

Making Sense of Web Fraud With Splunk Stream

An in-depth look at Stream use cases and customer success stories with a focus on stream:http

Jim Apger | Minister of Mayhem – Senior Security Architect

Matthew Joseff | Minister of Reality – Security Architect

Beau Morgan | Senior Sales Engineer

September 28, 2017 | Washington, DC

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance 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 could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. 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 functionality described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2017 Splunk Inc. All rights reserved.

Agenda

Making Sense of Web Fraud with Splunk Stream

- ▶ Introductions
- ▶ Stream Architecture
- ▶ Web Fraud Detection
- ▶ Customer Success



```
130.60.4 - - [07/Jun 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.20
128.241.220.82 - - [07/Jun 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=FL-SW-01" "Opera/9.80.20
317.27.160.0.0 - - [07/Jun 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01" "Opera/9.80.20
130.60.4 - - [07/Jun 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.20
128.241.220.82 - - [07/Jun 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=FL-SW-01" "Opera/9.80.20
317.27.160.0.0 - - [07/Jun 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01" "Opera/9.80.20
130.60.4 - - [07/Jun 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.20
128.241.220.82 - - [07/Jun 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=FL-SW-01" "Opera/9.80.20
317.27.160.0.0 - - [07/Jun 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01" "Opera/9.80.20
```

What is Stream?

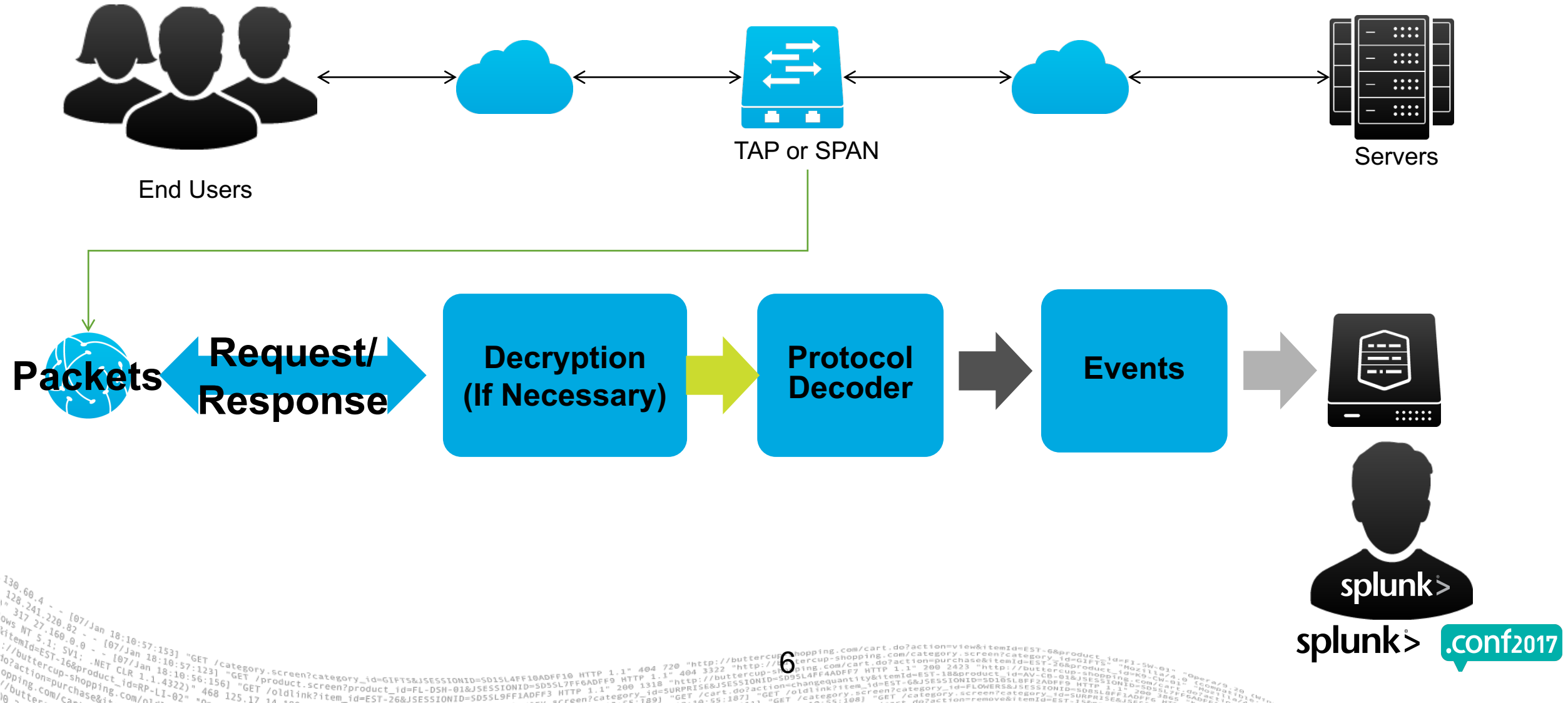
What is rē(ə)l 'tīm/?

Time is a Nonrenewable Resource

<i>Layer</i>	<i>Examples</i>
7. Application	HTTP, SMTP
6. Presentation	TLS
5. Session	SCP
4. Transport	TCP, UDP
3. Network	IPv4, IPv6
2. Data Link	Ethernet
1. Physical	Ethernet, WiFi



