Correlation Analysis

Document Usage Guidelines

- Should be used only for enrolled students
- Not meant to be a self-paced document, an instructor is needed
- Do not distribute

Course Goals

- Define correlation and co-occurrence
- Calculate co-occurrence between fields
- Analyze the relationship between variables
- Combine matching results from multiple queries

Course Outline

- Calculate Co-Occurrence Between Fields
- Analyze Multiple Datasets

Calculate Co-Occurrence Between Fields

Correlation vs. Co-occurrence

- Correlation is a statistical measure
- Measures how the changes in one variable are associated with the changes in another variable
- Typically used to analyze numerical data

- Co-occurrence is a measure of frequency
- Measures the frequency with which one or more events appear together in a dataset
- Can be used to analyze any type of data, even text-based

Co-Occurrence Analysis

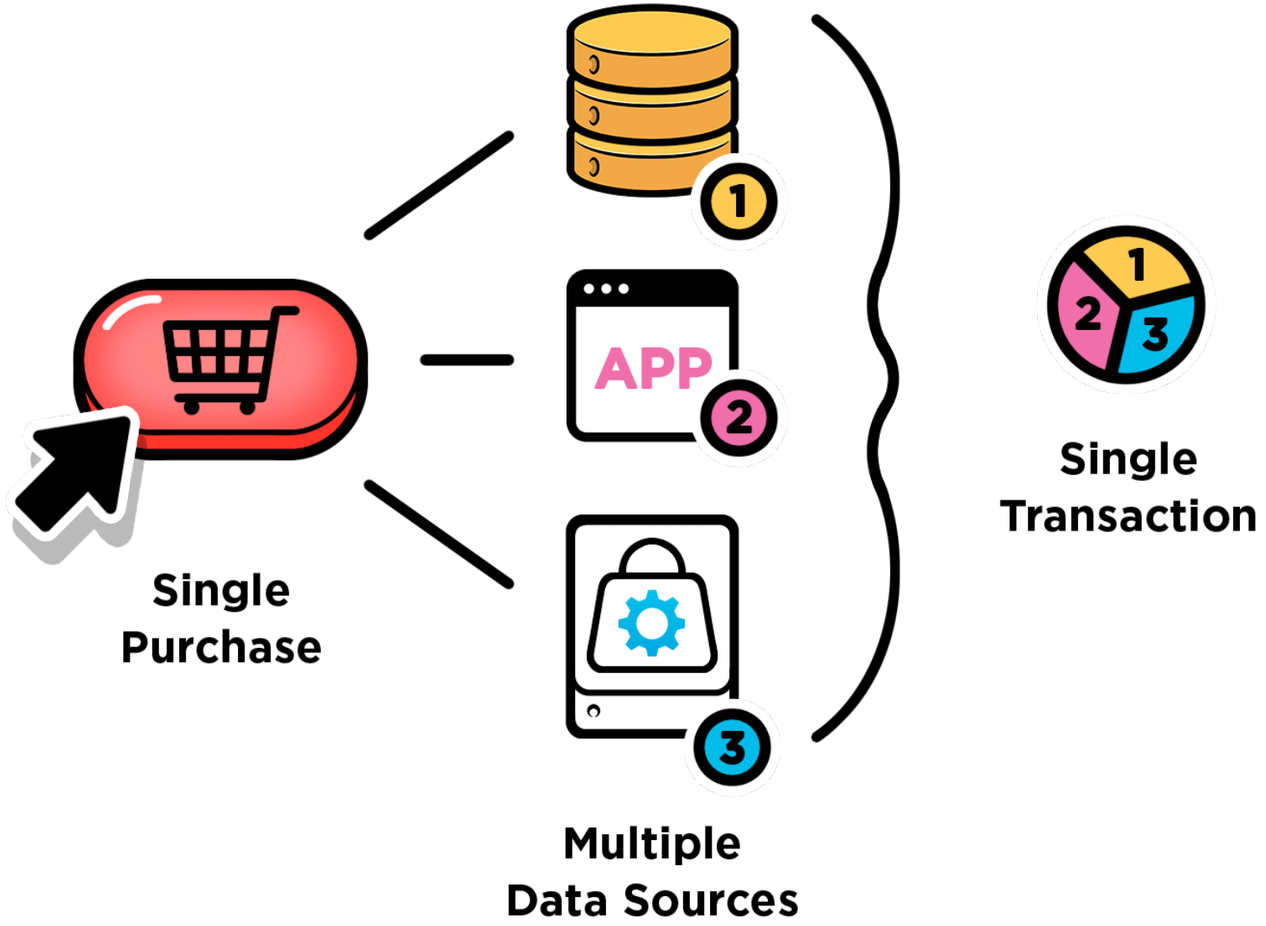
- Identifies patterns and relationships within your dataset
- Can provide actionable insights into the underlying structure of your dataset and help inform strategy development
- The commands taught in this course will help you identify relationships between fields, within a single dataset, and across multiple datasets

Topic Objectives

- Understand transactions
- Explore the **`transaction`** command

What are Transactions

A group of related events from one or many data sources



`transaction` Command

```
...| transaction (<field>|<field-list>) [options]
```

- Groups events that share one or more fields
  - Group events on values from **`<field>`**
  - Group events based on shared values from **`<field-list>`**
- Determine event grouping behavior using **`options`**:
  - Ranges of time: **`maxspan`**, **`maxpause`**
  - Maximum number of events in a transaction: **`maxevents`**
  - Text contained in the first/last events: **`startswith`**, **`endswith`**
- Adds **`duration`**, **`eventcount`**, and **`closed_txn`** fields to events

What Do Transactions Look Like?

```
index=web sourcetype=access_combined
```

Time	Event
4/30/21 6:23:23.000 PM	107.3.146.207 - - [30/Apr/2021:18:23:23] "POST /cart/success.do?JSESSIONID=SD6SL5FF8ADFF4951 HTTP 1.1" 200 2752 "http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-12" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 774 host = www3 source = /opt/log/www3/access.log sourcetype = access_combined
4/30/21 6:23:23.000 PM	107.3.146.207 - - [30/Apr/2021:18:23:23] "POST /cart.do?action=purchase&itemId=EST-12&JSESSIONID=SD6SL5FF8ADFF4951 HTTP 1.1" 200 2646 "http://www.buttercupgames.com/cart.do?action=addtocart&itemId=EST-12&categoryId=SHOOTER&productId=WC-SH-G04" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 848
4/30/21 6:23:19.000 PM	&JSESSIONID=SD6SL5FF8ADFF4951 HTTP 1.1" 200 1284 "http://www.buttercupgames.com/product.screen?productId=WC-SH-G04" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 974 host = www3 source = /opt/log/www3/access.log sourcetype = access_combined
4/30/21 6:23:15.000 PM	107.3.146.207 - - [30/Apr/2021:18:23:15] "GET /product.screen?productId=WC-SH-G04&JSESSIONID=SD6SL5FF8ADFF4951 HTTP 1.1" 200 1533 "http://www.buttercupgames.com/category.screen?categoryId=SHOOTER" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 146 host = www3 source = /opt/log/www3/access.log sourcetype = access_combined
4/30/21 6:22:36.000 PM	178.19.3.199 - - [30/Apr/2021:18:22:36] "GET /product.screen?productId=FI-AG-G08&JSESSIONID=SD9SL3FF1ADFF4956 HTTP 1.1" 200 929 "http://www.buttercupgames.com/cart.do?action=remove&itemId=EST-19&productId=FI-AG-G08" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)" 888 host = www3 source = /opt/log/www3/access.log sourcetype = access_combined
4/30/21 6:22:18.000 PM	178.19.3.199 - - [30/Apr/2021:18:22:18] "GET /category.screen?categoryId=STRATEGY&JSESSIONID=SD9SL3FF1ADFF4956 HTTP 1.1" 200 3879 "http://www.buttercupgames.com/product.screen?productId=PZ-SG-G05" "Mozilla/4.0 (c
4/30/21 6:22:07.000 PM	178.19.3.199 - - [30/Apr/2021:18:22:07] "POST /cart/success.do?JSESSIONID=SD9SL3FF1ADFF4956 HTTP 1.1" 200 928 "http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-21" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)" 554 host = www3 source = /opt/log/www3/access.log sourcetype = access_combined
4/30/21	178.19.3.199 - - [30/Apr/2021:18:22:07] "POST /cart.do?action=purchase&itemId=EST-21&JSESSIONID=SD9SL3FF1A

Events from one JSESSIONID

Events from another JESSIONID

```
index=web sourcetype=access_combined
| transaction JSESSIONID
```

Time	Event
4/30/21 6:23:15.000 PM	107.3.146.207 - - [30/Apr/2021:18:23:15] "GET /product.screen?productId=WC-SH-G04&JSESSIONID=SD6SL5FF8ADFF4951 HTTP 1.1" 200 1533 "http://www.buttercupgames.com/category.screen?categoryId=SHOOTER" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 146 107.3.146.207 - - [30/Apr/2021:18:23:19] "POST /cart.do?action=addtocart&itemId=EST-12&productId=WC-SH-G04&JSESSIONID=SD6SL5FF8ADFF4951 HTTP 1.1" 200 1284 "http://www.buttercupgames.com/product.screen?productId=WC-SH-G04" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 974 107.3.146.207 - - [30/Apr/2021:18:23:23] "POST /cart.do?action=purchase&itemId=EST-12&JSESSIONID=SD6SL5FF8ADFF4951 HTT... (KHTML, like Gecko) Chrome/19.0... 107.3.146.20... FF4951 HTTP 1.1" 200 2752 "http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-12" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 774 107.3.146.207 - - [30/Apr/2021:18:23:39] "GET /category.screen?categoryId=ARCADE&JSESSIONID=SD6SL5FF8ADFF4951 HTTP 1.1" 200 307 "http://www.buttercupgames.com/cart.do?action=changequantity&itemId=EST-6&productId=MB-AG-G07" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 138 Show all 8 lines host = www3 source = /opt/log/www3/access.log sourcetype = access_combined
4/30/21 6:21:43.000 PM	178.19.3.199 - - [30/Apr/2021:18:21:43] "GET /product.screen?productId=WC-SH-A02&JSESSIONID=SD9SL3FF1ADFF4956 HTTP 1.1" 200 2234 "http://www.buttercupgames.com/category.screen?categoryId=ACCESSORIES" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)" 204 178.19.3.199 - - [30/Apr/2021:18:21:48] "POST /cart.do?action=addtocart&itemId=EST-21&productId=WC-SH-A02&JSESSIONID=SD9SL3FF1ADFF4956 HTTP 1.1" 200 421 "http://www.buttercupgames.com/product.screen?productId=WC-SH-A02" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)" 429 178.19.3.199... DFF4956 HTTP... itemId=EST-21&categoryId=ACCESSORIE... .1; SV1)" 206 178.19.3.199... ADFF4956 HTTP 1.1" 200 2226 "http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-21" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)" 998 178.19.3.199 - - [30/Apr/2021:18:22:01] "GET /product.screen?productId=DB-SG-G01&JSESSIONID=SD9SL3FF1ADFF4956 HTTP 1.1" 200 1668 "http://www.buttercupgames.com/category.screen?categoryId=STRATEGY" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)" 778 Show all 10 lines

