



**SELKS**

# Lets talk about US

## **Stamus Networks**

Bring professional grade products and services through the Suricata IDPS eco-system

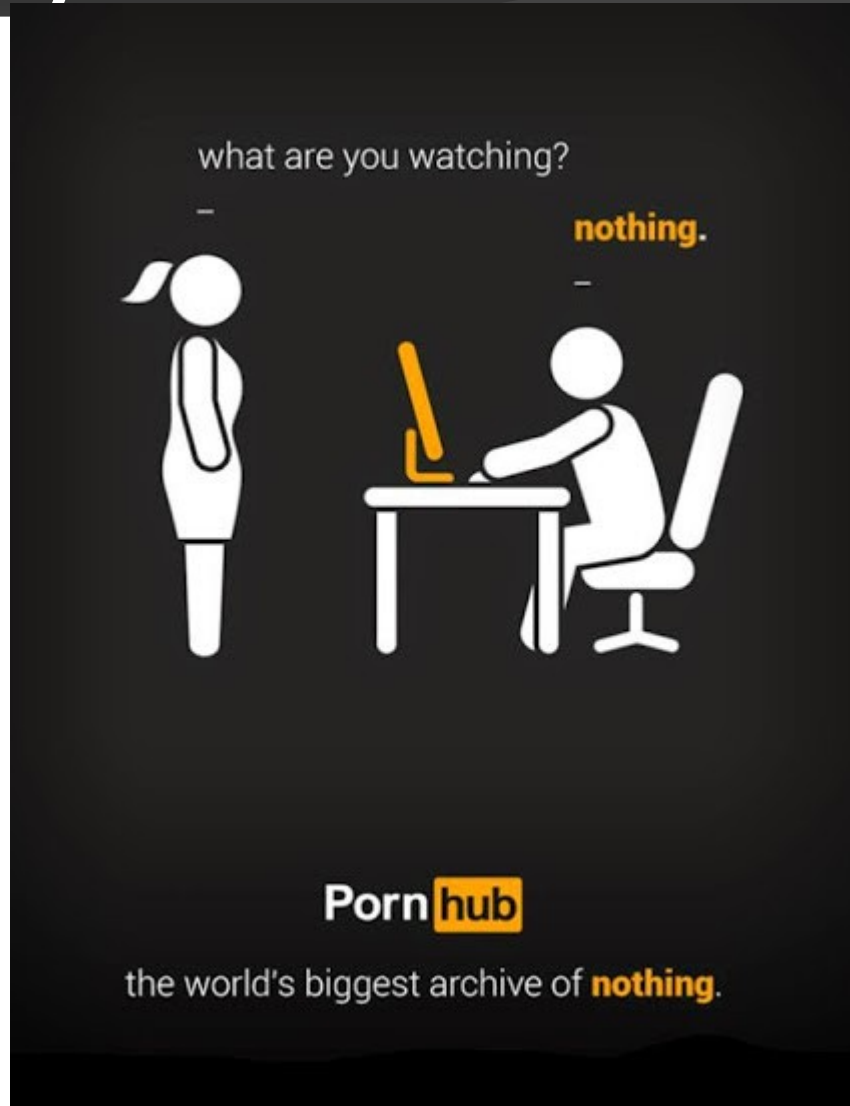
## **Open Source Projects**

- SELKS
- Amsterdam
- Scirius Community Edition

## **Products**

- Scirius Enterprise Edition
- Stamus Network Probes

# Problem of defensive security

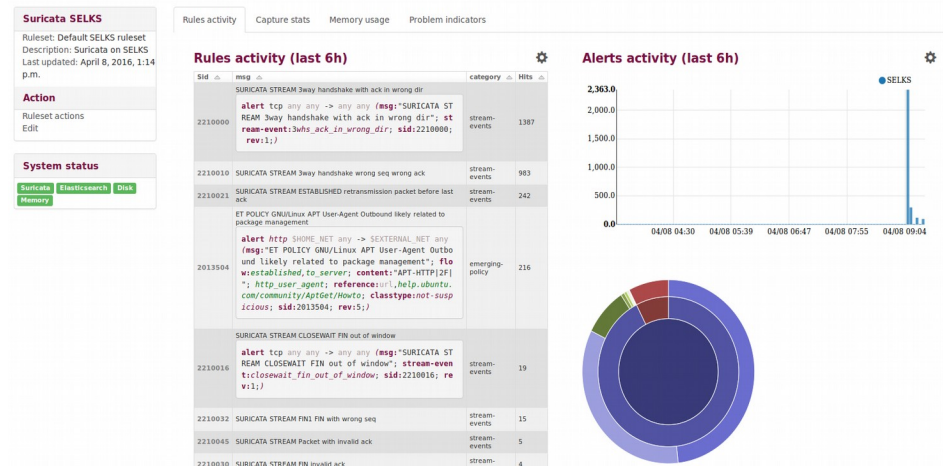
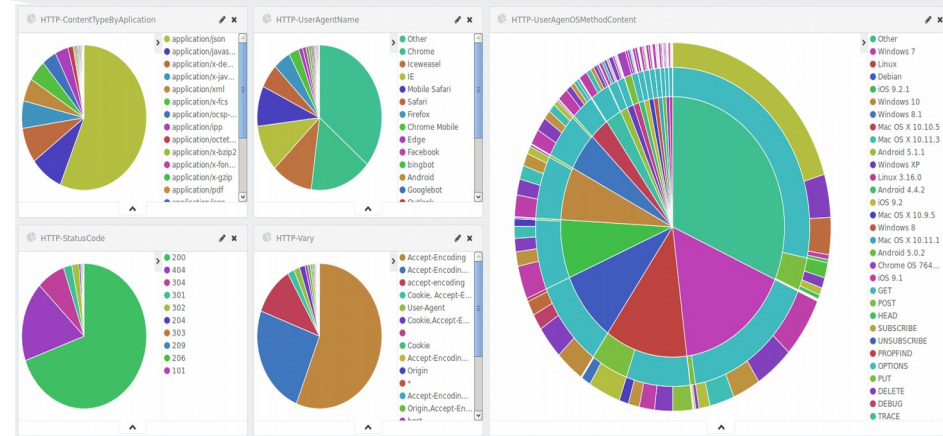


# Why we need SELKS ?

- Entirely Open Source
  - The only graphic Suricata's rule manager
  - Standard Debian Jessie 64 bit live and installable distro
  - Want to get the best out of Suricata
  - Showcase build for Suricata
- Scalable
- Modular
- Flexible
- Correlate

# Why this SELKS name ?

- **S** - Suricata IDPS
- **E** - Elasticsearch
- **L** - Logstash
- **K** - Kibana
