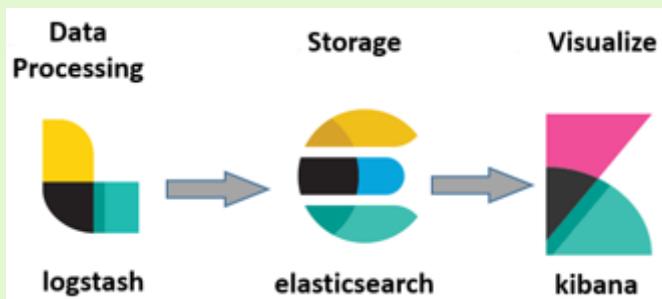




## Gestión de Eventos e Información de Seguridad



[Elastic. ELK Stack \(CC0\)](#)

La detección IDS es el primer estadio de tratamiento de la información en un SOC. La información recolectada en esta etapa deberá ser filtrada, clasificada y almacenada en las siguientes etapas de tratamiento, mediante las herramientas adecuadas.

Hecho esto, dará comienzo la etapa final, que se desarrollará de forma continua una vez iniciada, esto es, el análisis de información para detectar patrones de ataque y sacar las conclusiones correspondientes de cara a la Prevención de Incidentes de Ciberseguridad.

Esta unidad complementa las tareas efectuadas en la unidad anterior, esto es, Detección IDS, por lo que se partirá con Snort instalado, configurado y funcionando en la máquina del laboratorio.

Así pues, se añadirán a la máquina el resto de componentes necesarios para disponer de un SIEM completo y operativo (se recomienda utilizar como mínimo una Raspberry Pi 4B 4GB como escenario de trabajo).



[Ministerio de Educación y Formación Profesional \(Dominio público\)](#)

**Materiales formativos de FP Online propiedad del Ministerio de  
Educación y Formación Profesional.**

[Aviso Legal](#)

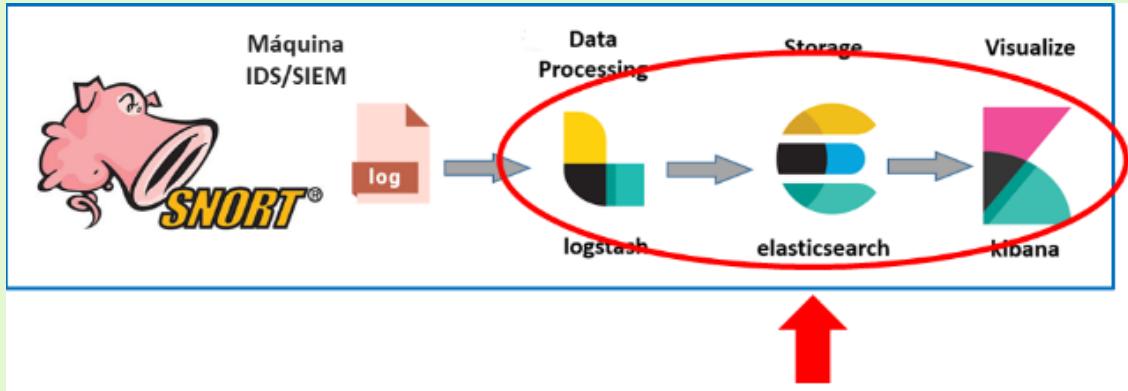
# 1.- Escenario de Trabajo SIEM.



## Caso práctico

Para implementar el SIEM se instalarán en Raspbian los componentes Linux del Stack ELK, y se visualizará en un PC el dashboard para monitorización de información y eventos de seguridad. No será preciso instalar ningún SW en el PC, sólo hará falta disponer de un navegador.

El sistema resultante permitirá efectuar las labores de Detección de Intrusos, Prevención de Ataques, monitorización de intrusiones, preparación de Cuadros de Mando, Gestión de Alarmas, etc., que son las que se efectúan habitualmente en un SOC.



[Francisco Artés - Elaboración Propia. ELK Stack en el SOC \(CC0\)](#)

Esta unidad conecta con las tareas efectuadas en la unidad anterior, esto es, Detección IDS, por lo que se partirá con Snort instalado, configurado y funcionando en la máquina DMZ1.

En esta sesión se añadirán a la máquina el resto de componentes necesarios para disponer de un SIEM completo y operativo (se recomienda utilizar como mínimo una Raspberry Pi 4B 4GB como escenario de trabajo).

Para ello, se instalarán en Raspbian los componentes Linux del Stack ELK, y se visualizará en un PC el dashboard para monitorización de información y eventos de seguridad (no se precisa instalar ningún SW en el PC, sólo hará falta disponer de un navegador).

En resumidas cuentas, el sistema resultante permitirá efectuar las labores de Detección de Intrusos, Prevención de Ataques, monitorización de intrusiones, preparación de Cuadros de Mando, Gestión de Alarmas, etc., que son las que se efectúan habitualmente en un SOC.

## 1.1.- Premisas para la Práctica SIEM.

Premisas de Partida – Snort instalado y operativo

En primer lugar y para evitar problemas durante la instalación del SIEM, nos debemos asegurar de que el fichero de alertas de Snort tenga todos los permisos:

```
sudo chmod 777 /var/log/snort_alerts.log
```

En la sesión anterior ya incluimos las reglas de detección de ICMP y TCP para levantar alertas de acceso ping y ssh, por lo que pudimos comprobar que el fichero de alertas va creciendo adecuadamente según la progresión de los ataques.

Antes de proseguir con la instalación del SW del SIEM, es conveniente comprobar también que se actualiza la fecha y hora del fichero de log interno binario de Snort:

```
ls -l /var/log/snort/snort.log
```

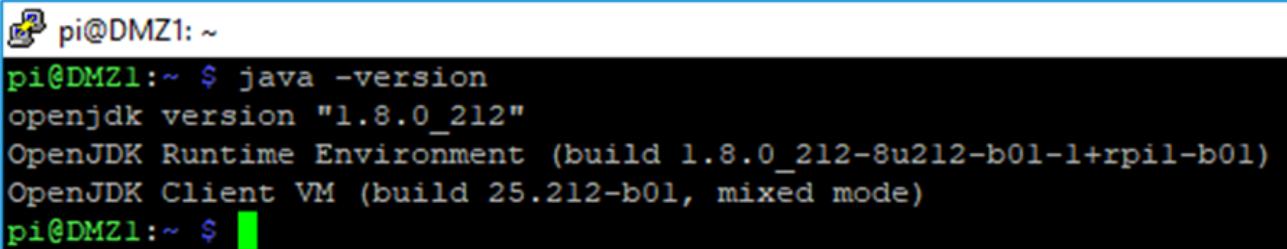
Efectuadas estas comprobaciones, detenemos Snort antes de proseguir con la instalación del SIEM:

```
sudo systemctl stop snort
```

## 1.2.- Instalación de OpenJDK.

Para comenzar, el stack ELK requiere la instalación del Open Java Development Kit, al menos en su versión 8, junto con un par de librerías adicionales (no obstante, se deberá chequear la versión del OpenJDK requerida por la versión de los productos de ELK que se vayan a instalar en cada caso):

```
sudo apt install openjdk-8-jdk libjffi-java libjffi-jni
```



A terminal window titled 'pi@DMZ1: ~' displays the command 'java -version'. The output shows the Java version as 'openjdk version "1.8.0\_212"', the 'OpenJDK Runtime Environment (build 1.8.0\_212-8u212-b01-1+rpi1-b01)', and the 'OpenJDK Client VM (build 25.212-b01, mixed mode)'. The terminal prompt 'pi@DMZ1: ~ \$' is visible at the bottom.

```
pi@DMZ1: ~ $ java -version
openjdk version "1.8.0_212"
OpenJDK Runtime Environment (build 1.8.0_212-8u212-b01-1+rpi1-b01)
OpenJDK Client VM (build 25.212-b01, mixed mode)
pi@DMZ1: ~ $
```

[Francisco Artés - Elaboración Propia. Captura de Pantalla con la Comprobación de Versión de JAVA \(CC0\)](#)

**NOTA IMPORTANTE:** Al ejecutar los comandos y transcribir los textos indicados a los ficheros correspondientes, deberemos poner especial atención en las comillas, como ya comentamos en la sesión anterior. Deberán figurar en todos los lugares indicados y no deberán ser las comillas tipográficas que en ocasiones insertan las aplicaciones de edición de textos.

## 1.3.- Instalación de Elasticsearch.

---

Elasticsearch es el corazón del SIEM.

Se trata de una base de datos tipo NoSQL, esto es, Not Only SQL. Estas bases de datos están preparadas para almacenar cualquier tipo de información de forma inmediata, aunque su formato no cuadre exactamente con la estructura interna. Esta flexibilidad unida a su capacidad para manejar grandes cantidades de datos, hacen que estos gestores de bases de datos sean muy apropiados para el ámbito de Big Data.

En el caso del SIEM su misión será almacenar toda la información relacionada con los incidentes detectados, para poder analizarla adecuadamente y extraer rápidamente las conclusiones necesarias de cara a la prevención.

## 1.3.1.- Descarga y Edición del Fichero de Configuración.

---

Descargamos el paquete Elasticsearch, que indexará y almacenará en su base de datos nuestras alertas de seguridad y nuestros logs. Lo haremos con wget y lo instalaremos con dpkg:

```
sudo wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-6.5.4.deb  
sudo dpkg -i elasticsearch-6.5.4.deb
```

Editamos el fichero de configuración de elasticsearch y asignamos los siguientes valores a las variables:

```
sudo nano /etc/elasticsearch/elasticsearch.yml
```

