Éric Leblond

Co-founder of Stamus Networks

- Company providing network probes based on Suricata
- Focusing on bringing you the best of Suricata IDS technology

OISF team member

- Core developer
- In charge of Suricata packet capture

Netfilter Coreteam member

- Work on kernel-userspace interaction
- Kernel hacking
- Ulogd2 maintainer
- Port of Openoffice firewall to Libreoffice

SELKS

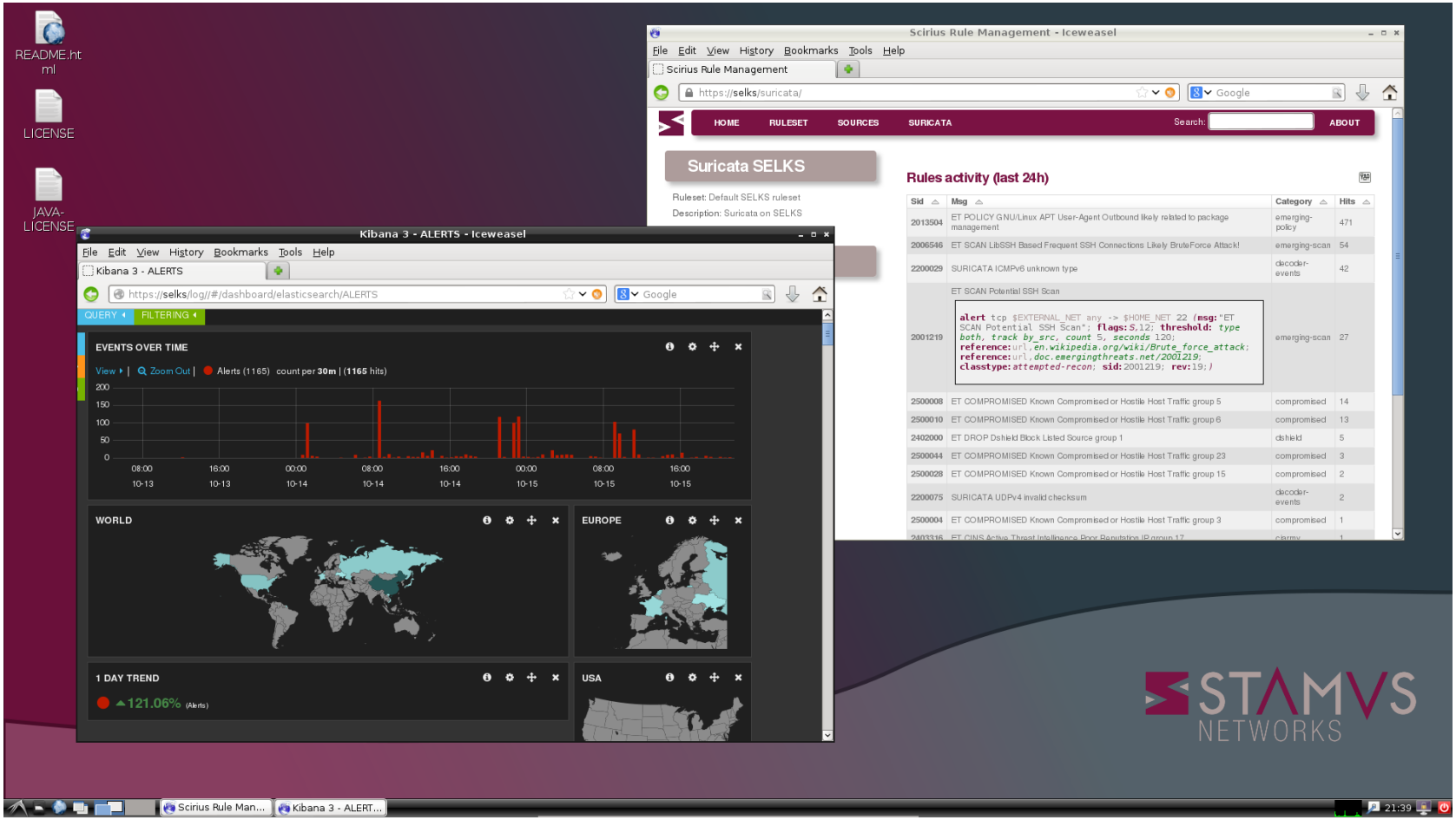
An installable and live ISO

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

Content

- Suricata: 2.1beta4 version
- 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

Screenshot: the desktop



What is Suricata?

