Fraud, The Missing Link

SEC1164

Andrew Morris

Sr. Security Strategist | Splunk

Gleb Esman

Staff Security Strategist | Splunk

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or plans of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only, and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.

splunk> .conf20

Andrew Morris

Sr. Security Strategist | Splunk

Gleb Esman

Staff Security Strategist | Splunk

splunk> .conf20

Agenda

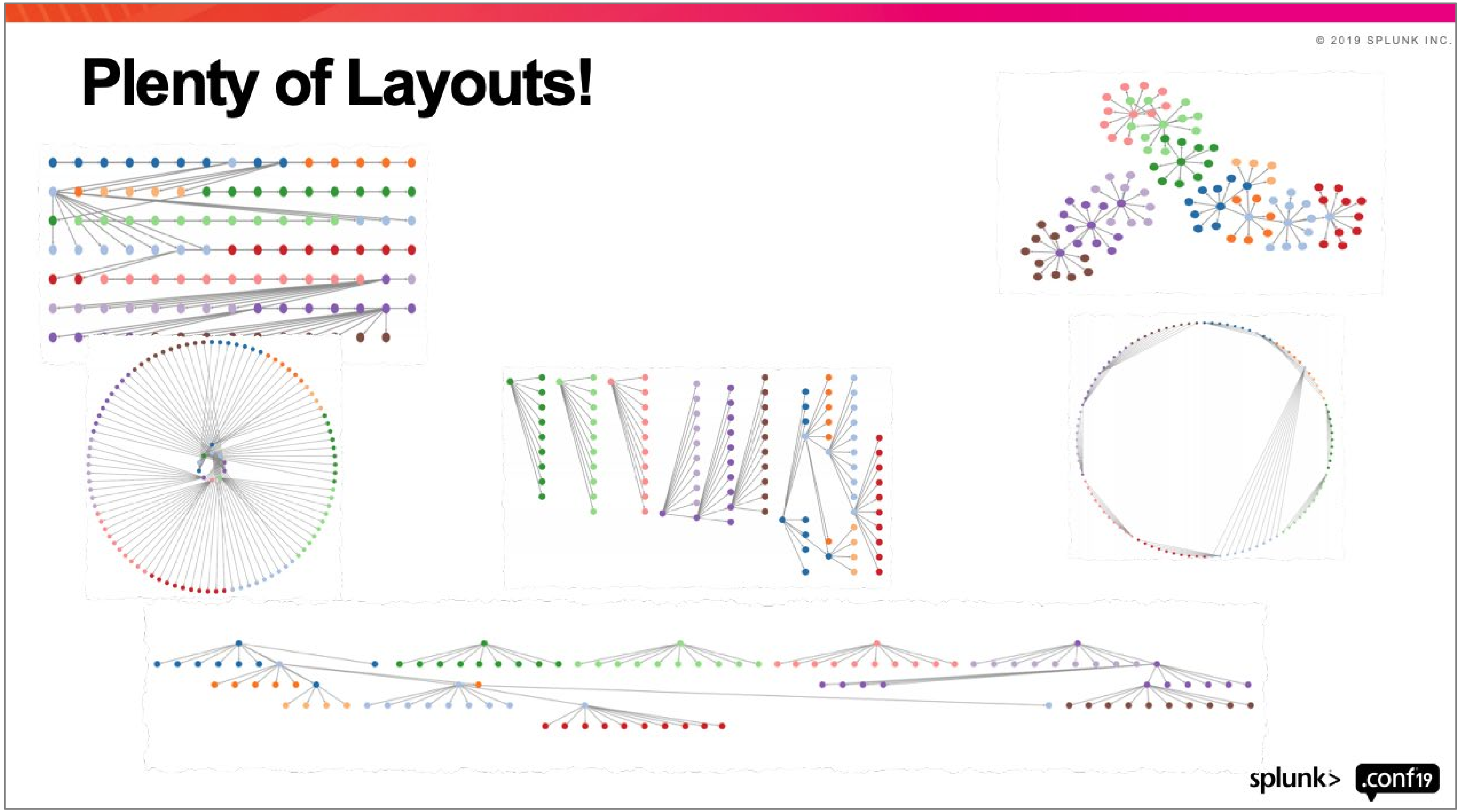
1. **What's been covered before**
   .Conf19 BOTS the Missing Link (not required)
2. **What was missing**
   Things I wanted to do
3. **Techniques**
   Data manipulation
4. **Visualization options**
   New stuff
5. **Demo**
   Even more really new stuff

Investigations Are Fun!

Fraud – Security - IT - and more

Last Year….. Link Analysis App for Splunk

.Conf19 – SEC1781 BOTS the Missing Link

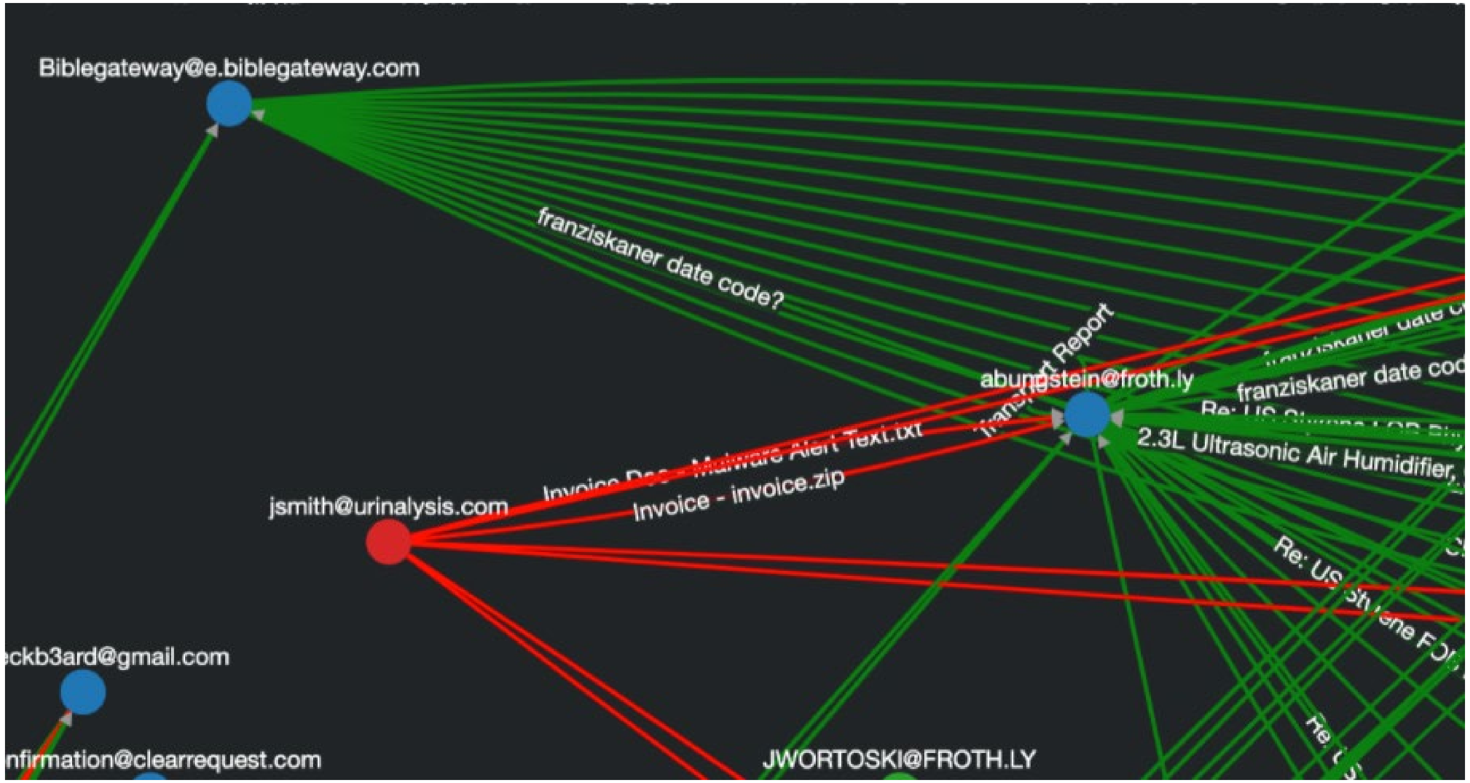


Plenty of Layouts!

But Things Were Missing for Me….

I Want More!

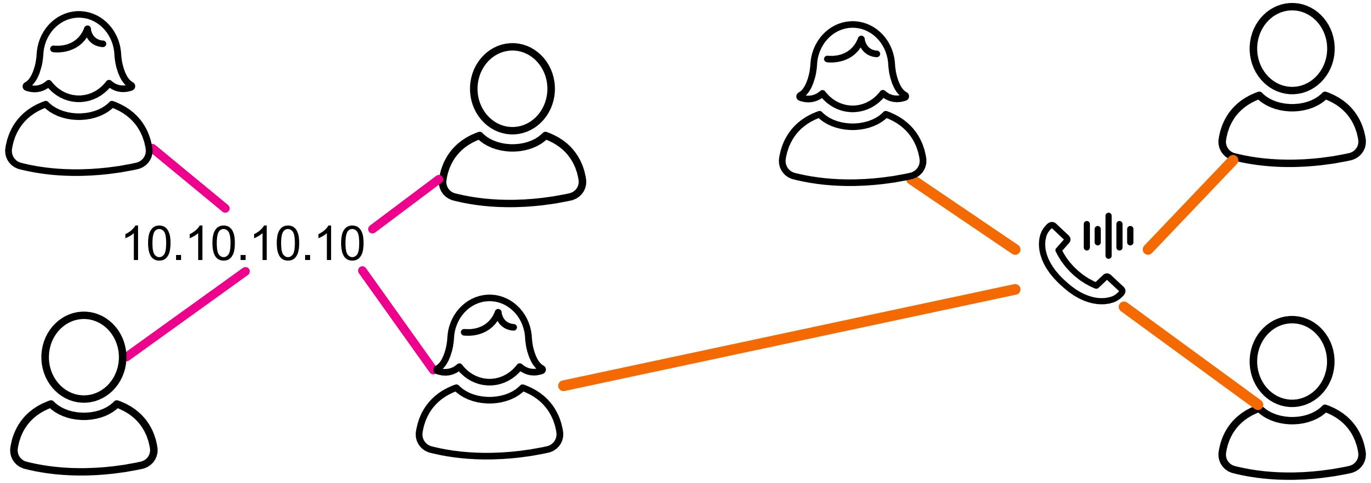
Too many nodes or the diagrams to busy



But Things Are Missing…

I Want More!

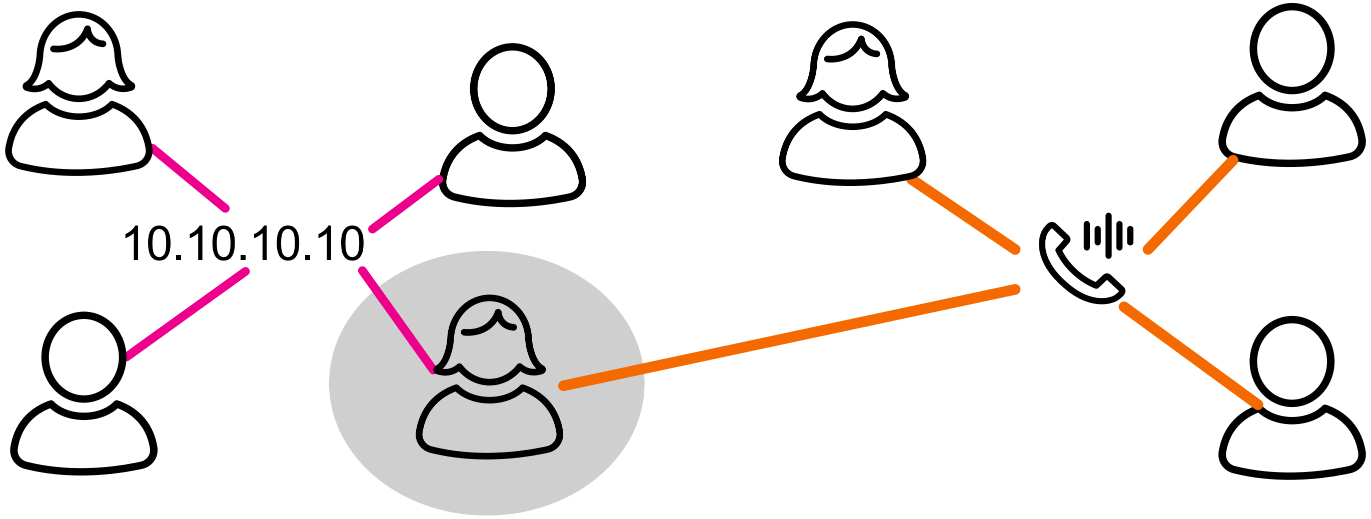
Field Limitations – multi-relationship



But Things Are Missing…

I Want More!

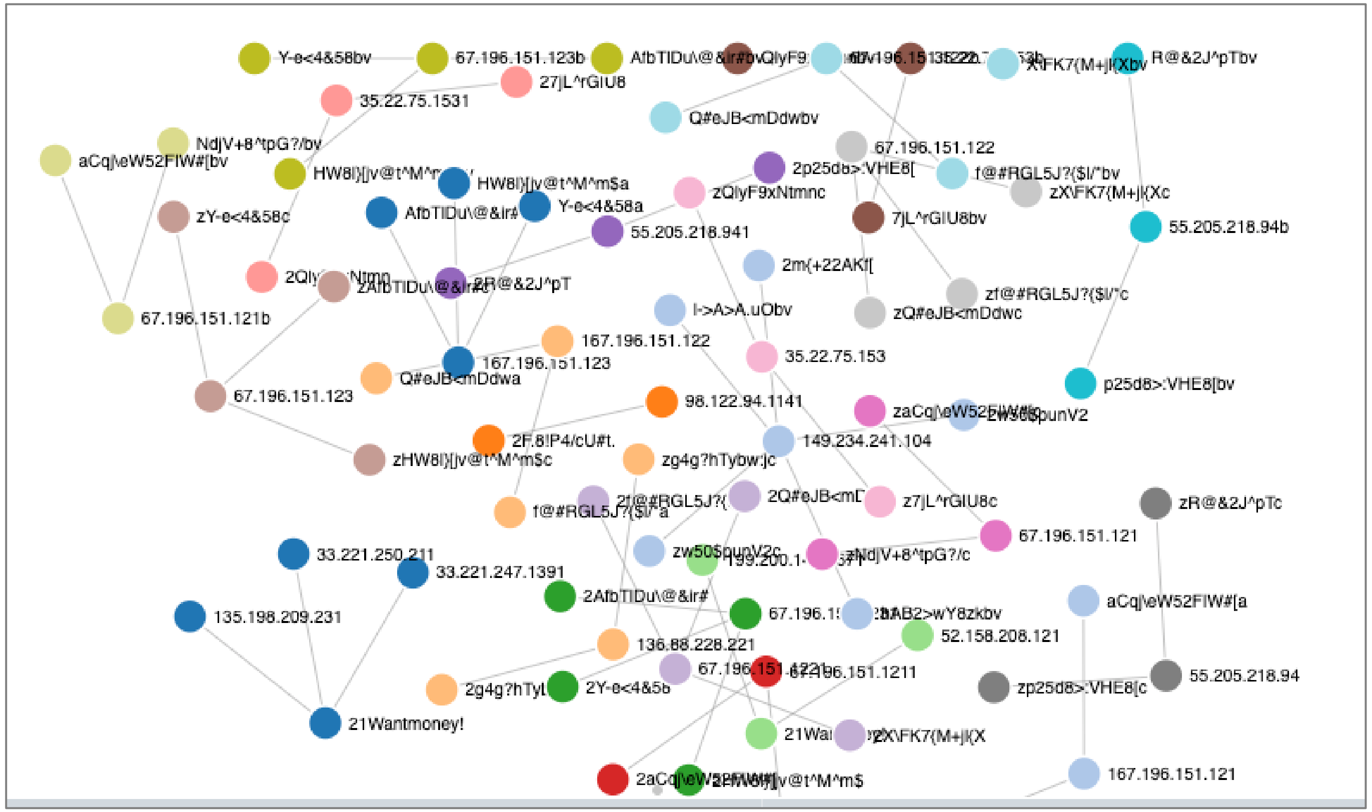
Field Limitations – multi-relationship



But Things Are Missing…

I Want More!

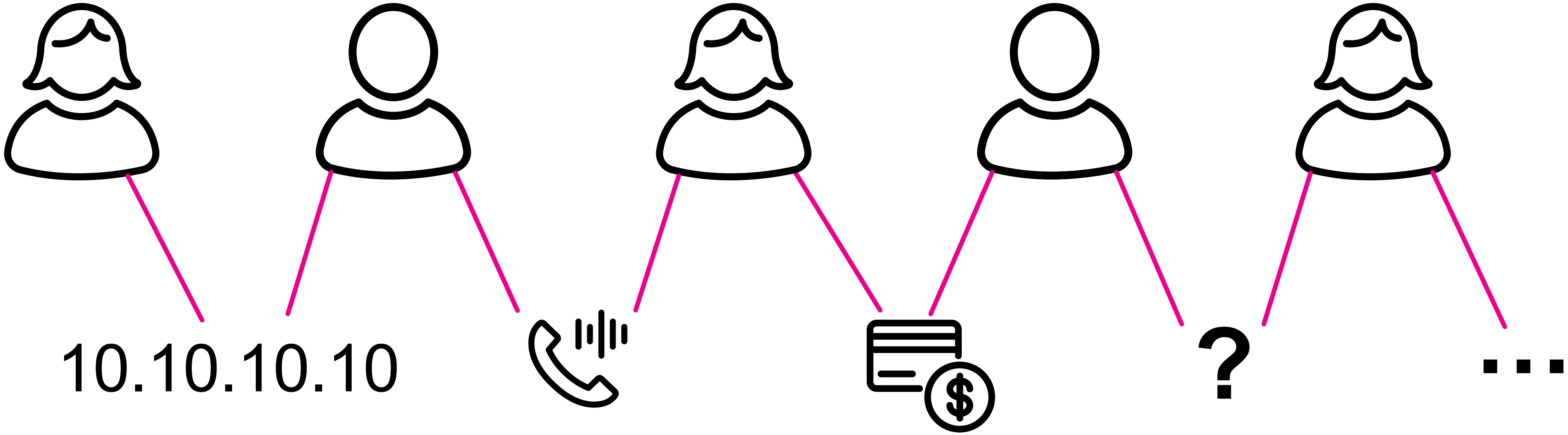
Circles and lines: Boring…..



But Things Are Missing…

I Want More!

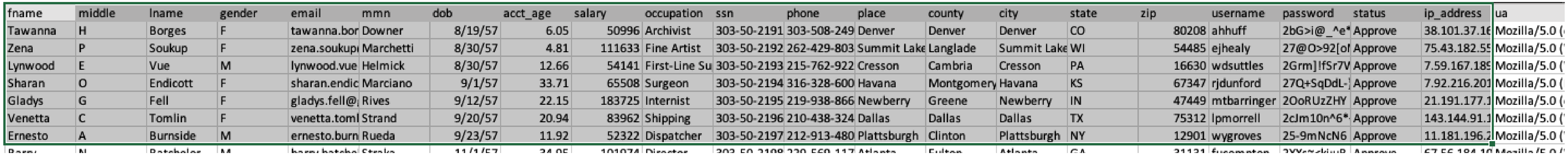
Extensibility and Discovery



Let’s Address These Issues!

Sample Data

15000+ events



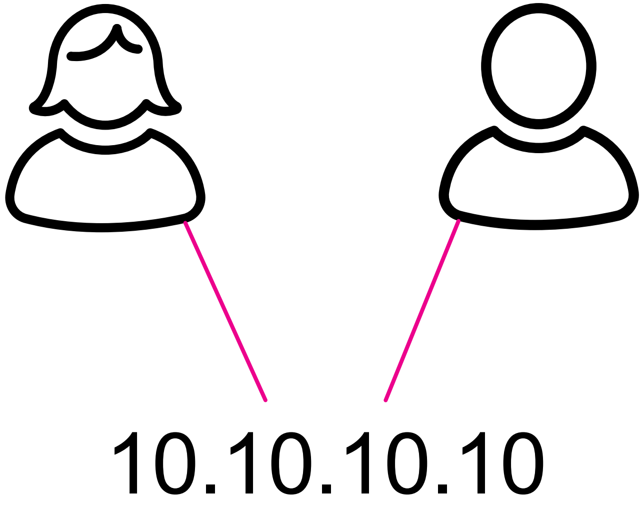
fname	middle	lname	gender	email	mmn	dob	acct_age	salary	occupation	ssn	phone	place	county	city	state	zip	username	password	status	ip_address	ua
Tawanna	H	Borges	F	tawanna.bor	Downer	8/19/57	6.05	50996	Archivist	303-50-2191	303-508-249	Denver	Denver	Denver	CO	80208	ahhuff	2bG>i@_^e*	Approve	38.101.37.16	Mozilla/5.0 (
Zena	P	Soukup	F	zena.soukup	Marchetti	8/30/57	4.81	111633	Fine Artist	303-50-2192	262-429-803	Summit Lake	Langlade	Summit Lake	WI	54485	ejhealy	27@O>92[ol	Approve	75.43.182.55	Mozilla/5.0 ('
Lynwood	E	Vue	M	lynwood.vue	Helmick	8/30/57	12.66	54141	First-Line Su	303-50-2193	215-762-922	Cresson	Cambria	Cresson	PA	16630	wdsuttles	2Grm]!fSr7V	Approve	7.59.167.189	Mozilla/5.0 ('
Sharan	O	Endicott	F	sharan.endic	Marciano	9/1/57	33.71	65508	Surgeon	303-50-2194	316-328-600	Havana	Montgomery	Havana	KS	67347	rjdunford	27Q+SqDdL-]	Approve	7.92.216.201	Mozilla/5.0 (
Gladys	G	Fell	F	gladys.fell@	Rives	9/12/57	22.15	183725	Internist	303-50-2195	219-938-866	Newberry	Greene	Newberry	IN	47449	mtbarringer	2OoRUzZHY	Approve	21.191.177.1	Mozilla/5.0 (
Venetta	C	Tomlin	F	venetta.toml	Strand	9/20/57	20.94	83962	Shipping	303-50-2196	210-438-324	Dallas	Dallas	Dallas	TX	75312	lpmorrell	2cJm10n^6*-	Approve	143.144.91.1	Mozilla/5.0 ('
Ernesto	A	Burnside	M	ernesto.burn	Rueda	9/23/57	11.92	52322	Dispatcher	303-50-2197	212-913-480	Plattsburgh	Clinton	Plattsburgh	NY	12901	wygroves	25-9mNcN6	Approve	11.181.196.2	Mozilla/5.0 ('
Barry	N	Batchelor	M	barry.batche	Straka	11/1/57	34.05	101074	Director	303-50-2198	229-560-117	Atlanta	Fulton	Atlanta	GA	31131	[illegible]	[illegible]	Approve	67.56.184.10	Mozilla/5.0 ('

Important fields

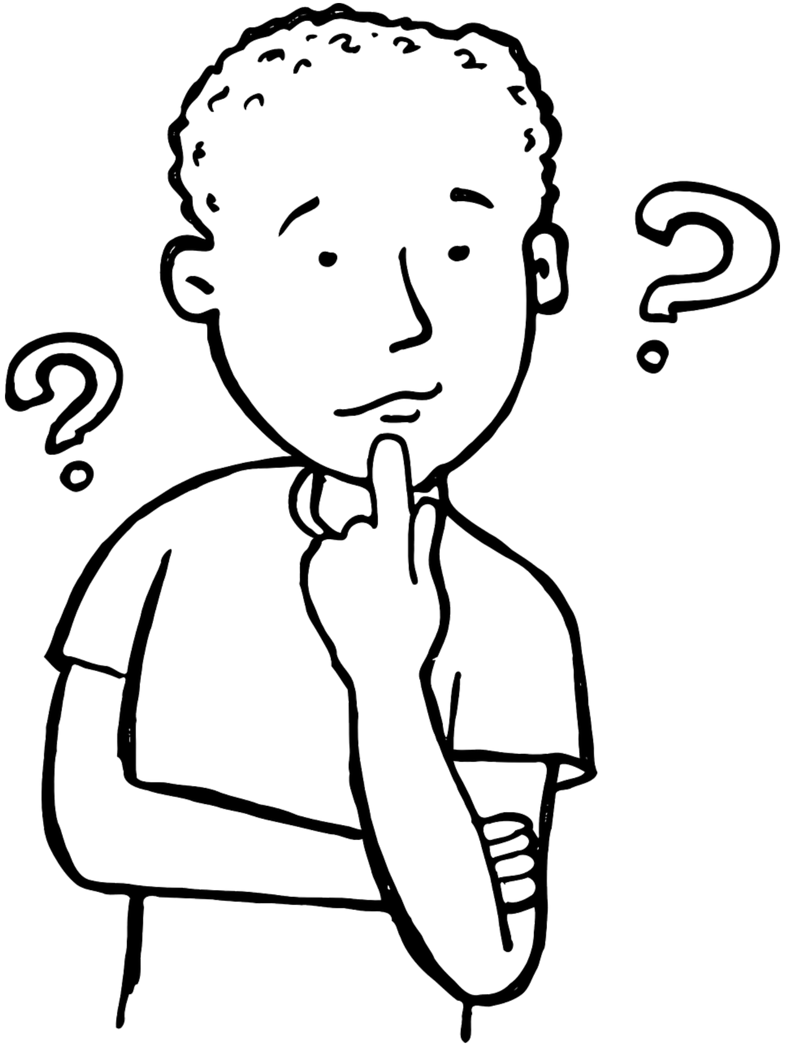
- Username (unique)
- Phone
- Password
- IP_address
- Destination account

What Is a Link?

Can it be this simple?

