RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: AIR-W04

Dreaming of IoCs
Adding Time Context to Threat Intelligence

Travis Smith

Senior Security Research Engineer
Tripwire, Inc.
@MrTrav

#RSAC

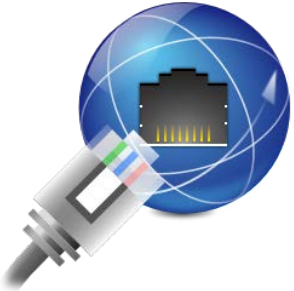
THREAT INTEL

Longitude: -117.9190333

Latitide: 33.8120584

What is an Indicator of Compromise

An artifact observed on the network or operating system



tripwire @MrTrav

Formats

TAXII™

STIX™

CybOX™

OpenIOC

yara

IETF®

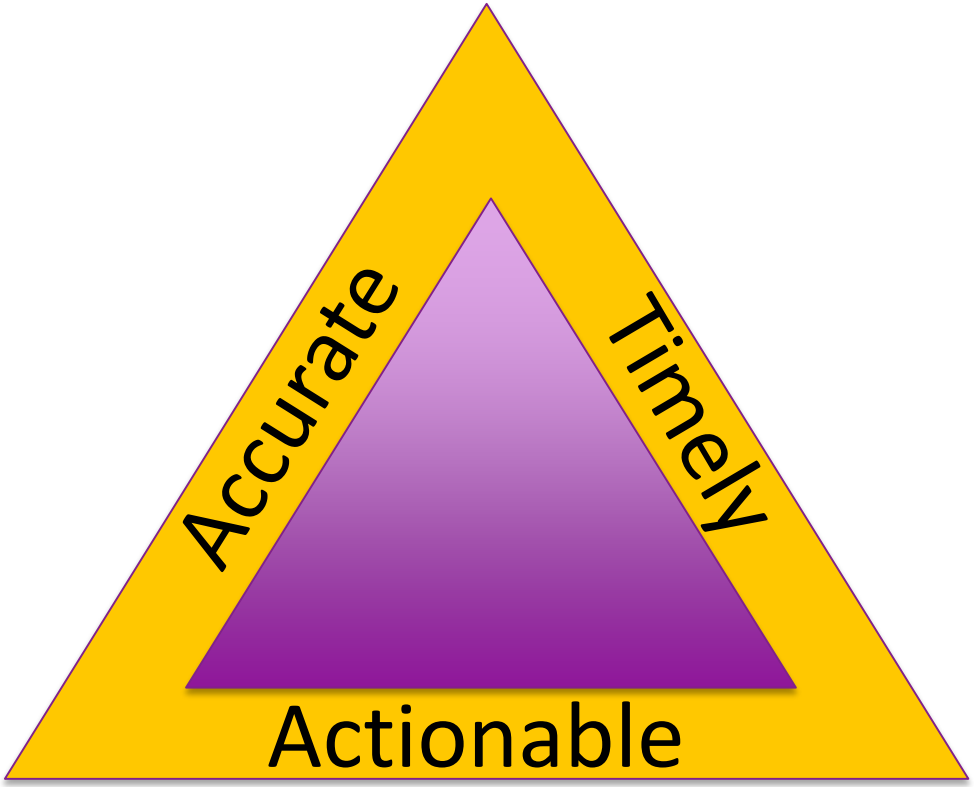
tripwire

@MrTrav

What Is Threat Intelligence

- "Evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard."
- "Intelligence is information that has been analyzed and refined so that it is useful to policymakers in making decisions."

CTI Triad



@MrTrav

THREAT INTEL

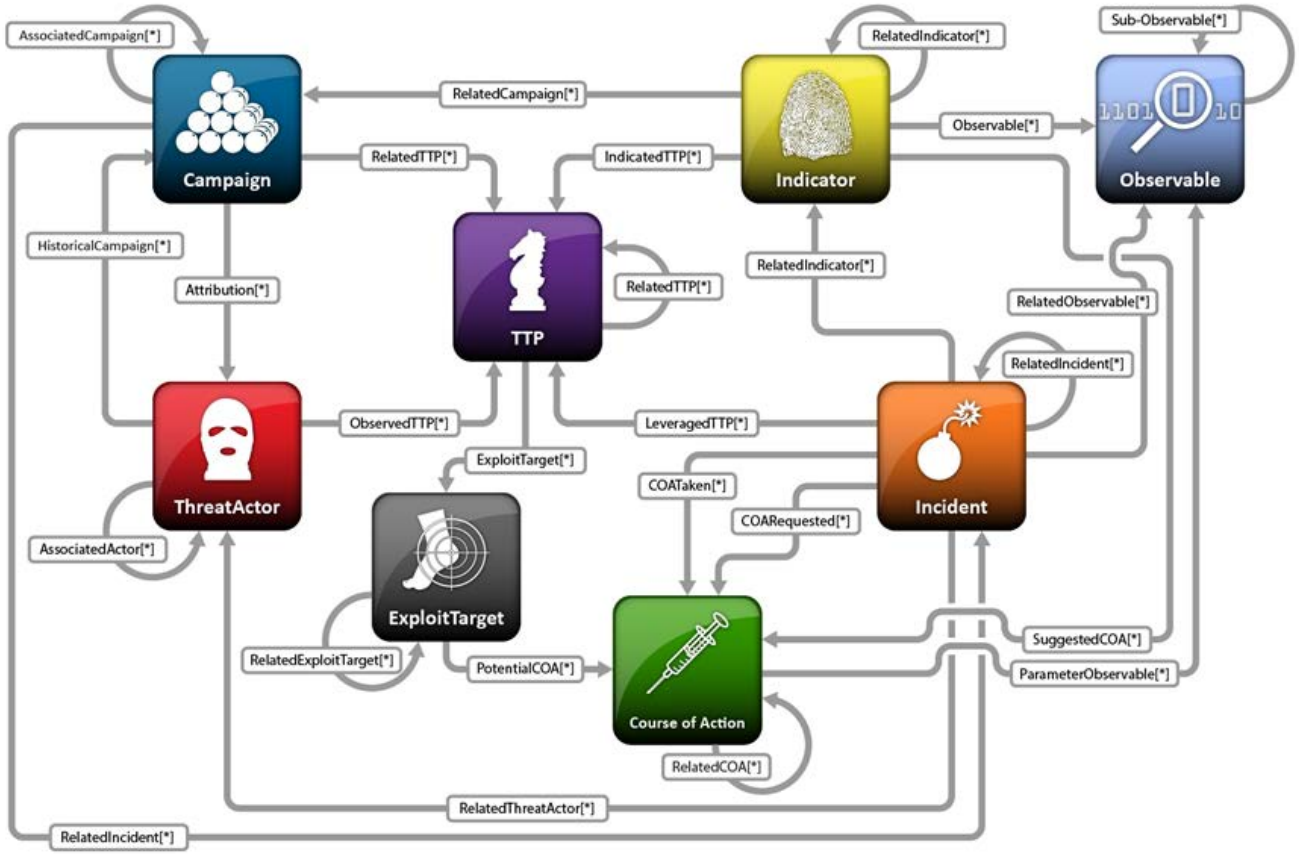
Longitude: -117.9190333
Latitude: 33.8120584
Culprit: Billy Two Tone
Affiliations: Slingers
Victims: Elderly
Tactics: Slingshot
Time: 1949

THREAT INTEL

Longitude: -117.9190333
Latitude: 33.8120584
Culprit: Billy Two Tone
Affiliations: Slingers
Victims: Elderly
Tactics: Slingshot
Time: 1949


