Cybersecurity

Project 3 Review Questions

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

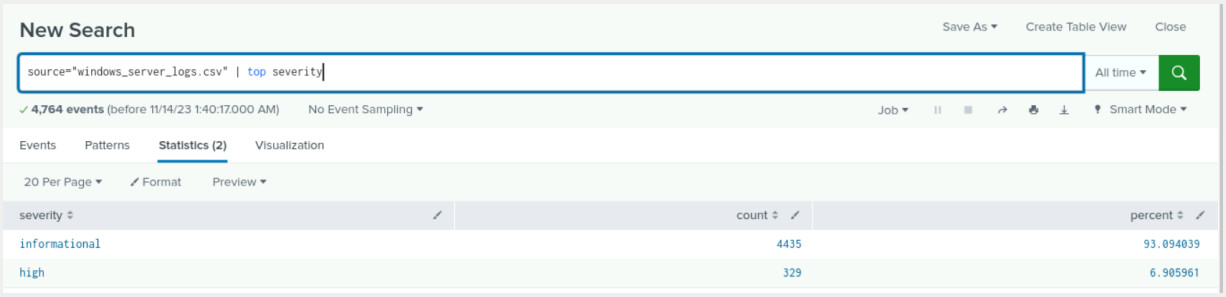
Windows Server Log Questions

Report Analysis for Severity

- Did you detect any suspicious changes in severity?

We did, we observed an increase in severity from

windows_server_logs.csv
High - 6.905961
Informational - 93.094039



To
Windows_server_attack_logs.csv
High - 20.222060
Informational - 79.777940

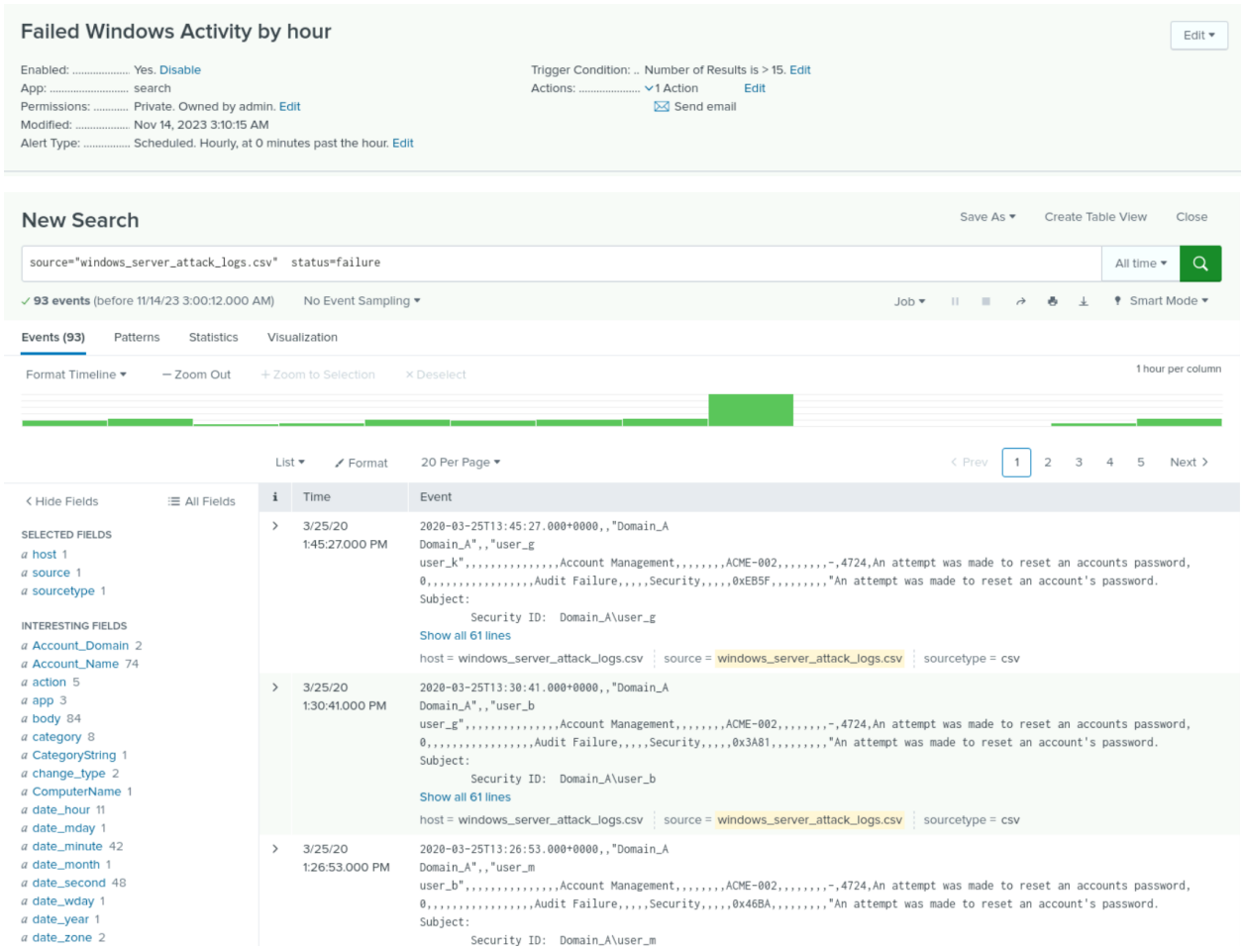
Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

Affirmative there were alterations from
windows_server_logs.csv
Success - 97.019312
Failure - 2.980688

To
Windows_server_attack_logs.csv
Success - 98.436712
Failure - 1.563288

Alert Analysis for Failed Windows Activity



- Did you detect a suspicious volume of failed activity?

```
The suspicious activities occurred between 0800 to 0900 on 03/25/20. There
was a suspicious amount of failed activities.
```

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

```
There were 35 events from 0800 to 0900.
```

