Universidad del Caribe
2000 CANCUN, QUINTANA ROO, MÉXICO
CONOCIMIENTO Y CULTURA PARA EL DESARROLLO HUMANO

Asignatura:

Teoría de la información

Tema:
Representación de la información de los datos

Trabajo para realizar:
investigar como la computadora representa cada formato (texto,ascii,imagen,video,audios)

Alumno:

Pérez Barahona Pedro Luis

Programa educativo:

Ingeniería en datos e inteligencia organizacional

Presentado a:

Jiménez Sánchez Ismael

Fecha:

21/02/2026

Serie de laboratorio en casa: SOC de código abierto n.° 1: Implementación de Wazuh, The Hive, Cortex y MISP (renovado)

Alguna vez soñaste con tener un Centro de Operaciones de Seguridad completo sin el precio empresarial? ¡Estás de suerte! Hoy te guiaré en la implementación de un SOC de código abierto totalmente integrado usando Docker, combinando el poder de Wazuh, The Hive, Cortex y MISP en una única pila de seguridad fácil de implementar

¿Qué hace diferente a esta guía? Lo hacemos todo con un solo archivo docker-compose :)

¿Por qué construir un SOC en su laboratorio en casa?

Seamos honestos: además del innegable factor genial de tener paneles parpadeantes que muestran eventos de seguridad en tiempo real, hay razones legítimas para construir su propio SOC:

- **Aprendizaje** : No hay mejor manera de entender las operaciones de seguridad que haciéndolo.
- **Entorno de laboratorio** : pruebe reglas de detección, automatización y respuesta a incidentes sin consecuencias.
- **Habilidades laborales** : Experiencia práctica que realmente importa a los empleadores.
- **Derechos de alarde** : "¿Ah, esa alerta en mi teléfono? Es solo que mi SOC local detectó un escaneo de puertos. No es para tanto".

Lo que estamos construyendo

Nuestra arquitectura SOC incluye una máquina virtual Ubuntu 22.04, en la que instalamos lo siguiente:

- **Wazuh (implementación de nodo único)** : para monitoreo de seguridad, detección de amenazas y análisis de registros
- **The Hive** : Para respuesta a incidentes y gestión de casos
- **Cortex** : para el análisis automatizado de observables e IOC
- **MISP** : Para la gestión y el intercambio de inteligencia sobre amenazas

Esta combinación le brinda capacidades de seguridad de nivel profesional que normalmente costarían miles en productos comerciales.

Especificaciones de hardware

Para esta implementación, utilicé una máquina virtual bastante modesta con las siguientes especificaciones:

Memory	7.91 GiB [balloon=0]
Processors	4 (2 sockets, 2 cores) [x86-64-v2-AES]
BIOS	Default (SeaBIOS)
Display	Default
Machine	Default (i440fx)
SCSI Controller	VirtIO SCSI single
CD/DVD Drive (ide2)	none,media=cdrom
Hard Disk (scsi0)	BigHdd-thin:vm-103-disk-0,iothread=1,size=80G
Network Device (net0)	virtio=BC:24:11:02:62:CE,bridge=vmbr0,firewall=1

Estas especificaciones proporcionan recursos suficientes para un entorno básico de pruebas o aprendizaje. Los componentes deberían funcionar con esta configuración, aunque con algunas limitaciones de rendimiento. Para un sistema más ágil, especialmente si planea

ingerir y analizar grandes volúmenes de datos, debería considerar optimizar los recursos de la máquina virtual.

2. Configuración Inicial del Entorno

Antes de levantar los contenedores, debes preparar el sistema Ubuntu en tu terminal:

1. **Ajustar la memoria virtual:** Elasticsearch (usado por The Hive y Wazuh) requiere un conteo alto de mapas de memoria.

```
luis@LUISBARAHONAPORTATIL:~$ sudo sysctl -w vm.max_map_count=262144

``` [cite: 357]
[sudo] password for luis:
vm.max_map_count = 262144
> sudo apt update
sudo apt install docker.io docker-compose -y
>
> mkdir -p cortex thehive && touch cortex/application.conf thehive/
application.conf
``` [cite: 359]
[cite:: command not found

WARNING: apt does not have a stable CLI interface. Use with caution
 in scripts.

mkdir -p cortex thehive && touch cortex/application.conf thehive/ap
plication.conf
``` [cite: 359]
```

Esta arquitectura te permitirá ver cómo la información se transforma de un evento crudo a inteligencia procesable:

| Componente | Función en el SOC | Relación con Teoría de la Información |
|---|---|---|
| **Wazuh** | Monitoreo, detección y análisis de registros. | Reducción de incertidumbre mediante el filtrado de logs. |
| **The Hive** | Gestión de casos y respuesta a incidentes. | Organización y codificación de eventos de seguridad. |
| **Cortex** | Análisis automatizado de observables (IPs, hashes). | Enriquecimiento de datos para generar contexto. |
| **MISP** | Intercambio de inteligencia sobre amenazas. | Distribución de información compartida entre comunidades. |

**El proceso de implementación**
**Ejecute el siguiente comando para clonar el repositorio de Wazuh:**
```

El proceso de implementación

Ejecute el siguiente comando para clonar el repositorio de Wazuh:

```
git clone https://github.com/wazuh/wazuh-docker.git -b v4.11.0

#Wazuh requiere certificados SSL para comunicaciones seguras entre sus component
```

Ingrese a la carpeta de nodo único y ejecute el generador de certificados:

```
cd wazuh-docker/single-node

docker-compose -f generate-indexer-certs.yml run --rm generator
```

Esto guarda los certificados en el `config/wazuh_indexer_ssl_certs` directorio.

Ahora es el momento de juntar nuestro archivo Docker Compose, deshacernos del contenido del archivo original y reemplazarlo con:

docker-compose.yml

Ahora es el momento de juntar nuestro archivo Docker Compose, deshacernos del contenido del archivo original y reemplazarlo con:

docker-compose.yml

2. Configuración Inicial del Entorno

```
luis@LUISBARAHONAPORTATIL:~$ mkdir laboratoriosoc
cd laboratoriosoc
luis@LUISBARAHONAPORTATIL:~/laboratoriosoc$ nano docker-compose.yml
luis@LUISBARAHONAPORTATIL:~/laboratoriosoc$ version: '3.8'
```

```
luis@LUISBARAHONAPORTATIL:~/laboratoriosoc$ nano docker-compose.yml
luis@LUISBARAHONAPORTATIL:~/laboratoriosoc$ docker-compose up -d [c
ite: 450]
ERROR: yaml.parser.ParserError: while parsing a block mapping
  in "./docker-compose.yml", line 6, column 5
expected <block end>, but found '<scalar>'
  in "./docker-compose.yml", line 7, column 17
luis@LUISBARAHONAPORTATIL:~/laboratoriosoc$ cd ~/laboratoriosoc
mkdir -p cortex/logs thehive/data misp/mysql wazuh/config
luis@LUISBARAHONAPORTATIL:~/laboratoriosoc$ git clone https://githu
```

4. Ajustar el sistema (Requisito crítico)

Antes de lanzar el comando, debes ejecutar esto en tu terminal de Ubuntu para que Elasticsearch no se detenga por falta de recursos:

Bash

```
sudo sysctl -w vm.max_map_count=262144
```

5. Lanzar el SOC

Ahora sí, ejecuta el comando final:

Bash

```
docker-compose up -d
```

Verificación

Puedes ver qué contenedores están corriendo con:

Bash

```
docker ps
```

```
generate-indexer-certs.yml'
luis@LUISBARAHONAPORTATIL:~/laboratoriosoc$ cd wazuh-docker/single-
node
luis@LUISBARAHONAPORTATIL:~/laboratoriosoc/wazuh-docker/single-node
$ nano docker-compose.yml
luis@LUISBARAHONAPORTATIL:~/laboratoriosoc/wazuh-docker/single-node
$ sudo sysctl -w vm.max_map_count=262144
[sudo] password for luis:
Sorry, try again.
[sudo] password for luis:
vm.max_map_count = 262144
luis@LUISBARAHONAPORTATIL:~/laboratoriosoc/wazuh-docker/single-node
$ docker-compose up -d
ERROR: yaml.parser.ParserError: while parsing a block mapping
  in "./docker-compose.yml", line 5, column 5
expected <block end>, but found '<scalar>'
  in "./docker-compose.yml", line 5, column 17
luis@LUISBARAHONAPORTATIL:~/laboratoriosoc/wazuh-docker/single-node
$ docker ps
CONTAINER ID   IMAGE     COMMAND   CREATED   STATUS    PORTS     NA
MES
```