- IDS and IPS engine
- Get it here:
  `http://www.suricata-ids.org`
- Open Source (GPLv2)
- Funded by US government and consortium members
- Run by Open Information Security Foundation (OISF)
- More information about OISF at
  `http://www.oisf.net/`

Suricata Features

- High performance, scalable through multi threading
- Protocol identification
- File identification, extraction, on the fly MD5 calculation
- TLS handshake analysis, detect/prevent things like Diginotar
- Hardware acceleration support:
  - Endace
  - Napatech,
  - CUDA
  - PF_RING

Suricata Features

- Rules and outputs compatible to Snort syntax
- useful logging like HTTP request log, TLS certificate log, DNS logging
- Lua scripting for detection

Suricata capture modes

IDS

- pcap: multi OS capture
- pf_ring: Linux high performance
- af_packet: Linux high performance on vanilla kernel
- ...

IPS

- NFQUEUE: Using Netfilter on Linux
- ipfw: Use divert socket on FreeBSD
- af_packet: Level 2 software bridge

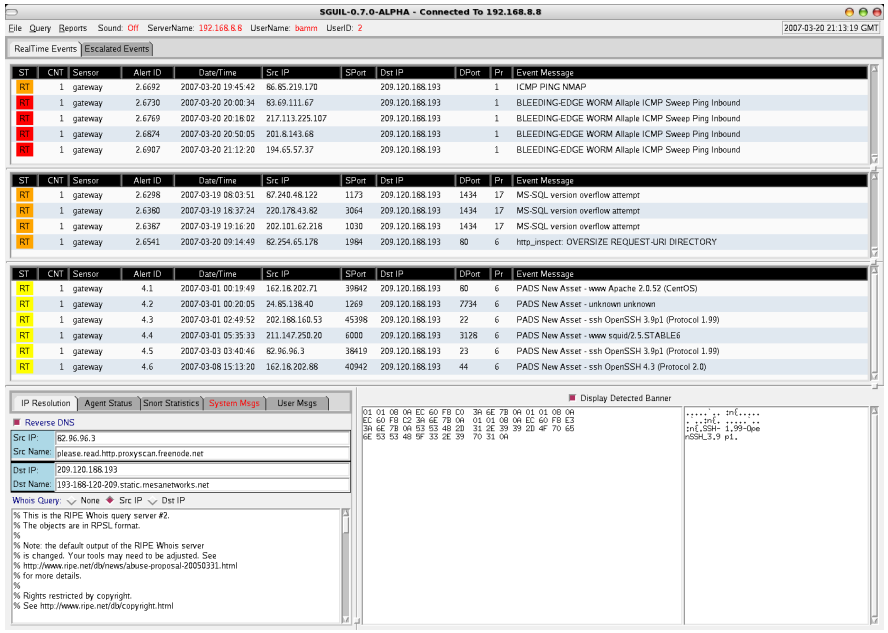
Offline analysis

- Pcap: Analyse pcap files
- Unix socket: Use Suricata for fast batch processing of pcap files

Defensive security

Total lack of sexiness

- Interface done by tech guys
- Good productivity
- But no fun



Defensive security

Let's get rid of the 90's

Let's kill unified2

- Binary format without real design
- Dedicated to alert
- Very hard to extend
- No API on devel side

We need something extensible

- To log alert and to log protocol request
- Easy to generate and easy to parse
- Extensible

JavaScript Object Notation

JSON

- JSON (`http://www.json.org/`) is a lightweight data-interchange format.
- It is easy for humans to read and write.
- It is easy for machines to parse and generate.
- An object is an unordered set of name/value pairs.

