Cybersecurity

Project 3 Review Questions

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

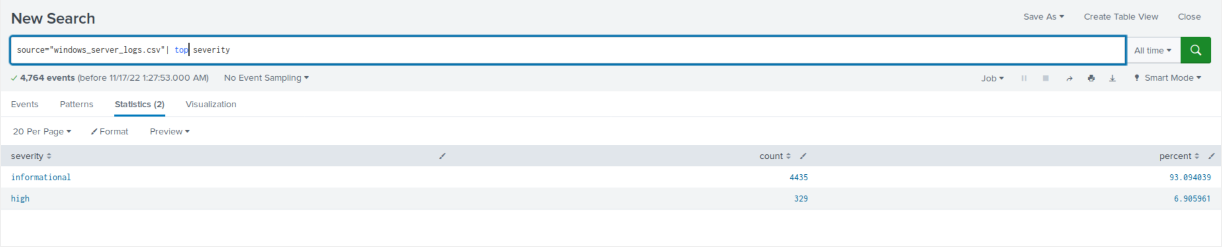
Windows Server Log Questions

Report Analysis for Severity

- Did you detect any suspicious changes in severity?

Yes, our report did detect changes in severity, the biggest being for high severity events. They increased from roughly 7% to 20% during the attack.

Normal activity logs:

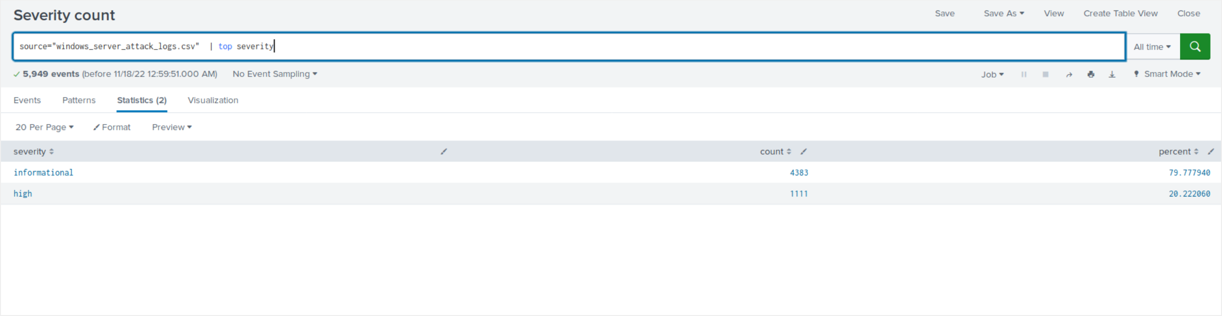


```
source="windows_server_logs.csv"| top severity
```

✓ 4,764 events (before 11/17/22 1:27:53.000 AM)

severity	count	percent
informational	4435	93.094039
high	329	6.905961

Attack logs:



```
source="windows_server_attack_logs.csv"  | top severity
```

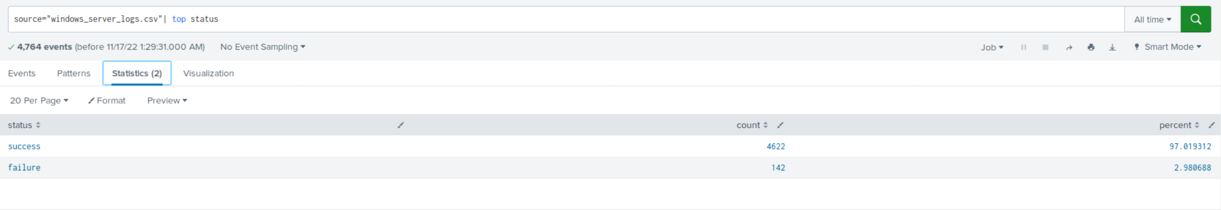
✓ 5,949 events (before 11/18/22 12:59:51.000 AM)

severity	count	percent
informational	4383	79.777940
high	1111	20.222060

Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

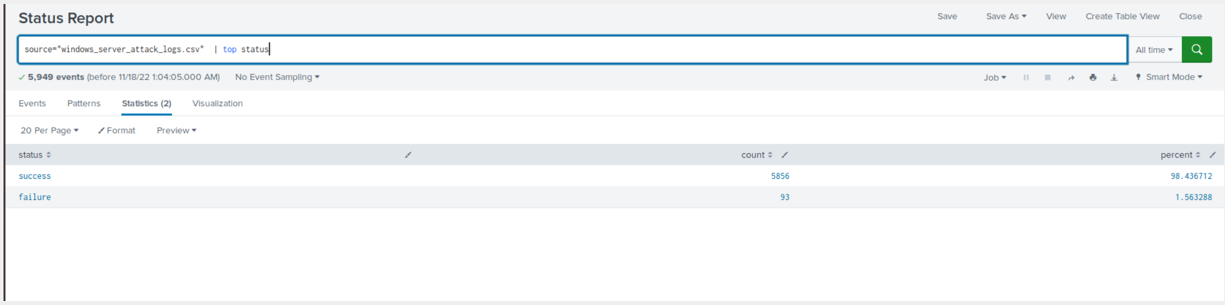
```
Yes, we did see changes in our report on the status of activities between
normal logs and the attack logs.  From our analysis we can see that the
number of successful activities increased and the number of failed
activities decreased.
Normal activity logs:
```



```
source="windows_server_logs.csv"| top status
```

status	count	percent
success	4622	97.019312
failure	142	2.980688

```
Attack logs:
```



Status Report

```
source="windows_server_attack_logs.csv"  | top status
```

status	count	percent
success	5856	98.436712
failure	93	1.563288

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

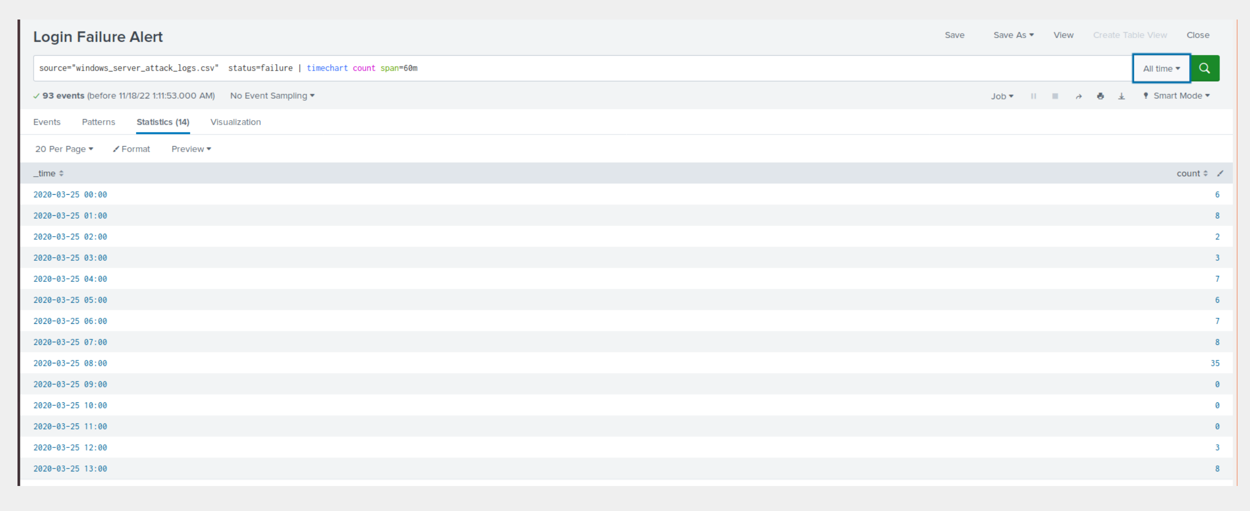
```
Our alert did detect a suspicious volume of failed Windows activity
```

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

```
The count was 35 failed Windows activities
```

- When did it occur?

```
It occurred at 08:00 AM on 2020-03-25
```



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

✓ **93 events** (before 11/18/22 1:11:53.000 AM)

_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
2020-03-25 09:00	0
2020-03-25 10:00	0
2020-03-25 11:00	0
2020-03-25 12:00	3
2020-03-25 13:00	8

- Would your alert be triggered for this activity?

Yes our alert would have been triggered as we set our threshold to alert us if there were more than 15 failed Windows activities in an hour.

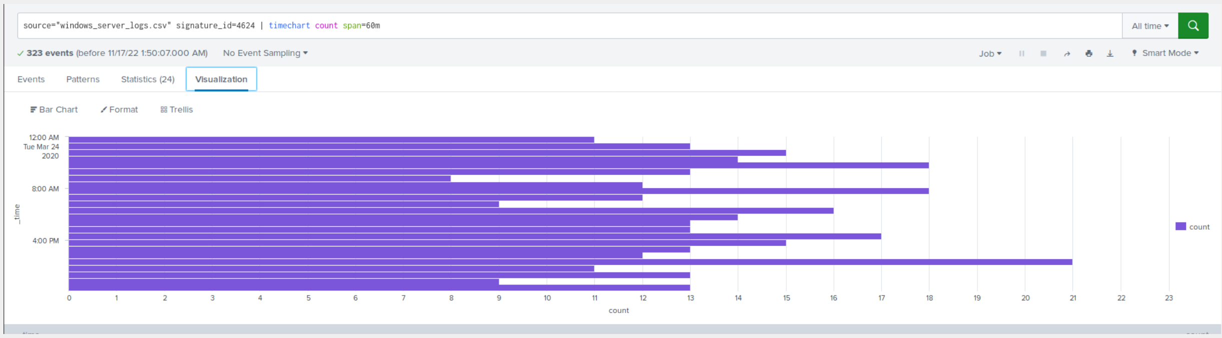
- After reviewing, would you change your threshold from what you previously selected?

I would not change our threshold as it was set low enough to be triggered by this attack and high enough that we were not getting false positives during the other hours of the attack resulting in alert fatigue.

Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

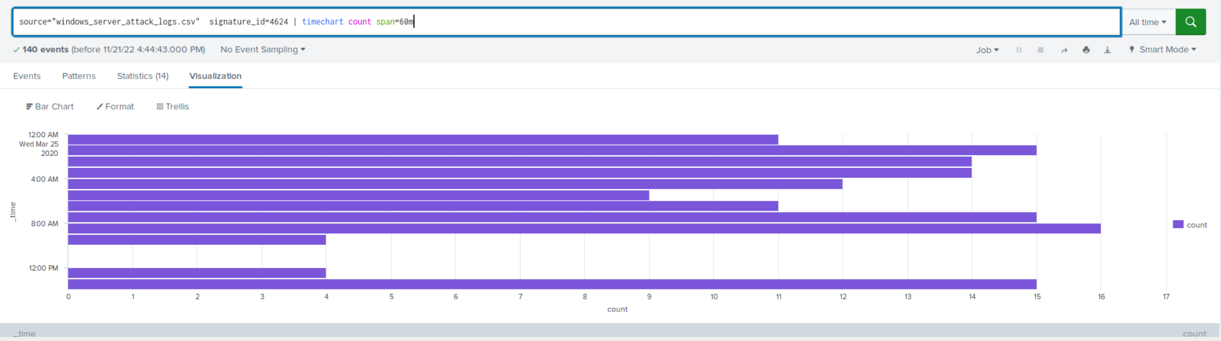
After review of the logs there is a suspicious level of successful logins, but not for an excessive amount but rather a lack of logins.
Normal Log Activity:



```
source="windows_server_logs.csv" signature_id=4624 | timechart count span=60m
```

✓ **323 events** (before 11/17/22 1:50:07.000 AM) No Event Sampling ▾

Attack logs

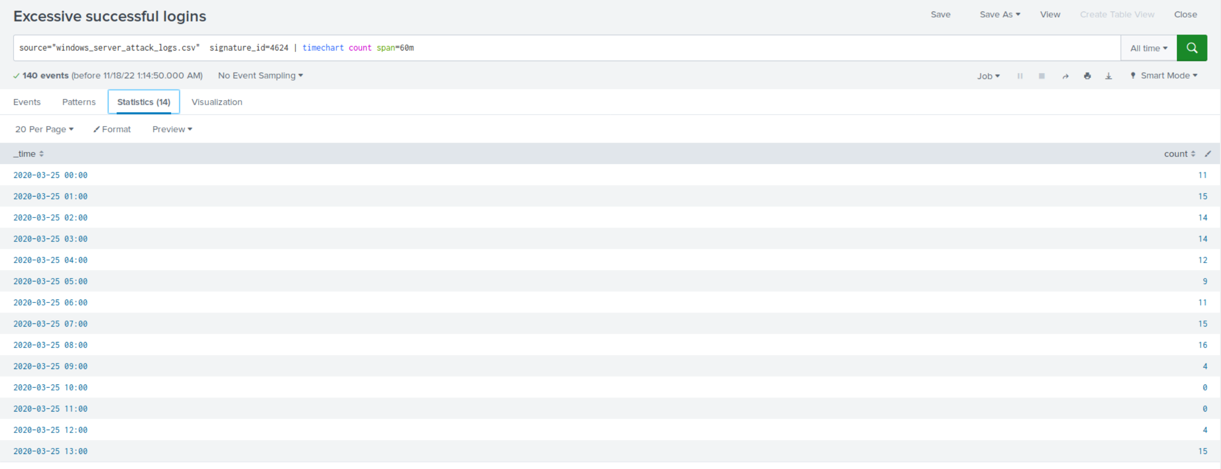


```
source="windows_server_attack_logs.csv"  signature_id=4624 | timechart count span=60m
```

✓ **140 events** (before 11/21/22 4:44:43.000 PM) No Event Sampling ▾

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

At 08:00 AM there were a total of 16 successful logins that occurred and then the number significantly drops to 4 at 09:00 AM AM and is at 0 logins from 10:00 AM to 11:00 AM and goes up to 4 logins at 12:00 PM.



Excessive successful logins

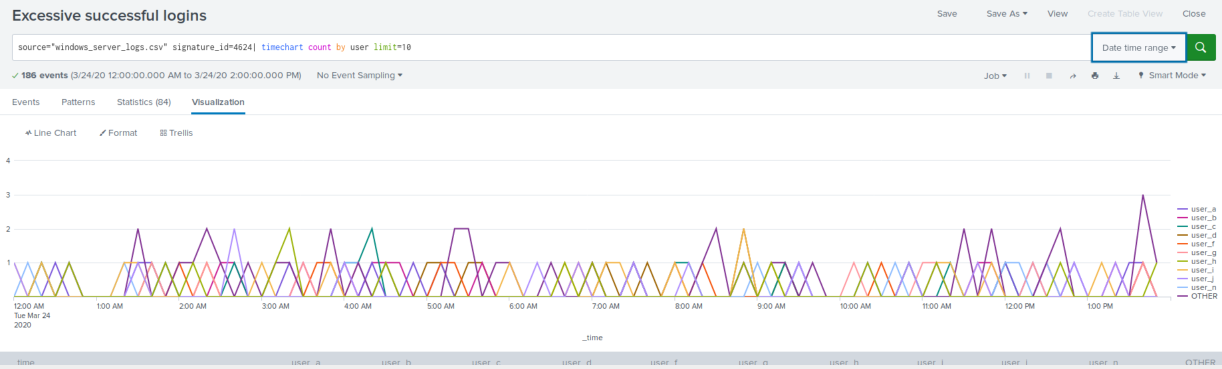
```
source="windows_server_attack_logs.csv"  signature_id=4624 | timechart count span=60m
```

✓ **140 events** (before 11/18/22 1:14:50.000 AM) No Event Sampling ▾

_time	count
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	0
2020-03-25 11:00	0
2020-03-25 12:00	4
2020-03-25 13:00	15

- Who is the primary user logging in?

```
Upon further analysis it appears that at 02:00 AM user_a had a spike in
logins for a total count of 10.
Normal Log:
```

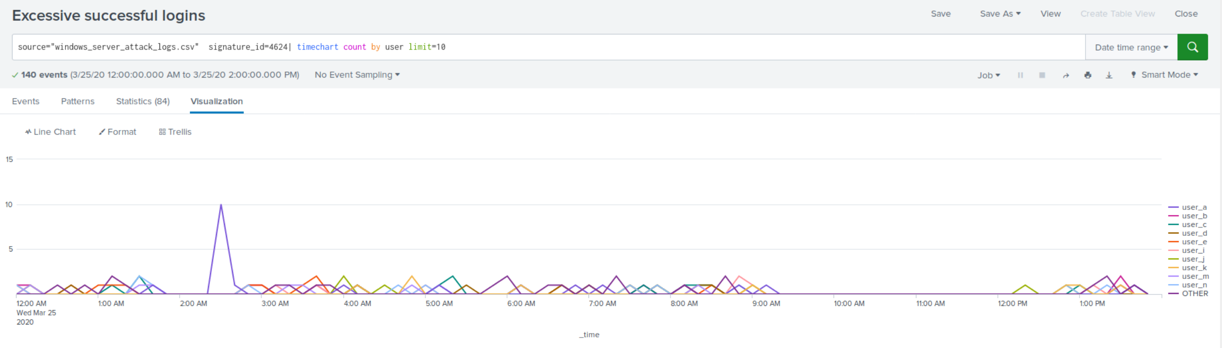


Excessive successful logins

```
source="windows_server_logs.csv" signature_id=4624| timechart count by user limit=10
```

✓ **186 events** (3/24/20 12:00:00.000 AM to 3/24/20 2:00:00.000 PM) No Event Sampling ▾

```
Attack Log:
```



Excessive successful logins

```
source="windows_server_attack_logs.csv"  signature_id=4624| timechart count by user limit=10
```

✓ **140 events** (3/25/20 12:00:00.000 AM to 3/25/20 2:00:00.000 PM) No Event Sampling ▾

- When did it occur?

```
At 02:00 am on 2020-03-25
```

- Would your alert be triggered for this activity?

```
No, our alert would not have been triggered by this activity as we set our
threshold count to 30 or more successful logins an hour to alert the SOC.
```

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

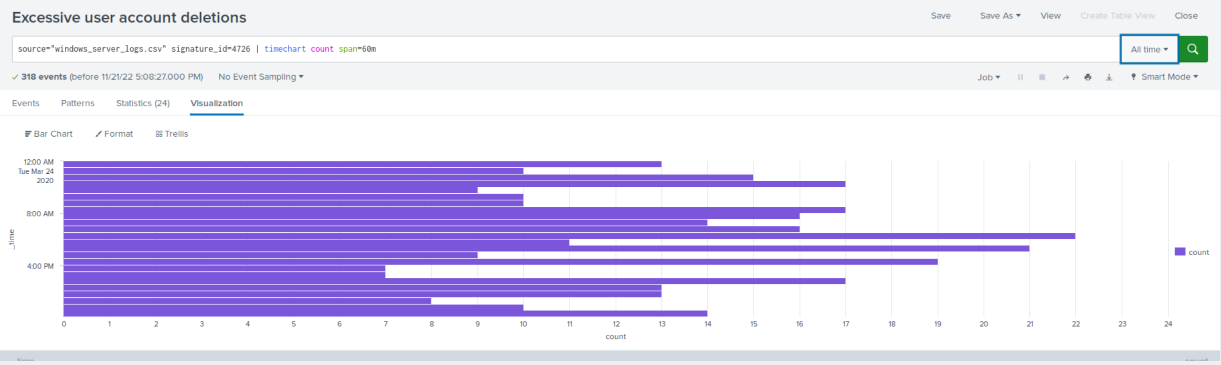
```
I would change the threshold number slightly, but I do think more log data
would need to be analyzed to make that determination as we would want to
avoid alert fatigue. We would want to create an alert if logins dips below a
```

certain number per hour as this attack affected login capabilities. I also think we would need to add in additional alerts as the activity for other signature events increased that we were not monitoring for.

