STUDENT HANDOUT · WEEK 14

Incident Response and Investigation

SY0-701 objectives 4.8, 4.9. Notes, exercises, review questions, and the lab.

Name	
Date	

THIS WEEK YOU WILL

1. Sequence the seven incident response phases and name the key work done in each.
2. Choose a containment action that limits spread while preserving evidence.
3. Compare tabletop exercises and simulations and explain what each one tests.
4. Apply root cause analysis and explain how threat hunting differs from alert response.
5. Explain legal hold, chain of custody, acquisition, preservation, reporting, and e-discovery.
6. Select the log or data source that best answers a given investigation question.

KEY IDEAS

Preparation, detection, and analysis come first

1. Preparation	Plan, team, contacts, tools, and tested backups
2. Detection	Alerts, user reports, or outside warnings raise a flag
3. Analysis	Confirm it is real, find the scope, set severity

Contain, eradicate, recover, then learn

1. Containment	Stop the spread: isolate hosts, disable accounts
2. Eradication	Remove malware, persistence, and attacker access
3. Recovery	Restore from clean backups and monitor closely
4. Lessons learned	Review what happened and update plan and controls

Tabletops test decisions, simulations test skill

Tabletop exercise	Simulation
Discussion around a table, no systems touched	The scenario is acted out in real time
Facilitator adds injects at set times	Lab or production systems, with safeguards
Tests the plan, roles, and decisions	Tests people, tools, and response times
Cheap and safe enough to run every year	Costs more and takes longer to set up

Find the cause and hunt for what alerts miss

Root cause analysis	Find the underlying reason so the fix actually sticks (No MFA on remote access)
Five whys	Keep asking why until you reach something you can fix (Often ends at a process gap)
Threat hunting	Search for attackers before any alert fires (Hypothesis from threat intel)
Hunt outputs	A found intrusion or a new detection rule (Rule for ATT&CK T1053)

Six forensic terms you must keep straight

Term	What it means
Legal hold	Preserve data for a case; overrides deletion
Chain of custody	Log of who handled evidence, when, and why
Acquisition	Collect a forensic image using a write blocker
Preservation	Keep it unchanged; hash it and store it securely
Reporting	Factual write-up others can repeat and verify
E-discovery	Find and produce electronic records for a case

Collect the most volatile evidence first

1. Registers, cache	Gone in nanoseconds; rarely captured by hand
2. RAM	Processes, connections, keys; lost at power-off
3. Swap and temp	Page files and temp folders change constantly
4. Disk	Image it with a write blocker, then hash it
5. Remote logs	SIEM and syslog copies; may roll over in days
6. Backups	Archival media; the most stable source

Each log answers a different question

Log source	Best for
Firewall	Connections allowed or denied, by IP and port
Application	User actions inside an app, such as exports
Endpoint	Processes, file changes, and EDR detections
OS-specific security	Logons, failures, privilege use (4624, 4625)
IPS/IDS	Which signature fired and whether it blocked
Network	DNS, DHCP, proxy, and flow records

Metadata, scans, reports, dashboards, and PCAPs

Metadata	Data about data: headers, authors, timestamps (Email Received headers)
Vulnerability scans	Which systems have which known weaknesses (Is the exploited flaw elsewhere?)
Automated reports	Scheduled summaries that show trends over time (Weekly failed logon report)
Dashboards	Live visual summary; drill down for evidence (Alerts by severity)
Packet captures	Full traffic contents, payload included (Wireshark, tcpdump)

EXERCISE 1: PUT THE CLINIC'S RANSOMWARE RESPONSE IN ORDER

8 MINUTES · PAIRS

Assign each action to an incident response phase, then put all eight in the order they happened at the clinic.

#	Prompt	Your answer
1	A: Restore the file server from a clean offline backup	
2	B: Pull two infected PCs off the network, leave them on	
3	C: Install EDR on every laptop and write the call list	
4	D: Add offline backups and remote access MFA to the plan	
5	E: The SIEM alerts on hundreds of files renamed at once	
6	F: Delete the malicious scheduled task, reset passwords	
7	G: Confirm the alert, identify the family, list affected hosts	
8	H: Block the attacker's command-and-control domain	

EXERCISE 2: WHICH DATA SOURCE ANSWERS EACH QUESTION

7 MINUTES · SMALL GROUPS

For each investigation question, name the single best data source and one backup source. Be ready to defend your pick.

