Workshop de Monitoreo

Ricardo Monreal Llop
rmonreal@finsin.cl

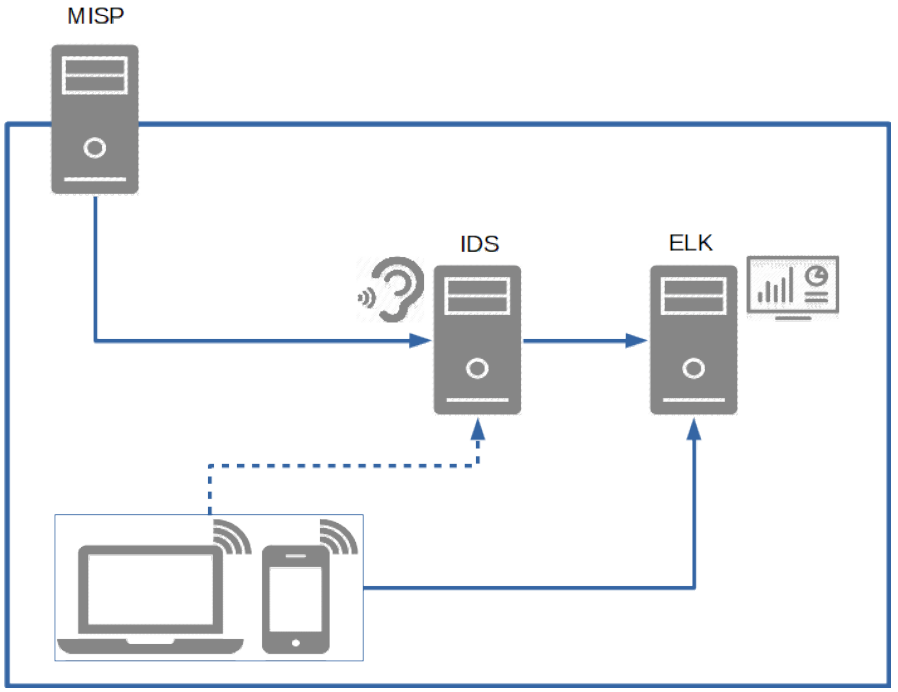
Temario

- Armar ambiente
  - VMWare
  - Virtual Box
- IDS
  - Maltrail
  - Suricata
- ELK
  - Elastic
  - Logstash
  - Kibana
  - Beats
- MISP

Ambiente

- 1 máquina de usuario
- 1 máquina de IDSs
- 1 máquina de almacenamiento y dashboards
- 1 máquina de feed nuevos

Diagrama general



Paso 0: OS

https://www.ubuntu.com/download/server

- En este caso
  - Ubuntu 18.04.2 LTS
- Preparar interfaz (ens33?)
  - Modo promiscuo

