



ColossuSIEM

Michael McAloon y Cosmin Bora



— ÍNDICE

1. ColossuSIEM
2. Estructura
3. Componentes
4. Funcionamiento
5. Futuras Posibilidades
6. Conclusiones



— PRESENTACIÓN DEL EQUIPO



**Michael Dylan
McAloon Torres**

ASIXc

La eternidad es mucho
tiempo, especialmente hacia
el final



**Cosmin Bora
Tomoiaga**

ASIXc

La simplicidad es una
cuestión de gusto

1. COLOSSUSIEM

Nuestra Empresa

— CREACIÓN Y EXPLICACIÓN DE LA EMPRESA

NUESTRO NOMBRE

Colossus proviene del latín y en Grecia se usaba para nombrar a las gigantescas estatuas.

Siem significa Sistema de Gestión de Eventos e Información de Seguridad que es el principal servicio que ofrecemos.

Nos pareció una buena idea el nombre dado a la cantidad de posibilidades que ofrecemos con nuestros servicios.

Para poder visualizar nuestro código diríjase al siguiente link
GitHub: <https://github.com/SkytheK/ColossuSIEM>

QUE OFRECEMOS

Integración de Port Mirror + Snort + Elastic Stack + TheHive + Cortex + MISP



COLOSSUSIEM

— DAFO

FORTALEZAS

Una gran cantidad de servicios con rápido despliegue y todo integrado

DEBILIDADES

Necesidad de mucho tiempo de dedicación y monitoreo

F

D

O

A

Innovador y ofrece seguridad

OPORTUNIDADES

Que las empresas no entiendan la arquitectura de ColossuSIEM

AMENAZAS

2. ESTRUCTURA

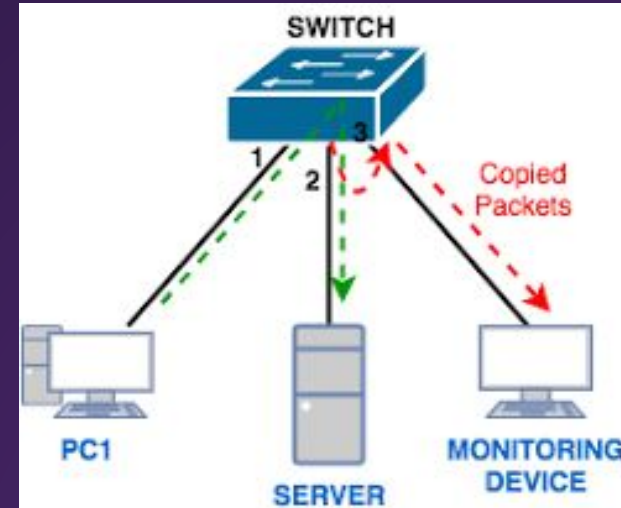
Desarrollo de la Empresa

— PORT MIRRORING

- Envía copias de paquetes de un puerto origen del switch a un puerto de destino en otro puerto del switch.

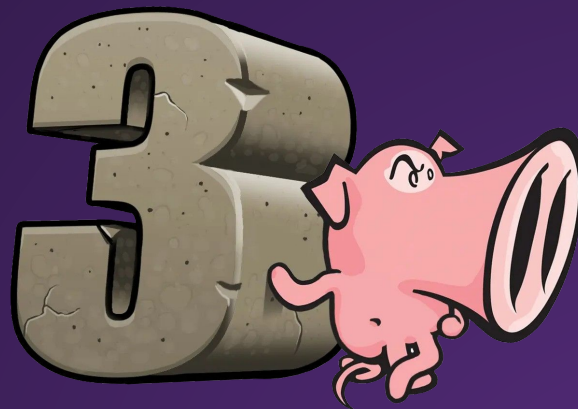
Switch(config)# monitor session 1 source interface FastEthernet 0/1

Switch(config)# monitor session 1 destination interface FastEthernet 0/3



— SNORT 3.0

- Configuración (Variables \$HOME_NET / \$EXTERNAL_NET)
`/usr/local/etc/snort/snort.lua`
- Creación de Reglas
`/usr/local/etc/rules/local.rules`
- Alertas y Logs
`/var/log/snort/alert_fast.txt`



```
snort -c /usr/local/etc/snort/snort.lua -R /usr/local/etc/rules/local.rules -i enp0s3 -s 65535 -k none -l /var/log/snort/
```

— FILEBEAT /ELASTICSEARCH / KIBANA

- Filebeat Short
`./filebeat -e -c filebeat.yml`
- Elasticsearch datos
`./elasticsearch`
- Kibana visualización
`./kibana`



