Cybersecurity

Dawa Sherpa Project 3 Review Questions

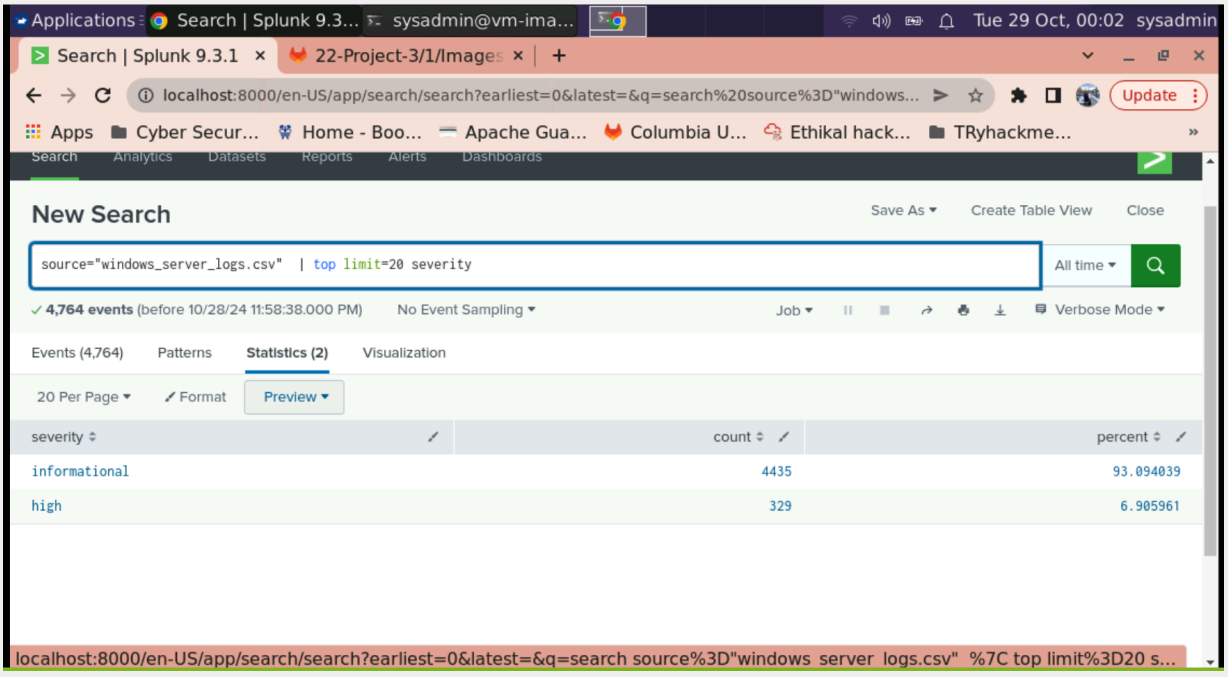
Make a copy of this document before you begin. Place your answers below each question.

Windows Server Log Questions

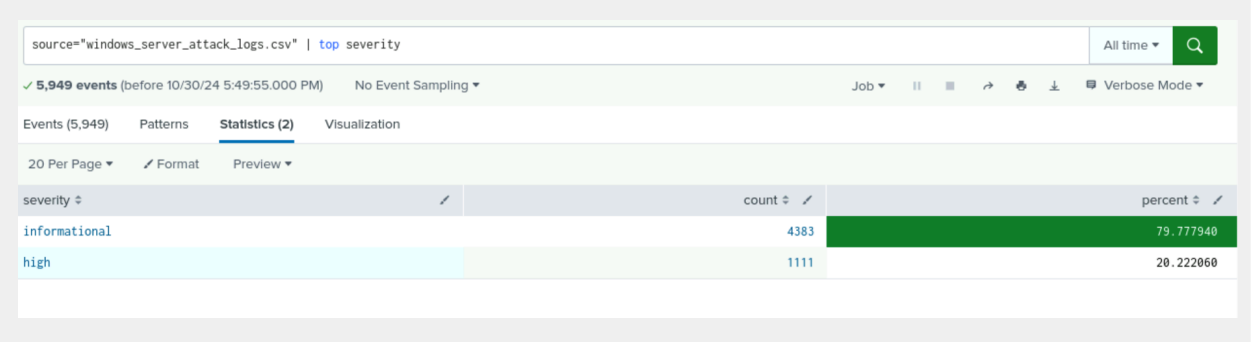
Report Analysis for Severity

- Did you detect any suspicious changes in severity?

Yes, my report did detect changes in severity. The bigger is for high severity events. It increased from 7% normal to 20% in attack logs
Regular Windows_logs:



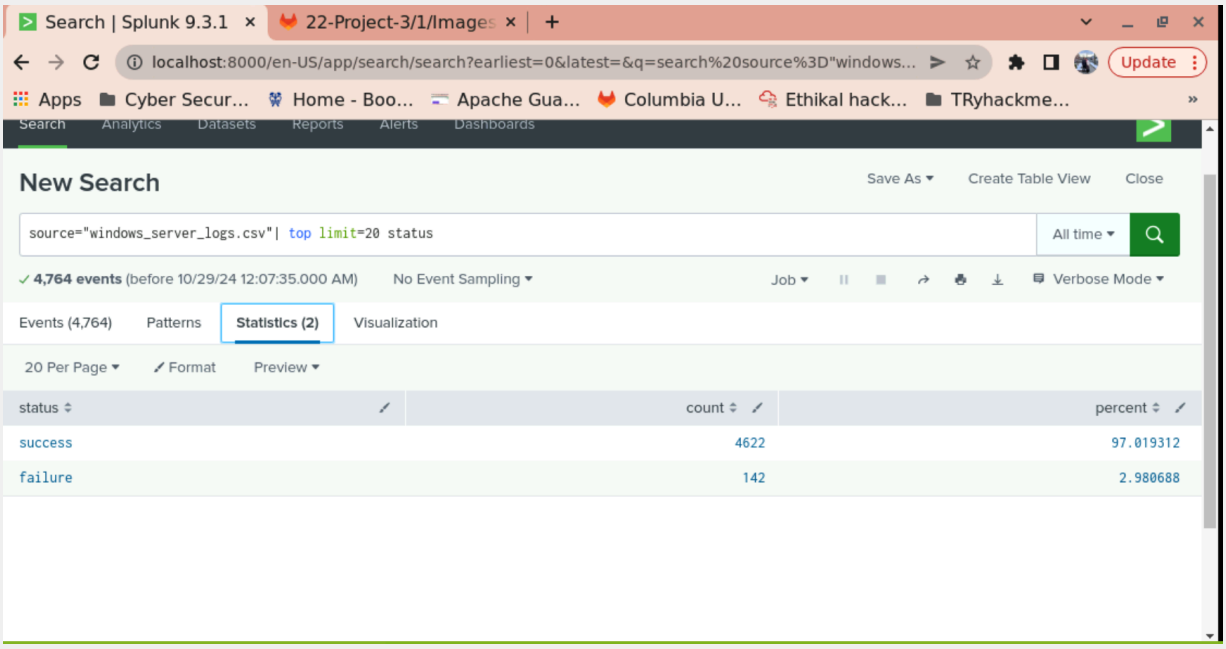
Windows_attack_logs:



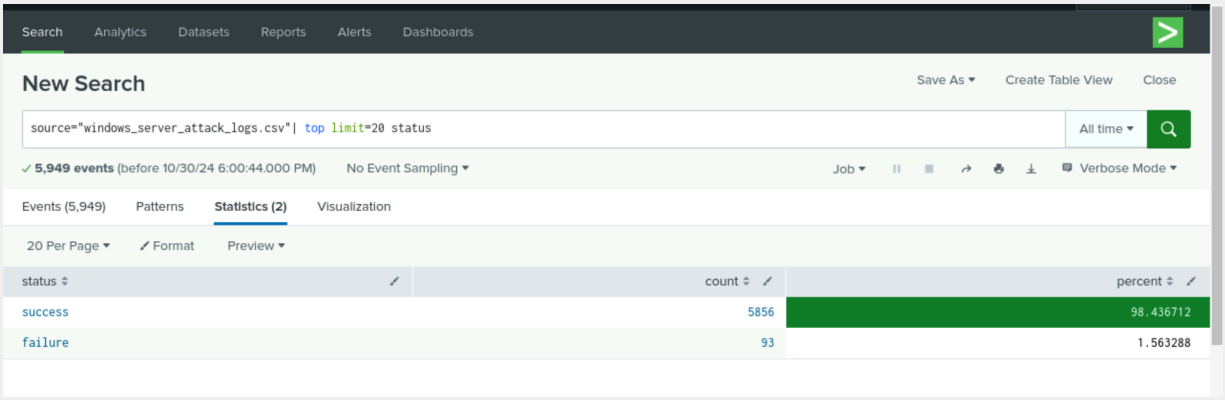
Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

Yes, I see changes in our report on the status activity between normal logs and attack logs. By our analysis we can see that number of successful activities increased and number of failed activities decreased
Regular windows_logs:



window_attack_logs:



Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

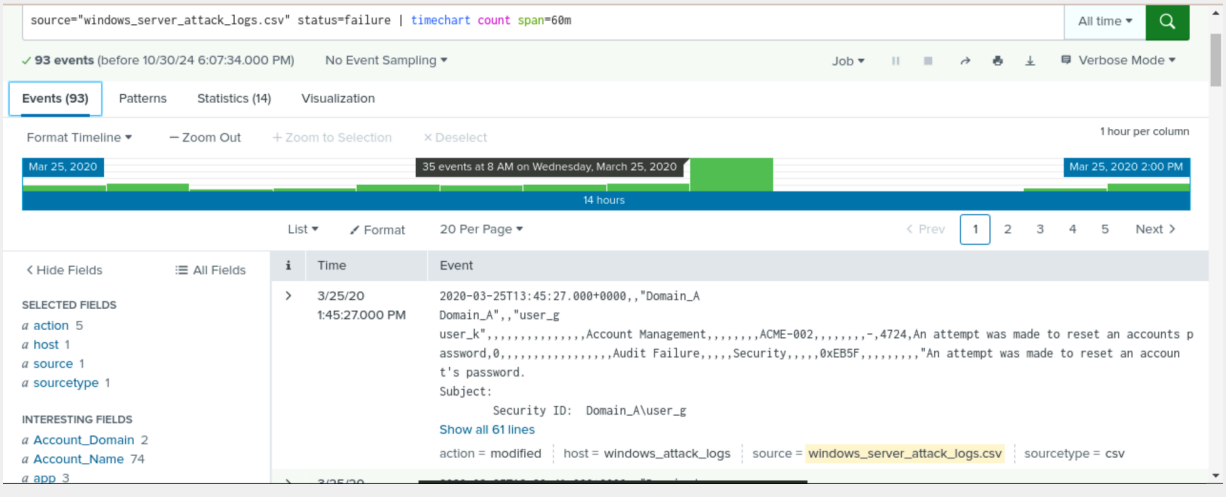
Yes, my alert did detect a suspicious volume of failed windows activity

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

There are 35 counts failed windows activities

- When did it occur?

