Threat Hunting With Splunk

August 16, 2017 | Cincinnati, OH

Lee Imrey | Splunk Security Specialist

splunk> workshop

Agenda

- Threat Hunting Basics
- Threat Hunting Data Sources
- Know Your Endpoint
- Cyber Kill Chain
- Walkthrough of Attack Scenario Using Core Splunk (hands on)
- Advanced Threat Hunting Techniques & Tools
- Enterprise Security Walkthrough
- Applying Machine Learning and Data Science to Security

Hands On? This Won't Work.

Am I in the right place?

Some familiarity with…

- CSIRT/SOC Operations
- General understanding of Threat Intelligence
- General understanding of DNS, Proxy, and Endpoint types of data

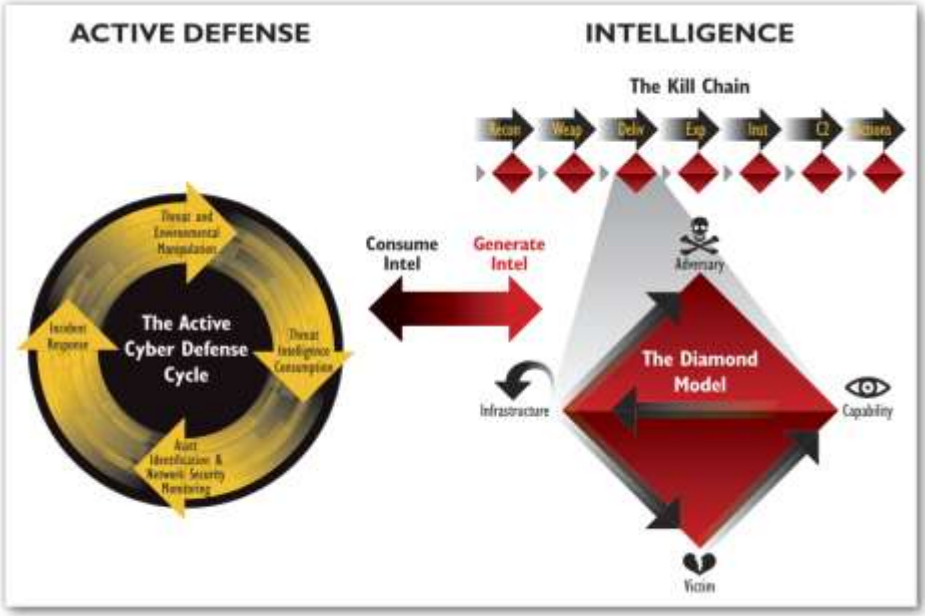
What is Threat Hunting, Why do You Need it?

What?

Threat hunting - the act of aggressively intercepting, tracking and eliminating cyber adversaries as early as possible in the Cyber Kill Chain[2]

Why?

Threats are human. Focused and funded adversaries will not be countered by security boxes on the network alone. Threat hunters are actively searching for threats to prevent or minimize damage [before it happens] [1]



"Threat Hunting is not new, it's just evolving!"

[1] The Who, What, Where, When, Why and How of Effective Threat Hunting, SANS Feb 2016
[2] Cyber Threat Hunting - Samuel Alonso blog, Jan 2016

splunk> workshop

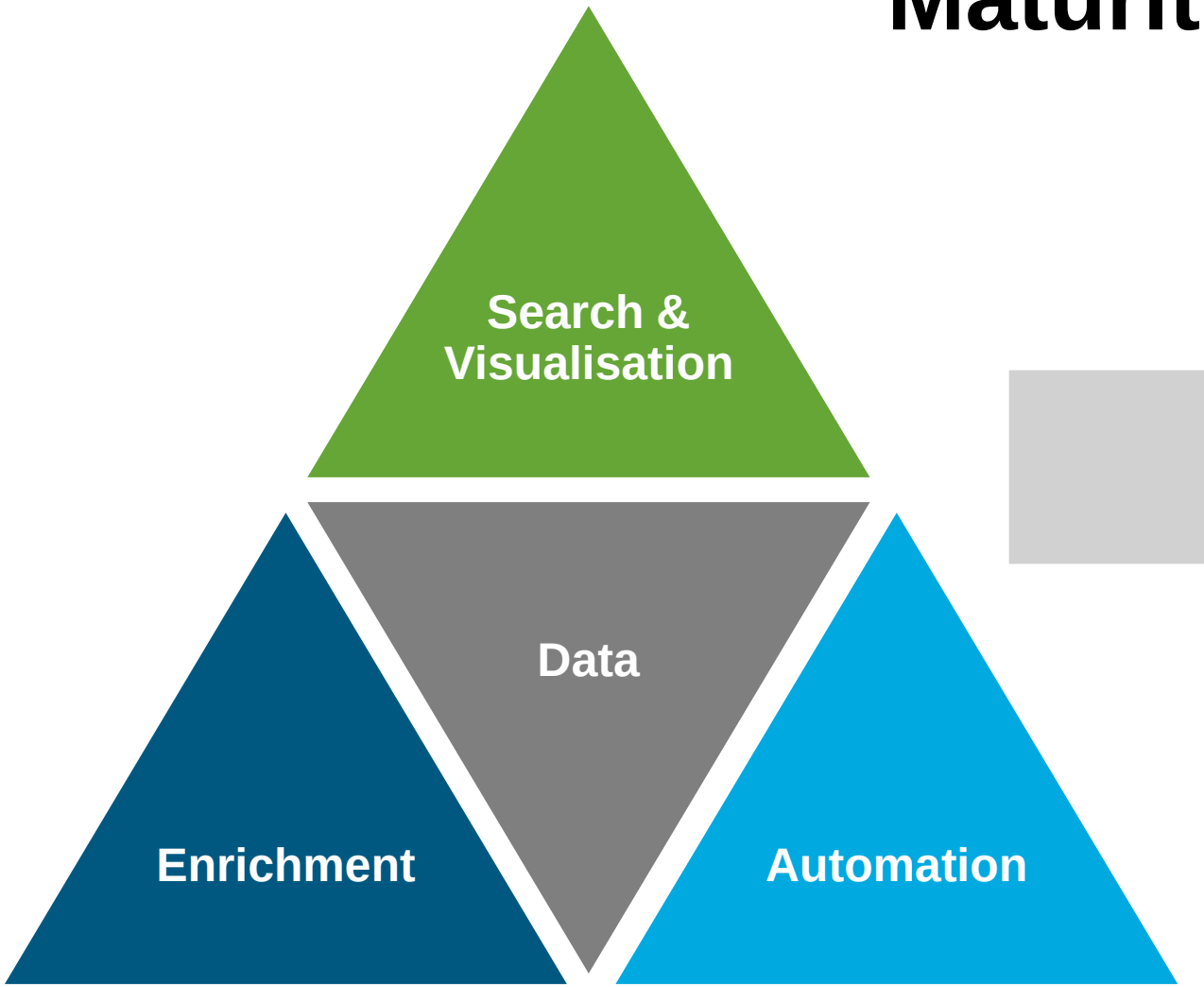
Locard’s Exchange Principle

Threat Hunting With Splunk

VS

splunk> workshop

Key Building Blocks to Drive Threat Hunting Maturity



Objectives > Hypotheses > Expertise

Ref: The Who, What, Where, When, Why and How of Effective Threat Hunting, SANS Feb 2016

splunk> workshop

"A good intelligence officer cultivates an awareness of what he or she does not know. You need a dose of modesty to acknowledge your own ignorance - even more, to seek out your ignorance."

Henry A. Crumpton

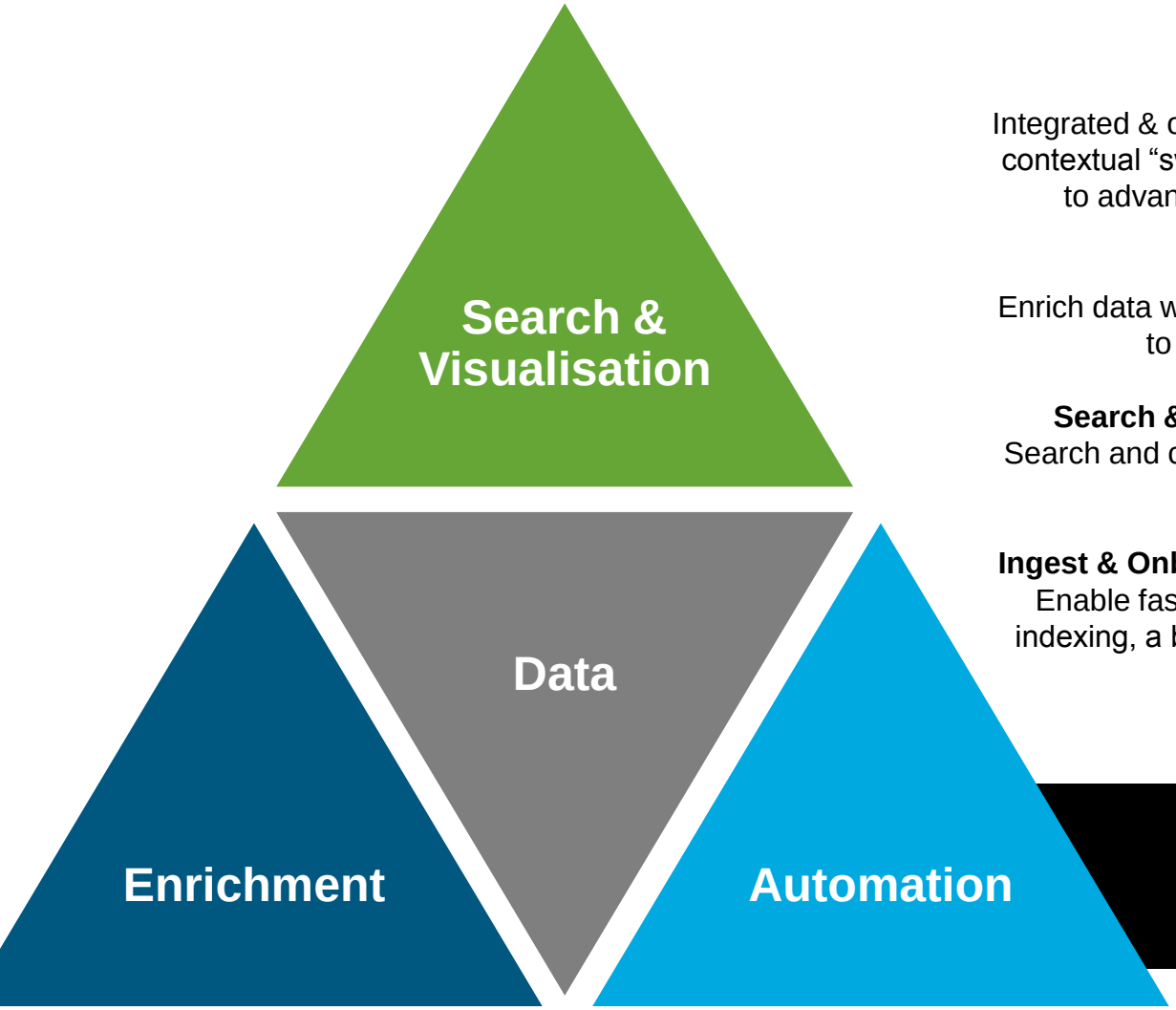
The Art of Intelligence: Lessons From a Life in the CIA's Clandestine Service

SANS Threat Hunting Maturity

Ad Hoc Search | **Statistical Analysis** | **Visualization Techniques** | **Aggregation** | **Machine Learning/ Data Science**

Source: SANS IR & Threat Hunting Summit 2016

How Splunk Helps You Drive Threat Hunting Maturity

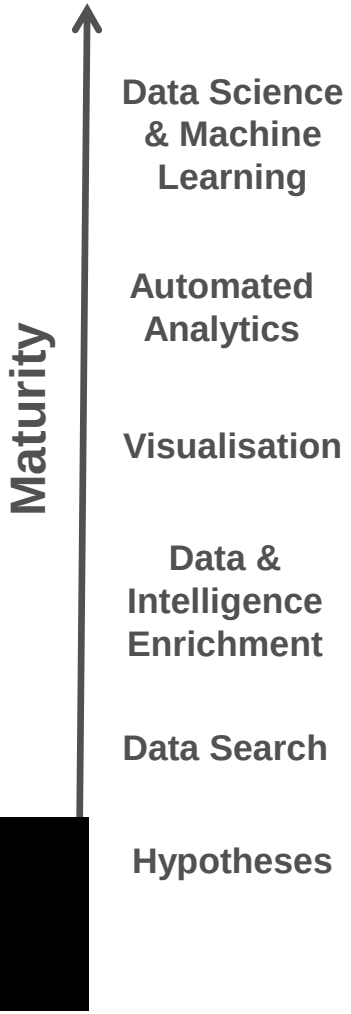


Threat Hunting Automation
Integrated & out of the box automation tooling from artifact query, contextual “swim-lane analysis”, anomaly & time series analysis to advanced data science leveraging machine learning

Threat Hunting Data Enrichment
Enrich data with context and threat-intel across the stack or time to discern deeper patterns or relationships

Search & Visualise Relationships for Faster Hunting
Search and correlate data while visually fusing results for faster context, analysis and insight

Ingest & Onboard Any Threat Hunting Machine Data Source
Enable fast ingestion of any machine data through efficient indexing, a big data real time architecture and ‘schema on the read’ technology



splunk> workshop

Hunting Tools: Internal Data

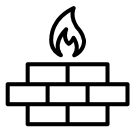
- **IP Addresses:** threat intelligence, blacklist, whitelist, reputation monitoring
  Tools: Firewalls, Proxies, Splunk Stream, Bro, IDS
- **Network Artifacts and Patterns:** network flow, packet capture, active network connections, historic network connections, ports and services
  Tools: Splunk Stream, Bro IDS, FPC, Netflow
- **DNS:** activity, queries and responses, zone transfer activity
  Tools: Splunk Stream, Bro IDS, OpenDNS
- **Endpoint – Host Artifacts and Patterns:** users, processes, services, drivers, files, registry, hardware, memory, disk activity, file monitoring: hash values, integrity checking and alerts, creation or deletion
  Tools: Windows/Linux, Carbon Black, Tanium, Tripwire, Active Directory
- **Vulnerability Management Data**
  Tools: Tripwire IP360, Qualys, Nessus
- **User Behavior Analytics:** TTPs, user monitoring, time of day location, HR watchlist
  Splunk UBA, (All of the above)

Typical Data Sources

Threat intelligence

- Third-party threat intel
- Open-source blacklist
- Internal threat intelligence

Attacker, know relay/C2 sites, infected sites, IOC, attack/campaign intent and attribution



Network

- Firewall, IDS, IPS
- DNS
- Email
- Web proxy
- NetFlow
- Network

Where they went, who talked to whom, attack transmitted, abnormal traffic, malware download

Endpoint

- Endpoint (AV/IPS/FW)
- Malware detection
- PCLM
- DHCP
- OS logs
- Patching

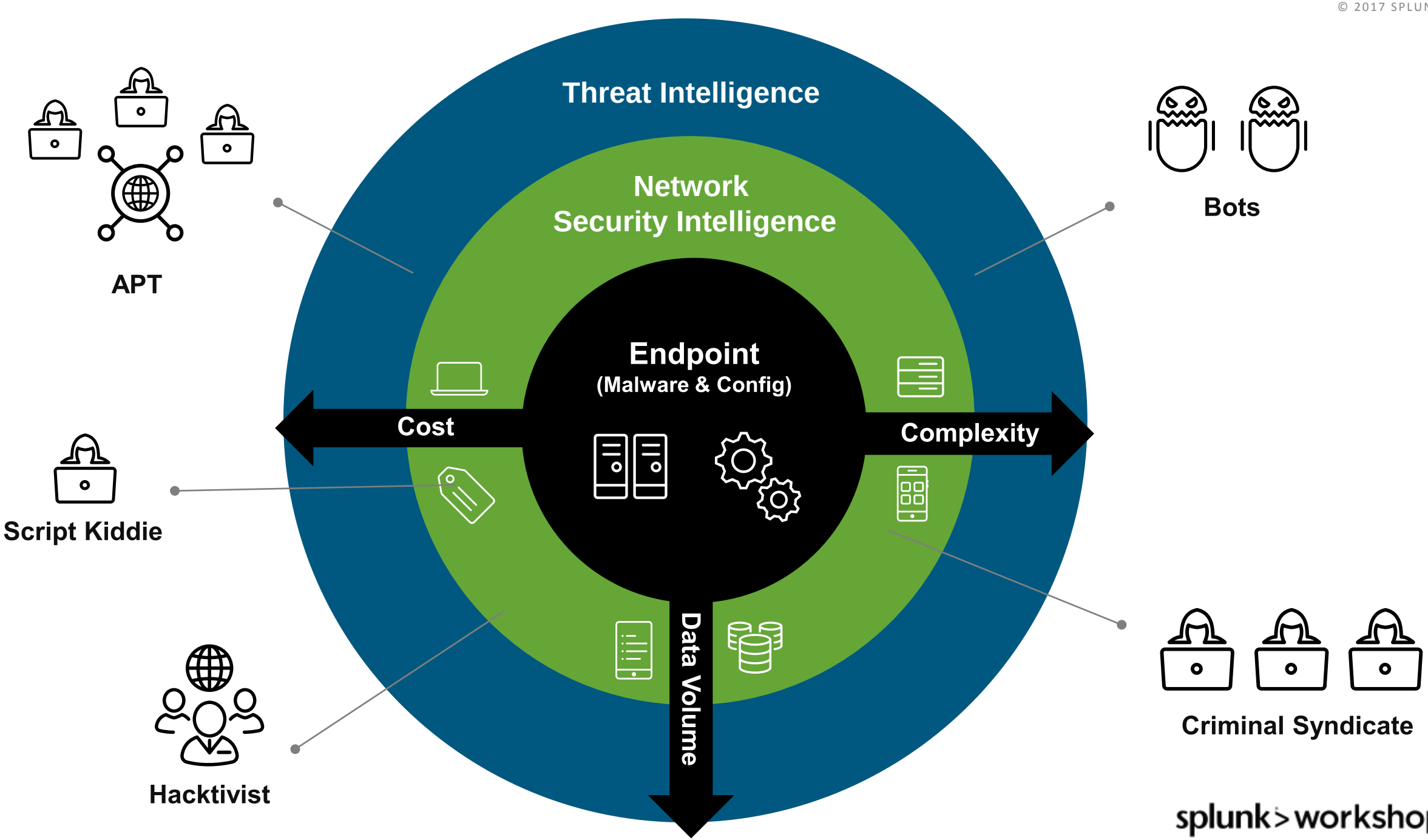
What process is running (malicious, abnormal, etc.) Process owner, registry mods, attack/malware artifacts, patching level, attack susceptibility

Access/Identity

- Active Directory
- LDAP
- CMDB
- Operating system
- Database
- VPN, AAA, SSO

Access level, privileged users, likelihood of infection, where they might be in kill chain

splunk> workshop



splunk> workshop

Know Your Endpoint: Microsoft Sysmon Primer

- TA Available on the App Store
- Great blog post to get you started
- Increases the fidelity of Microsoft Logging

Blog Post:
http://blogs.splunk.com/2014/11/24/monitoring-network-traffic-with-sysmon-and-splunk/

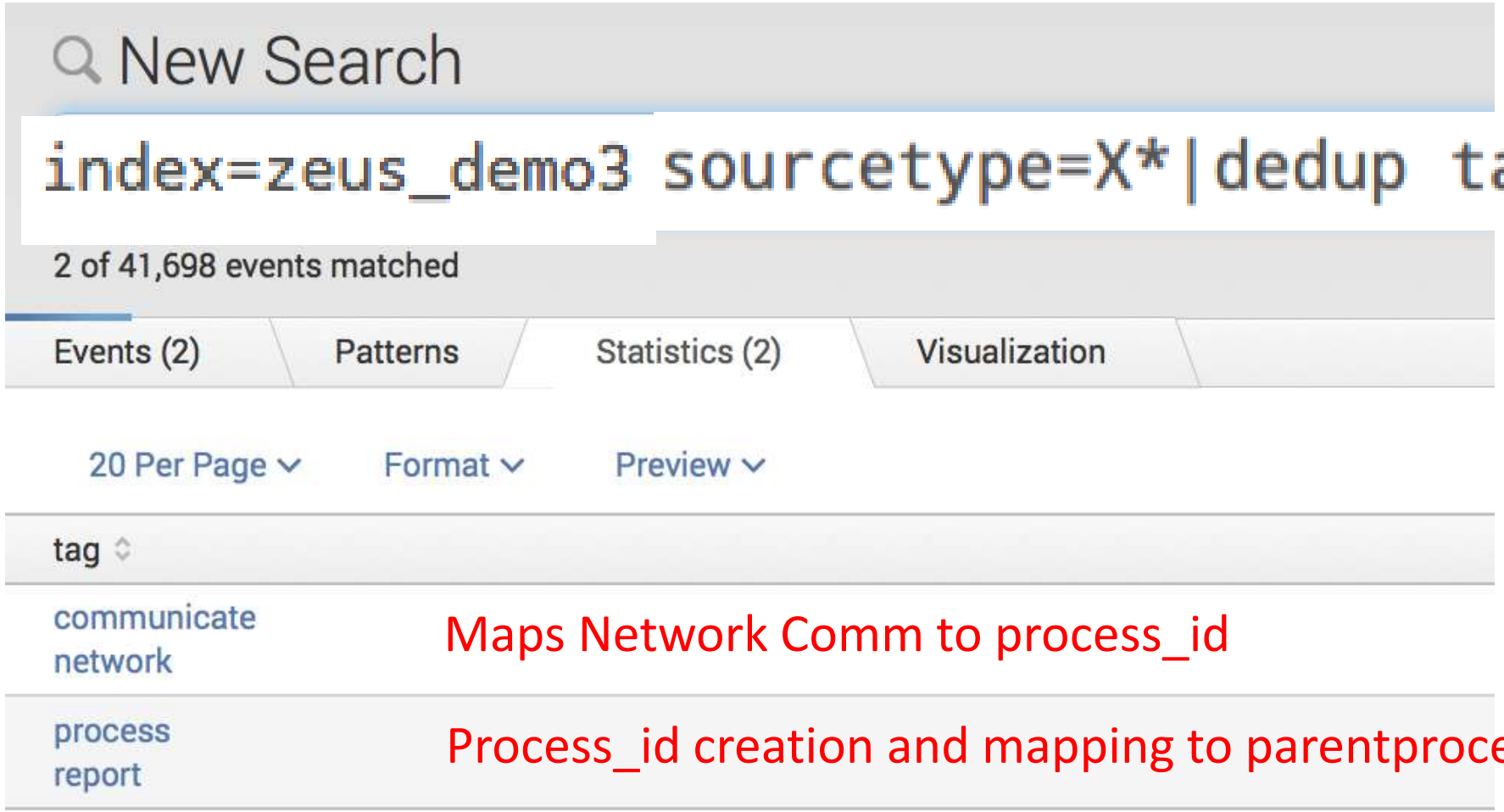
Log In Credentials

Birth Month

January & February	https://od-threat-hunting-wrksp-portland-**01**.splunkoxygen.com
March & April	https://od-threat-hunting-wrksp-portland-**02**.splunkoxygen.com
May & June	https://od-threat-hunting-wrksp-portland-**03**.splunkoxygen.com
July & August	https://od-threat-hunting-wrksp-portland-**04**.splunkoxygen.com
September & October	https://od-threat-hunting-wrksp-portland-**05**.splunkoxygen.com
November & December	https://od-threat-hunting-wrksp-portland-**06**.splunkoxygen.com

User: hunter
Password: pr3dat0r

Sysmon Event Tags: Optional Search



Maps Network Comm to process_id

Process_id creation and mapping to parentprocess_id

sourcetype=X* | search tag=communicate

<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>3</EventID><Version>3</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2015-02-05T07:16:00.595Z'/><EventRecordID>350809</EventRecordID><Correlation/><Execution ProcessID='1092' ThreadID='2728'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>server1</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='UtcTime'>02-05-2015 7:16 AM</Data><Data Name='ProcessGuid'>{00000000-535B-54BA-0000-001065FEA309}</Data><Data Name='ProcessId'>4768</Data><Data Name='Image'>C:\Program Files (x86)\Adobe\Reader 10.0\Reader\AcroRd32.exe</Data><Data Name='User'>server1\jim</Data><Data Name='Protocol'>tcp</Data><Data Name='Initiated'>true</Data><Data Name='SourceIsIpv6'>false</Data><Data Name='SourceIp'>192.168.1.87</Data><Data Name='SourceHostname'>server1</Data><Data Name='SourcePort'>65175</Data><Data Name='SourcePortName'></Data><Data Name='DestinationIsIpv6'>false</Data><Data Name='DestinationIp'>96.16.7.81</Data><Data Name='DestinationHostname'>a96-16-7-81.deploy.akamaitechnologies.com</Data><Data Name='DestinationPort'>80</Data><Data Name='DestinationPortName'>http</Data></EventData></Event>

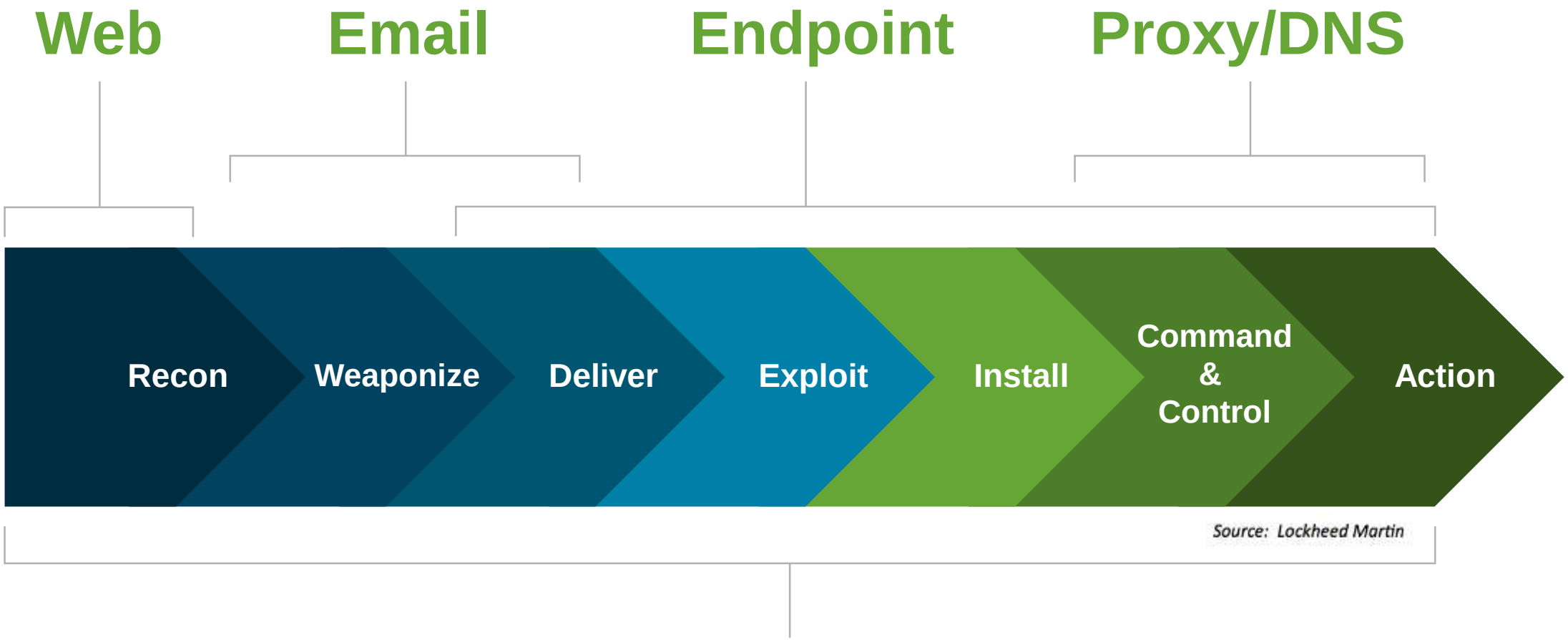
splunk> workshop

sourcetype=X* | dedup tag| search tag=process

<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name
='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>1</Even
tID><Version>3</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000
000000000</Keywords><TimeCreated SystemTime='2014-05-12T23:54:42.308'/><EventRecordID>35079
9</EventRecordID><Correlation/><Execution ProcessID='1092' ThreadID='3200'/><Channel>Micros
oft-Windows-Sysmon/Operational</Channel><Computer>NSM-Server2008</Computer><Security UserID
='S-1-5-18'/></System><EventData><Data Name='UtcTime'>5/12/2015 11:54 PM</Data><Data Name='
ProcessGuid'>{00000000-535B-54BA-0000-001065FEA309}</Data><Data Name='ProcessId'>4768</Data
><Data Name='Image'>c:\Users\cgilbert\AppData\Roaming\Irqe\svch exe</Data><Data Name='Co
mmandLine'>""c:\Users\cgilbert\AppData\Roaming\Irqe\svchost.ex "</Data><Data Name='User'>
NSM-SERVER2008\cgilbert</Data><Data Name='LogonGuid'>{0000 000-AC18-54B8-0000-00202ABEE602}
</Data><Data Name='LogonId'>0x2e6be2a</Data><Data Na TerminalSessionId'>2</Data><Data Na
me='IntegrityLevel'>Medium</Data><Data Name='HashTy SHA1</Data><Data Name='Hash'>3CBE3D4
E0ACFDC5809EF63EFD2FD42586B014686</Data><Data Name='ParentProcessGuid'>{00000000-AC1A-54B8-
0000-00104BF2E602}</Data><Data Name='ParentProcessId'>4000</Data><Data Name='ParentImage'>c
:\Users\cgilbert\AppData\Local\Temp\calc.exe</Data><Data Name='ParentCommandLine'>c:\Users\
cgilbert\AppData\Local\Temp\calc.exe</Data></EventData></Event>

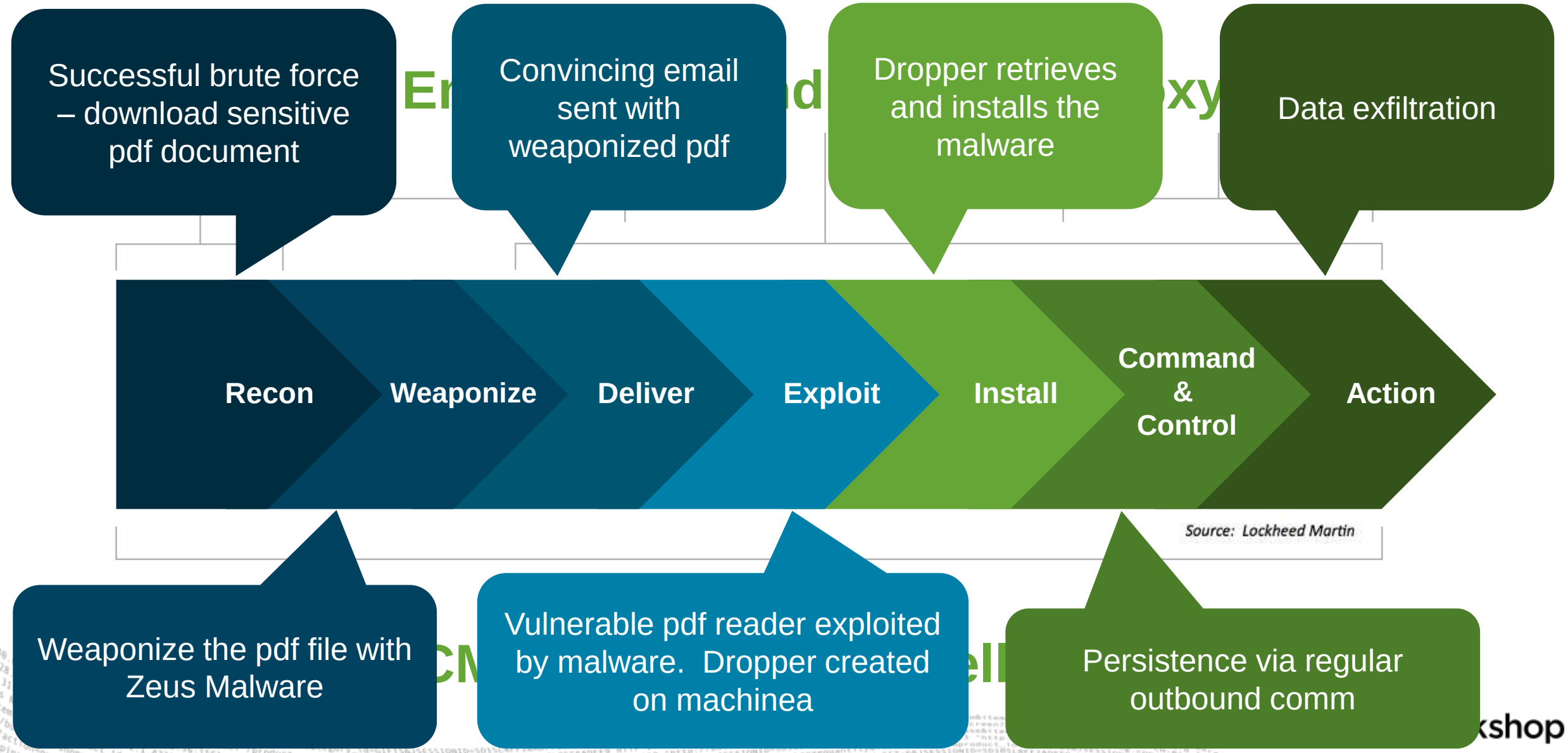
splunk> workshop

Data Source Mapping



splunk> workshop

Demo Story - Kill Chain Framework



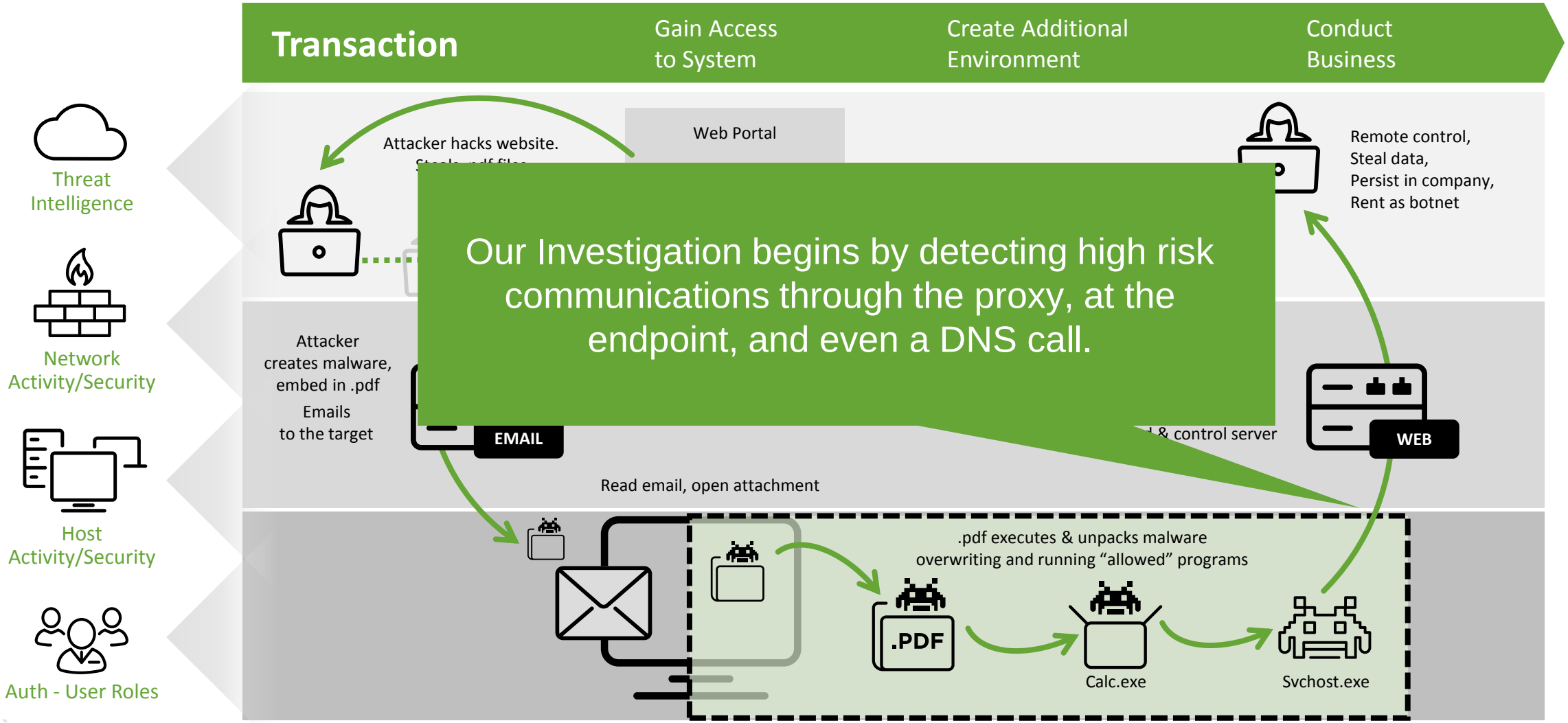
Stream Investigations – Choose Your Data Wisely

