Cybersecurity

Project 3 Review Questions

Make a copy of this document before you begin. Place your answers below each question.

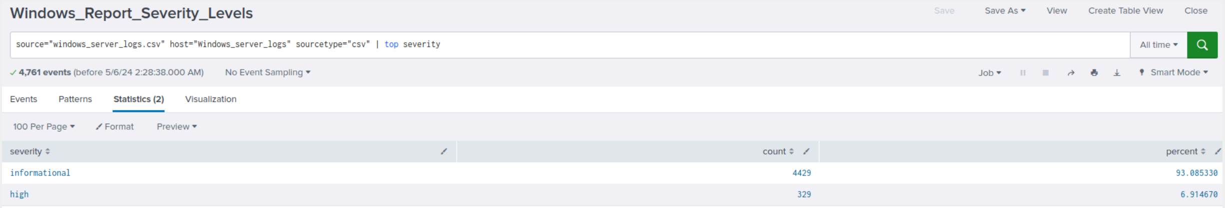
Windows Server Log Questions

Report Analysis for Severity

- Did you detect any suspicious changes in severity?

Severity Levels shoot up from count of 329 and in our simulation we see it jump to 1111.

Regular Report:



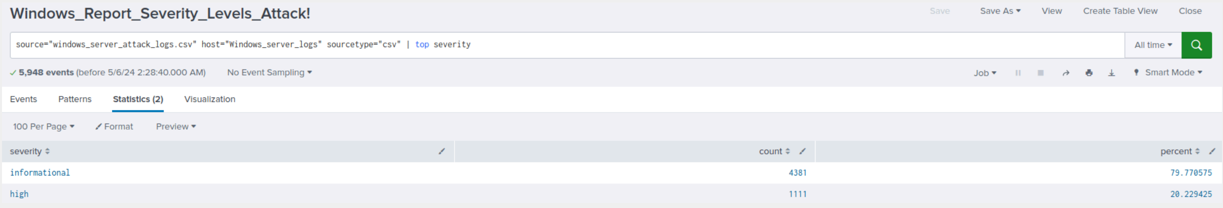
Windows_Report_Severity_Levels

```
source="windows_server_logs.csv" host="Windows_server_logs" sourcetype="csv" | top severity
```

✓ 4,761 events (before 5/6/24 2:28:38.000 AM)

severity	count	percent
informational	4429	93.085330
high	329	6.914670

Attack Report:



Windows_Report_Severity_Levels_Attack!

```
source="windows_server_attack_logs.csv" host="Windows_server_logs" sourcetype="csv" | top severity
```

✓ 5,948 events (before 5/6/24 2:28:40.000 AM)

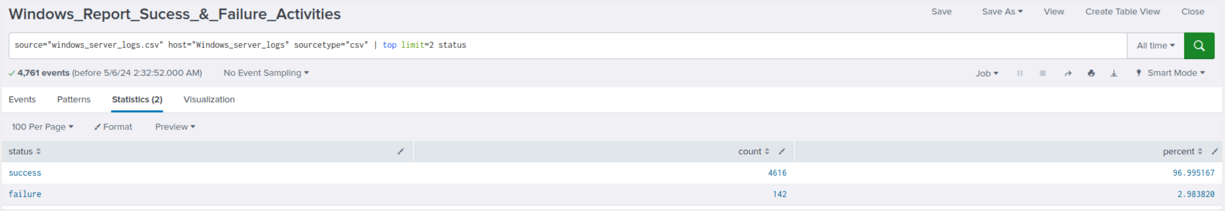
severity	count	percent
informational	4381	79.770575
high	1111	20.229425

Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

Failed Activities only have a 1% difference, no suspicious activity shown.

Regular Report:



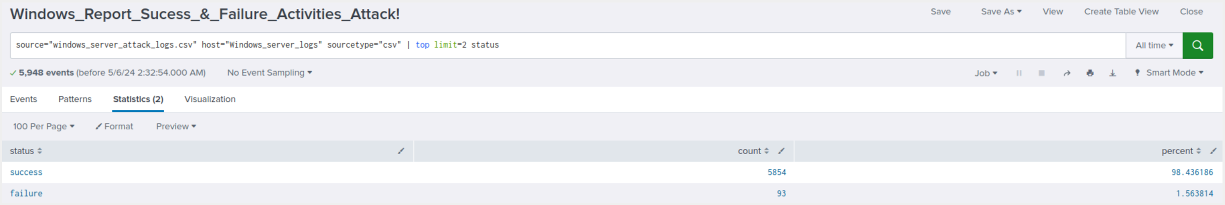
Windows_Report_Sucess_&_Failure_Activities

```
source="windows_server_logs.csv" host="Windows_server_logs" sourcetype="csv" | top limit=2 status
```

✓ **4,761 events** (before 5/6/24 2:32:52.000 AM) No Event Sampling ▾

status	count	percent
success	4616	96.995167
failure	142	2.983820

Attack Report:



Windows_Report_Sucess_&_Failure_Activities_Attack!

```
source="windows_server_attack_logs.csv" host="Windows_server_logs" sourcetype="csv" | top limit=2 status
```

✓ **5,948 events** (before 5/6/24 2:32:54.000 AM) No Event Sampling ▾

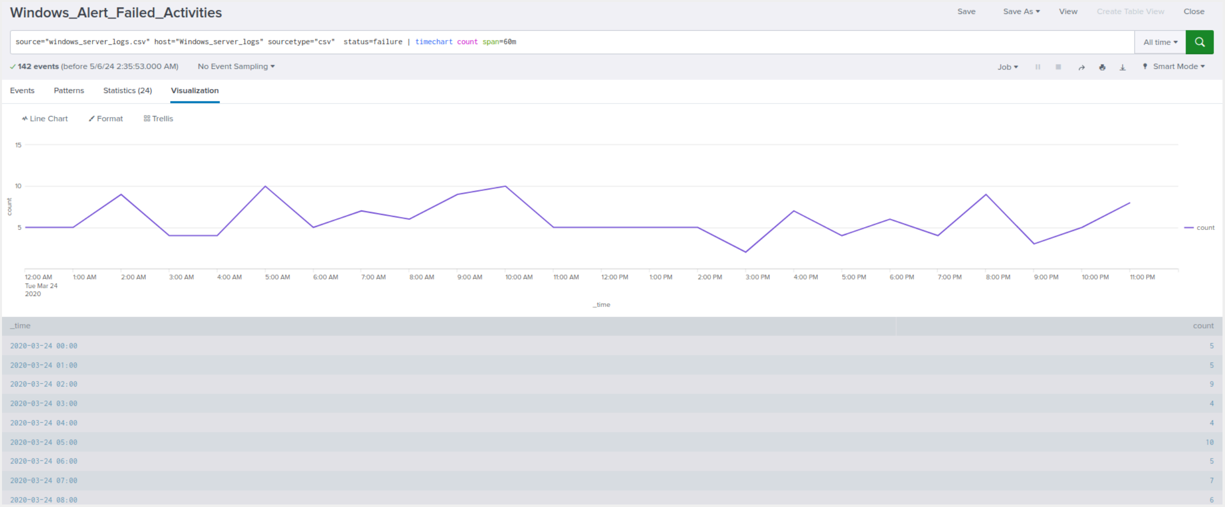
status	count	percent
success	5854	98.436186
failure	93	1.563814

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

We see in our Attack Alert a sudden peek.

Regular Alert:



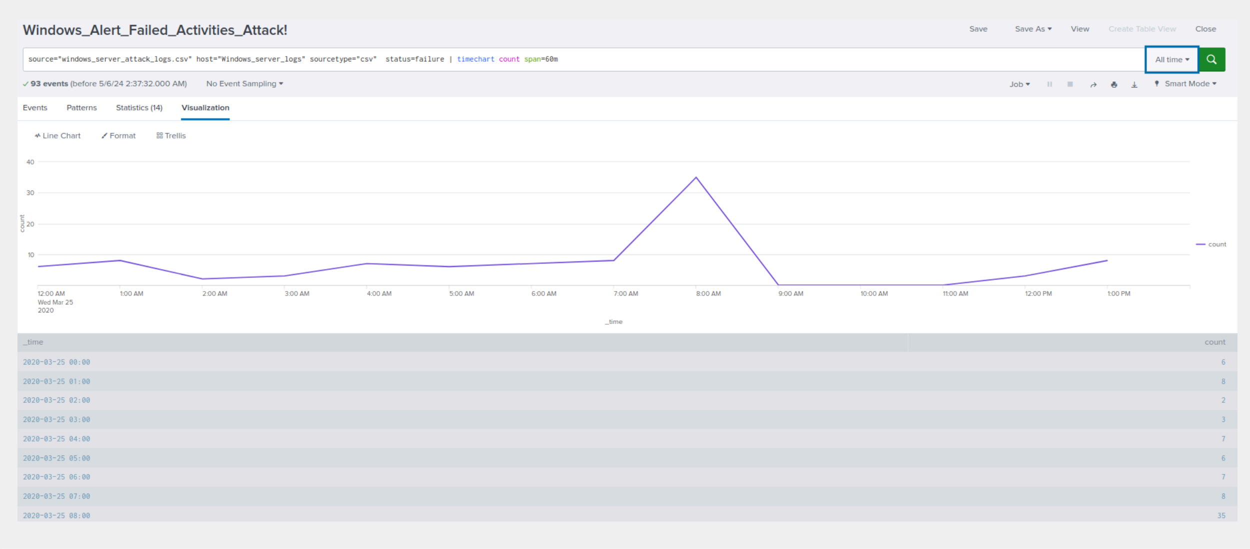
Windows_Alert_Failed_Activities

```
source="windows_server_logs.csv" host="Windows_server_logs" sourcetype="csv"  status=failure | timechart count span=60m
```

✓ **142 events** (before 5/6/24 2:35:53.000 AM) No Event Sampling ▾

_time	count
2020-03-24 00:00	5
2020-03-24 01:00	5
2020-03-24 02:00	9
2020-03-24 03:00	4
2020-03-24 04:00	4
2020-03-24 05:00	10
2020-03-24 06:00	5
2020-03-24 07:00	7
2020-03-24 08:00	6

Attack Alert:



```
source="windows_server_attack_logs.csv" host="Windows_server_logs" sourcetype="csv"  status=failure | timechart count span=60m
```

✓ **93 events** (before 5/6/24 2:37:32.000 AM) No Event Sampling ▾

_time	count
2020-03-25 00:00	6
2020-03-25 01:00	8
2020-03-25 02:00	2
2020-03-25 03:00	3
2020-03-25 04:00	7
2020-03-25 05:00	6
2020-03-25 06:00	7
2020-03-25 07:00	8
2020-03-25 08:00	35

- If so, what was the count of events in the hour(s) it occurred?

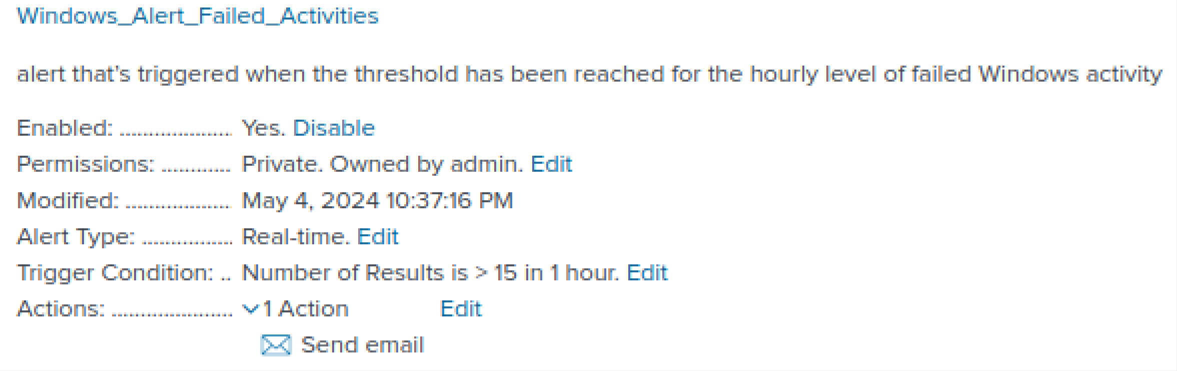
The Count of events indicates 35 at 8:00AM

- When did it occur?

The Date of the spike occurred on March 20, 2020

- Would your alert be triggered for this activity?

The current threshold is > 15 in 1 hour therefore the alert would activate when the threshold has been reached.



Windows_Alert_Failed_Activities

alert that's triggered when the threshold has been reached for the hourly level of failed Windows activity

Enabled: .... Yes. Disable
Permissions: .... Private. Owned by admin. Edit
Modified: .... May 4, 2024 10:37:16 PM
Alert Type: .... Real-time. Edit
Trigger Condition: .. Number of Results is > 15 in 1 hour. Edit
Actions: .... ⌄1 Action Edit
✉ Send email

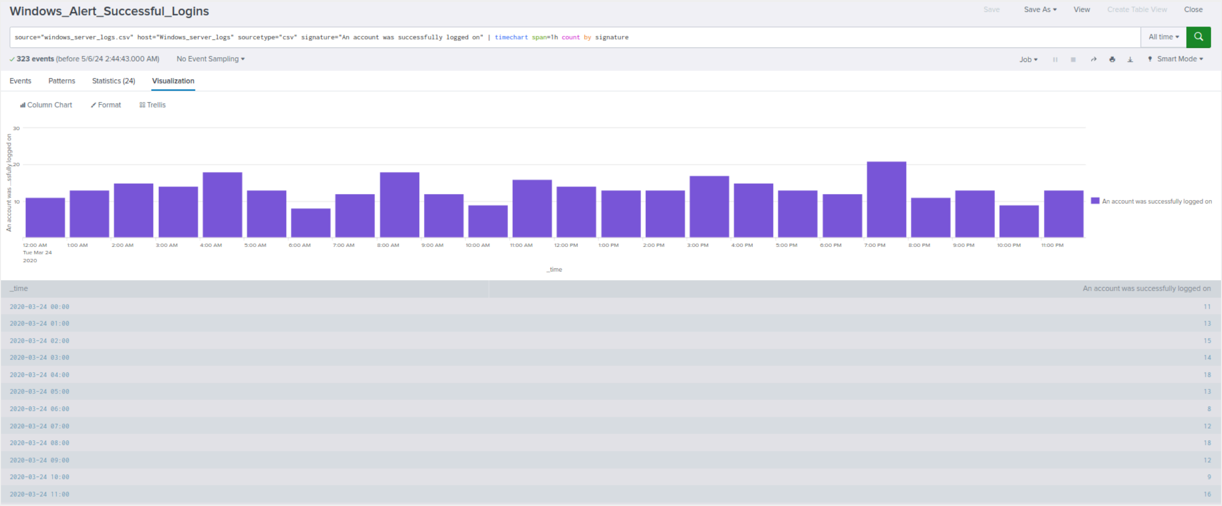
- After reviewing, would you change your threshold from what you previously selected?

```
After reviewing the events I would not make any changes.
```

Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

```
Our current charts indicate that during the attack many users were not
successful and we see a volume decrease.

Regular Report:
```



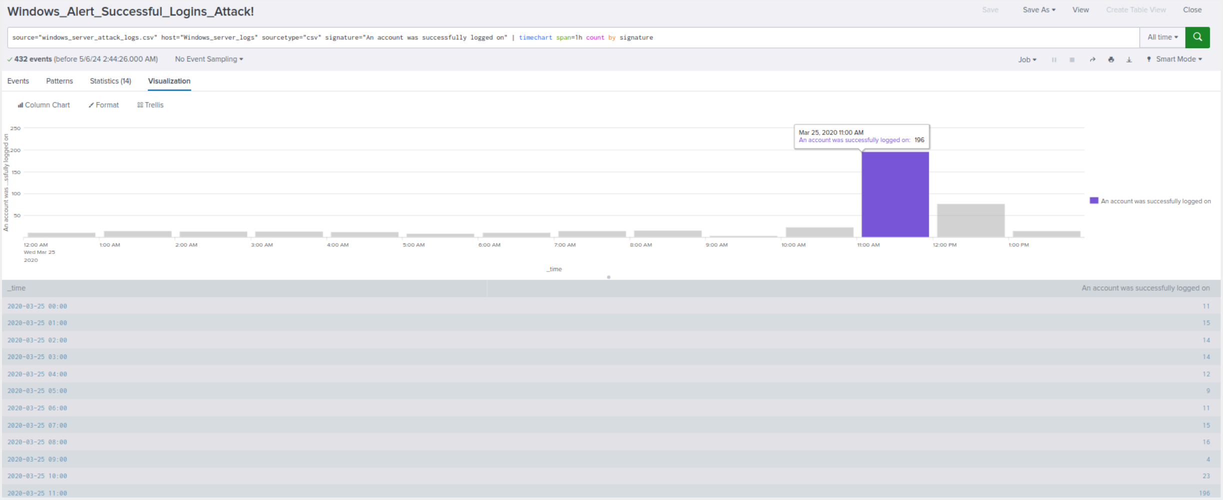
Windows_Alert_Successful_Logins

```
source="windows_server_logs.csv" host="Windows_server_logs" sourcetype="csv" signature="An account was successfully logged on" | timechart span=1h count by signature
```

