

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.
- 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/qPUT0luBkZVCVb3dqBTHADCWvX20HAFwLBhcpQ.
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	<button>Edit password</button>	<button>Renew</button> <button>Revoke</button> <button>Reveal</button>

- 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.



- 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.