Threat Intelligence
Email
Web
Desktops
Servers
DHCP/ DNS
CMDB

Traditional

Hypervisor
Badges
Firewall
Authentication
Vulnerability Scans
Custom Apps
Network Flows
Storage
Mobile
Intrusion Detection
Data Loss Prevention
Anti-Malware
Physical Access
Transaction Records

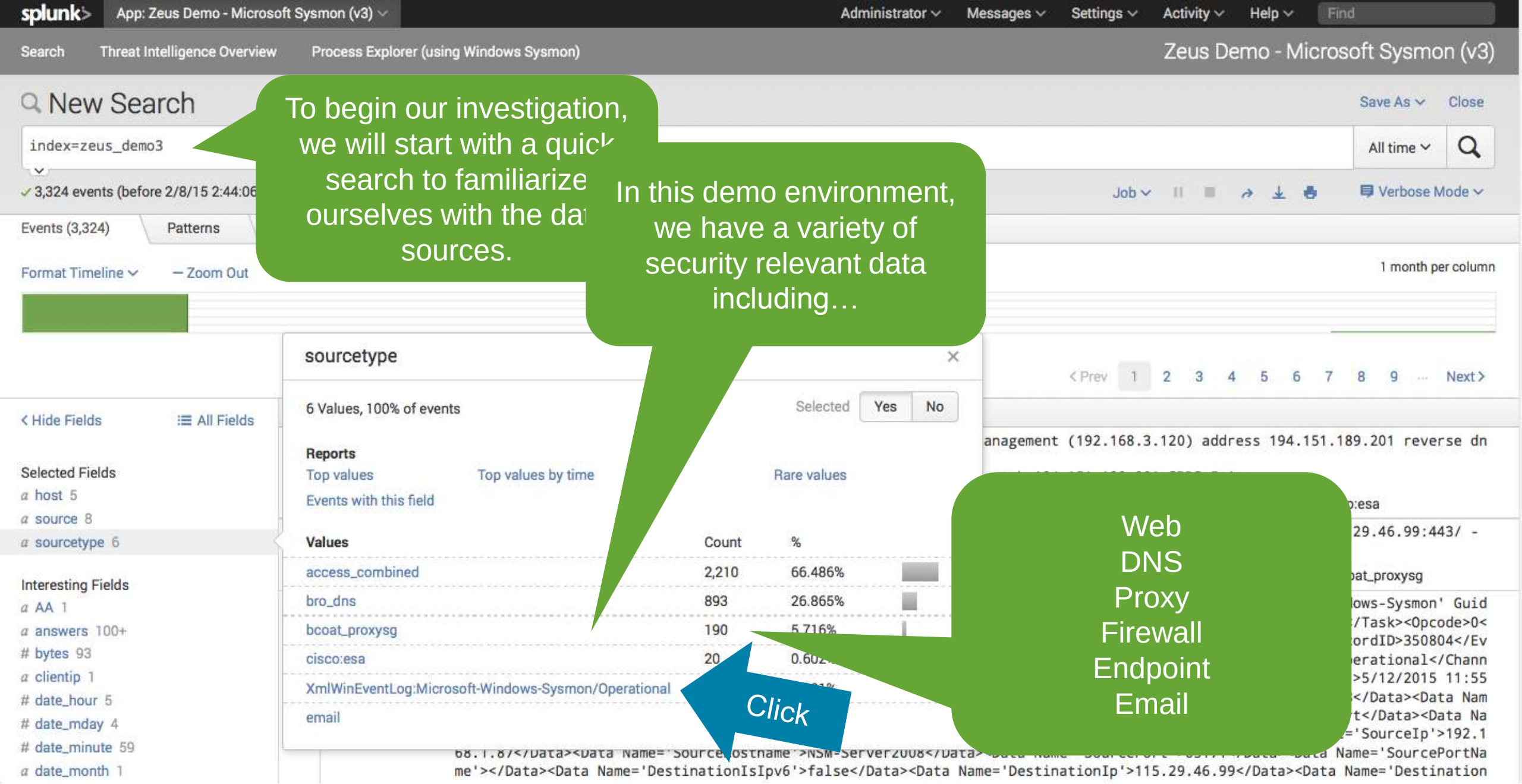
APT Transaction Flow Across Data Sources

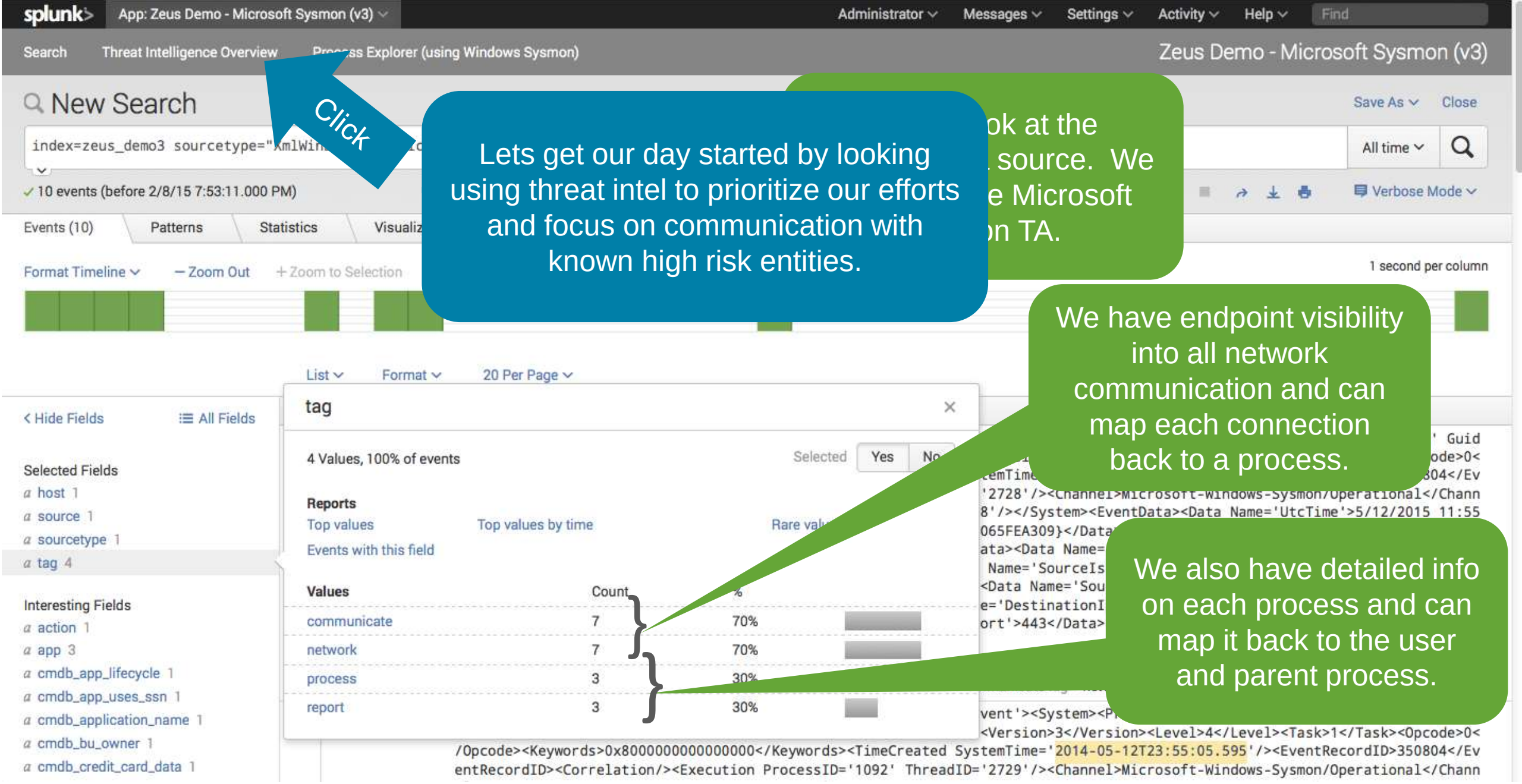


splunk> workshop

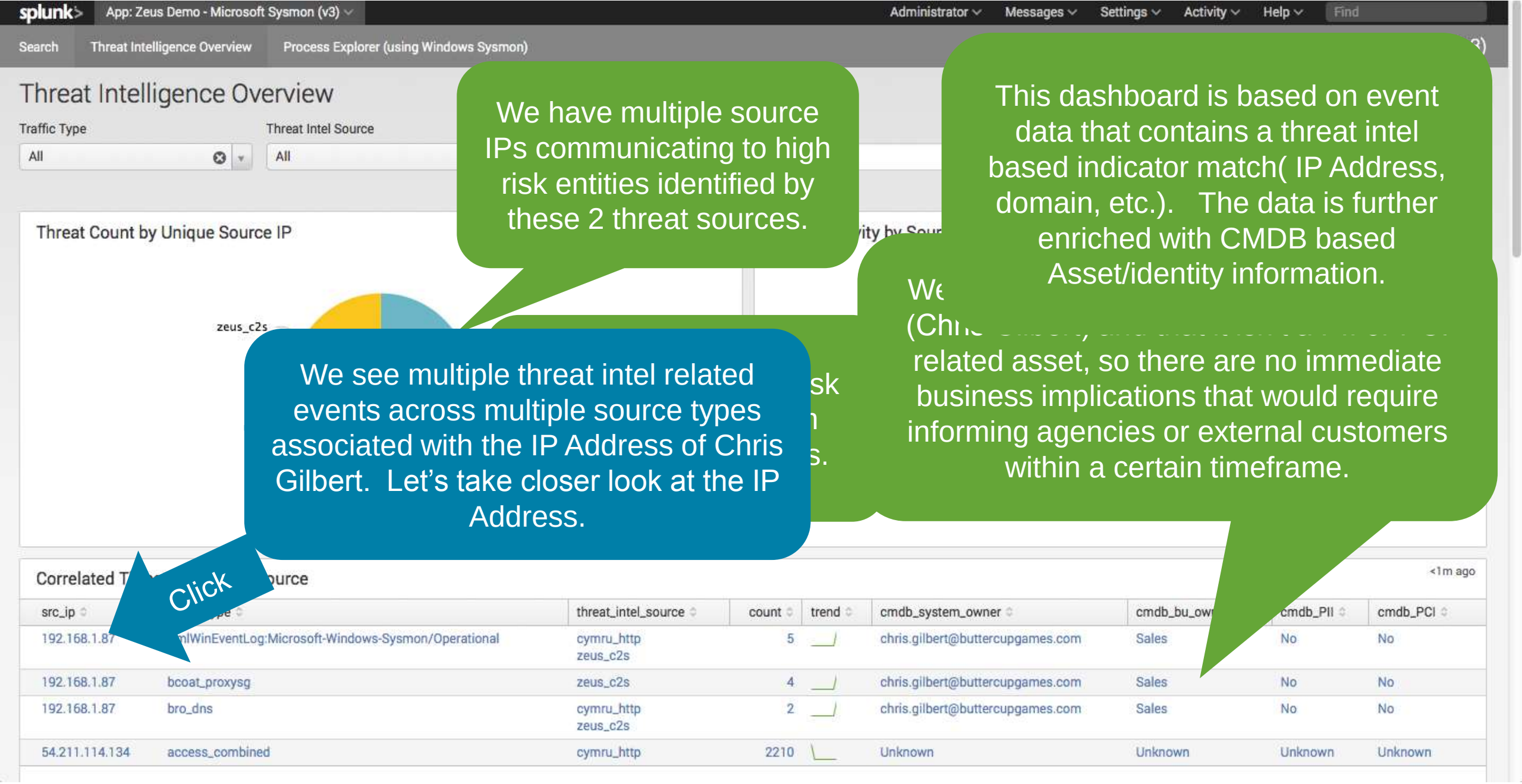
in search:

index=zeus_demo3


splunk> App: Zeus Demo - Microsoft Sysmon (v3)
Administrator Messages Settings Activity Help Find
Search Threat Intelligence Overview Process Explorer (using Windows Sysmon)
Zeus Demo - Microsoft Sysmon (v3)
New Search
Save As Close
index=zeus_demo3
All time
3,324 events (before 2/8/15 2:44:06
Job Verbose Mode
Events (3,324) Patterns
Format Timeline Zoom Out
1 month per column
Prev 1 2 3 4 5 6 7 8 9 Next
To begin our investigation, we will start with a quick search to familiarize ourselves with the data sources.
In this demo environment, we have a variety of security relevant data including…
sourcetype
6 Values, 100% of events
Selected Yes No
Reports
Top values Top values by time Rare values
Events with this field
Values Count %
access_combined 2,210 66.486%
bro_dns 893 26.865%
bcoat_proxysg 190 5.716%
cisco:esa 20 0.602%
XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
email
Click
Web
DNS
Proxy
Firewall
Endpoint
Email
Hide Fields All Fields
Selected Fields
a host 5
a source 8
a sourcetype 6
Interesting Fields
a AA 1
a answers 100+
bytes 93
a clientip 1
date_hour 5
date_mday 4
date_minute 59
a date_month 1
anagement (192.168.3.120) address 194.151.189.201 reverse dn
:esa
29.46.99:443/ -
at_proxysg
lows-Sysmon' Guid
/Task><Opcode>0<
ordID>350804</Ev
erational</Chann
>5/12/2015 11:55
</Data><Data Nam
t</Data><Data Na
='SourceIp'>192.1
68.1.87</Data><Data Name='SourceHostname'>NSM-Server2008</Data><Data Name='SourcePortNa
me'></Data><Data Name='DestinationIsIpv6'>false</Data><Data Name='DestinationIp'>115.29.46.99</Data><Data Name='Destination
splunk> workshop



splunk> workshop


splunk> App: Zeus Demo - Microsoft Sysmon (v3)
Administrator Messages Settings Activity Help Find
Search Threat Intelligence Overview Process Explorer (using Windows Sysmon)
Threat Intelligence Overview
Traffic Type
All
Threat Intel Source
All
Threat Count by Unique Source IP
zeus_c2s
We have multiple source IPs communicating to high risk entities identified by these 2 threat sources.
This dashboard is based on event data that contains a threat intel based indicator match(IP Address, domain, etc.). The data is further enriched with CMDB based Asset/identity information.
We see multiple threat intel related events across multiple source types associated with the IP Address of Chris Gilbert. Let's take closer look at the IP Address.
related asset, so there are no immediate business implications that would require informing agencies or external customers within a certain timeframe.
Click
Correlated T urce
<1m ago
src_ip
threat_intel_source
count
trend
cmdb_system_owner
cmdb_bu_ow
cmdb_PII
cmdb_PCI
192.168.1.87 nlWinEventLog:Microsoft-Windows-Sysmon/Operational cymru_http zeus_c2s 5 chris.gilbert@buttercupgames.com Sales No No
192.168.1.87 bcoat_proxysg zeus_c2s 4 chris.gilbert@buttercupgames.com Sales No No
192.168.1.87 bro_dns cymru_http zeus_c2s 2 chris.gilbert@buttercupgames.com Sales No No
54.211.114.134 access_combined cymru_http 2210 Unknown Unknown Unknown Unknown

Threat Intelligence Overview

Edit More Info

Traffic Type: All
Threat Intel Source: All
Source Type: All
Search Terms: 192.168.1.87
All time

Threat Count by Unique Source IP

10m ago

Threat Activity by Sourcetype

10m ago

We are now looking at only threat intel related activity for the IP Address associated with Chris Gilbert and see activity spanning endpoint, proxy, and DNS data sources.

Scroll d
thes

We then see threat intel related endpoint and proxy events occurring periodically and likely communicating with a known Zeus botnet based on the threat intel source (zeus_c2s).

Correlated Threat Activity by Source

src_ip	sourcetype	threat_intel_source	count	trend	cmdb_	cmdb_bu_owner	cmdb_PII	cm
192.168.1.87	XmlWinEventLog:Microsoft-Windows-Sysmon/Operational	cymru_http zeus_c2s	5		chris ttercupgames.com	Sales	No	No
192.168.1.87	bcoat_proxysg	zeus_c2s	4		.gilbert@buttercupgames.com	Sales	No	No
192.168.1.87	bro_dns	cymru_http zeus_c2s	2		chris.gilbert@buttercupgames.com	Sales	No	No

Scroll Dow

It's worth mentioning that at this point you could create a ticket to have someone re-image the machine to prevent further damage as we continue our investigation within Splunk.

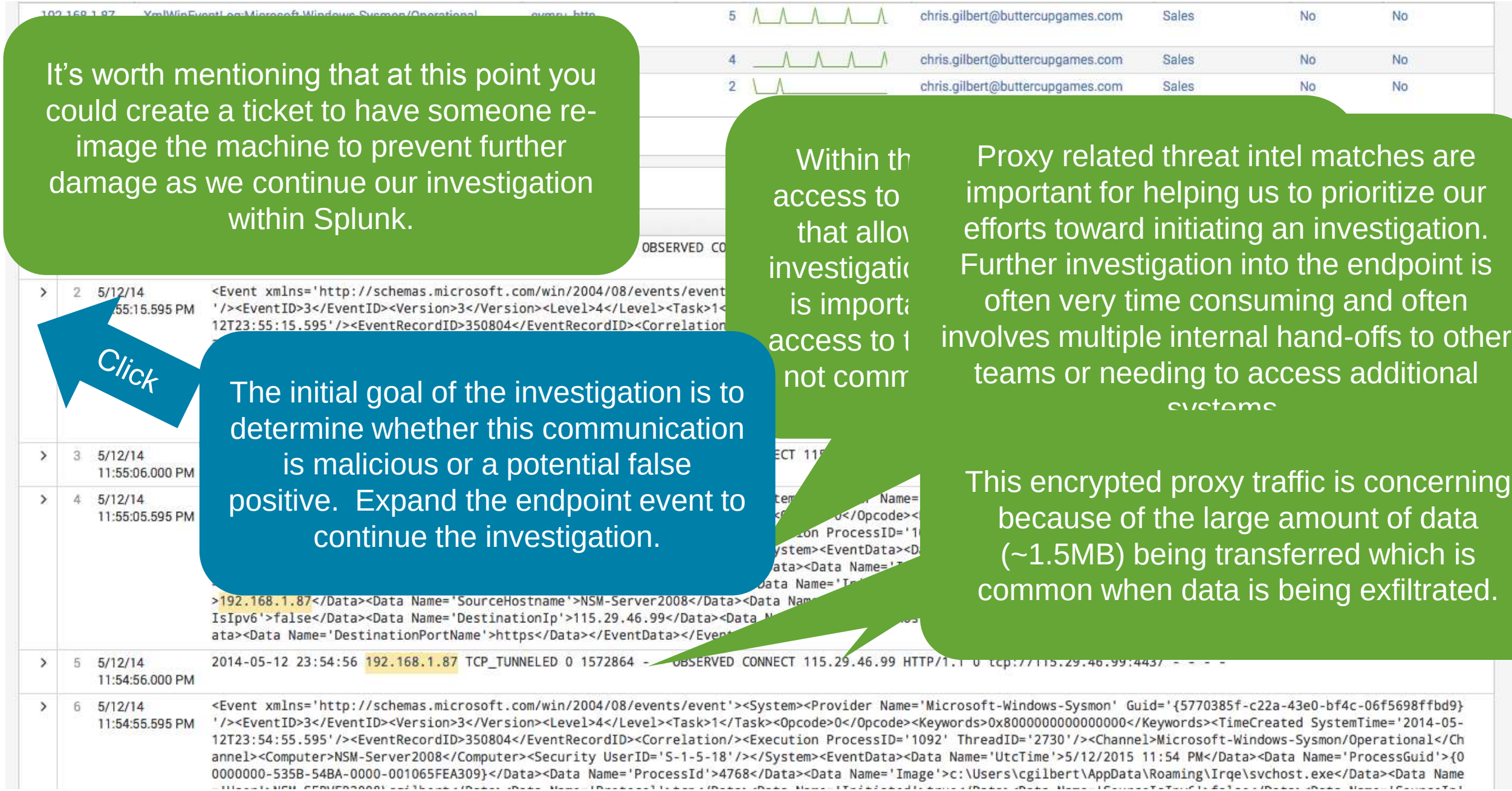
Click

The initial goal of the investigation is to determine whether this communication is malicious or a potential false positive. Expand the endpoint event to continue the investigation.

Within th
access to
that allo
investigati
is import
access to
not comm

Proxy related threat intel matches are important for helping us to prioritize our efforts toward initiating an investigation. Further investigation into the endpoint is often very time consuming and often involves multiple internal hand-offs to other teams or needing to access additional systems.

This encrypted proxy traffic is concerning because of the large amount of data (~1.5MB) being transferred which is common when data is being exfiltrated.



2 5/12/14
11:55:15.595 PM

<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>3</EventID><Version>3</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2014-05-12T23:55:15.595'/><EventRecordID>350804</EventRecordID><Correlation/><Execution ProcessID='1092' ThreadID='2728'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>NSM-Server2008</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='UtcTime'>5/12/2015 11:55 PM</Data><Data Name='ProcessGuid'>{00000000-535B-54BA-0000-001065FEA309}</Data><Data Name='ProcessId'>4768</Data><Data Name='Image'>c:\Users\cgilbert\AppData\Roaming\Irqe\svchost.exe</Data><Data Name='User'>NSM-SERVER2008\cgilbert</Data><Data Name='Protocol'>tcp</Data><Data Name='Initiated'>true</Data><Data Name='SourceIsIpv6'>false</Data><Data Name='SourceIp'>192.168.1.87</Data><Data Name='SourceHostname'>NSM-Server2008</Data><Data Name='SourcePort'>65171</Data><Data Name='SourcePortName'></Data><Data Name='DestinationIsIpv6'>false</Data><Data Name='DestinationIp'>115.29.46.99</Data><Data Name='DestinationHostname'>www.vh44850.eurodir.ru</Data><Data Name='DestinationPort'>443</Data><Data Name='DestinationPortName'>https</Data></EventData></Event>

Event Actions

Type	Field	
Event	Computer	
	DestinationHostname	
	DestinationIp	
	DestinationIsIpv6	false
	DestinationPort	443
	DestinationPortName	https
	EventChannel	Microsoft-Win
	EventCode	3
	Guid	'{5770385f-c22
	Image	c:\Users\cgilb
	Initiated	true
	Keywords	0x8000000000000000
	Level	4
	Name	'Microsoft-Windows-Sysmon'
	Opcode	0
	ProcessGuid	{00000000-535B-54BA-0000-001065FEA309}
	ProcessID	'1092'
	ProcessId	4768
	Protocol	tcp
	RecordID	350804
	SecurityID	S-1-5-18
	SourceHostname	NSM-Server2008
	SourceIp	192.168.1.87
	SourceIsIpv6	false
	SourcePort	65171
	SystemTime	'2014-05-12T23:55:15.595'
	Task	1
	ThreadID	'2728'

Click

Lets continue the inv

We immediately see the outbound communication with 115.29.46.99 via https is associated with the svchost.exe process on the windows endpoint. The process id is 4768. There is a great deal more information from the endpoint as you scroll down such as the user ID that started the process and the associated CMDB enrichment information.

Another clue. We also see that svchost.exe should be located in a Windows system directory but this is being run in the user space. Not good.

2 5/12/14 11:55:15.595 PM

<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>3</EventID><Version>3</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2014-05-12T23:55:15.595'/><EventRecordID>350804</EventRecordID><Correlation/><Execution ProcessID='1092' ThreadID='2728'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>NSM-Server2008</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='UtcTime'>5/12/2015 11:55 PM</Data><Data Name='ProcessGuid'>{00000000-535B-54BA-0000-001065FEA309}</Data><Data Name='ProcessId'>4768</Data><Data Name='Image'>c:\Users\cgilbert\AppData\Roaming\Irqe\svchost.exe</Data><Data Name='User'>NSM-SERVER2008\cgilbert</Data><Data Name='Protocol'>tcp</Data><Data Name='Initiated'>true</Data><Data Name='SourceIsIpv6'>false</Data><Data Name='SourceIp'>192.168.1.87</Data><Data Name='SourceHostname'>NSM-Server2008</Data><Data Name='SourcePort'>65171</Data><Data Name='SourcePortName'></Data><Data Name='DestinationIsIpv6'>false</Data><Data Name='DestinationIp'>115.29.46.99</Data><Data Name='DestinationHostname'>www.vh44850.eurodir.ru</Data><Data Name='DestinationPort'>443</Data><Data Name='DestinationPortName'>https</Data></EventData></Event>

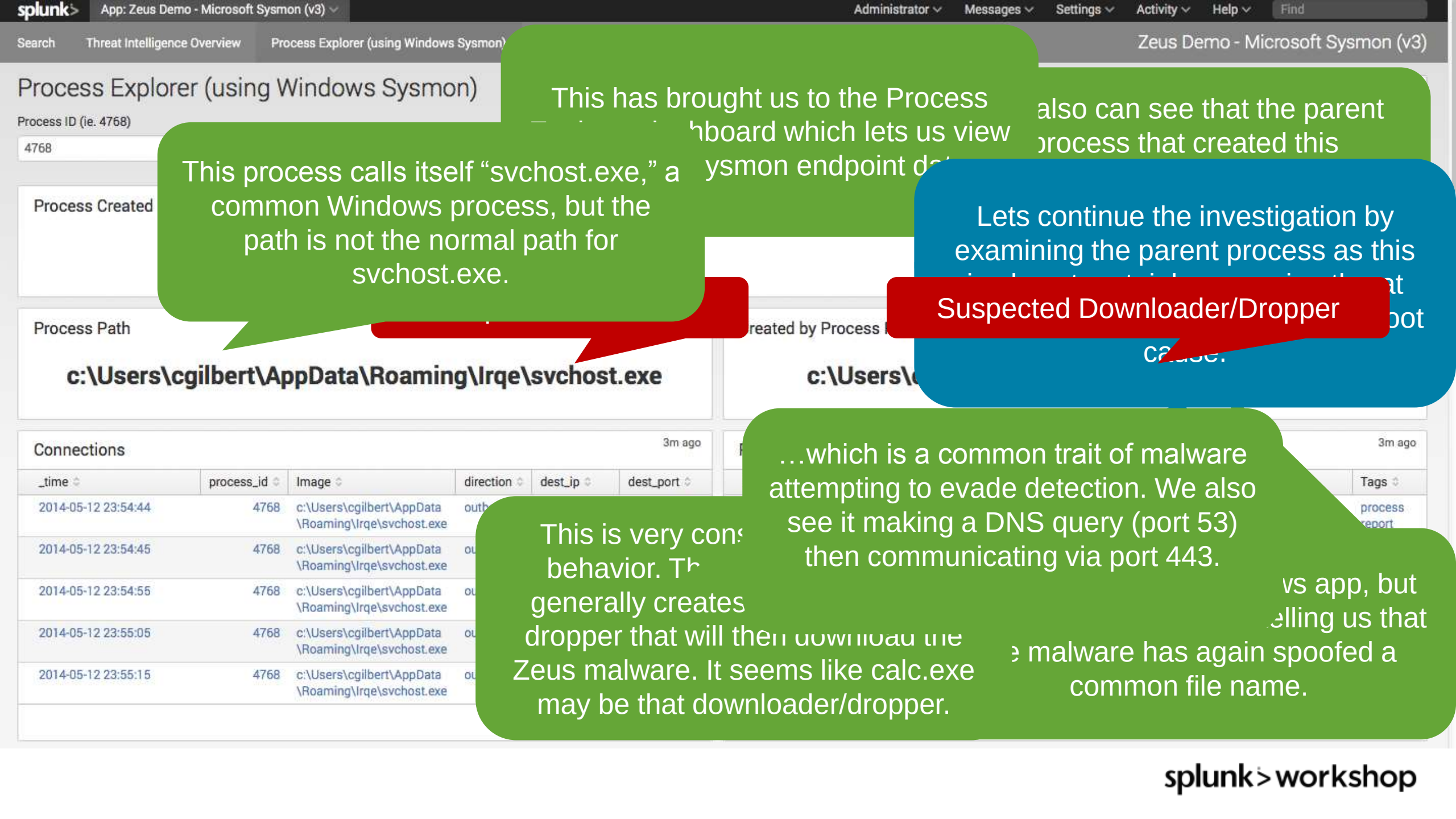
Event Actions

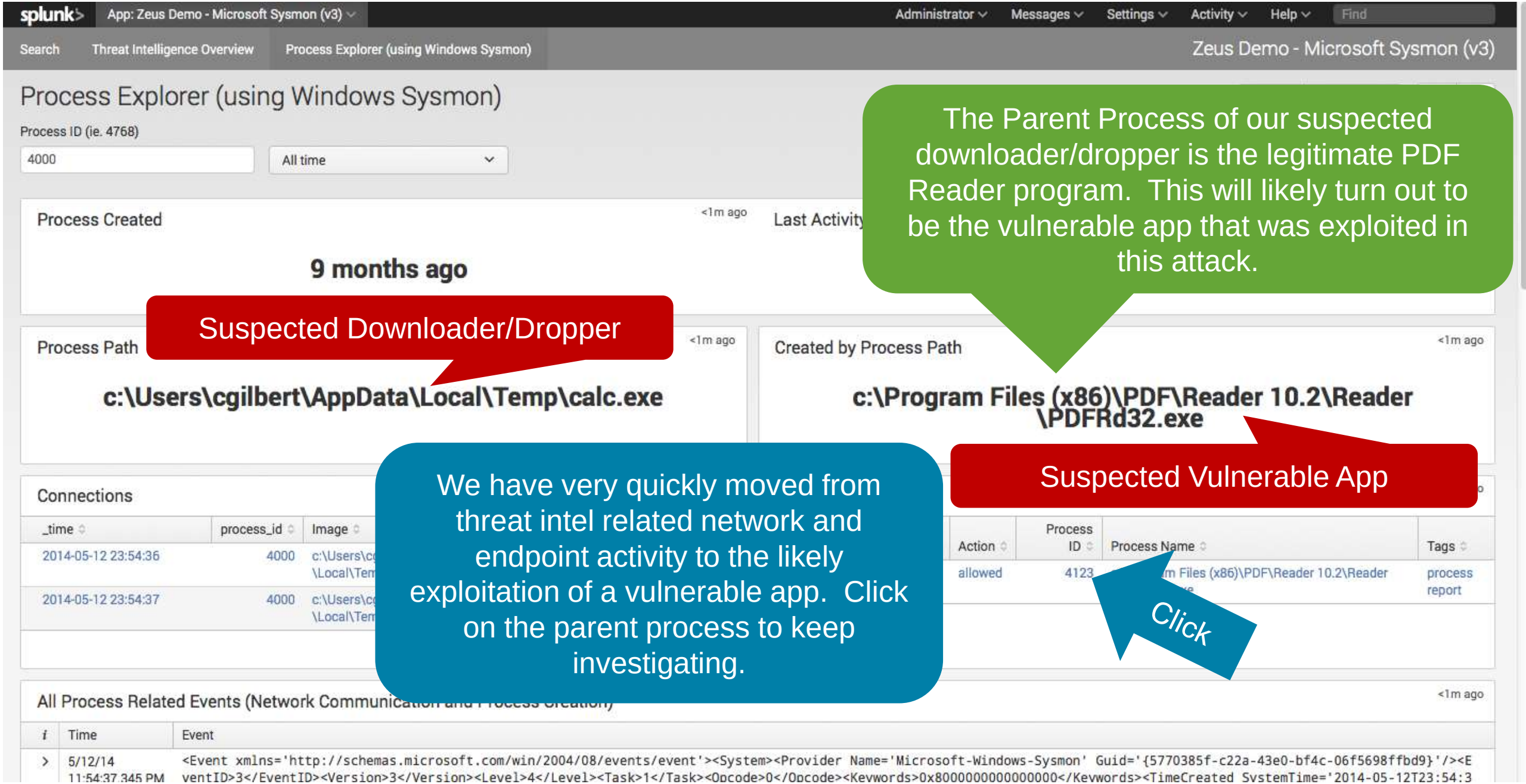
- Build Event Type
- Extract Fields
- Explore Process: 4768
- Show Source

