Training Course on Serverless Forensics and Investigation in the Cloud

Professional Development Training Course Outline

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

Course Introduction

With the rapid adoption of cloud-native architectures, serverless computing has revolutionized how organizations build and deploy applications. However, this evolution also introduces complex challenges for digital investigators and incident response teams. Training Course on Serverless Forensics and Investigation in the Cloud equips IT professionals, security analysts, and digital forensics teams with hands-on skills and best practices to effectively manage security incidents, perform forensic analysis, and ensure compliance in modern serverless environments.

Designed for the modern cloud-native threat landscape, this course delivers high-impact, keyword-rich insights into AWS Lambda, Azure Functions, Google Cloud Functions, serverless attack vectors, forensic artifacts, and automation. Attendees will master cutting-edge forensic techniques, learn real-world incident response strategies, and enhance their expertise in cloud-native threat hunting, event tracking, and compliance-ready forensic documentation.

Programme Curriculum

Training Course on Serverless Forensics and Investigation in the Cloud

Introduction

With the rapid adoption of cloud-native architectures, serverless computing has revolutionized how organizations build and deploy applications. However, this evolution also introduces complex challenges for digital investigators and incident response teams. Training Course on Serverless Forensics and Investigation in the Cloud equips IT professionals, security analysts, and digital forensics teams with hands-on skills and best practices to effectively manage security incidents, perform forensic analysis, and ensure compliance in modern serverless environments.

Designed for the modern cloud-native threat landscape, this course delivers high-impact, keyword-rich insights into AWS Lambda, Azure Functions, Google Cloud Functions, serverless attack vectors, forensic artifacts, and automation. Attendees will master cutting-edge forensic techniques, learn real-world incident response strategies, and enhance their expertise in

cloud-native threat hunting, event tracking, and compliance-ready forensic documentation.

Course Objectives

1. Understand the architecture of serverless environments and forensic limitations.
2. Identify digital evidence across AWS Lambda, Azure Functions, and Google Cloud Functions.
3. Utilize cloud-native logs and event data for forensic investigations.
4. Learn incident response workflows for serverless environments.
5. Master event-driven security monitoring and alerts.
6. Develop skills in automated evidence collection using cloud tools.
7. Recognize malicious behavior patterns in ephemeral environments.
8. Apply threat intelligence to enrich forensic findings.
9. Perform root cause analysis in stateless and short-lived execution contexts.
10. Implement chain-of-custody protocols in a cloud-native way.
11. Use open-source forensics tools compatible with serverless platforms.
12. Map forensic results to compliance frameworks like NIST, GDPR, and ISO 27001.
13. Prepare forensic reports and dashboards for audit and executive reviews.

Target Audience

1. Cloud Security Engineers
2. Digital Forensics Investigators
3. Incident Response Teams
4. Cybersecurity Analysts
5. Cloud Infrastructure Architects
6. Compliance and Audit Professionals
7. DevSecOps Engineers
8. IT Managers and Risk Officers

Course Duration: 5 days

Course Modules

Module 1: Introduction to Serverless Forensics

- Definition and fundamentals of serverless architecture
- Unique forensic challenges in serverless ecosystems
- Understanding cloud-native execution models
- Introduction to relevant cloud platforms
- Importance of forensic readiness
- **Case Study**: AWS Lambda compromise and evidence collection

Module 2: Logging and Monitoring in Serverless

- Collecting logs from AWS CloudWatch, Azure Monitor, and GCP Logs
- Parsing and correlating ephemeral data sources
- Event-driven forensic investigation
- Integrating SIEM with serverless telemetry
- Setting up real-time alerts for suspicious activity
- **Case Study**: Unauthorized access through misconfigured log policies

Module 3: Threat Detection in Stateless Environments

- Common attack vectors targeting serverless
- Identifying malicious payloads and injections

- Detecting lateral movement and privilege escalation
- Use of behavioral analytics and anomaly detection
- Mitigating threats using IAM best practices
- **Case Study**: Detection of privilege escalation using misused roles

Module 4: Evidence Acquisition and Preservation

- Best practices for evidence handling in cloud
- Automating evidence collection using Lambda and Cloud Functions
- Understanding metadata preservation in cloud environments
- Ensuring data integrity and hash verification
- Storing evidence securely and compliantly
- **Case Study**: Automated snapshot collection following a breach

Module 5: Forensic Analysis of Serverless Functions

- Investigating code execution and runtime behavior
- Identifying suspicious imports and outbound connections
- Analyzing logs for IOCs (Indicators of Compromise)
- Isolating affected components in microservice environments
- Using open-source tools for analysis
- **Case Study**: Code injection via event trigger in Azure Function

Module 6: Incident Response Planning and Execution

- Incident response lifecycle in cloud-native environments
- Role of SOAR (Security Orchestration, Automation, Response)
- Coordinating with cloud providers during IR
- Documentation and timeline reconstruction
- Post-incident lessons learned and hardening strategies
- **Case Study**: Coordinated multi-function attack response in GCP

Module 7: Compliance and Regulatory Considerations

- GDPR, HIPAA, PCI DSS implications in serverless environments
- Implementing audit trails and data residency controls
- Mapping forensic practices to NIST and ISO standards
- Maintaining privacy during investigations
- Preparing compliance-ready reports and dashboards
- **Case Study**: Regulatory breach investigation with NIST alignment

Module 8: Future of Serverless Forensics

- Emerging trends: eBPF, extended Berkeley Packet Filters
- Use of AI and ML in forensic analysis
- Zero Trust architectures and impact on forensics
- Policy-as-code and automated compliance
- Skills for the next-gen forensic analyst
- **Case Study**: Predictive breach detection using ML in Lambda functions

Training Methodology

- Instructor-led presentations with live demonstrations
- Hands-on lab exercises using AWS, Azure, and GCP environments
- Real-world case study walkthroughs
- Group-based incident simulation exercises

- Q&A and interactive breakout sessions
- Digital resource packs and post-training support

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.com 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
07 Sep 2026	11 Sep 2026	Physical	$1,500
14 Sep 2026	18 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$1,500
28 Sep 2026	02 Oct 2026	Physical	$1,500
05 Oct 2026	09 Oct 2026	Physical	$1,500
12 Oct 2026	16 Oct 2026	Physical	$1,500
19 Oct 2026	23 Oct 2026	Physical	$1,500
26 Oct 2026	30 Oct 2026	Physical	$1,500

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

Register Online Now

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