SPLUNK
QUERY, ALERT, AND DASHBOARD CREATION

Jordan Patterson

This document contains examples of Query creation, Alert creation, and Dashboard creation in SPLUNK.

Table of Contents

Scenario 1: Basic HTTP Status Code Count

Title: Counting HTTP Status Codes

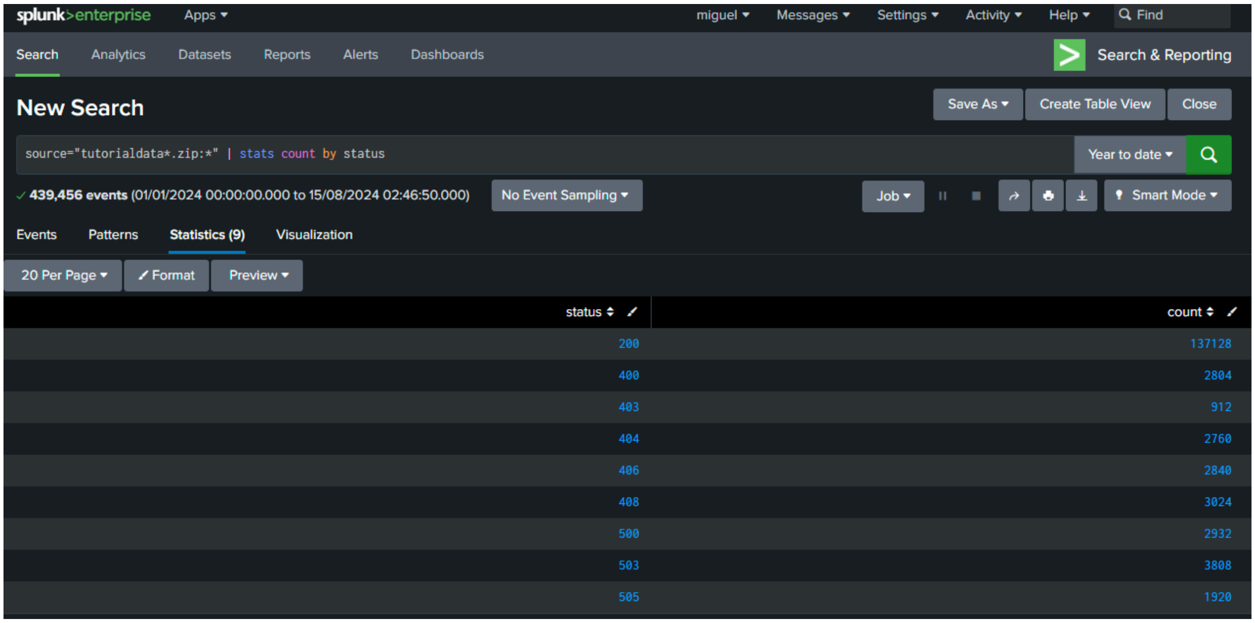
Steps to Create Search and Panel:

- Open Splunk and navigate to the Search & Reporting app.
- In the search bar, enter the query to count HTTP status codes.
- Create a table visualization for the results.

Search Query:

source="tutorialdata*.zip:*" | stats count by status

Scenario 1 Search Results:



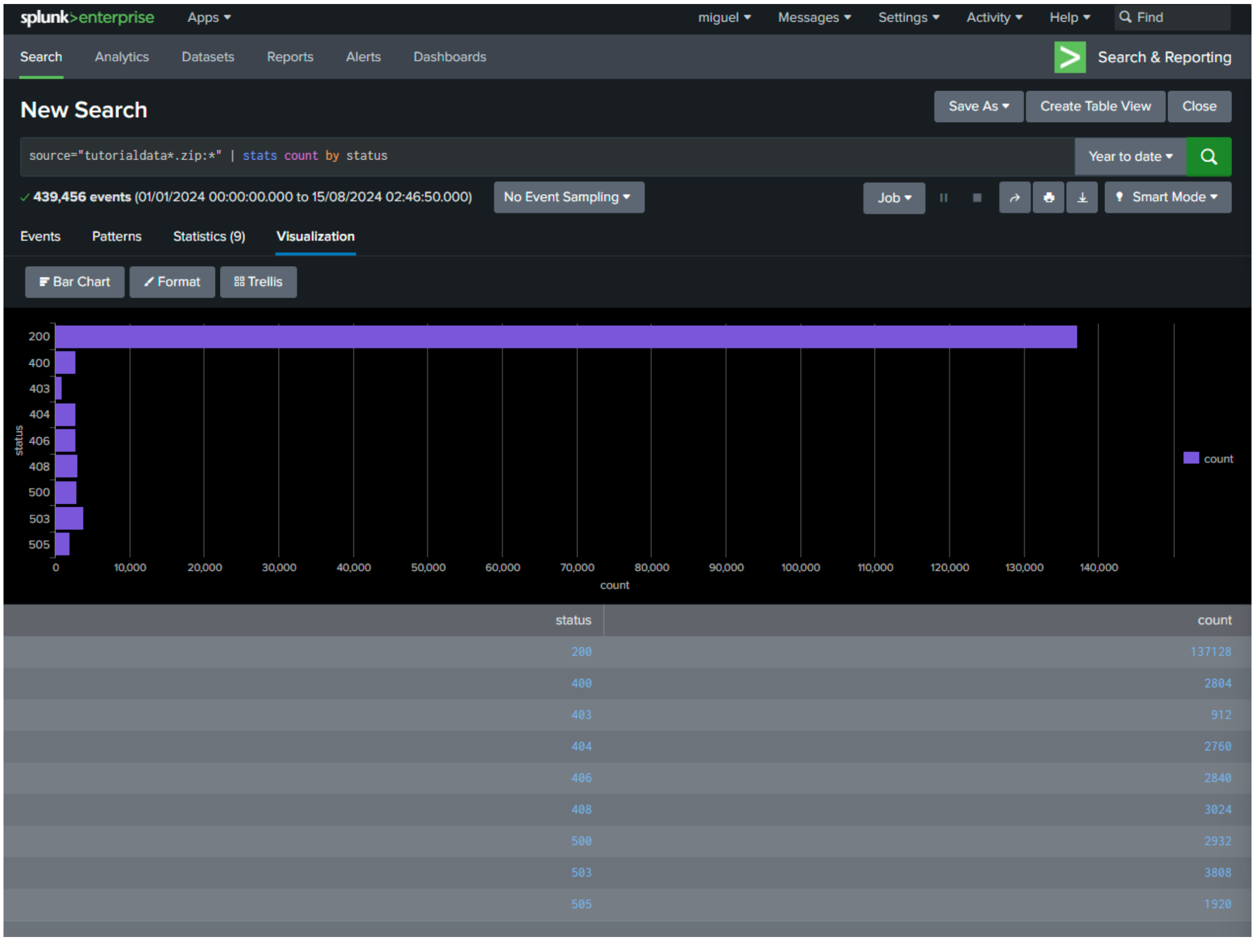
New Search

```
source="tutorialdata*.zip:*" | stats count by status
```

✓ 439,456 events (01/01/2024 00:00:00.000 to 15/08/2024 02:46:50.000)

status	count
200	137128
400	2804
403	912
404	2760
406	2840
408	3024
500	2932
503	3808
505	1920

Scenario 1 Visualized as a Table:



```
source="tutorialdata*.zip:*" | stats count by status
```

✓ **439,456 events** (01/01/2024 00:00:00.000 to 15/08/2024 02:46:50.000)

status	count
200	137128
400	2804
403	912
404	2760
406	2840
408	3024
500	2932
503	3808
505	1920

Scenario 2: Failed Login Attempts

Title: Identifying Failed Login Attempts

Description: Find and count failed login attempts in the secure logs.

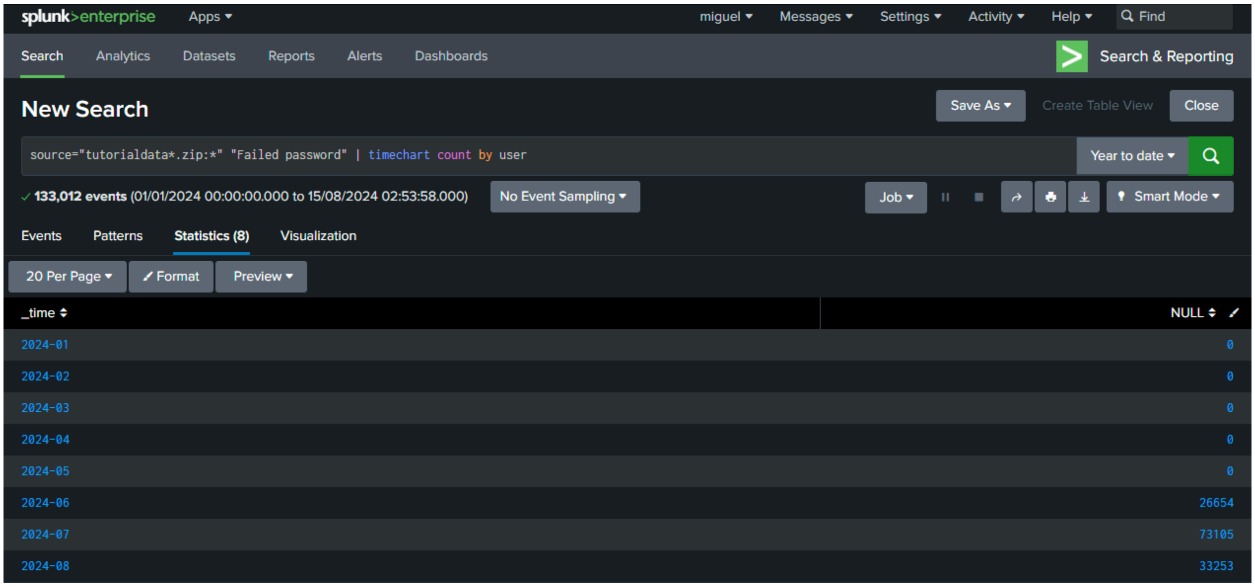
Steps to Create Search and Panel:

- Open Splunk and go to the Search & Reporting app.
- Enter the query to search for failed password attempts.
- Visualize the results as a time chart.

