ENSIAS

جامعة محمد الخامس بالرباط
Université Mohammed V de Rabat

Projet de fin d'année

SMART IDS

Réalisé par :

AGOULZI Imane

JOUIJATE Rim

Membre de Jury :

M. BERQIA Amine

M. ERRADI Mohamed

Encadré par :

M. BERQIA Amine

Année universitaire 2022-2023

SOMMAIRE

Introduction

01 Système de détection d'intrusion

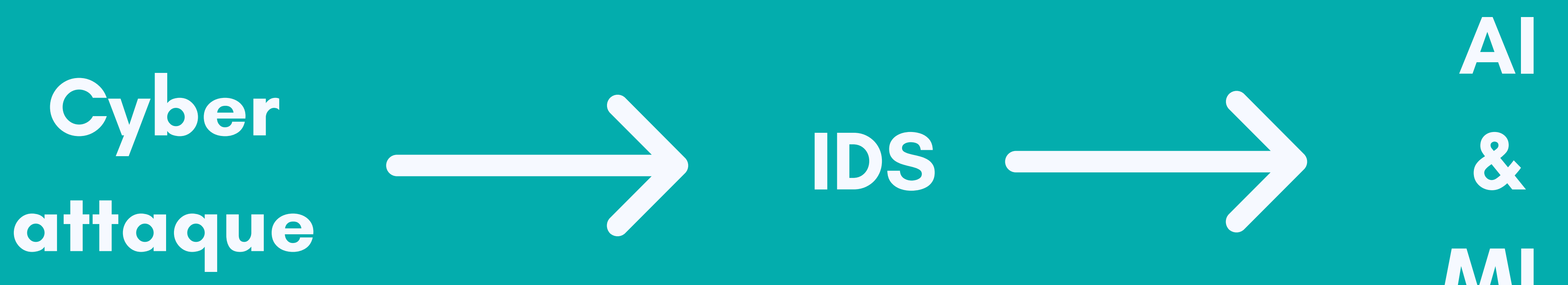
02 Déploiement de suricata au sein de raspberry pi

03 Problème et solution proposée

04 Smart IDS

Conclusion

Introduction



Cyber attaque → IDS → AI & ML

SOMMAIRE

Introduction

01 Système de détection d'intrusion

02 Déploiement de suricata au sein de raspberry pi

03 Problème et solution proposée

04 Smart IDS

Conclusion

Système de détection d'intrusion

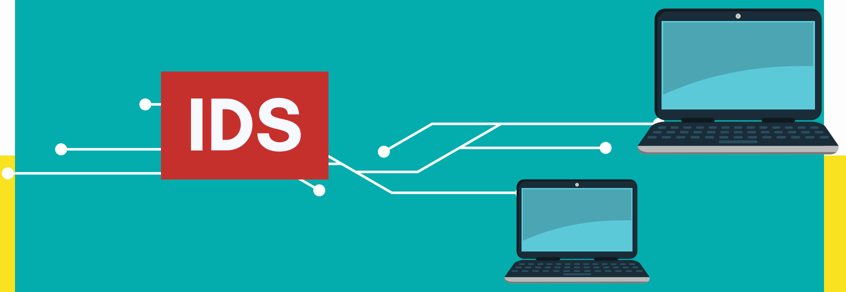
Un système de détection d'intrusion est utilisé pour surveiller les réseaux et les systèmes informatiques, et détecter les activités suspectes ou malveillantes.

Système de détection d'intrusion

TYPES

01 Basé sur des signatures

02 Basé sur des anomalies



03 Basé sur le réseau

04 Basé sur l'hôte

SOMMAIRE

Introduction

01 Système de détection d'intrusion

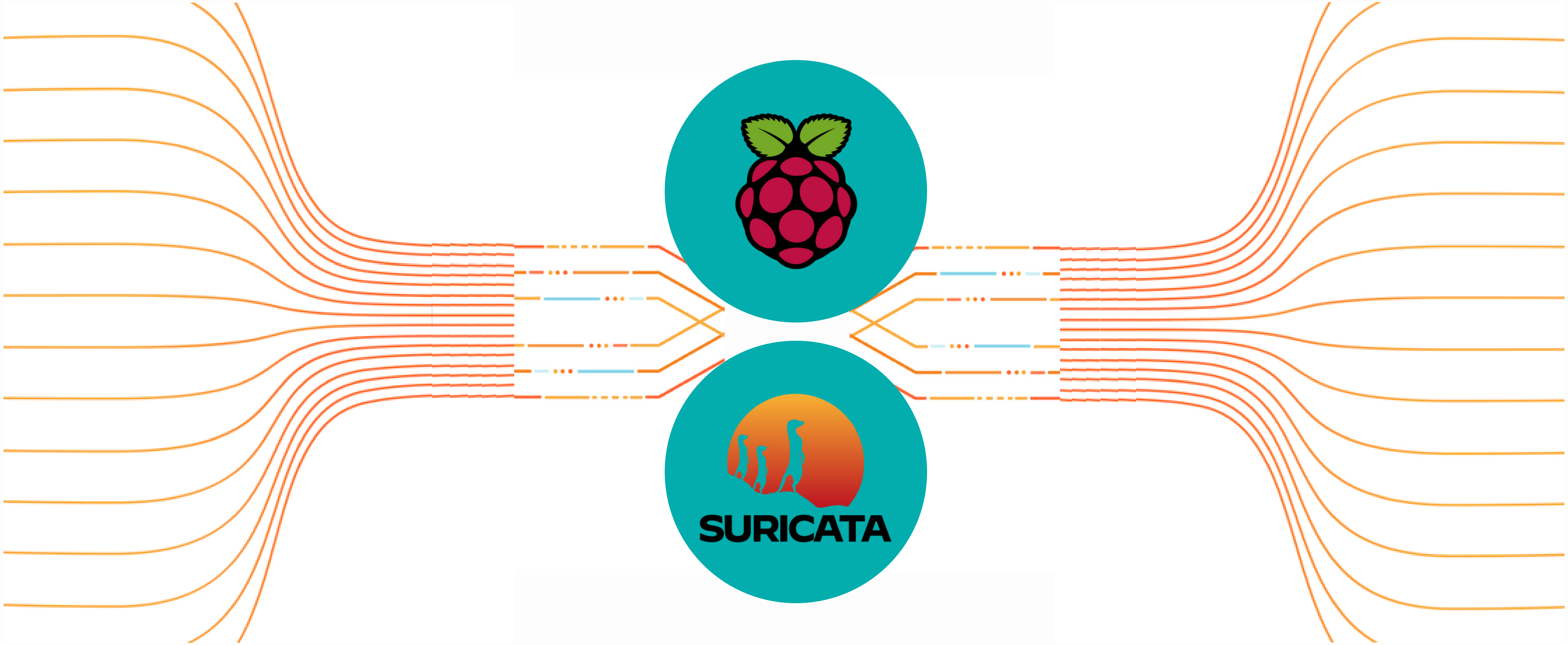
02 **Déploiement de suricata au sein de raspberry pi**