Pega lo siguiente, asegurándote de que los nombres de los hosts coincidan con los de tu archivo

```
luis@LUISBARAHONAPORTATIL:~/laboratoriosoc/wazuh-docker/single-node
$ # Clave secreta para la sesión
play.http.secret.key="5jU6hleuT1jMJt3uCe3fb02iGcoXOkF97XESPxkALivHb
lLd3vw8Vh4rJY"

# Configuración de red
http.address=0.0.0.0
http.port=9001

# Conexión con Elasticsearch
search {
  index = cortex
  uri = "http://elasticsearch:9200/"
}

# Configuración del ejecutor de Docker para analizadores
job {
  runner = [docker]
}

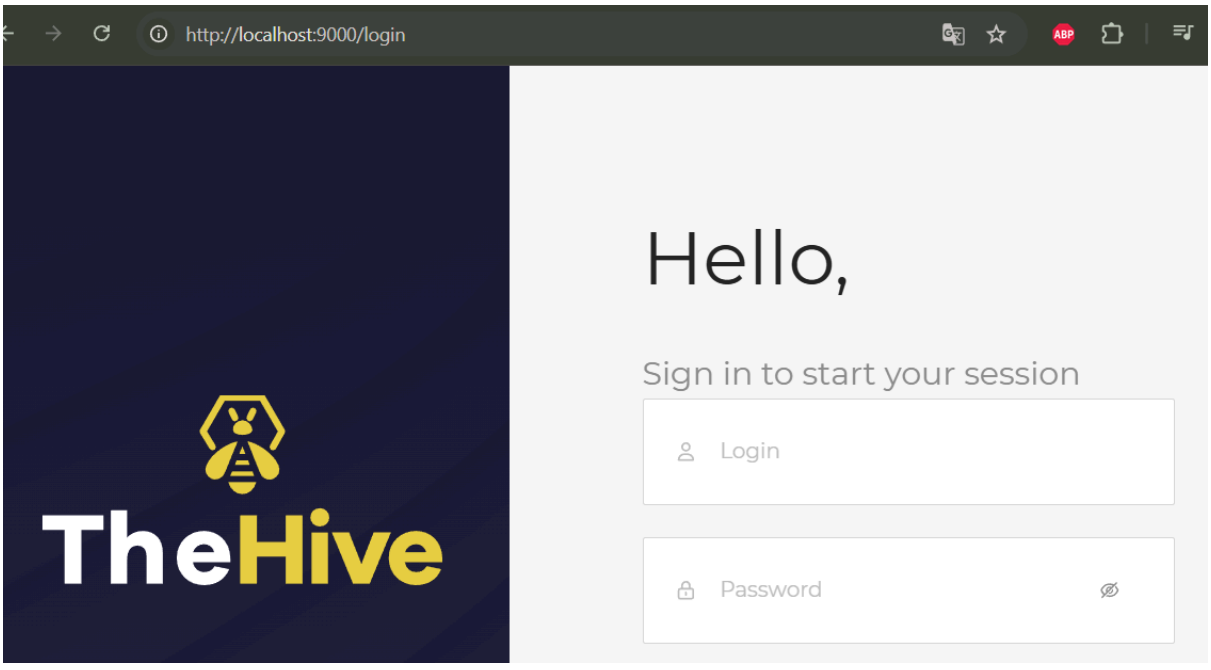
docker {
  directory = /tmp/cortex-jobs
}
play.http.secret.key=5jU6hleuT1jMJt3uCe3fb02iGcoXOkF97XESPxkALivHbl
Ld3vw8Vh4rJY: command not found
http.address=0.0.0.0: command not found
http.port=9001: command not found
Command 'search' not found, did you mean:
  command 'fsearch' from snap fsearch (0.1.4)
  command 'esearch' from deb ncbi-entrez-direct (19.2.20230331+dfsg
-3ubuntu0.24.04.3)
  command 'vsearch' from deb vsearch (2.26.1-1)
  command 'starch' from deb coop-computing-tools (9.9-4ubuntu1)
  command 'csearch' from deb codesearch (0.0~hg20120502-3ubuntu0.24
```

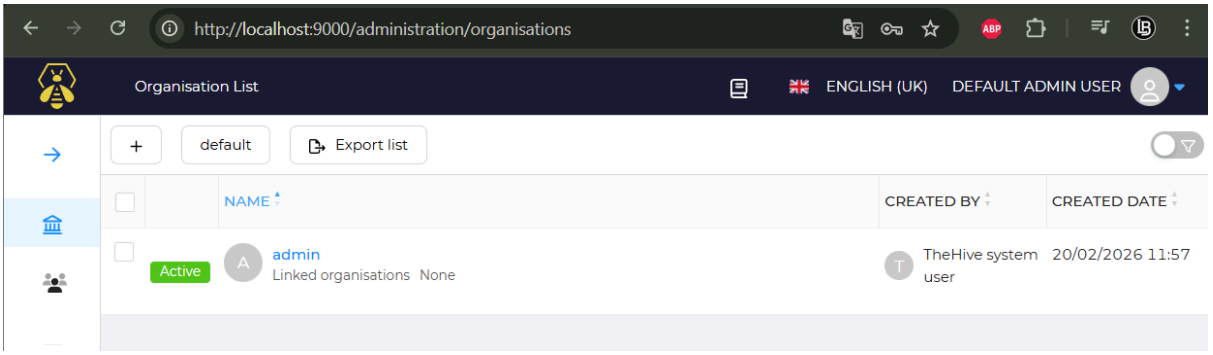
```
luis@LUISBARAHONAPORTATIL:~/laboratoriosoc$ nano docker-compose.yml
luis@LUISBARAHONAPORTATIL:~/laboratoriosoc$ cd ~/laboratoriosoc
luis@LUISBARAHONAPORTATIL:~/laboratoriosoc$ nano docker-compose.yml
luis@LUISBARAHONAPORTATIL:~/laboratoriosoc$ sudo sysctl -w vm.max_m
ap_count=262144
vm.max_map_count = 262144
luis@LUISBARAHONAPORTATIL:~/laboratoriosoc$ docker-compose up -d
Creating network "laboratoriosoc_SOC_NET" with driver "bridge"
Pulling elasticsearch (docker.elastic.co/elasticsearch/elasticsearc
h:7.17.9)...
7.17.9: Pulling from elasticsearch/elasticsearch
36a9c60c46d0: Pull complete
e702cbf68995: Pull complete
d42ba0f6aa39: Pull complete
13c59ecc70cc: Pull complete
12d112623fed: Pull complete
3e95eee02a15: Pull complete
e8819c48f163: Pull complete
ea0623c40fc9: Pull complete
a621ebe36959: Pull complete
Digest: sha256:59b37f77bd8b015d5b60f75bebb22d06028f7f15036f9d3559d2
b7c16ece74db
Status: Downloaded newer image for docker.elastic.co/elasticsearch/
elasticsearch:7.17.9
Pulling cassandra (cassandra:4)...
4: Pulling from library/cassandra
4831516dd0cb: Pull complete
cda8bafb86fb: Pull complete
a1f50de5de73: Extracting [==================>
          ]  6.881MB/18.15MBete
7a2a6d412ca6: Download complete
====>      ]  41.72MB/47.29MBte
92b375c80b7d: Download complete
==========> ]  52.59MB/52.91MBte
==========>]  1.224kB/1.224kB
```

3. Ejecución del Entorno, levantar los servicios y la verificación

```
Digest: sha256:5ff4b9edd5d6a5bc38c1ef25a38b829527a2944b750b595e7647
965097e91bdb
Status: Downloaded newer image for strangebee/thehive:5.2
Creating cassandra     ... done
Creating elasticsearch ... done
Creating thehive       ... done
luis@LUISBARAHONAPORTATIL:~/laboratoriosoc$ docker ps
CONTAINER ID   IMAGE
   COMMAND                  CREATED              STATUS
  PORTS                                                 NAMES
82eeac9eae31   strangebee/thehive:5.2
   "/opt/thehive/entryp…"   About a minute ago   Up About a minute
  0.0.0.0:9000->9000/tcp, [::]:9000->9000/tcp           thehive
413fa020dda7   docker.elastic.co/elasticsearch/elasticsearch:7.17.9
   "/bin/tini -- /usr/l…"   About a minute ago   Up About a minute
  0.0.0.0:9200->9200/tcp, [::]:9200->9200/tcp, 9300/tcp   elasticse
arch
2a73958fb52d   cassandra:4
   "docker-entrypoint.s…"   About a minute ago   Up About a minute
  7000-7001/tcp, 7199/tcp, 9042/tcp, 9160/tcp           cassandra
luis@LUISBARAHONAPORTATIL:~/laboratoriosoc$
```

Los contenedores de TheHive, Elasticsearch y Cassandra ya están corriendo (Up) y con sus puertos correctamente mapeados.





Abre el navegador en Windows 11.

Ingresa a: http://localhost:9000.

Usa las credenciales por defecto: Usuario: admin@thehive.local |

Contraseña:secret

Despues de hacer la prueba implementar el codigo de la pagina del ejercicio para ejecutar un nuevo contenedor:

