Amsterdamize your firewall

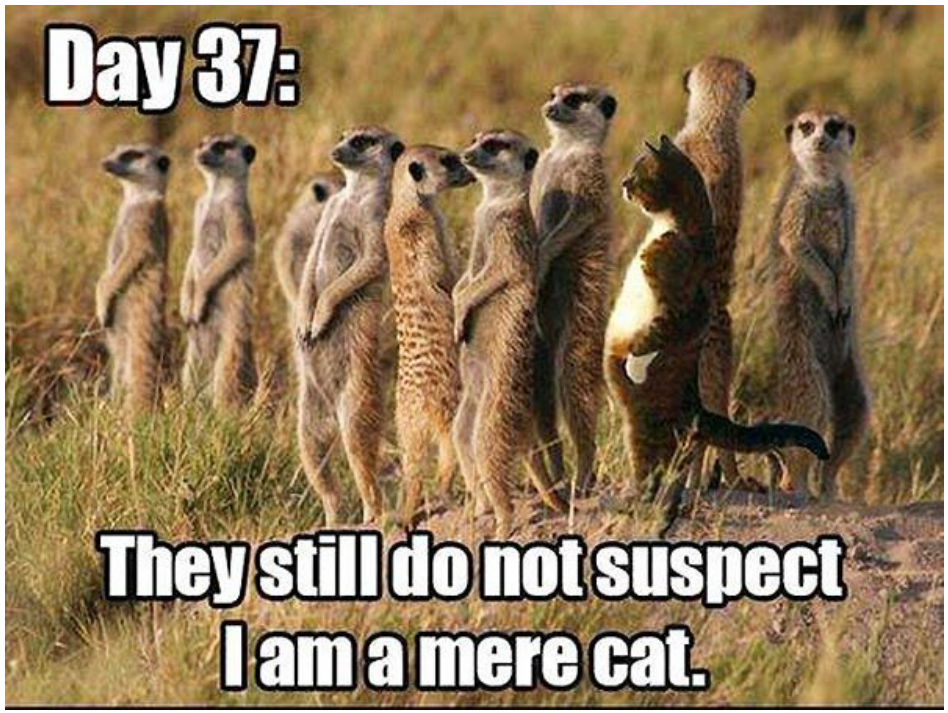
É. Leblond

Stamus Networks

2016 June 27

STAMUS NETWORKS

Éric Leblond



- Éric Leblond aka @Regiteric
- Netfitler coreteam and Suricata core developer
- Co-founder of Stamus Networks

