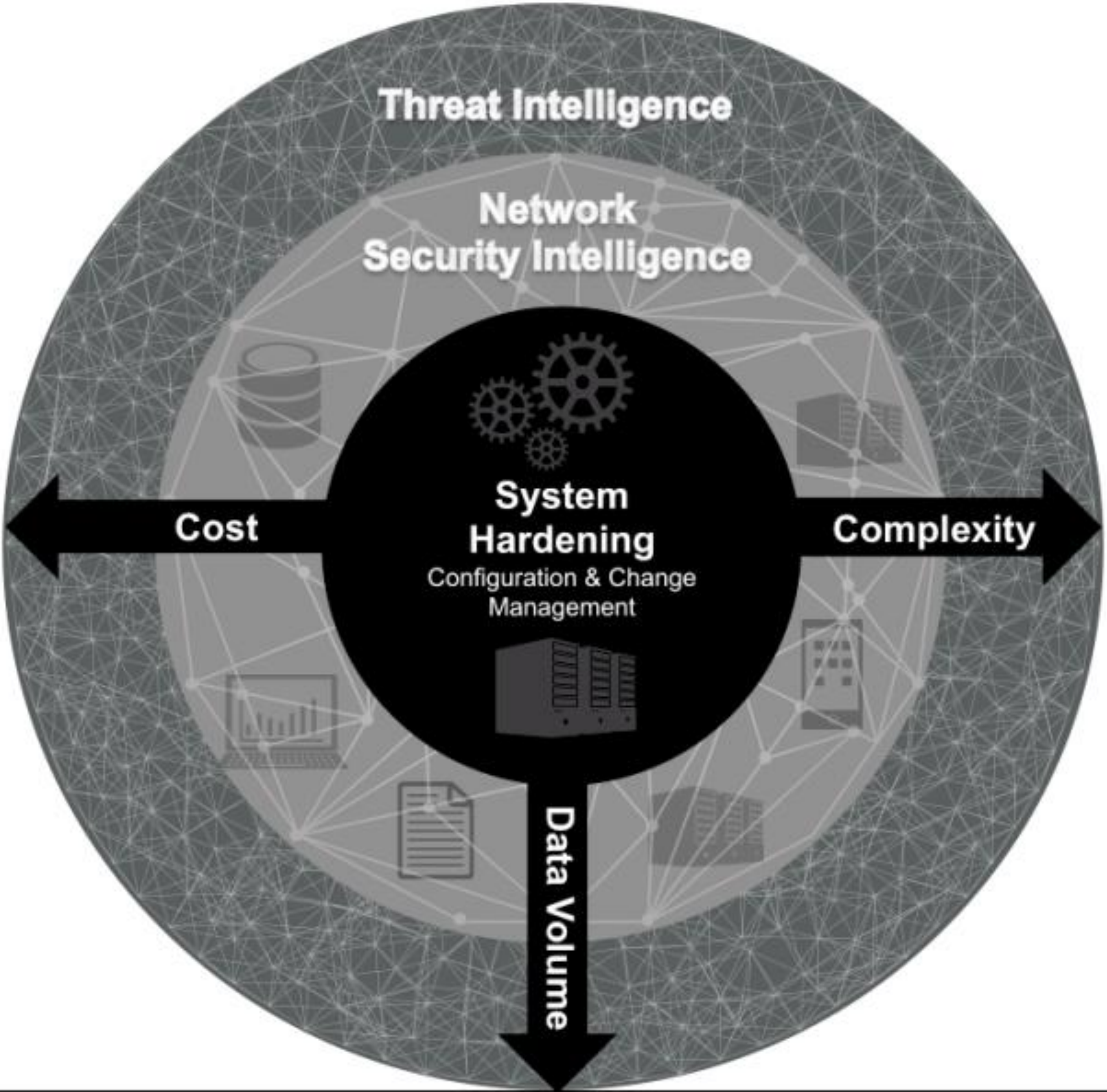
My Bro The ELK

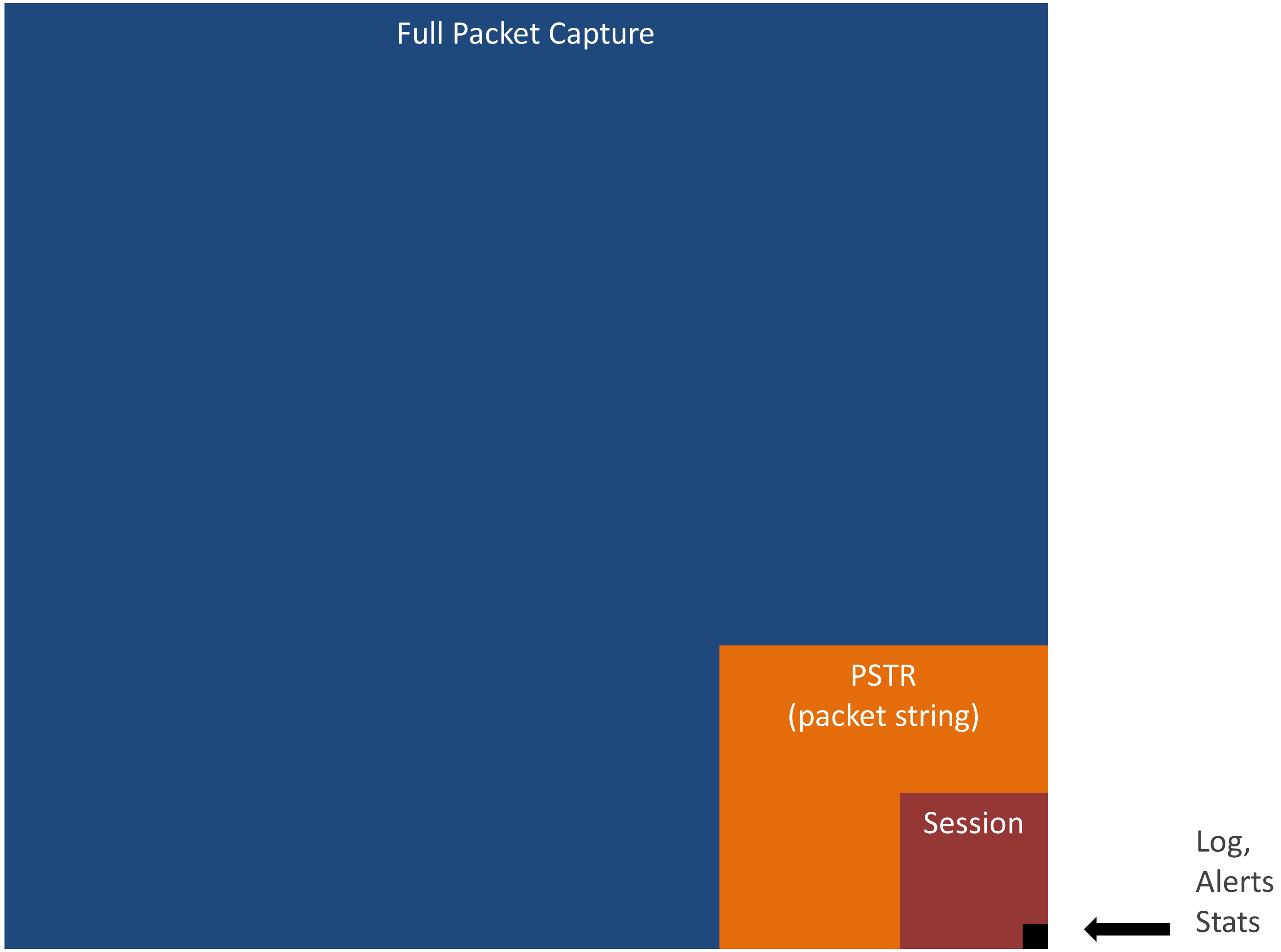
Obtaining Security Context from Security Events

Travis Smith
tsmith@tripwire.com

Agenda

- What is the problem?
- Who is the Bro?
- What is an ELK?
- Beefing up the ELK
- Making Your Bro the ELK Intelligent
- Visualization w/ Kibana
- Introducing the TARDIS framework


Threat Intelligence
Network Security Intelligence
System Hardening
Configuration & Change Management
Cost
Complexity
Data Volume



