



SÉCURITÉ D'UN RASPBERRY PI

Réalisé par :

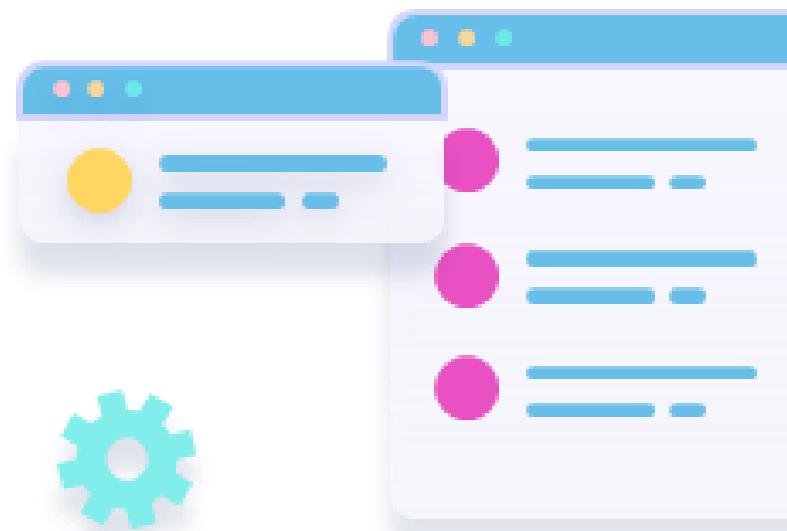
AGOULZI Imane et JOUIJATE Rim

Membres du jury :

M. BERQIA Amine

M. HABBANI Ahmed

PLAN



Introduction

- 1 Le Raspberry Pi
- 2 Les systèmes de détection d'intrusion
- 3 L'IDS Suricata
- 4 La prise en main de Raspberry Pi

