.conf2015

Turning Indicators of Compromise into Tangible Protection

Katie Winslow

Sr. Manager, Kaiser Permanente

Mike Slavick

Lead Cyber Threat Intel, Kaiser Permanente

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 the 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.

> “It is by comparing a variety of information, we are frequently enabled to investigate facts, which were so intricate or hidden, that no single clue could have lead to the knowledge of them.”
>
> *- George Washington*

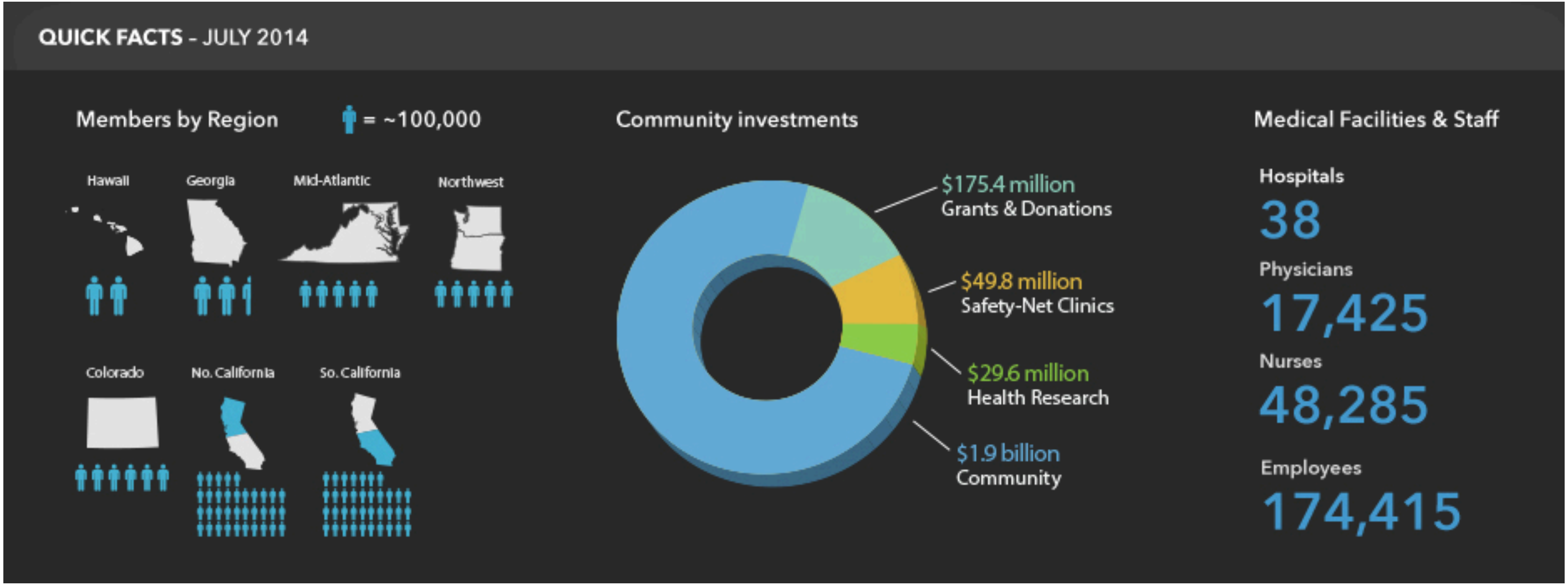
Personal Introduction

- Katie Winslow, Kaiser Permanente
- Sr. Manager, Threat Management and Governance

