Cloud Defense Engineering and Automation 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

The exponential growth of multi-cloud environments has created a critical gap in security expertise, demanding a shift from manual defenses to Cloud-Native Defense Engineering and Hyperautomation. Cloud Defense Engineering and Automation Training Course is meticulously designed to equip security professionals, DevOps engineers, and architects with the highly sought-after skills to build, deploy, and manage an integrated, automated, and proactive cloud security posture. You?ÇÖll master Infrastructure as Code (IaC) security principles, implement DevSecOps pipelines, and leverage cutting-edge tools for Security Orchestration, Automation, and Response. By focusing on AI-Driven Threat Detection, Cloud Security Posture Management, and Zero Trust Architecture, this program transforms participants into elite Cloud Defense Engineers capable of defending against modern, automated cyber threats and ensuring continuous, automated Compliance-as-Code across major cloud platforms.

In today?ÇÖs volatile threat landscape, traditional security models are obsolete. The modern imperative is to implement shift-left security and achieve continuous security validation through engineering excellence. This training delivers the tactical, hands-on experience needed to integrate security controls directly into the CI/CD pipeline, minimizing human error and maximizing protection. Participants will learn to automate everything from vulnerability management to incident response, establishing a resilient security mesh architecture. Graduate with a skillset that drives risk reduction, ensures data sovereignty, and positions you as a leader in securing the future of enterprise cloud computing.

Programme Curriculum

Cloud Defense Engineering and Automation Training Course

Introduction

The exponential growth of multi-cloud environments has created a critical gap in security expertise, demanding a shift from manual defenses to Cloud-Native Defense Engineering and Hyperautomation. Cloud Defense Engineering and Automation Training Course is meticulously designed to equip security professionals, DevOps engineers, and architects with the highly sought-after skills to build, deploy, and manage an integrated, automated, and proactive cloud security posture. You?ÇÖll master Infrastructure as Code (IaC) security principles, implement DevSecOps pipelines, and leverage cutting-edge tools for Security Orchestration, Automation, and Response. By focusing on AI-Driven Threat Detection, Cloud Security Posture Management, and Zero Trust Architecture, this program transforms participants into elite Cloud Defense Engineers capable of defending against modern, automated cyber threats and ensuring continuous, automated Compliance-as-Code across major cloud platforms.

In today?ÇÖs volatile threat landscape, traditional security models are obsolete. The modern imperative is to implement shift-left security and achieve continuous security validation through engineering excellence. This training delivers the tactical, hands-on experience needed to integrate security controls directly into the CI/CD pipeline, minimizing human error and maximizing protection. Participants will learn to automate everything from vulnerability management to incident response, establishing a resilient security mesh architecture. Graduate with a skillset that drives risk reduction, ensures data sovereignty, and positions you as a leader in securing the future of enterprise cloud computing.

Course Duration

10 days

Course Objectives

Upon completion, participants will be able to:

1. Engineer and deploy secure Cloud-Native Architectures across hybrid and multi-cloud environments.
2. Implement Policy-as-Code (PaC) for automated governance and Cloud Security Posture Management (CSPM).
3. Design and operationalize a robust Zero Trust Architecture (ZTA), minimizing implicit trust.
4. Automate threat modeling and secure Infrastructure as Code (IaC) using tools like Terraform and CloudFormation.
5. Integrate DevSecOps practices to achieve shift-left security in CI/CD pipelines.
6. Develop and implement Security Orchestration, Automation, and Response (SOAR) playbooks for incident handling.
7. Leverage AI/ML for real-time anomaly detection and proactive threat hunting.
8. Secure Container Security and Serverless Computing workloads
9. Conduct and automate Vulnerability Management and Continuous Security Validation (CSV).
10. Master Cloud Identity and Access Management (IAM) and privileged access control with automated reviews.
11. Implement Data Security Posture Management (DSPM) and Data Loss Prevention (DLP) controls.
12. Establish an advanced Cloud Detection and Response (CDR) capability using native services
13. Drive and prove Compliance-as-Code for regulatory standards.

