¡Felicitaciones! ¡Aprobaste!

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

Ir al siguiente elemento

1. ¿Cuál es el propósito principal de los registros durante la investigación de un incidente? **1 / 1 punto**

- (●) Proporcionar un historial de detalles del evento
- ( ) Mejorar la experiencia del usuario
- ( ) Gestionar los volúmenes de alertas
- ( ) Identificar y diagnosticar problemas del sistema

Correcto
El propósito principal de los registros durante la investigación de un incidente es proporcionar un historial de detalles del evento. Saber qué pasó en los sistemas, las redes y los dispositivos ayuda a los analistas de seguridad a identificar actividades inusuales o maliciosas.

2. Un analista de seguridad quiere averiguar si un inicio de sesión sospechoso fue exitoso. ¿Qué tipo de registro sería el más útil para este fin? **1 / 1 punto**

- ( ) Cortafuegos (firewall)
- ( ) Red
- (●) Autenticación
- ( ) Sistema

Correcto
Un registro de autenticación sería el más útil para este fin. Estos registran intentos de inicio de sesión, incluso información acerca de si un inicio de sesión tuvo éxito.

3. En el registro siguiente, ¿qué acción registra la entrada del registro? **1 / 1 punto**

```
[ALLOW: wikipedia.org] Source: 192.167.1.1 Friday, 10 June 2022 11:36:12
```

- (●) `ALLOW`
- ( ) `192.167.1.1`
- ( ) `Source`
- ( ) `Friday, 10 June 2022 11:36:12`

Correcto
`ALLOW` (Permitir) hace referencia a la acción que se registró. En este caso, permite acceder a wikipedia.org.

4. Completa el espacio en blanco: El _____ es el proceso de examinar registros para identificar eventos de interés. **1 / 1 punto**

- ( ) registro
- (●) análisis de registros
- ( ) reenviador de registros
- ( ) archivo de registro

Correcto
El análisis de registros es el proceso de examinar registros para identificar eventos de interés.