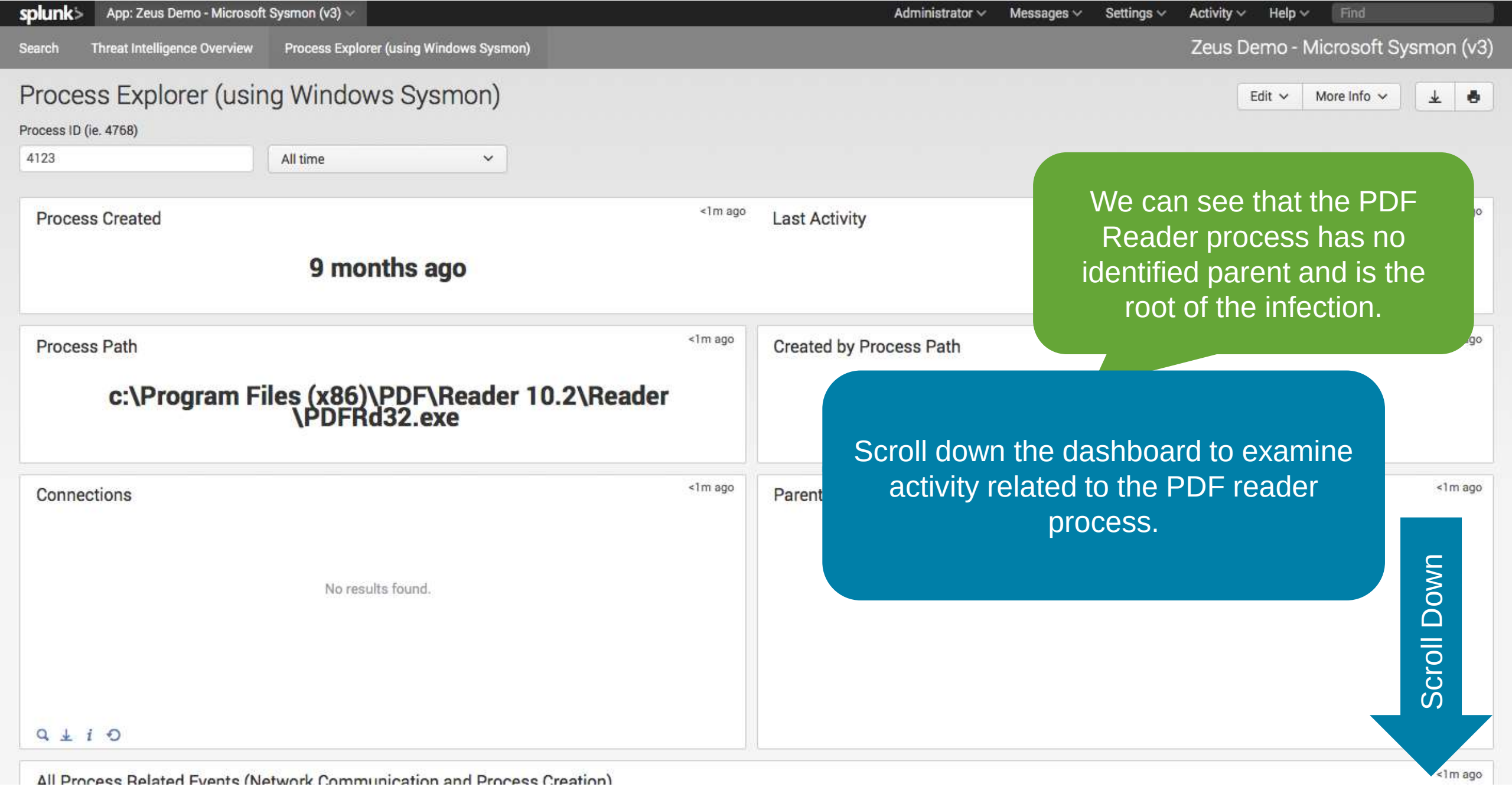
Click

	Value	Actions
	NSM-Server2008	
	www.vh44850.eurodir.ru	
	115.29.46.99	
DestinationPo		
DestinationPortName		
EventChannel	Micro t-W	
EventCode	3	
Guid	'{5770385f-	
Image	c:\Users\cg	
Initiated	true	
Keywords	0x8000000	
Level	4	
Name	'Microsoft-W	
Opcode	0	
ProcessGuid	{00000000-53	
ProcessID	'1092'	
ProcessId	4768	
Protocol	tcp	
RecordID	350804	
SecurityID	S-1-5-18	
SourceHostname	NSM-Server2008	
SourceIp	192.168.1.87	
SourceIsIpv6	false	
SourcePort	65171	
SystemTime	'2014-05-12T23:55:15.595'	
Task	1	
ThreadID	'2728'	

We have a workflow action that will link us to a Process Explorer dashboard and populate it with the process id extracted from the event (4768).


splunk> App: Zeus Demo - Microsoft Sysmon (v3)
Administrator Messages Settings Activity Help Find
Search Threat Intelligence Overview Process Explorer (using Windows Sysmon)
Zeus Demo - Microsoft Sysmon (v3)
Process Explorer (using Windows Sysmon)
Process ID (ie. 4768)
4768
Process Created
Process Path
c:\Users\cgilbert\AppData\Roaming\Irqe\svchost.exe
Connections
3m ago
_time
process_id
Image
direction
dest_ip
dest_port
2014-05-12 23:54:44 4768 c:\Users\cgilbert\AppData\Roaming\Irqe\svchost.exe
2014-05-12 23:54:45 4768 c:\Users\cgilbert\AppData\Roaming\Irqe\svchost.exe
2014-05-12 23:54:55 4768 c:\Users\cgilbert\AppData\Roaming\Irqe\svchost.exe
2014-05-12 23:55:05 4768 c:\Users\cgilbert\AppData\Roaming\Irqe\svchost.exe
2014-05-12 23:55:15 4768 c:\Users\cgilbert\AppData\Roaming\Irqe\svchost.exe
Tags
process
report
This has brought us to the Process
hboard which lets us view
ysmon endpoint da
also can see that the parent
process that created this
This process calls itself “svchost.exe,” a common Windows process, but the path is not the normal path for svchost.exe.
Lets continue the investigation by examining the parent process as this
at
ot
Suspected Downloader/Dropper
…which is a common trait of malware attempting to evade detection. We also see it making a DNS query (port 53) then communicating via port 443.
This is very cons
behavior. Th
generates
dropper that will then download the
Zeus malware. It seems like calc.exe may be that downloader/dropper.
vs app, but
elling us that
e malware has again spoofed a common file name.
splunk> workshop


splunk> App: Zeus Demo - Microsoft Sysmon (v3)
Administrator Messages Settings Activity Help Find
Search Threat Intelligence Overview Process Explorer (using Windows Sysmon)
Zeus Demo - Microsoft Sysmon (v3)
Process Explorer (using Windows Sysmon)
Process ID (ie. 4768)
4000
All time
Process Created
<1m ago
9 months ago
Last Activity
The Parent Process of our suspected downloader/dropper is the legitimate PDF Reader program. This will likely turn out to be the vulnerable app that was exploited in this attack.
Suspected Downloader/Dropper
Process Path
<1m ago
c:\Users\cgilbert\AppData\Local\Temp\calc.exe
Created by Process Path
<1m ago
c:\Program Files (x86)\PDF\Reader 10.2\Reader \PDFRd32.exe
Suspected Vulnerable App
Connections
_time
process_id
Image
2014-05-12 23:54:36
4000
2014-05-12 23:54:37
4000
Action
Process ID
Process Name
Tags
allowed
4123
m Files (x86)\PDF\Reader 10.2\Reader
process report
We have very quickly moved from threat intel related network and endpoint activity to the likely exploitation of a vulnerable app. Click on the parent process to keep investigating.
Click
All Process Related Events (Network Communication and Process Creation)
<1m ago
i
Time
Event
5/12/14 11:54:37.345 PM
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>3</EventID><Version>3</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2014-05-12T23:54:3
splunk> workshop


splunk> App: Zeus Demo - Microsoft Sysmon (v3)
Administrator Messages Settings Activity Help Find
Search Threat Intelligence Overview Process Explorer (using Windows Sysmon)
Zeus Demo - Microsoft Sysmon (v3)
Process Explorer (using Windows Sysmon)
Edit More Info
Process ID (ie. 4768)
4123
All time
Process Created
<1m ago
9 months ago
Last Activity
Process Path
<1m ago
c:\Program Files (x86)\PDF\Reader 10.2\Reader\PDFRd32.exe
Created by Process Path
Connections
<1m ago
No results found.
Parent
<1m ago
All Process Related Events (Network Communication and Process Creation)
<1m ago
We can see that the PDF Reader process has no identified parent and is the root of the infection.
Scroll down the dashboard to examine activity related to the PDF reader process.
Scroll Down
splunk> workshop

All Process Related Events (Network Communication and Process Creation)

3m ago

i	Time	Event
⌄	5/13/15 10:54:34.100 AM	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event' c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>1</EventID><Version>3</Ver 000000000000</Keywords><TimeCreated SystemTime='2015-05-12T23:54:3 ProcessID='1092' ThreadID='3499'/><Channel>Microsoft-Windows-Sysm UserID='S-1-5-18'/></System><EventData><Data Name='UtcTime'>5/12/2 001065FEA309}</Data><Data Name='ProcessId'>4123</Data><Data Name=' a><Data Name='CommandLine'>c:\Program Files (x86)\PDF\Reader 10.2\ Temporary Internet Files\Content.Outlook\FNYT5PQV\2nd_qtr_2015_rep ame='LogonGuid'>{00000000-AC18-54B8-0000-00202ABEE602}</Data><Data a><Data Name='IntegrityLevel'>Medium</Data><Data Name='HashType'>S /Data><Data Name='ParentProcessGuid'></Data><Data Name='ParentProc ndLine'></Data></EventData></Event>

Event Actions ⌄

Type	Field	Value
Selected	host ⌄	sfo-proxy-01.it.buttercupgames.com
	source ⌄	/opt/splunk/Malware/etc/apps/zeus_demo-v3/log/sysmon-v3.log
	sourcetype ⌄	XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
Event	CommandLine ⌄	c:\Program Files (x86)\PDF\Reader 10.2\Reader\PDFRd32.exe c:\users\cgilbert\AppData\Local\Microsoft\Windows \Temporary Internet Files\Content.Outlook\FNYT5PQV\2nd_qtr_2015_report.pdf
	CommandLineFilename ⌄	2nd_qtr_2015_report.pdf
	Computer ⌄	NSM-Server2008
	EventChannel ⌄	Microsoft-Windows-Sysmon/Operational
	EventCode ⌄	1
	Guid ⌄	'{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'
	Hash ⌄	3CBE3D4E0ACFDC5809EF63EFD2FD42586B032459
	HashType ⌄	SHA1
	Image ⌄	c:\Program Files (x86)\PDF\Reader 10.2\Reader\PDFRd32.exe
	IntegrityLevel ⌄	Medium
	Keywords ⌄	0x8000000000000000

We have our root cause! Chris opened a weaponized .pdf file which contained the Zeus malware. It appears to have been delivered via email and we have access to our email logs as one of our important data sources. Lets copy the filename 2nd_qtr_2014_report.pdf and search a bit further to determine the scope of this compromise.

Chris opened 2nd_qtr_2014_report.pdf which was an attachment to an email!

splunk> workshop

All Process Related Events (Network Communication and Process Creation)

3m ago

i	Time	Event
⌄	5/13/15 10:54:34.100 AM	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'> c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>1</EventID><Version>3</Versio 000000000000</Keywords><TimeCreated SystemTime='2015-05-12T23:54:34.1 ProcessID='1092' ThreadID='3499'/><Channel>Microsoft-Windows-Sysmon/ UserID='S-1-5-18'/></System><EventData><Data Name='UtcTime'>5/12/2015 001065FEA309}</Data><Data Name='ProcessId'>4123</Data><Data Name='Ima a><Data Name='CommandLine'>c:\Program Files (x86)\PDF\Reader 10.2\Rea Temporary Internet Files\Content.Outlook\FNYT5PQV\2nd_qtr_2015_report ame='LogonGuid'>{00000000-AC18-54B8-0000-00202ABEE602}</Data><Data Nam a><Data Name='IntegrityLevel'>Medium</Data><Data Name='HashType'>SHA1</Data><Data Name='Hash'>3CBE3D4E0ACFDC5809EF63EFD2FD42586B032459 /Data><Data Name='ParentProcessGuid'></Data><Data Name='ParentProcessId'></Data><Data Name='ParentImage'></Data><Data Name='ParentComma ndLine'></Data></EventData></Event>

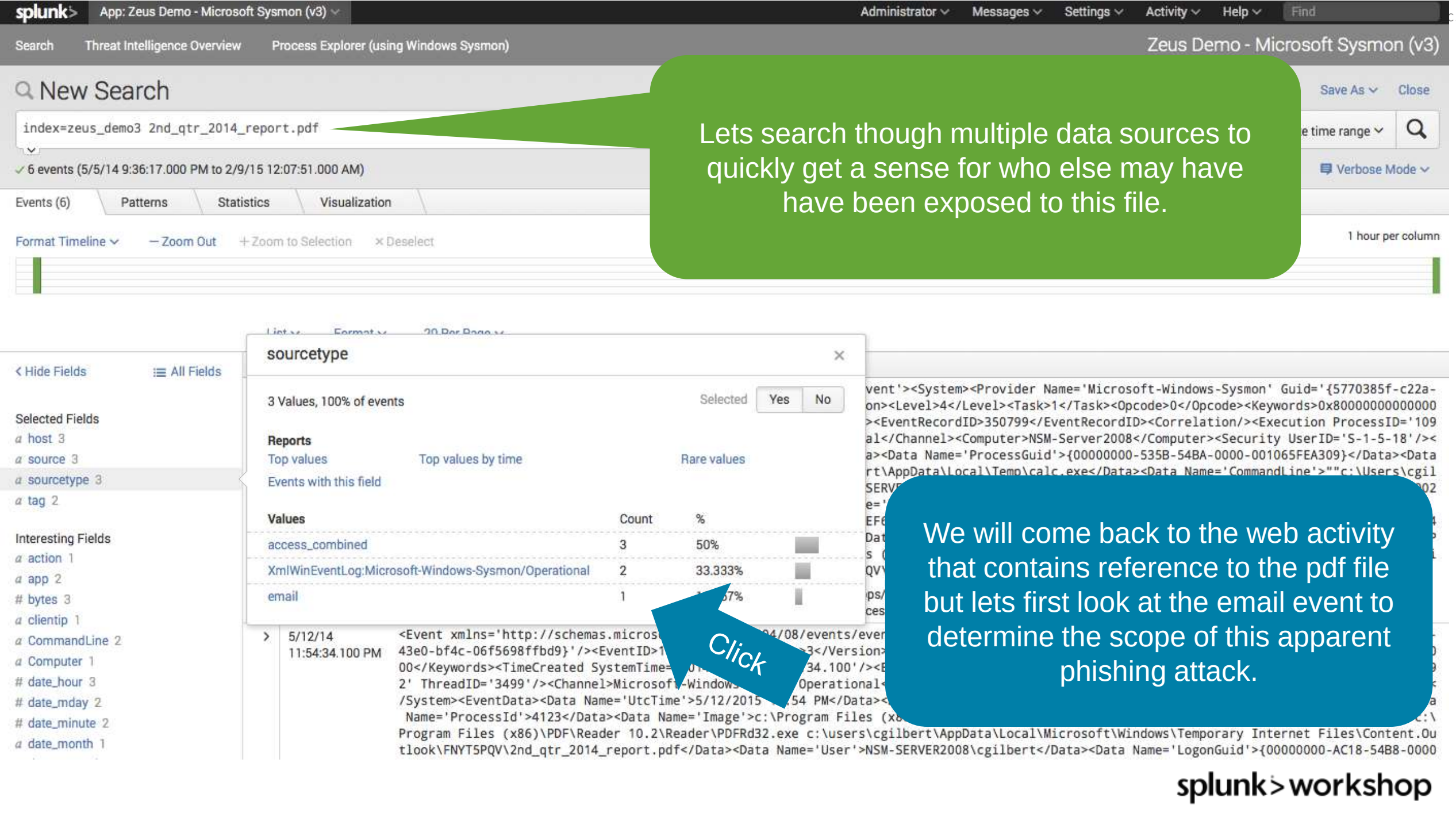
Lets dig a little further into 2nd_qtr_2014_report.pdf to determine the scope of this compromise.

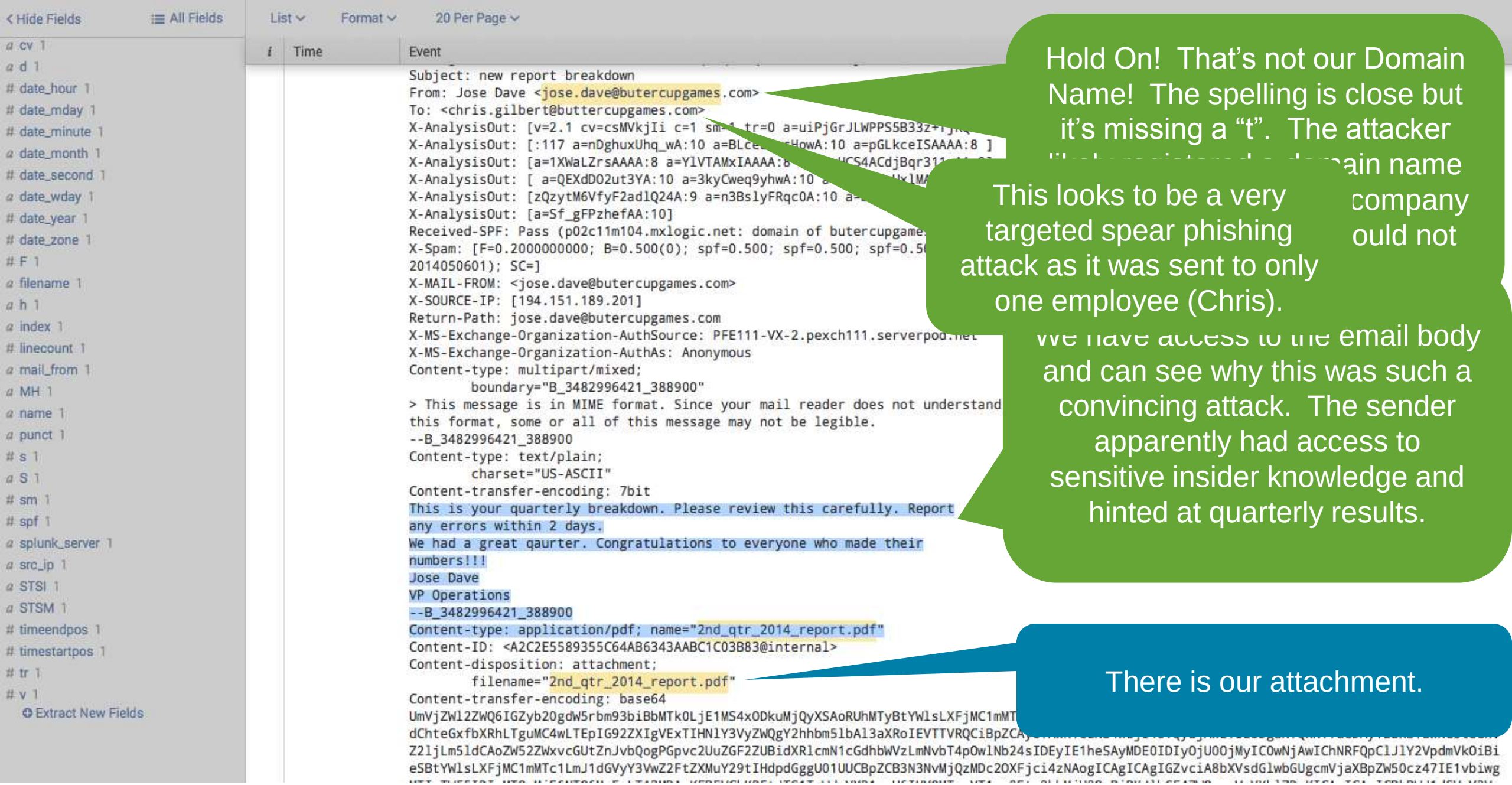
Event Actions ⌄

Type	Field	Value	Actions
Selected	host ⌄	sfo-proxy-01.it.buttercupgames.com	⌄
	source ⌄	/opt/splunk/Malware/etc/apps/zeus_demo-v3/log/sysmon-v3.log	⌄
	sourcetype ⌄	XmlWinEventLog:Microsoft-Windows-Sysmon/Operational	⌄
Event	CommandLine ⌄	c:\Program Files (x86)\PDF\Reader 10.2\Reader\PDFRd32.exe c:\users\cgilbert\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\FNYT5PQV\2nd_qtr_2015_report.pdf	⌄
	CommandLineFilename ⌄	2nd_qtr_2015_report.pdf	⌄
	Computer ⌄	NSM-Server2008	⌄
	EventChannel ⌄	Microsoft-Windows-Sysmon/Operational	⌄
	EventCode ⌄	1	⌄
	Guid ⌄	'{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'	⌄
	Hash ⌄	3CBE3D4E0ACFDC5809EF63EFD2FD42586B032459	⌄
	HashType ⌄	SHA1	⌄
	Image ⌄	c:\Program Files (x86)\PDF\Reader 10.2\Reader\PDFRd32.exe	⌄
	IntegrityLevel ⌄	Medium	⌄
	Keywords ⌄	0x8000000000000000	⌄

in search:

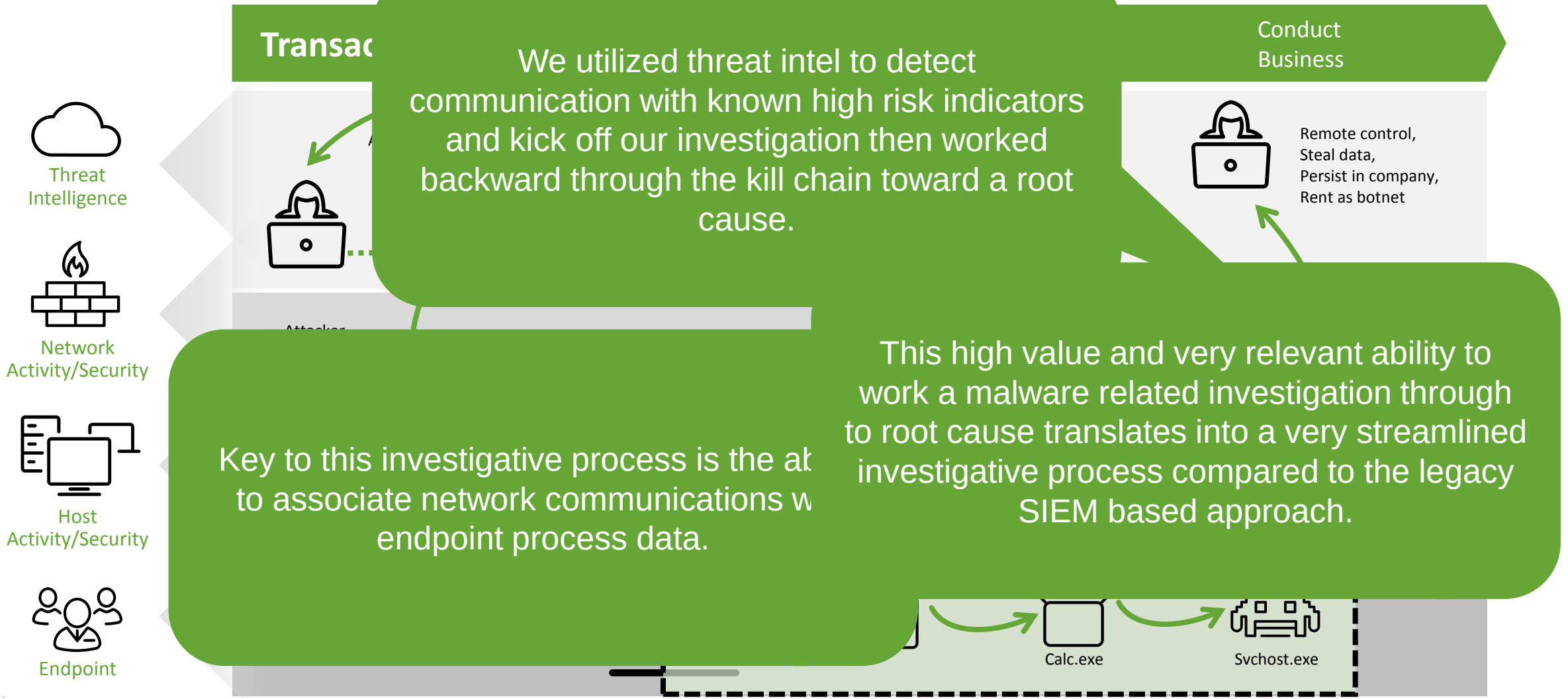
index=zeus_demo3 2nd_qtr_2014_report.pdf


splunk> App: Zeus Demo - Microsoft Sysmon (v3)
Administrator Messages Settings Activity Help Find
Search Threat Intelligence Overview Process Explorer (using Windows Sysmon)
Zeus Demo - Microsoft Sysmon (v3)
New Search
Save As Close
index=zeus_demo3 2nd_qtr_2014_report.pdf
6 events (5/5/14 9:36:17.000 PM to 2/9/15 12:07:51.000 AM)
Verbose Mode
Events (6) Patterns Statistics Visualization
Format Timeline Zoom Out Zoom to Selection Deselect
1 hour per column
Lets search though multiple data sources to quickly get a sense for who else may have have been exposed to this file.
Hide Fields All Fields
Selected Fields
host 3
source 3
sourcetype 3
tag 2
Interesting Fields
action 1
app 2
bytes 3
clientip 1
CommandLine 2
Computer 1
date_hour 3
date_mday 2
date_minute 2
date_month 1
sourcetype
3 Values, 100% of events
Selected Yes No
Reports
Top values Top values by time Rare values
Events with this field
Values Count %
access_combined 3 50%
XmlWinEventLog:Microsoft-Windows-Sysmon/Operational 2 33.333%
email 1
Click
We will come back to the web activity that contains reference to the pdf file but lets first look at the email event to determine the scope of this apparent phishing attack.
5/12/14 11:54:34.100 PM
Program Files (x86)\PDF\Reader 10.2\Reader\PDFRd32.exe c:\users\cgilbert\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\FNYT5PQV\2nd_qtr_2014_report.pdf</Data><Data Name='User'>NSM-SERVER2008\cgilbert</Data><Data Name='LogonGuid'>{00000000-AC18-54B8-0000
splunk> workshop



splunk> workshop

Root Cause Recap

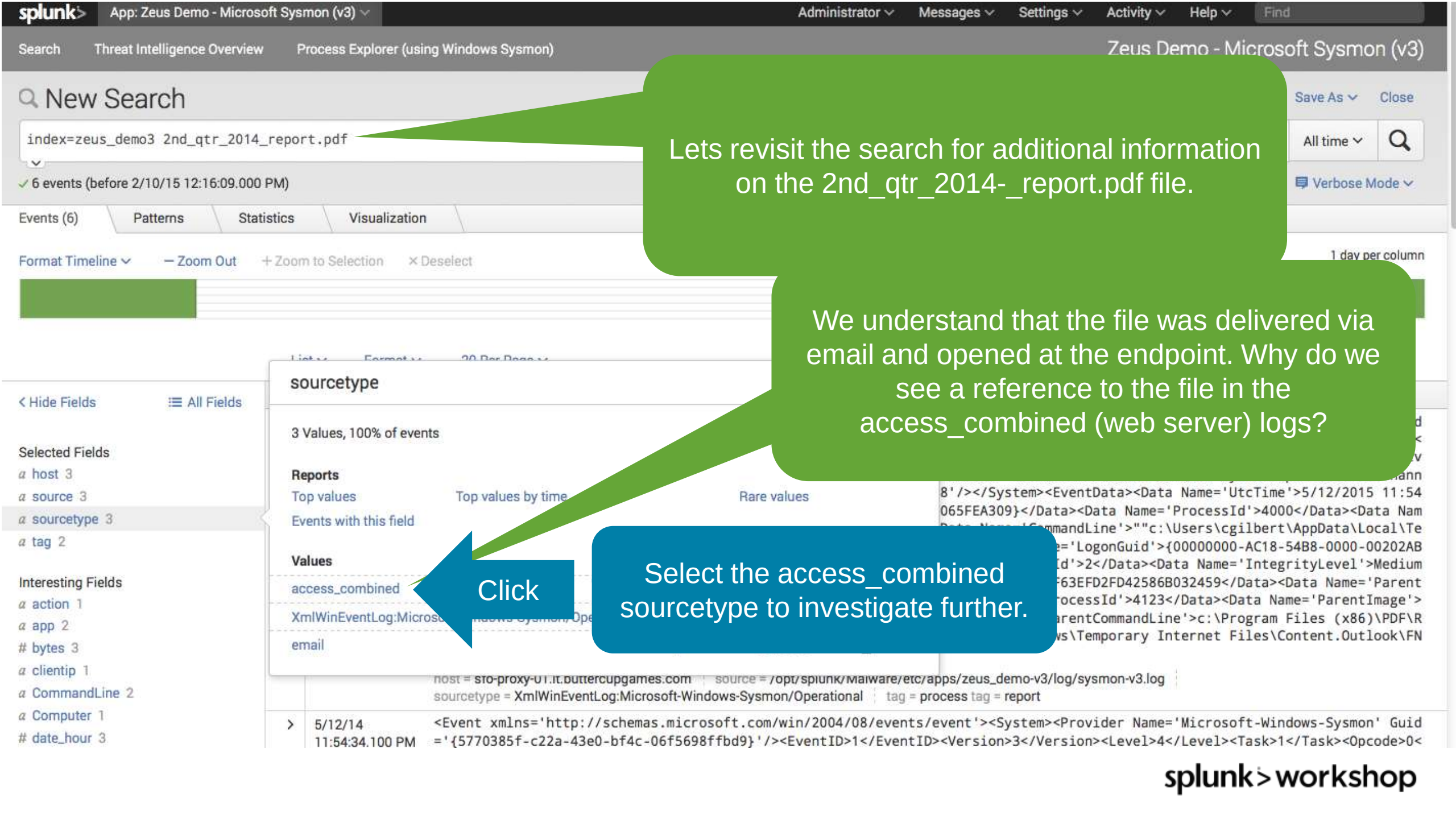


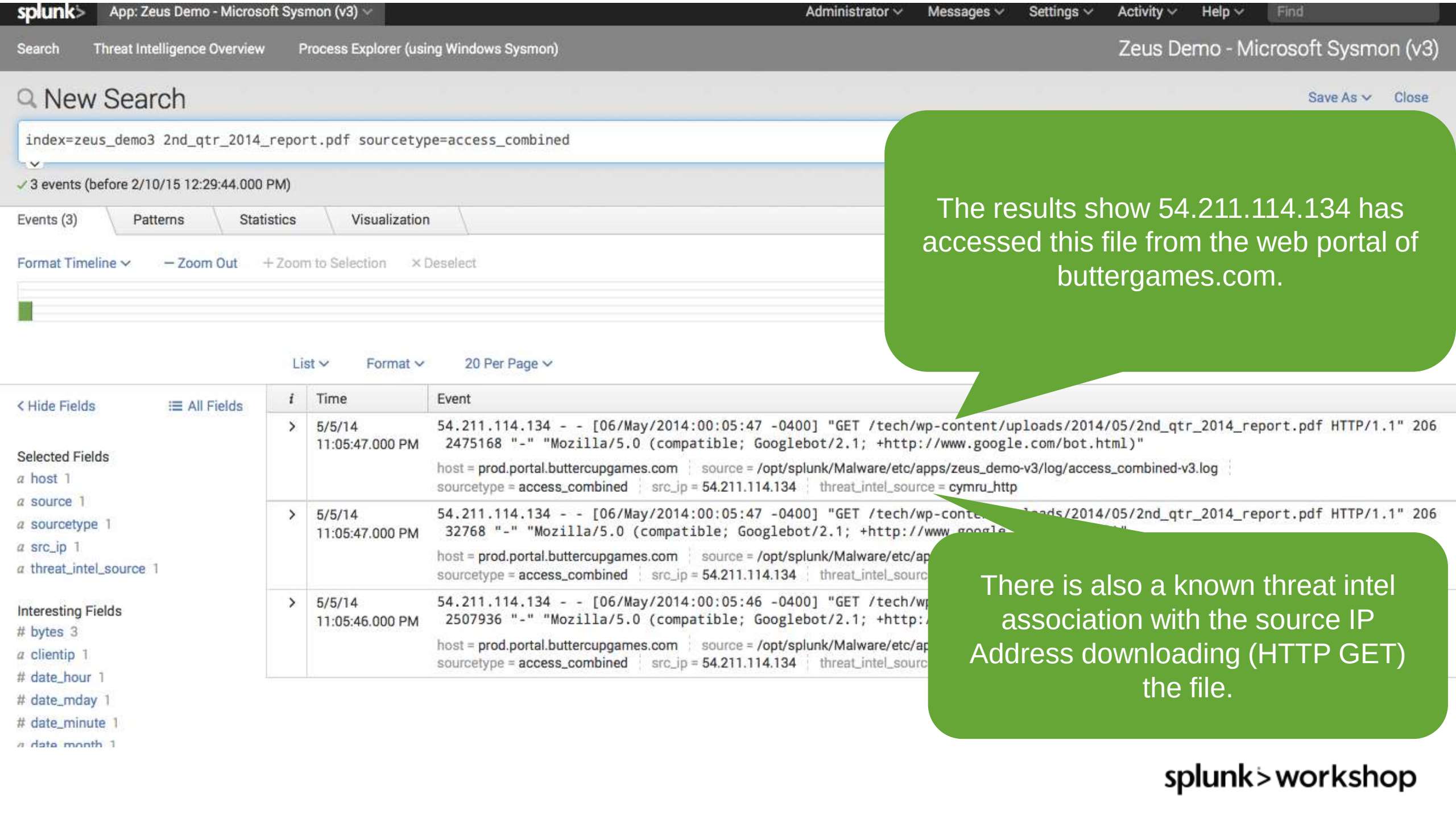
We utilized threat intel to detect communication with known high risk indicators and kick off our investigation then worked backward through the kill chain toward a root cause.