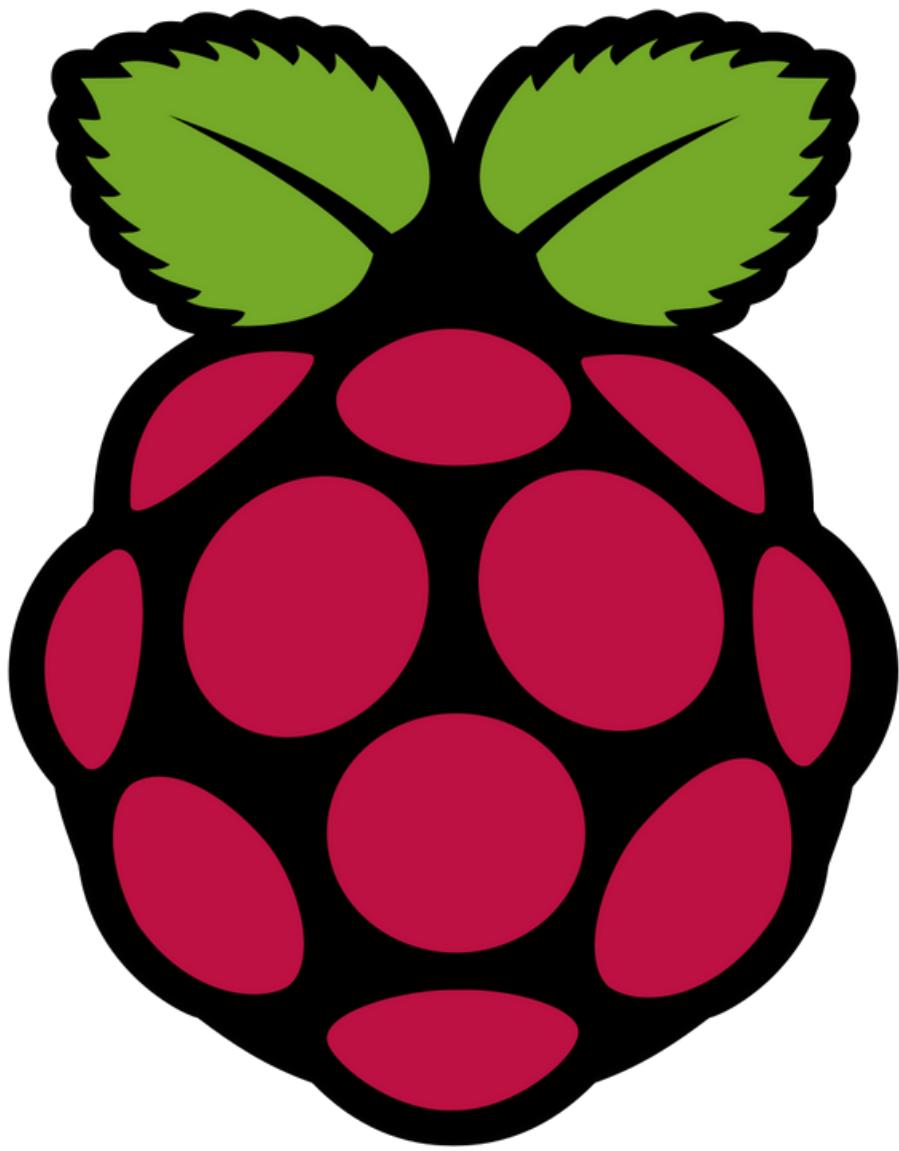
Conclusion

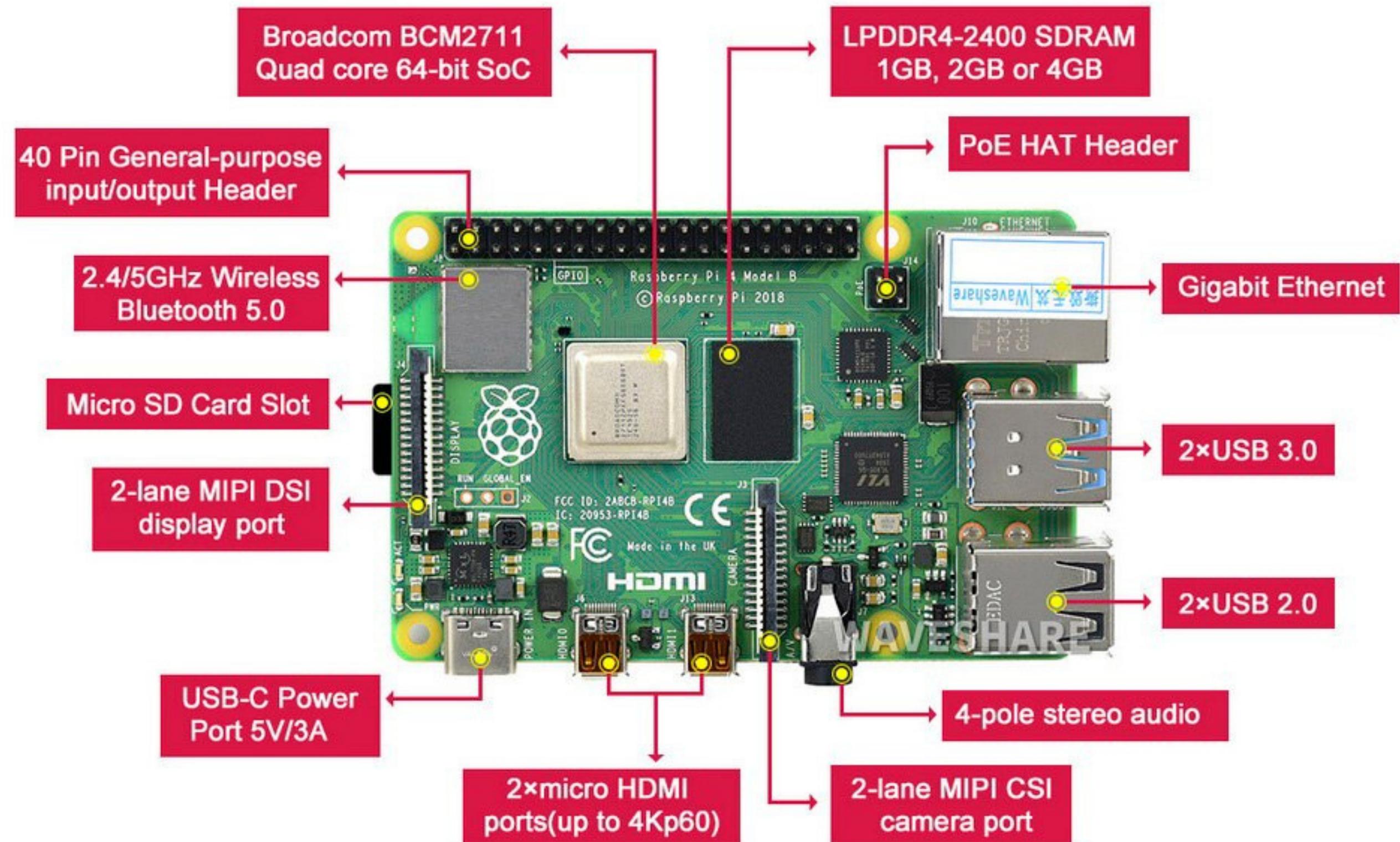
Introduction

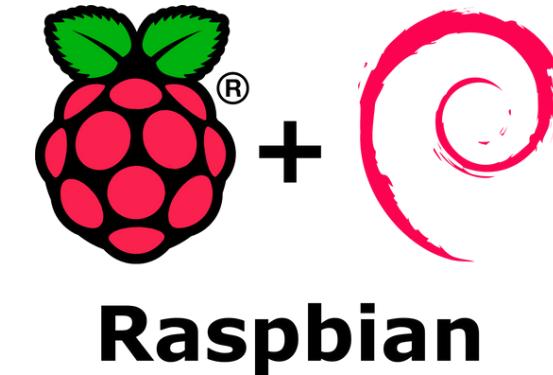
Objectif

1

Le Raspberry Pi

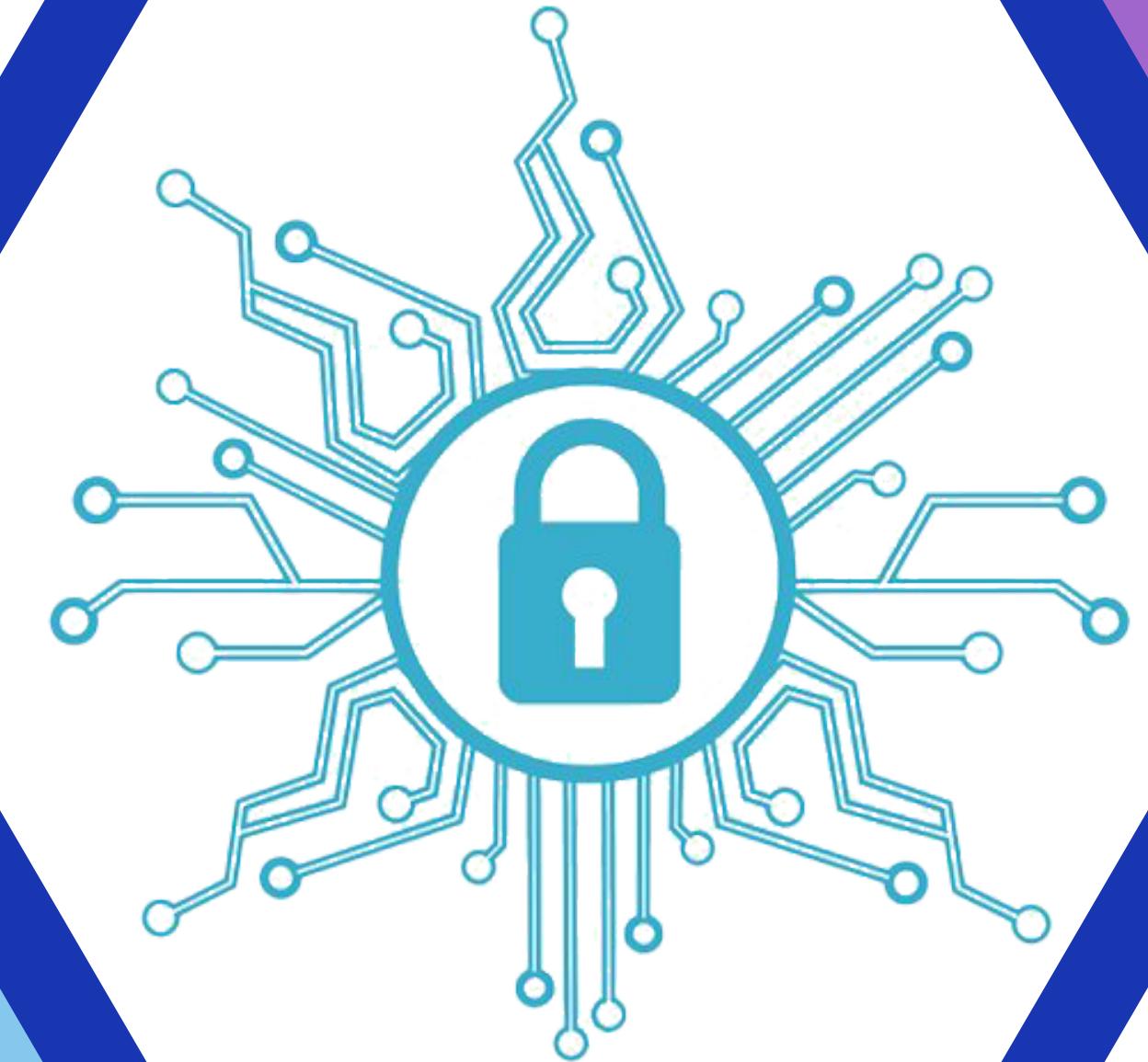


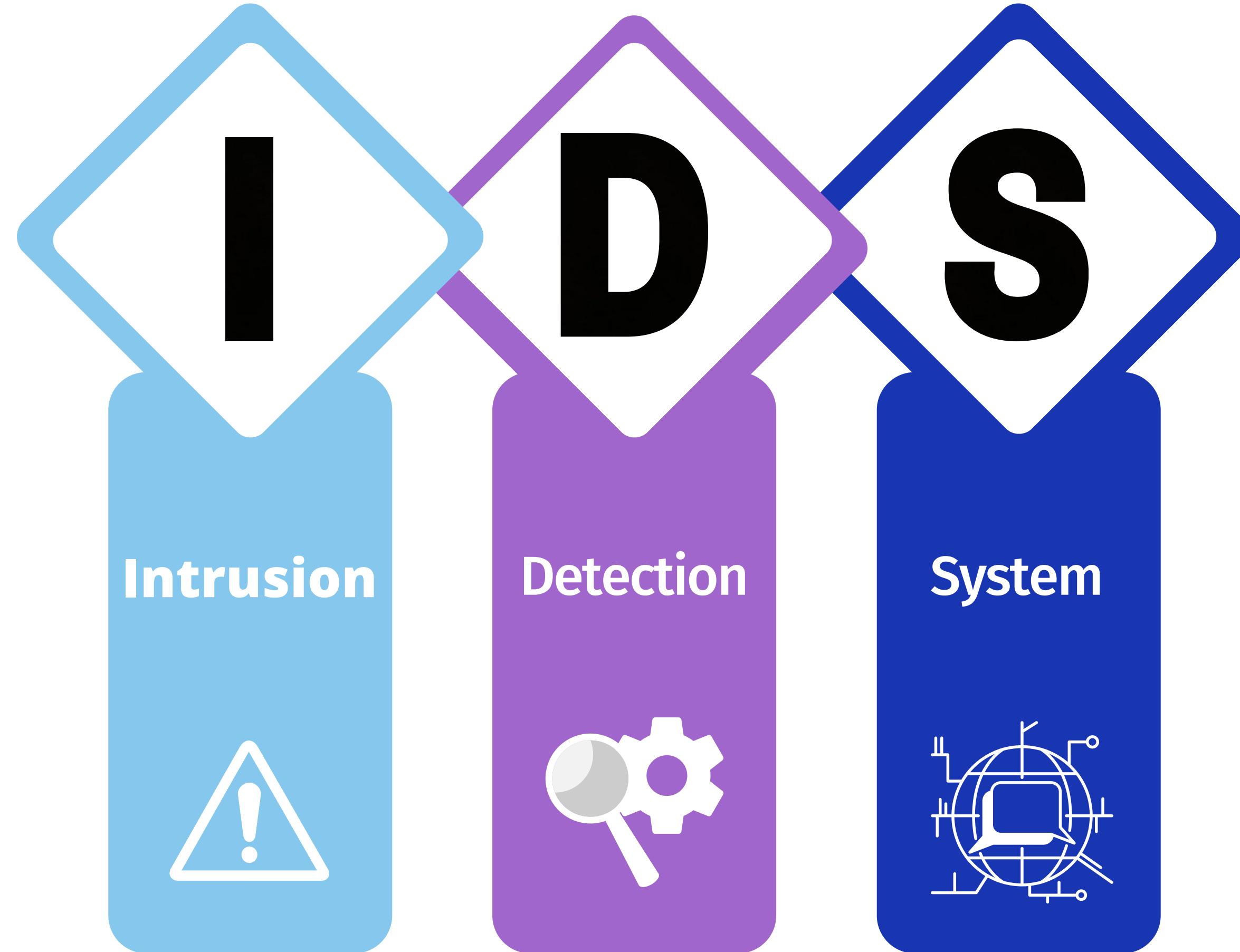




2

