Let's 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
SELKS – EveBox

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

- Filter and visualize on over 360 metadata fields
- GeoIP 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 ?