Training Course on Investigating Cloud Storage and Object Storage Incidents

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	5 Days
Base Fee	$1,100 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In the era of digital transformation, cloud storage and object storage solutions such as Amazon S3, Google Cloud Storage, and Microsoft Azure Blob Storage have become foundational in enterprise data infrastructure. However, these technologies also introduce new vectors for cyber threats, data breaches, misconfigurations, and insider threats. As data continues to move beyond traditional boundaries, investigating incidents in these complex environments demands cutting-edge forensic capabilities and a deep understanding of cloud-native technologies.

Training Course on Investigating Cloud Storage and Object Storage Incidents equips digital forensic professionals, incident responders, and cybersecurity analysts with in-depth skills to detect, analyze, and mitigate security breaches in cloud data environments. Leveraging real-world scenarios and cloud-native tools, this course emphasizes forensic evidence preservation, metadata investigation, threat hunting, and compliance readiness in environments such as AWS, Azure, and GCP. Learners will explore advanced investigation techniques in object storage security, API abuse, encryption misuse, and bucket misconfiguration.

Programme Curriculum

Training Course on Investigating Cloud Storage and Object Storage Incidents

Introduction

In the era of digital transformation, cloud storage and object storage solutions such as Amazon S3, Google Cloud Storage, and Microsoft Azure Blob Storage have become foundational in enterprise data infrastructure. However, these technologies also introduce new vectors for cyber threats, data breaches, misconfigurations, and insider threats. As data continues to move beyond traditional boundaries, investigating incidents in these complex environments demands cutting-edge forensic capabilities and a deep understanding of cloud-native technologies.

Training Course on Investigating Cloud Storage and Object Storage Incidents equips digital forensic professionals, incident responders, and cybersecurity analysts with in-depth skills to detect, analyze, and mitigate security breaches in cloud data environments. Leveraging real-world scenarios and cloud-native tools, this course emphasizes forensic evidence preservation, metadata investigation, threat hunting, and compliance readiness in environments such as AWS, Azure, and GCP. Learners will explore advanced investigation techniques in object storage security, API abuse, encryption misuse, and bucket misconfiguration.

Course Objectives

1. Understand cloud-native forensic methodologies and incident response in storage environments.
2. Identify and mitigate unauthorized access to public and private cloud storage buckets.
3. Conduct forensic analysis of object metadata and storage access logs.
4. Analyze data exfiltration patterns in AWS S3, Azure Blob, and Google Cloud Storage.
5. Investigate API abuse and privilege escalation in cloud storage configurations.
6. Explore multi-cloud forensics frameworks for diverse storage platforms.
7. Apply threat intelligence correlation in cloud data breach investigations.
8. Implement compliance-focused investigation methods (HIPAA, GDPR, CCPA).
9. Detect malware delivery and ransomware via object storage services.
10. Use cloud-native logging tools (CloudTrail, Storage Analytics) for auditing.
11. Reconstruct incident timelines using object storage artifacts.
12. Develop automated incident detection workflows using SIEM and SOAR.
13. Build actionable incident response playbooks for cloud storage incidents.

Target Audience

1. Cloud Security Engineers
2. Digital Forensics Investigators
3. Incident Response Teams
4. Compliance and Risk Officers
5. Cybersecurity Consultants
6. IT Auditors
7. System Administrators
8. Law Enforcement Cyber Units

Course Duration: 5 days

Course Modules

Module 1: Fundamentals of Cloud and Object Storage Forensics

- Introduction to cloud storage architecture
- Object vs. file/block storage explained
- Cloud-native logging and visibility challenges
- Access control and IAM review
- Common incident types in object storage
- **Case Study**: Analyzing a public AWS S3 bucket data leak

Module 2: AWS S3 Incident Investigation

- S3 versioning and metadata analysis
- S3 logging (CloudTrail, S3 access logs)
- Bucket policy misconfiguration detection
- Detecting abnormal read/write operations
- Identifying malware in stored objects

- **Case Study**: Detecting exfiltration through S3 bucket

Module 3: Azure Blob Storage Breach Analysis

- Blob Storage tiers and security mechanisms
- Azure Monitor and Diagnostic Logs
- Forensic acquisition from Azure Blob
- Investigating Shared Access Signatures (SAS)
- Preventing insider data theft
- **Case Study**: SAS token misuse and privilege abuse

Module 4: GCP Cloud Storage Threat Investigation

- Object lifecycle and retention analysis
- IAM and ACL audit in GCP
- Investigating access through signed URLs
- GCP audit log deep dive
- Integrating Chronicle with GCS for threat detection
- **Case Study**: Exposing sensitive logs through misconfigured GCS bucket

Module 5: Metadata and Object-Level Forensics

- What metadata reveals: timestamps, versions, access
- Identifying tampered files using hash comparison
- Preserving volatile storage evidence
- Chain of custody in cloud investigations
- Logging correlation across storage and compute
- **Case Study**: Investigating tampered evidence in object metadata

Module 6: Detection of Malware and Ransomware in Storage

- Scanning object storage for ransomware indicators
- File entropy and anomaly detection
- Integrating antivirus and malware sandboxes
- SIEM alerts and signature-based detection
- Malware propagation through cloud sync features
- **Case Study**: Detecting ransomware in cloud backup repositories

Module 7: API Abuse and Misconfiguration Exploitation

- Common misconfigurations in storage APIs
- Tools to simulate and test API vulnerabilities
- Investigating excessive permissions and escalation paths
- Forensics from compromised cloud API keys
- API call pattern anomalies using UEBA
- **Case Study**: Incident response to stolen API key abuse

Module 8: Incident Response Playbooks and Automation

- Building automated response workflows
- SOAR integration with cloud environments
- Trigger-based bucket quarantine actions
- Cloud-native threat intel enrichment
- Legal and regulatory response preparation
- **Case Study**: Automating detection and response for S3 policy tampering

Training Methodology

- Instructor-led, hands-on labs with real cloud environments
- Live case simulation and evidence reconstruction
- Interactive threat modeling and risk assessment exercises
- Daily incident walkthrough and cloud service analysis
- Access to digital lab portal and take-home scenarios

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254724527104*

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
10 Aug 2026	14 Aug 2026	Online	$1,100
17 Aug 2026	21 Aug 2026	Online	$1,100
24 Aug 2026	28 Aug 2026	Online	$1,100
31 Aug 2026	04 Sep 2026	Online	$1,100
07 Sep 2026	11 Sep 2026	Online	$1,100
14 Sep 2026	18 Sep 2026	Online	$1,100

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 2026	Online	$1,100
28 Sep 2026	02 Oct 2026	Online	$1,100

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

Register Online Now

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