- Mike Slavick, Kaiser Permanente
- Lead Cyber Threat Intelligence

About Kaiser Permanente

KAISER PERMANENTE®



QUICK FACTS - JULY 2014

Members by Region = ~100,000

Community investments

$175.4 million Grants & Donations

$49.8 million Safety-Net Clinics

$29.6 million Health Research

$1.9 billion Community

Medical Facilities & Staff

Hospitals	38
Physicians	17,425
Nurses	48,285
Employees	174,415

10 Million Members and Growing!

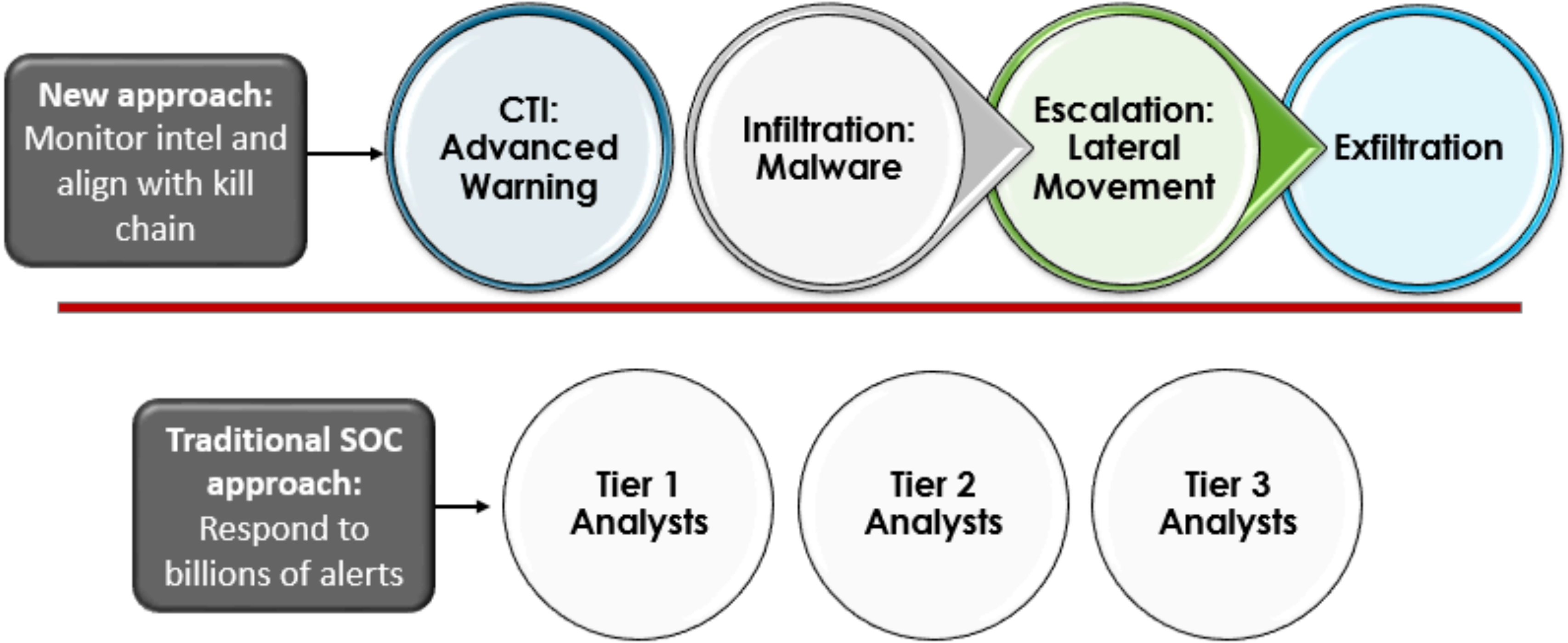
Healthcare is a Primary Target

Company Name	Breach Date	Records Lost
CHS Community Health Systems	August 2014	4.5M
Anthem	February 2015	80M
PREMERA BLUE CROSS	March 2015	11M
UCLA Health	July 2015	4.5M

👤 = 1M records

Healthcare Data is Valuable and Marketable

Cyber Risk Defense Center



New approach: Monitor intel and align with kill chain

CTI: Advanced Warning

Infiltration: Malware

Escalation: Lateral Movement

Exfiltration

Traditional SOC approach: Respond to billions of alerts

Tier 1 Analysts

Tier 2 Analysts

Tier 3 Analysts

Advanced Warning: Cyber Threat Intelligence

Input: Threat Data Sources

- 3 Letter Agencies
- Relationships
- Vendor Subscriptions
- ISACs

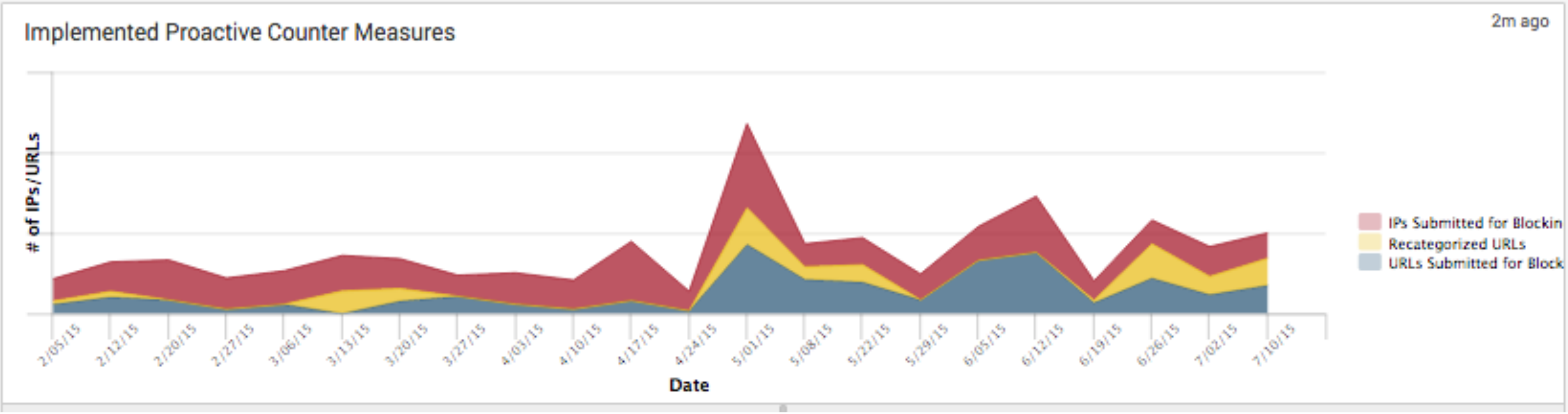
CTI: Advanced Warning

Output: Actionable Intelligence

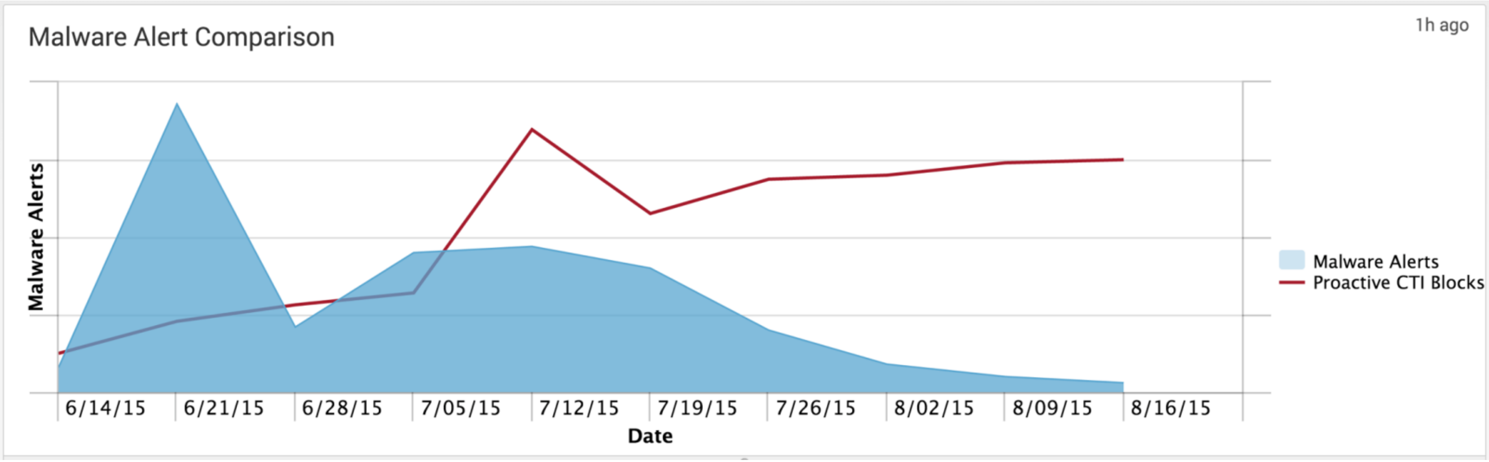
- Malicious IP / URLs Blocked
- Compromised Credentials Remediated
- Impostor and New Domains Identified

Sharing Threat Data Makes CTI Successful!

