**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:**  09/08/24 | **Entry:**  #1 |
| Description | Documenting a cybersecurity incident |
| Tool(s) used | - |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: Group of unethical hackers. * **What**: A ransomware attack * **When**: Tuesday, 9:00 am. * **Where**: Health company * **Why**: The group of unethical hackers managed to gain access using a phishing attack. The attackers ran their ransomware on company’s systems, encrypting the data and asking for a large amount of money. |
| Additional notes | The healthcare company can prevent future incidents by implementing employee cybersecurity training, advanced email filtering, multi-factor authentication, regular data backups, and a strong incident response plan.  The company should avoid paying the ransom, as it does not guarantee data recovery. |

|  |  |
| --- | --- |
| **Date:**  10/09/24 | **Entry:**  #2 |
| Description | Verifying a file based on hash value |
| Tool(s) used | Virustotal |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: BlackTech, known threat actor. * **What**: A potentially malicious file was detected by various security vendors during a VirusTotal scan. * **When**: The exact date when the file was introduced into the environment isn't provided, but the VirusTotal report was generated when the hash was checked. * **Where**: The incident occurred wherever the malicious file was discovered, such as on a specific endpoint, server, or within the corporate network * **Why**: The file itself was designed to act as a backdoor or trojan, which indicates that the intent behind the attack could be to gain unauthorized access to systems |
| Additional notes | Sha256 hash: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b |

|  |  |
| --- | --- |
| **Date:**  10/09/24 | **Entry:**  #3 |
| Description | An employee downloaded a file which affected his system. |
| Tool(s) used | Virustotal |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: external threat * **What**: employee received an phishing email * **When**: During work hours, when the employee opened his email. * **Where**: On the employees machine. * **Why**: The incident happened because the employee fell victim to a phishing attack. |
| Additional notes | The malware has been already checked before, using it’s file hash. It is a known backdoor threat used by BlackTech. |

|  |  |
| --- | --- |
| **Date:**  11/09/2024 | **Entry:**  #4 |
| Description | The organization experienced a security incident during which an unauthorized individual gained access to customer Personally Identifiable Information (PII) and financial information. |
| Tool(s) used | **-** |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: An external threat actor. * **What**: Unauthorized access to customer PII and financial information via a web application vulnerability. * **When**: 28 December 2022, at 7:20 p.m. * **Where**: The organization's e-commerce web application. * **Why**: The attacker exploited a vulnerability in the web application, specifically a forced browsing attack, by modifying the order number in the URL string of purchase confirmation pages. This allowed unauthorized access to customer transaction data, which was then exfiltrated |
| Additional notes | - |

|  |  |
| --- | --- |
| **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. |

|  |  |
| --- | --- |
| **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. |