

# Détection des processus non autorisés avec Wazuh

La fonctionnalité de surveillance des commandes **Wazuh** permet d'exécuter des commandes sur un point de terminaison et de surveiller les résultats.

#### I – Configuration du point de terminaison Linux

1. On ajoute le bloc de configuration suivant au fichier /var/ossec/etc/ossec.conf de l'agent Wazuh pour obtenir périodiquement une liste des processus en cours d'exécution :

```
<ossec_config>
<localfile>
  <log_format>full_command</log_format>
    <alias>process list</alias>
    <command>ps -e -o pid,uname,command>
    <frequency>30</frequency>
  </localfile>
</ossec_config>
```

2. On redémarre l'agent Wazuh pour appliquer les modifications :

systemctl restart wazuh-agent

#### II - Configuration du serveur Wazuh

1. On ajoute les règles suivantes au fichier /var/ossec/etc/rules/local\_rules.xml sur le serveur Wazuh :

```
<group name="ossec,">
<rule id="100050" level="0">
<if_sid>530</if_sid>
<match>^ossec: output: 'process list'</match>
<description>Liste des processus en cours d'exécution.</description>
<group>process_monitor,</group>
</rule>

<rule id="100051" level="7" ignore="900">
<if_sid>100050</if_sid>
<match>nc -l</match>
<description>Netcat à l'écoute de connexions entrantes.</description>
<group>process_monitor,</group>
</rule>
</group>
```

2. On redémarre le gestionnaire **Wazuh** pour appliquer les modifications :

.sudo systemctl restart wazuh-manager

### Test : Émulation d'Attaque

1. Sur le point de terminaison Linux surveillé, on exécute la commande suivante pendant 30 secondes :

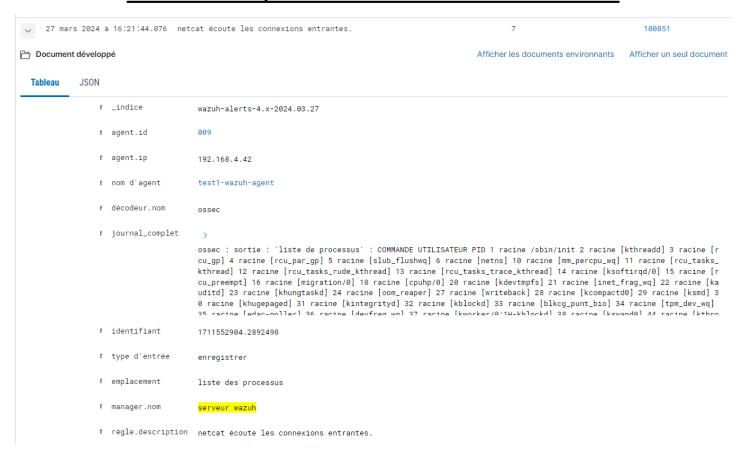
nc -I 8000

2. On visualise les données d'alerte dans le tableau de bord **Wazuh** en accédant au module « **Security Events** ».

AIST 21 Clément MASSON PAGES : 1 / 2



## Détection des processus non autorisés avec Wazuh



AIST 21 Clément MASSON PAGES : 2 / 2