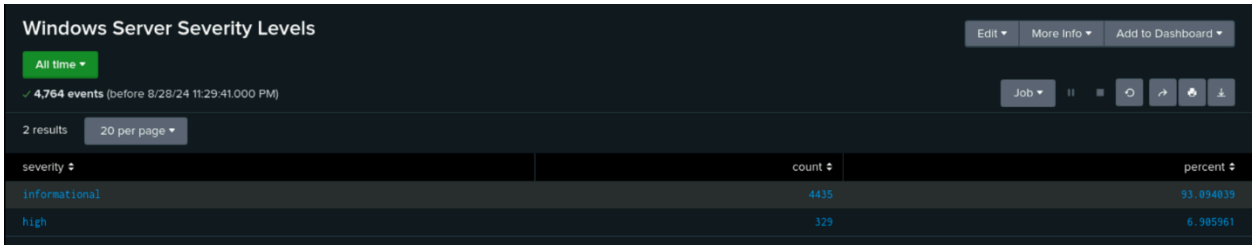
Cybersecurity

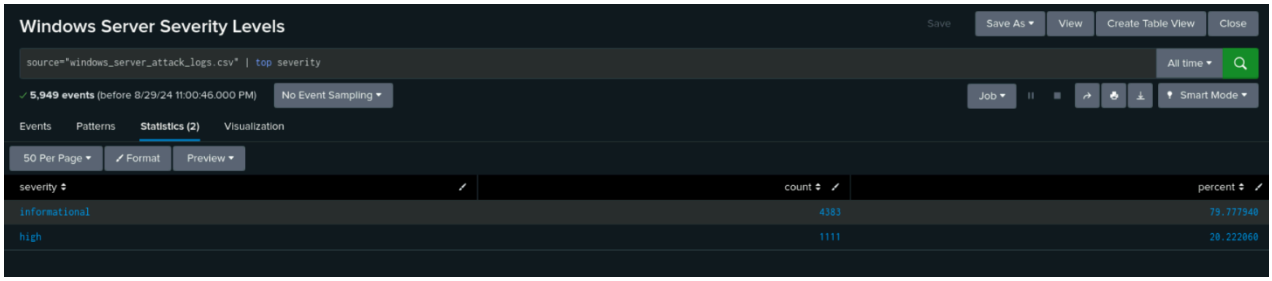
Project 3 Review Questions

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

Windows Server Log Questions

Report Analysis for Severity

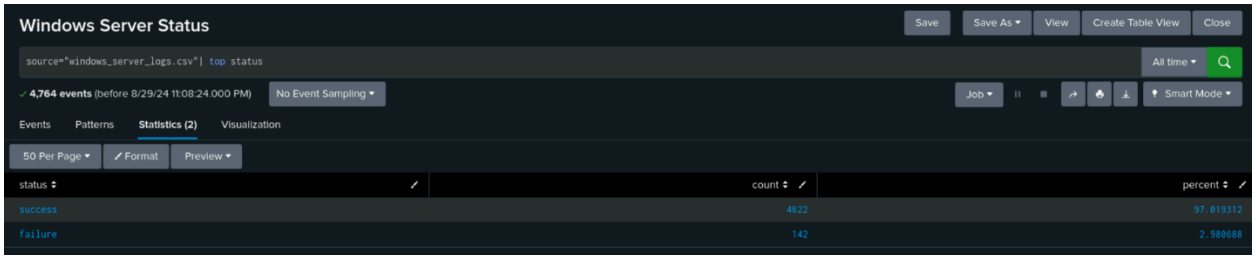


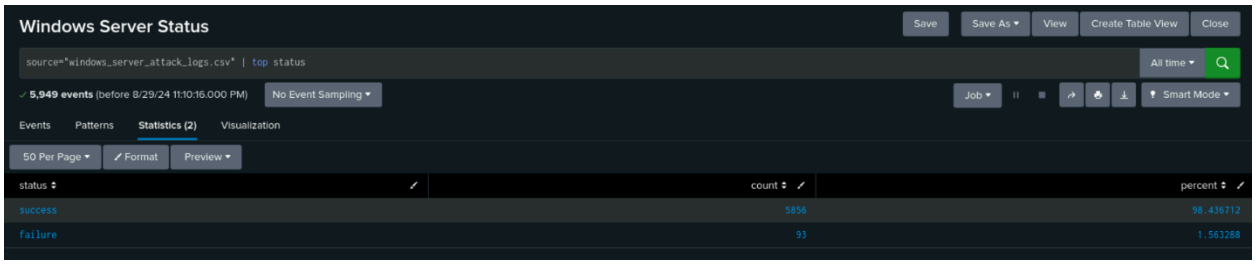


- Did you detect any suspicious changes in severity?

A significant shift in severity was observed. Informational severity decreased by 13%, from 93% to 80%. Equally, High severity events increased by 13%, rising from 7% to 20%. We consider these changes suspicious.

Report Analysis for Failed Activities

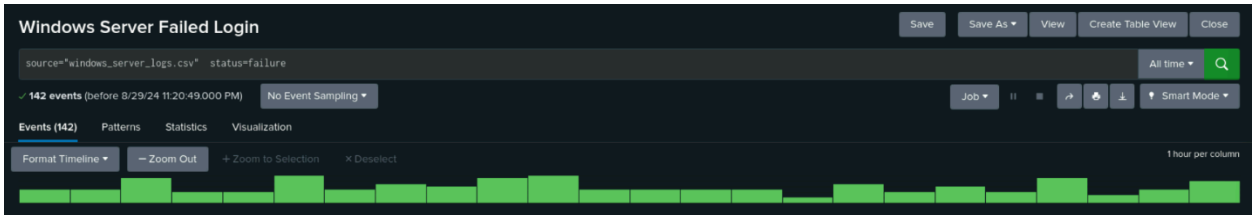


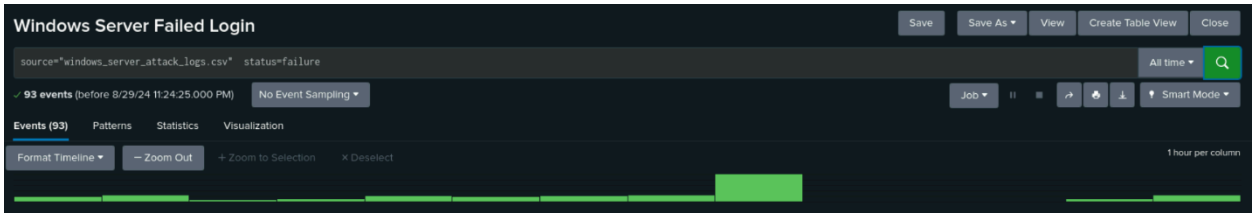


- Did you detect any suspicious changes in failed activities?

There were no significant changes in failed activities that would be considered suspicious. The failed activities decreased by 1%, from 3% to 2%, while successful activities increased by 1%, from 97% to 98%.

Alert Analysis for Failed Windows Activity





- Did you detect a suspicious volume of failed activity?

A high volume of failed activities was detected at 8:00 AM on Wednesday, March 25, 2020.

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

```
The count of failed activity was 35 events.
```

- When did it occur?

```
8:00 AM on Wednesday, March 25, 2020.
```

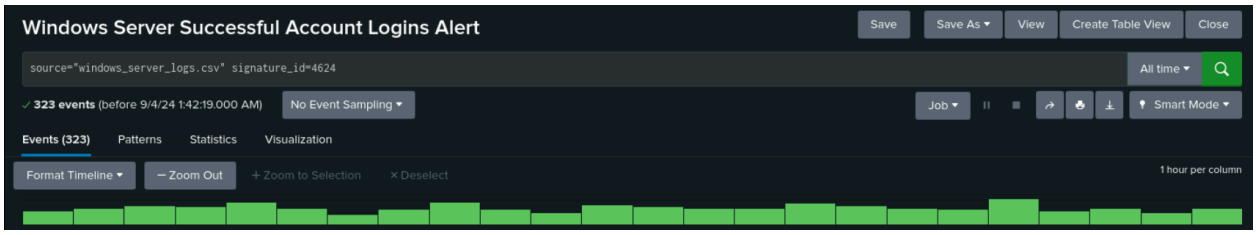
- Would your alert be triggered for this activity?

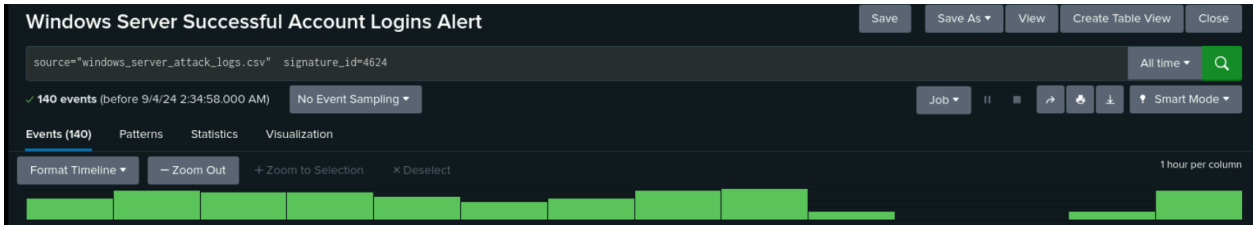
```
Yes, the activity exceeds the threshold.
```

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

```
No change needed.
```

Alert Analysis for Successful Logins





- Did you detect a suspicious volume of successful logins?

