**Diario de gestión de incidentes**

**Instrucciones**

A medida que avances en el curso, puedes utilizar esta plantilla para registrar tus observaciones después de finalizar una actividad o para tomar notas sobre lo que aprendiste acerca de una herramienta o un concepto en particular. También puedes emplear este diario para documentar las conclusiones clave sobre las distintas herramientas o conceptos de ciberseguridad que encuentres en este curso.

|  |  |
| --- | --- |
| **Fecha:**  Anota la fecha. | **Entrada: #1**  13/08/2024 \*Martes 09:00 am |
| Descripción | Describe brevemente la entrada.  INCIDENTE:  Una clínica sufrió un ataque de ransomware el día martes 13/08 sobre las 09:00 am. Los atacantes cifraron los datos, impidiendo las operaciones comerciales de la clínica, y exigieron una gran suma de dinero por la clave de descifrado.  SOLUCIÓN: |
| Herramienta(s) utilizada(s) | Enumera las herramientas de ciberseguridad que se utilizaron. |
| Las 5 W | Determina las 5 W de un incidente.   * **Who**: ¿Quién causó el incidente?   Un grupo organizado de hackers poco éticos   * **What**: ¿Qué sucedió?   Los archivos de la empresa fueron cifrados, impidiendo las operaciones comerciales.   * **When:** ¿Cuándo ocurrió el incidente?   Martes, 13 de agosto del 2024 a las 09:00 am   * **Where:** ¿Dónde ocurrió el incidente?   Una pequeña clínica de atención médica en Estados Unidos experimentó un incidente de seguridad.   * **Why:** ¿Por qué ocurrió el incidente?   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 cifró los archivos informáticos de la organización. |
| Notas complementarias | Capacitar a los empleados contra este tipo de ataques.  Considerar la segmentación de red para evitar que todo el sistema colapse.  Verificar si se cumplió el principio de mínimos privilegios.  ¿El empleado sabía lo que estaba descargando? |

|  |  |
| --- | --- |
| **Fecha:**  Anota la fecha. | **Entrada: #2**  23/08/2024 |
| Descripción | Un empleado recibe un correo en el cual hay un archivo adjunto, el empleado lo descarga y abre el archivo, se da cuenta que el archivo que se ejecuto crea varios ejecutables sin autorizacion en la computadora del empleado. Un IDS detecta los archivos ejecutables y procede a alertar al SOC |
| Herramienta(s) utilizada(s) | Enumera las herramientas de ciberseguridad que se utilizaron.  <https://www.virustotal.com/> |
| Las 5 W | Determina las 5 W de un incidente.   * **Who**: ¿Quién causó el incidente?   Se desconoce   * **What**: ¿Qué sucedió?   Un IDS informo a un SOC de archivos ejecutables que se instalaron sin autorización.   * **When:** ¿Cuándo ocurrió el incidente?   Viernes, 23 de agosto de 2024 a las 13:11:00 pm   * **Where:** ¿Dónde ocurrió el incidente?   Una empresa de servicios financieros.   * **Why:** ¿Por qué ocurrió el incidente?   Un empleado recibio un archivo el cual abrio e hizo que se crearan mas archivos ejecutables. |
| Notas complementarias | Capacitación del personal sobre correos sospechosos. |

|  |  |
| --- | --- |
| **Fecha:**  Anota la fecha. | **Entrada:**  Anota el número de entrada. |
| Descripción | Describe brevemente la entrada. |
| Herramienta(s) utilizada(s) | Enumera las herramientas de ciberseguridad que se utilizaron. |
| Las 5 W | Determina las 5 W de un incidente.   * **Who**: ¿Quién causó el incidente? * **What**: ¿Qué sucedió? * **When:** ¿Cuándo ocurrió el incidente? * **Where:** ¿Dónde ocurrió el incidente? * **Why:** ¿Por qué ocurrió el incidente? |
| Notas complementarias | Agrega cualquier otra observación, pregunta o conclusión. |

|  |  |
| --- | --- |
| **Fecha:**  Anota la fecha. | **Entrada:**  Anota el número de entrada. |
| Descripción | Describe brevemente la entrada. |
| Herramienta(s) utilizada(s) | Enumera las herramientas de ciberseguridad que se utilizaron. |
| Las 5 W | Determina las 5 W de un incidente.   * **Who**: ¿Quién causó el incidente? * **What**: ¿Qué sucedió? * **When:** ¿Cuándo ocurrió el incidente? * **Where:** ¿Dónde ocurrió el incidente? * **Why:** ¿Por qué ocurrió el incidente? |
| Notas complementarias | Agrega cualquier otra observación, pregunta o conclusión. |

|  |  |
| --- | --- |
| **Fecha:**  Anota la fecha. | **Entrada:**  Anota el número de entrada. |
| Descripción | Describe brevemente la entrada. |
| Herramienta(s) utilizada(s) | Enumera las herramientas de ciberseguridad que se utilizaron. |
| Las 5 W | Determina las 5 W de un incidente.   * **Who**: ¿Quién causó el incidente? * **What**: ¿Qué sucedió? * **When:** ¿Cuándo ocurrió el incidente? * **Where:** ¿Dónde ocurrió el incidente? * **Why:** ¿Por qué ocurrió el incidente? |
| Notas complementarias | Agrega cualquier otra observación, pregunta o conclusión. |

|  |  |
| --- | --- |
| **Fecha:**  Anota la fecha. | **Entrada:**  Anota el número de entrada. |
| Descripción | Describe brevemente la entrada. |
| Herramienta(s) utilizada(s) | Enumera las herramientas de ciberseguridad que se utilizaron. |
| Las 5 W | Determina las 5 W de un incidente.   * **Who**: ¿Quién causó el incidente? * **What**: ¿Qué sucedió? * **When:** ¿Cuándo ocurrió el incidente? * **Where:** ¿Dónde ocurrió el incidente? * **Why:** ¿Por qué ocurrió el incidente? |
| Notas complementarias | Agrega cualquier otra observación, pregunta o conclusión. |

¿Necesitas otra plantilla para las entradas?

Si deseas agregar más entradas, copia una de las tablas anteriores y pégala en la plantilla.

|  |
| --- |
| Reflexiones/notas: registra las notas adicionales. |