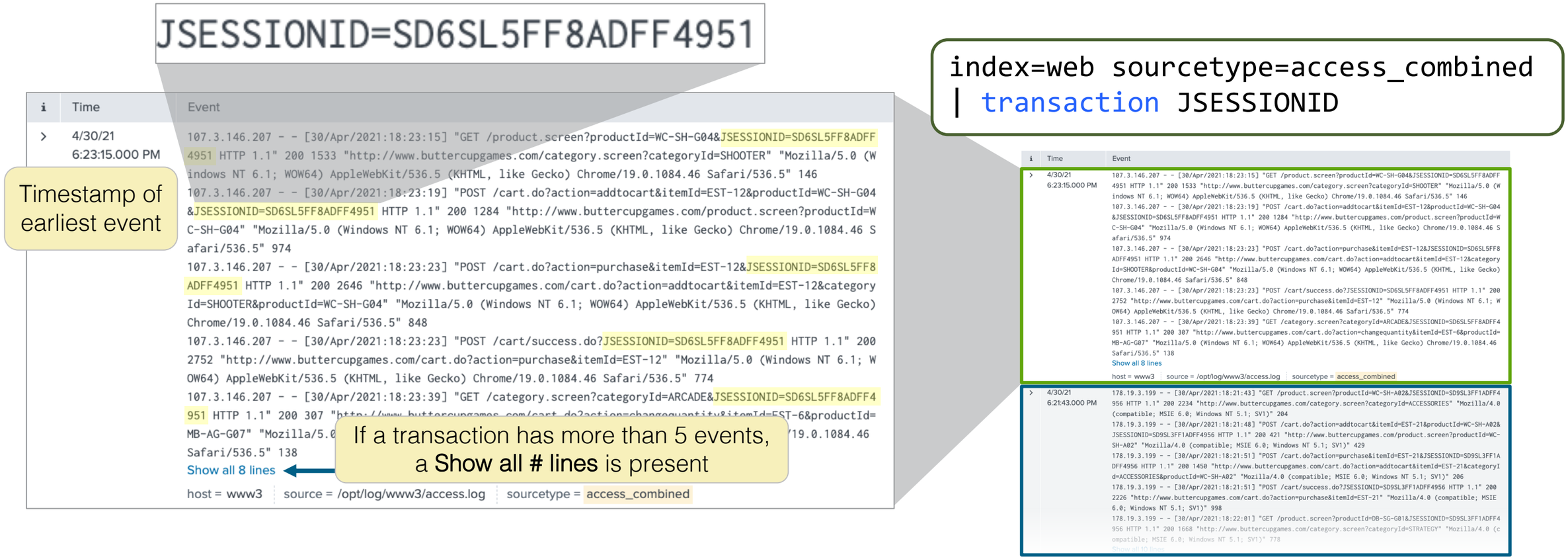
Transaction with multiple events from the most recent JSESSIONID

Transaction with multiple events from an earlier JSESSIONID

 | 6 March 2023

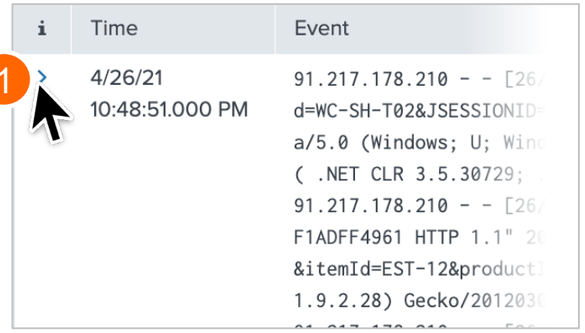
What Do Transactions Look Like? (cont.)

Contains the **_raw** field contents and the timestamp (time and date fields) of the earliest member



What Do Transactions Look Like? (cont.)

All other shared fields of a transaction are merged



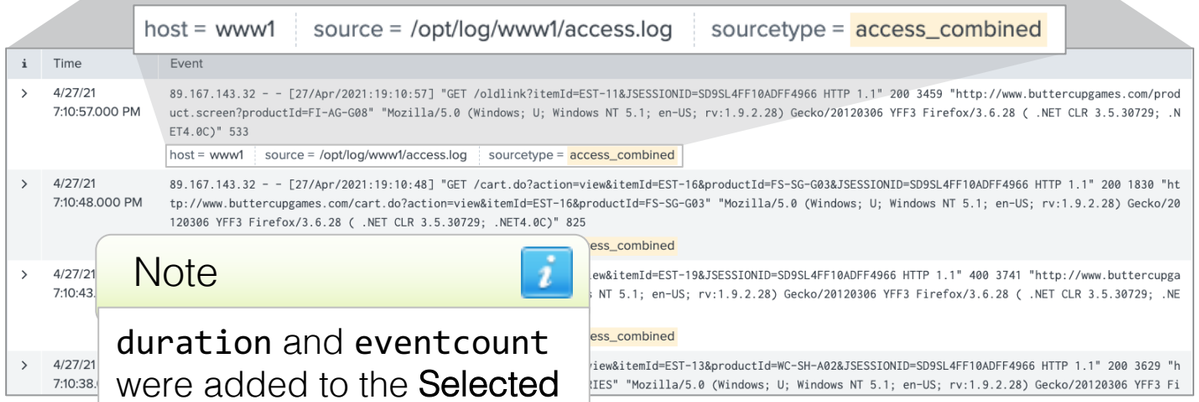
Type	Field	Value
Selected	categoryId	ACCESSORIES
		SHOOTER
	host	www3
	source	/opt/log/www3/access.log
	sourcetype	access_combined
	user	-
Event	Code	200
		500
	Description	Internal Server Error.
		OK.
	JSESSIONID	SD3SL9FF1ADFF4961
	action	addtocart
		changequantity
		purchase
		remove
		view
	bytes	1340

`Code` and `action` fields list the distinct values present in some or all the events

`duration` and `eventcount` Fields

- Added to raw events by **`transaction`** command
- **`duration`** represents the time difference, in seconds, between the first and last event timestamps
- **`eventcount`** is the number of events in the transaction

```
index=web sourcetype=access_combined
```



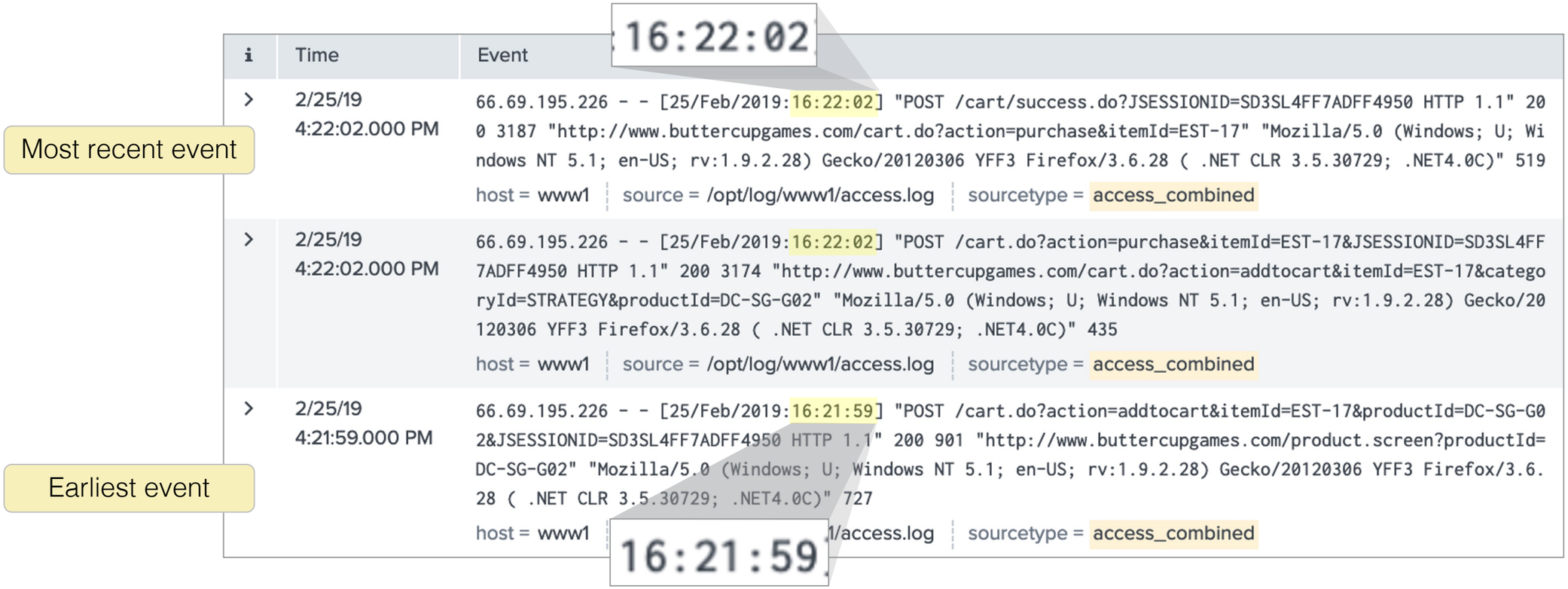
Note

`duration` and **`eventcount`** were added to the **Selected Fields** list for this example.

```
index=web sourcetype=access_combined
| transaction clientip
```

Ordering Events for `transaction`

`transaction` requires incoming events to be in reverse chronological order; if not, results may be misleading



Ordering Events for `transaction` (cont.)

- Transactions may not be grouped correctly if preceding commands change the event ordering
- Use the **`sort`** command with the **`_time`** field immediately before the **`transaction`** command to ensure correct event ordering

```
index=web sourcetype=access_combined
| ...
| sort -_time
| transaction JSESSIONID endswith=(status=503) maxevents=5
```

Warning

If the order of events has been changed in a way that would affect the **`transaction`** command, you will not see an error message!