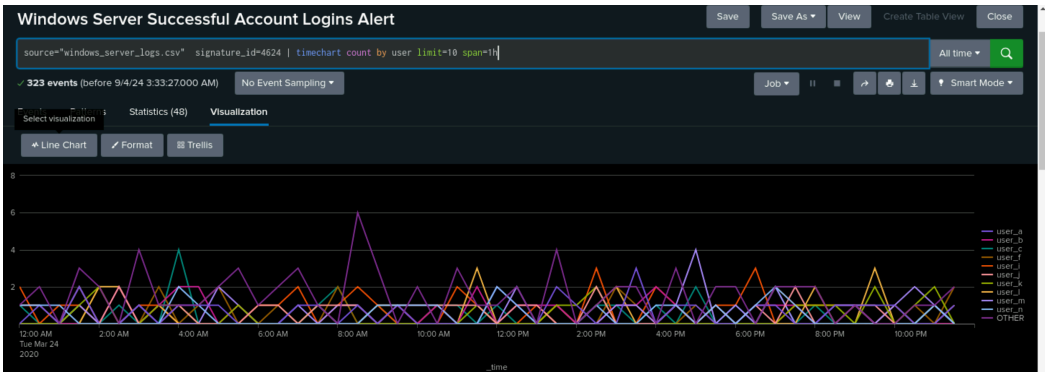
```
The unusually low volume of activity compared to normal levels is
suspicious. Additionally, the complete absence of successful account login
```

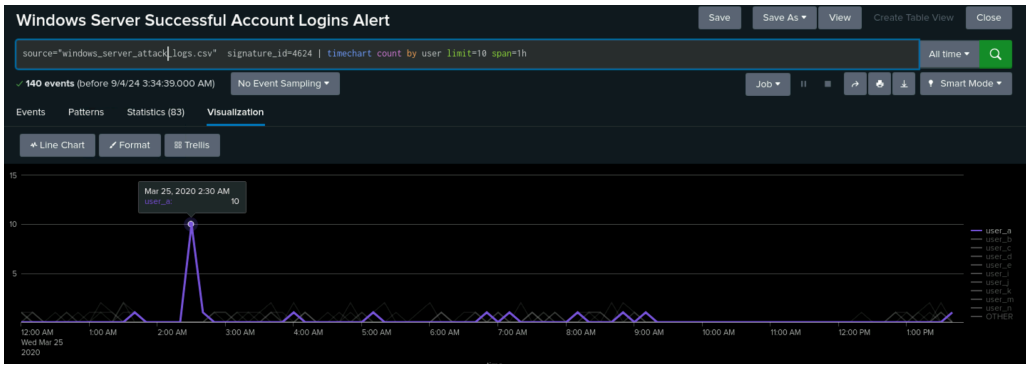
activity between 10 AM and 11 AM on March 25, 2020, is also considered highly unusual and potentially indicative of malicious activity.

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

There was a significant decrease in successful login activity between 8:00 AM and 11:00 AM. The number of successful logins dropped from 16 at 8:00 AM to 4 at 9:00 AM, then to 0 from 10:00 AM to 11:00 AM, before rebounding to 4 at 12 PM.

- Who is the primary user logging in?





We see a significant spike in login activity at 2:30 AM, with a total of 10 login attempts for user_a.

- When did it occur?

The suspicious activity occurred at 2:30 AM on Wednesday, March 25,2020.

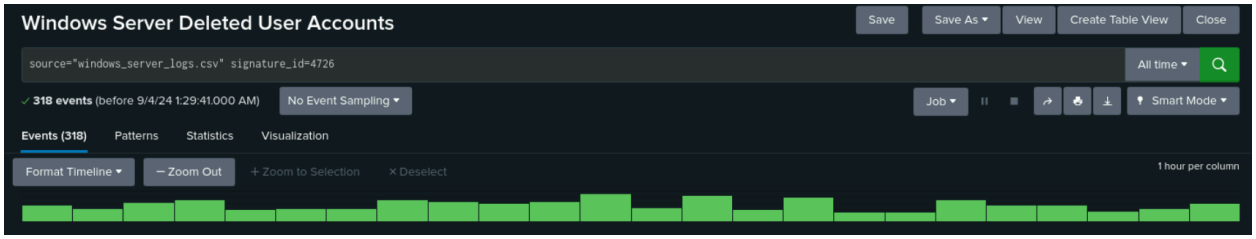
- Would your alert be triggered for this activity?

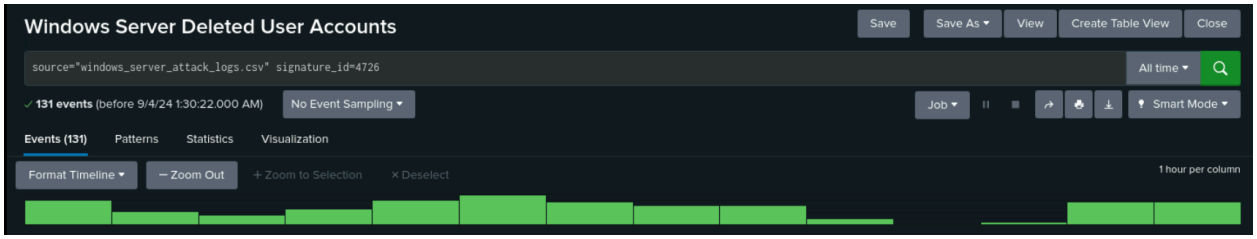
No, our alert would not have been triggered by this activity as we set the threshold count too low, >12 successful logins within an hour to alert the SOC.

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

The current alert threshold is set too low, which leads to false positive alerts being triggered. We would increase the threshold from 12 to 30.

Alert Analysis for Deleted Accounts

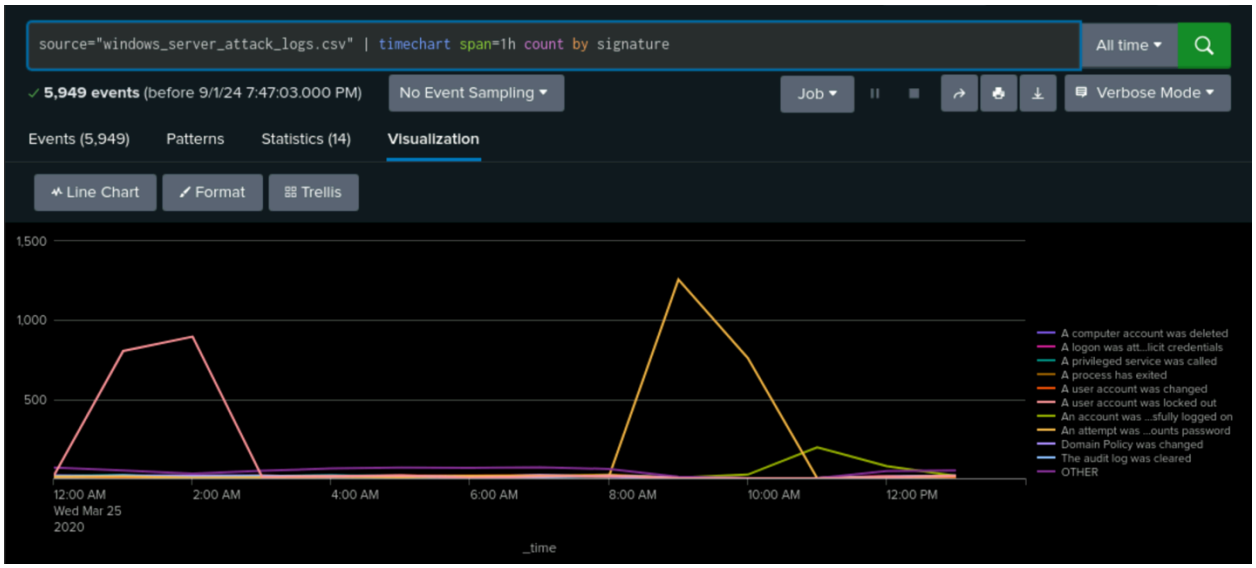




- Did you detect a suspicious volume of deleted accounts?

While we didn't find any unusually high number of deleted accounts, we did notice a significant drop in the number of deleted accounts and a gap in activity between 10:00 AM and 11:00 AM on March 25, 2020. This gap also appears in successful account login signatures, suggesting that the attackers may have been focusing on other methods of attack during this time, such as password reset attempts.

Dashboard Analysis for Time Chart of Signatures



- Does anything stand out as suspicious?

"An account was locked out" showed suspicious activity starting at 12:00 AM to 3:00 AM on Wednesday, March 25,2020, as well signature "An Attempt was made to Reset an Accounts Password" starting at 8:00 AM to 11:00 AM on Wednesday, March 25,2020.

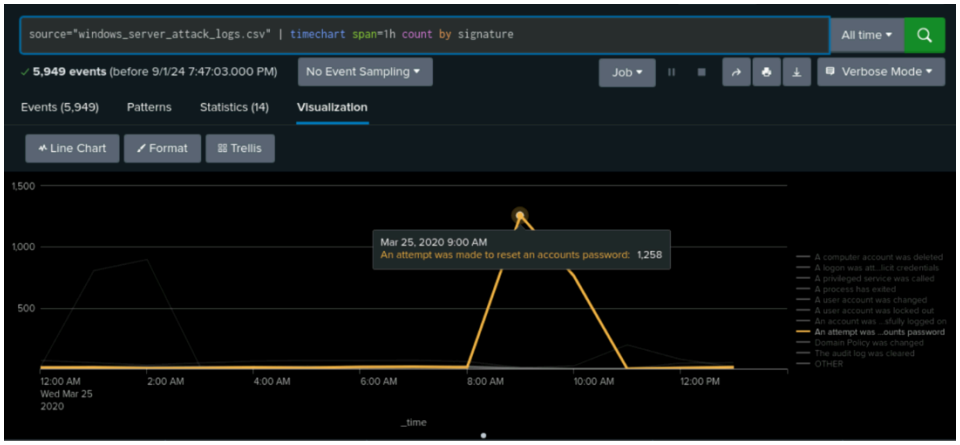
- What signatures stand out?

