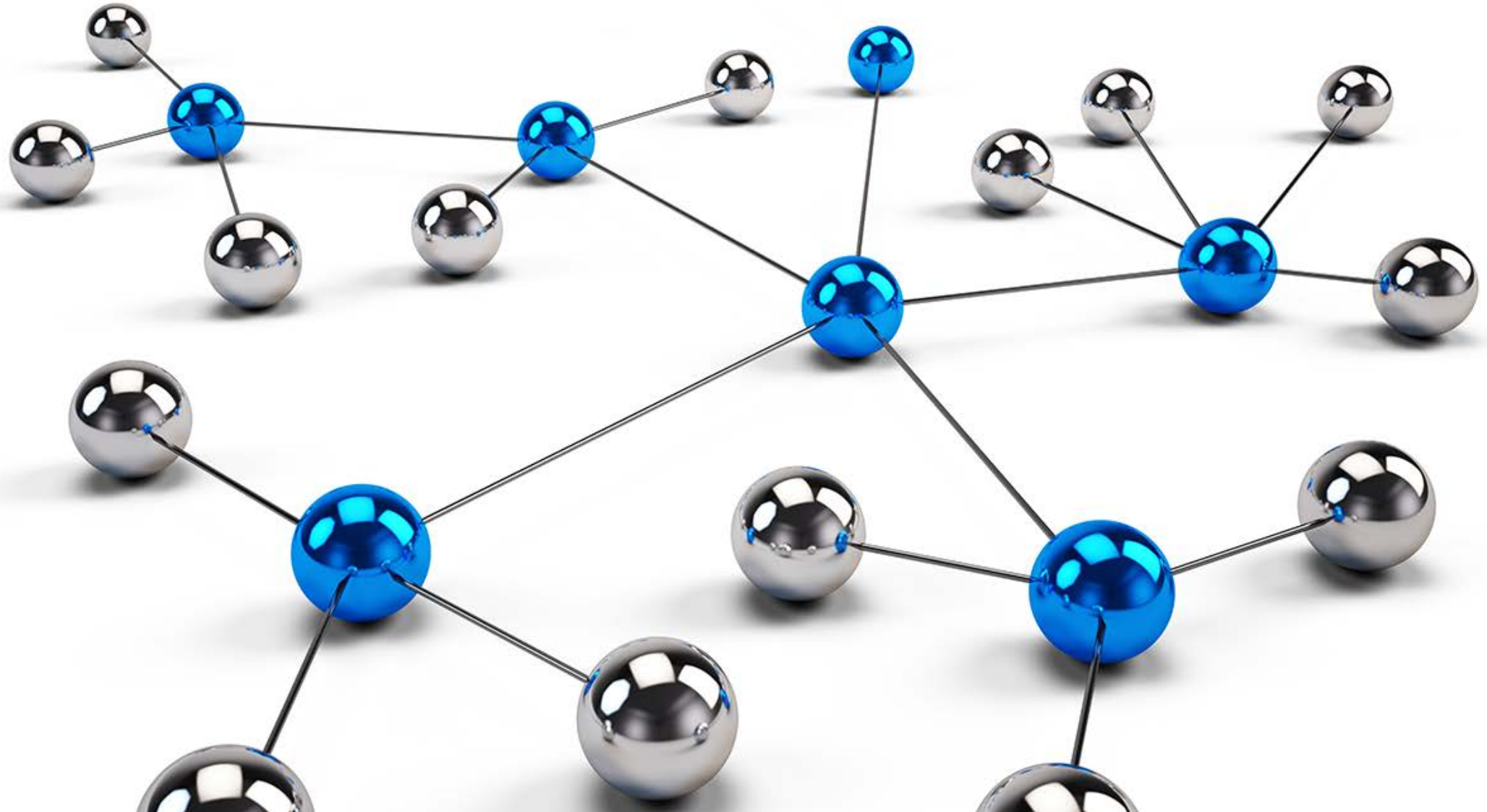


# Pivoting During the Hunt for Malware



- Fidelity : both low, medium and high
- Pivot : what is it
- Gains : from a pivot
- Pivot Fields : within the chart
- Pivot Chart : identifying data sources
- Example
- Curiosity and thinking
- System Automation

# AGENDA



fidelity

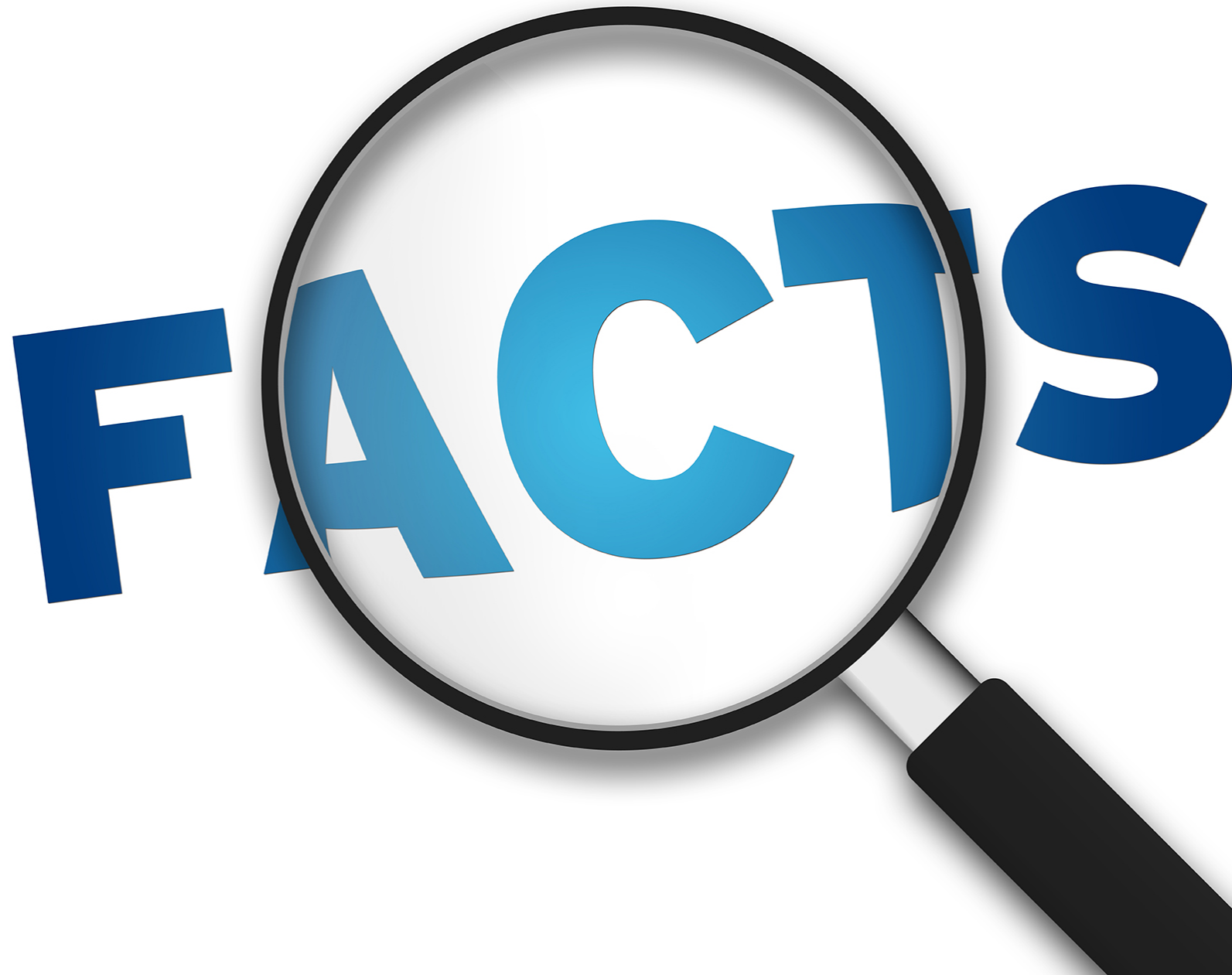
# fidelity

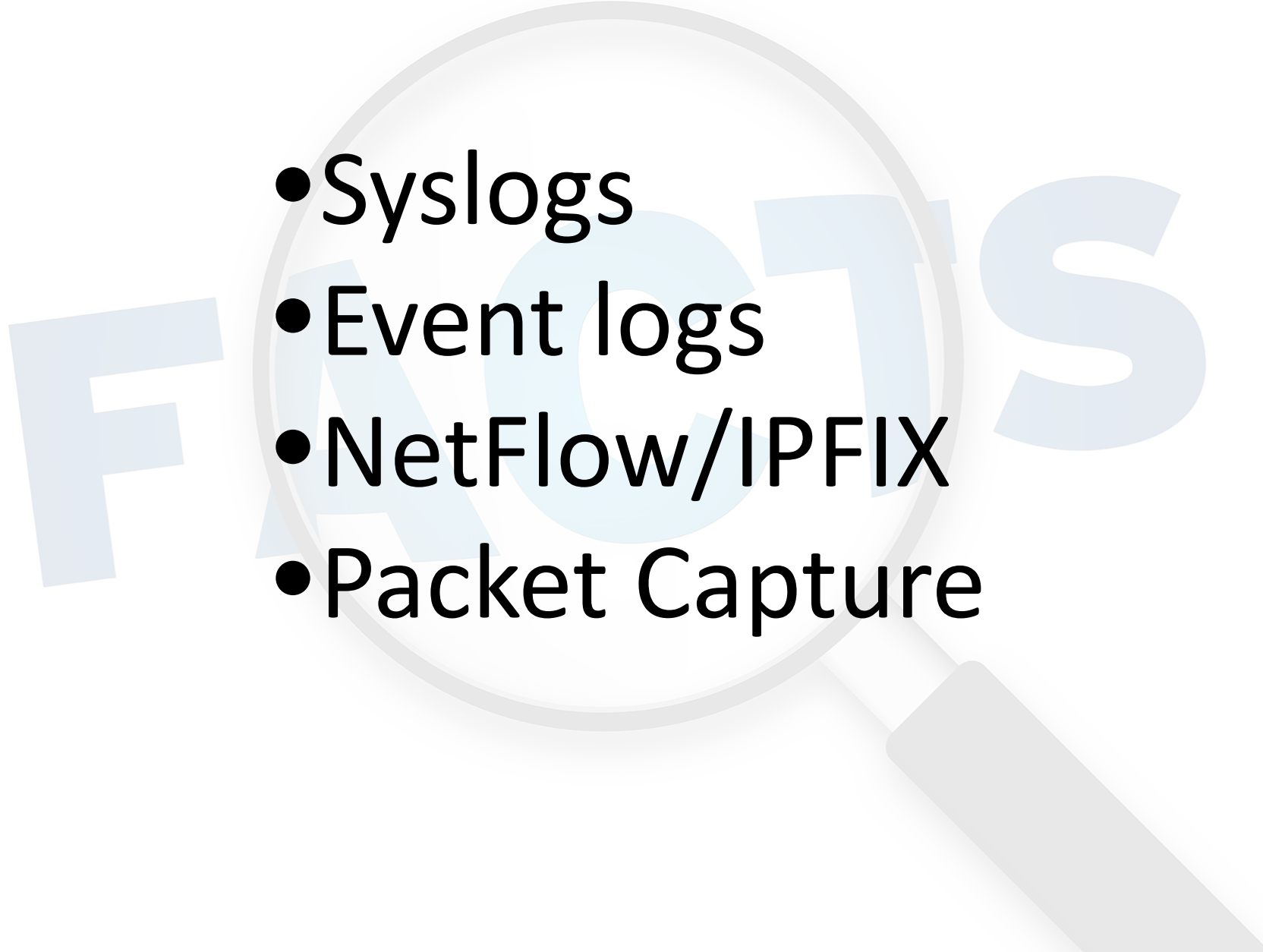
*noun*

pl. -·ties

pl. fi·del·i·ties

1. accuracy of a description, translation, etc.
2. exact correspondence with fact or with a given quality, condition, or event; accuracy



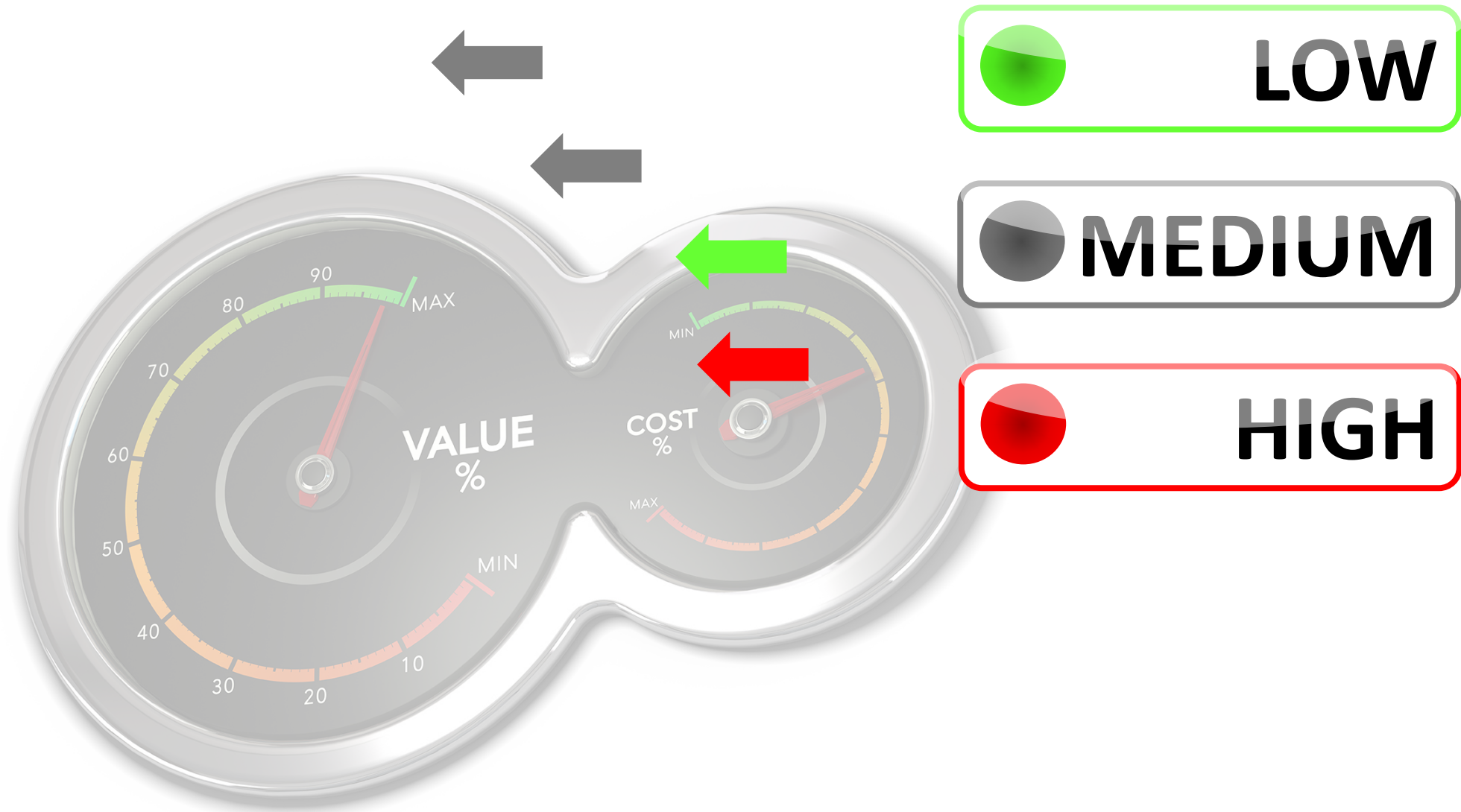
- 
- Syslogs
  - Event logs
  - NetFlow/IPFIX
  - Packet Capture



