Cybersecurity

Project 3 Review Questions

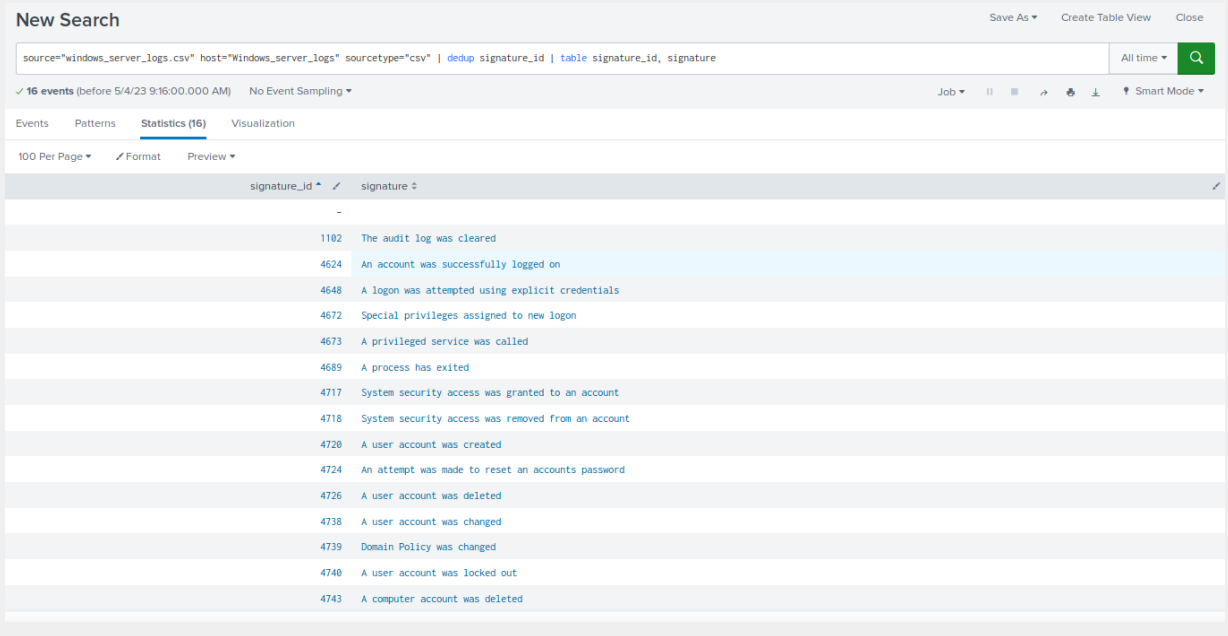
Make a copy of this document before you begin. Place your answers below each question.

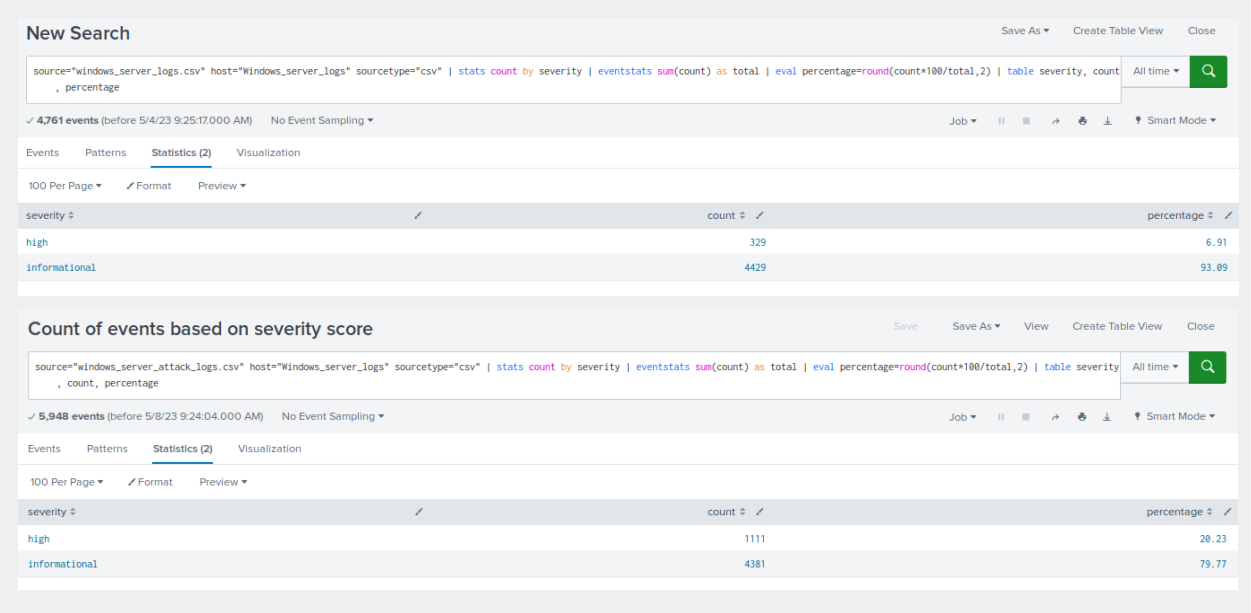
Windows Server Log Questions

Report Analysis for Severity

- Did you detect any suspicious changes in severity?

We identified a significant increase in the percentage of incidents categorized as "high" severity, which rose from 6.91% to 20.23%. This notable shift highlights a substantial increase in the number of incidents that fall under this severity category.

