Cybersecurity

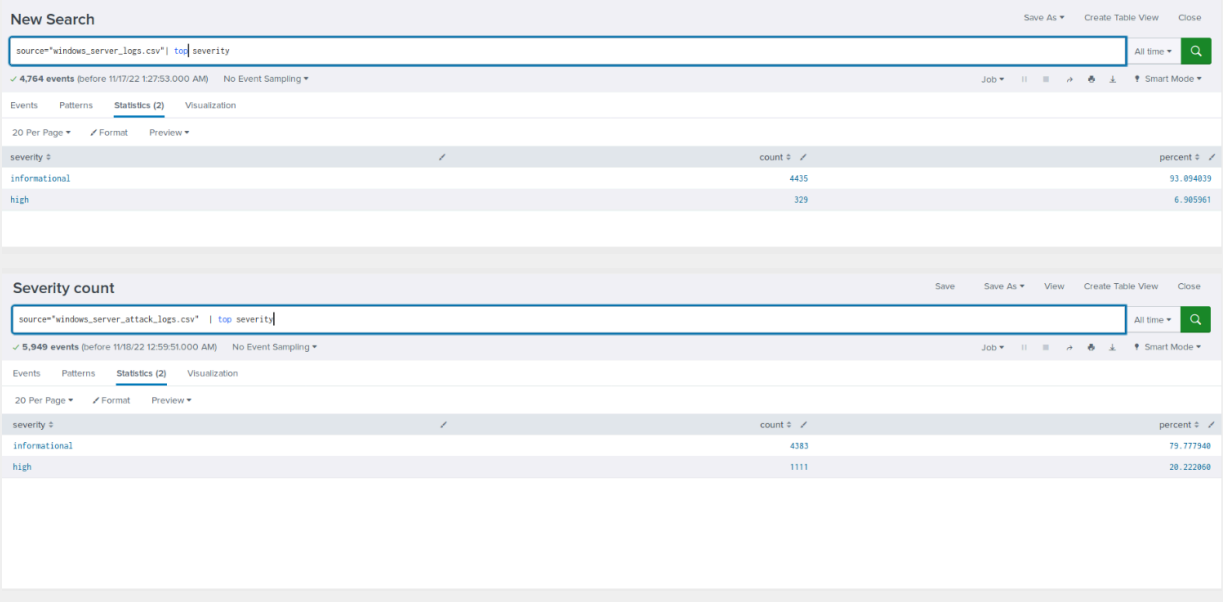
Designing and Implementing a Defensive Security Monitoring Solution for VSI

Windows Server Log Questions

Report Analysis for Severity

- Did you detect any suspicious changes in severity?

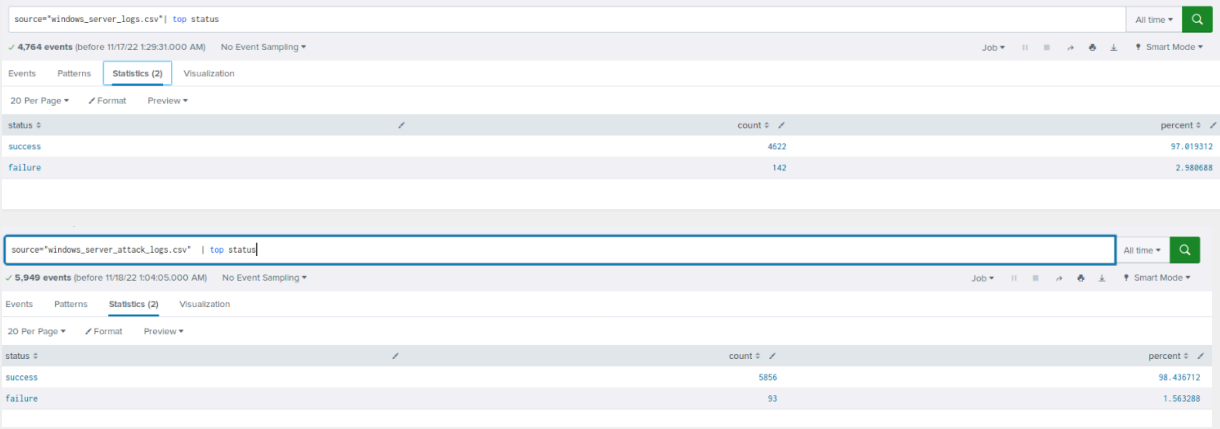
Our Splunk report did detect changes in severity, the biggest being for High severity events (Normal Log 7% to Attack Log's 20%)



Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

We did see many changes on the status of activities between normal and attack logs. The number of successful activities increased and the number of failed activities decreased.



Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

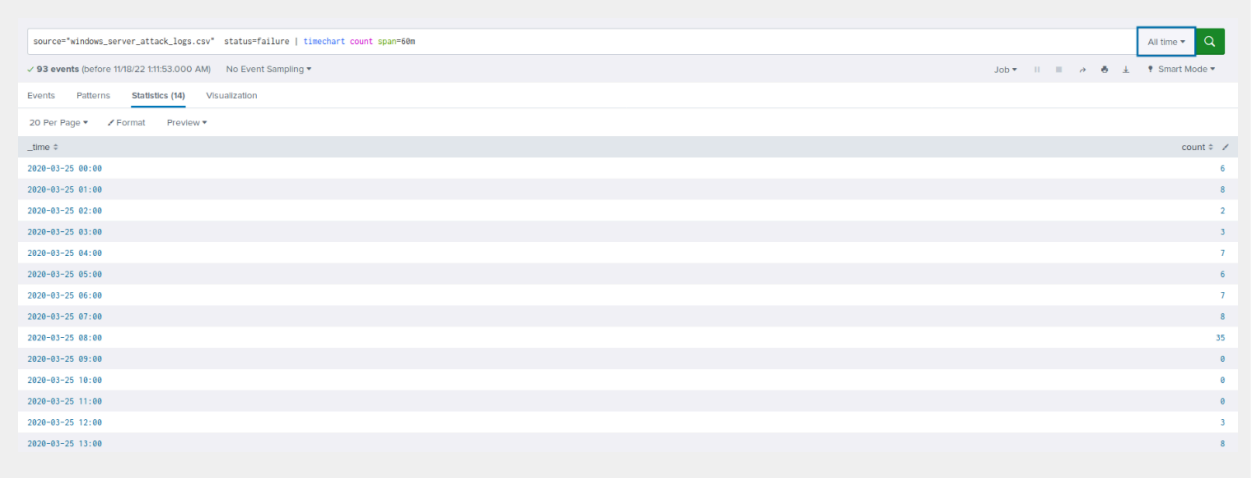
Yes

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

35 failed Windows activities

- When did it occur?

