Portfolio Activity: Document an incident with an incident handler's journal

In this activity, you will review the details of a security incident and document the incident using your incident handler's journal. Previously, you learned about the importance of documentation in the incident response process. You've also learned how an incident handler's journal is used to record information about security incidents as they are handled.

Throughout this course, you can apply your documentation skills using your incident handler's journal. With this journal, you can record information about the experiences you will have analyzing security incident scenarios through the course activities.

By the time you complete this course you will have multiple entries in your incident handler's journal that you can use as a helpful reference to recall concepts and tools. Later, you'll add this document to your cybersecurity portfolio, which you can share with prospective employers or recruiters. To review the importance of building a professional portfolio and options for creating your portfolio, read Create a cybersecurity portfolio.

Be sure to complete this activity and answer the questions that follow before moving on. The next course item will provide you with a completed exemplar to compare to your own work.

Note: *You can use your incident handler's journal as a personal space where you can keep track of your learning journey as you learn about incident detection and response concepts and interact with different cybersecurity tools. Feel free to include your thoughts, reflections, and any other important details or information.*

Scenario

Review the following scenario. Then complete the step-by-step instructions.

A small U.S. health care clinic specializing in delivering primary-care services experienced a security incident on a Tuesday morning, at approximately 9:00 a.m. Several employees reported that they were unable to use their computers to access files like medical records. Business operations shut down because employees were unable to access the files and software needed to do their job.

Additionally, employees also reported that a ransom note was displayed on their computers. The ransom note stated that all the company's files were encrypted by an organized group of unethical hackers who are known to target organizations in healthcare and transportation industries. In exchange for restoring access to the encrypted files, the ransom note demanded a large sum of money in exchange for the decryption key.

The attackers were able to gain access into the company's network by using targeted phishing emails, which were sent to several employees of the company. The phishing emails contained a malicious attachment that installed malware on the employee's computer once it was downloaded.

Once the attackers gained access, they deployed their ransomware, which encrypted critical files. The company was unable to access critical patient data, causing major disruptions in their business operations. The company was forced to shut down their computer systems and contact several organizations to report the incident and receive technical assistance.

Step-By-Step Instructions

Follow the instructions to complete each step of the activity. Then, answer the 5 questions at the end of the activity before going to the next course item to compare your work to a completed exemplar.

Step 1: Access the template

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: Record a journal entry

Use the incident handler's journal to document your first journal entry about the given scenario. Ensure that you fill in all of the fields:

1. In the Date section, record the date of your journal entry. This should be the actual date that you record the entry, not a fictional date.
2. In the Entry section, provide a journal entry number. For example, if it is your first journal entry, enter 1.
3. In the Description section, provide a description about the entry.
4. In the Tool(s) used section, if any cybersecurity tools were used, list them here.
5. In the The 5 W's section, record the details about the given scenario.
    a. Who caused the incident?
    b. What happened?
    c. When did the incident occur?
    d. Where did the incident happen?
    e. Why did the incident happen?
6. In the Additional notes row, record any thoughts or questions you have about the given scenario.

Pro Tip: Save a copy of your work

Finally, be sure to save a copy of your incident handler's journal so that you can quickly access it as you progress through the course. You can use it for your professional portfolio to demonstrate your knowledge and/or experience to potential employers.

What to Include in Your Response

Be sure to include the following elements in your completed activity:

- The journal entry date and number
- A description of the journal entry
- 1-2 sentences addressing each of the 5 W's of the scenario:
    - Who caused the incident?
    - What happened?
    - When did the incident occur?

    - Where did the incident happen?
    - Why did the incident happen?
- 1-2 sentences on any additional thoughts or questions about the scenario.