Cybersecurity

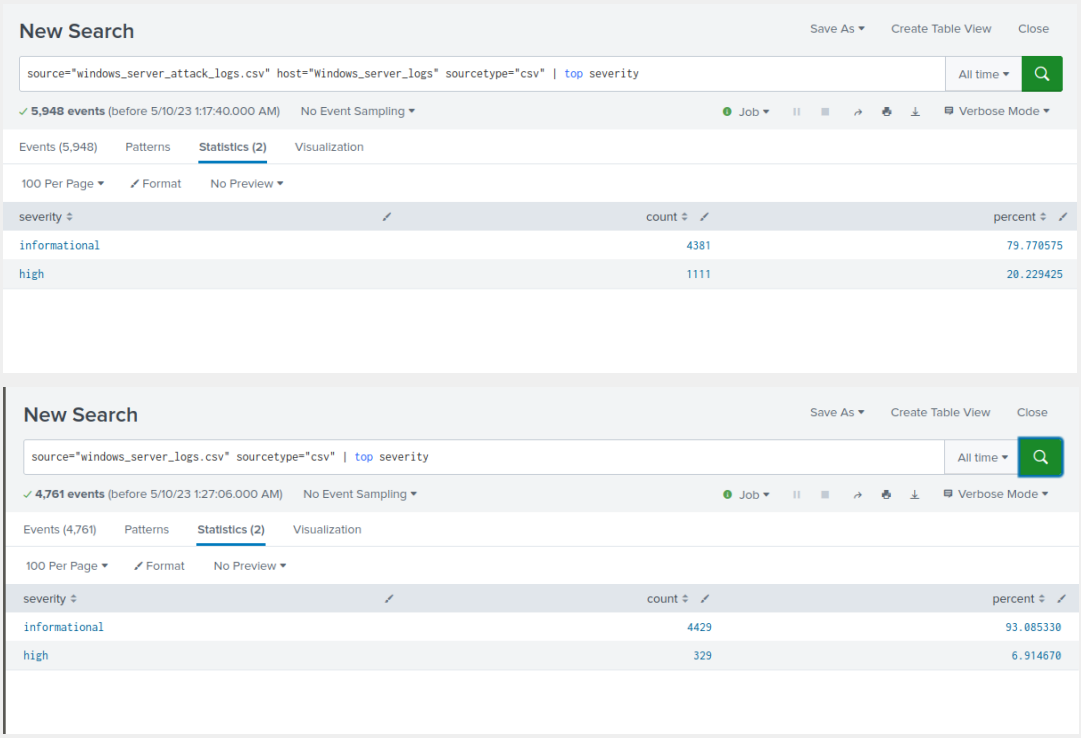
Project 3 Review Questions

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

Windows Server Log Questions

Report Analysis for Severity

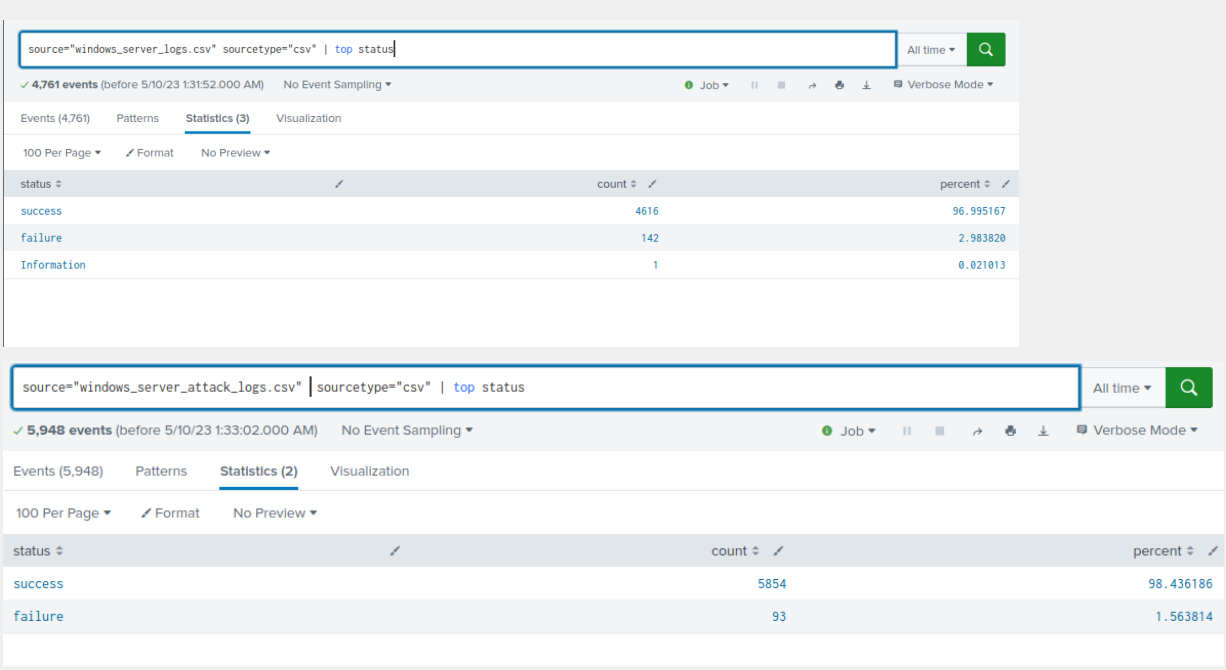
- Did you detect any suspicious changes in severity?