Logging in JSON

```
{"timestamp":"2012-02-05T15:55:06.661269", "src_ip":"173.194.34.51",
 "dest_ip":"192.168.1.22",
 "alert":{"action":"allowed",rev":1,"signature":"SURICATA TLS store"}}
```

Alert

The structure

- IP information are identical for all events and alert
- Follow Common Information Model
- Allow basic aggregation for all Suricata events and external sources

Example


```
{"timestamp":"2014-03-06T05:46:31.170567","event_type":"alert",
 "src_ip":"61.174.51.224","src_port":2555,
 "dest_ip":"192.168.1.129","dest_port":22,"proto":"TCP",
 "alert":{"action":"Pass","gid":1,"signature_id":2006435,"rev":8,
          "signature":"ET SCAN LibSSH Based SSH Connection - Often used as
          "category":"Misc activity","severity":3}
}
```

Network Security Monitoring

Protocols

- HTTP
- File
- TLS
- SSH
- DNS

Example


```
{"timestamp":"2014-04-10T13:26:05.500472","event_type":"ssh",
 "src_ip":"192.168.1.129","src_port":45005,
 "dest_ip":"192.30.252.129","dest_port":22,"proto":"TCP",
 "ssh":{
  "client":{
    "proto_version":"2.0","software_version":"OpenSSH_6.6p1 Debian-2" },
  "server":{
    "proto_version":"2.0","software_version":"libssh-0.6.3"}
 }
}
```

Pcap is dead

Enlarge your alerts: add metadata

- IDS is not a network grep anymore
- It alerts on reconstructed protocol data
  - De gzipped body in a HTTP answer
  - TLS fingerprint in a TLS handshake

Example


```
{"timestamp":"2014-04-10T13:26:05.500472","event_type":"alert",
 "src_ip":"192.168.1.129","src_port":45005,
 "dest_ip":"192.30.252.129","dest_port":22,"proto":"TCP",
 "alert":{"action":"Pass","gid":1,"signature_id":2006435,"rev":8,
          "signature":"ET SCAN LibSSH Based SSH Connection - Often used as
          "category":"Misc activity","severity":3}
 "ssh":{
  "client":{
    "proto_version":"2.0","software_version":"OpenSSH_6.6p1 Debian-2" },
  "server":{
    "proto_version":"2.0","software_version":"libssh-0.6.3"}
 }
}
```

ELK

- Elasticsearch is a distributed restful search and analytics
- Full text search, schema free
- Apache 2 open source license
- ELK stack
  - Elasticsearch
  - Logstash: log shipping
  - Kibana: web interface