- When did it occur?

```
This happened on 03/25/20 from 0800 to 0900.
```

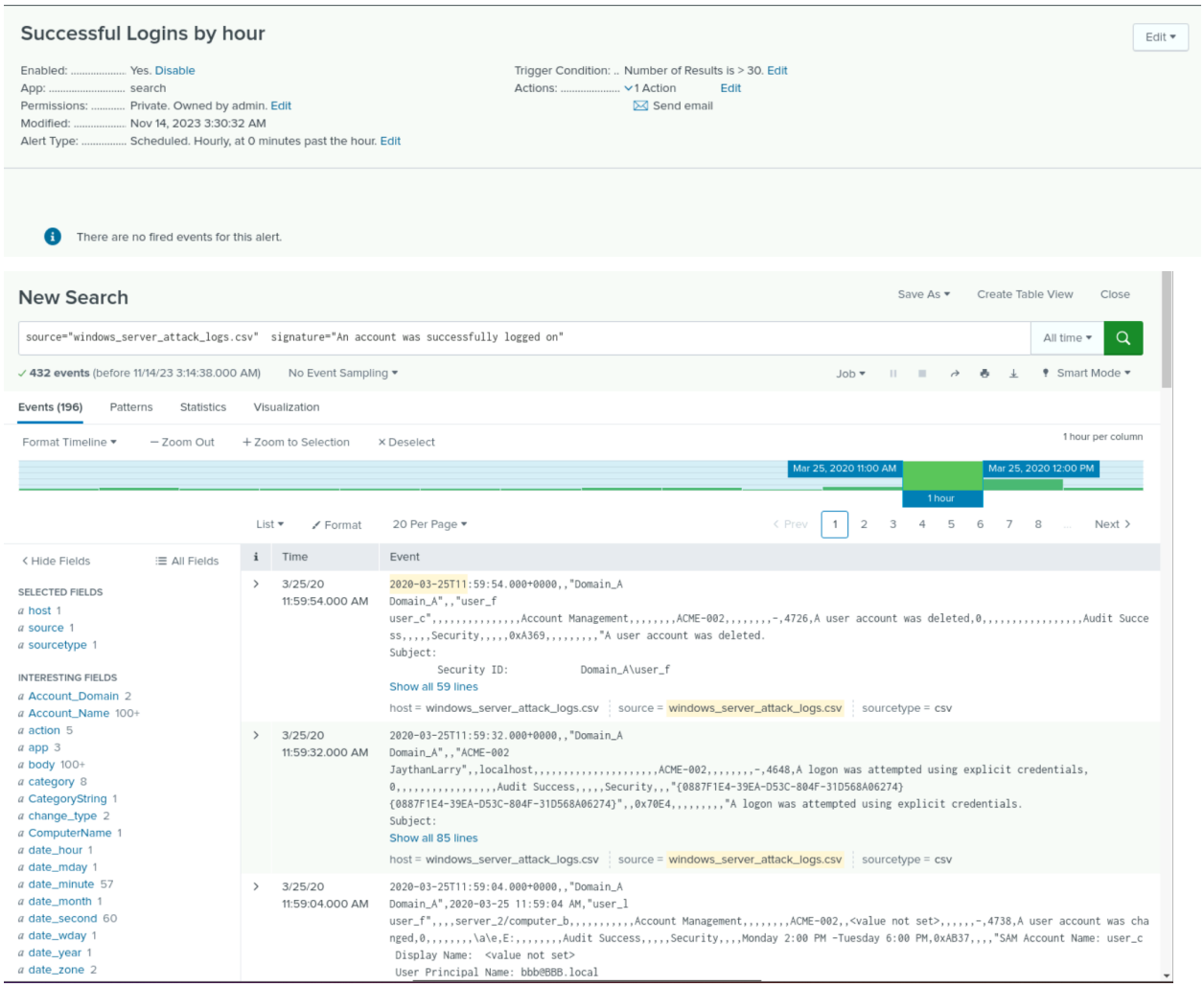
- Would your alert be triggered for this activity?

```
Yes it would, we set the trigger condition to > 15, it would then have alerted us.
```

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

```
Negative, We concluded that 15 is a perfectly adequate benchmark for alerts, because 15 alerts is higher than the average number of alerts per hour. This works out perfectly because it is not too high to nullify alerts from suspicious activity.
```

Alert Analysis for Successful Logins



- Did you detect a suspicious volume of successful logins?

```
Yes we did, at 1100 there were 196 events and at 1200 there were about 77 events. The average login events are from 10 to 25 each hour.
```

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

```
At 1100 there were 196 events as stated above and 77 events at 1200.
```

- Who is the primary user logging in?

```
User J
```

- When did it occur?

```
From 1100 to 1300
```

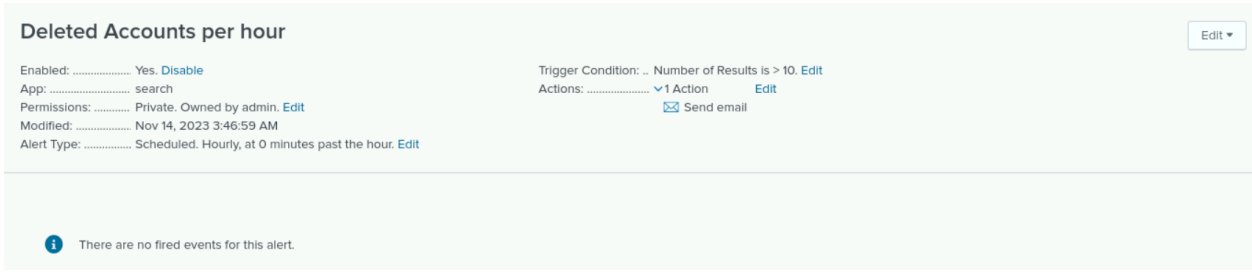
- Would your alert be triggered for this activity?

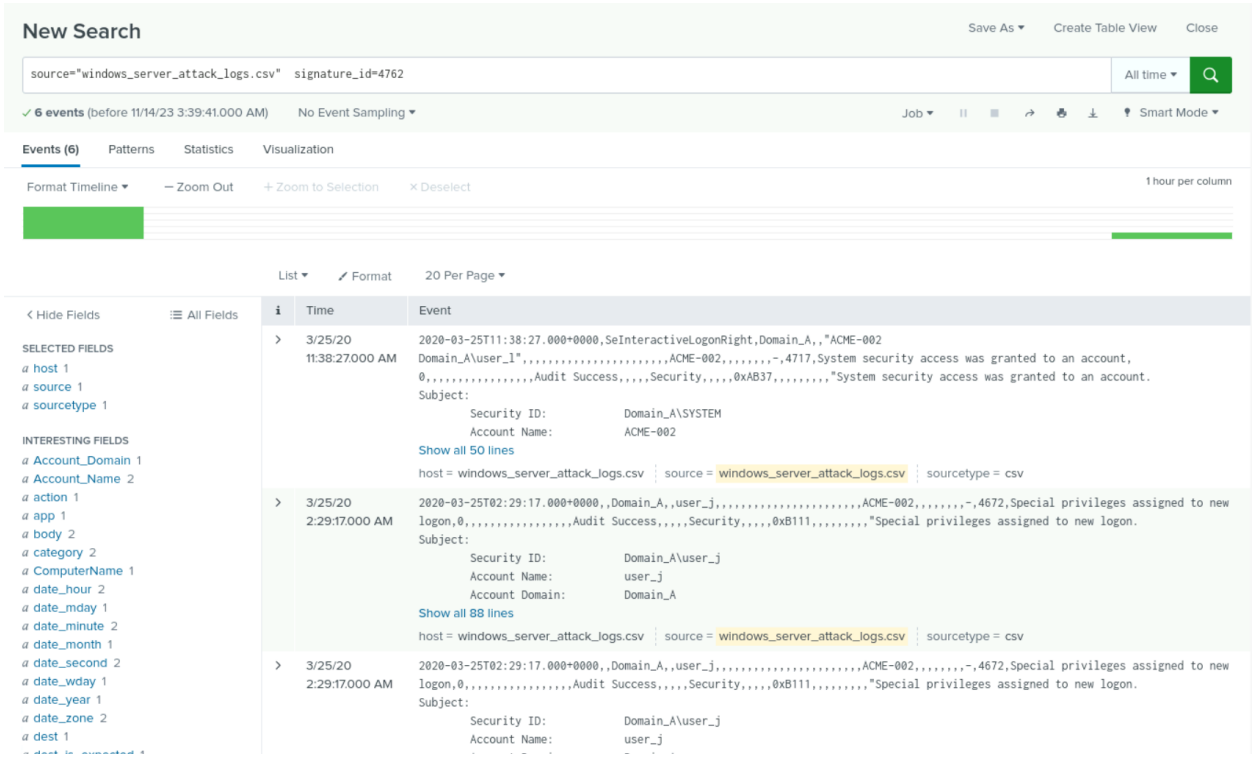
```
Yes our alert would be triggered because we set the trigger condition as > 30.
```