Actionable Intelligence



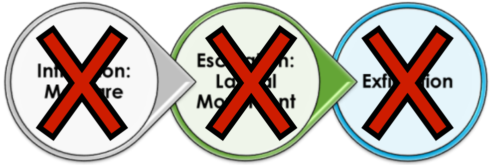
Results – Dramatic Reduction of Malware



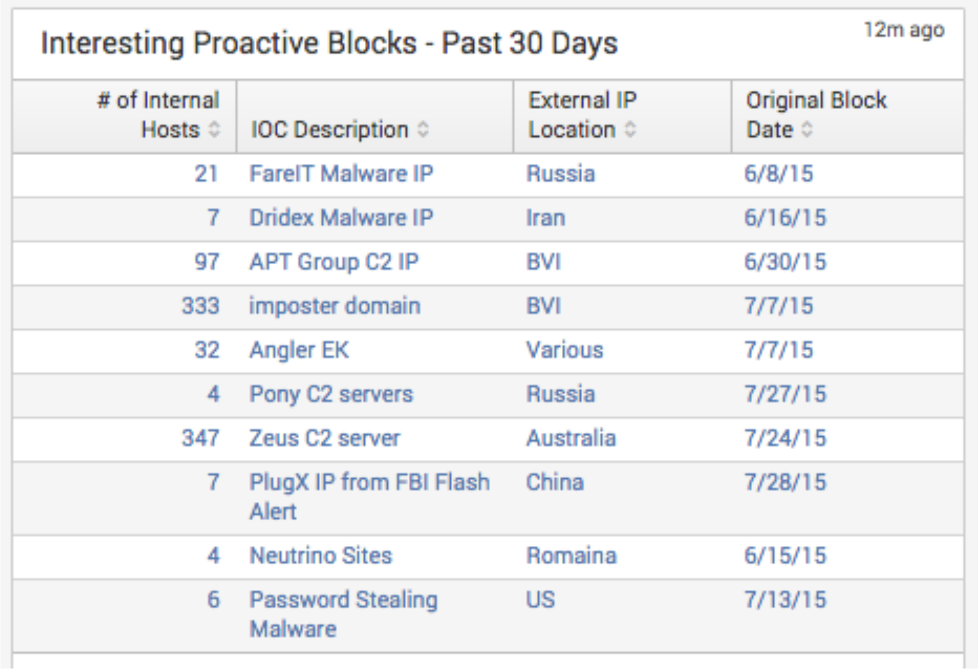
- Users still click on malicious links but 90% of infections are blocked
- Most malware alerts “eliminated” with no impact to user

Intel Driven Results – What Might Have Been…

- Users still led to malicious site
- Approach blocks “downstream” activity



- Allows us to
  - Find compromised accounts/activity
  - Block before infection occurs
  - Identify potential malicious activity



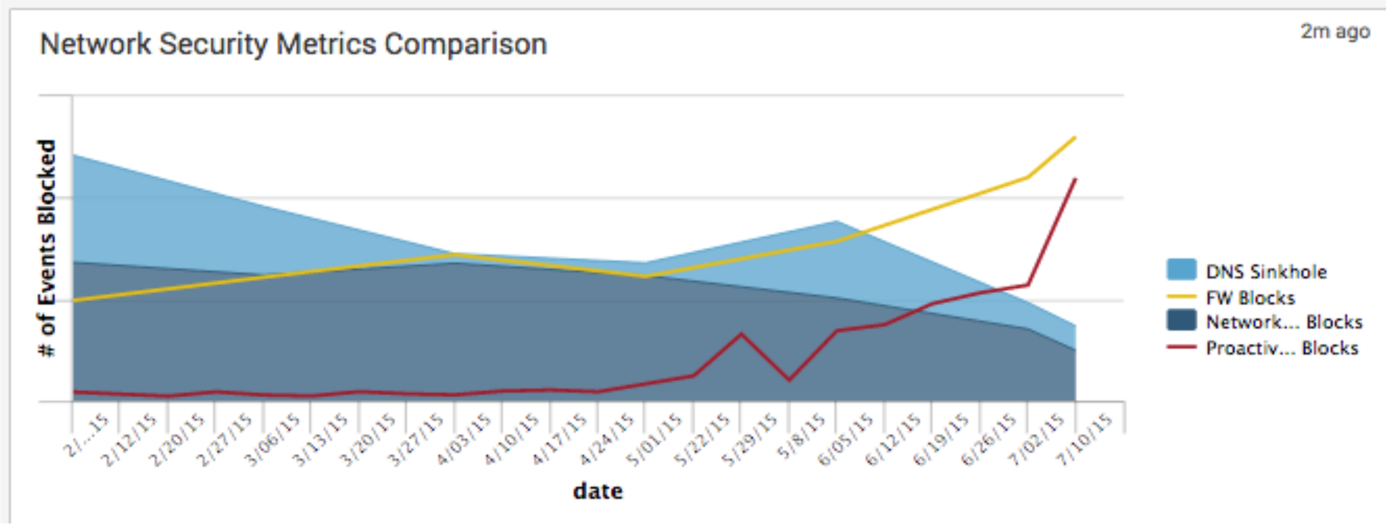
Interesting Proactive Blocks - Past 30 Days

