Securing Kubernetes - (CKS)

Course Duration: 5 Days
Exam Reference: CKS

Course Overview

This intensive course prepares students for the Certified Kubernetes Security Specialist (CKS) exam. It emphasizes the advanced skills and knowledge required for securing container-based applications and Kubernetes platforms across the entire lifecycle: build, deployment, and runtime. As a security expert in the DevOps world, you will learn to observe rapidly progressing processes, implement Zero Trust principles, and pinpoint security concerns within any container, process, or subsystem without hindering velocity.

Prerequisites

General Kubernetes cluster administration proficiency (equivalent to CKA), and deep working knowledge of Linux.

Course Objectives

- Harden Cluster and Components: Configure and implement cluster-level hardening techniques for Kubernetes master and worker nodes, ensuring components like the API server and etcd are secure.
- Secure System and Microservices: Apply system hardening best practices and deploy security policies to minimize microservices vulnerabilities during runtime and deployment.
- Manage Supply Chain Risk: Implement comprehensive supply chain security measures, including image signing and vulnerability scanning, to ensure container images are trusted and compliant.
- Monitor, Log, and Secure Runtime: Configure and manage solutions for monitoring, logging, and runtime security, enabling effective threat detection and incident response within the cluster.
- Leverage AI for Configuration: Utilize AI Large Language Model (LLM) prompt engineering to efficiently generate, validate, and troubleshoot Kubernetes configuration snippets, accelerating deployment and solution design.

APPLIED TECHNOLOGY ACADEMY

Contact Us

800.674.3550

2151 W. Hillsboro Blvd., Ste 210
Deerfield Beach, FL 33442

Connect With Us

Securing Kubernetes - (CKS)

Course Outline

Module 1: Learning Your Environment & Cluster Setup

- Underlying Infrastructure Tools (Vim, Tmux)
- Cloud Security Principles & Threat Analysis
- Apply CIS Benchmarks
- Install & Manage Kubernetes with Kubeadm
- Join Node to Cluster / Manage Kubeadm Tokens
- Kubeadm Cluster Upgrade
- Purge/Cleanup Kubernetes Environment

Module 2: Securing the Control Plane

- Kubernetes Architecture & Security Concepts
- Securing the kube-apiserver
- Configure and Enable Audit Logging
- Deploy Falco to Monitor System Calls
- Enable Pod Security Policies (PSPs)
- Encrypt Data at Rest (Encryption Configuration)
- Benchmark Cluster with Kube-Bench
- Securing ETCD (Isolation, Snapshot, and Restore)

Module 3: Container and Application Security

- Container Essentials and Secure Containers
- Creating and Scanning Images (Trivy, Snyk Security)
- Scan a Running Container (Tracee)
- Implement Security Contexts for Pods
- Deploy AppArmor Profiles
- Isolate Container Kernels (gVisor)
- Implement Pod Security Policies (PSPs)
- Enable Pod Security Standards (PSS)
- Deploy Open Policy Agent (OPA) / Gatekeeper
- Policy as Code Implementation

Module 4: Access Control and Networking

- User Administration (Contexts)
- Authentication and Authorization
- Configure Role Based Access Control (RBAC)
- Manage Service Accounts
- Secure and Consume Secrets
- Deploy Secrets with Hashicorp Vault
- Configure NetworkPolicy
- Implement mTLS with Linkerd or istio

Securing Kubernetes - (CKS)

Module 5: Threat Detection and Resilience

- Threat Detection and Active Analysis
- Host Intrusion Detection (OSSEC)
- Network Intrusion Detection (Suricata)
- Disaster Recovery and Response Plan Deployment
- Kasten K10 Backups
- Manually Install & Validate Kubernetes
- Validation with Sonobuoy
- Kubectl Commands (get, describe, sorting)
- Labels, Selectors, and Annotations