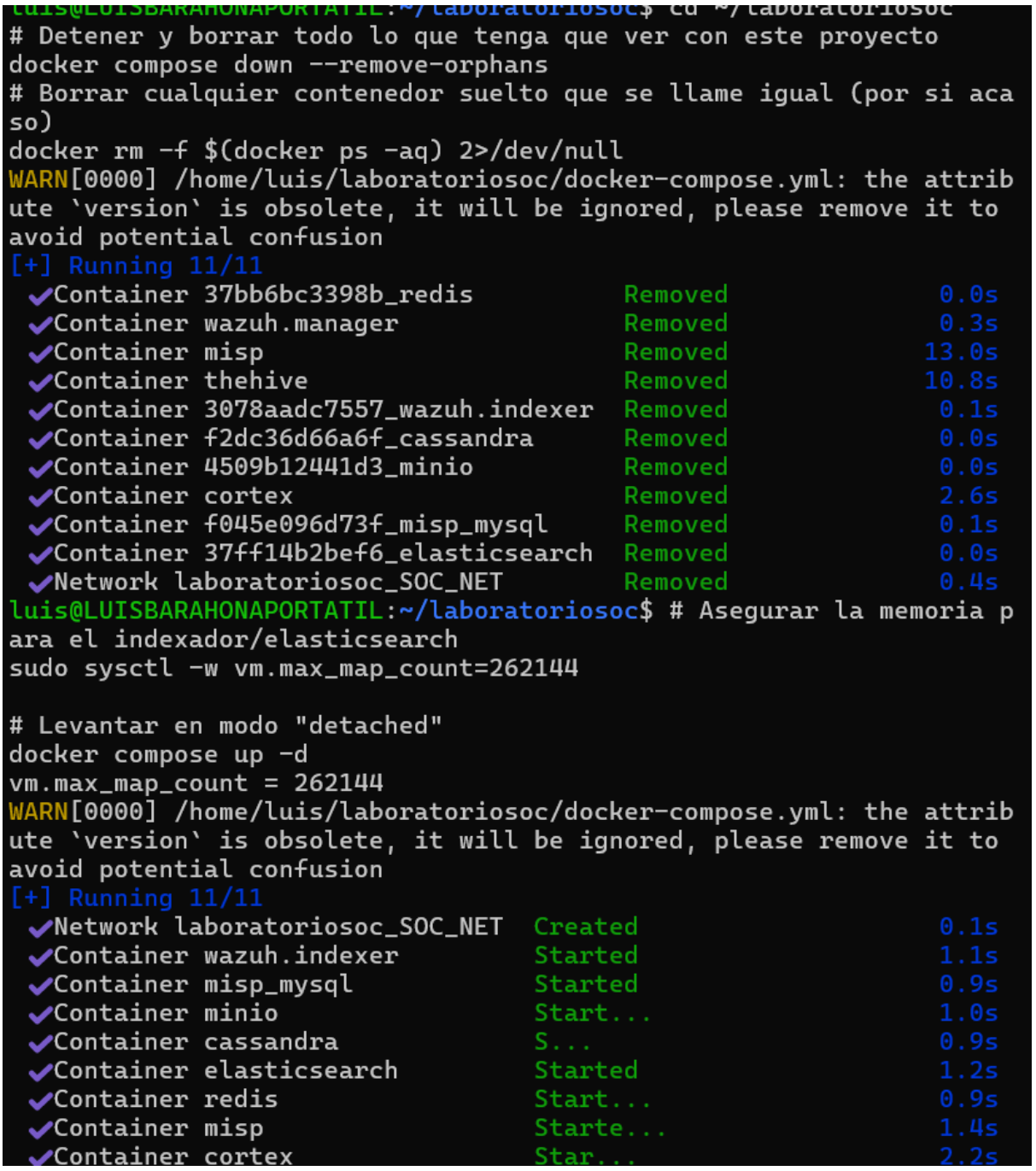
```
luis@LUISBARAHONAPORTATIL:~/laboratoriosoc$ docker-compose up -d
Creating volume "laboratoriosoc_miniodata" with default driver
Creating volume "laboratoriosoc_cassandradata" with default driver
Creating volume "laboratoriosoc_elasticsearchdata" with default dri
ver
Creating volume "laboratoriosoc_thehivedata" with default driver
Creating volume "laboratoriosoc_mispsqldata" with default driver
Creating volume "laboratoriosoc_wazuh-indexer-data" with default dr
iver
Creating volume "laboratoriosoc_wazuh_etc" with default driver
Creating volume "laboratoriosoc_wazuh_logs" with default driver
Pulling minio (quay.io/minio/minio:)...
latest: Pulling from minio/minio
b83ce1c86227: Pull complete
f94d28849fa3: Pull complete
81260b173076: Pull complete
f9c0805c25ee: Pull complete
1008deaf6ec4: Pull complete
71e9fc939447: Pull complete
c1bc68842c41: Pull complete
0288b5a0d7e7: Pull complete
34013573f278: Pull complete
Digest: sha256:14cea493d9a34af32f524e538b8346cf79f3321eff8e708c1e29
60462bd8936e
Status: Downloaded newer image for quay.io/minio/minio:latest
Pulling cortex (thehiveproject/cortex:latest)...
latest: Pulling from thehiveproject/cortex
0e4bc2bd6656: Extracting [=======>
6a0dd5dfd0ee: Downloading [======>
```

hubo error, por eso no se realizo el proceso, por la version antigua de docker que tengo en mi equipo de computo. Vamos a instalar la versión moderna (V2) que resuelve el error .

```
luis@LUISBARAHONAPORTATIL:~/laboratoriosoc$ # Elimina la versión vi
eja
sudo apt remove docker-compose -y
# Instala el plugin moderno
sudo apt update
sudo apt install docker-compose-plugin -y
[sudo] password for luis:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no long
er required:
  libdrm-nouveau2 libdrm-radeon1 libgl1-amber-dri libglapi-mesa
  libllvm17t64 libxcb-dri2-0 python3-compose python3-docker
  python3-dockerpty python3-docopt python3-dotenv
  python3-texttable python3-websocket
Use 'sudo apt autoremove' to remove them.
The following packages will be REMOVED:
  docker-compose
0 upgraded, 0 newly installed, 1 to remove and 154 not upgraded.
After this operation, 61.4 kB disk space will be freed.
(Reading database ... 59021 files and directories currently install
```

Problemas de conflictos de archivos corruptos viejos, pero ya listo el contenedor activo.

```
luis@LUISBARAHONAPORTATIL:~/laboratoriosoc/config/wazuh_indexer_ssl
_certs$ cd ~/laboratoriosoc
sudo sysctl -w vm.max_map_count=262144
docker compose up -d
vm.max_map_count = 262144
WARN[0000] /home/luis/laboratoriosoc/docker-compose.yml: the attrib
ute `version` is obsolete, it will be ignored, please remove it to
avoid potential confusion
[+] Running 1/6
 ⠿ Container f045e096d73f_misp_mysql     Recreate            0.0s
 ⠿ Container f2dc36d66a6f_cassandra      Recreate            0.0s
 ⠿ Container 3078aadc7557_wazuh.indexer  Recreate            0.0s
 ⠿ Container 37ff14b2bef6_elasticsearch  Recreate            0.0s
```



Estado Actual de tu SOC

Tu laboratorio está operando con la siguiente arquitectura de red:

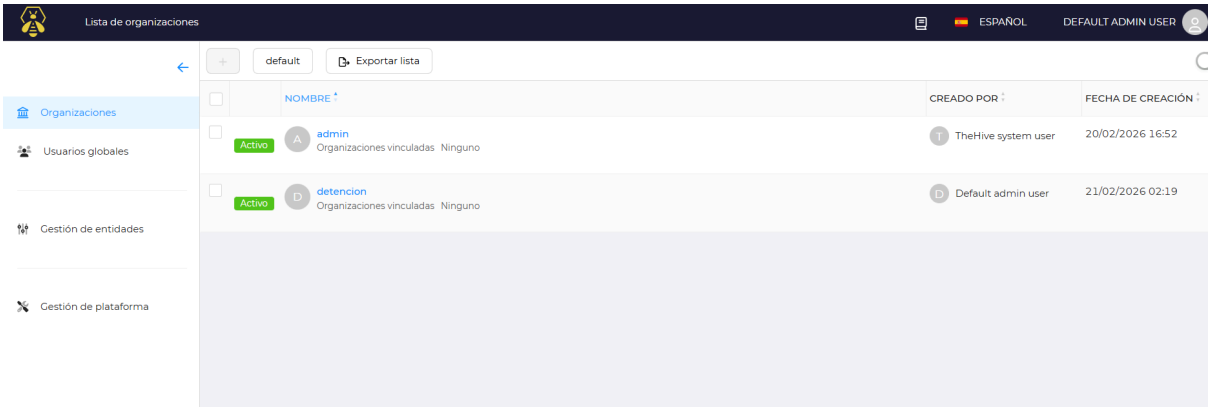
Servicio	URL de Acceso (desde Windows 11)	Usuario	Contraseña
TheHive	http://localhost:9000	admin@thehive.local	secreto
Cortex	http://localhost:9001	admin	admin
Wazuh Indexer	https://localhost:9201	admin	SecretPassword +1
Wazuh Dashboard	https://localhost:8443	admin	SecretPassword +1
MISP	https://localhost	admin@admin.test	admin