 **LOW**

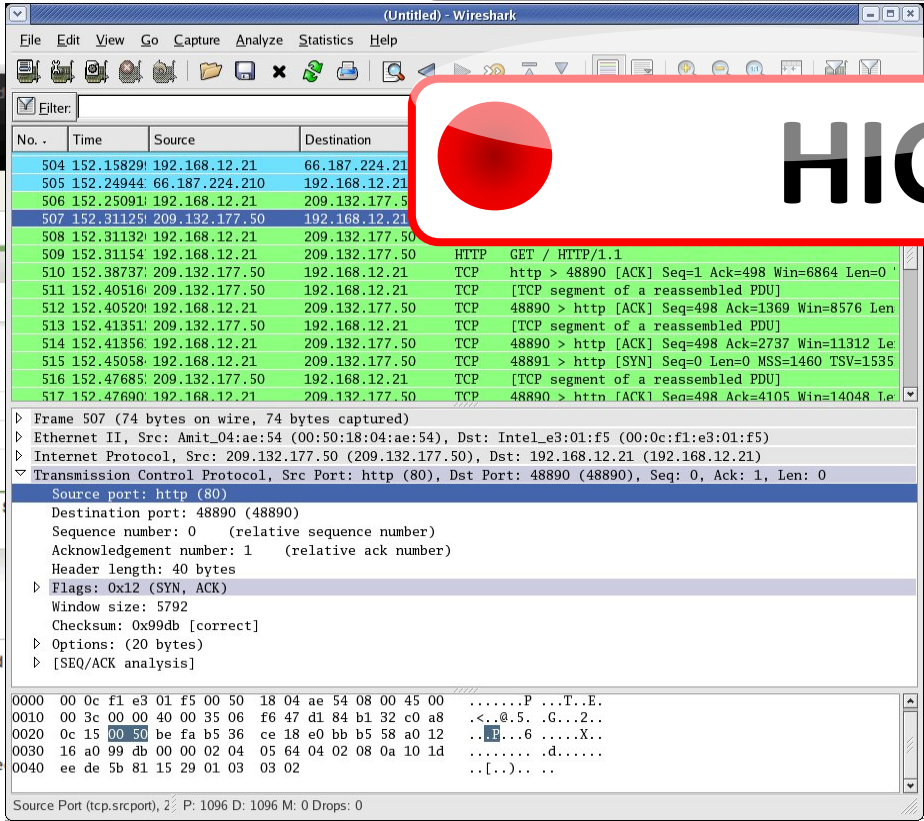
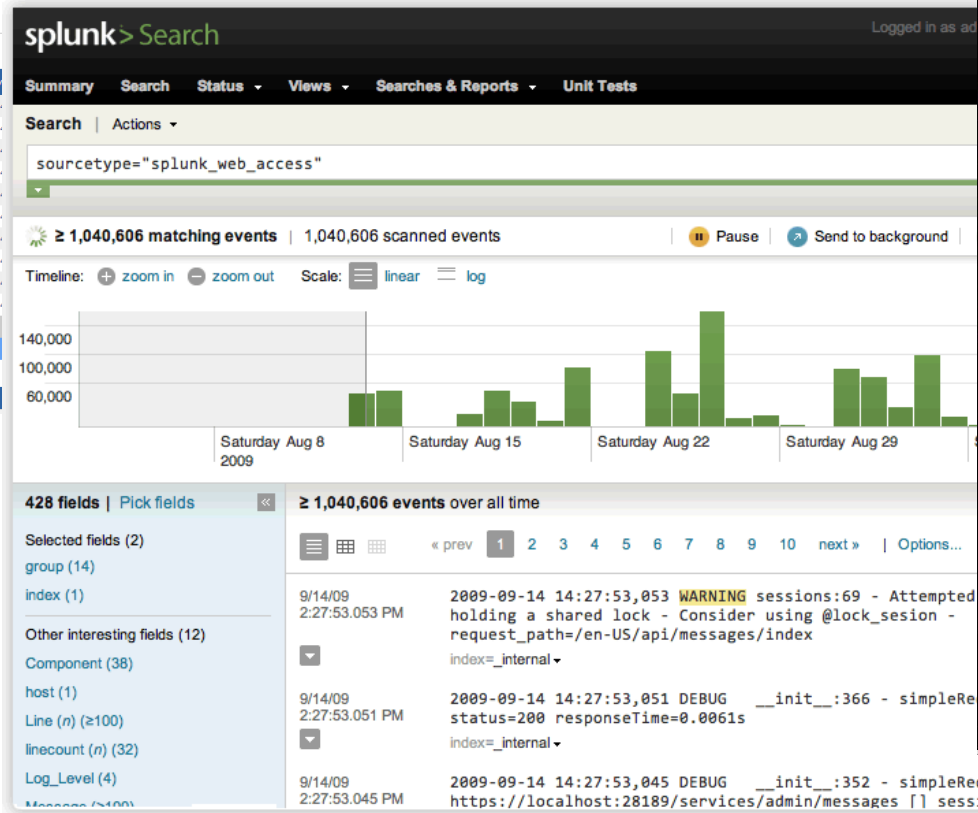
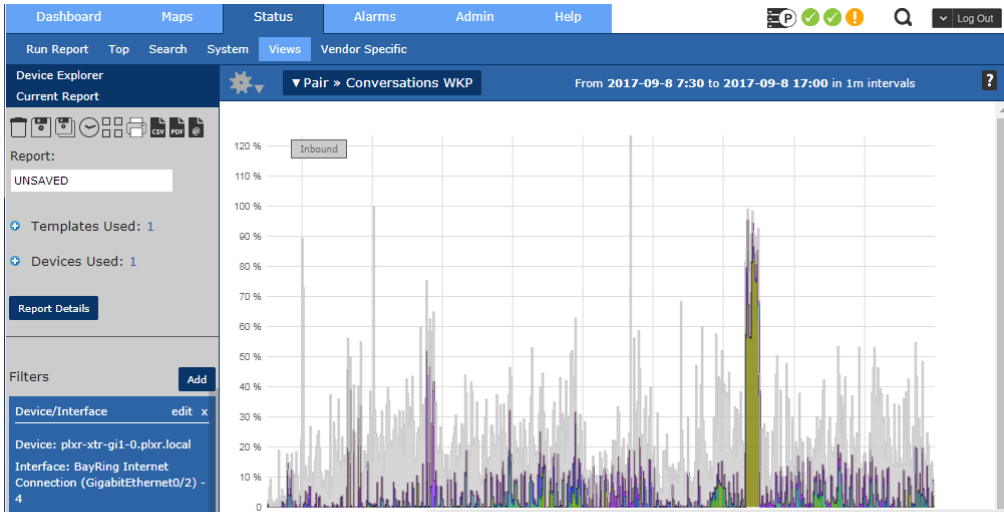
 **MEDIUM**

 **HIGH**



- Syslogs
- Event logs
- NetFlow/IPFIX
- Packet Capture





# Agenda

- Fidelity : both low, medium and high
- Pivot : what is it
- Gains : from a pivot
- Pivot Fields : within the chart
- Pivot Chart : identifying data sources
- Example
- Curiosity and thinking
- System Automation



# What is a Pivot?

- The ability to pass context between autonomous systems while researching a security or application performance event.
- Goal: to quickly gather additional details that could be related to the event being investigated.
- A good pivot will lower the cost of the event for the defending investigator and increase the cost of the attacker.



# Pivoting Lets You ...

- Connect data sources
- Move from host to network based data
- Shorten investigative times
- Pivot from lower to higher context data - seldom do you start with pcap



*“Start with flow data which is very fast to parse, very low in size you can parse it really quickly and then pivot from that to packet capture data.”*

# Example Pivots


- Move from internal (e.g. NetFlow or syslogs) to external data sources (E.g. virustotal, passivetotal, Talos Intelligence) .
- Example: Move from a proxy server log that is user name aware to a windows event log

*“Both server and Network data is needed in every security investigation” - Chris Sanders*

# Efficient Pivoting Requires ...

- Meta cognition – curiosity and next-step investigative mindset
- Ask good questions, stick to answering those questions
- Good data collection
- Integration of pivoting across systems

# Agenda

- Fidelity : both low, medium and high
- Pivot : what is it
- Gains : from a pivot
-  • Pivot Fields : within the chart
- Pivot Chart : identifying data sources
- Example
- Curiosity and thinking
- System Automation

**PLANNING  
YOUR PIVOT**

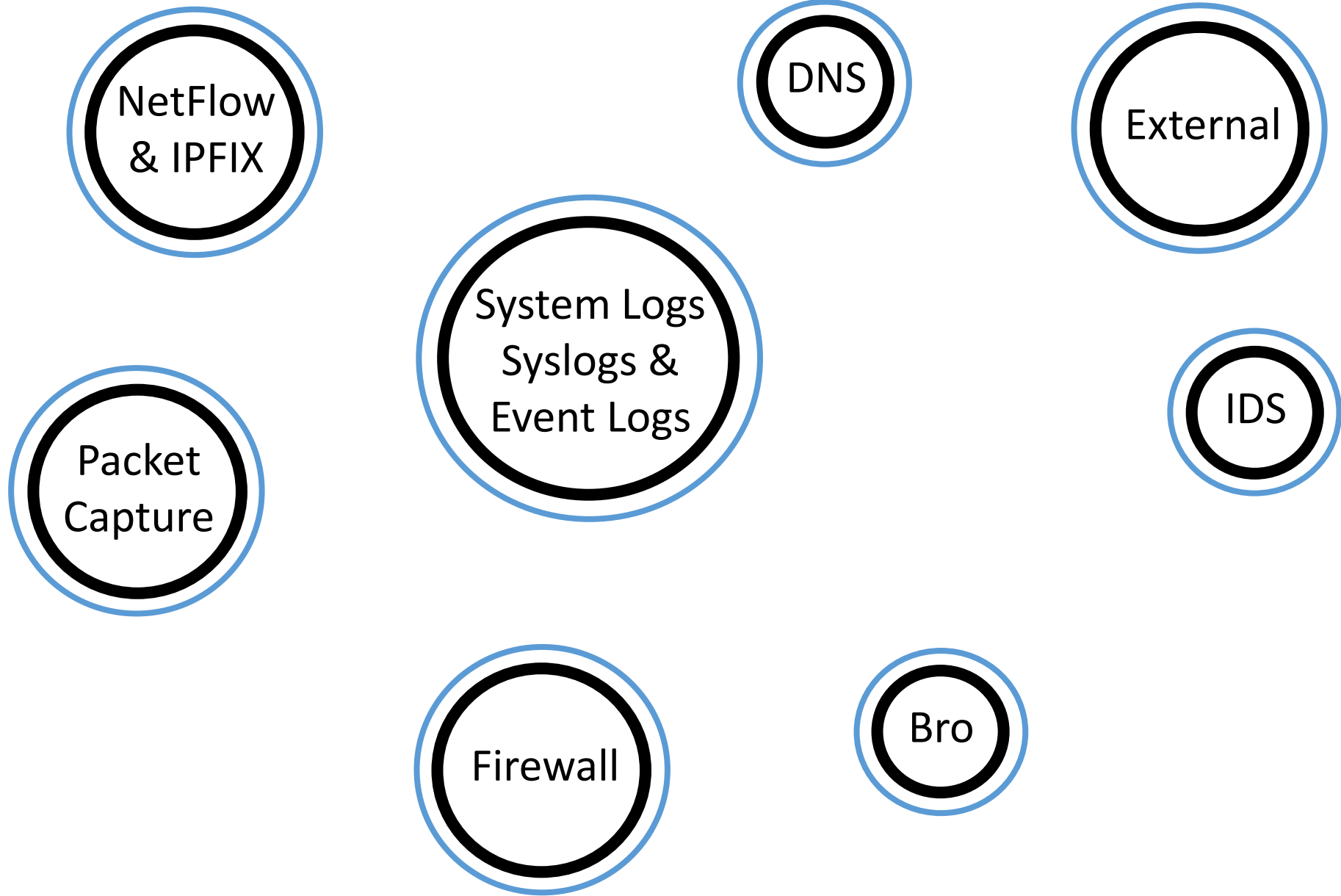




# Designer

- ① System logs
- ② Event logs
- ③ NetFlow & IPFIX
- ④ PCAP
- ⑤ DNS logs





NetFlow  
& IPFIX

DNS

External

System Logs  
Syslogs &  
Event Logs

IDS

Packet  
Capture

Firewall

Bro

# What are your pivoting fields?

- Alert name?
- IP addresses (most common pivot)
- Communication ports
- Time frame