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

```
No, because we can prevent triggering false alerts from the regular login volume by having our benchmark at 30. The benchmark is also high enough that we can be assured that in a triggering event, those activities are suspicious and not a false positive.
```

Alert Analysis for Deleted Accounts

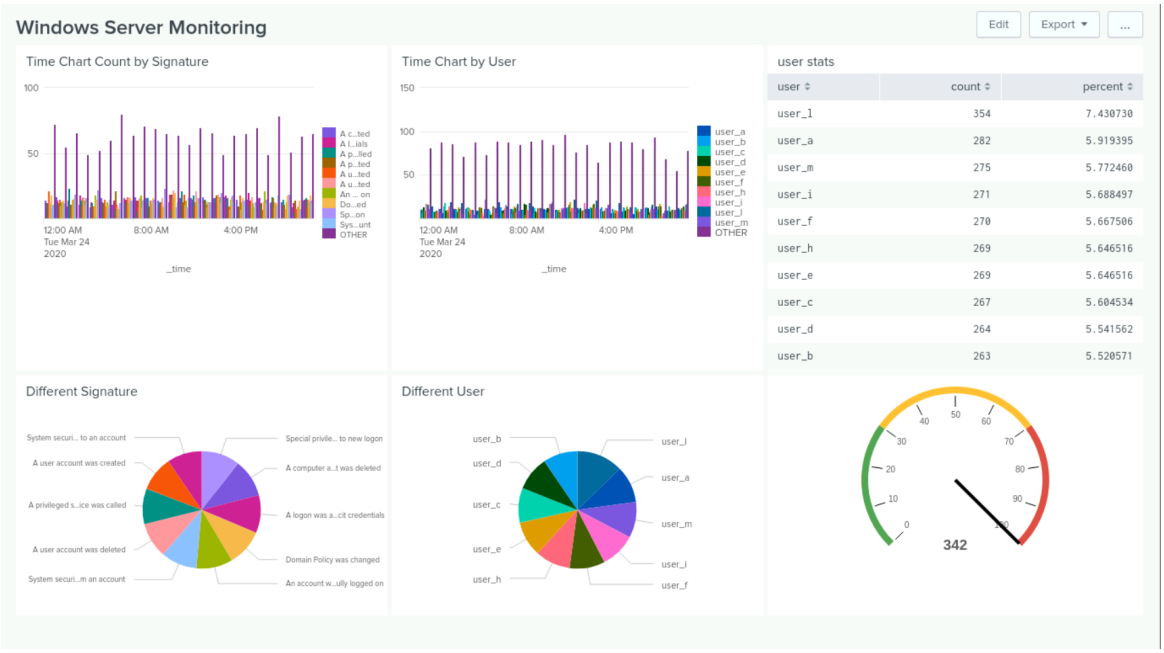


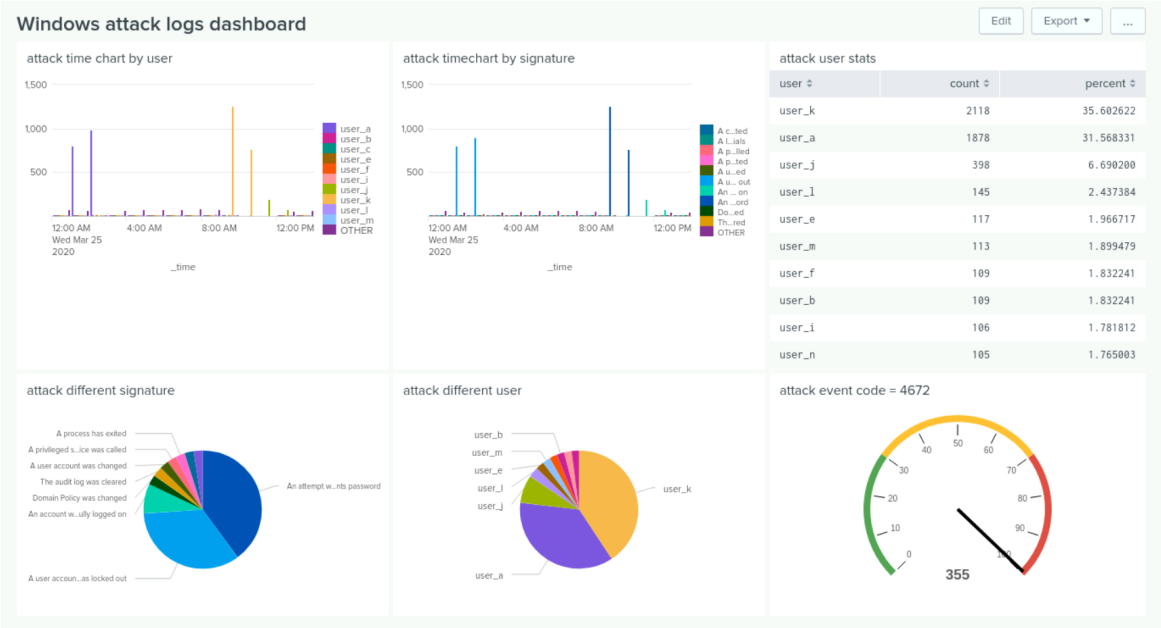


- Did you detect a suspicious volume of deleted accounts?

```
No we did not, there was not any suspicious volume of deleted accounts.
```

Dashboard Analysis for Time Chart of Signatures





- Does anything stand out as suspicious?

Yes, there was several things that stands out, such as users trying to reset passwords alot at 39.955%, a user got locked out of their account several times at 34.003%, and there were successful logins with 8.111%.

- What signatures stand out?

