**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:**  Apr 1, 2024 | **Entry: 1** | | |
| --- | --- | --- | --- |
| Description | Documenting a Cybersecurity incident | | |
| 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 health clinic experienced a security incident involving ransomware, triggered by a phishing email containing a malicious attachment that installed malware on an employee's computer once it was downloaded. * **When** did the incident occur? Tuesday, 9:00 a.m. * **Where** did the incident happen? The incident occurred within a small U.S health care clinic specializing in delivering primary-care services. * **Why** did the incident happen? Several employees within the organization fell victim to a targeted phishing email containing a malicious attachment that installed malware on an employee's computer once it was downloaded, leading to files being encrypted by an organized group of unethical hackers and demanded a large sum of money in exchange for the decryption key. | | |
| Additional notes | This incident highlights the need for cybersecurity awareness and training among employees in healthcare organizations to prevent this incident from happening again in the future, as well as the importance of a playbook for incident response plans to minimize the disruption and protect sensitive data such as the patient data. It is important or crucial to address such incidents to safeguard patient confidentiality and maintain business continuity. | | |

| **Date:**  Apr 4, 2024 | **Entry: 2** | | |
| --- | --- | --- | --- |
| Description | Analyzing a packet capture file | | |
| Tool(s) used | In this exercise, I'm using the Wireshark to analyze a packet capture or p-cap. Wireshark, as a network protocol analyzer with a graphical user interface, the value of wireshark is to capture and analyze network traffic that can help in detecting and investigating a security incident or malicious activity. | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? * **What** happened? * **When** did the incident occur? * **Where** did the incident happen? * **Why** did the incident happen? | | |
| Additional notes | I've never used Wireshark before, so I was excited to begin this exercise and  analyze a packet capture file. At first glance, the interface was very  overwhelming. I can see why it's such a powerful tool for understanding  network traffic. | | |

| **Date:**  Apr 4, 2024 | **Entry: 3** | | |
| --- | --- | --- | --- |
| Description | Respond to a phishing incident that involves a malicious file hash using a playbook instructions to investigate and resolve the incident's alert ticket. | | |
| Tool(s) used | In this exercise, I'm using the VirusTotal tool to analyze the indicator of compromise and the pyramid of pain to improve how indicators of compromise are used in incident detection. | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? * **What** happened? * **When** did the incident occur? * **Where** did the incident happen? * **Why** did the incident happen? | | |
| Additional notes | Include any additional thoughts, questions, or findings.  A playbook can help security teams minimize the impact of an incident and reduce the incident response time. As a security analyst, playbooks can help guide you to effectively support an organization's incident response efforts. | | |

| **Date:**  Apr 5, 2024. | **Entry: 4** | | |
| --- | --- | --- | --- |
| Description | analyze an artifact using VirusTotal and capture details about its related indicators of compromise using the Pyramid of Pain. | | |
| Tool(s) used | In this exercise, I'm using the VirusTotal tool to analyze the indicator of compromise and the pyramid of pain to improve how indicators of compromise are used in incident detection. | | |
| 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 health clinic experienced a security incident involving ransomware, triggered by a phishing email containing a malicious attachment that installed malware on an employee's computer once it was downloaded. * **When** did the incident occur? Tuesday, 9:00 a.m. * **Where** did the incident happen? The incident occurred within a small U.S health care clinic specializing in delivering primary-care services. * **Why** did the incident happen? Several employees within the organization fell victim to a targeted phishing email containing a malicious attachment that installed malware on an employee's computer once it was downloaded, leading to files being encrypted by an organized group of unethical hackers and demanded a large sum of money in exchange for the decryption key. | | |
| Additional notes | Include any additional thoughts, questions, or findings. This incident highlights the need for cybersecurity awareness and training among employees in Financial Service companies to prevent this incident from happening again in the future.. | | |

| **Date:**  Apr 8 2024 | **Entry: 5** | | |
| --- | --- | --- | --- |
| Description | Provide a brief description about the journal entry. | | |
| Tool(s) used | List any cybersecurity tools that were used. | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? * **What** happened? * **When** did the incident occur? * **Where** did the incident happen? * **Why** did the incident happen? | | |
| Additional notes | Include any additional thoughts, questions, or findings. | | |

### 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: Record additional notes.   1. **Were there any specific activities that were challenging for you? Why or why not?** The activity involving tcpdump is challenging for me. I am new to using a tcpdump because my familiarity with the command line was limited, and learning the syntax for a tool like tcpdump was a big learning curve. I felt a sense of frustration as I struggled to obtain the desired output. In order to make me more familiar with the syntax I decided to redo the activity and review the note I made. The experience reinforced the importance of careful instruction reading and methodical problem-solving. 2. **Has your understanding of incident detection and response changed after taking this course?** Upon completing the course my understanding of incident detection and response have changed and definitely improving. When I first started the course, I had a rudimentary grasp of the concepts behind detection and response, but I underestimated the intricacies involved. However, as I advanced through the course, I gained insight into the complete incident lifecycle, recognizing the significance of thorough plans, effective processes, and skilled individuals, as well as the various tools utilized in the field. In summary, my perception has evolved significantly, and I now possess a deeper understanding and a wealth of knowledge regarding incident detection and response. 3. **Was there a specific tool or concept that you enjoyed the most? Why?** I found myself deeply intrigued by the realm of network traffic analysis during the course, particularly in the practical utilization of network protocol analyzer tools. It marked my initial exposure to this field, presenting both challenges and exhilaration. The capacity to utilize tools for the real-time capture and analysis of network traffic held my fascination. Now, I am eager to further immerse myself in this domain, aiming to enhance my expertise in employing network protocol analyzer tools. |
| --- |