NetFlow  
& IPFIX

DNS

External

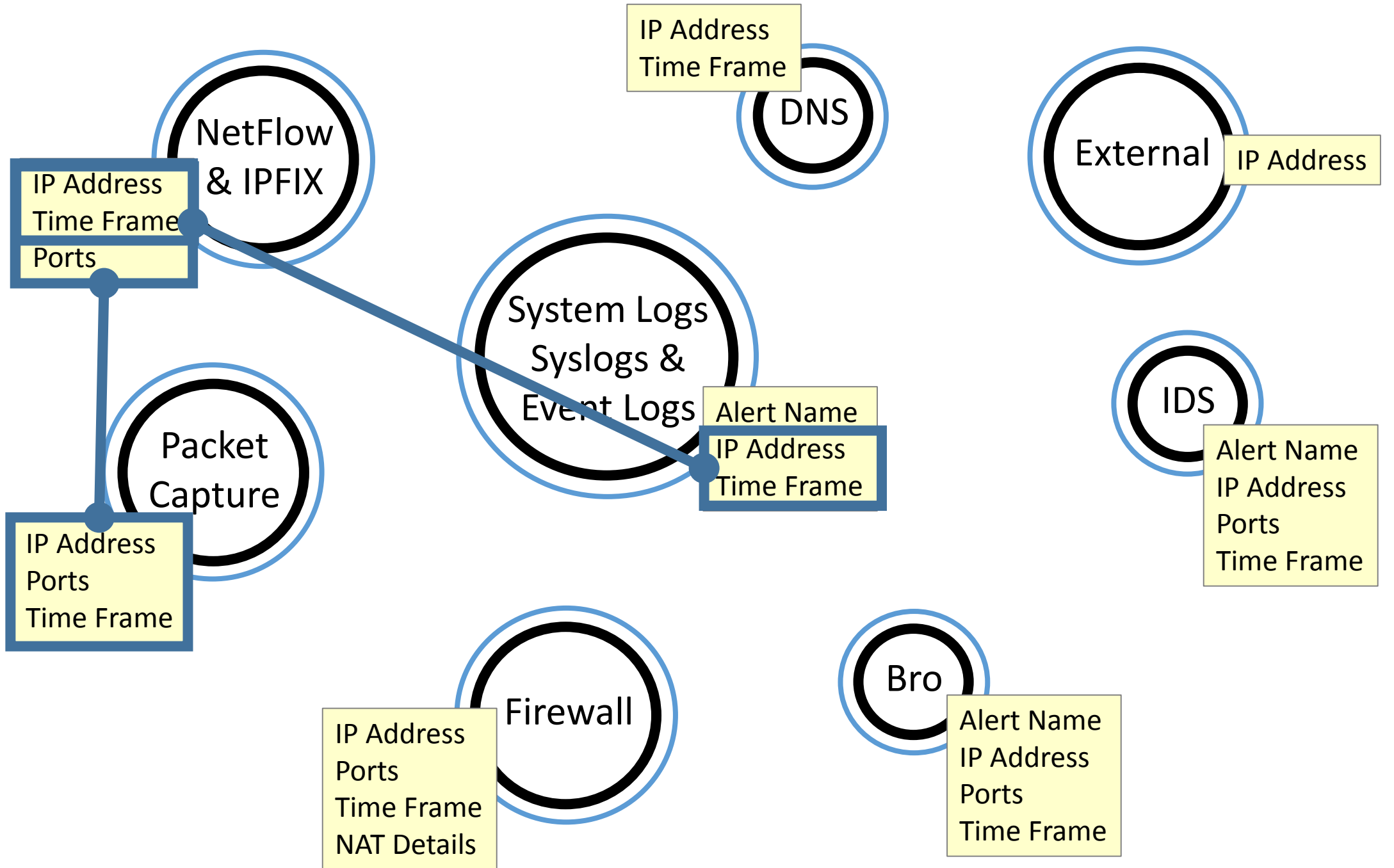
System Logs  
Syslogs &  
Event Logs

IDS

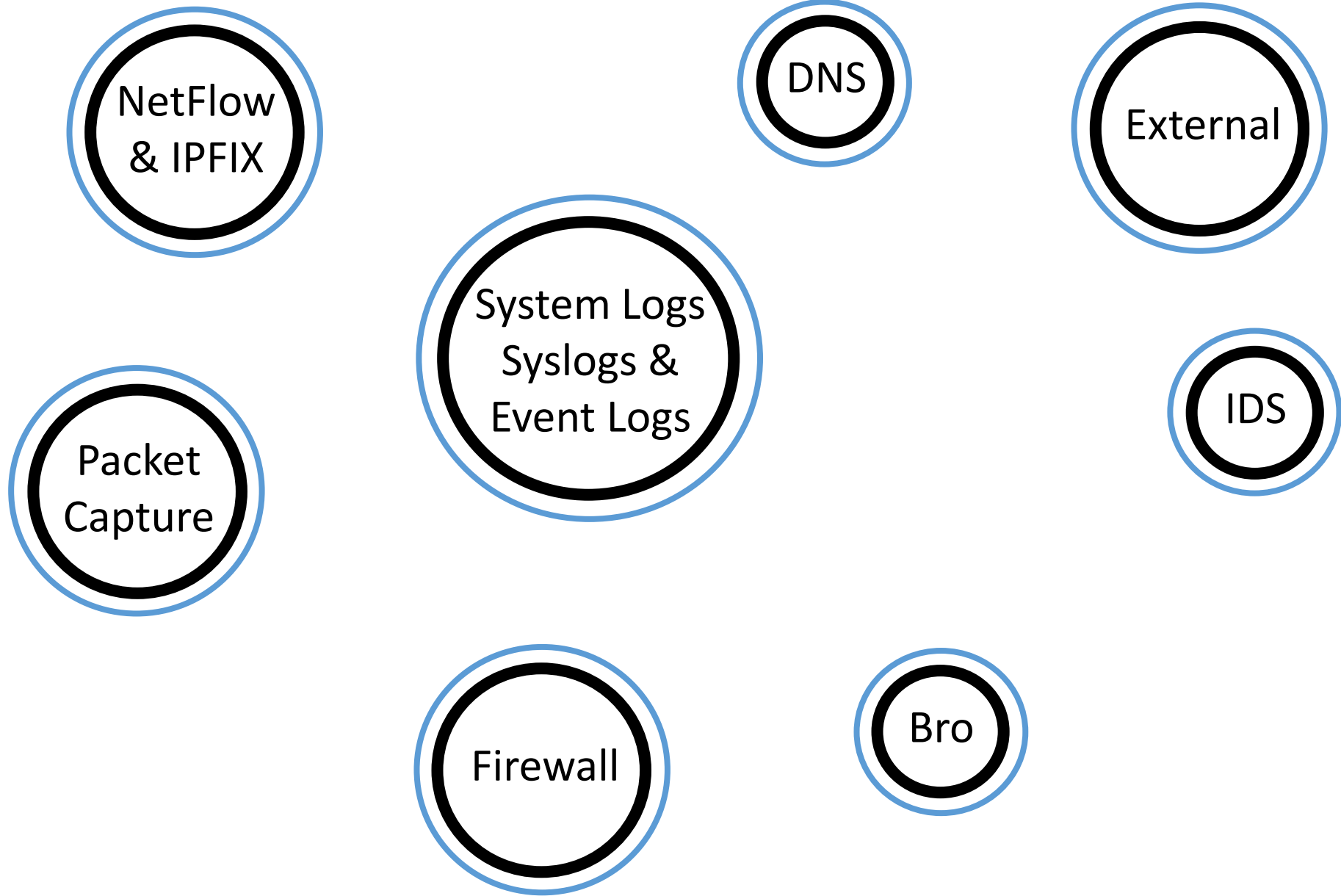
Packet  
Capture

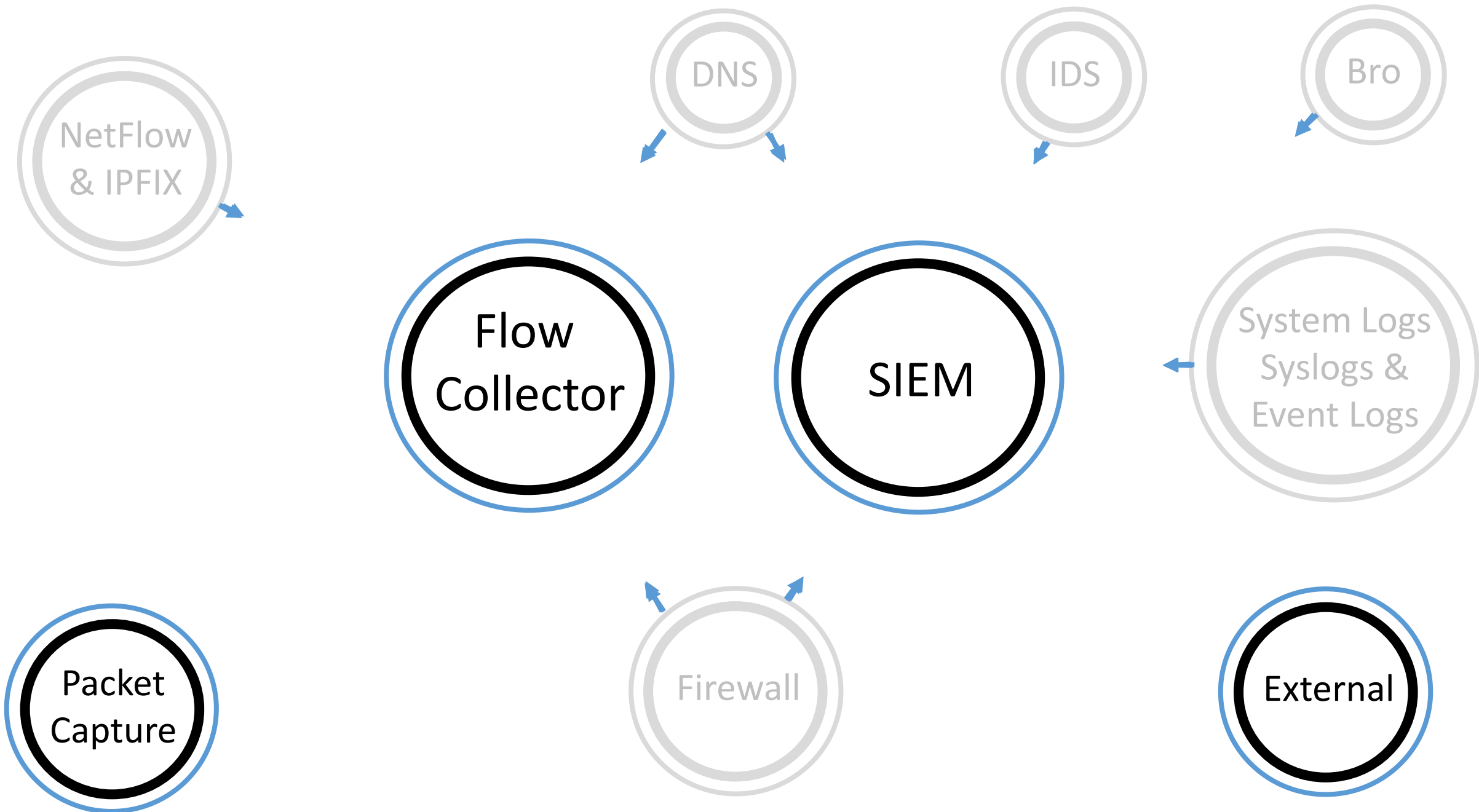
Firewall

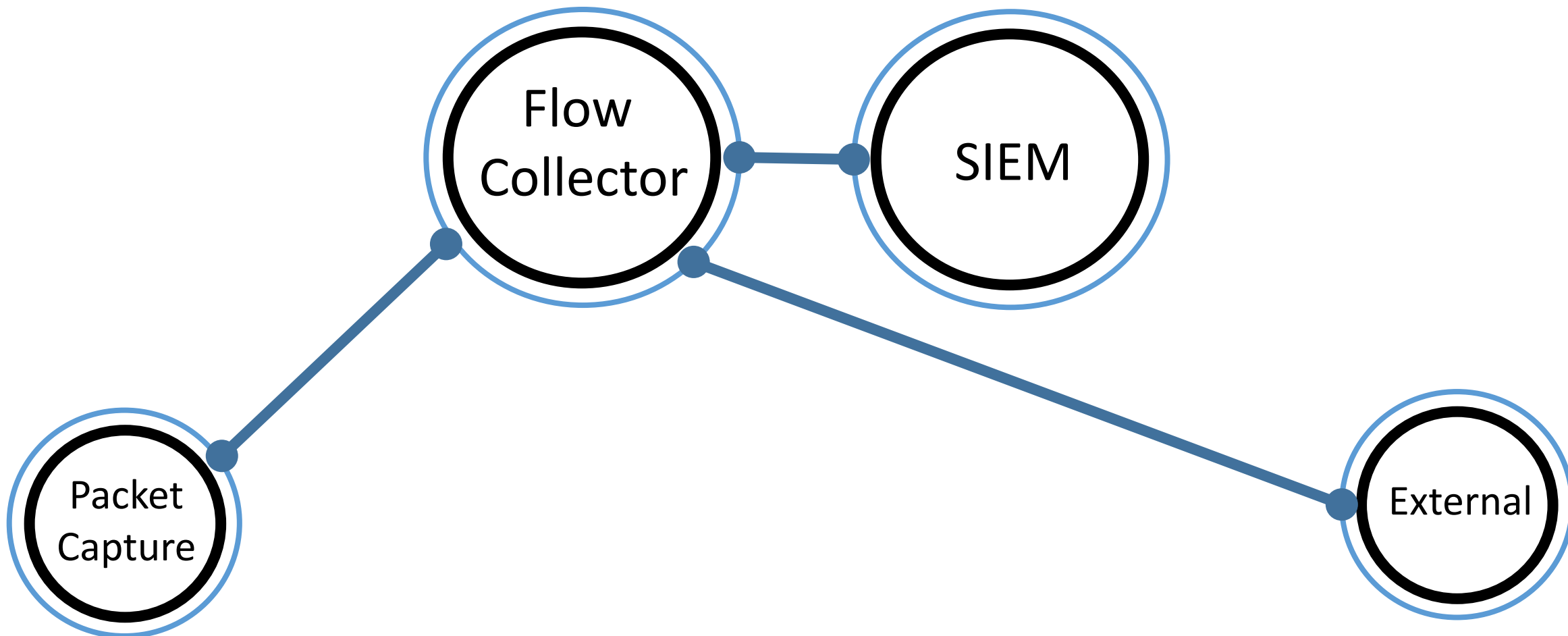
Bro



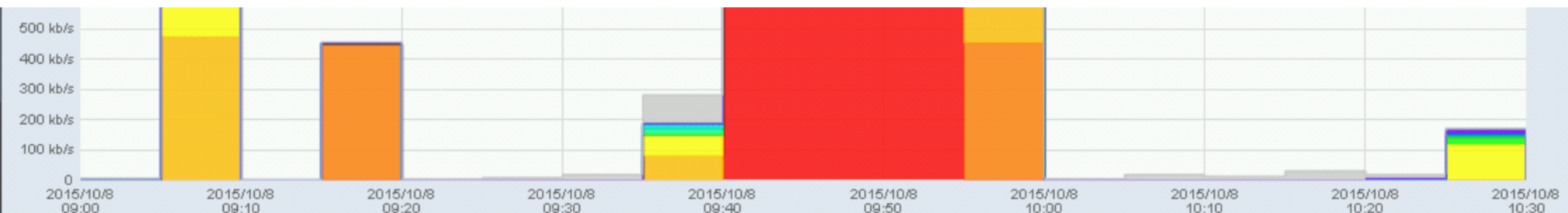












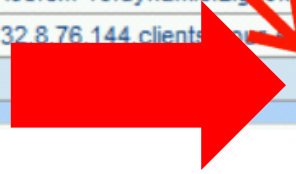
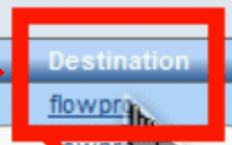
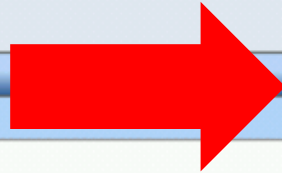
Custom 2015-10-8 09:00 to 2015-10-8 10:30  Business Hours Apply Dates

**Reports** ✕

Default Report	
Cisco ASA	10
Counts	7
Top Reports	4
Source Reports	6
Destination Reports	6
Pair Reports	11
NAT	8
Volume Reports	5
Firewall Events	7
Flow View	

**Inbound Results**

Source	Destination	Bits
1 WPIS-64-140-243-148.worldpath.net	flowpro	249 kb/s
2 www.plixer.com	flowpro	416 kb/s
3 WPIS-64-140-243-137.worldpath.net	WPIS-64-140-243-137.worldpath.net	472 kb/s
4 nms	10.20.1.4	551 kb/s
5 WPIS-64-140-243-137.worldpath.net	static.kpn.net	556 kb/s
6 lga25s40-in-f14.1e100.net	nms	246 kb/s
7 10.20.1.4	nms	2,336 b/s
8 iad23s26-in-f18.1e100.net	nms	3,646 b/s
9 WPIS-64-140-243-137.worldpath.net	3E91CA68.cm-13.dynamic.ziggo.nl	3,353 b/s
10 WPIS-64-140-243-137.worldpath.net	static.132.8.76.144.clients.your-server.com	3,007 b/s
Other -	-	837 kb/s
<b>Total</b>		<b>244 kb/s</b>

