¡Felicitaciones! ¡Aprobaste!

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

Ir al siguiente elemento

1. ¿Hay limitaciones a la hora de detectar en las herramientas de detección? **1 / 1 punto**

- (•) Sí
- ( ) No

Correcto
Las herramientas de detección tienen limitaciones a la hora de detectar. Si bien constituyen una parte importante de la detección y respuesta a incidentes, no pueden detectarlo todo. Se pueden utilizar métodos adicionales para mejorar la cobertura y la precisión.

2. ¿Por qué los analistas de seguridad refinan las reglas de alerta? Selecciona dos respuestas. **1 / 1 punto**

- [x] Para mejorar la precisión de las tecnologías de detección

Correcto
Los analistas de seguridad refinan las reglas de alerta para mejorar la precisión de las tecnologías de detección y reducir los falsos positivos. Las reglas se ajustan en función de la actividad que se pretende detectar.

- [ ] Para aumentar el volumen de alertas
- [ ] Para crear inteligencia sobre amenazas
- [x] Para reducir los falsos positivos

Correcto
Los analistas de seguridad refinan las reglas de alerta para mejorar la precisión de las tecnologías de detección y reducir los falsos positivos. Las reglas se ajustan en función de la actividad que se pretende detectar.

3. Completa el espacio en blanco: _____ implica la investigación y validación de alertas. **1 / 1 punto**

- (•) El análisis
- ( ) La caza de amenazas
- ( ) La detección
- ( ) El honeypot

Correcto
El análisis implica la investigación y validación de alertas.

4. ¿Cuáles son algunas de las causas de los volúmenes de alertas elevados? Selecciona dos respuestas. **1 / 1 punto**

- [ ] Las técnicas de evasión sofisticadas
- [x] Los ajustes de alerta mal configurados

Correcto
Los ajustes de alerta mal configurados y las reglas de detección amplias son algunas de las causas de los volúmenes de alertas elevados.

- [ ] Las reglas de detección refinadas
- [x] Reglas de detección amplias

Correcto
Los ajustes de alerta mal configurados y las reglas de detección amplias son algunas de las causas de los volúmenes de alertas elevados.