# Hunting for Adversary Tactics in Cloud Logs 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 exponential growth of Cloud-Native adoption across major platforms like AWS, Azure, and GCP has created a vast, complex attack surface. Traditional security tools often fail to provide adequate visibility, leaving organizations vulnerable to sophisticated, low-and-slow adversaries. This is compounded by the persistent threats of misconfiguration, identity abuse, and API exploitation, which are the cornerstones of modern cloud breaches. The need for a proactive defense has never been more critical. Security teams must shift from reactive alerting to proactive threat hunting, leveraging the rich, yet often overwhelming, telemetry data in cloud logs. Hunting for Adversary Tactics in Cloud Logs Training Course is specifically designed to bridge the skills gap between traditional SOC analysts and the specialized demands of the cloud environment, focusing on real-world Adversary Tactics, Techniques, and Procedures (TTPs) as mapped to the MITRE ATT&CK Cloud Matrix.

This intensive, hands-on training empowers participants to become Cloud Threat Hunters, mastering the art of deriving attack context from massive log volumes. By deeply analyzing key log sources, implementing advanced KQL/Splunk queries, and developing behavioral analytics hypotheses, students will learn to detect elusive threats like lateral movement via IAM roles, data exfiltration through storage APIs, and persistence via backdoored service principals. The curriculum emphasizes practical application, with dedicated labs focusing on common attack scenarios such as Cloud Shell abuse, metadata service exploitation, and Container Runtime Attacks. Upon completion, attendees will possess the crucial skills to transform raw cloud logs into actionable security intelligence, significantly enhancing their organization？ÇÖs Detection Engineering and Incident Response capabilities against Advanced Persistent Threats

## Programme Curriculum

**Hunting for Adversary Tactics in Cloud Logs Training Course**

**Introduction**

The exponential growth of Cloud-Native adoption across major platforms like AWS, Azure, and GCP has created a vast, complex attack surface. Traditional security tools often fail to provide adequate visibility, leaving organizations vulnerable to sophisticated, low-and-slow adversaries. This is compounded by the persistent threats of misconfiguration, identity abuse, and API exploitation, which are the cornerstones of modern cloud breaches. The need for a proactive defense has never been more critical. Security teams must shift from reactive alerting to proactive threat hunting, leveraging the rich, yet often overwhelming, telemetry data in cloud logs. Hunting for Adversary Tactics in Cloud Logs Training Course is specifically designed to bridge the skills gap between traditional SOC analysts and the specialized demands of the cloud environment, focusing on real-world Adversary Tactics, Techniques, and Procedures (TTPs) as mapped to the MITRE ATT&CK Cloud Matrix.

This intensive, hands-on training empowers participants to become Cloud Threat Hunters, mastering the art of deriving attack context from massive log volumes. By deeply analyzing key log sources, implementing advanced KQL/Splunk queries, and developing behavioral analytics hypotheses, students will learn to detect elusive threats like lateral movement via IAM roles, data exfiltration through storage APIs, and persistence via backdoored service principals. The curriculum emphasizes practical application, with dedicated labs focusing on common attack scenarios such as Cloud Shell abuse, metadata service exploitation, and Container Runtime Attacks. Upon completion, attendees will possess the crucial skills to transform raw cloud logs into actionable security intelligence, significantly enhancing their organization?ÇÖs Detection Engineering and Incident Response capabilities against Advanced Persistent Threats

**Course Duration**

5 days

**Course Objectives**

Upon completion, participants will be able to:

