

Informe de Implementación del Proyecto SOC-LAB

Este documento detalla el proceso de implementación del laboratorio de ciberseguridad SOC-LAB, integrando TheHive, Cortex, MISP y Wazuh en una máquina virtual con Ubuntu Server, utilizando contenedores Docker y orquestación con Docker Compose.

Proceso de Implementación

- Preparación del entorno: Se configuró una máquina virtual en VirtualBox con Ubuntu Server.
Desde Windows PowerShell se accedió a la VM mediante SSH.
- Instalación de Docker y Docker Compose: Se habilitó el servicio de Docker y se corrigieron problemas de permisos con el socket de Docker (`/var/run/docker.sock`) asignando correctamente el grupo `docker` al usuario. Finalmente, se migró del comando clásico `docker-compose` al nuevo `docker compose`.
- Descarga e inicio de servicios: Mediante `docker compose pull` y `docker compose up -d` se levantaron los contenedores de Cassandra, Elasticsearch, MinIO, Cortex y TheHive.

```
rocko@rockos:~/soc-lab$ sudo docker compose ps
[sudo] password for rocko:
WARN[0001] /home/rocko/soc-lab/docker-compose.yml: the attribute `version` is obsolete, it will be ignored, please remove it to avoid potential confusion
NAME                                IMAGE                                COMMAND                                SERVICE
-----                                -
soc-lab-cassandra-1                 cassandra:4                         "docker-entrypoint.s..."  cassandra
37 hours ago Up 3 hours 7000-7001/tcp, 7199/tcp, 9042/tcp, 9160/tcp
soc-lab-cortex-1                     thehiveproject/cortex:latest        "/opt/cortex/entrypo..."  cortex
37 hours ago Up 3 hours 0.0.0.0:9001->9001/tcp
soc-lab-elasticsearch-1             docker.elastic.co/elasticsearch/elasticsearch:7.17.9
37 hours ago Up 3 hours 0.0.0.0:9200->9200/tcp, 9300/tcp
soc-lab-minio-1                     quay.io/minio/minio                 "/usr/bin/docker-ent..."  minio
37 hours ago Up 3 hours 9000/tcp, 0.0.0.0:9002->9002/tcp
soc-lab-thehive-1                   strangebee/thehive:5.2              "/opt/thehive/entryp..."  thehive
2 hours ago Up 2 hours 0.0.0.0:9000->9000/tcp
```

- Problema inicial con TheHive: El servicio no levantaba en el puerto 9000. Se resolvió

```
rocko@rockos: ~/soc-lab
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Instale la versión más reciente de PowerShell para obtener nuevas características y mejoras. https://aka.ms/PSWindows

PS C:\WINDOWS\system32> ssh rocko@192.168.101.125
>>
The authenticity of host '192.168.101.125 (192.168.101.125)' can't be established.
ED25519 key fingerprint is SHA256:Z6Jm/qPUT01uBkZVCVb3dqBTHADCWvX20HAfwLBhpcQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.101.125' (ED25519) to the list of known hosts.
rocko@192.168.101.125's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-83-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of jue 18 sep 2025 13:10:42 UTC

System load:          0.18
Usage of /:            26.8% of 27.37GB
Memory usage:         3%
Swap usage:           0%
Processes:            183
Users logged in:      1
IPv4 address for enp0s3: 192.168.101.125
IPv6 address for enp0s3: 2806:2f0:8001:e147:a00:27ff:fef4:d75c

El mantenimiento de seguridad expandido para Applications está desactivado
Se pueden aplicar 0 actualizaciones de forma inmediata.

1 actualización de seguridad adicional se puede aplicar con ESM Apps.
Aprenda más sobre cómo activar el servicio ESM Apps at https://ubuntu.com/esm
```

eliminando el contenedor y el volumen de datos asociado, recreando la instancia y verificando logs. Posteriormente, TheHive quedó accesible en <http://192.168.101.125:9000>.

- Configuración en TheHive: Se creó una nueva organización llamada 'SOC-LAB'. Se añadieron usuarios, ajustando el login al formato de correo electrónico (ejemplo: usuario@hive.com). Se definieron contraseñas y perfiles de usuario como

'org-admin' y 'analyst'.



