Project: Creating Splunk Queries Based on Generated Prompts

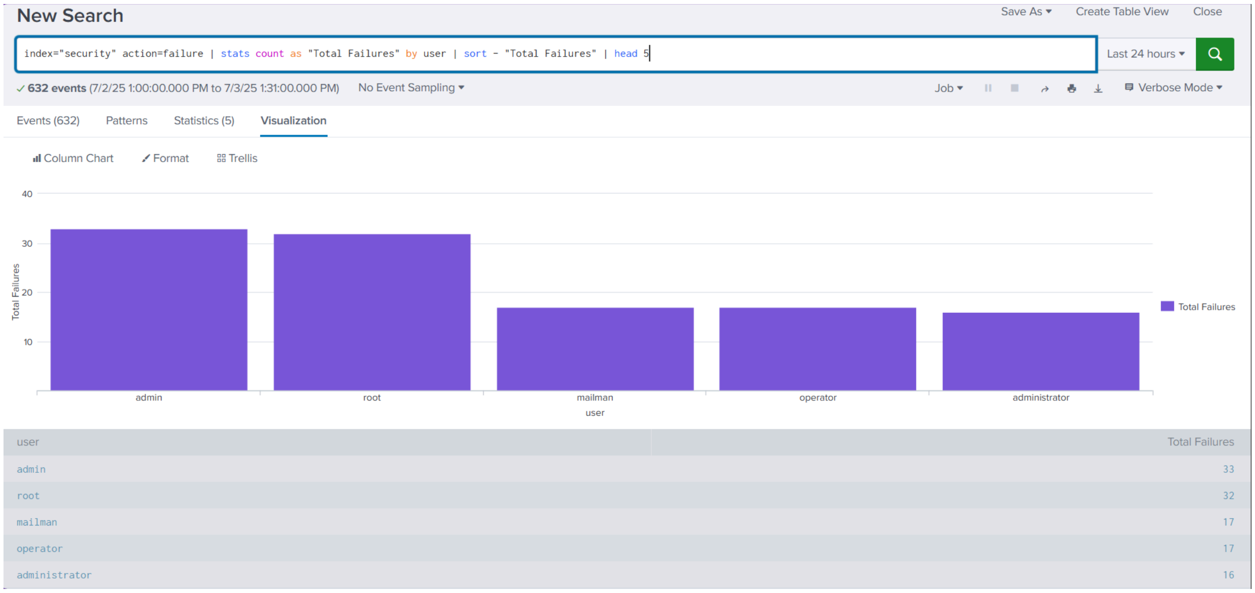
Clay Jones

Objective:

Use ChatGPT to create potential prompts to perform splunk queries. Using these sample prompts, I will create a splunk query based on the prompt. I will be doing this through Splunk and its tutorial data. The goal of this project was to help study for the splunk core and power user exams.

Prompt 1:

Create a chart of the users that had the most total log in failures.



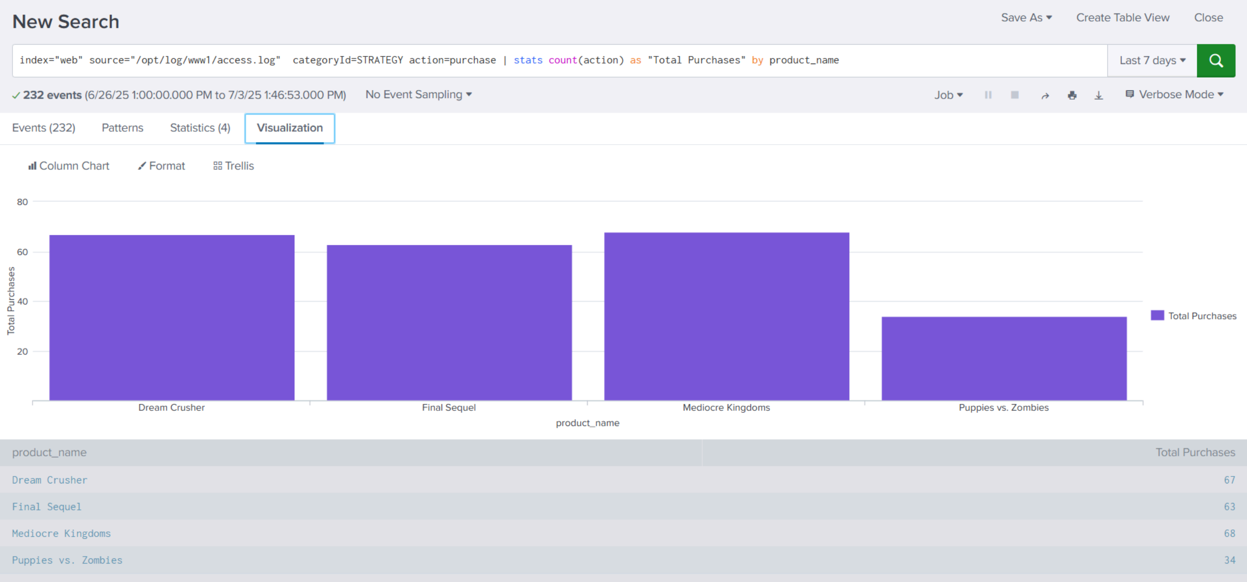
```
index="security" action=failure | stats count as "Total Failures" by user | sort - "Total Failures" | head 5
```

✓ 632 events (7/2/25 1:00:00.000 PM to 7/3/25 1:31:00.000 PM) No Event Sampling ▾

user	Total Failures
admin	33
root	32
mailman	17
operator	17
administrator	16

Prompt 2:

Create a chart of total purchases of each strategy game



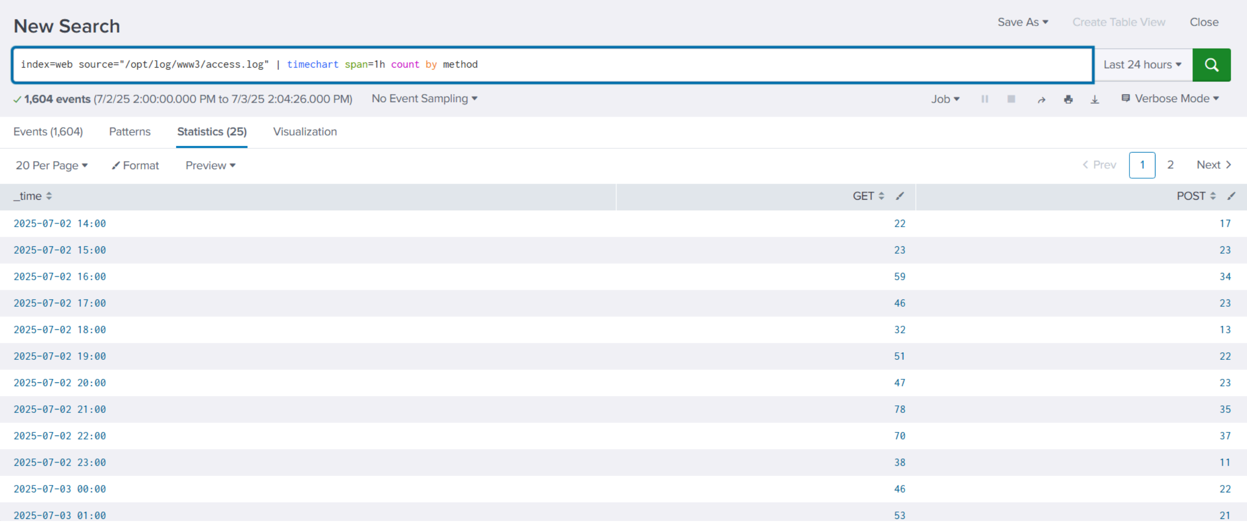
```
index="web" source="/opt/log/www1/access.log"  categoryId=STRATEGY action=purchase | stats count(action) as "Total Purchases" by product_name
```

✓ 232 events (6/26/25 1:00:00.000 PM to 7/3/25 1:46:53.000 PM) No Event Sampling ▾

product_name	Total Purchases
Dream Crusher	67
Final Sequel	63
Mediocre Kingdoms	68
Puppies vs. Zombies	34

Prompt 3:

Create a time chart of the GET and POST methods by each hour



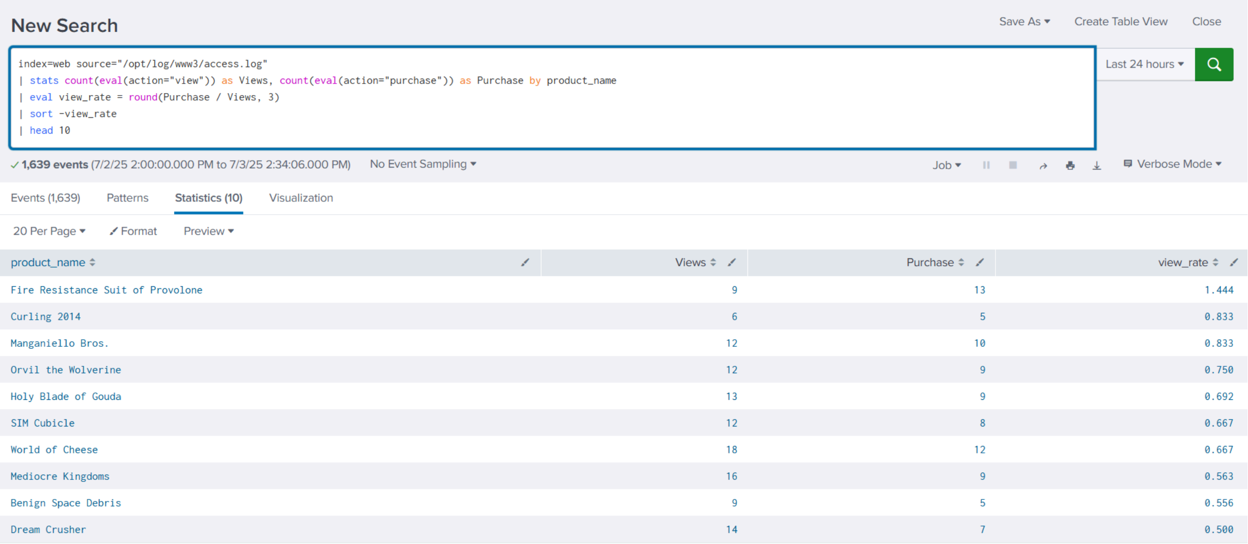
```
index=web source="/opt/log/www3/access.log" | timechart span=1h count by method
```

✓ 1,604 events (7/2/25 2:00:00.000 PM to 7/3/25 2:04:26.000 PM) No Event Sampling ▾

_time	GET	POST
2025-07-02 14:00	22	17
2025-07-02 15:00	23	23
2025-07-02 16:00	59	34
2025-07-02 17:00	46	23
2025-07-02 18:00	32	13
2025-07-02 19:00	51	22
2025-07-02 20:00	47	23
2025-07-02 21:00	78	35
2025-07-02 22:00	70	37
2025-07-02 23:00	38	11
2025-07-03 00:00	46	22
2025-07-03 01:00	53	21

Prompt 4:

Find the game with the most purchases per view



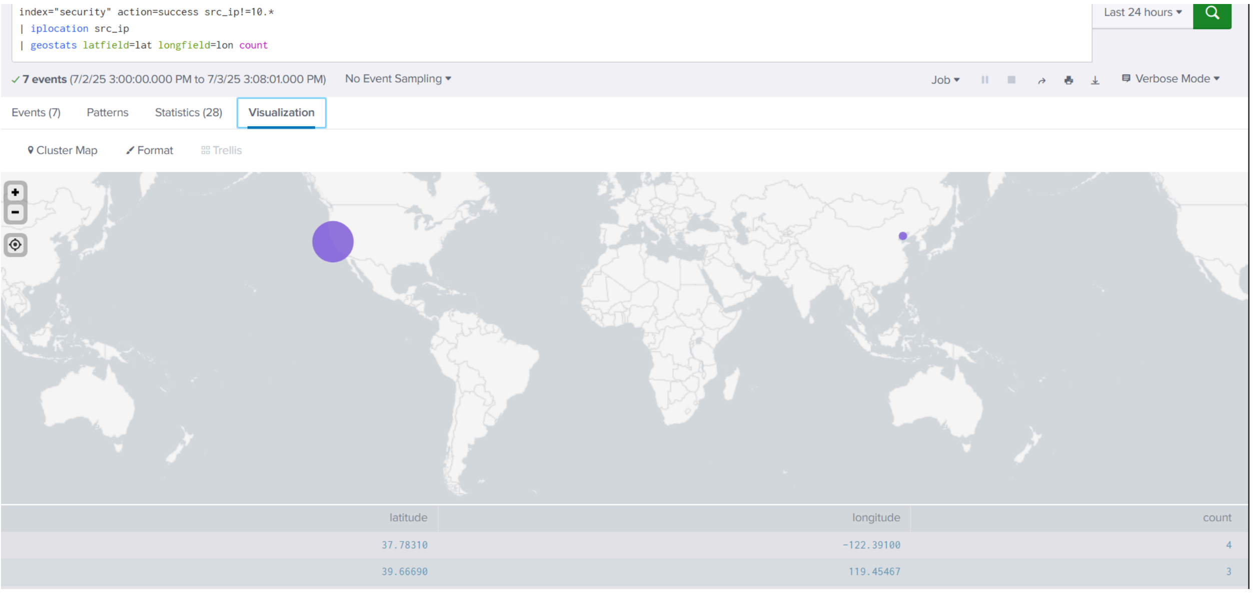
```
index=web source="/opt/log/www3/access.log"
| stats count(eval(action="view")) as Views, count(eval(action="purchase")) as Purchase by product_name
| eval view_rate = round(Purchase / Views, 3)
| sort -view_rate
| head 10
```

✓ 1,639 events (7/2/25 2:00:00.000 PM to 7/3/25 2:34:06.000 PM)   No Event Sampling ▾

product_name	Views	Purchase	view_rate
Fire Resistance Suit of Provolone	9	13	1.444
Curling 2014	6	5	0.833
Manganiello Bros.	12	10	0.833
Orvil the Wolverine	12	9	0.750
Holy Blade of Gouda	13	9	0.692
SIM Cubicle	12	8	0.667
World of Cheese	18	12	0.667
Mediocre Kingdoms	16	9	0.563
Benign Space Debris	9	5	0.556
Dream Crusher	14	7	0.500

Prompt 5:

Create a geographic visualization that shows non-private IP address by location



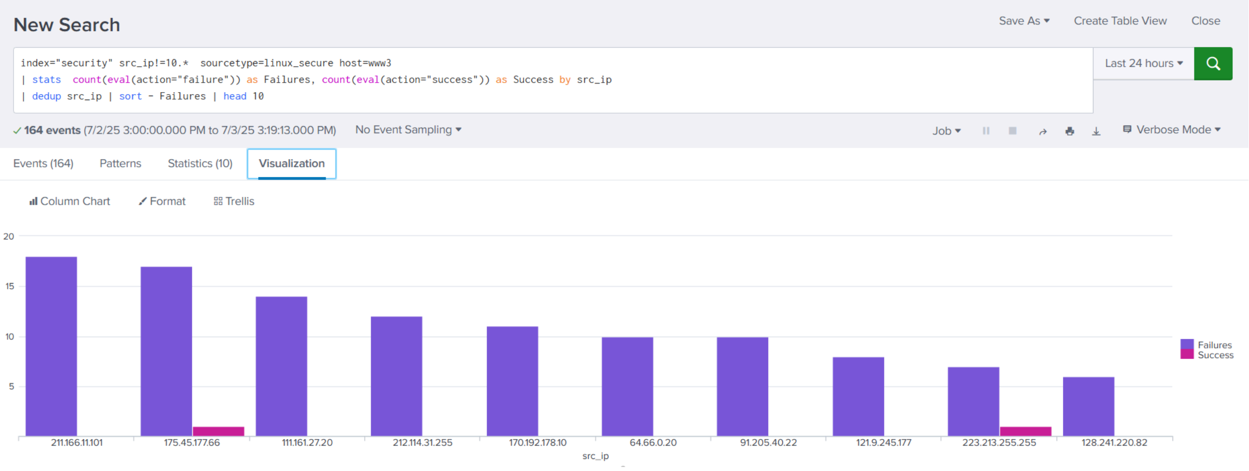
```
index="security" action=success src_ip!=10.*
| iplocation src_ip
| geostats latfield=lat longfield=lon count
```

✓ 7 events (7/2/25 3:00:00.000 PM to 7/3/25 3:08:01.000 PM)   No Event Sampling ▾

latitude	longitude	count
37.78310	-122.39100	4
39.66690	119.45467	3

Prompt 6:

Create a graph of the most failed logins why showing the amount of successful logins

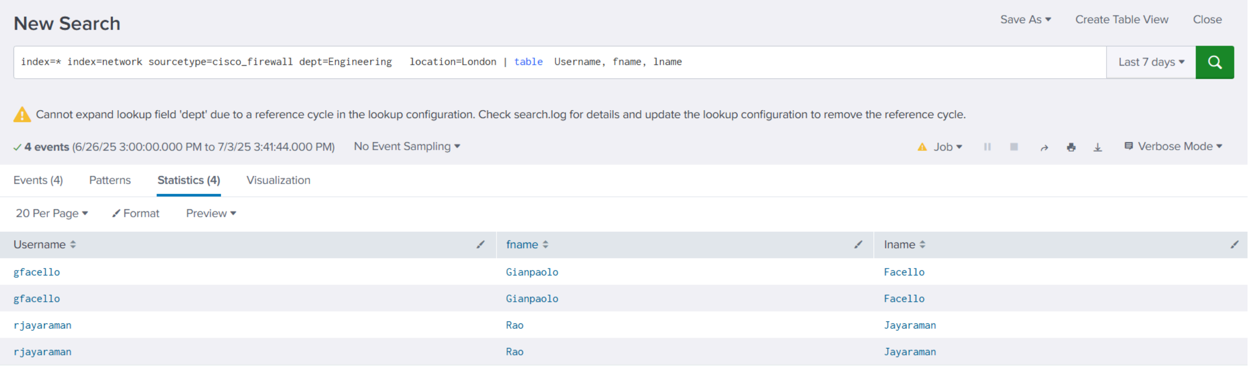


```
index="security" src_ip!=10.*  sourcetype=linux_secure host=www3
| stats  count(eval(action="failure")) as Failures, count(eval(action="success")) as Success by src_ip
| dedup src_ip | sort - Failures | head 10
```