Search Query:

source="tutorialdata*.zip:*" "Failed password" | timechart count by user

Scenario 2 search results:



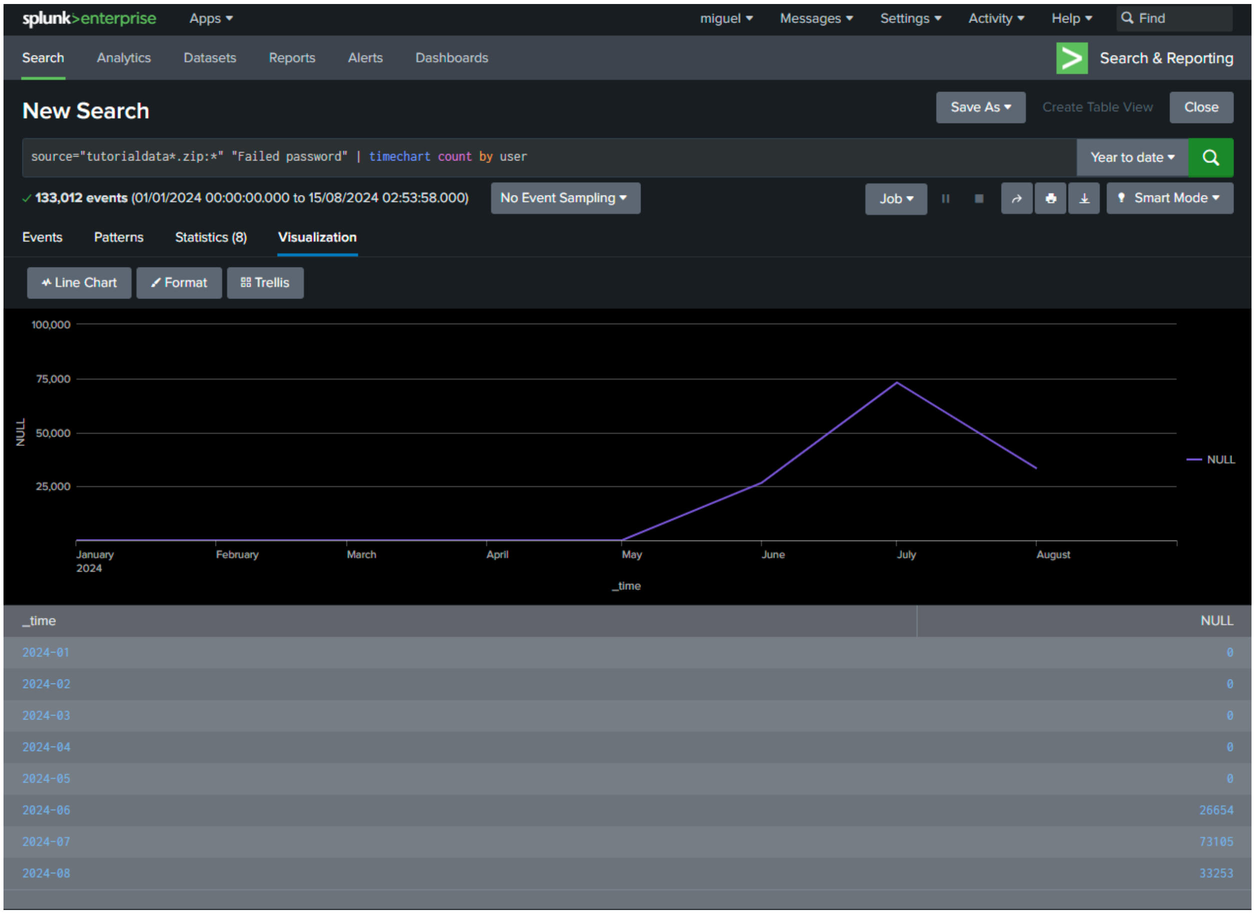
New Search

```
source="tutorialdata*.zip:*" "Failed password" | timechart count by user
```

✓ 133,012 events (01/01/2024 00:00:00.000 to 15/08/2024 02:53:58.000)

_time	NULL
2024-01	0
2024-02	0
2024-03	0
2024-04	0
2024-05	0
2024-06	26654
2024-07	73105
2024-08	33253

Scenario 2 Visualized as a Time Chart:



```
source="tutorialdata*.zip:*" "Failed password" | timechart count by user
```

✓ **133,012 events** (01/01/2024 00:00:00.000 to 15/08/2024 02:53:58.000)

_time	NULL
2024-01	0
2024-02	0
2024-03	0
2024-04	0
2024-05	0
2024-06	26654
2024-07	73105
2024-08	33253

Scenario 3: Vendor Sales by Code

Title: Vendor Sales Analysis by Code

Description: Analyze sales data by vendor codes from the vendor sales logs.

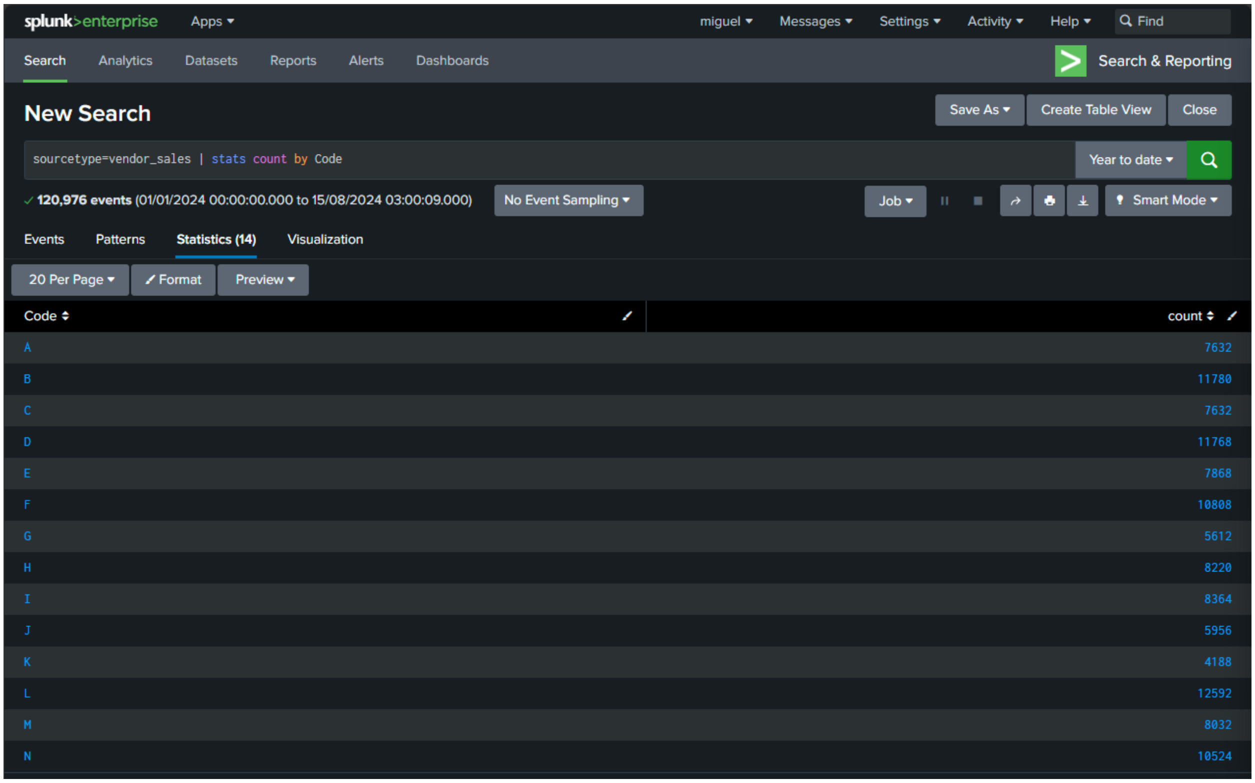
Steps to Create Search and Panel:

- Open the Search & Reporting app in Splunk.
- Enter the query to count sales by vendor code.
- Create a pie chart for the results.

Search Query:

sourcetype=vendor_sales | stats count by Code

Scenario 3 search results:

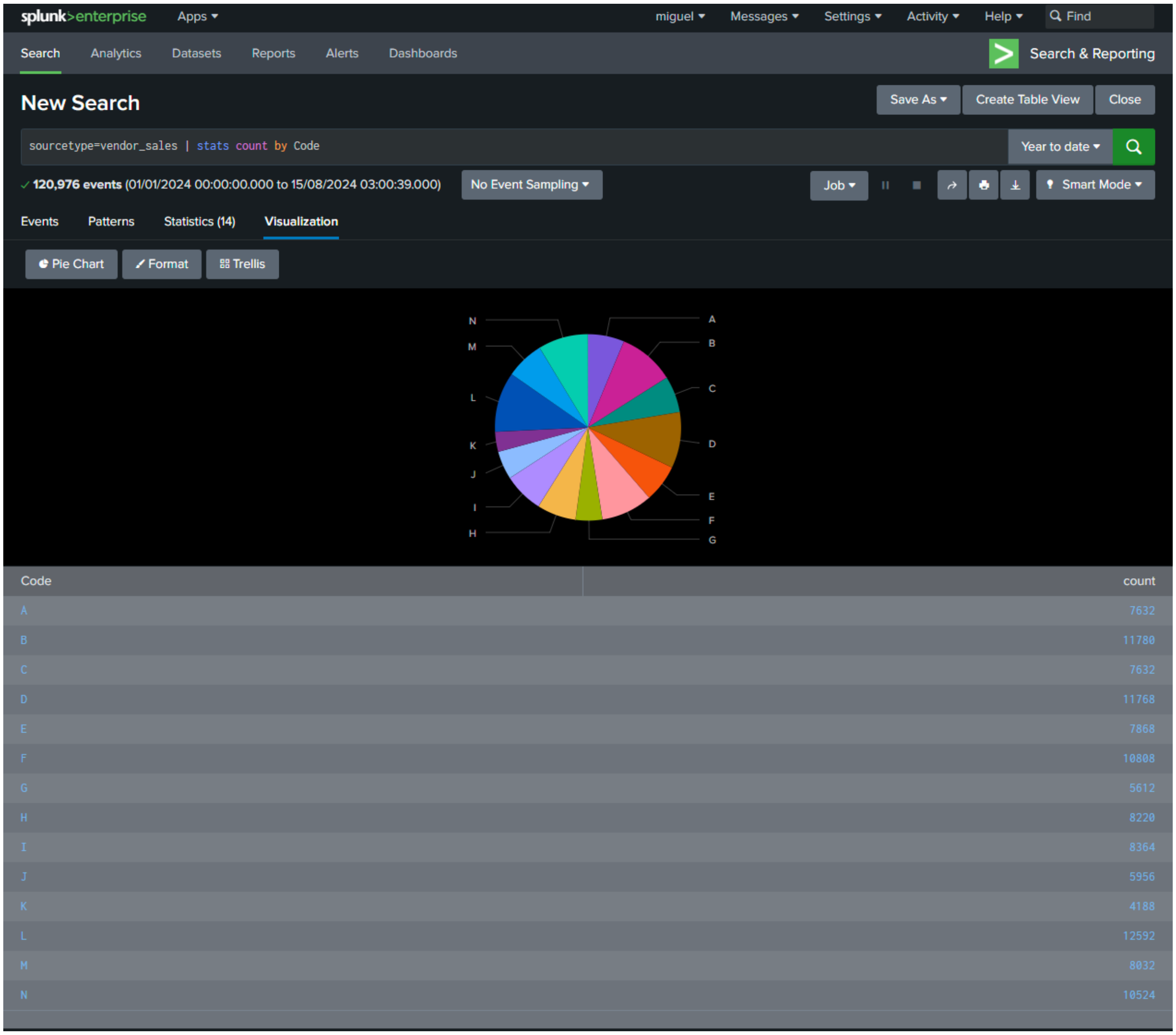


```
sourcetype=vendor_sales | stats count by Code
```

✓ 120,976 events (01/01/2024 00:00:00.000 to 15/08/2024 03:00:09.000)

Code	count
A	7632
B	11780
C	7632
D	11768
E	7868
F	10808
G	5612
H	8220
I	8364
J	5956
K	4188
L	12592
M	8032
N	10524

Scenario 3 Visualized as a Pie Chart:



```
sourcetype=vendor_sales | stats count by Code
```

✓ **120,976 events** (01/01/2024 00:00:00.000 to 15/08/2024 03:00:39.000)

Code	count
A	7632
B	11780
C	7632
D	11768
E	7868
F	10808
G	5612
H	8220
I	8364
J	5956
K	4188
L	12592
M	8032
N	10524

Scenario 4: Top IP Addresses Accessing Site

Title: Top IP Addresses Accessing the Website

Description: Identify the top IP addresses accessing the website from the access logs.