03 Problème et solution proposée

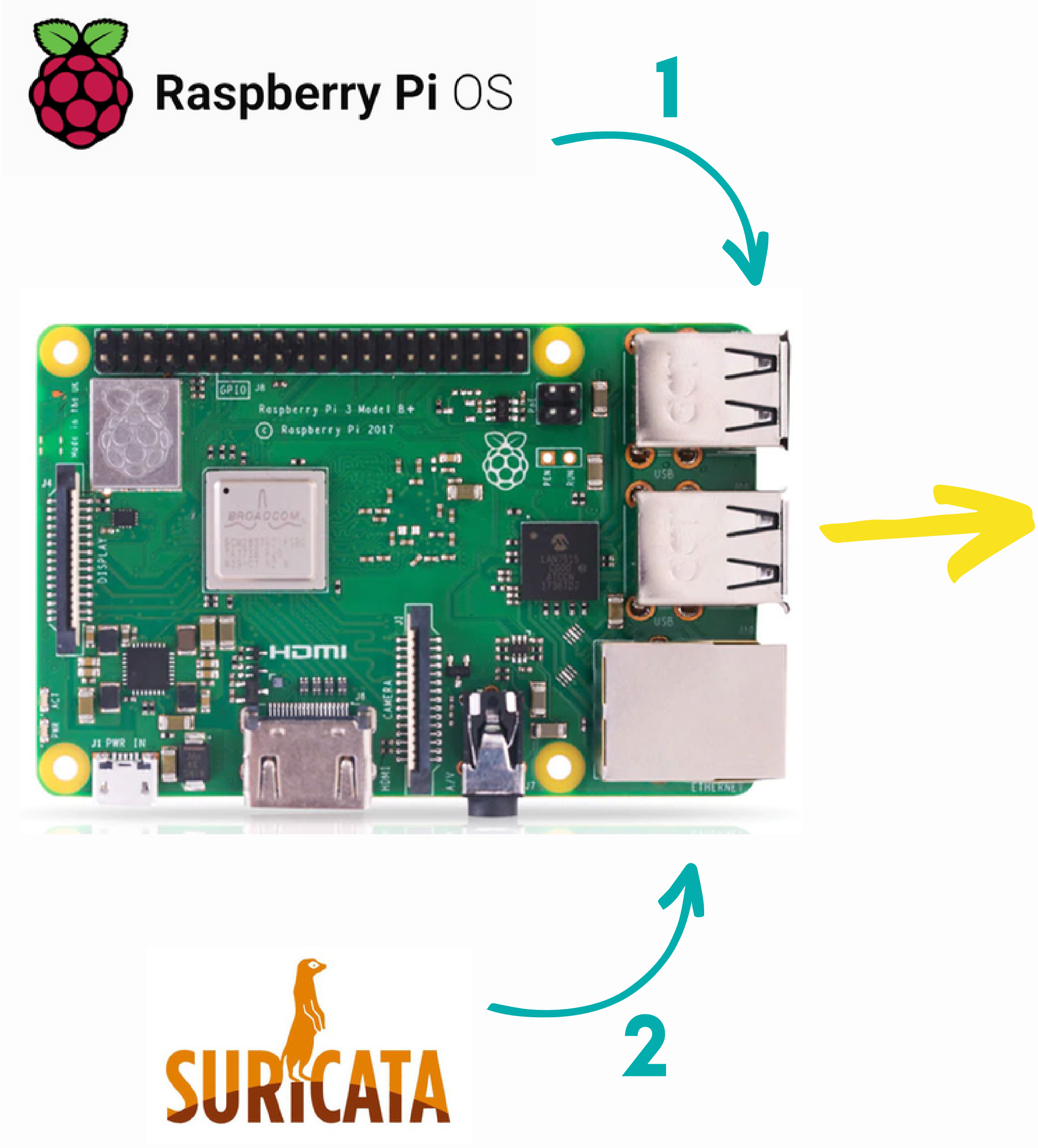
04 Smart IDS

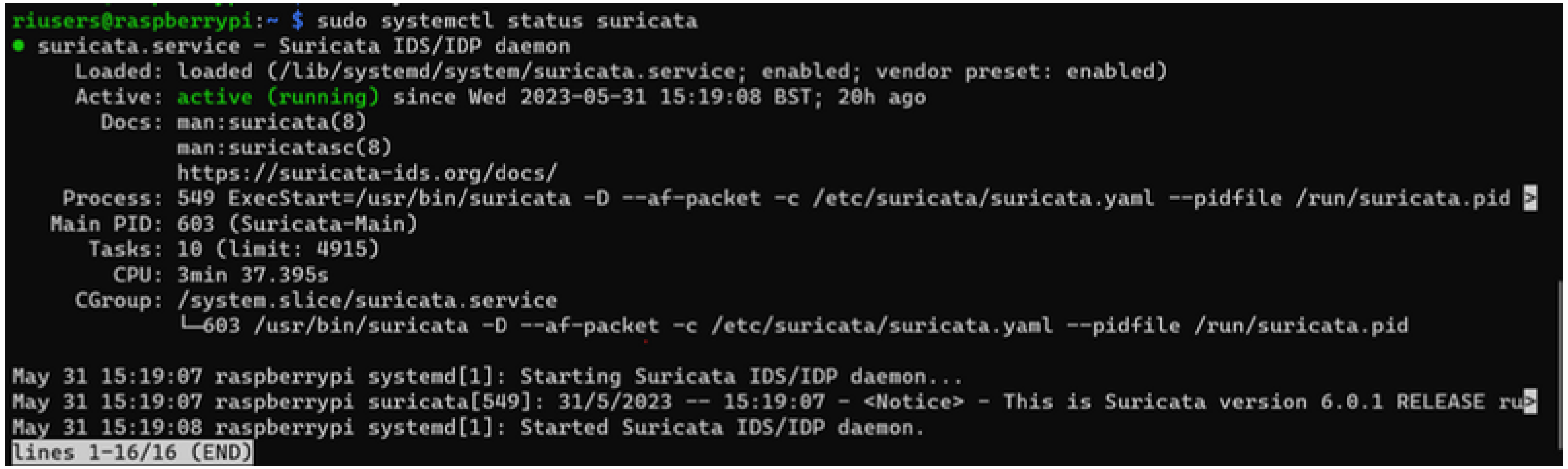
Conclusion

Déploiement de suricata au sein de raspberry pi



Déploiement de suricata au sein de raspberry pi

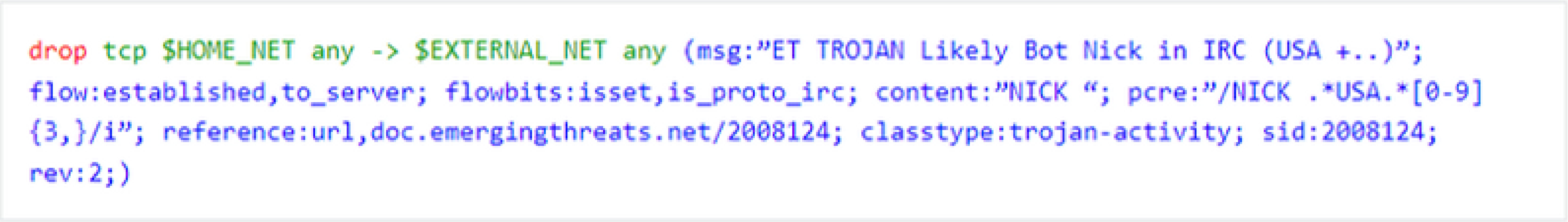




```
riusers@raspberrypi:~ $ sudo systemctl status suricata
● suricata.service - Suricata IDS/IDP daemon
     Loaded: loaded (/lib/systemd/system/suricata.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2023-05-31 15:19:08 BST; 20h ago
       Docs: man:suricata(8)
             man:suricatasc(8)
             https://suricata-ids.org/docs/
    Process: 549 ExecStart=/usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/suricata.pid >
   Main PID: 603 (Suricata-Main)
      Tasks: 10 (limit: 4915)
        CPU: 3min 37.395s
     CGroup: /system.slice/suricata.service
             └─603 /usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/suricata.pid

May 31 15:19:07 raspberrypi systemd[1]: Starting Suricata IDS/IDP daemon...
May 31 15:19:07 raspberrypi suricata[549]: 31/5/2023 -- 15:19:07 - <Notice> - This is Suricata version 6.0.1 RELEASE ru>
May 31 15:19:08 raspberrypi systemd[1]: Started Suricata IDS/IDP daemon.
lines 1-16/16 (END)
```