Elasticsearch key points

- REST API
- Cluster capacity
- Data redundancy

Logstash

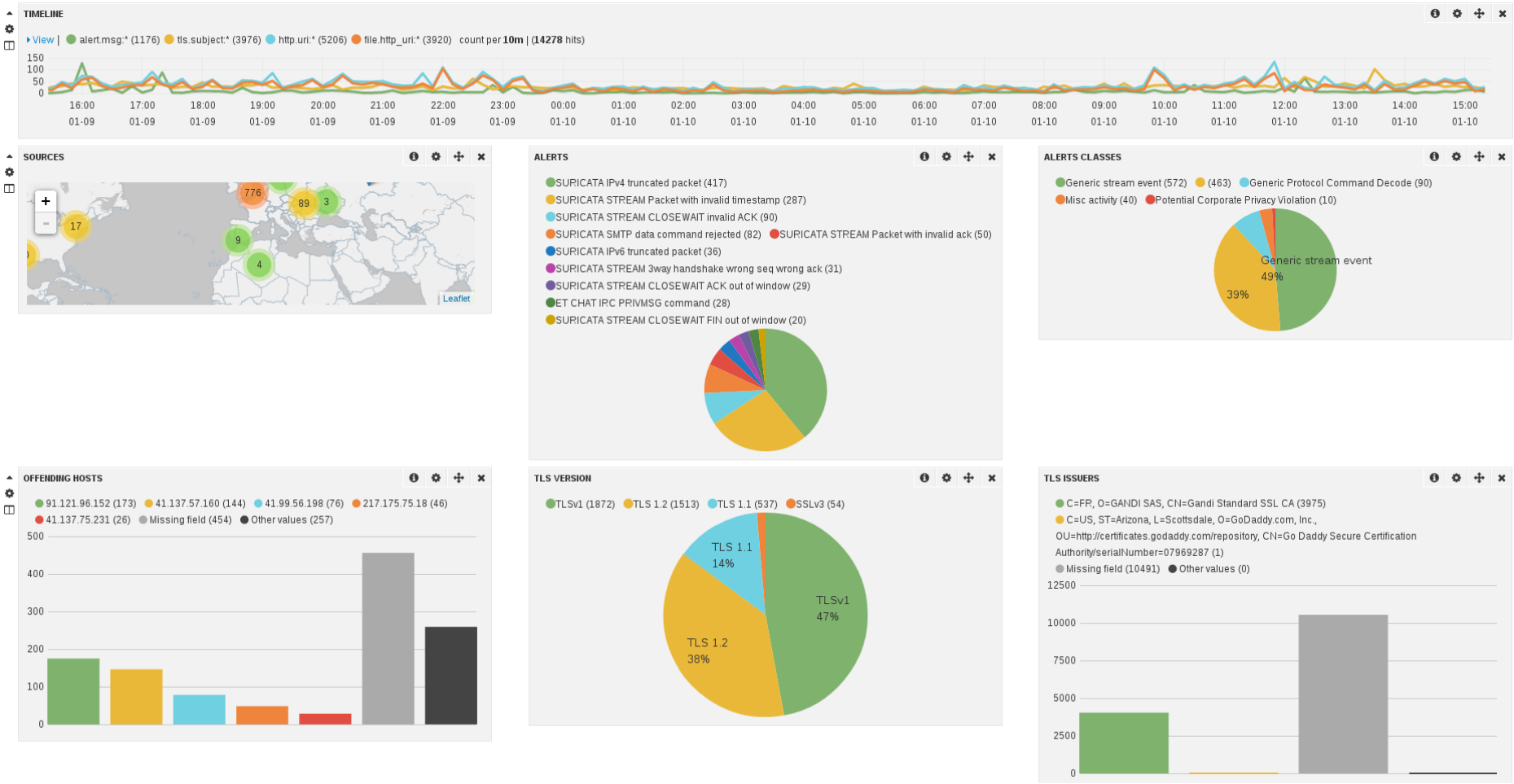
A tool for managing events and logs

- Collect logs, parse them, and store them in different outputs
  - elasticsearch
  - graphite
  - IRC
  - ...
- Apache 2.0 license
- Java and ruby

A simple configuration (for JSON)

```
input {
   file {
      path => [ "/var/log/suricata/eve.json", "/var/log/ulogd.json"]
      codec =>   json
   }
}
```

Kibana


TIMELINE
View | alert.msg:* (1176) tls.subject:* (3976) http.uri:* (5206) file.http_uri:* (3920) count per 10m | (14278 hits)
150
100
50
0
16:00 01-09
17:00 01-09
18:00 01-09
19:00 01-09
20:00 01-09
21:00 01-09
22:00 01-09
23:00 01-09
00:00 01-10
01:00 01-10
02:00 01-10
03:00 01-10
04:00 01-10
05:00 01-10
06:00 01-10
07:00 01-10
08:00 01-10
09:00 01-10
10:00 01-10
11:00 01-10
12:00 01-10
13:00 01-10
14:00 01-10
15:00 01-10
SOURCES
776
89
3
17
9
4
Leaflet
ALERTS
SURICATA IPv4 truncated packet (417)
SURICATA STREAM Packet with invalid timestamp (287)
SURICATA STREAM CLOSEWAIT invalid ACK (90)
SURICATA SMTP data command rejected (82)
SURICATA STREAM Packet with invalid ack (50)
SURICATA IPv6 truncated packet (36)
SURICATA STREAM 3way handshake wrong seq wrong ack (31)
SURICATA STREAM CLOSEWAIT ACK out of window (29)
ET CHAT IRC PRIVMSG command (28)
SURICATA STREAM CLOSEWAIT FIN out of window (20)
ALERTS CLASSES
Generic stream event (572)
(463)
Generic Protocol Command Decode (90)
Misc activity (40)
Potential Corporate Privacy Violation (10)
Generic stream event
49%
39%
OFFENDING HOSTS
91.121.96.152 (173)
41.137.57.160 (144)
41.99.56.198 (76)
217.175.75.18 (46)
41.137.75.231 (26)
Missing field (454)
Other values (257)
500
400
300
200
100
0
TLS VERSION
TLSv1 (1872)
TLS 1.2 (1513)
TLS 1.1 (537)
SSLv3 (54)
TLS 1.1
14%
TLSv1
47%
TLS 1.2
38%
TLS ISSUERS
C=FR, O=GANDI SAS, CN=Gandi Standard SSL CA (3975)
C=US, ST=Arizona, L=Scottsdale, O=GoDaddy.com, Inc., OU=http://certificates.godaddy.com/repository, CN=Go Daddy Secure Certification Authority/serialNumber=07969287 (1)
Missing field (10491)
Other values (0)
12500
10000
7500
5000
2500
0

