OPENDXL IN
ACTIVE RESPONSE SCENARIOS

Tarmo Randel
CCD COE

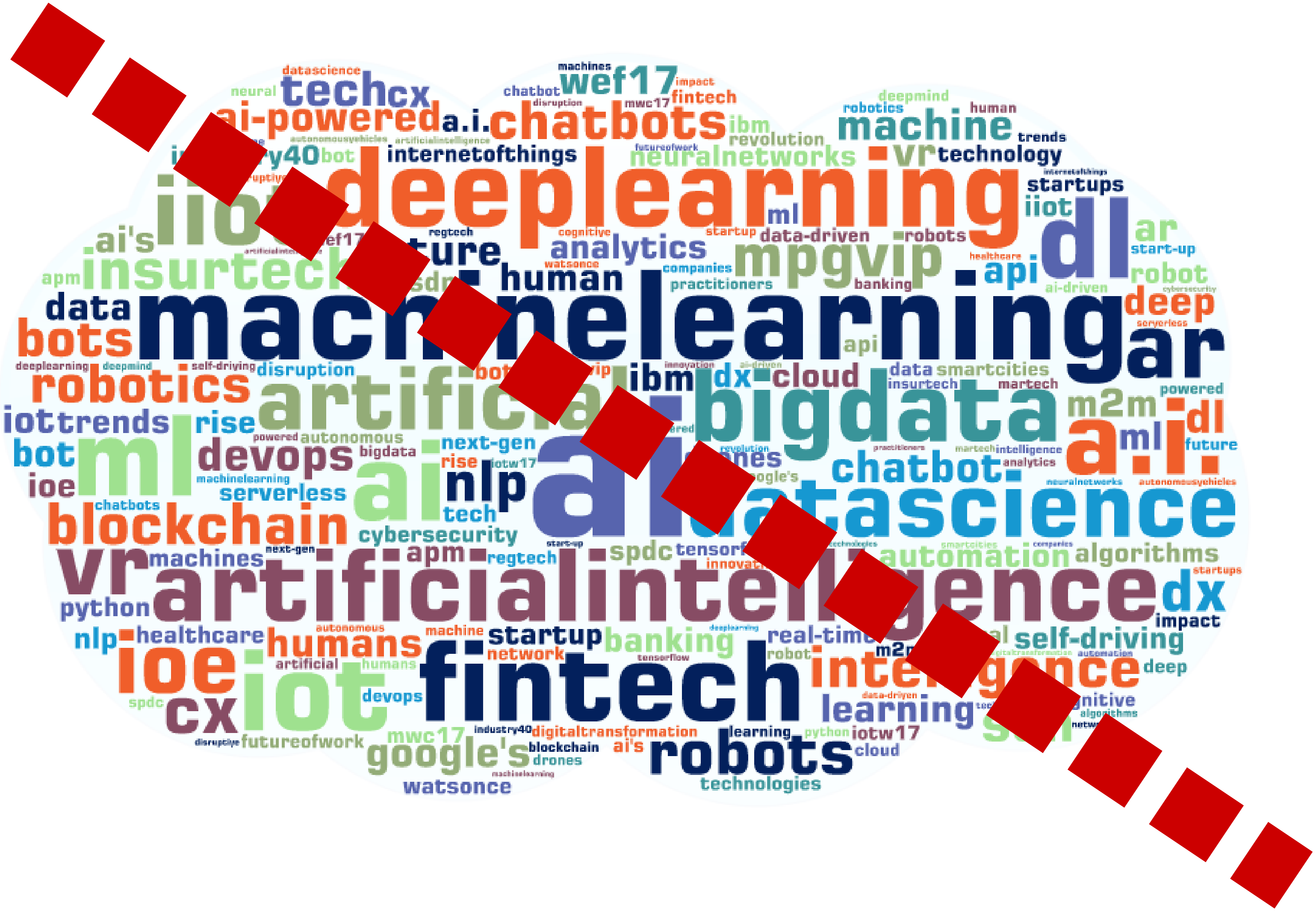
DEEPSEC

November 2017

AGENDA

- Who I am
- Why I am talking about OpenDXL
- How it works
- How we can/could use it
- Proof of Concept
- Conclusion and future work

BEWARE!



machinelearning
artificialintelligence
deeplearning
fintech
ai
bigdata
datascience
artificial
iiot
iot
ioe
ml
dl
a.i.
vr
ar
chatbots
chatbot
robotics
robots
blockchain
insurtech
mpgvip
techcx
ai-powered
machine
wef17
internetofthings
neuralnetworks
technology
startups
analytics
human
humans
bots
bot
data
devops
nlp
cloud
ibm
dx
m2m
cybersecurity
automation
algorithms
self-driving
intelligence
learning
banking
startup
healthcare
python
google's
watsonce
technologies
futureofwork
digitaltransformation
serverless
disruption
iottrends
rise
next-gen
tech
deep
api
robot
cx
apm
regtech
spdc
machines

ABOUT MYSELF

Andmekaitse Inspektsioon

TELE2

cert.ee

CCDCOE

NATO Cooperative Cyber Defence
Centre of Excellence
Tallinn, Estonia

IN RESPONSE TO KEYNOTE - THAT WAS OUR AWARENESS RISING CAMPAIGN!