Information went from 93% to 80%. High went from 7% to 13%. This suggests there may suspicious changes in severity

Report Analysis for Failed Activities

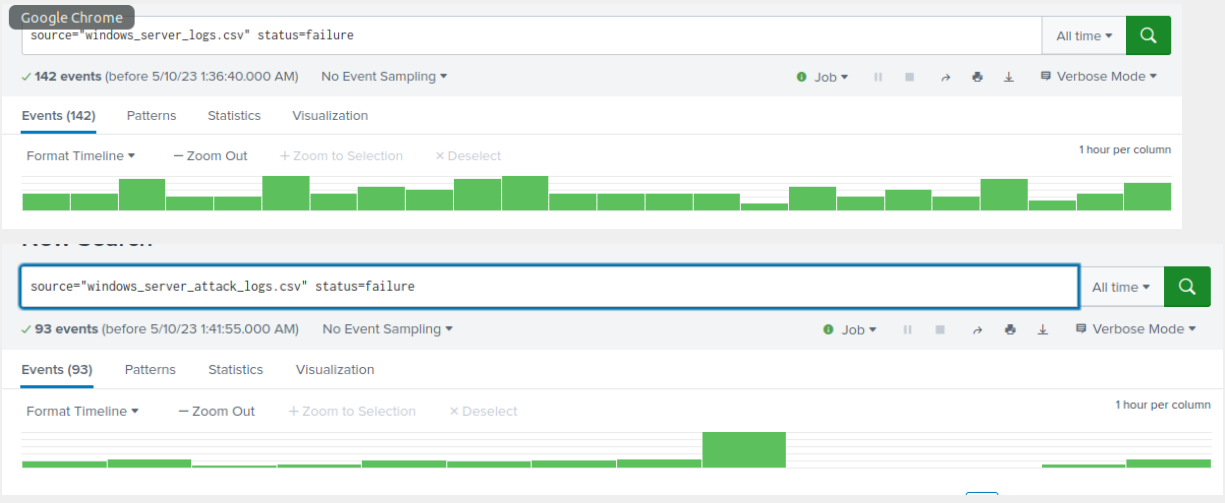
- Did you detect any suspicious changes in failed activities?



Success went from 97% to 98%. Failure went from 3% to 2%. This suggests there were no major changes in failed activities.

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?



```
There was suspicious volume of failed activity at March 25th @ 8am
```

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

```
The account of events that occurred at 8am March 25th was 35.
```

- When did it occur?

```
It occurred on Wednesday March 25th 2020
```

- Would your alert be triggered for this activity?

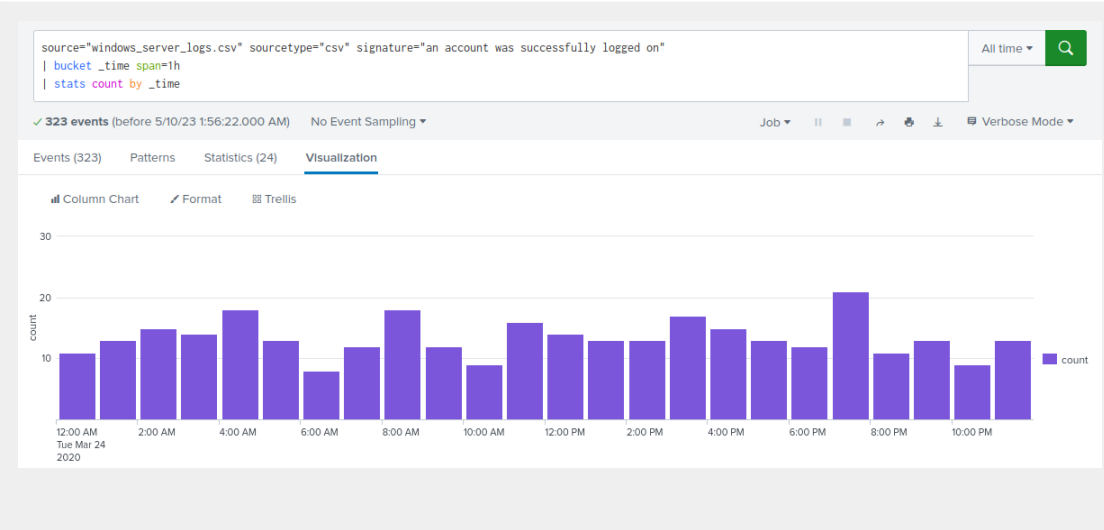
```
yes , my alert would be triggered by this event
```

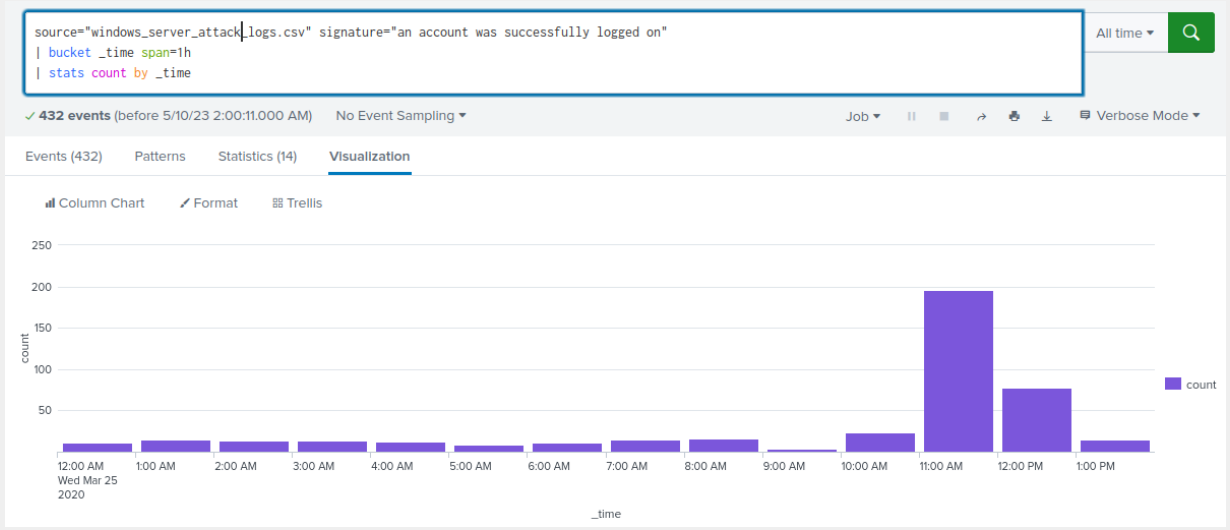
- After reviewing, would you change your threshold from what you previously selected?

```
As of now I would not change the threshold.
```

Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?



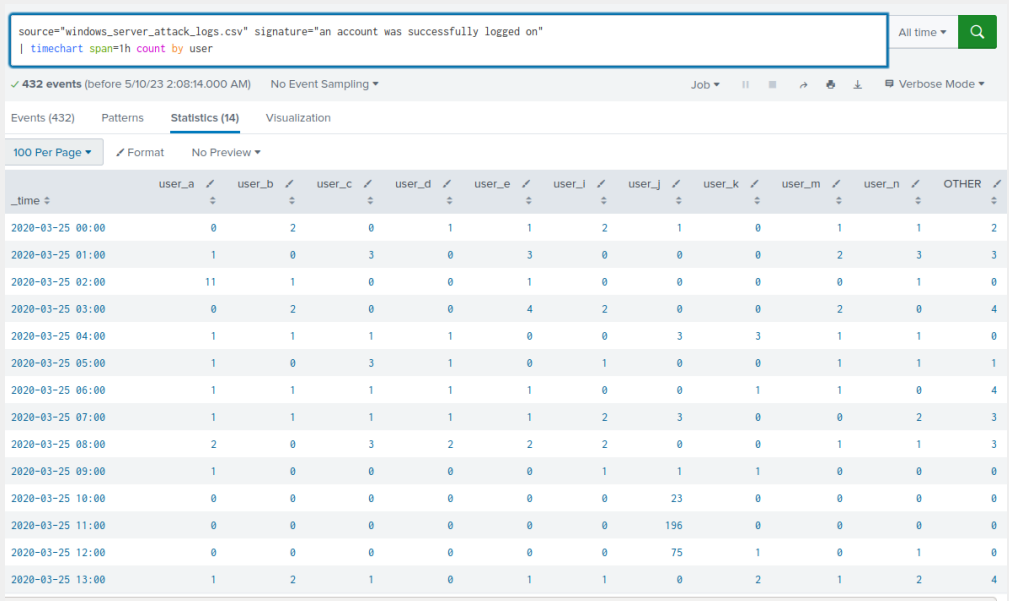


It looks as though there may have been suspicious activity at 11Am and 12pm

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

There was 196 events at 11am and 77 events at 12pm

- Who is the primary user logging in?



_time	user_a	user_b	user_c	user_d	user_e	user_i	user_j	user_k	user_m	user_n	OTHER
2020-03-25 00:00	0	2	0	1	1	2	1	0	1	1	2
2020-03-25 01:00	1	0	3	0	3	0	0	0	2	3	3
2020-03-25 02:00	11	1	0	0	1	0	0	0	0	1	0
2020-03-25 03:00	0	2	0	0	4	2	0	0	2	0	4
2020-03-25 04:00	1	1	1	1	0	0	3	3	1	1	0
2020-03-25 05:00	1	0	3	1	0	1	0	0	1	1	1
2020-03-25 06:00	1	1	1	1	1	0	0	1	1	0	4
2020-03-25 07:00	1	1	1	1	1	2	3	0	0	2	3
2020-03-25 08:00	2	0	3	2	2	2	0	0	1	1	3
2020-03-25 09:00	1	0	0	0	0	1	1	1	0	0	0
2020-03-25 10:00	0	0	0	0	0	0	23	0	0	0	0
2020-03-25 11:00	0	0	0	0	0	0	196	0	0	0	0
2020-03-25 12:00	0	0	0	0	0	0	75	1	0	1	0
2020-03-25 13:00	1	2	1	0	1	1	0	2	1	2	4

User_j was the primary user logging in

- When did it occur?

```
The activity occurred at 11am and 12pm on Wednesday March 25th
```

- Would your alert be triggered for this activity?

