Global Enterprise Security Without Security Analysts…Yes You Can!

Jason Bareiszis

Incident Response Manager

Agenda

- Transition from two former SIEMs to Splunk
- Incident Response Light (IR Light) Program
  - What it is
  - How it is used to offload work from Security Analysts
- IR Light Dashboard examples

Why Splunk?

Challenges then Success with Splunk

Support Model
Online/Phone

- Priority 1 events
- Response times

Search Times

- Search times for events that spanned long periods of time
- Multiple concurrent searches
- Console access

Ease of Use

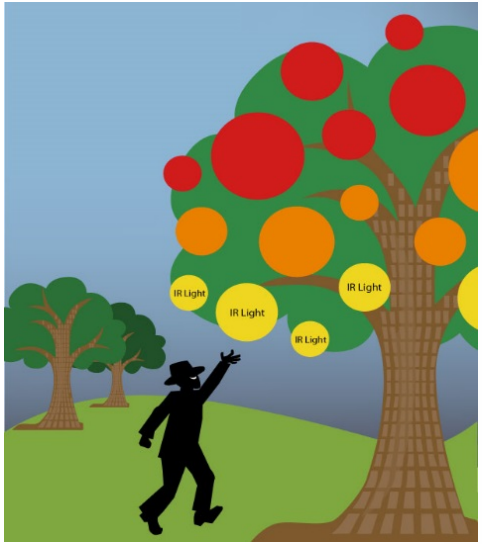
- Acquired taste
- Time to train

Flexibility

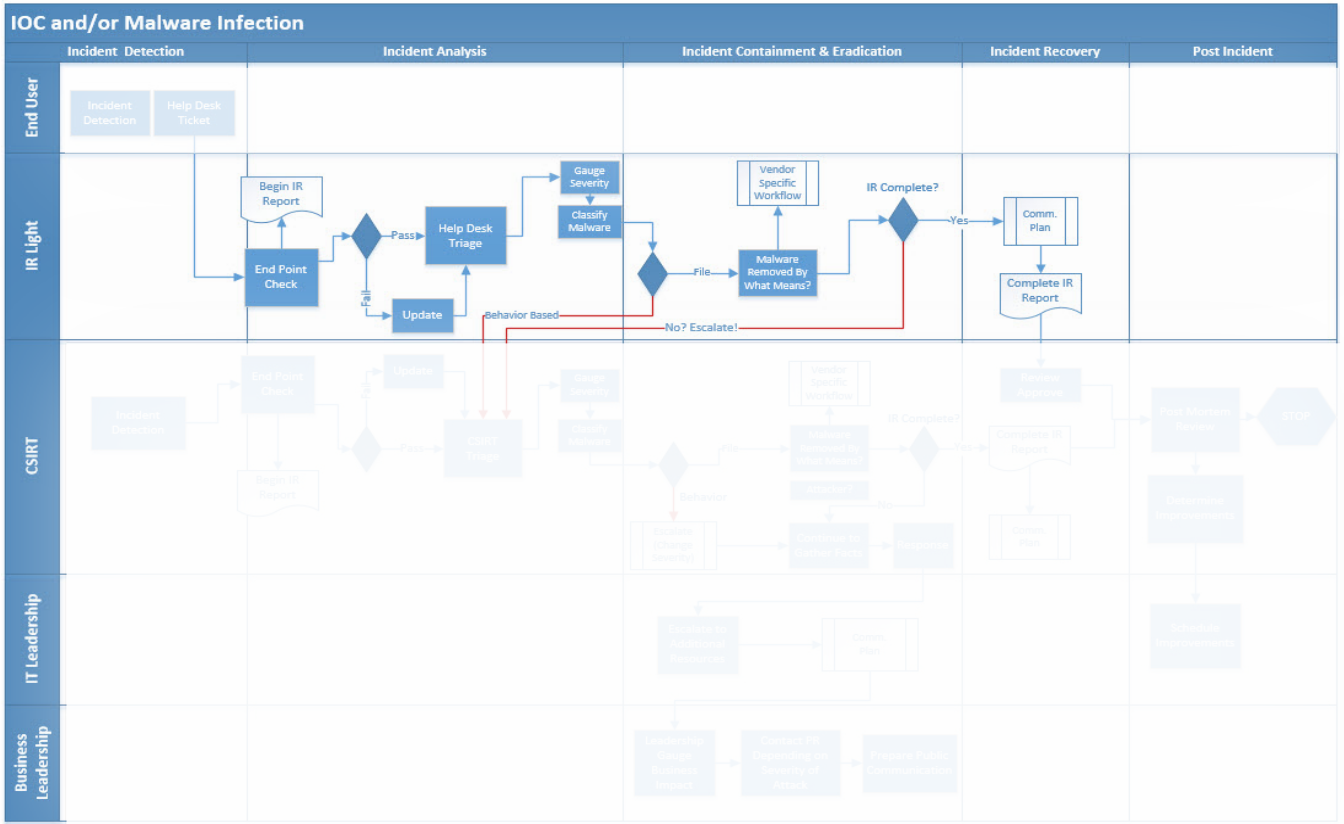
- Accelerate the overall IR process
- IR Light Program

