7. Create an Incident Response Report
Activities:

- **Task:** Document an incident using SANS templates**.**

  The SANS incident response lifecycle: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned

- Incident Identification
- Incident Description
- Incident Classification
- Actions Taken
- Recommendations
- Lessons Learned

1. Preparation

- **Establish an Incident Response Team (CSIRT):**

Create a dedicated team with defined roles and responsibilities for responding to incidents.

- **Develop an Incident Response Plan:**

Create a comprehensive plan outlining procedures, communication protocols, and escalation paths.

- **Implement Training Programs:**

Ensure the team is well-trained and knowledgeable about the incident response plan and relevant tools.

2. Identification

- **Detect Anomalies:**

Monitor for unusual activity, system logs, and alerts that could indicate a security incident.

- **Gather Initial Information:**

Collect preliminary data about the suspected incident from logs and user reports.

- **Classify and Prioritize:**

Determine the severity and scope of the incident to allocate resources effectively.

3. Containment

- **Isolate the Incident:**

Take immediate action to limit the spread of the threat, such as quarantining affected systems.

- **Preserve Evidence:**

Collect and preserve crucial data that may be needed for analysis or legal proceedings.

4. Eradication

- **Identify the Root Cause:** Determine the underlying cause of the incident.
- **Remove the Threat:** Eliminate the threat from the environment, which may involve patching vulnerabilities or removing malware.

5. Recovery

- **Restore Systems:**

Bring affected systems and services back online and restore them to their normal operational state.

- **Verify Functionality:**

Ensure that systems are functioning correctly and data integrity is maintained.

6. Lessons Learned

- **Conduct a Post-Incident Review:** Hold a meeting with the CSIRT and stakeholders to discuss the incident.
- **Create an Incident Report:** Document all aspects of the incident, detailing the event, the response, and its outcomes. Answer questions such as:
    - Who was involved?
    - What happened?
    - Where did it happen?
    - Why did it happen?
    - How was it handled?
- **Identify Areas for Improvement:** Extract actionable steps to improve the incident response process, tools, and procedures for future incidents.

Enhanced Tasks:

- **Report Draft:** Write a report for a simulated phishing incident, including Executive Summary, Timeline, and Mitigation Steps**.**

1. Incident Identification

- Date/Time Identified: August 21, 2025, 10:15 AM
- Incident Handler: Jane Doe, Security Analyst
- Incident Number: PHISH-2025-0821
- Incident Reporter: IT Security Team
- Contact Information: jane.doe@company.com

---

2. Executive Summary

On August 21, 2025, the IT Security Team conducted a simulated phishing campaign targeting employees across various departments to assess their awareness and response to phishing threats. The simulation involved sending a crafted phishing email mimicking a popular vendor requesting credential verification.

Out of 250 targeted employees, 42 clicked on the phishing link, and 18 submitted credentials on the fake landing page. The simulation provided valuable insights into employee susceptibility to phishing and highlighted areas requiring additional security awareness training. No real systems or data were compromised as this was a controlled exercise.

---

3. Timeline

Date/Time	Event Description
August 21, 2025, 09:00 AM	Simulated phishing emails sent to 250 employees.
August 21, 2025, 10:15 AM	First click detected on phishing link.
August 21, 2025, 12:00 PM	IT Security Team begins monitoring user interactions.
August 21, 2025, 03:30 PM	Simulation concludes; data collected and analyzed.

Date/Time	Event Description
August 22, 2025, 09:00 AM	Notification sent to employees who clicked or submitted credentials, with educational material.
August 23, 2025, 10:00 AM	Security awareness training scheduled for vulnerable departments.

---

4. Incident Description

- Summary:
  A simulated phishing attack was conducted to evaluate employee awareness of phishing tactics. The phishing email impersonated a vendor requesting immediate credential validation.
- Systems Affected:
  No actual systems were compromised. The campaign targeted employee email accounts.
- Detection Method:
  User interaction with the phishing email (clicks and credential submissions) was tracked through the phishing simulation platform.
- Initial Impact Assessment:
  The simulation exposed a vulnerability in user awareness, with a 16.8% click rate and 7.2% credential submission rate among employees.

---

5. Incident Classification

- Type of Incident: Simulated Phishing Exercise
- Severity Level: Low (Controlled Simulation with no real compromise)

---

6. Actions Taken

- Containment:
  No containment needed as the incident was simulated with no real threat.
- Eradication:
  N/A.
- Recovery:
  N/A.

- Communication:
  Employees who interacted with the phishing email were notified promptly with information on recognizing phishing and next steps.

---

7. Mitigation Steps and Recommendations

- Immediate Actions:
  - Deliver targeted security awareness training to employees who interacted with the phishing email.
  - Send organization-wide phishing awareness reminders emphasizing caution with unsolicited emails.
- Long-term Recommendations:
  - Implement regular phishing simulations (quarterly) to continuously assess and improve employee awareness.
  - Enhance email filtering systems to better detect and quarantine phishing emails.
  - Promote a “report phishing” button within email clients to encourage prompt user reporting.
  - Develop and distribute quick-reference phishing identification guides.

---

8. Lessons Learned

- What Went Well:
  The phishing simulation platform effectively tracked user behavior, and notifications to affected employees were timely. The incident reinforced the importance of ongoing security awareness.
- Areas for Improvement:
  Additional emphasis needed on phishing identification, especially in departments with the highest click rates. Consider integrating phishing simulations with broader security training programs.

- **Flowchart Creation:** Diagram of the incident response process (Detection → Containment → Recovery**).**