## KL 044.1.1:

# Kaspersky Container Security

## **Featured products**

Kaspersky Container Security

## **Course description**

The course covers containerization technologies, container infrastructures and secure development. It also introduces container orchestration and related security challenges. Potential attack vectors against container infrastructures are described, as well as best practices for their protection and risk mitigation. The course also explains how Kaspersky Container Security can protect container infrastructures taking into account these challenges and best practices.

The theoretical part of the course and hands-on labs provide participants with the knowledge and skills needed to:

- Protect container infrastructures using Kaspersky Container Security agents
- Scan containers for vulnerabilities, malicious code, configuration errors and confidential data
- Integrate the security solution into the CI/CD pipeline

#### What's new in course version 1.1

- Revised course structure to better reflect changes in the solution architecture
- Added information about new product functions:
  - a) Runtime profiles to protect running containers
  - b) Integration with image signature verification systems
  - c) Configuration of the scope
- The following tasks have been added to the labs:
  - a) Product installation
  - b) Scope configuration
  - c) Runtime profile configuration

#### Duration

1 day

## **Requirements for participants**

Basic Linux administration skills. Basic knowledge of information security principles. Basic knowledge of containerization technologies is desirable.

The course is intended for container infrastructure operations engineers, security specialists and administrators, technical support and pre-sales engineers.

## Contents

#### 1. Introduction to container security

- 1.1. CI/CD and microservices
- 1.2. Containers
- 1.3. Kubernetes
- 1.4. DevSecOps
- 1.5. Security in Kubernetes

#### 2. Architecture and deployment

- 2.1. Solution architecture
- 2.2. Pre-deployment
- 2.3. Scaling

#### 3. Operation and maintenance

- 3.1. Users, roles and scopes
- 3.2. Integrations
- 3.3. Deploying agents
- 3.4. Security policies
- 3.5. Event log and reports

#### 4. Integration with CI/CD

- 4.1. Scanner
- 4.2. CI/CD pipeline stop