SECURITY DATA > BIG DATA

TAXII/STIX/CYBOX



Data Model

- Package
- Report
- Campaign
- Couse of Action
- Exploit Target
- Incident
- Indicator
- Threat Actor
- TTP

http://stixproject.github.io/data-model/

Sharing is Caring

- Threat Intelligence / Information Sharing
  - Aggregators of data sources
  - Open Source
- Sandbox Solutions
  - Walled Gardens
  - Closed Source

Aggregators

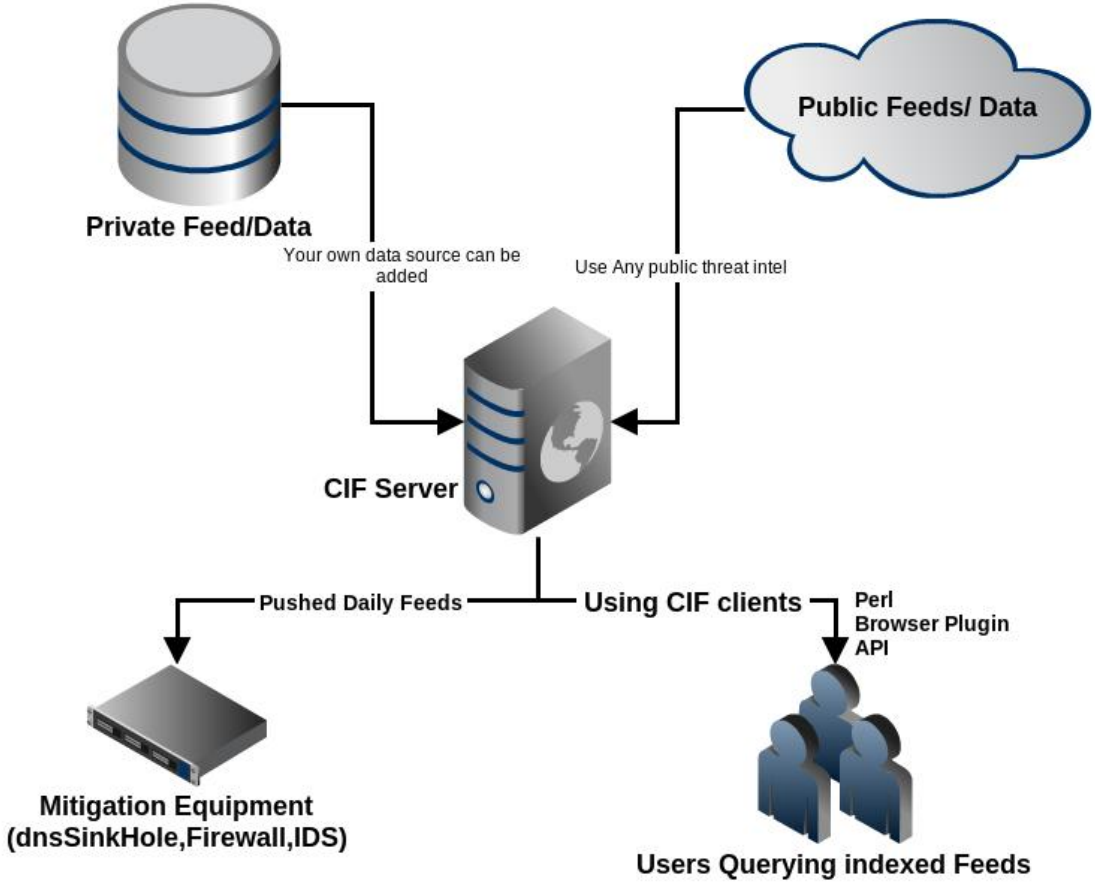
- I know this is bad, do I see it?
  - Search logs for hash/IP
- I have something, is it bad?
- Pros – proactive response
- Cons – open source/free providers, questionable sanitization

Walled Gardens

- I have something, tell me what you think of it
  - Find a file, reference it
  - See an IP, reference it
- Pros – Sanitized and timely data
- Cons
  - Can be expensive
  - Performance - lots of lookups

Collective Intelligence Framework

Collective Intelligence Framework



http://csirtgadgets.org/collective-intelligence-framework

https://github.com/csirtgadgets/massive-octo-spice

Collective Intelligence Framework

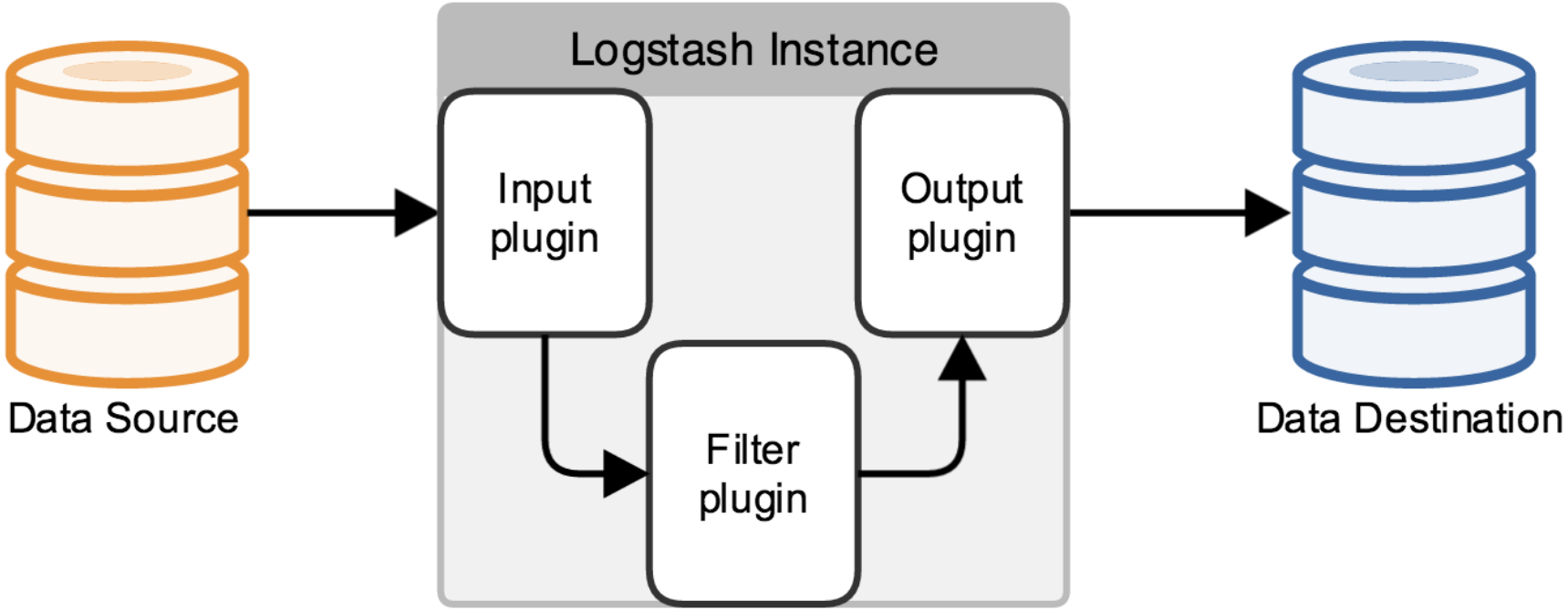
- Requirements
  - Small: 16GB/8 cores/250GB
  - Large: 32GB/16 cores/500GB
  - Extra Large: 64GB/32 cores/500GB
- CIFv1 Installation
  - Lots of dependencies, lots of effort
- CIFv2 Installation
  - EasyButton!