STAMUS NETWORKS

Disclaimer

Disclaimer

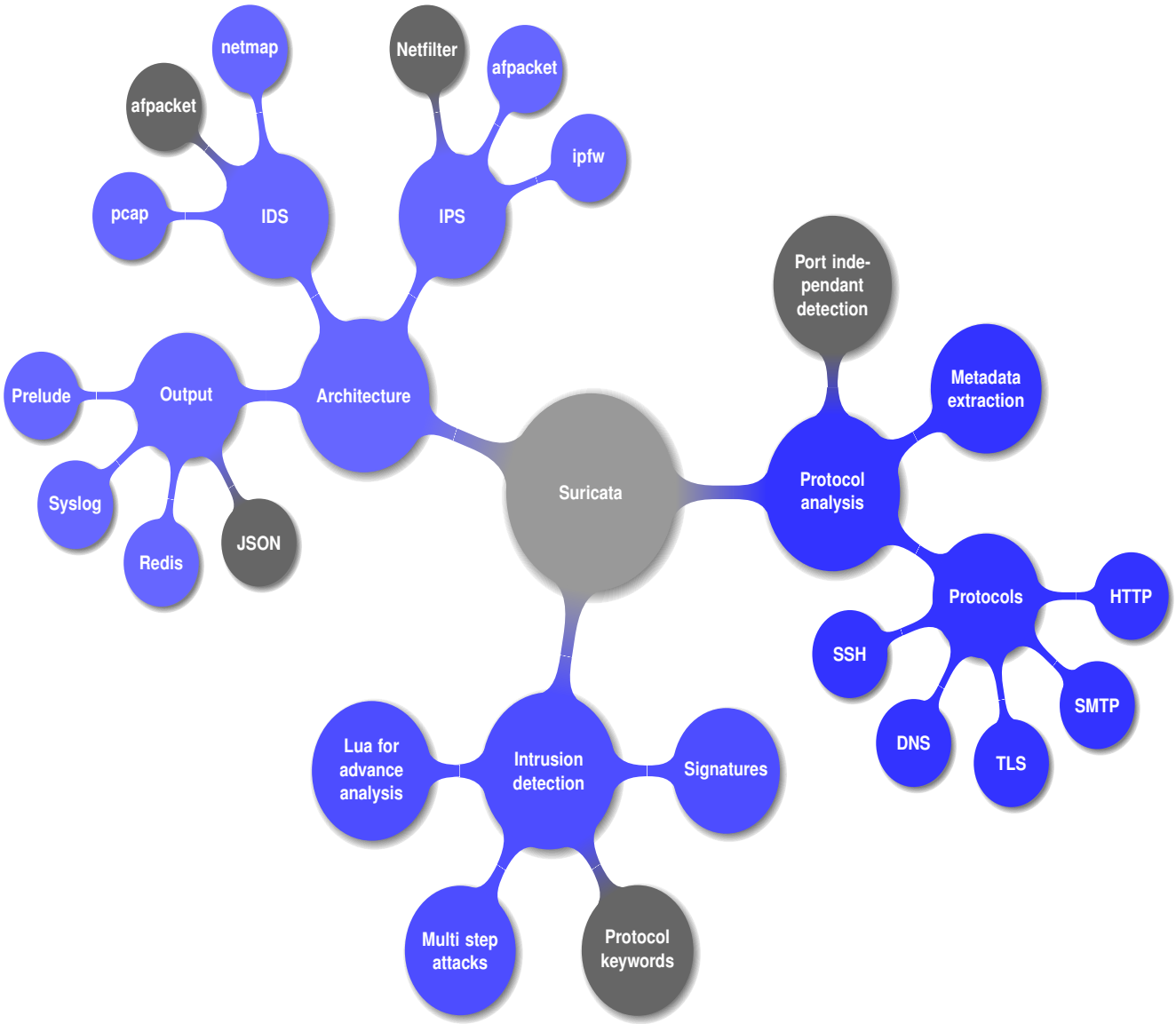
This talk does not aim to hurt the feeling of Dutch people in the assitance. So it will not cover subjects like certificates authorities or soccer.

Ontkenning

Katje poesje Nelletje waar ben je toch geweest? Je hebt verbrand je velletje je was zo'n aardig beest.

STAMUS NETWORKS

Suricata key points



STAMUS NETWORKS

SELKS

An installable and live ISO

- Based on Debian live
- A running Suricata configured and manageable via a web interface

Contenu

- Suricata: git version
  - Signature based IDS
  - Network Security Monitoring engine
  - Open source
- Elasticsearch: database, full search text
- Logstash: collect info and store them in Elasticsearch
- Kibana: dashboard interface for data analysis
- Scirius: web interface for suricata ruleset management

Docker

- Light weight virtualization
- Containers based
  - Use cgroup
  - Various namespaces
- Application repository
  - Pull an application
  - Fire it
  - Forget it

STAMUS NETWORKS

Suricata Docker QA

Buildbot and prscript

- A Python system to automate the compile/test cycle to validate code changes.
- Prscript is pre Pull Request script:
  - Known developers have to run it before PR
  - Trigger a series of build in the buildbot
  - Also some basic functional tests

Docker mode for prscript

- Buildbot installed in a docker container
- Ready to use via prscript
- Available in docker hub
- Configuration in the source

Docker compose

Orchestration

- Create distributed applications
- Distributed applications consist of many small applications that work together.