Incident Response Light (IR Light)

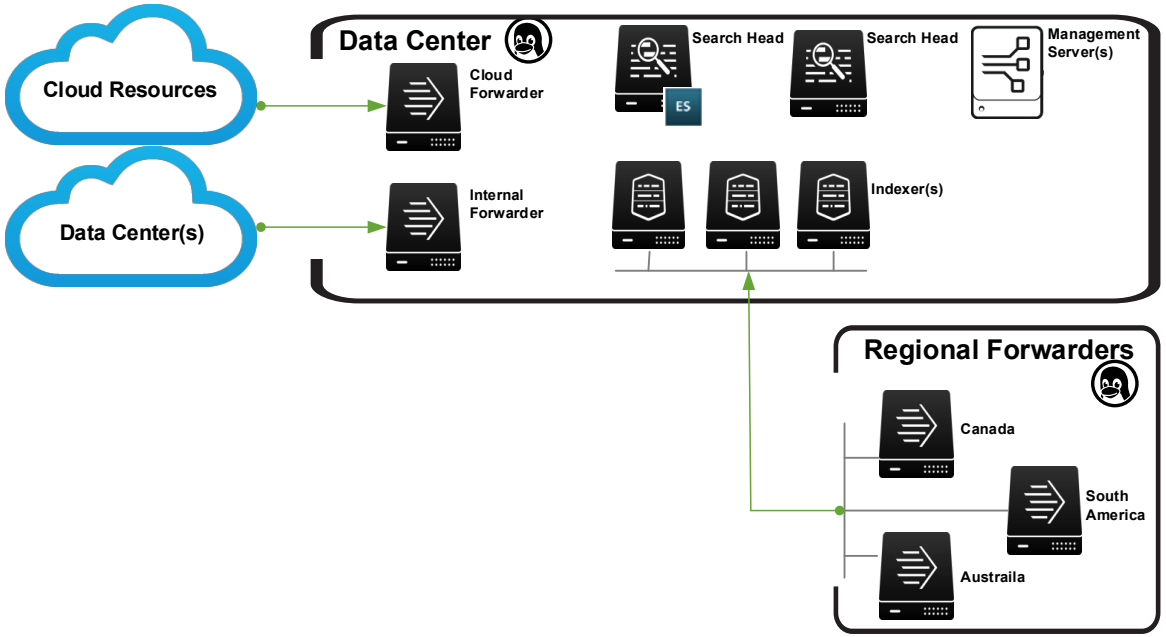
- Help Desk is a very process driven group
- No focus on security



