**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:**  Record the date of the journal entry.  **November 7, 2023** | **Entry:**  Record the journal entry number.  **Entry #1** |
| Description | Provide a brief description about the journal entry.  **Documenting a Cybersecurity Incident.** |
| Tool(s) used | List any cybersecurity tools that were used.   * **None** |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? * **Organized group of unethical hackers** * **What** happened? * **Ransomware attack** * **When** did the incident occur? * **Approximately Tuesday morning at 0900** * **Where** did the incident happen? * **A Small U.S. health Care Clinic** * **Why** did the incident happen? * **Unethical hacker group is known for attacking Healthcare and Transportation industries the Ransom is to make lots of money off stolen data and private information.** |
|  | Include any additional thoughts, questions, or findings.  **In the Scenario it does not say whether the employee who clicked on the Phishing email link and downloaded the Malicious threat did it by accident or if he was disgruntled with the company and did it on purpose.** |

|  |  |
| --- | --- |
| **Date:**  11/26/2023 | **Entry:**  2 |
| Description | **Employee received a phishing email in their inbox** |
| Tool(s) used | **Google Chronicle** |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? * **Employee who received the email** * **What** happened? * **Phishing Email** * **When** did the incident occur? * **January 31 2023 at 21:40:45** * **Where** did the incident happen? * **Signin.office365x24.com** * **Why** did the incident happen? * **Employee clicked on a phishing email link which downloaded the Malicious Malware** |
| Additional notes | Flagged as Malicious Malware from various sources including Sophos, CyRadar and VIPRE |

|  |  |
| --- | --- |
| **Date:**  11/26/2023 | **Entry:**  3 |
| Description | **Analyzing a packet capture file** |
| Tool(s) used | **Wireshark** |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** **N/A** * **What** **N/A** * **When** **N/A** * **Where** **N/A** * **Why** N/A |
| Additional notes | **Recently new to using Wireshark I cannot help but find the tool both interesting and can see why it useful in the cybersecurity field with how quickly it can pull up information related to the searches that the user requests.** |

|  |  |
| --- | --- |
| **Date:**  11/26/2023 | **Entry:**  #4 |
| Description | Investigate a suspicious file hash |
| Tool(s) used | For this activity, I used VirusTotal to analyze a file hash, which was reported as malicious. 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 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. |
| The 5 W's | * **Who Unknown Malicious Actor** * **What: an Email sent to an employee contained malicious file attachment with the SHA-256 file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b** * **When At 1:20 p.m., an alert was sent to the organization's SOC after the intrusion detection system detected the file** * **Where An employee's computer at a financial services company** * **Why An employee was able to download and execute a malicious file attachment via e-mail.** |
| Additional notes | **I suggest doing Security Awareness Training to try and help prevent repeat events as much as possible.** |