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

We did detect a suspicious amount of deleted accounts, but again not in excessive numbers. Between the hours of 09:00 AM and 11:00 AM there was a significant drop in the number of deletions.
Normal Windows Logs:

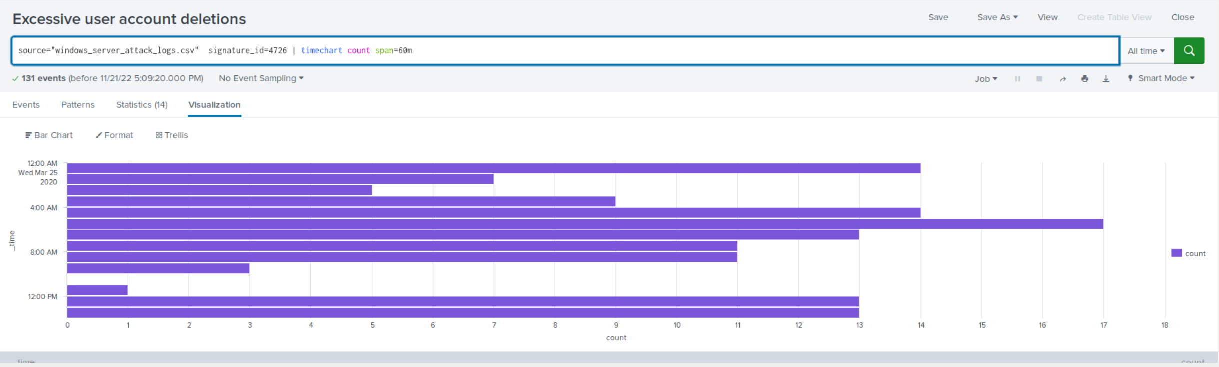


Excessive user account deletions

```
source="windows_server_logs.csv" signature_id=4726 | timechart count span=60m
```

✓ **318 events** (before 11/21/22 5:08:27.000 PM)

Attack logs:



Excessive user account deletions

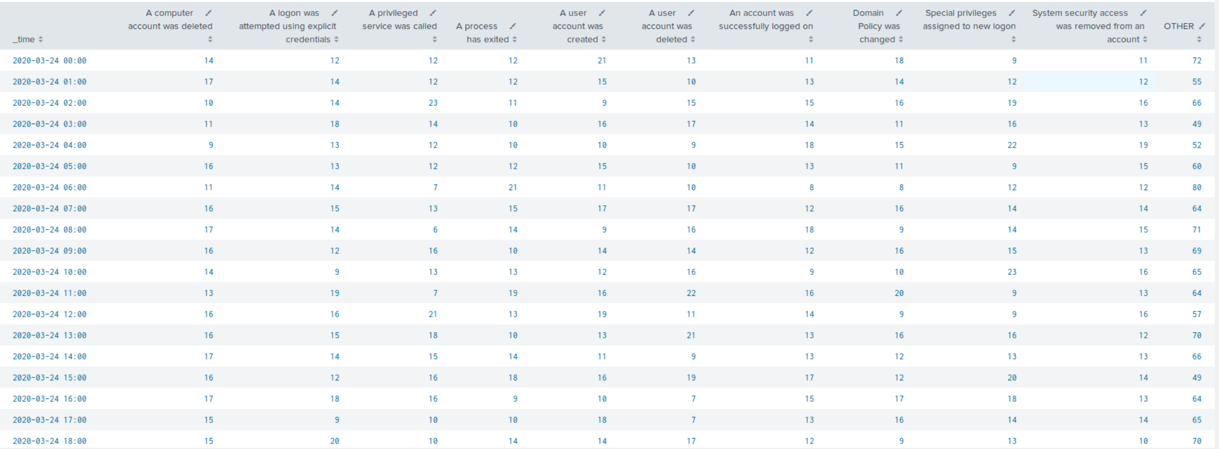
```
source="windows_server_attack_logs.csv"  signature_id=4726 | timechart count span=60m
```

✓ **131 events** (before 11/21/22 5:09:20.000 PM)

Dashboard Analysis for Time Chart of Signatures

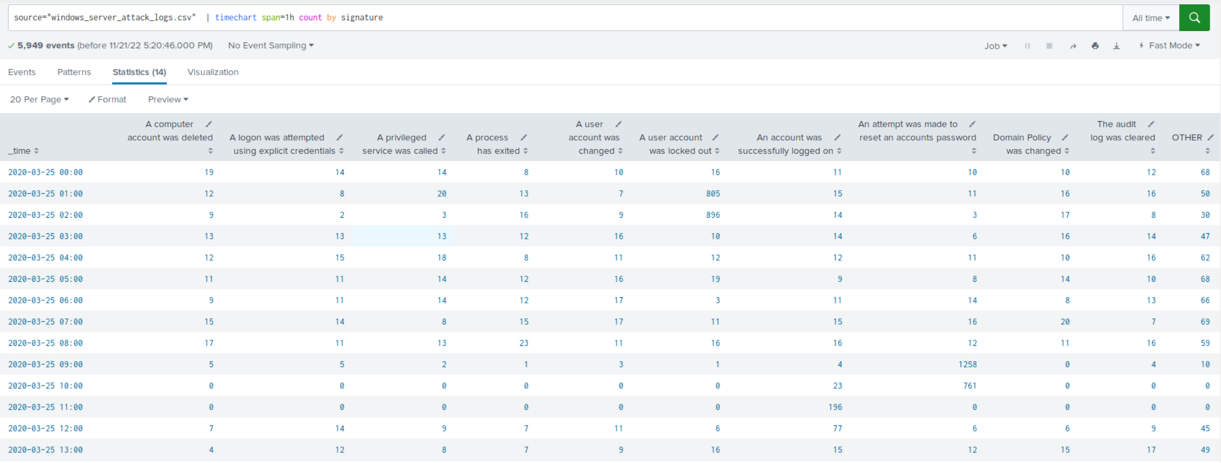
- Does anything stand out as suspicious?

In the time chart signatures for the attack logs there are events that stand out from the regular Windows activity logs.
Normal Activity Logs:



_time	A computer account was deleted	A logon was attempted using explicit credentials	A privileged service was called	A process has exited	A user account was created	A user account was deleted	An account was successfully logged on	Domain Policy was changed	Special privileges assigned to new logon	System security access was removed from an account	OTHER
2020-03-24 00:00	14	12	12	12	21	13	11	18	9	11	72
2020-03-24 01:00	17	14	12	12	15	10	13	14	12	12	55
2020-03-24 02:00	10	14	23	11	9	15	15	16	19	16	66
2020-03-24 03:00	11	18	14	10	16	17	14	11	16	13	49
2020-03-24 04:00	9	13	12	10	10	9	18	15	22	19	52
2020-03-24 05:00	16	13	12	12	15	10	13	11	9	15	60
2020-03-24 06:00	11	14	7	21	11	10	8	8	12	12	80
2020-03-24 07:00	16	15	13	15	17	17	12	16	14	14	64
2020-03-24 08:00	17	14	6	14	9	16	18	9	14	15	71
2020-03-24 09:00	16	12	16	10	14	14	12	16	15	13	69
2020-03-24 10:00	14	9	13	13	12	16	9	10	23	16	65
2020-03-24 11:00	13	19	7	19	16	22	16	20	9	13	64
2020-03-24 12:00	16	16	21	13	19	11	14	9	9	16	57
2020-03-24 13:00	16	15	18	10	13	21	13	16	16	12	70
2020-03-24 14:00	17	14	15	14	11	9	13	12	13	13	66
2020-03-24 15:00	16	12	16	18	16	19	17	12	20	14	49
2020-03-24 16:00	17	18	16	9	10	7	15	17	18	13	64
2020-03-24 17:00	15	9	10	10	18	7	13	16	14	14	65
2020-03-24 18:00	15	20	10	14	14	17	12	9	13	10	70

Attack logs:



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

_time	A computer account was deleted	A logon was attempted using explicit credentials	A privileged service was called	A process has exited	A user account was changed	A user account was locked out	An account was successfully logged on	An attempt was made to reset an accounts password	Domain Policy was changed	The audit log was cleared	OTHER
2020-03-25 00:00	19	14	14	8	10	16	11	10	10	12	68
2020-03-25 01:00	12	8	20	13	7	805	15	11	16	16	50
2020-03-25 02:00	9	2	3	16	9	896	14	3	17	8	30
2020-03-25 03:00	13	13	13	12	16	10	14	6	16	14	47
2020-03-25 04:00	12	15	18	8	11	12	12	11	10	16	62
2020-03-25 05:00	11	11	14	12	16	19	9	8	14	10	68
2020-03-25 06:00	9	11	14	12	17	3	11	14	8	13	66
2020-03-25 07:00	15	14	8	15	17	11	15	16	20	7	69
2020-03-25 08:00	17	11	13	23	11	16	16	12	11	16	59
2020-03-25 09:00	5	5	2	1	3	1	4	1258	0	4	10
2020-03-25 10:00	0	0	0	0	0	0	23	761	0	0	0
2020-03-25 11:00	0	0	0	0	0	0	196	0	0	0	0
2020-03-25 12:00	7	14	9	7	11	6	77	6	6	9	45
2020-03-25 13:00	4	12	8	7	9	16	15	12	15	17	49

- What signatures stand out?

