¡Felicitaciones! ¡Aprobaste!

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

Ir al siguiente elemento

1. Un analista de seguridad usa un analizador de protocolos de red para capturar el tráfico HTTP con el fin de analizar patrones. ¿Qué tipo de datos está usando? **1 / 1 punto**

- ○ Basados en firmas
- ○ Falsos positivos
- ○ Basados en host
- ◉ Telemetría de red

Correcto
Está usando datos de telemetría de red. La telemetría de red es la recopilación y transmisión de datos de red para análisis, como el tráfico HTTP.

2. ¿Qué afirmación describe con exactitud la diferencia entre un sistema de detección de intrusiones basado en la red (NIDS) y un sistema de detección de intrusiones basado en host (HIDS)? **1 / 1 punto**

- ◉ Un NIDS se instala en una red, en tanto que un HIDS se instala en dispositivos individuales.
- ○ Un NIDS solo detecta amenazas conocidas, en tanto que un HIDS detecta amenazas desconocidas.
- ○ Un NIDS se instala en dispositivos individuales, en tanto que un HIDS se instala en una red.
- ○ Un NIDS utiliza análisis de firmas para detectar amenazas, mientras que un HIDS utiliza agentes.

Correcto
Un NIDS se instala en una red y se usa para recopilar y supervisar datos del tráfico de la red y de la propia red. Un HIDS se instala en un host y se usa para supervisar su actividad.

3. Completa el espacio en blanco: El componente _____ de una firma IDS incluye información del tráfico de red. **1 / 1 punto**

- ○ opciones de regla
- ○ acción
- ◉ encabezado
- ○ ID de firma

Correcto
El componente encabezado de una firma IDS incluye información sobre tráfico de red. Este incluye direcciones IP de origen y de destino, puertos de origen y de destino, protocolos y dirección del tráfico.

4. Un analista de seguridad crea una firma de Suricata para identificar y detectar amenazas de seguridad en función de la dirección del tráfico de red. ¿Cuál de las siguientes opciones de regla debería usar? **1 / 1 punto**

- ○ Rev
- ○ Msg
- ○ Content
- ◉ Flow

Correcto
Debería usar Flow. La opción Flow coincide con la dirección del flujo del tráfico de red.