Suricata Installation

```
sudo add-apt-repository ppa:oisf/suricata-stable
sudo apt-get update
sudo apt-get install suricata
suricata -V
```

Rules

```
Outputs vs alerts both need

/etc/suricata/ - main configuration path
/var/lib/suricata/ - primary rule path
```

Suricata is deployed as a systemd unit called `suricata.service`. Normal systemd procedures apply here. It can also be managed using the `rockctl` command using the same syntax:

```
sudo systemctl start suricata
sudo systemctl status suricata
sudo systemctl stop suricata
sudo systemctl restart suricata
```

The default ROCK configuration has the Suricata service enabled on startup.

Suricata-update -h //rule manager for suricata

```
Suricata-update
Suricata-update list-sources
Suricata-update list-enabled-sources
Suricata-update enable-source
Suricata-update //apply the change
```

USAGE

```
suricata -c /etc/suricata/suricata.yaml -i ens33

suricata -c /etc/suricata/suricata.yaml -s
/etc/suricata/rules/local.rules -i ens33

sudo gedit /etc/suricata/suricata.yaml
```

```
        default-rule-path: /usr/local/etc/suricata/rules

                rule-files:
                - suricata.rules
                - /path/to/local.rules
```

LOGS

By default, Suricata will log alerts to two places

- eve.json
- fast.log

```
tail -f /var/log/suricata/fast.log
nano /etc/suricata/rules/local.rules

SCRIPT
./script.sh arxeiopcap.pcap
Chmod +x script.sh

https://gist.github.com/jstrosch/d9e31d364a80714856eb70fcf6f9b13f
script to check pcap files

https://github.com/jstrosch/malware-samples
lib for pcap files
```

USEFULL LINKS

https://suricata.readthedocs.io/en/latest/quickstart.html
https://www.youtube.com/watch?v=ycGoQgx6VhA&list=PLwSNSpUrMBASVsC5O6vJK6SJZhaOROOED&index=1&t=767s