Collective Intelligence Framework

- cif --otype **ipv4** --format csv
  - MD5
  - URL
  - FQDN
- cif --otype ipv4 --format **csv**
  - CSV
  - JSON

Logstash

Intro to Logstash



Intro to Logstash

INPUTS

- FILE
- SYSLOG
- EVENTLOG
- STDIN
- 40+ More

FILTERS

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

OUTPUTS

- ElasticSearch
- SYSLOG
- EMAIL
- STDOUT
- 50+ More

Logstash Filtering

- Utilizing Custom Patterns
- GROK Message Filtering
- Adding Custom Fields
- Date Match
- Using Translations for Threat Intelligence

Logstash Filtering


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

Logstash Filtering


```
filter {
    grok {
        patterns_dir => "/opt/logstash/custom_patterns"
        match => {
            message => "%{123456}"
        }
    }
}
```

Logstash Filtering

root@demobox:/opt/logstash/custom_patterns

```
[root@demobox custom_patterns]# ls -1
bro.rule
logstash_centos.rule
logstash_redhat.rule
logstash_windows.rule
te.rule
[root@demobox custom_patterns]#
```

root@demobox:/opt/logstash/custom_patterns

```
[root@demobox custom_patterns]# more te.rule
123456 (?<node_name>[^,]+),(?<node_type>[^,]+),(?<rule_name>[^,]+),(?<eleme
123457 (?<node_name>[^,]+),(?<node_type>[^,]+),(?<rule_name>[^,]+),(?<eleme
123458 (?<node_name>[^,]+),(?<node_type>[^,]+),(?<rule_name>[^,]+),(?<eleme
[root@demobox custom_patterns]#
```

tripwire @MrTrav

Logstash Filtering


```
filter {
    if [message] =~ /^(([^,]+),([^,]+),([^,]+),([^,]+),...)/ {
        grok {
            patterns_dir => "/opt/logstash/custom_patterns"
            match => {
                message => "%{123456}"
            }
        }
    }
}
```

Remove Capture Groups

(~~?<node_name>~~[^,]+),(~~?<node_type>~~[^,]+),(~~?<rule_name>~~[^,]+),(~~?<element_name>~~[^,]+),…

Logstash Filtering


```
filter {
     if [message] =~ /^(([^,]+),([^,]+),([^,]+),([^,]+),...)/ {
        grok {
            patterns_dir => "/opt/logstash/custom_patterns"
            match => {
                message => "%{291001}“
            }
            add_field => [ "rule_id", “123456" ]
            add_field => [ "Device Type", “FIM" ]
            add_field => [ "Object", “File" ]
            add_field => [ "Action", “Modified" ]
            add_field => [ "Status", “Success" ]
        }
    }
}
```

Logstash Filtering


```
filter {
    ....all normalization code above here ....
    date {
        match => [ "change_time", "M/d/YY h:m a"  ]
    }
}
```

change_time: 3/2/16 10:20 AM

Logstash Filtering


```
filter {
    ....all normalization code above here….
     translate {
        field => “md5"
        destination => “maliciousMD5"
        dictionary_path => /opt/logstash/maliciousMD5.yaml'
    }
}
```

- Logstash will check the YAML for updates every 300 seconds
  - Configurable by adding refresh_interval => numSeconds

Yet Another Python Script


```
cif –otype md5 --format csv
```

```
tlp,group,reporttime,observable,cc,asn,confidence,tags,description,rdata,provider,altid_tlp,altid
amber,everyone,2016-02-16T15:00:41Z,c3b48c837e8363bc2aacf4fe7495a5da,,,85,malware,,,malc0de.com,,http://malc0de.com/rss
amber,everyone,2016-02-16T15:00:41Z,302b4ecfdd8b504c2dfbdbfd4c093d4a,,,85,malware,,,malc0de.com,,http://malc0de.com/rss
amber,everyone,2016-02-16T15:00:41Z,874d5323afd44fa39e8aaf8de555bbef,,,85,malware,,,malc0de.com,,http://malc0de.com/rss
amber,everyone,2016-02-16T15:00:41Z,d0c6ae6f902330e503830742a525098a,,,85,malware,,,malc0de.com,,http://malc0de.com/rss
```

https://github.com/travisfsmith/iocdreaming

maliciousMD5.yaml

```
"c3b48c837e8363bc2aacf4fe7495a5da": "YES "
"302b4ecfdd8b504c2dfbdbfd4c093d4a": "YES "
"874d5323afd44fa39e8aaf8de555bbef": "YES "
"d0c6ae6f902330e503830742a525098a": "YES "
```

Intro to Logstash

INPUTS

FILE | SYSLOG | EVENTLOG | STDIN | 40+ More

FILTERS

GROK | GEOIP | TRANSLATE | DATE | 30+ More

OUTPUTS

ElasticSearch | SYSLOG | EMAIL | STDOUT | 50+ More

Logstash Filtering


```
root@demobox:/opt/logstash
[root@demobox logstash]# logstash -f TE_Change.conf
Logstash startup completed
companyDC,Windows Server,Secret Files,C:\Confidential_Files\virus.exe,3/2/16 10:
20 AM,Added,High,10000,,,"Name=""MD5"",Expected=""""",Observed=""cc1d4672c540156c
dd8a56c854913109""",
{
          "message" => "companyDC,Windows Server,Secret Files,C:\\Confidential_F
iles\\virus.exe,3/2/16 10:20 AM,Added,High,10000,,,\"Name=\"\"MD5\"\",Expected=\
"\"\"\",Observed=\"\"cc1d4672c540156cdd8a56c854913109\"\"\",",
         "@version" => "1",
       "@timestamp" => "2016-03-02T18:20:00.000Z",
             "host" => "demobox",
        "node_name" => "companyDC",
        "node_type" => "Windows Server",
        "rule_name" => "Secret Files",
     "element_name" => "C:\\Confidential_Files\\virus.exe",
      "change_time" => "3/2/16 10:20 AM",
           "Action" => "Added",
    "severity_text" => "High",
     "severity_num" => "10000",
              "md5" => "cc1d4672c540156cdd8a56c854913109",
          "rule_id" => "123457",
      "Device Type" => "FIMDevice",
           "Object" => "File",
           "Status" => "Success",
       "approvalID" => "none",
     "maliciousMD5" => "YES",
           "teTags" => [
        [0] "Monitoring Enabled",
        [1] "Microsoft Windows Server 2008 R2",
        [2] "Domain Controllers"
    ]
}
```

Custom Fields:

"Device Type" => "FIMDevice"

"Object" => "File"

"Action" => "Added"

"Status" => "Success"

Threat Intel Translations:

"maliciousMD5" => "YES"

Date Matching:

"change_time" => "3/2/16 10:20 AM"

"timestamp" => “2016-03-02T18:20:00.000Z"

Logstash Filtering

1. Collect intelligence feeds
2. Update security tools with intel
3. Monitor observable which doesn't match any feed
4. Feeds updated with observable previously already inspected….

TARDIS

TARDIS

- Threat Analysis, Reconnaissance, & Data Intelligence System
- Historical Exploit/IOC Detection
- Time Lord of Forensic Log Data
- Available at: https://github.com/tripwire/tardis