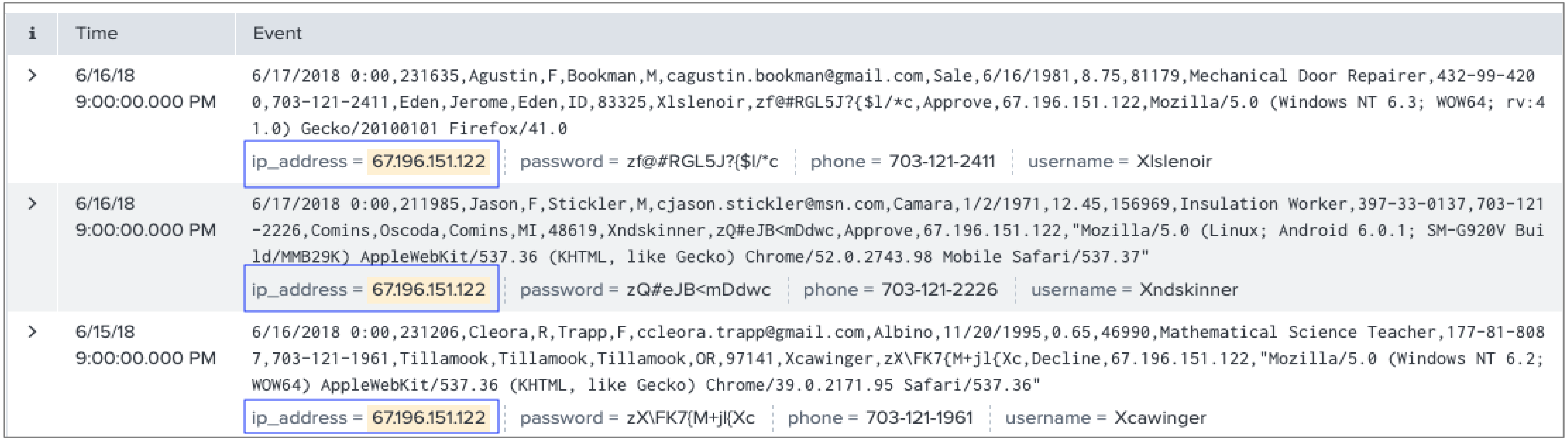


10.10.10.10



Duplicates

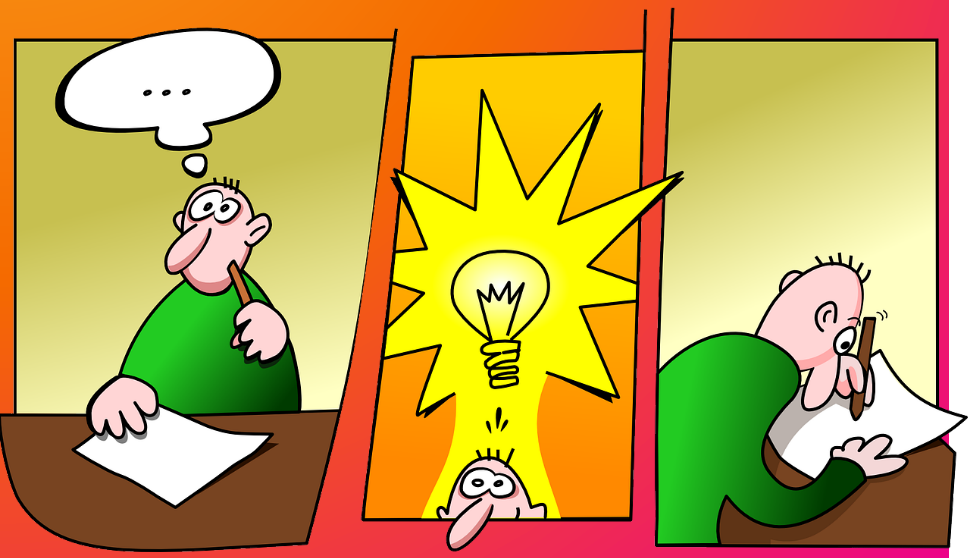
Splunk is great with duplicates



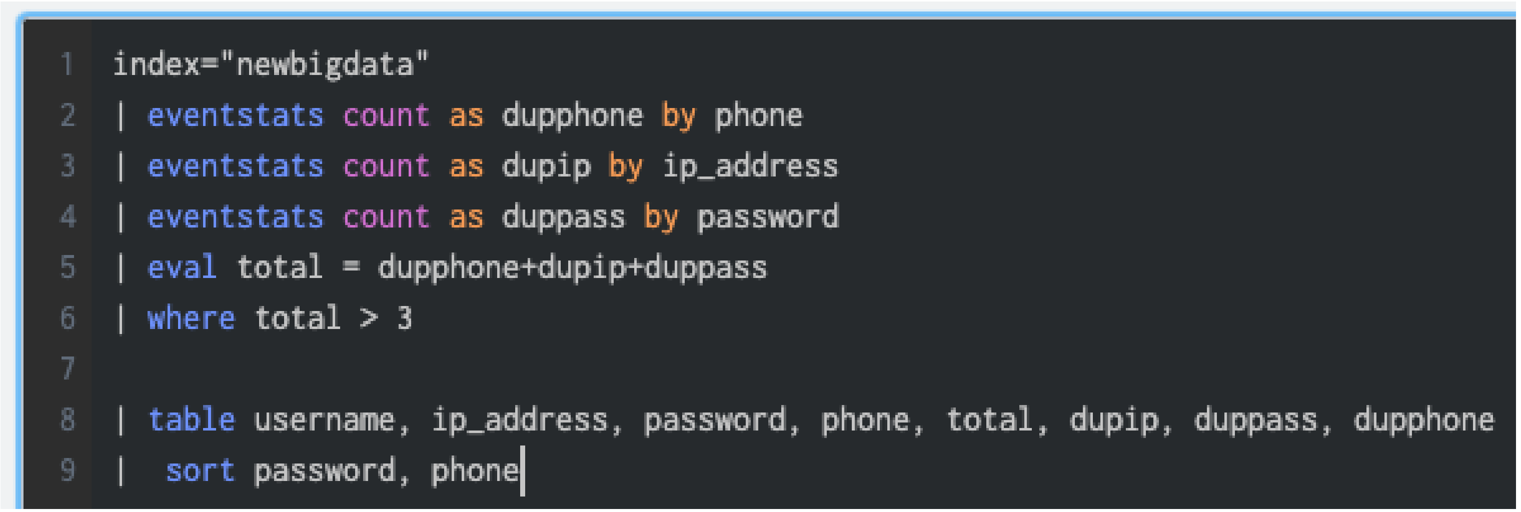
i	Time	Event
>	6/16/18 9:00:00.000 PM	6/17/2018 0:00,231635,Agustin,F,Bookman,M,cagustin.bookman@gmail.com,Sale,6/16/1981,8.75,81179,Mechanical Door Repairer,432-99-4200,703-121-2411,Eden,Jerome,Eden,ID,83325,Xlslenoir,zf@#RGL5J?{$l/*c,Approve,67.196.151.122,Mozilla/5.0 (Windows NT 6.3; WOW64; rv:41.0) Gecko/20100101 Firefox/41.0 ip_address = 67.196.151.122 ⁞ password = zf@#RGL5J?{$l/*c ⁞ phone = 703-121-2411 ⁞ username = Xlslenoir
>	6/16/18 9:00:00.000 PM	6/17/2018 0:00,211985,Jason,F,Stickler,M,cjason.stickler@msn.com,Camara,1/2/1971,12.45,156969,Insulation Worker,397-33-0137,703-121-2226,Comins,Oscoda,Comins,MI,48619,Xndskinner,zQ#eJB<mDdwc,Approve,67.196.151.122,"Mozilla/5.0 (Linux; Android 6.0.1; SM-G920V Build/MMB29K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.98 Mobile Safari/537.37" ip_address = 67.196.151.122 ⁞ password = zQ#eJB<mDdwc ⁞ phone = 703-121-2226 ⁞ username = Xndskinner
>	6/15/18 9:00:00.000 PM	6/16/2018 0:00,231206,Cleora,R,Trapp,F,ccleora.trapp@gmail.com,Albino,11/20/1995,0.65,46990,Mathematical Science Teacher,177-81-8087,703-121-1961,Tillamook,Tillamook,Tillamook,OR,97141,Xcawinger,zX\FK7{M+jl{Xc,Decline,67.196.151.122,"Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/39.0.2171.95 Safari/537.36" ip_address = 67.196.151.122 ⁞ password = zX\FK7{M+jl{Xc ⁞ phone = 703-121-1961 ⁞ username = Xcawinger

How do we detect, count and track duplicates?

Eureka!



Eventstats

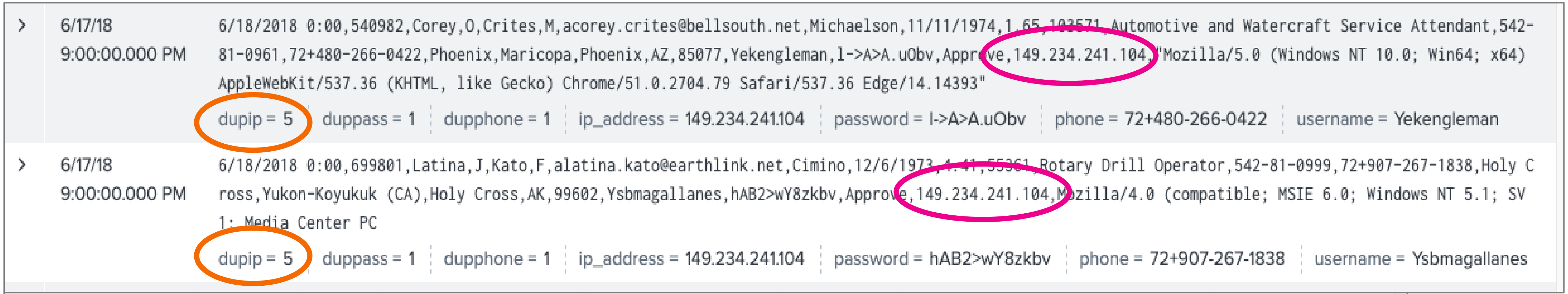


```
index="newbigdata"
| eventstats count as dupphone by phone
| eventstats count as dupip by ip_address
| eventstats count as duppass by password
| eval total = dupphone+dupip+duppass
| where total > 3

| table username, ip_address, password, phone, total, dupip, duppass, dupphone
|  sort password, phone
```

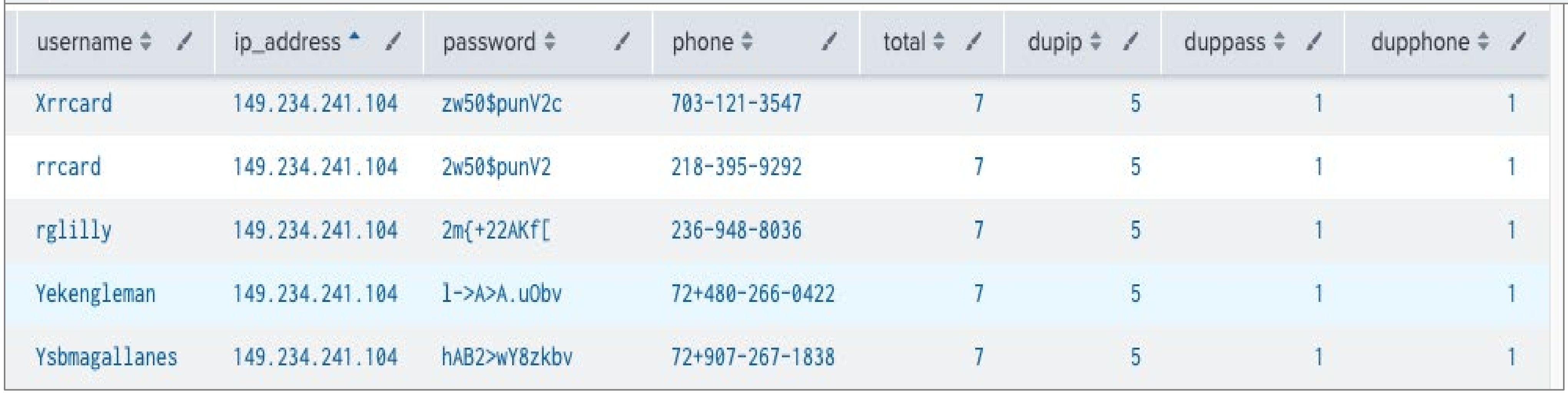
Generates summary statistics from fields in your events and saves those statistics in a new field.

SPL Results

| eventstats count as dupip by ip_address



```
> 6/17/18            6/18/2018 0:00,540982,Corey,O,Crites,M,acorey.crites@bellsouth.net,Michaelson,11/11/1974,1,65,103571,Automotive and Watercraft Service Attendant,542-
  9:00:00.000 PM     81-0961,72+480-266-0422,Phoenix,Maricopa,Phoenix,AZ,85077,Yekengleman,l->A>A.uObv,Approve,149.234.241.104,"Mozilla/5.0 (Windows NT 10.0; Win64; x64)
                     AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.79 Safari/537.36 Edge/14.14393"
                     dupip = 5 | duppass = 1 | dupphone = 1 | ip_address = 149.234.241.104 | password = l->A>A.uObv | phone = 72+480-266-0422 | username = Yekengleman

> 6/17/18            6/18/2018 0:00,699801,Latina,J,Kato,F,alatina.kato@earthlink.net,Cimino,12/6/1973,4,41,55361,Rotary Drill Operator,542-81-0999,72+907-267-1838,Holy C
  9:00:00.000 PM     ross,Yukon-Koyukuk (CA),Holy Cross,AK,99602,Ysbmagallanes,hAB2>wY8zkbv,Approve,149.234.241.104,Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV
                     1; Media Center PC
                     dupip = 5 | duppass = 1 | dupphone = 1 | ip_address = 149.234.241.104 | password = hAB2>wY8zkbv | phone = 72+907-267-1838 | username = Ysbmagallanes
```

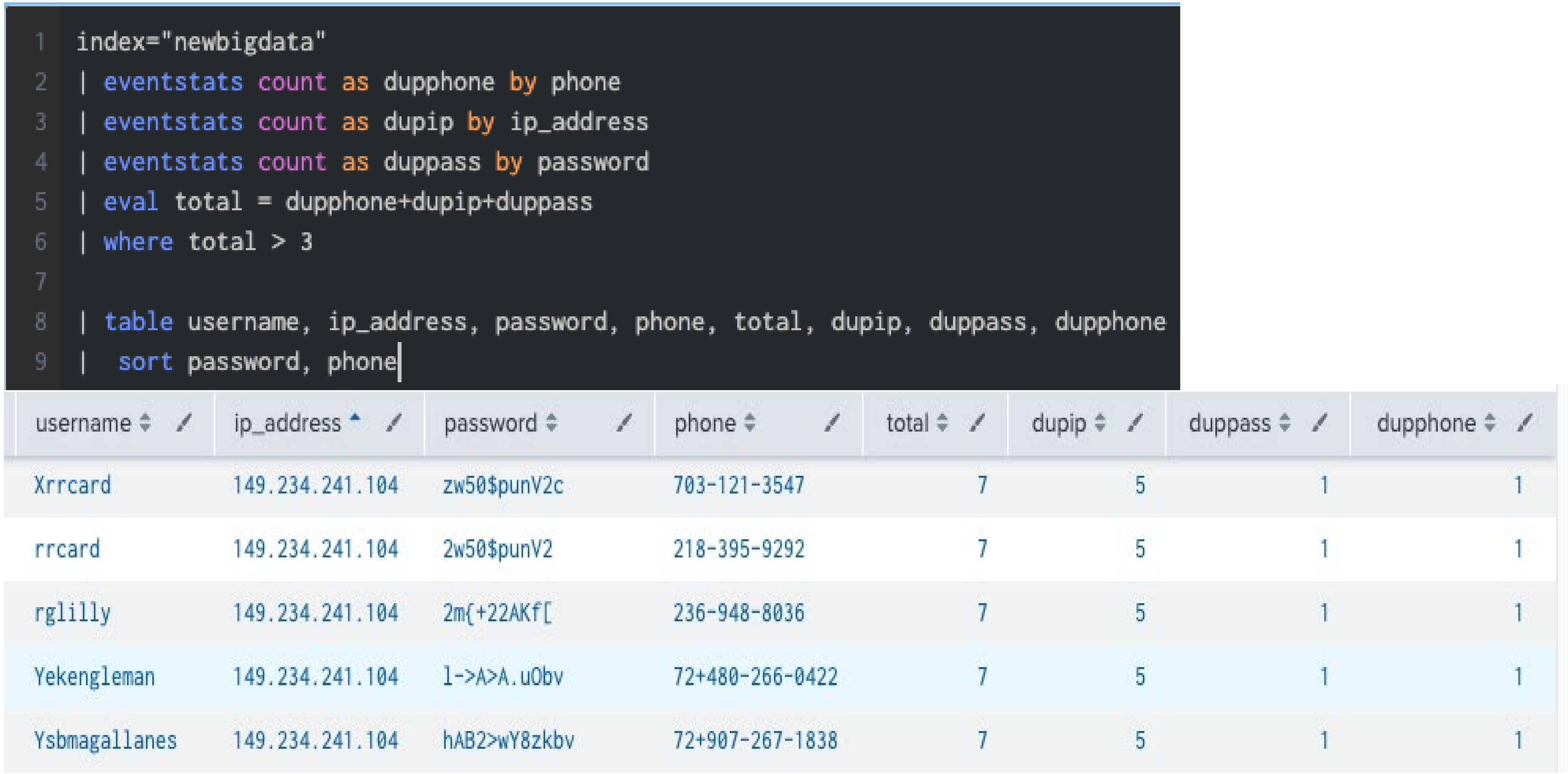


username	ip_address	password	phone	total	dupip	duppass	dupphone
Xrrcard	149.234.241.104	zw50$punV2c	703-121-3547	7	5	1	1
rrcard	149.234.241.104	2w50$punV2	218-395-9292	7	5	1	1
rglilly	149.234.241.104	2m{+22AKf[	236-948-8036	7	5	1	1
Yekengleman	149.234.241.104	l->A>A.uObv	72+480-266-0422	7	5	1	1
Ysbmagallanes	149.234.241.104	hAB2>wY8zkbv	72+907-267-1838	7	5	1	1

splunk> .conf20

SPL Results

| eventstats count as dupip by ip_address



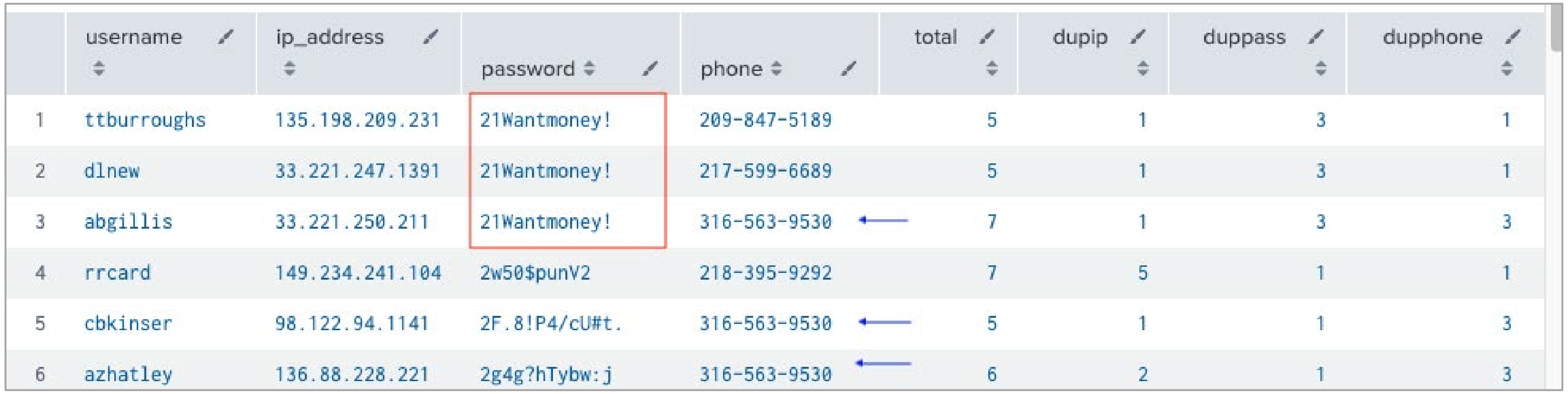
```
index="newbigdata"
| eventstats count as dupphone by phone
| eventstats count as dupip by ip_address
| eventstats count as duppass by password
| eval total = dupphone+dupip+duppass
| where total > 3

| table username, ip_address, password, phone, total, dupip, duppass, dupphone
|  sort password, phone
```

username	ip_address	password	phone	total	dupip	duppass	dupphone
Xrrcard	149.234.241.104	zw50$punV2c	703-121-3547	7	5	1	1
rrcard	149.234.241.104	2w50$punV2	218-395-9292	7	5	1	1
rglilly	149.234.241.104	2m{+22AKf[	236-948-8036	7	5	1	1
Yekengleman	149.234.241.104	l->A>A.uObv	72+480-266-0422	7	5	1	1
Ysbmagallanes	149.234.241.104	hAB2>wY8zkbv	72+907-267-1838	7	5	1	1

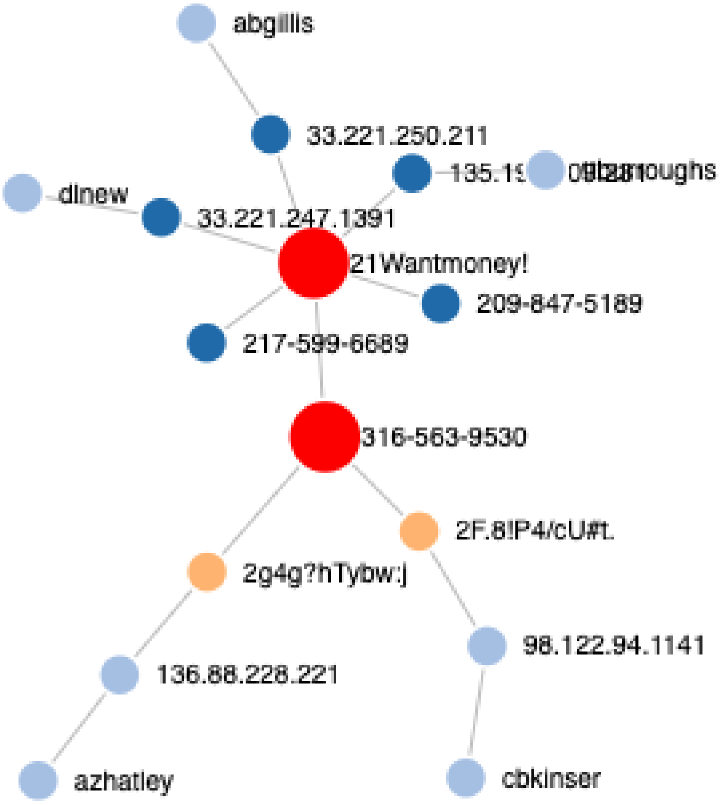
splunk> .conf20

Force Directed With “nodes”

Force Directed App for Splunk

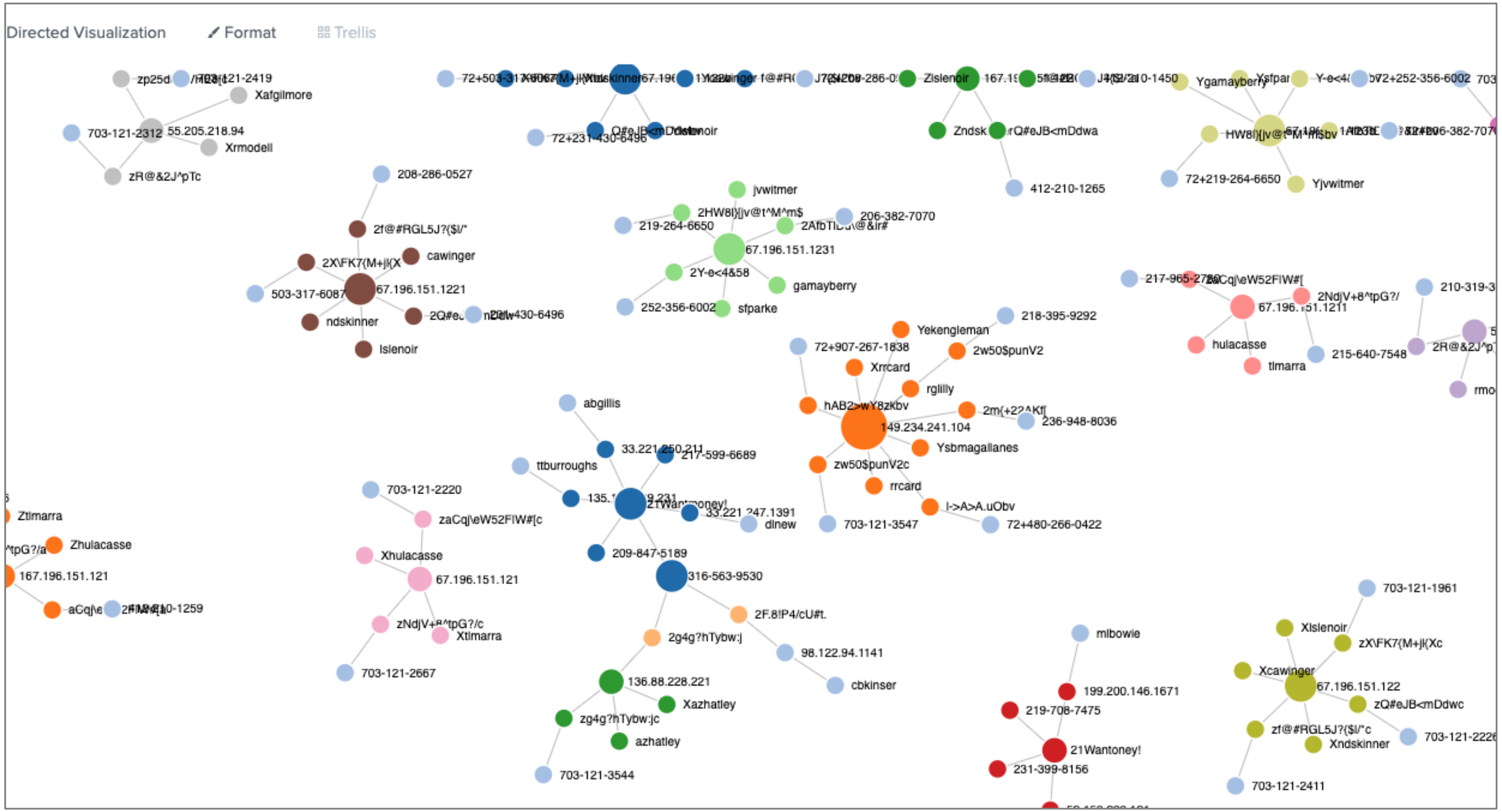


	username	ip_address	password	phone	total	dupip	duppass	dupphone
1	ttburroughs	135.198.209.231	21Wantmoney!	209-847-5189	5	1	3	1
2	dlnew	33.221.247.1391	21Wantmoney!	217-599-6689	5	1	3	1
3	abgillis	33.221.250.211	21Wantmoney!	316-563-9530 ←	7	1	3	3
4	rrcard	149.234.241.104	2w50$punV2	218-395-9292	7	5	1	1
5	cbkinser	98.122.94.1141	2F.8!P4/cU#t.	316-563-9530 ←	5	1	1	3
6	azhatley	136.88.228.221	2g4g?hTybw:j	316-563-9530 ←	6	2	1	3



That Was Good, but….

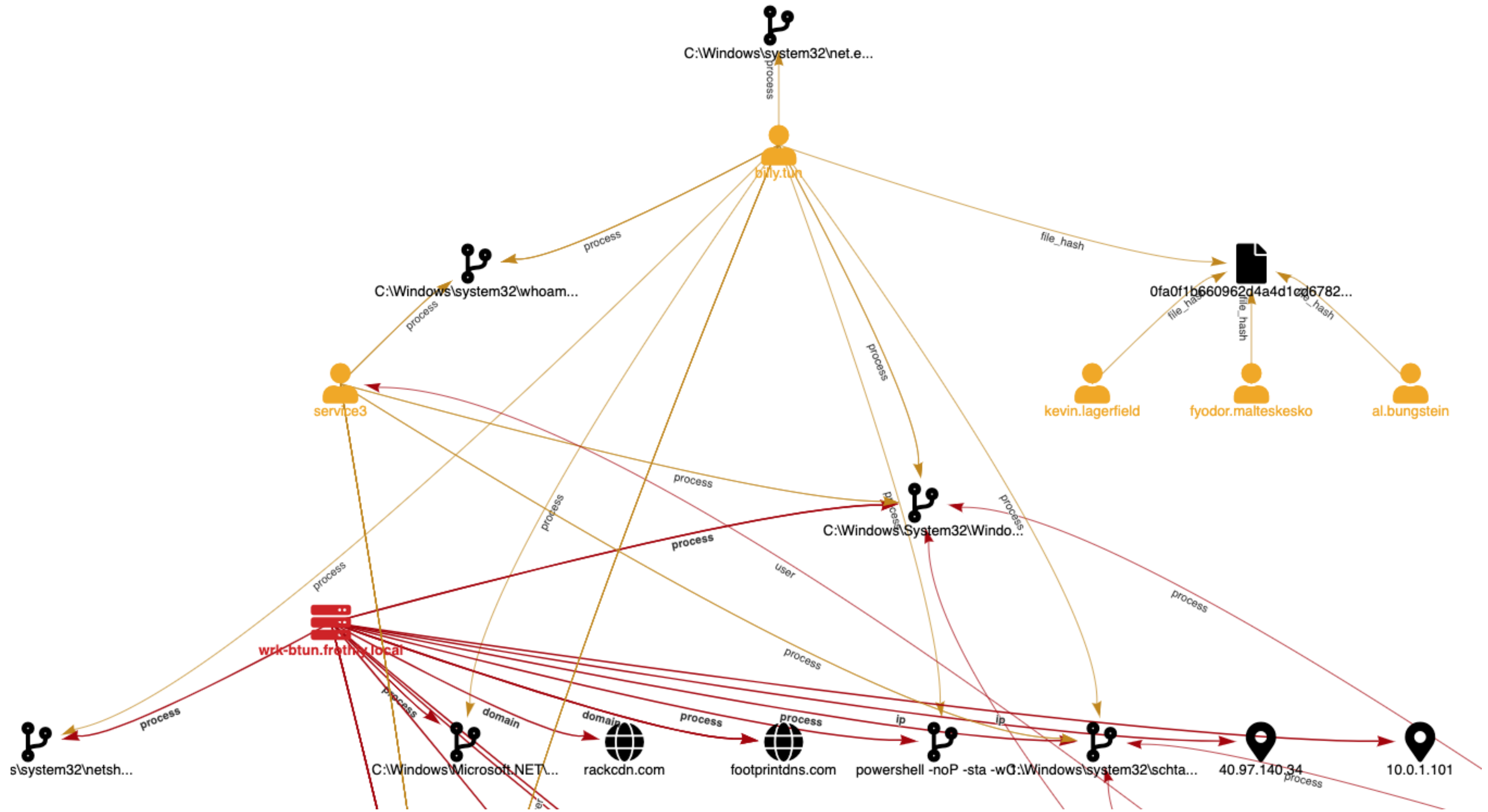
Formatting hard to control and CIRCLES!



