

Splunk, OSINT and Visualization Catching Bad Guys with Pictures

Jake Babbin

Director of Threat Intelligence, The Crypsis Group

.conf2016

splunk>

Disclaimer

During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC. The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not, be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

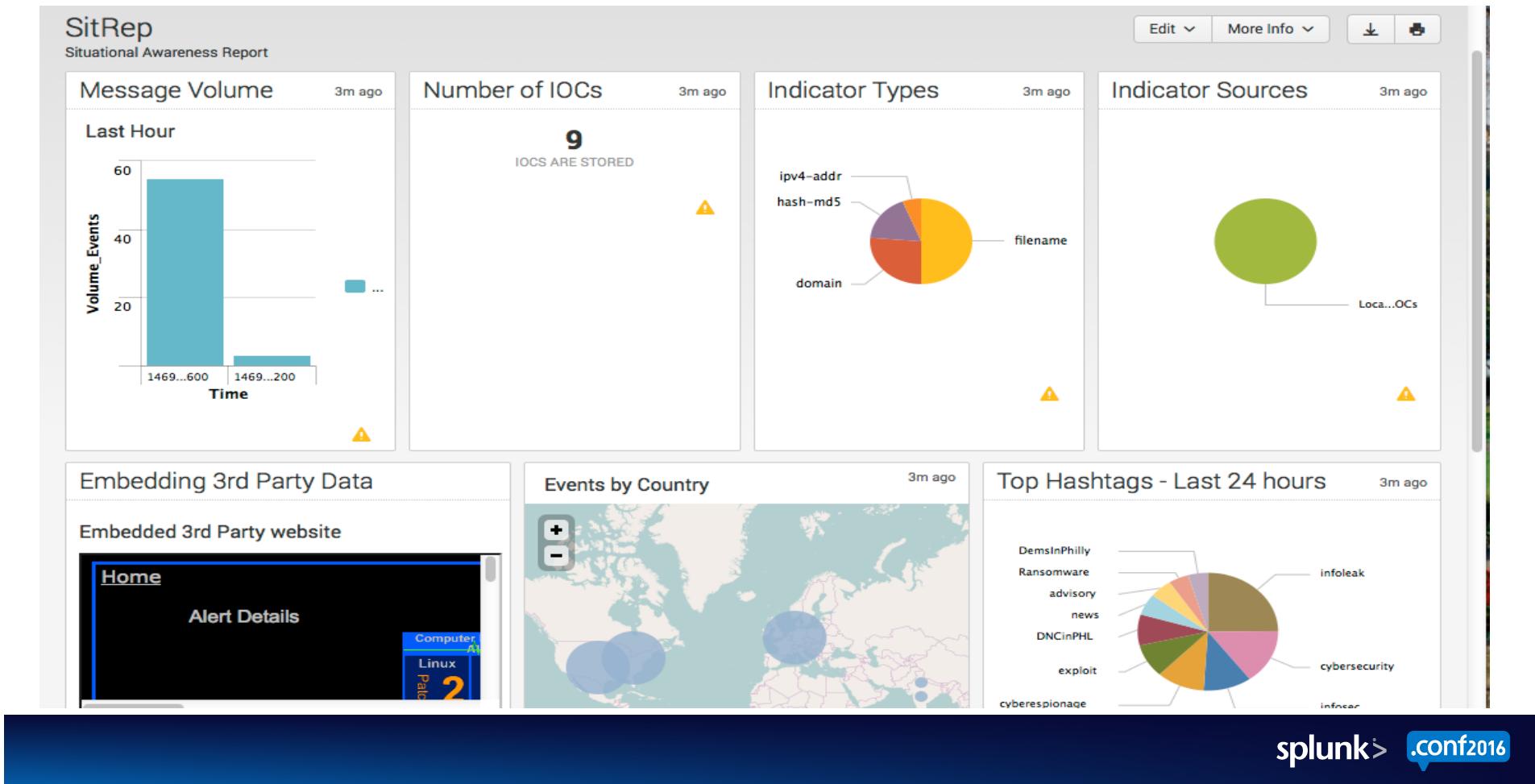
Jumping Right In – An Example

*Note All IP's, DNS names or other indicators are taken from open sources such as IOCbucket.com, or the open web project unless otherwise stated.

.conf2016

splunk>

Situational Awareness Dashboard



Agenda

- Introduction
- A Picture speaks a thousand words
- What is OSINT?
 - How can Splunk use this
- Visualization
- Hunting Bad Guys
- Conclusions

Speaker Background

- Currently
 - Director of Threat Intelligence, The Crypsis Group
- Prior
 - Practice Director – Incident Response and Forensics
McAfee/Intel Security (Americas)
 - Incident Response Auditor for DoD CIO CND-SP/CCRI team
 - Lead Analyst The White House Security Operation Center
(EOP)
 - Founded The White House Cyber Threat Cell
 - Over 15 year career spanning a variety of customers in US
Military, Intelligence Community, and Federal Law
Enforcement



Why Does Imagery and Visualization matter?

.conf2016

splunk>

Machine Data

Not really helpful to most humans

Splunk
Raw Data

Machine
readable,
Searchable,
difficult to
highlight
and identify
patterns

This example shows how to set up Searchbar and SearchControls views using Django tags, and sync them with a SearchManager using tokens.

Note: The Timeline view can't be synced using tokens. Use events instead.

Index: _internal | head: 100

All time

100 events (12/26/13 4:15:23.000 PM to 1/30/14 3:00:06.000 PM)

Job: Job complete

...
127.0.0.1 - admin [30/Jan/2014:15:00:04.057-0800] "GET /servicesNS/-/_search?search=sid%30t_admin_admin_search_search1_r,1391122738.445&count=1&output_mode=json HTTP/1.1" 200 5466 - - 9ms
127.0.0.1 - admin [30/Jan/2014:15:00:04.052-0800] "GET /en-US/splunkd/_new/servicesNS/-/_search?search=sid%30t_admin_admin_search_search1_r,1391122738.445&count=1&output_mode=json&_=>139112280409 HTTP/1.1" 200 1528 "http://localhost:8089/servicesNS/-/_search?search=sid%30t_admin_admin_search_search1_r,1391122738.445&count=1&output_mode=json&_=>139112280409"
127.0.0.1 - admin [30/Jan/2014:15:00:03.027-0800] "GET /servicesNS/-/_search?search=sid%30t_admin_admin_search_search1_r,1391122738.445&count=1&output_mode=json HTTP/1.1" 200 5466 - - 13ms
127.0.0.1 - admin [30/Jan/2014:15:00:03.021-0800] "GET /en-US/splunkd/_new/servicesNS/-/_search?search=sid%30t_admin_admin_search_search1_r,1391122738.445&count=1&output_mode=json&_=>1391122803019 HTTP/1.1" 200 1530 "http://localhost:8089/en-US/splunkd/_new/servicesNS/-/_search?search=sid%30t_admin_admin_search_search1_r,1391122738.445&count=1&output_mode=json&_=>1391122803019"
127.0.0.1 - admin [30/Jan/2014:15:00:03.003-0800] "GET /servicesNS/-/_search?search=sid%30t_admin_admin_search_search1_r,1391122738.445&count=1&output_mode=json HTTP/1.1" 200 5466 - - 9ms
127.0.0.1 - admin [30/Jan/2014:15:00:01.998-0800] "GET /en-US/splunkd/_new/servicesNS/-/_search?search=sid%30t_admin_admin_search_search1_r,1391122738.445&count=1&output_mode=json&_=>1391122801996 HTTP/1.1" 200 1530 "http://localhost:8089/en-US/splunkd/_new/servicesNS/-/_search?search=sid%30t_admin_admin_search_search1_r,1391122738.445&count=1&output_mode=json&_=>1391122801996"
127.0.0.1 - splunk-system-user [30/Jan/2014:15:00:01.338-0800] "GET /servicesNS/-/_data/models?sort_dir=asc&sort_key=name&count=30 HTTP/1.0" 200 83732 - - 4ms
127.0.0.1 - admin [30/Jan/2014:15:00:00.979-0800] "GET /servicesNS/-/_search?search=sid%30t_admin_admin_search_search1_r,1391122738.445&count=1&output_mode=json HTTP/1.1" 200 5466 - - 10ms
127.0.0.1 - admin [30/Jan/2014:15:00:00.979-0800] "GET /en-US/splunkd/_new/servicesNS/-/_search?search=sid%30t_admin_admin_search_search1_r,1391122738.445&count=1&output_mode=json&_=>1391122800966 HTTP/1.1" 200 1526 "http://localhost:8089/en-US/splunkd/_new/servicesNS/-/_search?search=sid%30t_admin_admin_search_search1_r,1391122738.445&count=1&output_mode=json&_=>1391122800966"
127.0.0.1 - admin [30/Jan/2014:14:59:59.947-0800] "GET /servicesNS/-/_search?search=sid%30t_admin_admin_search_search1_r,1391122738.445&count=1&output_mode=json HTTP/1.1" 200 5466 - - 11ms

1 prev 2 3 4 5 6 7 8 9 10 next >

Visualization/Imagery

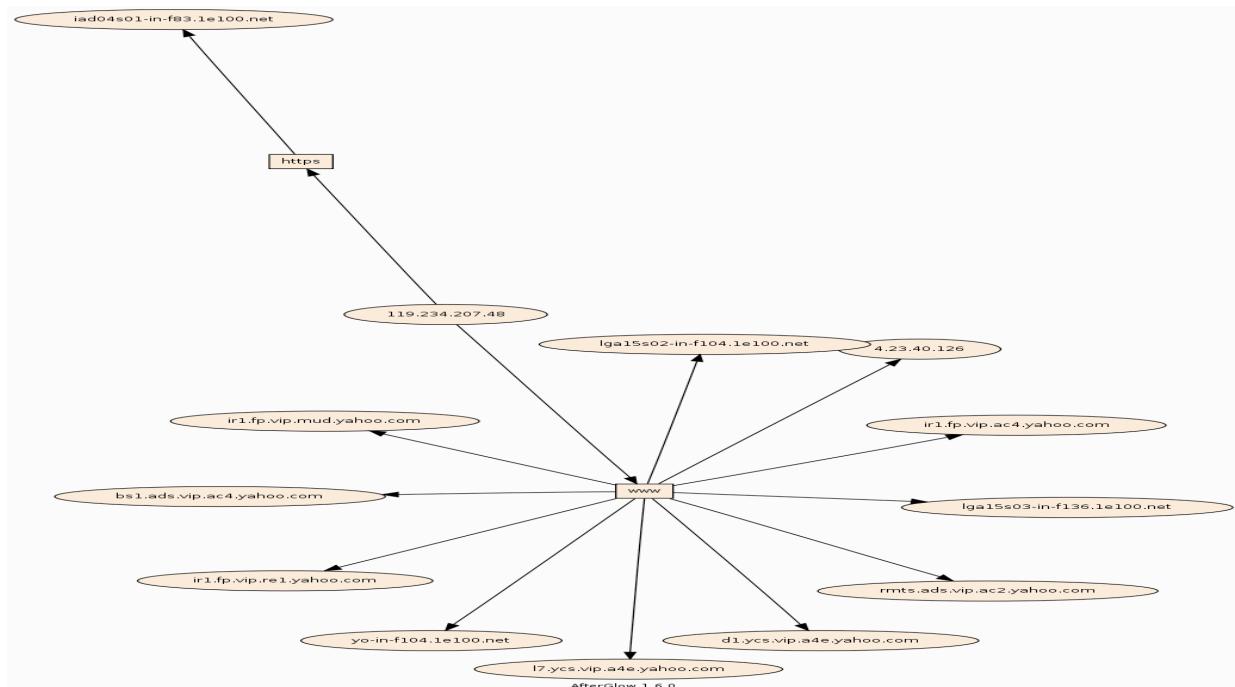
Very easy for Humans to understand

Images are much more powerful

As humans we process colors, shapes, and connections

These are much easier to spot patterns, odd or unknown items and convey critical information.