✓ **323 events** (before 5/6/24 2:44:43.000 AM) No Event Sampling ▾

_time	An account was successfully logged on
2020-03-24 00:00	11
2020-03-24 01:00	13
2020-03-24 02:00	15
2020-03-24 03:00	14
2020-03-24 04:00	18
2020-03-24 05:00	13
2020-03-24 06:00	8
2020-03-24 07:00	12
2020-03-24 08:00	18
2020-03-24 09:00	12
2020-03-24 10:00	9
2020-03-24 11:00	16

```
Attack Report:
```



Windows_Alert_Successful_Logins_Attack!

```
source="windows_server_attack_logs.csv" host="Windows_server_logs" sourcetype="csv" signature="An account was successfully logged on" | timechart span=1h count by signature
```

✓ **432 events** (before 5/6/24 2:44:26.000 AM) No Event Sampling ▾

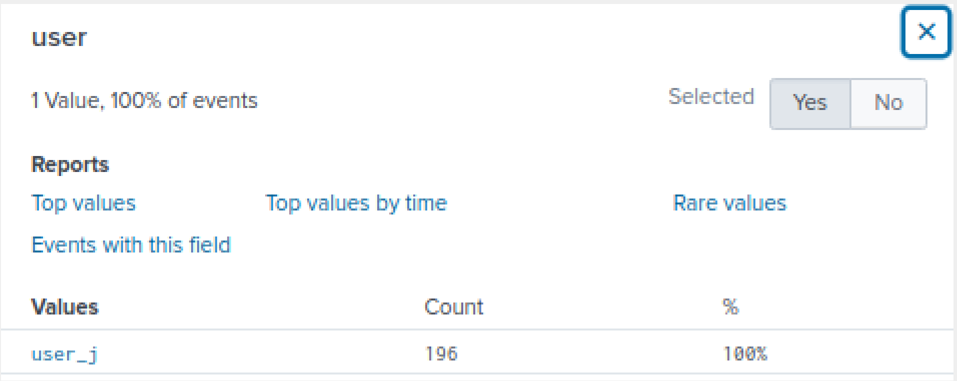
_time	An account was successfully logged on
2020-03-25 00:00	11
2020-03-25 01:00	15
2020-03-25 02:00	14
2020-03-25 03:00	14
2020-03-25 04:00	12
2020-03-25 05:00	9
2020-03-25 06:00	11
2020-03-25 07:00	15
2020-03-25 08:00	16
2020-03-25 09:00	4
2020-03-25 10:00	23
2020-03-25 11:00	196

- If so, what was the count of events in the hour(s) it occurred?

```
The count of events are shown to be 196 at 11:00AM
```

- Who is the primary user logging in?

```
Searching for the user through our alert we can confirm that the primary
login user is: user_j
```



user

1 Value, 100% of events

Reports

Top values · Top values by time · Rare values · Events with this field

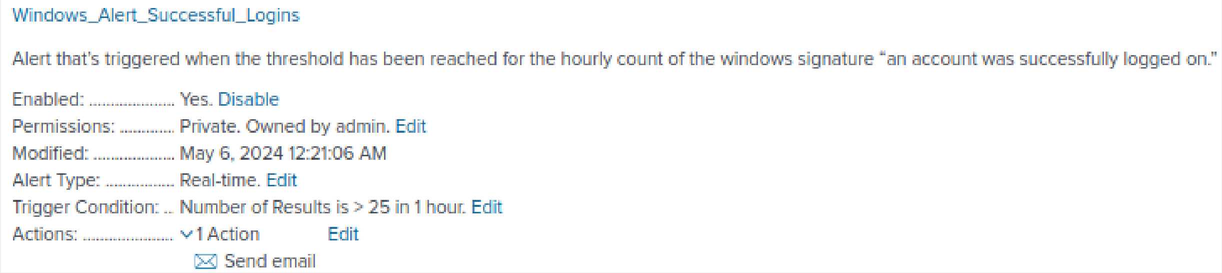
Values	Count	%
user_j	196	100%

- When did it occur?

```
The event occurred on March 25, 2020
```

- Would your alert be triggered for this activity?

```
The current threshold is > 25 in 1 hour, in conclusion the alert would have
been triggered.
```



Windows_Alert_Successful_Logins

Alert that's triggered when the threshold has been reached for the hourly count of the windows signature "an account was successfully logged on."

Enabled: .... Yes. Disable
Permissions: .... Private. Owned by admin. Edit
Modified: .... May 6, 2024 12:21:06 AM
Alert Type: .... Real-time. Edit
Trigger Condition: .. Number of Results is > 25 in 1 hour. Edit
Actions: .... 1 Action Edit
Send email

- After reviewing, would you change your threshold from what you previously selected?

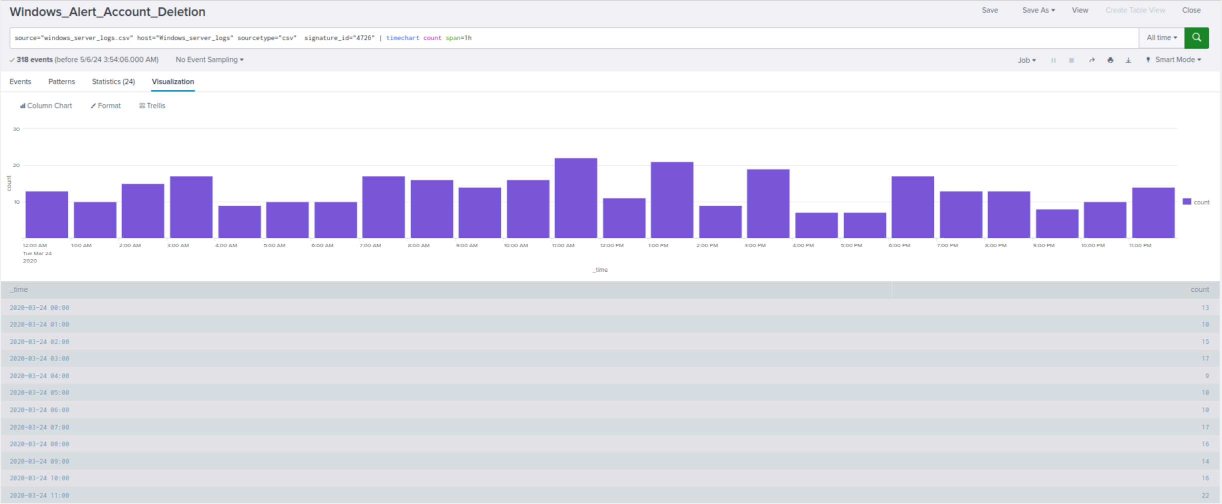
```
The results of the alert were successful therefore no changes are necessary.
```

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

Our alerts indicate there has been no activity on March 25, 2020 between the times of 10:00AM - 11:00AM at the moment no suspicious activity.

Regular Alert:



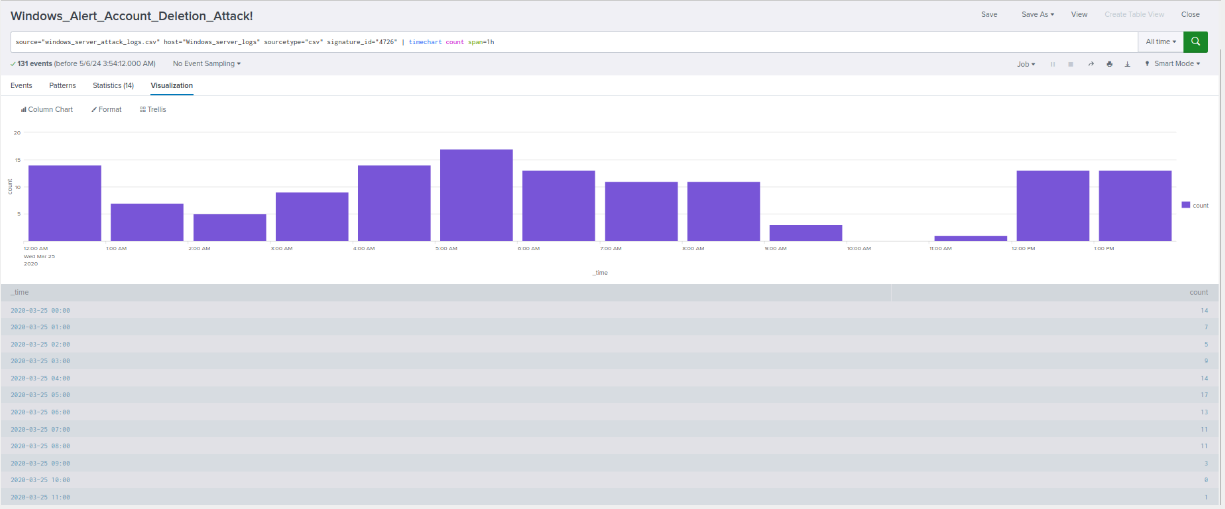
Windows_Alert_Account_Deletion

```
source="windows_server_logs.csv" host="Windows_server_logs" sourcetype="csv"  signature_id="4726" | timechart count span=1h
```

✓ **318 events** (before 5/6/24 3:54:06.000 AM) No Event Sampling ▾

_time	count
2020-03-24 00:00	13
2020-03-24 01:00	10
2020-03-24 02:00	15
2020-03-24 03:00	17
2020-03-24 04:00	9
2020-03-24 05:00	10
2020-03-24 06:00	10
2020-03-24 07:00	17
2020-03-24 08:00	16
2020-03-24 09:00	14
2020-03-24 10:00	16
2020-03-24 11:00	22

Attack Alert:



Windows_Alert_Account_Deletion_Attack!

```
source="windows_server_attack_logs.csv" host="Windows_server_logs" sourcetype="csv" signature_id="4726" | timechart count span=1h
```

✓ **131 events** (before 5/6/24 3:54:12.000 AM) No Event Sampling ▾

_time	count
2020-03-25 00:00	14
2020-03-25 01:00	7
2020-03-25 02:00	5
2020-03-25 03:00	9
2020-03-25 04:00	14
2020-03-25 05:00	17
2020-03-25 06:00	13
2020-03-25 07:00	11
2020-03-25 08:00	11
2020-03-25 09:00	3
2020-03-25 10:00	0
2020-03-25 11:00	1

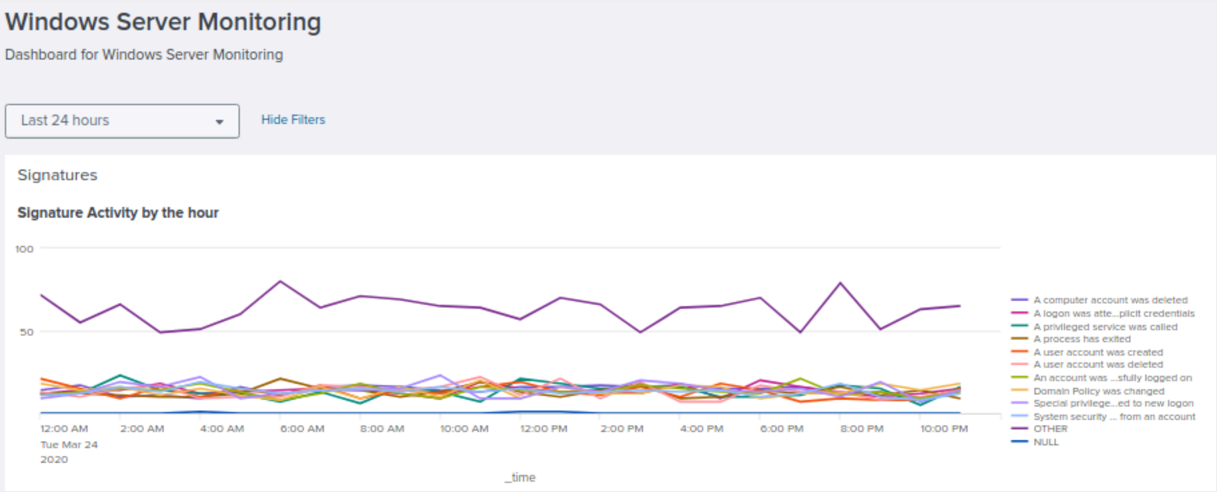
Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

Our Dashboards indicate a spike difference between 2 signatures.

Regular Dashboard:

```
source="windows_server_logs.csv" host="Windows_server_logs" sourcetype="csv" | timechart span=1h count by signature
```



Windows Server Monitoring

Dashboard for Windows Server Monitoring

Last 24 hours ▾ Hide Filters

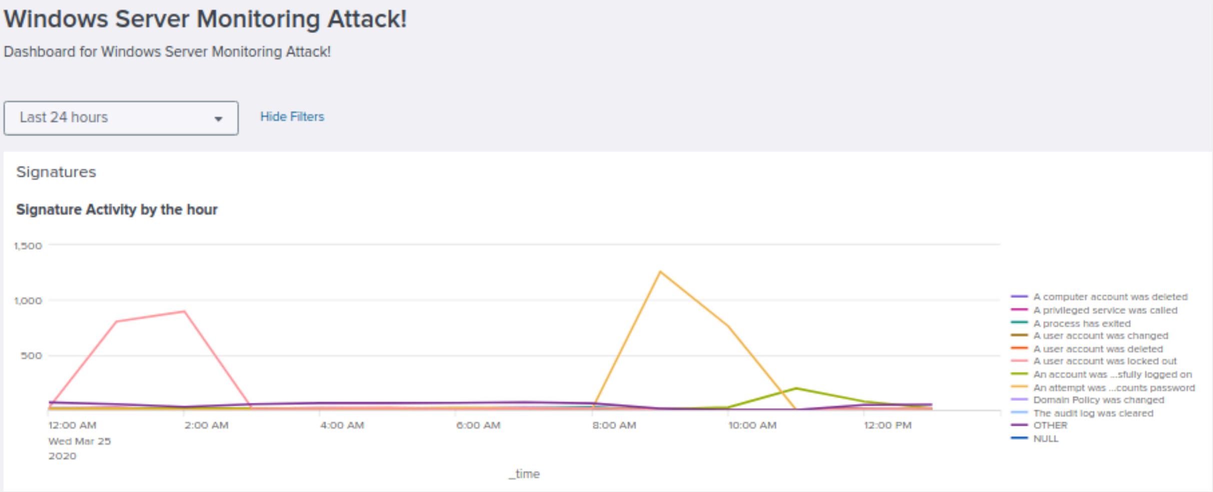
Signatures

Signature Activity by the hour

100
50
12:00 AM
Tue Mar 24
2020
2:00 AM
4:00 AM
6:00 AM
8:00 AM
10:00 AM
12:00 PM
2:00 PM
4:00 PM
6:00 PM
8:00 PM
10:00 PM
_time
A computer account was deleted
A logon was atte...plicit credentials
A privileged service was called
A process has exited
A user account was created
A user account was deleted
An account was ...sfully logged on
Domain Policy was changed
Special privilege...ed to new logon
System security ... from an account
OTHER
NULL

Attack Dashboard:

```
source="windows_server_attack_logs.csv" host="Windows_server_logs" sourcetype="csv" | timechart span=1h count by signature
```



Windows Server Monitoring Attack!

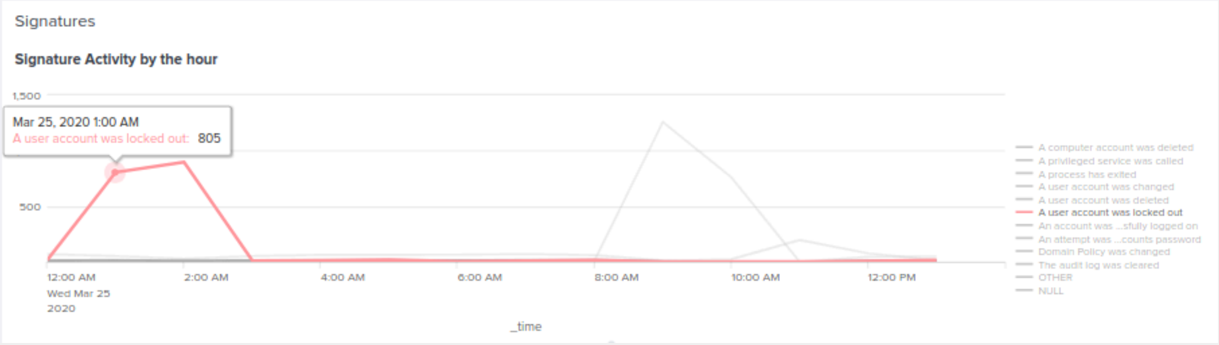
Dashboard for Windows Server Monitoring Attack!