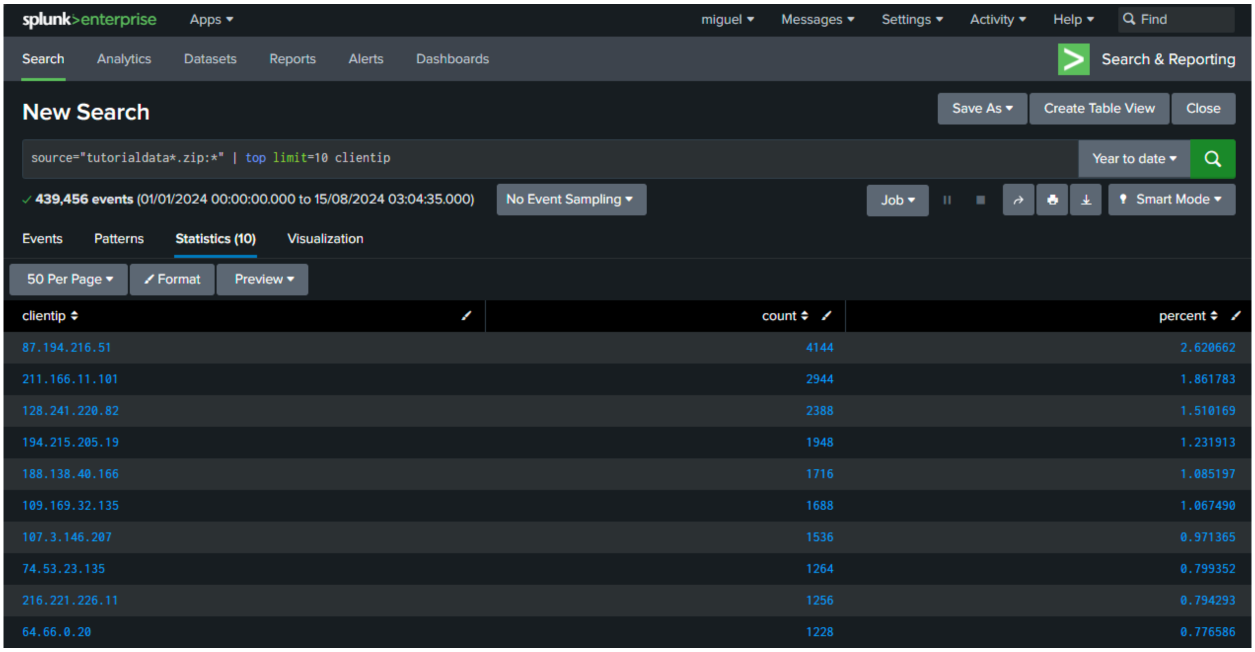
Steps to Create Search and Panel:

- Open Splunk and navigate to the Search & Reporting app.
- Enter the query to find the top IP addresses.
- Create a bar chart for the results.

Search Query:

source="tutorialdata*.zip:*" | top limit=10 clientip

Scenario 4 search results:



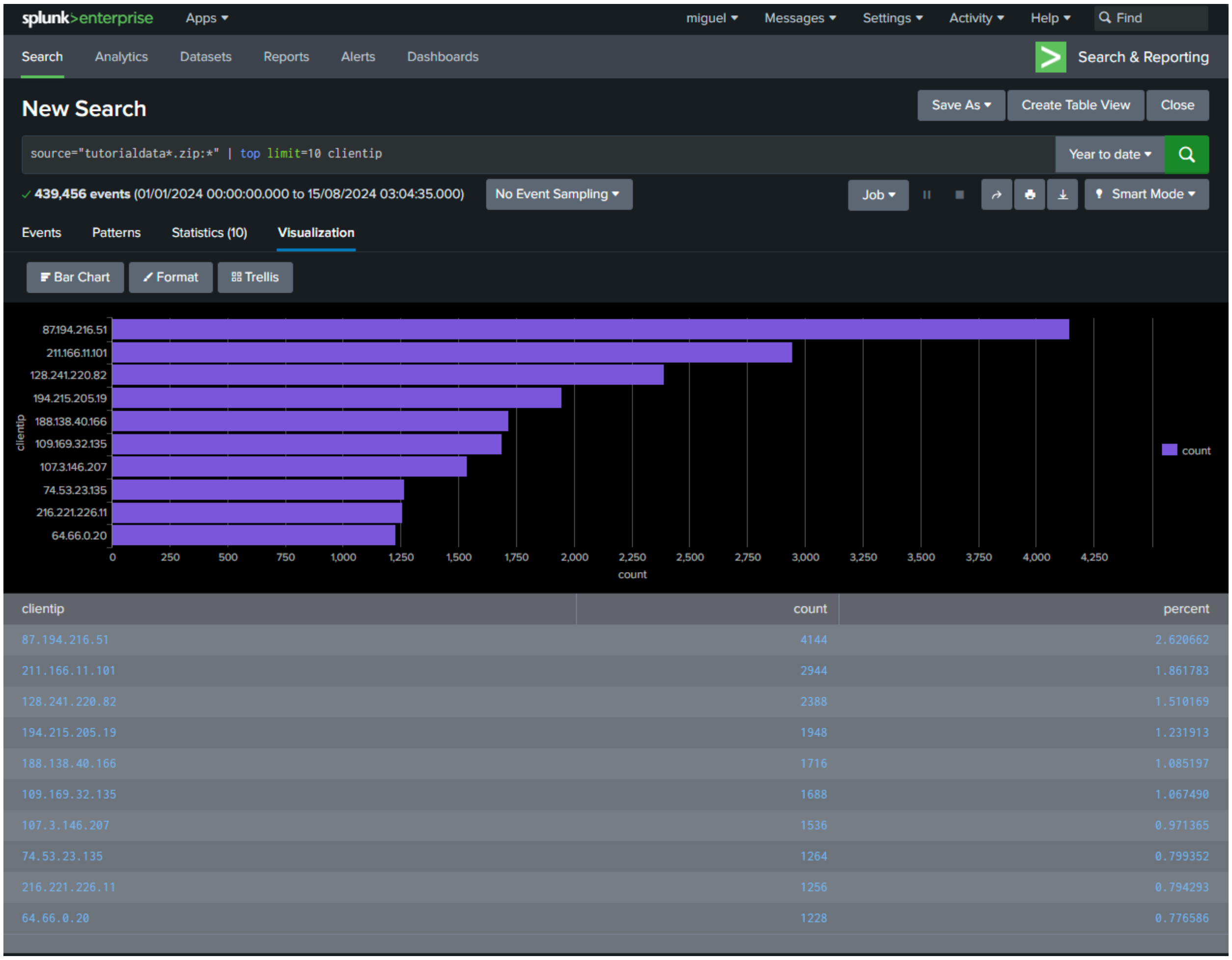
New Search

```
source="tutorialdata*.zip:*" | top limit=10 clientip
```

✓ 439,456 events (01/01/2024 00:00:00.000 to 15/08/2024 03:04:35.000) No Event Sampling

clientip	count	percent
87.194.216.51	4144	2.620662
211.166.11.101	2944	1.861783
128.241.220.82	2388	1.510169
194.215.205.19	1948	1.231913
188.138.40.166	1716	1.085197
109.169.32.135	1688	1.067490
107.3.146.207	1536	0.971365
74.53.23.135	1264	0.799352
216.221.226.11	1256	0.794293
64.66.0.20	1228	0.776586

Scenario 4 Visualized as a Bar Chart:



```
source="tutorialdata*.zip:*" | top limit=10 clientip
```

✓ **439,456 events** (01/01/2024 00:00:00.000 to 15/08/2024 03:04:35.000)

clientip	count	percent
87.194.216.51	4144	2.620662
211.166.11.101	2944	1.861783
128.241.220.82	2388	1.510169
194.215.205.19	1948	1.231913
188.138.40.166	1716	1.085197
109.169.32.135	1688	1.067490
107.3.146.207	1536	0.971365
74.53.23.135	1264	0.799352
216.221.226.11	1256	0.794293
64.66.0.20	1228	0.776586

Scenario 5: SSH Login Sessions

Title: Tracking SSH Login Sessions

Description: Track the number of successful SSH login sessions from the secure logs.

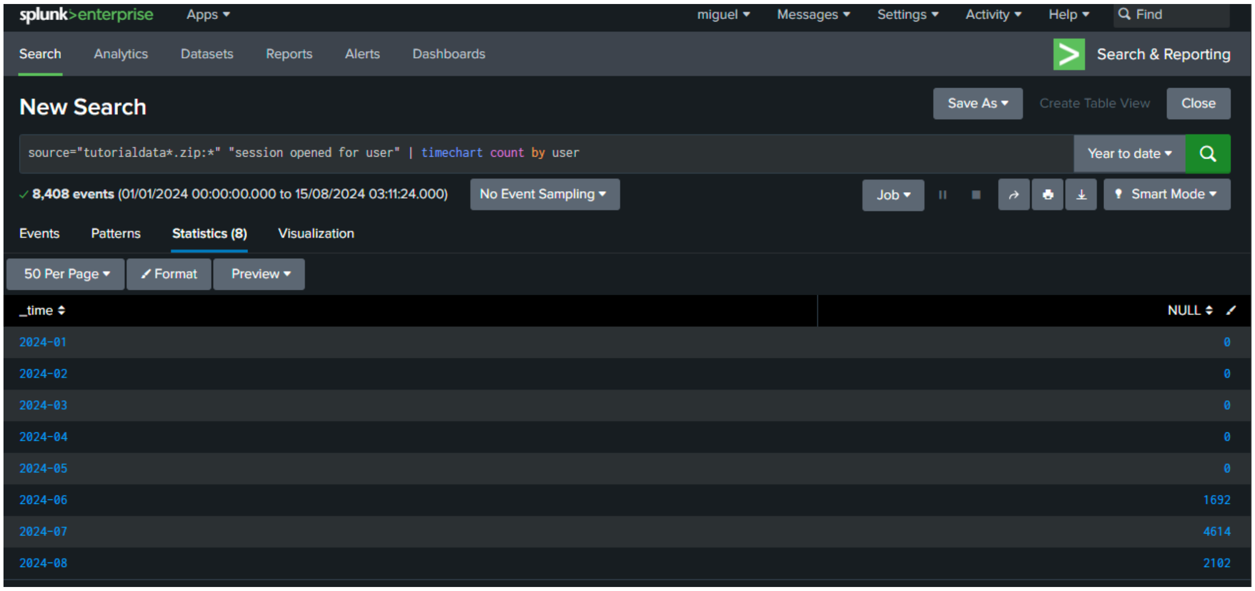
Steps to Create Search and Panel:

- Go to the Search & Reporting app in Splunk.
- Enter the query to find successful SSH login sessions.
- Create a time chart for the results.

