¡Felicitaciones! ¡Aprobaste!

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

Ir al siguiente elemento

1. ¿Qué herramienta está diseñada para capturar y analizar el tráfico de datos dentro de una red? 1 / 1 punto

- ○ Google Chronicle
- ◉ analizador de protocolo de red (programa rastreador de paquetes)
- ○ Splunk Enterprise
- ○ Lenguaje de consulta estructurado (SQL)

Correcto
Un programa rastreador de paquetes, también conocido como analizador de protocolo de red, es una herramienta diseñada para capturar y analizar el tráfico de datos dentro de una red.

2. ¿Cuáles de las siguientes son ejemplos de herramientas SIEM? Selecciona dos respuestas. 1 / 1 punto

- ☐ Linux
- ☐ Python
- ☑ Google Chronicle

Correcto
Splunk Enterprise y Google Chronicle son ejemplos de herramientas SIEM. Las/los analistas de seguridad utilizan herramientas SIEM para recopilar datos de múltiples lugares. Luego analizan y filtran esos datos para permitir que los equipos de seguridad prevengan y reaccionen rápidamente ante posibles amenazas de seguridad.

- ☑ Splunk Enterprise

Correcto
Splunk Enterprise y Google Chronicle son ejemplos de herramientas SIEM. Las/los analistas de seguridad utilizan herramientas SIEM para recopilar datos de múltiples lugares. Luego analizan y filtran esos datos para permitir que los equipos de seguridad prevengan y reaccionen rápidamente ante posibles amenazas de seguridad.

3. ¿Para qué utilizan los registros principalmente las/los profesionales de seguridad? 1 / 1 punto

- ◉ Para identificar vulnerabilidades y posibles fugas de información.
- ○ Para recopilar y analizar datos y así monitorear actividades críticas en una organización.
- ○ Para seleccionar qué miembros del equipo de seguridad responderán a un incidente.
- ○ Para investigar y optimizar las capacidades de procesamiento dentro de una red.

Correcto
Las/los profesionales de la seguridad utilizan principalmente los registros para identificar vulnerabilidades y posibles fugas de información.

4. Completa el espacio en blanco: _____ brinda detalles sobre las acciones operativas. 1 / 1 punto

- ○ Una lista de verificación
- ○ Un directorio
- ◉ Un manual de estrategias
- ○ Un historial de caso

Correcto
Un manual de estrategias brinda detalles sobre las acciones operativas. Los manuales de estrategias brindan orientación para manejar un incidente de seguridad antes, durante y después de que haya ocurrido.