12m ago

# of Internal Hosts	IOC Description	External IP Location	Original Block Date
21	FareIT Malware IP	Russia	6/8/15
7	Dridex Malware IP	Iran	6/16/15
97	APT Group C2 IP	BVI	6/30/15
333	imposter domain	BVI	7/7/15
32	Angler EK	Various	7/7/15
4	Pony C2 servers	Russia	7/27/15
347	Zeus C2 server	Australia	7/24/15
7	PlugX IP from FBI Flash Alert	China	7/28/15
4	Neutrino Sites	Romaina	6/15/15
6	Password Stealing Malware	US	7/13/15

Compromised accounts are inevitable but infections and downstream impact are preventable

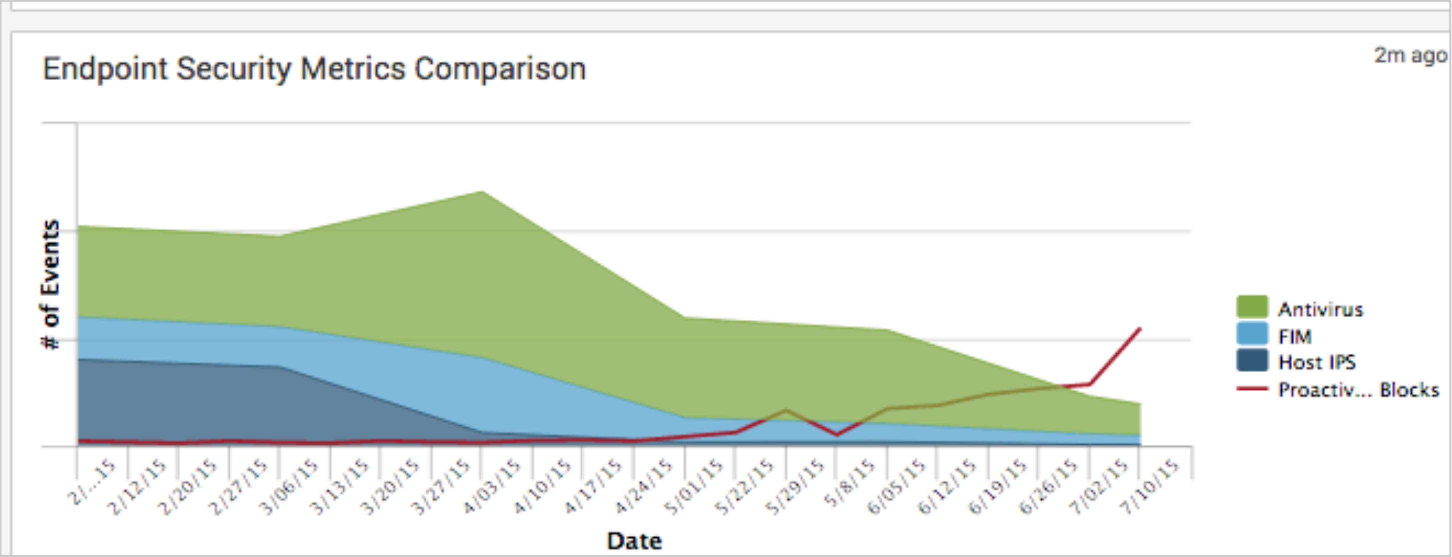
Results – Network Security & Endpoint Security



Reduction in IPS, DNS Sinkhole activity

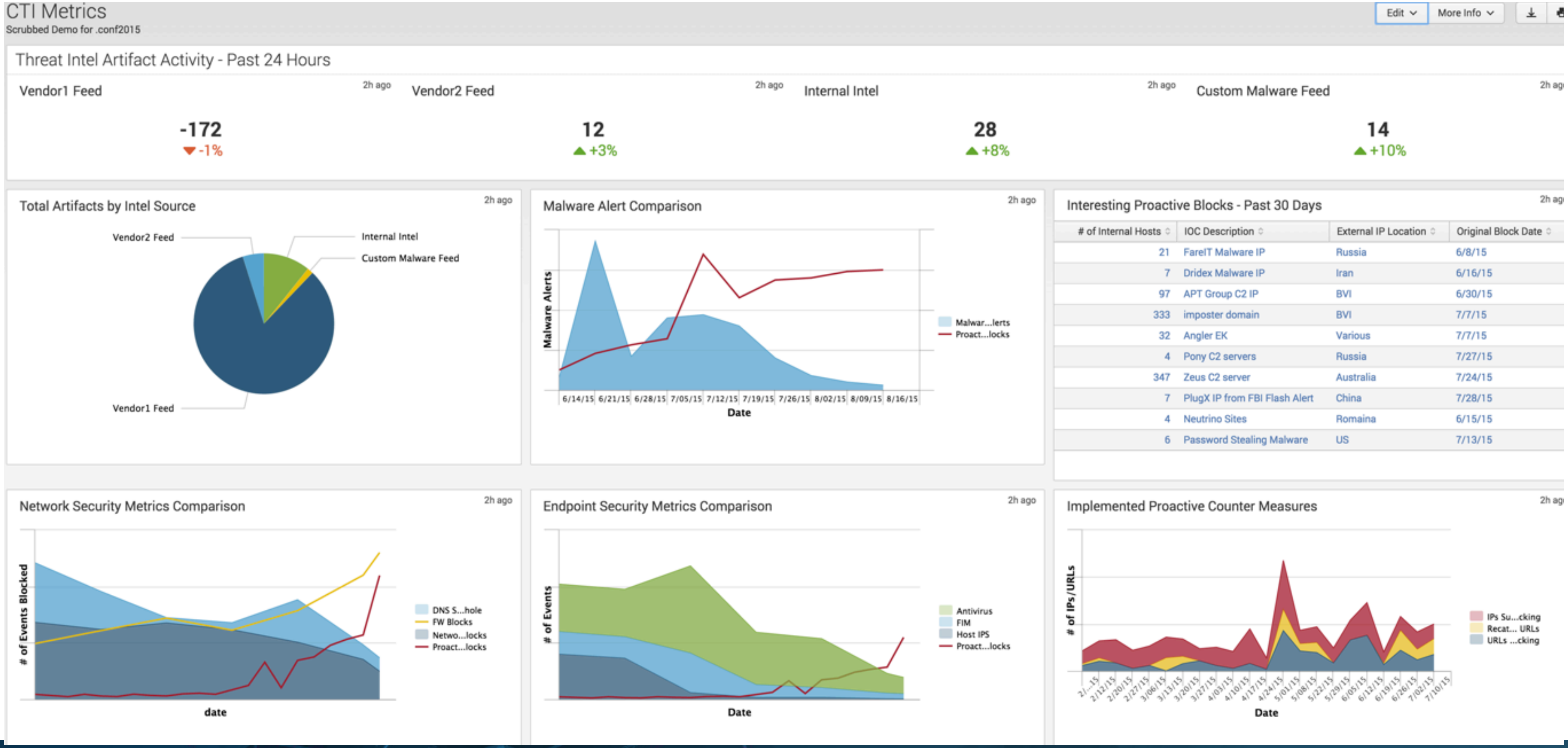
- Less malicious traffic
- Less noise to follow up