Search Query:

source="tutorialdata*.zip:*" "session opened for user" | timechart count by user

Scenario 5 search results:

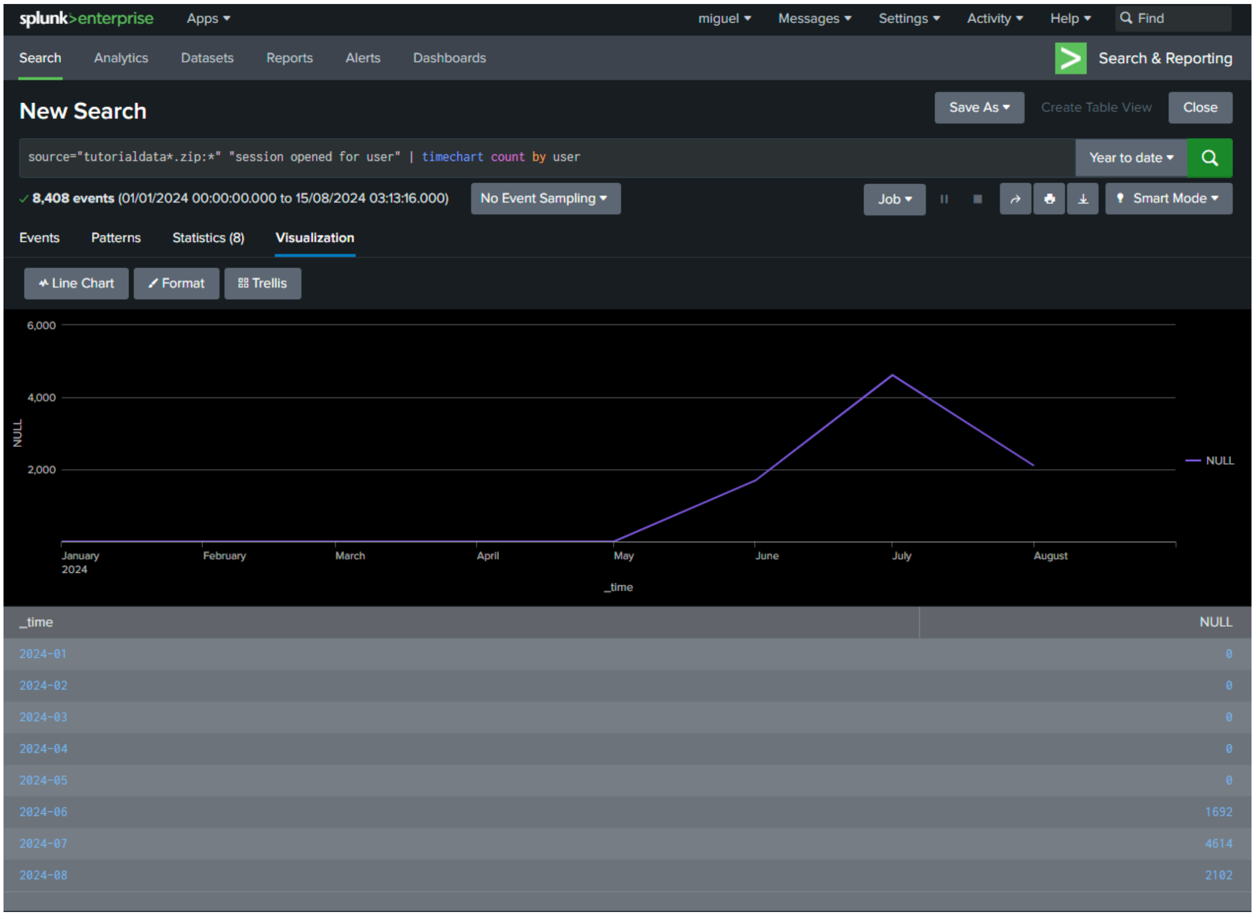


```
source="tutorialdata*.zip:*" "session opened for user" | timechart count by user
```

✓ 8,408 events (01/01/2024 00:00:00.000 to 15/08/2024 03:11:24.000)

_time	NULL
2024-01	0
2024-02	0
2024-03	0
2024-04	0
2024-05	0
2024-06	1692
2024-07	4614
2024-08	2102

Scenario 5 Visualized as a Time Chart:



```
source="tutorialdata*.zip:*" "session opened for user" | timechart count by user
```

✓ **8,408 events** (01/01/2024 00:00:00.000 to 15/08/2024 03:13:16.000)

_time	NULL
2024-01	0
2024-02	0
2024-03	0
2024-04	0
2024-05	0
2024-06	1692
2024-07	4614
2024-08	2102

Scenario 6: HTTP Methods Usage

Title: Analyzing HTTP Methods

Description: Analyze the usage of different HTTP methods from the access logs.

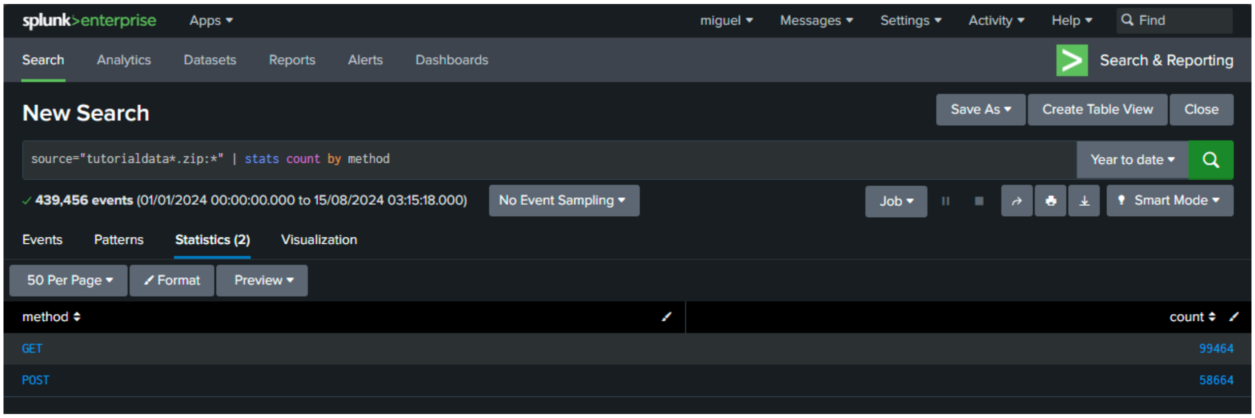
Steps to Create Search and Panel:

- Open Splunk and navigate to the Search & Reporting app.
- Enter the query to count the usage of HTTP methods.
- Create a bar chart for the results.

Search Query:

source="tutorialdata*.zip:*" | stats count by method

Scenario 6 search results:

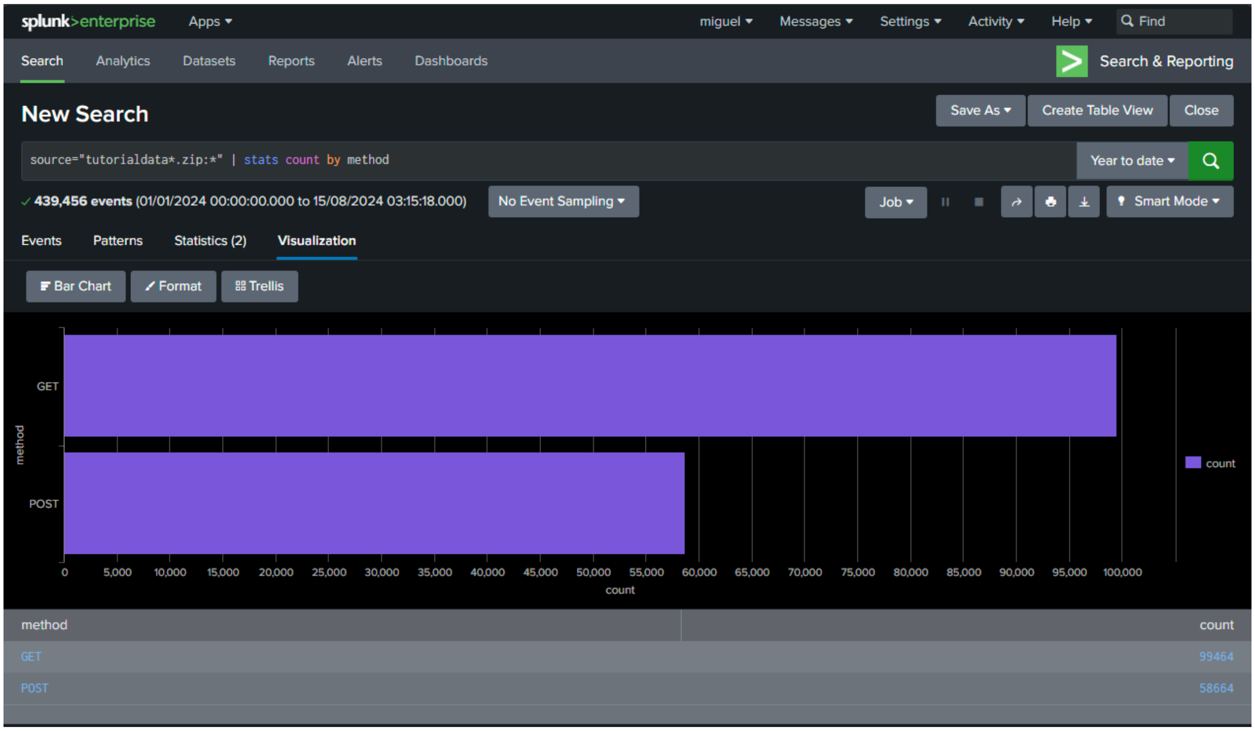


```
source="tutorialdata*.zip:*" | stats count by method
```

✓ 439,456 events (01/01/2024 00:00:00.000 to 15/08/2024 03:15:18.000)

method	count
GET	99464
POST	58664

Scenario 6 Visualized as a Bar Chart:



```
source="tutorialdata*.zip:*" | stats count by method
```

✓ **439,456 events** (01/01/2024 00:00:00.000 to 15/08/2024 03:15:18.000)

method	count
GET	99464
POST	58664

Scenario 7: Vendor Sales Over Time

Title: Sales Trends Over Time

Description: Track vendor sales trends over time from the vendor sales logs.

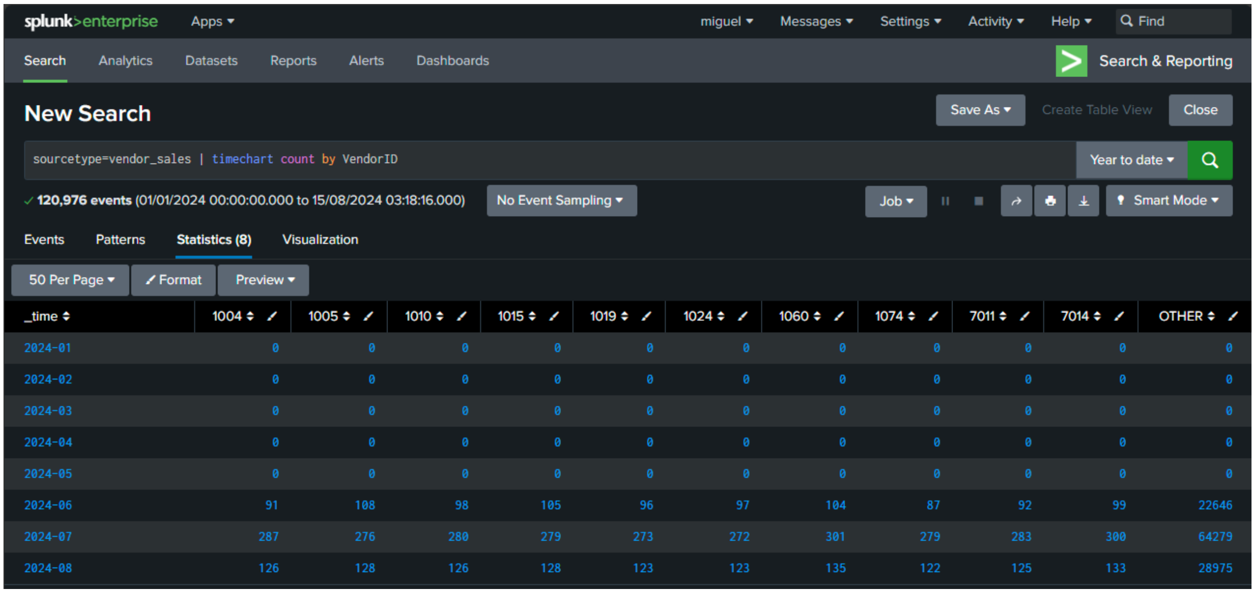
Steps to Create Search and Panel:

- Open the Search & Reporting app in Splunk.
- Enter the query to count sales over time.
- Create a line chart for the results.