Yet Another Python Script


```
cif -otype md5 --format csv
```

```
tlp,group,reporttime,observable,cc,asn,confidence,tags,description,rdata,provider,altid_tlp,altid
amber,everyone,2016-02-16T15:00:41Z,c3b48c837e8363bc2aacf4fe7495a5da,,,85,malware,,,malc0de.com,,http://malc0de.com/rss
amber,everyone,2016-02-16T15:00:41Z,302b4ecfdd8b504c2dfbdbfd4c093d4a,,,85,malware,,,malc0de.com,,http://malc0de.com/rss
amber,everyone,2016-02-16T15:00:41Z,874d5323afd44fa39e8aaf8de555bbef,,,85,malware,,,malc0de.com,,http://malc0de.com/rss
amber,everyone,2016-02-16T15:00:41Z,d0c6ae6f902330e503830742a525098a,,,85,malware,,,malc0de.com,,http://malc0de.com/rss
```

https://github.com/travisfsmith/iocdreaming

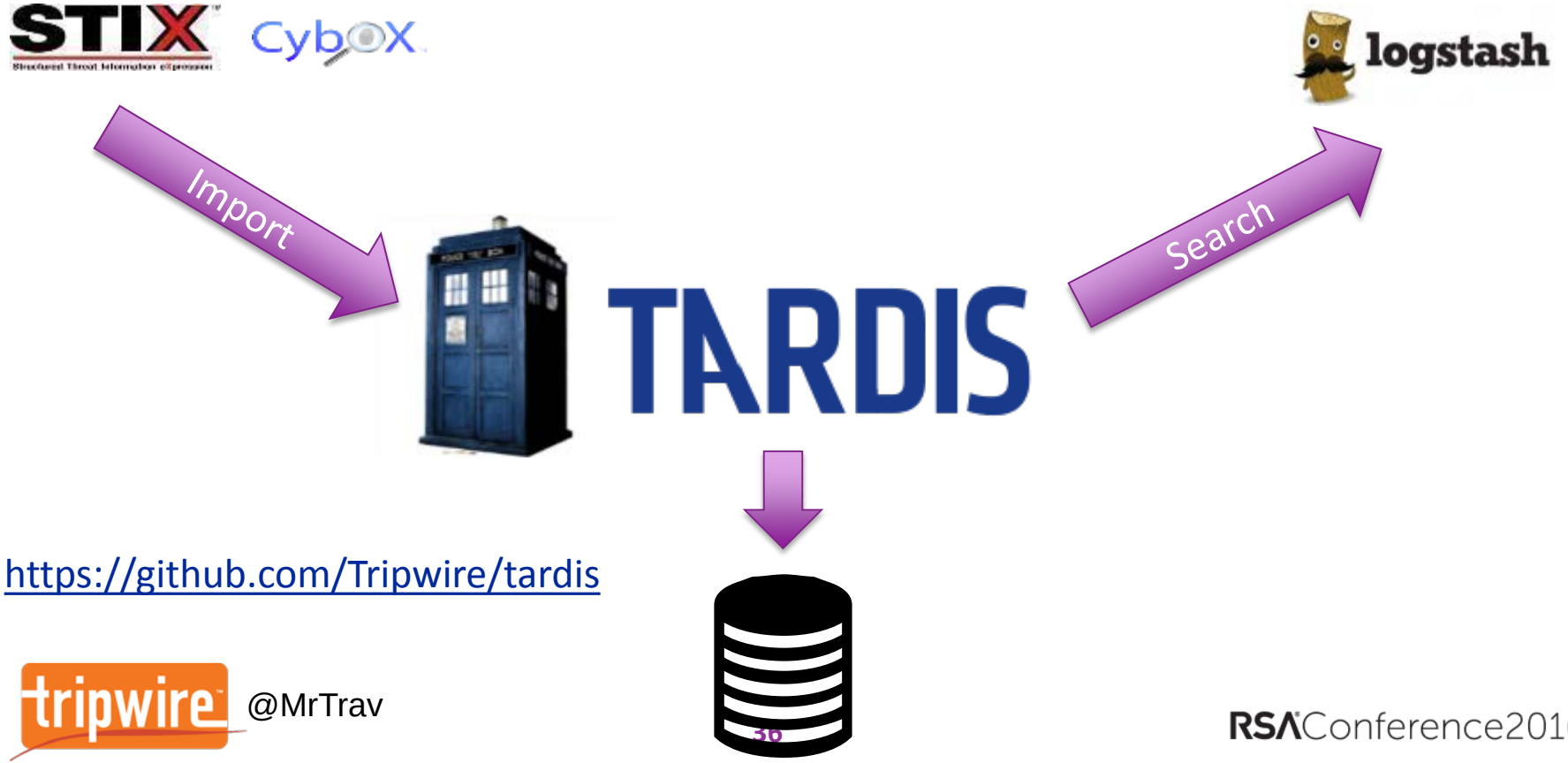
STIX
Structured Threat Information eXpression

Observable

c3b48c837e8363bc2aacf4fe7495a5da.stix
302b4ecfdd8b504c2dfbdbfd4c093d4a.stix
874d5323afd44fa39e8aaf8de555bbef.stix
d0c6ae6f902330e503830742a525098a.stix

tripwire @MrTrav

TARDIS



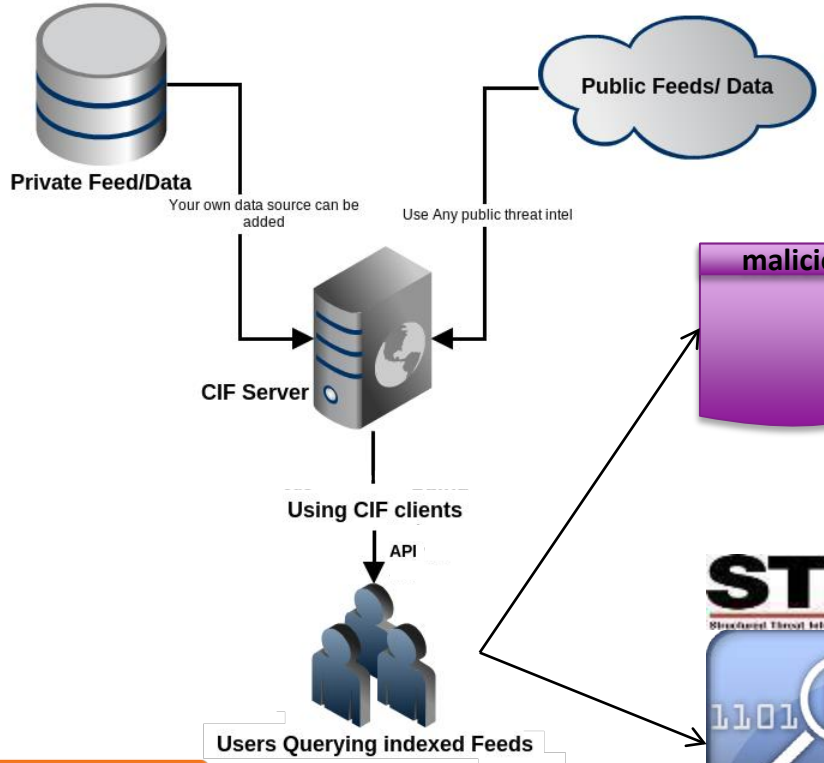
https://github.com/Tripwire/tardis

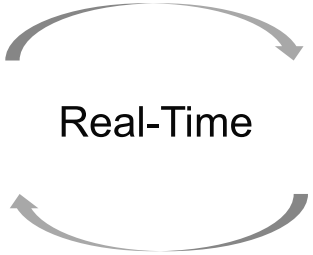
tripwire @MrTrav

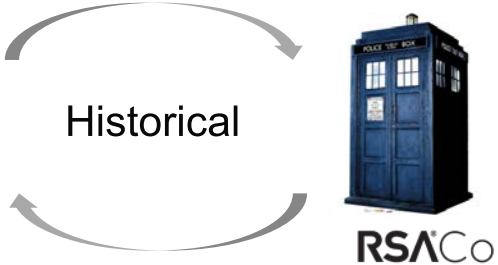
TARDIS

1. Collect intelligence feeds
2. Update security tools with intel
3. Monitor observable which doesn't match any feed
4. Feeds updated with observable previously already inspected….
5. Search repository for observable

Architecture







tripwire @MrTrav

Kibana Reporting

Kibana

- The ELK Stack
- Search, Visualize, Dashboard
- Zoom In & Out

kibana

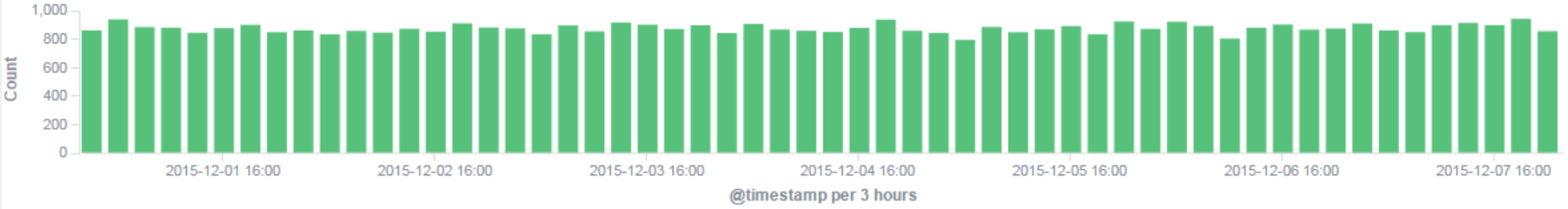
Discover | Visualize | Dashboard | Settings

December 1st 2015, 00:00:00.000 to December 7th 2015, 23:59:59.999

Search...