2020-03-25 08:00AM



- Would your alert be triggered for this activity?

```
The alert would trigger as we set the threshold to be 14 failed Windows activities.
```

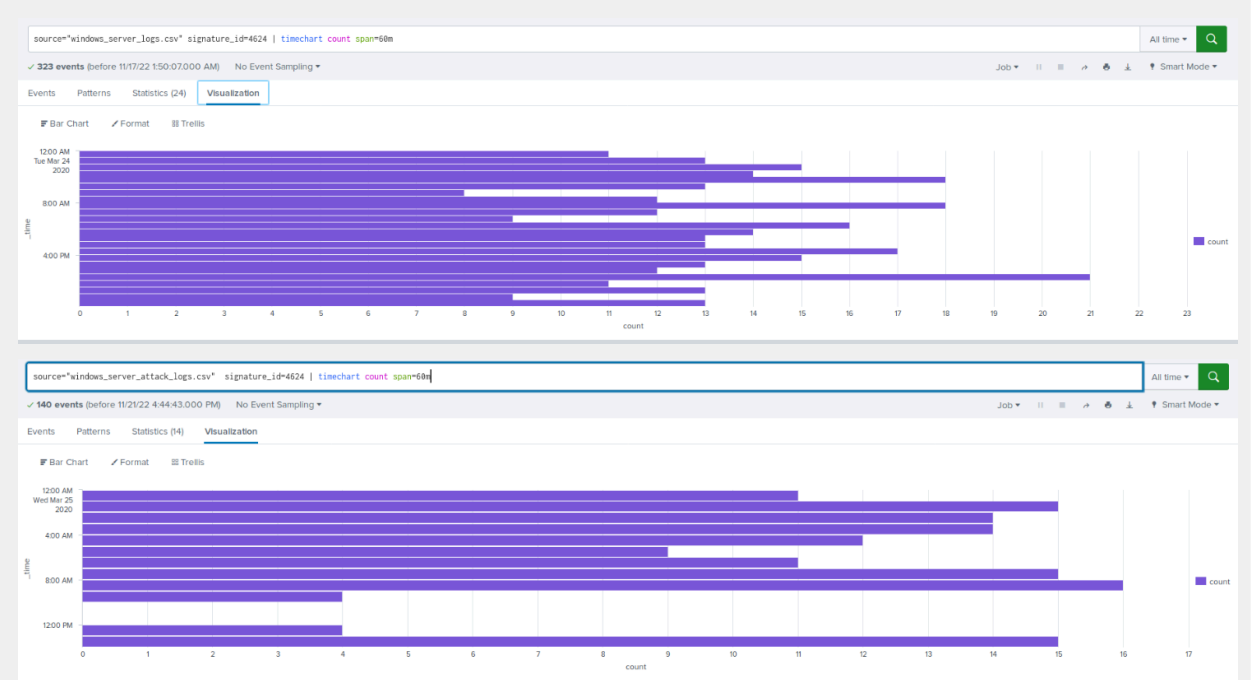
- After reviewing, would you change your threshold from what you previously selected?

```
No. It is double the average number of failed Windows Activities, which we believe is fair for both alert fatigue and user friendliness.
```

Alert Analysis for Successful Logins

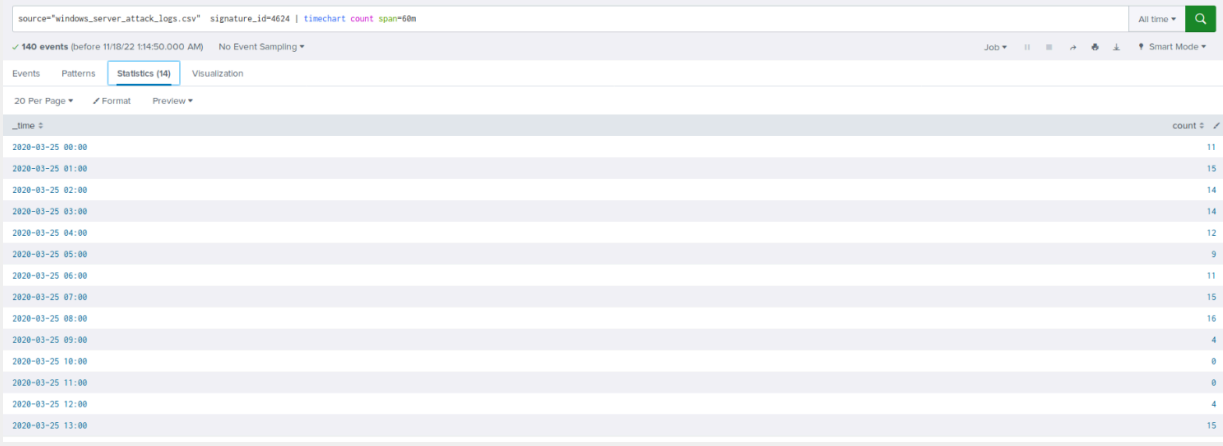
- Did you detect a suspicious volume of successful logins?

```
There is a suspicious lack of user logins.
```



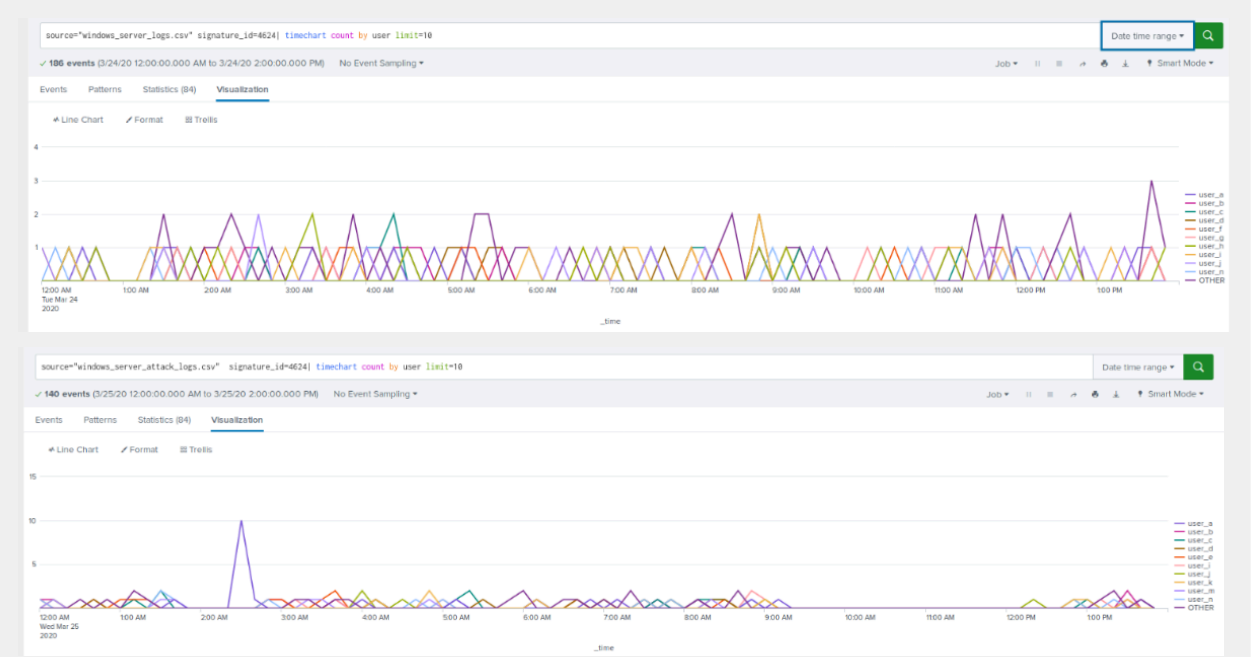
- If so, what was the count of events in the hour(s) it occurred?

