🎓 SOC Analyst Incident Response Methodology

Project Title: Documenting Incident Response for a Phishing Email Incident

Student Name: [Your Name]

Date: [Presentation Date]

Scenario: Employee receives a phishing email with a malicious link intended to harvest credentials.

# 🛡️ 1. Initial Response Protocols

Objective: Define clear, step-by-step actions a SOC Analyst takes upon initial detection.

SOC Analyst Actions:

- Monitor SIEM alerts (e.g., Splunk, QRadar) for anomalous email activity.

- Receive user report via internal phishing alert system or email security platform.

- Begin triage: validate authenticity of the alert, pull related logs, identify affected assets.

Phishing-Specific Actions:

- Analyze email headers, attachments, and embedded links.

- Cross-check indicators of compromise (IOCs) with threat intelligence sources.

- Isolate affected endpoints using EDR (e.g., CrowdStrike, SentinelOne).

# 📁 2. Case Management System Components

Objective: Describe tools used for documentation and workflow tracking.

Tools Used: ServiceNow, TheHive, or Jira

|  |  |
| --- | --- |
| Component | Description |
| Incident Ticket | Auto-generated with a unique ID upon detection |
| Categorization | Labeled as 'Phishing' under 'Social Engineering' |
| Severity Rating | Based on asset impact, exposure, and spread potential |
| Assignment | Routed to Tier 2 SOC Analyst for in-depth investigation |
| Time-stamped Actions | All analyst actions logged (detection, analysis, containment) |
| Final Resolution Report | Includes summary, remediation steps, and timeline |

# 📈 3. Incident Escalation Criteria

Objective: Define thresholds and procedures for escalation and communication.

Escalation Criteria:

- Affected asset is critical (e.g., executive email account).

- Evidence of data exfiltration or credential use.

- Threat actor is persistent or targeting multiple users.

- Compliance or legal obligations are triggered.

Escalation Path: Tier 1 SOC → Tier 2 SOC → IR Team → Management / Legal / CISO

Communication Protocols:

- Slack/MS Teams (MFA-enabled) for secure internal updates.

- Encrypted email for compliance or legal contact.

- Emergency bridge call if lateral movement or data loss is detected.

# 🧭 4. Decision Points

Objective: Identify and document key moments requiring SOC decisions.

|  |  |
| --- | --- |
| Decision Point | Action Taken |
| Is the alert a true positive? | If not, close ticket with documented justification. |
| Is containment required? | If yes, isolate device, disable affected accounts. |
| Is there external communication? | Notify Legal/PR for breach communication planning. |
| Is recovery immediately possible? | If not, escalate to IR team for full remediation. |

# 📋 5. Completed Incident Documentation Template

Incident Type: Phishing Email

Date Detected: April 29, 2025

Detected By: SIEM Alert + User Report

Assets Affected: john.doe@company.com - Workstation ID #2457

Containment Actions:

- Endpoint isolated from the network.

- Malicious sender domain blocked at email gateway and firewall.

Eradication & Recovery:

- Phishing email removed from all user inboxes.

- User coached on recognizing phishing attempts.

Post-Incident Actions:

- IOCs submitted to threat intel platform.

- Weekly metrics updated to include incident.

- Final ticket closed with full resolution report.

# 🧠 6. Incident Response Principles & Best Practices

Framework Used: NIST SP 800-61 Revision 2 — Computer Security Incident Handling Guide

|  |  |
| --- | --- |
| Phase | Actions Taken |
| Preparation | Email filtering enabled; phishing simulation training active |
| Detection & Analysis | Alert triage, IOC verification, endpoint log analysis |
| Containment & Eradication | Isolate device, delete malicious email, block domains |
| Recovery | Restore affected system, monitor user activity |
| Post-Incident Activity | Conduct review, update playbooks, brief stakeholders |

# ✅ Summary of Submission Goals Met

|  |  |
| --- | --- |
| Requirement | Addressed in Project? |
| Initial Response Protocols | ✅ |
| Case Management System Descriptions | ✅ |
| Incident Escalation Criteria & Communications | ✅ |
| Clear Decision Points | ✅ |
| Complete Response Documentation Template | ✅ |
| Demonstrated Understanding of IR Principles | ✅ |