Justin Lew

SOC Incident Response Playbook

Incident Type: Phishing Attack

1. Incident Identification and Reporting

- **Trigger:** User reports a suspicious email or system alerts detect phishing activity.
- **Initial Triage:**
    - SOC Analyst reviews the email header, sender details, and embedded URLs for indicators of compromise (IoC).
    - Use email security tools (e.g., Proofpoint, Mimecast) to analyze email behavior.
    - Verify if the domain is newly registered or associated with known phishing campaigns.
- **Incident Classification:**
    - **Spam:** No response needed.
    - **Phishing Attempt:** Proceed with containment.
    - **Credential Harvesting:** Escalate to threat response team.
    - **Malicious Attachment:** Quarantine and scan with sandboxing tools.

2. Containment and Mitigation

- **Immediate Actions:**
    - Block sender domain and flagged URLs in email security gateway.
    - Quarantine email across all inboxes using Microsoft Defender or Google Workspace.
    - Force password resets for impacted users and monitor account activity.
    - Disable compromised accounts if unauthorized activity is detected.
    - Alert all employees about ongoing phishing attempts and provide security guidance.
- **Network-Level Mitigation:**
    - Apply firewall rules to block access to known phishing sites.
    - Update IDS/IPS rules to detect similar phishing patterns.
    - Enable two-factor authentication (2FA) for affected users.
- **User Awareness:**
    - Notify affected employees with security awareness tips.
    - Provide mandatory phishing detection training within the next 30 days.

3. Investigation and Analysis

- **Forensic Examination:**
    - Analyze email headers and metadata for anomalies (SPF, DKIM, DMARC failures).
    - Check URLs and attachments using sandboxing tools like Cuckoo Sandbox or VirusTotal.
    - Extract and analyze payloads from attachments to determine malware involvement.
    - Identify any compromised accounts through SIEM login logs (Splunk, QRadar, ELK Stack).
- **Threat Intelligence Correlation:**
    - Cross-reference IoCs with threat intelligence feeds (AlienVault OTX, MITRE ATT&CK).
    - Determine if this attack is part of a larger phishing campaign.
    - Engage with external cybersecurity vendors if needed for deeper analysis.

4. Eradication and Recovery

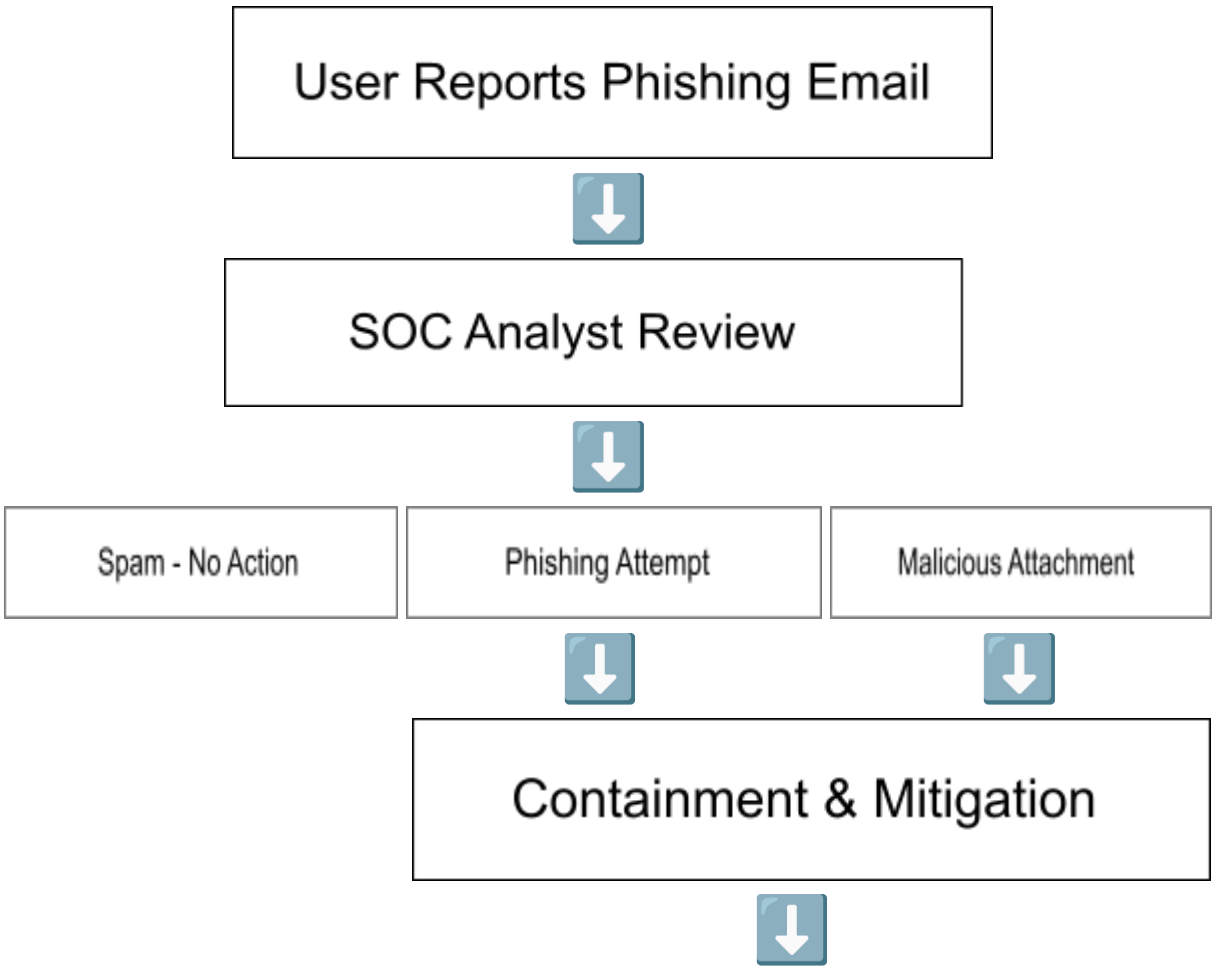
- **Incident Resolution:**
    - Remove all malicious emails from user inboxes using admin tools.
    - Conduct a mandatory password reset for affected users and implement stronger authentication policies.
    - Apply patches and update email security configurations to prevent future attacks.
- **Infrastructure Hardening:**
    - Enable stricter email security policies (SPF, DKIM, DMARC enforcement).
    - Restrict email forwarding rules to prevent auto-forwarding of emails to external addresses.
    - Implement domain monitoring tools to detect spoofed domains targeting employees.