Déploiement de suricata au sein de raspberry pi

Suricata RULES

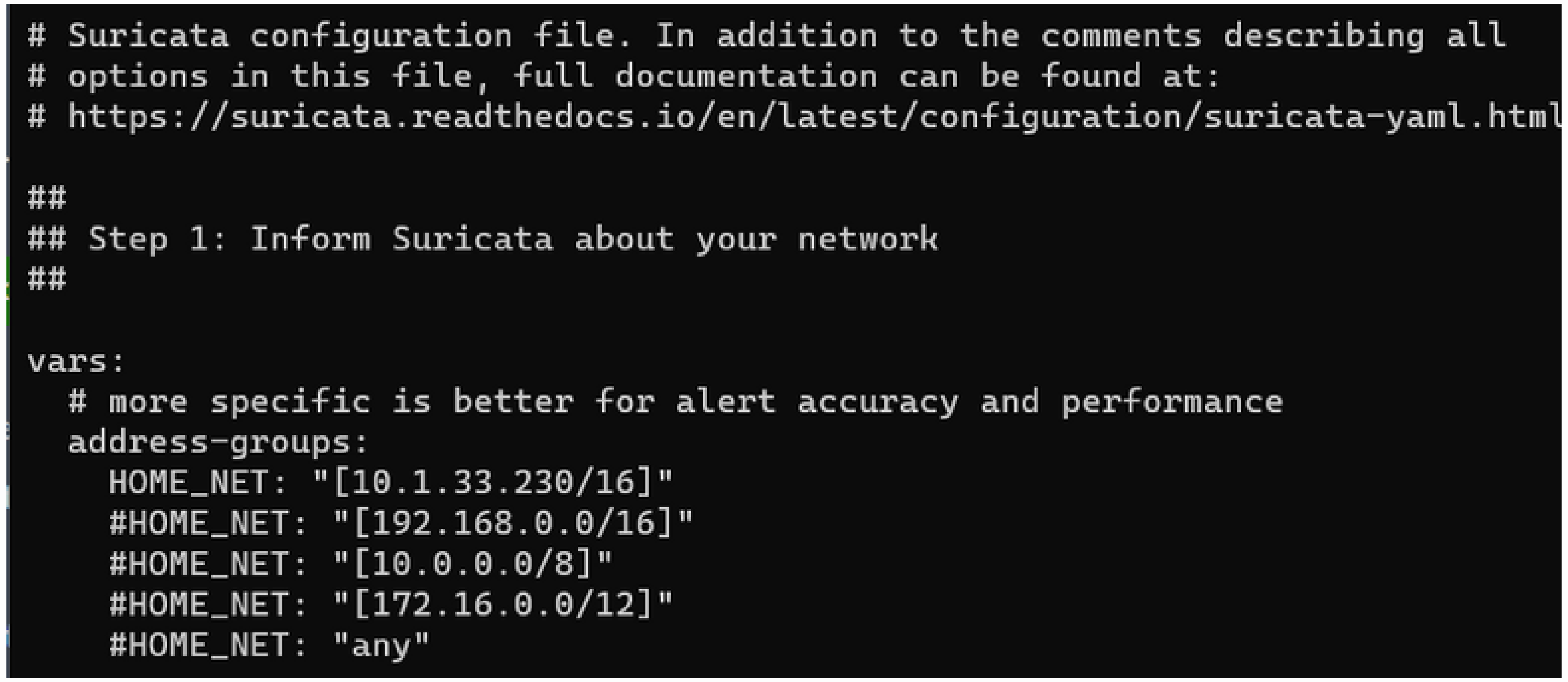


```
drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:”ET TROJAN Likely Bot Nick in IRC (USA +..)”;
flow:established,to_server; flowbits:isset,is_proto_irc; content:”NICK “; pcre:”/NICK .*USA.*[0-9]
{3,}/i”; reference:url,doc.emergingthreats.net/2008124; classtype:trojan-activity; sid:2008124;
rev:2;)
```