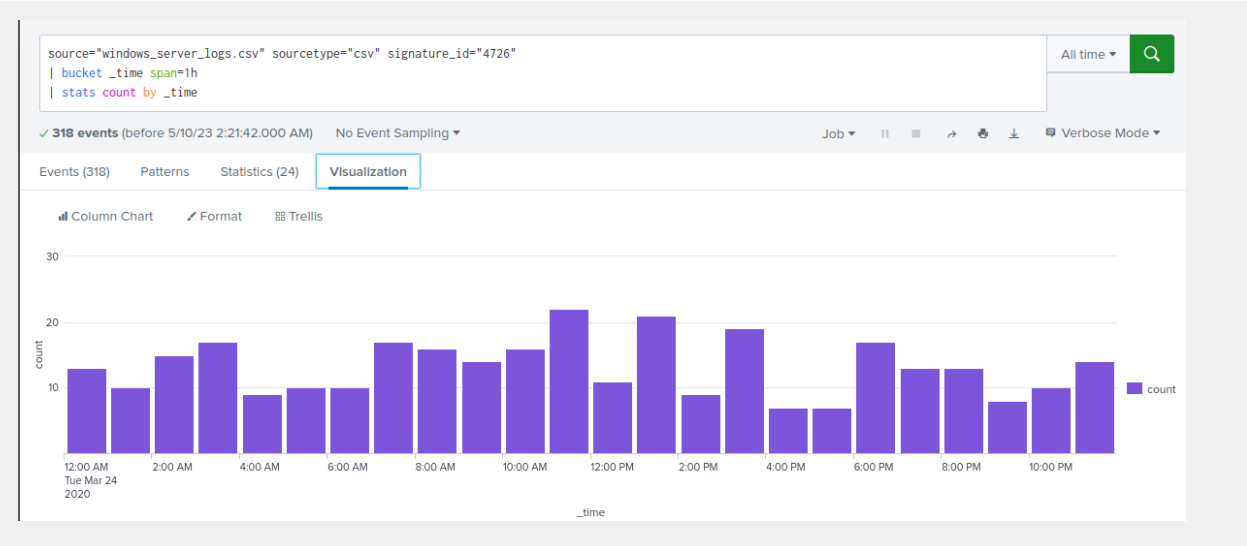
```
The activity at those times went over the threshold so it would have been triggered
```

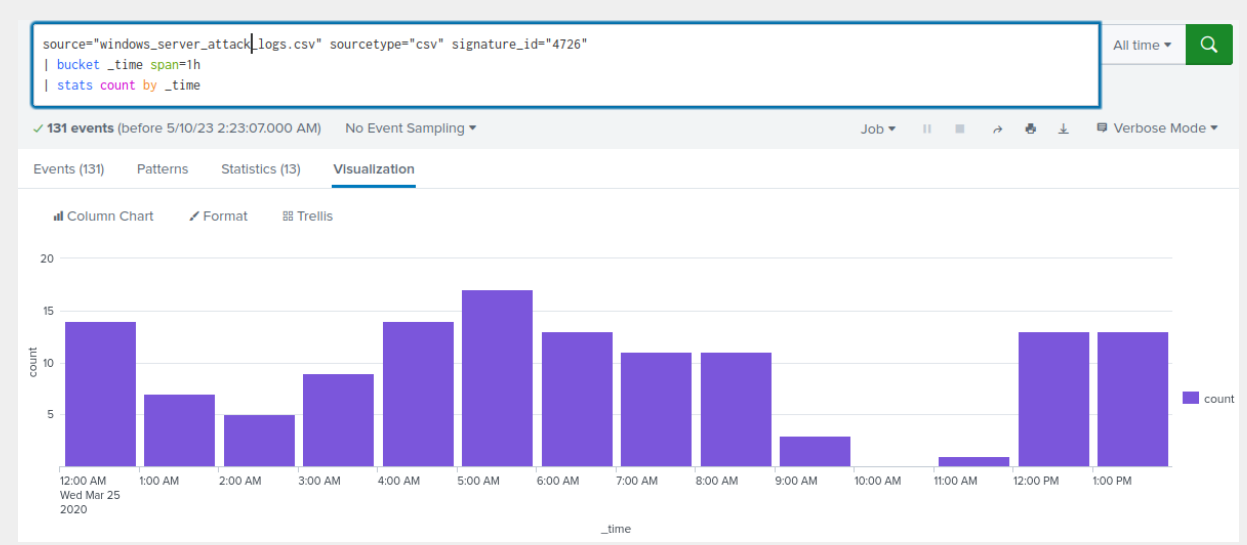
- After reviewing, would you change your threshold from what you previously selected?

```
No, i would not change my threshold
```

