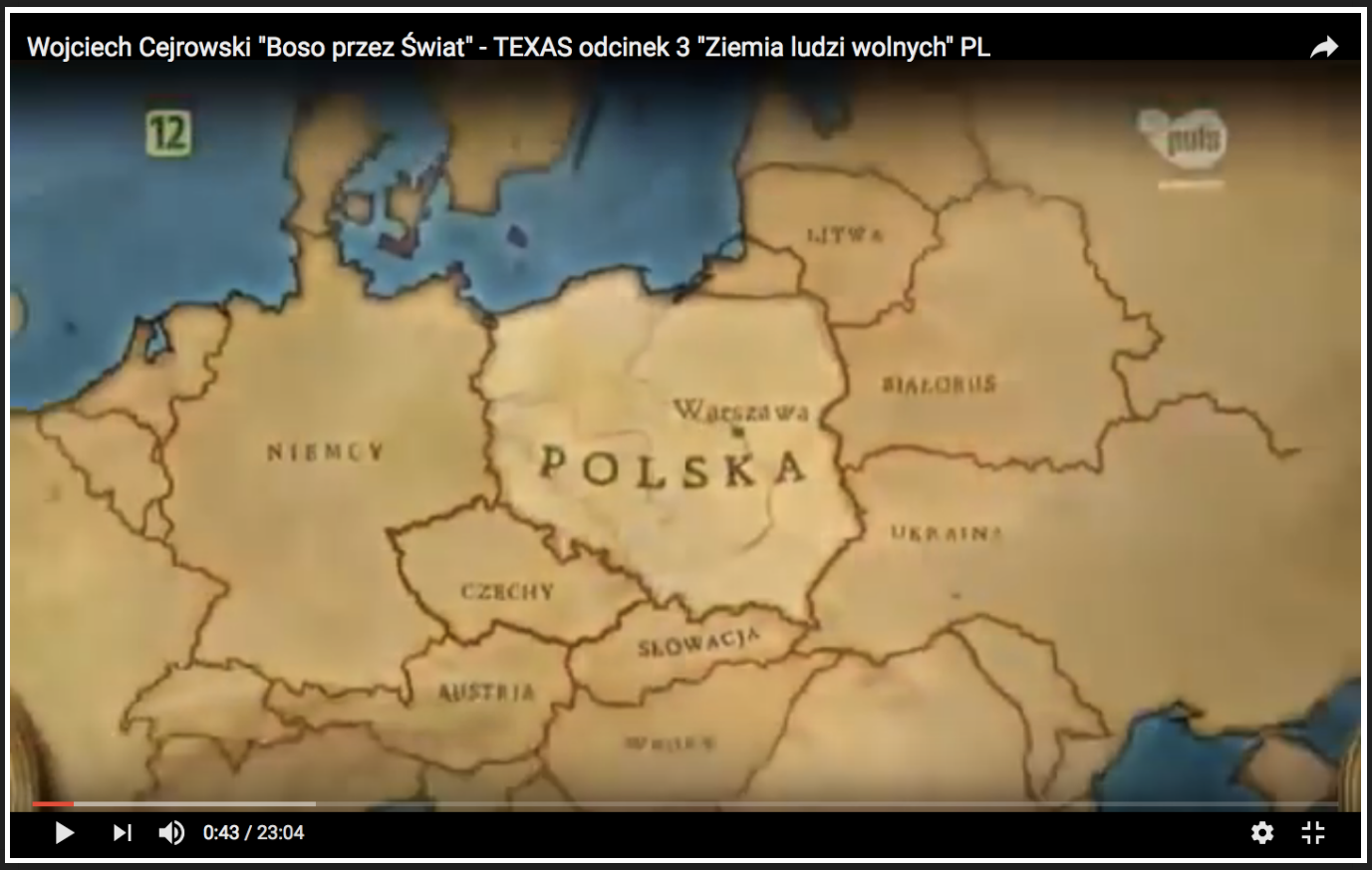
BRO BEFRIENDS SURICATA

SURICATA AND BRO FIGHTING MALWARE TOGETHER

Created by Michal Purzynski / @michalpurzynski

Scripts are here - https://github.com/michalpurzynski


Wojciech Cejrowski "Boso przez Świat" - TEXAS odcinek 3 "Ziemia ludzi wolnych" PL
12
LITWA
BIAŁORUŚ
Warszawa
NIEMCY
POLSKA
UKRAINA
CZECHY
SŁOWACJA
AUSTRIA
0:43 / 23:04


Wojciech Cejrowski "Boso przez Świat" - TEXAS odcinek 3 "Ziemia ludzi wolnych" PL
ZJEDNOCZONE
ARIZONA
NOWY MEKSYK
Amarillo
OKLAHOMA
ARKANSAS
TENNESSI
MISSISIPI
ALABAMA
Dallas
El Paso
TEXAS
Austin
Houston
LUIZJANA
San Antonio
MEK
0:52 / 23:04

WHOAMI

Part of the team doing enterprise information security

We don't do product security

We monitor our infrastructure

We respond to security investigations and incidents

We help developers design and implement security controls

We build tools & services to keep users secure

"A human wireshark". A threat. Management.

NSM IN MOZILLA

9	Offices
3	Continents
1	Datacenter
X	AWS

Around 20 sensors and who knows how many workers :-)

From 2012. Netoptics, now Arista.

MOZILLA CONTRIBUTIONS TO BRO IDS

PR. Tons of PR.

Largest (problematic) installation ever. AUS?

Heka-Lua scripts for parsing logs

Tons of bug reports (SSL, hello Bugzilla)

76 scripts - 4200 LoC - OpenSource

$$$$ 200 000

Myricom plugin (+Seth)

Ansible playbooks - OpenSource

WE HAVE A SECRET

I WILL SHARE A SECRET

IS SHARED SECRET STILL A SECRET?

BRO IS NOT THE ONLY IDS WE USE!!

We use Suricata too

Actually, a whole mob

BTW - WHAT IS AN IDS?

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station.