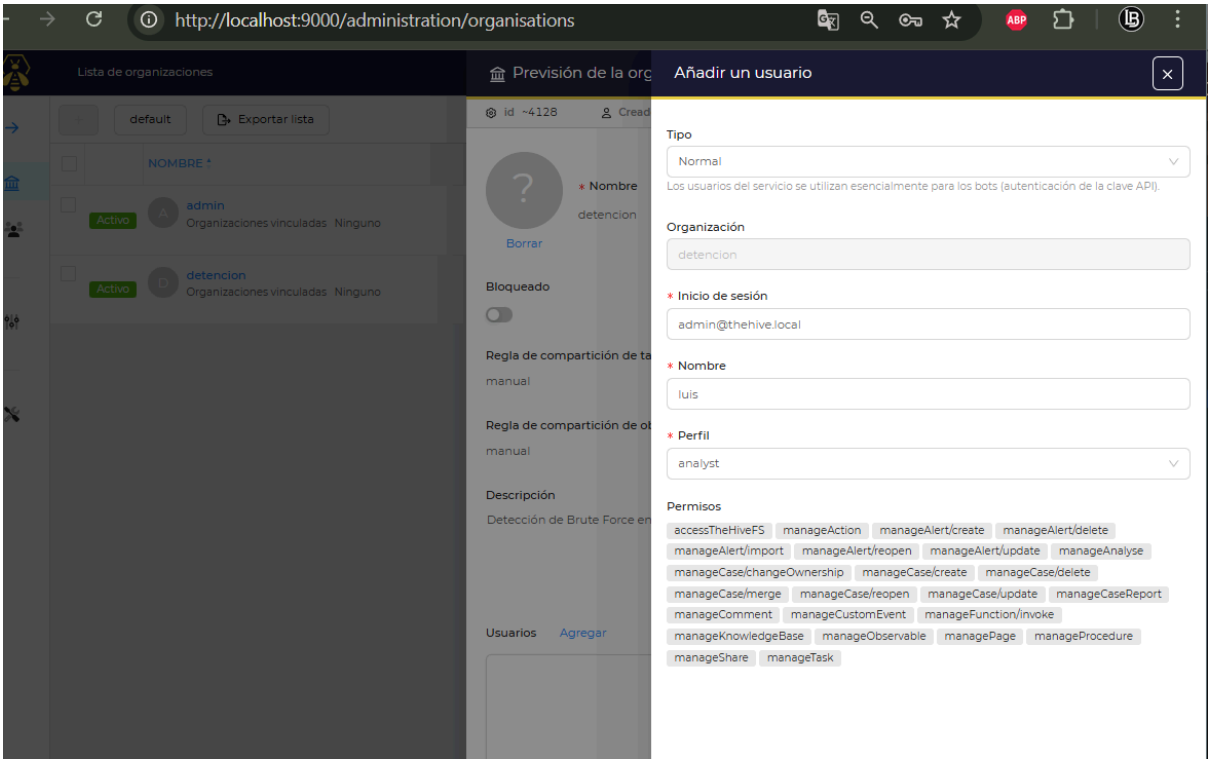
Notas Importantes para tu actividad

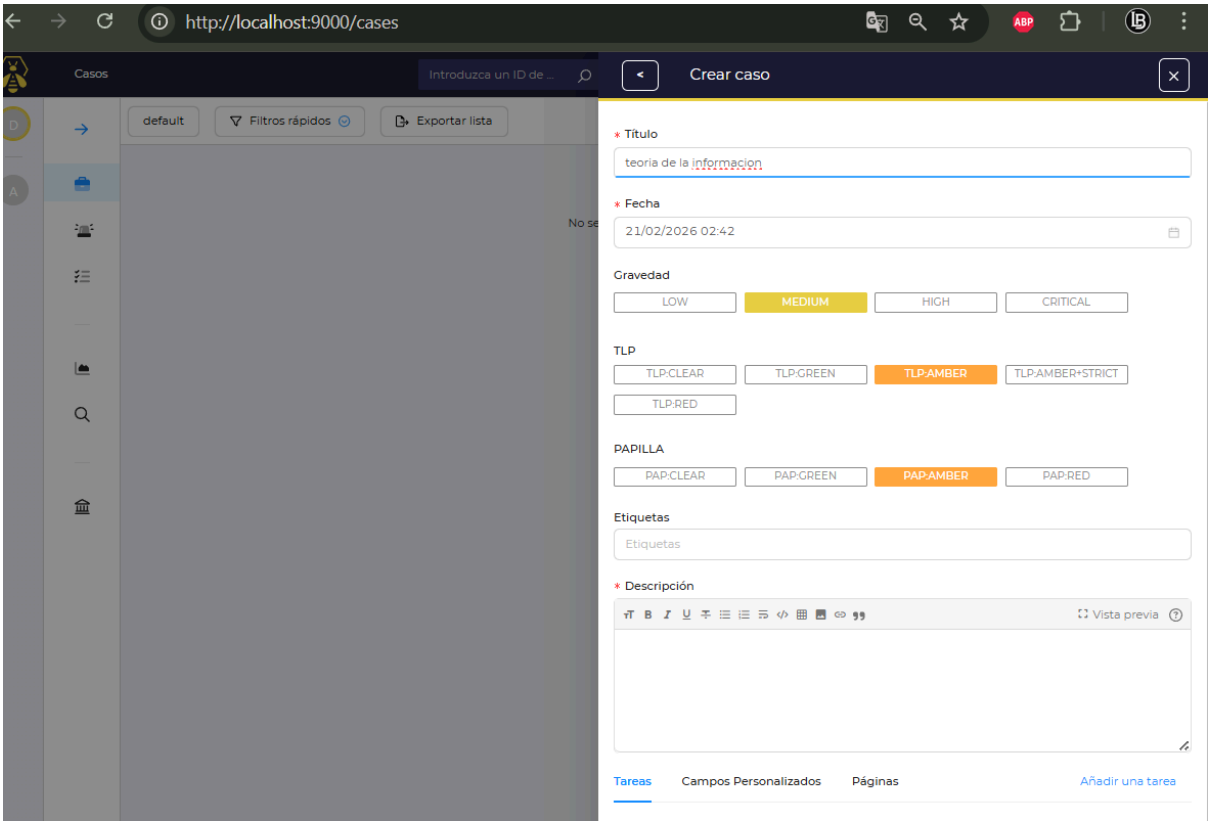
1. **Inicialización de MISP: Este servicio es el más pesado y puede tardar varios minutos en estar totalmente funcional, aunque aparezca como "Up".**
2. **Advertencia de Seguridad: Como indica tu guía, estas son credenciales predeterminadas no aptas para producción. Son perfectas para tu laboratorio académico, pero recuerda que en un entorno real la entropía de las contraseñas debe ser mucho mayor.**

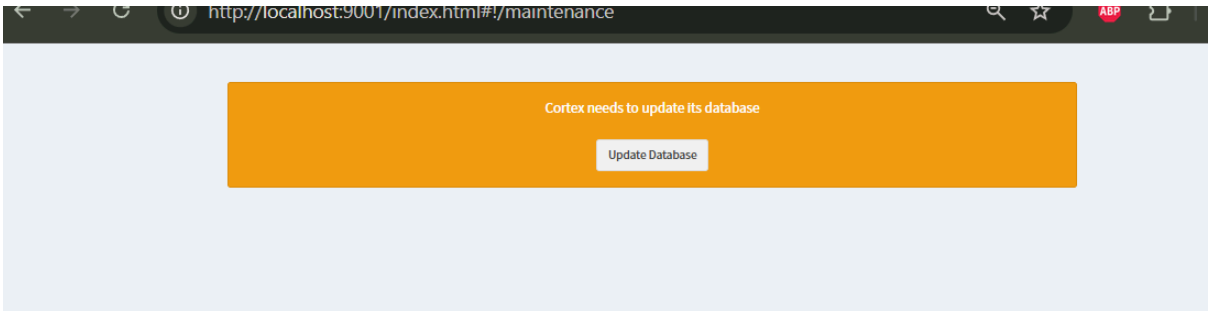
   +2

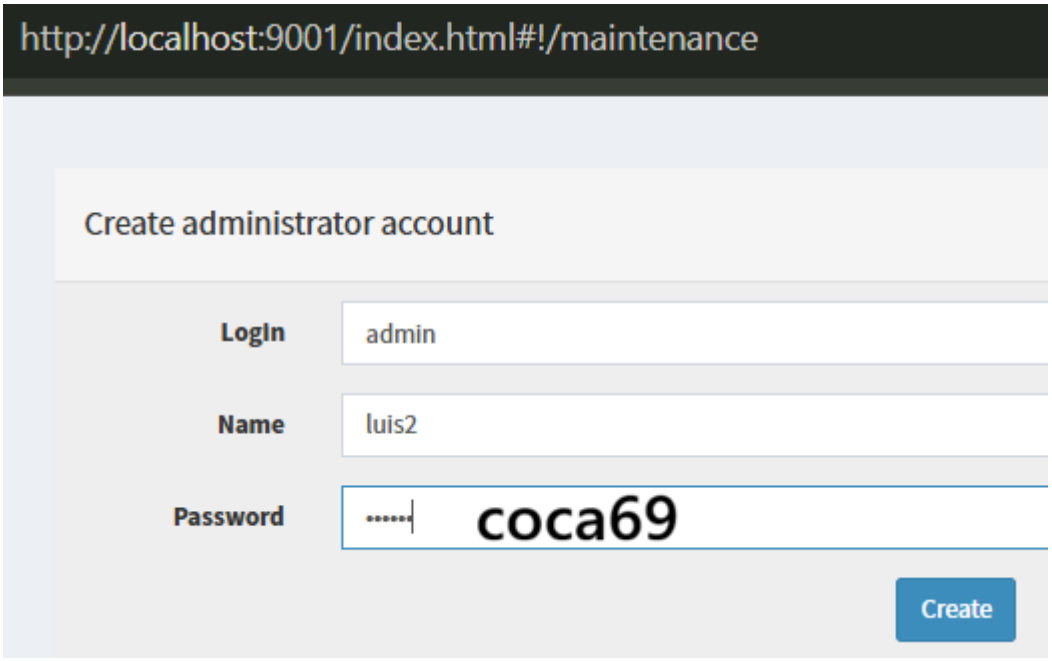
3. **Memoria Virtual: No olvides que si reinicias tu computadora, es posible que debas ejecutar nuevamente el comando `sudo sysctl -w vm.max_map_count=262144` para que Elasticsearch y el Indexer vuelvan a subir sin errores.**