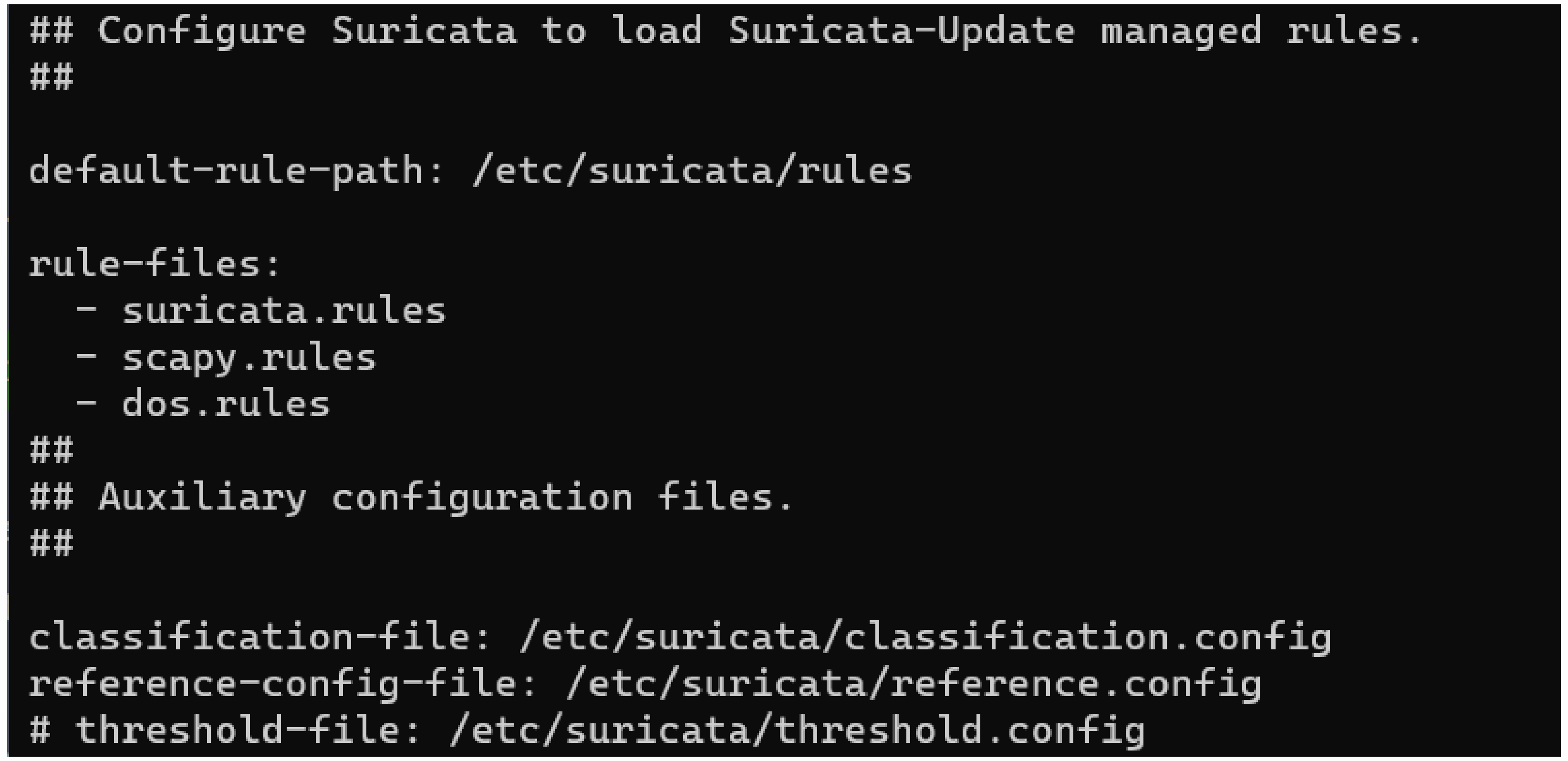
Action Header Options

Déploiement de suricata au sein de raspberry pi

Suricata.yaml



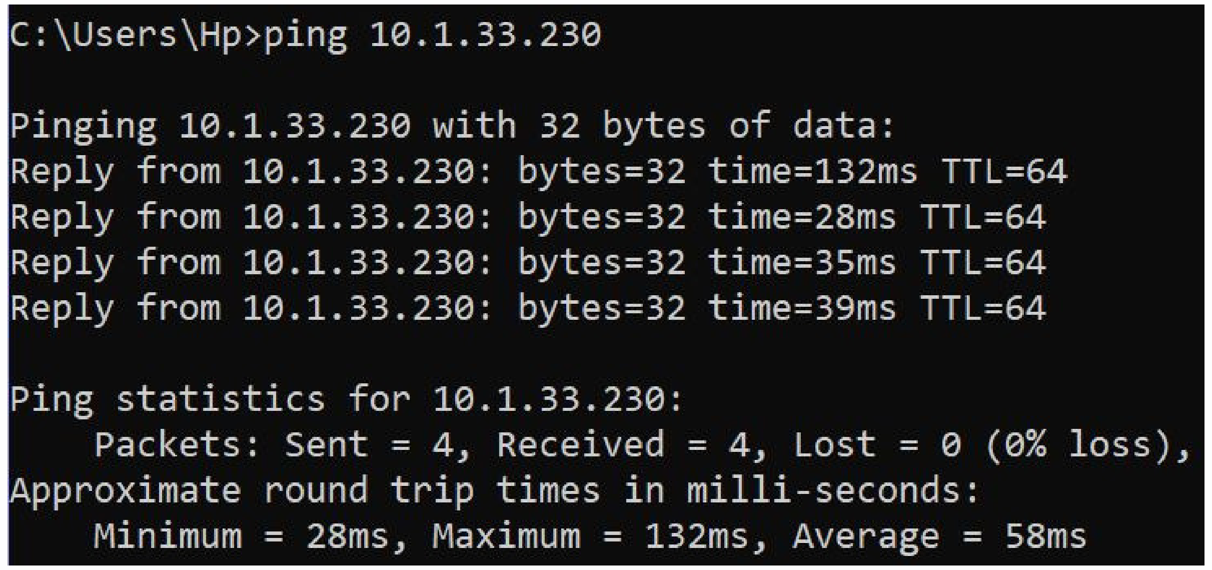
```
# Suricata configuration file. In addition to the comments describing all
# options in this file, full documentation can be found at:
# https://suricata.readthedocs.io/en/latest/configuration/suricata-yaml.html

##
## Step 1: Inform Suricata about your network
##

vars:
  # more specific is better for alert accuracy and performance
  address-groups:
    HOME_NET: "[10.1.33.230/16]"
    #HOME_NET: "[192.168.0.0/16]"
    #HOME_NET: "[10.0.0.0/8]"
    #HOME_NET: "[172.16.0.0/12]"
    #HOME_NET: "any"
```



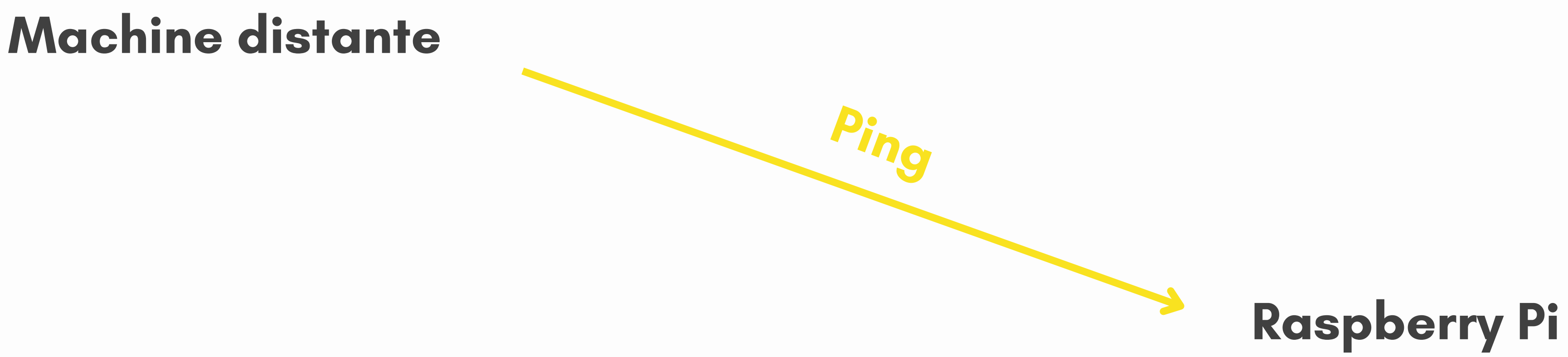
```
## Configure Suricata to load Suricata-Update managed rules.
##

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

rule-files:
  - suricata.rules
  - scapy.rules
  - dos.rules
##
## Auxiliary configuration files.
##

classification-file: /etc/suricata/classification.config
reference-config-file: /etc/suricata/reference.config
# threshold-file: /etc/suricata/threshold.config
```

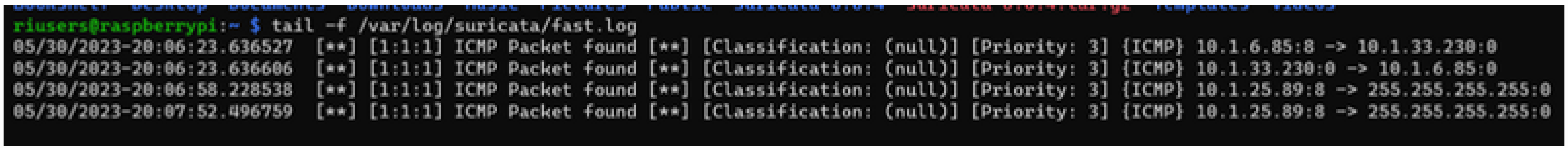
Déploiement de suricata au sein de raspberry pi

Test 1



```
C:\Users\Hp>ping 10.1.33.230

Pinging 10.1.33.230 with 32 bytes of data:
Reply from 10.1.33.230: bytes=32 time=132ms TTL=64
Reply from 10.1.33.230: bytes=32 time=28ms TTL=64
Reply from 10.1.33.230: bytes=32 time=35ms TTL=64
Reply from 10.1.33.230: bytes=32 time=39ms TTL=64

Ping statistics for 10.1.33.230:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 28ms, Maximum = 132ms, Average = 58ms
```





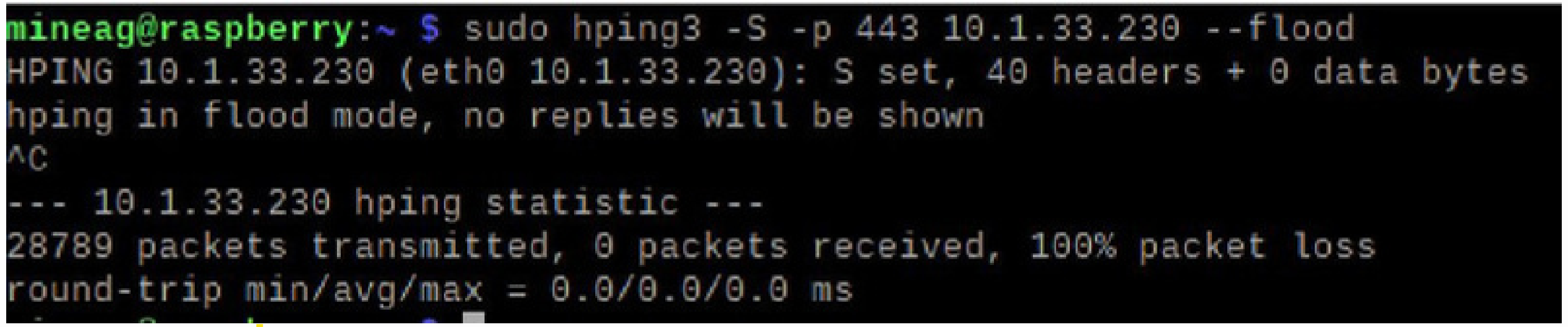
```
riusers@raspberrypi:~ $ tail -f /var/log/suricata/fast.log
05/30/2023-20:06:23.636527  [**] [1:1:1] ICMP Packet found [**] [Classification: (null)] [Priority: 3] {ICMP} 10.1.6.85:8 -> 10.1.33.230:0
05/30/2023-20:06:23.636606  [**] [1:1:1] ICMP Packet found [**] [Classification: (null)] [Priority: 3] {ICMP} 10.1.33.230:0 -> 10.1.6.85:0
05/30/2023-20:06:58.228538  [**] [1:1:1] ICMP Packet found [**] [Classification: (null)] [Priority: 3] {ICMP} 10.1.25.89:8 -> 255.255.255.255:0
05/30/2023-20:07:52.496759  [**] [1:1:1] ICMP Packet found [**] [Classification: (null)] [Priority: 3] {ICMP} 10.1.25.89:8 -> 255.255.255.255:0
```

alert icmp any any -> $HOME_NET any (msg: "ICMP Packet found"; sid:1 ;rev:1;)

