

Intégration des IDS réseau - Suricata

Wazuh s'intègre à un système de détection d'intrusion basé sur le réseau (**NIDS**) pour améliorer la détection des menaces en surveillant le trafic réseau.

Dans ce cas d'utilisation, nous expliquons comment intégrer **Suricata** à **Wazuh**. **Suricata** enrichit la surveillance du trafic réseau en fournissant des informations supplémentaires sur la sécurité de votre infrastructure grâce à ses fonctionnalités avancées d'inspection du trafic réseau.

I – Configuration du point de terminaison Ubuntu

1. Installation de **Suricata** :

- On exécute les commandes suivantes pour installer **Suricata** sur le point de terminaison **Ubuntu** :

```
sudo add-apt-repository ppa:oisf/suricata-stable
sudo apt-get update
sudo apt-get install suricata -y
```

2. On télécharge et on extrait les règles **Emerging Threats Suricata** :

```
cd /tmp/ && curl -LO https://rules.emergingthreats.net/open/suricata-6.0.8/emerging.rules.tar.gz
sudo tar -xvzf emerging.rules.tar.gz
```

3. On se déplace dans **/etc/suricata/** et on crée le répertoire **rules** :

```
cd
cd /etc/suricata
mkdir rules
```

4. On retourne dans le répertoire **/tmp**, on déplace toutes les règles dans le répertoire précédemment créée, puis on donne les droits nécessaires au répertoire et aux règles :

```
cd /tmp
sudo mv rules/*.rules /etc/suricata/rules/
sudo chmod 640 /etc/suricata/rules/*.rules
```

5. On modifie le fichier de configuration **/etc/suricata/suricata.yaml** pour définir les variables suivantes :

```
HOME_NET: "<UBUNTU_IP>"
EXTERNAL_NET: "any"

default-rule-path: /etc/suricata/rules
rule-files:
  - "*.rules"

# Global stats configuration
stats:
  enabled: no

# Linux high speed capture support
af-packet:
  - interface: enp0s3
```

Note : On peut commenter les variables de bases et ajouter les nouvelles en cas d'erreur, on pourra les décommenter et commenter celles ajoutées.

6. On redémarre le service **Suricata** :

```
sudo systemctl restart suricata
```

Intégration des IDS réseau - Suricata

II – Configuration de l'agent Wazuh

1. On ajoute les lignes suivantes au fichier de configuration `/var/ossec/etc/ossec.conf` de l'agent **Wazuh** :

```
<ossec_config>
<localfile>
  <log_format>json</log_format>
  <location>/var/log/suricata/eve.json</location>
</localfile>
</ossec_config>
```

2. On redémarre l'agent **Wazuh** :

```
sudo systemctl restart wazuh-agent
```

II – Émulation de l'attaque

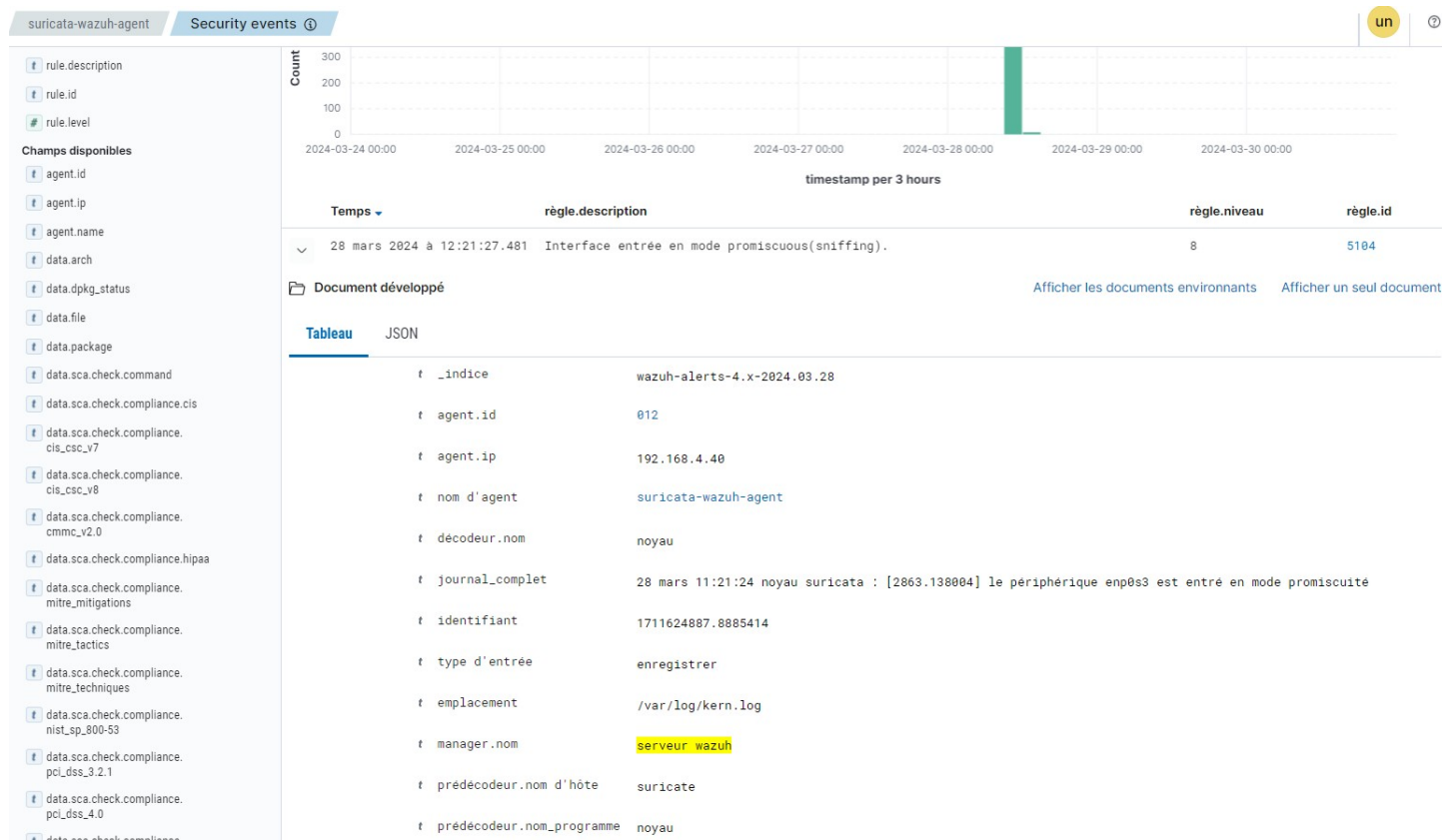
1. On ping l'adresse IP du point de terminaison Ubuntu :