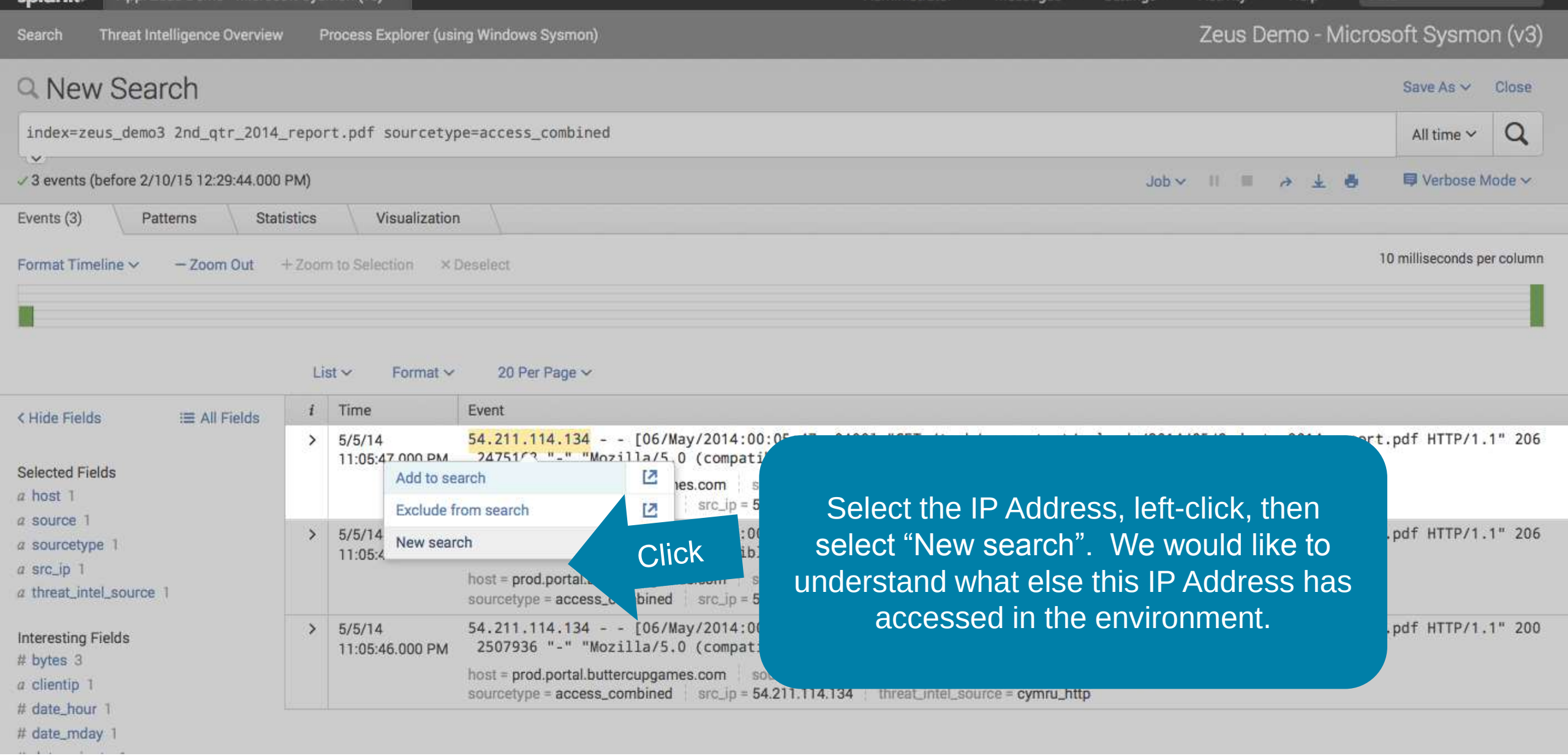
Key to this investigative process is the ab to associate network communications w endpoint process data.

This high value and very relevant ability to work a malware related investigation through to root cause translates into a very streamlined investigative process compared to the legacy SIEM based approach.

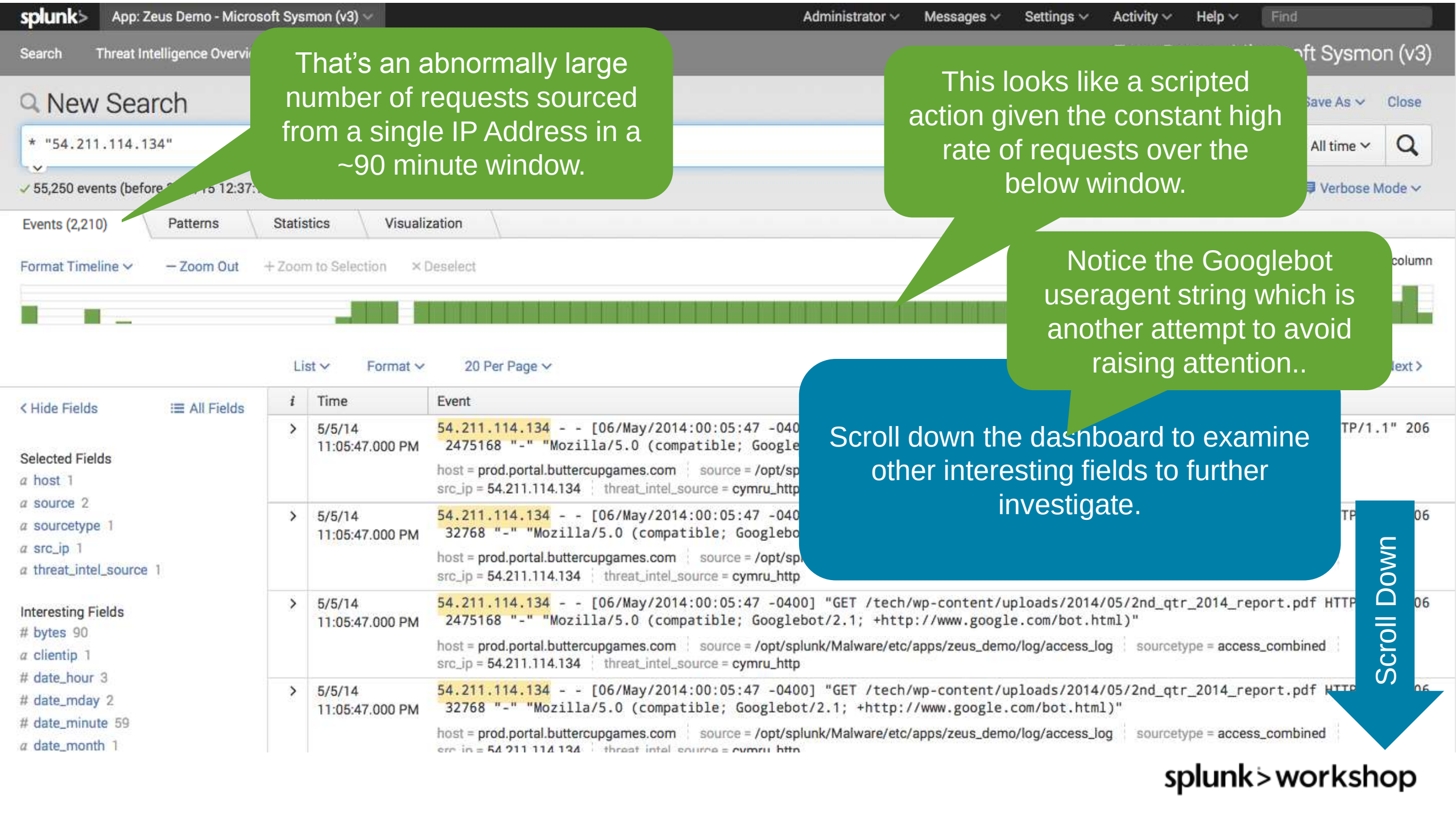
splunk> workshop


splunk> App: Zeus Demo - Microsoft Sysmon (v3)
Administrator
Messages
Settings
Activity
Help
Find
Search
Threat Intelligence Overview
Process Explorer (using Windows Sysmon)
Zeus Demo - Microsoft Sysmon (v3)
New Search
Save As
Close
index=zeus_demo3 2nd_qtr_2014_report.pdf
All time
6 events (before 2/10/15 12:16:09.000 PM)
Verbose Mode
Events (6)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 day per column
Hide Fields
All Fields
Selected Fields
host 3
source 3
sourcetype 3
tag 2
Interesting Fields
action 1
app 2
bytes 3
clientip 1
CommandLine 2
Computer 1
date_hour 3
sourcetype
3 Values, 100% of events
Reports
Top values
Top values by time
Rare values
Events with this field
Values
access_combined
email
Lets revisit the search for additional information on the 2nd_qtr_2014-_report.pdf file.
We understand that the file was delivered via email and opened at the endpoint. Why do we see a reference to the file in the access_combined (web server) logs?
Click
Select the access_combined sourcetype to investigate further.
sourcetype = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
tag = process
tag = report
5/12/14 11:54:34.100 PM
splunk> workshop


splunk> App: Zeus Demo - Microsoft Sysmon (v3)
Administrator Messages Settings Activity Help Find
Search Threat Intelligence Overview Process Explorer (using Windows Sysmon)
Zeus Demo - Microsoft Sysmon (v3)
New Search
Save As Close
index=zeus_demo3 2nd_qtr_2014_report.pdf sourcetype=access_combined
✓ 3 events (before 2/10/15 12:29:44.000 PM)
Events (3) Patterns Statistics Visualization
Format Timeline Zoom Out + Zoom to Selection × Deselect
List Format 20 Per Page
< Hide Fields All Fields
Selected Fields
a host 1
a source 1
a sourcetype 1
a src_ip 1
a threat_intel_source 1
Interesting Fields
bytes 3
a clientip 1
date_hour 1
date_mday 1
date_minute 1
a date_month 1
i Time Event
5/5/14 11:05:47.000 PM
54.211.114.134 - - [06/May/2014:00:05:47 -0400] "GET /tech/wp-content/uploads/2014/05/2nd_qtr_2014_report.pdf HTTP/1.1" 206 2475168 "-" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
host = prod.portal.buttercupgames.com source = /opt/splunk/Malware/etc/apps/zeus_demo-v3/log/access_combined-v3.log
sourcetype = access_combined src_ip = 54.211.114.134 threat_intel_source = cymru_http
5/5/14 11:05:47.000 PM
54.211.114.134 - - [06/May/2014:00:05:47 -0400] "GET /tech/wp-conte oads/2014/05/2nd_qtr_2014_report.pdf HTTP/1.1" 206 32768 "-" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google
host = prod.portal.buttercupgames.com source = /opt/splunk/Malware/etc/ap
sourcetype = access_combined src_ip = 54.211.114.134 threat_intel_sourc
5/5/14 11:05:46.000 PM
54.211.114.134 - - [06/May/2014:00:05:46 -0400] "GET /tech/wp 2507936 "-" "Mozilla/5.0 (compatible; Googlebot/2.1; +http:/
host = prod.portal.buttercupgames.com source = /opt/splunk/Malware/etc/ap
sourcetype = access_combined src_ip = 54.211.114.134 threat_intel_sourc
The results show 54.211.114.134 has accessed this file from the web portal of buttergames.com.
There is also a known threat intel association with the source IP Address downloading (HTTP GET) the file.
splunk> workshop



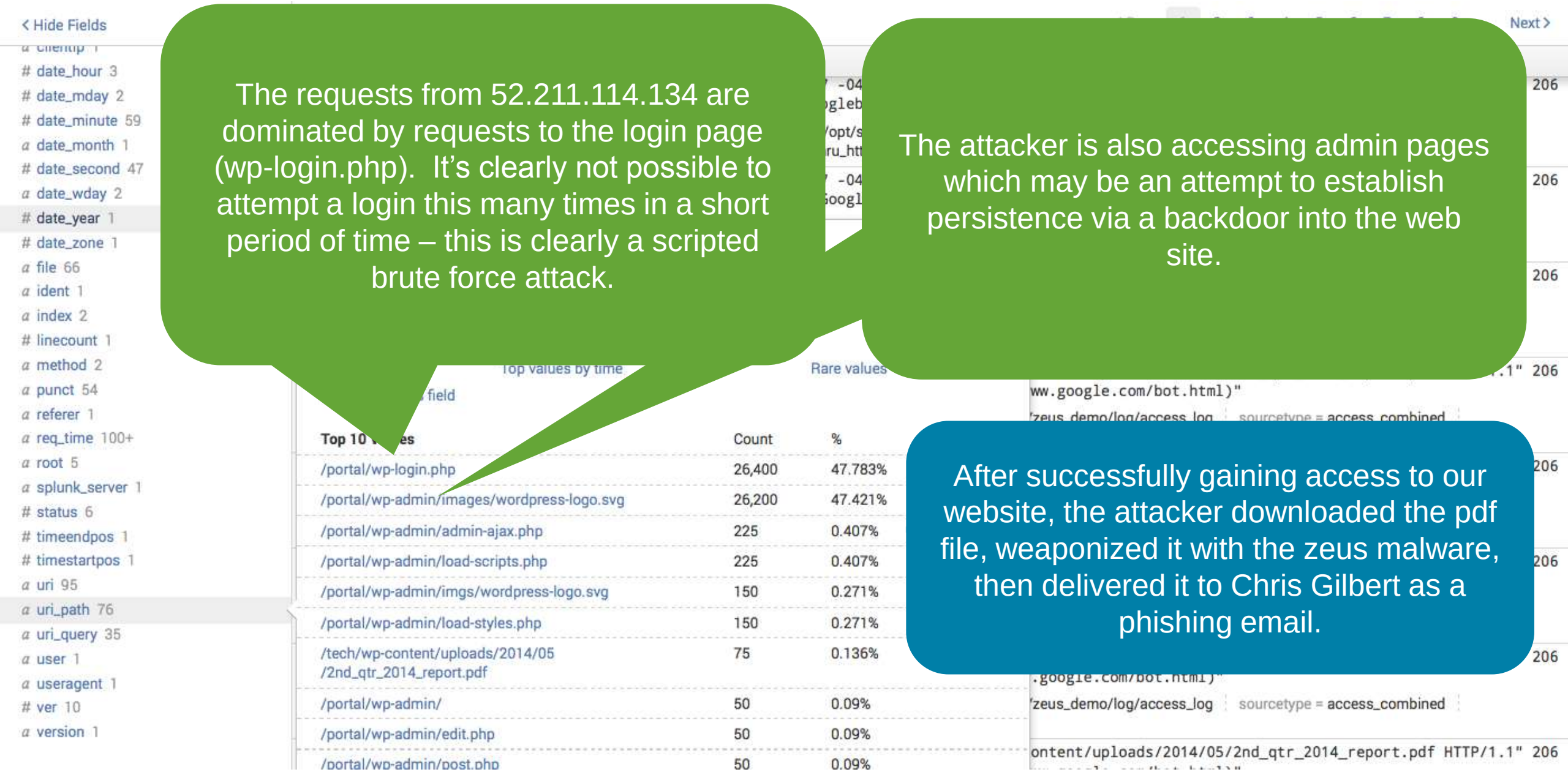
splunk> workshop


That's an abnormally large number of requests sourced from a single IP Address in a ~90 minute window.
This looks like a scripted action given the constant high rate of requests over the below window.
Notice the Googlebot useragent string which is another attempt to avoid raising attention..
Scroll down the dashboard to examine other interesting fields to further investigate.
Scroll Down
splunk> App: Zeus Demo - Microsoft Sysmon (v3)
Administrator Messages Settings Activity Help Find
Search Threat Intelligence Overvi
New Search
* "54.211.114.134"
All time
55,250 events (before
Verbose Mode
Events (2,210) Patterns Statistics Visualization
Format Timeline Zoom Out Zoom to Selection Deselect
List Format 20 Per Page
Hide Fields All Fields
Selected Fields
a host 1
a source 2
a sourcetype 1
a src_ip 1
a threat_intel_source 1
Interesting Fields
bytes 90
a clientip 1
date_hour 3
date_mday 2
date_minute 59
a date_month 1
Time
Event
5/5/14 11:05:47.000 PM
54.211.114.134 - - [06/May/2014:00:05:47 -040
2475168 "-" "Mozilla/5.0 (compatible; Google
host = prod.portal.buttercupgames.com source = /opt/sp
src_ip = 54.211.114.134 threat_intel_source = cymru_http
5/5/14 11:05:47.000 PM
54.211.114.134 - - [06/May/2014:00:05:47 -040
32768 "-" "Mozilla/5.0 (compatible; Googlebo
host = prod.portal.buttercupgames.com source = /opt/sp
src_ip = 54.211.114.134 threat_intel_source = cymru_http
5/5/14 11:05:47.000 PM
54.211.114.134 - - [06/May/2014:00:05:47 -0400] "GET /tech/wp-content/uploads/2014/05/2nd_qtr_2014_report.pdf HTTP
2475168 "-" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
host = prod.portal.buttercupgames.com source = /opt/splunk/Malware/etc/apps/zeus_demo/log/access_log sourcetype = access_combined
src_ip = 54.211.114.134 threat_intel_source = cymru_http
5/5/14 11:05:47.000 PM
54.211.114.134 - - [06/May/2014:00:05:47 -0400] "GET /tech/wp-content/uploads/2014/05/2nd_qtr_2014_report.pdf HTTP
32768 "-" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
host = prod.portal.buttercupgames.com source = /opt/splunk/Malware/etc/apps/zeus_demo/log/access_log sourcetype = access_combined
splunk> workshop

The requests from 52.211.114.134 are dominated by requests to the login page (wp-login.php). It's clearly not possible to attempt a login this many times in a short period of time – this is clearly a scripted brute force attack.

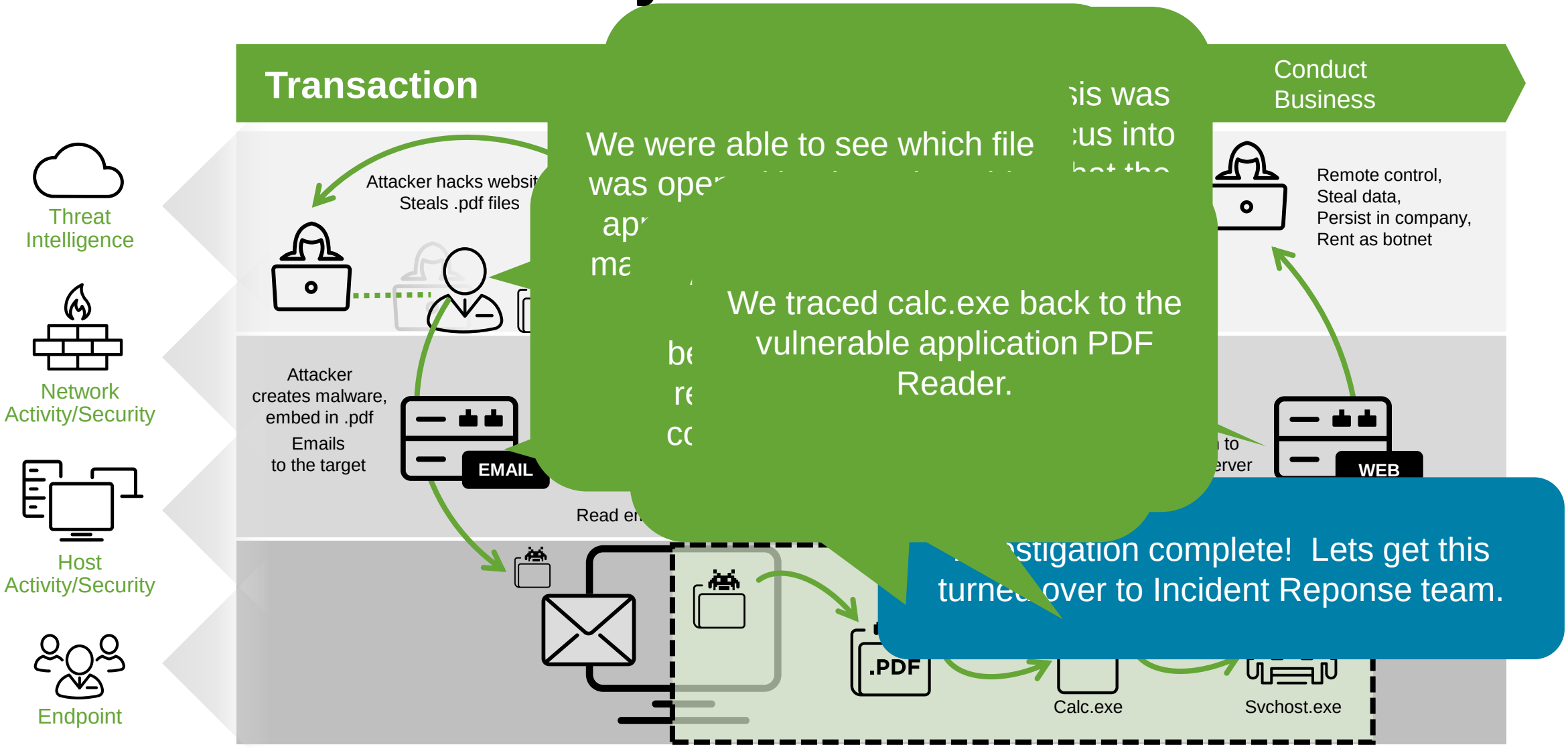
The attacker is also accessing admin pages which may be an attempt to establish persistence via a backdoor into the web site.

After successfully gaining access to our website, the attacker downloaded the pdf file, weaponized it with the zeus malware, then delivered it to Chris Gilbert as a phishing email.

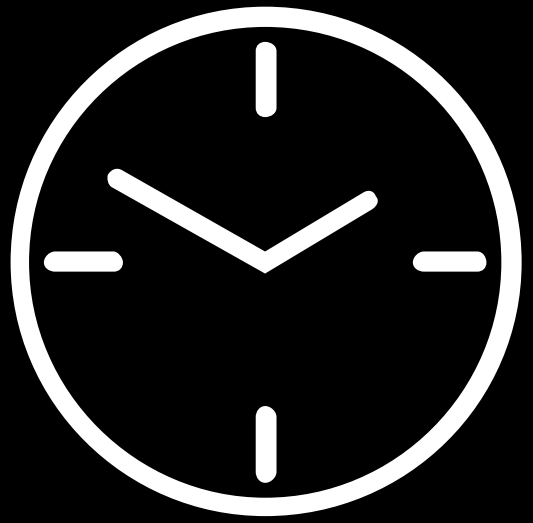


splunk> workshop

Kill Chain Analysis Across Data Sources



splunk> workshop



BREAK

10 MINUTES

splunk> workshop

BONUS!
- SQLi
- DNS Exfilatration
- Splunk Security Essentials

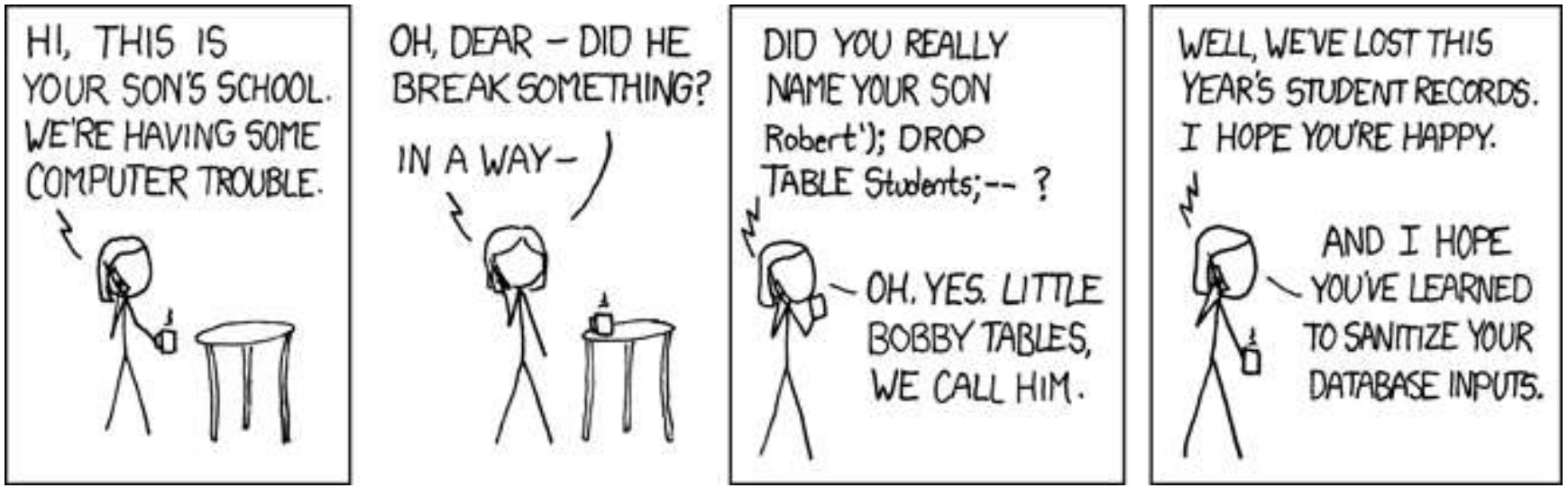
splunk> workshop

SQLi

splunk> workshop

SQL Injection

- SQL injection
- Code injection
- OS commanding
- LDAP injection
- XML injection
- XPath injection
- SSI injection
- IMAP/SMTP injection
- Buffer overflow



Imperva Web Attacks Report, 2015

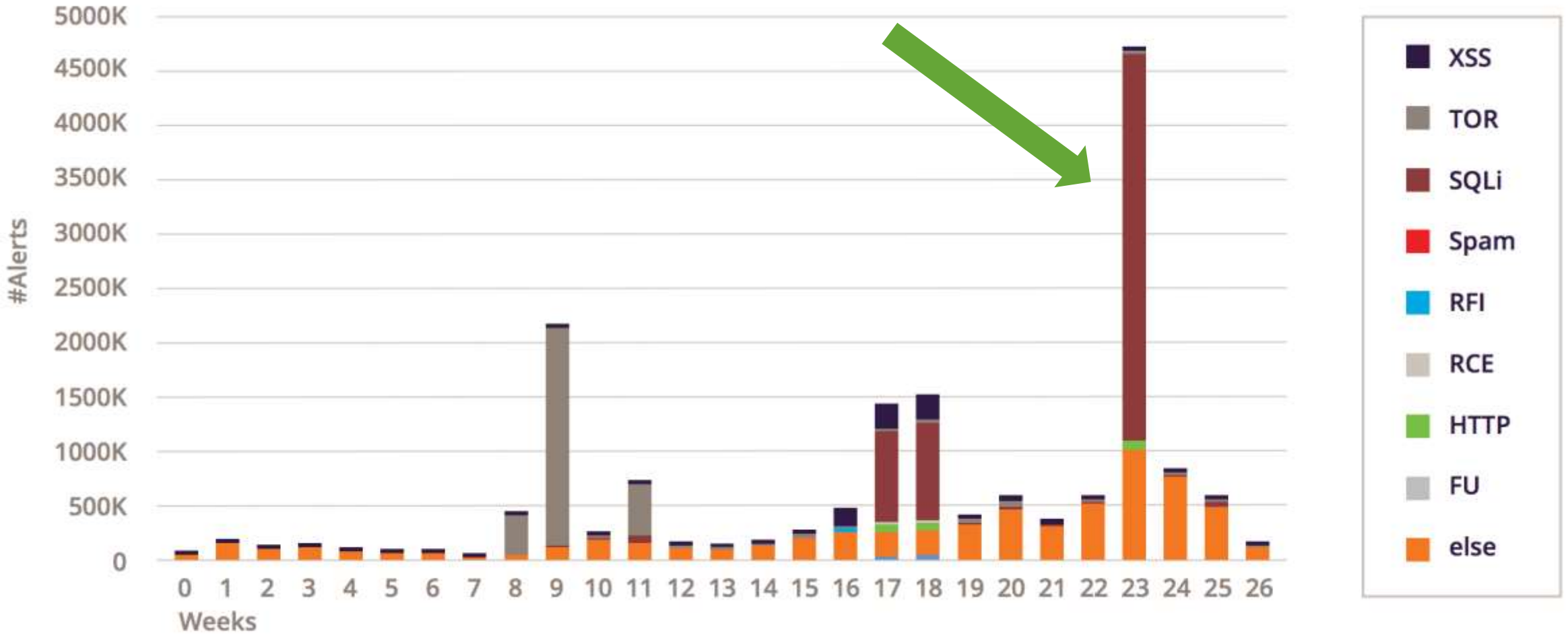
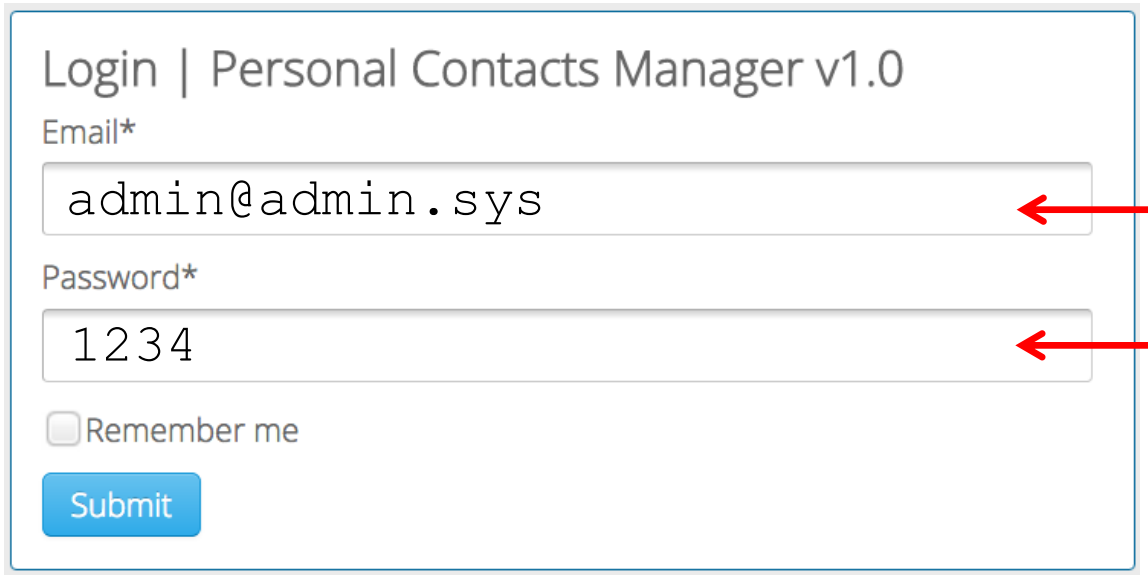


Figure 30: Distribution of Attacks Over Time


ZU 0666', 0, 0); DROP DATABASE TABLICE;

The Anatomy of an SQL Injection Attack



An attacker might supply:

`xxx@xxx.xxx' OR 1 = 1 -- '`

`xxx`

```
SELECT * FROM users WHERE email='xxx@xxx.com'
    OR 1 = 1 -- ' AND password='xxx';
```

SQLI HALL-OF-SHAME

Welcome to the SQL Injection Hall-of-Shame

Shame © by Ranger78

In this day and age it's ridiculous how frequently large organizations are falling prey to SQL Injection (SQLi) which is almost totally preventable as I've written previously.