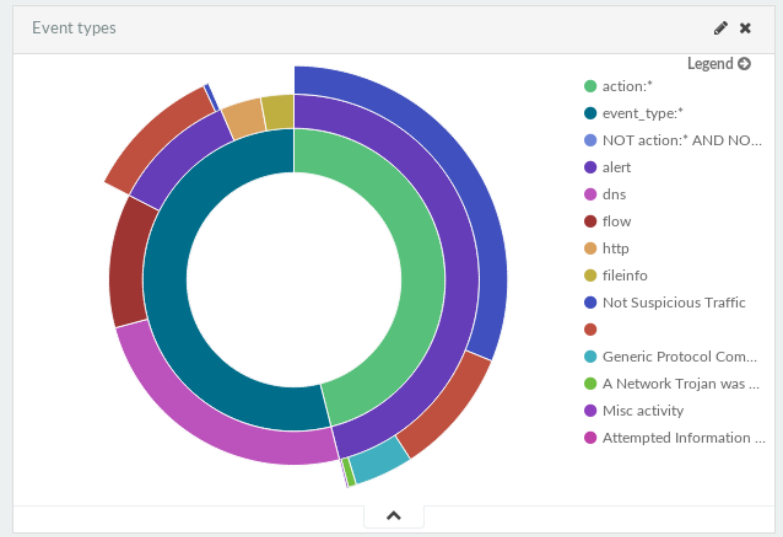
Kibana

Main points

- Dashboard application
- Javascript based
- Get data and configuration from Elasticsearch
- Drill down approach

Version 3 vs version 4

- Version 4 is a rewrite
- Use latest Elasticsearh features
  - Multi level aggregation
- More complex logic
- No dashboards export



Scirius

A web application

- Developed in Python
- A Django based application
- Using d3js and nvd3 for graphing

Available under GPLv3

- Github: `https://github.com/StamusNetworks/Scirius`
- Developed by Stamus Networks

Scirius

A web application

- Developed in Python
- A Django based application
- Using d3js and nvd3 for graphing