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

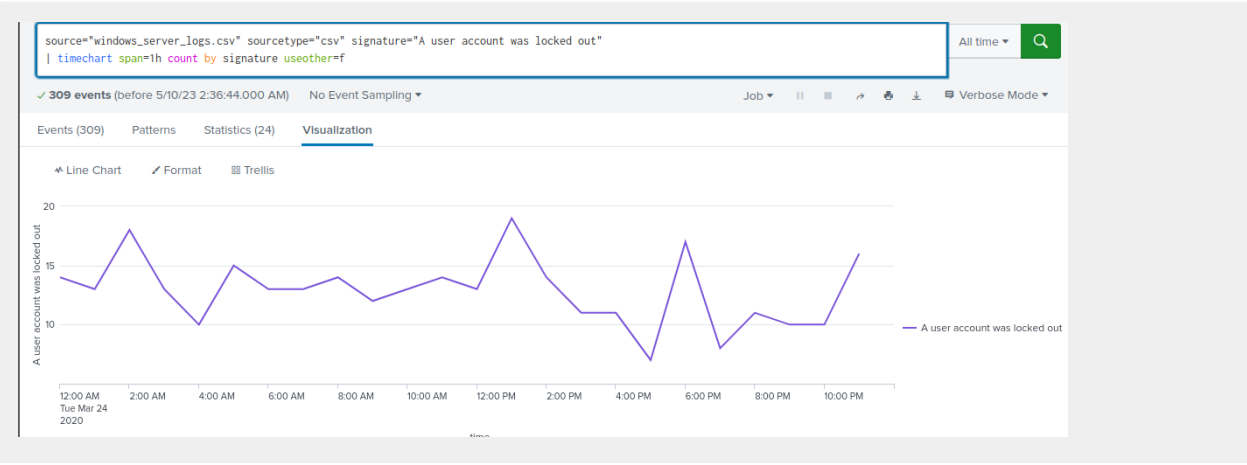


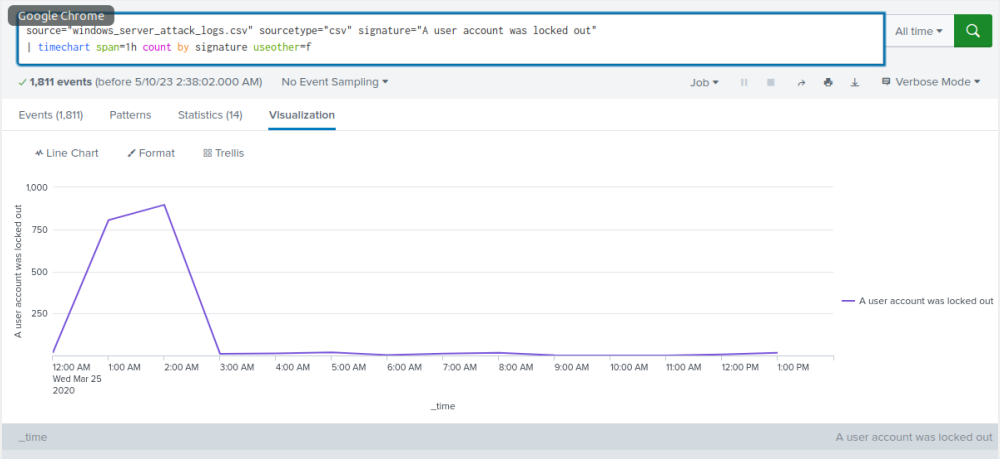


I do not see any suspicious activity.

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?





Yes

- What signatures stand out?

“A user Account was locked out” was the signature that stood out to me

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

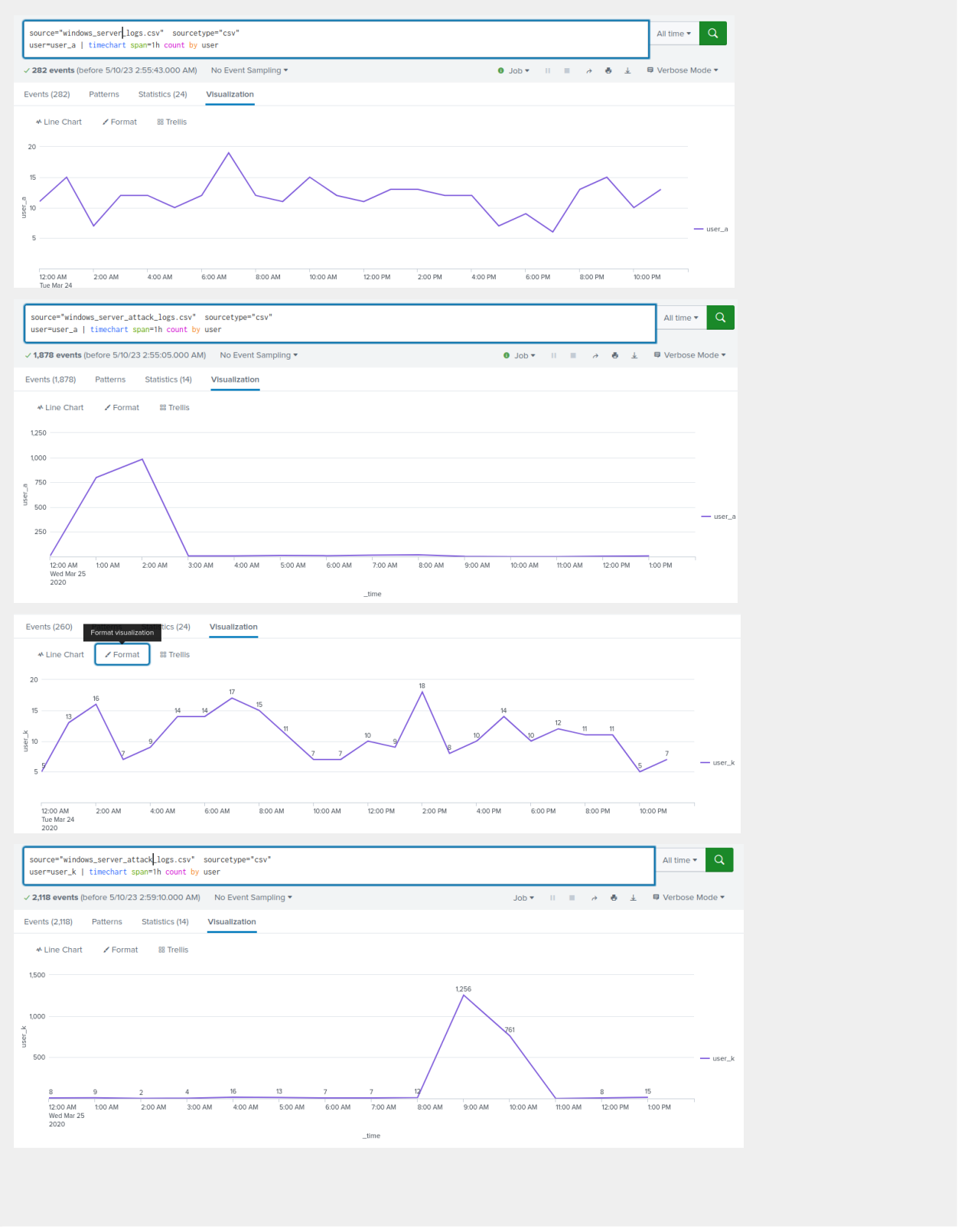
It started at 12am and went to 3am on wednesday March 25th.

