Step-By-Step Instructions

Follow the instructions and fill in the sections to complete the activity.

Part 1 - Access your incident handler's journal

To complete this activity, you'll need to access your incident handler's journal. If you have saved your incident handler's journal, open it now and keep it open throughout this activity.

Step 2: Review your journal entries

You might have multiple entries in your incident handler's journal. If your journal contains missing or incomplete entries, go back and review any previous sections of this course to add additional log entries to your journal. Here's a list of the course activities you can revisit to complete your journal:

- Activity: Document an incident with an incident handler's journal
- Activity: Analyze your first packet
- Activity: Capture your first packet
- Activity: Investigate a suspicious file hash
- Activity: Use a playbook to respond to an attack
- Activity: Review a final report
- Activity: Explore signatures and logs with Suricata
- Activity: Perform a query with Splunk
- Activity: Perform a query with Chronicle

At a minimum, you should have the following entries in your incident handler's journal:

- *At least* 4 dated and numbered journal entries, including:
    - 2 journal entries documenting an incident investigation using the 5 W's
    - 2 journal entries describing the use of a cybersecurity tool

Review your incident handler's journal and make any necessary changes. Here are some things to consider during your review:

- Errors in grammar, punctuation, and spelling
- Missing, inaccurate, or incomplete journal entries

Step 2: Review the scenario

Review the details of the scenario. Consider the following key details:

- A small U.S. health care clinic experienced a security incident on Tuesday at 9:00 a.m. which severely disrupted their business operations.

- The cause of the security incident was a phishing email that contained a malicious attachment. Once it was downloaded, ransomware was deployed encrypting the organization's computer files.

- An organized group of unethical hackers left a ransom note stating that the company's files were encrypted and demanded money in exchange for the decryption key

Step 3: Update your journal entries

Update the journal entries that record an incident investigation.

In the **Description** section in a journal entry in your incident handler's journal, include a brief description of the entry (20-50 words). You can also identify which phase(s) of the NIST Incident Response Lifecycle the incident investigation occurred in and why. As a refresher, the phases are: *Preparation; Detection and Analysis; Containment, Eradication, and Recovery; and Post-Incident Activity*.

Part 2 - Complete your incident handler's journal

Step 1: Write a reflection entry

Take a moment to reflect on your learning journey in this course so far. Copy and paste the following questions into the Reflections/Notes section in your incident handler's journal. Then, write a two to three sentence response (40-60 words) to each question.

1. Were there any specific activities that were challenging for you? Why or why not?

2. Has your understanding of incident detection and response changed since taking this course?

3. Was there a specific tool or concept that you enjoyed the most? Why?

What to Include in Your Response

Be sure to include the following in your completed activity:

- 4 completed journal entries, with the **Date**, **Entry**, and **Description** section filled in (50-80 words)

- 2 of the 4 entries document an incident investigation in the **5 W's** section (4-6 sentences or bullet points)

- 2 of the 4 entries outline the use of a cybersecurity tool in the **Tool(s) used** section (3-5 sentences or bullet points)

- The **Reflections/Notes** section addresses the reflection prompt (6-9 sentences or bullets)

Note: *Some of these items may be addressed in the same journal entry. For example, a journal entry might contain descriptions of a cybersecurity tool and the 5 W's of an incident.*