On the Right: Outgoing HTTP connections from a single IP



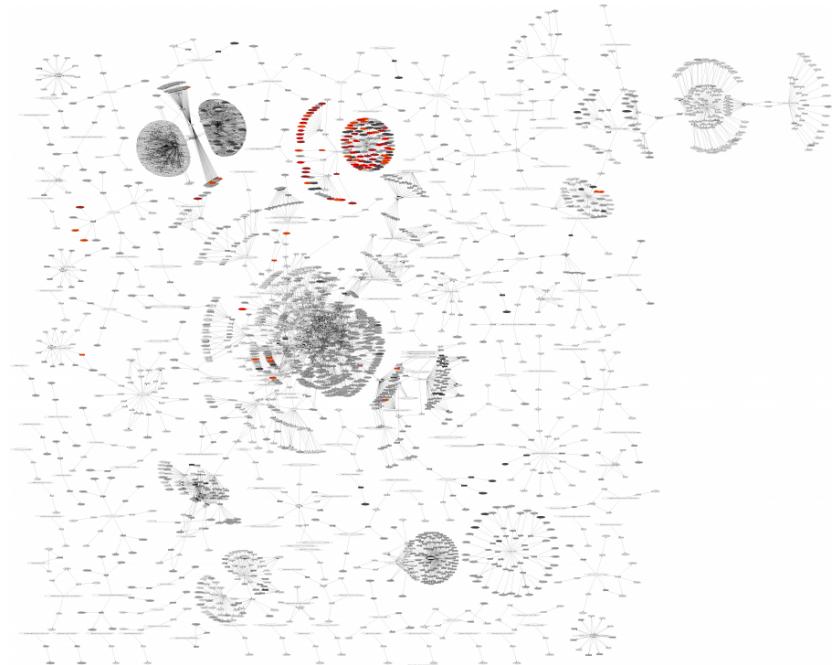
Examples of Visualization

.conf2016

splunk>

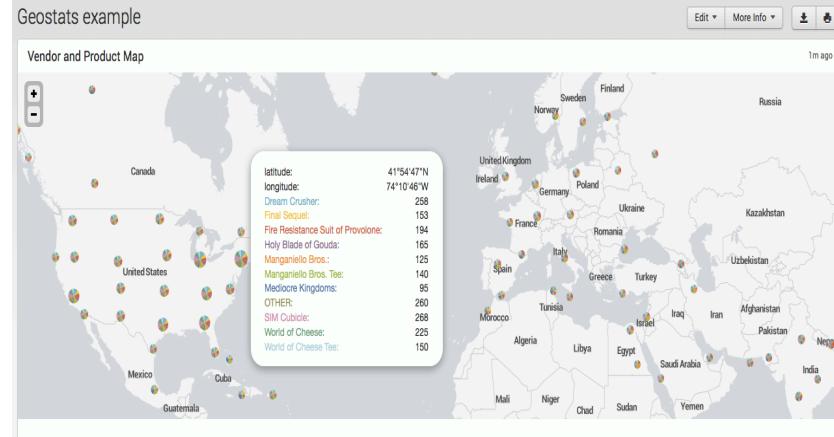
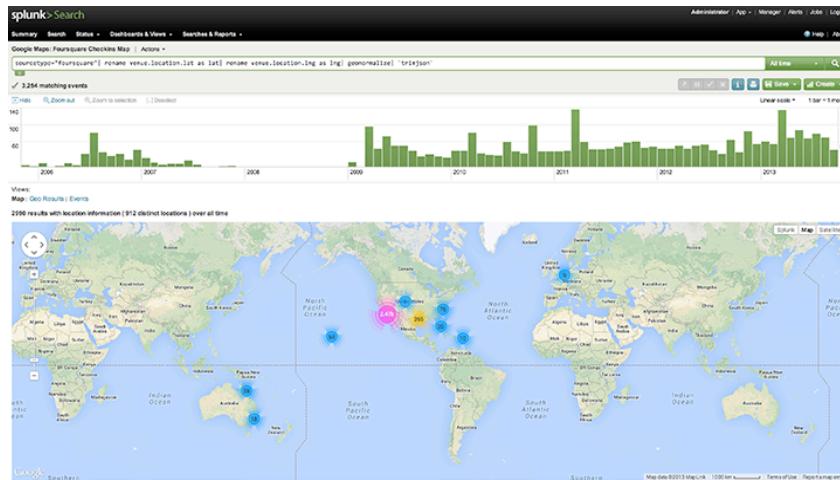
Link Analysis

- Splunk App - Afterglow
- From a search outputs/ visualizes ‘tuples’ of information
- In this case this is NIDS events – Signature, Source Address, Destination Address, Count
- Shows Blooms around specific Signatures



Heat Maps, iplocation and Geostats

- Splunk embedded commands – iplocation and geostats
- On the Left is an Example Dashboard with Google Maps bloom icons for hits
- On the Right is another Map using geostats and OpenStreetView



Traffic Light/Visual Acuity Clues

- Splunk App – TLP – Traffic Light Protocol
- Splunk icons and CSS stylesheets, that communicate overall information

The screenshot shows the "Traffic Light Examples" page within the "Traffic Light App". The top navigation bar includes links for "Administrator", "Messages", "Settings", "Activity", and "Help". Below the title "Traffic Light Examples", there is a sub-instruction: "Build traffic light visualisations into your app using this guide." The main area contains eight panels arranged in two rows of four. Each panel displays a traffic light icon and a numerical value. The first row contains panels for "None", "Low", "Elevated", and "Severe" levels, each with a value of 50, 150, 250, and 350 respectively. The second row contains panels for "None (icon only)", "Low (icon only)", "Elevated (icon only)", and "Severe (icon only)". A footer section titled "And here's how it's done..." provides an overview of the process, mentioning the use of Splunk's "rangemap" command and a "single value" panel.

D3 and the Splunk Web Framework

- Splunk extension/App – The Web Framework
- Leverages Advanced Splunk capabilities for visualization like D3



What Is OSINT and How can Splunk Use it?

.conf2016

splunk>

Open-Source INTelligence = OSINT

- **Open-Source Intelligence (OSINT)** refers to a broad array of information and sources that are generally available, including information obtained from the media (newspapers, radio, television, etc.), professional and academic records (papers, conferences, professional associations, etc.), and public data (government reports, demographics, hearings, speeches, etc.).
- Unlike the other INTs, open-source intelligence is not the responsibility of any one agency, but instead is collected by the entire USIC. One advantage of OSINT is its accessibility, although the sheer amount of available information can make it difficult to know what is of value. Determining the data's source and its reliability can also be complicated. OSINT data therefore still requires review and analysis to be of use to policymakers.

Source: <http://www.fbi.gov/about-us/intelligence/disciplines>

Why do I care about OSINT?

- Data Enrichment
 - Adding Context to events and searches
- Visual Acuity
 - Security Operations Centers
 - Warnings and Alerts
 - World Threat view/Big Screen Display (Funding Assistance Device)
 - Status System Overview
- Early Warnings and Alerts
 - Real-time alerting for sensitive (timeframe, political, etc) events.
 - Forward looking predictive search highlights – Sporting Events, etc

How Can I use OSINT in Splunk?

.conf2016

splunk>

Embedded Splunk functionality – Lookups

Lookups add fields from an external source to your events based on the values of fields that are already present in those events.

A simple lookup example – Adding HTTP comments to HTTP status codes

“200” = “OK”

“404” = “Not Found”

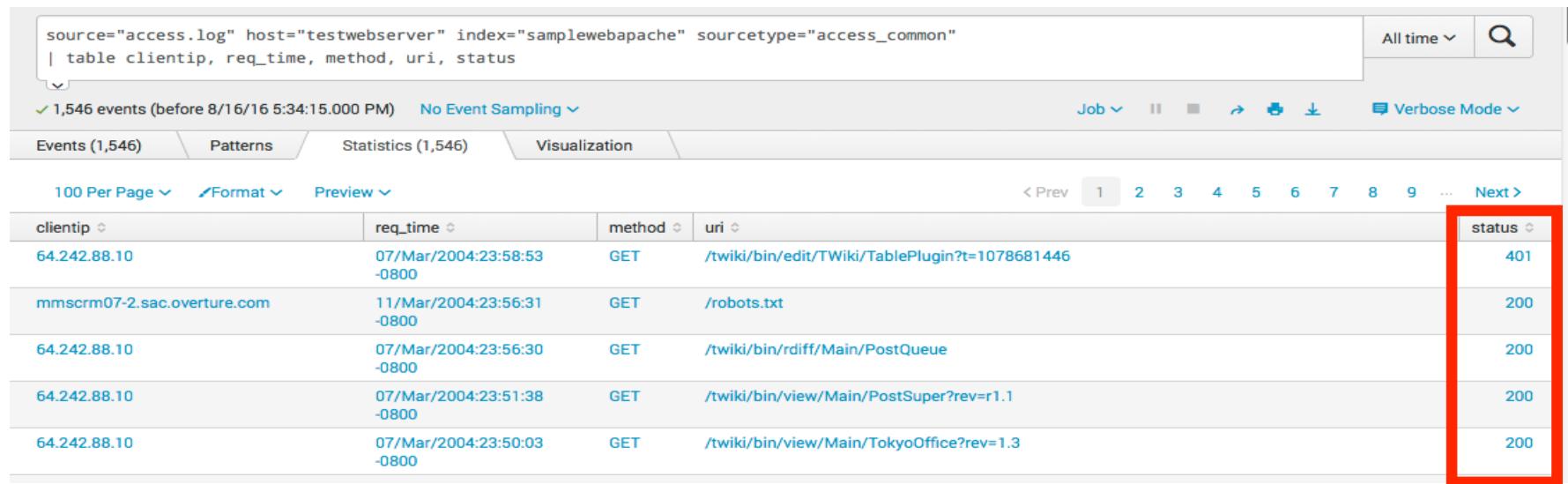
Multiple Types of Lookups – Reference below

Types of Splunk Lookups		
CSV lookup	A common separated file	Useful for static data
External	3 rd party such as a DNS server lookup	Useful for dynamic data
KV Store	KV Collection Store	Useful for KV tables of data
Geo-Spatial	KMZ file that is geographic boundary file	Useful for grouping events into places on earth

Lets add some context to that Data

Normal output from Apache web logs.

- Note the only the HTTP Code is present
“200”, “401”, etc



source="access.log" host="testwebserver" index="samplewebapache" sourcetype="access_common"
| table clientip, req_time, method, uri, status

All time ▾ 🔍

✓ 1,546 events (before 8/16/16 5:34:15.000 PM) No Event Sampling ▾

Job ▾ || ☰ ↶ ↷ ⬇ Verbose Mode ▾

Events (1,546) Patterns Statistics (1,546) Visualization

100 Per Page ▾ Format ▾ Preview ▾

clientip	req_time	method	uri	status
64.242.88.10	07/Mar/2004:23:58:53 -0800	GET	/twiki/bin/edit/TWiki/TablePlugin?t=1078681446	401
mmscrm07-2.sac.overture.com	11/Mar/2004:23:56:31 -0800	GET	/robots.txt	200
64.242.88.10	07/Mar/2004:23:56:30 -0800	GET	/twiki/bin/rdiff/Main/PostQueue	200
64.242.88.10	07/Mar/2004:23:51:38 -0800	GET	/twiki/bin/view/Main/PostSuper?rev=r1.1	200
64.242.88.10	07/Mar/2004:23:50:03 -0800	GET	/twiki/bin/view/Main/TokyoOffice?rev=1.3	200

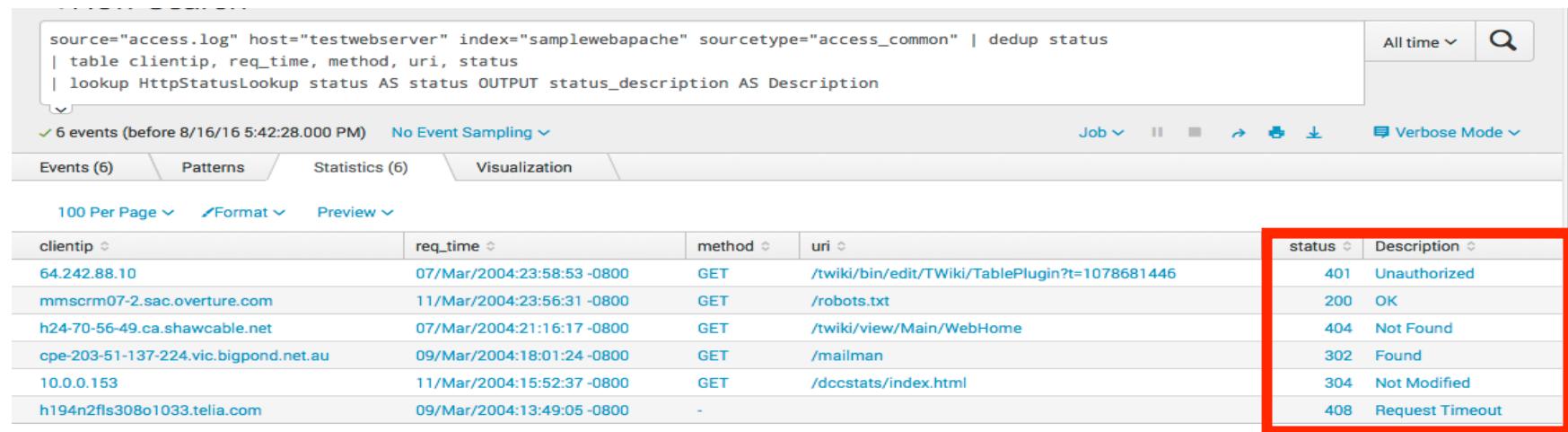
Lookup Definitions – Give that data context

- Splunk Community created a CSV file for HTTP Status messages.
 - http://wiki.splunk.com/Http_status.csv

Fields:

Status, status_description, status_type

- Create a Lookup File and Definition
- Call Lookup and provide Output column
*Mysearch | Lookup HttpStatusLookup
status AS status OUTPUT
status_description AS Description*



The screenshot shows a Splunk search interface. The search bar contains the following command:

```
source="access.log" host="testwebserver" index="samplewebapache" sourcetype="access_common" | dedup status  
| table clientip, req_time, method, uri, status  
| lookup HttpStatusLookup status AS status OUTPUT status_description AS Description
```

The search results table has six rows of event data. To the right of the table, a separate table titled "HttpStatusLookup" is displayed, which maps status codes to descriptions. This lookup table is highlighted with a red border.

status	Description
401	Unauthorized
200	OK
404	Not Found
302	Found
304	Not Modified
408	Request Timeout

Below the tables, there is a visualization section showing the distribution of status codes.

