Certified Kubernetes Security Specialist

Module 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 Setup Ingress Objects with Security Control
Protect Node Metadata and Endpoints
Minimize Use of, and Access to, GUI Elements
Verify Platform Binaries before Deploying

Module 2 – 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

Module 3 – System Hardening

Minimize Host OS Foorprint (Reduce Attack Surface)
Minimize IAM Roles
Minimize External Access to the Network
Appropriately Use Kernel Hardening Tools Such as AppArmor, Seccomp

Module 4 – Minimize Microservice Vulnerabilities

Setup Appropriate OS Level Security Domains e.g. Using PSP, OPA, Security Contexts
Manage Kubernetes Secrets
Use Kubernetes Runtime Sandboxes in Multi-Tenant Environments (e.g. Gvisor, Kata Containers)
Implement Pod to Pod encryption by use of MTLS

Module 5 – Supply Chain Security

Minimize Base Image Footprint
Secure your Supply Chain: Whitelist allowed Registries, Sign and Validate Images
Use Static Analysis of User Workloads (e.g. Kubernetes Resources, Docker Files) Scan Images for Known Vulnerabilities

Module 6 – 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 Physical Infrastructure, Apps, Networks, Data, Users and Workloads
Detect All Phases of Attack Regardless Where It Occurs and How It Works
Perform Deep Analytical Investigation and Identification of Bad Actors within Environment Ensure Immutability of Containers at Runtime
Use Audit Logs to Monitor Access