Principle

- Define containers to start
- Bind mount as shared folders
- `/etc/hosts` to established relation

STAMUS NETWORKS

Amsterdam: SELKS meet Docker

SELKS components

- Suricata: latest release
- ELK: latest version including Kibana 4
- Evebox
- Scirius

Docker

- Using Compose
- With official ELK containers

STAMUS NETWORKS

Install Amsterdam

Installation

```
pip install amsterdam
# verify version
pip show amsterdam
# create an instance in the ams directory
amsterdam -d ams -i wlan0 setup
# start instance
amsterdam -d ams start
```

Utilisation

Point your browser to `https://localhost/` or on the IP of server if on an external box.

STAMUS NETWORKS

Amsterdamize your firewall

Install Amsterdam on your firewall

- Amsterdam on an existing firewall
- Sniff one of the network interfaces

Dashboards everywhere

- Firewall do logs
- Logs are not in the dashboards

STAMUS NETWORKS

At the beginning was syslog

Pre Netfilter days

- Flat packet logging
- One line per packet
  - A lot of information
  - Non searchable

STAMUS NETWORKS

At the beginning was syslog

Pre Netfilter days

- Flat packet logging
- One line per packet
  - A lot of information
  - Non searchable

Not sexy

```
INPUT DROP IN=eth0 OUT= MAC=00:1a:92:05:ee:68:00:b0:8e:83:3b:f0:08:00 SRC=62.212.121.211 DST=91.12
IN IN=eth0 OUT= MAC=d4:be:d9:69:d1:51:00:11:95:63:c7:5e:08:00 SRC=31.13.80.7 DST=192.168.11.3 LEN=
IN IN=eth0 OUT= MAC=d4:be:d9:69:d1:51:00:11:95:63:c7:5e:08:00 SRC=31.13.80.23 DST=192.168.11.3 LEN
IN IN=eth0 OUT= MAC=d4:be:d9:69:d1:51:00:11:95:63:c7:5e:08:00 SRC=31.13.80.7 DST=192.168.11.3 LEN=
IN IN=eth0 OUT= MAC=d4:be:d9:69:d1:51:00:11:95:63:c7:5e:08:00 SRC=31.13.80.7 DST=192.168.11.3 LEN=
```

STAMUS NETWORKS

Ulogd2: complete Netfilter logging

Ulogd2

- Interact with the post 2.6.14 libraries
- Rewrite of ulogd
- SCTP support (developed during @philpraxis talk at hack.lu 2008)
- multiple output and input through the use of stack

libnetfilter_log (generalized ulog)

- Packet logging
- IPv6 ready
- Few structural modification

libnetfilter_conntrack (new)

- Connection tracking logging
- Accounting, logging

Ulogd: output and configuration

Sexify output

- Syslog and file output
- SQL output: PGSQL, MySQL, SQLite
- Graphite
- JSON output

Some stack examples

```
stack=log2:NFLOG,base1:BASE,ifi1:IFINDEX, \
      ip2str1:IP2STR,mac2str1:HWHDR,json1:JSON
stack=ct1:NFCT,mark1:MARK,ip2str1:IP2STR,pgsql2:PGSQL
```

STAMUS NETWORKS

Plan of Amsterdam

Data directories

- backups
- elasticsearch, scirius
- suricata

Config files directories

- sub directories of config directory: evebox logstash nginx scirius suricata
- docker directory
- docker-compose.yml