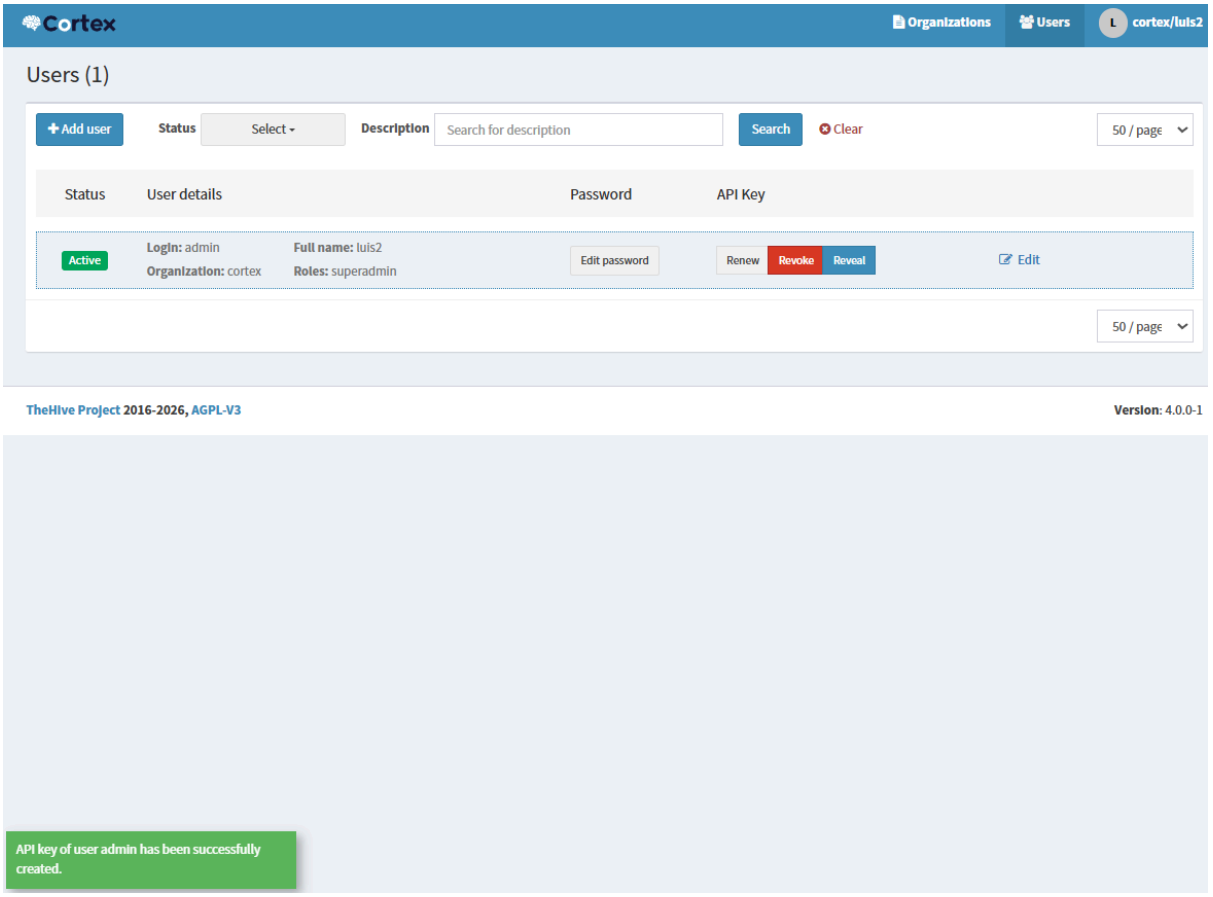


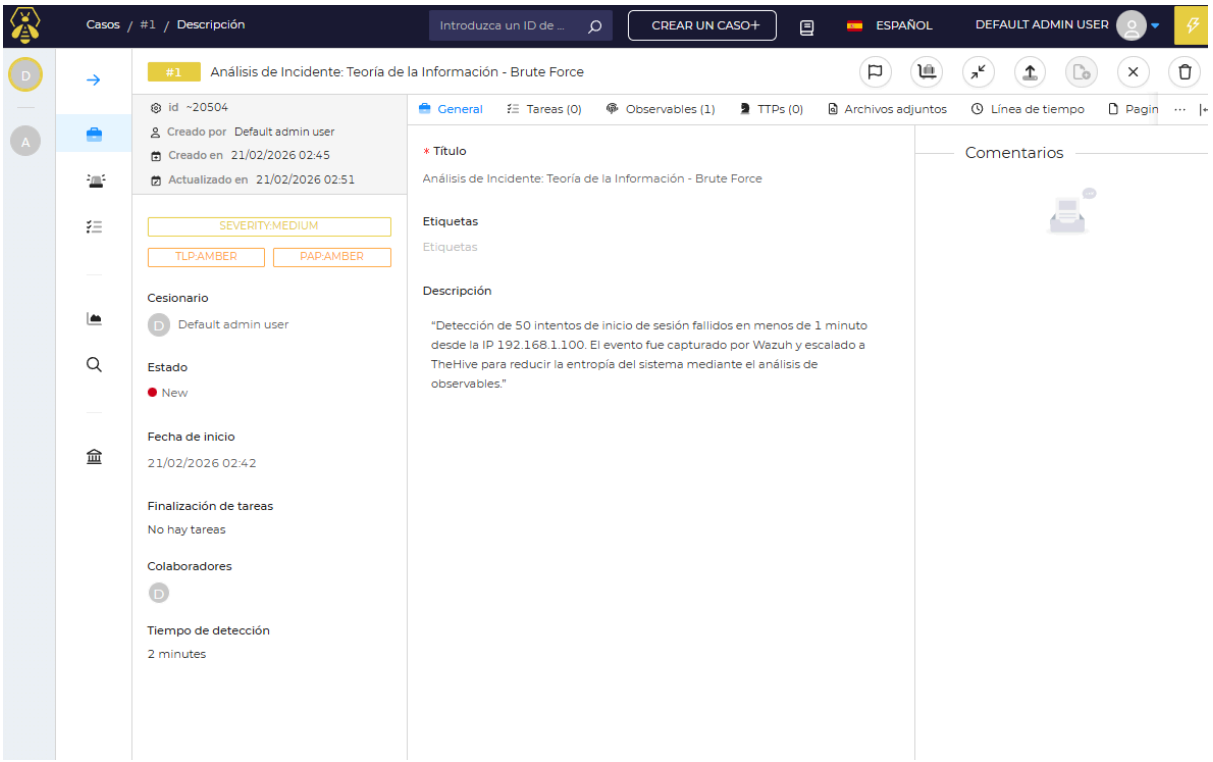



http://localhost:9000/cases
Casos
Introduzca un ID de ...
default
Filtros rápidos
Exportar lista
Crear caso
Título
teoria de la informacion
Fecha
21/02/2026 02:42
Gravedad
LOW
MEDIUM
HIGH
CRITICAL
TLP
TLP:CLEAR
TLP:GREEN
TLP:AMBER
TLP:AMBER+STRICT
TLP:RED
PAPILLA
PAP:CLEAR
PAP:GREEN
PAP:AMBER
PAP:RED
Etiquetas
Etiquetas
Descripción
Vista previa
Tareas
Campos Personalizados
Páginas
Añadir una tarea

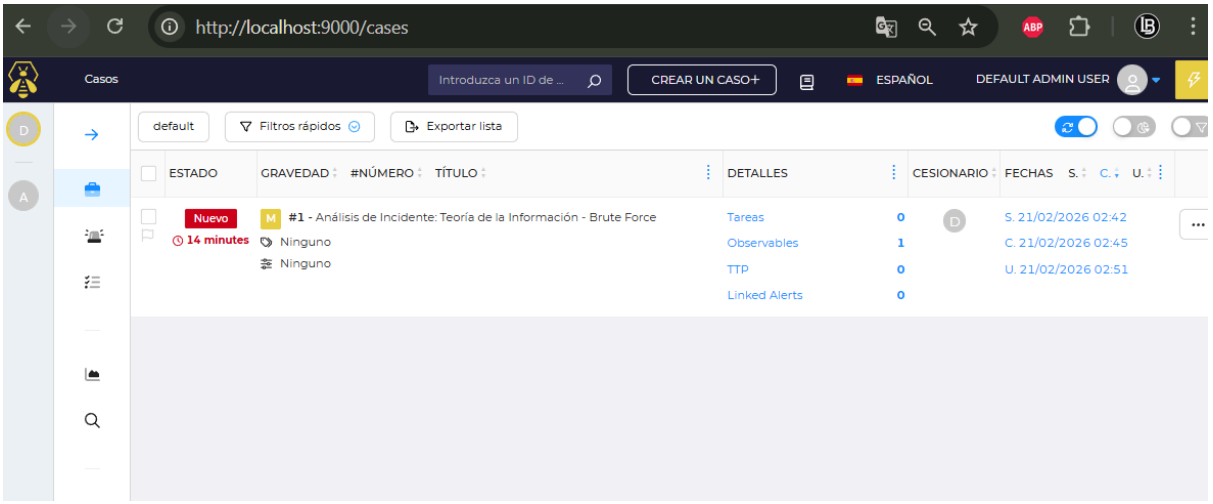

http://localhost:9001/index.html#!/maintenance
Cortex needs to update its database
Update Database


http://localhost:9001/index.html#!/maintenance
Create administrator account
Login
admin
Name
luis2
Password
coca69
Create

