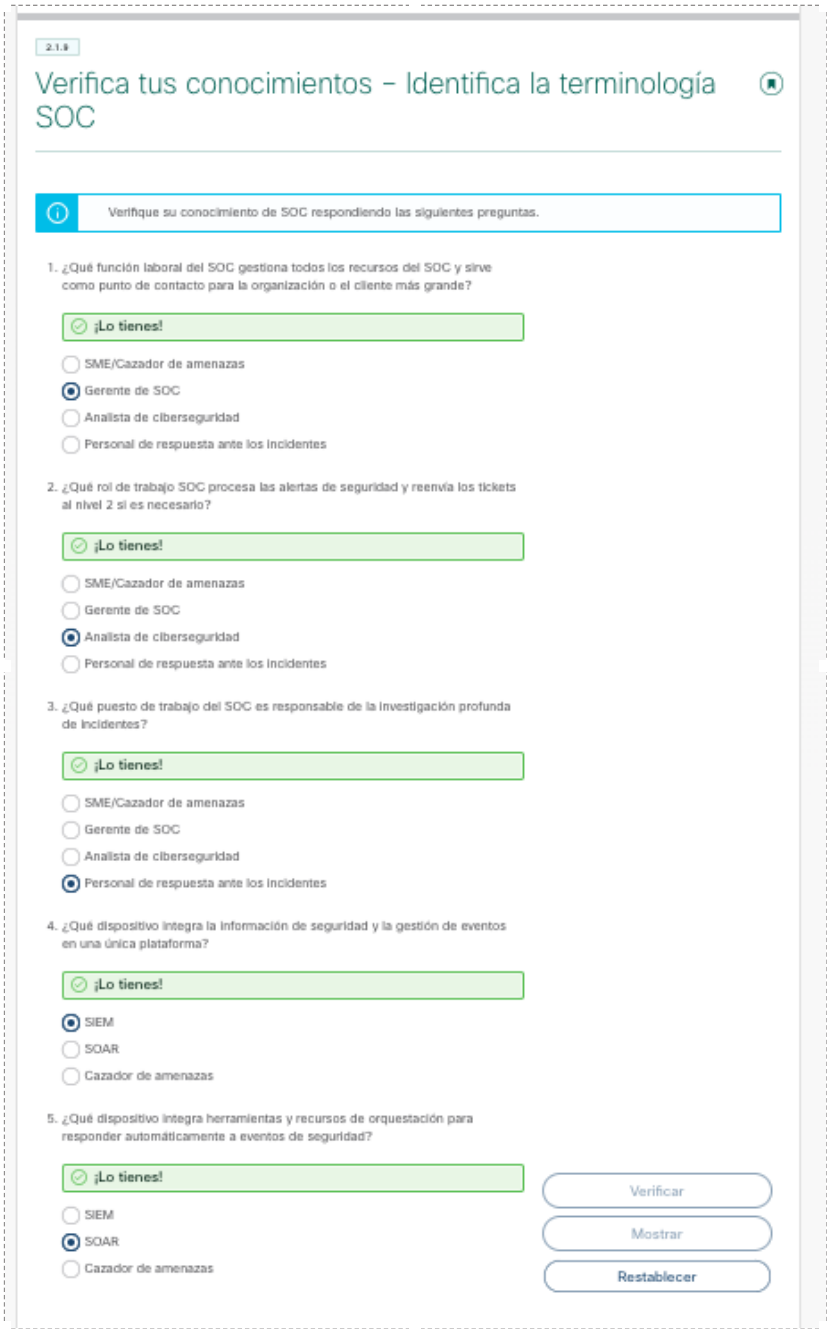
Tema2.2.1.9.EnriqueGomezTagle

sábado, 3 de febrero de 2024 18:37

Enrique Ulises Báez Gómez Tagle – 0241823 - 0241823@up.edu.mx
UP. 2024. Ene-Jun. Hackeo Ético y Recuperación Ante Desastres – Yoel Ledo Mezquita



2.1.9

Verifica tus conocimientos - Identifica la terminología SOC

Verifique su conocimiento de SOC respondiendo las siguientes preguntas.

1. ¿Qué función laboral del SOC gestiona todos los recursos del SOC y sirve como punto de contacto para la organización o el cliente más grande?

¡Lo tienes!

- SME/Cazador de amenazas
- (•) Gerente de SOC
- Analista de ciberseguridad
- Personal de respuesta ante los incidentes

2. ¿Qué rol de trabajo SOC procesa las alertas de seguridad y reenvía los tickets al nivel 2 si es necesario?

¡Lo tienes!

- SME/Cazador de amenazas
- Gerente de SOC
- (•) Analista de ciberseguridad
- Personal de respuesta ante los incidentes

3. ¿Qué puesto de trabajo del SOC es responsable de la investigación profunda de incidentes?

¡Lo tienes!

- SME/Cazador de amenazas
- Gerente de SOC
- Analista de ciberseguridad
- (•) Personal de respuesta ante los incidentes

4. ¿Qué dispositivo integra la información de seguridad y la gestión de eventos en una única plataforma?

¡Lo tienes!

- (•) SIEM
- SOAR
- Cazador de amenazas

5. ¿Qué dispositivo integra herramientas y recursos de orquestación para responder automáticamente a eventos de seguridad?

¡Lo tienes!

- SIEM
- (•) SOAR
- Cazador de amenazas

Verificar
Mostrar
Restablecer