Pasos Previos

# Pasos previos :paw\_prints:

**Security Onion** permite realizar diveros tipos de instalaciones y en función de la instalación a realizar el nivel de los requisitos puede oscilar bastante.

## Tipos de instalaciones posibles :pushpin:

Tipo de instalación de SO

Funcionalidad

Import

Se usa para importar o analizar, sin necesidad de sensores, PCAPs y Logs.

Eval

Instalación rápida para realizar pruebas.

Standalone

Similar a Eval, pero para entornos de producción pequeños.

Manager

Nodo central para la administración de la infraestructura y el almacenamiento de datos. No realiza captura tráfico.

Manager Search

Manager con capacidad de búsqueda de datos.

Search Node

Nodo adicional para mejorar la búsqueda y el almacenamiento de los datos en despliegues grandes.

Sensor

Captura el tráfico de red y lo almacena en logs para enviarlos al Manager y poder analizarlos.

Heavy Node

Similar a un Sensor, aunque con más capacidad de procesamiento para realizar análisis locales.

IDH Node

Para analizar logs y tráfico de red en entornos aislados o de alta seguridad.

Fleet Node

Sensor especializado en la gestión de múltiples sensores distribuidos.

Receiver Node

Recibe datos y logs de otros sensores. Útil en arquitecturas distribuidas.

### Import

Una distribución del tipo **Importación** ejecuta la cantidad mínima de procesos para poder importar ficheros **PCAP** o **EVTX** para analizar.

### Eval

La distribución de tipo **Evaluación** ejecuta los procesos mínimos de una máquina, por ello sus requisitos son menores a los de una instalación **Standalone** y se ajusta a instalaciones temporales o de bajo presupuesto. No está diseñada para producción, por ello está bien para uso en fase de **desarrollo** e **investigación**.

**Eval** usa **Suricata** y no ejecuta Logstash o Redis para **economizar** el uso de **memoría RAM**.

## Requisitos en función del tipo de instalación :computer:

Node Type

CPUs

RAM

Storage

NICs

Import

2

4GB

50GB

1

Eval

4

8GB

200GB

2

Standalone

4

16GB

200GB

2

Manager

4

16GB

200GB

1

ManagerSearch

8

16GB

200GB

1

Search node

4

16GB

200GB

1

Sensor

4

12GB

200GB

2

Heavy node

4

16GB

200GB

2

IDH node

2

1GB

12GB

1

Fleet node

4

4GB

200GB

1

Receiver node

2

8GB

200GB

1