# Incident handler's journal

## Instructiones

A medida que avance en este curso, puede utilizar esta plantilla para registrar sus hallazgos después de completar una actividad o para tomar notas sobre lo que ha aprendido sobre una herramienta o un concepto específico. También puede utilizar este diario como una forma de registrar los puntos clave sobre las diferentes herramientas o conceptos de ciberseguridad que encuentre en este curso.

| **Date:** Record the date of the journal entry. | **Entry:** Martes por la mañana a las 9:00 AM. |
|---|---|
| Description | Muchos trabajadores informaron de que no podían acceder a los archivos necesarios para su trabajo. A otros les salía un mensaje en pantalla que tenían que pagar por los equipos bloqueados. |
| Tool(s) used | List any cybersecurity tools that were used. |
| The 5 W's | Capture the 5 W's of an incident.<br>El incidente se inició por correos electrónicos de  phishing que contenían archivos maliciosos.<br>Al descargar archivos maliciosos se activa un software que es conocido como ransomware.<br>El martes por la mañana, sobre las 9  AM. Ocurrió en una clínica sanitaria estadounidense.<br>Trabajadores fueron engañados con correos maliciosos y un ransomware llegó a los ordenadores y tomó el control de los dispositivos. |
| Additional notes | Faltaría estudiar los logs buscando si hubo otro tipo de ataque o intentos previos, o ver si tuvo algún tipo de ayuda. Si por el contrario no, ¿se deben |

| | |
|---|---|
| | tomar medidas para instruir al personal y minimizar este tipo de ataques?. |

---

| | |
|---|---|
| **Date:**<br>Record the date of the journal entry. | **Entry:**<br>Miércoles 20/07/2022 luego de la 9:30 que recibió el mail y ejecutará el archivo en su interior |
| Description | Un trabajador informa de que recibió un mail, el cual abrió y ejecutó un archivo en su interior. Se informa del hash del archivo y se busca información de el archivo y Virustotal informa que es un troyano. |
| Tool(s) used | Hash del archivo, banco de virus y su información en Virustotal para determinar el alcance. IP 114.114.114.114 ⟶ atacante – 176.157.125.93 ⟶ trabajador. |
| The 5 W's | Capture the 5 W's of an incident.<br>El incidente se inició por correos electrónicos de phishing que contenían archivos maliciosos.<br>El correo electrónico contenía un archivo malicioso el cual fue descargado y ejecutado por el empleado.<br>Desde su puesto de trabajo abrió y ejecuto el archivo, lo ejecuto y dio el aviso en el ticket A-2703<br>Un trabajador fue engañado y por lo visto descargo un troyano. |
| Additional notes | Se debería poner en cuarentena el ordenador, ya que tenemos pruebas suficientes de que fue un ataque para infectar su ordenador, y se debe escalar este ticket para resolverlo cuanto antes. |

---

| | |
|---|---|
| **Date:**<br>Record the date of the journal entry. | **Entry:**<br>7:20pm 28/12/2022. |
| Description | Una organización sufre un incidente de seguridad pierden datos de sus clientes(datos personales PII) |
| Tool(s) used | Registros de los acontecimientos(logs de acceso a la aplicación web). |
| The 5 W's | Capture the 5 W's of an incident.<br>Un agente malicioso encontró una vulnerabilidad que explotó para obtener información confidencial PII.<br>Se descubrió una vulnerabilidad que un agente malicioso utilizó para obtener registros de compradores y sus datos.<br>Atacaron la web de la empresa,donde generaban los recibos de transacciones.<br>Se aprovecharon de una vulnerabilidad no descubierta hasta ese momento, utilizaron eso para recopilar información de los clientes. |
| Additional notes | Para estos casos, se deberían hacer rutinariamente pruebas de penetración en todos los apartados de cara al público donde información relevante queda expuesta para asegurar su seguridad e integridad.<br>Se deben arreglar la vulnerabilidad que deja información tan importante expuesta. |

| | |
|---|---|
| **Date:**<br>Record the date of the journal entry. | **Entry:**<br>15/08/2024 |
| Description | Se hacen pruebas con Suricata para probar su uso y la configuración |
| Tool(s) used | Suricata |
| The 5 W's | Capture the 5 W's of an incident.<br>Se recopila información con suricata para ver su funcionamiento. Suricata al estar activo recopila información buscando patrones si es la configuración asignada y cuando estas se cumplen genera un informe y una acción determinada(avisar, bloquear,anular). Esto se puede instalar para revisar un terminal o un sistema y determinar si los datos que pasan sospechosos |
| Additional notes | El uso, la configuración y las condiciones que se dictan a Suricata son esenciales para controlar el flujo de datos y obtener los mejores resultados que sea información relevante. |

---

| | |
|---|---|
| **Date:**<br>Record the date of the journal entry. | |
| Description | |

| | |
|---|---|
| Tool(s) used | |
| The 5 W's | Capture the 5 W's of an incident. |
| Additional notes | |

---

| | |
|---|---|
| **Date:**<br>Record the date of the journal entry. | **Entry:**<br>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.<br>• **Who** caused the incident?<br>• **What** happened?<br>• **When** did the incident occur?<br>• **Where** did the incident happen?<br>• **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.

Los casos presentados son una muestra de las cosas que te puedes encontrar. Configurar estos programas como Suricata ayudan a comprender cómo se trabaja y qué debes tener una amplia visión para ser y configurar correctamente estos programas, mayor conocimiento te ayudará a ajustar los parámetros y mejorar la búsqueda de actividad maliciosa .