DOC201 - DEFENDING DOCKER

Course Learning Objectives

This course is part of the line of defending against threats to the cloud. Defending Docker builds on the foundations of cloud security but in the context of the Docker platform. Defending Docker is comprised of five modules that cover implementing best practices for kernel security, securing the Docker daemon, managing unverified Docker images, securing network communication and traffic, and configuring authentication and authorization in the Docker Trusted Registry (DTR) and Docker Universal Control Plane (UCP).

Description

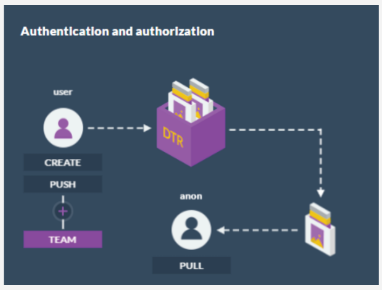
Defending Docker was created for DevOps and Ops Engineers who have experience using Docker and familiarity with application security. This course focuses on configuring the Docker platform to defend against the most common security threats.

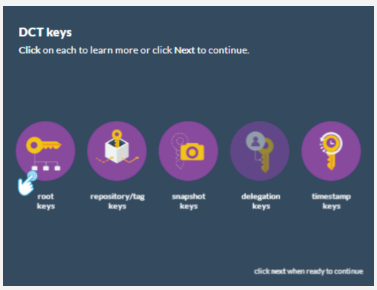
Audience

DevOps
Ops Engineers

Time Required

Tailored learning - 40 minutes total (approx.)





DOC201 - DEFENDING DOCKER

Course Outline

1. Kernel Security

- Introduction
- Resource isolation
- Kernel namespaces
- Cgroups
- Kernel and host threats
- Best practices
- Isolate containers
- Restrict kernel capabilities
- AppArmor
- Seccomp

2. Daemon Security

- Introduction
- Attack vectors
- Rootless mode
- Rootless mode and userns-remap
- Secure the socket

3. Unverified Docker Images

- Unverified Docker images
- Docker Content Trust
- Image tags and DCT
- DCT keys
- Implement client enforcement
- Sign images with Docker
- Manage keys for content trust
- Back up keys
- Lost keys

4. Communication and Network Traffic

- Secure communication among containers
- Protect the Docker daemon socket
- Create a CA, server, and client keys
- Verify the repository client
- Configure TLS in DTR
- External certificates in UCP
- MTLS
- Initiate a new CA and keys

5. Authentication and Authorization in DTR and UCP

- UCP overview
- Authentication with UPC - RBAC
- LDAP/AD with UCP
- DTR overview
- Authentication and authorization
- Permission levels in DTR

SecurityCompass