Threat Hunting with Splunk

Presenter: Ken Westin, M.Sc, OSCP
Splunk, Security Market Specialist

splunk>

Agenda

- Threat Huting Basics
- Threat Hunting Data Sources
- Sysmon Endpoint Data
- Cyber Kill Chain
- Walkthrough of Attack Scenario Using Core Splunk (hands on)
- Enterprise Security Walkthrough
- Applying Machine Learning and Data Science to Security

Log In Credentials

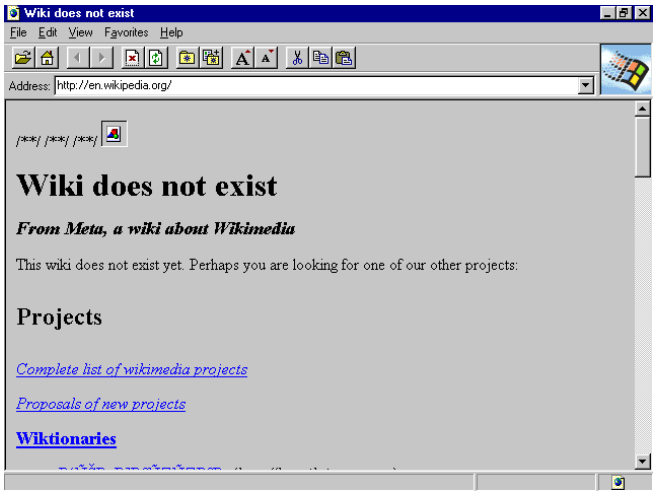
Birth Month

January, February & March	https://od-norcal-2.splunkoxygen.com
April, May & June	https://od-norcal-3.splunkoxygen.com
July, August & September	https://od-norcal-4.splunkoxygen.com
October, November & December	https://od-norcal-5.splunkoxygen.com

User: hunter

Pass: pr3dator

These 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


This is a hands-on session.
The overview slides are important for building your "hunt" methodology
10 minutes - Seriously.

Threat Hunting with Splunk

Vs.

SANS Threat Hunting Maturity

Ad Hoc Search	Statistical Analysis	Visualization Techniques	Aggregation	Machine Learning/ Data Science
85%	55%	50%	48%	32%

Source: SANS IR & Threat Hunting Summit 2016

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)

Log In Credentials

January, February & March	https://od-norcal-2.splunkoxygen.com
April, May & June	https://od-norcal-3.splunkoxygen.com
July, August & September	https://od-norcal-4.splunkoxygen.com
October, November & December	https://od-norcal-5.splunkoxygen.com

User: hunter

Pass: pr3dator

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/

Show app to click on

*** This is a hands-on session ***

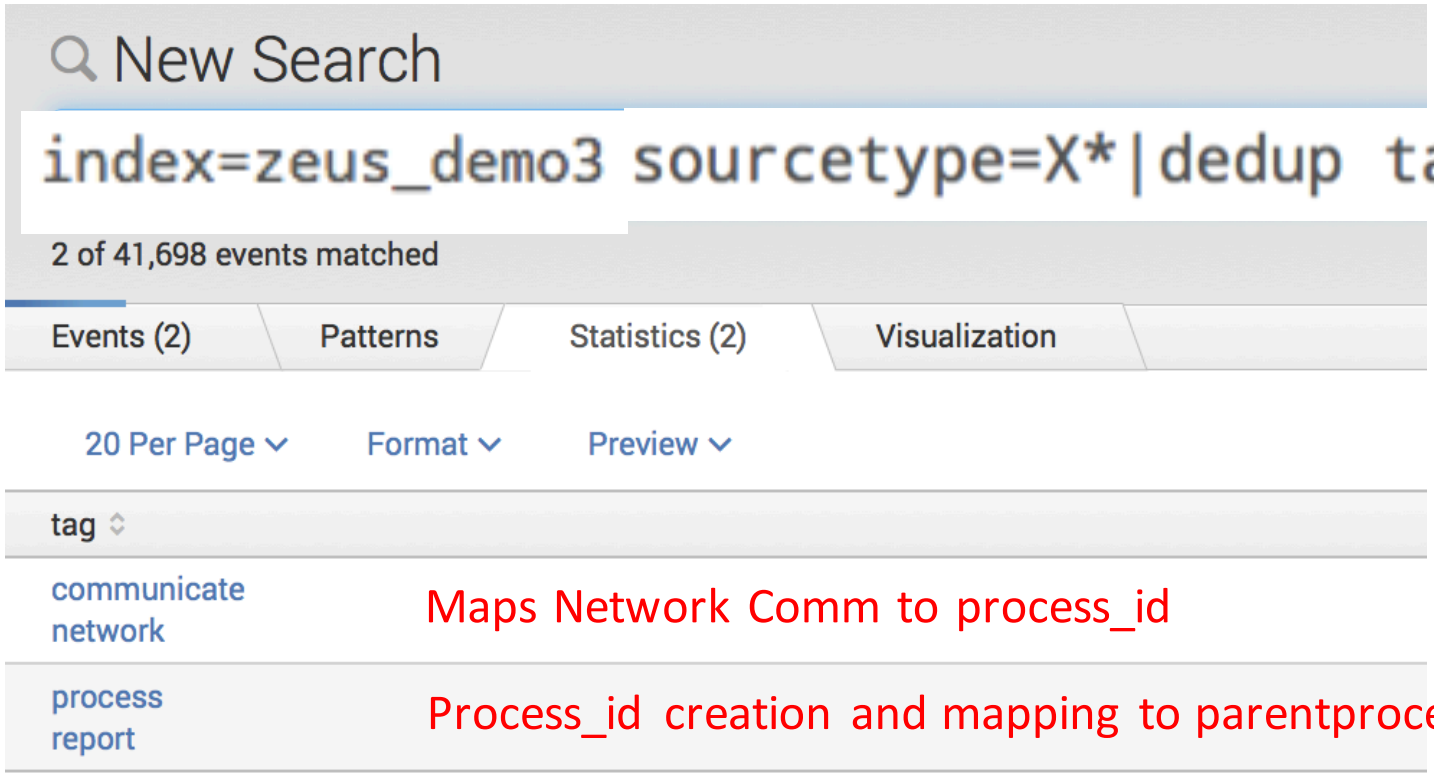
Please use your individual URLs and creds.

User: hunter

Pass: pr3dator

January, February & March	https://od-norcal-2.splunkoxygen.com
April, May & June	https://od-norcal-3.splunkoxygen.com
July, August & September	https://od-norcal-4.splunkoxygen.com
October, November & December	https://od-norcal-5.splunkoxygen.com

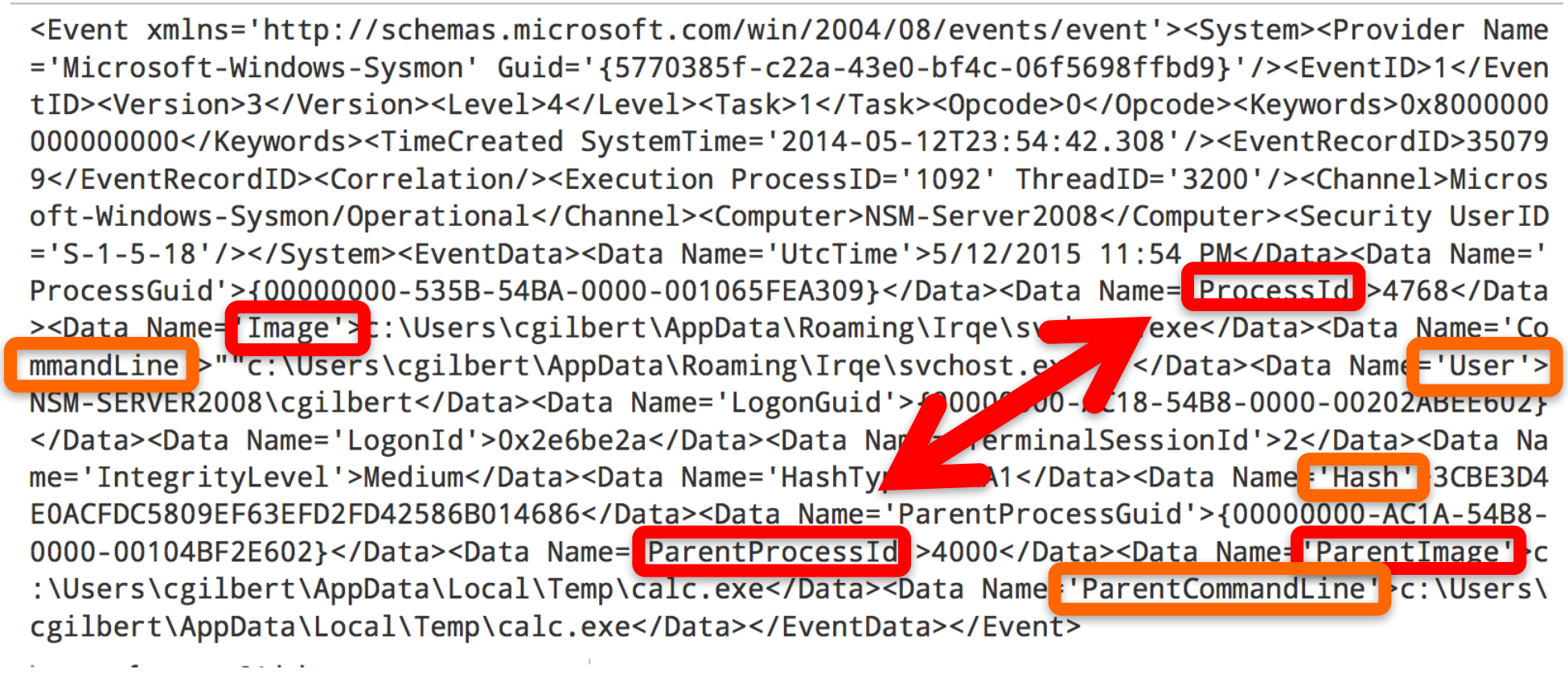
Sysmon Event Tags



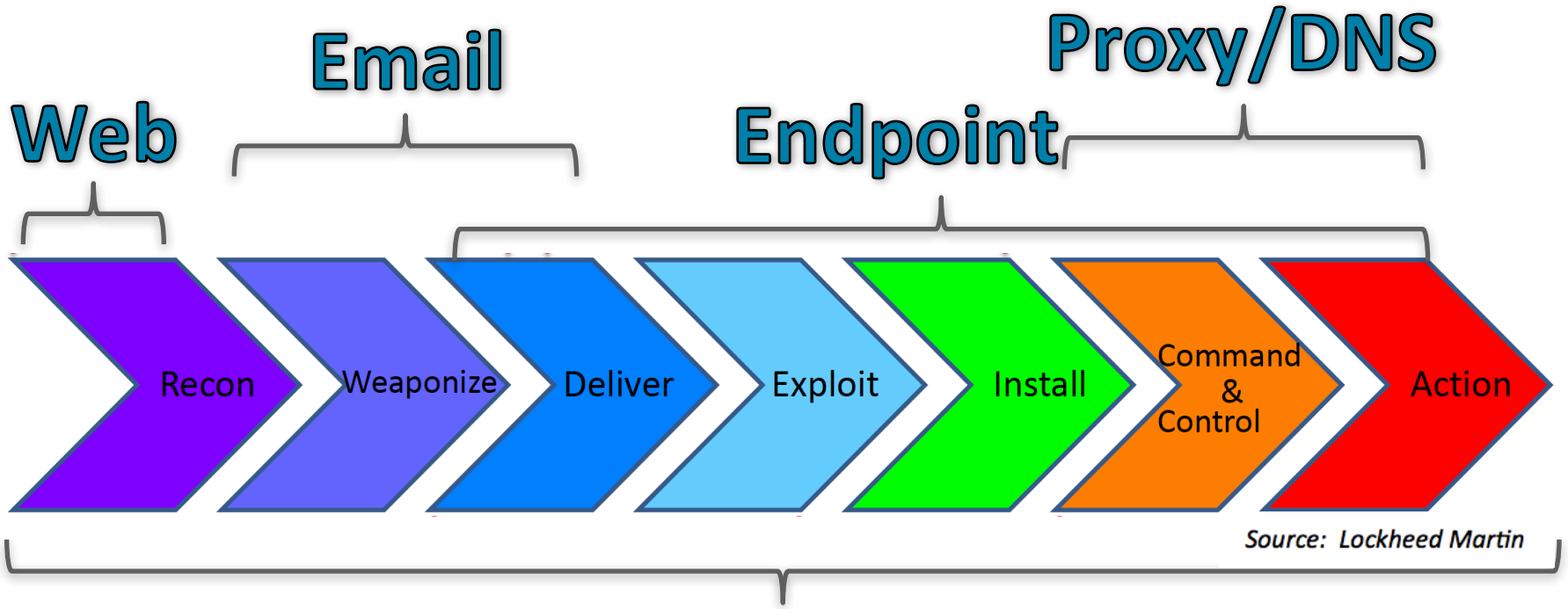
sourcetype=X* | search tag=communicate

<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</Leve
l><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2015-02-05T0
7:16:00.595Z'/><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)\Adob
e\Reader 10.0\Reader\AcroRd32.exe</Data><Data Name='User'>server1\jim</Data><Data Name='Protocol'>tcp</Data><D
ata 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'></D
ata><Data Name='DestinationIsIpv6'>false</Data><Data Name='DestinationIp'>96.16.7.81</Data><Data Name='Destina
tionHostname'>a96-16-7-81.deploy.akamaitechnologies.com</Data><Data Name='DestinationPort'>80</Data><Data Name
='DestinationPortName'>http</Data></EventData></Event>

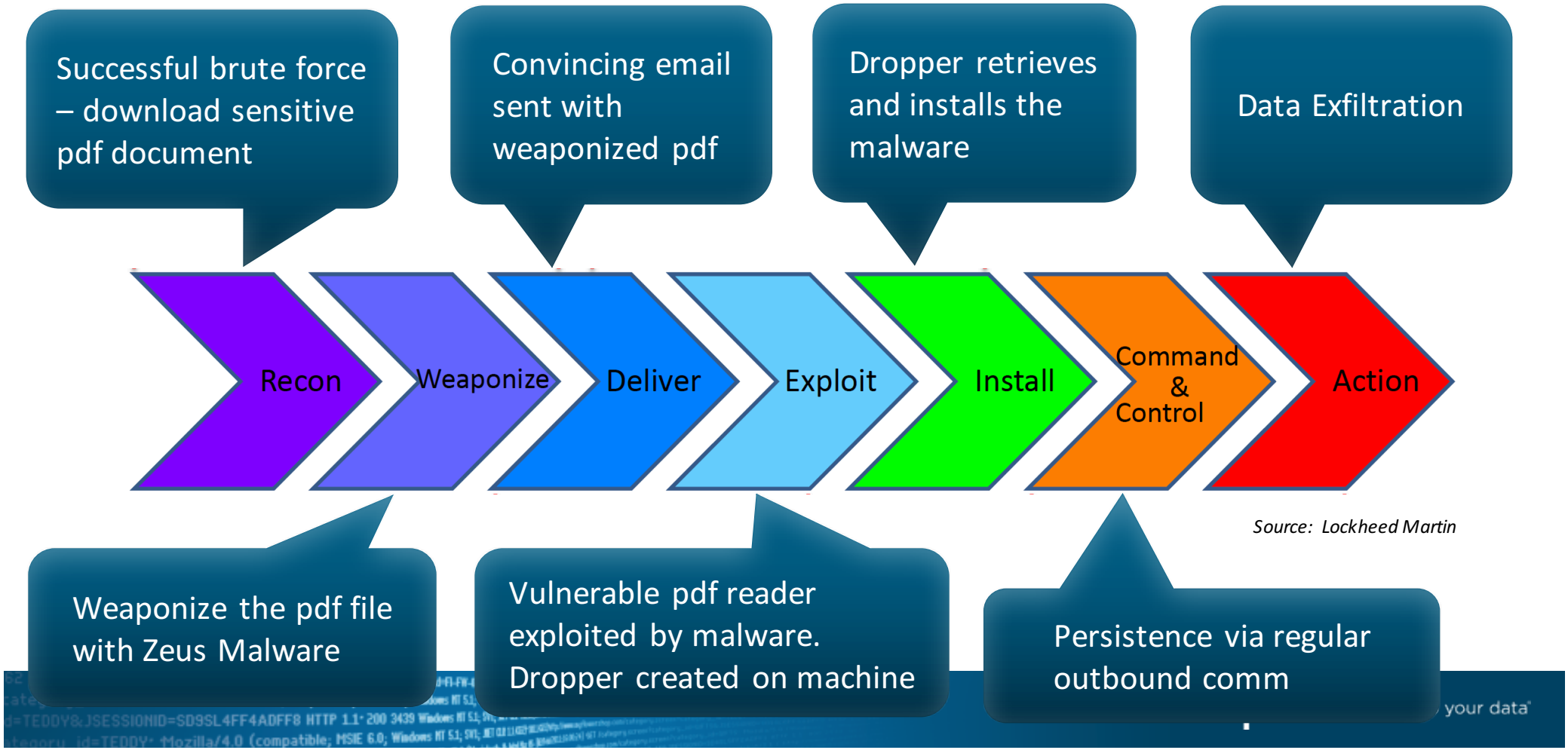
sourcetype=X* | dedup tag| search tag=process