Full Packet Capture

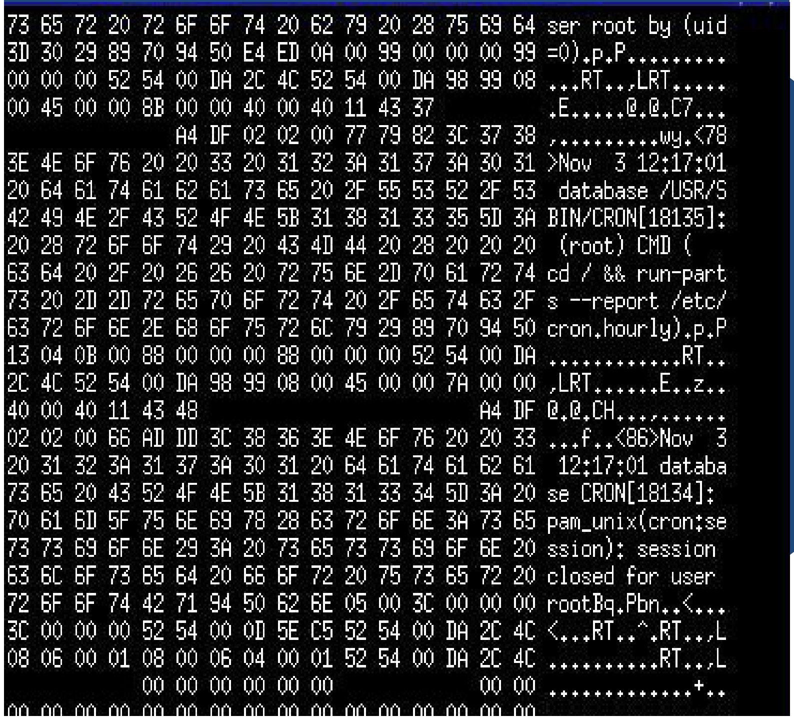
PSTR
(packet string)