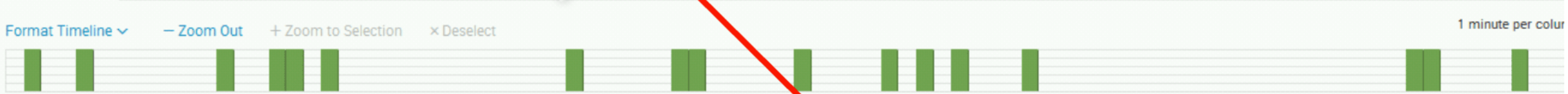


New Search Save As Close

192.168.2.23

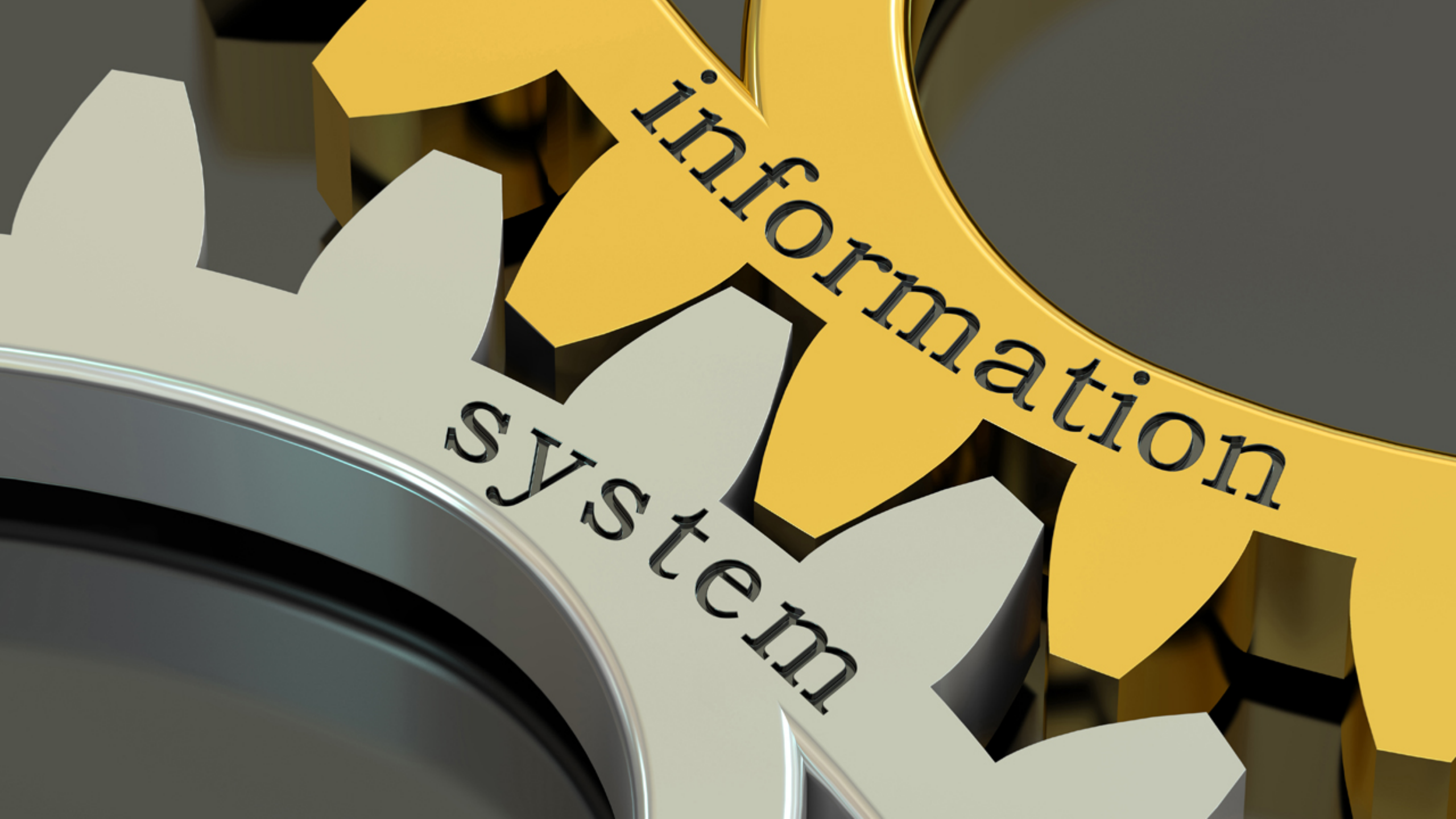
17 events (10/8/15 9:00:00.000 AM to 10/8/15 10:30:00.000 AM)

Events (17) Patterns Statistics Visualization



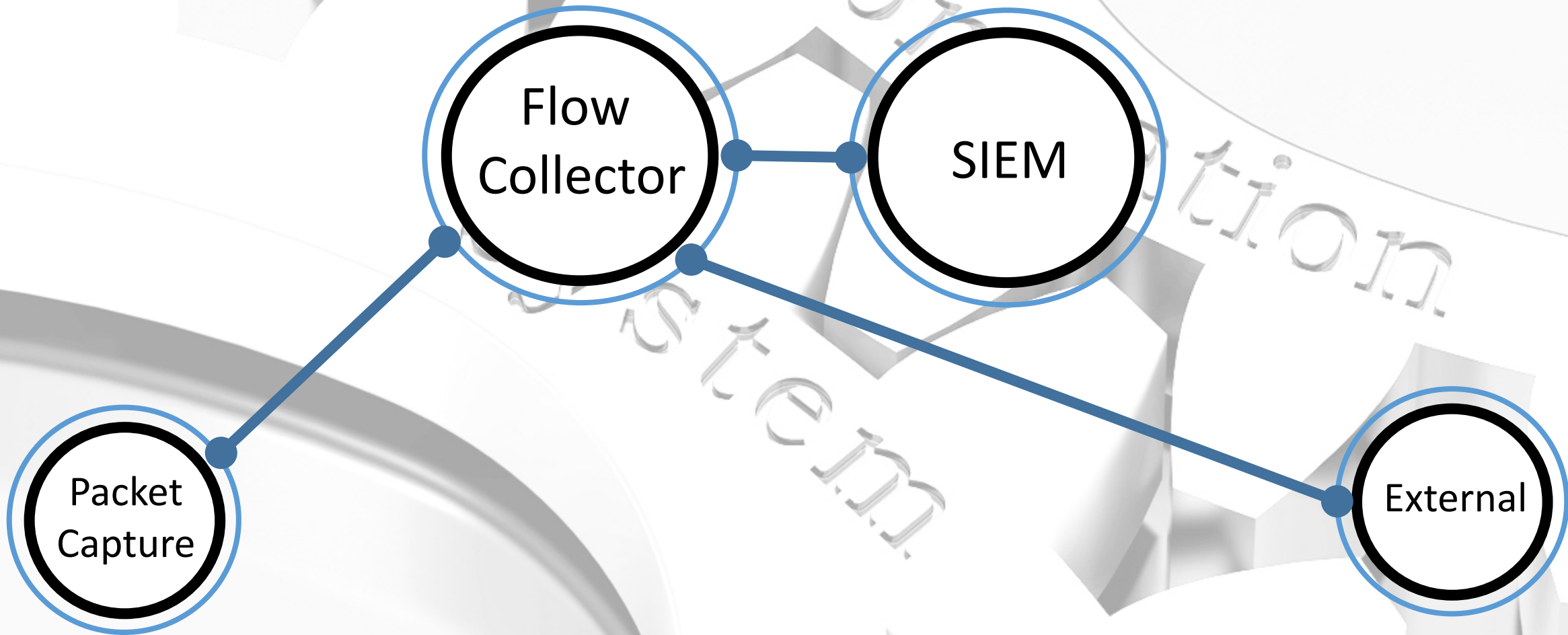
List Format 20 Per Page

i	Time	Event
>	10/8/15 10:26:51.000 AM	Oct 8 10:26:51 192.168.2.28 v... 05: 192.168.2.23 is sending more packets to replicate then is being replicated (IN: 101 > OUT: 98)
>	10/8/15 10:21:51.000 AM	Oct 8 10:21:51 192.168.2.28 vitals[26926]: P... 0005: 192.168.2.23 is sending more packets to replicate then is being replicated (IN: 80 > OUT: 79)
>	10/8/15 10:20:51.000 AM	Oct 8 10:20:51 192.168.2.28 vitals[26926]: PR10005: 192.168.2.23 is sending more packets to replicate then is being replicated (IN: 112 > OUT: 111)
>	10/8/15 9:58:51.000 AM	Oct 8 09:58:51 192.168.2.28 vitals[26926]: PR10005: 192.168.2.23 is sending more packets to replicate then is being replicated (IN: 84 > OUT: 83)
>	10/8/15 9:54:51.000 AM	Oct 8 09:54:51 192.168.2.28 vitals[26926]: PR10005: 192.168.2.23 is sending more packets to replicate then is being replicated (IN: 81 > OUT: 80)
>	10/8/15 9:52:51.000 AM	Oct 8 09:52:51 192.168.2.28 vitals[26926]: PR10005: 192.168.2.23 is sending more packets to replicate then is being replicated (IN: 49 > OUT: 48)



