

✓ **¡Felicitaciones! ¡Aprobaste!**

Calificación recibida **93,75 %** Calificación del último envío **93,75 %** Para Aprobar **80 %** o más

[Ir al siguiente elemento](#)


1. ¿Cuáles de las siguientes afirmaciones describen correctamente los registros? Selecciona tres respuestas.

0.5 / 1 punto

☒ Las acciones como las solicitudes de inicio de sesión se recopilan en un registro del servidor.

✓ Correcto

☒ Las conexiones entre dispositivos y servicios en una red se recopilan en un registro de firewall.

✗ **Esto no debería estar seleccionado**
Revisa [el video sobre los registros y las herramientas SIEM](#) .

☐ Las solicitudes salientes a Internet desde una red se recopilan en un registro de firewall.

☒ Los equipos de seguridad monitorean los registros para identificar vulnerabilidades y posibles violaciones de datos.

✓ Correcto

2. ¿Cuáles son algunos de los beneficios clave de las herramientas SIEM? Selecciona tres respuestas.

1 / 1 punto

☒ Ahorrar tiempo

✓ Correcto

☒ Proporcionar monitoreo y análisis de eventos

✓ Correcto

☐ Eliminar la necesidad de revisar manualmente los registros

☒ Recopilar datos de registro de diferentes fuentes

✓ Correcto

3. Completa el espacio en blanco: Para evaluar el rendimiento de una aplicación de software, las/los profesionales de seguridad usan _____, incluidos el tiempo de respuesta, la disponibilidad y la tasa de fallos.

1 / 1 punto

☐ los registros

☐ las herramientas SIEM

☒ las métricas

☐ los paneles

✓ Correcto

4. Un equipo de seguridad instala una herramienta SIEM dentro de la propia infraestructura de su empresa para mantener los datos privados en servidores internos. ¿Qué tipo de herramienta usa?

1 / 1 punto

☐ Alojada en la infraestructura

☐ Alojada en la nube

☐ Híbrida

☒ Autoalojada

✓ Correcto

5. Eres analista de seguridad y deseas una solución de seguridad que sea mantenida y gestionada completamente por tu proveedor de herramientas SIEM. ¿Qué tipo de

1 / 1 punto

herramienta eliges?

- ☐ Alojada en la solución
- ☐ Híbrida
- ☐ Autoalojada
- ☒ Alojada en la nube

✓ Correcto

6. Completa el espacio en blanco: Splunk Enterprise es una herramienta autoalojada que se usa para retener, analizar y buscar _____ de una organización para proporcionar información de seguridad y alertas en tiempo real.

1 / 1 punto

- ☐ el hardware
- ☐ una base de datos
- ☐ aplicaciones en la nube
- ☒ datos de registro

✓ Correcto

7. ¿Cuáles de las siguientes afirmaciones describen Chronicle con precisión? Selecciona tres respuestas.

1 / 1 punto

✓ Las herramientas nativas de la nube como Chronicle son mantenidas y administradas por el proveedor.

✓ Correcto

✓ Las herramientas nativas de la nube como Chronicle están diseñadas para aprovechar la adaptabilidad de la computación en la nube.

Chronicle ahorra tiempo a las empresas al eliminar la necesidad de que los equipos de seguridad monitoreen las amenazas y vulnerabilidades.

✓ Correcto

Revisa [el video sobre las herramientas SIEM comunes](#).

✓ Chronicle recopila datos.

✓ Correcto

8. ¿Qué tipo de herramienta suele requerir que los usuarios paguen por el uso?

1 / 1 punto

- ☐ Autoalojada
- ☐ Nativa de la nube
- ☐ Código abierto
- ☒ Propietaria

✓ Correcto