Results – Network Security & Endpoint Security



- Significantly less malicious files/activity @ the endpoint
- Less virus and file modification → fewer attackers getting to the endpoint

Shared Visibility



CTI Metrics

Scrubbed Demo for .conf2015

Threat Intel Artifact Activity - Past 24 Hours

Vendor1 Feed (2h ago)	Vendor2 Feed (2h ago)	Internal Intel (2h ago)	Custom Malware Feed (2h ag
-172 ▼ -1%	12 ▲ +3%	28 ▲ +8%	14 ▲ +10%

Total Artifacts by Intel Source (2h ago)

Malware Alert Comparison (2h ago)

Interesting Proactive Blocks - Past 30 Days (2h ag

# of Internal Hosts	IOC Description	External IP Location	Original Block Date
21	FareIT Malware IP	Russia	6/8/15
7	Dridex Malware IP	Iran	6/16/15
97	APT Group C2 IP	BVI	6/30/15
333	imposter domain	BVI	7/7/15
32	Angler EK	Various	7/7/15
4	Pony C2 servers	Russia	7/27/15
347	Zeus C2 server	Australia	7/24/15
7	PlugX IP from FBI Flash Alert	China	7/28/15
4	Neutrino Sites	Romaina	6/15/15
6	Password Stealing Malware	US	7/13/15

Network Security Metrics Comparison (2h ago)

Endpoint Security Metrics Comparison (2h ago)

Implemented Proactive Counter Measures (2h ag

Technology Examples

Now Time for Techy Stuff!

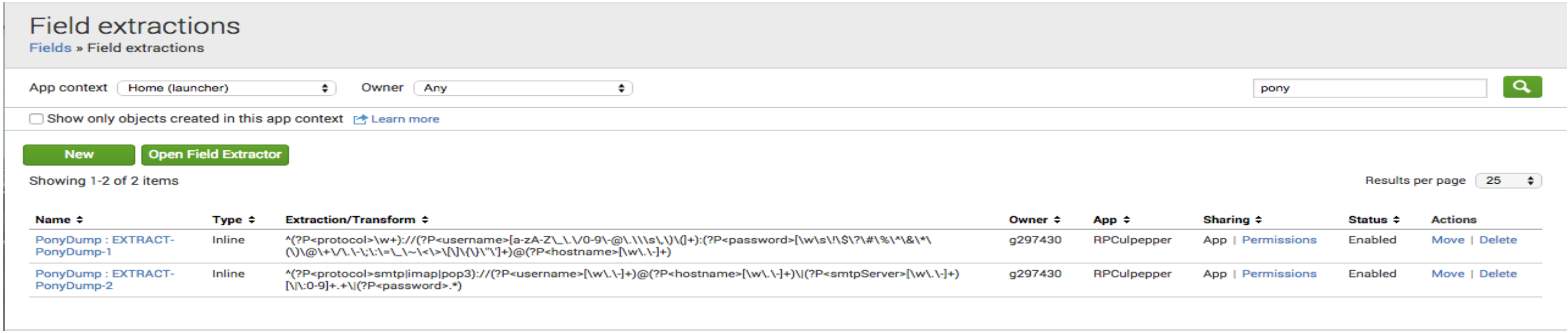
What we're going to talk about:

- Credential dump parsing
- Fun with PCRE!
- Newly created domains

Making Sense of Credential Dumps

- We’ll use a Pony C2 server in this example….

- “https://*REDACTED*@us.ibm.com:*REDACTED*@smc3apps.smc3.com/Login2/Login.asp”