ABOUT CCDCOE

RESEARCH

TRAINING

EXERCISE

TECHNOLOGY

STRATEGY

OPERATIONS

LAW

RESEARCH AREAS

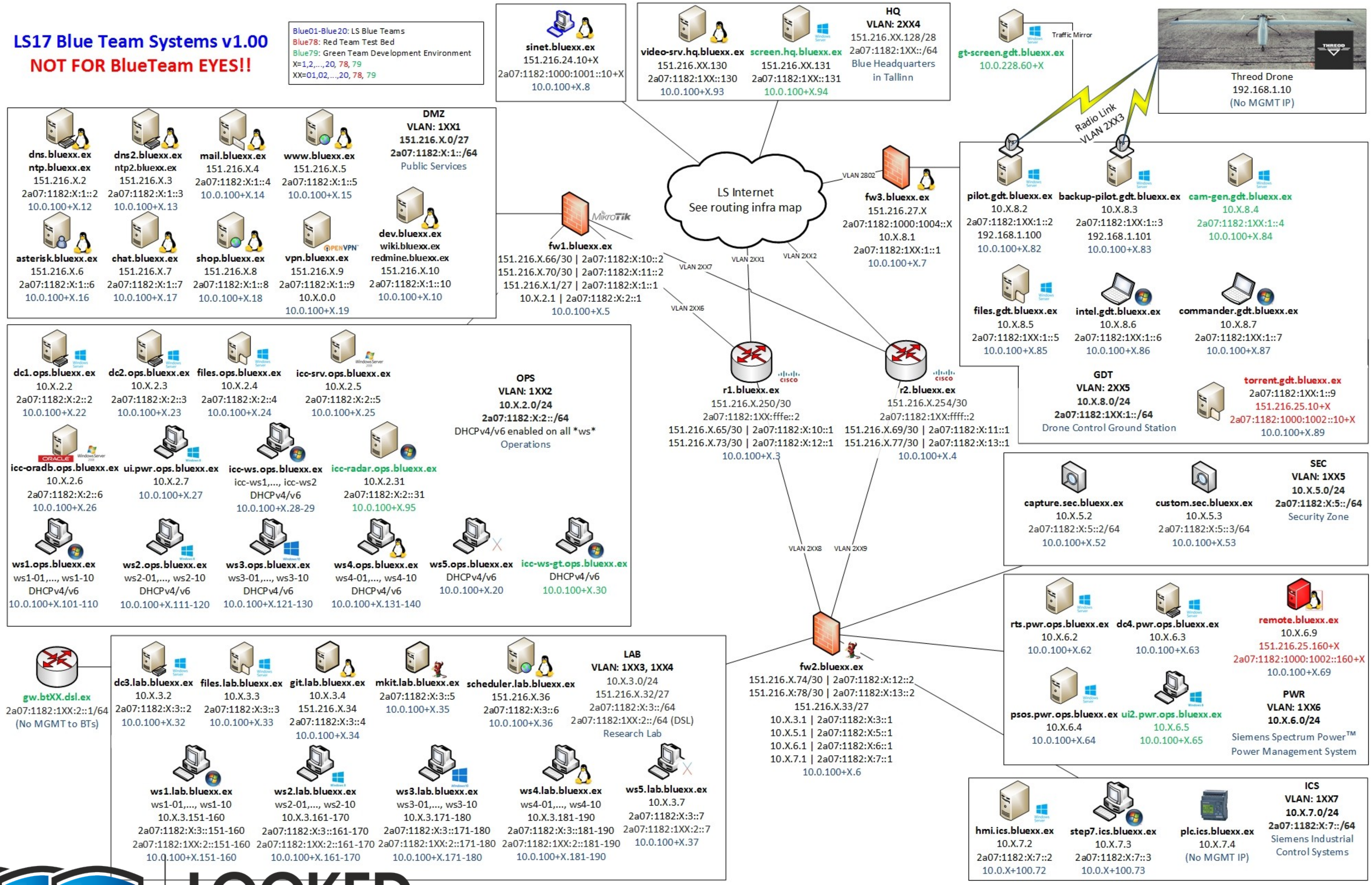
Image copyright: www.militaryaerospace.com

CLOSER TO THE TOPIC

LOCKED SHIELDS

CROSSED SWORDS

CLOSER TO THE TOPIC



LS17 Blue Team Systems v1.00
NOT FOR BlueTeam EYES!!

Blue01-Blue20: LS Blue Teams
Blue78: Red Team Test Bed
Blue79: Green Team Development Environment
X=1,2,...,20, 78, 79
XX=01,02,...,20, 78, 79

sinet.bluexx.ex
151.216.24.10+X
2a07:1182:1000:1001::10+X
10.0.100+X.8

video-srv.hq.bluexx.ex
151.216.XX.130
2a07:1182:1XX::130
10.0.100+X.93

screen.hq.bluexx.ex
151.216.XX.131
2a07:1182:1XX::131
10.0.100+X.94

HQ
VLAN: 2XX4
151.216.XX.128/28
2a07:1182:1XX::/64
Blue Headquarters in Tallinn

gt-screen.gdt.bluexx.ex
10.0.228.60+X

Traffic Mirror

Threod Drone
192.168.1.10
(No MGMT IP)

Radio Link
VLAN 2XX3

DMZ
VLAN: 1XX1
151.216.X.0/27
2a07:1182:X:1::/64
Public Services

dns.bluexx.ex
ntp.bluexx.ex
151.216.X.2
2a07:1182:X:1::2
10.0.100+X.12

dns2.bluexx.ex
ntp2.bluexx.ex
151.216.X.3
2a07:1182:X:1::3
10.0.100+X.13

mail.bluexx.ex
151.216.X.4
2a07:1182:X:1::4
10.0.100+X.14

www.bluexx.ex
151.216.X.5
2a07:1182:X:1::5
10.0.100+X.15

asterisk.bluexx.ex
151.216.X.6
2a07:1182:X:1::6
10.0.100+X.16

chat.bluexx.ex
151.216.X.7
2a07:1182:X:1::7
10.0.100+X.17

shop.bluexx.ex
151.216.X.8
2a07:1182:X:1::8
10.0.100+X.18

vpn.bluexx.ex
151.216.X.9
2a07:1182:X:1::9
10.X.0.0
10.0.100+X.19

dev.bluexx.ex
wiki.bluexx.ex
redmine.bluexx.ex
151.216.X.10
2a07:1182:X:1::10
10.0.100+X.10

fw1.bluexx.ex
151.216.X.66/30 | 2a07:1182:X:10::2
151.216.X.70/30 | 2a07:1182:X:11::2
151.216.X.1/27 | 2a07:1182:X:1::1
10.X.2.1 | 2a07:1182:X:2::1
10.0.100+X.5