Search Query:

sourcetype=vendor_sales | timechart count by VendorID

Scenario 7 search results:



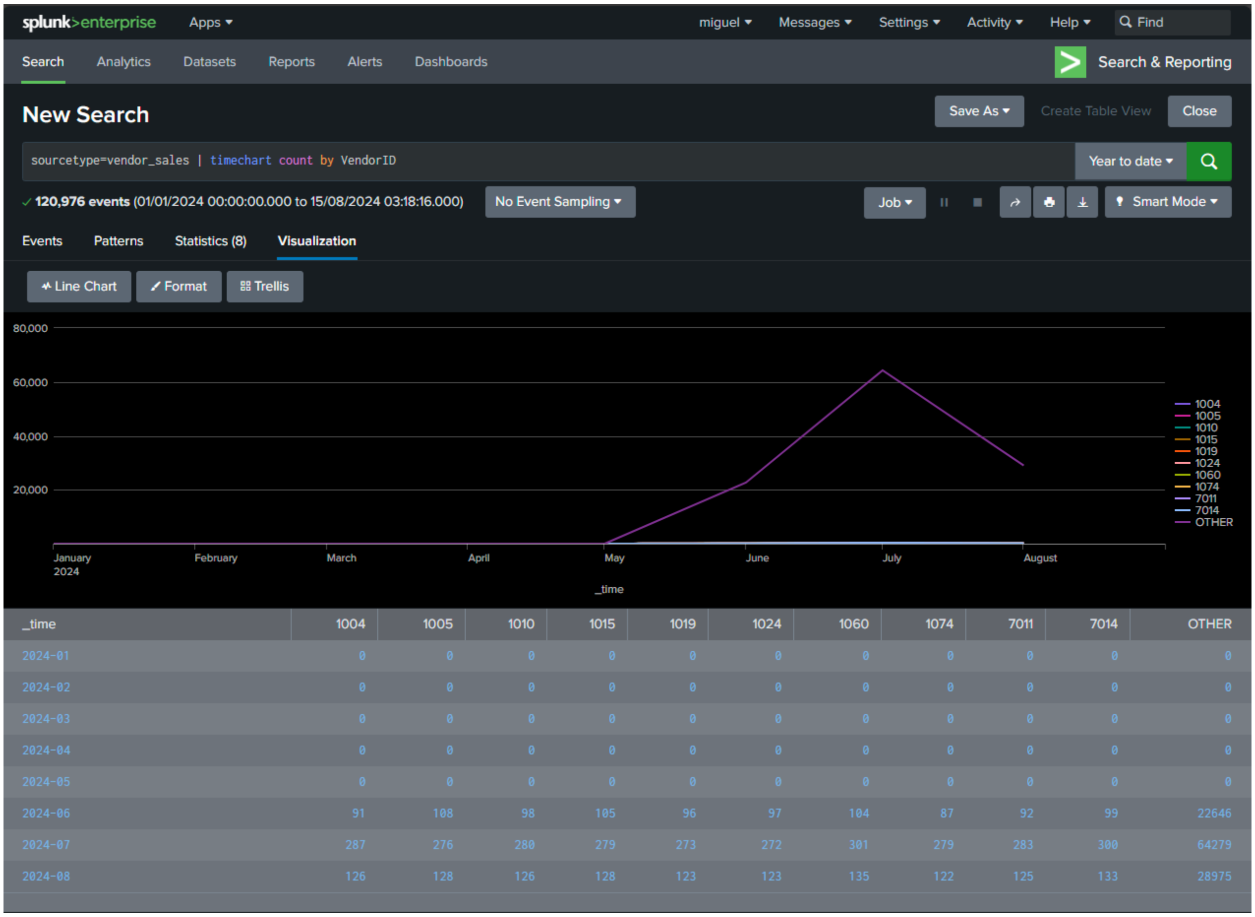
New Search

```
sourcetype=vendor_sales | timechart count by VendorID
```

✓ **120,976 events** (01/01/2024 00:00:00.000 to 15/08/2024 03:18:16.000)

_time	1004	1005	1010	1015	1019	1024	1060	1074	7011	7014	OTHER
2024-01	0	0	0	0	0	0	0	0	0	0	0
2024-02	0	0	0	0	0	0	0	0	0	0	0
2024-03	0	0	0	0	0	0	0	0	0	0	0
2024-04	0	0	0	0	0	0	0	0	0	0	0
2024-05	0	0	0	0	0	0	0	0	0	0	0
2024-06	91	108	98	105	96	97	104	87	92	99	22646
2024-07	287	276	280	279	273	272	301	279	283	300	64279
2024-08	126	128	126	128	123	123	135	122	125	133	28975

Scenario 7 Visualized as a Line Chart:



```
sourcetype=vendor_sales | timechart count by VendorID
```

✓ **120,976 events** (01/01/2024 00:00:00.000 to 15/08/2024 03:18:16.000)

_time	1004	1005	1010	1015	1019	1024	1060	1074	7011	7014	OTHER
2024-01	0	0	0	0	0	0	0	0	0	0	0
2024-02	0	0	0	0	0	0	0	0	0	0	0
2024-03	0	0	0	0	0	0	0	0	0	0	0
2024-04	0	0	0	0	0	0	0	0	0	0	0
2024-05	0	0	0	0	0	0	0	0	0	0	0
2024-06	91	108	98	105	96	97	104	87	92	99	22646
2024-07	287	276	280	279	273	272	301	279	283	300	64279
2024-08	126	128	126	128	123	123	135	122	125	133	28975

Scenario 8: Common User Agents

Title: Analyzing User Agents

Description: Identify the most common user agents accessing the website from the access logs.

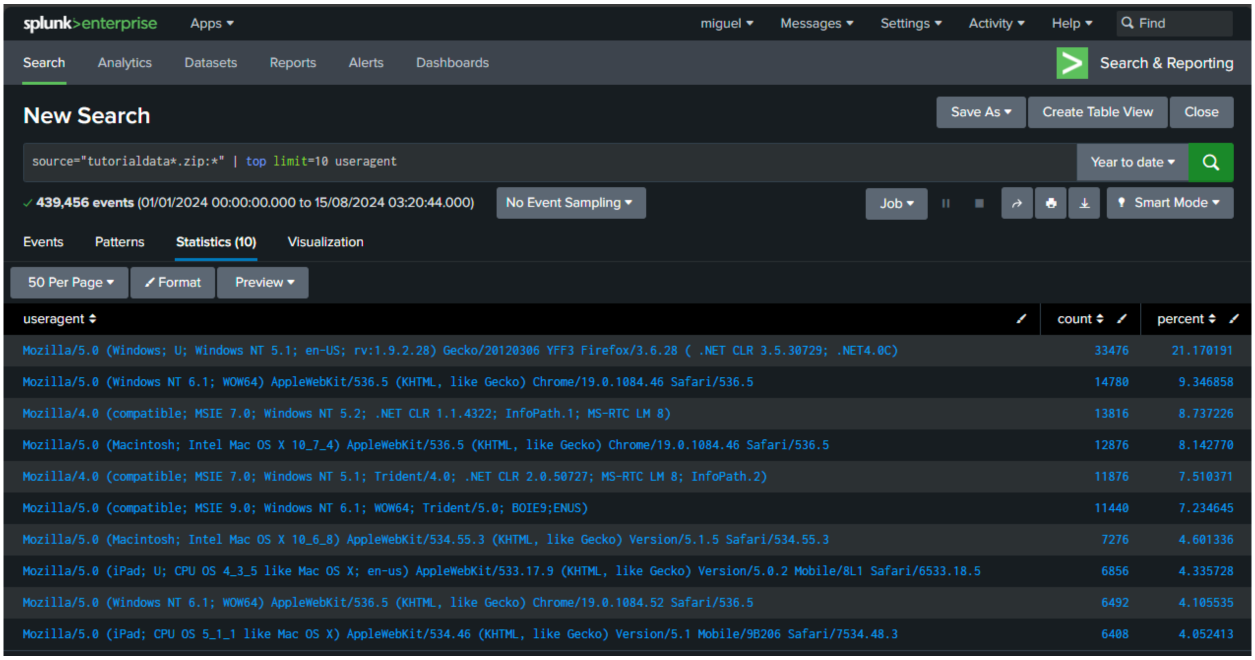
Steps to Create Search and Panel:

- Open Splunk and go to the Search & Reporting app.
- Enter the query to find the top user agents.
- Create a pie chart for the results.

Search Query:

source="tutorialdata*.zip:*" | top limit=10 useragent

Scenario 8 search results:

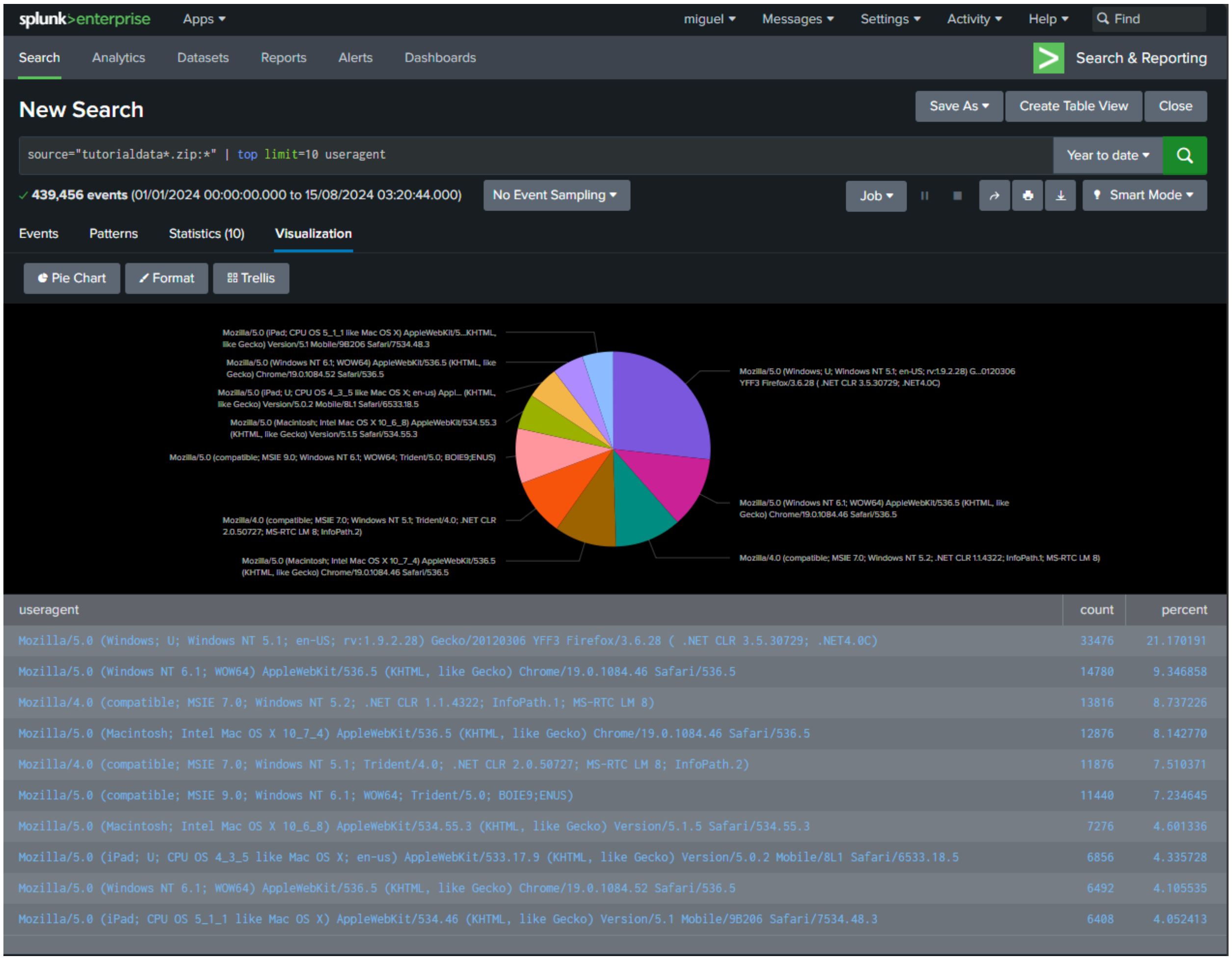


```
source="tutorialdata*.zip:*" | top limit=10 useragent
```