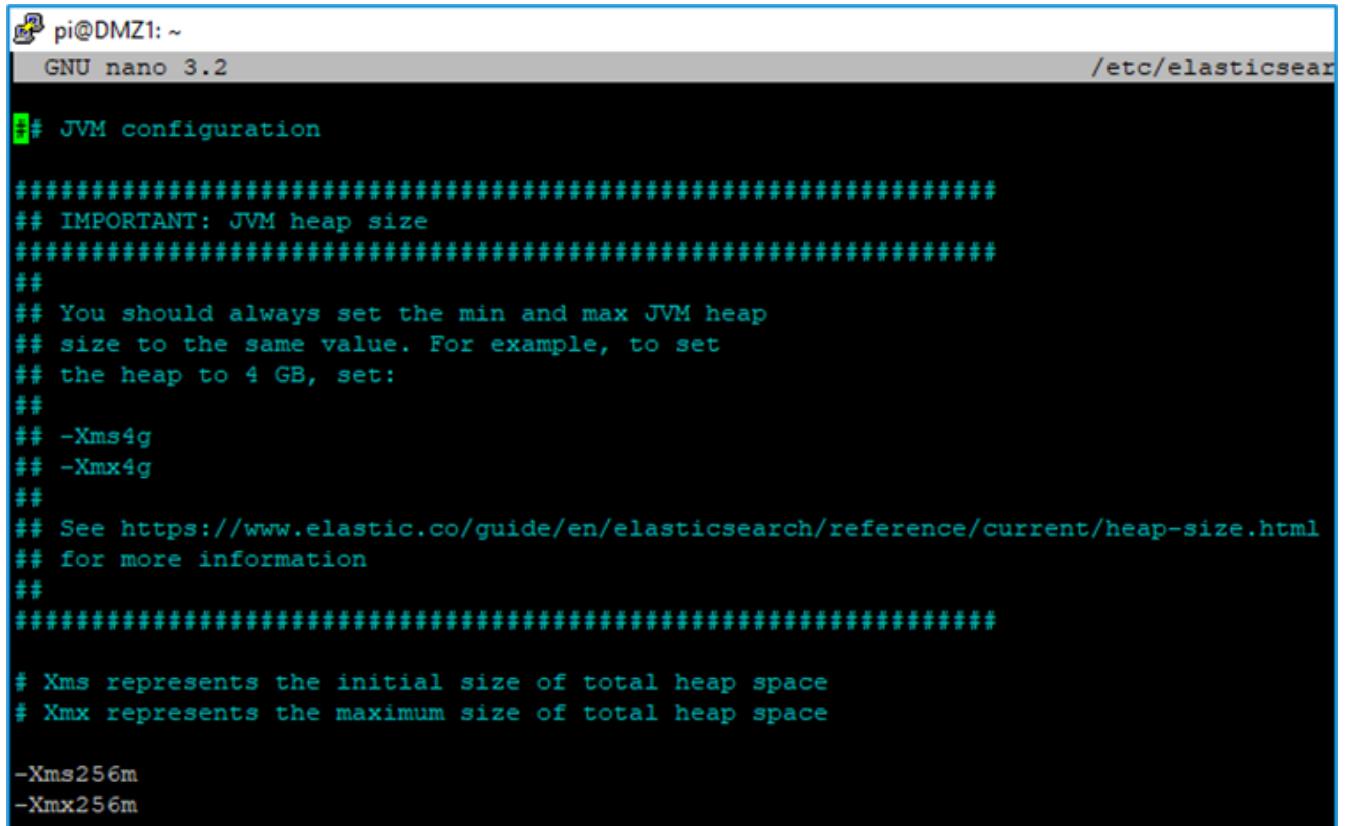
```
cluster.name: siem.sky.net  
  
node.name: node01.siem.sky.net  
  
network.host: 192.168.1.21  
  
discovery.type: single-node  
  
xpack.ml.enabled: false
```

## 1.3.2.- Limitación del Uso de la Memoria RAM.

Configuramos elasticsearch para que utilice un máximo de 256 MB de RAM, lo cual resulta más que suficiente para un ejercicio de laboratorio:

```
sudo nano /etc/elasticsearch/jvm.options
```

```
-Xms256m  
-Xmx256m
```



The screenshot shows a terminal window titled 'pi@DMZ1: ~'. The title bar also displays 'GNU nano 3.2' and the file path '/etc/elasticsearch/jvm.options'. The terminal content is a text file with the following content:

```
# JVM configuration

#####
## IMPORTANT: JVM heap size
#####
## You should always set the min and max JVM heap
## size to the same value. For example, to set
## the heap to 4 GB, set:
##
## -Xms4g
## -Xmx4g
##
## See https://www.elastic.co/guide/en/elasticsearch/reference/current/heap-size.html
## for more information
##

# Xms represents the initial size of total heap space
# Xmx represents the maximum size of total heap space

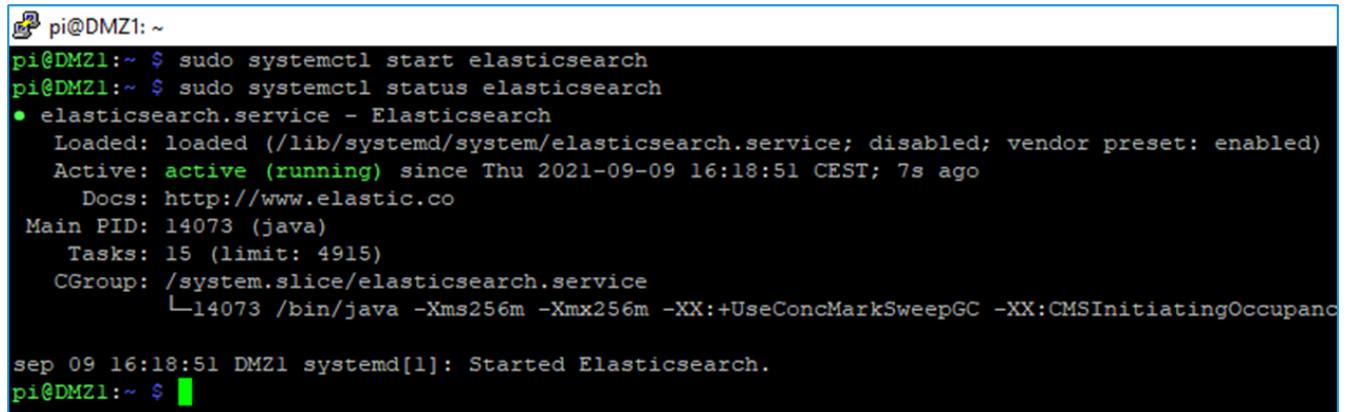
-Xms256m
-Xmx256m
```

[Francisco Artés - Elaboración Propia](#). Captura de Pantalla con el Ajuste de uso de RAM en Elasticsearch ([CC0](#))

## 1.3.3.- Arranque y Chequeo de Status.

Arrancamos Elasticsearch y comprobamos su estado:

```
sudo systemctl start elasticsearch  
sudo systemctl status elasticsearch
```



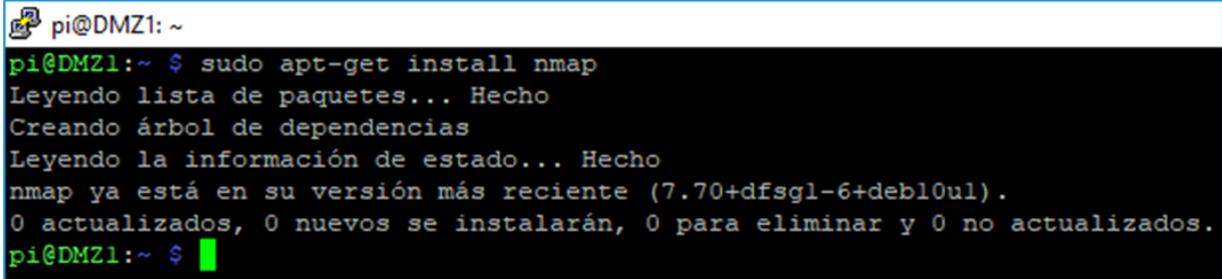
```
pi@DMZ1:~ $ sudo systemctl start elasticsearch  
pi@DMZ1:~ $ sudo systemctl status elasticsearch  
● elasticsearch.service - Elasticsearch  
  Loaded: loaded (/lib/systemd/system/elasticsearch.service; disabled; vendor preset: enabled)  
  Active: active (running) since Thu 2021-09-09 16:18:51 CEST; 7s ago  
    Docs: http://www.elastic.co  
   Main PID: 14073 (java)  
     Tasks: 15 (limit: 4915)  
    CGroup: /system.slice/elasticsearch.service  
           └─14073 /bin/java -Xms256m -Xmx256m -XX:+UseConcMarkSweepGC -XX:CMSInitiatingOccupancyFraction=75  
  
sep 09 16:18:51 DMZ1 systemd[1]: Started Elasticsearch.  
pi@DMZ1:~ $
```

[Francisco Artés - Elaboración Propia](#). Captura de Pantalla con el Arranque y Status de Elasticsearch ([CC0](#))

## 1.3.4.- Uso de Nmap para Comprobar Acceso a Elasticsearch.

Finalmente, instalamos nmap para chequear si Elasticsearch está a la escucha en el puerto adecuado:

```
sudo apt-get install nmap
```



```
pi@DMZ1: ~
pi@DMZ1: ~ $ sudo apt-get install nmap
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
nmap ya está en su versión más reciente (7.70+dfsg1-6+deb10ul).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
pi@DMZ1: ~ $
```

[Francisco Artés - Elaboración Propia](#). Captura de Pantalla con la Instalación de nmap (CC0)

Si todo está correctamente instalado y la aplicación está corriendo, Elasticsearch deberá estar a la escucha en el puerto 9200:

```
sudo nmap 192.168.1.21 -p9200
```

Además se podrá comprobar la operatividad de elasticsearch desde el PC, utilizando la dirección IP y el puerto 9200 en cualquier navegador:

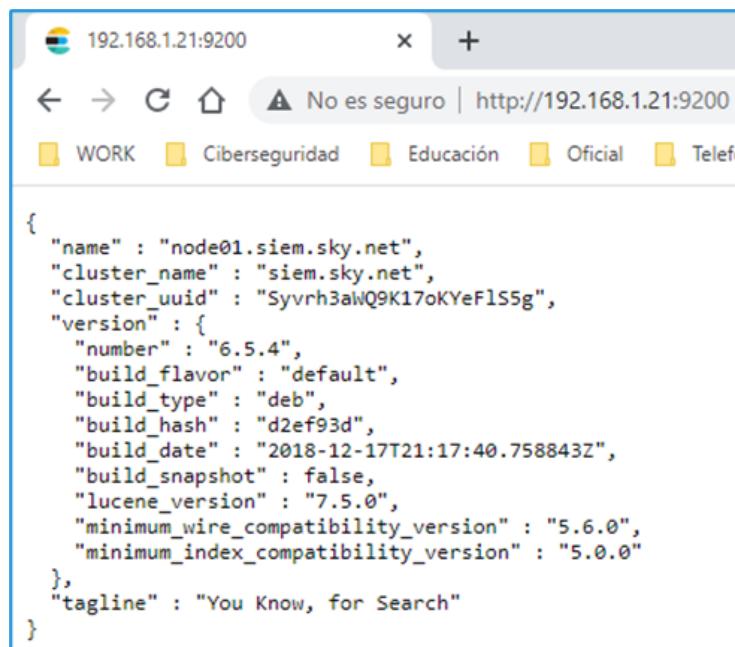
<http://192.168.1.21:9200>

```
pi@DMZ1: ~
pi@DMZ1:~ $ sudo nmap 192.168.1.21 -p9200
Starting Nmap 7.70 ( https://nmap.org ) at 2021-09-09 16:29 CEST
Nmap scan report for DMZ1 (192.168.1.21)
Host is up (0.00011s latency).

PORT      STATE SERVICE
9200/tcp  open  wap-wsp

Nmap done: 1 IP address (1 host up) scanned in 0.50 seconds
pi@DMZ1:~ $
```

Francisco Artés - Elaboración Propia. Captura de Pantalla con la Comprobación de Elasticsearch mediante nmap (CC0)



The screenshot shows a web browser window with the URL `192.168.1.21:9200` in the address bar. A warning message "No es seguro | http://192.168.1.21:9200" is displayed. Below the address bar, there is a navigation bar with icons for back, forward, search, and home, followed by a toolbar with categories: WORK, Ciberseguridad, Educación, Oficial, and Teléfono. The main content area displays the following JSON response from Elasticsearch:

```
{
  "name" : "node01.siem.sky.net",
  "cluster_name" : "siem.sky.net",
  "cluster_uuid" : "Syvrh3aWQ9K17oKYeFlSSg",
  "version" : {
    "number" : "6.5.4",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "d2ef93d",
    "build_date" : "2018-12-17T21:17:40.758843Z",
    "build_snapshot" : false,
    "lucene_version" : "7.5.0",
    "minimum_wire_compatibility_version" : "5.6.0",
    "minimum_index_compatibility_version" : "5.0.0"
  },
  "tagline" : "You Know, for Search"
}
```

Francisco Artés - Elaboración Propia. Captura de Pantalla con la Comprobación de Elasticsearch mediante Navegador (CC0)

## 1.4.- Instalación de Logstash.

---

Logstash es una herramienta de tipo ETL, esto es, *Extract, Translate & Load*.

