COMPTIA SECURITY+ SY0-701 · WEEK 14

Incident Response and Investigation



Objectives 4.8 and 4.9 · 90-minute lesson

Presenter: Trapper Brown

What you will be able to do in 90 minutes

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.

AGENDA

4 min	Why incident response is a process
10 min	Preparation, detection, and analysis
10 min	Containment, eradication, recovery, lessons
7 min	Training and testing the plan
10 min	Exercise 1: put the response in order
8 min	Root cause analysis and threat hunting
9 min	Digital forensics
6 min	Acquisition and the order of volatility
9 min	Log data
6 min	Other data sources
9 min	Exercise 2: pick the data source
2 min	Wrap-up

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

- Discussion around a table, no systems touched
- Facilitator adds injects at set times
- Tests the plan, roles, and decisions
- Cheap and safe enough to run every year

Simulation

- The scenario is acted out in real time
- Lab or production systems, with safeguards
- Tests people, tools, and response times
- Costs more and takes longer to set up

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.

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

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

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.

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

Five questions: write your answers first

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?

TAKEAWAYS

Four things to take with you

01

Follow the seven phases

Prepare, detect, analyze, contain, eradicate, recover, then learn.

02

Practice before the real one

Tabletops test decisions; simulations test people and tools.

03

Protect the evidence

Legal hold, chain of custody, hashes, and the order of volatility.

04

Match the source to the question

Each log answers different questions; know which one to pull.

NEXT Lab 14: Tabletop exercise, ransomware at Lakeside Family Clinic