Last 24 hours ▾ Hide Filters

Signatures

Signature Activity by the hour

1,500
1,000
500
12:00 AM
Wed Mar 25
2020
2:00 AM
4:00 AM
6:00 AM
8:00 AM
10:00 AM
12:00 PM
_time
A computer account was deleted
A privileged service was called
A process has exited
A user account was changed
A user account was deleted
A user account was locked out
An account was ...sfully logged on
An attempt was ...counts password
Domain Policy was changed
The audit log was cleared
OTHER
NULL



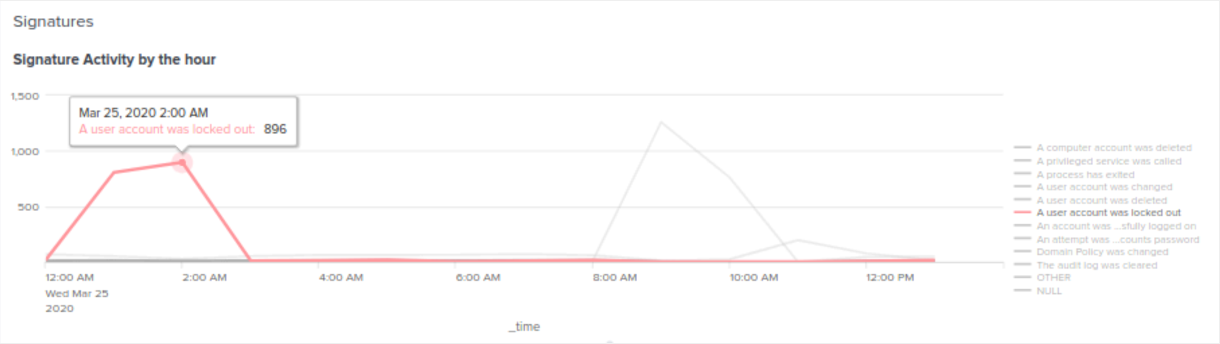
Signatures

Signature Activity by the hour

Mar 25, 2020 1:00 AM

A user account was locked out: 805

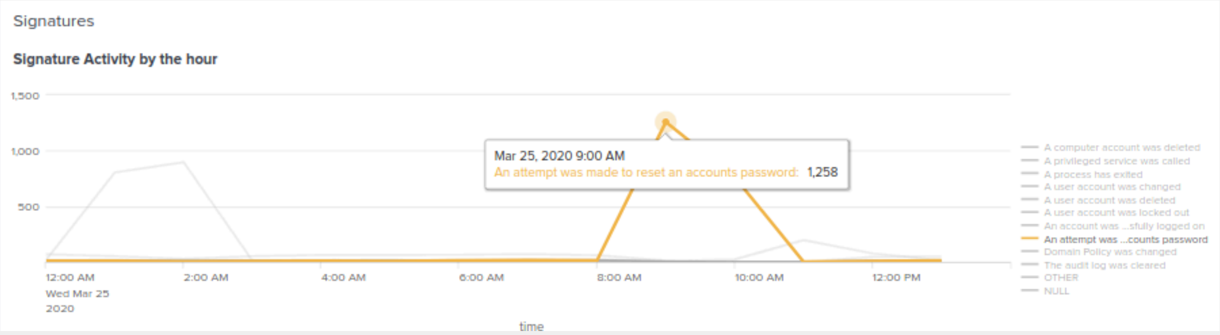
1,500
500
12:00 AM
Wed Mar 25
2020
2:00 AM
4:00 AM
6:00 AM
8:00 AM
10:00 AM
12:00 PM
_time
A computer account was deleted
A privileged service was called
A process has exited
A user account was changed
A user account was deleted
A user account was locked out
An account was ...sfully logged on
An attempt was ...counts password
Domain Policy was changed
The audit log was cleared
OTHER
NULL



Signatures

Signature Activity by the hour

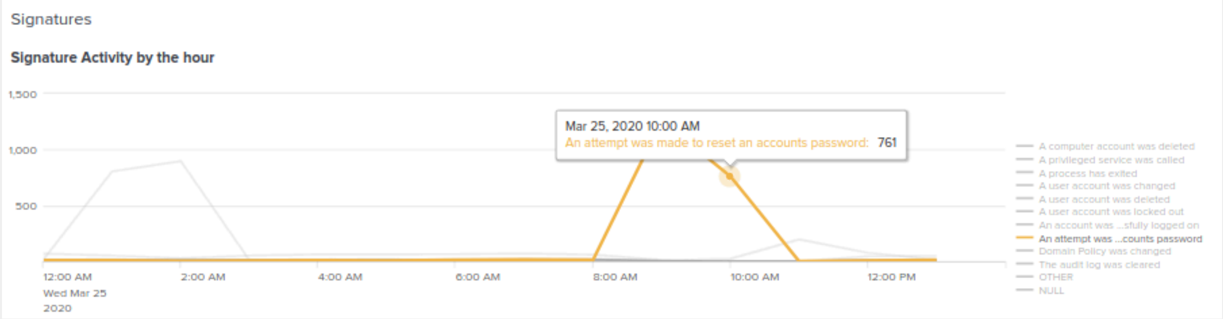
1,500
1,000
500
Mar 25, 2020 2:00 AM
A user account was locked out: 896
12:00 AM
Wed Mar 25
2020
2:00 AM
4:00 AM
6:00 AM
8:00 AM
10:00 AM
12:00 PM
_time
A computer account was deleted
A privileged service was called
A process has exited
A user account was changed
A user account was deleted
A user account was locked out
An account was ...sfully logged on
An attempt was ...counts password
Domain Policy was changed
The audit log was cleared
OTHER
NULL



Signatures

Signature Activity by the hour

1,500
1,000
500
Mar 25, 2020 9:00 AM
An attempt was made to reset an accounts password: 1,258
12:00 AM
Wed Mar 25
2020
2:00 AM
4:00 AM
6:00 AM
8:00 AM
10:00 AM
12:00 PM
time
A computer account was deleted
A privileged service was called
A process has exited
A user account was changed
A user account was deleted
A user account was locked out
An account was ...sfully logged on
An attempt was ...counts password
Domain Policy was changed
The audit log was cleared
OTHER
NULL



Signatures

Signature Activity by the hour

1,500
1,000
500
Mar 25, 2020 10:00 AM
An attempt was made to reset an accounts password: 761
12:00 AM
Wed Mar 25
2020
2:00 AM
4:00 AM
6:00 AM
8:00 AM
10:00 AM
12:00 PM
A computer account was deleted
A privileged service was called
A process has exited
A user account was changed
A user account was deleted
A user account was locked out
An account was ...sfully logged on
An attempt was ...counts password
Domain Policy was changed
The audit log was cleared
OTHER
NULL

- What signatures stand out?

```
The signatures that currently stand out are:
1. A user account was locked out
2. An attempt was made to reset an account password
```

- What time did it begin and stop for each signature?

```
The time it began and stopped were the following:
1) 1:00AM - 2:00AM    &    2) 9:00AM - 10:00AM
```

- What is the peak count of the different signatures?

The peak count of the different signatures were the following:
1) 896 & 2) 1258

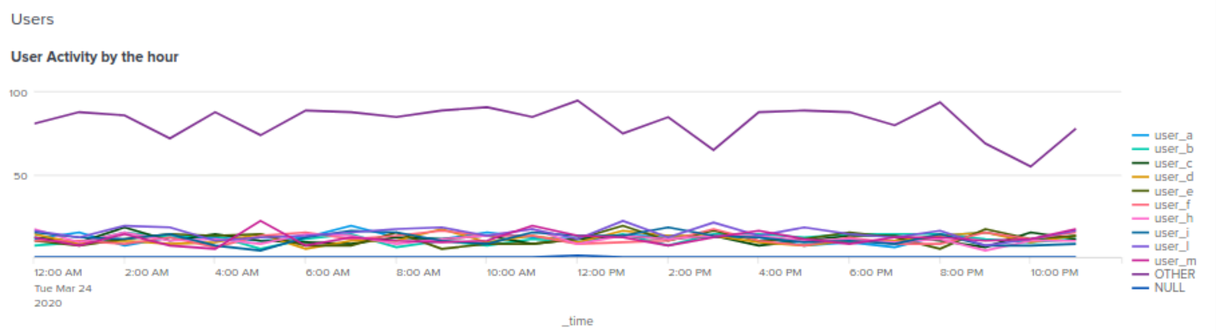
Dashboard Analysis for Users

- Does anything stand out as suspicious?

Our Dashboards indicate an activity irregularity between 2 users.

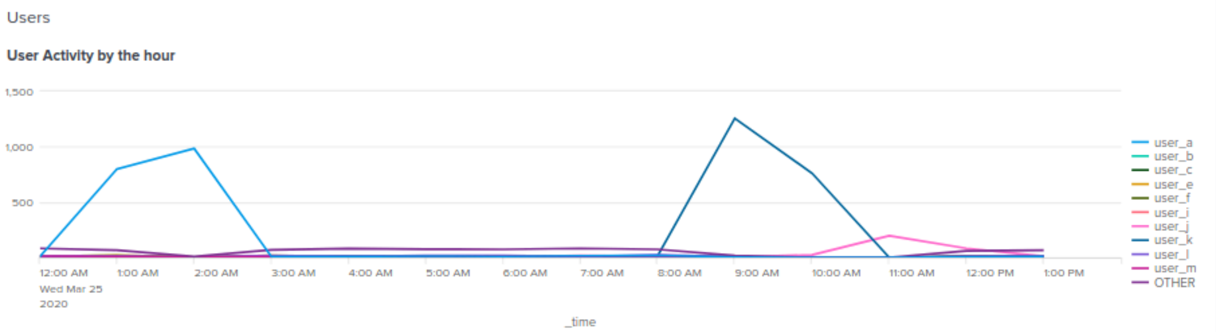
Regular Dashboard:

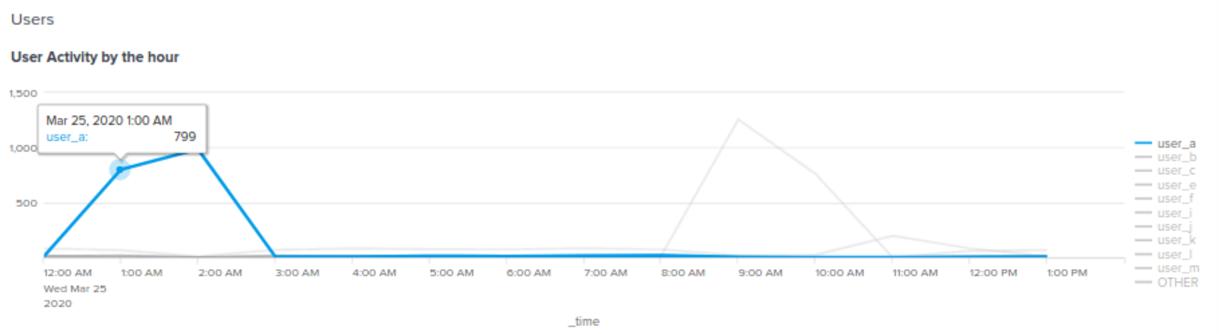
```
source="windows_server_logs.csv" host="Windows_server_logs" sourcetype="csv" | timechart span=1h count by user
```

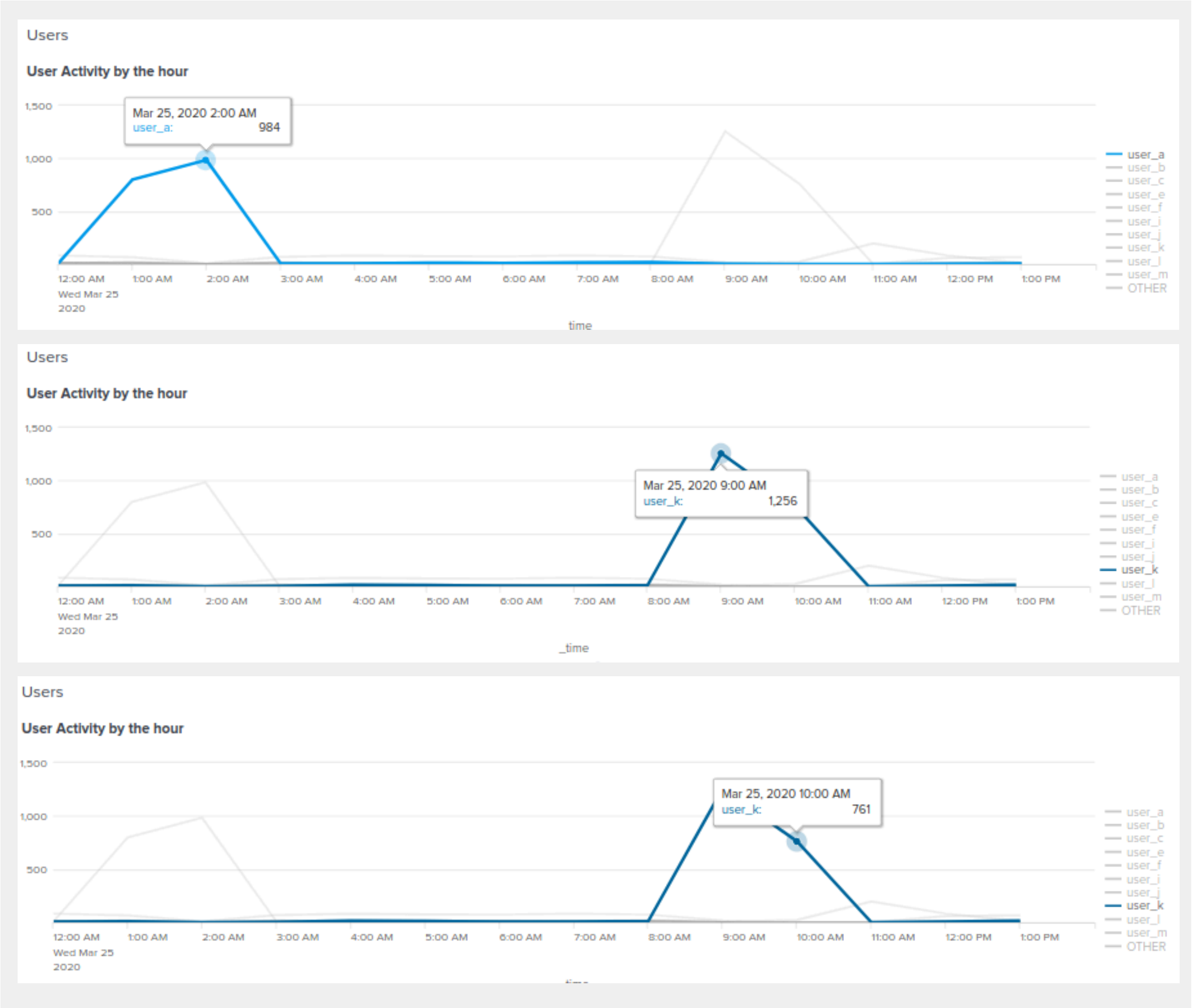


Attack Dashboard:

```
source="windows_server_attack_logs.csv" host="Windows_server_logs" sourcetype="csv" | timechart span=1h count by user
```







- Which users stand out?

```
The users that stand out were:
1) user_a
2) user_k
```

- What time did it begin and stop for each user?

```
The time it begins and stops for each user were:
1) 1:00AM - 2:00AM
2) 9:00AM - 10:00AM
```

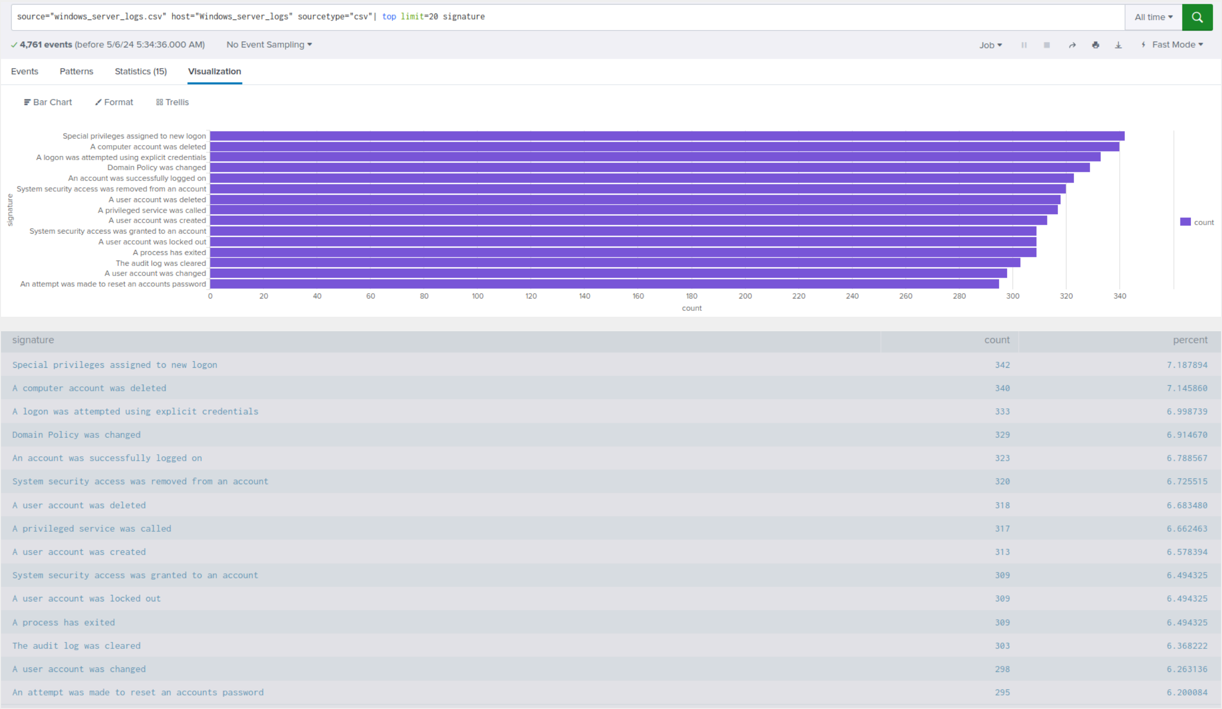
- What is the peak count of the different users?

```
The peak count shows:
1) 984
2) 1256
```

Dashboard Analysis for Signatures with Bar, Graph, and Pie Charts

- Does anything stand out as suspicious?

```
Our dashboard indicates we have a high volume for 2 signatures.

Regular Dashboard:
```