Su misión es filtrar los datos crudos procedentes del IDS e insertar la información seleccionada en la base de datos Elasticsearch.

Como se verá a continuación, esta misión se lleva a cabo mediante entidades denominadas *pipelines*.

## 1.4.1.- Descarga, Instalación y Limitación del Uso de la RAM.

Antes de pasar a la instalación de logstash, paramos elasticsearch:

```
sudo systemctl stop elasticsearch
```

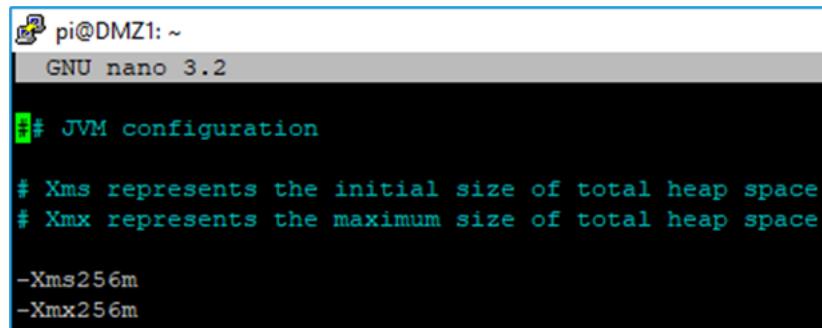
Logstash es la aplicación que analizará gramaticalmente las alertas y los logs de Snort, filtrando y estructurando la información antes de insertarla en la base de datos de Elasticsearch.

Se instala de una forma similar a elasticsearch, limitando igualmente la RAM utilizada en función de la CPU de que se disponga (recomendados también 256 MB):

```
sudo wget https://artifacts.elastic.co/downloads/logstash/logstash-6.5.4.deb  
sudo dpkg -i logstash-6.5.4.deb
```

```
sudo nano /etc/logstash/jvm.options
```

```
-Xms256m  
-Xmx256m
```



The screenshot shows a terminal window titled 'pi@DMZ1: ~' running 'GNU nano 3.2'. The content of the file is as follows:

```
# JVM configuration  
  
# Xms represents the initial size of total heap space  
# Xmx represents the maximum size of total heap space  
  
-Xms256m  
-Xmx256m
```

[Francisco Artés - Elaboración Propia](#). Captura de Pantalla con el Ajuste de RAM en Logstash (CC0)

## 1.4.2.- Edición del Fichero de Configuración, Arranque y Comprobación del Status.

---

Editamos el fichero de configuración de logstash y asignamos los siguientes valores a las variables (atención a la dirección IP, que en este caso va entre comillas dobles):

```
sudo nano /etc/logstash/logstash.yml
```

```
node.name: node01.siem.sky.net
http.host: "192.168.1.21"
xpack.monitoring.enabled: false
xpack.management.enabled: false
```

Finalmente, arrancamos logstash, chequeamos su log de arranque para ver si todo ha ido bien, y lo detenemos antes de proseguir con la instalación de kibana:

```
sudo systemctl start logstash
sudo systemctl status logstash
```

## 1.4.3.- Revisión del Log de Arranque y Parada de la Aplicación.

---

Esperamos 2 minutos y chequeamos el log de arranque:

```
sudo tail -f /var/log/logstash/logstash-plain.log
```

Se observarán varios mensajes de error notificando que aún falta completar la configuración, no obstante, si aparece el mensaje "Successfully started Logstash API endpoint", esto indicará que todo ha ido bien.

Antes de proseguir, detenemos logstash y comprobamos que está parado:

```
sudo systemctl stop logstash
```

```
sudo systemctl status logstash
```

Deberá aparecer que está "inactive" o "failed"

## 1.5.- Instalación de Kibana.

---

En el stack ELK, Kibana es la herramienta que se utiliza para construir cuadros de mando interactivos (dashboards) y monitorizar las notificaciones y las alarmas.

Kibana 6.5.4 depende de Node.js 8.14. Esta versión de Node.js no es la que incluye de serie la instalación de Kibana. A continuación veremos cómo sustituirla.

**IMPORTANTE:** Kibana no puede convivir con otras aplicaciones que ocupen el puerto 80 en la misma máquina, por ejemplo, Apache. Si las hubiera, sería necesario desinstalarlas antes de proseguir con la instalación de Kibana.



[Elastic](#). Logotipo de Kibana (CC0)

## 1.5.1.- Descarga de Node.js.

---

Situarse en el directorio home del usuario sudoer (pi):

```
cd
```

Descargar la versión mencionada de Node.js siguiendo detalladamente los pasos que se indican a continuación.

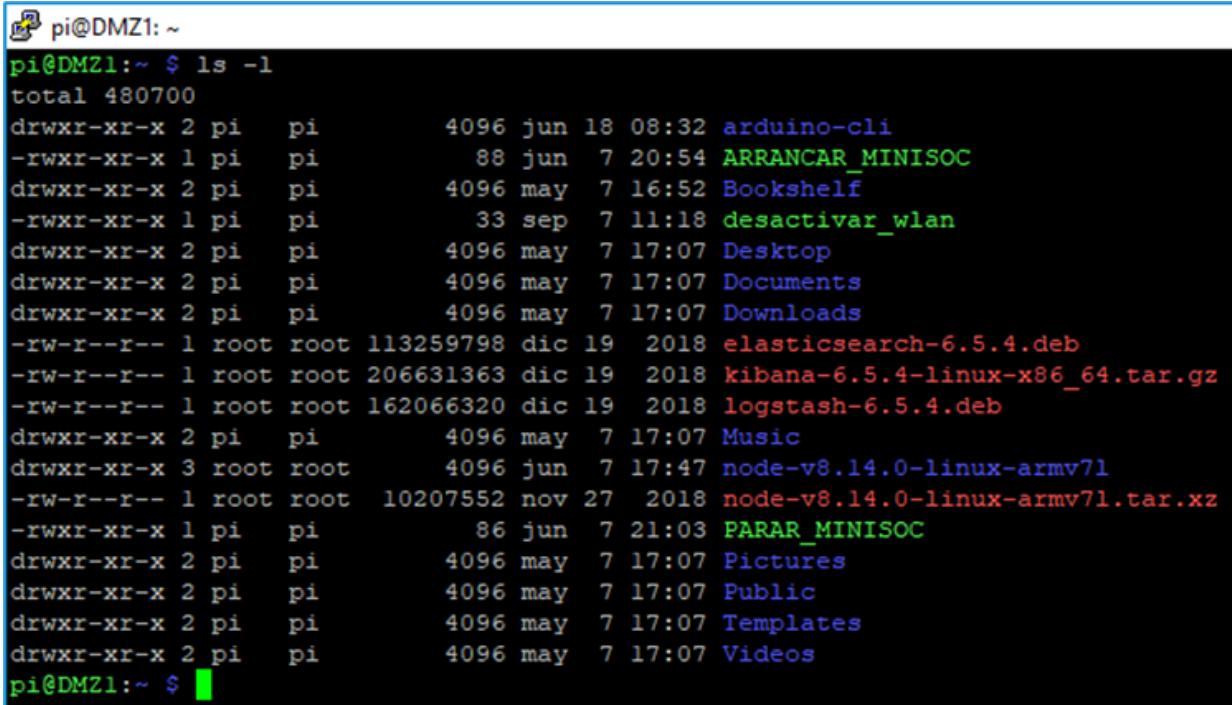
Tras este procedimiento, el ejecutable quedará situado en el directorio correcto.

```
sudo wget https://nodejs.org/dist/v8.14.0/node-v8.14.0-linux-armv7l.tar.xz  
sudo tar -xvf node-v8.14.0-linux-armv7l.tar.xz node-v8.14.0-linux-armv7l/bin/node  
cd node-v8.14.0-linux-armv7l/bin  
sudo cp ./node /usr/local/bin/  
cd
```

## 1.5.2.- Procedimiento de Instalación.

Instalar Kibana mediante el siguiente procedimiento:

```
sudo wget https://artifacts.elastic.co/downloads/kibana/kibana-6.5.4-linux-x86_64.tar.gz  
sudo mkdir /usr/share/kibana/  
sudo tar -xvf kibana-6.5.4-linux-x86_64.tar.gz --strip 1 --directory /usr/share/kibana/
```



```
pi@DMZ1:~ $ ls -l  
total 480700  
drwxr-xr-x 2 pi pi 4096 jun 18 08:32 arduino-cli  
-rwxr-xr-x 1 pi pi 88 jun 7 20:54 ARRANCAR_MINISOC  
drwxr-xr-x 2 pi pi 4096 may 7 16:52 Bookshelf  
-rwxr-xr-x 1 pi pi 33 sep 7 11:18 desactivar_wlan  
drwxr-xr-x 2 pi pi 4096 may 7 17:07 Desktop  
drwxr-xr-x 2 pi pi 4096 may 7 17:07 Documents  
drwxr-xr-x 2 pi pi 4096 may 7 17:07 Downloads  
-rw-r--r-- 1 root root 113259798 dic 19 2018 elasticsearch-6.5.4.deb  
-rw-r--r-- 1 root root 206631363 dic 19 2018 kibana-6.5.4-linux-x86_64.tar.gz  
-rw-r--r-- 1 root root 162066320 dic 19 2018 logstash-6.5.4.deb  
drwxr-xr-x 2 pi pi 4096 may 7 17:07 Music  
drwxr-xr-x 3 root root 4096 jun 7 17:47 node-v8.14.0-linux-armv7l  
-rw-r--r-- 1 root root 10207552 nov 27 2018 node-v8.14.0-linux-armv7l.tar.xz  
-rwxr-xr-x 1 pi pi 86 jun 7 21:03 PARAR_MINISOC  
drwxr-xr-x 2 pi pi 4096 may 7 17:07 Pictures  
drwxr-xr-x 2 pi pi 4096 may 7 17:07 Public  
drwxr-xr-x 2 pi pi 4096 may 7 17:07 Templates  
drwxr-xr-x 2 pi pi 4096 may 7 17:07 Videos  
pi@DMZ1:~ $
```

[Francisco Artés - Elaboración Propia](#). Captura de Pantalla con la Comprobación de la Descarga de Kibana ([CC0](#))

## 1.5.3.- Configuración de Kibana.

Configurar Kibana editando el fichero siguiente:

```
sudo nano /usr/share/kibana/config/kibana.yml
```

Incluyendo las siguientes variables en su interior (no borrar las comillas):

```
server.port: 80  
server.host: "192.168.1.21"  
server.name: node01.siem.sky.net  
elasticsearch.url: "http://192.168.1.21:9200"  
logging.dest: /var/log/kibana.log
```

```
# The Kibana server's name. This is used for display purposes.  
server.name: node01.siem.sky.net  
  
# The URL of the Elasticsearch instance to use for all your queries.  
elasticsearch.url: "http://192.168.1.21:9200"
```

