Primer intento: 9,00/10,00

1-¿Cuál es la opción del menú de Kibana que sirve para visualizar los índices de Elasticsearch y la información contenida en ellos?:

a. Discover.

b.Visualize.

c.Dashboard.

2- ¿Cuál es la misión de Kibana en el SOC?:

a.Filtrado de la información de los logs.

b.Monitorización de la información.

c.Detección y Prevención de Intrusiones.

d.Almacenamiento de la información.

3- ¿En qué módulo del SOC se definen los Pipelines?:

a.En Kibana.

b.En Elasticsearch.

c.En Logstash.

4-¿En qué módulo del SOC está ubicado el Grok Debugger?:

a.En Logstash

b.En Elasticsearch.

c.En Kibana.

5-¿Cuál es la misión de Logstash en el SOC?:

a.Monitorización de la información.

b.Filtrado de la información de los logs.

c.Detección y Prevención de Intrusiones.

d.Almacenamiento de la información.

6- ¿En qué entorno se basa Kibana?:

a.Node.js.

b.IBM WebSphere.

c.Ninguno de los anteriores.

d.Microsoft .net.

7- ¿Qué se puede comprobar con la aplicación Nmap?:

a.Ninguna de las anteriores.

b.Sólo si una aplicación está utilizando un puerto determinado de una dirección IP.

c.Si una aplicación usa un puerto, se encuentra a la escucha y con qué servicio o protocolo.

d.Si una aplicación usa un puerto y además está escuchando por él en un momento dado.

8-¿Qué software se debe instalar en un PC para trabajar con Kibana?:

a.Ninguno, basta con disponer de un navegador de Internet.

b.El framework .net.

c.El cliente de Kibana para PC.

9- ¿En qué formato se presenta la salida del Grok Debugger?:

a.En JSON.

b.En UML.

c.En XML.

10- ¿Para qué sirve el patrón Greedydata?:

a.Para capturar información en formato hexadecimal.

b.Para capturar sólo letras, mayúsculas y minúsculas.

c.Para capturar una cadena de caracteres completa y grabarla en una variable.

d.Para discriminar entre números y letras.

Segundo intento: 10,00/10,00

1- ¿En qué consiste la etapa final del proceso en un SIEM?:

a.En la presentación de información en forma de tableros.

b.En la presentación de información en forma de métricas e histogramas.

c.En el análisis de información para detectar patrones y sacar conclusiones de cara a la Prevención de Incidentes.

2- ¿Dónde se ajusta la RAM consumida por la Pila ELK?:

a.En los ajustes de los Pipelines.

b.En los ajustes de los ficheros de log.

c.En las opciones de la Máquina Virtual Java.

3-¿Cuál es la misión de Elasticsearch en el SOC?:

a.Almacenamiento de la información.

b.Detección y Prevención de Intrusiones.

c.Monitorización de la información.

d.Filtrado de la información de los logs.

4-¿Cuál es la opción del menú de Kibana que sirve para crear métricas con los Datos de un índice de Elasticsearch?:

a.Visualize.

b.Dashboard.

c.Discover.

5- ¿Qué módulos de la Pila ELK precisan un ajuste de los límites de memoria RAM?:

a.Todos los módulos de la pila.

b.Logstash y Elasticsearch.

c.Sólo Logstash.

d.Sólo Kibana.

6- ¿Cómo se presenta la información de Elasticsearch a través del navegador?:

a.En JSON.

b.Como un EJB.

c.En UML.

d.En XML.

e.Como un POJO.

7- ¿Cuál es el Comodín en el lenguaje Grok?:

a.El carácter "asterisco".

b.El carácter "punto".

c.El carácter "ampersand".

8- ¿Cuál debe ser el orden de arranque de las aplicaciones en el SIEM ELK?:

a.Kibana, Logstash y Elasticsearch.

b.Logstash, Kibana y Elasticsearch.

c.Se debe arrancar Elasticsearch en primer lugar, el orden del resto de aplicaciones es indiferente.

9- ¿En qué módulo del SOC se utiliza el lenguaje Grok?:

a.En Kibana.

b.En Elasticsearch.

c.En Logstash.

10- ¿En qué módulo del SOC se preparan los Cuadros de Mando?:

a.En Kibana.

b.En Elasticsearch.

c.En Logstash.