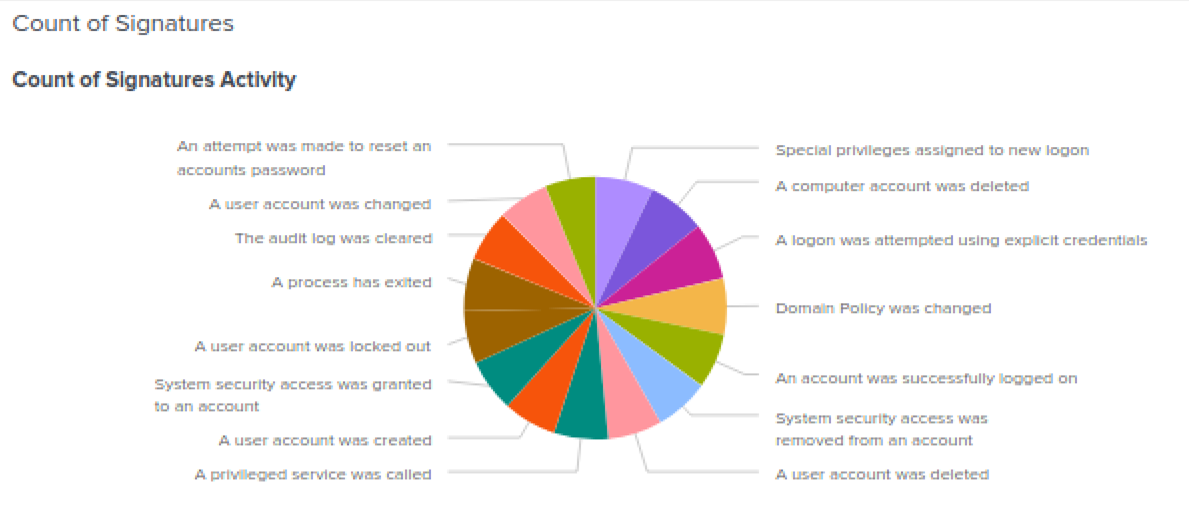


```
source="windows_server_logs.csv" host="Windows_server_logs" sourcetype="csv"| top limit=20 signature
```

✓ **4,761 events** (before 5/6/24 5:34:36.000 AM)

All time ▾
No Event Sampling ▾
Job ▾
Fast Mode ▾
Events
Patterns
Statistics (15)
Visualization
Bar Chart
Format
Trellis
signature
Special privileges assigned to new logon
A computer account was deleted
A logon was attempted using explicit credentials
Domain Policy was changed
An account was successfully logged on
System security access was removed from an account
A user account was deleted
A privileged service was called
A user account was created
System security access was granted to an account
A user account was locked out
A process has exited
The audit log was cleared
A user account was changed
An attempt was made to reset an accounts password
0
20
40
60
80
100
120
140
160
180
200
220
240
260
280
300
320
340
count
count

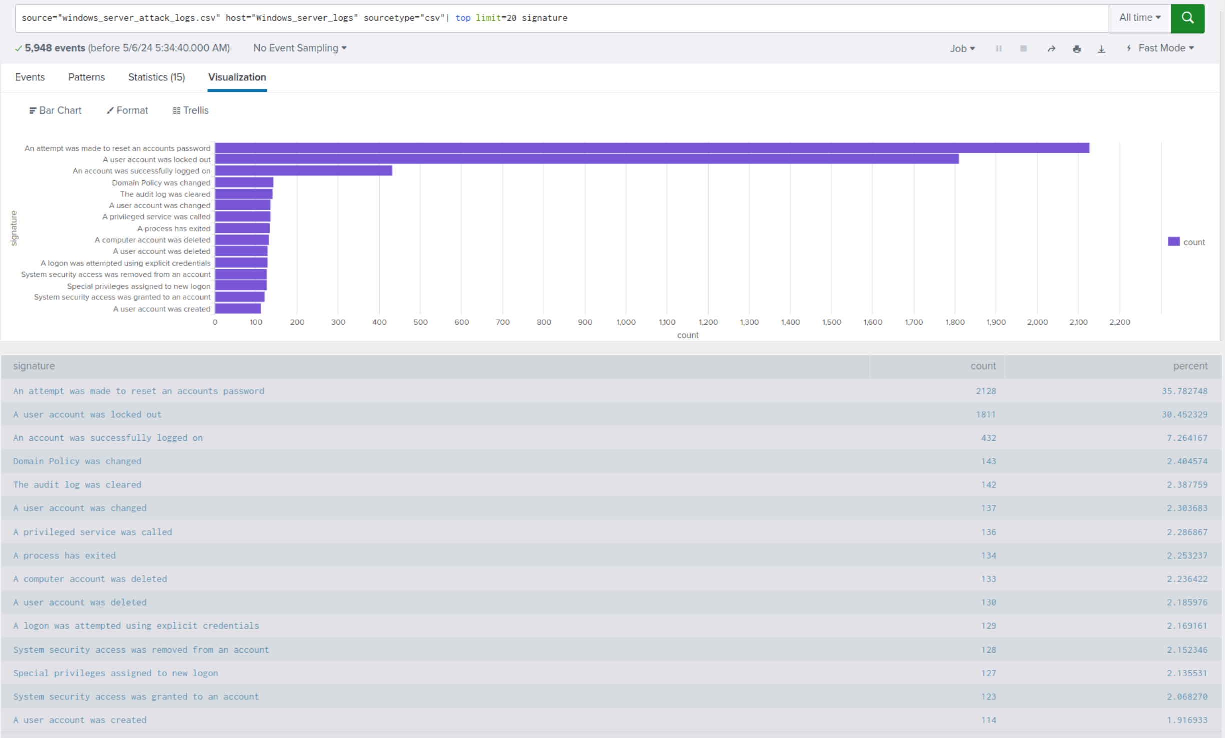
signature	count	percent
Special privileges assigned to new logon	342	7.187894
A computer account was deleted	340	7.145860
A logon was attempted using explicit credentials	333	6.998739
Domain Policy was changed	329	6.914670
An account was successfully logged on	323	6.788567
System security access was removed from an account	320	6.725515
A user account was deleted	318	6.683480
A privileged service was called	317	6.662463
A user account was created	313	6.578394
System security access was granted to an account	309	6.494325
A user account was locked out	309	6.494325
A process has exited	309	6.494325
The audit log was cleared	303	6.368222
A user account was changed	298	6.263136
An attempt was made to reset an accounts password	295	6.200084



Count of Signatures

Count of Signatures Activity

Attack Dashboard:

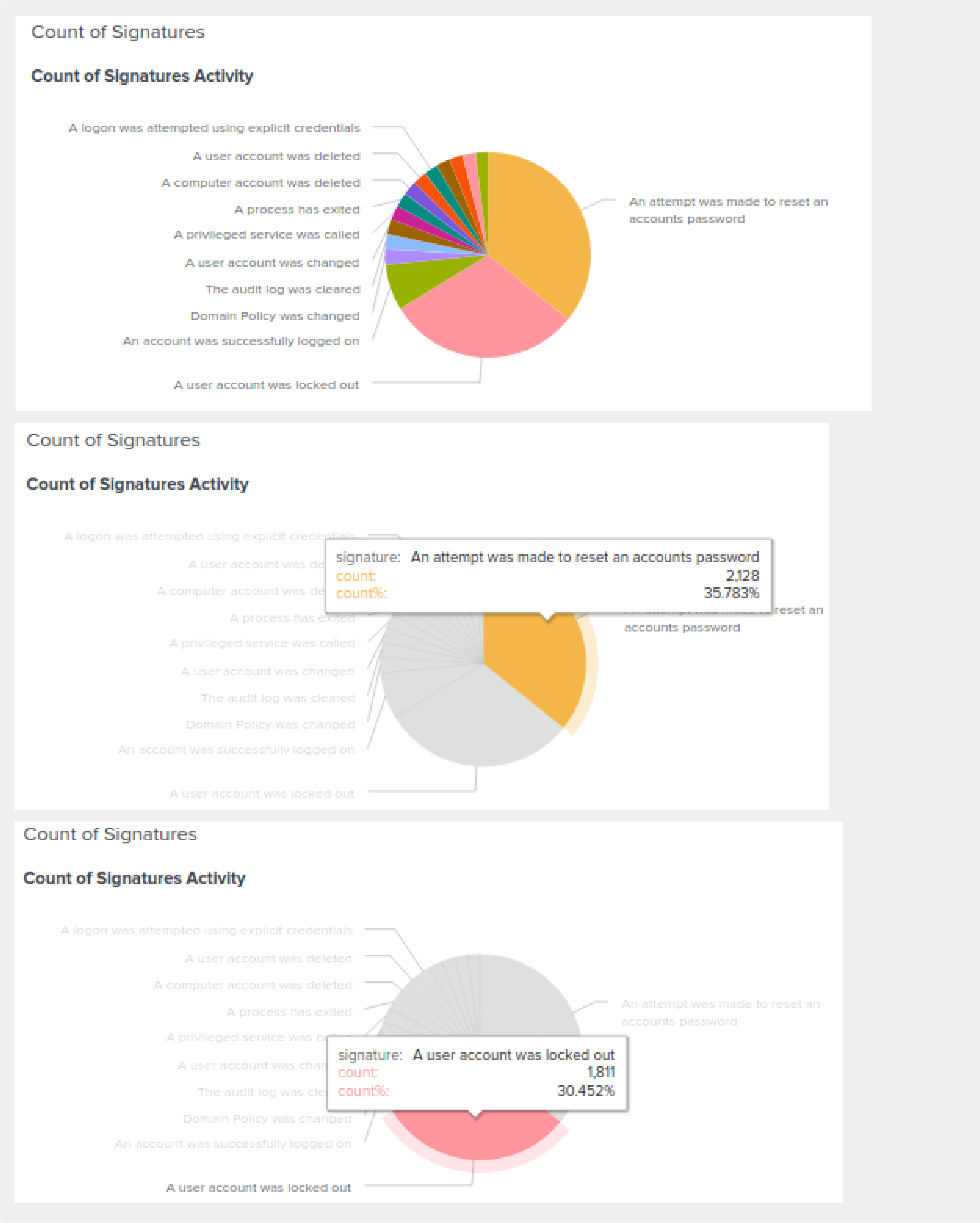


```
source="windows_server_attack_logs.csv" host="Windows_server_logs" sourcetype="csv"| top limit=20 signature
```

✓ **5,948 events** (before 5/6/24 5:34:40.000 AM)

All time ▾
No Event Sampling ▾
Job ▾
Fast Mode ▾
Events
Patterns
Statistics (15)
Visualization
Bar Chart
Format
Trellis
signature
An attempt was made to reset an accounts password
A user account was locked out
An account was successfully logged on
Domain Policy was changed
The audit log was cleared
A user account was changed
A privileged service was called
A process has exited
A computer account was deleted
A user account was deleted
A logon was attempted using explicit credentials
System security access was removed from an account
Special privileges assigned to new logon
System security access was granted to an account
A user account was created
0
100
200
300
400
500
600
700
800
900
1,000
1,100
1,200
1,300
1,400
1,500
1,600
1,700
1,800
1,900
2,000
2,100
2,200
count
count

signature	count	percent
An attempt was made to reset an accounts password	2128	35.782748
A user account was locked out	1811	30.452329
An account was successfully logged on	432	7.264167
Domain Policy was changed	143	2.404574
The audit log was cleared	142	2.387759
A user account was changed	137	2.303683
A privileged service was called	136	2.286867
A process has exited	134	2.253237
A computer account was deleted	133	2.236422
A user account was deleted	130	2.185976
A logon was attempted using explicit credentials	129	2.169161
System security access was removed from an account	128	2.152346
Special privileges assigned to new logon	127	2.135531
System security access was granted to an account	123	2.068270
A user account was created	114	1.916933



Count of Signatures

Count of Signatures Activity

A logon was attempted using explicit credentials
A user account was deleted
A computer account was deleted
A process has exited
A privileged service was called
A user account was changed
The audit log was cleared
Domain Policy was changed
An account was successfully logged on
A user account was locked out
An attempt was made to reset an accounts password

Count of Signatures

Count of Signatures Activity

signature: An attempt was made to reset an accounts password
count: 2,128
count%: 35.783%

Count of Signatures

Count of Signatures Activity

signature: A user account was locked out
count: 1,811
count%: 30.452%

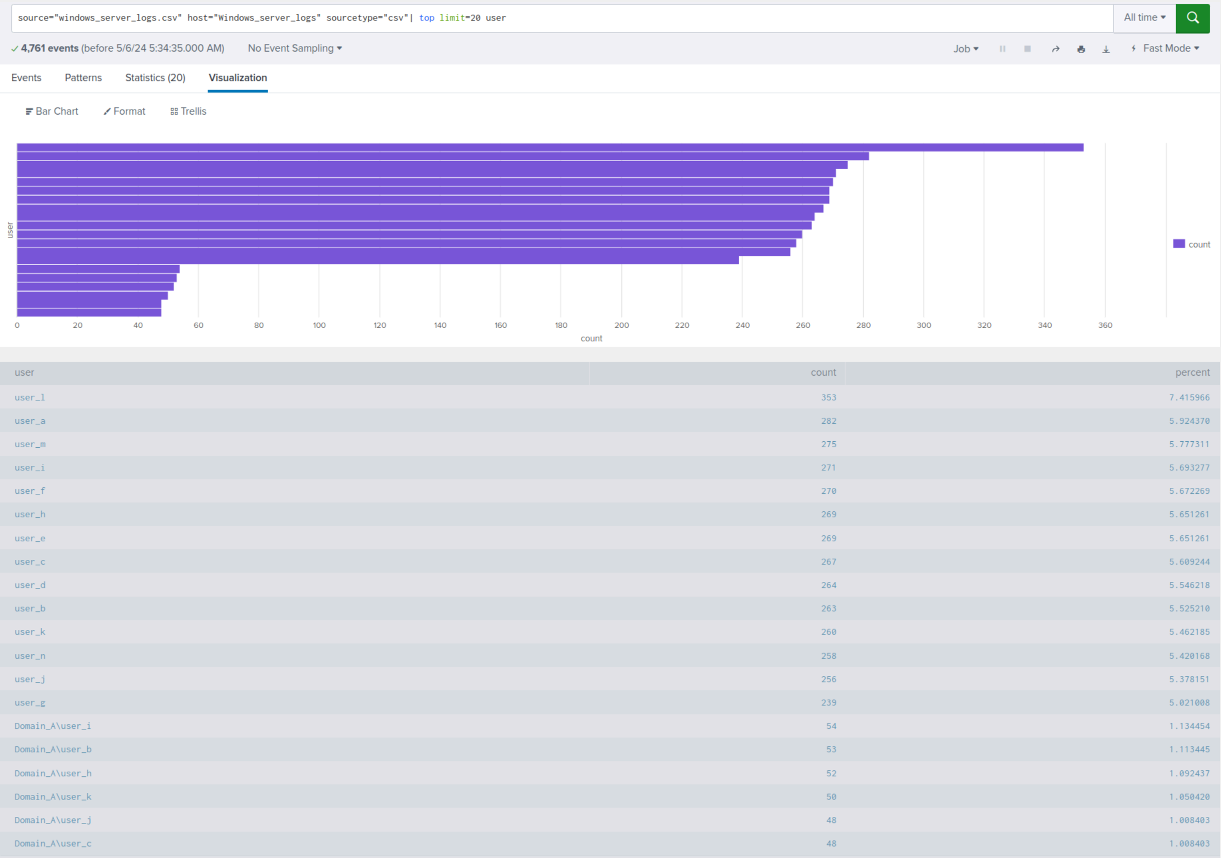
- Do the results match your findings in your time chart for signatures?

```
The Results match our findings for signatures.
```

Dashboard Analysis for Users with Bar, Graph, and Pie Charts

- Does anything stand out as suspicious?