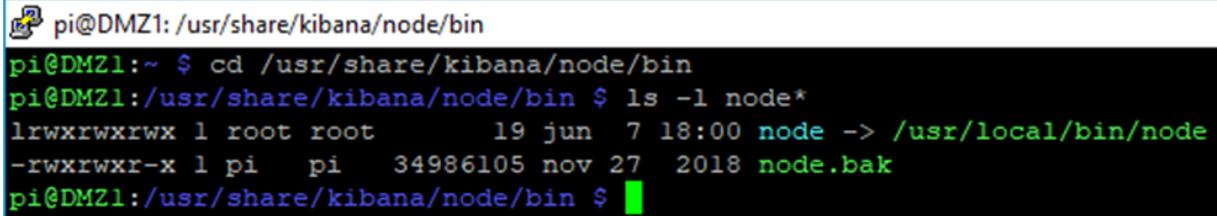
[Francisco Artés - Elaboración Propia](#). Captura de Pantalla con la Configuración de Kibana ([CC0](#))

## 1.5.4.- Sustitución de Node.js por su Versión Correcta.

---

Desactivar el Node.js que trae incluido Kibana, e indicarle que use la versión descargada ad hoc:

```
sudo mv /usr/share/kibana/node/bin/node /usr/share/kibana/node/bin/node.bak  
sudo ln -s /usr/local/bin/node /usr/share/kibana/node/bin/node
```



```
pi@DMZ1: /usr/share/kibana/node/bin  
pi@DMZ1:~ $ cd /usr/share/kibana/node/bin  
pi@DMZ1:/usr/share/kibana/node/bin $ ls -l node*  
lrwxrwxrwx 1 root root    19 jun  7 18:00 node -> /usr/local/bin/node  
-rwxrwxr-x 1 pi   pi  34986105 nov 27  2018 node.bak  
pi@DMZ1:/usr/share/kibana/node/bin $
```

[Francisco Artés - Elaboración Propia](#). Captura de Pantalla con la Sustitución de Node (CC0)

## 1.5.5.- Edición de un Fichero de Servicio y Arranque.

Escribir un fichero de servicio "Systemd" para arrancar y parar Kibana:

```
sudo nano /etc/systemd/system/kibana.service
```

Incluir este contenido en el fichero de servicio:

```
[Unit]
Description=Kibana

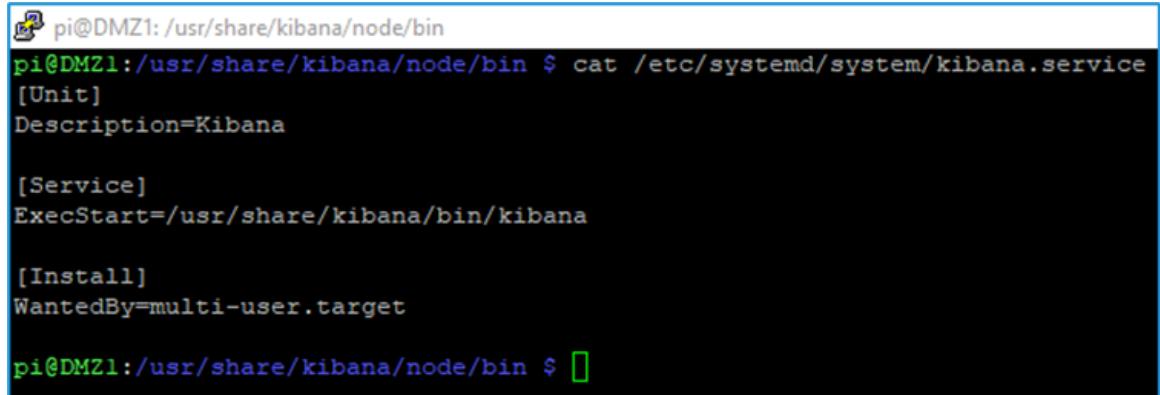
[Service]
ExecStart=/usr/share/kibana/bin/kibana

[Install]
WantedBy=multi-user.target
```

Arrancar Kibana y comprobar su status:

```
sudo systemctl start kibana
sudo systemctl status kibana
```

Deberá aparecer que está "active (running)"



```
pi@DMZ1: /usr/share/kibana/node/bin
pi@DMZ1:/usr/share/kibana/node/bin $ cat /etc/systemd/system/kibana.service
[Unit]
Description=Kibana

[Service]
ExecStart=/usr/share/kibana/bin/kibana

[Install]
WantedBy=multi-user.target

pi@DMZ1:/usr/share/kibana/node/bin $
```



## 1.6.- Configuración SIEM.

---

Una vez que se han instalado todas las piezas de la torre ELK y se ha efectuado su configuración de bajo nivel, se puede dar paso al proceso de configuración funcional.

En él se verá que la configuración de Elasticsearch es prácticamente inexistente, mientras que Logstash requerirá definir pipelines y Kibana requerirá definir métricas y tableros.

## 1.6.1.- Arranque del SIEM.

---

Reiniciar el host:

```
sudo reboot
```

Arrancar Elasticsearch siempre ANTES que kibana:

```
sudo systemctl start elasticsearch  
sudo systemctl status elasticsearch
```

Arrancar Kibana:

```
sudo systemctl start kibana  
sudo systemctl status kibana
```

Comprobar que está arrancado Elasticsearch mediante el navegador del PC (devolverá su lista de características en formato JSON):

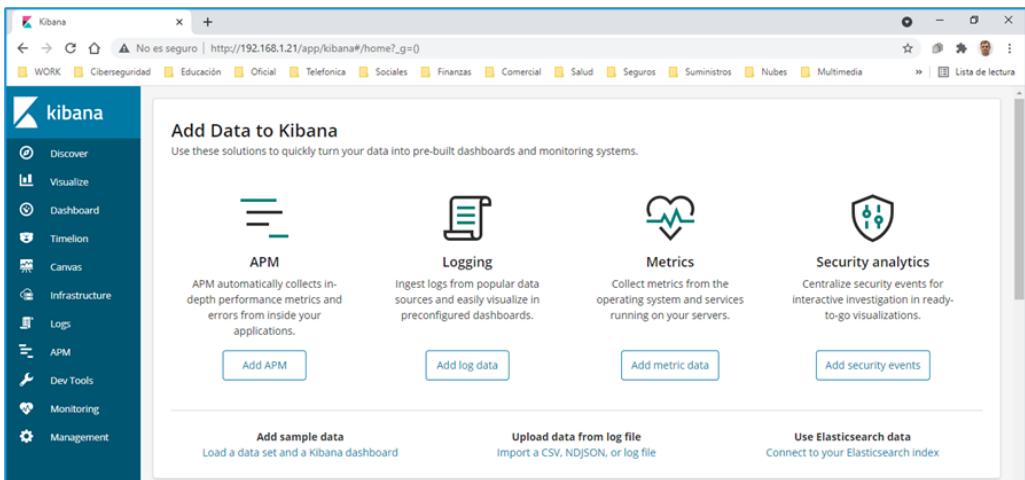
```
http://192.168.1.21:9200
```

Esperar 10 minutos antes de comprobar que está arrancado Kibana, introduciendo su URL en el navegador del PC (arrancará la Home de Kibana):

```
http://192.168.1.21
```

Arrancar el resto de las aplicaciones del SOC y comprobar que quedan activas:

```
sudo systemctl start logstash  
sudo systemctl status logstash  
sudo systemctl start snort  
sudo systemctl status snort
```



[Francisco Artés - Elaboración Propia](#). Captura de Pantalla con la Home de Kibana ([CC0](#))

## 1.6.2.- Pipelines en Logstash.

Configuración de logstash para capturar el log de Snort, procesar sus mensajes y grabarlos en Elasticsearch.

Para esto hay que definir una tubería de logstash (pipeline), con entrada, filtrado y salida hacia elasticsearch, en el fichero `/etc/logstash/conf.d/logstash.conf`

Las tuberías o pipelines tienen:

- ✓ **Entrada.** Indicación del punto de captura de datos, que puede ser un fichero local o remoto, un punto de acceso a un protocolo de comunicaciones, etc.
- ✓ **Filtrado.** La información de los logs y de los ficheros de trabajo está estructurada de forma muy variada, por lo que hay que utilizar la herramienta de filtrado Grok para formatearla antes de insertarla en la base de datos. Esta herramienta está incluida dentro de Logstash.
- ✓ **Salida.** Logstash puede producir salidas en varios formatos de ficheros, o bien, grabarla directamente en una base de datos NoSQL, como es el caso de Elasticsearch.

### Entrada al Pipeline

Log de Snort que leerá Logstash:

```
/var/log/snort_alerts.log
```

Como resultado de la configuración efectuada en la sesión anterior, en el fichero `/etc/snort/rules/local.rules` tendremos las reglas siguientes:

```
# Regla para detectar un ping (ICMP)

alert icmp any any -> $HOME_NET any (msg: "¡Trafico ICMP!"; sid:3000001;)

#Regla para detectar un ssh (TCP y puerto 22)

alert tcp any any -> any 22 (msg: "Acceso SSH"; sid:3000002;)
```

Editamos pues el fichero `/etc/logstash/conf.d/logstash.conf`.

Creamos la entrada a Logstash, para captura del fichero de log de Snort.

```
input {
    file {
        path => ["/var/log/snort_alerts.log"]
```

```
    start_position => beginning

}

}
```

## Filtrado Grok en el Pipeline

Se efectuará el filtrado de la información entrante al pipeline con la potente herramienta Grok. Aunque la construcción de los patrones Grok se revisará a continuación con varios ejemplos, en este momento estudiaremos un patrón sencillo, con la sintaxis siguiente:

```
filter {

  grok {

    match => {"message" => "%{GREEDYDATA:cadena}"}

  }
}
```

Este patrón es el más simple de todos, pues captura una línea completa del log de Snort, la asigna a variable “cadena” como un string, y la inserta en la base de datos de elasticsearch.

Existe abundante documentación descriptiva de la sintaxis de los Grok Patterns.

Además, en Kibana hay un depurador Grok que permite ejecutar reglas de forma unitaria sobre una línea de log de muestra y comprobar si las reglas funcionan correctamente.

kibana -> Dev Tools -> Grok Debugger

Sample Data

```
1 Sep 29 17:37:38 claudiosiem snort: [1:3000002:0] Acceso SSH {TCP} 192.168.1.64:55317 -> 192.168.1.29:22
2
```

Grok Pattern

```
1 %{GREEDYDATA:cadena}
2
```

> Custom Patterns

[Simulate](#)

Structured Data

```
1 {
2   "cadena": "Sep 29 17:37:38 claudiosiem snort: [1:3000002:0] Acceso SSH {TCP} 192.168.1.64:55317 -> 192.168.1.29:22"
3 }
```

[Francisco Artés - Elaboración Propia](#). Captura de Pantalla del Grok Debugger ([CC0](#))

## Salida del Pipeline hacia Elasticsearch

Definición de la salida del pipeline, que en este caso será el índice “logstash” en la base de datos Elasticsearch:

```
output {
  elasticsearch {
    hosts => [ "http://192.168.1.21:9200" ]
    index => "logstash"
  }
}
```

## Comprobación del Funcionamiento del Pipeline

Para comprobar el funcionamiento del pipeline recién creado, lanzaremos un Ping y un ataque SSH desde otra máquina en sendos terminales, de forma que se registren los eventos asociados a dichos ataques.

[Francisco Artés - Elaboración Propia](#). Captura de Pantalla con Detección de Tráfico SSH ([CCO](#))

Desde kibana se podrá comprobar que Elasticsearch está ingiriendo la información formateada que le envía logstash a través de la tubería creada.