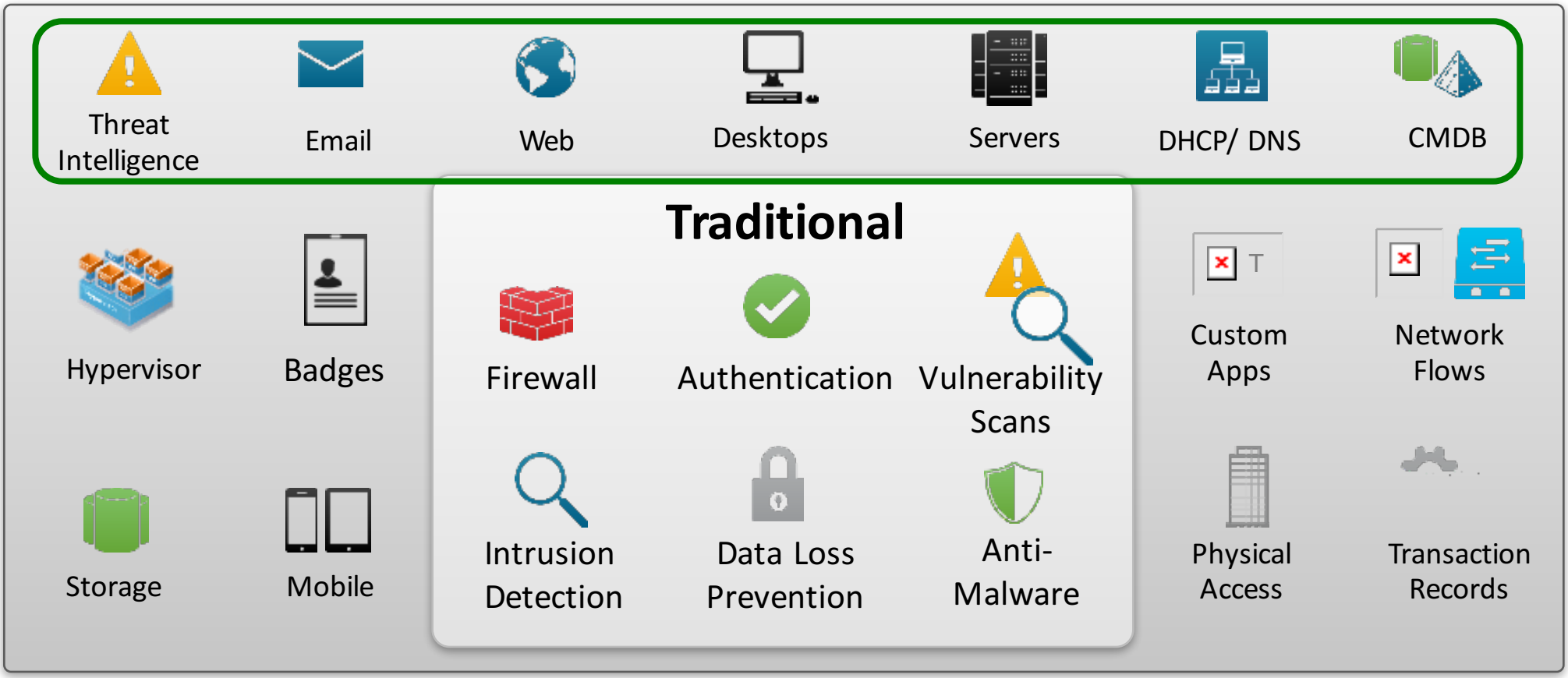
Data Source Mapping



Demo Story - Kill Chain Framework

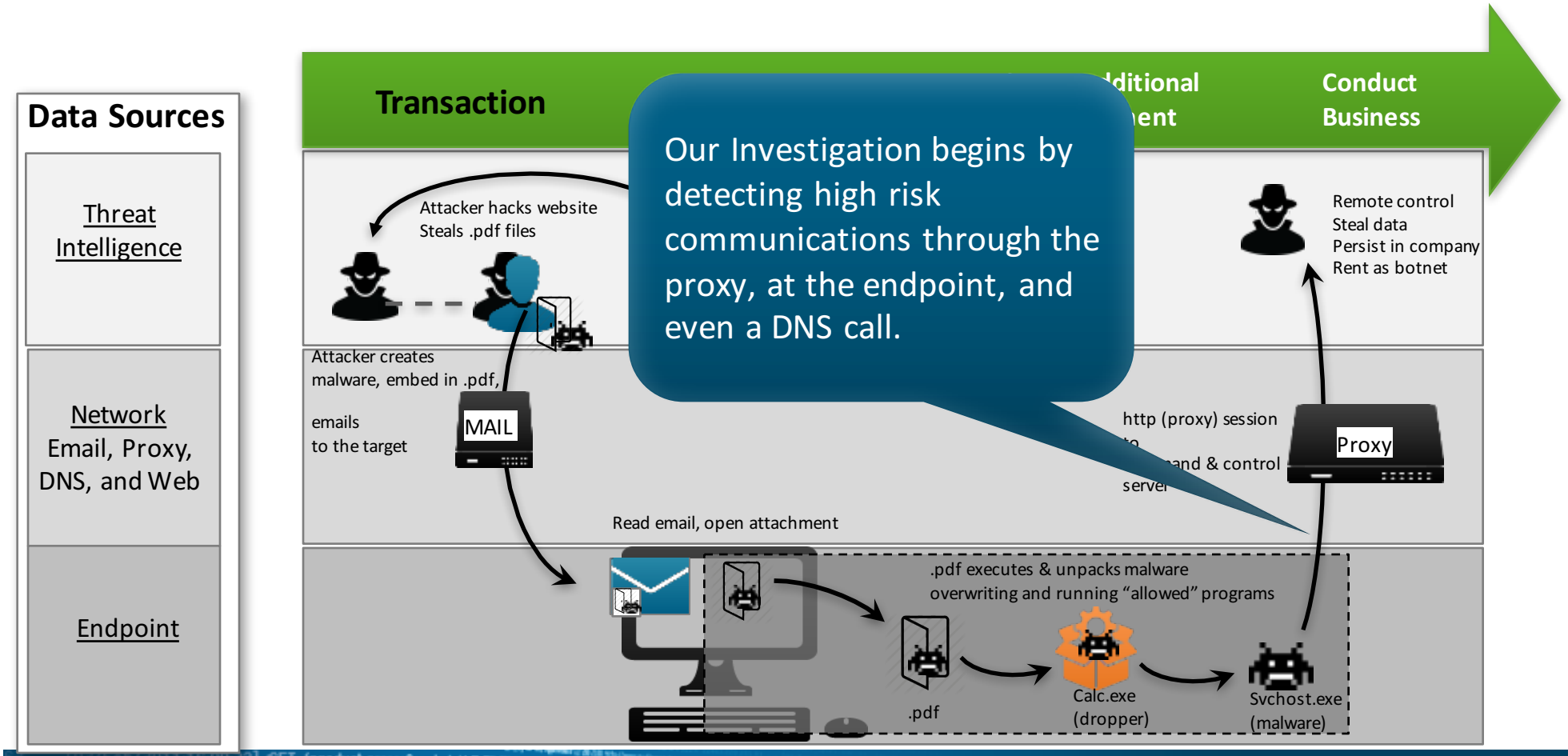


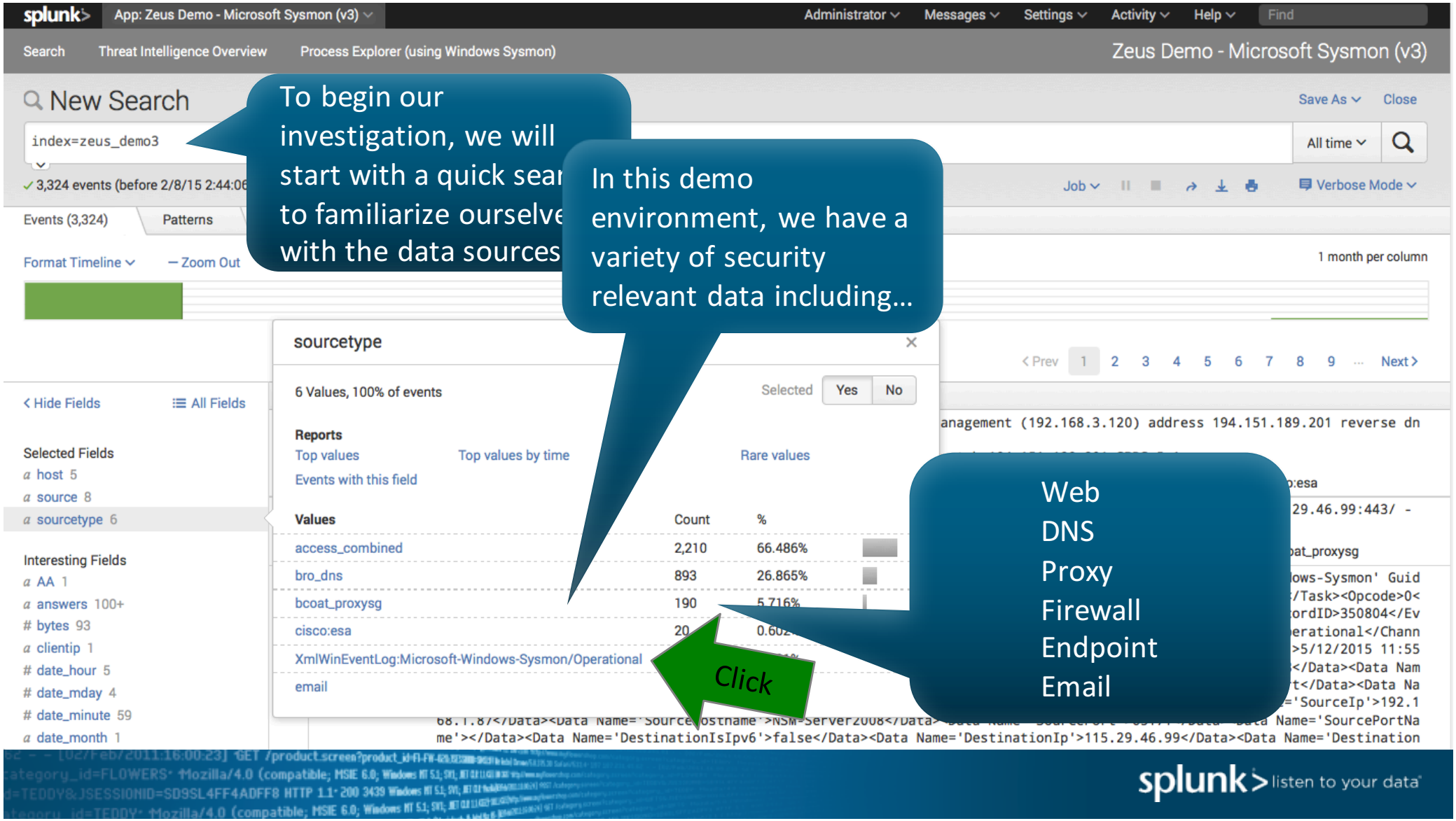
Stream Investigations – choose your data wisely

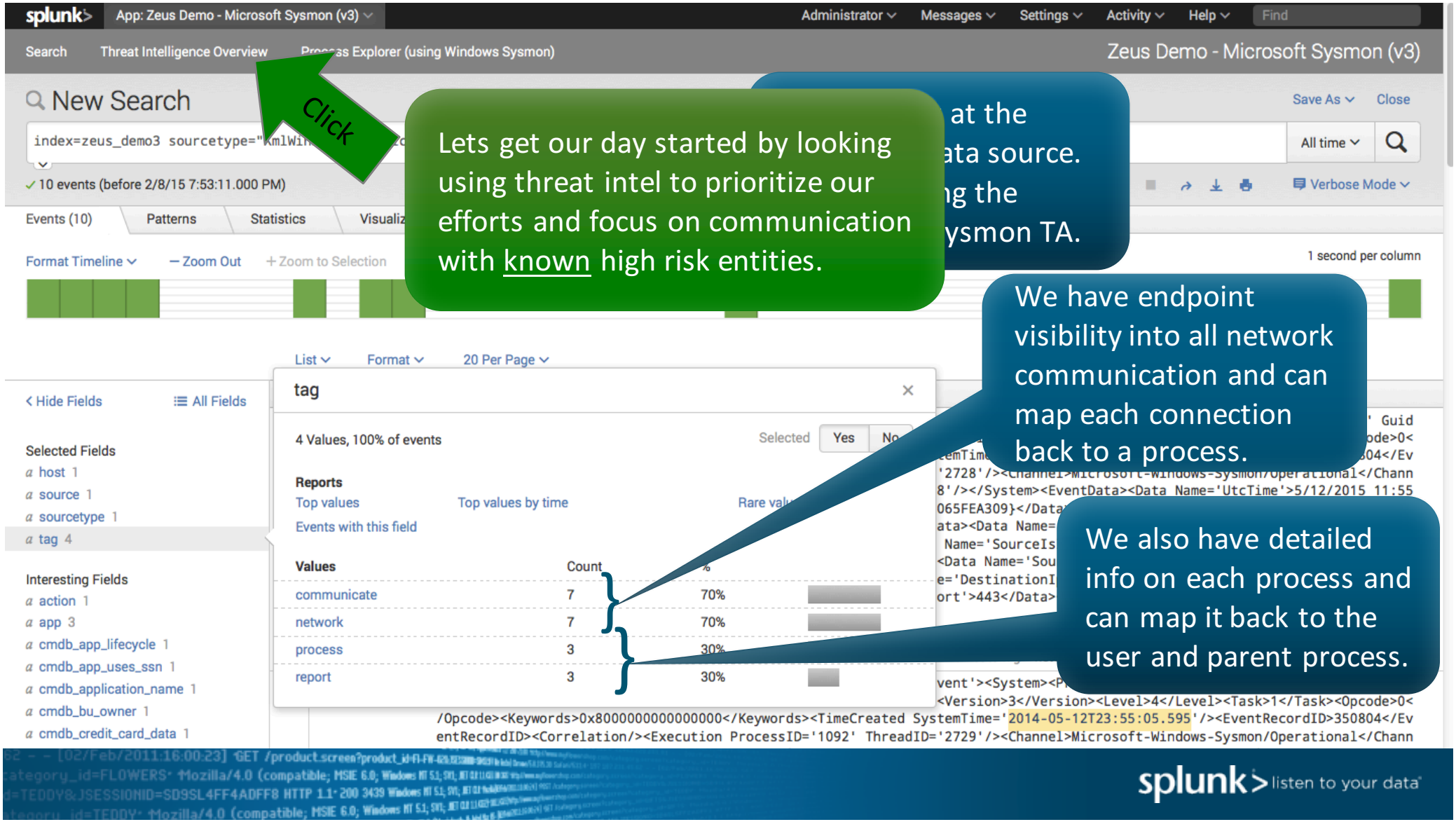


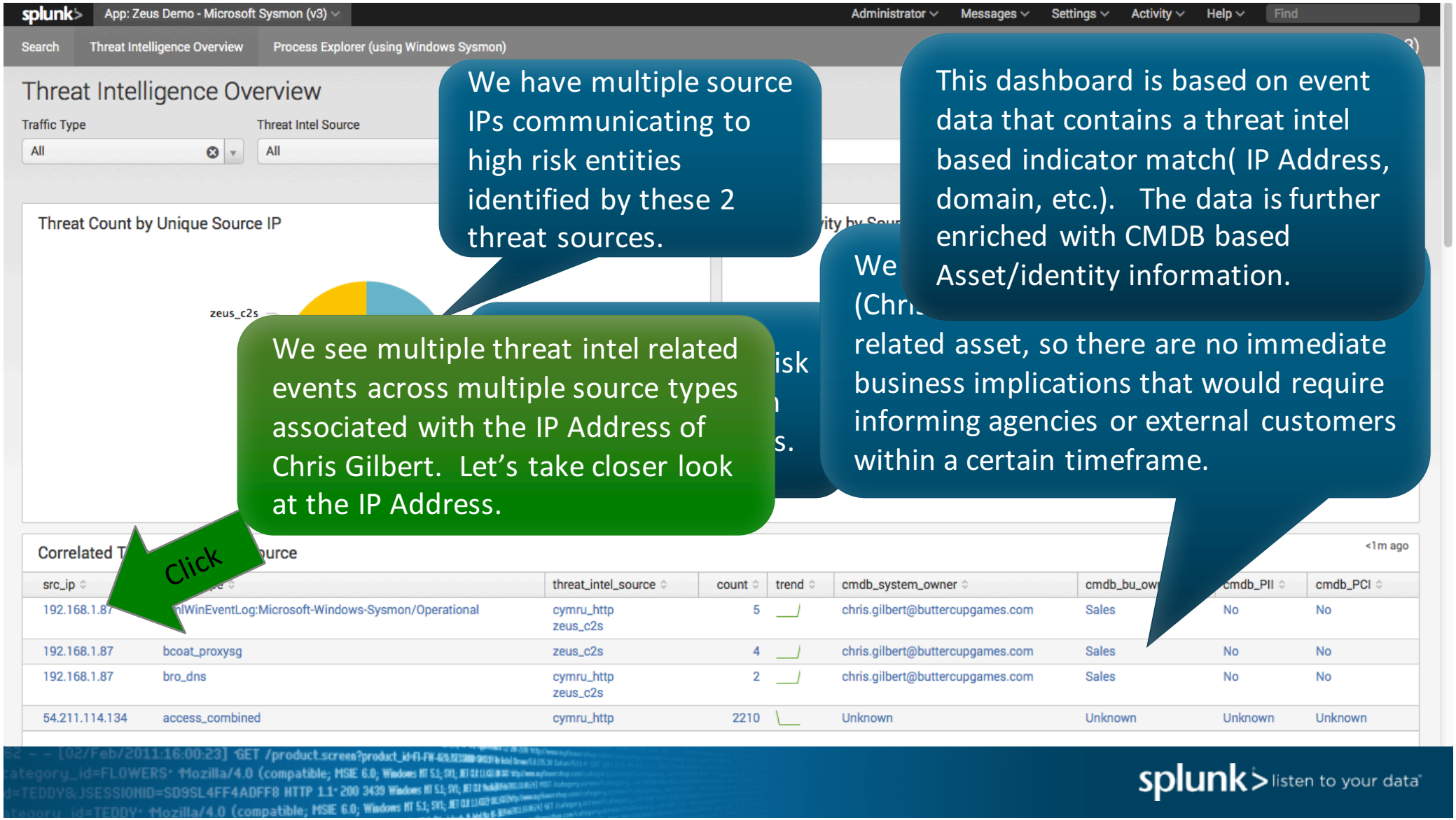

Let’s dig in!
Please, raise that hand if you need us to hit the pause button
20
40
60
80
100
120
140
160
180
200
220
240
km/h

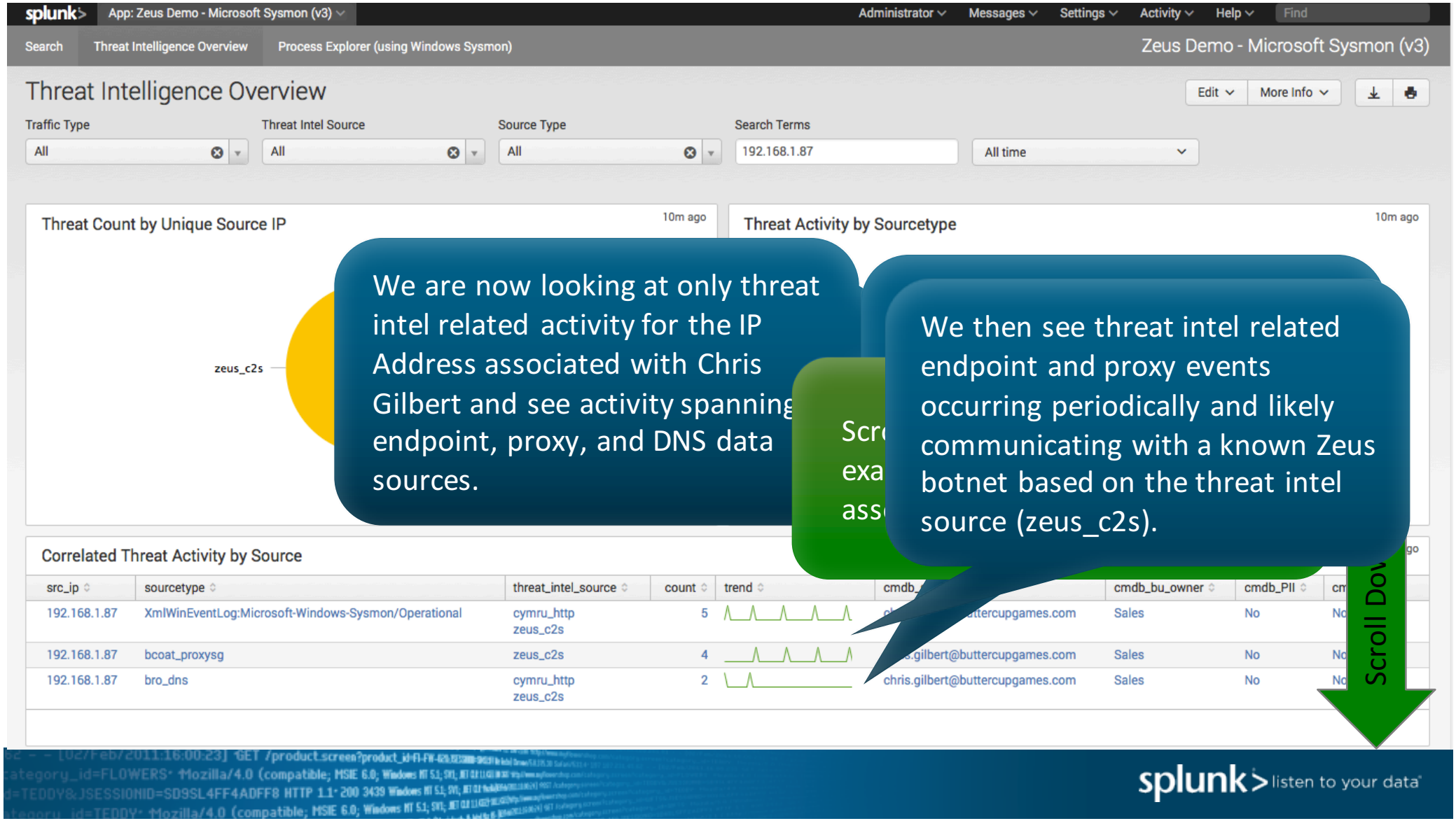
APT Transaction Flow Across Data Sources

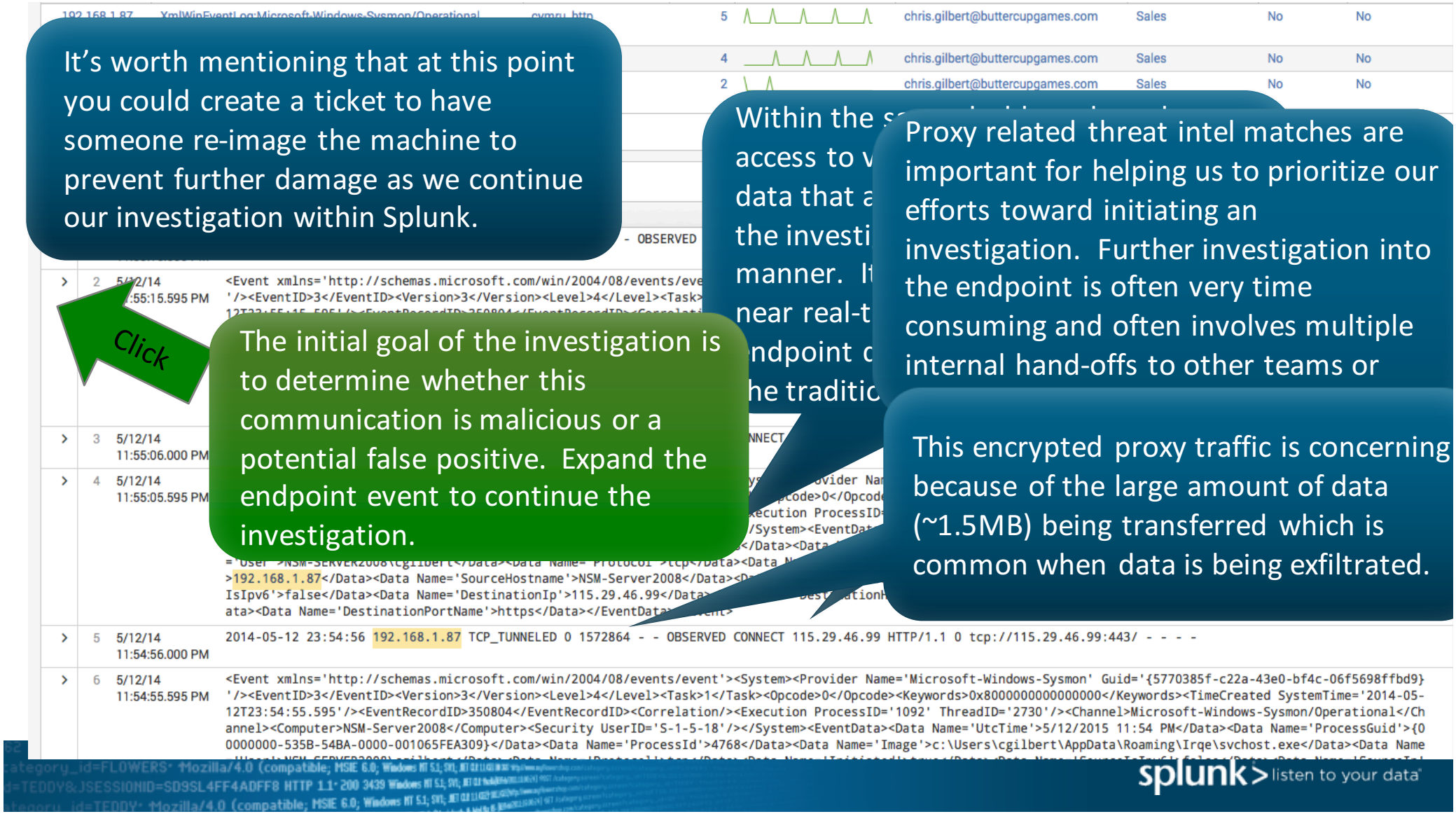



splunk> App: Zeus Demo - Microsoft Sysmon (v3)
Administrator
Messages
Settings
Activity
Help
Find
Search
Threat Intelligence Overview
Process Explorer (using Windows Sysmon)
Zeus Demo - Microsoft Sysmon (v3)
New Search
Save As
Close
index=zeus_demo3
All time
3,324 events (before 2/8/15 2:44:06
Job
Verbose Mode
Events (3,324)
Patterns
Format Timeline
Zoom Out
1 month per column
Prev 1 2 3 4 5 6 7 8 9 ... Next
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
To begin our investigation, we will start with a quick sear to familiarize ourselve 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
splunk> listen to your data


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 sourcetype="XmlWin
All time
10 events (before 2/8/15 7:53:11.000 PM)
Verbose Mode
Events (10)
Patterns
Statistics
Visualiz
Format Timeline
Zoom Out
Zoom to Selection
1 second per column
List
Format
20 Per Page
Hide Fields
All Fields
Selected Fields
host 1
source 1
sourcetype 1
tag 4
Interesting Fields
action 1
app 3
cmdb_app_lifecycle 1
cmdb_app_uses_ssn 1
cmdb_application_name 1
cmdb_bu_owner 1
cmdb_credit_card_data 1
tag
4 Values, 100% of events
Selected
Yes
No
Reports
Top values
Top values by time
Events with this field
Values
Count
%
communicate
7
70%
network
7
70%
process
3
30%
report
3
30%
Click
Lets get our day started by looking using threat intel to prioritize our efforts and focus on communication with known high risk entities.
at the
ata source.
g the
ysmon TA.
We have endpoint visibility into all network communication and can map each connection back to a process.
We also have detailed info on each process and can map it back to the user and parent process.
/Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2014-05-12T23:55:05.595'/><EventRecordID>350804</Ev
entRecordID><Correlation/><Execution ProcessID='1092' ThreadID='2729'/><Channel>Microsoft-Windows-Sysmon/Operational</Chann
splunk> listen to your data


