Training Course on Securing Cloud-Native Applications for Forensic Readiness

Professional Development Training Course Outline

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

Course Introduction

In today’s digital era, cloud-native applications are the cornerstone of agile software delivery and scalability. However, they present unique challenges when it comes to security, incident response, and digital forensics. Training Course on Securing Cloud-Native Applications for Forensic Readiness is specifically designed for cybersecurity professionals, DevSecOps teams, and IT leaders who aim to implement proactive strategies to secure cloud-native systems while ensuring forensic readiness. Through advanced hands-on labs, real-world case studies, and cloud-native tools like Kubernetes, Docker, and CI/CD pipelines, this course empowers professionals to mitigate threats and establish evidence-preserving security frameworks.

This course addresses the critical need for forensic-ready cloud environments that align with compliance, legal, and operational standards. Learners will explore topics including cloud workload protection, container security, event logging, zero-trust architecture, immutable infrastructure, and threat intelligence integration. By the end of this program, participants will be able to detect, respond, and analyze cloud-native threats efficiently while maintaining evidence admissibility. The course bridges the knowledge gap between cloud security and digital forensics, making it essential for both offensive and defensive security practitioners.

Programme Curriculum

Training Course on Securing Cloud-Native Applications for Forensic Readiness

Introduction

In today’s digital era, cloud-native applications are the cornerstone of agile software delivery and scalability. However, they present unique challenges when it comes to security, incident response, and digital forensics. Training Course on Securing Cloud-Native Applications for Forensic Readiness is specifically designed for cybersecurity professionals, DevSecOps teams, and IT leaders who aim to implement proactive strategies to secure cloud-native systems while ensuring forensic readiness. Through advanced hands-on labs, real-world case studies, and cloud-native tools like

Kubernetes, Docker, and CI/CD pipelines, this course empowers professionals to mitigate threats and establish evidence-preserving security frameworks.

This course addresses the critical need for forensic-ready cloud environments that align with compliance, legal, and operational standards. Learners will explore topics including cloud workload protection, container security, event logging, zero-trust architecture, immutable infrastructure, and threat intelligence integration. By the end of this program, participants will be able to detect, respond, and analyze cloud-native threats efficiently while maintaining evidence admissibility. The course bridges the knowledge gap between cloud security and digital forensics, making it essential for both offensive and defensive security practitioners.

Course Objectives

1. Understand the principles of cloud-native security architecture.
2. Implement forensic readiness frameworks in containerized environments.
3. Configure secure logging and monitoring for Kubernetes and Docker.
4. Apply zero-trust principles to microservices and APIs.
5. Identify and respond to cloud-native cyber threats.
6. Integrate threat intelligence feeds for real-time detection.
7. Automate incident response workflows using SIEM and SOAR tools.
8. Analyze logs and events for post-breach forensics.
9. Harden container images using policy-as-code tools.
10. Conduct cloud workload protection platform (CWPP) assessments.
11. Implement immutable infrastructure for attack surface reduction.
12. Maintain chain-of-custody for forensic evidence in cloud systems.
13. Build resilient CI/CD pipelines with embedded security gates.

Target Audience

1. Cloud Security Engineers
2. DevSecOps Professionals
3. Forensic Analysts
4. Cybersecurity Architects
5. Compliance Officers
6. Penetration Testers
7. IT Auditors
8. Platform Engineers

Course Duration: 5 days

Course Modules

Module 1: Foundations of Cloud-Native Forensics

- Key components of cloud-native applications
- Introduction to forensic readiness principles
- Threat landscape in containerized systems
- Legal considerations in cloud forensics
- Toolkits for cloud-native evidence collection
- **Case Study**: Forensic gaps in a Kubernetes-based breach

Module 2: Kubernetes Security & Evidence Collection

- Securing the Kubernetes control plane
- Monitoring audit logs and API activity
- Forensic data collection from pods and containers

- RBAC configuration for evidence access
- Leveraging Falco and Kubeaudit tools
- **Case Study**: Investigating privilege escalation in K8s

Module 3: Container Image Hardening and Validation

- Risks in container image supply chains
- Implementing image scanning and signing
- Container runtime security practices
- Policy-as-code tools like OPA & Kyverno
- Validating integrity during incident response
- **Case Study**: Malicious container deployed via CI/CD

Module 4: Securing CI/CD for Forensic Integrity

- CI/CD pipeline attack vectors
- Embedding security gates and audits
- Logging build-time and deploy-time events
- Securing secrets and credentials
- Ensuring forensic traceability in pipelines
- **Case Study**: Source-code tampering incident analysis

Module 5: SIEM & SOAR Integration in Cloud Environments

- Designing cloud-native SIEM pipelines
- Enriching logs with threat intel feeds
- Automating response using SOAR playbooks
- Managing multi-cloud log aggregation
- Ensuring data retention for forensics
- **Case Study**: Cross-cloud intrusion response automation

Module 6: Threat Hunting in Cloud-Native Infrastructure

- Indicators of compromise (IoCs) in cloud logs
- Setting up detection rules with open-source tools
- Timeline reconstruction using audit logs
- Pivoting across microservices during hunts
- Reporting and documentation best practices
- **Case Study**: Insider threat uncovered through log analysis

Module 7: Legal and Compliance Frameworks for Cloud Forensics

- Understanding GDPR, HIPAA, and ISO requirements
- Admissibility of cloud forensic evidence
- Building forensic-ready service level agreements (SLAs)
- Data sovereignty and access controls
- Managing chain-of-custody in the cloud
- **Case Study**: Non-compliance fines from poor logging practices

Module 8: Building a Forensic-Ready Cloud Security Strategy

- Architecting security-first cloud-native deployments
- Aligning business and security objectives
- Playbook development for forensic scenarios
- Training teams for incident response
- Continuous improvement and validation techniques

- **Case Study**: Successful containment and legal defense post-breach

Training Methodology

- Interactive lectures using real-world cloud platforms
- Hands-on labs with Kubernetes, Docker, CI/CD, and SIEM
- Threat simulations and incident response drills
- Case study walkthroughs and group discussions
- Quizzes and mini-projects to reinforce learning
- Certification of completion and digital badge

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
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

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

Register Online Now

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