It has occurred at 8:00 AM on /03/25/2020



- Would your alert be triggered for this activity?

```
Yes, my alert would have been triggered as we set our threshold 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 will not change my threshold as it is set low enough to be triggered by
this attack and high enough that I am not getting false positives during the
hours of attack resulting in alert fatigue.
```

Alert Analysis for Successful Logins

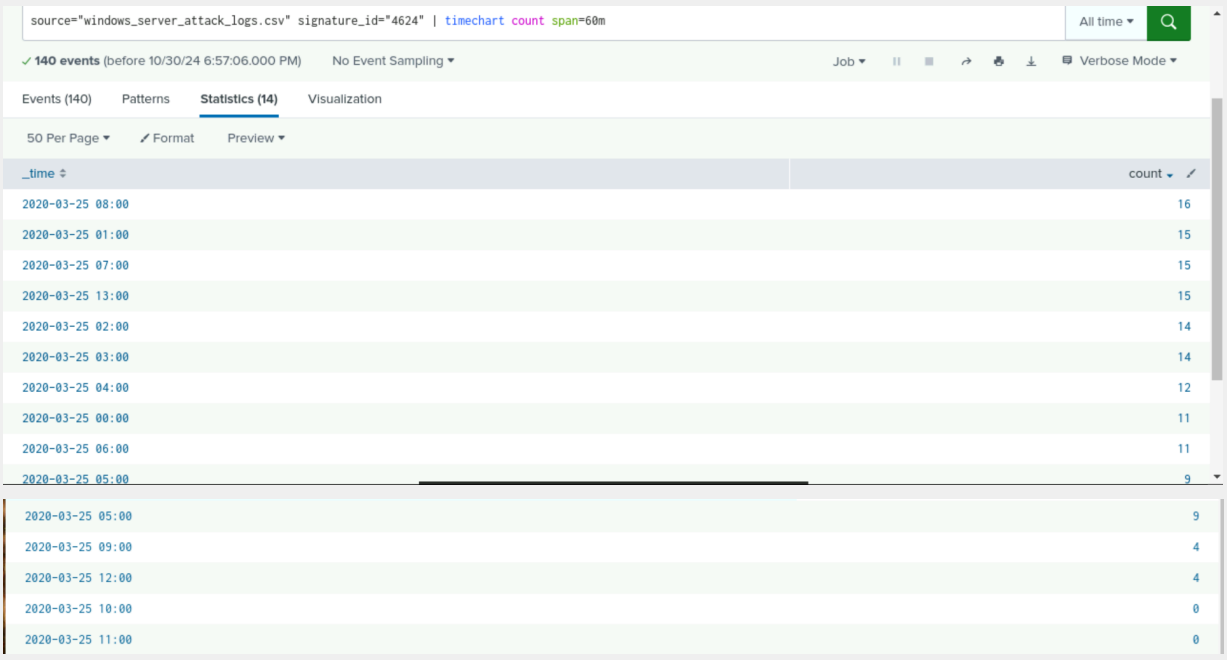
- Did you detect a suspicious volume of successful logins?

```
Yes, after review of logs there is a suspicious level of successful logins
Regular windows_logs:
```


```
windows_attack_logs:
```

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

At 8:00 AM there were 16 successful logins and the number drops to 4 logins at 9:00 AM and goes to 0 logins from 10:00 AM to 11:00 AM

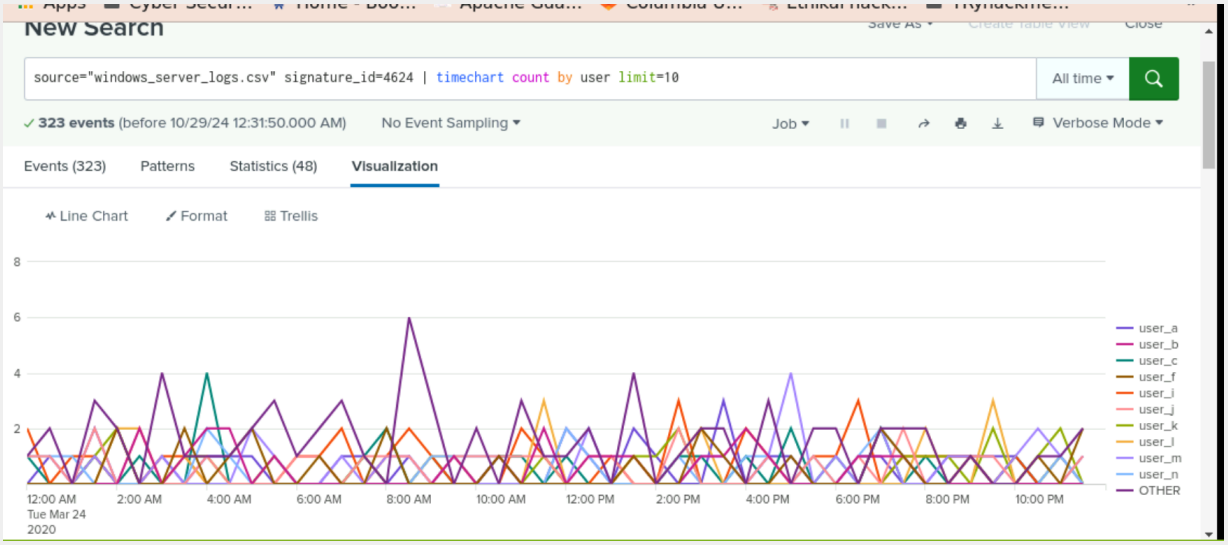


- Who is the primary user logging in?

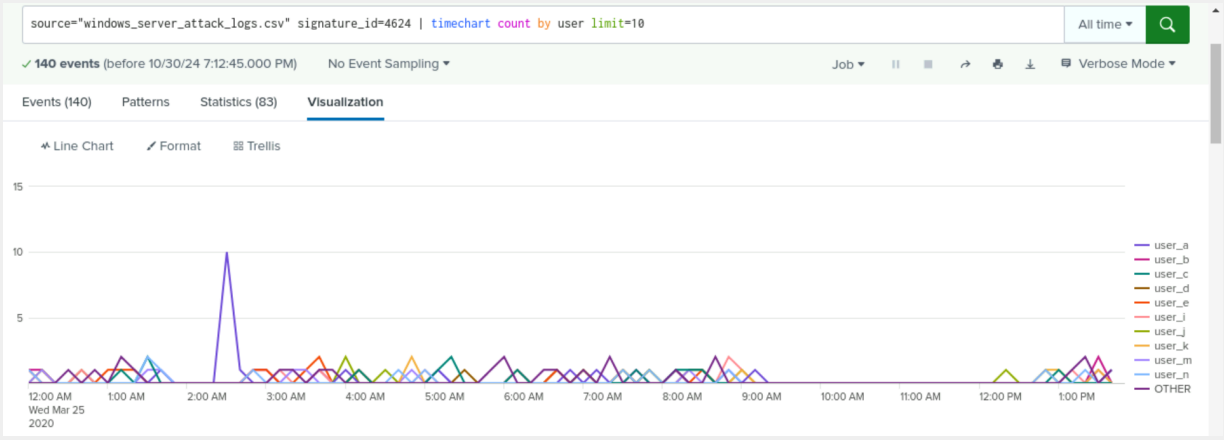
user_a

After analysis it appears that 2:30 AM user_a had a spike in logins for a total count of 10.

Regular windows_logs:



windows_attack_logs:



- When did it occur?

```
2:30 AM on 03-25-2020
```

- Would your alert be triggered for this activity?

```
No, my alert would not be triggered by this activity as I set my threshold count to 15 or more successful logins an hour to alert SOC.
```

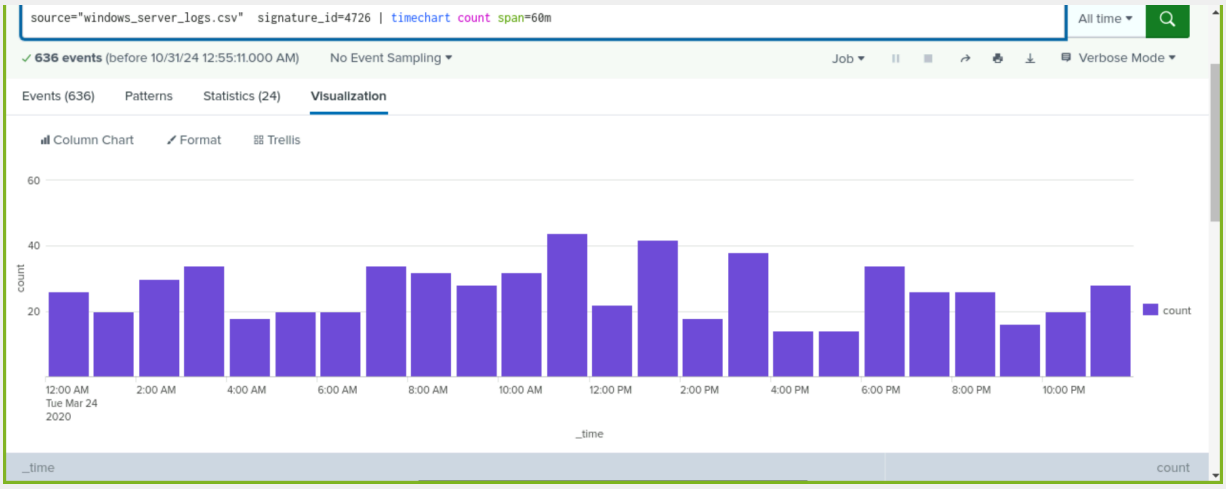
- After reviewing, would you change your threshold from what you previously selected?

```
Yes, I would change the threshold number slightly, up or down but i think i need more log data to be analyzed to make that change as we i want to avoid alert fatigue.
```

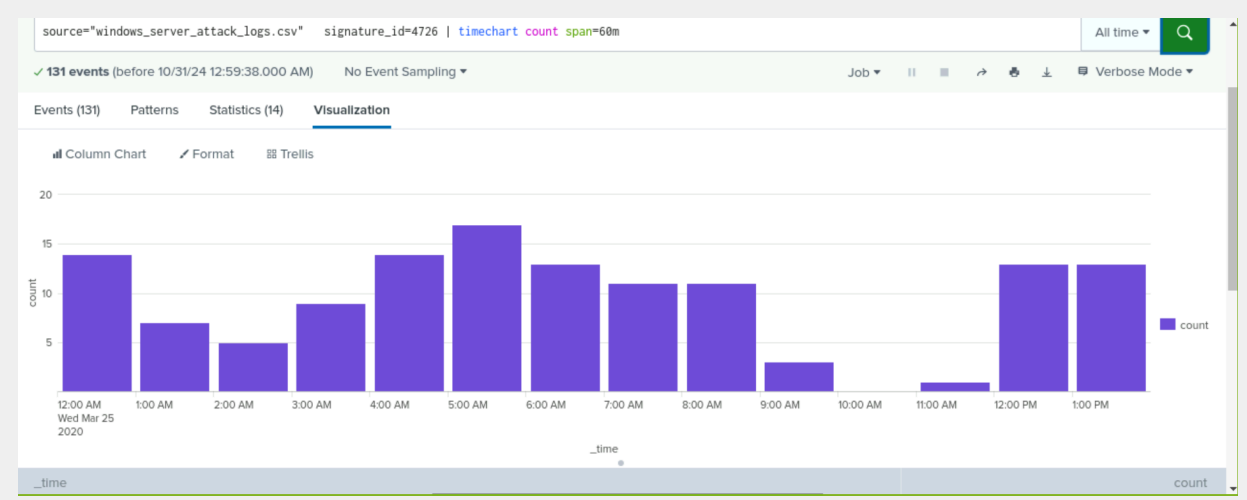
Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

```
Yes, i detect a suspicious amount to deleted accounts, but between the hours of 9:00 AM and 11:00 AM there was a significant drop in the number of deletions
Regular windows_logs:
```