THEHIVE

- Plataforma de respuesta de incidentes
- Integraciones Cortex y MISP

/ColossuSIEM/thehive/application.conf



CORTEX

- Analizador para los datos que le de TheHive
- Contiene miles de Analizadores

/ColossuSIEM/cortex/application.conf



— MISP

- Analizador para TheHive



3. COMPONENTES

Componentes Utilizados

— PORT MIRROR

- Switch Cisco Catalyst 2950



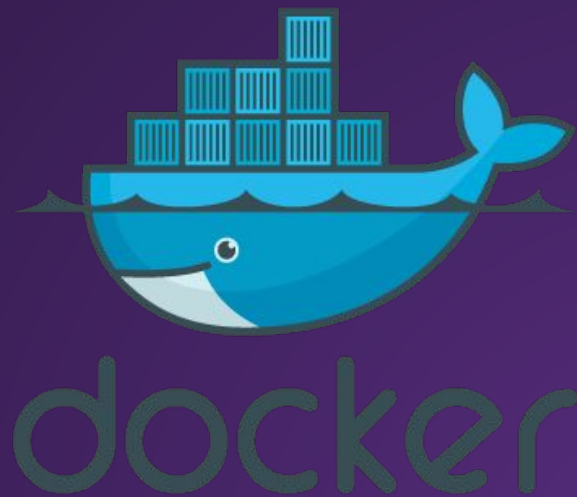
— ORDENADORES

- Conectamos dos ordenadores.



— SIEM

- Docker y Docker-Compose

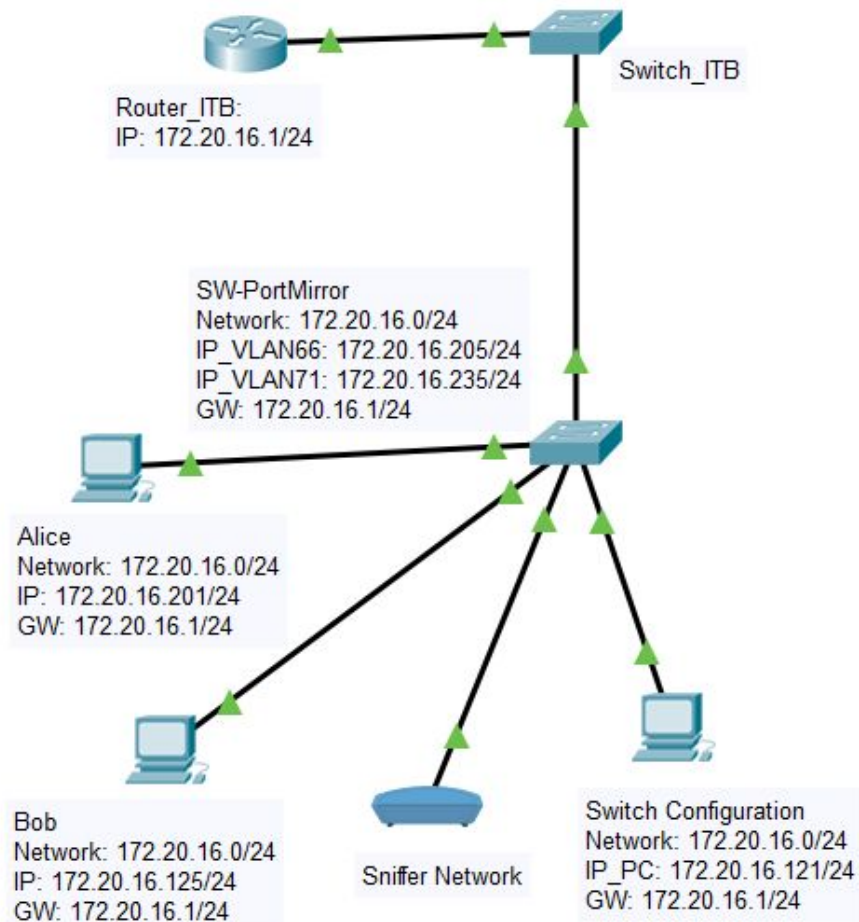


4. FUNCIONAMIENTO

¿Como funciona ColossuSIEM?

