Scenario

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.

Steps

Step 1: Review the playbook and flowchart

Before you begin investigating the alert, take a moment to review the playbook and flowchart because you'll be using them throughout the investigation.

The **Phishing Playbook** instructions provide detailed, written instructions about each step represented in the flowchart.

The **Phishing Flowchart** provides a high-level overview and visual representation of the sequence of steps and substeps you'll take to respond to a phishing alert.

Step 2: Update the alert ticket status

In the **Alert ticket** template, begin the investigation by updating the **Ticket status** dropdown list to **Investigating**.

Step 3: Evaluate the alert

For this exercise, begin with the second step in the playbook, **Evaluate the alert**, because you've already received and accessed the phishing alert ticket.

As a security analyst, you'll want to gain a complete understanding of why the alert was triggered. Create a new entry in your incident handler's journal to record the details of this security incident and gather your thoughts. You'll refer to these notes as you progress through the steps in the playbook.

Then, evaluate the contents of the **Alert ticket**, including the content in the **Additional information** section. Here are some examples of elements to examine when you are evaluating the alert ticket details:

- **Alert severity**: According to the playbook instructions, an alert severity of Medium or High is a good indication that a ticket might require escalation.
- **Sender Details**: Analyzing the sender details of an email is important because it can reveal inconsistencies that can indicate a phishing attempt. Often, phishing emails try to impersonate trusted entities. For example, if there is a mismatch between the sender's email address and the sender's name, this is a good indication that the email might be a phishing email.
- **Message body**: It's important to analyze the message body (and subject line) of an email because phishing emails often contain grammatical errors, which can be an indication of a phishing attempt.
- **Attachments or links**: Phishing emails contain malicious links or attachments that are used to steal sensitive information or download malicious software or code on the recipient's device. Check to see whether a file has been attached to this email.

After you've evaluated the contents of the alert ticket, answer the 5 W's of this incident to gather the information you need to understand the nature of the alert. **The 5 W's are**:

- Who caused the incident?
- What happened?
- When did the incident take place?
- Where did the incident occur?
- Why did it happen?

At the end of this step, you should have 2-3 reasons on why you believe the phishing alert is or isn't legitimate.

Step 4: Determine whether the alert should be escalated

After evaluating the alert details, use the Phishing Playbook's **Step 3.0** and **Step 3.1** to determine whether the email contains links or attachments and whether these links or attachments are malicious. Remember you've already determined that the email contains an attachment that has been verified as malicious through its file hash.

Proceed to the Phishing Playbook's **Step 3.2** if you've determined that the alert should be escalated. If you've determined that the alert should not be escalated, proceed to the Phishing Playbook's **Step 4**.

Step 5: Update the alert ticket status

Now that you've examined the email details, complete the final step of the playbook and update the alert ticket in the activity template. Depending on whether you want to escalate or close the alert:

- Under the **Ticket status** column of the alert ticket template, update the status of the ticket to either **Closed** or **Escalated**.
- Under the **Ticket comments** column of the alert ticket template, use the details you've found to explain the steps taken and why you chose to escalate or close the ticket. Include 2-3 reasons as to why you believe this alert should be escalated or closed.

Be sure to address the following steps:

- In the Alert ticket, update the Ticket status column using the dropdown list.
- In the Ticket comments section in the Alert ticket, provide a sentence briefly describing the alert and what happened.
- In the Ticket comments section in the Alert ticket, provide 2-3 sentences describing the reasons why you chose to escalate or close the ticket. Support your reasons using specific details from the alert ticket.