✓ 439,456 events (01/01/2024 00:00:00.000 to 15/08/2024 03:20:44.000)

useragent	count	percent
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)	33476	21.170191
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5	14780	9.346858
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; .NET CLR 1.1.4322; InfoPath.1; MS-RTC LM 8)	13816	8.737226
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	12876	8.142770
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; MS-RTC LM 8; InfoPath.2)	11876	7.510371
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)	11440	7.234645
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_6_8) AppleWebKit/534.55.3 (KHTML, like Gecko) Version/5.1.5 Safari/534.55.3	7276	4.601336
Mozilla/5.0 (iPad; U; CPU OS 4_3_5 like Mac OS X; en-us) AppleWebKit/533.17.9 (KHTML, like Gecko) Version/5.0.2 Mobile/8L1 Safari/6533.18.5	6856	4.335728
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.52 Safari/536.5	6492	4.105535
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	6408	4.052413

Scenario 8 Visualized as a Pie Chart:


splunk>enterprise
Apps ▾
miguel ▾
Messages ▾
Settings ▾
Activity ▾
Help ▾
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As ▾
Create Table View
Close
Year to date ▾
No Event Sampling ▾
Job ▾
Smart Mode ▾
Events
Patterns
Statistics (10)
Visualization
Pie Chart
Format
Trellis
Mozilla/5.0 (iPad; CPU OS 5_1_1 like Mac OS X) AppleWebKit/5...KHTML, like Gecko) Version/5.1 Mobile/9B206 Safari/7534.48.3
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.52 Safari/536.5
Mozilla/5.0 (iPad; U; CPU OS 4_3_5 like Mac OS X; en-us) Appl... (KHTML, like Gecko) Version/5.0.2 Mobile/8L1 Safari/6533.18.5
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_6_8) AppleWebKit/534.55.3 (KHTML, like Gecko) Version/5.1.5 Safari/534.55.3
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; MS-RTC LM 8; InfoPath.2)
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
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) G...0120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; .NET CLR 1.1.4322; InfoPath.1; MS-RTC LM 8)

```
source="tutorialdata*.zip:*" | top limit=10 useragent
```

✓ 439,456 events (01/01/2024 00:00:00.000 to 15/08/2024 03:20:44.000)

useragent	count	percent
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)	33476	21.170191
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5	14780	9.346858
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; .NET CLR 1.1.4322; InfoPath.1; MS-RTC LM 8)	13816	8.737226
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	12876	8.142770
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; MS-RTC LM 8; InfoPath.2)	11876	7.510371
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)	11440	7.234645
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_6_8) AppleWebKit/534.55.3 (KHTML, like Gecko) Version/5.1.5 Safari/534.55.3	7276	4.601336
Mozilla/5.0 (iPad; U; CPU OS 4_3_5 like Mac OS X; en-us) AppleWebKit/533.17.9 (KHTML, like Gecko) Version/5.0.2 Mobile/8L1 Safari/6533.18.5	6856	4.335728
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.52 Safari/536.5	6492	4.105535
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	6408	4.052413

Scenario 9: Unsuccessful SSH Attempts by IP

Title: Failed SSH Attempts by IP

Description: Identify the IP addresses with the most failed SSH login attempts from the secure logs.

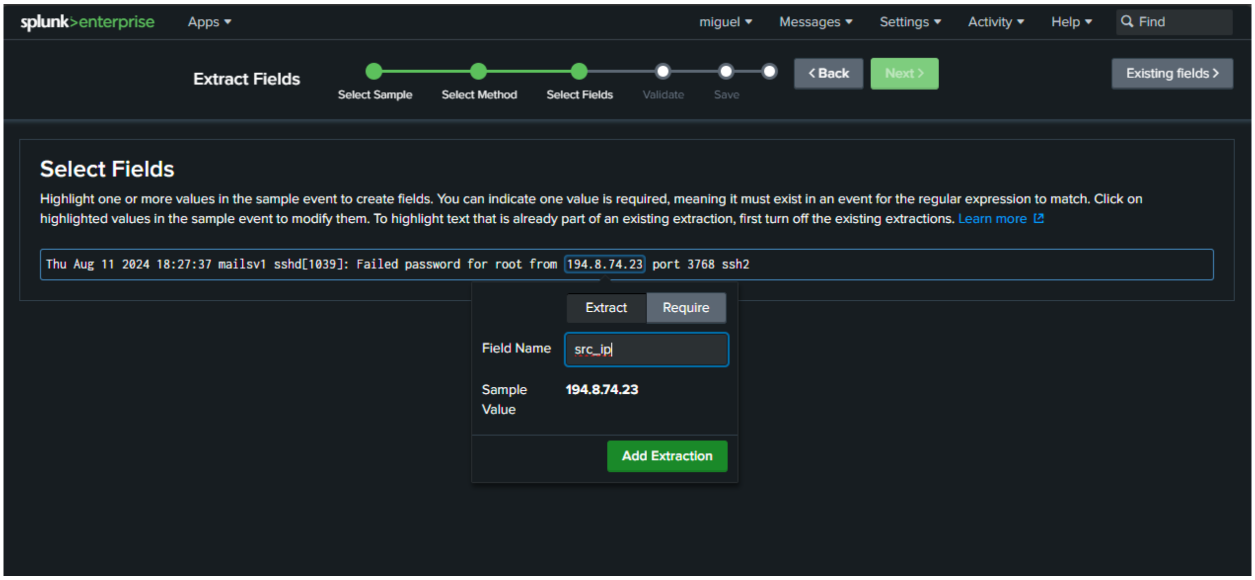
Steps to Create Search and Panel:

- Go to the Search & Reporting app in Splunk.
- Enter the query to find the IP addresses with the most failed attempts.
- Create a bar chart for the results.

Search Query:

source="tutorialdata*.zip:*" "Failed password" | top limit=10 src_ip

For this scenario we had to extract the src_ip field using Splunks "Extract Fields" wizard. Once extracted, we can now proceed with statistic and visualization.



Select Fields

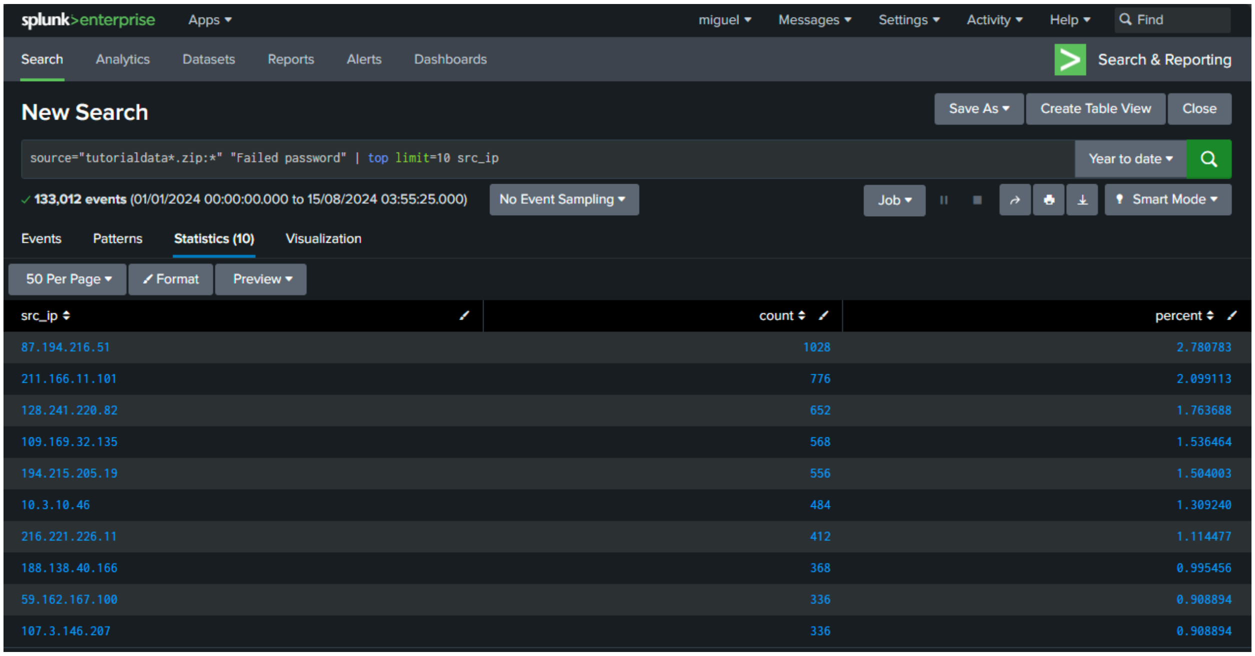
Highlight one or more values in the sample event to create fields. You can indicate one value is required, meaning it must exist in an event for the regular expression to match. Click on highlighted values in the sample event to modify them. To highlight text that is already part of an existing extraction, first turn off the existing extractions. Learn more

```
Thu Aug 11 2024 18:27:37 mailsv1 sshd[1039]: Failed password for root from 194.8.74.23 port 3768 ssh2
```

Field Name: src_ip

Sample Value: 194.8.74.23

Scenario 9 search results:

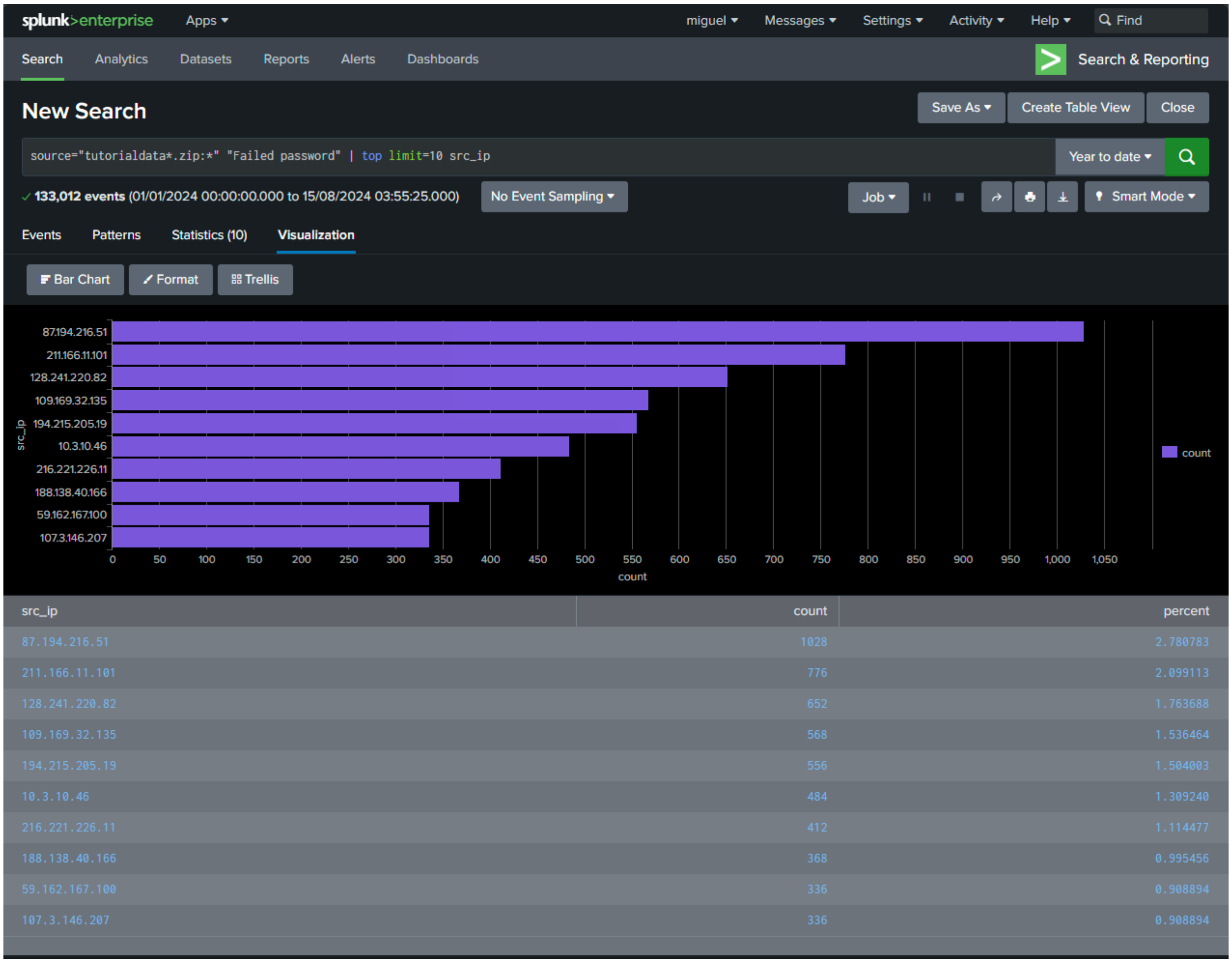


```
source="tutorialdata*.zip:*" "Failed password" | top limit=10 src_ip
```

