Certified Kubernetes Security Specialist (CKS)

Curriculum 3 Days

Day - 1

- **Cluster Setup**
  - Use Network security policies to restrict cluster level access
  - Use CIS benchmark to review the security configuration of Kubernetes components (etcd,
  - Kubelet, Kubedns, Kubeapi)
  - Properly set up Ingress objects with security control
  - Protect node metadata and endpoints
  - Minimize use of, and access to, GUI elements
  - Verify platform binaries before deploying
- **Cluster Hardening**
  - Restrict access to Kubernetes API
  - Use Role-Based Access Controls to minimize exposure
  - Exercise caution in using service accounts e.g. disable defaults, minimize permissions on
  - newly created ones
  - Update Kubernetes frequently
- **System Hardening**
  - Minimize host OS footprint (reduce attack surface)
  - Minimize IAM roles
  - Minimize external access to the network
  - Appropriately use kernel hardening tools such as AppArmor, seccomp

Day - 2

- **Microservices**
  - Introduction to Microservices
  - Microservices Architecture
  - What is Istio?
  - What is a service mesh?
  - Why use Istio?
  - Core features
  - Traffic management
  - Security
- **Minimize Microservice Vulnerabilities**
  - Setup appropriate OS level security domains e.g. using PSP, OPA, security contexts
  - Manage Kubernetes secrets
  - Use container runtime sandboxes in multi-tenant environments (e.g. gvisor, kata containers)
  - Implement pod to pod encryption by use of mTLS

Day - 3

- **Supply Chain Security**
  - Minimize base image footprint
  - Secure your supply chain: whitelist allowed image registries, sign and validate images
  - Use static analysis of user workloads (e.g. Kubernetes resources, docker files)
  - Scan images for known vulnerabilities
- **Monitoring, Logging and Runtime Security**
  - Perform behavioral analytics of syscall process and file activities at the host and container
  - level to detect malicious activities
  - Detect threats within a physical infrastructure, apps, networks, data, users, and workloads
  - Detect all phases of attack regardless where it occurs and how it spreads
  - Perform deep analytical investigation and identification of bad actors within environment
  - Ensure immutability of containers at runtime
  - Use Audit Logs to monitor access