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
<1m ago
src_ip
threat_intel_source
count
trend
cmdb_system_owner
cmdb_PII
cmdb_PCI
192.168.1.87
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
splunk> listen to your data


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)
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
zeus_c2s
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.
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
192.168.1.87 XmlWinEventLog:Microsoft-Windows-Sysmon/Operational cymru_http zeus_c2s 5 ttercupgames.com Sales No
192.168.1.87 bcoat_proxysg zeus_c2s 4 s.gilbert@buttercupgames.com Sales No
192.168.1.87 bro_dns cymru_http zeus_c2s 2 chris.gilbert@buttercupgames.com Sales No
Scroll Dow
splunk> listen to your data


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.
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
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.
chris.gilbert@buttercupgames.com
Sales
No
No
- OBSERVED
2014-05-12 23:54:56 192.168.1.87 TCP_TUNNELED 0 1572864 - - OBSERVED CONNECT 115.29.46.99 HTTP/1.1 0 tcp://115.29.46.99:443/ - - - -
splunk> listen to your data

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	115.29.46.99
	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 investi

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>

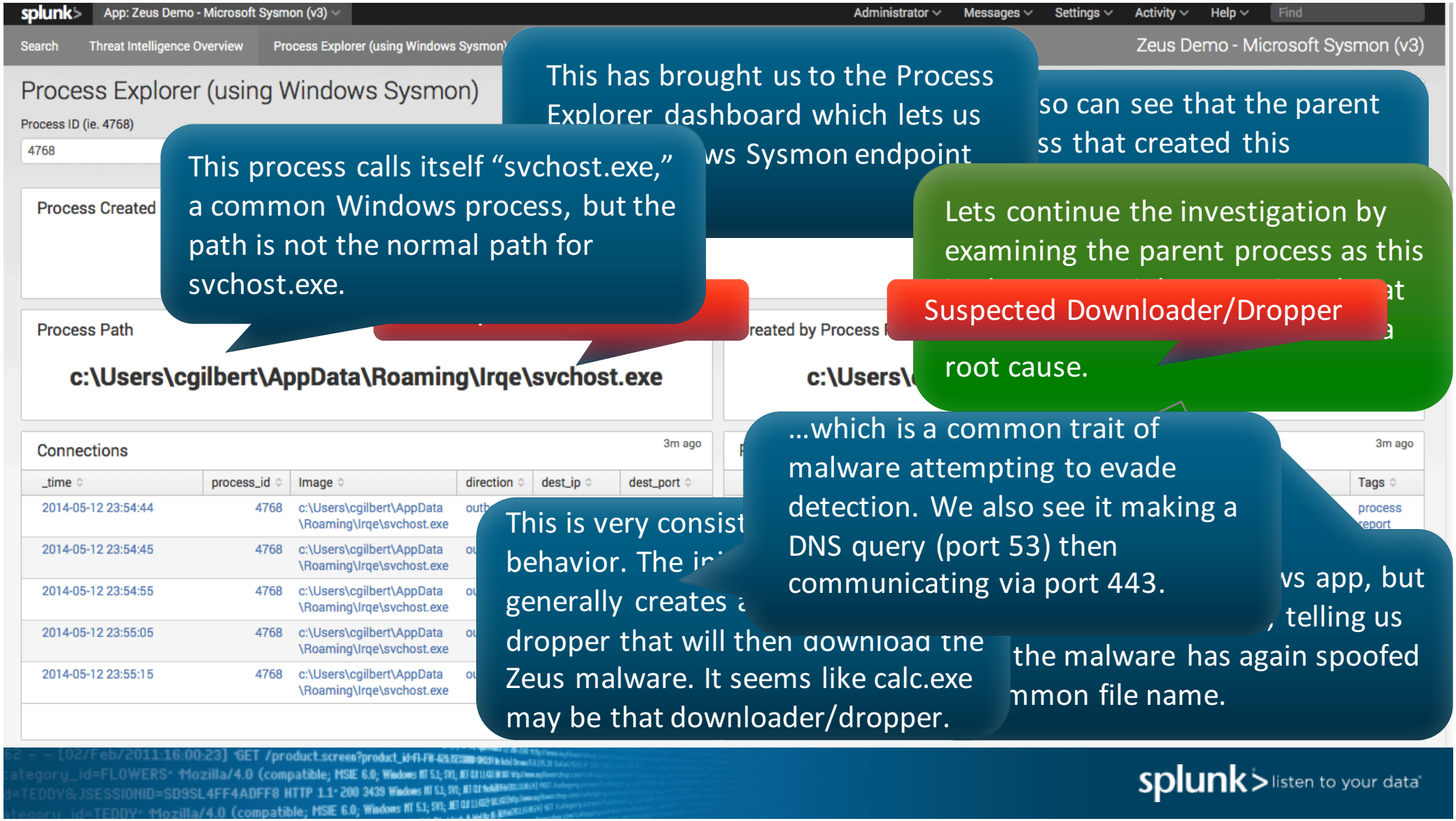
Event Actions

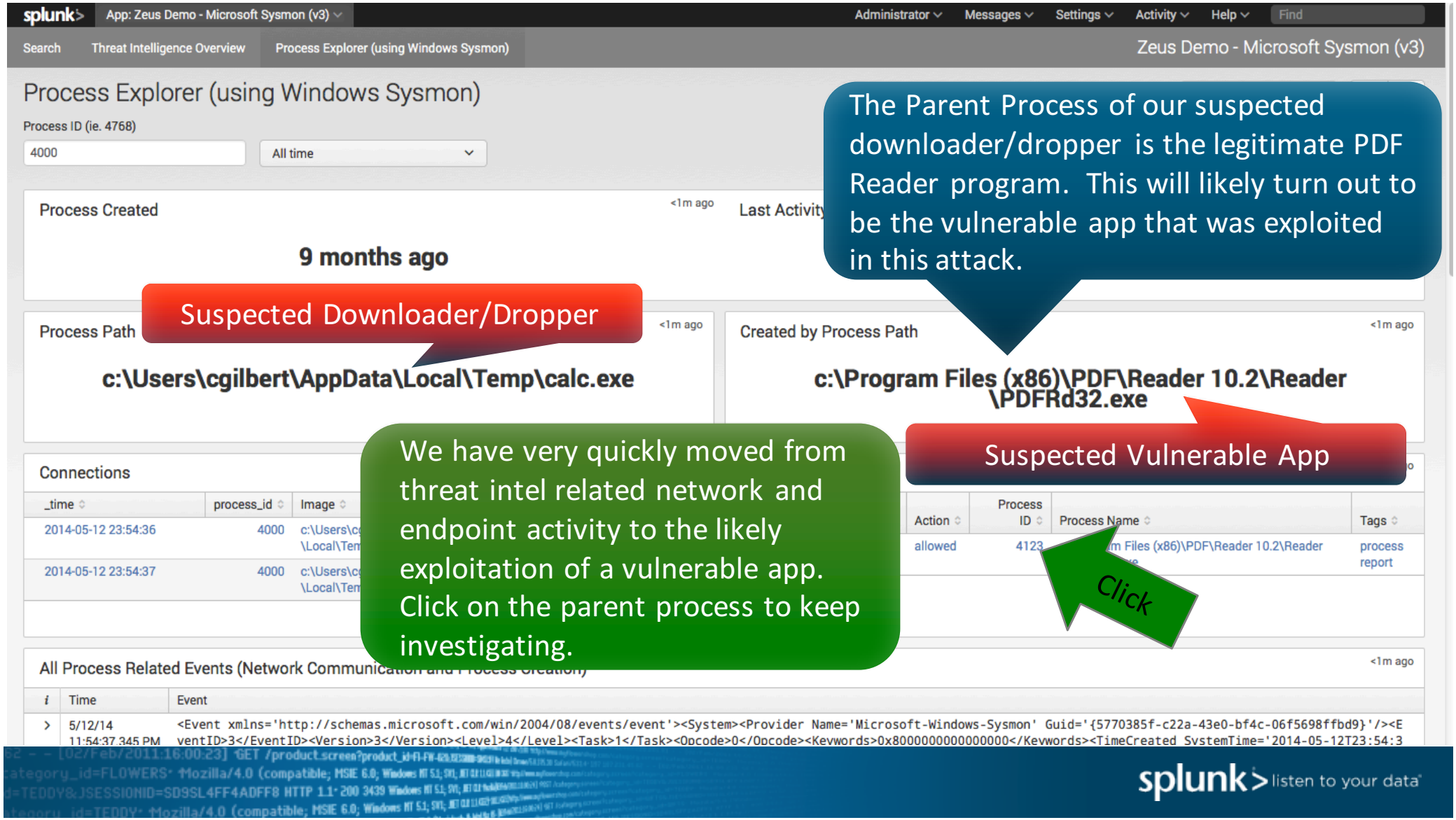
- Build Event Type
- Extract Fields
- Explore Process: 4768
- Show Source

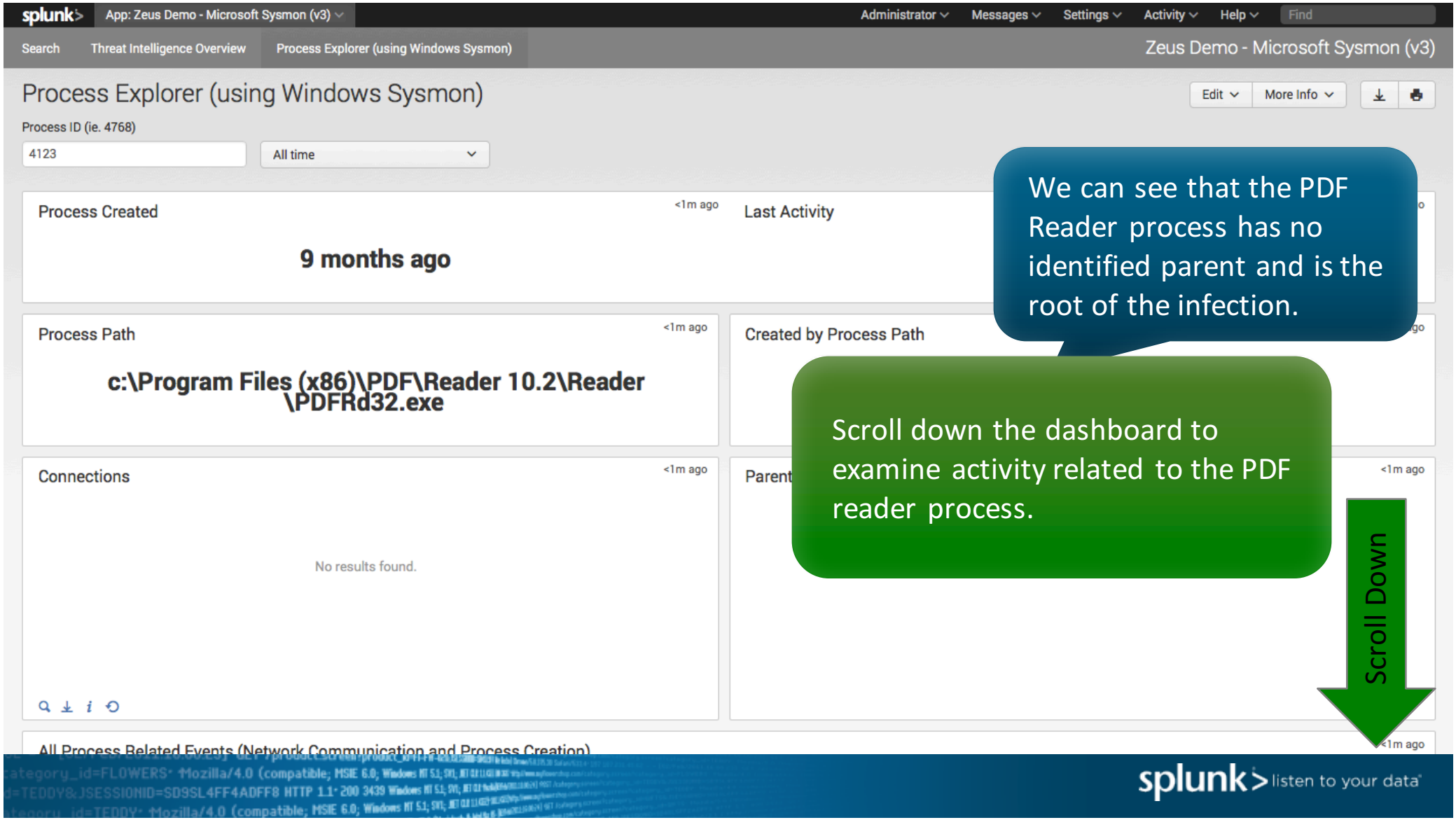
Click

	Value	Actions
	NSM-Server2008	
	www.vh44850.eurodir.ru	
	115.29.46.99	
DestinationPort		
DestinationPortName		
EventChannel	Micro t-W	
EventCode	3	
Guid	'{5770385f-	
Image	c:\Users\cg	
Initiated	true	
Keywords	0x80000000	
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
2014-05-12 23:54:45
2014-05-12 23:54:55
2014-05-12 23:55:05
2014-05-12 23:55:15
4768
c:\Users\cgilbert\AppData\Roaming\Irqe\svchost.exe
This has brought us to the Process Explorer dashboard which lets us
ws Sysmon endpoint
so can see that the parent
ss 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
Suspected Downloader/Dropper
root cause.
…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 consist
behavior. The in
generally creates a
dropper that will then download the Zeus malware. It seems like calc.exe may be that downloader/dropper.
vs app, but
, telling us
the malware has again spoofed
mmon file name.
Tags
process
report
splunk> listen to your data


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
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.
Connections
_time
process_id
Image
Action
Process ID
Process Name
Tags
2014-05-12 23:54:36
4000
allowed
4123
process report
2014-05-12 23:54:37
4000
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> listen to your data


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> listen to your data

All Process Related Events (Network Communication and Process Creation)

3m ag

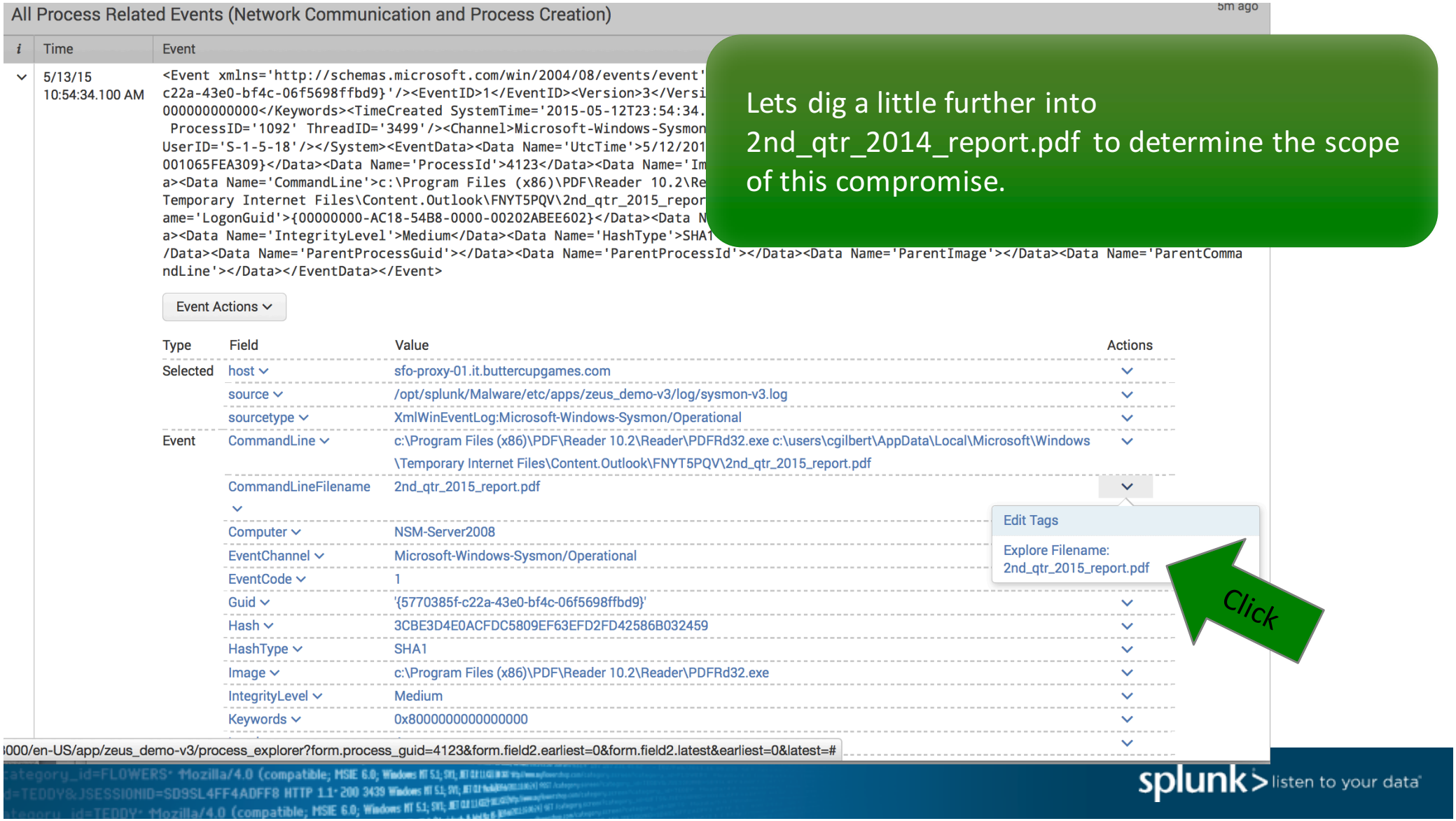
i	Time	Event
⌄	5/13/15 10:54:34.100 AM	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'> c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>1</EventID><Version>3</Ver 000000000000</Keywords><TimeCreated SystemTime='2015-05-12T23:54:3 ProcessID='1092' ThreadID='3499'/><Channel>Microsoft-Windows-Sysm 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>

