¡Felicitaciones! ¡Aprobaste!

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

Ir al siguiente elemento

1. Los manuales de estrategias son documentos permanentes que compilan las mejores prácticas, por lo que un equipo de seguridad no debe realizar cambios en ellos. **1 / 1 punto**

- ○ Verdadero
- ◉ Falso

Correcto
Los manuales de estrategias son documentos vivos; un equipo de seguridad realizará cambios, modificaciones y mejoras frecuentes para abordar nuevas amenazas y vulnerabilidades.

2. Recientemente, una empresa experimentó una fuga de información. Las/los profesionales de seguridad actualmente están restaurando los datos afectados utilizando una copia de seguridad limpia que se creó antes del incidente. ¿Qué fase del manual de estrategia describe este escenario? **1 / 1 punto**

- ◉ Erradicación y recuperación
- ○ Contención
- ○ Detección y análisis
- ○ Actividad posterior al incidente

Correcto
Este escenario describe la erradicación y la recuperación. Esta fase implica eliminar los artefactos del incidente y restaurar el entorno afectado a un estado seguro.

3. Completa el espacio en blanco: Una vez que se resuelve un incidente de seguridad, las/los analistas de seguridad realizan varias actividades posteriores al incidente y trabajan en la _____ con el equipo de seguridad. **1 / 1 punto**

- ○ preparación
- ○ detección
- ○ erradicación
- ◉ coordinación

Correcto
Una vez que se resuelve un incidente de seguridad, las/los analistas de seguridad realizan varias actividades posteriores al incidente y trabajan en la coordinación con el equipo de seguridad. La coordinación implica reportar incidentes y compartir información basada en estándares establecidos.

4. ¿Qué acción puede tomar un/a analista de seguridad cuando evalúa una alerta SIEM? **1 / 1 punto**

- ◉ Analizar los datos de registro y las métricas relacionadas
- ○ Aislar un sistema de red infectado
- ○ Restaurar los datos afectados con una copia de seguridad limpia
- ○ Crear un informe final

Correcto
Una acción que un/a analista de seguridad puede tomar cuando está evaluando una alerta SIEM es analizar los datos de registro y las métricas relacionadas. Esto ayuda a identificar por qué la alerta fue generada por la herramienta SIEM y determinar si es válida.