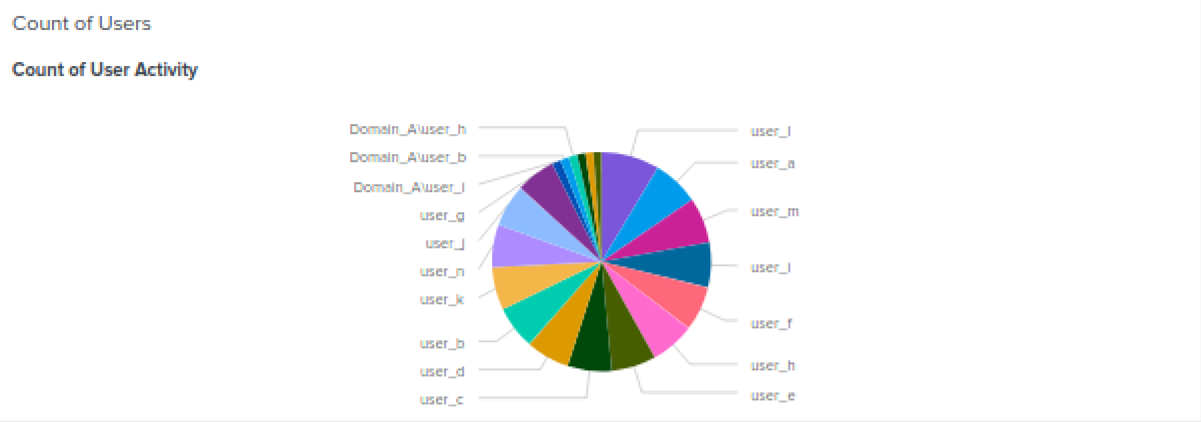
```
Our Dashboard indicates an Increase in activity for 2 users.

Regular Dashboard:
```



```
source="windows_server_logs.csv" host="Windows_server_logs" sourcetype="csv"| top limit=20 user
```

✓ 4,761 events (before 5/6/24 5:34:35.000 AM)

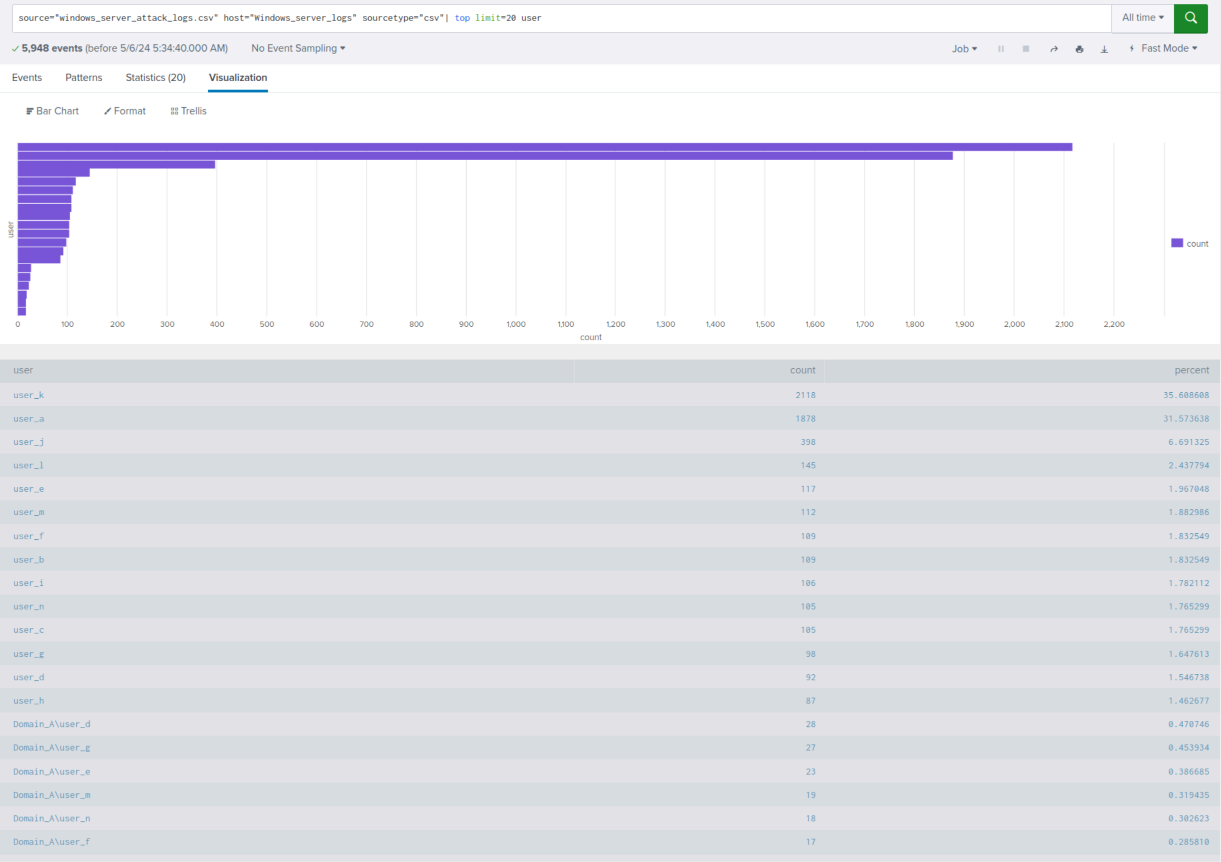
user	count	percent
user_l	353	7.415966
user_a	282	5.924370
user_m	275	5.777311
user_i	271	5.693277
user_f	270	5.672269
user_h	269	5.651261
user_e	269	5.651261
user_c	267	5.609244
user_d	264	5.546218
user_b	263	5.525210
user_k	260	5.462185
user_n	258	5.420168
user_j	256	5.378151
user_g	239	5.021008
Domain_A\user_i	54	1.134454
Domain_A\user_b	53	1.113445
Domain_A\user_h	52	1.092437
Domain_A\user_k	50	1.050420
Domain_A\user_j	48	1.008403
Domain_A\user_c	48	1.008403



Count of Users

Count of User Activity

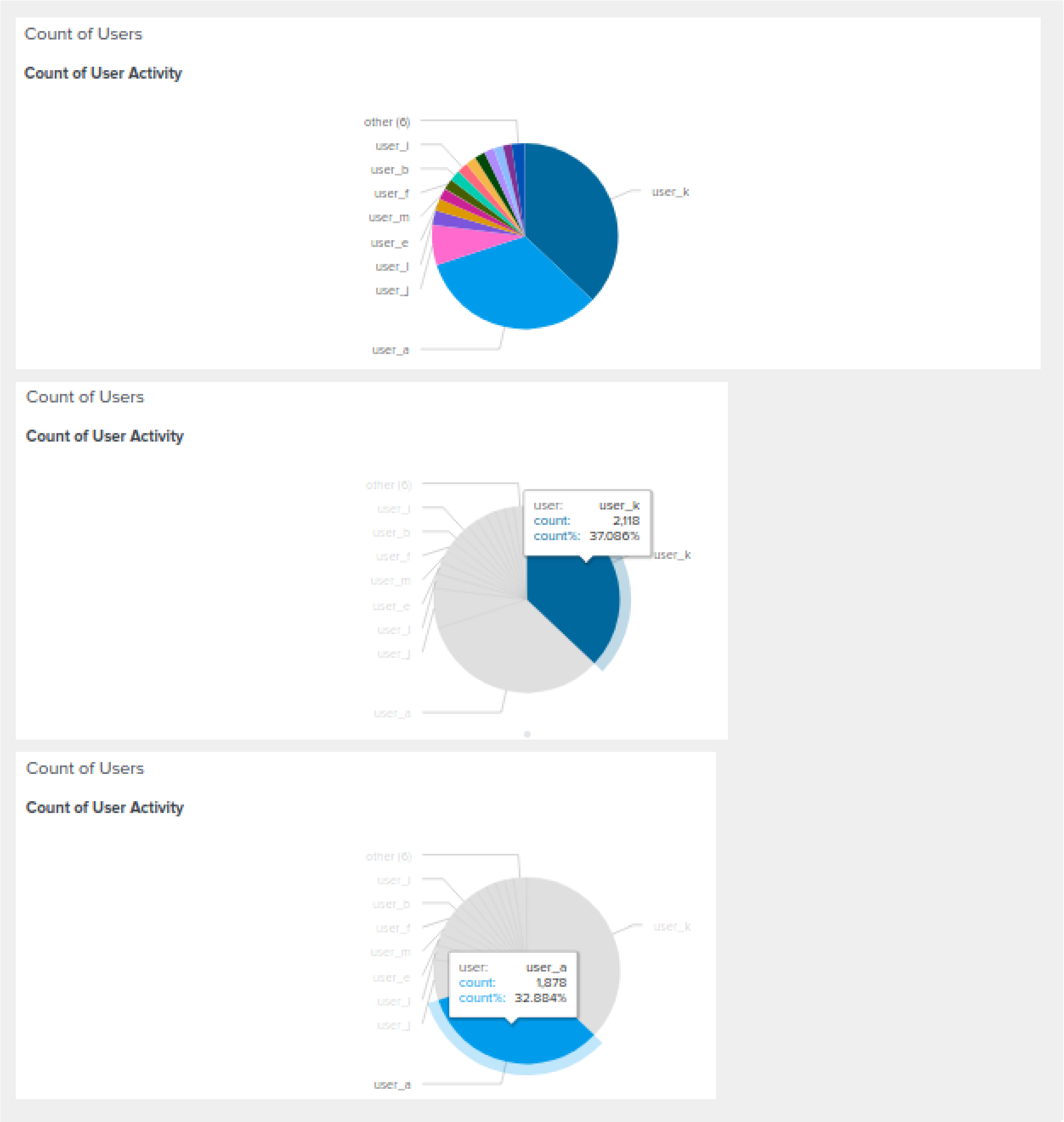
Attack Dashboard:



```
source="windows_server_attack_logs.csv" host="Windows_server_logs" sourcetype="csv"| top limit=20 user
```

✓ **5,948 events** (before 5/6/24 5:34:40.000 AM)

user	count	percent
user_k	2118	35.608608
user_a	1878	31.573638
user_j	398	6.691325
user_l	145	2.437794
user_e	117	1.967048
user_m	112	1.882986
user_f	109	1.832549
user_b	109	1.832549
user_i	106	1.782112
user_n	105	1.765299
user_c	105	1.765299
user_g	98	1.647613
user_d	92	1.546738
user_h	87	1.462677
Domain_A\user_d	28	0.470746
Domain_A\user_g	27	0.453934
Domain_A\user_e	23	0.386685
Domain_A\user_m	19	0.319435
Domain_A\user_n	18	0.302623
Domain_A\user_f	17	0.285810



- Do the results match your findings in your time chart for users?

```
The results match our findings for users.
```

Dashboard Analysis for Users with Statistical Charts

- What are the advantages and disadvantages of using this report, compared to the other user panels that you created?

One of the benefits of utilizing statistical time charts for signatures and users is the ability to swiftly ascertain the count of each event or user on an hourly basis. However, a potential drawback of these charts, when compared to bar graphs and pie charts, is the lack of immediate clarity regarding shifts in activity.

Visualizations such as bar graphs and pie charts provide a quick overview of where there are surges or decreases in an event and at what time. Specifically, pie charts offer a rapid understanding of which event or user has seen an increase in activity, along with the corresponding count. These graphical representations can be instrumental in identifying patterns and trends in the data.

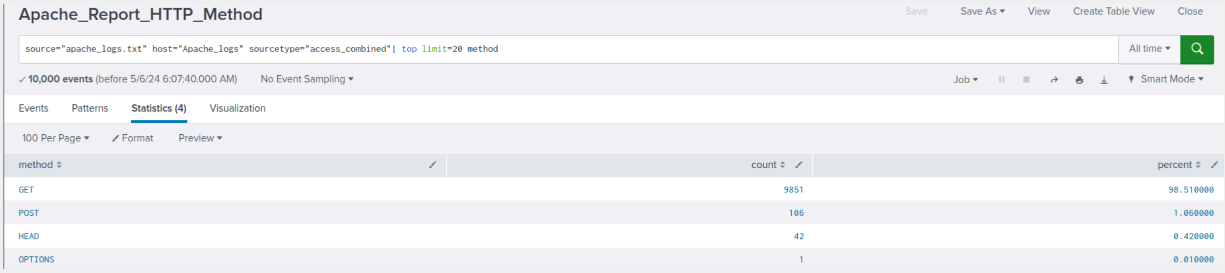
Apache Web Server Log Questions

Report Analysis for Methods

- Did you detect any suspicious changes in HTTP methods? If so, which one?

We have identified suspicious changes associated with HTTP methods, particularly in relation to POST requests.

Regular Report:



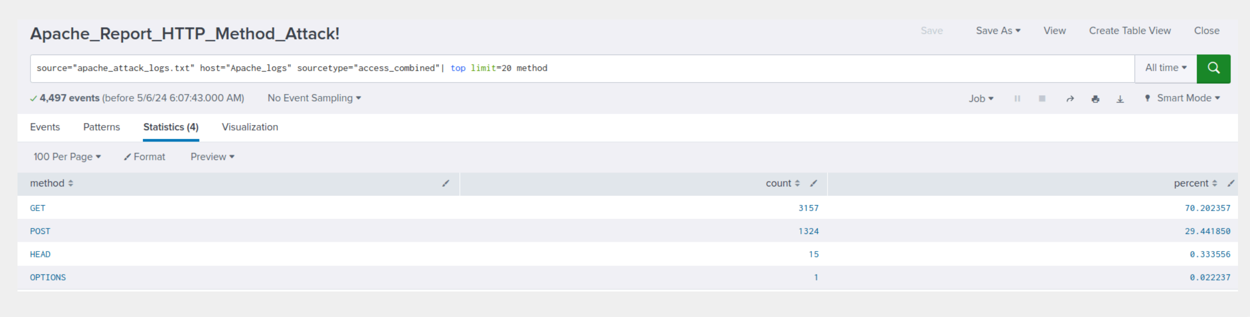
Apache_Report_HTTP_Method

```
source="apache_logs.txt" host="Apache_logs" sourcetype="access_combined"| top limit=20 method
```

✓ 10,000 events (before 5/6/24 6:07:40.000 AM)

method	count	percent
GET	9851	98.510000
POST	106	1.060000
HEAD	42	0.420000
OPTIONS	1	0.010000

Attack Report:



Apache_Report_HTTP_Method_Attack!

```
source="apache_attack_logs.txt" host="Apache_logs" sourcetype="access_combined"| top limit=20 method
```

✓ 4,497 events (before 5/6/24 6:07:43.000 AM) No Event Sampling

method	count	percent
GET	3157	70.202357
POST	1324	29.441850
HEAD	15	0.333556
OPTIONS	1	0.022237

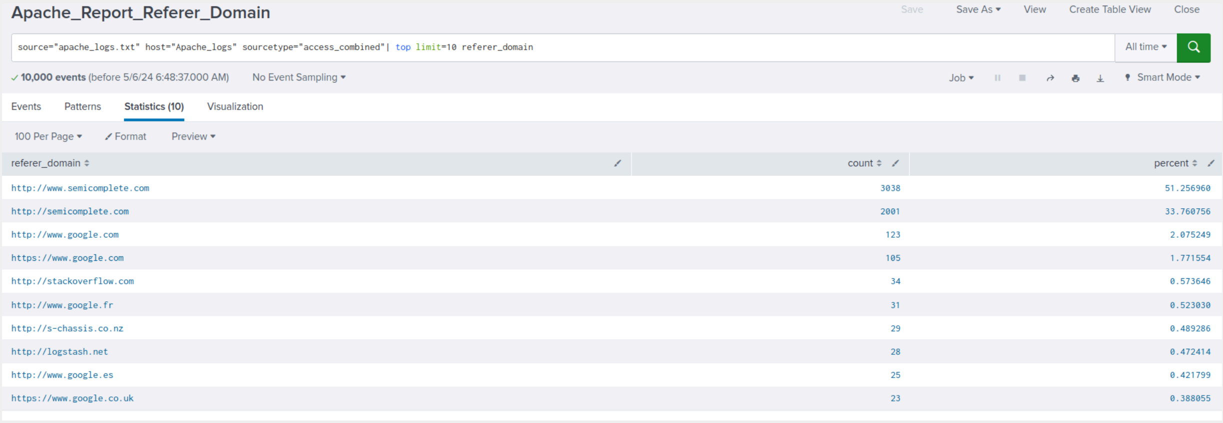
- What is that method used for?

```
The POST method is used to send data to a server to create/update a
resource.
```

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

```
Our Report indicates there is a decrease in Referrer Domain count.

Normal Report:
```



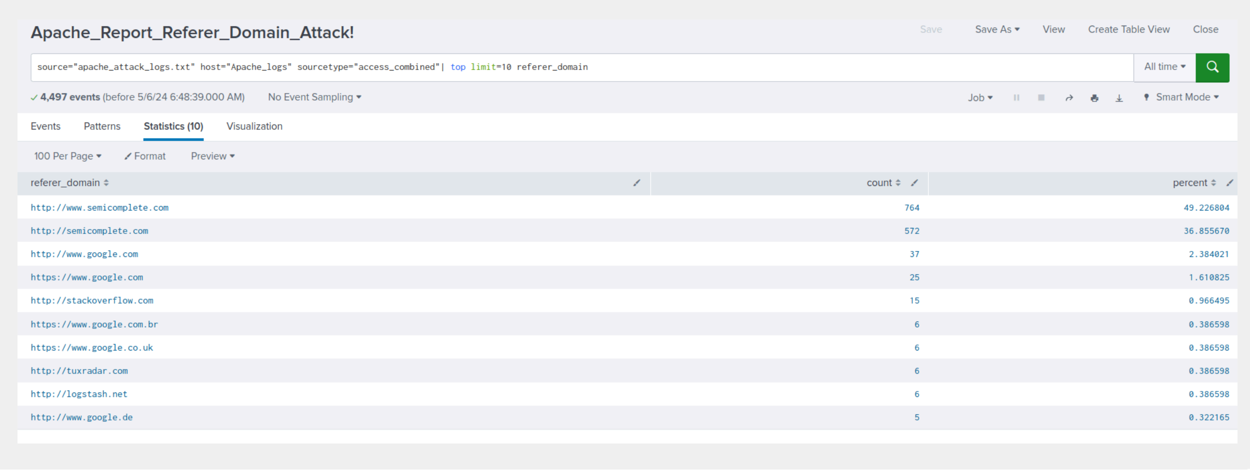
Apache_Report_Referer_Domain

```
source="apache_logs.txt" host="Apache_logs" sourcetype="access_combined"| top limit=10 referer_domain
```

✓ 10,000 events (before 5/6/24 6:48:37.000 AM) No Event Sampling

referer_domain	count	percent
http://www.semicomplete.com	3038	51.256960
http://semicomplete.com	2001	33.760756
http://www.google.com	123	2.075249
https://www.google.com	105	1.771554
http://stackoverflow.com	34	0.573646
http://www.google.fr	31	0.523030
http://s-chassis.co.nz	29	0.489286
http://logstash.net	28	0.472414
http://www.google.es	25	0.421799
https://www.google.co.uk	23	0.388055

```
Attack Report:
```