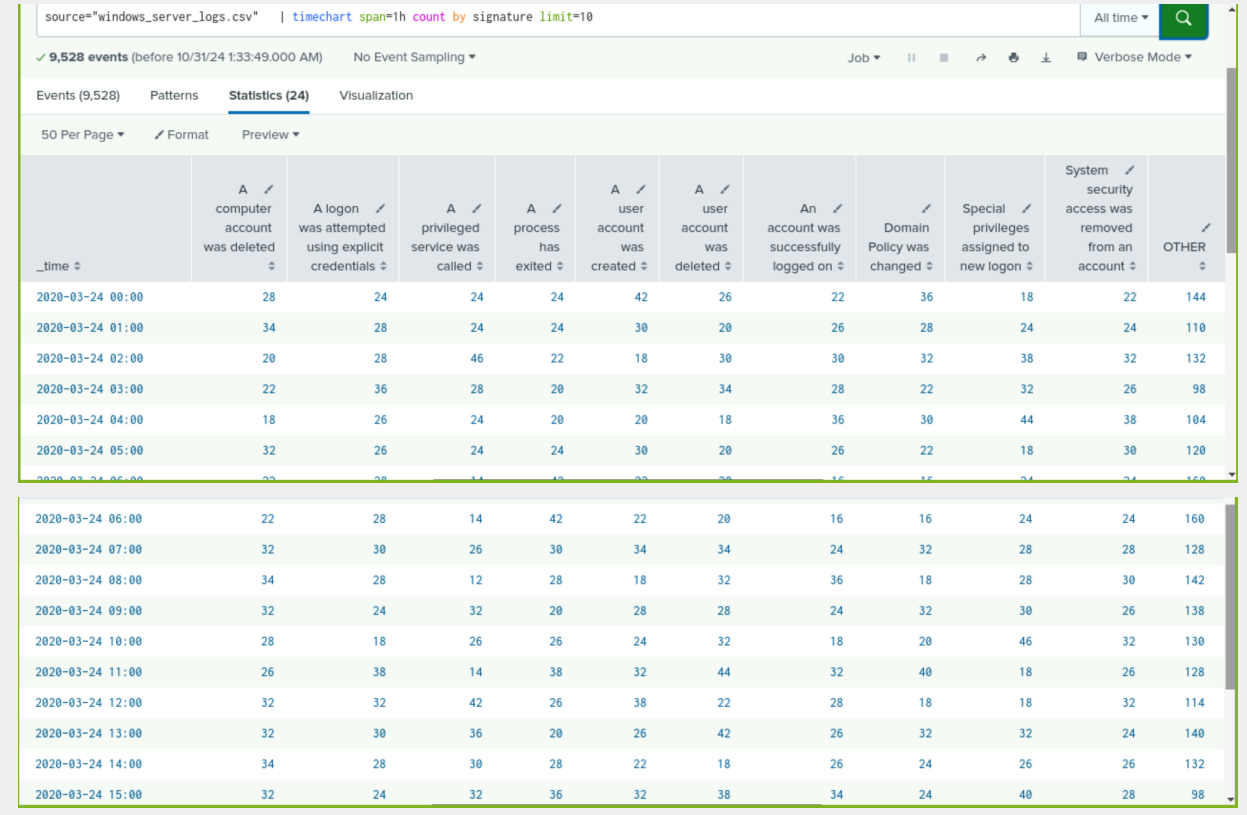

```
windows_attack_logs:
```



Dashboard Analysis for Time Chart of Signatures

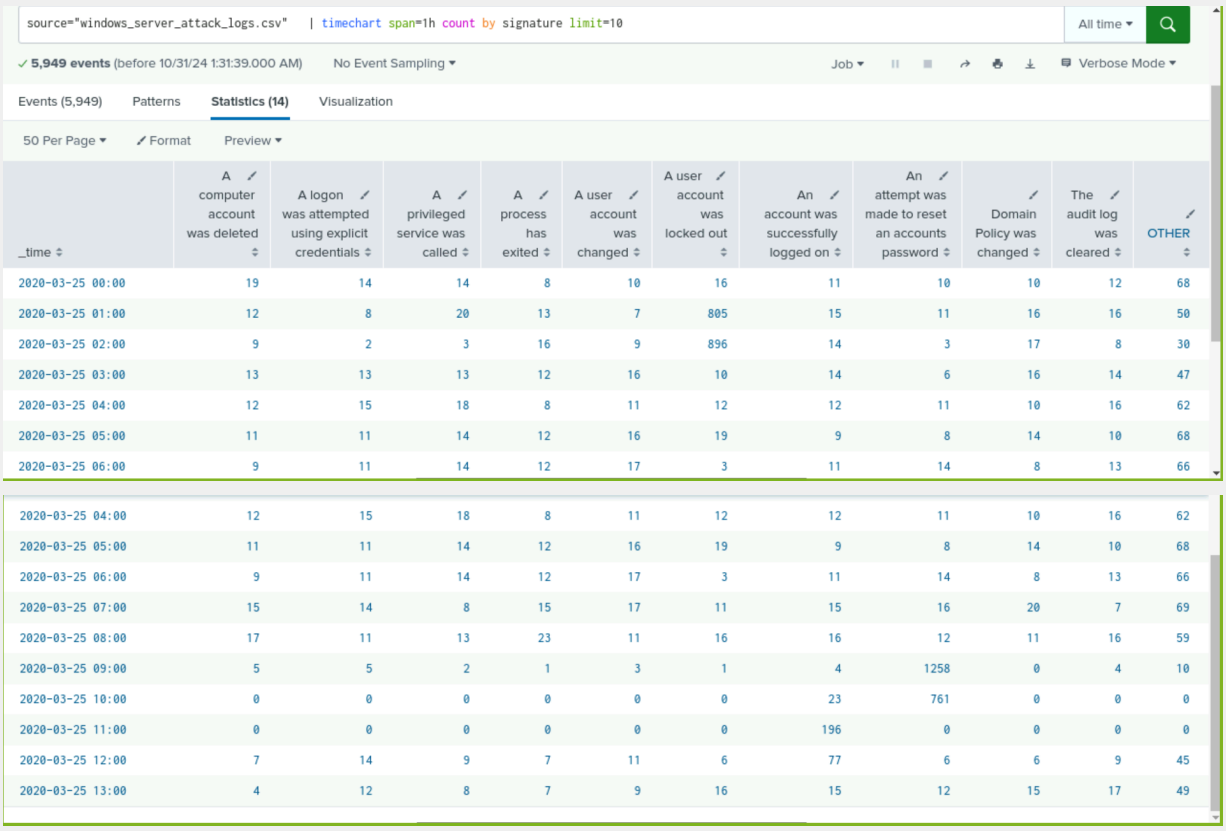
- Does anything stand out as suspicious?

Yes, in the timechat signature for the attack logs there are events that stand out from the Normal windows activity logs.
Regular windwos_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	28	24	24	24	42	26	22	36	18	22	144
2020-03-24 01:00	34	28	24	24	30	20	26	28	24	24	110
2020-03-24 02:00	20	28	46	22	18	30	30	32	38	32	132
2020-03-24 03:00	22	36	28	20	32	34	28	22	32	26	98
2020-03-24 04:00	18	26	24	20	20	18	36	30	44	38	104
2020-03-24 05:00	32	26	24	24	30	20	26	22	18	30	120
2020-03-24 06:00	22	28	14	42	22	20	16	16	24	24	160
2020-03-24 07:00	32	30	26	30	34	34	24	32	28	28	128
2020-03-24 08:00	34	28	12	28	18	32	36	18	28	30	142
2020-03-24 09:00	32	24	32	20	28	28	24	32	30	26	138
2020-03-24 10:00	28	18	26	26	24	32	18	20	46	32	130
2020-03-24 11:00	26	38	14	38	32	44	32	40	18	26	128
2020-03-24 12:00	32	32	42	26	38	22	28	18	18	32	114
2020-03-24 13:00	32	30	36	20	26	42	26	32	32	24	140
2020-03-24 14:00	34	28	30	28	22	18	26	24	26	26	132
2020-03-24 15:00	32	24	32	36	32	38	34	24	40	28	98

Windows_attack_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 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 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 timechart signature there are two events that have significant increase in activity

1. An attempt was made to reset the account password
2. A use account was locked out

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

1.An attempt to reset account password was occurred between 9:00 AM and 10:00 AM
2.A user account was locked out between 01:00 AM and 02:30 AM

- What is the peak count of the different signatures?

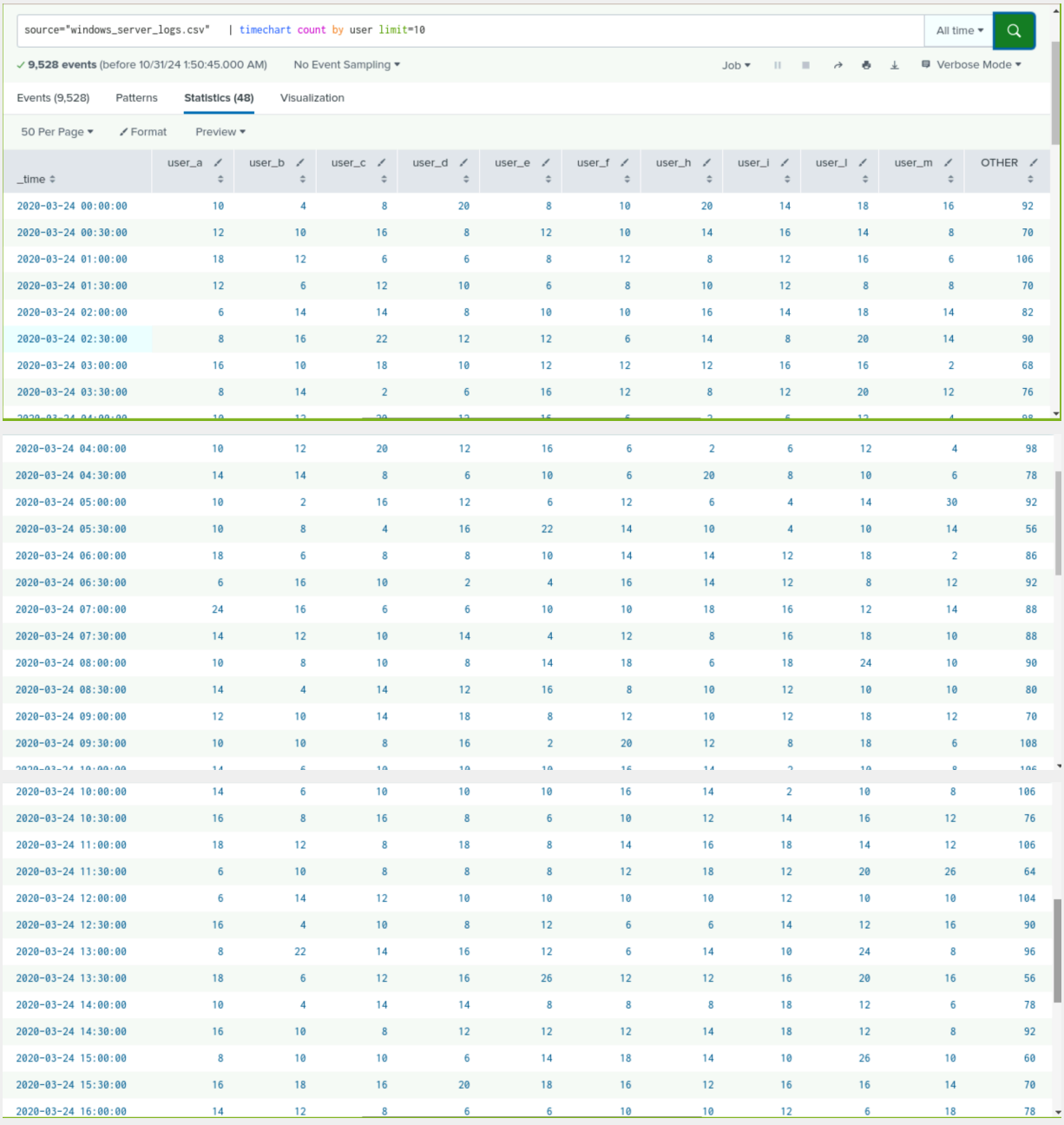
Account locked out peaked at 896

```
Attempt to reset password peaked at 1258
```