“An account was locked out” and “An Attempt was made to Reset an Accounts Password”.

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

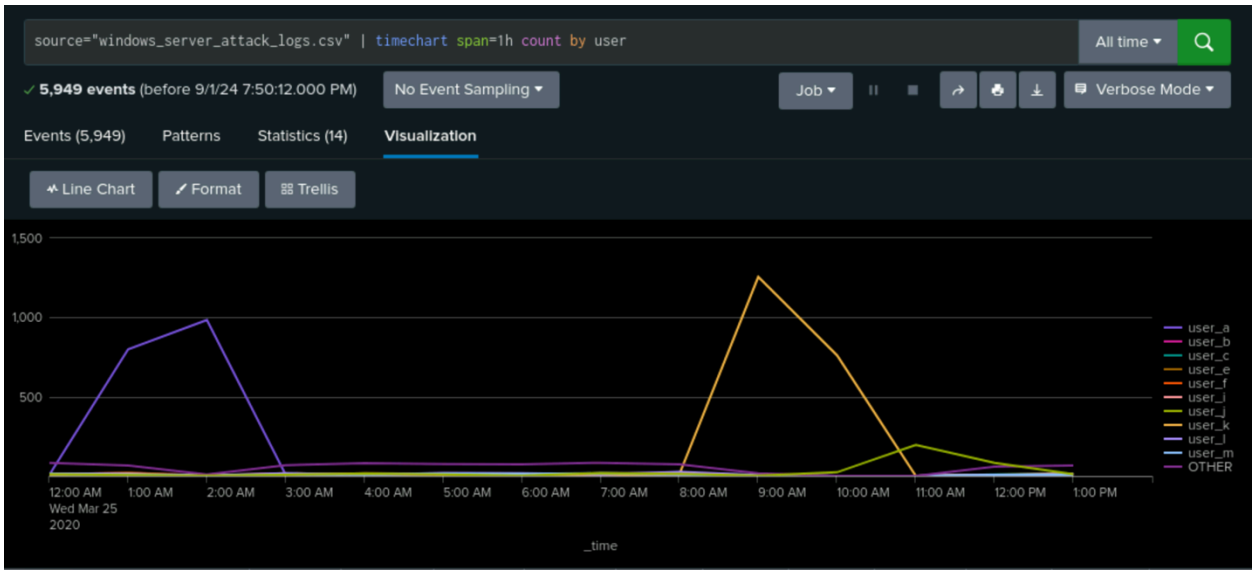
“An account was locked out” - 12:00 AM to 3:00 AM on Wednesday, March 25,2020
“An Attempt was made to Reset an Accounts Password” - 8:00 AM to 11:00 AM on Wednesday, March 25,2020.

- What is the peak count of the different signatures?



“An account was locked out” - 896 counts
“An Attempt was made to Reset an Accounts Password” - 1258 counts

Dashboard Analysis for Users



- Does anything stand out as suspicious?

```
user_a and user_k showed suspicious activity.
user_a at 12am to 3am on Wednesday, March 25, 2020 and user_k at 8am to 11am
on Wednesday, March 25, 2020.
```

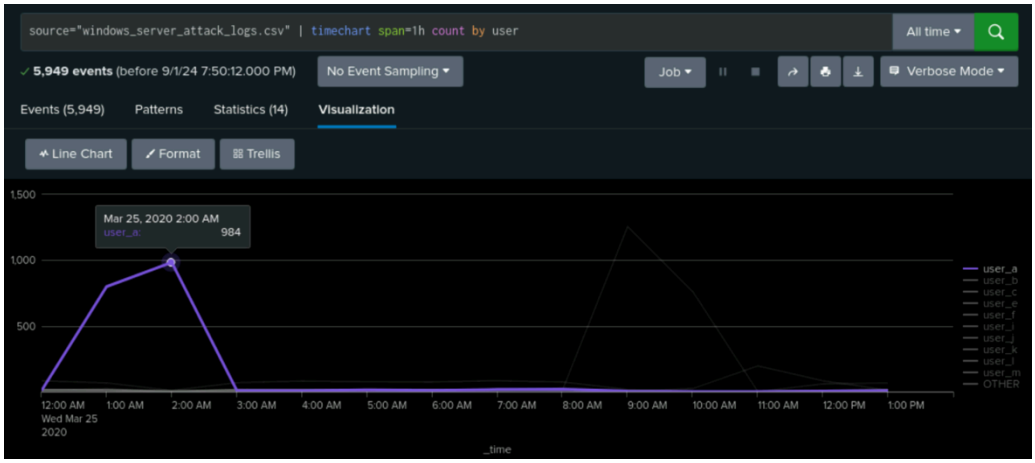
- Which users stand out?

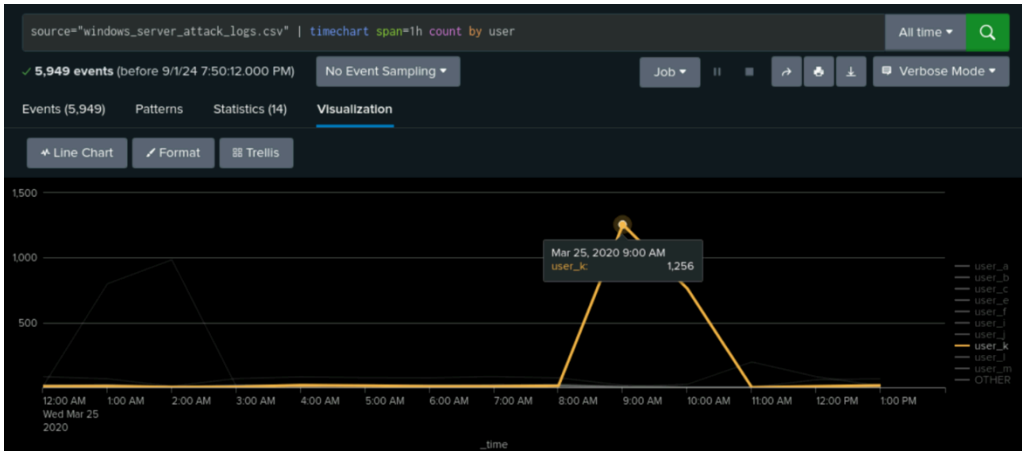
```
user_a and user_k stand out.
```

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

```
user_a - Began at 12:00 AM and stopped at 3:00 AM on Wednesday, March 25, 2020
user_k - Began 8:00 AM and stopped at 11:00 AM on Wednesday, March 25, 2020
```

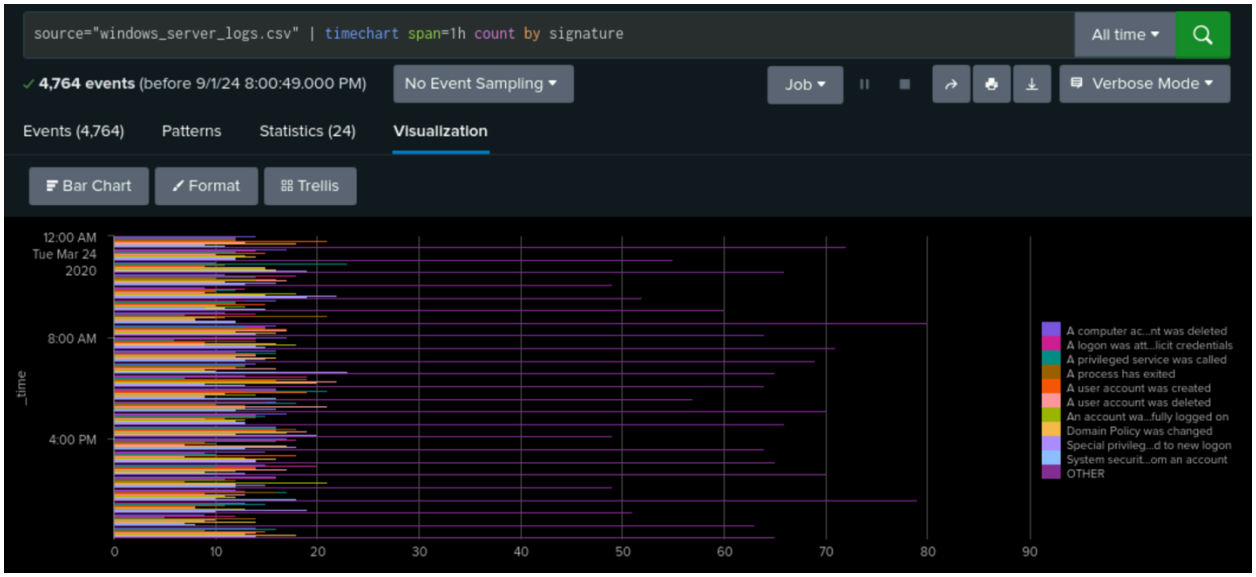
- What is the peak count of the different users?






```
user_a - 984 counts
user_k - 1256 counts
```