Apache_Report_Referer_Domain_Attack!

```
source="apache_attack_logs.txt" host="Apache_logs" sourcetype="access_combined"| top limit=10 referer_domain
```

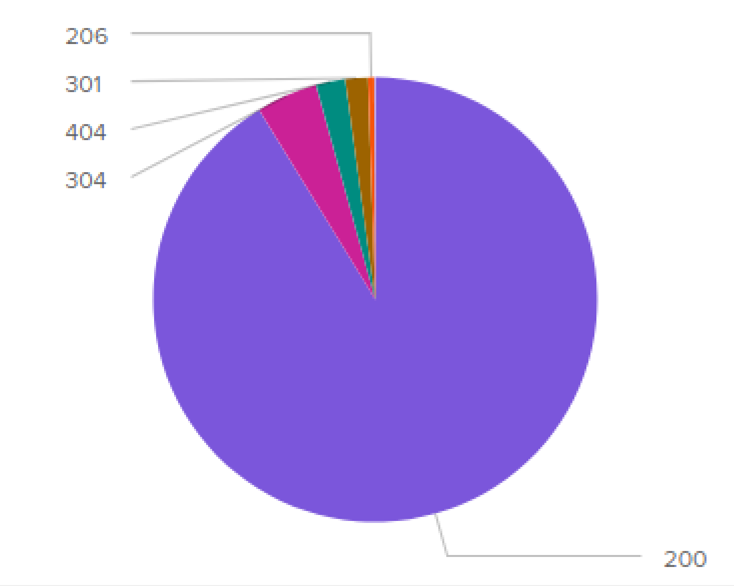
✓ **4,497 events** (before 5/6/24 6:48:39.000 AM) No Event Sampling

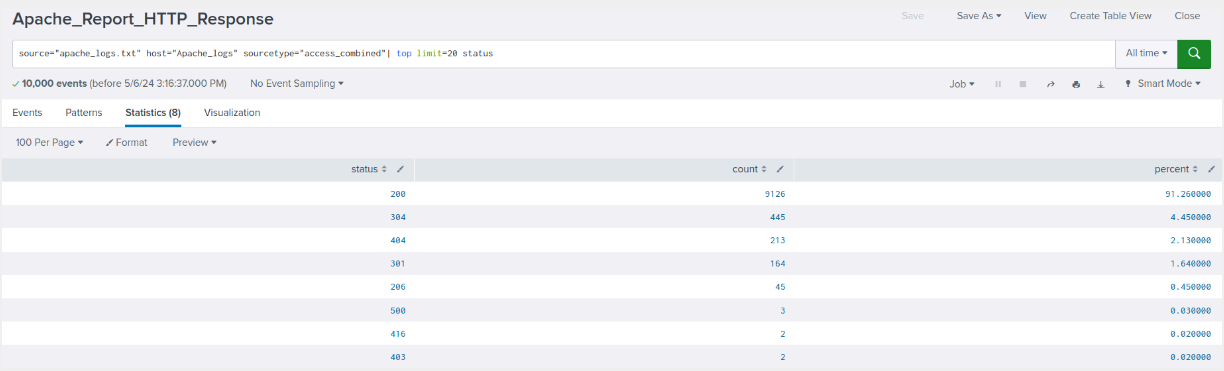
referer_domain	count	percent
http://www.semicomplete.com	764	49.226804
http://semicomplete.com	572	36.855670
http://www.google.com	37	2.384021
https://www.google.com	25	1.610825
http://stackoverflow.com	15	0.966495
https://www.google.com.br	6	0.386598
https://www.google.co.uk	6	0.386598
http://tuxradar.com	6	0.386598
http://logstash.net	6	0.386598
http://www.google.de	5	0.322165

Report Analysis for HTTP Response Codes

- Did you detect any suspicious changes in HTTP response codes?

```
HTTP Response for 200 has around 8% decrease in events
As for the HTTP Response for 404 has an increase around 13% in events

Regular Report:
```





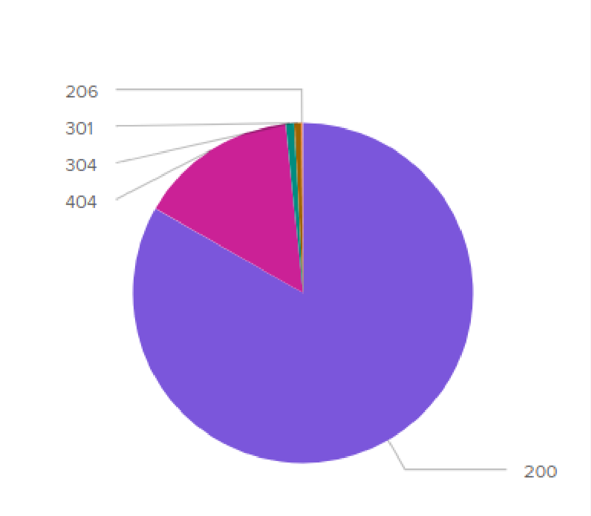
Apache_Report_HTTP_Response

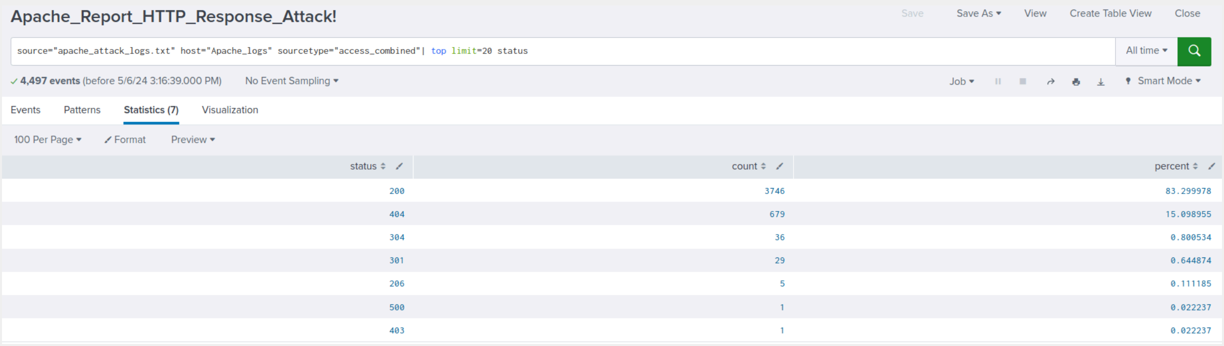
```
source="apache_logs.txt" host="Apache_logs" sourcetype="access_combined"| top limit=20 status
```

✓ 10,000 events (before 5/6/24 3:16:37.000 PM) No Event Sampling

status	count	percent
200	9126	91.260000
304	445	4.450000
404	213	2.130000
301	164	1.640000
206	45	0.450000
500	3	0.030000
416	2	0.020000
403	2	0.020000

```
Attack Report:
```





Apache_Report_HTTP_Response_Attack!

```
source="apache_attack_logs.txt" host="Apache_logs" sourcetype="access_combined"| top limit=20 status
```

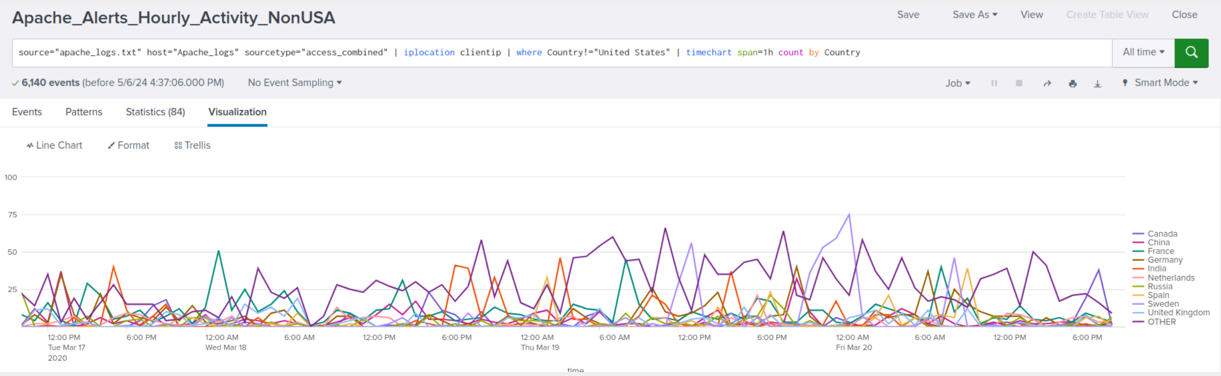
✓ 4,497 events (before 5/6/24 3:16:39.000 PM) No Event Sampling

status	count	percent
200	3746	83.299978
404	679	15.098955
304	36	0.800534
301	29	0.644874
206	5	0.111185
500	1	0.022237
403	1	0.022237

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

```
Our Alert demonstrates an increased spike of events from Ukraine.

Regular Alert:
```

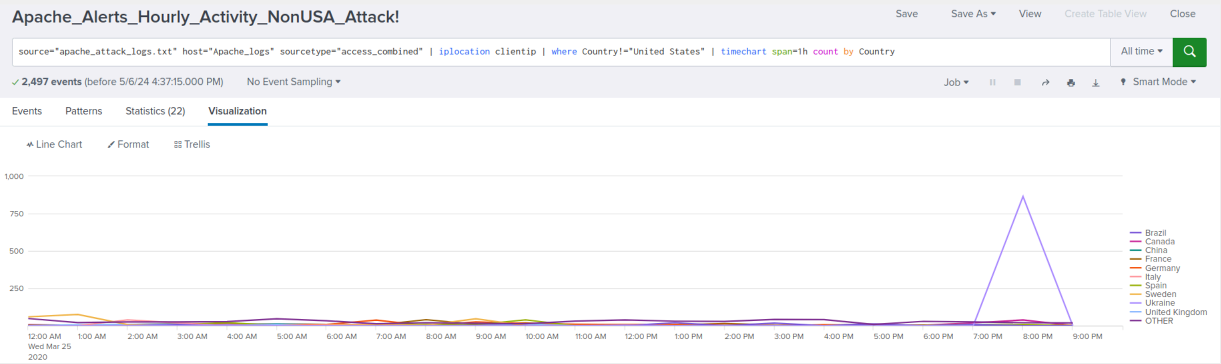


Apache_Alerts_Hourly_Activity_NonUSA

```
source="apache_logs.txt" host="Apache_logs" sourcetype="access_combined" | iplocation clientip | where Country!="United States" | timechart span=1h count by Country
```

✓ **6,140 events** (before 5/6/24 4:37:06.000 PM) No Event Sampling

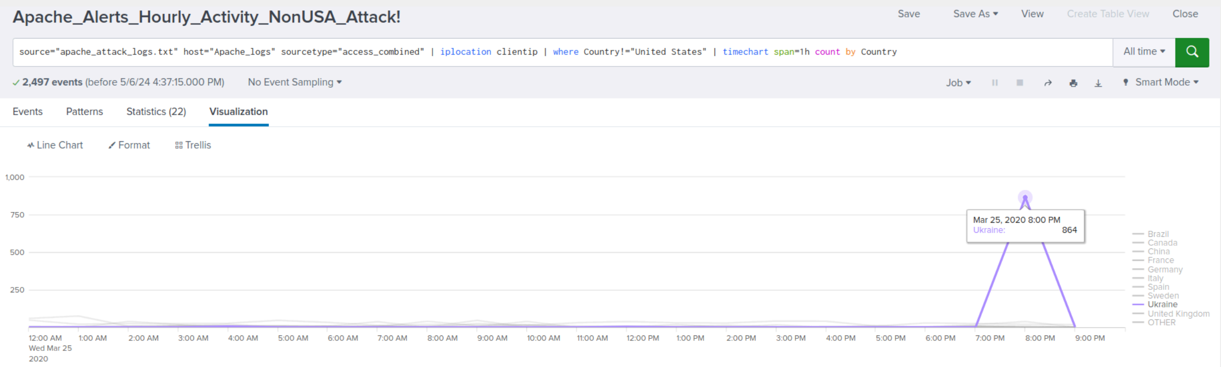
Attack Alert:



Apache_Alerts_Hourly_Activity_NonUSA_Attack!

```
source="apache_attack_logs.txt" host="Apache_logs" sourcetype="access_combined" | iplocation clientip | where Country!="United States" | timechart span=1h count by Country
```

✓ **2,497 events** (before 5/6/24 4:37:15.000 PM) No Event Sampling



Apache_Alerts_Hourly_Activity_NonUSA_Attack!

```
source="apache_attack_logs.txt" host="Apache_logs" sourcetype="access_combined" | iplocation clientip | where Country!="United States" | timechart span=1h count by Country
```

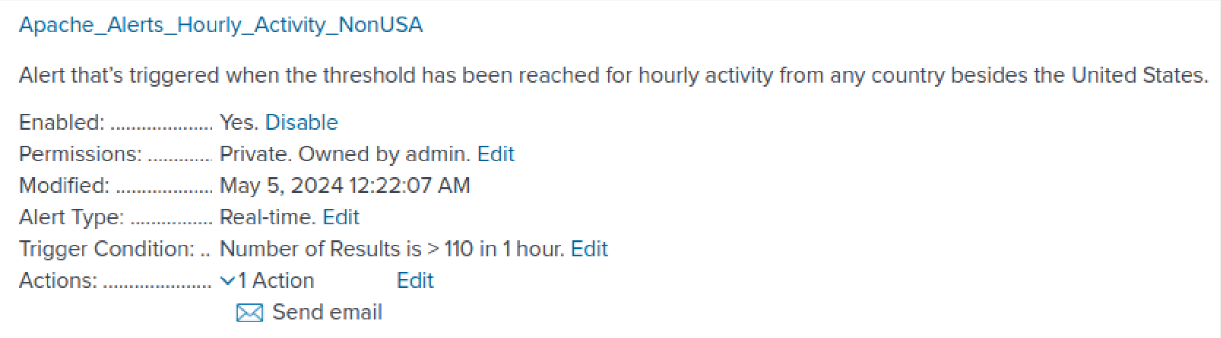
✓ **2,497 events** (before 5/6/24 4:37:15.000 PM) No Event Sampling

- If so, what was the count of the hour(s) it occurred in?

The count shows as 864 at 8:00PM

- Would your alert be triggered for this activity?

Our Alert has a current threshold of >110 in 1 hour, In conclusion the alert would have triggered.


Apache_Alerts_Hourly_Activity_NonUSA

Alert that's triggered when the threshold has been reached for hourly activity from any country besides the United States.

Enabled: .... Yes. Disable
Permissions: .... Private. Owned by admin. Edit
Modified: .... May 5, 2024 12:22:07 AM
Alert Type: .... Real-time. Edit
Trigger Condition: .. Number of Results is > 110 in 1 hour. Edit
Actions: .... 1 Action Edit
Send email

- After reviewing, would you change the threshold that you previously selected?

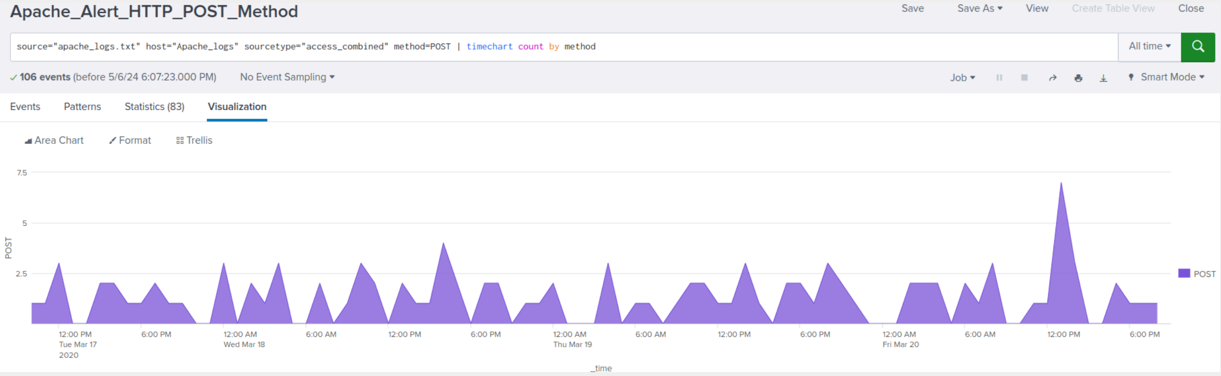
After reviewing our current Alert, we intend to uphold the existing threshold. However we will continuously inspect the Apache events with the prospect of augmenting the threshold value in the forthcoming period.

Alert Analysis for HTTP POST Activity

- Did you detect any suspicious volume of HTTP POST activity?

Our Alert shows a decreased number of events for HTTP POST for several hours & A spike occurrence later on.