Les systèmes de détection d'intrusion





Les types d'IDS

Selon la cible surveillée

Selon le principe de détection

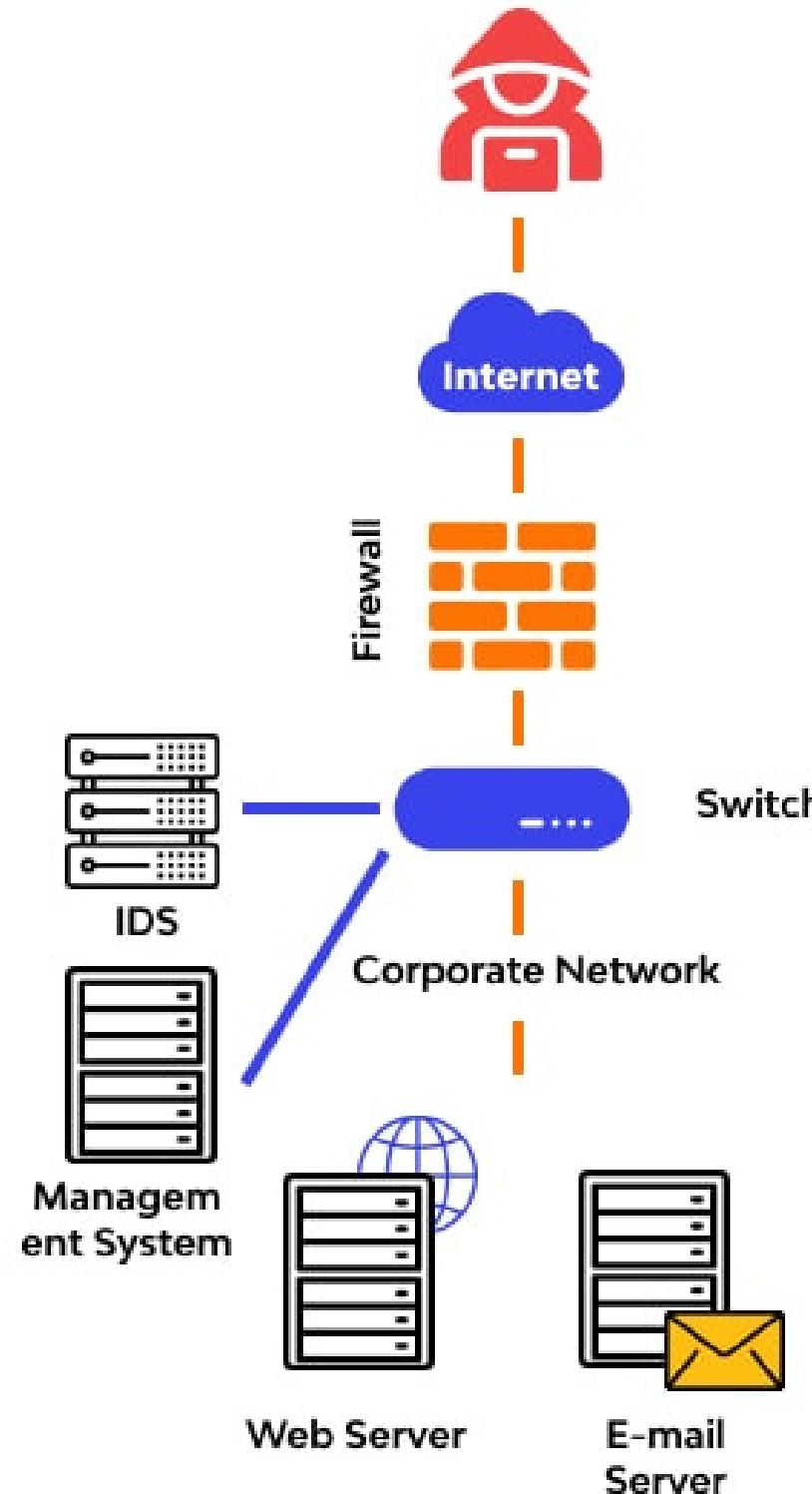
NIDS

HIDS

AIDS

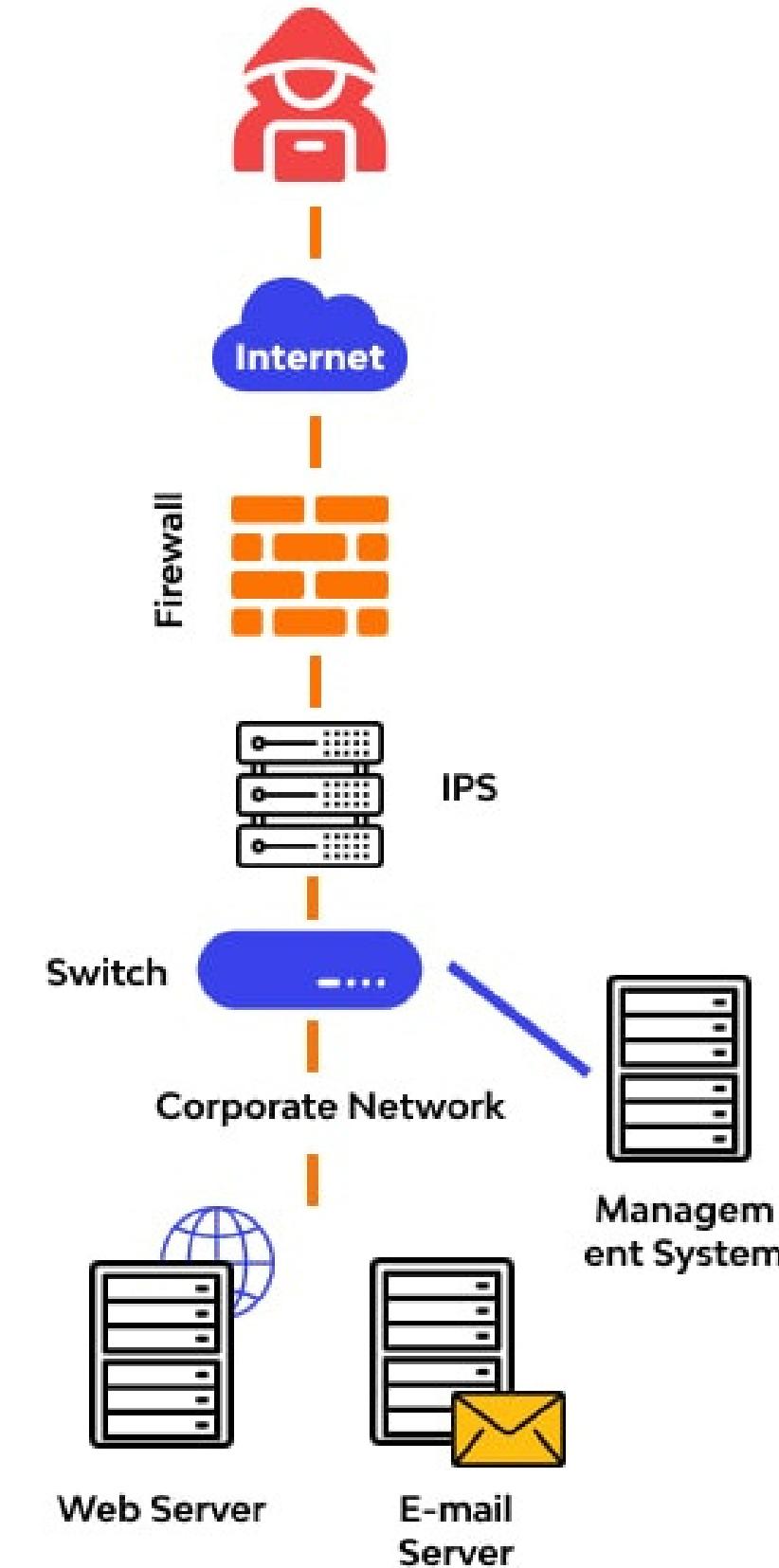
SIDS

Intrusion Detection System (IDS)



VS

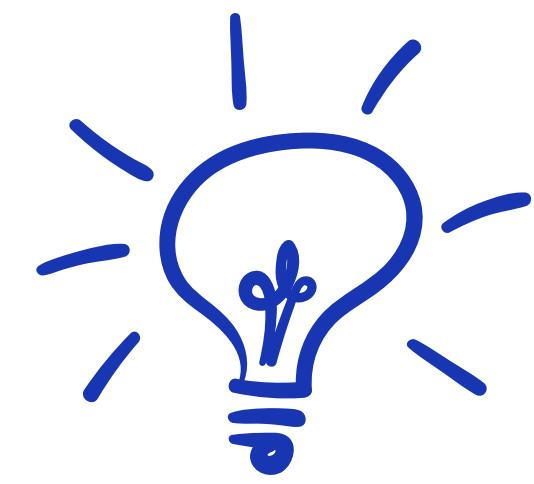
Intrusion Prevention System (IPS)



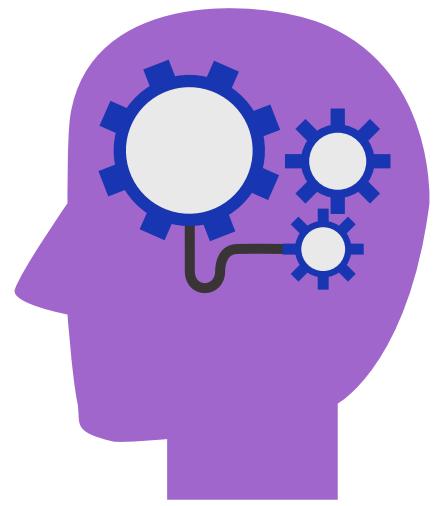
3

L'IDS Suricata





SURICATA

The word "SURICATA" is written in large, bold, orange letters. A yellow silhouette of a meerkat is standing on its hind legs, positioned behind the letter "I" in the word.

