Examen para BRS07

Intento 1.

Pregunta 1

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

Pregunta 2

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

a. Parseo
b. Reenvío
c. Indexado

Pregunta 3

El SIEM es una herramienta de seguridad:

a. Nula
b. Proactiva
c. Reactiva

Pregunta 4

¿Cuál de las siguientes tareas no es responsabilidad del SOC

a. Mejorar las reglas de detección
b. Investigación de alertas de seguridad
c. Configuración del firewall

Pregunta 5

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

Pregunta 6

La inteligencia de amenazas (threat intelligence) nos puede ayudar a prevenir ataques de DoS. ¿Verdadero o falso?.
Seleccione una:

Verdadero
Falso

Pregunta 7

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

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

Pregunta 8

¿Qué información puede integrarse en un proxy para mejorar su efectividad?

a. Canales RSS
b. Datos de IOCs
c. Virus

Pregunta 9

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

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

Pregunta 10

¿Qué técnica permiten la evasión del firewall?

a. Envío masivo de paquetes
b. Ataque de fuerza bruta contra la autenticación
c. Fragmentación de paquetes

Intento 2.

Pregunta 1

La capacidad de detección de nuevas amenazas por parte del SIEM se basa únicamente en la actualización del software. ¿Verdadero o falso?.
Seleccione una:

Verdadero
Falso

Pregunta 2

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

a. AEPD
b. ENISA
c. ISP

Pregunta 3

Los procedimientos operativos del SOC que ayudan actuar en cada tipo de incidente de seguridad se denominan.

a. Playbooks
b. Whitebook
c. HideBooks

Pregunta 4

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

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

Pregunta 5

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

Verdadero
Falso

Pregunta 6

¿Dónde se instalan mayoritariamente los endpoints?

a. Switch
b. Router
c. Equipos de los usuarios

Pregunta 7

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

Verdadero
Falso

Pregunta 8

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

Pregunta 9

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

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

Pregunta 10

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

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

Intento 3.

Pregunta 1

Qué servicio utiliza SPF(Sender Policy Framework) para validar a los remitentes:

a. FTPS
b. SSH
c. DNS

Pregunta 2

¿Qué es un SOAR?

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

Pregunta 3

Los firewall sólo se colocan en el perímetro de una red o sistema. ¿Verdadero o falso?.
Seleccione una:

Verdadero
Falso

Pregunta 4

Cuál es el orden secuencial correcto en el tratamiento de un log antes de que llegue al SIEM

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

Pregunta 5

¿Por qué un correo electrónico con un fichero adjunto cifrado supone una amenaza?:

a. Porque no es necesario mandar ficheros cifrados, ya lo hacen los mecanismos del correo.
b. Porque el fichero va a intentar ser descifrado por el servidor y se puede colapsar el servicio.
c. El contenido no puede ser analizado por los mecanismos de protección del correo.

Pregunta 6

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.

Pregunta 7

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

a. DMARC
b. NTLM
c. OSPF.

Pregunta 8

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

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

Pregunta 9

¿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).

Pregunta 10

Reducir el tiempo de inoperatividad de un firewall es responsabilidad del

a. SOC.
b. NOC.
c. Seguridad física.