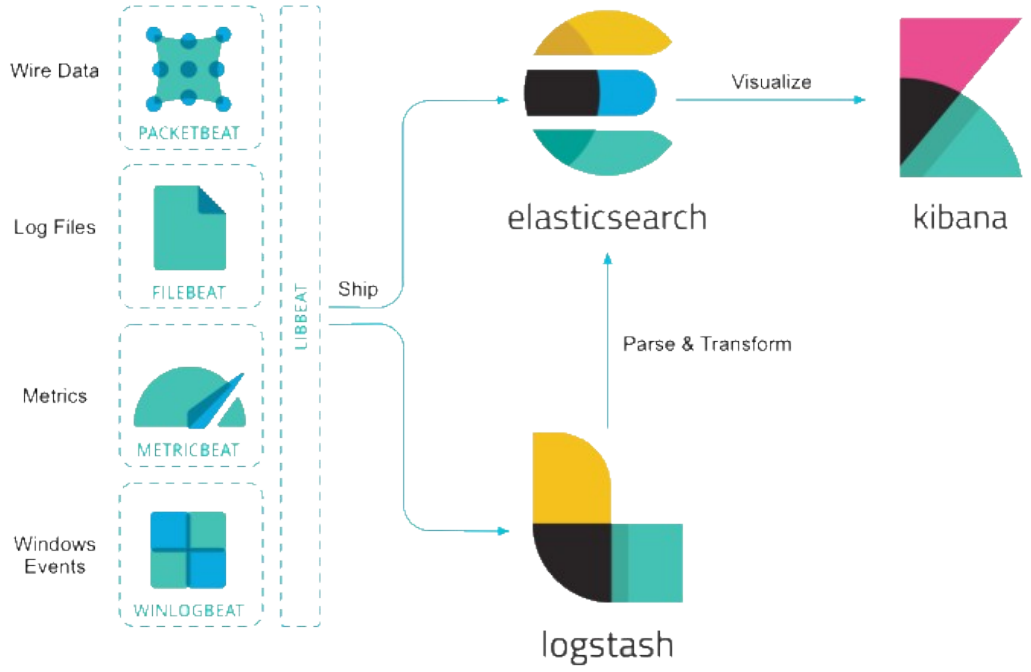
Paso 1: Maltrail

https://github.com/stamparm/maltrail

- IDS enfocado en malware
- Muchas trazas por defecto
- Tiene interfaz Web

Comenzar con primer archivo .txt

Paso 2: Diagrama ELK



Paso 2: ELK

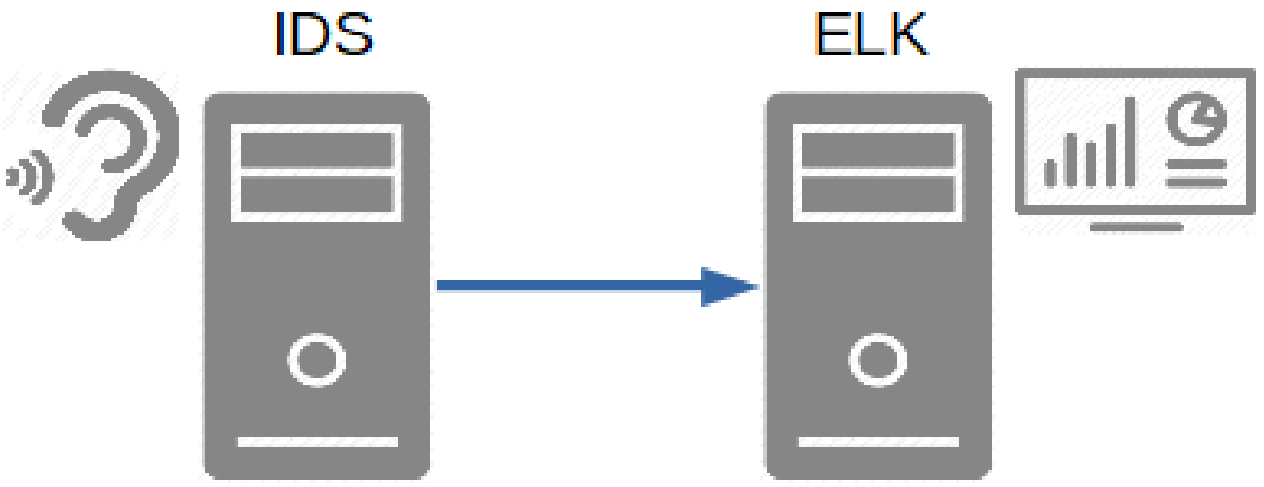
https://www.elastic.co/es/downloads/

- Almacenamiento y procesamiento de logs
- Aplicaciones especialistas
  - Elasticsearch: Almacenamiento y búsqueda
  - Logstash: Preprocesamiento
  - Kibana: Visualización

