**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 | Incidente de ciberseguridad |
| Tool(s) used | Ninguna herramienta de ciberseguridad utilizada. |
| 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 del martes.**   * **Where** did the incident happen?   **El incidente ocurrió en las instalaciones de la empresa**   * **Why** did the incident happen?   La clínica sanitaria sufrió un incidente de seguridad 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 exigía dinero a cambio de la clave de descifrado para la entrega de los documentos. |
| 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:**  31/10/2024 | **Entry:**  #2 |
| Description | Incidente archivo malicioso adjunto en email |
| Tool(s) used | SHA256, es un método criptográfico utilizado para identificar de forma única el malware, actuando como la huella dactilar única del archivo.  Se utilizo VirusTotal para determinar si el SHA era maliciosos. |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident?   **Actor malicioso**   * **What** happened?   **Se descargo en el ordenador del usuario de la empresa un archivo malicioso.** **Se crean varios archivos ejecutables no autorizados en el ordenador del empleado**   * **When** did the incident occur?   **----**   * **Where** did the incident happen?   **El daño paso en el ordenador del usuario de la empresa.**   * **Why** did the incident happen?   **Un empleado recibió un correo electrónico que contenía un archivo adjunto. El archivo adjunto era una hoja de cálculo protegida por contraseña. La contraseña de la hoja de cálculo se facilitaba en el correo electrónico. El empleado descargó el archivo e introdujo la contraseña para abrirlo. Cuando el empleado abrió el archivo, se ejecutó una carga maliciosa en su ordenador** |
| Additional notes | Con el análisis de VirusTotal se pudo confirmar que el archivo era malicioso y además otras empresas se ha visto afectados por el. |

|  |  |
| --- | --- |
| **Date:**  04/11/2024 | **Entry:**  #3. |
| Description | Seguimiento phishing. |
| 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?   **Actor malicioso**   * **What** happened?   **Análisis del contenido del phishing**   * **When** did the incident occur?   **20/07/2022 a las 9:30:14 hrs.**   * **Where** did the incident happen?   **El incidente se registró en el ordenador del usuario de la empresa.**   * **Why** did the incident happen?   **Un empleado recibió un correo electrónico que contenía un archivo adjunto, que decía ser un CV. La posibilidad de descargar el fichero y abrirlo es medida para activar una alerta.** |
| Additional notes | Se puede percatar que el actor malicioso que usan la técnica del engaño (Ingeniería Social) para que el empleado descargue el fichero e ingrese una contraseña.  Otro factor importante es que la dirección de email no utiliza el nombre de la persona que quiere aplicar al empleo por lo que su email es sospechoso. |

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