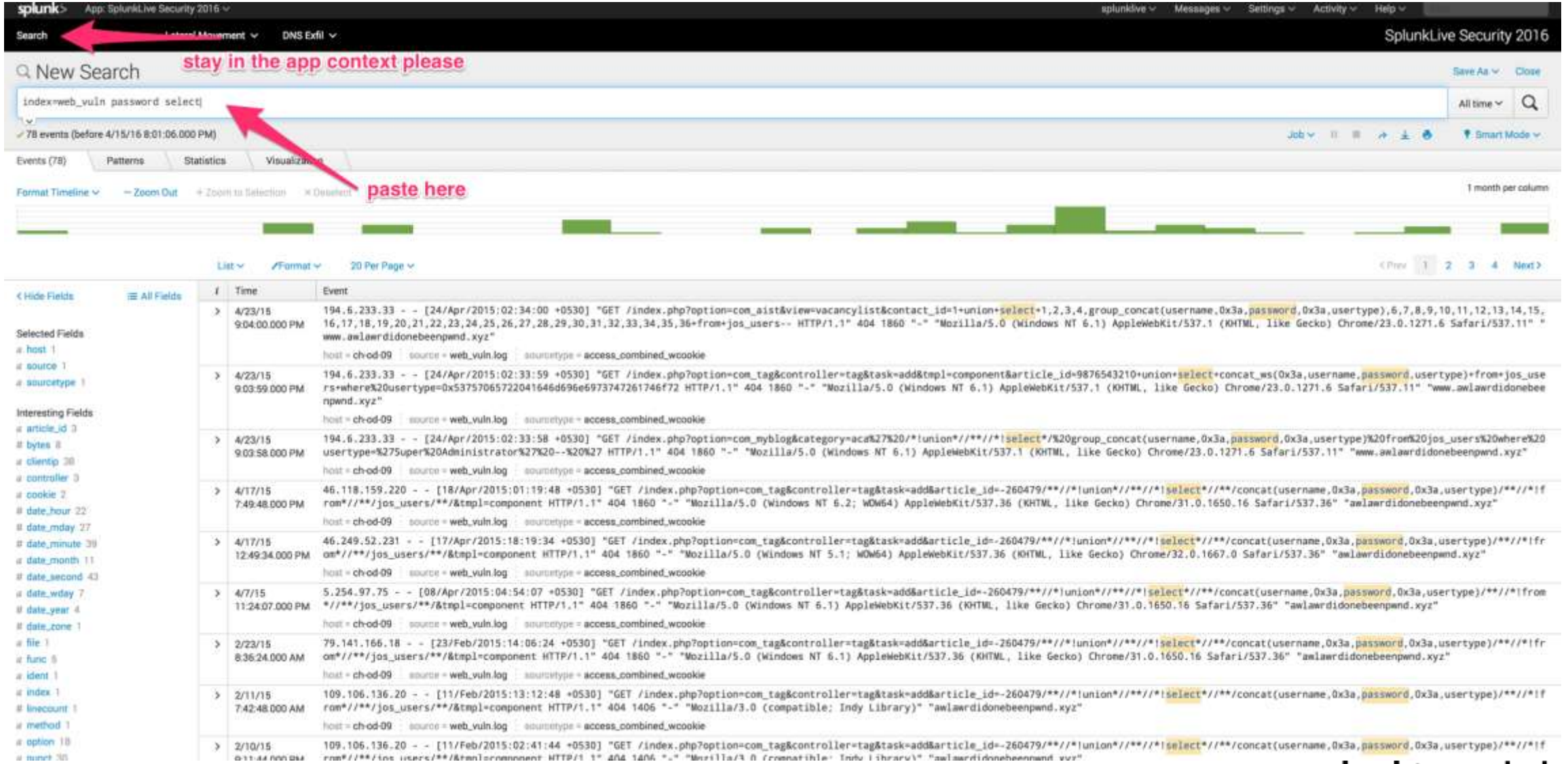
Note that this is a work in progress. If I've missed something you're aware of please let me know in the comments at the bottom of the page.

Don't let this happen to you! For some simple tips see the OWASP SQL Injection Prevention Cheat Sheet. For more security info check out the secur
and Defense
vention: Web

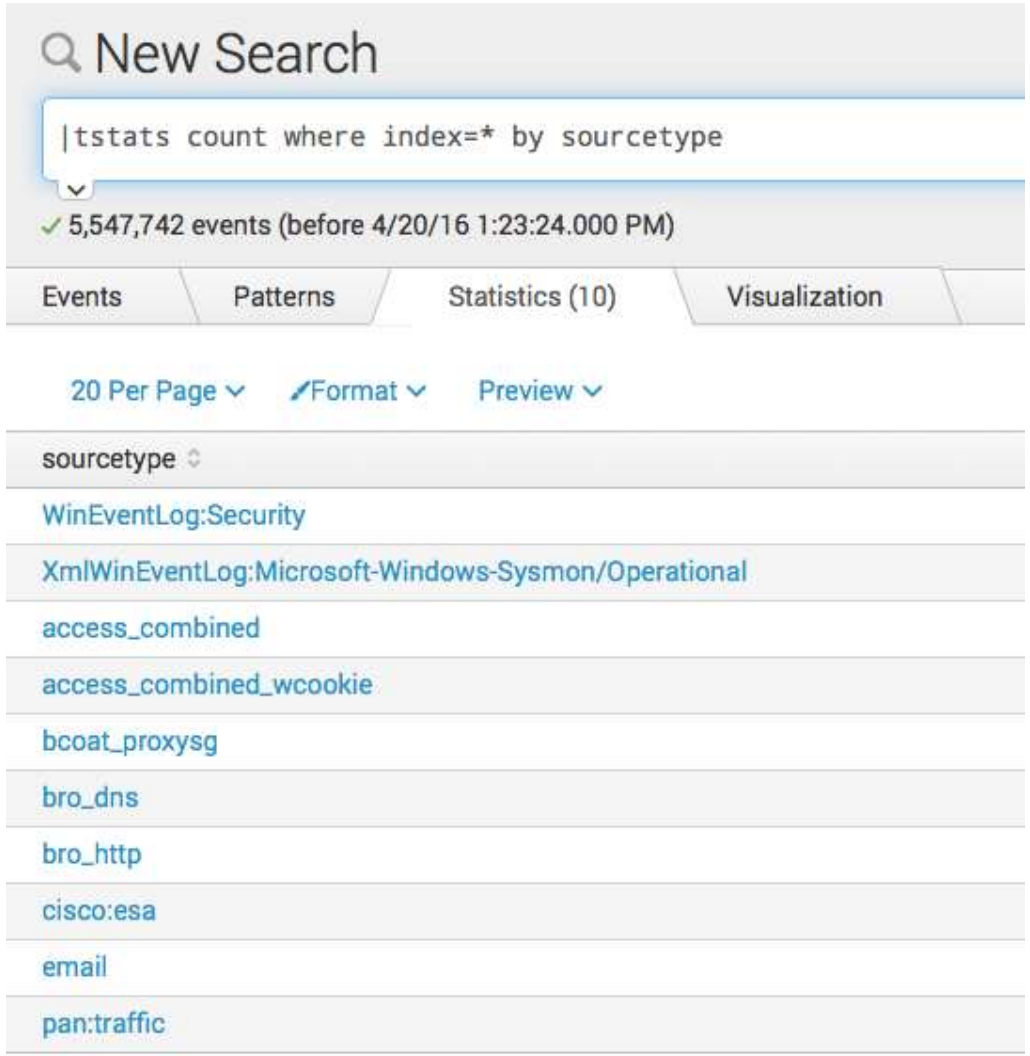
…and so far this year… 39

COMPANY	DATE	RESULTS	REFERENCE
GTA Fan Forum	2016-08	email addresses, passwords and other profile data for 197,000 users.	GTAGaming Hack Blamed on old Vbulletin Software
vBulletin on 11 websites	2016-08	personal information for 27 million accounts from 11 websites	Hackers exploit vBulletin flaw to access 27M accounts on 11 websites
CodeIgniter	2016-08	Vulnerability in PHP framework - unknown breaches.	Future Hosting Advises Users of the CodeIgniter Framework to Update
ReadyDesk	2016-08	vulnerability found in help desk application used by more than 400,000 people.	CERT warns of vulnerabilities in ReadyDesk
Epic Games	2016-08	80,000 users accounts from online forums	Epic Games Forums Hacked
Navis port software at various ports	2016-08	Various port authorities around the world had possible data loss.	Attackers Exploit Flaw in Software Used by US Ports
WordPress Ninja Forms plugin	2016-08	vulnerability on 600,000 sites	WordPress Plugin Fixes SQL Injection Flaw That Let Attackers Dump Site Passwords

index=web_vuln password select



What have we here?



Our learning environment consists of:

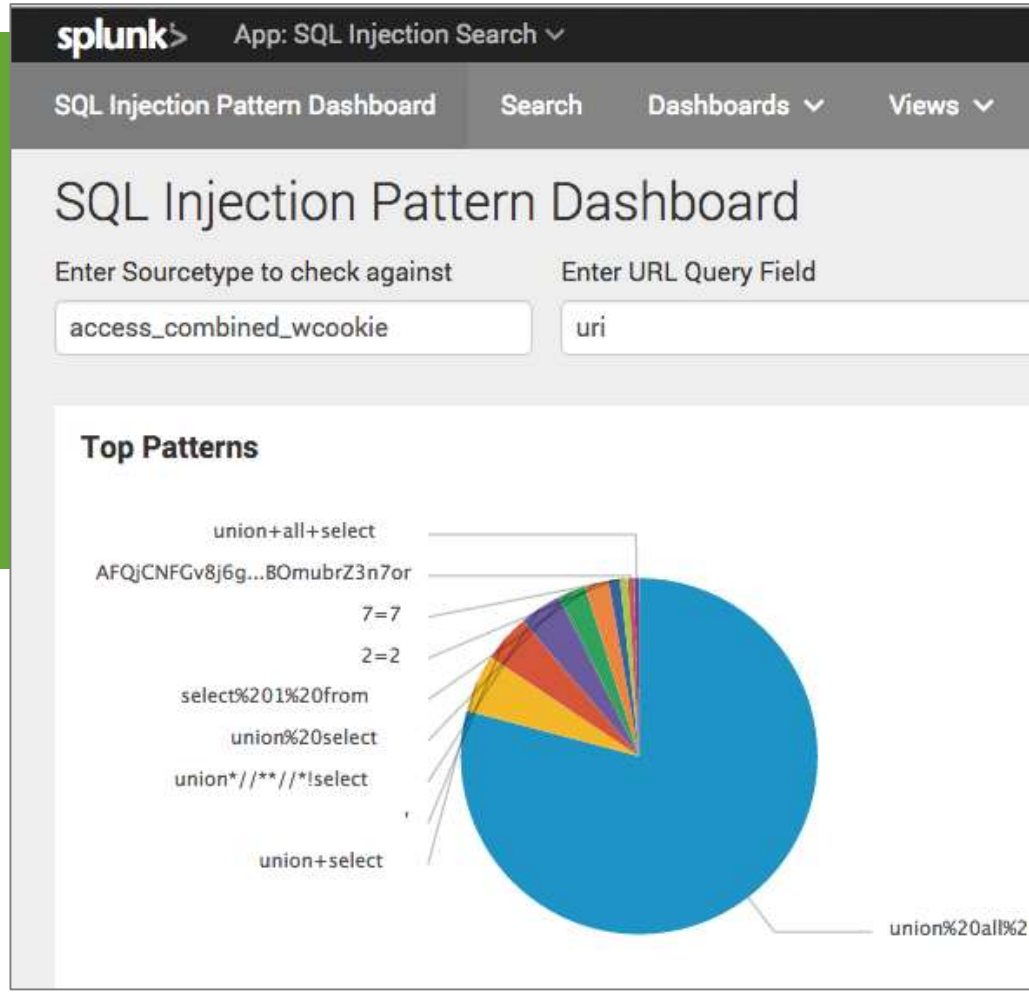
- A bunch of publically-accessible single Splunk servers
- Each with ~5.5M events, from real environments but massaged:
  - Windows Security events
  - Apache web access logs
  - Bro DNS & HTTP
  - Palo Alto traffic logs
  - Some other various bits

SQL Injection Search

https://splunkbase.splunk.com/app/1528/

Search for possible SQL injection in your events:

- looks for patterns in URI query field to see if anyone has injected them with SQL statements
- use standard deviations that are 2.5 times greater than the average length of your URI query field



- Macros used
  - sqlinjection_pattern(sourcetype, uri query field)
  - sqlinjection_stats(sourcetype, uri query field)

splunk> workshop

Regular Expression FTW

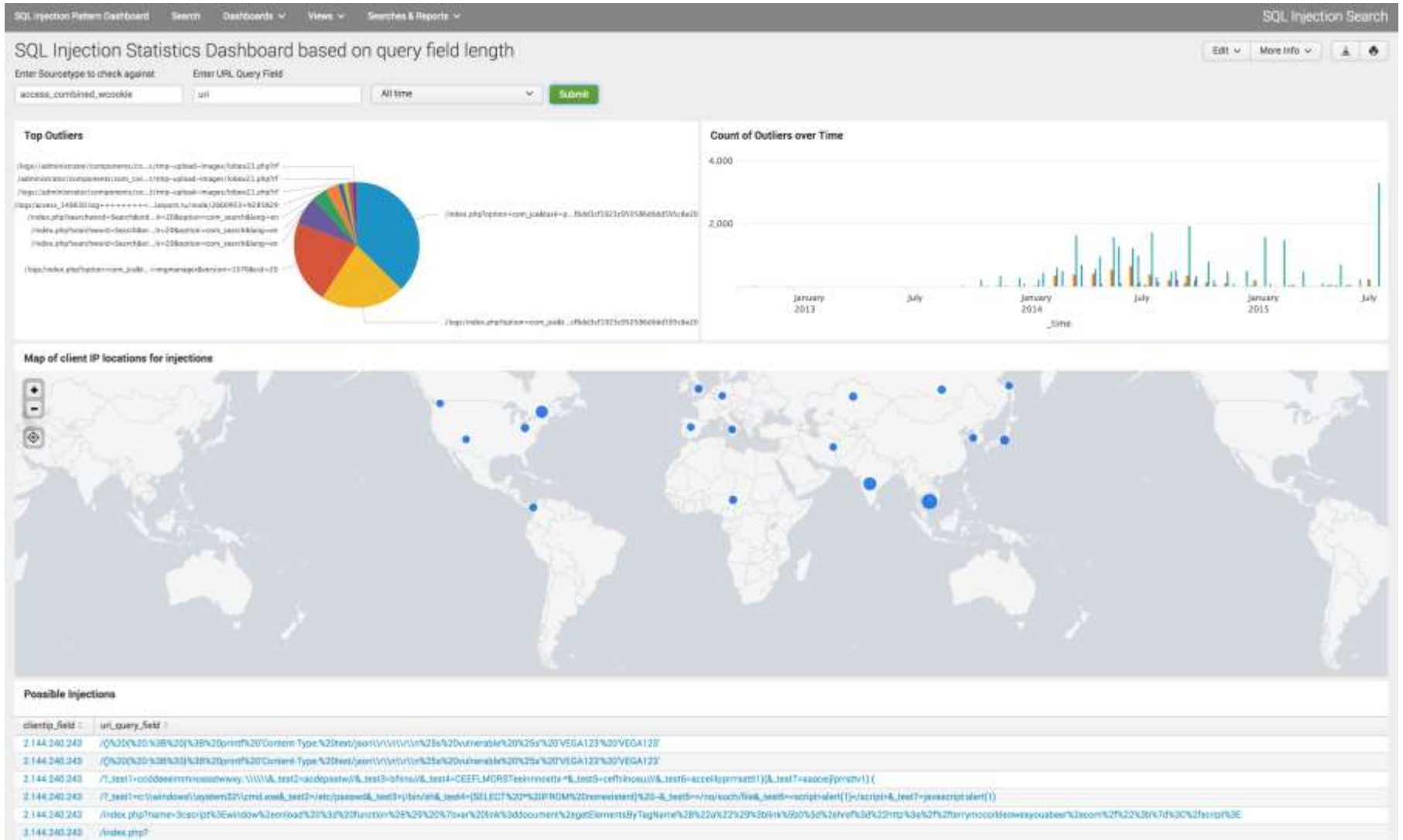
sqlinjection_rex is a *search macro*. It contains:

(?<injection>(?i)select.?from|union.*?select|\'$|delete.*?from|update.*?set|alter.*?table|([\%27|\'](%20)*=(%20)*[\%27|\'])|\w*[%27|\']or)*

Which means: In the string we are given, look for **ANY** of the following matches and put that into the "injection" field.

- Anything containing SELECT followed by FROM
- Anything containing UNION followed by SELECT
- Anything with a ' at the end
- Anything containing DELETE followed by FROM
- Anything containing UPDATE followed by SET
- Anything containing ALTER followed by TABLE
- A %27 OR a ' and then a %20 and any amount of characters then a %20 and then a %27 OR a '
  - Note: %27 is encoded "'" and %20 is encoded <space>
- Any amount of word characters followed by a %27 OR a ' and then "or"

Bonus: Try out the SQL Injection app!



splunk> workshop

Summary: Web Attacks/SQL Injection

- SQL injection provide attackers with easy access to data
- Detecting advanced SQL injection is hard – use an app!
- Understand where SQLi is happening on your network and put a stop to it.
- Augment your WAF with enterprise-wide Splunk searches.

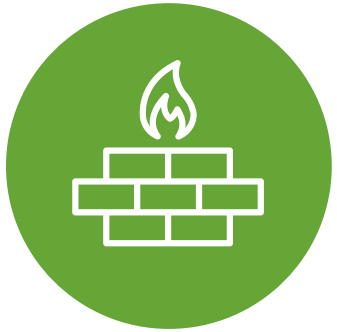
DNS Exfiltration

splunk> workshop

DNS Exfiltration

domain=corp;user=dave;password=12345

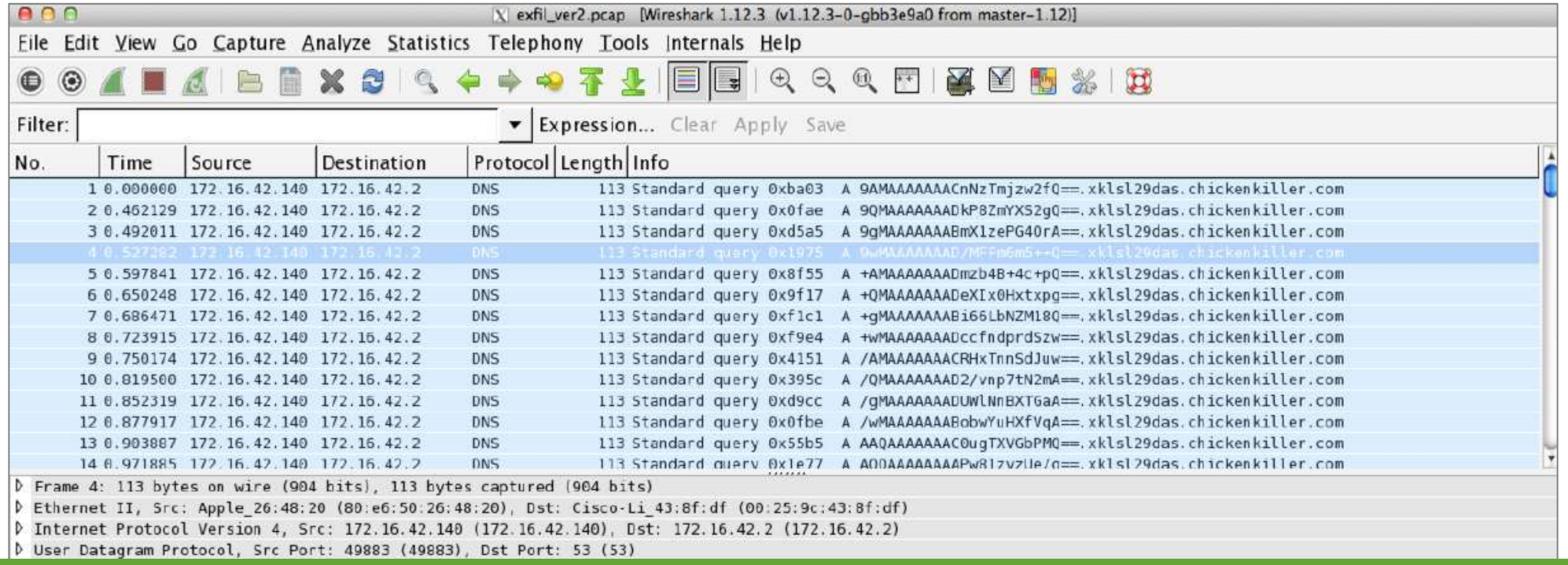
ZG9tYWluPWNvcnA7dXNlcj1kYXZlO3Bhc3N3b3JkPTEyMzQ1DQoNCg==



Firewall

DNS Query:
ZG9tYWluPWNvcnA7dXNlcj1kYXZlO3Bhc3N3b3JkPTEyMzQ1DQoNCg==.attack.com

DNS Exfiltration



DNS exfil tends to be overlooked within an ocean of DNS data.

Let's fix that!

splunk> workshop

DNS Exfiltration

- FrameworkPOS: a card-stealing program that exfiltrates data from the target's network by transmitting it as domain name system (DNS) traffic

"But the big difference is the way how stolen data is exfiltrated: the malware used DNS requests!"
https://blog.gdatasoftware.com/2014/10/23942-new-frameworkpos-variant-exfiltrates-data-via-dns-requests

"… few organizations actually keep detailed logs or records of the DNS traffic traversing their networks — making it an ideal way to siphon data from a hacked network."
http://krebsonsecurity.com/2015/05/deconstructing-the-2014-sally-beauty-breach/#more-30872

URL Toolbox

https://splunkbase.splunk.com/app/2734/

DNS exfil detection – tricks of the trade

- ✓ parse URLs & complicated TLDs (Top Level Domain)
- ✓ calculate Shannon Entropy

```
index=bro sourcetype=bro_dns query=nsa.gov.openwifi.defcon.org| head 1
| `ut_parse(query)`| `ut_shannon(ut_subdomain)` |fields url ut*|transpose
```

✓ 1 event (before 3/9/16 4:03:16.000 PM)

Events | Patterns | Statistics (24) | Visualization

20 Per Page | Format | Preview

column	row 1
url	nsa.gov.openwifi.defcon.org
ut_domain	defcon.org
ut_domain_without_tld	defcon
ut_fragment	None
ut_netloc	nsa.gov.openwifi.defcon.org
ut_params	None
ut_path	None
ut_port	80
ut_query	None
ut_scheme	None
ut_shannon	3.5
ut_subdomain	nsa.gov.openwifi
ut_subdomain_count	3
ut_subdomain_level_1	openwifi
ut_subdomain_level_2	gov
ut_subdomain_level_3	nsa
ut_tld	org

List of provided lookups

- ut_parse_simple(url)
- ut_parse(url, list) or ut_parse_extended(url, list)
- ut_shannon(word)
- ut_countset(word, set)
- ut_suites(word, sets)
- ut_meaning(word)
- ut_bayesian(word)
- ut_levenshtein(word1, word2)

Shannon Entropy

Layman's definition: a score reflecting the randomness or measure of uncertainty of a string

- **Examples**
- The domain *aaaaa.com* has a Shannon Entropy score of **1.8** (very low)
- The domain *google.com* has a Shannon Entropy score of **2.6** (rather low)
- *A00wlkj—(-a.aslkn-C.a.2.sk.esasdfasf1111)-890209uC.4.com* has a Shannon Entropy score of **3** (rather high)

Detecting Data Exfiltration

- TIPS
  - Leverage our Bro DNS data
  - Calculate Shannon Entropy scores
  - Calculate subdomain length
  - Display details

```
index=bro sourcetype=bro_dns
| `ut_parse(query)`
| `ut_shannon(ut_subdomain)`
| eval sublen =
length(ut_subdomain)
| table ut_domain ut_subdomain
ut_shannon sublen
```

Detecting Data Exfiltration

- TIPS
  - Leverage our Bro DNS data
  - Calculate Shannon Entropy scores
  - Calculate subdomain length
  - Display count, scores, lengths, deviations

```
… | stats
count
avg(ut_shannon) as avg_sha
avg(sublen) as avg_sublen
stdev(sublen) as stdev_sublen
by ut_domain
| search avg_sha>3
avg_sublen>20 stdev_sublen<2
```

Detecting Data Exfiltration

- **RESULTS**
  - Exfiltrating data requires many DNS requests – look for high counts
  - DNS exfiltration to mooo.com and chickenkiller.com

	ut_domain	count	avg_sha	avg_sublen	stdev_sublen	subdomain_samples
1	mooo.com	15497	3.839370	34.990514	0.531142	+0eaaaaaaaanduocqspvfa==.xklsl29das +0iaaaaaaabzuil7pzmkxa==.xklsl29das +0maaaaaaabphjehptqkbg==.xklsl29das +0qaaaaaaaahruabi2fmcg==.xklsl29das +0uaaaaaaad20fapu32nga==.xklsl29das
2	chickenkiller.com	1971	3.749215	35.000000	0.000000	+aeaaaaaaaakicagzgvzyw==.xklsl29das +aiaaaaaaabiawegzm9yia==.xklsl29das +amaaaaaaabldyagywn0aq==.xklsl29das +aqaaaaaaablcibozxvtyq==.xklsl29das +auaaaaaaaagy29yzglhba==.xklsl29das
3	nerd.dk	48	3.887892	26.125000	0.732963	104.92.136.41.zz.countries 121.27.152.194.zz.countries

splunk> workshop

Summary: DNS exfiltration

- Exfiltration by DNS and ICMP is a very common technique
- Many organizations do not analyze DNS activity – do not be like them!
- No DNS logs? No Splunk Stream? Look at FW byte counts

Splunk Security Essentials

splunk> workshop

Security Essentials: Free as in Beer

splunk> workshop

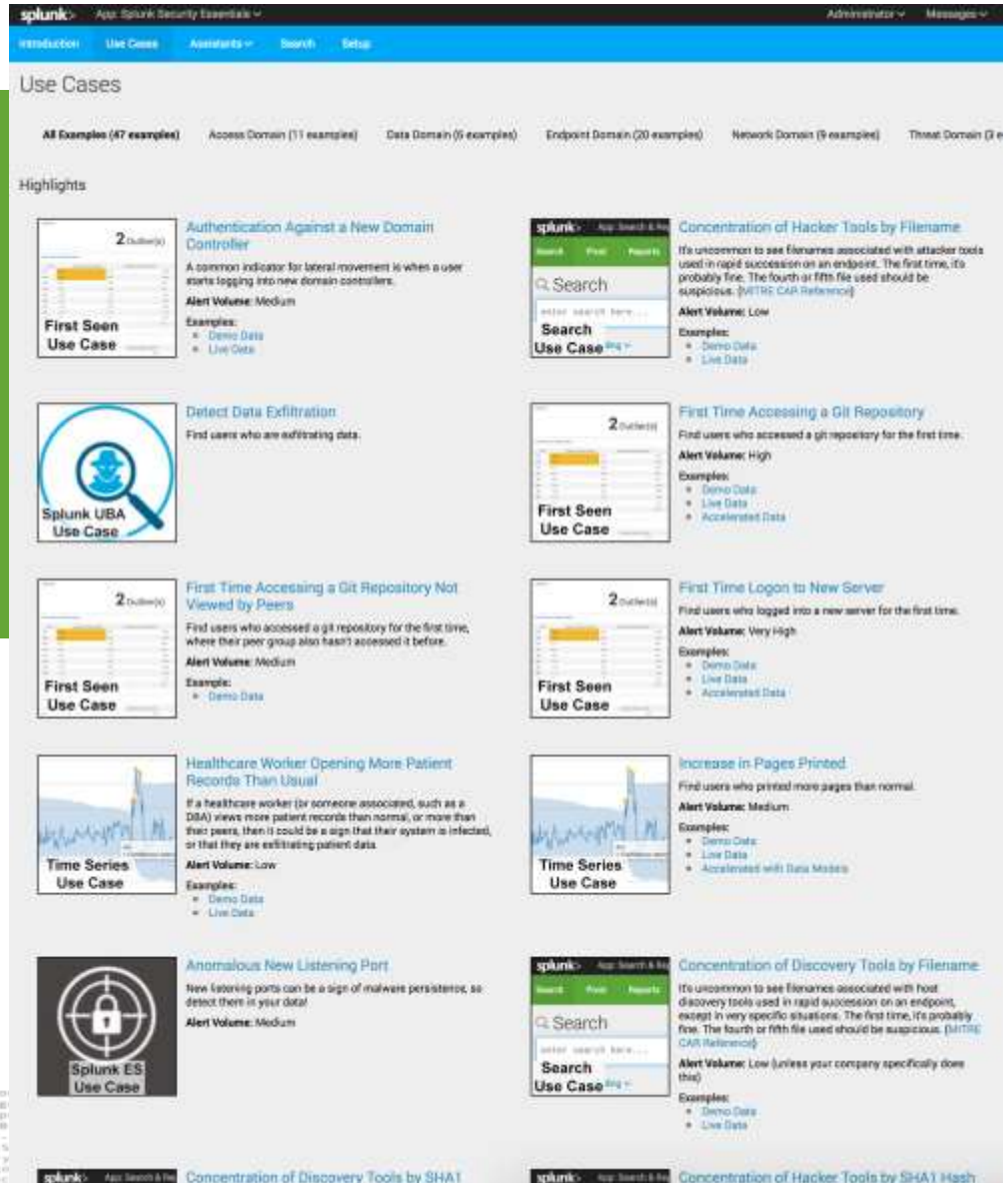
Splunk Security Essentials

https://splunkbase.splunk.com/app/3435/

Identify bad guys in your environment:

- ✓ 45+ use cases common in UEBA products, all free on Splunk Enterprise
- ✓ Target external attackers and insider threat
- ✓ Scales from small to massive companies
- ✓ Save from the app, send results to ES/UBA

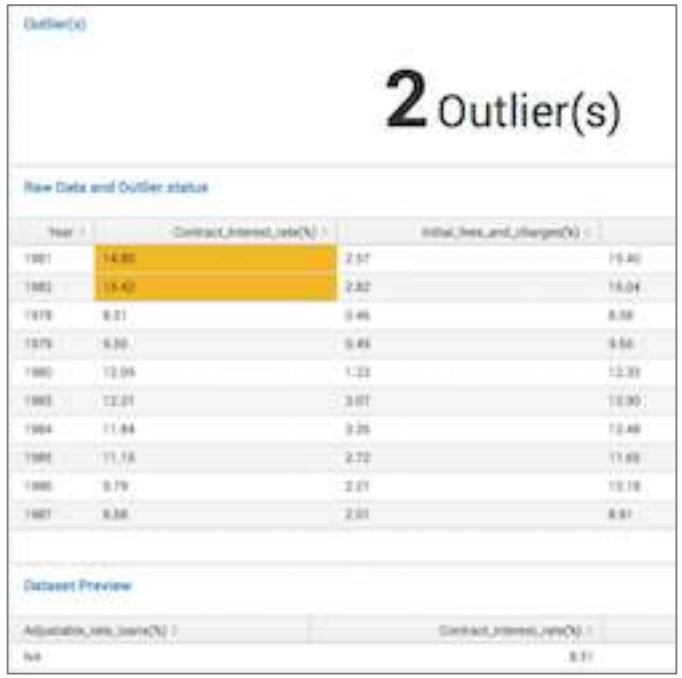
You can solve use cases today for free, then use Splunk UBA for advanced ML detection.



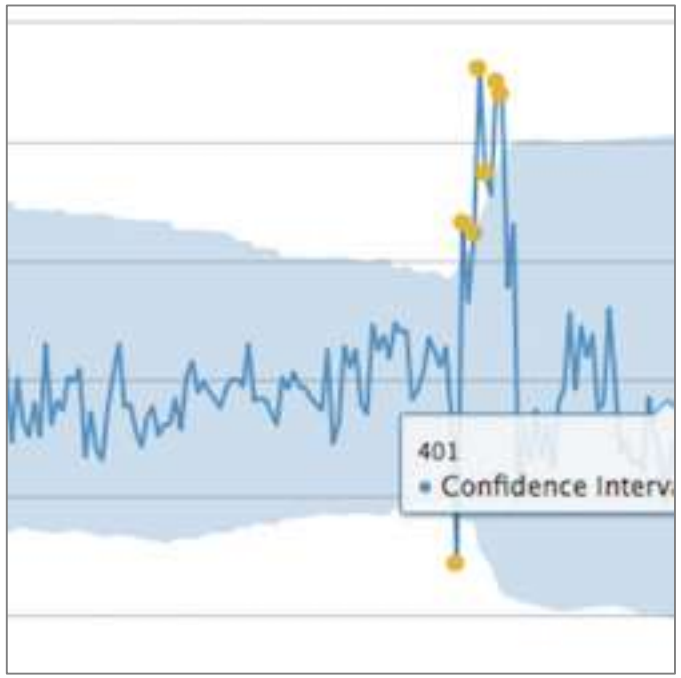
Splunk Security Essentials

Types of Use Cases

- First Time Seen Powered by Stats



- Time Series Analysis With Standard Deviation



- General Security Analytics Searches

splunk> workshop

Splunk Security Essentials

Data Sources

splunk>

Firewall

Logs

Email

Bitbucket

Source Code Repository

Cerner

Electronic Medical Records

Windows

Windows Sysmon

splunk> workshop

How does the app work?

- Leverages primarily | stats for UEBA
- Also implements several advanced Splunk searches (URL Toolbox, etc.)