5. Post-Incident Activities

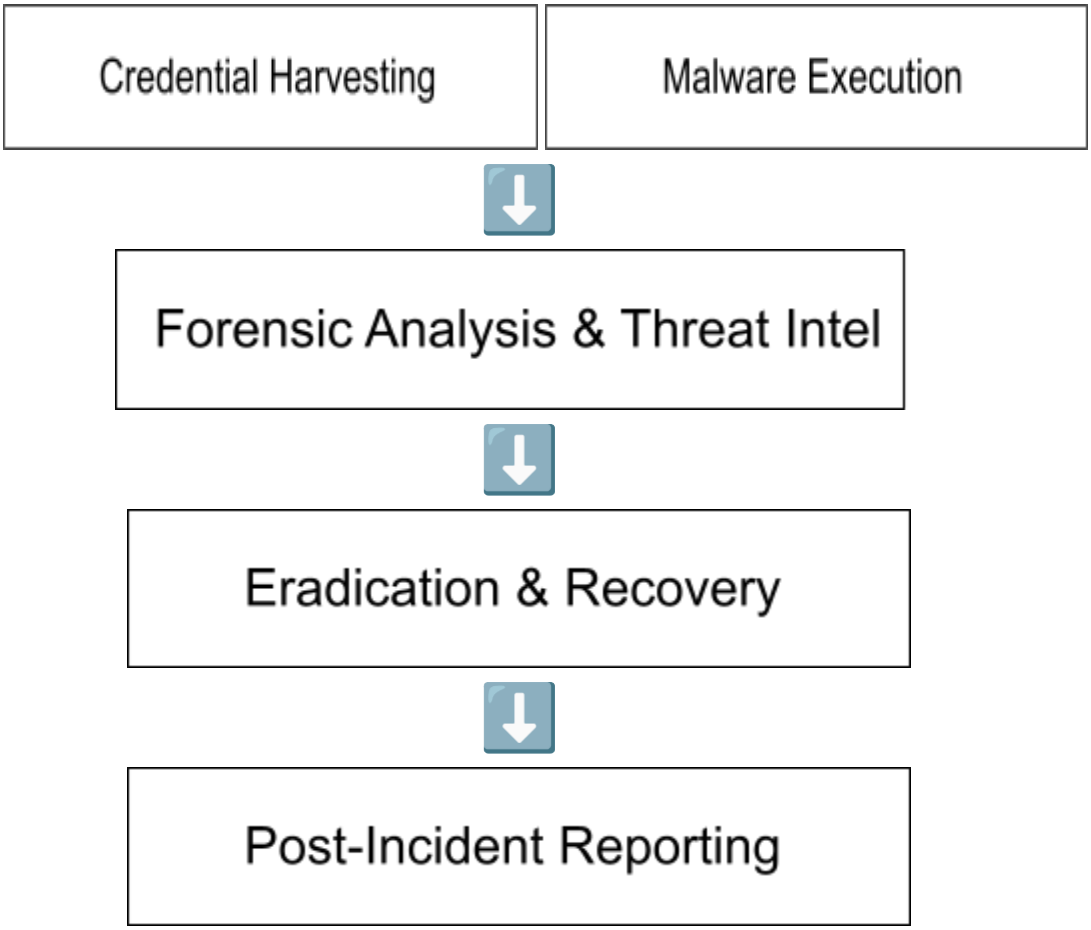
- **Documentation and Reporting:**
    - Log the incident details in the SOC incident management system (ServiceNow, TheHive, Splunk).
    - Generate a detailed incident report outlining IoCs, affected users, and response actions.
    - Conduct a debrief with all stakeholders, including IT, security, and leadership teams.
- **Lessons Learned:**
    - Conduct a retrospective analysis with incident response and SOC teams.