Session

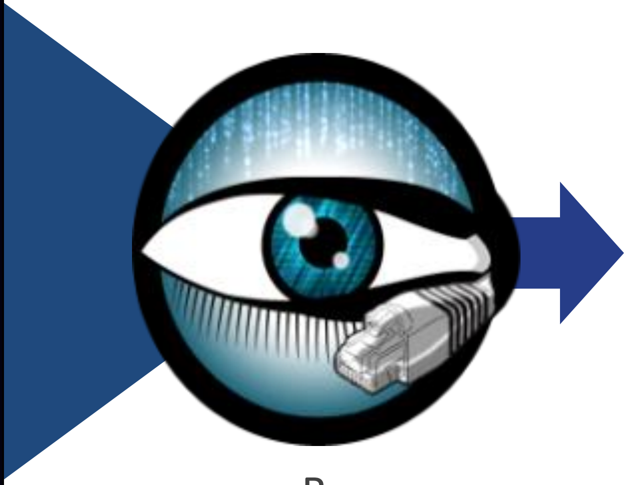
Log,
Alerts
Stats

Source: Applied Network Security Monitoring

Full Packet Capture



```
73 65 72 20 72 6F 6F 74 20 62 79 20 28 75 69 64 ser root by (uid
3D 30 29 89 70 94 50 E4 ED 0A 00 99 00 00 00 99 =0).p.P.........
00 00 00 52 54 00 DA 2C 4C 52 54 00 DA 98 99 08 ...RT..,LRT.....
00 45 00 00 8B 00 00 40 00 40 11 43 37           .E.....@.@.C7...
               A4 DF 02 02 00 77 79 82 3C 37 38 ,.........wy.<78
3E 4E 6F 76 20 20 33 20 31 32 3A 31 37 3A 30 31 >Nov  3 12:17:01
20 64 61 74 61 62 61 73 65 20 2F 55 53 52 2F 53  database /USR/S
42 49 4E 2F 43 52 4F 4E 5B 31 38 31 33 35 5D 3A BIN/CRON[18135]:
20 28 72 6F 6F 74 29 20 43 4D 44 20 28 20 20 20  (root) CMD (
63 64 20 2F 20 26 26 20 72 75 6E 2D 70 61 72 74 cd / && run-part
73 20 2D 2D 72 65 70 6F 72 74 20 2F 65 74 63 2F s --report /etc/
63 72 6F 6E 2E 68 6F 75 72 6C 79 29 89 70 94 50 cron.hourly).p.P
13 04 0B 00 88 00 00 00 88 00 00 00 52 54 00 DA ............RT..
2C 4C 52 54 00 DA 98 99 08 00 45 00 00 7A 00 00 ,LRT......E..z..
40 00 40 11 43 48                         A4 DF @.@.CH...,......
02 02 00 66 AD DD 3C 38 36 3E 4E 6F 76 20 20 33 ...f..<86>Nov  3
20 31 32 3A 31 37 3A 30 31 20 64 61 74 61 62 61  12:17:01 databa
73 65 20 43 52 4F 4E 5B 31 38 31 33 34 5D 3A 20 se CRON[18134]:
70 61 6D 5F 75 6E 69 78 28 63 72 6F 6E 3A 73 65 pam_unix(cron:se
73 73 69 6F 6E 29 3A 20 73 65 73 73 69 6F 6E 20 ssion): session
63 6C 6F 73 65 64 20 66 6F 72 20 75 73 65 72 20 closed for user
72 6F 6F 74 42 71 94 50 62 6E 05 00 3C 00 00 00 rootBq.Pbn..<...
3C 00 00 00 52 54 00 0D 5E C5 52 54 00 DA 2C 4C <...RT..^.RT..,L
08 06 00 01 08 00 06 04 00 01 52 54 00 DA 2C 4C ..........RT..,L
            00 00 00 00 00 00             00 00 .............+..
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```



Bro

conn.log
dhcp.log
dnp3.log
dns.log
ftp.log
http.log
irc.log
known_services.log
modbus.log
ius.log
smtp.log
snmp.log
ssh.log
ssl.log
syslog.log
tunnel.log
intel.log
notice.log

INPUTS

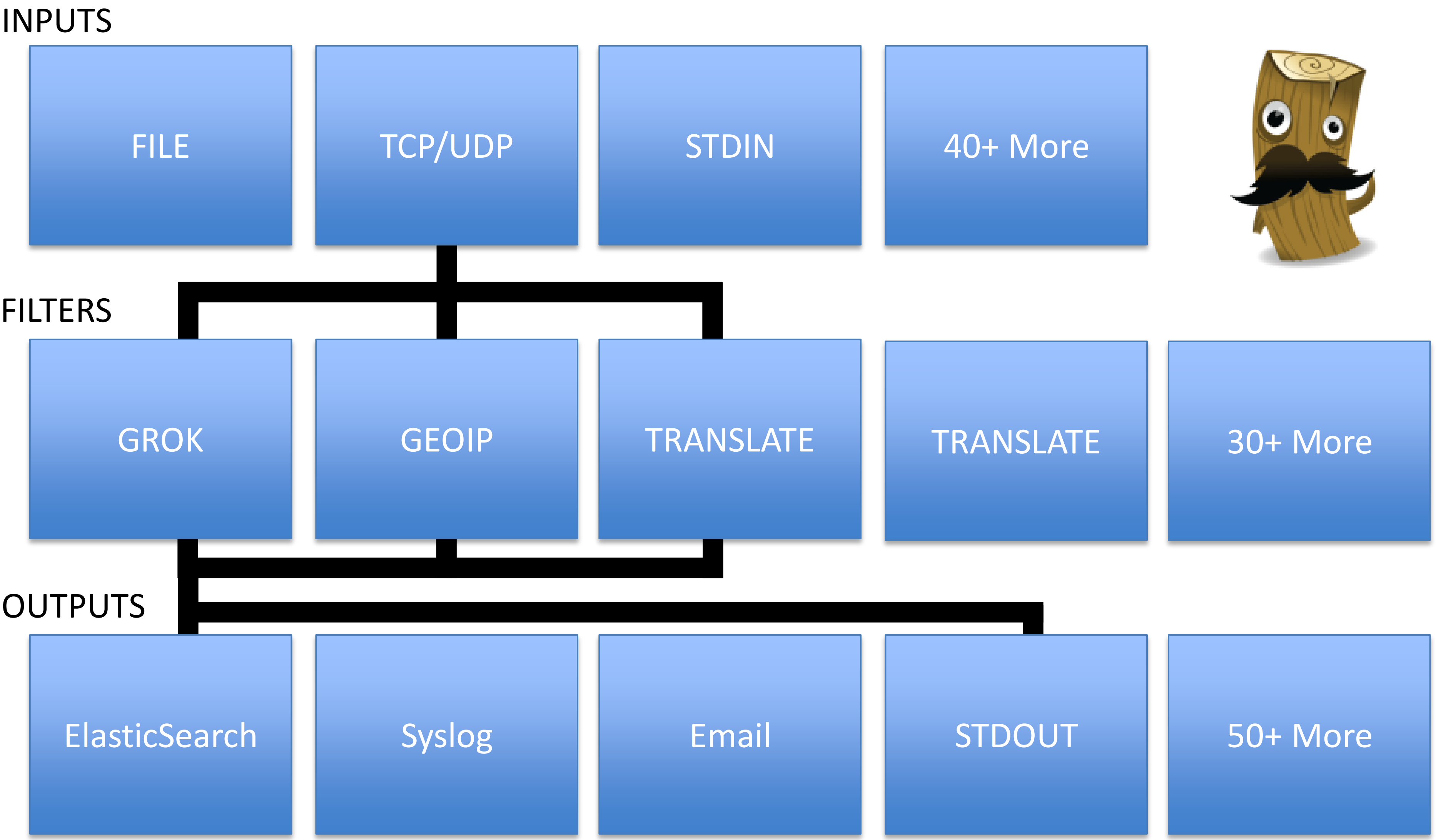
FILE | TCP/UDP | STDIN | 40+ More

FILTERS

GROK | GEOIP | TRANSLATE | TRANSLATE | 30+ More

OUTPUTS

ElasticSearch | Syslog | Email | STDOUT | 50+ More



INPUTS

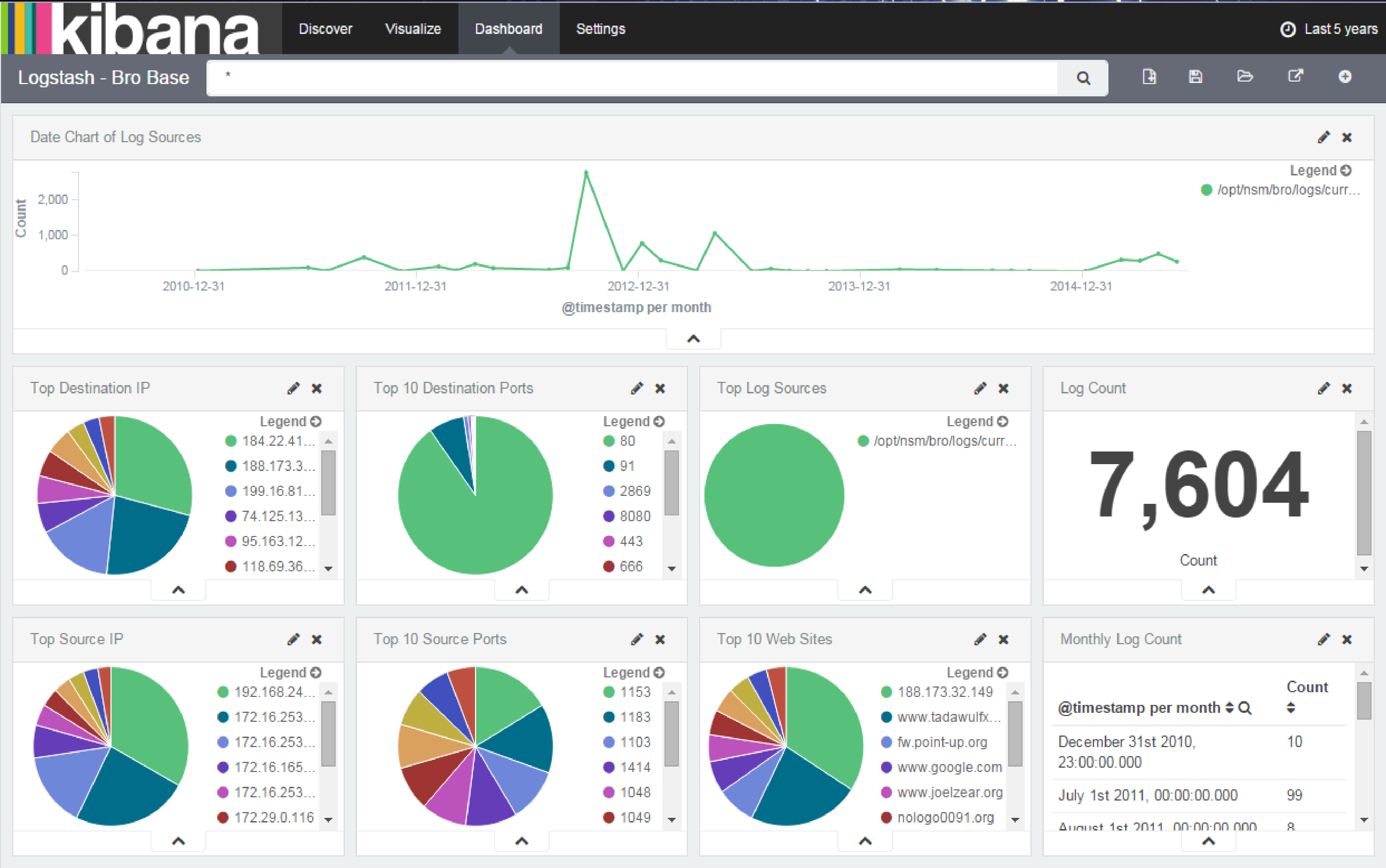
- FILE
- TCP/UDP
- STDIN
- 40+ More

FILTERS

- GROK
- GEOIP
- TRANSLATE
- TRANSLATE
- 30+ More

OUTPUTS

- ElasticSearch
- Syslog
- Email
- STDOUT
- 50+ More


kibana
Discover
Visualize
Dashboard
Settings
Last 5 years
Logstash - Bro Base
*
Date Chart of Log Sources
Count
2,000
1,000
0
2010-12-31
2011-12-31
2012-12-31
2013-12-31
2014-12-31
@timestamp per month
Legend
/opt/nsm/bro/logs/curr...
Top Destination IP
Legend
184.22.41...
188.173.3...
199.16.81...
74.125.13...
95.163.12...
118.69.36...
Top 10 Destination Ports
Legend
80
91
2869
8080
443
666
Top Log Sources
Legend
/opt/nsm/bro/logs/curr...
Log Count
Top Source IP
Legend
192.168.24...
172.16.253...
172.16.253...
172.16.165...
172.16.253...
172.29.0.116
Top 10 Source Ports
Legend
1153
1183
1103
1414
1048
1049
Top 10 Web Sites
Legend
188.173.32.149
www.tadawulfx...
fw.point-up.org
www.google.com
www.joelzear.org
nologo0091.org
Monthly Log Count

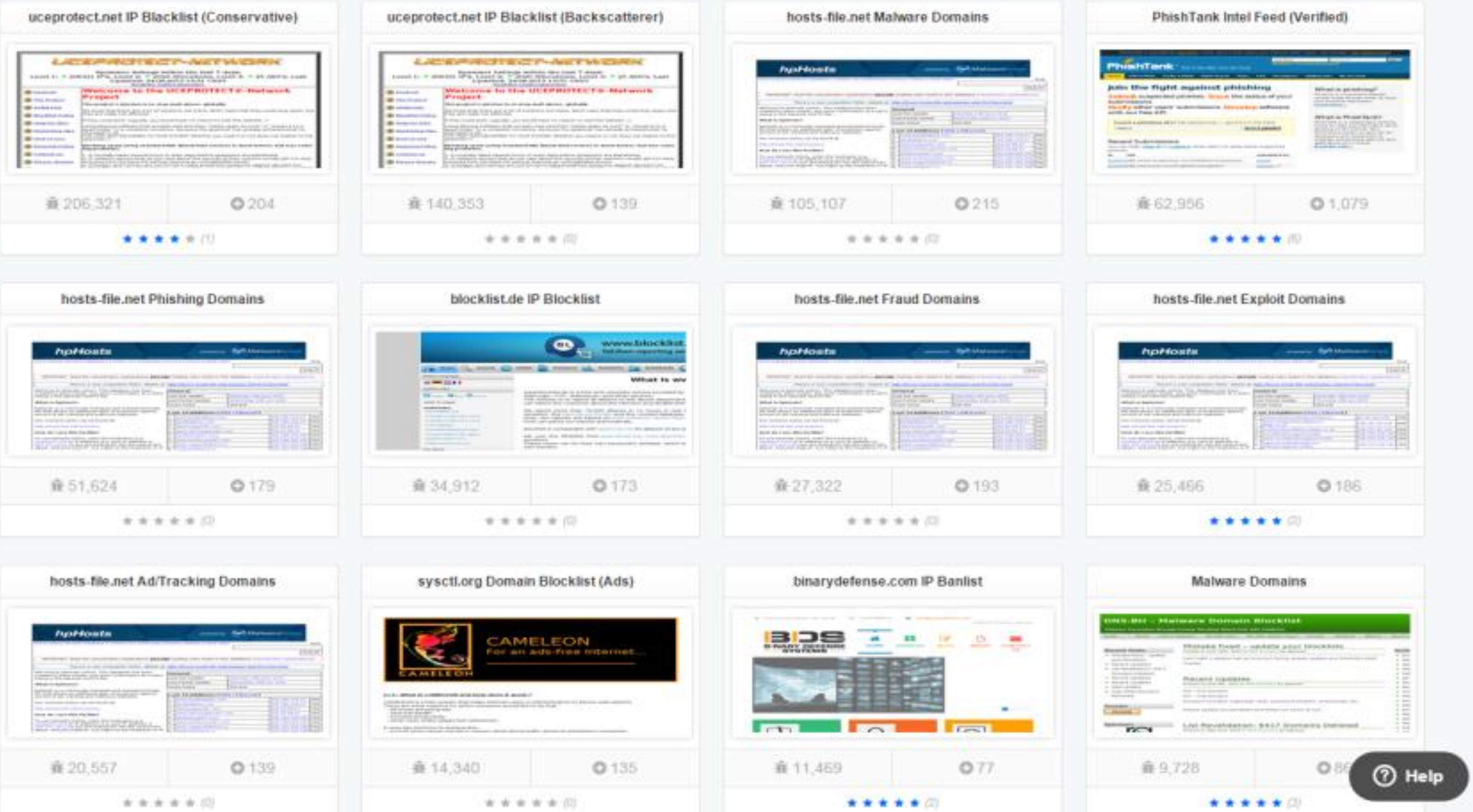
7,604

Count

@timestamp per month	Count
December 31st 2010, 23:00:00.000	10
July 1st 2011, 00:00:00.000	99
August 1st 2011, 00:00:00.000	8

SECURITY DATA > BIG DATA

Threat Intelligence Made Easy



uceprotect.net IP Blacklist (Conservative)
206,321 · 204
★★★★☆ (1)

uceprotect.net IP Blacklist (Backscatterer)
140,353 · 139
☆☆☆☆☆ (0)

hosts-file.net Malware Domains
105,107 · 215
☆☆☆☆☆ (0)

PhishTank Intel Feed (Verified)
62,956 · 1,079
★★★★★ (6)

hosts-file.net Phishing Domains
51,624 · 179
☆☆☆☆☆ (0)

blocklist.de IP Blocklist
34,912 · 173
☆☆☆☆☆ (0)

hosts-file.net Fraud Domains
27,322 · 193
☆☆☆☆☆ (0)

hosts-file.net Exploit Domains
25,466 · 186
★★★★★ (2)

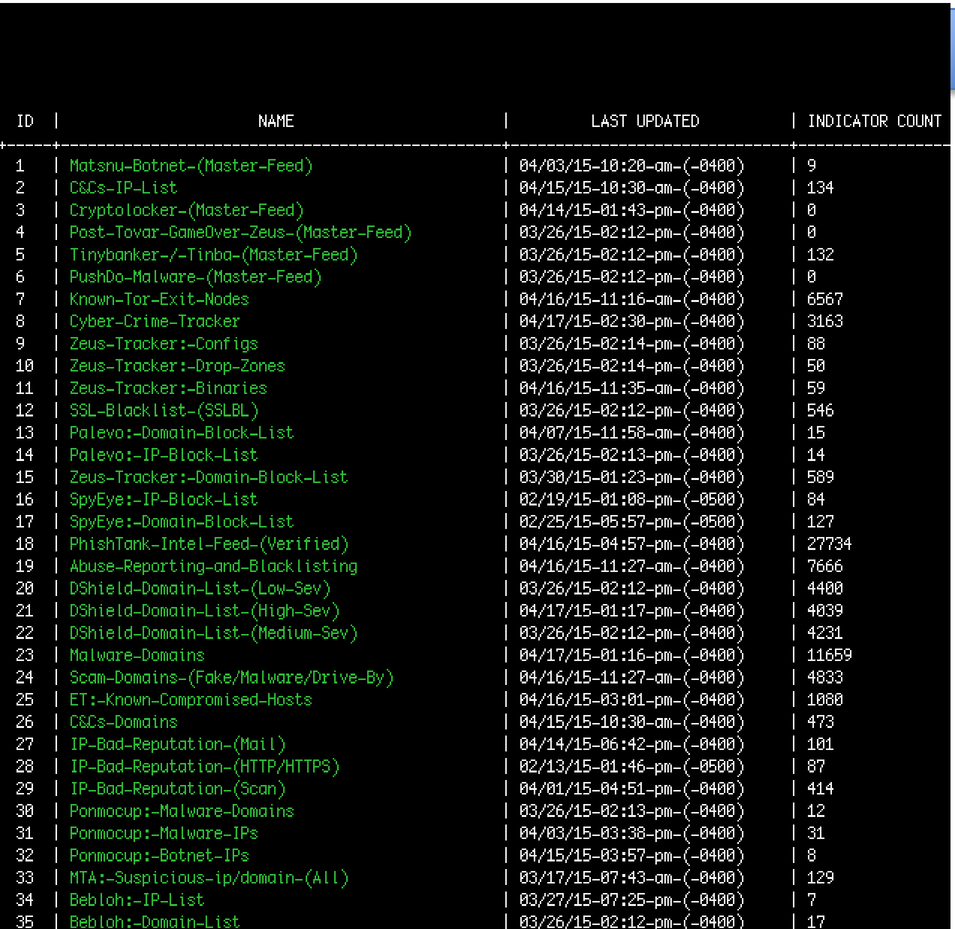
hosts-file.net Ad/Tracking Domains
20,557 · 139
☆☆☆☆☆ (0)

sysctl.org Domain Blocklist (Ads)
14,340 · 135
☆☆☆☆☆ (0)

binarydefense.com IP Banlist
11,469 · 77
★★★★★ (2)

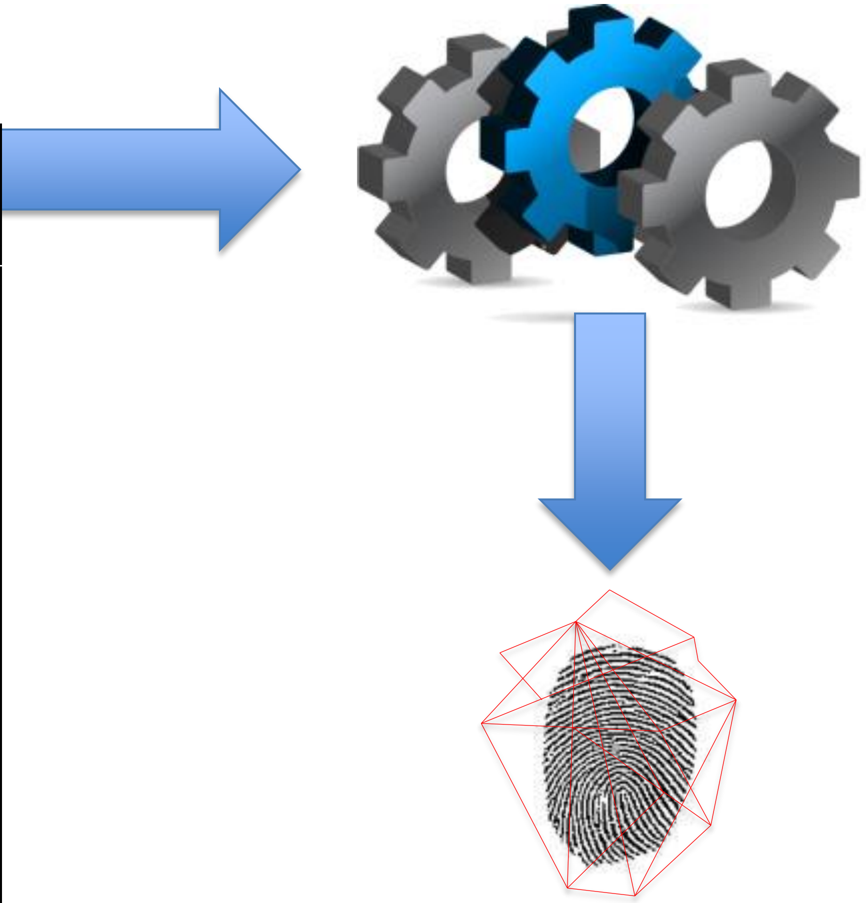
Malware Domains
9,728 · 86
★★★★★ (3)

Critical Stack Agent