Embedded Splunk functionality - Search Commands/ Search Scripts

Allow for scripts to be used as Lookups

IP Lookups for Tor Records

Search for an IP address to see if it's part of the Tor Network.

Invoked By

CLI:

```
python ip_blacklist_tor.py <IP_address>
```

Splunk:

```
index=security_logs sourcetype=nids |  
lookup torLookup ip AS clientip OUTPUT torinfo AS TorInfo  
| table sourcetype, clientip, TorInfo
```

Positive Hit (CLI)

IP=162.247.72.201 **Nodename=CalyxInstitute14 PORTS=443,80**
FLAGS=Exit,Fast,Guard,HSDIR,Running,Stable,V2Dir,Valid

Negative Hit (CLI)

IP=199.231.120.81.tor.dan.me.uk **Nodename=NOT_TOR**
PORTS=NOT_TOR FLAGS=NOT_TOR

200 N:CalyxInstitute14/P:443,80/F:EFHRSDV

URL	status	TorHost
icons/gnu-head-tiny.jpg	200	No
dateEmail.html	200	No
images/msgops.JPG	200	NotTorHost
mailman/listinfo/webber	200	NotTorHost
wiki/bin/view/Main/LinksOfUse	200	NotTorHost
azor.html	200	NotTorHost

Info
NodeName: CalyxInstitute14
Avail Ports: 443/tcp and 80/tcp Flags
Exit, Fast, Guard, HSDIR, Running, Stable, V2Dir, Valid

Embedded Splunk functionality - Search Commands/ Search Scripts

Allow for scripts to be used as Lookups

Enhanced DNS Lookup

- Start with the default dnslookup script
 - Ships with Splunk
- Prototype (not ready for production)
- DNS Lookup for IP resolution then extended
 - For multiple DNS servers
 - Google DNS, OpenDNS, and AlterNet

DNS lookup Multiple DNS servers

CLI:

```
python external_lookups.py <IP_address>
```

Splunk:

```
index=security_logs sourcetype=nids | lookup EnhancedDNS  
clientip OUTPUT AltDNSResults| table _time, clientip, AltDNSResults
```

Example CLI Output (Prototype -- Need to limit for Splunk)

Method #1 - Socket Lookup

```
Socket lookup static.75.118.4.46.clients.your-server.de
```

Method #2 - DNSPython Lookup

```
DNS Reverse 75.118.4.46.in-addr.arpa.
```

Method #3 - DNS resolver Lookup - Google Pub DNS

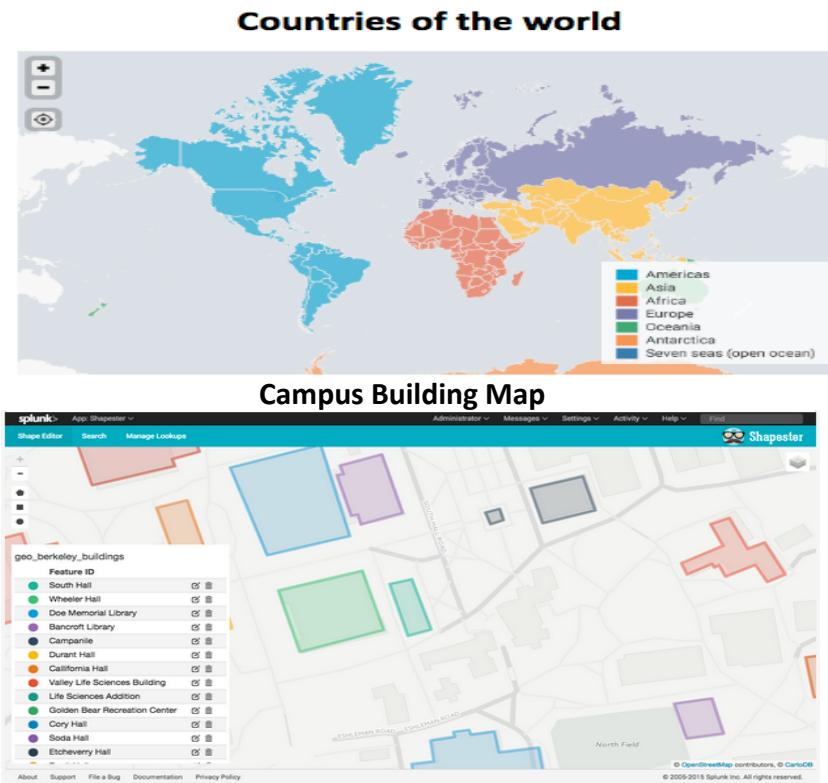
```
DNS Resolution Name1 NO DNS RESPONSE
```

Method #3 - DNS resolver Lookup – OpenDNS

```
DNS Resolution Name NO DNS RESPONSE
```

Geospatial Lookups

- New feature in Splunk 6.3 – Choropleth's
A thematic map with areas shaded in proportion to the measurement of a variable
- Visualizes how a measurement varies by geographic region
- You can add your own! KMZ (Compressed KML file format)
 - Top – Splunk provided
 - Bottom – App Shapester



Splunk Apps – A rich landscape

Splunk Apps

Generally offer extensive user interfaces that enable you to work with your data, and they often make use of one or more add-ons to ingest different types of data.

Some Examples of Apps

- **Splunk ES (Enterprise Security) – (263)**
 - Splunk Enterprise Security gives teams the insight to quickly detect and respond to internal and external attacks, to simplify threat management while minimizing risk. ES helps teams gain organization-wide visibility and security intelligence for continuous monitoring, incident response, SOC operations, and providing executives a window into business risk.
- **Splice – (now SA-Splice – 2637)**
 - SPLICE currently supports STIX 1.1, CybOX 2.1, OpenIOC 1.0 and 1.1 formats and provides a way of consuming IOCs in Splunk to leverage the indicators and provide greater context than common threat feeds. SPLICE can monitor local directories, or mount points, for incoming IOCs as well as TAXII feeds like Soltra Edge to periodically poll IOCs.
- **Shapester –(2893)**
 - This app lets you draw your own shapes and polygons directly on the map and save them as a geospatial lookup. You can then use this lookup to set up alerts based on geofences. Or you can create a building map by drawing the buildings of your campus.
- **Here Maps (Paid) – (1887)**
 - The here maps app brings a couple of nice added map visualization options: marker maps, cluster maps, heat maps, line maps and choropleth maps. All of them can be customized. It also adds a reverse geocoder for translating lat/lng combinations into human readable addresses.

Splunk ES –Enterprise Security

Paid app from Splunk

Features

- CIM compliant data access (standardized splunk data)
- Out-of-the-box alerting, reporting, and dashboards
- Incident and Event Management options

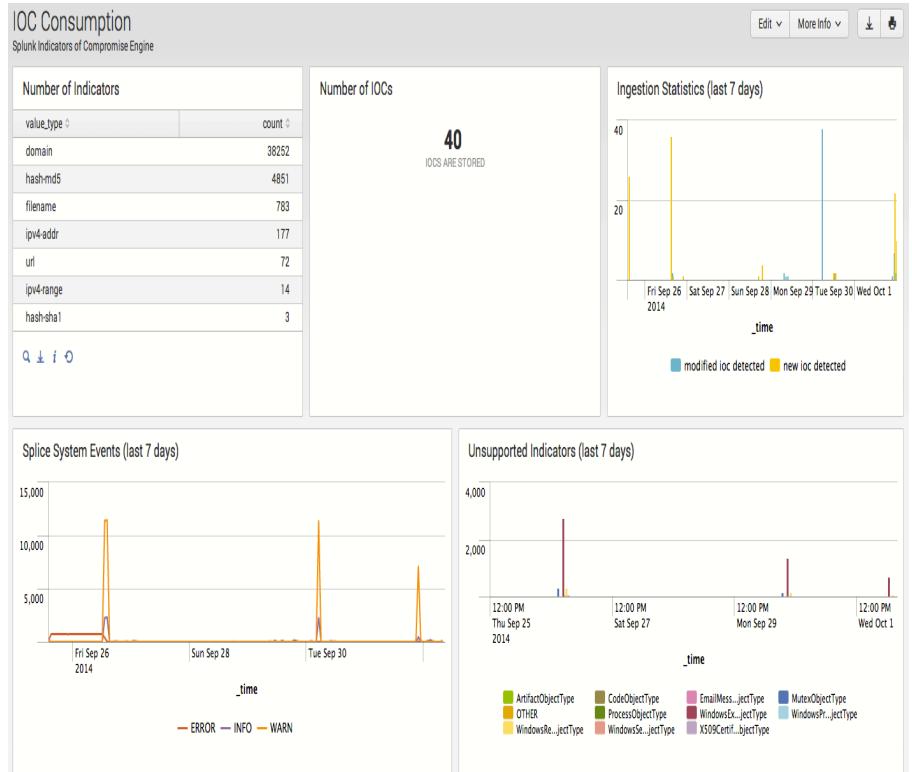


Splice – Indicator focused, ES-like

Free app from Splunk

Features

- Data enrichment
 - Support indicators in multiple formats
 - STIX, CyBox, OpenIOC, Yara
- Out of the box rules, dashboards, and lookup tables for threat information

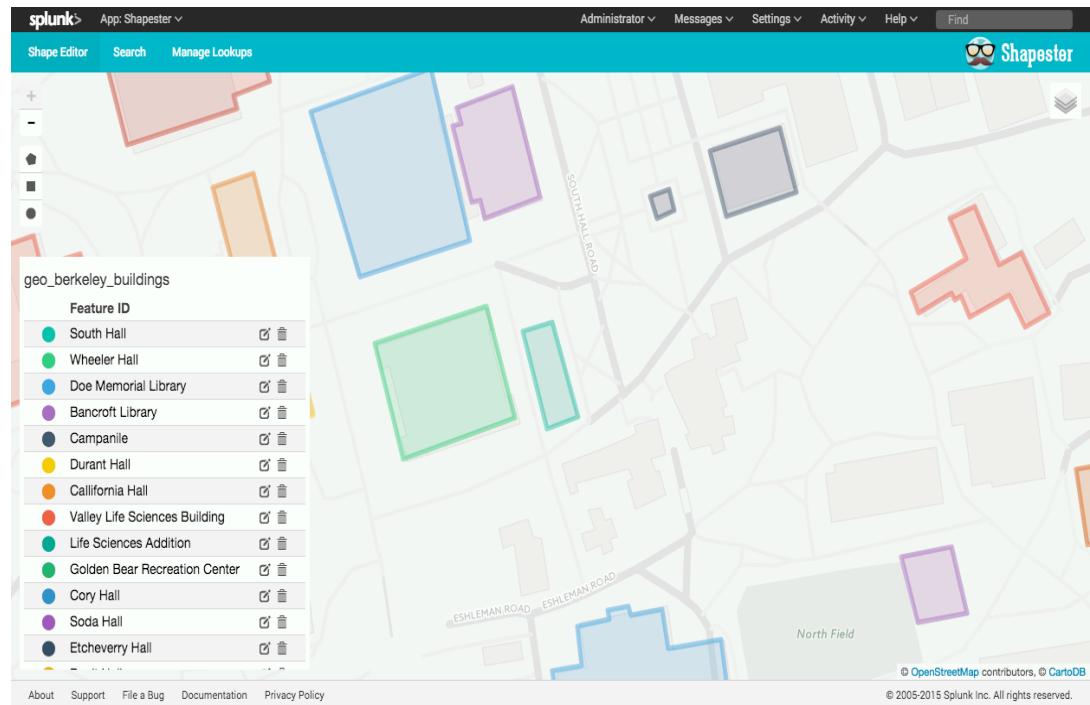


Shapester – Geo-fencing the world

Free App

Features

- Create shapes and polygons on Geomaps
 - Saved as Geospatial lookups
- Ability to create Splunk Alerts for ‘Geo-fenced’ areas such as a campus or office locations.



