Lab 5.1 – Analyzing a Simulated Security Incident

1. Lab Overview

1.1 Lab Description

In this lab, you'll step into the role of a **security analyst responding to an incident**. Using a simulated scenario, you'll follow the full **incident response lifecycle**:

- Investigate alerts and logs.
- Identify Indicators of Compromise (IOCs).
- Contain, eradicate, and recover from the threat.
- Document your actions and evidence.
- Conduct a post-incident review with lessons learned.

This exercise combines technical skills (log analysis, response actions) with **critical thinking and structured reporting** — exactly what real-world cybersecurity teams do when responding to attacks.

1.2 Learning Objectives

After completing this lab, you will be able to:

- Analyze logs to identify suspicious activity and confirm incidents.
- Recognize and document **Indicators of Compromise (IOCs)**.
- Apply the **Contain → Eradicate → Recover** response model.
- Preserve evidence while maintaining **chain of custody**.
- Complete an **incident response report** (timeline, systems, accounts, actions).
- Conduct a **post-incident review** and propose improvements to detection, policies, and training.

1.3 Prerequisites

Before starting this lab, you should:

- Understand the basics of **incident response lifecycle** (NIST or similar).

- Be comfortable reviewing system logs and recognizing unusual patterns.
- Have access to:
    - A **log dataset** (provided in course materials or instructor guidance).
    - A text editor or spreadsheet for organizing findings.
    - An **incident response template** (timeline, actions, next steps).

Optional but recommended: familiarity with SIEM concepts and basic forensic practices.

1.4 Estimated Completion Time

Activity	**Estimated Time**
Scenario intro & alert review	30 minutes
Log review & IOC identification	45 minutes
Incident response steps	60 minutes
Documentation & evidence handling	45 minutes
Post-incident review & lessons learned	30–45 minutes
Wrap-up & reflection	15 minutes
Total Estimated Time	**~4–4.5 hours**

Checkpoint
Before moving on, make sure you:

- Understand the purpose of this simulation (practice the end-to-end incident lifecycle).
- Have your log files, template, and note-taking tools ready.
- Can dedicate about **4–4.5 hours** to complete the lab in full.

2. Scenario Setup – The Initial Alert

2.1 Background

It's late at night — **2:41 AM** — when your organization's **Security Information and Event Management (SIEM)** system generates an alert. As the analyst on call, you must determine if this is:

- A harmless anomaly, or
- A legitimate **security incident in progress**.

2.2 The Alert Details

The SIEM alert includes the following suspicious indicators:

- **Login activity**: A successful login from IP address 203.0.113.41.
- **User account**: The login used the **dbadmin** account, which normally operates only during business hours.
- **Time of login**: **2:41 AM**, well outside normal usage patterns.
- **Follow-up activity**: A sudden spike in **outbound network traffic** from the company's HR database server to an external FTP server.

2.3 Your Role

You are acting as the **Incident Responder**. Your responsibilities are to:

1. **Review the alert** carefully.
2. **Gather additional evidence** from logs and network activity.
3. **Decide** whether this is a false positive or a confirmed incident.
4. **Take action** if necessary.

Tip: Don't jump to conclusions based on the alert alone — treat it as a starting point for investigation.

2.4 Investigation Goals

At this stage, your goals are to:

- Validate whether the login was legitimate.
- Determine if the data exfiltration was **authorized** or **malicious**.
- Identify any early **Indicators of Compromise (IOCs)** for deeper investigation in the next steps.

Checkpoint
Before moving on:

- Do you understand the details of the initial alert (time, account, IP, data transfer)?
- Do you have a way to take notes as you review logs and build your timeline?
- Are you ready to begin **log review and IOC identification**?

3. Log Review and IOC Identification

3.1 Reviewing Authentication Logs

Your first step is to check the **authentication logs** for details about the suspicious login.

The logs show:

```
2025-09-21 02:41:06 LOGIN SUCCESS user=dbadmin ip=203.0.113.41
2025-09-21 09:15:42 LOGIN SUCCESS user=dbadmin ip=10.0.2.15
2025-09-20 14:05:33 LOGIN SUCCESS user=dbadmin ip=10.0.2.15
```

Observations:

- The **2:41 AM login** stands out as unusual.
- Previous logins came from an **internal IP (10.0.2.15)** during business hours.
- The suspicious login came from a **foreign external IP (203.0.113.41)**.

3.2 File Access Logs

Next, you check file access logs on the HR database server.

```
2025-09-21 02:43:11 FILE ACCESS user=dbadmin /HR/employee_records.xlsx
2025-09-21 02:44:27 FILE ACCESS user=dbadmin /HR/salary_data.csv
2025-09-21 02:45:03 FILE ACCESS user=dbadmin /HR/benefits.docx
```

Observations:

- Sensitive HR files were accessed immediately after the suspicious login.
- These files are rarely accessed outside of monthly payroll cycles.

