

Homework

Extend your log-triage skills beyond the lab: build a reusable detection pack, benchmark AI against a human analyst, and stand up a personal SIEM notebook.

Task 1 — Detection Pack

Objective: Convert your Exercise 1-4 findings into a reusable set of 5 Sigma rules covering web, Linux, Windows, and cloud sources.

Instructions:

- Pick one high-value detection per lesson exercise
- Write each rule with correct fields for its log source
- Include a `falsepositives` section with at least 2 realistic items
- Include a `references` section linking to the MITRE technique

Deliverable: A single markdown file with 5 Sigma rules, each tagged with a MITRE technique and estimated FP rate.

Task 2 — Detection Benchmark

Objective: Measure how much faster AI-assisted log triage is than manual.

Instructions:

- Take one of the lab log files (pick the smallest you had trouble with)
- First, analyze it manually for 15 minutes — record findings
- Then, re-analyze it with AI for 15 minutes — record findings
- Compare: what did you miss? What did AI miss?

Deliverable: A short table (manual vs AI: findings, time-per-finding, false positives) plus a 100-word reflection on where each approach wins.

Task 3 — Personal SIEM Notebook

Objective: Build a reusable AI prompt library for your future log work.

Instructions:

- Save 5 prompts you would actually reuse: one for each of web, Linux, Windows, cloud, correlation
- For each, document: when to use it, what to paste, what good output looks like
- Format as markdown with code fences

Deliverable: A `personal-siem-prompts.md` file with 5 annotated prompts.