Serverless Computing Security and Best Practices 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 Serverless Computing paradigm has revolutionized cloud development, offering unprecedented scalability, agility, and cost-efficiency by abstracting away server management. However, this shift from traditional servers to Functions as a Service and event-driven architectures introduces unique, complex security challenges that traditional perimeter defenses fail to address. Organizations are struggling with the implications of the Shared Responsibility Model, where security is tightly tied to function configurations, IAM permissions, and event-data validation. Mastery of this new security landscape is critical for protecting sensitive data and maintaining DevSecOps velocity.

Serverless Computing Security and Best Practices Training Course will provide developers, security professionals, and architects with the deep, practical knowledge required to secure modern cloud-native applications. We move beyond theory to focus on actionable best practices for mitigating top threats like over-privileged functions, insecure configuration, and event injection attacks. By mastering Least Privilege Access Control (LPAC), runtime protection, and Infrastructure as Code (IaC) security, participants will learn to build, test, and deploy resilient serverless workloads that comply with enterprise governance and compliance standards, ensuring a robust security posture from code to cloud.

Programme Curriculum

Serverless Computing Security and Best Practices Training Course

Introduction

The Serverless Computing paradigm has revolutionized cloud development, offering unprecedented scalability, agility, and cost-efficiency by abstracting away server management. However, this shift from traditional servers to Functions as a Service and event-driven architectures introduces unique, complex security challenges that traditional perimeter defenses fail to address. Organizations are struggling with the implications of the Shared

Responsibility Model, where security is tightly tied to function configurations, IAM permissions, and event-data validation. Mastery of this new security landscape is critical for protecting sensitive data and maintaining DevSecOps velocity.

Serverless Computing Security and Best Practices Training Course will provide developers, security professionals, and architects with the deep, practical knowledge required to secure modern cloud-native applications. We move beyond theory to focus on actionable best practices for mitigating top threats like over-privileged functions, insecure configuration, and event injection attacks. By mastering Least Privilege Access Control (LPAC), runtime protection, and Infrastructure as Code (IaC) security, participants will learn to build, test, and deploy resilient serverless workloads that comply with enterprise governance and compliance standards, ensuring a robust security posture from code to cloud.

Course Duration

10 days

Course Objectives

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

1. Design and implement robust, secure serverless architectures across major cloud providers
2. Master AWS IAM and Azure RBAC to define granular, minimum-required permissions for every function.
3. Implement stringent input validation and output sanitization to protect against Event Injection Attacks.
4. Secure the application code lifecycle, including dependency scanning and managing third-party library vulnerabilities.
5. Implement data encryption and secure secrets management for data at rest and in transit between serverless components.
6. Identify and remediate misconfigurations in API Gateways, Triggers, and other event sources using security policy checks.
7. Deploy advanced tools and techniques for runtime defense and anomaly detection within ephemeral function environments.
8. Utilize cloud-specific services like AWS WAF, Azure Sentinel, and CloudTrail for enhanced serverless protection.
9. Integrate security testing and Infrastructure as Code (IaC) scanning into the CI/CD pipeline.
10. Configure comprehensive logging, tracing, and security alerting for real-time threat detection and incident response.
11. Understand the critical differences in the Shared Responsibility Model and security controls between major FaaS platforms.
12. Employ rate limiting and concurrency controls to prevent resource exhaustion attacks in serverless environments.
13. Develop organizational policies and standards for continuous serverless security posture management.

Target Audience

1. Cloud Security Engineers
2. DevSecOps Practitioners
3. Serverless/Cloud Developers
4. Solution/Cloud Architects
5. Security Auditors and Compliance Managers
6. SREs (Site Reliability Engineers)
7. Technical Team Leads

8. Security Operations Center (SOC) Analysts

Course Modules

1. Introduction to Serverless Security Fundamentals

- FaaS, BaaS, and Event-Driven Architecture.
- The Shared Responsibility Model in a Serverless Context.
- The Serverless Attack Surface and the OWASP Serverless Top 10.
- Ephemeral Containers, Cold Start Risks, Decentralization.
- Security Governance and Compliance Requirements
- Case Study: Analysis of the Capital One Breach and how a misconfigured WAF/IAM role on a serverless component exposed critical data.

2. Identity and Access Management Best Practices

- Principle of Least Privilege Access Control for functions.
- Defining and scoping IAM roles and policies for individual functions.
- Preventing Over-privileged Functions and Groundhog Day Attacks.
- Using managed policies and inline policies for security.
- Federated identity and using external identity providers with serverless.
- Case Study: Auditing and remediation of a major retail application where a Lambda function had s3:* full access, far beyond the s3:GetObject it required.

3. Securing the Serverless Function Code

- Input Validation, Output Sanitization, and Error Handling.
- Managing and Auditing Third-Party Dependencies and open-source risk.
- Preventing Code and Event-Data Injection Flaws.
- Static Application Security Testing in the build pipeline.
- Handling runtime environments and container image hardening.
- Case Study: Exploitation of an outdated, vulnerable NPM library used in an Azure Function that led to remote code execution.

