**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:**  28/10/2024 | **Entry:**  1. |
| Description | Una pequeña clínica sanitaria estadounidense sufrió un incidente de seguridad el martes a las 9:00 a.m. que interrumpió gravemente sus operaciones comerciales.  La causa del incidente de seguridad fue un correo electrónico de phishing que contenía un archivo adjunto malicioso. Una vez descargado, se desplegó un ransomware que encriptó los archivos (informáticos) de la organización.  Un grupo organizado de piratas informáticos poco éticos dejó una nota de rescate en la que se indicaba que los archivos de la empresa estaban cifrados y exigía dinero a cambio de la clave de descifrado |
| Tool(s) used | Ninguna herramienta de ciberseguridad utilizada, pero se apagón sus sistemas informáticos y se puso en contacto con varias organizaciones para informar del incidente y recibir asistencia técnica. |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident?   **Un actor malicioso envió un correo electrónico de phishing**   * **What** happened?   **Desplego un ransomware que encriptó los archivos informáticos de la organización.**   * **When** did the incident occur?   **El incidente se produjo sobre las 9:00 de la mañana**   * **Where** did the incident happen?   **El incidente ocurrió en las instalaciones de la empresa**   * **Why** did the incident happen?   **Ocurrió por un correo electrónico de phishing** |
| Additional notes | No se sabe si el personal está capacitado ante situaciones correos electrónicos maliciosos.  Se debe de capacitar al personal sobre phishing para evitar futuros incidentes relacionados con este tema. |

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

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