- Phases of traditional IR
- Phases of IR Light



Architecture And Indexes

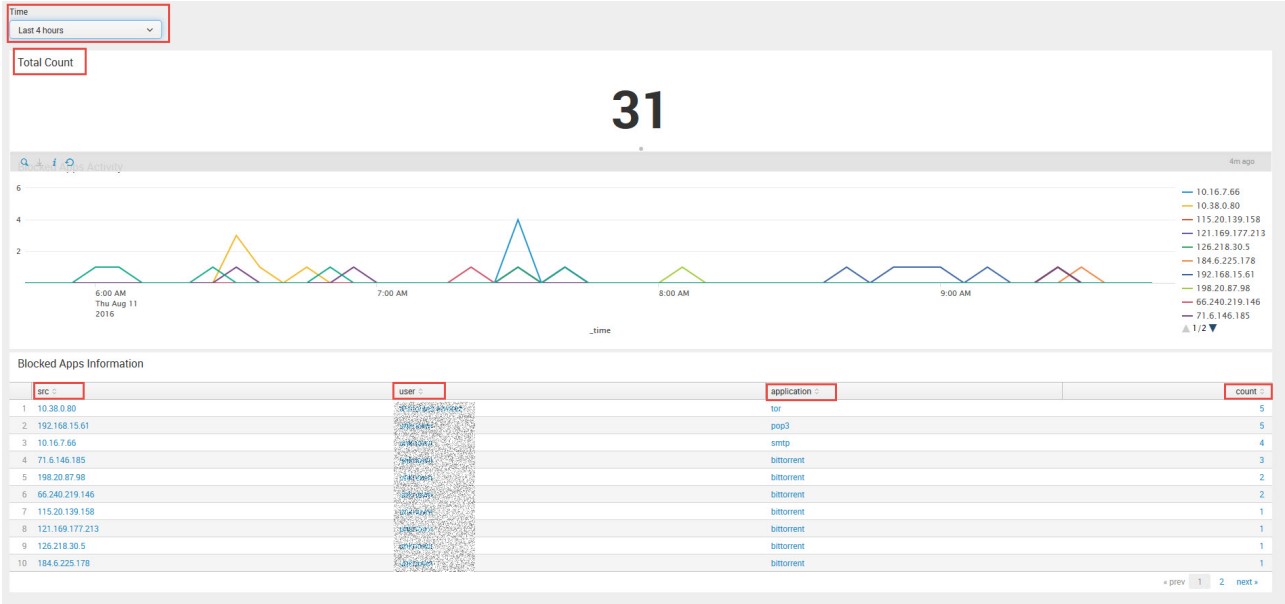


Indexes for IR Light

- Firewall traffic
- EndPoint Security Agents
  - -Cylance Protect
  - -ScanSafe
- Threat Lists
- Active directory

IR Light Dashboard Concept

- Simple, not overly complicated
- Congruent
- Address one specific problem where the activity is “blocked”
- Contain actionable information



Endpoint Security Software Status

Endpoint Check

Endpoint Security Software Status

Edit | More Info

Time: Previous week

Host Name: TTL-9Q80YZ1 Submit

Security Applications Installed

Host	owner	name	version
TTL-9Q80YZ1	jason.bareiszis	Cisco AnyConnect Web Security Module	4.2.01035

Total CylancePROTECT Hosts

14,006

Total CylancePROTECT Hosts

Total ScanSafe Hosts

10,465

Total ScanSafe Hosts

CylancePROTECT Agents Installed

version	count
1.2.1290.17	1094
1.2.1300.29	16
1.2.1330.31	1745
1.2.1360.571	1
1.2.1380.41	2181

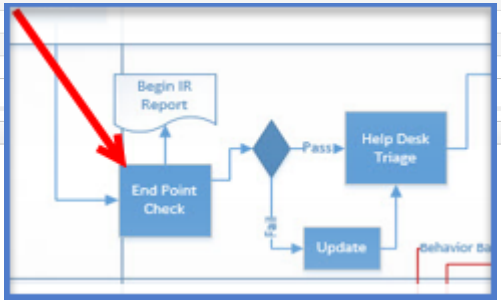
« prev 1 2 next »