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



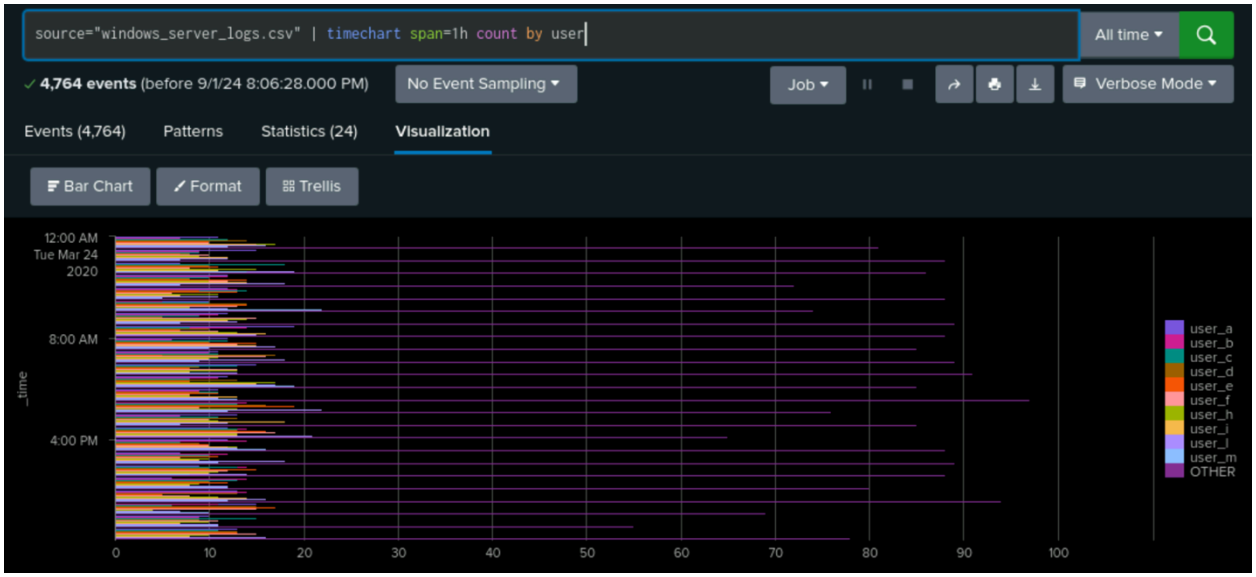
- Does anything stand out as suspicious?

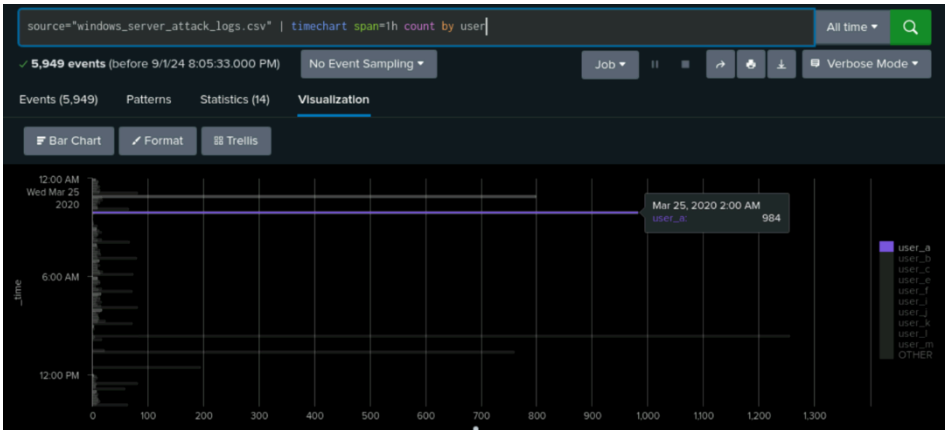
```
There was suspicious activity on Wednesday, March 25, 2020, at 1:00 AM, 2:00 AM, 9:00 AM and 10:00 AM.
```

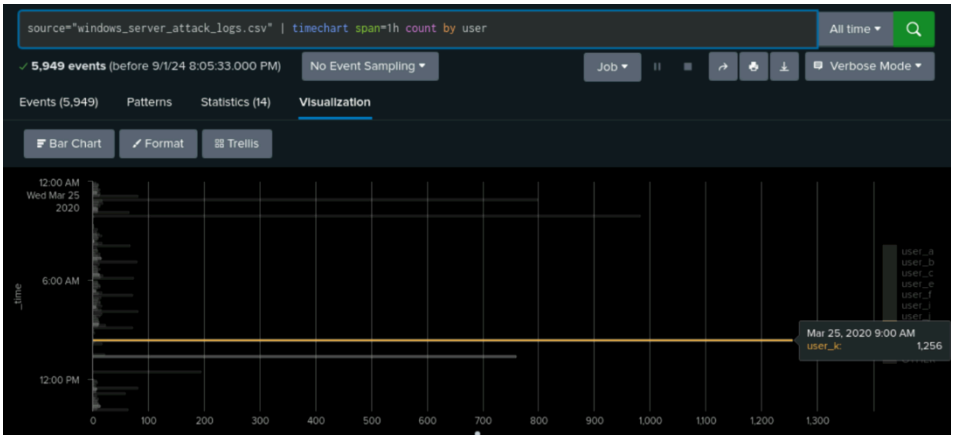
- Do the results match your findings in your time chart for signatures?

```
Yes, they do.
```

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







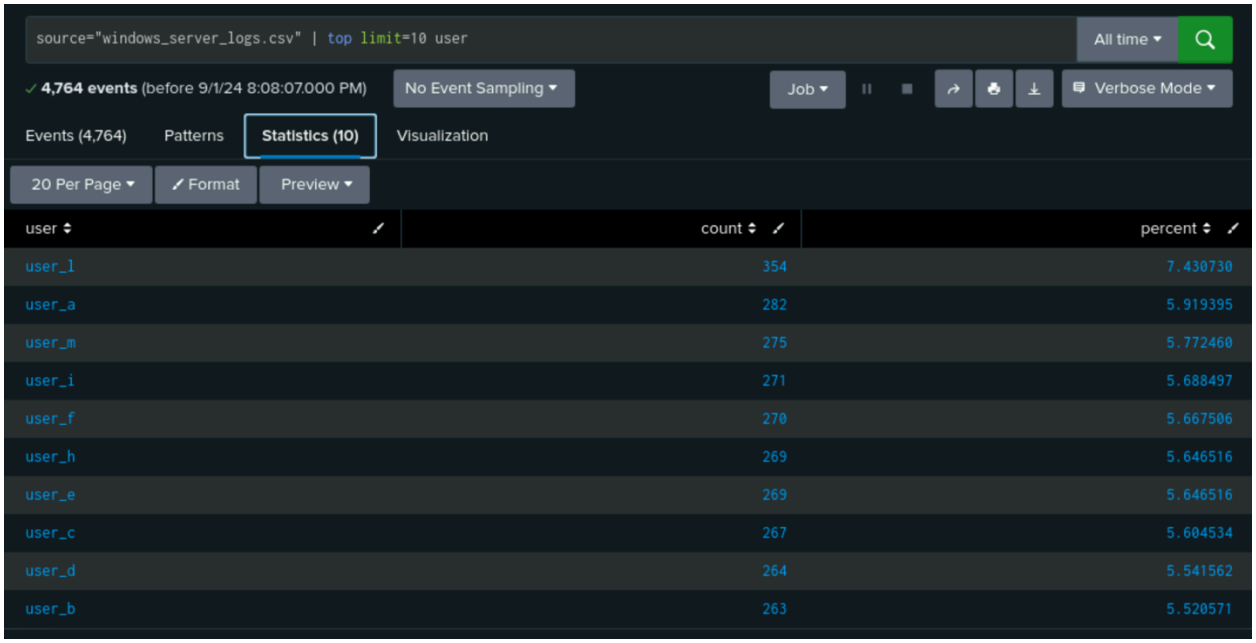
- Does anything stand out as suspicious?

There was suspicious activity on Wednesday, March 25, 2020, at 1:00 AM, 2:00 AM, 9:00 AM and 10:00 AM.

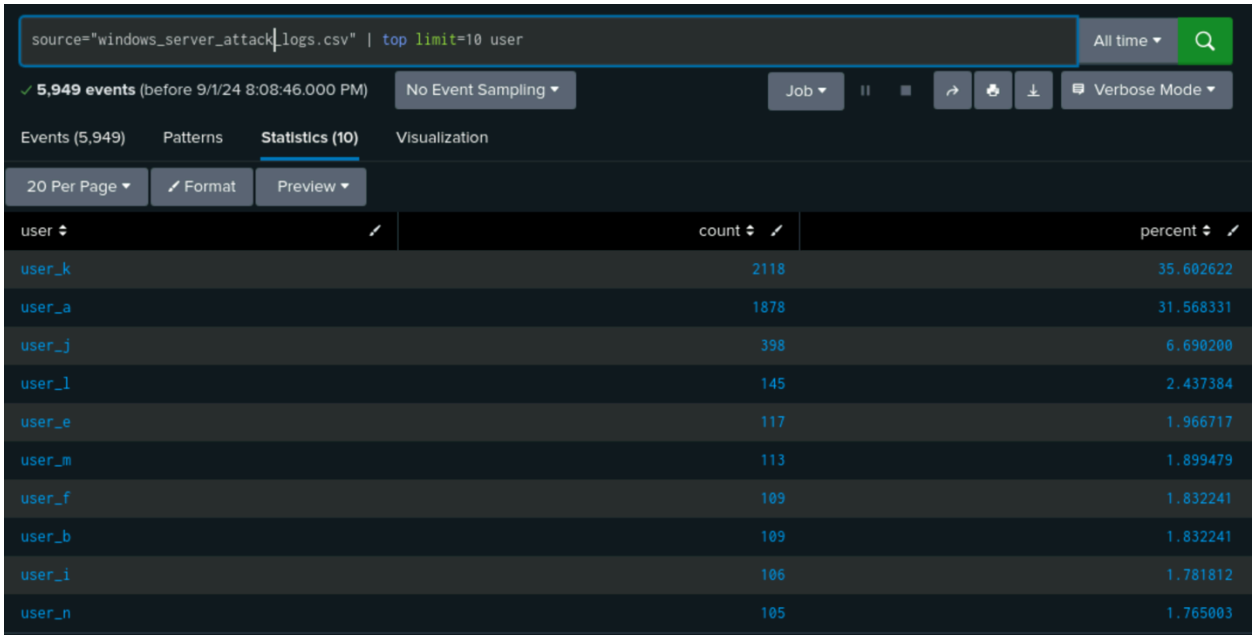
- Do the results match your findings in your time chart for users?

