Cloud Forensics

Four-week internship task & guidance guide

A provider-neutral fictional cloud audit export contains identity, object access and configuration events. It is a supplied log exercise with no need for credentials or live tenant access.

Working format

Four independent weekly submissions, each assessed out of 100. Each upload must include a PDF report and a separate description of at least 200 words in the student portal. Complete weeks 1-4 in order; early completion is permitted. Calendar deadlines are set by academy staff, not inferred from this guide.

What you need

A laptop, spreadsheet editor, PDF exporter and a SHA-256 hashing utility. The database domain also needs a SQLite viewer that supports read-only mode. Use only the accompanying synthetic dataset and document every transformation.

Evidence pack

Download cloud-training-data.zip beside this PDF on the website. The ZIP includes source exports, a README and a SHA-256 manifest. These are deliberately small teaching exports, not a complete forensic image. All identities and events are fictional.

Learning outcomes

Preserve integrity; document a reproducible examination; correlate evidence cautiously; separate observation from inference; communicate supported findings and limitations.

WEEK 1

Cloud audit scope and preservation

Goal: Establish scope and a verifiable evidence baseline.

Task checklist

1. Inventory audit.jsonl and assets.csv; hash files and record the fictional tenant boundary.

2. Map event ID, principal, action, target, result and timestamp. Separate user principals from service accounts.

3. Write a preservation plan covering retention, export method and missing provider-side context.

Required hand-in

cloud_scope.pdf, evidence_register.csv and field_map.csv

Portal description

Write at least 200 words in your own language explaining your method, source files and row/event IDs, observations, assumptions, uncertainty and learning. Put this text in the description box as well as any report appendix. Do not use filler to satisfy the word count.

Quality checks before upload

Keep the original evidence unchanged. Preserve raw timestamps and units. Identify tool versions and filters. Cite evidence IDs in findings. Recompute hashes of preserved files and include the result. Name your main file PFSA_<student-id>_cloud_W1.pdf. Supporting tables may be placed in one ZIP. Keep the uploaded file below 10 MB.

Week assessment: integrity 20 | method 25 | analysis 25 | evidence references 20 | clarity 10

WEEK 2

Identity and configuration review

Goal: Examine source records and document defensible observations.

Task checklist

1. Classify supplied events into authentication, object access and configuration changes.

2. Build a principal-action matrix and identify denied actions separately from successful access.

3. Review the configuration-change event and list what before/after state evidence would be required to judge its effect.

Required hand-in

principal_matrix.csv, access_review.csv and configuration_notes.pdf

Portal description

Write at least 200 words in your own language explaining your method, source files and row/event IDs, observations, assumptions, uncertainty and learning. Put this text in the description box as well as any report appendix. Do not use filler to satisfy the word count.

Quality checks before upload

Keep the original evidence unchanged. Preserve raw timestamps and units. Identify tool versions and filters. Cite evidence IDs in findings. Recompute hashes of preserved files and include the result. Name your main file PFSA_<student-id>_cloud_W2.pdf. Supporting tables may be placed in one ZIP. Keep the uploaded file below 10 MB.

Week assessment: integrity 20 | method 25 | analysis 25 | evidence references 20 | clarity 10

WEEK 3

Object-access timeline

Goal: Correlate sources and evaluate competing explanations.

Task checklist

1. Correlate authentication, object reads and configuration events using event IDs and UTC time.

2. Compare a scheduled automation explanation with an unverified account-use explanation for the service activity.

3. Document gaps caused by export scope, log delay, shared credentials or absent content records; do not infer file contents from a read event.

Required hand-in

cloud_timeline.csv and confidence_assessment.pdf

Portal description

Write at least 200 words in your own language explaining your method, source files and row/event IDs, observations, assumptions, uncertainty and learning. Put this text in the description box as well as any report appendix. Do not use filler to satisfy the word count.

Quality checks before upload

Keep the original evidence unchanged. Preserve raw timestamps and units. Identify tool versions and filters. Cite evidence IDs in findings. Recompute hashes of preserved files and include the result. Name your main file PFSA_<student-id>_cloud_W3.pdf. Supporting tables may be placed in one ZIP. Keep the uploaded file below 10 MB.

Week assessment: integrity 20 | method 25 | analysis 25 | evidence references 20 | clarity 10

WEEK 4

Cloud case report

Goal: Present a reproducible, evidence-supported conclusion.

Task checklist

1. Write a 4-6 page provider-neutral report describing scope, identity context, chronology and observed changes.

2. Cite the exact audit event IDs supporting each finding and note that these logs are fictional teaching data.

3. Deliver a handover pack with hashes, field map, principal matrix, queries or filters, and unresolved questions.

Required hand-in

cloud_report.pdf and cloud_appendix.zip

Portal description

Write at least 200 words in your own language explaining your method, source files and row/event IDs, observations, assumptions, uncertainty and learning. Put this text in the description box as well as any report appendix. Do not use filler to satisfy the word count.

Quality checks before upload

Keep the original evidence unchanged. Preserve raw timestamps and units. Identify tool versions and filters. Cite evidence IDs in findings. Recompute hashes of preserved files and include the result. Name your main file PFSA_<student-id>_cloud_W4.pdf. Supporting tables may be placed in one ZIP. Keep the uploaded file below 10 MB.

Week assessment: integrity 20 | method 25 | analysis 25 | evidence references 20 | clarity 10

Assessment & handover

Each week: 100 marks

Criterion	Marks	Expected evidence
Integrity and scope	20	Hashes, scope, preserved originals
Method and reproducibility	25	Clear steps, versions, filters or queries
Analysis and reasoning	25	Supported observations and alternatives
Evidence references	20	Exact file and row/event references
Communication	10	Clear report and 200-word portal narrative

Academic integrity

State which tools or writing assistance you used. Submit your own analysis and explain any reused template. A confident unsupported claim is weaker than a clearly stated uncertainty. This guide does not confer professional licensing, accreditation or an official affiliation.

Completion documents

Four submitted weeks unlock the document request stage. Assessment, payment confirmation and publication remain staff-controlled. A recommendation depends on evaluation; it is not automatic.

Further reading

NIST SP 800-86: Guide to Integrating Forensic Techniques into Incident Response.
https://csrc.nist.gov/pubs/sp/800/86/final

These publications are background reading. PFSA authored the task sequence and synthetic evidence pack; NIST has not endorsed this programme.