ScanSafe Agents Installed

version	count
4.2.04018	25
4.2.03013	1
4.2.01035	9171
4.2.01022	13
3.1.11004	2

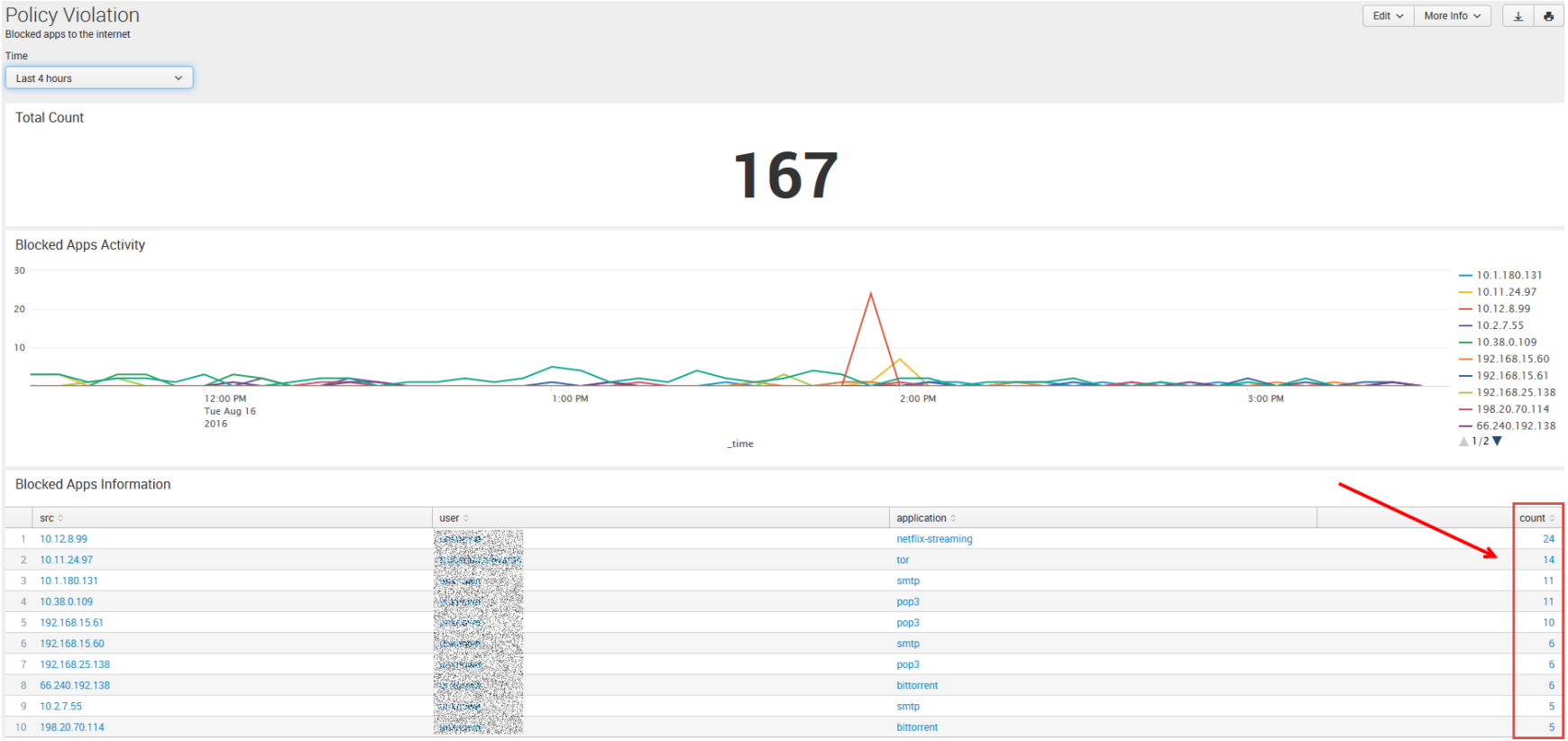
next »

	user_bunit	hosts	owner
1	100 AMC	DIVL-B79GFV1 DIVL-DCNPFS1 TTL-1CR9L72 TTL-2ZVBCW1 TTL-337F262 TTL-4DDML72 TTL-4TVLP12 TTL-4VDJR32 TTL-5HRNJ72 TTL-5V1QJ72 TTL-5Z3NL72 TTL-60QBH72 TTL-60Y5S72 TTL-670DY52	[redacted]



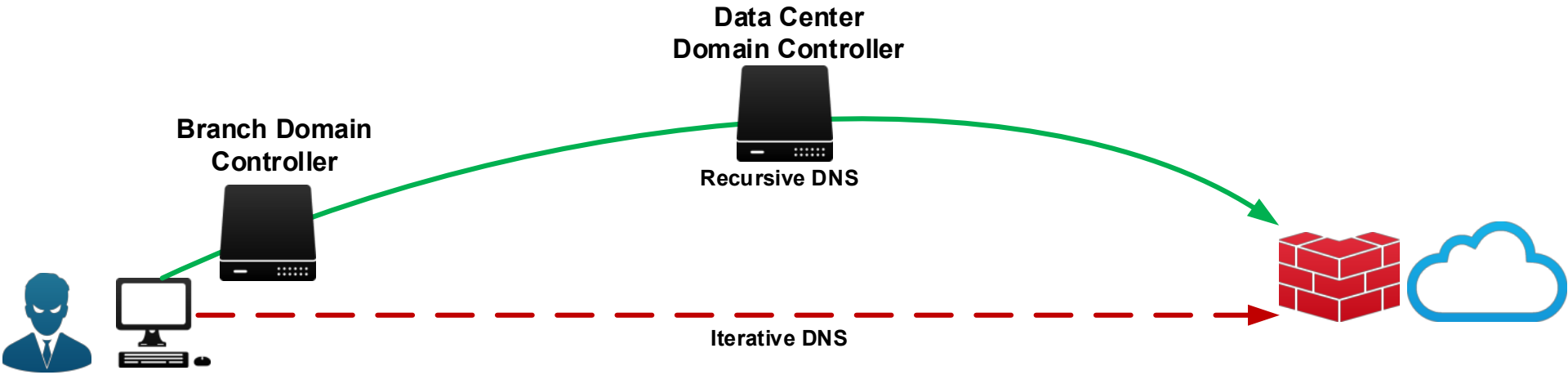
No investigation is currently loaded. Please create (+) or load an existing one (≡).

