Tutorial download suricata

```
sudo add-apt-repository ppa:oisf/suricata-stable

sudo apt-get update

sudo apt-get install suricata -y
```

setelah selesai

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

sudo tar -xvzf emerging.rules.tar.gz && sudo mv rules/*.rules /etc/suricata/rules/

sudo chmod 777 /etc/suricata/rules/*.rules
```

setelah itu akses config dengan

```
sudo nano /etc/suricata/suricata.yaml
```

lalu cari

```
HOME_NET: "<UBUNTU_IP>"

EXTERNAL_NET: "any"


default-rule-path: /etc/suricata/rules

rule-files:

- "*.rules"


stats:

enabled: no


af-packet:

  - interface: enp0s3
```

Sesuaikan interface dengan interface yang digunakan di ubuntu

Lalu

```
sudo systemctl restart suricata
```

kemudian buka config di wazuh agent dengan

```
/var/ossec/etc/ossec.conf
```

Lalu masukkan

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

Setelah itu kita membuat custom rules di suricata

```
sudo nano /etc/suricata/rules/hping-flood.rules
```

jika directory not found silahkan dibuat sendiri

lalu masukkan

```
alert tcp any any -> $HOME_NET any (msg:"SYN Flood Detected"; flags:S; threshold:type both, track by_src, count 100, seconds 1; sid:600010; rev:1;)

alert tcp any any -> $HOME_NET any (msg:"ACK Flood Detected"; flags:A; threshold:type both, track by_src, count 100, seconds 1; sid:600011; rev:1;)

alert udp any any -> $HOME_NET any (msg:"UDP Flood Detected"; threshold:type both, track by_src, count 200, seconds 1; sid:600012; rev:1;)

alert icmp any any -> $HOME_NET any (msg:"ICMP Flood Detected"; itype:8; threshold:type both, track by_src, count 50, seconds 1; sid:600013; rev:1;)

alert ip any any -> $HOME_NET any (msg:"Raw Packet Anomaly (possible hping3)"; id:0; ttl:64; fragbits:D; threshold:type both, track by_src, count 50, seconds 1; sid:600014; rev:1;)
```

check keberhasilan dengan

```
sudo suricata -T -c /etc/suricata/suricata.yaml -v
```

jika ada error cari di internet untuk solusinya kemudian restart kembali suricata

Setelah itu kita costumasikan dengan local_rules di wazuh manager

Buka dengan

```
Sudo nano /var/ossec/etc/rules/local_rules.xml
```

Kemudian tambahkan

```
<rule id="160000" level="3">
  <decoded_as>json</decoded_as>
  <field name="event_type">^alert$</field>
  <description>Suricata generic alert (eve.json)</description>
 </rule>

 <rule id="160001" level="12">
  <if_sid>160000</if_sid>
  <field name="alert.signature">SYN Flood Detected</field>
  <description>Suricata: SYN flood</description>
 </rule>

 <rule id="160002" level="12">
  <if_sid>160000</if_sid>
  <field name="alert.signature">ACK Flood Detected</field>
  <description>Suricata: ACK flood</description>
 </rule>
```

```
<rule id="160003" level="12">
  <if_sid>160000</if_sid>
  <field name="alert.signature">UDP Flood Detected</field>
  <description>Suricata: UDP flood</description>
</rule>

<rule id="160004" level="12">
  <if_sid>160000</if_sid>
  <field name="alert.signature">ICMP Flood Detected</field>
  <description>Suricata: ICMP / ping flood</description>
</rule>
```