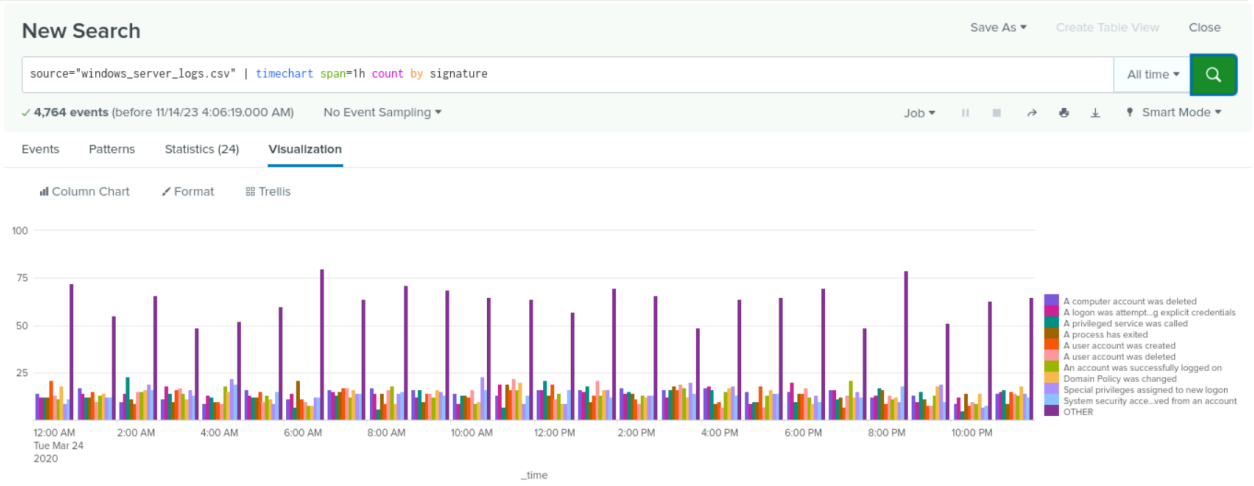
```
The reset passwords attempts at 39.955% ,then user lockouts at 34.003%, and lastly successful logins at 8.111%
```

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

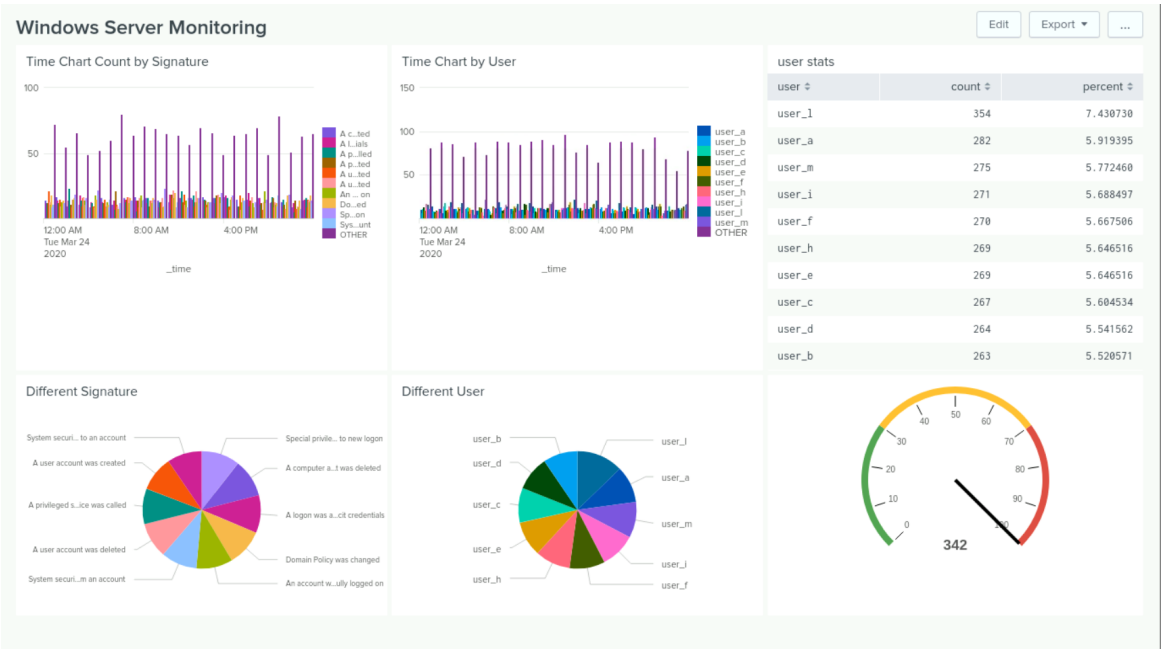
```
“A user account was locked out” - from 0100 to 0300 on 03/25/20
“An attempt was made to reset a users password” - from 0900. to 1100 on 03/25/20
“The account was successfully logged on” - from 1100 and ended at 1300 on 03/25/20
```

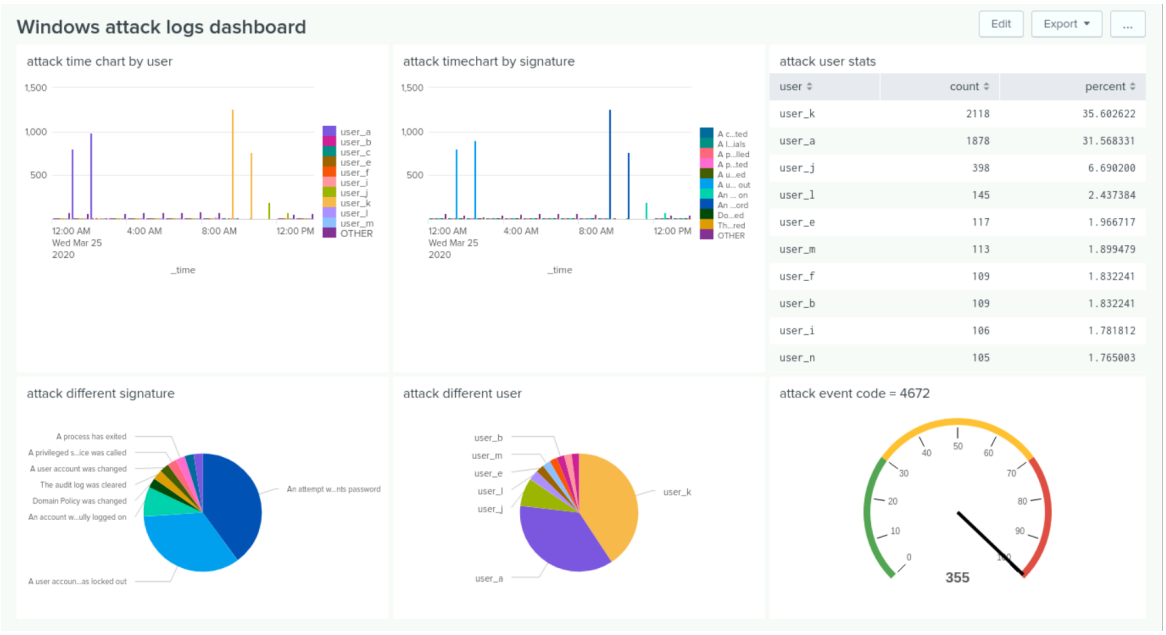
- What is the peak count of the different signatures?

```
“A user account was locked out” - peak 896 total from 0100 to 0300. was 1701
“An attempt was made to reset a users password” - peak 1,258  total from 0900-1100 was 2019
“The account was successfully logged on” - peak 196 total from 1100-1300 was 273
```



Dashboard Analysis for Users





- Does anything stand out as suspicious?

```
Users A, K, and J are the ones who causing these suspicious activities
```

- Which users stand out?

```
These following Users A,K and J
```

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

```
User A - from from 0100 to 0300 on 03/25/20
User K - from 0900 to 1100 on 03/25/20
User J - from 1100 to 0100 on 03/25/20
```

- What is the peak count of the different users?

```
User A - peak 984 total at 1783
User K - peak 1256 total at 2017
User J - peak 196 total 278
```

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

- Does anything stand out as suspicious?

```
No
```

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

```
All of our visualization and chart information matches the Signatures above
```

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

- Does anything stand out as suspicious?

```
No
```

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

```
Yes, all of our charts information matches with the Users information
```

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?