- **S** - Scirius
- EveBox



# SELKS – The ELK stack

- **Elasticsearch 2.x**
  - Distributed, scalable, and highly available
  - Real-time search and analytics capabilities
  - Sophisticated RESTful API
  - Schema free, Apache Lucene™
- **Logstash 2.x**
  - Centralize data processing of all types
  - Log collector
- **Kibana 4.x**
  - Flexible analytics and visualization platform
  - Real-time summary and charting of streaming data
  - Intuitive interface for a variety of users
  - Instant sharing and embedding of dashboards

# SELKS - Scirius

- Suricata graphic rule set manager

**Suricata SELKS**

Ruleset: Default SELKS ruleset  
 Description: Suricata on SELKS  
 Last updated: May 5, 2015, 6:20 p.m.

---

**Action**

Update  
 Edit

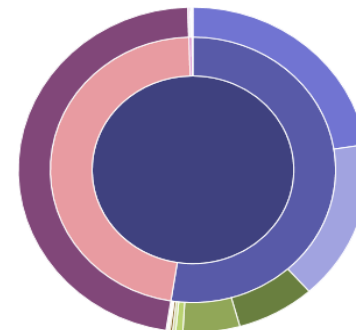
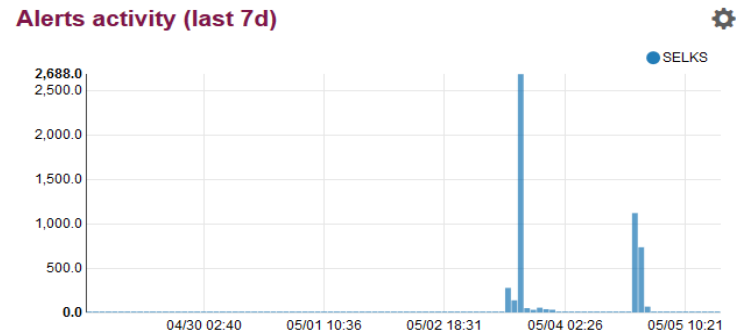
---

