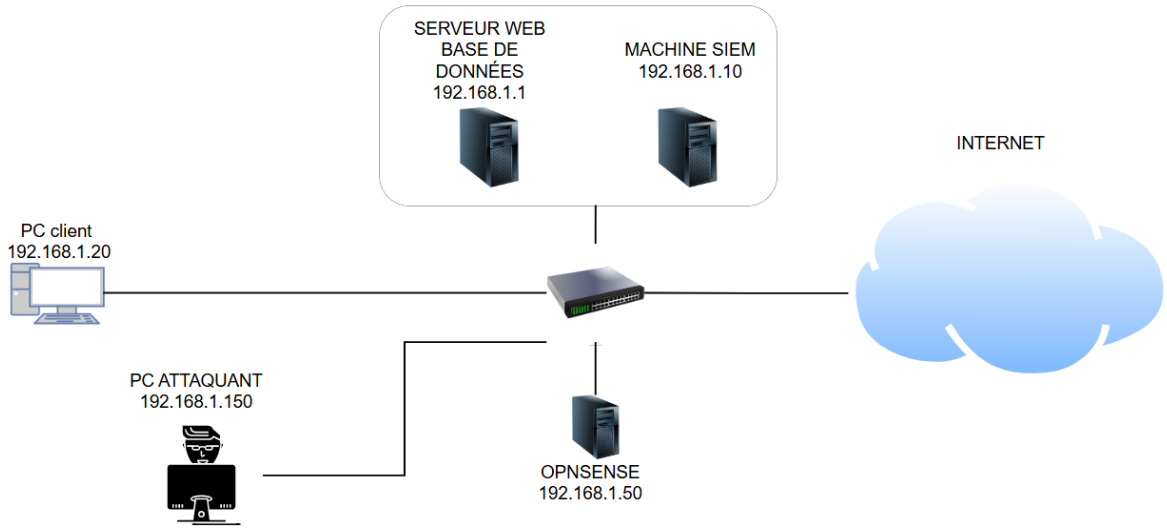
Elmedin SULTANOVIC
Gabin BECU

Dashboard Kibana

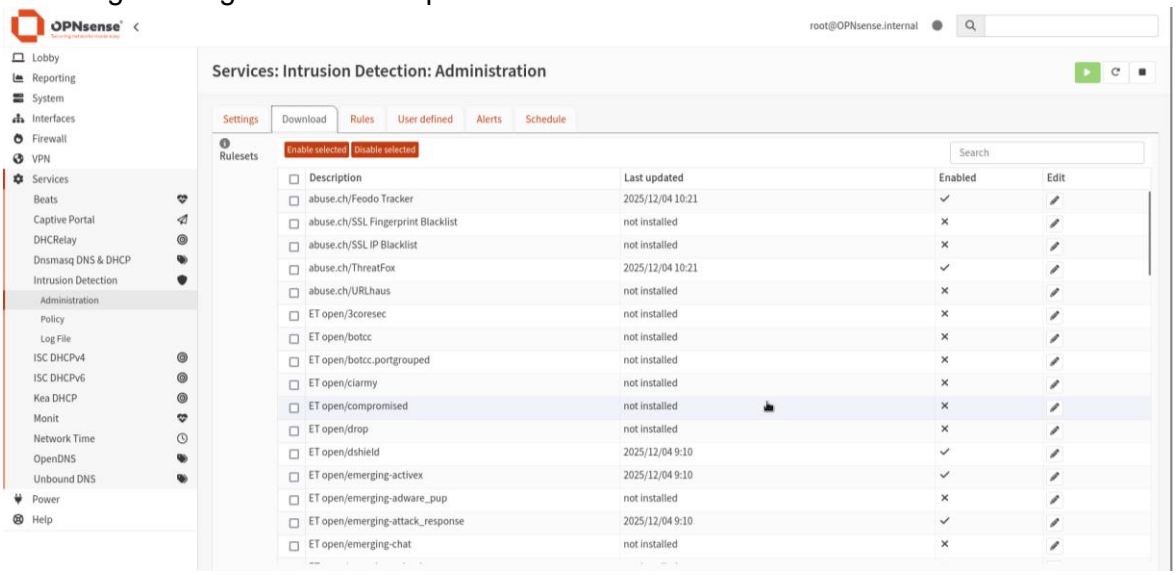
Dans le cadre de ce projet, nous avons mis en place une infrastructure de supervision de la sécurité complète s'appuyant sur un SIEM (ELK Stack) et un IDS/IPS (Suricata). Cette phase finale vise à valider la capacité du système à détecter et corréler différents types d'activités malveillantes simulées à partir d'une machine attaquante. Les tests réalisés couvrent des scénarios d'intrusion classiques : scans réseau, tentatives de brute-force…

