

# Let's talk about SELKS

Éric Leblond

Stamus Networks

5 juin 2014

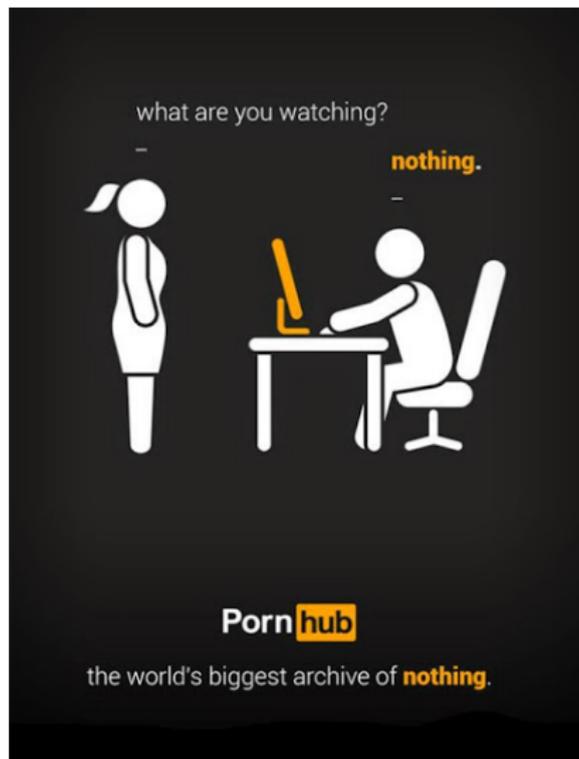
eleblond@stamus-networks.com

- Fondateur de Stamus Networks
- Core développeur de l'IDS/IPS Suricata

eric@regit.org

- Travail sur les interactions noyau-espace utilisateur
- Hacking noyau
- Mainteneur de ulogd2
- @Regiteric sur twitter





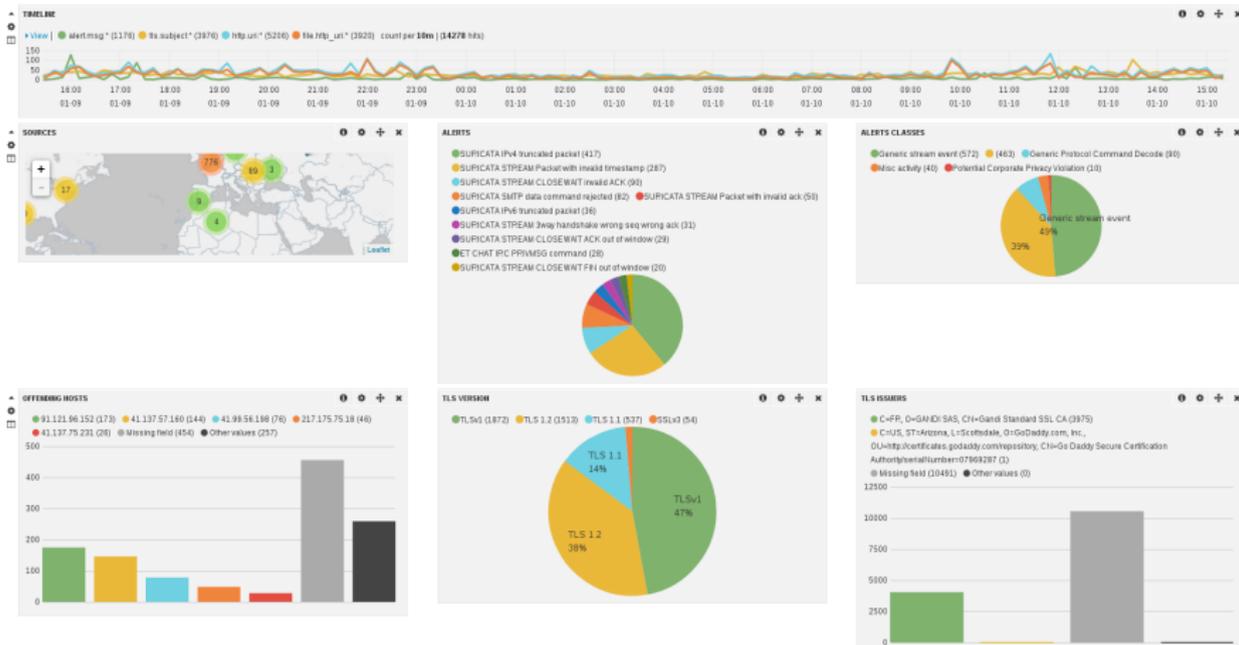
## EVE

- Nouvelle sortie unifiée en JSON
- Branchement facile de solutions comme Logstash ou Splunk

## Contenu

- Alertes
- Événements :
  - HTTP
  - File
  - TLS
  - DNS
  - SSH

# Suricata + Kibana



# Un exemple d'événements

```
{
  "timestamp": "2014-06-05T09:59:03.829619",
  "event_type": "ssh",
  "src_ip": "1.2.3.4", "src_port": 49316,
  "dest_ip": "4.5.6.7", "dest_port": 22,
  "proto": "TCP",
  "ssh": {
    "client": {
      "proto_version": "2.0",
      "software_version": "libssh-0.1"
    },
    "server": {
      "proto_version": "2.0",
      "software_version": "OpenSSH_6.6.1p1 Debian-5"
    }
  }
}
```

