Certified Kubernetes Security Specialist(CKS)

- Master Kubernetes Security with CNCF's Most Advanced Certification.

- The Certified Kubernetes Security Specialist (CKS) program provides assurance that a CKS has the skills, knowledge, and competence on a broad range of best practices for securing container-based applications and Kubernetes platforms during build, deployment and runtime.

Prerequisites

- Advanced security certification
- CKA prerequisite required
- Enterprise security focus
- Highest earning potential

Certified Kubernetes Security Specialist(CKS)

Module 1. Cluster Setup (10%)

- Use Network security policies to restrict cluster level access
- Use CIS benchmark to review the security configuration of Kubernetes components
- 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.

Module 2. Cluster Hardening (15%)

- Restrict access to Kubernetes API
- Use Role Based Access Controls to minimize exposure
- Exercise caution in using service accounts
- Update Kubernetes frequently

Module 3. System Hardening (15%)

- 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.

Module 4. Minimize Micro service Vulnerabilities (20%)

- Setup appropriate OS level security domains
- Manage Kubernetes secrets
- Use container runtime sandboxes in multi-tenant environments
- Implement pod to pod encryption by use of mTLS

Module 5. Supply Chain Security (20%)

- Minimize base image footprint
- Secure your supply chain: whitelist allowed registries, sign and validate images
- Use static analysis of user workloads
- Scan images for known vulnerabilities

Module 6. Monitoring, Logging and Runtime Security (20%)

- Perform behavioral analytics of syscall process and file 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