¡Felicitaciones! ¡Aprobaste!

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

Ir al siguiente elemento

1. ¿Qué carácter especial puedes usar para sustituir por cualquier otro carácter en el lenguaje de procesamiento de búsqueda (SPL)? **1 / 1 punto**

- (•) `*`
- ( ) `|`
- ( ) `=`
- ( ) `!=`

Correcto
El carácter `*` también se conoce como comodín, que es un carácter especial que se puede sustituir por cualquier otro carácter.

2. ¿Cuáles de los siguientes pasos forma parte del proceso SIEM para la recopilación de datos? Selecciona tres respuestas. **1 / 1 punto**

- [x] Recopilar y procesar datos.

Correcto
Las herramientas SIEM recopilan, procesan e indexan datos generados por dispositivos y sistemas de todo un entorno.

- [x] Normalizar los datos para que estén listos para su lectura y análisis.

Correcto
Las herramientas SIEM recopilan, procesan e indexan datos generados por dispositivos y sistemas de todo un entorno. La normalización de los datos facilita en mayor medida su lectura y análisis. Los datos sin procesar se procesan de manera que tengan un formato consistente, y solo se incluye la información del evento relevante.

- [x] Las herramientas SIEM indexan los datos para que se puedan buscar.

Correcto
Las herramientas SIEM recopilan, procesan e indexan datos generados por dispositivos y sistemas de todo un entorno. Mediante la indexación, es posible acceder fácilmente a los datos a través de una búsqueda.

- [ ] Supervisar la actividad y las alertas asociadas a intrusiones.

3. Completa el espacio en blanco: ____ es un lenguaje informático que se usa con el fin de crear reglas para buscar datos de registro ingeridos. **0 / 1 punto**

- (•) YARA-L
- ( ) EVE JSON
- ( ) NIDS
- ( ) SIEM

Incorrecto
Chronicle usa el lenguaje informático YARA-L con el fin de crear reglas para buscar datos de registro ingeridos.

4. ¿Cuál de las siguientes opciones es un lenguaje de consulta de Splunk? **1 / 1 punto**

- (•) SPL
- ( ) IDS
- ( ) UDM
- ( ) SQL

Correcto
Splunk usa su propio lenguaje de consulta, conocido como lenguaje de procesamiento de búsqueda (SP).