Field extractions

Fields » Field extractions

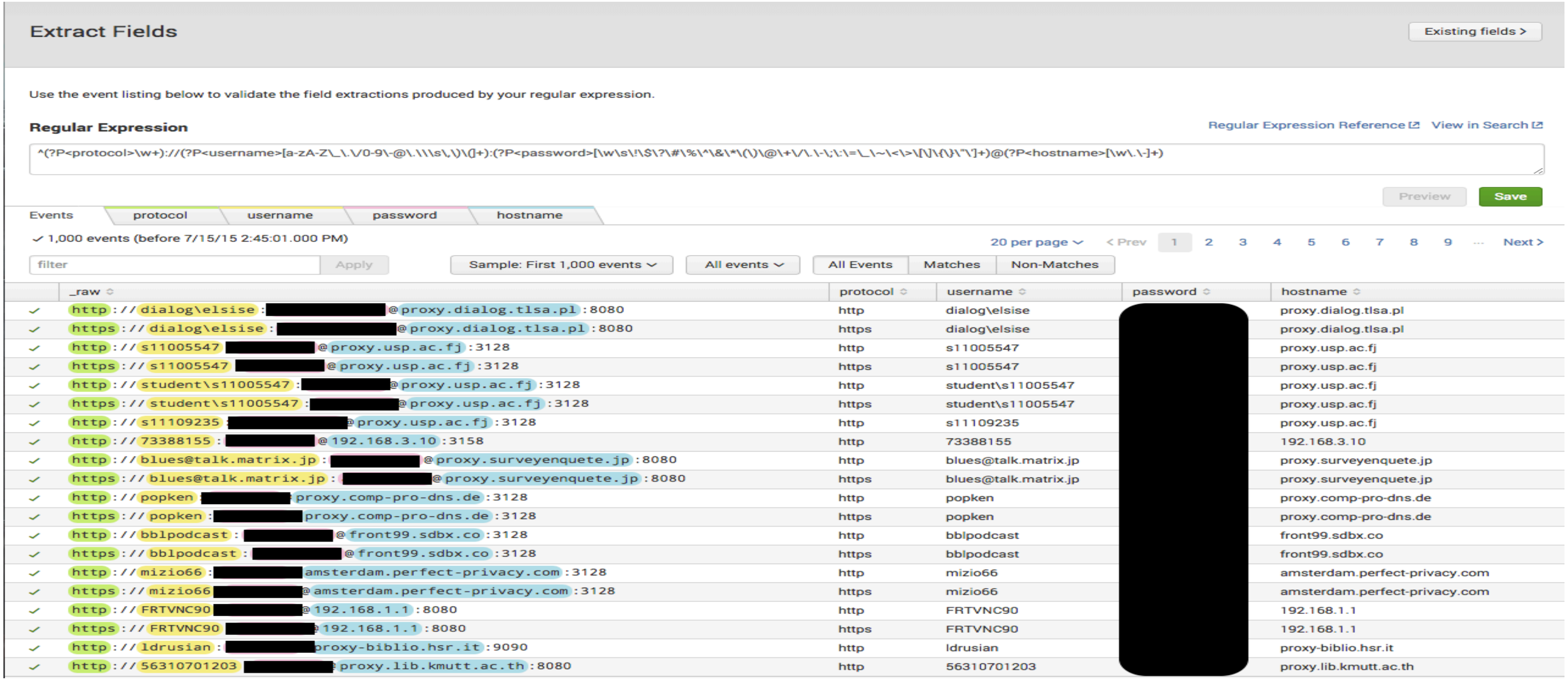
App context: Home (launcher) — Owner: Any — pony

☐ Show only objects created in this app context — Learn more

Showing 1-2 of 2 items — Results per page: 25

Name	Type	Extraction/Transform	Owner	App	Sharing	Status	Actions
PonyDump : EXTRACT-PonyDump-1	Inline	^(?P<protocol>\w+)://(?P<username>[a-zA-Z_\.\/0-9\-@\.\\\s\,\)\(]+):(?P<password>[\w\s\!\$\?\#\%\^\&*\(\)\@\+\/\.\-\;\:\=_\~\<\>\[\]\{\}\"\']+)@(?P<hostname>[\w\.\-]+)	g297430	RPCulpepper	App | Permissions	Enabled	Move | Delete
PonyDump : EXTRACT-PonyDump-2	Inline	^(?P<protocol>smtp|imap|pop3)://(?P<username>[\w\.\-]+)@(?P<hostname>[\w\.\-]+)\\|(?P<smtpServer>[\w\.\-]+)[\\|\:0-9]+.+\\|(?P<password>.*)	g297430	RPCulpepper	App | Permissions	Enabled	Move | Delete

Did the Field Extraction Work?



Use the event listing below to validate the field extractions produced by your regular expression.

Regular Expression

```
^(?P<protocol>\w+)://(?P<username>[a-zA-Z\_\.\/0-9\-@\.\\\s\,\)\(]+):(?P<password>[\w\s\!\$\?\#\%\^\&\*\(\)\@\+\/\.\-\;\:\=\_\~\<\>\[\]\{\}\"\']+)@(?P<hostname>[\w\.\-]+)
```

✓ 1,000 events (before 7/15/15 2:45:01.000 PM)