Dashboard Analysis for Users

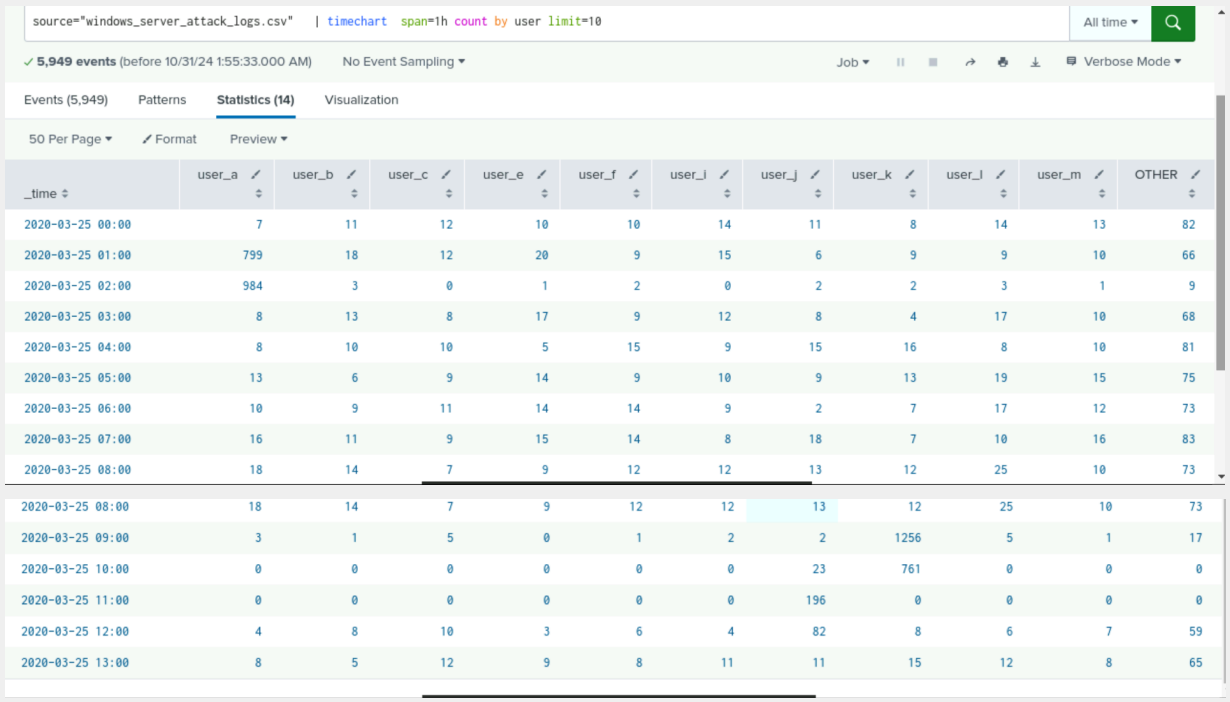
- Does anything stand out as suspicious?

```
Yes, there is a significant amount of acreases in user activity for two
users that is shown in the User and Hours timechart
Regular windwos_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 00:00:00	10	4	8	20	8	10	20	14	18	16	92
2020-03-24 00:30:00	12	10	16	8	12	10	14	16	14	8	70
2020-03-24 01:00:00	18	12	6	6	8	12	8	12	16	6	106
2020-03-24 01:30:00	12	6	12	10	6	8	10	12	8	8	70
2020-03-24 02:00:00	6	14	14	8	10	10	16	14	18	14	82
2020-03-24 02:30:00	8	16	22	12	12	6	14	8	20	14	90
2020-03-24 03:00:00	16	10	18	10	12	12	12	16	16	2	68
2020-03-24 03:30:00	8	14	2	6	16	12	8	12	20	12	76
2020-03-24 04:00:00	10	12	20	12	16	6	2	6	12	4	98
2020-03-24 04:30:00	14	14	8	6	10	6	20	8	10	6	78
2020-03-24 05:00:00	10	2	16	12	6	12	6	4	14	30	92
2020-03-24 05:30:00	10	8	4	16	22	14	10	4	10	14	56
2020-03-24 06:00:00	18	6	8	8	10	14	14	12	18	2	86
2020-03-24 06:30:00	6	16	10	2	4	16	14	12	8	12	92
2020-03-24 07:00:00	24	16	6	6	10	10	18	16	12	14	88
2020-03-24 07:30:00	14	12	10	14	4	12	8	16	18	10	88
2020-03-24 08:00:00	10	8	10	8	14	18	6	18	24	10	90
2020-03-24 08:30:00	14	4	14	12	16	8	10	12	10	10	80
2020-03-24 09:00:00	12	10	14	18	8	12	10	12	18	12	70
2020-03-24 09:30:00	10	10	8	16	2	20	12	8	18	6	108
2020-03-24 10:00:00	14	6	10	10	10	16	14	2	10	8	106
2020-03-24 10:30:00	16	8	16	8	6	10	12	14	16	12	76
2020-03-24 11:00:00	18	12	8	18	8	14	16	18	14	12	106
2020-03-24 11:30:00	6	10	8	8	8	12	18	12	20	26	64
2020-03-24 12:00:00	6	14	12	10	10	10	10	12	10	10	104
2020-03-24 12:30:00	16	4	10	8	12	6	6	14	12	16	90
2020-03-24 13:00:00	8	22	14	16	12	6	14	10	24	8	96
2020-03-24 13:30:00	18	6	12	16	26	12	12	16	20	16	56
2020-03-24 14:00:00	10	4	14	14	8	8	8	18	12	6	78
2020-03-24 14:30:00	16	10	8	12	12	12	14	18	12	8	92
2020-03-24 15:00:00	8	10	10	6	14	18	14	10	26	10	60
2020-03-24 15:30:00	16	18	16	20	18	16	12	16	16	14	70
2020-03-24 16:00:00	14	12	8	6	6	10	10	12	6	18	78

windows_attack_logs:



_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 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?