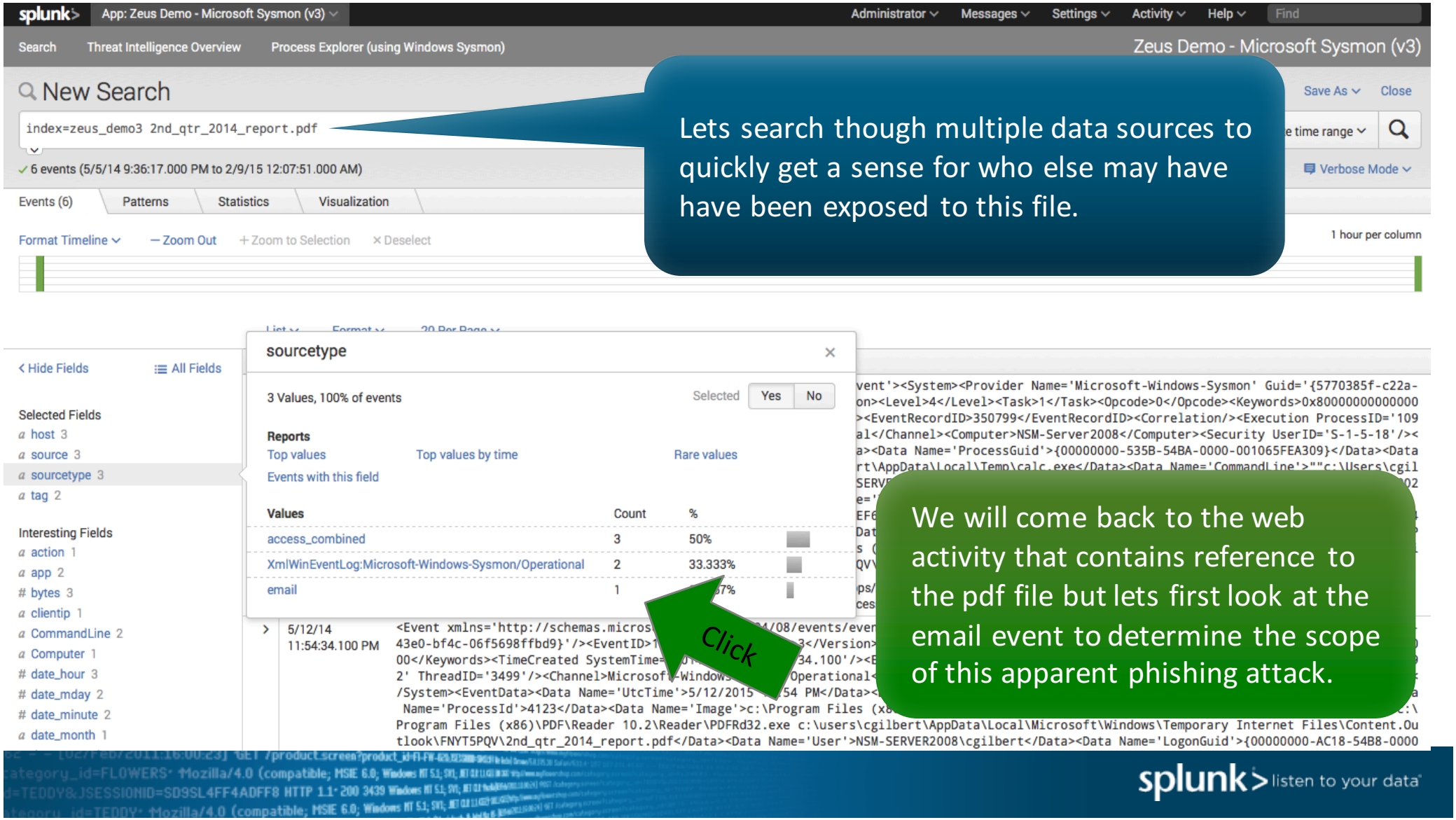
Event Actions ⌄

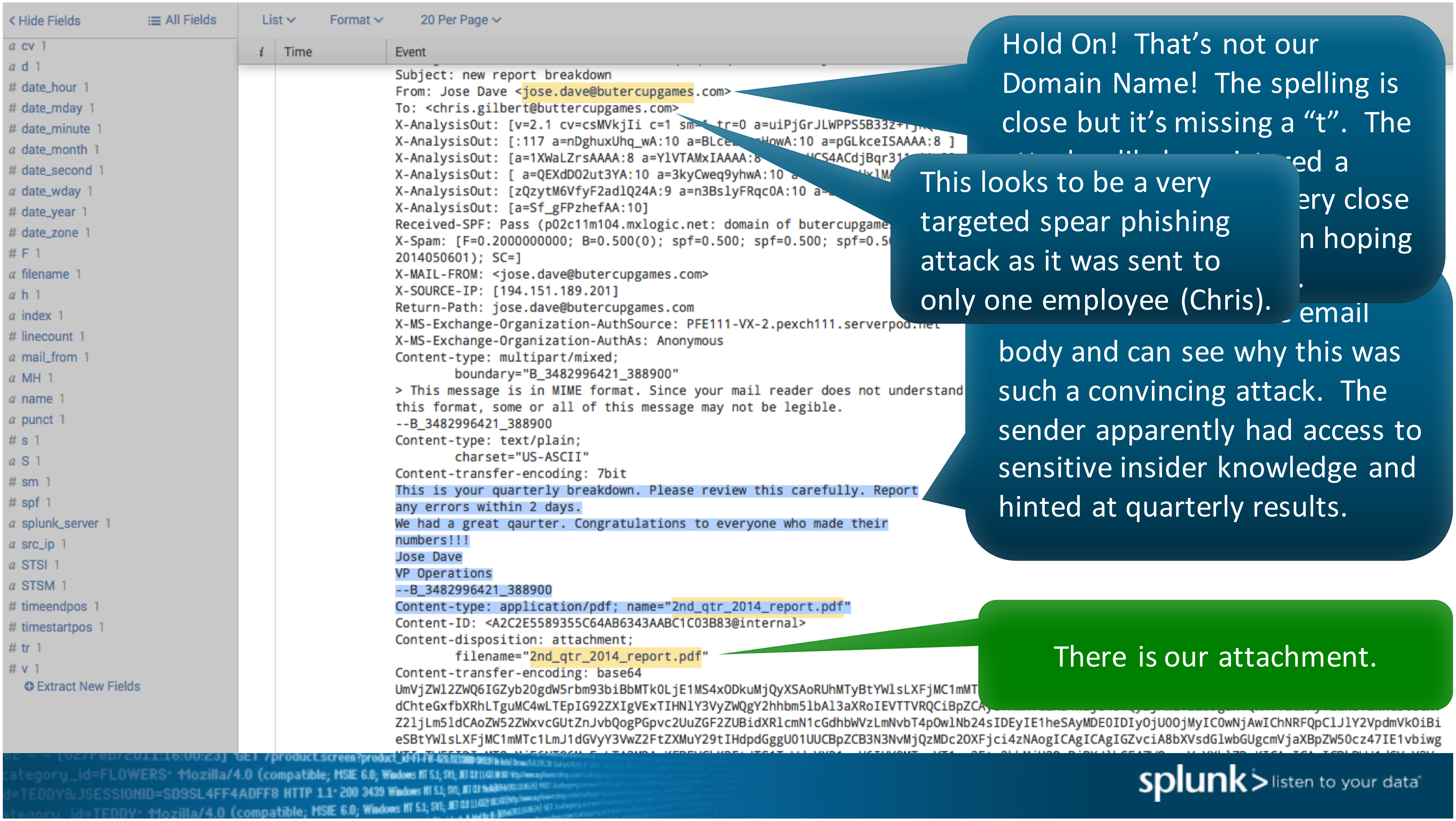
Type	Field	Value
Selected	host ⌄	sfo-proxy-01.it.buttercupgames.com
	source ⌄	/opt/splunk/Malware/etc/apps/zeus_demo-v3/log/sysmon-v3.log
	sourcetype ⌄	XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
Event	CommandLine ⌄	c:\Program Files (x86)\PDF\Reader 10.2\Reader\PDFRd32.exe c:\users\cgilbert\AppData\Local\Microsoft\Windows\Temporary 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!

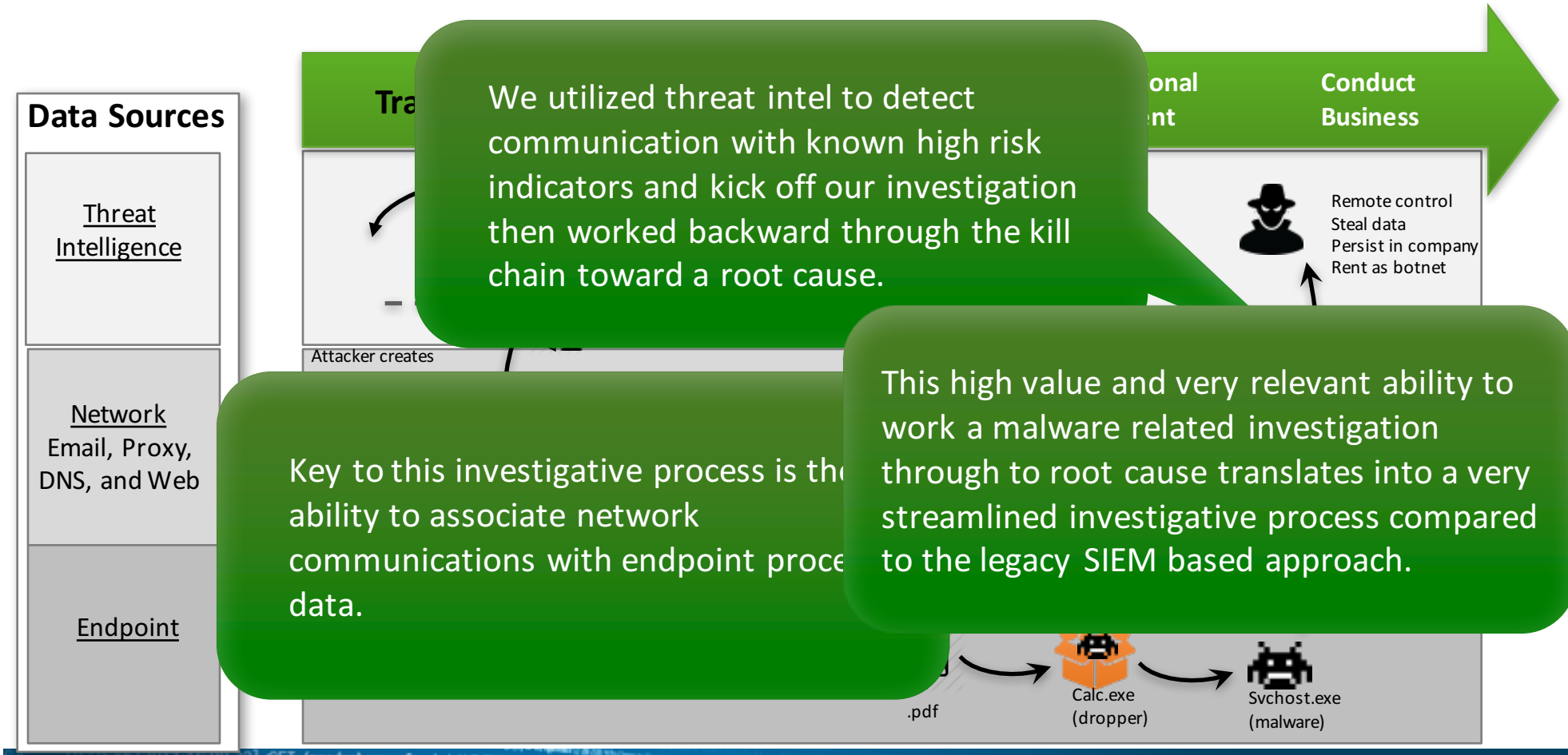

All Process Related Events (Network Communication and Process Creation)
5m ago
Time
Event
5/13/15
10:54:34.100 AM
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'
c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>1</EventID><Version>3</Versi
000000000000</Keywords><TimeCreated SystemTime='2015-05-12T23:54:34.
ProcessID='1092' ThreadID='3499'/><Channel>Microsoft-Windows-Sysmon
UserID='S-1-5-18'/></System><EventData><Data Name='UtcTime'>5/12/201
001065FEA309}</Data><Data Name='ProcessId'>4123</Data><Data Name='Im
a><Data Name='CommandLine'>c:\Program Files (x86)\PDF\Reader 10.2\Re
Temporary Internet Files\Content.Outlook\FNYT5PQV\2nd_qtr_2015_repor
ame='LogonGuid'>{00000000-AC18-54B8-0000-00202ABEE602}</Data><Data N
a><Data Name='IntegrityLevel'>Medium</Data><Data Name='HashType'>SHA1
/Data><Data Name='ParentProcessGuid'></Data><Data Name='ParentProcessId'></Data><Data Name='ParentImage'></Data><Data Name='ParentComma
ndLine'></Data></EventData></Event>
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
Edit Tags
Explore Filename:
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
Click
Lets dig a little further into 2nd_qtr_2014_report.pdf to determine the scope of this compromise.
000/en-US/app/zeus_demo-v3/process_explorer?form.process_guid=4123&form.field2.earliest=0&form.field2.latest&earliest=0&latest=#
splunk> listen to your data


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
time range
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
splunk> listen to your data



Hide Fields
All Fields
List
Format
20 Per Page
Time
Event
Subject: new report breakdown
From: Jose Dave <jose.dave@butercupgames.com>
To: <chris.gilbert@buttercupgames.com>
Received-SPF: Pass (p02c11m104.mxlogic.net: domain of butercupgame
X-MAIL-FROM: <jose.dave@butercupgames.com>
X-SOURCE-IP: [194.151.189.201]
Return-Path: jose.dave@butercupgames.com
X-MS-Exchange-Organization-AuthAs: Anonymous
Content-type: multipart/mixed;
boundary="B_3482996421_388900"
> This message is in MIME format. Since your mail reader does not understand
this format, some or all of this message may not be legible.
--B_3482996421_388900
Content-type: text/plain;
charset="US-ASCII"
Content-transfer-encoding: 7bit
This is your quarterly breakdown. Please review this carefully. Report
any errors within 2 days.
We had a great qaurter. Congratulations to everyone who made their
numbers!!!
Jose Dave
VP Operations
--B_3482996421_388900
Content-type: application/pdf; name="2nd_qtr_2014_report.pdf"
Content-ID: <A2C2E5589355C64AB6343AABC1C03B83@internal>
Content-disposition: attachment;
filename="2nd_qtr_2014_report.pdf"
Content-transfer-encoding: base64
Hold On! That's not our Domain Name! The spelling is close but it's missing a "t". The
ed a
ery close
n hoping
email
This looks to be a very targeted spear phishing attack as it was sent to only one employee (Chris).
body and can see why this was such a convincing attack. The sender apparently had access to sensitive insider knowledge and hinted at quarterly results.
There is our attachment.
splunk> listen to your data

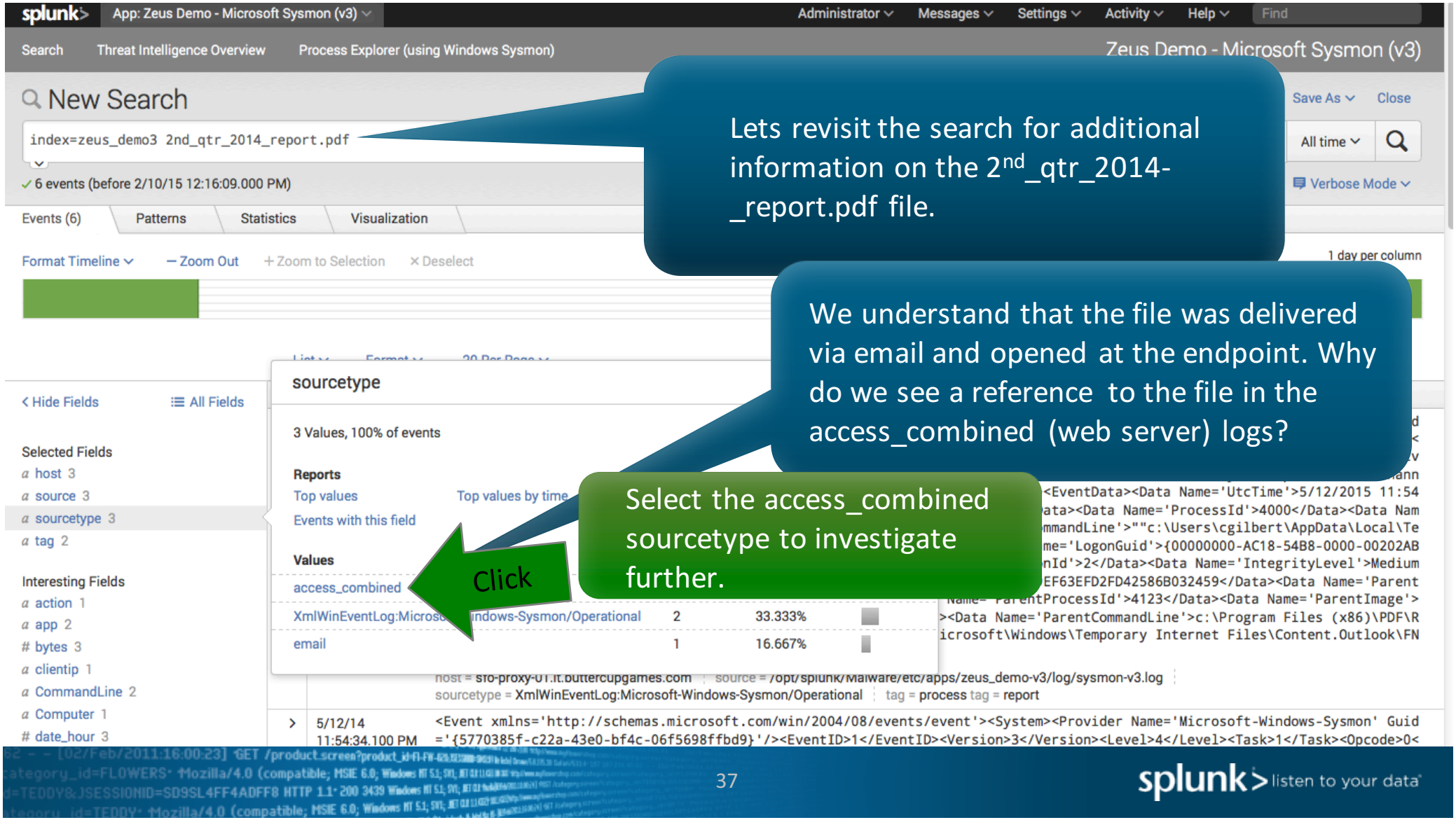
Root Cause Recap

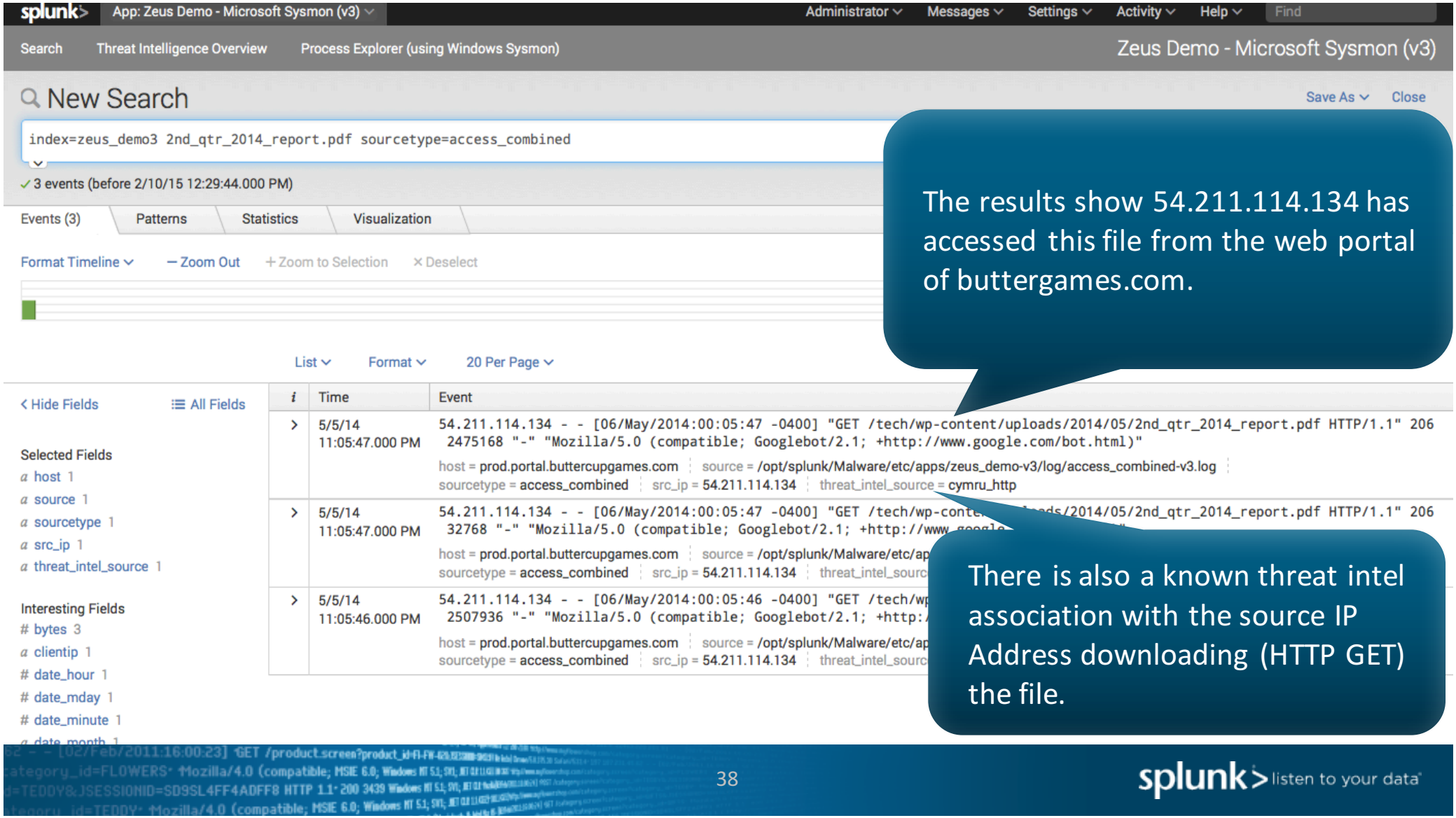


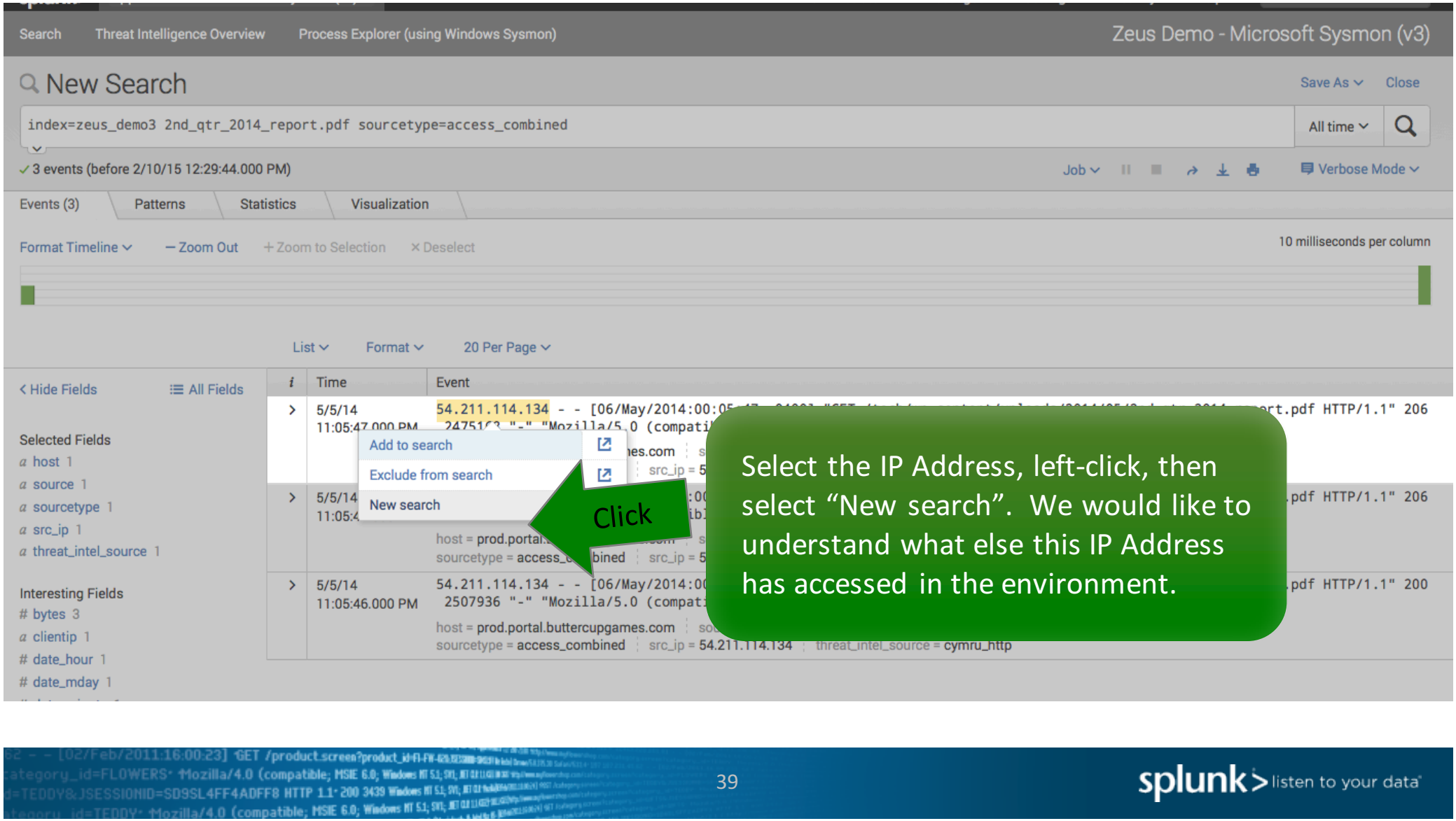
We utilized threat intel to detect communication with known high risk indicators and kick off our investigation then worked backward through the kill chain toward a root cause.