```
ID  |                    NAME                         |          LAST UPDATED          | INDICATOR COUNT
+-----+-------------------------------------------------+--------------------------------+----------------
1   | Matsnu-Botnet-(Master-Feed)                     | 04/03/15-10:20-am-(-0400)      | 9
2   | C&Cs-IP-List                                    | 04/15/15-10:30-am-(-0400)      | 134
3   | Cryptolocker-(Master-Feed)                      | 04/14/15-01:43-pm-(-0400)      | 0
4   | Post-Tovar-GameOver-Zeus-(Master-Feed)          | 03/26/15-02:12-pm-(-0400)      | 0
5   | Tinybanker-/-Tinba-(Master-Feed)                | 03/26/15-02:12-pm-(-0400)      | 132
6   | PushDo-Malware-(Master-Feed)                    | 03/26/15-02:12-pm-(-0400)      | 0
7   | Known-Tor-Exit-Nodes                            | 04/16/15-11:16-am-(-0400)      | 6567
8   | Cyber-Crime-Tracker                             | 04/17/15-02:30-pm-(-0400)      | 3163
9   | Zeus-Tracker:-Configs                           | 03/26/15-02:14-pm-(-0400)      | 88
10  | Zeus-Tracker:-Drop-Zones                        | 03/26/15-02:14-pm-(-0400)      | 50
11  | Zeus-Tracker:-Binaries                          | 04/16/15-11:35-am-(-0400)      | 59
12  | SSL-Blacklist-(SSLBL)                           | 03/26/15-02:12-pm-(-0400)      | 546
13  | Palevo:-Domain-Block-List                       | 04/07/15-11:58-am-(-0400)      | 15
14  | Palevo:-IP-Block-List                           | 03/26/15-02:13-pm-(-0400)      | 14
15  | Zeus-Tracker:-Domain-Block-List                 | 03/30/15-01:23-pm-(-0400)      | 589
16  | SpyEye:-IP-Block-List                           | 02/19/15-01:08-pm-(-0500)      | 84
17  | SpyEye:-Domain-Block-List                       | 02/25/15-05:57-pm-(-0500)      | 127
18  | PhishTank-Intel-Feed-(Verified)                 | 04/16/15-04:57-pm-(-0400)      | 27734
19  | Abuse-Reporting-and-Blacklisting                | 04/16/15-11:27-am-(-0400)      | 7666
20  | DShield-Domain-List-(Low-Sev)                   | 03/26/15-02:12-pm-(-0400)      | 4400
21  | DShield-Domain-List-(High-Sev)                  | 04/17/15-01:17-pm-(-0400)      | 4039
22  | DShield-Domain-List-(Medium-Sev)                | 03/26/15-02:12-pm-(-0400)      | 4231
23  | Malware-Domains                                 | 04/17/15-01:16-pm-(-0400)      | 11659
24  | Scam-Domains-(Fake/Malware/Drive-By)            | 04/16/15-11:27-am-(-0400)      | 4833
25  | ET:-Known-Compromised-Hosts                     | 04/16/15-03:01-pm-(-0400)      | 1080
26  | C&Cs-Domains                                    | 04/15/15-10:30-am-(-0400)      | 473
27  | IP-Bad-Reputation-(Mail)                        | 04/14/15-06:42-pm-(-0400)      | 101
28  | IP-Bad-Reputation-(HTTP/HTTPS)                  | 02/13/15-01:46-pm-(-0500)      | 87
29  | IP-Bad-Reputation-(Scan)                        | 04/01/15-04:51-pm-(-0400)      | 414
30  | Ponmocup:-Malware-Domains                       | 03/26/15-02:13-pm-(-0400)      | 12
31  | Ponmocup:-Malware-IPs                           | 04/03/15-03:38-pm-(-0400)      | 31
32  | Ponmocup:-Botnet-IPs                            | 04/15/15-03:57-pm-(-0400)      | 8
33  | MTA:-Suspicious-ip/domain-(All)                 | 03/17/15-07:43-am-(-0400)      | 129
34  | Bebloh:-IP-List                                 | 03/27/15-07:25-pm-(-0400)      | 7
35  | Bebloh:-Domain-List                             | 03/26/15-02:12-pm-(-0400)      | 17
```

98 Threat Feeds



800,000+ Indicators

Logstash Filtering

- Utilizing Custom Patterns
- GROK Message Filtering
- Adding Custom Fields
- Adding Geo IP Data
- Date Match
- Using Translations for Threat Intel

Logstash Configuration