information

system



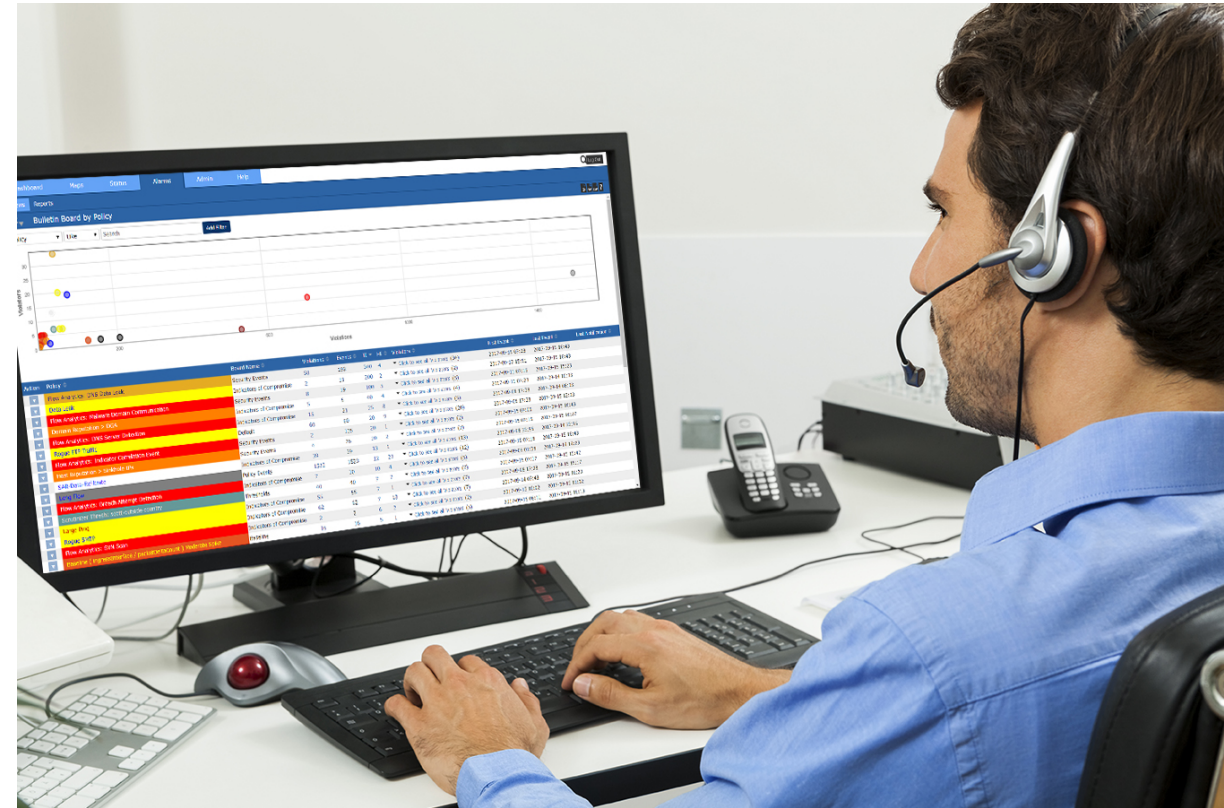


# Investigative Process



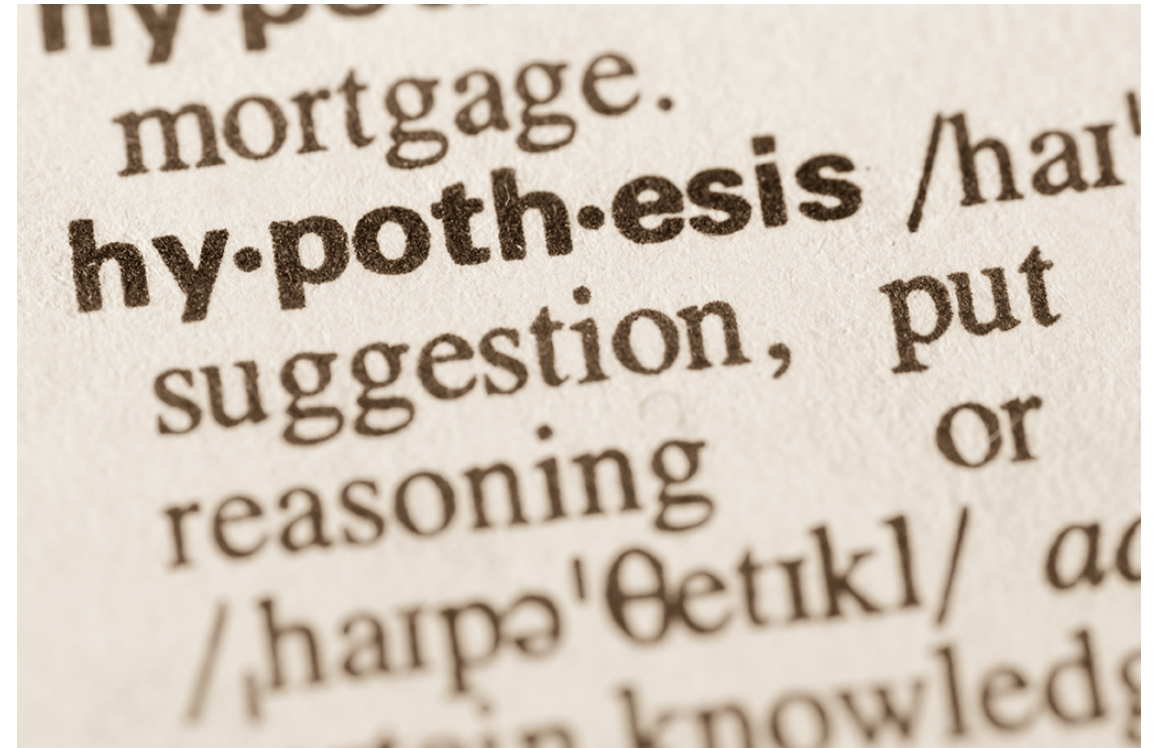
# Investigative Process

- Observation - How you find out:
  - Receive a call
  - Receive an alarm



# Investigative Process

- Observation - How you find out:
  - Receive a call
  - Receive an alarm
- Generate a Hypothesis – humans are biased and that is a good thing





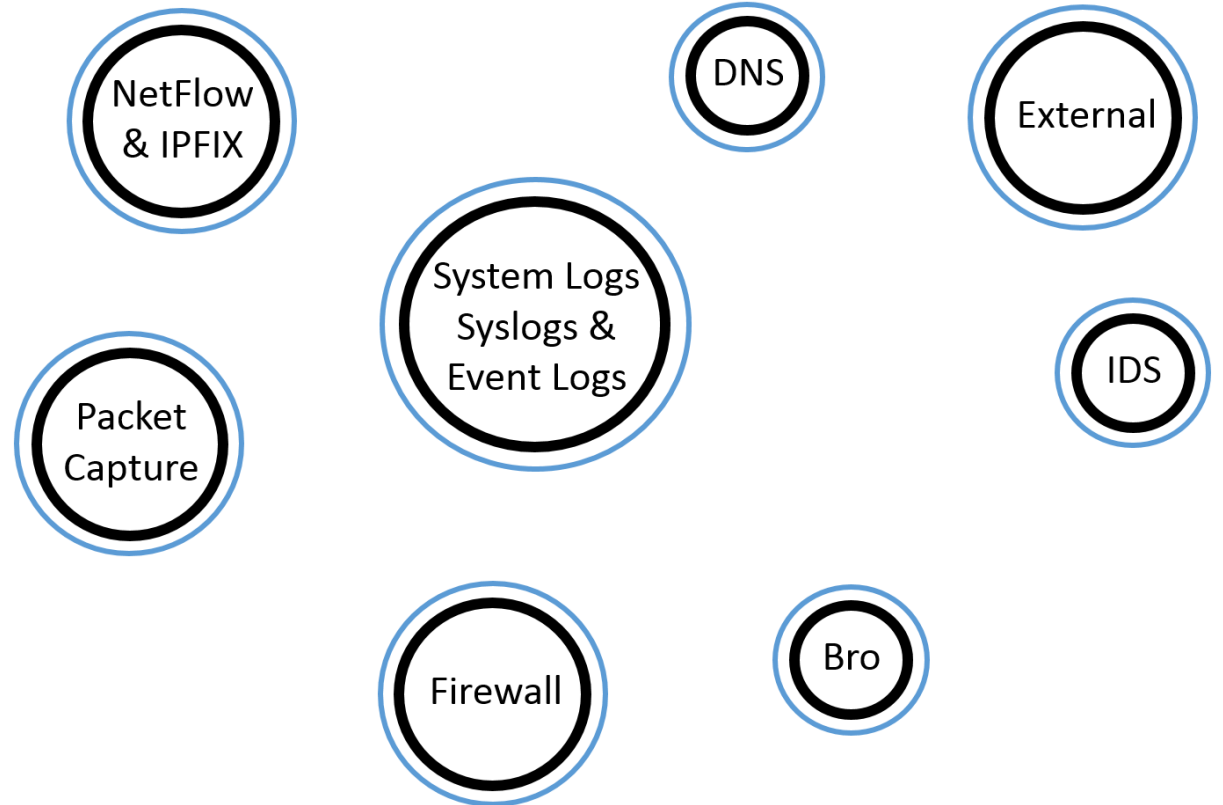
# Investigative Process

- Observation - How you find out:
  - Receive a call
  - Receive an alarm
- Generate a Hypothesis
- Try to define what you are looking for before you look!



# Investigative Process

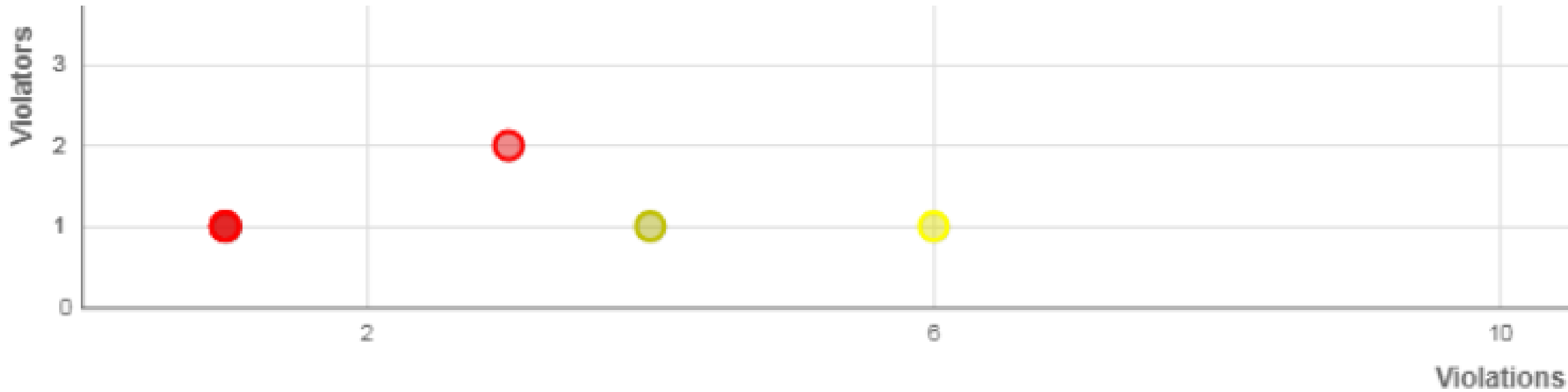
- Observation - How you find out:
  - Receive a call
  - Receive an alarm
- Generate a Hypothesis
- Define what you are looking for before you look!
- What data do you have that will allow you to answer questions?



# Agenda

- Fidelity : both low, medium and high
- Pivot : what is it
- Gains : from a pivot
- Pivot Fields : within the chart
- Pivot Chart : identifying data sources
- Examples
- Curiosity and thinking
- System Automation





Acknowledge

Acti...	<input type="checkbox"/>	Policy	Board Name	Violations	Events
▼	<input type="checkbox"/>	Flow Analytics: DNS Data Leak [Edit] [FA]	Security Events	1	2
▼	<input type="checkbox"/>	Scrutinizer Thresh: Foreign Country Threshold [Edit]	Thresholds	8	8
▼	<input type="checkbox"/>	Data Leak [Edit] [FA]	Indicators of Compromise	10	28
▼	<input type="checkbox"/>	Flow Analytics: Breach Attempt Detection [Edit] [FA]	Indicators of Compromise	3	3
▼	<input type="checkbox"/>	Rogue SMTP [Edit] [FA]	Indicators of Compromise	6	9
▼	<input type="checkbox"/>	Flow Analytics: Denied Flows [Edit] [FA]	Indicators of Compromise	1	3

▼	64.140.243.133	ec2-52-7-9-220.amazonaws.com	-	2017-11-07 11:21	2017-11-07 11:49	27m 9s	5	Indicators of Compromise	Possible Data Leak via iop with PCR: 1 First Seen: 2017-10-17 18:18:40.835828 External IP 52.7.9.220:39958 Internal IP 64.140.243.133:2055 Bytes Inbound 0.00 B Bytes Outbound 1.17 GB
▼	sddgj8bg2sea-pc.plxr.local	filemonster.com	seamus.mahone... anonymous log...	2017-11-07 11:43	N/A	N/A	1	Indicators of Compromise	Possible Data Leak via HTTP with PCR: 0.97 First Seen: 2017-11-07 11:38:54.94428 External IP 71.255.152.69:51054 Internal IP 10.60.1.65:80 Bytes Inbound 3.45 MB Bytes Outbound 205.27 MB

DNS\_Search

Default Flow Report

FTP

Default Flow Report

Flow Analytics Configuration

Pivot2Vision

SSH

View All Alarms for Violator 10.60.1.65

What is this?

ciscoIronPort

▼	64.140.243.133	ec2-52-7-9-
▼	sddgj8bg2sea-pc.plxr.local	filemo

Peak
CR: 1
7-10-17
28
7.9.220:39958
:2055
0.00 B
1.17 GB
Peak
CR: 0.97
7-11-07
3
51054
0.1.65:80
3.45 MB
205.27 MB



