Cloud Native Security and DevSecOps Automation 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

In today?ÇÖs accelerated development landscape, the integration of Cloud Native Security and DevSecOps Automation is no longer optional it is a critical necessity. Cloud Native Security and DevSecOps Automation Training Course is engineered to empower modern security, development, and operations professionals to effectively implement a Shift-Left Security strategy within dynamic, Kubernetes-centric environments. Participants will master the art of Security as Code, leveraging Infrastructure as Code (IaC) scanning, automated vulnerability detection, and Continuous Compliance to secure the entire Software Supply Chain. By focusing on AI-Driven Security Automation and Zero Trust Architecture principles, the program provides the practical, hands-on skills required to build resilient, compliant, and rapidly-deployable cloud-native applications, transitioning security from a bottleneck to a core value-driver in the CI/CD pipeline.

This comprehensive training emphasizes automated security gates and runtime protection for microservices and containers, addressing the unique complexities of multi-cloud architectures. We dive deep into practical applications of tools for Secret Management, Container Security, and Cloud Security Posture Management (CSPM). Graduates will be prepared to architect, deploy, and maintain robust, high-velocity delivery pipelines that intrinsically embed security controls. By mastering DevSecOps principles and cutting-edge Cloud-Native Application Protection Platforms (CNAPP), you will transform your organization?ÇÖs security culture into one of shared responsibility and proactive risk mitigation, ensuring speed and safety go hand-in-hand.

Programme Curriculum

Cloud Native Security and DevSecOps Automation Training Course

Introduction

In today?ÇÖs accelerated development landscape, the integration of Cloud Native Security and DevSecOps Automation is no longer optional it is a critical necessity. Cloud Native Security and DevSecOps Automation Training Course is engineered to empower modern security, development, and operations professionals to effectively implement a Shift-Left Security strategy within dynamic, Kubernetes-centric environments. Participants will master the art of Security as Code, leveraging Infrastructure as Code (IaC) scanning, automated vulnerability detection, and Continuous Compliance to secure the entire Software Supply Chain. By focusing on AI-Driven Security Automation and Zero Trust Architecture principles, the program provides the practical, hands-on skills required to build resilient, compliant, and rapidly-deployable cloud-native applications, transitioning security from a bottleneck to a core value-driver in the CI/CD pipeline.

This comprehensive training emphasizes automated security gates and runtime protection for microservices and containers, addressing the unique complexities of multi-cloud architectures. We dive deep into practical applications of tools for Secret Management, Container Security, and Cloud Security Posture Management (CSPM). Graduates will be prepared to architect, deploy, and maintain robust, high-velocity delivery pipelines that intrinsically embed security controls. By mastering DevSecOps principles and cutting-edge Cloud-Native Application Protection Platforms (CNAPP), you will transform your organization?ÇÖs security culture into one of shared responsibility and proactive risk mitigation, ensuring speed and safety go hand-in-hand.

Course Duration

5 days

Course Objectives

1. Implement a Shift-Left Security strategy by integrating automated security controls from initial commit.
2. Master Security as Code principles using policy engines and version-controlled security configurations.
3. Secure Infrastructure as Code (IaC) templates against misconfigurations using automated scanning tools like Checkov and Terrascan.
4. Apply advanced Container Security best practices, including image scanning, registry protection, and runtime enforcement.
5. Architect and deploy Zero Trust Architecture principles for microservices using dynamic authorization and service mesh technologies.
6. Automate Secret Management within CI/CD pipelines and cloud-native environments using tools like HashiCorp Vault or AWS Secrets Manager.
7. Integrate SAST, DAST, and SCA tools into the CI/CD pipeline for continuous vulnerability and dependency management.
8. Enforce Continuous Compliance by implementing Policy as Code for regulatory standards like GDPR or SOC 2.
9. Configure and secure Kubernetes Clusters and workloads using native controls like RBAC, Network Policies, and Admission Controllers.
10. Implement Cloud Security Posture Management (CSPM) and Cloud Workload Protection (CWPP) for multi-cloud environments.
11. Perform automated Threat Modeling and Risk Assessment at the design and iteration stages of the SDLC.
12. Establish robust Runtime Security monitoring and logging with tools like Prometheus and Grafana for active threat detection and response.
13. Leverage AI-Driven Security Automation to enable intelligent threat detection and autonomous remediation workflows.

Target Audience

1. DevOps Engineers and SREs
2. Application Security Professionals and Security Analysts
3. Cloud Architects and Cloud Engineers
4. Software Developers and Engineers
5. DevSecOps Engineers/Specialists
6. Security Consultants and Auditors
7. Technical Project Managers
8. IT Leaders and C-Level Executives

Course Modules

Module 1: DevSecOps Culture, Principles, and Automation Foundations

- DevSecOps Culture and Shared Responsibility
- The "Shift Left" Paradigm.
- CI/CD Pipeline Security Hardening.
- Introducing Security as Code.
- Vulnerability and Risk Management in the Pipeline.
- Case Study: Target Breach Post-Mortem and DevOps Response.

Module 2: Cloud Native Security: Containers and Kubernetes

- Container Security Deep Dive.
- Kubernetes Cluster Hardening
- Kubernetes Workload Security.
- Network Segmentation with Kubernetes Network Policies.
- Runtime Security for Containers.
- Case Study: The Tesla Kubernetes Cluster Compromise.

Module 3: Infrastructure as Code (IaC) and Policy as Code (PaC)

- Securing IaC.
- Automated IaC Scanning Tools.
- Introduction to Policy as Code
- Continuous Compliance Enforcement.
- Secrets Management with IaC.
- Case Study: Misconfigured S3 Bucket Remediation with IaC.

Module 4: Application Security Testing Automation (SAST/DAST/SCA)

- Static Application Security Testing (SAST) Automation.
- Dynamic Application Security Testing (DAST) in Staging.
- Software Composition Analysis (SCA) for Supply Chain Integrity.
- Interactive Application Security Testing (IAST) and RASP.
- Security Orchestration, Automation, and Response.
- Case Study: Log4Shell Vulnerability Response.

Module 5: Advanced Secret and Identity Management

- Zero Trust Identity and Access Management.
- Centralized Secrets Management
- Securing Service-to-Service Communication.

- Cloud Infrastructure Entitlement Management.
- Workload Identity Federation.
- Case Study: Hardcoded Credentials to Vault Integration.

Module 6: Runtime Security, Monitoring, and Observability

- Cloud Security Posture Management
- Cloud Workload Protection Platform.
- Security Monitoring and Logging.
- Automated Incident Response
- Threat Hunting in Cloud Native Environments.
- Case Study: Real-time Alert and Response.

Module 7: Serverless and API Security

- Serverless Function Security.
- API Gateway Protection.
- The OWASP API Security Top 10.
- Infrastructure for Serverless.
- API Security Testing Automation.
- Case Study: Broken Object Level Authorization (BOLA) in an API.

Module 8: Advanced Topics: Zero Trust, AI, and Future Trends

- Deep Dive into Zero Trust Architecture.
- Adopting Cloud-Native Application Protection Platforms.
- AI/ML for DevSecOps.
- Chaos Engineering for Security Resilience.
- The Future of DevSecOps.
- Case Study: Implementing Micro-segmentation with ZTA.

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
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
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