Securing Kubernetes - (CKS)

- 5 days
- Lecture & Labs

Course Overview

Kubernetes is a Cloud Orchestration Platform providing reliability, replication, and stability while maximizing resource utilization for applications and services. Our Securing Kubernetes course emphasizes the skills and knowledge for securing container-based applications and Kubernetes platforms, during build, deployment and runtime. As a security expert in the DEVOPS world, your role is to observe and track activity. This means you need to understand processes without inserting secure systems or gatekeepers into the process and slowing it down. You must be able to observe rapidly progressing devops processes and pinpoint which container, process, or subsystem causes a security concern.

Who Should Attend

- This course is ideal for anyone holding a CKA certification and interested in or responsible for cloud security.

What You'll Learn

- Cluster Setup
- Cluster Hardening
- System Hardening
- Minimizing Microservices Vulnerabilities
- Supply Chain Security
- Monitoring, Logging and Runtime Security
- AI LLM prompt engineering for generating configuration snippets and solutions

Outline

Cloud Security Primer

- 💬 Lecture: Basic Principles
- 💬 Lecture: Threat Analysis
- 💬 Lecture: Approach
- 💻 Lecture + Lab: CIS Benchmarks

Securing your Kubernetes Cluster

- 💬 Lecture: Kubernetes Architecture
- 💬 Lecture: Pods and the Control Plane
- 💬 Lecture: Kubernetes Security Concepts

Install Kubernetes using kubeadm

- 💬 Lecture: Configure Network Plugin Requirements
- 💻 Lecture + Lab: Configure Network Plugin Requirements

- 💬 Lecture: Kubeadm Basic Cluster
- 💻 Lecture + Lab: Installing Kubeadm
- 💬 Lecture: Join Node to Cluster
- 💻 Lecture + Lab: Join Node to Cluster
- 💬 Lecture: Kubeadm Token
- 💻 Lecture + Lab: Manage Kubeadm Tokens
- 💬 Lecture: Kubeadm Cluster Upgrade
- 💻 Lecture + Lab: Kubeadm Cluster Upgrade

Securing the kube-apiserver

- 💬 Lecture: Configuring the kube-apiserver
- 💻 Lecture + Lab: Enable Audit Logging
- 💬 Lecture: Falco
- 💻 Lecture + Lab: Deploy Falco to Monitor System Calls
- 💬 Lecture: Enable Pod Security Policies
- 💬 Lecture: Encrypt Data at Rest
- 💻 Lecture + Lab: Encryption Configuration
- 💬 Lecture: Benchmark Cluster with Kube-Bench
- 💻 Lecture + Lab: Kube-Bench

Securing ETCD

- 💬 Lecture: ETCD Isolation
- 💬 Lecture: ETCD Disaster Recovery
- 💬 Lecture: ETCD Snapshot and Restore
- 💻 Lecture + Lab: ETCD Snapshot and Restore

Purge Kubernetes

- 💬 Lecture: Purge Kubeadm
- 💻 Lecture + Lab: Purge Kubeadm

Image Scanning

- 💬 Lecture: Container Essentials
- 💬 Lecture: Secure Containers
- 💻 Lecture + Lab: Creating a Docker Image
- 💬 Lecture: Scanning with Trivy
- 💻 Lecture + Lab: Trivy
- 💬 Lecture: Snyk Security

Manually Installing Kubernetes

- 💬 Lecture: Kubernetes the Alta3 Way
- 💻 Lecture + Lab: Deploy Kubernetes the Alta3 Way
- 💬 Lecture: Validate your Kubernetes Installation
- 💻 Lecture + Lab: Sonobuoy K8s Validation Test

Kubectl (Optional)

- 💬 Lecture: Kubectl get and sorting
- 💻 Lecture + Lab: kubectl get
- 💻 Lecture + Lab: kubectl describe

Labels (Optional)

- 💬 Lecture: Labels
- 💻 Lecture + Lab: Labels and Selectors
- 💬 Lecture: Annotations
- 💻 Lecture + Lab: Insert an Annotation

Securing your Application

- 💬 Lecture: Scan a Running Container
- 💻 Lecture + Lab: Tracee
- 💬 Lecture: Security Contexts for Pods
- 💻 Lecture + Lab: Understanding Security Contexts
- 💬 Lecture: AppArmor Profiles
- 💻 Lecture + Lab: AppArmor
- 💬 Lecture: Isolate Container Kernels
- 💻 Lecture + Lab: gVisor

User Administration

- 💬 Lecture: Contexts
- 💻 Lecture + Lab: Contexts
- 💬 Lecture: Authentication and Authorization
- 💬 Lecture: Role Based Access Control
- 💻 Lecture + Lab: Role Based Access Control
- 💻 Lecture + Lab: RBAC Distributing Access
- 💬 Lecture: Service Accounts
- 💻 Lecture + Lab: Limit Pod Service Accounts

Implementing Pod Policy

- 💬 Lecture: Admission Controller
- 💻 Lecture + Lab: Create a LimitRange
- 💬 Lecture: Pod Security Standards
- 💻 Lecture + Lab: Enable PSS
- 💬 Lecture: Open Policy Agent
- 💻 Lecture + Lab: Deploy Gatekeeper

Securing Secrets

- 💬 Lecture: Secrets
- 💻 Lecture + Lab: Create and Consume Secrets
- 💬 Lecture: Hashicorp Vault

Securing the Network

- 💬 Lecture: Networking Plugins
- 💬 Lecture: NetworkPolicy
- 💻 Lecture + Lab: Deploy a NetworkPolicy
- 💻 Lecture + Lab: Namespace Network Policy
- 💬 Lecture: mTLS
- 💻 Lecture + Lab: mTLS with Linkerd
- 💻 Lecture + Lab: Linkerd Dashboard

Threat Analysis and Detection

- 💬 Lecture: Active Threat Analysis
- 💬 Lecture: Host Intrusion Detection
- 💬 Lecture: Network Intrusion Detection
- 💬 Lecture: Physical Intrusion Detection

Prerequisites

```
- Working knowledge of Kubernetes and/or CKA
- Basic Linux skills are helpful.
- Familiarity with a text editor like vi, vim, or nano is helpful.
```