```
filter {
	grok {
		match => {
			"message" => "%{IP:client} %{WORD:method} %{URIPATHPARAM:request} %{NUMBER:bytes} %{NUMBER:duration}"
		}
	}
}
```

Utilize Custom Patterns

```
filter {
        grok {
                patterns_dir => "/opt/logstash/custom_patterns"
                match => {
                        message => "%{291001}“
                }
        }
}
```

```
/opt/logstash/custom_patterns/bro.rule
291001 (?<start_time>\d{10}\.\d{6})\t(?<evt_srcip>[\d\.]+)\t(?<evt_dstip>[\d\.]+)\t(?<evt_srcport>\d+)\t…
```

Message Filtering

```
filter {
        if [message] =~ /^((\d{10}\.\d{6})\t([\d\.]+)([\d\.]+)\t(\d+)\t(\d+)\t(\w+))/ {
                grok {
                        patterns_dir => "/opt/logstash/custom_patterns"
                        match => {
                                message => "%{291001}“
                        }
                }
        }
}
```

Remove Capture Groups

~~291001~~ (~~?<start_time>~~\d{10}\.\d{6})\t(~~?<evt_srcip>~~[\d\.]+)\t(~~?<evt_dstip>~~[\d\.]+)\t(~~?<evt_srcport>~~\d+)\t…

Add Custom Fields

```
filter {
        if [message] =~ /^((\d{10}\.\d{6})\t([\d\.]+)([\d\.]+)\t(\d+)\t(\d+)\t(\w+))/ {
                grok {
                        patterns_dir => "/opt/logstash/custom_patterns"
                        match => {
                                message => "%{291001}“
                        }
                        add_field => [ "rule_id", "291001" ]
                        add_field => [ "Device Type", "IPSIDSDevice" ]
                        add_field => [ "Object", "NetworkTraffic" ]
                        add_field => [ "Action", "General" ]
                        add_field => [ "Status", "Informational" ]
                }
        }
}
```

Geo IP

```
filter {
        .....all normalization code above here....
        geoip {
                source => "evt_dstip"
                target => "geoip_dst"
                database => “/etc/logstash/conf.d/GeoLiteCity.dat“
                add_field => [ "[geoip_dst][coordinates]", "%{[geoip_dst][longitude]}" ]
                add_field => [ "[geoip_dst][coordinates]", "%{[geoip_dst][latitude]}"  ]
                add_field => [ "[geoip_dst][coordinates]", "%{[geoip_dst][city\_name]}"  ]
                add_field => [ "[geoip_dst][coordinates]", "%{[geoip_dst][continent\_code]}"  ]
                add_field => [ "[geoip_dst][coordinates]", "%{[geoip_dst][country\_name]}"  ]
                add_field => [ "[geoip_dst][coordinates]", "%{[geoip_dst][postal\_code]}"  ]}
        mutate {
                convert => [ "[geoip_dst][coordinates]", "float"]
        }
}
```

New ElasticSearch
Template Needed

GeoIP Template Update

```
curl -XGET localhost:9200/_template/logstash
{"logstash":{
    "order":0,
    "template":"logstash-*",
    "settings":{
        "index.refresh_interval":"5s"
    },
    "mappings":{
        "properties":{
            "geoip":{
                "dynamic":true,
                "properties":{
                    "location":{
                        "type":"geo_point"
                    }
                },
                "type":"object"
            },
            …
```

```
{~~"logstash":{~~
    ~~"order":0,~~
    "template":"logstash-*",
    "settings":{
        "index.refresh_interval":"5s"
    },
    "mappings":{
        "properties":{
            "geoip_dst":{
                "dynamic":true,
                "properties":{
                    "location":{
                        "type":"geo_point"
                    }
                },
                "type":"object"
            },
            …
```