LS Internet
See routing infra map

VLAN 2802

fw3.bluexx.ex
151.216.27.X
2a07:1182:1000:1004::X
10.X.8.1
2a07:1182:1XX:1::1
10.0.100+X.7

VLAN 2XX7
VLAN 2XX1
VLAN 2XX2
VLAN 2XX6

r1.bluexx.ex
151.216.X.250/30
2a07:1182:1XX:fffe::2
151.216.X.65/30 | 2a07:1182:X:10::1
151.216.X.73/30 | 2a07:1182:X:12::1
10.0.100+X.3

r2.bluexx.ex
151.216.X.254/30
2a07:1182:1XX:ffff::2
151.216.X.69/30 | 2a07:1182:X:11::1
151.216.X.77/30 | 2a07:1182:X:13::1
10.0.100+X.4

pilot.gdt.bluexx.ex
10.X.8.2
2a07:1182:1XX:1::2
192.168.1.100
10.0.100+X.82

backup-pilot.gdt.bluexx.ex
10.X.8.3
2a07:1182:1XX:1::3
192.168.1.101
10.0.100+X.83

cam-gen.gdt.bluexx.ex
10.X.8.4
2a07:1182:1XX:1::4
10.0.100+X.84

files.gdt.bluexx.ex
10.X.8.5
2a07:1182:1XX:1::5
10.0.100+X.85

intel.gdt.bluexx.ex
10.X.8.6
2a07:1182:1XX:1::6
10.0.100+X.86

commander.gdt.bluexx.ex
10.X.8.7
2a07:1182:1XX:1::7
10.0.100+X.87

GDT
VLAN: 2XX5
10.X.8.0/24
2a07:1182:1XX:1::/64
Drone Control Ground Station

torrent.gdt.bluexx.ex
2a07:1182:1XX:1::9
151.216.25.10+X
2a07:1182:1000:1002::10+X
10.0.100+X.89

OPS
VLAN: 1XX2
10.X.2.0/24
2a07:1182:X:2::/64
DHCPv4/v6 enabled on all *ws*
Operations

dc1.ops.bluexx.ex
10.X.2.2
2a07:1182:X:2::2
10.0.100+X.22

dc2.ops.bluexx.ex
10.X.2.3
2a07:1182:X:2::3
10.0.100+X.23

files.ops.bluexx.ex
10.X.2.4
2a07:1182:X:2::4
10.0.100+X.24

icc-srv.ops.bluexx.ex
10.X.2.5
2a07:1182:X:2::5
10.0.100+X.25

icc-oradb.ops.bluexx.ex
10.X.2.6
2a07:1182:X:2::6
10.0.100+X.26

ui.pwr.ops.bluexx.ex
10.X.2.7
10.0.100+X.27

icc-ws.ops.bluexx.ex
icc-ws1,..., icc-ws2
DHCPv4/v6
10.0.100+X.28-29

icc-radar.ops.bluexx.ex
10.X.2.31
2a07:1182:X:2::31
10.0.100+X.95

ws1.ops.bluexx.ex
ws1-01,..., ws1-10
DHCPv4/v6
10.0.100+X.101-110

ws2.ops.bluexx.ex
ws2-01,..., ws2-10
DHCPv4/v6
10.0.100+X.111-120

ws3.ops.bluexx.ex
ws3-01,..., ws3-10
DHCPv4/v6
10.0.100+X.121-130

ws4.ops.bluexx.ex
ws4-01,..., ws4-10
DHCPv4/v6
10.0.100+X.131-140

ws5.ops.bluexx.ex
DHCPv4/v6
10.0.100+X.20

icc-ws-gt.ops.bluexx.ex
DHCPv4/v6
10.0.100+X.30

SEC
VLAN: 1XX5
10.X.5.0/24
2a07:1182:X:5::/64
Security Zone

capture.sec.bluexx.ex
10.X.5.2
2a07:1182:X:5::2/64
10.0.100+X.52

custom.sec.bluexx.ex
10.X.5.3
2a07:1182:X:5::3/64
10.0.100+X.53

VLAN 2XX8
VLAN 2XX9

fw2.bluexx.ex
151.216.X.74/30 | 2a07:1182:X:12::2
151.216.X:78/30 | 2a07:1182:X:13::2
151.216.X.33/27
10.X.3.1 | 2a07:1182:X:3::1
10.X.5.1 | 2a07:1182:X:5::1
10.X.6.1 | 2a07:1182:X:6::1
10.X.7.1 | 2a07:1182:X:7::1
10.0.100+X.6

rts.pwr.ops.bluexx.ex
10.X.6.2
10.0.100+X.62

dc4.pwr.ops.bluexx.ex
10.X.6.3
10.0.100+X.63

remote.bluexx.ex
10.X.6.9
151.216.25.160+X
2a07:1182:1000:1002::160+X
10.0.100+X.69

psos.pwr.ops.bluexx.ex
10.X.6.4
10.0.100+X.64

ui2.pwr.ops.bluexx.ex
10.X.6.5
10.0.100+X.65

PWR
VLAN: 1XX6
10.X.6.0/24
Siemens Spectrum Power™
Power Management System

gw.btXX.dsl.ex
2a07:1182:1XX:2::1/64
(No MGMT to BTs)

