# 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

## 10% - 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 security control
- Protect node metadata and endpoints
- Minimize use of, and access to, GUI elements
- Verify platform binaries before deploying

## 15% - Cluster Hardening

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

## 15% - System Hardening

- Minimize host OS footprint (reduce attack surface)
- Minimize IAM roles
- 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

- Setup appropriate OS level security domains
- Manage kubernetes secrets
- Use container runtime sandboxes in multi-tenant environments (e.g. gvisor, kata containers)
- Implement pod to pod encryption by use of mTLS

## 20% - Supply Chain Security

- Minimize base image footprint
- Secure your supply chain: whitelist allowed image registries, sign and validate images
- Use static analysis of user workloads (e.g. kubernetes resources, docker files)
- Scan images for known vulnerabilities

## 20% - Monitoring, Logging and Runtime Security

- Perform behavioral analytics of syscall process and file activities at the host and container level to detect malicious activities
- Detect threats within physical infrastructure, apps, networks, data, users and workloads
- Detect all phases of attack regardless where it occurs and how it spreads
- Perform deep analytical investigation and identification of bad actors within environment
- Ensure immutability of containers at runtime
- Use 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/.