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

Here is a completed exemplar along with an explanation of how the exemplar fulfills the expectations for the activity.

Completed Exemplar

To review the exemplar for this course item, click the link and select *Use Template*.

Link to exemplar: Incident handler's journal entry exemplar

OR

If you don't have a Google account, you can download the exemplar directly from the following attachment.

Incident handler's journal entry exemplar
DOCX File

Assessment of Exemplar

Compare the exemplar to your completed activity. Review your work using each of the criteria in the exemplar. What did you do well? Where can you improve? Use your answers to these questions to guide you as you continue to progress through the course.

Note: *The exemplar represents one of many possible ways to complete this activity. Yours will likely differ in certain ways. What's important is that your incident handler's journal records the details of the scenario. Knowing how to use an incident handler's journal to record notes and additional details during an incident investigation is important because it can be used as a reference for future incident response efforts.*

The exemplar contains one completed journal entry. The journal entry is dated, numbered, and provides a brief description of the scenario. Additionally, in the **The 5 W's section**, the journal entry addresses the following about the scenario:

- Who caused the incident?
- What happened?
- When did the incident occur?
- Where did the incident happen?
- Why did the incident happen?

Lastly, the journal entry includes additional questions about the scenario in the **Additional notes** section.

Note: The exemplar contains the first entry in the incident handler's journal. As you progress through the course, you'll complete the subsequent journal entries in your incident handler's journal template.

Key takeaways

This activity enabled you to practice applying your documentation skills to complete a journal entry about a ransomware scenario. Accurate and thorough documentation is a critical aspect in incident response because it helps to ensure that important information is not lost or overlooked, and it also allows you to capture aspects of an incident for future use. Continue practicing your documentation skills by creating additional journal entries as you complete the course activities. By the end of the course, you will add this document to your cybersecurity portfolio.

Mark as completed