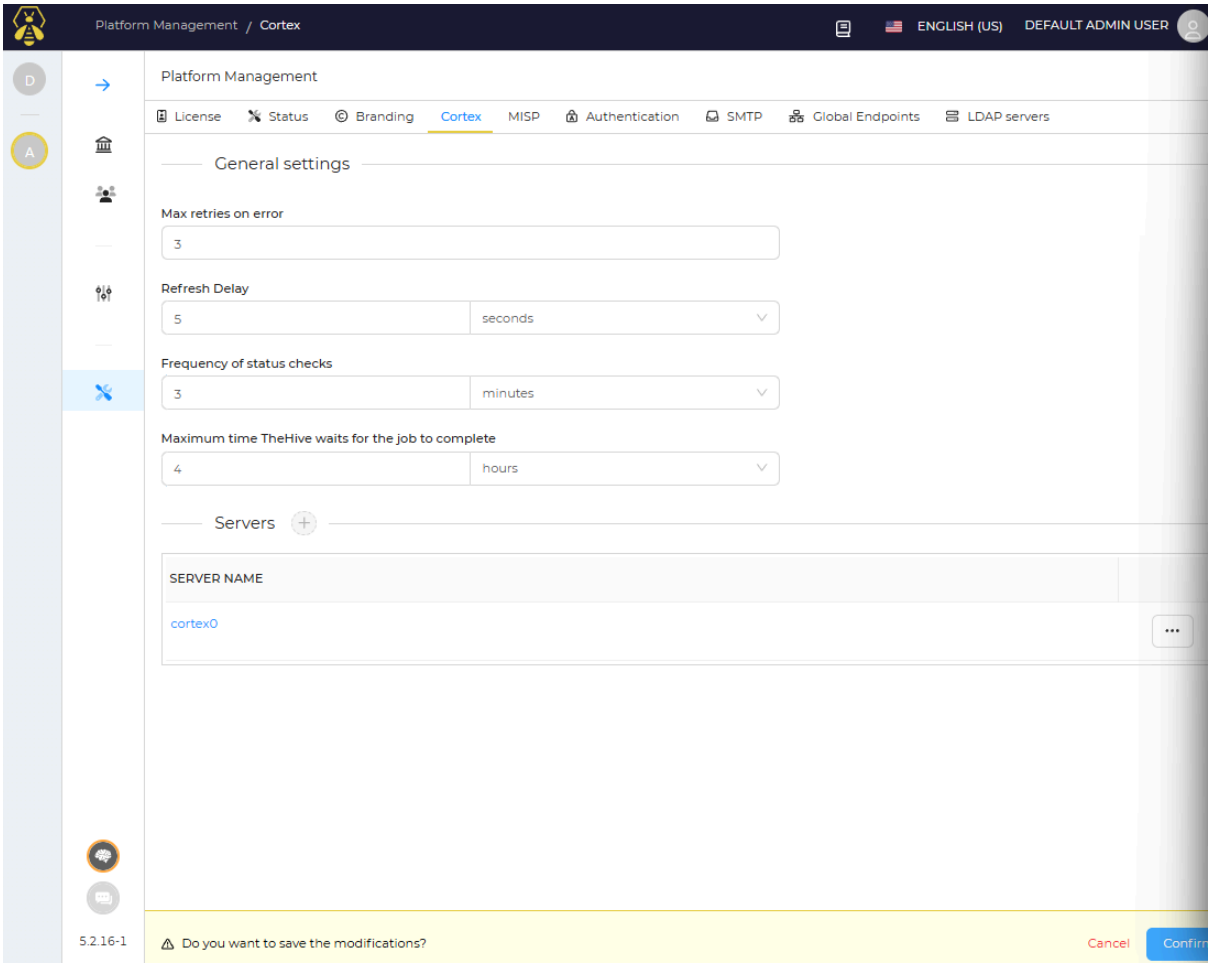


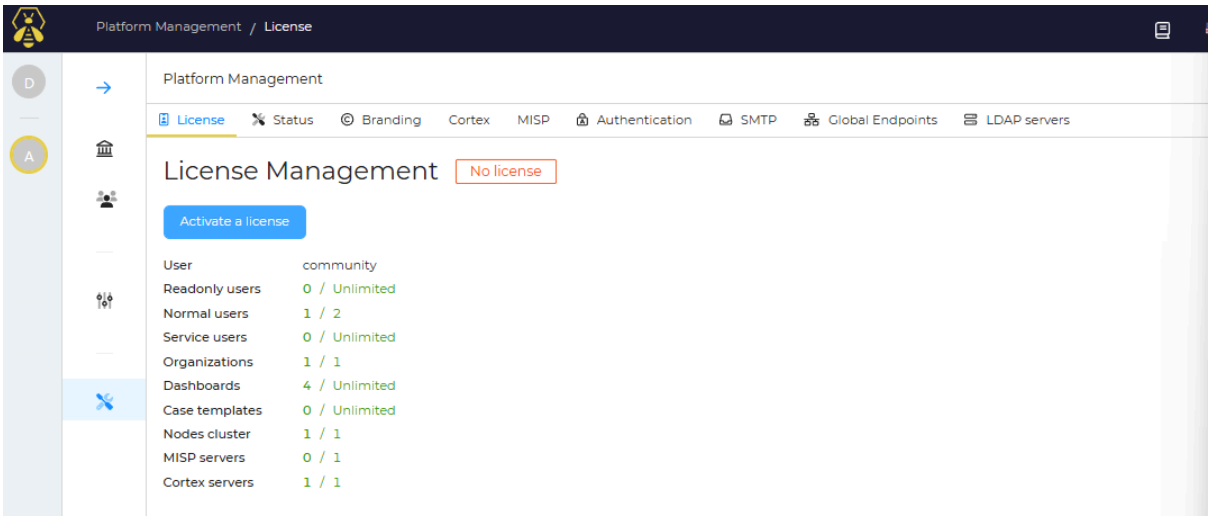


PÉREZ BARAHONA PEDRO LUIS 190300395



PÉREZ BARAHONA PEDRO LUIS 190300395





Despues de usar la pagina de hive de prueba, realizaremos en ejercicio pendiente,porque no levantaba le contenedor por dificultades de credenciales y versiones viejas ...

PÉREZ BARAHONA PEDRO LUIS 190300395

Esto guarda los certificados en el `config/wazuh_indexer_ssl_certs`directorio.Ahora es el momento de juntar nuestro archivo Docker Compose, deshacernos del contenido del archivo original y reemplazarlo con:docker-compose.yml

```
luis@LUISBARAHONAPORTATIL:~/laboratoriosoc$ ls -lh ~/laboratoriosoc
/docker-compose.yml
-rw-r--r-- 1 luis luis 2.6K Feb 21 03:45 /home/luis/laboratoriosoc/
docker-compose.yml
luis@LUISBARAHONAPORTATIL:~/laboratoriosoc$ docker compose up -d
WARN[0000] /home/luis/laboratoriosoc/docker-compose.yml: the attrib
ute `version` is obsolete, it will be ignored, please remove it to
avoid potential confusion
WARN[0000] Found orphan containers ([wazuh.manager misp redis wazuh
.indexer misp_mysql]) for this project. If you removed or renamed t
his service in your compose file, you can run this command with the
 --remove-orphans flag to clean it up.
[+] Running 5/5
 ✔Container elasticsearch  Star...                          17.5s
 ✔Container minio          Started                          17.4s
 ✔Container cassandra      Started                          17.6s
 ✔Container cortex         Started                          16.5s
 ✔Container thehive        Started                          12.4s
luis@LUISBARAHONAPORTATIL:~/laboratoriosoc$ docker compose ps
WARN[0000] /home/luis/laboratoriosoc/docker-compose.yml: the attrib
ute `version` is obsolete, it will be ignored, please remove it to
avoid potential confusion
NAME           IMAGE
    COMMAND                  SERVICE         CREATED              S
```

```
luis@LUISBARAHONAPORTATIL:~/laboratoriosoc$ docker-compose up -d
-bash: /usr/bin/docker-compose: No such file or directory
luis@LUISBARAHONAPORTATIL:~/laboratoriosoc$ cat <<EOF > ~/laborator
iosoc/docker-compose.yml
version: '3.8'

services:
  # --- TheHive, MISP, Cortex Services ---
  thehive:
    container_name: thehive
    image: strangebee/thehive:5.2
    restart: unless-stopped
    depends_on:
      - cassandra
      - elasticsearch
      - minio
      - cortex
```

```
luis@LUISBARAHONAPORTATIL:~/laboratoriosoc$ docker compose up -d
WARN[0000] /home/luis/laboratoriosoc/docker-compose.yml: the attrib
ute `version` is obsolete, it will be ignored, please remove it to
avoid potential confusion
[+] Running 12/14
[+] Running 12/14d [################] 323.3MB / 326.4MB Pulling 100.0s
[+] Running 12/14d [################] 323.3MB / 326.4MB Pulling 100.1s
[+] Running 12/14d [################] 323.3MB / 326.4MB Pulling 100.2s
[+] Running 12/14d [################] 323.3MB / 326.4MB Pulling 100.3s
[+] Running 12/14d [################] 323.3MB / 326.4MB Pulling 100.4s
[+] Running 12/14d [################] 323.3MB / 326.4MB Pulling 100.5s
[+] Running 12/14d [################] 323.3MB / 326.4MB Pulling 100.6s
[+] Running 12/14d [################] 323.3MB / 326.4MB Pulling 100.7s
[+] Running 12/14d [################] 323.3MB / 326.4MB Pulling 100.8s
[+] Running 12/14d [################] 323.3MB / 326.4MB Pulling 100.9s
[+] Running 12/14d [################] 323.3MB / 326.4MB Pulling 101.0s
[+] Running 12/14d [################] 323.3MB / 326.4MB Pulling 101.1s
[+] Running 12/14d [################] 323.3MB / 326.4MB Pulling 101.2s
```

```
WARN[0124] Found orphan containers ([redis]) for this project. If y
ou removed or renamed this service in your compose file, you can ru
n this command with the --remove-orphans flag to clean it up.
[+] Running 10/10
 ✔Container cassandra        Runnin...                    0.0s
 ✔Container elasticsearch    Ru...                        0.0s
 ✔Container cortex           Running                      0.0s
 ✔Container minio            Running                      0.0s
 ✔Container misp_mysql       Start...                    18.6s
 ✔Container thehive          Running                      0.0s
 ✔Container wazuh.manager    St...                       19.0s
 ✔Container wazuh.indexer    St...                       18.6s
 ✔Container wazuh.dashboard  Started                     17.3s
 ✔Container misp             Started                     16.0s
luis@LUISBARAHONAPORTATIL:~/laboratoriosoc$
```

Actualice el recuento máximo de mapas de la máquina virtual para los contenedores de Elasticsearch ejecutando lo siguiente:

```
sudo sysctl -w vm.max_map_count=262144
```

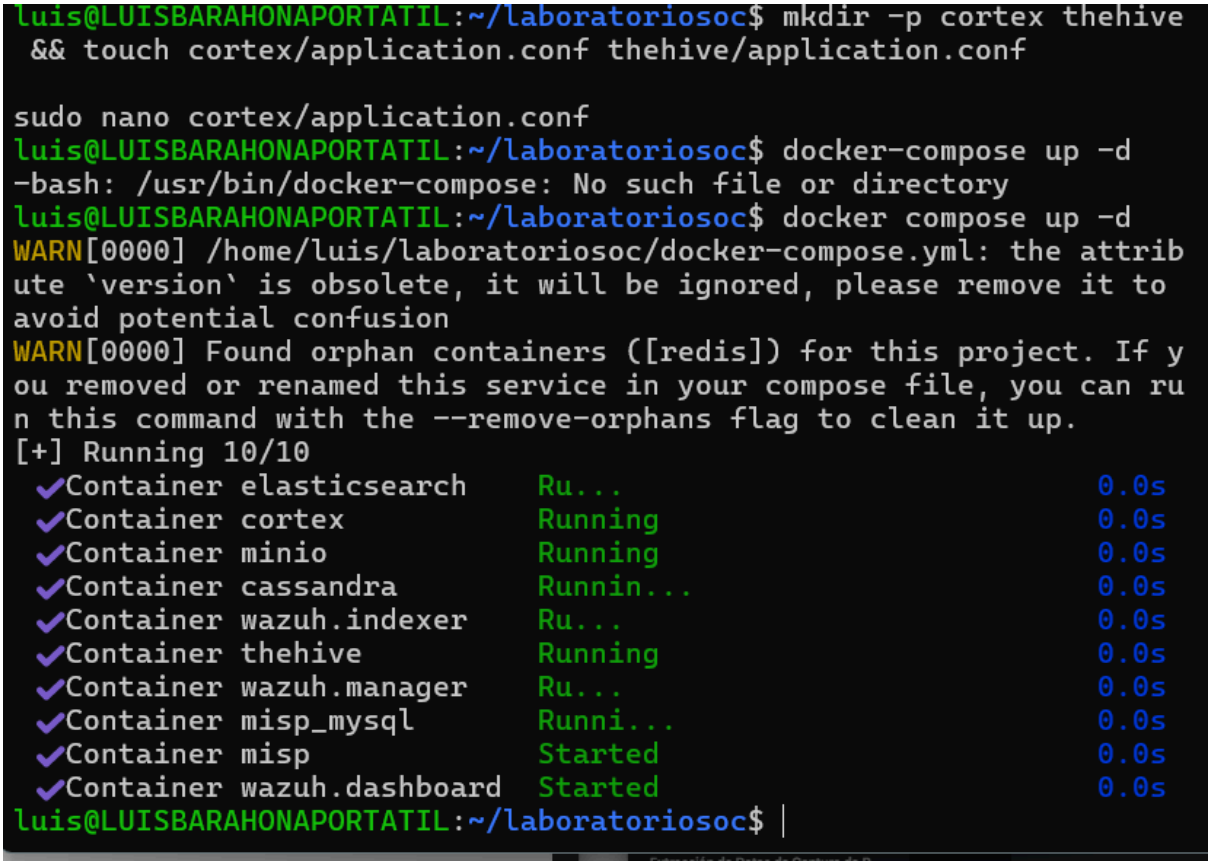
Ejecute el siguiente comando para crear la estructura de carpetas para Cortex y The Hive, así como los archivos de configuración.

```
mkdir -p cortex thehive && touch cortex/application.conf thehive/application.c

sudo nano cortex/application.conf
```