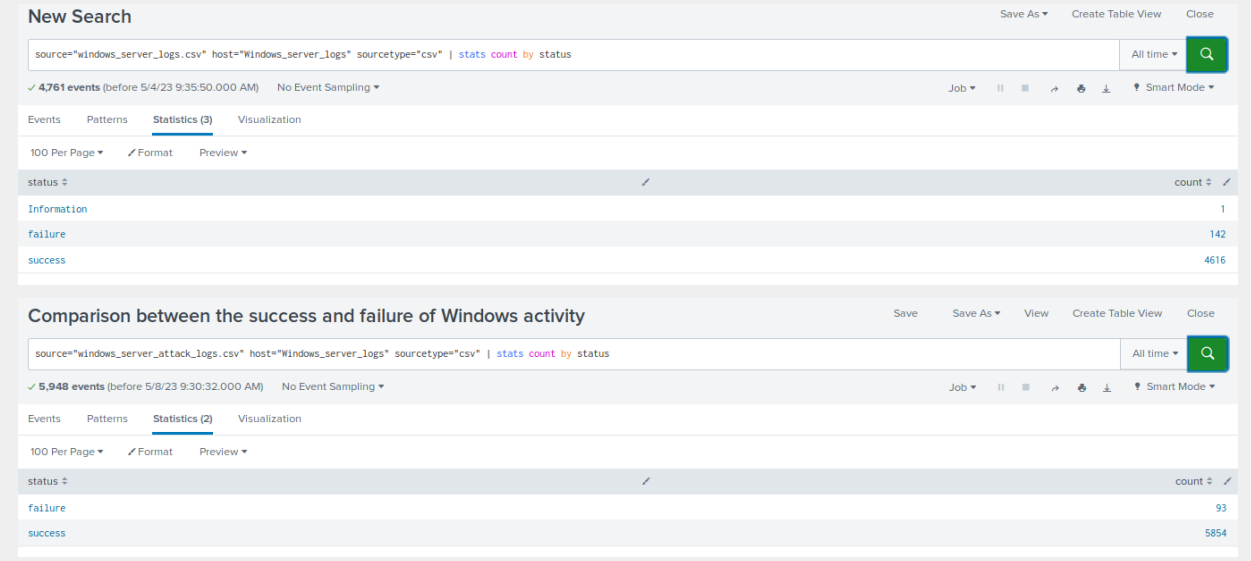




Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

During the post-attack period, there were 93 failed attempts, which is a decrease of 49 attempts compared to the pre-attack period when there were 142 failed attempts.



Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

During the attack, there was a spike of 35 failed events at 8am followed by no failed events until 12pm, which is a suspicious activity that may indicate a possible attack or intrusion during that time period.

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

```
During the attack, there were 35 failed events detected at 8am, followed by a prolonged period of no activity until 12pm, with only 3 additional events recorded at that time.
```

- When did it occur?

```
8am
```

- Would your alert be triggered for this activity?

```
Yes, alerts are triggered when events reach a threshold greater than 7. This was decided as we found 5 to be baseline
```

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

```
No
```

Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

```
The number of successful logins was abnormally low at 9am (only 4 events), and it continued to decrease thereafter, with 0 events from 10am until 12pm.
```

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

```
The number of successful logins was abnormally low at 9am (only 4 events), and it continued to decrease thereafter, with 0 events from 10am until 12pm.
```

- Who is the primary user logging in?

```
User K
```

- When did it occur?

```
Approx. 9AM till 12PM
```

- Would your alert be triggered for this activity?

```
No, our alert would not have been triggered, as the threshold was set to only monitor successful logins greater than 15 per hour. This is because we determined a baseline of 13
```

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

To enhance our monitoring, we would not alter the threshold for successful logins that exceeds 15 per hour, but rather include an alert to also notify us when successful logins fall below a certain threshold per hour.

Alert Analysis for Deleted Accounts

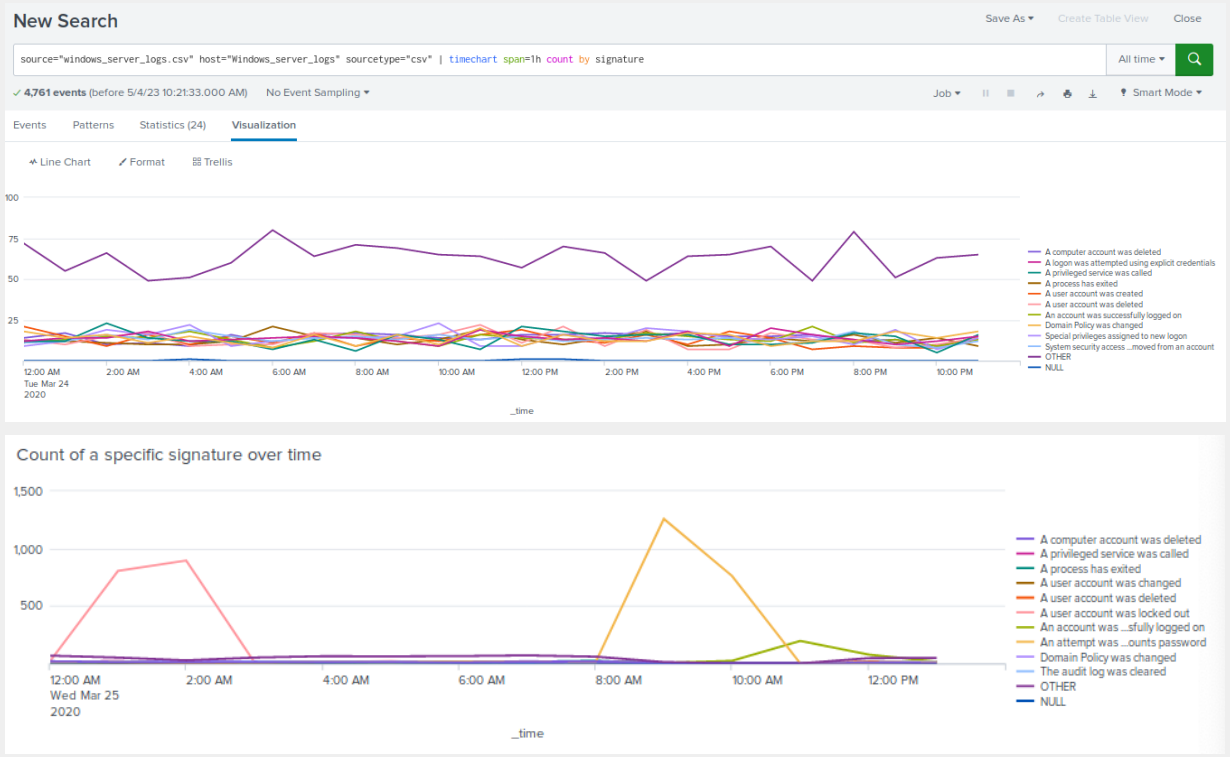
- Did you detect a suspicious volume of deleted accounts?

After analyzing the data, we found that no user account deletions were recorded after 1PM, which is suspicious. It's suspicious because the baseline we found was 13. So this wouldn't even trigger an alert as our threshold was anything greater than 15

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

At 1AM there was a sudden increase in the number of user accounts being locked out. This spike reached a peak of 896 at 2AM, before a sharp drop to only 10 by 3AM. Later, at 9am, there was a surge in the number of attempts to reset an account's password, reaching a high of 1258. This peak then declined and was back to normal levels by 11AM. At this time, there was also a spike in the number of accounts successfully logged on, 196 events recorded.



- What signatures stand out?

-a user account was locked out
-an attempt was made to reset an accounts password
-an account was successfully logged on

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

```
-a user account was locked out: 1am till 3am
-an attempt was made to reset an accounts password: 9am till 11am
-an account was successfully logged on: 11am till 12pm
```

- What is the peak count of the different signatures?

```
-a user account was locked out: 896
-an attempt was made to reset an accounts password: 1258
-an account was successfully logged on: 196
```

Dashboard Analysis for Users

- Does anything stand out as suspicious?