`transaction` Command Example 1

- Use **`maxspan`** to control the maximum total time between the earliest and latest events; defaults to **`-1`** (no max time limit)
- Use **`maxpause`** to control the maximum total time between events; defaults to **`-1`** (no max time pause limit)

Scenario

Display customer actions on the website during the last 4 hours.

Note

`eval` command reformats duration as readable time HH:MM:SS.

```
index=web sourcetype=access_combined
| transaction clientip maxspan=180s maxpause=1m
| eval duration=tostring(duration,"duration")
| sort -duration
| table clientip duration
```

clientip	duration
194.215.205.19	00:03:00
86.9.190.90	00:03:00
178.162.239.192	00:02:44
89.11.192.18	00:02:42
141.146.8.66	00:02:39
89.106.20.218	00:02:39

`transaction` Command Example 2

Scenario

SecOps is trying to track an issue with the web servers in the online store. Over the last 24 hours, find 503 errors generated by user sessions in the online store, and display 4 related events before it.

Find related events that occur before a specific event using **`endswith`** and **`maxevents`**

```
index=web sourcetype=access_combined
| transaction JSESSIONID endswith=(status=503) maxevents=5
```

`JSESSIONID=SD2SL8FF3ADFF4963` `503`

2/12/18
2:12:22.000 PM

59.99.230.91 - - [12/Feb/2018:14:12:22] "POST /cart/success.do?JSESSIONID=SD2SL8FF3ADFF4963 HTTP 1.1" 200 1072 "http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-13" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 499 — 1st event (earliest)

59.99.230.91 - - [12/Feb/2018:14:12:39] "GET /oldlink?itemId=EST-15&JSESSIONID=SD2SL8FF3ADFF4963 HTTP 1.1" 200 998 "http://www.buttercupgames.com/product.screen?productId=DC-SG-G02" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 237 — 2nd event

59.99.230.91 - - [12/Feb/2018:14:12:52] "GET /product.screen?productId=WC-SH-A02&JSESSIONID=SD2SL8FF3ADFF4963 HTTP 1.1" 200 2678 "http://www.buttercupgames.com/category.screen?categoryId=ACCESSORIES" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 614 — 3rd event

59.99.230.91 - - [12/Feb/2018:14:12:55] "POST /cart.do?action=addtocart&itemId=EST-17&productId=WC-SH-A02&JSESSIONID=SD2SL8FF3ADFF4963 HTTP 1.1" 200 3883 "http://www.buttercupgames.com/product.screen?productId=WC-SH-A02" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 163 — 4th event

59.99.230.91 - - [12/Feb/2018:14:12:58] "POST /cart.do?action=purchase&itemId=EST-17&JSESSIONID=SD2SL8FF3ADFF4963 HTTP 1.1" 503 2389 "http://www.buttercupgames.com/cart.do?action=addtocart&itemId=EST-17&categoryId=ACCESSORIES&productId=WC-SH-A02" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 894 — 5th event (most recent)

host = www2 | source = /opt/log/www2/access.log | sourcetype = access_combined

`transaction` Command Example 3

Scenario

SecOps is trying to track an issue with the web servers in the online store. Over the last 24 hours, find status code 200 (“success”) generated by user sessions in the online store, and display 3 related events after it.

Find related events that occur after a specific event using **`startswith`** and **`maxevents`**

```
index=web sourcetype=access_combined
| transaction JSESSIONID startswith=(status=200) maxevents=4
```

200

2/12/18
6:55:55.000 PM

```
67.133.102.54 - - [12/Feb/2018:23:55:55] "GET /oldlink?itemId=EST-15&JSESSIONID=SD10SL8FF2ADFF4960 HTTP 1.1" 200 996 "
http://www.buttercupgames.com/cart.do?action=view&itemId=EST-15&productId=WC-SH-A01" "Mozilla/5.0 (iPad; CPU OS 5_1_1
like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B206 Safari/7534.48.3" 813
67.133.102.54 - - [12/Feb/2018:23:55:59] "GET /productscreen.html?t=ou812&JSESSIONID=SD10SL8FF2ADFF4960 HTTP 1.1" 404
464 "http://www.buttercupgames.com/category.screen?categoryId=NULL" "Mozilla/5.0 (iPad; CPU OS 5_1_1 like Mac OS X) Ap
pleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B206 Safari/7534.48.3" 529
67.133.102.54 - - [12/Feb/2018:23:56:07] "GET /category.screen?categoryId=NULL&JSESSIONID=SD10SL8FF2ADFF4960 HTTP 1.1"
 406 2105 "http://www.buttercupgames.com/category.screen?categoryId=NULL" "Mozilla/5.0 (iPad; CPU OS 5_1_1 like Mac OS
 X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B206 Safari/7534.48.3" 715
67.133.102.54 - - [12/Feb/2018:23:56:25] "GET /oldlink?itemId=EST-15&JSESSIONID=SD10SL8FF2ADFF4960 HTTP 1.1" 408 2784
 "http://www.buttercupgames.com/category.screen?categoryId=NULL" "Mozilla/5.0 (iPad; CPU OS 5_1_1 like Mac OS X) Apple
WebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B206 Safari/7534.48.3" 148
```

host = www2 | source = /opt/log/www2/access.log | sourcetype = access_combined

`transaction` Command Example 4

Use the **`search`** command after the **`transaction`** command to filter whole transactions

Scenario

Display transactions that included a 404 error during the last 60 minutes.

```
index=web sourcetype=access_combined
| transaction JSESSIONID
| search status=404
| highlight JSESSIONID, 404
```

i	Time	Event
>	4/26/21 11:24:35.000 PM	210.76.124.106 - - [26/Apr/2021:23:24:35] "GET /category.screen?categoryId=NULL&JSESSIONID=SD0SL10FF7ADFF4953 HTTP 1.1" 408 3492 "http://www.bing.com" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 545 210.76.124.106 - - [26/Apr/2021:23:24:53] "POST /category.screen?categoryId=ACCESSORIES&JSESSIONID=SD0SL10FF7ADFF4953 HTTP 1.1" 200 3934 "http://www.buttercupgames.com/cart.do?action=remove&itemId=EST-12&productId=WC-SH-A02" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 212 210.76.124.106 - - [26/Apr/2021:23:25:01] "GET /product.screen?productId=SF-BVS-01&JSESSIONID=SD0SL10FF7ADFF4953 HTTP 1.1" 404 2218 "http://www.buttercupgames.com/oldlink?itemId=EST-26" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET4.0C)" 965 210.76.124.106 - - [26/Apr/2021:23:25:08] "GET /oldlink?itemId=EST-11&JSESSIONID=SD0SL10FF7ADFF4953 HTTP 1.1" 503 1337 "http://www.buttercupgames.com/cart.do?action=remove&itemId=EST-11" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (9; .NET4.0C)" 272 host = www1 | source = /opt/log/www1/access.log | sourcetype = access_combined

Note

`access_combined` is highlighted because it appears in the basic search.

Using `eval` Expressions with `transaction`

Use `eval` filtering expressions with `startswith` and `endswith` to form transactions based on terms, field values, or evaluations

Scenario

Determine the length of time spent to complete a purchase by customers in the online store over the last 24 hours.

```
index=web sourcetype=access_combined
| transaction clientip JSESSIONID
  startswith=eval(action="addtocart" AND status=200)
  endswith=eval(action="purchase" AND status=200)
| table clientip, JSESSIONID, duration, eventcount
```

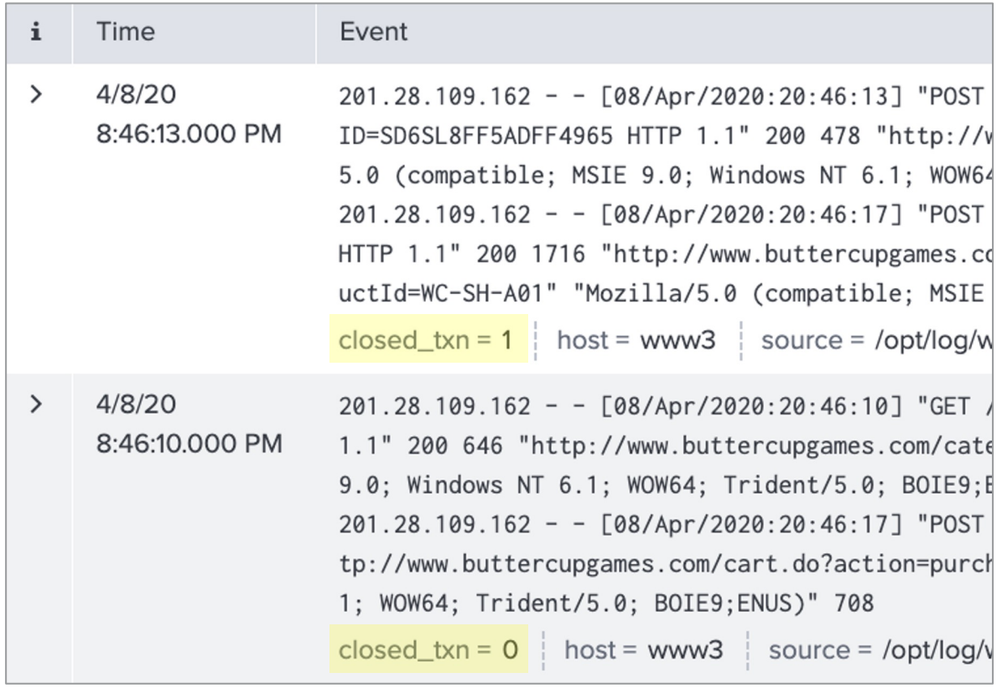
clientip	JSESSIONID	duration	eventcount
86.9.190.90	SD6SL7FF10ADFF4955	1	2
202.91.242.117	SD4SL7FF3ADFF4950	5	2
67.170.226.218	SD2SL8FF1ADFF4965	4	2
67.170.226.218	SD2SL8FF1ADFF4965	12	3
67.170.226.218	SD2SL8FF1ADFF4965	1	2
67.170.226.218	SD2SL8FF1ADFF4965	2	2

Note

The `table` command puts specific fields in a table.