STAMUS NETWORKS

Inject Ulogd2 data in Amsterdam

The suricata data directory

- Readable by logstash
- Any JSON files will be parsed by ulogd2

STAMUS NETWORKS

Inject Ulogd2 data in Amsterdam

The suricata data directory

- Readable by logstash
- Any JSON files will be parsed by ulogd2

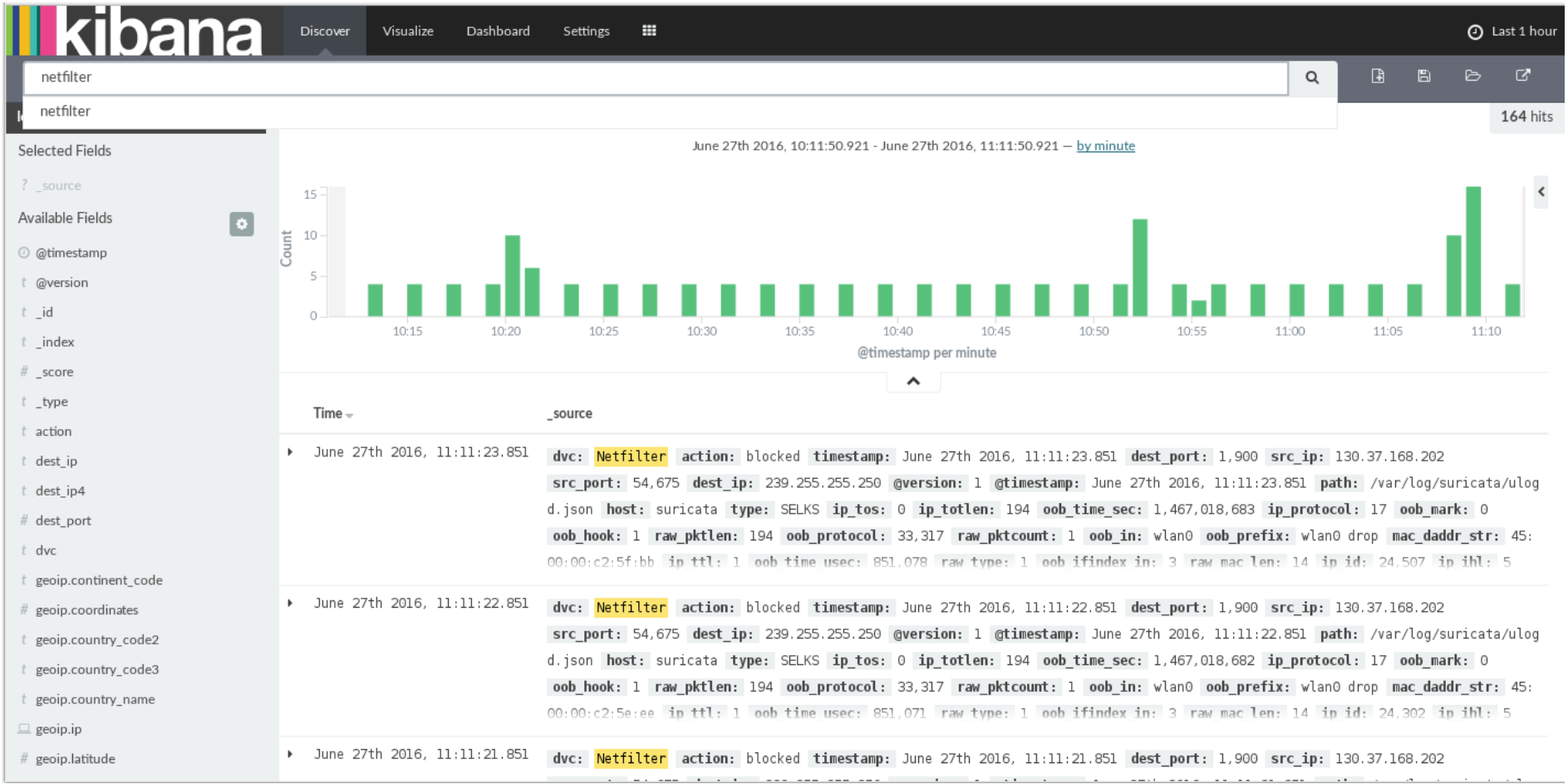
Inject data

- Update ulogd2 configuration
- Change output target:

```
[json1]
sync=1
file="/path/to/amsterdam/suricata/ulogd.json"
```