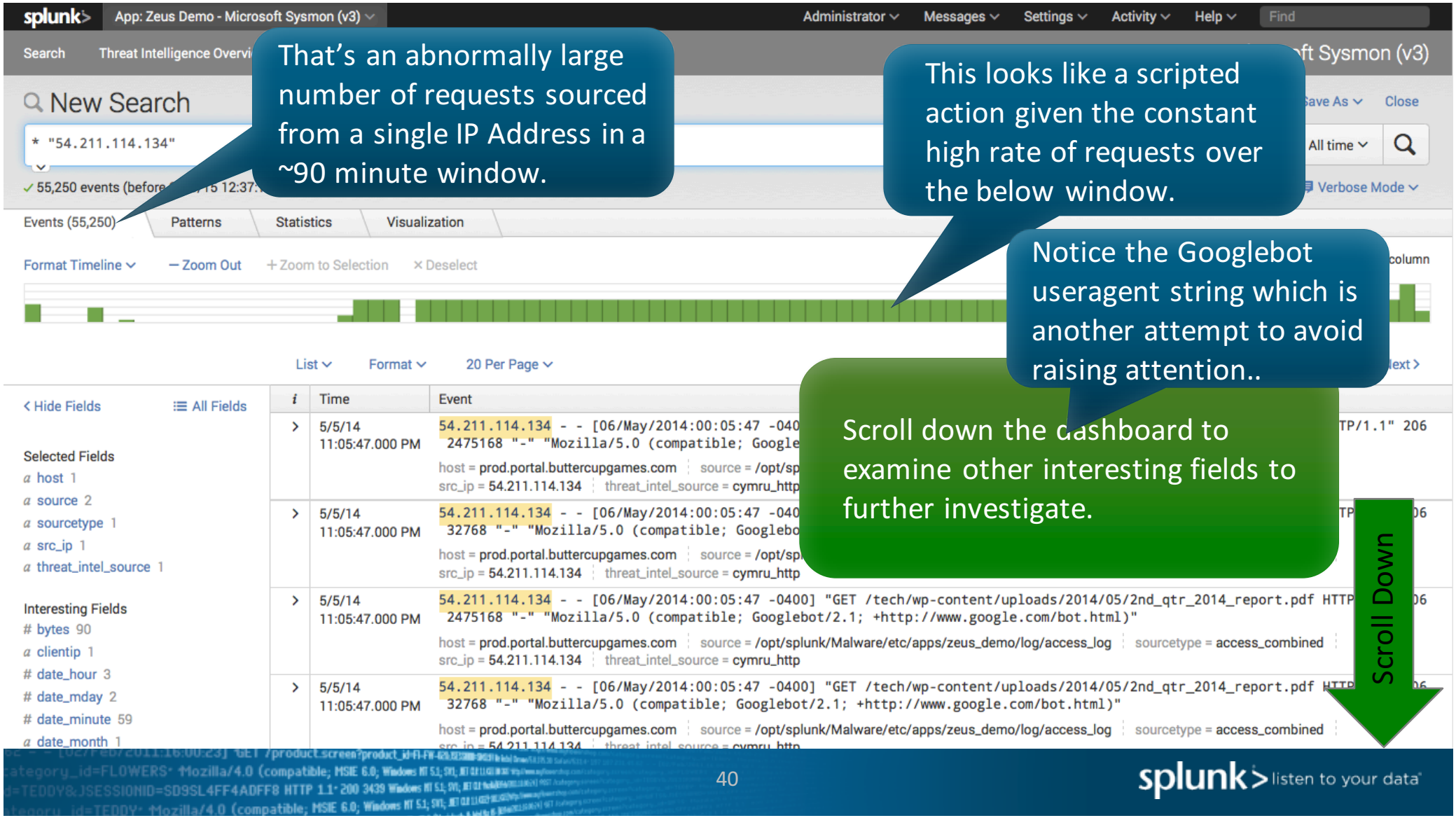
Key to this investigative process is the ability to associate network communications with endpoint proce data.

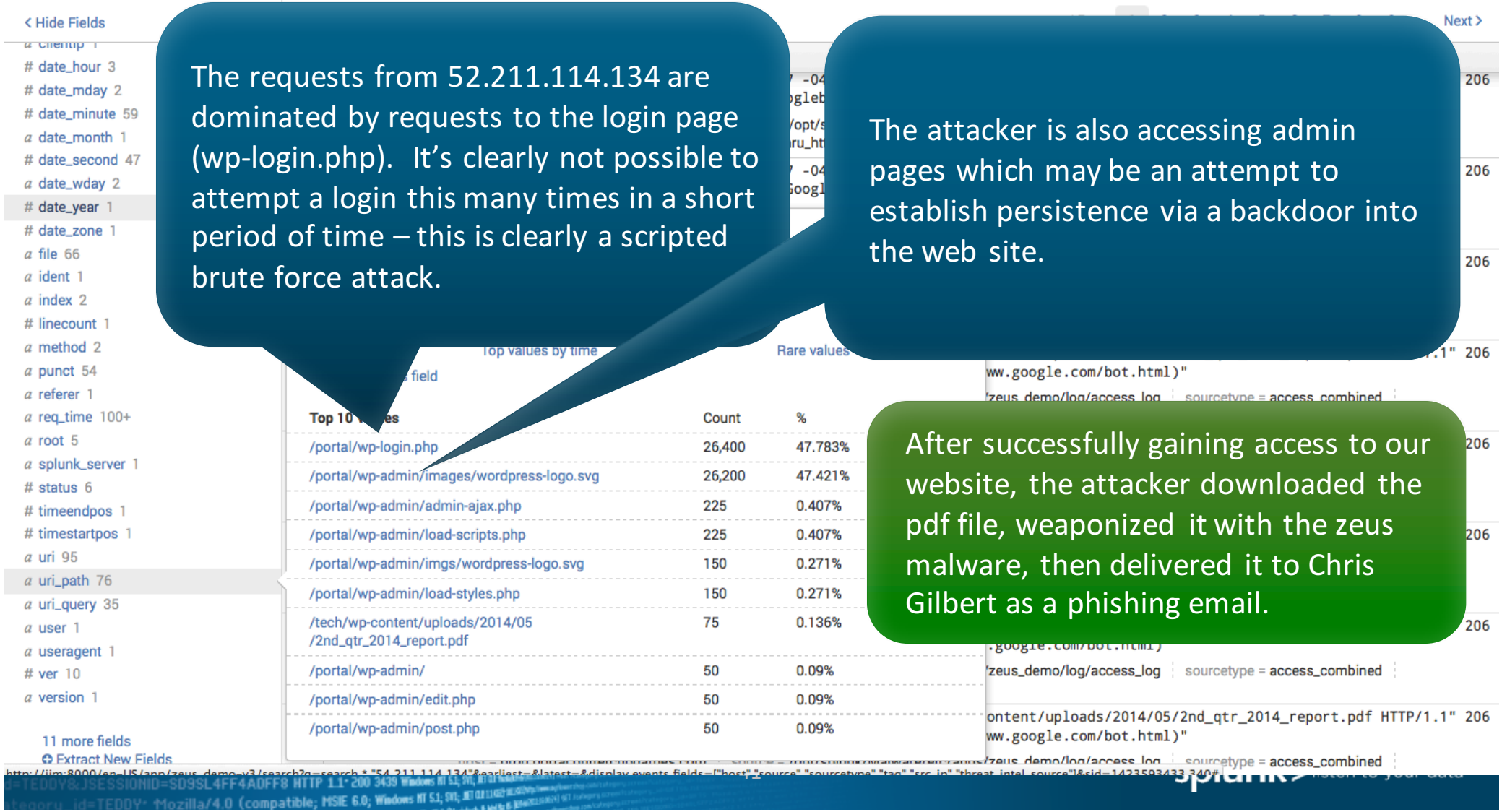
This high value and very relevant ability to work a malware related investigation through to root cause translates into a very streamlined investigative process compared to the legacy SIEM based approach.



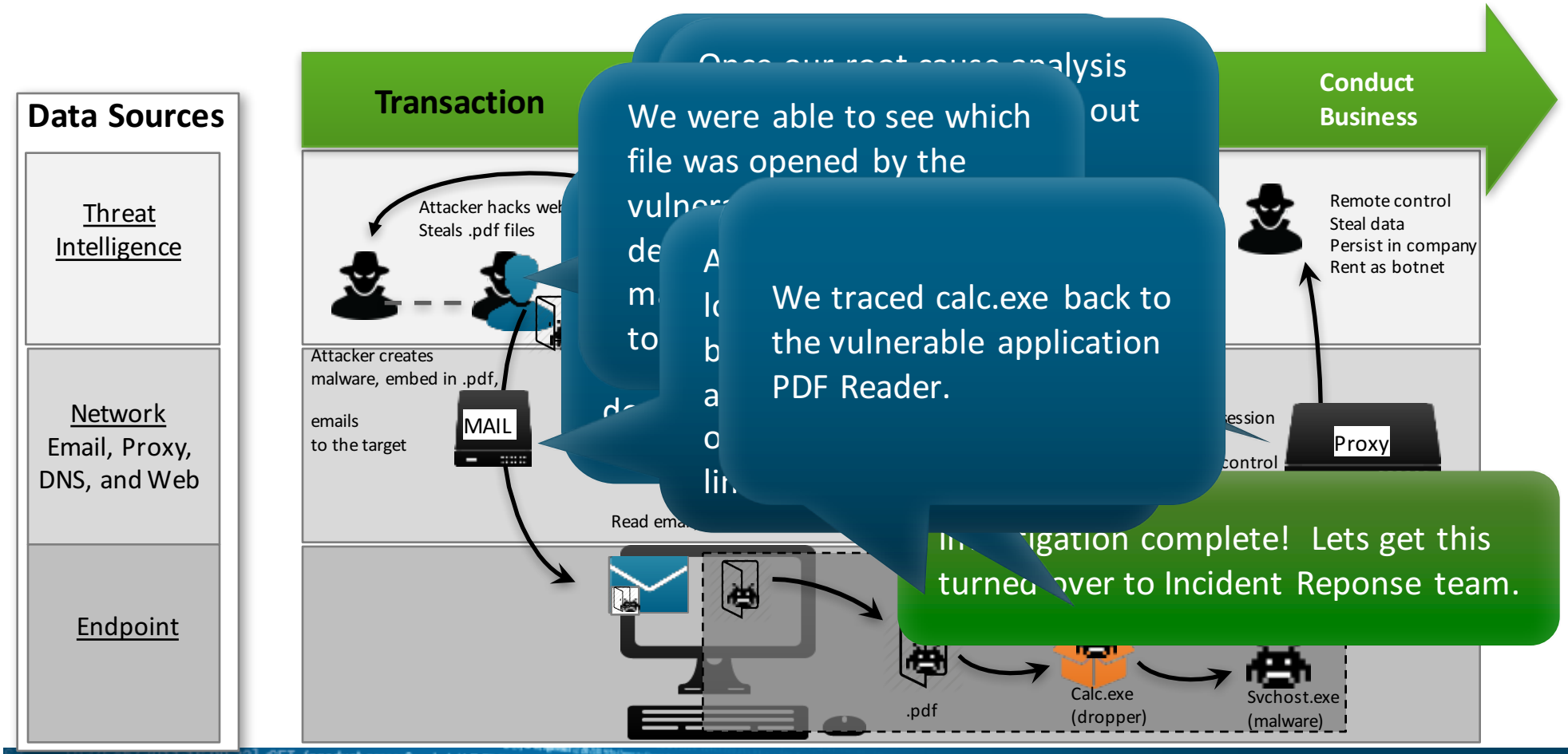






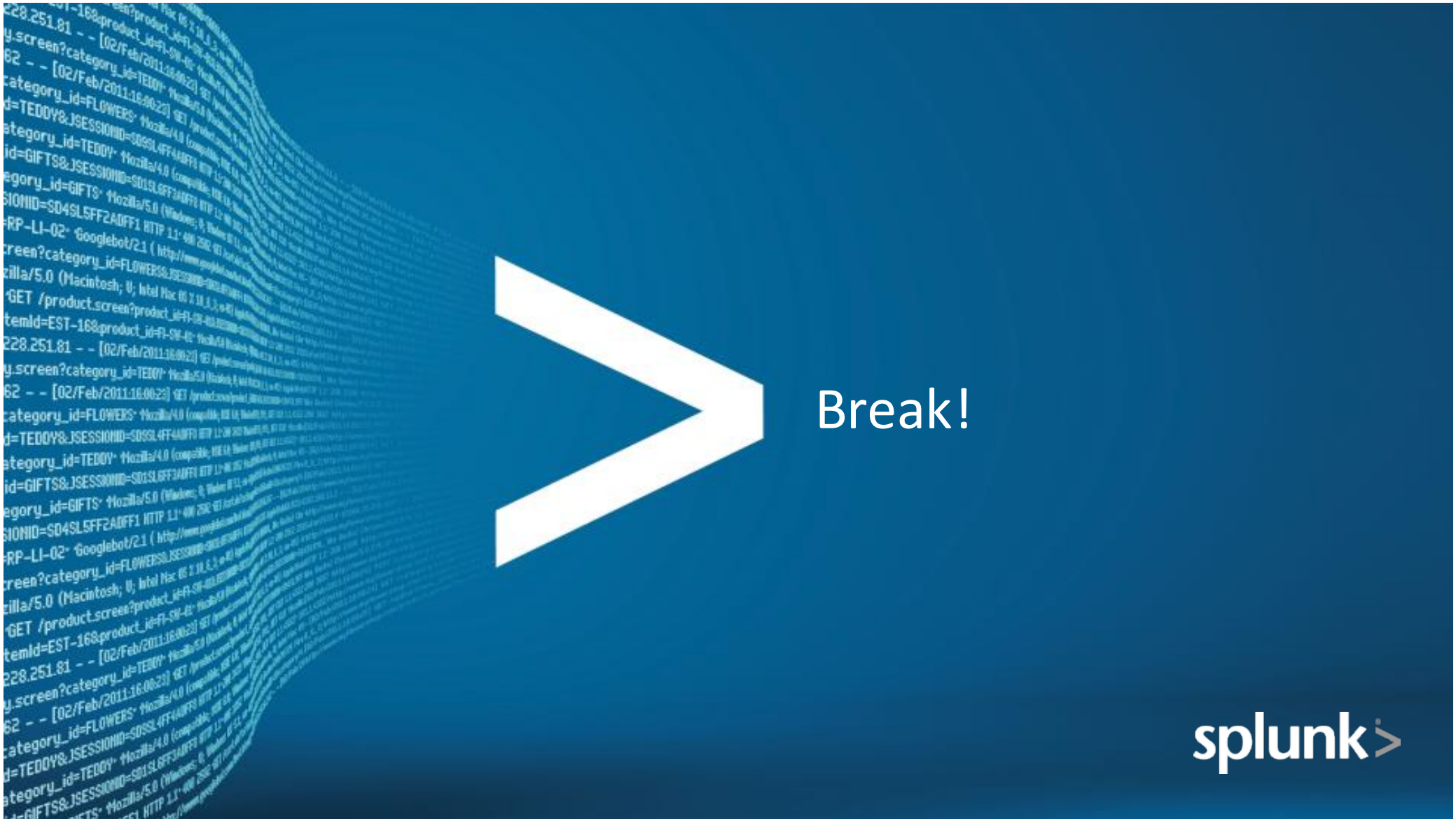

The requests from 52.211.114.134 are dominated by requests to the login page (wp-login.php). It's clearly not possible to attempt a login this many times in a short period of time – this is clearly a scripted brute force attack.
The attacker is also accessing admin pages which may be an attempt to establish 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.
Hide Fields
Next
Top values by time
Rare values
Count
%
/portal/wp-login.php 26,400 47.783%
/portal/wp-admin/images/wordpress-logo.svg 26,200 47.421%
/portal/wp-admin/admin-ajax.php 225 0.407%
/portal/wp-admin/load-scripts.php 225 0.407%
/portal/wp-admin/imgs/wordpress-logo.svg 150 0.271%
/portal/wp-admin/load-styles.php 150 0.271%
/tech/wp-content/uploads/2014/05/2nd_qtr_2014_report.pdf 75 0.136%
/portal/wp-admin/ 50 0.09%
/portal/wp-admin/edit.php 50 0.09%
/portal/wp-admin/post.php 50 0.09%
date_hour 3
date_mday 2
date_minute 59
a date_month 1
date_second 47
a date_wday 2
date_year 1
date_zone 1
a file 66
a ident 1
a index 2
linecount 1
a method 2
a punct 54
a referer 1
a req_time 100+
a root 5
a splunk_server 1
status 6
timeendpos 1
timestartpos 1
a uri 95
a uri_path 76
a uri_query 35
a user 1
a useragent 1
ver 10
a version 1
11 more fields
Extract New Fields
206
sourcetype = access_combined
splunk>

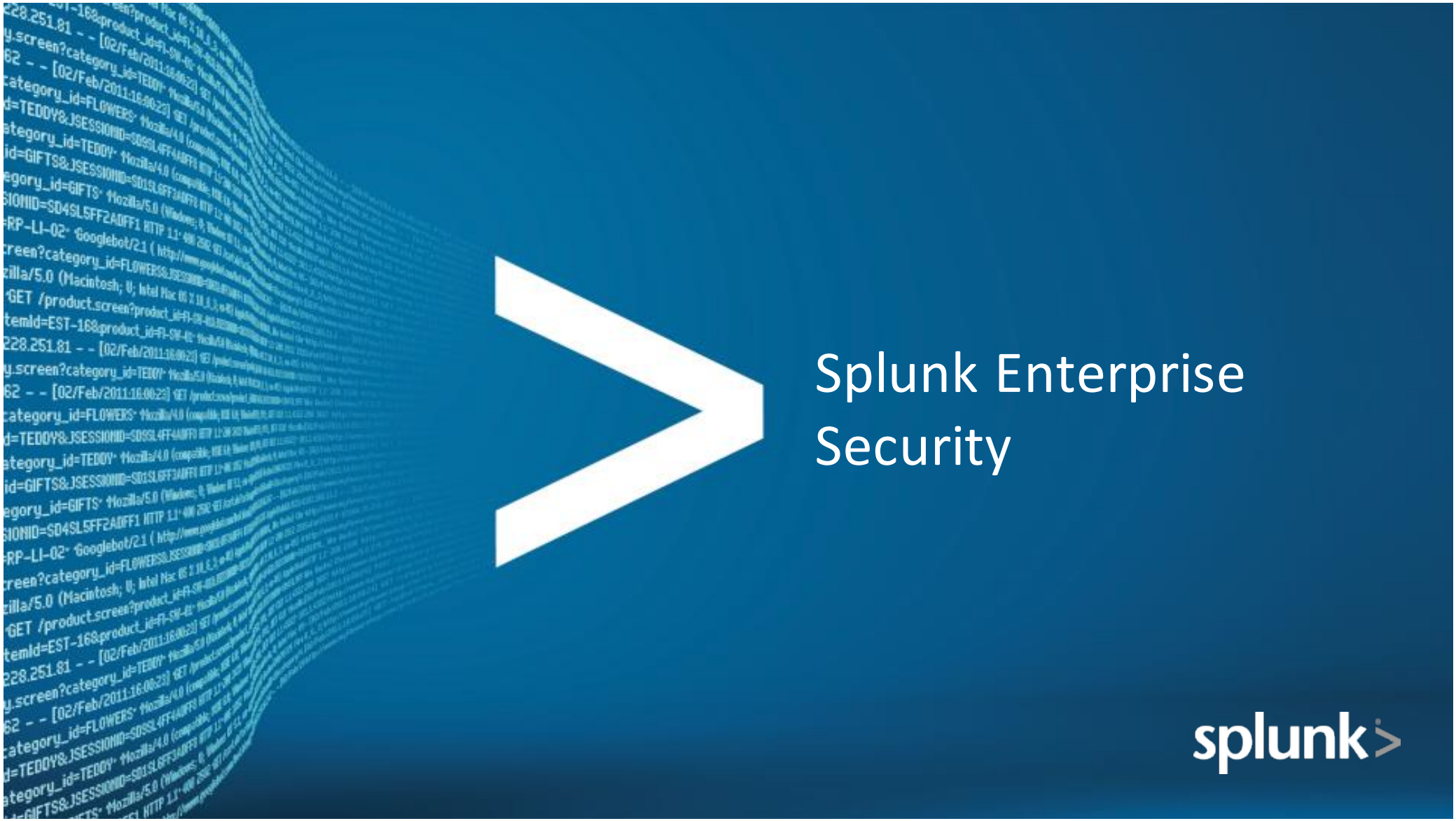
Kill Chain Analysis Across Data Sources

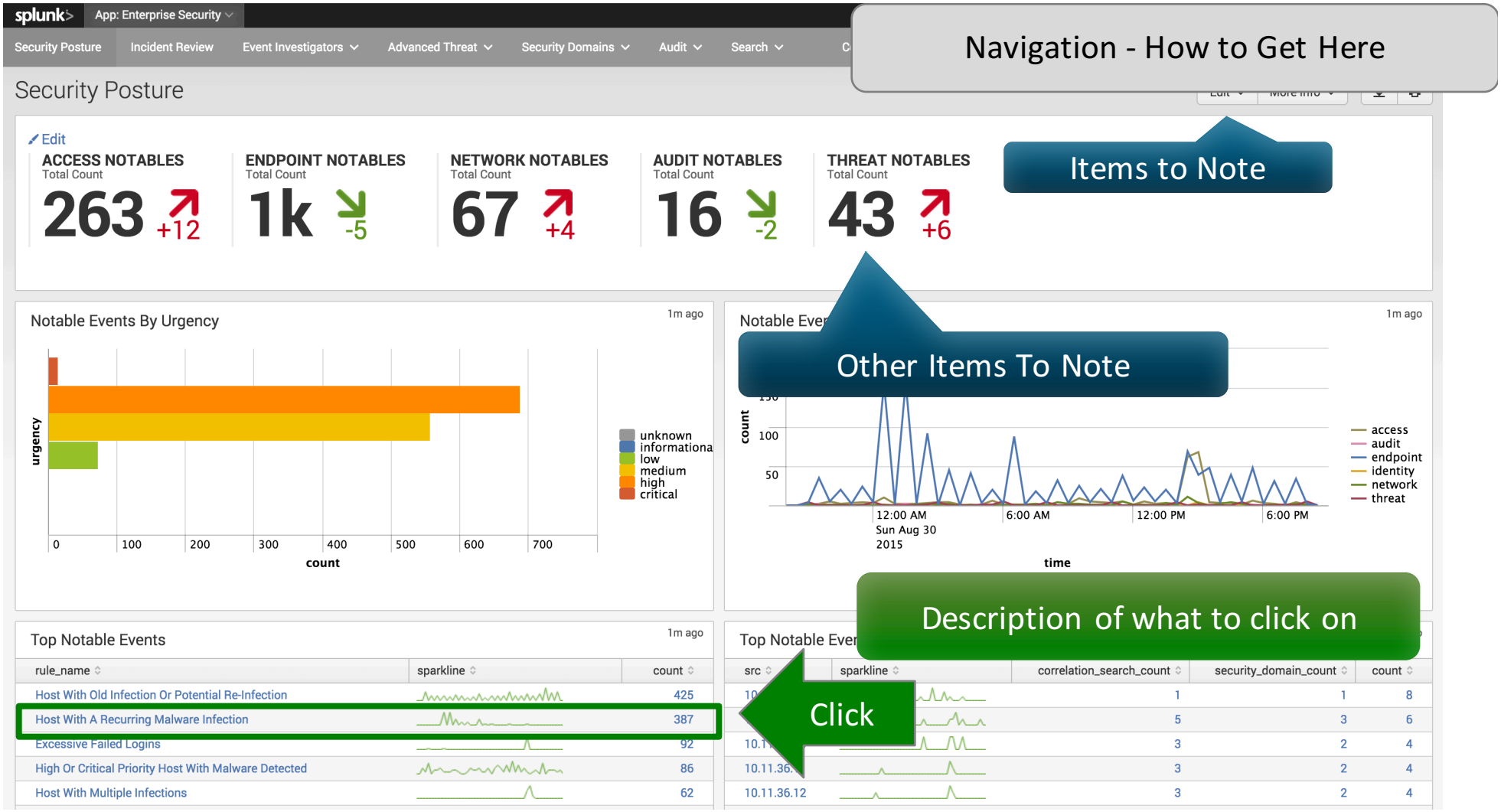


Want to Follow Along?