closed_txn

- Transactions are assigned either a **0** or **1** in the **closed_txn** field
  - **1** = conditions are met and the transaction is "complete"
  - **0** = conditions are not met and the transaction is "incomplete"
- **closed_txn=1** if one of these conditions is met: **startswith**, **maxevents**, **maxpause**, and **maxspan**



i	Time	Event
>	4/8/20 8:46:13.000 PM	201.28.109.162 - - [08/Apr/2020:20:46:13] "POST ID=SD6SL8FF5ADFF4965 HTTP 1.1" 200 478 "http://w 5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64 201.28.109.162 - - [08/Apr/2020:20:46:17] "POST HTTP 1.1" 200 1716 "http://www.buttercupgames.co uctId=WC-SH-A01" "Mozilla/5.0 (compatible; MSIE closed_txn = 1 host = www3 source = /opt/log/w
>	4/8/20 8:46:10.000 PM	201.28.109.162 - - [08/Apr/2020:20:46:10] "GET / 1.1" 200 646 "http://www.buttercupgames.com/cate 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;E 201.28.109.162 - - [08/Apr/2020:20:46:17] "POST tp://www.buttercupgames.com/cart.do?action=purch 1; WOW64; Trident/5.0; BOIE9;ENUS)" 708 closed_txn = 0 host = www3 source = /opt/log/v

Note

If no options are specified, all transactions are displayed even if **closed_txn=0**.

keepevicted

```
...| transaction (<field>|<field-list>) startswith=<arg> endswith=<arg>
     keepevicted=<Boolean>
```

- When a transaction fails to meet conditions (**closed_txn=0**) it is evicted from the results
- To keep incomplete transactions, use the **keepevicted** option
  - **keepevicted=1** shows complete and incomplete transactions
  - **keepevicted=0** only shows complete transactions (default)
- Memory limitations can also prematurely evict transactions

keepevicted Example

Scenario

Business Operations needs to identify the success rate of transactions on its production web servers over the last 24 hours. Evaluate transactions and provide total attempted, total completed, and percent completed.

1. Transaction conditions are specified
2. Keep evicted transactions that did not satisfy the requirements of the options

```
index=web sourcetype=access_combined
| transaction JSESSIONID startswith=(action=addtocart)
  endswith=(action=purchase) keepevicted=1
| search action=addtocart
| stats count(eval(closed_txn=0)) as "Total Failed",
  count(eval(closed_txn=1)) as "Total Completed",
  count as "Total Attempted"
| eval "Percent Completed" = round((('Total Attempted'
  - 'Total Failed')*100)/'Total Attempted'),0)."%"
| table "Total Attempted","Total Completed","Percent Completed"
```

Total Attempted	Total Completed	Percent Completed
2076	1941	93%

`keepevicted` Example (cont.)

3. Only keep transactions where at least one event involved the action, **`addtocart`**
4. Count the number of failed and complete transactions using the **`closed_txn`** field, and then the total number of transactions

```
index=web sourcetype=access_combined
| transaction JSESSIONID startswith=(action=addtocart)
  endswith=(action=purchase) keepevicted=1
3 | search action=addtocart
| stats count(eval(closed_txn=0)) as "Total Failed",
4 count(eval(closed_txn=1)) as "Total Completed",
  count as "Total Attempted"
| eval "Percent Completed" = round((('Total Attempted'
  - 'Total Failed')*100)/'Total Attempted'),0) . "%"
| table "Total Attempted","Total Completed","Percent Completed"
```

Total Attempted	Total Completed	Percent Completed
2076	1941	93%

`keepevicted` Example (cont.)

`eval` and `table` commands are used to reformat and display results in a table

```
index=web sourcetype=access_combined
| transaction JSESSIONID startswith=(action=addtocart)
  endswith=(action=purchase) keepevicted=1
| search action=addtocart
| stats count(eval(closed_txn=0)) as "Total Failed",
  count(eval(closed_txn=1)) as "Total Completed",
  count as "Total Attempted"
| eval "Percent Completed" = round((('Total Attempted'
  - 'Total Failed')*100)/'Total Attempted'),0) . "%"
| table "Total Attempted","Total Completed","Percent Completed"
```

Total Attempted	Total Completed	Percent Completed
2076	1941	93%

Optimizing Search for `transaction`

Make the search before transaction as efficient as possible

```
index=web sourcetype=access_combined
| transaction JSESSIONID startswith=(action=addtocart)
  endswith=(action=purchase) keepevicted=1
| search action=addtocart
| stats count(eval(closed_txn=0)) as "Total Failed",
  count(eval(closed_txn=1)) as "Total Completed",
  count as "Total Attempted"
| eval "Percent Completed" = round((('Total Attempted'
  - 'Total Failed')*100)/'Total Attempted'),0) . "%"
| table "Total Attempted","Total Completed","Percent Completed"
```

This search has completed and has returned **1** results

by scanning **9,052** events in **1.133** seconds

```
index=web sourcetype=access_combined (action=purchase OR
  action=addtocart)
| transaction JSESSIONID startswith=(action=addtocart)
  endswith=(action=purchase) keepevicted=1
| search action=addtocart
| stats count(eval(closed_txn=0)) as "Total Failed",
  count(eval(closed_txn=1)) as "Total Completed",
  count as "Total Attempted"
| eval "Percent Completed" = round((('Total Attempted'
  - 'Total Failed')*100)/'Total Attempted'),0) . "%"
| table "Total Attempted","Total Completed","Percent Completed"
```

This search has completed and has returned **1** results

by scanning **5,058** events in **0.819** seconds

Note

The **`JSESSIONID`**s in this search may have other actions associated with their website visits. However, those other actions do not help us fulfill the scenario request.

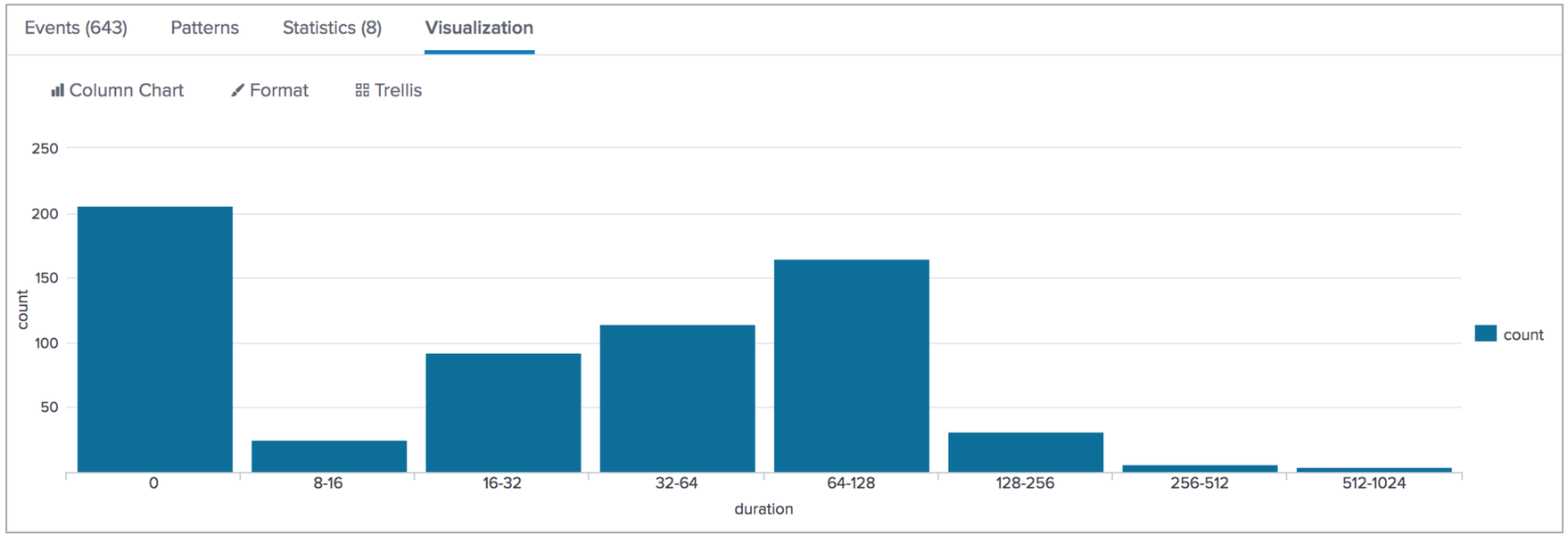
Reporting on Transactions

Use statistics and transforming commands with transactions to create reports and visualizations

Scenario

Create a chart to show the number of purchase transactions based on their duration.

```
index=web sourcetype=access_combined status=200 action=purchase
| transaction clientip maxspan=10m
| chart count by duration span=log2
```



Note

The `chart` command transforms events into chartable results.

`transaction` Considerations

- The **`transaction`** command is resource intensive
- Only use **`transaction`** if you:
  - Need to group events on values from multiple fields
  - Need to define event grouping on start/end values or segment on time
  - Want to keep raw data associated with each event
- Otherwise use **`stats`** command
  - Faster and more efficient
  - Can perform calculations
  - Can group events based on a single field value (e.g. **`by src_ip`**)

`transaction` vs. `stats` Example 1

These searches produce the same results, but `stats` is faster

```
index=web sourcetype=access_combined earliest=-1y latest=now
| transaction JSESSIONID
| table JSESSIONID, action, product_name
| sort JSESSIONID
```

This search has completed and has returned **4,999** results by scanning **1,931,573** events in **38.843** seconds

```
index=web sourcetype=access_combined earliest=-1y latest=now
| stats values(action) as "action",
  values(product_name) as "product_name" by JSESSIONID
| sort JSESSIONID
```

This search has completed and has returned **10,000** results by scanning **1,931,617** events in **21.012** seconds

JSESSIONID	action	product_name
SD0SL10FF10ADFF4953	addtocart purchase	Dream Crusher World of Cheese
SD0SL10FF10ADFF4954	addtocart purchase view	Benign Space Debris Dream Crusher Fire Resistance Suit of Provolone Holy Blade of Gouda Manganiello Bros. Tee Orvil the Wolverine
SD0SL10FF10ADFF4958	addtocart changequantity purchase	Dream Crusher Final Sequel Orvil the Wolverine
SD0SL10FF10ADFF4962	addtocart	Manganiello Bros.

 |

`transaction` vs. `stats` Example 2

- `transaction` has a limit of 1000 events per transaction
- `stats` has no limit

```
index=security sourcetype=linux_secure failed
| transaction src_ip
| table src_ip, eventcount
| sort - eventcount
```

src_ip	eventcount
87.194.216.51	1000
87.194.216.51	120
211.166.11.101	859
194.215.205.19	647

```
index=security sourcetype=linux_secure failed
| stats count as eventcount by src_ip
| sort - eventcount
```

src_ip	eventcount
87.194.216.51	1120
211.166.11.101	859
194.215.205.19	647
128.241.220.82	624

Calculate Co-Occurrence Lab Exercise

Time: 30 minutes

Tasks:

- Correlate events based on **`JSESSIONID`** and filter results to show only events that involved a **`purchase`** action
- Edit the previous search so that the **`duration`** field is available to use as a filter on your results
- Use the **`transaction`** command with the **`startswith`** and **`endswith`** options to group events with specific conditions
- Challenge: Use the **`transaction`** command with the **`maxspan`** option to find common HTTP status errors from two sourcetypes

Analyze Multiple Data Sources

Topic Objectives

- Understand subsearch
- Work with commands that use subsearch to combine, analyze, and compare multiple data sources:
  - `append`
  - `appendcols`
  - `union`
  - `join`

What is a Subsearch?