KEYWORDS

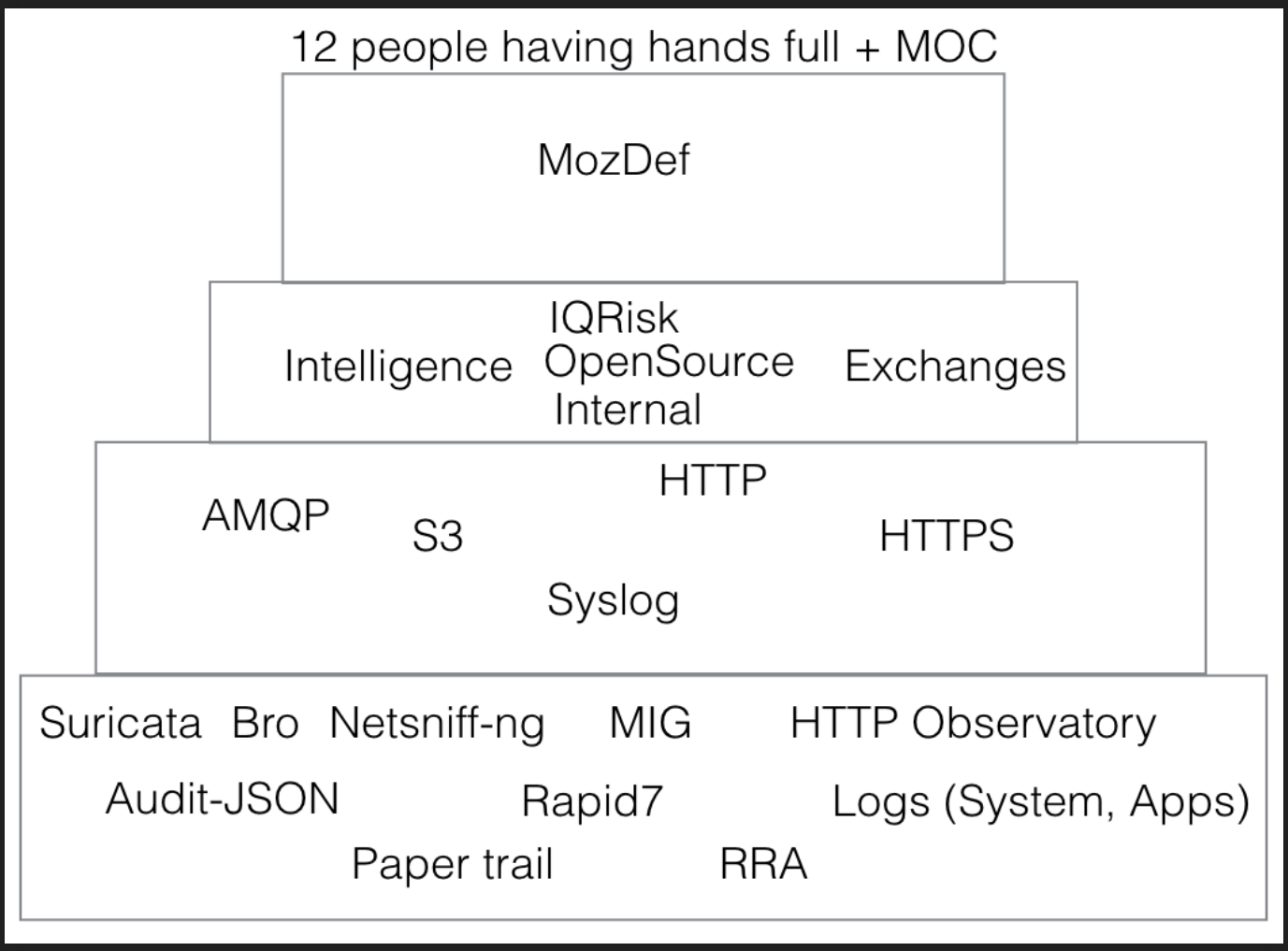
malicious activity <-- known indicators

policy violations <-- known rules

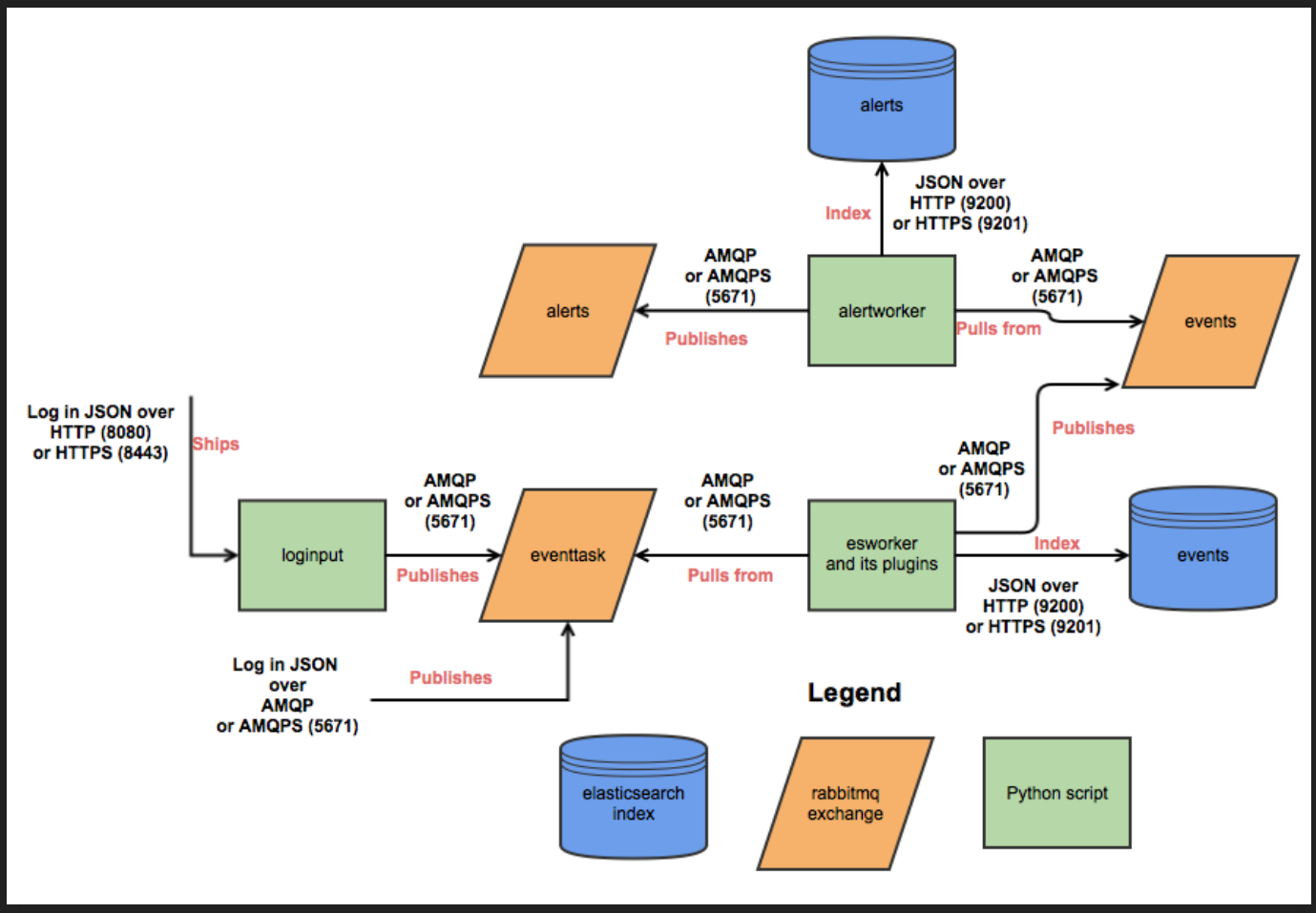
Missing? 'anomalies' <-- unknown

No perfect tool for the job

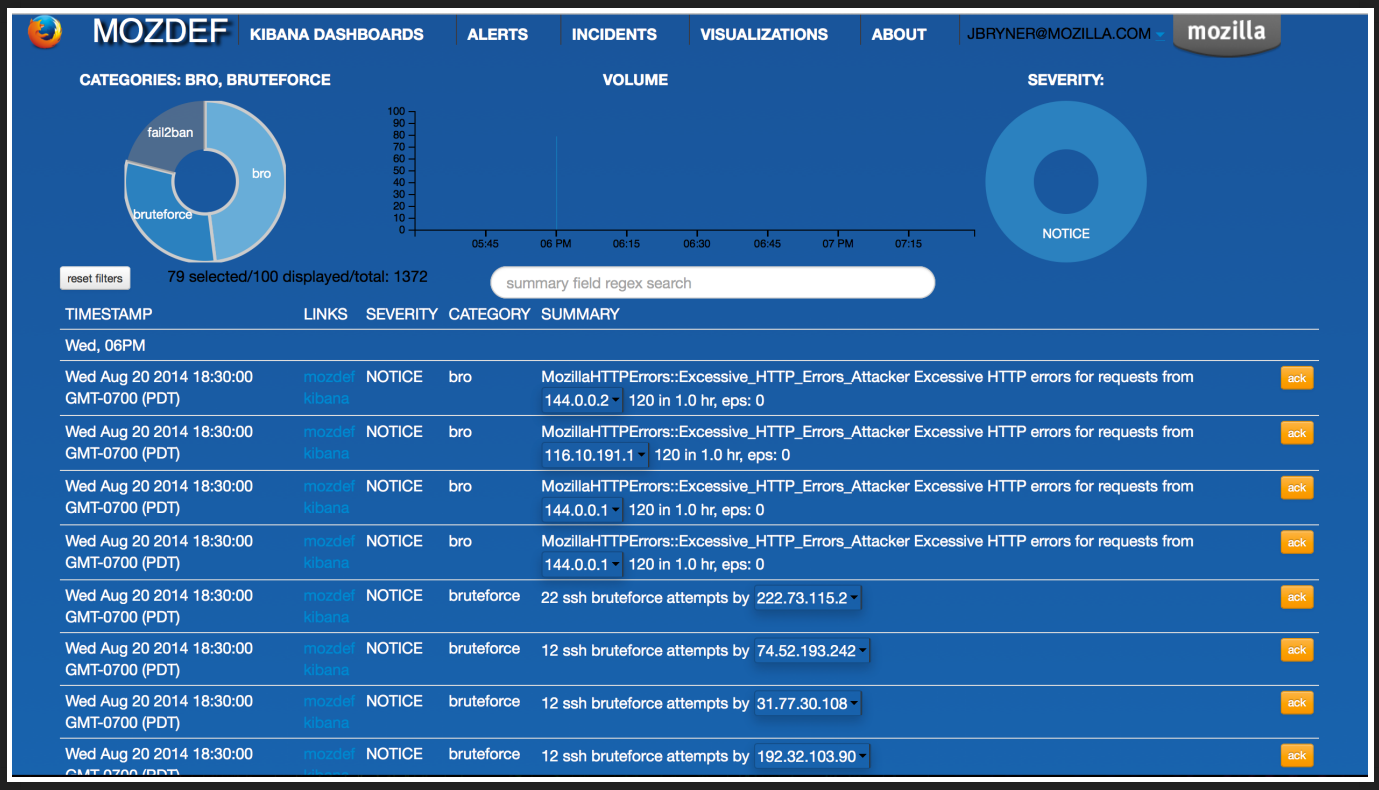
NSA? FSB? Ransomware and old Java? Risk managent FTW!!


12 people having hands full + MOC
MozDef
IQRisk
Intelligence
OpenSource
Exchanges
Internal
HTTP
AMQP
S3
HTTPS
Syslog
Suricata
Bro
Netsniff-ng
MIG
HTTP Observatory
Audit-JSON
Rapid7
Logs (System, Apps)
Paper trail
RRA

