SHI | TRAINING & ADOPTION

Course Outline

Securing Kubernetes
Course CKSS: 5 days Instructor Led

About this course
This class prepares students for the Certified Kubernetes Security Specialist (CKS) exam. Kubernetes is a Cloud Orchestration Platform providing reliability, replication, and stability while maximizing resource utilization for applications and services. By the conclusion of this hands-on, vendor agnostic training you will be equipped with a thorough understanding of cloud security fundamentals, along with the knowledge, skills and abilities to secure a Kubernetes cluster, detect threats, and properly resolve a security catastrophe. This course includes hands-on instruction which develops skills and knowledge for securing container-based applications and Kubernetes platforms, during build, deployment, and runtime.

We prioritize covering all objectives and concepts necessary for passing the Certified Kubernetes Security Specialist (CKS) exam. You will be provided the components necessary to assemble your own high availability Kubernetes environment and harden it for your security needs.

Audience profile
- Security Professionals working with Kubernetes Clusters
- Container Orchestration Engineers
- DevOps Professionals

At course completion
After completing this course, students will be able to:
- Cloud Security Fundamentals
- Cluster Hardening
- System Hardening
- Minimize Microservice Vulnerabilities
- Supply Chain Security
- Disaster Recovery
- Secure Back-up and Restore

Course Outline

Learning Your Environment

- Underlying Infrastructure
    - Lab - Using Vim
    - Lab - Tmux

Cloud Security Primer

- Basic Principles
- Threat Analysis
- Approach

Course Outline

- Lab - CIS Benchmarks

Securing your Kubernetes Cluster

- Kubernetes Architecture
- Pods and the Control Plane
- Kubernetes Security Concepts

Install Kubernetes using kubeadm

- Configure Network Plugin Requirements
  - Lab - Configure Network Plugin Requirements
- Kubeadm Basic Cluster
  - Lab - Installing Kubeadm
- Join Node to Cluster
  - Lab - Join Node to Cluster
- Kubeadm Token
  - Lab - Manage Kubeadm Tokens
- Kubeadm Cluster Upgrade
  - Lab - Kubeadm Cluster Upgrade

Securing the kube-apiserver

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

Securing ETCD

- ETCD Isolation
- ETCD Disaster Recovery
- ETCD Snapshot and Restore
  - Lab - ETCD Snapshot and Restore

Course Outline

Purge Kubernetes

- Purge Kubeadm
    - Lab - 3Purge Kubeadm

Image Scanning

- Container Essentials
- Secure Containers
    - Lab - Creating a Docker Image
- Scanning with Trivy
    - Lab - Trivy
- Snyk Security

Manually Installing Kubernetes

- Kubernetes the Alta3 Way
    - Lab - Deploy Kubernetes the Alta3 Way
- Validate your Kubernetes Installation
    - Lab - Sonobuoy K8s Validation Test

Kubectl (Optional)

- Kubectl get and sorting
    - Lab - kubectl get
    - Lab - kubectl describe

Labels (Optional)

- Labels
    - Lab - Labels and Selectors
- Annotations
    - Lab - Insert an Annotation

Securing your Application

- Scan a Running Container
    - Lab - Tracee
- Security Contexts for Pods

Course Outline

    - Lab - Understanding Security Contexts
- AppArmor Profiles
- AppArmor
- Isolate Container Kernels
    - Lab - gVisor

Pod Security

- Pod Security Policies
    - Lab - Deploy a PSP
- Pod Security Standards
    - Lab - Enable PSS

Open Policy Agent (OPA)

- Admission Controller
    - Lab - Create a LimitRange
- Open Policy Agent
- Policy as Code
    - Lab - Deploy Gatekeeper

User Administration

- Contexts
    - Lab - Contexts
- Authentication and Authorization
- Role Based Access Control
    - Lab - Role Based Access Control
    - Lab - RBAC Distributing Access
- Service Accounts
    - Lab - Limit Pod Service Accounts

Securing Secrets

- Secrets
    - Lab - Create and Consume Secrets
- Hashicorp Vault
    - Lab - Deploy Vault

SHI | TRAINING & ADOPTION

Course Outline

Securing the Network

- Networking Plugins
- NetworkPolicy
    - Lab - Deploy a NetworkPolicy
- mTLS
    - Lab - Linkerd
- mTLS with istio
    - Lab - istio

Threat Detection

- Active Threat Analysis
- Host Intrusion Detection
    - Lab - Deploy OSSEC
- Network Intrusion Detection
    - Lab - Deploy Suricata
- Physical Intrusion Detection

Disaster Recovery

- Harsh Reality of Security
- Deploy a Response Plan
- Kasten K10 Backups
    - Lab - Deploy K10