STAMUS NETWORKS

Ulogd2 in Amsterdam



STAMUS NETWORKS

Plotting TCP window at start

OS passive fingerprinting

- Value of TCP window at start is not specified in RFC
- The value is a choice of the OS
- We can use this for identification

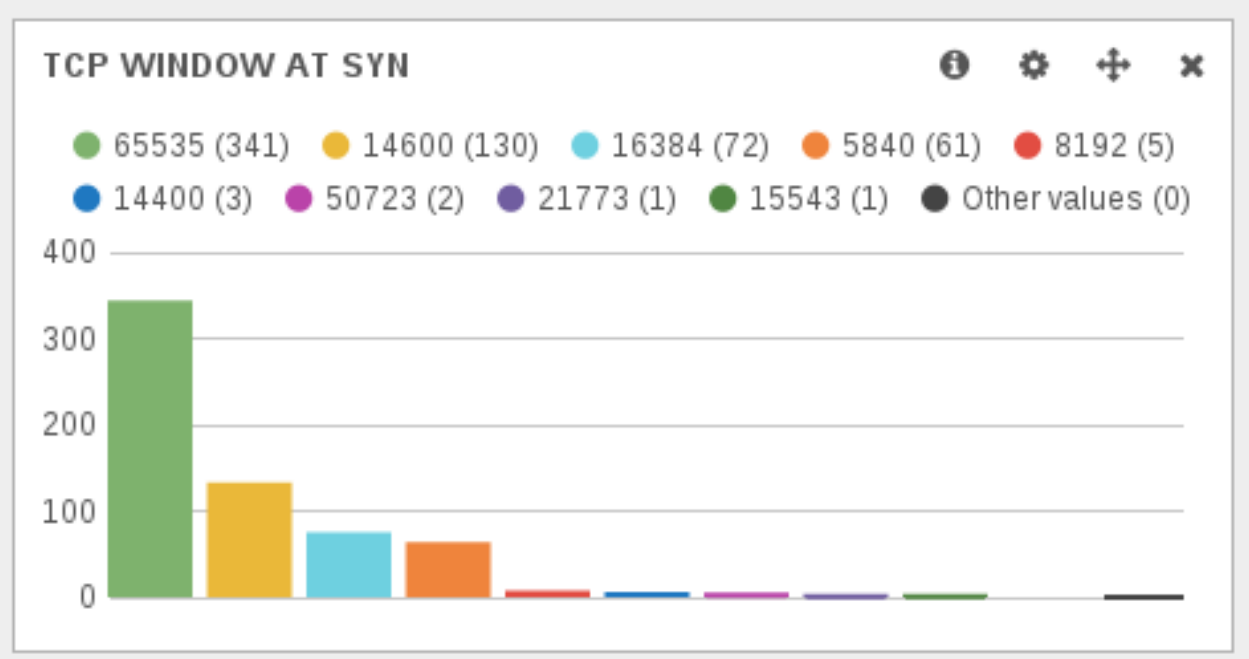
Value for some OSes

- 8192: Windows 7 SP1
- 65535: Mac OS X 10.2 - 10.7
- 14600: Some Linux
- 5840: Some other Linux

Source: `http://noc.to/#Help:TcpSynPacketSignature`

STAMUS NETWORKS

The facts



STAMUS NETWORKS

The facts

STAMUS NETWORKS

The facts

@timestamp	src_ip	src_port	dest_port
2014-02-02T12:58:11.735Z	61.174.51.219	6000	22
2014-02-02T12:55:24.699Z	222.186.62.20	6000	22
2014-02-02T12:49:04.621Z	222.186.62.42	6000	22
2014-02-02T12:28:28.150Z	222.186.62.53	6000	22
2014-02-02T12:26:02.045Z	61.160.195.250	6000	22
2014-02-02T12:21:00.961Z	61.160.215.5	6000	22
2014-02-02T11:45:40.916Z	61.174.51.201	6000	22
2014-02-02T11:44:09.874Z	115.230.126.87	6000	22