LAB
VLAN: 1XX3, 1XX4
10.X.3.0/24
151.216.X.32/27
2a07:1182:X:3::/64
2a07:1182:1XX:2::/64 (DSL)
Research Lab

dc3.lab.bluexx.ex
10.X.3.2
2a07:1182:X:3::2
10.0.100+X.32

files.lab.bluexx.ex
10.X.3.3
2a07:1182:X:3::3
10.0.100+X.33

git.lab.bluexx.ex
10.X.3.4
151.216.X.34
2a07:1182:X:3::4
10.0.100+X.34

mkit.lab.bluexx.ex
2a07:1182:X:3::5
10.0.100+X.35

scheduler.lab.bluexx.ex
151.216.X.36
2a07:1182:X:3::6
10.0.100+X.36

ws1.lab.bluexx.ex
ws1-01,..., ws1-10
10.X.3.151-160
2a07:1182:X:3::151-160
2a07:1182:1XX:2::151-160
10.0.100+X.151-160

ws2.lab.bluexx.ex
ws2-01,..., ws2-10
10.X.3.161-170
2a07:1182:X:3::161-170
2a07:1182:1XX:2::161-170
10.0.100+X.161-170

ws3.lab.bluexx.ex
ws3-01,..., ws3-10
10.X.3.171-180
2a07:1182:X:3::171-180
2a07:1182:1XX:2::171-180
10.0.100+X.171-180

ws4.lab.bluexx.ex
ws4-01,..., ws4-10
10.X.3.181-190
2a07:1182:X:3::181-190
2a07:1182:1XX:2::181-190
10.0.100+X.181-190

ws5.lab.bluexx.ex
10.X.3.7
2a07:1182:X:3::7
2a07:1182:1XX:2::7
10.0.100+X.37

ICS
VLAN: 1XX7
10.X.7.0/24
2a07:1182:X:7::/64
Siemens Industrial Control Systems

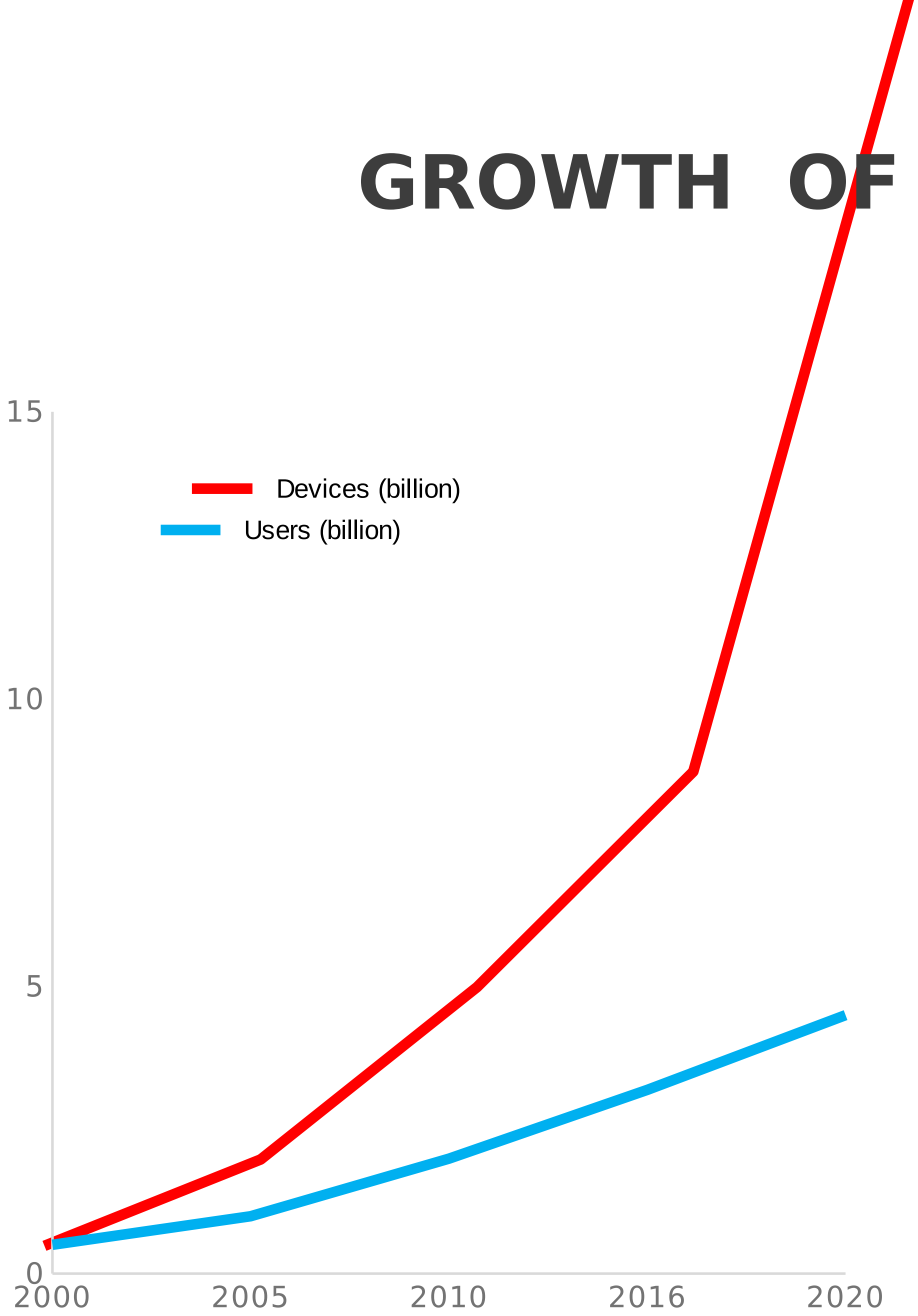
hmi.ics.bluexx.ex
10.X.7.2
2a07:1182:X:7::2
10.0.X+100.72

step7.ics.bluexx.ex
10.X.7.3
2a07:1182:X:7::3
10.0.X+100.73

plc.ics.bluexx.ex
10.X.7.4
(No MGMT IP)