Déploiement de suricata au sein de raspberry pi

Test 2

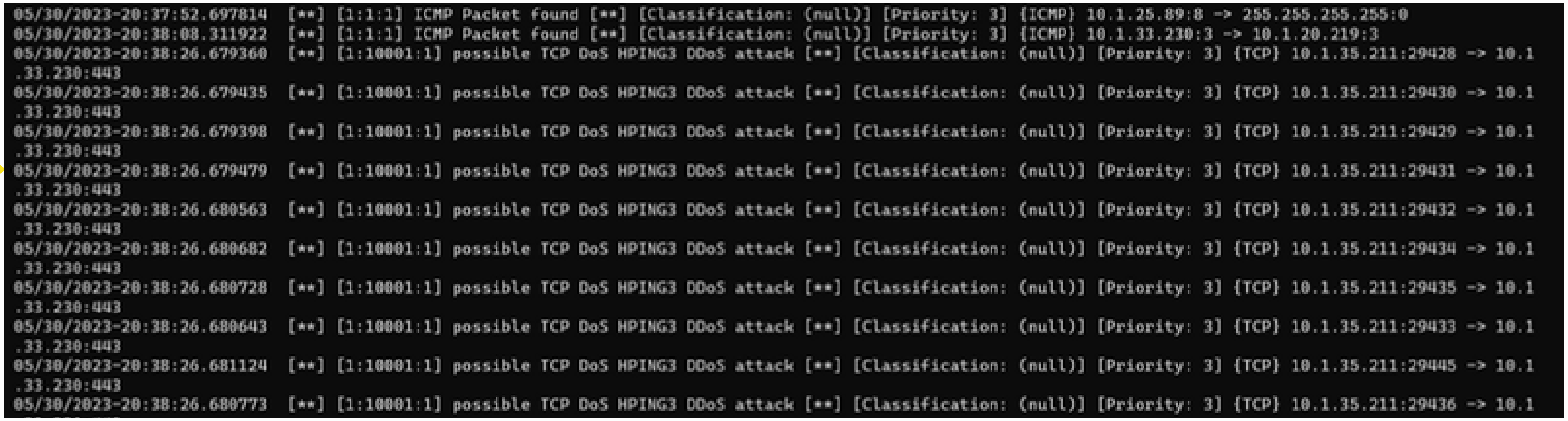
Machine distante



```
mineag@raspberry:~ $ sudo hping3 -S -p 443 10.1.33.230 --flood
HPING 10.1.33.230 (eth0 10.1.33.230): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 10.1.33.230 hping statistic ---
28789 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

DoS

Raspberry Pi

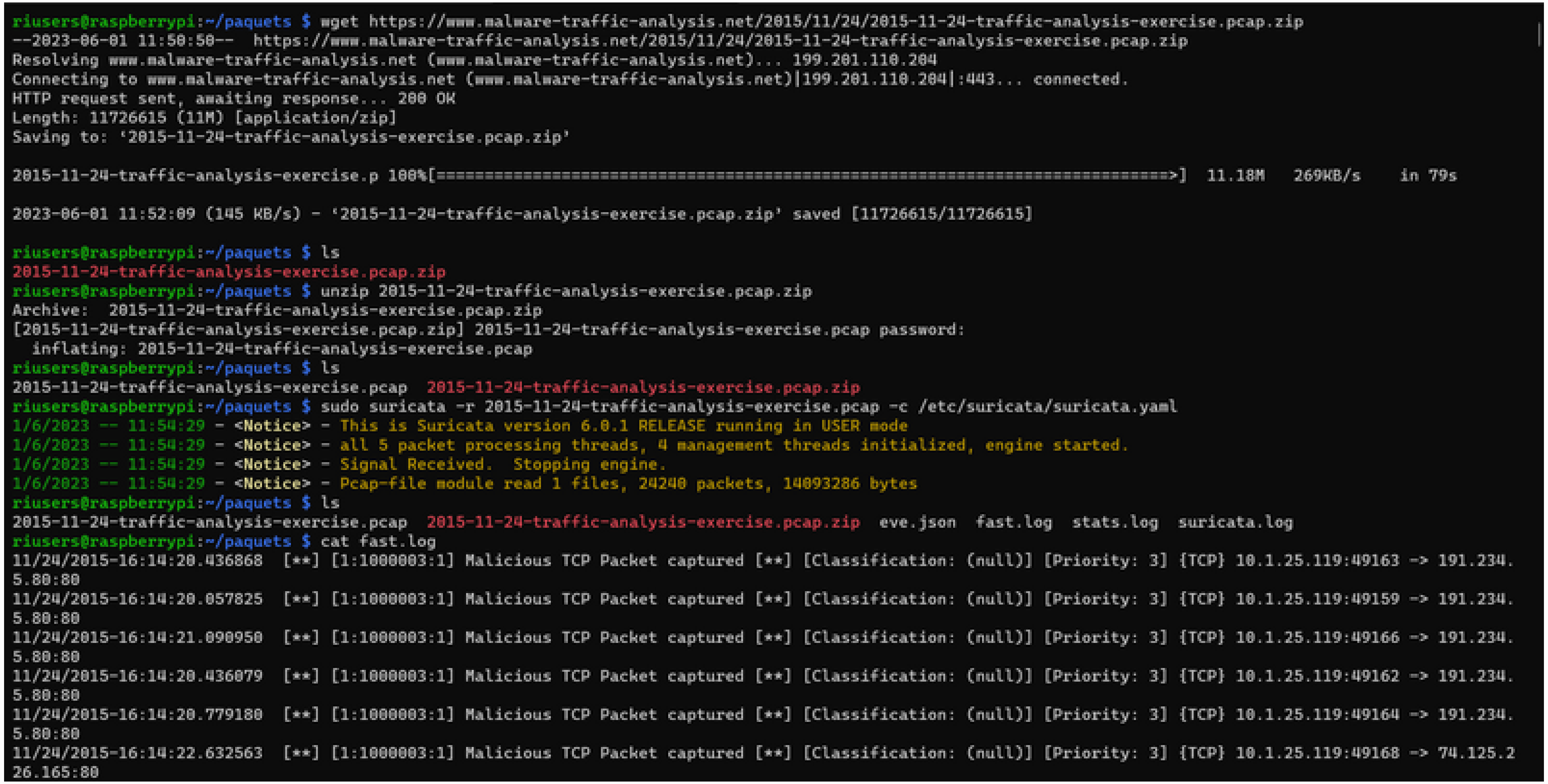