The event counts after the attack indicate that user A and user K were responsible for a large portion of the events, with user A accounting for approximately 32% and user K with around 36%, as shown in the pie chart. User A activity peaked at 2am after a sudden spike at 1am, before settling at 3am. User K activity, on the other hand, came in peaking at 9am before returning to normal levels at 11am.

- Which users stand out?

```
User A and User K stand out
```

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

User A's activity started at 1AM and ended at 3AM, while User K's activity started at 9AM and ended at 11AM.

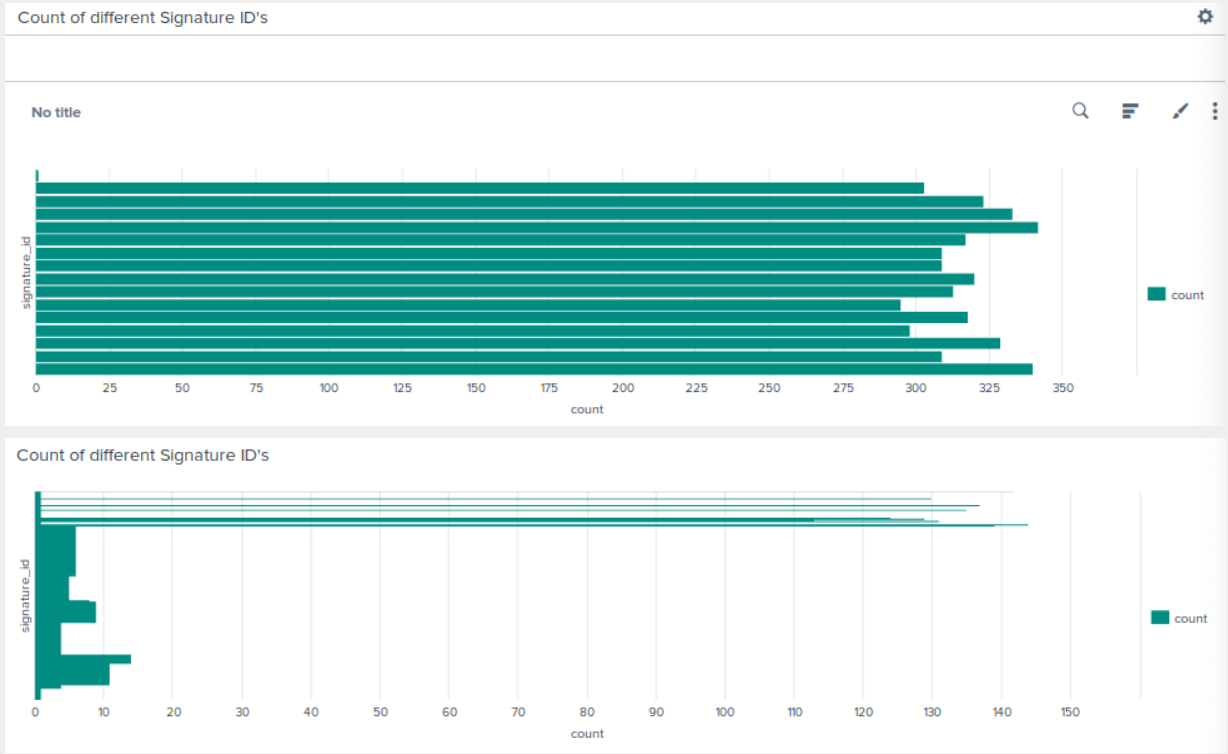
- What is the peak count of the different users?

984 for user A and 1256 for user K.

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

- Does anything stand out as suspicious?

Between 1am and 3am we witnessed a spike in incidents where a user account was locked out. At 1am there were 805 incidents reported, at 2am there were 896 incidents reported. Also, the number of unique signatures has increased, but their individual frequencies are now lower than they were previously



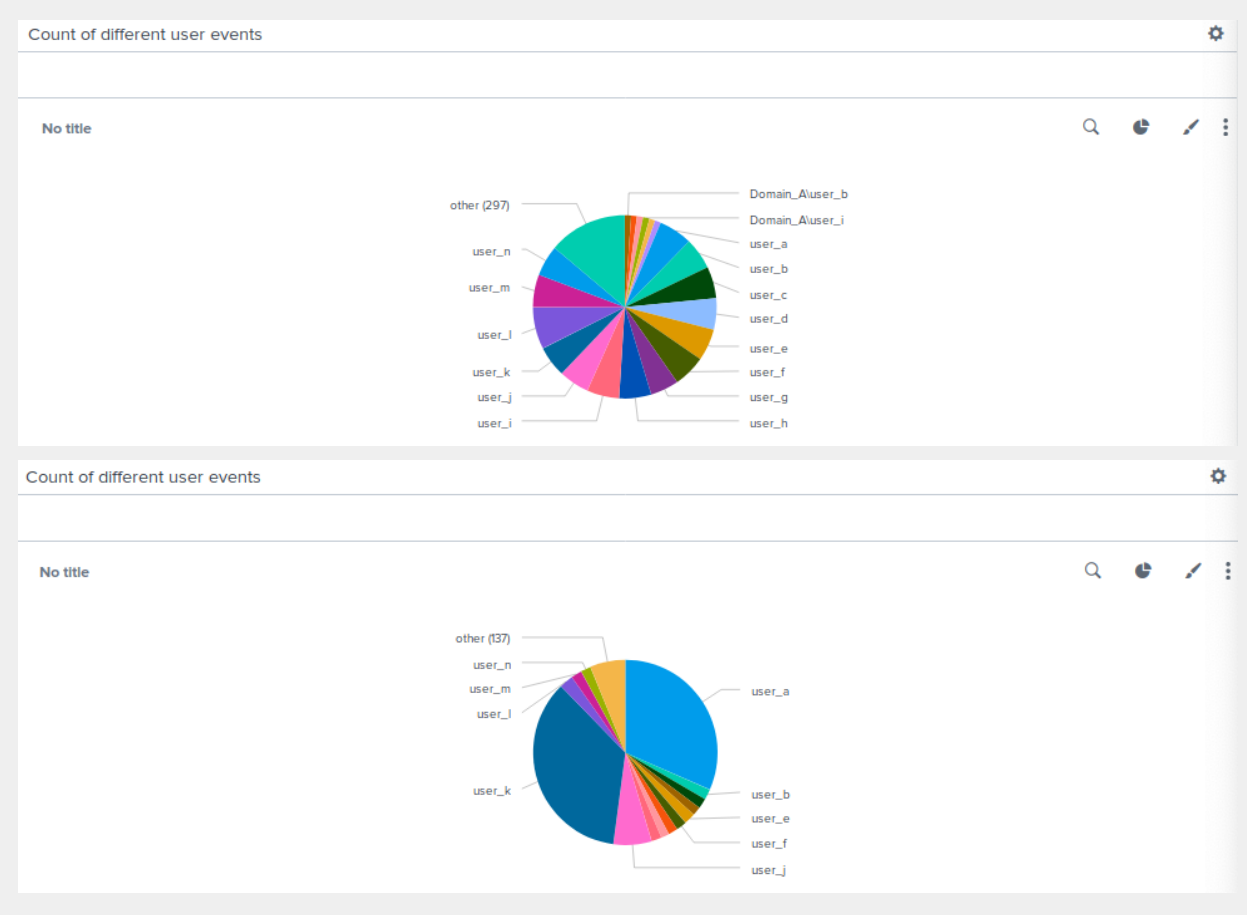
- Do the results match your findings in your time chart for signatures?