LOCKED SHIELDS

GROWTH OF CYBERSPACE



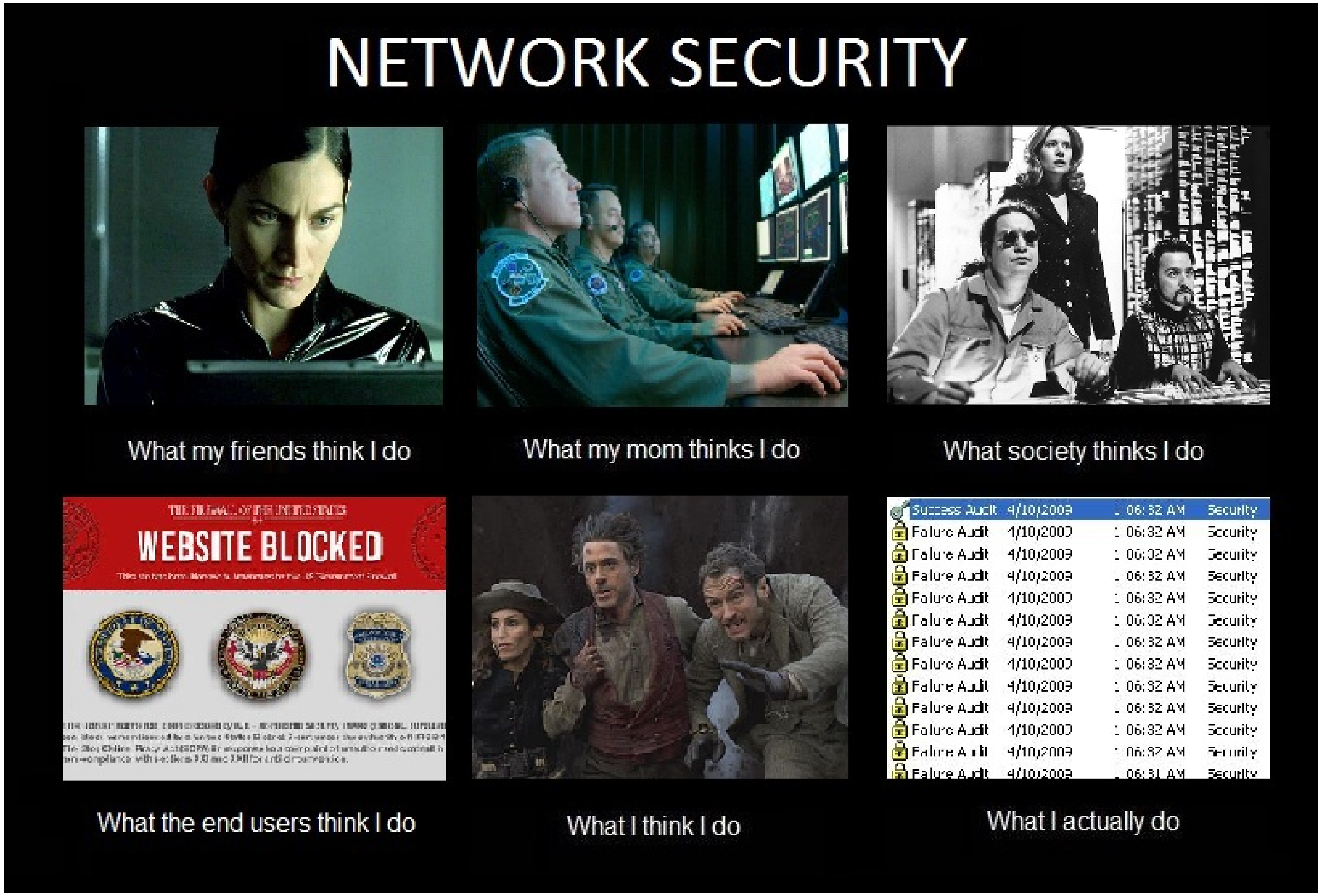
95 Countries developing legislative initiatives

77 Countries with national cybersecurity strategies

17 Countries with declared offensive capabilities

20+ Cyber commands

SHOULD
WANT
MUST ...



```
Success Audit  4/10/2009   06:32 AM  Security
Failure Audit  4/10/2009   06:32 AM  Security
Failure Audit  4/10/2009   06:32 AM  Security
Failure Audit  4/10/2009   06:32 AM  Security
Failure Audit  4/10/2009   06:32 AM  Security
Failure Audit  4/10/2009   06:32 AM  Security
Failure Audit  4/10/2009   06:32 AM  Security
Failure Audit  4/10/2009   06:32 AM  Security
Failure Audit  4/10/2009   06:32 AM  Security
Failure Audit  4/10/2009   06:32 AM  Security
Failure Audit  4/10/2009   06:32 AM  Security
Failure Audit  4/10/2009   06:32 AM  Security
Failure Audit  4/10/2009   06:31 AM  Security
```

Picture copyright: probably tisiphone.net

SUMMARIZING INTRO

- We are daily handling large amount of events and incidents with various tools and appliances
- Integration “could be better” (=it should not take hundreds of man hours to make things work together)
- Evolution makes keeping integrated stuff working together harder
- We are short of time and people