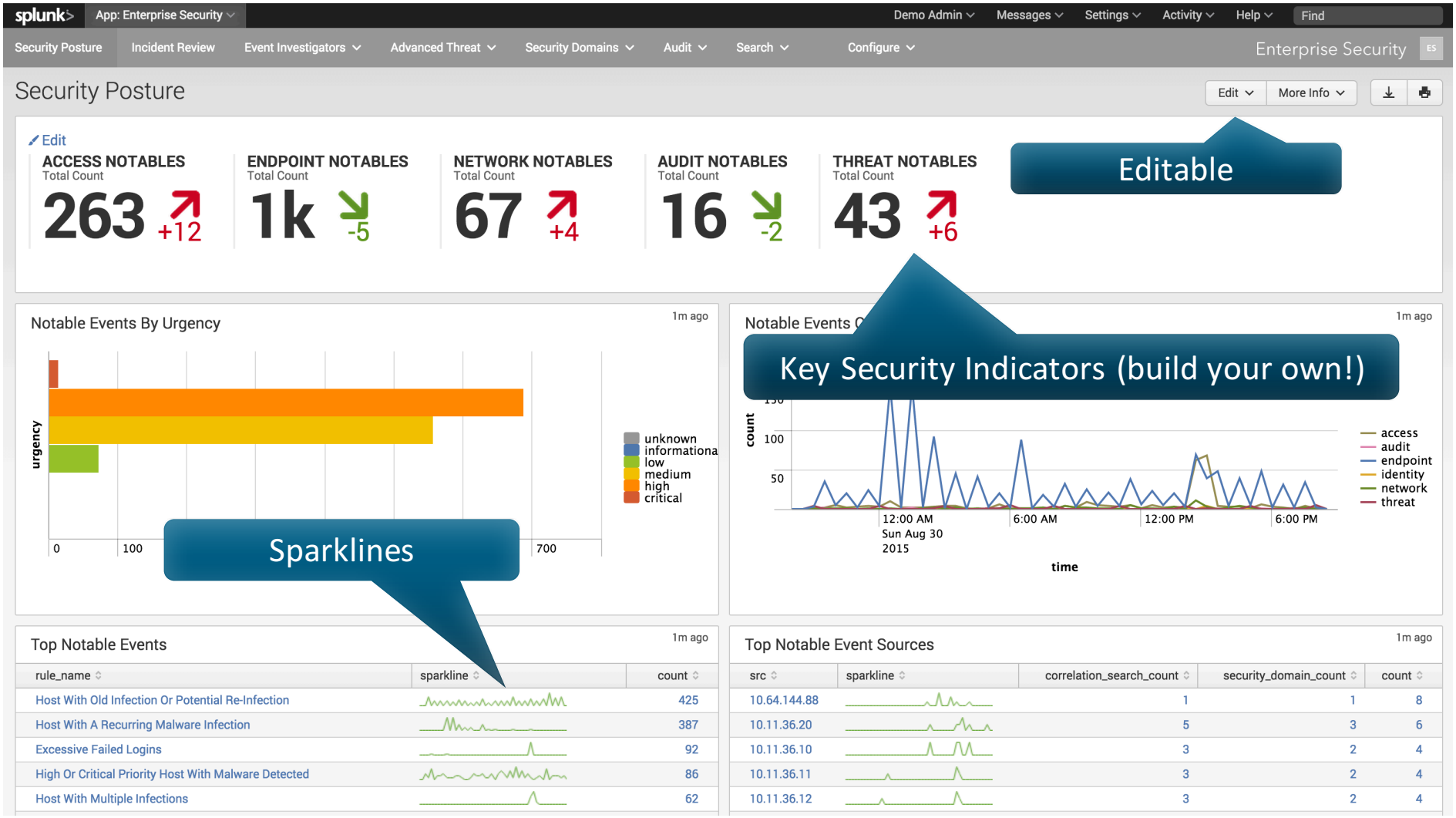
- Download Splunk **6.4.2**http://www.splunk.com/en_us/download-21.html
- Download & Install the Machine Learning Toolkit http://tiny.cc/splunkmlapp

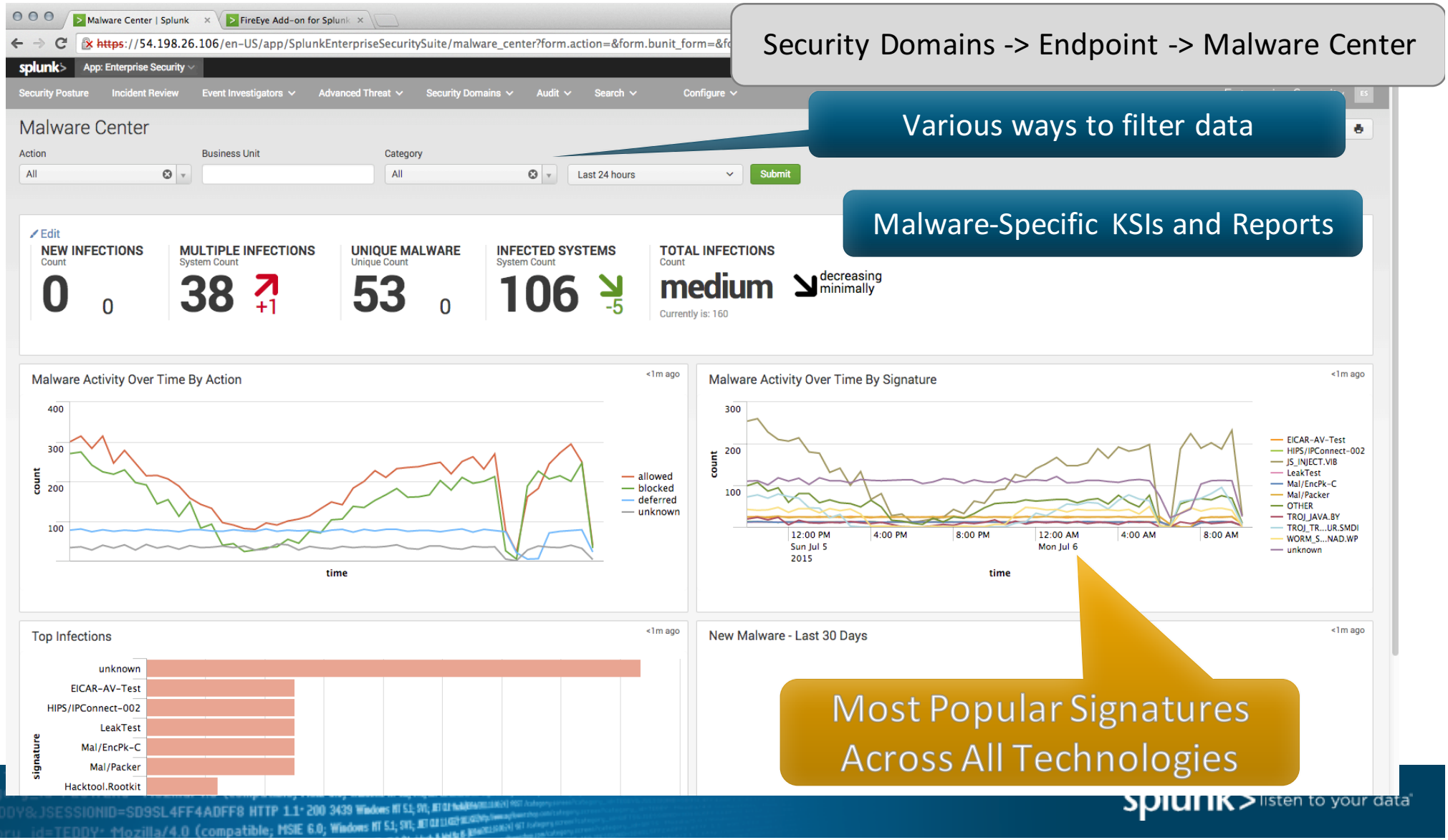

Break!
splunk>

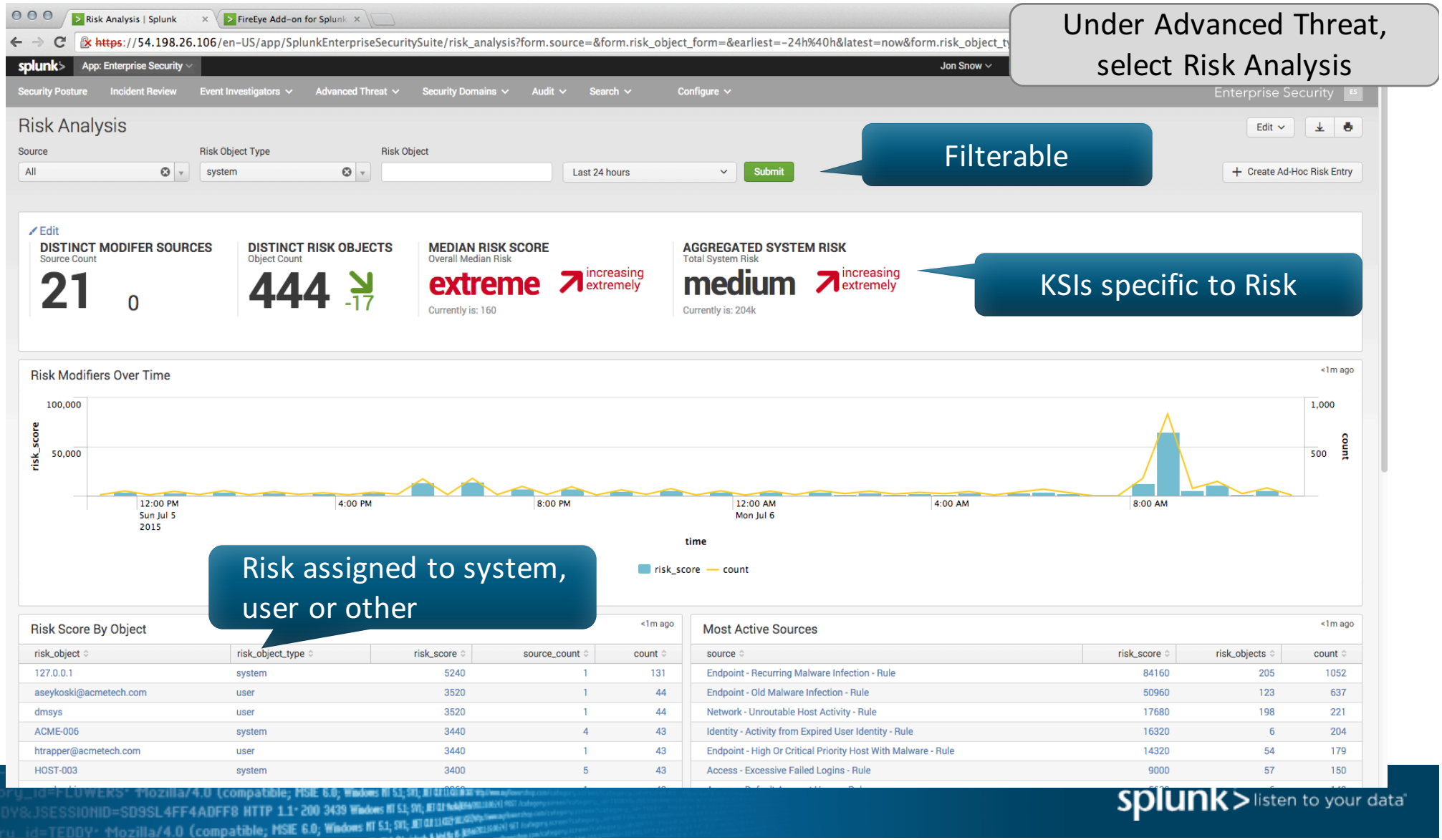

Splunk Enterprise
Security
splunk>

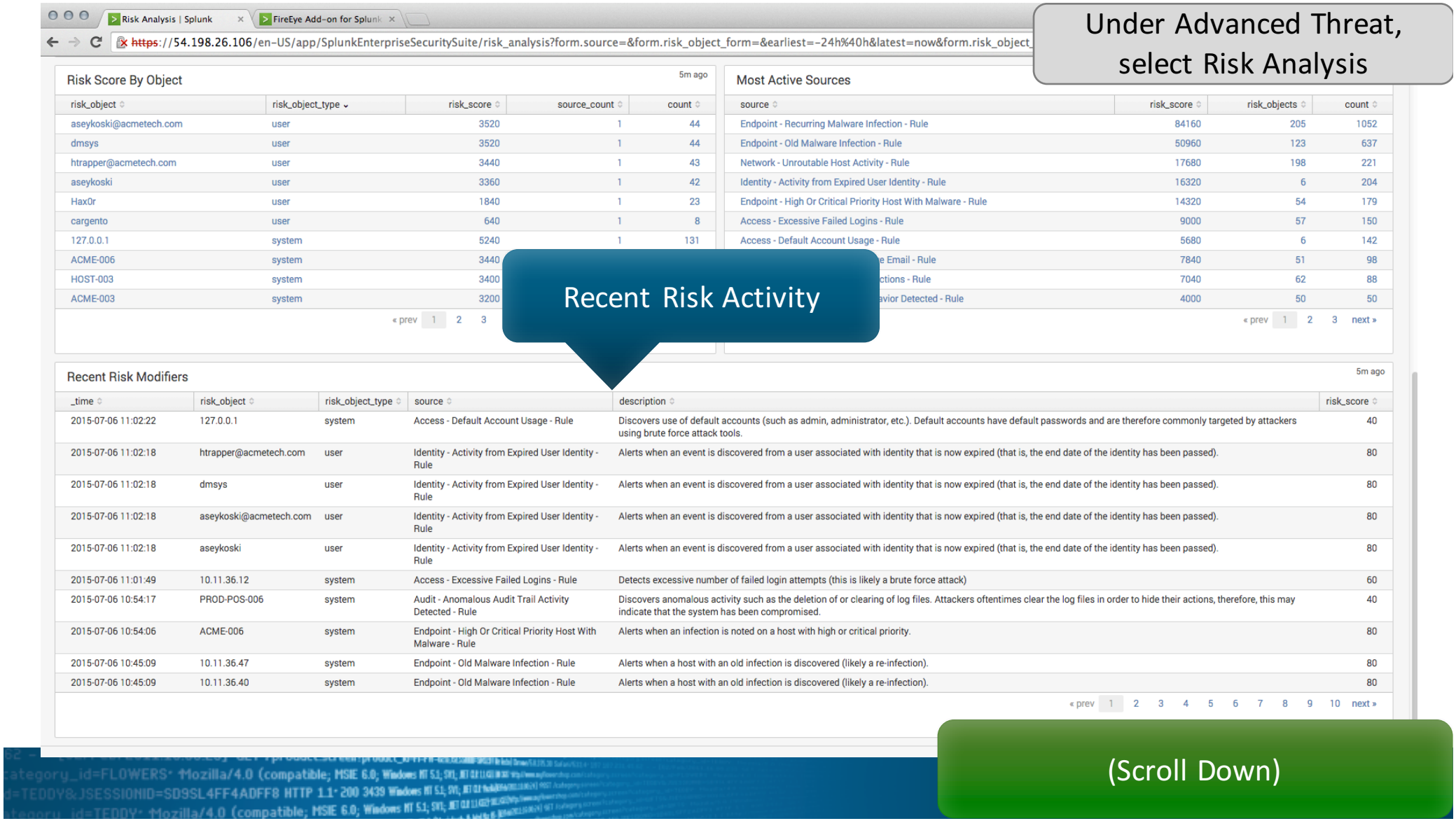


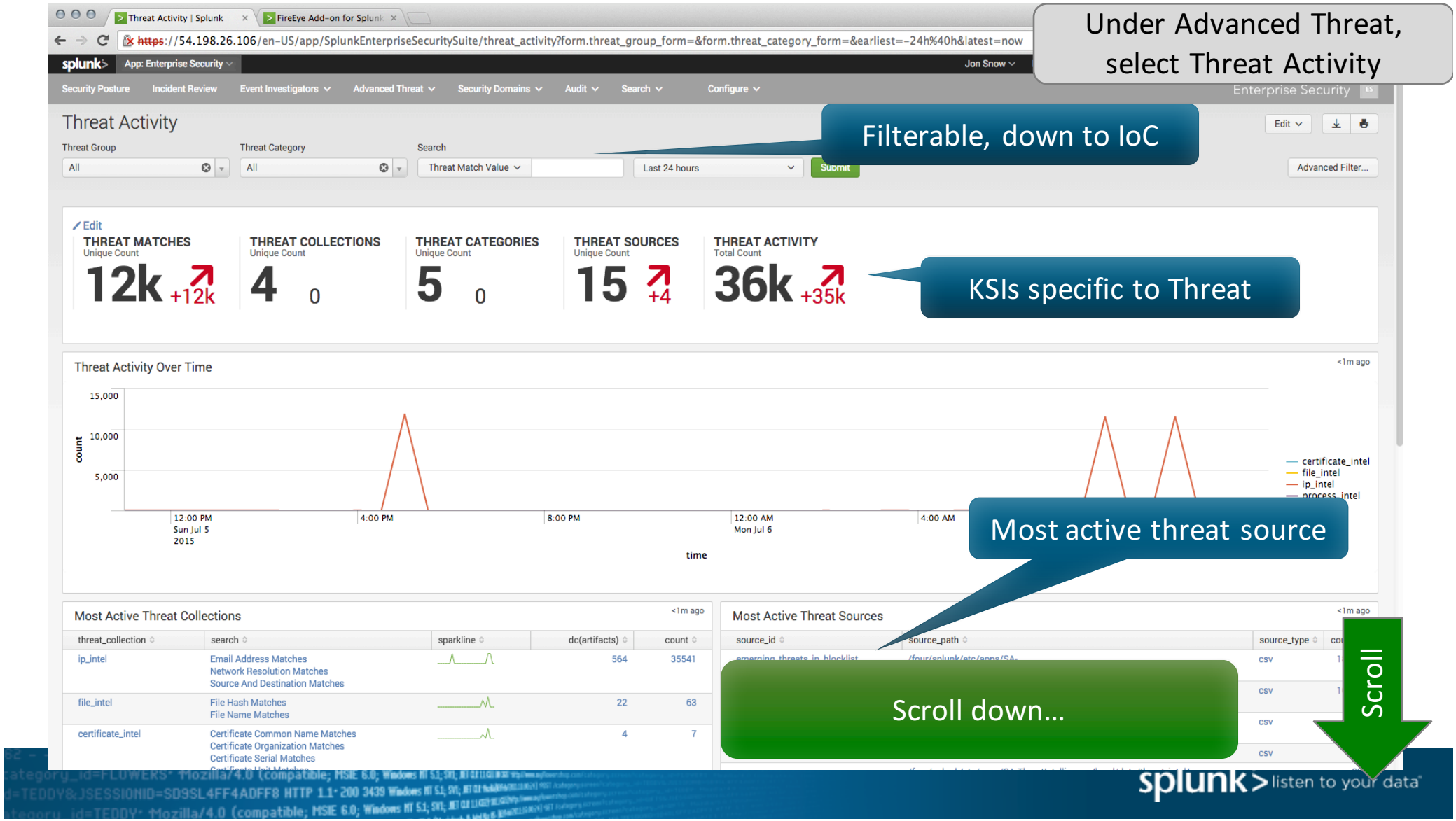
splunk> listen to your data




Security Domains -> Endpoint -> Malware Center
Various ways to filter data
Malware-Specific KSIs and Reports
Most Popular Signatures Across All Technologies
Malware Center | Splunk
FireEye Add-on for Splunk
https://54.198.26.106/en-US/app/SplunkEnterpriseSecuritySuite/malware_center?form.action=&form.bunit_form=&f
splunk> App: Enterprise Security
Security Posture
Incident Review
Event Investigators
Advanced Threat
Security Domains
Audit
Search
Configure
Malware Center
Action
All
Business Unit
Category
All
Last 24 hours
Submit
Edit
NEW INFECTIONS
Count
0
0
MULTIPLE INFECTIONS
System Count
38
+1
UNIQUE MALWARE
Unique Count
53
0
INFECTED SYSTEMS
System Count
106
-5
TOTAL INFECTIONS
Count
medium
decreasing minimally
Currently is: 160
Malware Activity Over Time By Action
<1m ago
400
300
200
100
count
time
allowed
blocked
deferred
unknown
Malware Activity Over Time By Signature
<1m ago
300
200
100
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
EICAR-AV-Test
HIPS/IPConnect-002
JS_INJECT.VIB
LeakTest
Mal/EncPk-C
Mal/Packer
OTHER
TROJ_JAVA.BY
TROJ_TR...UR.SMDI
WORM_S...NAD.WP
unknown
Top Infections
<1m ago
unknown
EICAR-AV-Test
HIPS/IPConnect-002
LeakTest
Mal/EncPk-C
Mal/Packer
Hacktool.Rootkit
signature
New Malware - Last 30 Days
<1m ago
splunk> listen to your data


