Security Operation Center@home

We'll use SecurityOnion
Minimum requirements as of version 2.4 are :

- 4 Cores
- 16GB RAM
- 200GB HDD

On top of this you'll need: **2 NICs** (1 for management, 1 for the monitoring)
 You ARE NOT ALLOWED TO SNIFF/MONITOR network you don't own or for which you are not authorized:!:
That being said let's jump on it.

2.4 installation

boot on the ISO

first setup

- Operating system device: sdb. (in my case  256GB)
- same device for nsm ? NO
- NSM storage: sda (in my case 2TB)
- continue: yes  it will erase EVERYTHING 
- username
- pass

~5 minutes later if it's not frozen for whatever reason, reboot by pressing [enter]

First reboot

- log in
- install
- STANDALONE (in my case)
- Elastic search AGREE
- node install: standard
- name: soc
- description [enter] (in my case)
- management interface: eno1
- IP address: static (recommended! or you can force your DHCP always to give you the same

IP....)
- IP: 192.168.1.XX/24
- gateway: 192.168.1.YY
- DNS: 192.168.1.ZZ,192.168.1.WW
- domain: fortier-family.com (in my case)
- connection method: Direct (in my case, no proxy)
- default Docker IP: yes
- NIC monitoring interface: enp1s0 (in my case) [space] to select
- Email address for admin account
- pass: 12345678
- web access method: OTHER
- type in the FQDN
- allow access through web interface?: .... YES (!!)
- IP range: 192.168.1.0/24
- Telemetry Yes/no
- summary

Troubleshooting

The installer is a piece of shit... you cannot go back, it freezes, and once at first reboot mgmt NIC was dead !! I had to reinstall it completely.

if the network is not working at the end, just log in, then:

```
sudo SecurityOnion/so-setup-network
```

Good luck 😎

Virtual or Physical

It's really up to you, personally, I have a Dell Optiplex 7010 (16GB RAM i5-3470 256GB SSD) I tried using Security Onion under VMWare ESXi 7 but couldn't make it see all devices of my home network. So I bought an 8-port SWITCH with port mirroring (TP-link TL-SG108E)and used the Optiplex as standalone physical machine. I installed using sda as system disk and sdb (2TB SSD) for NSM data. I chose to run all services available and installed Security Onion as "**STANDALONE**" ❗ set the management NIC with a static IP ❗

Once installed and setup you can access the web interface using https://static_IP_of_Security_Onion

SWAP

16GB is a bit tight ...

```
dd if=/dev/zero of=/nsm/16GB.swap count=16384 bs=1MiB
chmod 600 /nsm/16GB.swap
mkswap /nsm/16GB.swap
swapon /nsm/16GB.swap
echo "/nsm/16GB.swap  swap swap sw 0 0" >> /etc/fstab
```

EPEL

```
 dnf install -y epel-release
dnf update
dnf install -y htop toilet
```

NTP

```
timedatectl set-timezone Europe/Zurich
timedatectl
vi /etc/chrony.conf
```

```
# NTP server list
#server 0.pool.ntp.org iburst
#server 1.pool.ntp.org iburst
server ntp.fortier-family.com

# Config options
driftfile /var/lib/chrony/drift
makestep 1.0 3
rtcsync
logdir /var/log/chrony
```

```
systemctl restart chronyd
chronyc sources
```

SSL Certs

Like for the rest of my local webservice I use a A record in my DNS then use certbot

```
sudo certbot -d yoursoc.yourdomain.tld --server https://acme-
```

```
v02.api.letsencrypt.org/directory --manual --preferred-challenges dns
certonly
```

- /etc/salt/minion.d/signing_policies.conf

```
grep ssl -A10 /etc/salt/minion.d/signing_policies.conf
```

First time (backup original files)

```
cd /etc/pki
cp ca.key ca.key.org
cp ca.crt ca.crt.org
cp managerssl.crt managerssl.crt.org
cp managerssl.key managerssl.key.org
```

Renewal/Install

```
sudo su
cd /etc/letsencrypt/live/soc.fortier-family.com/
scp fullchain.pem privkey.pem warnaud@soc.fortier-family.com:~/.
ssh soc.fortier-family.com
cd /etc/pki
cp /home/warnaud/fullchain.pem managerssl.crt
cp: overwrite ‘managerssl.crt’? y
cp /home/warnaud/privkey.pem managerssl.key
cp: overwrite ‘managerssl.key’? y
so-nginx-restart
```

Wazuh Agent

Download from https://soc.fqdn.tld/#/downloads
Then

- https://docs.securityonion.net/en/2.3/wazuh.html
- https://documentation.wazuh.com/3.13/user-manual/registering/command-line-registration.html

Silence rule

- https://docs.securityonion.net/en/2.3/managing-alerts.html#suppressions

```
grep  2033078 /opt/so/rules/nids/all.rules
```

where 2033078 is the rule.uuid in “Alerts”

```
vi /opt/so/saltstack/local/pillar/minions/soc_standalone.sls
```

```
...
idstools:
  config:
    ruleset: 'ETOPEN'
    oinkcode: ''
    urls:
  sids:
    enabled:
    disabled:
        - 2033078
    modify:
```

 as always it's NOT WORKING and SCREW UP TOTALLY ALL SO containers 
(!!!!!!!!!!!!!!!!!!!!)

References

- https://docs.securityonion.net/en/2.3/index.html
- https://docs.saltproject.io/en/latest/ref/configuration/minion.html
- https://z3r0th.medium.com/setting-up-security-onion-at-home-717340816b4e
- https://github.com/Security-Onion-Solutions/securityonion/issues/1766
- https://docs.securityonion.net/en/2.3/wazuh.html
- https://documentation.wazuh.com/3.13/user-manual/registering/command-line-registration.html
- https://github.com/Security-Onion-Solutions/securityonion/discussions/5117 | SSL certs
- https://docs.securityonion.net/en/2.3/url-base.html | change IP to FQDN for web manager
- https://github.com/Security-Onion-Solutions/security-onion/wiki/Cheat-Sheet
- https://docs.securityonion.net/en/2.3/installation.html