Incident Response Template

Introduction

This document covers a Mock Phishing Attack report. The report was made according to the Official SANS Incident Response Template format. SANS templates usually structure incidents into sections like Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned.

Mock Phishing Attack

1. Preparation

- Ensure endpoint isolation tools and email security systems are available.
- Maintain a phishing detection checklist: email headers, link reputation, affected users.
- Prepare forensic collection tools: memory dump utilities, logs, and analysis software.

2. Identification

Timestamp	Action
2025-08-18 14:00:00	Alert received for suspicious email
2025-08-18 14:05:00	Analyzed email headers and links for phishing indicators
2025-08-18 14:15:00	Identified potentially affected users

Indicators of Compromise (IoCs):

- Suspicious sender domain
- Malicious URL in email body
- Unusual login attempts from affected users

3. Containment

- Isolated affected endpoint to prevent lateral movement.

- Blocked phishing domain in email filtering and firewall rules.
- Temporarily disabled affected accounts until verified clean.

4. Eradication

- Removed malicious emails from user inboxes.
- Cleared memory and temporary files from impacted systems.
- Reset passwords for affected users as a precaution.

5. Recovery

- Verified endpoint cleanliness and restored network connectivity.
- Re-enabled user accounts and resumed normal operations.
- Monitored for recurring attacks or suspicious activity for 24 hours.

6. Lessons Learned

The simulated phishing incident demonstrated the need for rapid isolation, comprehensive email analysis, and strong employee awareness. Automated link scanning and SIEM alerts can improve response speed. Documenting steps ensures process consistency and highlights areas for continuous improvement.

7. Timeline

Timestamp	Action
2025-08-18 14:00:00	Alert received
2025-08-18 14:30:00	Endpoint isolated
2025-08-18 15:00:00	Email analysed
2025-08-18 15:30:00	Affected users identified
2025-08-18 16:00:00	Domain blocked

8. Investigation Steps

Timestamp	Action
2025-08-18 14:00:00	Isolated endpoint
2025-08-18 14:30:00	Collected memory dump
2025-08-18 15:00:00	Analyzed phishing email
2025-08-18 15:30:00	Identified affected users
2025-08-18 16:00:00	Documented findings

9. Phishing Checklist

- Confirm email headers for authenticity
- Check link reputation via VirusTotal or similar tools
- Identify affected users
- Isolate impacted endpoints
- Collect forensic evidence (memory, logs)
- Block malicious domain and sender
- Notify relevant stakeholders

10. Post-Mortem Summary

The phishing simulation highlighted the value of rapid isolation, meticulous email analysis, and proactive user awareness. Automated link scanning and alerting can reduce response times. Documentation improved repeatability and clarity of processes. Future exercises will refine coordination, enhance checklists, and reinforce phishing detection training across the organization.

End of Mock Phishing Attack report.

References

- https://www.exabeam.com/explainers/incident-response/sans-incident-response-6-step-process-critical-best-practices/
- https://learn.microsoft.com/en-us/defender-office-365/attack-simulation-training-simulations
- https://www.ibm.com/think/topics/phishing-simulation
- https://cdn.fedweb.org/fed-34/2/Cyber-Security-Incident-Response-Template.pdf