- What is the peak count of the different signatures?

“A user account was locked out” peaked at 896

Dashboard Analysis for Users

- Does anything stand out as suspicious?



- Which users stand out?

```
The users that stand out are user_a & user_k.
```

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

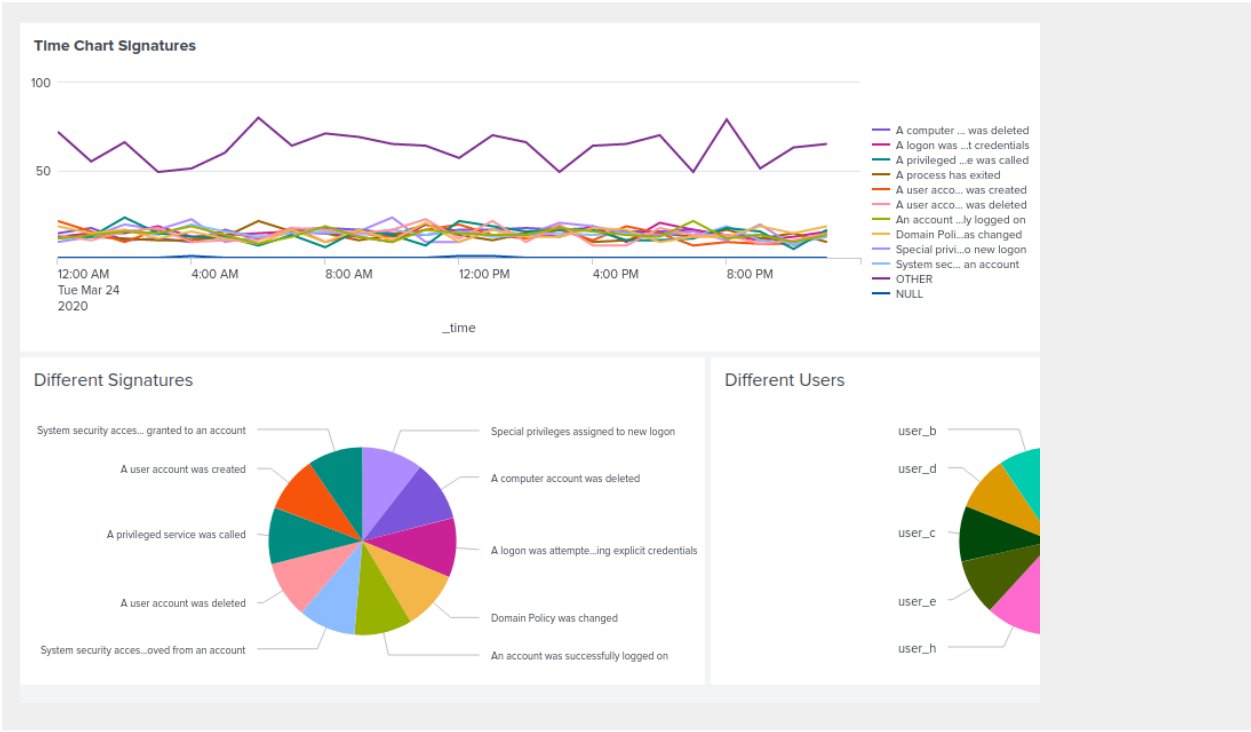
```
User_a started at 12am and ended at 3am on Wednesday March 25th
User_k started at 8am and ended at 11am on Wednesday March 25th
```

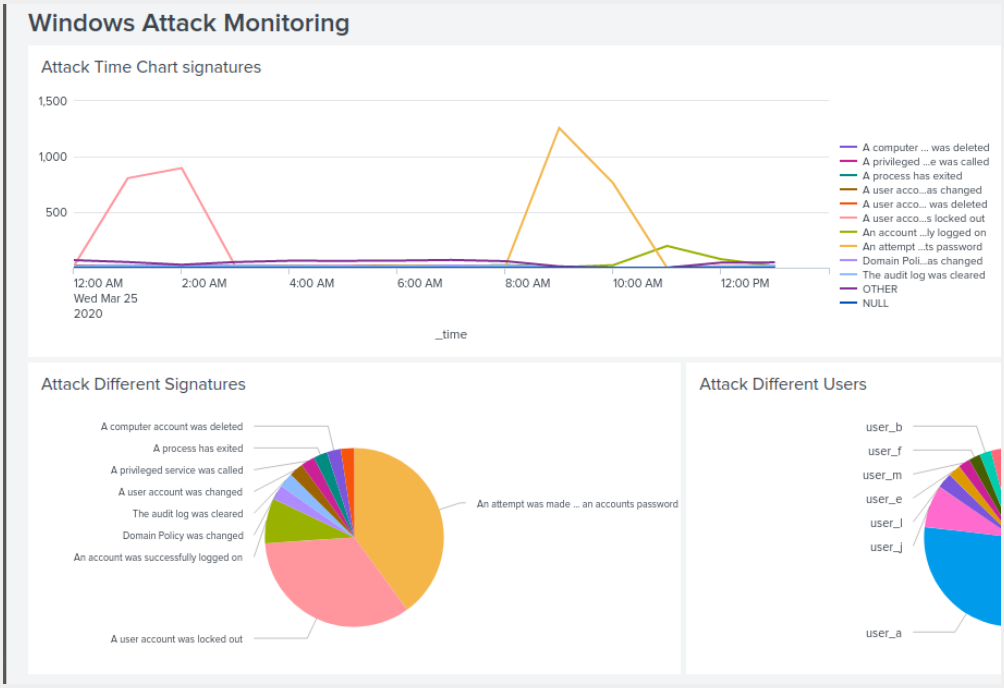
- What is the peak count of the different users?

```
User_a peak count was 984
User_k peak count was 1256
```

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

- Does anything stand out as suspicious?