- On utilise la commande ping pour simuler une activité réseau depuis le serveur **Wazuh** :

```
ping -c 20 "<UBUNTU_IP>"
```

2. On visualise les alertes :

- On accède au tableau de bord **Wazuh** et consultez les alertes générées dans le module « **Security Events** » (en utilisant les filtres appropriés = facultatif).



The screenshot shows the Wazuh Security Events dashboard. On the left, there's a sidebar with a search bar and a list of available fields for filtering. The main area displays a bar chart at the top showing the count of events over time. Below the chart, a table lists the security events. The first event is highlighted, showing details for a rule triggered on March 28, 2024, at 12:21:27.481. The rule description is 'Interface entrée en mode promiscuous(sniffing)'. The event is associated with agent ID 012, IP 192.168.4.40, and is categorized as a 'sniffing' event. The event details table below shows various attributes like _indice, agent.id, agent.ip, nom d'agent, decodeur.nom, journal_complet, identifiant, type d'entrée, emplacement, manager.nom (highlighted as 'serveur_wazuh'), précodeur.nom d'hôte, and précodeur.nom_programme.

Timestamp	Rule Description	Rule Level	Rule ID
28 mars 2024 à 12:21:27.481	Interface entrée en mode promiscuous(sniffing).	8	5104

Document développé

Afficher les documents environnants Afficher un seul document

Tableau JSON

Field	Value
_indice	wazuh-alerts-4.x-2024.03.28
agent.id	012
agent.ip	192.168.4.40
nom d'agent	suricata-wazuh-agent
décodeur.nom	noyau
journal_complet	28 mars 11:21:24 noyau suricata : [2863.138004] le périphérique enp0s3 est entré en mode promiscuité
identifiant	1711624887.8885414
type d'entrée	enregistrer
emplacement	/var/log/kern.log
manager.nom	serveur_wazuh
précodeur.nom d'hôte	suricata
précodeur.nom_programme	noyau

Alerte Wazuh : Activation du mode promiscuous (sniffing) sur l'interface enp0s3

Intégration des IDS réseau - Suricata

Quelques erreurs peuvent survenir lorsqu'on regarde le statut de Suricata avec systemctl :

- suricata.service: Failed with result 'exit-code'
- suricata.service: Found left-over process 19318 (Suricata-Main) in control group while starting unit. Ignoring./
- This usually indicates unclean termination of a previous run, or service implementation deficiencies.
- suricata.service: Found left-over process 19394 (Suricata-Main) in control group while starting unit. Ignoring.
- This usually indicates unclean termination of a previous run, or service implementation deficiencies.

Pour cela, il faut arrêter manuellement les processus **Suricata** en cours d'exécution (lors que la commande **ps -aux | grep suricata** et **kill PID**) et supprimer les fichiers PID restants dans le répertoire **/var/run/suricata.pid** puis de redémarrer **Suricata**.

Il ne doit y avoir que cette ligne :

```
root@suricata:~# ps -aux | grep suricata
root    19603  0.0  0.1  6612 2324 pts/4    S+   12:05   0:00 grep --color=auto suricata
```