✓ **164 events** (7/2/25 3:00:00.000 PM to 7/3/25 3:19:13.000 PM)

Prompt 7:

Create a table of user information based on team and location



```
index=* index=network sourcetype=cisco_firewall dept=Engineering   location=London | table  Username, fname, lname
```

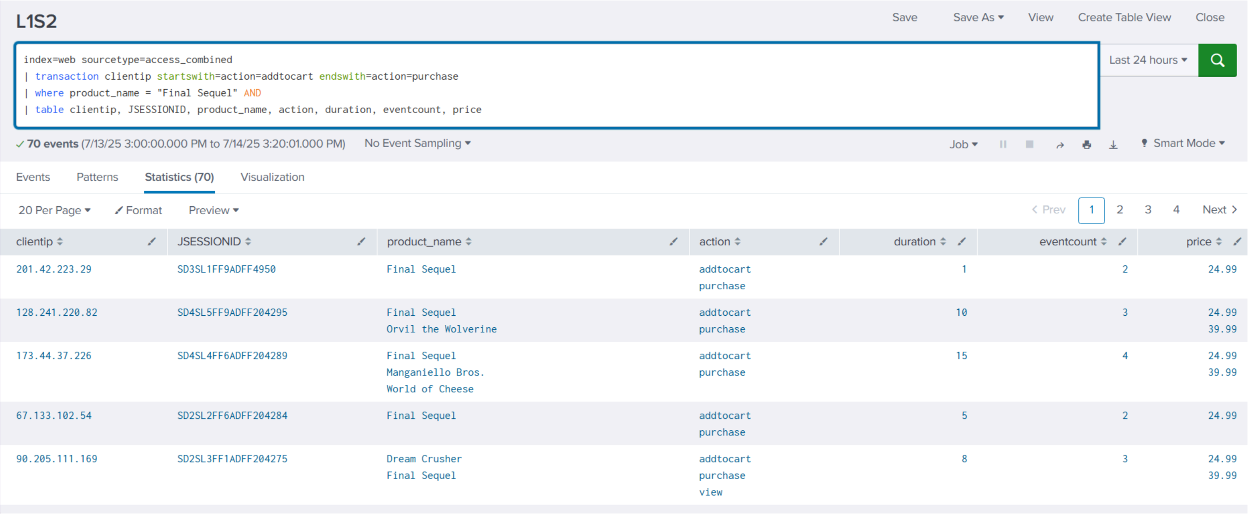
⚠ Cannot expand lookup field 'dept' due to a reference cycle in the lookup configuration. Check search.log for details and update the lookup configuration to remove the reference cycle.

✓ **4 events** (6/26/25 3:00:00.000 PM to 7/3/25 3:41:44.000 PM)

Username	fname	lname
gfacello	Gianpaolo	Facello
gfacello	Gianpaolo	Facello
rjayaraman	Rao	Jayaraman
rjayaraman	Rao	Jayaraman

Prompt 8:

Create a table of transactions for the game “Final Sequel”



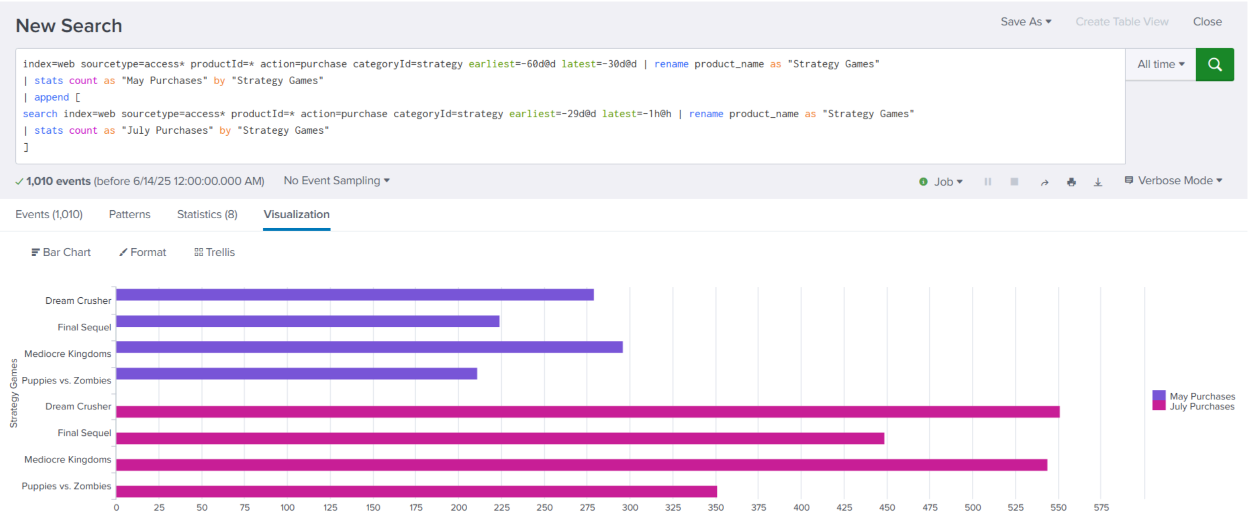
```
index=web sourcetype=access_combined
| transaction clientip startswith=action=addtocart endswith=action=purchase
| where product_name = "Final Sequel" AND
| table clientip, JSESSIONID, product_name, action, duration, eventcount, price
```