Here Maps

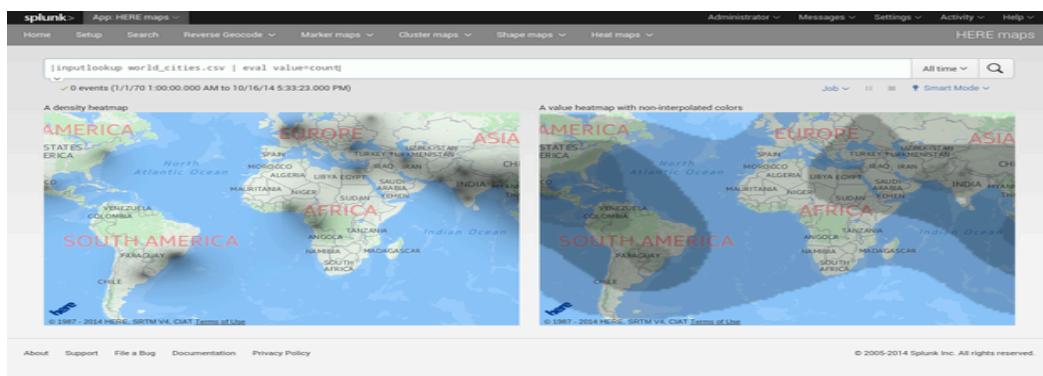
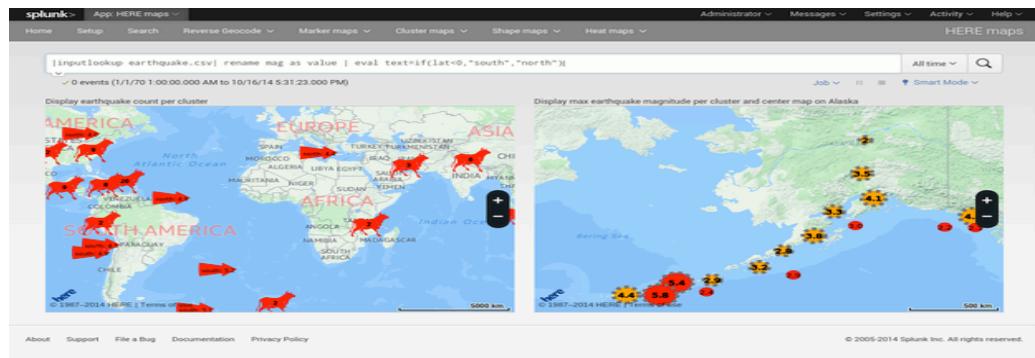
Free App

(but needs a paid API to take full advantage)

Part of larger ArcGIS/ESRI application suite

Features

- Additional Visualizations
 - Marker Maps, cluster Maps, Heat Maps, etc
 - Custom Iconography



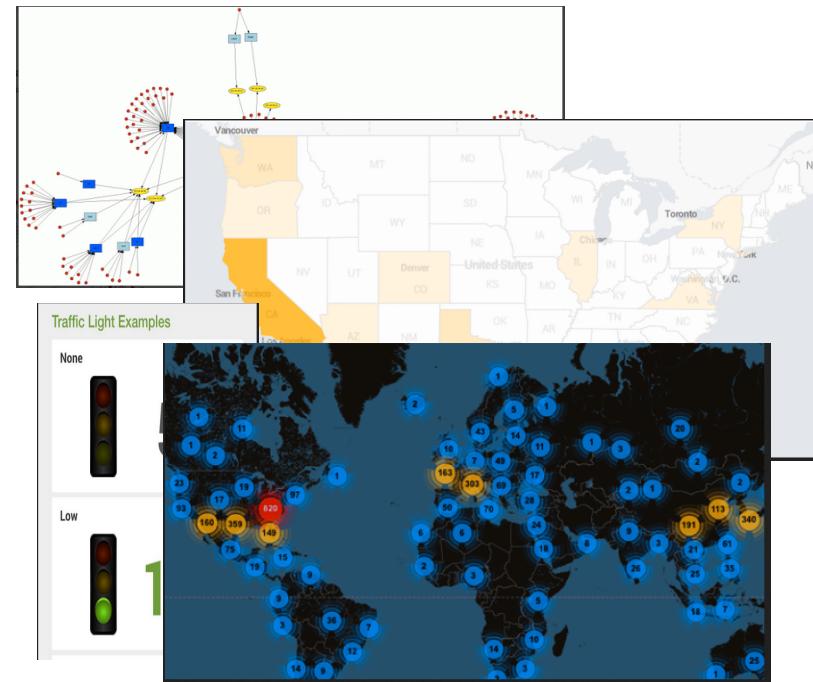
Visualization



Visualization

Splunk has lots of Options

- Splunk Dashboards - Makes the data look good
 - Provide a multi-faceted view into data
 - Large Data volumes – Grouping to the rescue
 - Afterglow – Flower blooms
- Choropleth – Geo/Country boundaries
 - Fence in office locations or metropolitan areas
 - Countries of interest
- Heat Maps – Focus areas
 - Identify concentrations of attacks/victims
- TLP – High level visibility
 - Operating Status from a high level



Hunting Bad Guys

.conf2016

splunk>

Hunting Bad Guys

- Easy Wins
 - Geo-location mapping
 - Dashboards with Lookups
 - Search Commands with external input – Reports, Dashboards, etc
- Advanced Wins
 - STIXX and TAXII feeds
 - Splunk REST API
 - IOCs, and Yara signatures Oh my!

Hunting Bad Guys

Easy Wins

.conf2016

splunk>

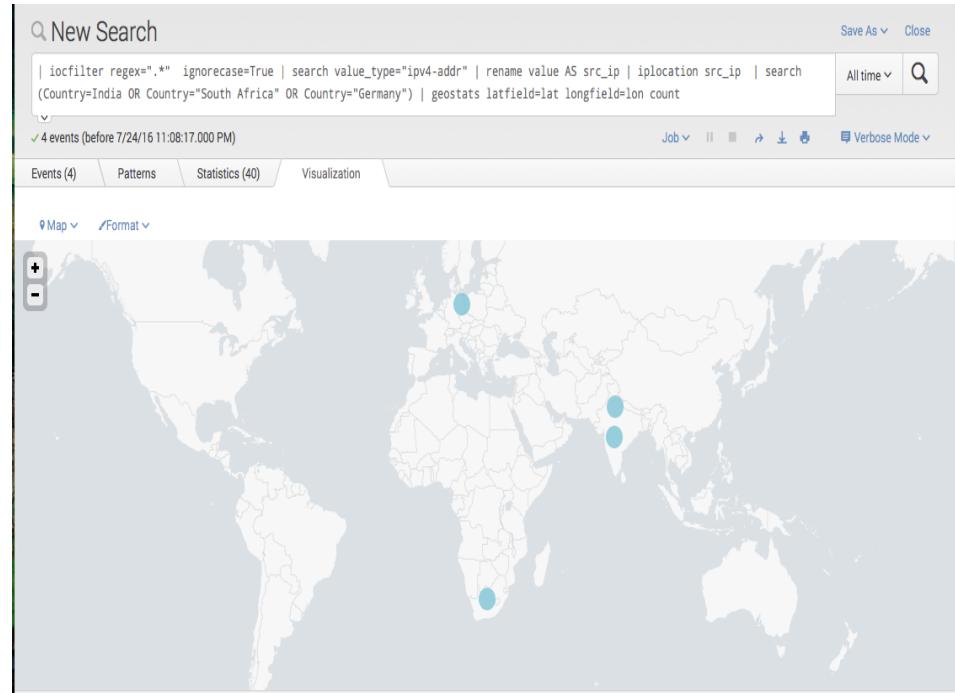
Easy Win

Geo-location Mapping

- Simple Country filtering

```
Mysearch | iplocation src_ip | search  
(Country=India OR Country="South Africa"  
OR Country="Germany") | geostats  
latfield=lat longfield=lon count
```

- Splunk embedded commands used
 - iplocation/geostats – geo-coding information
 - Geom (Newer command)
Geom - Allows for Geo-fencing framing via polygons
 - Geomfilter – geo-fencing limiting



Easy Wins

Dashboards with Content

- Dashboards with Lookups – Tor search script to dashboard
 - Enriching Dashboards with lookup data
 - Visualize Tor lookup via country/iplocation map and table
 - Embedded command - outputlookup create a lookup from dynamic data
- Search Commands with external input – Reports, Dashboards, etc
 - Interacting with other API's Lookups, search scripts and more

Dashboards with Lookups

External lookups - Tor lookup in Dashboard Panel

- Visualize Tor lookup via country/olocation map and table

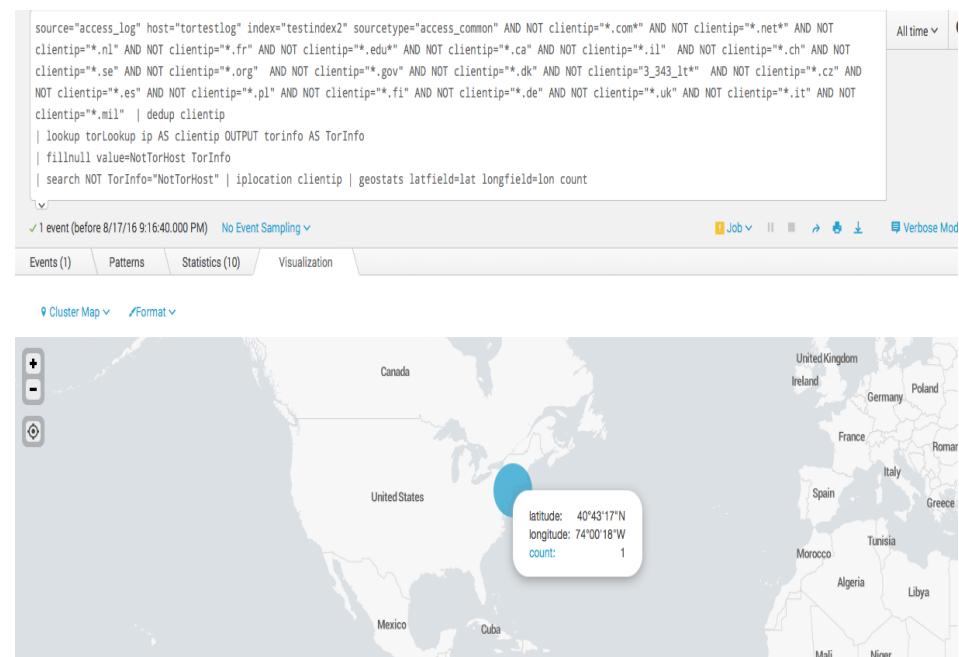
Examples:

- **Add content as a field**

```
Index=security_logs sourcetype=nids
| lookup torlookup clientip OUTPUT torvalue
| table alert, clientip, torvalue
```

- **Map NIDS alerts that are from Tor devices**

```
Index= security_logs sourcetype=nids
| lookup torlookup clientip OUTPUT torvalue
| search NOT torvalue="*NOT_TOR*"
| iplocation clientip | geostats latfield=lat
longfield=lon count
```



Create Dynamic Lists

Use Embedded Splunk command - outputlookup

Splunk SPL command 'outputlookup'

Used to transform results from a search into a new lookup table search (dynamic) data

Useful for building 'correlated' events

Example

IP's from a specific NIDS signature add to a watchlist for VPN logins to monitor for attackers.