There were 16 successful logins on 08:00AM, dropping to 4 at 09:00AM, then it goes from 0 between 10:00AM-11:00AM before jumping to 4 logins at 12:00PM



- Who is the primary user logging in?

User_a



- When did it occur?

```
02:00AM 2020-03-25
```

- Would your alert be triggered for this activity?

```
No since our threshold is 30 events required to alert the SOC
```

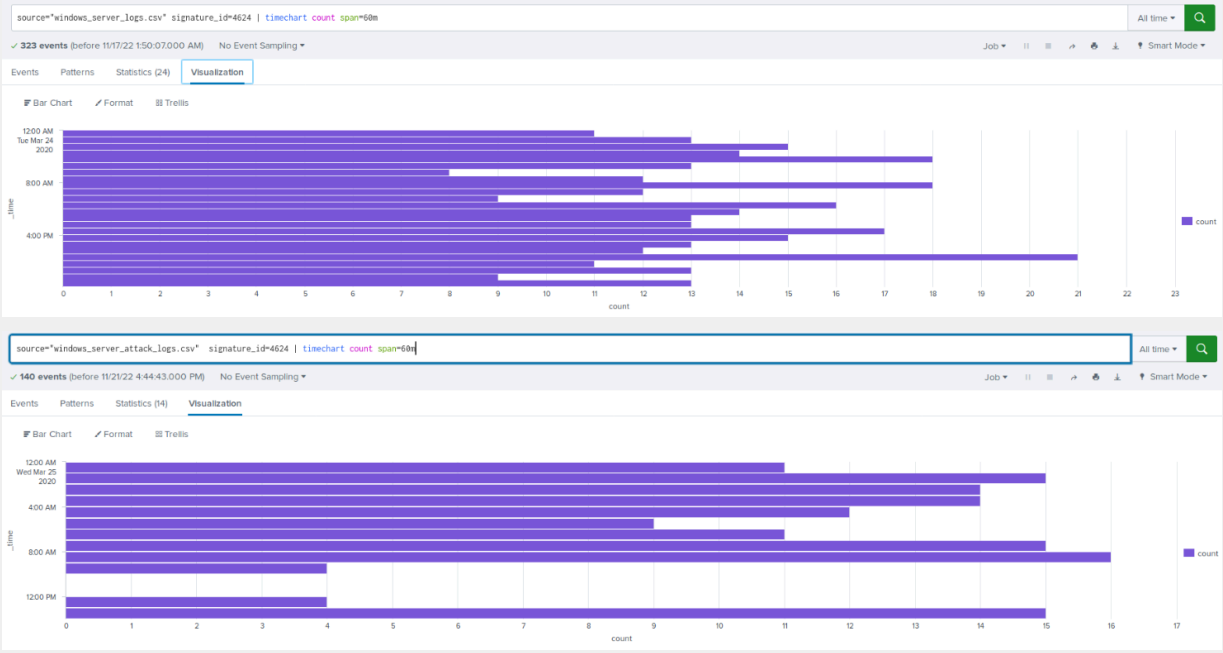
- After reviewing, would you change your threshold from what you previously selected?

```
I think creating two alerts (one minor, one major) to ensure that SOC is not overwhelmed with triggered activity. Alert fatigue could cause SOC or other sysadmin to ignore these potentially dangerous alerts if there is only one threshold or if the threshold is lowered too much.
```

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

While we detected a bit of a suspicious volume of deleted accounts, only from 09:00AM to 11:00AM was there any difference in numbers of deletion (it dropped).



Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

_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

- What signatures stand out?

The Time Chart shows two significant increases in activity for both “An attempt was made to reset an account password” and “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” happened between 09:00-10:00AM
“A user account was locked out” happened between 01:00-02:30AM

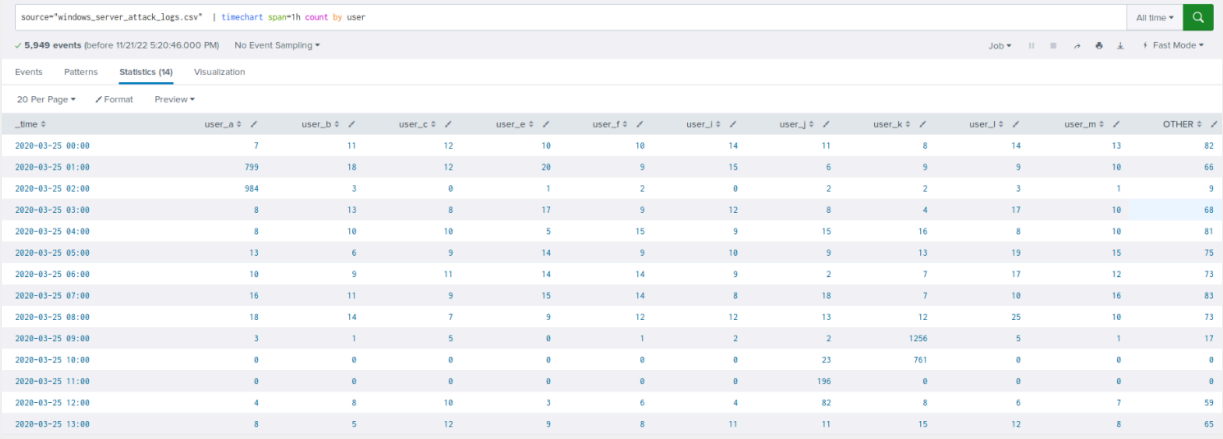
- What is the peak count of the different signatures?