Petite mise en contexte rapide de notre réseaux grâce au schéma :

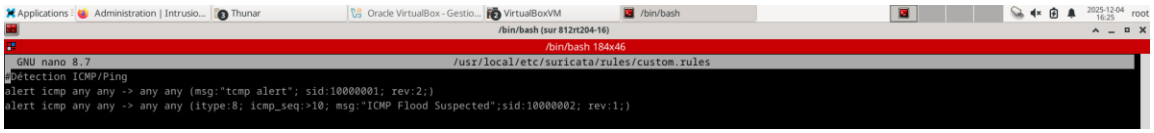


Dans ce livrable nous allons vous présenter, les résultats des tests d'attaques menées

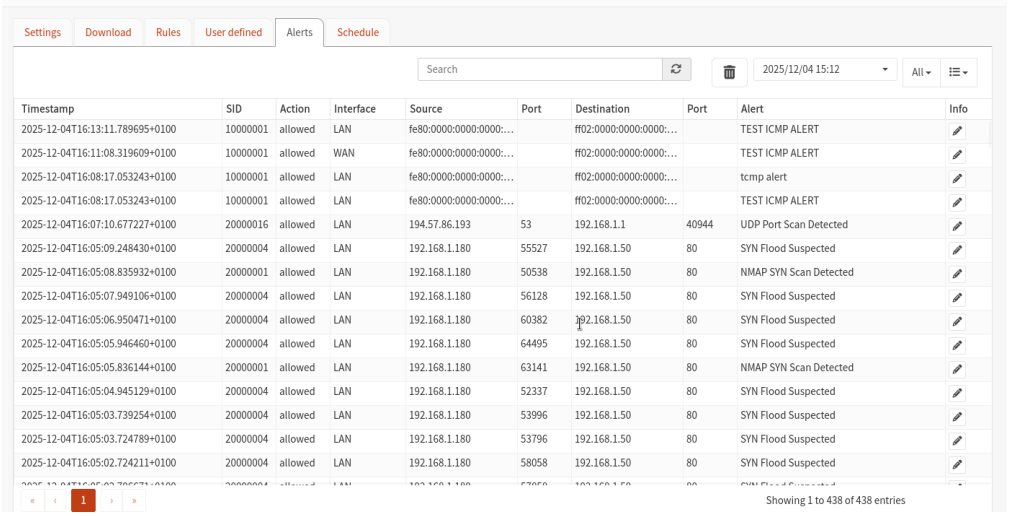
Pour détecter ces attaques on s'est reposé sur les alertes OPNsense nous avons d'abord téléchargé les règles de bases open source



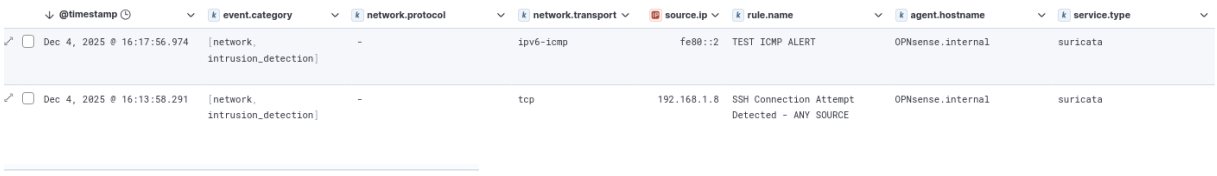
Puis par la suite nous avons créé nos propre règles afin de pouvoir maitriser parfaitement la sévérité des règles et faciliter nos test.

