¡Felicitaciones! ¡Aprobaste!

Calificación recibida 100 % **Calificación del último envío** 100 % **Para Aprobar** 80 % o más

Ir al siguiente elemento

1. ¿Qué detalles contienen los registros? Selecciona todas las opciones que correspondan. **1 / 1 punto**

- [x] Hora
  - Correcto
- [x] Ubicación
  - Correcto
- [x] Fecha
  - Correcto
- [ ] Reenviador

2. Examina el registro siguiente: **1 / 1 punto**

```
[2022/12/21 17:46:35.232748] NOTIFY: NetworkPropertiesUpdated: wifi_psk_13
```

¿De qué tipo de registro se trata?

- ( ) De aplicación
- (•) De red
- ( ) De autenticación
- ( ) De ubicación

Correcto

3. Examina el registro siguiente: **1 / 1 punto**

```
<111>1 2020-04-12T23:20:50.52Z my.machine.com evntslog - ID01[user@98274 iut="2" eventSource="Mobile" eventID="24"]
[Priority@98274 class="low"] Computer A
```

¿Qué valor de campo indica el tipo de dispositivo desde el que se originó este evento?

- ( ) `my.machine.com`
- (•) `Mobile`
- ( ) `Computer A`
- ( ) `low`

Correcto

4. ¿Cuál es 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 monitorea la actividad del host en el que está instalado. Un HIDS utiliza análisis de firmas para analizar la actividad de la red.
- ( ) Tanto un NIDS como un HIDS supervisan sistemas y generan alertas, pero un NIDS usa agentes.
- (•) Un NIDS recopila y supervisa el tráfico de red y los datos de red. Un HIDS monitorea la actividad del host en el que está instalado.
- ( ) Un NIDS registra y genera alertas. Un sistema HIDS monitorea la actividad de los puntos de conexión.

Correcto

5. ¿Qué información se incluye en el encabezado de una firma? Selecciona todas las opciones que correspondan. **1 / 1 punto**

- [x] Número de puerto

Correcto

- [x] Protocolo

Correcto

- [x] Dirección IP

Correcto

- [ ] Acción

6. Analiza esta firma de Suricata: **1 / 1 punto**

```
alert http 167.215.72.95 any -> 156.150.71.141 80 (msg:"GET on wire"; flow:established,to_server; content:"GET"; sid:12345; rev:2;)
```

¿Cuál es el puerto de destino?

- (•) `80`
- ( ) `2`
- ( ) `12345`
- ( ) `141`

Correcto

7. Completa el espacio en blanco: Suricata usa el formato _____ para resultados de eventos y alertas. **1 / 1 punto**

- ( ) HTTP
- ( ) HTML
- (•) EVE JSON
- ( ) CEF

Correcto

8. ¿Qué lenguaje de consulta usa Splunk? **1 / 1 punto**

- ( ) Lenguaje de procesamiento SIEM
- ( ) Lenguaje de procesamiento estructurado
- (•) Lenguaje de procesamiento de búsqueda
- ( ) Lenguaje de consulta estructurado

Correcto

9. ¿Qué búsqueda de campos de un modelo de datos unificado (UDM) especifica una acción de seguridad? **1 / 1 punto**

- ( ) `block`
- ( ) `action`
- ( ) `metadata.event_type`
- (•) `security_result.action`

Correcto

10. Completa el espacio en blanco: Las herramientas SIEM _____ datos sin procesar para que tengan un formato consistente. **1 / 1 punto**

- ( ) introducen

- procesan
- recopilan
- normalizan

Correcto