1. Master Cloud Log Analysis across AWS CloudTrail, Azure Activity Logs, and GCP Audit Logs.
2. Develop Hypothesis-Driven Threat Hunts using the MITRE ATT&CK Cloud Matrix.
3. Design and implement advanced search queries in SIEM/SOAR platforms for cloud telemetry.
4. Identify and track Identity and Access Management (IAM) Abuse and Stolen Credential usage patterns.
5. Detect Lateral Movement and Privilege Escalation techniques unique to multi-cloud environments.
6. Uncover hidden Persistence Mechanisms in cloud environments
7. Analyze container and Serverless logs for signs of Container Runtime Attacks and Function Hijacking.
8. Perform in-depth forensic analysis of Data Exfiltration via cloud storage and network logs.
9. Apply Behavioral Analytics to establish baselines and spot anomalous user or service principal activity.
10. Integrate Cloud Threat Intelligence to prioritize hunting efforts for emerging Cloud APTs.
11. Build effective Detection-as-Code rules based on successful hunting outcomes for improved Detection Engineering.
12. Automate triage and data enrichment workflows for Cloud Incident Response.
13. Leverage VPC Flow Logs/NSG Logs to map and hunt for suspicious Command and Control (C2) traffic.

**Target Audience**

1. Security Operations Center Analysts
2. Cloud Security Engineers/Architects
3. Threat Hunters and Threat Intelligence Analysts
4. Digital Forensics and Incident Response Professionals

5. Detection Engineers
6. Red Team/Penetration Testers.
7. Cyber Security Consultants.
8. IT/Security Managers.

**Course Modules**

**Module 1: Foundations of Cloud Log Forensics**

- Cloud Log Landscape.
- Log Normalization & Centralization.
- Query Language Mastery.
- Adversary Tactics Overview.
- Case Study: Analyzing a Public S3 Bucket Misconfiguration exploit timeline using CloudTrail GetObject and PutObject events.

**Module 2: Hunting IAM & Credential Abuse**

- Initial Access TTPs.
- Privilege Escalation via IAM.
- Service Principal & API Key Abuse.
- MFA Bypass & Persistence.
- Case Study: Tracing the full kill chain of an attack that used Stolen AWS Access Keys to escalate privileges and create a persistent backdoor user.

**Module 3: Lateral Movement and Defense Evasion**

- Cross-Account & Lateral Movement.
- Cloud Network Hunting.
- Metadata Service Exploitation.
- Log Tampering & Defense Evasion.
- Case Study: Investigating a breach where an attacker leveraged a compromised VM to perform IMDSv1 exploitation and move laterally to a high-value database host.

**Module 4: Container and Serverless Threat Hunting**

- Container Runtime Visibility.
- Serverless Function Analysis.
- Container Escape TTPs.
- Supply Chain Attacks in CI/CD.
- Case Study: Forensically analyzing logs from an EKS Cluster to identify the deployment of a cryptomining container and its subsequent C2 communication.

**Module 5: Data Exfiltration and Impact Analysis**

- Storage Access Hunting.
- Exfiltration via APIs.
- Impact TTPs.
- Data Loss Prevention (DLP) Logging.
- Case Study: Following the log trail of a large-scale GCP Data Exfiltration where an attacker used a service account to stage and transfer sensitive BigQuery data to an external bucket.

**Module 6: Advanced Hunting Techniques and Automation**

- Behavioral Analytics.
- Statistical Analysis & Clustering.
- Hunting with Threat Intelligence.
- Automated Triage and Enrichment.
- Case Study: Building a Splunk Search that uses statistical functions to identify cloud roles with a statistically anomalous number of API calls after hours.

**Module 7: Detection Engineering and Operationalization**

- The Hunting Loop
- Rule Fidelity and Alert Tuning.
- Custom Alerting.
- Testing and Validation.
- Case Study: Developing a high-fidelity Azure Sentinel rule using KQL to detect a specific multi-stage Azure Function Persistence technique.

**Module 8: Multi-Cloud & Hybrid Environment Hunting**

- Cross-Platform Correlation.
- SaaS Log Hunting.
- Federated Identity Huntin.
- Continuous Threat Exposure Management.
- Case Study: Tracing a sophisticated phishing attack that compromised an Okta account, which was then used to gain Initial Access into both AWS and Azure environments.

## 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