Policy Violation

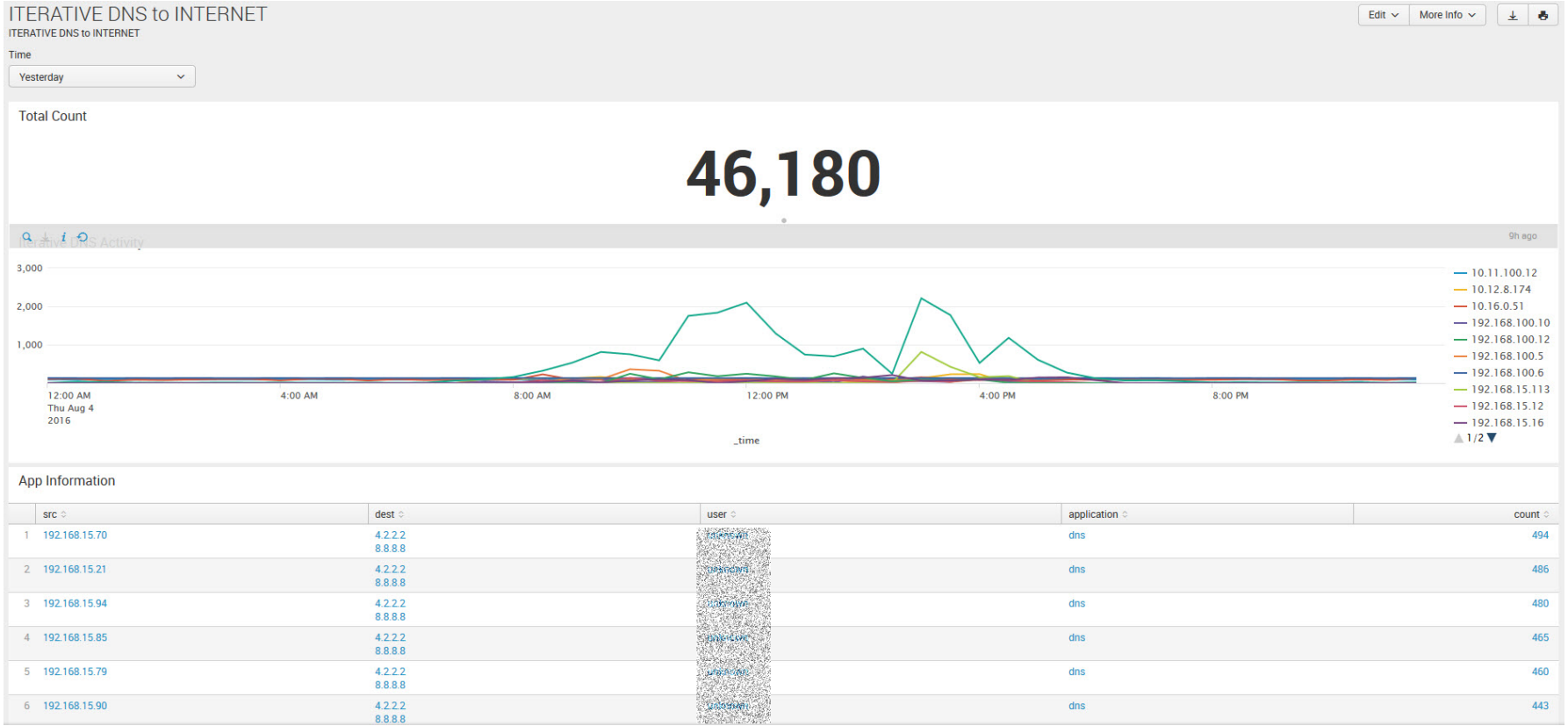


	src	user	application	count
1	10.12.8.99	[redacted]	netflix-streaming	24
2	10.11.24.97	[redacted]	tor	14
3	10.1.180.131	[redacted]	smtp	11
4	10.38.0.109	[redacted]	pop3	11
5	192.168.15.61	[redacted]	pop3	10
6	192.168.15.60	[redacted]	smtp	6
7	192.168.25.138	[redacted]	pop3	6
8	66.240.192.138	[redacted]	bittorrent	6
9	10.2.7.55	[redacted]	smtp	5
10	198.20.70.114	[redacted]	bittorrent	5