```
05/30/2023-20:37:52.697814  [**] [1:1:1] ICMP Packet found [**] [Classification: (null)] [Priority: 3] {ICMP} 10.1.25.89:8 -> 255.255.255.255:0
05/30/2023-20:38:08.311922  [**] [1:1:1] ICMP Packet found [**] [Classification: (null)] [Priority: 3] {ICMP} 10.1.33.230:3 -> 10.1.20.219:3
05/30/2023-20:38:26.679360  [**] [1:10001:1] possible TCP DoS HPING3 DDoS attack [**] [Classification: (null)] [Priority: 3] {TCP} 10.1.35.211:29428 -> 10.1
.33.230:443
05/30/2023-20:38:26.679435  [**] [1:10001:1] possible TCP DoS HPING3 DDoS attack [**] [Classification: (null)] [Priority: 3] {TCP} 10.1.35.211:29430 -> 10.1
.33.230:443
05/30/2023-20:38:26.679398  [**] [1:10001:1] possible TCP DoS HPING3 DDoS attack [**] [Classification: (null)] [Priority: 3] {TCP} 10.1.35.211:29429 -> 10.1
.33.230:443
05/30/2023-20:38:26.679479  [**] [1:10001:1] possible TCP DoS HPING3 DDoS attack [**] [Classification: (null)] [Priority: 3] {TCP} 10.1.35.211:29431 -> 10.1
.33.230:443
05/30/2023-20:38:26.680563  [**] [1:10001:1] possible TCP DoS HPING3 DDoS attack [**] [Classification: (null)] [Priority: 3] {TCP} 10.1.35.211:29432 -> 10.1
.33.230:443
05/30/2023-20:38:26.680682  [**] [1:10001:1] possible TCP DoS HPING3 DDoS attack [**] [Classification: (null)] [Priority: 3] {TCP} 10.1.35.211:29434 -> 10.1
.33.230:443
05/30/2023-20:38:26.680728  [**] [1:10001:1] possible TCP DoS HPING3 DDoS attack [**] [Classification: (null)] [Priority: 3] {TCP} 10.1.35.211:29435 -> 10.1
.33.230:443
05/30/2023-20:38:26.680643  [**] [1:10001:1] possible TCP DoS HPING3 DDoS attack [**] [Classification: (null)] [Priority: 3] {TCP} 10.1.35.211:29433 -> 10.1
.33.230:443
05/30/2023-20:38:26.681124  [**] [1:10001:1] possible TCP DoS HPING3 DDoS attack [**] [Classification: (null)] [Priority: 3] {TCP} 10.1.35.211:29445 -> 10.1
.33.230:443
05/30/2023-20:38:26.680773  [**] [1:10001:1] possible TCP DoS HPING3 DDoS attack [**] [Classification: (null)] [Priority: 3] {TCP} 10.1.35.211:29436 -> 10.1
```

alert tcp any any -> any any (flags: S; msg: "Possible TCP DoS HPING3 DDoS attack"; flow: stateless; detection_filter: track by_dst, count 100, seconds 5; sid:10001; rev:1;)

Déploiement de suricata au sein de raspberry pi

Test 3



```
riusers@raspberrypi:~/paquets $ wget https://www.malware-traffic-analysis.net/2015/11/24/2015-11-24-traffic-analysis-exercise.pcap.zip
--2023-06-01 11:50:50--  https://www.malware-traffic-analysis.net/2015/11/24/2015-11-24-traffic-analysis-exercise.pcap.zip
Resolving www.malware-traffic-analysis.net (www.malware-traffic-analysis.net)... 199.201.110.204
Connecting to www.malware-traffic-analysis.net (www.malware-traffic-analysis.net)|199.201.110.204|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 11726615 (11M) [application/zip]
Saving to: ‘2015-11-24-traffic-analysis-exercise.pcap.zip’

2015-11-24-traffic-analysis-exercise.p 100%[============================================================================>]  11.18M   269KB/s    in 79s

2023-06-01 11:52:09 (145 KB/s) - ‘2015-11-24-traffic-analysis-exercise.pcap.zip’ saved [11726615/11726615]