Account locked out was peaking at 896
Reset password attempts wa speaking at 1268

Dashboard Analysis for Users

- Does anything stand out as suspicious?

User_a has an increase in their amount of activity time during the attack logs between 01:00-02:00AM. User_k had an increase in their activity from 09:00-10:00AM.



_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?

User_a and user_k

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

User_a has an increase in their amount of activity time during the attack logs between 01:00-02:00AM. User_k had an increase in their activity from 09:00-10:00AM.

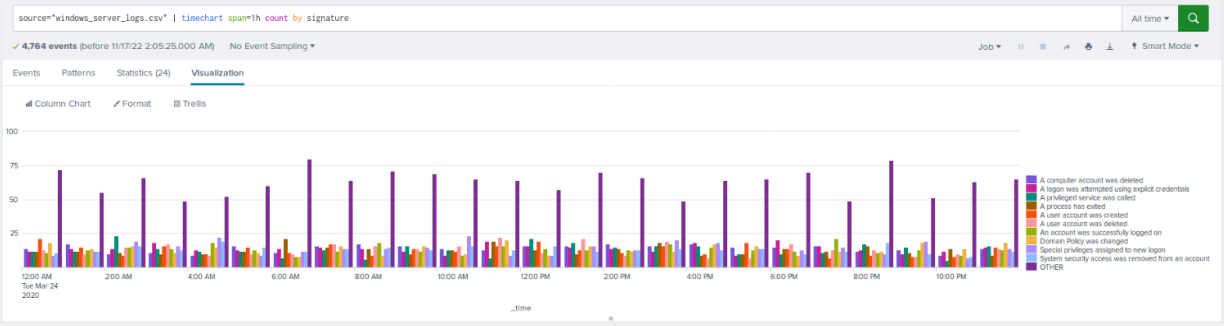
- What is the peak count of the different users?

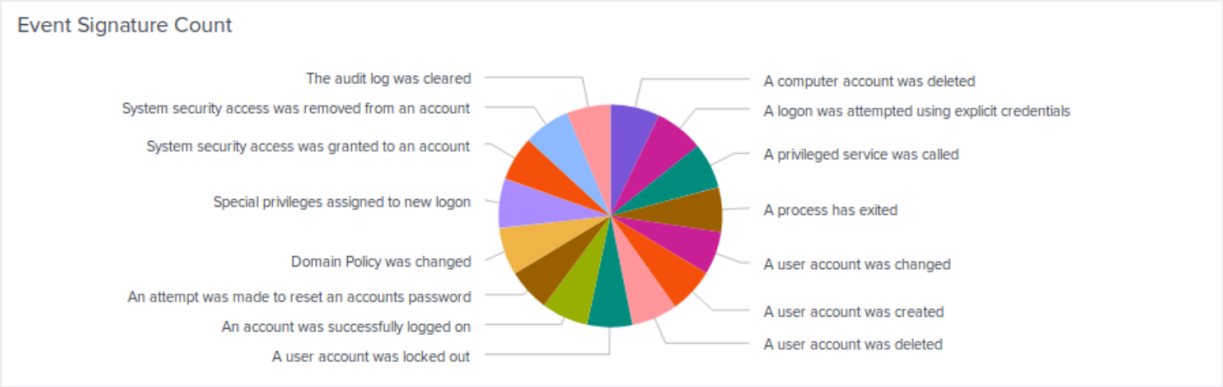
User_a peaked at 984 and user_k peaked at 1256

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

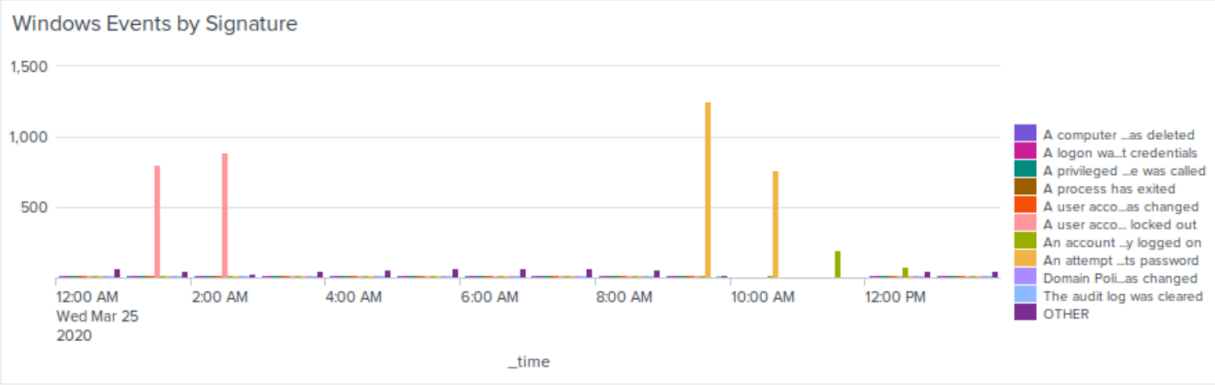
- Does anything stand out as suspicious?

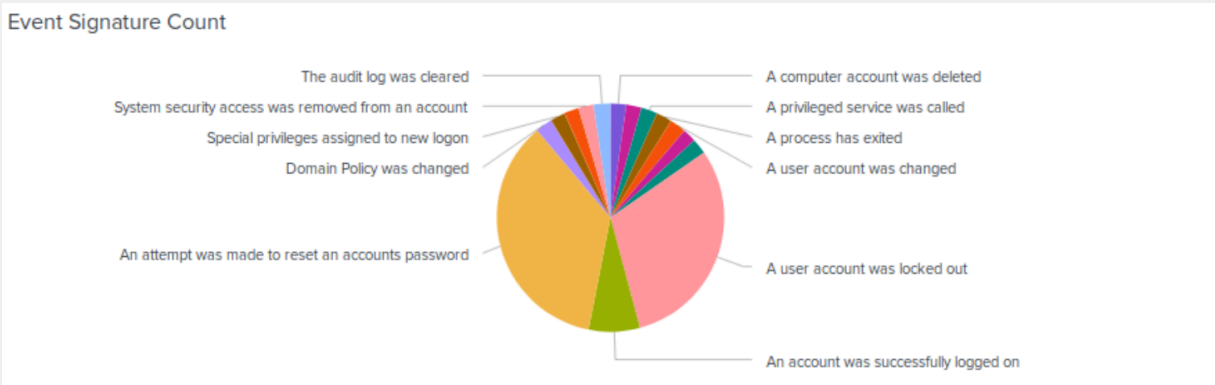
Yes - both “An attempt was made to reset an account password” and “A user account was locked out” increased in the attack logs compared to the regular Windows server logs.
Normal Logs:





Attack Logs:





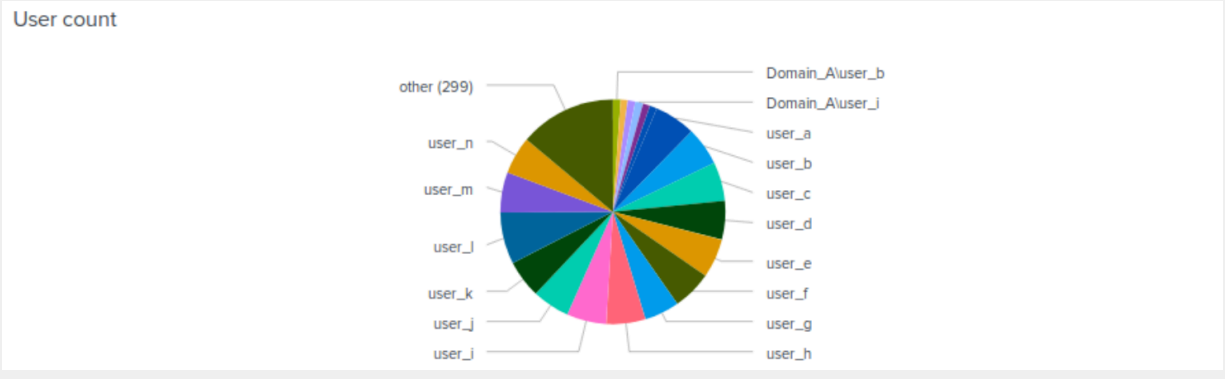
- Do the results match your findings in your time chart for signatures?

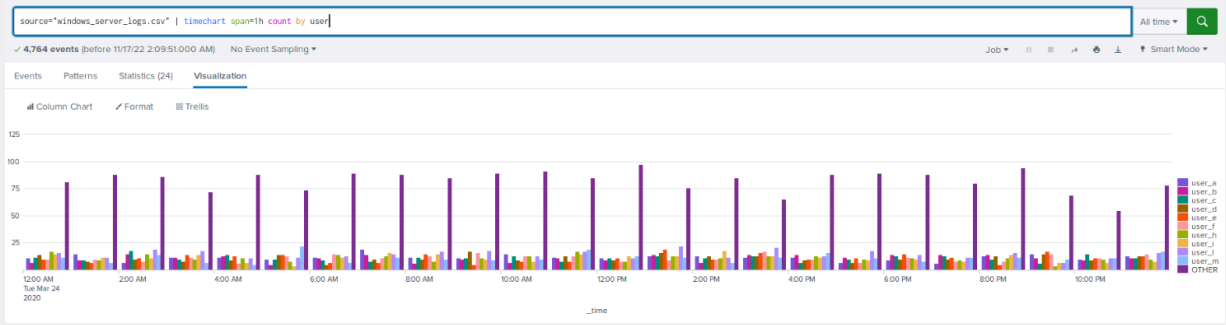
```
Yesx
```

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

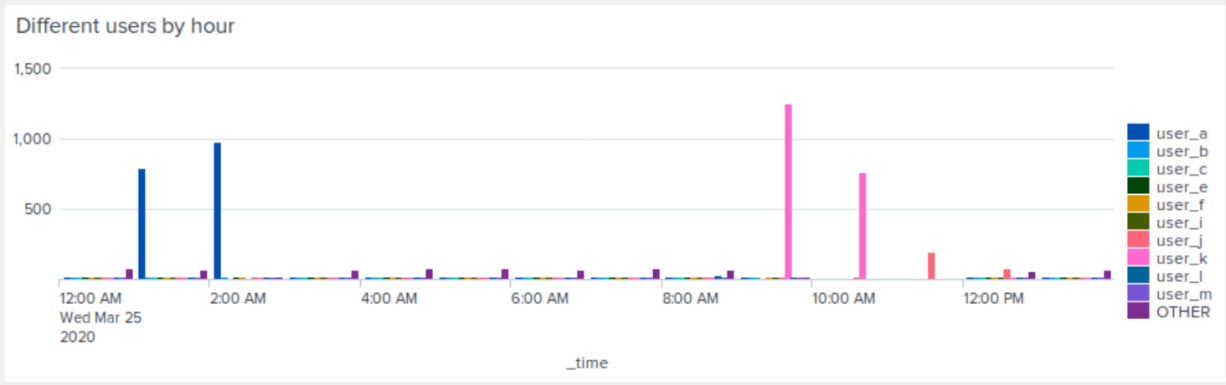
- Does anything stand out as suspicious?

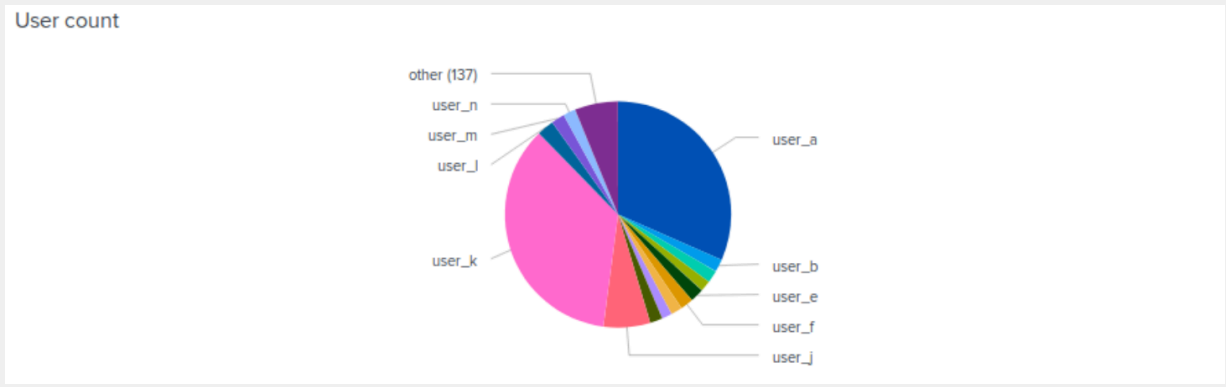
```
Yes, still user_a and user_k
```





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?

