**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:**  27/11/2023 | **Entry:**  01 | | |
| --- | --- | --- | --- |
| Description | Documenting the details of a ransomware incident. | | |
| Tool(s) used | None | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** : A group of unethical hackers * **What** : Deployed ransomware through a phishing email. * **When** : Tuesday around 9:00 am * **Where** : A small health care clinic, USA * **Why** : By compromising employee computers via emailed malware, attackers infiltrated the organization's network. They leveraged this access to deploy ransomware, encrypting vital data files across multiple systems. The accompanying ransom note's financial demands indicated the motive of the hackers is money. | | |
| Additional notes | * Should the company pay the ransom for their data. * How can they improve their security so that they can avoid this in future. | | |

| **Date:**  29/11/2023 | **Entry:**  02 | | |
| --- | --- | --- | --- |
| Description | Documenting the details of a data theft incident. | | |
| Tool(s) used | None | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** : An unidentified individual (hacker) * **What** : Unauthorized access and data theft * **When** : December 28,2022 at 7:20pm * **Where** : E-commerce web application * **Why** : The root cause of the incident was identified as a vulnerability in the web application allowing a forced browsing attack. This permitted the attacker to modify the order number in the URL of a purchase confirmation page, granting access to customer transaction data. The security team confirmed the vulnerability by analyzing web application access logs, revealing that the attacker accessed thousands of purchase confirmation pages. The motive of the hacker seems to be money as he demanded $50,000 to prevent public release. | | |
| Additional notes | * Should the company pay the ransom for their data? * How can they improve their security so that they can avoid this in future. | | |

| **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. | | |

| **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. |
| --- |