What Were Others Doing?

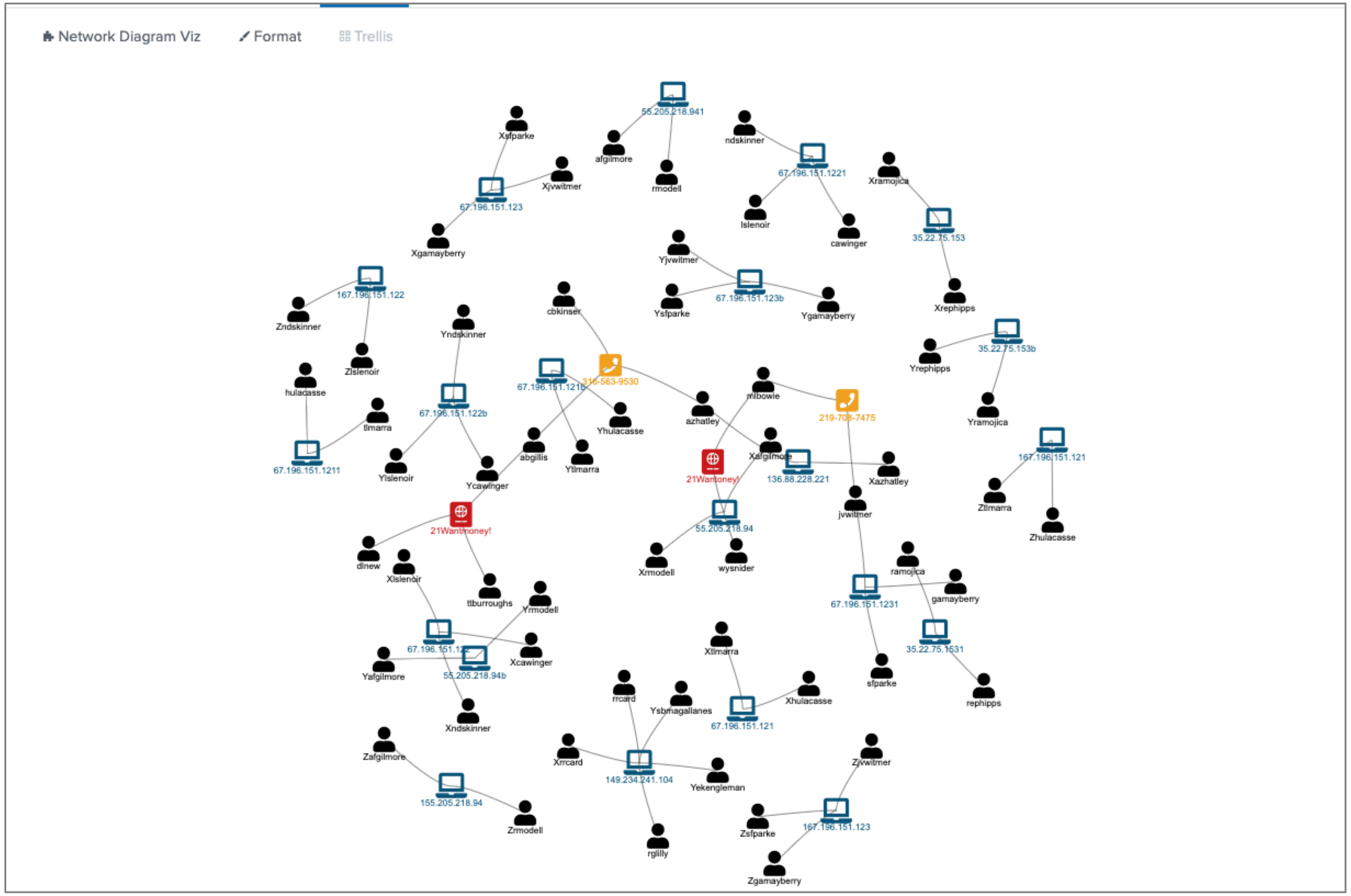
What Were Others Doing?

RBA! and “Network Diagram Viz” App



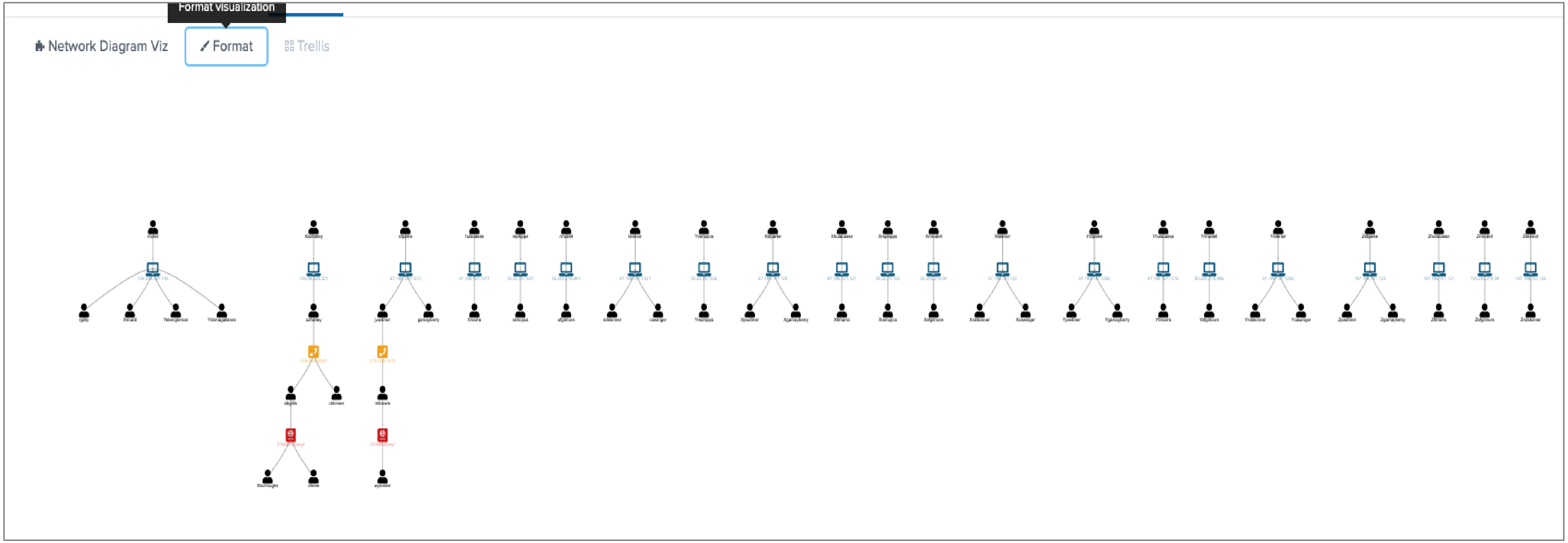
Bending the Tool to My Will!

Getting closer



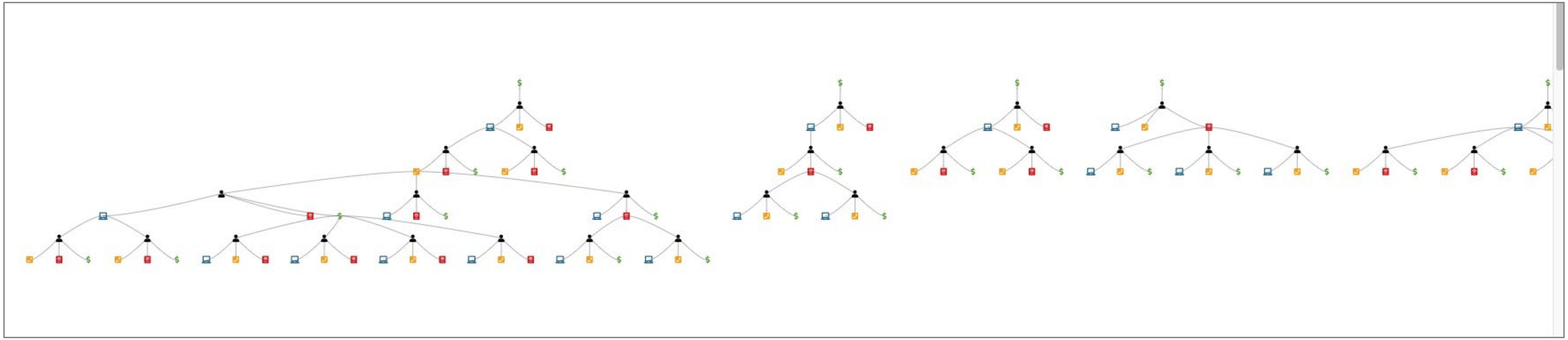
Making It Easier to Read

But still can be noisy



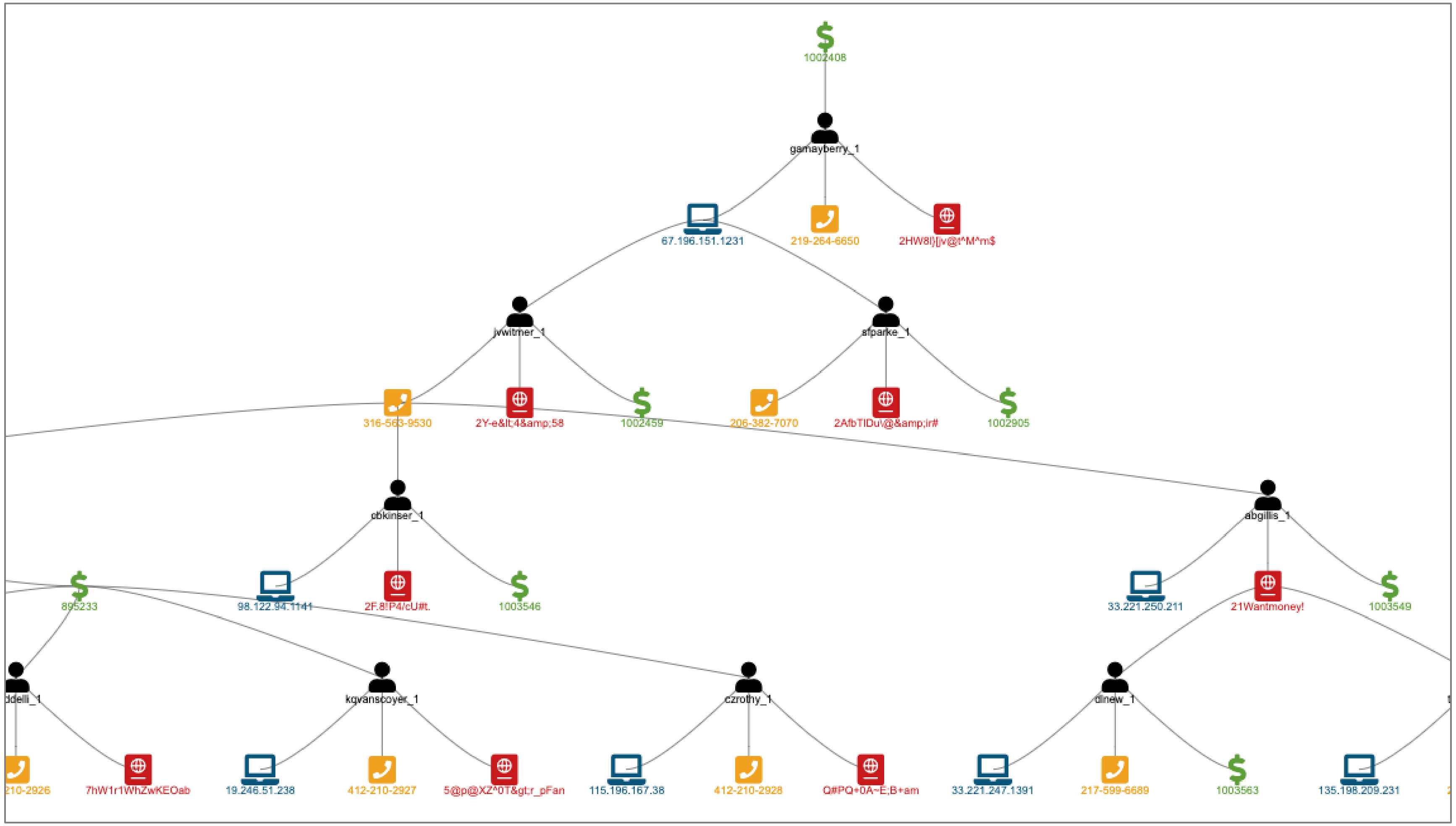
Size Might Matter….

How about 500K records?



Making Sense of It All

Zooming in



Considerations:

And other details:

Performance

- Eventstats is not instantaneous
- Additional time per command
- Good candidate for scheduled search

More SPL was used – see upcoming blog posts

- How I included single entities in larger diagrams
- How I made Network Diagram Viz show node icons for all

Network Diagram Viz app supports drill downs and more not shown

What If… I Don't Want to Do Data Reduction

Or, I don't know what I am looking for?

Gleb Esman

Staff Security Strategist

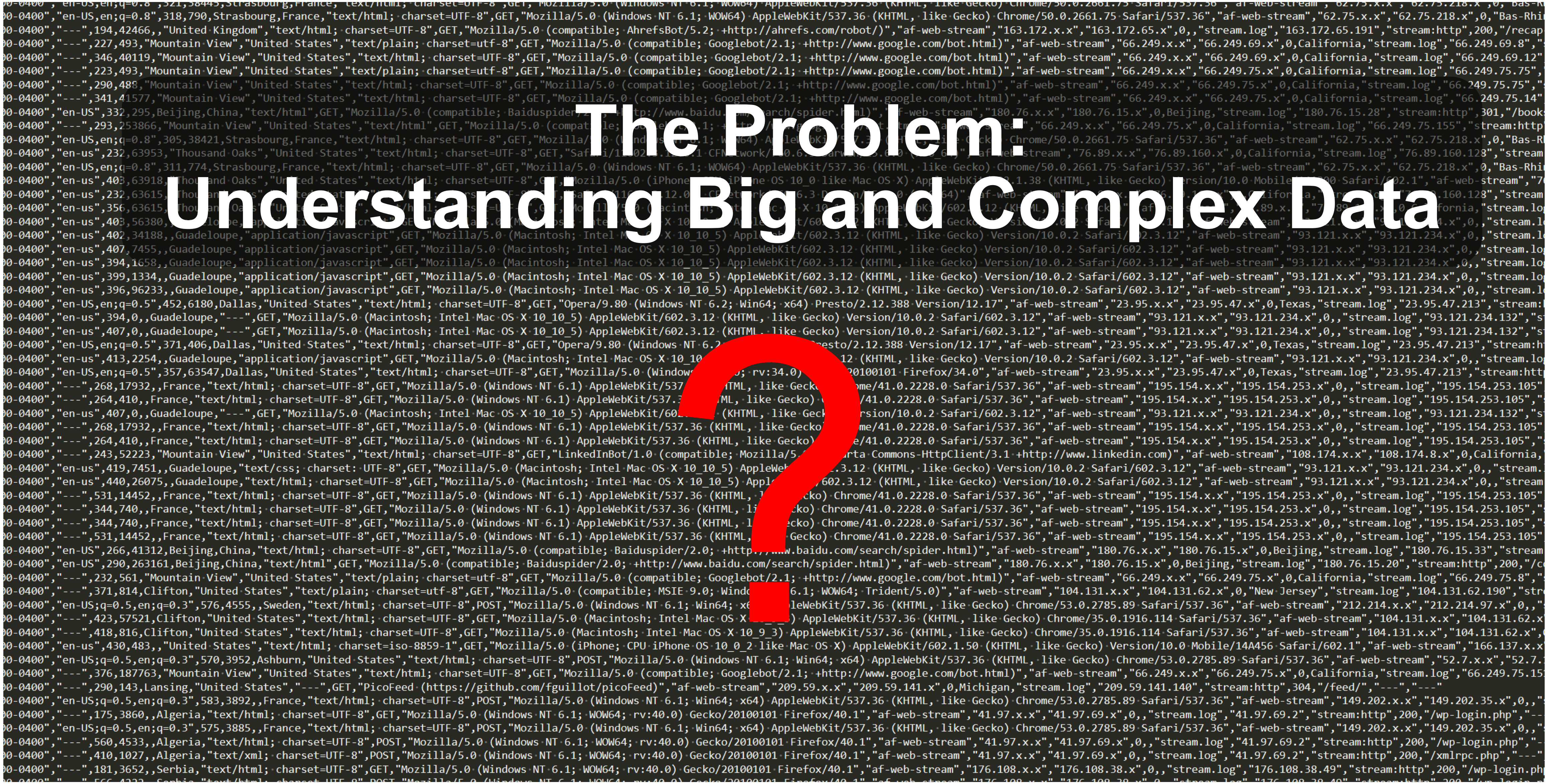
- IBM T.J.Watson Research
- Payment processing and DLP technologies
- Morgan Stanley
- Staff Security Strategist @ Splunk, 5 yrs