Report: UNSAVED

Templates Used: 2

Devices Used: 1

Report Details

Filters Add

Device/Interface edit x

Device: 0a3c010a

**Host to Host** edit x

Include

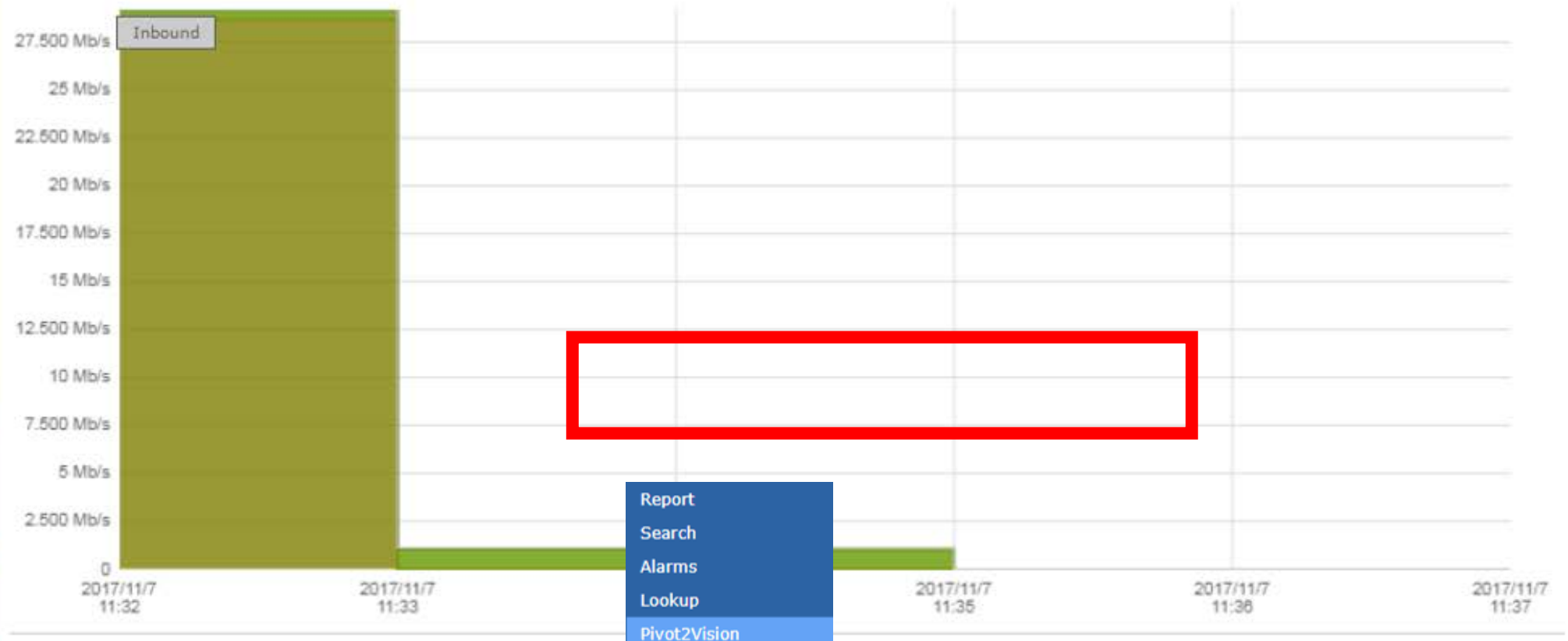
hostAip: 10.60.1.65

hostBip: 71.255.152.69

Applications Defined edit x

393296

Threshold Add



- Report
- Search
- Alarms
- Lookup
- Pivot2Vision
- DNS\_Search
- Investigations
- GEO IP
- Cisco IronPort
- Cisco ISE

Inbound Results

	Source	Destination	Packets	Traffic %	Bits
1	sddgj8bg2sea-pc.plxr.local	filemonster.com	489.327 p/s	91.60 %	5.744 Mb/s
2	filemonster.com	sddgj8bg2sea-pc.plxr.local	288.023 p/s	8.40 %	526.416 kb/s
Other			-		0.000 b/s
Total*			777.350 p/s		6.270 Mb/s

Results 1-2 of 2

Prev 1 Next



## Scrutinizer-Investigation

Layout Tools Send

1 Source endace-9abe02:test4TB Filter Directionless IP is 10.60.1.65 Time 2 mins; 19 minutes ago Cancel Apply

Data Sources endace-9abe02:test4TB

2017/11/7 16:32:00.0 (UTC) - 2017/11/7 16:34:00.0 (UTC) 2 mins Undo

Mon, Oct 23rd 2017 at 19:30:19 (UTC) Metadata 7 days, 11 mins Packet Data 14 days, 21 hours

Tue, Nov 7th 2017 at 16:51:12 (UTC)

## Conversations

By IP Address

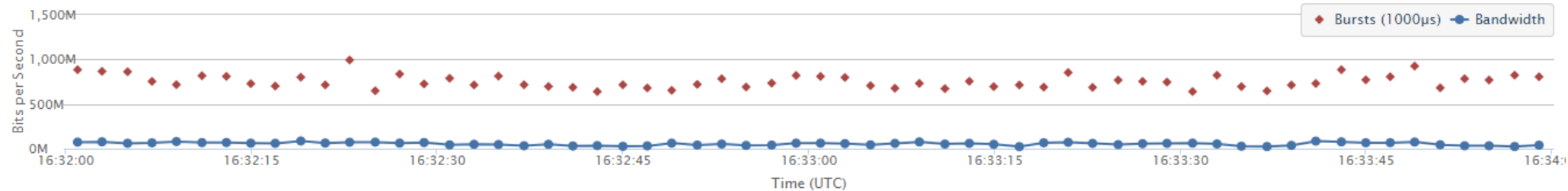
Undo

IPs				Packets			Bits			Bits/s			TCP Initial Round Trip Time			T
Host A	Host B	Sessions	Duration	Total	A>B	B>A	Total	A>B	B>A	Total	A>B	B>A	Max	Avg	Min	In
10.60.1.65	71.255.152.69	7	1m 24s	57,362	36,131	21,231	471.7 Mb	429.0 Mb	42.7 Mb	5.6 Mb/s	5.1 Mb/s	508.9 Kb/s	23.271ms	15.481ms	0ms	6
10.60.1.65	108.174.10.10	2	1m 22s	66	30	36	136.0 Kb	103.3 Kb	32.7 Kb	1.7 Kb/s	1.3 Kb/s	399.0 b/s	0ms	0ms	0ms	0
10.60.1.65	64.140.243.154	1	1s	22	11	11	77.7 Kb	23.0 Kb	54.7 Kb	77.7 Kb/s	23.0 Kb/s	54.7 Kb/s	1.224ms	1.224ms	1.224ms	1
10.60.1.65	172.217.12.170	2	2s	11	7	4	7.2 Kb	4.5 Kb	2.7 Kb	3.6 Kb/s	2.2 Kb/s	1.3 Kb/s	0ms	0ms	0ms	0
10.60.1.65	13.33.35.79	2	2s	9	6	3	5.8 Kb	3.9 Kb	1.9 Kb	2.9 Kb/s	2.0 Kb/s	928.0 b/s	0ms	0ms	0ms	0
10.60.1.65	104.45.11.195	1	1s	1	1	0	512.0 bits	512.0 bits	0	512.0 b/s	512.0 b/s	0	0ms	0ms	0ms	0

## Bandwidth

Note. Filters are not applied to this tool

Undo





Packet	Hostname	Content Type	Size	Filename
168	filemonster.com	application/x-www-form-urlencoded	131 bytes	?login=1
213	filemonster.com	text/html	46 kB	?cd=
233	filemonster.com	image/png	20 kB	icons30px.png
110204	file			
110288	file			
110991	file			%20Training.mp4
111617	file			
111689	file			
112113	file			
113705	file			
113714	file			
113725	filemonster.com	application/x-www-form-urlencoded	131 bytes	?login=1
113776	filemonster.com	text/html	47 kB	?cd=
113806	filemonster.com	text/html	6831 bytes	?logout=1
114494	filemonster.com	video/mp4	657 kB	Marblehead%20Bank%20%20Training.mp4

# Training.mp4

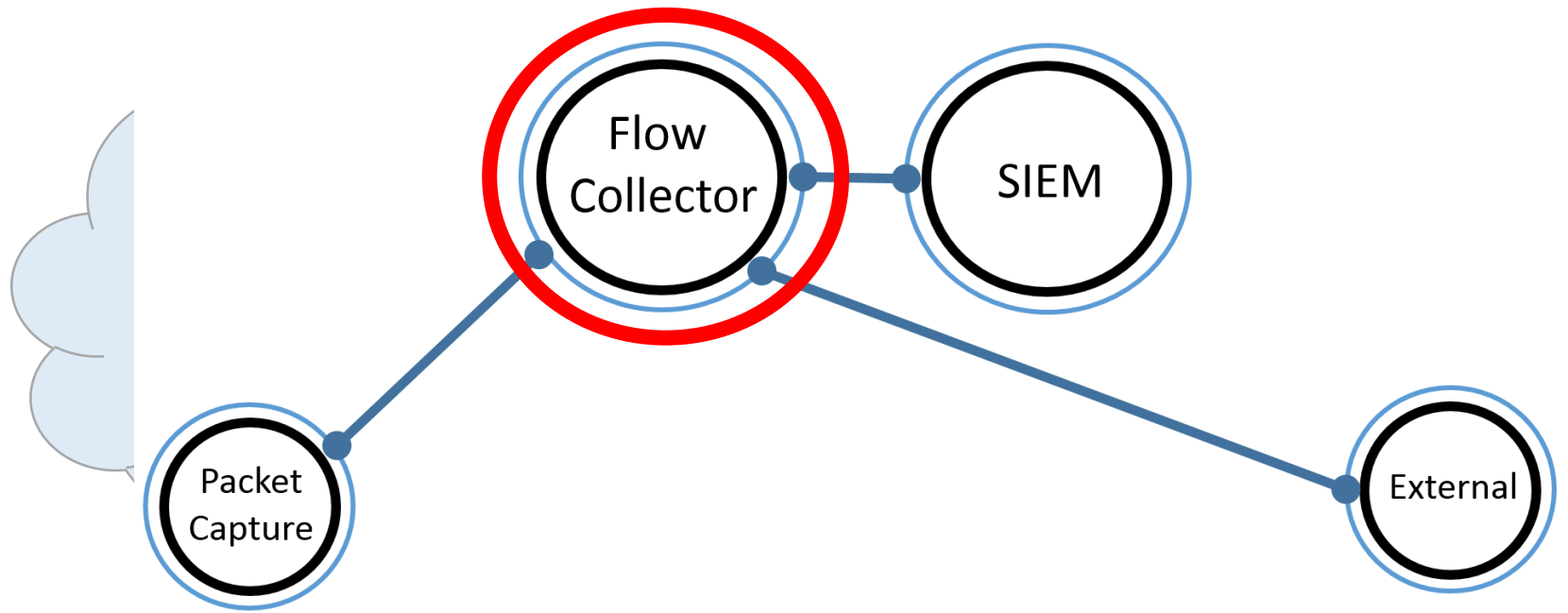
Save

Save All

Close

Help

# Example 2



I have an IP address, show me all the things I can pivot to.

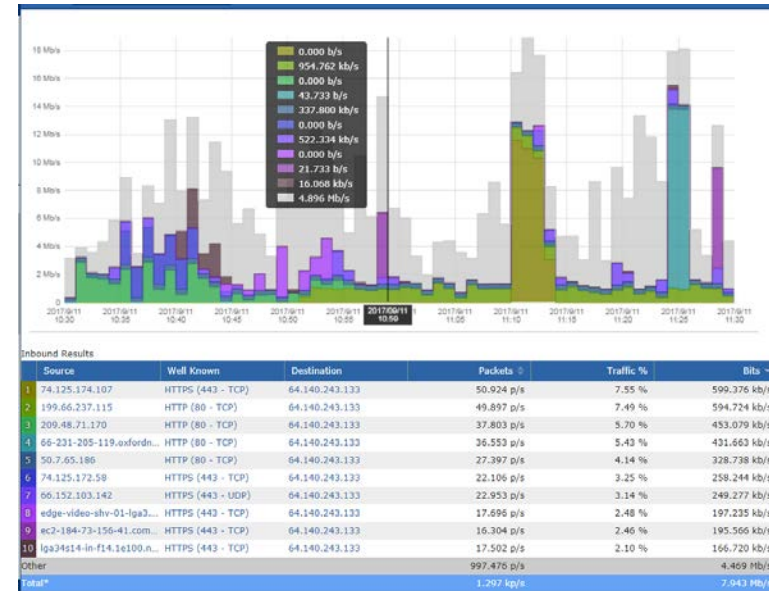


## Host Index

Search IP:

151.101.117.67

Search





Report: UNSAVED

+ Templates Used: 2

+ Devices Used: 1

Report Details

Filters

Add

Device/Interface edit x

Device: 3850b-Closet.plxr.local

Interface: ALL

IP Host edit x

Include

IP: 151.101.117.67

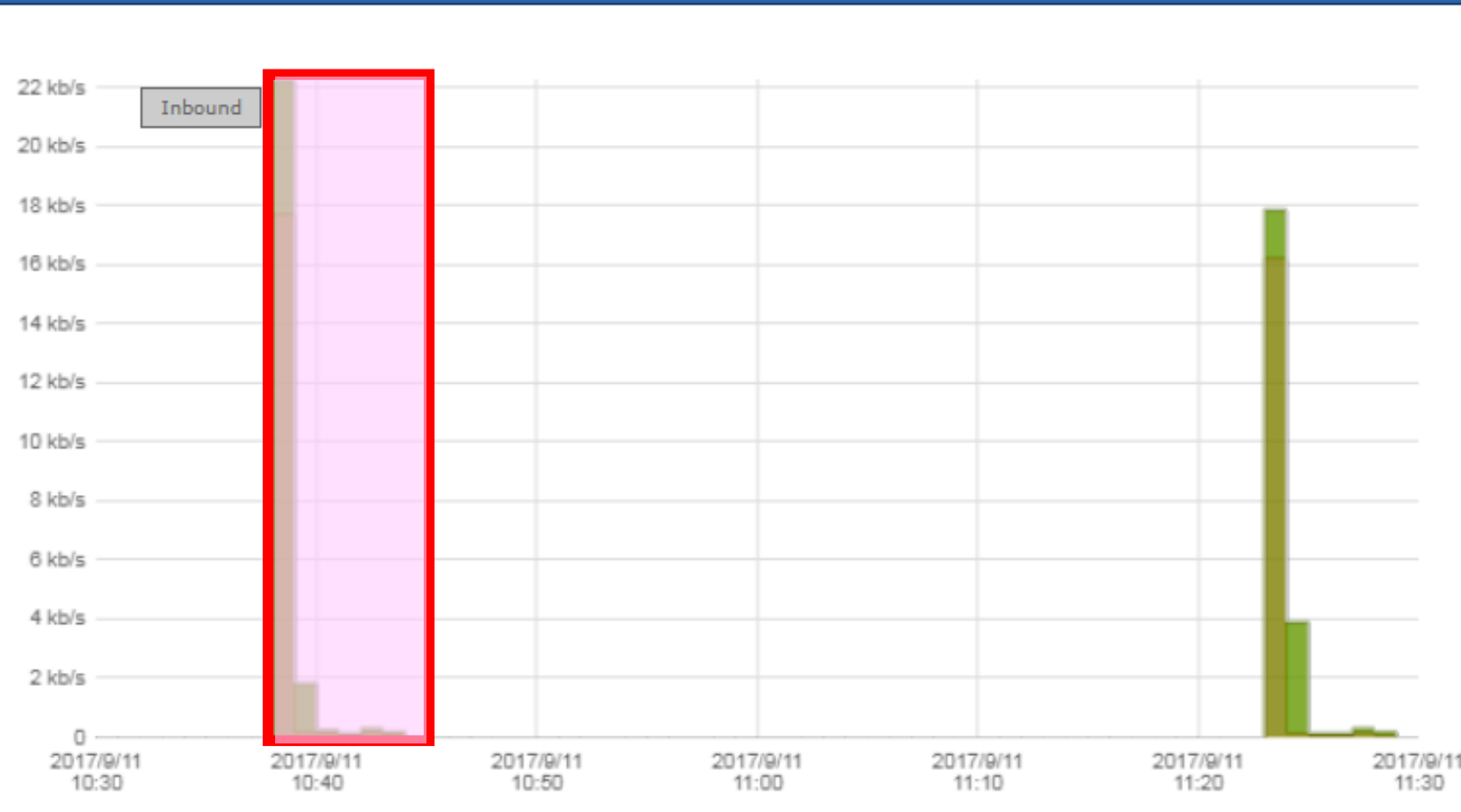
Source Or Destination

Threshold

Add



(1m) intervals



## Inbound Results

	Source	Well Known	Destination	Packets	Traffic %	Bits
1	151.101.117.67	HTTP (80 - TCP)	sa20sblc2-pc.plxr...	0.127 p/s	73.72 %	585.884 b/s
2	sa20sblc2-pc.plxr...	HTTP (80 - TCP)	151.101.117.67	0.128 p/s	26.28 %	208.893 b/s
	Other			-		0.000 b/s
	Total*			0.255 p/s		794.778 b/s



