Let's talk about SELKS

Éric Leblond

Stamus Networks

5 juin 2014

Éric Leblond

eleblond@stamus-networks.com

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

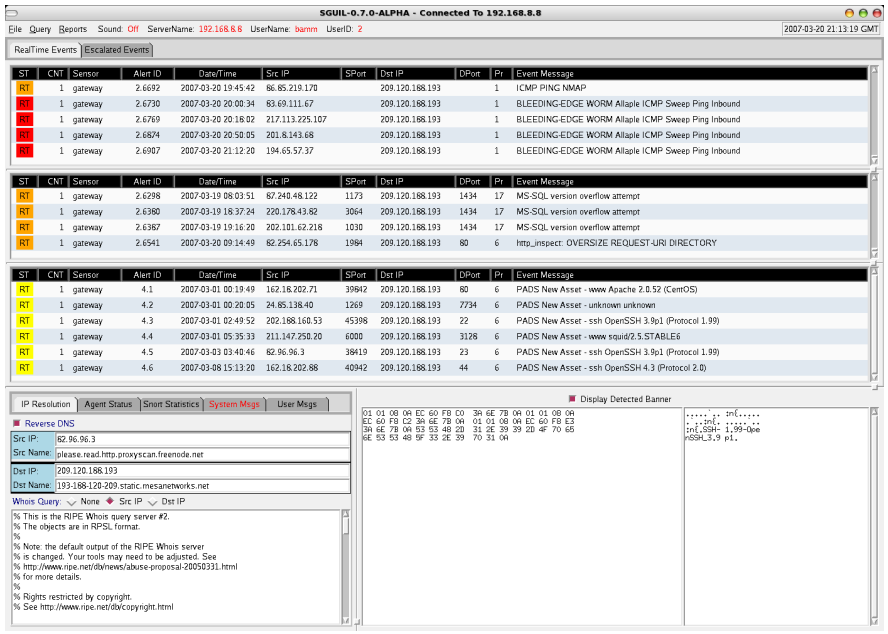
eric@regit.org

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

Sécurité défensive

Un grand manque de sexy

- Interface réalisée par des techs
- Productivité peut-être
- Mais pas de fun



Sécurité défensive

Suricata 2.0

