Su calificación final en este cuestionario es 10,00/10,00

Promedio de calificaciones: 10,00 / 10,00

Pregunta 1

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

Cuál es el orde secuenial correcto en el tratamiento de un log antes de que llegue al SIEM

- a. Envío, extracción y parseo
- b. Parseo, extracción y envío
- c. Extracción, envío y parseo

Quitar mi elección

Siguiente página

Pregunta 2

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

Qué ataque de denegación de servicios, DoS, se aprvecha del protocolo TCP de inicio de conexión de 3 vías (handshake).

- a. Syn Flooding
- b. IP Spoofing
- c. Ping de la muerte

Quitar mi elección

Página anterior

Siguiente página

Pregunta 3

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

Durante el proceso de almacenamiento de logs, ¿qué es el parseo?

- a. Un procedimiento para añadir información al log
- b. El proceso de envío cifado de logs al servidor central de información.
- c. Proceso por el que se extrae la información útil de los logs de cada una de las fuentes

Quitar mi elección

Página anterior

Siguiente página

Pregunta **4**

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

Qué fase del almacenamiento de los logs es el más crítico para poder posteriormente realizar búsqueda de manera rápida y eficiente:

- a. Parseo
- b. Indexado
- c. Reenvío

Quitar mi elección

Página anterior

Siguiente página

Pregunta **5**

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

Reducir el tiempo de inoperatividad de un firewall es responsabilidad del

- a. Seguridad física
- b. SOC
- c. NOC

Quitar mi elección

Página anterior

Siguiente página

Pregunta **6**

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

Las herramientas antiAPT no necesitan actualizarse. ¿Verdadero o falso?

Seleccione una:

- Verdadero
- Falso

Página anterior

Siguiente página

Pregunta 7

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

¿Quién puede ayudarnos en la protección de los ataques de DoS/DDoS?

- a. ISP
- b. AEPD
- c. ENISA

Quitar mi elección

Página anterior

Siguiente página

Pregunta 8

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

Los logs de los diferentes dispostivos de una red tienen diferentes formatos, cantidad de información y número de campos ¿Verdadero o falso?.

Seleccione una:

- Verdadero
- Falso

Página anterior

Siguiente página

Pregunta 9

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

Qué protección aplica las mejoras prácticas de seguridad de SPF y DKIM:

- a. OSPF
- b. DMARC
- c. NTLM

Quitar mi elección

Página anterior

Siguiente página

Pregunta 10

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

El SIEM es una herramienta de seguridad:

- a. Nula
- b. Reactiva
- c. Proactiva

Quitar mi elección

Página anterior

Terminar intento...

Segundo intento: Su calificación en este cuestionario es 10,00/10,00

Pregunta 1

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

De las siguietes alternativas, qué parte de un SOC es necesario tener en cuenta para que esté bien dimensionado:

- a. La planta en la que esté situado
- b. El número de recursos humanos que dispone
- c. La ciudad donde se aloje

Quitar mi elección

Siguiente página

Pregunta **2**

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

El protocolo SNMP permite obtener información de un dispositivo de la red. ¿Qué versión del protocolo es considerada segura?

- a. v3
- b. v1
- c. v2

Quitar mi elección

Página anterior

Siguiente página

Pregunta **3**

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

¿Qué mecanismo complementario necesitan los atacanes para infectar los equipos de los usuarios?

- a. El Blockchain
- b. Ingeniería social
- c. Los medios de comunicación

Quitar mi elección

Página anterior

Siguiente página

Pregunta **4**

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

Si una de las alertas que se ha producido en el SIEM finalmente no corresponde a un incidente se denomina:

- a. Falsa alarma
- b. Error de búsqueda
- c. Falso positivo

Quitar mi elección

Página anterior

Siguiente página

Pregunta **5**

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

Las herramientas de almacenamiento de logs tiene que dimensionarse en base a:

- a. Cantidad de fuentes
- b. Tamaño y formato de los logs
- c. Todas son correctas
- d. Tiempo de retención

Quitar mi elección

Página anterior

Siguiente página

Pregunta **6**

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

¿Cuál es uno de los principales vectores de entrada en el sistema y objetivo de los atacantes?

- a. SIEM
- b. Equipos de los usuarios
- c. Infraestructura en la nube (IaaS)

Quitar mi elección

Página anterior

Siguiente página

Pregunta **7**

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

¿El personal de un NOC tiene que tener visibilidad de las alertas del SIEM? . ¿Verdadero o falso?

Seleccione una:

- Verdadero
- Falso

Página anterior

Siguiente página

Pregunta **8**

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

¿Qué es un SOAR?

- a. Sistema automático de tratamiento de incidentes más comunes
- b. Dispositivo de red
- c. Antivirus de última generación

Quitar mi elección

Página anterior

Siguiente página

Pregunta **9**

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

Ante un incidente que deriva en un resultado de falso positivo no es necesario hacer nada sobre el SIEM o el dispositivo que la genera. ¿Verdadero o falso?.

Seleccione una:

- Verdadero
- Falso

Página anterior

Siguiente página

Pregunta **10**

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

¿Qué información puede ser de utilidad a la hora de diseñar reglas de filtrado en el servidio de correo electrónico?

- a. Cabeceras
- b. Firma del correo
- c. El idioma en el que está escrito

Quitar mi elección

Página anterior

Terminar intento...