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: 05/12/2024	**Entrada:** #1
Descripción	Documenta un evento Una clínica de atención médica sufrió un incidente de ransomware, lo que provocó que los empleados no pudieran acceder a los archivos y sistemas críticos necesarios para sus operaciones diarias.
Herramienta(s) utilizada(s)	Ninguna.
Las 5 W	• **Who**: Un grupo organizado de hackers. • **What**: Los sistemas de la clínica fueron atacados con ransomware, cifrando archivos críticos. • **When:** Martes por la mañana, alrededor de las 9:00 a.m. • **Where:** En la red de una clínica médica en Estados Unidos. • **Why:** Para exigir un rescate a cambio de la clave de descifrado de los archivos cifrados.
Notas complementarias	¿Se debería pagar el rescate para recuperar los documentos cifrados?

Fecha: 10/12/2024	**Entrada:** #2
Descripción	Analiza tu primer paquete Se realizaron actividades de aprendizaje utilizando Wireshark, enfocándose en la apertura y análisis de archivos de captura de paquetes, exploración de información de paquetes y aplicación de filtros de visualización.
Herramienta(s) utilizada(s)	Wireshark
Las 5 W	Determina las 5 W de un incidente. ● **Who**: N/D ● **What**: N/D ● **When:** N/D ● **Where:** N/D ● **Why:** N/D
Notas complementarias	Este ejercicio permitió familiarizarse con los filtros y el análisis detallado de protocolos y capas de red.

Fecha: 11/12/2024	**Entrada:** #3
Descripción	Captura de un paquete. Se utilizó la herramienta tcpdump para identificar interfaces de red, capturar tráfico de red en vivo, guardar este tráfico en un archivo de captura y filtrar los datos del archivo.
Herramienta(s)	tcpdump

utilizada(s)	
Las 5 W	Determina las 5 W de un incidente. ● **Who**: N/D ● **What**: N/D ● **When:** N/D ● **Where:** N/D ● **Why:** N/D
Notas complementarias	tcpdump, se me hace una herramienta muy ligera y a la vez eficiente, pero puede llegar a ser difícil de utilizar para principiantes.

Fecha: 14/12/2024	**Entrada:** #4
Descripción	Investigar un hash de archivo sospechoso. Se investigó un archivo malicioso descargado desde un correo electrónico de phishing. Se generó un hash SHA256 del archivo y se utilizó VirusTotal para identificar indicadores de compromiso (IoC) asociados.
Herramienta(s) utilizada(s)	VirusTotal Algoritmo de hashing SHA256
Las 5 W	Determina las 5 W de un incidente. ● **Who**: Un agente de amenaza desconocido. ● **What**: Un archivo malicioso ejecutó una carga dañina en la computadora del empleado tras abrir una hoja de cálculo protegida. ● **When:** Una computadora de un empleado de una compañía de servicios financieros. ● **Where:** A la 1:20 p.m. se envió una alerta al SOC de la organización después de que se detectara el archivo.

	• **Why:** Un empleado descargó y ejecutó un archivo adjunto malicioso que recibió por correo electrónico.
Notas complementarias	Se recomienda reforzar la capacitación de los empleados sobre phishing.

Fecha: 17/12/2024	**Entrada:** #5
Descripción	Uso de un manual de estrategias para responder a un incidente de phishing Se siguieron las políticas y procedimientos del SOC para investigar una alerta de phishing relacionada con un archivo malicioso. El análisis confirmó la amenaza, y se completaron los pasos necesarios para resolver la alerta y documentar las conclusiones en el ticket correspondiente.
Herramienta(s) utilizada(s)	Manual de estrategias de la empresa
Las 5 W	Determina las 5 W de un incidente. • **Who**: N/D • **What**: N/D • **When:** N/D • **Where:** N/D • **Why:** N/D
Notas complementarias	Se recomienda capacitación adicional a los empleados sobre cómo identificar correos de phishing.