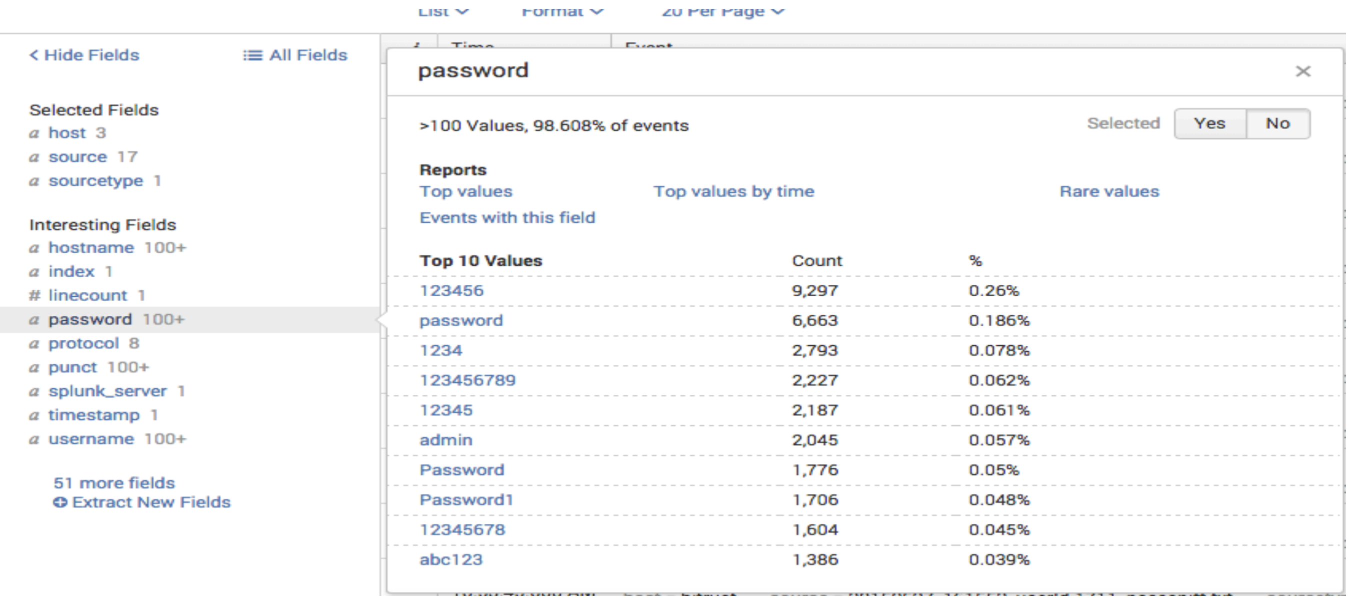
	_raw	protocol	username	password	hostname
✓	http://dialog\elsise:[redacted]@proxy.dialog.tlsa.pl:8080	http	dialog\elsise	[redacted]	proxy.dialog.tlsa.pl
✓	https://dialog\elsise:[redacted]@proxy.dialog.tlsa.pl:8080	https	dialog\elsise	[redacted]	proxy.dialog.tlsa.pl
✓	http://s11005547[redacted]@proxy.usp.ac.fj:3128	http	s11005547	[redacted]	proxy.usp.ac.fj
✓	https://s11005547[redacted]@proxy.usp.ac.fj:3128	https	s11005547	[redacted]	proxy.usp.ac.fj
✓	http://student\s11005547:[redacted]@proxy.usp.ac.fj:3128	http	student\s11005547	[redacted]	proxy.usp.ac.fj
✓	https://student\s11005547:[redacted]@proxy.usp.ac.fj:3128	https	student\s11005547	[redacted]	proxy.usp.ac.fj
✓	http://s11109235[redacted]@proxy.usp.ac.fj:3128	http	s11109235	[redacted]	proxy.usp.ac.fj
✓	http://73388155:[redacted]@192.168.3.10:3158	http	73388155	[redacted]	192.168.3.10
✓	http://blues@talk.matrix.jp:[redacted]@proxy.surveyenquete.jp:8080	http	blues@talk.matrix.jp	[redacted]	proxy.surveyenquete.jp
✓	https://blues@talk.matrix.jp:[redacted]@proxy.surveyenquete.jp:8080	https	blues@talk.matrix.jp	[redacted]	proxy.surveyenquete.jp
✓	http://popken[redacted]proxy.comp-pro-dns.de:3128	http	popken	[redacted]	proxy.comp-pro-dns.de
✓	https://popken:[redacted]proxy.comp-pro-dns.de:3128	https	popken	[redacted]	proxy.comp-pro-dns.de
✓	http://bblpodcast:[redacted]@front99.sdbx.co:3128	http	bblpodcast	[redacted]	front99.sdbx.co
✓	https://bblpodcast:[redacted]@front99.sdbx.co:3128	https	bblpodcast	[redacted]	front99.sdbx.co
✓	http://mizio66:[redacted]amsterdam.perfect-privacy.com:3128	http	mizio66	[redacted]	amsterdam.perfect-privacy.com
✓	https://mizio66[redacted]@amsterdam.perfect-privacy.com:3128	https	mizio66	[redacted]	amsterdam.perfect-privacy.com
✓	http://FRTVNC90[redacted]@192.168.1.1:8080	http	FRTVNC90	[redacted]	192.168.1.1
✓	https://FRTVNC90[redacted]192.168.1.1:8080	https	FRTVNC90	[redacted]	192.168.1.1
✓	http://ldrusian:[redacted]proxy-biblio.hsr.it:9090	http	ldrusian	[redacted]	proxy-biblio.hsr.it
✓	http://56310701203[redacted]proxy.lib.kmutt.ac.th:8080	http	56310701203	[redacted]	proxy.lib.kmutt.ac.th

.conf2015

splunk>

Take Action on All Compromised Credentials

- Search and filter on a list of company domains…
- Share exposed credentials with industry partners….
- Laugh at horrible passwords ☺



Selected Fields
- host 3
- source 17
- sourcetype 1

Interesting Fields
- hostname 100+
- index 1
- linecount 1
- password 100+
- protocol 8
- punct 100+
- splunk_server 1
- timestamp 1
- username 100+

51 more fields
Extract New Fields

password

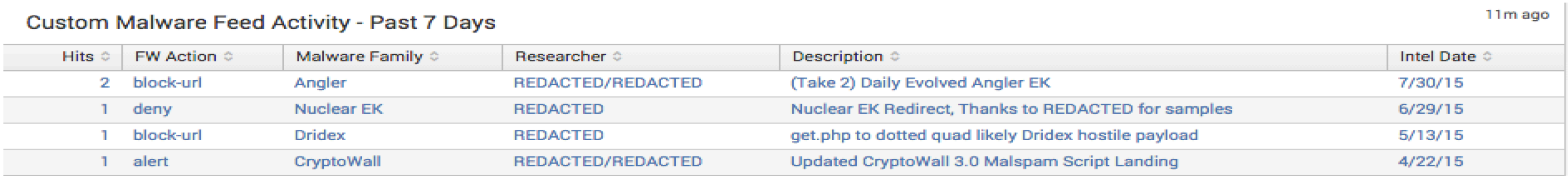
>100 Values, 98.608% of events

Reports
Top values
Top values by time
Rare values
Events with this field

Top 10 Values	Count	%
123456	9,297	0.26%
password	6,663	0.186%
1234	2,793	0.078%
123456789	2,227	0.062%
12345	2,187	0.061%
admin	2,045	0.057%
Password	1,776	0.05%
Password1	1,706	0.048%
12345678	1,604	0.045%
abc123	1,386	0.039%

Fun with PCRE!