```
Therere two users stand out in Users by Hour visualization
   1. User_a
   2. User_k
```

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

User_a had increased activity between 01:00 AM and 02:30 AM
User-k had increased activity between 09:00 AM and 10:00 AM

- What is the peak count of the different users?

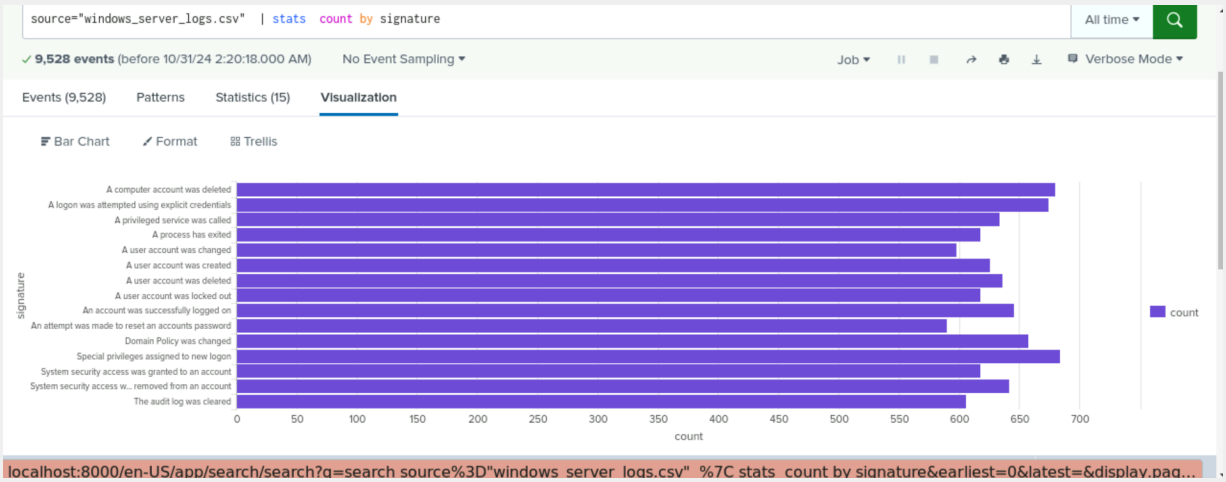
```
User_a peaked at 984
User_k peaked at 1256
```

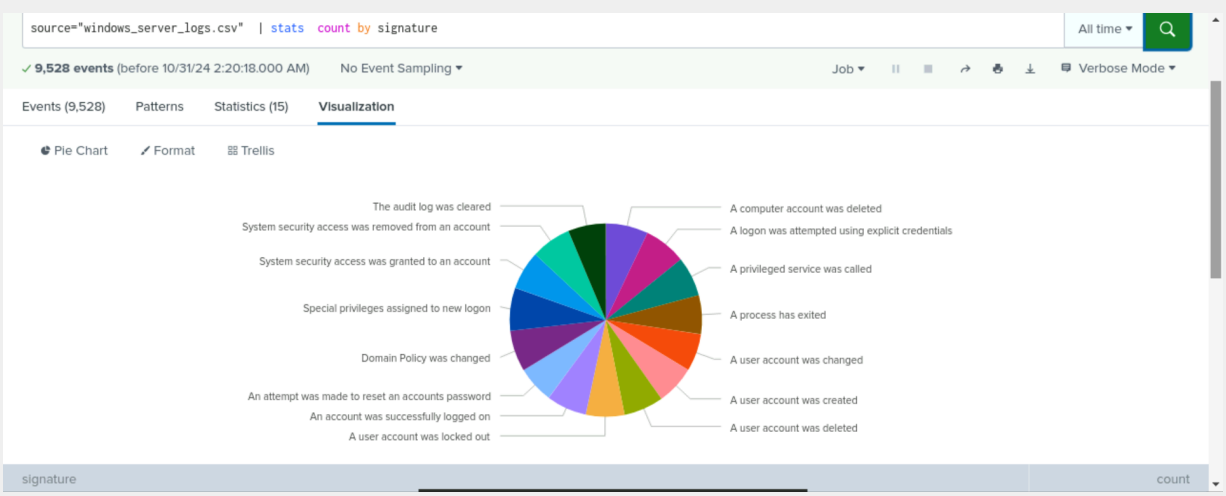
Dashboard Analysis for Signatures with Bar, Graph, and Pie Charts

- Does anything stand out as suspicious?

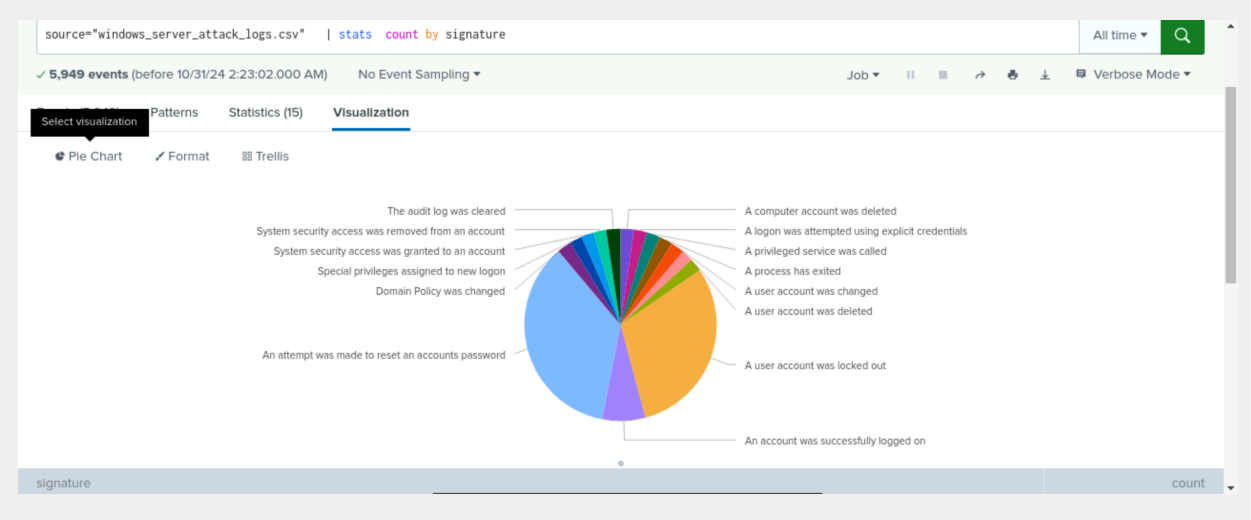
Yes , there's a significant increase in two signature types: An attempt to reset account password and A user account was locked out.

Regular windows_logs:





Windows_attack_logs:



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

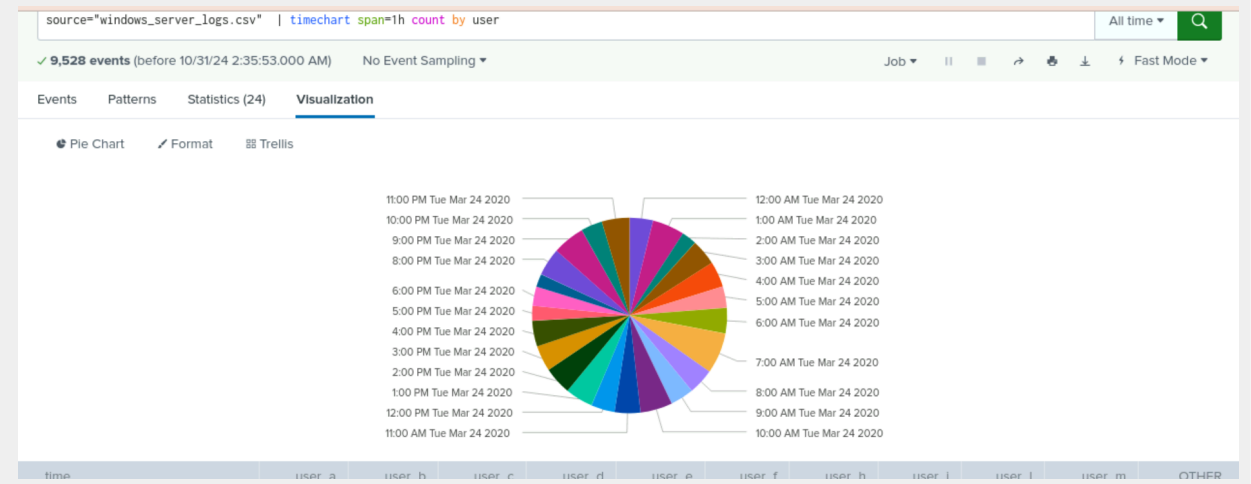
```
Yes they match
```

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

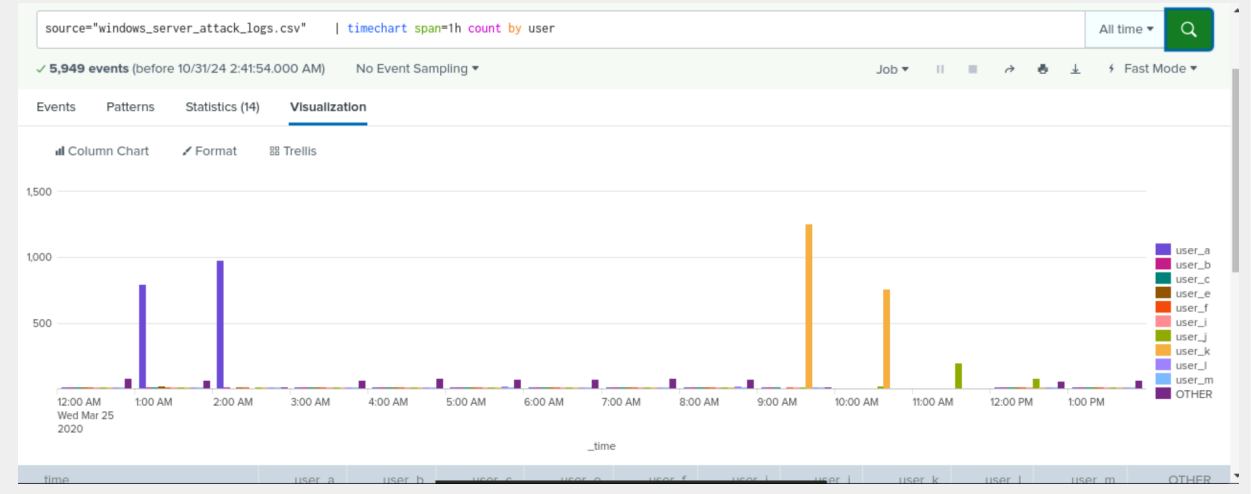
- Does anything stand out as suspicious?

