Securing Kubernetes and Container Environments in the Cloud Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Securing Kubernetes and Container Environments in the Cloud Training Course a comprehensive, hands-on deep dive into securing modern, cloud-native application architectures built on Kubernetes and containerization technologies like Docker. It adopts a DevSecOps and Shift-Left philosophy, moving beyond traditional perimeter defenses to embed security controls across the entire Container Lifecycle from source code and Image Build through deployment, orchestration, and Runtime Protection. Participants will master the art of hardening the critical 4Cs of cloud-native security Cloud, Cluster, Container, and Code to mitigate risks like supply chain attacks, privilege escalation, and misconfiguration in high-stakes, multi-cloud environments.

The training emphasizes practical, Zero Trust principles, focusing on Role-Based Access Control, advanced Network Policies, and Secret Management within major cloud platforms. By engaging with real-world attack and defense scenarios in dedicated lab environments, attendees will gain the skills necessary to implement Policy-as-Code, automate Vulnerability Scanning, and establish robust Cloud-Native Security Posture Management. This prepares security professionals and DevOps teams to build immutable infrastructure and defend against the evolving threats targeting ephemeral workloads and complex distributed systems.

Programme Curriculum

Securing Kubernetes and Container Environments in the Cloud Training Course

Introduction

Securing Kubernetes and Container Environments in the Cloud Training Course a comprehensive, hands-on deep dive into securing modern, cloud-native application architectures built on Kubernetes and containerization technologies like Docker. It adopts a DevSecOps and Shift-Left philosophy, moving beyond traditional perimeter defenses to embed security controls across the entire Container Lifecycle from source code and Image Build

through deployment, orchestration, and Runtime Protection. Participants will master the art of hardening the critical 4Cs of cloud-native security Cloud, Cluster, Container, and Code to mitigate risks like supply chain attacks, privilege escalation, and misconfiguration in high-stakes, multi-cloud environments.

The training emphasizes practical, Zero Trust principles, focusing on Role-Based Access Control, advanced Network Policies, and Secret Management within major cloud platforms. By engaging with real-world attack and defense scenarios in dedicated lab environments, attendees will gain the skills necessary to implement Policy-as-Code, automate Vulnerability Scanning, and establish robust Cloud-Native Security Posture Management. This prepares security professionals and DevOps teams to build immutable infrastructure and defend against the evolving threats targeting ephemeral workloads and complex distributed systems.

Course Duration

10 days

Course Objectives

Upon completion, participants will be able to:

1. Implement Zero Trust principles across the entire Kubernetes cluster and container ecosystem.
2. Master Cloud-Native Security Posture Management for continuous risk assessment.
3. Harden the Kubernetes Control Plane and data store against unauthorized access and modification.
4. Apply Policy-as-Code using tools like Open Policy Agent or Kyverno for mandatory security controls.
5. Perform advanced Container Image Scanning and Vulnerability Management within the CI/CD pipeline
6. Configure granular Role-Based Access Control and Service Accounts to enforce Least Privilege.
7. Design and implement fine-grained Kubernetes Network Policies for micro-segmentation and lateral movement prevention.
8. Establish robust and encrypted Secret Management strategies using tools like HashiCorp Vault and cloud-native key management services.
9. Secure the Container Runtime using seccomp AppArmor, and behavioral threat detection mechanisms.
10. Develop a comprehensive strategy for Supply Chain Security for containerized applications
11. Implement thorough Audit Logging and Threat Detection for forensic analysis and incident response in cloud environments.
12. Protect sensitive data with Encryption at Rest and in Transit throughout the cluster.
13. Integrate container security practices into a cohesive DevSecOps workflow for automation and continuous compliance.

Target Audience

- Cloud Security Engineers
- DevSecOps Engineers
- Kubernetes Administrators/SREs
- Application Security Specialists (AppSec)
- Cloud Architects
- Security Consultants/Pentesters
- Lead Developers working with containerized applications
- IT Security Managers overseeing cloud-native adoption

Course Modules

Module 1: Cloud-Native Security Fundamentals and Architecture

- The 4Cs of Cloud-Native Security.
- Understanding the Container Lifecycle and attack surface
- Principles of Zero Trust and Least Privilege in Kubernetes.
- Introduction to DevSecOps and Shift-Left security practices.
- Case Study: Analyzing the Capital One breach to understand the impact of cloud and configuration missteps.

Module 2: Container Image Security

- Minimizing the attack surface
- Best practices for writing secure Dockerfiles
- Automated Vulnerability Scanning in the CI/CD pipeline
- Enforcing Image Signing and provenance
- Case Study: The Log4Shell vulnerability and its impact on container image supply chain security.

Module 3: Container Registry and Distribution Security

- Hardening the Container Registry
- Implementing strong IAM and access controls for image pull/push.
- Scanning images at rest and blocking deployment of images with critical CVEs.
- Using private registries and geo-replication for business continuity.
- Case Study: A private registry breach leading to the deployment of malicious images in a production environment.