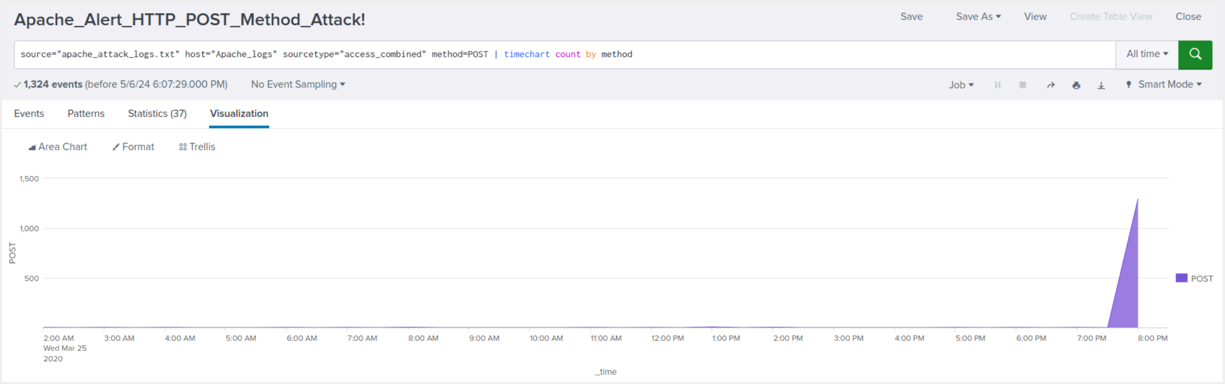
Regular Alert:


Apache_Alert_HTTP_POST_Method

```
source="apache_logs.txt" host="Apache_logs" sourcetype="access_combined" method=POST | timechart count by method
```

✓ 106 events (before 5/6/24 6:07:23.000 PM) No Event Sampling

Attack Alert:



Apache_Alert_HTTP_POST_Method_Attack!

```
source="apache_attack_logs.txt" host="Apache_logs" sourcetype="access_combined" method=POST | timechart count by method
```

✓ **1,324 events** (before 5/6/24 6:07:29.000 PM) No Event Sampling ▾

- If so, what was the count of the hour(s) it occurred in?

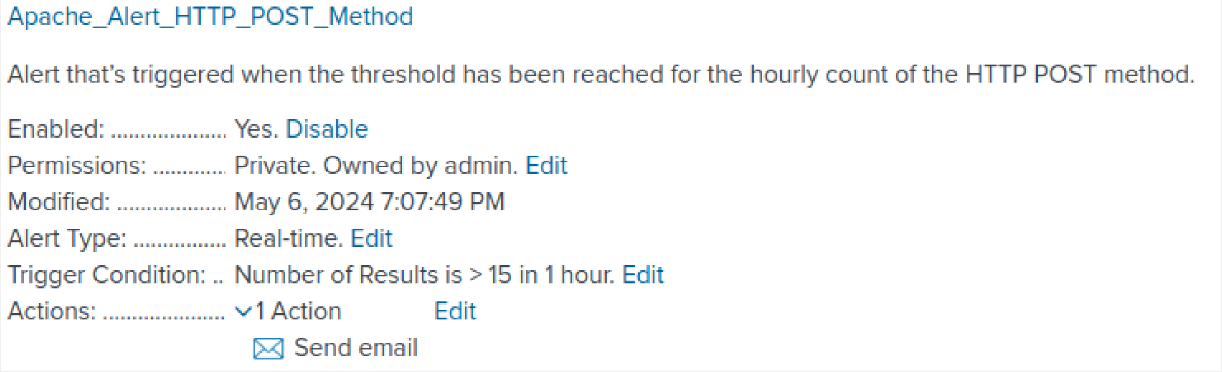
```
The count transpired to be at 1296 and occurred at 8:00PM
```

- When did it occur?

```
The event transpired on March 25, 2020
```

- After reviewing, would you change the threshold that you previously selected?

```
Our current threshold is >15 in 1 hour. After reviewing we would refrain
from altering the threshold. However, we will undertake an in-depth
examination of the daily occurrences to ascertain whether a future increase
is warranted.
```



Apache_Alert_HTTP_POST_Method

Alert that's triggered when the threshold has been reached for the hourly count of the HTTP POST method.

Enabled: .... Yes. Disable
Permissions: .... Private. Owned by admin. Edit
Modified: .... May 6, 2024 7:07:49 PM
Alert Type: .... Real-time. Edit
Trigger Condition: .. Number of Results is > 15 in 1 hour. Edit
Actions: .... ✓1 Action Edit
✉ Send email

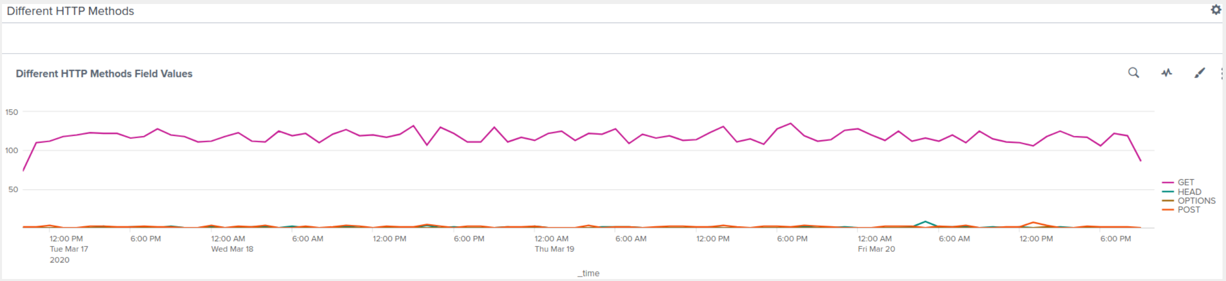
Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

The timechart displays a significant difference for HTTP Methods.

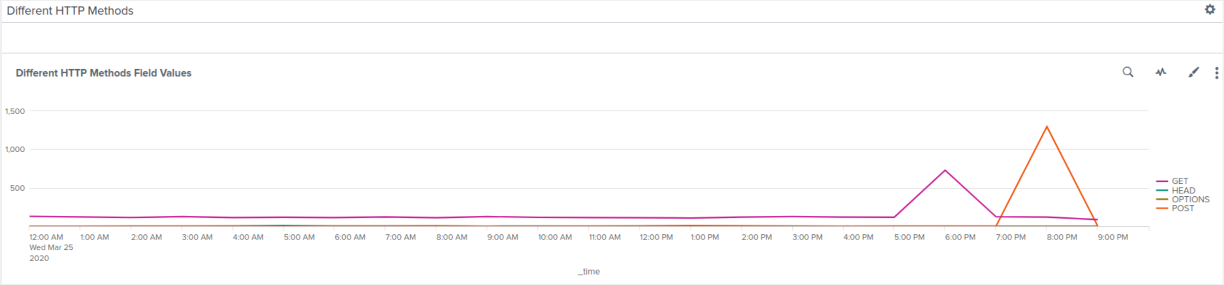
Regular Dashboard:

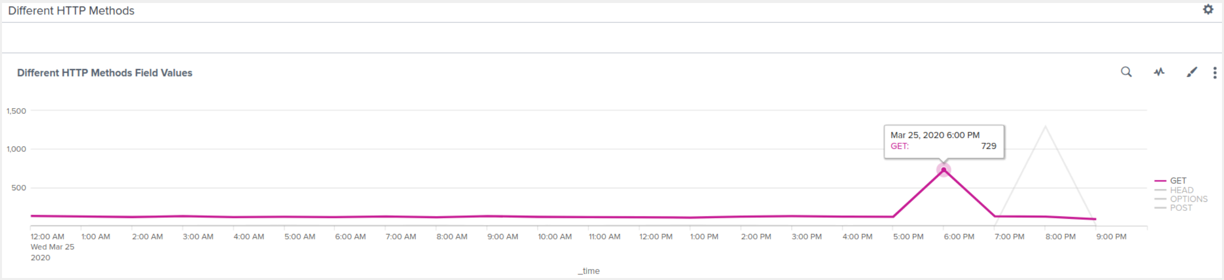
```
source="apache_logs.txt" host="Apache_logs" sourcetype="access_combined" | timechart span=1h count by method
```

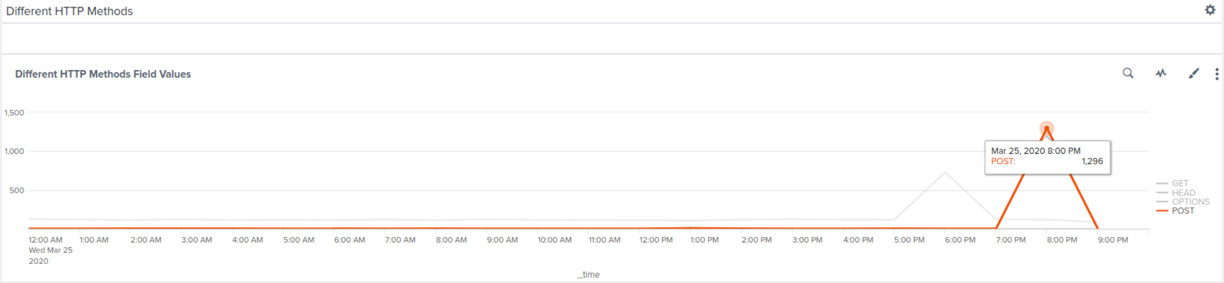


Attack Dashboard:

```
source="apache_attack_logs.txt" host="Apache_logs" sourcetype="access_combined" | timechart span=1h count by method
```







- Which method seems to be used in the attack?

The Method used in the current attack demonstrates GET & POST

- At what times did the attack start and stop?

```
The time of the attack as displayed on our dashboard indicate the following:
GET 5:00PM - 7:00PM
POST 7:00PM - 9:00PM
```

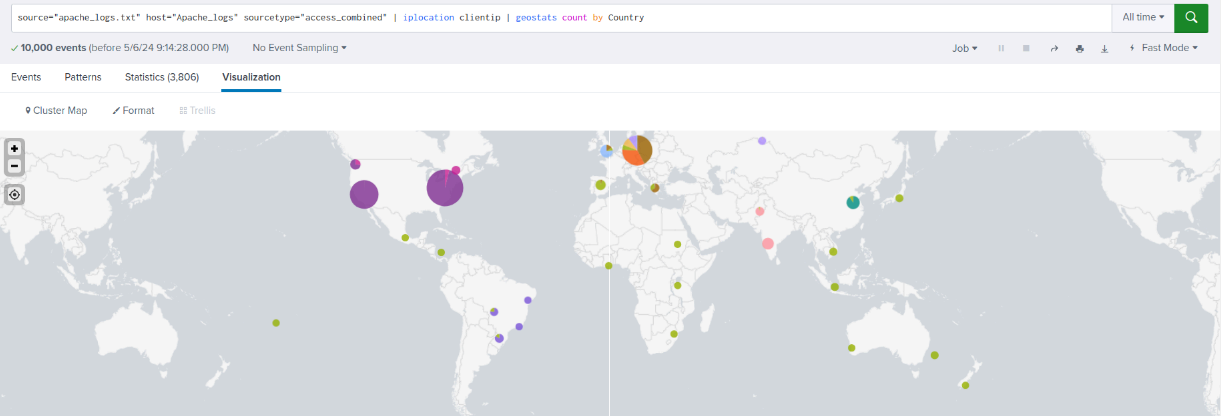
- What is the peak count of the top method during the attack?

The top Method Count during the attack would be for **POST at 1,296** following **GET at 729** count.

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

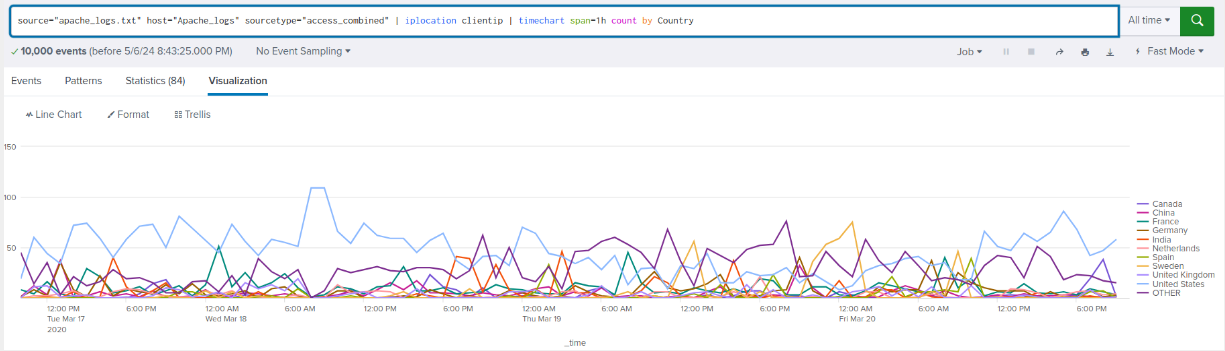
Regular Dashboard:



```
source="apache_logs.txt" host="Apache_logs" sourcetype="access_combined" | iplocation clientip | geostats count by Country
```

✓ 10,000 events (before 5/6/24 9:14:28.000 PM)

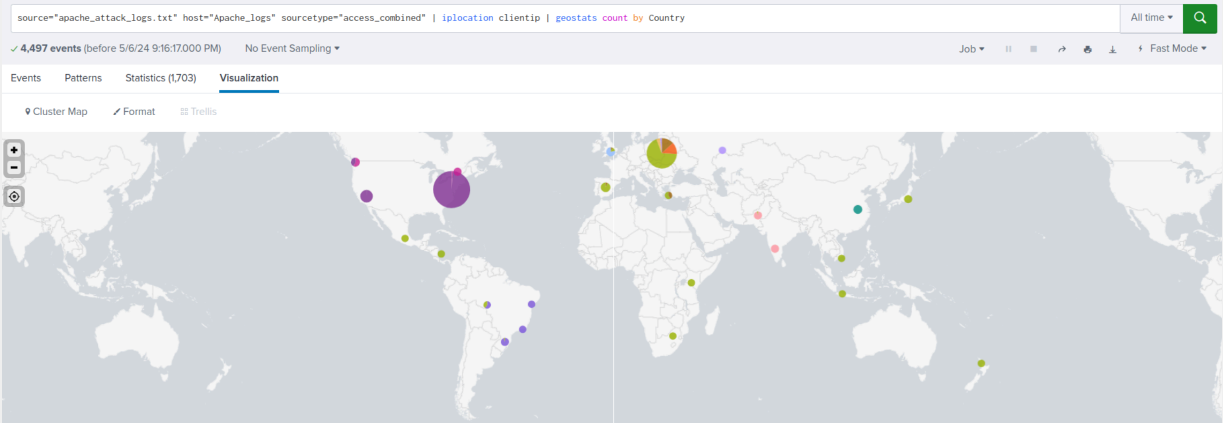
Regular Dashboard: Line Chart Comparison



```
source="apache_logs.txt" host="Apache_logs" sourcetype="access_combined" | iplocation clientip | timechart span=1h count by Country
```

✓ 10,000 events (before 5/6/24 8:43:25.000 PM)

Attack Dashboard:

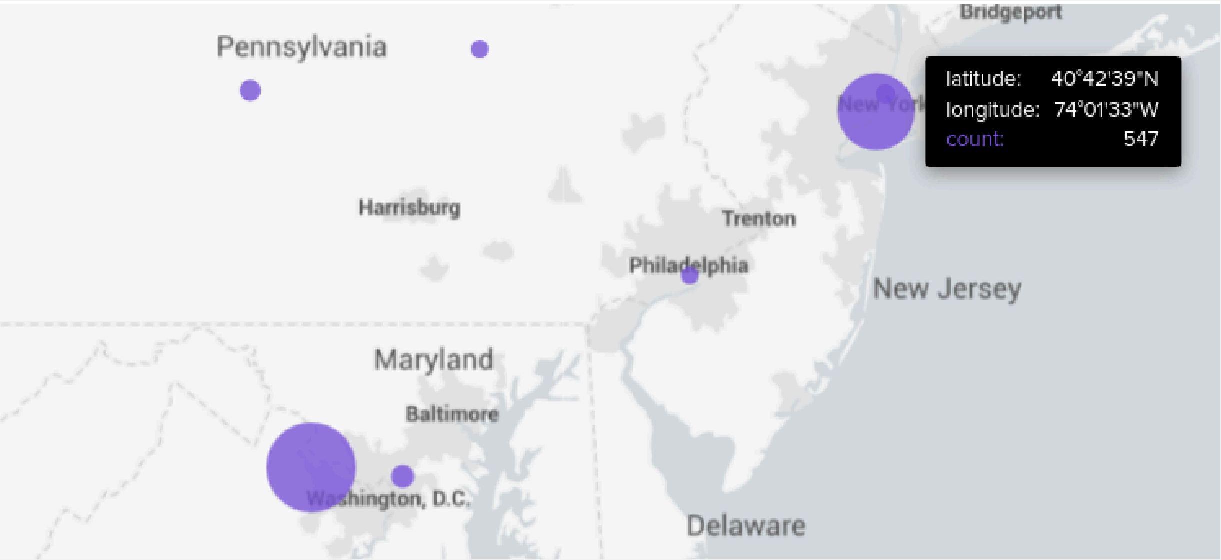


```
source="apache_attack_logs.txt" host="Apache_logs" sourcetype="access_combined" | iplocation clientip | geostats count by Country
```

