Certified Kubernetes Security Specialist (CKS)

Course Duration : 24 Hours **Course code : CKS**

1. Course Overview

The **Certified Kubernetes Security Specialist (CKS)** course focuses on securing Kubernetes clusters and containerized applications. This course prepares professionals to protect Kubernetes environments by implementing security best practices across cluster setup, workload security, networking, and runtime protection, aligned with the official CKS certification objectives.

2. What you'll learn?

- Kubernetes security architecture
- Cluster hardening techniques
- Securing workloads and containers
- Kubernetes network security
- Runtime security and monitoring
- Incident response and troubleshooting

3. Target Audience

- Kubernetes administrators
- DevSecOps engineers
- Cloud security professionals
- Platform engineers
- IT security specialists

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com

4. Pre-Requisites

- Experience with Kubernetes administration
- Knowledge of containers and Docker
- Understanding of Linux and networking concepts

5. Course Content (Modules)

Module 1: Kubernetes Security Fundamentals

- Threat model and attack surface
- Security architecture overview

Module 2: Cluster Setup and Hardening

- Securing control plane components
- Node security best practices

Module 3: Workload Security

- Pod security standards
- Securing container images

Module 4: Network Security

- Network policies
- Service and ingress security

Module 5: Runtime Security

- Detecting abnormal behavior
- Runtime protection tools

Module 6: Monitoring, Auditing, and Incident Response

- Logging and auditing
- Responding to security incidents