"Elastic Security"

Jean-Marc Pouchoulon

octobre 2023

Elastic security est une suite de sécurité qui permet de collecter des logs, de les analyser et de les visualiser. La suite est libre sauf pour certaines fonctionnalités avancées comme le "machine learning" et intègre des dashboards sécurité. Les logs sont collectées dans le but de permettre la détection d'intrusion à l'aide de règles fournies par Elastic ou par la communauté. et vos propres règles.

1 Mise en place d'un environnement Elastic Security

Faire un "git clone `https://github.com/pushou/siem.git`" afin d'installer "elastic SIEM" , l'IDS "Suricata", Evebox, et Zeek. La configuration nécessaire est musclée et une machine avec 16go de Ram est un minimum. Vous obtiendrez de l'aide en lançant la commande "make help". Modifiez le fichier /etc/sysctl.conf

```
vm.max_map_count=262144
```

Puis

```
systctl -p
```

Vous lancerez les commandes suivantes pour installer les différents composants.

```
make es
make siem
make fleet
```

"make pass" vous permettra de visualiser le mot de passe pour l'utilisateur "elastic" qui est le super utilisateur de la suite.

Vous pouvez vous connecter à l'interface web de la suite à l'adresse `http://ip_de_votre_machine:5601` avec le compte "elastic" et le mot de passe obtenu précédemment.

2 Installation de l'agent Elastic sur un poste Windows et Linux