In the Windows Events by Signature Time Chart there are two events that have significant increases in activity:

1. An attempt was made to reset an account password
2. A user account was locked out

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

An attempt was made to reset an account password occurred between 09:00 AM and 10:00 AM
A user account was locked out occurred between 01:00 AM and 02:30 AM

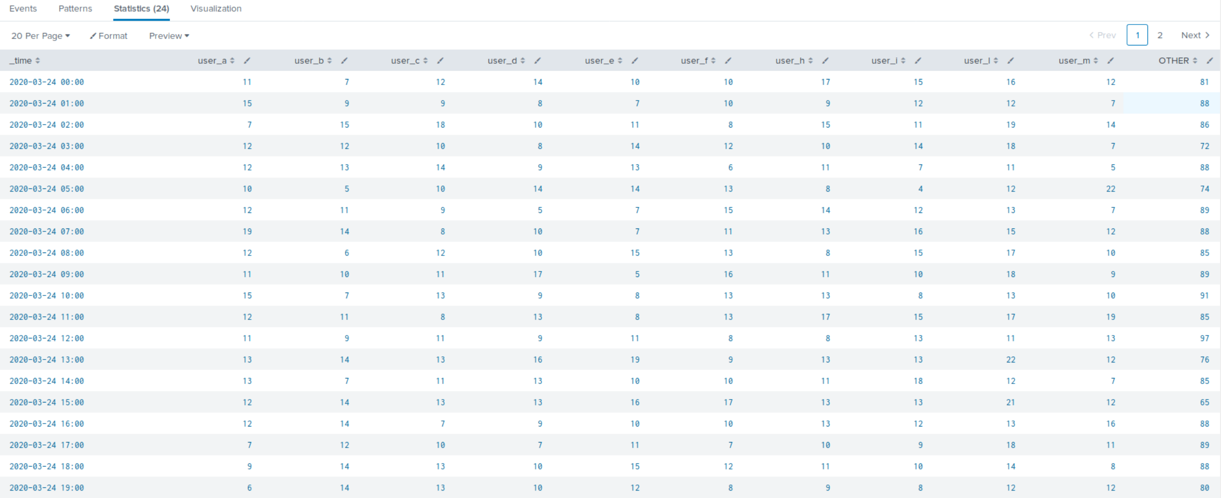
- What is the peak count of the different signatures?

```
Account locked out peaked at 896
Attempt to reset password peaked at 1268
```

Dashboard Analysis for Users

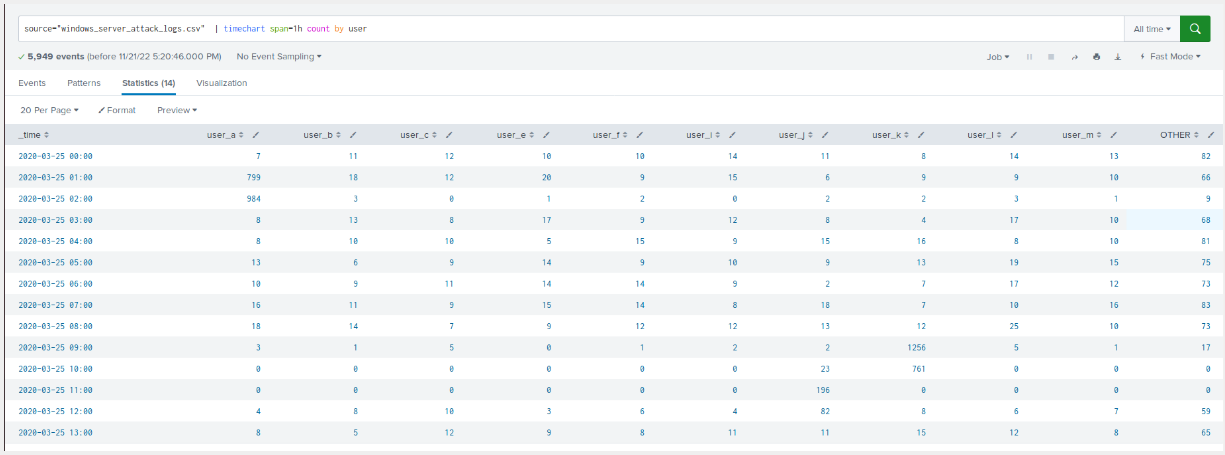
- Does anything stand out as suspicious?

```
Yes there is significant increases in the amount of user activity for two
users that is shown in the Users by Hour Time Chart
Normal Activity Logs:
```



_time	user_a	user_b	user_c	user_d	user_e	user_f	user_h	user_i	user_l	user_m	OTHER
2020-03-24 00:00	11	7	12	14	10	10	17	15	16	12	81
2020-03-24 01:00	15	9	9	8	7	10	9	12	12	7	88
2020-03-24 02:00	7	15	18	10	11	8	15	11	19	14	86
2020-03-24 03:00	12	12	10	8	14	12	10	14	18	7	72
2020-03-24 04:00	12	13	14	9	13	6	11	7	11	5	88
2020-03-24 05:00	10	5	10	14	14	13	8	4	12	22	74
2020-03-24 06:00	12	11	9	5	7	15	14	12	13	7	89
2020-03-24 07:00	19	14	8	10	7	11	13	16	15	12	88
2020-03-24 08:00	12	6	12	10	15	13	8	15	17	10	85
2020-03-24 09:00	11	10	11	17	5	16	11	10	18	9	89
2020-03-24 10:00	15	7	13	9	8	13	13	8	13	10	91
2020-03-24 11:00	12	11	8	13	8	13	17	15	17	19	85
2020-03-24 12:00	11	9	11	9	11	8	8	13	11	13	97
2020-03-24 13:00	13	14	13	16	19	9	13	13	22	12	76
2020-03-24 14:00	13	7	11	13	10	10	11	18	12	7	85
2020-03-24 15:00	12	14	13	13	16	17	13	13	21	12	65
2020-03-24 16:00	12	14	7	9	10	10	13	12	13	16	88
2020-03-24 17:00	7	12	10	7	11	7	10	9	18	11	89
2020-03-24 18:00	9	14	13	10	15	12	11	10	14	8	88
2020-03-24 19:00	6	14	13	10	12	8	9	8	12	12	80

```
Attack Logs:
```



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

✓ 5,949 events (before 11/21/22 5:20:46.000 PM) No Event Sampling

_time	user_a	user_b	user_c	user_e	user_f	user_i	user_j	user_k	user_l	user_m	OTHER
2020-03-25 00:00	7	11	12	10	10	14	11	8	14	13	82
2020-03-25 01:00	799	18	12	20	9	15	6	9	9	10	66
2020-03-25 02:00	984	3	0	1	2	0	2	2	3	1	9
2020-03-25 03:00	8	13	8	17	9	12	8	4	17	10	68
2020-03-25 04:00	8	10	10	5	15	9	15	16	8	10	81
2020-03-25 05:00	13	6	9	14	9	10	9	13	19	15	75
2020-03-25 06:00	10	9	11	14	14	9	2	7	17	12	73
2020-03-25 07:00	16	11	9	15	14	8	18	7	10	16	83
2020-03-25 08:00	18	14	7	9	12	12	13	12	25	10	73
2020-03-25 09:00	3	1	5	0	1	2	2	1256	5	1	17
2020-03-25 10:00	0	0	0	0	0	0	23	761	0	0	0
2020-03-25 11:00	0	0	0	0	0	0	196	0	0	0	0
2020-03-25 12:00	4	8	10	3	6	4	82	8	6	7	59
2020-03-25 13:00	8	5	12	9	8	11	11	15	12	8	65

- Which users stand out?

```
In the Users by Hour Visualization there are two users who have significant
increases in activity:
   1. User_a
   2. User_k
```

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

```
User_a had increased activity occur between 01:00 AM and 02:30 AM
User_k had increased activity occur between 09:00 AM and 10:00 AM
```

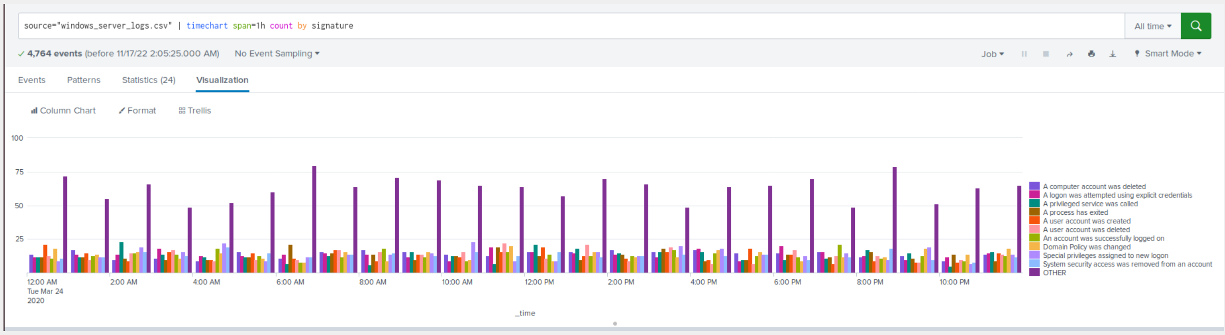
- What is the peak count of the different users?

```
User_a peaked at 984
User_k peaked at 1256
```

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

- Does anything stand out as suspicious?

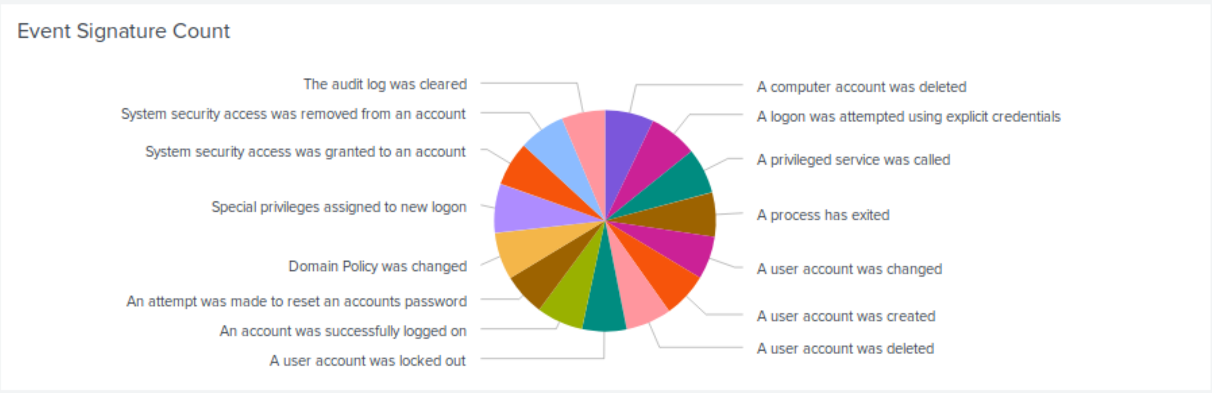
```
Yes there is a significant increase in two signature types: An attempt was
made to reset a account password and A user account was locked out
Normal Windows logs:
```