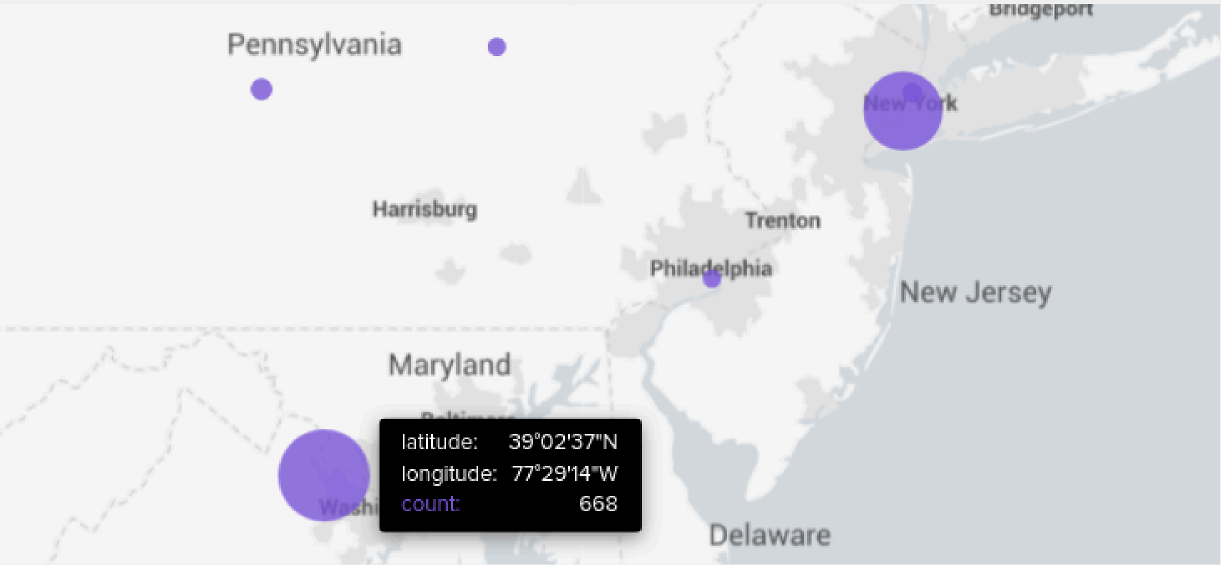
✓ 4,497 events (before 5/6/24 9:16:17.000 PM) No Event Sampling ▾

Results:

1) United States:

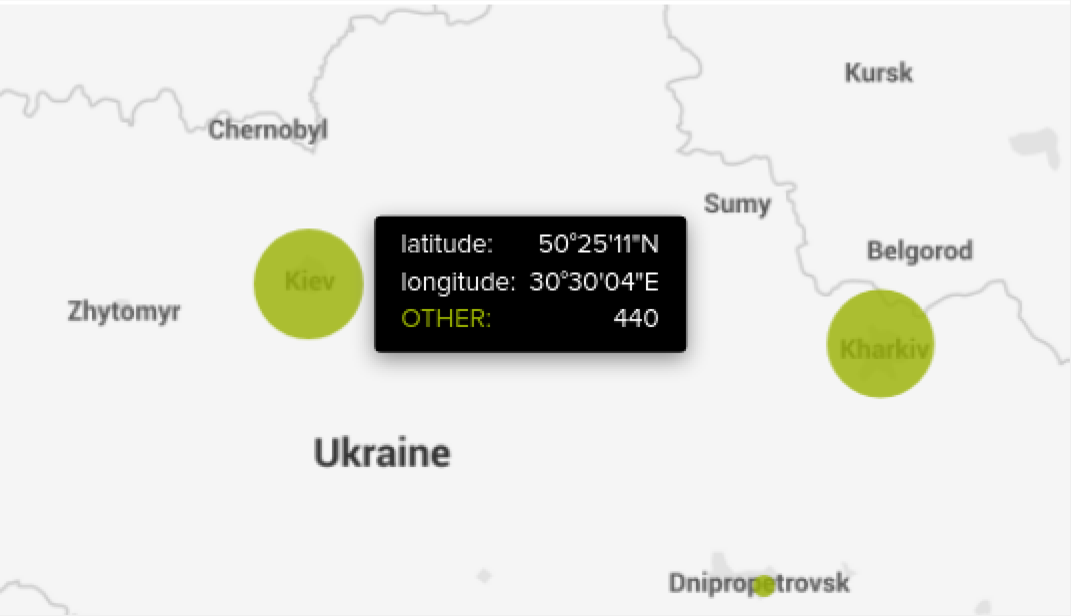


latitude: 40°42'39"N
longitude: 74°01'33"W
count: 547

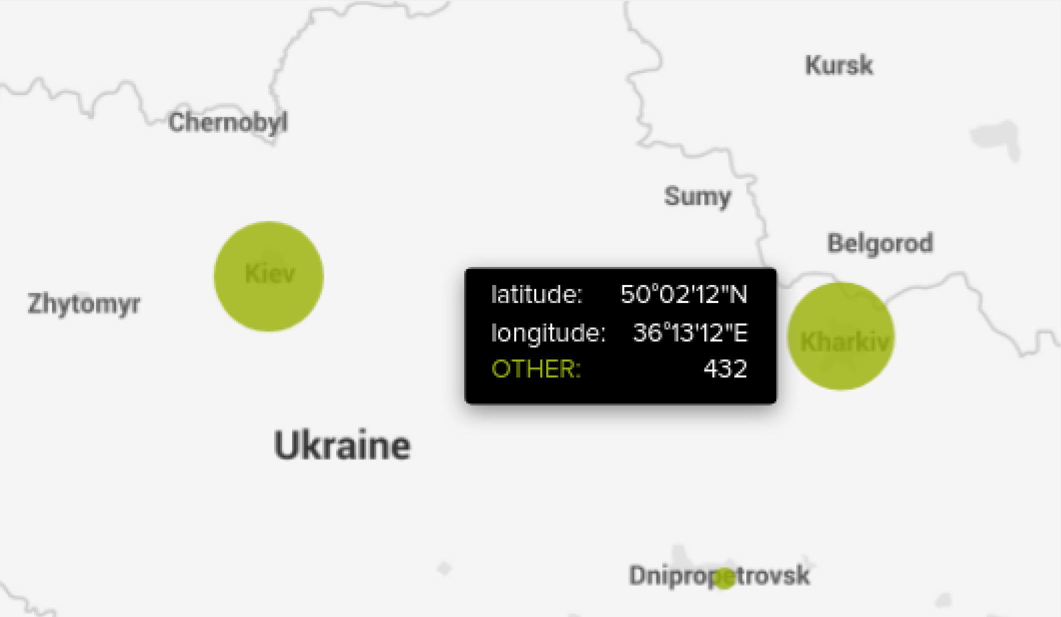


latitude: 39°02'37"N
longitude: 77°29'14"W
count: 668

```
2) Ukraine:
```



latitude: 50°25'11"N
longitude: 30°30'04"E
OTHER: 440



latitude: 50°02'12"N
longitude: 36°13'12"E
OTHER: 432

- Which new location (city, country) on the map has a high volume of activity? (**Hint**: Zoom in on the map.)

```
The current high Country volume of activity are:
1) United States: New York, Washington DC
2) Ukraine: Kiev, Kharkiv
```

- What is the count of that city?

The Count of activities are demonstrated as follows:

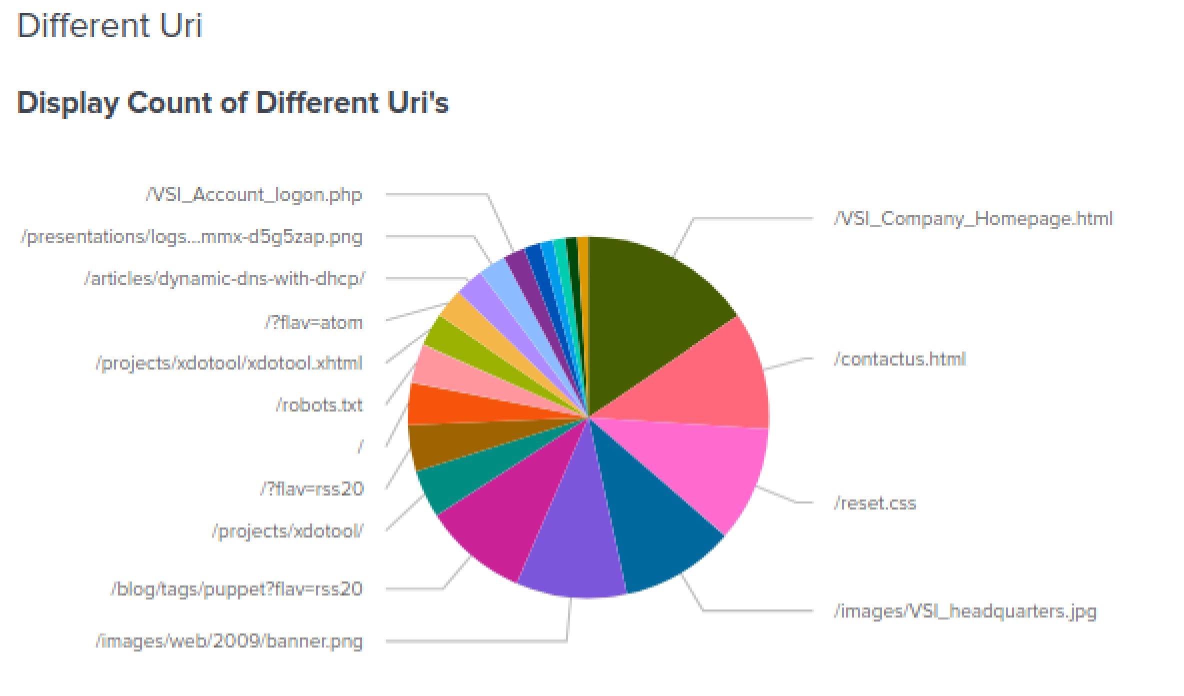
1) United States:
   - **New York** 547
   - **Washington DC** 668
2) Ukraine:
   - **Kiev** 440
   - **Kharkiv** 432

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

There are suspicious anomalies occurring on our URI Data.

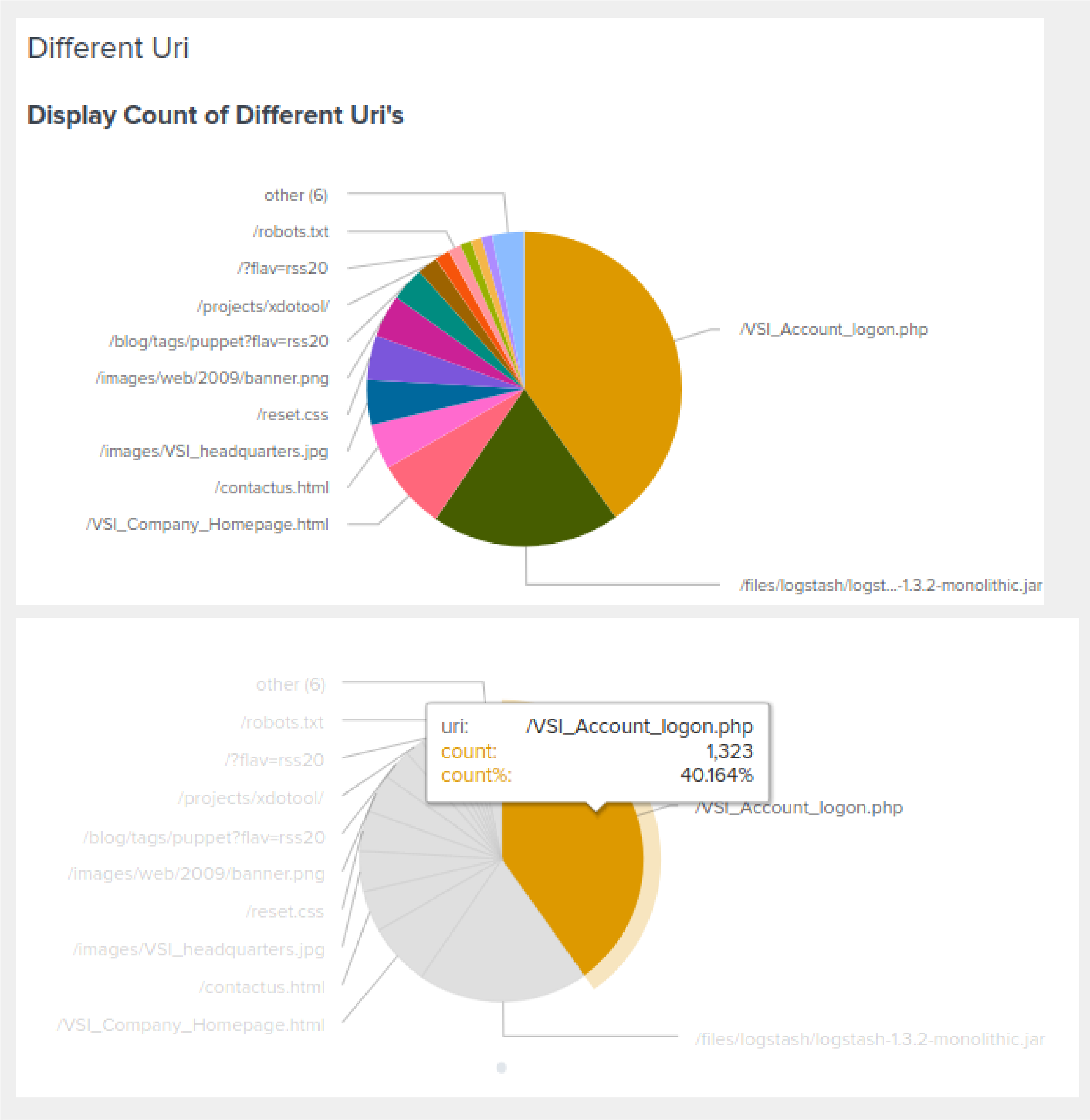
Regular Dashboard:



Different Uri

Display Count of Different Uri's

Attack Dashboard:

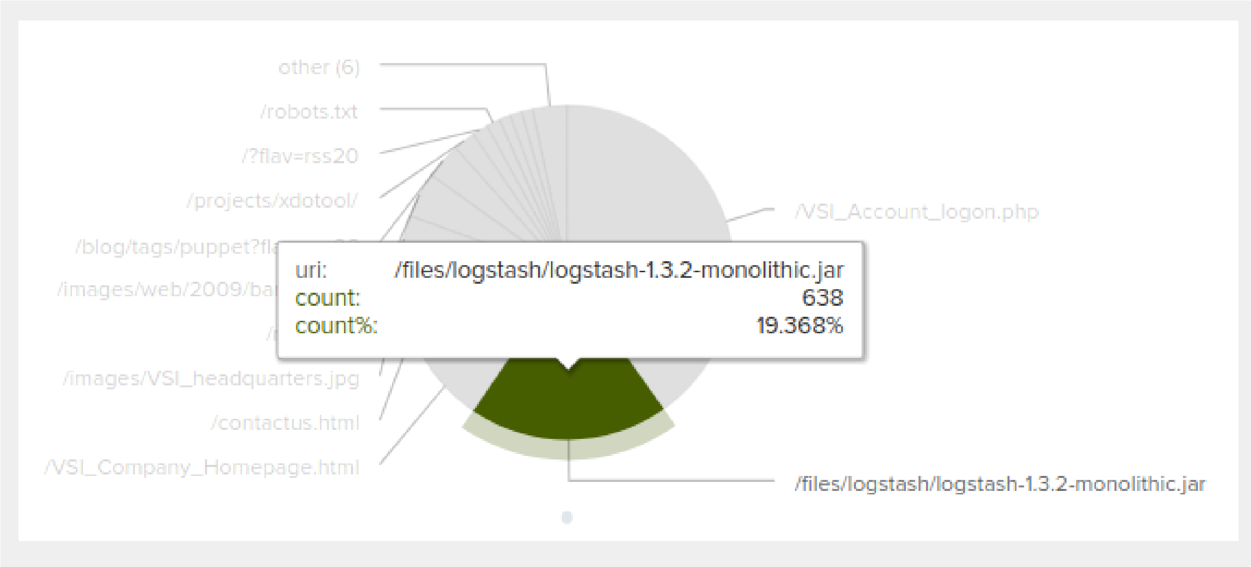


Different Uri

Display Count of Different Uri's

other (6)
/robots.txt
/?flav=rss20
/projects/xdotool/
/blog/tags/puppet?flav=rss20
/images/web/2009/banner.png
/reset.css
/images/VSI_headquarters.jpg
/contactus.html
/VSI_Company_Homepage.html
/VSI_Account_logon.php
/files/logstash/logst...-1.3.2-monolithic.jar
other (6)
/robots.txt
/?flav=rss20
/projects/xdotool/
/blog/tags/puppet?flav=rss20
/images/web/2009/banner.png
/reset.css
/images/VSI_headquarters.jpg
/contactus.html
/VSI_Company_Homepage.html
/VSI_Account_logon.php
/files/logstash/logstash-1.3.2-monolithic.jar

uri: /VSI_Account_logon.php
count: 1,323
count%: 40.164%



- What URI is hit the most?

The Current Uris affected the most are the following:

1) **/VSI/_Account_logon.php** at 1323
2) **/files/logstash-1.3.2-monolithic.jar** at 638

- Based on the URI being accessed, what could the attacker potentially be doing?

Based on the URI being accessed, the High traffic on ***/VSI/_Account_logon.php*** and ***/files/logstash-1.3.2-monolithic.jar*** the attacker could potentially be doing the following:

Brute Force Attack: Multiple attempts to log in by guessing username and password combinations on the /VSI/_Account_logon.php page.

Denial of Service (DoS) Attack: Overwhelming server traffic on any page, possibly causing server unavailability.

SQL Injection: Inserting malicious SQL statements into entry fields, if the login code isn’t properly secured.