```
curl -XPUT localhost:9200/_template/logstash -d ‘….’
```

Date Match

```
filter {
        ....all normalization code above here....
        ....all GeoIP code here....
        date {
                match => [ "start_time", "UNIX" ]
        }
}
```

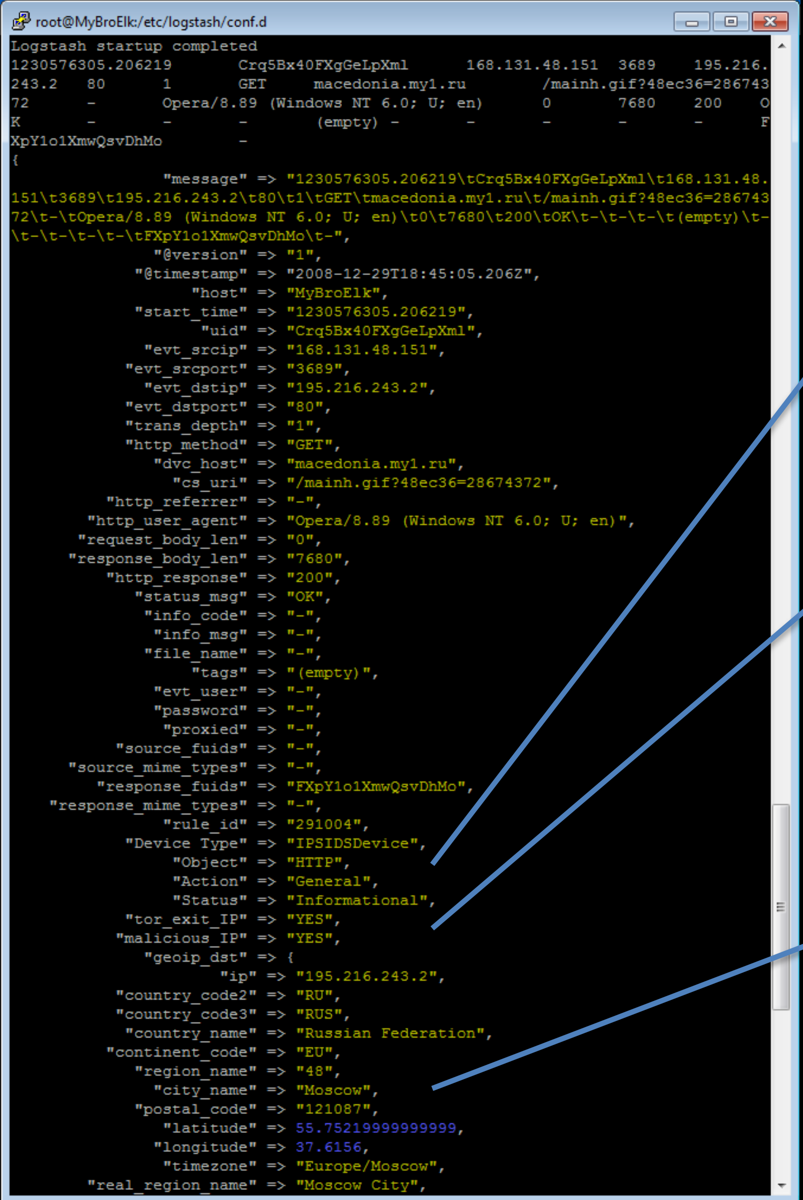
Threat Intel

```
filter {
        ....all normalization code above here....
        ....all GeoIP code here....
         translate {
                field => "evt_dstip"
                destination => "tor_exit_IP"
                dictionary_path => '/etc/logstash/conf.d/torexit.yaml'
        }
}
```

torexil.yaml

```
"162.247.72.201": "YES"
"24.187.20.8": "YES"
"193.34.117.51": "YES"
```

- Run Scripts to update the YAML files on a regular basis
- Logstash will check the YAML for updates every 300 seconds
  - Configurable by adding refresh_interval => numSeconds