Yes, they do.

Dashboard Analysis for Users with Statistical Charts



user	count	percent
user_l	354	7.430730
user_a	282	5.919395
user_m	275	5.772460
user_i	271	5.688497
user_f	270	5.667506
user_h	269	5.646516
user_e	269	5.646516
user_c	267	5.604534
user_d	264	5.541562
user_b	263	5.520571



user	count	percent
user_k	2118	35.602622
user_a	1878	31.568331
user_j	398	6.690200
user_l	145	2.437384
user_e	117	1.966717
user_m	113	1.899479
user_f	109	1.832241
user_b	109	1.832241
user_i	106	1.781812
user_n	105	1.765003

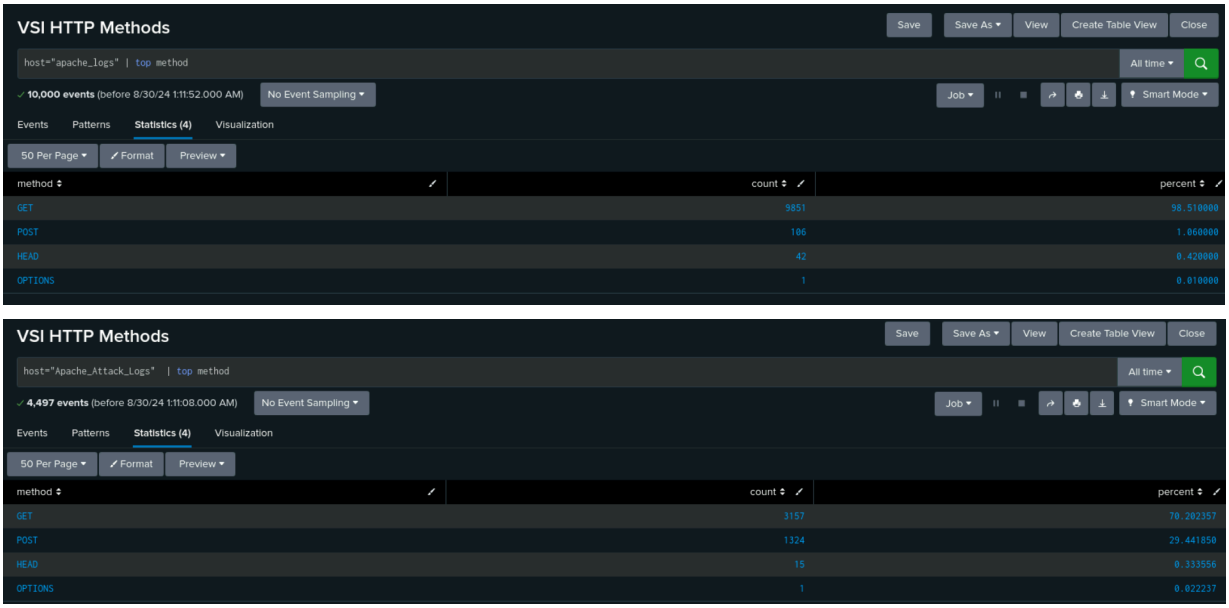
- What are the advantages and disadvantages of using this report, compared to the other user panels that you created?

The advantage of a statistical table chart is that the information is arranged in a clear and condensed manner, while the disadvantage is its inability to show specific data points for particular dates and times since

total cumulative data is displayed. In contrast, time-series visualizations like line or bar charts can effectively display data over time, providing a more granular view of trends and patterns.

Apache Web Server Log Questions

Report Analysis for Methods



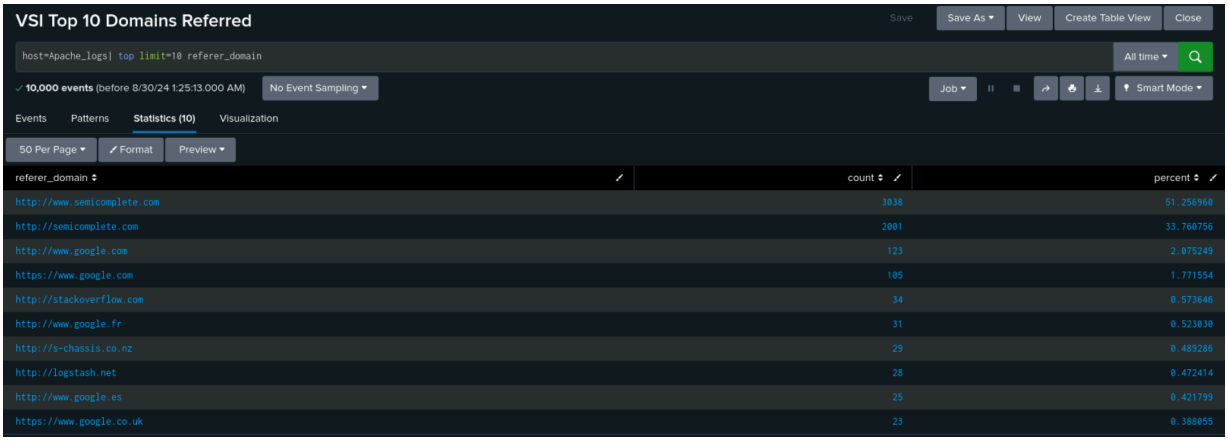
- Did you detect any suspicious changes in HTTP methods? If so, which one?

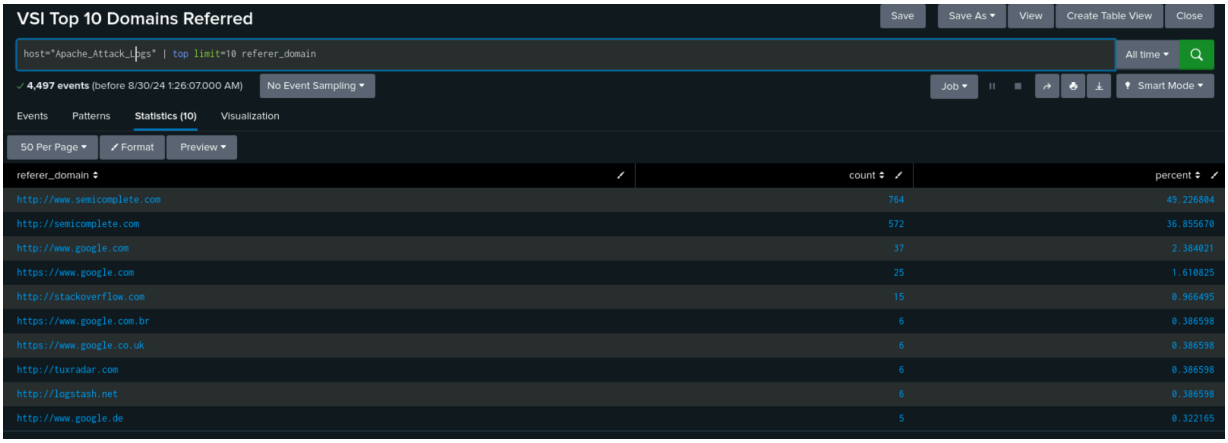
Yes, a significant 29% decline in activity was observed for the GET method, from 99% to 70%. On the other hand, the POST method saw a substantial 28% increase in activity, rising from 1% to 29%. Both changes are considered suspicious.

- What is that method used for?

- GET: Fetches data/information from a web server, such as web pages, images, or other resources.
- POST: Sends data to a web server for processing, often used for tasks like submitting forms, uploading files, or creating new content.