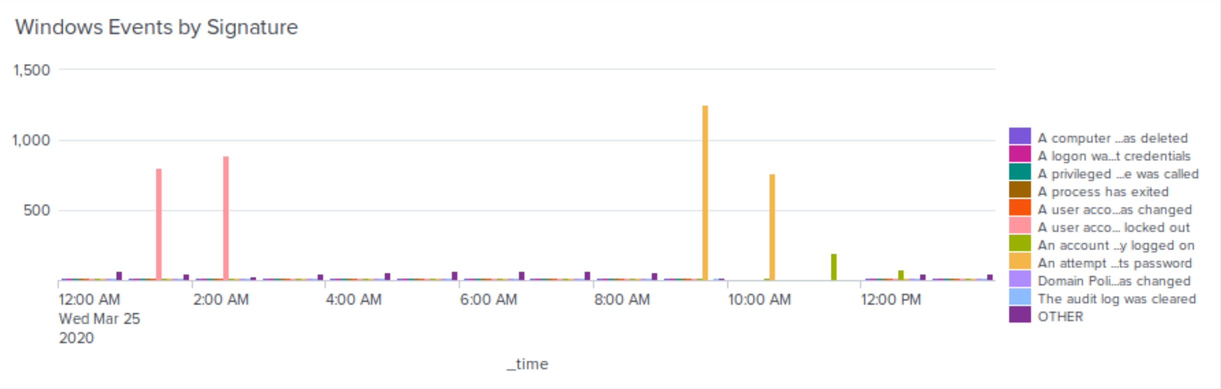
```
source="windows_server_logs.csv" | timechart span=1h count by signature
```

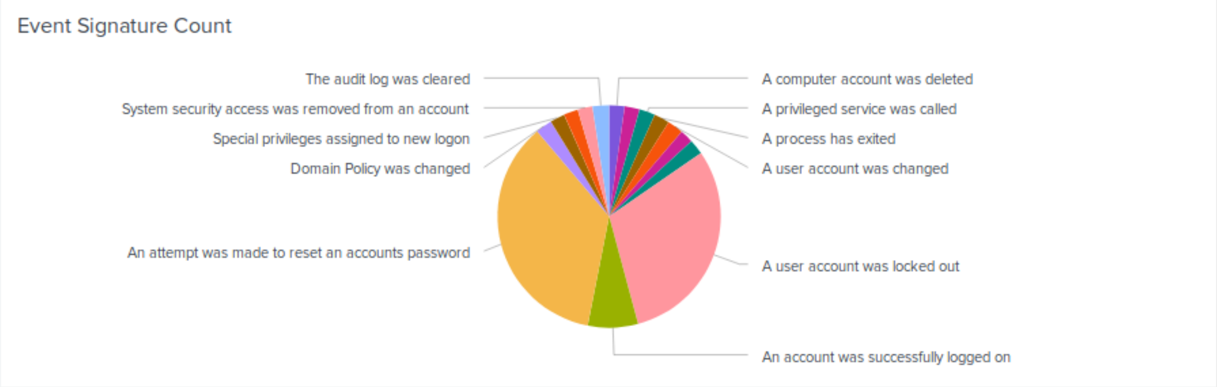
✓ 4,764 events (before 11/17/22 2:05:25.000 AM)

All time ▾
No Event Sampling ▾
Job ▾
Smart Mode ▾
Events
Patterns
Statistics (24)
Visualization
Column Chart
Format
Trellis
100
75
50
25
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 attempted using explicit credentials
A privileged service was called
A process has exited
A user account was created
A user account was deleted
An account was successfully logged on
Domain Policy was changed
Special privileges assigned to new logon
System security access was removed from an account
OTHER



Attack Logs:





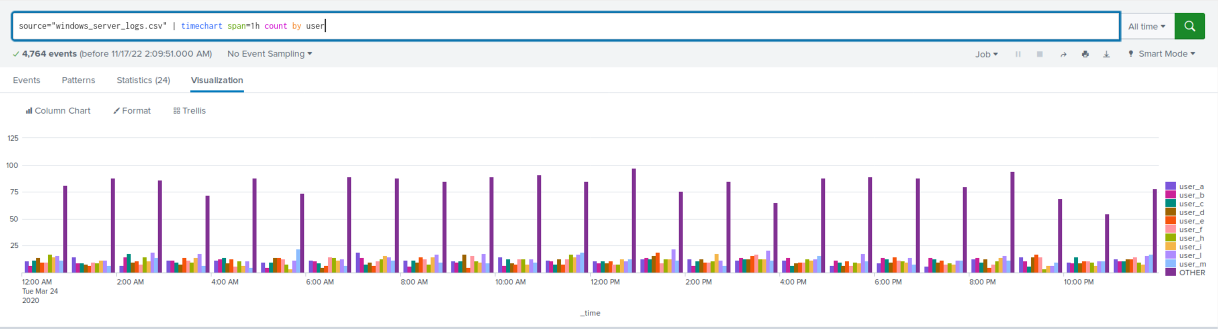
- Do the results match your findings in your time chart for signatures?

Yes they do match

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

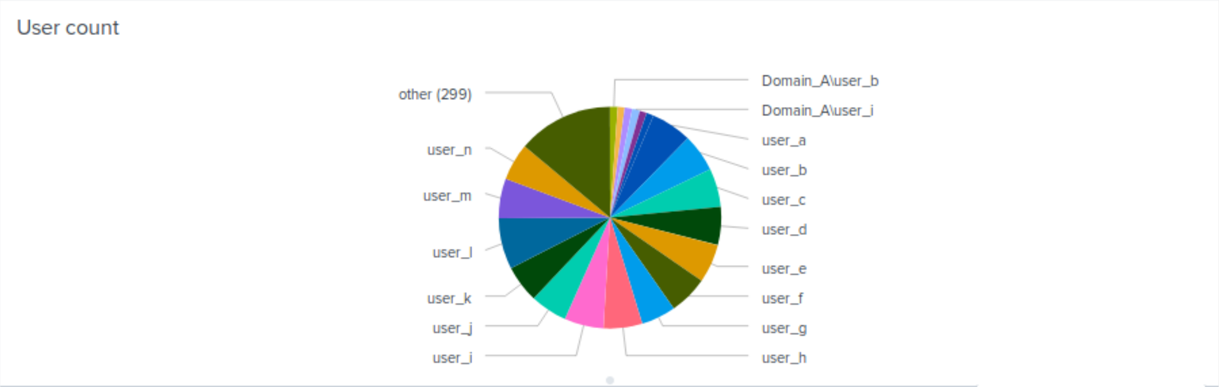
- Does anything stand out as suspicious?

Yes, there is increased activity from user_a and user_k

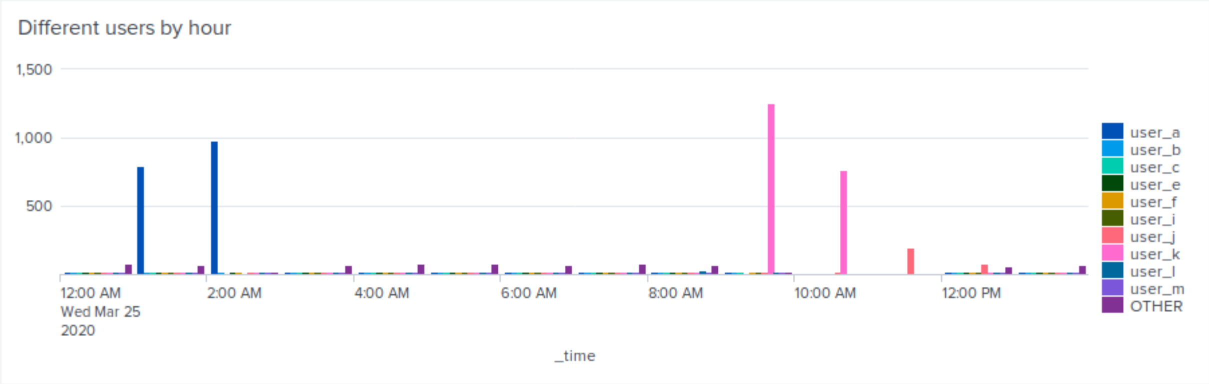


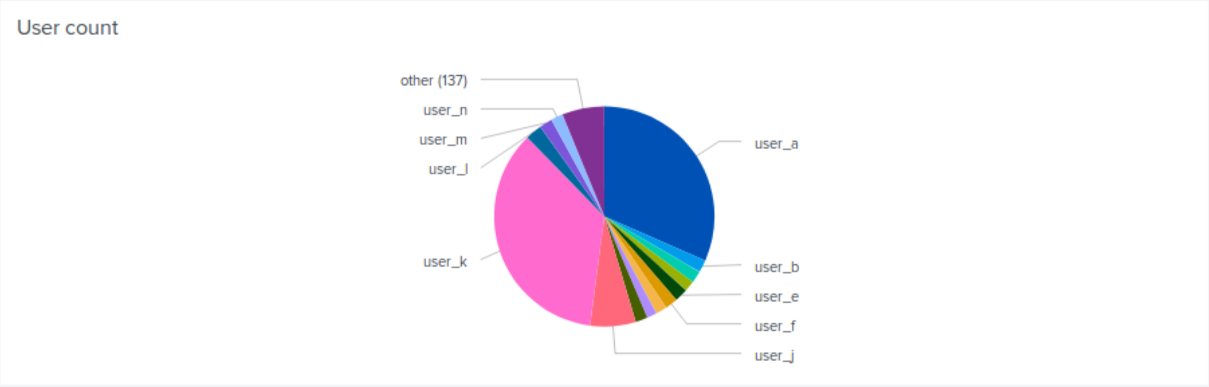
```
source="windows_server_logs.csv" | timechart span=1h count by user
```

✓ 4,764 events (before 11/17/22 2:09:51.000 AM) No Event Sampling ▾



Attack Logs:





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

Yes

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?

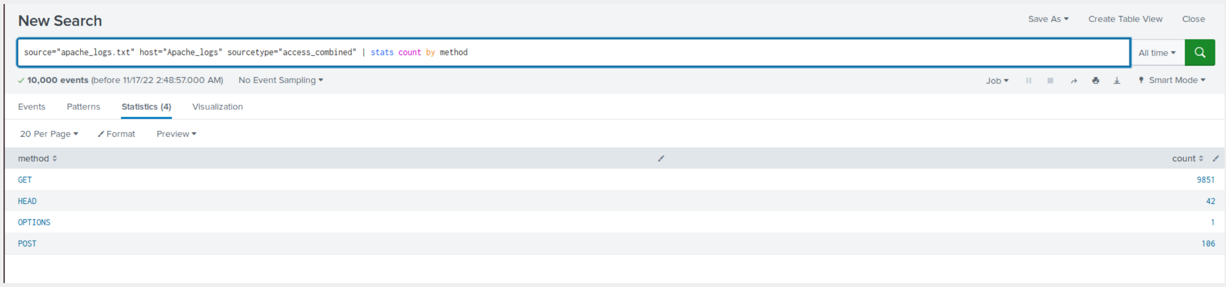
An advantage of using the statistical time charts for signatures and users is that you can quickly find the count for each event or for the user per hour. A disadvantage of using these over the bar graph and pie chart is that it isn’t obvious when there was a change in activity. The visualizations quickly show you where there are spikes or declines in an event and what time. The pie chart quickly shows you which event or user has an increase in activity.