✓ **70 events** (7/13/25 3:00:00.000 PM to 7/14/25 3:20:01.000 PM) No Event Sampling ▾

clientip	JSESSIONID	product_name	action	duration	eventcount	price
201.42.223.29	SD3SL1FF9ADFF4950	Final Sequel	addtocart purchase	1	2	24.99
128.241.220.82	SD4SL5FF9ADFF204295	Final Sequel Orvil the Wolverine	addtocart purchase	10	3	24.99 39.99
173.44.37.226	SD4SL4FF6ADFF204289	Final Sequel Manganiello Bros. World of Cheese	addtocart purchase	15	4	24.99 39.99
67.133.102.54	SD2SL2FF6ADFF204284	Final Sequel	addtocart purchase	5	2	24.99
90.205.111.169	SD2SL3FF1ADFF204275	Dream Crusher Final Sequel	addtocart purchase view	8	3	24.99 39.99

Prompt 9:

Create a chart that compares the amount of strategy games purchased by month

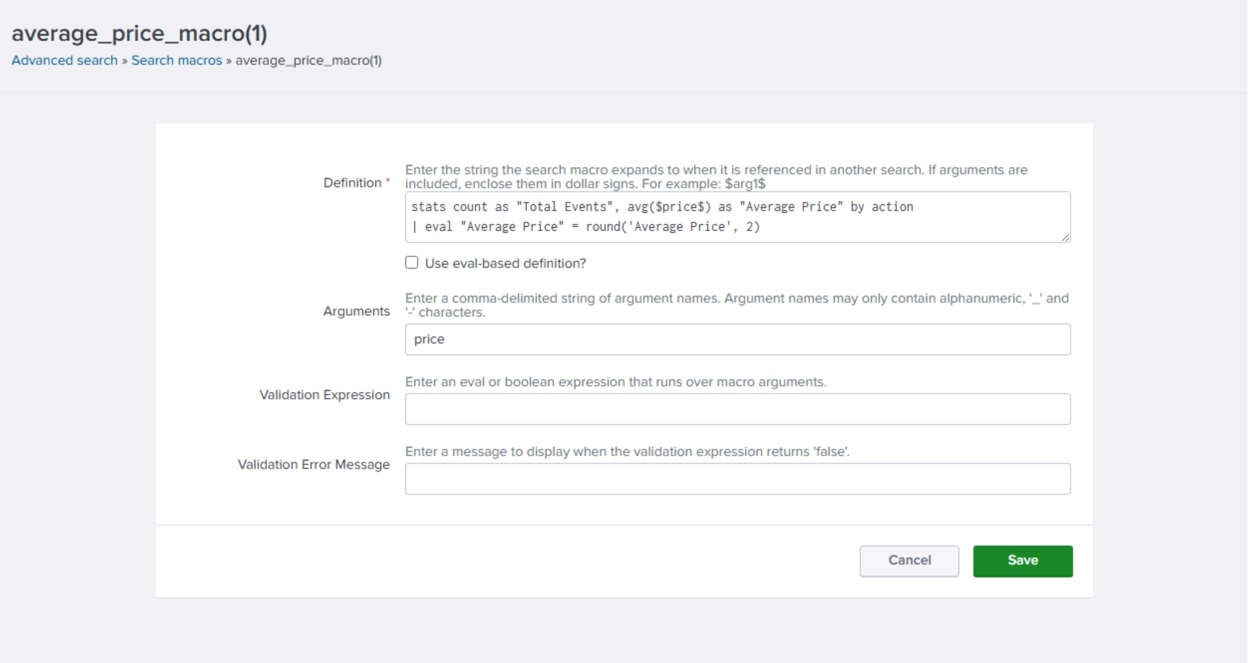


```
index=web sourcetype=access* productId=* action=purchase categoryId=strategy earliest=-60d@d latest=-30d@d | rename product_name as "Strategy Games"
| stats count as "May Purchases" by "Strategy Games"
| append [
search index=web sourcetype=access* productId=* action=purchase categoryId=strategy earliest=-29d@d latest=-1h@h | rename product_name as "Strategy Games"
| stats count as "July Purchases" by "Strategy Games"
]
```

✓ **1,010 events** (before 6/14/25 12:00:00.000 AM) No Event Sampling ▾

Prompt 10:

Create a macro that calculates the average price and then use that macro to make a chart



average_price_macro(1)

Advanced search » Search macros » average_price_macro(1)

Definition *

Enter the string the search macro expands to when it is referenced in another search. If arguments are included, enclose them in dollar signs. For example: $arg1$

```
stats count as "Total Events", avg($price$) as "Average Price" by action
| eval "Average Price" = round('Average Price', 2)
```

□ Use eval-based definition?

Arguments

Enter a comma-delimited string of argument names. Argument names may only contain alphanumeric, '_' and '-' characters.