Statistical time charts for users and signatures allows SOC to hastily find the counts of each event and user by the hour; however, bar and pie charts make it difficult to see small yet potentially significant differences or changes when used as a comparison tool. The bar graph was more effective at showing these differences over a specified timeline in the form of spikes in activity. More minor changes or non-timeline specific issues would be better seen in a pie chart, like looking for which user has more significant activity.

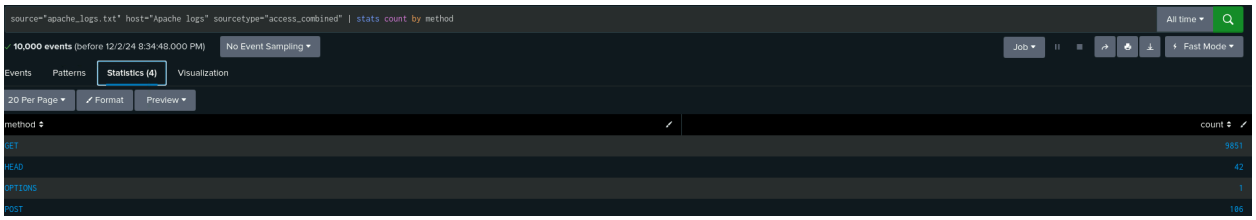
Apache Web Server Log Questions

Report Analysis for Methods

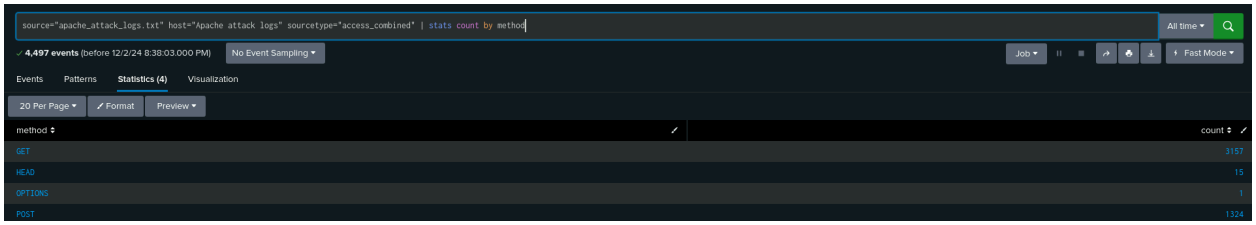
- Did you detect any suspicious changes in HTTP methods? If so, which one?

Yes, we detected suspicious changes in the HTTP methods. Specifically, post Had a drastic increase.

Normal Logs



Attack Logs



- What is that method used for?

POST: Used to send Data to the server from the HTTP client

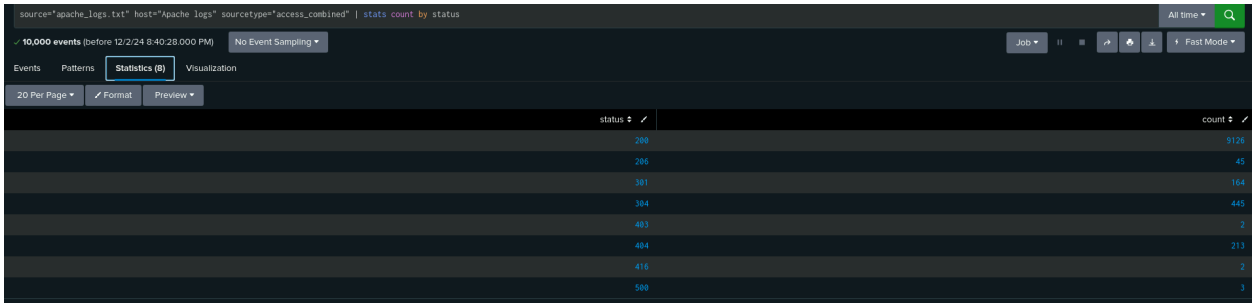
Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

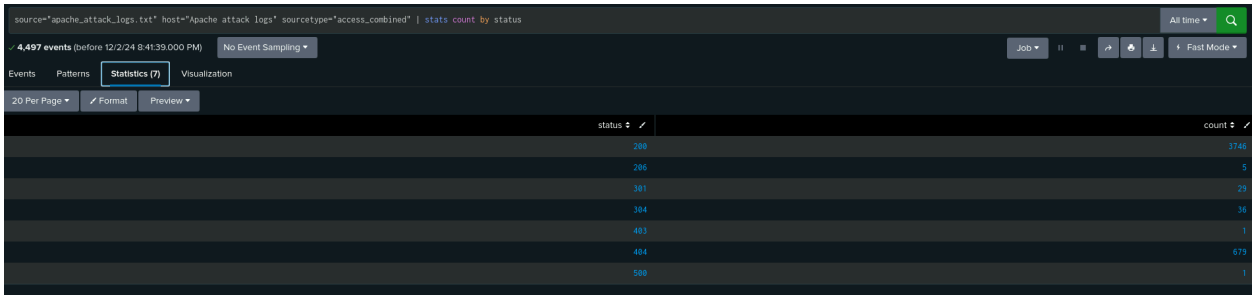
```
Suspicious changes in the results of the top 10 referrer domains (the last five)
```

Report Analysis for HTTP Response Codes

Apache Logs:



Attack Logs:

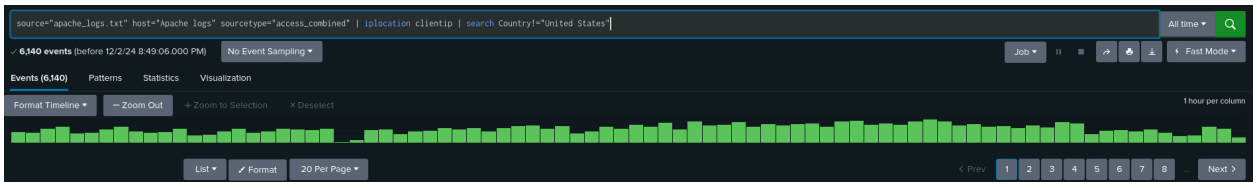


- Did you detect any suspicious changes in HTTP response codes?