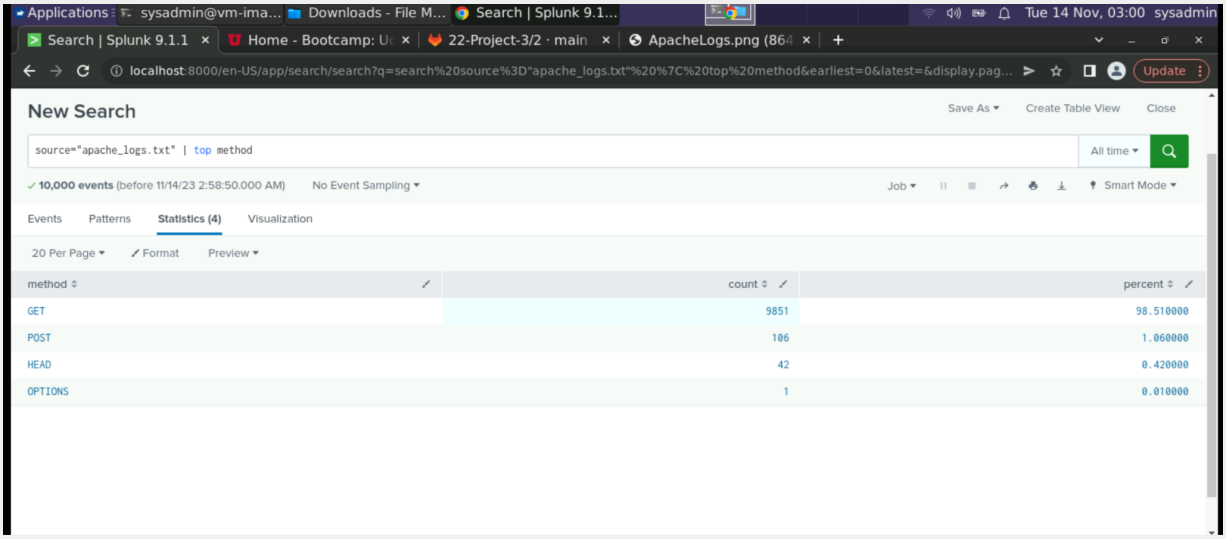
```
Advantage - Provides a comprehensive overview of total user activity or
activity percentage.

Disadvantage - Lacks the cumulative perspective offered by a time chart, as
Time charts offer a more specific and shorter time frame for detecting
suspicious activity.
```

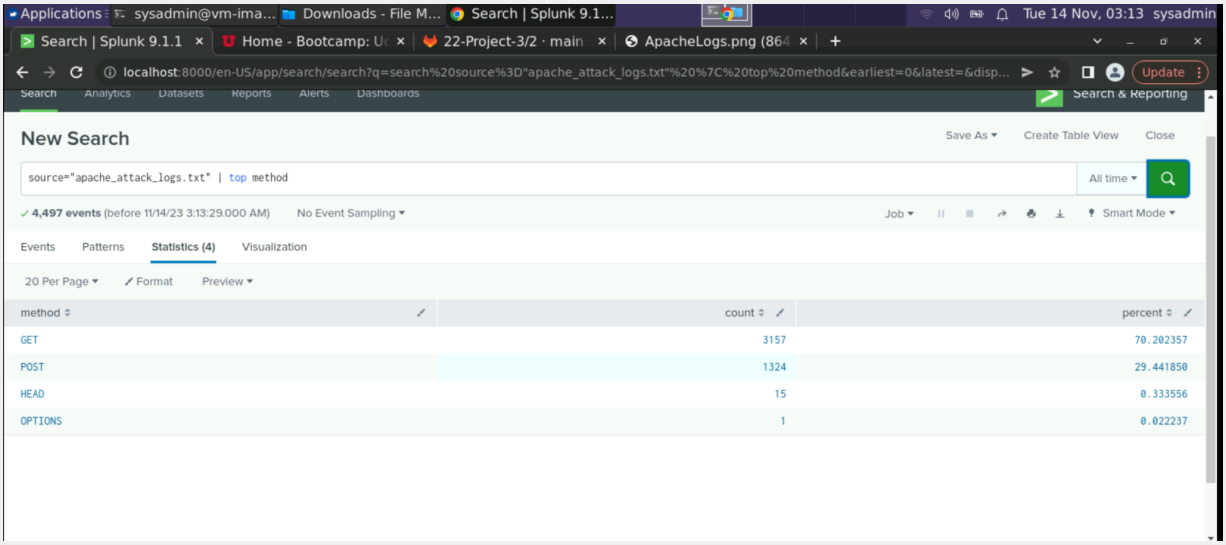
Apache Web Server Log Questions

Report Analysis for Methods

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

Yes we did, there was a conspicuous alteration in the HTTP POST method. It increased exponentially from 1% to 29% and the count raised from 106 to 1324





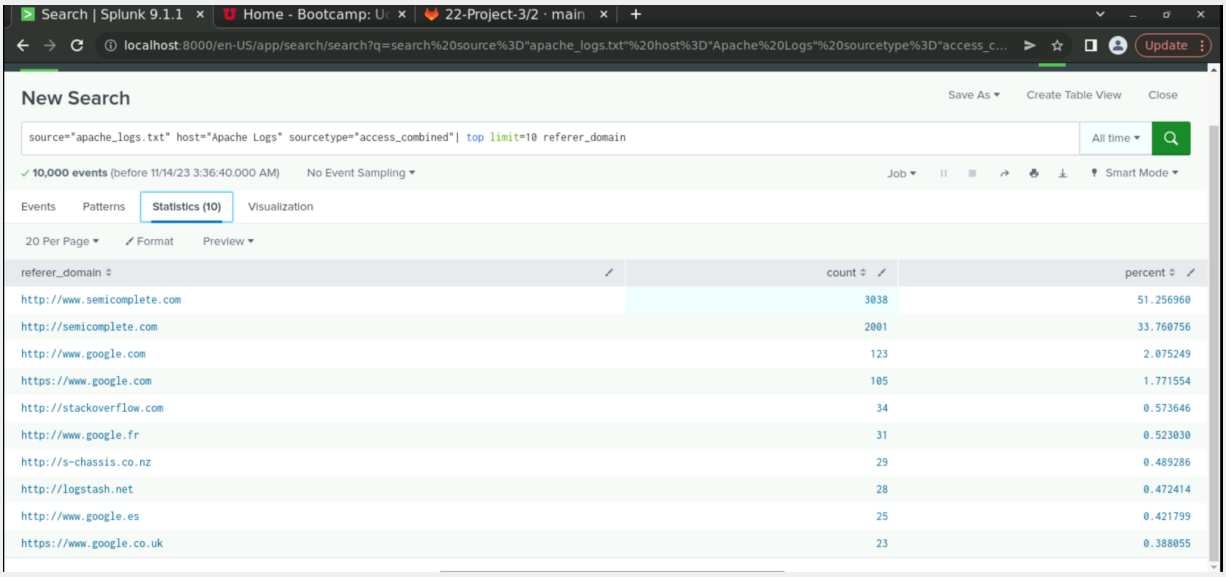
- What is that method used for?