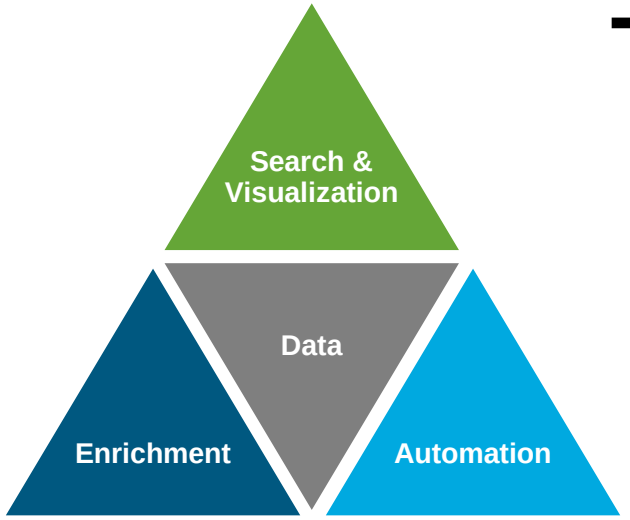
How does the app scale?

- App automates the utilization of high scale techniques
- Summary indexing for Time Series, caching in lookup for First Time

Splunk Enterprise Security

splunk> workshop

Threat Hunting With Splunk



Threat Hunting Data Enrichment

Threat Hunting Automation

Ingest & Onboard Any Threat Hunting Machine Data Source

Search & Visualise Relationships for Faster Hunting

Splunk Enterprise Security

- Security Analytics Platform -

User Behavior Analytics

- Security Data Science Platform -

Splunk Enterprise

- Big Data Analytics Platform -

Data Science & Machine Learning

Automated Analytics

Visualisation

Data & Intelligence Enrichment

Data Search

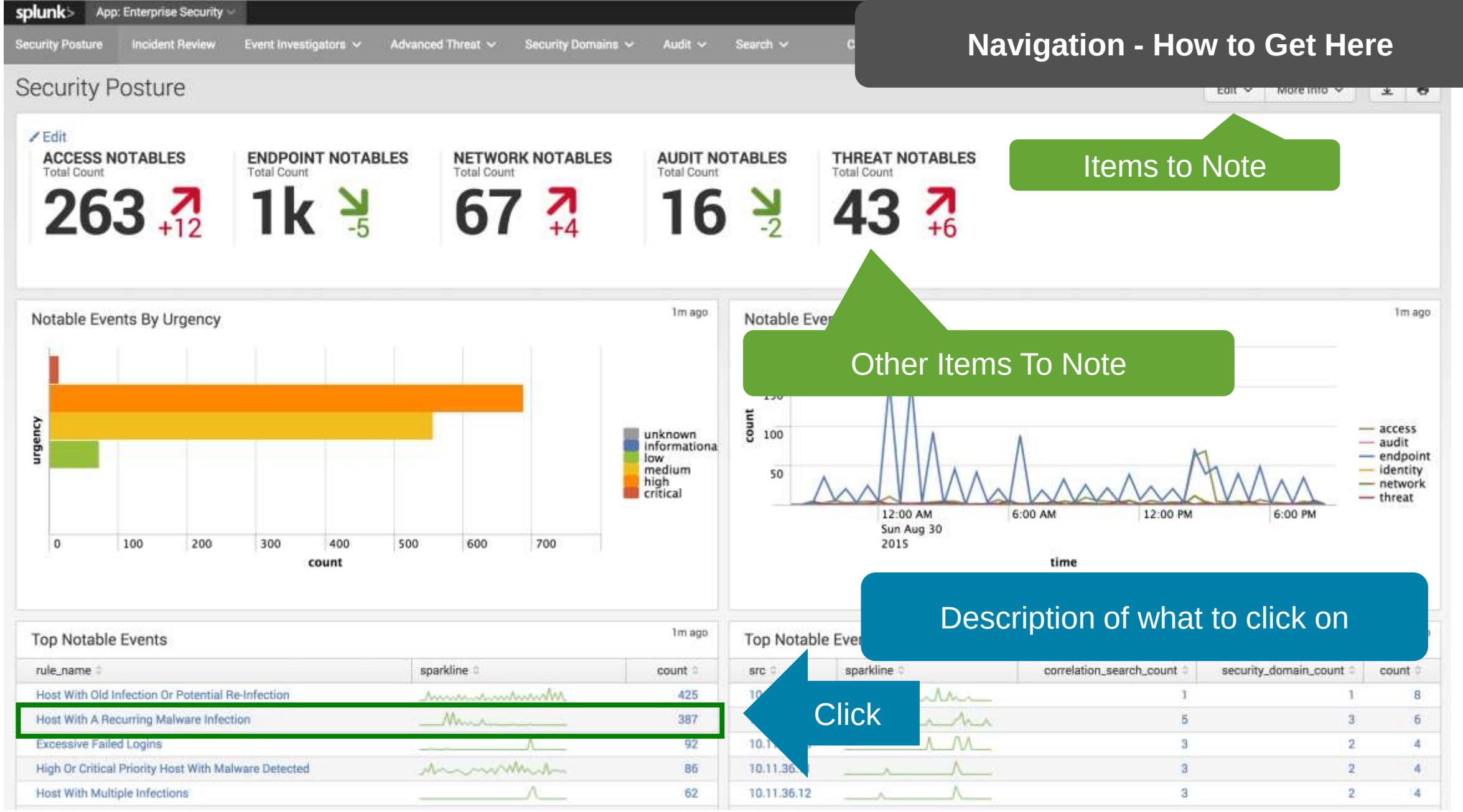
Hypotheses

Maturity

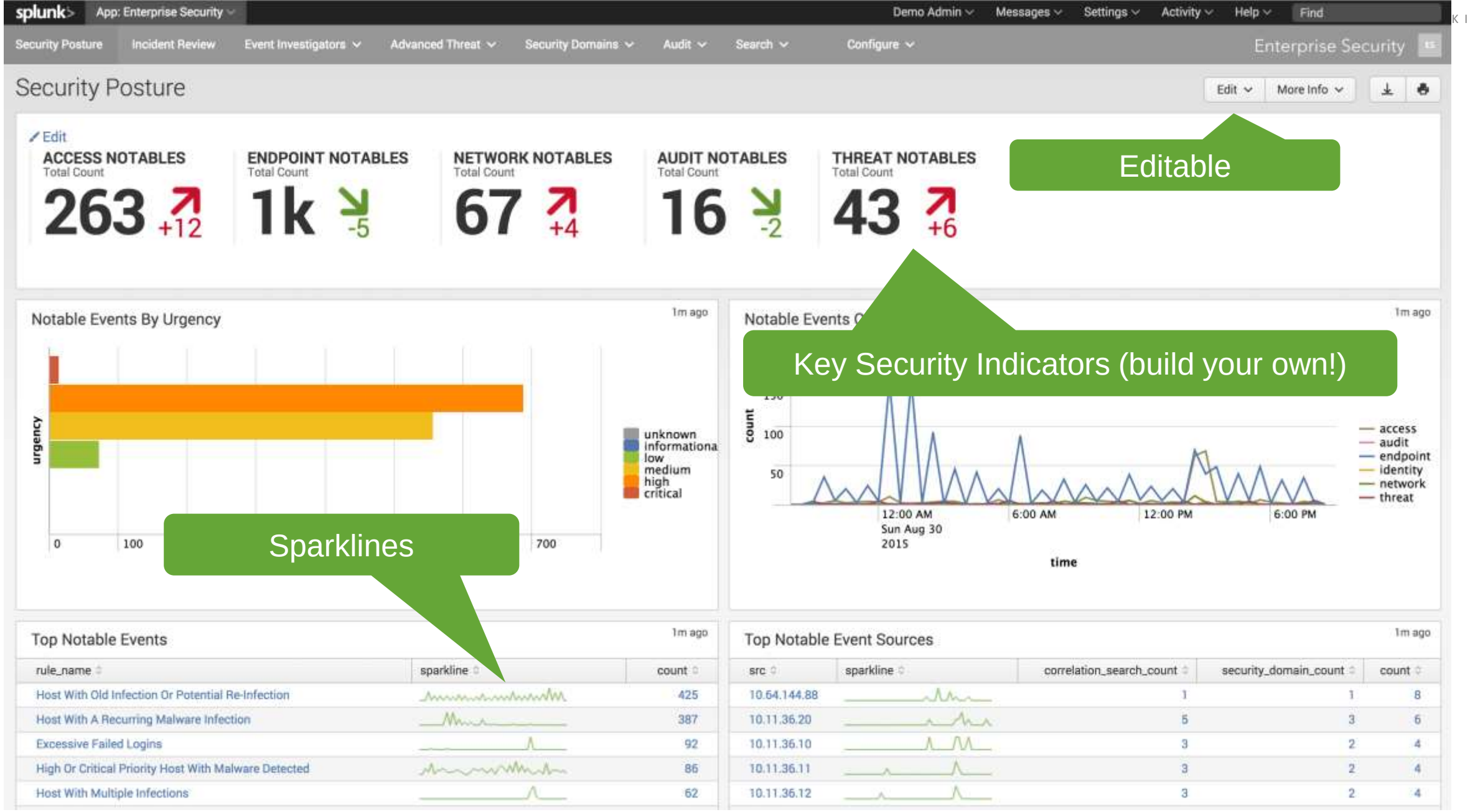
splunk>

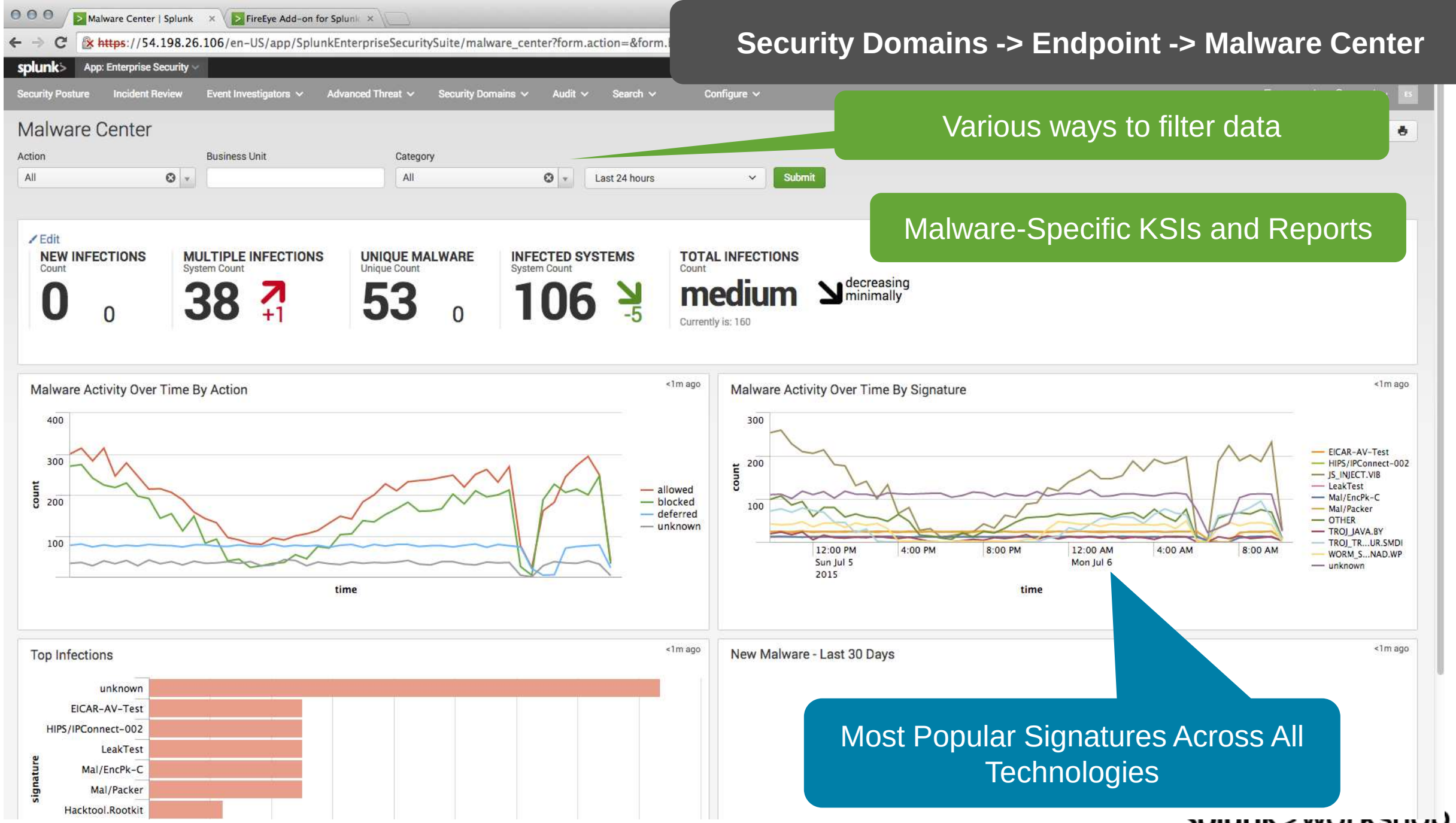
splunk> workshop

Navigation - How to Get Here



splunk> workshop


splunk> App: Enterprise Security
Demo Admin Messages Settings Activity Help Find
Security Posture Incident Review Event Investigators Advanced Threat Security Domains Audit Search Configure
Enterprise Security
Security Posture
Edit More Info
Edit
ACCESS NOTABLES
Total Count
263 +12
ENDPOINT NOTABLES
Total Count
1k -5
NETWORK NOTABLES
Total Count
67 +4
AUDIT NOTABLES
Total Count
16 -2
THREAT NOTABLES
Total Count
43 +6
Editable
Key Security Indicators (build your own!)
Notable Events By Urgency
1m ago
urgency
0
100
700
unknown
informationa
low
medium
high
critical
Sparklines
Notable Events C
1m ago
count
100
50
12:00 AM
Sun Aug 30
2015
6:00 AM
12:00 PM
6:00 PM
time
access
audit
endpoint
identity
network
threat
Top Notable Events
1m ago
rule_name
sparkline
count
Host With Old Infection Or Potential Re-Infection 425
Host With A Recurring Malware Infection 387
Excessive Failed Logins 92
High Or Critical Priority Host With Malware Detected 86
Host With Multiple Infections 62
Top Notable Event Sources
1m ago
src
sparkline
correlation_search_count
security_domain_count
count
10.64.144.88 1 1 8
10.11.36.20 5 3 6
10.11.36.10 3 2 4
10.11.36.11 3 2 4
10.11.36.12 3 2 4

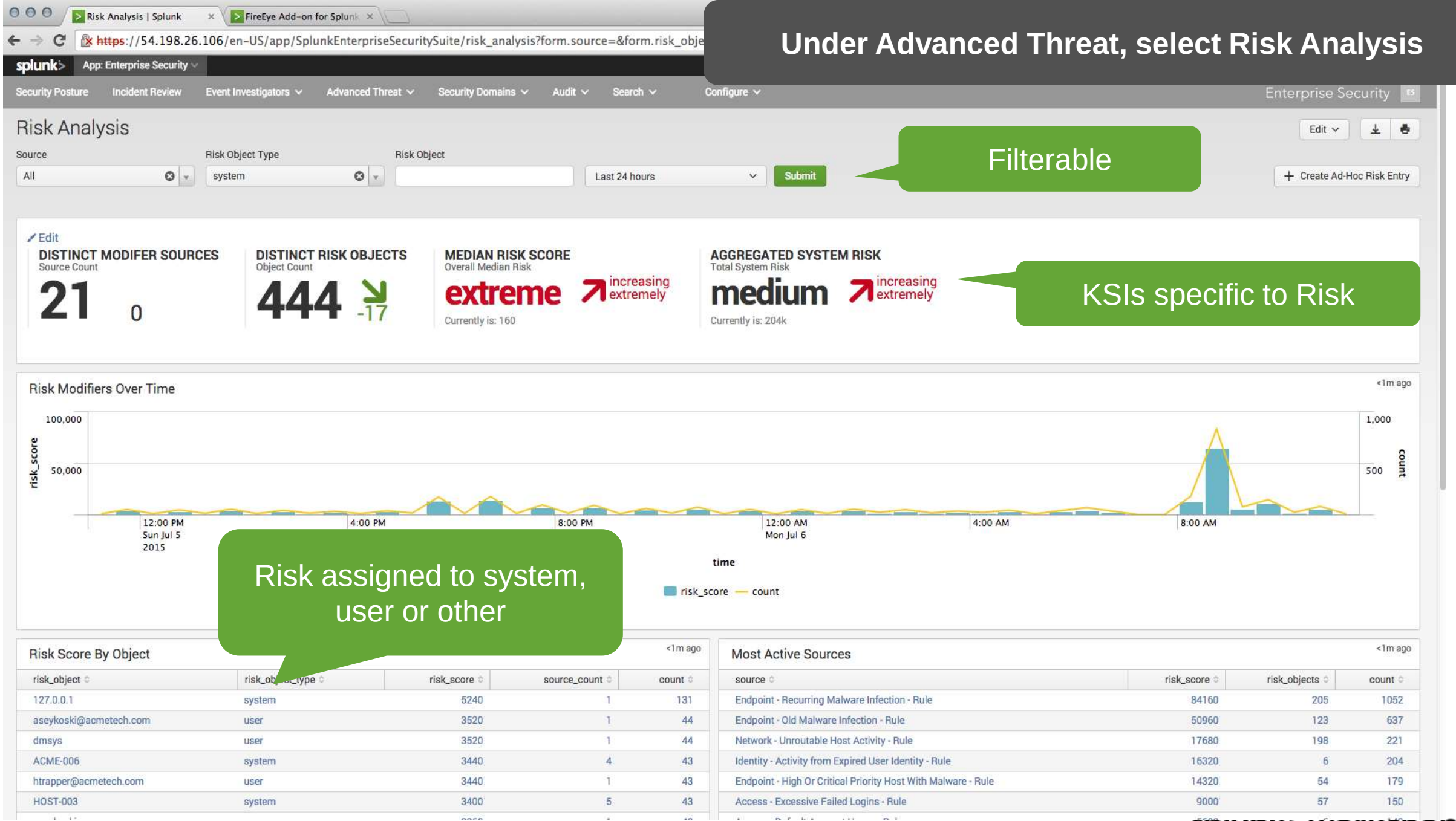


Security Domains -> Endpoint -> Malware Center

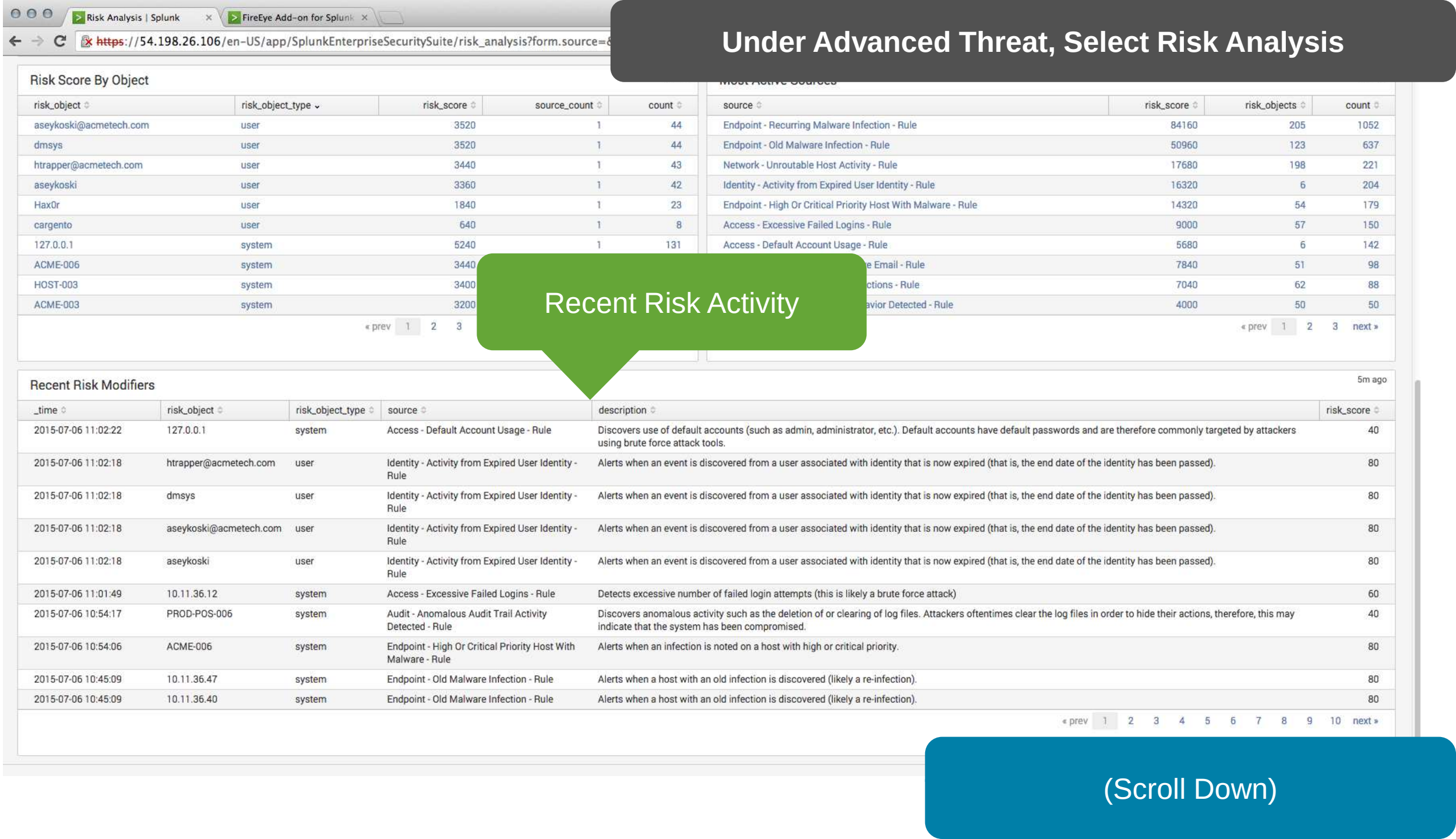
Various ways to filter data

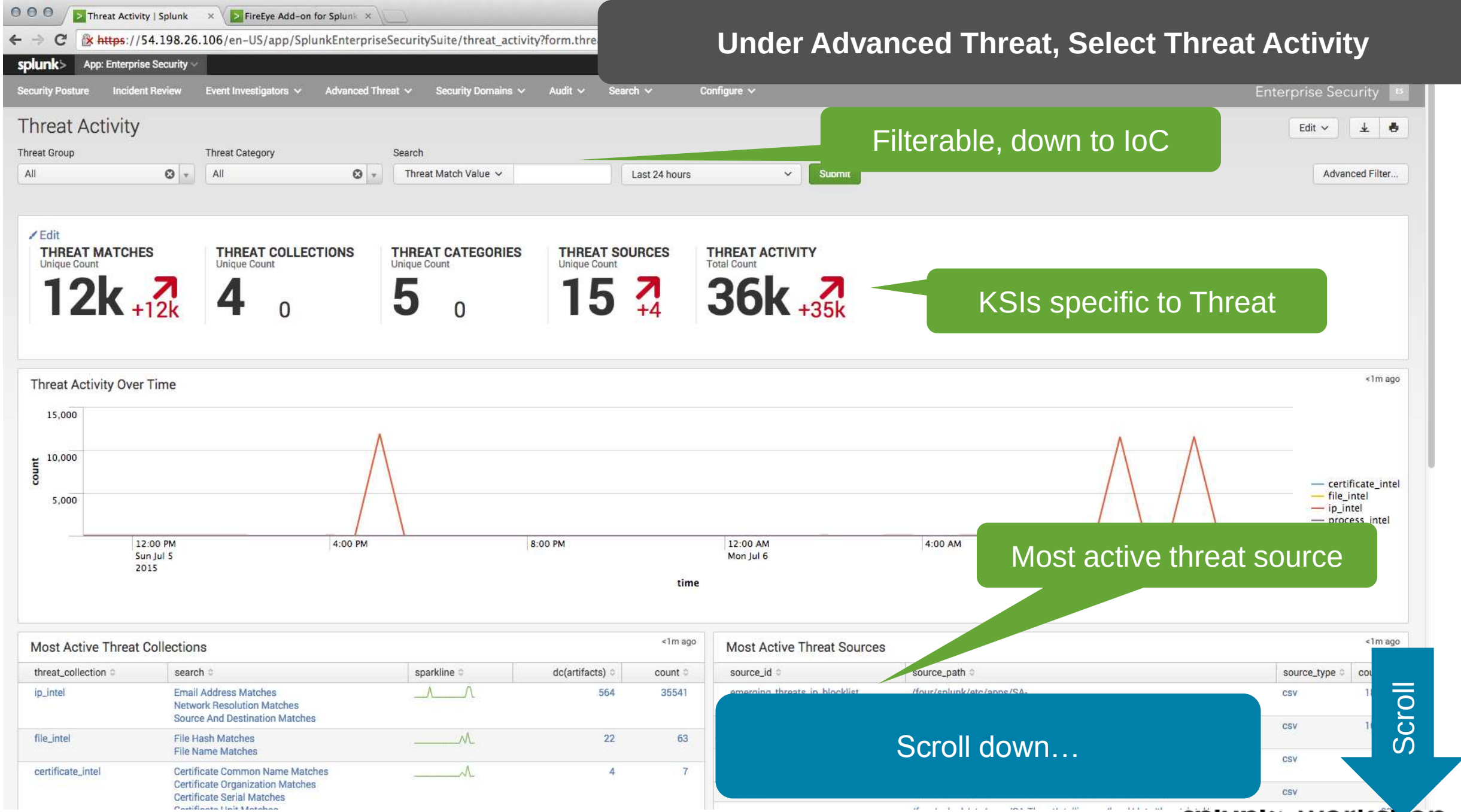
Malware-Specific KSIs and Reports

Most Popular Signatures Across All Technologies



splunk> workshop


Risk Analysis | Splunk
FireEye Add-on for Splunk
https://54.198.26.106/en-US/app/SplunkEnterpriseSecuritySuite/risk_analysis?form.source=
Under Advanced Threat, Select Risk Analysis
Risk Score By Object
risk_object
risk_object_type
risk_score
source_count
count
aseykoski@acmetech.com user 3520 1 44
dmsys user 3520 1 44
htrapper@acmetech.com user 3440 1 43
aseykoski user 3360 1 42
Hax0r user 1840 1 23
cargento user 640 1 8
127.0.0.1 system 5240 1 131
ACME-006 system 3440
HOST-003 system 3400
ACME-003 system 3200
« prev 1 2 3
source
risk_score
risk_objects
count
Endpoint - Recurring Malware Infection - Rule 84160 205 1052
Endpoint - Old Malware Infection - Rule 50960 123 637
Network - Unroutable Host Activity - Rule 17680 198 221
Identity - Activity from Expired User Identity - Rule 16320 6 204
Endpoint - High Or Critical Priority Host With Malware - Rule 14320 54 179
Access - Excessive Failed Logins - Rule 9000 57 150
Access - Default Account Usage - Rule 5680 6 142
e Email - Rule 7840 51 98
ctions - Rule 7040 62 88
avior Detected - Rule 4000 50 50
« prev 1 2 3 next »
Recent Risk Activity
Recent Risk Modifiers
5m ago
_time
risk_object
risk_object_type
source
description
risk_score
2015-07-06 11:02:22 127.0.0.1 system Access - Default Account Usage - Rule Discovers use of default accounts (such as admin, administrator, etc.). Default accounts have default passwords and are therefore commonly targeted by attackers using brute force attack tools. 40
2015-07-06 11:02:18 htrapper@acmetech.com user Identity - Activity from Expired User Identity - Rule Alerts when an event is discovered from a user associated with identity that is now expired (that is, the end date of the identity has been passed). 80
2015-07-06 11:02:18 dmsys user Identity - Activity from Expired User Identity - Rule Alerts when an event is discovered from a user associated with identity that is now expired (that is, the end date of the identity has been passed). 80
2015-07-06 11:02:18 aseykoski@acmetech.com user Identity - Activity from Expired User Identity - Rule Alerts when an event is discovered from a user associated with identity that is now expired (that is, the end date of the identity has been passed). 80
2015-07-06 11:02:18 aseykoski user Identity - Activity from Expired User Identity - Rule Alerts when an event is discovered from a user associated with identity that is now expired (that is, the end date of the identity has been passed). 80
2015-07-06 11:01:49 10.11.36.12 system Access - Excessive Failed Logins - Rule Detects excessive number of failed login attempts (this is likely a brute force attack) 60
2015-07-06 10:54:17 PROD-POS-006 system Audit - Anomalous Audit Trail Activity Detected - Rule Discovers anomalous activity such as the deletion of or clearing of log files. Attackers oftentimes clear the log files in order to hide their actions, therefore, this may indicate that the system has been compromised. 40
2015-07-06 10:54:06 ACME-006 system Endpoint - High Or Critical Priority Host With Malware - Rule Alerts when an infection is noted on a host with high or critical priority. 80
2015-07-06 10:45:09 10.11.36.47 system Endpoint - Old Malware Infection - Rule Alerts when a host with an old infection is discovered (likely a re-infection). 80
2015-07-06 10:45:09 10.11.36.40 system Endpoint - Old Malware Infection - Rule Alerts when a host with an old infection is discovered (likely a re-infection). 80
« prev 1 2 3 4 5 6 7 8 9 10 next »
(Scroll Down)


Under Advanced Threat, Select Threat Activity
Threat Activity | Splunk
FireEye Add-on for Splunk
https://54.198.26.106/en-US/app/SplunkEnterpriseSecuritySuite/threat_activity?form.thre
splunk> App: Enterprise Security
Security Posture
Incident Review
Event Investigators
Advanced Threat
Security Domains
Audit
Search
Configure
Enterprise Security
Threat Activity
Edit
Advanced Filter...
Threat Group
All
Threat Category
All
Search
Threat Match Value
Last 24 hours
Submit
Filterable, down to IoC
Edit
THREAT MATCHES
Unique Count
12k +12k
THREAT COLLECTIONS
Unique Count
4 0
THREAT CATEGORIES
Unique Count
5 0
THREAT SOURCES
Unique Count
15 +4
THREAT ACTIVITY
Total Count
36k +35k
KSIs specific to Threat
Threat Activity Over Time
<1m ago
15,000
10,000
5,000
count
12:00 PM
Sun Jul 5
2015
4:00 PM
8:00 PM
12:00 AM
Mon Jul 6
4:00 AM
time
certificate_intel
file_intel
ip_intel
process_intel
Most active threat source
Most Active Threat Collections
<1m ago
threat_collection
search
sparkline
dc(artifacts)
count
ip_intel
Email Address Matches
Network Resolution Matches
Source And Destination Matches
564
35541
file_intel
File Hash Matches
File Name Matches
22
63
certificate_intel
Certificate Common Name Matches
Certificate Organization Matches
Certificate Serial Matches
4
7
Most Active Threat Sources
<1m ago
source_id
source_path
source_type
csv
Scroll down…
Scroll
splunk>workshop

Under Advanced Threat, Select Threat Activity

ip_intel	Email Address Matches Network Resolution Matches Source And Destination Matches		564	
file_intel	File Hash Matches File Name Matches		22	
certificate_intel	Certificate Common Name Matches Certificate Organization Matches Certificate Serial Matches Certificate Unit Matches Email Address Matches		4	7
process_intel	Process Matches		1	1

	ThreatIntelligence/local/data/threat_intel/iblocklist_spyware.csv		
bad_ips	/four/splunk/etc/apps/SA-zeus-demo/lookups/bad_ips.csv	csv	150
sans	/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/sans.csv	csv	93
mandiant:package-190593d6-1861-4cfe-b212-c016fce1e240	/four/splunk/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel/Appendix_G_IOCs_No_OpenIOC.xml	stix	64
	csv	csv	39
	csv	csv	19
		csv	18
	ificates.xml	stix	7

« prev 1 2 next »

