¡Felicitaciones! ¡Aprobaste!

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

Ir al siguiente elemento

1. ¿Cómo ayudan los indicadores de compromiso (IoC) a los analistas de seguridad a detectar anomalías en el tráfico de red? **1 / 1 punto**

- ○ Definen las intenciones del atacante.
- ◉ Proporcionan una forma de identificar un ataque.
- ○ Confirman que ocurrió un incidente de seguridad.
- ○ Capturan la actividad de la red.

Correcto
Los IoC ayudan a los analistas de seguridad a detectar anomalías en el tráfico de red ya que proporcionan una forma de detectar un ataque. Brindan evidencia específica asociada con un ataque, como una dirección IP maliciosa conocida, que puede ayudar a identificar y responder con rapidez ante un posible incidente de seguridad.

2. Completa el espacio en blanco: _____ de datos es el término que se usa para referirse a la transmisión no autorizada de datos desde un sistema. **1 / 1 punto**

- ○ La infiltración
- ○ El tráfico de red
- ○ El pivoteo
- ◉ La exfiltración

Correcto
La exfiltración de datos es la transmisión no autorizada de datos desde un sistema.

3. Un atacante se infiltró en una red. Luego dedica un tiempo prudencial a explorarla, para expandir y mantener su acceso. Busca activos valiosos, como código propietario y registros financieros. ¿Qué describe esta situación? **1 / 1 punto**

- ◉ Movimiento lateral
- ○ Transferencia de archivos internos grandes
- ○ Datos de red
- ○ Phishing (suplantación de identidad)

Correcto
Esta situación describe el movimiento lateral. El movimiento lateral, también llamado pivoteo, describe a un atacante que explora una red con el objetivo de expandir y mantener su acceso.

4. ¿Para qué pueden utilizar los profesionales de seguridad el análisis de tráfico de red? Selecciona tres respuestas. **1 / 1 punto**

- ☑ Identificar actividad maliciosa

Correcto
El análisis del tráfico de red brinda a los profesionales de la seguridad una forma de supervisar la actividad de la red, identificar la actividad maliciosa y entender los patrones de tráfico.

- ☑ Entender los patrones de tráfico de la red

Correcto
El análisis del tráfico de red brinda a los profesionales de la seguridad una forma de supervisar la actividad de la red, identificar la actividad maliciosa y entender los patrones de tráfico.

- ☐ Asegurar los activos críticos
- ☑ Monitorear la actividad de la red

Correcto
El análisis del tráfico de red brinda a los profesionales de la seguridad una forma de supervisar la actividad de la red, identificar la actividad maliciosa y entender

los patrones de tráfico.