4. Secure Secrets and Configuration Management

- The dangers of hardcoding secrets in environment variables.
- Integrating with Cloud Key Management Services.
- Securely passing configuration data to functions.
- Best practices for rotating and revoking credentials.
- Securing database and API credentials used by functions.
- Case Study: Review of a financial startup's incident where plain-text database credentials were exposed in a Git repository connected to a deployment pipeline.

5. API Gateway and Event Source Security

- Securing the API Gateway front-end.
- Validating and securing event sources
- Implementing Custom Authorizers and JWT validation.
- Mitigating Denial-of-Service and Resource Exhaustion attacks.
- Applying network controls to serverless components.

- Case Study: Demonstrating a successful Event Injection attack on a function triggered by an S3 bucket notification with malicious metadata.

6. Security Testing and DevSecOps Integration

- Integrating security into the CI/CD Pipeline.
- Infrastructure as Code security scanning.
- Dynamic Application Security Testing for serverless APIs.
- Fuzz testing and chaos engineering for resilience.
- Automated policy enforcement and drift detection.
- Case Study: Setting up a fully automated pipeline that fails a deployment if an IAM role grants an overly permissive policy using a Cloud Security Posture Management tool.

7. Serverless Logging, Monitoring, and Observability

- Implementing comprehensive security logging
- Setting up real-time alerting for suspicious activity
- Distributed tracing and log correlation across microservices.
- Using specialized Serverless Runtime Protection tools for anomaly detection.
- Building a centralized Security Information and Event Management view.
- Case Study: Using a log-based metric filter and an alarm to detect and alert on unauthorized API calls or function environment tampering within milliseconds.

8. Data Security and Encryption in Serverless

- Enforcing encryption for data at rest
- Using TLS/SSL for data in transit and securing inter-function communication.
- Data classification and implementing data loss prevention strategies.
- Securely processing and handling personally identifiable information.
- Using secure data patterns
- Case Study: The accidental exposure of PII due to an unencrypted S3 bucket that was an event source, and the fix using S3 bucket policies and KMS.

9. Advanced Cloud-Specific Serverless Security

- Securing AWS Lambda and its integrations
- Configuring VPC Lambda and securing network access.
- Using Lambda Layers for shared, secure dependencies.
- Advanced IAM Policy conditions and fine-tuning.
- Security implications of Step Functions and Serverless Workflows.
- Case Study: Hardening a serverless data processing pipeline orchestrated by Step Functions by applying least-privilege roles to each individual step/task.

10. Advanced Cloud-Specific Serverless Security

- Securing Azure Functions and its triggers
- Using Virtual Network Integration and Private Endpoints for network isolation.
- Leveraging Managed Identity for secure access to Azure services.
- Integrating with Azure Security Center/Defender for Cloud.
- Security implications of Azure Logic Apps and Durable Functions.

- Case Study: Protecting an Azure Function that processes financial transactions by using a VNet to restrict inbound traffic only to trusted cloud resources.

11. Containerized Serverless

- Security considerations for running containers on a serverless platform.
- Container image security and using minimal base images.
- Scanning container images for vulnerabilities
- Implementing runtime security controls for containers.
- Security Context and its role in containerized serverless.
- Case Study: Securing a legacy application refactored into a containerized Fargate service by implementing CIS Benchmarks for container configuration.

12. Security Policy and Compliance Automation

- Defining and enforcing Security as Code policies
- Automating compliance checks against industry benchmarks
- Continuous Cloud Security Posture Management
- Handling security exceptions and risk acceptance processes.
- Auditing and reporting on serverless security posture.
- Case Study: Using a CSPM solution to automatically detect and alert on any serverless component that is configured with a public-facing unauthenticated endpoint.

13. Incident Response and Remediation

- Developing a Serverless Incident Response Plan.
- Steps for isolating a compromised serverless function.
- Forensics in an ephemeral environment
- Post-incident analysis and rapid remediation strategies.
- The role of WAF and API Gateway in threat mitigation.
- Case Study: Simulating an incident where a function is compromised via a zero-day dependency and executing the full isolate, analyze, and redeploy process.

14. Financial/Cost Security

- Security implications of the Pay-per-Execution Model.
- Protecting against billing attacks and denial of wallet.
- Using concurrency limits and throttling to control costs and risks.
- Monitoring usage anomalies as a security indicator.
- Cost optimization techniques that maintain a strong security posture.
- Case Study: Analyzing a large utility bill spike caused by a recursive function bug.

15. The Future of Serverless Security

- The rise of Serverless AI/ML security challenges.
- Security in the context of Multi-Cloud/Hybrid Serverless deployments.
- Emerging runtime security technologies and trends.
- Best practices for securing serverless databases
- Securing Edge Computing and serverless functions at the edge.
- Case Study: Discussing the security architecture for a new multi-cloud serverless application using a centralized secrets manager and identity federation across cloud providers.

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

Start Date	End Date	Location	Price
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