Activity Overview

In this activity, you will respond to a phishing incident that involves a malicious file hash. This is the same SHA256 file hash you investigated and verified as malicious in a previous activity. You'll follow playbook instructions to investigate and resolve the incident's alert ticket.

Previously, you learned how playbooks outline the step-by-step actions necessary to properly respond to a security incident. Coordinated, effective, and quick action is critical during incident response. A playbook can help security teams minimize the impact of an incident and reduce the incident response time. As a security analyst, playbooks can help guide you to support an organization’s incident response efforts effectively.

Scenario

Review the 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 maliciously. 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.

The playbook has 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.

Note: *Use the incident handler's journal you started in a previous activity to take notes during the activity and keep track of your findings.*