Process to respond to a phishing incident

**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.

**Information about the Ticket:**

**Known malicious file hash**: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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. | **Open** |

Every organization has their own playbooks designed to follow the steps of closing the Incident. I am using Google’s Playbook as part of my Certification process

**StepsA screenshot of a computer screen

Description automatically generated from playbook:**

|  |  |
| --- | --- |
| **Date:**  Wednesday, July 20, 2022 09:30:14 AM | **Entry:**  #1 |
| Description | Threat actors sends a Phishing email with attachment which triggered the Incident |
| Tool(s) used | Virus Total to detect if the file has any malware |
| The 5 W's | * **Who** caused the incident? Employee of organization and threat actor * **What** happened? Malware was installed into a system * **When** did the incident occur? Wednesday, July 20, 2022 09:30:14 AM * **Where** did the incident happen? Inergy organization * **Why** did the incident happen? Employee misinterpreted malicious email with legitimate email |
| Recommendations | Employee awareness training benefits in avoiding such risks |

By using the Incident response handlers and the steps in the playbook, we are escalating this issue further.

**Ticket Closing Comments:** The alert detected that an employee downloaded and opened a malicious file from a phishing email. There is an inconsistency between the sender’s email address “76tguy6hh6tgftrt7tg.su’” the name used in the email body “Clyde West,” and the sender’s name, “Def Communications.” The email body and subject line contained grammatical errors. The email’s body also contained a password-protected attachment, “bfsvc.exe,” which was downloaded and opened on the affected machine. Having previously investigated the file hash using Virus Total. It is confirmed to be a known malicious file. Furthermore, the alert severity is reported as medium. With these findings, I chose to escalate this ticket to a level-two SOC analyst to take further action.