Amsterdamize your firewall

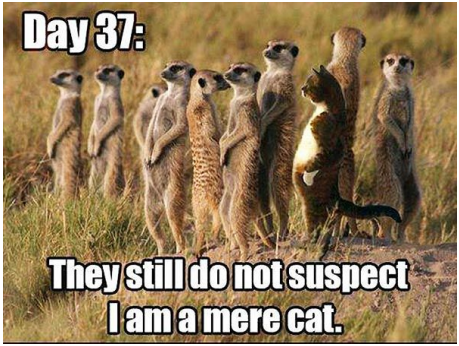
É. Leblond

Stamus Networks

July 5, 2016

STAMUS NETWORKS

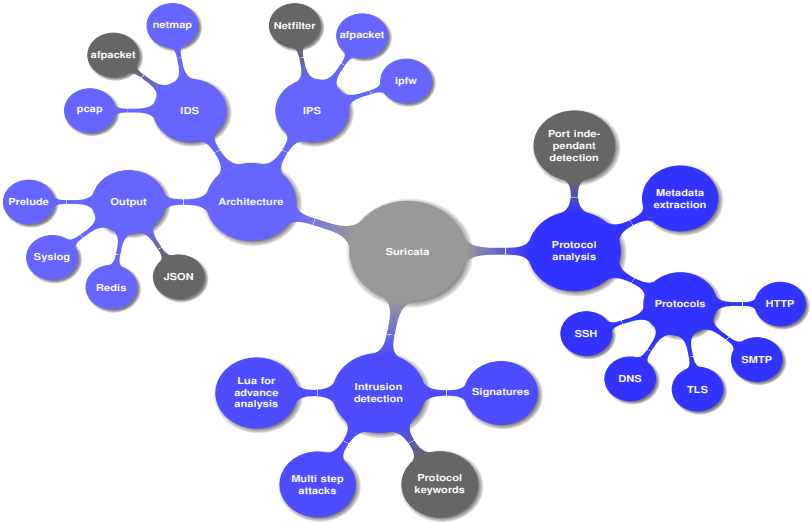
Éric Leblond



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

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

Content

- 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

Amsterdam: SELKS meet Docker

SELKS components

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

Docker

- Using Compose for orchestration
- With official ELK containers

STAMUS NETWORKS

Install Amsterdam

Installation

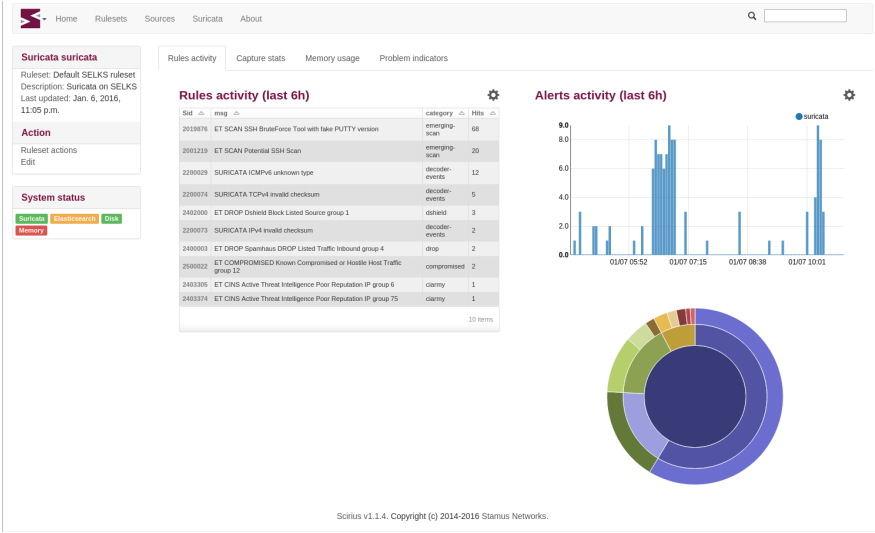
```
pip install amsterdam
# verify version
pip show amsterdam
# create an instance in the ams directory
amsterdam -d ams -i wlan0 setup
# start instance
amsterdam -d ams start
```