No

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

- Does anything stand out as suspicious?

The pie charts reveal a clear suspicion: prior to the attack, the distribution of user events was fairly even among all users, but after the attack, User K and User A exhibited a disproportionately large share of the total counts.



- 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?

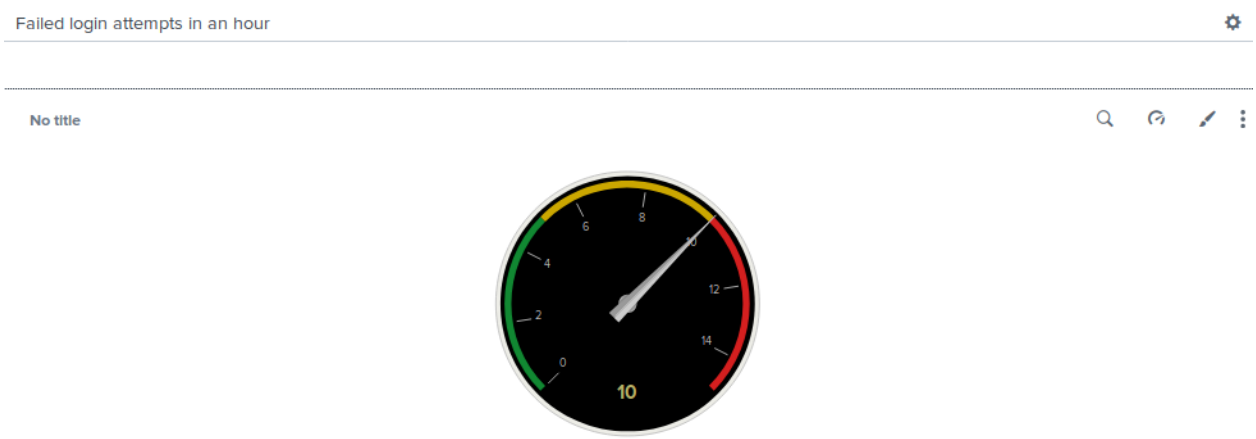
```
Advantages of the Pie Chart Over the Line Chart:

    • better at displaying the proportion or percentage of different categories
    • easier to interpret and compare the relative size of different categories or parts
    • quickly show the biggest or smallest category
    • suitable for presenting simple data sets

Disadvantages of the Pie Chart Over the Line Chart:

    • not able to display trends over time
    • less effective at showing changes or trends in data over time
    • can be harder to accurately read exact values or counts
```

- not suitable for more complex data sets with many categories or data points

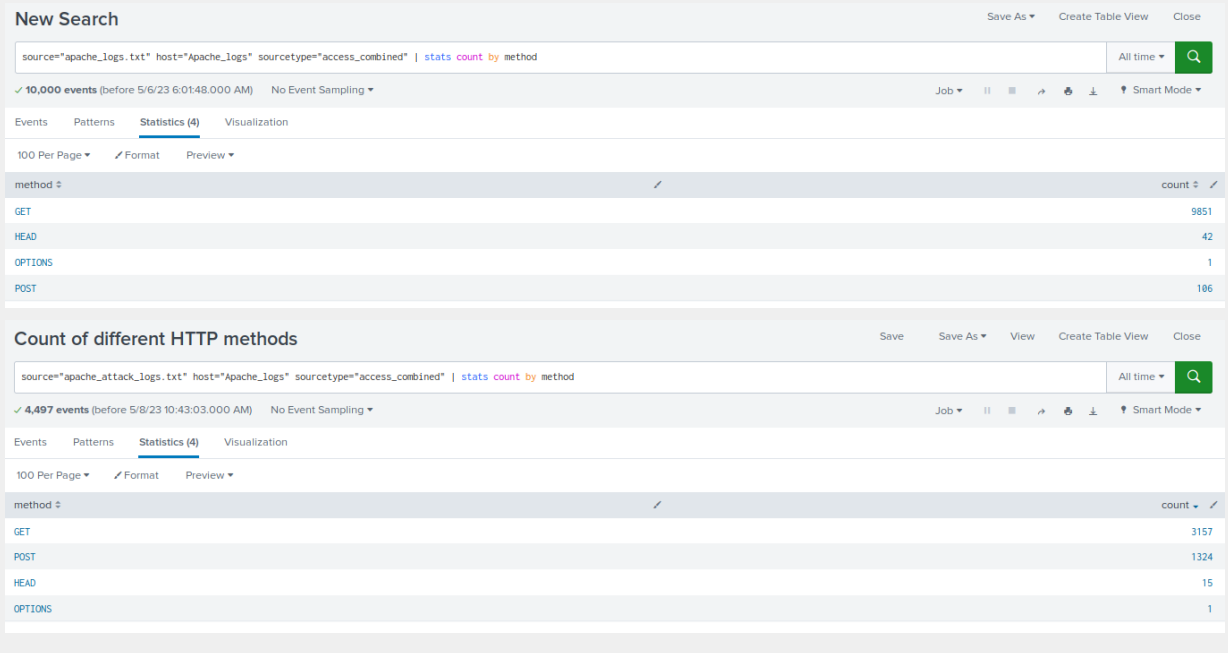


Apache Web Server Log Questions

Report Analysis for Methods

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

GET methods decreased by 6694, HEAD method decreased by 27 events and POST method increased dramatically by 1218 events