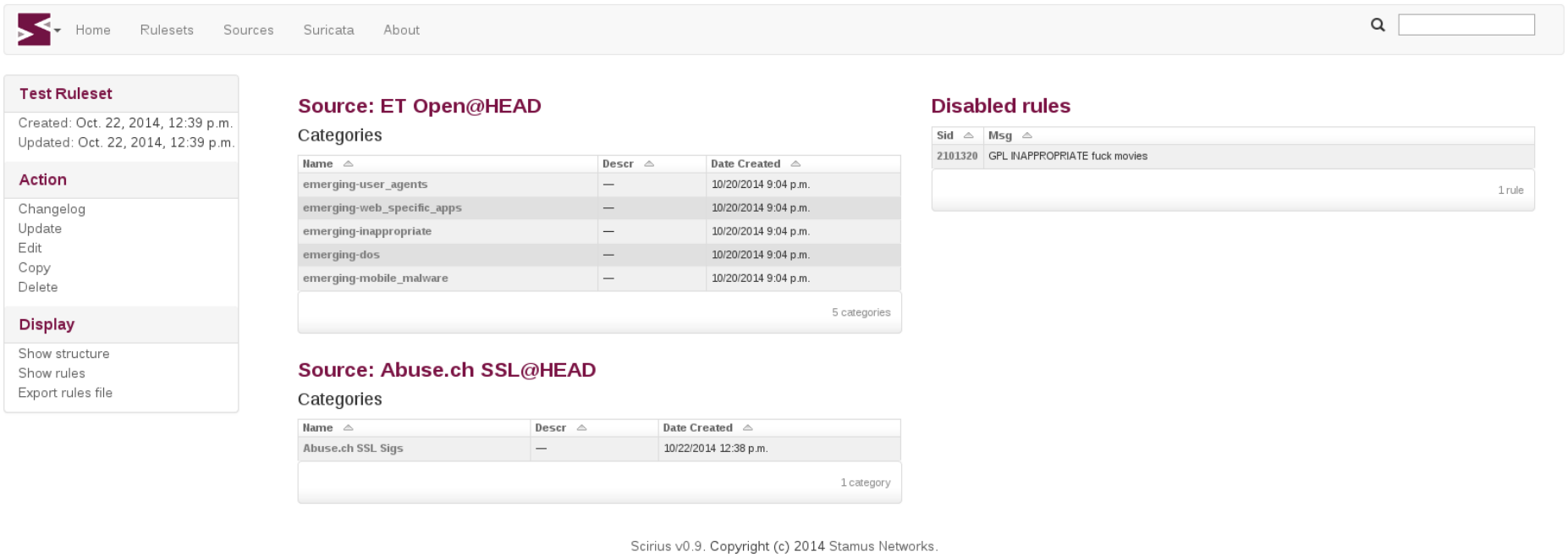
Available under GPLv3

- Github: `https://github.com/StamusNetworks/Scirius`
- Developed by Stamus Networks

SciEnt

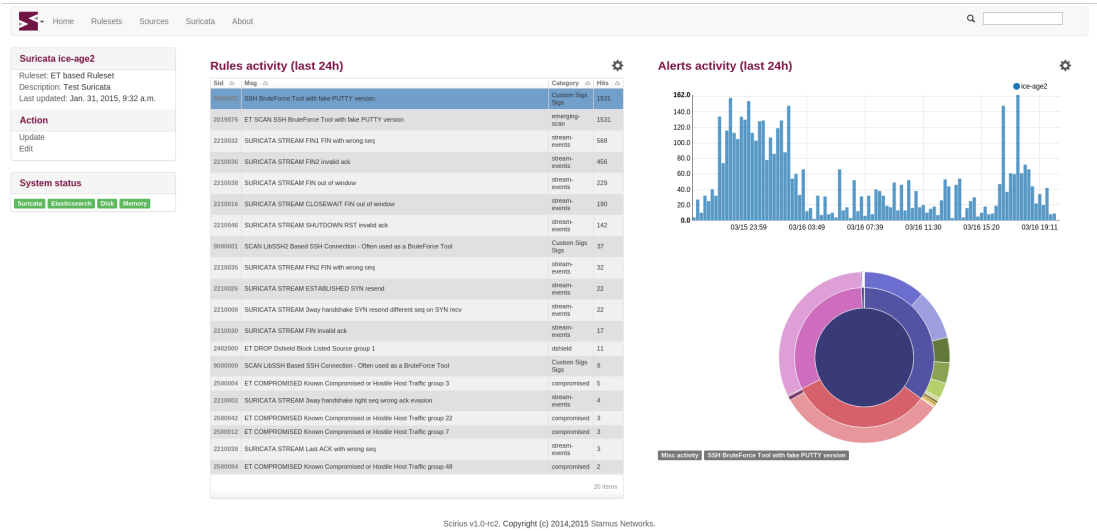
- Scirius Enterprise with multi probes support

Screenshot and demo: Scirius



Scirius rules handling

- Arbitrary sources
- Uploaded or fetched
- Categories handling
- Graphing to detect noisy signatures



Get SELKS up (and running) in 30 seconds

- Start a VM with the ISO as live CD
  - At least 2Gb of RAM (4Gb recommended and necessary for prod usage)
  - Maximum of core possible
  - Bridged network interface with promiscuous enable (will capture host trafic)
- Connect your browser
- Watch the data flow in dashboards

SELKS dashboards

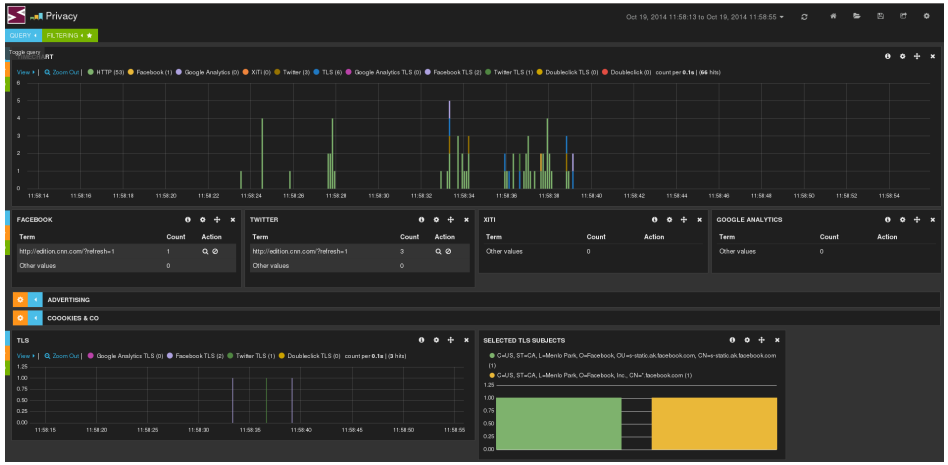
10+ Suricata dashboards

- Pre installed
- `https://github.com/pevma/Suricata-Logstash-Templates`

List

TLS , ALL , VLAN , HTTP , PRIVACY , FLOW , HTTP-Extended-Custom , ALERTS , SMTP , SSH , DNS , FILE-Transactions