Apache Web Server Log Questions

Report Analysis for Methods

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

Yes we did detect suspicious changes in HTTP methods, specifically with POST.
Normal Apache Logs:

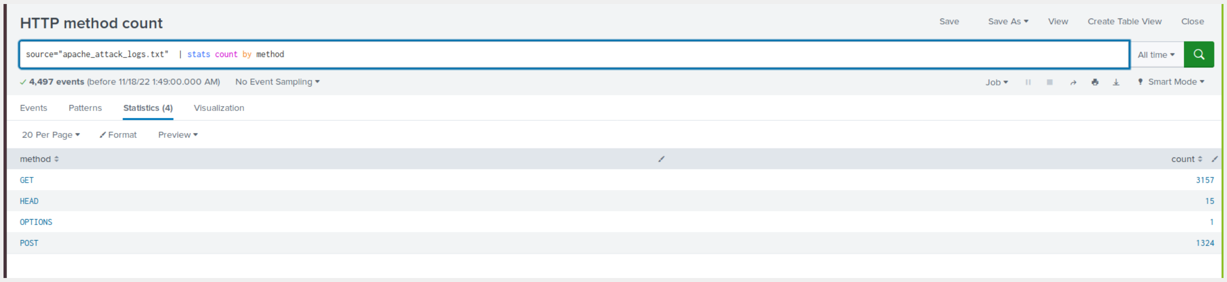


```
source="apache_logs.txt" host="Apache_logs" sourcetype="access_combined" | stats count by method
```

✓ 10,000 events (before 11/17/22 2:48:57.000 AM) No Event Sampling ▾

method	count
GET	9851
HEAD	42
OPTIONS	1
POST	106

Attack Logs:



```
source="apache_attack_logs.txt"  | stats count by method
```

✓ 4,497 events (before 11/18/22 1:49:00.000 AM) No Event Sampling ▾

method	count
GET	3157
HEAD	15
OPTIONS	1
POST	1324

- What is that method used for?

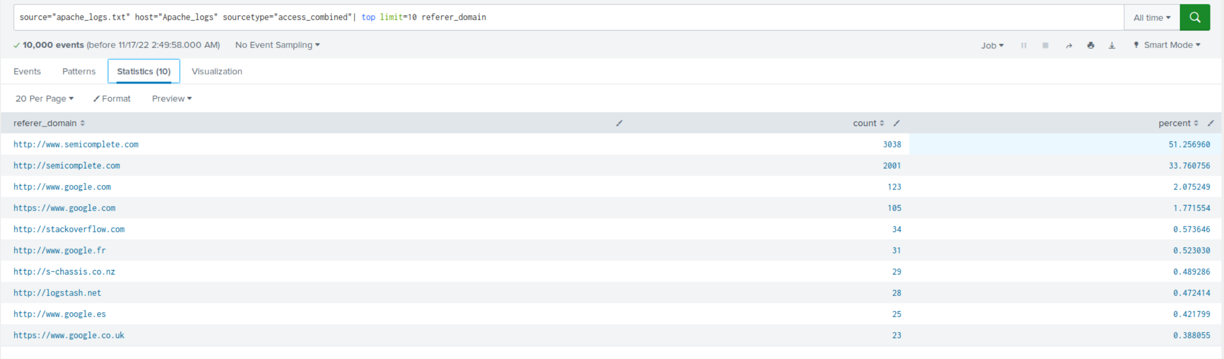
```
POST: used to send data to the server from the HTTP client
```

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

We did see some changes in the results of the top 10 referrer domains, specifically with the last 5 of the list.

Normal Apache Logs:

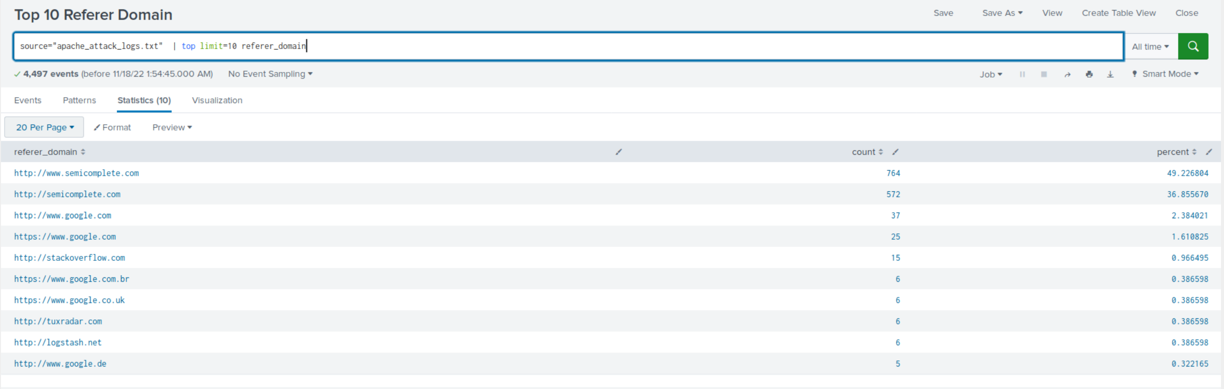


```
source="apache_logs.txt" host="Apache_logs" sourcetype="access_combined"| top limit=10 referer_domain
```

✓ 10,000 events (before 11/17/22 2:49:58.000 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 Logs:



```
source="apache_attack_logs.txt"  | top limit=10 referer_domain
```

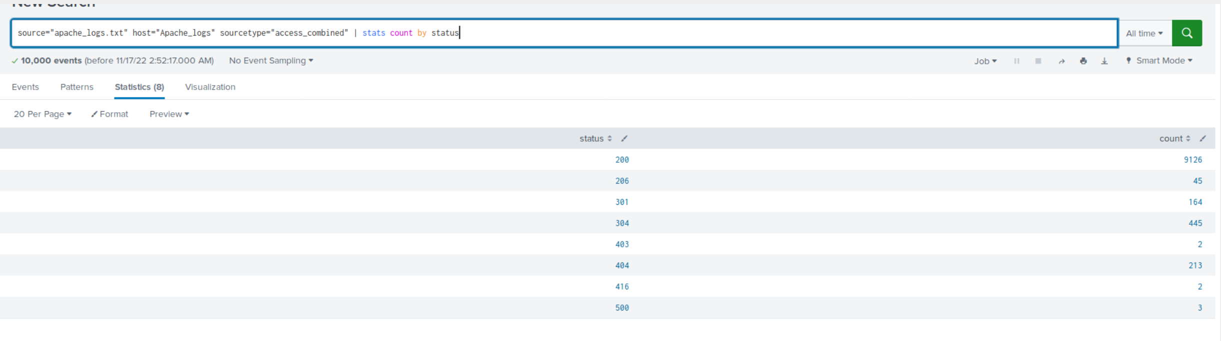
✓ 4,497 events (before 11/18/22 1:54:45.000 AM) No Event Sampling ▾

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?

```
We did detect a suspicious change in HTTP response codes, specifically with
response code 200 and 404.  Response code 200 saw a decrease in amount and
404 saw an increase.
Normal Apache Logs:
```

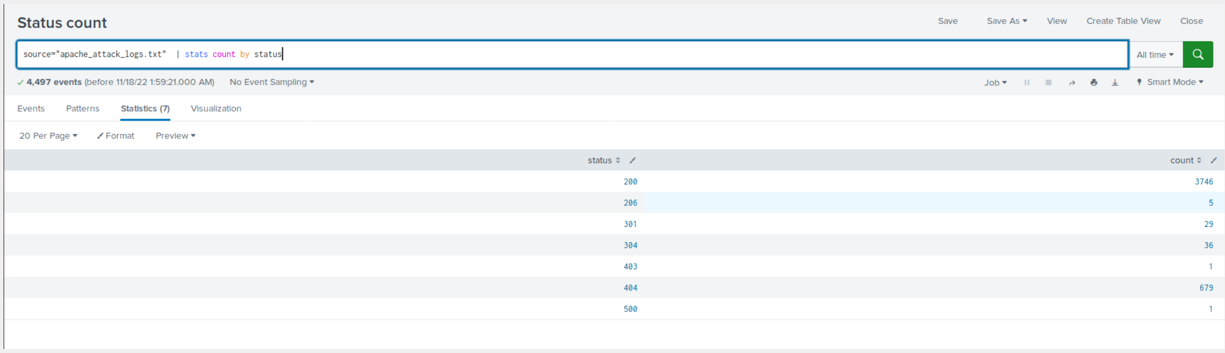


```
source="apache_logs.txt" host="Apache_logs" sourcetype="access_combined" | stats count by status
```

✓ 10,000 events (before 11/17/22 2:52:17.000 AM)

status	count
200	9126
206	45
301	164
304	445
403	2
404	213
416	2
500	3

```
Attack Logs:
```