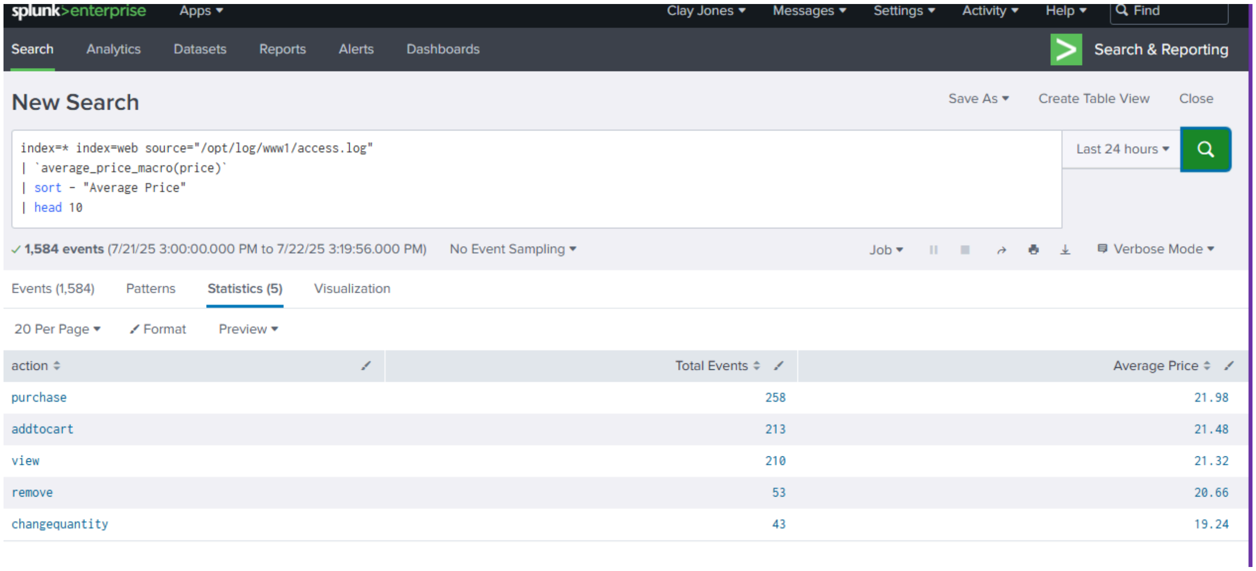
price

Validation Expression

Enter an eval or boolean expression that runs over macro arguments.

Validation Error Message

Enter a message to display when the validation expression returns 'false'.



New Search

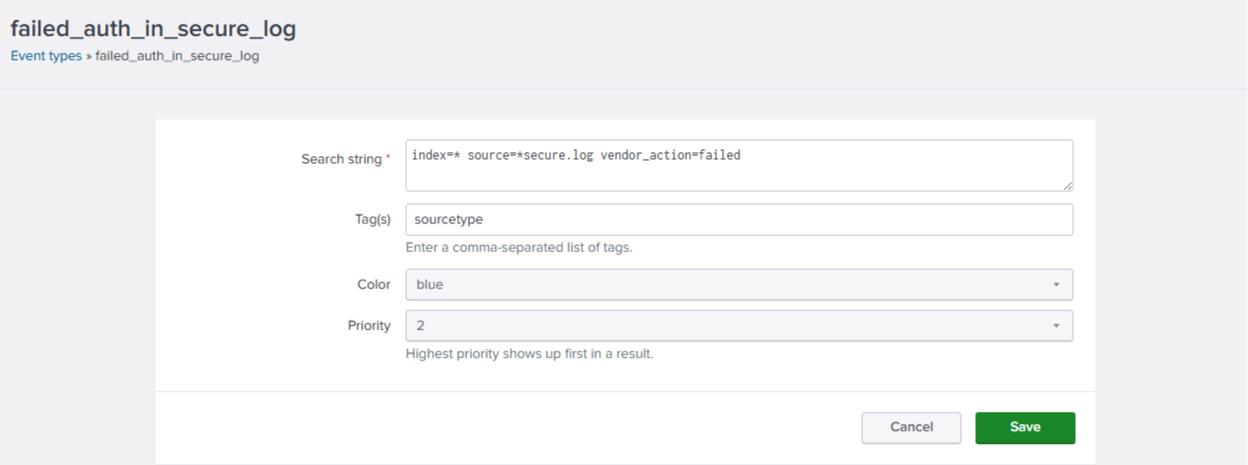
```
index=* index=web source="/opt/log/www1/access.log"
| `average_price_macro(price)`
| sort - "Average Price"
| head 10
```

✓ 1,584 events (7/21/25 3:00:00.000 PM to 7/22/25 3:19:56.000 PM)   No Event Sampling ▾

action	Total Events	Average Price
purchase	258	21.98
addtocart	213	21.48
view	210	21.32
remove	53	20.66
changequantity	43	19.24

Prompt 11:

Create an event type that returns failed logins



failed_auth_in_secure_log

Event types » failed_auth_in_secure_log

Search string *: `index=* source=*secure.log vendor_action=failed`

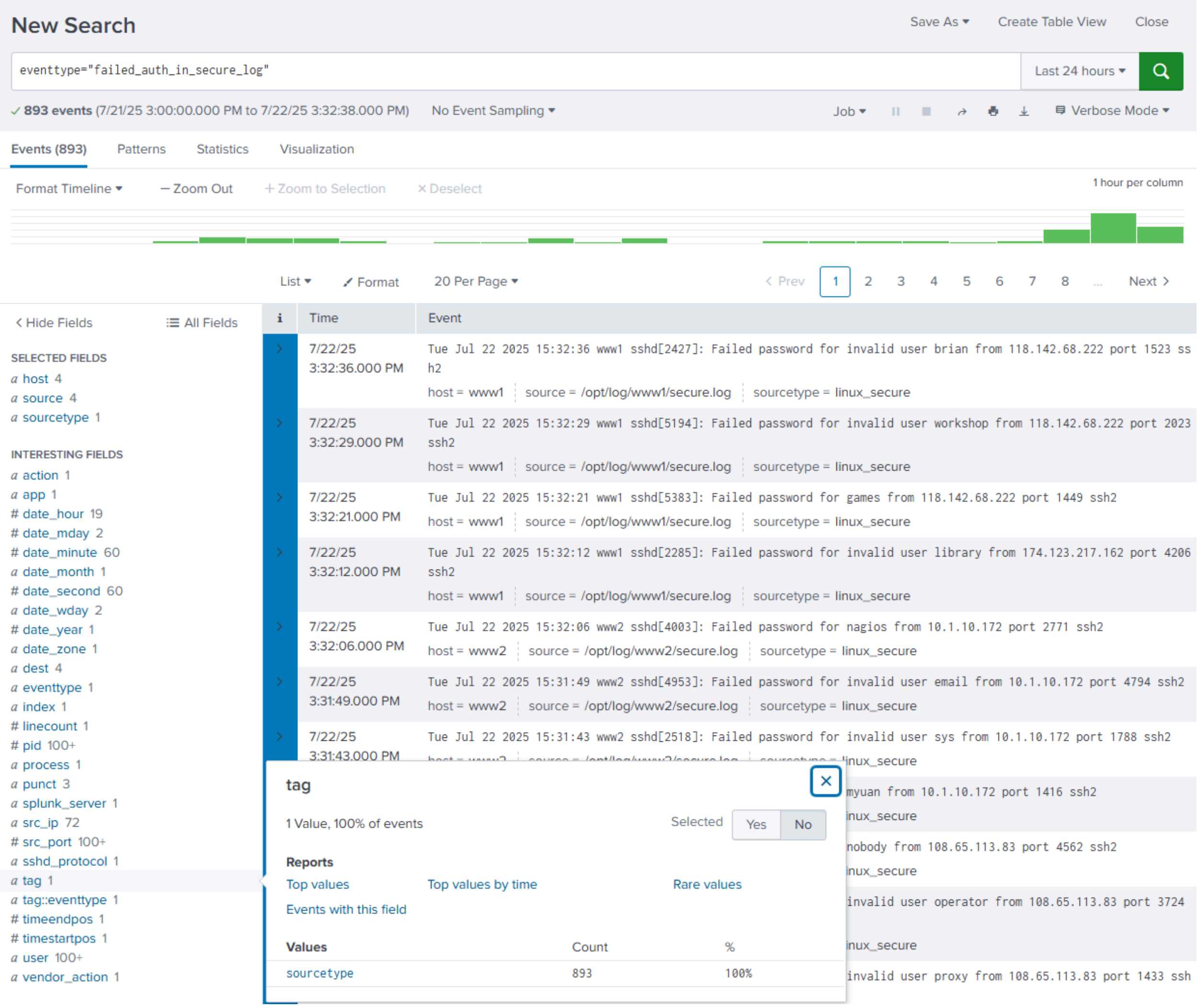
Tag(s): sourcetype

Enter a comma-separated list of tags.

Color: blue

Priority: 2

Highest priority shows up first in a result.



New Search

`eventtype="failed_auth_in_secure_log"`

Last 24 hours ▾

✓ 893 events (7/21/25 3:00:00.000 PM to 7/22/25 3:32:38.000 PM) No Event Sampling ▾

SELECTED FIELDS

- a host 4
- a source 4
- a sourcetype 1

INTERESTING FIELDS

- a action 1
- a app 1
- # date_hour 19
- # date_mday 2
- # date_minute 60
- a date_month 1
- # date_second 60
- a date_wday 2
- # date_year 1
- a date_zone 1
- a dest 4
- a eventtype 1
- a index 1
- # linecount 1
- # pid 100+
- a process 1
- a punct 3
- a splunk_server 1
- a src_ip 72
- # src_port 100+
- a sshd_protocol 1
- a tag 1
- a tag::eventtype 1
- # timeendpos 1
- # timestartpos 1
- a user 100+
- a vendor_action 1

i	Time	Event
›	7/22/25 3:32:36.000 PM	Tue Jul 22 2025 15:32:36 www1 sshd[2427]: Failed password for invalid user brian from 118.142.68.222 port 1523 ssh2 host = www1 source = /opt/log/www1/secure.log sourcetype = linux_secure
›	7/22/25 3:32:29.000 PM	Tue Jul 22 2025 15:32:29 www1 sshd[5194]: Failed password for invalid user workshop from 118.142.68.222 port 2023 ssh2 host = www1 source = /opt/log/www1/secure.log sourcetype = linux_secure
›	7/22/25 3:32:21.000 PM	Tue Jul 22 2025 15:32:21 www1 sshd[5383]: Failed password for games from 118.142.68.222 port 1449 ssh2 host = www1 source = /opt/log/www1/secure.log sourcetype = linux_secure
›	7/22/25 3:32:12.000 PM	Tue Jul 22 2025 15:32:12 www1 sshd[2285]: Failed password for invalid user library from 174.123.217.162 port 4206 ssh2 host = www1 source = /opt/log/www1/secure.log sourcetype = linux_secure
›	7/22/25 3:32:06.000 PM	Tue Jul 22 2025 15:32:06 www2 sshd[4003]: Failed password for nagios from 10.1.10.172 port 2771 ssh2 host = www2 source = /opt/log/www2/secure.log sourcetype = linux_secure
›	7/22/25 3:31:49.000 PM	Tue Jul 22 2025 15:31:49 www2 sshd[4953]: Failed password for invalid user email from 10.1.10.172 port 4794 ssh2 host = www2 source = /opt/log/www2/secure.log sourcetype = linux_secure
›	7/22/25 3:31:43.000 PM	Tue Jul 22 2025 15:31:43 www2 sshd[2518]: Failed password for invalid user sys from 10.1.10.172 port 1788 ssh2 linux_secure
		myuan from 10.1.10.172 port 1416 ssh2 inux_secure
		nobody from 108.65.113.83 port 4562 ssh2 inux_secure
		invalid user operator from 108.65.113.83 port 3724 inux_secure
		invalid user proxy from 108.65.113.83 port 1433 ssh

tag

1 Value, 100% of events

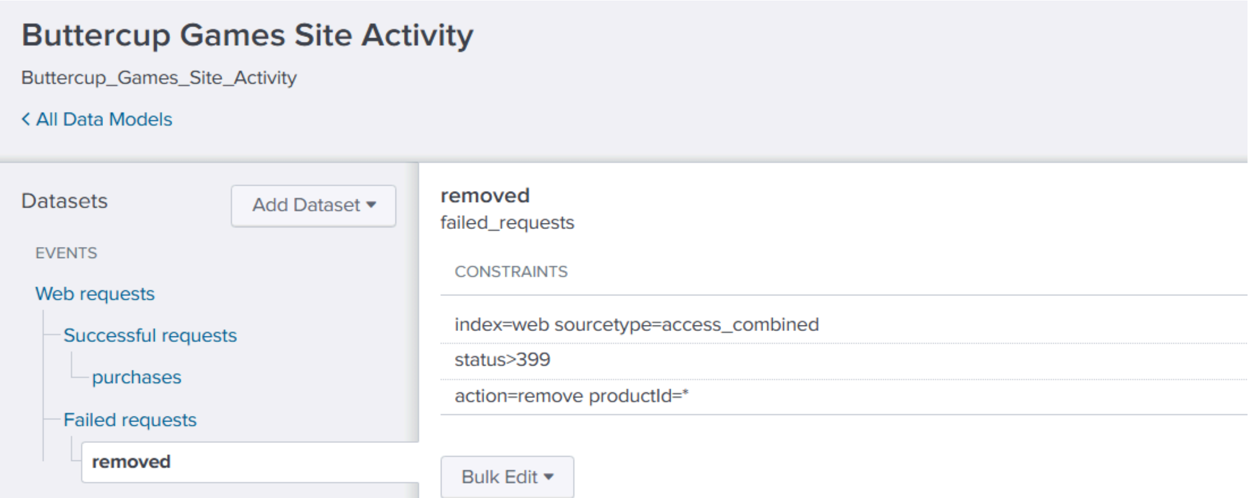
Selected: Yes [✓ No]

Reports

Values	Count	%
sourcetype	893	100%

Prompt 12:

Create a data model, run a pivot, and then accelerate that data model.