Report: UNSAVED

Templates Used: 2

Devices Used: 1

Report Details

Filters

Add

Device/Interface edit x

Device: 3850b-Closet.plxr.local

Interface: ALL

IP Host edit x

Include

IP: 151.101.117.67

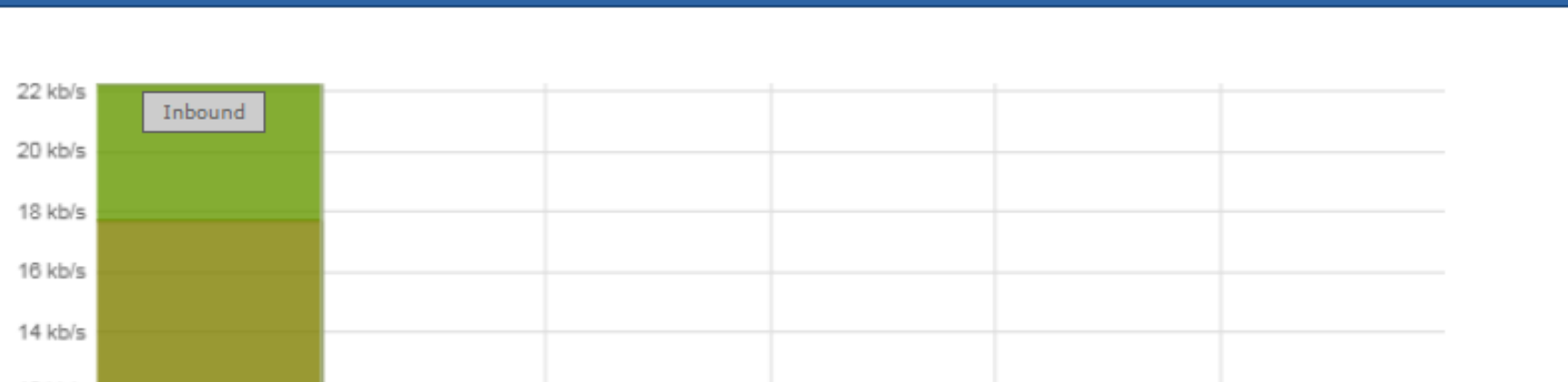
Source Or Destination

Threshold

Add



(1m) intervals



Save Changes

Cancel Changes

Gigamon-1

show ip



Use All



	Source					
1	151.101.117.67	HTTP (80 - TCP)	sa20sblc2-pc.plxr...	0.639 p/s	73.36 %	3.063 kb/s
2	sa20sblc2-pc.plxr...	HTTP (80 - TCP)	151.101.117.67	0.628 p/s	26.64 %	1.112 kb/s
	Other			-		0.000 b/s
Total*				1.267 p/s		4.176 kb/s

(1m) intervals



Report: UNSAVED

Templates Used: 2

Devices Used: 1

Report Details

Filters

Add

Device/Interface

edit x

Device: Gigamon-1

Interface: ALL

IP Host

edit x

Include

IP: 151.101.117.67

Source Or Destination

Threshold

Add



Reports

Default Report

Counts 8

Top Reports 7

Source Reports 12

Destination Reports 11

Pair Reports 16

Volume Reports 4

Designed Reports 2

Gigamon 9

Summary Reports 4

Flow View

Outbound Results

	Source	Well Known	De	Traffic %	Bits
1	151.101.117.67	HTTP (80 - TCP)	de2	88.54 %	60.995 kb/s
2	de27jtc72benp.pl...	HTTP (80 - TCP)	151	11.15 %	7.683 kb/s
3	151.101.117.67	HTTP (80 - TCP)	sa2	0.17 %	119.556 b/s
4	sa20sblc2-pc.plxr...	HTTP (80 - TCP)	151.101.117.67	0.13 %	92.356 b/s
Other					0.000 b/s
Total*					68.890 kb/s

Destination Name and URL

Hosts with URL

Pair Names and URL

Return Codes

SSL All Details

SSL Version Count

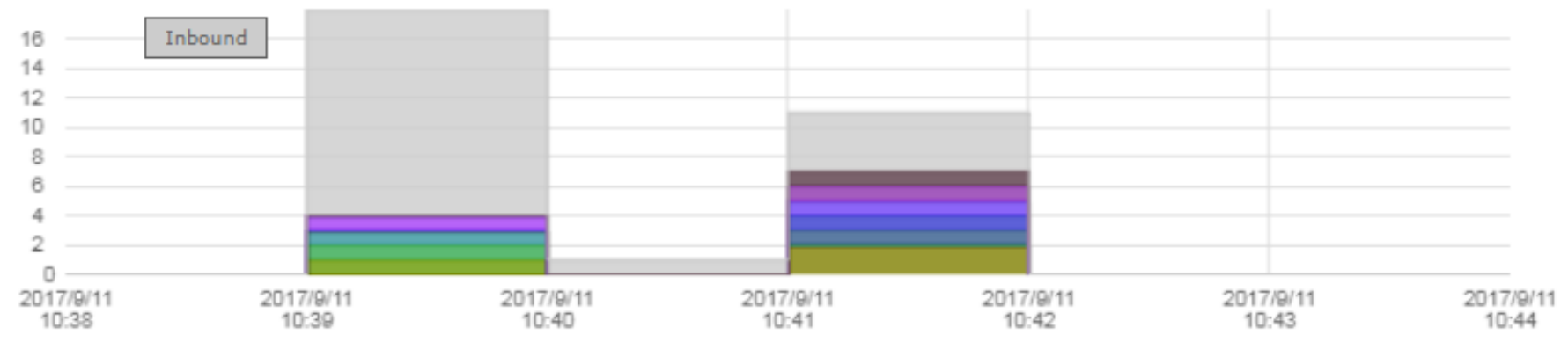
Source Name and URL

URL Count

URL and Return Codes



intervals



Report: UNSAVED

Templates Used: 1

Devices Used: 1

Report Details

Exclude Filter

Filters Add

Device/Interface edit x

Device: Gigamon-1

Interface: ALL

IP Host edit x

Include

IP: 151.101.117.67

Source Or Destination

Results

	URL	Return Code	Count
1	::ffff:172.17.3.2	0	2
2	www. .... com/.a/2.37.0/js/cnn-an...	0	1
3	www. .... com/.a/fonts/cnn/3.5.0/c...	0	1
4	www. .... com/.a/2.37.0/js/cnn-foo...	0	1
5	www. .... com/.a/2.37.0/js/cnn-sta...	0	1
6	::ffff: .. .16	0	1
7	www. .... nteractive/storm-tracker/..	0	1
8	www. .... com/.a/2.37.0/assets/vid..	0	1
9	www. .... nteractive/storm-tracker/..	0	1
10	www. .... nteractive/storm-tracker/..	0	1
	Other		19
	<b>Total*</b>		<b>30</b>

Drag 0 to add as a filter





intervals

# Return Code

# 503

2017/9/11  
10:44

Report:

UNSAVED

Templates Used: 1

Devices Used: 1

Report Details

Filters

Add

Device/Interface edit x

Device: Gigamon-1

Interface: ALL

IP Host edit x

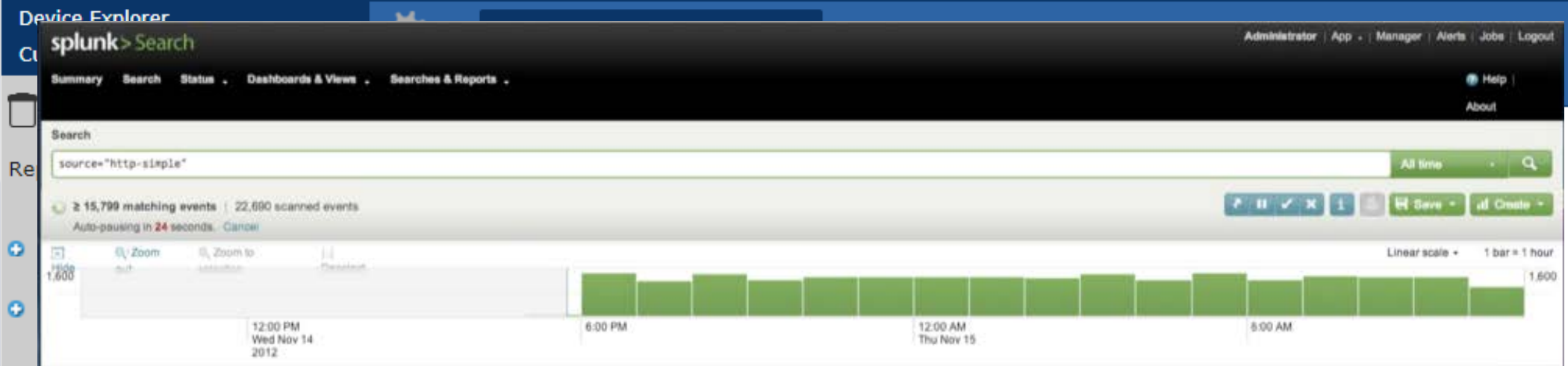
Include

IP: 151.101.117.67

Results

	URL	Return Code	Count
1	cache-bos8221-BOS	503	1
Other			0
Total*			1

Results 1-1 of 1



Field discovery is:  On

3 selected fields: host (1), source (1), sourcetype (1)

26 interesting fields: ad\_application\_id (1), ad\_application\_name (1), ad\_event\_types (2), ad\_num\_events\_for\_types (45), ad\_summary\_id (x100), ad\_summary\_severity (1), ad\_summary\_time (x100), ad\_summary\_type (3), ad\_tag (1), desc (17), duration (1), dvc\_time (86), event\_id (2), eventsummary (x100), index (1)

15,799 events over all time

Time	Event ID	Description
11/15/12 10:30:25.068 AM	2012-11-15 18:30:25:068+0000	name="InfoEvents" event_id="6" desc="Errors in Request [[Error] Request was slower than static threshold (700 ms) - UncategorizedJmsException: Uncategorized exception occurred during JMS processing; nested exception is javax.jms.JMSException: Wire format negotiation timeout: peer did not send his wire format.; nested exception is java.io.IOException: Wire format negotiation timeout: peer did not send his wire format. - ]" ad_summary_id="948645" ad_application_name="Acme Online Book Store" ad_application_id="7" event_id="6" severity="INFO" url="http://ec2-23-23-50-203.compute-1.amazonaws.com:8090/controller/#location=APP_EVENT_VIEWER_MODAL&eventSummary=948645" ad_summary_type="ERROR" ad_event_types="{APPLICATION_ERROR, ERROR}" duration="15" ad_summary_time="Thu Nov 15 18:13:39 UTC 2012" priority="1" ad_tag="AppDynamics Event" name="InfoEvents" ad_summary_severity="ERROR" ad_num_events_for_types="{45, 174}" dvc_time="Thu Nov 15 18:29:55 UTC 2012"
11/15/12 10:30:25.062 AM	2012-11-15 18:30:25:062+0000	name="InfoEvents" event_id="6" desc="Errors in Request [[Error] Request was slower than static threshold (700 ms) - UncategorizedJmsException: Uncategorized exception occurred during JMS processing; nested exception is javax.jms.JMSException: Wire format negotiation timeout: peer did not send his wire format.; nested exception is java.io.IOException: Wire format negotiation timeout: peer did not send his wire format. - ]" ad_summary_id="948641" ad_application_name="Acme Online Book Store" ad_application_id="7" event_id="6" severity="INFO" url="http://ec2-23-23-50-203.compute-1.amazonaws.com:8090/controller/#location=APP_EVENT_VIEWER_MODAL&eventSummary=948641" ad_summary_type="ERROR" ad_event_types="{APPLICATION_ERROR, ERROR}" duration="15" ad_summary_time="Thu Nov 15 18:13:49 UTC 2012" priority="1" ad_tag="AppDynamics Event" name="InfoEvents" ad_summary_severity="ERROR" ad_num_events_for_types="{45, 174}" dvc_time="Thu Nov 15 18:29:55 UTC 2012"
11/15/12 10:30:25.056 AM	2012-11-15 18:30:25:056+0000	name="InfoEvents" event_id="6" desc="Errors in Request [[Error] Request was slower than static threshold (700 ms) - UncategorizedJmsException: Uncategorized exception occurred during JMS processing; nested exception is javax.jms.JMSException: Wire format negotiation timeout: peer did not send his wire format.; nested exception is java.io.IOException: Wire format negotiation timeout: peer did not send his wire format. - ]" ad_summary_id="948639" ad_application_name="Acme Online Book Store" ad_application_id="7" event_id="6" severity="INFO" url="http://ec2-23-23-50-203.compute-1.amazonaws.com:8090/controller/#location=APP_EVENT_VIEWER_MODAL&eventSummary=948639" ad_summary_type="ERROR" ad_event_types="{APPLICATION_ERROR, ERROR}" duration="15" ad_summary_time="Thu Nov 15 18:13:59 UTC 2012" priority="1" ad_tag="AppDynamics Event" name="InfoEvents" ad_summary_severity="ERROR" ad_num_events_for_types="{45, 174}" dvc_time="Thu Nov 15 18:29:55 UTC 2012"
11/15/12 10:30:25.052 AM	2012-11-15 18:30:25:052+0000	name="InfoEvents" event_id="6" desc="Errors in Request [[Error] Request was slower than static threshold (700 ms) - UncategorizedJmsException: Uncategorized exception occurred during JMS processing; nested exception is javax.jms.JMSException: Wire format negotiation timeout: peer did not send his wire format.; nested exception is java.io.IOException: Wire format negotiation timeout: peer did not send his wire format. - ]" ad_summary_id="948648" ad_application_name="Acme Online Book Store" ad_application_id="7" event_id="6" severity="INFO" url="http://ec2-23-23-50-203.compute-1.amazonaws.com:8090/controller/#location=APP_EVENT_VIEWER_MODAL&eventSummary=948648" ad_summary_type="ERROR" ad_event_types="{APPLICATION_ERROR, ERROR}" duration="15" ad_summary_time="Thu Nov 15 18:14:16 UTC 2012" priority="1" ad_tag="AppDynamics Event" name="InfoEvents" ad_summary_severity="ERROR" ad_num_events_for_types="{45, 174}" dvc_time="Thu Nov 15 18:29:55 UTC 2012"