Wire Data Collection / Metadata Generation



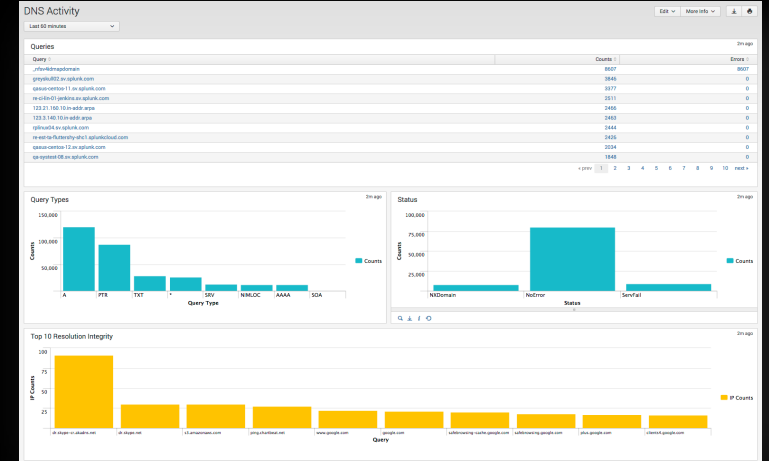
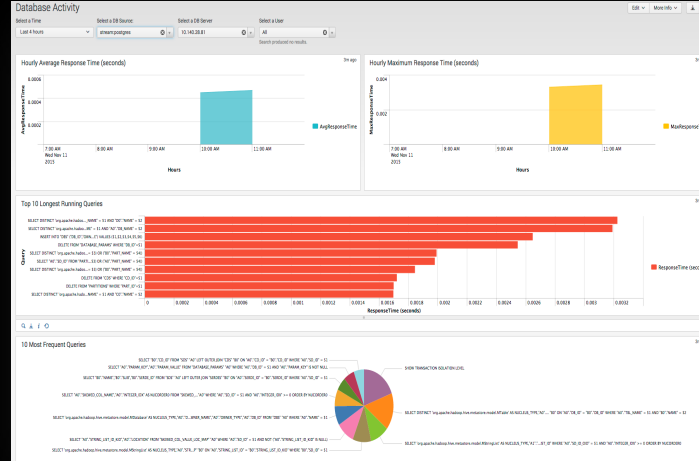
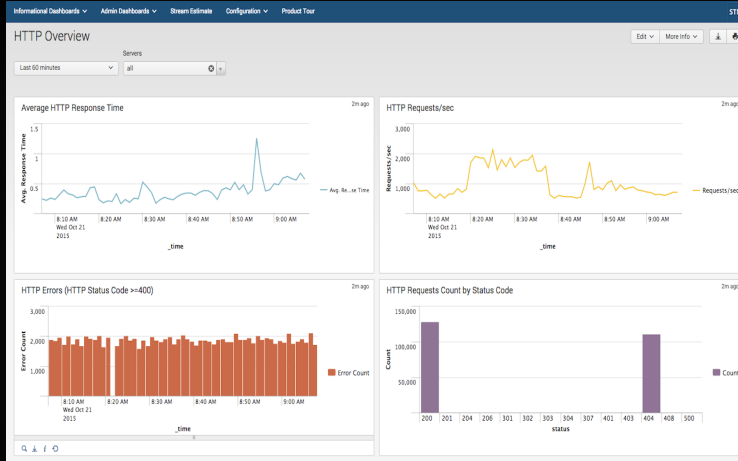
Example of Applications in Search

`sourcetype=stream:* | stats count by app`

amazon_aws	31	krb5	30
apple	5	live_hotmail	6
apple_location	2	norton_update	5
dhcp	6	ntp	2
facebook	6	ocsp	81
flickr	1	pinterest	1
google	58	skype	1411
google_analytics	4	smb	12
google_gen	29	spdy	4
google_safebrowsing	8	spotify	3
google_tags	3	teredo	15
gstatic	11	tumblr	28
http	7945	twitter	11
http2	11	yahoo	129
https	214	yahoo_search	1
icloud	8	ymsg_webmessenger	3
imgur	9	youtube	1

Prebuilt Reporting

What does real time mean to you?



Get visibility into applications performance and user experience

Understand database activity and performance without impacting database operation

Improve security and application intelligence with DNS analytics

Web Fraud Detection With Stream

Using Stream to “sessionize” clicks into complete web clickstreams

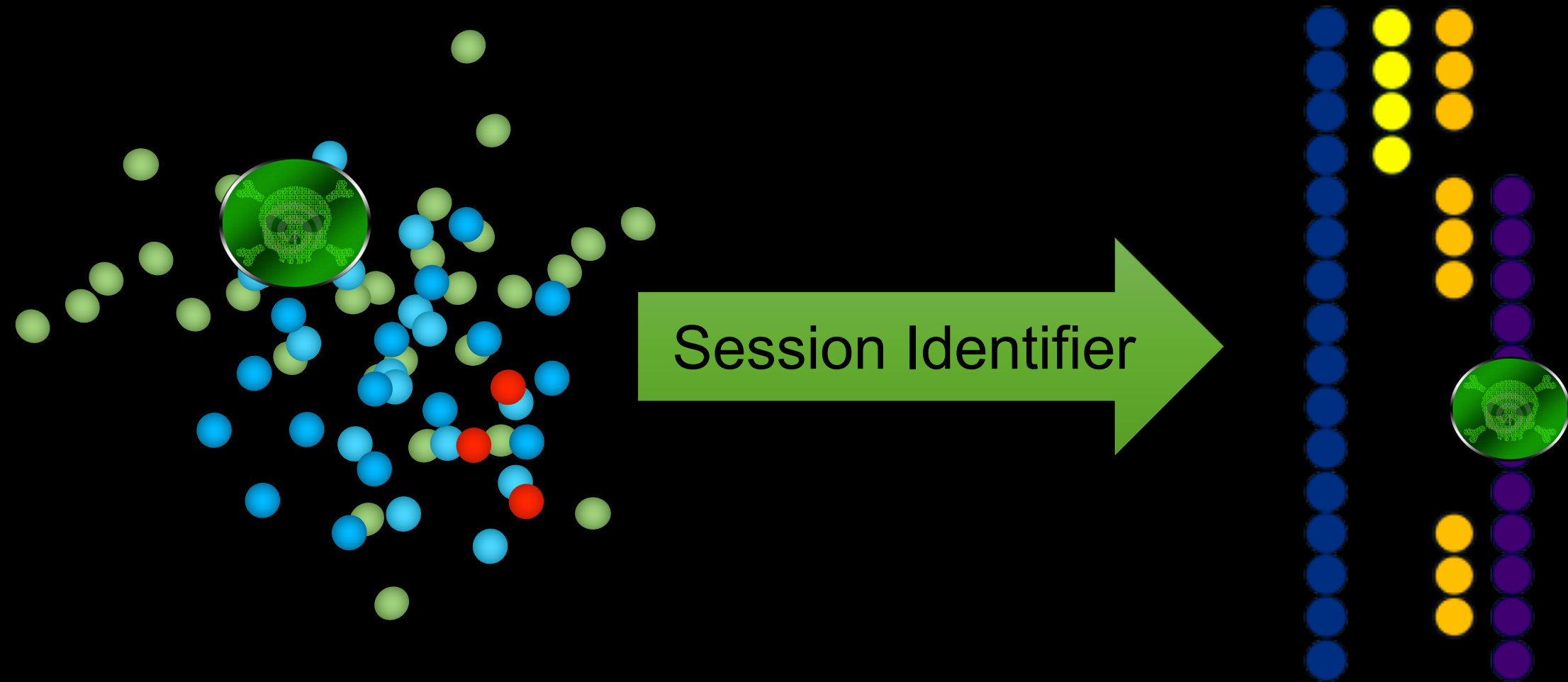
A speedometer with a black face and white markings, surrounded by intense orange and yellow flames. The needle is red and points to approximately 240 km/h. The scale ranges from 0 to 240 km/h. There are two odometer displays: the top one shows '258911' and the bottom one shows '8295'. The unit 'km/h' is printed at the bottom. The entire speedometer is engulfed in a large, swirling fire.