ACTIVE RESPONSE

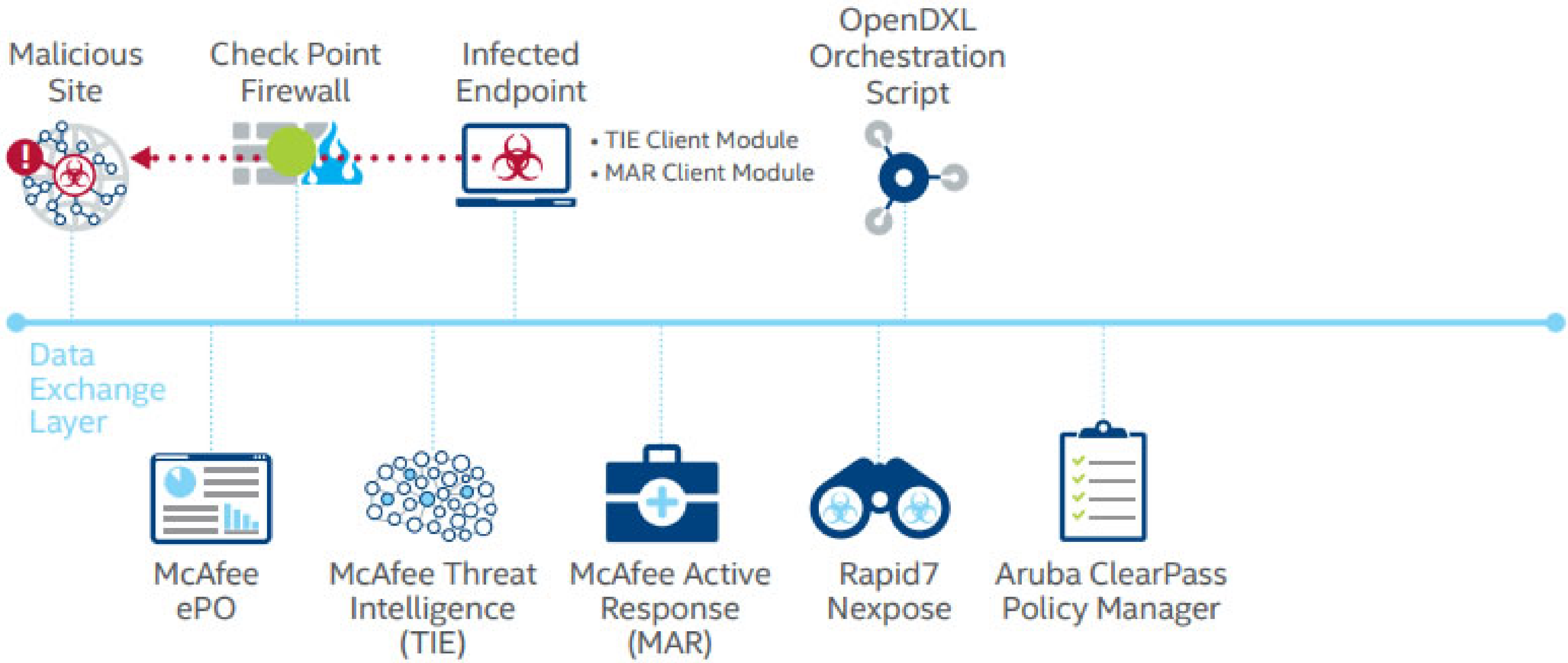
- Security incident flow orchestration tools have arrived!
- What about active response, what is it?
  - Is it about blocking?
  - Is it about deception?
  - Is it about attribution?
  - Is it about getting even?
  - Is it about getting “our stuff back”?

ACTIVE PROTECTION

According to Christopher Ensey 2 there are six conditions to be met in order to have active protection in place:

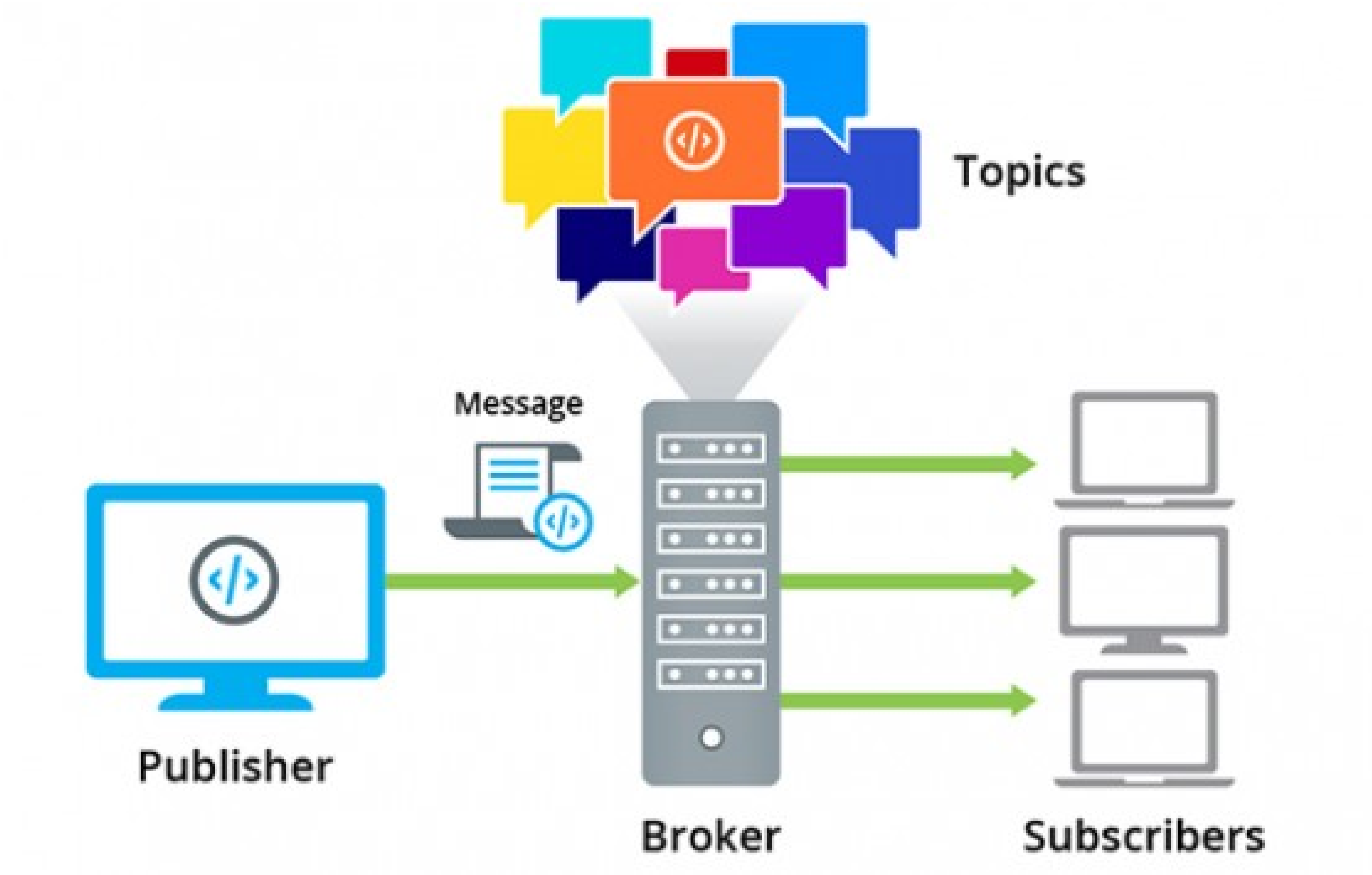
1. Centralized event management
2. Analytics
3. Open APIs
4. Dynamic infrastructure.
5. The Human element
6. Complete visibility

SURPRISING MOVE FROM THE INDUSTRY



Picture copyright: McAfee

OPEN ARCHITECTURE



Picture copyright: McAfee

“OPEN” IN OPENDXL

- Based on open standard protocol: MQTT
- No implementation guidelines
    - No rules or registry for central element – topic
- Client libraries on GitHub
- Broker as Docker image

CORE: MQTT

- Connected clients may subscribe to the data paths (topics) and process the data received from there however they see fit, clients can also publish data
- Goals: speed and reliability
- Feature: since queuing is not required to be supported as a standard feature you’ll miss the messages if you are off-line
    - Logger/historian type of service could be useful ...