1. A search that will send results to the outer search as arguments
   - Enclosed in square brackets
   - Executed first
   - Must start with a generating command (**`inputlookup`**, **`search`**, etc.)
2. Subsearch results are combined with an **`OR`** boolean and attached to the outer search with an **`AND`** boolean

```
index=indexName sourcetype=sourcetypeName
  [subsearch] 1
| additional commands
```

1 `[subsearch]` → `field="value1" OR field="value2" OR field="value3"…`

2
```
index=indexName sourcetype=sourcetypeName AND (field="value1"
  OR field="value2" OR field="value3"…)
| additional commands
```

Events from this index/sourcetype containing one of these fields are then processed by the remaining commands in the outer search

Note

Subsearches can return field pairs in the form of
`(field1="valueA" AND field2="valueA") OR`
`(field1="valueB" AND field2="valueB") AND…`

What is a Subsearch? (cont.)

- Multiple subsearches can be used in a search
- Subsearches can be nested
- Great for filtering data that you cannot describe directly in a search expression

Scenario

Find the most active user over the last 7 days and count this user's events by usage.

```
index=network sourcetype=cisco_wsa_squid
  [search index=network sourcetype=cisco_wsa_squid
   | stats count by username
   | sort -count
   | return 1 username]
| stats count by usage, username
| stats list(usage) as usage,
  list(count) as count by username
```

What the subsearch sends to the outer search

```
username="podessa"
```

username	usage	count
podessa	Borderline	1
	Business	24
	Personal	80
	Unknown	12
	Violation	1

Commands That Use Multiple Searches

- This topic discusses commands that use subsearch:
  - `append`
  - `appencols`
  - `union`
  - `join`

append Command

```
...| append
     [subsearch]
```

- Used to combine results from a dissimilar search into a unified results set
- Attaches the results of **[subsearch]** to the end of current results
- Does not produce results if run in real-time

append Command Example 1

Scenario

The Sales department wants to see a list of sales by **productId** for the last hour and for the previous hour.

```
index=web sourcetype=access* productId=* action=purchase status=200
   earliest=-1h@h latest=@h
| stats sum(price) as lastHourSales by productId
| append
    [search index=web sourcetype=access* productId=* action=purchase
       status=200 earliest=-2h@h latest=-1h@h
     | stats sum(price) as previousHourSales by productId]
```

- **append** adds results of the subsearch to the end of the outer search results
- Results are not aligned despite sharing **productIds**

productId	lastHourSales	previousHourSales
BS-AG-G09	99.96	
CU-PG-G06	59.97	
DB-SG-G01	199.92	
DC-SG-G02	279.93	
BS-AG-G09		74.97
CU-PG-G06		79.96
DB-SG-G01		199.92
DC-SG-G02		199.95

 | 6 March 2023

append Command Example 1 (cont.)

- Misaligned data creates misaligned and meaningless visualizations
- To make this search meaningful, you should overlay the results

productId	lastHourSales	previousHourSales
BS-AG-G09	99.96	
CU-PG-G06	59.97	
DB-SG-G01	199.92	
DC-SG-G02	279.93	
BS-AG-G09		74.97
CU-PG-G06		79.96
DB-SG-G01		199.92
DC-SG-G02		199.95

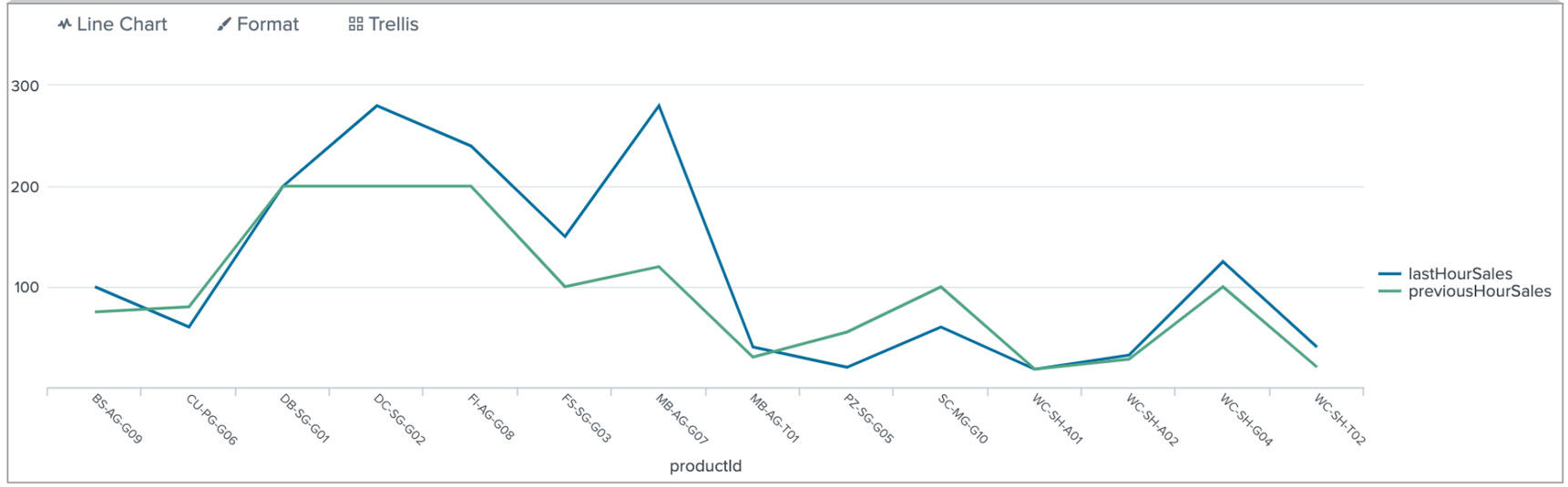
append Command Example 1 (cont.)

Scenario

The Sales department wants to see a list of sales by productId for the last hour and for the previous hour.

Use the event order function `first(*) as *` to overlay results by `productId`

```
index=web sourcetype=access* productId=* action=purchase status=200
   earliest=-1h@h latest=@h
| stats sum(price) as lastHourSales by productId
| append
    [search index=web sourcetype=access* productId=* action=purchase
     status=200 earliest=-2h@h latest=-1h@h
     | stats sum(price) as previousHourSales by productId]
| stats first(*) as * by productId
```



The `first` Function

```
...| stats first(<field>) [as <field>] [by <field-list>]
```

- Returns the first value seen for **<field>**
  - Replace **<field>** with * to perform the **first** function on all fields
  - Use an **as** * clause to keep the same field names
- Can be used with **stats**, **timechart**, and **chart** commands
- Use after **append** to align values
  - A If used with **stats**, Splunk aligns results based on the **by** clause

The last pipe on the previous slide makes use of * with the **as** and **by** clause to align values following the use of **append**

```
|...
| append
      [...]
A ...| stats first(*) as * by productId
```

`appendcols` Command

```
...| appendcols
     [subsearch]
```

- Appends the fields of the **`[subsearch]`** results with outer search results
- The first subsearch result is aligned with the first outer search result, the second subsearch result is aligned with the second outer search result, etc.

outerResult1	subsearchResult1
outerResult2	subsearchResult2
etc…	etc…

appendcols Command Example

Scenario

SecOps noticed an increase in attempted hacking. Compare the number of password failures for known users vs. unknown users over the last 4 hours.

```
index=security sourcetype=linux_secure "failed password" NOT "invalid user"
| timechart count as known_users
| appendcols
    [search index=security sourcetype=linux_secure "failed password"
    "invalid user"
    | timechart count as unknown_users ]
```

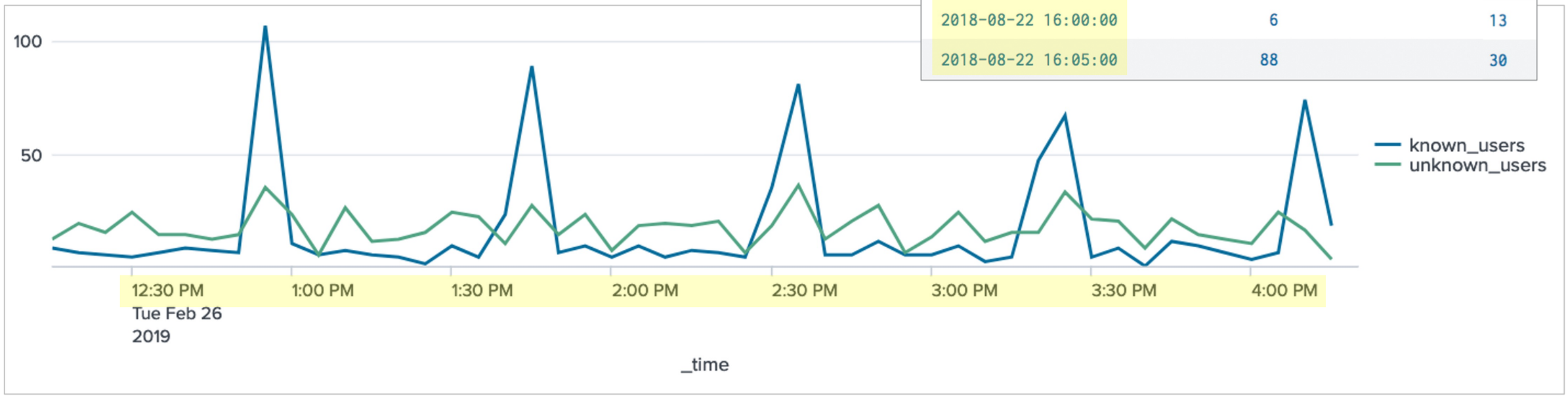
appendcols overlays the search results in one step

_time	known_users	unknown_users
2018-08-22 15:40:00	6	14
2018-08-22 15:45:00	6	25
2018-08-22 15:50:00	5	14
2018-08-22 15:55:00	7	9
2018-08-22 16:00:00	6	13
2018-08-22 16:05:00	88	30

`appendcols` Command Example (cont.)