The action

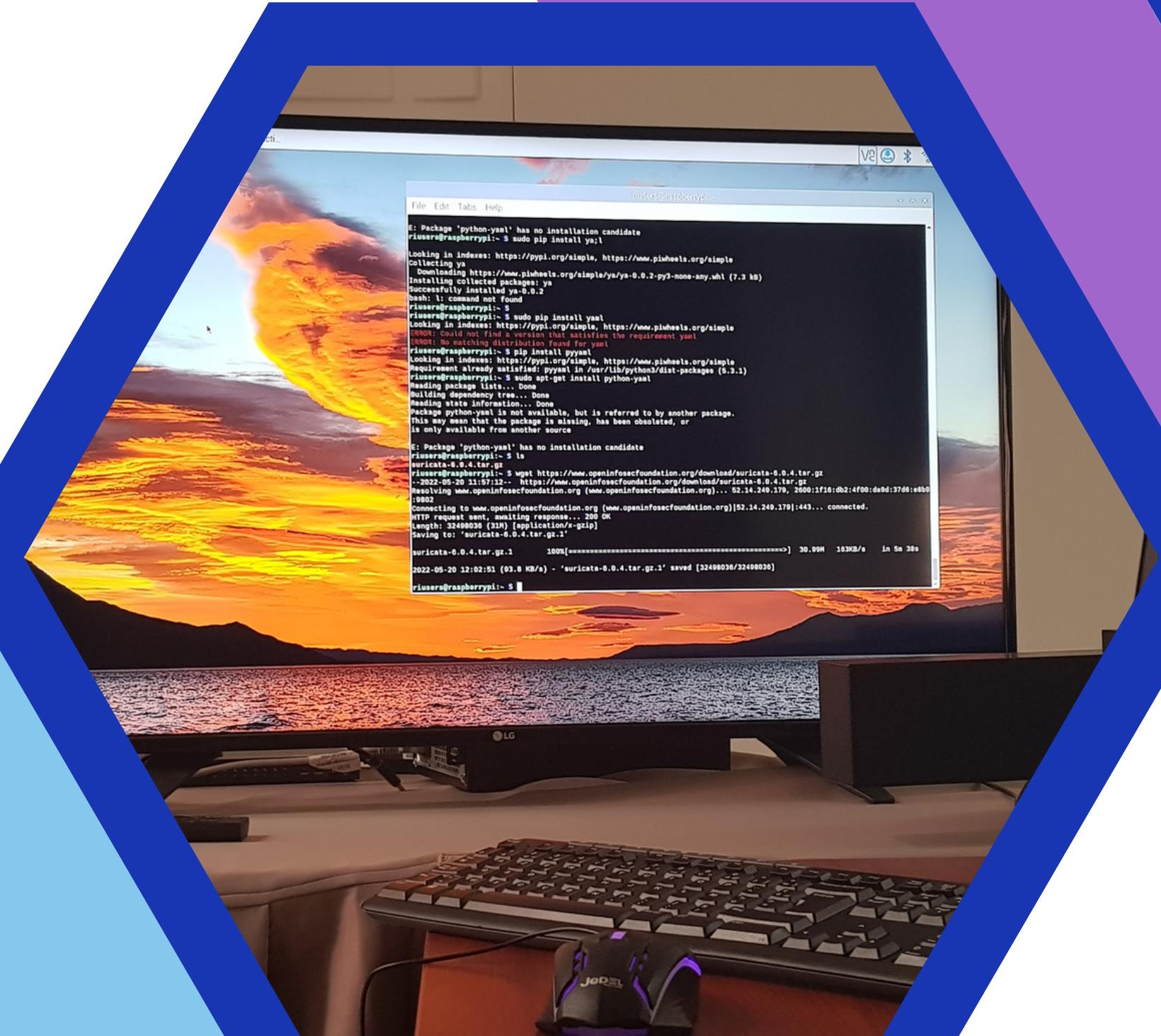
```
drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Likely Bot Nick in IRC (USA +..)";  
flow:established,to_server; flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK .*USA.*[0-9]  
{3,}/i"; reference:url,doc.emergingthreats.net/2008124; classtype:trojan-activity; sid:2008124;  
rev:2;)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

The header

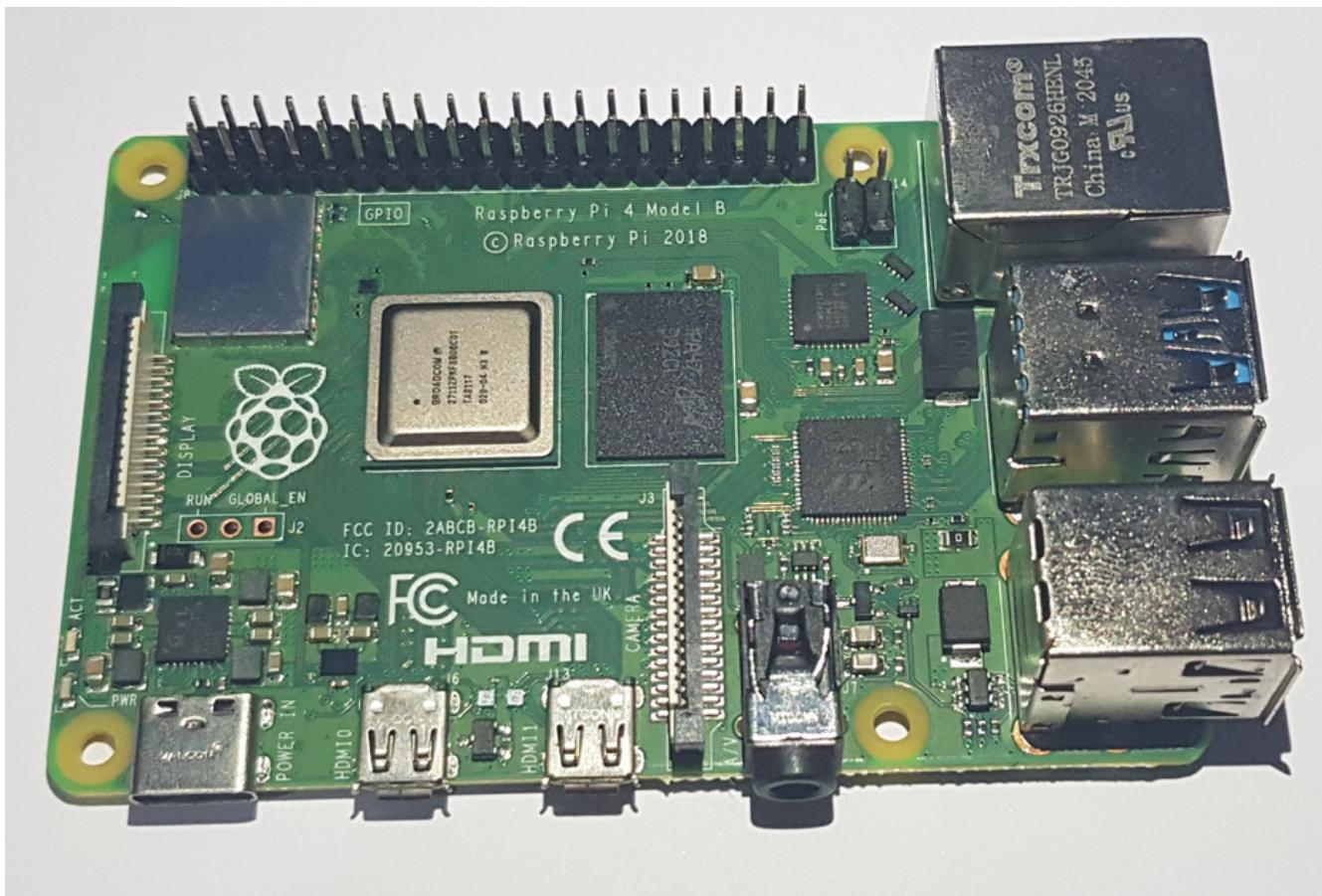
The options



La prise en main de Raspberry Pi



Matériel utilisé :



Cable HDMI



RPi 4 model B

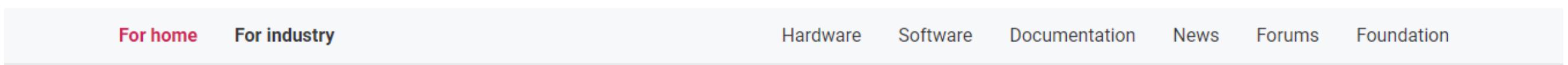


Carte SD

Chargeur Type C



1 - Installation de Raspberry OS :



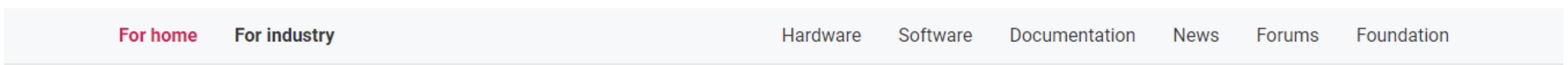
The image shows the top navigation bar of the official Raspberry Pi website. It features the Raspberry Pi logo (a red raspberry with green leaves) and the text "Raspberry Pi". Below the logo are two main categories: "For home" (highlighted in red) and "For industry". A horizontal line separates this from the main menu which includes: Hardware, Software, Documentation, News, Forums, and Foundation.

Raspberry Pi OS

Your Raspberry Pi needs an operating system to work. This is it. Raspberry Pi OS (previously called Raspbian) is our official supported operating system.



1 - Installation de Raspberry OS :



The screenshot shows the official Raspberry Pi website's header. It features the Raspberry Pi logo (a red and white circuit board icon) and the text "Raspberry Pi". Below the header is a navigation bar with links: "For home" (highlighted in red), "For industry", "Hardware", "Software", "Documentation", "News", "Forums", and "Foundation".

Raspberry Pi OS

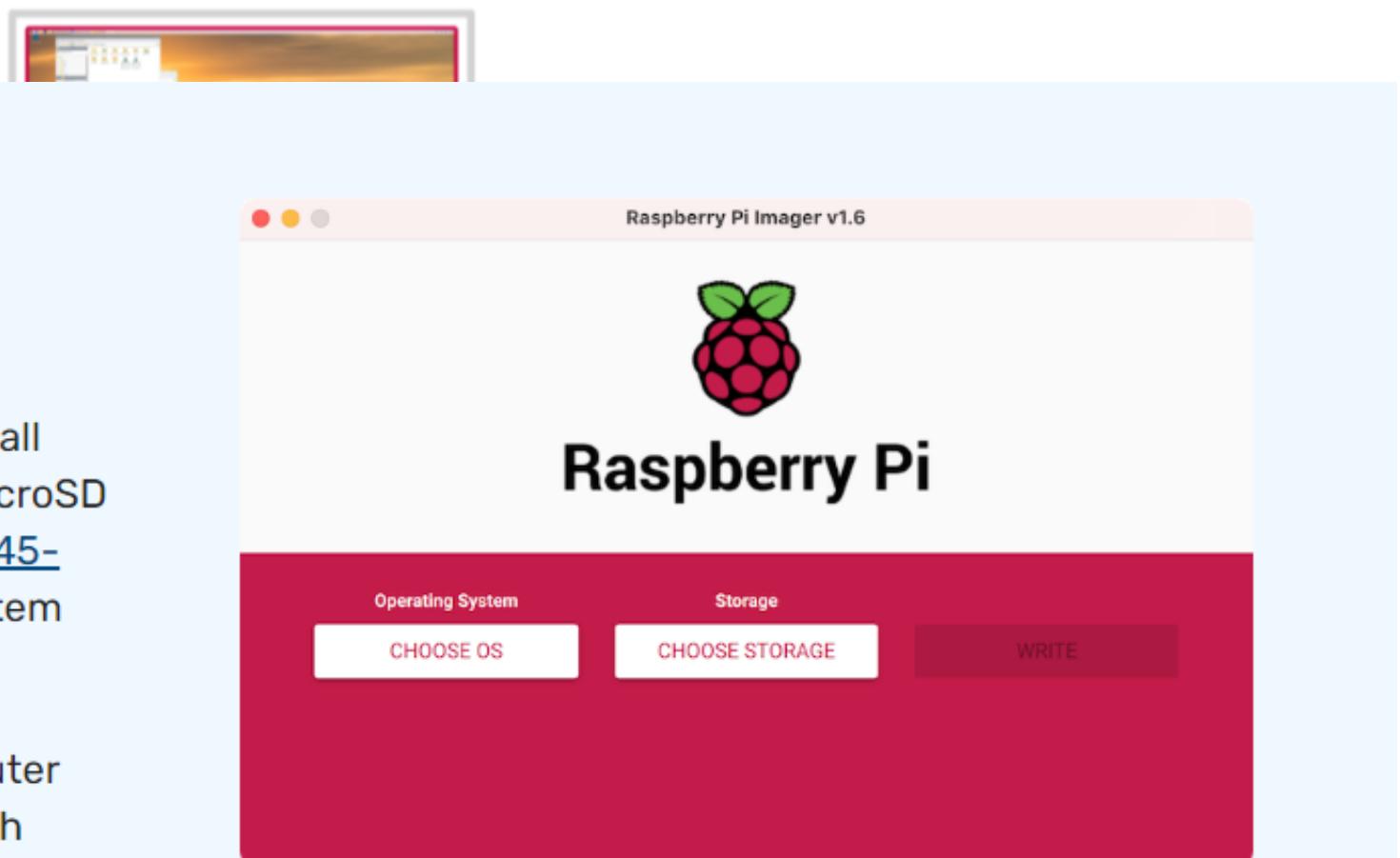
Your Raspberry Pi needs a work. This is it. Raspberry (Raspbian) is our official system.

Install Raspberry Pi OS using Raspberry Pi Imager

Raspberry Pi Imager is the quick and easy way to install Raspberry Pi OS and other operating systems to a microSD card, ready to use with your Raspberry Pi. [Watch our 45-second video](#) to learn how to install an operating system using Raspberry Pi Imager.

Download and install Raspberry Pi Imager to a computer with an SD card reader. Put the SD card you'll use with your Raspberry Pi into the reader and run Raspberry Pi Imager.

[Download for Windows](#)



1 - Installation de Raspberry OS :

The screenshot shows the Raspberry Pi Imager v1.6 application window. On the left, a sidebar titled "Operating System" lists several options:

- Raspberry Pi OS (32-bit)**: A port of Debian Bullseye with the Raspberry Pi Desktop (Recommended). Released: 2022-04-04. Cached on your computer.
- Raspberry Pi OS (other)**: Other Raspberry Pi OS based images.
- Other general-purpose OS**: Other general-purpose operating systems.
- Media player OS**: Media player operating systems.
- Emulation and game OS**.

On the right, the main area displays the "Foundation" logo and the text "Raspberry Pi Imager v1.6". Below this are buttons for "CHOOSE OS", "CHOOSE STORAGE", and "WRITE". At the bottom of the main window, there is a note: "This tool is part of the official Raspberry Pi Imager. It is not affiliated with or endorsed by the Raspberry Pi Foundation." A "Download for Windows" button is located at the bottom of the sidebar.

1 - Installation de Raspberry OS :

The screenshot shows the Raspberry Pi Imager interface. On the left, the 'Operating System' tab is selected, displaying a list of available OS images:

- Raspberry Pi OS (32-bit)**: A port of Debian Bullseye with the Raspberry Pi logo. Released: 2022-04-04. Cached on your computer.
- Raspberry Pi OS (other)**: Other Raspberry Pi OS based images.
- Other general-purpose OS**: Other general-purpose operating systems.
- Media player OS**: Media player operating systems.
- Emulation and game OS**.

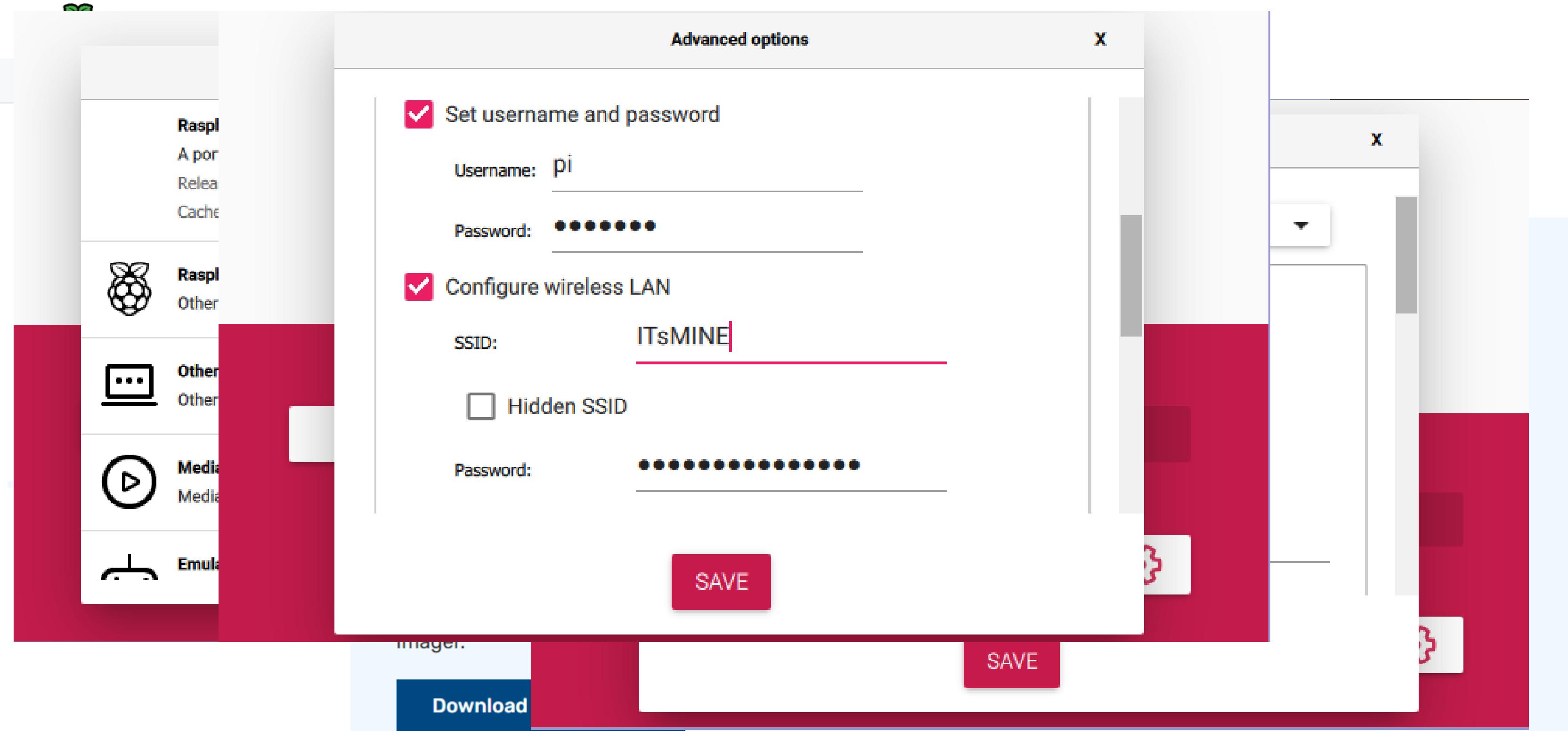
At the bottom of this section is a 'Download' button.

On the right, the 'Advanced options' tab is selected, showing customization settings:

- Image customization options: for this session only
- Set hostname: `raspberrypi`.local
- Enable SSH
 - Use password authentication
 - Allow public-key authentication only
- Set authorized_keys for 'pi':
- Get username and password

A large red 'SAVE' button is at the bottom right of the customization panel.

1 - Installation de Raspberry OS :



2 - Configuration du Raspberry Pi :



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19044.1645]
(c) Microsoft Corporation. All rights reserved.

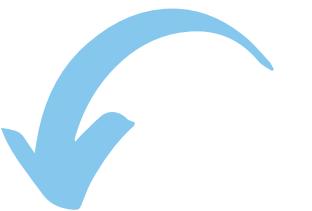
C:\WINDOWS\system32>ping raspberrypi.local

Pinging raspberrypi.local [fe80::c65:e1c1:728a:33c9%19] with 32 bytes
Reply from fe80::c65:e1c1:728a:33c9%19: time=2ms
Reply from fe80::c65:e1c1:728a:33c9%19: time=3ms
Reply from fe80::c65:e1c1:728a:33c9%19: time=6ms
Reply from fe80::c65:e1c1:728a:33c9%19: time=2ms

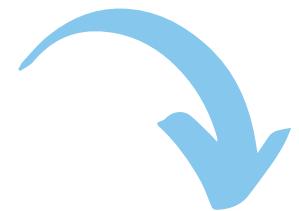
Ping statistics for fe80::c65:e1c1:728a:33c9%19:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 6ms, Average = 3ms

C:\WINDOWS\system32>
```