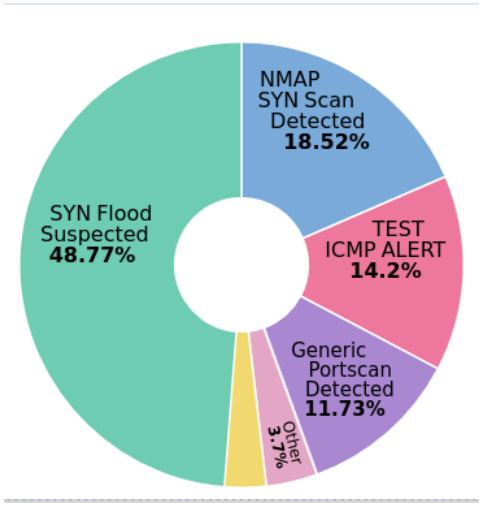


Pour commencer nous avons utiliser une alerte la plus simple possible qui détectaient les ping et qui envoyait une alerte. Cette alerte on pouvait la visualiser de deux manière la première directement dans l'interface d'OPNsense dans l'onglet « Alerts »



Et la deuxième dans Elastic qui facilite sous formes d'une log qu'on pouvait ensuite traiter avec un Dashboard par exemple





Après un résultats concluant on a utilisé le même protocoles de test pour plusieurs attaques :

Le SSH brutforce on a donc crée un script qui envoyait de nombreuse connexion.
Et on recevait bien une alerte :

2025-12-04T14:35:24.794069+0100	20000005	allowed	LAN	192.168.1.8	53800	192.168.1.50	22	SSH Brute Force Attempt

On a ensuite voulu détecter les scan NMAP.
on a donc crée un règle

```
alert tcp any any -> $HOME_NET any (flags:S; threshold:type both, track by_src, count 12, seconds 3; msg:"NMAP SYN Scan Detected"; sid:20000001; rev:1;)
```

et fait un scan nmap qui envoyait bien une alerte

2025-12-04T16:05:05.836144+0100	20000001	allowed	LAN	192.168.1.180	63141	192.168.1.50	80	NMAP SYN Scan Detected

On avais aussi un cas de scan de port UDP qu'on a su détecter

```
alert udp any any -> $HOME_NET any (threshold:type both, track by_src, count 25, seconds 5; msg:"UDP Port Scan Detected"; sid:20000016; rev:1;)
```

Dec 4, 2025 @ 16:07:10.677	[network, intrusion_detection]	dns	udp	194.57.86.193	UDP Port Scan Detected	OPNsense.internal	suricata

Pour finir on a voulu détecter les attaques flood on a commencé par détecter les attaques SYN flood qui est l'attaque flood de base on a donc une fois de plus crée une règle qui le détecte pour les attaques flood SYN. Puis on a aussi fait les attaques flood UDP avec *hping3 --flood --udp -p 53 192.168.1.50*

```
#SYN Flood
alert tcp any any -> $HOME_NET any (flags:S; threshold:type both, track by_src, count 200, seconds 1; msg:"SYN Flood Suspected"; sid:20000004; rev:1;)
```

Dec 4, 2025 @ 16:05:09.248	[network, intrusion_detection]	-	tcp	192.168.1.180	SYN Flood Suspected	OPNsense.internal	suricata

Les multiples tests d'attaque réalisés ont permis de valider le bon fonctionnement de notre système de supervision puisque les scans, les tentatives de brute-force et les attaques par flood ont tous été correctement détectés et remontés par Suricata puis visualisés dans ELK. Les règles, qu'elles soient open-source ou personnalisées, ont permis d'assurer une détection fiable et en adéquation avec les scénarios testés.