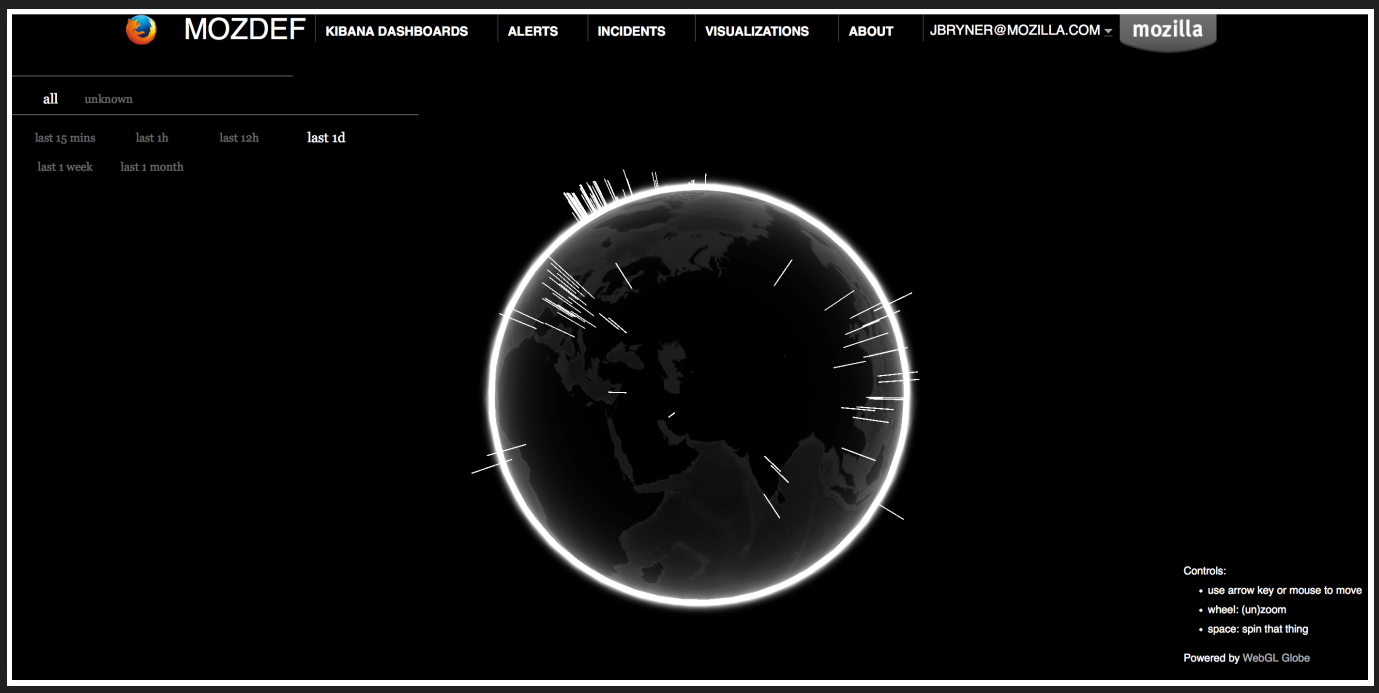
CAN'T GET ENOUGH



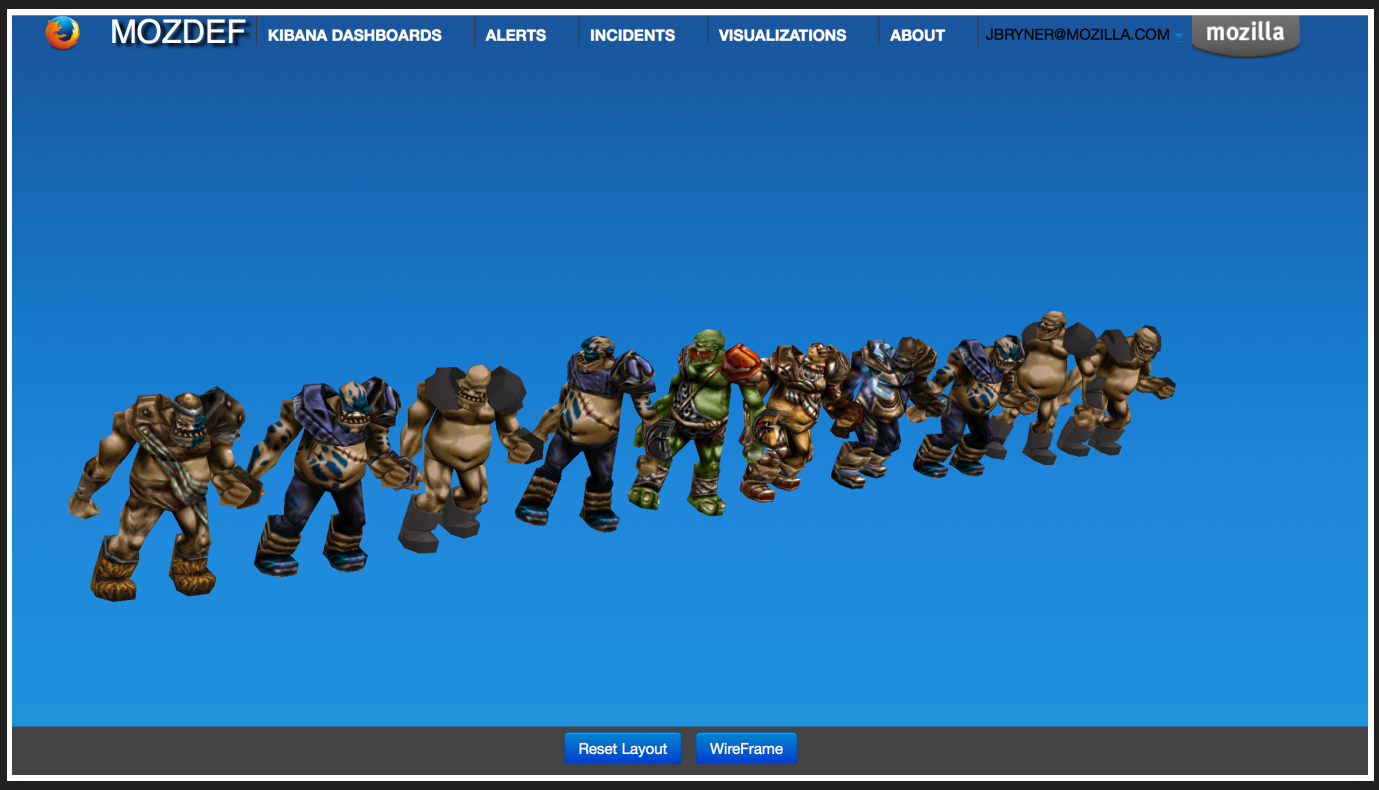
SPEAKING ABOUT TOOLS



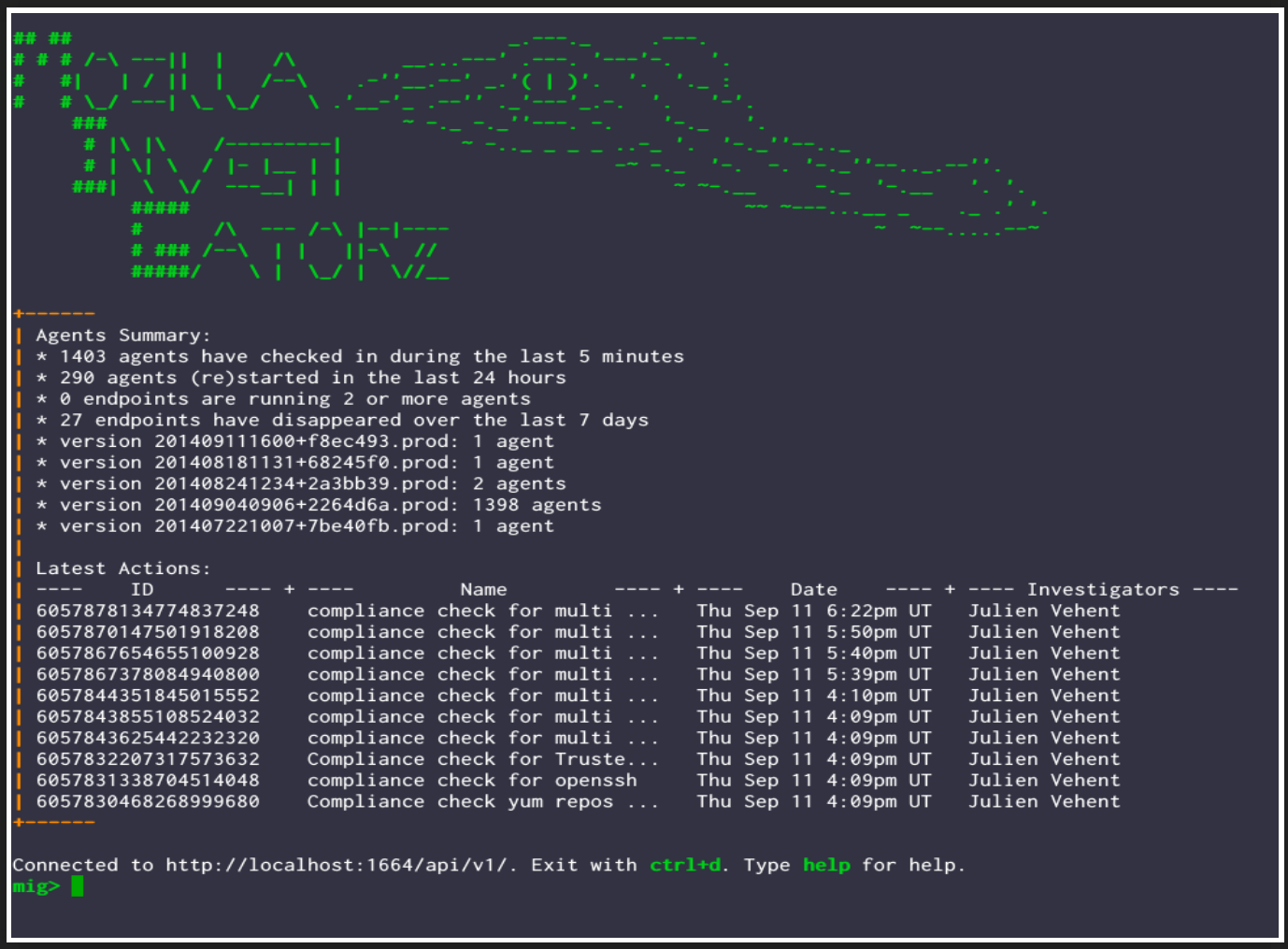
SPEAKING ABOUT TOOLS



SPEAKING ABOUT TOOLS



SPEAKING ABOUT TOOLS



```
+------
| Agents Summary:
| * 1403 agents have checked in during the last 5 minutes
| * 290 agents (re)started in the last 24 hours
| * 0 endpoints are running 2 or more agents
| * 27 endpoints have disappeared over the last 7 days
| * version 201409111600+f8ec493.prod: 1 agent
| * version 201408181131+68245f0.prod: 1 agent
| * version 201408241234+2a3bb39.prod: 2 agents
| * version 201409040906+2264d6a.prod: 1398 agents
| * version 201407221007+7be40fb.prod: 1 agent
|
| Latest Actions:
| ----    ID      ---- + ----         Name         ---- + ----    Date    ---- + ---- Investigators ----
| 6057878134774837248    compliance check for multi ...   Thu Sep 11 6:22pm UT   Julien Vehent
| 6057870147501918208    compliance check for multi ...   Thu Sep 11 5:50pm UT   Julien Vehent
| 6057867654655100928    compliance check for multi ...   Thu Sep 11 5:40pm UT   Julien Vehent
| 6057867378084940800    compliance check for multi ...   Thu Sep 11 5:39pm UT   Julien Vehent