Fill in the lookup

```
Index=security_logs sourcetype=NIDS  
signature="Cisco VPN DoS" | dedup src_ip  
| table src_ip  
| outputlookup CiscoVPNAttackers
```

Now search for the attackers in the VPN logs

```
Index=remote_access_logs sourcetype=cisco  
| lookup CiscoVPNAttackers src_ip OUTPUT  
ListVpnAttackers | where isnotnull(ListVpnAttackers)  
| table sourcetype, ListVpnAttackers
```

The image displays three vertically stacked Splunk search results. The top search bar shows a search for NIDS signatures related to Cisco VPN DoS. The middle search bar shows a search for Cisco VPN logs, performing a lookup against the previously defined dynamic list of VPN attackers. The bottom search bar shows the resulting list of client IP addresses found in the VPN logs, which were identified as attackers based on the NIDS signature. This demonstrates how the outputlookup command can be used to build a dynamic list of sources for further analysis.

Interacting with External Commands

Interacting with other API's Lookups, search scripts and more

- Search for an IP address to see if it's part of the Tor

```
index=security_logs sourcetype=nids  
| lookup torlookup ip AS clientip  
OUTPUT torvalue AS TorInfo  
| fillnull value=NotTorHost TorInfo  
| table sourcetype, clientip, TorInfo
```

Positive Hit

200 N:CalyxInstitute14/P:443,80/F:EFHRSDV

Negative Hit – (Custom result)

NotTorHost

- String value

The screenshot shows the Splunk search interface with the following details:

- Search Bar:** All time, Q
- Search String:** source="access_log" host="tortestlog" index="testindex2" sourcetype="access_common" AND NOT clientip=".com*" AND NOT clientip=".net*" AND NOT clientip=".nl*" AND NOT clientip=".fr*" AND NOT clientip=".edu*" AND NOT clientip=".ca*" AND NOT clientip=".il*" AND NOT clientip=".ch*" AND NOT clientip=".se*" AND NOT clientip=".org*" AND NOT clientip=".gov*" AND NOT clientip=".dk*" AND NOT clientip="3_343_it*" AND NOT clientip=".cz*" AND NOT clientip=".es*" AND NOT clientip=".pl*" AND NOT clientip=".fi*" AND NOT clientip=".de*" AND NOT clientip=".uk*" AND NOT clientip=".it*" AND NOT clientip=".mil*" | dedup clientip | lookup torlookup ip AS clientip OUTPUT torinfo AS TorInfo | fillnull value=NotTorHost TorInfo | table clientip, method, uri, status, TorInfo
- Results Panel:** 26 events (before 8/17/16 8:29:40,000 PM) No Event Sampling
- Event View:** Events (26), Patterns, Statistics (26), Visualization, Job, Verbose Mode
- Table Headers:** clientip, method, uri, status, Torinfo
- Table Data:**

clientip	method	uri	status	Torinfo
61.165.64.6	GET	/icons/gnu-head-tiny.jpg	200	NotTorHost
213.181.81.4	GET	/LateEmail.html	200	NotTorHost
194.151.73.43	GET	/images/msgops.JPG	200	NotTorHost
162.247.72.201	GET	/mailman/listInfo/webber	200	N:CalyxInstitute14/P:443,80/F:EFHRSDV
195.246.13.119	GET	/twiki/bin/view/Main/LinksOfUse	200	NotTorHost
212.21.228.26	GET	/razor.html	200	NotTorHost

Interacting with Multiple Field Output

Lookup BGP information for an IP – Taking the fight beyond your perimeter

- Show the BGP information to an IP
- BGP or Border Gateway Protocol
 - Short version
 - Routing around the world and among the Telecoms/ISPs
 - BGP contains IPv4 CIDR blocks within an ASN (Autonomous System Number)
 - Allows routing large segments of the internet
- **Why Do we care?**
 - What if you could block all of a phishing campaign by issuing one command for all of their IP ranges?

Searches for the BGP information for a given IP

(Team Cymru Service) (others such as HE are available as well)

CLI:

```
python bgp_cymru.py <IP_address> <asnvalues>
```

Splunk:

```
index=security_logs sourcetype=nids  
| lookup bgp_lookup clientip OUTPUT BGPRResults1, BGPRResults2,  
BGPRResults3, BGPRResults4  
| rename BGPRResults1 as ASN, BGPRResult2 as BGPOwner,  
BGPRResult3 as BGPCountry, BGPRResult4 as BGPCIDR
```

Example Output (Prototype For Now)

CLI:

```
python bgp_cymru.py 41.168.5.140
```

OUTPUT: test 36937,Neotel-AS, ZA,41.168.0.0/16

Hunting Bad Guys

Advanced Wins

.conf2016

splunk>

Indicator Management - Standards

What is TAXII and STIX ?

TAXII –

Trusted Automated eXchange of
Indicator Information

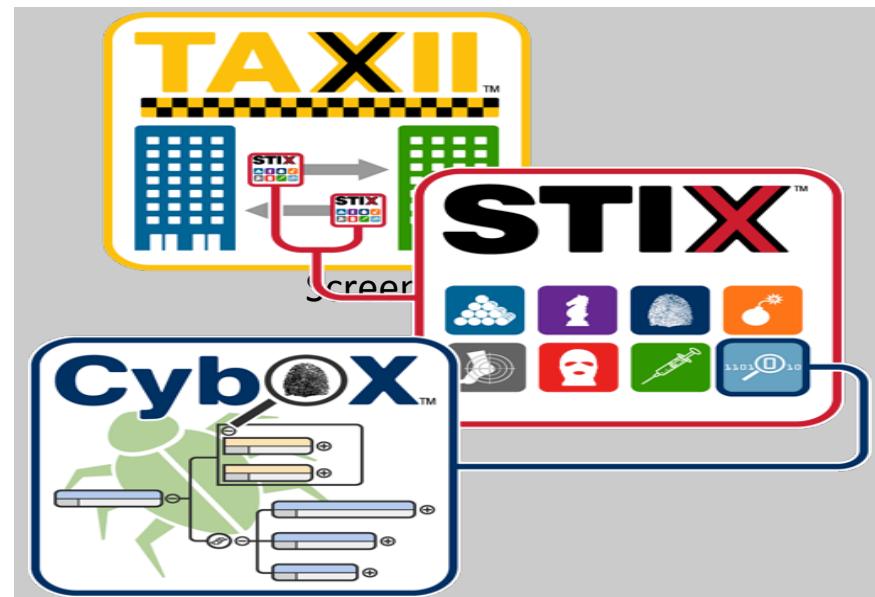
STIX –

Structured Threat Information
eXpression

CybOX –

Cyber Observable eXpression

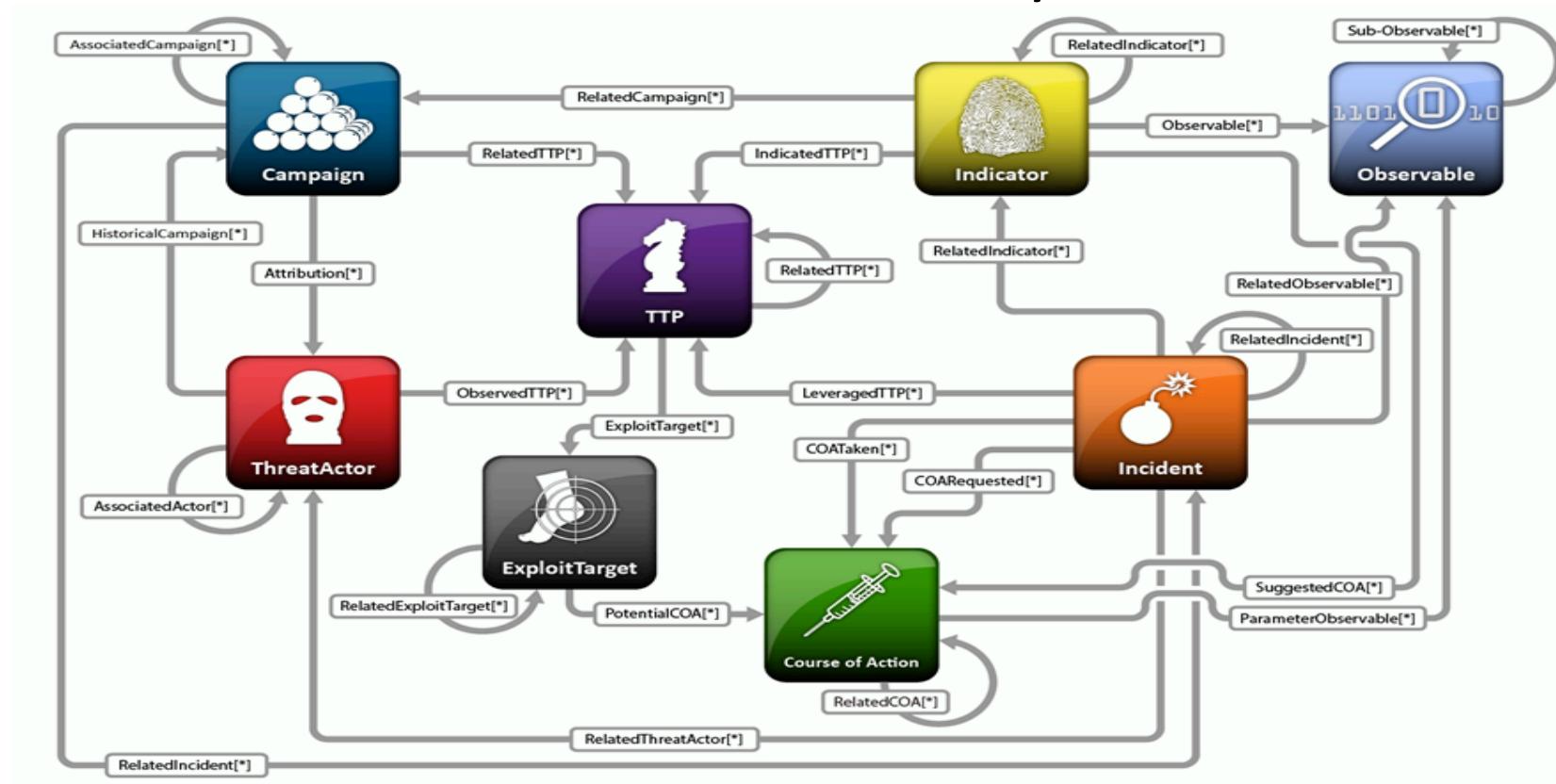
US-CERT Definitions and Icons



Advanced Wins

- STIXX and TAXII feeds
 - TAXII
 - The delivery system “Uber of Indicators” (vehicle used to transport indicators)
 - STIX
 - The person in the “Uber” (enriched indicators with content/context labels)
 - CybOX
 - What the person is carrying (Threat Data Management)
- Splunk REST API
 - Using Splunk’s API to manage lookups
- IOCs, and Yara signatures Oh my!
 - Integration of other threat types

TAXII and STIX Ecosystem



Threat Management – Enterprise Security (ES)

Splunk ES

- ES allows for integration of TAXII sources
- Creates several data models, accelerations and workflow (ES) integration

- Ships with an number of ‘threat sources’ that can be useful for demonstrating how to use Threat Feeds
- Supported Indicators Types
 - X509 Certificates
 - Email
 - Files names/hashes
 - HTTP
 - IP/Domains
 - Processes
 - Registry entries
 - Services
 - Users

Splunk ES

Default App Dashboard Example

Screenshot of the Splunk Enterprise Security (ES) Default App Dashboard.

