Training Course on Cloud Log Analysis and Correlation for Investigations

Professional Development Training Course Outline

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

Course Introduction

In today’s cloud-driven digital era, cybersecurity professionals must evolve beyond traditional methods to tackle cloud-native threats. Training Course on Cloud Log Analysis and Correlation for Investigations offers a comprehensive, hands-on approach to understanding how log data from cloud platforms can be analyzed and correlated for effective forensic investigations. With the exponential growth of SaaS, IaaS, and hybrid infrastructures, the ability to rapidly identify suspicious behaviors, detect insider threats, and trace unauthorized access through cloud logs is crucial for securing sensitive assets and maintaining compliance.

This course empowers learners with cutting-edge tools and techniques in SIEM integration, multi-cloud investigation, and log correlation engines to enhance incident response and threat hunting capabilities. Through real-world case studies, expert-led modules, and simulation exercises, participants will gain the skills needed to identify anomalies, perform timeline reconstructions, and uncover the root cause of security incidents within dynamic cloud environments such as AWS, Azure, and Google Cloud.

Programme Curriculum

Training Course on Cloud Log Analysis and Correlation for Investigations

Introduction

In today’s cloud-driven digital era, cybersecurity professionals must evolve beyond traditional methods to tackle cloud-native threats. Training Course on Cloud Log Analysis and Correlation for Investigations offers a comprehensive, hands-on approach to understanding how log data from cloud platforms can be analyzed and correlated for effective forensic investigations. With the exponential growth of SaaS, IaaS, and hybrid infrastructures, the ability to rapidly identify suspicious behaviors, detect insider threats, and trace unauthorized access through cloud logs is crucial for securing sensitive assets and maintaining compliance.

This course empowers learners with cutting-edge tools and techniques in SIEM integration, multi-cloud investigation, and log correlation engines to enhance incident response and threat hunting capabilities. Through real-world case studies, expert-led modules, and simulation exercises, participants will gain the skills needed to identify anomalies, perform timeline reconstructions, and uncover the root cause of security incidents within dynamic cloud environments such as AWS, Azure, and Google Cloud.

Course Objectives

1. Understand the fundamentals of cloud logging and log management.
2. Analyze cloud-native security logs (e.g., AWS CloudTrail, Azure Monitor, GCP Logs).
3. Implement advanced log correlation techniques across multi-cloud environments.
4. Detect malicious activity using anomaly detection and behavioral analytics.
5. Integrate cloud logs with SIEM tools like Splunk, ELK, and Microsoft Sentinel.
6. Apply forensic methods to identify and trace security incidents in real time.
7. Perform incident timeline reconstruction using log artifacts.
8. Differentiate between normal and suspicious user behavior in cloud environments.
9. Design automated alerting and response workflows.
10. Ensure compliance with log retention and audit regulations (e.g., SOC 2, ISO 27001).
11. Conduct investigations involving container logs (e.g., Kubernetes, Docker).
12. Correlate logs from cloud-based identity and access management systems.
13. Develop investigative reports from correlated log data.

Target Audiences

1. Cloud Security Analysts
2. SOC Analysts & Incident Responders
3. Digital Forensic Investigators
4. Penetration Testers
5. Cybersecurity Managers
6. Cloud Architects and Engineers
7. Compliance Officers
8. IT Auditors and Risk Analysts

Course Duration: 5 days

Course Modules

Module 1: Introduction to Cloud Log Analysis

- Types of cloud logs: system, application, network
- Importance of log retention and compliance
- Key logging tools in AWS, Azure, and GCP
- Challenges in cloud log collection
- Real-time log ingestion basics
- **Case Study**: Misconfigured S3 bucket breach analysis

Module 2: Log Collection and Centralization

- Collecting logs using agents and native services
- Centralized log storage strategies
- Log normalization and enrichment
- Integration with open-source and commercial SIEMs
- Secure log transmission methods

- **Case Study**: Correlating Azure activity logs after ransomware alert

Module 3: Multi-Cloud Log Correlation Techniques

- Correlation logic and rule creation
- Normalizing diverse log formats
- Cross-platform correlation challenges
- Using ELK and Sentinel for multi-cloud analytics
- Real-time threat detection rules
- **Case Study**: Detecting cross-cloud lateral movement

Module 4: Anomaly Detection and Behavior Analysis

- Behavioral baselining techniques
- Machine learning for anomaly detection
- Identifying compromised accounts
- Alert tuning to reduce false positives
- User and entity behavior analytics (UEBA)
- **Case Study**: Insider threat in Office365 with login pattern anomalies

Module 5: SIEM and Cloud-Native Tool Integration

- Connecting cloud logs to SIEM platforms
- Splunk and Sentinel correlation rules
- Building custom dashboards and alerts
- Mapping to MITRE ATT&CK framework
- Detection engineering for cloud-native threats
- **Case Study**: Using Splunk to detect data exfiltration in AWS

Module 6: Forensic Investigation in Cloud Environments

- Log-based timeline reconstruction
- Artifact collection from cloud systems
- Chain of custody and evidence integrity
- Data carving from log trails
- Reporting and documenting investigations
- **Case Study**: Timeline reconstruction of a GCP compromise

Module 7: Logs from Containers and Microservices

- Kubernetes and Docker log management
- Container-specific attack patterns
- Correlating pod, cluster, and API gateway logs
- Using Fluentd and Promtail in microservice architectures
- Threat detection in ephemeral environments
- **Case Study**: Kubernetes audit log analysis after container escape

Module 8: Regulatory Compliance and Audit Readiness

- Log requirements for HIPAA, SOC 2, PCI-DSS
- Retention strategies and automation
- Evidence presentation in legal proceedings
- Audit trail integrity and validation
- Role of logs in risk assessment and reporting
- **Case Study**: Cloud log audit in a GDPR compliance investigation

Training Methodology

- Interactive lectures with real-world examples
- Hands-on labs using AWS, Azure, and GCP environments
- Group-based log analysis simulations
- Practical exercises with Splunk, ELK Stack, Sentinel
- Quizzes and recap assignments to reinforce learning
- Capstone project based on a real-world investigation scenario

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

Start Date	End Date	Location	Price
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