- `appendcols` creates an aligned visualization
- However, this only works because the time span is the same

_time	known_users	unknown_users
2018-08-22 15:40:00	6	14
2018-08-22 15:45:00	6	25
2018-08-22 15:50:00	5	14
2018-08-22 15:55:00	7	9
2018-08-22 16:00:00	6	13
2018-08-22 16:05:00	88	30



appendcols and Missing Values

If a field is missing data then using **appendcols** is not desirable and can create misleading results

```
index=web sourcetype=access_combined action=purchase
earliest=-1d@d latest=@d
| stats sum(price) as "Yesterday" by product_name
| append
      [search index=web  sourcetype=access_combined
      action=purchase earliest=-15m latest=now
      | stats sum(price) as "Last 15 Minutes" by
      product_name]
| stats first(*) as * by product_name
```

product_name	Yesterday	Previous 15 Minutes
Benign Space Debris	2449.02	
Curling 2014	1739.13	19.99
Dream Crusher	5678.58	79.98
Final Sequel	3598.56	24.99
Fire Resistance Suit of Provolone	630.42	15.96
Holy Blade of Gouda	640.93	5.99
Manganiello Bros.	3719.07	79.98

```
index=web sourcetype=access_combined action=purchase
earliest=-1d@d latest=@d
| stats sum(price) as "Yesterday" by product_name
| appendcols
      [search index=web  sourcetype=access_combined
      action=purchase earliest=-15m latest=now
      | stats sum(price) as "Last 15 Minutes" by
      product_name]
```

product_name	Yesterday	Previous 15 Minutes
Benign Space Debris	2449.02	19.99
Curling 2014	1739.13	79.98
Dream Crusher	5678.58	24.99
Final Sequel	3598.56	15.96
Fire Resistance Suit of Provolone	630.42	5.99
Holy Blade of Gouda	640.93	79.98
Manganiello Bros.	3719.07	49.98

An Alternative Approach to `appendcols`

Generally, for a larger volume of data, faster performance can be achieved using **`eval`** instead of **`append`** or **`appendcols`**

```
index=security sourcetype=linux_secure
"failed password" NOT "invalid user"
| timechart count as known_users
| appendcols
    [search index=security sourcetype=linux_secure
    "failed password" "invalid user"
    | timechart count as unknown_users ]
```

_time	known_users	unknown_users
2020-10-08 14:35:00	6	14
2020-10-08 14:40:00	5	22
2020-10-08 14:45:00	87	29
2020-10-08 14:50:00	35	21
2020-10-08 14:55:00	5	6
2020-10-08 15:00:00	4	15

```
index=security sourcetype=linux_secure
"failed password"
| eval known_unknown=if(searchmatch("invalid user"),"unknown","known")
| timechart count by known_unknown
| rename known as "known_users", unknown as "unknown_users"
```

Note

The **`eval`** command is outside the scope of this module.

`join` Command

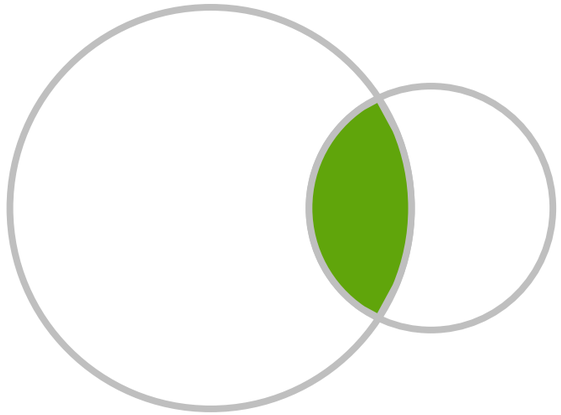
```
...| join [type=arg] [<field-list>]
       [subsearch]
```

- Combines the results of **`[subsearch]`** with the results of the outer search
- Specify **`<field-list>`** to be used for the join; if not specified, all shared fields from the subsearch are used
  - One or more fields must be shared between the subsearch and the outer search
- Control how results are joined by using various **`options`**

`join` Command (cont.)

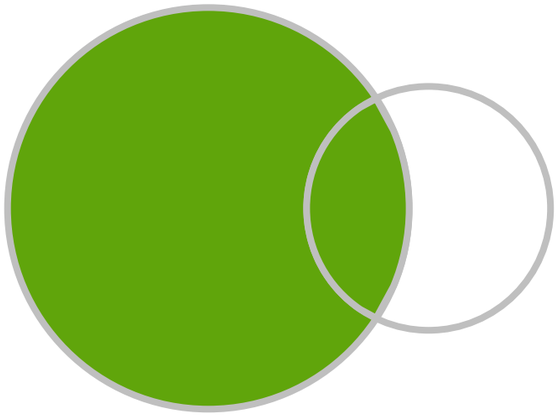
The **`type`** option indicates what type of join to perform

```
| join type=inner
```



An **`inner`** join (default) only includes events from the outer search that match events from the inner search

```
| join type=outer
```



An **`outer`** (**`left`**) join includes all events from the outer search and the matching events from an inner search

`join` Command Example

Scenario

Sales wants a list of all products sold over the last six hours in the Asia-Pacific region that have also sold in Africa.

```
index=sales sourcetype=vendor_sales VendorID>=9000
| join product_name 2
    [ search index=sales sourcetype=vendor_sales
    1 VendorID>=7000 AND VendorID<9000
    | dedup product_name]
| dedup product_name
| table product_name
```

product_name
Benign Space Debris
Final Sequel
Fire Resistance Suit of Provolone
Mediocre Kingdoms

1. The subsearch returns unique **`product_name`** values that have sold in stores in the Asia-Pacific region
2. **`product_name`** is used to join the inner and outer search results
   - By default, results represent an inner join

An Alternative Approach to `join`

Scenario

Sales wants a list of all products sold over the last six hours in the Asia-Pacific region that have also sold in Africa.

This search has completed and has returned **4** results by scanning **262** events in **0.492** seconds

Search using an inner **`join`**

This search has completed and has returned **4** results by scanning **262** events in **0.233** seconds

Search using **`eval`** and **`stats`**

- An **`eval`** and **`stats`**-based search executes faster and provides the same results

1. **`eval`** creates a field (**`region`**) that identifies each set of data you want to compare
2. **`stats`** reports on **`region`**

```
index=sales sourcetype=vendor_sales VendorID>=7000
1 | eval region = if (VendorID>=9000,"Africa","Asia")
2 | stats dc(region) as occurrences by product_name
  | where occurrences=2
  | fields product_name
```

product_name
Benign Space Debris
Final Sequel
Fire Resistance Suit of Provolone
Mediocre Kingdoms

 |

`union` Command

```
| union <dataset>, [<dataset>]
```

- Combines results from two or more datasets and returns a single result set
- `<dataset>` can be one or a combination of data models, saved searches, lookups, or subsearches, separated by a comma

Note

Data models, saved searches, and lookups are named datasets and are accessible by using a naming syntax.

`union` Command: Named Dataset Syntax

Data model datasets, saved searches, and lookups are named datasets and must follow this syntax:

```
| union datasetType:datasetName
```

`datamodel:`*`datamodel.dataset`*	`datamodel:vsales.afr`
`savedsearch:`*`savedsearchName`*	`savedsearch:"Very Official Report"`
`lookup:`*`LookupName`*	`lookup:employee_lookup` `lookup:employee.csv`

`union` Command: Combining Datasets Syntax

```
| union datamodel:datamodel1.dataset1, datamodel:datamodel2.dataset2 ...
```

Syntax using datamodels

```
| union
  [subsearch1]
  [subsearch2]
...
```

Syntax using subsearches

```
| union datamodel:datamodel1.dataset1,
  [subsearch]
```

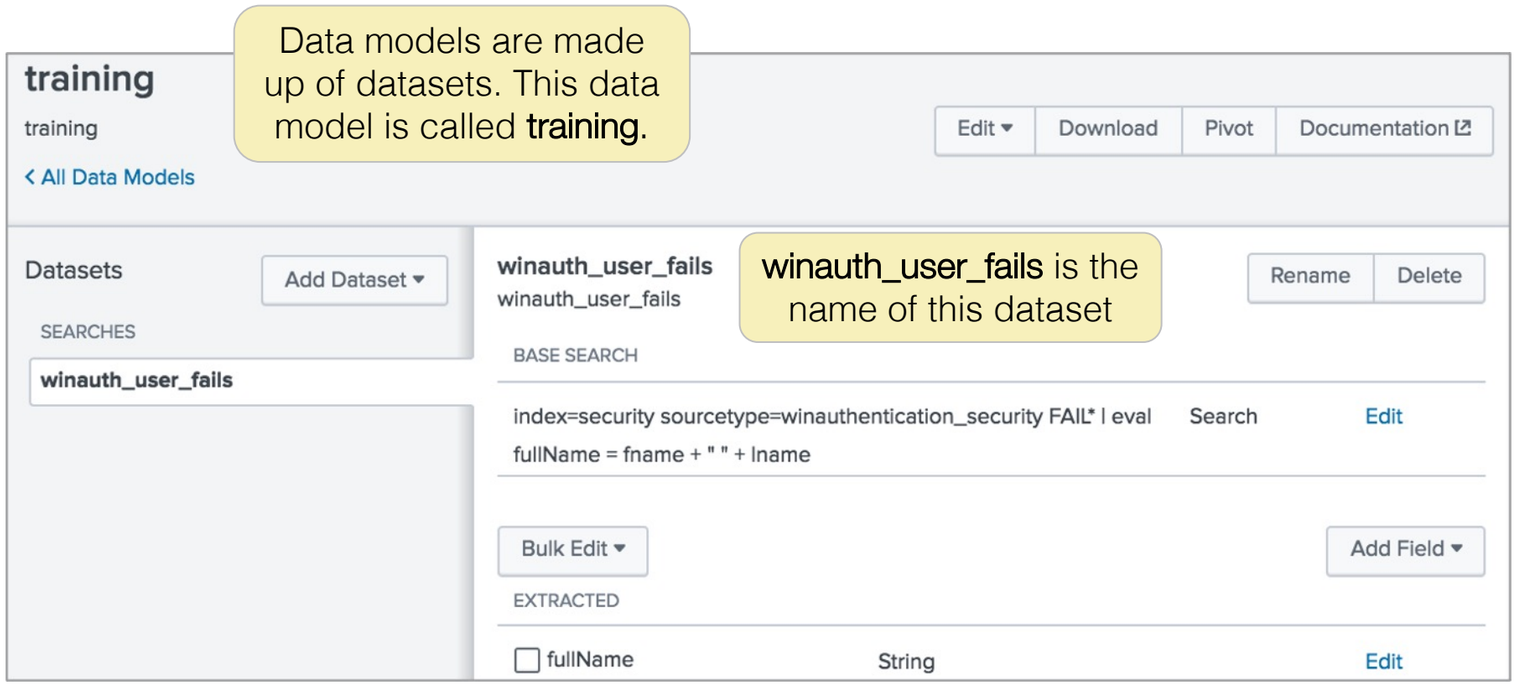
Syntax using both

Note

A subsearch is an unnamed dataset. If joining two subsearches, a comma is not needed between them.