-
- A speedometer with a black face and white markings, surrounded by intense orange and yellow flames. The needle is red and points to approximately 240 km/h. The scale ranges from 0 to 240 km/h. There are two odometer displays: the top one shows '258911' and the bottom one shows '8295'. The unit 'km/h' is printed at the bottom. The entire speedometer is engulfed in a large, swirling fire.



- ▶ Session Analytics
- ▶ History (1st time X)
- ▶ Outliers
- ▶ Risk

“Sessionizing” 101



From this mess of **clicks**

To these nice **clickstreams**

“Sessionizing” 101



SessionID is changing!

Login Page Click

SessionID=1234,5678

Username=Newman

LoginSucess=1

Pre-Login Clicks

SessionID=1234

Post Login Clicks

SessionID=5678,9012

CheckOut Clicks

SessionID=9012

OrderTotal=\$435.23

CCNum-<hash>

“Sessionizing” 101



session

111

222

sessionID

2222

3333

sessionID

3333

4444

Pro Tip: the "transaction" command will accept a multivalue field and will link on ****any**** of the specified field values

1111

2222

3333

4444

|transaction sessionId

“Sessionizing” 101

|rex field=cookie max_match=5 "fronten[^=]+=(<?splSessionid>\w+)"

cookie	splSessionid	uri_path
splunkweb_csrf_token_8000=10728691767422127257; session_id_8000=7bb05c7a397f69c0f30da27f6458650335058957; splunkd_8000=A5qt6zPKN10Vymy5DMljpAztPvDYAZN7kMtqPllciAltppPEjBstsjeM7jzRDOEutbzEPKb*UHxoaCk28_ih6Rpo_E0Gk68Zz_zme5*YWRjtnJN_TN0Gwd5KqExmCu3c26_bo3K; frontend_cid=kXXDzuPBnbCbBhdf; frontend=ir0r7uv32qcur4ruefl2sc3946; external_no_cache=1	kXXDzuPBnbCbBhdf ir0r7uv32qcur4ruefl2sc3946	/index.php/customer/account/logout/
splunkweb_csrf_token_8000=10728691767422127257; session_id_8000=7bb05c7a397f69c0f30da27f6458650335058957; splunkd_8000=A5qt6zPKN10Vymy5DMljpAztPvDYAZN7kMtqPllciAltppPEjBstsjeM7jzRDOEutbzEPKb*UHxoaCk28_ih6Rpo_E0Gk68Zz_zme5*YWRjtnJN_TN0Gwd5KqExmCu3c26_bo3K; frontend_cid=kXXDzuPBnbCbBhdf; external_no_cache=1; frontend=hpuubppcprg1cb1pkju1g2ph14	kXXDzuPBnbCbBhdf hpuubppcprg1cb1pkju1g2ph14	/index.php/customer/account/logoutSuccess/
splunkweb_csrf_token_8000=10728691767422127257; session_id_8000=7bb05c7a397f69c0f30da27f6458650335058957; splunkd_8000=A5qt6zPKN10Vymy5DMljpAztPvDYAZN7kMtqPllciAltppPEjBstsjeM7jzRDOEutbzEPKb*UHxoaCk28_ih6Rpo_E0Gk68Zz_zme5*YWRjtnJN_TN0Gwd5KqExmCu3c26_bo3K; frontend_cid=kXXDzuPBnbCbBhdf; external_no_cache=1; frontend=hpuubppcprg1cb1pkju1g2ph14	kXXDzuPBnbCbBhdf hpuubppcprg1cb1pkju1g2ph14	/index.php/customer/account/login/
splunkweb_csrf_token_8000=10728691767422127257; session_id_8000=7bb05c7a397f69c0f30da27f6458650335058957; splunkd_8000=A5qt6zPKN10Vymy5DMljpAztPvDYAZN7kMtqPllciAltppPEjBstsjeM7jzRDOEutbzEPKb*UHxoaCk28_ih6Rpo_E0Gk68Zz_zme5*YWRjtnJN_TN0Gwd5KqExmCu3c26_bo3K; frontend_cid=kXXDzuPBnbCbBhdf; external_no_cache=1; frontend=hpuubppcprg1cb1pkju1g2ph14	kXXDzuPBnbCbBhdf hpuubppcprg1cb1pkju1g2ph14	/index.php/customer/account/loginPost/
splunkweb_csrf_token_8000=10728691767422127257; session_id_8000=7bb05c7a397f69c0f30da27f6458650335058957; splunkd_8000=A5qt6zPKN10Vymy5DMljpAztPvDYAZN7kMtqPllciAltppPEjBstsjeM7jzRDOEutbzEPKb*UHxoaCk28_ih6Rpo_E0Gk68Zz_zme5*YWRjtnJN_TN0Gwd5KqExmCu3c26_bo3K; frontend_cid=kXXDzuPBnbCbBhdf; external_no_cache=1; frontend=hpuubppcprg1cb1pkju1g2ph14	kXXDzuPBnbCbBhdf hpuubppcprg1cb1pkju1g2ph14	/index.php/customer/account/login/
splunkweb_csrf_token_8000=10728691767422127257; session_id_8000=7bb05c7a397f69c0f30da27f6458650335058957; splunkd_8000=A5qt6zPKN10Vymy5DMljpAztPvDYAZN7kMtqPllciAltppPEjBstsjeM7jzRDOEutbzEPKb*UHxoaCk28_ih6Rpo_E0Gk68Zz_zme5*YWRjtnJN_TN0Gwd5KqExmCu3c26_bo3K; frontend_cid=kXXDzuPBnbCbBhdf; external_no_cache=1; frontend=hpuubppcprg1cb1pkju1g2ph14	kXXDzuPBnbCbBhdf hpuubppcprg1cb1pkju1g2ph14	/index.php/customer/account/loginPost/
splunkweb_csrf_token_8000=10728691767422127257; session_id_8000=7bb05c7a397f69c0f30da27f6458650335058957; splunkd_8000=A5qt6zPKN10Vymy5DMljpAztPvDYAZN7kMtqPllciAltppPEjBstsjeM7jzRDOEutbzEPKb*UHxoaCk28_ih6Rpo_E0Gk68Zz_zme5*YWRjtnJN_TN0Gwd5KqExmCu3c26_bo3K; frontend_cid=kXXDzuPBnbCbBhdf; external_no_cache=1; frontend=6g1dhc70eije6thr5emhgek313	kXXDzuPBnbCbBhdf 6g1dhc70eije6thr5emhgek313	/index.php/customer/account/
splunkweb_csrf_token_8000=10728691767422127257; session_id_8000=7bb05c7a397f69c0f30da27f6458650335058957; splunkd_8000=A5qt6zPKN10Vymy5DMljpAztPvDYAZN7kMtqPllciAltppPEjBstsjeM7jzRDOEutbzEPKb*UHxoaCk28_ih6Rpo_E0Gk68Zz_zme5*YWRjtnJN_TN0Gwd5KqExmCu3c26_bo3K; external_no_cache=1; frontend=6g1dhc70eije6thr5emhgek313	6g1dhc70eije6thr5emhgek313	/index.php/men.html