Utilisation

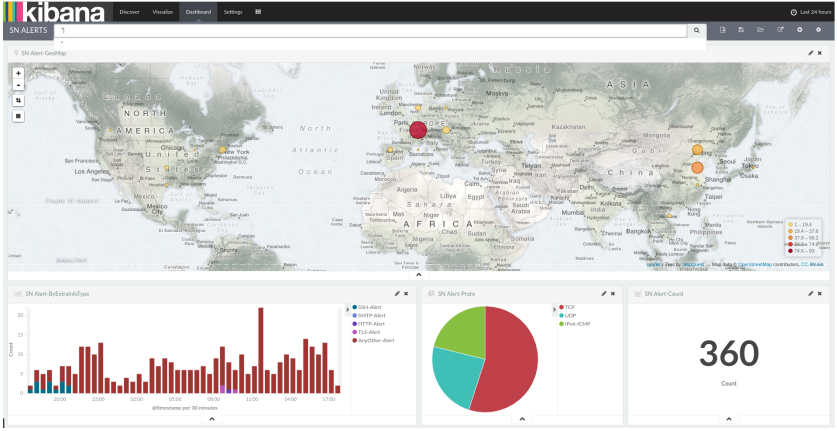
Point your browser to `https://localhost/` or on the IP of server if on an external box.

STAMUS NETWORKS

Scirius: ruleset management



Kibana


kibana
Discover
Visualize
Dashboard
Settings
Last 24 hours
SN ALERTS
SN Alert-GeoMap
NORTH AMERICA
United States
Canada
Mexico
Europe
ASIA
China
India
AFRICA
Sahara
Atlantic Ocean
SN Alert-ByExtraInfoType
SSH-Alert
SMTP-Alert
HTTP-Alert
TLS-Alert
AnyOther-Alert
Count
@timestamp per 30 minutes
SN Alert-Proto
TCP
UDP
IPv6-ICMP
SN Alert-Count
360
Count

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

Ulogd2: complete Netfilter logging

Ulogd2

- Interact with all Netfilter components
- Rewrite of ulogd
- 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

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

Elasticsearch 2.0 and backward compatibility

...

theuntergeek Aaron Mildenstein Logstash Developer Oct '15

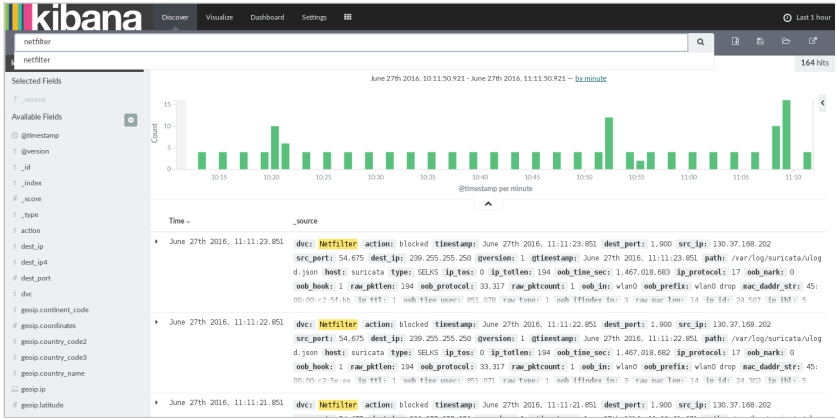
Field names cannot contain the `.` character in Elasticsearch 2.0.

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

Install logstash config in config/logstash

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

Ulogd in Kibana



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/`

Learn more

- Suricata developer training (Paris, September): `https://5-daydevtraining-paris.eventbrite.com/?discount=EarlyBird`
- Suricon (Washington, November):`http://suricon.net/`