```
Yes , there's a increased activity from user_a and user_k

Regular windows_logs:
```



`windows_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?

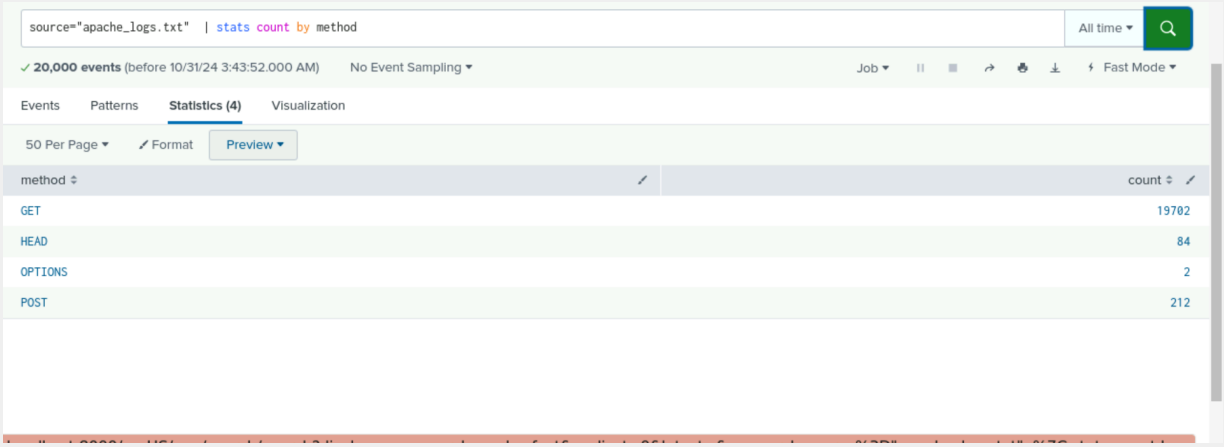
The advantage of using a statistical chart is its ability to quickly display counts for each user's event or track users per hour. However, unlike bar charts, line graphs, and pie charts, it doesn't clearly indicate changes in activity over time. Visualizations like bar and line graphs help spot spikes or declines in events by time, while a pie chart effectively shows which events or users have the most significant increases in activity, making trends easier to interpret.

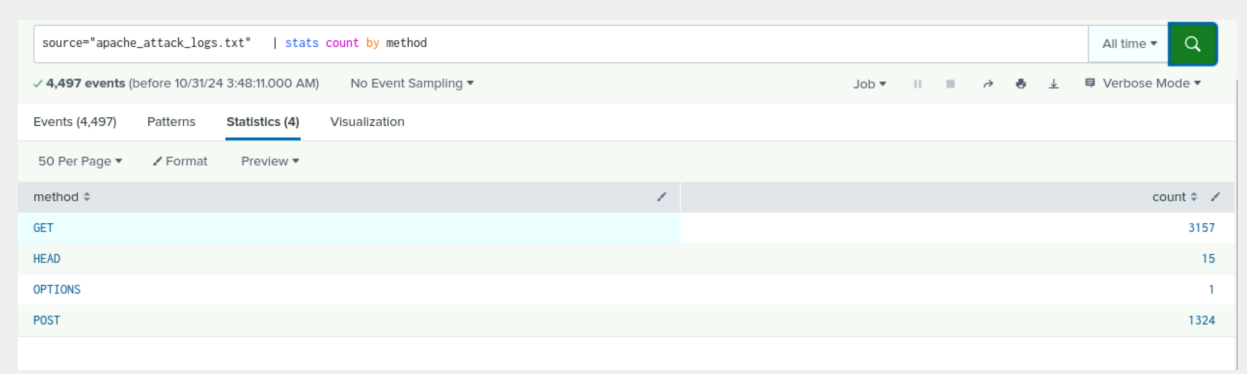
Apache Web Server Log Questions

Report Analysis for Methods

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

Yes, in an analysis with the HTTP method, I detected a suspicious change in with POST.
Regular apache_logs:





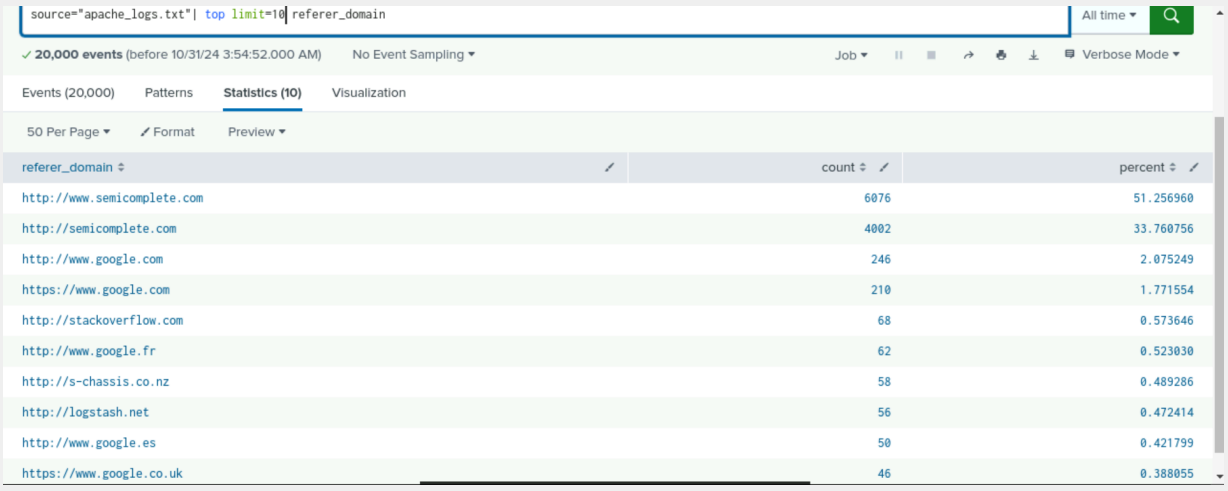
- What is that method used for?

POST:This method is used to send data to a server from the HTTP client to create or update resources, commonly used for submitting forms, login data, or file uploads.

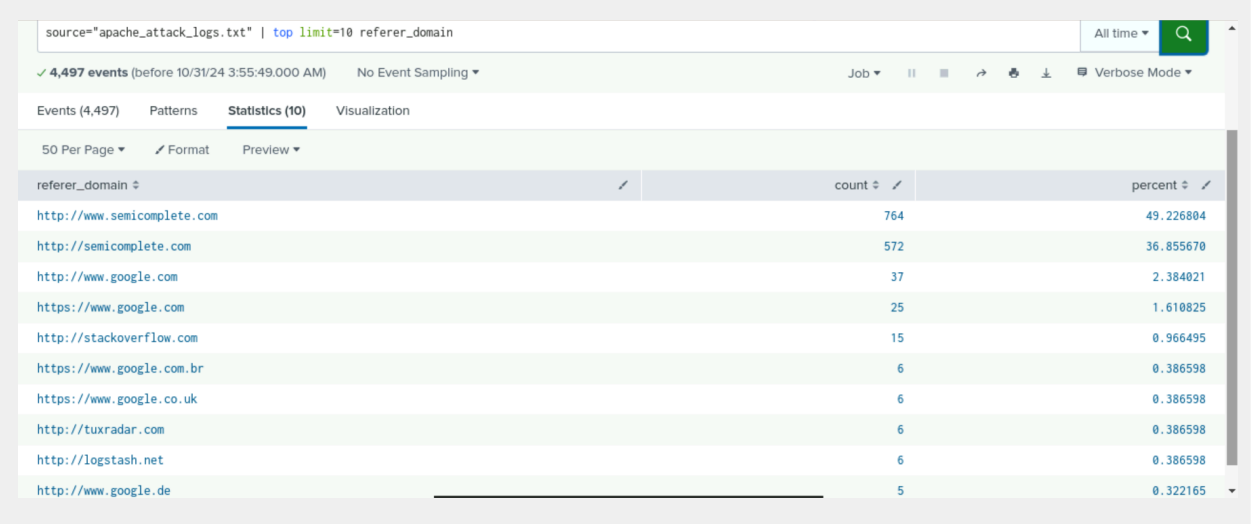
Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

I did see some suspicious changes in the result of top10 referral domains specifically in the last 5 list.
Regular Apache_logs:



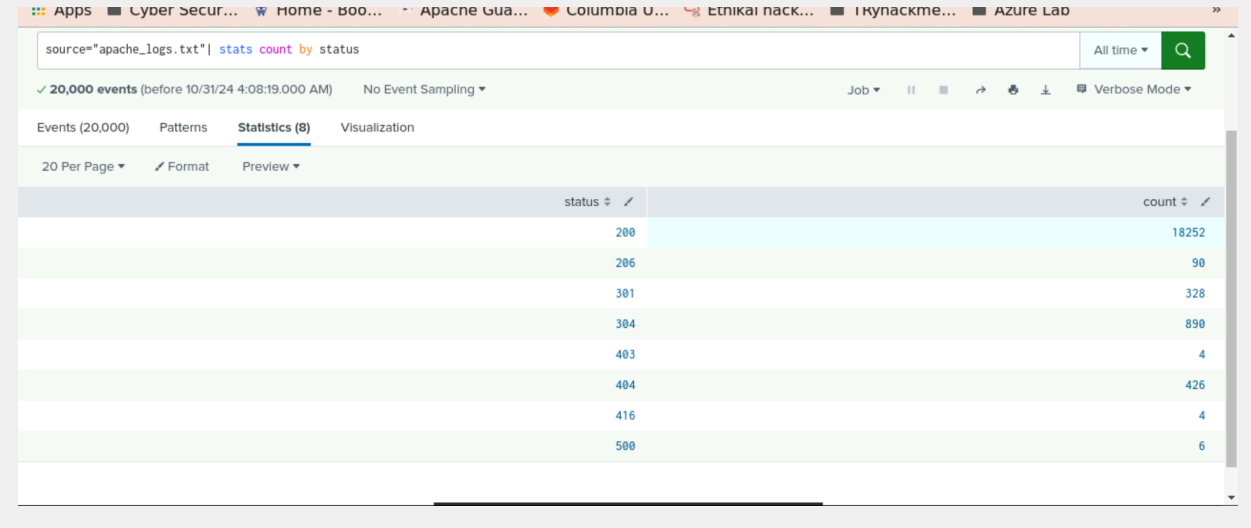
Apache_attack_logs:



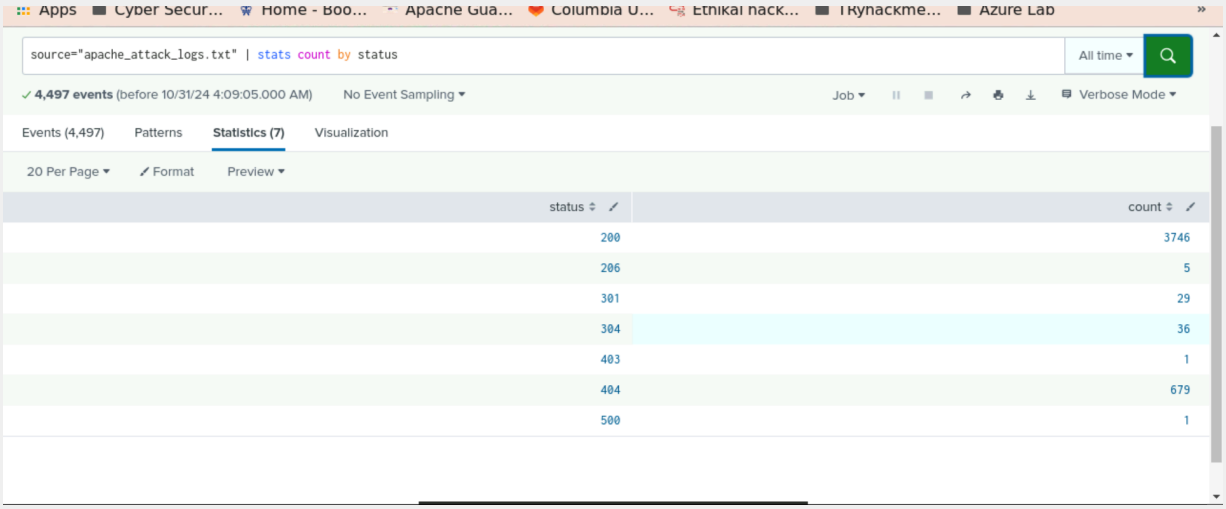
Report Analysis for HTTP Response Codes

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

Yes , I detect a suspicious change in HTTP response codes, specially with response code 200 and 404. Response code 200 shows decrease and response code 404 shows an increase.
Regular apache_logs:



apche_attach_logs:



Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

```
Yes , I detected a suspicious volume of international activity.

Regular Apache_logs:
```

```
source="apache_logs.txt"     | iplocation clientip | where  Country!="United States" | bin _time span=1h | stats count AS activity_count
    by _time, Country
```

All time

✓ **12,280 events** (before 10/31/24 5:12:48.000 AM) No Event Sampling Job Verbose Mode

Events (12,280) Patterns **Statistics (1,059)** Visualization

20 Per Page Format Preview Prev 1 2 3 4 5 6 7 8 ... Next

_time	Country	activity_count
2020-03-17 10:00	Belgium	12
2020-03-17 10:00	China	2
2020-03-17 10:00	France	16
2020-03-17 10:00	Germany	2
2020-03-17 10:00	Guatemala	8
2020-03-17 10:00	Indonesia	12
2020-03-17 10:00	Romania	12
2020-03-17 10:00	Russia	46
2020-03-17 11:00	Algeria	12
2020-03-17 11:00	Brazil	2
2020-03-17 11:00	China	24
2020-03-17 11:00	France	8
2020-03-17 11:00	Germany	16
2020-03-17 11:00	Japan	2
2020-03-17 11:00	Netherlands	4
2020-03-17 11:00	Singapore	12
2020-03-17 11:00	United Kingdom	22
2020-03-17 12:00	Austria	8
2020-03-17 12:00	Cambodia	2
2020-03-17 12:00	China	6

Apache_attack_logs:

```
source="apache_attack_logs.txt"     | iplocation clientip | where  Country!="United States" | bin _time span=1h | stats count AS activity_count by
    _time, Country
```

All time

✓ **2,497 events** (before 10/31/24 5:25:40.000 AM) No Event Sampling Job Verbose Mode

Events (2,497) Patterns **Statistics (265)** Visualization

20 Per Page Format Preview Prev 1 2 3 4 5 6 7 8 ... Next

_time	Country	activity_count
2020-03-25 20:00	Ukraine	864
2020-03-25 01:00	Sweden	75
2020-03-25 00:00	Sweden	59
2020-03-25 09:00	Sweden	46
2020-03-25 08:00	France	40
2020-03-25 02:00	Italy	39
2020-03-25 10:00	Spain	39
2020-03-25 20:00	Canada	38

2020-03-25 07:00	Germany	37
2020-03-25 16:00	El Salvador	33
2020-03-25 00:00	Israel	29
2020-03-25 11:00	Japan	26
2020-03-25 09:00	Germany	25
2020-03-25 04:00	Spain	21
2020-03-25 12:00	Poland	20
2020-03-25 13:00	Brazil	20
2020-03-25 03:00	Italy	19
2020-03-25 10:00	France	19
2020-03-25 19:00	Canada	19
2020-03-25 00:00	India	17

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

```
The count was 864 at 8:00 PM
```

- Would your alert be triggered for this activity?