In depth: “Exploiting IoT's MQTT Protocol by (Moshe Zioni)”

SECURITY

- **Security is the “S” in IoT** ;-)
- TLS securing communication
- Topic based access
- PKI infrastructure for authentication
  - Challenge: setting up and maintaining your own CA
  - Challenge: deal with compromised client on CA level

OPTION 1. ORCHESTRATION

- Transmitted data is interpreted same way by all parties
- Interface to control the systems/devices
- Workflow design challenges and opportunities
- Good birds eye view of the events
- Many HUGE! mistakes can be avoided

OPTION 2. INDEPENDENT AGENTS

- Can be deployed quickly
- Requires support from appliance/application/system
- Anarchy in MQTT topics can be a blocking point
- BAD things can (and will) happen
- It is good starting point though ...

OPTION 1. IN MQTT LANGUAGE

Orchestrated

/mcafee/service/tie/cert/reputation/get

/mcafee/service/tie/cert/reputation/set

/mcafee/service/tie/file/reputation/get

/mcafee/service/tie/file/reputation/set

/mcafee/service/tie/file/url/reputation/add

… etc ...

PS! Concept is not so different from RESTTful API, example: /v2/hash/:hash

OPTION 2. IN MQTT LANGUAGE

Independent

/feed/bad/ipv4

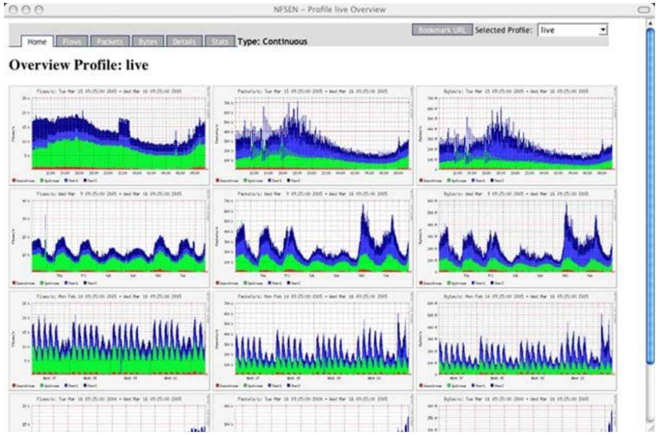
/feed/bad/ipv6

/feed/compromised/ipv4

/feed/compromised/ipv6

… etc ...

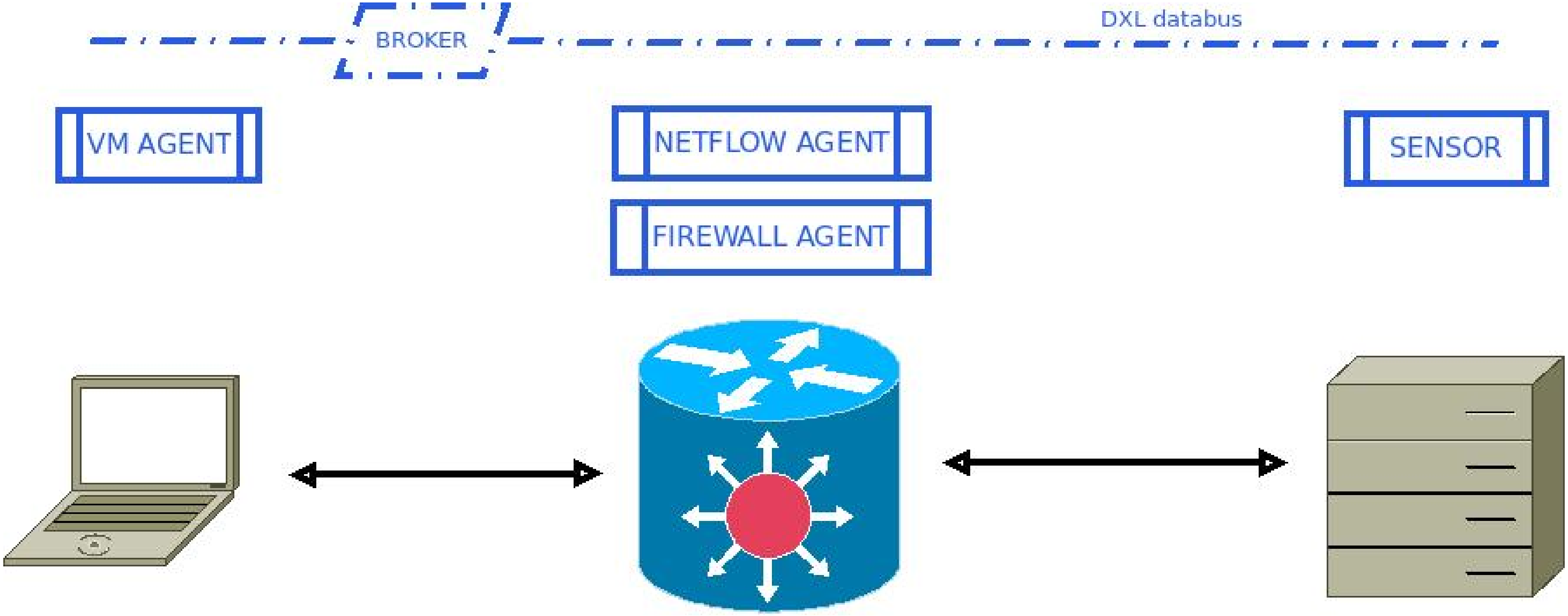
PROOF OF CONCEPT



Type: Continuous

Overview Profile: live

PROOF OF CONCEPT



SETTING UP BROKER

- NB! we will **not** be using any McAfee commercial products
- The Docker is required in our broker machine
- It’ll take about 5 minutes to set up the broker (*the coffee machine is far away @ office …*)