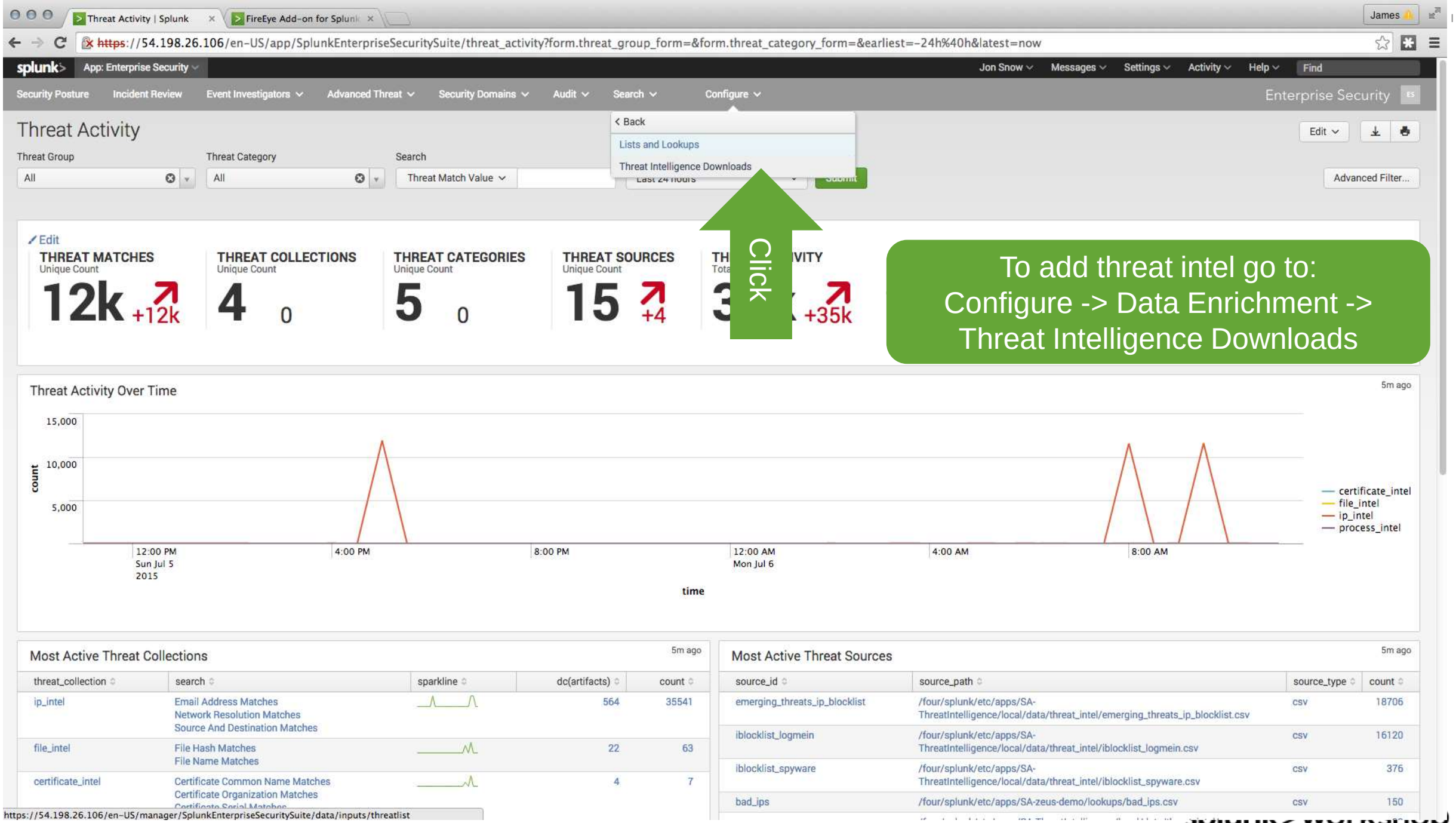
Specifics about recent threat matches

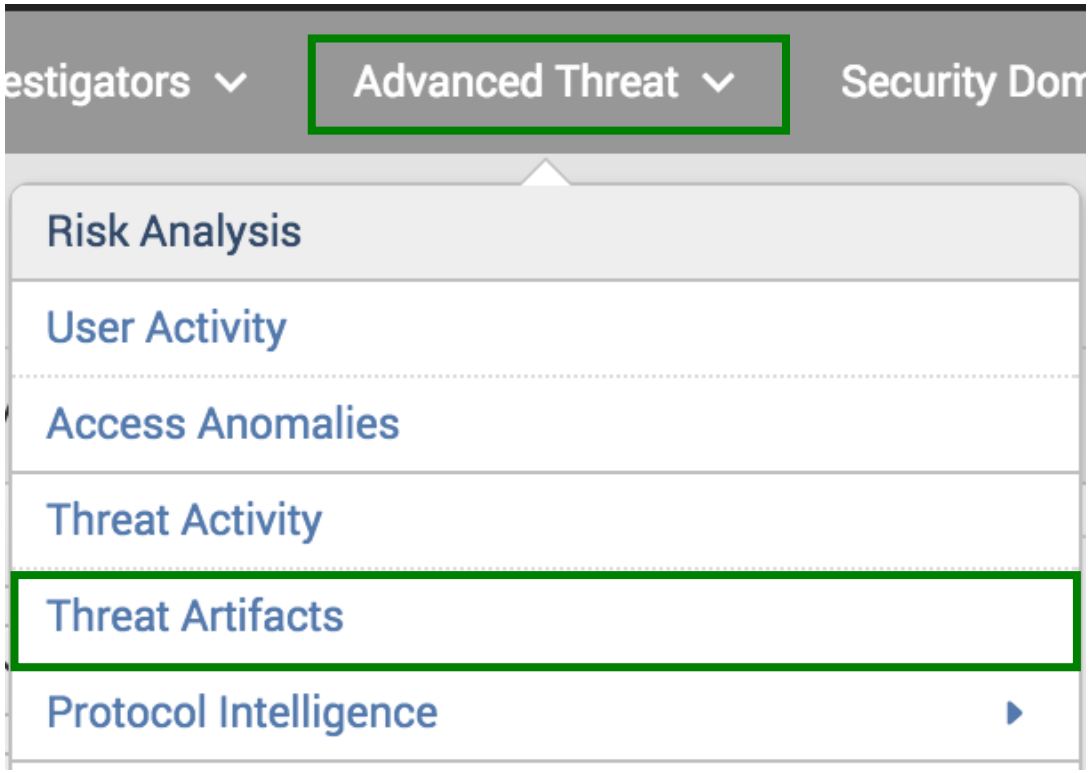
Threat Activity Details

3m ago

_time	threat_match_field	threat_match_value	filter	sourcetype	src	dest	threat_collection	threat_group	threat_category
2015-7-6 11:45:00	dest	116.130.232.192		stream:http	46.22.61.32	116.130.232.192	ip_intel	emerging_threats_ip_blocklist	threatlist
2015-7-6 11:45:00	dest	116.154.114.169		stream:http	22.173.51.112	116.154.114.169	ip_intel	emerging_threats_ip_blocklist	threatlist
2015-7-6 11:45:00	dest	119.232.20.125		stream:http	249.62.211.72	119.232.20.125	ip_intel	emerging_threats_ip_blocklist	threatlist
2015-7-6 11:45:00	dest	25.28.54.208		stream:http	188.170.103.69	25.28.54.208	ip_intel	iblocklist_logmein	threatlist
2015-7-6 11:45:00	src	116.190.110.117		stream:http	116.190.110.117	216.88.184.58	ip_intel	emerging_threats_ip_blocklist	threatlist
2015-7-6 11:45:00	src	152.147.135.107		stream:http	152.147.135.107	144.147.31.191	ip_intel	emerging_threats_ip_blocklist	threatlist
2015-7-6 11:45:00	src	25.128.19.236		stream:http	25.128.19.236	189.218.8.187	ip_intel	iblocklist_logmein	threatlist
2015-7-6 11:45:00	src	25.187.178.36		stream:http	25.187.178.36	68.186.233.221	ip_intel	iblocklist_logmein	threatlist
2015-7-6 11:45:00	src	25.206.155.229		stream:http	25.206.155.229	51.210.248.78	ip_intel	iblocklist_logmein	threatlist
2015-7-6 11:45:00	src	25.5.39.36		stream:http	25.5.39.36	214.8.105.241	ip_intel	iblocklist_logmein	threatlist

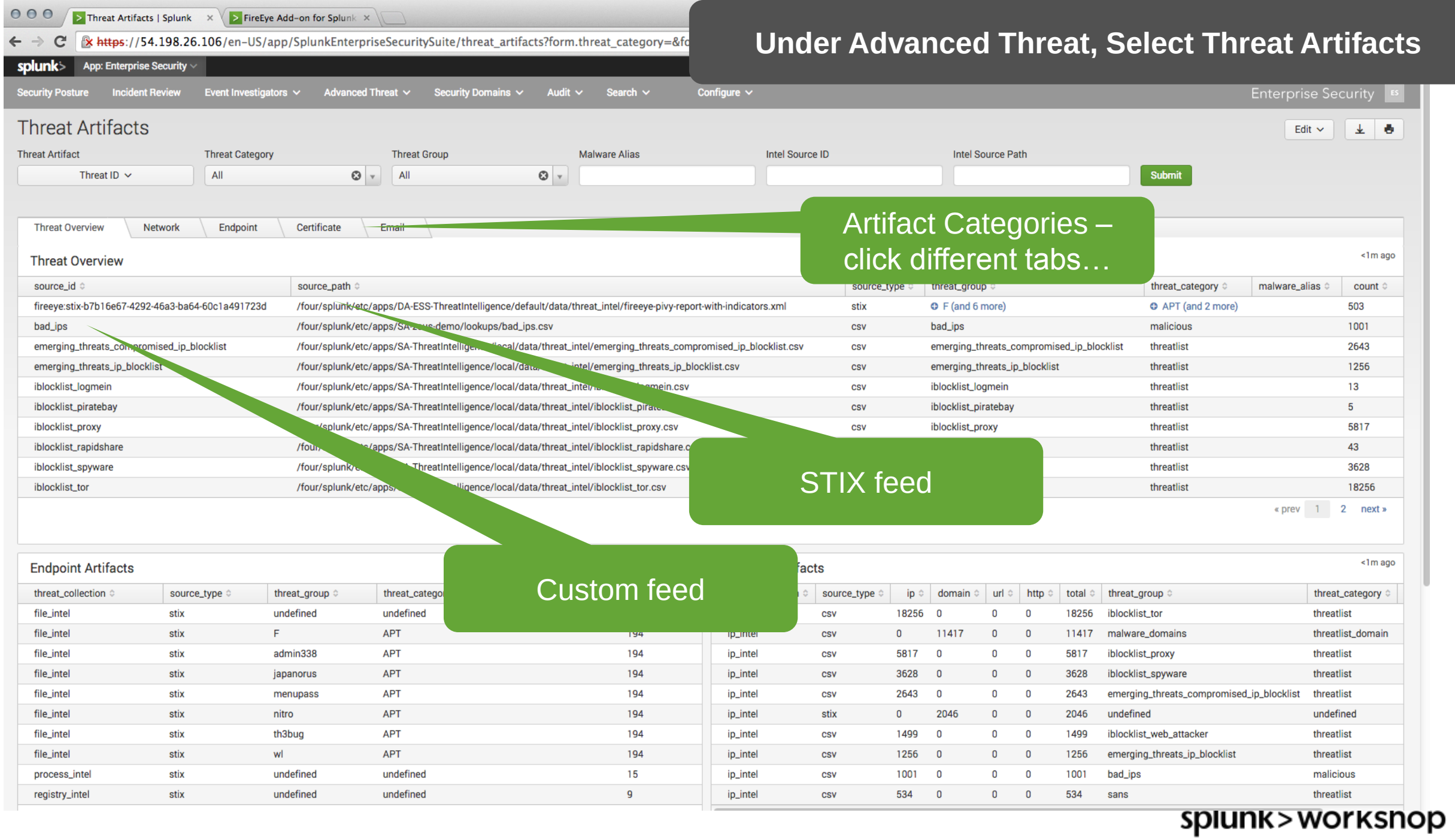
« prev 1 2 3 4 5 6 7 8 9 10 next »

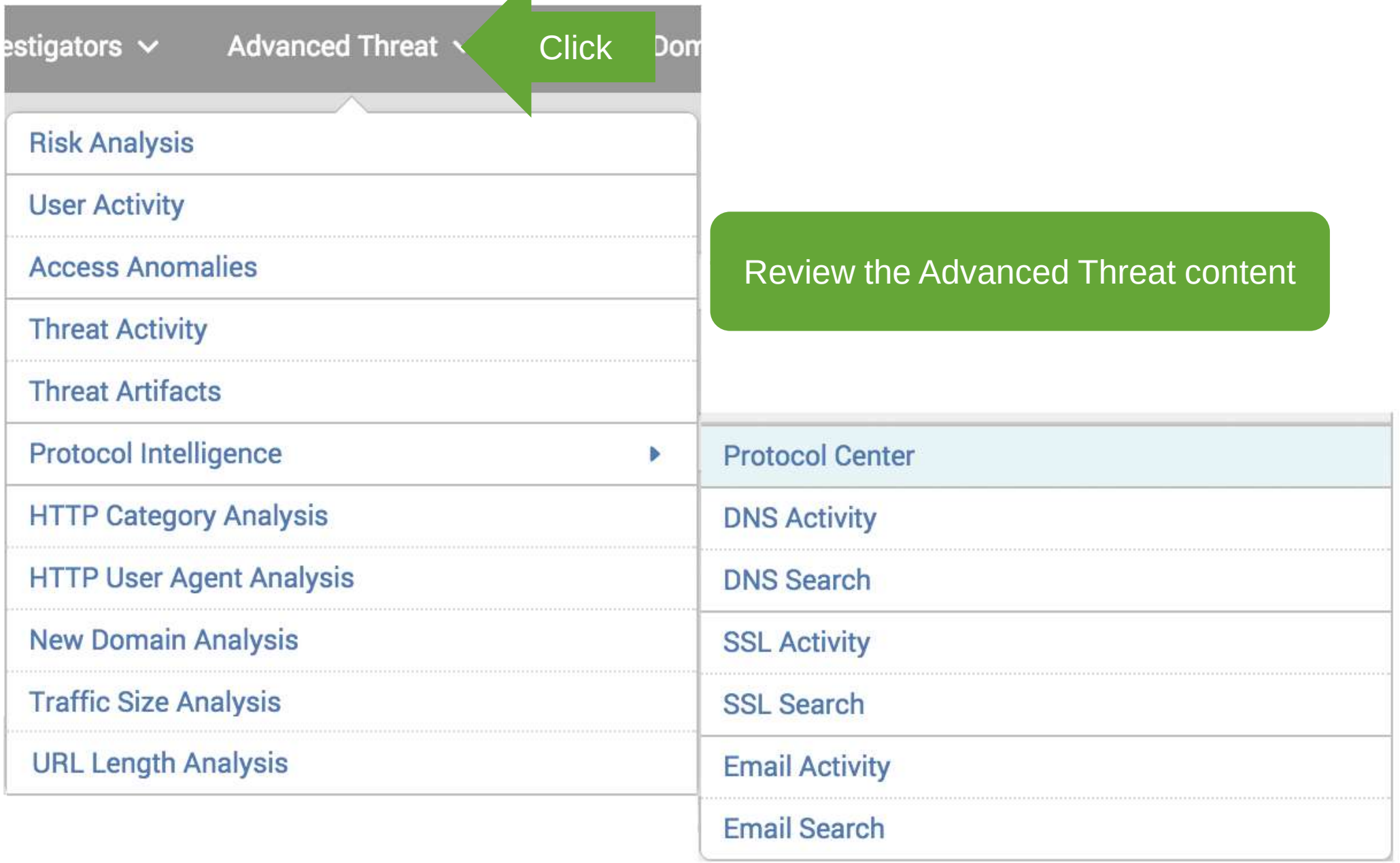

Threat Activity | Splunk
FireEye Add-on for Splunk
James
https://54.198.26.106/en-US/app/SplunkEnterpriseSecuritySuite/threat_activity?form.threat_group_form=&form.threat_category_form=&earliest=-24h%40h&latest=now
splunk> App: Enterprise Security
Jon Snow
Messages
Settings
Activity
Help
Find
Security Posture
Incident Review
Event Investigators
Advanced Threat
Security Domains
Audit
Search
Configure
Enterprise Security
Back
Lists and Lookups
Threat Intelligence Downloads
Threat Activity
Edit
Export
Threat Group
All
Threat Category
All
Search
Threat Match Value
Last 24 hours
Submit
Advanced Filter...
Edit
THREAT MATCHES
Unique Count
12k
+12k
THREAT COLLECTIONS
Unique Count
4
0
THREAT CATEGORIES
Unique Count
5
0
THREAT SOURCES
Unique Count
15
+4
+35k
Click
To add threat intel go to:
Configure -> Data Enrichment ->
Threat Intelligence Downloads
Threat Activity Over Time
5m ago
15,000
10,000
5,000
count
12:00 PM
Sun Jul 5
2015
4:00 PM
8:00 PM
12:00 AM
Mon Jul 6
4:00 AM
8:00 AM
time
certificate_intel
file_intel
ip_intel
process_intel
Most Active Threat Collections
5m ago
threat_collection
search
sparkline
dc(artifacts)
count
ip_intel
Email Address Matches
Network Resolution Matches
Source And Destination Matches
564
35541
file_intel
File Hash Matches
File Name Matches
22
63
certificate_intel
Certificate Common Name Matches
Certificate Organization Matches
4
7
Most Active Threat Sources
5m ago
source_id
source_path
source_type
count
emerging_threats_ip_blocklist
/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/emerging_threats_ip_blocklist.csv
csv
18706
iblocklist_logmein
/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_logmein.csv
csv
16120
iblocklist_spyware
/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_spyware.csv
csv
376
bad_ips
/four/splunk/etc/apps/SA-zeus-demo/lookups/bad_ips.csv
csv
150
https://54.198.26.106/en-US/manager/SplunkEnterpriseSecuritySuite/data/inputs/threatlist



Click “Threat Artifacts”
Under “Advanced Threat”

Click


Under Advanced Threat, Select Threat Artifacts
Threat Artifacts | Splunk
FireEye Add-on for Splunk
https://54.198.26.106/en-US/app/SplunkEnterpriseSecuritySuite/threat_artifacts?form.threat_category=&fo
splunk> App: Enterprise Security
Security Posture
Incident Review
Event Investigators
Advanced Threat
Security Domains
Audit
Search
Configure
Enterprise Security
Threat Artifacts
Edit
Threat Artifact
Threat ID
Threat Category
All
Threat Group
All
Malware Alias
Intel Source ID
Intel Source Path
Submit
Threat Overview
Network
Endpoint
Certificate
Email
Artifact Categories – click different tabs…
Threat Overview
<1m ago
source_id
source_path
source_type
threat_group
threat_category
malware_alias
count
fireeye:stix-b7b16e67-4292-46a3-ba64-60c1a491723d
/four/splunk/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel/fireeye-pivy-report-with-indicators.xml
stix
F (and 6 more)
APT (and 2 more)
503
bad_ips
/four/splunk/etc/apps/SA-[illegible]-demo/lookups/bad_ips.csv
csv
bad_ips
malicious
1001
emerging_threats_compromised_ip_blocklist
/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/emerging_threats_compromised_ip_blocklist.csv
csv
emerging_threats_compromised_ip_blocklist
threatlist
2643
emerging_threats_ip_blocklist
/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/emerging_threats_ip_blocklist.csv
csv
emerging_threats_ip_blocklist
threatlist
1256
iblocklist_logmein
/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_logmein.csv
csv
iblocklist_logmein
threatlist
13
iblocklist_piratebay
/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_piratebay.csv
csv
iblocklist_piratebay
threatlist
5
iblocklist_proxy
/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_proxy.csv
csv
iblocklist_proxy
threatlist
5817
iblocklist_rapidshare
/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_rapidshare.csv
threatlist
43
iblocklist_spyware
/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_spyware.csv
threatlist
3628
iblocklist_tor
/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_tor.csv
threatlist
18256
« prev 1 2 next »
STIX feed
Custom feed
Endpoint Artifacts
<1m ago
threat_collection
source_type
threat_group
threat_category
file_intel stix undefined undefined
file_intel stix F APT 194
file_intel stix admin338 APT 194
file_intel stix japanorus APT 194
file_intel stix menupass APT 194
file_intel stix nitro APT 194
file_intel stix th3bug APT 194
file_intel stix wl APT 194
process_intel stix undefined undefined 15
registry_intel stix undefined undefined 9
source_type
ip
domain
url
http
total
threat_group
threat_category
csv 18256 0 0 0 18256 iblocklist_tor threatlist
csv 0 11417 0 0 11417 malware_domains threatlist_domain
ip_intel csv 5817 0 0 0 5817 iblocklist_proxy threatlist
ip_intel csv 3628 0 0 0 3628 iblocklist_spyware threatlist
ip_intel csv 2643 0 0 0 2643 emerging_threats_compromised_ip_blocklist threatlist
ip_intel stix 0 2046 0 0 2046 undefined undefined
ip_intel csv 1499 0 0 0 1499 iblocklist_web_attacker threatlist
ip_intel csv 1256 0 0 0 1256 emerging_threats_ip_blocklist threatlist
ip_intel csv 1001 0 0 0 1001 bad_ips malicious
ip_intel csv 534 0 0 0 534 sans threatlist
splunk>workshop



Review the Advanced Threat content

splunk> workshop

Asset Investigator

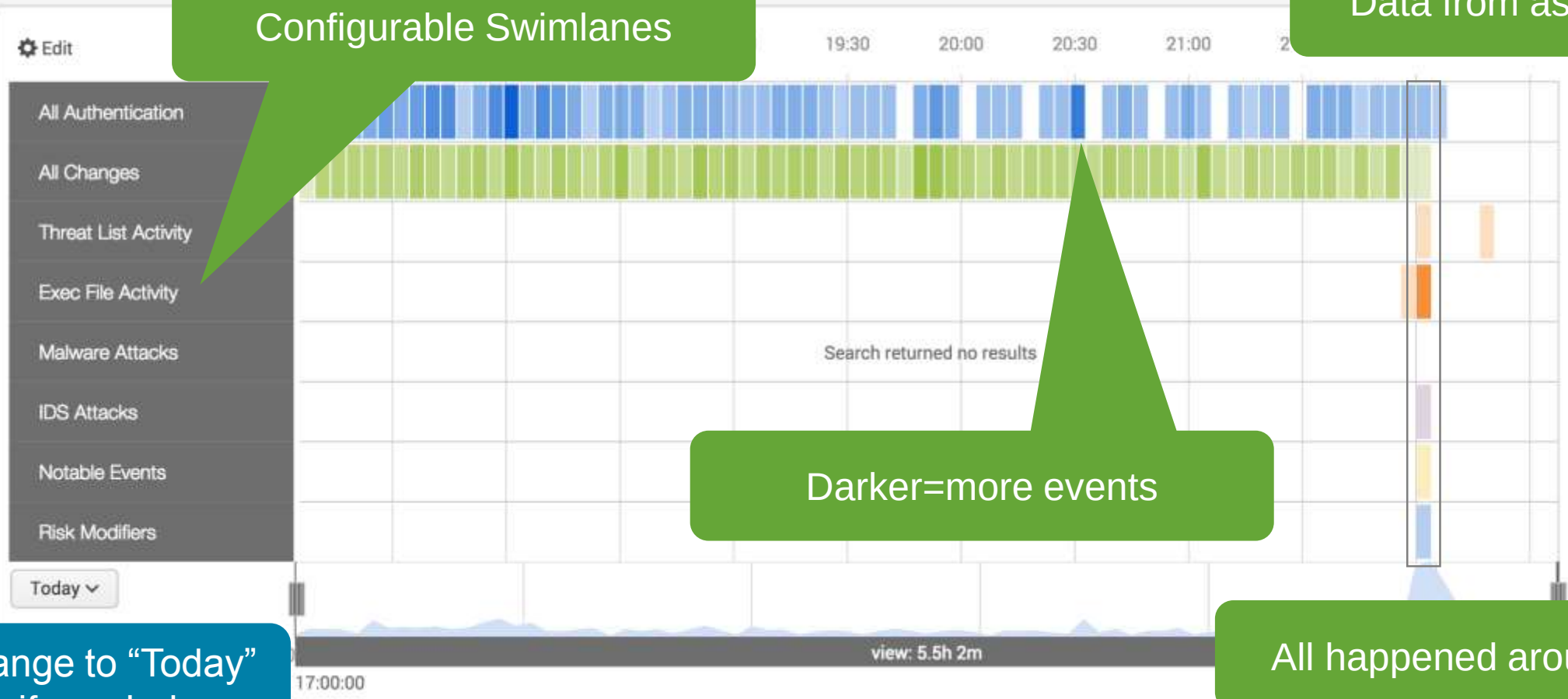
Asset Investigator, enter “192.168.56.102”

192.168.56.102

priority: **high**
dns: **cgilbert-DC3A297.buttercupgames.com**
owner: **chris.gilbert@buttercupgames.com**
long: **-122.390978**
should_timesync: **true**
bunit: **Sales**
city: **San Francisco**
pci_domain: **N/A**
nt_host: **cgilbert-DC3A297**
lat: **37.782955**
category: **Laptop**
should_update: **true**
ip: **192.168.56.102**
is_expected: **true**
requires_av: **true**
country: **USA**

Data from asset framework

Configurable Swimlanes



Darker=more events

Change to “Today” if needed

All happened around same time

splunk> workshop

Data Science & Machine Learning In Security

splunk> workshop

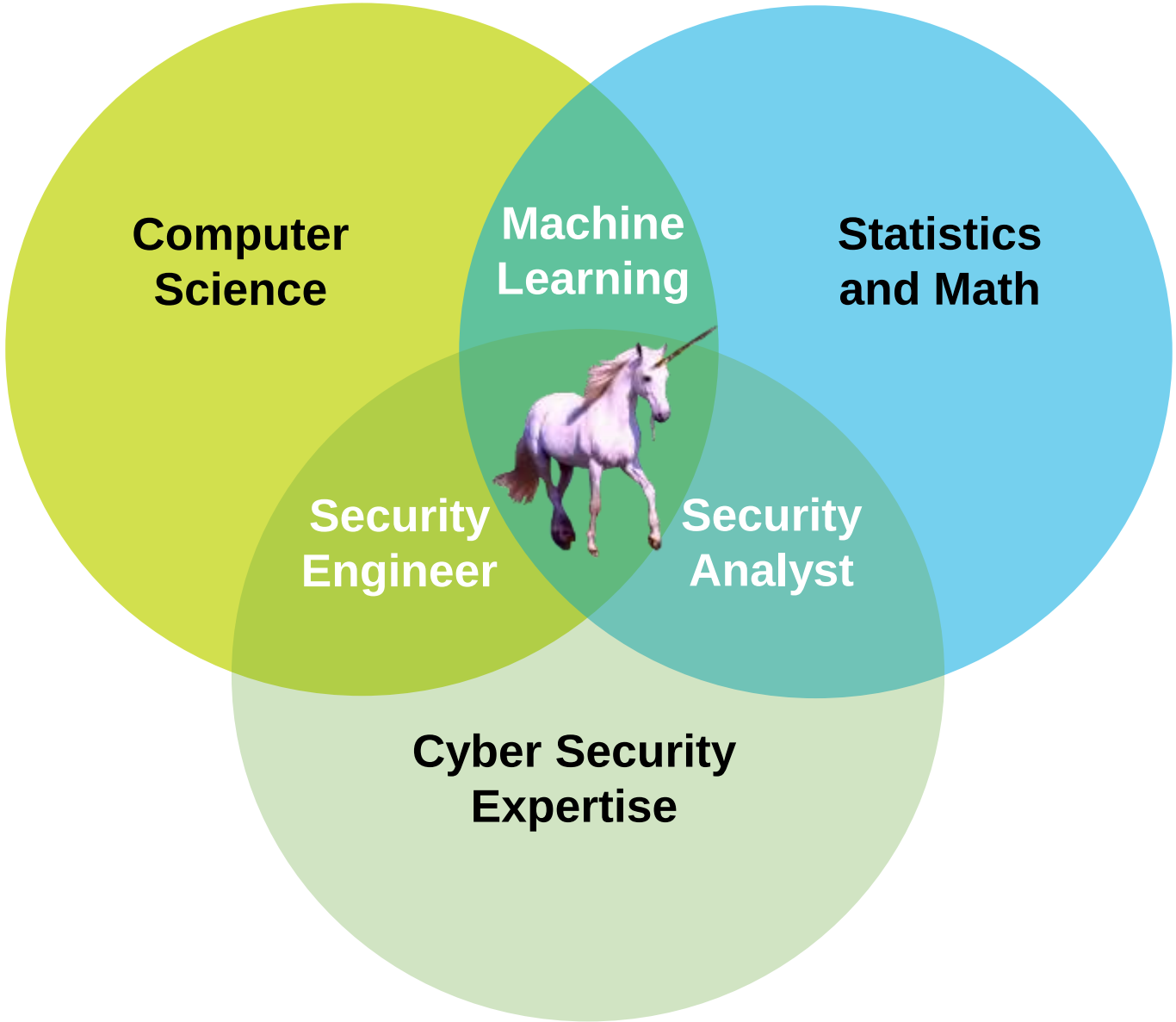
Disclaimer: I am not a data scientist

BIG DATA vs DATA SCIENCE

COLLECTION vs INSIGHT

Security data isn't just big data
It's morbidly obese data

Security Data Science



splunk> workshop

Types of Machine Learning

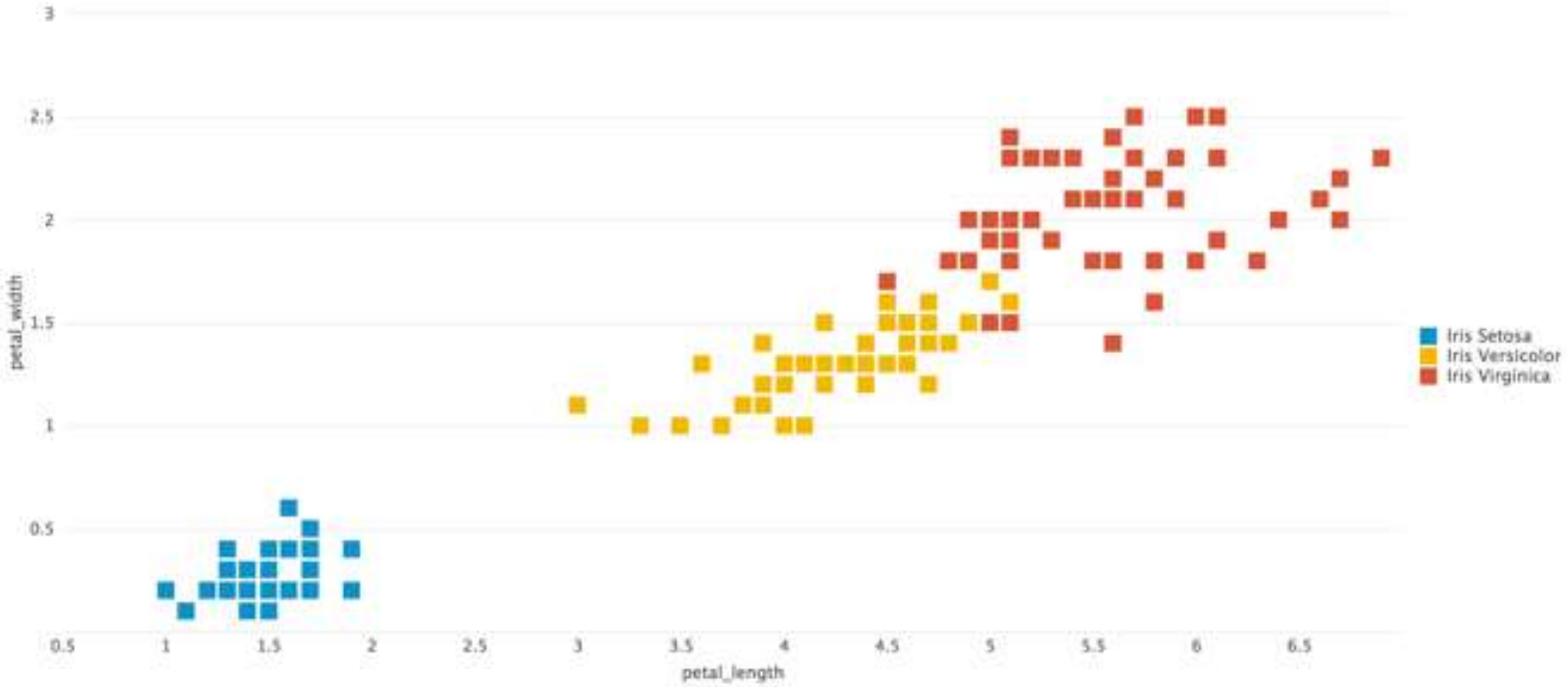
Supervised Machine Learning: Focus is to build models that make predictions based on evidence (labeled data) in the presence of uncertainty. As adaptive algorithms identify patterns in data, it "learns" from the observations.

Unsupervised Machine Learning: Used to draw inferences from datasets consisting of input data without labeled responses.

Semi-Supervised Machine Learning

Types of Machine Learning

Supervised Learning: Generalizing from labeled data



Supervised Machine Learning

- Regression: A regression problem is when the output variable is a real value, such as “authorizations over time”.
- Classification: A classification problem is when the output variable is a category, such as “malicious” or “non-malicious.” or “authorized” and “not authorized”.
- Anomaly Detection: Identify unusual activity, learn what normal looks like. Example: A history of normal web authorizations to then identify anything significantly different.

Supervised Machine Learning Regression

- Regression is used for predictive modeling to investigate the relationship between a dependent (target) and independent variables (predictors).

