ComponentSoft
open cloud trainings and consultation

CNS-413: Practical cloud native security

Course Length: 3 days

Course Description:

This 3-days long training focuses on providing hands-on knowledge in Cloud Native security. It 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, obtaining supply chain security as well as monitoring, logging, and runtime security.

This course does not only deal with the daily security administration of Kubernetes-based systems but also prepares delegates for the official Certified Kubernetes Security Specialist (CKS) exam of the Cloud Native Computing Foundation (CNCF) and aligns with the requirements of the GSMA NESAS Security Requirements for Vendor Development and Product Lifecycle Processes.

Structure: 50% theory 50% hands on lab exercises

Target audience: System administrators, developers and Devops who want to understand the concepts and tools of cloud-native security and want to implement it in practice.

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

Main Topics:

- Core cloud native security concepts:
    - OpenShift SCC vs PSS
    - RBAC
    - Network Policies
    - namespaces/quotas
    - secrets
    - audit
- Security for developers:
    - Container hardening:
        - Openshift UBI / minimal images
        - non-root
        - Capabilities
        - SecComp
        - Security Profiles Operator
    - Policy aware admission
        - integrating tests into a CI/CD pipeline: SBOM/scan/sign/verify
- Security for infrastructure maintainers:
    - Cluster hardening:
        - FIPS
        - Machine Config Operator
        - Node immutability.
        - Compliance Operator
        - File Integrity Operator.
    - Multi tenancy
        - Logging/audit to SIEM
        - Falco / eBPF runtime sensors
    - Air-gapped environments:
        - oc mirror
        - ImageContentSourcePolicy/image provenance enforcement.
        - Harbor
- Security for testers:
    - Security test automation
        - integrating Conftest/Kyverno into CI
        - API fuzz testing
    - Performance + security:
        - validate CP/UP segmentation and latency under policies.
- Securing application delivery:
    - Onboarding playbooks
    - Evidence packs for audits