#	Prompt	Your answer
1	Which host connected to 203.0.113.50 at 2 a.m.?	
2	Did someone guess passwords on the billing PC's local account?	
3	Which user exported the patient list from the EHR?	
4	Did a signature catch the exploit against the web portal?	
5	Which process launched PowerShell on the nurse's laptop?	
6	Which other systems still have the flaw the attacker used?	
7	What did the attacker type in the cleartext Telnet session?	
8	Which servers relayed the phishing email to the clinic?	

REVIEW QUESTIONS

1. Which phase comes right after containment, and what happens in it?

2. What is the difference between a tabletop exercise and a simulation?

3. What does a chain of custody record, and why does it matter?

4. A responder can capture either a disk image or RAM first on a running server. Which comes first, and why?

5. An analyst wants to know which internal host talked to a known bad IP last night. Which source is best?

KEY TAKEAWAYS

- **Follow the seven phases.** Prepare, detect, analyze, contain, eradicate, recover, then learn.
- **Practice before the real one.** Tabletops test decisions; simulations test people and tools.
- **Protect the evidence.** Legal hold, chain of custody, hashes, and the order of volatility.
- **Match the source to the question.** Each log answers different questions; know which one to pull.

LAB 14: TABLETOP EXERCISE, RANSOMWARE AT LAKESIDE FAMILY CLINIC

60 MINUTES

Work in groups of four to six with your project notes on Lakeside Family Clinic, a timer, and a printed copy of the scenario and the four injects below. This is a discussion exercise: no computers or tools are needed, and no one touches a real system.

Steps

1. Assign roles: a facilitator who reads the injects and keeps time, an incident commander, an IT lead, the practice manager (patients and operations), a privacy and compliance officer, and a scribe who records every decision with a timestamp.
2. Read the scenario aloud: at 7:40 a.m. on a Monday, front desk staff find that the scheduling system will not open and every file on the shared drive ends in .lckd. A ransom note on each desktop demands payment in cryptocurrency within 72 hours.
3. Inject 1 (minutes 0 to 10): the IT lead finds that the shared administrator account logged on to the file server at 2:13 a.m. from a front desk PC. Decide how you confirm the incident, who gets called and in what order, and what you contain first.
4. Inject 2 (minutes 10 to 20): the external backup drive was plugged in overnight and is also encrypted. Decide how the clinic sees patients today using paper downtime procedures, and which evidence you preserve, in what order, before anyone wipes a machine.
5. Inject 3 (minutes 20 to 30): a post on a leak site claims the attackers copied patient records. Decide who owns the notification decision, what the privacy officer must check under the HIPAA Breach Notification Rule, and when you call the cyber insurer and law enforcement.
6. Inject 4 (minutes 30 to 40): the owner-physician asks whether the clinic should pay the ransom. List the facts the group needs before anyone can answer, and record who has the authority to decide.
7. Hotwash (minutes 40 to 50): name three things that went well and three gaps in the plan, then run the five whys to find a root cause for the attackers' initial access.
8. Write five lessons learned actions, each with an owner by role and a due date, and map each one to the incident response phase it improves.

Hand in

A two-page after-action report: the timeline of decisions from the scribe's notes, who filled each role, the evidence you would preserve and in what order, your five whys, and the five lessons learned actions with owners and dates. This report feeds your final project.

Questions to answer in your report

1. At what point did your group move from analysis to containment, and what evidence could a careless containment step have destroyed?

2. Which data sources would confirm the 2:13 a.m. logon and the claim that patient records were copied?
3. What was your root cause for initial access, and which control from earlier weeks would have stopped it?
4. Who had the authority to decide on paying the ransom and on breach notification, and was that written in the plan before the exercise?
5. What would you need to change to run this scenario as a simulation instead of a tabletop?