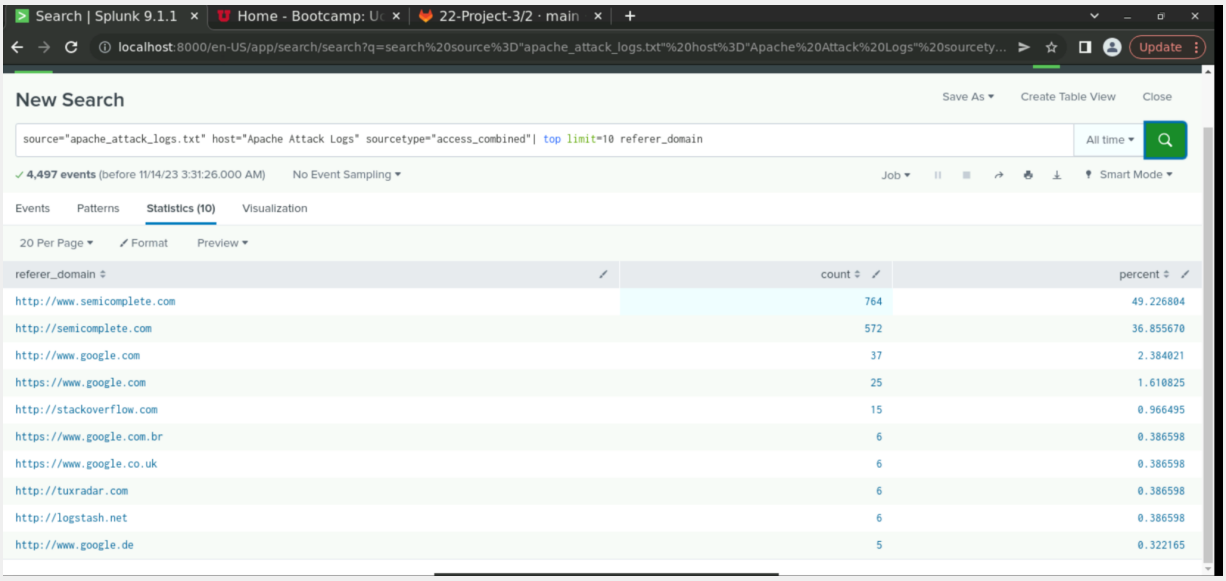
The method of POST is designed to update or submit info to a web server.

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

There weren't any questionable referees during this assault. There was only a miniscule alteration in the1st two domains by a few percentages.

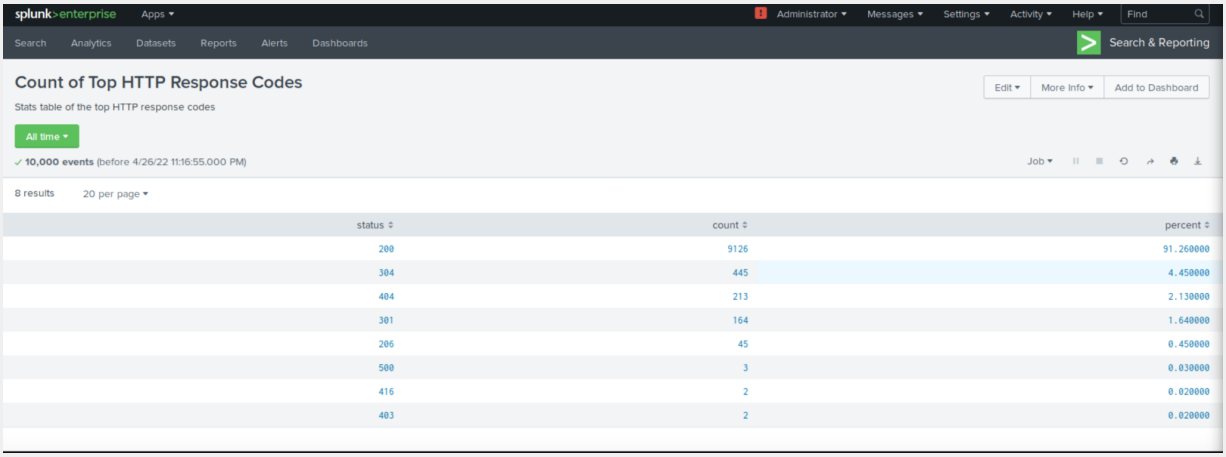


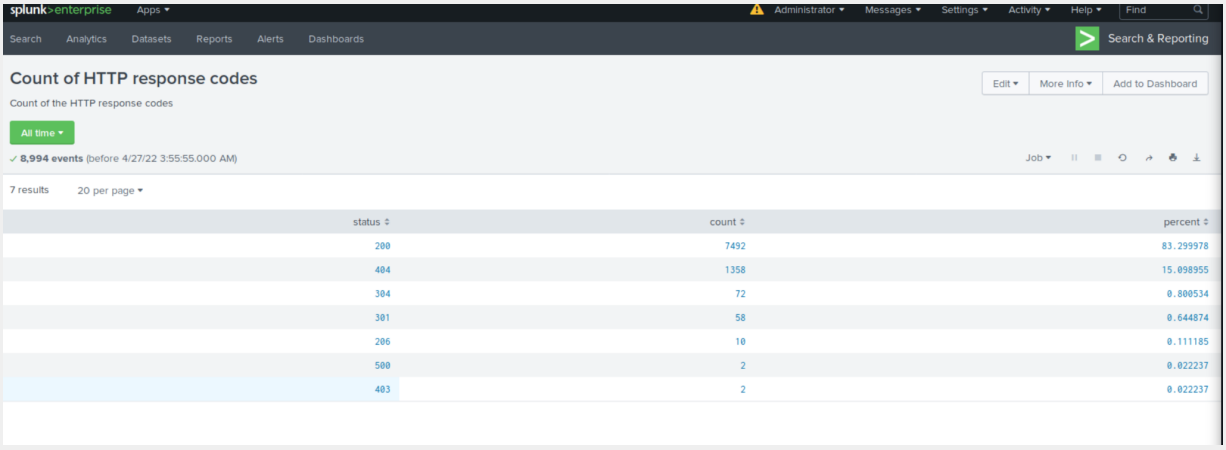


Report Analysis for HTTP Response Codes

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

There are several small changes, but the most prominent is the 404 response code, which increased from 2% to 15%. The 200 response code went down from 91% to 83%.