Threat Activity

- Threat Matches:** Unique Count: 109 (+8)
- Threat Collections:** Unique Count: 5 (0)
- Threat Categories:** Unique Count: 4 (0)
- Threat Sources:** Unique Count: 7 (-1)
- Threat Activity:** Total Count: 139 (+7)

Threat Activity Over Time

Most Active Threat Collections

threat_collection	search	sparkline	dc(artifacts)	count
ip_intel	Email Address Matches Network Resolution Matches Source IP Information Matches		40	95
file_intel	File Hash Matches File Name Matches		22	37
certificate_intel	Certificate Common Name Matches Certificate Organization Matches Certificate Subject Name Matches Certificate Unit Matches Email Address Matches		4	5
process_intel	Process Matches		1	1
service_intel	Service Matches		1	1

Most Active Threat Sources

source_id	source_path	source_type	count
emerging_threats_ip_blocklist	/var/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/emerging_threats_ip_blocklist.csv	csv	44
iblocklist_logmein	/var/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_logmein.csv	csv	43
mandiant_package-190593d6-1861-4cf6-b212-c016fce1e240	/var/splunk/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel/Appendix_G_IOCs_No_OpenIOC.xml	stix	39
mandiant_package-190593d6-1861-4cf6-b212-c016fce1e249	/var/splunk/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel/Appendix_F_SSLCertificates.xml	stix	5
malware_domains	/var/splunk/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/malware_domains.csv	csv	4
fireeye_stix-b7b16e67-4292-46a3-be64-60c1a491723d	/var/splunk/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel/fireeye-pivx-report-with-intel&stix	stix	2
mandiant_package-190593d6-1861-4cf6-b212-c016fce1e242	/var/splunk/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel/Appendix_D_FQDNs.xml	stix	2

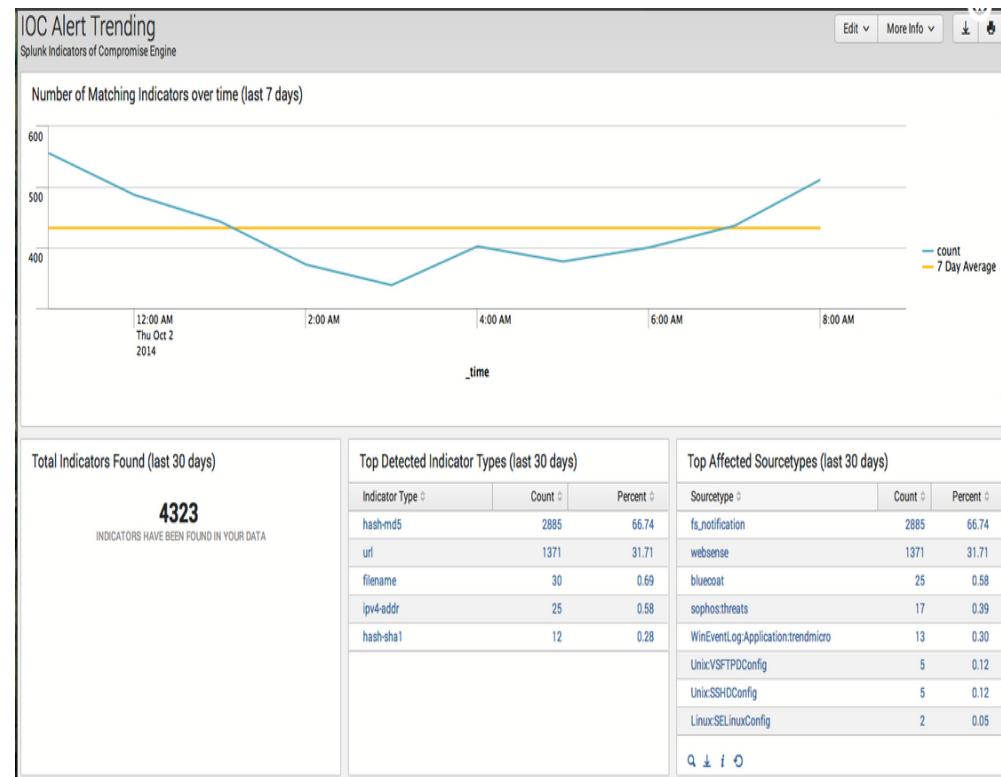
Threat Activity Details

_time	threat_match_field	threat_match_value	filter	source_type	src	dest	threat_collection	threat_group	threat_category
2015-7-28 13:35:00	file_name	setup.exe	WinEventLog:Application:trendmicro	unknown	L-mickey02	file_intel	undefined	undefined	
2015-7-28 13:35:00	file_name	svchost.exe	WinEventLog:Application:trendmicro	unknown	OWNER-PC	file_intel	undefined	undefined	
2015-7-28 13:30:00	ssl_subject_common_name	SLR	stream:tcp	unknown	unknown	certificate_intel	undefined	undefined	
2015-7-28 13:30:00	file_hash	05cc052646fbdf25fb610c1fe120195f	ts_notification	unknown	es-is0-na.demo.splunk.com	file_intel	undefined	undefined	
2015-7-28 13:30:00	ssl_hash	af2f7b070245c90bd2a0a0845314173a	stream:tcp	unknown	unknown	file_intel	undefined	undefined	

Threat Management – Splice

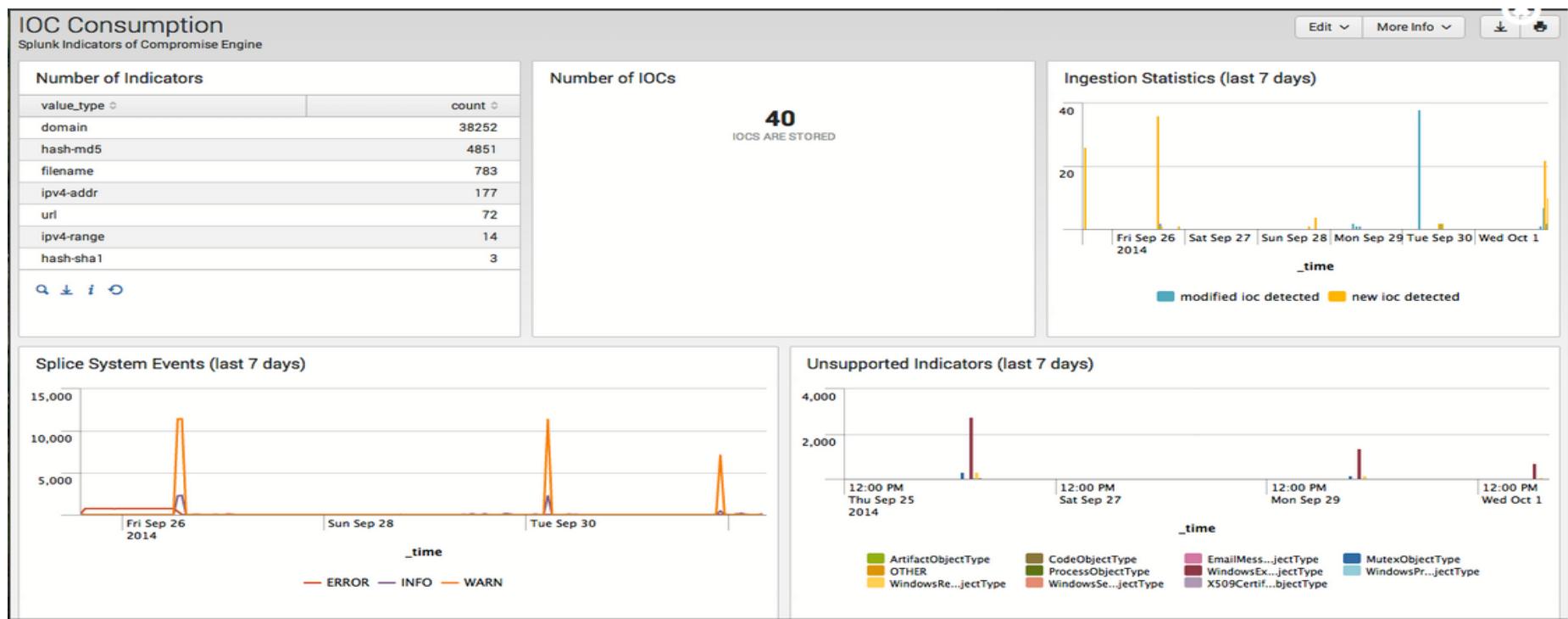
SA-Splice

- Splice has some of the features of a full ES deployment but is focused more on indicator management as it uses a stand alone MongoDB to store indicators.
 - **NOTE:** Splice also *does not* require the deployment to be CIM compliant, making it attractive to 'try' Threat Intelligence.
- Adds several 'ioc*' specific commands to allow for searching and filtering of indicators.
- Great for small or low budget environments to enable integration of threat source information



SA-Splice

Default Dashboard Example



Splunk RESTful API

Splunk's REST API provides powerful access to Splunk.

Create/Edit Objects in Splunk

List and query indexes
| rest /services/data/indexes count=0

Run Saved Searches
| rest /services/search/jobs count=0
splunk_server=local | search isSaved=1

Manage a lookup table?

Now that's useful for security...

Only have to upload the csv file to
\$SPLUNK_HOME to allow the REST API
to access

Splunk Documentation has several examples

List all of the lookup tables

```
curl -k -u admin:pass https://localhost:8089/servicesNS/  
admin/search/data/lookup-table-files
```

Modify a specific lookup table

*Warning – modifies by replacement
Good for indicators though

```
curl -k -u admin:pass \ https://localhost:8089/servicesNS/  
admin/search/data/lookup-table-files/lookup.csv \ -d  
eai:data=/opt/splunk/var/run/splunk/lookup_tmp/  
another-lookup-in-staging-dir.csv
```

IOCs, and Yara signatures Oh my!

What other types of Indicators Of Compromise (IOC) can Splunk use ?

- **OpenIOC**

- An IOC standard proposed by Mandiant
- XML based
- Similar structure to STIX/CyBOX
- Splice and ES can both Integrate
 - › Splice uses a custom Data Input called IOC Mount
 - › ES uses a file mount as well with additional requirements
- Splice
 - › One solution is file based input from either subscription or feed
 - › File contents read, parsed and indicators extracted

Example

Use an Open Threat Service to collect IOC's(IOCbucket.com)

Requirement

- Produce OpenIOC and Yara signatures
- Release IOCs via RSS streaming service

Solution

- I created a Python script to subscribe, read, and decode the IOCs as they are published.
- Script places them in a path for access by Splunk for parsing.

Yara Indicator Files –

* Development Only *

```
ghostmobile:searchscripts jbabbins$ ls /opt/INDICATOR_LISTS/
ASN_Lists           DNS_Lists          Open_IOCs
CarbonBlack_Threat_Feeds   IP_Lists          SSL_Lists
ghostmobile:searchscripts jbabbins$ ls /opt/INDICATOR_LISTS/Open_IOCs/
6d2a1b03-b216-4cd8-9a9e-8827af6ebf93.ioc
af2e8c80-13db-4a57-99ac-460cccd192333.ioc
iocbucket_08441c5d5f339359e526d6705465c30777092bda_xtreme_rat.ioc
iocbucket_2183166efc891d4014028fd0f10c46a4773efd.ioc
iocbucket_2224f9311a8b9bd6e051c485142a7dd2728cf40_xtremerat.ioc
```

```
Splunk_Threat_List
libtaxii_client.py
```

```
iocbucket_4b0e620a0099aa8cea619ba84ed5fd54b44f7aef_cridex_banking_malware.ioc
iocbucket_77c6895dde02b37b50b78e0326e07c9978a55980.ioc
iocbucket_95c6df2e29186f0de13eaalcae49cb8626fba9ae_ngrbot_rootkit.ioc
iocbucket_cdf7e4a7735d2505bd5c75ca5c23b50f57664ec2_ramnit_rootkit.ioc
```

Threat Intelligence platform Integration

- **CRITS**
 - MITRE developed and released Open-Source Threat management platform
- Can we integrate this with Splunk?
 - Experiment to use communications platform (Slack channel) to query the TI platform, Splunk and access a 3rd party API?
 - Yes! Successfully tested and produced by the Crypsis intern team in only a short period of time.
 - › **Splunk – Queries instance of Tor IP information**
 - › **Custom 3rd party - Threat Feeds**
 - › **Geo-location mapping result**

@crits lookup 98.232.234.54

crits BOT 11:46 AM

SPLUNK

IP=54.234.232.98.tor.dan.me.uk

Nodename=NOT_TOR PORTS=NOT_TOR

FLAGS=NOT_TOR

NOT ZEUS

NOT RANSOMWARE

NOT FEODO BOTNET TROJAN

98.232.234.54,US,United States,OR,Oregon,Beaverton,97007,America/Los_Angeles,45.45,-122.88,820

Future Ideas

.conf2016

splunk>

Future Ideas

- **Event Enrichment**
 - Threat Source Evaluation
 - BGP tagging
 - External Threat Management
 - CRITS, Soltra Edge, etc
 - Social Media – Keywords matched to Geo-location
 - Twitter text to content
- **Enhanced Splunk extension**
 - D3 overview/Examples
- **External Tools**
 - Maltego Examples

Future Threat Source Evaluation

- **Dashboards and Reports**

- Highlight value of threat sources
 - How many IOC's are being triggered?
 - From which Threat Source?
 - What type of indicator Network? Host?