```
Yes , my alert will be triggered as I set the threshold to more than 150 in an hour.
```

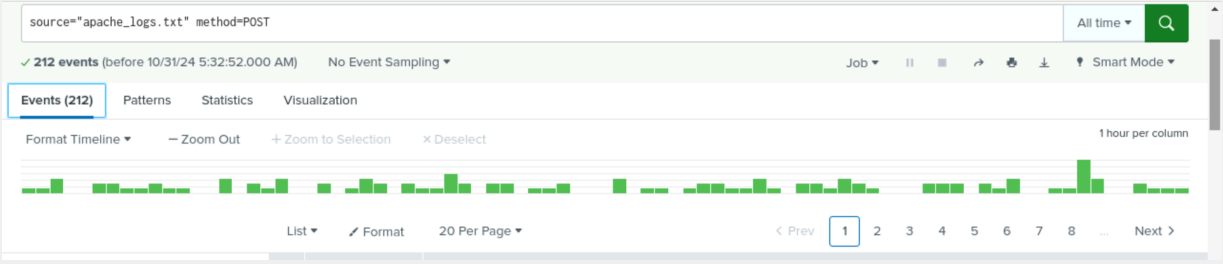
- After reviewing, would you change the threshold that you previously selected?

```
I will keep my threshold the same but continue monitoring the Apache logs to see if I can raise the threshold in case of need.
```

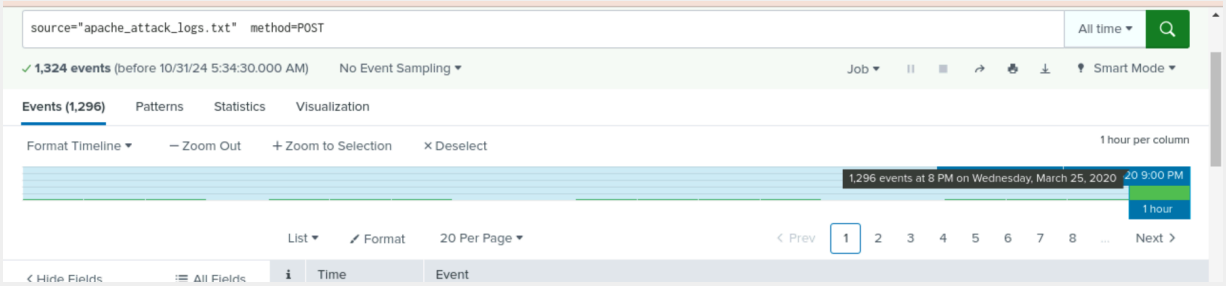
Alert Analysis for HTTP POST Activity

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

```
Yes, I detected a suspicious amount of HTTP POST activity.
Regular Apache_logs:
```



Apache_attach_logs:



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

```
The count was 1296 at 8:00 PM
```

- When did it occur?

```
On 03-25-2020
```

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

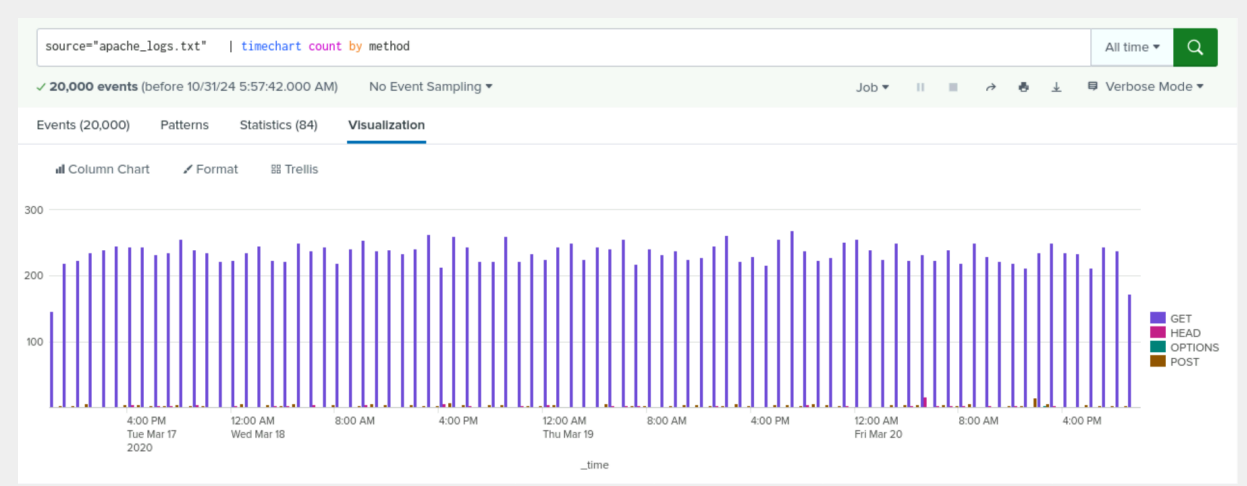
```
No, I won't change the threshold number which I set at 15. I will conduct a
further analysis of the apache logs daily to determine if the number needs
to be increased.
```

Dashboard Analysis for Time Chart of HTTP Methods

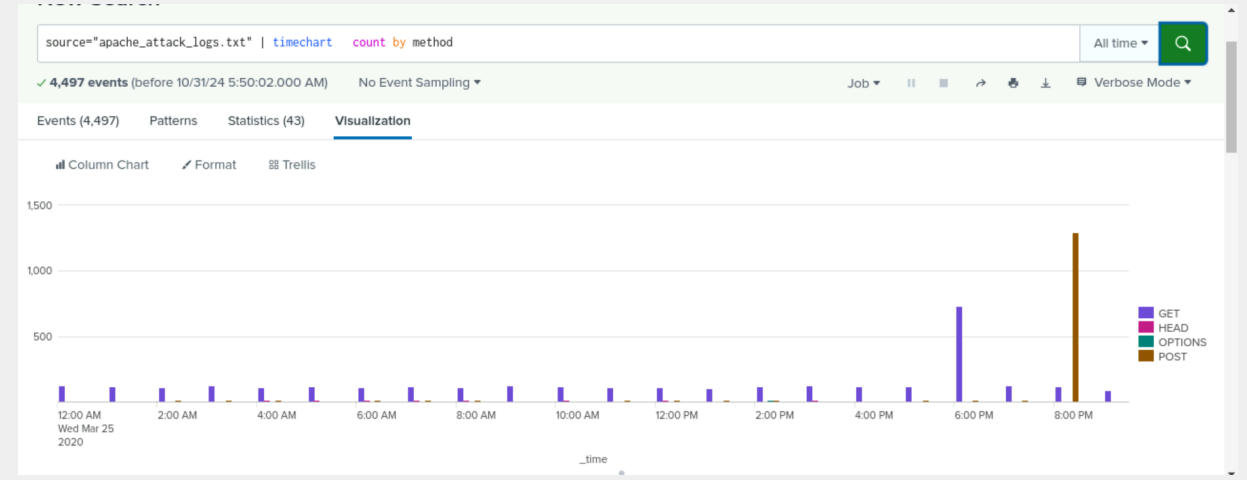
- Does anything stand out as suspicious?

```
Yes, there was a significant difference in the HTTP method timecharts.

Regular Apache_logs:
```



Apache_attack_logs:



- Which method seems to be used in the attack?

```
HTTP method POST
```

- At what times did the attack start and stop?

```
The attack started at 7:30 PM and stopped at 8:30 PM
```

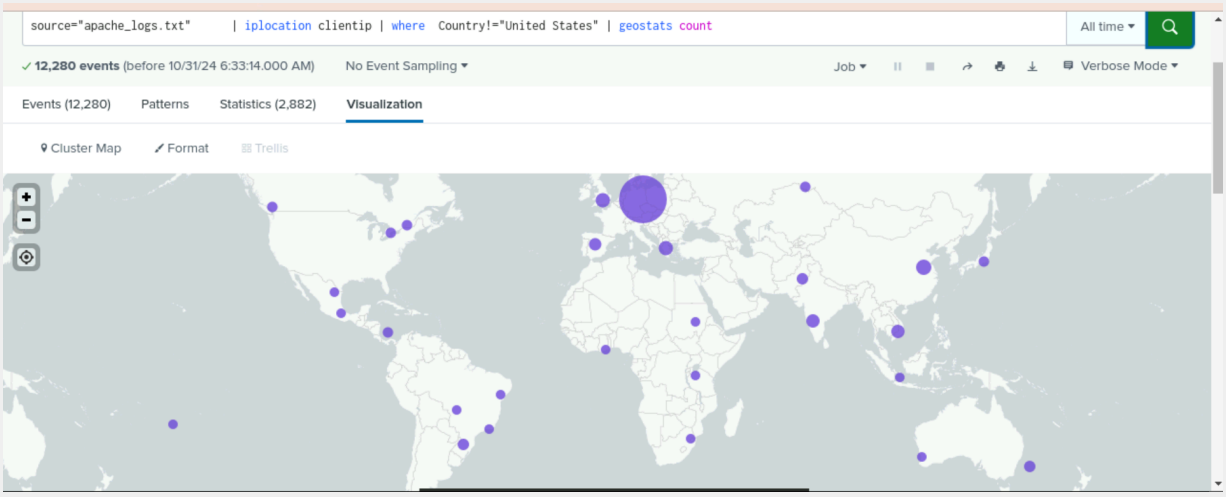
- What is the peak count of the top method during the attack?

