**KBS-302: Kubernetes and Container-based Application Security with CKS exam.prep.**

**Course Length:** 2 days

**Course Description:**

This 2-days long training introduces concepts, procedures, and best practices to harden Kubernetes based systems and container-based applications against security threats. It deals with the main areas of cloud-native security: Kubernetes cluster setup, Kubernetes cluster hardening, hardening the underlying operating system and networks, minimizing microservices vulnerabilities, supply chain security as well as monitoring, logging, and runtime security.

This course does not only prepare delegates for the daily security administration of Kubernetes- based systems but also for the official Certified Kubernetes Security Specialist (CKS) exams of the Cloud Native Computing Foundation (CNCF).

**Structure:** 50% theory 50% hands on lab exercises

**Target audience:** Kubernetes administrators who participated on one of our Kubernetes administration trainings or have a Certified Kubernetes Administrator (CKA) certification and want to learn about securing Kubernetes based systems and container-based applications.

**Prerequisites:** Linux container (e.g. Docker) and Kubernetes admin. skills, for instance by participating on our Docker and Kubernetes administration courses.

**Detailed Course Outline**

**Module 1: User and authorization management**

- Users and service accounts in Kubernetes
- Authenticating users
- Managing authorizations with RBAC

**Module 2: Supply chain security**

- Vulnerability checking for images
- Image validation in Kubernetes
- Reducing image footprint
- Secure image registries

**Module 3: Validating cluster setup and penetration testing**

- Use CIS benchmark to review the security configuration of Kubernetes components
- Modify the cluster components' configuration to match the CIS Benchmark
- Penetration testing Kubernetes for known vulnerabilities

**Module 4: System hardening**

- Use kernel hardening tools
- Setup appropriate OS level security domains
- Container runtime sandboxes
- Limit network access

**Module 5: Monitoring and logging**

- Configure Kubernetes audit logs
- Configure Audit Policies
- Monitor applications behaviour with Falco