Scenario 2: Follow-Up Analysis and Actions

You are a level-one security operations centre (SOC) analyst at a financial services company. Previously, you received a phishing alert about a suspicious file being downloaded on an employee's computer. After investigating the email attachment file's hash, the attachment has already been verified malicious. Now that you have this information, you must follow your organization's process to complete your investigation and resolve the alert.

Your organization's security policies and procedures describe how to respond to specific alerts, including what to do when you receive a phishing alert.

In the playbook, there is a flowchart and written instructions to help you complete your investigation and resolve the alert. At the end of your investigation, you will update the alert ticket with your findings about the incident.

Date: **July 27 2024**.	**Entry:** # 2
Description	An investigation was conducted into an alert ticket involving a phishing attempt. The structured response plan, outlined in the organization's playbook, provided guidance through the incident response lifecycle. This systematic approach ensured a coordinated and thorough resolution of the issue while minimizing its impact.
Tool(s) used	• **Playbook:** Guided the response process and ensured adherence to best practices. • **Virus Total:** Verified the malicious file by analyzing the SHA-256 hash. • **Alert Ticket System (JIRA):** Tracked the incident's progress and facilitated communication between team members.

The 5 W's	• **Who:** A malicious cybercriminal claiming to be Clyde West initiated the attack. • **What:** A phishing email with a malicious file attachment (SHA-256 hash:`54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b`) was sent to an employee. • **Where**: The incident occurred on an employee's computer at Inergy, a financial services company. • **When**: Detected by the organization's intrusion detection system on August 31, 2024, at 6:30 a.m. • **Why**: The attacker, posing as a prospective employee, aimed to steal sensitive information or deploy malicious software by sending a password-protected executable disguised as a resume.
Additional notes	**Preventative Measures:** 1. Train employees to recognize and report suspicious emails. 2. Conduct regular phishing simulations and improve security awareness programs. 3. Escalate similar incidents to Level 2 SOC Analysts for detailed analysis and mitigation. 4. Update the organization's playbook to incorporate lessons learned and refine response strategies.

Scenario 2: Follow-Up Analysis and Actions	This incident demonstrated the critical role of preparation in mitigating cybersecurity threats. The playbook provided a clear framework for response, ensuring efficiency across all phases of the investigation. However, the incident also revealed a gap in employee awareness, as

	the phishing email initially bypassed human scrutiny. Virus Total played a key role in confirming the malicious nature of the file, while JIRA facilitated seamless collaboration and progress tracking. Moving forward, refining employee training programs and enhancing the playbook with insights gained from this incident will be essential. Additionally, involving higher-level analysts early in the response process can ensure a more thorough investigation, reducing the risk of escalation.

Ticket ID	Alert Message	Severity	Details	Ticket status
A-2703	SERVER-MAIL Phishing attempt possible download of malware	Medium	The user may have opened a malicious email and opened attachments or clicked links.	**Escalated**

Ticket comments
The alert revealed that an employee had downloaded and opened a malicious file from a phishing email. Upon analysis, several inconsistencies were identified: the sender's email address, "76tguy6hh6tgftrt7tg.su," did not match the name referenced in the email body, "Clyde West," or the sender's displayed name, "Def Communications." Additionally, the email contained grammatical errors in both the subject line and body.

The email also included a password-protected attachment named “bfsvc.exe,” which the employee downloaded and executed on the affected machine. A hash analysis of the file confirmed it as a known malicious executable. The alert severity was classified as medium.

Based on these findings, I escalated the ticket to a Level 2 SOC analyst for further investigation and appropriate action to ensure a thorough response.

Additional information

Known malicious file hash:

`54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b`

Email:

From: Def Communications <76tguyhh6tgftrt7tg.su> <114.114.114.114>

Sent: Wednesday, July 20, 2022 09:30:14 AM

To: <hr@inergy.com> <176.157.125.93>

Subject: Re: Infrastructure Egnieer role

Dear HR at Ingergy,

I am writing for to express my interest in the engineer role posted from the website.

There is attached my resume and cover letter. For privacy, the file is password protected. Use the password paradise10789 to open.

Thank you,

Clyde West

Attachment: filename="bfsvc.exe"