```
1296
```

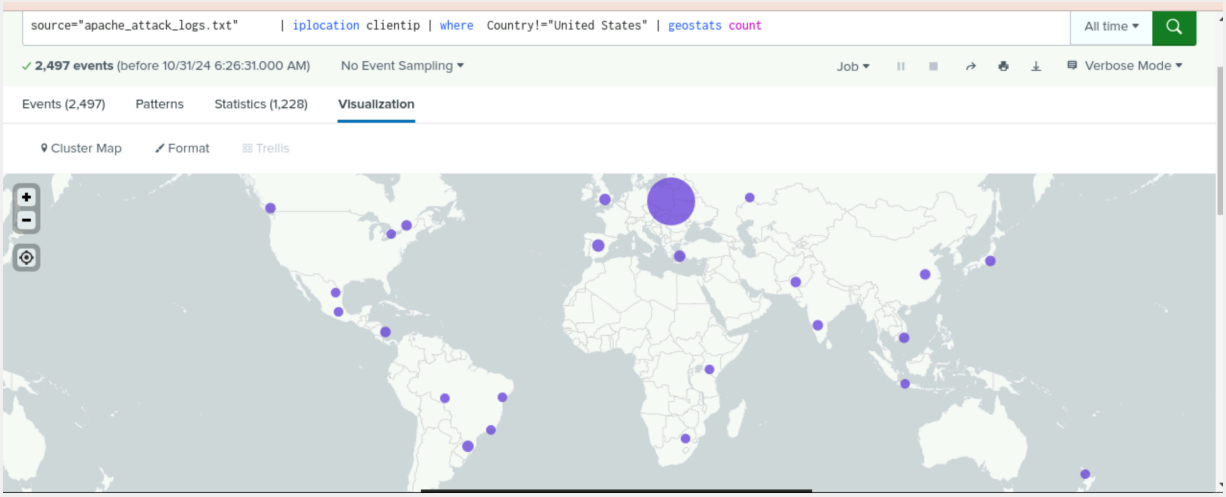
Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

Yes, there was suspicious activity in the country of Ukraine's city Kiev and Kharkiv.
Regular Apache_logs:



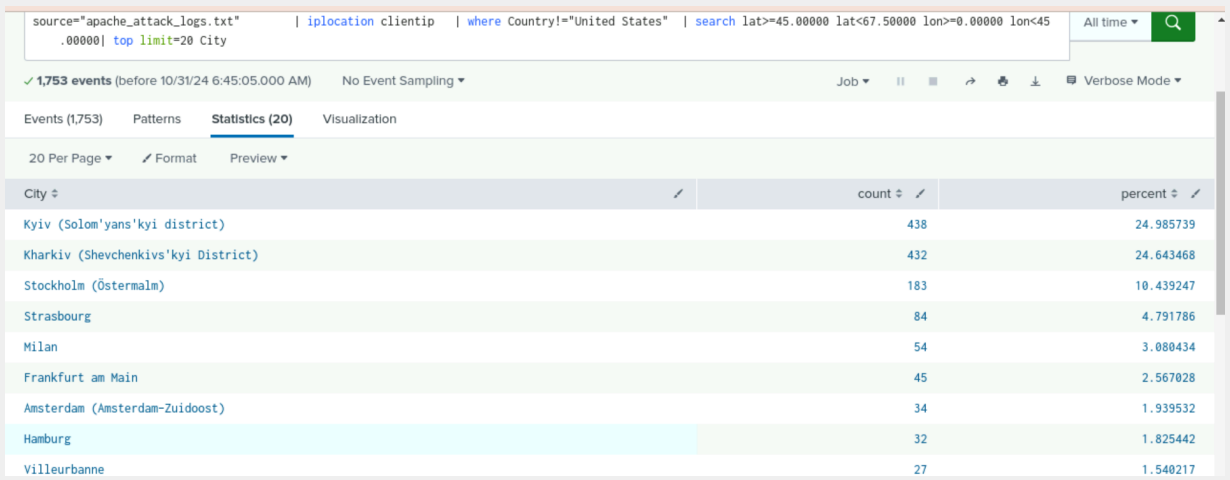
Apache_attack_logs:



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

Both Kyiv and Kharkiv in Ukraine had a increase in activity

- What is the count of that city?



Kyiv-438
Kharkiv-432

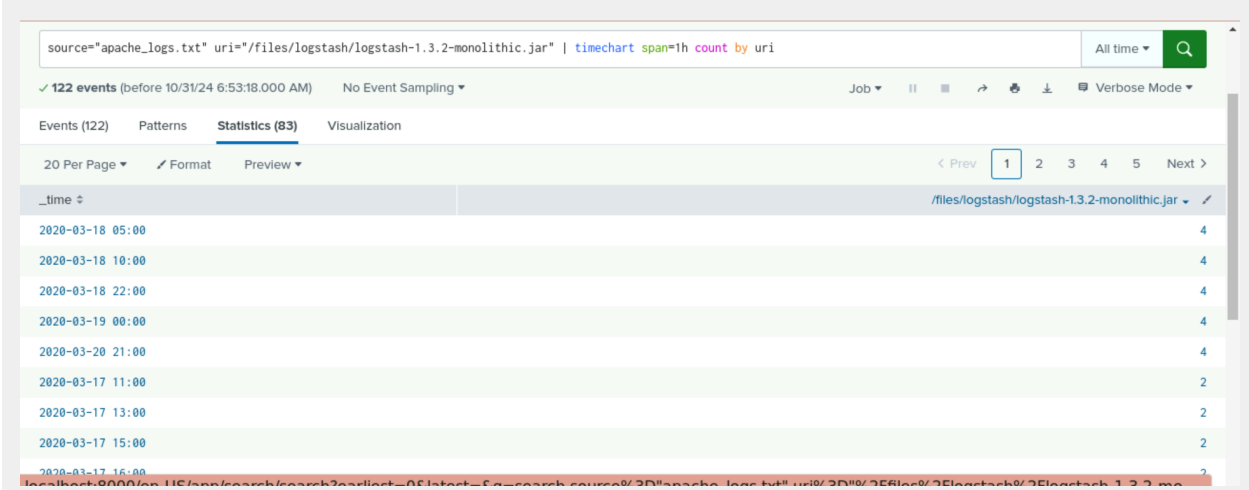
Dashboard Analysis for URI Data

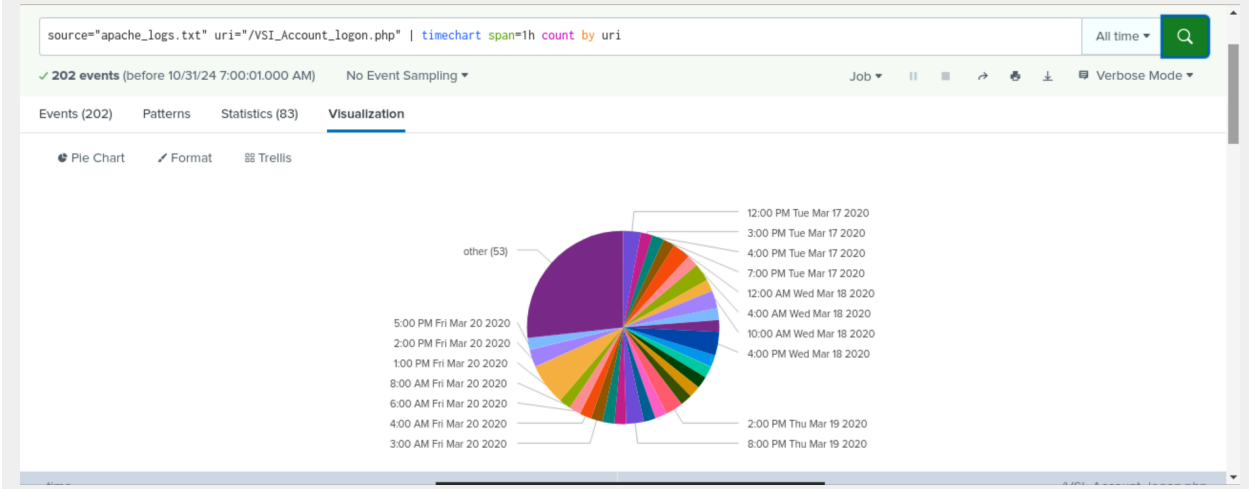
- Does anything stand out as suspicious?

There was a suspicious activity with the uri=”/files/logstash/logstash-1.3.2-monolithic.jar” at 06:00 PM. on 03-25-2020 and uri=”/VSI_Account_logon.php at 08:00 PM. on 03-25-2020

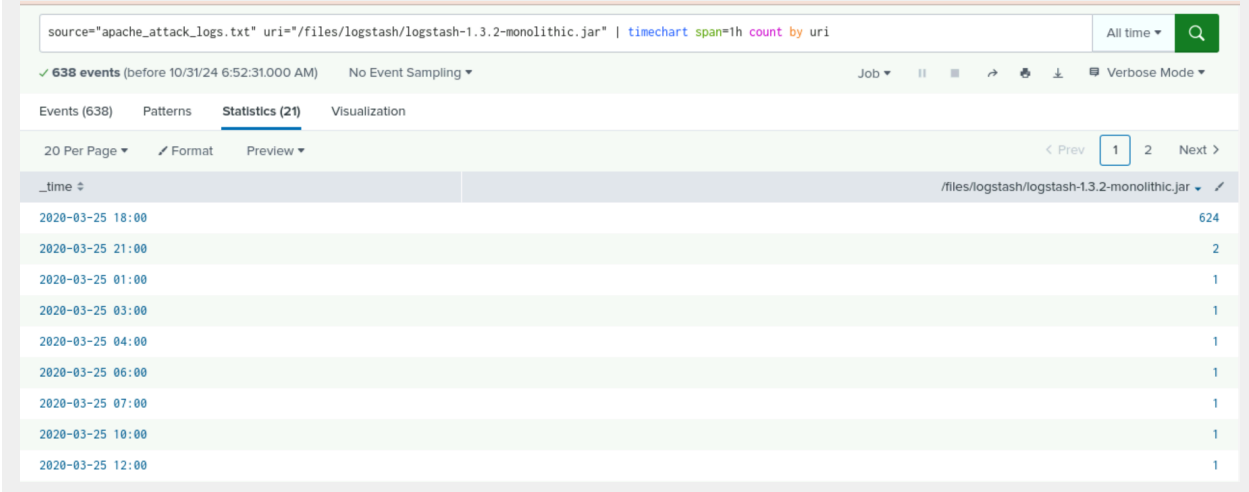
Top 10 Values	Count	%
/VSI_Account_logon.php	1,323	29.42%
/files/logstash/logstash-1.3.2-monolithic.jar	638	14.187%
/VSI_Company_Homepage.html	235	5.226%
/contactus.html	153	3.402%
/images/VSI_headquarters.jpg	152	3.38%
/reset.css	151	3.358%
/images/web/2009/banner.png	145	3.224%
/	122	2.713%
/blog/tags/puppet	115	2.557%
/projects/xdotool/	70	1.556%

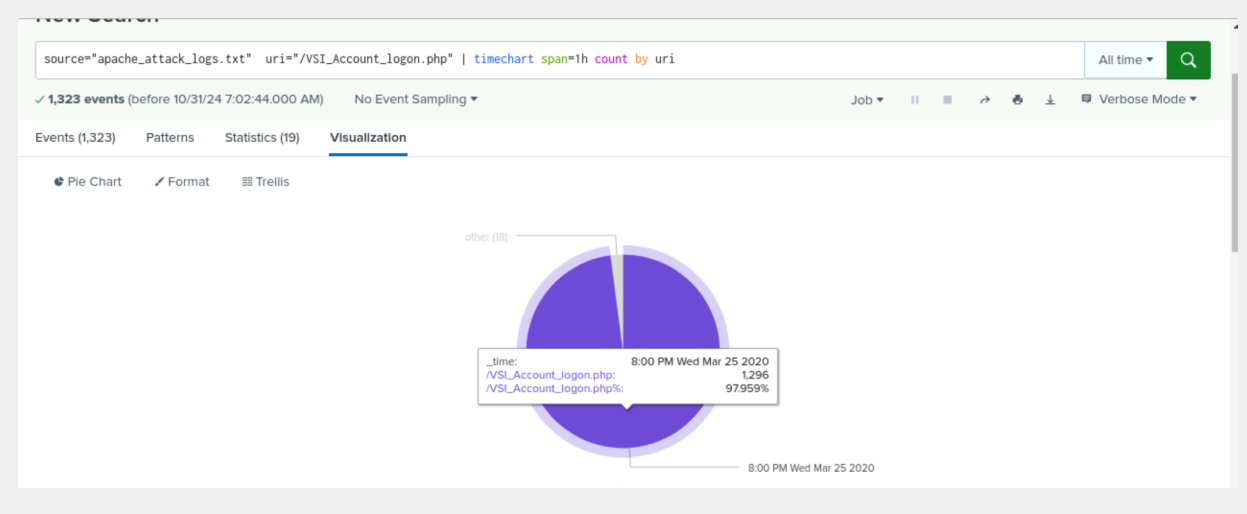
Regular Apache_logs:





Apache_attack_logs





- What URI is hit the most?

The `uri=/VSI_Account_logon.php`

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

```
Based on the uri=/VSI_Account_logon.php, the attacker may be trying to do a
brute force attack or SQL injection.
```