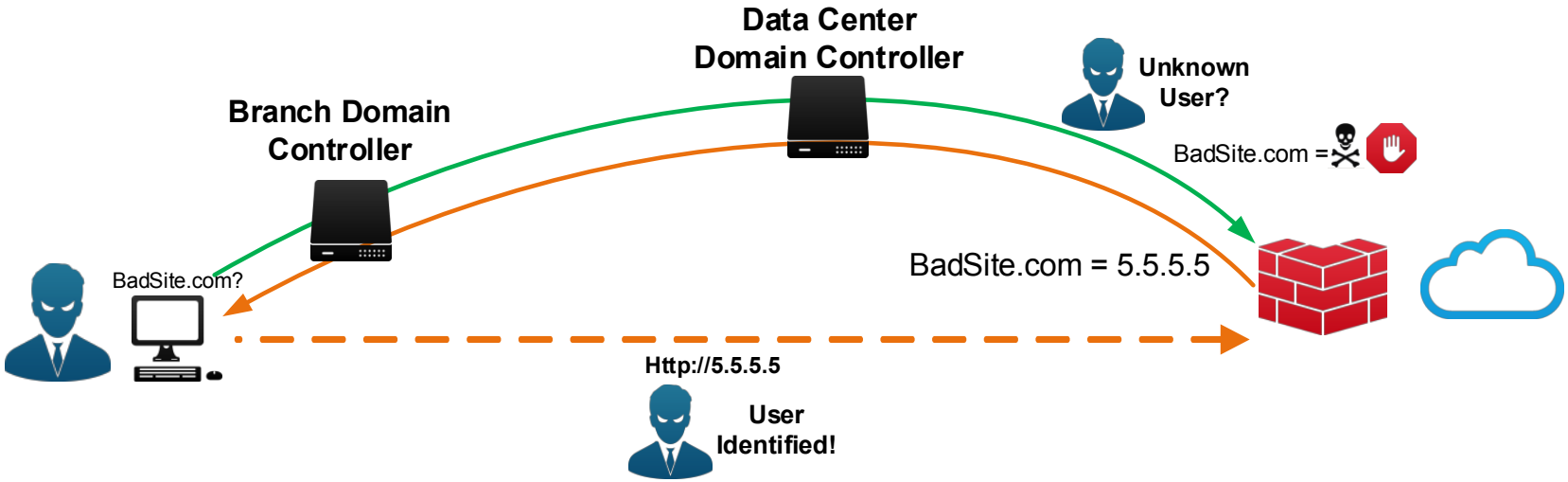
Recursive vs Iterative DNS



Iterative DNS



DNS Sinkhole Explained



DNS Sinkhole

Tetra Tech Sinkhole

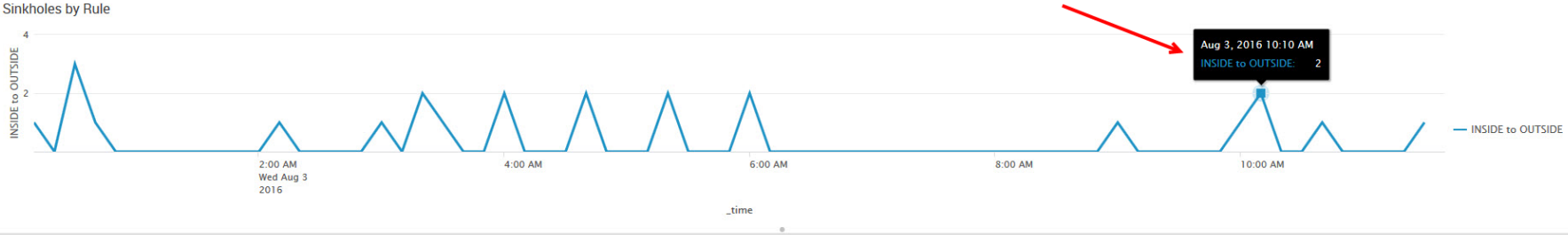
DNS Sinkhole activity

Time

Last 12 hours

Edit | More Info

Sinkholes by Rule



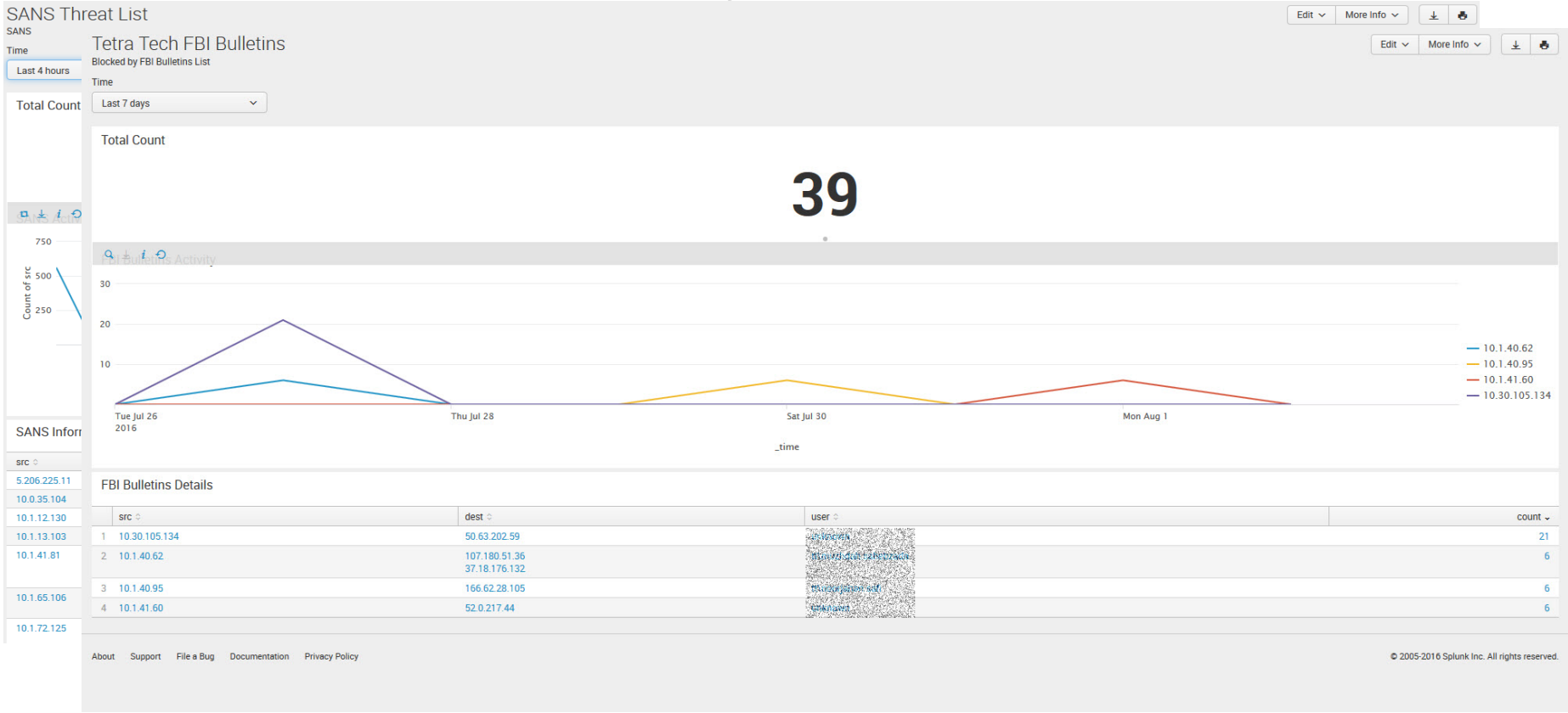
3m ago

	_time	rule	count	values(src_ip)	values(dest_ip)	values(signature)	values(user)	values(dvc)	values(threat_name)
1	2016-08-03 10:05:01	INSIDE to OUTSIDE	1	10.5.1.30	8.8.8.8	DNS Botnet signatures(4012422)	[redacted]	Site000-Texas-Core-HA1	Suspicious DNS Query (generic:pushcodered.com)(4012422)
2	2016-08-03 10:16:02	INSIDE to OUTSIDE	1	10.5.1.32	8.8.8.8	DNS Botnet signatures(4012422)	[redacted]	Site000-Texas-Core-HA1	Suspicious DNS Query (generic:pushcodered.com)(4012422)
3	2016-08-03 10:18:21	INSIDE to OUTSIDE	1	10.5.1.32	8.8.8.8	DNS Botnet signatures(4012422)	[redacted]	Site000-Texas-Core-HA1	Suspicious DNS Query (generic:pushcodered.com)(4012422)