riusers@raspberrypi:~/paquets $ ls
2015-11-24-traffic-analysis-exercise.pcap.zip
riusers@raspberrypi:~/paquets $ unzip 2015-11-24-traffic-analysis-exercise.pcap.zip
Archive:  2015-11-24-traffic-analysis-exercise.pcap.zip
[2015-11-24-traffic-analysis-exercise.pcap.zip] 2015-11-24-traffic-analysis-exercise.pcap password:
  inflating: 2015-11-24-traffic-analysis-exercise.pcap
riusers@raspberrypi:~/paquets $ ls
2015-11-24-traffic-analysis-exercise.pcap  2015-11-24-traffic-analysis-exercise.pcap.zip
riusers@raspberrypi:~/paquets $ sudo suricata -r 2015-11-24-traffic-analysis-exercise.pcap -c /etc/suricata/suricata.yaml
1/6/2023 -- 11:54:29 - <Notice> - This is Suricata version 6.0.1 RELEASE running in USER mode
1/6/2023 -- 11:54:29 - <Notice> - all 5 packet processing threads, 4 management threads initialized, engine started.
1/6/2023 -- 11:54:29 - <Notice> - Signal Received.  Stopping engine.
1/6/2023 -- 11:54:29 - <Notice> - Pcap-file module read 1 files, 24240 packets, 14093286 bytes
riusers@raspberrypi:~/paquets $ ls
2015-11-24-traffic-analysis-exercise.pcap  2015-11-24-traffic-analysis-exercise.pcap.zip  eve.json  fast.log  stats.log  suricata.log
riusers@raspberrypi:~/paquets $ cat fast.log
11/24/2015-16:14:20.436868  [**] [1:1000003:1] Malicious TCP Packet captured [**] [Classification: (null)] [Priority: 3] {TCP} 10.1.25.119:49163 -> 191.234.
5.80:80
11/24/2015-16:14:20.057825  [**] [1:1000003:1] Malicious TCP Packet captured [**] [Classification: (null)] [Priority: 3] {TCP} 10.1.25.119:49159 -> 191.234.
5.80:80
11/24/2015-16:14:21.090950  [**] [1:1000003:1] Malicious TCP Packet captured [**] [Classification: (null)] [Priority: 3] {TCP} 10.1.25.119:49166 -> 191.234.
5.80:80
11/24/2015-16:14:20.436079  [**] [1:1000003:1] Malicious TCP Packet captured [**] [Classification: (null)] [Priority: 3] {TCP} 10.1.25.119:49162 -> 191.234.
5.80:80