✓ **133,012 events** (01/01/2024 00:00:00.000 to 15/08/2024 03:55:25.000)

src_ip	count	percent
87.194.216.51	1028	2.780783
211.166.11.101	776	2.099113
128.241.220.82	652	1.763688
109.169.32.135	568	1.536464
194.215.205.19	556	1.504003
10.3.10.46	484	1.309240
216.221.226.11	412	1.114477
188.138.40.166	368	0.995456
59.162.167.100	336	0.908894
107.3.146.207	336	0.908894

Scenario 9 Visualized as a Bar Chart:



New Search

```
source="tutorialdata*.zip:*" "Failed password" | top limit=10 src_ip
```

✓ 133,012 events (01/01/2024 00:00:00.000 to 15/08/2024 03:55:25.000)

src_ip	count	percent
87.194.216.51	1028	2.780783
211.166.11.101	776	2.099113
128.241.220.82	652	1.763688
109.169.32.135	568	1.536464
194.215.205.19	556	1.504003
10.3.10.46	484	1.309240
216.221.226.11	412	1.114477
188.138.40.166	368	0.995456
59.162.167.100	336	0.908894
107.3.146.207	336	0.908894

Scenario 10: Peak Traffic Times

Title: Identifying Peak Traffic Times

Description: Determine peak traffic times on the website from the access logs.

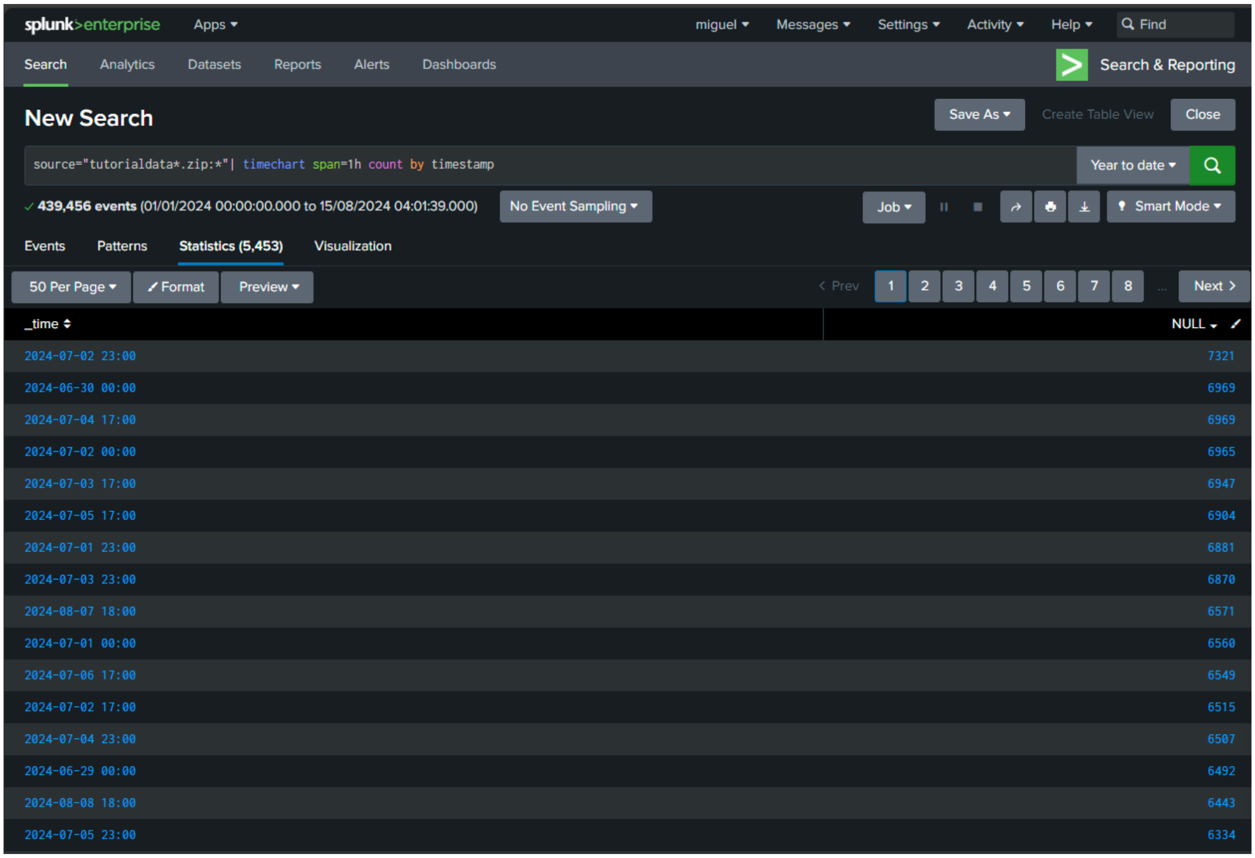
Steps to Create Search and Panel:

- Open the Search & Reporting app in Splunk.
- Enter the query to count website hits over time.
- Create a time chart for the results.

Search Query:

source="tutorialdata*.zip:*" | timechart count by _time span=1h

Scenario 10 search results:



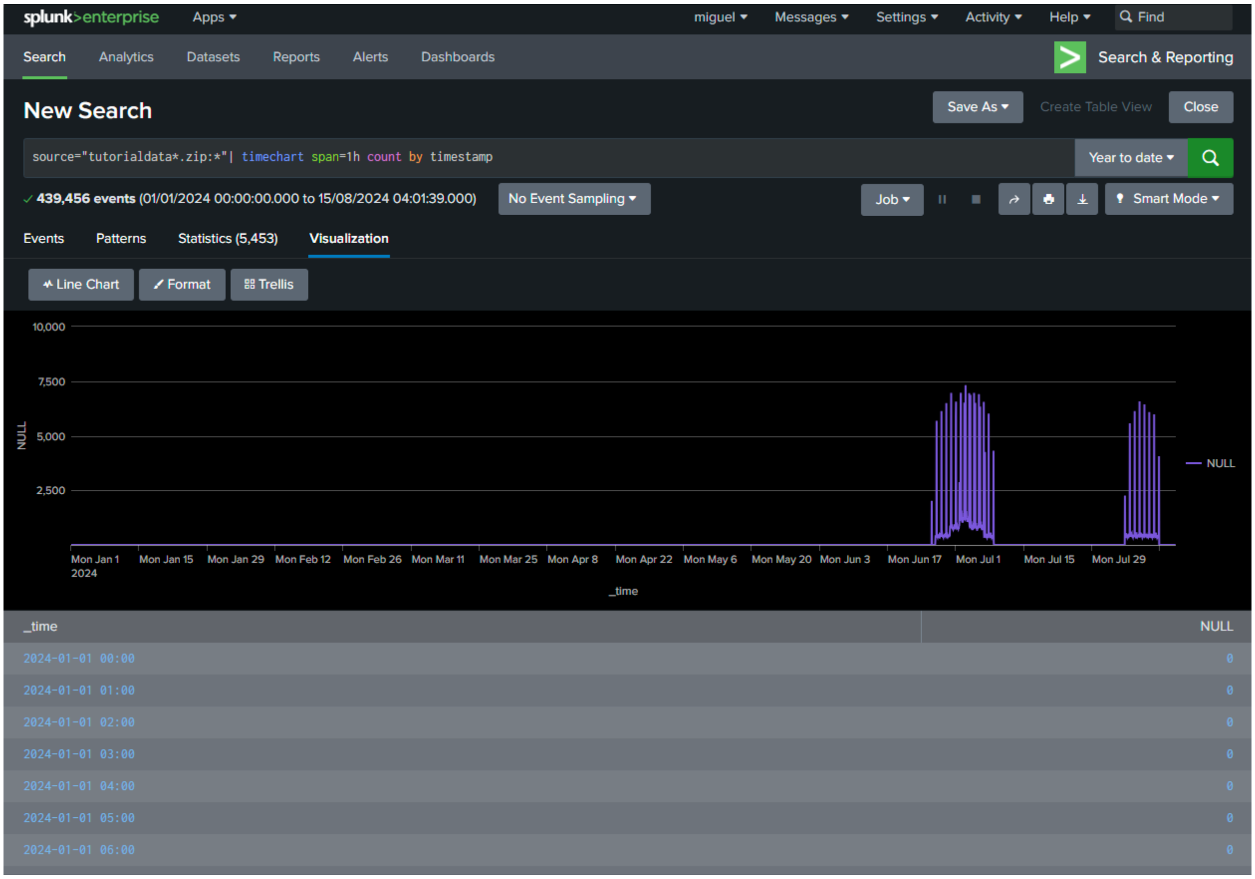
New Search

```
source="tutorialdata*.zip:*"| timechart span=1h count by timestamp
```

✓ **439,456 events** (01/01/2024 00:00:00.000 to 15/08/2024 04:01:39.000)

_time	NULL
2024-07-02 23:00	7321
2024-06-30 00:00	6969
2024-07-04 17:00	6969
2024-07-02 00:00	6965
2024-07-03 17:00	6947
2024-07-05 17:00	6904
2024-07-01 23:00	6881
2024-07-03 23:00	6870
2024-08-07 18:00	6571
2024-07-01 00:00	6560
2024-07-06 17:00	6549
2024-07-02 17:00	6515
2024-07-04 23:00	6507
2024-06-29 00:00	6492
2024-08-08 18:00	6443
2024-07-05 23:00	6334

Scenario 10 Visualized as a Time Chart:



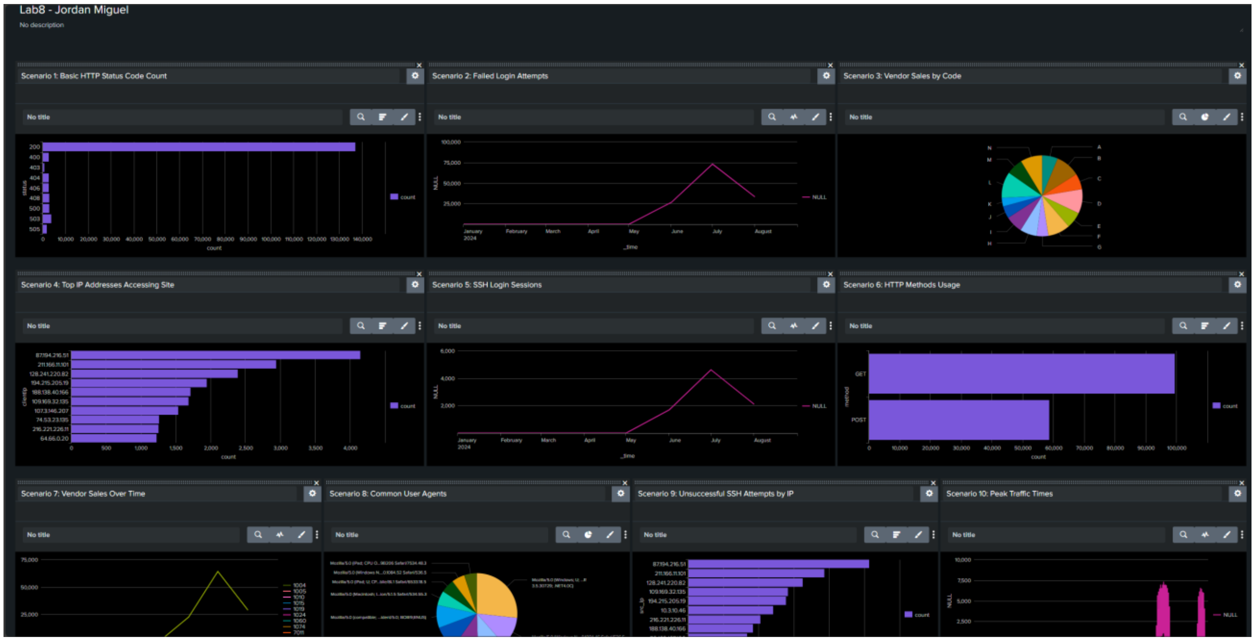
```
source="tutorialdata*.zip:*"| timechart span=1h count by timestamp
```