2 - Configuration du Raspberry Pi :



```
Administrator: Command Prompt  
Microsoft Windows [Version 10.0.19044.1645]  
(c) Microsoft Corporation. All rights reserved.  
  
C:\WINDOWS\system32>ping raspberrypi.local  
  
Pinging raspberrypi.local [fe80::c65:e1c1:728a:33c9%19] with 32 bytes  
Reply from fe80::c65:e1c1:728a:33c9%19: time=2ms  
Reply from fe80::c65:e1c1:728a:33c9%19: time=3ms  
Reply from fe80::c65:e1c1:728a:33c9%19: time=6ms  
Reply from fe80::c65:e1c1:728a:33c9%19: time=2ms  
  
Ping statistics for fe80::c65:e1c1:728a:33c9%19:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
    Minimum = 2ms, Maximum = 6ms, Average = 3ms  
  
C:\WINDOWS\system32>
```



Administrator: Command Prompt

Microsoft Windows [Version 10.0.19044.1645]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>ping raspberrypi.local

Pinging raspberrypi.local [fe80::c65:e1c1:728a:33c9%19] with 32 bytes of data:

Reply from fe80::c65:e1c1:728a:33c9%19: time=2ms
Reply from fe80::c65:e1c1:728a:33c9%19: time=3ms
Reply from fe80::c65:e1c1:728a:33c9%19: time=6ms
Reply from fe80::c65:e1c1:728a:33c9%19: time=2ms

Ping statistics for fe80::c65:e1c1:728a:33c9%19:

 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

 Minimum = 2ms, Maximum = 6ms, Average = 3ms

C:\WINDOWS\system32>

Administrator: Command Prompt

Microsoft Windows [Version 10.0.19044.1645]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>ping raspberrypi.local

Pinging raspberrypi.local [fe80::c65:e1c1:728a:33c9%19] with 32 bytes of data:

Reply from fe80::c65:e1c1:728a:33c9%19: time=2ms
Reply from fe80::c65:e1c1:728a:33c9%19: time=3ms
Reply from fe80::c65:e1c1:728a:33c9%19: time=6ms
Reply from fe80::c65:e1c1:728a:33c9%19: time=2ms

Ping statistics for fe80::c65:e1c1:728a:33c9%19:

 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

 Minimum = 2ms, Maximum = 6ms, Average = 3ms

C:\WINDOWS\system32>

C:\WINDOWS\system32>ssh riusers@raspberrypi.local
riusers@raspberrypi.local's password:
Linux raspberrypi 5.15.32-v7l+ #1538 SMP Thu Mar 31 19:39:41 BST 2022 armv7l

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

Last login: Wed Apr 13 16:42:42 2022 from fe80::f021:8192:be7c:3066%wlan0
riusers@raspberrypi:~ \$

Administrator: Command Prompt

Microsoft Windows [Version 10.0.19044.1645]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>ping raspberrypi.local

pi@raspberrypi:~ \$ sudo apt update

Hit:1 http://archive.raspberrypi.org/debian bullseye InRelease
Hit:2 https://download.docker.com/linux/raspbian bullseye InRelease
Hit:3 http://raspbian.raspberrypi.org/raspbian bullseye InRelease

Reading package lists... Done

Building dependency tree... Done

Reading state information... Done

16 packages can be upgraded. Run 'apt list --upgradable' to see them.

C:\WINDOWS\system32>ssh riusers@raspberrypi.local

riusers@raspberrypi.local's password:

Linux raspberrypi 5.15.32-v7l+ #1538 SMP Thu Mar 31 19:39:41 BST 2022 armv7l

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

Last login: Wed Apr 13 16:42:42 2022 from fe80::f021:8192:be7c:3066%wlan0

riusers@raspberrypi:~ \$

Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.19044.1645]
(c) Microsoft Corporation. All rights reserved.
```

```
C:\WINDOWS\system32>ping raspberrypi.local
```

```
pi@raspberrypi:~ $ sudo apt upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  libauthen-sasl-perl libclone-perl libdata-dump-perl libencode-locale-perl libevent-core-2.1-7
  libevent-pthreads-2.1-7 libfile-listing-perl libfont-afm-perl libfuse2 libhiredis0.14 libhtml-form-perl
  libhtml-format-perl libhtml-parser-perl libhtml-tagset-perl libhtml-tree-perl libhttp2 libhttp-cookies-perl
  libhttp-daemon-perl libhttp-date-perl libhttp-message-perl libhttp-negotiate-perl libio-html-perl
  libio-socket-ssl-perl liblwp-mediatypes-perl liblwp-protocol-https-perl libmailtools-perl libnet-http-perl
  libnet-smtp-ssl-perl libnet-ssleay-perl libnet1 libnetfilter-log1 libnetfilter-queue1 libtimedate-perl
  libtry-tiny-perl liburi-perl libwww-perl libwww-robotrules-perl oinkmaster perl-openssl-defaults snort-rules-default
  suricata-update
Use 'sudo apt autoremove' to remove them.
The following packages will be upgraded:
  cifs-utils cups cups-client cups-common cups-core-drivers cups-daemon cups-ipp-utils cups-ppdc cups-server-common
  dpkg dpkg-dev libcups2 libcupsimage2 libdpkg-perl rpi-chromium-mods rsyslog
16 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

```
Last login: Wed Apr 13 16:42:42 2022 from fe80::f021:8192:be7c:3066%wlan0
piusers@raspberrypi:~ $
```

```
pi@raspberrypi:~ $ sudo /usr/sbin/useradd --groups sudo -m riusers
pi@raspberrypi:~ $ whoiam
bash: whoiam: command not found
pi@raspberrypi:~ $ whoami
pi
pi@raspberrypi:~ $ sudo passwd riusers
New password:
Retype new password:
passwd: password updated successfully
pi@raspberrypi:~ $
```

3 - Installation de Suricata IDS :