splunkweb_csrf_token_8000=10728691767422127257; session_id_8000=7bb05c7a397f69c0f30da27f6458650335058957; 6g1dhc70eije6thr5emhgek313 /index.php/men.html

Use Case: Profile Change + Large Purchase

Single Stream with Profile Edit and Large Purchase

cookie	spl_sessionid	uri_path	_time	splUsername	splPassword	splLoginTime	splProfileEditTime	splPurchaseTime	splGrandtotal
splunkweb_csrf_token_8000=8167458972397087860		/	2017-08-08 08:42:07.300						
splunkweb_csrf_token_8000=8167458972397087860; frontend=mh9f5ms81iarvrltg4jni5vl2	mh9f5ms81iarvrltg4jni5vl2	/index.php/customer/account/login/	2017-08-08 08:48:42.997						
splunkweb_csrf_token_8000=8167458972397087860; frontend=mh9f5ms81iarvrltg4jni5vl2	JFyxteppe6ytdD7F; frontend=mh9f5ms81iarvrltg4jni5vl2	/index.php/customer/account/loginPost/	2017-08-08 08:48:53.953	jim@jim.com	GreenTea	1502200133.953312			
splunkweb_csrf_token_8000=8167458972397087860; frontend=n6tfr23janodtbh3787ec5mj26	JFyxteppe6ytdD7F; n6tfr23janodtbh3787ec5mj26	/index.php/customer/account/	2017-08-08 08:48:54.097						
splunkweb_csrf_token_8000=8167458972397087860; frontend=n6tfr23janodtbh3787ec5mj26	JFyxteppe6ytdD7F; n6tfr23janodtbh3787ec5mj26	/index.php/customer/account/edit/	2017-08-08 08:49:05.155						
splunkweb_csrf_token_8000=8167458972397087860; frontend=n6tfr23janodtbh3787ec5mj26	JFyxteppe6ytdD7F; n6tfr23janodtbh3787ec5mj26	/index.php/customer/account/editPost/	2017-08-08 08:49:40.546				1502200180.546753		
splunkweb_csrf_token_8000=8167458972397087860; frontend=n6tfr23janodtbh3787ec5mj26	JFyxteppe6ytdD7F; n6tfr23janodtbh3787ec5mj26	/index.php/customer/account/	2017-08-08 08:49:40.677						
splunkweb_csrf_token_8000=8167458972397087860; frontend=n6tfr23janodtbh3787ec5mj26	n6tfr23janodtbh3787ec5mj26	/index.php/men.html	2017-08-08 08:49:50.024						
splunkweb_csrf_token_8000=8167458972397087860; frontend=n6tfr23janodtbh3787ec5mj26	n6tfr23janodtbh3787ec5mj26	/index.php/men.html	2017-08-08 08:49:57.610						
splunkweb_csrf_token_8000=8167458972397087860; frontend=n6tfr23janodtbh3787ec5mj26	n6tfr23janodtbh3787ec5mj26	/index.php/men.html	2017-08-08 08:50:03.279						
splunkweb_csrf_token_8000=8167458972397087860; frontend=n6tfr23janodtbh3787ec5mj26	n6tfr23janodtbh3787ec5mj26	/index.php/men/shirts.html	2017-08-08 08:50:06.728						
splunkweb_csrf_token_8000=8167458972397087860; frontend=n6tfr23janodtbh3787ec5mj26	n6tfr23janodtbh3787ec5mj26	/index.php/men/shirts/plaid-cotton-shirt-485.html	2017-08-08 08:50:11.794						
splunkweb_csrf_token_8000=8167458972397087860; external_no_cache=1; frontend=n6tfr23janodtbh3787ec5mj26	n6tfr23janodtbh3787ec5mj26	/index.php/checkout/cart/	2017-08-08 08:50:30.119						
splunkweb_csrf_token_8000=8167458972397087860; frontend=n6tfr23janodtbh3787ec5mj26	JFyxteppe6ytdD7F; n6tfr23janodtbh3787ec5mj26	/index.php/checkout/onepage/	2017-08-08 08:50:51.682						
splunkweb_csrf_token_8000=8167458972397087860; frontend=n6tfr23janodtbh3787ec5mj26	JFyxteppe6ytdD7F; n6tfr23janodtbh3787ec5mj26	/index.php/checkout/onepage/saveBilling/	2017-08-08 08:52:31.700						
splunkweb_csrf_token_8000=8167458972397087860; frontend=n6tfr23janodtbh3787ec5mj26	JFyxteppe6ytdD7F; n6tfr23janodtbh3787ec5mj26	/index.php/checkout/onepage/getAdditional/	2017-08-08 08:52:31.813						
splunkweb_csrf_token_8000=8167458972397087860; frontend=n6tfr23janodtbh3787ec5mj26	JFyxteppe6ytdD7F; n6tfr23janodtbh3787ec5mj26	/index.php/checkout/onepage/progress/	2017-08-08 08:52:31.960						
splunkweb_csrf_token_8000=8167458972397087860; frontend=n6tfr23janodtbh3787ec5mj26	JFyxteppe6ytdD7F; n6tfr23janodtbh3787ec5mj26	/index.php/checkout/onepage/progress/	2017-08-08 08:52:32.074						
splunkweb_csrf_token_8000=8167458972397087860; frontend=n6tfr23janodtbh3787ec5mj26	JFyxteppe6ytdD7F; n6tfr23janodtbh3787ec5mj26	/index.php/checkout/onepage/saveShippingMethod/	2017-08-08 08:52:51.866						
splunkweb_csrf_token_8000=8167458972397087860; frontend=n6tfr23janodtbh3787ec5mj26	JFyxteppe6ytdD7F; n6tfr23janodtbh3787ec5mj26	/index.php/checkout/onepage/progress/	2017-08-08 08:52:51.975						
splunkweb_csrf_token_8000=8167458972397087860; frontend=n6tfr23janodtbh3787ec5mj26	JFyxteppe6ytdD7F; n6tfr23janodtbh3787ec5mj26	/index.php/checkout/onepage/progress/	2017-08-08 08:52:52.075						
splunkweb_csrf_token_8000=8167458972397087860; frontend=n6tfr23janodtbh3787ec5mj26	JFyxteppe6ytdD7F; n6tfr23janodtbh3787ec5mj26	/index.php/checkout/onepage/savePayment/	2017-08-08 08:53:37.087					1,865.22	
splunkweb_csrf_token_8000=8167458972397087860; frontend=n6tfr23janodtbh3787ec5mj26	JFyxteppe6ytdD7F; n6tfr23janodtbh3787ec5mj26	/index.php/checkout/onepage/progress/	2017-08-08 08:53:37.207						
splunkweb_csrf_token_8000=8167458972397087860; frontend=n6tfr23janodtbh3787ec5mj26	JFyxteppe6ytdD7F; n6tfr23janodtbh3787ec5mj26	/index.php/checkout/onepage/saveOrder	2017-08-08 08:53:49.404						
splunkweb_csrf_token_8000=8167458972397087860; frontend=n6tfr23janodtbh3787ec5mj26	JFyxteppe6ytdD7F; n6tfr23janodtbh3787ec5mj26	/index.php/checkout/onepage/success/	2017-08-08 08:53:49.558				1502200429.558113		
splunkweb_csrf_token_8000=8167458972397087860; frontend=n6tfr23janodtbh3787ec5mj26	n6tfr23janodtbh3787ec5mj26	/index.php/	2017-08-08 08:54:10.021						