Creation date

18/09/2025 11:06 🕒 an hour ago

Description

Laboratorio de ciberseguridad para pruebas con TheHive, Cortex y MISP

Tasks sharing rule

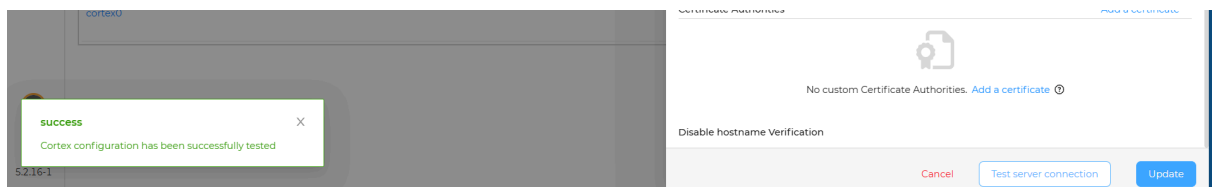
manual

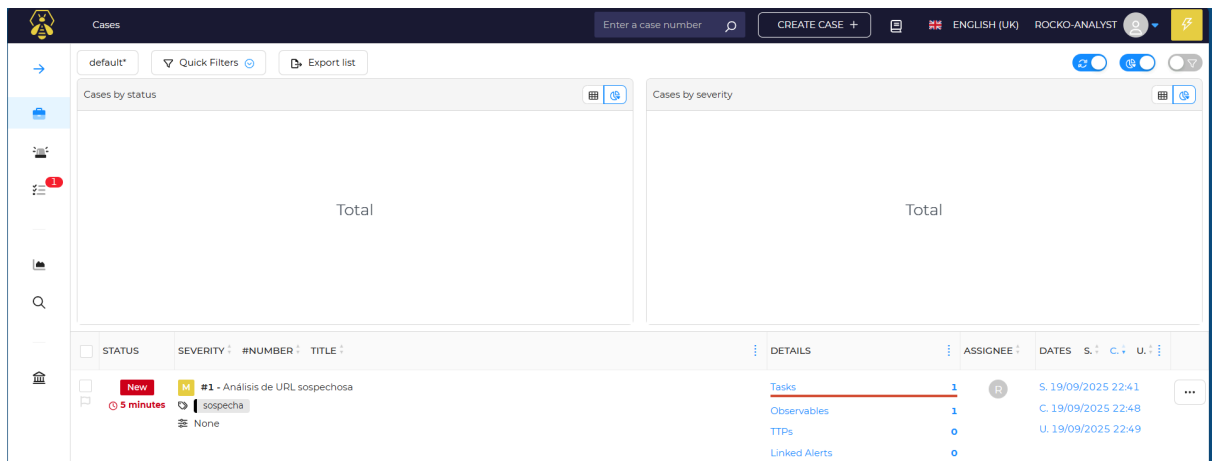
Observables sharing rule

manual

- Conexión TheHive ↔ Cortex: Desde la interfaz de TheHive (Administración → Connectors → Cortex), se añadió un conector hacia Cortex en <http://cortex:9001> (alternativamente con la IP del host). Se generó y utilizó una API Key para la autenticación.

Status	User details	Password	API Key
Active	Login: admin@hive.com Organization: cortex	Full name: admin Roles: superadmin Edit password	Renew Revoke Reveal