49,059 hits

December 1st 2015, 00:00:00.000 - December 7th 2015, 23:59:59.999 — by 3 hours



Time	_source
December 7th 2015, 23:58:00.000	message: "pdx-9","Windows Server","Critical Change Audit","C:\Windows\System32\wbem\PrintFilterPipelineSvc.mof","12/07/2015 11:58 PM","Modified","High",10000,"","","Name=""MD5"",Expected=""""",Observed=""912795a0675142948a6612ba4186cd30"";Name=""Write"",Expected=""""",Observed=""12/07/2015 11:58 PM""", @version: 1 @timestamp: December 7th 2015, 23:58:00.000 host: rsa-demo path: /opt/TE/reports/te_changeData.csv node_name: pdx-9 node_type: Windows Server rule_name: Critical Change Audit element_name: C:\Windows\System32\wbem\PrintFilterPipelineSvc.mof change_time: 12/07/2015 11:58 PM Action: Modified severity_text: High
December 7th 2015, 23:58:00.000	message: "pdx-7","Windows Server","Critical Change Audit","C:\Windows\System32\wbem\SensorsClassExtension.mof","12/07/2015 11:58 PM","Modified","High",10000,"","","Name=""MD5"",Expected=""""",Observed=""023c8a2c47464436a8d4b2da2062b4d0"";Name=""Write"",Expected=""""",Observed=""12/07/2015 11:58 PM""", @version: 1 @timestamp: December 7th 2015, 23:58:00.000 host: rsa-demo path: /opt/TE/reports/te_changeData.csv node_name: pdx-7 node_type: Windows Server rule_name: Critical Change Audit element_name: C:\Windows\System32\wbem\SensorsClassExtension.mof change_time: 12/07/2015 11:58 PM Action: Modified severity_text: High severity_num: 1
December 7th 2015, 23:58:00.000	message: "pdx-1","Windows Server","Critical Change Audit","C:\Windows\System32\drivers\usbccgp.sys","12/07/2015 11:58 PM","Modifi

kibana

Discover | Visualize | Dashboard | Settings

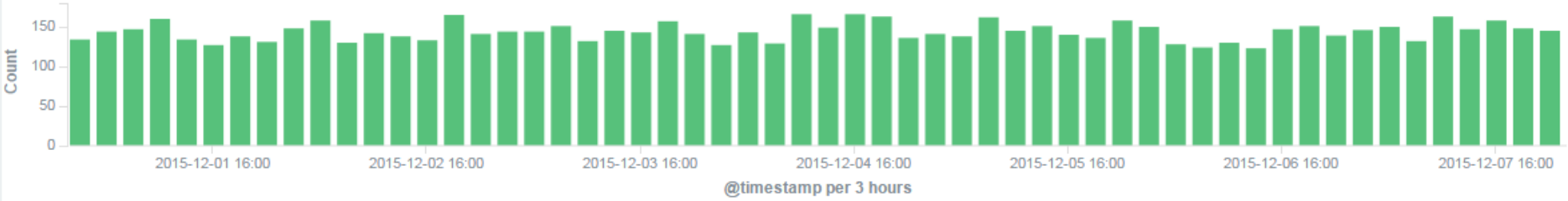
December 1st 2015, 00:00:00.000 to December 7th 2015, 23:59:59.999

node_name="pdx-9"

node_name="pdx-9"

8,058 hits

December 1st 2015, 00:00:00.000 - December 7th 2015, 23:59:59.999 — by 3 hours



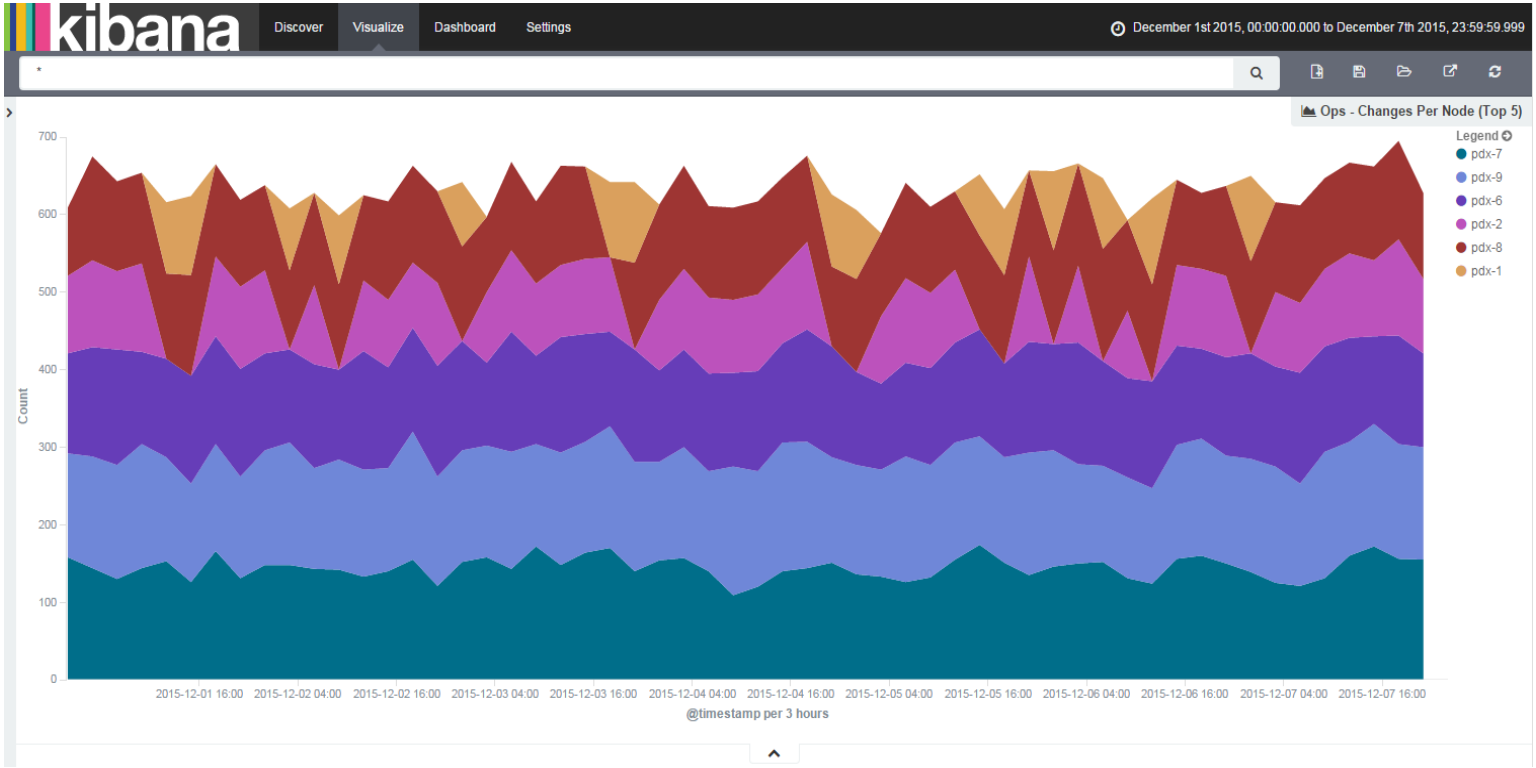
Time	_source
December 7th 2015, 23:58:00.000	message: "pdx-9","Windows Server","Critical Change Audit","C:\Windows\System32\wbem\PrintFilterPipelineSvc.mof","12/07/2015 11:58 PM","Modified","High",10000,"","","Name=""MD5"",Expected=""""",Observed=""912795a0675142948a6612ba4186cd30"";Name=""Write"",Expected=""""",Observed=""12/07/2015 11:58 PM""", node_name: pdx-9 @version: 1 @timestamp: December 7th 2015, 23:58:00.000 host: rsa-demo path: /opt/TE/reports/te_changeData.csv node_type: Windows Server rule_name: Critical Change Audit element_name: C:\Windows\System32\wbem\PrintFilterPipelineSvc.mof change_time: 12/07/2015 11:58 PM Action: Modified
December 7th 2015, 23:55:00.000	message: "pdx-9","Windows Server","Critical Change Audit","C:\Windows\SysWOW64\KBDINUK2.DLL","12/07/2015 11:55 PM","Modified","High",10000,"","","Name=""MD5"",Expected=""""",Observed=""675b0326ff4d40fab97defe42111ba68"";Name=""Write"",Expected=""""",Observed=""12/07/2015 11:55 PM""", node_name: pdx-9 @version: 1 @timestamp: December 7th 2015, 23:55:00.000 host: rsa-demo path: /opt/TE/reports/te_changeData.csv node_type: Windows Server rule_name: Critical Change Audit element_name: C:\Windows\SysWOW64\KBDINUK2.DLL change_time: 12/07/2015 11:55 PM Action: Modified severity_text: High severity_num: 10000 md5: 675b0326ff4d
December 7th 2015, 23:55:00.000	message: "pdx-9","Windows Server","Critical Change Audit","C:\Windows\SysWOW64\vmGuestLibJava.dll","12/07/2015 11:55 PM","Modif