Resumen Técnico para tu reporte

- **Comando Docker Compose**: Se actualizó a la V2 (sin guion) para mayor compatibilidad con el motor de Docker moderno.
- **Configuración de Aplicación**: Al editar los archivos `.conf`, estás definiendo los **parámetros de entrada** del sistema, permitiendo que la organización pase de tener datos crudos a una arquitectura capaz de procesar inteligencia de amenazas.



¿Por qué hacemos esto? (Ingeniería en Datos)

En tu programa de **Ingeniería en datos e inteligencia organizacional**, este paso es fundamental para la **automatización de procesos**. Al definir estas URLs, Cortex ahora sabe dónde "ir a buscar" los algoritmos necesarios (analizadores) para procesar datos de entrada.

Esto reduce drásticamente la **entropía** de tu sistema de seguridad, ya que permite que la organización pase de una investigación manual a una búsqueda automatizada de inteligencia de amenazas.

Al agregar estas URLs en `application.conf`, estás definiendo el **Diccionario de Analizadores**. En la Teoría de la Información, esto reduce la **entropía** del sistema, ya que permites que Cortex sepa exactamente cómo decodificar observables (como una IP) consultando fuentes externas de inteligencia.

verifiquemos el estado de los contenedores con `docker compose ps` después de que apliques estos cambios

```
luis@LUISBARAHONAPORTATIL:~/laboratoriosoc$ echo 'play.http.secret.
key="lab123456789"' > ~/laboratoriosoc/thehive/application.conf
luis@LUISBARAHONAPORTATIL:~/laboratoriosoc$ docker compose up -d
WARN[0000] /home/luis/laboratoriosoc/docker-compose.yml: the attrib
ute `version` is obsolete, it will be ignored, please remove it to
avoid potential confusion
WARN[0000] Found orphan containers ([redis]) for this project. If y
ou removed or renamed this service in your compose file, you can ru
n this command with the --remove-orphans flag to clean it up.
[+] Running 10/10
 ✔Container wazuh.manager    Ru...                    0.0s
 ✔Container minio            Running                  0.0s
 ✔Container cassandra        Runnin...                0.0s
 ✔Container wazuh.dashboard  Running                  0.0s
 ✔Container misp_mysql       Runni...                 0.0s
 ✔Container elasticsearch    Ru...                    0.0s
 ✔Container cortex           Running                  0.0s
 ✔Container thehive          Running                  0.0s
 ✔Container misp             Started                  0.0s
 ✔Container wazuh.indexer    St...                    0.0s
luis@LUISBARAHONAPORTATIL:~/laboratoriosoc$
```

Ahora pegue lo siguiente: esto agregará los analizadores y respondedores en Cortex.

```
# Clave secreta
play.http.secret.key="5jU6h1euT1jMJt3uCe3fbO2iGcoXOkF97XESPxkALivHblLd3
vw8Vh4rJYpfL2wXcc"


# Configuración HTTP
http.address=0.0.0.0
http.port=9001


# Configuración de Akka
akka {
 cluster.enable = off
 actor {
   provider = local
 }
}


# Configuración de ElasticSearch
search {
 index = cortex
 # Nombre del índice
 uri = "http://elasticsearch:9200/"
}


# Configuración de caché
cache.job = 10 minutos
cache.user = 5 minutos
```

```
cache.organization = 5 minutos

job {
 runner = [docker]
}

# Configuración del ejecutor de trabajos de Docker
dockerJobRunner {
 # Directorio donde se encuentran los archivos de trabajo
 directory = /tmp/cortex-jobs
 # Tiempo de espera de la imagen de Docker
 timeout = 30 minutos
 # Ruta al ejecutable de Docker
 dockerExecutable = "docker"
}

analyzer {
 config {
   # Configuración del proxy HTTP
   # proxy.host = proxy.example.com
   # proxy.port = 3128

   # Configuración del proxy HTTPS
   # proxy.https.host = proxy.example.com
   # proxy.https.port = 3128

   # Autenticación del proxy
   # proxy.auth.username = nombre de usuario
   # proxy.auth.password = contraseña

   # Ignorar el proxy para estos hosts
   # proxy.nonProxyHosts = ["localhost", "127.0.0.1"]
 }

 # Tiempos de espera del analizador
 timeout = 120 segundos

 # Grupo de unión de bifurcación para analizadores
 fork-join-executor {
   parallelism-factor = 2.0
   parallelism-max = 4
 }
}

# Configuración de autenticación
auth {
 provider = [local]

 # Autenticación multifactor multifactor
```

```
 = [totp]

 # Tiempo de espera de la sesión
 session.warning = 5m
 session.inactivity = 1h
}

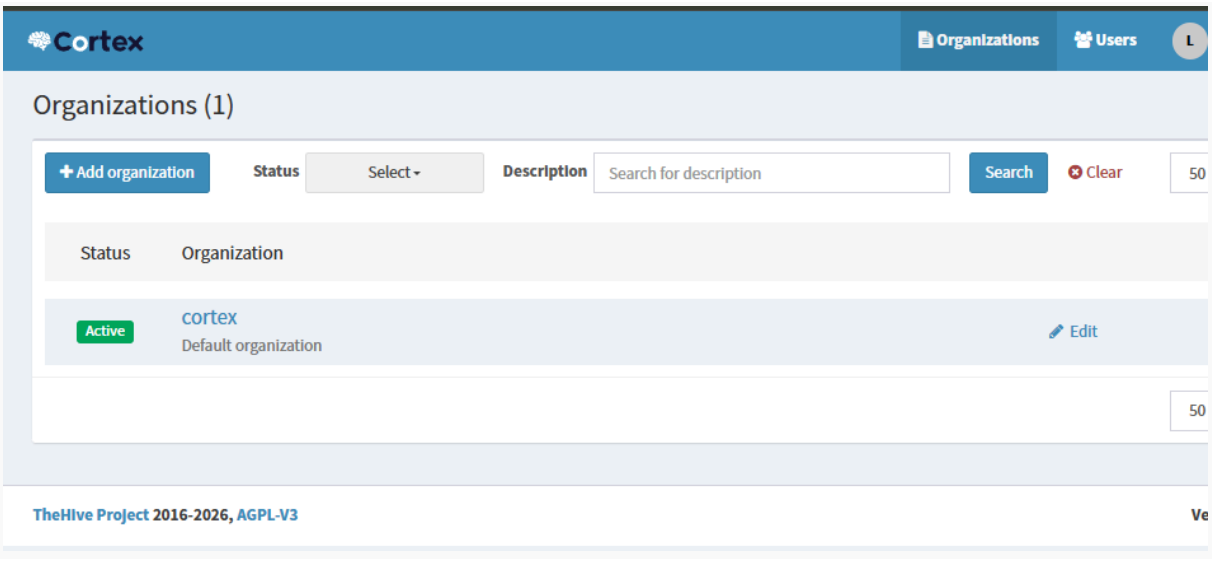

# Configuración
del almacén de datos datastore {
 name = data
 # Tamaño de los archivos almacenados
 chunksize = 1m
 hash {
   main = "SHA-256"
   extra = ["SHA-1", "MD5"]
 }
 attachment.password = "malware"
}

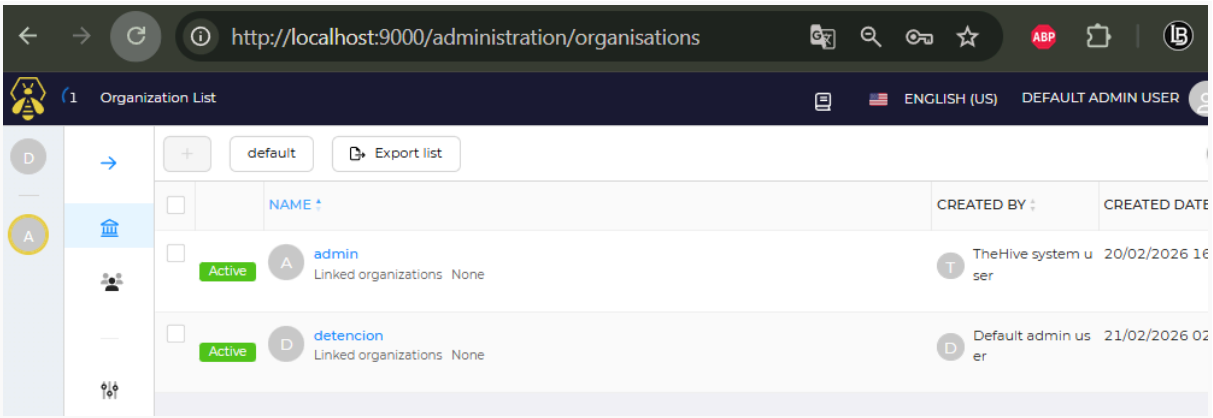

# Longitud máxima del texto
play.http.parser.maxMemoryBuffer = 1M
play.http.parser.maxDiskBuffer = 1G
```

```
luis@LUISBARAHONAPORTATIL:~/laboratoriosoc$ docker compose up -d
WARN[0000] /home/luis/laboratoriosoc/docker-compose.yml: the attrib
ute `version` is obsolete, it will be ignored, please remove it to
avoid potential confusion
WARN[0000] Found orphan containers ([redis]) for this project. If y
ou removed or renamed this service in your compose file, you can ru
n this command with the --remove-orphans flag to clean it up.
[+] Running 10/10
 ✔Container cassandra        Runnin...                          0.0s
 ✔Container elasticsearch    Ru...                              0.0s
 ✔Container wazuh.manager    Ru...                              0.0s
 ✔Container minio            Running                            0.0s
 ✔Container cortex           Running                            0.0s
 ✔Container misp_mysql       Runni...                           0.0s
 ✔Container thehive          Running                            0.0s
 ✔Container wazuh.dashboard  Running                            0.0s
 ✔Container wazuh.indexer    St...                              0.0s
 ✔Container misp             Started                            0.0s
luis@LUISBARAHONAPORTATIL:~/laboratoriosoc$ docker compose ps corte
x
WARN[0000] /home/luis/laboratoriosoc/docker-compose.yml: the attrib
ute `version` is obsolete, it will be ignored, please remove it to
avoid potential confusion
NAME      IMAGE                              COMMAND                  S
ERVICE   CREATED          STATUS          PORTS
cortex    thehiveproject/cortex:latest   "/opt/cortex/entrypo…"   c
ortex    28 minutes ago   Up 27 minutes   0.0.0.0:9001->9001/tcp, [
```

```
luis@LUISBARAHONAPORTATIL:~/laboratoriosoc$ docker compose ps
WARN[0001] /home/luis/laboratoriosoc/docker-compose.yml: the attrib
ute `version` is obsolete, it will be ignored, please remove it to
avoid potential confusion
NAME              IMAGE
      COMMAND                  SERVICE           CREATED          S
TATUS                   PORTS
cassandra         cassandra:4
      "docker-entrypoint.s…"   cassandra         44 seconds ago   U
p 43 seconds            7000-7001/tcp, 7199/tcp, 9160/tcp, 0.0.0.0
:9042->9042/tcp, [::]:9042->9042/tcp
cortex            thehiveproject/cortex:latest
      "/opt/cortex/entrypo…"   cortex            44 seconds ago   U
```

```
luis@LUISBARAHONAPORTATIL:~/laboratoriosoc$ docker compose up -d --
remove-orphans
WARN[0000] /home/luis/laboratoriosoc/docker-compose.yml: the attrib
ute `version` is obsolete, it will be ignored, please remove it to
avoid potential confusion
[+] Running 11/11
 ✔Container redis             Removed                          2.6s
 ✔Container elasticsearch     Ru...                            0.0s
 ✔Container wazuh.manager     Ru...                            0.0s
 ✔Container minio             Running                          0.0s
 ✔Container wazuh.indexer     Ru...                            0.0s
 ✔Container misp_mysql        Runni...                         0.0s
 ✔Container cassandra         Runnin...                        0.0s
 ✔Container wazuh.dashboard   Running                          0.0s
 ✔Container cortex            Running                          0.0s
 ✔Container thehive           Running                          0.0s
 ✔Container misp              Started                          0.0s
luis@LUISBARAHONAPORTATIL:~/laboratoriosoc$
```