✓ **439,456 events** (01/01/2024 00:00:00.000 to 15/08/2024 04:01:39.000)

_time	NULL
2024-01-01 00:00	0
2024-01-01 01:00	0
2024-01-01 02:00	0
2024-01-01 03:00	0
2024-01-01 04:00	0
2024-01-01 05:00	0
2024-01-01 06:00	0

Final Task: Create Dashboard and Alerts

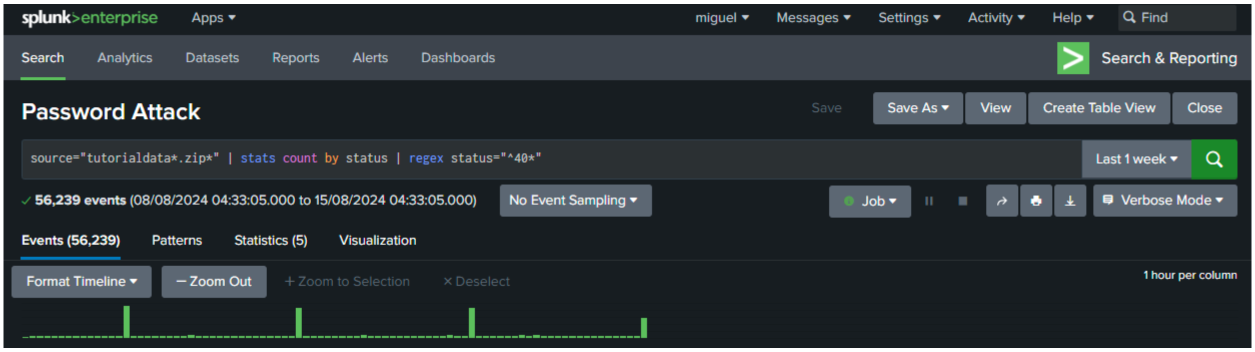
Add each of the above search scenarios as panels in a new Splunk dashboard


Lab8 - Jordan Miguel
No description
Scenario 1: Basic HTTP Status Code Count
Scenario 2: Failed Login Attempts
Scenario 3: Vendor Sales by Code
Scenario 4: Top IP Addresses Accessing Site
Scenario 5: SSH Login Sessions
Scenario 6: HTTP Methods Usage
Scenario 7: Vendor Sales Over Time
Scenario 8: Common User Agents
Scenario 9: Unsuccessful SSH Attempts by IP
Scenario 10: Peak Traffic Times
No title
count
NULL
_time
GET
POST

Set up alerts based on the aggregated data from each panel

Alert to the possibility of a Password/Dictionary Attack:

source="tutorialdata*.zip*" | stats count by status | regex status="^40*"



Password Attack

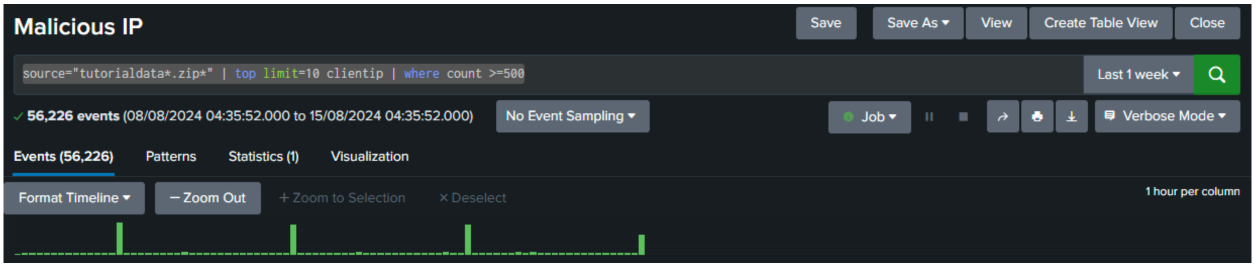
```
source="tutorialdata*.zip*" | stats count by status | regex status="^40*"
```

✓ 56,239 events (08/08/2024 04:33:05.000 to 15/08/2024 04:33:05.000)

Events (56,239)

Alert to potential malicious IP’s making over 500 connections:

source="tutorialdata*.zip*" | top limit=10 clientip | where count >=500

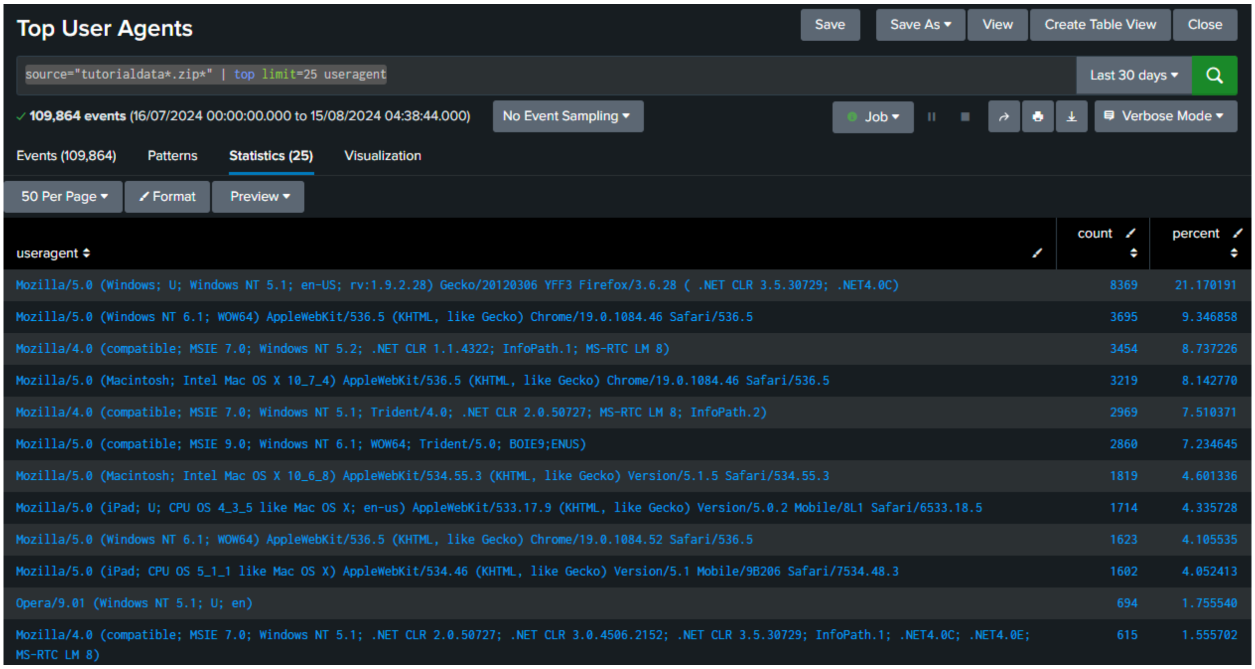


```
source="tutorialdata*.zip*" | top limit=10 clientip | where count >=500
```

✓ 56,226 events (08/08/2024 04:35:52.000 to 15/08/2024 04:35:52.000)

Monthly alert showing the top 25 user agents over the last 30 days:

source="tutorialdata*.zip*" | top limit=25 useragent

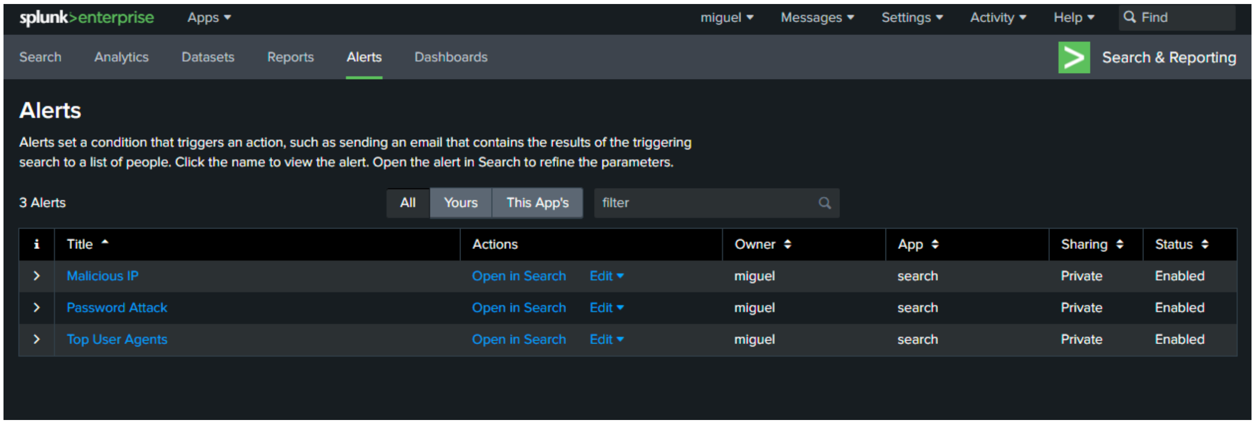


```
source="tutorialdata*.zip*" | top limit=25 useragent
```

✓ 109,864 events (16/07/2024 00:00:00.000 to 15/08/2024 04:38:44.000)

useragent	count	percent
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)	8369	21.170191
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5	3695	9.346858
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; .NET CLR 1.1.4322; InfoPath.1; MS-RTC LM 8)	3454	8.737226
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	3219	8.142770
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; MS-RTC LM 8; InfoPath.2)	2969	7.510371
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)	2860	7.234645
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_6_8) AppleWebKit/534.55.3 (KHTML, like Gecko) Version/5.1.5 Safari/534.55.3	1819	4.601336
Mozilla/5.0 (iPad; U; CPU OS 4_3_5 like Mac OS X; en-us) AppleWebKit/533.17.9 (KHTML, like Gecko) Version/5.0.2 Mobile/8L1 Safari/6533.18.5	1714	4.335728
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.52 Safari/536.5	1623	4.105535
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	1602	4.052413
Opera/9.01 (Windows NT 5.1; U; en)	694	1.755540
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; InfoPath.1; .NET4.0C; .NET4.0E; MS-RTC LM 8)	615	1.555702

View of all created Alerts:



Alerts

Alerts set a condition that triggers an action, such as sending an email that contains the results of the triggering search to a list of people. Click the name to view the alert. Open the alert in Search to refine the parameters.

3 Alerts

i	Title	Actions		Owner	App	Sharing	Status
>	Malicious IP	Open in Search	Edit	miguel	search	Private	Enabled
>	Password Attack	Open in Search	Edit	miguel	search	Private	Enabled
>	Top User Agents	Open in Search	Edit	miguel	search	Private	Enabled