- Using PCRE expressions you can then match these against your proxy logs to find evil!
- ^http:\/\/[^\x3f]+\/search\.php\?keywords=[0-9a-z&]+&fid\[?0\]?=[0-9a-z]+$
- REDACTED/REDACTED/REDACTED, 2015-07-27, Angler EK evolved redirect



Custom Malware Feed Activity - Past 7 Days

11m ago

Hits	FW Action	Malware Family	Researcher	Description	Intel Date
2	block-url	Angler	REDACTED/REDACTED	(Take 2) Daily Evolved Angler EK	7/30/15
1	deny	Nuclear EK	REDACTED	Nuclear EK Redirect, Thanks to REDACTED for samples	6/29/15
1	block-url	Dridex	REDACTED	get.php to dotted quad likely Dridex hostile payload	5/13/15
1	alert	CryptoWall	REDACTED/REDACTED	Updated CryptoWall 3.0 Malspam Script Landing	4/22/15

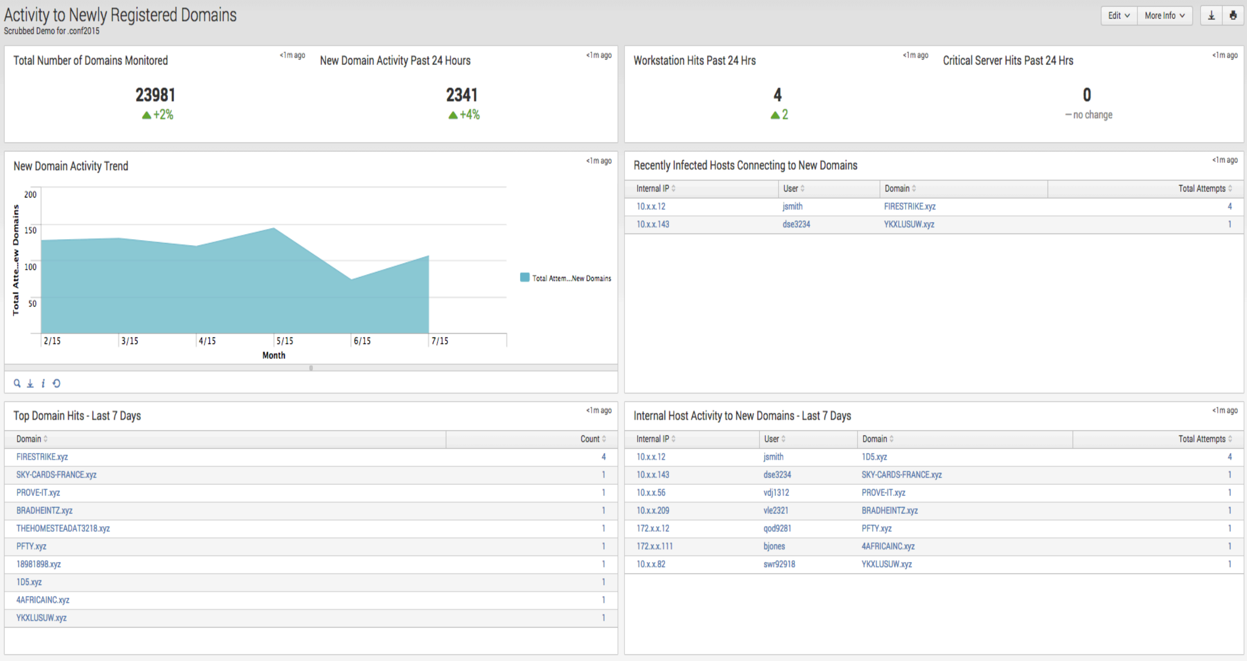
Special thanks to Packetmail!

Newly Created Domain Shenanigans

New Domains

Research

WIN!



Activity to Newly Registered Domains

Scrubbed Demo for .conf2015

Total Number of Domains Monitored

23981

▲+2%

New Domain Activity Past 24 Hours

2341

▲+4%

Workstation Hits Past 24 Hrs

4

▲2

Critical Server Hits Past 24 Hrs

0

— no change

New Domain Activity Trend

Recently Infected Hosts Connecting to New Domains

Internal IP	User	Domain	Total Attempts
10.x.x.12	jsmith	FIRESTRIKE.xyz	4
10.x.x.143	dse3234	YKXLUSUW.xyz	1

Top Domain Hits - Last 7 Days

Domain	Count
FIRESTRIKE.xyz	4
SKY-CARDS-FRANCE.xyz	1
PROVE-IT.xyz	1
BRADHEINTZ.xyz	1
THEHOMESTEADAT3218.xyz	1
PFTY.xyz	1
18981898.xyz	1
1D5.xyz	1
4AFRICAINC.xyz	1
YKXLUSUW.xyz	1

Internal Host Activity to New Domains - Last 7 Days

Internal IP	User	Domain	Total Attempts
10.x.x.12	jsmith	1D5.xyz	4
10.x.x.143	dse3234	SKY-CARDS-FRANCE.xyz	1
10.x.x.56	vdj1312	PROVE-IT.xyz	1
10.x.x.209	vle2321	BRADHEINTZ.xyz	1
172.x.x.12	qod9281	PFTY.xyz	1
172.x.x.111	bjones	4AFRICAINC.xyz	1
10.x.x.82	swr92918	YKXLUSUW.xyz	1

Takeaways

- Integrate CTI with your SOC
- Not all CTI feeds are created equal
- Smart people to transform information into intelligence
- Collaborate, consolidate data and share value
- **Sharing, Sharing, Sharing!**

Resources

- FS-ISAC https://www.fs-isac.com/
- NH-ISAC http://www.nhisac.org/
- Packetmail PCREs http://www.packetmail.com
- InfraGard https://www.infragard.net

Questions?

.conf2015

THANK YOU!

splunk>