STAMUS NETWORKS

The facts

@timestamp	src_ip	src_port	dest_port	geoip.country_name	tcp.window
2014-01-31T08:11:15.314Z	61.160.223.102	6000	22	China	16384
2014-01-31T08:19:16.371Z	61.160.223.102	4585	22	China	65535
2014-01-31T08:20:08.378Z	61.160.223.102	1901	22	China	65535
2014-01-31T08:20:35.381Z	61.160.223.102	2363	22	China	65535
2014-01-31T08:20:44.383Z	61.160.223.102	2919	22	China	65535
2014-01-31T08:20:57.385Z	61.160.223.102	1208	22	China	65535
2014-01-31T08:21:07.387Z	61.160.223.102	4382	22	China	65535
2014-01-31T08:21:30.390Z	61.160.223.102	4519	22	China	65535
2014-01-31T08:21:51.393Z	61.160.223.102	4219	22	China	65535
2014-01-31T08:22:13.396Z	61.160.223.102	3548	22	China	65535
2014-01-31T08:22:33.399Z	61.160.223.102	1798	22	China	65535
2014-01-31T08:22:55.402Z	61.160.223.102	1275	22	China	65535
2014-02-02T10:56:04.435Z	61.160.223.102	6000	22	China	16384
2014-02-02T11:04:29.575Z	61.160.223.102	4075	22	China	65535
2014-02-02T11:04:52.582Z	61.160.223.102	4793	22	China	65535

STAMUS NETWORKS

Suricata meet Netfilter

Ulogd2 as an Amsterdam component

- Install ulogd2 inside a container
- Get the netlink message to the container

STAMUS NETWORKS

Suricata meet Netfilter

Ulogd2 as an Amsterdam component

- Install ulogd2 inside a container
- Get the netlink message to the container

Docker compose configuration

```
ulogd:
    build: /path/to/ams/docker/ulogd
    volumes:
        - /path/to/ams/suricata:/var/log/suricata:rw
        - /path/to/ams/config/ulogd/ulogd.conf:/etc/ulogd.conf:ro
    cap_add:
        - NET_ADMIN
    net: host
```

STAMUS NETWORKS

Add ulogd

Ulogd2 Dockerfile

```
FROM debian:jessie

run apt-get update
run DEBIAN_FRONTEND=noninteractive apt-get install -y ulogd2

CMD ["/usr/sbin/ulogd", "-c", "/etc/ulogd.conf"]
```

Start the system

```
amsterdam -d ams start
```

STAMUS NETWORKS

Elasticsearch 2.0 and backward compatibility

theuntergeek Aaron Mildenstein Logstash Developer Oct '15

Field names cannot contain the `.` character in Elasticsearch 2.0.

I apologize for the inconvenience this will be, but you'll have to change all field names to not have a period in them.

STAMVS NETWORKS

Get a fix in Amsterdam

Install logstash plugin: update docker/logstash/Dockerfile

```
FROM logstash:2.3

ADD elasticsearch-template.json /opt/logstash/vendor/bundle/jruby/1.9/gems

RUN /opt/logstash/bin/logstash-plugin install logstash-filter-de_dot
```

Install logstash config in config/logstash

```
filter {
   de_dot {
  }
...
```

STAMUS NETWORKS

Conclusion

Amsterdam

- Easy to install Suricata ecosystem
- Easy tuning

More information

- Suricata: `http://www.suricata-ids.org/`
- Amsterdam : `https://github.com/StamusNetworks/Amsterdam`
- Stamus Networks : `https://www.stamus-networks.com/`

STAMUS NETWORKS