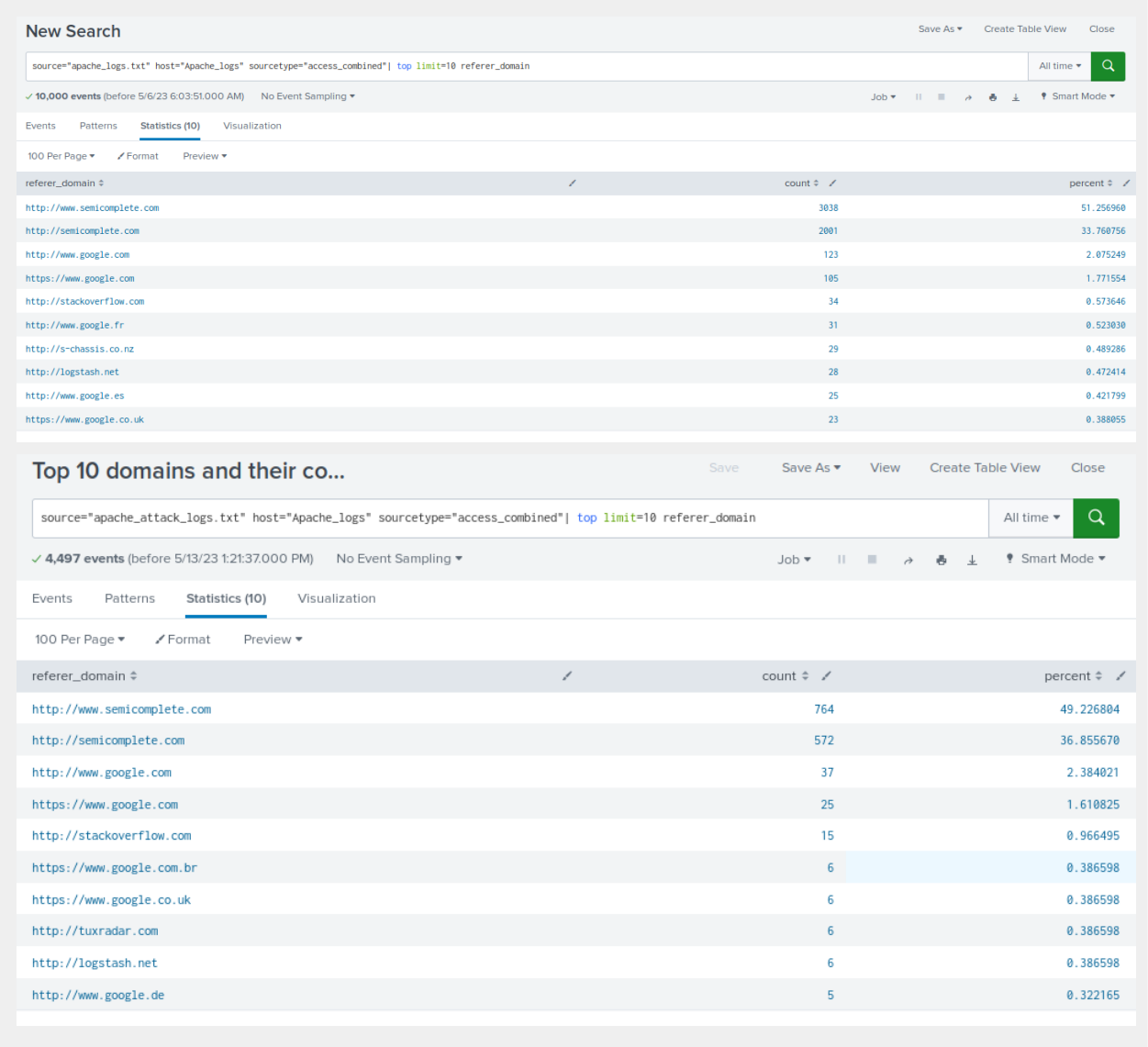
- What is that method used for?

  - GET method is used to retrieve information from a server. It is commonly used to read data from a web page.
  - HEAD method is similar to GET, but it only retrieves the header information of the requested resource, without actually transferring the data. It is useful for checking the status of a resource or verifying its existence.
  - POST method is used to submit data to be processed by a server. It is commonly used to create or update resources on a web server, such as submitting a form or uploading a file.

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

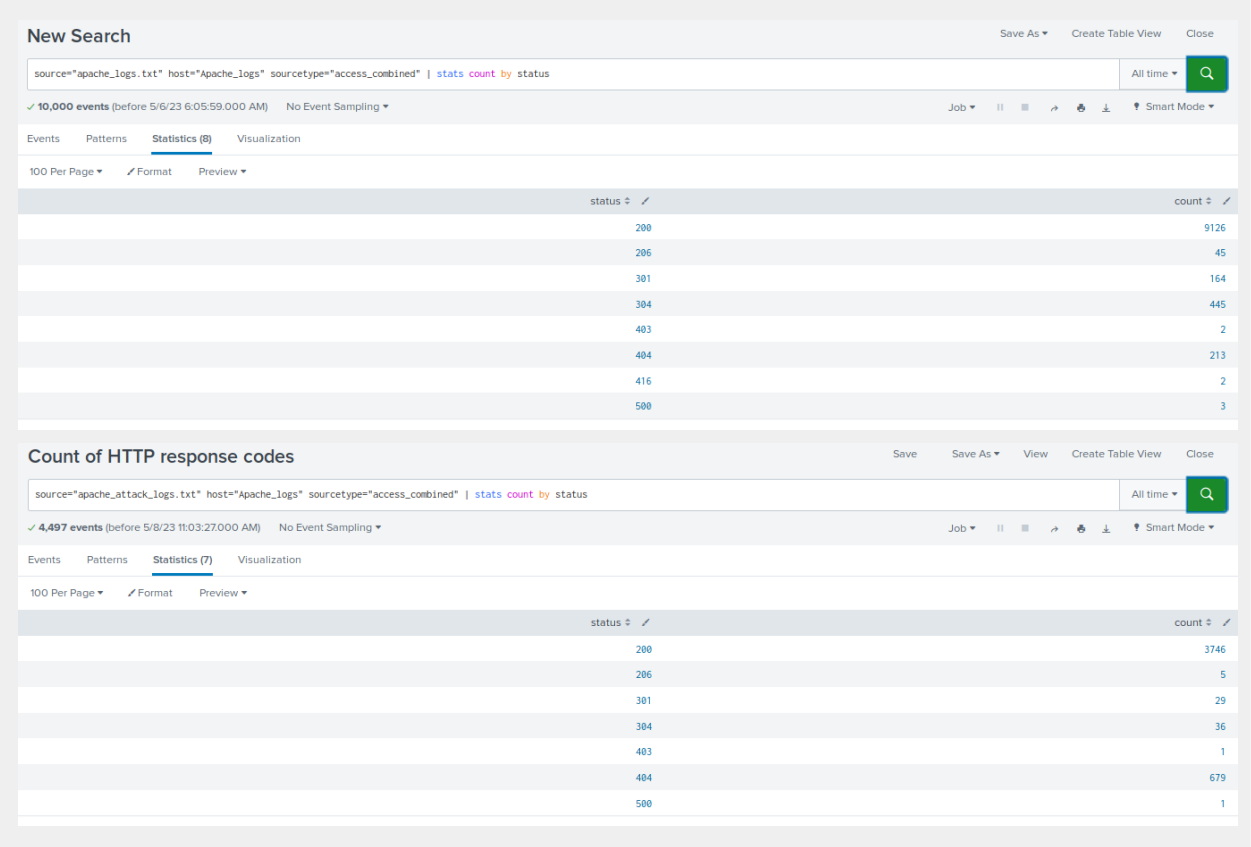
Although the actual count for each domain drastically decreased, the top 5 domains remained the same, and their percentage share of the event count stayed relatively close to how it was before the cyber attack. For example, the top domain, http://www.semicomplete.com, experienced a significant decrease in event count, dropping from 3038 events to 764 events.