Report Analysis for Referrer Domains

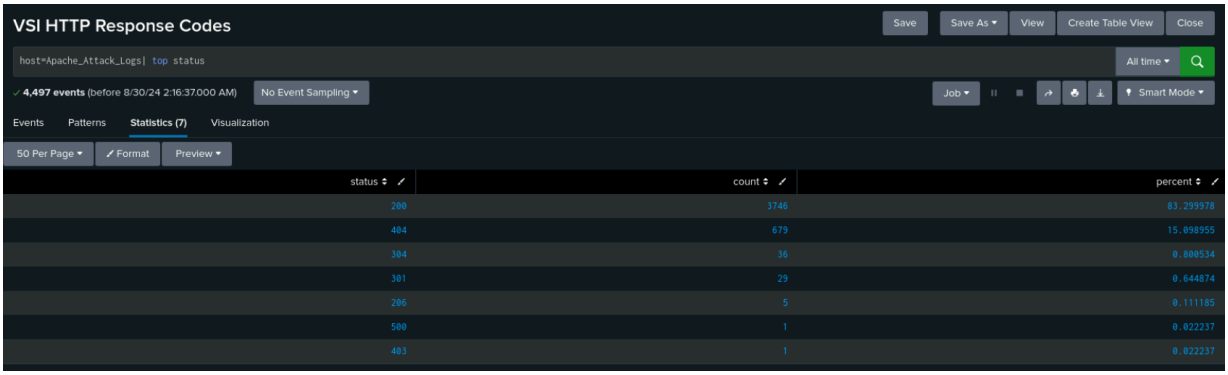




- Did you detect any suspicious changes in referrer domains?

```
No suspicious referrer domains were identified in the attack log.
```

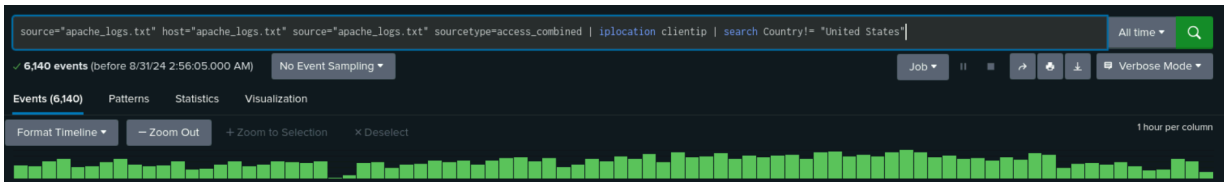
Report Analysis for HTTP Response Codes

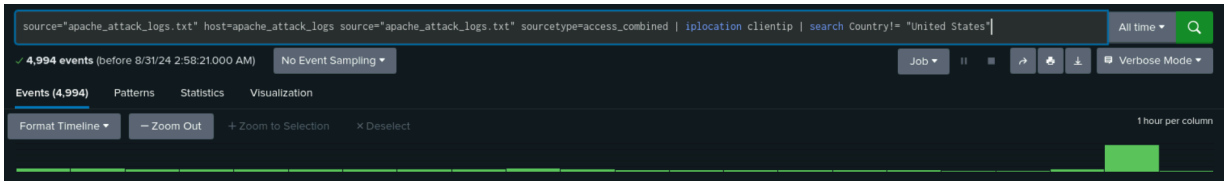


- Did you detect any suspicious changes in HTTP response codes?

The number of 200 and 304 responses decreased by 8% and 4.5%, respectively. However, the most notable change was a substantial 13% increase in 404 errors, rising from 2% to 15%, which suggests potential suspicious activity.

Alert Analysis for International Activity





- Did you detect a suspicious volume of international activity?

```
Yes, we did detect a suspicious volume of international activity,
specifically for Ukraine at 8:00 PM on Wednesday, March 25th.
```

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

```
The count was 1874 at 8:00 PM on Wednesday, 25th March 2020.
```

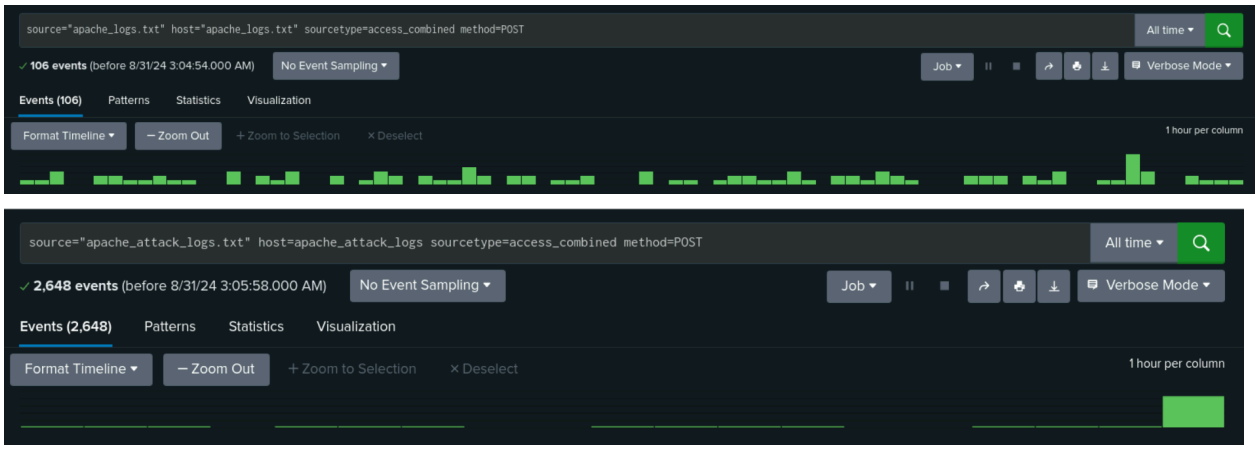
- Would your alert be triggered for this activity?

```
Yes, our alert would have been triggered as we set the threshold to more
than 170 in an hour to send an alert.
```

- 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 detected a rise in the volume of HTTP POST activities, which is
considered suspicious.
```

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

```
The count was 2592 events at 8:00 PM.
```

- When did it occur?

```
The event occurred at 8:00 PM on 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 12. 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?

There was suspicious “GET” method activity on Wednesday, March 25, 2020, from 5:00 PM to 7:00 PM and suspicious “POST” method activity on Wednesday, March 25, 2020, from 7:00 PM to 9:00 PM.

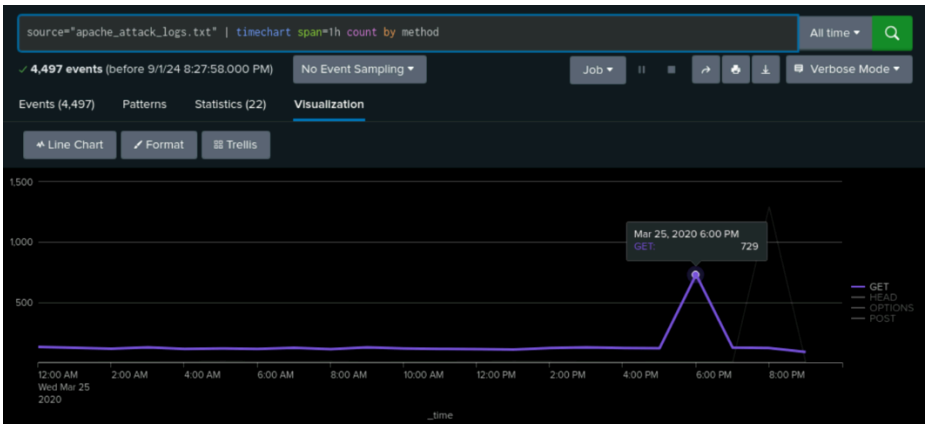
- Which method seems to be used in the attack?

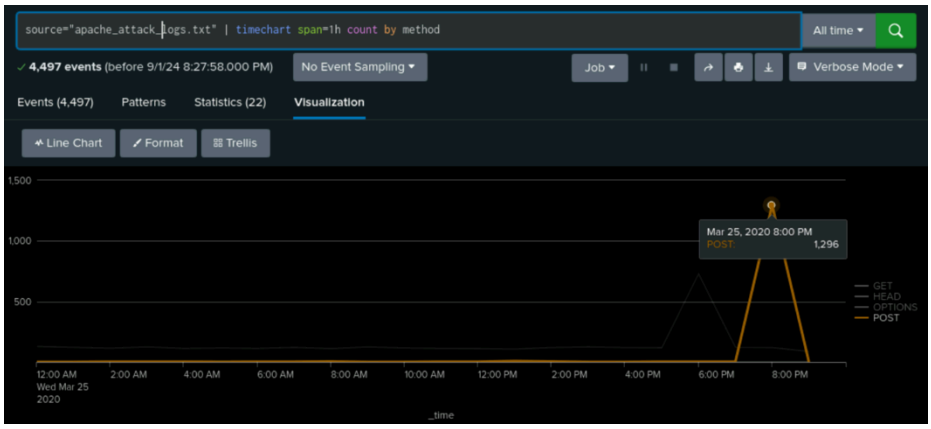
The “GET” and “POST” methods were used in the attack.

- At what times did the attack start and stop?

“GET” - Began Wednesday, March 25, 2020, at 5:00 PM and stopped at 7:00 PM.
“POST” - Began Wednesday, March 25, 2020, at 7:00 PM and stopped at 9:00 PM.

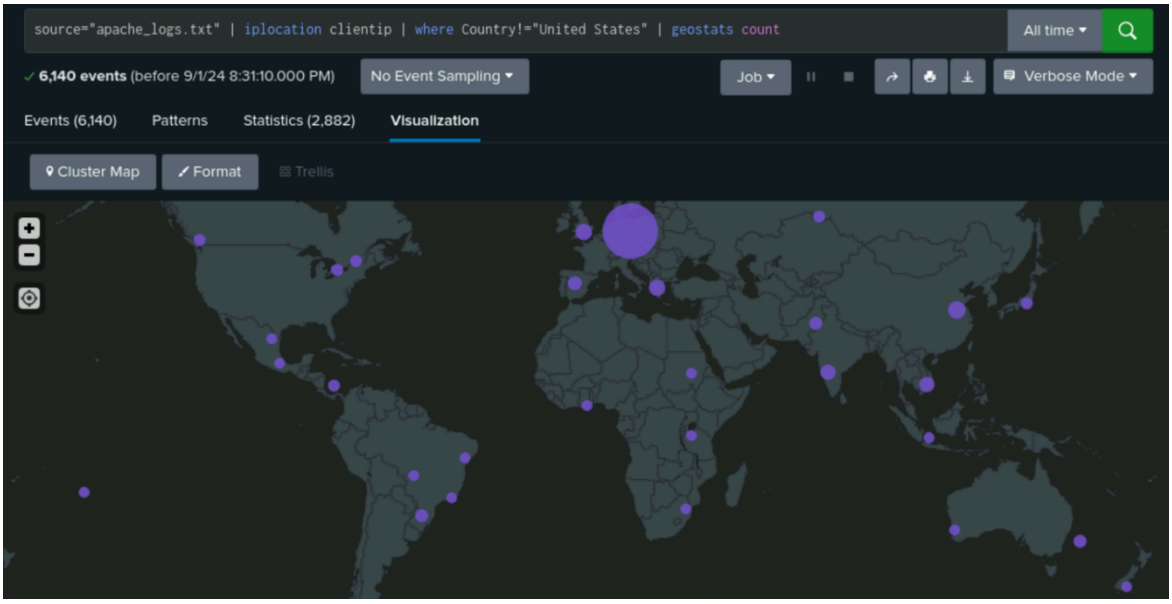
- What is the peak count of the top method during the attack?

