## Task:

In this activity, you will respond to a phishing incident that involves a malicious file hash. You'll follow playbook instructions to investigate and resolve the incident's alert ticket.

## 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.

| **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 flagged an employee who downloaded and opened a malicious file from a phishing email. There was a mismatch between the sender's email address, "76tguy6hh6tgftrt7tg.su," the name in the email body, "Clyde West," and the sender's name, "Def Communications." Additionally, the email contained grammatical errors in both the body and subject line. The body of the email also included a password-protected attachment, "bfsvc.exe," which was downloaded and opened on the affected machine. After confirming the file hash was known |

to be malicious, and noting the alert's medium severity, I decided to escalate this ticket to a level-two SOC analyst for further investigation.

## 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"