Para ello se deberá ir a Dev Tools, seleccionar Console y lanzar el comando siguiente para ver el contenido del índice logstash:

POST logstash/\_search

The screenshot shows the Kibana interface with the sidebar menu open. The 'Dev Tools' option is selected. In the main area, the 'Console' tab is active, displaying a command-line interface. A POST request is being typed into the input field:

```
1 POST logstash/_search
```

[Francisco Artés - Elaboración Propia](#). Captura de Pantalla con el Comando POST (CC0)

Se obtendrá una respuesta similar a la de la figura adjunta.

The screenshot shows the Kibana interface with the sidebar menu open. The 'Dev Tools' option is selected. In the main area, the 'Console' tab is active, displaying a command-line interface. The previous POST request has been executed, and the resulting JSON response is shown in the output area:

```
1 {  
2   "took" : 16,  
3   "timed_out" : false,  
4   "_shards" : {  
5     "total" : 5,  
6     "successful" : 5,  
7     "skipped" : 0,  
8     "failed" : 0  
9   },  
10  "hits" : {  
11    "total" : 1454347,  
12    "max_score" : 1.0,  
13    "hits" : [  
14      {  
15        "_index" : "logstash",  
16        "_type" : "doc",  
17        "_id" : "xb0qDXUBy2YtQahxgJ41",  
18        "score" : 1.0,  
19        "_source" : {  
20          "@timestamp" : "2020-10-09T15:11:13.328Z",  
21          "path" : "/var/log/snort_alerts.log",  
22          "@version" : "1",  
23          "message" : "Oct 9 17:11:12 claudiosiem snort: [1:527:8] BAD  
-TRAFFIC same SRC/DST [Classification: Potentially Bad Traffic]  
[Priority: 2] {IPV6-ICMP} :: -> ff02::1:ff3b:4c89",  
24          "tags" : [  
25            "_grokparsefailure"  
26          ],  
27          "host" : "claudiosiem"  
28      }  
29    }  
30  }  
31 }
```

[Francisco Artés - Elaboración Propia](#). Captura de Pantalla con el Resultado del Comando POST (CC0)

## Patrón Grok Genérico para un String

Sep 29 17:37:38 claudiosiem snort: [1:3000002:0] Acceso SSH {TCP} 192.168.1.64:55317 -> 192.168.1.64:22

```
%{GREEDYDATA:cadena}

{
    "cadena": "Sep 29 17:37:38 claudiosiem snort: [1:3000002:0] Acceso SSH {TCP} 192.168.1.64:55317 -> 192.168.1.64:55317"
}
```

Nota. GREEDYDATA. Patrón “Codicioso” – No filtra nada. Captura TODO y lo guarda en una variable

## Patrón Grok para Extraer Varios Campos

```
Sep 29 17:37:38 claudiosiem snort: [1:3000002:0] Acceso SSH {TCP} 192.168.1.64:55317 -> 192.168.1.64:55317

%{MONTH:mes}%{SPACE}%{MONTHDAY:dia}%{SPACE}%{HOUR:hora}: %{MINUTE:minutos}: %{SECOND:segundos} %{CRLF}

{
    "hora": "17",
    "resto_mensaje": " claudiosiem snort: [1:3000002:0] Acceso SSH {TCP} 192.168.1.64:55317 -> 192.168.1.64:55317",
    "segundos": "38",
    "mes": "Sep",
    "minutos": "37",
    "dia": "29"
}
```

## Patrón Grok Literal para Extraer Todos los Campos

```
Sep 29 17:37:38 claudiosiem snort: [1:3000002:0] Acceso SSH {TCP} 192.168.1.64:55317 -> 192.168.1.29

%{MONTH:mes}%{SPACE}%{MONTHDAY:dia}%{SPACE}%{HOUR:hora}: %{MINUTE:minutos}: %{SECOND:segundos} %{

{
    "accion": "Acceso", "nombre_maquina": "claudiosiem", "ip_destino": "192.168.1.29", "ip_o
```

## Patrón con Comodines (Puntos)

```
Sep 29 17:37:38 claudiosiem snort: [1:3000002:0] Acceso SSH {TCP} 192.168.1.64:55317 -> 192.168.1.29

%{MONTH:mes}.%{MONTHDAY:dia}.%{HOUR:hora}.%{MINUTE:minutos}.%{SECOND:segundos}.%{WORD:nombre_maquina}

{
    "accion": "Acceso",
    "nombre_maquina": "claudiosiem",
    "ip_destino": "192.168.1.29",
    "ip_origen": "192.168.1.64"
}
```

## Patrón Grok con Timestamp y Greedydata

```
Sep 29 17:37:38 claudiosiem snort: [1:3000002:0] Acceso SSH {TCP} 192.168.1.64:55317 -> 192.168.1.29:22  
%{SYSLOGTIMESTAMP:fecha}.%{WORD:maquina}%{GREEDYDATA:mensaje}%{IP:dir_a}:%{INT:port_a}...%{IP:dir_b}:%{INT:port_b}  
{ "fecha": "Sep 29 17:37:38", "dir_b": "192.168.1.29", "port_a": "55317", "port_b": "22",  
  "maquina": "claudiosiem", "mensaje": "Acceso SSH", "dir_a": "192.168.1.64", "ip": "192.168.1.64", "int": 55317}
```

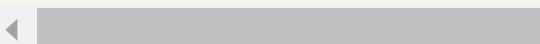
## Pipeline para Inyección de Snort a Kibana

Para continuar con nuestro laboratorio y diseñar un dashboard en Kibana, asignaremos el siguiente contenido al fichero /etc/logstash/conf.d/logstash.conf, antes de proseguir:

```
input {
    file {
        path => [ "/var/log/snort_alerts.log" ]
        start_position => beginning
    }
}

filter {
    grok {
        match => { "message" => "%{SYSLOGTIMESTAMP:fecha_y_hora}.%{WORD:maquina}.%{WORD:nombre_ids}" }
        match => { "message" => "%{SYSLOGTIMESTAMP:fecha_y_hora}.%{WORD:maquina}.%{WORD:nombre_ids}" }
    }
}

output {
    elasticsearch {
        hosts => [ "http://192.168.1.21:9200" ]
        index => "logstash"
    }
}
```

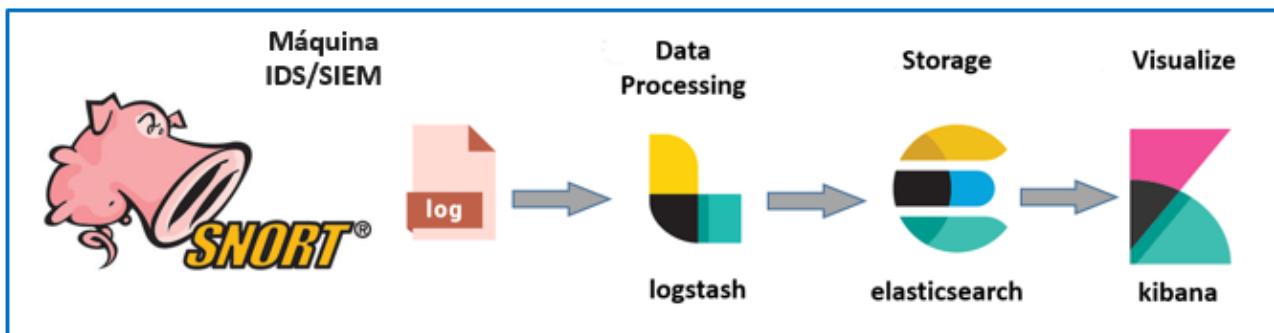


## 1.7.- Visualización SIEM.

A continuación monitorizaremos con Kibana la información que Logstash ha capturado de Snort, filtrado con Grok, e insertado en la base de datos de Elasticsearch.

Para ello, localizaremos la información en Elasticsearch a partir del índice creado por Logstash, añadiremos métricas basadas en dicho índice, y finalmente crearemos tableros basados en estas métricas.

Hecho esto, generaremos tráfico ICMP y SSH desde otra máquina para ver cómo se detectan dichos ataques y cómo se muestran en el tablero correspondiente.

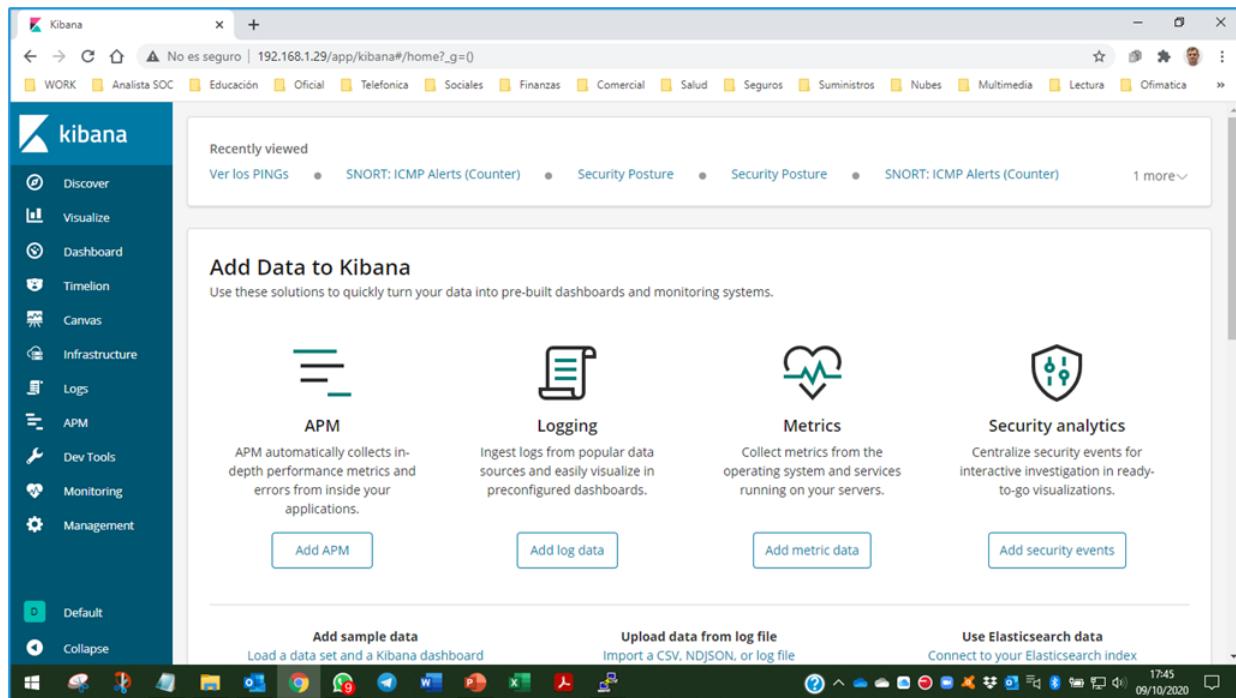


[Francisco Artés - Elaboración Propia. IDS y SIEM \(CC0\)](#)

# 1.7.1.- Arranque de Kibana desde el Navegador.

Arrancamos un navegador en el PC y escribimos la dirección de la máquina DMZ1 (sin especificar ningún puerto).

Si el stack ELK está correctamente arrancado, se visualizará la Home de Kibana.