3.3 Network Activity Logs

Finally, you examine the network traffic logs.

```
2025-09-21 02:46:10 OUTBOUND TRANSFER user=dbadmin server=203.0.113.50 protocol=FTP size=1.2GB
2025-09-21 02:49:55 OUTBOUND TRANSFER user=dbadmin server=203.0.113.50 protocol=FTP size=850MB
```

Observations:

- Large amounts of data were exfiltrated to an **external FTP server**.
- Normal database traffic usually uses **SQL over port 1433**, not FTP.

3.4 Identifying Indicators of Compromise (IOCs)

From your log review, you identify the following IOCs:

- **Suspicious IP address**: 203.0.113.41 (login source).
- **Unusual login time**: 2:41 AM.
- **Account used**: dbadmin (likely compromised).
- **Sensitive files accessed**: HR records and payroll data.
- **Outbound traffic**: Large FTP transfers to 203.0.113.50.

3.5 Confirming the Incident

At this point, the evidence indicates this is a **confirmed incident**:

- External login from unusual IP → **Unauthorized access**.
- Access to HR data → **Sensitive information at risk**.
- Large outbound FTP transfers → **Data exfiltration confirmed**.

Conclusion: This is **not a false positive** — containment actions must begin.

Checkpoint
Before moving on:

- Did you identify at least **three IOCs** from the logs?
- Do you understand why this is a confirmed breach?
- Are you ready to take **incident response actions**?

4. Incident Response Actions

4.1 Containment

The first priority is to **stop the attack from continuing**.

Actions you should take immediately:

1. **Disable the compromised account** (dbadmin).
2. **Isolate the affected server** from the network to prevent further data exfiltration.
3. Notify the **Incident Response (IR) team lead** and escalate per policy.

Goal: Contain the threat before it spreads further.

4.2 Eradication

Once the threat is contained, focus on **removing the attacker's presence**.

Steps include:

- Scan the affected system for **malware, rootkits, or backdoors**.
- Remove any malicious files or unauthorized scheduled tasks.
- Check for **secondary compromised accounts** created by the attacker.

Goal: Ensure the attacker no longer has access.

4.3 Recovery

After eradication, move into **restoring normal operations**:

1. Restore the compromised system from a **known clean backup**.
2. Apply **security patches** and update configurations before bringing it back online.
3. Closely monitor the system for signs of recurring malicious activity.

Goal: Return to business as usual with improved defenses in place.

4.4 Documenting Response Actions

As you go through Containment → Eradication → Recovery:

- Record **timestamps** of each action.
- Note **who performed the action**.
- Ensure actions are logged in the official **incident response report**.

This documentation is critical for compliance, reporting, and learning.

Checkpoint
Before moving on:

- Did you capture all three phases (Contain → Eradicate → Recover)?
- Have you started documenting each action with time and details?
- Do you understand why recovery must include monitoring?

5. Documentation and Evidence Handling

5.1 Why Documentation Matters

Every action during an incident must be **recorded and time-stamped**.

- Creates a **clear timeline** of what happened and when.
- Provides evidence for **post-incident review** and legal investigations.
- Ensures compliance with **organizational policies** and frameworks (e.g., ISO 27001, NIST, GDPR).

5.2 Preserving Logs

Logs are your primary evidence. Secure them before they are rotated or deleted.

- Export SIEM alert logs.
- Copy system authentication logs.
- Save network traffic logs.
- Ensure backups are stored in a **read-only location**.

Tip: Always keep the **original copy untouched** — work on duplicates.

5.3 Capturing Volatile Data

Some evidence disappears quickly unless captured immediately.

- Memory dump of the compromised server (RAM contents).
- Active process lists and network connections.
- Screenshots of suspicious sessions.

5.4 Chain of Custody

To maintain integrity, follow a **chain of custody** procedure:

1. Record **who collected the evidence**, **when**, and **how**.

2. Store evidence securely (e.g., encrypted drive, forensic locker).
3. Document every handoff if evidence is transferred.

This ensures the evidence is **legally defensible** and tamper-proof.

5.5 Completing the Incident Report

Your incident response template should include:

- **Timeline of events** (alert, detection, response).
- **Systems affected**.
- **Accounts involved**.
- **Actions taken**.
- **Outstanding next steps**.

Checkpoint
Before moving on:

- Did you export and preserve all relevant logs?
- Did you capture any volatile evidence before it was lost?
- Did you record actions in the incident report with timestamps?
- Did you maintain chain of custody for any critical evidence?

6. Post-Incident Review and Lessons Learned

6.1 Why Post-Incident Reviews Matter

Resolving an incident isn't the end — it's the **beginning of improvement**. A structured review ensures that:

- Root causes are understood.
- Detection rules are updated.
- Teams learn from mistakes and successes.
- The organization becomes more resilient.

6.2 Review Findings

After containment and recovery, gather the incident response team to review:

- **Timeline of events** (alert → investigation → containment → recovery).
- **How quickly the team responded**.
- **What worked well** (e.g., quick detection, strong escalation).
- **What failed** (e.g., weak monitoring, delayed communication).