Module 4: Kubernetes Control Plane Hardening

- Securing the API Server
- Protecting etcd
- Implementing Kubernetes Audit Logging for forensic analysis.
- Understanding and configuring Admission Controllers
- Case Study: A real-world attack exploiting an exposed Kubelet or unauthenticated API server.

Module 5: Authentication and Authorization with RBAC

- Deep dive into Kubernetes Role-Based Access Control architecture.
- Defining Roles, ClusterRoles, RoleBindings, and ClusterRoleBindings.
- Enforcing Least Privilege for users, groups, and Service Accounts.
- Integrating with Cloud IAM and external identity providers
- Case Study: Exploitation due to overly permissive ClusterRoleBindings and lateral movement within the cluster.

Module 6: Advanced Pod Security Standards

- Understanding the three Pod Security Standards
- Implementing Security Contexts for fine-grained control
- Restricting container privileges with Linux capabilities and seccomp profiles.
- Utilizing Pod Security Admission for enforcement across namespaces.
- Case Study: Mitigating the risk of a container breakout attack using an appropriate Pod Security Standard.

Module 7: Network Security and Micro-segmentation

- Implementing Kubernetes Network Policies Calico, Cilium for isolation.
- Securing North-South and East-West traffic.
- Introduction to Service Mesh Security for Mutual TLS.
- Hardening the Node OS and cloud-specific networking security groups.
- Case Study: How implementing NetworkPolicy prevented a lateral movement-based ransomware attack in a multi-tenant cluster.

Module 8: Secrets Management and Encryption

- The risk of plain-text Kubernetes Secrets and why they are insufficient alone.
- Integration with external Secret Managers
- Encrypting secrets at rest in etcd and transit
- Best practices for Secret Rotation and injection into pods.
- Case Study: A production incident where GitHub tokens were discovered in a leaked Kubernetes Secret.

Module 9: Runtime Security and Threat Detection

- Monitoring container and cluster activity for anomalous behavior.
- Utilizing Falco or similar tools for Behavioral Anomaly Detection.
- Implementing Intrusion Detection/Prevention Systems for containers.
- Responding to and isolating a Container Breakout or Cryptomining threat.
- Case Study: Detecting and responding to a Cryptojacking malware running inside a seemingly legitimate container.

Module 10: Infrastructure as Code (IaC) Security

- Scanning Kubernetes manifests for Misconfigurations
- Implementing Policy-as-Code to enforce security governance.
- Securing the GitOps pipeline and Terraform/CloudFormation templates.
- Automated remediation of configuration drift and policy violations.
- Case Study: Preventing a configuration drift attack where an administrator manually created an insecure deployment that bypassed CI/CD scans.

Module 11: Cloud-Native Security Posture Management

- Understanding the features and value proposition of CNAPP platforms.
- Continuous Compliance Monitoring against industry benchmarks
- Integration of Cloud Security Posture Management with container security.
- Prioritizing and remediating risks across the entire cloud-native stack.
- Case Study: A financial institution utilizing a CNAPP platform to achieve PCI DSS compliance for their containerized payment system.

Module 12: Security Monitoring, Logging, and Auditing

- Centralized logging for containers and the Kubernetes control plane
- Configuring and analyzing Kubernetes Audit Logs for suspicious activities.
- Implementing a Security Information and Event Management solution for alert correlation.
- Creating effective dashboards for real-time security visibility.
- Case Study: Using a timeline derived from Kubernetes Audit Logs to perform a root cause analysis of a security incident.

Module 13: Supply Chain Security for the Cloud-Native Era

- Vetting open-source dependencies and Software Bill of Materials generation.
- Secure build environments and isolating build agents.
- Implementing policies to ensure only Signed Images are deployed.
- Mitigating risks from third-party tools and vendor compromises.
- Case Study: The SolarWinds attack and the necessary container security mitigations for similar supply chain breaches.

Module 14: Serverless and Function Security

- Securing Cloud Functions
- Best practices for IAM and network isolation for serverless workloads.
- The unique runtime security challenges of FaaS
- Securing the function code and managing environment variables.
- Case Study: A logic flaw in an AWS Lambda function that was exploited for data exfiltration due to misconfigured permissions.

Module 15: Incident Response and Disaster Recovery

- Developing a specific Container and Kubernetes Incident Response plan.
- Steps for isolating a compromised node or namespace
- Forensic collection from ephemeral container environments.
- Strategies for backing up etcd and application state for rapid recovery.
- Case Study: A company's post-mortem analysis of a service disruption caused by a denial-of-service attack on their Kubernetes cluster.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.com or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to FINESKILL TRAINING CENTER account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
07 Sep 2026	18 Sep 2026	Online	$2,200
14 Sep 2026	25 Sep 2026	Online	$2,200
21 Sep 2026	02 Oct 2026	Online	$2,200
28 Sep 2026	09 Oct 2026	Online	$2,200
05 Oct 2026	16 Oct 2026	Online	$2,200
12 Oct 2026	23 Oct 2026	Online	$2,200
19 Oct 2026	30 Oct 2026	Online	$2,200
26 Oct 2026	06 Nov 2026	Online	$2,200

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com