Gemini ha dicho

¡Exacto! El despliegue de la infraestructura técnica ha terminado. En este momento, las "páginas" (las interfaces web) ya deberían ser accesibles, y lo que verás en ellas es el **cascarón operativo** de tu SOC listo para ser configurado.

Como estudiante de **Ingeniería en datos e inteligencia organizacional**, aquí te explico qué verás y cuál es la función de cada servicio en este ecosistema:

¿Qué deberías ver en cada página?

1. Wazuh Dashboard (`https://localhost:8443`)

- **Lo que verás:** Un panel de control (SIEM) inicialmente vacío o con datos de "salud" del propio servidor.
- **Función:** Es tu **fuente de datos**. Se encarga de recolectar logs de tus computadoras y servidores para detectar ataques (como el "Brute Force" que planeas simular).

2. TheHive (`http://localhost:9000`**)**

- **Lo que verás:** Una plataforma de gestión de incidentes donde podrás crear "Casos".
- **Función:** Es el **cerebro de la operación**. Aquí es donde organizas la respuesta al incidente. Por ejemplo, si Wazuh detecta un ataque, se crea un caso aquí para que tú lo analices.

3. Cortex (`http://localhost:9001`**)**

- **Lo que verás:** Una lista de "Analizadores" que puedes activar (VirusTotal, AbuseIPDB, etc.).
- **Función:** Es el **motor de inteligencia**. Su trabajo es tomar un dato crudo (una IP sospechosa) y enriquecerlo consultando bases de datos externas para decirte si es peligrosa.

4. MISP (`https://localhost`**)**

- **Lo que verás:** Un repositorio de indicadores de compromiso (IoC).
- **Función:** Es la **base de conocimientos compartida**. Sirve para almacenar y compartir información sobre malware y amenazas con otras organizaciones.

Tu Reporte: Reducción de Entropía

Para tu proyecto de **Teoría de la Información**, este despliegue demuestra cómo la tecnología reduce la incertidumbre:

- **Sin el SOC:** Recibes miles de logs (datos con alta entropía/desorden) y no sabes cuáles son ataques.
- **Con el SOC:** Wazuh filtra el ruido, TheHive organiza la información y Cortex añade certidumbre al análisis. Estás transformando **datos** en **inteligencia organizacional**.

ultimo paso, para verificar que todos los servicios este funcionando:

docker compose ps

```
luis@LUISBARAHONAPORTATIL:~/laboratoriosoc$ docker compose ps
WARN[0000] /home/luis/laboratoriosoc/docker-compose.yml: the attrib
ute `version` is obsolete, it will be ignored, please remove it to
avoid potential confusion
NAME              IMAGE
      COMMAND                  SERVICE           CREATED         ST
ATUS                          PORTS
cassandra         cassandra:4
      "docker-entrypoint.s…"   cassandra         7 minutes ago   Up
 7 minutes                    7000-7001/tcp, 7199/tcp, 9160/tcp, 0.
0.0.0:9042->9042/tcp, [::]:9042->9042/tcp
cortex            thehiveproject/cortex:latest
      "/opt/cortex/entrypo…"   cortex            7 minutes ago   Up
 7 minutes                    0.0.0.0:9001->9001/tcp, [::]:9001->90
01/tcp
elasticsearch     docker.elastic.co/elasticsearch/elasticsearch:7.1
7.9   "/bin/tini -- /usr/l…"   elasticsearch     7 minutes ago   Up
 7 minutes                    0.0.0.0:9200->9200/tcp, [::]:9200->92
00/tcp, 9300/tcp
minio             quay.io/minio/minio
      "/usr/bin/docker-ent…"   minio             7 minutes ago   Up
 7 minutes                    9000/tcp, 0.0.0.0:9002->9002/tcp, [::
]:9002->9002/tcp
misp              coolacid/misp-docker:core-latest
      "/entrypoint.sh"         misp              7 minutes ago   Re
starting (2) 2 seconds ago
misp_mysql        mysql/mysql-server:5.7
      "/entrypoint.sh mysq…"   misp_mysql        7 minutes ago   Up
 7 minutes (healthy)          3306/tcp, 33060/tcp
thehive           strangebee/thehive:5.2
      "/opt/thehive/entryp…"   thehive           7 minutes ago   Up
 7 minutes                    0.0.0.0:9000->9000/tcp, [::]:9000->90
00/tcp
wazuh.dashboard   wazuh/wazuh-dashboard:4.11.0
      "/entrypoint.sh"         wazuh.dashboard   7 minutes ago   Up
 9 seconds                    443/tcp, 0.0.0.0:8443->5601/tcp, [::]
:8443->5601/tcp
wazuh.indexer     wazuh/wazuh-indexer:4.11.0
      "/entrypoint.sh open…"   wazuh.indexer     7 minutes ago   Re
starting (1) 10 seconds ago
```

⚠️ AVISO LEGAL IMPORTANTE DE SEGURIDAD:

Esta implementación está diseñada únicamente para fines de laboratorio y aprendizaje. Utiliza credenciales y configuraciones predeterminadas que NO SON SEGURAS PARA ENTORNOS DE PRODUCCIÓN . Antes de implementar en un entorno de producción, debe:

Cambiar todas las contraseñas predeterminadas
Configurar certificados TLS/SSL adecuados
Implementar la segmentación de la red
Configurar controles de acceso adecuados
Configurar procedimientos de copia de seguridad
Implementar el monitoreo de la propia infraestructura

Ejecutar estas herramientas con credenciales predeterminadas en un entorno de producción o en un servidor con acceso a Internet plantearía graves riesgos de seguridad.

¡Eso es todo por la configuración inicial del entorno SOC! En las próximas historias, exploraremos cómo configurar estas herramientas para que se comuniquen entre sí, implementar algunos agentes de Wazuh, generar registros de prueba para su análisis y desarrollar reglas de detección.

También veremos cómo crear flujos de trabajo automatizados entre TheHive y MISP para compartir inteligencia sobre amenazas y configurar analizadores Cortex para enriquecer los eventos de seguridad.

Referencias:

https://strangebee.com

https://wazuh.com

https://www.misp-project.org