Phishing Alert Investigation and Escalation – SOC Playbook Response

Objective

The purpose of this lab was to simulate the process of responding to a phishing alert as a Level-1 Security Operations Center (SOC) analyst. The exercise followed an organizational Phishing Playbook, including steps for evaluating alerts, identifying indicators of compromise (IoCs), and determining whether to escalate or close a ticket based on severity and evidence.

Scenario Overview

A phishing alert was generated after an employee at a financial services company downloaded a password-protected spreadsheet attachment from a suspicious email. Upon investigation, the attachment's SHA256 hash matched a known malicious file previously verified through VirusTotal. The analyst must now document findings, determine the appropriate escalation path using the Phishing Playbook, and update the alert ticket with investigation results.

Tools and Resources Used

• Tools: Incident Handler's Journal, Alert Ticket Template, VirusTotal, Phishing Playbook and Flowchart
• Frameworks: Incident Response Lifecycle, SOC Triage Procedures

Step 1: Evaluate the Alert

Attribute	Description
Alert Severity	High
Sender	accounts@financesecure-support.com (spoofed domain)
Subject Line	Urgent Account Update – Verify Immediately
Attachment	Update_Report.xls (password-protected)
File Hash (SHA256)	54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b
Hash Result (VirusTotal)	32 vendors flagged as malicious

5 W's Analysis

• **Who:** The incident was caused by a malicious actor impersonating a financial institution.
• **What:** A phishing email containing a malicious attachment executed malware upon opening.
• **When:** Occurred at approximately 1:20 p.m.
• **Where:** On an employee workstation within the company network.
• **Why:** The attacker aimed to deploy malware to gain access or steal data.

Assessment: The alert is legitimate and demonstrates clear signs of phishing and malware execution.

Step 2: Determine Whether the Alert Should Be Escalated

According to the Phishing Playbook, escalation is warranted when:
- The email contains verified malicious attachments or URLs.
- The malware was executed successfully on a host.
- Unauthorized processes or outbound connections are observed.

All of these conditions were met. Therefore, the alert should be escalated to the Incident Response (IR) Team for containment and remediation.

Step 3: Update the Alert Ticket

Ticket Field	Update
Ticket Status	Escalated
Ticket Comments	A phishing alert was received involving a malicious Excel attachment. The attachment’s SH
Reasoning	1. The attachment was verified as malicious through multiple AV vendors. 2. The payload executed unauthorized processes on the endpoint. 3. Potential C2 communication was detected during sandbox analysis.

Summary of Findings

- The phishing attempt involved a spoofed sender domain, urgent subject line, and password-protected malicious attachment.
- VirusTotal confirmed the file’s malicious nature.
- The alert met all escalation criteria in the organization’s Phishing Response Playbook.

Cybersecurity Relevance

This lab demonstrates real-world SOC capabilities including phishing email analysis, alert triage and escalation, documentation and ticket handling, and coordination with IR teams. These skills directly align with Tier-1 SOC Analyst and Cybersecurity Operations roles.

Key Takeaway

Through this activity, I learned to evaluate phishing alerts systematically, apply a structured playbook for decision-making, accurately document incident findings, and coordinate escalation for effective incident response.