Report Analysis for HTTP Response Codes

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

During the simulated cyber attack, there was a significant decrease in the number of events with a 200 response code, indicating a successful request, with a decrease of 5380 events for code 200 and 40 events for code 206. Similarly, the number of events with a 300 response code, indicating a redirection to a different resource, also decreased, with a decrease of 135 events for code 301 and 409 events for code 304. However, it's worth noting that the number of events with a 404 response code, indicating that the requested resource could not be found on the server, increased substantially, with an increase of 466 events.



Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

There was a significant decline in user activity within France following the attack. Prior to the attack, the normal range of traffic count was between 15 and 79. However, after the attack, the number of user events from France dropped to single digits during most time periods.

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

There was a decrease in the number of user events during most hours, but two hours stood out in particular. At midnight after the attack, there were only three user events compared to 24 before the attack. Additionally, at 6am, the number of user events dropped from 41 to 6.

- Would your alert be triggered for this activity?

The alert would not have triggered this suspicious activity as we set a threshold to be anything greater than 44. We chose this as our baseline was 40.

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

```
Yes, the threshold should be changed to allow for an alert to be set when there is less traffic than usual as well, our alert was set to when the traffic was much higher than usual.
```

Alert Analysis for HTTP POST Activity

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

```
Yes, there was a large volume of POST responses at 20:00. The usual activity is within the single digits. The activity at 20:00 was well above 1000.
```

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

```
At 20:00 the count was 1296
```

- When did it occur?

```
This occurred at 8pm
```

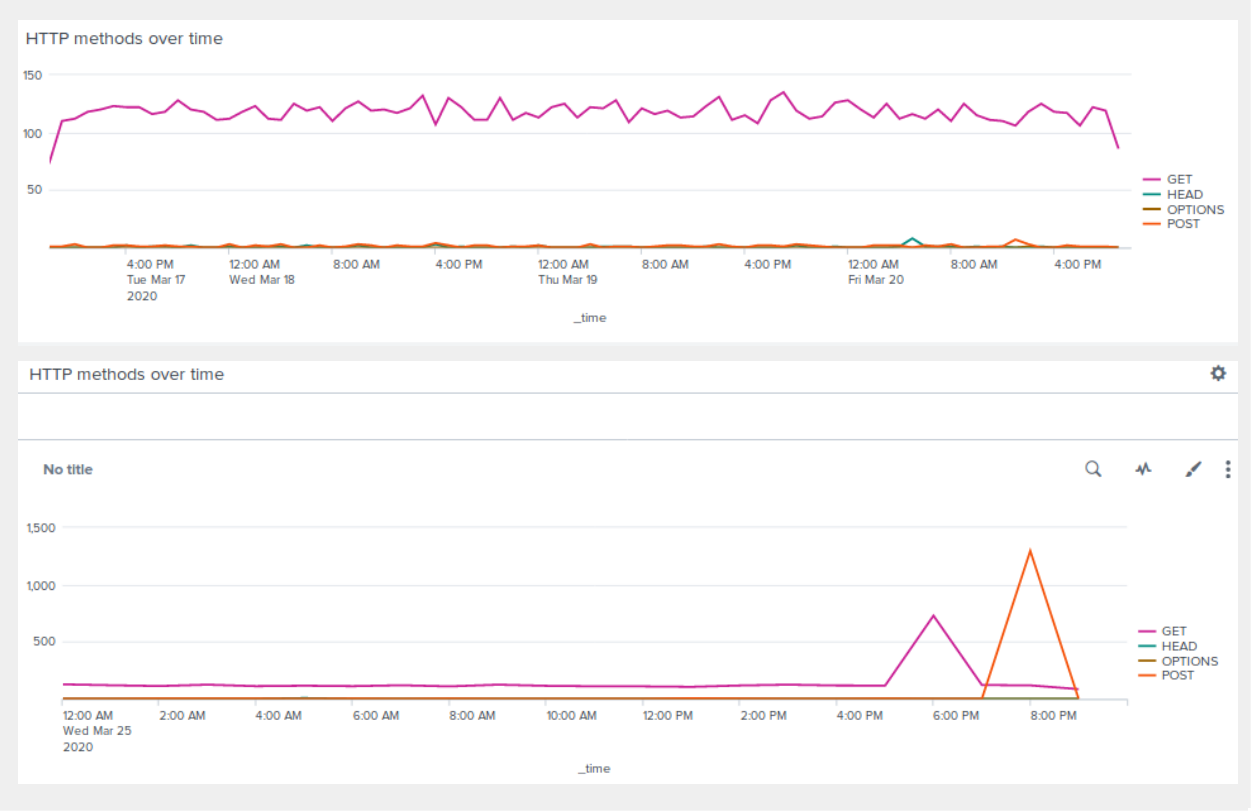
- After reviewing, would you change the threshold that you previously selected?

```
No we wouldn't because we set an alert threshold to be triggered if the count reached greater than 6, which we determined because a baseline for normal behaviour was 4. Anything over this we would be alerted to and we would have been alerted to the suspicious behaviour which was picked up above.
```

Dashboard Analysis for Time Chart of HTTP Methods - CHLOE

- Does anything stand out as suspicious?

```
There was a spike in GET responses at 6pm and there was also a spike in POST responses at 8pm
```



- Which method seems to be used in the attack?

```
The POST method appears to be used for the attack.
```

- At what times did the attack start and stop?

```
The attack appears to have begun at 7pm and finished at 9pm.
```

