**Exemplar**

**Incident handler's journal**

**Instructions**

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this journal as a way to log the key takeaways about the different cybersecurity tools or concepts you encounter in this course.

| **Date:** July 23, 2024 | **Entry:** #1 | | |
| --- | --- | --- | --- |
| Description | Documenting a cybersecurity incident | | |
| Tool(s) used | None. | | |
| The 5 W's | * **Who**: An organized group of unethical hackers * **What**: A ransomware security incident * **Where**: At a health care company * **When**: Tuesday 9:00 a.m. * **Why**: The incident happened because unethical hackers were able to access the company's systems using a phishing attack. After gaining access, the attackers launched their ransomware on the company's systems, encrypting critical files. The attackers' motivation appears to be financial because the ransom note they left demanded a large sum of money in exchange for the decryption key. | | |
| Additional notes | 1. How could the health care company prevent an incident like this from occurring again? 2. Should the company pay the ransom to retrieve the decryption key? | | |

**My work.**

**Incident handler's journal**

**Instructions**

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this journal as a way to log the key takeaways about the different cybersecurity tools or concepts you encounter in this course.

| **Date:**  12/02/2023 | **Entry:**  Document 1 | | |
| --- | --- | --- | --- |
| Description | * 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 | | |
| Tool(s) used | NONE | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? * An organized group of unethical hackers * **What** happened? * 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. * **When** did the incident occur? * Tuesday at 9:00 a.m.. * **Where** did the incident happen? * A small U.S. health care clinic * **Why** did the incident happen? * phishing email that contained a malicious attachment. Once it was downloaded, ransomware was deployed encrypting the organization's computer files. | | |
| Additional notes | Unethical Hackers, Phishing Email, Ransomware, Encrypting computer files. | | |