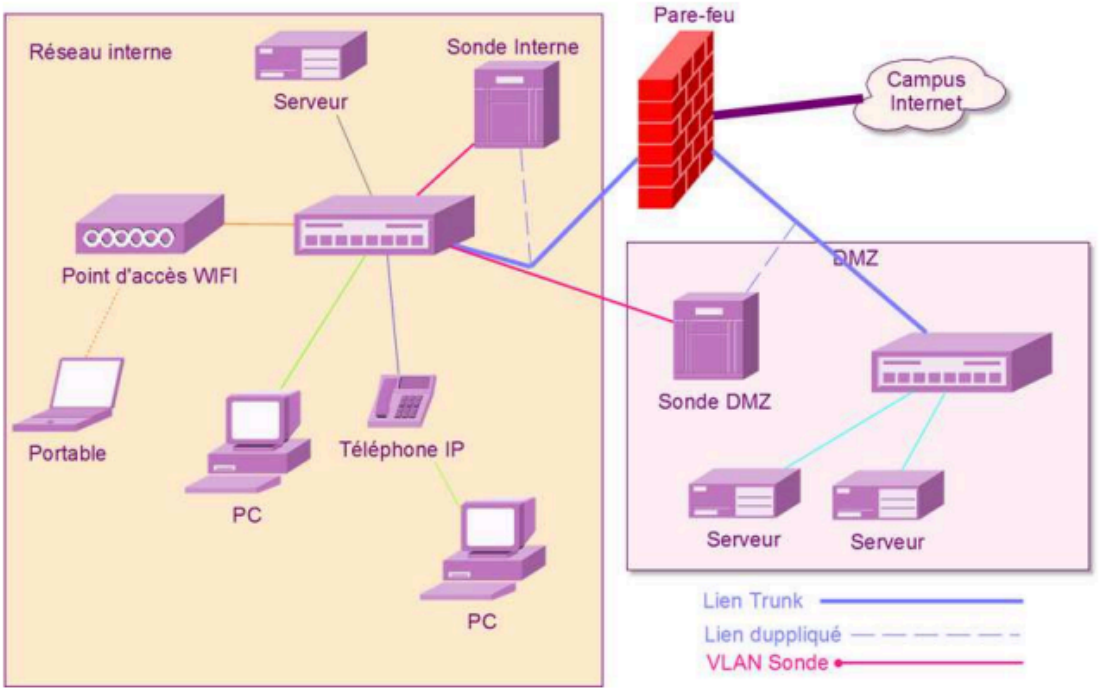
Suricata

#linux #schoolproject #suricata


```
● suricata.service - Suricata IDS/IDP daemon
     Loaded: loaded (/lib/systemd/system/suricata.service; enabled; preset: enabled)
     Active: active (running) since Mon 2025-02-10 11:06:17 CET; 2 days ago
```

Schéma potentiel d'utilisation de notre IPS/IDS :

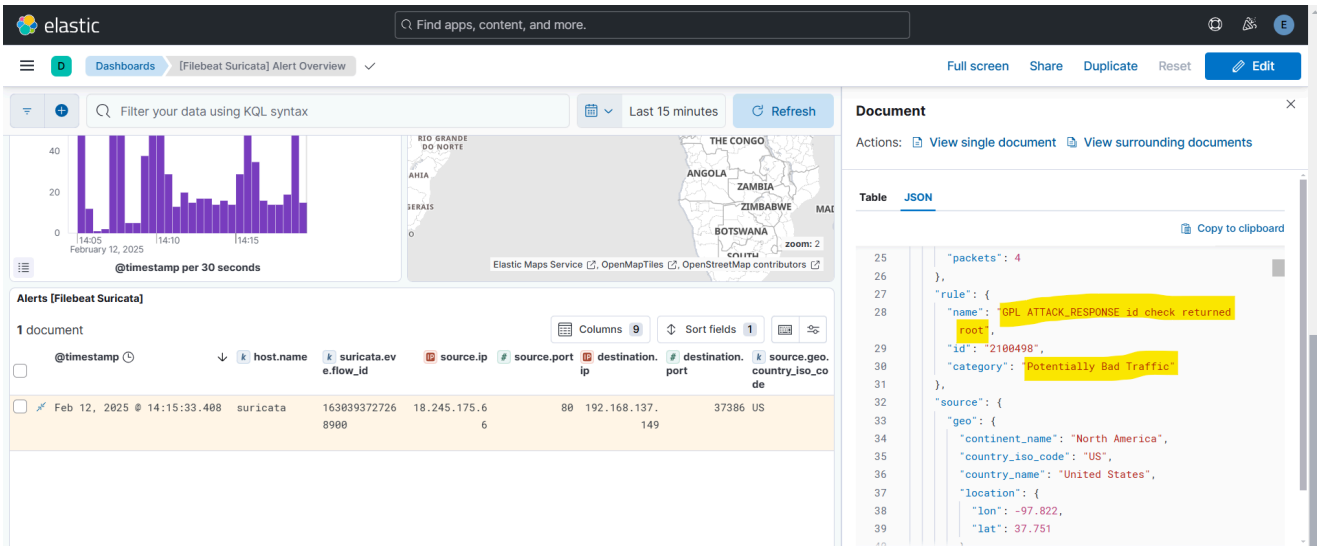


Test de notre Suricata :

```
curl http://testmynids.org/uid/index.html
```

```
dylan@suricata:~$ curl http://testmynids.org/uid/index.html
uid=0(root) gid=0(root) groups=0(root)
```