```
Logstash startup completed
1230576305.206219       Crq5Bx40FXgGeLpXml      168.131.48.151  3689    195.216.
243.2   80      1       GET     macedonia.my1.ru        /mainh.gif?48ec36=286743
72      -       Opera/8.89 (Windows NT 6.0; U; en)      0       7680    200     O
K       -       -       -       (empty) -       -       -       -       -       F
XpY1o1XmwQsvDhMo        -
{
                "message" => "1230576305.206219\tCrq5Bx40FXgGeLpXml\t168.131.48.
151\t3689\t195.216.243.2\t80\t1\tGET\tmacedonia.my1.ru\t/mainh.gif?48ec36=286743
72\t-\tOpera/8.89 (Windows NT 6.0; U; en)\t0\t7680\t200\tOK\t-\t-\t-\t(empty)\t-
\t-\t-\t-\t-\tFXpY1o1XmwQsvDhMo\t-",
               "@version" => "1",
             "@timestamp" => "2008-12-29T18:45:05.206Z",
                   "host" => "MyBroElk",
             "start_time" => "1230576305.206219",
                    "uid" => "Crq5Bx40FXgGeLpXml",
              "evt_srcip" => "168.131.48.151",
            "evt_srcport" => "3689",
              "evt_dstip" => "195.216.243.2",
            "evt_dstport" => "80",
            "trans_depth" => "1",
            "http_method" => "GET",
               "dvc_host" => "macedonia.my1.ru",
                 "cs_uri" => "/mainh.gif?48ec36=28674372",
          "http_referrer" => "-",
        "http_user_agent" => "Opera/8.89 (Windows NT 6.0; U; en)",
       "request_body_len" => "0",
      "response_body_len" => "7680",
          "http_response" => "200",
             "status_msg" => "OK",
              "info_code" => "-",
               "info_msg" => "-",
              "file_name" => "-",
                   "tags" => "(empty)",
               "evt_user" => "-",
               "password" => "-",
                "proxied" => "-",
           "source_fuids" => "-",
      "source_mime_types" => "-",
         "response_fuids" => "FXpY1o1XmwQsvDhMo",
    "response_mime_types" => "-",
                "rule_id" => "291004",
            "Device Type" => "IPSIDSDevice",
                 "Object" => "HTTP",
                 "Action" => "General",
                 "Status" => "Informational",
            "tor_exit_IP" => "YES",
           "malicious_IP" => "YES",
              "geoip_dst" => {
                      "ip" => "195.216.243.2",
           "country_code2" => "RU",
           "country_code3" => "RUS",
            "country_name" => "Russian Federation",
          "continent_code" => "EU",
             "region_name" => "48",
               "city_name" => "Moscow",
             "postal_code" => "121087",
                "latitude" => 55.75219999999999,
               "longitude" => 37.6156,
                "timezone" => "Europe/Moscow",
        "real_region_name" => "Moscow City",
```

Custom Fields:

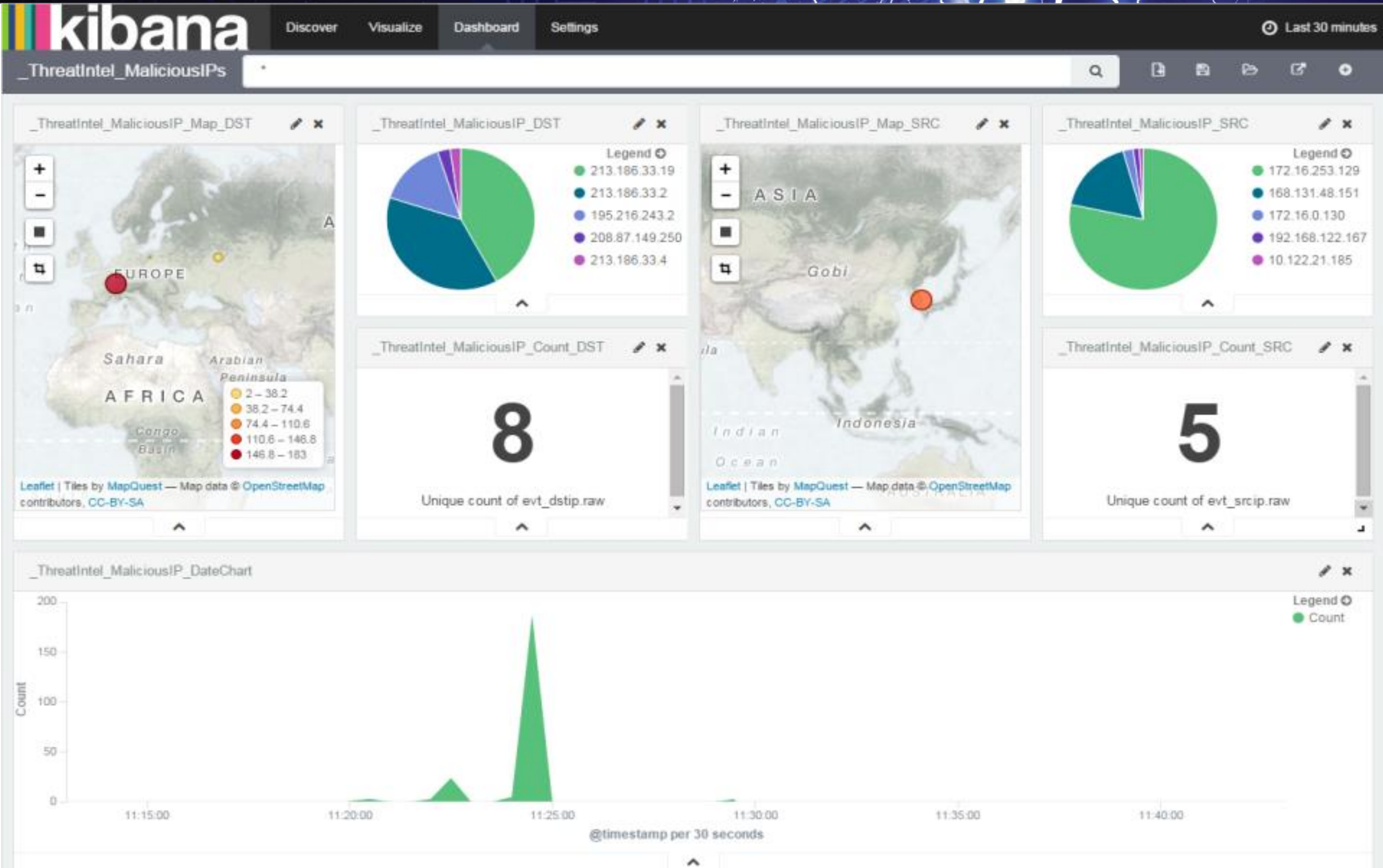
"Device Type" => "IPSIDSDevice"
"Object" => "HTTP"
"Action" => "General"
"Status" => "Informational"

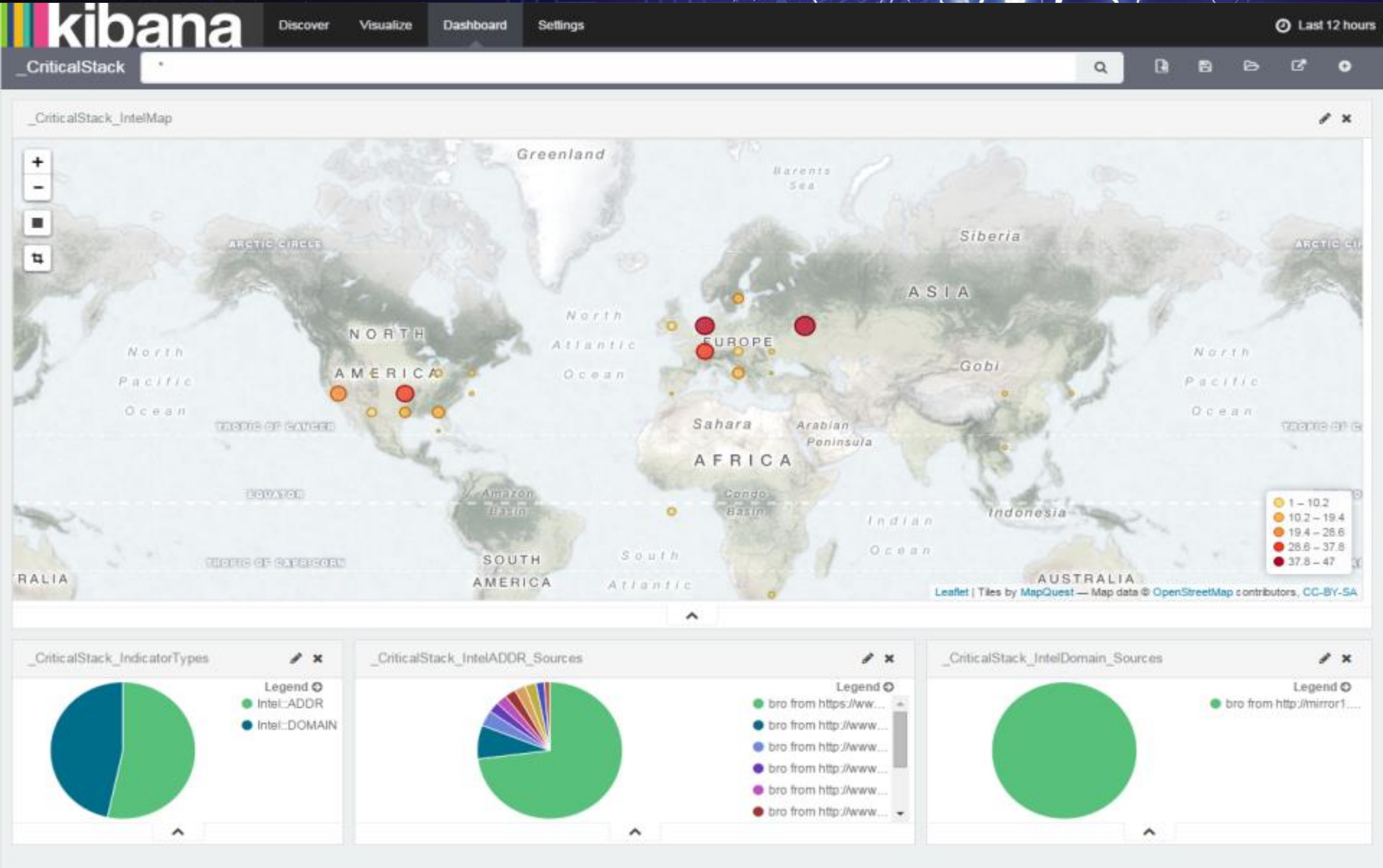
Threat Intel Translations:

"tor_exit_IP" => "YES"
"malicious_IP" => "YES"

Geo IP Data:

"country_code2" => "RU"
"country_code3" => "RUS"
"country_name" => "Russian Federation"
"continent_code" => "EU"
"city_name" => "Moscow"
"postal_code" => "121087"
"latitude" => 55.75219999999999
"longitude" => 37.6156
"timezone" => "Europe/Moscow"


kibana
Discover
Visualize
Dashboard
Settings
Last 30 minutes
_ThreatIntel_MaliciousIPs
*
_ThreatIntel_MaliciousIP_Map_DST
EUROPE
Sahara
Arabian Peninsula
AFRICA
Congo Basin
2 – 38.2
38.2 – 74.4
74.4 – 110.6
110.6 – 146.8
146.8 – 183
Leaflet | Tiles by MapQuest — Map data © OpenStreetMap contributors, CC-BY-SA
_ThreatIntel_MaliciousIP_DST
Legend
213.186.33.19
213.186.33.2
195.216.243.2
208.87.149.250
213.186.33.4
_ThreatIntel_MaliciousIP_Count_DST
8
Unique count of evt_dstip.raw
_ThreatIntel_MaliciousIP_Map_SRC
ASIA
Gobi
Indonesia
Indian Ocean
Leaflet | Tiles by MapQuest — Map data © OpenStreetMap contributors, CC-BY-SA
_ThreatIntel_MaliciousIP_SRC
Legend
172.16.253.129
168.131.48.151
172.16.0.130
192.168.122.167
10.122.21.185
_ThreatIntel_MaliciousIP_Count_SRC
5
Unique count of evt_srcip.raw
_ThreatIntel_MaliciousIP_DateChart
Legend
Count
Count
200
150
100
50
0
11:15:00
11:20:00
11:25:00
11:30:00
11:35:00
11:40:00
@timestamp per 30 seconds


kibana
Discover
Visualize
Dashboard
Settings
Last 12 hours
_CriticalStack
*
_CriticalStack_IntelMap
Greenland
Barents Sea
Siberia
ASIA
NORTH AMERICA
EUROPE
Gobi
North Atlantic Ocean
North Pacific Ocean
Sahara
Arabian Peninsula
AFRICA
Amazon Basin
Congo Basin
Indian Ocean
Indonesia
SOUTH AMERICA
South Atlantic
AUSTRALIA
1 – 10.2
10.2 – 19.4
19.4 – 28.6
28.6 – 37.8
37.8 – 47
Leaflet | Tiles by MapQuest — Map data © OpenStreetMap contributors, CC-BY-SA
_CriticalStack_IndicatorTypes
Legend
Intel::ADDR
Intel::DOMAIN
_CriticalStack_IntelADDR_Sources
Legend
bro from https://ww...
bro from http://www...
bro from http://www...
bro from http://www...
bro from http://www...
bro from http://www...
_CriticalStack_IntelDomain_Sources
Legend
bro from http://mirror1....

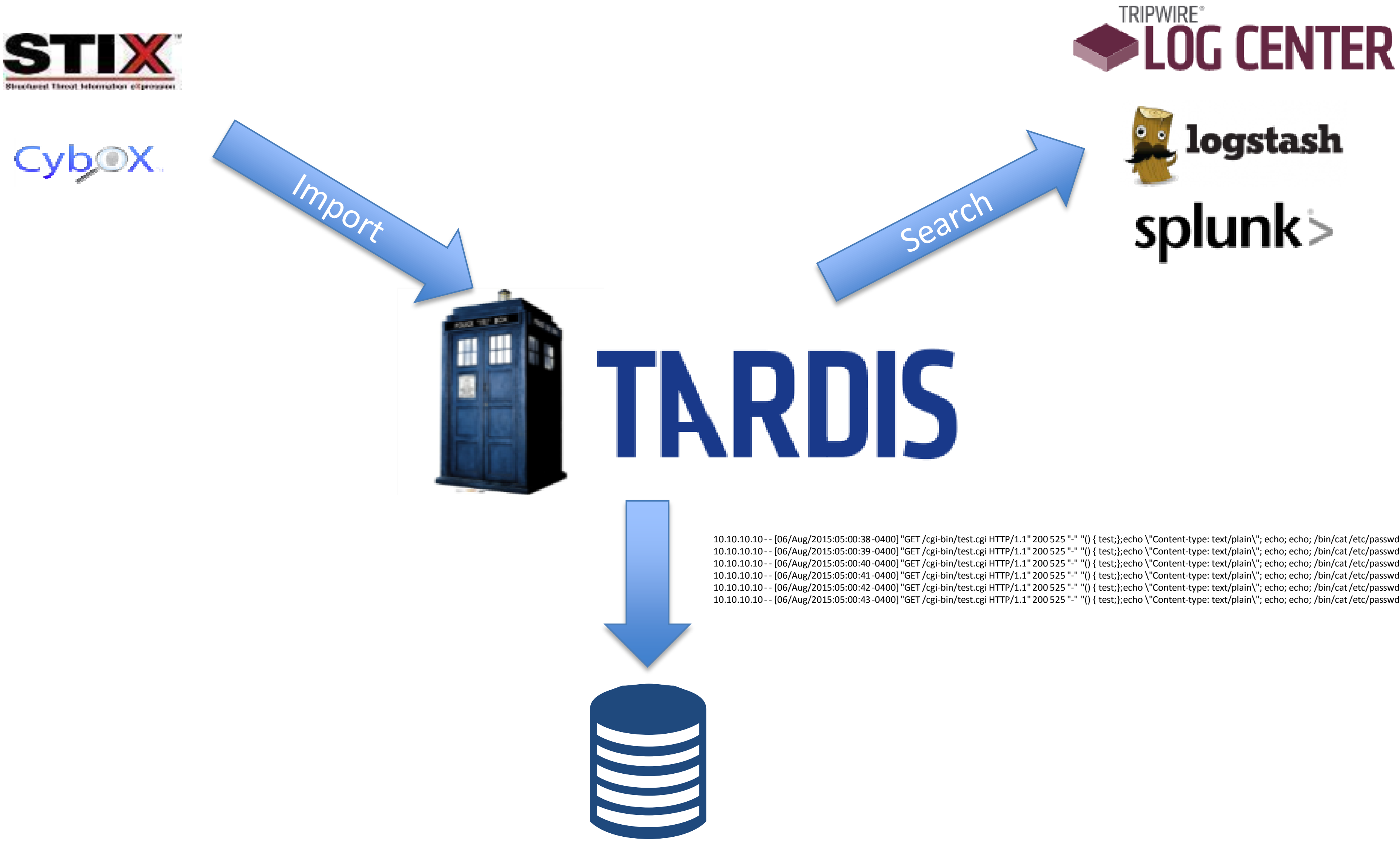
The TARDIS Framework

- Threat Analysis, Reconnaissance, & Data Intelligence System
- Historical exploit/IOC detection
- Time Lord of forensic log data
- Available at

https://github.com/tripwire/tardis

- Demo at Arsenal Thursday @ 12:45

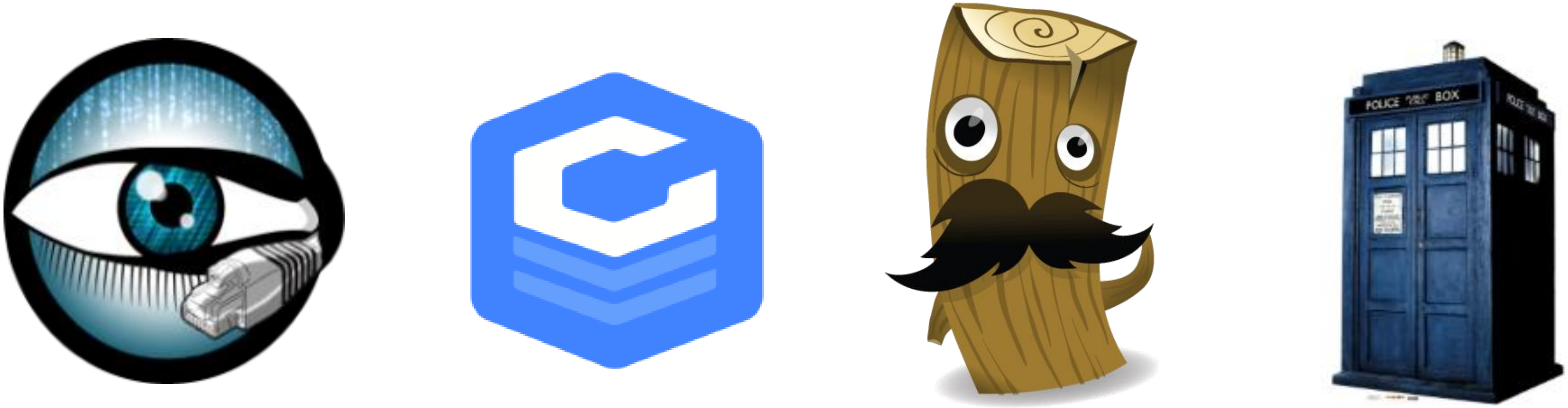
POLICE PUBLIC CALL BOX


STIX
Structured Threat Information eXpression
CybOX
Import
TARDIS
Search
TRIPWIRE LOG CENTER
logstash
splunk>

