Evidence-Driven Log Triage Seminar

College & University Faculty | Lesson Plan | 90 minutes

Before class: Use only the sanitized fictional log set supplied by the instructor. Remove real names, credentials, tokens, IPs tied to live systems, or other sensitive data before class.

Outcome: Students will build an evidence-based incident timeline, maintain competing hypotheses, and explain confidence without overstating what the logs prove.

Materials

- Sanitized fictional log set
- Timeline worksheet
- Competing-hypotheses table
- Markers or spreadsheet

Learning Objectives

- Normalize time and event data into a coherent timeline.
- Separate observation from interpretation.
- Maintain at least two plausible hypotheses while evidence is incomplete.
- State confidence and identify missing evidence.

Opening (10 minutes)

- Show three log entries and ask students to distinguish facts from assumptions.

Timeline Build (25 minutes)

- Teams normalize timestamps, order events, and mark gaps or conflicts.
- Every timeline entry must cite the source log or artifact.

Competing Hypotheses (20 minutes)

- Teams write at least two explanations for the observed sequence.
- For each hypothesis, identify supporting evidence, contradictory evidence, and unknowns.

Evidence Update (20 minutes)

- Release a second packet of fictional evidence.
- Teams update the timeline and confidence ratings without deleting the original reasoning trail.

Debrief (15 minutes)

- What changed your confidence?
- Which evidence was most discriminating?
- Where could confirmation bias have affected the team?

Evidence and Assessment

- Collect the timeline and hypothesis table. Assess source traceability, disciplined uncertainty, quality of competing explanations, and revision when new evidence appears.

Optional Companion

- Pair with “Sanitized Log Triage” from Labs & Activities for a longer lab-oriented version.

Source and use

The Complete Cybersecurity Educator, Dr. Jason Edwards. College & University lesson-plan extension derived from the companion course-design, lab, and assessment resources.

Sharing and reuse: Please do not resell this resource. You may repost or share it with other educators. Please leave the Bare Metal Cyber Educators Hub URL and source attribution below intact. Use fictional or appropriately authorized data where applicable.

Read online: https://educate.baremetalcyber.com/resources/evidence-driven-log-triage-seminar/