Create a new visualization

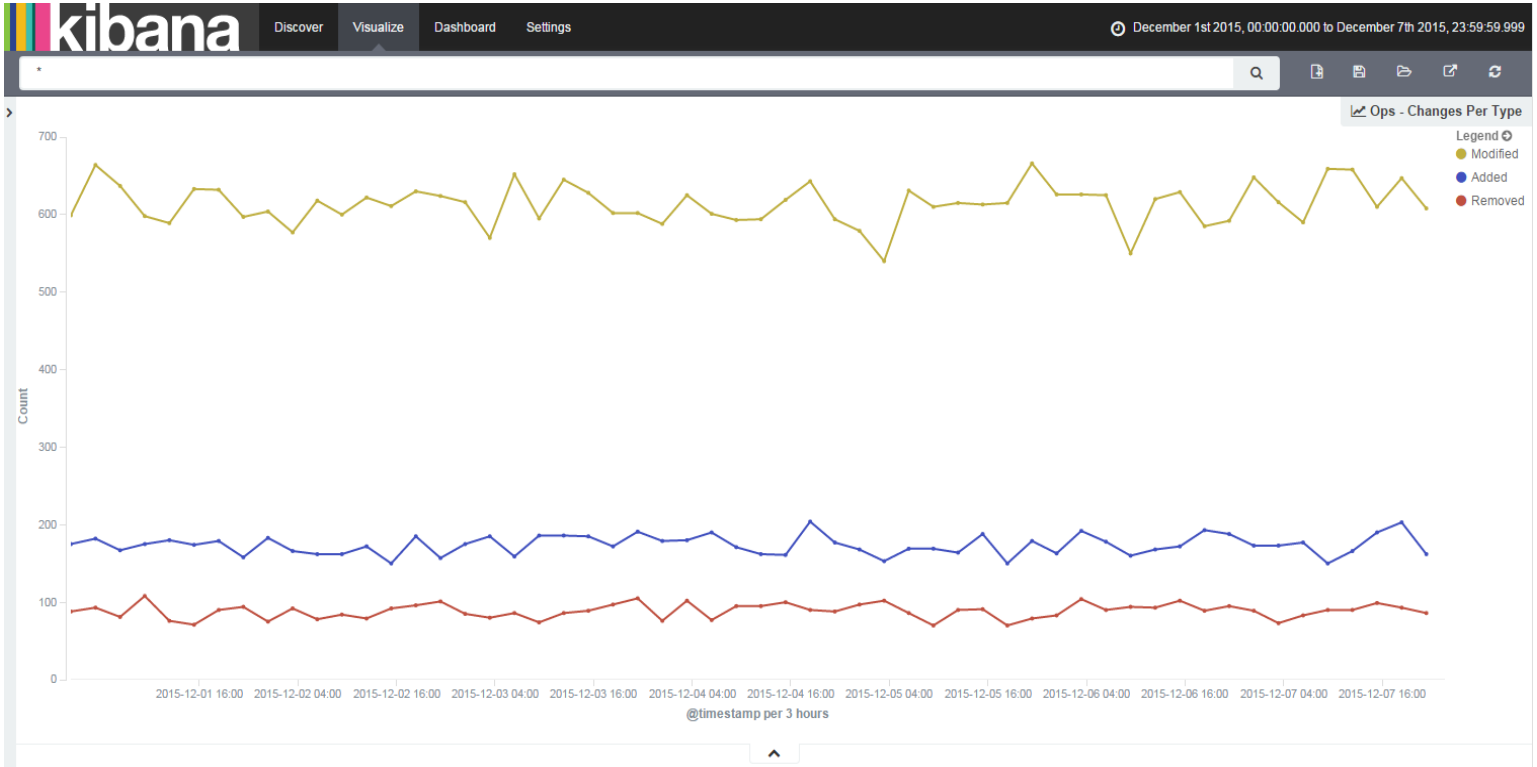
Step 1

Area chart	Great for stacked timelines in which the total of all series is more important than comparing any two or more series. Less useful for assessing the relative change of unrelated data points as changes in a series lower down the stack will have a difficult to gauge effect on the series above it.
Data table	The data table provides a detailed breakdown, in tabular format, of the results of a composed aggregation. Tip, a data table is available from many other charts by clicking grey bar at the bottom of the chart.
Line chart	Often the best chart for high density time series. Great for comparing one series to another. Be careful with sparse sets as the connection between points can be misleading.
Markdown widget	Useful for displaying explanations or instructions for dashboards.
Metric	One big number for all of your one big number needs. Perfect for showing a count of hits, or the exact average a numeric field.
Pie chart	Pie charts are ideal for displaying the parts of some whole. For example, sales percentages by department.Pro Tip: Pie charts are best used sparingly, and with no more than 7 slices per pie.
Tile map	Your source for geographic maps. Requires an elasticsearch geo_point field. More specifically, a field that is mapped as type:geo_point with latitude and longitude coordinates.
Vertical bar chart	The goto chart for oh-so-many needs. Great for time and non-time data. Stacked or grouped, exact numbers or percentages. If you are not sure which chart your need, you could do worse than to start here.