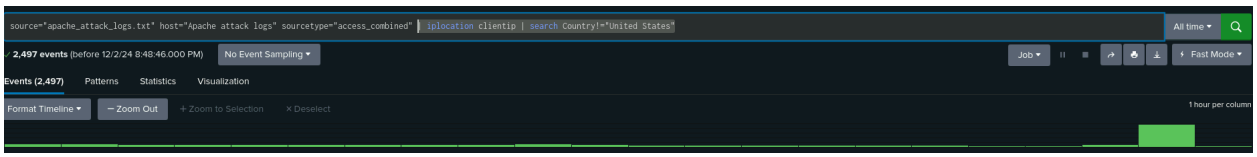
```
There were suspicious changes in the HTTP response codes: response code 200 decreased, while 404 increased.
```

Alert Analysis for International Activity

Normal Logs



Attack Logs



- Did you detect a suspicious volume of international activity?

```
Yes
```

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

```
With a count of 939 at 8:00
```

- Would your alert be triggered for this activity?

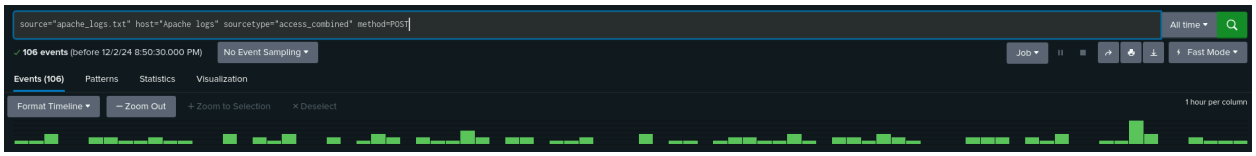
```
Yes, our alert would have been triggered. The threshold was set to more than
150 in an hour, which would trigger an alert.
```

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

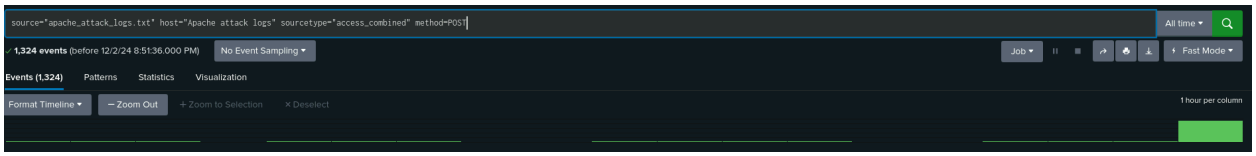
```
There is no evidence that the threshold should be changed.
```

Alert Analysis for HTTP POST Activity

Normal Logs



Attack Logs



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

```
Yes
```

- 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?

```
8pm Wednesday, March 25
```

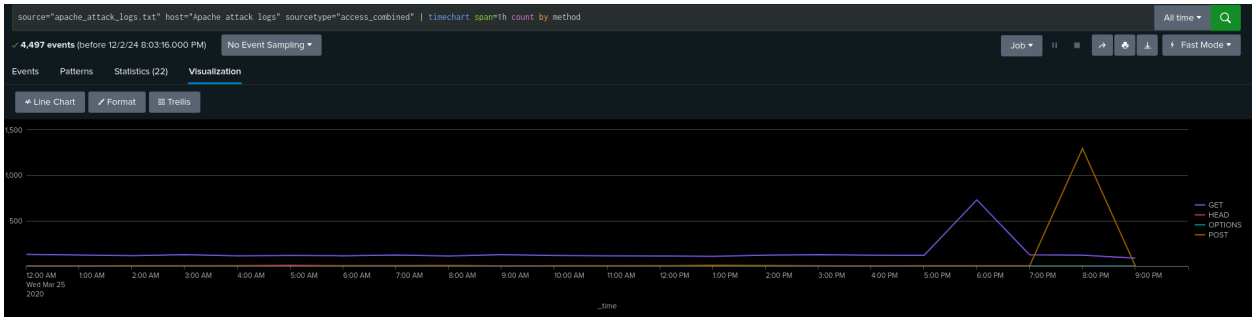
- After reviewing, would you change the threshold that you previously selected?

```
Without further analysis of the daily Apache logs, I would not have changed
the threshold number.
```

Dashboard Analysis for Time Chart of HTTP Methods

Attack Logs

Normal Logs



- Does anything stand out as suspicious?

```
Yes, Notice the difference in the HTTP method time charts.
```

- Which method seems to be used in the attack?

```
Attackers are utilizing a POST based attack.
```

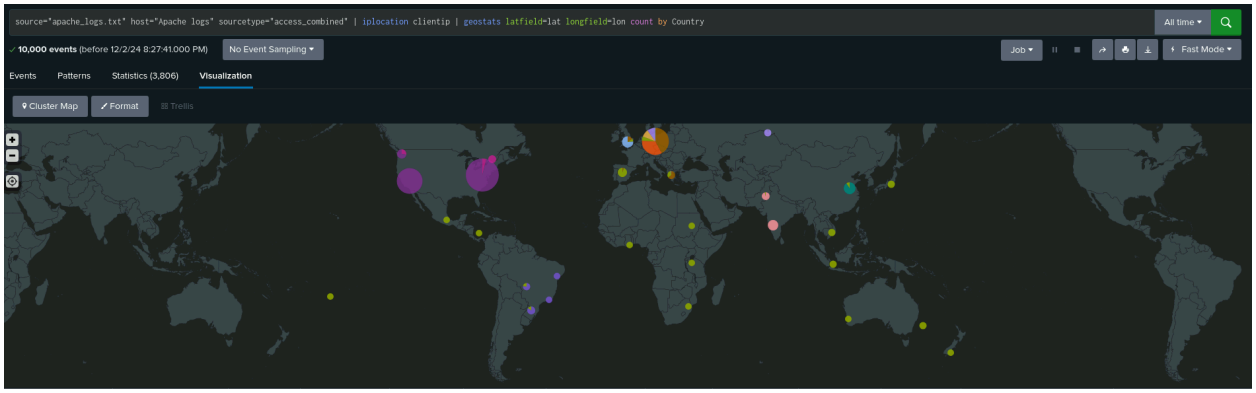
- At what times did the attack start and stop?

```
Between 7:00 PM and 9:00 PM.
```

