and container engine, and how to ensure security while running multiple containers at scale by restricting network activity and using logging and monitoring.

Audience

DevOps Engineers

Time Required

Tailored learning - 45 minutes total (approx.)



CON101 - DEFENDING CONTAINERS

Course Outline

1. Introduction to Containers and Microservices

- About
- Containers vs virtualization
- Containerized applications
- Containerized applications exploits
- Container ecosystem
- Containerization and DevOps
- Container security overview
- Container security considerations

2. Hardening the Host OS and Container Engine

- Hardening the build environment
- The build environment
- Secure source code management
- Secure build and delivery tools
- Hardening the host environment
- Hardening the container engine
- Resource usage analysis
- Avoid long-running containers
- Hardening container images
- Secure container registry
- Scanning container content
- Removing extra content
- Immutable images
- Access management
- Secure key management

3. Orchestration, Networking, and Monitoring

- Major security risks
- Orchestration
- Access control
- Network security
- Network namespaces
- Network segmentation
- Logging and monitoring
- Threat detection and incident response

SecurityCompass