

Lab Guide

Four exercises: alert triage, IOC pivoting, impact scoping, and stakeholder comms — run an incident response with AI as your force-multiplier.

Authorized Use Only

All incident artifacts are **synthetic**. Never paste live incident data with PII or privileged content into a public AI.

Prerequisites

- Completed the [Theory](#) reading
- Access to an AI assistant (Claude, ChatGPT, or local LLM)
- Downloaded all four files into a folder named `ir-lab/`
- Familiarity with: MITRE ATT&CK, kill chain, IR playbook structure

Lab Scenario

It is 02:00. A SIEM ticket just paged you: suspicious activity across several hosts. You have the alert bundle, a list of affected systems, IOCs pulled from quick triage, and a comms template for the exec team. Your job: run the first two hours of incident response.

Download Lab Files

Save all 4 files into a folder named `ir-lab/` before starting the exercises.

↓ [affected-systems.txt](#) ~10 KB

↓ [incident-alerts.txt](#) ~9 KB

↓ [ioc-list.txt](#) ~10 KB

↓ [ir-comms-template.txt](#) ~16 KB

Exercise 1 — Alert Triage

Open [incident-alerts.txt](#). The first hour is won or lost on alert triage quality.

Task 1.1 — Is this an incident?

Below are SIEM alerts that fired in the last 30 minutes. Decide:

1. Are these one incident or multiple?
2. For each alert: true positive, benign true, or false positive?
3. What phase of the kill chain?
4. What data would confirm / refute?
5. Severity and confidence.
6. The ONE question you would ask the on-call engineer first.

Output a short triage note (paste-ready for the IR channel).

[paste incident-alerts.txt]

✓ **Self-check: Your triage note should fit in a single Slack message and answer: "is this a real incident, yes/no, and what's next?"**

Exercise 2 — IOC Pivoting

Open [ioc-list.txt](#). Every IOC is a thread to pull.

Task 2.1 — Expand the IOC set

Below are initial IOCs (hashes, IPs, domains, user accounts).
For each, suggest pivots:

1. Hash -> other hosts that executed it; parent process;
imphash neighbors.
2. IP -> other endpoints that connected; DNS history; ASN peers.
3. Domain -> subdomains, co-hosted domains, certificate SANs.
4. User account -> all logons in 24h, group changes, new keys.
5. Parent process -> children, command lines, loaded DLLs.

Output a pivoting tree and 5 queries to run right now
(OSQuery / Splunk / Sentinel / KQL style).

[paste ioc-list.txt]

✓ Self-check: Each pivot should produce an executable query, not just "check firewall logs".

Exercise 3 — Impact Scoping

Open `affected-systems.txt`. Scope first, contain second, eradicate third.

Task 3.1 — Map the blast radius

Below is a list of hosts with their role, data classification, and observed indicators. Produce:

1. Blast radius: which data / users / systems are in scope?
2. Containment options per host: isolate / reimage / monitor.
3. Evidence-preservation priority (which hosts to image first).
4. Business-impact per containment option.
5. Decision table: contain now vs. watch + catch attacker.
6. Regulatory exposure (GDPR / HIPAA / PCI) if data is accessed.

Output:

- The containment plan (host -> action)
- The legal / compliance flag list

[paste affected-systems.txt]

✓ Self-check: You should have a clear rationale for any host you leave NOT contained.

Exercise 4 — Stakeholder Comms

Open `ir-comms-template.txt`. Incidents are won or lost on communication as much as on forensics.

Task 4.1 — Draft the messages

Below is a comms template for an IR. Fill in three specific messages:

1. Technical SITREP for the IR channel (every hour)
2. Executive update for the CISO (concise, risk-framed)
3. Customer-facing update (only if required, legal-safe, no speculation)

Tone guidance:

- Technical: precise, IOC-rich, action-oriented
- Executive: outcomes, risk, decisions needed
- Customer: empathetic, factual, no blame

Output all three messages.

[paste ir-comms-template.txt]

✓ Self-check: The three messages should be the same incident in three voices — not three different incidents.

Final Exercise — Incident Report

Task 5.1 — 2-hour report

Combine the four outputs into a 2-hour incident report:

1. Summary (3 sentences)
2. Timeline
3. Scope (systems, data, users)
4. Current state (contained? active?)
5. Next-hour plan
6. Resource asks (who needs to be paged next)

Format as markdown, max 1 page.

✓ **Self-check: The report should make the reader confident the IR lead has control of the situation.**

What's Next

Lesson 09 shifts from live response to **forensics** — memory, disk, and network evidence analysis.