| 6057844351845015552    compliance check for multi ...   Thu Sep 11 4:10pm UT   Julien Vehent
| 6057843855108524032    compliance check for multi ...   Thu Sep 11 4:09pm UT   Julien Vehent
| 6057843625442232320    compliance check for multi ...   Thu Sep 11 4:09pm UT   Julien Vehent
| 6057832207317573632    Compliance check for Truste...   Thu Sep 11 4:09pm UT   Julien Vehent
| 6057831338704514048    compliance check for openssh     Thu Sep 11 4:09pm UT   Julien Vehent
| 6057830468268999680    Compliance check yum repos ...   Thu Sep 11 4:09pm UT   Julien Vehent
+------

Connected to http://localhost:1664/api/v1/. Exit with ctrl+d. Type help for help.
mig>
```

SPEAKING ABOUT TOOLS


```
{
"category": "execve",
"processid": "0",
"receivedtimestamp": "2014-03-01T15:22:54.457658+00:00",
"severity": "INFO",
"utctimestamp": "2014-03-01T15:22:54+00:00",
"tags": ["audisp-json", "2.0.0", "audit"],
"timestamp": "2014-03-01T15:22:54+00:00",
"hostname": "admin1a.private.scl3.mozilla.com",
"mozdefhostname": "mozdef2.private.scl3.mozilla.com",
"summary": "Execve: nmap 63.245.214.53 -p22 -Pn",
"processname": "audisp-json",
"details": {
"fsuid": "3407",
"tty": "(none)",
```

