Training Course on Cloud Identity and Access Management (IAM) Forensics

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 migration of enterprises to cloud platforms such as AWS, Azure, and Google Cloud, Identity and Access Management (IAM) has become the cornerstone of secure cloud operations. However, threat actors are increasingly exploiting misconfigurations, privilege escalations, and identity abuse to gain unauthorized access. Training Course on Cloud Identity and Access Management (IAM) Forensics equips security professionals with critical skills to investigate and mitigate IAM-related incidents. Leveraging real-world cloud breach scenarios, this course provides a hands-on, evidence-based framework for IAM forensic investigations in cloud environments.

Designed for today’s cloud-centric threat landscape, the course emphasizes IAM threat detection, role misuse analysis, access key forensic tracking, and insider threat identification. Participants will develop expertise in tools such as AWS CloudTrail, Azure AD Logs, GCP Audit Logs, and cloud-native SIEMs, mastering techniques to uncover the who, what, when, and how of IAM abuse. By the end of the training, learners will be prepared to detect, investigate, and contain IAM-related security events effectively across multi-cloud infrastructures.

Programme Curriculum

Training Course on Cloud Identity and Access Management (IAM) Forensics

Introduction

With the rapid migration of enterprises to cloud platforms such as AWS, Azure, and Google Cloud, Identity and Access Management (IAM) has become the cornerstone of secure cloud operations. However, threat actors are increasingly exploiting misconfigurations, privilege escalations, and identity abuse to gain unauthorized access. Training Course on Cloud Identity and Access Management (IAM) Forensics equips security professionals with critical skills to investigate and mitigate IAM-related incidents. Leveraging real-world cloud breach scenarios, this course provides a hands-on, evidence-based framework for IAM forensic investigations in cloud environments.

Designed for today’s cloud-centric threat landscape, the course emphasizes IAM threat detection, role misuse analysis, access key forensic tracking, and insider threat identification. Participants will develop expertise in tools such as AWS CloudTrail, Azure AD Logs, GCP Audit Logs, and cloud-native SIEMs, mastering techniques to uncover the who, what, when, and how of IAM abuse. By the end of the training, learners will be prepared to detect, investigate, and contain IAM-related security events effectively across multi-cloud infrastructures.

Course Objectives

1. Understand foundational concepts of Cloud IAM architecture and its security implications.
2. Perform IAM forensic investigations using logs and audit trails from AWS, Azure, and GCP.
3. Analyze role-based access control (RBAC) misuse and misconfiguration scenarios.
4. Trace compromised API keys and credentials using forensic methodologies.
5. Detect and investigate privilege escalation attempts in cloud environments.
6. Identify indicators of IAM-based insider threats using behavioral analysis.
7. Use cloud-native tools and third-party solutions for IAM log analysis.
8. Evaluate and correlate IAM events across multi-cloud environments.
9. Apply forensic techniques to OAuth and SAML-based authentication incidents.
10. Build a cloud IAM incident response playbook for rapid remediation.
11. Understand the forensic implications of IAM policy changes and deletions.
12. Map IAM forensic artifacts to compliance frameworks like NIST, ISO, and CIS.
13. Use machine learning and UEBA to enhance IAM threat detection capabilities

Target Audiences

1. Cloud Security Engineers
2. Digital Forensics Investigators
3. Incident Response Teams
4. SOC Analysts
5. DevSecOps Professionals
6. Cloud Compliance Officers
7. Cybersecurity Consultants
8. IT Auditors & Risk Managers

Course Duration: 5 days

Course Modules

Module 1: Introduction to Cloud IAM Forensics

- Overview of IAM in AWS, Azure, and GCP
- Role of IAM in cloud security architecture
- Common attack vectors and IAM vulnerabilities
- Key IAM forensic artifacts
- IAM attack lifecycle
- **Case Study**: Analysis of a misconfigured S3 bucket due to IAM mismanagement

Module 2: Log Collection and IAM Audit Trail Analysis

- Accessing and parsing AWS CloudTrail, Azure AD, and GCP Audit Logs
- IAM activity mapping to threat events
- Detecting anomalous login behaviors
- Timeline reconstruction using IAM logs
- Cloud log retention policies and limitations
- **Case Study**: Unauthorized login traced via CloudTrail logs

Module 3: Credential and API Key Abuse Forensics

- Types of credentials in cloud platforms
- Detecting exposed credentials on GitHub and public repositories
- Tracking API key usage and abuse
- Rotation and revocation policies
- Cloud-native alerting for suspicious credential use
- **Case Study**: API key abuse leading to data exfiltration

Module 4: Privilege Escalation and Role Misuse

- Detecting lateral movement using IAM roles
- Analysis of policy assignments and trust relationships
- Exploiting service roles for privilege elevation
- Real-time monitoring of privilege changes
- Investigating role assumption events
- **Case Study**: Privilege escalation via IAM role chaining

Module 5: Insider Threat Detection Using IAM Logs

- Behavioral indicators of insider abuse
- Correlation with HR and contextual data
- Risk scoring using user activity patterns
- Alerting thresholds for IAM misuse
- Integrating IAM logs with UEBA solutions
- **Case Study**: Insider exfiltrates data using legitimate credentials

Module 6: Forensic Investigation Across Multi-Cloud Environments

- Normalizing IAM events across cloud platforms
- Event correlation challenges and solutions
- Cross-cloud identity mapping
- Centralized IAM monitoring techniques
- Inter-cloud incident handling procedures
- **Case Study**: Coordinated attack across AWS and Azure

Module 7: Incident Response and IAM Playbook Design

- IAM-specific incident response lifecycle
- Triage and scoping IAM events
- Automated remediation techniques
- IAM playbook templates and response strategies
- Post-incident review and documentation
- **Case Study**: Developing an IR playbook post-OAuth token compromise

Module 8: Compliance, Reporting, and IAM Forensics Best Practices

- IAM logging requirements for compliance (NIST, CIS, ISO)
- Preparing forensic reports for legal and audit teams
- IAM governance and access review controls
- IAM policy monitoring and alerting best practices
- Future trends: Zero Trust, Just-In-Time access, ML-based IAM analytics
- **Case Study**: IAM forensic audit for regulatory compliance

Training Methodology

- Hands-on labs using AWS, Azure, and GCP sandboxes

- Real-world IAM breach simulations
- Interactive guided walk-throughs of case studies
- Use of forensic tools (e.g., Splunk, ELK, CloudTrail Viewer)
- Group activities and scenario-based role plays
- Quizzes and practical assessment after each module

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

Start Date	End Date	Location	Price
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