

Part 1 — Lab Answers

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

Exercise 1 — Alert Triage

Most lab alerts collapse into a single incident: a phishing-delivered loader followed by lateral movement. Triage note format: "3 alerts, 1 incident, probable credential theft on HOST-X, recommend isolate."

Exercise 2 — IOC Pivoting

Expect at least 5 executable queries: Splunk search for the hash fleet-wide, a KQL query for the parent process, a firewall log query for the C2 IP, an AD query for the suspect account's recent logons, a DNS log query for the domain.

Exercise 3 — Impact Scoping

Containment decision must explicitly name any hosts left online for observation and explain why (e.g., "watching attacker to catch C2 rotation"). Legal flags: GDPR if EU PII, PCI if card data in scope.

Exercise 4 — Stakeholder Comms

Three voices, one incident. Tech: "compromised HOST-X, contained, IOCs attached." Exec: "we detected and contained a credential-theft attempt; no customer data touched so far; next update in 1 hour." Customer: often not sent during early IR — draft is ready if needed.

Final Exercise — Incident Report

One-page report with timeline, scope, state, next hour plan, resource asks.
Confidence > speculation.

Part 2 — Homework Answers

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

Task 1 — Tabletop Drill

Journal should record decision points and where you stalled. Stall points are the training data for your next playbook.

Task 2 — Blameless Postmortem

Action items must have owners and dates. No names in the narrative. "The deployment process allowed" > "Alice deployed".

Task 3 — Comms Template

Three channels with placeholders and tone guide. Bonus: "next update at HH:MM" pattern for predictability.