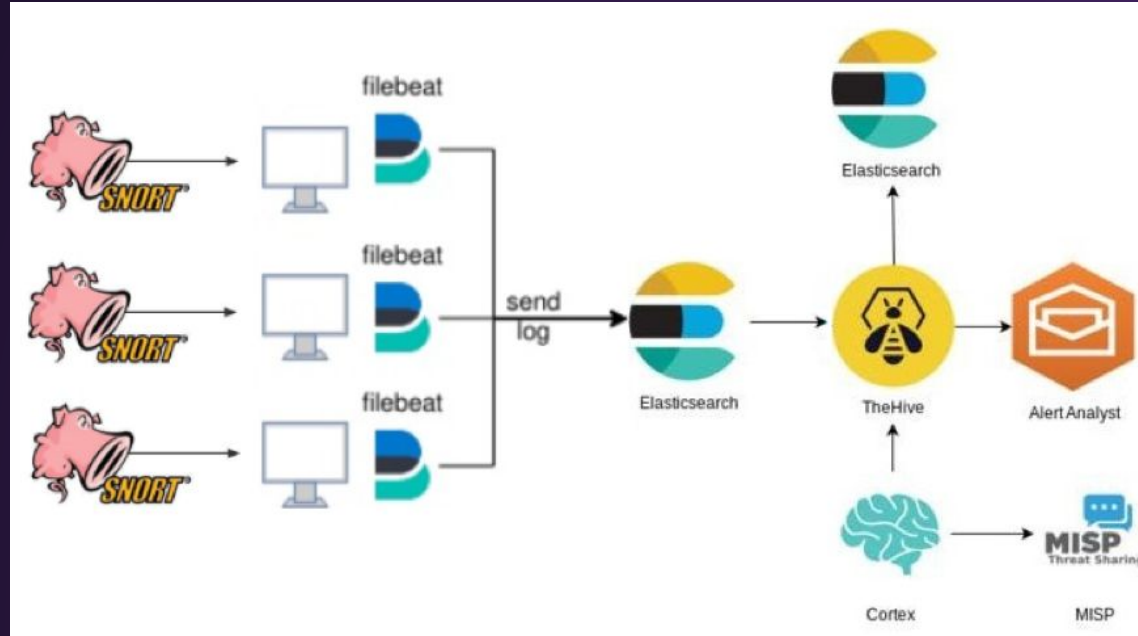
DIAGRAMA

- Port Mirror



— DIAGRAMA SIEM

- Funcionamiento de ColossuSIEM.





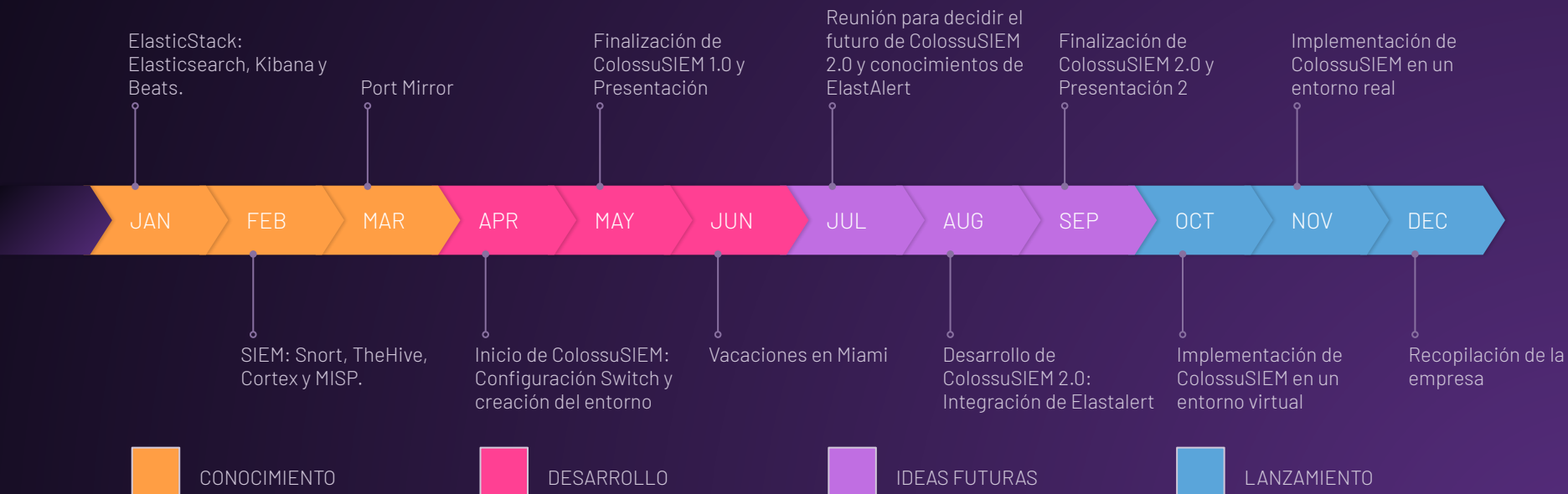
TEST

Test del Funcionamiento

5. Futuras Posibilidades

Ideas de Futuro

TIMELINE 2021



6. CONCLUSIONES

Final del Proyecto



FIN.
GRACIAS POR SU ATENCIÓN