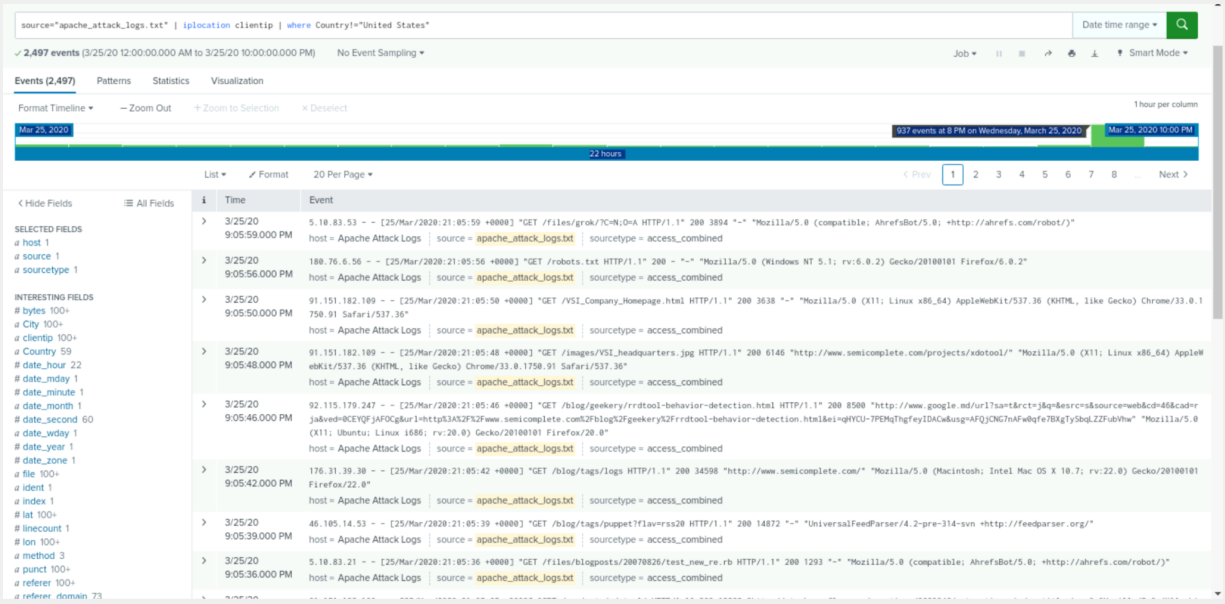


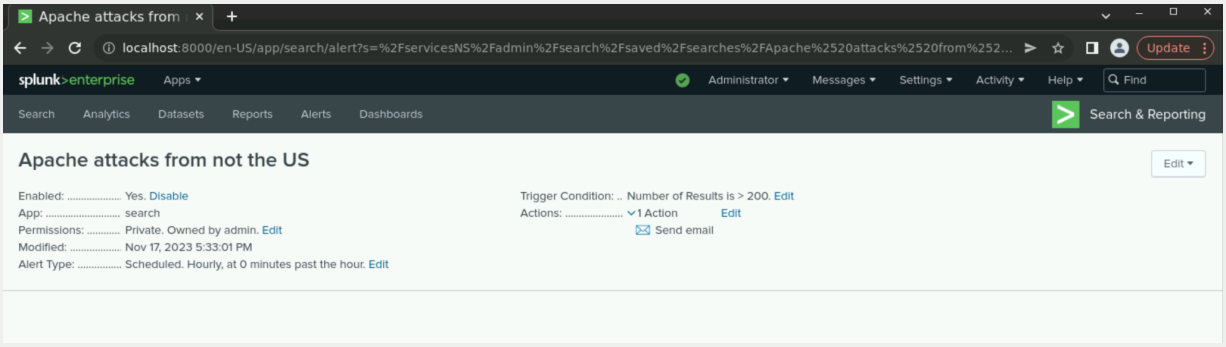


Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

There was activity in Ukraine at 8 p.m. on Wednesday March 25th, and had a count of 937 events.





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

There was a spike in POST method activity between 8 p.m. and 9 p.m. on Weds, March 25th, and had a count of 1,296 events.

- Would your alert be triggered for this activity?

The average activity per hour was about 75.
We concluded the threshold should be set for 200.

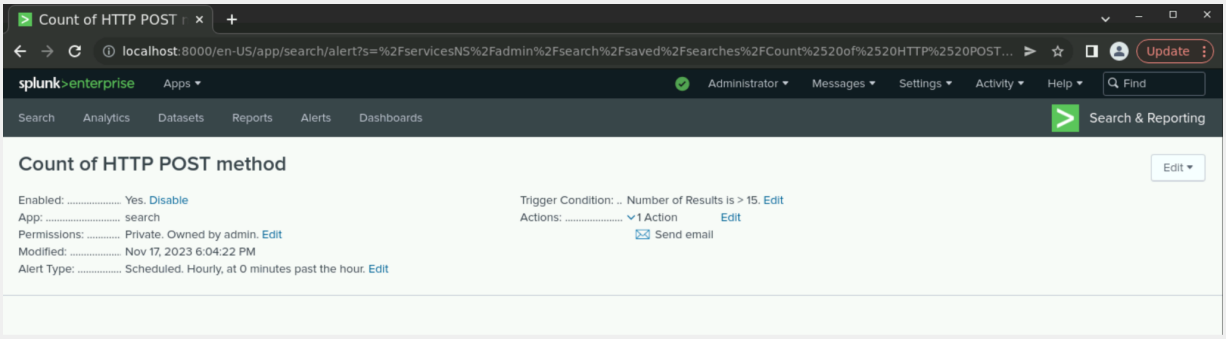
- After reviewing, would you change the threshold that you previously selected?

No as it's above the activity set threshold.

Alert Analysis for HTTP POST Activity

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

There was a sudden increase in POST method activity and the threshold set is at 15 count.



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

The count was 1,296 events between 8 p.m. and 9 p.m. on Weds, March 25th 2020

- When did it occur?

March 25th 2020 between 8pm and 9pm

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

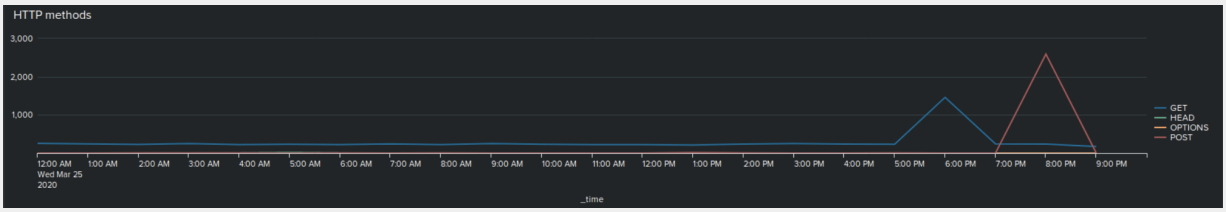
No, we determine 15 is an adequate amount, which would trigger.
The average activity per hour is approximately 5.

```
Therefore the threshold is set for 15.
We set it to run every hour.
The alert triggers when count is greater than chosen threshold of 15
```

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

```
Yes, there were suspicious activities of the POST and GET method.
```



- Which method seems to be used in the attack?

```
The POST method was used and the GET method was used
```

- At what times did the attack start and stop?

```
POST Method commenced at 8 p.m. and finished at 9 p.m.
Get method began at 6 p.m. and ended at 7 p.m.
```