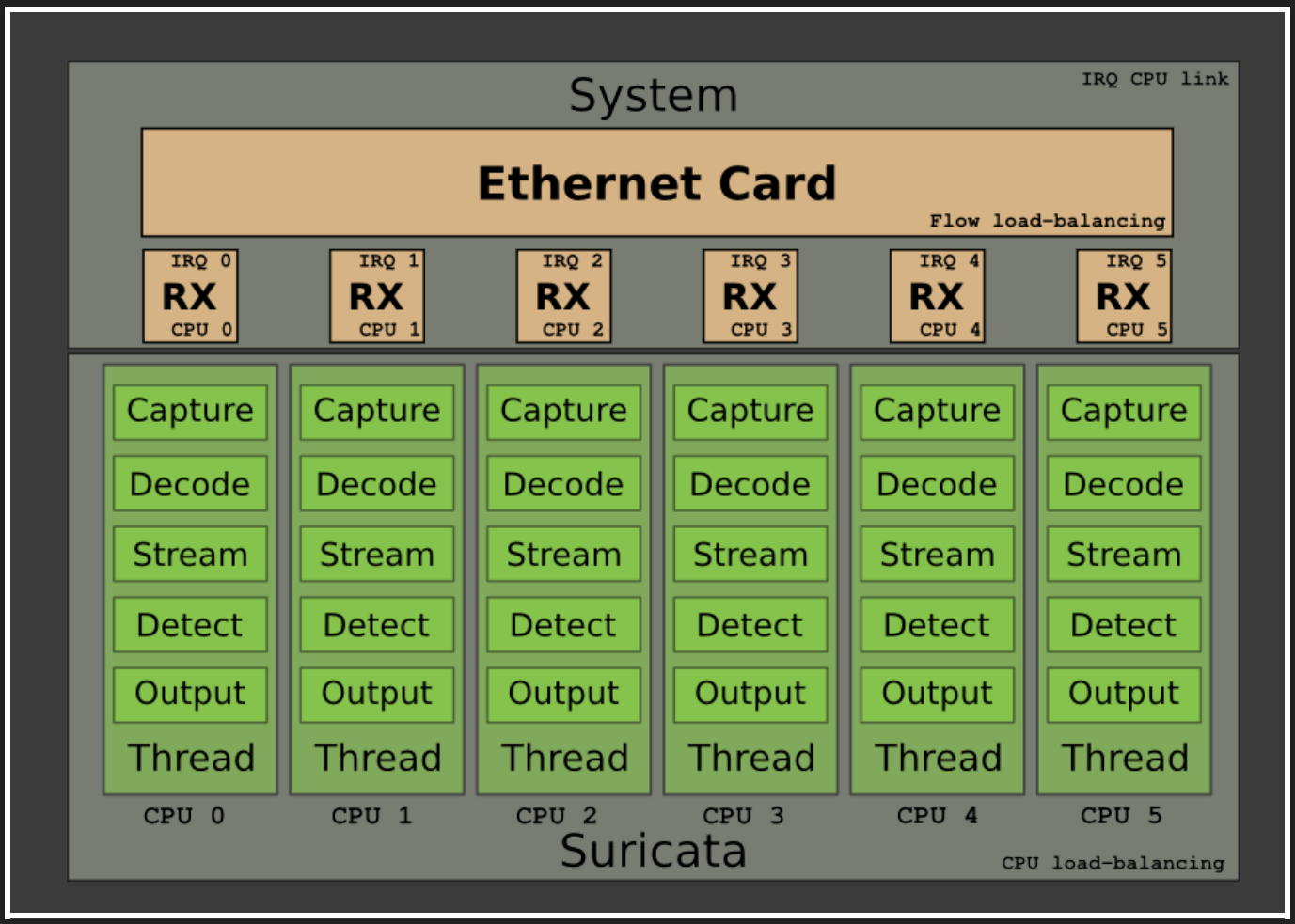
BASIC IDS FUNCTIONALITY

Stream reconstruction

Protocol level analysis

Pattern recognition

Decompressing content (HTTP)


System
IRQ CPU link
Ethernet Card
Flow load-balancing
IRQ 0
RX
CPU 0
IRQ 1
RX
CPU 1
IRQ 2
RX
CPU 2
IRQ 3
RX
CPU 3
IRQ 4
RX
CPU 4
IRQ 5
RX
CPU 5
Capture
Decode
Stream
Detect
Output
Thread
CPU 0
CPU 1
CPU 2
CPU 3
CPU 4
CPU 5
Suricata
CPU load-balancing

SURICATA IN 2016

IDS and IPS (nfq)

Multi threading

Protocol identification (port independent)

File identification and extraction, hash calculation

Deep TLS analysis

Application layer logs (in JSON)

Lua scripting

```
alert http $HOME_NET any -> $EXTERNAL_NET
any (msg:"ET CURRENT_EVENTS Unknown
Malicious Second Stage Download URI Struct
Sept 15 2015"; flow:established,to_server;
urilen:>46; content:".php?id="; http_uri;
fast_pattern:only; content:"&rnd=";
http_uri; pcre:"/\.php\?id=[0-9A-F]
{32,}&rnd=\d+$/U"; content:!"Referer|3a|";
http_header; classtype:trojan-activity;
sid:2021787; rev:2;)
```

LOOK MUM - NO PORTS!!

```
alert http $EXTERNAL_NET any -> $HOME_NET
any (msg:"ET CURRENT_EVENTS Cryptowall
docs campaign Sept 2015 encrypted binary
(1)"; flow:established,to_client;
file_data; content:"|23 31 f9 4f 62 57 73
67|"; within:8;
flowbits:set,et.exploitkitlanding;
classtype:trojan-activity; sid:2021778;
rev:2;)
```

MATCHING FILE_DATA LIKE A B^HPRO

EVENT LOGS


```
{
    "timestamp": "2009-11-24T21:27:09.534255",
    "event_type": "alert",
    "src_ip": "192.168.2.7",
    "src_port": 1041,
    "dest_ip": "x.x.250.50",
    "dest_port": 80,
    "proto": "TCP",
    "alert": {
        "action": "allowed",
        "gid": 1,
        "signature_id" :2001999,
        "rev": 9,
        "signature": "ET MALWARE BTGrab.com Spyware Downloading Ads"
        "category": "A Network Trojan was detected",
```

LUA IS COOL. AND RICH, TOO.

```
--[[
Detection for CVE-2016-0056 expects DOCX

This lua script can be run standalone and verbosely on a Flash file v
echo "run()" | luajit -i script name docx file

Francis Trudeau
With no help from Darien even though he loves LUA.
--]]

require("zip")

function init (args)
    local needs = {}
    needs["http.response_body"] = tostring(true)
```

```
alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"ET LUAJIT MS Off
```

CUSTOM HEADER MISSING?

Adding new protocol level fields - C code changes

Something invisible from Lua - C code changes

New input like Myricom/Netmap - C code changes

Sometimes add on functionality presents challenges

```
                        module MozillaHTTPHeaders;

export {
    redef record Intel::Info += {
        ## True client IP address added by our ZLBs
        cluster_client_ip: string &log &optional;
    };

    redef record Intel::Seen += {
        ## Log value of the X-CLUSTER-CLIENT-IP
        ## True client IP address added by our ZLBs
        cluster_client_ip: string &log &optional;
    };

    redef record HTTP::Info += {
```

I JUST COULD NOT RESIST

	Bro	Suricata
Intel Framework	Extend it - custom fields	Hardcoded fields
Logs	Rich, easy to extend	Hardcoded
Scripting	Bro IS scripting	Lua - hardcoded but powerful

ON THE OTHER HAND

	Bro	Suricata
Care and feed	Lots	Just runs
Performance	A few Gbit/sec	10? 20? 40Gbit/sec? 20 000 rules

WHAT ARE WE HUNTING FOR?