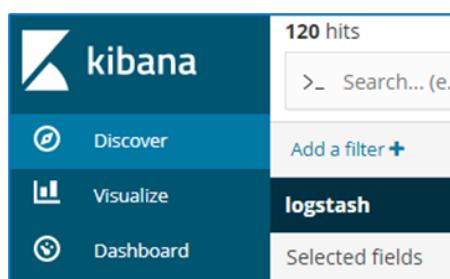


[Francisco Artés - Elaboración Propia.](#) Captura de Pantalla con la Home de Kibana (CC0)

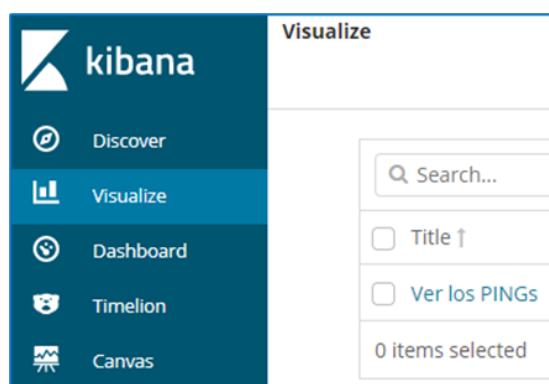
## 1.7.2.- Configuración de Kibana.

Para la configuración de Kibana, usaremos principalmente las siguientes secciones del menú de la página web:

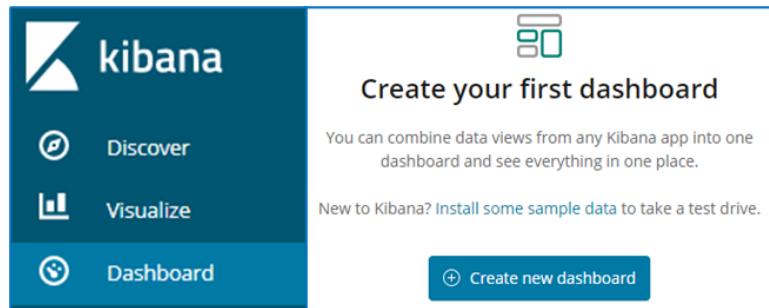
- ✓ **Discover.** En esta sección se localizan los índices creados en la base de datos. En nuestro caso, el índice que ha creado y que alimenta nuestro pipeline se denomina “logstash”.
- ✓ **Visualize.** Sección para la creación de métricas. Aquí definiremos métricas para Ping y para SSH. Programaremos además un refresco periódico (por ejemplo, 5 segundos), porque en caso contrario el tablero sólo efectuará una primera consulta al índice y se detendrá.
- ✓ **Dashboard.** Sección para diseño de Tableros o Cuadros de Mando, en función de las métricas definidas en el paso anterior.



[Francisco Artés - Elaboración Propia. Captura de Pantalla con Kibana Discover \(CC0\)](#)



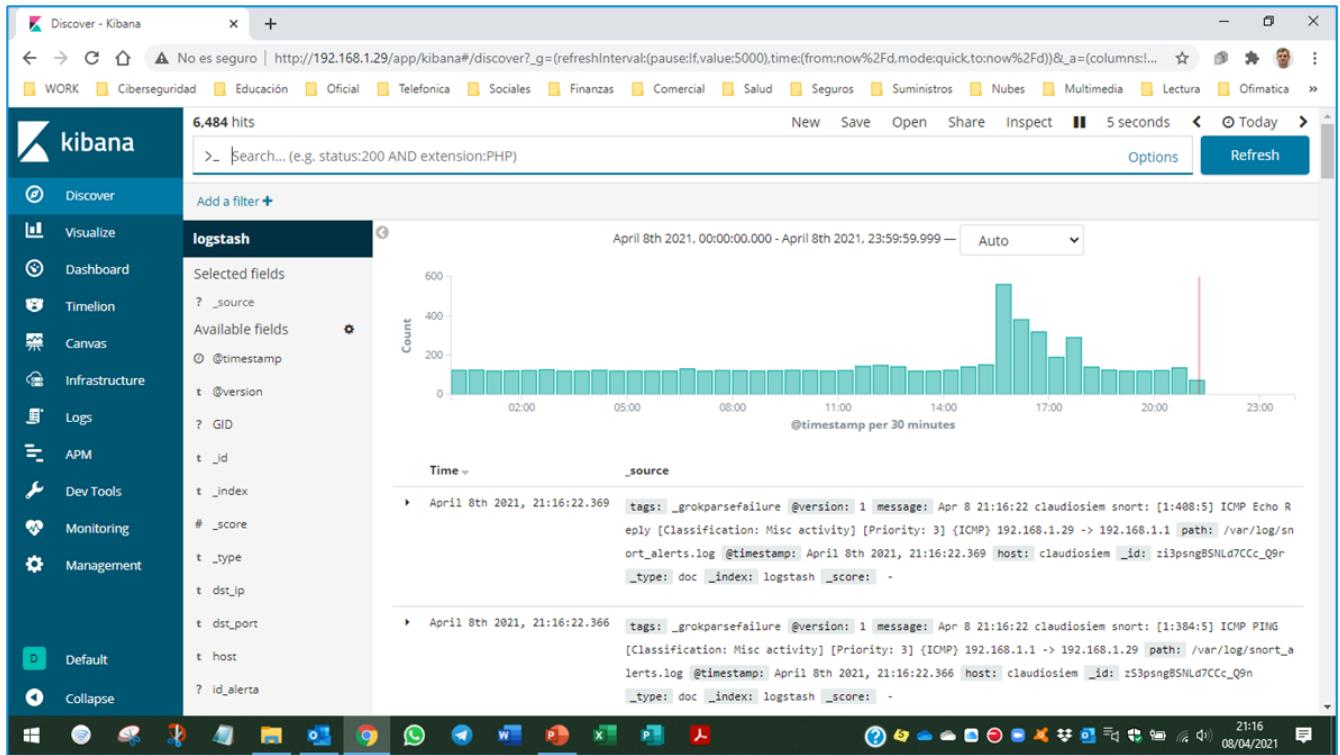
[Francisco Artés - Elaboración Propia. Captura de Pantalla con Kibana Visualize \(CC0\)](#)



[Francisco Artés - Elaboración Propia](#). Captura de Pantalla con Kibana Dashboard ([CC0](#))

## 1.7.3.- Manejo de Kibana.

El índice "logstash" que hemos creado ya contiene la historia de todos los ataques efectuados desde el momento de su creación.



Francisco Artés - Elaboración Propia. Captura de Pantalla con el Contenido del Índice Logstash (CCO)

The screenshot shows the Kibana Discover interface. On the left sidebar, the 'Discover' option is selected. In the main area, the 'logstash' index is chosen. A yellow callout box highlights the 'Selected fields' section, which lists '\_source', 'puerto\_a', 'message', 'dir\_b', 'proceso', 'host', 'fecha\_y\_hora', 'maquina', 'mensaje', 'dir\_a', 'path', 'protocolo', 'TCP', 'nombre\_ids', 'snort', '@timestamp', and '\_id'. Below this, a list of log entries is displayed, each containing these fields. The status bar at the bottom shows the date as 10/09/2021 and the time as 11:17.

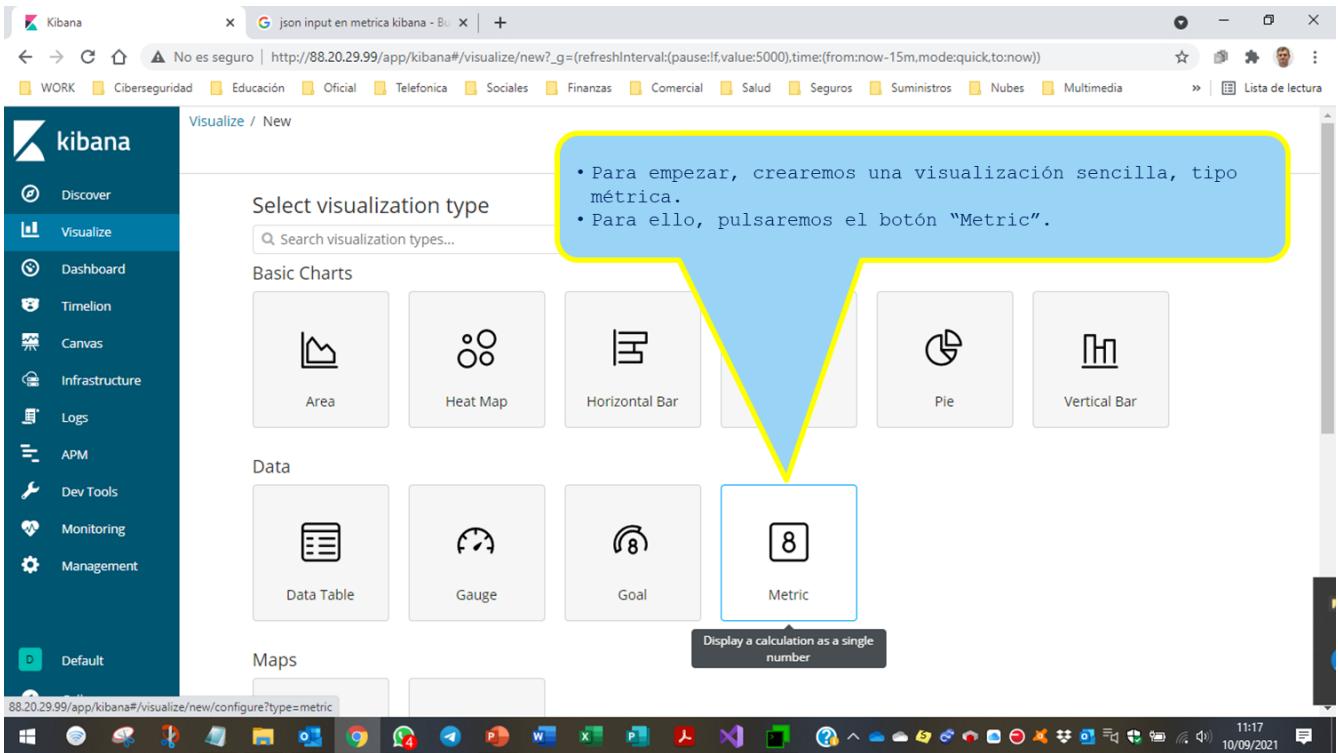
- Mediante la opción "Discover" Se abrirá una pantalla en la que podremos ver el índice "logstash" creado en la base de datos Elasticsearch.
- Seleccionando dicho índice, podremos ver también la información que se está registrando en él a partir del log de Snort.