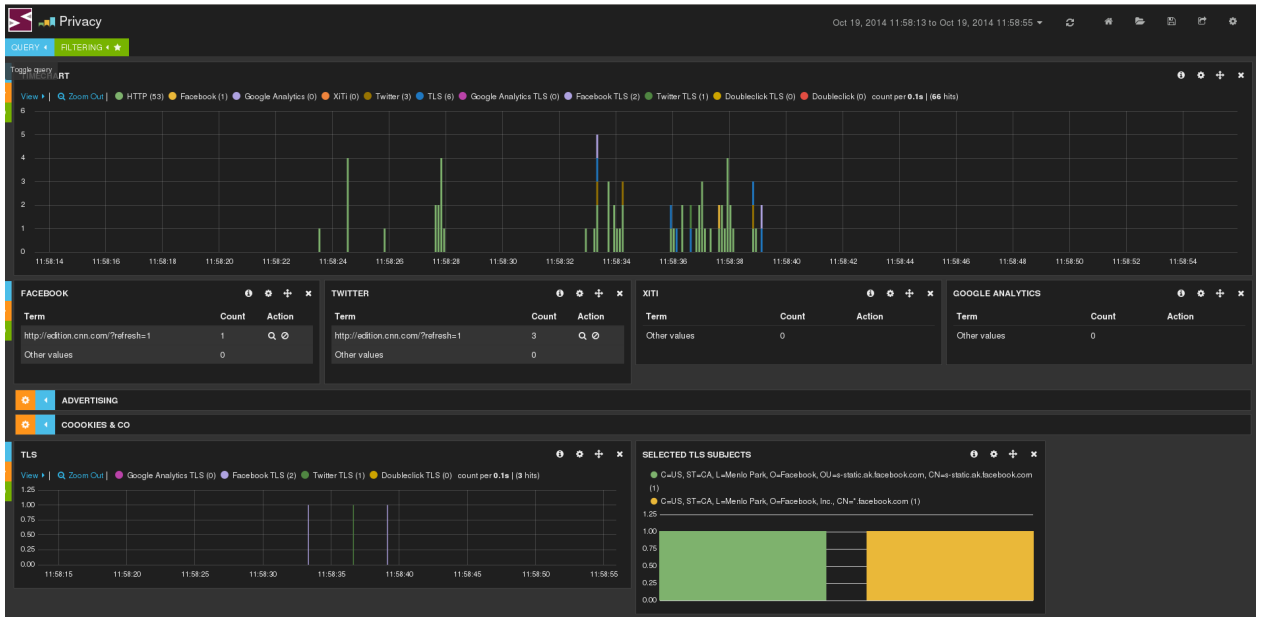
Alert dashboard: small demo



Custom Kibana

- Kibana 3
- Patched: link and alert info

SELKS and privacy dashboard: small demo



https://www.youtube.com/watch?v=wXtgHRmZkNc

SELKS availability

Available under GPLv3

- ready to use ISO
- Developed by Stamus Networks

Two flavours

- Desktop
- No desktop

Build your own

- Github: `https://github.com/StamusNetworks/SELKS`
- Wiki: `https://github.com/StamusNetworks/SELKS/wiki/Building-SELKS`