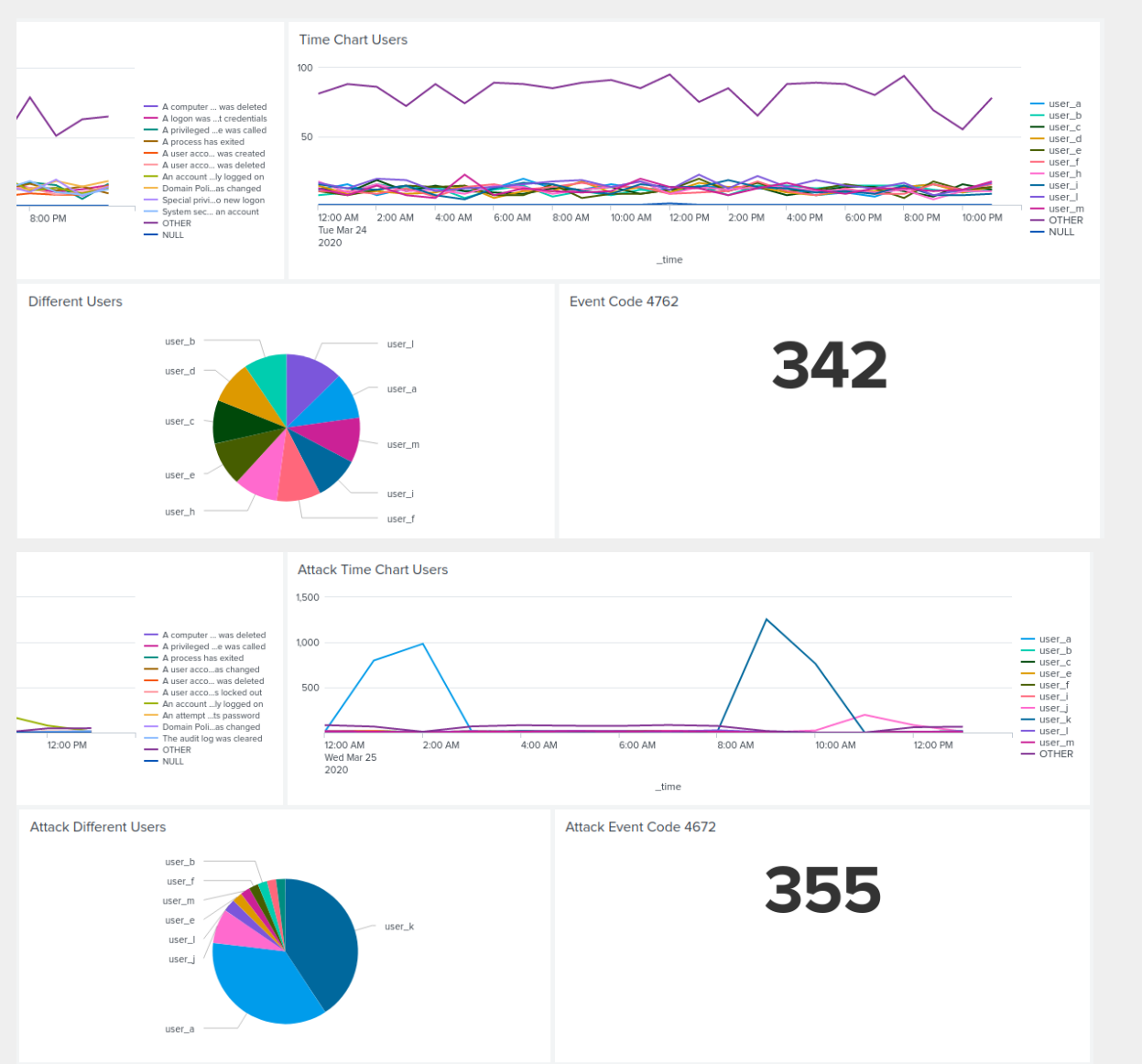
Yes the signatures that have suspicious activity are, An attempt was made to reset an accounts password and A user was locked out. As you can see they both peaked on the attack monitoring which is out of the ordinary.

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

Yes the results match my findings in my time chart for signatures

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

- Does anything stand out as suspicious?



