Escenario

Revisa el siguiente escenario. Luego, completa las instrucciones paso a paso.
Eres analista de nivel uno del centro de operaciones de seguridad (SOC) en una empresa de servicios financieros. Anteriormente, recibiste una alerta de phishing sobre la descarga de un archivo sospechoso en la computadora de un empleado. Al investigar el hash del archivo adjunto del correo electrónico, se verificó que este es malicioso. Ahora, que dispones de esta información, debes seguir el proceso de tu organización para completar la investigación y resolver la alerta.
Las políticas y procedimientos de seguridad de la empresa para la que trabajas describen cómo responder a alertas específicas, incluyendo qué hacer cuando recibes una de phishing. En el manual de estrategias, se detalla un diagrama de flujo e instrucciones que te ayudarán a completar la investigación y resolver la alerta. Al final de tu investigación, actualizarás el ticket con tus conclusiones sobre el incidente.

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

Ticket comments
Insert your comments here.

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"

Paso 1: Evaluar la alerta

Datos del ticket:

- **Ticket ID**: A-2703
- **Mensaje de alerta**: SERVER-MAIL Phishing attempt, possible download of malware
- **Gravedad**: Media
- **Detalles**: El usuario puede haber abierto un correo electrónico malicioso con un archivo adjunto o enlace malicioso.
- **Información adicional**:
    - **Hash del archivo malicioso**: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b
    - **Remitente del correo**: Def Communications <76tguyhh6tgftrt7tg.su>
    - **Destinatario**: hr@inergy.com
    - **Asunto**: Infrastructure Engineer role
    - **Adjunto**: **bfsvc.exe** (malicioso)

Evaluación de la alerta:

- **Gravedad**: Media, lo que indica que debe tener prioridad para evitar posibles daños.
- **Datos del remitente**: Inconsistencia entre el nombre del remitente ("Def Communications") y el dominio del correo electrónico <76tguyhh6tgftrt7tg.su>, lo que sugiere un intento de suplantación.
- **Cuerpo del correo**: Errores gramaticales y una solicitud inusual de un archivo protegido por contraseña sugieren un intento de phishing.
- **Adjunto malicioso**: El archivo adjunto **bfsvc.exe** ha sido identificado como malicioso por su hash SHA256, lo que confirma la amenaza.

5 W del incidente:

- **Quién**: El remitente **Def Communications** con una dirección de correo sospechosa.
- **Qué**: Intento de phishing con un archivo adjunto malicioso.
- **Cuándo**: 20 de julio de 2022.
- **Dónde**: El incidente ocurrió en el sistema de correo de la empresa.
- **Por qué**: El correo intentaba engañar al destinatario para que descargara un archivo malicioso.

Paso 2: Determinación de la acción

El archivo adjunto se verificó como malicioso a través de su hash. Siguiendo los procedimientos de la organización, es necesario **elevar** este ticket a un nivel superior, ya que implica un posible acceso no autorizado y descarga de malware.

Paso 3: Actualización del ticket

- **Estado del ticket**: **Elevado**
- **Comentarios del ticket**:
    - Se ha recibido un correo de phishing con un archivo adjunto malicioso identificado como **bfsvc.exe**. El hash del archivo (SHA256: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b) confirma que es malicioso.
    - **Razones para elevar**:
        1. El correo proviene de una dirección sospechosa con inconsistencias en su dominio.
        2. El archivo adjunto ha sido verificado como malicioso, lo que representa una amenaza potencial significativa.
        3. Se necesita intervención de un equipo de nivel superior para realizar una contención adecuada y garantizar que el malware no haya causado daños adicionales.