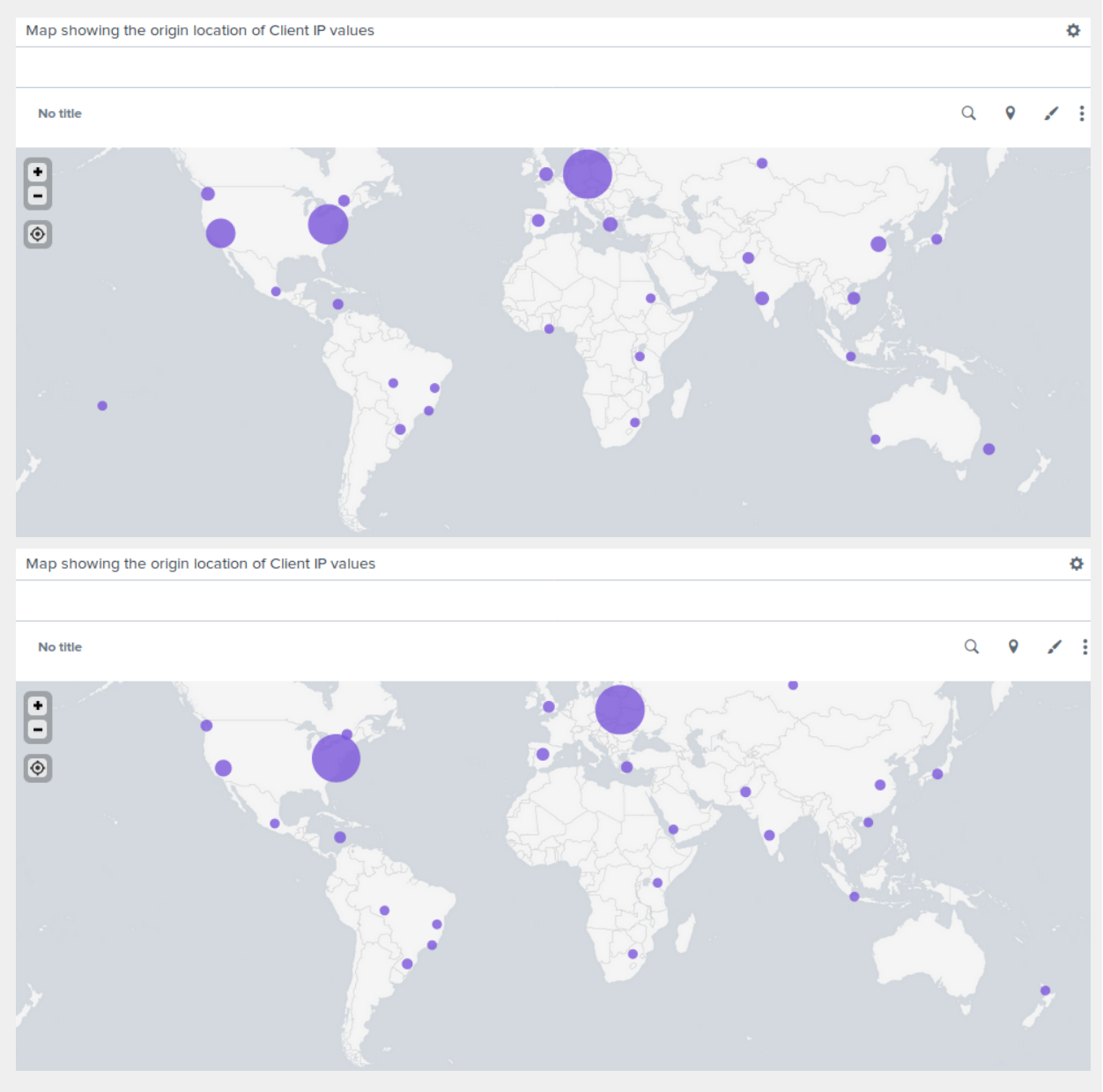
- What is the peak count of the top method during the attack?

```
The peak of the POST method was at 1296.
```

Dashboard Analysis for Cluster Map

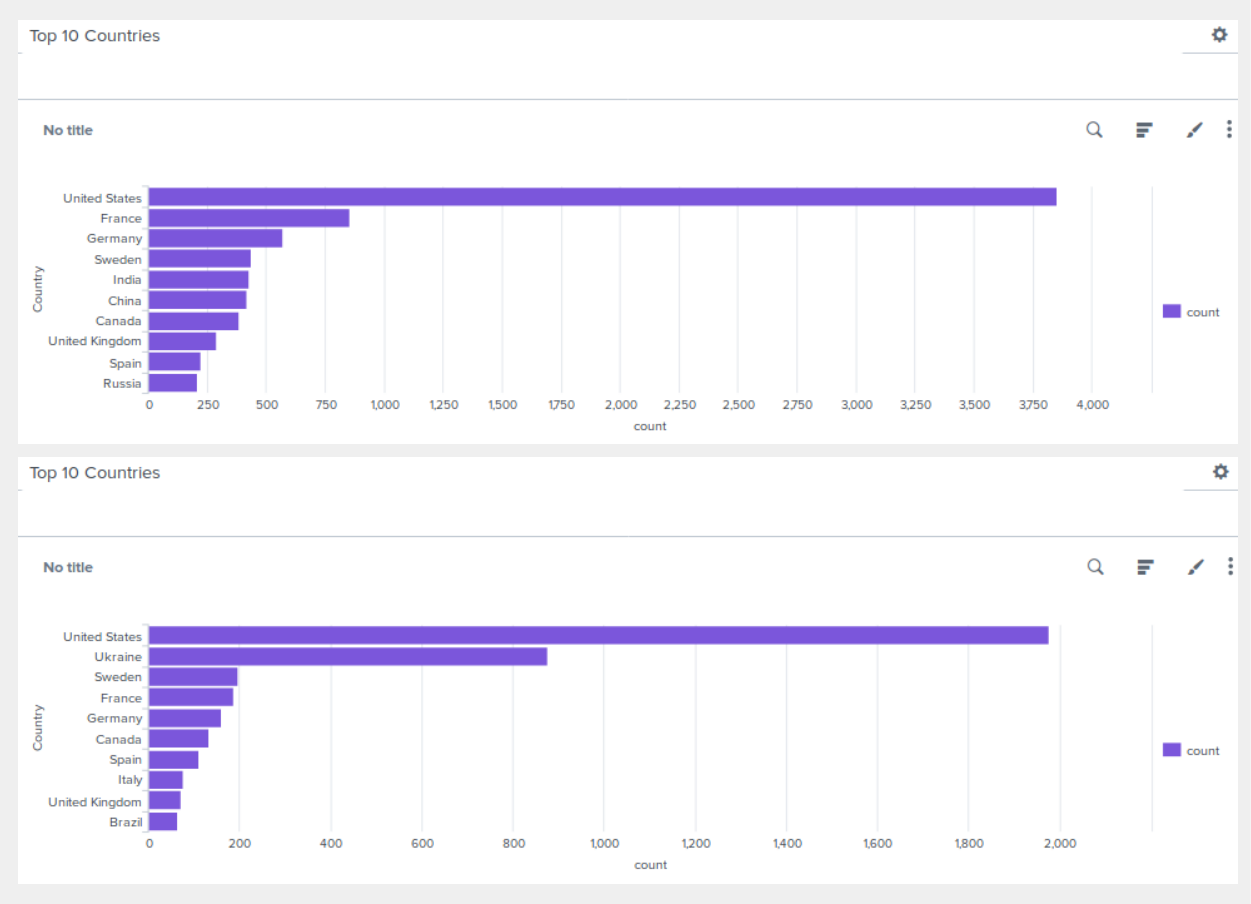
- Does anything stand out as suspicious?

```
There was a major worldwide decline in activity. The counts for each place within the
cluster map reduced significantly.
```