Flow ID	Destination	Protocol	IP Address	Rate	Percentage
2	de27jtc72benp.pl...	HTTP (80 - TCP)	151.101.117.67	8.300 p/s	11.15 %
3	151.101.117.67	HTTP (80 - TCP)	sa20sblc2-pc.plxr...	0.256 p/s	0.17 %
4	sa20sblc2-pc.plxr...	HTTP (80 - TCP)	151.101.117.67	0.283 p/s	0.13 %
Other				-	0.000 b/s
Total*				16.022 p/s	68.890 kb/s

nPort  
Splunk  
Probe P2P

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.60.1.16	151.101.117.67	TCP	60	56042->80 [ACK] Seq=1 Ack=1 win=
2	0.384838	10.60.1.16	151.101.117.67	TCP	1514	[TCP segment of a reassembled
3	0.384856	10.60.1.16	151.101.117.67	HTTP	841	GET /data/ocs/section/_homepage
4	0.387100	10.60.1.16	151.101.117.67	TCP	66	56085->80 [SYN] Seq=0 win=8192

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)

- Ethernet II, Src: Cisco\_80:5e:c0 (c4:64:13:80:5e:c0), Dst: sonicwa\_e0:23:b8 (00:17:c5:e0:23:b8)
- Internet Protocol Version 4, Src: 10.60.1.16 (10.60.1.16), Dst: 151.101.117.67 (151.101.117.67)
- Transmission Control Protocol, Src Port: 56042 (56042), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 0
  - Source Port: 56042 (56042)
  - Destination Port: 80 (80)
  - [Stream index: 0]
  - [TCP Segment Len: 0]
  - Sequence number: 1 (relative sequence number)
  - Acknowledgment number: 1 (relative ack number)
  - Header Length: 20 bytes
  - .... 0000 0001 0000 = Flags: 0x010 (ACK)
  - window size value: 251
  - [Calculated window size: 251]
  - [window size scaling factor: -1 (unknown)]
  - Checksum: 0xec4e [validation disabled]
  - Urgent pointer: 0

```

0000 00 17 c5 e0 23 b8 c4 64 13 80 5e c0 08 00 45 00  ....#.d ..^...E.
0010 00 28 6f 4a 40 00 7f 06 74 91 0a 3c 01 10 97 65  .(oJ@... t.<...e
0020 75 43 da ea 00 50 5d 67 05 13 c2 43 aa 9d 50 10  uC...P]g ...C..P.
0030 00 fb ec 4e 00 00 00 00 00 00 00 00  ....N.....

```

44 in auto ?

- Report
- Search
- Alarms
- Lookup
- GEO IP
- Cisco IronPort
- Search Splunk
- HP Arc
- EndaceProbe P2P**
- Moloch
- Cisco ISE

119.330 b/s  
92.356 b/s  
0.000 b/s  
68.890 kb/s



Report: UNSAVE

+ Templates U

+ Devices Use

Report Details

Filters

Device/Interface

Device: Gigamon

Interface: ALL

IP Host

Include

IP: 151.101.117.

Source Or Destin

Threshold



Lookup data results for IP Address

151.101.117.67

Search by IP, domain, or network owner for real-time threat data.

Reputation Overview | Email & Spam Data | Malware Data | Reputation Support

### LOCATION DATA

San Francisco, United States



### OWNER DETAILS

IP ADDRESS 151.101.117.67

FWD/REV DNS MATCH No

NETWORK OWNER Fastly

### REPUTATION DETAILS

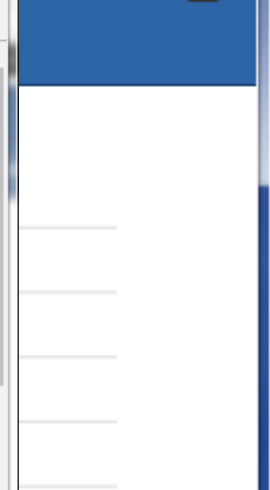
EMAIL REPUTATION Neutral

WEB REPUTATION Neutral

SPAM LEVEL None

LAST DAY LAST MONTH

SPAM LEVEL None None



Report

Search

Alarms

Lookup

GEO IP

Cisco IronPort

Search Splunk

HP Arc

EndaceProbe P2P

Moloch

Cisco ISE

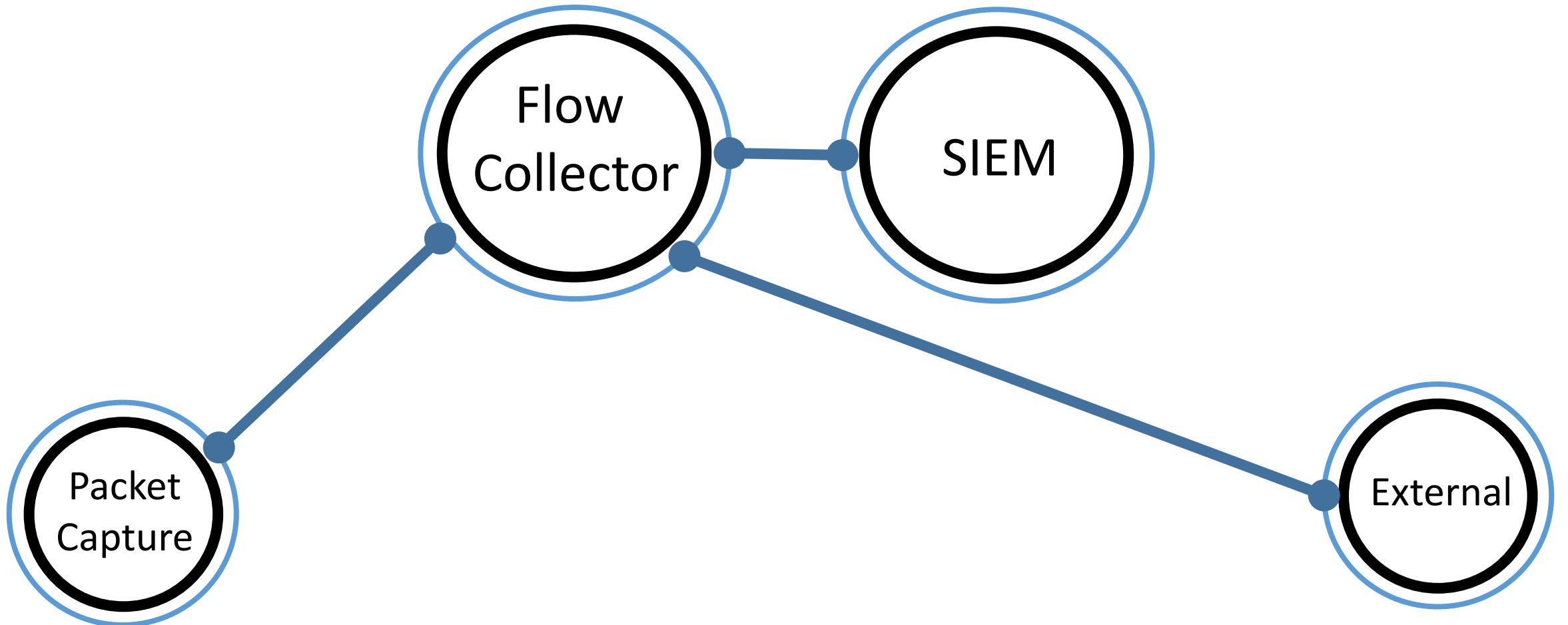
119.350 b/s

92.356 b/s

0.000 b/s

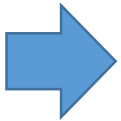
68.800 kb/s

“100% of analysts use pivots” - Chris Sanders



# Agenda

- Fidelity : both low, medium and high
- Pivot : what is it
- Gains : from a pivot
- Pivot Chart : identifying data sources
- Pivot Fields : within the chart
- Example
- Curiosity and thinking
- System Automation



**Curiosity**



# Curiosity makes Effective Hunters

- The desire to find out
- Create a curiosity culture by promoting discussion
- Learn how to ask the right questions. “Is this an anomaly or something I haven’t run into before?”
- Don’t be intimidated. Years at the job does not make someone proficient
- Be careful: Years of experience can lead to less curiosity

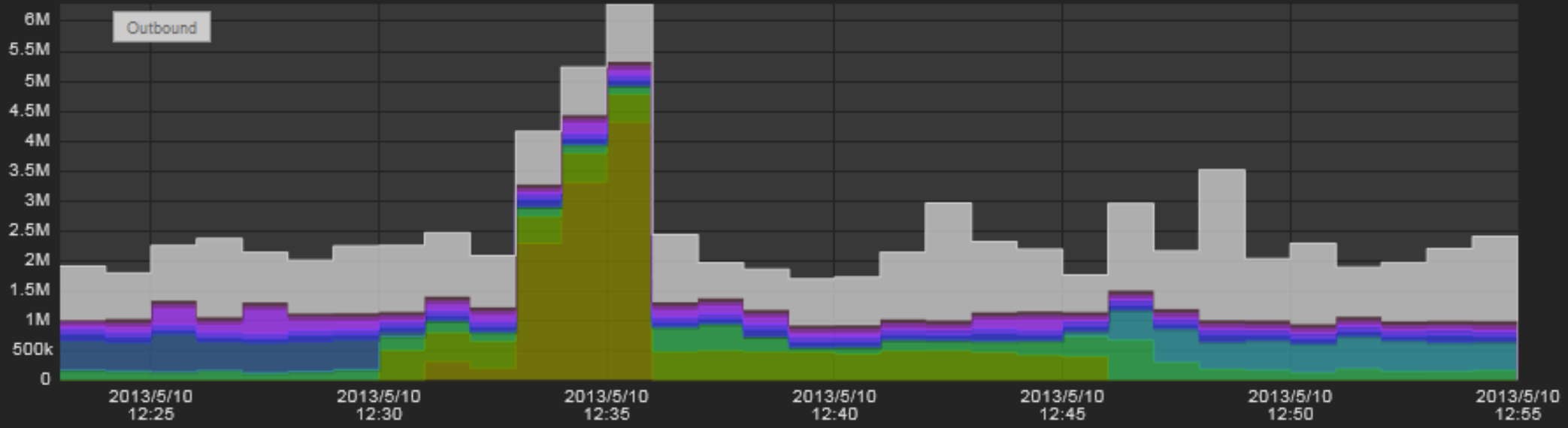




automation

processes

1m Interval (Rate)



Custom 2013-5-10 12:23 to 2013-5-10 12:55 Apply Dates View Raw Flows ( Outbound )

Outbound Results 1 - 10 of 971 (0.26s)

Metering: Ingress

	Source	User Name(s)	Packets	Percent	Bits
1	10.11.1.102	LXR/debbyc, LXR/ldapbind, PLXR/marc, PLXR/mikek, PLXR/ogk	33.47 p/s	13.10 %	325.97 Kb/s
2	10.11.1.55	LXR/ellenl, PLXR/debbyc, PLXR/ldapbind, PLXR/marc, PLXR/mikek, PLXR/oglas	17.77 p/s	7.12 %	233.18 Kb/s
3	10.11.1.67	LXR/patriciaa	48.42 p/s	8.52 %	212.14 Kb/s
4	10.11.1.53	LXR/danielp	12.02 p/s	5.75 %	143.07 Kb/s
5	10.11.1.49	LXR/ryanj	9.29 p/s	4.44 %	110.49 Kb/s
6	10.11.1.38	LXR/andrewy	45.49 p/s	3.54 %	88.12 Kb/s
7	10.11.1.106	LXR/justinj	50.30 p/s	3.53 %	87.91 Kb/s
8	10.11.1.118	LXR/pauld	28.49 p/s	3.41 %	84.77 Kb/s
9	10.11.1.100	LXR/scottr	6.90 p/s	2.93 %	72.90 Kb/s
10	10.11.1.48	LXR/seanh	5.48 p/s	2.65 %	65.85 Kb/s
Other	(What is this?)		349.89 p/s	42.77 %	1.06 Mb/s
Total	(from conv tables)		609.54 p/s	100 %	2.49 Mb/s

“Reviewing network perimeter NetFlow will help determine whether a network has experienced suspicious activity.”

Oct 21, 2017



US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

# Summary on Pivoting

- Single pivots almost never happen. Plan for at least 4.
- Pivots often require decisions by the analyst. (e.g. should you pivot to the event logs, the flows or external site for details). Pivot decisions are guided by the questions you are trying to answer.
- Keep economy in mind. The Defense team absolutely must have efficiencies. Pivots need to be fast to improve speed.
  - Extra pivot steps defeats efficiency
  - Pivots need to be short to decrease time spent
  - Improves accuracy to bridge the perception to reality gap
- Share frequently used pivots with others