Area Chart

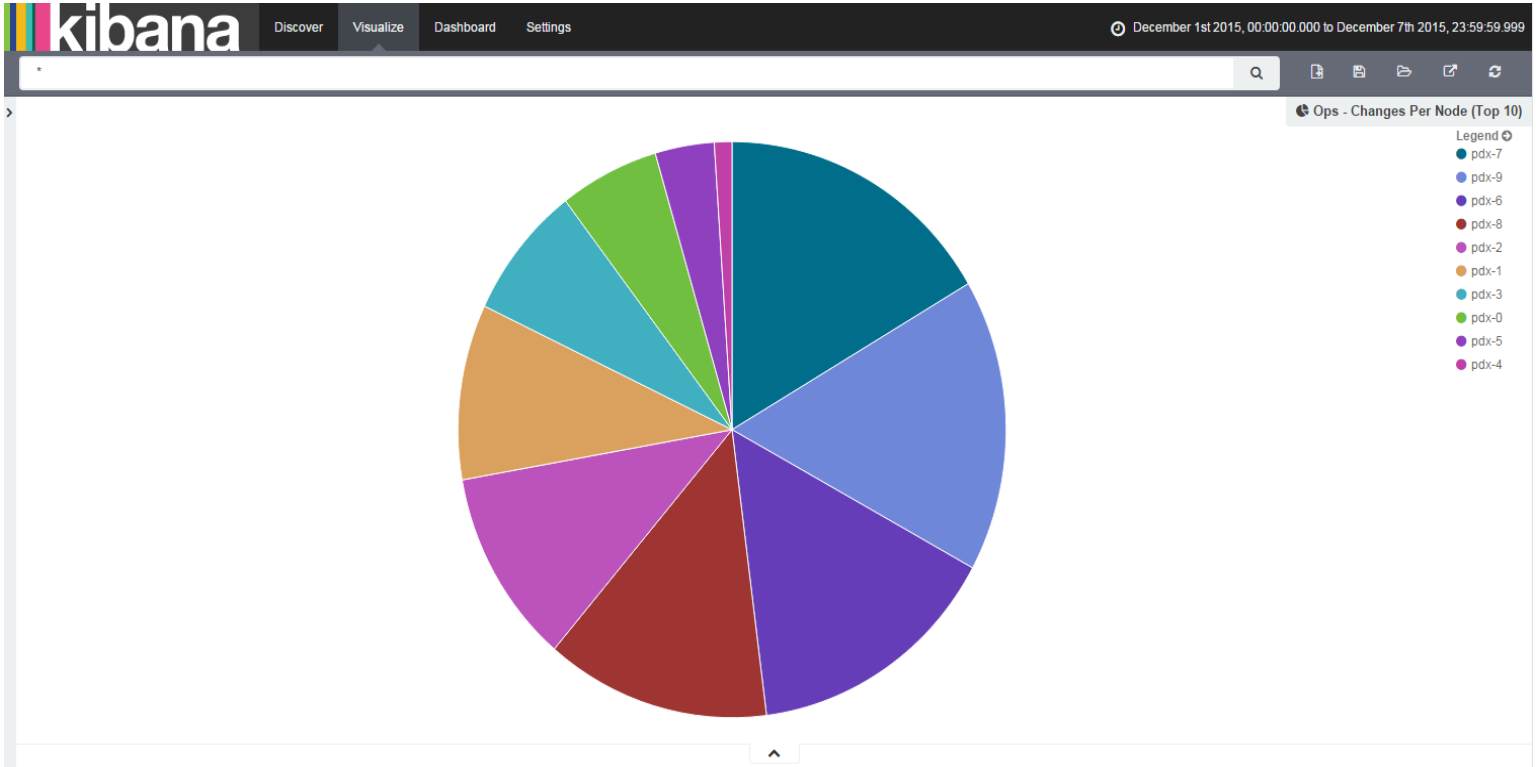

kibana
Discover
Visualize
Dashboard
Settings
December 1st 2015, 00:00:00.000 to December 7th 2015, 23:59:59.999
*
Ops - Changes Per Node (Top 5)
Legend
pdx-7
pdx-9
pdx-6
pdx-2
pdx-8
pdx-1
Count
700
600
500
400
300
200
100
0
2015-12-01 16:00
2015-12-02 04:00
2015-12-02 16:00
2015-12-03 04:00
2015-12-03 16:00
2015-12-04 04:00
2015-12-04 16:00
2015-12-05 04:00
2015-12-05 16:00
2015-12-06 04:00
2015-12-06 16:00
2015-12-07 04:00
2015-12-07 16:00
@timestamp per 3 hours

Line Chart

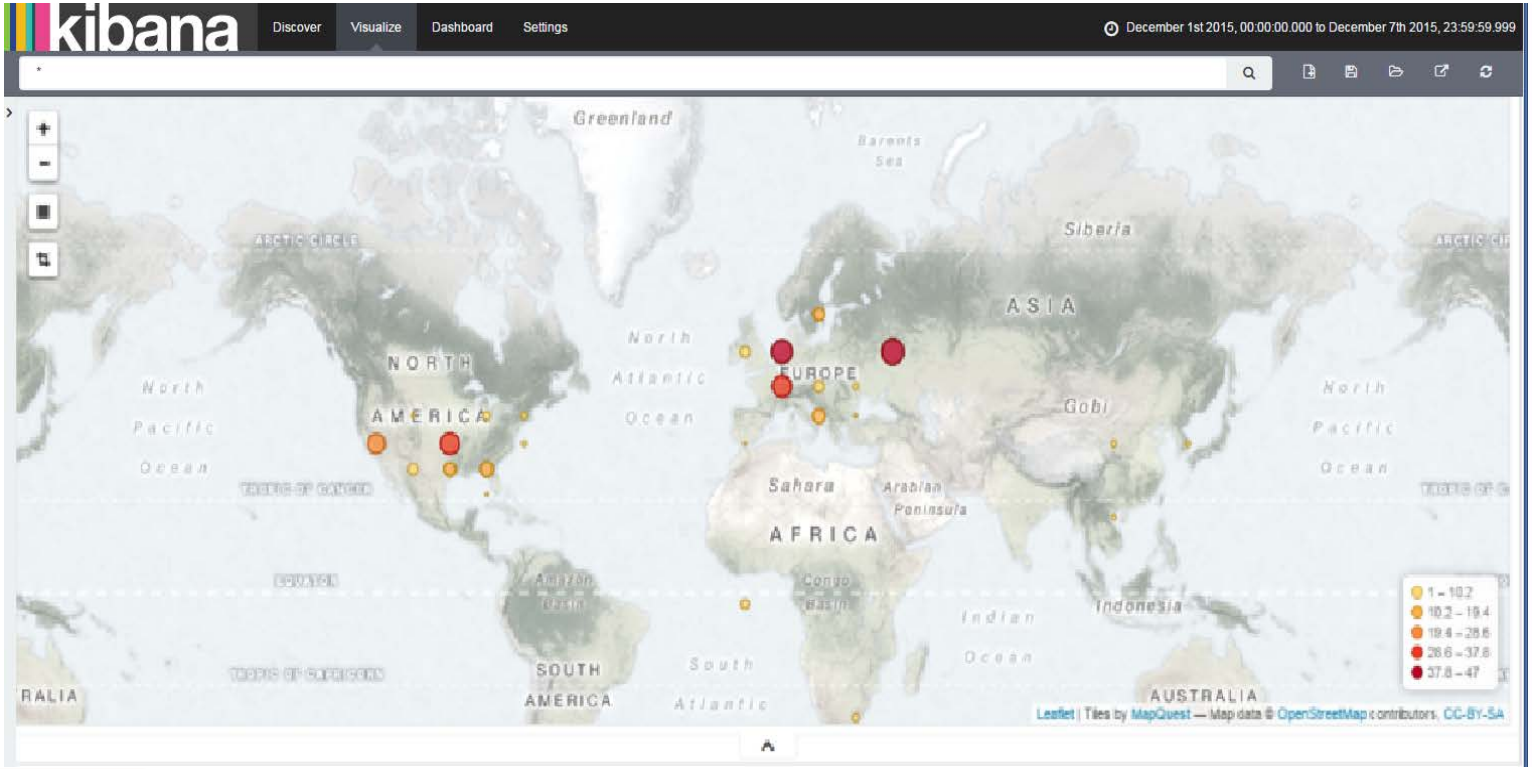


tripwire @MrTrav

Pie Chart


kibana
Discover
Visualize
Dashboard
Settings
December 1st 2015, 00:00:00.000 to December 7th 2015, 23:59:59.999
Ops - Changes Per Node (Top 10)
Legend
pdx-7
pdx-9
pdx-6
pdx-8
pdx-2
pdx-1
pdx-3
pdx-0
pdx-5
pdx-4