Target Audience

1. Cloud Security Engineers
2. DevSecOps Engineers
3. Security Architects
4. Security Operations Center (SOC) Analysts (Level II/III)

5. Cloud Architects and Cloud Consultants
6. SREs (Site Reliability Engineers) with a security focus
7. Cybersecurity Analysts and Threat Hunters
8. IT/Security Compliance and Audit Professionals

Course Modules

Module 1: Foundations of Cloud Defense and Zero Trust

- Cloud Threat Landscape.
- Shared Responsibility Model.
- Cloud Security Architecture.
- Zero Trust Architecture (ZTA).
- Case Study: Large Financial Institution's ZTA Migration.

Module 2: Automated Cloud Security Posture Management (CSPM)

- Writing and enforcing security guardrails using OPA and Cloud-Native PaC tools.
- Continuous Compliance Scanning.
- Automated Remediation Workflows.
- CIS Benchmarks & Custom Policies.
- Case Study: Global Retailer?ÇÖs Real-Time Misconfiguration Fix.

Module 3: Securing Infrastructure as Code (IaC)

- IaC Security Best Practices.
- Shift-Left IaC Scanning.
- Secrets Management Automation.
- Drift Detection and Remediation.
- Case Study: Tech Unicorn?ÇÖs Secure IaC Pipeline.

Module 4: Cloud Identity and Access Management (IAM) Automation

- Least Privilege Automation.
- Just-in-Time (JIT) Access.
- Federated Identity and SSO.
- Credential Rotation and Key Management.
- Case Study: Telecom Giant's Automated IAM Review.

Module 5: DevSecOps Integration and Pipeline Security

- CI/CD Pipeline Hardening.
- Software Composition Analysis.
- Dynamic Application Security Testing.
- Security Gates and Quality Checks.
- Case Study: E-Commerce Platform's DevSecOps Transformation

Module 6: Container and Serverless Security Automation

- Container Image Scanning
- Kubernetes Security Automation.
- Serverless Function Security.

- Container Runtime Defense.
- Case Study: Fintech Startup's Kubernetes Defense.

Module 7: Cloud Detection and Response (CDR)

- Log Ingestion and Normalization.
- Detection-as-Code
- Threat Hunting Automation
- Tuning and Alert Reduction
- Case Study: Managed Security Provider?ÇÖs AI-Driven SOC.

Module 8: Security Orchestration, Automation, and Response (SOAR)

- SOAR Playbook Development.
- Integration with Cloud APIs.
- Human-in-the-Loop Automation.
- Metrics and ROI of Automation.
- Case Study: Enterprise Phishing Response Automation

Module 9: Data Security and Encryption Automation

- Automated Data Classification.
- Encryption-in-Transit/at-Rest.
- Key Management Service (KMS) Automation.
- Data Loss Prevention (DLP) Policies.
- Case Study: Healthcare Provider?ÇÖs Automated Data Sovereignty.

Module 10: Advanced Network and Perimeter Automation

- Automated Network Segmentation.
- Web Application Firewall (WAF) Automation.
- DDoS Protection Automation.
- VPC Flow Log Analysis.
- Case Study: Global SaaS Company?ÇÖs WAF Defense

Module 11: Security Analytics and AI/ML for Defense

- AI-Driven Anomaly Detection
- Generative AI for Security.
- Security Data Lake Architecture.
- Predictive Security Analytics.
- Case Study: AI-Powered Threat Prioritization.

Module 12: Cloud Vulnerability Management Automation

- Continuous Vulnerability Scanning.
- Automated Patch Management
- Risk-Based Prioritization.
- Vulnerability Remediation Tracking.
- Case Study: Logistics Firm?ÇÖs Automated Patching.

Module 13: Cloud Security Compliance and Audit Automation

- Compliance-as-Code Frameworks
- Automated Evidence Collection.
- Reporting and Dashboarding.
- Cross-Cloud Compliance Harmonization.
- Case Study: Regulated Industry's Continuous Audit.

Module 14: Disaster Recovery (DR) and Business Continuity Automation

- Automated Backup and Restore Policies.
- Immutable Infrastructure for DR.
- Automated Failover and Failback Testing.
- Ransomware Defense Automation.
- Case Study: Insurance Company?ÇÖs One-Click DR.

Module 15: Future-Proofing Cloud Defense: Emerging Tech

- Sovereign Cloud Security.
- Quantum-Resistant Cryptography.
- Automated Supply Chain Security.
- Cloud-Native Observability.
- Case Study: Defense Contractor's Supply Chain Hardening.

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	04 Dec 2026	Online	$2,000
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

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

Register Online Now

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