- Enjoying Pro photography
- Based in Las Vegas, NV, USA

The Most Important Key Element in Fraud Analytics

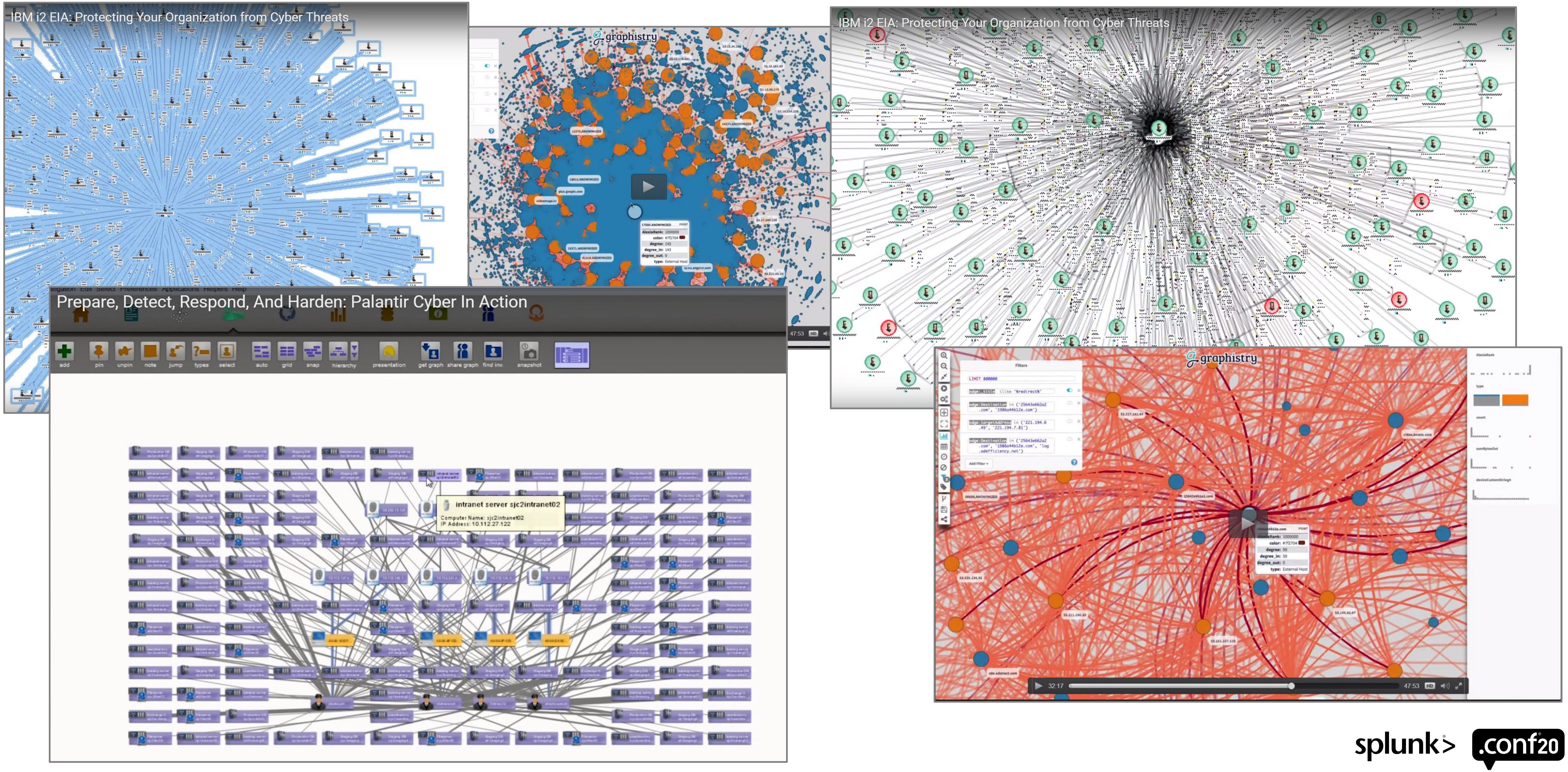
Business User

The Problem: Understanding Big and Complex Data



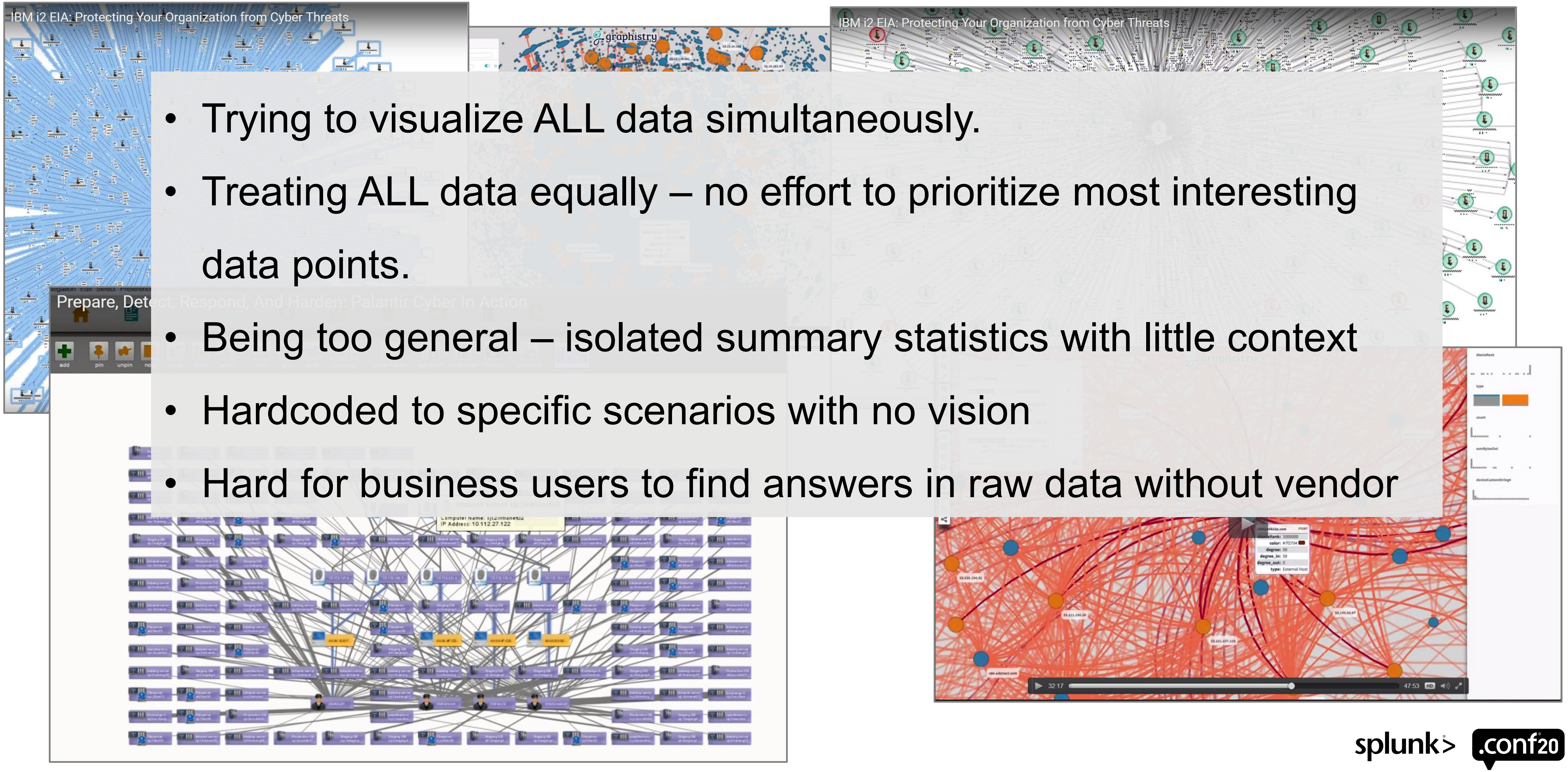
```
0-0400","en-US,en;q=0.8",318,790,Strasbourg,France,"text/html; charset=UTF-8",GET,"Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.75 Safari/537.36","af-web-stream","62.75.x.x","62.75.218.x",0,"Bas-Rhi
0-0400","---",194,42466,,"United Kingdom","text/html; charset=UTF-8",GET,"Mozilla/5.0 (compatible; AhrefsBot/5.2; +http://ahrefs.com/robot/)","af-web-stream","163.172.x.x","163.172.65.x",0,,"stream.log","163.172.65.191","stream:http",200,"/recap
0-0400","---",227,493,"Mountain View","United States","text/plain; charset=utf-8",GET,"Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)","af-web-stream","66.249.x.x","66.249.69.x",0,California,"stream.log","66.249.69.8","
0-0400","---",346,40119,"Mountain View","United States","text/html; charset=UTF-8",GET,"Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)","af-web-stream","66.249.x.x","66.249.69.x",0,California,"stream.log","66.249.69.12"
0-0400","---",223,493,"Mountain View","United States","text/plain; charset=utf-8",GET,"Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)","af-web-stream","66.249.x.x","66.249.75.x",0,California,"stream.log","66.249.75.75",
0-0400","---",290,488,"Mountain View","United States","text/html; charset=UTF-8",GET,"Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)","af-web-stream","66.249.x.x","66.249.75.x",0,California,"stream.log","66.249.75.75",
0-0400","---",341,41577,"Mountain View","United States","text/html; charset=UTF-8",GET,"Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)","af-web-stream","66.249.x.x","66.249.75.x",0,California,"stream.log","66.249.75.14"
0-0400","en-US",332,295,Beijing,China,"text/html",GET,"Mozilla/5.0 (compatible; Baiduspider[illegible]tp://www.baidu.[illegible]arch/spider.[illegible]ml)","af-web-stream","180.76.x.x","180.76.15.x",0,Beijing,"stream.log","180.76.15.28","stream:http",301,"/book
0-0400","---",293,253866,"Mountain View","United States","text/html",GET,"Mozilla/5.0 (compat[illegible]","66.249.x.x","66.249.75.x",0,California,"stream.log","66.249.75.155","stream:http
0-0400","en-US,en;q=0.8",305,38421,Strasbourg,France,"text/html; charset=UTF-8",GET,"Mozilla/[illegible]Chrome/50.0.2661.75 Safari/537.36","af-web-stream","62.75.x.x","62.75.218.x",0,"Bas-R
0-0400","en-us",232,63953,"Thousand Oaks","United States","text/html; charset=UTF-8",GET,"Saf[illegible]","af-web-stream","76.89.x.x","76.89.160.x",0,California,"stream.log","76.89.160.128","stream
0-0400","en-US,en;q=0.8",311,774,Strasbourg,France,"text/html; charset=UTF-8",GET,"Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.75 Safari/537.36","af-web-stream","62.75.x.x","62.75.218.x",0,"Bas-Rhi
0-0400","en-us",403,63918,[illegible]ted States","text/html; charset=UTF-8",[illegible]ozilla/5.0 (iPhone[illegible]ne OS 10_0 like Mac OS X) AppleWebKi[illegible]1.38 (KHTML, like Gecko) [illegible]rsion/10.0 Mobile[illegible] Safari/[illegible]2.1","af-web-stream","7
0-0400","en-us",232,63615,[illegible]160.128","stream
0-0400","en-us",356,63615,[illegible]"stream.lo
0-0400","en-us",403,56380,[illegible]"stream.l
0-0400","en-us",402,34188,,Guadeloupe,"application/javascript",GET,"Mozilla/5.0 (Macintosh; Intel [illegible] X 10_10_5) Appl[illegible]t/602.3.12 (KHTML, like Gecko) Version/10.0.2 Safari/[illegible]2.3.12","af-web-stream","93.121.x.x","93.121.234.x",0,,"stream.l
0-0400","en-us",407,7455,,Guadeloupe,"application/javascript",GET,"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/602.3.12 (KHTML, like Gecko) Version/10.0.2 Safari/602.3.12","af-web-stream","93.121.x.x","93.121.234.x",0,,"stream.lo
0-0400","en-us",394,1658,,Guadeloupe,"application/javascript",GET,"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/602.3.12 (KHTML, like Gecko) Version/10.0.2 Safari/602.3.12","af-web-stream","93.121.x.x","93.121.234.x",0,,"stream.lo
0-0400","en-us",399,1334,,Guadeloupe,"application/javascript",GET,"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/602.3.12 (KHTML, like Gecko) Version/10.0.2 Safari/602.3.12","af-web-stream","93.121.x.x","93.121.234.x",0,,"stream.lo
0-0400","en-us",396,96233,,Guadeloupe,"application/javascript",GET,"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/602.3.12 (KHTML, like Gecko) Version/10.0.2 Safari/602.3.12","af-web-stream","93.121.x.x","93.121.234.x",0,,"stream.l
0-0400","en-US,en;q=0.5",452,6180,Dallas,"United States","text/html; charset=UTF-8",GET,"Opera/9.80 (Windows NT 6.2; Win64; x64) Presto/2.12.388 Version/12.17","af-web-stream","23.95.x.x","23.95.47.x",0,Texas,"stream.log","23.95.47.213","stream:
0-0400","en-us",394,0,,Guadeloupe,"---",GET,"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/602.3.12 (KHTML, like Gecko) Version/10.0.2 Safari/602.3.12","af-web-stream","93.121.x.x","93.121.234.x",0,,"stream.log","93.121.234.132","s
0-0400","en-us",407,0,,Guadeloupe,"---",GET,"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/602.3.12 (KHTML, like Gecko) Version/10.0.2 Safari/602.3.12","af-web-stream","93.121.x.x","93.121.234.x",0,,"stream.log","93.121.234.132","s
0-0400","en-US,en;q=0.5",371,406,Dallas,"United States","text/html; charset=UTF-8",GET,"Opera/9.80 (Windows NT 6.2[illegible]resto/2.12.388 Version/12.17","af-web-stream","23.95.x.x","23.95.47.x",0,Texas,"stream.log","23.95.47.213","stream:h
0-0400","en-us",413,2254,,Guadeloupe,"application/javascript",GET,"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10[illegible]12 (KHTML, like Gecko) Version/10.0.2 Safari/602.3.12","af-web-stream","93.121.x.x","93.121.234.x",0,,"stream.lo
0-0400","en-US,en;q=0.5",357,63547,Dallas,"United States","text/html; charset=UTF-8",GET,"Mozilla/5.0 (Window[illegible]; rv:34.0) [illegible]20100101 Firefox/34.0","af-web-stream","23.95.x.x","23.95.47.x",0,Texas,"stream.log","23.95.47.213","stream:htt
0-0400","---",268,17932,,France,"text/html; charset=UTF-8",GET,"Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537[illegible]TML, like Geck[illegible]ome/41.0.2228.0 Safari/537.36","af-web-stream","195.154.x.x","195.154.253.x",0,,"stream.log","195.154.253.105"
0-0400","---",264,410,,France,"text/html; charset=UTF-8",GET,"Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.[illegible]ML, like Gecko) [illegible]/41.0.2228.0 Safari/537.36","af-web-stream","195.154.x.x","195.154.253.x",0,,"stream.log","195.154.253.105","
0-0400","en-us",407,0,,Guadeloupe,"---",GET,"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/60[illegible] (KHTML, like Geck[illegible]rsion/10.0.2 Safari/602.3.12","af-web-stream","93.121.x.x","93.121.234.x",0,,"stream.log","93.121.234.132","s
0-0400","---",268,17932,,France,"text/html; charset=UTF-8",GET,"Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko[illegible]me/41.0.2228.0 Safari/537.36","af-web-stream","195.154.x.x","195.154.253.x",0,,"stream.log","195.154.253.105"
0-0400","---",264,410,,France,"text/html; charset=UTF-8",GET,"Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko)[illegible]e/41.0.2228.0 Safari/537.36","af-web-stream","195.154.x.x","195.154.253.x",0,,"stream.log","195.154.253.105","
0-0400","---",243,52223,"Mountain View","United States","text/html; charset=UTF-8",GET,"LinkedInBot/1.0 (compatible; Mozilla/5.[illegible]rta Commons-HttpClient/3.1 +http://www.linkedin.com)","af-web-stream","108.174.x.x","108.174.8.x",0,California,
0-0400","en-us",419,7451,,Guadeloupe,"text/css; charset: UTF-8",GET,"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWe[illegible].3.12 (KHTML, like Gecko) Version/10.0.2 Safari/602.3.12","af-web-stream","93.121.x.x","93.121.234.x",0,,"stream.
0-0400","en-us",440,26075,,Guadeloupe,"text/html; charset=UTF-8",GET,"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) Appl[illegible]602.3.12 (KHTML, like Gecko) Version/10.0.2 Safari/602.3.12","af-web-stream","93.121.x.x","93.121.234.x",0,,"stream
0-0400","---",531,14452,,France,"text/html; charset=UTF-8",GET,"Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, l[illegible]cko) Chrome/41.0.2228.0 Safari/537.36","af-web-stream","195.154.x.x","195.154.253.x",0,,"stream.log","195.154.253.105"
0-0400","---",344,740,,France,"text/html; charset=UTF-8",GET,"Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, li[illegible]cko) Chrome/41.0.2228.0 Safari/537.36","af-web-stream","195.154.x.x","195.154.253.x",0,,"stream.log","195.154.253.105","
0-0400","---",344,740,,France,"text/html; charset=UTF-8",GET,"Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, li[illegible]cko) Chrome/41.0.2228.0 Safari/537.36","af-web-stream","195.154.x.x","195.154.253.x",0,,"stream.log","195.154.253.105","
0-0400","---",531,14452,,France,"text/html; charset=UTF-8",GET,"Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML,[illegible] Gecko) Chrome/41.0.2228.0 Safari/537.36","af-web-stream","195.154.x.x","195.154.253.x",0,,"stream.log","195.154.253.105"
0-0400","en-US",266,41312,Beijing,China,"text/html; charset=UTF-8",GET,"Mozilla/5.0 (compatible; Baiduspider/2.0; +http[illegible]ww.baidu.com/search/spider.html)","af-web-stream","180.76.x.x","180.76.15.x",0,Beijing,"stream.log","180.76.15.33","stream
0-0400","en-US",290,263161,Beijing,China,"text/html",GET,"Mozilla/5.0 (compatible; Baiduspider/2.0; +http://www.baidu.com/search/spider.html)","af-web-stream","180.76.x.x","180.76.15.x",0,Beijing,"stream.log","180.76.15.20","stream:http",200,"/c
0-0400","---",232,561,"Mountain View","United States","text/plain; charset=utf-8",GET,"Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)","af-web-stream","66.249.x.x","66.249.75.x",0,California,"stream.log","66.249.75.8",
0-0400","---",371,814,Clifton,"United States","text/plain; charset=utf-8",GET,"Mozilla/5.0 (compatible; MSIE 9.0; Windo[illegible]6.1; WOW64; Trident/5.0)","af-web-stream","104.131.x.x","104.131.62.x",0,"New Jersey","stream.log","104.131.62.190","str
0-0400","en-US;q=0.5,en;q=0.3",576,4555,,Sweden,"text/html; charset=UTF-8",POST,"Mozilla/5.0 (Windows NT 6.1; Win64; x6[illegible]leWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.89 Safari/537.36","af-web-stream","212.214.x.x","212.214.97.x",0,,"
0-0400","---",423,57521,Clifton,"United States","text/html; charset=UTF-8",GET,"Mozilla/5.0 (Macintosh; Intel Mac OS X[illegible]) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/35.0.1916.114 Safari/537.36","af-web-stream","104.131.x.x","104.131.62.x
0-0400","---",418,816,Clifton,"United States","text/html; charset=UTF-8",GET,"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/35.0.1916.114 Safari/537.36","af-web-stream","104.131.x.x","104.131.62.x",
0-0400","en-us",430,483,,"United States","text/html; charset=iso-8859-1",GET,"Mozilla/5.0 (iPhone; CPU iPhone OS 10_0_2 like Mac OS X) AppleWebKit/602.1.50 (KHTML, like Gecko) Version/10.0 Mobile/14A456 Safari/602.1","af-web-stream","166.137.x.x
0-0400","en-US;q=0.5,en;q=0.3",570,3952,Ashburn,"United States","text/html; charset=UTF-8",POST,"Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.89 Safari/537.36","af-web-stream","52.7.x.x","52.7.
0-0400","---",376,187763,"Mountain View","United States","text/html; charset=UTF-8",GET,"Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)","af-web-stream","66.249.x.x","66.249.75.x",0,California,"stream.log","66.249.75.15
0-0400","---",290,143,Lansing,"United States","---",GET,"PicoFeed (https://github.com/fguillot/picoFeed)","af-web-stream","209.59.x.x","209.59.141.x",0,Michigan,"stream.log","209.59.141.140","stream:http",304,"/feed/","---","---
0-0400","en-US;q=0.5,en;q=0.3",583,3892,,France,"text/html; charset=UTF-8",POST,"Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.89 Safari/537.36","af-web-stream","149.202.x.x","149.202.35.x",0,,"
0-0400","---",175,3860,,Algeria,"text/html; charset=UTF-8",GET,"Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.1","af-web-stream","41.97.x.x","41.97.69.x",0,,"stream.log","41.97.69.2","stream:http",200,"/wp-login.php","--
0-0400","en-US;q=0.5,en;q=0.3",575,3885,,France,"text/html; charset=UTF-8",POST,"Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.89 Safari/537.36","af-web-stream","149.202.x.x","149.202.35.x",0,,"
0-0400","---",560,4533,,Algeria,"text/html; charset=UTF-8",POST,"Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.1","af-web-stream","41.97.x.x","41.97.69.x",0,,"stream.log","41.97.69.2","stream:http",200,"/wp-login.php","-
0-0400","---",410,1027,,Algeria,"text/xml; charset=UTF-8",POST,"Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.1","af-web-stream","41.97.x.x","41.97.69.x",0,,"stream.log","41.97.69.2","stream:http",200,"/xmlrpc.php","---
0-0400","---",181,3652,,Serbia,"text/html; charset=UTF-8",GET,"Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.1","af-web-stream","176.108.x.x","176.108.38.x",0,,"stream.log","176.108.38.49","stream:http",200,"/wp-login.ph
```

Real World Data Visualization Examples … *FAIL*


IBM i2 EIA: Protecting Your Organization from Cyber Threats
graphistry
IBM i2 EIA: Protecting Your Organization from Cyber Threats
Prepare, Detect, Respond, And Harden: Palantir Cyber In Action
add
pin
unpin
note
jump
types
select
auto
grid
snap
hierarchy
presentation
get graph
share graph
find inv.
snapshot
graphistry
Filters
32:17
47:53
HD

intranet server sjc2intranet02
Computer Name: sjc2intranet02
IP Address: 10.112.27.122

Non-Actionable Results Syndrome. *Why?*


IBM i2 EIA: Protecting Your Organization from Cyber Threats
graphistry
IBM i2 EIA: Protecting Your Organization from Cyber Threats
Prepare, Detect, Respond, And Harden: Palantir Cyber In Action
add
pin
unpin

- Trying to visualize ALL data simultaneously.
- Treating ALL data equally – no effort to prioritize most interesting data points.
- Being too general – isolated summary statistics with little context
- Hardcoded to specific scenarios with no vision
- Hard for business users to find answers in raw data without vendor

How to Detect Fraud in Data?
Warning Signs, AnomaLIES and Red Flags:

Quantity and Frequency – too many (logins per time, transfers, connections, password changes, errors), OR too small (expected behavior is not observed)

Rarity – too unusual (never seen before names, unmatched forensics, strange devices and user agents, rare ports, unusual requests, unusual combinations)

Velocity / Relationship – 1-to-many where 1-to-1 is expected

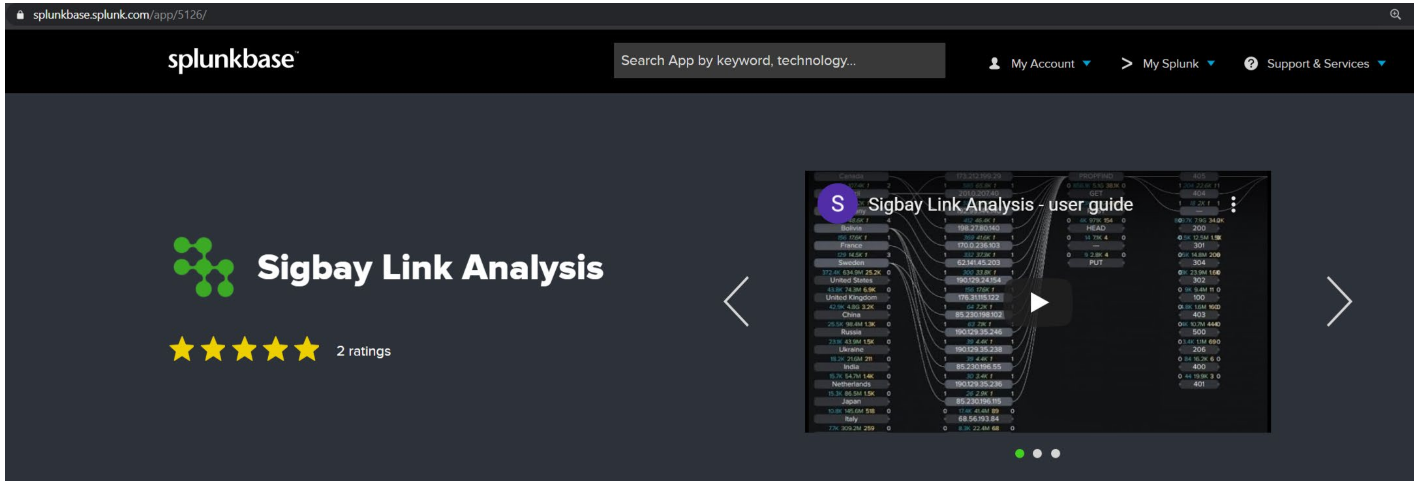
- Multiple IP's or multiple Geo sources accessing the same user account
- Single IP hitting multiple account
- Same phone/address shared by multiple customers/users
- Logins to same account from multiple geo locations

```
| tstats | stats | streamstats | eventstats | dc | values | avg | stdev | top | rare
| sum | max | regex |
```

Links and Relationships Analysis

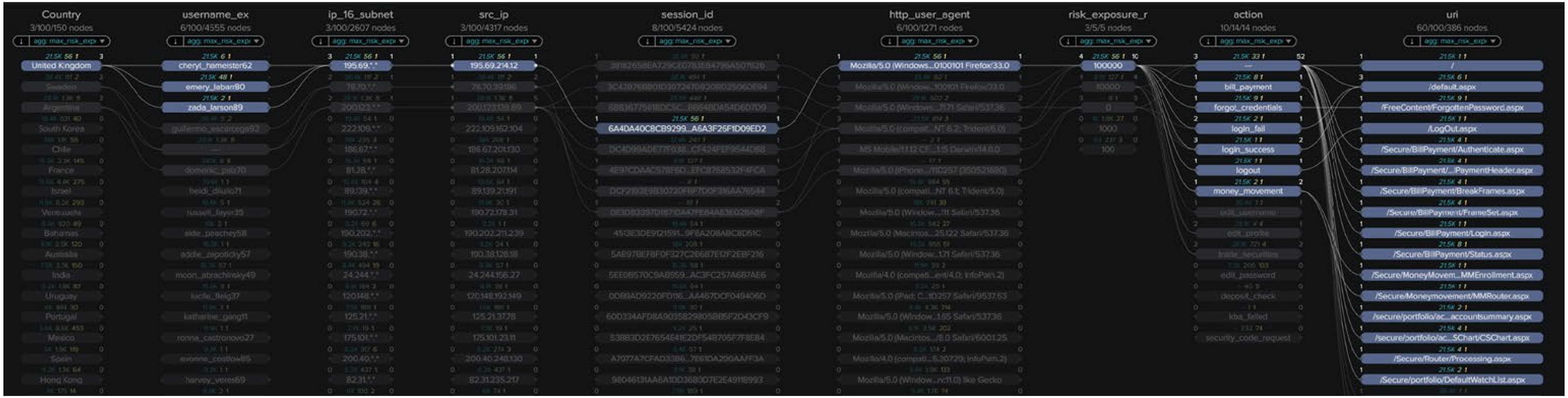
SigBay Link Analysis for Splunk

Free App on Splunkbase:
https://splunkbase.splunk.com/app/5126/


splunkbase.splunk.com/app/5126/
splunkbase
Search App by keyword, technology...
My Account
My Splunk
Support & Services
Sigbay Link Analysis
2 ratings
Sigbay Link Analysis - user guide

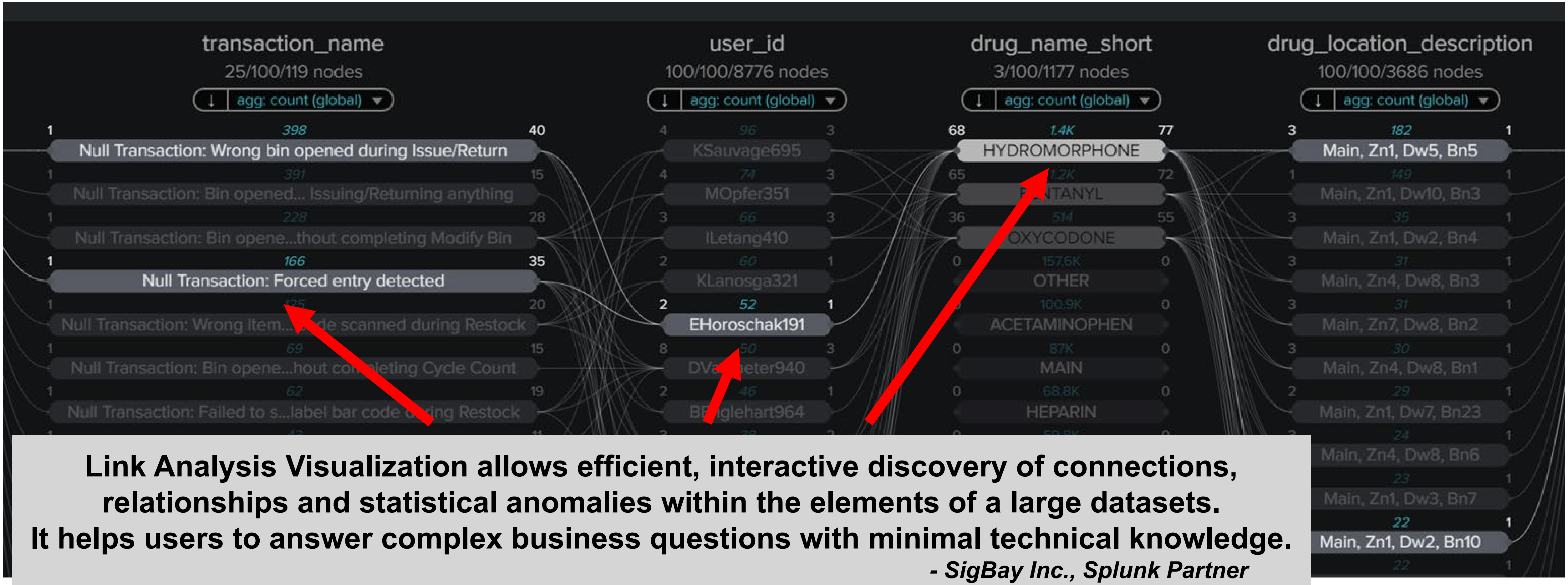
What Is SigBay Link Analysis?

- SigBay Link Analysis is an Interactive Data Exploration and Visualization Framework allowing non-technical business users to quickly gain actionable insights from large amounts of complex data.
- Its purpose is to reduce disconnect between less technical business users and complexity of the underlying datasets.
- Layered implementation allows interfacing with many data repositories.



splunk> .conf20

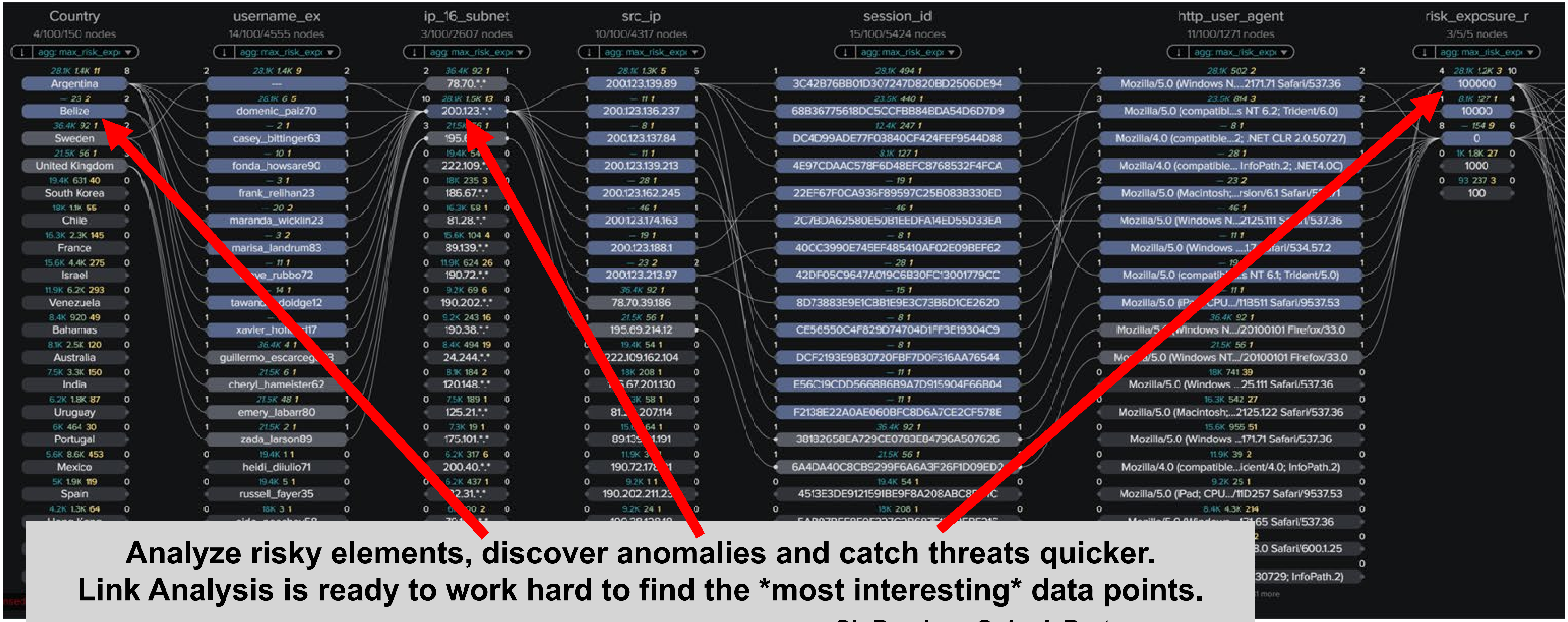
Interactive Data Analysis



Link Analysis Visualization allows efficient, interactive discovery of connections, relationships and statistical anomalies within the elements of a large datasets.
It helps users to answer complex business questions with minimal technical knowledge.

- SigBay Inc., Splunk Partner

Anomalies and Threats Discovery


Country
4/100/150 nodes
agg: max_risk_expo
Argentina
Belize
Sweden
United Kingdom
South Korea
Chile
France
Israel
Venezuela
Bahamas
Australia
India
Uruguay
Portugal
Mexico
Spain
username_ex
14/100/4555 nodes
domenic_palz70
casey_bittinger63
fonda_howsare90
frank_relihan23
maranda_wicklin23
marisa_landrum83
tawana_doidge12
xavier_hol
guillermo_escarceg
cheryl_hameister62
emery_labarr80
zada_larson89
heidi_diiulio71
russell_fayer35
ip_16_subnet
3/100/2607 nodes
78.70.*.*
200.123.*.*
222.109.*.*
186.67.*.*
81.28.*.*
89.139.*.*
190.72.*.*
190.202.*.*
190.38.*.*
24.244.*.*
120.148.*.*
125.21.*.*
175.101.*.*
200.40.*.*
src_ip
10/100/4317 nodes
200.123.139.89
200.123.136.237
200.123.137.84
200.123.139.213
200.123.162.245
200.123.174.163
200.123.188.1
200.123.213.97
78.70.39.186
195.69.214.12
222.109.162.104
190.202.211.2
session_id
15/100/5424 nodes
3C42B76BB01D307247D820BD2506DE94
68B36775618DC5CCFBB84BDA54D6D7D9
DC4D99ADE77F03840CF424FEF9544D88
4E97CDAAC578F6D48EFC8768532F4FCA
22EF67F0CA936F89597C25B083B330ED
2C7BDA62580E50B1EEDFA14ED55D33EA
40CC3990E745EF485410AF02E09BEF62
42DF05C9647A019C6B30FC13001779CC
8D73883E9E1CBB1E9E3C73B6D1CE2620
CE56550C4F829D74704D1FF3E19304C9
DCF2193E9B30720FBF7D0F316AA76544
E56C19CDD5668B6B9A7D915904F66B04
F2138E22A0AE060BFC8D6A7CE2CF578E
38182658EA729CE0783E84796A507626
http_user_agent
11/100/1271 nodes
Mozilla/5.0 (Windows N...2171.71 Safari/537.36
Mozilla/5.0 (compatibl...s NT 6.2; Trident/6.0)
Mozilla/4.0 (compatible...2; .NET CLR 2.0.50727)
Mozilla/4.0 (compatible... InfoPath.2; .NET4.0C)
Mozilla/5.0 (Windows ...25.111 Safari/537.36
Mozilla/5.0 (Macintosh;...2125.122 Safari/537.36
Mozilla/5.0 (Windows ...171.71 Safari/537.36
Mozilla/4.0 (compatible...ident/4.0; InfoPath.2)
Mozilla/5.0 (iPad; CPU.../11D257 Safari/9537.53
risk_exposure_r
3/5/5 nodes
100000
10000
0
1000
100

Analyze risky elements, discover anomalies and catch threats quicker.
Link Analysis is ready to work hard to find the *most interesting* data points.

