**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:**  5/15/2024 | **Entry:**  0001 |
| Description | Security incident that did not allow medical professional to use system |
| 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? Employee * **What** happened? Phishing email was downloaded * **When** did the incident occur? Tuesday at 9am * **Where** did the incident happen? US Health Care Clinic * **Why** did the incident happen? Unethical hackers attacked with ransomware |
| Additional notes | Include any additional thoughts, questions, or findings. |

|  |  |
| --- | --- |
| **Date:**  5/20/2024 | **Entry:**  0002 |
| Description | Analyzed a packet capture file |
| Tool(s) used | I used Wireshark |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? none * **What** happened? none * **When** did the incident occur? none * **Where** did the incident happen? none * **Why** did the incident happen? none |
| Additional notes | First time using WireShark, overwhelming but a ton of data to recover from wireshark!! |

|  |  |
| --- | --- |
| **Date:**  5/22/2024 | **Entry:**  0003 |
| Description | Captured first packet |
| Tool(s) used | Tcpdump |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? none * **What** happened? none * **When** did the incident occur? none * **Where** did the incident happen? none * **Why** did the incident happen? none |
| Additional notes | Tcpdump is a network protocol analyzer that's accessed using the  command-line interface. Similar to Wireshark, the value of tcpdump in  cybersecurity is that it allows security analysts to capture, filter, and analyze  network traffic. |

|  |  |
| --- | --- |
| **Date:**  5/24/2024 | **Entry:**  0004 |
| Description | Investigate file hash |
| Tool(s) used | I used VirusTotal to analyze a file hash, which was reported as malicious. |
| The 5 W's | Capture the 5 W's of an incident.  ● Who: An unknown malicious actor  ● What: An email sent to an employee contained a malicious file  attachment with the SHA-256 file hash of  54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab5  27f6b  ● Where: An employee's computer at a financial services company  ● When: At 1:20 p.m., an alert was sent to the organization's SOC after the  intrusion detection system detected the file  ● Why: An employee was able to download and execute a malicious file  attachment via e-mail. |
| Additional notes | How can this incident be prevented in the future? This incident occurred in the Detection and Analysis phase. The scenario put  me in the place of a security analyst at a SOC investigating a suspicious file  hash. After the suspicious file was detected by the security systems in place, I  had to perform deeper analysis and investigation to determine if the alert  signified a real threat. |

|  |  |
| --- | --- |
| **Date:** | **Entry:** |
| 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. |

|  |  |
| --- | --- |
| **Date:**  Record the date of the journal entry. | **Entry:**  Record the journal entry number. |
| 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. |