Use Case: Profile Change + Large Purchase

GOAL: Find a profile change occurring before a large purchase

```
index=wiredata dest_port=80 OR dest_port=443 http_content_type="text/html; charset=UTF-8"
[search index=wiredata sourcetype=stream:http dest_port=80 OR dest_port=443 splGrandtotal="*"
http_content_type="text/html; charset=UTF-8" |fields splGrandtotal src_ip|rex field=splGrandtotal mode=sed
"s/,/"|where splGrandtotal > 500|stats values(src_ip) as src_ip]
|reverse
|table _time cookie uri_path splGrandtotal splUsername
|rex field=cookie max_match=5 "fronten[^=]+= (?<splSessionid>\w+)"
|eval splLoginTime=if(uri_path="/index.php/customer/account/loginPost/",_time,NULL)
|eval splPurchaseTime=if(uri_path="/index.php/checkout/onepage/success/",_time,NULL)
|eval splProfileEditTime=if(uri_path="/index.php/customer/account/editPost/",_time,NULL)
|rex field=splGrandtotal mode=sed "s/,/"
|transaction splSessionid maxpause=20m maxspan=2h
|where splProfileEditTime < splPurchaseTime AND splGrandtotal > 500
|eval PurchaseTime=strftime(splPurchaseTime,"%F %T")
|eval LoginTime=strftime(splLoginTime,"%F %T")
|eval ProfileEditTime=strftime(splProfileEditTime,"%F %T")
|table splUsername duration PurchaseTime LoginTime ProfileEditTime splGrandtotal splSessionid uri_path
```

Use Case: Profile Change + Large Purchase

GOAL: Find a profile change occurring before a large purchase

```
index=wiredata dest_port=80 OR dest_port=443 http_content_type="text/html; charset=UTF-8"
[search index=wiredata sourcetype=stream:http dest_port=80 OR dest_port=443 splGrandtotal="*"
http_content_type="text/html; charset=UTF-8" |fields splGrandtotal src_ip|rex field=splGrandtotal mode=sed
"s/,/"|where splGrandtotal > 500|stats values(src_ip) as src_ip]
|reverse
|table _time cookie uri_path splGrandtotal splUsername
|rex field=cookie max_match=5 "fronten[^=]+=(<splSessionid>\w+)"
|eval splLoginTime=if(uri_path="/index.php/customer/account/loginPost/",_time,NULL)
|eval splPurchaseTime=if(uri_path="/index.php/checkout/onepage/success/",_time,NULL)
|eval splProfileEditTime=if(uri_path="/index.php/customer/account/editPost/",_time,NULL)
|rex field=splGrandtotal mode=sed "s/,/"
|transaction splSessionid maxpause=20m maxspan=2h
|where splProfileEditTime < splPurchaseTime AND splGrandtotal > 500
|eval PurchaseTime=strftime(splPurchaseTime,"%F %T")
|eval LoginTime=strftime(splLoginTime,"%F %T")
|eval ProfileEditTime=strftime(splProfileEditTime,"%F %T")
|table splUsername duration PurchaseTime LoginTime ProfileEditTime splGrandtotal splSessionid uri_path
```

Use Case: Profile Change + Large Purchase

GOAL: Find a profile change occurring before a large purchase

index=wiredata dest_port=80 OR dest_port=443 http_content_type="text/html; charset=UTF-8"

splUsername	duration	ProfileEditTime	PurchaseTime	LoginTime	splGrandtotal	splSessionid	uri_path
jim@jim.com	327.024214	2017-08-08 08:49:40	2017-08-08 08:53:49	2017-08-08 08:48:53	1865.22	JFyxtpege6ytdD7F mh9f5ms81iarvrjltg4jni5vl2 n6tfr23janodtbh3787ec5mj26	/index.php/ /index.php/checkout/cart/ /index.php/checkout/cart/add /uenc/aHR0cDovL21hZ2VudG8ubGVmdG92ZXJmdW5rLmNvbS9pbmRleC5waHAybWVuL3NoaXJ /product/404/form_key/xdPhUV05ng1bFdji/ /index.php/checkout/onepage/ /index.php/checkout/onepage/getAdditional/ /index.php/checkout/onepage/progress/ /index.php/checkout/onepage/saveBilling/ /index.php/checkout/onepage/saveOrder/form_key/xdPhUV05ng1bFdji/ /index.php/checkout/onepage/savePayment/ /index.php/checkout/onepage/saveShippingMethod/ /index.php/checkout/onepage/success/ /index.php/customer/account/ /index.php/customer/account/edit/ /index.php/customer/account/editPost/ /index.php/customer/account/login/ /index.php/customer/account/loginPost/ /index.php/men.html /index.php/men/shirts.html /index.php/men/shirts/plaid-cotton-shirt-485.html

eval ProfileEditTime=strftime(splProfileEditTime,"%F %T")

table splUsername duration PurchaseTime LoginTime ProfileEditTime splGrandtotal splSessionid uri_path