Buttercup Games Site Activity

Buttercup_Games_Site_Activity

< All Data Models

Datasets

EVENTS

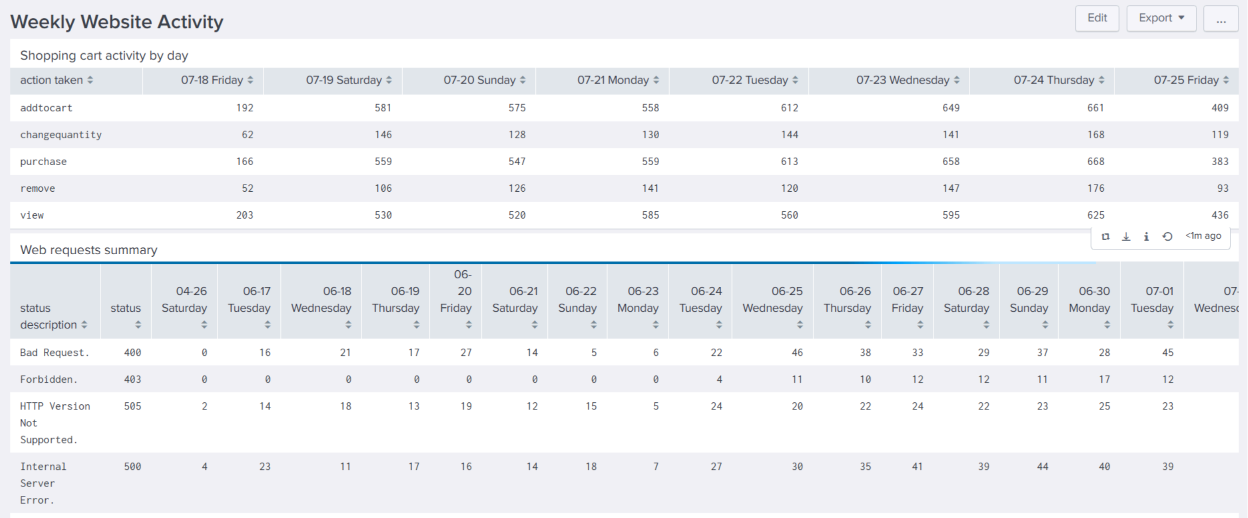
- Web requests
  - Successful requests
    - purchases
  - Failed requests
    - removed

removed

failed_requests

CONSTRAINTS

```
index=web sourcetype=access_combined
status>399
action=remove productId=*
```



Weekly Website Activity

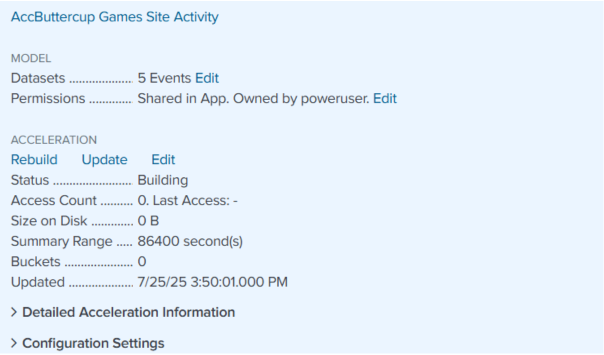
Shopping cart activity by day

action taken	07-18 Friday	07-19 Saturday	07-20 Sunday	07-21 Monday	07-22 Tuesday	07-23 Wednesday	07-24 Thursday	07-25 Friday
addtocart	192	581	575	558	612	649	661	409
changequantity	62	146	128	130	144	141	168	119
purchase	166	559	547	559	613	658	668	383
remove	52	106	126	141	120	147	176	93
view	203	530	520	585	560	595	625	436

<1m ago

Web requests summary

status description	status	04-26 Saturday	06-17 Tuesday	06-18 Wednesday	06-19 Thursday	06-20 Friday	06-21 Saturday	06-22 Sunday	06-23 Monday	06-24 Tuesday	06-25 Wednesday	06-26 Thursday	06-27 Friday	06-28 Saturday	06-29 Sunday	06-30 Monday	07-01 Tuesday	07- Wednesd
Bad Request.	400	0	16	21	17	27	14	5	6	22	46	38	33	29	37	28	45	
Forbidden.	403	0	0	0	0	0	0	0	0	4	11	10	12	12	11	17	12	
HTTP Version Not Supported.	505	2	14	18	13	19	12	15	5	24	20	22	24	22	23	25	23	
Internal Server Error.	500	4	23	11	17	16	14	18	7	27	30	35	41	39	44	40	39	



AccButtercup Games Site Activity

MODEL

Datasets .... 5 Events Edit

Permissions .... Shared in App. Owned by poweruser. Edit

ACCELERATION

Rebuild Update Edit

Status .... Building

Access Count .... 0. Last Access: -

Size on Disk .... 0 B

Summary Range ..... 86400 second(s)

Buckets 0

Updated .... 7/25/25 3:50:01.000 PM

> Detailed Acceleration Information

> Configuration Settings

Lessons Learned:

Overall, I learned how to perform splunk queries in an efficient manner while also taking advantage of the numerous knowledge objects splunk has to offer to streamline splunk actions.