**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:** 8/10/2023 | **Entry: #1** | | |
| --- | --- | --- | --- |
| Description | Documenting a cybersecurity incident | | |
| Tool(s) used | None. | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: Organized group of unethical hackers * **What**: Ransomware security incident. * **When**: Tuesday at 9:00am * **Where**: At a health care company. * **Why**: The incident happened because unethical hackers were able to gain access to the company's systems using a phishing attack. Once they gained 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. What can the healthcare company implement in order to prevent an incident like this in the future? 2. Is it potentially worth paying the attackers the ransom in order to retrieve the stolen decryption key? | | |

| **Date:**  Record the date of the journal entry. | **Entry: #2** | | |
| --- | --- | --- | --- |
| Description | Reviewing a final report to a cybersecurity incident. | | |
| Tool(s) used | None. | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: Organized group of unethical hackers * **What**: Forced browsing attack causing unauthorized access hack leading to PII leaks and financial loss. * **When**: December 28th 7:20pm * **Where**: Mid-sized retail company. * **Why**: The incident occurred because unethical hackers gained access to customer PII and company financial information, affecting 50,000 customers. | | |
| Additional notes | Why was the company targeted and what specific group wanted to perform such a daunting attack?  What preventative measures can be taken to fully prevent an attack from these specific threat actors and like minded threat actors? | | |

| **Date:**  Record the date of the journal entry. | **Entry: #3** | | |
| --- | --- | --- | --- |
| Description | Analyzing log data to detect any threats | | |
| Tool(s) used | Splunk | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who:** Threat actors/Irresponsible employees * **What:** Login authentication/ failed login attempts * **When:** 9/8/22 6:13pm * **Where:** Buttercup Games * **Why**: To gain access to confidential info, mishandling of sensitive company info | | |
| Additional notes | What steps can be taken to prevent login failures like this? How can issues like this be detected sooner? | | |

| Reflections/Notes: The only entry I had some trouble with was the splunk section as it took a while to get an email giving me access to the software. Apart from the bugged setup, I enjoyed it along with the other journal entries. Due to my natural inclination towards analysis I was able to smoothly record my thoughts throughout each scenario. My outlook of incident response has greatly improved as I've gotten familiar with the process and I am much more confident moving forward. I enjoyed splunk the most and am excited to continue my learning in it and hopefully specialize in it as well. |
| --- |