**System status**

Suricata Elasticsearch Disk  
 Memory

**Rules activity (last 7d)** ⚙

| Sid     | msg  | category         | Hits |
|---------|--|------------------|------|
| 2013504 | ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management   | emerging-policy  | 2489 |
| 2210000 | SURICATA STREAM 3way handshake with ack in wrong dir   | stream-events    | 1191 |
| 2210010 | SURICATA STREAM 3way handshake wrong seq wrong ack   | stream-events    | 842  |
| 2210021 | SURICATA STREAM ESTABLISHED retransmission packet before last ack  | stream-events    | 383  |
| 2200029 | SURICATA ICMPv6 unknown type   | decoder-events   | 278  |
| 2210042 | SURICATA STREAM TIMEWAIT ACK with wrong seq  | stream-events    | 35   |
| 2210045 | SURICATA STREAM Packet with invalid ack  | stream-events    | 15   |
| 2210044 | SURICATA STREAM Packet with invalid timestamp  | stream-events    | 13   |
| 2014799 | ET POLICY OpenVPN Update Check<br><br><b>alert http \$HOME_NET any -&gt; \$EXTERNAL_NET any (msg:"ET POLICY OpenVPN Update Check"; flow:established,to_server; content:"Host 3a  swupdate.openvpn.net 0d 0 a "; fast_pattern:14,14; http_header; content:"User-Agent 3a  Twisted PageGetter 0d 0a "; http_header; classtype:policy-violation; sid:2014799; rev:2;)</b> | emerging-policy  | 8    |
| 2210046 | SURICATA STREAM SHUTDOWN RST invalid ack   | stream-events    | 7    |
| 2018959 | ET POLICY PE EXE or DLL Windows file download HTTP   | emerging-policy  | 6    |
| 2008438 | ET MALWARE Possible Windows executable sent when remote host claims to send a Text File  | emerging-malware | 6    |
| 2210029 | SURICATA STREAM ESTABLISHED invalid ack  | stream-events    | 5    |
| 2210030 | SURICATA STREAM FIN invalid ack  | stream-events    | 3    |
| 2210020 | SURICATA STREAM ESTABLISHED packet out of window   | stream-events    | 2    |
| 2100230 | GPL CHAT Jabber/Google Talk Outgoing Traffic   | emerging-chat    | 2    |
| 2210038 | SURICATA STREAM FIN out of window  | stream-events    | 1    |
| 2200073 | SURICATA IPv4 invalid checksum   | decoder-events   | 1    |
| 2100232 | GPL CHAT Google Talk Logon   | emerging-chat    | 1    |
| 2002334 | ET CHAT Google IM traffic Jabber client sign-on  | emerging-chat    | 1    |



Potential Corporate Privacy Violation ET POLICY OpenVPN Update Check

# SELKS - EveBox

- EveBox is a web based Suricata "eve" event viewer for Elastic Search

The screenshot displays the SELKS EveBox interface. On the left, a web browser shows a search result for the event AVP2DIC5IZAhvkR9pIfA. The search details include Source (10.0.2.15:43442), Destination (184.72.244.137:80), In Interface (eth0), and Flow ID (1752768676). The HTTP details pane shows the request method (GET), URL (/kibana/4.5/debian/dists/stable/main/i18n/Translation-en), and user agent (Debian APT-HTTP/1.3 (1.0.9.8.3)).

On the right, Wireshark displays the captured packet. The packet list shows a single packet (No. 1) at time 0.000000, source 10.0.2.15, and destination 184.72.244.137, protocol HTTP, length 227 bytes. The packet details pane shows the Transmission Control Protocol (Src Port: 43442, Dst Port: 80) and Hypertext Transfer Protocol (Request Method: GET, Request URI: /kibana/4.5/debian/dists/stable/main/i18n/Translation-en, Request Version: HTTP/1.1, Host: packages.elastic.co, Cache-Control: max-age=0, Accept: text/\*, User-Agent: Debian APT-HTTP/1.3 (1.0.9.8.3)).

The packet bytes pane shows the raw data of the HTTP request, including the GET method, host, cache-control, accept, and user-agent headers, followed by the request URI and a blank line.



# Visualization & Filtering

- Filter and visualize on over 360 metadata fields
- GeolP Maps

# Dashboards

- 11 ready to use out of the box dashboards
  - ALL
  - ALERTS
  - DNS
  - FILE-Transactions
  - FLOW
  - HTTP
  - SMTP
  - STATS
  - TLS
  - SSH
  - VLAN

# Scirius: rule set manager

- Suricata's graphic rule set management
  - Rules to alerts direct mapping
  - Suricata performance indicators
  - Thresholding/Suppression of alerts
- Demonstration

# Black (file) Magic

Identify a file which:

- is a picture taken with a camera from Huawei Nexus 6p phone
- has a an extension “.docx”

# Getting SELKS

## Source & ISO:

- Build your from source or with a custom kernel version -
  - <https://github.com/StamusNetworks/SELKS#selks>
- Download ready to use ISO image -
  - <https://www.stamus-networks.com/open-source/#selks>

# Amsterdam

- SELKS and docker
  - Docker: lightweight containers
  - Docker-compose: orchestration
- Install amsterdam:
  - `pip install amsterdam`
- Create a amsterdam instance:
  - `amsterdam -d ams -i wlan0 setup`
  - `amsterdam -d ams start`
- Point browser to `https://localhost/`

# THANK YOU

# Questions ?