Potential Recursive DNS

	_time	Source IP	Destination IP	PA Device	User	Rule
1	2016-08-03 10:04:58	10.1.40.109	5.5.5.6	Site000-Texas-Core-HA1	[redacted]	Deny All
2	2016-08-03 10:05:01	10.1.40.109	5.5.5.6	Site000-Texas-Core-HA1	[redacted]	Deny All
3	2016-08-03 10:05:07	10.1.40.109	5.5.5.6	Site000-Texas-Core-HA1	[redacted]	Deny All
4	2016-08-03 10:15:56	10.1.40.109	5.5.5.6	Site000-Texas-Core-HA1	[redacted]	Deny All
5	2016-08-03 10:15:59	10.1.40.109	5.5.5.6	Site000-Texas-Core-HA1	[redacted]	Deny All
6	2016-08-03 10:16:05	10.1.40.109	5.5.5.6	Site000-Texas-Core-HA1	[redacted]	Deny All
7	2016-08-03 10:18:15	10.1.40.109	5.5.5.6	Site000-Texas-Core-HA1	[redacted]	Deny All
8	2016-08-03 10:18:18	10.1.40.109	5.5.5.6	Site000-Texas-Core-HA1	[redacted]	Deny All
9	2016-08-03 10:18:24	10.1.40.109	5.5.5.6	Site000-Texas-Core-HA1	[redacted]	Deny All

