Rumos valorizamos profissionais!

Workshop Docker Security

- **Formato do curso:** Live training
- **Preço:** 1265€
- **Duração:** 21 horas

The Docker Security course offers a hands-on overview and theory of important security features and best practices to protect containerized services and hosts. You will learn how to effectively use Docker to build secure and performant container images, how Linux containers are constructed and secured, including cgroups, namespaces, apparmor, seccomp filtering and many more. Also, you will learn about container clustering and orchestration with Docker Swarm.
All these features will be explained and demonstrated with hands on examples in the practice lab.

Esta formação é ministrada em Inglês.

Em parceria com a entidade acreditada:

DevOps Artisan

Destinatários

- Developer
- Operations
- DevOps
- Architects

Pré-requisitos

- Strong grasp of Docker (recommended training: Docker Fundamentals and Docker Advanced).

Nice to have:

- Required skills include running Unix commands, navigating the file system, and creating and editing text

files.

Programa

Docker Recap

- Age of Virtualization
- Why Containers?
- Docker History
- Containerization
- OS Components (Namespaces, Control Groups)
- Docker Engine
- Containers and VMs
- Docker Versions
- Docker Update Channels
- Installing Docker on Linux with steps
- Docker Images
- Image Contents
- Image Layers
- Multiple architectures support
- Image registry
- Image security
- Repositories
- Docker Commands
- Running and stopping containers
- Network types
- Working with networks
- Testing the network
- Persistent Storage in Docker
- Creating and mounting a volume
- Listing, inspecting and deleting volumes
- Logging Docker
- Explaining different log types

Secure Docker Connectivity

- Docker hub image vulnerabilities
- Possible attack vectors
- How does Docker handle security?
- Different layers of security
- Secure Docker connectivity overview
- TLS explained
- What is a Certificate Authority?
- Configuring secure Docker connectivity with steps

Hands-on Lab: Secure Docker Connectivity

Secure Docker Registry

- What is Docker Registry?
- Securing a Docker registry
- Authorization Options
- Basic authentication configuration
- Token-based authentication configuration

Hands-on Lab: Deploying a Secure Docker Registry

Role-Based Access Control

- Using authorization and roles
- Docker’s Plugin API for RBA
- Enabling the authorization plugin
- Open Policy Agent (OPA) Configuration

Hands-on Lab: Implementing RBAC using AuthN and AuthZ in Docker

Docker Swarm

- What is Docker Swarm?
- Docker Swarm components explained
- Docker CLI Cluster commands
- Docker Swarm Security
- Bootstrapping a Warm Cluster
- Secrets in a Swarm Cluster with Secret rotation
- Autolock in Warm Clusters
- Backing up and recovering a Swarm Cluster

Hands-on Lab: Docker Swarm Installation and Secure Docker Swarm cluster

Networking

- Network types
- Working with networks
- Testing the network

Hands-on Lab: Docker Networking

Managing Secrets

- What are secrets
- How to manage Docker Secrets

Hands-on Lab: Managing Secrets

Content Trust

- Docker Content Trust
- Image Tags signed or not signed
- Docker Content Trust Key
- Signing Images with DCT
- What is Notary

Hands-on Lab: Docker Content Trust

Linux capabilities

- What are Linux Capabilities?
- Dropping capabilities
- Using pscap tool
- Whitelisting
- Listing capabilities

Hands-on Lab: Linux Kernel Capabilities

Controlling Access to Resources with Control Groups

- Control Group
- Control Group Subsystems, hierarchy
- Managing cgroup for Containers
- Cgroup Parent Context
- Docker Cgroup Resource Limits

Hands-on Lab: Docker and Cgroups

AppArmor

- Linux Security Models
- AppArmor explained
- Developing an AppArmor Profile
- Docker and AppArmor Profiles
- Debugging AppArmor

Hands-on Lab: AppArmor and Docker

Seccomp

- How does Docker use Seccomp?
- Creating a custom Seccomp profile
- Using custom profiles for all containers
- Using the Whitelist

Hands-on Lab: Seccomp

SELinux

- SELinux explained
- SELinux Policy, labeling and type enforcement
- Enable SELinux in Docker
- Changing SELinux behavior per Container

Hands-on Lab: SELinux

DDos

- Security approach of DoS Attacks

Hands-on Lab: Docker DDoS attacks performance

Tools for security

- Docker bench
    - What is Docker Bench
    - Docker Bench Options
- InSpec
    - What is InSpec
    - InSpec Install
    - Running Chef InSpec
    - InSpec Profile Structure
    - InSpec Community Profiles
- Anchore
    - How does Anchore work
    - Ancore Engine
    - Installing Anchore Engine
    - Using Anchore
- Jenkins pipelines
    - Continuous integration flow
    - Continuous delivery flow
    - Continuous deployment flow
    - What is Jenkins?
    - What is a pipeline?
    - Securing Jenkins CI/CD Pipeline with Anchore
- Dagda
    - What is Dagda?
    - Installing and running Dagda
    - Dagda database
    - Analyzing docker images/containers
    - Monitoring running containers
    - Getting Docker daemon events
- Sysdig Falco
    - What is Sisdig?
    - What is Falco?

    - Falco rules
    - Installing Falco
    - Running Falco as a daemon

Hands-on Lab:

- Docker Bench
- InSpec
- Anchore
- Create a Jenkins pipeline for docker image security scanning with anchore
- Dagda
- Sysdig Falco

Best Practices

- Secure the build pipeline
- Secure the Network
- Secure the Host
- Secure the Container Runtime
- Secure the Orchestrator Config
- Secure the Data