Certified Kubernetes Security Specialist (CKS) Exam Curriculum

A Cloud Native Computing Foundation (CNCF) Publication

cncf.io

kubernetes

CLOUD NATIVE
COMPUTING FOUNDATION

This document provides the curriculum outline of the Knowledge, Skills and Abilities that a Certified Kubernetes Security Specialist (CKS) can be expected to demonstrate.

CKS Curriculum

15% - Cluster Setup

- Use Network security policies to restrict cluster level access
- Use CIS benchmark to review the security configuration of Kubernetes components (etcd, kubelet, kubedns, kubeapi)
- Properly set up Ingress objects with TLS
- Protect node metadata and endpoints
- Verify platform binaries before deploying

15% - Cluster Hardening

- Use Role Based Access Controls to minimize exposure
- Exercise caution in using service accounts e.g. disable defaults, minimize permissions on newly created ones
- Restrict access to Kubernetes API
- Upgrade Kubernetes to avoid vulnerabilities

10% - System Hardening

- Minimize host OS footprint (reduce attack surface)
- Using least-privilege identity and access management
- Minimize external access to the network
- Appropriately use kernel hardening tools such as AppArmor, seccomp

This document provides the curriculum outline of the Knowledge, Skills and Abilities that a Certified Kubernetes Security Specialist (CKS) can be expected to demonstrate.

CKS Curriculum

20% - Minimize Microservice Vulnerabilities

- Use appropriate pod security standards
- Manage kubernetes secrets
- Understand and implement isolation techniques (multi-tenancy, sandboxed containers, etc.)
- Implement Pod-to-Pod encryption using Cilium

20% - Supply Chain Security

- Minimize base image footprint
- Understand your supply chain (e.g. SBOM, CI/CD, artifact repositories)
- Secure your supply chain (permitted registries, sign and validate artifacts, etc.)
- Perform static analysis of user workloads and container images (e.g. Kubesec, KubeLinter)

20% - Monitoring, Logging and Runtime Security

- Perform behavioral analytics to detect malicious activities
- Detect threats within physical infrastructure, apps, networks, data, users and workloads
- Investigate and identify phases of attack and bad actors within the environment
- Ensure immutability of containers at runtime
- Use Kubernetes audit logs to monitor access

kubernetes

CLOUD NATIVE
COMPUTING FOUNDATION

Cloud native computing uses an open source software stack to deploy applications as microservices, packaging each part into its own container, and dynamically orchestrating those containers to optimize resource utilization. The Cloud Native Computing Foundation (CNCF) hosts critical components of those software stacks including Kubernetes, Fluentd, Linkerd, Prometheus, OpenTracing and gRPC; brings together the industry's top developers, end users, and vendors; and serves as a neutral home for collaboration. CNCF is part of The Linux Foundation, a nonprofit organization. For more information about CNCF, please visit: https://cncf.io/.