- Conexión TheHive ↔ MISP: Se configuró un conector hacia MISP en <https://192.168.101.125>. Se utilizó el usuario administrador de MISP y la clave API generada en su interfaz. Esto permitió enviar observables desde TheHive a MISP y enriquecer casos con inteligencia de amenazas.
- Integración con Wazuh: Se desplegó Wazuh Manager y Dashboard en <https://192.168.101.125:8443>. Se configuró el acceso con el usuario 'admin' y la contraseña definida en la instalación. Se documentó cómo integrar Wazuh con TheHive mediante webhooks y TheHive4py para crear casos automáticos a partir de alertas.

```

WARN[0002] /home/rocko/soc-lab/docker-compose.yml: the attribute `version` is obsolete, it will be ignored, please remove it to avoid potential confusion
[+] Running 5/43
  * wazuh.indexer [          ] Pulling                               11.2s
    : bab71400c7ab Waiting                                       7.2s
    : c8ae09df68a2 Waiting                                       7.2s
    : 275f81c85715 Waiting                                       7.2s
    : e66a44ce12c3 Waiting                                       7.2s
    : 40e455cc4f9e Waiting                                       7.2s
    : 47122897cd80 Waiting                                       7.2s
    : 117499635ace Waiting                                       7.2s
    : b50683980203 Waiting                                       7.2s
    : a03f5f266255 Waiting                                       7.2s
    : f3ae03c852cb Waiting                                       7.2s
    : b048ddb32f6 Waiting                                       7.2s
    : 24cea50d42ad Waiting                                       7.2s
    : 3877503365af Waiting                                       7.2s
  * wazuh.manager [          ] Pulling                               11.2s
    : a34f3425a987 Waiting                                       6.3s
    : d3e833975312 Waiting                                       6.3s
    : b8a0fe1474d3 Waiting                                       6.3s
    : 3fbff7726e90 Waiting                                       6.3s
    : 400d7021914f Waiting                                       6.3s
    : bbc542e39c4e Waiting                                       6.3s
    : 7936a8856003 Waiting                                       6.3s
    : 992ea5933a27 Waiting                                       6.3s
    : dfb01fe28adf Waiting                                       6.3s
    : 93296b6587ea Waiting                                       6.3s
    : 9f0d0e4bf209 Waiting                                       6.3s
    : 2a803331c5e3 Waiting                                       6.3s
    : af7190a8b8db Waiting                                       6.3s
    : 531ead2a685f Waiting                                       6.3s
  * wazuh.dashboard [.....] Pulling                               11.2s
    : 878bc77d48b9 Downloading [=====>] 8.079MB/...             7.3s
    : a6f26737fd15 Downloading [=====>] 10.19MB/...              7.3s
    : 4c7ae2f80294 Download complete                               1.5s
    : 8ac0613e7d5b Download complete                               3.1s
    : df1a6a512281 Download complete                               4.6s
    : b2bd2dfa12f8 Download complete                               6.3s
    : f37e3368004b Download complete                               7.1s
    : f0e458e9d7cf Waiting                                       7.3s
    : bbea8c2e6a48 Waiting                                       7.3s
    : d3297ba56cf9 Waiting                                       7.3s
    : 8402d4be7318 Waiting                                       7.2s
    : f6927f196915 Waiting                                       7.2s
    : 4f4fb700ef54 Waiting                                       7.2s

```

- Prueba de flujo de trabajo: Se creó un caso de prueba en TheHive (ejemplo: 'Phishing test'), se añadieron observables (como dominios maliciosos) y se ejecutaron analizadores de Cortex (VirusTotal, AbuseIPDB). Los resultados se vincularon con MISP, confirmando la integración entre los sistemas.

Configurar Wazuh

1. Accede al Dashboard de Wazuh: <https://192.168.101.125:8443>
 - Usuario: `admin`
 - Contraseña: la que definiste (`kibanaserver` si no cambiaste)
2. Comprueba que el Manager y el Indexer estén corriendo:
 - `sudo docker logs -f wazuh.manager`
 - `sudo docker logs -f wazuh.indexer`

3. Opcional: Configura Webhooks en Wazuh para enviar alertas a TheHive.

-

Dificultades y Soluciones

Durante la implementación se enfrentaron varias dificultades técnicas: - Problemas con permisos en el socket de Docker que impedían ejecutar `docker ps` sin sudo. - Error 'Connection reset by peer' al intentar acceder a TheHive en el puerto 9000, que se resolvió recreando contenedores y volúmenes. - El uso de `docker-compose` antiguo generaba errores de 'ContainerConfig'; se solucionó migrando al plugin oficial `docker compose`. - En la creación de usuarios en TheHive, el sistema requería que los logins fueran correos electrónicos válidos, lo cual no estaba documentado inicialmente.

Conclusiones

La implementación del SOC-LAB permitió integrar herramientas clave para la detección, análisis y respuesta ante incidentes de ciberseguridad. Con TheHive como plataforma central de gestión de casos, Cortex para análisis automatizados, MISP como repositorio de inteligencia de amenazas y Wazuh como sistema de monitoreo, se logró establecer un entorno funcional para pruebas y capacitación en operaciones de seguridad.