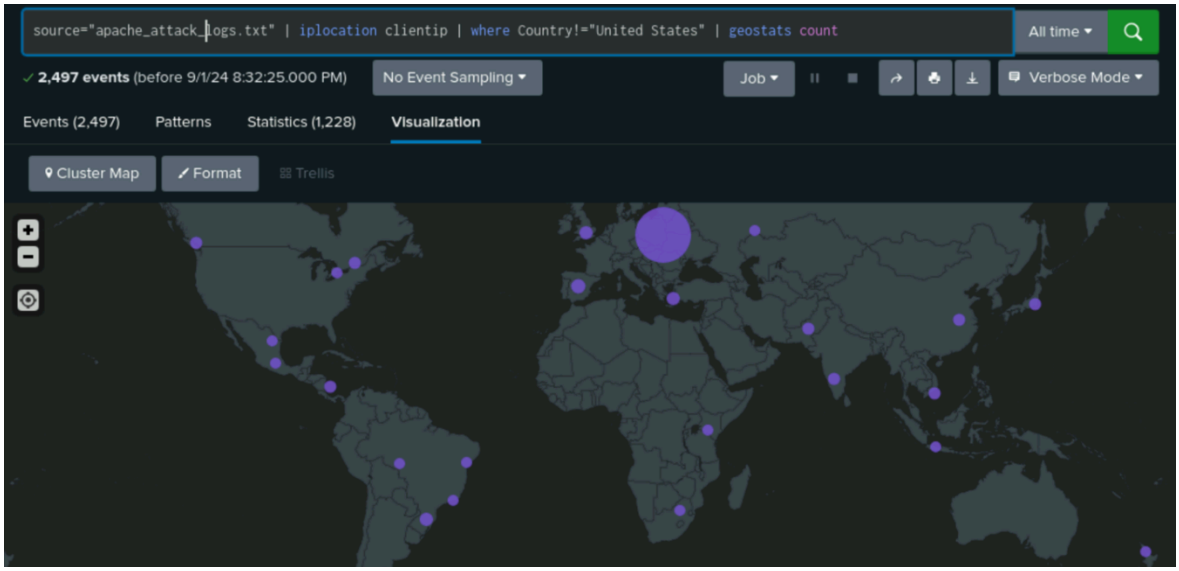


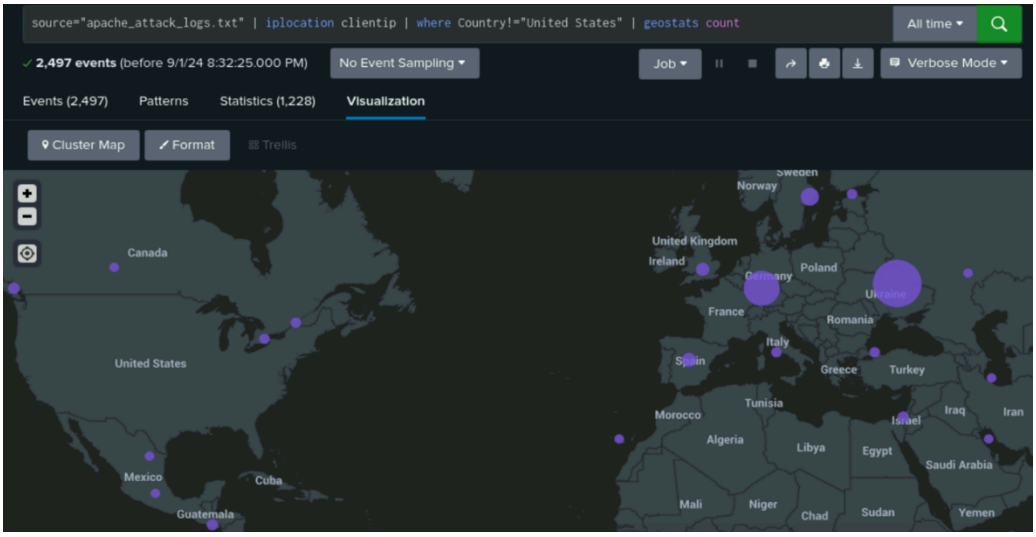


“GET” - peak count was 729.
“POST” - peak count was 1296.

Dashboard Analysis for Cluster Map



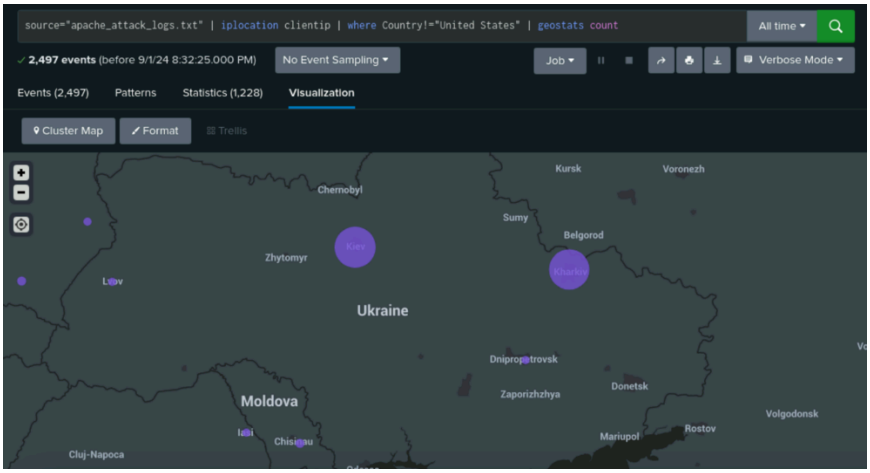




- Does anything stand out as suspicious?

Suspicious activity was detected within Ukraine, specifically in the cities of Kiev and Kharkiv.

