Suricata IDS/IPS

Victor Julien
NLUUG 19/11/2015

whoami

- @inliniac
- blog.inliniac.net
- Open Source hippie
- Suricata creator and lead dev
- Vuurmuur

Whats in a name?

Day 37:
They still do not suspect
I am a mere cat.
more funny stuff at FUNNYASDUCK.NET

Who still knows their network?

- Increasing complexity
- BYOD
- IoT
- VM's and containers
- ICS/SCADA

Suricata is an engine for...

Network Intrusion Detection

Network Intrusion Prevention

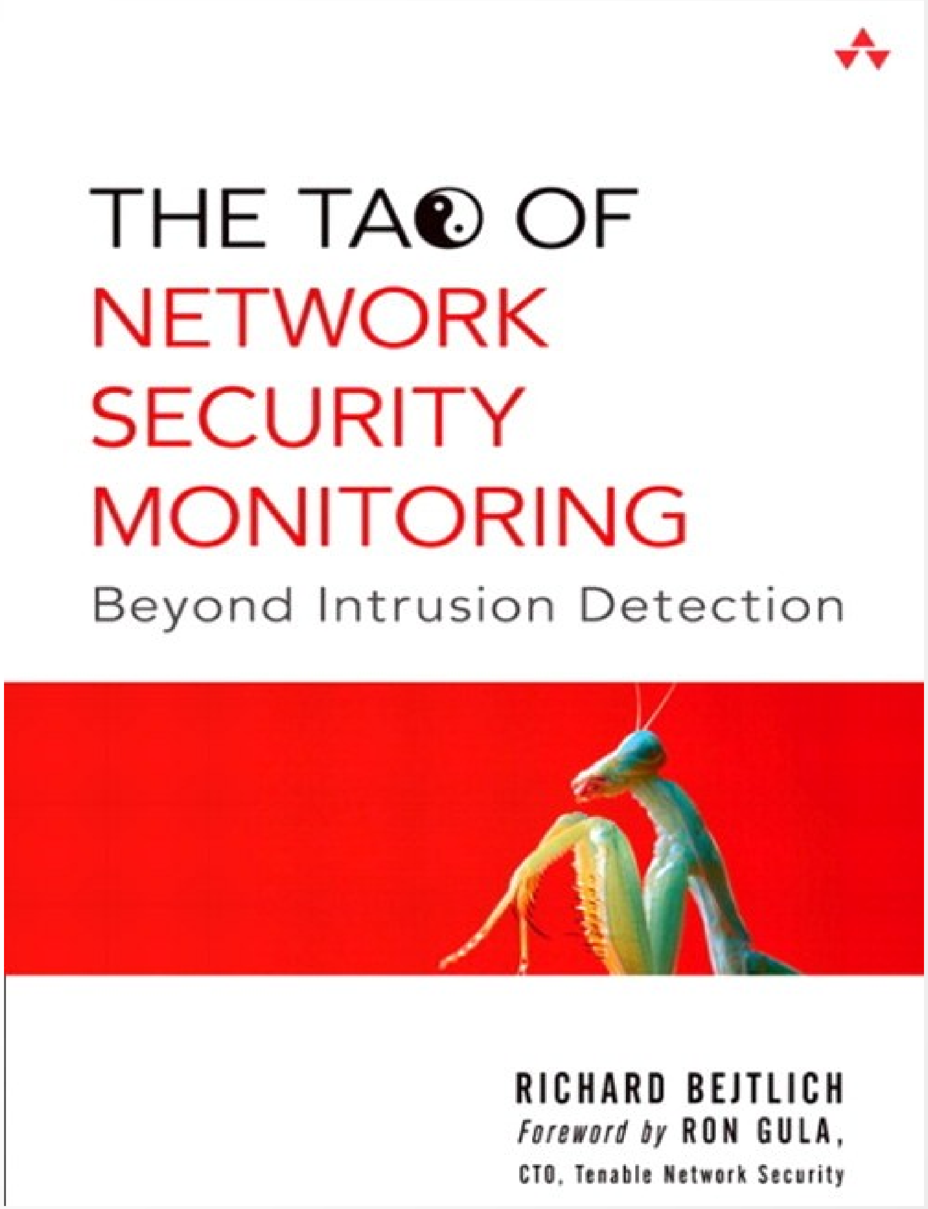
Network Security Monitoring

IDS? IPS?

- (N)IDS: (Network) Intrustion Detection System
- IPS: Intrusion Prevention System
- “System to uncover malicious/unwanted activity on your network by inspecting the network traffic”
- System? => Engine

NSM

- Traditionally IDS was “alert” based
- Network Security Monitoring (NSM) does much more
- “collect everything”, including FPC



Suricata Features

- Inspect traffic for known bad using Snort language
- Lua based scripting for detection
- Unified JSON output for easy post-processing
- Extract files
- Scalable through multi-threading

Suricata ecosystem

- Distributions
  - SELKS
  - SecurityOnion
- Management tools
  - Evebox
  - Scirius
- Event processing
  - Mobster
  - Barnyard2

OISF

- Open Information Security Foundation
- US based non-profit
- Owns Suricata code
- Community driven and controlled

Getting paid for OSS

Platinum Level
FireEye
proofpoint
OISF

Demo's!

- Commandline foo
- SELKS
- “Amsterdam”

No animals will be hurt

© Newspix / Rex Features

Commandline foo

- Replay pcap
- Show what Suricata logs
- Tool used: 'jq'

SELKS

- “Suricata Elasticsearch Logstash Kibana Scirius”
- Open source Debian Jessie based (live) distro with:
  - Suricata
  - ELK stack
  - Scirius rule manager
- Currently with Kibana 3

“Amsterdam”

- SELKS on Docker
- Uses docker compose
- Takes Docker images from various sources
  - e.g. various ELK parts from the official ELK images
- Has Kibana 4 (but no preset dashboards yet)

Try Suricata

- http://suricata-ids.org
  - Source
  - Ubuntu PPA
  - @Suricata_IDS
- https://www.stamus-networks.com/open-source/#selks
  - @StamusN

Questions?