**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, 2023 | **Entry:** #1 |
| Description | Documenting a cybersecurity incident |
| Tool(s) used | None |
| The 5 W's | * **Who**: An organized group of unethical hackers * **What**: Ransomware security incident * **Where**: Health care company * **When**: Tuesday 9:00 a.m. * **Why**: This incident happened because the malicious actor was able to gain access to the system using a phishing attack. After gaining access they execute the ransomware and encrypted all the sensitive and important files, they are demanding 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? |

|  |  |
| --- | --- |
| **Date:** July 24, 2023 | **Entry:** #2 |
| Description | Investigate a suspicious file hash |
| Tool(s) used | Used a popular tool VirusTotal to analyze the file hash and scan it across the malicious files hash database for any suspicious file. |
| The 5 W's | * **Who**: Unknown * **What**: An email sent to an employee contained a malicious file * **Where**: Employee at financial services * **When**: 1:20 pm * **Why**: Employee downloaded the malicious attachment and executed the files |
| Additional notes | 1. How can this incident be prevented in the future? Should we consider   improving security awareness training so that employees are careful with what they click on? |