Diario de gestión de incidentes

Instrucciones

A medida que vas avanzando en este curso, puedes usar esta plantilla para registrar tus hallazgos después de completar una actividad o para tomar notas sobre lo aprendido de una herramienta o concepto específico. Además, puedes usar este diario para registrar las conclusiones clave sobre las diferentes herramientas o conceptos de ciberseguridad que aprenderás en este curso.

Fecha: 22/11/25	**Entrada:** N.º 1
Descripción	Documentar un incidente de ciberseguridad Este incidente ocurrió en las dos fases: 1. **Detección y análisis**: El escenario describe cómo la organización detectó por primera vez el incidente de ransomware. Para la etapa de análisis, la empresa se puso en contacto con varias organizaciones para obtener asistencia técnica. 2. **Contención, erradicación y recuperación**: El escenario detalla algunos pasos que implementó la organización para contener el incidente. Por ejemplo, apagó los sistemas informáticos. Sin embargo, como no podían erradicar y recuperarse del incidente por su cuenta, contactaron a varias otras organizaciones para obtener ayuda.
Herramienta(s) utilizada(s)	Ninguna
Las 5 W	• **Quién (who)**: Un grupo organizado de hackers poco éticos. • **Qué (what)**: Un incidente de seguridad de ransomware. • **Dónde (where)**: En una empresa de atención médica. • **Cuándo (when)**: Martes 9:00 a.m. • **Por qué (why)**: El incidente ocurrió porque hackers poco éticos pudieron acceder a los sistemas de la compañía mediante un ataque de phishing. Acto seguido, los atacantes lanzaron su ransomware en los sistemas de la compañía y cifraron archivos críticos. Su motivación parecía ser financiera porque la nota de rescate exigía una gran suma de dinero a cambio de la clave para descifrar los archivos.

Notas complementarias	1. ¿De qué manera la compañía de atención médica podría evitar que vuelva a ocurrir un incidente como este? 2. ¿La empresa debería pagar el rescate para recuperar la clave de descifrado?

Fecha: 22/11/25	**Entrada:** N.º 2
Descripción	Análisis de un archivo de captura de paquetes
Herramienta(s) utilizada(s)	Para esta actividad, utilicé Wireshark para analizar un archivo de captura de paquetes. Wireshark es un analizador de protocolos de red que utiliza una interfaz gráfica de usuario. El valor de Wireshark en ciberseguridad es que permite a los analistas capturar y analizar el tráfico de red. Esto puede ayudar a detectar e investigar actividades maliciosas.
Las 5 W	● **Quién (who)**: N/D ● **Qué (what)**: N/D ● **Dónde (where)**: N/D ● **Cuándo (when)**: N/D ● **Por qué (why)**: N/D
Notas complementarias	Antes nunca había usado Wireshark, así que me interesaba mucho comenzar este ejercicio y analizar un archivo de captura de paquetes. A primera vista, la interfaz era muy abrumadora. Ahora entiendo por qué es una herramienta tan poderosa para comprender el tráfico de red.

Fecha: 22/11/25	**Entrada:** N.º 3
Descripción	Capturar mi primer paquete
Herramienta(s)	Para esta actividad, utilicé tcpdump para capturar y analizar el tráfico de red.

utilizada(s)	Tcpdump es un analizador de protocolos de red al que se accede mediante la interfaz de línea de comandos. Al igual que Wireshark, el valor de tcpdump en ciberseguridad es que permite a los analistas capturar, filtrar y analizar el tráfico de red.
Las 5 W	• **Quién (who)**: N/D • **Qué (what)**: N/D • **Dónde (where)**: N/D • **Cuándo (when)**: N/D • **Por qué (why)**: N/D
Notas complementarias	Aún no domino el uso de la interfaz de línea de comandos, por lo que usarla para capturar y filtrar el tráfico de red me supuso un desafío. Me atasqué algunas veces porque usé los comandos equivocados. Pero después de seguir cuidadosamente las instrucciones y rehacer algunos pasos, pude superar esta actividad y capturar el tráfico de la red.

Fecha: 22/11/25	**Entrada:** N.º 4
Descripción	Investigar un hash de archivo sospechoso
Herramienta(s) utilizada(s)	Para esta actividad, utilicé VirusTotal, que es una herramienta de investigación que analiza archivos y URL en busca de contenido malicioso, como virus, gusanos, troyanos y más. Es una herramienta muy útil si lo que necesitas es verificar rápidamente si otros integrantes de la comunidad de ciberseguridad denunciaron como malicioso un indicador de compromiso (como un sitio web o archivo). Para esta actividad, utilicé VirusTotal con el fin de analizar un hash de archivo que se reportó como malicioso. Este incidente ocurrió en la fase de **detección y análisis**. Tuve que asumir el rol de un analista de seguridad en un SOC que investiga un hash de archivo sospechoso. Después de que los sistemas de seguridad detectaron el archivo sospechoso, tuve que realizar un análisis y una investigación más profundos para determinar si la alerta era una amenaza real.

Las 5 W	• **Quién (who)**: Un agente de amenaza desconocido. • **Qué (what)**: Un correo electrónico enviado a un empleado contenía un archivo adjunto malicioso con el hash de archivo SHA-256 de 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b. • **Dónde (where)**: La computadora de un empleado de una compañía de servicios financieros. • **Cuándo (where)**: A la 1:20 p.m., se envió una alerta al SOC de la organización después de que el sistema de detección de intrusiones detectara el archivo. • **Por qué (why)**: Un empleado pudo descargar y ejecutar un archivo adjunto malicioso que recibió por correo electrónico.
Notas complementarias	¿Cómo se puede prevenir este incidente en el futuro? ¿Deberíamos considerar mejorar la capacitación en concientización de seguridad para que los empleados tengan cuidado con dónde hacen clic?

Reflexiones/Notas:

1. **¿Hubo alguna actividad específica que te haya resultado desafiante? ¿Por qué sí o por qué no?**

La actividad con tcpdump me resultó verdaderamente desafiante. Aún no domino el uso de la línea de comandos, y aprender la sintaxis de una herramienta como tcpdump fue un gran proceso de aprendizaje. Al principio, me resultó muy frustrante porque no lograba el resultado correcto. Repetí la actividad y me di cuenta de dónde me había equivocado. Aprendí que tengo que leer las instrucciones con atención e ir avanzando en el proceso paso a paso.

2. **Después de completar este curso, ¿entiendes mejor el proceso de detectar y dar respuesta a incidentes?**

Sí, definitivamente, después de completar el curso comprendo mejor la detección y respuesta a incidentes. Al comenzar el curso, tenía un conocimiento básico de lo que implicaba el proceso de detección y respuesta, pero no llegaba a comprender toda su complejidad. A medida que fui avanzando, aprendí sobre el ciclo de vida de un incidente y de la importancia de los planes, los procesos y las personas, así como las herramientas utilizadas. En general, siento que ahora lo entiendo mejor y que cuento con más conocimientos para detectar incidentes y dar respuesta a ellos.

3. **¿Hubo alguna herramienta o concepto específico que te haya gustado más? ¿Por qué?**

Disfruté mucho de aprender sobre el análisis del tráfico de red y aplicar los conocimientos mediante las herramientas del analizador de protocolos de red. Era la primera vez que aprendía sobre análisis de tráfico de red, por lo que fue desafiante y emocionante. Me fascinó el hecho de haber podido usar herramientas para capturar el tráfico de la red y analizarlo en tiempo real. Definitivamente, me interesa aprender más sobre este tema y espero algún día poder dominar las herramientas de los analizadores de protocolos de red.

¿Necesitas otra plantilla de entradas del diario?

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