**Incident handler's journal Entry 3**

**Instructions**

You are a level-one security operations center (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:**  10/21/2023 | **Entry:**  Entry 3 |
| Description | Use a playbook to respond to a phishing incident |
| Tool(s) used | Phishing SOC1 Play Book/Flowchart, and Alert Ticket |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? The sender of the email, Clyde West, is likely not a legitimate Ingergy employee. * **What** happened? The user may have opened the malicious attachment (bfsvc.exe) in the email. * **When** did the incident occur? The email was sent on Wednesday, July 20, 2022 at 09:30:14 AM. * **Where** did the incident happen? The incident occurred on the user's computer. * **Why** did the incident happen? The user may have been tricked into opening the malicious attachment by the sender's impersonation of a legitimate Ingergy employee. |
| Additional notes | Assessment:  Based on the initial findings, it is likely that this is a legitimate phishing alert. The sender's email address, IP address, and the attachment's hash are all indicators of a phishing attempt. Additionally, the email is poorly written and contains grammatical errors, which are common in phishing emails.  Next Steps:  Update the alert ticket with the findings of this investigation.  Escalate the ticket to a level-two SOC analyst for further investigation.  Notify the user of the phishing attempt and advise them to not open any attachments or click on any links in emails from unknown senders.  Scan the user's computer for malware.  Update the organization's security awareness training to include information about phishing attempts. |