Geo Location



tripwire @MrTrav

kibana

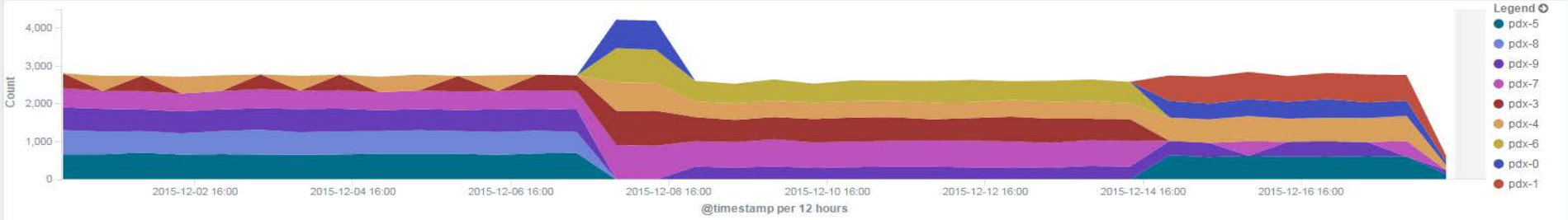
Discover | Visualize | Dashboard | Settings

Month to date

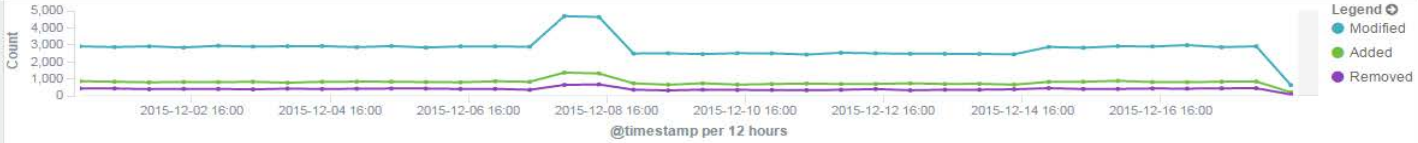
Tripwire Operational Dashboard

*

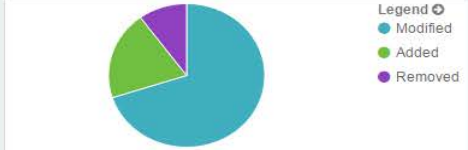
Ops - Changes Per Node (Top 5)



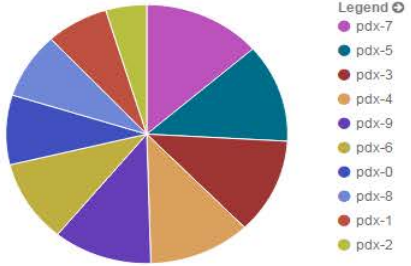
Ops - Changes Per Type



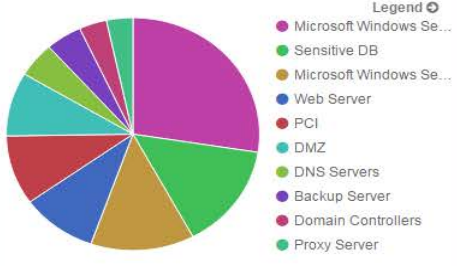
Ops - Top Actions



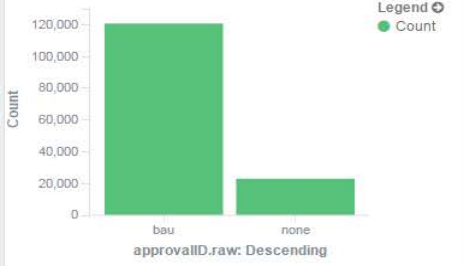
Ops - Changes Per Node (Top 10)



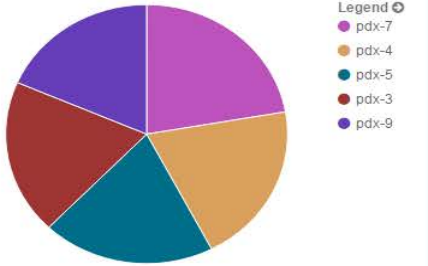
Ops - Tripwire Tags



Ops - Change Approval ID



Ops - Nodes with No Approval ID

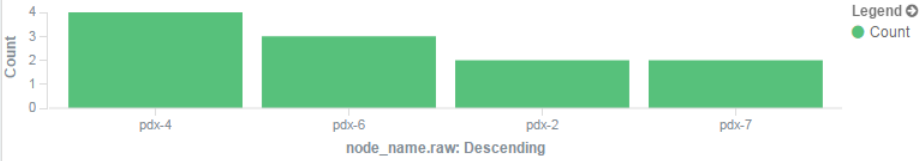


kibana | Discover | Visualize | Dashboard | Settings | Month to date

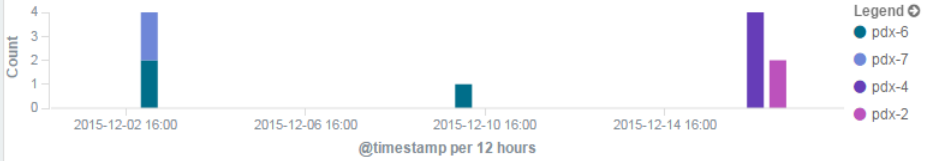
Malware Dashboard

*

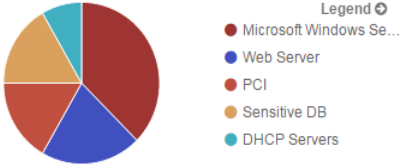
Malware - Infected Nodes



Malware - Infected Histogram



Malware - Tripwire Tags



Malware - Approval ID

Malware - Infected File Count

11

Count

Malware - Infected Machine Count

4

Unique count of node_name.raw

Malware - Infected File List

element_name.raw: Descending	node_name.raw: Descending	Count
C:\Windows\System32\apache.exe	pdx-7	1
C:\Windows\System32\database.exe	pdx-4	1
C:\Windows\System32\dhcp.exe	pdx-2	1
C:\Windows\System32\dns.exe	pdx-2	1
C:\Windows\System32\drivers\cipher.sys	pdx-6	1
C:\Windows\System32\drivers\mysql.dll	pdx-4	1
C:\Windows\System32\drivers\oracle.dll	pdx-4	1

Live Demo

Notable Resources

- https://github.com/tripwire/tardis
- https://github.com/travisfsmith/iocdreaming
- http://www.elastic.co
- http://csirtgadgets.org/collective-intelligence-framework/

Next Steps

- 0-3 Months
  - Identify Security Components
    - Which currently don’t integrate with Threat Intel?
    - Which capture valuable observables?
- 3-6 Months
  - Integrate security tools with actionable threat intelligence
- 6+ Months
  - Fine tune workflows

RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: AIR-W04

Dreaming of IoCs
Adding Time Context to Threat Intelligence

Travis Smith

Senior Security Research Engineer
Tripwire, Inc.
@MrTrav

#RSAC