**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:**  Monday, February 26, 2024 | **Entry:**  1 | | |
| --- | --- | --- | --- |
| Description | Incident response to the ransomware security incident targeting the U.S. health clinic. | | |
| Tool(s) used | No cybersecurity related tools were used. | | |
| The 5 W's | Capture the 5 W's of an incident.   * The attack was orchestrated by a group of unethical hackers * Malware encrypted critical files and softwares putting a stop to business operations. * The incident occurred Tuesday at 9:00am. * The incident took place at U.S. health clinic. * The incident was financially motivated. Hackers demanded payment for access to the encrypted files. | | |
| Additional notes | * Hackers were able to gain access to the health clinic’s systems through a targeted phishing email strategy. Employee’s downloaded a file infected with malware enabling the attackers to access and encrypt critical files and software. | | |

| **Date:**  Wednesday, February 28, 2024 | **Entry:**  2 | | |
| --- | --- | --- | --- |
| Description | Received an IDS alert notifying of a suspicious file download to an employee’s workstation | | |
| Tool(s) used | Intrusion Detection System, VirusTotal | | |
| The 5 W's | Capture the 5 W's of an incident.   * IDS system triggered an alert. * The user downloaded a suspicious file from an email received from an unknown source. * The IDS triggered the alert at 1:20pm. * At the employee’s company workstation. * Potential threat seeking to gain access to company files and systems through a phishing email attack. | | |
| Additional notes | * What can the company do to better train employees to identify potential phishing emails? * Could any other company employees have received this email or was this a targeted attack? | | |

| **Date:**  Wednesday, February 28 | **Entry:**  3 | | |
| --- | --- | --- | --- |
| Description | Review of the final report regarding the recent security breach at the retail company | | |
| Tool(s) used | Incident Final Report | | |
| The 5 W's | Capture the 5 W's of an incident.   * An unauthorized individual was the threat actor in the incident. * The unauthorized individual gained access to confidential customer PII and financial information. * The incident occurred on December 28, 2022 at 7:20pm P.T. * The incident took place on the retail company’s website. * The threat actor conducted the attack for financial gain. | | |
| Additional notes | * How did the threat actor know how to exploit the vulnerability on the e-commerce website? * Have other retailers experienced similar incidents? | | |

### Need another journal entry template?

If you want to add more journal entries, please copy one of the tables above and paste it into the template to use for future entries.

| Reflections/Notes: It was beneficial to practice learning how to write good journal entries that are detailed and accurately reflect the investigation process I would be conducting as a security analyst. I still require more practice to really perfect the practice but I am optimistic it will be a quick learning experience. |
| --- |