Examen para IDC07.

Intento 1.

Pregunta 1

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

a. El cliente de Kibana para PC.
b. El framework .net.
c. Ninguno, basta con disponer de un navegador de Internet.

Pregunta 2

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

a. En Logstash.
b. En Elasticsearch.
c. En Kibana.

Pregunta 3

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

a. En los ajustes de los ficheros de log.
b. En los ajustes de los Pipelines.
c. En las opciones de la Máquina Virtual Java.

Pregunta 4

¿En qué entorno se basa Kibana?:

a. Node.js.
b. Microsoft .net.
c. IBM WebSphere.
d. Ninguno de los anteriores.

Pregunta 5

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

a. En la presentación de información en forma de métricas e histogramas.
b. En la presentación de información en forma de tableros.
c. En el análisis de información para detectar patrones y sacar conclusiones de cara a la Prevención de Incidentes.

Pregunta 6

¿Cuál es el puerto por defecto de Elasticsearch?:

a. 8200.
b. 1200.
c. 9200.
d. Ninguno de los anteriores.

Pregunta 7

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

a. En Elasticsearch.
b. En Kibana.
c. En Logstash.

Pregunta 8

¿Cuál es el Comodín en el lenguaje Grok?:

a. El carácter "asterisco".
b. El carácter "punto".
c. El carácter "ampersand".

Pregunta 9

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

a. En JSON.
b. Como un EJB.
c. Como un POJO.
d. En UML.
e. En XML.

Pregunta 10

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

a. Filtrado de la información de los logs.
b. Almacenamiento de la información.
c. Detección y Prevención de Intrusiones.
d. Monitorización de la información.

Intento 2.

Pregunta 1

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

a. En Logstash.
b. En Kibana.
c. En Elasticsearch.

Pregunta 2

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

a. En Elasticsearch.
b. En Logstash.
c. En Kibana.

Pregunta 3

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

a. Filtrado de la información de los logs.
b. Detección y Prevención de Intrusiones.
c. Almacenamiento de la información.
d. Monitorización de la información.

Pregunta 4

¿Dónde se guarda la información del SIEM?:

a. En los Pipelines de Logstash.
b. En los ficheros de log del IDS.
c. En un índice de Elasticsearch.

Pregunta 5

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

a. Dashboard.
b. Visualize.
c. Discover.

Pregunta 6

¿A qué categoría de herramientas pertenece Logstash?:

a. Es un sniffer.
b. Es un ETL.
c. Es un compilador.
d. Es un conmutador de paquetes.

Pregunta 7

¿Para qué sirve el patrón Greedydata?:

a. Para capturar sólo letras, mayúsculas y minúsculas.
b. Para discriminar entre números y letras.
c. Para capturar una cadena de caracteres completa y grabarla en una variable.
d. Para capturar información en formato hexadecimal.

Pregunta 8

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

a. Filtrado de la información de los logs.
b. Almacenamiento de la información.
c. Detección y Prevención de Intrusiones.
d. Monitorización de la información.

Pregunta 9

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

a. En XML.
b. En UML.
c. En JSON.

Pregunta 10

¿Cuál es la opción del menú de Kibana que sirve para crear tableros de visualización con las métricas?:

a. Discover.
b. Dashboard.
c. Visualize.

Intento 3.

Pregunta 1

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

a. Se debe arrancar Elasticsearch en primer lugar, el orden del resto de aplicaciones es indiferente.
b. Logstash, Kibana y Elasticsearch.
c. Kibana, Logstash y Elasticsearch.

Pregunta 2

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

a. Logstash y Elasticsearch.
b. Todos los módulos de la pila.
c. Sólo Logstash.
d. Sólo Kibana.

Pregunta 3

¿Qué se puede comprobar con la aplicación Nmap?:

a. Si una aplicación usa un puerto y además está escuchando por él en un momento dado.
b. Si una aplicación usa un puerto, se encuentra a la escucha y con qué servicio o protocolo.
c. Ninguna de las anteriores.
d. Sólo si una aplicación está utilizando un puerto determinado de una dirección IP.

Pregunta 4

¿Qué ocurre cuando una base de datos es NoSQL?:

a. Que entiende cualquier lenguaje, sea SQL o no.
b. Ninguna de las anteriores.
c. Que sólo entiende comandos no escritos en SQL.

Pregunta 5

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

a. Dashboard.
b. Discover.
c. Visualize.