- **Solution**

- Splice Provides several insights into the data via dashboards
 - IOC Consumption
 - IOC Types

Enable evalution of threat sources

*-ISAC data being used ?

- Produce a dashboard or report to show **Indicators by Volume over time**

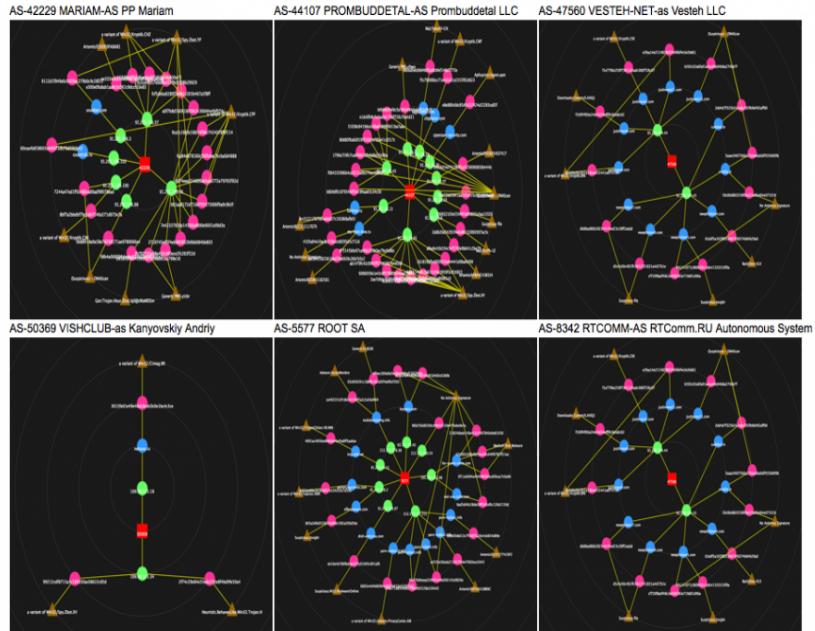
Number of Indicators		<1m ago
value_type	count	
filename	76	
domain	40	
hash-md5	27	
ipv4-addr	9	

Total Indicators by IOC Source (last 30 days)			1m ago
IOC Source	Count	Percent	
Local_IOCs	152	100.00	

Future – Threats outside your borders (BGP)

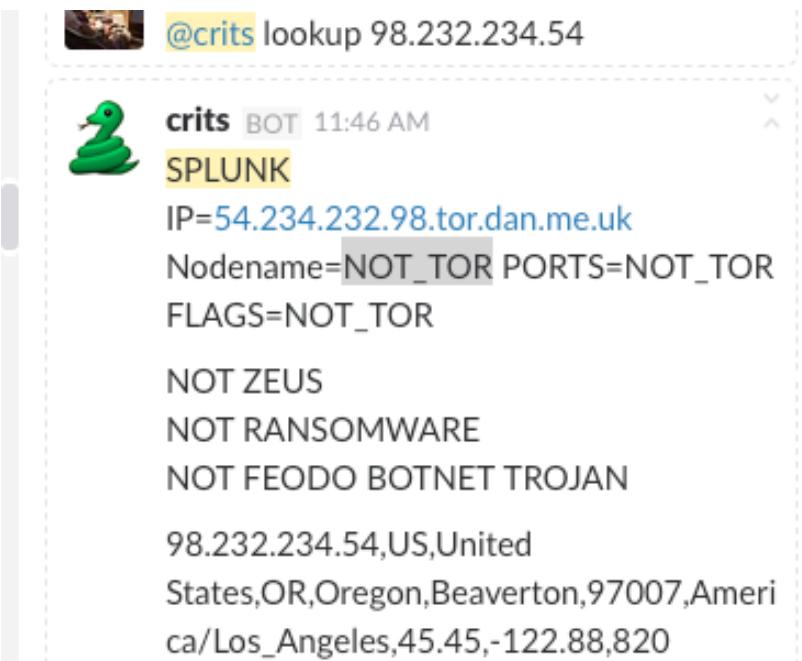
- **BGP tagging**
 - Search Scripts to perform BGP lookup for IP addresses
 - Extract or report on ASN owners or geo-location
- **Example**
 - A takedown of a hostile network by ‘de-peering’ BGP routes to/from it
 - Used Afterglow visualization to highlight takedown
 - Splunk –
 - Search BGP lookup results to show trimming down the peer AS list over time

Takedown – Troyak (Zeus) botnet



Future - Threat Management

- CRITS Integration with Splunk
 - **Slack**
 - Communications platform to query CRITS and Splunk
 - Splunk instance stores information such as Tor records
 - 3rd party API searches other data source
 - **Splunk**
 - Return back to communications platform the information
- Other enhancements being worked out



@crits lookup 98.232.234.54

crits BOT 11:46 AM

SPLUNK

IP=54.234.232.98.tor.dan.me.uk

Nodename=NOT_TOR PORTS=NOT_TOR

FLAGS=NOT_TOR

NOT ZEUS

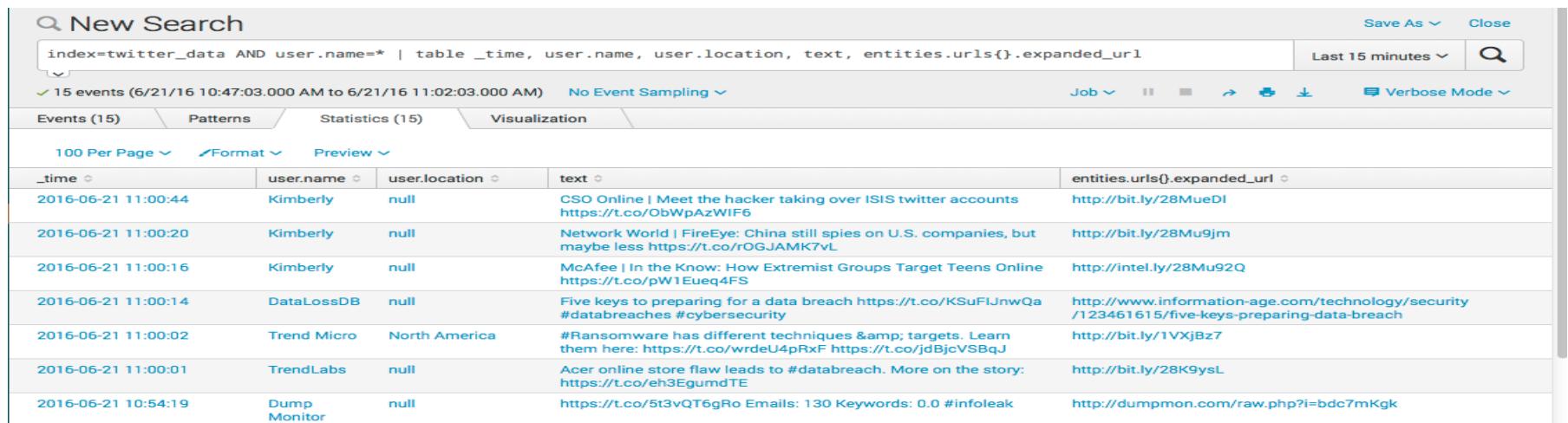
NOT RANSOMWARE

NOT FEODO BOTNET TROJAN

98.232.234.54,US,United States,OR,Oregon,Beaverton,97007,America/Los_Angeles,45.45,-122.88,820

Future – Social Media

- Lazy me – recording and tracking my twitter feed in splunk
 - REST API as data input (It's only JSON right? ☺)
 - Store in index only for messages, urls and names for now
 - Run a lookup of 'dirty' words then add to alert
 - Generates a daily report of tweets per day



The screenshot shows a Splunk search interface titled "New Search". The search query is: "index=twitter_data AND user.name=* | table _time, user.name, user.location, text, entities.urls{}.expanded_url". The results show 15 events from June 21, 2016, between 10:47:03 AM and 11:02:03 AM. The table has columns for _time, user.name, user.location, text, and entities.urls{}.expanded_url. The data includes various tweets from users like Kimberly, DataLossDB, Trend Micro, and TrendLabs, along with their locations and URLs.

_time	user.name	user.location	text	entities.urls{}.expanded_url
2016-06-21 11:00:44	Kimberly	null	CSO Online Meet the hacker taking over ISIS twitter accounts https://t.co/ObWpAzWf6	http://bit.ly/28MuE6I
2016-06-21 11:00:20	Kimberly	null	Network World FireEye: China still spies on U.S. companies, but maybe less https://t.co/rOGJAMK7vL	http://bit.ly/28Mu9jm
2016-06-21 11:00:16	Kimberly	null	McAfee In the Know: How Extremist Groups Target Teens Online https://t.co/pW1Eueq4FS	http://intel.ly/28Mu92Q
2016-06-21 11:00:14	DataLossDB	null	Five keys to preparing for a data breach https://t.co/KSuFIJnwQa #databreaches #cybersecurity	http://www.information-age.com/technology/security/123461615/five-keys-preparing-data-breach
2016-06-21 11:00:02	Trend Micro	North America	#Ransomware has different techniques & targets. Learn them here: https://t.co/wrdU4pRxF https://t.co/dBjcVSBqJ	http://bit.ly/1VXjBz7
2016-06-21 11:00:01	TrendLabs	null	Acer online store flaw leads to #databreach. More on the story: https://t.co/eh3EgumdTE	http://bit.ly/28K9ysL
2016-06-21 10:54:19	Dump Monitor	null	https://t.co/5t3vQT6gRo Emails: 130 Keywords: 0.0 #infoleak	http://dumpmon.com/raw.php?i=bdc7mKgk

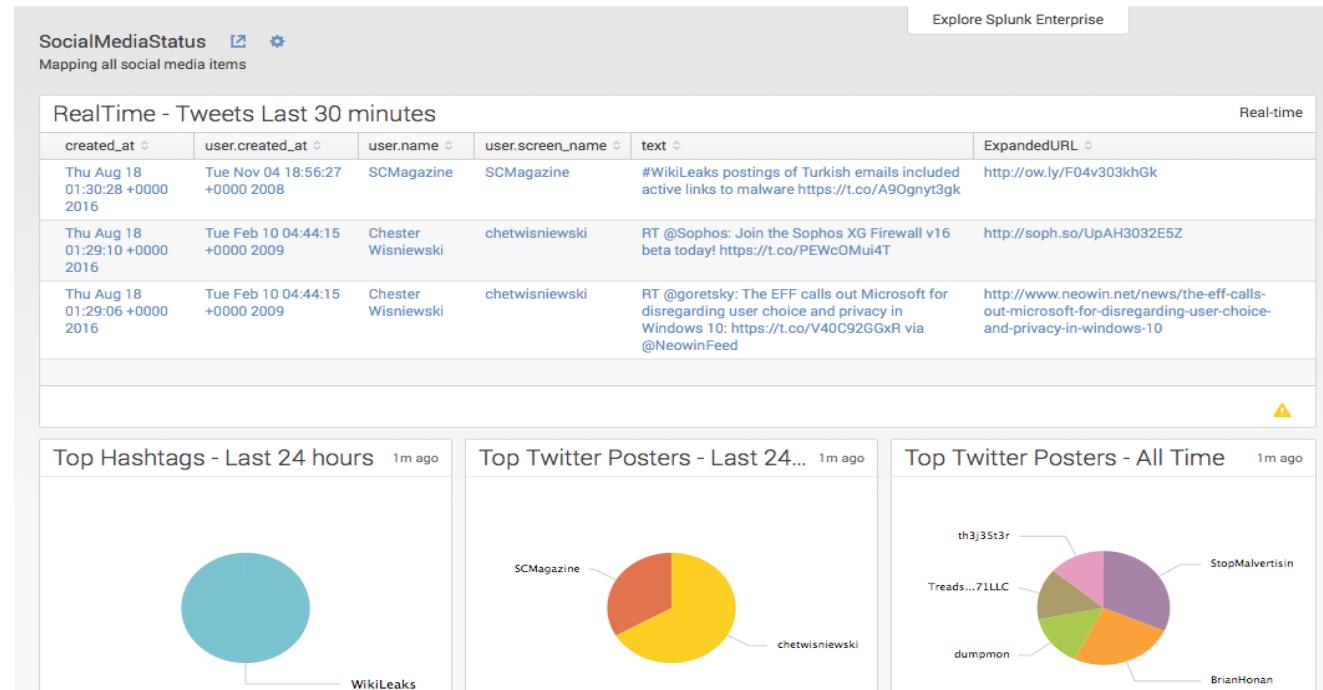
Future – Social Media Dashboard

Quick Stats

- Useful for Profile/ brand status and awareness

Example Content

- **Last 30 minutes of tweets**
- **Last 24 Hours**
 - Top Hashtags
 - Top Posters
- **All Time**
 - Top Poster



Enhanced Splunk Visualization

- **What is D3?**

D3 (Data-Driven Documents or D3.js) is a JavaScript library for visualizing data using web standards.