```
10.10.10.10 - - [06/Aug/2015:05:00:38 -0400] "GET /cgi-bin/test.cgi HTTP/1.1" 200 525 "-" "() { test;};echo \"Content-type: text/plain\"; echo; echo; /bin/cat /etc/passwd“
10.10.10.10 - - [06/Aug/2015:05:00:39 -0400] "GET /cgi-bin/test.cgi HTTP/1.1" 200 525 "-" "() { test;};echo \"Content-type: text/plain\"; echo; echo; /bin/cat /etc/passwd"
10.10.10.10 - - [06/Aug/2015:05:00:40 -0400] "GET /cgi-bin/test.cgi HTTP/1.1" 200 525 "-" "() { test;};echo \"Content-type: text/plain\"; echo; echo; /bin/cat /etc/passwd"
10.10.10.10 - - [06/Aug/2015:05:00:41 -0400] "GET /cgi-bin/test.cgi HTTP/1.1" 200 525 "-" "() { test;};echo \"Content-type: text/plain\"; echo; echo; /bin/cat /etc/passwd"
10.10.10.10 - - [06/Aug/2015:05:00:42 -0400] "GET /cgi-bin/test.cgi HTTP/1.1" 200 525 "-" "() { test;};echo \"Content-type: text/plain\"; echo; echo; /bin/cat /etc/passwd"
10.10.10.10 - - [06/Aug/2015:05:00:43 -0400] "GET /cgi-bin/test.cgi HTTP/1.1" 200 525 "-" "() { test;};echo \"Content-type: text/plain\"; echo; echo; /bin/cat /etc/passwd"
```

Sound Bytes

- Use NSM With Log
- Security Tools Are Better With Intelligence
- Take Integrations to the Next Level With TARDIS


POLICE PUBLIC CALL BOX

Thank You

Travis Smith

tsmith@tripwire.com

https://github.com/Tripwire/tardis

https://github.com/TravisFSmith/MyBroElk