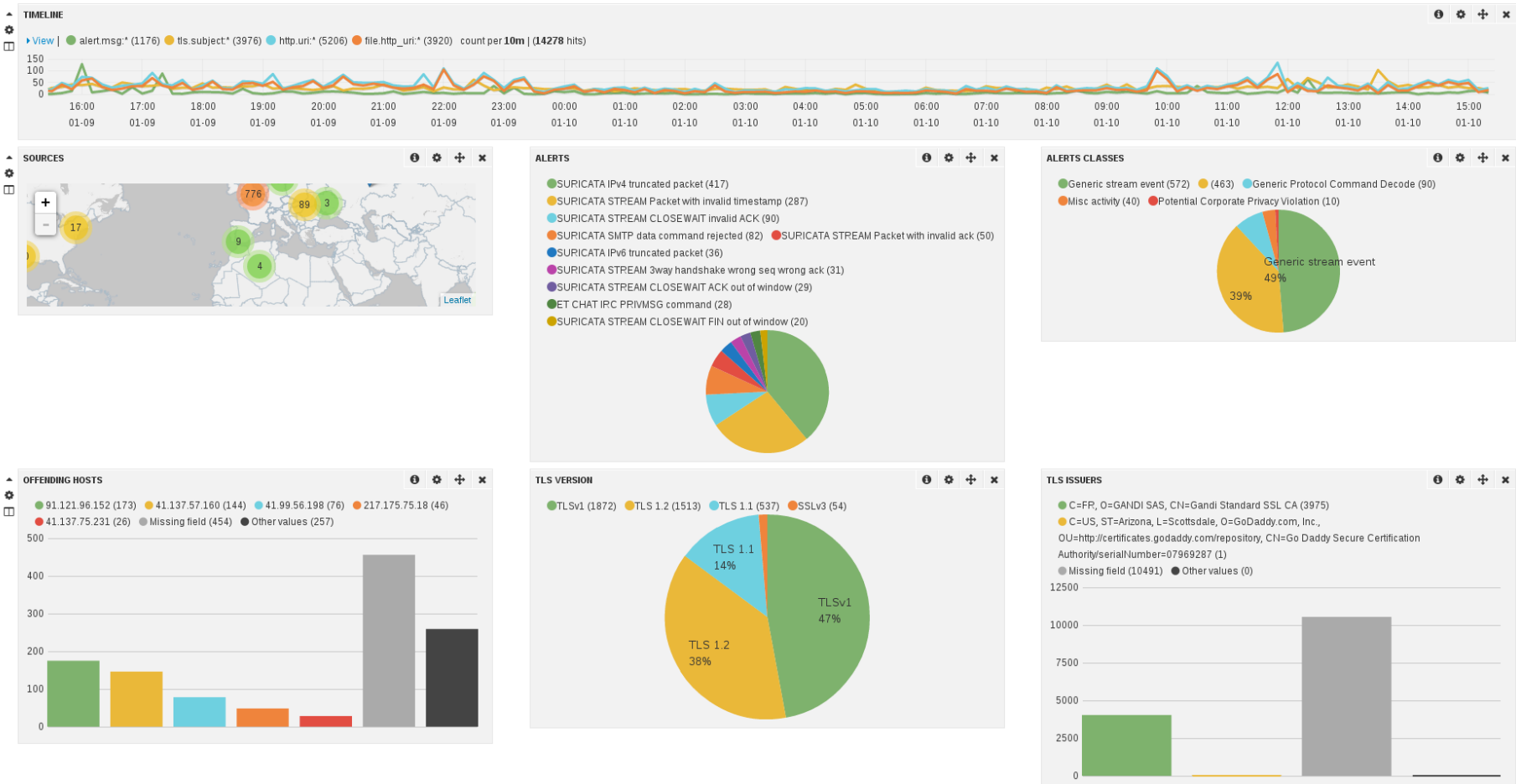
EVE

- Nouvelle sortie unifiée en JSON
- Branchement facile de solutions comme Logstah 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']])
```

Deny On Monitoring

Quelques retours utilisateurs

Deny On Monitoring

Quelques retours utilisateurs

Dom est une des protections essentielles du réseau du FMI

Christine Lagarde

Deny On Monitoring

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