Under Advanced Threat, select Risk Analysis
Risk Analysis | Splunk
FireEye Add-on for Splunk
https://54.198.26.106/en-US/app/SplunkEnterpriseSecuritySuite/risk_analysis?form.source=&form.risk_object_form=&earliest=-24h%40h&latest=now&form.risk_object_t
splunk> App: Enterprise Security
Jon Snow
Security Posture
Incident Review
Event Investigators
Advanced Threat
Security Domains
Audit
Search
Configure
Enterprise Security
Risk Analysis
Edit
Source
All
Risk Object Type
system
Risk Object
Last 24 hours
Submit
Filterable
Create Ad-Hoc Risk Entry
Edit
DISTINCT MODIFER SOURCES
Source Count
21
0
DISTINCT RISK OBJECTS
Object Count
444
-17
MEDIAN RISK SCORE
Overall Median Risk
extreme
increasing extremely
Currently is: 160
AGGREGATED SYSTEM RISK
Total System Risk
medium
increasing extremely
Currently is: 204k
KSIs specific to Risk
Risk Modifiers Over Time
<1m ago
100,000
50,000
risk_score
1,000
500
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
risk_score
count
Risk assigned to system, user or other
Risk Score By Object
<1m ago
risk_object
risk_object_type
risk_score
source_count
count
127.0.0.1 system 5240 1 131
aseykoski@acmetech.com user 3520 1 44
dmsys user 3520 1 44
ACME-006 system 3440 4 43
htrapper@acmetech.com user 3440 1 43
HOST-003 system 3400 5 43
Most Active Sources
<1m ago
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
splunk> listen to your data


Risk Analysis | Splunk
FireEye Add-on for Splunk
https://54.198.26.106/en-US/app/SplunkEnterpriseSecuritySuite/risk_analysis?form.source=&form.risk_object_form=&earliest=-24h%40h&latest=now&form.risk_object_
Under Advanced Threat, select Risk Analysis
Risk Score By Object
5m ago
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
Most Active Sources
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.threat_group_form=&form.threat_category_form=&earliest=-24h%40h&latest=now
splunk> App: Enterprise Security
Jon Snow
Security Posture
Incident Review
Event Investigators
Advanced Threat
Security Domains
Audit
Search
Configure
Enterprise Security
Threat Activity
Edit
Export
Filterable, down to IoC
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
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> listen to your data

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 Certificate Unit Matches Email Address Matches		4	7
process_intel	Process Matches		1	1

emerging_threats_ip_blocklist	/four/splunk/etc/apps/... ThreatIntelligence/loca...		
iblocklist_logmein	/four/splunk/etc/apps/... ThreatIntelligence/loca...		
iblocklist_spyware	/four/splunk/etc/apps/... 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
...blocklist_web_attacker	/four/splunk/etc/apps/SA-...	csv	39
	...csv	csv	19
		csv	18
	...rificates.xml	stix	7

« prev 1 2 next »

Under Advanced Threat, select Threat Activity

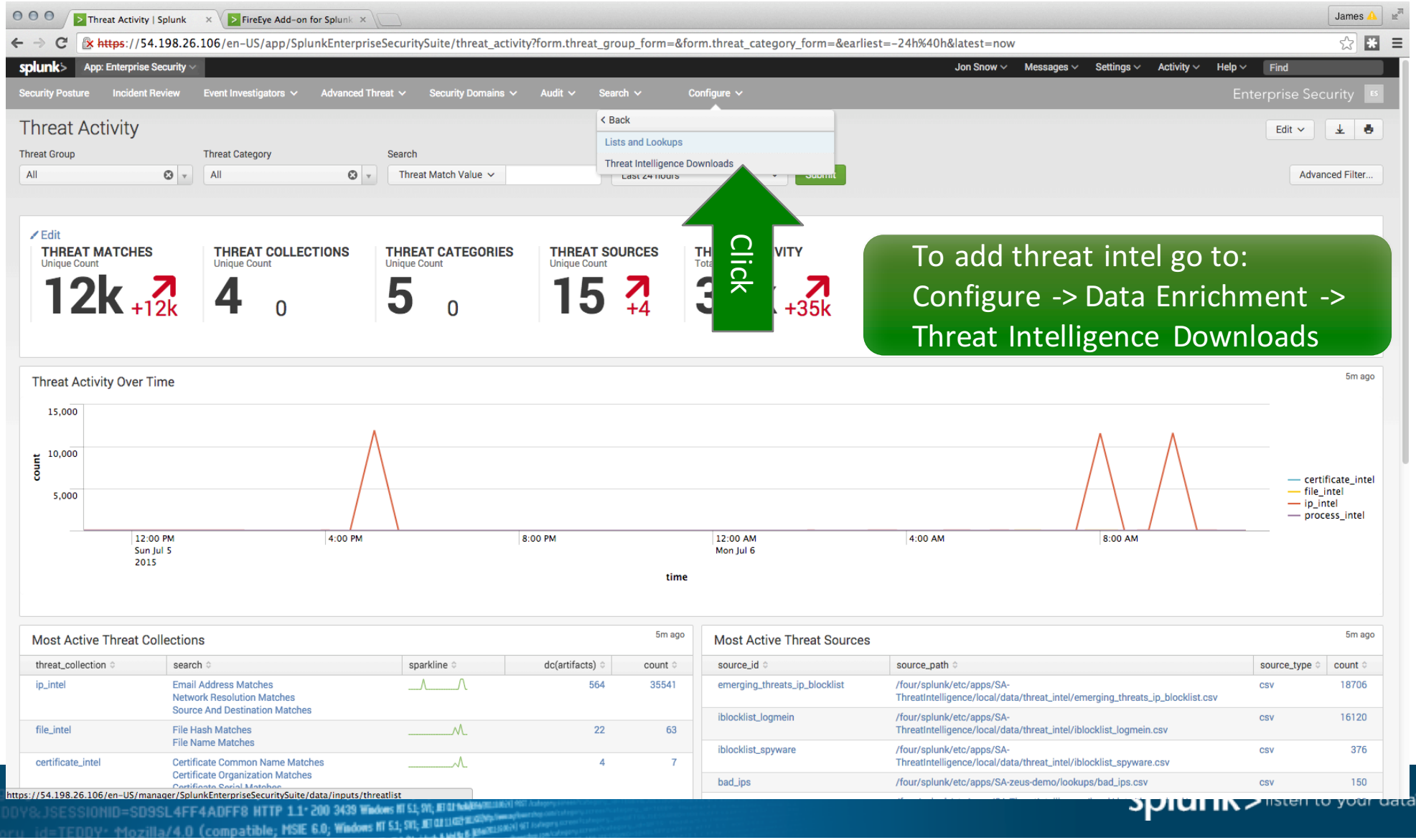
Specifics about recent threat matches

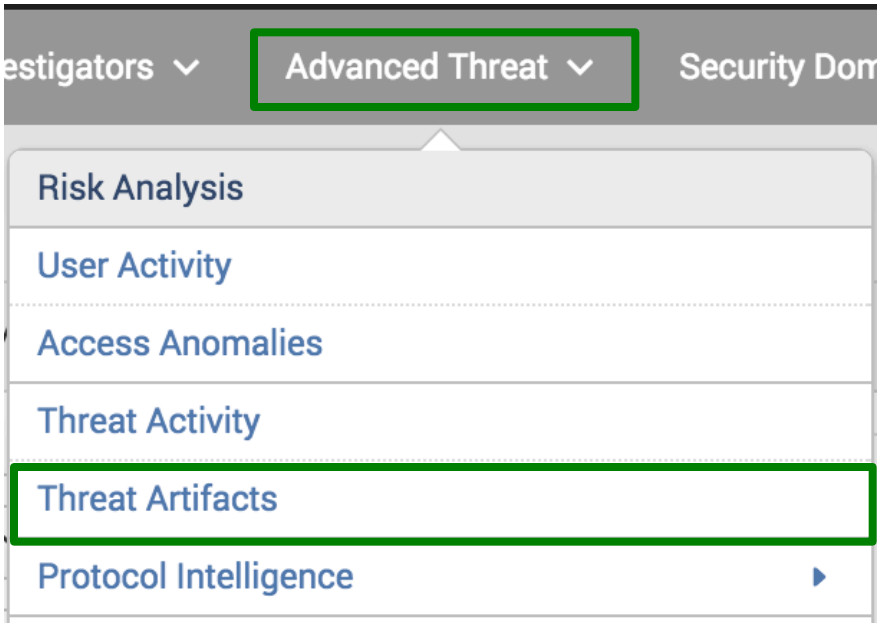
Threat Activity Details

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

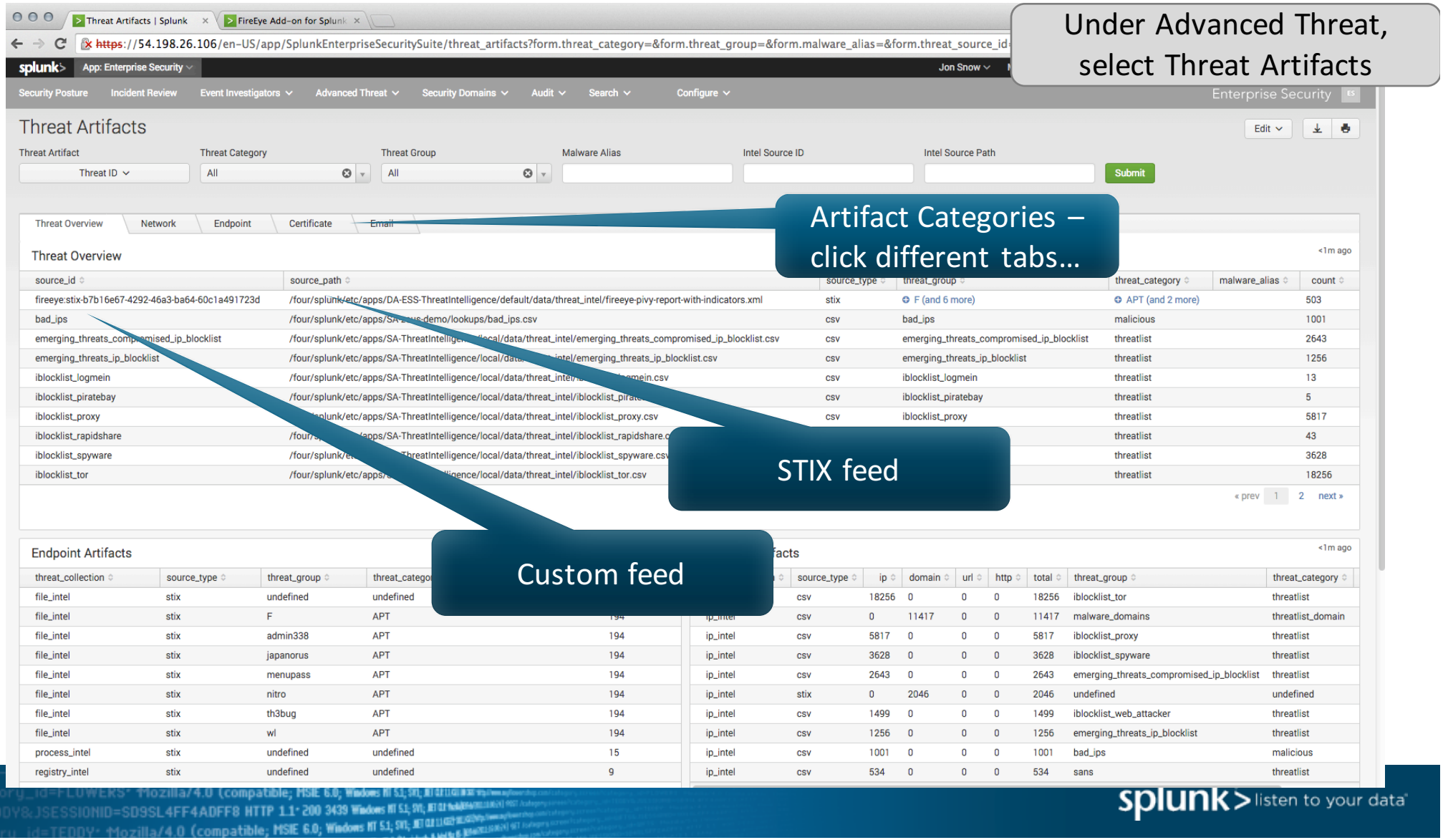
« prev 1 2 3 4 5 6 7 8 9 10 next »

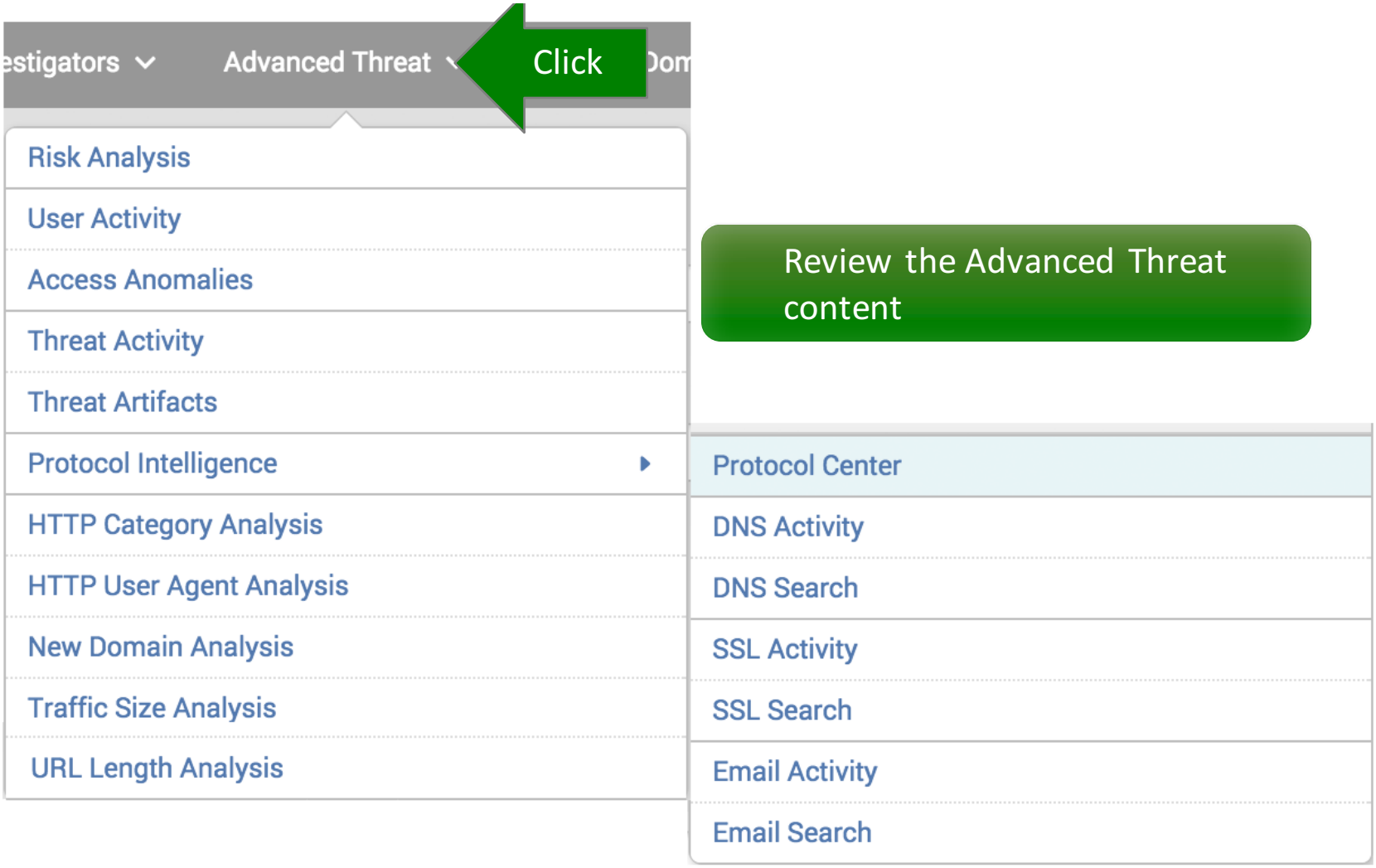

Threat Activity | Splunk
FireEye Add-on for Splunk
James
https://54.198.26.106/en-US/app/SplunkEnterpriseSecuritySuite/threat_activity?form.threat_group_form=&form.threat_category_form=&earliest=-24h%40h&latest=now
splunk> App: Enterprise Security
Jon Snow
Messages
Settings
Activity
Help
Find
Security Posture
Incident Review
Event Investigators
Advanced Threat
Security Domains
Audit
Search
Configure
Enterprise Security
Back
Lists and Lookups
Threat Intelligence Downloads
Threat Activity
Edit
Threat Group
All
Threat Category
All
Search
Threat Match Value
Advanced Filter...
Click
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
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
splunk> listen to your data

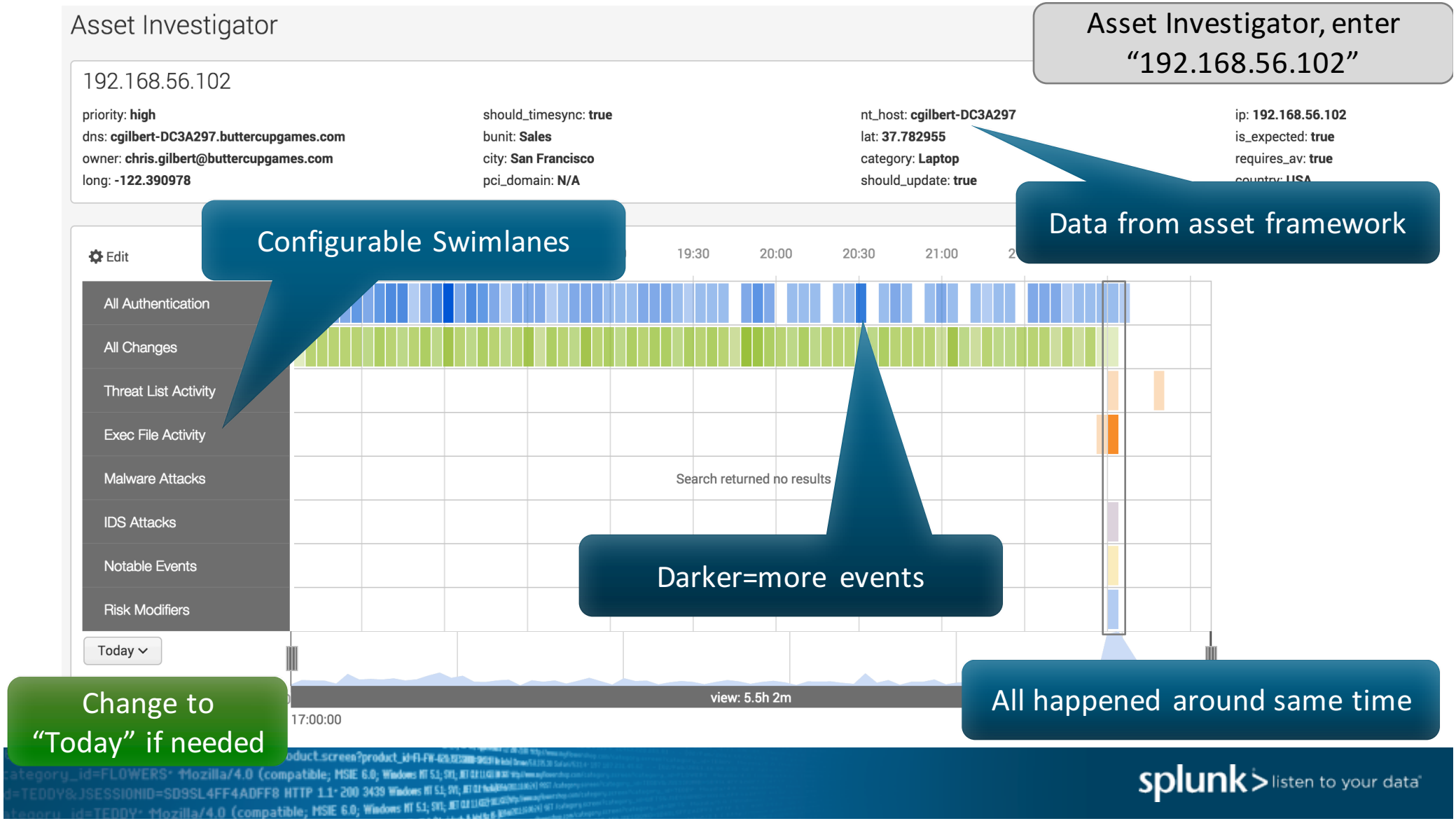


Click “Threat Artifacts”
Under “Advanced Threat”

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=&form.threat_group=&form.malware_alias=&form.threat_source_id
splunk> App: Enterprise Security
Jon Snow
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
csv
bad_ips
malicious
1001
emerging_threats_compromised_ip_blocklist
csv
emerging_threats_compromised_ip_blocklist
threatlist
2643
emerging_threats_ip_blocklist
csv
emerging_threats_ip_blocklist
threatlist
1256
iblocklist_logmein
csv
iblocklist_logmein
threatlist
13
iblocklist_piratebay
csv
iblocklist_piratebay
threatlist
5
iblocklist_proxy
csv
iblocklist_proxy
threatlist
5817
iblocklist_rapidshare
threatlist
43
iblocklist_spyware
threatlist
3628
iblocklist_tor
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
APT
194
F
admin338
japanorus
menupass
nitro
th3bug
wl
process_intel
registry_intel
9
ip_intel
csv
ip
domain
url
http
total
malware_domains
threatlist_domain
iblocklist_web_attacker
sans
splunk> listen to your data


estigators
Advanced Threat
Click
Risk Analysis
User Activity
Access Anomalies
Threat Activity
Threat Artifacts
Protocol Intelligence
HTTP Category Analysis
HTTP User Agent Analysis
New Domain Analysis
Traffic Size Analysis
URL Length Analysis
Protocol Center
DNS Activity
DNS Search
SSL Activity
SSL Search
Email Activity
Email Search
Review the Advanced Threat content