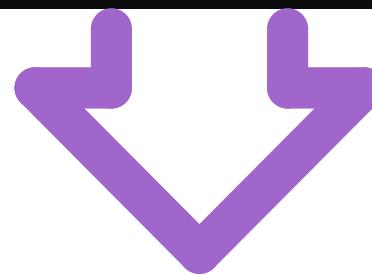


3 - Installation de Suricata IDS :

```
riusers@raspberrypi:~/suricata-6.0.1 $ hostname -I  
10.1.6.117 172.17.0.1  
riusers@raspberrypi:~/suricata-6.0.1 $ sudo nano /etc/suricata/suricata.yaml  
[sudo] password for riusers:
```

3 - Installation de Suricata IDS :

```
riusers@raspberrypi:~/suricata-6.0.1 $ hostname -I  
10.1.6.117 172.17.0.1  
riusers@raspberrypi:~/suricata-6.0.1 $ sudo nano /etc/suricata/suricata.yaml  
[sudo] password for riusers:
```



3 - Installation de Suricata IDS :

```
riusers@raspberrypi:~/suricata-6.0.1 $ hostname -I  
10.1.6.117 172.17.0.1  
riusers@raspberrypi:~/suricata-6.0.1 $ sudo nano /etc/suricata/suricata.yaml  
[sudo] password for riusers:
```



```
GNU nano 5.4                               /etc/suricata/suricata.yaml  
%YAML 1.1  
---  
  
# 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: "[192.168.1.101]"  
        #HOME_NET: "[192.168.0.0/16]"  
        #HOME_NET: "[10.0.0.0/8]"  
        #HOME_NET: "[172.16.0.0/12]"  
        #HOME_NET: "any"  
  
        EXTERNAL_NET: "!$HOME_NET"  
        #EXTERNAL_NET: "any"
```

4 - Lancement de Suricata IDS :

fichier de configuration à utiliser

```
riusers@raspberrypi:~ $ sudo suricata -c /etc/suricata/suricata.yaml -i eth0 -S /var/lib/suricata/rules/suricata.rules
31/5/2022 -- 15:37:01 - <Notice> - This is Suricata version 6.0.4 RELEASE running
in SYSTEM mode
^Z
[11]+  Stopped                  sudo suricata -c /etc/suricata/suricata.yaml -i et
h0 -S /var/lib/suricata/rules/suricata.rules
```

4 - Lancement de Suricata IDS :

interface Ethernet à surveiller

```
riusers@raspberrypi:~ $ sudo suricata -c /etc/suricata/suricata.yaml -i eth0 -S /var/lib/suricata/rules/suricata.rules
31/5/2022 -- 15:37:01 - <Notice> - This is Suricata version 6.0.4 RELEASE running
in SYSTEM mode
^Z
[11]+  Stopped                  sudo suricata -c /etc/suricata/suricata.yaml -i et
h0 -S /var/lib/suricata/rules/suricata.rules
```

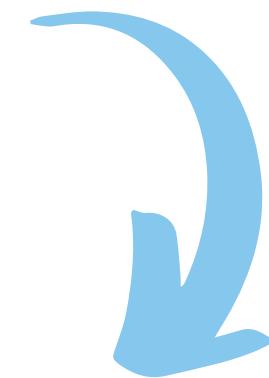
4 - Lancement de Suricata IDS :

fichier contenant les règles à utiliser

```
riusers@raspberrypi:~ $ sudo suricata -c /etc/suricata/suricata.yaml -i eth0 -S /var/lib/suricata/rules/suricata.rules
31/5/2022 -- 15:37:01 - <Notice> - This is Suricata version 6.0.4 RELEASE running
in SYSTEM mode
^Z
[11]+  Stopped                  sudo suricata -c /etc/suricata/suricata.yaml -i et
h0 -S /var/lib/suricata/rules/suricata.rules
```

5 - Test de Suricata IDS :

la règle : alert icmp any any -gt ; any any (msg :"ICMP Packet found"; sid :1; rev :1;)



```
-bash: /var/lib/suricata/rules/suricata.rules: Permission denied
riusers@raspberrypi:~ $ sudo nano /var/lib/suricata/rules/suricata.rules
riusers@raspberrypi:~ $ riusers@raspberrypi:~ $ sudo tail -f /var/log/suricata/fast.log
05/24/2022-19:43:40.503135  [**] [1:1:1] ICMP Packet found [**] [Classification: (null)] [Priority: 3] {ICMP} 10.1.8.156
:8 -> 255.255.255.255:0
05/24/2022-19:43:54.944055  [**] [1:2027397:1] ET POLICY Spotify P2P Client [**] [Classification: Not Suspicious Traffic]
] [Priority: 3] {UDP} 10.1.7.16:57621 -> 10.1.255.255:57621
05/24/2022-19:44:40.502582  [**] [1:1:1] ICMP Packet found [**] [Classification: (null)] [Priority: 3] {ICMP} 10.1.8.156
:8 -> 255.255.255.255:0
05/24/2022-19:45:07.947273  [**] [1:2027397:1] ET POLICY Spotify P2P Client [**] [Classification: Not Suspicious Traffic]
] [Priority: 3] {UDP} 10.1.5.49:57621 -> 10.1.255.255:57621
05/24/2022-19:45:40.523152  [**] [1:1:1] ICMP Packet found [**] [Classification: (null)] [Priority: 3] {ICMP} 10.1.8.156
:8 -> 255.255.255.255:0
05/24/2022-19:46:14.203110  [**] [1:2027397:1] ET POLICY Spotify P2P Client [**] [Classification: Not Suspicious Traffic]
] [Priority: 3] {UDP} 10.1.7.135:57621 -> 10.1.255.255:57621
05/24/2022-19:46:38.463529  [**] [1:2027397:1] ET POLICY Spotify P2P Client [**] [Classification: Not Suspicious Traffic]
```

6 - Utilisation du Suricata en mode service

Création du fichier dans : /etc/systemd/system/suricata.service



```
GNU nano 5.4          /etc/systemd/system/suricata.service
# Sample Suricata systemd unit file.
[Unit]
Description=Suricata Intrusion Detection Service
After=network.target syslog.target
[Service]
ExecStart=/usr/bin/suricata -c /etc/suricata/suricata.yaml -i eth0 -S /var/lib/s>
ExecReload=/bin/kill -HUP $MAINPID
ExecStop=/bin/kill $MAINPID
[Install]
WantedBy=multi-user.target
```

6 - Utilisation du Suricata en mode service

Création du fichier dans : /etc/systemd/system/suricata.service

7 - Utilisation des ressources du Raspberry Pi

Utilisation de processeur



top											COMMAND
		Swap:			Mem:			CPU:			COMMAND
PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
551	root	20	0	577348	457844	8240	S	17.8%	5.7	2:12.04	Suricata-M+
888	root	0	-20	0	0	0	I	0.3%	0.0	0:02.00	kworker/u9+
1523	riusers	20	0	11364	2952	2496	R	0.3	0.0	0:00.29	top
1	root	20	0	33904	8808	6924	S	0.0	0.1	0:03.13	systemd

7 - Utilisation des ressources du Raspberry Pi

Utilisation de la mémoire



```
piusers@raspberrypi:~ $ free
              total        used        free      shared  buff/cache   available
Mem:    8088496     676728  6792020        22456      619756    7155052
Swap:  102396          0  102396
```

7 - Utilisation des ressources du Raspberry Pi

Utilisation de la carte SD



```
piusers@raspberrypi:~ $ df
Filesystem      1K-blocks   Used   Available  Use% Mounted on
/dev/root        29583108 5633125 22693940  20% /
devtmpfs          3879384    0  3879384   0% /dev
tmpfs            4044248    0  4044248   0% /dev/shm
tmpfs            1617700 1244  1616456   1% /run
tmpfs              5120     4   5116   1% /run/lock
/dev/mmcblk0p1    258095 50413  207683  20% /boot
tmpfs            808848    20  808828   1% /run/user/1000
tmpfs            808848    16  808832   1% /run/user/1001
```

Conclusion

MERCI DE VOTRE ATTENTION !