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

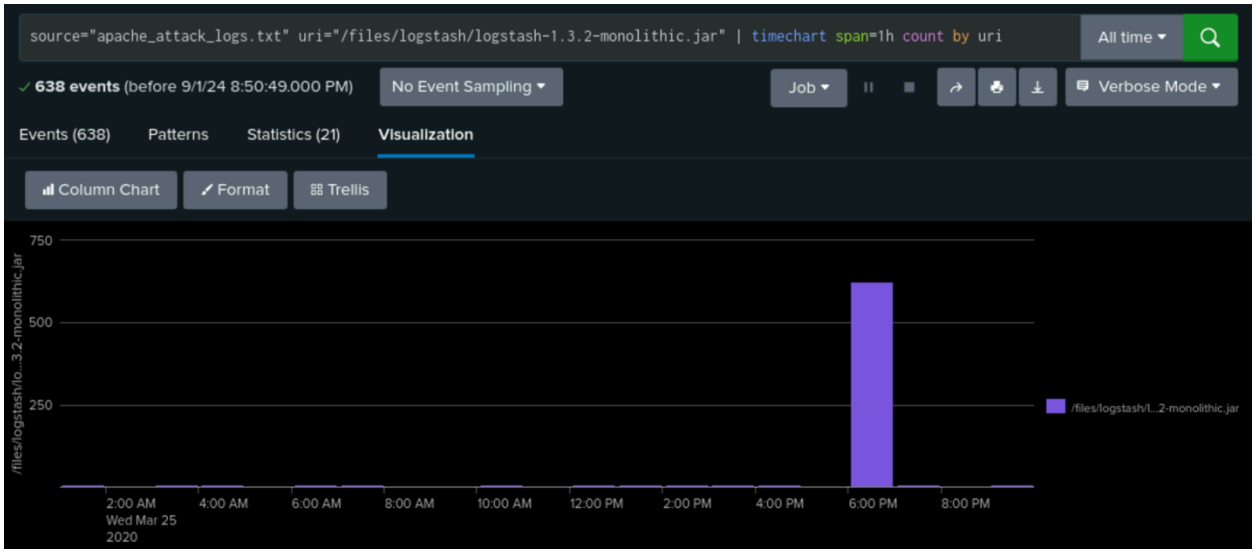


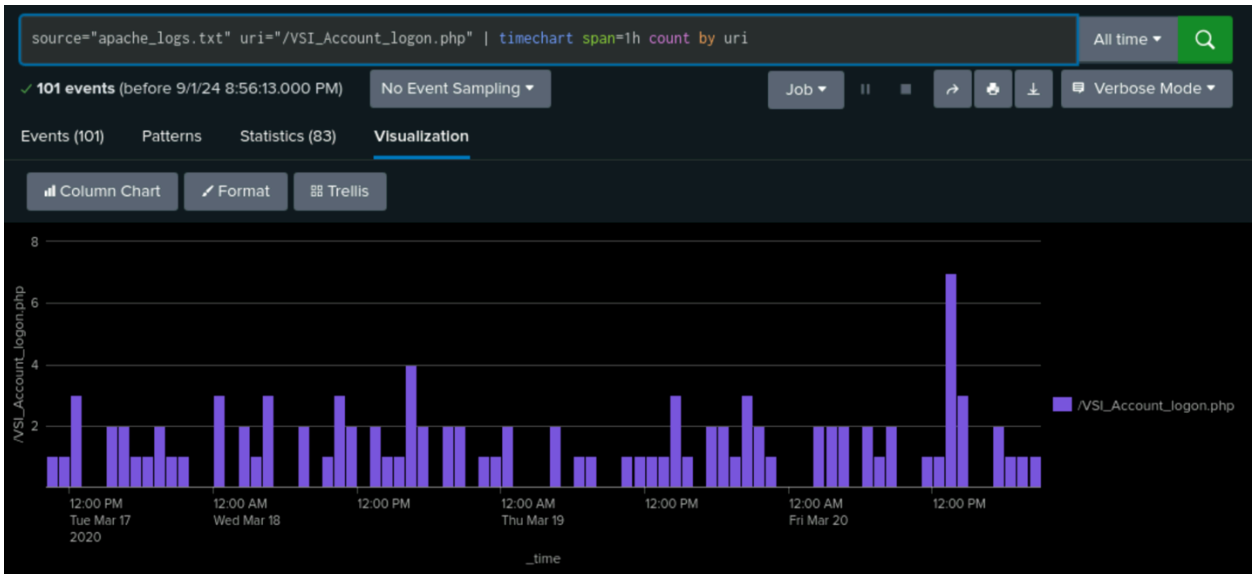
Both Kiev and Kharkiv cities in Ukraine had significantly high volumes of activity.

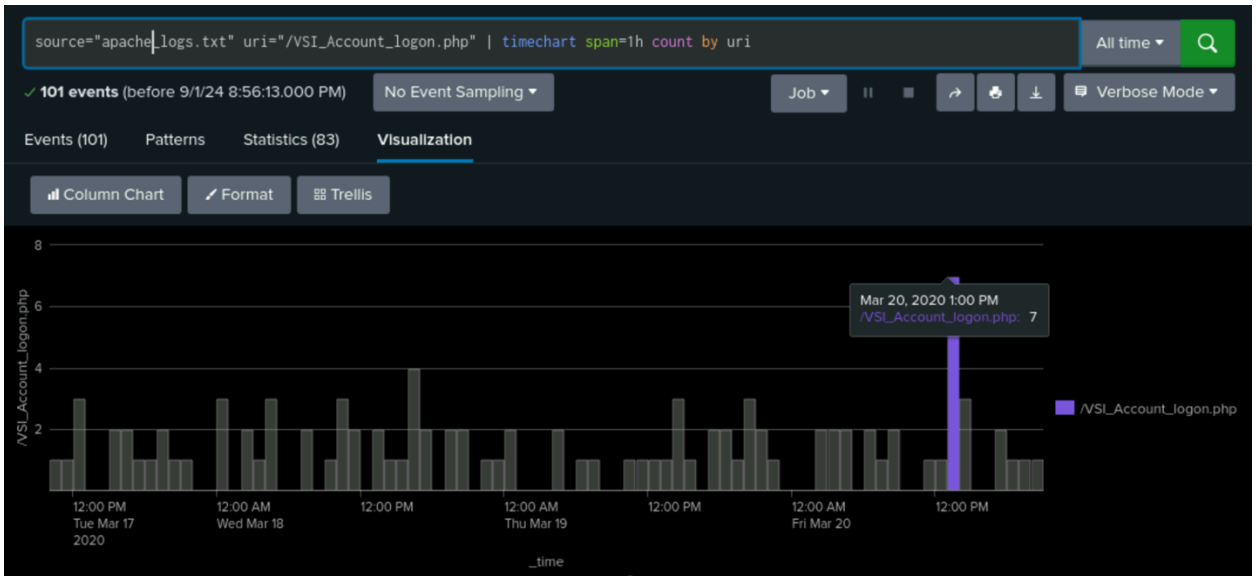
- What is the count of that city?

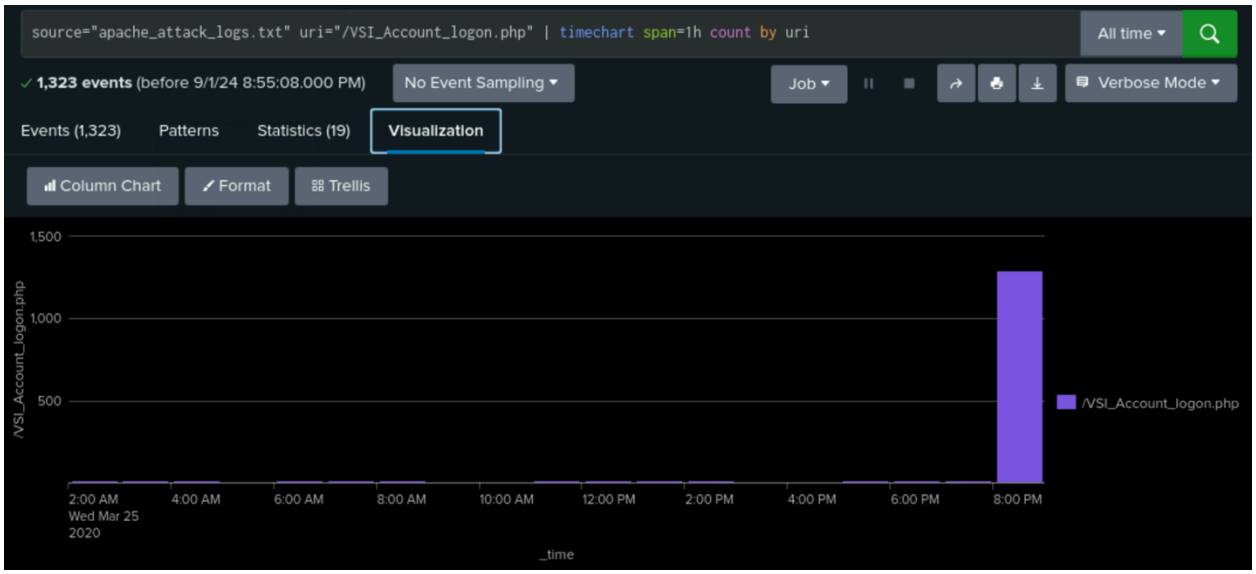
```
Activity count for Kiev is 439 and Kharkiv is 432.
```

Dashboard Analysis for URI Data




source="apache_logs.txt" uri="/VSI_Account_logon.php" | timechart span=1h count by uri
All time
101 events (before 9/1/24 8:56:13.000 PM)
No Event Sampling
Job
Verbose Mode
Events (101)
Patterns
Statistics (83)
Visualization
Column Chart
Format
Trellis
8
6
4
2
/VSI_Account_logon.php
12:00 PM
Tue Mar 17
2020
12:00 AM
Wed Mar 18
12:00 PM
12:00 AM
Thu Mar 19
12:00 PM
12:00 AM
Fri Mar 20
12:00 PM
_time
/VSI_Account_logon.php

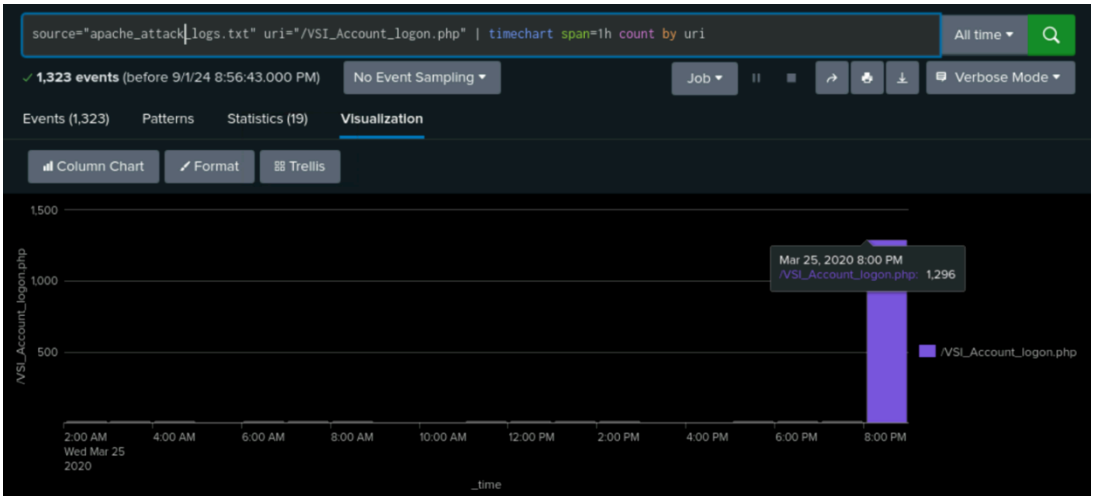




- Does anything stand out as suspicious?

There is a sudden spike in activity with "/files/logstash/logstach-1.3.2-monolithic.jar and VSI_Account_logon.php" URI's as compared to normal activity. The spike occurs on Wednesday, March 25, 2020, at 6:00 PM and 8:00 PM, respectively.

- What URI is hit the most?



“VSI_Account_logon.php” was hit the most with 1296 events.

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

The attacker was attempting a brute force attack on the VSI logon page.