KL 044.2:

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 2.0

- Added information about new product functions:
    a) File operation monitoring
    b) Incident investigation
    c) Autoprofiling
    d) Kubernetes cluster compliance with industry standards
    e) Integration with SIEM
    f) Integration with Git and Vault
    g) Maintenance and troubleshooting
- The following tasks have been added to the labs:
    a) File operation monitoring
    b) Compliance with industry standards
    c) Autoprofiling
    d) Working with the API
- The first chapter, which covers the basics of Kubernetes security, is now optional and intended for self-study. We recommend that instructors start the training course from chapter two.

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