Document these findings in the official report.

6.3 Improvements to Implement

Based on your findings, take action to strengthen defenses:

- **Detection rules** → Update SIEM to flag unusual login times or FTP transfers.
- **Firewalls** → Block suspicious IPs and restrict outbound FTP traffic.
- **User training** → Provide awareness sessions on account hygiene and suspicious activity reporting.
- **Incident playbooks** → Add this scenario to your runbooks for faster future response.

6.4 Training the Team

A post-incident review is also a **learning opportunity**:

- Share lessons across IT, security, and leadership.
- Run a **tabletop exercise** to rehearse the same scenario.
- Update onboarding for new team members with lessons from this incident.

Every incident is a chance to sharpen team skills.

6.5 Example Lessons Learned (From This Lab Scenario)

- Shared administrative accounts (dbadmin) pose a risk → Implement least privilege and monitoring.
- Outbound FTP traffic should be **monitored or restricted**.
- Off-hours logins should trigger **alerts by default**.
- Incident documentation must be standardized and reviewed regularly.

Checkpoint
Before moving on:

- Did you summarize what worked and what failed in this incident?
- Did you propose at least **two improvements** to tools, policies, or training?
- Did you record lessons for future incidents and share them with your team?

7. Wrap Up

7.1 Key Takeaways

In this lab, you completed a **simulated incident response exercise** that brought together the full lifecycle of cybersecurity response. You:
Investigated an alert from a SIEM.
Identified Indicators of Compromise (IOCs) in logs and network data.
Applied the **Contain → Eradicate → Recover** response framework.
Preserved evidence and maintained a proper chain of custody.
Documented the incident timeline and actions in a formal report.
Conducted a post-incident review and identified lessons learned.

7.2 Skills You've Gained

By finishing this lab, you can now:

- Analyze logs to confirm or reject suspicious activity.
- Respond systematically to incidents using best practices.
- Create professional **incident reports** with timelines, actions, and evidence.
- Propose actionable **improvements** to detection, response, and user training.

7.3 Next Step: Module 5 Final Quiz

You've now completed the **practical capstone lab of Module 5: Threat Detection and Incident Response**.

Your next step is to take the **Module 5 Final Quiz**, which will cover:

- Threat detection concepts (alerts, IOCs, SIEM basics).
- Incident response lifecycle (Contain, Eradicate, Recover).
- Evidence handling and chain of custody.
- Post-incident review and continuous improvement.

Final Checkpoint
Before moving on to the quiz:

- Have you completed and saved your incident response report?
- Can you clearly explain what made this incident a **confirmed breach**?
- Can you summarize **three lessons learned** from this lab?

If yes — you're ready for the quiz! 🎉

8. Appendix

8.1 Sample Incident Response Template

Use this template to structure your incident documentation:

Field	Details
Incident ID	[Unique identifier]
Date/Time Detected	[e.g., 2025-09-21 02:41 AM]
Reported By	[SIEM / Analyst / User]
Systems Affected	[Database server, HR files]
Accounts Involved	[dbadmin]
Indicators of Compromise (IOCs)	[Suspicious IPs, abnormal logins, FTP transfers]
Containment Actions	[Disabled account, isolated server]
Eradication Actions	[Malware scan, removed backdoors]
Recovery Actions	[Restored from clean backup]
Evidence Collected	[Logs, memory dump, chain of custody form]
Next Steps	[Block IPs, update SIEM rules, user training]
Status	[In Progress / Closed]

8.2 IOC (Indicators of Compromise) Reference List

Common IOC categories to watch for:

- **Authentication logs** → Unusual login times, foreign IPs, repeated failures followed by success.
- **File activity** → Unusual access to sensitive directories, large file transfers.
- **Network traffic** → Outbound connections to unknown IPs, abnormal protocols (e.g., FTP instead of HTTPS).

- **Process activity** → Unexpected services, scheduled tasks, or command execution.

Tip: Always cross-check IOCs with **known threat intelligence feeds** for confirmation.

8.3 Common Mistakes in Incident Response

- **Jumping straight to containment** without confirming the incident.
- **Failing to document actions** as they happen.
- **Not preserving volatile evidence** (RAM, live connections).
- **Ignoring chain of custody** — which may invalidate evidence in legal contexts.
- **Skipping the post-incident review**, missing opportunities to improve defenses.

8.4 Further Reading & Resources

- **NIST Computer Security Incident Handling Guide (SP 800-61r2)** https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
- **SANS Incident Handler's Handbook** https://www.sans.org/white-papers/33901/
- **FIRST (Forum of Incident Response and Security Teams)** Best Practices https://www.first.org/
- **MITRE ATT&CK Framework** – For mapping attacker techniques and behaviors https://attack.mitre.org/

Suggested Reading: *Incident Response & Computer Forensics* (Luttgens, Pepe, Mandia).