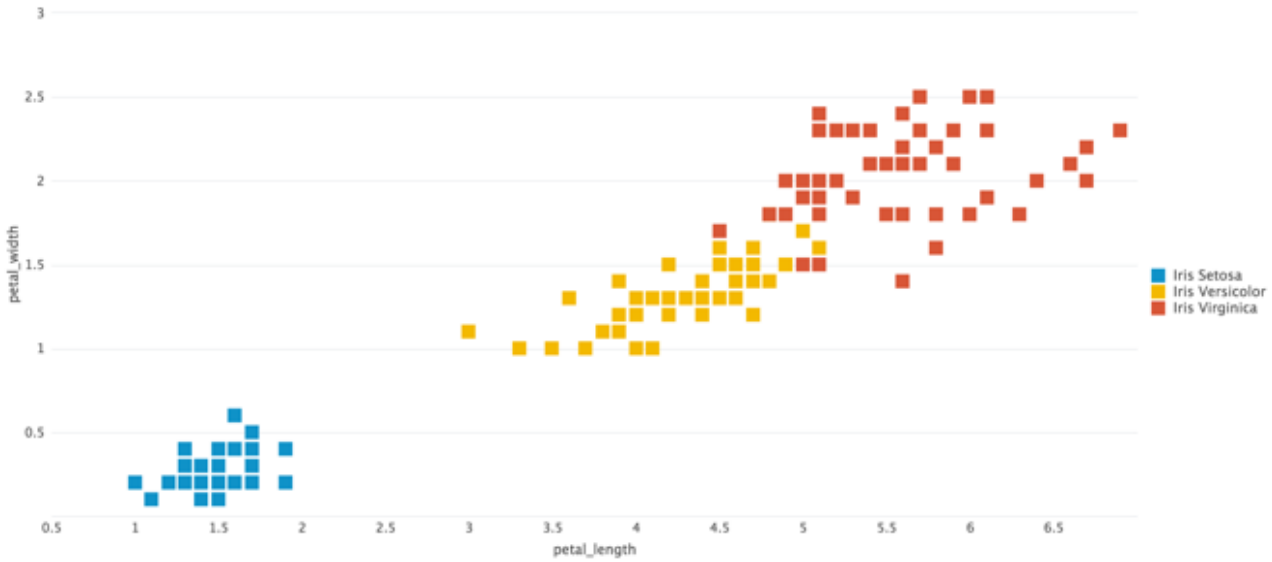

Asset Investigator
Asset Investigator, enter "192.168.56.102"
192.168.56.102
priority: high
dns: cgilbert-DC3A297.buttercupgames.com
owner: chris.gilbert@buttercupgames.com
long: -122.390978
should_timesync: true
bunit: Sales
city: San Francisco
pci_domain: N/A
nt_host: cgilbert-DC3A297
lat: 37.782955
category: Laptop
should_update: true
ip: 192.168.56.102
is_expected: true
requires_av: true
Data from asset framework
Configurable Swimlanes
Edit
19:30
20:00
20:30
21:00
All Authentication
All Changes
Threat List Activity
Exec File Activity
Malware Attacks
IDS Attacks
Notable Events
Risk Modifiers
Search returned no results
Darker=more events
Today
view: 5.5h 2m
17:00:00
All happened around same time
Change to "Today" if needed
splunk> listen to your data


Data Science &
Machine Learning In
Security
splunk>

Disclaimer: I am not a data scientist

Types of Machine Learning

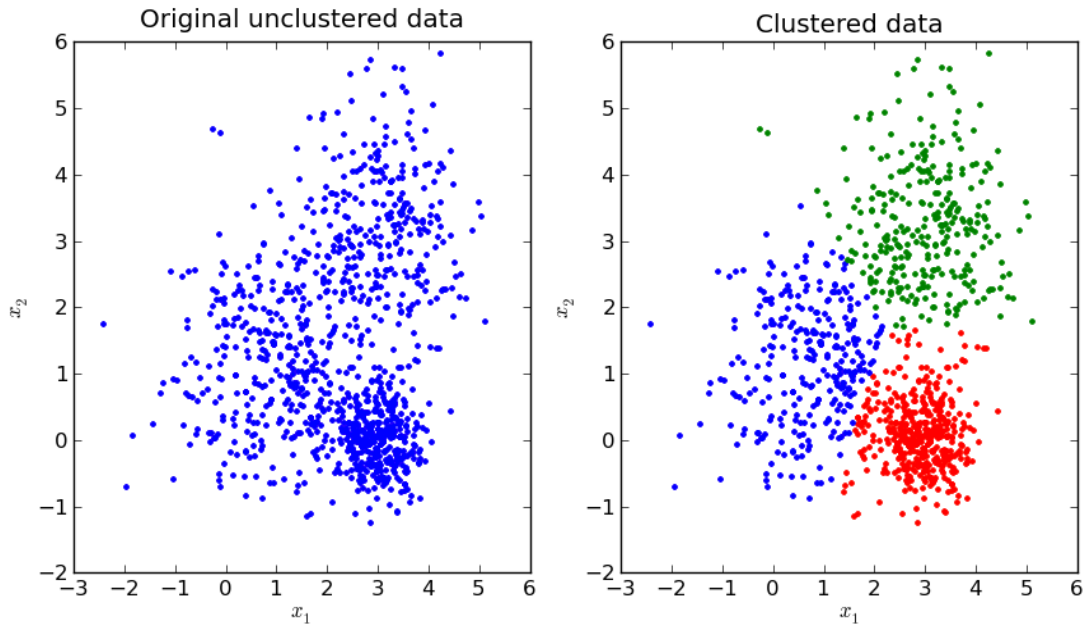
Supervised Learning: generalizing from labeled data



Supervised Machine Learning

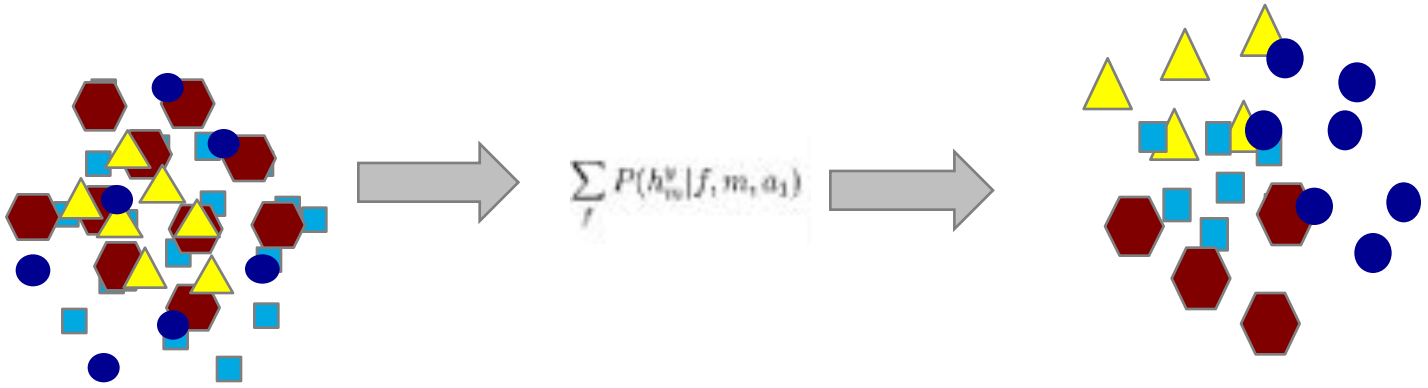
Domain Name	TotalCnt	RiskFactor	AGD	SessionTime	RefEntropy	NullUa	Outcome
yyfaimjmocdu.com	144	6.05	1	1	0	0	Malicious
jjeyd2u37an30.com	6192	5.05	0	1	0	0	Malicious
cdn4s.steelhousemedia.com	107	3	0	0	0	0	Benign
log.tagcade.com	111	2	0	1	0	0	Benign
go.vidprocess.com	170	2	0	0	0	0	Benign
statse.webtrendslive.com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

Unsupervised Learning: generalizing from unlabeled data



Unsupervised Machine Learning

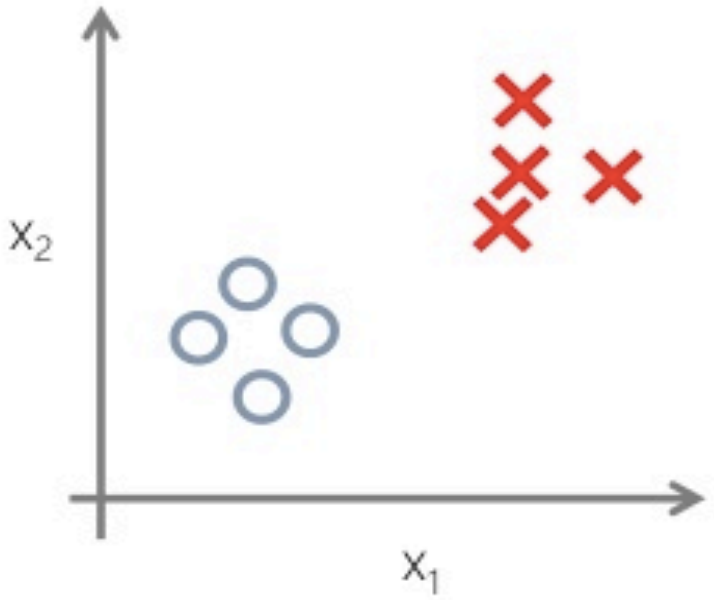
- **No tuning**
- Programmatically finds trends
- UBA is **primarily** unsupervised
- Rigorously tested for fit



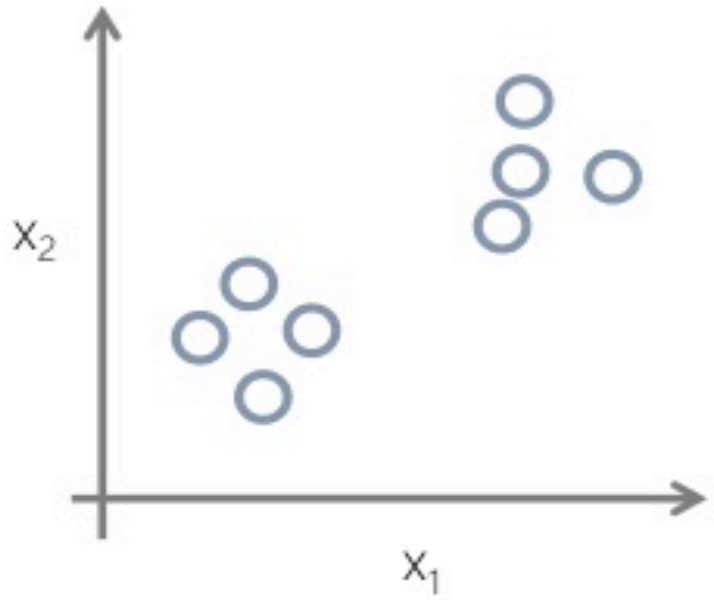
Raw Security Data Algorithm Automated Clustering

Supervised vs. Unsupervised

Supervised Learning

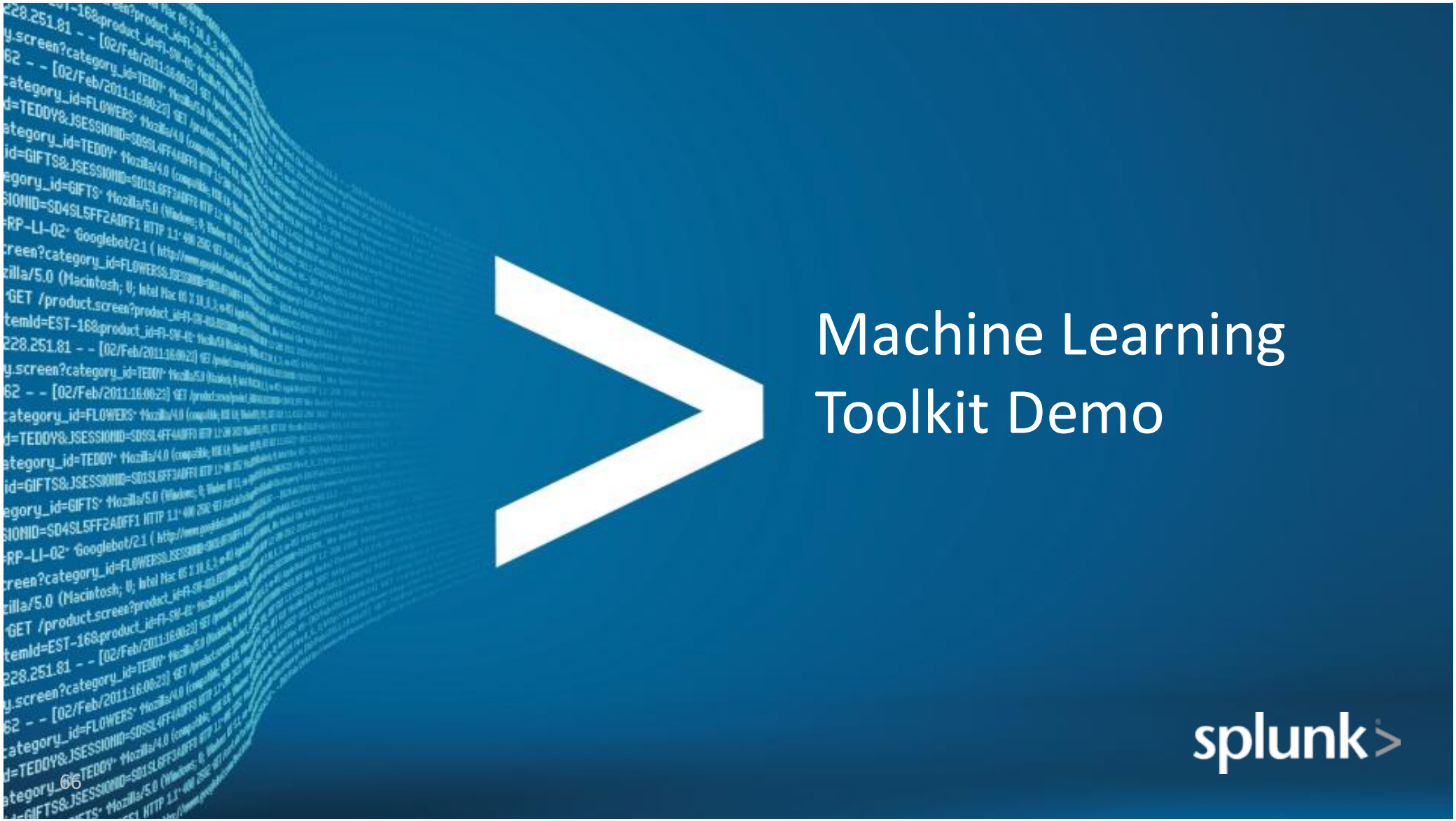


Unsupervised Learning



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


Machine Learning
Toolkit Demo
splunk>

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 »

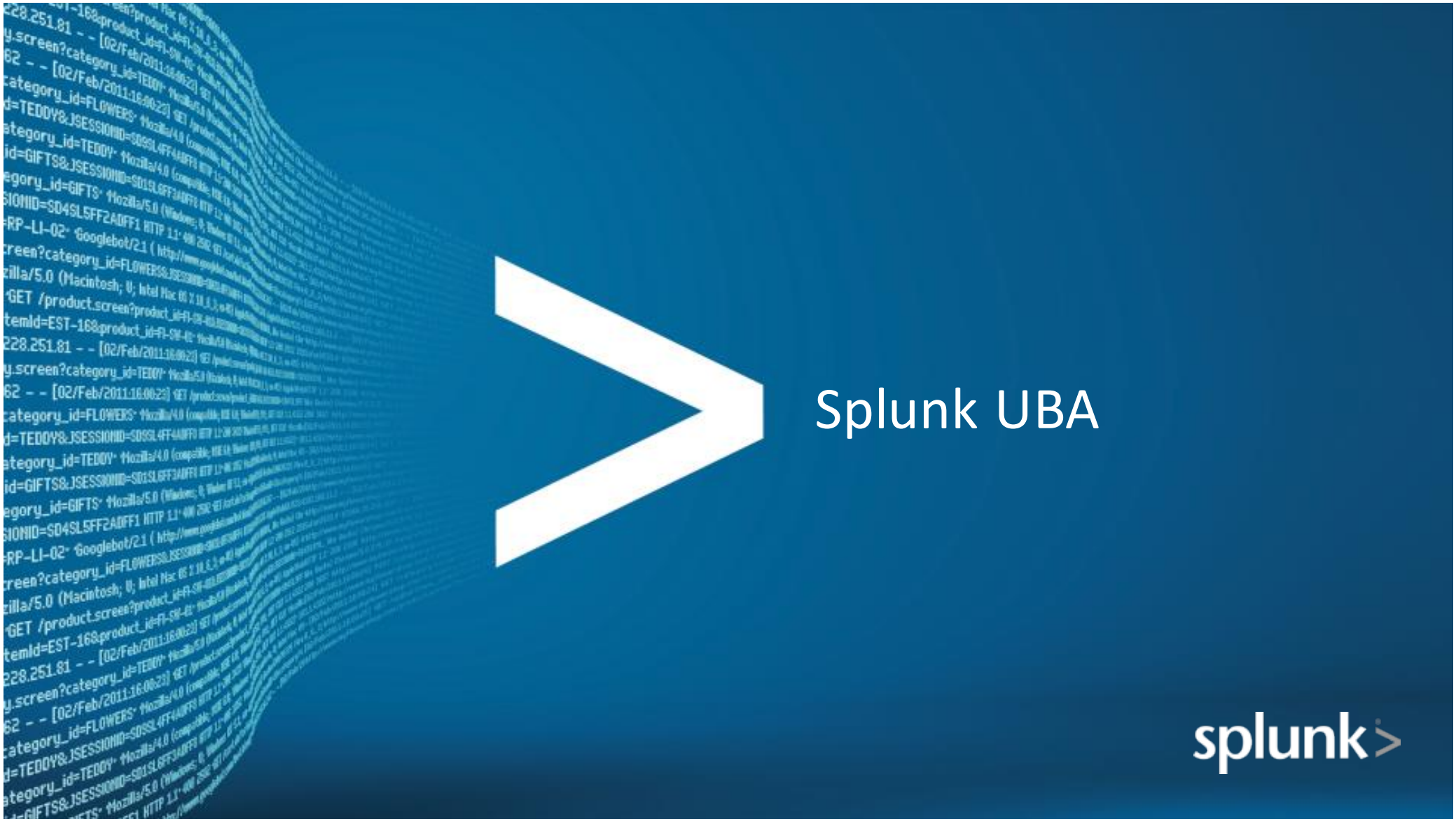
Upcoming Classes

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*

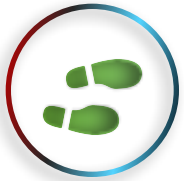

Splunk UBA
splunk>

Splunk UBA Use Cases

INSIDER THREATS

ACCOUNT TAKEOVER

- Privileged account compromise
- Data exfiltration



LATERAL MOVEMENT

- Pass-the-hash kill chain
- Privilege escalation

SUSPICIOUS ACTIVITY

- Misuse of credentials
- Geo-location anomalies

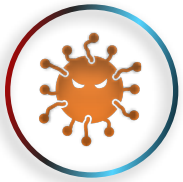
EXTERNAL THREATS

MALWARE ATTACKS

- Hidden malware activity

BOTNET, COMMAND & CONTROL

- Malware beaconing
- Data leakage

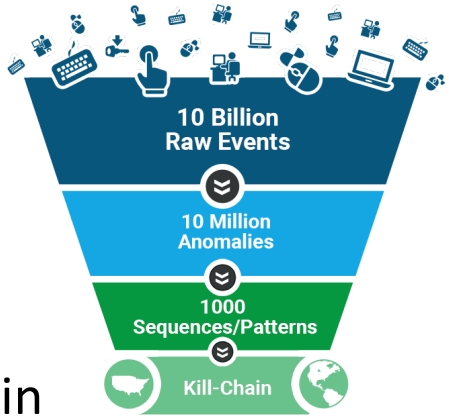


USER & ENTITY BEHAVIOR ANALYTICS

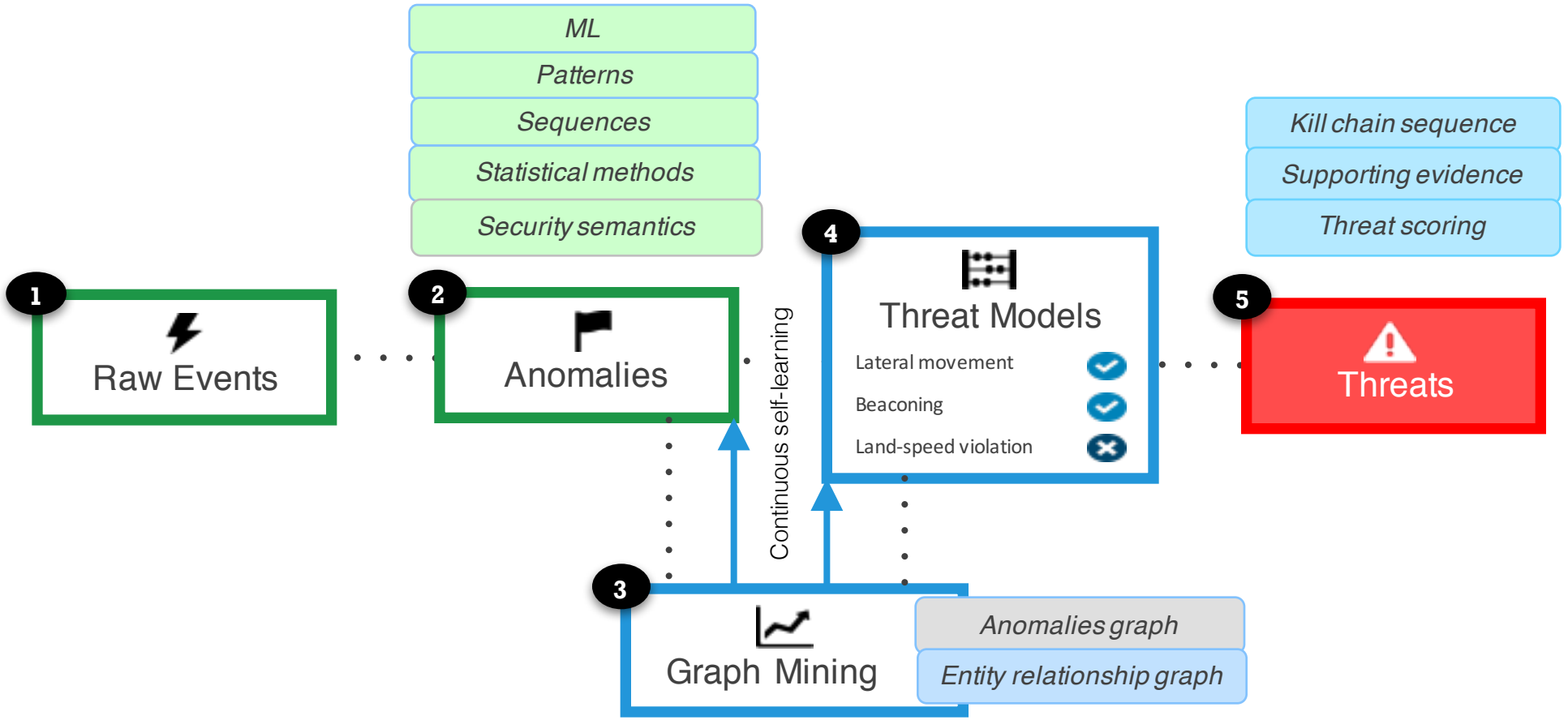
- Suspicious behavior by accounts or devices

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



Workflow




Splunk UBA Demo
splunk>

Security Workshops

- Security Readiness Assessments
- Splunk UBA Data Science Workshop
- Enterprise Security Benchmark Assessment


Security Workshop Survey
https://www.surveymonkey.com/r/8BCWHSF