Security Operation Center@home

We'll use SecurityOnion
Minimum requirement as of version 2.3.30 are :

- 4 Cores
- 12GB 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 authorised 
That being said let's jump on it.

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 a 8 ports 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

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