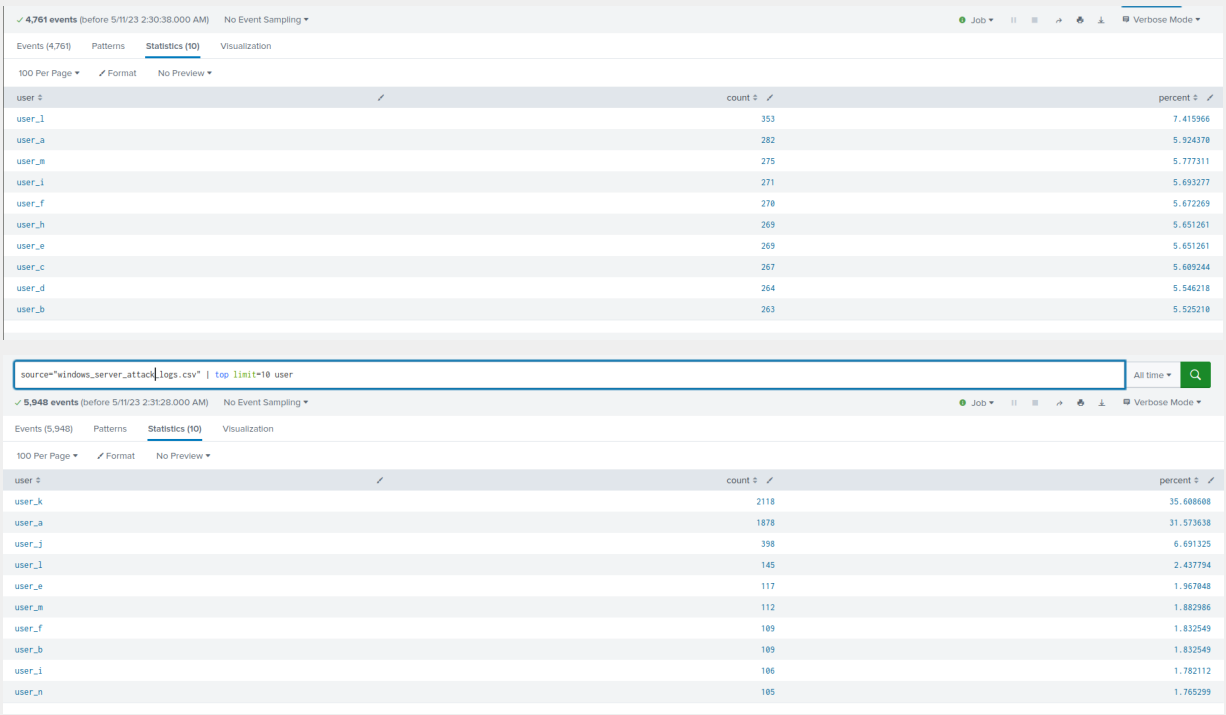
There was obvious suspicious activity on the attack charts. User_a and user_k look to be the culprits looking at my charts.

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

Yes, the results match my findings in my time chart 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?



Statistical charts help analyze data in detail and show patterns and trends. They can be complex but offer advanced calculations. Dashboard graphs and charts look nice and are customizable. They simplify data and integrate it from different sources. However, they may oversimplify complex data and have fewer analysis options. Both types have their strengths, so you choose based on what you need. We would use statistical charts for in-depth analysis, and dashboard graphs for visually appealing presentations

Apache Web Server Log Questions

Report Analysis for Methods

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

Yes we saw a decrease in GET activity by about 28% and an increase in POST activity by about 28%.

- What is that method used for?

```
GET is used to retrieve data from a web server, and POST is used to submit data like a comment to a web server.
```

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

```
There is no suspicious activity because the referred domains are similar in both logs.
```

Report Analysis for HTTP Response Codes

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

```
There were slight changes in the percentage of the HTTP response code, but there was one outlier. HTTP response code 404 went from 2% to 15%.
```

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

```
Yes there was a big rise in activity in Ukraine at 8:00 p.m. on March 25th.
```

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

```
There was a count of 864 events from Ukraine during the 8:00 p.m attack.
```

- Would your alert be triggered for this activity?

```
Yes the alert would be triggered since we set the threshold at 140.
```

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

```
We may need to raise the threshold by a little in order to avoid false positive alerts.
```

Alert Analysis for HTTP POST Activity

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

```
Yes there was a suspicious increase in POST activity in one hour.
```

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

```
There was a count of 1,296 events, and if you look closely you can see that
all the 1,296 events happened in 1 minute at 8:05 p.m.
```

- When did it occur?

```
The exact time of the attack was Wednesday, March 25 2020 at 8:05 p.m.
```

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

```
Like the first alert I would raise the threshold because it was at 10 events
in an hour, and we just saw 1,296 events in one hour.
```

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

```
There was suspicious activity with the methods GET and POST with each of
them having spikes on March 25, 2020 from 5:00 p.m. to 9:00 p.m.
```

- Which method seems to be used in the attack?

```
Both GET and POST seemed to be used in the attack.
```

- At what times did the attack start and stop?

```
The GET attack happened on March 25, 2020 from 5:00 p.m. to 7:00 p.m. The
POST attack happened on March 25, 2020 from 7:00 p.m. to 9:00 p.m.
```

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

```
The peak count for the GET attack was 729, and the peak count for the POST attack was 1,296.
```

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

```
Yes there was a huge spike in activity in Ukraine. During the normal apache log there were only 88 events from Ukraine, and in the attack log there were 877 events.
```

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

```
Both locations with spiked activity were in Ukraine. One was in the city of Kiev and the other was in Kharkiv.
```

- What is the count of that city?

```
The count for Kiev was 439 and the count for Kharkiv was 433.
```

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

```
There was suspicious activity with the URI /files/logstash/logstash-1.3.2-monolithic.jar from 6:00 p.m to 7:00 p.m. on Wednesday, March 25 2020 with a count of 624 during that time. There was also suspicious activity with the URI /VSI_Account_logon.php from 8:00 p.m. to 9:00 p.m. on Wednesday, March 25 2020 with a count of 1,296 during that time.
```

- What URI is hit the most?

```
/VSI_Account_logon.php hit the most with a count of 1,323.
```

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

```
Since the URI with the most events was /VSI_Account_logon.php the attacker
could be trying to attempt a brute force attack on the VSI logon page.
```