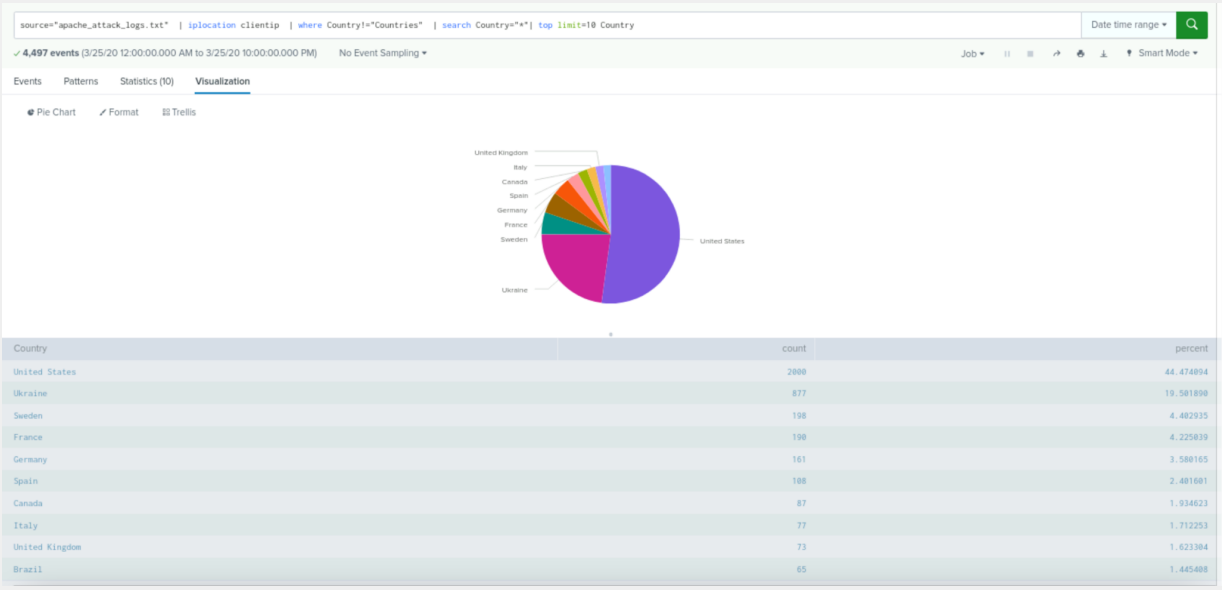
- What is the peak count of the top method during the attack?

```
The peak count for the Get method was 3,157.
The peak count for the POST method was 1,324.
```

Dashboard Analysis for Cluster Map

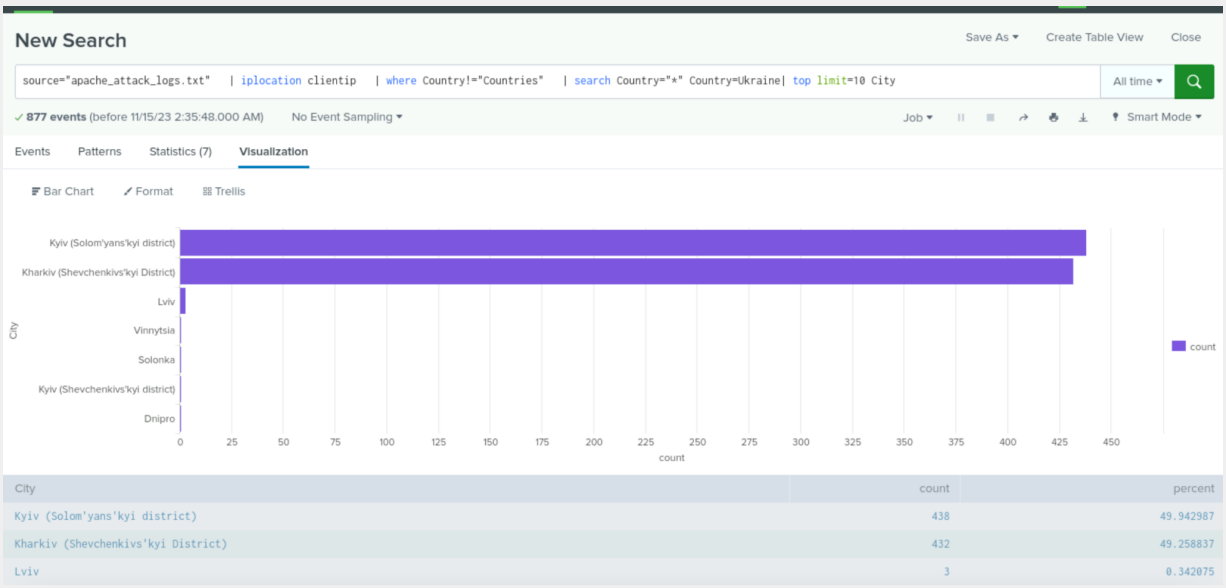
- Does anything stand out as suspicious?

The 2nd highest country of suspicious activity is Ukraine.



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

Kiev, Kharkiv and Lvov



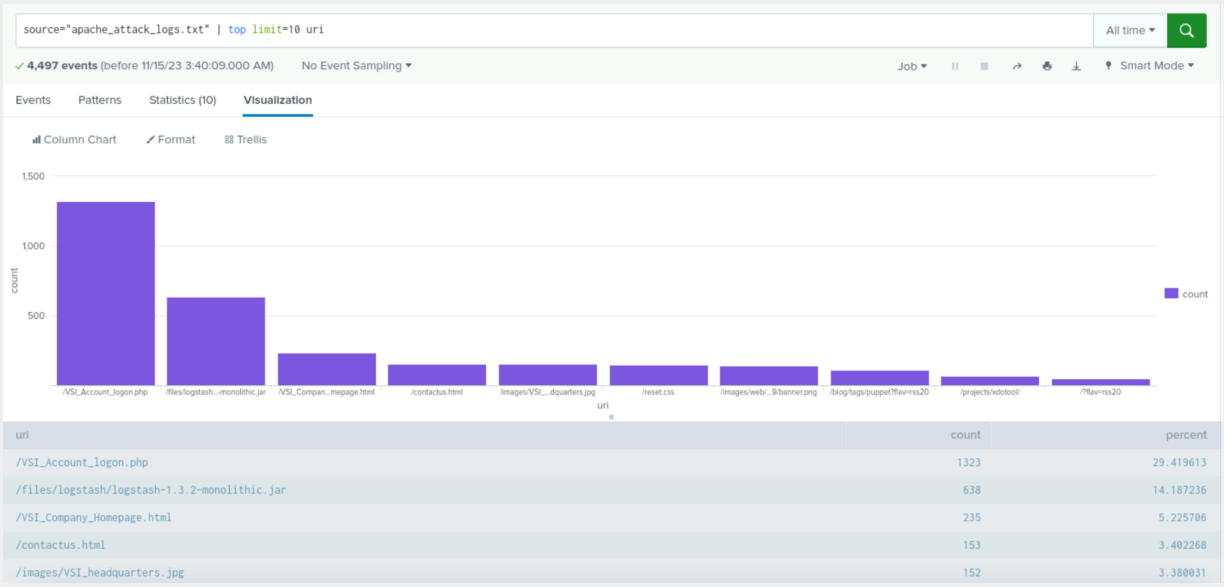
- What is the count of that city?

```
kiev:Count of 438. Kharkiv:Count of 432. Lvov:Count of 3.
```

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

Yes, there is suspicious activity against the main VSI logon page: /VSI_Account_logon.php.



- What URI is hit the most?

/VSI_Account_logon.php.

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

The attacker may be attempting to brute force the VSI logon page