Status count

```
source="apache_attack_logs.txt"  | stats count by status
```

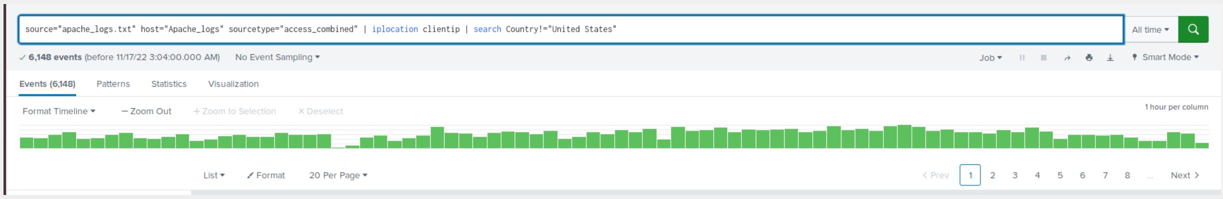
✓ 4,497 events (before 11/18/22 1:59:21.000 AM)

status	count
200	3746
206	5
301	29
304	36
403	1
404	679
500	1

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

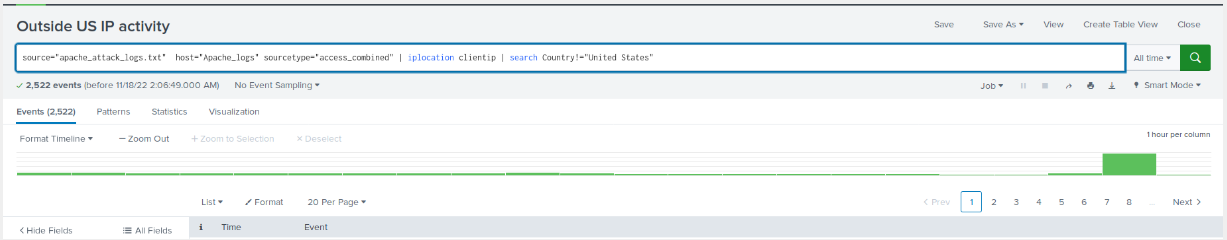
```
Yes we did detect a suspicious volume of international activity
Normal Apache Logs:
```



```
source="apache_logs.txt" host="Apache_logs" sourcetype="access_combined" | iplocation clientip | search Country!="United States"
```

✓ 6,148 events (before 11/17/22 3:04:00.000 AM)

```
Attack Logs:
```



Outside US IP activity

```
source="apache_attack_logs.txt"  host="Apache_logs" sourcetype="access_combined" | iplocation clientip | search Country!="United States"
```

✓ 2,522 events (before 11/18/22 2:06:49.000 AM)

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

The count was 939 at 08:00 PM

- Would your alert be triggered for this activity?

Yes our alert would have been triggered as we set the threshold to more than 150 in an hour to send an alert and this was well above that.

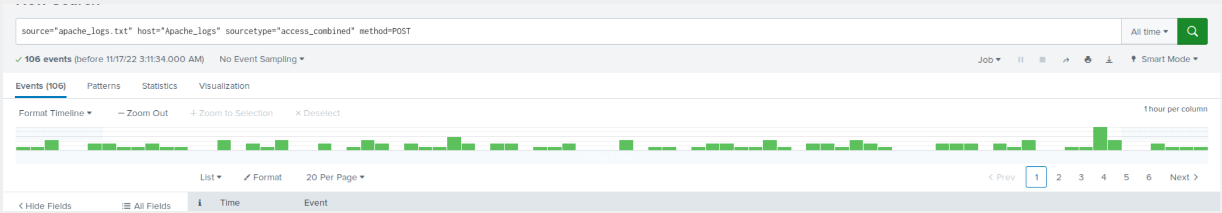
- After reviewing, would you change the threshold that you previously selected?

I would keep my threshold the same but continue monitoring the Apache logs to see if we could safely raise the threshold amount in the future.

Alert Analysis for HTTP POST Activity

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

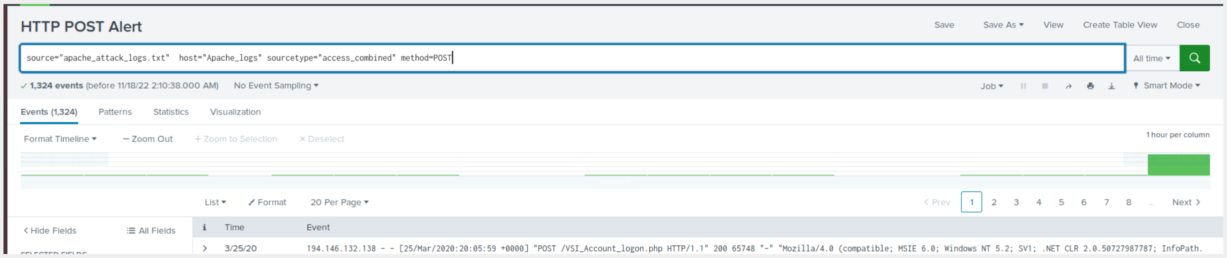
Yes we did detect a suspicious volume of HTTP POST activity.
Normal Apache Logs:



```
source="apache_logs.txt" host="Apache_logs" sourcetype="access_combined" method=POST
```

✓ 106 events (before 11/17/22 3:11:34.000 AM)

Attack Logs:


HTTP POST Alert

```
source="apache_attack_logs.txt"  host="Apache_logs" sourcetype="access_combined" method=POST
```

✓ 1,324 events (before 11/18/22 2:10:38.000 AM)

Events (1,324)

i	Time	Event
>	3/25/20	194.146.132.138 - - [25/Mar/2020:20:05:59 +0000] "POST /VSI_Account_logon.php HTTP/1.1" 200 65748 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.

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

The count was 1296 at 08:00 PM

- When did it occur?

8 pm Wednesday March 25, 2020

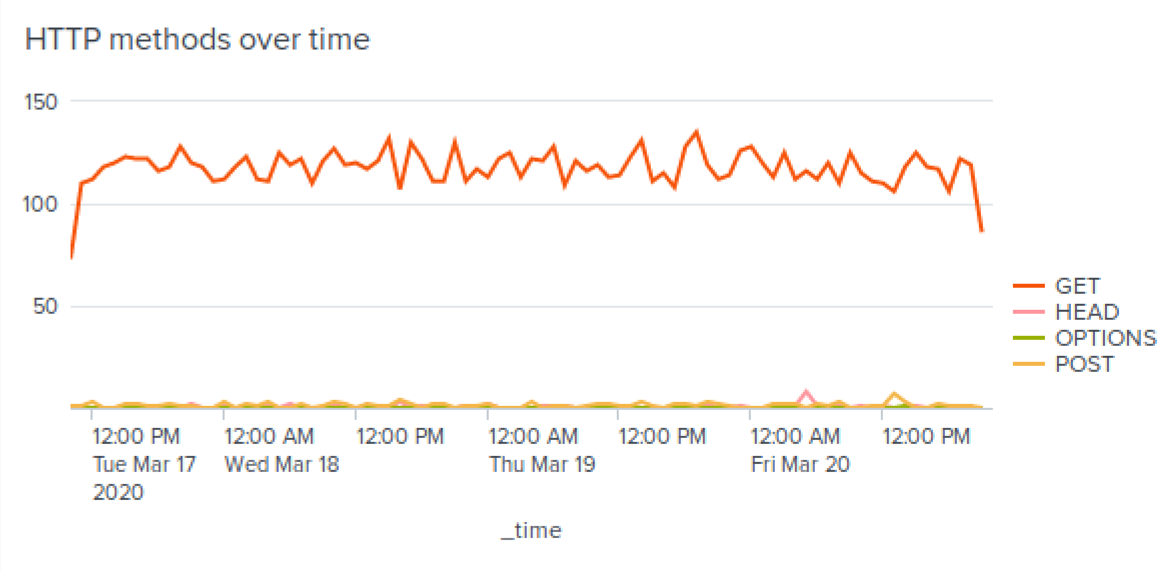
- After reviewing, would you change the threshold that you previously selected?

I would not initially change my threshold number, which was set at 15. I would conduct further analysis of the daily apache logs to determine if the number could be safely increased.

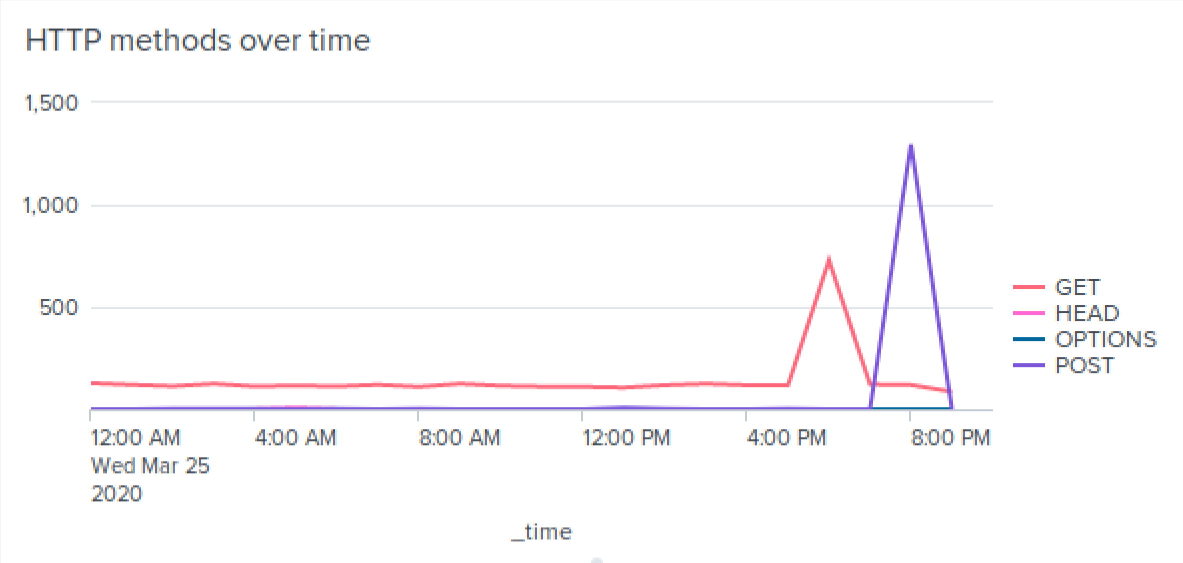
Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

Yes there is a significant difference in the HTTP method time charts.
Normal Apache Logs:



Attack Logs:



- Which method seems to be used in the attack?

POST

- At what times did the attack start and stop?