cette commande est censé nous renvoyer une alerte dans le style **GPL_ATTACK_RESPONSE**



Ici on voit que notre suricata a bien détecter le log effectué au par avant et a classer ceci comme "potentiel bad traffic", ce qui nous montre bien que notre système marche.

De plus nous allons effectué un test avec Exegol voir si Suricata détecte bien nos test d'intrusion.

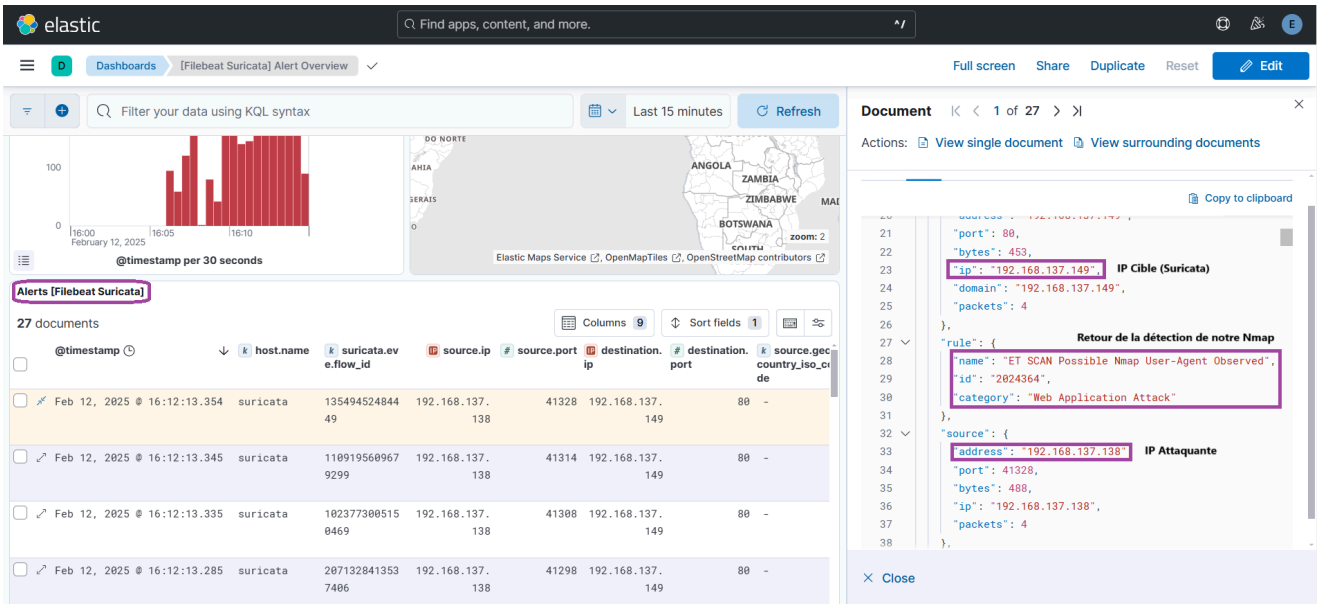
Exegol est un environnement de pentest basé sur Docker, offrant une alternative moderne et flexible aux traditionnels Kali Linux. Exegol vise à fournir un environnement isolé et reproductible adapté à divers besoins en cybersécurité.

Test :

```
[Feb 12, 2025 - 15:45:34 (CET)] exegol-daily /workspace # nmap 192.168.137.149
Starting Nmap 7.93 ( https://nmap.org ) at 2025-02-12 15:53 CET
Nmap scan report for 192.168.137.149
Host is up (0.0030s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
9200/tcp open  wap-wsp
MAC Address: 00:0C:29:0E:23:FA (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.36 seconds
```

Voici un simple Nmap effectué pour voir si suricata va détecter quelque chose



Ici, Suricata a bien détecter notre Nmap effectué et nous a remonté les infos de celle ci, nous recueillions diverse informations tel que l'IP Cible et Attaquante, le nom ainsi que ca catégorie ici "Web Application Attack". Suricata de s'arrête pas seulement a ces informations la, nous pouvons voir aussi quel protocole a été utilisé, quel type de transport (tcp/udp), l'heure, le lieu et bien d'autres...