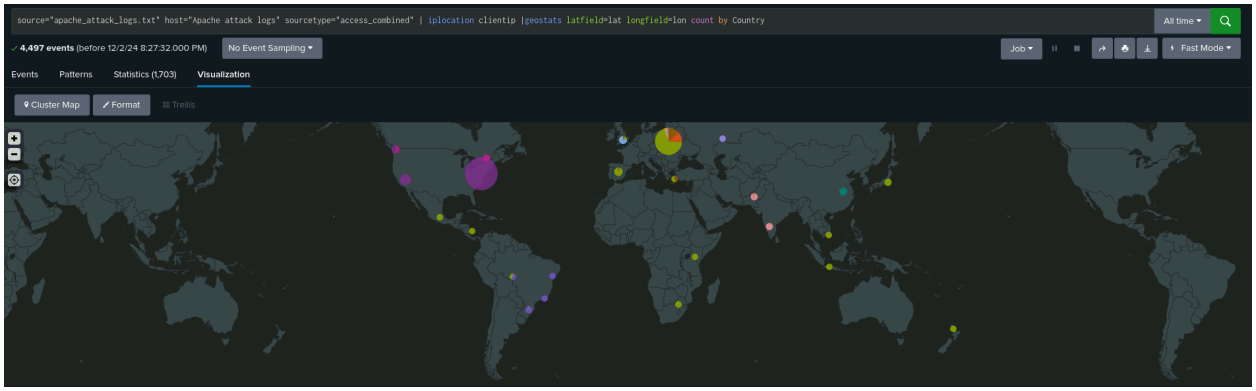
- What is the peak count of the top method during the attack?

```
1296
```

Dashboard Analysis for Cluster Map
Normal Logs



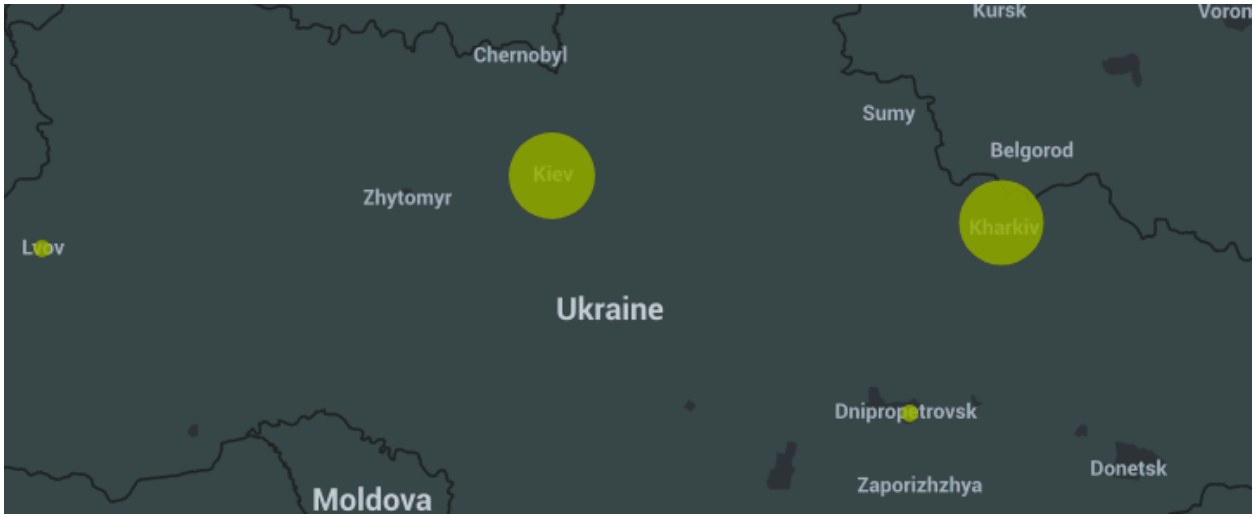
Attack Logs



- Does anything stand out as suspicious?

```
Yes
```

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



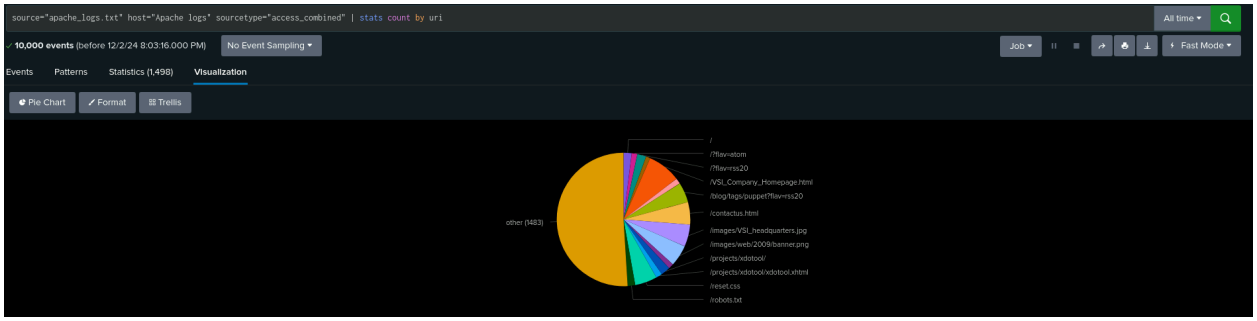

```
Luvov, Kyiv and Kharkiv in Ukraine all showed an increase in activity.
```

- What is the count of that city?

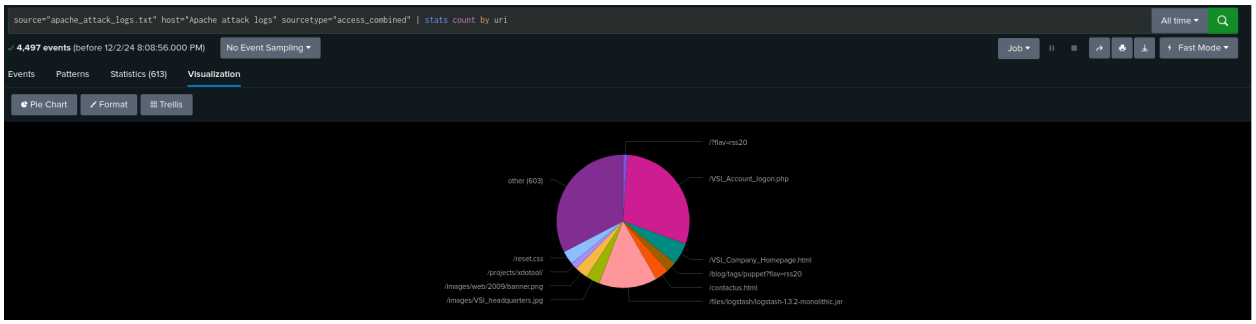
```
Kyiv = 439
Kharkiv = 433
Lvov = 4
```

Dashboard Analysis for URI Data

Normal Logs



Attack Logs



- Does anything stand out as suspicious?

```
Yes
```

- What URI is hit the most?

```
The Uri hit the most is VSI_Account_logon.php
```

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

```
The Attacker could be attempting a Brute force or an SQL injection.
Factoring in the large number of 404 errors would help narrow down an
attacker scanning the network via brute force to gain information through
reconnaissance.
```