

Part 1 — Lab Answers

Reference solutions for the lab exercises. Use these only after attempting the exercises yourself.

Exercise 1 — SOC Alert Feed Triage

Expect 2-3 real incidents buried under dozens of low-fidelity alerts. Cluster by asset + technique. Every cluster gets an owner and a next action. Noisy rules: any hitting >100 times per day without a real catch.

Exercise 2 — Playbook Authoring

A complete playbook has 10 sections, with detection queries in the SIEM's native language and containment steps as exact commands. A tier-1 analyst can execute without escalation.

Exercise 3 — Detection Gap Analysis

Quick wins are usually tuning-based: an existing rule with poor fidelity that becomes useful once you add a context filter. The first fix often costs <4 hours and closes 1-2 MITRE techniques.

Exercise 4 — SOC Metrics Report

MTTD/MTTR trendline is the headline. Top wins: 1-2 concrete incidents where SOC made a measurable difference. Top asks: specific, quantified, tied to a risk reduction.

Final Exercise — 90-Day SOC Plan

Month 1: tune top 20 noisy rules, finalize top 5 playbooks. Month 2: close 5 highest-impact detection gaps. Month 3: automate 3 workflows (alert enrichment, containment, comms) and publish dashboards.

Part 2 — Homework Answers

Model answers for the homework tasks. Your solution may differ and still be correct.

Task 1 — 90-Day SOC Plan

Full doc includes owners, weekly milestones, budget asks, and a risk section. Mentioning specific tools is fine — they show grounding.

Task 2 — Metrics Dashboard Mock

5 panels with data source and threshold. Good mocks explain what action follows from a red panel, not just the number.

Task 3 — Stakeholder Presentation

Lead with the decision you need. Anticipate "what if we said no?", "how much?", and "what is the risk of doing nothing?" with prepared answers.