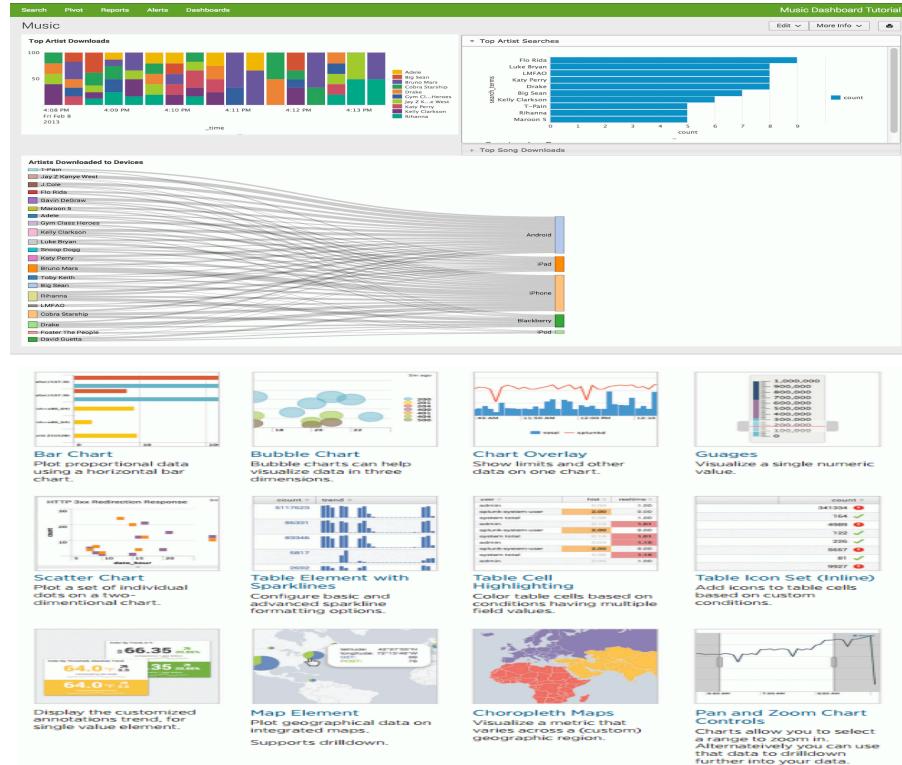
- **How does Splunk use this?**

- To make really cool visualizations!
- Detailed discussion

Splunk conf2014 - Splunk for Data Science

- **Experiment on your own Splunk Apps**

- The Web Framework (1613)
- D3 Extension (2856)



External Examples

- **Maltego**

- A rich link analysis platform that handles data from multiple sources including Splunk and external API's
- Great tool to map out campaigns or visualize disparate data into relationships
- Cheap!
Home: <http://www.paterva.com>

- **Successful uses of Splunk and Maltego**

- Example 1 – Bad Guys who Share infrastructure
- Example 2 - Those Random cases can't be related?
- Example 3 – When Phishers show their hand

External Examples

.conf2016

splunk>

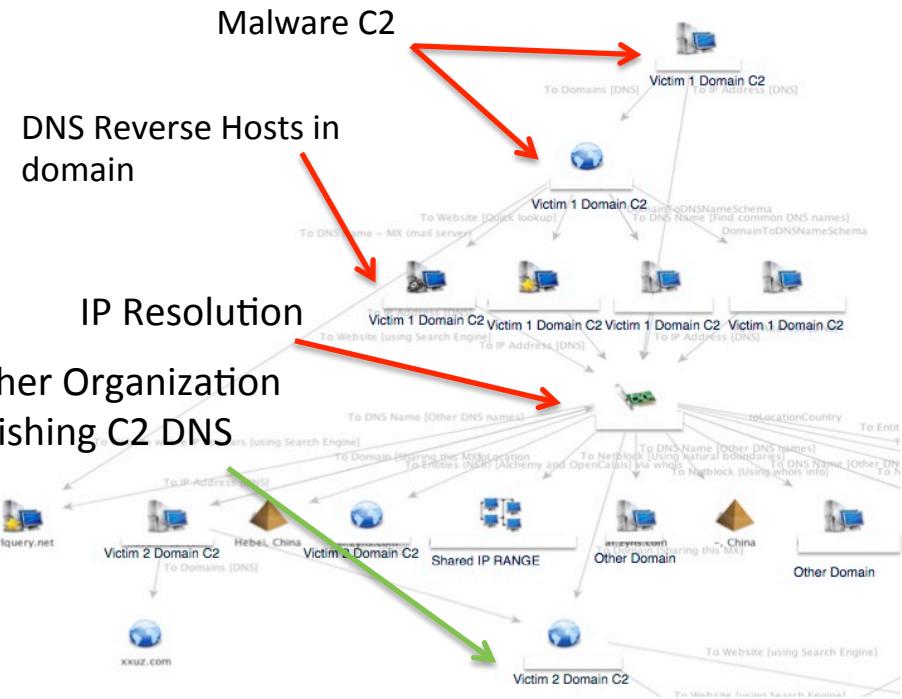
Example 1 – Bad Guys who Share infrastructure

Goal:

- Determine if targeted malware communications (C2 traffic) from one victim site has any associations to other attacks.

Discovered:

- Malware shared network infrastructure for multiple attacks
- Found a newly created Domain that indicated another victim. Contacted their security team and discovered they were just starting an investigation into a spear phishing campaign that was launched earlier in the day!



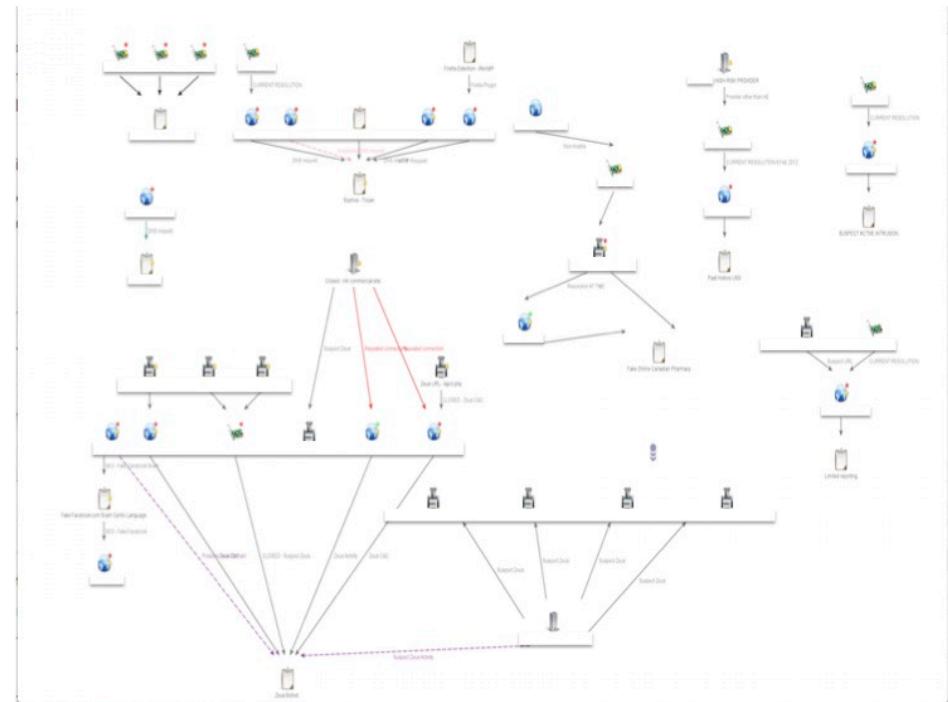
Example 2 - Those Random cases can't be related?

Goal:

- Take a random sample of IP's and Domain names, and hashes to see if anything is related

Discovered:

- Of the sample set
 - 8 of the indicators were related to the same Zeus Family of Malware
 - 1 Cyrillic language Fake Facebook login (only worked from EU IP's)
 - 1 Fake Canadian Pharmacy Scam (PII stealing malware)
 - 1 Active intrusion with C2 information to a US Military site



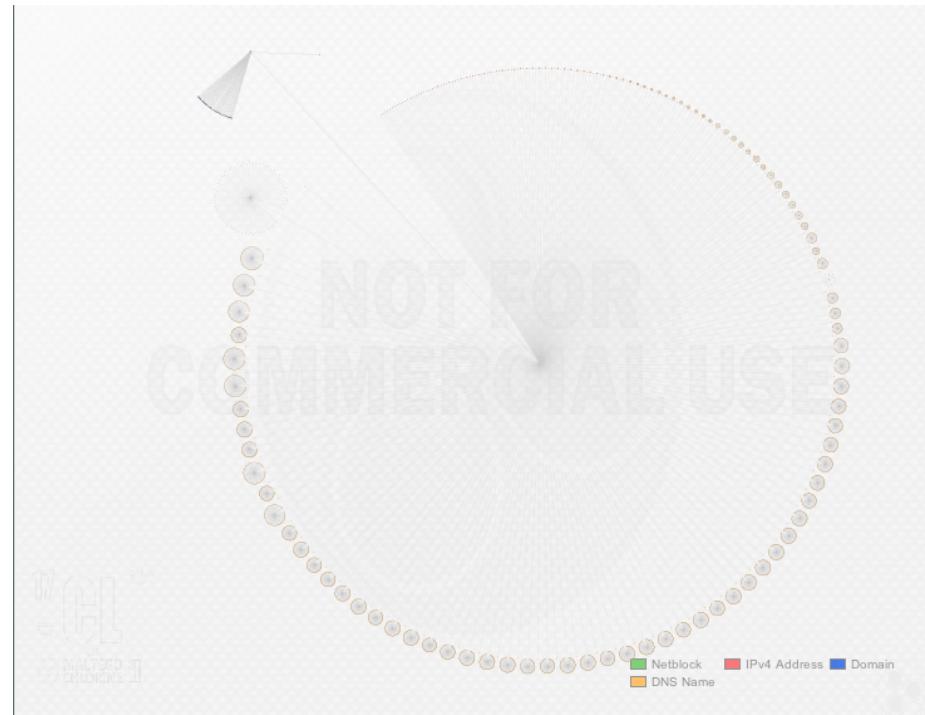
Example 3 – When Phishers show their hand

Goal:

- Investigate source of Spam email (originating sender)
- DNS name: mail.atlanticrisk.com

Discovered:

- Hosted server in the Cayman Islands
- DNS resolutions showed several thousand Domains being parked on this server.
- Including several faked Banking scams (BoA, WF, HSBC, and more)
- Joy for us the phishers had only placed the files there.
- Visible was still the C2's and email templates for the phish campaign.
- Turned over all domains for Blocking, Shared the phishing campaign details with several Banks and handed over the Server information for takedown.



Conclusions

- Visualization can help play a key role in cyber events
- Splunk has wide variety of options that can help an organization, a security, and even an analyst to visualize, enrich, and present data.
- Combining these into data enables faster, and more accurate identification of threats and attack(s/ers)
- More work can be done to improve or provide additional solutions.
- Creativity is your only limit.

What Now?

Any other questions?

Later today

Crypsis Meet and Greet

WHERE: Dolphin Resort - Todd English's bluezoo

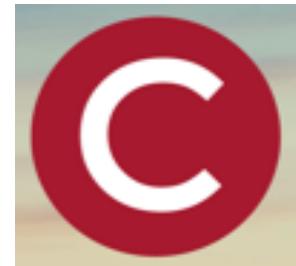
WHEN: 5:00 to 7:00

Questions/Comments?

Jake Babbin

jake.babbin@crypsisgroup.com

The Crypsis Group



THANK YOU

.conf2016

splunk®