With Suricata. And Why.

Can I do it with Bro?

CnC - insane detection capabilities, tons of rules

```
2016-07-15T17:57:58+0000 CT7wYb3MaOc2KNL6P
10.252.28.186 60158 70.38.27.158 80 1 GET
support.pckeeper.com /ping.html - PCKAV
(1.1.1049.0) 6.2.9200.0 x64 0 6 200 OK - -
(empty) - - - - - FHii7k1cPGiCRJdDvk - - -
1.1
```

Where can we send this function? Nowhere. It stays here.

Interesting User-Agents

```
alert http any any -> any any
(msg:"SURICATA NetSession in
http_user_agent"; content:"NetSession";
http_user_agent; sid:2500024; rev:1;)
```

Where can we send this function?

```
event http_header(c: connection, is_orig:
bool, name: string, value: string)
```

Interesting DNS queries

```
alert udp any any -> any 53 (msg:"SURICATA DNS Query to a Suspicious
```

```
alert http any any -> any any (msg:"SURICATA HTTP Request to a Suspi
```

```
alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"ET INFO SUSPICIOU
                    <p></p>
```

Where can we send this function?

```
event http_header(c: connection, is_orig:
    bool, name: string, value: string)
```

```
event dns_*_reply()
```

```
ssl_extension_server_name(c: connection,
    is_orig: bool, names: string_vec)
```

SSL_* FUNCTIONS LET US FINGERPRINT AND MATCH ON PARTS OF SSL HANDSHAKE

Spoofed SSL certificates

```
alert tls any any -> any any (msg:"SURICATA SSL Gmail certificate no
```

```
alert tls any any -> any any (msg:"SURICATA SSL Google certificate n
```

Where can we send this function?

```
event log_ssl(rec: SSL::Info)
```

Or somewhere else. Ask Johanna ;-)

Private and public keys in clear

```
alert http any any -> any any (msg:"SURICATA FILE plaintext PEM RSA
```

```
alert http any any -> any any (msg:"SURICATA FILE plaintext OpenSSH
```

Where can we send this function?

Nowhere. It stays there.

Known cleartext malicious communication - think DFIR

```
alert udp any any -> any 53,1024 (msg:"example_message"; flow:to_ser
```

Where can we send this function?

Nowhere. It stays there.

Protocol anomalies

```
alert tcp any any -> any 80 (msg:"SURICATA non-HTTP on TCP port 80";
```

```
alert tcp any any -> any 53 (msg:"SURICATA non-DNS-TCP on TCP port 5
```

Two kinds of rules

X on non-X port

not-X on X-port

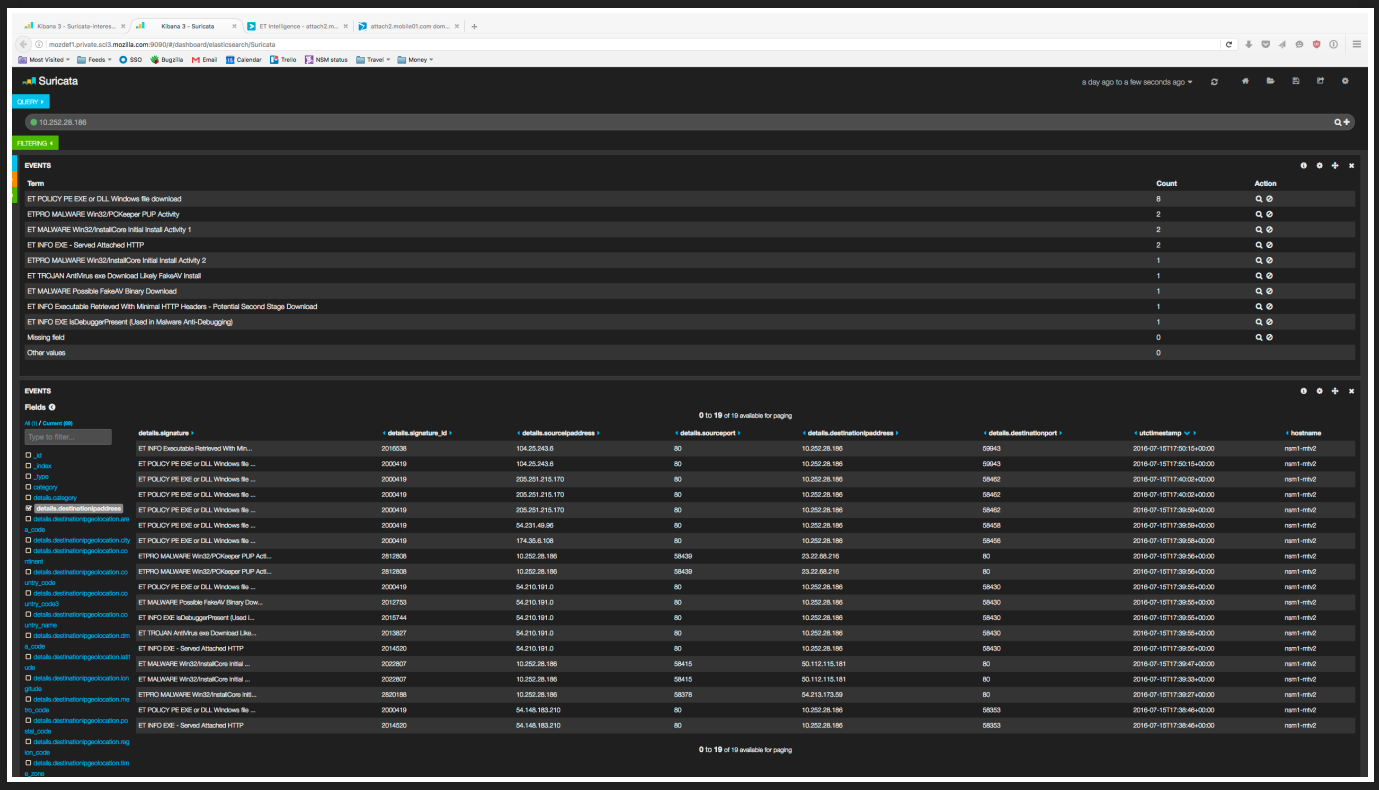
Where can we send this function?