SELKS monitoring

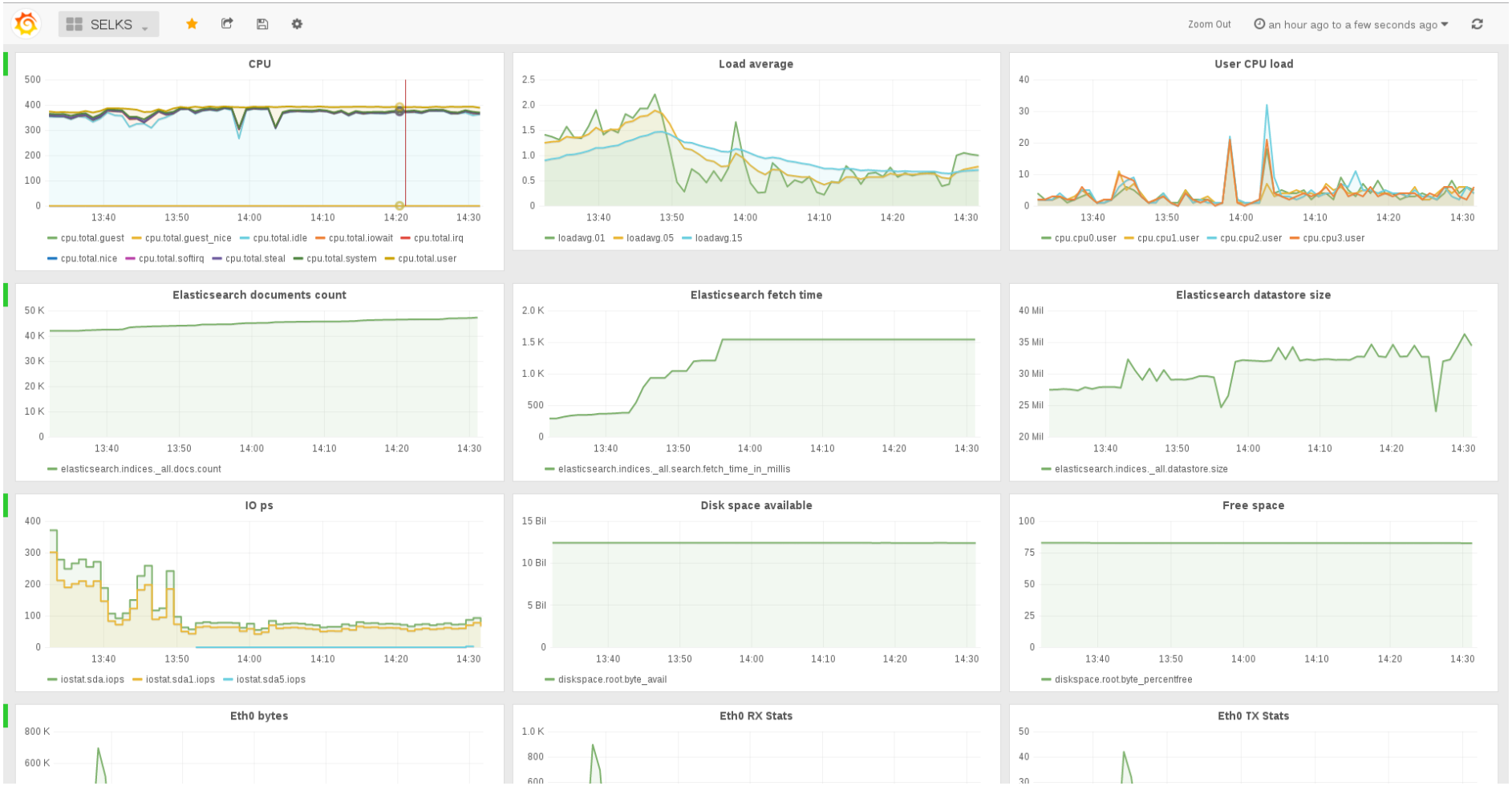
Improve understanding

- Graph performance data
- Allow easier tuning

Components

- influxdb
- telegraf
- grafana

Screenshot: upcoming monitoring



Project Amsterdam: SELKS and Docker

Docker

- An open platform for distributed applications for developers and sysadmins
- Lightweight containers
- See Jerome Petazzoni talk tomorrow

2 commands installation

- Make SELKS pullable from docker hub
- Start a container sniffing on a physical interface

Conclusion

Don't fear to be sexy

- Sexy charts and interfaces are not only for finance guys thanks to Elasticsearch
- Suricata can boost the sex appeal of network monitoring
- Use SELKS to get an impression of the mix

More information

- SELKS: `https://www.stamus-networks.com/open-source/#selks`
- SELKS wiki: `https://github.com/StamusNetworks/SELKS/wiki`
- Suricata user conference: `http://oisfevents.net/`
- Elasticsearch: `http://www.elasticsearch.org/`