- SigBay Inc., Splunk Partner

Capabilities

- Fully Interactive, every node and data element supports multiple contexts
- Discovery and Clear Presentation of the Most Interesting Data Points
- Discovery of Any-to-Any: Relationships, Connections and Correlations
- Automatic calculation of multiple summary, aggregate and statistical functions simultaneously over ALL data elements
- Automatic and manual sorting by any chosen metric, order and number of connections by any other entity or group.
- Discovery of anomalous relationships, unusual velocities and suspicious data patterns.
- Peer group analysis and outlier discovery.
- Multi-selecting, global searching and hot-keys controls over all functions.
- Real-time REST API calls to get specific answers and retrieve/update data points. Can communicate with other systems such as Phantom.
- Support for (require) Splunk Accelerated Data Model to tap into large datasets dynamically.

Implementation and Underlying Technology

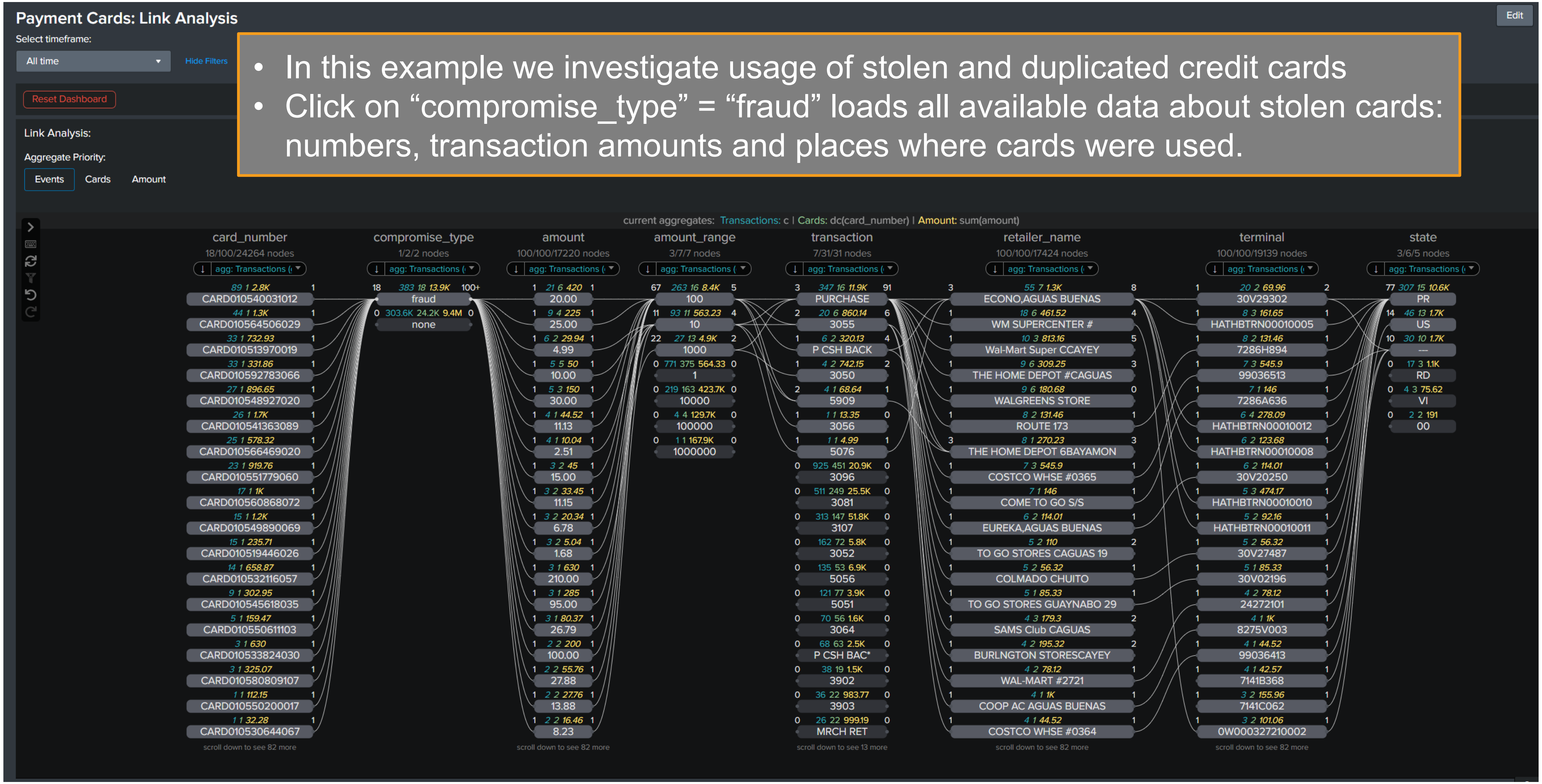
- Custom built using industry standard libraries.
- The UI part is driven by React (open source library developed by Facebook). React utilizing Virtual DOM approach for faster incremental HTML updates only when they are needed.
- The data and state management part is done with MobX library.
- The visualization part is based on D3 and SVG.
- The overall project is bundled into a single Splunk visualization using Webpack, allowing to be used as component in the Splunk Web UI or independently by using the REST API to communicate with Splunk and other data analytical solutions.

Examples

Finding Stolen Credit Cards: Case 1

Detecting Suspicious Access to Patient Records

Link Analysis: Detecting Suspicious Access to Records

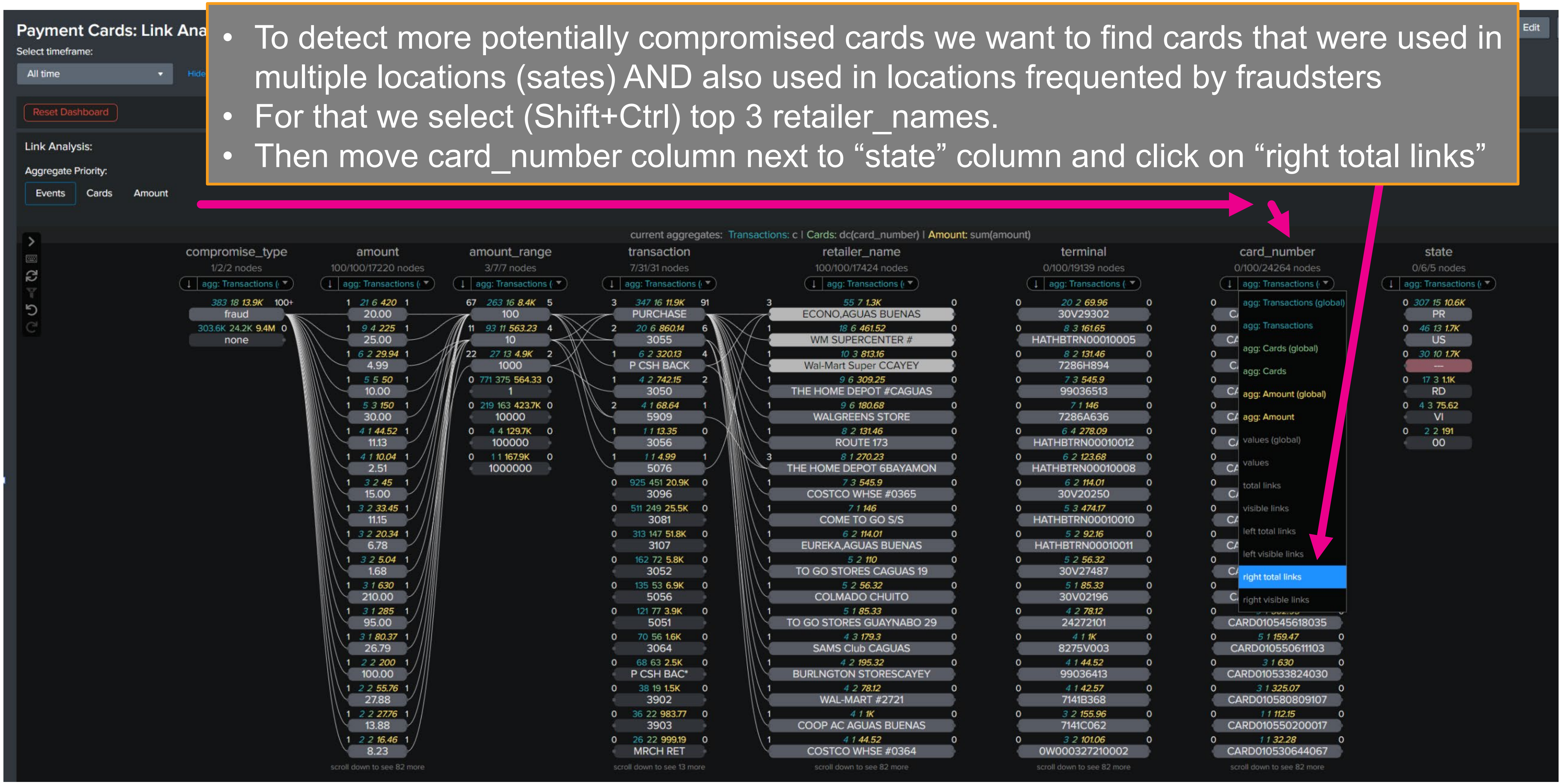


- In this example we investigate usage of stolen and duplicated credit cards
- Click on "compromise_type" = "fraud" loads all available data about stolen cards: numbers, transaction amounts and places where cards were used.

splunk> .conf20

Link Analysis: Detecting Suspicious Access to Records

- To detect more potentially compromised cards we want to find cards that were used in multiple locations (sates) AND also used in locations frequented by fraudsters
- For that we select (Shift+Ctrl) top 3 retailer_names.
- Then move card_number column next to “state” column and click on “right total links”



Payment Cards: Link Ana

Select timeframe: All time

Reset Dashboard

Link Analysis:

Aggregate Priority: Events | Cards | Amount

current aggregates: Transactions: c | Cards: dc(card_number) | Amount: sum(amount)

compromise_type — 1/2/2 nodes — agg: Transactions (

```
383 18 13.9K  100+   fraud
303.6K 24.2K 9.4M  0   none
```

amount — 100/100/17220 nodes — agg: Transactions (

```
1  21 6 420  1      20.00
1  9 4 225  1       25.00
1  6 2 29.94  1     4.99
1  5 5 50  1        10.00
1  5 3 150  1       30.00
1  4 1 44.52  1     11.13
1  4 1 10.04  1     2.51
1  3 2 45  1        15.00
1  3 2 33.45  1     11.15
1  3 2 20.34  1     6.78
1  3 2 5.04  1      1.68
1  3 1 630  1       210.00
1  3 1 285  1       95.00
1  3 1 80.37  1     26.79
1  2 2 200  1       100.00
1  2 2 55.76  1     27.88
1  2 2 27.76  1     13.88
1  2 2 16.46  1     8.23
scroll down to see 82 more
```

amount_range — 3/7/7 nodes — agg: Transactions (

```
67  263 16 8.4K  5         100
11  93 11 563.23  4        10
22  27 13 4.9K  2          1000
0  771 375 564.33  0       1
0  219 163 423.7K  0       10000
0  4 4 129.7K  0           100000
0  1 1 167.9K  0           1000000
```

transaction — 7/31/31 nodes — agg: Transactions (

```
3  347 16 11.9K  91        PURCHASE
2  20 6 860.14  6          3055
1  6 2 320.13  4           P CSH BACK
1  4 2 742.15  2           3050
2  4 1 68.64  1            5909
1  1 1 13.35  0            3056
1  1 1 4.99  1             5076
0  925 451 20.9K  0        3096
0  511 249 25.5K  0        3081
0  313 147 51.8K  0        3107
0  162 72 5.8K  0          3052
0  135 53 6.9K  0          5056
0  121 77 3.9K  0          5051
0  70 56 1.6K  0           3064
0  68 63 2.5K  0           P CSH BAC*
0  38 19 1.5K  0           3902
0  36 22 983.77  0         3903
0  26 22 999.19  0         MRCH RET
scroll down to see 13 more
```

retailer_name — 100/100/17424 nodes — agg: Transactions (

```
3  55 7 1.3K  0            ECONO,AGUAS BUENAS
1  18 6 461.52  0          WM SUPERCENTER #
1  10 3 813.16  0          Wal-Mart Super CCAYEY
1  9 6 309.25  0           THE HOME DEPOT #CAGUAS
1  9 6 180.68  0           WALGREENS STORE
1  8 2 131.46  0           ROUTE 173
3  8 1 270.23  0           THE HOME DEPOT 6BAYAMON
1  7 3 545.9  0            COSTCO WHSE #0365
1  7 1 146  0              COME TO GO S/S
1  6 2 114.01  0           EUREKA,AGUAS BUENAS
1  5 2 110  0              TO GO STORES CAGUAS 19
1  5 2 56.32  0            COLMADO CHUITO
1  5 1 85.33  0            TO GO STORES GUAYNABO 29
1  4 3 179.3  0            SAMS Club CAGUAS
1  4 2 195.32  0           BURLNGTON STORESCAYEY
1  4 2 78.12  0            WAL-MART #2721
1  4 1 1K  0               COOP AC AGUAS BUENAS
1  4 1 44.52  0            COSTCO WHSE #0364
scroll down to see 82 more
```

terminal — 0/100/19139 nodes — agg: Transactions (

```
0  20 2 69.96  0           30V29302
0  8 3 161.65  0           HATHBTRN00010005
0  8 2 131.46  0           7286H894
0  7 3 545.9  0            99036513
0  7 1 146  0              7286A636
0  6 4 278.09  0           HATHBTRN00010012
0  6 2 123.68  0           HATHBTRN00010008
0  6 2 114.01  0           30V20250
0  5 3 474.17  0           HATHBTRN00010010
0  5 2 92.16  0            HATHBTRN00010011
0  5 2 56.32  0            30V27487
0  5 1 85.33  0            30V02196
0  4 2 78.12  0            24272101
0  4 1 1K  0               8275V003
0  4 1 44.52  0            99036413
0  4 1 42.57  0            7141B368
0  3 2 155.96  0           7141C062
0  3 2 101.06  0           0W000327210002
scroll down to see 82 more
```

card_number — 0/100/24264 nodes — agg: Transactions (

```
0  CARD010545618035
0  5 1 159.47  0           CARD010550611103
0  3 1 630  0              CARD010533824030
0  3 1 325.07  0           CARD010580809107
0  1 1 112.15  0           CARD010550200017
0  1 1 32.28  0            CARD010530644067
scroll down to see 82 more
```

state — 0/6/5 nodes — agg: Transactions (

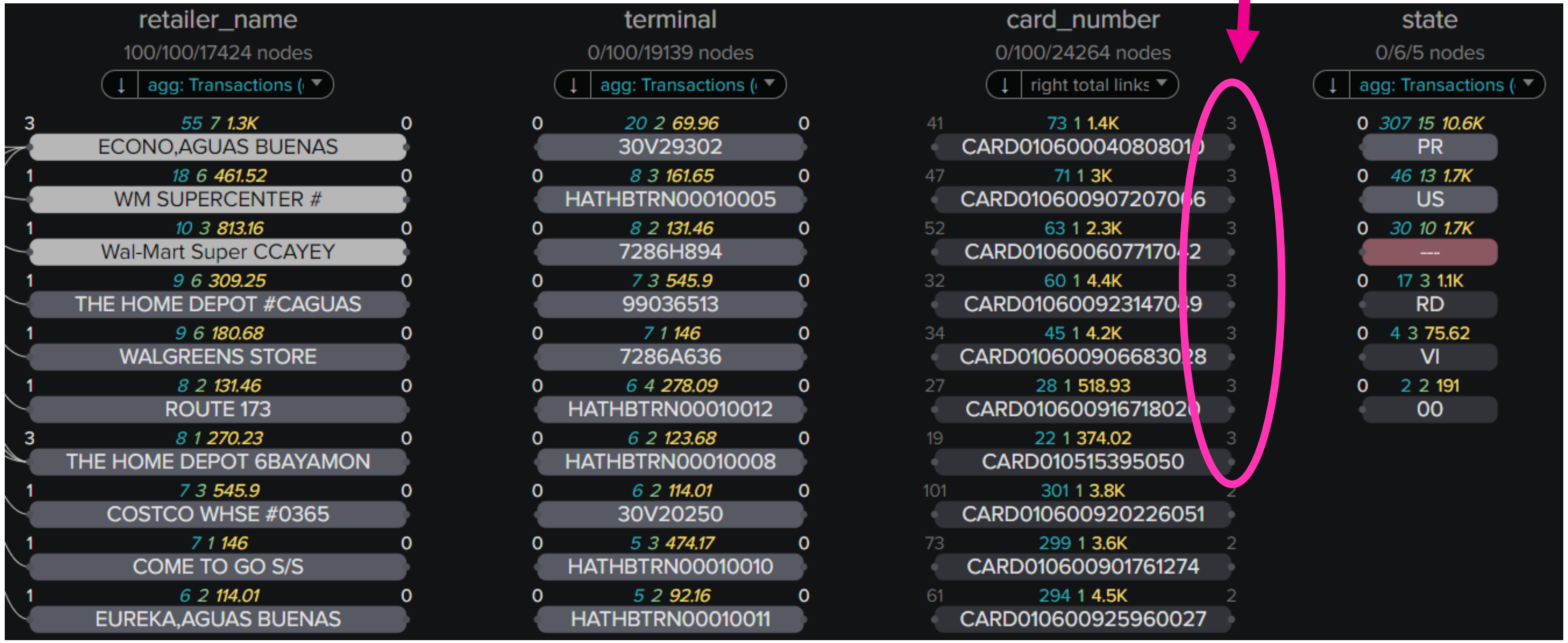
```
0  307 15 10.6K            PR
0  46 13 1.7K              US
0  30 10 1.7K              ---
0  17 3 1.1K               RD
0  4 3 75.62               VI
0  2 2 191                 00
```

splunk> .conf20

Link Analysis: Detecting Suspicious Access to Records

- When you click on any node or interact with Link Analysis visualization – it sends dynamic request to Accelerated Data Model and retrieves fresh results.
- In this case the query returned 7 cards that matches our query:

Find cards that been used in different states
(top 7 cards been used in 3 states)



retailer_name
100/100/17424 nodes
↓ agg: Transactions (

3 55 7 1.3K 0
ECONO,AGUAS BUENAS
1 18 6 461.52 0
WM SUPERCENTER #
1 10 3 813.16 0
Wal-Mart Super CCAYEY
1 9 6 309.25 0
THE HOME DEPOT #CAGUAS
1 9 6 180.68 0
WALGREENS STORE
1 8 2 131.46 0
ROUTE 173
3 8 1 270.23 0
THE HOME DEPOT 6BAYAMON
1 7 3 545.9 0
COSTCO WHSE #0365
1 7 1 146 0
COME TO GO S/S
1 6 2 114.01 0
EUREKA,AGUAS BUENAS

terminal
0/100/19139 nodes
↓ agg: Transactions (

0 20 2 69.96 0
30V29302
0 8 3 161.65 0
HATHBTRN00010005
0 8 2 131.46 0
7286H894
0 7 3 545.9 0
99036513
0 7 1 146 0
7286A636
0 6 4 278.09 0
HATHBTRN00010012
0 6 2 123.68 0
HATHBTRN00010008
0 6 2 114.01 0
30V20250
0 5 3 474.17 0
HATHBTRN00010010
0 5 2 92.16 0
HATHBTRN00010011

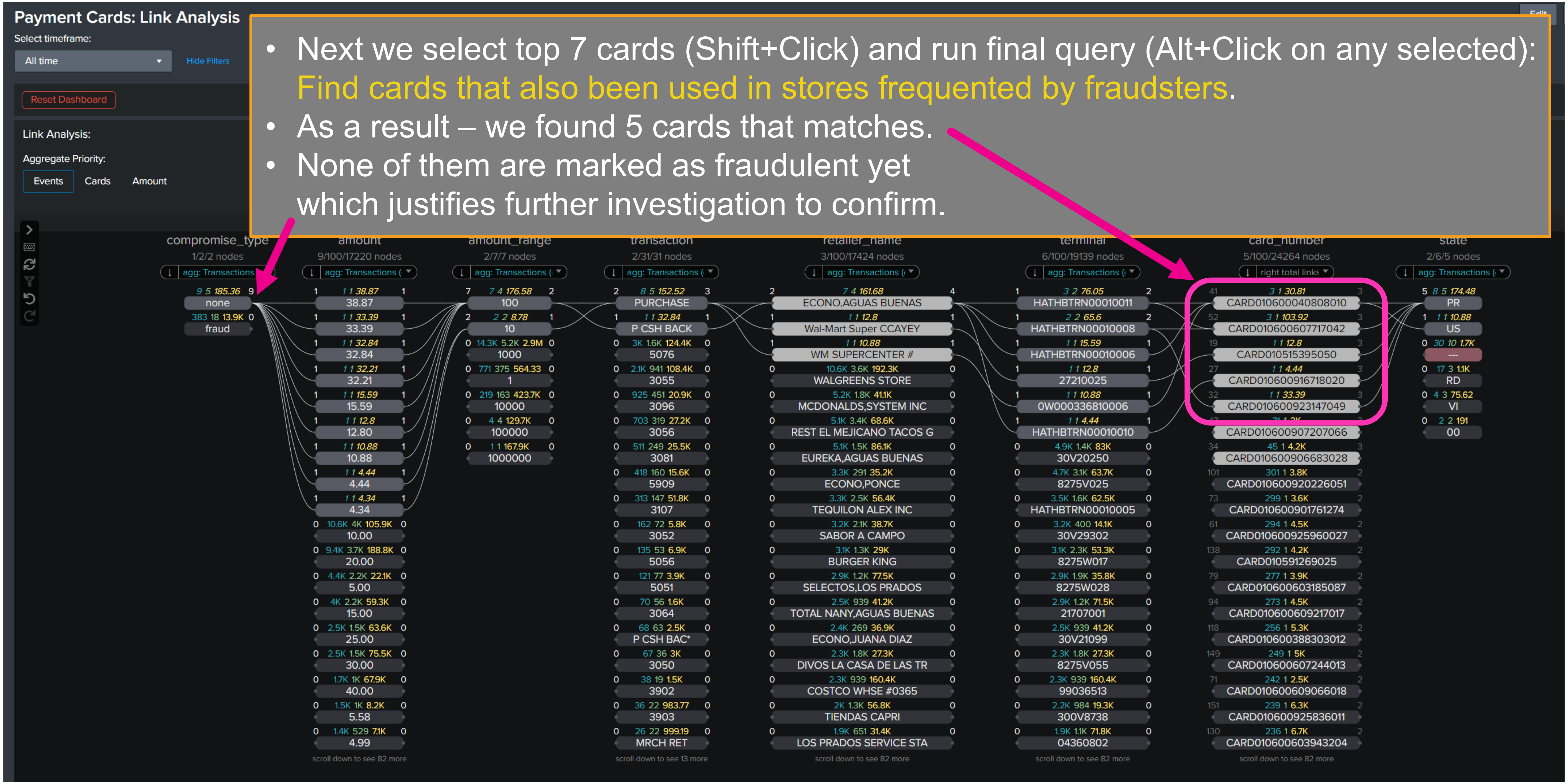
card_number
0/100/24264 nodes
↓ right total links

41 73 1 1.4K 3
CARD010600040808010
47 71 1 3K 3
CARD010600907207066
52 63 1 2.3K 3
CARD010600607717042
32 60 1 4.4K 3
CARD010600923147049
34 45 1 4.2K 3
CARD010600906683028
27 28 1 518.93 3
CARD010600916718020
19 22 1 374.02 3
CARD010515395050
101 301 1 3.8K 2
CARD010600920226051
73 299 1 3.6K 2
CARD010600901761274
61 294 1 4.5K 2
CARD010600925960027

state
0/6/5 nodes
↓ agg: Transactions (

0 307 15 10.6K
PR
0 46 13 1.7K
US
0 30 10 1.7K
---
0 17 3 1.1K
RD
0 4 3 75.62
VI
0 2 2 191
00

Link Analysis: Detecting Suspicious Access to Records

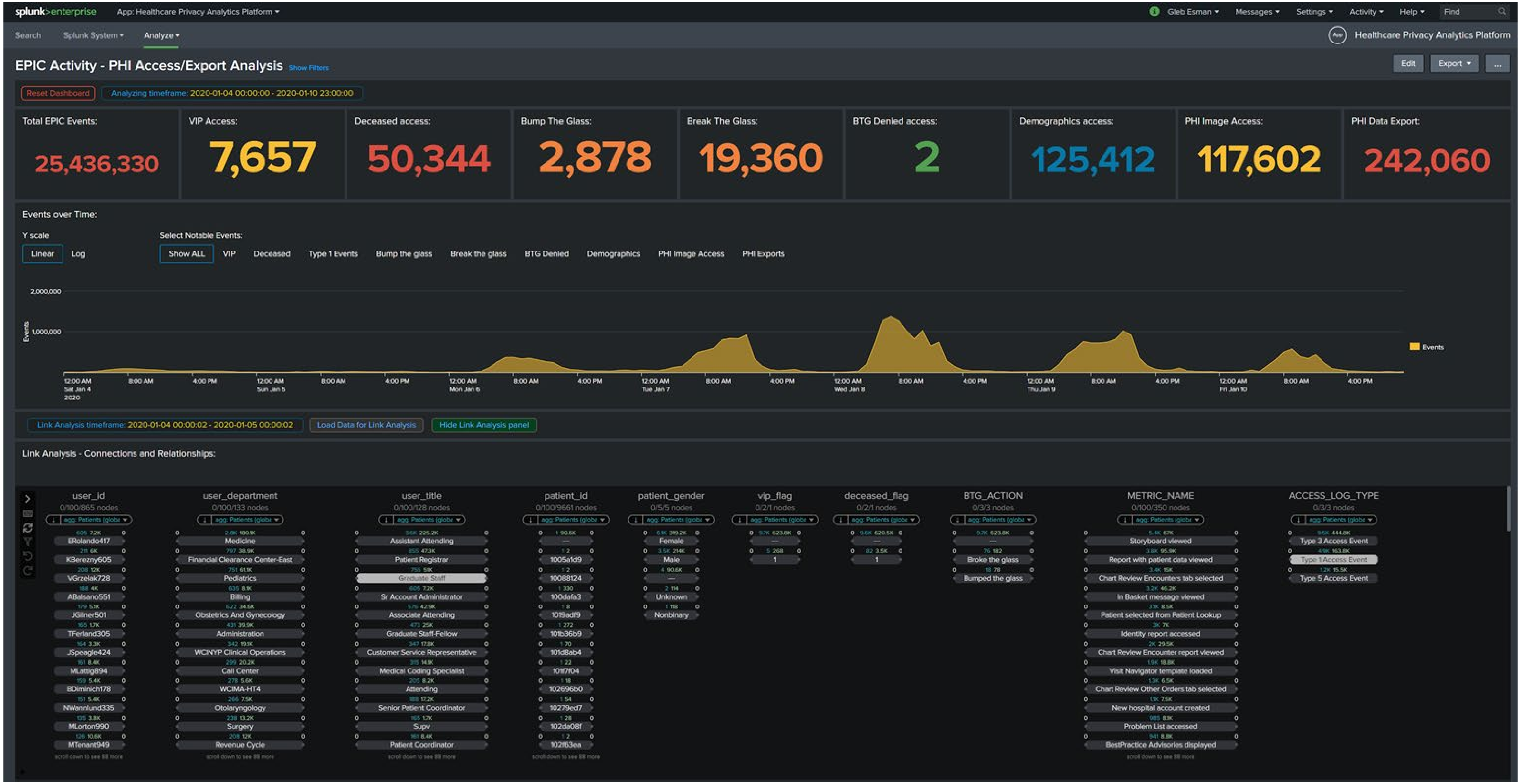


- Next we select top 7 cards (Shift+Click) and run final query (Alt+Click on any selected): Find cards that also been used in stores frequented by fraudsters.
- As a result – we found 5 cards that matches.
- None of them are marked as fraudulent yet which justifies further investigation to confirm.