DPD, maybe?

```
event protocol_confirmation(c: connection, atype: Analyzer::Tag, aid
```

```
event protocol_violation(c: connection, atype: Analyzer::Tag, aid: c
```

IS THIS A FALSE POSITIVE?



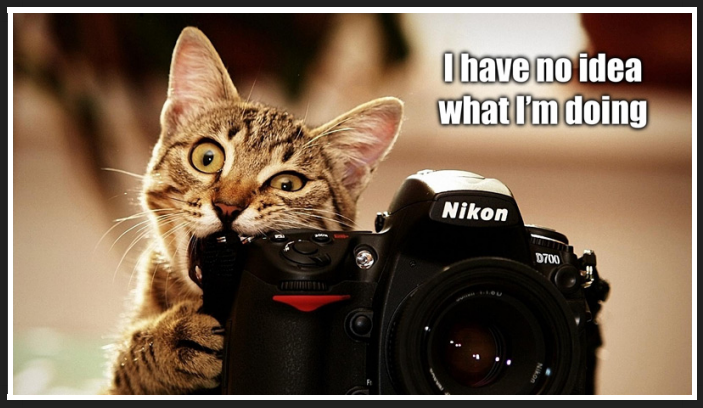
IS THIS A FALSE POSITIVE?

```
ET INFO Executable Retrieved With Minimal HTTP Headers - Potential S
ET POLICY PE EXE or DLL Windows file download
ET POLICY PE EXE or DLL Windows file download
ET POLICY PE EXE or DLL Windows file download
ET POLICY PE EXE or DLL Windows file download
ET POLICY PE EXE or DLL Windows file download
ET POLICY PE EXE or DLL Windows file download
ETPRO MALWARE Win32/PCKeeper PUP Activity
ETPRO MALWARE Win32/PCKeeper PUP Activity
ET POLICY PE EXE or DLL Windows file download
ET MALWARE Possible FakeAV Binary Download
ET TROJAN AntiVirus exe Download Likely FakeAV Install
ET INFO EXE IsDebuggerPresent (Used in Malware Anti-Debugging)
ET INFO EXE - Served Attached HTTP
ET MALWARE Win32/InstallCore Initial Install Activity 1
```

Likely a true positive. Likely is not enough.

Trust matters.

WHAT IF YOU DON'T KNOW?



False or True positive?

Who that is? IP -> MAC -> User

CONN.LOG - DNS.LOG - HTTP.LOG - SSL.LOG - X509.LOG - RADIUS.LOG - DHCP.LOG

```
2016-07-15T17:39:54+0000    C4uKjW65TBDf4szi5   10.252.28.186   5843
2016-07-15T17:39:56+0000    Cg4wDIyAY57iEt8h8   10.252.28.186   5843
2016-07-15T17:39:56+0000    Cg4wDIyAY57iEt8h8   10.252.28.186   5843
2016-07-15T17:39:59+0000    CM2Vh1chCZvJXiaM8   10.252.28.186   5846
2016-07-15T17:39:59+0000    CM2Vh1chCZvJXiaM8   10.252.28.186   5846
2016-07-15T17:39:59+0000    CM2Vh1chCZvJXiaM8   10.252.28.186   5846
2016-07-15T17:40:00+0000    CM2Vh1chCZvJXiaM8   10.252.28.186   5846
2016-07-15T17:40:00+0000    CM2Vh1chCZvJXiaM8   10.252.28.186   5846
2016-07-15T17:40:00+0000    CM2Vh1chCZvJXiaM8   10.252.28.186   5846
2016-07-15T17:40:00+0000    CM2Vh1chCZvJXiaM8   10.252.28.186   5846
2016-07-15T17:39:59+0000    CJkoAg4fmQ2KRPGT9c  10.252.28.186   5846
2016-07-15T17:40:00+0000    CJkoAg4fmQ2KRPGT9c  10.252.28.186   5846
2016-07-15T17:40:00+0000    CM2Vh1chCZvJXiaM8   10.252.28.186   5846
2016-07-15T17:40:01+0000    CM2Vh1chCZvJXiaM8   10.252.28.186   5846
2016-07-15T17:40:01+0000    CM2Vh1chCZvJXiaM8   10.252.28.186   5846
```

Infection confirmed End User Services unleashed

THE POWER OF CONTEXT

XCodeGhost detected. Multiple rules triggered. IP from a guest network. Anonymous to me. Isolated office. What if Mozillian?

ETPRO TROJAN XCodeGhost Beacon	2	ET TROJAN XcodeGhost CnC M2	2	ET TROJAN XcodeGhost CnC Checkin	2	ET TROJ XCodeGh DNS Lookup	

```
bro@nsm1-mtv2:/nsm/bro/logs$ zcat 2016-08-22/dns.* | bro-cut id.orig_
(...)
1 10.252.35.219   init.icloud-analysis.com    5.79.71.205,5.79.71.22
2 10.252.35.219   g1.163.com  123.58.176.66,123.58.176.65,123.58.179
2 10.252.35.219   music.163.com   103.251.128.85,103.251.128.86
```

```
10.252.35.219   POST    init.icloud-analysis.com    /   -   %E7%BD%9
10.252.35.219   POST    init.icloud-analysis.com    /   -   %E7%BD%9
```

WHO ARE YOU?

HTTP logs - User Agent `iPhone; iPhone OS 9.3.4; zh-Hans_US`

HTTP / SSL / DNS logs - multiple Mandarin apps

DHCP logs - user visits MTV2 irregularly

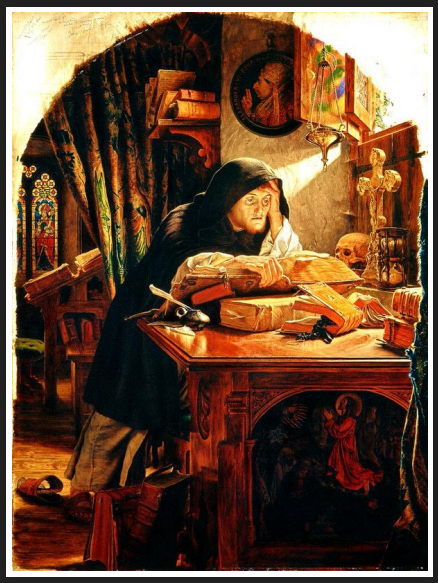
Opportunistic connections to the Guest WiFi. Little to no traffic.

Badging system logs!!

TUNNING

Developer looking at production logs after a regression with downtime. Oil canvas, circa 1580

Overheard: looks like Michal



https://github.com/michalpurzynski
@MichalPurzynski