Use Case: Profile Change + Large Purchase

splUsername	duration	ProfileEditTime	PurchaseTime	LoginTime	splGrandtotal	splSessionid	uri_path
MihajloPupin@att.net	177.637588		2017-08-10 19:16:36	2017-08-10 19:14:37	731.53	Neur8e0ielNnUFT1 dnlchj0183st2lttn9dg0fgi14 jnrV2df7h4rsg49tjbnik5dhr2	/index.php/ /index.php/checkout/cart/ /index.php/checkout/cart/add /uenc/aHR0cDovL21hZ2VudG8ubGVmdG92ZXJmdW5rLmNvbS9pbmRleC5waHAvG9tZS1kZWVnci9 /445/form_key/DqFP562FbcMc1Ubg/ /index.php/checkout/onepage/ /index.php/checkout/onepage/getAdditional/
LoniLove@aol.com	135.846551		2017-08-10 19:13:17	2017-08-10 19:11:10	774.88	6kq2urt4c3ll6vmcvrfn1djin13 l2mpA2sJGE32FDcj kffid94ine4pu7ujs9t6kg8263	/index.php/ /index.php/checkout/cart/ /index.php/checkout/cart/add/uenc/aHR0cDovL21hZ2VudG8ubGVmdG92ZXJmdW5rLmNvbS9pbmR /XUqlynJLqZQp2mLv/ /index.php/checkout/onepage/ /index.php/checkout/onepage/getAdditional/
GeorgeWestinghouse@yahoo.com	187.132008		2017-08-10 19:10:39	2017-08-10 19:07:43	541.55	VvW58CQjx5MzpoBZ kpcikdaqvncrfs6suf80vo7g50 tph1ccml9i81pa77qavtph1dp5	/index.php/ /index.php/checkout/cart/ /index.php/checkout/cart/add /uenc/aHR0cDovL21hZ2VudG8ubGVmdG92ZXJmdW5rLmNvbS9pbmRleC5waHAvbWVuL2JsYXplcnk /407/form_key/pPhbH9FSyJRyMVkx/ /index.php/checkout/onepage/ /index.php/checkout/onepage/getAdditional/
LeeForest@gmail.com	219.195976		2017-08-10 19:07:06	2017-08-10 19:04:50	552.71	4por7icd9eggmcgrjbuovoc9p7 mghlr03lv11cmqek00lp57fp14 paWBa1NNAqou5lfw	/index.php/ /index.php/accessories/jewelry.html /index.php/checkout/cart/ /index.php/checkout/cart/add /uenc/aHR0cDovL21hZ2VudG8ubGVmdG92ZXJmdW5rLmNvbS9pbmRleC5waHAvbWVuL2JsYXplcnk /405/form_key/w25nVUb8hiOaOgKf/ /index.php/checkout/onepage/
MFaraday@aol.com	173.403543		2017-08-10 19:03:02	2017-08-10 19:00:19	487.36	g029fgieacgsvd456i4jof4ae1 k3srjh4pl6giueupdj1c15f0 quyHxySk69nK6d8R	/index.php/ /index.php/accessories/jewelry.html /index.php/accessories/jewelry/pearl-necklace-set-test.html /index.php/checkout/cart/ /index.php/checkout/cart/add /uenc/aHR0cDovL21hZ2VudG8ubGVmdG92ZXJmdW5rLmNvbS9pbmRleC5waHAvYWNjZXNzb3JpZXN /product/555/form_key/OI2mc3GZ4izU5IE4/
GuglielmoMarconi@yahoo.com	259.963875		2017-08-10 18:59:28	2017-08-10 18:55:22	541.88	abbvkr6dqj26hakg1qtoi82jg4 t8s86ctbfrf0mdq70qm7cgn4t3 vK8TFr9rVRUdrrnU	/index.php/ /index.php/accessories/jewelry.html /index.php/checkout/cart/ /index.php/checkout/cart/add/uenc/aHR0cDovL21hZ2VudG8ubGVmdG92ZXJmdW5rLmNvbS9pbmR /AcyqLV3iAOPUdC4/ /index.php/checkout/onepage/
GeorgeWestinghouse@yahoo.com GuglielmoMarconi@yahoo.com LeeForest@gmail.com	540.5895			2017-08-10 18:45:36 2017-08-10 18:45:18		1alv0j54e250pt1tefds4ug135 7vto4uls4u6j1g26d146eo6ha4 PFUvK3lmGwwVuYO	/ /admin /index.php/admin

Remove the 'where' constraint
Limit to 5 URIs to make pretty

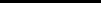
Use Case: Multiple Accounts -> Same Address

How does this happen?

- ▶ Account Take-Over
- ▶ Account Harvesting
- ▶ Often preceded by Account Peeking