Francisco Artés - Elaboración Propia. Captura de Pantalla con el Discover del Índice Logstash (CC0)

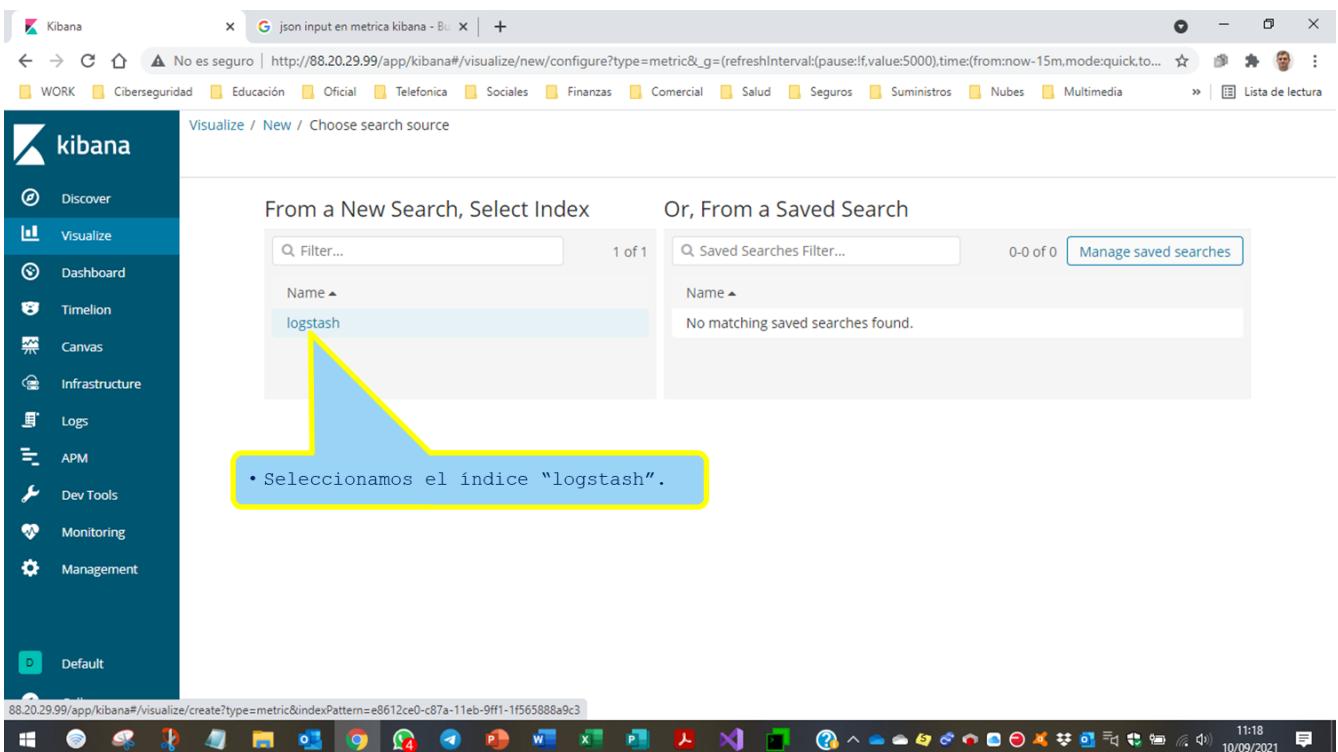
The screenshot shows the Kibana Visualize interface. On the left sidebar, the 'Visualize' option is selected. The main area displays a search bar, a button to 'Create a visualization', and a message stating 'Looks like you don't have any visualizations. Let's create some!'. Below this, it says '0 items selected'. A yellow callout box highlights the 'Create a visualization' button. The status bar at the bottom shows the date as 10/09/2021 and the time as 11:17.

- Para crear una visualización a partir de los datos del índice, seleccionamos la opción "Visualize" y pulsamos el botón "Create a visualization"

Francisco Artés - Elaboración Propia. Captura de Pantalla con la Creación de una Visualización (CC0)



Francisco Artés - Elaboración Propia. Captura de Pantalla con la Creación de una Métrica (CC0)



Francisco Artés - Elaboración Propia. Captura de Pantalla con la Selección de Índice (CC0)

The screenshot shows the Kibana Visualize interface. On the left, the sidebar includes options like Discover, Visualize, Dashboard, Timelion, Canvas, Infrastructure, Logs, APM, Dev Tools, Monitoring, and Management. The main area is titled "Visualize / New Visualization (unsaved)". It has a search bar and a "Add a filter" button. Below that is a "logstash" card with "Metrics" and "Buckets" sections. In the Metrics section, there is a "Metric Count" entry with a "Count help" link. A yellow callout box points to this entry with the following text:

- Creamos un contador, para lo cual seleccionaremos la opción "Count".
- Por el momento hay creado ningún filtro, por lo que se visualizará el recuento de todos los eventos registrados en el índice hasta el momento, independientemente de su naturaleza.

On the right, a large digital gauge displays the value "8,728" with the label "Count" below it. The top right of the interface shows "Save", "Share", "Inspect", "Refresh", "Options", and a "Refresh" button. The bottom right shows the date and time: "11:18 10/09/2021".

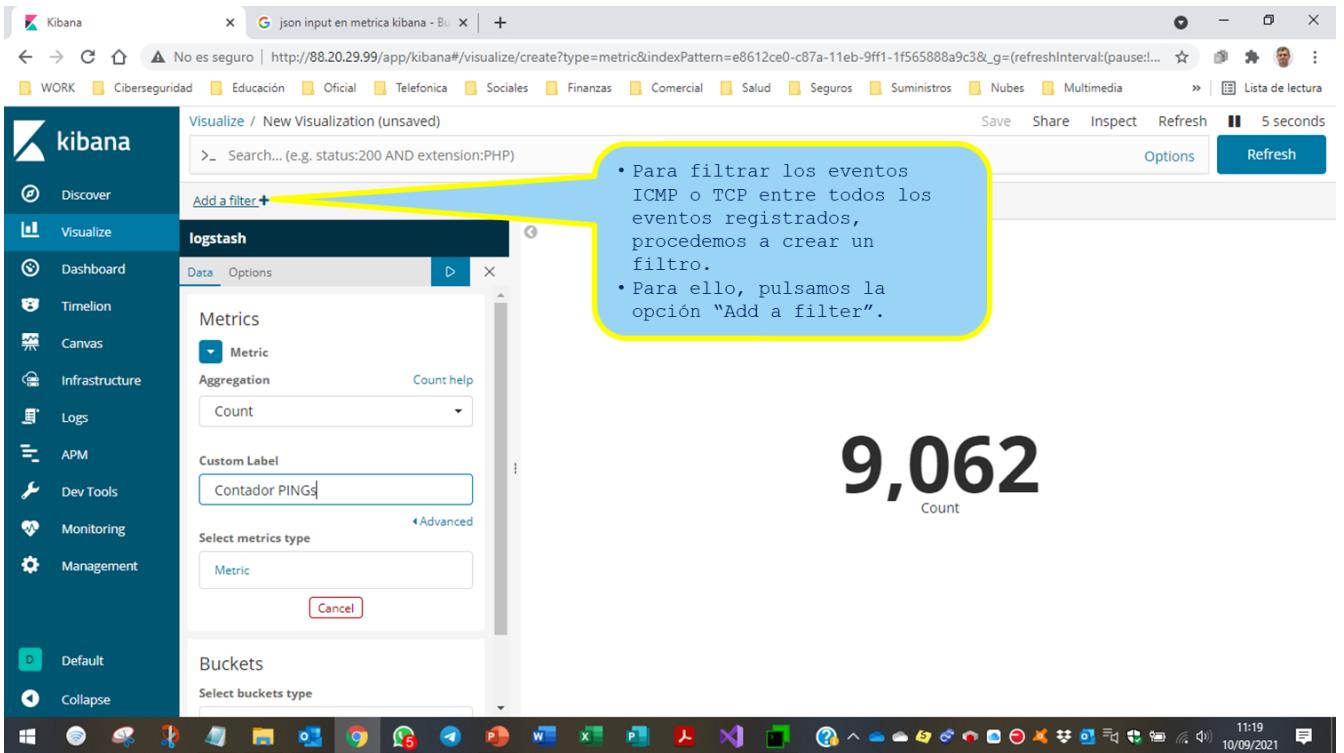
Francisco Artés - Elaboración Propia. Captura de Pantalla con la Creación de un Contador (CC0)

This screenshot shows the same Kibana Visualize interface as the previous one, but with a different configuration. The "Metrics" section now shows a "Metric" entry with a "Count" aggregation type and a "Custom Label" field containing "Contador PINGs". A yellow callout box points to this "Custom Label" field with the following text:

- Vamos a crear dos contadores, uno para ICMP y otro para eventos TCP, por lo que los denominaremos "Contador PINGs" y "Contador SSH".

On the right, the digital gauge displays the value "8,973" with the label "Count" below it. The top right of the interface shows "Save", "Share", "Inspect", "Refresh", "Options", and a "Refresh" button. The bottom right shows the date and time: "11:18 10/09/2021".

Francisco Artés - Elaboración Propia. Captura de Pantalla con el Etiquetado del Contador (CC0)



Visualize / New Visualization (unsaved)

Search... (e.g. status:200 AND extension:PHP)

Add a filter +

logstash

Data Options

Metrics

Metric

Aggregation Count help

Count

Custom Label Contador PING\$

Select metrics type Metric

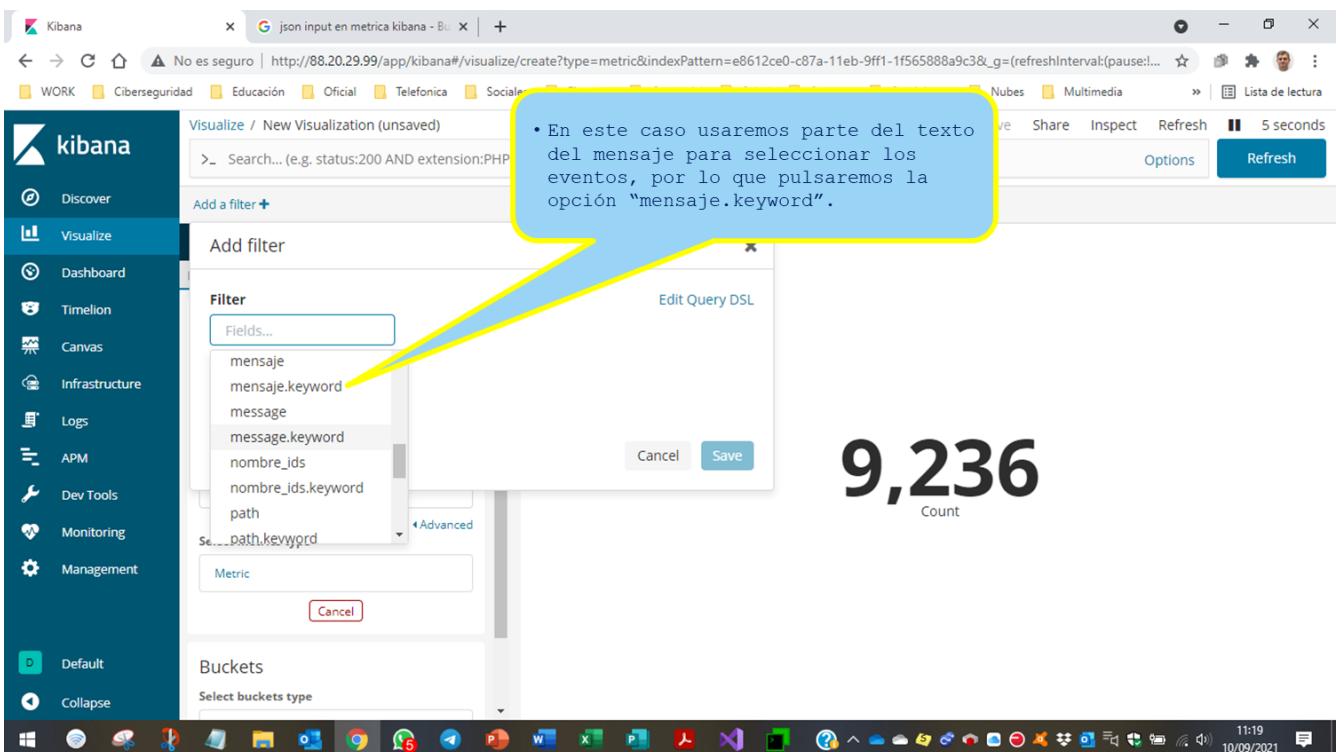
Cancel

Buckets

Select buckets type

9,062 Count

Francisco Artés - Elaboración Propia. Captura de Pantalla con la Creación de un Filtro (CC0)