# Deny On Monitoring

---

```
def main_task(args):
    setup_logging(args)
    file = open(args.file, 'r')
    while 1:
        where = file.tell()
        line = file.readline()
        if not line:
            # Dodo
            time.sleep(0.3)
            file.seek(where)
        else:
            try:
                event = json.loads(line)
            except json.decoder.JSONDecodeError:
                time.sleep(0.3)
                break
            if event['event_type'] == 'ssh':
                if 'libssh' in event['ssh']['client']['software_version']:
                    # Vas-y Francis, c'est bon bon bon
                    call([IPSET, 'add', args.ipset, event['src_ip']])
```

---

## Quelques retours utilisateurs

## Quelques retours utilisateurs

Dom est une des protections essentielles du réseau du FMI

---

Christine Lagarde

## Quelques retours utilisateurs

Dom est une des protections essentielles du réseau du FMI

---

Christine Lagarde

Dom, c'est vraiment bien contre le scan de porc

---

Marcela Lacub

## Quelques retours utilisateurs

Dom est une des protections essentielles du réseau du FMI

---

Christine Lagarde

Dom, c'est vraiment bien contre le scan de porc

---

Marcela Lacub

Dom, y nique trop de scans

---

Dodo la saumure

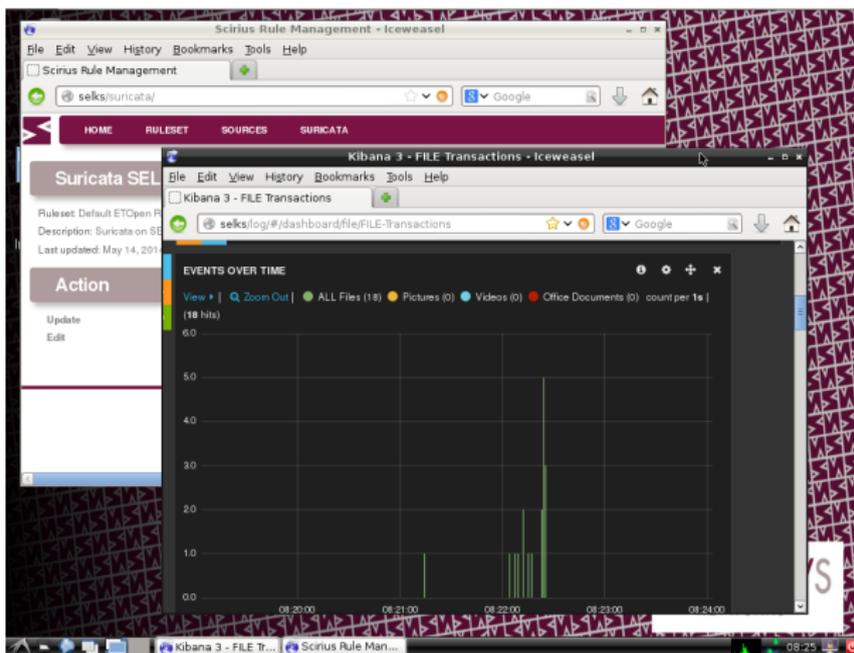
## Une ISO live et installable

- Basée sur debian live
- Un Suricata configuré et gérable par le web

## Contenu

- Suricata : en version 2.0.1
- Elasticsearch : base de données, recherche plein texte.
- Logstash : collecte des infos et stockage dans Elasticsearch
- Kibana : interface d'analyse des données
- Scirius : interface web de management de ruleset

# Capture d'écrans : le bureau



# Capture d'écrans : Scirius

**HOME**   **RULESET**   **SOURCES**   **SURICATA**   **ABOUT**

## Default ETOpen Ruleset

Created: May 14, 2014, 7:51 a.m.  
Updated: May 19, 2014, 9:19 a.m.

### Action

- Update
- Edit
- Copy
- Delete

### Display

- Show structure
- Show rules
- Export rules file

## Source: ETOpen Ruleset@HEAD

### Categories

Name <small>▲</small>	Descr <small>▲</small>	Date Created <small>▲</small>
emerging-smp	—	05/14/2014 7:50 a.m.
emerging-icmp	—	05/14/2014 7:50 a.m.
emerging-user_agents	—	05/14/2014 7:50 a.m.
emerging-web_specific_apps	—	05/14/2014 7:50 a.m.
emerging-inappropriate	—	05/14/2014 7:50 a.m.
emerging-activex	—	05/14/2014 7:50 a.m.
emerging-icmp_info	—	05/14/2014 7:50 a.m.
emerging-smp	—	05/14/2014 7:50 a.m.
emerging-dos	—	05/14/2014 7:50 a.m.
drop	—	05/14/2014 7:50 a.m.
emerging-web_client	—	05/14/2014 7:50 a.m.
emerging-malware	—	05/14/2014 7:50 a.m.
dsshield	—	05/14/2014 7:50 a.m.
emerging-attack_response	—	05/14/2014 7:50 a.m.
emerging-imap	—	05/14/2014 7:50 a.m.

Page 1 of 4   [Next](#) 15 of 53 categories

### Suppressed rules

Sid <small>▲</small>	Msg <small>▲</small>
2290029	SURICATA ICMPv6 unknown type

1 rule

SCIRIUS V0.2. COPYRIGHT (C)2014 STAMUS NETWORKS. CSS DESIGN BY FREECSSTEMPLATES.ORG.

# Questions ?

## Contact

- E-mail : [eleblond@stamus-networks.com](mailto:eleblond@stamus-networks.com)
- Twitter : [@Regiteric](https://twitter.com/Regiteric)

## Plus d'infos

- **SELKS** : `https://www.stamus-networks.com/open-source/#selks`
- **Suricata** : `http://www.suricata-ids.org/`
- **Elasticsearch** : `http://www.elasticsearch.org`
- **DOM** : `https://github.com/regit/DOM`