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

```
Kiev, Ukraine has a high volume of activity from the cluster map, which it did not have before.
```



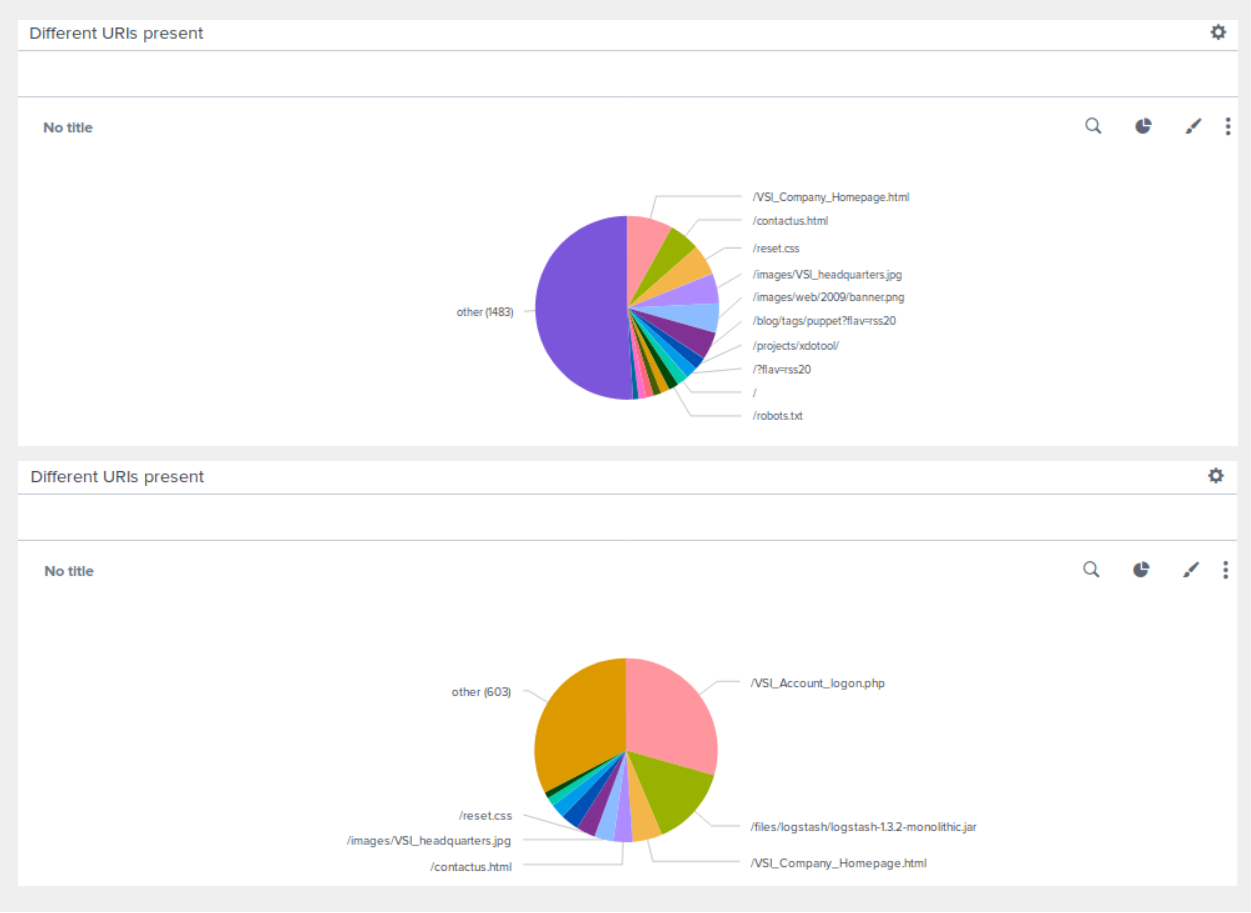
- What is the count of that city?

```
439 is the count of Kiev, Ukraine.
```

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

```
There were changes to the count in two of the URI's compared to normal activity. They were
visited much more frequently than normal.They are depicted in the pie chart below
```

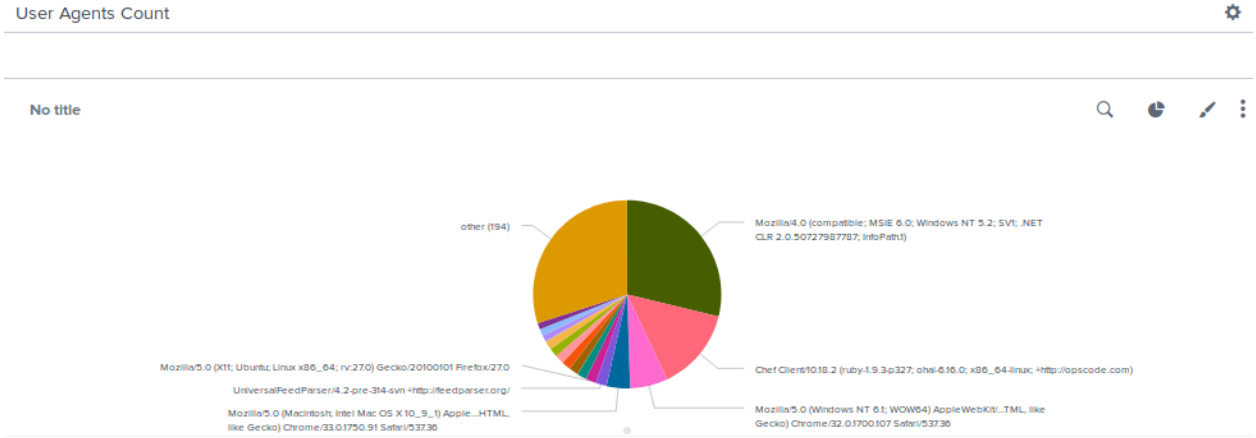


- What URI is hit the most?

```
/VSI_Account_logon.php
```

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

```
The attacker could potentially be brute forcing login credentials to gain access into the company.
```



Count of 404 status at specific time

No title