- Examples of regression algorithms:
  - Linear Regression
  - Logistic Regression
  - Stepwise Regression
  - Multivariate Adaptive Regression Splines (MARS)
  - Locally Estimated Scatterplot Smoothing (LOESS)
  - Ordinary Least Squares Regression (OLSR)

Regression Demo

Predict VPN Usage

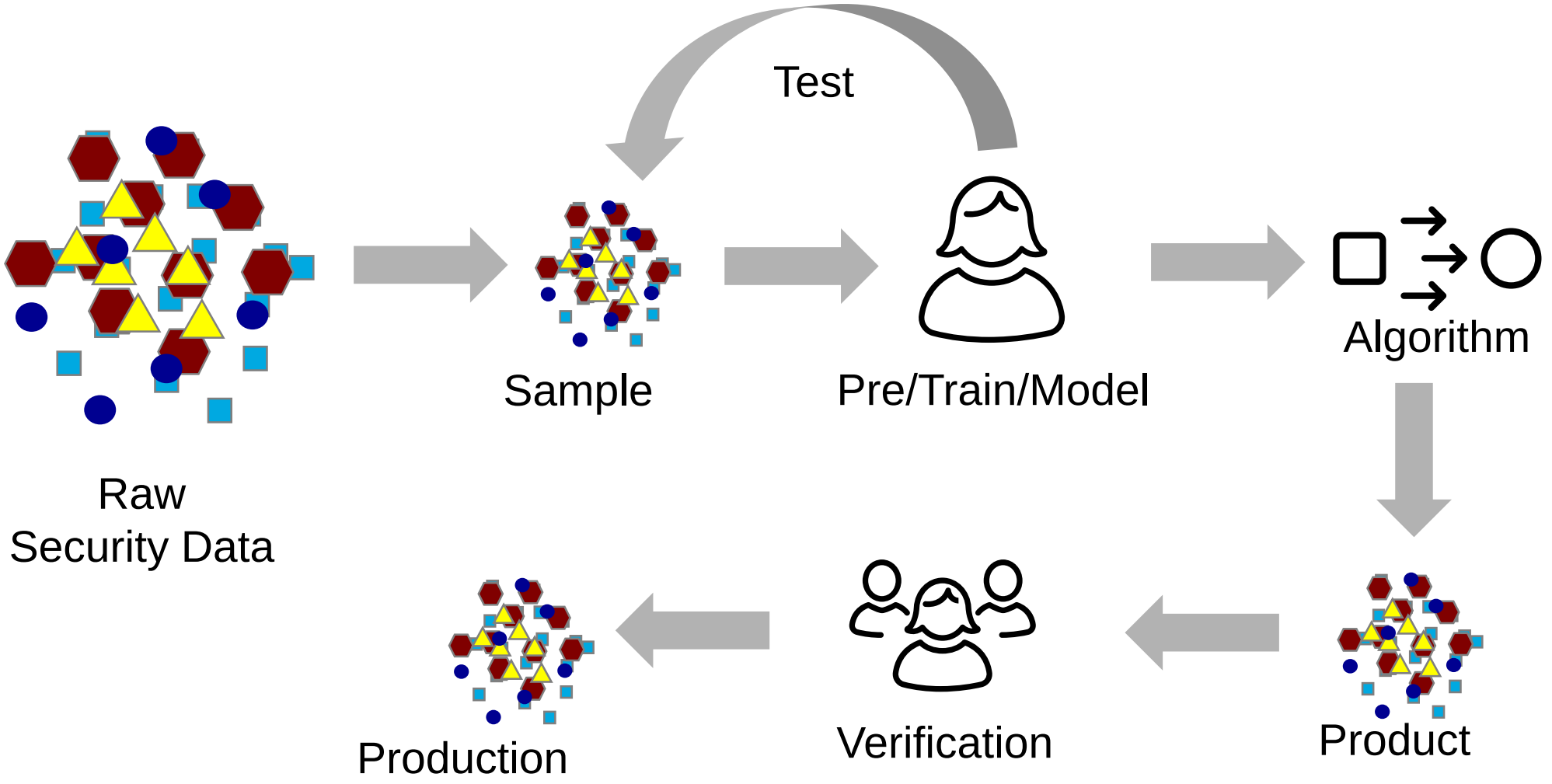
	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	CRM	CloudDrive	ERP	Expenses	HR1	HR2	ITOps	OTHER	Recruiting	RemoteAcce	Webmail	_time		
2	49	99	17	38	0	0	18	144	33	283	141	2015-06-06T00:00:00.000-0700		
3	107	148	28	54	0	0	38	188	30	430	213	2015-06-07T00:00:00.000-0700		
4	639	796	221	216	0	0	133	1175	297	732	579	2015-06-08T00:00:00.000-0700		
5	653	767	203	191	0	0	139	1475	308	738	549	2015-06-09T00:00:00.000-0700		
6	670	738	196	140	0	0	128	1111	305	781	678	2015-06-10T00:00:00.000-0700		
7	562	672	218	173	0	0	110	994	313	663	843	2015-06-11T00:00:00.000-0700		
8	547	537	148	174	0	0	81	977	252	631	588	2015-06-12T00:00:00.000-0700		
9	51	108	8	40	0	0	13	362	27	235	148	2015-06-13T00:00:00.000-0700		
10	120	176	18	66	0	0	26	413	62	298	191	2015-06-14T00:00:00.000-0700		
11	622	655	189	319	0	0	114	2102	304	825	670	2015-06-15T00:00:00.000-0700		
12	667	673	172	164	0	0	155	1112	241	732	708	2015-06-16T00:00:00.000-0700		
13	545	577	154	145	302	0	138	627	238	616	539	2015-06-17T00:00:00.000-0700		
14	620	705	207	192	952	0	121	336	311	624	625	2015-06-18T00:00:00.000-0700		
15	520	470	172	147	730	0	108	210	215	593	469	2015-06-19T00:00:00.000-0700		
16	51	61	6	28	121	0	8	26	21	133	108	2015-06-20T00:00:00.000-0700		
17	98	138	20	40	83	0	15	40	24	248	193	2015-06-21T00:00:00.000-0700		
18	633	737	191	212	743	0	115	358	292	623	831	2015-06-22T00:00:00.000-0700		

splunk> workshop

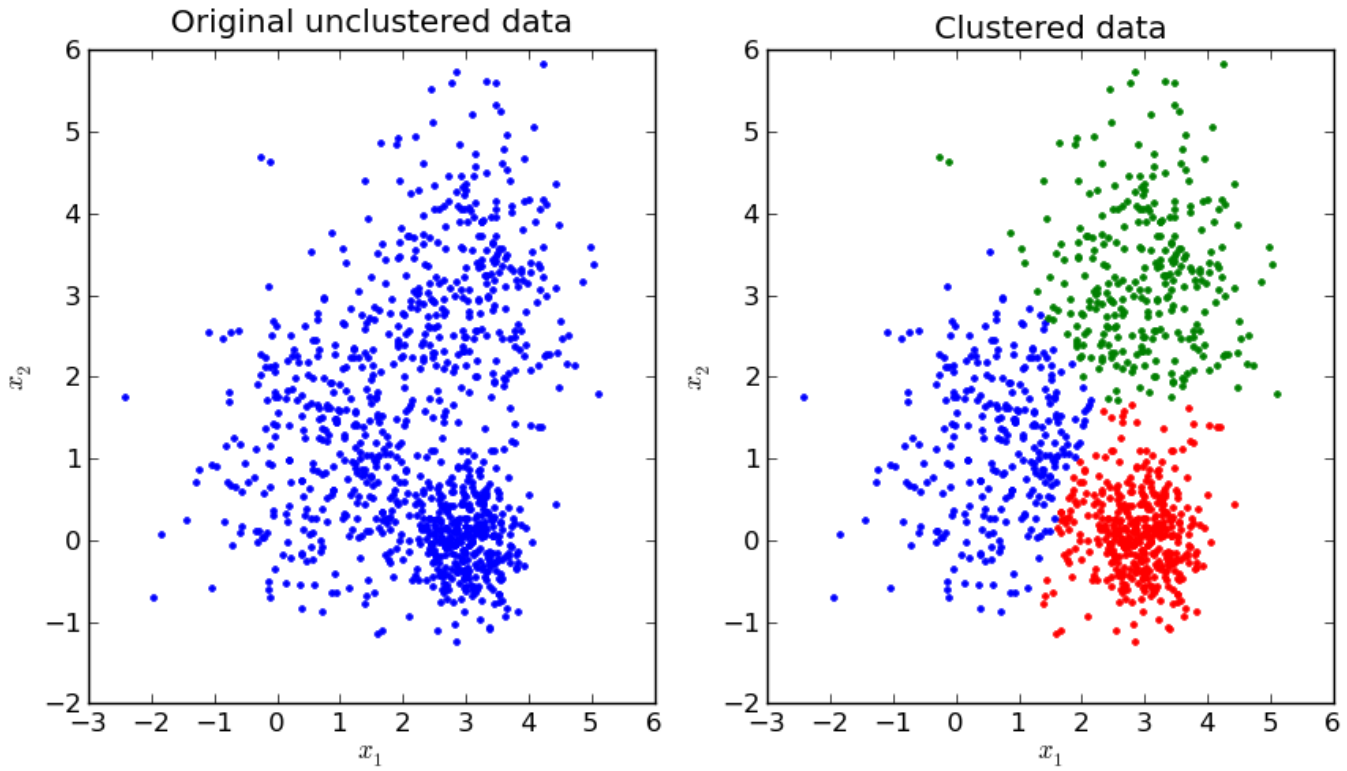
Supervised Machine Learning

Domain Name	TotalCnt	RiskFactor	AGD	SessionTime	RefEntropy	NullUa	Outcome
yyfaimjmocdu.com	144	6.05	1	1	0	0	Malicious
jjeyd2u37an30.com	6192	5.05	0	1	0	0	Malicious
cdn4s.steelhousemedia.com	107	3	0	0	0	0	Benign
log.tagcade.com	111	2	0	1	0	0	Benign
go.vidprocess.com	170	2	0	0	0	0	Benign
statse.webtrendslive.com	310	2	0	1	0	0	Benign
cdn4s.steelhousemedia.com	107	1	0	0	0	0	Benign
log.tagcade.com	111	1	0	1	0	0	Benign

Supervised Machine Learning Process



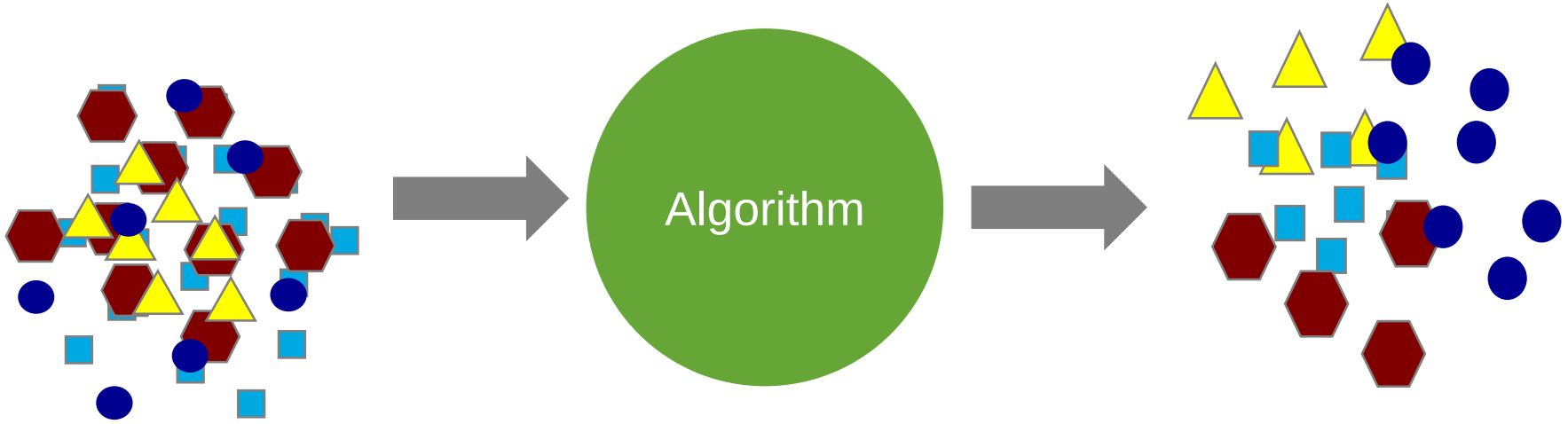
Unsupervised Learning: Generalizing from unlabeled data



Unsupervised Machine Learning

- No tuning
- Programmatically finds trends

- UBA is primarily unsupervised
- Rigorously tested for fit

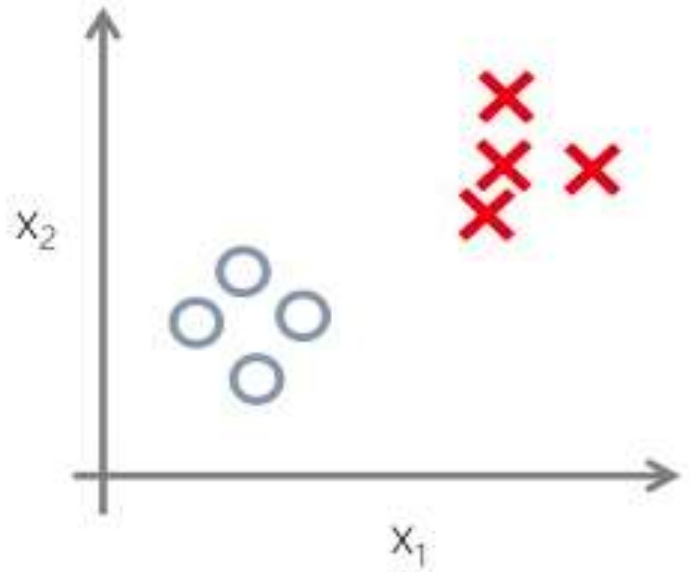


Raw Security Data

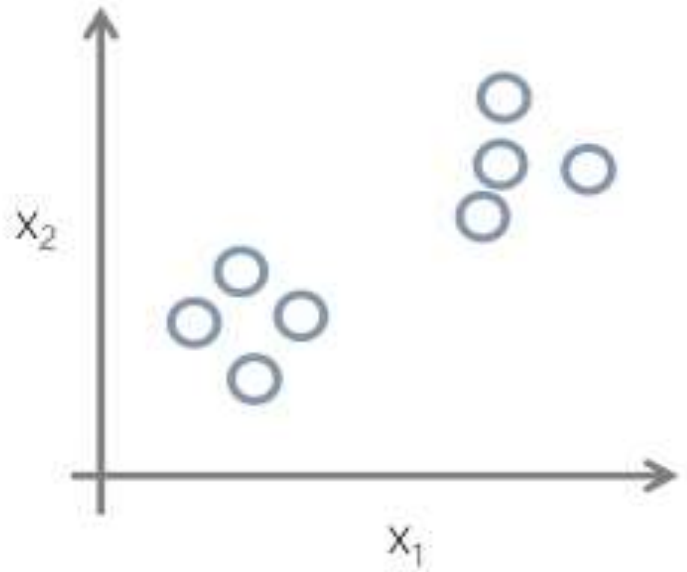
Automated Clustering

Supervised vs. Unsupervised

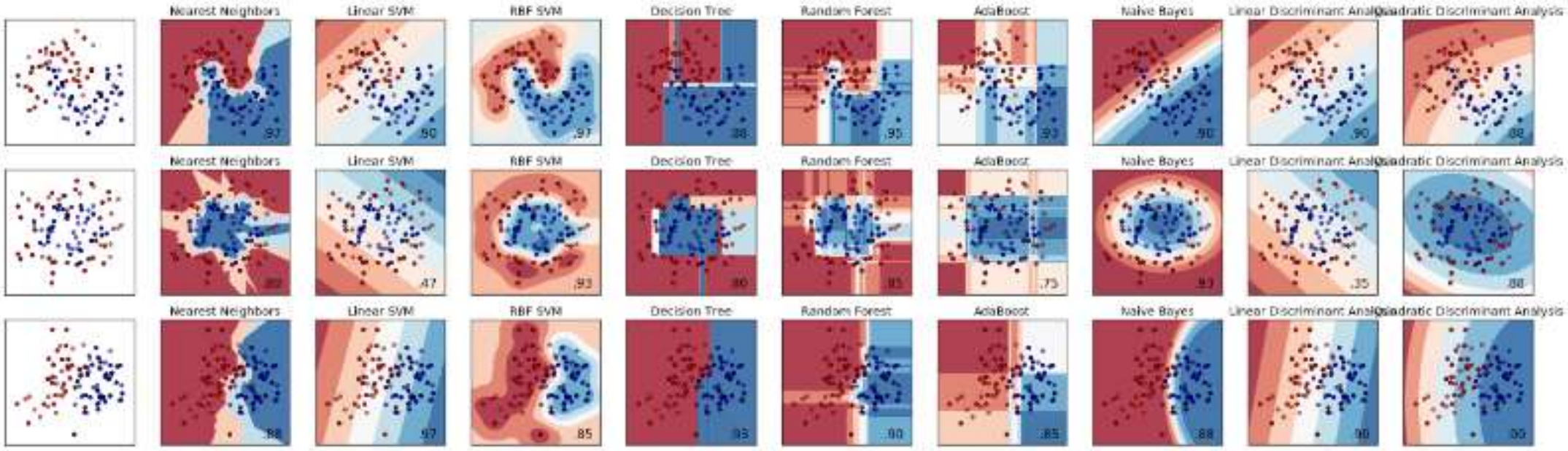
Supervised Learning



Unsupervised Learning



SCI-Kit Learn



splunk> workshop

SCI-Kit Learn

Classification

Identifying to which category an object belongs to.

Applications: Spam detection, Image recognition.
Algorithms: SVM, nearest neighbors, random forest, ... — Examples

Regression

Predicting a continuous-valued attribute associated with an object.

Applications: Drug response, Stock prices.
Algorithms: SVR, ridge regression, Lasso, ... — Examples

Clustering

Automatic grouping of similar objects into sets.

Applications: Customer segmentation, Grouping experiment outcomes
Algorithms: k-Means, spectral clustering, mean-shift, ... — Examples

Dimensionality reduction

Reducing the number of random variables to consider.

Applications: Visualization, Increased efficiency
Algorithms: PCA, feature selection, non-negative matrix factorization. — Examples

Model selection

Comparing, validating and choosing parameters and models.

Goal: Improved accuracy via parameter tuning
Modules: grid search, cross validation, metrics. — Examples

Preprocessing

Feature extraction and normalization.

Application: Transforming input data such as text for use with machine learning algorithms.
Modules: preprocessing, feature extraction. — Examples

splunk> workshop

ML Toolkit & Showcase

- Splunk Supported framework for building ML Apps
  - **Get it for free:** http://tiny.cc/splunkmlapp
- Leverages **Python for Scientific Computing** (PSC) add-on:
  - Open-source Python data science ecosystem
  - NumPy, SciPy, scitkit-learn, pandas, statsmodels
- **Showcase use cases**: Predict Hard Drive Failure, Server Power Consumption, Application Usage, Customer Churn & more
- **Standard algorithms** out of the box:
  - Supervised: **Logistic Regression, SVM, Linear Regression, Random Forest, etc.**
  - Unsupervised: **KMeans, DBSCAN, Spectral Clustering, PCA, KernelPCA, etc.**
- Implement one of 300+ algorithms by editing Python scripts

ML Toolkit and Showcase

Machine Learning Toolkit Demo

splunk> workshop

Splunk for Analytics and Data Science

This course, delivered over three virtual days, covers implementing analytics and data science projects using Splunk's statistics, machine learning, built-in and custom visualization capabilities.

View schedule »

Download course description »

Upcoming Classes

Course Topics

- Analytics Framework
- Exploratory Data Analysis
- Machine Learning
- Market Segmentation
- Transactional Analysis
- Anomaly Detection
- Estimation and Prediction
- Classification
- Data Visualization

Course Prerequisites

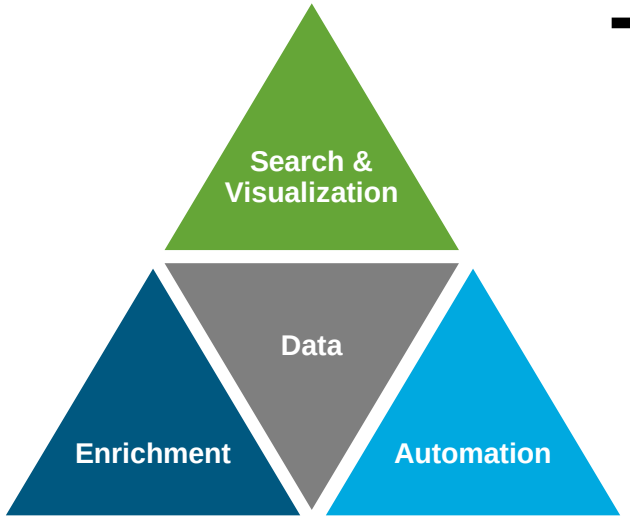
- Using Splunk
- Searching and Reporting with Splunk
- Creating Splunk Knowledge Objects
- Advanced Searching and Reporting with Splunk
- *OR equivalent Splunk experience*

splunk> workshop

Splunk UBA

splunk> workshop

Threat Hunting With Splunk



Threat Hunting Data Enrichment

Threat Hunting Automation

Ingest & Onboard Any Threat Hunting Machine Data Source

Search & Visualise Relationships for Faster Hunting

Splunk Enterprise Security

- Security Analytics Platform -

User Behavior Analytics

- Security Data Science Platform -

Splunk Enterprise

- Big Data Analytics Platform -

Data Science & Machine Learning

Automated Analytics

Visualisation

Data & Intelligence Enrichment

Data Search

Hypotheses

Maturity

splunk>

splunk> workshop

Machine Learning Security Use Cases

Machine Learning Use Cases

- User & Entity Behavior Baseline
- Behavioral Peer Group Analysis
- Insider Threat Detection
- IP Reputation Analysis
- Reconnaissance, Botnet and C&C Analysis
- Statistical Analysis
- Data Exfiltration Models
- Lateral Movement Analysis
- Polymorphic Attack Analysis
- Cyber Attack / External Threat Detection
- Entropy/Rare Event Detection
- User/Device Dynamic Fingerprinting

Splunk UBA Use Cases

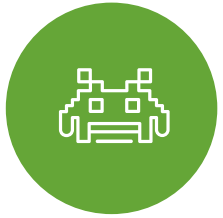
Insider Treats

- **Account Takeover**
  - Privileged account compromise
  - Data exfiltration

- **Lateral Movement**
  - Pass-the-hash kill chain
  - Privilege escalation

- **Suspicious Activity**
  - Misuse of credentials
  - Geo-location anomalies

External Threats



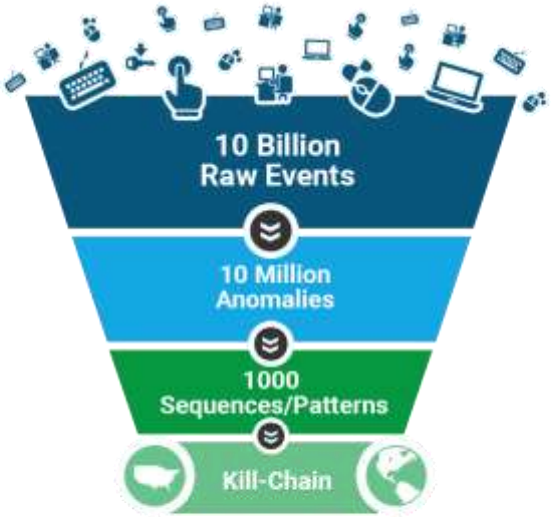
- **Malware Attacks**
  - Hidden malware activity

- **Botnet, Command & Control**
  - Malware beaconing
  - Data leakage

- **User & Entity Behavior Analytics**
  - Suspicious behavior by accounts or devices

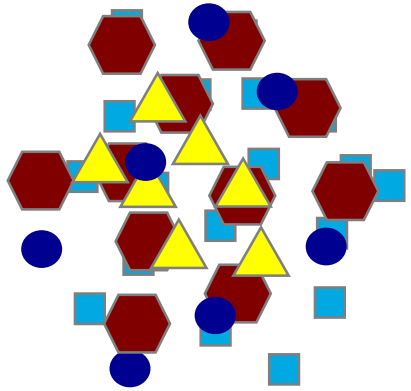
Splunk User Behavior Analytics (UBA)

- ~100% of breaches involve valid credentials (Mandiant Report)
- Need to understand normal & anomalous behaviors for ALL users
- UBA detects Advanced Cyberattacks and Malicious Insider Threats
- Lots of ML under the hood:
  - Behavior Baselining & Modeling
  - Anomaly Detection (30+ models)
  - Advanced Threat Detection
- E.g., Data Exfil Threat:
  - “Saw this strange login & data transferfor user kwestin at 3am in China…”
  - Surface threat to SOC Analysts



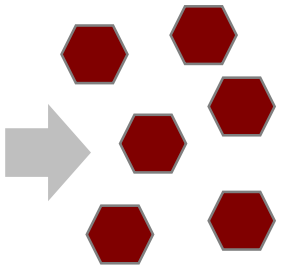
splunk> workshop

Raw Security Events



Machine Learning

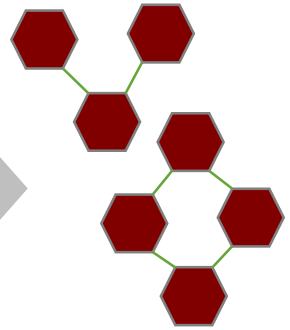
Anomalies



Anomalies graph
Entity relationship graph

Graph Mining

Anomaly Chains (Threats)



Lateral Movement
Beaconing
Land-Speed Violation

Threat Models

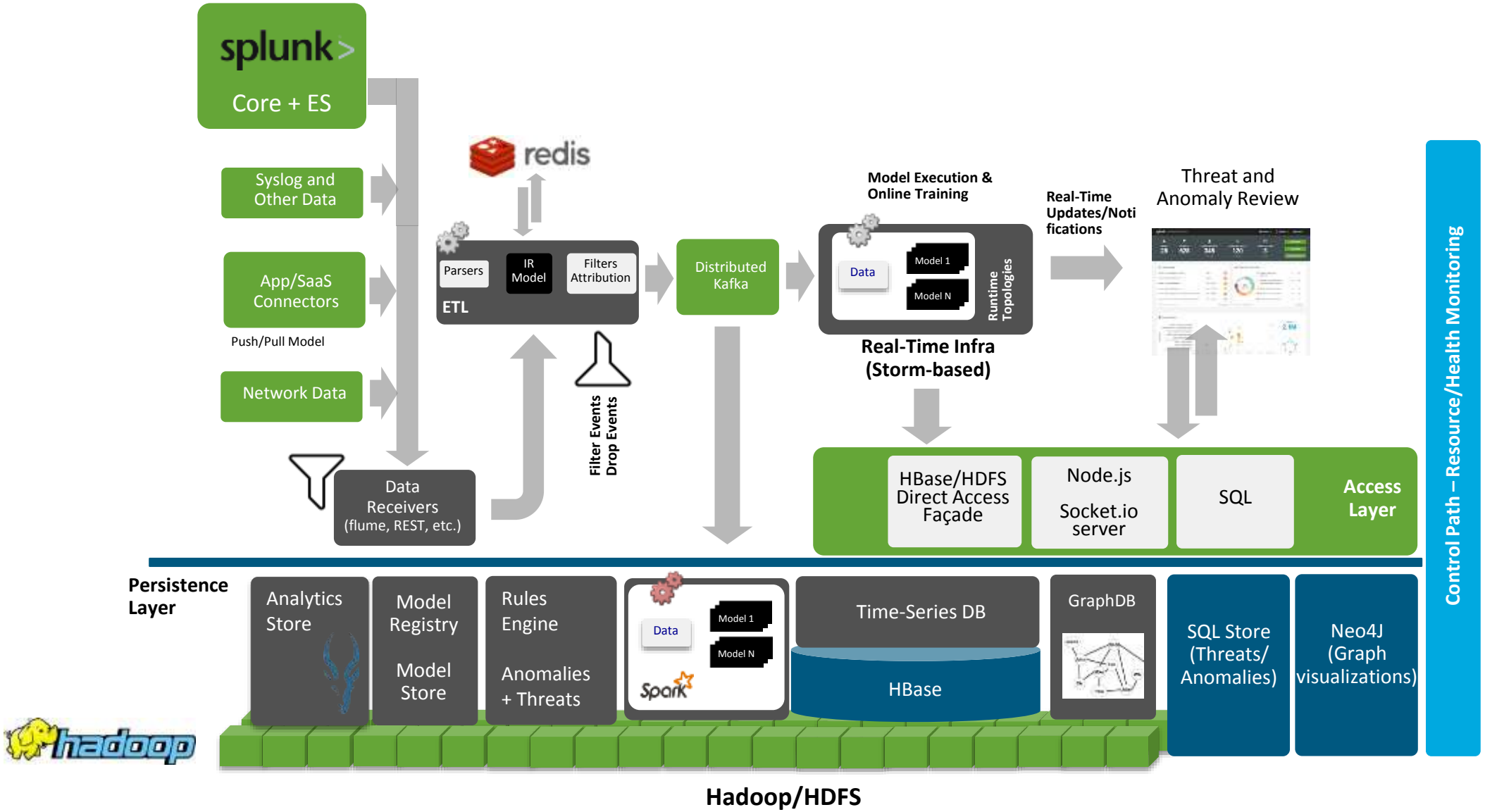
HCI

Kill chain sequence
Forensic artifacts
Threat/Risk scoring

Feedback

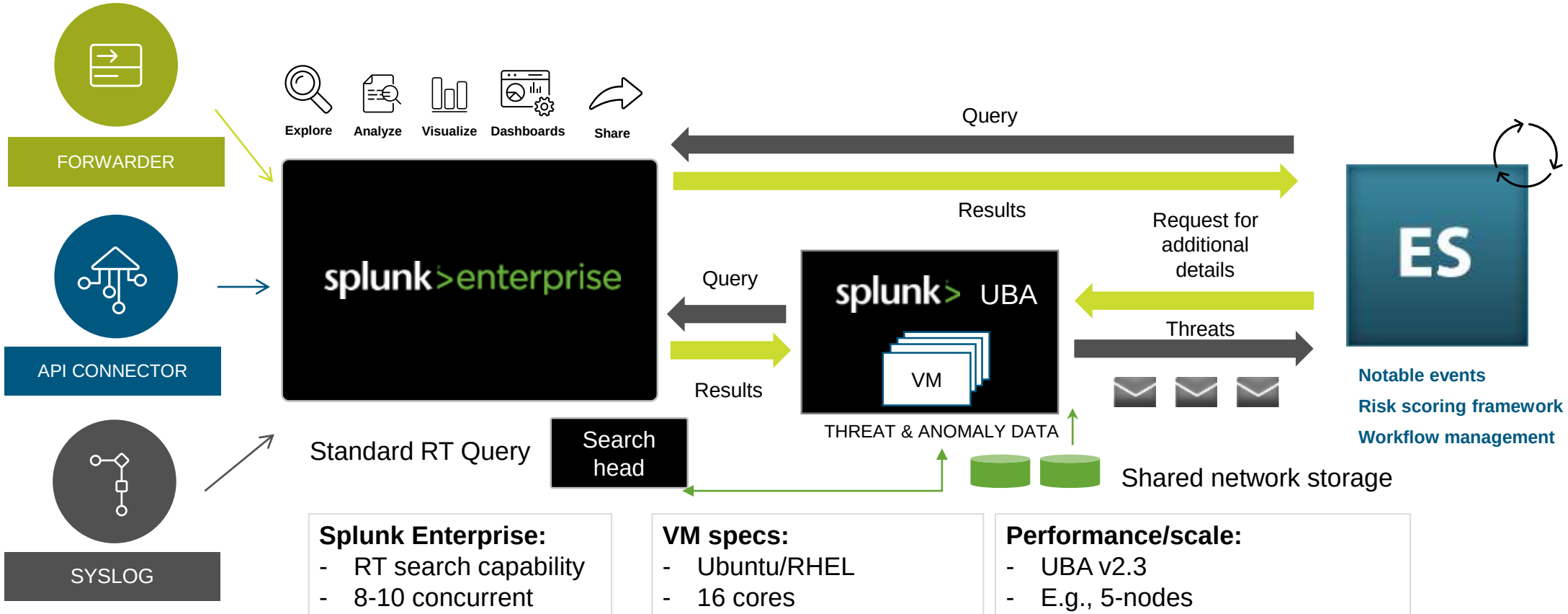
splunk> workshop

Overall Architecture



splunk> workshop

Data Flow and System Requirements



Splunk Enterprise:
- RT search capability
- 8-10 concurrent searches
- REST API port (8089)
- SA-LDAPSEARCH

VM specs:
- Ubuntu/RHEL
- 16 cores
- 64 GB RAM
- Local and network disks
- GigE connectivity

Performance/scale:
- UBA v2.3
- E.g., 5-nodes
  - 25K EPS
- Add nodes for near-linear scale

splunk> workshop

Splunk UBA Demo

splunk> workshop

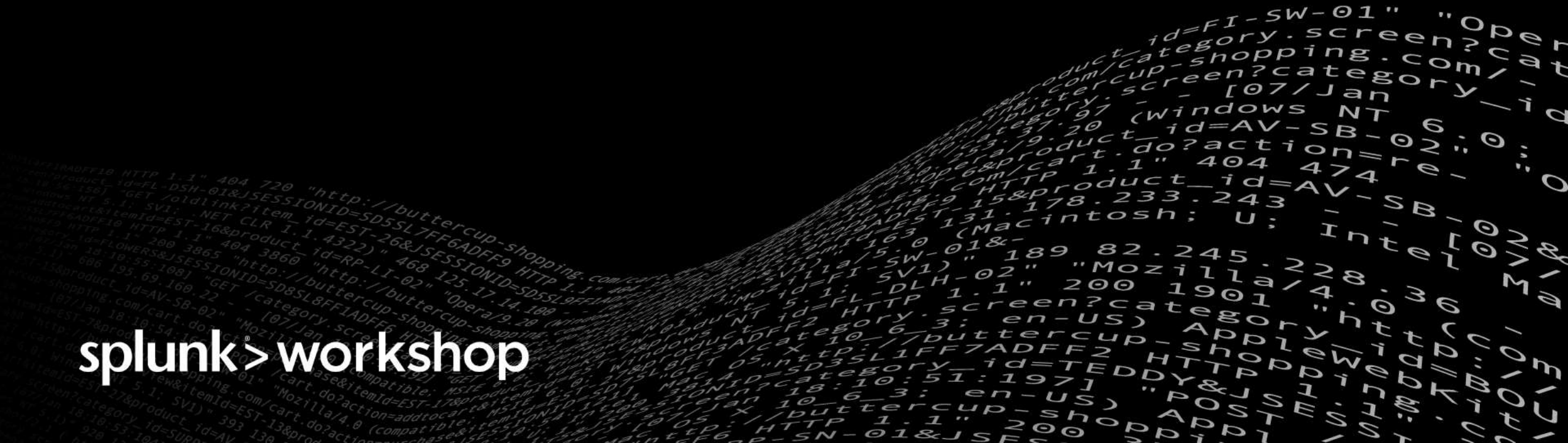
More Security Workshops!

- Security Readiness Workshop
- Data Science Workshop
- Enterprise Security Benchmark Assessment
- Boss of the SOC

Security Workshop Survey

splunk> workshop

Thank You!



splunk> workshop