Serverless Security on AWS Lambda and Azure Functions 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 proliferation of serverless computing has revolutionized application development, offering unprecedented scale and agility. However, the architectural shift moving away from traditional network perimeters has introduced a new, critical security frontier. Serverless Security on AWS Lambda and Azure Functions Training Course focuses on equipping security engineers, DevSecOps professionals, and cloud developers with the advanced, vendor-neutral and multi-cloud expertise necessary to secure Function-as-a-Service (FaaS) applications. We move beyond generic cloud security principles to dive deep into identity-driven micro-perimeters, runtime protection, and the automated defense of code and configurations for the two dominant FaaS platforms.

This intensive course zeroes in on current threats like overprivileged IAM roles, supply chain attacks via poisoned dependencies, and event-data injection. Participants will learn to implement Zero Trust principles at the function level, utilizing native cloud services such as AWS IAM, Secrets Manager, CloudTrail, Azure AD, and Azure Key Vault. By mastering Infrastructure as Code (IaC) security with tools like Terraform and CloudFormation, and enforcing security guardrails in the CI/CD pipeline, attendees will gain the practical skills to build and maintain secure-by-design serverless applications, ensuring compliance and minimizing the attack surface in high-velocity development environments.

Programme Curriculum

Serverless Security on AWS Lambda and Azure Functions Training Course

Introduction

The proliferation of serverless computing has revolutionized application development, offering unprecedented scale and agility. However, the architectural shift moving away from traditional network perimeters has introduced a new, critical security frontier. Serverless Security on AWS Lambda and Azure Functions Training

Course focuses on equipping security engineers, DevSecOps professionals, and cloud developers with the advanced, vendor-neutral and multi-cloud expertise necessary to secure Function-as-a-Service (FaaS) applications. We move beyond generic cloud security principles to dive deep into identity-driven micro-perimeters, runtime protection, and the automated defense of code and configurations for the two dominant FaaS platforms.

This intensive course zeroes in on current threats like overprivileged IAM roles, supply chain attacks via poisoned dependencies, and event-data injection. Participants will learn to implement Zero Trust principles at the function level, utilizing native cloud services such as AWS IAM, Secrets Manager, CloudTrail, Azure AD, and Azure Key Vault. By mastering Infrastructure as Code (IaC) security with tools like Terraform and CloudFormation, and enforcing security guardrails in the CI/CD pipeline, attendees will gain the practical skills to build and maintain secure-by-design serverless applications, ensuring compliance and minimizing the attack surface in high-velocity development environments.

Course Duration

5 days

Course Objectives

1. Master the Serverless Shared Responsibility Model across AWS and Azure, clarifying customer versus provider security duties.
2. Implement Least Privilege Access Control using AWS IAM policies and Azure RBAC for FaaS functions and associated resources.
3. Design and deploy secure secrets management using AWS Secrets Manager and Azure Key Vault to eliminate plaintext credentials.
4. Mitigate Supply Chain Attacks by scanning and enforcing policies on third-party libraries and dependencies.
5. Prevent Function Event-Data Injection via rigorous input validation and context-aware sanitization.
6. Configure and secure API gateways including throttling, WAF, and strong authentication.
7. Establish comprehensive Inadequate Function Monitoring & Logging controls using CloudWatch, CloudTrail, and Azure Monitor/Sentinel.
8. Implement runtime protection and threat detection strategies for ephemeral execution environments.
9. Apply Security-as-Code principles to secure Infrastructure as Code templates
10. Harden the serverless deployment pipeline to integrate static and dynamic analysis
11. Secure data at rest and in transit using service-specific encryption techniques
12. Develop an effective Serverless Incident Response plan, focusing on rapid containment and forensic analysis in ephemeral environments.
13. Leverage Cloud Security Posture Management tools for continuous audit and compliance with standards like OWASP Serverless Top 10.

Target Audience

1. Cloud Security Engineers
2. DevSecOps Engineers / Application Security (AppSec) Engineers
3. Cloud Architects / Serverless Architects
4. AWS & Azure Developers / Full-Stack Developers building serverless applications
5. Security Operations Center (SOC) Analysts focused on cloud environments
6. IT Auditors / Compliance Officers needing platform-specific security knowledge
7. SRE (Site Reliability Engineers) / Platform Engineers managing serverless deployments

8. Technical Leaders / Engineering Managers

Course Modules

Module 1: Serverless Security Fundamentals & Shared Responsibility

- Serverless Architecture, Ephemeral Execution, and Event-Driven Attack Surface.
- Shared Responsibility Deep Dive.
- Risk & Threat Landscape.
- Regulatory Compliance
- Introduction to IaC Security.
- Case Study: The consequences of the Capital One Breach (2019) demonstrating how a misconfigured WAF/API Gateway led to an SSRF vulnerability exploiting a sensitive Lambda role.

Module 2: Identity, Access, and Least Privilege (IAM/RBAC)

- AWS Lambda IAM.
- Azure Functions RBAC.
- Principle of Least Privilege (PoLP) Enforcement.
- Federated Identity
- Securing Temporary Credentials.
- Case Study: Simulating an attacker exploiting an overly permissive IAM role to perform resource enumeration across an AWS account.

Module 3: Secret and Configuration Management

- Secrets Storage Best Practices.
- AWS Secrets Manager Integration.
- Azure Key Vault Integration.
- Hardening Environment Variables.
- Credential Rotation & Auditing.
- Case Study: The risk of plaintext secrets exposure via logs after a function crash or verbose logging incident.

Module 4: Secure Code and Dependency Management

- Function Event-Data Injection.
- Serverless Supply Chain Security.
- Code Integrity & Signing.
- SAST Integration.
- Function Isolation
- Case Study: Analyzing a dependency confusion attack where a malicious package was inadvertently pulled, leading to data exfiltration via an ephemeral function.

Module 5: Network and API Security (API Gateways and VPC)

- API Gateway Hardening.
- Azure API Management Security.
- WAF Integration.
- VPC Integration.
- Service Endpoints.

- Case Study: Investigating a DDoS attack scenario and the effectiveness of API Gateway/API Management rate limiting and WAF rules in prevention.

Module 6: Monitoring, Logging, and Observability

- Centralized Logging.
- Real-time Threat Detection.
- Audit Logging.
- Data Exfiltration Monitoring.
- Serverless-Aware SIEM Integration.
- Case Study: Detecting a Groundhog Day Attack a series of rapid, low-volume, successful breaches that exploit ephemeral logging gaps.

Module 7: Infrastructure as Code (IaC) and DevSecOps Automation

- Security Guardrails.
- IaC Security Scanning.
- Shift-Left Security.
- Pipeline Hardening.
- Configuration Drift Management.
- Case Study: Applying a Cloud Security Posture Management tool to identify and automatically remediate non-compliant function configurations across multiple environments.

Module 8: Data Protection and Incident Response

- Data Encryption
- Securing Data in Transit.
- Forensics in Serverless.
- Containment and Eradication.
- Response Playbooks
- Case Study: A full-cycle Incident Response walkthrough following a database credentials leak from a temporary file in a Lambda execution environment.

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