It appears to have occurred between 07:00 PM and 09:00 PM

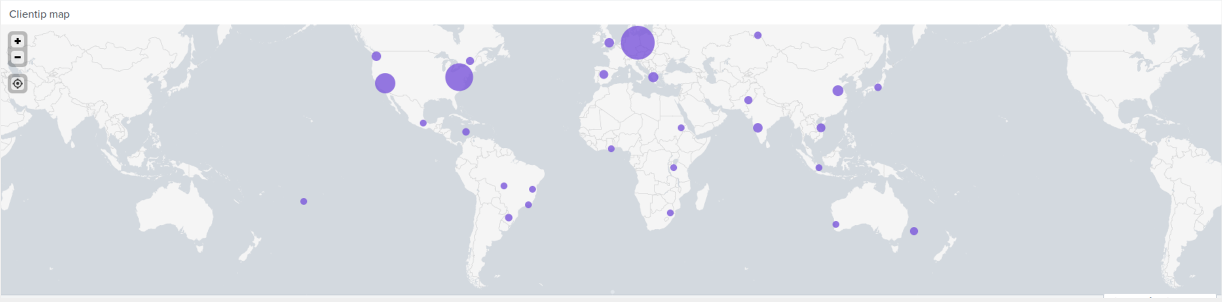
- What is the peak count of the top method during the attack?

```
1296
```

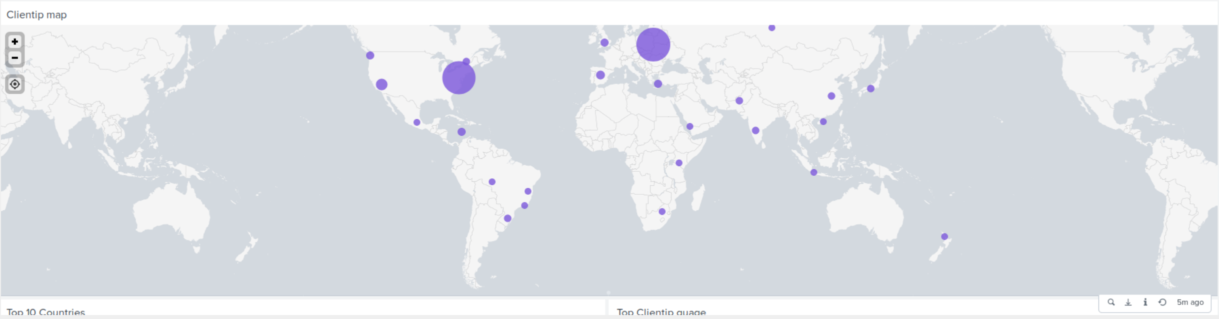
Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

```
Yes
Normal Apache Logs:
```

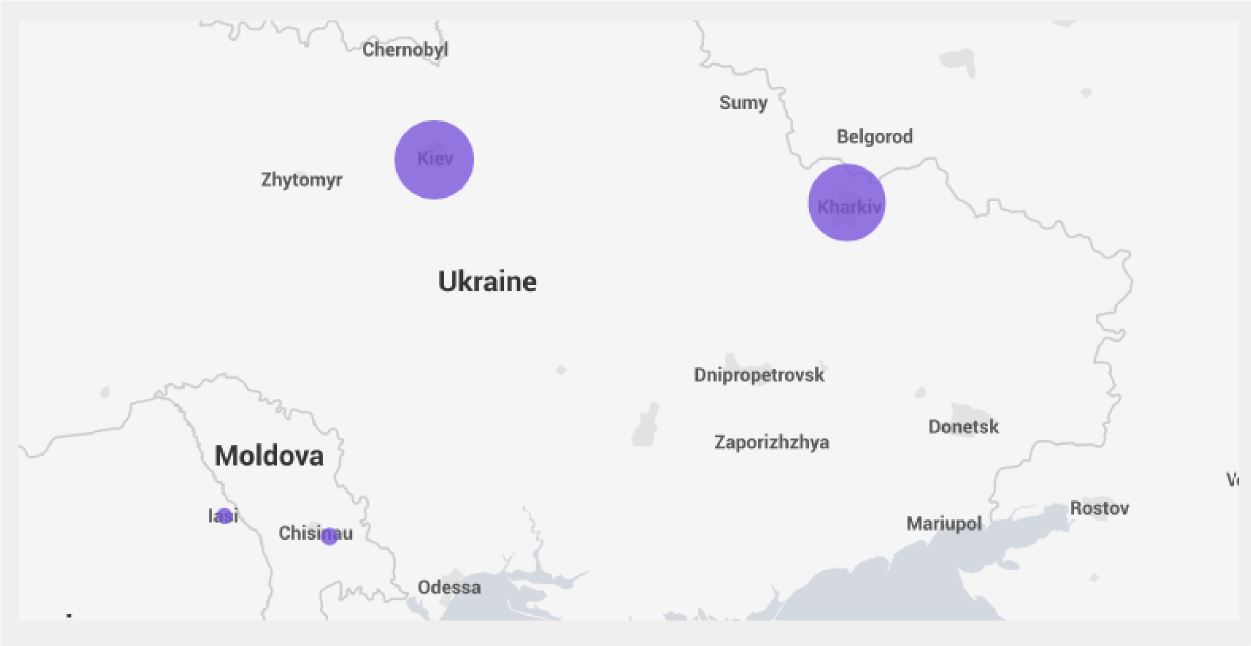


```
Attack Logs:
```



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

```
Kiev and Kharkiv in Ukraine both had an increase in activity
```



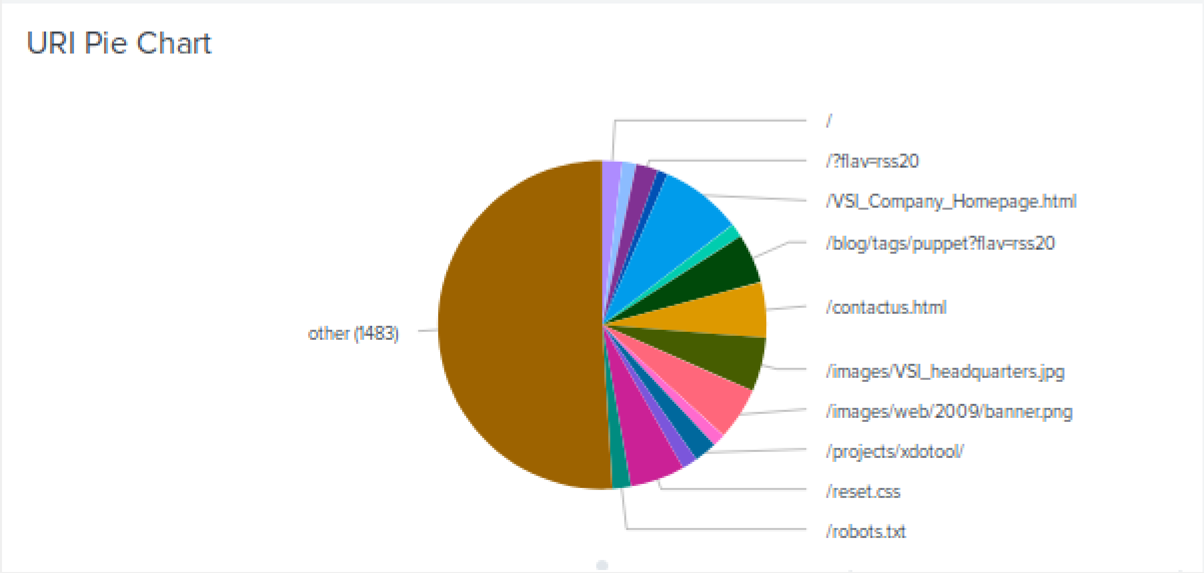
- What is the count of that city?

```
Kiev = 439
Kharkiv = 433
```

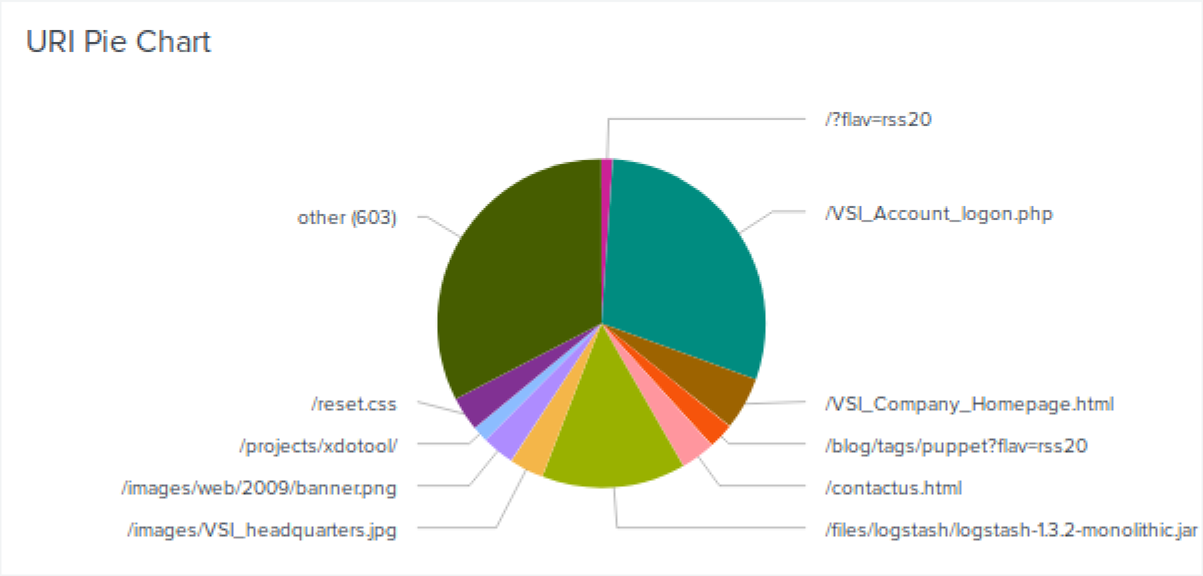
Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

```
Yes the URI Chart shows suspicious activity
Normal Apache Logs:
```



```
Attack Logs:
```



- What URI is hit the most?

```
Taking out ‘other’ as it is composed of many URIs too small to chart, the
URI hit the most is VSI_Account_logon.php
```

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

```
Based on the URI being accessed the attacker could potentially be trying a
brute force attack or an SQL injection.
Factoring in the large amounts of 404 errors would help us to better narrow
it down to an attacker scanning the network through a brute force attempt in
an effort to gain information through reconnaissance.
```