Finding Patient Privacy Violations: Case 2

Detecting Suspicious Access to Patient Records

Link Analysis: Detecting Suspicious Access to Records



EPIC Activity - PHI Access/Export Analysis Show Filters

Reset Dashboard | Analyzing timeframe: 2020-01-04 00:00:00 - 2020-01-10 23:00:00

Total EPIC Events:	VIP Access:	Deceased access:	Bump The Glass:	Break The Glass:	BTG Denied access:	Demographics access:	PHI Image Access:	PHI Data Export:
25,436,330	7,657	50,344	2,878	19,360	2	125,412	117,602	242,060

Events over Time:

Y scale: Linear | Log

Select Notable Events: Show ALL | VIP | Deceased | Type 1 Events | Bump the glass | Break the glass | BTG Denied | Demographics | PHI Image Access | PHI Exports

Link Analysis timeframe: 2020-01-04 00:00:02 - 2020-01-05 00:00:02 | Load Data for Link Analysis | Hide Link Analysis panel

Link Analysis - Connections and Relationships:

user_id — 0/100/865 nodes — agg: Patients (globa ▾
- 605 7.2K ERolando417
- 211 6K KBerezny605
- 208 12K VGrzelak728
- 188 4K ABalsano551
- 179 5.1K JGilner501
- 165 1.7K TFerland305
- 164 3.3K JSpeagle424
- 161 8.4K MLattig894
- 159 5.4K BDiminich178
- 151 5.4K NWannlund335
- 135 3.8K MLorton990
- 126 10.6K MTenant949
- scroll down to see 88 more

user_department — 0/100/133 nodes — agg: Patients (globa ▾
- 2.8K 180.1K Medicine
- 797 38.9K Financial Clearance Center-East
- 751 61.1K Pediatrics
- 635 8.1K Billing
- 622 34.6K Obstetrics And Gynecology
- 431 39.9K Administration
- 342 19.1K WCINYP Clinical Operations
- 299 20.2K Call Center
- 278 5.6K WCIMA-HT4
- 266 7.5K Otolaryngology
- 238 13.2K Surgery
- 208 12K Revenue Cycle
- scroll down to see 88 more

user_title — 0/100/128 nodes — agg: Patients (globa ▾
- 3.6K 225.2K Assistant Attending
- 855 47.3K Patient Registrar
- 755 59K Graduate Staff
- 605 7.2K Sr Account Administrator
- 576 42.9K Associate Attending
- 473 25K Graduate Staff-Fellow
- 347 17.8K Customer Service Representative
- 315 14.1K Medical Coding Specialist
- 205 8.2K Attending
- 188 17.2K Senior Patient Coordinator
- 165 1.7K Supv
- 161 8.4K Patient Coordinator
- scroll down to see 88 more

patient_id — 0/100/9661 nodes — agg: Patients (globa ▾
- 1 90.6K —
- 1 2 1005a1d9
- 1 2 10088124
- 1 330 100dafa3
- 1 8 1019adf9
- 1 272 101b36b9
- 1 70 101d8ab4
- 1 22 101f7f04
- 1 18 102696b0
- 1 54 10279ed7
- 1 28 102da08f
- 1 2 102f63ea
- scroll down to see 88 more

patient_gender — 0/5/5 nodes — agg: Patients (globa ▾
- 6.1K 389.2K Female
- 3.5K 214K Male
- 4 90.6K —
- 2 114 Unknown
- 1 118 Nonbinary

vip_flag — 0/2/1 nodes — agg: Patients (globa ▾
- 9.7K 623.8K —
- 5 268 1

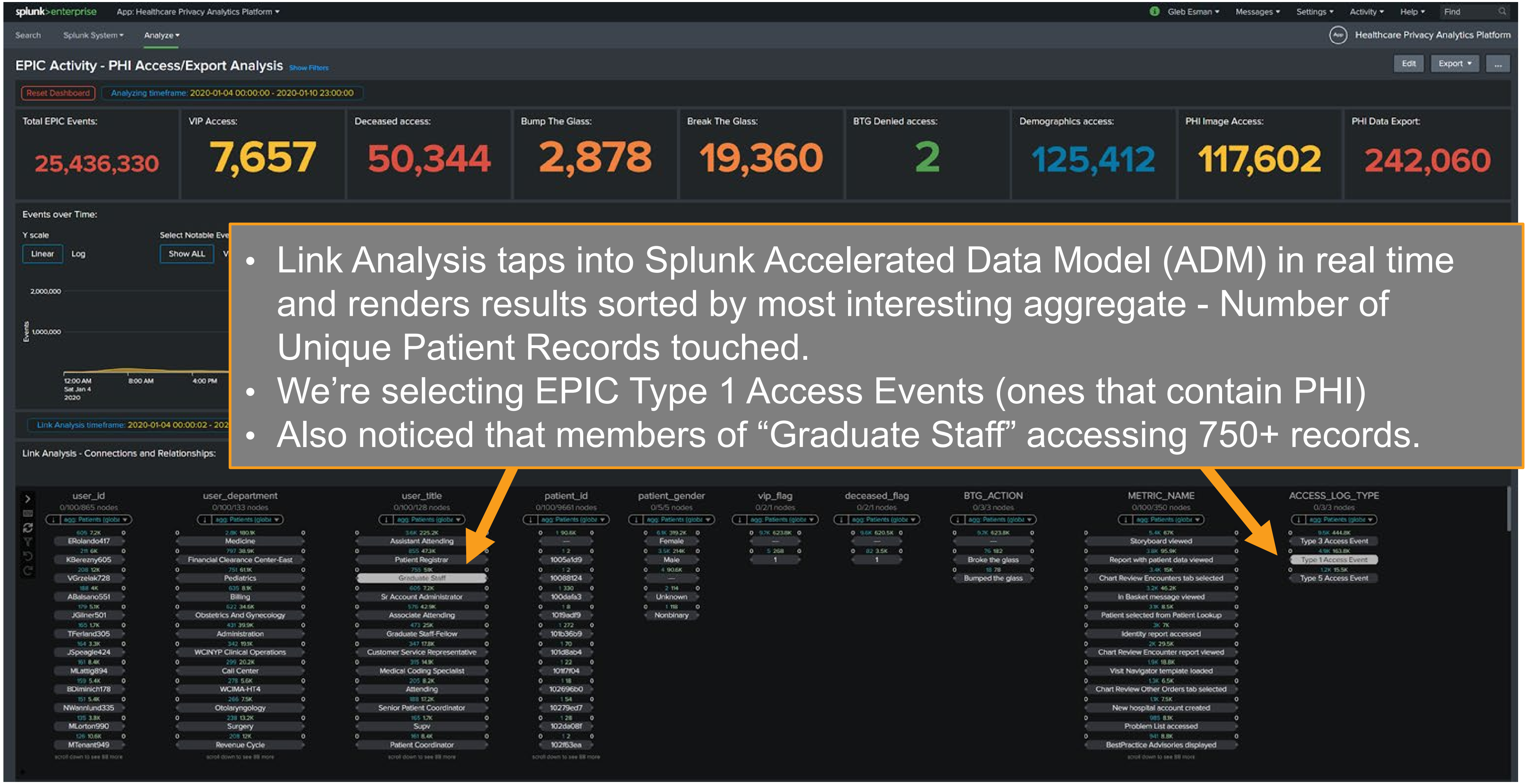
deceased_flag — 0/2/1 nodes — agg: Patients (globa ▾
- 9.6K 620.5K —
- 82 3.5K 1

BTG_ACTION — 0/3/3 nodes — agg: Patients (globa ▾
- 9.7K 623.8K —
- 76 182 Broke the glass
- 18 78 Bumped the glass

METRIC_NAME — 0/100/350 nodes — agg: Patients (globa ▾
- 5.4K 67K Storyboard viewed
- 3.8K 95.9K Report with patient data viewed
- 3.4K 15K Chart Review Encounters tab selected
- 3.2K 46.2K In Basket message viewed
- 3.1K 8.5K Patient selected from Patient Lookup
- 3K 7K Identity report accessed
- 2K 29.5K Chart Review Encounter report viewed
- 1.9K 18.8K Visit Navigator template loaded
- 1.3K 6.5K Chart Review Other Orders tab selected
- 1.1K 7.5K New hospital account created
- 985 8.1K Problem List accessed
- 941 8.8K BestPractice Advisories displayed
- scroll down to see 88 more

ACCESS_LOG_TYPE — 0/3/3 nodes — agg: Patients (globa ▾
- 9.5K 444.8K Type 3 Access Event
- 4.9K 163.8K Type 1 Access Event
- 1.2K 15.5K Type 5 Access Event

Link Analysis: Detecting Suspicious Access to Records



EPIC Activity - PHI Access/Export Analysis

Analyzing timeframe: 2020-01-04 00:00:00 - 2020-01-10 23:00:00

Total EPIC Events:	VIP Access:	Deceased access:	Bump The Glass:	Break The Glass:	BTG Denied access:	Demographics access:	PHI Image Access:	PHI Data Export:
25,436,330	7,657	50,344	2,878	19,360	2	125,412	117,602	242,060

Events over Time:

Link Analysis timeframe: 2020-01-04 00:00:02 - 202

Link Analysis - Connections and Relationships:

user_id
0/100/865 nodes
agg: Patients (globa
605 7.2K ERolando417
211 6K KBerezny605
208 12K VGrzelak728
188 4K ABalsano551
179 5.1K JGilner501
165 1.7K TFerland305
164 3.3K JSpeagle424
161 8.4K MLattig894
159 5.4K BDiminich178
151 5.4K NWannlund335
135 3.8K MLorton990
126 10.6K MTenant949
scroll down to see 88 more

user_department
0/100/133 nodes
agg: Patients (globa
2.8K 180.9K Medicine
797 38.9K Financial Clearance Center-East
751 61.1K Pediatrics
635 8.1K Billing
622 34.6K Obstetrics And Gynecology
431 39.9K Administration
342 19.1K WCINYP Clinical Operations
299 20.2K Call Center
278 5.6K WCIMA-HT4
266 7.5K Otolaryngology
238 13.2K Surgery
208 12K Revenue Cycle
scroll down to see 88 more

user_title
0/100/128 nodes
agg: Patients (globa
3.6K 225.2K Assistant Attending
855 47.3K Patient Registrar
755 59K Graduate Staff
605 7.2K Sr Account Administrator
576 42.9K Associate Attending
473 25K Graduate Staff-Fellow
347 17.8K Customer Service Representative
315 14.9K Medical Coding Specialist
205 8.2K Attending
188 17.2K Senior Patient Coordinator
165 1.7K Supv
161 8.4K Patient Coordinator
scroll down to see 88 more

patient_id
0/100/9661 nodes
agg: Patients (globa
1 90.6K —
1 2 1005a1d9
1 2 10088124
1 330 100dafa3
1 8 1019adf9
1 272 101b36b9
1 70 101d8ab4
1 22 101f7f04
1 18 102696b0
1 54 10279ed7
1 28 102da08f
1 2 102f63ea
scroll down to see 88 more

patient_gender
0/5/5 nodes
agg: Patients (globa
6.9K 319.2K Female
3.5K 214K Male
4 90.6K —
2 114 Unknown
1 118 Nonbinary

vip_flag
0/2/1 nodes
agg: Patients (globa
9.7K 623.8K —
5 268 1

deceased_flag
0/2/1 nodes
agg: Patients (globa
9.6K 620.5K —
82 3.5K 1

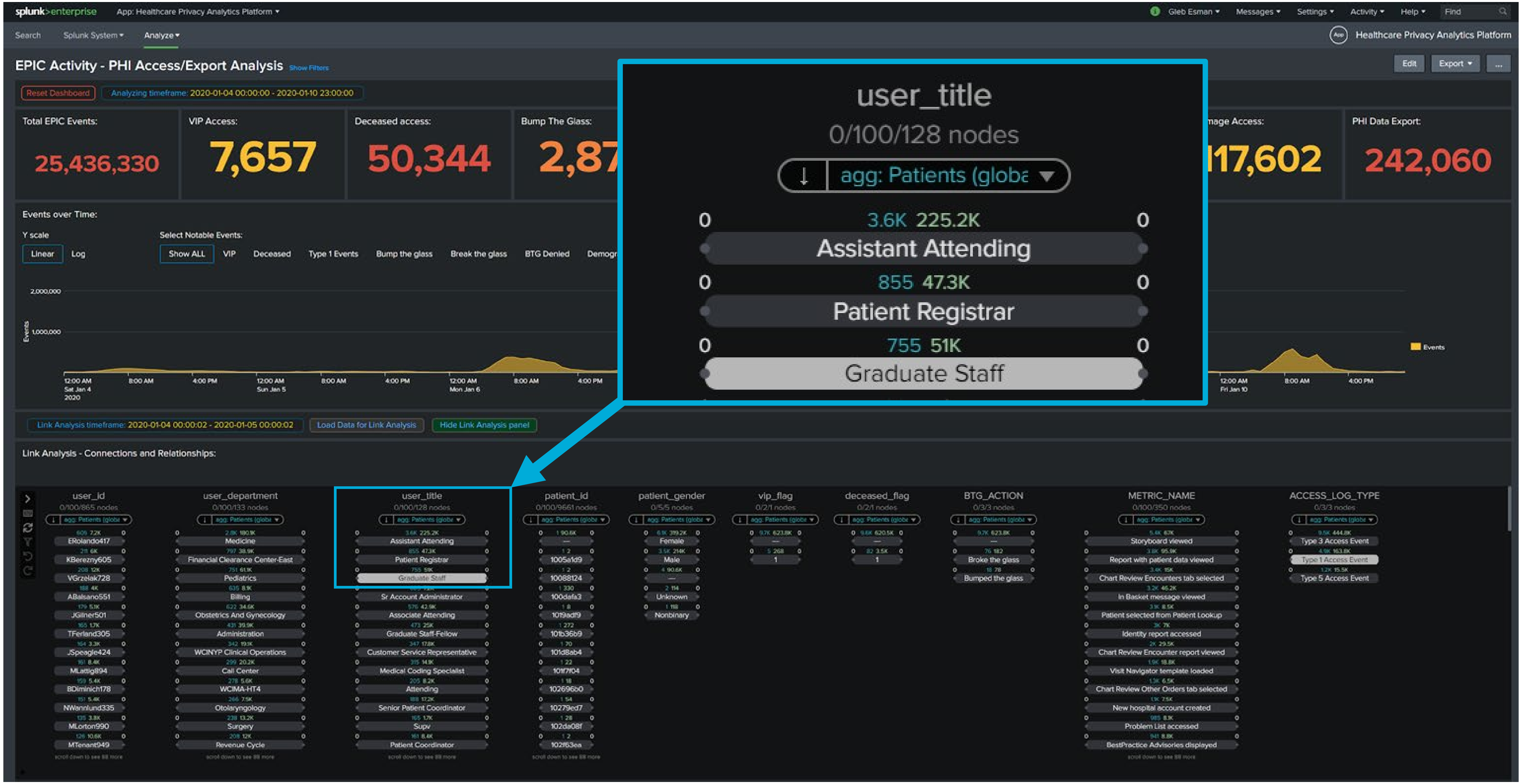
BTG_ACTION
0/3/3 nodes
agg: Patients (globa
9.7K 623.8K —
76 182 Broke the glass
18 78 Bumped the glass

METRIC_NAME
0/100/350 nodes
agg: Patients (globa
5.4K 67K Storyboard viewed
3.8K 95.9K Report with patient data viewed
3.4K 15K Chart Review Encounters tab selected
3.2K 46.2K In Basket message viewed
3.1K 8.5K Patient selected from Patient Lookup
3K 7K Identity report accessed
2K 29.5K Chart Review Encounter report viewed
1.9K 18.8K Visit Navigator template loaded
1.3K 6.5K Chart Review Other Orders tab selected
1.1K 7.5K New hospital account created
985 8.1K Problem List accessed
941 8.8K BestPractice Advisories displayed
scroll down to see 88 more

ACCESS_LOG_TYPE
0/3/3 nodes
agg: Patients (globa
9.5K 444.8K Type 3 Access Event
4.9K 163.8K Type 1 Access Event
1.2K 15.5K Type 5 Access Event

- Link Analysis taps into Splunk Accelerated Data Model (ADM) in real time and renders results sorted by most interesting aggregate - Number of Unique Patient Records touched.
- We're selecting EPIC Type 1 Access Events (ones that contain PHI)
- Also noticed that members of "Graduate Staff" accessing 750+ records.

Link Analysis: Detecting Suspicious Access to Records



EPIC Activity - PHI Access/Export Analysis Show Filters

Analyzing timeframe: 2020-01-04 00:00:00 - 2020-01-10 23:00:00

Total EPIC Events:	VIP Access:	Deceased access:	Bump The Glass:	…mage Access:	PHI Data Export:
25,436,330	7,657	50,344	2,87…	…117,602	242,060

Events over Time:

Y scale: Linear Log

Select Notable Events: Show ALL VIP Deceased Type 1 Events Bump the glass Break the glass BTG Denied Demogr…

Link Analysis timeframe: 2020-01-04 00:00:02 - 2020-01-05 00:00:02

Link Analysis - Connections and Relationships:

user_id
0/100/865 nodes
↓ agg: Patients (globa ▾
605 7.2K ERolando417
211 6K KBerezny605
208 12K VGrzelak728
188 4K ABalsano551
179 5.1K JGilner501
165 1.7K TFerland305
164 3.3K JSpeagle424
161 8.4K MLattig894
159 5.4K BDiminich178
151 5.4K NWannlund335
135 3.8K MLorton990
126 10.6K MTenant949
scroll down to see 88 more

user_department
0/100/133 nodes
↓ agg: Patients (globa ▾
2.8K 180.1K Medicine
797 38.9K Financial Clearance Center-East
751 61.1K Pediatrics
635 8.1K Billing
622 34.6K Obstetrics And Gynecology
431 39.9K Administration
342 19.1K WCINYP Clinical Operations
299 20.2K Call Center
278 5.6K WCIMA-HT4
266 7.5K Otolaryngology
238 13.2K Surgery
208 12K Revenue Cycle
scroll down to see 88 more

user_title
0/100/128 nodes
↓ agg: Patients (globa ▾
3.6K 225.2K Assistant Attending
855 47.3K Patient Registrar
755 59K Graduate Staff
[illegible] Sr Account Administrator
576 42.9K Associate Attending
473 25K Graduate Staff-Fellow
347 17.8K Customer Service Representative
315 14.9K Medical Coding Specialist
205 8.2K Attending
188 17.2K Senior Patient Coordinator
165 1.7K Supv
161 8.4K Patient Coordinator
scroll down to see 88 more

patient_id
0/100/9661 nodes
↓ agg: Patients (globa ▾
1 90.6K —
1 2 1005a1d9
1 2 10088124
1 330 100dafa3
1 8 1019adf9
1 272 101b36b9
1 70 101d8ab4
1 22 101f7f04
1 18 102696b0
1 54 10279ed7
1 28 102da08f
1 2 102f63ea
scroll down to see 88 more

patient_gender
0/5/5 nodes
↓ agg: Patients (globa ▾
6.1K 319.2K Female
3.5K 214K Male
4 90.6K —
2 114 Unknown
1 118 Nonbinary

vip_flag
0/2/1 nodes
↓ agg: Patients (globa ▾
9.7K 623.8K —
5 268 1

deceased_flag
0/2/1 nodes
↓ agg: Patients (globa ▾
9.6K 620.5K —
82 3.5K 1

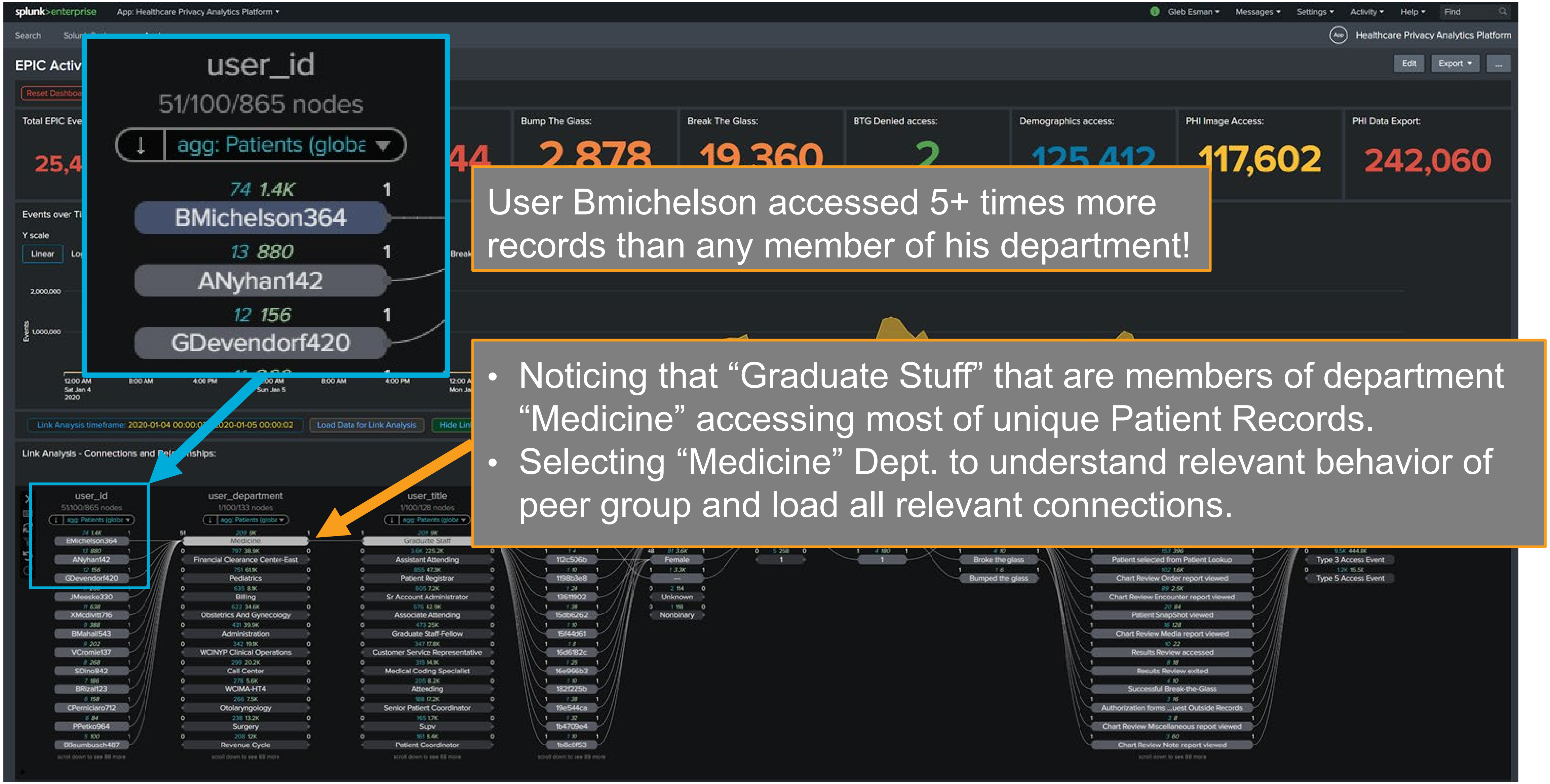
BTG_ACTION
0/3/3 nodes
↓ agg: Patients (globa ▾
9.7K 623.8K —
76 182 Broke the glass
18 78 Bumped the glass

METRIC_NAME
0/100/350 nodes
↓ agg: Patients (globa ▾
5.4K 67K Storyboard viewed
3.8K 95.9K Report with patient data viewed
3.4K 15K Chart Review Encounters tab selected
3.2K 46.2K In Basket message viewed
3.1K 8.5K Patient selected from Patient Lookup
3K 7K Identity report accessed
2K 29.5K Chart Review Encounter report viewed
1.9K 18.8K Visit Navigator template loaded
1.3K 6.5K Chart Review Other Orders tab selected
1.1K 7.5K New hospital account created
985 8.1K Problem List accessed
941 8.8K BestPractice Advisories displayed
scroll down to see 88 more

ACCESS_LOG_TYPE
0/3/3 nodes
↓ agg: Patients (globa ▾
9.5K 444.8K Type 3 Access Event
4.9K 163.8K Type 1 Access Event
1.2K 15.5K Type 5 Access Event

user_title
0/100/128 nodes
↓ agg: Patients (globa ▾
0 3.6K 225.2K 0 Assistant Attending
0 855 47.3K 0 Patient Registrar
0 755 51K 0 Graduate Staff

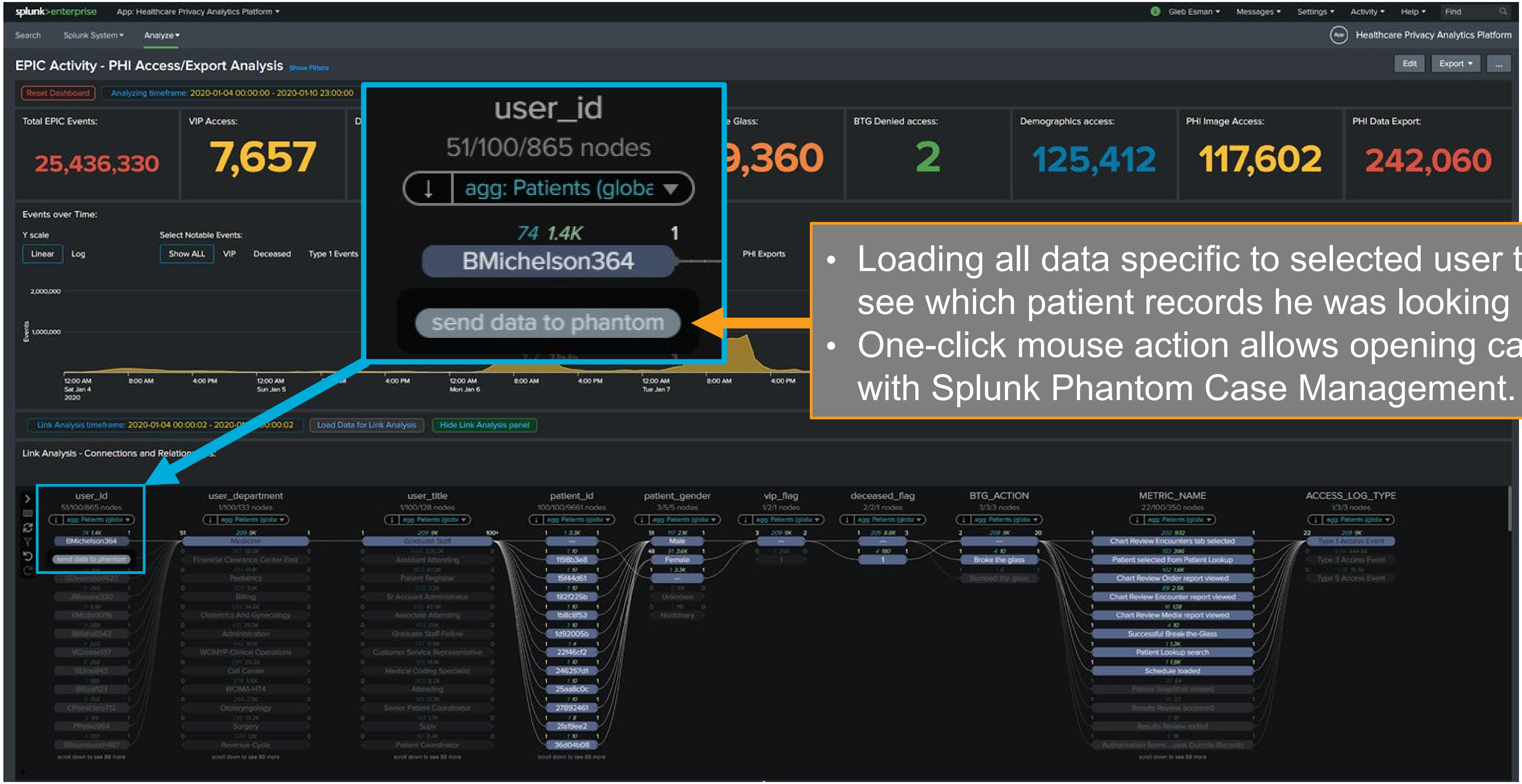
Link Analysis: Detecting Suspicious Access to Records



User Bmichelson accessed 5+ times more records than any member of his department!