11/24/2015-16:14:20.779180  [**] [1:1000003:1] Malicious TCP Packet captured [**] [Classification: (null)] [Priority: 3] {TCP} 10.1.25.119:49164 -> 191.234.
5.80:80
11/24/2015-16:14:22.632563  [**] [1:1000003:1] Malicious TCP Packet captured [**] [Classification: (null)] [Priority: 3] {TCP} 10.1.25.119:49168 -> 74.125.2
26.165:80
```

SOMMAIRE

Introduction

01 Système de détection d'intrusion

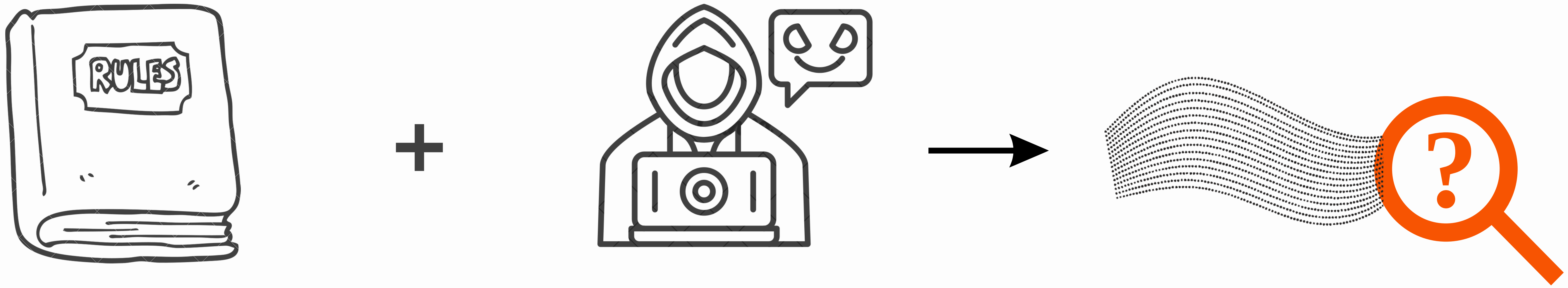
02 Déploiement de suricata au sein de raspberry pi

03 Problème et solution proposée

04 Smart IDS

Conclusion

Problématique



IDS basé sur les signatures

Nouvelles attaques

Problématique

IDS basé sur les signatures

Nouvelles attaques

Solution : IDS **Hybride**

SOMMAIRE

Introduction

01 Système de détection d'intrusion

02 Déploiement de suricata au sein de raspberry pi

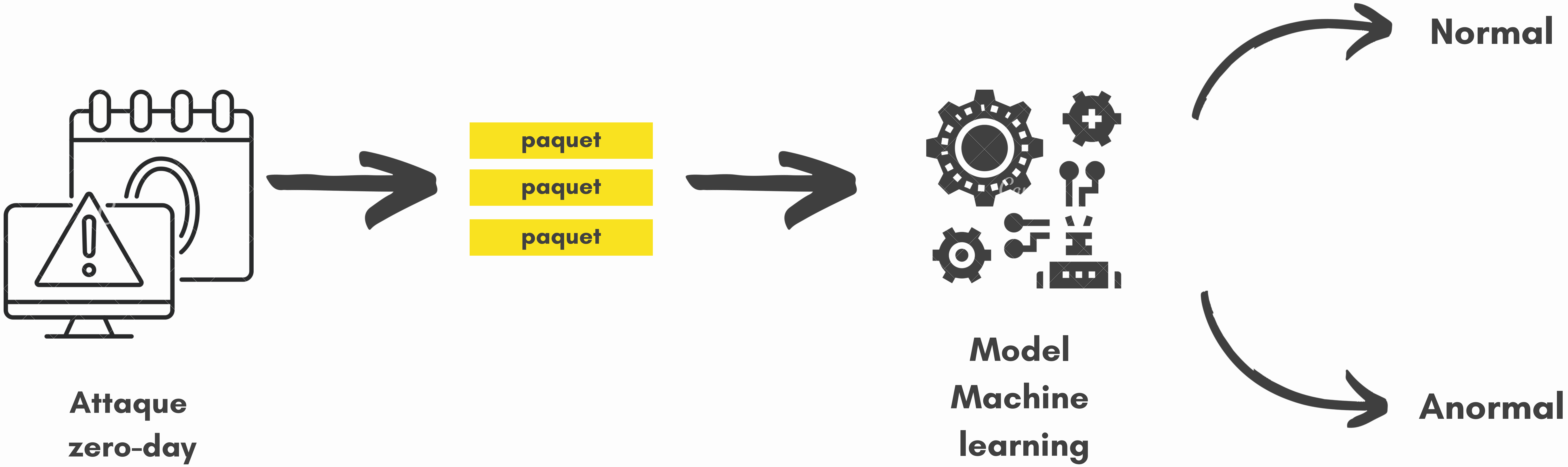
03 Problème et solution proposée

04 Smart IDS

Conclusion

IDS basé sur anomalies

Principe



Attaque zero-day

paquet

paquet

paquet

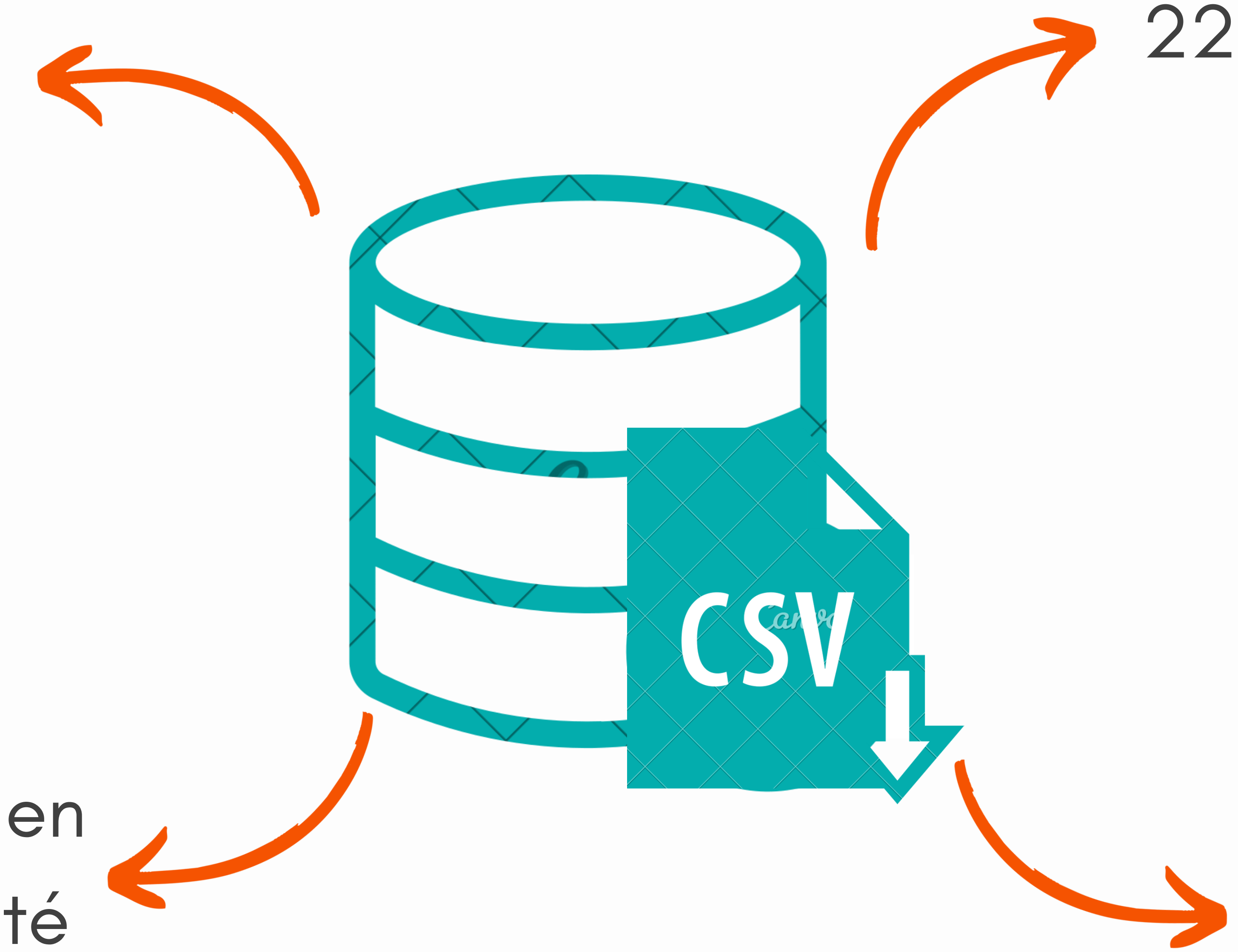
Model Machine learning

Normal

Anormal

IDS basé sur anomalies

Dataset



CICIDS2017

2214468 enregistrements

l'institut canadien
de cybersécurité

79 attributs

IDS basé sur anomalies

préparation de données

Les variables corrélées

Éléminer 46 attributs fortement corrélés

Les valeurs manquantes

Remplacées par la moyenne

Les valeurs redondantes

supprimer les enregistrements dupliqués

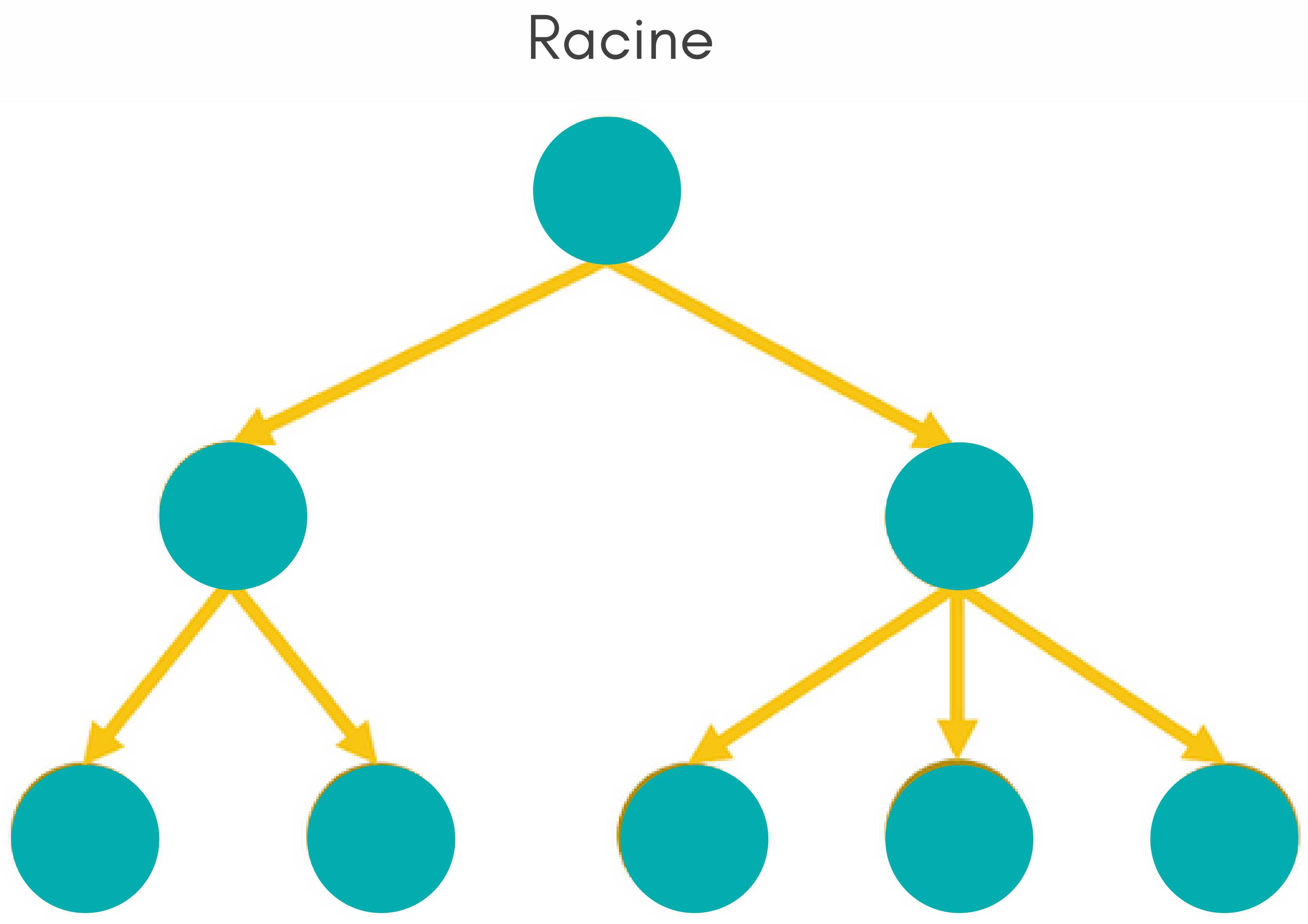
Equilibrage de jeu de données

Utilisation de "Undersampling"

IDS basé sur anomalies

Entrainement de modèle

Algorithme de Machine Learning :
Arbre de décision



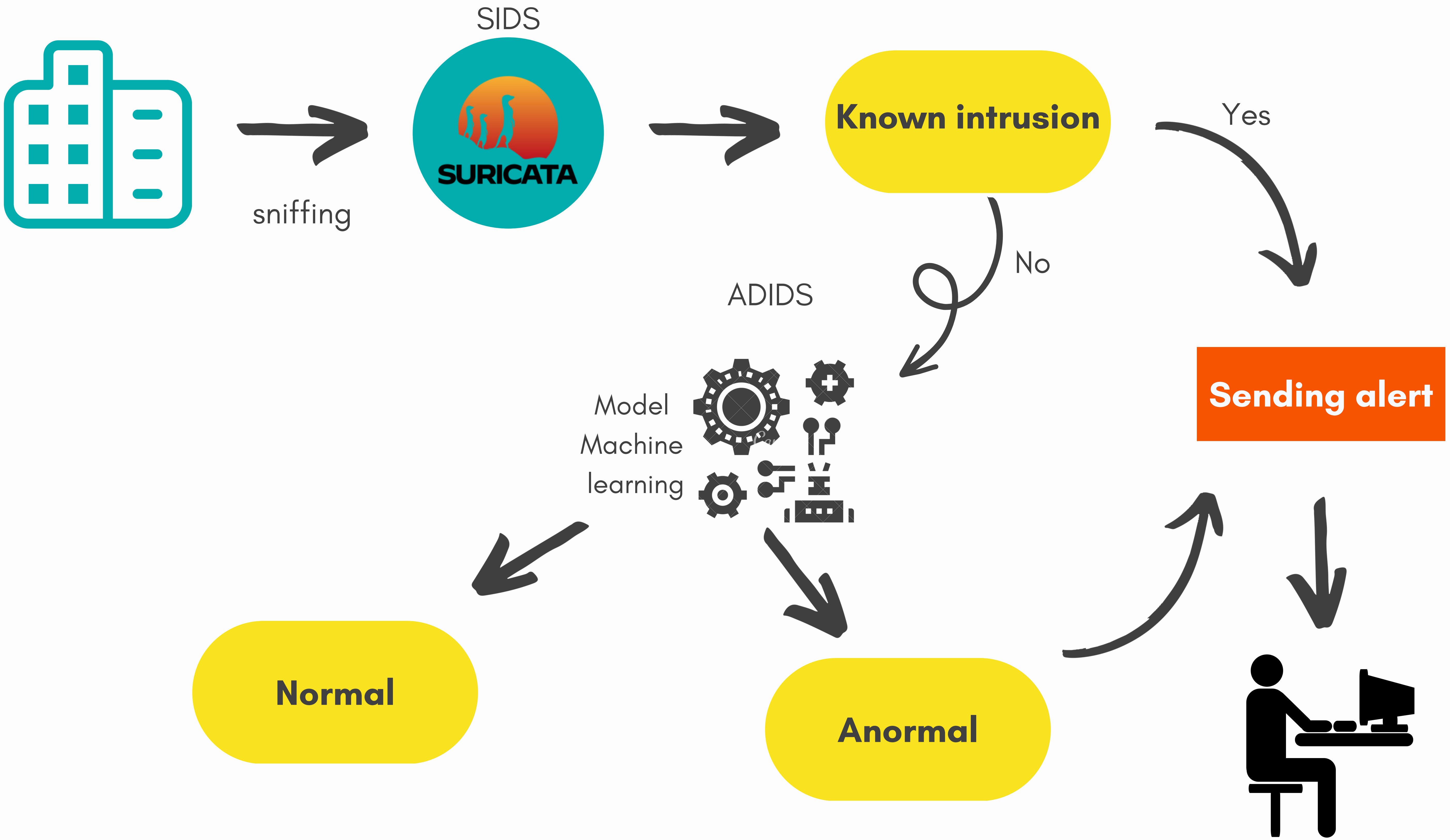
IDS basé sur anomalies

Evaluation de modèle

Performance de modèle

Accuracy	Precision	Recall	F1-score
99,8%	99,6%	99,6%	99,6%

Combinaison de Suriata et le modèle réalisé



Conclusion

MERCI POUR VOTRE ATTENTION