FIREWALL AGENT

- Simple Python interface to Linux iptables
- Respond to events emitted in topics:
  - /feed/bad/ipv4
  - /feed/bad/ipv6
- Apply DENY rule

NETFLOW AGENT

- Python interface to open source tool nfdump
- React to events by looking up records for current day:
  - /feed/bad/ipv4
  - /feed/bad/ipv6
- by looking up records for current day and emitting event (only if match is found) with:
  - /feed/compromised/ipv4
  - /feed/compromised/ipv6

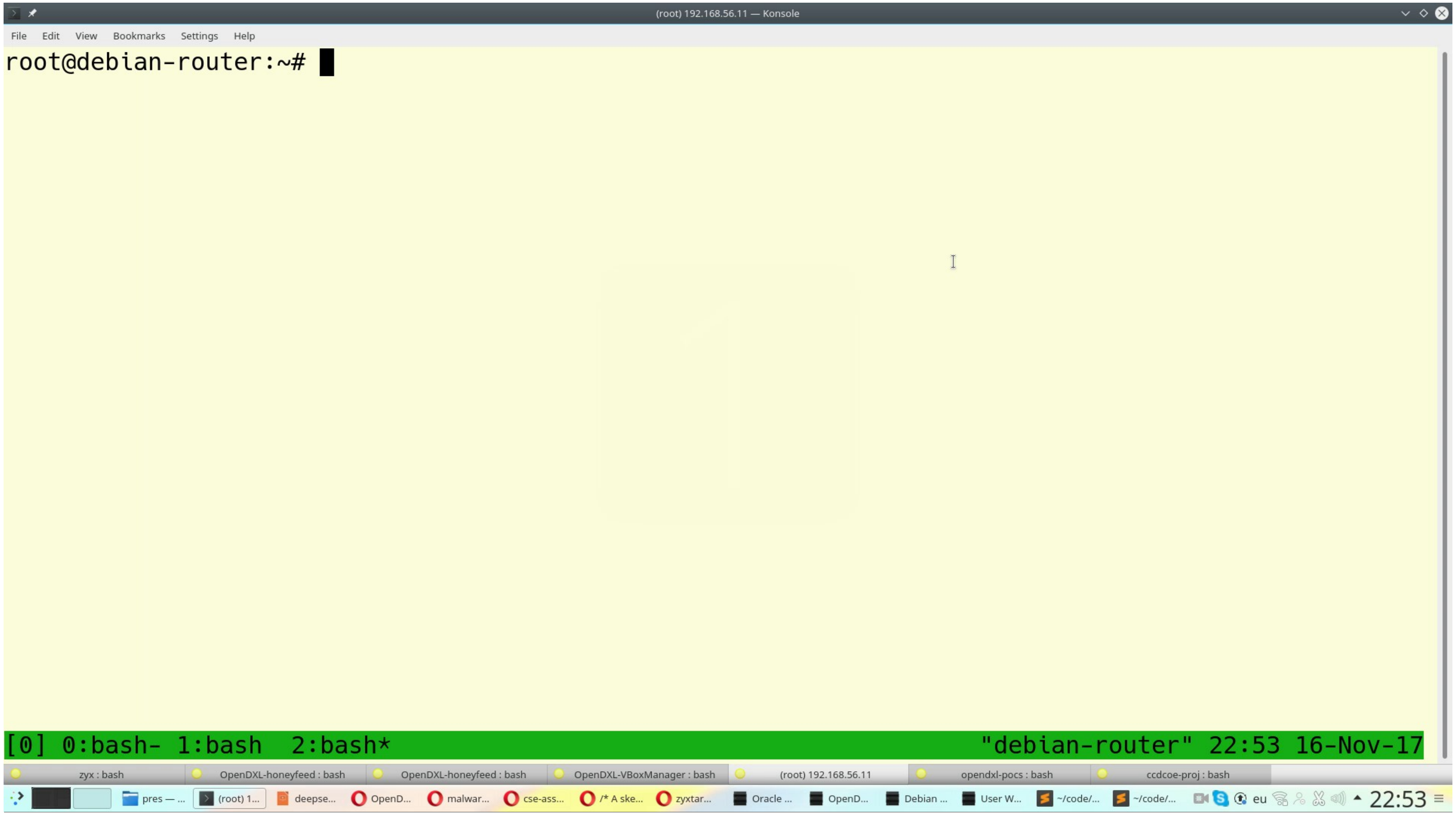
“BADNESS” SENSOR AGENT

- (Really) simple Python logtailer
- Collect *3v1l* IPs from file and emit:
  - /feed/bad/ipv4
  - /feed/bad/ipv6

VM MANAGING AGENT

- Python interface to Virtualbox manager
- React to events:
  - /feed/compromised/ipv4
  - /feed/compromised/ipv6
- by looking up IP matches from internal dictionary and reverting machine to known good state.

RESULT



```
root@debian-router:~# 
```

```
[0] 0:bash- 1:bash  2:bash*                          "debian-router" 22:53 16-Nov-17
```

CONCLUSION

- Great technology to keep an eye on
- Can be a bit challenging to deploy on large installations
- Topic use needs to be regulated to at least two levels from “root”
- Once the OpenDXL data bus client is compromised it can be hard to detect and mitigate, meanwhile adversary has in-depth look of security databus
- Time will tell if the industry goes with the trend
- Go Play with it!
  - https://github.com/opendxl
  - https://github.com/zyxtarmo/opendxl-pocs

THANK YOU!

Research on
Automated Active Response Orchestration
using OpenDXL will be completed 2018

Ping me if you are interested