

Lab Guide

Capstone: alert feed triage, playbook authoring, detection-gap analysis, and SOC metrics reporting — run a full defensive scenario end-to-end.

Authorized Use Only

All capstone artifacts are **synthetic**. Treat this as a desk exercise, not a live SOC engagement.

Prerequisites

- Completed Lessons 01–09
- Access to an AI assistant (Claude, ChatGPT, or local LLM)
- Downloaded all five files into a folder named `blue-capstone-lab/`
- Your notes from the previous nine labs

Lab Scenario

You are the new SOC lead at AcmeCorp. Five artifacts landed in your first morning: the alert feed backlog, the current IR playbook template, a detection gap report from the prior assessor, last month's SOC metrics, and the network topology. Your mission: triage the alerts, finalize a playbook, close gaps, and brief the CISO on metrics.

Download Lab Files

Save all 5 files into a folder named `blue-capstone-lab/` before starting the exercises.

↓ `detection-gaps.txt` ~14 KB

↓ [metrics-data.txt](#) ~4 KB

↓ [network-topology.txt](#) ~11 KB

↓ [playbook-template.txt](#) ~12 KB

↓ [soc-alert-feed.txt](#) ~12 KB

Exercise 1 — SOC Alert Feed Triage

Open [soc-alert-feed.txt](#). Real SOC alerts down in alerts; prioritization is the job.

Task 1.1 — Handle the backlog

Below is a SOC alert feed (24 hours). Produce:

1. Deduplicate and cluster by incident.
2. Rank clusters by (confidence x impact).
3. Per cluster: initial triage verdict, next action, owner.
4. Identify noisy rules to tune out.
5. Identify 3 alerts that should have fired but did not (inferred from gaps).

Output: a triage board with columns
[new | in-progress | closed-fp | escalated].

[paste soc-alert-feed.txt]

✓ Self-check: Every cluster should have a named owner and a next action.

Exercise 2 — Playbook Authoring

Open [playbook-template.txt](#). A good playbook is the difference between chaos and control.

Task 2.1 — Fill in the playbook

Below is an IR playbook template. Complete it for THE top incident you identified in Exercise 1:

1. Trigger conditions
2. Severity matrix
3. Detection queries (Splunk / Sentinel / Elastic)
4. Containment steps (exact commands)
5. Eradication steps
6. Recovery validation
7. Communication template
8. Lessons-learned template
9. MITRE technique mapping
10. Metrics to capture (MTTD, MTTR)

Output: the completed playbook, ready for the SOC knowledge base.

[paste playbook-template.txt]

✓ Self-check: A tier-1 analyst with no context should be able to run this playbook at 03:00.

Exercise 3 — Detection Gap Analysis

Open `detection-gaps.txt`. You cannot fix what you cannot name.

Task 3.1 — Map to MITRE ATT&CK

Below is a detection-gap assessment. For each gap:

1. MITRE technique ID
2. Why it is uncovered (missing log source, no rule, low fidelity)
3. Fix: new sensor / new rule / tune existing rule
4. Effort (hours) and impact (low / med / high)

Then produce a coverage heatmap (text format) showing:

- 100% covered

- Partially covered
- Not covered

Rank fixes by (impact / effort) and produce a quarterly detection engineering roadmap.

[paste detection-gaps.txt]

✓ Self-check: You should have at least one "quick win" fix (<4 hours, high impact).

Exercise 4 — SOC Metrics for the CISO

Open `metrics-data.txt`. Metrics are how the SOC earns its next budget.

Task 4.1 — Build the exec report

Below is last month's SOC metrics data. Produce a CISO-level report:

1. MTTD / MTTR trendline
2. Alerts per analyst per day
3. False positive rate
4. Incidents by severity
5. Coverage improvement vs. prior month
6. Top 3 wins
7. Top 3 asks (budget, headcount, tooling)
8. One chart narrative: "the story the numbers tell"

Tone: confident, data-driven, no spin.

Format as markdown, one page.

[paste metrics-data.txt]

✓ Self-check: A CISO should be able to read this in 5 minutes and make one budget decision.

Final Exercise — 90-Day SOC Plan

Task 5.1 — Lead like a SOC manager

Combine all exercises into a 90-day SOC improvement plan:

- Month 1: quick wins (alert tuning, top playbooks)
- Month 2: detection gap closure
- Month 3: automation and metrics maturity

For each month list: objectives, owners, success criteria.

Include a stretch objective and a budget request.

Format as markdown, max 2000 words.

✓ **Self-check: The plan should be specific enough to review at weekly stand-up.**

Course Reflection

- Across all 10 lessons, which defensive discipline benefited most from AI assistance?
- Where did AI fall short and a human analyst still won?
- What would you automate end-to-end, and what would you keep human-in-the-loop?
- How has your SOC mental model changed from Lesson 01 to here?

Course Complete

You have finished the CTF Blue Team course. If you have not yet, run through the companion **CTF Red Team** course — the same scenarios, viewed from the attacker's side. The best defenders have walked the red team path.