    - Update the SOC Incident Playbook based on findings and new attack vectors.
    - Schedule periodic phishing simulation exercises to assess employee awareness.
- **KPI Tracking:**
    - Mean Time to Detect (MTTD) – Time taken from email receipt to analyst review.
    - Mean Time to Respond (MTTR) – Time taken from identification to containment.
    - Containment Success Rate – Percentage of incidents mitigated before user interaction.
    - User Awareness Score – Improvement in phishing simulation results post-incident.
    - Incident Recurrence Rate – Number of repeated phishing incidents over six months.

Escalation Flowchart



Justin Lew



1. **User Reports Phishing Email**
    - The incident response process starts when an employee or system alerts the SOC team about a potential phishing email.

2. **SOC Analyst Review**
    - A SOC analyst reviews the email, checking its headers, links, attachments, and any anomalies that might indicate a phishing attempt.

3. **Classification Stage**
    - Based on the review, the email is classified into one of three categories:
        - **Spam:** No security threat detected. No further action required.
        - **Phishing Attempt:** Email contains malicious links or deceptive content meant to trick users. Proceed to containment.

        - **Malicious Attachment:** The email contains a suspicious attachment that could deliver malware. Quarantine and analyze the file.

4. **Containment & Mitigation**
    - If the email is classified as a **Phishing Attempt**, it moves to containment measures like blocking the sender, removing the email from inboxes, and alerting employees.
    - If it involves **Credential Harvesting**, the SOC will reset affected users' passwords and check for suspicious login activity.
    - If it contains **Malware Execution**, the team investigates whether any users opened the attachment and takes necessary remediation steps.

5. **Forensic Analysis & Threat Intelligence**
    - The SOC team examines logs, correlates indicators of compromise (IoCs) with known threat intelligence databases, and determines if this is part of a larger campaign.

6. **Eradication & Recovery**
    - Steps are taken to remove malicious emails, update security policies (e.g., DMARC, SPF, DKIM enforcement), and strengthen defenses to prevent recurrence.

7. **Post-Incident Reporting**
    - The final stage involves documentation, reporting findings, and conducting a review to improve future phishing defenses.

Justin Lew

RACI Matrix for Phishing Incident Response

Task	Responsible	Accountable	Consulted	Informed
Initial Triage	SOC Analyst	SOC Lead	IT Admin	CISO
Email Blocking	Email Security	SOC Lead	IT Admin	CISO
Sandboxing Malicious Files	Threat Intel Team	SOC Lead	IT Admin	CISO
Password Resets	IT Admin	SOC Lead	HR	Employees
Incident Reporting	SOC Analyst	SOC Lead	Legal	CISO
Security Awareness Training	IT Security	CISO	HR	Employees
SIEM Log Analysis	Threat Intel Team	SOC Lead	IT Admin	SOC Team
Phishing Simulation Deployment	Security Awareness Team	CISO	HR	Employees

---

Key Performance Indicators (KPIs)

- **Detection Time:** Time taken from email receipt to analyst review.
- **Response Time:** Time taken from identification to containment.
- **Containment Success Rate:** Percentage of incidents contained before user interaction.
- **User Awareness Score:** Improvement in phishing simulation results.
- **Incident Recurrence Rate:** Number of repeated phishing incidents over six months.
- **False Positive Rate:** Percentage of non-malicious emails incorrectly flagged as phishing.