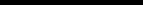
```
index=wireddata sourcetype="stream:http" dest_port=80 OR dest_port=443
[search index=wireddata sourcetype=stream:http dest_port=80 OR dest_port=443 splShippingStreet="*"
http_content_type="text/html; charset=UTF-8" |stats values(src_ip) as src_ip]
|fields splPurchaseTime splUsername splPassword splSessionid splGrandtotal splShipping* cookie uri_path dest_content
|rex field=cookie max_match=5 "fronten[^=]+= (?<splSessionid>\w+)"
|eval splPurchaseTime=if(uri_path="/index.php/checkout/onepage/success/",_time,NULL)
|rex field=dest_content "Your order # is:[^>]+> (?<splOrderNumber>[^>]+)<"
|reverse
|transaction splSessionid maxpause=10m maxspan=2h
|eval PurchaseTime=strftime(splPurchaseTime,"%F %T")
|stats list(splOrderNumber) as OrderNum list(splUsername) as Username list(splPassword) as Password
list(splShippingFirstname) as ShippingFirstname list(splShippingLastname) as ShippingLstname list(splShippingPhone) as
ShippingPhone list(PurchaseTime) as PurchaseTime count by splShippingStreet splShippingCity splShippingZip
splShippingCountry
|where count > 2
```



```
index=wireddata sourcetype="stream:http" dest_port=80 OR dest_port=443
[search index=wireddata sourcetype=stream:http dest_port=80 OR dest_port=443 splShippingStreet="*"
http_content_type="text/html; charset=UTF-8" |stats values(src_ip) as src_ip]
|fields splPurchaseTime splUsername splPassword splSessionid splGrandtotal splShipping* cookie uri_path dest_content
|rex field=cookie max_match=5 "fronten[^=]+= (?<splSessionid>\w+)"
|eval splPurchaseTime=if(uri_path="/index.php/checkout/onepage/success/",_time,NULL)
|rex field=dest_content "Your order # is:[^>]+> (?<splOrderNumber>[^>]+)<"
|reverse
|transaction splSessionid maxpause=10m maxspan=2h
|eval PurchaseTime=strftime(splPurchaseTime,"%F %T")
|stats list(splOrderNumber) as OrderNum list(splUsername) as Username list(splPassword) as Password
list(splShippingFirstname) as ShippingFirstname list(splShippingLastname) as ShippingLstname list(splShippingPhone) as
ShippingPhone list(PurchaseTime) as PurchaseTime count by splShippingStreet splShippingCity splShippingZip
splShippingCountry
|where count > 2
```



```
index=wiredata sourcetype="stream:http" dest_port=80 OR dest_port=443
[search index=wiredata sourcetype=stream:http dest_port=80 OR dest_port=443 splShippingStreet="*"
http_content_type="text/html; charset=UTF-8" |stats values(src_ip) as src_ip]
|fields splPurchaseTime splUsername splPassword splSessionid splGrandtotal splShipping* cookie uri_path dest_content
|rex field=cookie max_match=5 "fronten[^=]+= (?<splSessionid>\w+)"
|eval splPurchaseTime=if(uri_path="/index.php/checkout/onepage/success/",_time,NULL)
|rex field=dest_content "Your order # is:[^>]+> (?<splOrderNumber>[^>]+)<"
|reverse
|transaction splSessionid maxpause=10m maxspan=2h
|eval PurchaseTime=strftime(splPurchaseTime,"%F %T")
|stats list(splOrderNumber) as OrderNum list(splUsername) as Username list(splPassword) as Password
list(splShippingFirstname) as ShippingFirstname list(splShippingLastname) as ShippingLstname list(splShippingPhone) as
ShippingPhone list(PurchaseTime) as PurchaseTime count by splShippingStreet splShippingCity splShippingZip
splShippingCountry
|where count > 2
```



Use Case: Multiple Accounts -> Same Address

```

index=wiredata sourcetype="stream:http" dest_port=80 OR dest_port=443
[search index=wiredata sourcetype=stream:http dest_port=80 OR dest_port=443 splShippingStreet="*"
http_content_type="text/html; charset=UTF-8" |stats values(src_ip) as src_ip]
|fields splPurchaseTime splUsername splPassword splSessionid splGrandtotal splShipping* cookie uri_path dest_content
|rex field=cookie max_match=5 "fronten[^=]+=(?<splSessionid>\w+)"
|eval splPurchaseTime=if(uri_path="/index.php/checkout/onepage/success/",_time,NULL)
|rex field=dest_content "Your order # is:[^>]+>(?<splOrderNumber>[^>]+)<"
|reverse
|transaction splSessionid maxpause=10m maxspan=2h
|eval PurchaseTime=strftime(splPurchaseTime,"%F %T")
|stats list(splOrderNumber) as OrderNum list(splUsername) as Username list(splPassword) as Password
list(splShippingFirstname) as ShippingFirstname list(splShippingLastname) as ShippingLstname list(splShippingPhone) as
ShippingPhone list(PurchaseTime) as PurchaseTime count by splShippingStreet splShippingCity splShippingZip
splShippingCountry
|where count > 2

```

splShippingStreet	splShippingCity	splShippingZip	splShippingCountry	OrderNum	Username	Password	ShippingFirstname	ShippingLstname	ShippingPhone	PurchaseTime	count
200 Franklin St	Brooklyn	11222	US	145000022	MihajloPupin@att.net	IGotGame1858	Mihajlo	Pupin	(718) 389-3904	2017-08-10 19:16:36	6
				145000021	LoniLove@aol.com	ComedyCentralRox	Loni	Love	(718) 389-3904	2017-08-10 19:13:17	
				145000020	GeorgeWestinghouse@yahoo.com	ScrewThomasEdison	George	Westinghouse	(718) 389-3904	2017-08-10 19:10:39	
				145000019	LeeForest@gmail.com	SolidAsGranite	Lee	Forest	(718) 389-3904	2017-08-10 19:07:06	
				145000018	MFaraday@aol.com	KingOfEmag1791	Michael	Faraday	(718) 389-3904	2017-08-10 19:03:02	
				145000017	GuglielmoMarconi@yahoo.com	87d68bTT	Guglielmo	Marconi	(718) 389-3904	2017-08-10 18:59:28	