Comenzar con segundo archivo .txt

Paso 3 Integración

- Juntamos las 2 primeras partes



Comenzar con el tercer archivo .txt

Paso 4: Suricata

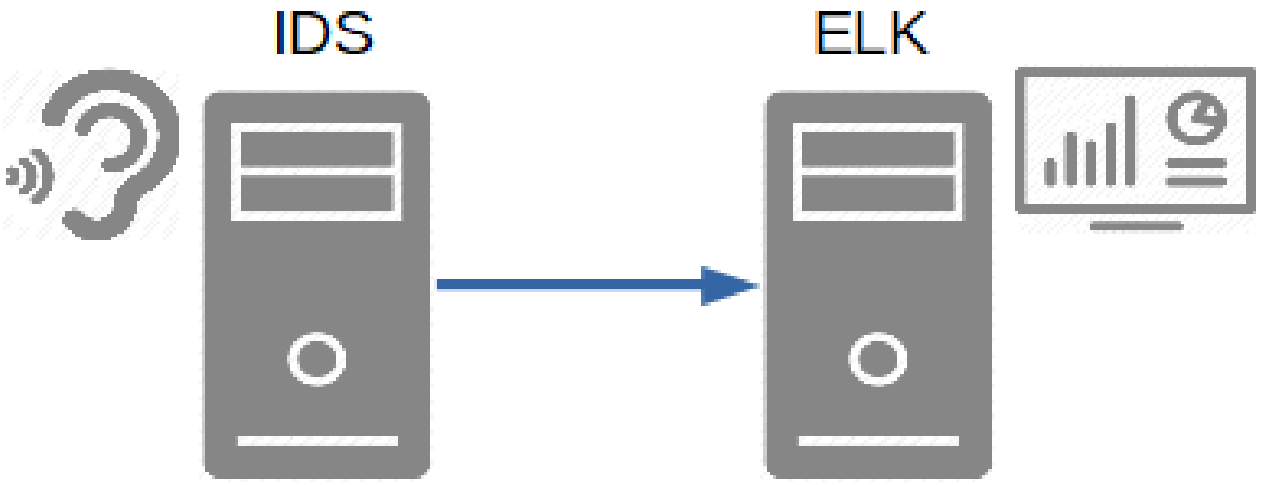
https://suricata-ids.org/download/

- IDS con mucha información
- Usa feeds variados

Comenzar con el cuarto archivo .txt

Paso 5: Integración

- Juntamos Suricata con ELK



Comenzar con el quinto archivo .txt

Paso 6: Winlogbeat (opcional)

https://www.elastic.co/es/downloads/beats/winlogbeat

- Extracción de eventos de Windows
- Logra visibilidad centralizada

Comenzar con el sexto archivo

Paso 7: Fuentes “Custom”

- Integrar fuentes de otros lados
- Usaremos MISP de FINSIN
  - https://misp.finsin.cl
- “2 líneas” y reinicio

Comenzar con parte final del séptimo archivo .txt

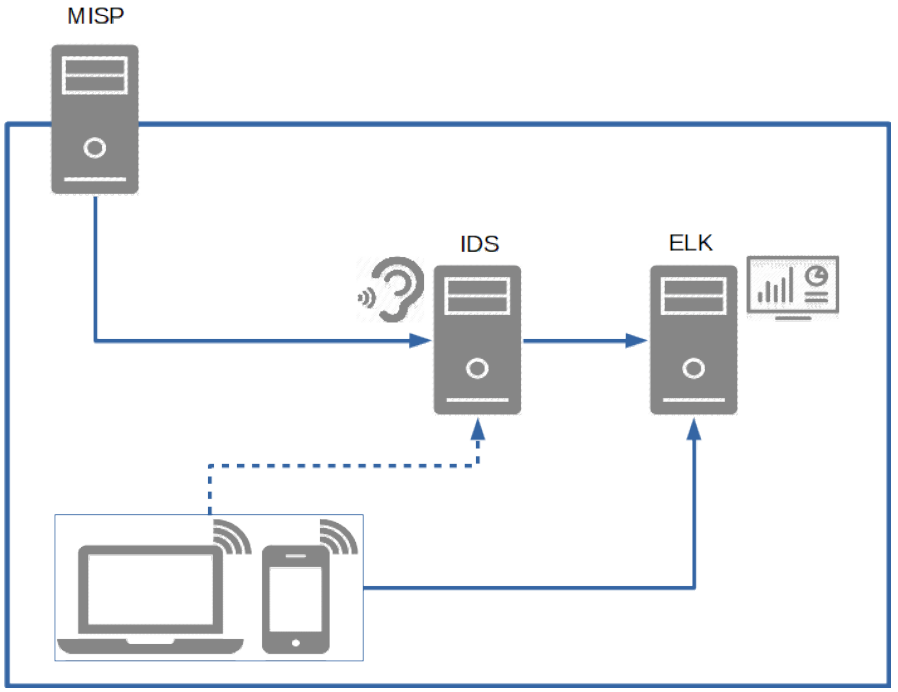
Paso 7: MISP

https://www.misp-project.org/

- Repositorio de IOC
- Almacenamiento de Investigaciones

Comenzar con el inicio del séptimo archivo

Ya tenemos algo más formado



Mucho más que hacer

- ELK puede recibir más datos
  - AV?
  - EDR?
  - Email Server?

Cualquier cosa me contactan

Ricardo Monreal Llop

rmonreal@finsin.cl