Fecha: 20/12/2024	**Entrada:** #6
Descripción	Revisa un informe final Revisión de un informe final sobre un incidente de seguridad en el que se filtraron datos de más de un millón de usuarios. Se identificaron detalles del incidente, medidas de respuesta y recomendaciones futuras para prevenir eventos similares.
Herramienta(s) utilizada(s)	Informe final
Las 5 W	Determina las 5 W de un incidente. ● **Who**: N/D ● **What**: N/D ● **When:** N/D ● **Where:** N/D ● **Why:** N/D
Notas complementarias	Se destacó la importancia de proteger datos críticos y mejorar los controles de seguridad en las plataformas de comercio electrónico.

Fecha: 21/12/2024	**Entrada:** #7
Descripción	Explorar firmas y registros con Suricata Se utilizó Suricata para examinar, activar y analizar reglas personalizadas, generando registros de alerta. Se revisaron los resultados generados en el archivo eve.json para evaluar el funcionamiento de las reglas.
Herramienta(s) utilizada(s)	Suricata Archivo eve.json

Las 5 W	Determina las 5 W de un incidente. ● **Who**: N/D ● **What**: N/D ● **When:** N/D ● **Where:** N/D ● **Why:** N/D
Notas complementarias	Esta actividad permitió familiarizarse con la creación de reglas personalizadas en Suricata y la interpretación de registros de alerta en formato JSON.

Fecha: 21/12/2024	**Entrada:** #8
Descripción	Realiza una consulta con Splunk Se utilizó Splunk Cloud para cargar datos, realizar búsquedas y analizar patrones de actividad en un servidor. El objetivo era investigar incidentes de seguridad relacionados con intentos fallidos de inicio de sesión SSH para la cuenta root.
Herramienta(s) utilizada(s)	Splunk
Las 5 W	Determina las 5 W de un incidente. ● **Who**: N/D ● **What**: N/D ● **When:** N/D ● **Where:** N/D ● **Why:** N/D
Notas complementarias	Se recomienda seguir explorando el uso de SPL para mejorar la precisión en la detección de incidentes.

Fecha: 21/12/2024	**Entrada:** #9
Descripción	Realiza una consulta con Chronicle Se utilizó la herramienta Chronicle para investigar un incidente de phishing relacionado con un dominio sospechoso identificado en un correo electrónico: signin.office365x24.com. El objetivo era determinar si otros empleados habían recibido correos similares o habían visitado el dominio.
Herramienta(s) utilizada(s)	Chronicle
Las 5 W	Determina las 5 W de un incidente. ● **Who**: Un empleado de la empresa y posibles otros destinatarios del correo sospechoso. ● **What**: Un intento de phishing utilizando un dominio sospechoso en un correo electrónico. ● **When:** Durante la revisión de una alerta de seguridad en el SOC. ● **Where:** En la bandeja de entrada de empleados de una empresa de servicios financieros. ● **Why:** Para identificar y mitigar intentos de suplantación de identidad que podrían comprometer la seguridad de la organización.
Notas complementarias	Se recomienda educar a los empleados sobre cómo identificar y reportar intentos de phishing.

Reflexiones/notas: registra las notas adicionales.

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

La entrada 8 y 9 porque son herramientas (Splunk y Chronicle) que nunca he utilizado, lo cual requirió un esfuerzo adicional para comprender su funcionamiento y aplicarlas correctamente.

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

Sí, porque a través de las actividades prácticas aprendí a utilizar herramientas como Splunk, Chronicle y VirusTotal, lo que me permitió desarrollar un enfoque estructurado para identificar patrones, analizar registros y responder de manera efectiva a incidentes.

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

Splunk me gustó más porque su capacidad para realizar búsquedas rápidas y precisas en grandes volúmenes de datos es muy útil para identificar patrones y anomalías, lo que lo convierte en una herramienta esencial en la gestión de incidentes de seguridad.