¡Felicitaciones! ¡Aprobaste!

Calificación recibida 100 % **Para Aprobar** 75 % o más

Ir al siguiente elemento

Para aprobar esta práctica, debes obtener un puntaje del 75%, o 3 puntos sobre 4, respondiendo a una serie de preguntas. Una vez que completes el cuestionario, revisa los comentarios. Puedes conocer más sobre las prácticas y los ejercicios con calificación en la descripción general del curso.

Resumen de la actividad

En esta actividad, revisarás un ejemplo de informe final y responderás a una serie de preguntas.

Hasta ahora, aprendiste sobre las acciones involucradas en la fase de actividad posterior al incidente del ciclo de vida de respuesta a incidentes del NIST. Esto incluye el desarrollo del **informe final**, que es la documentación que proporciona una revisión exhaustiva de un incidente. Contiene datos esenciales de todos los eventos relacionados con el incidente y recomendaciones para la prevención futura.

Escenario

Revisa el siguiente escenario. Luego, completa las instrucciones paso a paso.

Te incorporaste recientemente al equipo de seguridad como analista de nivel uno del centro de operaciones de seguridad (SOC) en una empresa minorista de tamaño medio. Además de sus tiendas físicas, la compañía también opera a través de comercio electrónico, canal que representan el 80% de sus ventas.

Estás pasando tu primera semana de capacitación, familiarizándote con los procesos y procedimientos de seguridad de la empresa. Recientemente, esta experimentó un importante incidente de seguridad, que involucró una filtración de datos de más de un millón de usuarios. Dado que se trata de un incidente de seguridad reciente e importante, tu equipo está trabajando para evitar que algo así vuelva a ocurrir. Esta filtración se produjo antes de que comenzaras a trabajar en la empresa. Te han pedido que revises el informe final.

Para comprender el ciclo de vida del incidente, los objetivos de tu revisión son los siguientes:

- Objetivo 1: Identifica exactamente qué sucedió.
- Objetivo 2: Identifica cuándo ocurrió.
- Objetivo 3: Identifica las medidas de respuesta adoptadas por la empresa.
- Objetivo 4: Identifica las recomendaciones futuras.

Nota: *Utiliza el diario de gestión de incidentes que iniciaste en una actividad anterior para tomar notas durante la actividad y hacer un seguimiento de tus hallazgos.*

Instrucciones paso a paso

Consulta el material de apoyo para responder a las preguntas del cuestionario que aparecen a continuación. Tras completar el cuestionario, puedes comparar tus respuestas con los comentarios proporcionados.

Paso 1: Accede a los materiales de apoyo

Los materiales de apoyo te ayudarán a completar esta actividad. Manténlos abiertos a medida que avances en los siguientes pasos.

Si quieres utilizar los materiales de apoyo para este tema del curso, haz clic en el siguiente enlace y selecciona “Usar plantilla.

Enlace a los materiales de apoyo: Informe final

O BIEN

Si no tienes una cuenta de Google, puedes descargar los materiales de apoyo directamente desde el siguiente archivo adjunto.

Activity Review a final report_Final-report
DOCX File

Paso 2: Responde a las preguntas sobre el informe final

Paso 2: Responde a las preguntas sobre el informe final

1. ¿Qué tipo de incidente de seguridad afectó a la organización? **1 / 1 punto**

- ○ Software malicioso (malware)
- ○ Vishing
- ○ Phishing (suplantación de identidad)
- ◉ Robo de datos

Correcto
La organización se vio afectada por un incidente de seguridad relacionado con el robo de datos.

2. ¿Qué sección del informe incluye una explicación del origen del incidente? **1 / 1 punto**

- ○ Recomendaciones
- ◉ Investigación
- ○ Línea de tiempo
- ○ Resumen ejecutivo

Correcto
La sección de investigación del informe final incluye una explicación del origen del incidente, que fue una vulnerabilidad en la aplicación web de comercio electrónico.

3. ¿Qué utilizó el atacante para explotar la vulnerabilidad de la aplicación web de comercio electrónico? **1 / 1 punto**

- ○ Filtración de datos
- ○ Error del usuario
- ○ Registros del servidor web
- ◉ Navegación forzada

Correcto
El atacante utilizó la navegación forzada para explotar la vulnerabilidad de la aplicación web de comercio electrónico.

4. ¿Qué recomendaciones aplicó la organización para evitar que se repitan en el futuro? Selecciona dos respuestas. **1 / 1 punto**

- ☑ Implementación de mecanismos de control de acceso

Correcto
Como parte de sus recomendaciones para prevenir futuras recurrencias, la organización implementó mecanismos de control de acceso, así como análisis rutinarios de vulnerabilidades.

- ☐ Pagó los US$ 50.000 solicitados
- ☐ Prestación de servicios de protección de la identidad a los clientes afectados
- ☑ Implementación de análisis rutinarios de vulnerabilidades

Correcto
Como parte de sus recomendaciones para prevenir futuras recurrencias, la organización implementó mecanismos de control de acceso, así como análisis rutinarios de vulnerabilidades.