Container Orchestration Security with Amazon EKS Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The shift to cloud-native architectures powered by containerization and microservices has dramatically increased development velocity, yet it simultaneously expanded the enterprise attack surface. As the industry standard for orchestration, Kubernetes specifically managed by Amazon EKS (Elastic Kubernetes Service) introduces unique security challenges across the entire DevSecOps pipeline. Container Orchestration Security with Amazon EKS Training Course is meticulously designed to equip security and DevOps engineers with the advanced, practical knowledge needed to enforce zero-trust principles and implement robust, layered security controls. We move beyond fundamental cluster setup to deep-dive into the security architecture of EKS, mastering the intersection of AWS IAM, Kubernetes RBAC, and network policy to achieve a truly hardened EKS environment.

A proactive security posture is non-negotiable for production-grade, highly-regulated cloud workloads. This training emphasizes a shift-left security approach, integrating automated security tooling from image scanning in Amazon ECR to continuous runtime security monitoring. We explore best practices for secrets management using AWS Secrets Manager and KMS, configure network segmentation with VPC CNI and Network Policies, and implement fine-grained Pod Identity for least-privilege access. Successful completion ensures participants can not only defend against contemporary threats like supply chain attacks and container escapes but also establish a Kubernetes Security Posture Management (KSPM) framework that meets strict regulatory compliance standards.

Programme Curriculum

Container Orchestration Security with Amazon EKS Training Course

Introduction

The shift to cloud-native architectures powered by containerization and microservices has dramatically increased development velocity, yet it simultaneously expanded the enterprise attack surface. As the industry standard for orchestration, Kubernetes specifically managed by Amazon EKS (Elastic Kubernetes Service) introduces unique security challenges across the entire DevSecOps pipeline. Container Orchestration Security with Amazon EKS Training Course is meticulously designed to equip security and DevOps engineers with the advanced, practical knowledge needed to enforce zero-trust principles and implement robust, layered security controls. We move beyond fundamental cluster setup to deep-dive into the security architecture of EKS, mastering the intersection of AWS IAM, Kubernetes RBAC, and network policy to achieve a truly hardened EKS environment.

A proactive security posture is non-negotiable for production-grade, highly-regulated cloud workloads. This training emphasizes a shift-left security approach, integrating automated security tooling from image scanning in Amazon ECR to continuous runtime security monitoring. We explore best practices for secrets management using AWS Secrets Manager and KMS, configure network segmentation with VPC CNI and Network Policies, and implement fine-grained Pod Identity for least-privilege access. Successful completion ensures participants can not only defend against contemporary threats like supply chain attacks and container escapes but also establish a Kubernetes Security Posture Management (KSPM) framework that meets strict regulatory compliance standards.

Course Duration

5 days

Course Objectives

Upon completion of this course, participants will be able to:

1. Harden the Amazon EKS control and data planes according to CIS benchmarks and AWS Best Practices.
2. Design and implement a robust Identity and Access Management (IAM) strategy for EKS using IAM Roles for Service Accounts (IRSA).
3. Configure fine-grained authorization within Kubernetes using Role-Based Access Control (RBAC) to enforce the Principle of Least Privilege.
4. Master secrets management by integrating EKS with AWS Secrets Manager and KMS for data-at-rest encryption.
5. Implement comprehensive container image security, including automated vulnerability scanning in Amazon ECR.
6. Apply Pod Security Standards (PSS) and Network Policies for effective network segmentation and blast radius reduction.
7. Establish continuous runtime security monitoring and threat detection using tools like Amazon GuardDuty and Falco.
8. Secure the CI/CD pipeline to prevent software supply chain attacks against containerized applications.
9. Configure EKS logging and auditing using AWS CloudTrail and EKS Control Plane Logs for forensics and compliance.
10. Implement secure service mesh architectures for encrypted, authorized, and observable inter-service communication.
11. Perform security assessment and Kubernetes Security Posture Management using industry-standard open-source and AWS tools.
12. Securely manage and rotate API keys and certificates within the EKS cluster lifecycle.
13. Develop an incident response plan tailored for container orchestration security in the AWS environment.

Target Audience

1. DevOps Engineers and SREs.
2. Cloud Security Engineers.
3. Security Architects.
4. Application Developers.
5. Platform Engineers.
6. Information Security Analysts.
7. System Administrators.
8. Technical Leaders.

Course Modules

Module 1: EKS Security Foundation & Shared Responsibility

- Container Security landscape and threat model for Kubernetes/EKS.
- Understanding the AWS Shared Responsibility Model specifically for EKS.
- EKS Control Plane and Data Plane hardening.
- Implementing CIS Kubernetes Benchmarks for EKS.
- Case Study: Analyzing a misconfigured EKS API server endpoint and its exploitation.

Module 2: Identity & Access Management (IAM/RBAC)

- Deep dive into IAM Roles for Service Accounts for least privilege.
- Mastering Kubernetes Role-Based Access Control for internal cluster authorization.
- Securing Worker Node access and using Instance Profiles.
- Integrating External Identity Providers via OIDC.
- Case Study: Remediation of a privilege escalation vulnerability via an over-permissive Service Account.

Module 3: Container Image & Supply Chain Security

- Secure Dockerfile creation and multi-stage builds.
- Automated Vulnerability Scanning and policy enforcement with Amazon ECR and third-party tools.
- Implementing Image Signing and Verification
- Managing trusted base images and minimizing image size.
- Case Study: Preventing a supply chain attack by blocking a compromised third-party base image from deployment.

Module 4: Pod Security & Runtime Protection

- Enforcing security policies using Pod Security Standards.
- Deep dive into Runtime Security using tools like Falco or AWS GuardDuty.
- Limiting host access with Security Contexts and restricting Linux capabilities.
- Implementing mandatory access controls.
- Case Study: Detecting and blocking a live container escape attempt based on abnormal process execution.

Module 5: Network Security & Segmentation

- Configuring VPC CNI and Security Groups for Pods.
- Implementing Kubernetes Network Policies for micro-segmentation.
- Securing ingress and egress traffic using Load Balancers and Ingress Controllers.

- Utilizing Service Mesh for mutual TLS and traffic authorization.
- Case Study: Designing and applying zero-trust Network Policies to isolate a sensitive microservice.

Module 6: Secrets Management and Data Protection

- Centralizing secrets with AWS Secrets Manager and AWS Parameter Store.
- Integrating secrets into Pods securely.
- Encrypting data at rest using AWS KMS for etcd and EBS volumes.
- Managing encryption keys and key rotation strategies.
- Case Study: Migrating an application's hardcoded credentials into a secure, KMS-encrypted secret store.

Module 7: Observability, Auditing & Compliance

- Configuring EKS Control Plane Logs and Audit Logging via CloudWatch/S3.
- Implementing centralized logging and monitoring for security events.
- Using AWS CloudTrail for API activity auditing.
- Establishing a Kubernetes Security Posture Management workflow and generating compliance reports.
- Case Study: Using audit logs to perform a post-incident forensic analysis of unauthorized API calls.

Module 8: Advanced Security Topics & Best Practices

- Securely managing and executing Cluster Upgrades and patches.
- Securing Serverless Containers using AWS Fargate security model.
- Automating security checks using Infrastructure as Code tools.
- Developing and testing a container incident response plan.
- Case Study: Automating the deployment of an updated, secure EKS cluster with Blue/Green strategies via GitOps.

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.org 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
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

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

Register Online Now

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