Deny On Monitoring

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

SELKS

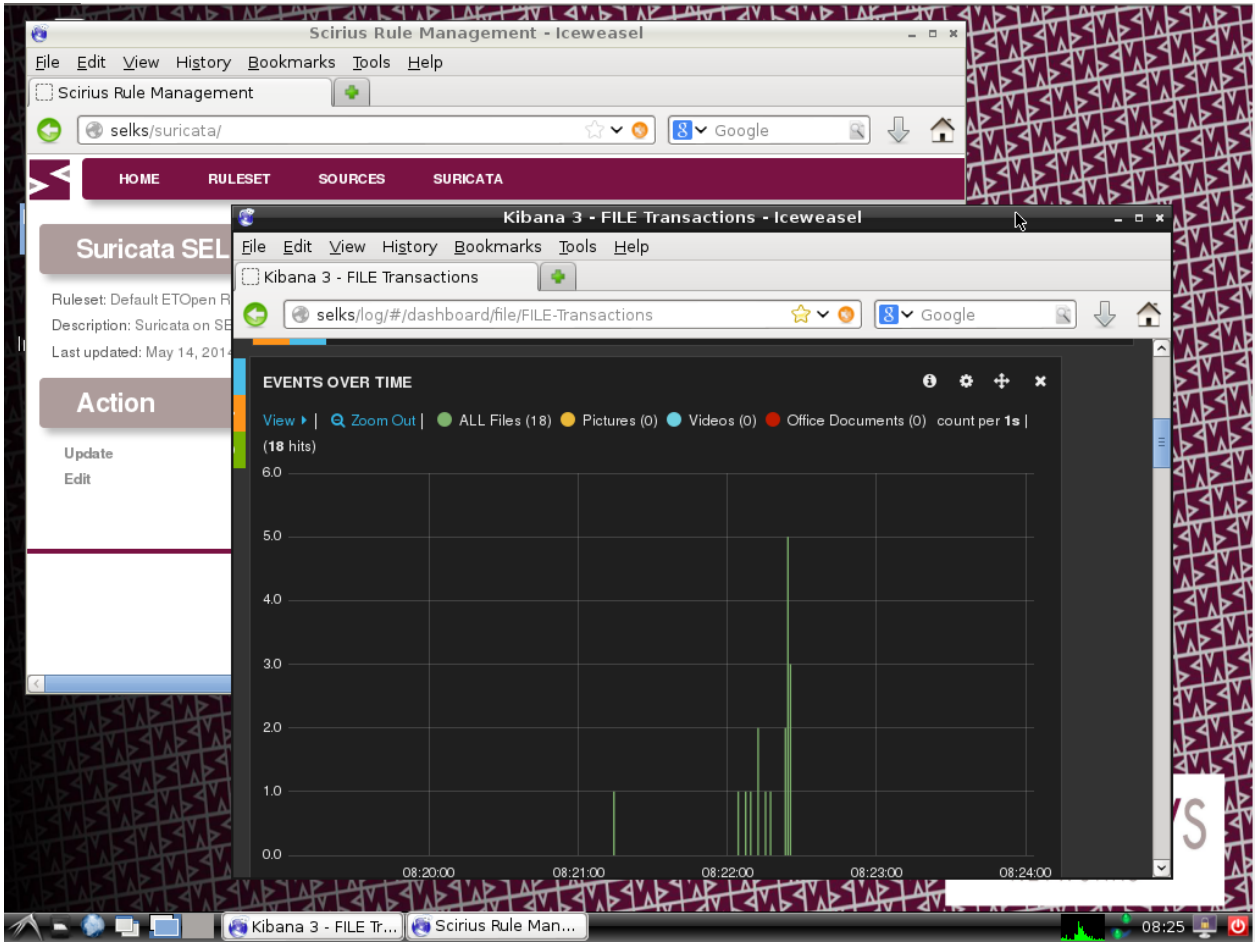
Une ISO live et installable

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

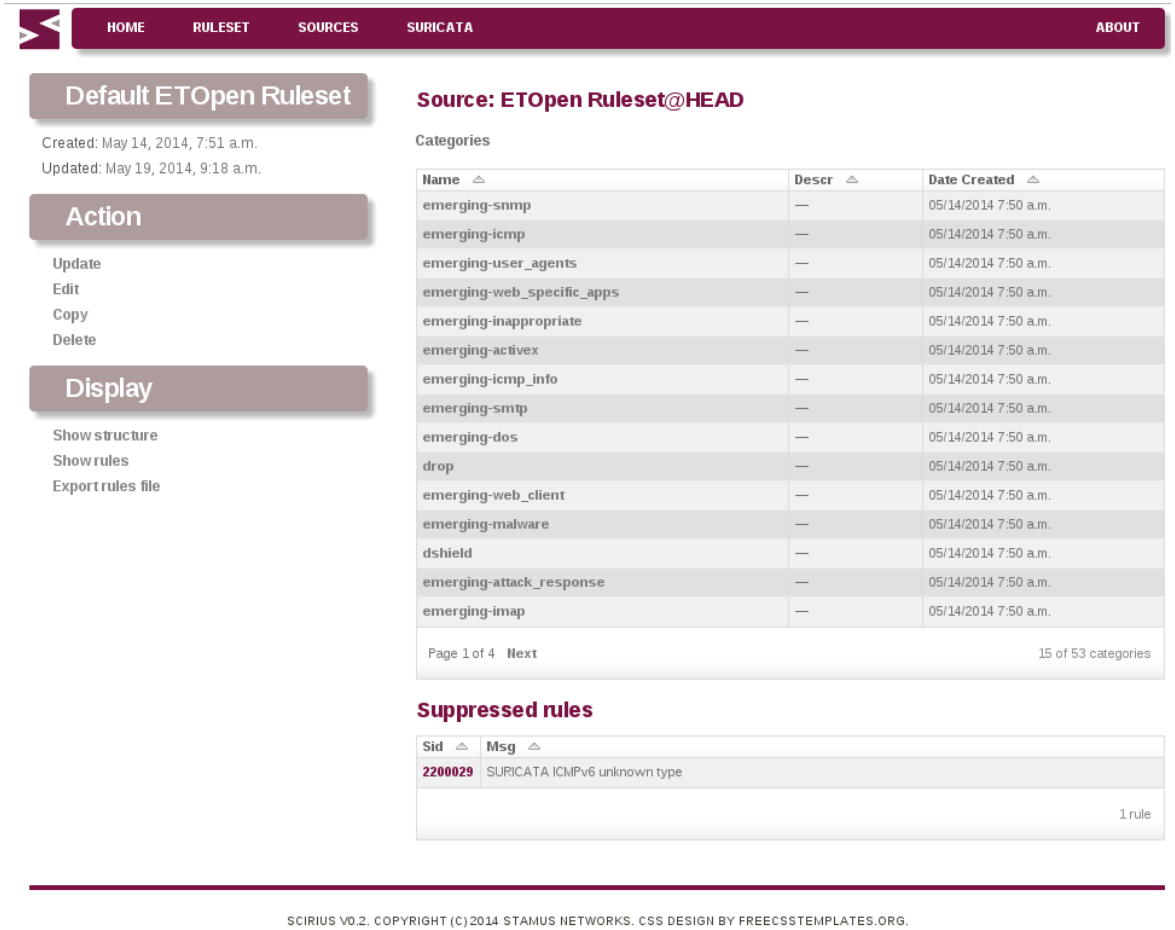
Contenu

- 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



Questions ?

Contact

- E-mail : eleblond@stamus-networks.com
- Twitter : @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`