Customer Success With Stream

From Fraud to DevOps

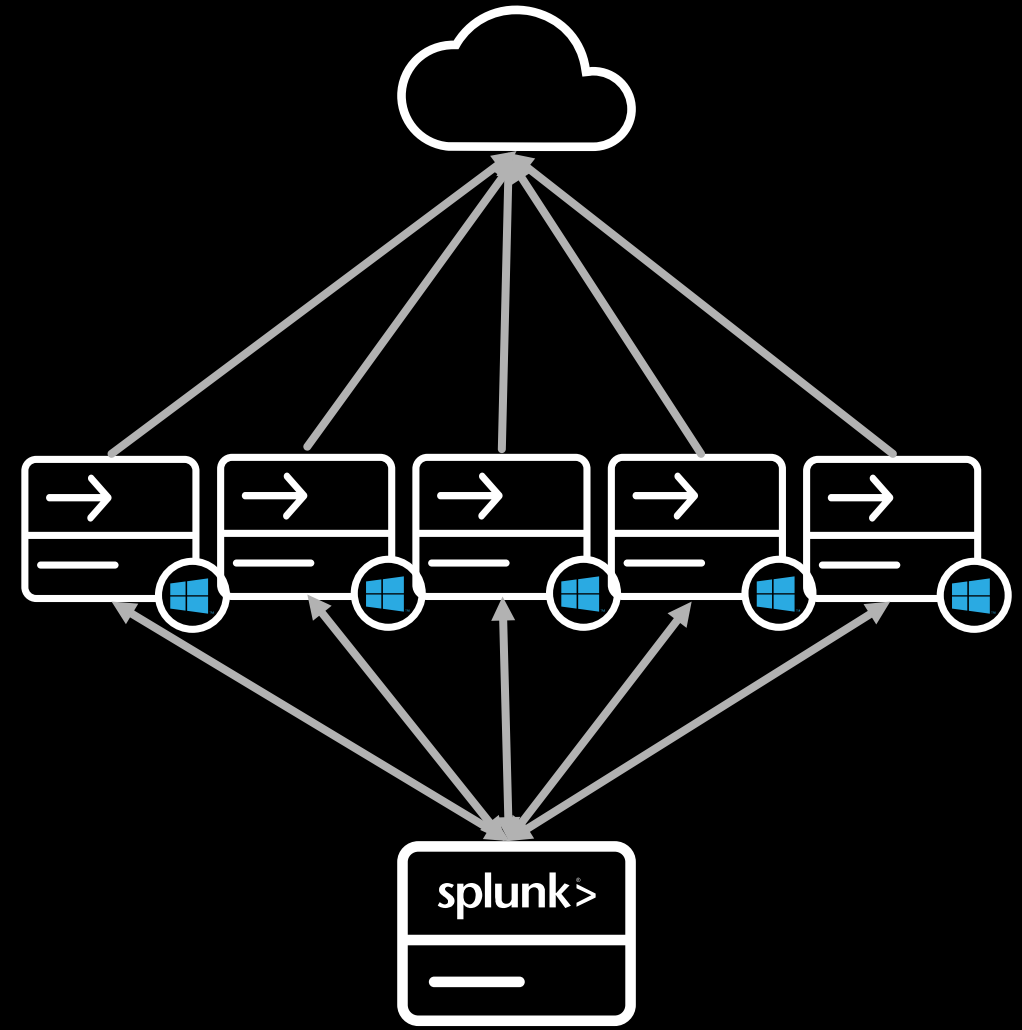
It all started with EASY fraud detection use cases...

- ▶ Single IP address using multiple user IDs
- ▶ Single user ID being accessed by < 3 IP addresses
- ▶ Multiple user IDs using the same CC number (hashed) for purchases
- ▶ Single user ID with multiple shipping addresses used
- ▶ Multiple user IDs using same complex password (hashed)
- ▶ User IDs created with email accounts with high shannon entropy scores

Customer Architecture

Deploying Stream with Splunk Cloud

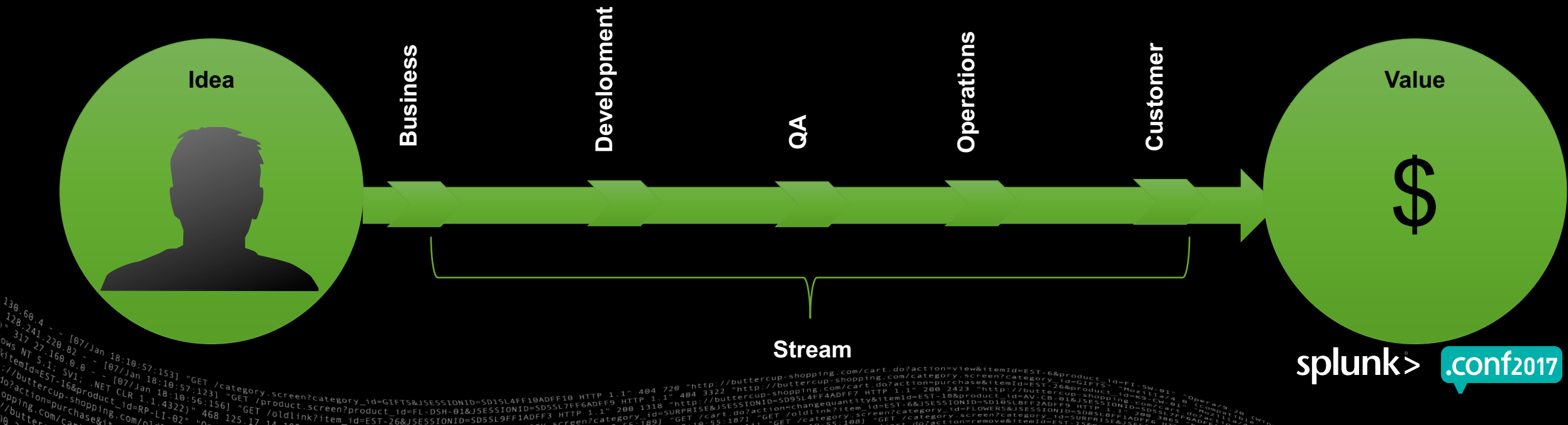
- ▶ Used Deployment Server to push out Splunk_TA_stream to 120+ webserver
- ▶ Configure Stream app on Deployment server for pushing stream configs
- ▶ Install Stream app on Cloud for dashboards
- ▶ Gathering data in minutes



DevOps Use Cases

Enter DevOps and stream:tds (Tabular Data Stream)

- ▶ Troubleshoot application calls to internal and 3rd party systems
- ▶ Real-time capacity planning for calls to 3rd party systems where license is usage based
- ▶ Provide visibility in transition to microservices architecture



“Stream is essential to any organization migrating to microservices”

What Now?

Call to Action

- ▶ Visit the Fraud Detection Booth in the source=*Pavilion
- ▶ Contact your Splunk representative for a **free** Fraud Workshop
- ▶ Attend the next Fraud talk: “Using Splunk for Retail Banking Cross Channel Fraud Analysis, Detection & Investigation” tomorrow, Thursday at 1135
- ▶ Schedule a BOTS 2.0 engagement: Now with Fraud use cases!

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01"
1317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D5SL7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01"
1317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=5D5SL7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01"
1317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=5D5SL7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01"
1317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=5D5SL7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01"
1317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=5D5SL7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01"
1317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=5D5SL7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01"
1317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=5D5SL7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01"
1317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=5D5SL7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01"

Thank You

Don't forget to **rate this session** in the
.conf2017 mobile app

splunk> .conf2017