Ticket Status: Escalated

Ticket Comments:
After reviewing the alert details, I have determined that the phishing alert is legitimate and should be escalated for further investigation.

Findings:

1. **Verified Malicious Attachment**
    - The SHA256 hash of the email attachment was checked using VirusTotal and flagged as malicious by multiple security vendors.
    - The attachment contained a password-protected spreadsheet that executed a malicious payload when opened.
2. **Indicators of Compromise (IoCs) Identified**
    - The malicious file contacted known malicious IP addresses and domain names, indicating potential command-and-control (C2) communication.
    - Unauthorized executable files were created on the employee's computer after opening the attachment, confirming post-execution activity.
3. **Potential Compromise of Employee's System**
    - The timeline of events shows that the malware executed shortly after the file was opened, suggesting that the employee's machine may have been compromised.
    - Further forensic analysis is required to determine the extent of the compromise and mitigate any risks to the organization's network.

Next Steps:

- **Immediate containment:** Isolate the affected system to prevent further network spread.
- **Incident response team involvement:** The case should be escalated for deeper forensic analysis and remediation.
- **User awareness and training:** The employee should be informed about the incident to prevent similar occurrences in the future.

Step 1: Receive phishing alert

- The alert ticket was received, indicating that a phishing attempt was detected.

Step 2: Evaluate the alert

- The **alert severity** was assessed. Since the presence of a malicious attachment was confirmed, the alert was treated as a high-severity case.
- **Receiver details** were checked to identify the impacted user.
- **Sender details** were analyzed to detect inconsistencies (such as spoofing or impersonation).
- **Subject line and message body** were reviewed for indicators of phishing (e.g., grammatical errors, urgency tactics).
- **Attachments or links** were identified, and the attachment was confirmed malicious through a file hash lookup.

Step 3.0: Does the email contain any links or attachments?

- **Yes,** the email contained an attachment. The investigation proceeded to Step 3.1.

Step 3.1: Are the links or attachments malicious?

- The attachment's **hash was checked using VirusTotal**, confirming it as malicious.
- **Indicators of Compromise (IoCs)** were identified, suggesting the potential for system compromise.

Step 3.2: Update the alert ticket and escalate

- Since the attachment was **verified as malicious**, the alert ticket was **updated and escalated** to a level-two SOC analyst.
- A **summary of findings** was provided, including:
    1. The attachment was confirmed as malicious.
    2. Indicators of compromise were detected.
    3. The affected system may be compromised and requires immediate response.

Step 4: Close the alert ticket (Not Applicable in this case)

- The ticket was **not closed** because it contained a malicious attachment, requiring escalation instead.