Visualize / New Visualization (unsaved)

Search... (e.g. status:200 AND extension:PHP)

Add a filter +

Add filter

Filter Fields...

mensaje  
mensaje.keyword  
message  
message.keyword  
nombre\_ids  
nombre\_ids.keyword  
path  
path.keyword

Cancel Save

Edit Query DSL

Metric

Cancel

Buckets

Select buckets type

9,236 Count

Francisco Artés - Elaboración Propia. Captura de Pantalla con la Selección de Eventos (CC0)

A screenshot of the Kibana interface. On the left is the navigation sidebar with options like Discover, Visualize, Dashboard, etc. The main area shows a visualization titled 'Contador PINGS' with a count of 642. A yellow callout box points to a dropdown menu under 'Add filter'. The menu has a 'Label' field set to 'Optional' and a 'Select metrics type' dropdown set to 'Metric'. A tooltip in the callout box contains the following text:

- A continuación, pulsaremos el operador "is".
- Al pulsar en el campo de contenidos, nos mostrará los diversos contenidos recibidos hasta el momento en el campo "Mensaje".
- Seleccionaremos el contenido correspondiente en el momento de crear cada uno de los dos contadores para detectar eventos ICMP/ping y TCP/SSH.

Francisco Artés - Elaboración Propia. Captura de Pantalla con la Selección de Contenidos (CC0)

A screenshot of the Kibana interface. The top bar shows a URL starting with 'http://88.20.29.99/app/kibana#/visualize/create?'. The main area shows a visualization titled 'logstash' with a count of 4,422. A yellow callout box points to a button labeled 'Add a filter +'. A tooltip in the callout box contains the following text:

- Hecho esto, quedará guardado el filtro en cuestión dentro de la visualización.

Francisco Artés - Elaboración Propia. Captura de Pantalla con el Registro del Filtro dentro de la Visualización (CC0)

The screenshot shows the Kibana interface with a "Refresh Interval" dropdown menu open. The menu includes options like Off, 5 seconds, 10 seconds, 1 minute, 5 minutes, 15 minutes, 30 minutes, 1 hour, 2 hours, 12 hours, and 1 day. A yellow callout box points to the "5 seconds" option, which is highlighted.

• Para que empiece a funcionar el filtro, tendremos que pulsar la opción "Refresh", o bien, activar un intervalo de refresco automático, por ejemplo, de 5 segundos.

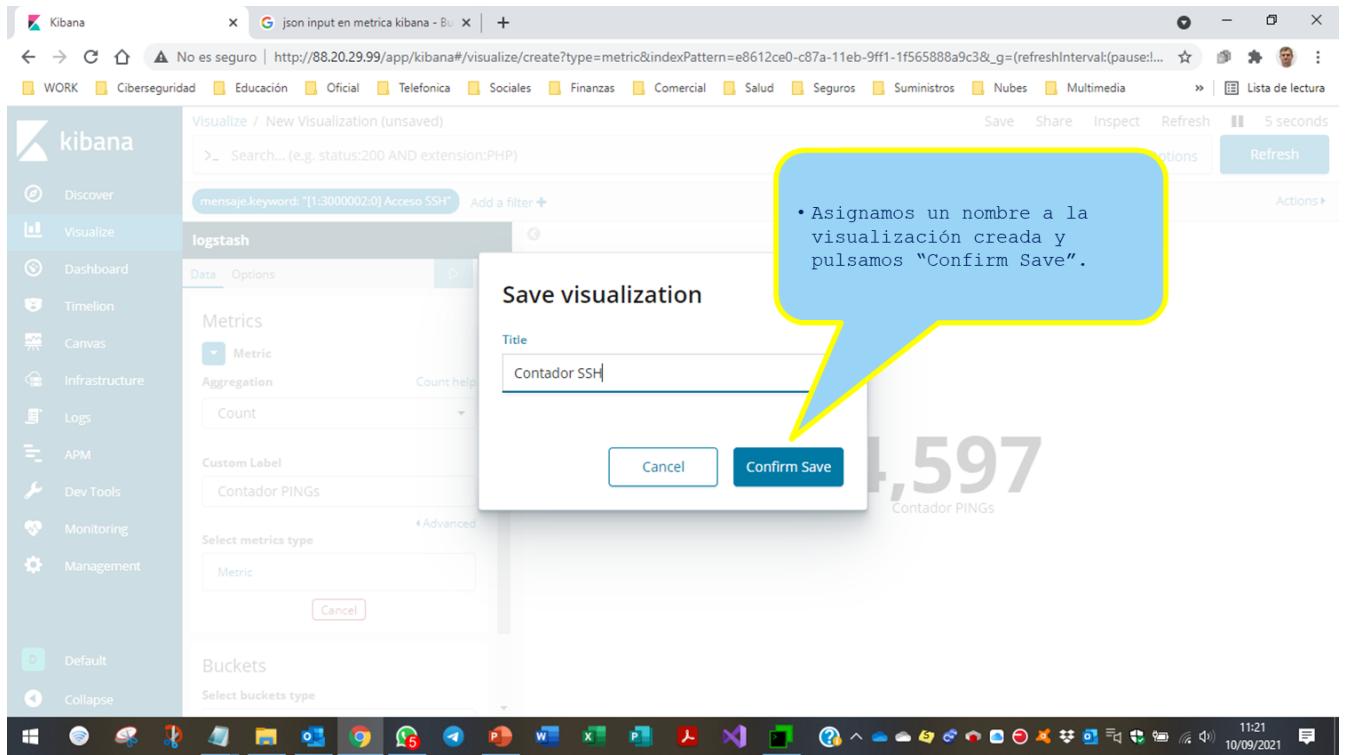
Francisco Artés - Elaboración Propia. Captura de Pantalla con la Activación del Refresco (CC0)

The screenshot shows the Kibana interface with the "Save" button highlighted in red. A yellow callout box points to the "Save" button, which is labeled "Save".

• Pulsamos el botón "Save" para guardar los cambios efectuados.

• ATENCIÓN: Si el botón "Save" aparece inhibido, pulsar la flechita de "play" y se activará.

Francisco Artés - Elaboración Propia. Captura de Pantalla con la Activación del Filtro y su Salvado (CC0)



• Asignamos un nombre a la visualización creada y pulsamos "Confirm Save".

Kibana

No es seguro | http://88.20.29.99/app/kibana#/visualize/create?type=metric&indexPattern=e8612ce0-c87a-11eb-9ff1-1f565888a9c3&\_g=(refreshInterval:(pause:...)

WORK Ciberseguridad Educación Oficial Telefónica Sociales Finanzas Comercial Salud Seguros Suministros Nubes Multimedia

Visualize / New Visualization (unsaved)

Discover

Visualize

Dashboard

Timelion

Canvas

Infrastructure

Logs

APM

Dev Tools

Monitoring

Management

logstash

mensaje.keyword: "[1:300002:0] Acceso SSH"

Search... (e.g. status:200 AND extension:PHP)

Add a filter +

Metrics

Metric

Count

Custom Label

Contador PINGs

Select metrics type

Metric

Buckets

Select buckets type

Save Share Inspect Refresh 5 seconds Actions

1,597 Contador PINGs

Francisco Artés - Elaboración Propia. Captura de Pantalla con el Etiquetado de la Visualización y su Salvado (CC0)

## 1.7.4.- Creación de un Histograma.

---

- ✓ Pulsar "Visualize"
- ✓ Pulsar "+" para añadir una visualización
- ✓ Seleccionar "Vertical Bar"
- ✓ Pulsar "logstash\*"
- ✓ Pulsar la flechita azul de "Y-Axis Count"
- ✓ Se abrirá un submenú, en el que seleccionaremos "Count" como "Aggregation" (generalmente vendrá seleccionado por defecto)
- ✓ Pondremos nombre al eje Y en el campo "Custom Label" (Número de PINGs / Número de SSHs)
- ✓ Pulsaremos "Add a Filter" y añadiremos el filtro de la forma habitual
- ✓ En el submenú "Buckets" pulsaremos X-Axis
- ✓ En "Aggregation" seleccionaremos la opción "Date Histogram", con Field="@timestamp" e intervalo automático.
- ✓ Tras lo anterior, pulsaremos la flechita azul de "play"
- ✓ Si el resultado es satisfactorio se pulsará "Save" en la barra de menú superior (se puede ver la gráfica interactiva si se ataca con ping o con ssh, en función del filtro elegido).

## 1.7.5.- Creación de un Tablero.

- ✓ Pulsar "Dashboard"
- ✓ Pulsar "Add" en la barra de menú superior para añadir visualizaciones al tablero
- ✓ Seleccionar secuencialmente todas las visualizaciones deseadas
- ✓ Cerrar el submenú
- ✓ Redimensionar y reposicionar las visualizaciones a gusto del usuario
- ✓ Pulsar "Save" y asignarle un nombre al tablero

The screenshot shows the Kibana interface with the 'Dashboards' page open. On the left is a sidebar with various navigation options like Discover, Visualize, Dashboard, etc. The main area shows a table titled 'Dashboards' with one entry: 'Tablero Principal'. A yellow arrow points from the 'Create new dashboard' button at the top right of the table area to a blue callout box containing the following text:

- A partir de este momento, las visualizaciones se podrán mostrar en pantalla de forma independiente, al seleccionarlas dentro de la opción "Visualize", no obstante, lo normal es crear un tablero de monitorización.
- Vamos a la opción "Dashboard", pusamos el botón "Create new dashboard" y creamos un tablero denominado "Tablero Principal".

At the bottom of the screen, there is a taskbar with various icons and system status information.

[Francisco Artés - Elaboración Propia](#). Captura de Pantalla con la Creación de un Tablero Kibana (CC0)

Tablero Principal - Kibana

A continuación, creamos dos nuevas visualizaciones gráficas con los mismos filtros anteriores y con formato de histograma, totalizando cada 5 minutos.

Pulsamos el nombre "Tablero Principal" y añadimos las cuatro visualizaciones, esto es, los dos contadores y los dos histogramas.

A partir de ese momento, el tablero quedará operativo y veremos los cambios en tiempo real.

Visualize

Dashboard

Timelion

Canvas

Infrastructure

Logs

APM

Dev Tools

Monitoring

Management

Default

Collapse

Contador PINGs

3,842

Contador PINGs

Grafico PING

Count

120

110

100

90

80

70

60

50

40

30

20

10

0

11:00 11:15 11:30 11:45 12:00 12:15

Cada 5 minutos

Contador SSH

15,175

Contador SSH

Grafico SSH

SSH Count

300

200

100

0

11:00 11:15 11:30 11:45 12:00 12:15

Cada 5 minutos

Francisco Artés - Elaboración Propia. Captura de Pantalla con la Visualización de un Tablero Kibana (CC0)

## **2.- Bibliografía.**

---

[Bibliografía](#) (pdf - 60141 B)