What are Datasets?

- A collection of data defined for a specific purpose
- Can be based on events, searches, or transactions
- Only users with access to the dataset can read the dataset with **`union`**




```
| union datamodel:training.winauth_user_fails
```

union Command Example

Scenario

IT wants a list of the users with password failures on Windows and Linux systems last week.

```
| union datamodel:"training.winauth_user_fails"
  [ search index=security sourcetype=linux_secure FAIL* user=* ]
| eval user = coalesce(user, User)
| dedup user
| table user
| sort user
```

user
Administrator
abc
adm
admin
administrator
adombrowski
agushto

Analyze Multiple Datasets Lab Exercise

Time: 15 minutes

Tasks:

- Use the **`append`** command to create a search that displays results from two different time ranges and use the **`first`** function to align results by a specific field

Wrap-up Slides

Wrap-up

- You should now be able to:
  - Use **`transaction`** command to correlate multiple events
  - Add information to search results with **`append`** and **`appendcols`**
  - Correlate results from different data sources with **`join`**
  - Combine results from multiple datasets with **`union`**

Community

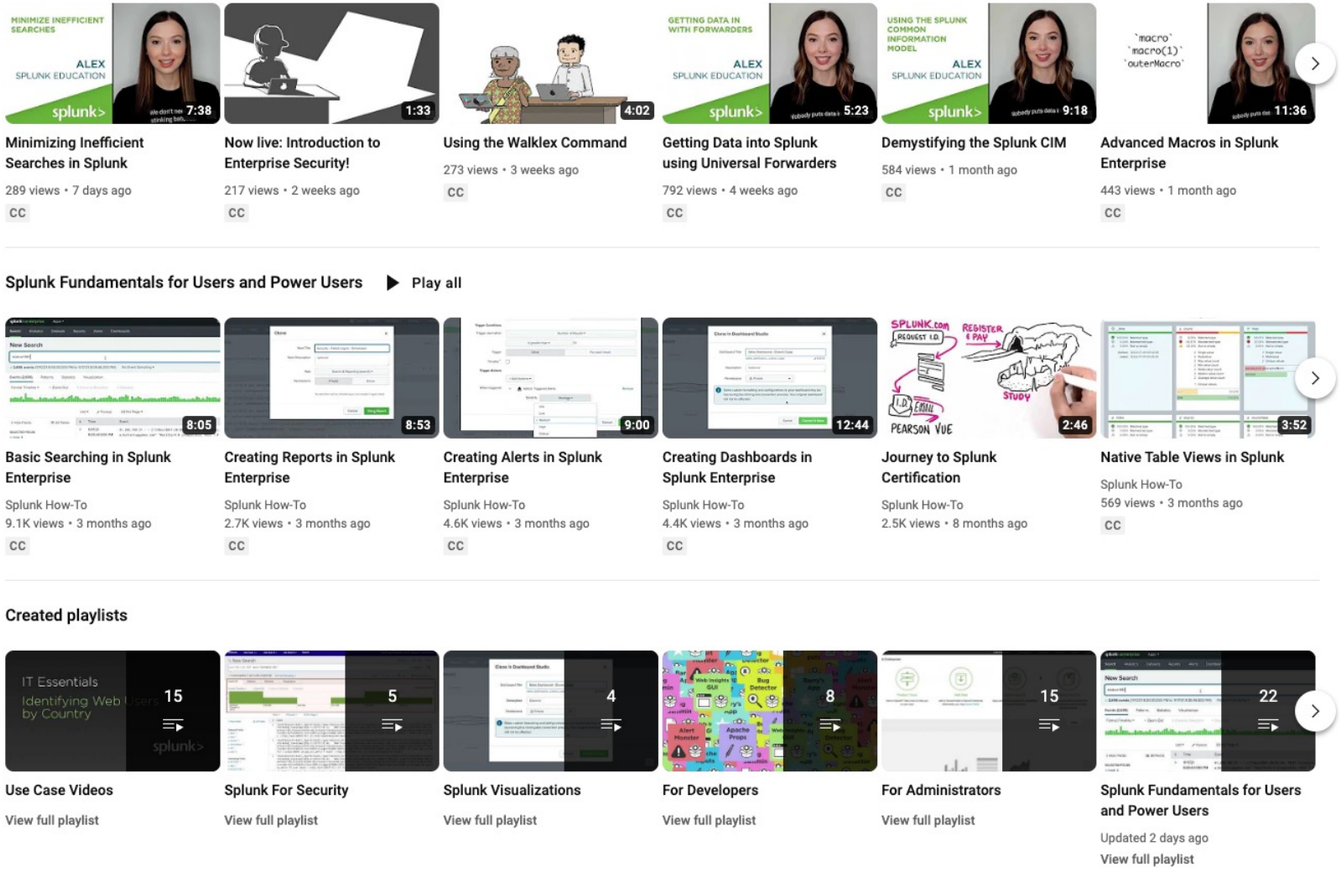
- Splunk Community Portal – community.splunk.com
  - Answers
  - Discussions
  - Splunk Trust
  - User Groups
  - Ideas
- Splunk Blogs – splunk.com/blog/
- Splunk Base – splunkbase.com
  - Apps
  - Curated Collections
- Splunk Docs on Twitter – twitter.com/splunkdocs
- Splunk Dev on Twitter – twitter.com/splunkdev
- Splunk on Slack – splk.it/slack
- .conf – conf.splunk.com

Community

- Knowledge Base – Search knowledge base, answers, and docs to troubleshoot your issue
- splunk>dev – Documentation for developers
- Splunk Docs – Product, best practices, and tools documentation for all Splunk products
- Splunk Lantern – Actionable guidance by experts
- Create a case – Support for critical issues
- Contact Us – Find region-specific support
  - (855) SPLUNK.S or (855) 775.8657
  - Not in the US? Find your local office
- System Status – Cloud Services, Observability Cloud, Splunk On-Call, Synthetic Monitoring
- Splunk Product Security – Critical Security Alerts, Quarterly Security Patches, and 3rd Party Bulletins

Splunk How-To Channel

Free, short videos on a variety of Splunk topics: splk.it/How-To



Learning Paths

Search Expert – Recommended Courses

Free eLearning courses are highlighted in blue and courses with an * are present in both learning paths.

- What is Splunk *
- Introduction to Splunk *
- Using Fields *
- Scheduling Reports and Alerts
- Visualizations
- Statistical Processing
- Working with Time
- Comparing Values
- Result Modification
- Leveraging Lookups and Subsearches
- Correlation Analysis
- Search Under the Hood
- Multivalue Fields
- Search Optimization *

Learning Paths

Knowledge Manager – Recommended Courses

Free eLearning courses are highlighted in blue and courses with an * are present in both learning paths.

- What is Splunk *
- Introduction to Splunk *
- Using Fields *
- Introduction to Knowledge Objects
- Creating Knowledge Objects
- Creating Field Extractions
- Enriching Data with Lookups
- Data Models
- Introduction to Dashboards
- Dynamic Dashboards
- Using Choropleth
- Search Optimization *

Splunk Mobile

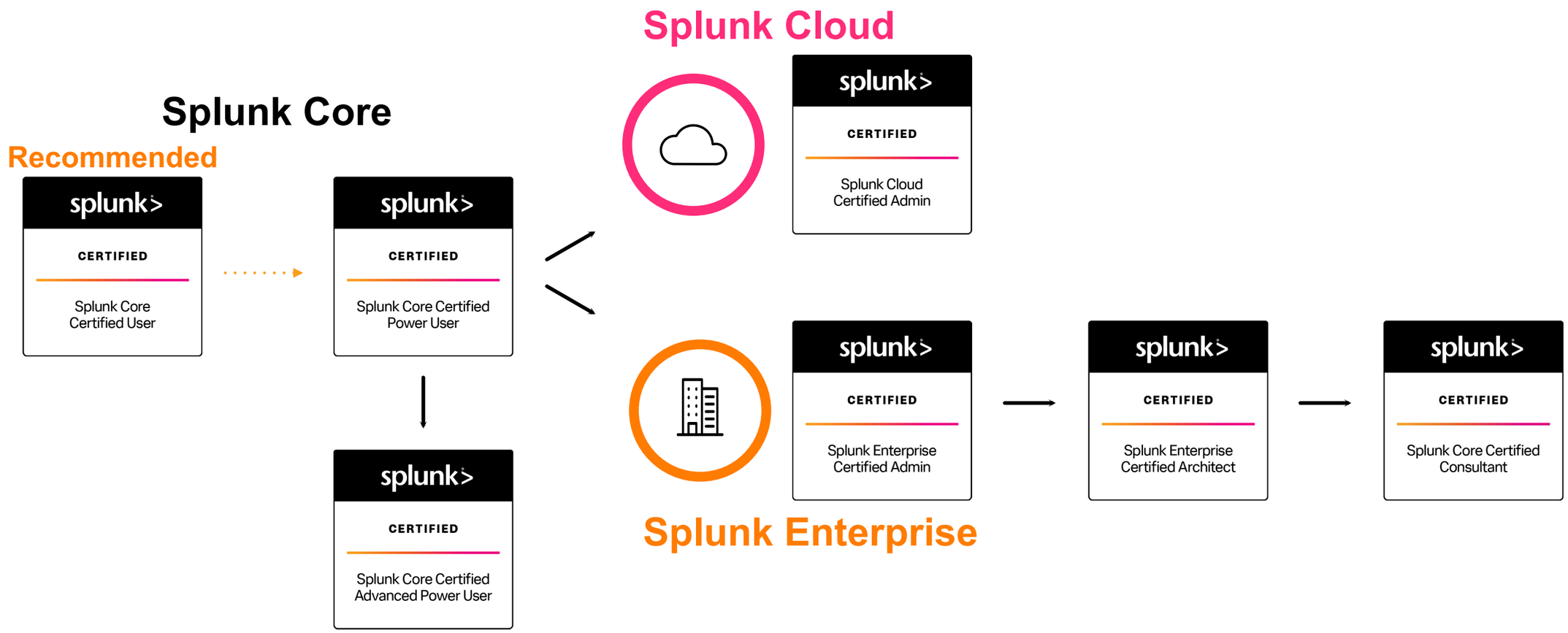
- Free app available to all Splunk Cloud and Splunk Enterprise customers
- Analyze data and receive actionable alerts on-the-go with mobile-friendly dashboards
- iOS and Android
- See the Product Brief
- Download for iOS splk.it/ios