Third Party Threat List



splunk> .conf2016

Infected Host

Tetra Tech Infected Host Denied

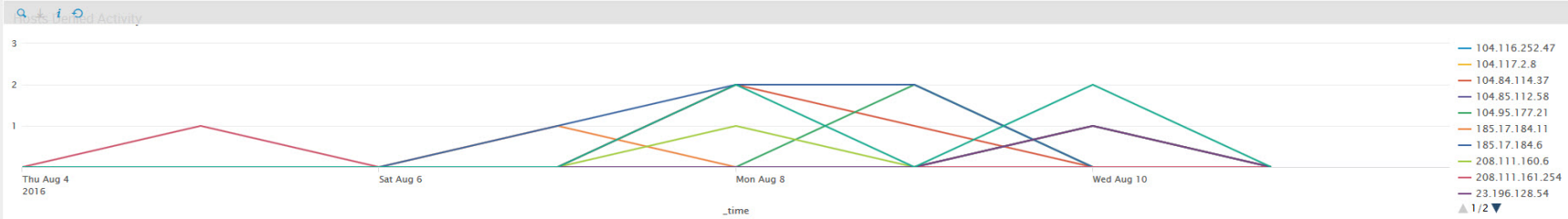
Infected host denied on firewall

Edit | More Info

Time: Last 7 days

Total Count

21



Hosts Denied Details

src	dest	threat name	user	app	count
185.17.184.6	10.2.2.214	Virus/Win32.WGeneric.jjmuo(2586428)	[redacted]	web-browsing	5
104.84.114.37	192.168.100.27 192.168.15.54 192.168.15.90	Trojan/Win32.ramnit.gceeg(2781632) Trojan/Win32.ramnit.gdbzj(2217686)	[redacted]	web-browsing	3
104.95.177.21	192.168.15.57 192.168.15.7	Trojan/Win32.ramnit.gceeg(2781632) Trojan/Win32.ramnit.gdbzj(2217686)	[redacted]	web-browsing	2
104.116.252.47	192.168.15.107	Trojan/Win32.ramnit.gdbzj(2217686)	[redacted]	web-browsing	1
104.117.2.8	192.168.15.52	Trojan/Win32.ramnit.gceeg(2781632)	[redacted]	web-browsing	1
104.85.112.58	192.168.15.68	Trojan/Win32.ramnit.gdbzj(2217686)	[redacted]	web-browsing	1
185.17.184.11	10.2.2.214	Virus/Win32.WGeneric.jjmuo(2586428)	[redacted]	web-browsing	1
208.111.160.6	10.1.40.62	Virus/Win32.WGeneric.jjxhj(2498692)	[redacted]	web-browsing	1
208.111.161.254	10.1.40.109	Virus/Win32.WGeneric.jiuhm(2161001)	[redacted]	web-browsing	1
23.196.128.54	192.168.15.9	Trojan/Win32.ramnit.gdbzj(2217686)	[redacted]	web-browsing	1

Summary

- Is it possible to do Incident Response without analysis... **no**, BUT you can take a big chunk of the work load off of them by using Splunk
- Byproduct – IR Light has become a great mentoring program

Special Thank You

BAI is a group of Solution Architects focused on network monitoring, security, and control. They have spent nearly 40 years working with Fortune 1000 accounts, the Civilian government, the Department of Defense and the Intelligence Community to build and maintain highly secure, reliable, and resilient networks. BAI's goal is not to rip and replace current solutions – it is to help customers evolve in the way they control their networks and in their ability to react and respond to network, application, and security incidents.

Aplura is committed to improving the IT security of organizations by providing expert knowledge and ingenuity to produce solutions tailored to our clients' specific needs. Our measurable results are highlighted by diminished security-related incidents leading to reduced overall client costs. Aplura's staff of credentialed IT security professionals provides our clients information security resources for daily operations as well as project-based expert technical assistance.

THANK YOU

splunk>