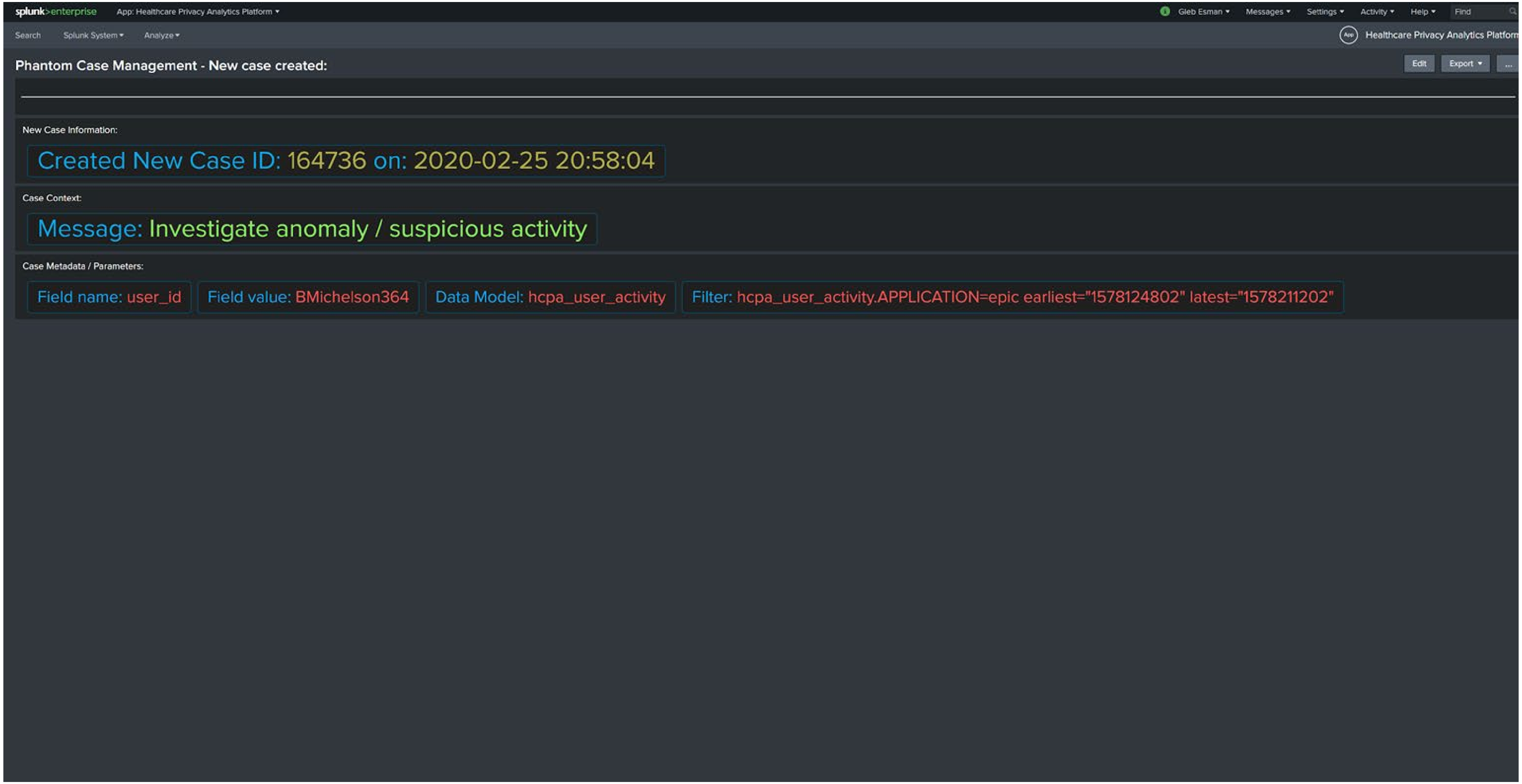
- Noticing that “Graduate Stuff” that are members of department “Medicine” accessing most of unique Patient Records.
- Selecting “Medicine” Dept. to understand relevant behavior of peer group and load all relevant connections.

Link Analysis: Detecting Suspicious Access to Records



- Loading all data specific to selected user to see which patient records he was looking at.
- One-click mouse action allows opening case with Splunk Phantom Case Management.

Creating Case within Phantom Case Management



Phantom Case Management - New case created:

New Case Information:

Created New Case ID: 164736 on: 2020-02-25 20:58:04

Case Context:

Message: Investigate anomaly / suspicious activity

Case Metadata / Parameters:

Field name: user_id | Field value: BMichelson364 | Data Model: hcpa_user_activity | Filter: hcpa_user_activity.APPLICATION=epic earliest="1578124802" latest="1578211202"

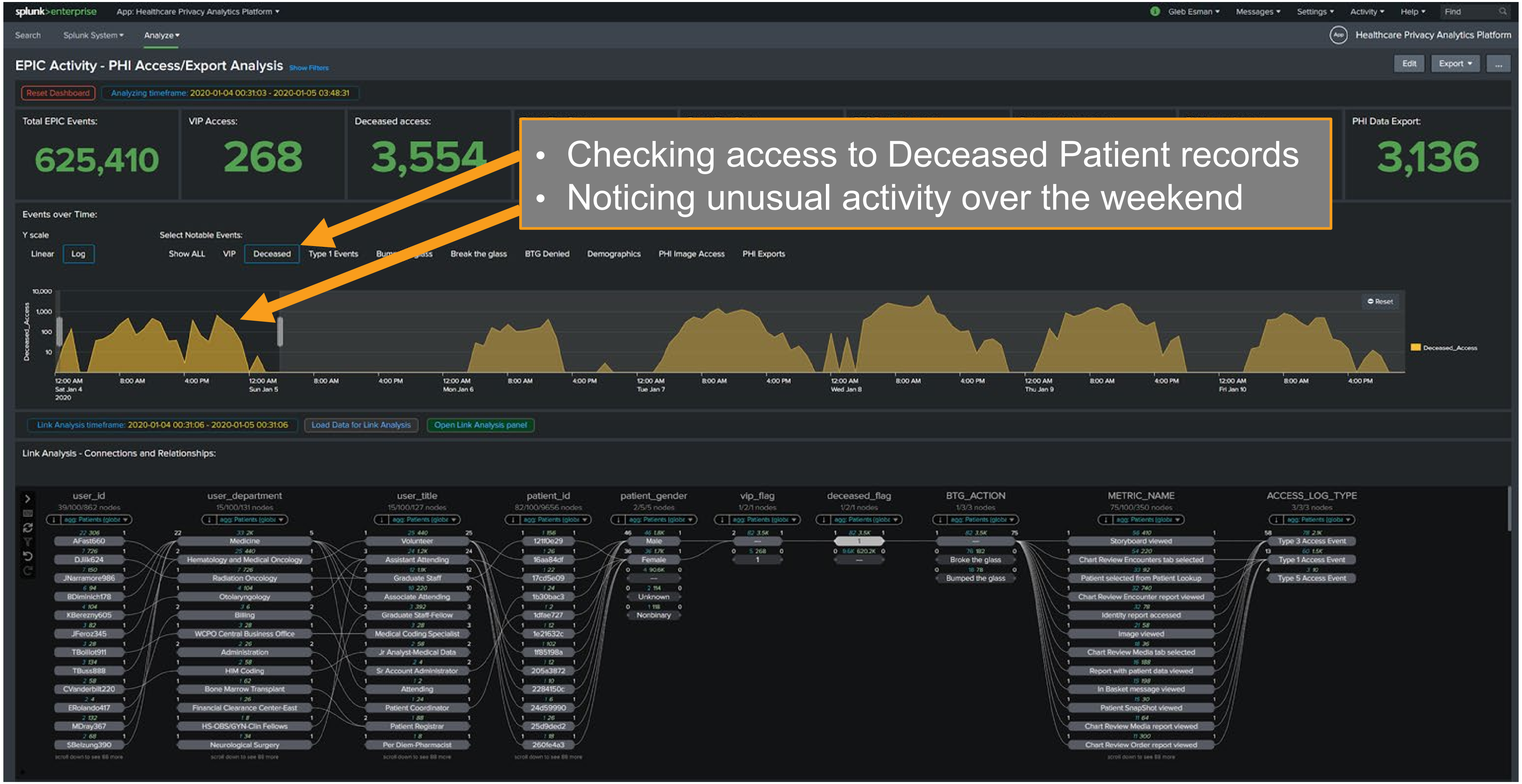
.conf20

splunk>

Finding Patient Privacy Violations: Case 3

Investigating Weekend Access Anomaly

Link Analysis: Investigating Weekend Access Anomaly



- Checking access to Deceased Patient records
- Noticing unusual activity over the weekend

EPIC Activity - PHI Access/Export Analysis

Analyzing timeframe: 2020-01-04 00:31:03 - 2020-01-05 03:48:31

Total EPIC Events: 625,410

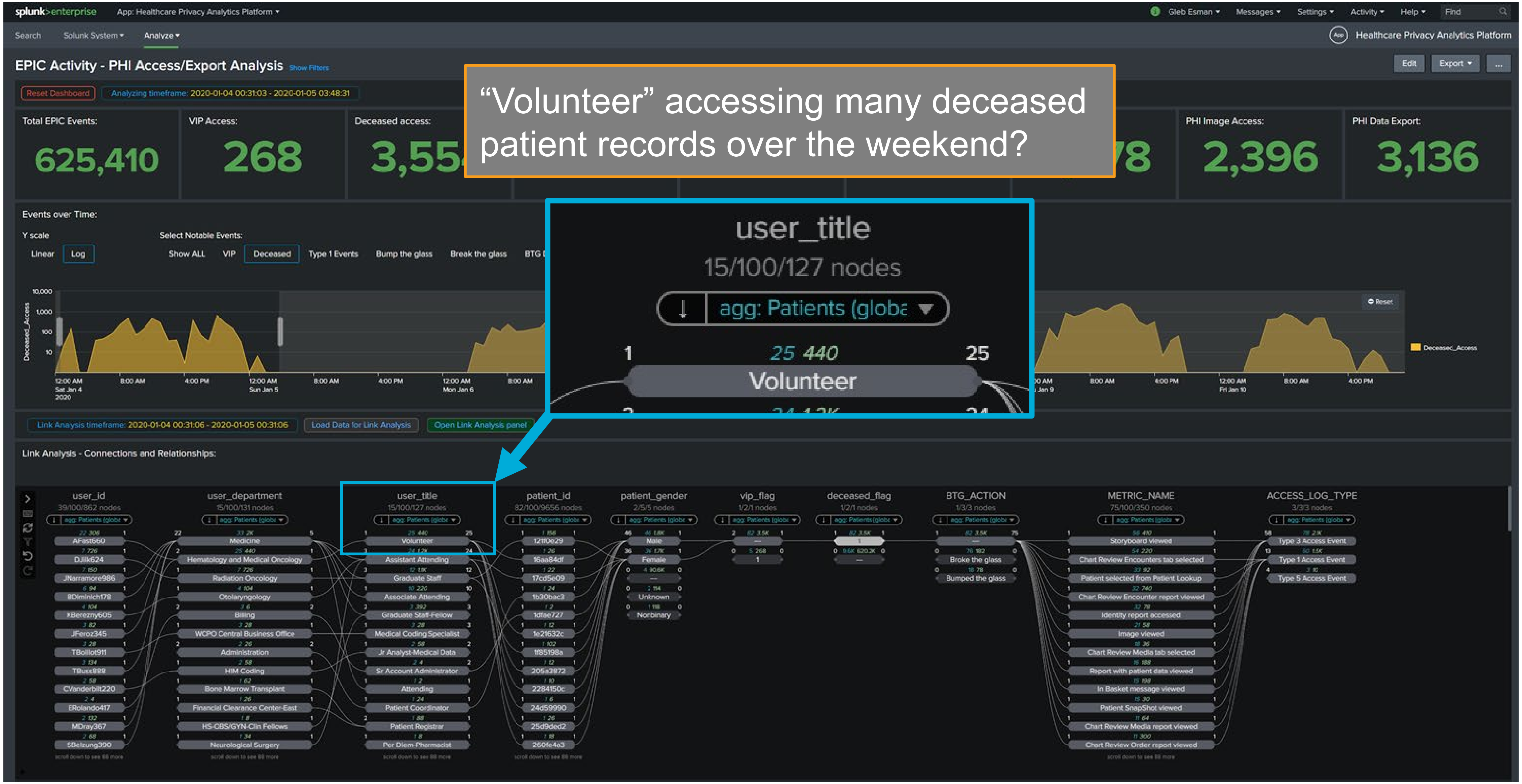
VIP Access: 268

Deceased access: 3,554

PHI Data Export: 3,136

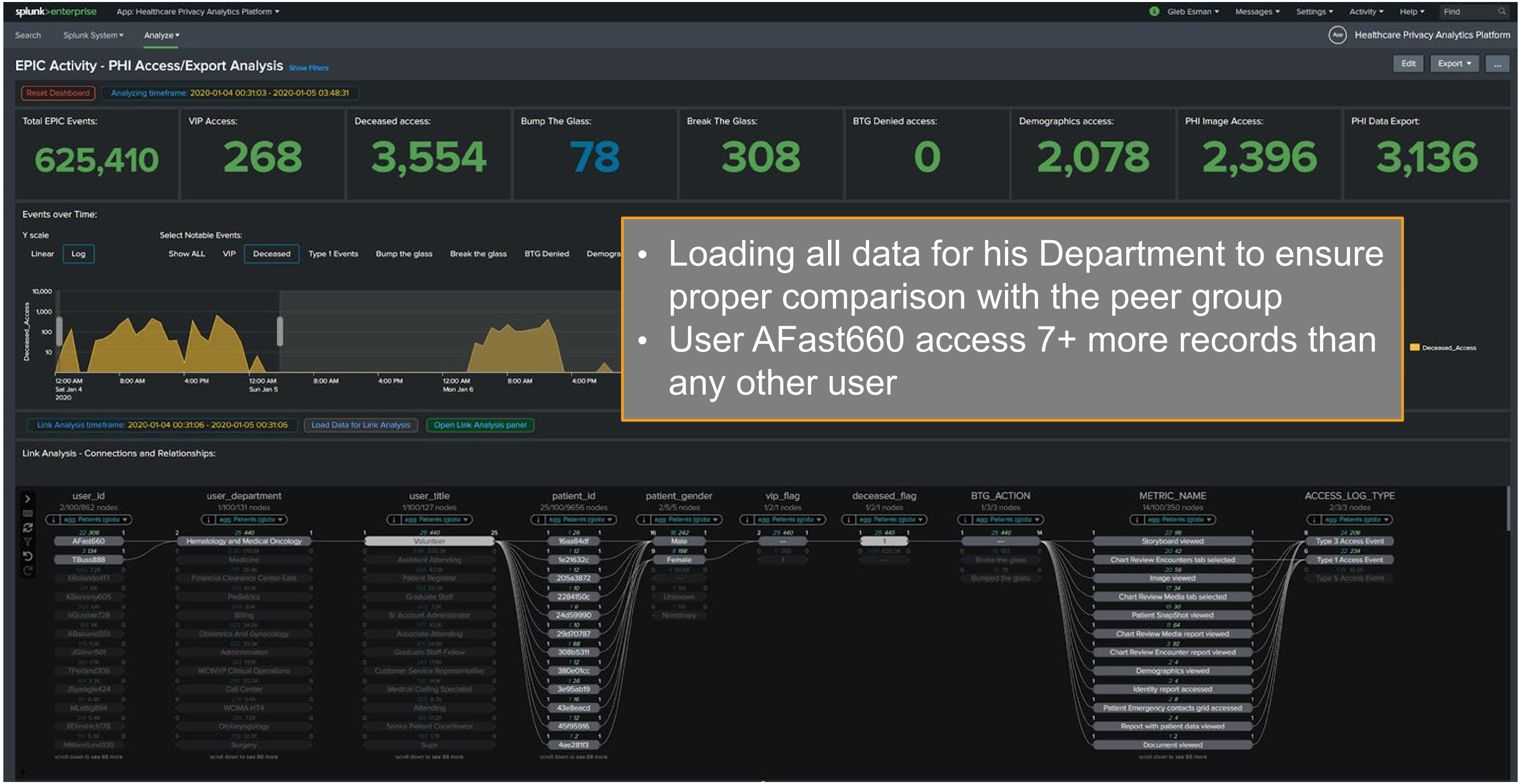
Link Analysis timeframe: 2020-01-04 00:31:06 - 2020-01-05 00:31:06

Link Analysis: Investigating Weekend Access Anomaly



“Volunteer” accessing many deceased patient records over the weekend?

Link Analysis: Investigating Weekend Access Anomaly



EPIC Activity - PHI Access/Export Analysis

Analyzing timeframe: 2020-01-04 00:31:03 - 2020-01-05 03:48:31

Total EPIC Events:	VIP Access:	Deceased access:	Bump The Glass:	Break The Glass:	BTG Denied access:	Demographics access:	PHI Image Access:	PHI Data Export:
625,410	268	3,554	78	308	0	2,078	2,396	3,136

Events over Time:

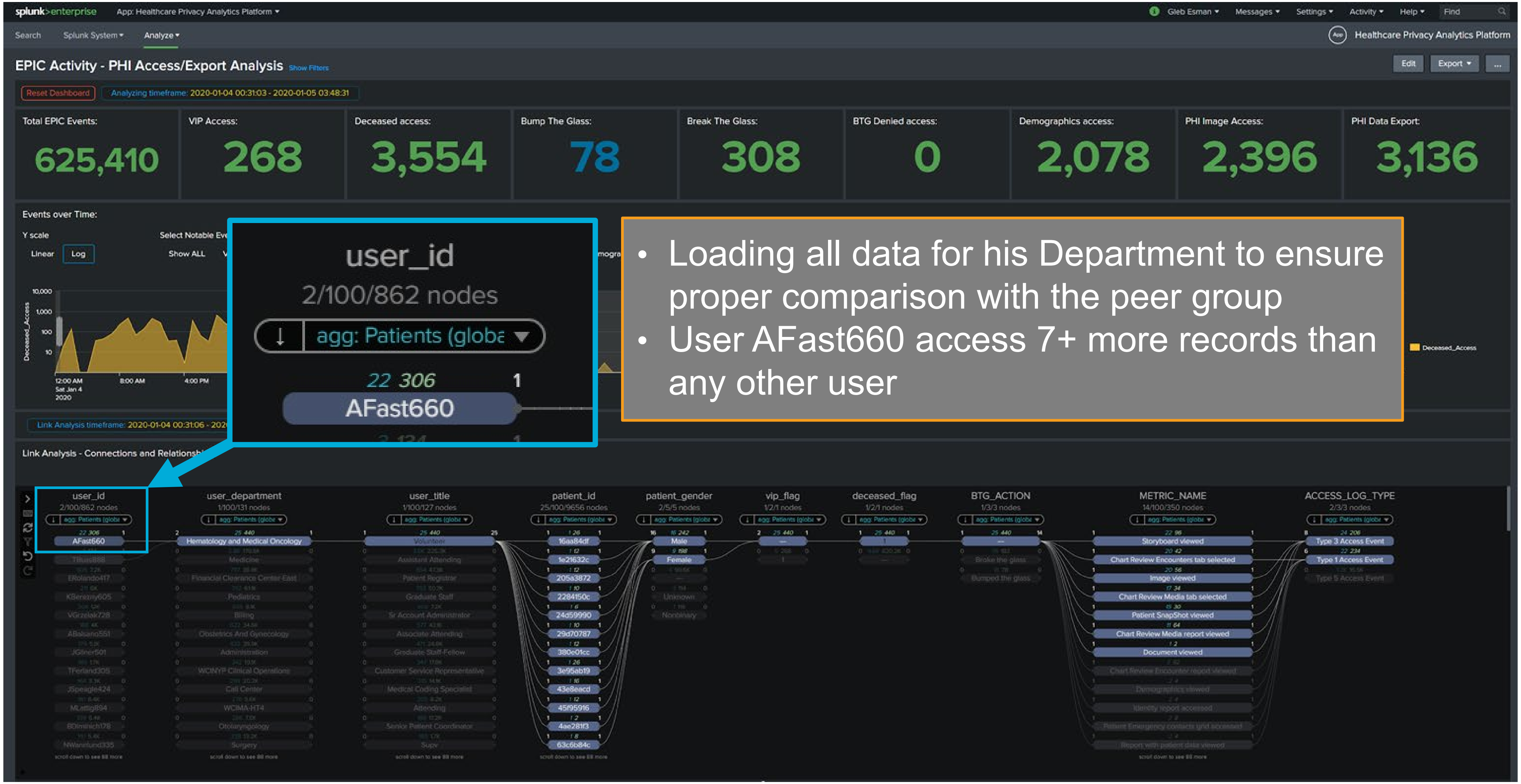
Link Analysis timeframe: 2020-01-04 00:31:06 - 2020-01-05 00:31:06

Link Analysis - Connections and Relationships:

- Loading all data for his Department to ensure proper comparison with the peer group
- User AFast660 access 7+ more records than any other user

splunk> .conf20

Link Analysis: Investigating Weekend Access Anomaly



splunk>enterprise App: Healthcare Privacy Analytics Platform

Search Splunk System Analyze

Healthcare Privacy Analytics Platform

EPIC Activity - PHI Access/Export Analysis Show Filters

Reset Dashboard Analyzing timeframe: 2020-01-04 00:31:03 - 2020-01-05 03:48:31

Total EPIC Events: 625,410

VIP Access: 268

Deceased access: 3,554

Bump The Glass: 78

Break The Glass: 308

BTG Denied access: 0

Demographics access: 2,078

PHI Image Access: 2,396

PHI Data Export: 3,136

Events over Time:

Link Analysis timeframe: 2020-01-04 00:31:06 - 202

Link Analysis - Connections and Relationsh

- Loading all data for his Department to ensure proper comparison with the peer group
- User AFast660 access 7+ more records than any other user

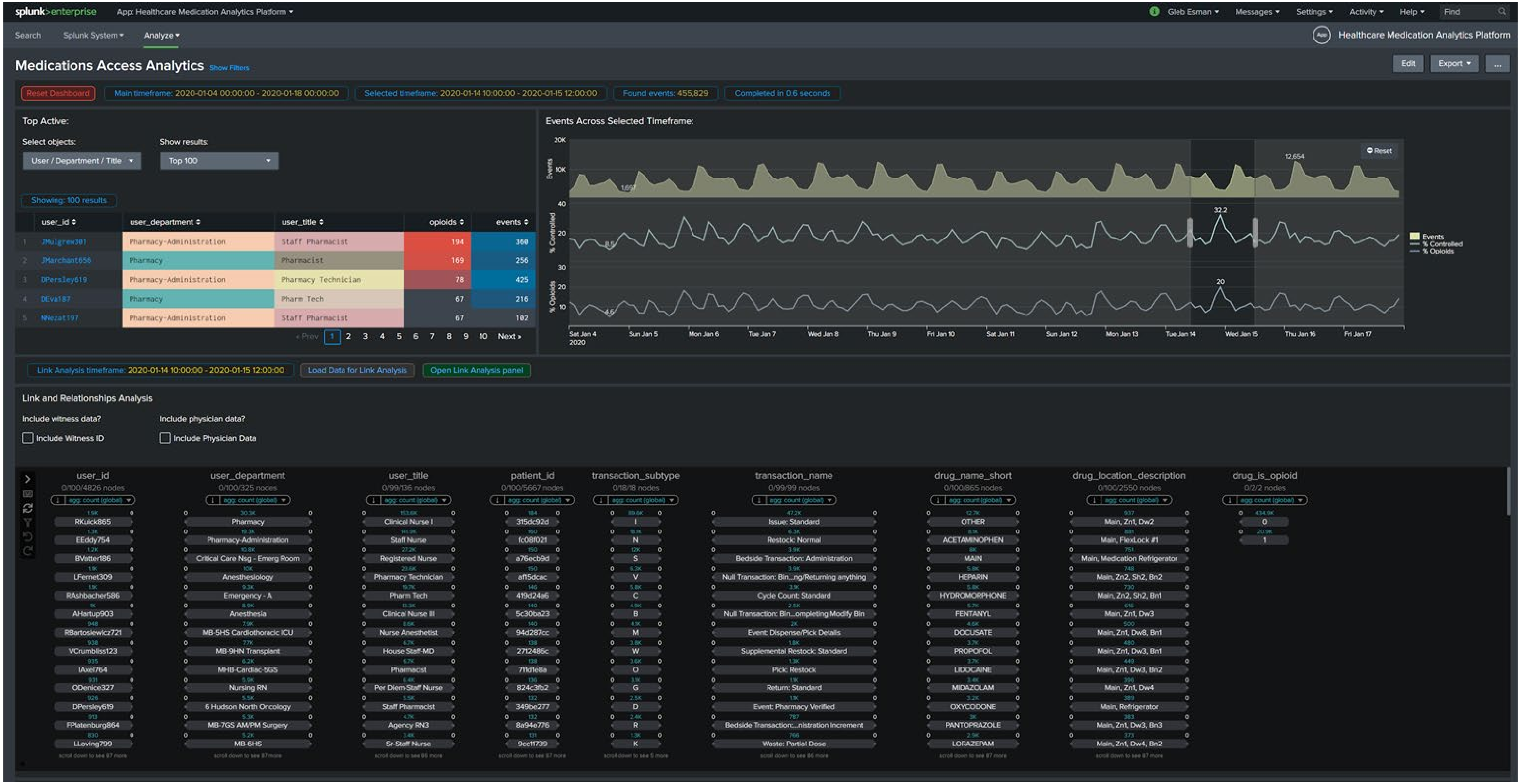
.conf20

splunk>

Detecting Opiod Diversion: Case 4

Accessing Drugs: NULL Transactions and Force Entry events

Link Analysis: Detecting Opioid Diversion



Medications Access Analytics

Main timeframe: 2020-01-04 00:00:00 - 2020-01-18 00:00:00

Selected timeframe: 2020-01-14 10:00:00 - 2020-01-15 12:00:00

Found events: 455,829

Completed in 0.6 seconds

Top Active:

Select objects: User / Department / Title ▾

Show results: Top 100 ▾

Showing: 100 results

	user_id	user_department	user_title	opioids	events
1	JMulgrew301	Pharmacy-Administration	Staff Pharmacist	194	360
2	JMarchant656	Pharmacy	Pharmacist	169	256
3	DPersley619	Pharmacy-Administration	Pharmacy Technician	78	425
4	DEva187	Pharmacy	Pharm Tech	67	216
5	NNezat197	Pharmacy-Administration	Staff Pharmacist	67	102

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

Events Across Selected Timeframe:

Link Analysis timeframe: 2020-01-14 10:00:00 - 2020-01-15 12:00:00

Load Data for Link Analysis

Open Link Analysis panel

Link and Relationships Analysis

Include witness data?