Splunk Certification

Offerings & Requirements

Splunk Core and Beyond

Regardless of which Splunk product you use, it all starts with Splunk Core



App-Specific Offerings

For Splunk Add-Ons

App Developer

ES Administration

ITSI Administration

SOAR Automation Developer

Splunk Core Certified User

This entry-level certification demonstrates an individual's basic ability to navigate and use Splunk software

Prerequisite Certification(s):

- None

Prerequisite Course(s):

- None

Splunk Core Certified User Exam

Time to study! We suggest candidates looking to prepare for this exam complete Fundamentals 1 **or** the following courses:

- What is Splunk?
- Intro to Splunk
- Using Fields
- Scheduling Reports and Alerts
- Visualizations
- Statistical Processing
- Working with Time
- Leveraging Lookups and Subsearches
- Search Optimization
- Enriching Data with Lookups
- Data Models

See here for registration assistance.

Congratulations! You are a...

Recommended Next Step

- Splunk Core Certified Power User

Splunk Core Certified Power User

This entry-level certification demonstrates an individual's foundational competence of Splunk’s core software

Prerequisite Certification(s):

- None

Prerequisite Course(s):

- None

Splunk Core Certified Power User Exam

Time to study! We suggest candidates looking to prepare for this exam complete Fundamentals 2 **or** the following courses:

- Visualizations
- Statistical Processing
- Working with Time
- Comparing Values
- Result Modification
- Correlation Analysis
- Search Under the Hood
- Introduction to Knowledge Objects
- Creating Knowledge Objects
- Creating Field Extractions
- Data Models
- Using Choropleth

See here for registration assistance.

Congratulations! You are a...

Recommended Next Steps

- Splunk Core Certified Advanced Power User
- Splunk Enterprise Certified Admin
- Splunk Cloud Certified Admin

Splunk Core Certified Advanced Power User

This certification demonstrates an individual's ability to generate complex searches, reports, and dashboards with Splunk's core software to get the most out of their data

Prerequisite Certification(s):

- Splunk Core Certified Power User

Prerequisite Course(s):

- None

Splunk Core Certified Advanced Power User Exam

Time to study! We suggest candidates looking to prepare for this exam complete Fundamentals 3, Creating Dashboards, and Advanced Searching & Reporting **or** the following courses:

- Using Fields
- Working with Time
- Comparing Values
- Result Modification
- Leveraging Lookups and Subsearches
- Correlation Analysis
- Search Under the Hood
- Multivalue Fields
- Search Optimization
- Creating Field Extractions
- Enriching Data with Lookups
- Data Models
- Using Choropleth
- Introduction to Dashboards
- Dynamic Dashboards

See here for registration assistance.

Congratulations! You are a...

Recommended Next Steps

- Splunk Enterprise Certified Admin
- Splunk Cloud Certified Admin

Splunk Cloud Certified Admin

This certification demonstrates an individual's ability to support the day-to-day administration and health of a Splunk Cloud environment

Prerequisite Certification(s):

- Splunk Core Certified Power User

Prerequisite Course(s):

- None

Splunk Cloud Certified Admin Exam

Time to study! We suggest candidates looking to prepare for this exam complete **either** the Splunk Cloud Administration **or** the Transitioning to Splunk Cloud course.

Both courses will equally prepare candidates for the exam, but are tailored to meet the needs of the individual based on prior Splunk experience.

Splunk Cloud Administration is designed for net-new administrators working in a Splunk Cloud environment. **Transitioning to Splunk Cloud** is for experienced Enterprise administrators looking to maximize their success in migrating to a Cloud environment.

See here for registration assistance.

Congratulations! You are a...

Recommended Next Steps

- Splunk Certified Developer

Splunk Enterprise Certified Admin

This certification demonstrates an individual's ability to support the day-to-day administration and health of a Splunk Enterprise environment

Prerequisite Certification(s):

- Splunk Core Certified Power User

Prerequisite Course(s):

- None

Splunk Enterprise Certified Admin Exam

Time to study! We suggest candidates looking to prepare for this exam complete the following courses:

- Splunk System Administration
- Splunk Data Administration

See here for registration assistance.

Congratulations! You are a...

Recommended Next Steps

- Splunk Enterprise Certified Architect
- Splunk Certified Developer

Splunk Certified Architect

This certification demonstrates an individual's ability to deploy, manage, and troubleshoot complex Splunk Enterprise environments

Prerequisite Certification(s):

- Splunk Core Certified Power User
- Splunk Enterprise Certified Admin

Prerequisite Course(s):

- Architecting Splunk Enterprise Deployments
- Troubleshooting Splunk Enterprise
- Splunk Cluster Administration
- Splunk Deployment Practical Lab

Splunk Enterprise Certified Architect Exam

Time to study! We **require** candidates looking to register for this exam to complete the following prerequisite courses:

- Architecting Splunk Enterprise Deployments
- Troubleshooting Splunk Enterprise
- Splunk Cluster Administration
- Splunk Deployment Practical Lab

Candidates who are **Splunk Enterprise Certified Admin** and have completed all of the above courses will automatically receive an exam authorization for the Splunk Enterprise Certified Architect exam within 5-7 business days of receiving their passing lab results.

See here for registration assistance.

Congratulations! You are a...

splunk>

CERTIFIED

Splunk Enterprise Certified Architect

Recommended Next Steps

- Splunk Core Certified Consultant

Splunk Core Certified Consultant

This certification demonstrates an individual's ability to properly size, install, and implement Splunk environments and to advise others on how to utilize the product and maximize its value for their needs

Prerequisite Certification(s):

- Splunk Core Certified Power User
- Splunk Enterprise Certified Admin
- Splunk Enterprise Certified Architect

Prerequisite Course(s):

- *Advanced Power User courses **or** digital badge**
- Core Consultant Labs
  - Indexer Cluster Implementation
  - Distributed Search Migration
  - Implementation Fundamentals
  - Architect Implementation 1-3
- Services Core Implementation

Splunk Core Certified Consultant Exam

Time to study! We **require** candidates looking to register for this exam to complete the following prerequisite courses:

- *Fundamentals 3*, *Creating Dashboards*, *Advanced Searching & Reporting**
- Core Consultant Labs
- Services Core Implementation

Candidates who are **Splunk Enterprise Certified Architects** and have completed all of the above courses must contact certification@splunk.com to request their Core Consultant exam authorization.

See here for registration assistance.

These Advanced Power User courses can be replaced with a Splunk Certified Advanced Power User badge **or completion of the following courses:*

- Using Fields
- Creating Field Extractions
- Enriching Data with Lookups
- Data Models
- Search Optimization
- Working with Time
- Leveraging Lookups and Subsearches
- Comparing Values
- Correlation Analysis
- Result Modification
- Multivalue Fields
- Search Under the Hood
- Introduction to Dashboards
- Dynamic Dashboards
- Using Choropleth

Congratulations! You are a...

Recommended Next Steps

- None

Splunk Certified Developer

This certification demonstrates an individual's expertise in drilldowns, advanced behaviors and visualizations, planning, creating, and packaging apps, and REST endpoints

Prerequisite Certification(s):

- Splunk Core Certified Power User

AND

- Splunk Enterprise Certified Admin

OR

- Splunk Cloud Certified Admin

Prerequisite Course(s):

- None

Splunk Certified Developer Exam

Time to study! We suggest candidates looking to prepare for this exam complete the following courses:

- Creating Dashboards with Splunk*
- Advanced Dashboards & Visualizations
- Building Splunk Apps
- Developing with Splunk's REST API

This course may also be substituted with the following newly-launched courses:

- Introduction to Dashboards
- Dynamic Dashboards
- Using Choropleth

See here for registration assistance.

Congratulations! You are a...

Recommended Next Steps

- None

Splunk Enterprise Security Certified Admin

This certification demonstrates an individual's ability to install, configure, and manage a Splunk Enterprise Security deployment

Prerequisite Certification(s):

- None

Prerequisite Course(s):

- None

Splunk Enterprise Security Certified Admin Exam

Time to study! We suggest candidates looking to prepare for this exam complete the following course:

- Administering Splunk Enterprise Security

Please note: all candidates are expected to have working knowledge and experience as either Splunk Cloud or Splunk Enterprise Administrators.

See here for registration assistance.

Congratulations! You are a...

Recommended Next Steps

- Splunk Phantom Certified Admin

Splunk IT Service Intelligence Certified Admin

This certification demonstrates an individual's ability to deploy, manage, and utilize Splunk ITSI to monitor mission-critical services

Prerequisite Certification(s):

- None

Prerequisite Course(s):

- None

Splunk IT Service Intelligence Certified Admin Exam

Time to study! We suggest candidates looking to prepare for this exam complete the following course:

- Implementing Splunk IT Service Intelligence

Please note: all candidates are expected to have working knowledge and experience as either Splunk Cloud or Splunk Enterprise Administrators.

See here for registration assistance.

Congratulations! You are a...

Recommended Next Steps

- Courses on Observability

Splunk SOAR Certified Automation Developer

This certification demonstrates an individual's ability to install and configure a SOAR server, integrate it with Splunk, and plan, design, create, and debug playbooks

Prerequisite Certification(s):

- None

Prerequisite Course(s):

- None

Splunk SOAR Certified Automation Developer Exam

Time to study! We suggest candidates looking to prepare for this exam complete the following courses:

- Administering SOAR (Phantom)
- Developing SOAR (Phantom) Playbooks
- Advanced SOAR (Phantom) Implementation

Please note: all candidates are expected to have working knowledge and experience as either Splunk Cloud or Splunk Enterprise Administrators.

See here for registration assistance.

Congratulations! You are a...

Recommended Next Steps

- None

Thank You

splunk> turn data into doing™