Kubernetes Security Specialist (CKS)

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 WILL BENEFIT FROM THIS COURSE?

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

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

COURSE OBJECTIVES

- Cluster Setup
- Cluster Hardening
- System Hardening
- Minimizing Microservices Vulnerabilities
- Supply Chain Security
- Monitoring, Logging, and Runtime Security

COURSE OUTLINE

Cloud Security Overview

- Introduction to DevSecOps
- Assessment
- Prevention
- Detection
- Reaction
- Classes of Attackers
- Types of Attacks
- Attack Surfaces
- Hardware and Firmware Considerations
- Security Agencies
- Manage External Access

Security procedures during Installation planning

- Container Image Supply Chain
- Runtime Sandbox
- Verify Platform Binaries
- Minimize Access to GUI
- Policy Based Control

Securing Cluster Installation

- Kubernetes version control
- Why the Kernel selection is so important with container-based logic
- Tools to Harden the Kernel
- Kernel Hardening Examples
- Mitigating Kernel Vulnerabilities

Securing the kube-apiserver

- Restrict Access to API
- Enable Kube-apiserver Auditing
- Configuring RBAC
- Pod Security Standards
- Minimize Identity and Access Management Roles
- Understanding the critical role of etcd in kubernetes
- Protecting etcd
- CIS Benchmark
- Using Service Accounts

Network Security

- Firewalling Basics
- Network Plugins
- iptables
- Mitigate Brute Force Login Attempts
- Netfilter rule management
- Netfilter Implementation
- Netfilter (nft) command line skills
- Ingress Objects
- Pod to Pod Encryption
- Restrict Cluster Level Access

Workload Considerations

- Minimize Base Image
- Static Analysis of Workloads
- Runtime Analysis of Workloads
- Container Immutability
- Mandatory Access Control
- AppArmor
- Generate AppArmor Profiles

Issue Detection

- Understanding Phases of Attack
- Preparation
- Understanding an Attack Progression
- During an Incident
- Handling Incident Aftermath
- Intrusion Detection Systems
- Threat Detection
- Behavioral Analytics

Hands-On Labs

- Basic Principles
- Threat Analysis
- Approach
- CIS Benchmarks

Securing your Kubernetes Cluster

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

Install Kubernetes using kubeadm

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

Securing the kube-apiserver

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

Securing ETCD

- ETCD Isolation
- ETCD Disaster Recovery

- ETCD Snapshot and Restore
- ETCD Snapshot and Restore

Purge Kubernetes
- Purge Kubeadm
- Purge Kubeadm

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

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

Kubectl (Optional)
- Kubectl get and sorting
- kubectl get
- kubectl describe

Labels (Optional)
- Labels
- Labels and Selectors
- Annotations
- Insert an Annotation

Securing your Application
- Scan a Running Container
- Tracee
- Security Contexts for Pods
- Understanding Security Contexts
- AppArmor Profiles
- AppArmor
- Isolate Container Kernels
- gVisor

User Administration
- Contexts
- Contexts
- Authentication and Authorization
- Role-Based Access Control
- Role Based Access Control
- RBAC Distributing Access

- Service Accounts
- Limit Pod Service Accounts

Implementing Pod Policy

- Admission Controller
- Create a LimitRange
- Pod Security Standards
- Enable PSS
- Open Policy Agent
- Deploy Gatekeeper

Securing Secrets

- Secrets
- Create and Consume Secrets
- Hashicorp Vault

Securing the Network

- Networking Plugins
- NetworkPolicy
- Deploy a NetworkPolicy
- Namespace Network Policy
- mTLS
- mTLS with Linkerd
- Linkerd Dashboard

Threat Analysis and Detection

- Active Threat Analysis
- Host Intrusion Detection
- Network Intrusion Detection
- Physical Intrusion Detection

Continuing Education

- Continuing Education

WHY TRAIN WITH SUNSET LEARNING INSTITUTE?

Sunset Learning Institute (SLI) has been an innovative leader in developing and delivering authorized technical training since 1996. Our goal is to help our customers optimize their technology Investments by providing convenient, high quality technical training that our customers can rely on. We empower students to master their desired technologies for their unique environments.

What sets SLI apart is not only our immense selection of trainings options, but our convenient and consistent delivery system. No matter how complex your environment is or where you are located, SLI is sure to have a training solution that you can count on!

Premiere World Class Instruction Team

- All SLI instructors have a four-year technical degree, instructor level certifications and field consulting work experience
- Sunset Learning has won numerous Instructor Excellence and Instructor Quality Distinction awards since 2012

Enhanced Learning Experience

- The goal of our instructors during class is ensure students understand the material, guide them through our labs and encourage questions and interactive discussions.

Convenient and Reliable Training Experience

- You have the option to attend classes live with the instructor, at any of our established training facilities, or from the convenience of your home or office
- All Sunset Learning Institute classes are guaranteed to run – you can count on us to deliver the training you need when you need it!

Outstanding Customer Service

- You will work with a dedicated account manager to suggest the optimal learning path for you and/or your team
- An enthusiastic student services team is available to answer any questions and ensure a quality training experience

Interested in Private Group Training?

Contact Us