Contexto

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.