□ Include Witness ID

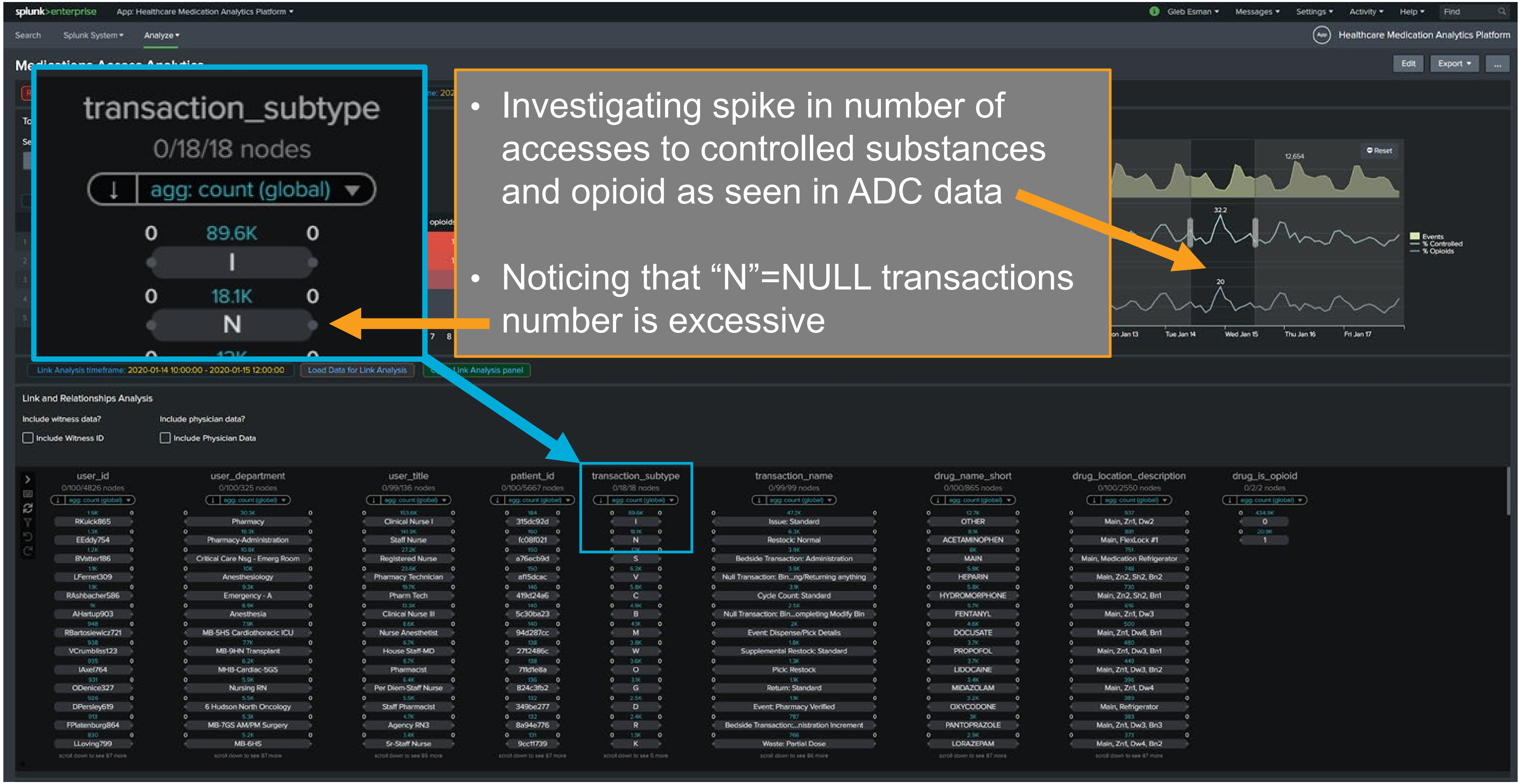
Include physician data?

□ Include Physician Data

user_id	user_department	user_title	patient_id	transaction_subtype	transaction_name	drug_name_short	drug_location_description	drug_is_opioid
0/100/4826 nodes	0/100/325 nodes	0/99/136 nodes	0/100/5667 nodes	0/18/18 nodes	0/99/99 nodes	0/100/865 nodes	0/100/2550 nodes	0/2/2 nodes
agg: count (global)	agg: count (global)	agg: count (global)	agg: count (global)	agg: count (global)	agg: count (global)	agg: count (global)	agg: count (global)	agg: count (global)
1.9K RKuick865	30.3K Pharmacy	153.6K Clinical Nurse I	184 315dc92d	89.6K I	47.2K Issue: Standard	12.7K OTHER	937 Main, Zn1, Dw2	434.9K 0
1.3K EEddy754	19.3K Pharmacy-Administration	141.9K Staff Nurse	160 fc08f021	18.1K N	6.3K Restock: Normal	8.1K ACETAMINOPHEN	881 Main, FlexLock #1	20.9K 1
1.2K BVatter186	10.8K Critical Care Nsg - Emerg Room	27.2K Registered Nurse	150 a76ecb9d	12K S	3.9K Bedside Transaction: Administration	8K MAIN	751 Main, Medication Refrigerator	
1.1K LFernet309	10K Anesthesiology	23.6K Pharmacy Technician	150 af15dcac	6.2K V	3.9K Null Transaction: Bin...ng/Returning anything	5.8K HEPARIN	748 Main, Zn2, Sh2, Bn2	
1.1K RAshbacher586	9.3K Emergency - A	19.7K Pharm Tech	146 419d24a6	5.8K C	3.1K Cycle Count: Standard	5.8K HYDROMORPHONE	730 Main, Zn2, Sh2, Bn1	
1K AHartup903	8.9K Anesthesia	13.3K Clinical Nurse III	140 5c30ba23	4.9K B	2.5K Null Transaction: Bin...ompleting Modify Bin	5.7K FENTANYL	616 Main, Zn1, Dw3	
948 RBartosiewicz721	7.9K MB-5HS Cardiothoracic ICU	8.6K Nurse Anesthetist	140 94d287cc	4.1K M	2K Event: Dispense/Pick Details	4.6K DOCUSATE	500 Main, Zn1, Dw8, Bn1	
938 VCrumbliss123	7.7K MB-9HN Transplant	6.7K House Staff-MD	138 2712486c	3.8K W	1.8K Supplemental Restock: Standard	3.7K PROPOFOL	480 Main, Zn1, Dw3, Bn1	
935 IAxel764	6.2K MHB-Cardiac-5GS	6.7K Pharmacist	138 71fd1e8a	3.6K O	1.3K Pick: Restock	3.7K LIDOCAINE	449 Main, Zn1, Dw3, Bn2	
931 ODenice327	5.9K Nursing RN	6.4K Per Diem-Staff Nurse	136 824c3fb2	3.1K G	1.1K Return: Standard	3.4K MIDAZOLAM	396 Main, Zn1, Dw4	
926 DPersley619	5.5K 6 Hudson North Oncology	5.5K Staff Pharmacist	132 349be277	2.5K D	1.1K Event: Pharmacy Verified	3.2K OXYCODONE	389 Main, Refrigerator	
913 FPlatenburg864	5.3K MB-7GS AM/PM Surgery	4.7K Agency RN3	132 8a94e776	2.4K R	787 Bedside Transaction:...nistration Increment	3K PANTOPRAZOLE	383 Main, Zn1, Dw3, Bn3	
830 LLoving799	5.2K MB-6HS	3.4K Sr-Staff Nurse	131 9cc11739	1.3K K	766 Waste: Partial Dose	2.9K LORAZEPAM	373 Main, Zn1, Dw4, Bn2	
scroll down to see 87 more	scroll down to see 87 more	scroll down to see 86 more	scroll down to see 87 more	scroll down to see 5 more	scroll down to see 86 more	scroll down to see 87 more	scroll down to see 87 more	

splunk> .conf20

Link Analysis: Detecting Opioid Diversion



- Investigating spike in number of accesses to controlled substances and opioid as seen in ADC data
- Noticing that "N"=NULL transactions number is excessive

transaction_subtype

0/18/18 nodes

↓ agg: count (global) ▾

0	89.6K	0
	I	
0	18.1K	0
	N	
0	12K	0

Link Analysis timeframe: 2020-01-14 10:00:00 - 2020-01-15 12:00:00

Load Data for Link Analysis

Link Analysis panel

Link and Relationships Analysis

Include witness data?

□ Include Witness ID

Include physician data?

□ Include Physician Data

user_id — 0/100/4826 nodes — ↓ agg: count (global) ▾

Count	user_id
1.9K	RKuick865
1.3K	EEddy754
1.2K	BVatter186
1.1K	LFernet309
1.1K	RAshbacher586
1K	AHartup903
948	RBartosiewicz721
938	VCrumbliss123
935	IAxel764
931	ODenice327
926	DPersley619
913	FPlatenburg864
830	LLoving799

scroll down to see 87 more

user_department — 0/100/325 nodes — ↓ agg: count (global) ▾

Count	user_department
30.3K	Pharmacy
19.3K	Pharmacy-Administration
10.8K	Critical Care Nsg - Emerg Room
10K	Anesthesiology
9.3K	Emergency - A
8.9K	Anesthesia
7.9K	MB-5HS Cardiothoracic ICU
7.7K	MB-9HN Transplant
6.2K	MHB-Cardiac-5GS
5.9K	Nursing RN
5.5K	6 Hudson North Oncology
5.3K	MB-7GS AM/PM Surgery
5.2K	MB-6HS

scroll down to see 87 more

user_title — 0/99/136 nodes — ↓ agg: count (global) ▾

Count	user_title
153.6K	Clinical Nurse I
141.9K	Staff Nurse
27.2K	Registered Nurse
23.6K	Pharmacy Technician
19.7K	Pharm Tech
13.3K	Clinical Nurse III
8.6K	Nurse Anesthetist
6.7K	House Staff-MD
6.7K	Pharmacist
6.4K	Per Diem-Staff Nurse
5.5K	Staff Pharmacist
4.7K	Agency RN3
3.4K	Sr-Staff Nurse

scroll down to see 86 more

patient_id — 0/100/5667 nodes — ↓ agg: count (global) ▾

Count	patient_id
184	315dc92d
160	fc08f021
150	a76ecb9d
150	af15dcac
146	419d24a6
140	5c30ba23
140	94d287cc
138	2712486c
138	71fd1e8a
136	824c3fb2
132	349be277
132	8a94e776
131	9cc11739

scroll down to see 87 more

transaction_subtype — 0/18/18 nodes — ↓ agg: count (global) ▾

Count	transaction_subtype
89.6K	I
18.1K	N
12K	S
6.3K	V
5.8K	C
4.9K	B
4.1K	M
3.8K	W
3.6K	O
3.1K	G
2.5K	D
2.4K	R
1.3K	K

scroll down to see 5 more

transaction_name — 0/99/99 nodes — ↓ agg: count (global) ▾

Count	transaction_name
47.2K	Issue: Standard
6.3K	Restock: Normal
3.9K	Bedside Transaction: Administration
3.9K	Null Transaction: Bin...ng/Returning anything
3.9K	Cycle Count: Standard
2.5K	Null Transaction: Bin...ompleting Modify Bin
2K	Event: Dispense/Pick Details
1.8K	Supplemental Restock: Standard
1.3K	Pick: Restock
1.1K	Return: Standard
1.1K	Event: Pharmacy Verified
787	Bedside Transaction:...nistration Increment
766	Waste: Partial Dose

scroll down to see 86 more

drug_name_short — 0/100/865 nodes — ↓ agg: count (global) ▾

Count	drug_name_short
12.7K	OTHER
8.1K	ACETAMINOPHEN
8K	MAIN
5.8K	HEPARIN
5.8K	HYDROMORPHONE
5.7K	FENTANYL
4.6K	DOCUSATE
3.7K	PROPOFOL
3.7K	LIDOCAINE
3.4K	MIDAZOLAM
3.2K	OXYCODONE
3K	PANTOPRAZOLE
2.9K	LORAZEPAM

scroll down to see 87 more

drug_location_description — 0/100/2550 nodes — ↓ agg: count (global) ▾

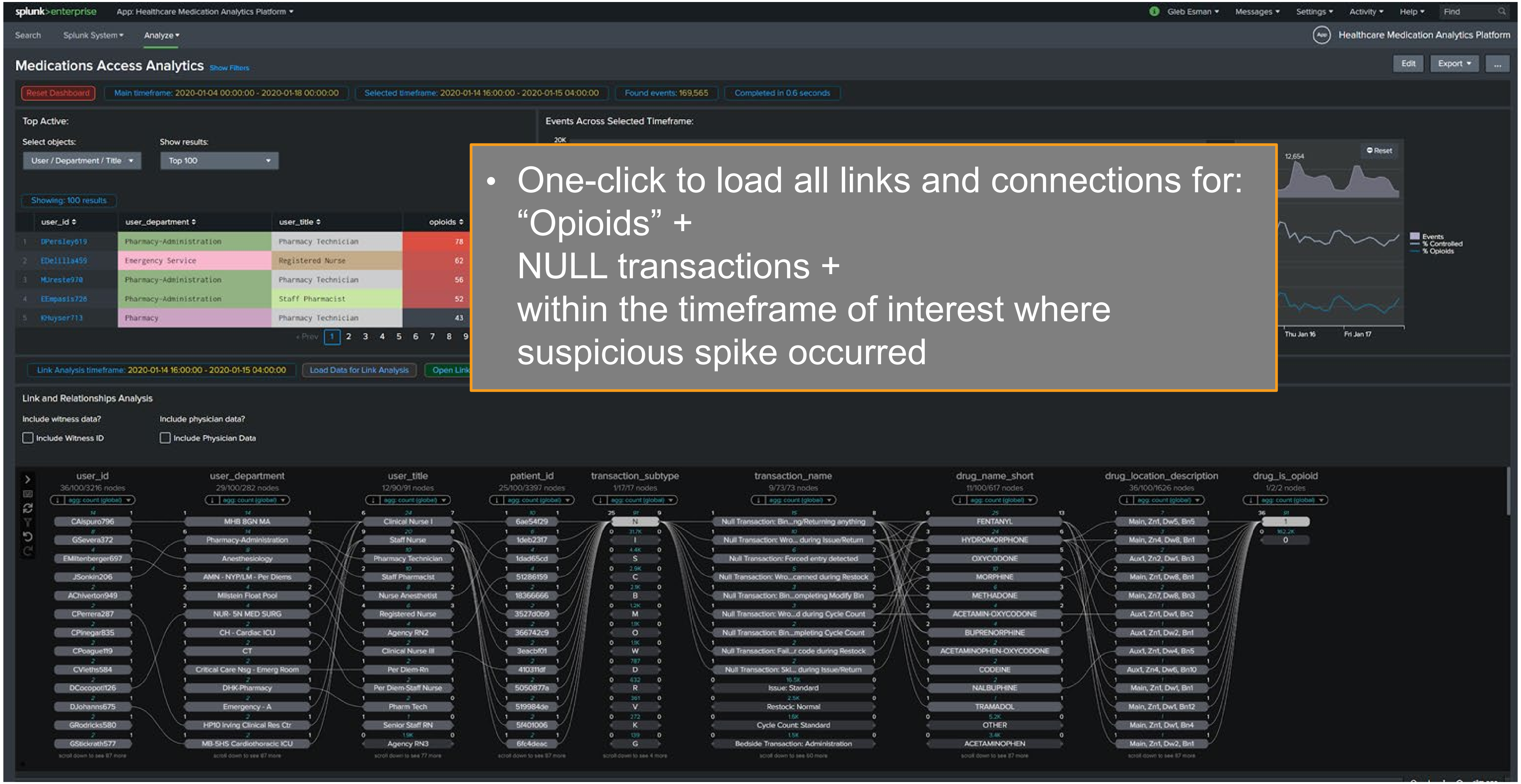
Count	drug_location_description
937	Main, Zn1, Dw2
881	Main, FlexLock #1
751	Main, Medication Refrigerator
748	Main, Zn2, Sh2, Bn2
730	Main, Zn2, Sh2, Bn1
616	Main, Zn1, Dw3
500	Main, Zn1, Dw8, Bn1
480	Main, Zn1, Dw3, Bn1
449	Main, Zn1, Dw3, Bn2
396	Main, Zn1, Dw4
389	Main, Refrigerator
383	Main, Zn1, Dw3, Bn3
373	Main, Zn1, Dw4, Bn2

scroll down to see 87 more

drug_is_opioid — 0/2/2 nodes — ↓ agg: count (global) ▾

Count	drug_is_opioid
434.9K	0
20.9K	1

Link Analysis: Detecting Opioid Diversion



Medications Access Analytics

Show Filters

Main timeframe: 2020-01-04 00:00:00 - 2020-01-18 00:00:00

Selected timeframe: 2020-01-14 16:00:00 - 2020-01-15 04:00:00

Found events: 169,565

Completed in 0.6 seconds

Top Active:

Select objects: User / Department / Title

Show results: Top 100

Events Across Selected Timeframe:

Showing: 100 results

	user_id	user_department	user_title	opioids
1	DPersley619	Pharmacy-Administration	Pharmacy Technician	78
2	EDellila459	Emergency Service	Registered Nurse	62
3	MUreste970	Pharmacy-Administration	Pharmacy Technician	56
4	EEmpasis726	Pharmacy-Administration	Staff Pharmacist	52
5	KHuyser713	Pharmacy	Pharmacy Technician	43

« Prev 1 2 3 4 5 6 7 8 9

Link Analysis timeframe: 2020-01-14 16:00:00 - 2020-01-15 04:00:00

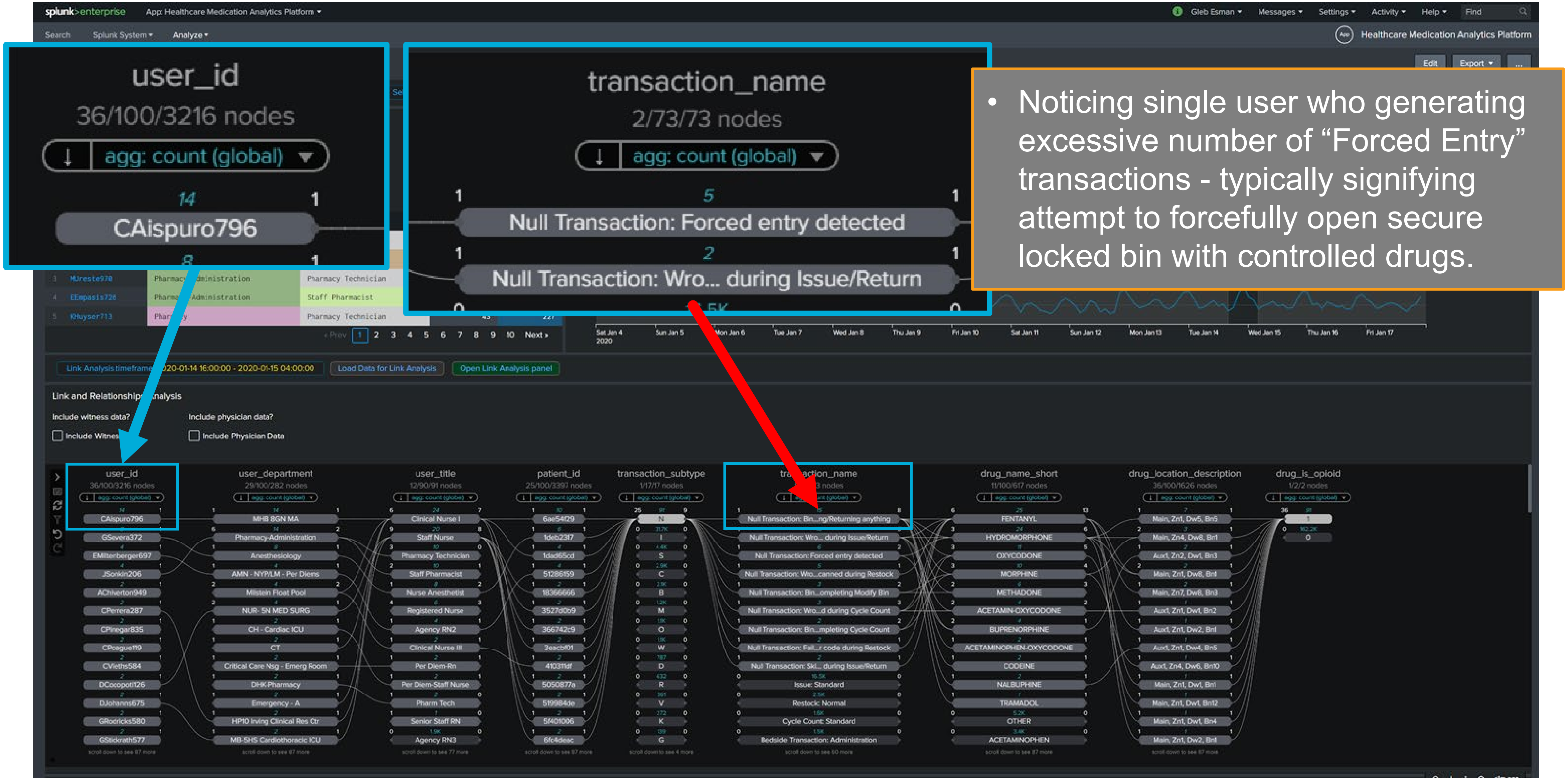
Link and Relationships Analysis

Include witness data? ☐ Include Witness ID

Include physician data? ☐ Include Physician Data

- One-click to load all links and connections for: “Opioids” +
  NULL transactions +
  within the timeframe of interest where suspicious spike occurred

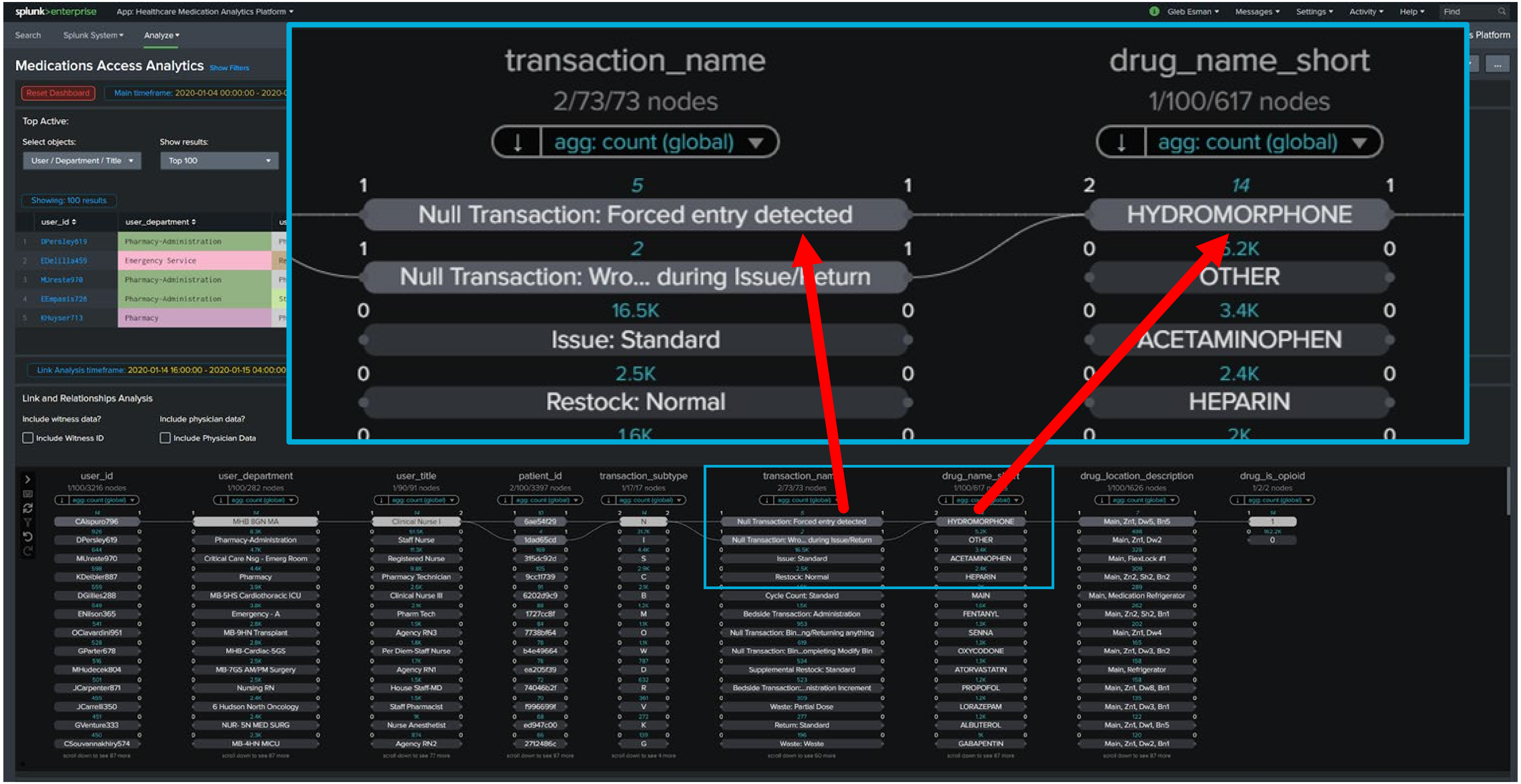
Link Analysis: Detecting Opioid Diversion



- Noticing single user who generating excessive number of “Forced Entry” transactions - typically signifying attempt to forcefully open secure locked bin with controlled drugs.

splunk> .conf20

Link Analysis: Detecting Opioid Diversion



splunk>enterprise App: Healthcare Medication Analytics Platform ▾

Search | Splunk System ▾ | Analyze ▾

Medications Access Analytics

Show Filters

Reset Dashboard

Main timeframe: 2020-01-04 00:00:00 - 2020-0

Top Active:

Select objects: User / Department / Title ▾

Show results: Top 100

Showing: 100 results

	user_id ⇕	user_department ⇕	us
1	DPersley619	Pharmacy-Administration	Ph
2	EDellila459	Emergency Service	Re
3	MUreste970	Pharmacy-Administration	Ph
4	EEmpasis726	Pharmacy-Administration	St
5	KHuyser713	Pharmacy	Ph

Link Analysis timeframe: 2020-01-14 16:00:00 - 2020-01-15 04:00:00

Link and Relationships Analysis

Include witness data? ☐ Include Witness ID

Include physician data? ☐ Include Physician Data

Key Takeaways

1. Many link analysis visualization options for Splunk
2. SigBay Link Analysis Viz App allows for sophisticated, interactive investigations within the large datasets without need to write complex SPL queries.
3. Other link visualization options onSplunkbase, but may require data manipulation/reduction for concise view.

More Information?

Links

- Force Directed App https://splunkbase.splunk.com/app/3767/
- Network Diagram Viz https://splunkbase.splunk.com/app/4438/
- Sigbay Link Analysis https://splunkbase.splunk.com/app/5126/#/details
- Eventstats https://docs.splunk.com/Documentation/Splunk/8.0.5/SearchReference/Eventstats
- Link Analysis App for Splunk (.Conf19) https://splunkbase.splunk.com/app/4676/#/details
- .Conf19 BOTS, The Missing Link https://conf.splunk.com/watch/conf-online.html?search=bots%20the%20missing%20link#/
- Splunk Blog posts https://www.splunk.com/en_us/blog

Thank You

Please provide feedback via the

SESSION SURVEY